Panduan Developer

AWS WAF, AWS Firewall Manager, dan AWS Shield Advanced

AWS WAF, AWS Firewall Manager, dan AWS Shield Advanced: Panduan Developer

Table of Contents

Apa itu AWS WAF, AWS Shield Advanced;, dan AWS Firewall Manager?

Anda dapat menggunakanAWS WAF,AWS Shield, dan AWS Firewall Manager bersama-sama untuk membuat solusi keamanan yang komprehensif. AWS WAF adalah firewall aplikasi web yang dapat Anda gunakan untuk memantau permintaan web yang dikirim pengguna akhir Anda ke aplikasi Anda dan untuk mengontrol akses ke konten Anda. Shield Advanced memberikan perlindungan terhadap serangan distributed denial of service (DDoS) untuk AWS sumber daya, pada lapisan jaringan dan transport (lapisan 3 dan 4) dan lapisan aplikasi (layer 7). AWS Firewall Manager menyediakan pengelolaan perlindungan seperti AWS WAF dan Shield Advanced di seluruh akun dan sumber daya, bahkan saat sumber daya baru ditambahkan.

Topik

Apa itu AWS WAF?

AWS WAF adalah firewall aplikasi web yang memungkinkan Anda memantau permintaan HTTP dan HTTPS yang diteruskan ke sumber daya aplikasi web Anda yang dilindungi. Anda dapat melindungi jenis sumber daya berikut:

- CloudFront Distribusi Amazon
- API REST Amazon API Gateway
- Penyeimbang Beban Aplikasi
- AWS AppSync GraphQL API
- Kolam pengguna Amazon Cognito
- AWS App Runner layanan
- AWS Instans Akses Terverifikasi

AWS WAF memungkinkan Anda mengontrol akses ke konten Anda. Berdasarkan kondisi yang Anda tentukan, seperti alamat IP tempat permintaan berasal atau nilai string kueri, sumber daya yang

dilindungi merespons permintaan baik dengan konten yang diminta, dengan kode status HTTP 403 (Terlarang), atau dengan respons khusus.

Pada tingkat yang paling sederhana, AWS WAF memungkinkan Anda memilih salah satu perilaku berikut:

- Izinkan semua permintaan kecuali yang Anda tentukan — Ini berguna saat Anda ingin Amazon CloudFront, Amazon API Gateway, Application Load Balancer, AWS AppSync, Amazon Cognito, AWS App Runner, AWS atau Akses Terverifikasi untuk menayangkan konten untuk situs web publik, tetapi Anda juga ingin memblokir permintaan dari penyerang.
- Blokir semua permintaan kecuali yang Anda tentukan — Ini berguna ketika Anda ingin menyajikan konten untuk situs web terbatas yang penggunanya mudah diidentifikasi oleh properti dalam permintaan web, seperti alamat IP yang mereka gunakan untuk menjelajah ke situs web.
- Hitung permintaan yang sesuai dengan kriteria Anda — Anda dapat menggunakan Count tindakan untuk melacak lalu lintas web Anda tanpa mengubah cara Anda menanganinya. Anda dapat menggunakan ini untuk pemantauan umum dan juga untuk menguji aturan penanganan permintaan web baru Anda. Saat Anda ingin mengizinkan atau memblokir permintaan berdasarkan properti baru dalam permintaan web, Anda dapat mengonfigurasi terlebih dahulu AWS WAF untuk menghitung permintaan yang cocok dengan properti tersebut. Ini memungkinkan Anda mengonfirmasi pengaturan konfigurasi baru sebelum mengganti aturan untuk mengizinkan atau memblokir permintaan yang cocok.
- Jalankan CAPTCHA atau tantang pemeriksaan terhadap permintaan yang sesuai dengan kriteria Anda — Anda dapat menerapkan CAPTCHA dan kontrol tantangan senyap terhadap permintaan untuk membantu mengurangi lalu lintas bot ke sumber daya yang dilindungi.

Menggunakan AWS WAF memiliki beberapa manfaat:

- Perlindungan tambahan terhadap serangan web menggunakan kriteria yang Anda tentukan. Anda dapat menentukan kriteria menggunakan karakteristik permintaan web seperti berikut ini:
  - Alamat IP tempat permintaan berasal.
  - Negara tempat permintaan berasal.
  - Nilai dalam header permintaan.
  - String yang muncul dalam permintaan, baik string atau string tertentu yang cocok dengan pola ekspresi reguler (regex).
  - Panjang permintaan.

  - Adanya kode SQL yang cenderung berbahaya (dikenal sebagai injeksi SQL).
  - Kehadiran skrip yang cenderung berbahaya (dikenal sebagai cross-site scripting).
- Aturan yang memungkinkan, memblokir, atau menghitung permintaan web yang memenuhi kriteria yang ditentukan. Atau, aturan dapat memblokir atau menghitung permintaan web yang tidak hanya memenuhi kriteria yang ditentukan, tetapi juga melebihi jumlah permintaan tertentu dalam satu menit atau dalam lima menit.
- Aturan yang dapat Anda gunakan kembali untuk beberapa aplikasi web.
- Grup aturan terkelola dari AWS dan AWS Marketplace penjual.
- Metrik waktu nyata dan permintaan web sampel.
- Administrasi otomatis menggunakan AWS WAF API.

Jika Anda ingin kontrol terperinci atas perlindungan yang Anda tambahkan ke sumber daya Anda, AWS WAF sendirian mungkin merupakan pilihan yang tepat. Untuk informasi lebih lanjut tentang AWS WAF, lihatAWS WAF.

Apa itu AWS Shield Advanced?

Anda dapat menggunakan daftar kontrol akses AWS WAF web (web ACL) untuk membantu meminimalkan efek serangan Distributed Denial of Service (DDoS). Untuk perlindungan tambahan terhadap serangan DDoS, AWS juga menyediakan AWS Shield Standard dan AWS Shield Advanced. AWS Shield Standard secara otomatis disertakan tanpa biaya tambahan di luar apa yang sudah Anda bayar AWS WAF dan AWS layanan Anda yang lain.

Shield Advanced menyediakan perlindungan serangan DDoS yang diperluas untuk instans Amazon EC2, penyeimbang beban Elastic Load Balancing CloudFront , distribusi, zona host Route 53, dan akselerator standar. AWS Global Accelerator Shield Advanced dikenakan biaya tambahan. Opsi dan fitur Shield Advanced mencakup mitigasi DDoS lapisan aplikasi otomatis, visibilitas acara lanjutan, dan dukungan khusus dari Shield Response Team (SRT). Jika Anda memiliki situs web dengan visibilitas tinggi atau rentan terhadap serangan DDoS yang sering terjadi, pertimbangkan untuk membeli perlindungan tambahan yang disediakan Shield Advanced. Untuk informasi tambahan, lihat AWS Shield Advanced kemampuan dan opsi danMemutuskan apakah akan berlangganan AWS Shield Advanced dan menerapkan perlindungan tambahan.

Apa itu AWS Firewall Manager?

AWS Firewall Manager menyederhanakan tugas administrasi dan pemeliharaan Anda di beberapa akun dan sumber daya untuk berbagai perlindungan, termasuk AWS WAF, grup keamanan AWS Shield Advanced Amazon VPC dan ACL jaringan, serta Amazon Route 53 Resolver AWS Network Firewall DNS Firewall. Dengan Firewall Manager, Anda mengatur perlindungan hanya sekali dan layanan secara otomatis menerapkannya di seluruh akun dan sumber daya Anda, bahkan saat Anda menambahkan akun dan sumber daya baru.

Untuk informasi selengkapnya tentang Firewall Manager, lihatAWS Firewall Manager.

Menyiapkan akun Anda untuk menggunakan layanan

Topik ini menjelaskan langkah-langkah awal, seperti membuat akun, mempersiapkan Anda untuk menggunakan AWS WAF AWS Firewall Manager, dan AWS Shield Advanced. Anda tidak dikenakan biaya untuk item awal ini. Anda hanya dikenakan biaya untuk AWS layanan yang Anda gunakan.

Topik

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/signup.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan mengunjungi https://aws.amazon.com/ dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

   Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.
2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .
2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

  Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuknya, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.
2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

Unduh alat

AWS Management Console Termasuk konsol untuk AWS WAF,, dan AWS Shield Advanced AWS Firewall Manager, tetapi jika Anda ingin mengakses layanan secara terprogram, lihat berikut ini:

- Panduan API mendokumentasikan operasi yang didukung layanan dan menyediakan tautan ke dokumentasi SDK dan CLI terkait:
  - AWS WAF Referensi API
  - AWS Shield Advanced Referensi API
  - AWS Firewall Manager Referensi API
- Untuk memanggil API tanpa harus menangani detail tingkat rendah seperti merakit permintaan HTTP mentah, Anda dapat menggunakan SDK. AWS AWS SDK menyediakan fungsi dan tipe data yang merangkum fungsionalitas layanan. AWS Untuk mengunduh AWS SDK dan mengakses petunjuk penginstalan, lihat halaman yang berlaku:
  - Java
  - JavaScript
  - .NET
  - Node.js
  - PHP
  - Python
  - Ruby

  Untuk daftar lengkap AWS SDK, lihat Alat untuk Amazon Web Services.

- Anda dapat menggunakan AWS Command Line Interface (AWS CLI) untuk mengontrol beberapa AWS layanan dari baris perintah. Anda juga dapat mengotomatiskan perintah Anda menggunakan skrip. Untuk informasi selengkapnya, lihat AWS Command Line Interface.
- AWS Tools for Windows PowerShell mendukung AWS layanan ini. Untuk informasi selengkapnya, lihat AWS Tools for PowerShell Referensi Cmdlet.

AWS WAF

AWS WAF adalah firewall aplikasi web yang memungkinkan Anda memantau permintaan HTTP (S) yang diteruskan ke sumber daya aplikasi web Anda yang dilindungi. Anda dapat melindungi jenis sumber daya berikut:

- CloudFront Distribusi Amazon
- API REST Amazon API Gateway
- Penyeimbang Beban Aplikasi
- AWS AppSync GraphQL API
- Kolam pengguna Amazon Cognito
- AWS App Runner layanan
- AWS Contoh Akses Terverifikasi

AWS WAF memungkinkan Anda mengontrol akses ke konten Anda. Berdasarkan kriteria yang Anda tentukan, seperti alamat IP tempat permintaan berasal atau nilai string kueri, layanan yang terkait dengan sumber daya yang dilindungi merespons permintaan baik dengan konten yang diminta, dengan kode status HTTP 403 (Terlarang), atau dengan respons khusus.

> **Note**
>
> Anda juga dapat menggunakan AWS WAF untuk melindungi aplikasi Anda yang di-host di wadah Amazon Elastic Container Service (Amazon ECS). Amazon ECS adalah layanan manajemen kontainer yang sangat skalabel dan cepat yang memudahkan untuk menjalankan, menghentikan, dan mengelola kontainer Docker di cluster. Untuk menggunakan opsi ini, Anda mengonfigurasi Amazon ECS untuk menggunakan Application Load Balancer yang diaktifkan AWS WAF untuk merutekan dan melindungi lalu lintas HTTP (S) layer 7 di seluruh tugas dalam layanan Anda. Untuk informasi selengkapnya, lihat Service Load Balancing di Panduan Pengembang Layanan Amazon Elastic Container.

Topik

- AWS WAF daftar kontrol akses web (ACL web)
- AWS WAF kelompok aturan
- AWS WAF aturan
- Penanganan komponen permintaan kebesaran di AWS WAF
- Pencocokan pola ekspresi reguler di AWS WAF
- Set IP dan set pola regex di AWS WAF
- Permintaan dan tanggapan web yang disesuaikan di AWS WAF
- AWS WAF label pada permintaan web
- AWS WAF mitigasi ancaman cerdas
- Pencatatan AWS WAF lalu lintas ACL web
- Menguji dan menyetel perlindungan Anda AWS WAF
- Cara AWS WAF bekerja dengan CloudFront fitur Amazon
- Keamanan dalam penggunaan AWS WAF layanan Anda
- AWS WAF kuota
- Memigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF

Bagaimana cara AWS WAF kerja

Anda gunakan AWS WAF untuk mengontrol bagaimana sumber daya yang dilindungi merespons permintaan web HTTP (S). Anda melakukan ini dengan mendefinisikan daftar kontrol akses web (ACL) dan kemudian mengaitkannya dengan satu atau lebih sumber daya aplikasi web yang ingin Anda lindungi. Sumber daya terkait meneruskan permintaan masuk AWS WAF untuk diperiksa oleh ACL web.

Di ACL web Anda, Anda membuat aturan untuk menentukan pola lalu lintas yang akan dicari dalam permintaan dan menentukan tindakan yang akan diambil pada permintaan yang cocok. Pilihan tindakan meliputi yang berikut:

- Izinkan permintaan untuk pergi ke sumber daya yang dilindungi untuk diproses dan direspon.
- Blokir permintaan.
- Hitung permintaan.
- Jalankan CAPTCHA atau tantang pemeriksaan terhadap permintaan untuk memverifikasi pengguna manusia dan penggunaan browser standar.

AWS WAF komponen

Berikut ini adalah komponen utama dari AWS WAF:

- Web ACL — Anda menggunakan daftar kontrol akses web (ACL) untuk melindungi sekumpulan sumber daya. AWS Anda membuat ACL web dan menentukan strategi perlindungannya dengan menambahkan aturan. Aturan menentukan kriteria untuk memeriksa permintaan web dan menentukan tindakan yang akan diambil pada permintaan yang sesuai dengan kriteria mereka. Anda juga menetapkan tindakan default untuk ACL web yang menunjukkan apakah akan memblokir atau mengizinkan melalui permintaan apa pun yang aturan belum diblokir atau diizinkan. Untuk informasi selengkapnya tentang ACL web, lihatAWS WAF daftar kontrol akses web (ACL web).

  Web ACL adalah AWS WAF sumber daya.
- Aturan — Setiap aturan berisi pernyataan yang mendefinisikan kriteria inspeksi, dan tindakan yang harus diambil jika permintaan web memenuhi kriteria. Ketika permintaan web memenuhi kriteria, itu cocok. Anda dapat mengonfigurasi aturan untuk memblokir permintaan yang cocok, mengizinkannya melalui, menghitungnya, atau menjalankan kontrol bot terhadap mereka yang menggunakan teka-teki CAPTCHA atau tantangan browser klien senyap. Untuk informasi selengkapnya tentang aturan, lihatAWS WAF aturan.

  Aturan bukanlah sumber AWS WAF daya. Itu hanya ada dalam konteks ACL web atau grup aturan.
- Grup aturan - Anda dapat menentukan aturan langsung di dalam ACL web atau dalam grup aturan yang dapat digunakan kembali. AWS Aturan dan AWS Marketplace penjual terkelola menyediakan grup aturan terkelola untuk Anda gunakan. Anda juga dapat menentukan grup aturan Anda sendiri. Untuk informasi selengkapnya tentang grup aturan, lihatAWS WAF kelompok aturan.

  Kelompok aturan adalah sumber AWS WAF daya.

Topik

- AWS WAF unit kapasitas ACL web (WCU)
- Sumber daya yang dapat Anda lindungi dengan AWS WAF

AWS WAF unit kapasitas ACL web (WCU)

AWS WAF menggunakan unit kapasitas ACL web (WCU) untuk menghitung dan mengontrol sumber daya operasi yang diperlukan untuk menjalankan aturan, grup aturan, dan ACL web Anda. AWS

WAF memberlakukan batas WCU saat Anda mengonfigurasi grup aturan dan ACL web. WCU tidak memengaruhi cara AWS WAF memeriksa lalu lintas web.

AWS WAF mengelola kapasitas untuk aturan, grup aturan, dan ACL web.

Aturan WCU

AWS WAF menghitung kapasitas aturan saat Anda membuat atau memperbarui aturan. AWS WAF menghitung kapasitas secara berbeda untuk setiap jenis aturan, untuk mencerminkan biaya relatif masing-masing aturan. Aturan sederhana dengan biaya sedikit untuk menjalankan menggunakan lebih sedikit WCU daripada aturan lebih kompleks yang menggunakan lebih banyak kekuatan pemrosesan. Misalnya, pernyataan aturan batasan ukuran menggunakan WCU lebih sedikit daripada pernyataan yang memeriksa permintaan menggunakan kumpulan pola regex.

Persyaratan kapasitas aturan umumnya dimulai dengan biaya dasar untuk jenis aturan dan meningkat dengan kompleksitas, misalnya, ketika Anda menambahkan transformasi teks sebelum inspeksi atau jika Anda memeriksa badan JSON. Untuk informasi tentang persyaratan kapasitas aturan, lihat daftar untuk pernyataan aturan diDasar-dasar pernyataan aturan.

Kelompok aturan WCU

Persyaratan WCU untuk grup aturan ditentukan oleh aturan yang Anda tentukan di dalam grup aturan. Kapasitas maksimum untuk kelompok aturan adalah 5.000 WCU.

Setiap kelompok aturan memiliki pengaturan kapasitas yang tidak dapat diubah, yang diberikan pemilik pada saat pembuatan. Ini berlaku untuk grup aturan terkelola dan grup aturan yang Anda buat AWS WAF. Saat Anda memodifikasi grup aturan, perubahan Anda harus menjaga WCU grup aturan dalam kapasitasnya. Ini memastikan bahwa ACL web yang menggunakan grup aturan tetap dalam persyaratan kapasitasnya.

WCU yang digunakan dalam grup aturan adalah jumlah WCU untuk aturan dikurangi pengoptimalan pemrosesan apa pun yang dapat AWS WAF diperoleh dengan menggabungkan perilaku aturan. Misalnya, jika Anda mendefinisikan dua aturan untuk memeriksa komponen permintaan web yang sama, dan aturan masing-masing menerapkan transformasi tertentu ke komponen sebelum memeriksanya, AWS WAF mungkin dapat menagih Anda sekali saja untuk menerapkan transformasi. Biaya WCU untuk menggunakan grup aturan di ACL web selalu merupakan pengaturan WCU tetap yang Anda tentukan pada pembuatan grup aturan.

Saat Anda membuat grup aturan, berhati-hatilah untuk mengatur kapasitas yang cukup tinggi untuk mengakomodasi aturan yang ingin Anda gunakan selama masa pakai grup aturan.

Web ACL WCU

Persyaratan WCU untuk ACL web ditentukan oleh aturan dan grup aturan yang Anda gunakan di dalam ACL web.

- Biaya menggunakan grup aturan di ACL web adalah pengaturan kapasitas grup aturan.
- Biaya penggunaan aturan adalah WCU yang dihitung aturan dikurangi pengoptimalan pemrosesan apa pun yang dapat AWS WAF diperoleh dari kombinasi aturan ACL web. Misalnya, jika Anda mendefinisikan dua aturan untuk memeriksa komponen permintaan web yang sama, dan aturan masing-masing menerapkan transformasi tertentu ke komponen sebelum memeriksanya, AWS WAF mungkin dapat menagih Anda sekali saja untuk menerapkan transformasi.

Harga dasar untuk ACL web mencakup hingga 1.500 WCU. Menggunakan lebih dari 1.500 WCU menimbulkan biaya tambahan, menurut model harga berjenjang. AWS WAF secara otomatis menyesuaikan harga ACL web Anda saat penggunaan ACL WCU web Anda berubah. Untuk detail harga, lihat AWS WAF Harga.

Kapasitas maksimum untuk ACL web adalah 5.000 WCU.

Menentukan WCU untuk grup aturan atau web ACL

Seperti disebutkan di bagian sebelumnya, total WCU yang digunakan dalam grup aturan atau ACL web akan sama dengan atau kurang dari jumlah WCU untuk semua aturan yang didefinisikan dalam grup aturan atau ACL web.

Di AWS WAF konsol, Anda dapat melihat kapasitas yang dikonsumsi saat menambahkan aturan ke ACL web atau grup aturan. Konsol menampilkan unit kapasitas saat ini yang digunakan saat Anda menambahkan aturan.

Melalui API, Anda dapat memeriksa persyaratan kapasitas maksimum untuk aturan yang ingin Anda gunakan di ACL web atau grup aturan. Untuk melakukan ini, berikan daftar aturan JSON ke panggilan kapasitas cek. Untuk informasi selengkapnya, lihat CheckCapacitydi Referensi API AWS WAF V2.

Sumber daya yang dapat Anda lindungi dengan AWS WAF

Anda dapat menggunakan ACL AWS WAF web untuk melindungi jenis sumber daya global atau regional. Anda melakukan ini dengan mengaitkan ACL web dengan sumber daya yang ingin Anda lindungi. ACL web dan AWS WAF sumber daya apa pun yang digunakannya harus ditempatkan di

Wilayah tempat sumber daya terkait berada. Untuk CloudFront distribusi Amazon, ini diatur ke US East (Virginia N.).

CloudFront Distribusi Amazon

Anda dapat mengaitkan ACL AWS WAF web dengan CloudFront distribusi menggunakan AWS WAF konsol atau API. Anda juga dapat mengaitkan ACL web dengan CloudFront distribusi saat Anda membuat atau memperbarui distribusi itu sendiri. Untuk mengonfigurasi asosiasi di AWS CloudFormation, Anda harus menggunakan konfigurasi CloudFront distribusi. Untuk informasi tentang Amazon CloudFront, lihat Menggunakan AWS WAF untuk Mengontrol Akses ke Konten Anda di Panduan CloudFront Pengembang Amazon.

AWS WAF tersedia secara global untuk CloudFront distribusi, tetapi Anda harus menggunakan Wilayah AS Timur (Virginia N.) untuk membuat ACL web Anda dan sumber daya apa pun yang digunakan dalam ACL web, seperti grup aturan, set IP, dan set pola regex. Beberapa antarmuka menawarkan pilihan wilayah “Global (CloudFront)”. Memilih ini identik dengan memilih Wilayah AS Timur (Virginia N.) atau "us-east-1”.

Sumber daya regional

Anda dapat melindungi sumber daya regional di semua Wilayah jika AWS WAF tersedia. Anda dapat melihat daftar di AWS WAF titik akhir dan kuota di. Referensi Umum Amazon Web

Anda dapat menggunakan AWS WAF untuk melindungi jenis sumber daya regional berikut:

- API REST Amazon API Gateway
- Penyeimbang Beban Aplikasi
- AWS AppSync GraphQL API
- Kolam pengguna Amazon Cognito
- AWS App Runner layanan
- AWS Contoh Akses Terverifikasi

Anda hanya dapat mengaitkan ACL web ke Application Load Balancer yang ada di dalamnya. Wilayah AWS Misalnya, Anda tidak dapat mengaitkan ACL web ke Application Load Balancer yang aktif. AWS Outposts

ACL web dan AWS WAF sumber daya lain yang digunakannya harus berada di Wilayah yang sama dengan sumber daya yang dilindungi. Saat memantau dan mengelola permintaan web untuk sumber

daya regional yang dilindungi, AWS WAF simpan semua data di Wilayah yang sama dengan sumber daya yang dilindungi.

Pembatasan pada beberapa asosiasi sumber daya

Anda dapat mengaitkan satu ACL web dengan satu atau lebih AWS sumber daya, dengan batasan berikut:

- Anda dapat mengaitkan setiap AWS sumber daya hanya dengan satu ACL web. Hubungan antara web ACL dan AWS sumber daya adalah one-to-many.
- Anda dapat mengaitkan ACL web dengan satu atau lebih CloudFront distribusi. Anda tidak dapat mengaitkan ACL web yang telah Anda kaitkan dengan CloudFront distribusi dengan jenis AWS sumber daya lainnya.

Memulai dengan AWS WAF

Tutorial ini menunjukkan bagaimana menggunakan AWS WAF untuk melakukan tugas-tugas berikut:

- Mengatur AWS WAF.
- Buat daftar kontrol akses web (web ACL) menggunakan wizard di AWS WAF konsol.
- Pilih AWS sumber daya yang AWS WAF ingin Anda periksa permintaan web. Tutorial ini mencakup langkah-langkah untuk Amazon CloudFront. Prosesnya pada dasarnya sama untuk Amazon API Gateway REST API, Application Load Balancer, GraphQL API AWS AppSync , kumpulan pengguna Amazon Cognito, layanan, atau instance Akses Terverifikasi. AWS App Runner AWS
- Tambahkan aturan dan grup aturan yang ingin Anda gunakan untuk memfilter permintaan web. Misalnya, Anda dapat menentukan alamat IP tempat permintaan berasal dan menentukan nilai dalam permintaan yang hanya digunakan oleh penyerang. Untuk setiap aturan, Anda menentukan cara menangani permintaan web yang cocok. Anda dapat melakukan hal-hal seperti memblokir atau menghitungnya dan Anda dapat menjalankan tantangan bot seperti CAPTCHA. Anda menentukan tindakan untuk setiap aturan yang Anda tentukan di dalam ACL web dan untuk setiap aturan yang Anda tentukan di dalam grup aturan.
- Tentukan tindakan default untuk ACL web, salah satu Block atauAllow. Ini adalah tindakan yang AWS WAF mengambil permintaan ketika aturan di web ACL tidak secara eksplisit mengizinkan atau memblokirnya.

> **Note**
>
> AWS biasanya menagih Anda kurang dari US $0,25 per hari untuk sumber daya yang Anda buat selama tutorial ini. Ketika Anda selesai dengan tutorial, kami sarankan Anda menghapus sumber daya untuk mencegah timbulnya biaya yang tidak perlu.

Topik

Langkah 1: Mengatur AWS WAF

Jika Anda belum mengikuti langkah-langkah pengaturan umumMenyiapkan akun Anda untuk menggunakan layanan, lakukan sekarang.

Langkah 2: Buat Web ACL

AWS WAF Konsol memandu Anda melalui proses konfigurasi AWS WAF untuk memblokir atau mengizinkan permintaan web berdasarkan kriteria yang Anda tentukan, seperti alamat IP tempat permintaan berasal atau nilai dalam permintaan. Pada langkah ini, Anda membuat ACL web. Untuk informasi selengkapnya tentang ACL AWS WAF web, lihatAWS WAF daftar kontrol akses web (ACL web).

Untuk membuat web ACL

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.
2. Dari AWS WAF halaman beranda, pilih Buat web ACL.
3. Untuk Nama, masukkan nama yang ingin Anda gunakan untuk mengidentifikasi ACL web ini.

> **Note**
>
> Anda tidak dapat mengubah nama setelah membuat ACL web.

4. (Opsional) Untuk Deskripsi - opsional, masukkan deskripsi yang lebih panjang untuk ACL web jika Anda mau.
5. Untuk nama CloudWatch metrik, ubah nama default jika berlaku. Ikuti panduan di konsol untuk karakter yang valid. Nama tidak dapat berisi karakter khusus, spasi putih, atau nama metrik yang disediakan untuk AWS WAF, termasuk “Semua” dan “Default_Action.”

> **Note**
>
> Anda tidak dapat mengubah nama CloudWatch metrik setelah membuat ACL web.

6. Untuk jenis Sumber Daya, pilih CloudFrontdistribusi. Region secara otomatis mengisi ke Global (CloudFront) untuk CloudFront distribusi.
7. (Opsional) Untuk AWS sumber daya terkait - opsional, pilih Tambahkan AWS sumber daya. Di kotak dialog, pilih sumber daya yang ingin Anda kaitkan, lalu pilih Tambah. AWS WAF mengembalikan Anda ke halaman Deskripsikan web ACL dan AWS sumber daya terkait.
8. Pilih Berikutnya.

Langkah 3: Tambahkan aturan kecocokan string

Pada langkah ini, Anda membuat aturan dengan pernyataan pencocokan string dan menunjukkan apa yang harus dilakukan dengan permintaan yang cocok. Pernyataan aturan pencocokan string mengidentifikasi string yang AWS WAF ingin Anda cari dalam permintaan. Biasanya, string terdiri dari karakter ASCII yang dapat dicetak, tetapi Anda dapat menentukan karakter apa pun dari heksadesimal 0x00 hingga 0xFF (desimal 0 hingga 255). Selain menentukan string yang akan dicari, Anda menentukan komponen permintaan web yang ingin Anda cari, seperti header, string kueri, atau badan permintaan.

Jenis pernyataan ini beroperasi pada komponen permintaan web, dan memerlukan pengaturan komponen permintaan berikut:

- Komponen permintaan — Bagian dari permintaan web untuk memeriksa, misalnya, string kueri atau badan.

> **Warning**
>
> Jika Anda memeriksa komponen permintaan Badan, badan JSON, Header, atau Cookie, baca tentang batasan jumlah konten yang AWS WAF dapat diperiksa. Penanganan komponen permintaan kebesaran di AWS WAF

Untuk informasi tentang komponen permintaan web, lihatSpesifikasi dan penanganan komponen permintaan web.

- Transformasi teks opsional — Transformasi yang AWS WAF ingin Anda lakukan pada komponen permintaan sebelum memeriksanya. Misalnya, Anda dapat mengubah ke huruf kecil atau menormalkan ruang putih. Jika Anda menentukan lebih dari satu transformasi, AWS WAF proses mereka dalam urutan yang tercantum. Untuk informasi, lihat Opsi transformasi teks.

Untuk informasi tambahan tentang AWS WAF aturan, lihatAWS WAF aturan.

Untuk membuat pernyataan aturan kecocokan string

1. Pada halaman Tambahkan aturan dan grup aturan, pilih Tambahkan aturan, Tambahkan aturan dan grup aturan saya sendiri, Pembuat aturan, lalu Editor visual Aturan.

   > **Note**
   >
   > Konsol menyediakan editor visual Rule dan juga editor Rule JSON. Editor JSON memudahkan Anda untuk menyalin konfigurasi antara ACL web dan diperlukan untuk kumpulan aturan yang lebih kompleks, seperti yang memiliki beberapa tingkat bersarang. Prosedur ini menggunakan editor visual Rule.

2. Untuk Nama, masukkan nama yang ingin Anda gunakan untuk mengidentifikasi aturan ini.
3. Untuk Jenis pilih Aturan reguler.
4. Untuk Jika permintaan pilih cocok dengan pernyataan.

   Pilihan lainnya adalah untuk jenis pernyataan aturan logis. Anda dapat menggunakannya untuk menggabungkan atau meniadakan hasil pernyataan aturan lainnya.
5. Pada Pernyataan, untuk Inspect, buka dropdown dan pilih komponen permintaan web yang ingin AWS WAF Anda periksa. Untuk contoh ini, pilih Header.

Saat Anda memilih Header, Anda juga menentukan header mana yang AWS WAF ingin Anda periksa. Masukkan **`User-Agent`**. Nilai ini tidak peka huruf besar/kecil.

6. Untuk jenis Match, pilih di mana string yang ditentukan harus muncul di `User-Agent` header.

   Untuk contoh ini, pilih Tepat cocok dengan string. Ini menunjukkan bahwa AWS WAF memeriksa header user-agent di setiap permintaan web untuk string yang identik dengan string yang Anda tentukan.

7. Agar String cocok, tentukan string yang AWS WAF ingin Anda cari. Panjang maksimum String untuk dicocokkan adalah 200 karakter. Jika Anda ingin menentukan nilai yang dikodekan base64, Anda dapat menentukan hingga 200 karakter sebelum pengkodean.

   Untuk contoh ini, masukkan MyAgent. AWS WAF akan memeriksa `User-Agent` header dalam permintaan web untuk nilainya`MyAgent`.

8. Biarkan transformasi Teks disetel ke Tidak Ada.
9. Untuk Tindakan, pilih tindakan yang ingin diambil aturan saat cocok dengan permintaan web. Untuk contoh ini, pilih Hitung dan biarkan pilihan lain apa adanya. Tindakan hitungan membuat metrik untuk permintaan web yang cocok dengan aturan, tetapi tidak memengaruhi apakah permintaan diizinkan atau diblokir. Untuk informasi selengkapnya tentang pilihan tindakan, lihat Tindakan aturan danEvaluasi aturan dan kelompok aturan ACL Web.
10. Pilih Tambahkan aturan.

Langkah 4: Tambahkan grup aturan Aturan AWS Terkelola

AWS Aturan Terkelola menawarkan sekumpulan grup aturan terkelola untuk Anda gunakan, yang sebagian besar gratis bagi AWS WAF pelanggan. Untuk informasi selengkapnya tentang grup aturan, lihatAWS WAF kelompok aturan. Kami akan menambahkan grup aturan Aturan AWS Terkelola ke ACL web ini.

Untuk menambahkan grup aturan Aturan AWS Terkelola

1. Pada halaman Tambahkan aturan dan grup aturan, pilih Tambahkan aturan, lalu pilih Tambahkan grup aturan terkelola.
2. Pada halaman Tambahkan grup aturan terkelola, perluas daftar untuk grup aturan AWS terkelola. (Anda juga akan melihat daftar yang ditawarkan untuk AWS Marketplace penjual. Anda dapat berlangganan penawaran mereka dan kemudian menggunakannya dengan cara yang sama seperti untuk grup aturan Aturan AWS Terkelola.)

3. Untuk grup aturan yang ingin Anda tambahkan, lakukan hal berikut:

   a. Di kolom Action, aktifkan tombol Add to web ACL.

   b. Pilih Edit dan, dalam daftar Aturan grup aturan, buka dropdown Ganti semua tindakan aturan dan pilih. Count Ini menetapkan tindakan untuk semua aturan dalam kelompok aturan untuk dihitung saja. Hal ini memungkinkan Anda untuk melihat bagaimana semua aturan dalam kelompok aturan berperilaku dengan permintaan web Anda sebelum Anda menempatkan salah satu dari mereka untuk digunakan.

   c. Pilih Simpan aturan.

4. Di halaman Tambahkan grup aturan terkelola, pilih Tambahkan aturan. Ini mengembalikan Anda ke halaman Tambahkan aturan dan grup aturan.

Langkah 5: Selesaikan konfigurasi ACL web Anda

Setelah selesai menambahkan aturan dan grup aturan ke konfigurasi ACL web Anda, selesaikan dengan mengelola prioritas aturan di ACL web dan mengonfigurasi pengaturan seperti metrik, penandaan, dan pencatatan.

Untuk menyelesaikan konfigurasi ACL web Anda

1. Pada halaman Tambahkan aturan dan grup aturan, pilih Berikutnya.
2. Pada halaman Tetapkan prioritas aturan, Anda dapat melihat urutan pemrosesan untuk aturan dan grup aturan di ACL web. AWS WAF memprosesnya mulai dari bagian atas daftar. Anda dapat mengubah urutan pemrosesan dengan memindahkan aturan ke atas atau ke bawah. Untuk melakukan ini, pilih salah satu dalam daftar dan pilih Pindah ke atas atau Pindah ke bawah. Untuk informasi selengkapnya tentang prioritas aturan, lihat Memproses urutan aturan dan kelompok aturan dalam ACL web.
3. Pilih Berikutnya.
4. Pada halaman Konfigurasi metrik, untuk CloudWatchmetrik Amazon, Anda dapat melihat metrik yang direncanakan untuk aturan dan grup aturan dan Anda dapat melihat opsi pengambilan sampel permintaan web. Untuk informasi tentang melihat permintaan sampel, lihatMelihat contoh permintaan web. Untuk informasi tentang CloudWatch metrik Amazon, lihatPemantauan CloudWatch dengan Amazon.

   Anda dapat mengakses ringkasan metrik lalu lintas web di halaman ACL web di AWS WAF konsol, di bawah tab Ikhtisar lalu lintas. Dasbor konsol menyediakan ringkasan hampir real-time

dari metrik Amazon ACL web. CloudWatch Untuk informasi selengkapnya, lihat Dasbor ikhtisar lalu lintas ACL web.

5. Pilih Berikutnya.
6. Pada halaman Tinjau dan buat web ACL, tinjau pengaturan Anda, lalu pilih Buat ACL web.

Wizard mengembalikan Anda ke halaman Web ACL, di mana ACL web baru Anda terdaftar.

Langkah 6: Bersihkan sumber daya Anda

Anda sudah berhasil menyelesaikan tutorial ini. Untuk mencegah akun Anda AWS WAF dikenakan biaya tambahan, bersihkan AWS WAF objek yang Anda buat. Atau, Anda dapat mengubah konfigurasi agar sesuai dengan permintaan web yang benar-benar ingin Anda kelola AWS WAF.

> **Note**
>
> AWS biasanya menagih Anda kurang dari US $0,25 per hari untuk sumber daya yang Anda buat selama tutorial ini. Setelah selesai, kami sarankan Anda menghapus sumber daya untuk mencegah timbulnya biaya yang tidak perlu.

Untuk menghapus objek yang AWS WAF dikenakan biaya

1. Di halaman Web ACL, pilih ACL web Anda dari daftar dan pilih Edit.
2. Pada tab AWS Sumber daya terkait, untuk setiap sumber daya terkait, pilih tombol radio di sebelah nama sumber daya lalu pilih Disassociate. Ini memisahkan ACL web dari sumber daya Anda. AWS
3. Di setiap layar berikut, pilih Berikutnya sampai Anda kembali ke halaman Web ACL.

   Di halaman Web ACL, pilih ACL web Anda dari daftar dan pilih Hapus.

Aturan dan pernyataan aturan tidak ada di luar definisi grup aturan dan ACL web. Jika Anda menghapus ACL web, ini akan menghapus semua aturan individual yang telah Anda tetapkan di ACL web. Ketika Anda menghapus grup aturan dari ACL web, Anda hanya menghapus referensi untuk itu.

AWS WAF daftar kontrol akses web (ACL web)

Daftar kontrol akses web (web ACL) memberi Anda kontrol halus atas semua permintaan web HTTP (S) yang ditanggapi oleh sumber daya terlindungi Anda. Anda dapat melindungi Amazon CloudFront, Amazon API Gateway, Application Load Balancer, Amazon Cognito AWS AppSync, AWS App Runner, AWS dan sumber daya Akses Terverifikasi.

Anda dapat menggunakan kriteria seperti berikut ini untuk mengizinkan atau memblokir permintaan:

- Alamat IP asal permintaan
- Negara asal permintaan
- Pencocokan string atau ekspresi reguler (regex) cocok di bagian permintaan
- Ukuran bagian tertentu dari permintaan
- Deteksi kode SQL berbahaya atau scripting

Anda juga dapat menguji kombinasi dari kondisi ini. Anda dapat memblokir atau menghitung permintaan web yang tidak hanya memenuhi kondisi yang ditentukan, tetapi juga melebihi jumlah permintaan tertentu dalam satu menit. Anda dapat menggabungkan kondisi menggunakan operator logis. Anda juga dapat menjalankan teka-teki CAPTCHA dan tantangan sesi klien diam terhadap permintaan.

Anda memberikan kriteria pencocokan dan tindakan untuk melakukan kecocokan dalam pernyataan AWS WAF aturan. Anda dapat menentukan pernyataan aturan langsung di dalam ACL web Anda dan dalam grup aturan yang dapat digunakan kembali yang Anda gunakan di ACL web Anda. Untuk daftar lengkap opsi, lihat Dasar-dasar pernyataan aturan danTindakan aturan.

Untuk menentukan kriteria pemeriksaan dan penanganan permintaan web Anda, lakukan tugas-tugas berikut:

1. Pilih tindakan default ACL web, baik Allow atauBlock, untuk permintaan web yang tidak cocok dengan aturan apa pun yang Anda tentukan. Untuk informasi selengkapnya, lihat Tindakan default ACL web.
2. Tambahkan grup aturan apa pun yang ingin Anda gunakan di ACL web Anda. Grup aturan terkelola biasanya berisi aturan yang memblokir permintaan web. Untuk informasi tentang grup aturan, lihat AWS WAF kelompok aturan.
3. Tentukan kriteria pencocokan tambahan dan instruksi penanganan dalam satu atau beberapa aturan. Untuk menambahkan lebih dari satu aturan, mulailah dengan `AND` atau pernyataan `OR`

aturan dan sarang aturan yang ingin Anda gabungkan di bawahnya. Jika Anda ingin meniadakan opsi aturan, sarangkan aturan dalam pernyataan NOT. Anda dapat secara opsional menggunakan aturan berbasis tarif alih-alih aturan reguler untuk membatasi jumlah permintaan dari alamat IP tunggal mana pun yang memenuhi ketentuan. Untuk informasi tentang aturan, lihat AWS WAF aturan.

Jika Anda menambahkan lebih dari satu aturan ke ACL web, AWS WAF evaluasi aturan dalam urutan yang terdaftar untuk ACL web. Untuk informasi selengkapnya, lihat Evaluasi aturan dan kelompok aturan ACL Web.

Saat Anda membuat ACL web, Anda menentukan jenis sumber daya yang ingin Anda gunakan. Untuk informasi, lihat Membuat web ACL. Setelah Anda menentukan ACL web, Anda dapat mengaitkannya dengan sumber daya Anda untuk mulai memberikan perlindungan bagi mereka. Untuk informasi selengkapnya, lihat Mengaitkan atau memisahkan ACL web dengan sumber daya AWS.

Bagaimana AWS sumber daya menangani penundaan respons AWS WAF

Pada beberapa kesempatan, AWS WAF mungkin mengalami kesalahan internal yang menunda respons terhadap AWS sumber daya terkait tentang apakah akan mengizinkan atau memblokir permintaan. Pada kesempatan tersebut, CloudFront biasanya mengizinkan permintaan atau menyajikan konten, sedangkan layanan Regional biasanya menolak permintaan dan tidak menyajikan konten.

Topik

- Evaluasi aturan dan kelompok aturan ACL Web
- Tindakan default ACL web
- Mengelola batas ukuran inspeksi tubuh
- Konfigurasi untuk CAPTCHA, tantangan, dan token
- Bekerja dengan ACL web

Evaluasi aturan dan kelompok aturan ACL Web

Cara ACL web menangani permintaan web bergantung pada hal berikut:

- Pengaturan prioritas numerik aturan di ACL web dan di dalam grup aturan

- Pengaturan tindakan pada aturan dan web ACL
- Setiap penggantian yang Anda tempatkan pada aturan di grup aturan yang Anda tambahkan

Untuk daftar pengaturan tindakan aturan, lihatTindakan aturan.

Anda dapat menyesuaikan penanganan permintaan dan respons dalam pengaturan tindakan aturan dan pengaturan tindakan ACL web default. Untuk informasi, lihat Permintaan dan tanggapan web yang disesuaikan di AWS WAF.

Topik

- Memproses urutan aturan dan kelompok aturan dalam ACL web
- Cara AWS WAF menangani tindakan kelompok aturan dan aturan di ACL web
- Opsi penggantian tindakan untuk grup aturan

Memproses urutan aturan dan kelompok aturan dalam ACL web

Di ACL web dan di dalam grup aturan apa pun, Anda menentukan urutan evaluasi aturan menggunakan pengaturan prioritas numerik. Anda harus memberikan setiap aturan dalam ACL web pengaturan prioritas unik dalam ACL web itu, dan Anda harus memberikan setiap aturan dalam grup aturan pengaturan prioritas unik dalam grup aturan itu.

> **Note**
>
> Saat Anda mengelola grup aturan dan ACL web melalui konsol, AWS WAF tetapkan setelan prioritas numerik unik untuk Anda berdasarkan urutan aturan dalam daftar. AWS WAF menetapkan prioritas numerik terendah untuk aturan di bagian atas daftar, dan prioritas numerik tertinggi untuk aturan di bagian bawah.

Ketika AWS WAF mengevaluasi ACL web atau grup aturan apa pun terhadap permintaan web, itu mengevaluasi aturan dari pengaturan prioritas numerik terendah hingga menemukan kecocokan yang mengakhiri evaluasi atau menghabiskan semua aturan.

Misalnya, Anda memiliki aturan dan grup aturan berikut di ACL web Anda, yang diprioritaskan seperti yang ditunjukkan:

- Aturan1 - prioritas 0

- RuleGroupA - prioritas 100
  - RuleA1 — prioritas 10.000
  - RuleA2 — prioritas 20,000
- Aturan2 - prioritas 200
- RuleGroupB - prioritas 300
  - RuleB1 — prioritas 0
  - RuleB2 — prioritas 1

AWS WAF akan mengevaluasi aturan untuk ACL web ini dengan urutan sebagai berikut:

- Aturan1
- RuleGroupSebuah aturanA1
- RuleGroupSebuah aturanA2
- Aturan2
- RuleGroupB RuleB1
- RuleGroupB RuleB2

Cara AWS WAF menangani tindakan kelompok aturan dan aturan di ACL web

Saat mengonfigurasi aturan dan grup aturan, Anda memilih AWS WAF cara menangani permintaan web yang cocok:

- Allowdan Block menghentikan tindakan — Allow dan Block tindakan menghentikan semua pemrosesan ACL web lainnya pada permintaan web yang cocok. Jika aturan di ACL web menemukan kecocokan untuk permintaan dan tindakan aturan adalah Allow atauBlock, kecocokan itu menentukan disposisi akhir permintaan web untuk ACL web. AWS WAF tidak memproses aturan lain di ACL web yang muncul setelah yang cocok. Ini berlaku untuk aturan yang Anda tambahkan langsung ke ACL web dan aturan yang ada di dalam grup aturan tambahan. Dengan Block tindakan tersebut, sumber daya yang dilindungi tidak menerima atau memproses permintaan web.
- Countadalah tindakan non-penghentian — Ketika aturan dengan Count tindakan cocok dengan permintaan, AWS WAF hitung permintaan, lalu lanjutkan pemrosesan aturan yang mengikuti dalam kumpulan aturan ACL web.

- CAPTCHAdan Challenge dapat berupa tindakan non-penghentian atau penghentian — Ketika aturan dengan salah satu tindakan ini cocok dengan permintaan, AWS WAF periksa status tokennya. Jika permintaan memiliki token yang valid, AWS WAF perlakukan kecocokan yang mirip dengan Count kecocokan, lalu lanjutkan pemrosesan aturan yang mengikuti dalam kumpulan aturan ACL web. Jika permintaan tidak memiliki token yang valid, AWS WAF hentikan evaluasi dan kirimkan teka-teki CAPTCHA atau tantangan sesi klien latar belakang diam untuk dipecahkan.

Jika evaluasi aturan tidak menghasilkan tindakan penghentian apa pun, maka AWS WAF terapkan tindakan default ACL web ke permintaan. Untuk informasi, lihat Tindakan default ACL web.

Di ACL web Anda, Anda dapat mengganti pengaturan tindakan untuk aturan di dalam grup aturan dan Anda dapat mengganti tindakan yang dikembalikan oleh grup aturan. Untuk informasi, lihat Opsi penggantian tindakan untuk grup aturan.

Interaksi antara tindakan dan pengaturan prioritas

Tindakan yang AWS WAF berlaku untuk permintaan web dipengaruhi oleh pengaturan prioritas numerik aturan di ACL web. Misalnya, katakan bahwa ACL web Anda memiliki aturan dengan Allow tindakan dan prioritas numerik 50 dan aturan lain dengan Count tindakan dan prioritas numerik 100. AWS WAF mengevaluasi aturan dalam ACL web dalam urutan prioritas mereka, mulai dari pengaturan terendah, sehingga akan mengevaluasi aturan izinkan sebelum aturan hitungan. Permintaan web yang cocok dengan kedua aturan akan cocok dengan aturan izinkan terlebih dahulu. Karena Allow merupakan tindakan penghentian, AWS WAF akan menghentikan evaluasi pada pertandingan ini dan tidak akan mengevaluasi permintaan terhadap aturan hitungan.

- Jika Anda hanya ingin menyertakan permintaan yang tidak cocok dengan aturan izinkan dalam metrik aturan hitungan Anda, maka pengaturan prioritas aturan akan berfungsi.
- Di sisi lain, jika Anda ingin menghitung metrik dari aturan hitungan bahkan untuk permintaan yang cocok dengan aturan izinkan, Anda harus memberi aturan hitungan setelan prioritas numerik yang lebih rendah daripada aturan izinkan, sehingga aturan tersebut berjalan lebih dulu.

Untuk informasi selengkapnya tentang setelan prioritas, lihatMemproses urutan aturan dan kelompok aturan dalam ACL web.

Opsi penggantian tindakan untuk grup aturan

Saat menambahkan grup aturan ke ACL web, Anda dapat mengganti tindakan yang dilakukan saat mencocokkan permintaan web. Mengganti tindakan untuk grup aturan di dalam konfigurasi ACL web

Anda tidak mengubah grup aturan itu sendiri. Ini hanya mengubah cara AWS WAF menggunakan kelompok aturan dalam konteks ACL web.

Pengesampingan tindakan aturan kelompok aturan

Anda dapat mengganti tindakan aturan di dalam grup aturan ke tindakan aturan yang valid. Saat Anda melakukan ini, permintaan yang cocok ditangani persis seolah-olah tindakan aturan yang dikonfigurasi adalah pengaturan penggantian.

> **Note**
>
> Tindakan aturan dapat mengakhiri atau tidak mengakhiri. Tindakan penghentian menghentikan evaluasi ACL web dari permintaan dan memungkinkannya melanjutkan ke aplikasi Anda yang dilindungi atau memblokirnya.

Berikut adalah opsi tindakan aturan:

- Allow— AWS WAF memungkinkan permintaan diteruskan ke AWS sumber daya yang dilindungi untuk diproses dan direspon. Ini adalah tindakan penghentian. Dalam aturan yang Anda tentukan, Anda dapat menyisipkan header khusus ke dalam permintaan sebelum meneruskannya ke sumber daya yang dilindungi.
- Block— AWS WAF memblokir permintaan. Ini adalah tindakan penghentian. Secara default, AWS sumber daya Anda yang dilindungi merespons dengan kode `403 (Forbidden)` status HTTP. Dalam aturan yang Anda tentukan, Anda dapat menyesuaikan respons. Saat AWS WAF memblokir permintaan, pengaturan Block tindakan menentukan respons yang dikirim kembali oleh sumber daya yang dilindungi ke klien.
- Count— AWS WAF menghitung permintaan tetapi tidak menentukan apakah akan mengizinkan atau memblokirnya. Ini adalah tindakan yang tidak mengakhiri. AWS WAF terus memproses aturan yang tersisa di ACL web. Dalam aturan yang Anda tentukan, Anda dapat menyisipkan header khusus ke dalam permintaan dan Anda dapat menambahkan label yang dapat dicocokkan dengan aturan lain.
- CAPTCHAdan Challenge — AWS WAF menggunakan teka-teki CAPTCHA dan tantangan diam untuk memverifikasi bahwa permintaan tersebut tidak berasal dari bot, dan AWS WAF menggunakan token untuk melacak respons klien yang berhasil baru-baru ini.

  Teka-teki CAPTCHA dan tantangan diam hanya dapat berjalan ketika browser mengakses titik akhir HTTPS. Klien browser harus berjalan dalam konteks aman untuk mendapatkan token.

> **Note**
>
> Anda akan dikenakan biaya tambahan ketika Anda menggunakan tindakan CAPTCHA atau Challenge aturan di salah satu aturan Anda atau sebagai penggantian tindakan aturan dalam grup aturan. Untuk informasi selengkapnya, silakan lihat Harga AWS WAF.

Tindakan aturan ini dapat mengakhiri atau tidak mengakhiri, tergantung pada status token dalam permintaan:

- Non-terminating untuk token yang valid dan belum kedaluwarsa — Jika token valid dan belum kedaluwarsa sesuai dengan CAPTCHA yang dikonfigurasi atau waktu kekebalan tantangan, AWS WAF menangani permintaan yang serupa dengan tindakan. Count AWS WAF terus memeriksa permintaan web berdasarkan aturan yang tersisa di ACL web. Mirip dengan Count konfigurasi, dalam aturan yang Anda tentukan, Anda dapat mengonfigurasi tindakan ini secara opsional dengan header khusus untuk dimasukkan ke dalam permintaan, dan Anda dapat menambahkan label yang dapat dicocokkan dengan aturan lain.
- Mengakhiri dengan permintaan yang diblokir untuk token yang tidak valid atau kedaluwarsa - Jika token tidak valid atau stempel waktu yang ditunjukkan kedaluwarsa, AWS WAF menghentikan pemeriksaan permintaan web dan memblokir permintaan, mirip dengan tindakan. Block AWS WAF kemudian merespons klien dengan kode respons khusus. SebabCAPTCHA, jika isi permintaan menunjukkan bahwa browser klien dapat menanganinya, AWS WAF mengirimkan teka-teki CAPTCHA dalam JavaScript interstisial, yang dirancang untuk membedakan klien manusia dari bot. Untuk Challenge aksinya, AWS WAF kirimkan JavaScript pengantara dengan tantangan diam yang dirancang untuk membedakan browser normal dari sesi yang dijalankan oleh bot.

Untuk informasi tambahan, lihat CAPTCHAdan Challenge di AWS WAF.

Untuk informasi tentang cara menggunakan opsi ini, lihatMengesampingkan tindakan aturan dalam grup aturan.

Mengesampingkan tindakan aturan untuk Count

Kasus penggunaan yang paling umum untuk penggantian tindakan aturan adalah mengesampingkan beberapa atau semua tindakan aturan keCount, untuk menguji dan memantau perilaku kelompok aturan sebelum memasukkannya ke dalam produksi.

Anda juga dapat menggunakan ini untuk memecahkan masalah grup aturan yang menghasilkan positif palsu. Positif palsu terjadi ketika grup aturan memblokir lalu lintas yang tidak Anda harapkan untuk diblokir. Jika Anda mengidentifikasi aturan dalam grup aturan yang akan memblokir permintaan yang ingin Anda izinkan, Anda dapat menyimpan penggantian tindakan hitungan pada aturan tersebut, untuk mengecualikannya agar tidak bertindak sesuai permintaan Anda.

Untuk informasi selengkapnya tentang penggunaan penggantian tindakan aturan dalam pengujian, lihatMenguji dan menyetel perlindungan Anda AWS WAF.

Daftar JSON: menggantikan **`RuleActionOverridesExcludedRules`**

Jika Anda menetapkan tindakan aturan grup aturan ke Count dalam konfigurasi ACL web Anda sebelum 27 Oktober 2022, AWS WAF simpan penggantian Anda di web ACL JSON sebagai. `ExcludedRules` Sekarang, pengaturan JSON untuk mengganti aturan Count ada di pengaturan. `RuleActionOverrides`

Saat Anda menggunakan AWS WAF konsol untuk mengedit pengaturan grup aturan yang ada, konsol secara otomatis mengonversi `ExcludedRules` pengaturan apa pun di JSON ke `RuleActionOverrides` pengaturan, dengan tindakan penggantian disetel ke. Count

- Contoh pengaturan saat ini:

```
       "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesAdminProtectionRuleSet",
          "RuleActionOverrides": [
            {
              "Name": "AdminProtection_URIPATH",
              "ActionToUse": {
                "Count": {}
              }
            }
          ]
```

- Contoh pengaturan lama:

```
OLD SETTING
       "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesAdminProtectionRuleSet",
          "ExcludedRules": [
```

```
            {
              "Name": "AdminProtection_URIPATH"
            }
          ]
OLD SETTING
```

Kami menyarankan Anda memperbarui semua `ExcludedRules` pengaturan Anda di daftar JSON Anda ke `RuleActionOverrides` pengaturan dengan tindakan yang disetel keCount. API menerima salah satu pengaturan, tetapi Anda akan mendapatkan konsistensi dalam daftar JSON Anda, antara pekerjaan konsol Anda dan pekerjaan API Anda, jika Anda hanya menggunakan setelan baru`RuleActionOverrides`.

Tindakan pengembalian grup aturan akan ditimpa Count

Anda dapat mengganti tindakan yang dikembalikan grup aturan, menyetelnya. Count

> **Note**
>
> Ini bukan pilihan yang baik untuk menguji aturan dalam kelompok aturan, karena tidak mengubah cara AWS WAF mengevaluasi kelompok aturan itu sendiri. Ini hanya mempengaruhi bagaimana AWS WAF menangani hasil yang dikembalikan ke ACL web dari evaluasi kelompok aturan. Jika Anda ingin menguji aturan dalam grup aturan, gunakan opsi yang dijelaskan di bagian sebelumnya,. Pengesampingan tindakan aturan kelompok aturan

Saat Anda mengganti tindakan grup aturanCount, AWS WAF memproses evaluasi grup aturan secara normal.

Jika tidak ada aturan dalam grup aturan yang cocok atau jika semua aturan yang cocok memiliki Count tindakan, maka penggantian ini tidak berpengaruh pada pemrosesan grup aturan atau ACL web.

Aturan pertama dalam grup aturan yang cocok dengan permintaan web dan yang memiliki tindakan aturan penghentian AWS WAF menyebabkan berhenti mengevaluasi grup aturan dan mengembalikan hasil tindakan penghentian ke tingkat evaluasi ACL web. Pada titik ini, dalam evaluasi ACL web, penggantian ini berlaku. AWS WAF mengesampingkan tindakan penghentian sehingga hasil evaluasi kelompok aturan hanyalah tindakan. Count AWS WAF kemudian terus memproses sisa aturan di web ACL.

Untuk informasi tentang cara menggunakan opsi ini, lihatMengesampingkan hasil evaluasi kelompok aturan ke Count.

Tindakan default ACL web

Saat Anda membuat dan mengkonfigurasi ACL web, Anda harus mengatur tindakan default ACL web. AWS WAF menerapkan tindakan ini ke permintaan web apa pun yang membuatnya melalui semua evaluasi aturan ACL web tanpa tindakan penghentian yang diterapkan padanya. Tindakan penghentian menghentikan evaluasi ACL web dari permintaan dan memungkinkannya melanjutkan ke aplikasi Anda yang dilindungi atau memblokirnya. Untuk informasi tentang tindakan aturan, lihatTindakan aturan.

Tindakan default ACL web harus menentukan disposisi akhir permintaan web, jadi ini adalah tindakan penghentian:

- AllowJika Anda ingin mengizinkan sebagian besar pengguna mengakses situs web Anda, tetapi Anda ingin memblokir akses ke penyerang yang permintaannya berasal dari alamat IP tertentu, atau yang permintaannya tampaknya berisi kode SQL berbahaya atau nilai yang ditentukan, pilih tindakan Allow default. Kemudian, ketika Anda menambahkan aturan ke ACL web Anda, tambahkan aturan yang mengidentifikasi dan memblokir permintaan spesifik yang ingin Anda blokir. Dengan tindakan ini, Anda dapat menyisipkan header khusus ke dalam permintaan sebelum meneruskannya ke sumber daya yang dilindungi.
- BlockJika Anda ingin mencegah sebagian besar pengguna mengakses situs web Anda, tetapi Anda ingin mengizinkan akses ke pengguna yang permintaannya berasal dari alamat IP tertentu, atau yang permintaannya berisi nilai tertentu, pilih Block tindakan default. Kemudian ketika Anda menambahkan aturan ke ACL web Anda, tambahkan aturan yang mengidentifikasi dan mengizinkan permintaan spesifik yang ingin Anda izinkan masuk. Secara default, untuk Block tindakan, AWS sumber daya merespons dengan kode `403 (Forbidden)` status HTTP, tetapi Anda dapat menyesuaikan respons.

Untuk informasi tentang menyesuaikan permintaan dan tanggapan, lihatPermintaan dan tanggapan web yang disesuaikan di AWS WAF.

Konfigurasi aturan dan grup aturan Anda sendiri sebagian bergantung pada apakah Anda ingin mengizinkan atau memblokir sebagian besar permintaan web. Misalnya, jika Anda ingin mengizinkan sebagian besar permintaan, Anda akan mengatur tindakan default ACL web keAllow, dan kemudian menambahkan aturan yang mengidentifikasi permintaan web yang ingin Anda blokir, seperti berikut ini:

- Permintaan yang berasal dari alamat IP yang membuat jumlah permintaan yang tidak masuk akal
- Permintaan yang berasal dari negara tempat Anda tidak berbisnis atau sering menjadi sumber serangan
- Permintaan yang menyertakan nilai palsu di `User-agent` header
- Permintaan yang tampaknya menyertakan kode SQL berbahaya

Aturan grup aturan terkelola biasanya menggunakan Block tindakan, tetapi tidak semua melakukannya. Misalnya, beberapa aturan yang digunakan untuk Kontrol Bot menggunakan pengaturan CAPTCHA dan Challenge tindakan. Untuk informasi tentang grup aturan terkelola, lihatGrup aturan terkelola.

Mengelola batas ukuran inspeksi tubuh

Batas ukuran inspeksi tubuh adalah ukuran badan permintaan maksimum yang AWS WAF dapat diperiksa. Ketika badan permintaan web lebih besar dari batas, layanan host yang mendasarinya hanya meneruskan konten yang berada dalam batas AWS WAF untuk diperiksa.

- Untuk Application Load Balancer dan AWS AppSync, limit ditetapkan pada 8 KB (8.192 byte).
- Untuk CloudFront API Gateway, Amazon Cognito, App Runner, dan Akses Terverifikasi, batas default adalah 16 KB (16.384 byte), dan Anda dapat meningkatkan batas untuk salah satu jenis sumber daya dengan penambahan 16 KB, hingga 64 KB. Opsi pengaturan adalah 16 KB, 32 KB, 48 KB, dan 64 KB.

Penanganan tubuh yang terlalu besar

Jika lalu lintas web Anda mencakup badan yang lebih besar dari batas, penanganan oversize yang dikonfigurasi akan berlaku. Untuk informasi tentang opsi penanganan ukuran besar, lihatPenanganan komponen permintaan kebesaran di AWS WAF.

Pertimbangan harga untuk meningkatkan pengaturan batas

AWS WAF mengenakan tarif dasar untuk memeriksa lalu lintas yang berada dalam batas default untuk jenis sumber daya.

Untuk CloudFront sumber daya API Gateway, Amazon Cognito, App Runner, dan Akses Terverifikasi, jika Anda meningkatkan setelan batas, lalu lintas yang AWS WAF dapat diperiksa mencakup ukuran tubuh hingga batas baru Anda. Anda dikenakan biaya tambahan hanya untuk pemeriksaan

permintaan yang memiliki ukuran tubuh lebih besar dari 16 KB default. Untuk informasi lebih lanjut tentang harga, lihat AWS WAF Harga.

Opsi untuk memodifikasi batas ukuran inspeksi tubuh

Anda dapat mengonfigurasi batas ukuran pemeriksaan tubuh untuk CloudFront, API Gateway, Amazon Cognito, App Runner, atau sumber daya Akses Terverifikasi.

Saat membuat atau mengedit ACL web, Anda dapat mengubah batas ukuran pemeriksaan tubuh dalam konfigurasi asosiasi sumber daya. Untuk API, lihat konfigurasi asosiasi ACL web di AssociationConfig. Untuk konsol, lihat konfigurasi pada halaman tempat Anda menentukan sumber daya terkait ACL web. Untuk panduan tentang konfigurasi konsol, lihatBekerja dengan ACL web.

Konfigurasi untuk CAPTCHA, tantangan, dan token

Anda dapat mengonfigurasi opsi di ACL web Anda untuk aturan yang menggunakan tindakan CAPTCHA atau Challenge aturan dan untuk SDK integrasi aplikasi yang mengelola tantangan klien diam untuk perlindungan AWS WAF terkelola.

Fitur-fitur ini mengurangi aktivitas bot dengan menantang pengguna akhir dengan teka-teki CAPTCHA dan dengan menghadirkan sesi klien dengan tantangan diam. Ketika klien merespons dengan sukses, AWS WAF berikan token untuk mereka gunakan dalam permintaan web mereka, diberi cap waktu dengan teka-teki terakhir yang berhasil dan tanggapan tantangan. Untuk informasi selengkapnya, lihat AWS WAF mitigasi ancaman cerdas.

Dalam konfigurasi ACL web Anda, Anda dapat mengonfigurasi cara AWS WAF mengelola token ini:

- CAPTCHA dan tantangan waktu kekebalan — Ini menentukan berapa lama CAPTCHA atau stempel waktu tantangan tetap valid. Pengaturan ACL web diwarisi oleh semua aturan yang tidak memiliki pengaturan waktu kekebalan sendiri yang dikonfigurasi dan juga oleh SDK integrasi aplikasi. Untuk informasi selengkapnya, lihat Kedaluwarsa stempel waktu: waktu kekebalan token AWS WAF.
- Domain token — Secara default, AWS WAF menerima token hanya untuk domain sumber daya yang terkait dengan ACL web. Jika Anda mengonfigurasi daftar domain token, AWS WAF menerima token untuk semua domain dalam daftar dan untuk domain sumber daya terkait. Untuk informasi selengkapnya, lihat AWS WAF konfigurasi daftar domain token ACL web.

Bekerja dengan ACL web

Bagian ini menyediakan prosedur untuk membuat, mengelola, dan menggunakan ACL web melalui AWS konsol.

Untuk ACL web apa pun yang Anda gunakan, Anda dapat mengakses ringkasan metrik lalu lintas web di halaman ACL web di AWS WAF konsol, di bawah tab Ikhtisar lalu lintas. Dasbor konsol menyediakan ringkasan hampir real-time dari CloudWatch metrik Amazon yang AWS WAF dikumpulkan saat mengevaluasi lalu lintas web aplikasi Anda. Untuk informasi selengkapnya tentang dasbor, lihatDasbor ikhtisar lalu lintas ACL web. Untuk informasi tambahan tentang memantau lalu lintas ACL web Anda, lihatPemantauan dan penyetelan.

> **Risiko lalu lintas produksi**
>
> Sebelum Anda menerapkan perubahan di ACL web Anda untuk lalu lintas produksi, uji dan sesuaikan di lingkungan pementasan atau pengujian hingga Anda merasa nyaman dengan potensi dampak terhadap lalu lintas Anda. Kemudian uji dan sesuaikan aturan Anda yang diperbarui dalam mode hitungan dengan lalu lintas produksi Anda sebelum mengaktifkannya. Untuk panduan, lihat Menguji dan menyetel perlindungan Anda AWS WAF.

> **Note**
>
> Menggunakan lebih dari 1.500 WCU dalam ACL web menimbulkan biaya di luar harga ACL web dasar. Untuk informasi selengkapnya, lihat AWS WAF unit kapasitas ACL web (WCU) dan Harga AWS WAF.

Inkonsistensi sementara selama pembaruan

Saat Anda membuat atau mengubah ACL web atau AWS WAF sumber daya lainnya, perubahan membutuhkan sedikit waktu untuk menyebar ke semua area tempat sumber daya disimpan. Waktu propagasi bisa dari beberapa detik hingga beberapa menit.

Berikut ini adalah contoh inkonsistensi sementara yang mungkin Anda perhatikan selama propagasi perubahan:

- Setelah Anda membuat ACL web, jika Anda mencoba mengaitkannya dengan sumber daya, Anda mungkin mendapatkan pengecualian yang menunjukkan bahwa ACL web tidak tersedia.

- Setelah Anda menambahkan grup aturan ke ACL web, aturan grup aturan baru mungkin berlaku di satu area di mana ACL web digunakan dan tidak di area lain.
- Setelah mengubah setelan tindakan aturan, Anda mungkin melihat tindakan lama di beberapa tempat dan tindakan baru di tempat lain.
- Setelah Anda menambahkan alamat IP ke set IP yang digunakan dalam aturan pemblokiran, alamat baru mungkin diblokir di satu area sementara masih diizinkan di area lain.

Topik

Membuat web ACL

Untuk membuat ACL web baru, gunakan wizard pembuatan ACL web mengikuti prosedur di halaman ini.

> **Risiko lalu lintas produksi**
>
> Sebelum Anda menerapkan perubahan di ACL web Anda untuk lalu lintas produksi, uji dan sesuaikan di lingkungan pementasan atau pengujian hingga Anda merasa nyaman dengan potensi dampak terhadap lalu lintas Anda. Kemudian uji dan sesuaikan aturan Anda yang diperbarui dalam mode hitungan dengan lalu lintas produksi Anda sebelum mengaktifkannya. Untuk panduan, lihat Menguji dan menyetel perlindungan Anda AWS WAF.

> **Note**
>
> Menggunakan lebih dari 1.500 WCU dalam ACL web menimbulkan biaya di luar harga ACL web dasar. Untuk informasi selengkapnya, lihat AWS WAF unit kapasitas ACL web (WCU) dan Harga AWS WAF.

Untuk membuat web ACL

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.
2. Pilih Web ACL di panel navigasi, lalu pilih Buat web ACL.
3. Untuk Nama, masukkan nama yang ingin Anda gunakan untuk mengidentifikasi ACL web ini.

   > **Note**
   >
   > Anda tidak dapat mengubah nama setelah membuat ACL web.

4. (Opsional) Untuk Deskripsi - opsional, masukkan deskripsi yang lebih panjang untuk ACL web jika Anda mau.
5. Untuk nama CloudWatch metrik, ubah nama default jika berlaku. Ikuti panduan di konsol untuk karakter yang valid. Nama tidak dapat berisi karakter khusus, spasi putih, atau nama metrik yang disediakan untuk AWS WAF, termasuk “Semua” dan “Default_Action.”

   > **Note**
   >
   > Anda tidak dapat mengubah nama CloudWatch metrik setelah membuat ACL web.

6. Di bawah Jenis sumber daya, pilih kategori AWS sumber daya yang ingin Anda kaitkan dengan ACL web ini, baik CloudFront distribusi Amazon atau sumber daya Regional. Untuk informasi selengkapnya, lihat Mengaitkan atau memisahkan ACL web dengan sumber daya AWS.
7. Untuk Wilayah, jika Anda telah memilih jenis sumber daya Regional, pilih Wilayah tempat Anda AWS WAF ingin menyimpan ACL web.

   Anda hanya perlu memilih opsi ini untuk jenis sumber daya Regional. Untuk CloudFront distribusi, Wilayah ini dikodekan dengan keras ke Wilayah AS Timur (Virginia N.),`us-east-1`, untuk aplikasi Global (). CloudFront
8. (CloudFront, API Gateway, Amazon Cognito, App Runner, dan Akses Terverifikasi) Untuk batas ukuran pemeriksaan permintaan Web - opsional, jika Anda ingin menentukan batas ukuran pemeriksaan tubuh yang berbeda, pilih batasnya. Memeriksa ukuran tubuh di atas default 16 KB dapat menimbulkan biaya tambahan. Untuk informasi tentang opsi ini, lihatMengelola batas ukuran inspeksi tubuh.
9. (Opsional) Untuk AWS sumber daya terkait - opsional, jika Anda ingin menentukan sumber daya Anda sekarang, pilih Tambahkan AWS sumber daya. Di kotak dialog, pilih sumber daya yang

ingin Anda kaitkan, lalu pilih Tambah. AWS WAF mengembalikan Anda ke halaman Deskripsikan web ACL dan AWS sumber daya terkait.

10. Pilih Berikutnya.
11. (Opsional) Jika Anda ingin menambahkan grup aturan terkelola, pada halaman Tambahkan aturan dan grup aturan, pilih Tambahkan aturan, lalu pilih Tambahkan grup aturan terkelola. Lakukan hal berikut untuk setiap grup aturan terkelola yang ingin Anda tambahkan:

    a. Pada halaman Tambahkan grup aturan terkelola, perluas daftar untuk grup aturan AWS terkelola atau untuk AWS Marketplace penjual pilihan Anda.

    b. Untuk grup aturan yang ingin Anda tambahkan, di kolom Tindakan, aktifkan sakelar Tambahkan ke web ACL.

    Untuk menyesuaikan cara ACL web Anda menggunakan grup aturan, pilih Edit. Berikut ini adalah pengaturan kustomisasi umum:

    - Ganti tindakan aturan untuk beberapa atau semua aturan. Jika Anda tidak menentukan tindakan penggantian untuk aturan, evaluasi menggunakan tindakan aturan yang ditentukan di dalam grup aturan. Untuk informasi tentang opsi ini, lihatOpsi penggantian tindakan untuk grup aturan.
    - Kurangi cakupan permintaan web yang diperiksa grup aturan dengan menambahkan pernyataan cakupan ke bawah. Untuk informasi tentang opsi ini, lihatPernyataan cakupan ke bawah.
    - Beberapa grup aturan terkelola mengharuskan Anda untuk menyediakan konfigurasi tambahan. Lihat dokumentasi dari penyedia grup aturan terkelola Anda. Untuk informasi khusus tentang grup aturan Aturan AWS Terkelola, lihatAWS Aturan Terkelola untuk AWS WAF.

    Setelah selesai dengan pengaturan, pilih Simpan aturan.

    Pilih Tambahkan aturan untuk menyelesaikan penambahan aturan terkelola dan kembali ke halaman Tambahkan aturan dan grup aturan.

12. (Opsional) Jika Anda ingin menambahkan grup aturan Anda sendiri, pada halaman Tambahkan aturan dan grup aturan, pilih Tambahkan aturan, lalu pilih Tambahkan aturan dan grup aturan saya sendiri. Lakukan hal berikut untuk setiap grup aturan yang ingin Anda tambahkan:

    a. Pada halaman Tambahkan aturan dan grup aturan saya sendiri, pilih Grup aturan.

b. Untuk Nama, masukkan nama yang ingin Anda gunakan untuk aturan grup aturan di ACL web ini. Jangan gunakan nama yang dimulai dengan `AWSShield`,`PreFM`, atau`PostFM`. String ini dicadangkan atau dapat menyebabkan kebingungan dengan grup aturan yang dikelola untuk Anda oleh layanan lain. Lihat Grup aturan yang disediakan oleh layanan lain.

c. Pilih grup aturan Anda dari daftar.

> **Note**
>
> Jika Anda ingin mengganti tindakan aturan untuk grup aturan Anda sendiri, pertama-tama simpan ke ACL web, lalu edit ACL web dan pernyataan referensi grup aturan dalam daftar aturan ACL web. Anda dapat mengganti tindakan aturan ke setelan tindakan yang valid, sama seperti yang dapat Anda lakukan untuk grup aturan terkelola.

d. Pilih Tambahkan aturan.

13. (Opsional) Jika Anda ingin menambahkan aturan Anda sendiri, pada halaman Tambahkan aturan dan grup aturan, pilih Tambahkan aturan, Tambahkan aturan dan grup aturan saya sendiri, Pembuat aturan, lalu Editor visual Aturan.

> **Note**
>
> Editor visual Aturan konsol mendukung satu tingkat bersarang. Misalnya, Anda dapat menggunakan satu logika `AND` atau `OR` pernyataan dan sarang satu tingkat pernyataan lain di dalamnya, tetapi Anda tidak dapat membuat pernyataan logis dalam pernyataan logis. Untuk mengelola pernyataan aturan yang lebih kompleks, gunakan editor Rule JSON. Untuk informasi tentang semua opsi untuk aturan, lihatAWS WAF aturan. Prosedur ini mencakup editor visual Rule.

a. Untuk Nama, masukkan nama yang ingin Anda gunakan untuk mengidentifikasi aturan ini. Jangan gunakan nama yang dimulai dengan `AWSShield`,`PreFM`, atau`PostFM`. String ini dicadangkan atau dapat menyebabkan kebingungan dengan grup aturan yang dikelola untuk Anda oleh layanan lain.

b. Masukkan definisi aturan Anda, sesuai dengan kebutuhan Anda. Anda dapat menggabungkan aturan di dalam pernyataan logis `AND` dan `OR` aturan. Wizard memandu

Anda melalui opsi untuk setiap aturan, sesuai dengan konteksnya. Untuk informasi tentang opsi aturan Anda, lihatAWS WAF aturan.

c. Untuk Tindakan, pilih tindakan yang ingin diambil aturan saat cocok dengan permintaan web. Untuk informasi tentang pilihan Anda, lihat Tindakan aturan danEvaluasi aturan dan kelompok aturan ACL Web.

Jika Anda menggunakan Challengetindakan CAPTCHAatau, sesuaikan konfigurasi waktu Imunitas sesuai kebutuhan untuk aturan. Jika Anda tidak menentukan pengaturan, aturan mewarisinya dari ACL web. Untuk memodifikasi pengaturan waktu kekebalan ACL web, edit ACL web setelah Anda membuatnya. Untuk informasi lebih lanjut tentang waktu kekebalan, lihatKedaluwarsa stempel waktu: waktu kekebalan token AWS WAF.

> **Note**
>
> Anda akan dikenakan biaya tambahan ketika Anda menggunakan tindakan CAPTCHA atau Challenge aturan di salah satu aturan Anda atau sebagai penggantian tindakan aturan dalam grup aturan. Untuk informasi selengkapnya, silakan lihat Harga AWS WAF.

Jika Anda ingin menyesuaikan permintaan atau respons, pilih opsi untuk itu dan isi detail penyesuaian Anda. Untuk informasi selengkapnya, lihat Permintaan dan tanggapan web yang disesuaikan di AWS WAF.

Jika Anda ingin aturan Anda menambahkan label ke permintaan web yang cocok, pilih opsi untuk itu dan isi detail label Anda. Untuk informasi selengkapnya, lihat AWS WAF label pada permintaan web.

d. Pilih Tambahkan aturan.

14. Pilih tindakan default untuk ACL web, salah satu Block atauAllow. Ini adalah tindakan yang AWS WAF mengambil permintaan ketika aturan di web ACL tidak secara eksplisit mengizinkan atau memblokirnya. Untuk informasi selengkapnya, lihat Tindakan default ACL web.

    Jika Anda ingin menyesuaikan tindakan default, pilih opsi untuk itu dan isi detail penyesuaian Anda. Untuk informasi selengkapnya, lihat Permintaan dan tanggapan web yang disesuaikan di AWS WAF.

15. Anda dapat menentukan daftar domain Token untuk mengaktifkan berbagi token antara aplikasi yang dilindungi. Token digunakan oleh CAPTCHA dan Challenge tindakan dan oleh SDK

integrasi aplikasi yang Anda terapkan saat Anda menggunakan grup aturan Aturan AWS Terkelola untuk pencegahan AWS WAF penipuan pembuatan akun Kontrol Penipuan (ACFP), pencegahan pengambilalihan akun Kontrol AWS WAF Penipuan (ATP), dan Kontrol Bot. AWS WAF

Sufiks publik tidak diizinkan. Misalnya, Anda tidak dapat menggunakan `gov.au` atau `co.uk` sebagai domain token.

Secara default, AWS WAF menerima token hanya untuk domain sumber daya yang dilindungi. Jika Anda menambahkan domain token dalam daftar ini, AWS WAF menerima token untuk semua domain dalam daftar dan untuk domain sumber daya terkait. Untuk informasi selengkapnya, lihat AWS WAF konfigurasi daftar domain token ACL web.

16. Pilih Berikutnya.
17. Di halaman Tetapkan prioritas aturan, pilih dan pindahkan aturan dan grup aturan Anda ke urutan yang AWS WAF ingin Anda proses. AWS WAF Memproses aturan mulai dari bagian atas daftar. Saat Anda menyimpan web ACL AWS WAF menetapkan pengaturan prioritas numerik ke aturan, dalam urutan yang Anda daftarkan. Untuk informasi selengkapnya, lihat Memproses urutan aturan dan kelompok aturan dalam ACL web.
18. Pilih Berikutnya.
19. Di halaman Konfigurasi metrik, tinjau opsi dan terapkan pembaruan apa pun yang Anda butuhkan. Anda dapat menggabungkan metrik dari berbagai sumber dengan memberikan nama CloudWatch metrik yang sama untuk mereka.
20. Pilih Berikutnya.
21. Di halaman Tinjau dan buat web ACL, periksa definisi Anda. Jika Anda ingin mengubah area apa pun, pilih Edit untuk area tersebut. Ini mengembalikan Anda ke halaman di wizard ACL web. Buat perubahan apa pun, lalu pilih Berikutnya melalui halaman sampai Anda kembali ke halaman Review dan buat web ACL.
22. Pilih Buat web ACL. ACL web baru Anda tercantum di halaman ACL Web.

Mengedit ACL web

Untuk menambah atau menghapus aturan dari ACL web atau mengubah pengaturan konfigurasi, akses ACL web menggunakan prosedur di halaman ini. Saat memperbarui ACL web, AWS WAF menyediakan cakupan berkelanjutan ke sumber daya yang telah Anda kaitkan dengan ACL web.

Risiko lalu lintas produksi

Sebelum Anda menerapkan perubahan di ACL web Anda untuk lalu lintas produksi, uji dan sesuaikan di lingkungan pementasan atau pengujian hingga Anda merasa nyaman dengan potensi dampak terhadap lalu lintas Anda. Kemudian uji dan sesuaikan aturan Anda yang diperbarui dalam mode hitungan dengan lalu lintas produksi Anda sebelum mengaktifkannya. Untuk panduan, lihat Menguji dan menyetel perlindungan Anda AWS WAF.

Note

Menggunakan lebih dari 1.500 WCU dalam ACL web menimbulkan biaya di luar harga ACL web dasar. Untuk informasi selengkapnya, lihat AWS WAF unit kapasitas ACL web (WCU) dan Harga AWS WAF.

Untuk mengedit ACL web

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.
2. Di panel navigasi, pilih Web ACL.
3. Pilih nama ACL web yang ingin Anda edit. Konsol membawa Anda ke deskripsi ACL web.

   Note

   Web ACL yang dikelola oleh AWS Firewall Manager memiliki nama yang dimulai dengan`FMManagedWebACLV2-`. Administrator Firewall Manager mengelola ini dalam AWS WAF kebijakan Firewall Manager. ACL web ini mungkin berisi kumpulan grup aturan yang ditetapkan untuk dijalankan pertama dan terakhir di ACL web, di kedua sisi aturan atau grup aturan apa pun yang Anda tambahkan dan kelola. Anda tidak dapat mengubah spesifikasi grup aturan pertama dan terakhir ini. Kelompok aturan pertama dan terakhir memiliki nama yang dimulai dengan `PREFMManaged-` dan`POSTFMManaged-`, masing-masing. Untuk informasi selengkapnya tentang kebijakan ini, lihatAWS WAF kebijakan.
4. Edit ACL web sesuai kebutuhan. Pilih tab untuk area konfigurasi yang Anda minati dan edit pengaturan yang bisa berubah. Untuk setiap pengaturan yang Anda edit, ketika Anda memilih

Simpan dan kembali ke halaman deskripsi ACL web, konsol menyimpan perubahan Anda ke ACL web.

Berikut ini daftar tab yang berisi komponen konfigurasi ACL web.

- Tab Aturan
  - Aturan yang didefinisikan dalam ACL web — Anda dapat mengedit dan mengelola aturan yang telah Anda tetapkan di ACL web mirip dengan yang Anda lakukan selama pembuatan ACL web.

    > **Note**
    >
    > Jangan mengubah nama aturan apa pun yang tidak Anda tambahkan dengan tangan ke ACL web Anda. Jika Anda menggunakan layanan lain untuk mengelola aturan untuk Anda, mengubah nama mereka dapat menghapus atau mengurangi kemampuan mereka untuk memberikan perlindungan yang dimaksudkan. AWS Shield Advanced dan AWS Firewall Manager keduanya membuat aturan di ACL web Anda. Untuk informasi, lihat Grup aturan yang disediakan oleh layanan lain.

    > **Note**
    >
    > Jika Anda mengubah nama aturan dan Anda ingin nama metrik aturan mencerminkan perubahan, Anda harus memperbarui nama metrik juga. AWS WAF tidak secara otomatis memperbarui nama metrik untuk aturan saat Anda mengubah nama aturan. Anda dapat mengubah nama metrik saat mengedit aturan di konsol, dengan menggunakan editor JSON aturan. Anda juga dapat mengubah kedua nama melalui API dan dalam daftar JSON apa pun yang Anda gunakan untuk menentukan ACL web atau grup aturan.

    Untuk informasi tentang aturan dan pengaturan grup aturan, lihat AWS WAF aturan danAWS WAF kelompok aturan.
  - Unit kapasitas aturan ACL Web yang digunakan — Penggunaan kapasitas saat ini untuk ACL web Anda. Ini hanya tampilan.
  - Tindakan ACL web default untuk permintaan yang tidak cocok dengan aturan apa pun — Untuk informasi tentang setelan ini, lihatTindakan default ACL web.

    - Web ACL CAPTCHA dan konfigurasi tantangan — Waktu kekebalan ini menentukan berapa lama CAPTCHA atau token tantangan tetap valid setelah diperoleh. Anda hanya dapat mengubah pengaturan ini di sini, setelah Anda membuat web ACL. Untuk informasi tentang pengaturan ini, lihat Kedaluwarsa stempel waktu: waktu kekebalan token AWS WAF.
    - Daftar domain Token — AWS WAF menerima token untuk semua domain dalam daftar dan untuk domain sumber daya terkait. Untuk informasi selengkapnya, lihat AWS WAF konfigurasi daftar domain token ACL web.
- Tab AWS sumber daya terkait
    - Batas ukuran pemeriksaan permintaan web - Termasuk hanya untuk ACL web yang melindungi CloudFront distribusi. Batas ukuran inspeksi tubuh menentukan berapa banyak komponen tubuh yang diteruskan AWS WAF untuk diperiksa. Untuk informasi selengkapnya tentang pengaturan ini, lihatMengelola batas ukuran inspeksi tubuh.
    - AWS Sumber daya terkait — Daftar sumber daya yang saat ini dikaitkan dan dilindungi oleh ACL web. Anda dapat menemukan sumber daya yang berada dalam Wilayah yang sama dengan ACL web dan mengaitkannya ke ACL web. Untuk informasi selengkapnya, lihat Mengaitkan atau memisahkan ACL web dengan sumber daya AWS.
- Tab badan respons khusus
    - Badan respons khusus yang tersedia untuk digunakan oleh aturan ACL web Anda yang memiliki tindakan yang disetel keBlock. Untuk informasi selengkapnya, lihat Tanggapan khusus untuk Block tindakan.
- Tab logging dan metrik
    - Logging — Logging untuk lalu lintas yang dievaluasi ACL web. Untuk informasi, lihat Pencatatan AWS WAF lalu lintas ACL web.
    - Permintaan sampel — Informasi tentang aturan yang cocok dengan permintaan web. Untuk informasi tentang melihat permintaan sampel, lihatMelihat contoh permintaan web.
    - CloudWatch metrik — Metrik untuk aturan di ACL web Anda. Untuk informasi tentang CloudWatch metrik Amazon, lihatPemantauan CloudWatch dengan Amazon.

Ketidakkonsistenan sementara selama pembaruan

Saat Anda membuat atau mengubah ACL web atau AWS WAF sumber daya lainnya, perubahan membutuhkan sedikit waktu untuk menyebar ke semua area tempat sumber daya disimpan. Waktu propagasi bisa dari beberapa detik hingga beberapa menit.

Berikut ini adalah contoh inkonsistensi sementara yang mungkin Anda perhatikan selama propagasi perubahan:

- Setelah Anda membuat ACL web, jika Anda mencoba mengaitkannya dengan sumber daya, Anda mungkin mendapatkan pengecualian yang menunjukkan bahwa ACL web tidak tersedia.
- Setelah Anda menambahkan grup aturan ke ACL web, aturan grup aturan baru mungkin berlaku di satu area di mana ACL web digunakan dan tidak di area lain.
- Setelah mengubah setelan tindakan aturan, Anda mungkin melihat tindakan lama di beberapa tempat dan tindakan baru di tempat lain.
- Setelah Anda menambahkan alamat IP ke set IP yang digunakan dalam aturan pemblokiran, alamat baru mungkin diblokir di satu area sementara masih diizinkan di area lain.

Mengelola perilaku grup aturan di ACL web

Bagian ini menjelaskan opsi Anda untuk memodifikasi cara Anda menggunakan grup aturan di ACL web Anda. Informasi ini berlaku untuk semua jenis grup aturan. Setelah menambahkan grup aturan ke ACL web, Anda dapat mengganti tindakan aturan individual dalam grup aturan ke Count atau ke setelan tindakan aturan lain yang valid. Anda juga dapat mengganti tindakan grup aturan yang dihasilkanCount, yang tidak berpengaruh pada bagaimana aturan dievaluasi di dalam grup aturan.

Untuk informasi tentang opsi ini, lihat Opsi penggantian tindakan untuk grup aturan.

Mengesampingkan tindakan aturan dalam grup aturan

Untuk setiap grup aturan di ACL web, Anda dapat mengganti tindakan aturan yang terkandung untuk beberapa atau semua aturan.

Kasus penggunaan yang paling umum untuk ini adalah mengesampingkan tindakan aturan Count untuk menguji aturan baru atau yang diperbarui. Jika metrik diaktifkan, Anda menerima metrik untuk setiap aturan yang Anda timpa. Untuk informasi lebih lanjut tentang pengujian, lihatMenguji dan menyetel perlindungan Anda AWS WAF.

Untuk mengganti tindakan aturan dalam grup aturan

Anda dapat membuat perubahan ini saat menambahkan grup aturan terkelola ke ACL web, dan Anda dapat membuatnya ke semua jenis grup aturan saat mengedit ACL web. Instruksi ini untuk grup aturan yang telah ditambahkan ke ACL web. Lihat informasi tambahan tentang opsi ini diPengesampingan tindakan aturan kelompok aturan.

1. Edit ACL web.
2. Di tab Aturan halaman ACL web, pilih grup aturan, lalu pilih Edit.
3. Di bagian Aturan untuk grup aturan, kelola pengaturan tindakan sesuai kebutuhan.
   - Semua aturan — Untuk menetapkan tindakan penggantian untuk semua aturan dalam grup aturan, buka dropdown Override all rule actions dan pilih tindakan override. Untuk menghapus penggantian untuk semua aturan, pilih Hapus semua penggantian.
   - Aturan tunggal — Untuk menetapkan tindakan override untuk satu aturan, buka dropdown aturan dan pilih tindakan override. Untuk menghapus penggantian aturan, buka dropdown aturan dan pilih Hapus penggantian.
4. Setelah selesai membuat perubahan, pilih Simpan aturan. Tindakan aturan dan pengaturan tindakan penggantian tercantum di halaman grup aturan.

Contoh daftar JSON berikut menunjukkan deklarasi grup aturan di dalam ACL web yang mengesampingkan tindakan aturan Count untuk aturan dan. `CategoryVerifiedSearchEngine` `CategoryVerifiedSocialMedia` Di JSON, Anda mengganti semua tindakan aturan dengan menyediakan `RuleActionOverrides` entri untuk setiap aturan individual.

```
{
    "Name": "AWS-AWSBotControl-Example",
   "Priority": 5,
   "Statement": {
    "ManagedRuleGroupStatement": {
        "VendorName": "AWS",
        "Name": "AWSManagedRulesBotControlRuleSet",
        "RuleActionOverrides": [
          {
            "ActionToUse": {
              "Count": {}
            },
            "Name": "CategoryVerifiedSearchEngine"
          },
          {
            "ActionToUse": {
              "Count": {}
            },
            "Name": "CategoryVerifiedSocialMedia"
          }
        ],
```

```
        "ExcludedRules": []
    },
   "VisibilityConfig": {
       "SampledRequestsEnabled": true,
       "CloudWatchMetricsEnabled": true,
       "MetricName": "AWS-AWSBotControl-Example"
   }
}
```

Mengesampingkan hasil evaluasi kelompok aturan ke Count

Anda dapat mengganti tindakan yang dihasilkan dari evaluasi grup aturan, tanpa mengubah cara aturan dalam grup aturan dikonfigurasi atau dievaluasi. Opsi ini tidak umum digunakan. Jika ada aturan dalam grup aturan yang menghasilkan kecocokan, penggantian ini akan menetapkan tindakan yang dihasilkan dari grup aturan menjadiCount.

> **Note**
>
> Ini adalah kasus penggunaan yang tidak umum. Sebagian besar penggantian tindakan dilakukan pada tingkat aturan, di dalam grup aturan, seperti yang dijelaskan dalam. Mengesampingkan tindakan aturan dalam grup aturan

Anda dapat mengganti tindakan yang dihasilkan grup aturan di ACL web saat menambahkan atau mengedit grup aturan. Di konsol, buka tindakan grup aturan Override grup aturan - panel opsional dan aktifkan penggantian. Dalam JSON ditetapkan `OverrideAction` dalam pernyataan kelompok aturan, seperti yang ditunjukkan dalam daftar contoh berikut:

```
{
   "Name": "AWS-AWSBotControl-Example",
   "Priority": 5,
   "Statement": {
    "ManagedRuleGroupStatement": {
     "VendorName": "AWS",
     "Name": "AWSManagedRulesBotControlRuleSet"
     }
   },
    "OverrideAction": {
       "Count": {}
    },
   "VisibilityConfig": {
```

```
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSBotControl-Example"
    }
}
```

Mengaitkan atau memisahkan ACL web dengan sumber daya AWS

Anda dapat menggunakan AWS WAF untuk membuat asosiasi berikut antara ACLS web dan sumber daya Anda:

- Kaitkan ACL web regional dengan salah satu sumber daya regional yang tercantum di bawah ini. Untuk opsi ini, ACL web harus berada di wilayah yang sama dengan sumber daya Anda.
  - API REST Amazon API Gateway
  - Penyeimbang Beban Aplikasi
  - AWS AppSync GraphQL API
  - Kolam pengguna Amazon Cognito
  - AWS App Runner layanan
  - AWS Instans Akses Terverifikasi
- Kaitkan ACL web global dengan CloudFront distribusi Amazon. ACL web global akan memiliki Wilayah Wilayah AS Timur (Virginia N.) yang dikodekan dengan keras.

Anda juga dapat mengaitkan ACL web dengan CloudFront distribusi saat Anda membuat atau memperbarui distribusi itu sendiri. Untuk selengkapnya, lihat Menggunakan AWS WAF untuk Mengontrol Akses ke Konten Anda di Panduan CloudFront Pengembang Amazon.

Pembatasan pada beberapa asosiasi

Anda dapat mengaitkan satu ACL web dengan satu atau lebih AWS sumber daya, sesuai dengan batasan berikut:

- Anda dapat mengaitkan setiap AWS sumber daya hanya dengan satu ACL web. Hubungan antara web ACL dan AWS sumber daya adalah one-to-many.
- Anda dapat mengaitkan ACL web dengan satu atau lebih CloudFront distribusi. Anda tidak dapat mengaitkan ACL web yang telah Anda kaitkan dengan CloudFront distribusi dengan jenis AWS sumber daya lainnya.

Pembatasan tambahan

Pembatasan tambahan berikut berlaku untuk asosiasi ACL web:

- Anda hanya dapat mengaitkan ACL web ke Application Load Wilayah AWS Balancer di dalamnya. Misalnya, Anda tidak dapat mengaitkan ACL web ke Application Load Balancer yang aktif. AWS Outposts
- Anda tidak dapat mengaitkan kumpulan pengguna Amazon Cognito dengan ACL web yang menggunakan grup aturan terkelola pencegahan AWS WAF penipuan pembuatan akun Kontrol Penipuan (ACFP) `AWSManagedRulesACFPRuleSet` atau grup aturan terkelola pencegahan pengambilalihan akun Kontrol AWS WAF Penipuan (ATP). `AWSManagedRulesATPRuleSet` Untuk informasi tentang pencegahan penipuan pembuatan akun, lihatAWS WAF Pencegahan penipuan pembuatan akun Kontrol Penipuan (ACFP). Untuk informasi tentang pencegahan pengambilalihan akun, lihatAWS WAF Pencegahan pengambilalihan akun Kontrol Penipuan (ATP).

⚠ Risiko lalu lintas produksi

Sebelum Anda menyebarkan ACL web Anda untuk lalu lintas produksi, uji dan sesuaikan di lingkungan pementasan atau pengujian sampai Anda merasa nyaman dengan dampak potensial terhadap lalu lintas Anda. Kemudian uji dan sesuaikan aturan Anda dalam mode hitungan dengan lalu lintas produksi Anda sebelum mengaktifkannya. Untuk panduan, lihat Menguji dan menyetel perlindungan Anda AWS WAF.

Untuk mengaitkan ACL web dengan sumber daya AWS

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.
2. Di panel navigasi, pilih Web ACL.
3. Pilih nama ACL web yang ingin Anda kaitkan dengan sumber daya. Konsol membawa Anda ke deskripsi ACL web, di mana Anda dapat mengeditnya.
4. Pada tab AWS Sumber daya terkait, pilih Tambahkan AWS sumber daya.
5. Saat diminta, pilih jenis sumber daya, pilih tombol radio di sebelah sumber daya yang ingin Anda kaitkan, lalu pilih Tambah.

Untuk memisahkan ACL web dari sumber daya AWS

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.
2. Di panel navigasi, pilih Web ACL.
3. Pilih nama ACL web yang ingin Anda putuskan dari sumber daya Anda. Konsol membawa Anda ke deskripsi ACL web, di mana Anda dapat mengeditnya.
4. Pada tab AWS Sumber daya terkait, pilih sumber daya yang ingin Anda putuskan dari ACL web ini.

   > **Note**
   >
   > Anda harus memisahkan satu sumber daya pada satu waktu. Jangan memilih banyak sumber daya.

5. Pilih Pisahkan. Konsol membuka dialog konfirmasi. Konfirmasikan pilihan Anda untuk memisahkan ACL web dari sumber daya. AWS

Menghapus ACL web

Untuk menghapus ACL web, pertama-tama Anda memisahkan semua AWS sumber daya dari ACL web. Lakukan prosedur berikut.

Untuk menghapus ACL web

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.
2. Di panel navigasi, pilih Web ACL.
3. Pilih nama ACL web yang ingin Anda hapus. Konsol membawa Anda ke deskripsi ACL web, di mana Anda dapat mengeditnya.
4. Pada tab AWS Sumber daya terkait, untuk setiap sumber daya terkait, pilih tombol radio di sebelah nama sumber daya, lalu pilih Putuskan. Ini memisahkan ACL web dari sumber daya Anda. AWS
5. Di panel navigasi, pilih Web ACL.
6. Pilih tombol radio di sebelah ACL web yang Anda hapus, lalu pilih Hapus.

AWS WAF kelompok aturan

Grup aturan adalah seperangkat aturan yang dapat digunakan kembali yang dapat Anda tambahkan ke ACL web. Untuk informasi selengkapnya tentang ACL web, lihatAWS WAF daftar kontrol akses web (ACL web).

Kelompok aturan termasuk dalam kategori utama berikut:

- Grup aturan Anda sendiri, yang Anda buat dan pertahankan.
- Grup aturan AWS terkelola yang dibuat dan dipelihara oleh tim Aturan Terkelola untuk Anda.
- Grup aturan terkelola yang dibuat dan dipelihara AWS Marketplace penjual untuk Anda.
- Grup aturan yang dimiliki dan dikelola oleh layanan lain seperti AWS Firewall Manager dan Shield Advanced.

Perbedaan antara grup aturan dan ACL web

Grup aturan dan ACL web keduanya berisi aturan, yang didefinisikan dengan cara yang sama di kedua tempat. Grup aturan berbeda dari ACL web dengan cara berikut:

- Grup aturan tidak dapat berisi pernyataan referensi grup aturan.
- Anda dapat menggunakan kembali grup aturan tunggal di beberapa ACL web dengan menambahkan pernyataan referensi grup aturan ke setiap ACL web. Anda tidak dapat menggunakan kembali ACL web.
- Grup aturan tidak memiliki tindakan default. Di ACL web, Anda menetapkan tindakan default untuk setiap aturan atau grup aturan yang Anda sertakan. Setiap aturan individu di dalam grup aturan atau web ACL memiliki tindakan yang ditentukan.
- Anda tidak secara langsung mengaitkan grup aturan dengan AWS sumber daya. Untuk melindungi sumber daya menggunakan grup aturan, Anda menggunakan grup aturan di ACL web.
- Web ACL memiliki kapasitas maksimum yang ditentukan sistem sebesar 5.000 unit kapasitas ACL web (WCU). Setiap grup aturan memiliki pengaturan WCU yang harus ditetapkan pada saat pembuatan. Anda dapat menggunakan pengaturan ini untuk menghitung persyaratan kapasitas tambahan yang akan ditambahkan oleh grup aturan ke ACL web Anda. Untuk informasi lebih lanjut tentang WCU, lihatAWS WAF unit kapasitas ACL web (WCU).

Untuk informasi tentang aturan, lihat AWS WAF aturan.

Bagian ini memberikan panduan untuk membuat dan mengelola grup aturan Anda sendiri, menjelaskan grup aturan terkelola yang tersedia untuk Anda, dan memberikan panduan untuk menggunakan grup aturan terkelola.

Topik

Grup aturan terkelola

Grup aturan terkelola adalah kumpulan ready-to-use aturan yang telah ditentukan sebelumnya, yang ditulis AWS dan dipelihara oleh AWS Marketplace penjual untuk Anda. AWS WAF Harga dasar berlaku untuk penggunaan grup aturan terkelola oleh Anda. Untuk informasi AWS WAF harga, lihat AWS WAF Harga.

- Kelompok aturan Aturan AWS Terkelola untuk Kontrol AWS WAF Bot, Pencegahan Pengambilalihan Akun Kontrol AWS WAF Penipuan (ATP), dan pencegahan AWS WAF penipuan pembuatan akun Kontrol Penipuan (ACFP) tersedia dengan biaya tambahan, di luar biaya dasar. AWS WAF Untuk detail harga, lihat AWS WAF Harga.
- Semua grup aturan Aturan AWS Terkelola lainnya tersedia untuk AWS WAF pelanggan tanpa biaya tambahan.
- AWS Marketplace grup aturan terkelola tersedia dengan berlangganan melalui AWS Marketplace. Masing-masing kelompok aturan ini dimiliki dan dikelola oleh AWS Marketplace penjual. Untuk informasi harga menggunakan grup aturan AWS Marketplace terkelola, hubungi AWS Marketplace penjual.

Beberapa grup aturan terkelola dirancang untuk membantu melindungi jenis aplikasi web tertentu sepertiWordPress, Joomla, atau PHP. Yang lain menawarkan perlindungan luas terhadap ancaman yang diketahui atau kerentanan aplikasi web umum, termasuk beberapa yang tercantum dalam OWASP Top 10. Jika Anda tunduk pada kepatuhan peraturan seperti PCI atau HIPAA, Anda mungkin dapat menggunakan grup aturan terkelola untuk memenuhi persyaratan firewall aplikasi web.

Pembaruan otomatis

Terus memantau kondisi terbaru terkait lanskap ancaman yang terus berubah dapat memakan waktu dan biaya yang besar. Grup aturan terkelola dapat menghemat waktu Anda saat menerapkan

dan menggunakan AWS WAF. Banyak AWS dan AWS Marketplace penjual secara otomatis memperbarui grup aturan terkelola dan menyediakan versi baru grup aturan saat kerentanan dan ancaman baru muncul.

Dalam beberapa kasus, AWS diberitahukan tentang kerentanan baru sebelum pengungkapan publik, karena partisipasinya dalam sejumlah komunitas pengungkapan pribadi. Dalam kasus tersebut, AWS dapat memperbarui grup aturan Aturan AWS Terkelola dan menyebarkannya untuk Anda bahkan sebelum ancaman baru diketahui secara luas.

Akses terbatas ke aturan dalam grup aturan terkelola

Setiap grup aturan terkelola memberikan deskripsi komprehensif tentang jenis serangan dan kerentanan yang dirancang untuk melindunginya. Untuk melindungi kekayaan intelektual penyedia grup aturan, Anda tidak dapat melihat semua detail untuk aturan individual dalam grup aturan. Pembatasan ini juga membantu mencegah pengguna jahat merancang ancaman yang secara khusus menghindari aturan yang diterbitkan.

Topik

- Grup aturan terkelola berversi
- Bekerja dengan kelompok aturan terkelola
- AWS Aturan Terkelola untuk AWS WAF
- AWS Marketplace kelompok aturan terkelola

Grup aturan terkelola berversi

Banyak penyedia grup aturan terkelola menggunakan pembuatan versi untuk memperbarui opsi dan kemampuan grup aturan. Biasanya, versi spesifik dari grup aturan terkelola bersifat statis. Kadang-kadang, penyedia mungkin perlu memperbarui beberapa atau semua versi statis dari grup aturan terkelola, misalnya, untuk menanggapi ancaman keamanan yang muncul.

Bila Anda menggunakan grup aturan terkelola berversi di ACL web Anda, Anda dapat memilih versi default dan membiarkan penyedia mengelola versi statis yang Anda gunakan, atau Anda dapat memilih versi statis tertentu.

Tidak dapat menemukan versi yang Anda inginkan?

Jika Anda tidak melihat versi dalam daftar versi grup aturan, versi mungkin dijadwalkan kedaluwarsa atau sudah kedaluwarsa. Setelah versi dijadwalkan kedaluwarsa, Anda AWS WAF tidak lagi dapat memilihnya untuk grup aturan.

Pemberitahuan SNS untuk grup aturan Aturan AWS Terkelola

Aturan Aturan AWS Terkelola mengelompokkan semuanya menyediakan pemberitahuan pemutakhiran versi dan pembaruan SNS kecuali untuk grup aturan reputasi IP. Grup aturan Aturan AWS Terkelola yang menyediakan notifikasi semuanya menggunakan topik SNS yang sama Nama Sumber Daya Amazon (ARN). Untuk mendaftar notifikasi SNS, lihatMendapatkan pemberitahuan tentang versi dan pembaruan baru.

Topik

- Siklus hidup versi untuk grup aturan terkelola
- Kedaluwarsa versi untuk grup aturan terkelola
- Praktik terbaik untuk menangani versi grup aturan terkelola

Siklus hidup versi untuk grup aturan terkelola

Penyedia menangani tahapan siklus hidup berikut dari versi statis grup aturan terkelola:

- Rilis dan pembaruan — Penyedia grup aturan terkelola mengumumkan versi statis yang akan datang dan baru dari grup aturan terkelola mereka melalui pemberitahuan ke topik Amazon Simple Notification Service (Amazon SNS). Penyedia mungkin juga menggunakan topik untuk mengkomunikasikan informasi penting lainnya tentang kelompok aturan mereka, seperti pembaruan yang diperlukan secara mendesak.

  Anda dapat berlangganan topik grup aturan dan mengonfigurasi cara Anda ingin menerima notifikasi. Untuk mengetahui informasi selengkapnya, lihat Mendapatkan pemberitahuan tentang versi dan pembaruan baru.
- Penjadwalan kedaluwarsa — Penyedia grup aturan terkelola menjadwalkan versi grup aturan yang lebih lama untuk kedaluwarsa. Versi yang dijadwalkan kedaluwarsa tidak dapat ditambahkan ke aturan ACL web Anda. Setelah kedaluwarsa dijadwalkan untuk versi, lacak AWS WAF kedaluwarsa dengan metrik hitung mundur di Amazon. CloudWatch
- Kedaluwarsa versi — Jika Anda memiliki ACL web yang dikonfigurasi untuk menggunakan versi kedaluwarsa grup aturan terkelola, maka selama evaluasi ACL web, AWS WAF gunakan versi default grup aturan. Selain itu, AWS WAF memblokir pembaruan apa pun ke ACL web yang tidak menghapus grup aturan atau mengubah versinya menjadi yang belum kedaluwarsa.

Jika Anda menggunakan grup aturan AWS Marketplace terkelola, tanyakan penyedia informasi tambahan tentang siklus hidup versi.

Kedaluwarsa versi untuk grup aturan terkelola

Jika Anda menggunakan versi tertentu dari grup aturan, pastikan Anda tidak tetap menggunakan versi yang melewati tanggal kedaluwarsanya. Anda dapat memantau kedaluwarsa versi melalui notifikasi SNS grup aturan dan melalui metrik Amazon. CloudWatch

Jika versi yang Anda gunakan di ACL web kedaluwarsa, AWS WAF blokir pembaruan apa pun ke ACL web yang tidak termasuk memindahkan grup aturan ke versi yang belum kedaluwarsa. Anda dapat memperbarui grup aturan ke versi yang tersedia atau menghapusnya dari ACL web Anda.

Penanganan kedaluwarsa untuk grup aturan terkelola bergantung pada penyedia grup aturan. Untuk grup aturan Aturan AWS Terkelola, versi kedaluwarsa secara otomatis diubah ke versi default grup aturan. Untuk grup AWS Marketplace aturan, tanyakan penyedia bagaimana mereka menangani kedaluwarsa.

Saat penyedia membuat versi baru dari grup aturan, penyedia menetapkan perkiraan masa pakai versi. Meskipun versi tidak dijadwalkan kedaluwarsa, nilai CloudWatch metrik Amazon disetel ke pengaturan masa pakai yang diperkirakan, dan di CloudWatch, Anda akan melihat nilai datar untuk metrik tersebut. Setelah penyedia menjadwalkan metrik untuk kedaluwarsa, nilai metrik berkurang setiap hari hingga mencapai nol pada hari kedaluwarsa. Untuk informasi tentang pemantauan kedaluwarsa, lihat. Melacak kedaluwarsa versi

Praktik terbaik untuk menangani versi grup aturan terkelola

Ikuti panduan praktik terbaik ini untuk menangani pembuatan versi saat Anda menggunakan grup aturan terkelola berversi.

Bila Anda menggunakan grup aturan terkelola di ACL web Anda, Anda dapat memilih untuk menggunakan versi statis tertentu dari grup aturan, atau Anda dapat memilih untuk menggunakan versi default:

- Versi default — AWS WAF selalu menetapkan versi default ke versi statis yang saat ini direkomendasikan oleh penyedia. Saat penyedia memperbarui versi statis yang direkomendasikan, AWS WAF secara otomatis memperbarui setelan versi default untuk grup aturan di ACL web Anda.

  Bila Anda menggunakan versi default grup aturan terkelola, lakukan hal berikut sebagai praktik terbaik:

  - Berlangganan notifikasi — Berlangganan pemberitahuan untuk perubahan pada grup aturan dan awasi itu. Sebagian besar penyedia mengirim pemberitahuan lanjutan tentang versi statis

baru dan perubahan versi default. Ini memungkinkan Anda memeriksa efek dari versi statis baru sebelum AWS beralih versi default ke versi itu. Untuk mengetahui informasi selengkapnya, lihat Mendapatkan pemberitahuan tentang versi dan pembaruan baru.

- Tinjau efek pengaturan versi statis dan buat penyesuaian sesuai kebutuhan sebelum default Anda disetel ke sana — Sebelum default Anda diatur ke versi statis baru, tinjau efek versi statis pada pemantauan dan pengelolaan permintaan web Anda. Versi statis baru mungkin memiliki aturan baru untuk ditinjau. Cari positif palsu atau perilaku tak terduga lainnya, jika Anda perlu mengubah cara Anda menggunakan grup aturan. Anda dapat menetapkan aturan untuk menghitung, misalnya, untuk menghentikannya memblokir lalu lintas saat Anda mengetahui bagaimana Anda ingin menangani perilaku baru. Untuk informasi selengkapnya, lihat Menguji dan menyetel perlindungan Anda AWS WAF.

- Versi statis - Jika Anda memilih untuk menggunakan versi statis, Anda harus memperbarui pengaturan versi secara manual saat Anda siap untuk mengadopsi versi baru dari grup aturan.

  Bila Anda menggunakan versi statis dari grup aturan terkelola, lakukan hal berikut sebagai praktik terbaik:

  - Tetap perbarui versi Anda — Pertahankan grup aturan terkelola sedekat mungkin dengan versi terbaru. Saat versi baru dirilis, ujilah, sesuaikan pengaturan sesuai kebutuhan, dan terapkan tepat waktu. Untuk informasi tentang pengujian, lihatMenguji dan menyetel perlindungan Anda AWS WAF.
  - Berlangganan notifikasi — Berlangganan notifikasi untuk perubahan pada grup aturan, sehingga Anda tahu kapan penyedia Anda merilis versi statis baru. Sebagian besar penyedia memberikan pemberitahuan lanjutan tentang perubahan versi. Selain itu, penyedia Anda mungkin perlu memperbarui versi statis yang Anda gunakan untuk menutup celah keamanan atau karena alasan mendesak lainnya. Anda akan tahu apa yang terjadi jika berlangganan notifikasi penyedia. Untuk informasi selengkapnya, lihat Mendapatkan pemberitahuan tentang versi dan pembaruan baru.
  - Hindari kedaluwarsa versi - Jangan biarkan versi statis kedaluwarsa saat Anda menggunakannya. Penanganan penyedia versi kedaluwarsa dapat bervariasi dan mungkin termasuk memaksa upgrade ke versi yang tersedia atau perubahan lain yang dapat memiliki konsekuensi tak terduga. Lacak metrik AWS WAF kedaluwarsa dan setel alarm yang memberi Anda jumlah hari yang cukup untuk berhasil meningkatkan ke versi yang didukung. Untuk informasi selengkapnya, lihat Melacak kedaluwarsa versi.

Bekerja dengan kelompok aturan terkelola

Bagian ini memberikan panduan untuk mengakses dan mengelola grup aturan terkelola Anda.

Saat menambahkan grup aturan terkelola ke ACL web, Anda dapat memilih opsi konfigurasi yang sama seperti grup aturan Anda sendiri, ditambah pengaturan tambahan.

Melalui konsol, Anda mengakses informasi grup aturan terkelola selama proses menambahkan dan mengedit aturan di ACL web Anda. Melalui API dan antarmuka baris perintah (CLI), Anda dapat langsung meminta informasi grup aturan terkelola.

Bila Anda menggunakan grup aturan terkelola di ACL web Anda, Anda dapat mengedit pengaturan berikut:

- Versi - Ini hanya tersedia jika grup aturan berversi. Untuk informasi selengkapnya, lihat Grup aturan terkelola berversi.
- Mengganti tindakan aturan — Anda dapat mengganti tindakan untuk aturan dalam grup aturan ke tindakan apa pun. CountMengaturnya berguna untuk menguji grup aturan sebelum menggunakannya untuk mengelola permintaan web Anda. Untuk informasi selengkapnya, lihat Pengesampingan tindakan aturan kelompok aturan.
- Pernyataan cakupan bawah - Anda dapat menambahkan pernyataan cakupan ke bawah, untuk menyaring permintaan web yang tidak ingin Anda evaluasi dengan grup aturan. Untuk informasi selengkapnya, lihat Pernyataan cakupan ke bawah.
- Ganti tindakan grup aturan — Anda dapat mengganti tindakan yang dihasilkan dari evaluasi grup aturan, dan mengaturnya menjadi Count hanya. Opsi ini tidak umum digunakan. Itu tidak mengubah cara AWS WAF mengevaluasi aturan dalam kelompok aturan. Untuk informasi selengkapnya, lihat Tindakan pengembalian grup aturan akan ditimpa Count.

Untuk mengedit pengaturan grup aturan terkelola di ACL web Anda

- Konsol
  - (Opsi) Saat menambahkan grup aturan terkelola ke ACL web, Anda dapat memilih Edit untuk melihat dan mengedit pengaturan.
  - (Opsi) Setelah Anda menambahkan grup aturan terkelola ke ACL web Anda, dari halaman ACL Web, pilih ACL web yang baru saja Anda buat. Ini membawa Anda ke halaman edit ACL web.
    - Pilih Aturan.
    - Pilih grup aturan, lalu pilih Edit untuk melihat dan mengedit pengaturan.

- API dan CLI — Di luar konsol, Anda dapat mengelola pengaturan grup aturan terkelola saat membuat dan memperbarui ACL web.

Mengambil daftar grup aturan terkelola

Anda dapat mengambil daftar grup aturan terkelola yang tersedia untuk Anda gunakan di ACL web Anda. Daftar ini mencakup yang berikut:

- Semua grup aturan Aturan AWS Terkelola.
- Grup AWS Marketplace aturan yang telah Anda berlangganan.

> **Note**
>
> Untuk informasi tentang berlangganan grup AWS Marketplace aturan, lihatAWS Marketplace kelompok aturan terkelola.

Saat Anda mengambil daftar grup aturan terkelola, daftar yang Anda dapatkan kembali bergantung pada antarmuka yang Anda gunakan:

- Konsol — Melalui konsol, Anda dapat melihat semua grup aturan terkelola, termasuk grup AWS Marketplace aturan yang belum berlangganan. Untuk yang belum berlangganan, antarmuka menyediakan tautan yang dapat Anda ikuti untuk berlangganan.
- API dan CLI — Di luar konsol, permintaan Anda hanya menampilkan grup aturan yang tersedia untuk Anda gunakan.

Untuk mengambil daftar grup aturan terkelola

- Konsol — Selama proses pembuatan ACL web, pada halaman Tambahkan aturan dan grup aturan, pilih Tambahkan grup aturan terkelola. Di tingkat atas, nama penyedia terdaftar. Perluas setiap daftar penyedia untuk melihat daftar grup aturan terkelola. Untuk grup aturan berversi, informasi yang ditampilkan pada level ini adalah untuk versi default. Saat Anda menambahkan grup aturan terkelola ke ACL web Anda, konsol mencantumkannya berdasarkan skema `<Vendor Name>-<Managed Rule Group Name>` penamaan.
- API —
  - `ListAvailableManagedRuleGroups`
- CLI —

- `aws wafv2 list-available-managed-rule-groups --scope=<CLOUDFRONT|REGIONAL>`

Mengambil aturan dalam grup aturan terkelola

Anda dapat mengambil daftar aturan dalam grup aturan terkelola. Panggilan API dan CLI mengembalikan spesifikasi aturan yang dapat Anda referensikan dalam model JSON atau melalui. AWS CloudFormation

Untuk mengambil daftar aturan dalam grup aturan terkelola

- Konsol
  - (Opsi) Saat menambahkan grup aturan terkelola ke ACL web, Anda dapat memilih Edit untuk melihat aturan.
  - (Opsi) Setelah Anda menambahkan grup aturan terkelola ke ACL web Anda, dari halaman ACL Web, pilih ACL web yang baru saja Anda buat. Ini membawa Anda ke halaman edit ACL web.
    - Pilih Aturan.
    - Pilih grup aturan yang ingin Anda lihat daftar aturan, lalu pilih Edit. AWS WAF menunjukkan daftar aturan dalam kelompok aturan.
- API — `DescribeManagedRuleGroup`
- CLI — `aws wafv2 describe-managed-rule-group --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

Mengambil versi yang tersedia untuk grup aturan terkelola

Versi yang tersedia dari grup aturan terkelola adalah versi yang belum dijadwalkan untuk kedaluwarsa. Daftar menunjukkan versi mana yang merupakan versi default saat ini untuk grup aturan.

Untuk mengambil daftar versi yang tersedia dari grup aturan terkelola

- Konsol
  - (Opsi) Saat Anda menambahkan grup aturan terkelola ke ACL web Anda, pilih Edit untuk melihat informasi grup aturan. Perluas dropdown Versi untuk melihat daftar versi yang tersedia.

- (Opsi) Setelah menambahkan grup aturan terkelola ke ACL web Anda, pilih Edit di ACL web, lalu pilih dan edit aturan grup aturan. Perluas dropdown Versi untuk melihat daftar versi yang tersedia.

- API —
  - `ListAvailableManagedRuleGroupVersions`
- CLI —
  - `aws wafv2 list-available-managed-rule-group-versions --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

Menambahkan grup aturan terkelola ke ACL web melalui konsol

Panduan ini berlaku untuk semua grup aturan Aturan AWS Terkelola dan grup AWS Marketplace aturan tempat Anda berlangganan.

> **Risiko lalu lintas produksi**
>
> Sebelum Anda menerapkan perubahan di ACL web Anda untuk lalu lintas produksi, uji dan sesuaikan di lingkungan pementasan atau pengujian hingga Anda merasa nyaman dengan potensi dampak terhadap lalu lintas Anda. Kemudian uji dan sesuaikan aturan Anda yang diperbarui dalam mode hitungan dengan lalu lintas produksi Anda sebelum mengaktifkannya. Untuk panduan, lihat Menguji dan menyetel perlindungan Anda AWS WAF.

> **Note**
>
> Menggunakan lebih dari 1.500 WCU dalam ACL web menimbulkan biaya di luar harga ACL web dasar. Untuk informasi selengkapnya, lihat AWS WAF unit kapasitas ACL web (WCU) dan Harga AWS WAF.

Untuk menambahkan grup aturan terkelola ke ACL web melalui konsol

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.
2. Pilih Web ACL di panel navigasi.

3. Di halaman ACL Web, dari daftar ACL web, pilih salah satu yang ingin Anda tambahkan grup aturan. Ini membawa Anda ke halaman untuk ACL web tunggal.
4. Di halaman ACL web Anda, pilih tab Aturan.
5. Di panel Aturan, pilih Tambahkan aturan, lalu pilih Tambahkan grup aturan terkelola.
6. Di halaman Tambahkan grup aturan terkelola, perluas pilihan vendor grup aturan Anda, untuk melihat daftar grup aturan yang tersedia.
7. Untuk setiap grup aturan yang ingin Anda tambahkan, pilih Tambahkan ke web ACL. Jika Anda ingin mengubah konfigurasi ACL web untuk grup aturan, pilih Edit, buat perubahan, lalu pilih Simpan aturan. Untuk informasi tentang opsi, lihat panduan pembuatan versi di Grup aturan terkelola berversi dan panduan untuk menggunakan grup aturan terkelola di ACL web di. Pernyataan grup aturan terkelola
8. Di bagian bawah halaman Tambahkan grup aturan terkelola, pilih Tambahkan aturan.
9. Di halaman Tetapkan prioritas aturan, sesuaikan urutan aturan yang dijalankan sesuai kebutuhan, lalu pilih Simpan. Untuk informasi selengkapnya, lihat Memproses urutan aturan dan kelompok aturan dalam ACL web.

Di halaman ACL web Anda, grup aturan terkelola yang telah Anda tambahkan tercantum di bawah tab Aturan.

Uji dan sesuaikan perubahan apa pun pada AWS WAF perlindungan Anda sebelum Anda menggunakannya untuk lalu lintas produksi. Untuk informasi, lihat Menguji dan menyetel perlindungan Anda AWS WAF.

Ketidakkonsistenan sementara selama pembaruan

Saat Anda membuat atau mengubah ACL web atau AWS WAF sumber daya lainnya, perubahan membutuhkan sedikit waktu untuk menyebar ke semua area tempat sumber daya disimpan. Waktu propagasi bisa dari beberapa detik hingga beberapa menit.

Berikut ini adalah contoh inkonsistensi sementara yang mungkin Anda perhatikan selama propagasi perubahan:

- Setelah Anda membuat ACL web, jika Anda mencoba mengaitkannya dengan sumber daya, Anda mungkin mendapatkan pengecualian yang menunjukkan bahwa ACL web tidak tersedia.
- Setelah Anda menambahkan grup aturan ke ACL web, aturan grup aturan baru mungkin berlaku di satu area di mana ACL web digunakan dan tidak di area lain.

- Setelah mengubah setelan tindakan aturan, Anda mungkin melihat tindakan lama di beberapa tempat dan tindakan baru di tempat lain.
- Setelah Anda menambahkan alamat IP ke set IP yang digunakan dalam aturan pemblokiran, alamat baru mungkin diblokir di satu area sementara masih diizinkan di area lain.

Mendapatkan pemberitahuan tentang versi baru dan pembaruan ke grup aturan terkelola

Penyedia grup aturan terkelola menggunakan pemberitahuan SNS untuk mengumumkan perubahan grup aturan, seperti versi baru yang akan datang dan pembaruan keamanan yang mendesak.

Cara berlangganan notifikasi SNS

Untuk berlangganan pemberitahuan untuk grup aturan, Anda membuat langganan Amazon SNS untuk topik Amazon SNS grup aturan ARN di Wilayah AS Timur (Virginia Utara) us-east-1.

Untuk informasi tentang cara berlangganan, lihat Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

> **Note**
>
> Buat langganan Anda untuk topik SNS hanya di Wilayah us-east-1.

Aturan Aturan AWS Terkelola berversi mengelompokkan semuanya menggunakan topik SNS yang sama Nama Sumber Daya Amazon (ARN). Untuk informasi selengkapnya tentang pemberitahuan grup aturan Aturan AWS Terkelola, lihatPemberitahuan penyebaran.

Di mana menemukan ARN topik Amazon SNS untuk grup aturan terkelola

AWS Grup aturan Aturan Terkelola menggunakan satu topik SNS ARN, sehingga Anda dapat mengambil topik ARN dari salah satu grup aturan dan berlangganan untuk mendapatkan pemberitahuan untuk semua grup aturan Aturan Terkelola yang menyediakan AWS pemberitahuan SNS.

- Konsol
  - (Opsi) Saat Anda menambahkan grup aturan terkelola ke ACL web Anda, pilih Edit untuk melihat informasi grup aturan, yang mencakup topik Amazon SNS grup aturan ARN.
  - (Opsi) Setelah menambahkan grup aturan terkelola ke ACL web Anda, pilih Edit di ACL web, lalu pilih dan edit aturan grup aturan untuk melihat ARN topik Amazon SNS grup aturan.

- API — `DescribeManagedRuleGroup`
- CLI — `aws wafv2 describe-managed-rule-group --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

Untuk informasi umum tentang format notifikasi Amazon SNS dan cara memfilter notifikasi yang Anda terima, lihat Mengurai format pesan dan kebijakan filter langganan Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

Melacak kedaluwarsa versi grup aturan

Jika Anda menggunakan versi tertentu dari grup aturan, pastikan Anda tidak tetap menggunakan versi yang melewati tanggal kedaluwarsanya.

> **Tip**
>
> Mendaftar untuk pemberitahuan Amazon SNS untuk grup aturan terkelola, dan tetap mengikuti versi grup aturan terkelola. Anda akan mendapat manfaat dari sebagian besar up-to-date perlindungan dari kelompok aturan dan tetap berada di depan kedaluwarsa. Untuk informasi, lihat Mendapatkan pemberitahuan tentang versi dan pembaruan baru.

Untuk memantau penjadwalan kedaluwarsa untuk grup aturan terkelola melalui Amazon CloudWatch

1. Di CloudWatch, cari metrik kedaluwarsa dari AWS WAF grup aturan terkelola Anda. Metrik memiliki nama dan dimensi metrik berikut:
   - Nama metrik: DaysToExpiry
   - Dimensi metrik: RegionManagedRuleGroup,,Vendor, dan Version

   Jika Anda memiliki grup aturan terkelola di ACL web Anda yang mengevaluasi lalu lintas, Anda akan mendapatkan metrik untuk itu. Metrik tidak tersedia untuk grup aturan yang tidak Anda gunakan.
2. Setel alarm pada metrik yang Anda minati, sehingga Anda diberi tahu tepat waktu untuk beralih ke versi grup aturan yang lebih baru.

Untuk informasi tentang menggunakan CloudWatch metrik Amazon dan mengonfigurasi alarm, lihat Panduan Pengguna Amazon CloudWatch .

Contoh konfigurasi grup aturan terkelola di JSON dan YAMAL

Panggilan API dan CLI menampilkan daftar semua aturan dalam grup aturan terkelola yang dapat Anda referensikan dalam model JSON atau melalui. AWS CloudFormation

JSON

Anda dapat mereferensikan dan memodifikasi grup aturan terkelola dalam pernyataan aturan menggunakan JSON. Daftar berikut menunjukkan kelompok aturan Aturan AWS Terkelola,`AWSManagedRulesCommonRuleSet`, dalam format JSON. RuleActionOverridesSpesifikasi mencantumkan aturan yang tindakannya telah diganti. Count

```
{
    "Name": "AWS-AWSManagedRulesCommonRuleSet",
    "Priority": 0,
    "Statement": {
      "ManagedRuleGroupStatement": {
        "VendorName": "AWS",
        "Name": "AWSManagedRulesCommonRuleSet",
        "RuleActionOverrides": [

          {

            "ActionToUse": {

              "Count": {}

            },

            "Name": "NoUserAgent_HEADER"

          }

        ],
        "ExcludedRules": []
      }
    },
    "OverrideAction": {
      "None": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
```

```
      "MetricName": "AWS-AWSManagedRulesCommonRuleSet"
    }
}
```

YAML

Anda dapat mereferensikan dan memodifikasi grup aturan terkelola dalam pernyataan aturan menggunakan template AWS CloudFormation YAMAL. Daftar berikut menunjukkan grup aturan Aturan AWS Terkelola,`AWSManagedRulesCommonRuleSet`, dalam AWS CloudFormation templat. RuleActionOverridesSpesifikasi mencantumkan aturan yang tindakannya telah diganti. Count

```
Name: AWS-AWSManagedRulesCommonRuleSet
Priority: 0
Statement:
  ManagedRuleGroupStatement:
    VendorName: AWS
    Name: AWSManagedRulesCommonRuleSet
    RuleActionOverrides:
    - ActionToUse:
        Count: {}
      Name: NoUserAgent_HEADER
    ExcludedRules: []
OverrideAction:
  None: {}
VisibilityConfig:
  SampledRequestsEnabled: true
  CloudWatchMetricsEnabled: true
  MetricName: AWS-AWSManagedRulesCommonRuleSet
```

AWS Aturan Terkelola untuk AWS WAF

AWS Aturan Terkelola untuk AWS WAF adalah layanan terkelola yang memberikan perlindungan terhadap kerentanan aplikasi umum atau lalu lintas yang tidak diinginkan lainnya. Anda memiliki opsi untuk memilih satu atau beberapa grup aturan dari Aturan AWS Terkelola untuk setiap ACL web, hingga batas maksimum unit kapasitas ACL web (WCU).

Mengurangi positif palsu dan menguji perubahan grup aturan

Sebelum menggunakan kelompok aturan terkelola apa pun dalam produksi, ujilah di lingkungan non-produksi sesuai dengan panduan di[Menguji dan menyetel perlindungan Anda AWS WAF](). Ikuti panduan pengujian dan penyetelan saat Anda menambahkan grup aturan ke ACL web Anda, untuk

menguji versi baru grup aturan, dan kapan pun grup aturan tidak menangani lalu lintas web Anda sesuai kebutuhan.

Tanggung jawab keamanan bersama

AWS Aturan Terkelola dirancang untuk melindungi Anda dari ancaman web umum. Bila digunakan sesuai dengan dokumentasi, grup aturan Aturan AWS Terkelola menambahkan lapisan keamanan lain untuk aplikasi Anda. Namun, grup aturan Aturan AWS Terkelola tidak dimaksudkan sebagai pengganti tanggung jawab keamanan Anda, yang ditentukan oleh AWS sumber daya yang Anda pilih. Lihat Model Tanggung Jawab Bersama untuk memastikan bahwa sumber daya Anda AWS dilindungi dengan benar.

AWS Daftar grup aturan Aturan Terkelola

Informasi yang kami publikasikan untuk aturan dalam kelompok aturan Aturan AWS Terkelola dimaksudkan untuk memberi Anda informasi yang cukup untuk menggunakan aturan sementara tidak memberikan informasi yang dapat digunakan oleh pelaku jahat untuk menghindari aturan. Jika Anda memerlukan informasi lebih lanjut daripada yang Anda temukan dalam dokumentasi ini, hubungi AWS Support Pusat.

Bagian ini menjelaskan versi terbaru dari grup aturan Aturan AWS Terkelola. Anda melihat ini di konsol saat menambahkan grup aturan terkelola ke ACL web Anda. Melalui API, Anda dapat mengambil daftar ini bersama dengan grup aturan AWS Marketplace terkelola yang Anda berlangganan dengan menelepon. `ListAvailableManagedRuleGroups`

> **Note**
>
> Untuk informasi tentang mengambil versi grup aturan Aturan AWS Terkelola, lihatMengambil versi yang tersedia untuk grup aturan terkelola.

Semua grup aturan Aturan AWS Terkelola mendukung pelabelan, dan daftar aturan di bagian ini menyertakan spesifikasi label. Anda dapat mengambil label untuk grup aturan terkelola melalui API dengan memanggil`DescribeManagedRuleGroup`. Label tercantum di AvailableLabels properti dalam tanggapan. Untuk informasi tentang pelabelan, lihatAWS WAF label pada permintaan web.

Uji dan sesuaikan perubahan apa pun pada AWS WAF perlindungan Anda sebelum Anda menggunakannya untuk lalu lintas produksi. Untuk informasi, lihat Menguji dan menyetel perlindungan Anda AWS WAF.

AWS Kelompok aturan Aturan Terkelola

- Kelompok aturan dasar
  - Grup aturan terkelola set aturan inti (CRS)
  - Kelompok aturan terkelola perlindungan admin
  - Kelompok aturan terkelola masukan buruk yang diketahui
- Kelompok aturan khusus kasus penggunaan
  - Grup aturan terkelola database SQL
  - Grup aturan terkelola sistem operasi Linux
  - Grup aturan terkelola sistem operasi POSIX
  - Grup aturan terkelola sistem operasi Windows
  - Grup aturan terkelola aplikasi PHP
  - WordPress kelompok aturan terkelola aplikasi
- Grup aturan reputasi IP
  - Grup aturan terkelola daftar reputasi IP Amazon
  - Grup aturan terkelola daftar IP anonim
- AWS WAF Grup aturan pencegahan penipuan (ACFP) pembuatan akun Kontrol Penipuan
  - Pertimbangan untuk menggunakan grup aturan ini
  - Label ditambahkan oleh grup aturan ini
    - Label token
    - Label ACFP
  - Daftar aturan pencegahan penipuan pembuatan akun
- AWS WAF Kelompok aturan pencegahan pengambilalihan akun Kontrol Penipuan (ATP)
  - Pertimbangan untuk menggunakan grup aturan ini
  - Label ditambahkan oleh grup aturan ini
    - Label token
    - Label ATP
  - Daftar aturan pencegahan pengambilalihan akun
- AWS WAF Grup aturan Bot Control
  - Tingkat perlindungan
  - Pertimbangan untuk menggunakan grup aturan ini

- Label ditambahkan oleh grup aturan ini
  - Label token
  - Label Kontrol Bot
- Daftar aturan Bot Control

Kelompok aturan dasar

Kelompok aturan yang dikelola dasar memberikan perlindungan umum terhadap berbagai ancaman umum. Pilih satu atau beberapa kelompok aturan ini untuk menetapkan perlindungan dasar untuk sumber daya Anda.

> **Note**
>
> Informasi yang kami publikasikan untuk aturan dalam kelompok aturan Aturan AWS Terkelola dimaksudkan untuk memberi Anda informasi yang cukup untuk menggunakan aturan sementara tidak memberikan informasi yang dapat digunakan oleh pelaku jahat untuk menghindari aturan. Jika Anda memerlukan informasi lebih lanjut daripada yang Anda temukan dalam dokumentasi ini, hubungi AWS Support Pusat.

Grup aturan terkelola set aturan inti (CRS)

VendorName:`AWS`, Nama:`AWSManagedRulesCommonRuleSet`, WCU: 700

Kelompok aturan set inti (CRS) berisi aturan yang umumnya berlaku untuk aplikasi web. Ini memberikan perlindungan terhadap eksploitasi berbagai kerentanan, termasuk beberapa risiko tinggi dan kerentanan yang umum terjadi yang dijelaskan dalam publikasi OWASP seperti OWASP Top 10. Pertimbangkan untuk menggunakan grup aturan ini untuk kasus AWS WAF penggunaan apa pun.

Grup aturan terkelola ini menambahkan label ke permintaan web yang dievaluasi, yang tersedia untuk aturan yang berjalan setelah grup aturan ini di ACL web Anda. AWS WAF juga mencatat label ke CloudWatch metrik Amazon. Untuk informasi umum tentang label dan metrik label, lihat Label pada permintaan web danLabel metrik dan dimensi.

> **Note**
>
> Tabel ini menjelaskan versi statis terbaru dari grup aturan ini. Untuk versi lain, gunakan perintah API DescribeManagedRuleGroup.

Nama aturan	Deskripsi dan label
`NoUserAgent_HEADER`	Memeriksa permintaan yang tidak memiliki `User-Agent` header HTTP. Tindakan aturan: Block label: `awswaf:managed:aws:core-rule-set:NoUserAgent_Header`
`UserAgent_BadBots_HEADER`	Memeriksa nilai `User-Agent` header umum yang menunjukkan bahwa permintaan tersebut adalah bot yang buruk. Contoh pola meliputi`nessus`, dan`nmap`. Untuk manajemen bot, lihat juga[AWS WAF Grup aturan Bot Control](#). Tindakan aturan: Block label: `awswaf:managed:aws:core-rule-set:BadBots_Header`
`SizeRestrictions_QUERYSTRING`	Memeriksa string kueri URI yang lebih dari 2.048 byte. Tindakan aturan: Block label: `awswaf:managed:aws:core-rule-set:SizeRestrictions_QueryString`
`SizeRestrictions_Cookie_HEADER`	Memeriksa header cookie yang lebih dari 10.240 byte. Tindakan aturan: Block

Nama aturan	Deskripsi dan label
	label: `awswaf:managed:aws:core-rule-set:SizeRestrictions_Cookie_Header`
`SizeRestrictions_BODY`	Memeriksa badan permintaan yang lebih dari 8 KB (8.192 byte). Tindakan aturan: Block label: `awswaf:managed:aws:core-rule-set:SizeRestrictions_Body`
`SizeRestrictions_URIPATH`	Memeriksa jalur URI yang lebih dari 1.024 byte. Tindakan aturan: Block label: `awswaf:managed:aws:core-rule-set:SizeRestrictions_URIPath`

Nama aturan	Deskripsi dan label
`EC2MetaDataSSRF_BODY`	Memeriksa upaya untuk mengeksfiltrasi metadata Amazon EC2 dari badan permintaan. **Warning** Aturan ini hanya memeriksa badan permintaan hingga batas ukuran tubuh untuk ACL web dan jenis sumber daya. Untuk Application Load Balancer dan AWS AppSync, limit ditetapkan pada 8 KB. Untuk CloudFront API Gateway, Amazon Cognito, App Runner, dan Akses Terverifikasi, batas default adalah 16 KB dan Anda dapat meningkatkan batas hingga 64 KB dalam konfigurasi ACL web Anda. Aturan ini menggunakan `Continue` opsi untuk penanganan konten yang terlalu besar. Untuk informasi selengkapnya, lihat Penanganan komponen permintaan kebesaran di AWS WAF. Tindakan aturan: Block label: `awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_Body`

Nama aturan	Deskripsi dan label
`EC2MetaDataSSRF_COOKIE`	Memeriksa upaya untuk mengekstrasi metadata Amazon EC2 dari cookie permintaan. Tindakan aturan: Block label: `awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_Cookie`
`EC2MetaDataSSRF_URIPATH`	Memeriksa upaya untuk mengeksfiltrasi metadata Amazon EC2 dari jalur URI permintaan. Tindakan aturan: Block label: `awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_URIPath`
`EC2MetaDataSSRF_QUERYARGUMENTS`	Memeriksa upaya untuk mengekstrasi metadata Amazon EC2 dari argumen kueri permintaan. Tindakan aturan: Block label: `awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_QueryArguments`

Nama aturan	Deskripsi dan label
`GenericLFI_QUERYARGUMENTS`	Memeriksa keberadaan eksploitasi Local File Inclusion (LFI) dalam argumen kueri. Contohnya termasuk upaya traversal jalur menggunakan teknik seperti `../../`. Tindakan aturan: Block label: `awswaf:managed:aws:core-rule-set:GenericLFI_QueryArguments`
`GenericLFI_URIPATH`	Memeriksa keberadaan eksploitasi Local File Inclusion (LFI) di jalur URI. Contohnya termasuk upaya traversal jalur menggunakan teknik seperti `../../`. Tindakan aturan: Block label: `awswaf:managed:aws:core-rule-set:GenericLFI_URIPath`

Nama aturan	Deskripsi dan label
`GenericLFI_BODY`	Memeriksa keberadaan eksploitasi Local File Inclusion (LFI) di badan permintaan. Contohnya termasuk upaya traversal jalur menggunakan teknik seperti `../../`. **Warning** Aturan ini hanya memeriksa badan permintaan hingga batas ukuran tubuh untuk ACL web dan jenis sumber daya. Untuk Application Load Balancer dan AWS AppSync, limit ditetapkan pada 8 KB. Untuk CloudFront API Gateway, Amazon Cognito, App Runner, dan Akses Terverifikasi, batas default adalah 16 KB dan Anda dapat meningkatkan batas hingga 64 KB dalam konfigurasi ACL web Anda. Aturan ini menggunakan `Continue` opsi untuk penanganan konten yang terlalu besar. Untuk informasi selengkapnya, lihat Penanganan komponen permintaan kebesaran di AWS WAF. Tindakan aturan: Block label: `awswaf:managed:aws:core-rule-set:GenericLFI_Body`

Nama aturan	Deskripsi dan label
`RestrictedExtensions_URIPATH`	Memeriksa permintaan yang jalur URI berisi ekstensi file sistem yang tidak aman untuk dibaca atau dijalankan. Contoh pola termasuk ekstensi seperti `.log` dan`.ini`. Tindakan aturan: Block label: `awswaf:managed:aws:core-rule-set:RestrictedExtensions_URIPath`
`RestrictedExtensions_QUERYARGUMENTS`	Memeriksa permintaan yang argumen kuerinya berisi ekstensi file sistem yang tidak aman untuk dibaca atau dijalankan. Contoh pola termasuk ekstensi seperti `.log` dan`.ini`. Tindakan aturan: Block label: `awswaf:managed:aws:core-rule-set:RestrictedExtensions_QueryArguments`
`GenericRFI_QUERYARGUMENTS`	Memeriksa nilai semua parameter kueri untuk upaya mengeksploitasi RFI (Remote File Inclusion) dalam aplikasi web dengan menyematkan URL yang berisi alamat IPv4. Contohnya termasuk pola sepertihttp://,https://,ftp://,ftps://, danfile://, dengan header host IPv4 dalam upaya eksploitasi. Tindakan aturan: Block label: `awswaf:managed:aws:core-rule-set:GenericRFI_QueryArguments`

Nama aturan	Deskripsi dan label
`GenericRFI_BODY`	Memeriksa badan permintaan untuk upaya mengeksploitasi RFI (Remote File Inclusion) dalam aplikasi web dengan menyematkan URL yang berisi alamat IPv4. Contohnya termasuk pola seperti`http://`,`https://`,`ftp://`,`ftps://`, dan`file://`, dengan header host IPv4 dalam upaya eksploitasi. **Warning** Aturan ini hanya memeriksa badan permintaan hingga batas ukuran tubuh untuk ACL web dan jenis sumber daya. Untuk Application Load Balancer dan AWS AppSync, limit ditetapka n pada 8 KB. Untuk CloudFront API Gateway, Amazon Cognito, App Runner, dan Akses Terverifikasi, batas default adalah 16 KB dan Anda dapat meningkatkan batas hingga 64 KB dalam konfigurasi ACL web Anda. Aturan ini menggunakan `Continue` opsi untuk penanganan konten yang terlalu besar. Untuk informasi selengkapnya, lihat Penanganan komponen permintaan kebesaran di AWS WAF. Tindakan aturan: Block label: `awswaf:managed:aws:core-rul e-set:GenericRFI_Body`

Nama aturan	Deskripsi dan label
`GenericRFI_URIPATH`	Memeriksa jalur URI untuk upaya mengekspl oitasi RFI (Remote File Inclusion) dalam aplikasi web dengan menyematkan URL yang berisi alamat IPv4. Contohnya termasuk pola sepertihttp://,https://,ftp://,ftps://, danfile://, dengan header host IPv4 dalam upaya eksploitasi. Tindakan aturan: Block label: awswaf:managed:aws:core-rul e-set:GenericRFI_URIPath
`CrossSiteScripting_COOKIE`	Memeriksa nilai-nilai header cookie untuk pola cross-site scripting (XSS) umum menggunak an built-in. AWS WAF Pernyataan aturan serangan skrip lintas situs Contoh pola termasuk skrip seperti<script>alert("hel lo")</script> . **Note** Rincian pencocokan aturan di AWS WAF log tidak diisi untuk versi 2.0 dari grup aturan ini. Tindakan aturan: Block label: awswaf:managed:aws:core-rul e-set:CrossSiteScripting_Cookie

Nama aturan	Deskripsi dan label
`CrossSiteScripting_QUERYARGUMENTS`	Memeriksa nilai-nilai argumen kueri untuk pola cross-site scripting (XSS) umum menggunakan built-in. AWS WAF Pernyataan aturan serangan skrip lintas situs Contoh pola termasuk skrip seperti`<script>alert("hello")</script>` . **Note** Rincian pencocokan aturan di AWS WAF log tidak diisi untuk versi 2.0 dari grup aturan ini. Tindakan aturan: Block label: `awswaf:managed:aws:core-rule-set:CrossSiteScripting_QueryArguments`

Nama aturan	Deskripsi dan label
`CrossSiteScripting_BODY`	Memeriksa badan permintaan untuk pola cross-site scripting (XSS) umum menggunakan built-in. AWS WAF Pernyataan aturan serangan skrip lintas situs Contoh pola termasuk skrip seperti`<script>alert("hello")</script>` . **Note** Rincian pencocokan aturan di AWS WAF log tidak diisi untuk versi 2.0 dari grup aturan ini. **Warning** Aturan ini hanya memeriksa badan permintaan hingga batas ukuran tubuh untuk ACL web dan jenis sumber daya. Untuk Application Load Balancer dan AWS AppSync, limit ditetapkan pada 8 KB. Untuk CloudFront API Gateway, Amazon Cognito, App Runner, dan Akses Terverifikasi, batas default adalah 16 KB dan Anda dapat meningkatkan batas hingga 64 KB dalam konfigurasi ACL web Anda. Aturan ini menggunakan `Continue` opsi untuk penanganan konten yang terlalu besar. Untuk informasi selengkapnya, lihat Penanganan komponen permintaan kebesaran di AWS WAF.

Nama aturan	Deskripsi dan label
	Tindakan aturan: Block label: `awswaf:managed:aws:core-rule-set:CrossSiteScripting_Body`
`CrossSiteScripting_URIPATH`	Memeriksa nilai jalur URI untuk pola cross-site scripting (XSS) umum menggunakan built-in. AWS WAF Pernyataan aturan serangan skrip lintas situs Contoh pola termasuk skrip seperti`<script>alert("hello")</script>` . **Note** Rincian pencocokan aturan di AWS WAF log tidak diisi untuk versi 2.0 dari grup aturan ini. Tindakan aturan: Block label: `awswaf:managed:aws:core-rule-set:CrossSiteScripting_URIPath`

Kelompok aturan terkelola perlindungan admin

VendorName:`AWS`, Nama:`AWSManagedRulesAdminProtectionRuleSet`, WCU: 100

Grup aturan perlindungan Admin berisi aturan yang memungkinkan Anda memblokir akses eksternal ke halaman administratif yang terbuka. Ini mungkin berguna jika Anda menjalankan perangkat lunak pihak ketiga atau ingin mengurangi risiko aktor jahat mendapatkan akses administratif ke aplikasi Anda.

Grup aturan terkelola ini menambahkan label ke permintaan web yang dievaluasi, yang tersedia untuk aturan yang berjalan setelah grup aturan ini di ACL web Anda. AWS WAF juga mencatat label ke CloudWatch metrik Amazon. Untuk informasi umum tentang label dan metrik label, lihat Label pada permintaan web danLabel metrik dan dimensi.

> **Note**
>
> Tabel ini menjelaskan versi statis terbaru dari grup aturan ini. Untuk versi lain, gunakan perintah API DescribeManagedRuleGroup.

Nama aturan	Deskripsi dan label
`AdminProtection_URIPATH`	Memeriksa jalur URI yang umumnya dicadangkan untuk administrasi server web atau aplikasi. Contoh pola meliputi`sqlmanager` . Tindakan aturan: Block label: `awswaf:managed:aws:admin-protection:AdminProtection_URIPath`

Kelompok aturan terkelola masukan buruk yang diketahui

VendorName:`AWS`, Nama:`AWSManagedRulesKnownBadInputsRuleSet`, WCU: 200

Kelompok aturan input buruk yang diketahui berisi aturan untuk memblokir pola permintaan yang diketahui tidak valid dan terkait dengan eksploitasi atau penemuan kerentanan. Ini dapat membantu mengurangi risiko aktor jahat menemukan aplikasi yang rentan.

Grup aturan terkelola ini menambahkan label ke permintaan web yang dievaluasi, yang tersedia untuk aturan yang berjalan setelah grup aturan ini di ACL web Anda. AWS WAF juga mencatat label ke CloudWatch metrik Amazon. Untuk informasi umum tentang label dan metrik label, lihat Label pada permintaan web danLabel metrik dan dimensi.

> **Note**
>
> Tabel ini menjelaskan versi statis terbaru dari grup aturan ini. Untuk versi lain, gunakan perintah API DescribeManagedRuleGroup.

Nama aturan	Deskripsi dan label
`JavaDeserializationRCE_HEADER`	Memeriksa kunci dan nilai header permintaan HTTP untuk pola yang menunjukkan upaya deserialisasi Java Remote Command Execution (RCE), seperti kerentanan Spring Core dan Cloud Function RCE (CVE-2022-22963, CVE-2022-22965). Contoh pola meliputi `(java.lang.Runtime).getRuntime().exec("whoami")` . **Warning** Aturan ini hanya memeriksa 8 KB pertama dari header permintaan atau 200 header pertama, batas mana pun yang tercapai terlebih dahulu, dan menggunakan opsi untuk penanganan konten yang terlalu besar. `Continue` Untuk informasi selengkapnya, lihat Penanganan komponen permintaan kebesaran di AWS WAF. Tindakan aturan: Block label: `awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_Header`

Nama aturan	Deskripsi dan label
`JavaDeserializationRCE_BODY`	Memeriksa badan permintaan untuk pola yang menunjukkan upaya deserialisasi Java Remote Command Execution (RCE), seperti kerentanan Spring Core dan Cloud Function RCE (CVE-2022-22963, CVE-2022-22965). Contoh pola meliputi`(java.lang.Runtime ).getRuntime().exec("whoami")` . **Warning** Aturan ini hanya memeriksa badan permintaan hingga batas ukuran tubuh untuk ACL web dan jenis sumber daya. Untuk Application Load Balancer dan AWS AppSync, limit ditetapkan pada 8 KB. Untuk CloudFront API Gateway, Amazon Cognito, App Runner, dan Akses Terverifikasi, batas default adalah 16 KB dan Anda dapat meningkatkan batas hingga 64 KB dalam konfigurasi ACL web Anda. Aturan ini menggunakan `Continue` opsi untuk penanganan konten yang terlalu besar. Untuk informasi selengkapnya, lihat Penanganan komponen permintaan kebesaran di AWS WAF. Tindakan aturan: Block label: `awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_Body`

Nama aturan	Deskripsi dan label
`JavaDeserializationRCE_URIPATH`	Memeriksa URI permintaan untuk pola yang menunjukkan upaya deserialisasi Java Remote Command Execution (RCE), seperti kerentanan Spring Core dan Cloud Function RCE (CVE-2022-22963, CVE-2022-22965). Contoh pola meliputi`(java.lang.Runtime).getRuntime().exec("whoami")` . Tindakan aturan: Block label: `awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_URIPath`
`JavaDeserializationRCE_QUERYSTRING`	Memeriksa string kueri permintaan untuk pola yang menunjukkan upaya deserialisasi Java Remote Command Execution (RCE), seperti kerentanan Spring Core dan Cloud Function RCE (CVE-2022-22963, CVE-2022-22965). Contoh pola meliputi`(java.lang.Runtime).getRuntime().exec("whoami")` . Tindakan aturan: Block label: `awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_QueryString`

Nama aturan	Deskripsi dan label
`Host_localhost_HEADER`	Memeriksa header host dalam permintaan untuk pola yang menunjukkan localhost. Contoh pola meliputi`localhost` . Tindakan aturan: Block label: `awswaf:managed:aws:known-bad-inputs:Host_Localhost_Header`
`PROPFIND_METHOD`	Memeriksa metode HTTP dalam permintaan`PROPFIND`, yang merupakan metode yang mirip dengan`HEAD`, tetapi dengan niat ekstra untuk mengeksfiltrasi objek XHTML. Tindakan aturan: Block label: `awswaf:managed:aws:known-bad-inputs:Propfind_Method`
`ExploitablePaths_URIPATH`	Memeriksa jalur URI untuk upaya mengakses jalur aplikasi web yang dapat dieksploitasi. Contoh pola termasuk jalur seperti`web-inf`. Tindakan aturan: Block label: `awswaf:managed:aws:known-bad-inputs:ExploitablePaths_URIPath`

Nama aturan	Deskripsi dan label
`Log4JRCE_HEADER`	Memeriksa kunci dan nilai header permintaan untuk keberadaan kerentanan Log4j (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) dan melindungi terhadap upaya Eksekusi Kode Jarak Jauh (RCE). Contoh pola meliputi `${jndi:ldap://example.com/}` . **Warning** Aturan ini hanya memeriksa 8 KB pertama dari header permintaan atau 200 header pertama, batas mana pun yang tercapai terlebih dahulu, dan menggunakan opsi untuk penanganan konten yang terlalu besar. `Continue` Untuk informasi selengkapnya, lihat Penanganan komponen permintaan kebesaran di AWS WAF. Tindakan aturan: Block label: `awswaf:managed:aws:known-bad-inputs:Log4JRCE_Header`

Nama aturan	Deskripsi dan label
`Log4JRCE_QUERYSTRING`	Memeriksa string kueri untuk keberadaan kerentanan Log4j (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) dan melindungi terhadap upaya Eksekusi Kode Jarak Jauh (RCE). Contoh pola meliputi`${jndi:ldap://example.com/}` . Tindakan aturan: Block label: `awswaf:managed:aws:known-bad-inputs:Log4JRCE_QueryString`

Nama aturan	Deskripsi dan label
`Log4JRCE_BODY`	Memeriksa tubuh untuk keberadaan kerentanan Log4j (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) dan melindungi terhadap upaya Eksekusi Kode Jarak Jauh (RCE). Contoh pola meliputi`${jndi:ldap://example.com/}` . **Warning** Aturan ini hanya memeriksa badan permintaan hingga batas ukuran tubuh untuk ACL web dan jenis sumber daya. Untuk Application Load Balancer dan AWS AppSync, limit ditetapkan pada 8 KB. Untuk CloudFront API Gateway, Amazon Cognito, App Runner, dan Akses Terverifikasi, batas default adalah 16 KB dan Anda dapat meningkatkan batas hingga 64 KB dalam konfigurasi ACL web Anda. Aturan ini menggunakan `Continue` opsi untuk penanganan konten yang terlalu besar. Untuk informasi selengkapnya, lihat Penanganan komponen permintaan kebesaran di AWS WAF. Tindakan aturan: Block label: `awswaf:managed:aws:known-bad-inputs:Log4JRCE_Body`

Nama aturan	Deskripsi dan label
`Log4JRCE_URIPATH`	Memeriksa jalur URI untuk keberadaan kerentanan Log4j (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) dan melindungi terhadap upaya Eksekusi Kode Jarak Jauh (RCE). Contoh pola meliputi`${jndi:ldap://example.com/}` . Tindakan aturan: Block label: `awswaf:managed:aws:known-bad-inputs:Log4JRCE_URIPath`

Kelompok aturan khusus kasus penggunaan

Kelompok aturan khusus kasus penggunaan memberikan perlindungan tambahan untuk banyak kasus penggunaan yang beragam AWS WAF . Pilih grup aturan yang berlaku untuk aplikasi Anda.

> **Note**
>
> Informasi yang kami publikasikan untuk aturan dalam kelompok aturan Aturan AWS Terkelola dimaksudkan untuk memberi Anda informasi yang cukup untuk menggunakan aturan sementara tidak memberikan informasi yang dapat digunakan oleh pelaku jahat untuk menghindari aturan. Jika Anda memerlukan informasi lebih lanjut daripada yang Anda temukan dalam dokumentasi ini, hubungi AWS Support Pusat.

Grup aturan terkelola database SQL

VendorName:`AWS`, Nama:`AWSManagedRulesSQLiRuleSet`, WCU: 200

Grup aturan database SQL berisi aturan untuk memblokir pola permintaan yang terkait dengan eksploitasi database SQL, seperti serangan injeksi SQL. Ini dapat membantu mencegah injeksi jarak jauh dari kueri yang tidak sah. Evaluasi grup aturan ini untuk digunakan jika aplikasi Anda berinteraksi dengan database SQL.

Grup aturan terkelola ini menambahkan label ke permintaan web yang dievaluasi, yang tersedia untuk aturan yang berjalan setelah grup aturan ini di ACL web Anda. AWS WAF juga mencatat label ke CloudWatch metrik Amazon. Untuk informasi umum tentang label dan metrik label, lihat Label pada permintaan web danLabel metrik dan dimensi.

> **Note**
>
> Tabel ini menjelaskan versi statis terbaru dari grup aturan ini. Untuk versi lain, gunakan perintah API DescribeManagedRuleGroup.

Nama aturan	Deskripsi dan label
`SQLi_QUERYARGUMENTS`	Menggunakan built-in AWS WAF Pernyataan aturan serangan injeksi SQL, dengan tingkat sensitivitas diatur keLow, untuk memeriksa nilai semua parameter kueri untuk pola yang cocok dengan kode SQL berbahaya. Tindakan aturan: Block label: `awswaf:managed:aws:sql-database:SQLi_QueryArguments`
`SQLiExtendedPatterns_QUERYARGUMENTS`	Memeriksa nilai semua parameter kueri untuk pola yang cocok dengan kode SQL berbahaya . Pola yang diperiksa aturan ini tidak tercakup oleh aturan`SQLi_QUERYARGUMENTS` . Tindakan aturan: Block label: `awswaf:managed:aws:sql-database:SQLiExtendedPatterns_QueryArguments`
`SQLi_BODY`	Menggunakan built-in AWS WAF Pernyataan aturan serangan injeksi SQL, dengan tingkat

Nama aturan	Deskripsi dan label
	sensitivitas disetel keLow, untuk memeriksa badan permintaan untuk pola yang cocok dengan kode SQL berbahaya. **Warning** Aturan ini hanya memeriksa badan permintaan hingga batas ukuran tubuh untuk ACL web dan jenis sumber daya. Untuk Application Load Balancer dan AWS AppSync, limit ditetapka n pada 8 KB. Untuk CloudFront API Gateway, Amazon Cognito, App Runner, dan Akses Terverifikasi, batas default adalah 16 KB dan Anda dapat meningkatkan batas hingga 64 KB dalam konfigurasi ACL web Anda. Aturan ini menggunakan `Continue` opsi untuk penanganan konten yang terlalu besar. Untuk informasi selengkapnya, lihat Penanganan komponen permintaan kebesaran di AWS WAF. Tindakan aturan: Block label: `awswaf:managed:aws:sql-data base:SQLi_Body`

Nama aturan	Deskripsi dan label
`SQLiExtendedPatterns_BODY`	Memeriksa badan permintaan untuk pola yang cocok dengan kode SQL berbahaya. Pola yang diperiksa aturan ini tidak tercakup oleh aturan`SQLi_BODY` . **Warning** Aturan ini hanya memeriksa badan permintaan hingga batas ukuran tubuh untuk ACL web dan jenis sumber daya. Untuk Application Load Balancer dan AWS AppSync, limit ditetapka n pada 8 KB. Untuk CloudFront API Gateway, Amazon Cognito, App Runner, dan Akses Terverifikasi, batas default adalah 16 KB dan Anda dapat meningkatkan batas hingga 64 KB dalam konfigurasi ACL web Anda. Aturan ini menggunakan `Continue` opsi untuk penanganan konten yang terlalu besar. Untuk informasi selengkapnya, lihat Penanganan komponen permintaan kebesaran di AWS WAF. Tindakan aturan: Block label: `awswaf:managed:aws:sql-data base:SQLiExtendedPatterns_Body`

Nama aturan	Deskripsi dan label
`SQLi_COOKIE`	Menggunakan built-in AWS WAF Pernyataan aturan serangan injeksi SQL, dengan tingkat sensitivitas diatur keLow, untuk memeriksa header cookie permintaan untuk pola yang cocok dengan kode SQL berbahaya. Tindakan aturan: Block label: `awswaf:managed:aws:sql-database:SQLi_Cookie`

Grup aturan terkelola sistem operasi Linux

VendorName:`AWS`, Nama:`AWSManagedRulesLinuxRuleSet`, WCU: 200

Grup aturan sistem operasi Linux berisi aturan yang memblokir pola permintaan yang terkait dengan eksploitasi kerentanan khusus untuk Linux, termasuk serangan Local File Inclusion (LFI) khusus Linux. Ini dapat membantu mencegah serangan yang mengekspos konten file atau menjalankan kode yang seharusnya tidak dapat diakses oleh penyerang. Anda harus mengevaluasi grup aturan ini jika ada bagian dari aplikasi Anda yang berjalan di Linux. Anda harus menggunakan grup aturan ini bersama dengan grup Sistem operasi POSIX aturan.

Grup aturan terkelola ini menambahkan label ke permintaan web yang dievaluasi, yang tersedia untuk aturan yang berjalan setelah grup aturan ini di ACL web Anda. AWS WAF juga mencatat label ke CloudWatch metrik Amazon. Untuk informasi umum tentang label dan metrik label, lihat Label pada permintaan web danLabel metrik dan dimensi.

> **Note**
>
> Tabel ini menjelaskan versi statis terbaru dari grup aturan ini. Untuk versi lain, gunakan perintah API DescribeManagedRuleGroup.

Nama aturan	Deskripsi dan label
`LFI_URIPATH`	Memeriksa jalur permintaan untuk upaya mengeksploitasi kerentanan Local File Inclusion (LFI) dalam aplikasi web. Contoh pola termasuk file seperti `/proc/version` , yang dapat memberikan informasi sistem operasi kepada penyerang. Tindakan aturan: Block label: `awswaf:managed:aws:linux-os:LFI_URIPath`
`LFI_QUERYSTRING`	Memeriksa nilai querystring untuk upaya mengeksploitasi kerentanan Local File Inclusion (LFI) dalam aplikasi web. Contoh pola termasuk file seperti `/proc/version` , yang dapat memberikan informasi sistem operasi kepada penyerang. Tindakan aturan: Block label: `awswaf:managed:aws:linux-os:LFI_QueryString`
`LFI_HEADER`	Memeriksa header permintaan untuk upaya mengeksploitasi kerentanan Local File Inclusion (LFI) dalam aplikasi web. Contoh pola termasuk file seperti `/proc/version` , yang dapat memberikan informasi sistem operasi kepada penyerang.

Nama aturan	Deskripsi dan label
	Warning Aturan ini hanya memeriksa 8 KB pertama dari header permintaan atau 200 header pertama, batas mana pun yang tercapai terlebih dahulu, dan menggunakan opsi untuk penanganan konten yang terlalu besar. `Continue` Untuk informasi selengkapnya, lihat Penanganan komponen permintaan kebesaran di AWS WAF. Tindakan aturan: Block label: `awswaf:managed:aws:linux-os:LFI_Header`

Grup aturan terkelola sistem operasi POSIX

VendorName:`AWS`, Nama:`AWSManagedRulesUnixRuleSet`, WCU: 100

Grup aturan sistem operasi POSIX berisi aturan yang memblokir pola permintaan yang terkait dengan eksploitasi kerentanan khusus untuk POSIX dan sistem operasi seperti POSIX, termasuk serangan Local File Inclusion (LFI). Ini dapat membantu mencegah serangan yang mengekspos konten file atau menjalankan kode yang seharusnya tidak dapat diakses oleh penyerang. Anda harus mengevaluasi grup aturan ini jika ada bagian dari aplikasi Anda yang berjalan pada POSIX atau sistem operasi seperti POSIX, termasuk Linux, AIX, HP-UX, macOS, Solaris, FreeBSD, dan OpenBSD.

Grup aturan terkelola ini menambahkan label ke permintaan web yang dievaluasi, yang tersedia untuk aturan yang berjalan setelah grup aturan ini di ACL web Anda. AWS WAF juga mencatat label ke CloudWatch metrik Amazon. Untuk informasi umum tentang label dan metrik label, lihat Label pada permintaan web danLabel metrik dan dimensi.

> **Note**
>
> Tabel ini menjelaskan versi statis terbaru dari grup aturan ini. Untuk versi lain, gunakan perintah API DescribeManagedRuleGroup.

Nama aturan	Deskripsi dan label
`UNIXShellCommandsVariables_QUERYSTRING`	Memeriksa nilai string kueri untuk upaya mengeksploitasi injeksi perintah, LFI, dan kerentanan traversal jalur dalam aplikasi web yang berjalan pada sistem Unix. Contohnya termasuk pola seperti `echo $HOME` dan`echo $PATH` . Tindakan aturan: Block label: `awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_QueryString`
`UNIXShellCommandsVariables_BODY`	Memeriksa badan permintaan untuk upaya mengeksploitasi injeksi perintah, LFI, dan kerentanan traversal jalur dalam aplikasi web yang berjalan pada sistem Unix. Contohnya termasuk pola seperti `echo $HOME` `danecho $PATH`. **Warning** Aturan ini hanya memeriksa badan permintaan hingga batas ukuran tubuh untuk ACL web dan jenis sumber daya. Untuk Application Load Balancer dan AWS AppSync, limit ditetapkan pada 8 KB. Untuk CloudFront API

Nama aturan	Deskripsi dan label
	Gateway, Amazon Cognito, App Runner, dan Akses Terverifikasi, batas default adalah 16 KB dan Anda dapat meningkatkan batas hingga 64 KB dalam konfigurasi ACL web Anda. Aturan ini menggunakan `Continue` opsi untuk penanganan konten yang terlalu besar. Untuk informasi selengkapnya, lihat Penanganan komponen permintaan kebesaran di AWS WAF. Tindakan aturan: Block label: `awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_Body`

Nama aturan	Deskripsi dan label
`UNIXShellCommandsVariables_HEADER`	Memeriksa semua header permintaan untuk upaya mengeksploitasi injeksi perintah, LFI, dan kerentanan traversal jalur dalam aplikasi web yang berjalan pada sistem Unix. Contohnya termasuk pola seperti `echo $HOME` dan `echo $PATH`. **Warning** Aturan ini hanya memeriksa 8 KB pertama dari header permintaan atau 200 header pertama, batas mana pun yang tercapai terlebih dahulu, dan menggunakan opsi untuk penanganan konten yang terlalu besar. `Continue` Untuk informasi selengkapnya, lihat Penanganan komponen permintaan kebesaran di AWS WAF. Tindakan aturan: Block label: `awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_Header`

Grup aturan terkelola sistem operasi Windows

VendorName:`AWS`, Nama:`AWSManagedRulesWindowsRuleSet`, WCU: 200

Grup aturan sistem operasi Windows berisi aturan yang memblokir pola permintaan yang terkait dengan eksploitasi kerentanan khusus untuk Windows, seperti eksekusi perintah jarak jauh. PowerShell Ini dapat membantu mencegah eksploitasi kerentanan yang memungkinkan penyerang

menjalankan perintah yang tidak sah atau menjalankan kode berbahaya. Evaluasi grup aturan ini jika ada bagian dari aplikasi Anda yang berjalan pada sistem operasi Windows.

Grup aturan terkelola ini menambahkan label ke permintaan web yang dievaluasi, yang tersedia untuk aturan yang berjalan setelah grup aturan ini di ACL web Anda. AWS WAF juga mencatat label ke CloudWatch metrik Amazon. Untuk informasi umum tentang label dan metrik label, lihat Label pada permintaan web danLabel metrik dan dimensi.

> **Note**
>
> Tabel ini menjelaskan versi statis terbaru dari grup aturan ini. Untuk versi lain, gunakan perintah API DescribeManagedRuleGroup.

Nama aturan	Deskripsi dan label
`WindowsShellCommands_COOKIE`	Memeriksa header cookie permintaan untuk upaya injeksi WindowsShell perintah dalam aplikasi web. Pola kecocokan mewakili WindowsShell perintah. Contoh pola meliputi `||nslookup` dan `;cmd`. Tindakan aturan: Block label: `awswaf:managed:aws:windows-os:WindowsShellCommands_Cookie`
`WindowsShellCommands_QUERYARGUMENTS`	Memeriksa nilai semua parameter kueri untuk upaya injeksi WindowsShell perintah dalam aplikasi web. Pola kecocokan mewakili WindowsShell perintah. Contoh pola meliputi `||nslookup` dan `;cmd`. Tindakan aturan: Block

Nama aturan	Deskripsi dan label
	label: `awswaf:managed:aws:windows-os:WindowsShellCommands_QueryArguments`

Nama aturan	Deskripsi dan label
`WindowsShellCommands_BODY`	Memeriksa badan permintaan untuk upaya injeksi WindowsShell perintah dalam aplikasi web. Pola pertandingan mewakili WindowsShell perintah. Contoh pola meliputi `||nslookup` dan `;cmd`. **Warning** Aturan ini hanya memeriksa badan permintaan hingga batas ukuran tubuh untuk ACL web dan jenis sumber daya. Untuk Application Load Balancer dan AWS AppSync, limit ditetapkan pada 8 KB. Untuk CloudFront API Gateway, Amazon Cognito, App Runner, dan Akses Terverifikasi, batas default adalah 16 KB dan Anda dapat meningkatkan batas hingga 64 KB dalam konfigurasi ACL web Anda. Aturan ini menggunakan `Continue` opsi untuk penanganan konten yang terlalu besar. Untuk informasi selengkapnya, lihat Penanganan komponen permintaan kebesaran di AWS WAF. Tindakan aturan: Block label: `awswaf:managed:aws:windows-os:WindowsShellCommands_Body`

Nama aturan	Deskripsi dan label
`PowerShellCommands_COOKIE`	Memeriksa header cookie permintaan untuk upaya injeksi PowerShell perintah dalam aplikasi web. Pola kecocokan mewakili PowerShell perintah. Misalnya, `Invoke-Expression` . Tindakan aturan: Block label: `awswaf:managed:aws:windows-os:PowerShellCommands_Cookie`
`PowerShellCommands_QUERYARGUMENTS`	Memeriksa nilai semua parameter kueri untuk upaya injeksi PowerShell perintah dalam aplikasi web. Pola kecocokan mewakili PowerShell perintah. Misalnya, `Invoke-Expression` . Tindakan aturan: Block label: `awswaf:managed:aws:windows-os:PowerShellCommands_QueryArguments`

Nama aturan	Deskripsi dan label
`PowerShellCommands_BODY`	Memeriksa badan permintaan untuk upaya injeksi PowerShell perintah dalam aplikasi web. Pola kecocokan mewakili PowerShell perintah. Misalnya, `Invoke-Expression` . **Warning** Aturan ini hanya memeriksa badan permintaan hingga batas ukuran tubuh untuk ACL web dan jenis sumber daya. Untuk Application Load Balancer dan AWS AppSync, limit ditetapka n pada 8 KB. Untuk CloudFront API Gateway, Amazon Cognito, App Runner, dan Akses Terverifikasi, batas default adalah 16 KB dan Anda dapat meningkatkan batas hingga 64 KB dalam konfigurasi ACL web Anda. Aturan ini menggunakan `Continue` opsi untuk penanganan konten yang terlalu besar. Untuk informasi selengkapnya, lihat Penanganan komponen permintaan kebesaran di AWS WAF. Tindakan aturan: Block label: `awswaf:managed:aws:windows-os:PowerShellCommands_Body`

Grup aturan terkelola aplikasi PHP

VendorName:`AWS`, Nama:`AWSManagedRulesPHPRuleSet`, WCU: 100

Grup aturan aplikasi PHP berisi aturan yang memblokir pola permintaan yang terkait dengan eksploitasi kerentanan khusus untuk penggunaan bahasa pemrograman PHP, termasuk injeksi fungsi PHP yang tidak aman. Ini dapat membantu mencegah eksploitasi kerentanan yang memungkinkan penyerang menjalankan kode atau perintah dari jarak jauh yang tidak diizinkan. Evaluasi grup aturan ini jika PHP diinstal pada server mana pun yang berinteraksi dengan aplikasi Anda.

Grup aturan terkelola ini menambahkan label ke permintaan web yang dievaluasi, yang tersedia untuk aturan yang berjalan setelah grup aturan ini di ACL web Anda. AWS WAF juga mencatat label ke CloudWatch metrik Amazon. Untuk informasi umum tentang label dan metrik label, lihat Label pada permintaan web danLabel metrik dan dimensi.

> **Note**
>
> Tabel ini menjelaskan versi statis terbaru dari grup aturan ini. Untuk versi lain, gunakan perintah API DescribeManagedRuleGroup.

Nama aturan	Deskripsi dan label
`PHPHighRiskMethodsVariables_HEADER`	Memeriksa semua header untuk upaya injeksi kode skrip PHP. Contoh pola termasuk fungsi seperti `fsockopen` dan variabel `$_GET` superglobal. **Warning** Aturan ini hanya memeriksa 8 KB pertama dari header permintaan atau 200 header pertama, batas mana pun yang tercapai terlebih dahulu, dan menggunakan opsi untuk penanganan konten yang terlalu besar. `Continue` Untuk informasi selengkapnya, lihat Penanganan komponen permintaan kebesaran di AWS WAF.

Nama aturan	Deskripsi dan label
	Tindakan aturan: Block label: `awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_Header`
`PHPHighRiskMethodsVariables_QUERYSTRING`	Memeriksa semuanya setelah yang pertama `?` di URL permintaan, mencari upaya injeksi kode skrip PHP. Contoh pola termasuk fungsi seperti `fsockopen` dan variabel `$_GET` superglobal. Tindakan aturan: Block label: `awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_QueryString`

Nama aturan	Deskripsi dan label
`PHPHighRiskMethodsVariables_BODY`	Memeriksa nilai-nilai badan permintaan untuk upaya injeksi kode skrip PHP. Contoh pola termasuk fungsi seperti `fsockopen` dan variabel `$_GET` superglobal. **Warning** Aturan ini hanya memeriksa badan permintaan hingga batas ukuran tubuh untuk ACL web dan jenis sumber daya. Untuk Application Load Balancer dan AWS AppSync, limit ditetapkan pada 8 KB. Untuk CloudFront API Gateway, Amazon Cognito, App Runner, dan Akses Terverifikasi, batas default adalah 16 KB dan Anda dapat meningkatkan batas hingga 64 KB dalam konfigurasi ACL web Anda. Aturan ini menggunakan `Continue` opsi untuk penanganan konten yang terlalu besar. Untuk informasi selengkapnya, lihat Penanganan komponen permintaan kebesaran di AWS WAF. Tindakan aturan: Block label: `awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_Body`

WordPress kelompok aturan terkelola aplikasi

VendorName:`AWS`, Nama:`AWSManagedRulesWordPressRuleSet`, WCU: 100

Grup aturan WordPress aplikasi berisi aturan yang memblokir pola permintaan yang terkait dengan eksploitasi kerentanan khusus untuk WordPress situs. Anda harus mengevaluasi kelompok aturan ini jika Anda menjalankanWordPress. Kelompok aturan ini harus digunakan bersama dengan kelompok Aplikasi PHP aturan Database SQL dan.

Grup aturan terkelola ini menambahkan label ke permintaan web yang dievaluasi, yang tersedia untuk aturan yang berjalan setelah grup aturan ini di ACL web Anda. AWS WAF juga mencatat label ke CloudWatch metrik Amazon. Untuk informasi umum tentang label dan metrik label, lihat Label pada permintaan web danLabel metrik dan dimensi.

> **Note**
>
> Tabel ini menjelaskan versi statis terbaru dari grup aturan ini. Untuk versi lain, gunakan perintah API DescribeManagedRuleGroup.

Nama aturan	Deskripsi dan label
`WordPressExploitableCommands_QUERYSTRING`	Memeriksa string permintaan permintaan untuk WordPress perintah berisiko tinggi yang dapat dieksploitasi dalam instalasi atau plugin yang rentan. Contoh pola termasuk perintah sepertido`-reset-wordpress` . Tindakan aturan: Block label: `awswaf:managed:aws:wordpress-app:WordPressExploitableCommands_QUERYSTRING`
`WordPressExploitablePaths_URIPATH`	Memeriksa jalur URI permintaan untuk WordPress file sepertixmlrpc.php , yang diketahui memiliki kerentanan yang mudah dieksploitasi.

Nama aturan	Deskripsi dan label
	Tindakan aturan: Block label: `awswaf:managed:aws:wordpress-app:WordPressExploitablePaths_URIPATH`

Grup aturan reputasi IP

Grup aturan reputasi IP memblokir permintaan berdasarkan alamat IP sumber mereka.

> **Note**
>
> Aturan ini menggunakan alamat IP sumber dari asal permintaan web. Jika Anda memiliki lalu lintas yang melewati satu atau lebih proxy atau penyeimbang beban, asal permintaan web akan berisi alamat proxy terakhir, dan bukan alamat asal klien.

Pilih satu atau beberapa grup aturan ini jika Anda ingin mengurangi eksposur terhadap lalu lintas bot atau upaya eksploitasi, atau jika Anda memberlakukan pembatasan geografis pada konten Anda. Untuk manajemen bot, lihat jugaAWS WAF Grup aturan Bot Control.

Grup aturan dalam kategori ini tidak menyediakan pemberitahuan pemutakhiran versi atau pembaruan SNS.

> **Note**
>
> Informasi yang kami publikasikan untuk aturan dalam kelompok aturan Aturan AWS Terkelola dimaksudkan untuk memberi Anda informasi yang cukup untuk menggunakan aturan sementara tidak memberikan informasi yang dapat digunakan oleh pelaku jahat untuk menghindari aturan. Jika Anda memerlukan informasi lebih lanjut daripada yang Anda temukan dalam dokumentasi ini, hubungi AWS Support Pusat.

Grup aturan terkelola daftar reputasi IP Amazon

VendorName:`AWS`, Nama:`AWSManagedRulesAmazonIpReputationList`, WCU: 25

Grup aturan daftar reputasi IP Amazon berisi aturan yang didasarkan pada intelijen ancaman internal Amazon. Ini berguna jika Anda ingin memblokir alamat IP yang biasanya terkait dengan bot atau ancaman lainnya. Memblokir alamat IP ini dapat membantu mengurangi bot dan mengurangi risiko aktor jahat menemukan aplikasi yang rentan.

Grup aturan terkelola ini menambahkan label ke permintaan web yang dievaluasi, yang tersedia untuk aturan yang berjalan setelah grup aturan ini di ACL web Anda. AWS WAF juga mencatat label ke CloudWatch metrik Amazon. Untuk informasi umum tentang label dan metrik label, lihat Label pada permintaan web danLabel metrik dan dimensi.

Nama aturan	Deskripsi dan label
`AWSManagedIPReputationList`	Memeriksa alamat IP yang telah diidentif ikasi sebagai aktif terlibat dalam aktivitas berbahaya. AWS WAF mengumpulkan daftar alamat IP dari berbagai sumber, termasuk MadPot, alat intelijen ancaman yang digunakan Amazon untuk melindungi pelanggan dari kejahatan dunia maya. Untuk informasi lebih lanjut tentang MadPot, lihathttps://www.about amazon.com/news/aws/amazon-madpot-stops-cybersecurity-crime. Tindakan aturan: Block Label: `awswaf:managed:aws:amazon-ip-list:AWSManagedIPReputati onList`
`AWSManagedReconnaissanceList`	Memeriksa koneksi dari alamat IP yang melakukan pengintaian terhadap sumber daya. AWS Tindakan aturan: Block Label: `awswaf:managed:aws:amazon-ip-list:AWSManagedReconnaiss anceList`

Nama aturan	Deskripsi dan label
`AWSManagedIPDDoSList`	Memeriksa alamat IP yang telah diidentifikasi sebagai aktif terlibat dalam aktivitas DDoS. Tindakan aturan: Count Label: `awswaf:managed:aws:amazon-ip-list:AWSManagedIPDDoSList`

Grup aturan terkelola daftar IP anonim

VendorName:`AWS`, Nama:`AWSManagedRulesAnonymousIpList`, WCU: 50

Grup aturan daftar IP Anonim berisi aturan untuk memblokir permintaan dari layanan yang mengizinkan pengaburan identitas penampil. Ini termasuk permintaan dari VPN, proxy, node Tor, dan penyedia hosting web. Grup aturan ini berguna jika Anda ingin memfilter pemirsa yang mungkin mencoba menyembunyikan identitas mereka dari aplikasi Anda. Memblokir alamat IP dari layanan ini dapat membantu mengurangi bot dan menghindari pembatasan geografis.

Grup aturan terkelola ini menambahkan label ke permintaan web yang dievaluasi, yang tersedia untuk aturan yang berjalan setelah grup aturan ini di ACL web Anda. AWS WAF juga mencatat label ke CloudWatch metrik Amazon. Untuk informasi umum tentang label dan metrik label, lihat Label pada permintaan web danLabel metrik dan dimensi.

Nama aturan	Deskripsi dan label
`AnonymousIPList`	Memeriksa daftar alamat IP sumber yang diketahui menganonimkan informasi klien, seperti node TOR, proxy sementara, dan layanan masking lainnya. Tindakan aturan: Block Label: `awswaf:managed:aws:anonymous-ip-list:AnonymousIPList`

Nama aturan	Deskripsi dan label
`HostingProviderIPList`	Memeriksa daftar alamat IP dari web hosting dan penyedia cloud, yang kecil kemungkin annya untuk sumber lalu lintas pengguna akhir. Daftar IP tidak termasuk alamat AWS IP. Tindakan aturan: Block Label: `awswaf:managed:aws:anonymou s-ip-list:HostingProviderIPList`

AWS WAF Grup aturan pencegahan penipuan (ACFP) pembuatan akun Kontrol Penipuan

VendorName:`AWS`, Nama:`AWSManagedRulesACFPRuleSet`, WCU: 50

Pencegahan AWS WAF penipuan pembuatan akun Kontrol Penipuan (ACFP) mengelola label grup aturan dan mengelola permintaan yang mungkin merupakan bagian dari upaya pembuatan akun palsu. Grup aturan melakukan ini dengan memeriksa permintaan pembuatan akun yang dikirim klien ke titik akhir pendaftaran dan pembuatan akun aplikasi Anda.

Grup aturan ACFP memeriksa upaya pembuatan akun dengan berbagai cara, untuk memberi Anda visibilitas dan kontrol atas interaksi yang berpotensi berbahaya. Grup aturan menggunakan token permintaan untuk mengumpulkan informasi tentang browser klien dan tentang tingkat interaktivitas manusia dalam pembuatan permintaan pembuatan akun. Grup aturan mendeteksi dan mengelola upaya pembuatan akun massal dengan menggabungkan permintaan berdasarkan alamat IP dan sesi klien, dan menggabungkan dengan informasi akun yang disediakan seperti alamat fisik dan nomor telepon. Selain itu, grup aturan mendeteksi dan memblokir pembuatan akun baru menggunakan kredensyal yang telah disusupi, yang membantu melindungi postur keamanan aplikasi Anda dan pengguna baru Anda.

Pertimbangan untuk menggunakan grup aturan ini

Grup aturan ini memerlukan konfigurasi khusus, yang mencakup spesifikasi pendaftaran akun aplikasi dan jalur pembuatan akun Anda. Kecuali jika disebutkan, aturan dalam grup aturan ini memeriksa semua permintaan yang dikirim klien Anda ke dua titik akhir ini. Untuk mengonfigurasi dan mengimplementasikan grup aturan ini, lihat panduan di[AWS WAF Pencegahan penipuan pembuatan akun Kontrol Penipuan (ACFP)](#).

> **Note**
>
> Anda akan dikenakan biaya tambahan saat menggunakan grup aturan terkelola ini. Untuk informasi selengkapnya, silakan lihat Harga AWS WAF.

Kelompok aturan ini adalah bagian dari perlindungan mitigasi ancaman cerdas di. AWS WAF Untuk informasi, lihat AWS WAF mitigasi ancaman cerdas.

Untuk menjaga biaya Anda turun dan memastikan Anda mengelola lalu lintas web Anda seperti yang Anda inginkan, gunakan kelompok aturan ini sesuai dengan panduan diPraktik terbaik untuk mitigasi ancaman cerdas.

Grup aturan ini tidak tersedia untuk digunakan dengan kumpulan pengguna Amazon Cognito. Anda tidak dapat mengaitkan ACL web yang menggunakan grup aturan ini dengan kumpulan pengguna, dan Anda tidak dapat menambahkan grup aturan ini ke ACL web yang sudah dikaitkan dengan kumpulan pengguna.

Label ditambahkan oleh grup aturan ini

Grup aturan terkelola ini menambahkan label ke permintaan web yang dievaluasi, yang tersedia untuk aturan yang berjalan setelah grup aturan ini di ACL web Anda. AWS WAF juga mencatat label ke CloudWatch metrik Amazon. Untuk informasi umum tentang label dan metrik label, lihat Label pada permintaan web danLabel metrik dan dimensi.

Label token

Grup aturan ini menggunakan manajemen AWS WAF token untuk memeriksa dan memberi label permintaan web sesuai dengan status AWS WAF token mereka. AWS WAF menggunakan token untuk pelacakan dan verifikasi sesi klien.

Untuk informasi tentang token dan manajemen token, lihatAWS WAF token permintaan web.

Untuk informasi tentang komponen label yang dijelaskan di sini, lihatAWS WAF sintaks label dan persyaratan penamaan.

Label sesi klien

Label `awswaf:managed:token:id:`*`identifier`* berisi pengenal unik yang digunakan manajemen AWS WAF token untuk mengidentifikasi sesi klien. Pengidentifikasi dapat berubah jika klien memperoleh token baru, misalnya setelah membuang token yang digunakannya.

> **Note**
>
> AWS WAF tidak melaporkan CloudWatch metrik Amazon untuk label ini.

Label status token: Awalan namespace label

Label status token melaporkan status token dan tantangan serta informasi CAPTCHA yang dikandungnya.

Setiap label status token dimulai dengan salah satu awalan namespace berikut:

- `awswaf:managed:token:` — Digunakan untuk melaporkan status umum token dan melaporkan status informasi tantangan token.
- `awswaf:managed:captcha:` — Digunakan untuk melaporkan status informasi CAPTCHA token.

Label status token: Nama label

Mengikuti awalan, sisa label memberikan informasi status token terperinci:

- `accepted` — Token permintaan hadir dan berisi yang berikut:
  - Tantangan yang valid atau solusi CAPTCHA.
  - Tantangan yang belum kedaluwarsa atau cap waktu CAPTCHA.
  - Spesifikasi domain yang valid untuk web ACL.

  Contoh: Label `awswaf:managed:token:accepted` menunjukkan bahwa token permintaan web memiliki solusi tantangan yang valid, stempel waktu tantangan yang belum kedaluwarsa, dan domain yang valid.
- `rejected` — Token permintaan ada tetapi tidak memenuhi kriteria penerimaan.

  Seiring dengan label yang ditolak, manajemen token menambahkan namespace dan nama label khusus untuk menunjukkan alasannya.
  - `rejected:not_solved` — Token tidak memiliki tantangan atau solusi CAPTCHA.
  - `rejected:expired` — Tantangan token atau cap waktu CAPTCHA telah kedaluwarsa, sesuai dengan waktu kekebalan token ACL web Anda yang dikonfigurasi.
  - `rejected:domain_mismatch` — Domain token tidak cocok untuk konfigurasi domain token ACL web Anda.

- `rejected:invalid`— AWS WAF tidak bisa membaca token yang ditunjukkan.

  Contoh: Label `awswaf:managed:captcha:rejected` dan `awswaf:managed:captcha:rejected:expired` menunjukkan bahwa permintaan ditolak karena cap waktu CAPTCHA dalam token telah melebihi waktu kekebalan token CAPTCHA yang dikonfigurasi di ACL web.

- `absent`— Permintaan tidak memiliki token atau manajer token tidak dapat membacanya.

  Contoh: Label `awswaf:managed:captcha:absent` menunjukkan bahwa permintaan tidak memiliki token.

Label ACFP

Grup aturan ini menghasilkan label dengan awalan namespace `awswaf:managed:aws:acfp:` diikuti oleh namespace kustom dan nama label. Grup aturan dapat menambahkan lebih dari satu label ke permintaan.

Anda dapat mengambil semua label untuk grup aturan melalui API dengan memanggil`DescribeManagedRuleGroup`. Label tercantum di `AvailableLabels` properti dalam tanggapan.

Daftar aturan pencegahan penipuan pembuatan akun

Bagian ini mencantumkan aturan ACFP `AWSManagedRulesACFPRuleSet` dan label yang ditambahkan aturan grup aturan ke permintaan web.

> **Note**
>
> Informasi yang kami publikasikan untuk aturan dalam kelompok aturan Aturan AWS Terkelola dimaksudkan untuk memberi Anda informasi yang cukup untuk menggunakan aturan sementara tidak memberikan informasi yang dapat digunakan oleh pelaku jahat untuk menghindari aturan. Jika Anda memerlukan informasi lebih lanjut daripada yang Anda temukan dalam dokumentasi ini, hubungi AWS Support Pusat.

Semua aturan dalam grup aturan ini memerlukan token permintaan web, kecuali untuk dua yang pertama `UnsupportedCognitoIDP` dan`AllRequests`. Untuk deskripsi informasi yang disediakan token, lihatAWS WAF karakteristik token.

Kecuali jika disebutkan, aturan dalam grup aturan ini memeriksa semua permintaan yang dikirim klien Anda ke jalur halaman pendaftaran akun dan pembuatan akun yang Anda berikan dalam konfigurasi grup aturan. Untuk informasi tentang mengonfigurasi grup aturan ini, lihatAWS WAF Pencegahan penipuan pembuatan akun Kontrol Penipuan (ACFP).

Nama aturan	Deskripsi dan label
`UnsupportedCognitoIDP`	Memeriksa lalu lintas web yang menuju ke kumpulan pengguna Amazon Cognito. ACFP tidak tersedia untuk digunakan dengan kumpulan pengguna Amazon Cognito, dan aturan ini membantu memastikan bahwa aturan grup aturan ACFP lainnya tidak digunakan untuk mengevaluasi lalu lintas kumpulan pengguna. Tindakan aturan: Block Label: `awswaf:managed:aws:acfp:unsupported:cognito_idp`
`AllRequests`	Menerapkan tindakan aturan untuk permintaan yang mengakses jalur halaman pendaftaran. Anda mengonfigurasi jalur halaman pendaftaran saat mengonfigurasi grup aturan. Secara default, aturan ini berlaku Challenge untuk permintaan. Dengan menerapkan tindakan ini, aturan memastikan bahwa klien memperoleh token tantangan sebelum permintaan apa pun dievaluasi oleh aturan lainnya di grup aturan. Pastikan bahwa pengguna akhir Anda memuat jalur halaman pendaftaran sebelum mereka mengirimkan permintaan pembuatan akun.

Nama aturan	Deskripsi dan label
	Token ditambahkan ke permintaan oleh SDK integrasi aplikasi klien dan oleh tindakan aturan CAPTCHA danChallenge. Untuk akuisisi token yang paling efisien, kami sangat menyarankan Anda menggunakan SDK integrasi aplikasi. Untuk informasi selengkapnya, lihat AWS WAF integrasi aplikasi klien. Tindakan aturan: Challenge Label: Tidak ada

Nama aturan	Deskripsi dan label
`RiskScoreHigh`	Memeriksa permintaan pembuatan akun dengan alamat IP atau faktor lain yang dianggap sangat mencurigakan. Evaluasi ini biasanya didasarkan pada beberapa faktor yang berkontribusi, yang dapat Anda lihat di `risk_score` label yang ditambahkan grup aturan ke permintaan. Tindakan aturan: Block Label: `awswaf:managed:aws:acfp:risk_score:high` Aturan mungkin juga berlaku `medium` atau label skor `low` risiko untuk permintaan. Jika AWS WAF tidak berhasil mengevaluasi skor risiko untuk permintaan web, aturan menambahkan label `awswaf:managed:aws:acfp:risk_score:evaluation_failed` Selain itu, aturan menambahkan label dengan namespace `awswaf:managed:aws:acfp:risk_score:contributor:` yang mencakup status evaluasi skor risiko dan hasil untuk kontributor skor risiko tertentu, seperti reputasi IP dan evaluasi kredensional yang dicuri.

Nama aturan	Deskripsi dan label
`SignalCredentialCompromised`	Mencari database kredensyal yang dicuri untuk kredensyal yang dikirimkan dalam permintaan pembuatan akun. Aturan ini memastikan bahwa klien baru menginisialisasi akun mereka dengan postur keamanan yang positif. **Note** Anda dapat menambahkan respons pemblokiran khusus, untuk menjelaskan masalah kepada pengguna akhir Anda dan memberi tahu mereka cara melanjutkan. Untuk informasi, lihat Contoh ACFP: Respons khusus untuk kredensil yang dikompromikan. Tindakan aturan: Block Label: `awswaf:managed:aws:acfp:signal:credential_compromised` Grup aturan menerapkan label terkait berikut, tetapi tidak mengambil tindakan terhadapnya, karena tidak semua permintaan dalam pembuatan akun akan memiliki kredensyal: `awswaf:managed:aws:acfp:signal:missing_credential`

Nama aturan	Deskripsi dan label
`SignalClientHumanInteractivityAbsentLow`	Memeriksa token permintaan pembuatan akun untuk data yang menunjukkan interaktivitas manusia abnormal dengan aplikasi. Interaktivitas manusia dideteksi melalui interaksi seperti gerakan mouse dan penekanan tombol. Jika halaman memiliki bentuk HTML, interaktivitas manusia mencakup interaksi dengan formulir. **Note** Aturan ini hanya memeriksa permintaan ke jalur pembuatan akun dan hanya dievaluasi jika Anda telah menerapkan SDK integrasi aplikasi. Implementasi SDK secara pasif menangkap interaktivitas manusia dan menyimpan informasi dalam token permintaan. Untuk informasi selengkapnya, lihat AWS WAF karakteristik token dan AWS WAF integrasi aplikasi klien. Tindakan aturan: CAPTCHA Label: Tidak ada. Aturan menentukan kecocokan berdasarkan berbagai faktor, sehingga tidak ada label individual yang berlaku untuk setiap skenario kecocokan yang mungkin. Grup aturan dapat menerapkan satu atau beberapa label berikut ke permintaan:

Nama aturan	Deskripsi dan label

	`awswaf:managed:aws:acfp:signal:client:human_interactivity:low/medium/high`
	
	`awswaf:managed:aws:acfp:signal:client:human_interactivity:insufficient_data`
	
	`awswaf:managed:aws:acfp:signal:form_detected` .

`SignalAutomatedBrowser`	Memeriksa permintaan indikator bahwa browser klien mungkin otomatis. Tindakan aturan: Block Label: `awswaf:managed:aws:acfp:signal:automated_browser`
`SignalBrowserInconsistency`	Memeriksa token permintaan untuk data interogasi browser yang tidak konsisten. Untuk informasi selengkapnya, lihat AWS WAF karakteristik token. Tindakan aturan: CAPTCHA Label: `awswaf:managed:aws:acfp:signal:browser_inconsistency`

Nama aturan	Deskripsi dan label
`VolumetricIpHigh`	Memeriksa volume permintaan pembuatan akun yang tinggi yang dikirim dari alamat IP individual. Volume tinggi lebih dari 20 permintaan dalam jendela 10 menit. **Note** Ambang batas yang diterapkan aturan ini dapat sedikit berbeda karena latensi. Untuk volume tinggi, beberapa permintaan mungkin berhasil melewati batas sebelum tindakan aturan diterapkan. Tindakan aturan: CAPTCHA Label: `awswaf:managed:aws:acfp:aggregate:volumetric:ip:creation:high` Aturan menerapkan label berikut untuk permintaan dengan volume sedang (lebih dari 15 permintaan per jendela 10 menit) dan volume rendah (lebih dari 10 permintaan per jendela 10 menit), tetapi tidak mengambil tindakan pada mereka: `awswaf:managed:aws:acfp:aggregate:volumetric:ip:creation:medium` dan`awswaf:managed:aws:acfp:aggregate:volumetric:ip:creation:low` .

Nama aturan	Deskripsi dan label
`VolumetricSessionHigh`	Memeriksa volume permintaan pembuatan akun yang tinggi yang dikirim dari sesi klien individual. Volume tinggi lebih dari 10 permintaan dalam jendela 30 menit. **Note** Ambang batas yang diterapkan aturan ini dapat sedikit berbeda karena latensi. Beberapa permintaan mungkin berhasil melewati batas sebelum tindakan aturan diterapkan. Tindakan aturan: Block Label: `awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:high` Grup aturan menerapkan label berikut untuk permintaan dengan volume sedang (lebih dari 5 permintaan per jendela 30 menit) dan volume rendah (lebih dari 1 permintaan per jendela 30 menit), tetapi tidak mengambil tindakan pada mereka: `awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:medium` dan`awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:low` .

Nama aturan	Deskripsi dan label
`AttributeUsernameTraversalHigh`	Memeriksa permintaan pembuatan akun tingkat tinggi dari satu sesi klien yang menggunakan nama pengguna yang berbeda. Ambang batas untuk evaluasi tinggi lebih dari 10 permintaan dalam 30 menit. **Note** Ambang batas yang diterapkan aturan ini dapat sedikit berbeda karena latensi. Beberapa permintaan mungkin berhasil melewati batas sebelum tindakan aturan diterapkan. Tindakan aturan: Block Label: `awswaf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:high` Grup aturan menerapkan label berikut untuk permintaan dengan volume sedang (lebih dari 5 permintaan per jendela 30 menit) dan volume rendah (lebih dari 1 permintaan per jendela 30 menit) permintaan traversal nama pengguna, tetapi tidak mengambil tindakan terhadapnya: `awswaf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:medium` dan`awswaf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:low` .

Nama aturan	Deskripsi dan label
`VolumetricPhoneNumberHigh`	Memeriksa volume tinggi permintaan pembuatan akun yang menggunakan nomor telepon yang sama. Ambang batas untuk evaluasi tinggi lebih dari 10 permintaan dalam 30 menit. **Note** Ambang batas yang diterapkan aturan ini dapat sedikit berbeda karena latensi. Beberapa permintaan mungkin berhasil melewati batas sebelum tindakan aturan diterapkan. Tindakan aturan: Block Label: `awswaf:managed:aws:acfp:aggregate:volumetric:phone_number:high` Grup aturan menerapkan label berikut untuk permintaan dengan volume sedang (lebih dari 5 permintaan per jendela 30 menit) dan volume rendah (lebih dari 1 permintaan per jendela 30 menit), tetapi tidak mengambil tindakan pada mereka: `awswaf:managed:aws:acfp:aggregate:volumetric:phone_number:medium` dan `awswaf:managed:aws:acfp:aggregate:volumetric:phone_number:low` .

Nama aturan	Deskripsi dan label
`VolumetricAddressHigh`	Memeriksa volume permintaan pembuatan akun yang tinggi yang menggunakan alamat fisik yang sama. Ambang batas untuk evaluasi tinggi lebih dari 100 permintaan per jendela 30 menit. **Note** Ambang batas yang diterapkan aturan ini dapat sedikit berbeda karena latensi. Beberapa permintaan mungkin berhasil melewati batas sebelum tindakan aturan diterapkan. Tindakan aturan: Block Label: `awswaf:managed:aws:acfp:aggregate:volumetric:address:high`

Nama aturan	Deskripsi dan label
`VolumetricAddressLow`	Memeriksa volume rendah dan menengah permintaan pembuatan akun yang menggunakan alamat fisik yang sama. Ambang batas untuk evaluasi menengah lebih dari 50 permintaan per jendela 30 menit, dan untuk evaluasi rendah lebih dari 10 permintaan per jendela 30 menit. Aturan tersebut menerapkan tindakan untuk volume sedang atau rendah. **Note** Ambang batas yang diterapkan aturan ini dapat sedikit berbeda karena latensi. Beberapa permintaan mungkin berhasil melewati batas sebelum tindakan aturan diterapkan. Tindakan aturan: CAPTCHA Label: `awswaf:managed:aws:acfp:aggregate:volumetric:address:low` atau `awswaf:managed:aws:acfp:aggregate:volumetric:address:medium`

Nama aturan	Deskripsi dan label
`VolumetricIPSuccessfulResponse`	Memeriksa volume tinggi permintaan pembuatan akun yang berhasil untuk satu alamat IP. Aturan ini menggabungkan respons sukses dari sumber daya yang dilindungi ke permintaan pembuatan akun. Ambang batas untuk evaluasi tinggi lebih dari 10 permintaan per jendela 10 menit. Aturan ini membantu melindungi terhadap upaya pembuatan akun massal. Ini memiliki ambang batas yang lebih rendah dari aturan`VolumetricIpHigh` , yang hanya menghitung permintaan. Jika Anda telah mengonfigurasi grup aturan untuk memeriksa badan respons atau komponen JSON, AWS WAF dapat memeriksa 65.536 byte (64 KB) pertama dari jenis komponen ini untuk indikator keberhasilan atau kegagalan. Aturan ini menerapkan tindakan aturan dan pelabelan untuk permintaan web baru dari alamat IP, berdasarkan respons keberhasi lan dan kegagalan dari sumber daya yang dilindungi untuk upaya login terbaru dari alamat IP yang sama. Anda menentukan cara menghitung keberhasilan dan kegagalan saat Anda mengonfigurasi grup aturan.

Nama aturan	Deskripsi dan label
	Note AWS WAF hanya mengevaluasi aturan ini di ACL web yang melindungi distribusi Amazon CloudFront .
	Note Ambang batas yang diterapkan aturan ini dapat sedikit berbeda karena latensi. Klien dapat mengirim upaya pembuatan akun yang lebih berhasil daripada yang diizinkan sebelum aturan mulai cocok pada upaya berikutnya.
	Tindakan aturan: Block Label: `awswaf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:high` Grup aturan juga menerapkan label terkait berikut ke permintaan, tanpa tindakan terkait apa pun. Semua hitungan adalah untuk jendela 10 menit. `awswaf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:medium` untuk lebih dari 5 permintaan yang berhasil, `awswaf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:low` untuk lebih dari 1 permintaa

Nama aturan	Deskripsi dan label
	n yang berhasil, `awswaf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:high` untuk lebih dari 10 permintaan gagal, `awswaf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:medium` untuk lebih dari 5 permintaan gagal, dan `awswaf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:low` untuk lebih dari 1 permintaan gagal.

Nama aturan	Deskripsi dan label
`VolumetricSessionSuccessful Response`	Memeriksa volume respons keberhasilan yang rendah dari sumber daya yang dilindungi ke permintaan pembuatan akun yang dikirim dari satu sesi klien. Ini membantu melindungi dari upaya pembuatan akun massal. Ambang batas untuk evaluasi rendah lebih dari 1 permintaan per jendela 30 menit. Ini membantu melindungi dari upaya pembuatan akun massal. Aturan ini menggunak an ambang batas yang lebih rendah dari aturan`VolumetricSessionHigh` , yang hanya melacak permintaan. Jika Anda telah mengonfigurasi grup aturan untuk memeriksa badan respons atau komponen JSON, AWS WAF dapat memeriksa 65.536 byte (64 KB) pertama dari jenis komponen ini untuk indikator keberhasilan atau kegagalan. Aturan ini menerapkan tindakan aturan dan pelabelan untuk permintaan web baru dari sesi klien, berdasarkan respons keberhasilan dan kegagalan dari sumber daya yang dilindungi untuk upaya login terbaru dari sesi klien yang sama. Anda menentukan cara menghitun g keberhasilan dan kegagalan saat Anda mengonfigurasi grup aturan.

Nama aturan	Deskripsi dan label
	Note AWS WAF hanya mengevaluasi aturan ini di ACL web yang melindungi distribusi Amazon CloudFront .
	Note Ambang batas yang diterapkan aturan ini dapat sedikit berbeda karena latensi. Klien dapat mengirim lebih banyak upaya pembuatan akun yang gagal daripada yang diizinkan sebelum aturan mulai cocok pada upaya berikutnya.
	Tindakan aturan: Block Label: `awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_response:low` Grup aturan juga menerapkan label terkait berikut untuk permintaan. Semua hitungan adalah untuk jendela 30 menit. `awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_response:high` untuk lebih dari 10 permintaan yang berhasil, `awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_response:medium` untuk lebih dari 5 permintaan

Nama aturan	Deskripsi dan label
	yang berhasil, `awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:high` untuk lebih dari 10 permintaan gagal, `awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:medium` untuk lebih dari 5 permintaan gagal, dan `awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:low` untuk lebih dari 1 permintaan gagal.
`VolumetricSessionTokenReuseIp`	Memeriksa permintaan pembuatan akun untuk penggunaan token tunggal di antara lebih dari 5 alamat IP yang berbeda. **Note** Ambang batas yang diterapkan aturan ini dapat sedikit berbeda karena latensi. Beberapa permintaan mungkin berhasil melewati batas sebelum tindakan aturan diterapkan. Tindakan aturan: Block Label: `awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:token_reuse:ip`

AWS WAF Kelompok aturan pencegahan pengambilalihan akun Kontrol Penipuan (ATP)

VendorName:`AWS`, Nama:`AWSManagedRulesATPRuleSet`, WCU: 50

Pencegahan Pengambilalihan Akun Kontrol AWS WAF Penipuan (ATP) mengelola label grup aturan dan mengelola permintaan yang mungkin merupakan bagian dari upaya pengambilalihan akun berbahaya. Grup aturan melakukan ini dengan memeriksa upaya login yang dikirim klien ke titik akhir login aplikasi Anda.

- Inspeksi permintaan — ATP memberi Anda visibilitas dan kontrol atas upaya login anomali dan upaya login yang menggunakan kredensi curian, untuk mencegah pengambilalihan akun yang dapat menyebabkan aktivitas penipuan. ATP memeriksa kombinasi email dan kata sandi terhadap basis data kredensialnya yang dicuri, yang diperbarui secara berkala karena kredensil baru yang bocor ditemukan di web gelap. ATP mengumpulkan data berdasarkan alamat IP dan sesi klien, untuk mendeteksi dan memblokir klien yang mengirim terlalu banyak permintaan yang bersifat mencurigakan.
- Inspeksi respons — Untuk CloudFront distribusi, selain memeriksa permintaan masuk masuk, grup aturan ATP memeriksa respons aplikasi Anda terhadap upaya login, untuk melacak tingkat keberhasilan dan kegagalan. Dengan menggunakan informasi ini, ATP dapat memblokir sementara sesi klien atau alamat IP yang memiliki terlalu banyak kegagalan login. AWS WAF melakukan inspeksi respons secara asinkron, jadi ini tidak meningkatkan latensi dalam lalu lintas web Anda.

Pertimbangan untuk menggunakan grup aturan ini

Grup aturan ini memerlukan konfigurasi khusus. Untuk mengonfigurasi dan mengimplementasikan grup aturan ini, lihat panduan diAWS WAF Pencegahan pengambilalihan akun Kontrol Penipuan (ATP).

Kelompok aturan ini adalah bagian dari perlindungan mitigasi ancaman cerdas di. AWS WAF Untuk informasi, lihat AWS WAF mitigasi ancaman cerdas.

> **Note**
>
> Anda akan dikenakan biaya tambahan saat menggunakan grup aturan terkelola ini. Untuk informasi selengkapnya, silakan lihat Harga AWS WAF.

Untuk menjaga biaya Anda turun dan memastikan Anda mengelola lalu lintas web Anda seperti yang Anda inginkan, gunakan kelompok aturan ini sesuai dengan panduan diPraktik terbaik untuk mitigasi ancaman cerdas.

Grup aturan ini tidak tersedia untuk digunakan dengan kumpulan pengguna Amazon Cognito. Anda tidak dapat mengaitkan ACL web yang menggunakan grup aturan ini dengan kumpulan pengguna, dan Anda tidak dapat menambahkan grup aturan ini ke ACL web yang sudah dikaitkan dengan kumpulan pengguna.

Label ditambahkan oleh grup aturan ini

Grup aturan terkelola ini menambahkan label ke permintaan web yang dievaluasi, yang tersedia untuk aturan yang berjalan setelah grup aturan ini di ACL web Anda. AWS WAF juga mencatat label ke CloudWatch metrik Amazon. Untuk informasi umum tentang label dan metrik label, lihat Label pada permintaan web danLabel metrik dan dimensi.

Label token

Grup aturan ini menggunakan manajemen AWS WAF token untuk memeriksa dan memberi label permintaan web sesuai dengan status AWS WAF token mereka. AWS WAF menggunakan token untuk pelacakan dan verifikasi sesi klien.

Untuk informasi tentang token dan manajemen token, lihatAWS WAF token permintaan web.

Untuk informasi tentang komponen label yang dijelaskan di sini, lihatAWS WAF sintaks label dan persyaratan penamaan.

Label sesi klien

Label `awswaf:managed:token:id:`*`identifier`* berisi pengidentifikasi unik yang digunakan manajemen AWS WAF token untuk mengidentifikasi sesi klien. Pengidentifikasi dapat berubah jika klien memperoleh token baru, misalnya setelah membuang token yang digunakannya.

> **Note**
>
> AWS WAF tidak melaporkan CloudWatch metrik Amazon untuk label ini.

Label status token: Awalan namespace label

Label status token melaporkan status token dan tantangan serta informasi CAPTCHA yang dikandungnya.

Setiap label status token dimulai dengan salah satu awalan namespace berikut:

- `awswaf:managed:token:` — Digunakan untuk melaporkan status umum token dan melaporkan status informasi tantangan token.
- `awswaf:managed:captcha:` — Digunakan untuk melaporkan status informasi CAPTCHA token.

Label status token: Nama label

Mengikuti awalan, sisa label memberikan informasi status token terperinci:

- `accepted` — Token permintaan hadir dan berisi yang berikut:
  - Tantangan yang valid atau solusi CAPTCHA.
  - Tantangan yang belum kedaluwarsa atau cap waktu CAPTCHA.
  - Spesifikasi domain yang valid untuk web ACL.

  Contoh: Label `awswaf:managed:token:accepted` menunjukkan bahwa token permintaan web memiliki solusi tantangan yang valid, stempel waktu tantangan yang belum kedaluwarsa, dan domain yang valid.
- `rejected` — Token permintaan ada tetapi tidak memenuhi kriteria penerimaan.

  Seiring dengan label yang ditolak, manajemen token menambahkan namespace dan nama label khusus untuk menunjukkan alasannya.
  - `rejected:not_solved` — Token tidak memiliki tantangan atau solusi CAPTCHA.
  - `rejected:expired` — Tantangan token atau cap waktu CAPTCHA telah kedaluwarsa, sesuai dengan waktu kekebalan token ACL web Anda yang dikonfigurasi.
  - `rejected:domain_mismatch` — Domain token tidak cocok untuk konfigurasi domain token ACL web Anda.
  - `rejected:invalid` — AWS WAF tidak bisa membaca token yang ditunjukkan.

  Contoh: Label `awswaf:managed:captcha:rejected` dan `awswaf:managed:captcha:rejected:expired` menunjukkan bahwa permintaan ditolak karena cap waktu CAPTCHA dalam token telah melebihi waktu kekebalan token CAPTCHA yang dikonfigurasi di ACL web.
- `absent` — Permintaan tidak memiliki token atau manajer token tidak dapat membacanya.

  Contoh: Label `awswaf:managed:captcha:absent` menunjukkan bahwa permintaan tidak memiliki token.

Label ATP

Grup aturan terkelola ATP menghasilkan label dengan awalan namespace `awswaf:managed:aws:atp:` diikuti dengan namespace kustom dan nama label.

Grup aturan dapat menambahkan salah satu label berikut selain label yang dicatat dalam daftar aturan:

- `awswaf:managed:aws:atp:signal:credential_compromised`— Menunjukkan bahwa kredensyal yang dikirimkan dalam permintaan ada di database kredensi yang dicuri.
- `awswaf:managed:aws:atp:aggregate:attribute:suspicious_tls_fingerprint`— Hanya tersedia untuk CloudFront distribusi Amazon yang dilindungi. Menunjukkan bahwa sesi klien telah mengirim beberapa permintaan yang menggunakan sidik jari TLS yang mencurigakan.
- `awswaf:managed:aws:atp:aggregate:volumetric:session:token_reuse:ip`— Menunjukkan penggunaan token tunggal di antara lebih dari 5 alamat IP yang berbeda. Ambang batas yang diterapkan aturan ini dapat sedikit berbeda karena latensi. Beberapa permintaan mungkin berhasil melewati batas sebelum label diterapkan.

Anda dapat mengambil semua label untuk grup aturan melalui API dengan memanggil`DescribeManagedRuleGroup`. Label tercantum di `AvailableLabels` properti dalam tanggapan.

Daftar aturan pencegahan pengambilalihan akun

Bagian ini mencantumkan aturan ATP `AWSManagedRulesATPRuleSet` dan label yang ditambahkan aturan grup aturan ke permintaan web.

> **Note**
>
> Informasi yang kami publikasikan untuk aturan dalam kelompok aturan Aturan AWS Terkelola dimaksudkan untuk memberi Anda informasi yang cukup untuk menggunakan aturan sementara tidak memberikan informasi yang dapat digunakan oleh pelaku jahat untuk menghindari aturan. Jika Anda memerlukan informasi lebih lanjut daripada yang Anda temukan dalam dokumentasi ini, hubungi AWS Support Pusat.

Nama aturan	Deskripsi dan label
`UnsupportedCognitoIDP`	Memeriksa lalu lintas web yang menuju ke kumpulan pengguna Amazon Cognito. ATP tidak tersedia untuk digunakan dengan kumpulan pengguna Amazon Cognito, dan aturan ini membantu memastikan bahwa aturan grup aturan ATP lainnya tidak digunakan untuk mengevaluasi lalu lintas kumpulan pengguna. Tindakan aturan: Block Label: `awswaf:managed:aws:atp:unsupported:cognito_idp`
`VolumetricIpHigh`	Memeriksa volume permintaan yang tinggi yang dikirim dari alamat IP individual. Volume tinggi lebih dari 20 permintaan dalam jendela 10 menit. **Note** Ambang batas yang diterapkan aturan ini dapat sedikit berbeda karena latensi. Untuk volume tinggi, beberapa permintaan mungkin berhasil melewati batas sebelum tindakan aturan diterapkan. Tindakan aturan: Block Label: `awswaf:managed:aws:atp:aggregate:volumetric:ip:high` Grup aturan menerapkan label berikut untuk permintaan dengan volume sedang

Nama aturan	Deskripsi dan label
	(lebih dari 15 permintaan per jendela 10 menit) dan volume rendah (lebih dari 10 permintaan per jendela 10 menit), tetapi tidak mengambil tindakan pada mereka: `awswaf:managed:aws:atp:aggregate:volumetric:ip:medium` dan `awswaf:managed:aws:atp:aggregate:volumetric:ip:low` .
`VolumetricSession`	Memeriksa volume permintaan yang tinggi yang dikirim dari sesi klien individual. Ambang batas lebih dari 20 permintaan per jendela 30 menit. Pemeriksaan ini hanya berlaku ketika permintaan web memiliki token. Token ditambahkan ke permintaan oleh SDK integrasi aplikasi dan oleh tindakan aturan CAPTCHA dan Challenge. Untuk informasi selengkapnya, lihat AWS WAF token permintaan web. **Note** Ambang batas yang diterapkan aturan ini dapat sedikit berbeda karena latensi. Beberapa permintaan mungkin berhasil melewati batas sebelum tindakan aturan diterapkan. Tindakan aturan: Block Label: `awswaf:managed:aws:atp:aggregate:volumetric:session`

Nama aturan	Deskripsi dan label
`AttributeCompromisedCredentials`	Memeriksa beberapa permintaan dari sesi klien yang sama yang menggunakan kredensyal curian. Tindakan aturan: Block Label: `awswaf:managed:aws:atp:aggregate:attribute:compromised_credentials`
`AttributeUsernameTraversal`	Memeriksa beberapa permintaan dari sesi klien yang sama yang menggunakan traversal nama pengguna. Tindakan aturan: Block Label: `awswaf:managed:aws:atp:aggregate:attribute:username_traversal`
`AttributePasswordTraversal`	Memeriksa beberapa permintaan dengan nama pengguna yang sama yang menggunakan traversal kata sandi. Tindakan aturan: Block Label: `awswaf:managed:aws:atp:aggregate:attribute:password_traversal`

Nama aturan	Deskripsi dan label
`AttributeLongSession`	Memeriksa beberapa permintaan dari sesi klien yang sama yang menggunakan sesi jangka panjang. Ambang batas lebih dari 6 jam lalu lintas yang memiliki setidaknya satu permintaan login setiap 30 menit. Pemeriksaan ini hanya berlaku ketika permintaan web memiliki token. Token ditambahkan ke permintaan oleh SDK integrasi aplikasi dan oleh tindakan aturan CAPTCHA danChallenge. Untuk informasi selengkapnya, lihat AWS WAF token permintaan web. Tindakan aturan: Block Label: `awswaf:managed:aws:atp:aggregate:attribute:long_session`
`TokenRejected`	Memeriksa permintaan dengan token yang ditolak oleh manajemen AWS WAF token. Pemeriksaan ini hanya berlaku ketika permintaan web memiliki token. Token ditambahkan ke permintaan oleh SDK integrasi aplikasi dan oleh tindakan aturan CAPTCHA danChallenge. Untuk informasi selengkapnya, lihat AWS WAF token permintaan web. Tindakan aturan: Block Label: Tidak ada. Untuk memeriksa token yang ditolak, gunakan aturan pencocokan label agar sesuai dengan label: `awswaf:managed:token:rejected`

Nama aturan	Deskripsi dan label
`SignalMissingCredential`	Memeriksa permintaan dengan kredensyal yang tidak memiliki nama pengguna atau kata sandi. Tindakan aturan: Block Label: `awswaf:managed:aws:atp:signal:missing_credential`

Nama aturan	Deskripsi dan label
`VolumetricIpFailedLoginResponseHigh`	Memeriksa alamat IP yang baru-baru ini menjadi sumber tingkat upaya login yang gagal terlalu tinggi. Volume tinggi lebih dari 10 permintaan login gagal dari alamat IP dalam jendela 10 menit. Jika Anda telah mengonfigurasi grup aturan untuk memeriksa badan respons atau komponen JSON, AWS WAF dapat memeriksa 65.536 byte (64 KB) pertama dari jenis komponen ini untuk indikator keberhasilan atau kegagalan. Aturan ini menerapkan tindakan aturan dan pelabelan untuk permintaan web baru dari alamat IP, berdasarkan respons keberhasilan dan kegagalan dari sumber daya yang dilindungi untuk upaya login terbaru dari alamat IP yang sama. Anda menentukan cara menghitung keberhasilan dan kegagalan saat Anda mengonfigurasi grup aturan. **Note** AWS WAF hanya mengevaluasi aturan ini di ACL web yang melindungi distribusi Amazon CloudFront. **Note** Ambang batas yang diterapkan aturan ini dapat sedikit berbeda karena latensi. Klien dapat mengirim lebih banyak

Nama aturan	Deskripsi dan label
	upaya login yang gagal daripada yang diizinkan sebelum aturan mulai cocok pada upaya berikutnya. Tindakan aturan: Block Label: `awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:high` Grup aturan juga menerapkan label terkait berikut ke permintaan, tanpa tindakan terkait apa pun. Semua hitungan untuk jendela 10 menit. `awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:medium` untuk lebih dari 5 permintaan gagal, `awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:low` untuk lebih dari 1 permintaan gagal, `awswaf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:high` untuk lebih dari 10 permintaan yang berhasil, `awswaf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:medium` untuk lebih dari 5 permintaan yang berhasil, dan `awswaf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:low` untuk lebih dari 1 permintaan yang berhasil.

Nama aturan	Deskripsi dan label
`VolumetricSessionFailedLogi nResponseHigh`	Memeriksa sesi klien yang baru-baru ini menjadi sumber tingkat upaya login yang gagal terlalu tinggi. Volume tinggi lebih dari 10 permintaan login gagal dari sesi klien dalam jendela 30 menit. Jika Anda telah mengonfigurasi grup aturan untuk memeriksa badan respons atau komponen JSON, AWS WAF dapat memeriksa 65.536 byte (64 KB) pertama dari jenis komponen ini untuk indikator keberhasilan atau kegagalan. Aturan ini menerapkan tindakan aturan dan pelabelan untuk permintaan web baru dari sesi klien, berdasarkan respons keberhasilan dan kegagalan dari sumber daya yang dilindungi untuk upaya login terbaru dari sesi klien yang sama. Anda menentukan cara menghitun g keberhasilan dan kegagalan saat Anda mengonfigurasi grup aturan. **Note** AWS WAF hanya mengevaluasi aturan ini di ACL web yang melindungi distribusi Amazon CloudFront . **Note** Ambang batas yang diterapkan aturan ini dapat sedikit berbeda karena latensi. Klien dapat mengirim lebih banyak

Nama aturan	Deskripsi dan label
	upaya login yang gagal daripada yang diizinkan sebelum aturan mulai cocok pada upaya berikutnya. Pemeriksaan ini hanya berlaku ketika permintaan web memiliki token. Token ditambahkan ke permintaan oleh SDK integrasi aplikasi dan oleh tindakan aturan CAPTCHA danChallenge. Untuk informasi selengkapnya, lihat AWS WAF token permintaan web. Tindakan aturan: Block Label: `awswaf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:high` Grup aturan juga menerapkan label terkait berikut ke permintaan, tanpa tindakan terkait apa pun. Semua hitungan adalah untuk jendela 30 menit. `awswaf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:medium` untuk lebih dari 5 permintaan gagal, `awswaf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:low` untuk lebih dari 1 permintaan gagal, `awswaf:managed:aws:atp:aggregate:volumetric:session:successful_login_response:high` untuk lebih dari 10 permintaan yang berhasil, `awswaf:managed:aws:atp:aggregate:volumetric:session:successful_`

Nama aturan	Deskripsi dan label
	`login_response:medium` untuk lebih dari 5 permintaan yang berhasil, dan `awswaf:managed:aws:atp:aggregate:volumetric:session:successful_login_response:low` untuk lebih dari 1 permintaan yang berhasil.

AWS WAF Grup aturan Bot Control

VendorName:`AWS`, Nama:`AWSManagedRulesBotControlRuleSet`, WCU: 50

Grup aturan terkelola Bot Control menyediakan aturan yang mengelola permintaan dari bot. Bot dapat mengkonsumsi sumber daya berlebih, mengubah metrik bisnis, menyebabkan downtime, dan melakukan aktivitas berbahaya.

Tingkat perlindungan

Grup aturan terkelola Bot Control menyediakan dua tingkat perlindungan yang dapat Anda pilih:

- Umum - Mendeteksi berbagai bot pengenal diri, seperti kerangka kerja pengikisan web, mesin pencari, dan browser otomatis. Perlindungan Bot Control pada tingkat ini mengidentifikasi bot umum menggunakan teknik deteksi bot tradisional, seperti analisis data permintaan statis. Aturan memberi label lalu lintas dari bot ini dan memblokir yang tidak dapat mereka verifikasi.
- Ditargetkan - Termasuk perlindungan tingkat umum dan menambahkan deteksi bertarget untuk bot canggih yang tidak mengidentifikasi diri. Perlindungan yang ditargetkan mengurangi aktivitas bot menggunakan kombinasi pembatasan kecepatan dan CAPTCHA dan tantangan browser latar belakang.
  - **`TGT_`**— Aturan yang memberikan perlindungan yang ditargetkan memiliki nama yang dimulai dengan`TGT_`. Semua perlindungan yang ditargetkan menggunakan teknik deteksi seperti interogasi browser, sidik jari, dan heuristik perilaku untuk mengidentifikasi lalu lintas bot yang buruk.
  - **`TGT_ML_`**— Aturan perlindungan yang ditargetkan yang menggunakan pembelajaran mesin memiliki nama yang dimulai dengan`TGT_ML_`. Aturan-aturan ini menggunakan analisis pembelajaran mesin otomatis dari statistik lalu lintas situs web untuk mendeteksi perilaku anomali yang menunjukkan aktivitas bot terdistribusi dan terkoordinasi. AWS WAF menganalisis

statistik tentang lalu lintas situs web Anda seperti stempel waktu, karakteristik browser, dan URL sebelumnya yang dikunjungi, untuk meningkatkan model pembelajaran mesin Kontrol Bot. Kemampuan pembelajaran mesin diaktifkan secara default, tetapi Anda dapat menonaktifkannya dalam konfigurasi grup aturan Anda. Ketika pembelajaran mesin dinonaktifkan, AWS WAF tidak mengevaluasi aturan ini.

Tingkat perlindungan yang ditargetkan dan pernyataan aturan AWS WAF berbasis tarif keduanya memberikan pembatasan tarif. Untuk perbandingan kedua opsi, lihatOpsi untuk membatasi tarif dalam aturan berbasis tarif dan aturan Kontrol Bot yang ditargetkan.

Pertimbangan untuk menggunakan grup aturan ini

Kelompok aturan ini adalah bagian dari perlindungan mitigasi ancaman cerdas di. AWS WAF Untuk informasi, lihat AWS WAF mitigasi ancaman cerdas.

> **Note**
>
> Anda akan dikenakan biaya tambahan saat menggunakan grup aturan terkelola ini. Untuk informasi selengkapnya, silakan lihat Harga AWS WAF.

Untuk menjaga biaya Anda turun dan memastikan Anda mengelola lalu lintas web Anda seperti yang Anda inginkan, gunakan kelompok aturan ini sesuai dengan panduan diPraktik terbaik untuk mitigasi ancaman cerdas.

Kami secara berkala memperbarui model pembelajaran mesin (ML) kami untuk aturan berbasis MP tingkat perlindungan yang ditargetkan, untuk meningkatkan prediksi bot. Aturan berbasis ML memiliki nama yang dimulai dengan. `TGT_ML_` Jika Anda melihat perubahan mendadak dan substansional dalam prediksi bot yang dibuat oleh aturan ini, hubungi kami melalui manajer akun Anda atau buka kasus di AWS Support Center.

Label ditambahkan oleh grup aturan ini

Grup aturan terkelola ini menambahkan label ke permintaan web yang dievaluasi, yang tersedia untuk aturan yang berjalan setelah grup aturan ini di ACL web Anda. AWS WAF juga mencatat label ke CloudWatch metrik Amazon. Untuk informasi umum tentang label dan metrik label, lihat Label pada permintaan web danLabel metrik dan dimensi.

Label token

Grup aturan ini menggunakan manajemen AWS WAF token untuk memeriksa dan memberi label permintaan web sesuai dengan status AWS WAF token mereka. AWS WAF menggunakan token untuk pelacakan dan verifikasi sesi klien.

Untuk informasi tentang token dan manajemen token, lihatAWS WAF token permintaan web.

Untuk informasi tentang komponen label yang dijelaskan di sini, lihatAWS WAF sintaks label dan persyaratan penamaan.

Label sesi klien

Label `awswaf:managed:token:id:`*`identifier`* berisi pengidentifikasi unik yang digunakan manajemen AWS WAF token untuk mengidentifikasi sesi klien. Pengidentifikasi dapat berubah jika klien memperoleh token baru, misalnya setelah membuang token yang digunakannya.

> **Note**
>
> AWS WAF tidak melaporkan CloudWatch metrik Amazon untuk label ini.

Label status token: Awalan namespace label

Label status token melaporkan status token dan tantangan serta informasi CAPTCHA yang dikandungnya.

Setiap label status token dimulai dengan salah satu awalan namespace berikut:

- `awswaf:managed:token:`— Digunakan untuk melaporkan status umum token dan melaporkan status informasi tantangan token.
- `awswaf:managed:captcha:`— Digunakan untuk melaporkan status informasi CAPTCHA token.

Label status token: Nama label

Mengikuti awalan, sisa label memberikan informasi status token terperinci:

- `accepted`— Token permintaan hadir dan berisi yang berikut:
  - Tantangan yang valid atau solusi CAPTCHA.

- Tantangan yang belum kedaluwarsa atau cap waktu CAPTCHA.
- Spesifikasi domain yang valid untuk web ACL.

Contoh: Label `awswaf:managed:token:accepted` menunjukkan bahwa token permintaan web memiliki solusi tantangan yang valid, stempel waktu tantangan yang belum kedaluwarsa, dan domain yang valid.

- `rejected`— Token permintaan ada tetapi tidak memenuhi kriteria penerimaan.

  Seiring dengan label yang ditolak, manajemen token menambahkan namespace dan nama label khusus untuk menunjukkan alasannya.

  - `rejected:not_solved`— Token tidak memiliki tantangan atau solusi CAPTCHA.
  - `rejected:expired`— Tantangan token atau cap waktu CAPTCHA telah kedaluwarsa, sesuai dengan waktu kekebalan token ACL web Anda yang dikonfigurasi.
  - `rejected:domain_mismatch`— Domain token tidak cocok untuk konfigurasi domain token ACL web Anda.
  - `rejected:invalid`— AWS WAF tidak bisa membaca token yang ditunjukkan.

  Contoh: Label `awswaf:managed:captcha:rejected` dan `awswaf:managed:captcha:rejected:expired` menunjukkan bahwa permintaan ditolak karena cap waktu CAPTCHA dalam token telah melebihi waktu kekebalan token CAPTCHA yang dikonfigurasi di ACL web.

- `absent`— Permintaan tidak memiliki token atau manajer token tidak dapat membacanya.

  Contoh: Label `awswaf:managed:captcha:absent` menunjukkan bahwa permintaan tidak memiliki token.

Label Kontrol Bot

Grup aturan terkelola Bot Control menghasilkan label dengan awalan namespace `awswaf:managed:aws:bot-control:` diikuti oleh namespace kustom dan nama label. Grup aturan dapat menambahkan lebih dari satu label ke permintaan.

Setiap label mencerminkan temuan aturan Kontrol Bot:

- `awswaf:managed:aws:bot-control:bot:`— Informasi tentang bot yang terkait dengan permintaan.

- `awswaf:managed:aws:bot-control:bot:name:<name>`— Nama bot, jika tersedia, misalnya, ruang nama khususbot:name:slurp,bot:name:googlebot, dan. bot:name:pocket_parser
- `awswaf:managed:aws:bot-control:bot:category:<category>`— Kategori bot, seperti yang didefinisikan oleh AWS WAF, misalnya, bot:category:search_engine danbot:category:content_fetcher.
- `awswaf:managed:aws:bot-control:bot:organization:<organization>`— Penerbit bot, misalnya,bot:organization:google.
- `awswaf:managed:aws:bot-control:bot:verified`— Digunakan untuk menunjukkan bot yang mengidentifikasi dirinya sendiri dan bahwa Bot Control telah dapat memverifikasi. Ini digunakan untuk bot umum yang diinginkan, dan dapat berguna bila dikombinasikan dengan label kategori seperti bot:category:search_engine atau label nama sepertibot:name:googlebot.

  > **Note**
  >
  > Bot Control menggunakan alamat IP dari asal permintaan web untuk membantu menentukan apakah bot diverifikasi. Anda tidak dapat mengonfigurasinya untuk menggunakan konfigurasi IP AWS WAF yang diteruskan, untuk memeriksa sumber alamat IP yang berbeda. Jika Anda telah memverifikasi bot yang merutekan melalui proxy atau penyeimbang beban, Anda dapat menambahkan aturan yang berjalan sebelum grup aturan Kontrol Bot untuk membantu hal ini. Konfigurasikan aturan baru Anda untuk menggunakan alamat IP yang diteruskan dan secara eksplisit mengizinkan permintaan dari bot yang diverifikasi. Untuk informasi tentang menggunakan alamat IP yang diteruskan, lihat. Alamat IP yang diteruskan

- `awswaf:managed:aws:bot-control:bot:user_triggered:verified`— Digunakan untuk menunjukkan bot yang mirip dengan bot terverifikasi, tetapi itu mungkin langsung dipanggil oleh pengguna akhir. Kategori bot ini diperlakukan oleh aturan Kontrol Bot seperti bot yang tidak diverifikasi.
- `awswaf:managed:aws:bot-control:bot:developer_platform:verified`— Digunakan untuk menunjukkan bot yang mirip dengan bot terverifikasi, tetapi digunakan oleh platform pengembang untuk skrip, misalnya Google Apps Script. Kategori bot ini diperlakukan oleh aturan Kontrol Bot seperti bot yang tidak diverifikasi.
- `awswaf:managed:aws:bot-control:bot:unverified`— Digunakan untuk menunjukkan bot yang mengidentifikasi dirinya sendiri, sehingga dapat diberi nama dan dikategorikan, tetapi

itu tidak mempublikasikan informasi yang dapat digunakan untuk memverifikasi identitasnya secara independen. Jenis tanda tangan bot ini dapat dipalsukan, dan diperlakukan sebagai tidak diverifikasi.

- `awswaf:managed:aws:bot-control:targeted:<additional-details>` — Digunakan untuk label yang khusus untuk perlindungan yang ditargetkan Bot Control.
- `awswaf:managed:aws:bot-control:signal:<signal-details>`dan `awswaf:managed:aws:bot-control:targeted:signal:<signal-details>` — Digunakan untuk memberikan informasi tambahan tentang permintaan dalam beberapa situasi.

  Berikut ini adalah contoh label sinyal. Ini bukan daftar lengkap:

  - `awswaf:managed:aws:bot-control:targeted:signal:browser_automation_extension`— Menunjukkan deteksi ekstensi browser yang membantu dalam otomatisasi, seperti Selenium IDE.

    Label ini ditambahkan setiap kali pengguna memiliki jenis ekstensi yang diinstal, bahkan jika mereka tidak aktif menggunakannya. Jika Anda menerapkan aturan pencocokan label untuk ini, perhatikan kemungkinan positif palsu ini dalam logika aturan dan setelan tindakan Anda. Misalnya, Anda mungkin menggunakan CAPTCHA tindakan sebagai gantinya Block atau Anda dapat menggabungkan kecocokan label ini dengan kecocokan label lainnya, untuk meningkatkan keyakinan Anda bahwa otomatisasi sedang digunakan.
  - `awswaf:managed:aws:bot-control:signal:automated_browser`— Menunjukkan bahwa permintaan berisi indikator bahwa browser klien mungkin otomatis.
  - `awswaf:managed:aws:bot-control:targeted:signal:automated_browser`— Menunjukkan bahwa AWS WAF token permintaan berisi indikator bahwa browser klien mungkin otomatis.

Anda dapat mengambil semua label untuk grup aturan melalui API dengan memanggil`DescribeManagedRuleGroup`. Label tercantum di `AvailableLabels` properti dalam tanggapan.

Grup aturan terkelola Bot Control menerapkan label ke satu set bot yang dapat diverifikasi yang biasanya diizinkan. Grup aturan tidak memblokir bot terverifikasi ini. Jika mau, Anda dapat memblokirnya, atau subset dari mereka dengan menulis aturan kustom yang menggunakan label yang diterapkan oleh grup aturan terkelola Bot Control. Untuk informasi lebih lanjut tentang ini dan contoh, lihatAWS WAF Kontrol Bot.

Daftar aturan Bot Control

Bagian ini mencantumkan aturan Kontrol Bot.

> **Note**
>
> Informasi yang kami publikasikan untuk aturan dalam kelompok aturan Aturan AWS Terkelola dimaksudkan untuk memberi Anda informasi yang cukup untuk menggunakan aturan sementara tidak memberikan informasi yang dapat digunakan oleh pelaku jahat untuk menghindari aturan. Jika Anda memerlukan informasi lebih lanjut daripada yang Anda temukan dalam dokumentasi ini, hubungi AWS Support Pusat.

Nama aturan	Deskripsi
`CategoryAdvertising`	Memeriksa bot yang digunakan untuk tujuan periklanan. Misalnya, Anda mungkin menggunakan layanan iklan pihak ketiga yang perlu mengakses situs web Anda secara terprogram. Tindakan aturan, hanya diterapkan pada bot yang tidak diverifikasi: Block Label: `awswaf:managed:aws:bot-control:bot:category:advertising` Untuk bot terverifikasi, grup aturan tidak mengambil tindakan, tetapi menambahkan pelabelan aturan ditambah label. `awswaf:managed:aws:bot-control:bot:verified`
`CategoryArchiver`	Memeriksa bot yang digunakan untuk tujuan pengarsipan. Bot ini merayapi web dan menangkap konten untuk tujuan membuat arsip.

Nama aturan	Deskripsi
	Tindakan aturan, hanya diterapkan pada bot yang tidak diverifikasi: Block Label: `awswaf:managed:aws:bot-control:bot:category:archiver` Untuk bot terverifikasi, grup aturan tidak mengambil tindakan, tetapi menambahkan pelabelan aturan ditambah label. `awswaf:managed:aws:bot-control:bot:verified`
`CategoryContentFetcher`	Memeriksa bot yang mengunjungi situs web aplikasi atas nama pengguna, untuk mengambil konten seperti umpan RSS atau untuk memverifikasi atau memvalidasi konten Anda. Tindakan aturan, hanya diterapkan pada bot yang tidak diverifikasi: Block Label: `awswaf:managed:aws:bot-control:bot:category:content_fetcher` Untuk bot terverifikasi, grup aturan tidak mengambil tindakan, tetapi menambahkan pelabelan aturan ditambah label. `awswaf:managed:aws:bot-control:bot:verified`

Nama aturan	Deskripsi
`CategoryEmailClient`	Periksa bot yang memeriksa tautan dalam email yang mengarah ke situs web aplikasi. Ini dapat mencakup bot yang dijalankan oleh bisnis dan penyedia email, untuk memverifikasi tautan dalam email dan menandai email yang mencurigakan. Tindakan aturan, hanya diterapkan pada bot yang tidak diverifikasi: Block Label: `awswaf:managed:aws:bot-control:bot:category:email_client` Untuk bot terverifikasi, grup aturan tidak mengambil tindakan, tetapi menambahkan pelabelan aturan ditambah label. `awswaf:managed:aws:bot-control:bot:verified`
`CategoryHttpLibrary`	Memeriksa permintaan yang dihasilkan oleh bot dari perpustakaan HTTP dari berbagai bahasa pemrograman. Ini mungkin termasuk permintaan API yang Anda pilih untuk diizinkan atau dipantau. Tindakan aturan, hanya diterapkan pada bot yang tidak diverifikasi: Block Label: `awswaf:managed:aws:bot-control:bot:category:http_library` Untuk bot terverifikasi, grup aturan tidak mengambil tindakan, tetapi menambahkan pelabelan aturan ditambah label. `awswaf:managed:aws:bot-control:bot:verified`

Nama aturan	Deskripsi
`CategoryLinkChecker`	Memeriksa bot yang memeriksa tautan yang rusak. Tindakan aturan, hanya diterapkan pada bot yang tidak diverifikasi: Block Label: `awswaf:managed:aws:bot-control:bot:category:link_checker` Untuk bot terverifikasi, grup aturan tidak mengambil tindakan, tetapi menambahkan pelabelan aturan ditambah label. `awswaf:managed:aws:bot-control:bot:verified`
`CategoryMiscellaneous`	Memeriksa bot lain-lain yang tidak cocok dengan kategori lain. Tindakan aturan, hanya diterapkan pada bot yang tidak diverifikasi: Block Label: `awswaf:managed:aws:bot-control:bot:category:miscellaneous` Untuk bot terverifikasi, grup aturan tidak mengambil tindakan, tetapi menambahkan pelabelan aturan ditambah label. `awswaf:managed:aws:bot-control:bot:verified`

Nama aturan	Deskripsi
`CategoryMonitoring`	Memeriksa bot yang digunakan untuk tujuan pemantauan. Misalnya, Anda mungkin menggunakan layanan pemantauan bot yang secara berkala melakukan ping ke situs web aplikasi Anda untuk memantau hal-hal seperti kinerja dan waktu aktif. Tindakan aturan, hanya diterapkan pada bot yang tidak diverifikasi: Block Label: `awswaf:managed:aws:bot-control:bot:category:monitoring` Untuk bot terverifikasi, grup aturan tidak mengambil tindakan, tetapi menambahkan pelabelan aturan ditambah label. `awswaf:managed:aws:bot-control:bot:verified`
`CategoryScrapingFramework`	Memeriksa bot dari kerangka kerja pengikisan web, yang digunakan untuk mengotomatiskan perayapan dan mengekstrak konten dari situs web. Tindakan aturan, hanya diterapkan pada bot yang tidak diverifikasi: Block Label: `awswaf:managed:aws:bot-control:bot:category:scraping_framework` Untuk bot terverifikasi, grup aturan tidak mengambil tindakan, tetapi menambahkan pelabelan aturan ditambah label. `awswaf:managed:aws:bot-control:bot:verified`

Nama aturan	Deskripsi
`CategorySearchEngine`	Memeriksa bot mesin pencari, yang merayapi situs web untuk mengindeks konten dan membuat informasi tersedia untuk hasil mesin pencari. Tindakan aturan, hanya diterapkan pada bot yang tidak diverifikasi: Block Label: `awswaf:managed:aws:bot-control:bot:category:search_engine` Untuk bot terverifikasi, grup aturan tidak mengambil tindakan, tetapi menambahkan pelabelan aturan ditambah label. `awswaf:managed:aws:bot-control:bot:verified`
`CategorySecurity`	Memeriksa bot yang memindai aplikasi web untuk kerentanan atau yang melakukan audit keamanan. Misalnya, Anda mungkin menggunakan vendor keamanan pihak ketiga yang memindai, memantau, atau mengaudit keamanan aplikasi web Anda. Tindakan aturan, hanya diterapkan pada bot yang tidak diverifikasi: Block Label: `awswaf:managed:aws:bot-control:bot:category:security` Untuk bot terverifikasi, grup aturan tidak mengambil tindakan, tetapi menambahkan pelabelan aturan ditambah label. `awswaf:managed:aws:bot-control:bot:verified`

Nama aturan	Deskripsi
`CategorySeo`	Memeriksa bot yang digunakan untuk optimasi mesin pencari. Misalnya, Anda mungkin menggunakan alat mesin pencari yang merayapi situs Anda untuk membantu Anda meningkatkan peringkat mesin pencari Anda. Tindakan aturan, hanya diterapkan pada bot yang tidak diverifikasi: Block Label: `awswaf:managed:aws:bot-control:bot:category:seo` Untuk bot terverifikasi, grup aturan tidak mengambil tindakan, tetapi menambahkan pelabelan aturan ditambah label. `awswaf:managed:aws:bot-control:bot:verified`
`CategorySocialMedia`	Periksa bot yang digunakan oleh platform media sosial untuk memberikan ringkasan konten saat pengguna membagikan konten Anda. Tindakan aturan, hanya diterapkan pada bot yang tidak diverifikasi: Block Label: `awswaf:managed:aws:bot-control:bot:category:social_media` Untuk bot terverifikasi, grup aturan tidak mengambil tindakan, tetapi menambahkan pelabelan aturan ditambah label. `awswaf:managed:aws:bot-control:bot:verified`

Nama aturan	Deskripsi
`CategoryAI`	Memeriksa bot kecerdasan buatan (AI). Tindakan aturan: Block Label: `awswaf:managed:aws:bot-control:bot:category:ai`
`SignalAutomatedBrowser`	Memeriksa permintaan indikator bahwa browser klien mungkin otomatis. Browser otomatis dapat digunakan untuk pengujian atau pengikisan. Misalnya, Anda dapat menggunakan jenis browser ini untuk memantau atau memverifikasi situs web aplikasi Anda. Tindakan aturan: Block Label: `awswaf:managed:aws:bot-control:signal:automated_browser`
`SignalKnownBotDataCenter`	Memeriksa indikator pusat data yang biasanya digunakan oleh bot. Tindakan aturan: Block Label: `awswaf:managed:aws:bot-control:signal:known_bot_data_center`

Nama aturan	Deskripsi
`SignalNonBrowserUserAgent`	Memeriksa string agen pengguna yang tampaknya tidak berasal dari browser web. Kategori ini dapat mencakup permintaan API. Tindakan aturan: Block Label: `awswaf:managed:aws:bot-control:signal:non_browser_user_agent`

Nama aturan	Deskripsi
`TGT_VolumetricIpTokenAbsent`	Memeriksa 5 atau lebih permintaan dari klien dalam 5 menit terakhir yang tidak menyertakan token tantangan yang valid. Untuk informasi tentang token, lihatAWS WAF token permintaan web. **Note** Aturan ini mungkin cocok dengan permintaan yang memiliki token jika permintaan dari klien yang sama baru-baru ini kehilangan token. Ambang batas yang diterapkan aturan ini dapat sedikit berbeda karena latensi. Aturan ini menangani token yang hilang secara berbeda dari pelabelan token:`awswaf:managed:token:absent` . Pelabelan token memberi label permintaan individual yang tidak memiliki token. Aturan ini mempertahankan jumlah permintaan yang kehilangan token mereka untuk setiap IP klien, dan cocok dengan klien yang melampaui batas. Tindakan aturan, diterapkan hanya untuk klien yang tidak diverifikasi bot: Challenge Label: `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:ip:token_absent` Untuk bot terverifikasi, grup aturan tidak mengambil tindakan, tetapi menambahkan pelabelan aturan ditambah label. `awswaf:ma`

Nama aturan	Deskripsi
	`naged:aws:bot-control:bot:verified`

Nama aturan	Deskripsi
`TGT_VolumetricSession`	Memeriksa jumlah permintaan yang sangat tinggi dari sesi klien dalam jendela 5 menit. Evaluasi ini didasarkan pada perbandingan dengan garis dasar volumetrik standar yang AWS WAF mempertahankan penggunaan pola lalu lintas historis. Pemeriksaan ini hanya berlaku ketika permintaan web memiliki token. Token ditambahkan ke permintaan oleh SDK integrasi aplikasi dan oleh tindakan aturan CAPTCHA danChallenge. Untuk informasi selengkapnya, lihat AWS WAF token permintaan web. **Note** Aturan ini dapat memakan waktu 5 menit untuk mulai berlaku setelah Anda mengaktifkannya. Bot Control mengidentifikasi perilaku anomali dalam lalu lintas web Anda dengan membandingkan lalu lintas saat ini dengan garis dasar lalu lintas yang dihitung. AWS WAF Tindakan aturan, diterapkan hanya untuk klien yang tidak diverifikasi bot: CAPTCHA Label: `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:high`

Nama aturan	Deskripsi
	Grup aturan menerapkan label berikut ke permintaan volume menengah dan volume rendah yang berada di atas ambang minimum. Untuk level ini, aturan tidak mengambil tindakan, terlepas dari apakah klien diverifikasi: `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:medium` dan`awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:low` . Untuk bot terverifikasi, grup aturan tidak mengambil tindakan, tetapi menambahkan pelabelan aturan ditambah label. `awswaf:managed:aws:bot-control:bot:verified`

Nama aturan	Deskripsi
`TGT_SignalAutomatedBrowser`	Memeriksa token permintaan untuk indikator bahwa browser klien mungkin otomatis. Untuk informasi selengkapnya, lihat AWS WAF karakteristik token. Pemeriksaan ini hanya berlaku ketika permintaan web memiliki token. Token ditambahkan ke permintaan oleh SDK integrasi aplikasi dan oleh tindakan aturan CAPTCHA danChallenge. Untuk informasi selengkapnya, lihat AWS WAF token permintaan web. Tindakan aturan, diterapkan hanya untuk klien yang tidak diverifikasi bot: CAPTCHA Label: `awswaf:managed:aws:bot-control:targeted:signal:automated_browser` Untuk bot terverifikasi, grup aturan tidak mengambil tindakan, tetapi menambahkan pelabelan aturan ditambah label. `awswaf:managed:aws:bot-control:bot:verified`

Nama aturan	Deskripsi
`TGT_SignalBrowserInconsistency`	Memeriksa data interogasi browser yang tidak konsisten. Untuk informasi selengkapnya, lihat AWS WAF karakteristik token. Pemeriksaan ini hanya berlaku ketika permintaan web memiliki token. Token ditambahkan ke permintaan oleh SDK integrasi aplikasi dan oleh tindakan aturan CAPTCHA danChallenge. Untuk informasi selengkapnya, lihat AWS WAF token permintaan web. Tindakan aturan, diterapkan hanya untuk klien yang tidak diverifikasi bot: CAPTCHA Label: `awswaf:managed:aws:bot-control:targeted:signal:browser_inconsistency` Untuk bot terverifikasi, grup aturan tidak mengambil tindakan, tetapi menambahkan pelabelan aturan ditambah label. `awswaf:managed:aws:bot-control:bot:verified`

Nama aturan	Deskripsi
`TGT_TokenReuseIp`	Memeriksa penggunaan token tunggal di antara lebih dari 5 alamat IP yang berbeda. **Note** Ambang batas yang diterapkan aturan ini dapat sedikit berbeda karena latensi. Beberapa permintaan mungkin berhasil melewati batas sebelum tindakan aturan diterapkan. Tindakan aturan: Count Label: `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:token_reuse:ip`

Nama aturan	Deskripsi
`TGT_ML_CoordinatedActivityMedium` dan `TGT_ML_CoordinatedActivityHigh`	Periksa perilaku anomali yang konsisten dengan aktivitas bot terdistribusi dan terkoordinasi. Tingkat aturan menunjukkan tingkat kepercayaan bahwa sekelompok permintaan adalah peserta dalam serangan terkoordinasi. **Note** Aturan ini hanya berjalan jika grup aturan dikonfigurasi untuk menggunakan pembelajaran mesin (ML). Untuk informasi tentang mengonfigurasi pilihan ini, lihat Menambahkan grup aturan terkelola AWS WAF Bot Control ke ACL web Anda. AWS WAF melakukan inspeksi ini melalui analisis pembelajaran mesin statistik lalu lintas situs web. AWS WAF menganalisis lalu lintas web setiap beberapa menit dan mengoptimalkan analisis untuk mendeteksi bot intensitas rendah dan durasi panjang yang didistribusikan di banyak alamat IP. Aturan-aturan ini mungkin cocok dengan sejumlah kecil permintaan sebelum menentukan bahwa serangan terkoordinasi tidak sedang berlangsung. Jadi jika Anda hanya melihat satu atau dua kecocokan, hasilnya mungkin positif palsu. Jika Anda melihat banyak pertandingan keluar dari aturan ini, maka Anda mungkin mengalami serangan terkoordinasi.

Nama aturan	Deskripsi
	Note Aturan ini dapat memakan waktu hingga 24 jam untuk mulai berlaku setelah Anda mengaktifkan aturan yang ditargetkan Bot Control dengan opsi ML. Bot Control mengidentifikasi perilaku anomali dalam lalu lintas web Anda dengan membandingkan lalu lintas saat ini dengan garis dasar lalu lintas yang telah dihitung. AWS WAF AWS WAF hanya menghitung baseline saat Anda menggunakan aturan yang ditargetkan Bot Control dengan opsi ML, dan itu bisa memakan waktu hingga 24 jam untuk menetapkan baseline yang bermakna. Kami secara berkala memperbarui model pembelajaran mesin kami untuk aturan ini, untuk meningkatkan prediksi bot. Jika Anda melihat perubahan mendadak dan substansi onal dalam prediksi bot yang dibuat oleh aturan ini, hubungi manajer akun Anda atau buka kasing di AWS Support Center. Tindakan aturan, diterapkan hanya untuk klien yang tidak diverifikasi bot: • Sedang: Count • Tinggi: Count

Nama aturan	Deskripsi
	Label: `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:medium` dan `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:high` Untuk bot terverifikasi, grup aturan tidak mengambil tindakan, tetapi menambahkan pelabelan aturan ditambah label. `awswaf:managed:aws:bot-control:bot:verified` Grup aturan juga menambahkan label `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:low` untuk menunjukkan tingkat kepercayaan rendah, tetapi tidak menerapkan aturan apa pun atau mengambil tindakan apa pun untuk permintaan ini.

Penerapan untuk grup aturan Aturan Terkelola berversi AWS

AWS menerapkan perubahan pada grup aturan Aturan AWS Terkelola berversi dalam tiga penerapan standar: kandidat rilis, versi statis, dan versi default. Selain itu, AWS terkadang perlu merilis penerapan pengecualian atau mengembalikan penerapan versi default.

> **Note**
>
> Bagian ini hanya berlaku untuk grup aturan Aturan AWS Terkelola yang berversi. Satu-satunya grup aturan yang tidak berversi adalah grup aturan reputasi IP.

Topik

- Pemberitahuan untuk penerapan grup aturan Aturan AWS Terkelola

- Ikhtisar penerapan standar untuk AWS Aturan Terkelola
- Status versi khas untuk Aturan AWS Terkelola
- Melepaskan penerapan kandidat untuk AWS Aturan Terkelola
- Penerapan versi statis untuk AWS Aturan Terkelola
- Penerapan versi default untuk AWS Aturan Terkelola
- Penerapan pengecualian untuk AWS Aturan Terkelola
- Rollback penerapan default untuk Aturan Terkelola AWS

Pemberitahuan untuk penerapan grup aturan Aturan AWS Terkelola

Grup aturan Aturan AWS Terkelola berversi semuanya menyediakan pemberitahuan pembaruan SNS untuk penerapan dan semuanya menggunakan topik SNS yang sama Nama Sumber Daya Amazon (ARN). Satu-satunya grup aturan yang tidak berversi adalah grup aturan reputasi IP.

Untuk penerapan yang memengaruhi perlindungan Anda, seperti perubahan pada versi default, AWS berikan notifikasi SNS untuk memberi tahu Anda tentang penerapan yang direncanakan dan memberi tahu Anda kapan penerapan dimulai. Untuk penerapan yang tidak memengaruhi perlindungan Anda, seperti kandidat rilis dan penerapan versi statis, AWS mungkin akan memberi tahu Anda setelah penerapan dimulai atau bahkan setelah penerapan selesai. Pada penyelesaian penerapan versi statis baru, AWS perbarui panduan ini, di changelog di AWS Aturan terkelola changelog dan di halaman riwayat dokumen di. Riwayat dokumen

Untuk menerima semua pembaruan yang AWS menyediakan grup aturan Aturan AWS Terkelola, berlangganan umpan RSS dari halaman HTML mana pun dalam panduan ini, dan berlangganan topik SNS untuk grup aturan Aturan AWS Terkelola. Untuk informasi tentang berlangganan notifikasi SNS, lihat. Mendapatkan pemberitahuan tentang versi baru dan pembaruan ke grup aturan terkelola

Isi notifikasi SNS

Bidang di notifikasi Amazon SNS selalu menyertakan Subjek, Pesan, dan. MessageAttributes Bidang tambahan bergantung pada jenis pesan dan grup aturan terkelola untuk notifikasi tersebut. Berikut ini menunjukkan contoh daftar pemberitahuan untuk`AWSManagedRulesCommonRuleSet`.

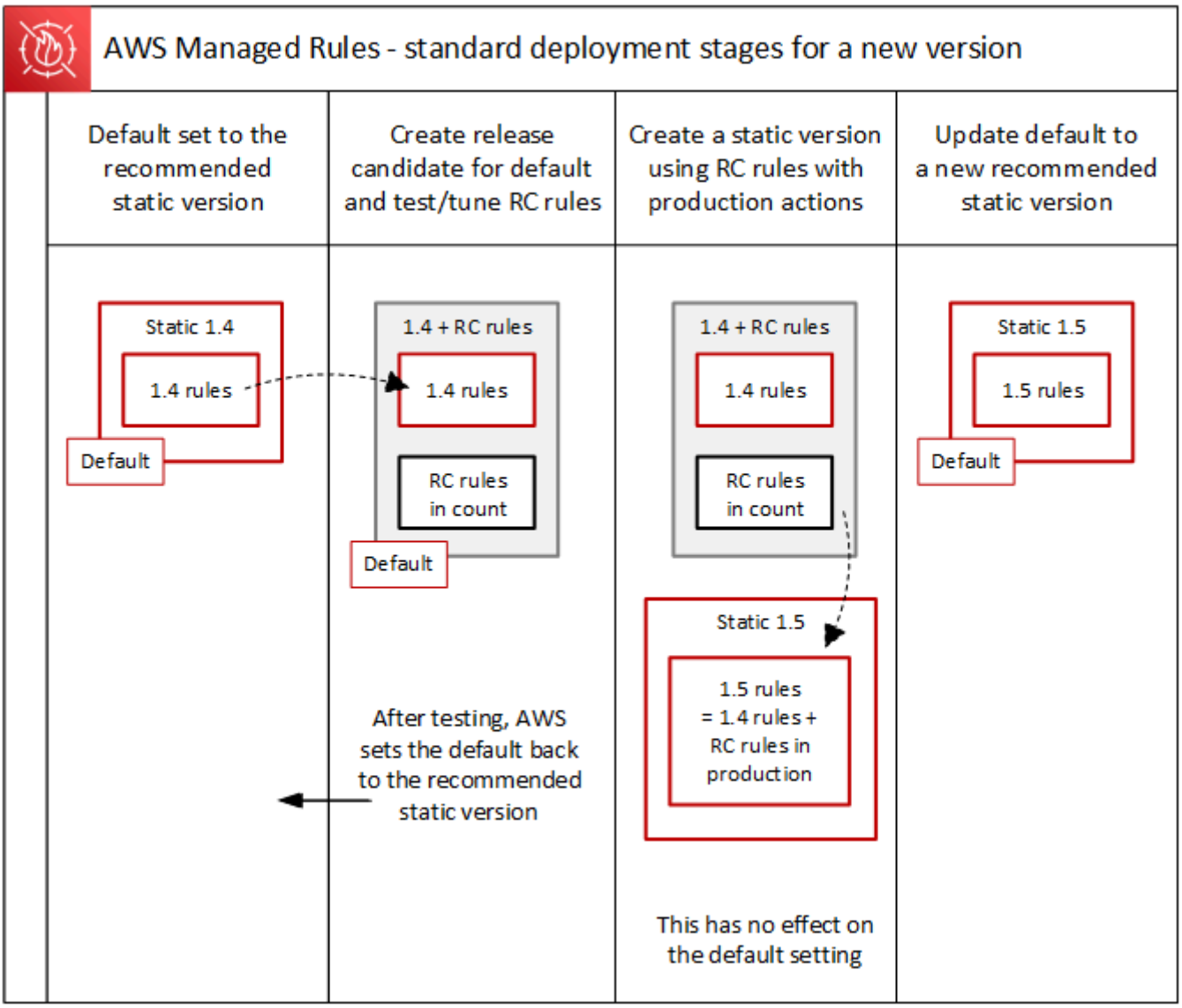
```
{
    "Type": "Notification",
    "MessageId": "4286b830-a463-5e61-bd15-e1ae72303868",
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:MyTopic",
```

```
    "Subject": "New version available for rule group AWSManagedRulesCommonRuleSet",
    "Message": "Welcome to AWSManagedRulesCommonRuleSet version 1.5! We've updated
 the regex specification in this version to improve protection coverage, adding
 protections against insecure deserialization. For details about this change, see
 http://updatedPublicDocs.html. Look for more exciting updates in the future! ",
    "Timestamp": "2021-08-24T11:12:19.810Z",
    "SignatureVersion": "1",
    "Signature": "EXAMPLEHXgJm...",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-
f3ecfb7224c7233fe7bb5f59f96de52f.pem",
    "SubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=ConfirmSubscription&TopicArn=arn:aws:sns:us-
west-2:123456789012:MyTopic&Token=2336412f37...",
    "MessageAttributes": {
        "major_version": {
            "Type": "String",
            "Value": "v1"
        },
        "managed_rule_group": {
            "Type": "String",
            "Value": "AWSManagedRulesCommonRuleSet"
        }
    }
}
```

Ikhtisar penerapan standar untuk AWS Aturan Terkelola

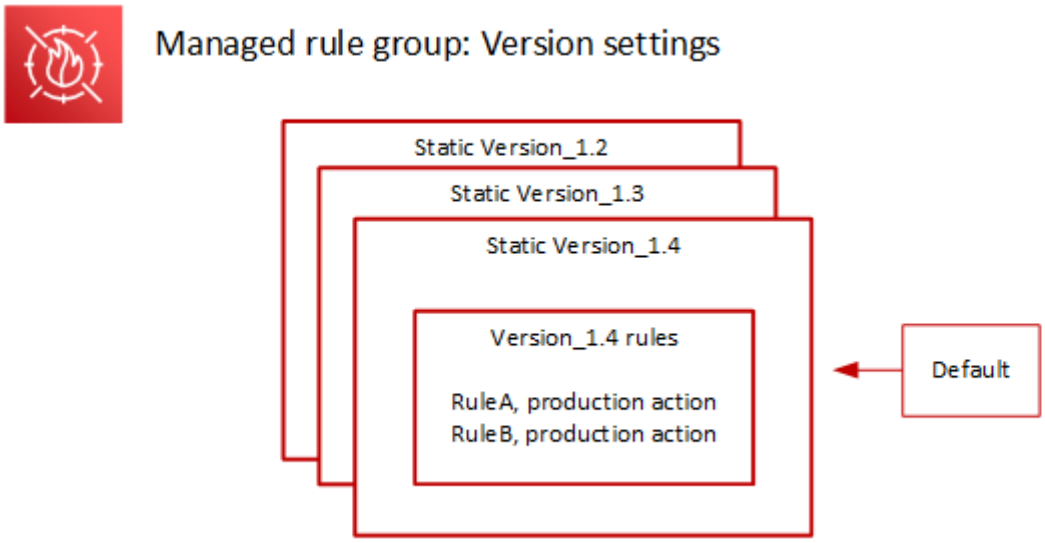
AWS meluncurkan fungsionalitas Aturan AWS Terkelola baru menggunakan tiga tahap penerapan standar: kandidat rilis, versi statis, dan versi default.

Diagram berikut menggambarkan penerapan standar ini. Masing-masing dijelaskan secara lebih rinci di bagian berikutnya.



Status versi khas untuk Aturan AWS Terkelola

Biasanya, grup aturan terkelola berversi memiliki sejumlah versi statis yang belum kedaluwarsa, dan versi default menunjuk ke versi statis yang merekomendasikan. AWS Gambar berikut menunjukkan contoh set tipikal versi statis dan pengaturan versi default.



Tindakan produksi untuk sebagian besar aturan dalam versi statis adalahBlock, tetapi mungkin diatur ke sesuatu yang berbeda. Untuk informasi rinci tentang setelan tindakan aturan, lihat daftar aturan untuk setiap grup aturan diAWS Daftar grup aturan Aturan Terkelola.

Melepaskan penerapan kandidat untuk AWS Aturan Terkelola

Ketika AWS ada serangkaian perubahan aturan kandidat untuk grup aturan terkelola, itu menguji mereka dalam penerapan kandidat rilis sementara. AWS mengevaluasi aturan kandidat dalam mode hitungan terhadap lalu lintas produksi, dan melakukan kegiatan penyetelan akhir, termasuk mengurangi positif palsu. AWS tes merilis aturan kandidat dengan cara ini untuk semua pelanggan yang menggunakan versi default grup aturan. Penerapan kandidat rilis tidak berlaku untuk pelanggan yang menggunakan versi statis grup aturan.

Jika Anda menggunakan versi default, penerapan kandidat rilis tidak akan mengubah cara lalu lintas web Anda dikelola oleh grup aturan. Anda mungkin memperhatikan hal berikut saat aturan kandidat sedang diuji:

- Nama versi default berubah dari `Default (using Version_X.Y)` menjadi`Default (using Version_X.Y_PLUS_RC_COUNT)`.
- Metrik hitungan tambahan di Amazon CloudWatch dengan `RC_COUNT` namanya. Ini dihasilkan oleh aturan kandidat rilis.

AWS menguji kandidat rilis selama sekitar satu minggu, lalu menghapusnya dan mengatur ulang versi default ke versi statis yang direkomendasikan saat ini.

AWS melakukan langkah-langkah berikut untuk penerapan kandidat rilis:

1. Buat kandidat rilis - AWS menambahkan kandidat rilis berdasarkan versi statis yang direkomendasikan saat ini, yang merupakan versi yang ditunjuk default.

   Nama kandidat rilis adalah nama versi statis yang ditambahkan. `_PLUS_RC_COUNT` Misalnya, jika versi statis yang direkomendasikan saat ini adalah`Version_2.1`, maka kandidat rilis akan diberi nama`Version_2.1_PLUS_RC_COUNT`.

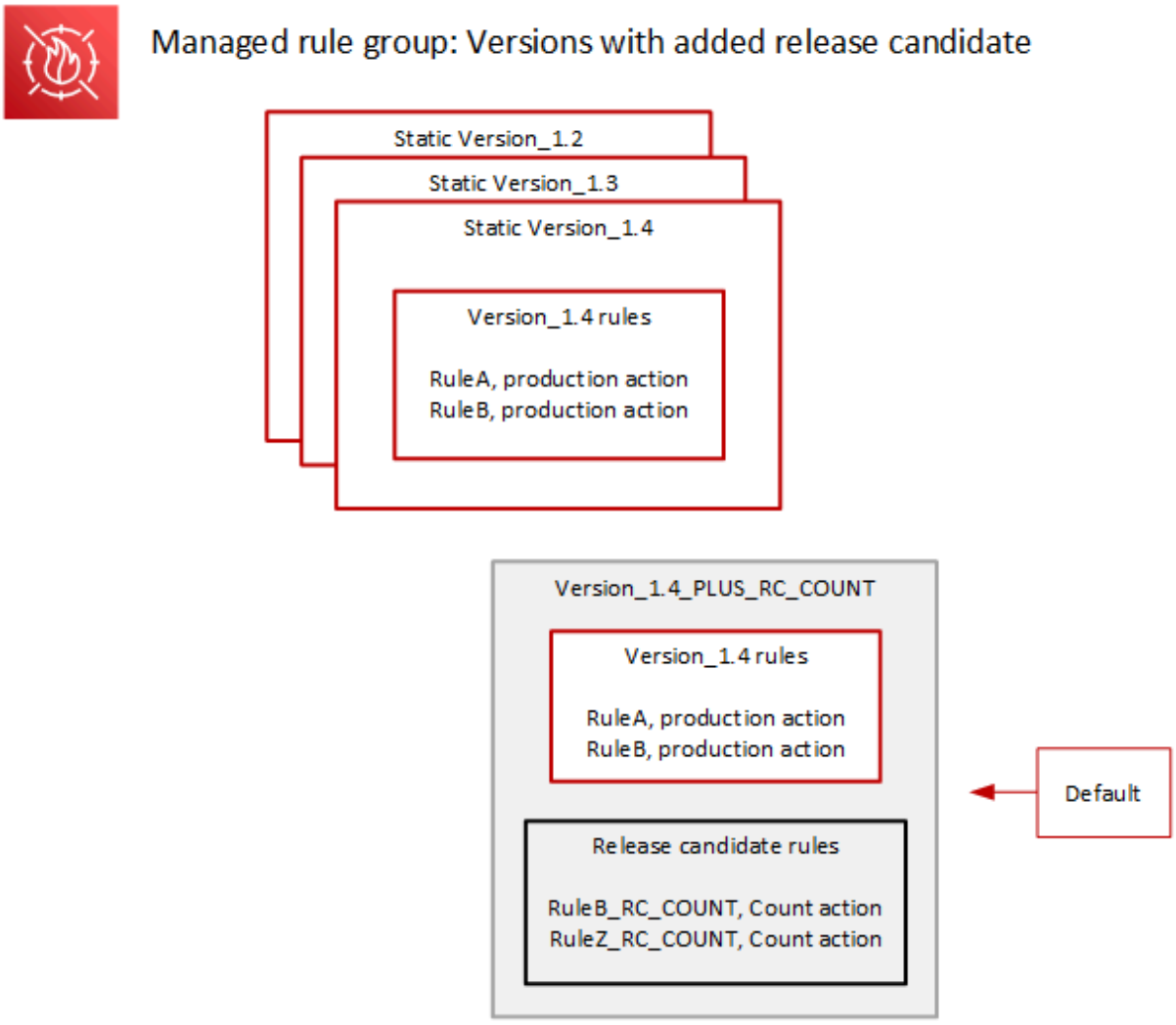
   Kandidat rilis berisi aturan berikut:

   - Aturan disalin persis dari versi statis yang direkomendasikan saat ini, tanpa perubahan pada konfigurasi aturan.
   - Kandidat aturan baru dengan tindakan aturan diatur ke Count dan dengan nama yang diakhiri dengan`_RC_COUNT`.

     Sebagian besar aturan kandidat memberikan perbaikan yang diusulkan untuk aturan yang sudah ada dalam kelompok aturan. Nama untuk masing-masing aturan ini adalah nama aturan yang ada yang `_RC_COUNT` ditambahkan.
2. Setel versi default ke kandidat rilis dan uji — AWS tetapkan versi default untuk menunjuk ke kandidat rilis baru, untuk melakukan pengujian terhadap lalu lintas produksi Anda. Pengujian biasanya memakan waktu sekitar satu minggu.

   Anda akan melihat perubahan nama versi default dari yang hanya menunjukkan versi statis, seperti`Default (using Version_1.4)`, ke yang menunjukkan versi statis ditambah aturan kandidat rilis, seperti`Default (using Version_1.4_PLUS_RC_COUNT)`. Skema penamaan ini memungkinkan Anda mengidentifikasi versi statis mana yang Anda gunakan untuk mengelola lalu lintas web Anda.

   Diagram berikut menunjukkan keadaan versi grup aturan contoh pada titik ini.



Aturan kandidat rilis selalu dikonfigurasi dengan Count tindakan, sehingga aturan tersebut tidak mengubah cara grup aturan mengelola lalu lintas web.

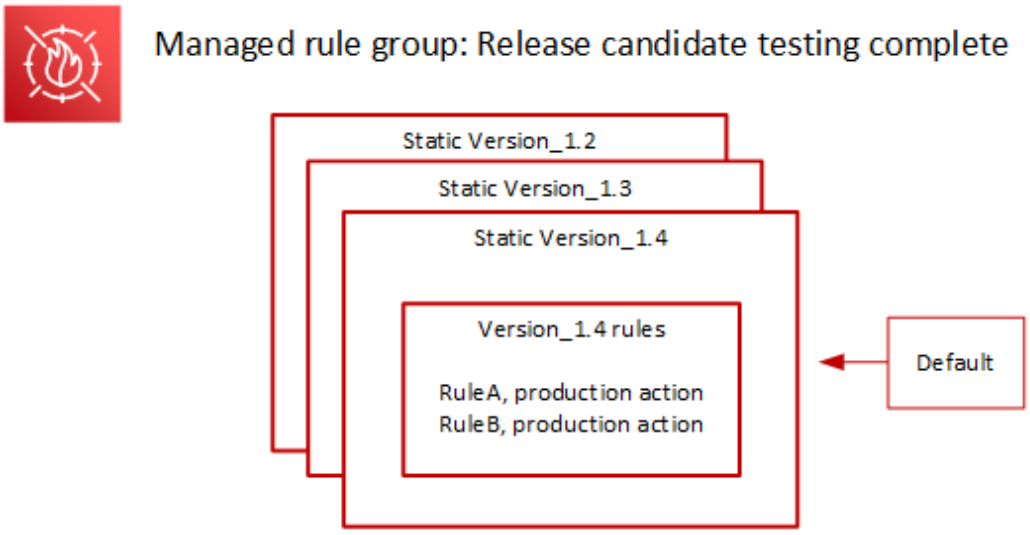
Aturan kandidat rilis menghasilkan metrik CloudWatch hitungan Amazon yang AWS digunakan untuk memverifikasi perilaku dan mengidentifikasi positif palsu. AWS membuat penyesuaian sesuai kebutuhan, untuk menyesuaikan perilaku aturan penghitungan kandidat rilis.

Versi kandidat rilis bukan versi statis, dan tidak tersedia bagi Anda untuk memilih dari daftar versi grup aturan statis. Anda hanya dapat melihat nama versi kandidat rilis dalam spesifikasi versi default.

3. Kembalikan versi default ke versi statis yang disarankan - Setelah menguji aturan kandidat rilis, AWS atur versi default kembali ke versi statis yang direkomendasikan saat ini. Setelan nama versi default menghapus `_PLUS_RC_COUNT` akhiran, dan grup aturan berhenti menghasilkan metrik

CloudWatch hitungan untuk aturan kandidat rilis. Ini adalah perubahan diam, dan tidak sama dengan penerapan rollback versi default.

Diagram berikut menunjukkan keadaan versi grup aturan contoh setelah pengujian kandidat rilis selesai.



Waktu dan pemberitahuan

AWS menyebarkan versi kandidat rilis sesuai kebutuhan, untuk menguji peningkatan pada grup aturan.

- SNS - AWS mengirimkan pemberitahuan SNS pada awal penerapan. Pemberitahuan menunjukkan perkiraan waktu kandidat rilis akan diuji. Saat pengujian selesai, AWS diam-diam mengembalikan default ke pengaturan versi statis, tanpa pemberitahuan kedua.
- Ubah log — AWS tidak memperbarui log perubahan atau bagian lain dari panduan ini untuk jenis penerapan ini.

Penerapan versi statis untuk AWS Aturan Terkelola

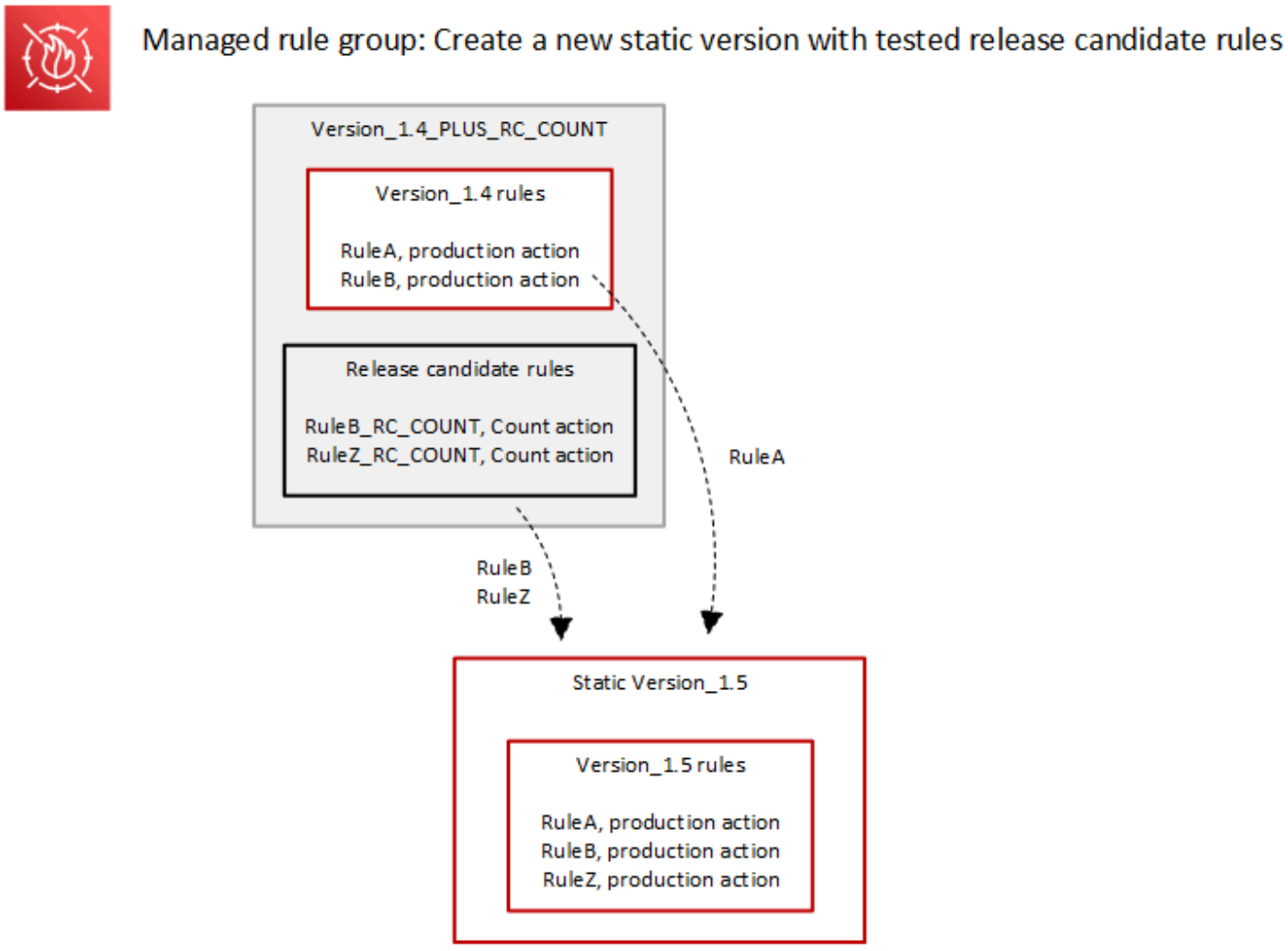
Saat AWS menentukan bahwa kandidat rilis memberikan perubahan berharga pada grup aturan, AWS menerapkan versi statis baru untuk grup aturan berdasarkan kandidat rilis. Penerapan ini tidak mengubah versi default grup aturan.

Versi statis baru berisi aturan berikut dari kandidat rilis:

- Aturan dari versi statis sebelumnya yang tidak memiliki kandidat pengganti di antara aturan kandidat rilis.
- Lepaskan aturan kandidat, dengan perubahan berikut:
  - AWS mengubah nama aturan dengan menghapus sufiks `_RC_COUNT` kandidat rilis.
  - AWS mengubah tindakan aturan dari Count tindakan aturan produksi mereka.

  Untuk aturan kandidat rilis yang merupakan pengganti aturan yang ada sebelumnya, ini menggantikan fungsionalitas aturan sebelumnya dalam versi statis baru.

Diagram berikut menggambarkan pembuatan versi statis baru dari kandidat rilis.



Setelah penerapan, versi statis baru tersedia untuk Anda uji dan gunakan dalam perlindungan Anda jika Anda mau. Anda dapat meninjau tindakan dan deskripsi aturan baru dan yang diperbarui dalam daftar aturan grup aturan di[AWS Daftar grup aturan Aturan Terkelola](#).

Versi statis tidak dapat diubah setelah penerapan, dan hanya berubah saat AWS kedaluwarsa. Untuk informasi tentang siklus hidup versi, lihatGrup aturan terkelola berversi.

Waktu dan pemberitahuan

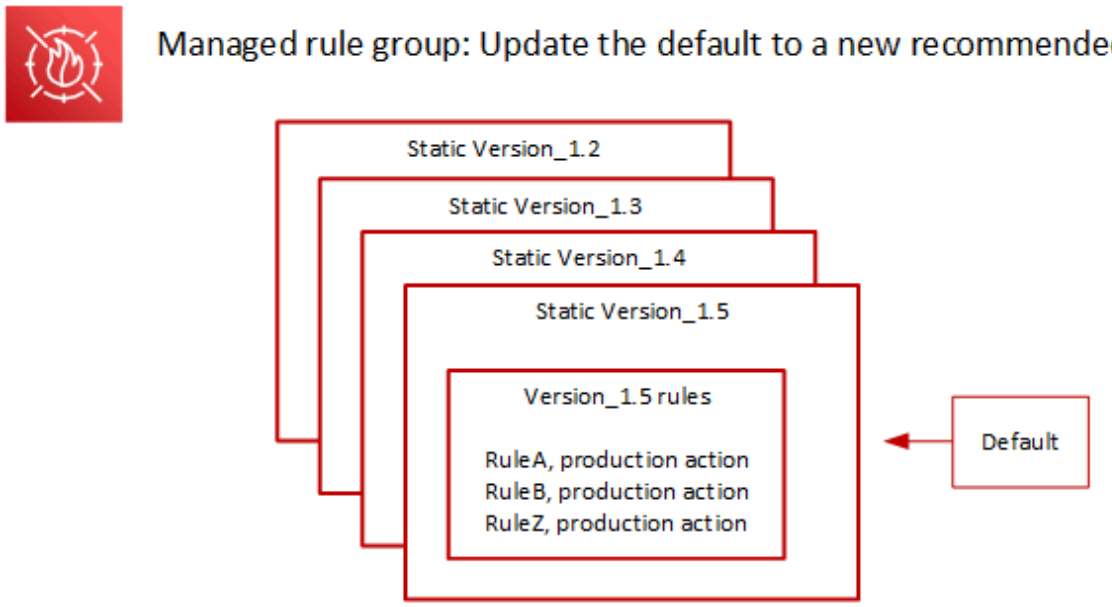
AWS menyebarkan versi statis baru sesuai kebutuhan, untuk menerapkan peningkatan pada fungsionalitas grup aturan. Penerapan versi statis tidak memengaruhi pengaturan versi default.

- SNS - AWS mengirimkan pemberitahuan SNS saat penerapan selesai.
- Ubah log - Setelah penerapan selesai di mana pun yang AWS WAF tersedia, AWS perbarui definisi grup aturan dalam panduan ini sesuai kebutuhan, lalu umumkan rilis di log perubahan grup aturan Aturan AWS Terkelola dan di halaman riwayat dokumentasi.

Penerapan versi default untuk AWS Aturan Terkelola

Saat AWS menentukan bahwa versi statis baru memberikan perlindungan yang lebih baik untuk grup aturan dibandingkan dengan default saat ini, AWS memperbarui versi default ke versi statis baru. AWS mungkin merilis beberapa versi statis sebelum mempromosikannya ke versi default grup aturan.

Diagram berikut menunjukkan status versi grup aturan contoh setelah AWS memindahkan pengaturan versi default ke versi statis baru.



Sebelum menerapkan perubahan ini ke versi default, AWS berikan pemberitahuan sehingga Anda dapat menguji dan mempersiapkan perubahan yang akan datang. Jika Anda menggunakan versi

default, Anda tidak dapat mengambil tindakan dan tetap menggunakannya melalui pembaruan. Jika Anda ingin menunda peralihan ke versi baru, sebelum memulai penerapan versi default yang direncanakan, Anda dapat mengonfigurasi grup aturan secara eksplisit untuk menggunakan versi statis yang disetel ke default.

Waktu dan pemberitahuan

AWS memperbarui versi default saat merekomendasikan versi statis yang berbeda untuk grup aturan daripada yang saat ini digunakan.

- SNS — AWS mengirimkan pemberitahuan SNS setidaknya satu minggu sebelum hari penyebaran yang ditargetkan dan kemudian yang lain pada hari penerapan, pada awal penerapan. Setiap pemberitahuan menyertakan nama grup aturan, versi statis tempat versi default diperbarui, tanggal penerapan, dan waktu penyebaran yang dijadwalkan untuk setiap AWS Wilayah tempat pembaruan dilakukan.
- Ubah log — AWS tidak memperbarui log perubahan atau bagian lain dari panduan ini untuk jenis penerapan ini.

Penerapan pengecualian untuk AWS Aturan Terkelola

AWS mungkin melewati tahapan penerapan standar untuk menyebarkan pembaruan dengan cepat yang mengatasi risiko keamanan kritis. Penerapan pengecualian mungkin melibatkan salah satu jenis penerapan standar, dan mungkin diluncurkan dengan cepat di seluruh Wilayah. AWS

AWS memberikan pemberitahuan terlebih dahulu sebanyak mungkin untuk penerapan pengecualian.

Waktu dan pemberitahuan

AWS melakukan penerapan pengecualian hanya jika diperlukan.

- SNS — AWS mengirimkan pemberitahuan SNS sejauh mungkin sebelum hari penyebaran yang ditargetkan dan kemudian satu lagi di awal penerapan. Setiap notifikasi menyertakan nama grup aturan, perubahan yang sedang dilakukan, dan tanggal penerapan.
- Ubah log - Jika penerapan untuk versi statis, setelah penerapan selesai di mana pun yang AWS WAF tersedia, AWS perbarui definisi grup aturan dalam panduan ini sesuai kebutuhan, lalu umumkan rilis di log perubahan grup aturan Aturan AWS Terkelola dan di halaman riwayat dokumentasi.

Rollback penerapan default untuk Aturan Terkelola AWS

Dalam kondisi tertentu, AWS mungkin memutar kembali versi default ke pengaturan sebelumnya. Rollback biasanya membutuhkan waktu kurang dari sepuluh menit untuk semua AWS Wilayah.

AWS melakukan rollback hanya untuk mengurangi masalah signifikan dalam versi statis, seperti tingkat positif palsu yang sangat tinggi.

Setelah rollback pengaturan versi default, AWS mempercepat kedaluwarsa versi statis yang memiliki masalah dan rilis versi statis baru untuk mengatasi masalah tersebut.

Waktu dan pemberitahuan

AWS melakukan rollback versi default hanya bila diperlukan.

- SNS - AWS mengirimkan pemberitahuan SNS tunggal pada saat rollback. Pemberitahuan mencakup nama grup aturan, versi yang disetel ke versi default, dan tanggal penerapan. Jenis penerapan ini sangat cepat, sehingga notifikasi tidak memberikan informasi waktu untuk Wilayah.
- Ubah log — AWS tidak memperbarui log perubahan atau bagian lain dari panduan ini untuk jenis penerapan ini.

AWS Penafian Aturan Terkelola

AWS Aturan Terkelola dirancang untuk melindungi Anda dari ancaman web umum. Bila digunakan sesuai dengan dokumentasi, grup aturan Aturan AWS Terkelola menambahkan lapisan keamanan lain untuk aplikasi Anda. Namun, grup aturan Aturan AWS Terkelola tidak dimaksudkan sebagai pengganti tanggung jawab keamanan Anda, yang ditentukan oleh AWS sumber daya yang Anda pilih. Lihat Model Tanggung Jawab Bersama untuk memastikan bahwa sumber daya Anda AWS dilindungi dengan benar.

AWS Aturan terkelola changelog

Bagian ini mencantumkan perubahan pada Aturan AWS Terkelola AWS WAF sejak dirilis pada November 2019.

> **Note**
>
> Changelog ini melaporkan perubahan pada aturan dan grup aturan dalam Aturan AWS Terkelola untuk. AWS WAF
> Untuk ituGrup aturan reputasi IP, changelog ini melaporkan perubahan pada aturan dan grup aturan, dan melaporkan perubahan signifikan pada sumber daftar alamat IP yang digunakan

aturan. Itu tidak melaporkan perubahan pada daftar alamat IP itu sendiri, karena sifat dinamis dari daftar tersebut. Jika Anda memiliki pertanyaan tentang daftar alamat IP, hubungi manajer akun Anda atau buka kasing di AWS Support Center.

Kelompok aturan dan aturan	Deskripsi	Tanggal
Grup aturan terkelola sistem operasi Linux Semua aturan	Dirilis versi statis 2.3 dari grup aturan ini. Ini tidak mengubah pengaturan versi default. Menambahkan tanda tangan untuk meningkatkan deteksi.	2024-06-06
AWS WAF Grup aturan Bot Control AWS WAF Kelompok aturan pencegahan pengambilalihan akun Kontrol Penipuan (ATP) AWS WAF Grup aturan pencegahan penipuan (ACFP) pembuatan akun Kontrol Penipuan	Grup aturan bot dan penipuan sekarang berversi. Jika Anda menggunakan salah satu grup aturan ini, pembaruan ini tidak mengubah cara mereka menangani lalu lintas web Anda. Pembaruan ini menetapkan versi grup aturan saat ini ke versi statis 1.0 dan menetapkan versi default untuk menunjuk ke sana. Untuk informasi selengkapnya tentang aturan terkelola berversi, lihat berikut ini: • Grup aturan terkelola berversi • Penerapan untuk grup aturan Aturan Terkelola berversi AWS	2024-05-29

Kelompok aturan dan aturan	Deskripsi	Tanggal
	• Mendapatkan pemberitahuan tentang versi baru dan pembaruan ke grup aturan terkelola	

Kelompok aturan dan aturan	Deskripsi	Tanggal
Grup aturan terkelola sistem operasi POSIX • `UNIXShellCommandsVariables_QUERYARGUMENTS` • `UNIXShellCommandsVariables_QUERYSTRING` • `UNIXShellCommandsVariables_HEADER` • `UNIXShellCommandsVariables_BODY`	Dirilis versi statis 3.0 dari grup aturan ini. Ini tidak mengubah pengaturan versi default. Dihapus `UNIXShellCommandsVariables_QUERYARGUMENTS` dan diganti dengan`UNIXShellCommandsVariables_QUERYSTRING`. Jika Anda memiliki aturan yang cocok pada label untuk`UNIXShellCommandsVariables_QUERYARGUMENTS`, saat Anda menggunakan versi ini, alihkan agar sesuai dengan label untuk`UNIXShellCommandsVariables_QUERYSTRING`. Label baru adalah`awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_QueryString`. Ditambahkan aturan`UNIXShellCommandsVariables_HEADER`, yang cocok pada semua header. Memperbarui semua aturan dalam grup aturan terkelola dengan logika deteksi yang ditingkatkan.	2024-05-28

Kelompok aturan dan aturan	Deskripsi	Tanggal
	Memperbaiki kapitalisasi label yang didokumentasikan untuk. `UNIXShellCommandsVariables_BODY`	
Grup aturan terkelola set aturan inti (CRS) • `CrossSiteScripting*`	Dirilis versi statis 1.12 dari grup aturan ini. Menambahkan tanda tangan ke semua aturan skrip lintas situs untuk meningkatkan deteksi dan mengurangi kesalahan positif.	2024-05-21
Grup aturan terkelola database SQL • `SQLi_BODY` • `SQLi_QUERYARGUMENTS` • `SQLiExtendedPatterns_QUERYARGUMENTS`	Dirilis versi statis 1.2 dari grup aturan ini. Menambahkan transformasi `JS_DECODE` teks ke aturan yang tercantum.	2024-05-14
Kelompok aturan terkelola masukan buruk yang diketahui • `JavaDeserializationRCE_BODY` • `JavaDeserializationRCE_QUERYSTRING` • `Log4JRCE_QUERYSTRING` • `Log4JRCE_BODY` • `Log4JRCE_HEADER`	Dirilis versi statis 1.22 dari grup aturan ini. Menambahkan transformasi `JS_DECODE` teks ke aturan yang tercantum.	2024-05-08

Kelompok aturan dan aturan	Deskripsi	Tanggal
Grup aturan terkelola sistem operasi POSIX	Dirilis versi statis 2.2 dari grup aturan ini. Menambahkan transformasi `JS_DECODE` teks ke kedua aturan.	2024-05-08
Grup aturan terkelola sistem operasi Windows • `PowerShellCommands_BODY`	Dirilis versi statis 2.1 dari grup aturan ini. Menambahkan tanda tangan `PowerShellCommands_BODY` untuk meningkatkan deteksi.	2024-05-03
Grup aturan terkelola daftar reputasi IP Amazon • `AWSManagedIPReputationList`	Memperbarui sumber daftar reputasi IP, untuk meningkatkan identifikasi alamat yang secara aktif terlibat dalam aktivitas jahat dan untuk mengurangi positif palsu. Pembaruan ini tidak melibatkan versi baru karena grup aturan ini tidak berversi.	2023-12-16
Kelompok aturan terkelola masukan buruk yang diketahui	Dirilis versi statis 1.21 dari grup aturan ini. Menambahkan tanda tangan untuk meningkatkan deteksi dan mengurangi positif palsu.	2023-12-16

Kelompok aturan dan aturan	Deskripsi	Tanggal
Kelompok aturan terkelola masukan buruk yang diketahui • `ExploitablePaths_URIPATH`	Dirilis versi statis 1.20 dari grup aturan ini. Memperbarui `ExploitablePaths_URIPATH` aturan untuk menambahkan deteksi permintaan yang cocok dengan kerentanan Otorisasi Tidak Benar Atlassian Confluence CVE-2023-22518. Kerentanan ini memengaruhi semua versi Confluence Data Center dan Server. Untuk informasi lebih lanjut, lihat NIST: Database Kerentanan Nasional: CVE-2023-22518 Detail.	2023-12-14
Grup aturan terkelola set aturan inti (CRS) • `CrossSiteScripting*`	Dirilis versi statis 1.11 dari grup aturan ini. Menambahkan tanda tangan ke semua aturan skrip lintas situs untuk meningkatkan deteksi dan mengurangi kesalahan positif.	2023-12-06

Kelompok aturan dan aturan	Deskripsi	Tanggal
AWS WAF Grup aturan Bot Control • Label baru: `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:low`	Menambahkan label rendah aktivitas terkoordinasi ke label tingkat perlindungan yang ditargetkan grup aturan. Label ini tidak terkait dengan aturan apa pun. Pelabelan ini merupakan tambahan dari aturan dan label tingkat menengah dan tinggi.	2023-12-05
Label Kontrol Bot • label: `awswaf:managed:aws:bot-control:targeted:signal:browser_automation_extension`	Menambahkan label sinyal ke grup aturan yang menunjukkan deteksi ekstensi browser yang membantu otomatisasi. Label ini tidak spesifik untuk aturan individual.	2023-11-14
Grup aturan terkelola set aturan inti (CRS) • `EC2MetaDataSSRF_QUERYARGUMENTS`	Dirilis versi statis 1.10 dari grup aturan ini. Memperbarui satu aturan untuk meningkatkan deteksi dan mengurangi positif palsu.	2023-11-02

Kelompok aturan dan aturan	Deskripsi	Tanggal
Grup aturan terkelola set aturan inti (CRS) • `EC2MetaDataSSRF_BODY` • `EC2MetaDataSSRF_COOKIE` • `EC2MetaDataSSRF_URIPATH` • `EC2MetaDataSSRF_QUERYARGUMENTS`	Dirilis versi statis 1.9 dari grup aturan ini. Aturan yang diperbarui untuk meningkatkan deteksi dan mengurangi positif palsu.	2023-10-30
Grup aturan terkelola sistem operasi POSIX • `UNIXShellCommandsVariables_QUERYARGUMENTS`	Dirilis versi statis 2.1 dari grup aturan ini. Memperbarui aturan argumen kueri untuk meningkatkan deteksi.	2023-10-12

Kelompok aturan dan aturan	Deskripsi	Tanggal
Grup aturan terkelola set aturan inti (CRS) • `GenericLFI_QUERYARGUMENTS` • `GenericLFI_URIPATH` • `RestrictedExtensions_URIPATH` • `RestrictedExtensions_QUERYARGUMENTS`	Dirilis versi statis 1.8 dari grup aturan ini. Aturan yang diperbarui untuk meningkatkan deteksi.	2023-10-11

Kelompok aturan dan aturan	Deskripsi	Tanggal
Kelompok aturan terkelola masukan buruk yang diketahui • `ExploitablePaths_URIPATH`	Penerapan pengecualian: merilis versi statis 1.19 dari grup aturan ini. Diperbarui versi default untuk menggunakan versi 1.19. Memperbarui `ExploitablePaths_URIPATH` aturan untuk menambahkan deteksi permintaan yang cocok dengan Kerentanan Eskalasi Privilege Atlassian Confluence CVE-2023-22515. Kerentanan ini memengaruhi beberapa versi Atlassian Confluence. Untuk informasi lebih lanjut, lihat NIST: National Vulnerability Database: CVE-2023-22515 Detail dan Atlassian Support: FAQ untuk CVE-2023-22515. Untuk informasi tentang jenis penerapan ini, lihatPenerapan pengecualian untuk AWS Aturan Terkelola.	2023-10-04

Kelompok aturan dan aturan	Deskripsi	Tanggal
Kelompok aturan terkelola masukan buruk yang diketahui • `Host_localhost_HEADER` • `Log4J*` • `JavaDeserialization*`	Penerapan pengecualian: merilis versi statis 1.18 dari grup aturan ini. Ini adalah peluncuran cepat dari versi statis ini untuk mengakomodasi pembuatan dan peluncuran versi 1.19. Memperbarui `Host_localhost_HEADER` aturan dan semua aturan deserialisasi Log4J dan Java untuk deteksi yang lebih baik. Untuk informasi tentang jenis penerapan ini, lihatPenerapan pengecualian untuk AWS Aturan Terkelola.	2023-10-04

Kelompok aturan dan aturan	Deskripsi	Tanggal
AWS WAF Grup aturan Bot Control • `TGT_TokenReuseIp` • `TGT_ML_CoordinatedActivityMedium` • `TGT_ML_CoordinatedActivityHigh`	Menambahkan aturan ke grup aturan dengan Count tindakan. Aturan IP penggunaan kembali token mendeteksi dan menghitung berbagi token di seluruh alamat IP. Aturan aktivitas terkoordinasi menggunakan analisis otomatis, pembelajaran mesin (ML) lalu lintas situs web untuk mendeteksi aktivitas terkait bot. Dalam konfigurasi grup aturan Anda, Anda dapat memilih keluar dari penggunaan ML. Dengan rilis ini, pelanggan yang saat ini menggunakan tingkat perlindungan yang ditargetkan akan memilih untuk menggunakan ML. Memilih keluar menonaktifkan aturan aktivitas terkoordinasi.	2023-09-06
AWS WAF Grup aturan Bot Control • `CategoryAI`	Menambahkan aturan `CategoryAI` ke grup aturan.	2023-08-30

Kelompok aturan dan aturan	Deskripsi	Tanggal
Grup aturan terkelola set aturan inti (CRS) • `RestrictedExtensions_URIPATH` • `RestrictedExtensions_QUERYARGUMENTS` • `EC2MetaDataSSRF_COOKIE` • `EC2MetaDataSSRF_QUERYARGUMENTS` • `EC2MetaDataSSRF_BODY` • `EC2MetaDataSSRF_URIPATH`	Dirilis versi statis 1.7 dari grup aturan ini. Memperbarui ekstensi terbatas dan aturan SSRF metadata EC2 untuk meningkatkan deteksi dan mengurangi kesalahan positif.	2023-07-26
AWS WAF Grup aturan pencegahan penipuan (ACFP) pembuatan akun Kontrol Penipuan Semua aturan dalam grup aturan baru	Ditambahkan kelompok aturan`AWSManagedRulesACFPRuleSet` .	2023-06-13

Kelompok aturan dan aturan	Deskripsi	Tanggal
Grup aturan terkelola sistem operasi Linux • LFI_HEADER • LFI_URIPATH • LFI_QUERYSTRING	Dirilis versi statis 2.2 dari grup aturan ini. Menambahkan tanda tangan untuk meningkatkan deteksi.	2023-05-22
Grup aturan terkelola set aturan inti (CRS) • RestrictedExtensions_URIPATH • RestrictedExtensions_QUERYARGUMENTS • CrossSiteScripting_COOKIE • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_BODY • CrossSiteScripting_URIPATH	Dirilis versi statis 1.6 dari grup aturan ini. Skrip lintas situs (XSS) yang diperbarui dan aturan ekstensi terbatas untuk meningkatkan deteksi dan mengurangi kesalahan positif.	2023-04-28

Kelompok aturan dan aturan	Deskripsi	Tanggal
Grup aturan terkelola aplikasi PHP • Diperbarui `PHPHighRiskMethodsVariables_BODY` • Dihapus `PHPHighRiskMethodsVariables_QUERYARGUMENTS` • Ditambahkan `PHPHighRiskMethodsVariables_QUERYSTRING` • Ditambahkan `PHPHighRiskMethodsVariables_HEADER`	Dirilis versi statis 2.0 dari grup aturan ini. Menambahkan tanda tangan untuk meningkatkan deteksi di semua aturan. Mengganti aturan `PHPHighRiskMethodsVariables_QUERYARGUMENTS` dengan`PHPHighRiskMethodsVariables_QUERYSTRING` , yang memeriksa seluruh string query bukan hanya argumen query. Menambahkan aturan`PHPHighRiskMethodsVariables_HEADER` , untuk memperluas cakupan untuk menyertakan semua header. Memperbarui label berikut agar selaras dengan pelabelan Aturan AWS Terkelola standar: • Nama lama: Nama `PHPHighRiskMethodsVariables_BODY` baru: `PHPHighRiskMethodsVariables_Body` • Nama lama: Nama `PHPHighRiskMethods`	2023-02-27

Kelompok aturan dan aturan	Deskripsi	Tanggal
	`Variables_QUERYARGUMENTS` baru: `PHPHighRiskMethodsVariables_QueryString`	
AWS WAF Kelompok aturan pencegahan pengambilalihan akun Kontrol Penipuan (ATP) • `VolumetricIpFailedLoginResponseHigh` • `VolumetricSessionFailedLoginResponseHigh`	Menambahkan aturan inspeksi respons login untuk digunakan dengan CloudFront distribusi Amazon yang dilindungi. Aturan ini dapat memblokir upaya login baru dari alamat IP dan sesi klien yang baru-baru ini menjadi sumber dari terlalu banyak upaya login yang gagal.	2023-02-15
Grup aturan terkelola set aturan inti (CRS) • `NoUserAgent_HEADER` • `CrossSiteScripting_COOKIE` • `CrossSiteScripting_QUERYARGUMENTS` • `CrossSiteScripting_BODY` • `CrossSiteScripting_URIPATH`	Dirilis versi statis 1.5 dari grup aturan ini. Filter Cross Site Scripting (XSS) yang diperbarui untuk meningkatkan deteksi.	2023-01-25

Kelompok aturan dan aturan	Deskripsi	Tanggal
Grup aturan terkelola sistem operasi Linux • `LFI_COOKIE` - dihapus • `LFI_HEADER` - ditambahkan • `LFI_URIPATH` • `LFI_QUERYSTRING`	Dirilis versi statis 2.1 dari grup aturan ini. Menghapus aturan `LFI_COOKIE` dan labelnya`awswaf:managed:aws:linux-os:LFI_Cookie`, dan menggantinya dengan aturan baru `LFI_HEADER` dan labelnya`awswaf:managed:aws:linux-os:LFI_Header`. Perubahan ini memperluas inspeksi ke beberapa header. Menambahkan transformasi teks dan tanda tangan ke semua aturan untuk meningkatkan deteksi.	2022-12-15

Kelompok aturan dan aturan	Deskripsi	Tanggal
Grup aturan terkelola set aturan inti (CRS) • `NoUserAgent_HEADER` • `CrossSiteScripting_COOKIE` • `CrossSiteScripting_QUERYARGUMENTS` • `CrossSiteScripting_BODY` • `CrossSiteScripting_URIPATH`	Dirilis versi statis 1.4 dari grup aturan ini. Ditambahkan transformasi teks `NoUserAgent_HEADER` untuk menghapus semua byte null. Memperbarui filter dalam aturan skrip lintas situs untuk meningkatkan deteksi.	2022-12-05

Kelompok aturan dan aturan	Deskripsi	Tanggal
Kelompok aturan terkelola masukan buruk yang diketahui • `JavaDeserializationRCE_BODY` • `JavaDeserializationRCE_URIPATH` • `JavaDeserializationRCE_HEADER` • `JavaDeserializationRCE_QUERYSTRING` • `Host_localhost_HEADER`	Dirilis versi statis 1.17 dari grup aturan ini. Memperbarui aturan deserialisasi Java untuk menambahkan deteksi permintaan yang cocok dengan Apache CVE-2022-42889, kerentanan eksekusi kode jarak jauh (RCE) dalam versi Teks Apache Commons sebelum 1.10.0. Untuk informasi lebih lanjut, lihat NIST: Database Kerentanan Nasional: CVE-2022-42889 Detail dan CVE-2022-42889: Teks Apache Commons sebelum 1.10.0 memungkinkan RCE ketika diterapkan ke input yang tidak tepercaya karena default interpolasi yang tidak aman. Deteksi yang ditingkatkan di`Host_localhost_HEADER` .	2022-10-20

Kelompok aturan dan aturan	Deskripsi	Tanggal
Kelompok aturan terkelola masukan buruk yang diketahui • `Log4JRCE_HEADER` • `Log4JRCE_QUERYSTRING` • `Log4JRCE_URIPATH` • `Log4JRCE_BODY`	Dirilis versi statis 1.16 dari grup aturan ini. Menghapus positif palsu yang AWS diidentifikasi dalam versi 1.15.	2022-10-05
Grup aturan terkelola sistem operasi POSIX Grup aturan terkelola aplikasi PHP WordPress kelompok aturan terkelola aplikasi	Memperbaiki nama label yang didokumentasikan.	2022-09-19
Grup aturan reputasi IP • `AWSManagedIPDDoSList`	Perubahan ini tidak mengubah cara grup aturan menangani lalu lintas web. Menambahkan aturan baru dengan Count tindakan untuk memeriksa alamat IP yang secara aktif terlibat dalam aktivitas DDoS, menurut intelijen ancaman Amazon.	2022-08-30

Kelompok aturan dan aturan	Deskripsi	Tanggal
Kelompok aturan terkelola masukan buruk yang diketahui • `Log4JRCE` • `Log4JRCE_HEADER` • `Log4JRCE_QUERYSTRING` • `Log4JRCE_URIPATH` • `Log4JRCE_BODY` • `JavaDeserializationRCE_HEADER` • `JavaDeserializationRCE_BODY` • `JavaDeserializationRCE_URIPATH` • `JavaDeserializationRCE_QUERYSTRING` • `Host_localhost_HEADER` • `PROPFIND_METHOD`	Dirilis versi statis 1.15 dari grup aturan ini. Dihapus `Log4JRCE` dan diganti dengan`Log4JRCE_HEADER` ,`Log4JRCE_QUERYSTRING` ,`Log4JRCE_URI` , dan`Log4JRCE_BODY` , untuk pemantauan dan pengelolaan positif palsu yang lebih terperinci. Menambahkan tanda tangan untuk meningkatkan deteksi dan pemblokiran ke `PROPFIND_METHOD` dan ke semua `JavaDeserializationRCE*` dan `Log4JRCE*` aturan. Label yang diperbarui untuk memperbaiki kapitalisasi di dalam `Host_localhost_HEADER` dan di semua `JavaDeserializationRCE*` aturan. Mengoreksi deskripsi. `JavaDeserializationRCE_HEADER`	2022-08-22

Kelompok aturan dan aturan	Deskripsi	Tanggal
AWS WAF Kelompok aturan pencegahan pengambilalihan akun Kontrol Penipuan (ATP) • `UnsupportedCognitoIDP`	Menambahkan aturan untuk mencegah penggunaan grup aturan terkelola pencegahan pengambilalihan akun untuk lalu lintas web kumpulan pengguna Amazon Cognito.	2022-08-11
Grup aturan terkelola set aturan inti (CRS)	AWS telah dijadwalkan kedaluwarsa untuk versi `Version_1.2` dan `Version_2.0` grup aturan. Versi akan kedaluwarsa pada 9 September 2022. Untuk informasi tentang kedaluwarsa versi, lihat. Grup aturan terkelola berversi	2022-06-09
Grup aturan terkelola set aturan inti (CRS) • `GenericLFI_URIPATH` `GenericRFI_URIPATH`	Dirilis versi 1.3 dari grup aturan ini. Rilis ini memperbarui tanda tangan kecocokan dalam aturan `GenericLFI_URIPATH` dan`GenericRFI_URIPATH` , untuk meningkatkan deteksi.	2022-05-24
AWS WAF Grup aturan Bot Control • `CategoryEmailClient`	Menambahkan aturan `CategoryEmailClient` ke grup aturan.	2022-04-06

Kelompok aturan dan aturan	Deskripsi	Tanggal
Kelompok aturan terkelola masukan buruk yang diketahui • `JavaDeserializationRCE_HEADER` • `JavaDeserializationRCE_BODY` • `JavaDeserializationRCE_URI` • `JavaDeserializationRCE_QUERYSTRING`	Dirilis versi 1.14 dari grup aturan ini. Keempat `JavaDeserializtion RCE` aturan dipindahkan ke Block mode.	2022-03-31
Kelompok aturan terkelola masukan buruk yang diketahui • `JavaDeserializationRCE_HEADER_RC_COUNT` • `JavaDeserializationRCE_BODY_RC_COUNT` • `JavaDeserializationRCE_URI_RC_COUNT` • `JavaDeserializationRCE_QUERYSTRING_RC_COUNT`	Dirilis versi 1.13 dari grup aturan ini. Memperbarui transformasi teks untuk kerentanan Spring Core dan Cloud Function RCE. Aturan-aturan ini berada dalam mode hitung untuk mengumpulkan metrik dan mengevaluasi pola yang cocok. Label dapat digunakan untuk memblokir permintaan dalam aturan khusus. Versi berikutnya akan digunakan dengan aturan ini dalam mode blok.	2022-03-31

Kelompok aturan dan aturan	Deskripsi	Tanggal
Kelompok aturan terkelola masukan buruk yang diketahui • JavaDeserializationRCE_HEADER_RC_COUNT • JavaDeserializationRCE_BODY_RC_COUNT • JavaDeserializationRCE_URI_RC_COUNT • JavaDeserializationRCE_QUERYSTRING_RC_COUNT • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URI • Log4JRCE_BODY • Log4JRCE	Dirilis versi 1.12 dari grup aturan ini. Menambahkan tanda tangan untuk kerentanan Spring Core dan Cloud Function RCE. Aturan-aturan ini berada dalam mode hitung untuk mengumpulkan metrik dan mengevaluasi pola yang cocok. Label dapat digunakan untuk memblokir permintaan dalam aturan khusus. Versi berikutnya akan digunakan dengan aturan ini dalam mode blok. Menghapus aturan Log4JRCE_HEADER Log4JRCE_QUERYSTRING ,Log4JRCE_URI ,, Log4JRCE_BODY dan menggantinya dengan aturanLog4JRCE.	2022-03-30
Grup aturan reputasi IP • AWSManagedReconnaissanceList	Memperbarui AWSManagedReconnaissanceList aturan untuk mengubah tindakan dari hitungan ke blok.	2022-02-15

Kelompok aturan dan aturan	Deskripsi	Tanggal
AWS WAF Kelompok aturan pencegahan pengambilalihan akun Kontrol Penipuan (ATP) Semua aturan dalam grup aturan baru	Ditambahkan kelompok aturan`AWSManage dRulesATPRuleSet` .	2022-02-11
Kelompok aturan terkelola masukan buruk yang diketahui • `Log4JRCE` • `Log4JRCE_HEADER` • `Log4JRCE_QUERYSTRI NG` • `Log4JRCE_URI` • `Log4JRCE_BODY`	Dirilis versi 1.9 dari grup aturan ini. Menghapus aturan `Log4JRCE` dan menggantinya dengan aturan`Log4JRCE_ HEADER` ,`Log4JRCE_ QUERYSTRING` ,`Log4JRCE_ URI` , dan`Log4JRCE_ BODY` , untuk fleksibilitas dalam penggunaan fungsi ini. Menambahkan tanda tangan untuk meningkatkan deteksi dan pemblokiran.	2022-01-28
Set aturan inti (CRS) • `CrossSiteScripting _URIPATH` • `CrossSiteScripting _BODY` • `CrossSiteScripting _QUERYARGUMENTS` • `CrossSiteScripting _COOKIE`	Dirilis versi 2.0 dari grup aturan ini. Untuk aturan ini, tanda tangan deteksi yang disetel untuk mengurang i positif palsu. Mengganti transformasi `URL_DECOD E` teks dengan transform asi `URL_DECODE_UNI` teks ganda. Ditambahkan transformasi `HTML_ENTI TY_DECODE` teks.	2022-01-10

Kelompok aturan dan aturan	Deskripsi	Tanggal
Set aturan inti (CRS) • `RestrictedExtensions_URIPATH` • `RestrictedExtensions_QUERYARGUMENTS`	Sebagai bagian dari rilis versi 2.0 dari grup aturan ini, menambahkan transformasi `URL_DECODE_UNI` teks. Menghapus transformasi `URL_DECODE` teks dari`RestrictedExtensions_URIPATH` .	2022-01-10
Database SQL • `SQLi_BODY` • `SQLi_QUERYARGUMENTS` • `SQLi_COOKIE` • `SQLi_URIPATH` • `SQLiExtendedPatterns_BODY` • `SQLiExtendedPatterns_QUERYARGUMENTS`	Dirilis versi 2.0 dari grup aturan ini. Mengganti transformasi `URL_DECODE` teks dengan transformasi `URL_DECODE_UNI` teks ganda dan menambahkan transformasi `COMPRESS_WHITE_SPACE` teks. Menambahkan lebih banyak tanda tangan deteksi ke. `SQLiExtendedPatterns_QUERYARGUMENTS` Menambahkan inspeksi JSON ke`SQLi_BODY` . Ditambahkan aturan`SQLiExtendedPatterns_BODY` . Menghapus aturan`SQLi_URIPATH` .	2022-01-10

Kelompok aturan dan aturan	Deskripsi	Tanggal
Masukan buruk yang diketahui • `Log4JRCE`	Dirilis versi 1.8 dari aturan `Log4JRCE` untuk meningkatkan pemeriksaan header dan kriteria pencocokan.	2021-12-17
Masukan buruk yang diketahui • `Log4JRCE`	Dirilis versi 1.4 dari aturan `Log4JRCE` untuk menyetel kriteria yang cocok dan untuk memeriksa header tambahan. Dirilis versi 1.5 untuk menyetel kriteria yang cocok.	2021-12-11
Masukan buruk yang diketahui • `Log4JRCE` • `BadAuthToken_COOKIE_AUTHORIZATION`	Menambahkan aturan `Log4JRCE` versi 1.2 sebagai tanggapan atas masalah keamanan yang baru-baru ini diungkapkan dalam Log4j. Untuk informasi lihat CVE-2021-44228. Aturan ini memeriksa jalur URI umum, string kueri, 8KB pertama dari badan permintaan, dan header umum. Aturan menggunakan transformasi `URL_DECODE_UNI` teks ganda. Dirilis versi 1.3 `Log4JRCE` untuk menyetel kriteria yang cocok dan untuk memeriksa header tambahan. Menghapus aturan`BadAuthToken_COOKIE_AUTHORIZATION` .	2021-12-10

Tabel berikut mencantumkan perubahan sebelum Desember 2021.

Kelompok aturan dan aturan	Deskripsi	Tanggal	
Daftar reputasi IP Amazon	`AWSManagedReconnaissanceList`	Ditambahkan `AWSManagedReconnaissanceList` aturan dalam modus monitoring/count. Aturan ini berisi alamat IP yang melakukan pengintaian terhadap sumber daya. AWS	2021-11-23

Sistem operasi Windows	`WindowsShellCommands`
	
	`PowerShellCommands`
		Menambahkan tiga aturan baru untuk WindowsShell perintah:`WindowsShellCommands_COOKIE` ,`WindowsShellCommands_QUERYARGUMENTS` , dan`WindowsShellCommands_BODY` .
		
		Menambahkan PowerShell aturan baru:`PowerShellCommands_COOKIE` .
			2021-11-23

Kelompok aturan dan aturan	Deskripsi	Tanggal	
		Merestrukturisasi `PowerShellComands` aturan penamaan dengan menghapus string _Set1 dan _Set2. Menambahkan tanda tangan deteksi yang lebih komprehensif ke. `PowerShellRules` Menambahkan transformasi `URL_DECODE_UNI` teks ke semua aturan sistem operasi Windows.	

Kelompok aturan dan aturan	Deskripsi	Tanggal	

Sistem operasi Linux	`LFI_URIPATH`
	
	`LFI_QUERYSTRING`
	
	`LFI_BODY`
	
	`LFI_COOKIE`
		Mengganti transformasi `URL_DECODE` teks ganda dengan ganda`URL_DECODE_UNI` .
		
		Ditambahkan `NORMALIZE_PATH_WIN` sebagai transformasi teks kedua.
		
		Mengganti `LFI_BODY` aturan dengan `LFI_COOKIE` aturan.
		
		Menambahkan tanda tangan deteksi yang lebih komprehensif untuk semua `LFI` aturan.
			2021-11-23

Set aturan inti (CRS)	`SizeRestrictions_BODY`	Mengurangi batas ukuran untuk memblokir permintaan web dengan muatan tubuh yang lebih besar dari 8 KB. Sebelumnya, batasnya adalah 10 KB.	2021-10-27

Kelompok aturan dan aturan	Deskripsi	Tanggal	

Set aturan inti (CRS)	`EC2MetaDataSSRF_BODY`
	`EC2MetaDataSSRF_COOKIE`
	`EC2MetaDataSSRF_URIPATH`
	`EC2MetaDataSSRF_QUERYARGUMENTS`
		Menambahkan lebih banyak tanda tangan deteksi. Menambahkan decode URL unicode ganda untuk meningkatkan pemblokiran.	2021-10-27

Set aturan inti (CRS)	`GenericLFI_QUERYARGUMENTS`
	`GenericLFI_URIPATH`
	`RestrictedExtensions_URIPATH`
	`RestrictedExtensions_QUERYARGUMENTS`
		Menambahkan decode URL unicode ganda untuk meningkatkan pemblokiran.	2021-10-27

Kelompok aturan dan aturan	Deskripsi	Tanggal	

Set aturan inti (CRS)	`GenericRFI_QUERYARGUMENTS`
	`GenericRFI_BODY`
	`GenericRFI_URIPATH`
		Memperbarui tanda tangan aturan untuk mengurangi positif palsu, berdasarkan umpan balik pelanggan. Menambahkan decode URL unicode ganda untuk meningkatkan pemblokiran.	2021-10-27

Semua	Semua aturan	Menambahkan dukungan untuk AWS WAF label ke semua aturan yang belum mendukung pelabelan.	2021-10-25
Daftar reputasi IP Amazon	`AWSManagedIPReputationList_xxxx`	Merestrukturisasi daftar reputasi IP, menghapus sufiks dari nama aturan, dan menambahkan dukungan untuk label. AWS WAF	2021-05-04
Daftar IP anonim	`AnonymousIPList` `HostingProviderList`	Menambahkan dukungan untuk AWS WAF label.	2021-05-04
Kontrol Bot	Semua	Menambahkan set aturan Bot Control.	2021-04-01

Kelompok aturan dan aturan	Deskripsi	Tanggal	
Set aturan inti (CRS)	`GenericRFI_QUERYARGUMENTS`	Ditambahkan decode URL ganda.	2021-03-03
Set aturan inti (CRS)	`RestrictedExtensions_URIPATH`	Meningkatkan konfigurasi aturan dan menambahkan decode URL tambahan.	2021-03-03
Perlindungan admin	`AdminProtection_URIPATH`	Ditambahkan decode URL ganda.	2021-03-03
Masukan buruk yang diketahui	`ExploitablePaths_URIPATH`	Meningkatkan konfigurasi aturan dan menambahkan decode URL tambahan.	2021-03-03
Sistem operasi Linux	`LFI_QUERYARGUMENTS`	Meningkatkan konfigurasi aturan dan menambahkan decode URL tambahan.	2021-03-03
Sistem operasi Windows	Semua	Meningkatkan konfigurasi aturan.	2020-09-23

Kelompok aturan dan aturan	Deskripsi	Tanggal	

Aplikasi PHP	`PHPHighRiskMethodsVariables_QUERYARGUMENTS`
	
	`PHPHighRiskMethodsVariables_BODY`
		Mengubah transformasi teks dari decode HTML ke decode URL, untuk meningkatkan pemblokiran.	2020-09-16

Sistem operasi POSIX	`UNIXShellCommandsVariables_QUERYARGUMENTS`
	
	`UNIXShellCommandsVariables_BODY`
		Mengubah transformasi teks dari decode HTML ke decode URL, untuk meningkatkan pemblokiran.	2020-09-16

Set aturan inti	`GenericLFI_QUERYARGUMENTS`
	
	`GenericLFI_URIPATH`
	
	Genericlfi_tubuh
		Mengubah transformasi teks dari decode HTML ke decode URL, untuk meningkatkan pemblokiran.	2020-08-07

Sistem operasi Linux	`LFI_URIPATH`
	
	`LFI_QUERYARGUMENTS`
	
	`LFI_BODY`
		Mengubah transformasi teks dari decode entitas HTML ke decode URL, untuk meningkatkan deteksi dan pemblokiran.	2020-05-19

Kelompok aturan dan aturan	Deskripsi	Tanggal	
Daftar IP Anonim	Semua	Grup aturan baru Grup aturan reputasi IP untuk memblokir permintaan dari layanan yang memungkinkan pengaburan identitas pemirsa, untuk membantu mengurangi bot dan penghindaran pembatasan geografis.	2020-03-06
WordPress aplikasi	`WordPressExploitableCommands_QUERYSTRING`	Aturan baru yang memeriksa perintah yang dapat dieksploitasi dalam string kueri.	2020-03-03

Set aturan inti (CRS)	`SizeRestrictions_QUERYSTRING`
	
	`SizeRestrictions_Cookie_HEADER`
	
	`SizeRestrictions_BODY`
	
	`SizeRestrictions_URIPATH`
		Menyesuaikan batasan nilai ukuran untuk meningkatkan akurasi.	2020-03-03

Kelompok aturan dan aturan	Deskripsi	Tanggal	
Database SQL	`SQLi_URIPATH`	Aturan sekarang memeriksa URI pesan.	2020-01-23

Database SQL	`SQLi_BODY`
	
	`SQLi_QUERYARGUMENTS`
	
	`SQLi_COOKIE`
		Transformasi teks yang diperbarui.	2019-12-20

Set aturan inti (CRS)	`CrossSite Scripting_URIPATH`
	
	`CrossSite Scripting_BODY`
	
	`CrossSite Scripting_QUERYARGUMENTS`
	
	`CrossSite Scripting_COOKIE`
		Transformasi teks yang diperbarui.	2019-12-20

AWS Marketplace kelompok aturan terkelola

AWS Marketplace grup aturan terkelola tersedia dengan berlangganan melalui AWS Marketplace konsol di AWS Marketplace. Setelah berlangganan grup aturan AWS Marketplace terkelola, Anda dapat menggunakannya di AWS WAF. Untuk menggunakan grup AWS Marketplace aturan dalam AWS Firewall Manager AWS WAF kebijakan, setiap akun di organisasi Anda harus berlangganan.

Uji dan sesuaikan perubahan apa pun pada AWS WAF perlindungan Anda sebelum Anda menggunakannya untuk lalu lintas produksi. Untuk informasi, lihat Menguji dan menyetel perlindungan Anda AWS WAF.

AWS Marketplace Harga Grup Aturan

AWS Marketplace kelompok aturan tersedia tanpa kontrak jangka panjang, dan tidak ada komitmen minimum. Saat Anda berlangganan grup aturan, Anda dikenakan biaya bulanan (prorata per jam) dan biaya permintaan berkelanjutan berdasarkan volume. Untuk informasi selengkapnya, lihat AWS WAF Harga dan deskripsi untuk setiap grup AWS Marketplace aturan di AWS Marketplace.

Punya pertanyaan tentang kelompok AWS Marketplace aturan?

Untuk pertanyaan tentang grup aturan yang dikelola oleh AWS Marketplace penjual dan untuk meminta perubahan fungsionalitas, hubungi tim dukungan pelanggan penyedia. Untuk menemukan informasi kontak, lihat daftar penyedia di AWS Marketplace.

Penyedia grup AWS Marketplace aturan menentukan cara mengelola grup aturan, misalnya cara memperbarui grup aturan dan apakah grup aturan diberi versi. Penyedia juga menentukan detail grup aturan, termasuk aturan, tindakan aturan, dan label apa pun yang ditambahkan aturan ke permintaan web yang cocok.

Berlangganan grup aturan AWS Marketplace terkelola

Anda dapat berlangganan dan berhenti berlangganan dari grup AWS Marketplace aturan di AWS WAF konsol.

> ⚠ Important
>
> Untuk menggunakan grup AWS Marketplace aturan dalam AWS Firewall Manager kebijakan, setiap akun di organisasi Anda harus terlebih dahulu berlangganan grup aturan tersebut.

Untuk berlangganan grup aturan AWS Marketplace terkelola

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.
2. Di panel navigasi, pilih AWS Marketplace.
3. Di bagian Produk pasar yang tersedia, pilih nama grup aturan untuk melihat detail dan informasi harga.

4. Jika Anda ingin berlangganan grup aturan, pilih Lanjutkan.

> **Note**
>
> Jika Anda tidak ingin berlangganan grup aturan ini, cukup tutup halaman ini di browser Anda.

5. Pilih Siapkan akun Anda.
6. Tambahkan grup aturan ke ACL web, mirip dengan cara Anda menambahkan aturan individual. Untuk informasi selengkapnya, lihat Membuat web ACL atau Mengedit ACL web.

> **Note**
>
> Saat menambahkan grup aturan ke ACL web, Anda dapat mengganti tindakan aturan dalam grup aturan dan hasil grup aturan. Untuk informasi selengkapnya, lihat Opsi penggantian tindakan untuk grup aturan.

Setelah berlangganan grup AWS Marketplace aturan, Anda menggunakannya di ACL web seperti halnya grup aturan terkelola lainnya. Untuk informasi, lihat Membuat web ACL.

Berhenti berlangganan dari grup aturan AWS Marketplace terkelola

Anda dapat berhenti berlangganan dari grup AWS Marketplace aturan di AWS WAF konsol.

> **Important**
>
> Untuk menghentikan biaya berlangganan untuk grup aturan AWS Marketplace terkelola, Anda harus menghapusnya dari semua ACL web di dalam AWS WAF dan dalam AWS WAF kebijakan Firewall Manager apa pun, selain berhenti berlangganan. Jika Anda berhenti berlangganan dari grup aturan AWS Marketplace terkelola tetapi tidak menghapusnya dari ACL web, Anda akan terus dikenakan biaya untuk langganan tersebut.

Untuk berhenti berlangganan dari grup aturan AWS Marketplace terkelola

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

2. Hapus grup aturan dari semua ACL web. Untuk informasi selengkapnya, lihat Mengedit ACL web.
3. Di panel navigasi, pilih AWS Marketplace.
4. Pilih Kelola langganan Anda.
5. Pilih Batalkan langganan di samping nama grup aturan tempat Anda ingin berhenti berlangganan.
6. Pilih Ya, batalkan langganan.

Grup aturan pemecahan masalah AWS Marketplace

Jika Anda menemukan bahwa grup AWS Marketplace aturan memblokir lalu lintas yang sah, Anda dapat memecahkan masalah dengan melakukan langkah-langkah berikut.

Untuk memecahkan masalah grup aturan AWS Marketplace

1. Ganti tindakan untuk menghitung aturan yang memblokir lalu lintas yang sah. Anda dapat mengidentifikasi aturan mana yang memblokir permintaan tertentu menggunakan permintaan AWS WAF sampel atau AWS WAF log. Anda dapat mengidentifikasi aturan dengan melihat `ruleGroupId` bidang di log atau permintaan sampel. `RuleWithinRuleGroup` Anda dapat mengidentifikasi aturan dalam pola`<Seller Name>#<RuleGroup Name>#<Rule Name>`.
2. Jika menyetel aturan khusus untuk hanya menghitung permintaan tidak menyelesaikan masalah, Anda dapat mengganti semua tindakan aturan atau mengubah tindakan untuk grup AWS Marketplace aturan itu sendiri dari No override ke Override untuk dihitung. Hal ini memungkinkan permintaan web untuk melewati, terlepas dari tindakan aturan individu dalam kelompok aturan.
3. Setelah mengganti tindakan aturan individual atau seluruh tindakan grup AWS Marketplace aturan, hubungi tim dukungan pelanggan penyedia grup aturan untuk memecahkan masalah lebih lanjut. Untuk informasi kontak, lihat daftar grup aturan di halaman daftar produk AWS Marketplace.

Menghubungi AWS dukungan

Untuk masalah dengan AWS WAF atau kelompok aturan yang dikelola oleh AWS, hubungi AWS Support. Untuk masalah dengan grup aturan yang dikelola oleh AWS Marketplace penjual, hubungi tim dukungan pelanggan penyedia. Untuk menemukan informasi kontak, lihat daftar penyedia di AWS Marketplace.

Mengelola grup aturan Anda sendiri

Anda dapat membuat grup aturan sendiri untuk menggunakan kembali kumpulan aturan yang tidak Anda temukan di penawaran grup aturan terkelola atau yang ingin Anda tangani sendiri.

Grup aturan yang Anda buat aturan penahanan seperti halnya ACL web, dan Anda menambahkan aturan ke grup aturan dengan cara yang sama seperti yang Anda lakukan ke ACL web. Ketika Anda membuat grup aturan Anda sendiri, Anda harus menetapkan kapasitas maksimum yang tidak dapat diubah untuk itu.

Topik

Membuat grup aturan

Untuk membuat grup aturan baru, ikuti prosedur di halaman ini.

Untuk membuat grup aturan

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.
2. Di panel navigasi, pilih Grup aturan, lalu Buat grup aturan.
3. Masukkan nama dan deskripsi untuk grup aturan. Anda akan menggunakan ini untuk mengidentifikasi aturan yang ditetapkan untuk mengelolanya dan menggunakannya.

   Jangan gunakan nama yang dimulai dengan `AWSShield`,`PreFM`, atau`PostFM`. String ini dicadangkan atau dapat menyebabkan kebingungan dengan grup aturan yang dikelola untuk Anda oleh layanan lain. Lihat Grup aturan yang disediakan oleh layanan lain.

   > **Note**
   >
   > Anda tidak dapat mengubah nama setelah membuat grup aturan.

4. Untuk Wilayah, pilih Wilayah tempat Anda ingin menyimpan grup aturan. Untuk menggunakan grup aturan di ACL web yang melindungi CloudFront distribusi Amazon, Anda harus menggunakan pengaturan global. Anda juga dapat menggunakan pengaturan global untuk aplikasi regional.
5. Pilih Selanjutnya.
6. Tambahkan aturan ke grup aturan menggunakan panduan pembuat Aturan, sama seperti yang Anda lakukan di manajemen ACL web. Satu-satunya perbedaan adalah Anda tidak dapat menambahkan grup aturan ke grup aturan lain.
7. Untuk Kapasitas, tetapkan maksimum untuk penggunaan unit kapasitas ACL web (WCU) grup aturan. Ini adalah pengaturan yang tidak dapat diubah. Untuk informasi tentang WCU, lihatAWS WAF unit kapasitas ACL web (WCU).

   Saat Anda menambahkan aturan ke grup aturan, panel Tambahkan aturan dan setel kapasitas menampilkan kapasitas minimum yang diperlukan, yang didasarkan pada aturan yang telah Anda tambahkan. Anda dapat menggunakan ini dan rencana future Anda untuk grup aturan untuk membantu memperkirakan kapasitas yang dibutuhkan kelompok aturan.
8. Tinjau pengaturan untuk grup aturan, dan pilih Buat.

Mengedit grup aturan

Untuk menambah atau menghapus aturan dari grup aturan atau mengubah pengaturan konfigurasi, akses grup aturan menggunakan prosedur di halaman ini.

> ⚠ Risiko lalu lintas produksi
>
> Jika Anda mengubah grup aturan yang saat ini Anda gunakan di ACL web, perubahan tersebut akan memengaruhi perilaku ACL web Anda di mana pun itu digunakan. Pastikan untuk menguji dan menyetel semua perubahan dalam lingkungan pementasan atau pengujian sampai Anda merasa nyaman dengan dampak potensial terhadap lalu lintas Anda. Kemudian uji dan sesuaikan aturan Anda yang diperbarui dalam mode hitungan dengan lalu lintas produksi Anda sebelum mengaktifkannya. Untuk panduan, lihat Menguji dan menyetel perlindungan Anda AWS WAF.

Untuk mengedit grup aturan

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.
2. Di panel navigasi, pilih Rule groups (Grup aturan).
3. Pilih nama grup aturan yang ingin Anda edit. Konsol membawa Anda ke halaman grup aturan.
4. Edit grup aturan sesuai kebutuhan. Anda dapat mengedit properti yang dapat diubah grup aturan, mirip dengan yang Anda lakukan selama pembuatan. Konsol menyimpan perubahan Anda saat Anda pergi.

> **Note**
>
> Jika Anda mengubah nama aturan dan Anda ingin nama metrik aturan mencerminkan perubahan, Anda harus memperbarui nama metrik juga. AWS WAF tidak secara otomatis memperbarui nama metrik untuk aturan saat Anda mengubah nama aturan. Anda dapat mengubah nama metrik saat mengedit aturan di konsol, dengan menggunakan editor JSON aturan. Anda juga dapat mengubah kedua nama melalui API dan dalam daftar JSON apa pun yang Anda gunakan untuk menentukan ACL web atau grup aturan.

Inkonsistensi sementara selama pembaruan

Saat Anda membuat atau mengubah ACL web atau AWS WAF sumber daya lainnya, perubahan membutuhkan sedikit waktu untuk menyebar ke semua area tempat sumber daya disimpan. Waktu propagasi bisa dari beberapa detik hingga beberapa menit.

Berikut ini adalah contoh inkonsistensi sementara yang mungkin Anda perhatikan selama propagasi perubahan:

- Setelah Anda membuat ACL web, jika Anda mencoba mengaitkannya dengan sumber daya, Anda mungkin mendapatkan pengecualian yang menunjukkan bahwa ACL web tidak tersedia.
- Setelah Anda menambahkan grup aturan ke ACL web, aturan grup aturan baru mungkin berlaku di satu area di mana ACL web digunakan dan tidak di area lain.
- Setelah mengubah setelan tindakan aturan, Anda mungkin melihat tindakan lama di beberapa tempat dan tindakan baru di tempat lain.

- Setelah Anda menambahkan alamat IP ke set IP yang digunakan dalam aturan pemblokiran, alamat baru mungkin diblokir di satu area sementara masih diizinkan di area lain.

Menggunakan grup aturan Anda di ACL web

Untuk menggunakan grup aturan di ACL web, Anda menambahkannya ke ACL web dalam pernyataan referensi grup aturan.

> **Risiko lalu lintas produksi**
>
> Sebelum Anda menerapkan perubahan di ACL web Anda untuk lalu lintas produksi, uji dan sesuaikan di lingkungan pementasan atau pengujian hingga Anda merasa nyaman dengan potensi dampak terhadap lalu lintas Anda. Kemudian uji dan sesuaikan aturan Anda yang diperbarui dalam mode hitungan dengan lalu lintas produksi Anda sebelum mengaktifkannya. Untuk panduan, lihat Menguji dan menyetel perlindungan Anda AWS WAF.

> **Note**
>
> Menggunakan lebih dari 1.500 WCU dalam ACL web menimbulkan biaya di luar harga ACL web dasar. Untuk informasi selengkapnya, lihat AWS WAF unit kapasitas ACL web (WCU) dan Harga AWS WAF.

Di konsol, saat Anda menambahkan atau memperbarui aturan di ACL web Anda, di halaman Tambahkan aturan dan grup aturan, pilih Tambahkan aturan, lalu pilih Tambahkan aturan dan grup aturan saya sendiri. Kemudian pilih Grup aturan dan pilih grup aturan Anda dari daftar.

Di ACL web Anda, Anda dapat mengubah perilaku grup aturan dan aturannya dengan menetapkan tindakan aturan individual ke Count atau tindakan lainnya. Ini dapat membantu Anda melakukan hal-hal seperti menguji grup aturan, mengidentifikasi positif palsu dari aturan dalam grup aturan, dan menyesuaikan cara grup aturan terkelola menangani permintaan Anda. Untuk informasi selengkapnya, lihat Opsi penggantian tindakan untuk grup aturan.

Jika grup aturan Anda berisi pernyataan berbasis laju, setiap ACL web tempat Anda menggunakan grup aturan memiliki pelacakan dan pengelolaan tarif tersendiri untuk aturan berbasis tarif, terlepas dari ACL web lain tempat Anda menggunakan grup aturan. Untuk informasi selengkapnya, lihat Pernyataan aturan berbasis tarif.

Ketidakkonsistenan sementara selama pembaruan

Saat Anda membuat atau mengubah ACL web atau AWS WAF sumber daya lainnya, perubahan membutuhkan sedikit waktu untuk menyebar ke semua area tempat sumber daya disimpan. Waktu propagasi bisa dari beberapa detik hingga beberapa menit.

Berikut ini adalah contoh inkonsistensi sementara yang mungkin Anda perhatikan selama propagasi perubahan:

- Setelah Anda membuat ACL web, jika Anda mencoba mengaitkannya dengan sumber daya, Anda mungkin mendapatkan pengecualian yang menunjukkan bahwa ACL web tidak tersedia.
- Setelah Anda menambahkan grup aturan ke ACL web, aturan grup aturan baru mungkin berlaku di satu area di mana ACL web digunakan dan tidak di area lain.
- Setelah mengubah setelan tindakan aturan, Anda mungkin melihat tindakan lama di beberapa tempat dan tindakan baru di tempat lain.
- Setelah Anda menambahkan alamat IP ke set IP yang digunakan dalam aturan pemblokiran, alamat baru mungkin diblokir di satu area sementara masih diizinkan di area lain.

Berbagi grup aturan dengan akun lain

Anda dapat membagikan grup aturan dengan acccount lain, untuk digunakan oleh akun tersebut. Anda dapat berbagi dengan satu atau beberapa akun tertentu, dan Anda dapat berbagi dengan semua akun dalam suatu organisasi.

Untuk melakukannya, Anda menggunakan AWS WAF API untuk membuat kebijakan untuk berbagi grup aturan yang Anda inginkan. Untuk informasi selengkapnya, lihat PutPermissionPolicydi Referensi AWS WAF API.

Menghapus grup aturann

Ikuti panduan di bagian ini untuk menghapus grup aturan.

Menghapus set yang direferensikan dan grup aturan

Saat Anda menghapus entitas yang dapat Anda gunakan di ACL web, seperti kumpulan IP, kumpulan pola regex, atau grup aturan, AWS WAF periksa untuk melihat apakah entitas saat ini sedang digunakan di ACL web. Jika menemukan bahwa itu sedang digunakan, AWS WAF memperingatkan Anda. AWS WAF hampir selalu dapat menentukan apakah suatu entitas sedang direferensikan oleh

ACL web. Namun, dalam kasus yang jarang terjadi mungkin DNS Firewall tidak dapat melakukannya. Jika Anda perlu memastikan bahwa saat ini tidak ada yang menggunakan entitas, periksa di ACL web Anda sebelum menghapusnya. Jika entitas adalah kumpulan yang direferensikan, periksa juga apakah tidak ada grup aturan yang menggunakannya.

Untuk menghapus grup aturan

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.
2. Di panel navigasi, pilih Rule groups (Grup aturan).
3. Pilih grup aturan yang ingin Anda hapus, lalu pilih Hapus.

Grup aturan yang disediakan oleh layanan lain

Jika Anda atau administrator di organisasi Anda menggunakan AWS Firewall Manager atau AWS Shield Advanced mengelola perlindungan sumber daya menggunakan AWS WAF, Anda mungkin melihat pernyataan referensi grup aturan ditambahkan ke ACL web di akun Anda.

Nama-nama grup aturan ini dimulai dengan string berikut:

- **`ShieldMitigationRuleGroup`**— Grup aturan ini dikelola oleh AWS Shield Advanced dan digunakan untuk menyediakan mitigasi DDoS lapisan aplikasi otomatis ke lapisan aplikasi yang dilindungi (lapisan 7) sumber daya.

  Saat Anda mengaktifkan mitigasi DDoS lapisan aplikasi otomatis untuk sumber daya yang dilindungi, Shield Advanced menambahkan salah satu grup aturan ini ke ACL web yang telah Anda kaitkan dengan sumber daya. Shield Advanced menetapkan pernyataan referensi grup aturan pengaturan prioritas 10.000.000, sehingga berjalan setelah aturan yang telah Anda konfigurasi di ACL web. Untuk informasi selengkapnya tentang grup aturan ini, lihatMitigasi DDoS lapisan aplikasi otomatis Shield Advanced.

  > **Warning**
  >
  > Jangan mencoba mengelola grup aturan ini secara manual di ACL web Anda. Secara khusus, jangan menghapus pernyataan referensi grup `ShieldMitigationRuleGroup` aturan secara manual dari ACL web Anda. Melakukan hal ini dapat memiliki konsekuensi yang tidak diinginkan untuk semua sumber daya yang terkait dengan ACL web. Sebagai gantinya, gunakan Shield Advanced untuk menonaktifkan mitigasi otomatis untuk sumber

daya yang terkait dengan ACL web. Shield Advanced akan menghapus grup aturan untuk Anda ketika tidak diperlukan untuk mitigasi otomatis.

- **`PREFMManaged`**dan **`POSTFMManaged`** — Kelompok aturan ini dikelola oleh AWS Firewall Manager. Firewall Manager menyediakannya di dalam ACL web yang dibuat dan dikelola oleh Firewall Manager. Nama-nama ACL web dimulai dengan`FMManagedWebACLV2`. Untuk informasi tentang ACL web dan grup aturan ini, lihatAWS WAF kebijakan.

AWS WAF aturan

AWS WAF Aturan menentukan cara memeriksa permintaan web HTTP (S) dan tindakan yang harus diambil pada permintaan saat cocok dengan kriteria inspeksi. Anda mendefinisikan aturan hanya dalam konteks grup aturan atau web ACL.

Aturan tidak ada dengan AWS WAF sendirinya. Mereka bukan AWS sumber daya, dan mereka tidak memiliki Nama Sumber Daya Amazon (ARN). Anda dapat mengakses aturan berdasarkan nama di grup aturan atau ACL web di mana aturan tersebut ditentukan. Anda dapat mengelola aturan dan menyalinnya ke ACL web lain dengan menggunakan tampilan JSON dari grup aturan atau ACL web yang berisi aturan. Anda juga dapat mengelolanya melalui pembuat aturan AWS WAF konsol, yang tersedia untuk ACL web dan grup aturan.

Nama aturan

Setiap aturan membutuhkan nama. Hindari nama yang dimulai dengan `AWS` dan nama yang digunakan untuk grup aturan atau aturan yang dikelola untuk Anda oleh layanan lain. Lihat Grup aturan yang disediakan oleh layanan lain.

> **Note**
>
> Jika Anda mengubah nama aturan dan Anda ingin nama metrik aturan mencerminkan perubahan, Anda harus memperbarui nama metrik juga. AWS WAF tidak secara otomatis memperbarui nama metrik untuk aturan saat Anda mengubah nama aturan. Anda dapat mengubah nama metrik saat mengedit aturan di konsol, dengan menggunakan editor JSON aturan. Anda juga dapat mengubah kedua nama melalui API dan dalam daftar JSON apa pun yang Anda gunakan untuk menentukan ACL web atau grup aturan.

Pernyataan aturan

Setiap aturan juga memerlukan pernyataan aturan yang mendefinisikan bagaimana aturan memeriksa permintaan web. Pernyataan aturan mungkin berisi pernyataan bersarang lainnya pada kedalaman apa pun, tergantung pada aturan dan jenis pernyataan. Beberapa pernyataan aturan mengambil serangkaian kriteria. Misalnya, Anda dapat menentukan hingga 10.000 alamat IP atau rentang alamat IP untuk aturan pencocokan set IP.

Anda dapat menentukan aturan yang memeriksa kriteria seperti berikut:

- Skrip yang cenderung berbahaya. Penyerang menyematkan skrip yang dapat mengeksploitasi kerentanan dalam aplikasi web. Ini dikenal sebagai cross-site scripting (XSS).
- Alamat IP atau rentang alamat tempat permintaan berasal.
- Negara atau lokasi geografis tempat permintaan berasal.
- Panjang bagian tertentu dari permintaan, seperti string query.
- Kode SQL yang kemungkinan berbahaya. Penyerang mencoba mengekstrak data dari database Anda dengan menyematkan kode SQL berbahaya dalam permintaan web. Ini dikenal sebagai injeksi SQL.
- String yang muncul dalam permintaan, misalnya, nilai yang muncul di `User-Agent` header atau string teks yang muncul dalam string kueri. Anda juga dapat menggunakan ekspresi reguler (regex) untuk menentukan string ini.
- Label bahwa aturan sebelumnya di web ACL telah ditambahkan ke permintaan.

Selain pernyataan dengan kriteria inspeksi permintaan web, seperti yang ada di daftar sebelumnya, AWS WAF mendukung pernyataan logis untuk`AND`,`OR`, dan `NOT` yang Anda gunakan untuk menggabungkan pernyataan dalam aturan.

Misalnya, berdasarkan permintaan terbaru yang Anda lihat dari penyerang, Anda dapat membuat aturan dengan `AND` pernyataan logis yang menggabungkan pernyataan bersarang berikut:

- Permintaan datang dari 192.0.2.44.
- Berisi nilai `BadBot` di header `User-Agent`.
- Mereka tampaknya menyertakan kode seperti SQL dalam string kueri.

Dalam hal ini, permintaan web harus mencocokkan semua pernyataan untuk menghasilkan kecocokan untuk tingkat atas`AND`.

Topik

Tindakan aturan

Tindakan aturan memberi tahu AWS WAF apa yang harus dilakukan dengan permintaan web ketika cocok dengan kriteria yang ditentukan dalam aturan. Anda dapat menambahkan perilaku kustom secara opsional ke setiap tindakan aturan.

> **Note**
>
> Tindakan aturan dapat mengakhiri atau tidak mengakhiri. Tindakan penghentian menghentikan evaluasi ACL web dari permintaan dan memungkinkannya melanjutkan ke aplikasi Anda yang dilindungi atau memblokirnya.

Berikut adalah opsi tindakan aturan:

- Allow— AWS WAF memungkinkan permintaan diteruskan ke AWS sumber daya yang dilindungi untuk diproses dan direspon. Ini adalah tindakan penghentian. Dalam aturan yang Anda tentukan, Anda dapat menyisipkan header khusus ke dalam permintaan sebelum meneruskannya ke sumber daya yang dilindungi.
- Block— AWS WAF memblokir permintaan. Ini adalah tindakan penghentian. Secara default, AWS sumber daya Anda yang dilindungi merespons dengan kode `403 (Forbidden)` status HTTP. Dalam aturan yang Anda tentukan, Anda dapat menyesuaikan respons. Saat AWS WAF memblokir permintaan, pengaturan Block tindakan menentukan respons yang dikirim kembali oleh sumber daya yang dilindungi ke klien.
- Count— AWS WAF menghitung permintaan tetapi tidak menentukan apakah akan mengizinkan atau memblokirnya. Ini adalah tindakan yang tidak mengakhiri. AWS WAF terus memproses aturan yang tersisa di ACL web. Dalam aturan yang Anda tentukan, Anda dapat menyisipkan header khusus ke dalam permintaan dan Anda dapat menambahkan label yang dapat dicocokkan dengan aturan lain.

- CAPTCHAdan Challenge — AWS WAF menggunakan teka-teki CAPTCHA dan tantangan diam untuk memverifikasi bahwa permintaan tersebut tidak berasal dari bot, dan AWS WAF menggunakan token untuk melacak respons klien yang berhasil baru-baru ini.

  Teka-teki CAPTCHA dan tantangan diam hanya dapat berjalan ketika browser mengakses titik akhir HTTPS. Klien browser harus berjalan dalam konteks aman untuk mendapatkan token.

  > **Note**
  >
  > Anda akan dikenakan biaya tambahan ketika Anda menggunakan tindakan CAPTCHA atau Challenge aturan di salah satu aturan Anda atau sebagai penggantian tindakan aturan dalam grup aturan. Untuk informasi selengkapnya, silakan lihat Harga AWS WAF.

  Tindakan aturan ini dapat mengakhiri atau tidak mengakhiri, tergantung pada status token dalam permintaan:

  - Non-terminating untuk token yang valid dan belum kedaluwarsa — Jika token valid dan belum kedaluwarsa sesuai dengan CAPTCHA yang dikonfigurasi atau waktu kekebalan tantangan, AWS WAF menangani permintaan yang serupa dengan tindakan. Count AWS WAF terus memeriksa permintaan web berdasarkan aturan yang tersisa di ACL web. Mirip dengan Count konfigurasi, dalam aturan yang Anda tentukan, Anda dapat mengonfigurasi tindakan ini secara opsional dengan header khusus untuk dimasukkan ke dalam permintaan, dan Anda dapat menambahkan label yang dapat dicocokkan dengan aturan lain.
  - Mengakhiri dengan permintaan yang diblokir untuk token yang tidak valid atau kedaluwarsa - Jika token tidak valid atau stempel waktu yang ditunjukkan kedaluwarsa, AWS WAF menghentikan pemeriksaan permintaan web dan memblokir permintaan, mirip dengan tindakan. Block AWS WAF kemudian merespons klien dengan kode respons khusus. SebabCAPTCHA, jika isi permintaan menunjukkan bahwa browser klien dapat menanganinya, AWS WAF mengirimkan teka-teki CAPTCHA dalam JavaScript interstisial, yang dirancang untuk membedakan klien manusia dari bot. Untuk Challenge aksinya, AWS WAF kirimkan JavaScript pengantara dengan tantangan diam yang dirancang untuk membedakan browser normal dari sesi yang dijalankan oleh bot.

  Untuk informasi tambahan, lihat CAPTCHAdan Challenge di AWS WAF.

Untuk informasi tentang menyesuaikan permintaan dan tanggapan, lihatPermintaan dan tanggapan web yang disesuaikan di AWS WAF.

Untuk informasi tentang menambahkan label ke permintaan yang cocok, lihatAWS WAF label pada permintaan web.

Untuk informasi tentang cara ACL web dan pengaturan aturan berinteraksi, lihatEvaluasi aturan dan kelompok aturan ACL Web.

Dasar-dasar pernyataan aturan

Pernyataan aturan adalah bagian dari aturan yang memberi tahu AWS WAF cara memeriksa permintaan web. Ketika AWS WAF menemukan kriteria inspeksi dalam permintaan web, kami mengatakan bahwa permintaan web cocok dengan pernyataan tersebut. Setiap pernyataan aturan menentukan apa yang harus dicari dan bagaimana, sesuai dengan jenis pernyataan.

Setiap aturan AWS WAF memiliki satu pernyataan aturan tingkat atas, yang dapat berisi pernyataan lain. Pernyataan aturan bisa sangat sederhana. Misalnya, Anda dapat memiliki pernyataan yang menyediakan sekumpulan negara asal untuk memeriksa permintaan web Anda atau Anda dapat memiliki pernyataan aturan di ACL web yang hanya mereferensikan grup aturan. Pernyataan aturan juga bisa sangat kompleks. Misalnya, Anda dapat memiliki pernyataan yang menggabungkan banyak pernyataan lain dengan logisAND,OR, dan NOT pernyataan.

Untuk sebagian besar aturan, Anda dapat menambahkan AWS WAF pelabelan khusus ke permintaan yang cocok. Aturan dalam grup aturan Aturan AWS Terkelola menambahkan label ke permintaan yang cocok. Label yang ditambahkan aturan memberikan informasi tentang permintaan ke aturan yang dievaluasi nanti di ACL web dan juga di AWS WAF log dan metrik. Untuk informasi tentang pelabelan, lihat AWS WAF label pada permintaan web danPernyataan aturan pencocokan label.

Pernyataan aturan bersarang

AWS WAF mendukung bersarang untuk banyak pernyataan aturan, tetapi tidak untuk semua. Misalnya, Anda tidak dapat membuat pernyataan grup aturan di dalam pernyataan lain. Anda perlu menggunakan nesting untuk beberapa skenario, seperti pernyataan scope-down dan pernyataan logis. Daftar pernyataan aturan dan detail aturan berikut menjelaskan kemampuan dan persyaratan bersarang untuk setiap kategori dan aturan.

Editor visual untuk aturan di konsol hanya mendukung satu tingkat penyarangan untuk pernyataan aturan. Misalnya, Anda dapat menyarangkan banyak jenis pernyataan di dalam logika AND atau OR aturan, tetapi Anda tidak dapat membuat sarang AND atau OR aturan lain, karena itu memerlukan tingkat penyarangan kedua. Untuk mengimplementasikan beberapa level nesting, berikan definisi aturan di JSON, baik melalui editor aturan JSON di konsol atau melalui API.

Topik

- Spesifikasi dan penanganan komponen permintaan web
- Pernyataan cakupan ke bawah
- Pernyataan yang mereferensikan kumpulan atau grup aturan

Spesifikasi dan penanganan komponen permintaan web

Bagian ini menjelaskan pengaturan yang dapat Anda tentukan dalam pernyataan aturan yang memeriksa komponen permintaan web. Untuk informasi tentang penggunaan, lihat pernyataan aturan individual diPernyataan aturan pertandingan.

Subset dari komponen permintaan web ini juga dapat digunakan dalam aturan berbasis tarif, sebagai kunci agregasi permintaan kustom. Untuk informasi, lihat Opsi dan kunci agregasi aturan berbasis tarif.

Untuk pengaturan komponen permintaan, Anda menentukan jenis komponen itu sendiri, dan opsi tambahan apa pun, tergantung pada jenis komponen. Misalnya, saat memeriksa jenis komponen yang berisi teks, Anda dapat menerapkan transformasi teks sebelum memeriksanya.

> **Note**
>
> Kecuali dinyatakan lain, jika permintaan web tidak memiliki komponen permintaan yang ditentukan dalam pernyataan aturan, AWS WAF mengevaluasi permintaan sebagai tidak cocok dengan kriteria aturan.

Daftar Isi

  - String kueri
  - Parameter kueri tunggal
  - Semua parameter kueri
  - Tubuh
  - Tubuh JSON
- Alamat IP yang diteruskan
- Opsi untuk memeriksa header pseudo HTTP/2
- Opsi transformasi teks

Minta opsi komponen

Bagian ini menjelaskan komponen permintaan web yang dapat Anda tentukan untuk diperiksa. Anda menentukan komponen permintaan untuk pernyataan aturan kecocokan yang mencari pola di dalam permintaan web. Jenis pernyataan ini termasuk pencocokan string, pencocokan regex, batasan ukuran, dan pernyataan serangan injeksi SQL. Untuk informasi tentang cara menggunakan setelan komponen permintaan ini, lihat pernyataan aturan individual di Pernyataan aturan pertandingan

Kecuali dinyatakan lain, jika permintaan web tidak memiliki komponen permintaan yang ditentukan dalam pernyataan aturan, AWS WAF mengevaluasi permintaan sebagai tidak cocok dengan kriteria aturan.

> **Note**
>
> Anda menentukan komponen permintaan tunggal untuk setiap pernyataan aturan yang memerlukannya. Untuk memeriksa lebih dari satu komponen permintaan, buat pernyataan aturan untuk setiap komponen.

Dokumentasi AWS WAF konsol dan API memberikan panduan untuk pengaturan komponen permintaan di lokasi berikut:

- Pembuat aturan di konsol — Dalam pengaturan Pernyataan untuk jenis aturan reguler, pilih komponen yang ingin Anda periksa dalam dialog Inspect di bawah Minta komponen.
- Isi pernyataan API - `FieldToMatch`

Sisa bagian ini menjelaskan opsi untuk bagian permintaan web untuk diperiksa.

Topik

Metode HTTP

Memeriksa metode HTTP untuk permintaan. Metode HTTP menunjukkan jenis operasi yang permintaan web meminta sumber daya yang dilindungi untuk melakukan, seperti `POST` atau`GET`.

Header tunggal

Memeriksa satu header bernama dalam permintaan.

Untuk opsi ini, Anda menentukan nama header, misalnya, `User-Agent` atau`Referer`. Pencocokan string untuk nama tersebut tidak peka huruf besar/kecil.

Semua header

Memeriksa semua header permintaan, termasuk cookie. Anda dapat menerapkan filter untuk memeriksa subset dari semua header.

Untuk opsi ini, Anda memberikan spesifikasi berikut:

- Pola kecocokan — Filter yang digunakan untuk mendapatkan subset header untuk diperiksa. AWS WAF mencari pola-pola ini di tombol header.

  Pengaturan pola kecocokan dapat berupa salah satu dari berikut ini:

  - Semua — Cocokkan semua kunci. Evaluasi kriteria pemeriksaan aturan untuk semua header.
  - Header yang dikecualikan - Periksa hanya header yang kuncinya tidak cocok dengan string yang Anda tentukan di sini. Pencocokan string untuk kunci tidak peka huruf besar/kecil.
  - Header yang disertakan - Periksa hanya header yang memiliki kunci yang cocok dengan salah satu string yang Anda tentukan di sini. Pencocokan string untuk kunci tidak peka huruf besar/kecil.
- Lingkup kecocokan — Bagian-bagian header yang AWS WAF harus diperiksa dengan kriteria pemeriksaan aturan. Anda dapat menentukan Kunci, Nilai, atau Semua untuk memeriksa kunci dan nilai untuk kecocokan.

  Semua tidak memerlukan kecocokan untuk ditemukan di kunci dan kecocokan yang dapat ditemukan dalam nilai. Ini membutuhkan kecocokan untuk ditemukan di kunci atau nilai atau keduanya. Untuk meminta kecocokan dalam kunci dan nilai, gunakan `AND` pernyataan logis untuk menggabungkan dua aturan kecocokan, satu yang memeriksa kunci dan yang lain yang memeriksa nilai.
- Oversize handling — Bagaimana AWS WAF seharusnya menangani permintaan yang memiliki data header yang lebih besar dari yang AWS WAF dapat diperiksa. AWS WAF dapat memeriksa paling banyak 8 KB pertama (8.192 byte) dari header permintaan dan paling banyak 200 header pertama. Konten tersedia untuk diperiksa AWS WAF hingga batas pertama yang tercapai. Anda dapat memilih untuk melanjutkan inspeksi, atau melewati inspeksi dan menandai permintaan sebagai cocok atau tidak cocok dengan aturan. Untuk informasi selengkapnya tentang penanganan konten yang terlalu besar, lihat[Penanganan komponen permintaan kebesaran di AWS WAF](#).

Urutan header

Periksa string yang berisi daftar nama header permintaan, diurutkan seperti yang muncul di permintaan web yang AWS WAF menerima untuk inspeksi. AWS WAF menghasilkan string dan kemudian menggunakannya sebagai bidang untuk mencocokkan komponen dalam pemeriksaannya. AWS WAF memisahkan nama header dalam string dengan titik dua dan tanpa spasi tambahan, misalnya. `host:user-agent:accept:authorization:referer`

Untuk opsi ini, Anda memberikan spesifikasi berikut:

- Oversize handling — Bagaimana AWS WAF seharusnya menangani permintaan yang memiliki data header yang lebih banyak atau lebih besar daripada yang AWS WAF dapat diperiksa. AWS WAF dapat memeriksa paling banyak 8 KB pertama (8.192 byte) dari header permintaan dan

paling banyak 200 header pertama. Konten tersedia untuk diperiksa AWS WAF hingga batas pertama yang tercapai. Anda dapat memilih untuk terus memeriksa header yang tersedia, atau melewati inspeksi dan menandai permintaan sebagai cocok atau tidak cocok dengan aturan. Untuk informasi selengkapnya tentang penanganan konten yang terlalu besar, lihatPenanganan komponen permintaan kebesaran di AWS WAF.

Cookie

Memeriksa semua cookie permintaan. Anda dapat menerapkan filter untuk memeriksa subset dari semua cookie.

Untuk opsi ini, Anda memberikan spesifikasi berikut:

- Pola kecocokan — Filter yang digunakan untuk mendapatkan subset cookie untuk diperiksa. AWS WAF mencari pola-pola ini di kunci cookie.

  Pengaturan pola kecocokan dapat berupa salah satu dari berikut ini:

  - Semua — Cocokkan semua kunci. Evaluasi kriteria pemeriksaan aturan untuk semua cookie.
  - Cookie yang dikecualikan — Periksa hanya cookie yang kuncinya tidak cocok dengan string apa pun yang Anda tentukan di sini. Pencocokan string untuk kunci peka huruf besar/kecil dan harus tepat.
  - Cookie yang disertakan — Periksa hanya cookie yang memiliki kunci yang cocok dengan salah satu string yang Anda tentukan di sini. Pencocokan string untuk kunci peka huruf besar/kecil dan harus tepat.
- Lingkup kecocokan — Bagian-bagian cookie yang AWS WAF harus diperiksa dengan kriteria pemeriksaan aturan. Anda dapat menentukan Kunci, Nilai, atau Semua untuk kedua kunci dan nilai.

  Semua tidak memerlukan kecocokan untuk ditemukan di kunci dan kecocokan yang dapat ditemukan dalam nilai. Ini membutuhkan kecocokan untuk ditemukan di kunci atau nilai atau keduanya. Untuk meminta kecocokan dalam kunci dan nilai, gunakan `AND` pernyataan logis untuk menggabungkan dua aturan kecocokan, satu yang memeriksa kunci dan yang lain yang memeriksa nilai.
- Oversize handling — Bagaimana AWS WAF seharusnya menangani permintaan yang memiliki data cookie yang lebih besar dari yang AWS WAF dapat diperiksa. AWS WAF dapat memeriksa paling banyak 8 KB pertama (8.192 byte) dari cookie permintaan dan paling banyak 200 cookie pertama. Konten tersedia untuk diperiksa AWS WAF hingga batas pertama yang

tercapai. Anda dapat memilih untuk melanjutkan inspeksi, atau melewati inspeksi dan menandai permintaan sebagai cocok atau tidak cocok dengan aturan. Untuk informasi selengkapnya tentang penanganan konten yang terlalu besar, lihatPenanganan komponen permintaan kebesaran di AWS WAF.

Jalur URI

Memeriksa bagian URL yang mengidentifikasi sumber daya, misalnya,. `/images/daily-ad.jpg` Untuk selengkapnya, lihat Uniform Resource Identifier (URI): Generic Syntax.

Jika Anda tidak menggunakan transformasi teks dengan opsi ini, AWS WAF tidak menormalkan URI dan memeriksanya persis seperti yang diterimanya dari klien dalam permintaan. Untuk informasi tentang transformasi teks, lihatOpsi transformasi teks.

Sidik jari JA3

Memeriksa sidik jari JA3 permintaan.

> **Note**
>
> Pemeriksaan sidik jari JA3 hanya tersedia untuk CloudFront distribusi Amazon dan Application Load Balancer.

Sidik jari JA3 adalah hash 32 karakter yang berasal dari TLS Client Hello dari permintaan yang masuk. Sidik jari ini berfungsi sebagai pengenal unik untuk konfigurasi TLS klien. AWS WAF menghitung dan mencatat sidik jari ini untuk setiap permintaan yang memiliki cukup informasi TLS Client Hello untuk perhitungan. Hampir semua permintaan web menyertakan informasi ini.

Cara mendapatkan sidik jari JA3 untuk klien

Anda dapat memperoleh sidik jari JA3 untuk permintaan klien dari log ACL web. Jika AWS WAF mampu menghitung sidik jari, itu termasuk dalam log. Untuk informasi tentang bidang logging, lihatBidang log.

Persyaratan pernyataan aturan

Anda dapat memeriksa sidik jari JA3 hanya di dalam pernyataan pencocokan string yang diatur agar sama persis dengan string yang Anda berikan. Berikan string sidik jari JA3 dari log dalam spesifikasi

pernyataan kecocokan string Anda, agar sesuai dengan permintaan future yang memiliki konfigurasi TLS yang sama. Untuk informasi tentang pernyataan kecocokan string, lihatPernyataan aturan kecocokan string.

Anda harus memberikan perilaku fallback untuk pernyataan aturan ini. Perilaku fallback adalah status pencocokan yang ingin Anda tetapkan AWS WAF ke permintaan web jika tidak dapat menghitung AWS WAF sidik jari JA3. Jika Anda memilih untuk mencocokkan, AWS WAF memperlakukan permintaan sebagai pencocokan pernyataan aturan dan menerapkan tindakan aturan ke permintaan. Jika Anda memilih untuk tidak cocok, AWS WAF memperlakukan permintaan sebagai tidak cocok dengan pernyataan aturan.

Untuk menggunakan opsi pencocokan ini, Anda harus mencatat lalu lintas ACL web Anda. Untuk informasi, lihat Pencatatan AWS WAF lalu lintas ACL web.

String kueri

Memeriksa bagian URL yang muncul setelah ? karakter, jika ada.

> **Note**
>
> Untuk pernyataan pencocokan skrip lintas situs, sebaiknya pilih Semua parameter kueri, bukan string Kueri. Memilih Semua parameter kueri menambahkan 10 WCU ke biaya dasar.

Parameter kueri tunggal

Memeriksa parameter query tunggal yang telah Anda definisikan sebagai bagian dari string query. AWS WAF memeriksa nilai parameter yang Anda tentukan.

Untuk opsi ini, Anda juga menentukan argumen Query. Misalnya, jika URL-nya`www.xyz.com?UserName=abc&SalesRegion=seattle`, Anda dapat menentukan `UserName` atau `SalesRegion` untuk argumen kueri. Panjang maksimum untuk nama argumen adalah 30 karakter. Nama ini tidak peka huruf besar/kecil, jadi jika Anda menentukan`UserName`, AWS WAF cocok dengan semua variasi`UserName`, termasuk `username` dan`UsERName`.

Jika string kueri berisi lebih dari satu contoh argumen kueri yang telah Anda tentukan, AWS WAF periksa semua nilai untuk kecocokan, menggunakan OR logika. Misalnya, di URL`www.xyz.com?SalesRegion=boston&SalesRegion=seattle`, AWS WAF mengevaluasi nama yang telah Anda tentukan terhadap `boston` dan`seattle`. Jika keduanya cocok, inspeksi adalah kecocokan.

Semua parameter kueri

Memeriksa semua parameter kueri dalam permintaan. Ini mirip dengan pilihan komponen parameter kueri tunggal, tetapi AWS WAF memeriksa nilai semua argumen dalam string kueri. Misalnya, jika URL-nya`www.xyz.com?UserName=abc&SalesRegion=seattle`, AWS WAF memicu kecocokan jika nilai `UserName` atau `SalesRegion` cocok dengan kriteria inspeksi.

Memilih opsi ini menambahkan 10 WCU ke biaya dasar.

Tubuh

Memeriksa badan permintaan, dievaluasi sebagai teks biasa. Anda juga dapat mengevaluasi tubuh sebagai JSON menggunakan jenis JSON konten.

Badan permintaan adalah bagian dari permintaan yang segera mengikuti header permintaan. Ini berisi data tambahan yang diperlukan untuk permintaan web, misalnya, data dari formulir.

- Di konsol, Anda memilih ini di bawah pilihan Request option Body, dengan memilih pilihan Jenis konten Teks biasa.
- Di API, dalam `FieldToMatch` spesifikasi aturan, Anda menentukan `Body` untuk memeriksa isi permintaan sebagai teks biasa.

Untuk Application Load Balancer dan AWS AppSync, AWS WAF dapat memeriksa 8 KB pertama dari badan permintaan. Untuk CloudFront, API Gateway, Amazon Cognito, App Runner, dan Akses Terverifikasi, secara default, AWS WAF dapat memeriksa 16 KB pertama, dan Anda dapat meningkatkan batas hingga 64 KB dalam konfigurasi ACL web Anda. Untuk informasi selengkapnya, lihat Mengelola batas ukuran inspeksi tubuh.

Anda harus menentukan penanganan oversize untuk jenis komponen ini. Oversize handling mendefinisikan bagaimana AWS WAF menangani permintaan yang memiliki data body yang lebih besar dari yang AWS WAF dapat diperiksa. Anda dapat memilih untuk melanjutkan inspeksi, atau melewati inspeksi dan menandai permintaan sebagai cocok atau tidak cocok dengan aturan. Untuk informasi selengkapnya tentang penanganan konten yang terlalu besar, lihatPenanganan komponen permintaan kebesaran di AWS WAF.

Anda juga dapat mengevaluasi tubuh sebagai JSON yang diurai. Untuk informasi tentang ini, lihat bagian berikut.

Tubuh JSON

Memeriksa badan permintaan, dievaluasi sebagai JSON. Anda juga dapat mengevaluasi tubuh sebagai teks biasa.

Badan permintaan adalah bagian dari permintaan yang segera mengikuti header permintaan. Ini berisi data tambahan yang diperlukan untuk permintaan web, misalnya, data dari formulir.

- Di konsol, Anda memilih ini di bawah pilihan opsi Request Body, dengan memilih pilihan Jenis konten JSON.
- Di API, dalam `FieldToMatch` spesifikasi aturan, Anda menentukan`JsonBody`.

Untuk Application Load Balancer dan AWS AppSync, AWS WAF dapat memeriksa 8 KB pertama dari badan permintaan. Untuk CloudFront, API Gateway, Amazon Cognito, App Runner, dan Akses Terverifikasi, secara default, AWS WAF dapat memeriksa 16 KB pertama, dan Anda dapat meningkatkan batas hingga 64 KB dalam konfigurasi ACL web Anda. Untuk informasi selengkapnya, lihat Mengelola batas ukuran inspeksi tubuh.

Anda harus menentukan penanganan oversize untuk jenis komponen ini. Oversize handling mendefinisikan bagaimana AWS WAF menangani permintaan yang memiliki data body yang lebih besar dari yang AWS WAF dapat diperiksa. Anda dapat memilih untuk melanjutkan inspeksi, atau melewati inspeksi dan menandai permintaan sebagai cocok atau tidak cocok dengan aturan. Untuk informasi selengkapnya tentang penanganan konten yang terlalu besar, lihatPenanganan komponen permintaan kebesaran di AWS WAF.

Memilih opsi ini menggandakan WCU biaya dasar pernyataan pertandingan. Misalnya, jika biaya dasar pernyataan kecocokan adalah 5 WCU tanpa penguraian JSON, menggunakan penguraian JSON menggandakan biaya menjadi 10 WCU.

Langkah dan opsi untuk inspeksi tubuh JSON

Saat AWS WAF memeriksa badan permintaan web sebagai JSON, ia melakukan langkah-langkah untuk mengurai tubuh dan mengekstrak elemen JSON untuk diperiksa. Berikut ini mencantumkan langkah-langkah dan opsi konfigurasi tambahan untuk jenis komponen permintaan ini.

1. Parse isi isi tubuh - AWS WAF mem-parsing isi badan permintaan web untuk mengekstrak elemen JSON untuk diperiksa. AWS WAF melakukan yang terbaik untuk mengurai seluruh isi tubuh, tetapi penguraian dapat gagal untuk berbagai status kesalahan dalam konten. Contohnya termasuk

karakter yang tidak valid, kunci duplikat, pemotongan, dan konten yang simpul akarnya bukan objek atau array.

Opsi Body parsing fallback behavior menentukan AWS WAF apa yang dilakukan jika gagal mengurai body JSON sepenuhnya:

- Tidak ada (perilaku default) - AWS WAF mengevaluasi konten hanya sampai pada titik di mana ia mengalami kesalahan penguraian.
- Evaluasi sebagai string - Periksa tubuh sebagai teks biasa. AWS WAF menerapkan transformasi teks dan kriteria inspeksi yang Anda tentukan untuk inspeksi JSON ke string teks isi.
- Cocokkan - Perlakukan permintaan web sebagai pencocokan pernyataan aturan. AWS WAF menerapkan tindakan aturan untuk permintaan.
- Tidak cocok - Perlakukan permintaan web sebagai tidak cocok dengan pernyataan aturan.

> **Note**
>
> Perilaku fallback ini hanya terpicu saat AWS WAF menemukan kesalahan saat mengurai string JSON.

Parsing tidak sepenuhnya memvalidasi JSON

AWS WAF penguraian tidak sepenuhnya memvalidasi string JSON input, sehingga penguraian dapat berhasil bahkan untuk JSON yang tidak valid.

Misalnya, AWS WAF mem-parsing JSON yang tidak valid berikut tanpa kesalahan:

- Kehilangan koma: `{"key1":"value1""key2":"value2"}`
- Kehilangan titik dua: `{"key1":"value1","key2""value2"}`
- Titik dua ekstra: `{"key1"::"value1","key2""value2"}`

Untuk kasus-kasus seperti ini di mana penguraian berhasil tetapi hasilnya tidak sepenuhnya valid JSON, hasil dari langkah-langkah selanjutnya dalam evaluasi dapat bervariasi. Ekstraksi mungkin kehilangan beberapa elemen, atau evaluasi aturan mungkin memiliki hasil yang tidak terduga. Kami menyarankan Anda memvalidasi JSON yang Anda terima dalam aplikasi Anda dan menangani JSON yang tidak valid sesuai kebutuhan.

2. Ekstrak elemen JSON - AWS WAF mengidentifikasi subset elemen JSON untuk memeriksa sesuai dengan pengaturan Anda:

- Pilihan lingkup pencocokan JSON menentukan jenis elemen dalam JSON yang AWS WAF harus memeriksa.

  Anda dapat menentukan Kunci, Nilai, atau Semua untuk kedua kunci dan nilai.

  Semua tidak memerlukan kecocokan untuk ditemukan di kunci dan kecocokan yang dapat ditemukan dalam nilai. Ini membutuhkan kecocokan untuk ditemukan di kunci atau nilai atau keduanya. Untuk meminta kecocokan dalam kunci dan nilai, gunakan AND pernyataan logis untuk menggabungkan dua aturan kecocokan, satu yang memeriksa kunci dan yang lain yang memeriksa nilai.
- Pilihan Konten untuk memeriksa menentukan bagaimana untuk menyaring elemen diatur ke subset yang Anda ingin AWS WAF memeriksa.

  Anda harus menentukan salah satu dari berikut ini:

  - Konten JSON penuh - Evaluasi semua elemen.
  - Hanya elemen yang disertakan - Evaluasi hanya elemen yang jalurnya cocok dengan kriteria JSON Pointer yang Anda berikan. Jangan gunakan opsi ini untuk menunjukkan semua jalur di JSON. Sebagai gantinya, gunakan konten JSON Penuh.

    Untuk informasi tentang sintaks JSON Pointer, lihat dokumentasi Internet Engineering Task Force (IETF) JavaScript Object Notation (JSON) Pointer.

    Misalnya, di konsol, Anda dapat memberikan yang berikut:

    ```
    /dogs/0/name
    /dogs/1/name
    ```

    Di API atau CLI, Anda dapat memberikan yang berikut:

    ```
    "IncludedPaths": ["/dogs/0/name", "/dogs/1/name"]
    ```

Misalnya, katakan bahwa pengaturan Konten untuk memeriksa hanya elemen yang disertakan, dan pengaturan elemen yang disertakan adalah`/a/b`.

Untuk contoh berikut badan JSON:

```
{
  "a":{
```

```
    "c":"d",
    "b":{
      "e":{
        "f":"g"
      }
    }
  }
}
```

Set elemen yang AWS WAF akan memeriksa untuk setiap pengaturan lingkup kecocokan JSON tercantum di bawah ini. Perhatikan bahwa kuncib, yang merupakan bagian dari jalur elemen yang disertakan, tidak dievaluasi.

- Semua:`e`, `f`, dang.
- Kunci: `e` dan`f`.
- Nilai:`g`.

3. Periksa set elemen JSON - AWS WAF menerapkan transformasi teks apa pun yang telah Anda tentukan ke elemen JSON yang diekstraksi dan kemudian mencocokkan elemen yang dihasilkan yang ditetapkan dengan kriteria pencocokan pernyataan aturan. Ini adalah perilaku transformasi dan evaluasi yang sama seperti untuk komponen permintaan web lainnya. Jika salah satu elemen JSON yang diekstraksi cocok, permintaan web cocok untuk aturan tersebut.

Alamat IP yang diteruskan

Bagian ini berlaku untuk pernyataan aturan yang menggunakan alamat IP permintaan web. Secara default, AWS WAF menggunakan alamat IP dari asal permintaan web. Namun, jika permintaan web melewati satu atau lebih proxy atau penyeimbang beban, asal permintaan web akan berisi alamat proxy terakhir, dan bukan alamat asal klien. Dalam hal ini, alamat klien yang berasal biasanya diteruskan di header HTTP lain. Header ini biasanya `X-Forwarded-For` (XFF), tetapi bisa berbeda.

Pernyataan aturan yang menggunakan alamat IP

Pernyataan aturan yang menggunakan alamat IP adalah sebagai berikut:

- Pertandingan set IP- Memeriksa alamat IP untuk kecocokan dengan alamat yang ditentukan dalam set IP.
- Pertandingan geografis- Menggunakan alamat IP untuk menentukan negara dan wilayah asal dan mencocokkan negara asal dengan daftar negara.

- Pernyataan aturan berbasis tarif- Dapat mengumpulkan permintaan dengan alamat IP mereka untuk memastikan bahwa tidak ada alamat IP individu yang mengirim permintaan pada tingkat yang terlalu tinggi. Anda dapat menggunakan agregasi alamat IP dengan sendirinya atau dalam kombinasi dengan kunci agregasi lainnya.

Anda dapat menginstruksikan AWS WAF untuk menggunakan alamat IP yang diteruskan untuk pernyataan aturan ini, baik dari `X-Forwarded-For` header atau dari header HTTP lain, alih-alih menggunakan asal permintaan web. Untuk detail tentang cara memberikan spesifikasi, lihat panduan untuk setiap jenis pernyataan aturan.

> **Note**
>
> Jika header yang Anda tentukan tidak ada dalam permintaan, AWS WAF tidak menerapkan aturan untuk permintaan web sama sekali.

Perilaku mundur

Saat Anda menggunakan alamat IP yang diteruskan, Anda menunjukkan status kecocokan AWS WAF untuk ditetapkan ke permintaan web jika permintaan tidak memiliki alamat IP yang valid di posisi yang ditentukan:

- MATCH - Perlakukan permintaan web sebagai pencocokan pernyataan aturan. AWS WAF menerapkan tindakan aturan untuk permintaan.
- NO MATCH - Perlakukan permintaan web sebagai tidak cocok dengan pernyataan aturan.

Alamat IP yang digunakan dalam Kontrol AWS WAF Bot

Grup aturan terkelola Bot Control memverifikasi bot menggunakan alamat IP dari. AWS WAF Jika Anda menggunakan Kontrol Bot dan Anda telah memverifikasi bot yang merutekan melalui proxy atau penyeimbang beban, Anda harus secara eksplisit mengizinkannya menggunakan aturan khusus. Misalnya, Anda dapat mengonfigurasi aturan pencocokan set IP kustom yang menggunakan alamat IP yang diteruskan untuk mendeteksi dan mengizinkan bot terverifikasi Anda. Anda dapat menggunakan aturan untuk menyesuaikan manajemen bot Anda dalam beberapa cara. Untuk informasi dan contoh, lihat AWS WAF Kontrol Bot.

Pertimbangan umum untuk menggunakan alamat IP yang diteruskan

Sebelum Anda menggunakan alamat IP yang diteruskan, perhatikan peringatan umum berikut:

- Header dapat dimodifikasi oleh proxy di sepanjang jalan, dan proxy mungkin menangani header dengan cara yang berbeda.
- Penyerang mungkin mengubah isi header dalam upaya untuk melewati AWS WAF inspeksi.
- Alamat IP di dalam header bisa cacat atau tidak valid.
- Header yang Anda tentukan mungkin tidak ada sama sekali dalam permintaan.

Pertimbangan untuk menggunakan alamat IP yang diteruskan dengan AWS WAF

Daftar berikut menjelaskan persyaratan dan peringatan untuk menggunakan alamat IP yang diteruskan di: AWS WAF

- Untuk aturan tunggal apa pun, Anda dapat menentukan satu header untuk alamat IP yang diteruskan. Spesifikasi header tidak peka huruf besar/kecil.
- Untuk pernyataan aturan berbasis kecepatan, setiap pernyataan pelingkupan bersarang tidak mewarisi konfigurasi IP yang diteruskan. Tentukan konfigurasi untuk setiap pernyataan yang menggunakan alamat IP yang diteruskan.
- Untuk aturan geo match dan rate-based, AWS WAF gunakan alamat pertama di header. Misalnya, jika header berisi `10.1.1.1, 127.0.0.0, 10.10.10.10` AWS WAF kegunaan `10.1.1.1`
- Untuk kecocokan set IP, Anda menunjukkan apakah akan cocok dengan alamat pertama, terakhir, atau alamat apa pun di header. Jika Anda menentukan, AWS WAF periksa semua alamat di header untuk kecocokan, hingga 10 alamat. Jika header berisi lebih dari 10 alamat, AWS WAF periksa 10 terakhir.
- Header yang berisi beberapa alamat harus menggunakan pemisah koma di antara alamat. Jika permintaan menggunakan pemisah selain koma, AWS WAF anggap alamat IP di header salah bentuk.
- Jika alamat IP di dalam header cacat atau tidak valid, AWS WAF menetapkan permintaan web sebagai cocok dengan aturan atau tidak cocok, sesuai dengan perilaku fallback yang Anda tentukan dalam konfigurasi IP yang diteruskan.
- Jika header yang Anda tentukan tidak ada dalam permintaan, AWS WAF tidak menerapkan aturan pada permintaan sama sekali. Ini AWS WAF berarti itu tidak menerapkan tindakan aturan dan tidak menerapkan perilaku fallback.
- Pernyataan aturan yang menggunakan header IP yang diteruskan untuk alamat IP tidak akan menggunakan alamat IP yang dilaporkan oleh asal permintaan web.

Praktik terbaik untuk menggunakan alamat IP yang diteruskan dengan AWS WAF

Saat Anda menggunakan alamat IP yang diteruskan, gunakan praktik terbaik berikut:

- Pertimbangkan dengan cermat semua kemungkinan status header permintaan Anda sebelum mengaktifkan konfigurasi IP yang diteruskan. Anda mungkin perlu menggunakan lebih dari satu aturan untuk mendapatkan perilaku yang Anda inginkan.
- Untuk memeriksa beberapa header IP yang diteruskan atau untuk memeriksa asal permintaan web dan header IP yang diteruskan, gunakan satu aturan untuk setiap sumber alamat IP.
- Untuk memblokir permintaan web yang memiliki header tidak valid, setel tindakan aturan untuk memblokir dan mengatur perilaku fallback untuk konfigurasi IP yang diteruskan agar cocok.

Contoh JSON untuk alamat IP yang diteruskan

Pernyataan geo match berikut hanya cocok jika `X-Forwarded-For` header berisi IP yang negara asalnya adalah`US`:

```
{
  "Name": "XFFTestGeo",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "XFFTestGeo"
  },
  "Statement": {
    "GeoMatchStatement": {
      "CountryCodes": [
        "US"
      ],
      "ForwardedIPConfig": {
        "HeaderName": "x-forwarded-for",
        "FallbackBehavior": "MATCH"
      }
    }
  }
}
```

Aturan berbasis laju berikut mengumpulkan permintaan berdasarkan IP pertama di header. `X-Forwarded-For` Aturan hanya menghitung permintaan yang cocok dengan pernyataan kecocokan geografis bersarang, dan hanya memblokir permintaan yang cocok dengan pernyataan kecocokan geografis. Pernyataan geo match bersarang juga menggunakan `X-Forwarded-For` header untuk menentukan apakah alamat IP menunjukkan negara asal. US Jika ya, atau jika header ada tetapi cacat, pernyataan geo match mengembalikan kecocokan.

```
{
  "Name": "XFFTestRateGeo",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "XFFTestRateGeo"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": "100",
      "AggregateKeyType": "FORWARDED_IP",
      "ScopeDownStatement": {
        "GeoMatchStatement": {
          "CountryCodes": [
            "US"
          ],
          "ForwardedIPConfig": {
            "HeaderName": "x-forwarded-for",
            "FallbackBehavior": "MATCH"
          }
        }
      },
      "ForwardedIPConfig": {
        "HeaderName": "x-forwarded-for",
        "FallbackBehavior": "MATCH"
      }
    }
  }
}
```

Opsi untuk memeriksa header pseudo HTTP/2

AWS Sumber daya yang dilindungi yang mendukung lalu lintas HTTP/2 tidak meneruskan header semu HTTP/2 AWS WAF untuk diperiksa, tetapi mereka menyediakan konten header semu dalam komponen permintaan web yang memeriksa. AWS WAF

Anda dapat menggunakan AWS WAF untuk memeriksa hanya header semu yang tercantum dalam tabel berikut.

Konten header semu HTTP/2 dipetakan ke komponen permintaan web

HTTP/2 header semu	Komponen permintaan web untuk diperiksa	Dokumentasi
`:method`	Metode HTTP	Metode HTTP
`:authority`	Header `Host`	Header tunggal Semua header
`:path`Jalur URI	Jalur URI	Jalur URI
`:path`kueri	String kueri	String kueri Parameter kueri tunggal Semua parameter kueri

Opsi transformasi teks

Dalam pernyataan yang mencari pola atau menetapkan batasan, Anda dapat memberikan transformasi AWS WAF untuk diterapkan sebelum memeriksa permintaan. Transformasi memformat ulang permintaan web untuk menghilangkan beberapa format yang tidak biasa yang digunakan penyerang dalam upaya untuk mem-bypass. AWS WAF

Saat Anda menggunakan ini dengan pemilihan komponen permintaan badan JSON, AWS WAF terapkan transformasi Anda setelah mengurai dan mengekstrak elemen untuk diperiksa dari JSON. Untuk informasi selengkapnya, lihat Tubuh JSON.

Jika Anda memberikan lebih dari satu transformasi, Anda juga mengatur urutan AWS WAF untuk menerapkannya.

WCU — Setiap transformasi teks adalah 10 WCU.

Dokumentasi AWS WAF konsol dan API juga memberikan panduan untuk pengaturan ini di lokasi berikut:

- Pembuat aturan di konsol — Transformasi teks. Opsi ini tersedia saat Anda menggunakan komponen permintaan.
- Isi pernyataan API - `TextTransformations`

Opsi untuk transformasi teks

Setiap daftar transformasi menunjukkan spesifikasi konsol dan API diikuti oleh deskripsi.

Base64 decode – `BASE64_DECODE`

AWS WAF menerjemahkan string yang dikodekan Base64.

Base64 decode extension – `BASE64_DECODE_EXT`

AWS WAF mendekode string yang dikodekan Base64, tetapi menggunakan implementasi pemaaf yang mengabaikan karakter yang tidak valid.

Command line – `CMD_LINE`

Opsi ini mengurangi situasi di mana penyerang mungkin menyuntikkan perintah baris perintah sistem operasi dan menggunakan format yang tidak biasa untuk menyamarkan beberapa atau semua perintah.

Gunakan opsi ini untuk melakukan transformasi berikut:

- Hapus karakter berikut: `\ " ' ^`
- Hapus spasi sebelum karakter berikut: `/ (`
- Ganti karakter berikut dengan spasi: `, ;`
- Ganti spasi ganda dengan satu spasi
- Ubah huruf besar,, ke huruf kecil`A-Z`, `a-z`

Compress whitespace – `COMPRESS_WHITE_SPACE`

AWS WAF kompres spasi putih dengan mengganti beberapa spasi dengan satu spasi dan mengganti karakter berikut dengan karakter spasi (ASCII 32):

- Formfeed (ASCII 12)
- Tab (ASCII 9)
- Baris baru (ASCII 10)
- Pengembalian kereta (ASCII 13)
- Tab vertikal (ASCII 11)
- Ruang tidak pecah (ASCII 160)

CSS decode – `CSS_DECODE`

AWS WAF menerjemahkan karakter yang dikodekan menggunakan aturan escape CSS 2.x. `syndata.html#characters` Fungsi ini menggunakan hingga dua byte dalam proses pendekodean, sehingga dapat membantu mengungkap karakter ASCII yang dikodekan menggunakan pengodean CSS yang biasanya tidak dikodekan. Ini juga berguna dalam melawan penghindaran, yang merupakan kombinasi dari garis miring terbalik dan karakter non-heksadesimal. Misalnya, `ja\vascript` untuk `javascript`.

Escape sequences decode – `ESCAPE_SEQ_DECODE`

AWS WAF menerjemahkan urutan escape ANSI C berikut:`\a`,,,,`\b`,`\f`,`\n`,`\r`, `\t` `\v` `\\?`, `\xHH` (heksadesimal) `\'\"`, (oktal). `\0000` Pengodean yang tidak valid tetap dalam output.

Hex decode – `HEX_DECODE`

AWS WAF menerjemahkan string karakter heksadesimal menjadi biner.

HTML entity decode – `HTML_ENTITY_DECODE`

AWS WAF menggantikan karakter yang diwakili dalam format heksadesimal `&#xhhhh;` atau format desimal dengan karakter yang sesuai. `&#nnnn;`

AWS WAF menggantikan karakter berkode HTML berikut dengan karakter yang tidak dikodekan. Daftar ini menggunakan pengkodean HTML huruf kecil, tetapi penanganannya tidak peka huruf besar/kecil, misalnya `&QuOt;` dan `&quot;` diperlakukan sama.

Karakter yang dikodekan HTML	diganti dengan...
`&quot;`	`"`
`&`	`&`
`<`	`<`

Karakter yang dikodekan HTML	diganti dengan...
>	>
atau	spasi tanpa pindah baris, desimal 160
\n, desimal 10
	\t, desimal 9
{ atau {	{
|,|, atau		|
} atau }	}
!	!
#	#
$	$
&percent; atau %	%
'	\
(	(
)	)
* atau *	*
+	+
,	,
.	.
/	/
:	:

Karakter yang dikodekan HTML	diganti dengan...
&semi;	;
&equals;	=
&quest;	?
˜ atau ˜	~
&minus;	-
[atau [	[
&bsol;	\\
] atau]	]
&hat;	^
_ atau &underbar;	_
` atau `	`

JS decode – `JS_DECODE`

AWS WAF menerjemahkan urutan JavaScript pelarian. Jika `\uHHHH` kode berada dalam rentang kode ASCII lebar penuh`FF01-FF5E`, maka byte yang lebih tinggi digunakan untuk mendeteksi dan menyesuaikan byte yang lebih rendah. Jika tidak, hanya byte yang lebih rendah yang digunakan dan byte yang lebih tinggi dinolkan, yang menyebabkan kemungkinan hilangnya informasi.

Lowercase – `LOWERCASE`

AWS WAF mengkonversi huruf besar (A-Z) ke huruf kecil (a-z).

MD5 – `MD5`

AWS WAF menghitung hash MD5 dari data dalam input. Hash dihitung dalam bentuk biner mentah.

None – `NONE`

AWS WAF memeriksa permintaan web seperti yang diterima, tanpa transformasi teks apa pun.

Normalize path – `NORMALIZE_PATH`

AWS WAF menormalkan string input dengan menghapus beberapa garis miring, referensi mandiri direktori, dan referensi balik direktori yang tidak ada di awal input.

Normalize path Windows – `NORMALIZE_PATH_WIN`

AWS WAF mengubah karakter garis miring terbalik menjadi garis miring maju dan kemudian memproses string yang dihasilkan menggunakan transformasi. `NORMALIZE_PATH`

Remove nulls – `REMOVE_NULLS`

AWS WAF menghapus semua `NULL` byte dari input.

Replace comments – `REPLACE_COMMENTS`

AWS WAF menggantikan setiap kemunculan komentar gaya-C (/*... */) dengan satu spasi. Itu tidak memampatkan beberapa kejadian berturut-turut. Ini menggantikan komentar yang tidak dihentikan dengan spasi (ASCII 0x20). Itu tidak mengubah penghentian komentar secara mandiri (*/).

Replace nulls – `REPLACE_NULLS`

AWS WAF menggantikan setiap `NULL` byte dalam input dengan karakter spasi (ASCII 0x20).

SQL hex decode – `SQL_HEX_DECODE`

AWS WAF menerjemahkan data hex SQL. Misalnya, AWS WAF menerjemahkan (`0x414243`) ke (`ABC`).

URL decode – `URL_DECODE`

AWS WAF menerjemahkan nilai yang dikodekan URL.

URL decode Unicode – `URL_DECODE_UNI`

Seperti`URL_DECODE`, tetapi dengan dukungan untuk pengkodean khusus Microsoft`%u`. Jika kode berada dalam rentang kode `FF01-FF5E` ASCII lebar penuh, byte yang lebih tinggi digunakan untuk mendeteksi dan menyesuaikan byte yang lebih rendah. Jika tidak, hanya byte yang lebih rendah digunakan dan byte yang lebih tinggi dinolkan.

UTF8 to Unicode – `UTF8_TO_UNICODE`

AWS WAF mengkonversi semua urutan karakter UTF-8 ke Unicode. Ini membantu menormalkan input dan meminimalkan positif palsu dan negatif palsu untuk bahasa non-Inggris.

Pernyataan cakupan ke bawah

Pernyataan scope-down adalah pernyataan aturan bersarang yang Anda tambahkan di dalam pernyataan grup aturan terkelola atau pernyataan berbasis laju untuk mempersempit kumpulan permintaan yang dievaluasi aturan yang mengandung. Aturan berisi hanya mengevaluasi permintaan yang pertama cocok dengan pernyataan scope-down.

- Pernyataan grup aturan terkelola - Jika Anda menambahkan pernyataan cakupan bawah ke pernyataan grup aturan terkelola, AWS WAF evaluasi permintaan apa pun yang tidak cocok dengan pernyataan cakupan bawah sebagai tidak cocok dengan grup aturan. Hanya permintaan yang cocok dengan pernyataan scope-down yang dievaluasi terhadap kelompok aturan. Untuk grup aturan terkelola dengan harga yang didasarkan pada jumlah permintaan yang dievaluasi, pernyataan cakupan bawah dapat membantu menahan biaya.

  Untuk informasi selengkapnya tentang pernyataan grup aturan terkelola, lihatPernyataan grup aturan terkelola.
- Pernyataan aturan berbasis tarif — Pernyataan aturan berbasis tarif tanpa tingkat pernyataan cakupan bawah membatasi semua permintaan yang dievaluasi aturan. Jika Anda hanya ingin mengontrol tingkat untuk kategori permintaan tertentu, tambahkan pernyataan cakupan bawah ke aturan berbasis tarif. Misalnya, untuk hanya melacak dan mengontrol tingkat permintaan dari wilayah geografis tertentu, Anda dapat menentukan wilayah geografis tersebut dalam pernyataan kecocokan geografis dan menambahkannya ke aturan berbasis tarif Anda sebagai pernyataan cakupan turun.

  Untuk informasi selengkapnya tentang pernyataan aturan berbasis tarif, lihat. Pernyataan aturan berbasis tarif

Anda dapat menggunakan aturan nestable apa pun dalam pernyataan scope-down. Untuk pernyataan yang tersedia, lihat Pernyataan aturan pertandingan danPernyataan aturan logis. WCU untuk pernyataan scope-down adalah WCU yang diperlukan untuk pernyataan aturan yang Anda definisikan di dalamnya. Tidak ada biaya tambahan untuk penggunaan pernyataan cakupan bawah.

Anda dapat mengonfigurasi pernyataan scope-down dengan cara yang sama seperti yang Anda lakukan ketika Anda menggunakan pernyataan dalam aturan reguler. Misalnya, Anda dapat menerapkan transformasi teks ke komponen permintaan web yang sedang Anda periksa dan Anda dapat menentukan alamat IP yang diteruskan untuk digunakan sebagai alamat IP. Konfigurasi ini hanya berlaku untuk pernyataan scope-down dan tidak diwarisi oleh grup aturan terkelola yang berisi atau pernyataan aturan berbasis tarif.

Misalnya, jika Anda menerapkan transformasi teks ke string kueri dalam pernyataan cakupan bawah Anda, pernyataan cakupan bawah akan memeriksa string kueri setelah menerapkan transformasi. Jika permintaan cocok dengan kriteria pernyataan cakupan bawah, AWS WAF maka meneruskan permintaan web ke aturan yang mengandung dalam keadaan aslinya, tanpa transformasi pernyataan cakupan ke bawah. Aturan yang berisi pernyataan scope-down mungkin menerapkan transformasi teksnya sendiri, tetapi tidak mewarisi pernyataan cakupan ke bawah.

Anda tidak dapat menggunakan pernyataan scope-down untuk menentukan konfigurasi inspeksi permintaan apa pun untuk pernyataan aturan yang berisi. Anda tidak dapat menggunakan pernyataan scope-down sebagai preprocessor permintaan web untuk pernyataan aturan yang berisi. Satu-satunya peran dari pernyataan scope-down adalah untuk menentukan permintaan mana yang diteruskan ke pernyataan aturan yang berisi untuk inspeksi.

Pernyataan yang mereferensikan kumpulan atau grup aturan

Beberapa aturan menggunakan entitas yang dapat digunakan kembali dan dikelola di luar ACL web Anda, baik oleh Anda AWS, atau penjual. AWS Marketplace Saat entitas yang dapat digunakan kembali diperbarui, AWS WAF menyebarkan pembaruan ke aturan Anda. Misalnya, jika Anda menggunakan grup aturan Aturan AWS Terkelola di ACL web, saat AWS memperbarui grup aturan, AWS menyebarkan perubahan ke ACL web Anda, untuk memperbarui perilakunya. Jika Anda menggunakan pernyataan kumpulan IP dalam aturan, saat Anda memperbarui set, AWS WAF menyebarkan perubahan ke semua aturan yang mereferensikannya, sehingga ACL web apa pun yang menggunakan aturan tersebut disimpan up-to-date dengan perubahan Anda.

Berikut ini adalah entitas yang dapat digunakan kembali yang dapat Anda gunakan dalam pernyataan aturan.

- Set IP — Anda membuat dan mengelola set IP Anda sendiri. Di konsol, Anda dapat mengaksesnya dari panel navigasi. Untuk informasi tentang mengelola set IP, lihatSet IP dan set pola regex di AWS WAF.

- Set pertandingan Regex — Anda membuat dan mengelola set pertandingan regex Anda sendiri. Di konsol, Anda dapat mengaksesnya dari panel navigasi. Untuk informasi tentang mengelola set pola regex, lihat. Set IP dan set pola regex di AWS WAF
- AWS Kelompok aturan Aturan AWS Terkelola — mengelola grup aturan ini. Di konsol, ini tersedia untuk Anda gunakan saat Anda menambahkan grup aturan terkelola ke ACL web Anda. Untuk informasi lebih lanjut tentang ini, lihatAWS Daftar grup aturan Aturan Terkelola.
- AWS Marketplace grup aturan terkelola — AWS Marketplace penjual mengelola grup aturan ini dan Anda dapat berlangganan untuk menggunakannya. Untuk mengelola langganan Anda, pada panel navigasi konsol, pilih. AWS Marketplace Grup aturan AWS Marketplace terkelola dicantumkan saat Anda menambahkan grup aturan terkelola ke ACL web Anda. Untuk grup aturan yang belum Anda berlangganan, Anda juga dapat menemukan tautan AWS Marketplace di halaman itu. Untuk informasi selengkapnya tentang grup aturan terkelola AWS Marketplace penjual, lihatAWS Marketplace kelompok aturan terkelola.
- Grup aturan Anda sendiri — Anda mengelola grup aturan Anda sendiri, biasanya ketika Anda memerlukan beberapa perilaku yang tidak tersedia melalui grup aturan terkelola. Di konsol, Anda dapat mengaksesnya dari panel navigasi. Untuk informasi selengkapnya, lihat Mengelola grup aturan Anda sendiri.

Menghapus kumpulan atau grup aturan yang direferensikan

Saat Anda menghapus entitas yang direferensikan, AWS WAF periksa apakah saat ini sedang digunakan di ACL web. Jika AWS WAF menemukan bahwa itu sedang digunakan, itu memperingatkan Anda. AWS WAF hampir selalu dapat menentukan apakah suatu entitas sedang direferensikan oleh ACL web. Namun, dalam kasus yang jarang terjadi, mungkin tidak dapat melakukannya. Jika Anda perlu memastikan bahwa entitas yang ingin Anda hapus tidak digunakan, periksa di ACL web Anda sebelum menghapusnya.

Pernyataan aturan pertandingan

Pernyataan kecocokan membandingkan permintaan web atau asalnya dengan kriteria yang Anda berikan. Untuk banyak pernyataan jenis ini, AWS WAF membandingkan komponen spesifik dari permintaan untuk konten yang cocok.

Pernyataan kecocokan adalah nestable. Anda dapat menyarangkan salah satu pernyataan ini di dalam pernyataan aturan logis dan Anda dapat menggunakannya dalam pernyataan cakupan bawah. Untuk informasi tentang pernyataan aturan logis, lihatPernyataan aturan logis. Untuk informasi tentang pernyataan cakupan bawah, lihat. Pernyataan cakupan ke bawah

Tabel ini menjelaskan pernyataan pencocokan reguler yang dapat Anda tambahkan ke aturan dan memberikan beberapa pedoman untuk menghitung penggunaan unit kapasitas ACL web (WCU) untuk masing-masing. Untuk informasi tentang WCU, lihatAWS WAF unit kapasitas ACL web (WCU).

Pernyataan Pertandingan	Deskripsi	WCU
Pertandingan geografis	Memeriksa negara asal permintaan dan menerapka n label untuk negara dan wilayah asal.	1
Pertandingan set IP	Memeriksa permintaan terhadap satu set alamat IP dan rentang alamat.	1 untuk sebagian besar kasus. Jika Anda mengonfig urasi pernyataan untuk menggunakan header dengan alamat IP yang diteruskan dan menentukan posisi di headerAny, maka tingkatkan WCU sebesar 4.
Pernyataan aturan pencocoka n label	Memeriksa permintaan label yang telah ditambahkan oleh aturan lain di ACL web yang sama.	1
Pernyataan aturan pertandin gan Regex	Membandingkan pola regex terhadap komponen permintaa n tertentu.	3, sebagai biaya dasar. Jika Anda menggunak an komponen permintaa n Semua parameter kueri, tambahkan 10 WCU. Jika Anda menggunakan isi JSON komponen permintaan, gandakan WCU biaya dasar. Untuk setiap transformasi

Pernyataan Pertandingan	Deskripsi	WCU
		Teks yang Anda terapkan, tambahkan 10 WCU.
Set pola regex	Membandingkan pola regex terhadap komponen permintaan tertentu.	25 per set pola, sebagai biaya dasar. Jika Anda menggunakan komponen permintaan Semua parameter kueri, tambahkan 10 WCU. Jika Anda menggunakan isi JSON komponen permintaan, gandakan WCU biaya dasar. Untuk setiap transformasi Teks yang Anda terapkan, tambahkan 10 WCU.
Kendala ukuran	Memeriksa batasan ukuran terhadap komponen permintaan tertentu.	1, sebagai biaya dasar. Jika Anda menggunakan komponen permintaan Semua parameter kueri, tambahkan 10 WCU. Jika Anda menggunakan isi JSON komponen permintaan, gandakan WCU biaya dasar. Untuk setiap transformasi Teks yang Anda terapkan, tambahkan 10 WCU.

Pernyataan Pertandingan	Deskripsi	WCU
Serangan SQLi	Memeriksa kode SQL berbahaya dalam komponen permintaan tertentu.	20, sebagai biaya dasar. Jika Anda menggunak an komponen permintaa n Semua parameter kueri, tambahkan 10 WCU. Jika Anda menggunakan isi JSON komponen permintaan, gandakan WCU biaya dasar. Untuk setiap transformasi Teks yang Anda terapkan, tambahkan 10 WCU.
Pertandingan string	Membandingkan string ke komponen permintaan tertentu.	Biaya dasar tergantung pada jenis kecocokan string dan antara 1 dan 10. Jika Anda menggunak an komponen permintaa n Semua parameter kueri, tambahkan 10 WCU. Jika Anda menggunakan isi JSON komponen permintaan, gandakan WCU biaya dasar. Untuk setiap transformasi Teks yang Anda terapkan, tambahkan 10 WCU.

Pernyataan Pertandingan	Deskripsi	WCU
Serangan skrip XSS	Memeriksa serangan scripting lintas situs dalam komponen permintaan tertentu.	40, sebagai biaya dasar. Jika Anda menggunak an komponen permintaa n Semua parameter kueri, tambahkan 10 WCU. Jika Anda menggunakan isi JSON komponen permintaan, gandakan WCU biaya dasar. Untuk setiap transformasi Teks yang Anda terapkan, tambahkan 10 WCU.

Pernyataan aturan kecocokan geografis

Gunakan pernyataan kecocokan geografis atau geografis untuk mengelola permintaan web berdasarkan negara dan wilayah asal. Pernyataan geo match menambahkan label ke permintaan web yang menunjukkan negara asal dan wilayah asal. Ini menambahkan label ini terlepas dari apakah kriteria pernyataan cocok untuk permintaan. Pernyataan geo match juga melakukan pencocokan terhadap negara asal permintaan.

Cara menggunakan pernyataan geo match

Anda dapat menggunakan pernyataan geo match untuk pencocokan negara atau wilayah, sebagai berikut:

- Negara — Anda dapat menggunakan aturan geo match dengan sendirinya untuk mengelola permintaan hanya berdasarkan negara asal mereka. Pernyataan aturan cocok dengan kode negara. Anda juga dapat mengikuti aturan geo match dengan aturan pencocokan label yang cocok dengan label negara asal.
- Wilayah — Gunakan aturan pencocokan geografis diikuti dengan aturan pencocokan label untuk mengelola permintaan berdasarkan wilayah asalnya. Anda tidak dapat menggunakan aturan geo match saja untuk mencocokkan dengan kode wilayah.

Untuk informasi tentang penggunaan aturan pencocokan label, lihat Pernyataan aturan pencocokan label danAWS WAF label pada permintaan web.

Cara kerja pernyataan geo match

Dengan pernyataan geo match, AWS WAF mengelola setiap permintaan web sebagai berikut:

1. Menentukan kode negara dan wilayah permintaan — AWS WAF menentukan negara dan wilayah permintaan berdasarkan alamat IP-nya. Secara default, AWS WAF menggunakan alamat IP asal permintaan web. Anda dapat menginstruksikan AWS WAF untuk menggunakan alamat IP dari header permintaan alternatif, seperti`X-Forwarded-For`, dengan mengaktifkan konfigurasi IP yang diteruskan dalam pengaturan pernyataan aturan.

   AWS WAF menentukan lokasi permintaan menggunakan database MaxMind GeoIP. MaxMind melaporkan akurasi data mereka yang sangat tinggi di tingkat negara, meskipun akurasi bervariasi sesuai dengan faktor-faktor seperti negara dan jenis IP. Untuk informasi selengkapnya MaxMind, lihat Geolokasi MaxMind IP. Jika menurut Anda salah satu data GeoIP salah, Anda dapat mengirimkan permintaan koreksi ke Maxmind di Data GeoIP2 MaxMind yang Benar.

   AWS WAF menggunakan kode negara dan wilayah alfa-2 dari standar Organisasi Internasional untuk Standardisasi (ISO) 3166. Anda dapat menemukan kode di lokasi berikut:

   - Di situs web ISO, Anda dapat mencari kode negara di ISO Online Browsing Platform (OBP).
   - Di Wikipedia, kode negara terdaftar di ISO 3166-2.

     Kode wilayah untuk suatu negara tercantum di URL`https://en.wikipedia.org/wiki/ISO_3166-2:`*`<ISO country code>`*. Misalnya, wilayah untuk Amerika Serikat berada pada ISO 3166-2:AS dan untuk Ukraina mereka berada di ISO 3166-2:UA.
2. Menentukan label negara dan label wilayah untuk ditambahkan ke permintaan — Label menunjukkan apakah pernyataan geo match menggunakan IP asal atau konfigurasi IP yang diteruskan.

   - IP Asal

     Label negara adalah`awswaf:clientip:geo:country:`*`<ISO country code>`*. Contoh untuk Amerika Serikat:`awswaf:clientip:geo:country:US`.

     Label wilayah adalah`awswaf:clientip:geo:region:`*`<ISO country code>`*`-`*`<ISO region code>`*. Contoh untuk Oregon di Amerika Serikat:`awswaf:clientip:geo:region:US-OR`.

- IP yang diteruskan

  Label negara adalah`awswaf:forwardedip:geo:country:<ISO country code>`. Contoh untuk Amerika Serikat:`awswaf:forwardedip:geo:country:US`.

  Label wilayah adalah`awswaf:forwardedip:geo:region:<ISO country code>-<ISO region code>`. Contoh untuk Oregon di Amerika Serikat:`awswaf:forwardedip:geo:region:US-OR`.

  Jika kode negara atau wilayah tidak tersedia untuk alamat IP yang ditentukan permintaan, AWS WAF gunakan XX label, sebagai pengganti nilai. Misalnya, label berikut adalah untuk IP klien yang kode negaranya tidak tersedia: `awswaf:clientip:geo:country:XX` dan berikut ini untuk IP yang diteruskan yang negaranya adalah Amerika Serikat, tetapi kode wilayahnya tidak tersedia: `awswaf:forwardedip:geo:region:US-XX`

3. Mengevaluasi kode negara permintaan terhadap kriteria aturan

Pernyataan geo match menambahkan label negara dan wilayah ke semua permintaan yang diperiksa, terlepas dari apakah ia menemukan kecocokan.

> **Note**
>
> AWS WAF menambahkan label apa pun di akhir evaluasi permintaan web aturan. Karena itu, setiap pencocokan label yang Anda gunakan terhadap label dari pernyataan geo match harus didefinisikan dalam aturan terpisah dari aturan yang berisi pernyataan geo match.

Jika Anda hanya ingin memeriksa nilai wilayah, Anda dapat menulis aturan kecocokan geografis dengan Count tindakan dan dengan kecocokan kode negara tunggal, diikuti dengan aturan pencocokan label untuk label wilayah. Anda diminta untuk memberikan kode negara untuk aturan geo match untuk dievaluasi, bahkan untuk pendekatan ini. Anda dapat mengurangi metrik pencatatan dan penghitungan dengan menentukan negara yang sangat tidak mungkin menjadi sumber lalu lintas ke situs Anda.

CloudFront distribusi dan fitur pembatasan CloudFront geografis

Untuk CloudFront distribusi, jika Anda menggunakan fitur pembatasan CloudFront geografis, ketahuilah bahwa fitur tersebut tidak meneruskan permintaan yang diblokir. AWS WAF Itu meneruskan permintaan yang diizinkan ke AWS WAF. Jika Anda ingin memblokir permintaan

berdasarkan geografi ditambah kriteria lain yang dapat Anda tentukan AWS WAF, gunakan pernyataan AWS WAF geo match dan jangan gunakan fitur pembatasan CloudFront geografis.

Karakteristik pernyataan kecocokan geo

Nestable - Anda dapat membuat jenis pernyataan ini.

WCU — 1 WCU.

Pengaturan - Pernyataan ini menggunakan pengaturan berikut:

- Kode negara — Array kode negara untuk dibandingkan untuk kecocokan geografis. Ini harus berupa kode negara dua karakter dari kode ISO negara alfa-2 dari standar internasional ISO 3166, misalnya,. `["US","CN"]`
- (Opsional) Konfigurasi IP yang diteruskan — Secara default, AWS WAF menggunakan alamat IP di asal permintaan web untuk menentukan negara asal. Atau, Anda dapat mengonfigurasi aturan untuk menggunakan IP yang diteruskan di header HTTP seperti `X-Forwarded-For` sebagai gantinya. AWS WAF menggunakan alamat IP pertama di header. Dengan konfigurasi ini, Anda juga menentukan perilaku fallback untuk diterapkan ke permintaan web dengan alamat IP cacat di header. Perilaku fallback menetapkan hasil pencocokan untuk permintaan, agar cocok atau tidak cocok. Untuk informasi selengkapnya, lihat Alamat IP yang diteruskan.

Di mana menemukan pernyataan aturan ini

- Pembuat aturan di konsol — Untuk opsi Permintaan, pilih Berasal dari negara di.
- API — GeoMatchStatement

Contoh-contoh

Anda dapat menggunakan pernyataan geo match untuk mengelola permintaan dari negara atau wilayah tertentu. Misalnya, jika Anda ingin memblokir permintaan dari negara tertentu, tetapi masih mengizinkan permintaan dari kumpulan alamat IP tertentu di negara tersebut, Anda dapat membuat aturan dengan tindakan yang disetel ke Block dan pernyataan bersarang berikut, yang ditunjukkan dalam pseudocode:

- Pernyataan AND
  - Pernyataan geo match mencantumkan negara yang ingin Anda blokir
  - Pernyataan NOT

- IP set pernyataan yang menentukan alamat IP yang ingin Anda izinkan melalui

Atau, jika Anda ingin memblokir beberapa wilayah di negara tertentu, tetapi masih mengizinkan permintaan dari wilayah lain di negara tersebut, Anda dapat terlebih dahulu menentukan aturan geo match dengan tindakan yang disetel keCount. Kemudian, tentukan aturan pencocokan label yang cocok dengan label kecocokan geografis yang ditambahkan dan tangani permintaan sesuai kebutuhan.

Kode semu berikut menjelaskan contoh pendekatan ini:

1. Pernyataan geo match mencantumkan negara dengan wilayah yang ingin Anda blokir, tetapi dengan tindakan yang disetel ke Hitung. Ini memberi label pada setiap permintaan web terlepas dari status kecocokan, dan ini juga memberi Anda metrik hitungan untuk negara yang diminati.
2. ANDpernyataan dengan tindakan Blokir
   - Pernyataan pencocokan label yang menentukan label untuk negara yang ingin Anda blokir
   - Pernyataan NOT
     - Pernyataan pencocokan label yang menentukan label wilayah di negara-negara yang ingin Anda izinkan

Daftar JSON berikut menunjukkan implementasi dari dua aturan yang dijelaskan dalam pseudocode sebelumnya. Aturan ini memblokir semua lalu lintas dari Amerika Serikat kecuali lalu lintas dari Oregon dan Washington. Pernyataan geo match menambahkan label negara dan wilayah ke semua permintaan yang diperiksa. Aturan pencocokan label berjalan setelah aturan kecocokan geografis, sehingga dapat cocok dengan label negara dan wilayah yang baru saja ditambahkan oleh aturan kecocokan geografis. Pernyataan geo match menggunakan alamat IP yang diteruskan, sehingga pencocokan label juga menentukan label IP yang diteruskan.

```
{
   "Name": "geoMatchForLabels",
   "Priority": 10,
   "Statement": {
     "GeoMatchStatement": {
       "CountryCodes": [
         "US"
       ],
       "ForwardedIPConfig": {
           "HeaderName": "X-Forwarded-For",
           "FallbackBehavior": "MATCH"
```

```
        }
      }
    },
    "Action": {
      "Count": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "geoMatchForLabels"
    }
},
{
    "Name": "blockUSButNotOROrWA",
    "Priority": 11,
    "Statement": {
      "AndStatement": {
        "Statements": [
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:forwardedip:geo:country:US"
            }
          },
          {
            "NotStatement": {
              "Statement": {
                 "OrStatement": {
                   "Statements": [
                     {
                        "LabelMatchStatement": {
                          "Scope": "LABEL",
                          "Key": "awswaf:forwardedip:geo:region:US-OR"
                        }
                     },
                     {
                        "LabelMatchStatement": {
                          "Scope": "LABEL",
                          "Key": "awswaf:forwardedip:geo:region:US-WA"
                        }
                     }
                   ]
                }
              }
```

```
            }
          }
        ]
      }
    },
    "Action": {
      "Block": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "blockUSButNotORIrWA"
    }
}
```

Sebagai contoh lain, Anda dapat menggabungkan pencocokan geografis dengan aturan berbasis tarif untuk memprioritaskan sumber daya bagi pengguna di negara atau wilayah tertentu. Anda membuat pernyataan berbasis tarif yang berbeda untuk setiap pernyataan kecocokan geografis atau pencocokan label yang Anda gunakan untuk membedakan pengguna Anda. Tetapkan batas tarif yang lebih tinggi untuk pengguna di negara atau wilayah pilihan dan tetapkan batas tarif yang lebih rendah untuk pengguna lain.

Daftar JSON berikut menunjukkan aturan kecocokan geografis diikuti oleh aturan berbasis tarif yang membatasi tingkat lalu lintas dari Amerika Serikat. Aturan memungkinkan lalu lintas dari Oregon masuk pada tingkat yang lebih tinggi daripada lalu lintas dari tempat lain di negara ini.

```
{
  "Name": "geoMatchForLabels",
  "Priority": 190,
  "Statement": {
    "GeoMatchStatement": {
      "CountryCodes": [
        "US"
      ]
    }
  },
  "Action": {
    "Count": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
```

```
    "MetricName": "geoMatchForLabels"
  }
},
{
  "Name": "rateLimitOregon",
  "Priority": 195,
  "Statement": {
    "RateBasedStatement": {
      "Limit": 3000,
      "AggregateKeyType": "IP",
      "ScopeDownStatement": {
        "LabelMatchStatement": {
          "Scope": "LABEL",
          "Key": "awswaf:clientip:geo:region:US-OR"
        }
      }
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "rateLimitOregon"
  }
},
{
  "Name": "rateLimitUSNotOR",
  "Priority": 200,
  "Statement": {
    "RateBasedStatement": {
      "Limit": 100,
      "AggregateKeyType": "IP",
      "ScopeDownStatement": {
        "AndStatement": {
          "Statements": [
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:clientip:geo:country:US"
              }
            },
            {
```

```
              "NotStatement": {
                "Statement": {
                  "LabelMatchStatement": {
                    "Scope": "LABEL",
                    "Key": "awswaf:clientip:geo:region:US-OR"
                  }
                }
              }
            }
          ]
        }
      }
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "rateLimitUSNotOR"
  }
}
```

Pernyataan aturan kecocokan set IP

Pernyataan pencocokan set IP memeriksa alamat IP permintaan web terhadap serangkaian alamat IP dan rentang alamat. Gunakan ini untuk mengizinkan atau memblokir permintaan web berdasarkan alamat IP tempat permintaan berasal. Secara default, AWS WAF menggunakan alamat IP dari asal permintaan web, tetapi Anda dapat mengonfigurasi aturan untuk menggunakan header HTTP seperti `X-Forwarded-For` sebagai gantinya.

AWS WAF mendukung semua rentang IPv4 dan IPv6 CIDR kecuali untuk. `/0` Untuk informasi lebih lanjut tentang notasi CIDR, lihat entri Wikipedia Classless Inter-Domain Routing. Satu set IP dapat menampung hingga 10.000 alamat IP atau rentang alamat IP untuk diperiksa.

> **Note**
>
> Setiap aturan pencocokan set IP mereferensikan kumpulan IP, yang Anda buat dan pertahankan secara independen dari aturan Anda. Anda dapat menggunakan satu set IP

dalam beberapa aturan, dan ketika Anda memperbarui set yang direferensikan, AWS WAF secara otomatis memperbarui semua aturan yang mereferensikannya.
Untuk informasi tentang membuat dan mengelola kumpulan IP, lihatMembuat dan mengelola set IP.

Saat Anda menambahkan atau memperbarui aturan di grup aturan atau ACL web Anda, pilih opsi IP set dan pilih nama set IP yang ingin Anda gunakan.

Nestable - Anda dapat membuat jenis pernyataan ini.

WCU — 1 WCU untuk sebagian besar. Jika Anda mengonfigurasi pernyataan untuk menggunakan alamat IP yang diteruskan dan menentukan posisiANY, tingkatkan penggunaan WCU sebesar 4.

Pernyataan ini menggunakan pengaturan berikut:

- Spesifikasi set IP - Pilih set IP yang ingin Anda gunakan dari daftar atau buat yang baru.
- (Opsional) Konfigurasi IP yang diteruskan - Nama header IP diteruskan alternatif untuk digunakan sebagai pengganti asal permintaan. Anda menentukan apakah akan cocok dengan alamat pertama, terakhir, atau alamat apa pun di header. Anda juga menentukan perilaku fallback untuk diterapkan ke permintaan web dengan alamat IP cacat di header yang ditentukan. Perilaku fallback menetapkan hasil pencocokan untuk permintaan, agar cocok atau tidak cocok. Untuk informasi selengkapnya, lihat Alamat IP yang diteruskan.

Di mana menemukan pernyataan aturan ini

- Pembuat aturan di konsol — Untuk opsi Permintaan, pilih Berasal dari alamat IP di.
- Tambahkan halaman aturan dan grup aturan saya sendiri di konsol — Pilih opsi set IP.
- API - IP SetReferenceStatement

Pernyataan aturan pencocokan label

Pernyataan pencocokan label memeriksa label yang ada di permintaan web terhadap spesifikasi string. Label yang tersedia untuk aturan untuk inspeksi adalah label yang telah ditambahkan ke permintaan web oleh aturan lain dalam evaluasi ACL web yang sama.

Label tidak bertahan di luar evaluasi ACL web, tetapi Anda dapat mengakses metrik label CloudWatch dan Anda dapat melihat ringkasan informasi label untuk ACL web apa pun di konsol.

AWS WAF Lihat informasi yang lebih lengkap di Label metrik dan dimensi dan Pemantauan dan penyetelan. Anda juga dapat melihat label di log. Untuk informasi, lihat Bidang log.

> **Note**
>
> Pernyataan pencocokan label hanya dapat melihat label dari aturan yang dievaluasi sebelumnya di ACL web. Untuk informasi tentang cara AWS WAF mengevaluasi aturan dan grup aturan di ACL web, lihat. Memproses urutan aturan dan kelompok aturan dalam ACL web

Untuk informasi selengkapnya tentang menambahkan dan mencocokkan label, lihatAWS WAF label pada permintaan web.

Nestable - Anda dapat membuat sarang jenis pernyataan ini.

WCU — 1 WCU

Pernyataan ini menggunakan pengaturan berikut:

- Lingkup pencocokan - Setel ini ke Label agar sesuai dengan nama label dan, secara opsional, ruang nama dan awalan sebelumnya. Setel ini ke Namespace agar sesuai dengan beberapa atau semua spesifikasi namespace dan, secara opsional, awalan sebelumnya.
- Key — String yang ingin Anda cocokkan. Jika Anda menentukan cakupan pencocokan namespace, ini seharusnya hanya menentukan ruang nama dan opsional awalan, dengan titik dua akhir. Jika Anda menentukan lingkup pencocokan label, ini harus menyertakan nama label dan secara opsional dapat menyertakan ruang nama dan awalan sebelumnya.

Untuk informasi selengkapnya tentang pengaturan ini, lihat AWS WAF aturan yang cocok dengan label danAWS WAF contoh kecocokan label.

Di mana menemukan pernyataan aturan ini

- Pembuat aturan di konsol — Untuk opsi Permintaan, pilih Memiliki label.
- API — LabelMatchStatement

Pernyataan aturan pertandingan Regex

Pernyataan pencocokan regex menginstruksikan AWS WAF untuk mencocokkan komponen permintaan terhadap ekspresi reguler tunggal (regex). Permintaan web cocok dengan pernyataan jika komponen permintaan cocok dengan regex yang Anda tentukan.

Jenis pernyataan ini adalah alternatif yang baik Pernyataan aturan kecocokan set pola regex untuk situasi di mana Anda ingin menggabungkan kriteria pencocokan Anda menggunakan logika matematika. Misalnya, jika Anda ingin komponen permintaan cocok dengan beberapa pola regex dan tidak cocok dengan yang lain, Anda dapat menggabungkan pernyataan pencocokan regex menggunakan dan. ANDpernyataan aturan NOTpernyataan aturan

AWS WAF mendukung sintaks pola yang digunakan oleh pustaka PCRE `libpcre` dengan beberapa pengecualian. Pustaka didokumentasikan di PCRE - Perl Compatible Regular Expressions. Untuk informasi tentang AWS WAF dukungan, lihatPencocokan pola ekspresi reguler di AWS WAF.

Nestable - Anda dapat membuat sarang jenis pernyataan ini.

WCU — 3 WCU, sebagai biaya dasar. Jika Anda menggunakan komponen permintaan Semua parameter kueri, tambahkan 10 WCU. Jika Anda menggunakan isi JSON komponen permintaan, gandakan WCU biaya dasar. Untuk setiap transformasi Teks yang Anda terapkan, tambahkan 10 WCU.

Jenis pernyataan ini beroperasi pada komponen permintaan web, dan memerlukan pengaturan komponen permintaan berikut:

- Komponen permintaan — Bagian dari permintaan web untuk memeriksa, misalnya, string kueri atau badan.

  > **Warning**
  >
  > Jika Anda memeriksa komponen permintaan Body, JSON body, Header, atau Cookie, baca tentang batasan jumlah konten yang AWS WAF dapat diperiksa. Penanganan komponen permintaan kebesaran di AWS WAF

  Untuk informasi tentang komponen permintaan web, lihatSpesifikasi dan penanganan komponen permintaan web.
- Transformasi teks opsional — Transformasi yang AWS WAF ingin Anda lakukan pada komponen permintaan sebelum memeriksanya. Misalnya, Anda dapat mengubah ke huruf kecil atau

menormalkan ruang putih. Jika Anda menentukan lebih dari satu transformasi, AWS WAF proses mereka dalam urutan yang tercantum. Untuk informasi, lihat Opsi transformasi teks.

Di mana menemukan pernyataan aturan ini

- Pembuat aturan di konsol — Untuk jenis Match, pilih Match regular expression.
- API — RegexMatchStatement

Pernyataan aturan kecocokan set pola regex

Pencocokan set pola regex memeriksa bagian permintaan web yang Anda tentukan untuk pola ekspresi reguler yang telah Anda tentukan di dalam kumpulan pola regex.

AWS WAF mendukung sintaks pola yang digunakan oleh pustaka PCRE `libpcre` dengan beberapa pengecualian. Pustaka didokumentasikan di PCRE - Perl Compatible Regular Expressions. Untuk informasi tentang AWS WAF dukungan, lihatPencocokan pola ekspresi reguler di AWS WAF.

> **Note**
>
> Setiap aturan pencocokan set pola regex mereferensikan kumpulan pola regex, yang Anda buat dan pertahankan terlepas dari aturan Anda. Anda dapat menggunakan pola regex tunggal yang diatur dalam beberapa aturan, dan ketika Anda memperbarui set yang direferensikan, AWS WAF secara otomatis memperbarui semua aturan yang mereferensikannya.
> Untuk informasi tentang membuat dan mengelola kumpulan pola regex, lihat. Membuat dan mengelola set pola regex

Pernyataan pencocokan set pola regex menginstruksikan AWS WAF untuk mencari salah satu pola dalam set di dalam komponen permintaan yang Anda pilih. Permintaan web akan cocok dengan pernyataan aturan set pola jika komponen permintaan cocok dengan salah satu pola dalam set.

Jika Anda ingin menggabungkan kecocokan pola regex Anda menggunakan logika, misalnya untuk mencocokkan dengan beberapa ekspresi reguler dan tidak cocok dengan yang lain, pertimbangkan untuk menggunakan. Pernyataan aturan pertandingan Regex

Nestable - Anda dapat membuat sarang jenis pernyataan ini.

WCU — 25 WCU, sebagai biaya dasar. Jika Anda menggunakan komponen permintaan Semua parameter kueri, tambahkan 10 WCU. Jika Anda menggunakan isi JSON komponen permintaan, gandakan WCU biaya dasar. Untuk setiap transformasi Teks yang Anda terapkan, tambahkan 10 WCU.

Jenis pernyataan ini beroperasi pada komponen permintaan web, dan memerlukan pengaturan komponen permintaan berikut:

- Komponen permintaan — Bagian dari permintaan web untuk memeriksa, misalnya, string kueri atau badan.

  > **Warning**
  >
  > Jika Anda memeriksa komponen permintaan Body, JSON body, Header, atau Cookie, baca tentang batasan jumlah konten yang AWS WAF dapat diperiksa. Penanganan komponen permintaan kebesaran di AWS WAF

  Untuk informasi tentang komponen permintaan web, lihatSpesifikasi dan penanganan komponen permintaan web.
- Transformasi teks opsional — Transformasi yang AWS WAF ingin Anda lakukan pada komponen permintaan sebelum memeriksanya. Misalnya, Anda dapat mengubah ke huruf kecil atau menormalkan ruang putih. Jika Anda menentukan lebih dari satu transformasi, AWS WAF proses mereka dalam urutan yang tercantum. Untuk informasi, lihat Opsi transformasi teks.

Pernyataan ini membutuhkan pengaturan berikut:

- Spesifikasi set pola Regex - Pilih set pola regex yang ingin Anda gunakan dari daftar atau buat yang baru.

Di mana menemukan pernyataan aturan ini

- Pembuat aturan di konsol — Untuk jenis Pencocokan, pilih Kondisi pencocokan string > Pola kecocokan dari kumpulan ekspresi reguler.
- API — RegexPatternSetReferenceStatement

Pernyataan aturan batasan ukuran

Pernyataan batasan ukuran membandingkan jumlah byte dalam komponen permintaan web dengan nomor yang Anda berikan, dan cocok sesuai dengan kriteria perbandingan Anda. Kriteria perbandingan adalah operator seperti lebih besar dari (>) atau kurang dari (<). Misalnya, Anda dapat mencocokkan permintaan yang memiliki string kueri dengan ukuran yang lebih besar dari 100 byte.

> **Note**
>
> Pernyataan ini hanya memeriksa ukuran komponen permintaan web. Itu tidak memeriksa isi komponen.

Jika Anda memeriksa jalur URI, apa pun `/` di jalur dihitung sebagai satu karakter. Misalnya, jalur URI `/logo.jpg` panjangnya sembilan karakter.

Nestable - Anda dapat membuat jenis pernyataan ini.

WCU — 1 WCU, sebagai biaya dasar. Jika Anda menggunakan komponen permintaan Semua parameter kueri, tambahkan 10 WCU. Jika Anda menggunakan isi JSON komponen permintaan, gandakan WCU biaya dasar. Untuk setiap transformasi Teks yang Anda terapkan, tambahkan 10 WCU.

Jenis pernyataan ini beroperasi pada komponen permintaan web, dan memerlukan pengaturan komponen permintaan berikut:

- Komponen permintaan — Bagian dari permintaan web untuk memeriksa, misalnya, string kueri atau badan. Untuk informasi tentang komponen permintaan web, lihatSpesifikasi dan penanganan komponen permintaan web.

  Pernyataan batasan ukuran hanya memeriksa ukuran komponen setelah transformasi apa pun diterapkan. Itu tidak memeriksa isi komponen.
- Transformasi teks opsional — Transformasi yang AWS WAF ingin Anda lakukan pada komponen permintaan sebelum memeriksa ukurannya. Misalnya, Anda dapat mengompres ruang putih atau memecahkan kode entitas HTML. Jika Anda menentukan lebih dari satu transformasi, AWS WAF proses mereka dalam urutan yang tercantum. Untuk informasi, lihat Opsi transformasi teks.

Selain itu, pernyataan ini memerlukan pengaturan berikut:

- Kondisi pencocokan ukuran - Ini menunjukkan operator perbandingan numerik yang akan digunakan untuk membandingkan ukuran yang Anda berikan dengan komponen permintaan yang Anda pilih. Pilih operator dari daftar.
- Ukuran - Pengaturan ukuran, dalam byte, untuk digunakan dalam perbandingan.

Di mana menemukan pernyataan aturan ini

- Pembuat aturan di konsol — Untuk jenis Pencocokan, di bawah Kondisi kecocokan ukuran, pilih kondisi yang ingin Anda gunakan.
- API — SizeConstraintStatement

Pernyataan aturan serangan injeksi SQL

Pernyataan aturan injeksi SQL memeriksa kode SQL berbahaya. Penyerang memasukkan kode SQL berbahaya ke dalam permintaan web untuk melakukan hal-hal seperti memodifikasi database Anda atau mengekstrak data darinya.

Nestable - Anda dapat membuat sarang jenis pernyataan ini.

WCU — Biaya dasar tergantung pada pengaturan tingkat sensitivitas untuk pernyataan aturan: Low biaya 20 dan High biaya 30.

Jika Anda menggunakan komponen permintaan Semua parameter kueri, tambahkan 10 WCU. Jika Anda menggunakan isi JSON komponen permintaan, gandakan WCU biaya dasar. Untuk setiap transformasi Teks yang Anda terapkan, tambahkan 10 WCU.

Jenis pernyataan ini beroperasi pada komponen permintaan web, dan memerlukan pengaturan komponen permintaan berikut:

- Komponen permintaan — Bagian dari permintaan web untuk memeriksa, misalnya, string kueri atau badan.

> **Warning**
>
> Jika Anda memeriksa komponen permintaan Body, JSON body, Header, atau Cookie, baca tentang batasan jumlah konten yang AWS WAF dapat diperiksa. Penanganan komponen permintaan kebesaran di AWS WAF

Untuk informasi tentang komponen permintaan web, lihatSpesifikasi dan penanganan komponen permintaan web.

- Transformasi teks opsional — Transformasi yang AWS WAF ingin Anda lakukan pada komponen permintaan sebelum memeriksanya. Misalnya, Anda dapat mengubah ke huruf kecil atau menormalkan ruang putih. Jika Anda menentukan lebih dari satu transformasi, AWS WAF proses mereka dalam urutan yang tercantum. Untuk informasi, lihat Opsi transformasi teks.

Selain itu, pernyataan ini memerlukan pengaturan berikut:

- Tingkat sensitivitas - Pengaturan ini menyetel sensitivitas kriteria kecocokan injeksi SQL. Opsi nya adalah LOW dan HIGH. Pengaturan default-nya adalah LOW.

  HIGHPengaturan mendeteksi lebih banyak serangan injeksi SQL, dan merupakan pengaturan yang disarankan. Karena sensitivitas yang lebih tinggi, pengaturan ini menghasilkan lebih banyak kesalahan positif, terutama jika permintaan web Anda biasanya berisi string yang tidak biasa. Selama pengujian dan penyetelan ACL web Anda, Anda mungkin perlu melakukan lebih banyak pekerjaan untuk mengurangi positif palsu. Untuk informasi, lihat Menguji dan menyetel perlindungan Anda AWS WAF.

  Pengaturan yang lebih rendah memberikan deteksi injeksi SQL yang kurang ketat, yang juga menghasilkan lebih sedikit positif palsu. LOWdapat menjadi pilihan yang lebih baik untuk sumber daya yang memiliki perlindungan lain terhadap serangan injeksi SQL atau yang memiliki toleransi rendah untuk positif palsu.

Di mana menemukan pernyataan aturan ini

- Pembuat aturan di konsol - Untuk jenis Match, pilih Kondisi kecocokan serang > Berisi serangan injeksi SQL.
- API — SqliMatchStatement

Pernyataan aturan kecocokan string

Pernyataan pencocokan string menunjukkan string yang AWS WAF ingin Anda cari dalam permintaan, di mana permintaan untuk mencari, dan bagaimana. Misalnya, Anda dapat mencari string tertentu di awal string kueri apa pun dalam permintaan atau sebagai pencocokan persis untuk

`User-agent` header permintaan. Biasanya, string terdiri dari karakter ASCII yang dapat dicetak, tetapi Anda dapat menggunakan karakter apa pun dari heksadesimal 0x00 hingga 0xFF (desimal 0 hingga 255).

Nestable - Anda dapat membuat jenis pernyataan ini.

WCU — Biaya dasar tergantung pada jenis kecocokan yang Anda gunakan.

- Tepat cocok dengan string — 2
- Dimulai dengan string - 2
- Berakhir dengan string — 2
- Berisi string - 10
- Berisi kata - 10

Jika Anda menggunakan komponen permintaan Semua parameter kueri, tambahkan 10 WCU. Jika Anda menggunakan isi JSON komponen permintaan, gandakan WCU biaya dasar. Untuk setiap transformasi Teks yang Anda terapkan, tambahkan 10 WCU.

Jenis pernyataan ini beroperasi pada komponen permintaan web, dan memerlukan pengaturan komponen permintaan berikut:

- Komponen permintaan — Bagian dari permintaan web untuk memeriksa, misalnya, string kueri atau badan.

  > **Warning**
  >
  > Jika Anda memeriksa komponen permintaan Body, JSON body, Header, atau Cookie, baca tentang batasan jumlah konten yang AWS WAF dapat diperiksa. Penanganan komponen permintaan kebesaran di AWS WAF

  Untuk informasi tentang komponen permintaan web, lihatSpesifikasi dan penanganan komponen permintaan web.
- Transformasi teks opsional — Transformasi yang AWS WAF ingin Anda lakukan pada komponen permintaan sebelum memeriksanya. Misalnya, Anda dapat mengubah ke huruf kecil atau menormalkan ruang putih. Jika Anda menentukan lebih dari satu transformasi, AWS WAF proses mereka dalam urutan yang tercantum. Untuk informasi, lihat Opsi transformasi teks.

Selain itu, pernyataan ini memerlukan pengaturan berikut:

- String to match - Ini adalah string yang AWS WAF ingin Anda bandingkan dengan komponen permintaan yang ditentukan. Biasanya, string terdiri dari karakter ASCII yang dapat dicetak, tetapi Anda dapat menggunakan karakter apa pun dari heksadesimal 0x00 hingga 0xFF (desimal 0 hingga 255).
- Kondisi pencocokan string - Ini menunjukkan jenis pencarian yang AWS WAF ingin Anda lakukan.
  - Tepat cocok dengan string - String dan nilai komponen permintaan identik.
  - Dimulai dengan string - String muncul di awal komponen permintaan.
  - Berakhir dengan string - String muncul di akhir komponen permintaan.
  - Berisi string - String muncul di mana saja dalam komponen permintaan.
  - Berisi kata - String yang Anda tentukan harus muncul di komponen permintaan.

    Untuk opsi ini, string yang Anda tentukan harus hanya berisi karakter alfanumerik atau garis bawah (A-Z, a-z, 0-9, atau _).

    Salah satu dari berikut ini harus benar agar permintaan cocok:
    - String sama persis dengan nilai komponen permintaan, seperti nilai header.
    - String berada di awal komponen permintaan dan diikuti oleh karakter selain karakter alfanumerik atau garis bawah (_), misalnya,. `BadBot;`
    - String berada di akhir komponen permintaan dan didahului oleh karakter selain karakter alfanumerik atau garis bawah (_), misalnya,. `;BadBot`
    - String berada di tengah komponen permintaan dan didahului dan diikuti oleh karakter selain karakter alfanumerik atau garis bawah (_), misalnya,. `-BadBot;`

Di mana menemukan pernyataan aturan ini

- Pembuat aturan di konsol — Untuk jenis Match, pilih Kondisi pencocokan String, lalu isi string yang ingin Anda cocokkan.
- API — ByteMatchStatement

Pernyataan aturan serangan skrip lintas situs

Pernyataan serangan XSS (cross-site scripting) memeriksa skrip berbahaya dalam komponen permintaan web. Dalam serangan XSS, penyerang menggunakan kerentanan di situs web jinak sebagai kendaraan untuk menyuntikkan skrip situs klien berbahaya ke browser web lain yang sah.

Nestable - Anda dapat membuat jenis pernyataan ini.

WCU — 40 WCU, sebagai biaya dasar. Jika Anda menggunakan komponen permintaan Semua parameter kueri, tambahkan 10 WCU. Jika Anda menggunakan isi JSON komponen permintaan, gandakan WCU biaya dasar. Untuk setiap transformasi Teks yang Anda terapkan, tambahkan 10 WCU.

Jenis pernyataan ini beroperasi pada komponen permintaan web, dan memerlukan pengaturan komponen permintaan berikut:

- Komponen permintaan — Bagian dari permintaan web untuk memeriksa, misalnya, string kueri atau badan.

  > **Warning**
  >
  > Jika Anda memeriksa komponen permintaan Badan, badan JSON, Header, atau Cookie, baca tentang batasan jumlah konten yang AWS WAF dapat diperiksa. Penanganan komponen permintaan kebesaran di AWS WAF

  Untuk informasi tentang komponen permintaan web, lihatSpesifikasi dan penanganan komponen permintaan web.
- Transformasi teks opsional — Transformasi yang AWS WAF ingin Anda lakukan pada komponen permintaan sebelum memeriksanya. Misalnya, Anda dapat mengubah ke huruf kecil atau menormalkan ruang putih. Jika Anda menentukan lebih dari satu transformasi, AWS WAF proses mereka dalam urutan yang tercantum. Untuk informasi, lihat Opsi transformasi teks.

Di mana menemukan pernyataan aturan ini

- Pembuat aturan di konsol — Untuk tipe Match, pilih Kondisi kecocokan serang > Mengandung serangan injeksi XSS.
- API — XssMatchStatement

Pernyataan aturan logis

Gunakan pernyataan aturan logis untuk menggabungkan pernyataan lain atau meniadakan hasilnya. Setiap pernyataan aturan logis membutuhkan setidaknya satu pernyataan bersarang.

Untuk secara logis menggabungkan atau meniadakan hasil pernyataan aturan, Anda menyarangkan pernyataan di bawah pernyataan aturan logis.

Pernyataan aturan logis adalah nestable. Anda dapat menyarangkannya di dalam pernyataan aturan logis lainnya dan menggunakannya dalam pernyataan cakupan ke bawah. Untuk informasi tentang pernyataan cakupan bawah, lihat. Pernyataan cakupan ke bawah

> **Note**
>
> Editor visual di konsol mendukung satu tingkat pernyataan aturan bersarang, yang berfungsi untuk banyak kebutuhan. Untuk membuat lebih banyak level, edit representasi JSON dari aturan di konsol atau gunakan API.

Tabel ini menjelaskan pernyataan aturan logis dan memberikan pedoman untuk menghitung penggunaan unit kapasitas ACL web (WCU) untuk masing-masing. Untuk informasi tentang WCU, lihatAWS WAF unit kapasitas ACL web (WCU).

Pernyataan Logis	Deskripsi	WCU
ANDlogika	Menggabungkan pernyataan bersarang dengan AND logika.	Berdasarkan pernyataan bersarang
NOTlogika	Menegasikan hasil pernyataan bersarang.	Berdasarkan pernyataan bersarang
ORlogika	Menggabungkan pernyataan bersarang dengan OR logika.	Berdasarkan pernyataan bersarang

ANDpernyataan aturan

Pernyataan AND aturan menggabungkan pernyataan bersarang dengan AND operasi logis, sehingga semua pernyataan bersarang harus cocok agar AND pernyataan tersebut cocok. Ini membutuhkan setidaknya dua pernyataan bersarang.

Nestable - Anda dapat membuat sarang jenis pernyataan ini.

WCU — Tergantung pada pernyataan bersarang.

Di mana menemukan pernyataan aturan ini

- Pembuat aturan di konsol — Untuk Jika permintaan, pilih cocok dengan semua pernyataan (AND), lalu isi pernyataan bersarang.
- API — AndStatement

Contoh

Daftar berikut menunjukkan penggunaan AND dan pernyataan aturan NOT logis untuk menghilangkan positif palsu dari kecocokan untuk pernyataan serangan injeksi SQL. Untuk contoh ini, misalkan kita dapat menulis pernyataan pencocokan byte tunggal untuk mencocokkan permintaan yang menghasilkan positif palsu.

Pernyataan AND cocok untuk permintaan yang tidak cocok dengan pernyataan pencocokan byte dan yang cocok dengan pernyataan serangan injeksi SQL.

```
{
      "Name": "SQLiExcludeFalsePositives",
      "Priority": 0,
      "Statement": {
        "AndStatement": {
          "Statements": [
            {
              "NotStatement": {
                "Statement": {
                  "ByteMatchStatement": {
                    "SearchString": "string identifying a false positive",
                    "FieldToMatch": {
                      "Body": {
                        "OversizeHandling": "MATCH"
                      }
```

```
                    },
                    "TextTransformations": [
                      {
                        "Priority": 0,
                        "Type": "NONE"
                      }
                    ],
                    "PositionalConstraint": "CONTAINS"
                  }
                }
              }
            },
            {
              "SqliMatchStatement": {
                "FieldToMatch": {
                  "Body": {
                    "OversizeHandling": "MATCH"
                  }
                },
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ]
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "SQLiExcludeFalsePositives"
      }
    }
```

Menggunakan editor visual aturan konsol, Anda dapat membuat pernyataan non-logis atau NOT pernyataan di bawah AND pernyataan OR atau. Penyarangan NOT pernyataan ditunjukkan pada contoh sebelumnya.

Menggunakan editor visual aturan konsol, Anda dapat membuat sarang sebagian besar pernyataan nestable di bawah pernyataan aturan logis, seperti yang ditunjukkan pada contoh sebelumnya. Anda tidak dapat menggunakan editor visual untuk membuat sarang OR atau AND pernyataan. Untuk mengonfigurasi jenis nesting ini, Anda perlu memberikan pernyataan aturan Anda di JSON. Misalnya, daftar aturan JSON berikut menyertakan OR pernyataan bersarang di dalam pernyataan. AND

```
{
  "Name": "match_rule",
  "Priority": 0,
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "awswaf:managed:aws:bot-control:bot:category:monitoring"
          }
        },
        {
          "NotStatement": {
            "Statement": {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:bot-control:bot:name:pingdom"
              }
            }
          }
        },
        {
          "OrStatement": {
            "Statements": [
              {
                "GeoMatchStatement": {
                  "CountryCodes": [
                    "JM",
                    "JP"
                  ]
                }
              },
              {
                "ByteMatchStatement": {
                  "SearchString": "JCountryString",
                  "FieldToMatch": {
```

```
                    "Body": {}
                  },
                  "TextTransformations": [
                    {
                      "Priority": 0,
                      "Type": "NONE"
                    }
                  ],
                  "PositionalConstraint": "CONTAINS"
                }
              }
            ]
          }
        }
      ]
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "match_rule"
  }
}
```

NOTpernyataan aturan

Pernyataan NOT aturan secara logis meniadakan hasil pernyataan bersarang tunggal, sehingga pernyataan bersarang tidak boleh cocok untuk NOT pernyataan yang cocok, dan sebaliknya. Ini membutuhkan satu pernyataan bersarang.

Misalnya, jika Anda ingin memblokir permintaan yang tidak berasal dari negara tertentu, buat NOT pernyataan dengan tindakan yang disetel ke blokir, dan sarang pernyataan kecocokan geografis yang menentukan negara.

Nestable - Anda dapat membuat jenis pernyataan ini.

WCU — Tergantung pada pernyataan bersarang.

Di mana menemukan pernyataan aturan ini

- Pembuat aturan di konsol — Untuk Jika permintaan, pilih tidak cocok dengan pernyataan (TIDAK), lalu isi pernyataan bersarang.
- API — NotStatement

ORpernyataan aturan

Pernyataan OR aturan menggabungkan pernyataan bersarang dengan OR logika, jadi salah satu pernyataan bersarang harus cocok agar OR pernyataan tersebut cocok. Ini membutuhkan setidaknya dua pernyataan bersarang.

Misalnya, jika Anda ingin memblokir permintaan yang berasal dari negara tertentu atau yang berisi string kueri tertentu, Anda dapat membuat OR pernyataan dan membuat pernyataan kecocokan geografis untuk negara dan pernyataan kecocokan string untuk string kueri.

Jika sebaliknya Anda ingin memblokir permintaan yang tidak berasal dari negara tertentu atau yang berisi string kueri tertentu, Anda akan memodifikasi OR pernyataan sebelumnya untuk menyarangkan pernyataan kecocokan geografis satu tingkat lebih rendah, di dalam NOT pernyataan. Tingkat bersarang ini mengharuskan Anda untuk menggunakan pemformatan JSON, karena konsol hanya mendukung satu tingkat bersarang.

Nestable - Anda dapat membuat jenis pernyataan ini.

WCU — Tergantung pada pernyataan bersarang.

Di mana menemukan pernyataan aturan ini

- Pembuat aturan di konsol — Untuk Jika permintaan, pilih kecocokan setidaknya salah satu pernyataan (OR), lalu isi pernyataan bersarang.
- API — OrStatement

Contoh

Daftar berikut menunjukkan penggunaan OR untuk menggabungkan dua pernyataan lainnya. ORPernyataan tersebut cocok jika salah satu pernyataan bersarang cocok.

```
{
  "Name": "neitherOfTwo",
  "Priority": 1,
```

```
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "neitherOfTwo"
  },
  "Statement": {
    "OrStatement": {
      "Statements": [
        {
          "GeoMatchStatement": {
            "CountryCodes": [
              "CA"
            ]
          }
        },
        {
          "IPSetReferenceStatement": {
            "ARN": "arn:aws:wafv2:us-east-1:111111111111:regional/ipset/test-ip-
set-22222222/33333333-4444-5555-6666-777777777777"
          }
        }
      ]
    }
  }
}
```

Menggunakan editor visual aturan konsol, Anda dapat membuat sarang sebagian besar pernyataan nestable di bawah pernyataan aturan logis, tetapi Anda tidak dapat menggunakan editor visual untuk membuat sarang OR atau AND pernyataan. Untuk mengonfigurasi jenis nesting ini, Anda perlu memberikan pernyataan aturan Anda di JSON. Misalnya, daftar aturan JSON berikut menyertakan OR pernyataan bersarang di dalam pernyataan. AND

```
{
  "Name": "match_rule",
  "Priority": 0,
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "LabelMatchStatement": {
```

```
            "Scope": "LABEL",
            "Key": "awswaf:managed:aws:bot-control:bot:category:monitoring"
          }
        },
        {
          "NotStatement": {
            "Statement": {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:bot-control:bot:name:pingdom"
              }
            }
          }
        },
        {
          "OrStatement": {
            "Statements": [
              {
                "GeoMatchStatement": {
                  "CountryCodes": [
                    "JM",
                    "JP"
                  ]
                }
              },
              {
                "ByteMatchStatement": {
                  "SearchString": "JCountryString",
                  "FieldToMatch": {
                    "Body": {}
                  },
                  "TextTransformations": [
                    {
                      "Priority": 0,
                      "Type": "NONE"
                    }
                  ],
                  "PositionalConstraint": "CONTAINS"
                }
              }
            ]
          }
        }
      ]
```

```
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "match_rule"
  }
}
```

Pernyataan aturan berbasis tarif

Aturan berbasis tarif menghitung permintaan masuk dan permintaan batas tarif ketika permintaan tersebut datang dengan tarif yang terlalu cepat. Aturan menggabungkan permintaan sesuai dengan kriteria Anda, dan menghitung serta membatasi pengelompokan agregat, berdasarkan jendela evaluasi aturan, batas permintaan, dan setelan tindakan.

> **Note**
>
> Anda juga dapat menilai batas permintaan web menggunakan tingkat perlindungan yang ditargetkan dari grup aturan Aturan AWS Terkelola Kontrol Bot. Menggunakan grup aturan terkelola ini menimbulkan biaya tambahan. Untuk informasi selengkapnya, lihat Opsi untuk membatasi tarif dalam aturan berbasis tarif dan aturan Kontrol Bot yang ditargetkan.

AWS WAF melacak dan mengelola permintaan web secara terpisah untuk setiap instance aturan berbasis tarif yang Anda gunakan. Misalnya, jika Anda memberikan pengaturan aturan berbasis laju yang sama di dua ACL web, masing-masing dari dua pernyataan aturan mewakili instance terpisah dari aturan berbasis laju dan masing-masing mendapatkan pelacakan dan pengelolaannya sendiri. AWS WAF Jika Anda menentukan aturan berbasis laju di dalam grup aturan, dan kemudian menggunakan grup aturan itu di beberapa tempat, setiap penggunaan akan membuat instance terpisah dari aturan berbasis tarif yang mendapatkan pelacakan dan pengelolaannya sendiri. AWS WAF

Tidak bersarang - Anda tidak dapat membuat jenis pernyataan ini di dalam pernyataan lain. Anda dapat memasukkannya langsung ke dalam ACL web atau grup aturan.

Scope-down statement — Jenis aturan ini dapat mengambil pernyataan scope-down, untuk mempersempit ruang lingkup permintaan yang dilacak aturan dan batas nilai. Pernyataan cakupan bawah dapat bersifat opsional atau wajib, tergantung pada pengaturan konfigurasi aturan Anda yang lain. Detailnya tercakup dalam bagian ini. Untuk informasi umum tentang pernyataan cakupan bawah, lihat. Pernyataan cakupan ke bawah

WCU — 2, sebagai biaya dasar. Untuk setiap kunci agregasi kustom yang Anda tentukan, tambahkan 30 WCU. Jika Anda menggunakan pernyataan scope-down dalam aturan, hitung dan tambahkan WCU untuk itu.

Di mana menemukan pernyataan aturan ini

- Pembuat aturan di ACL web Anda, di konsol — Di bawah Aturan, untuk Jenis, pilih Aturan berbasis tarif.
- API — RateBasedStatement

Topik

- Pengaturan tingkat tinggi aturan berbasis tarif
- Peringatan aturan berbasis tarif
- Opsi dan kunci agregasi aturan berbasis tarif
- Contoh dan hitungan agregasi aturan berbasis tarif
- Perilaku membatasi tingkat permintaan aturan berbasis tarif
- Contoh aturan berbasis tarif
- Daftar alamat IP yang dibatasi oleh aturan berbasis tarif

Pengaturan tingkat tinggi aturan berbasis tarif

Pernyataan aturan berbasis tarif menggunakan pengaturan tingkat tinggi berikut:

- Jendela evaluasi — Jumlah waktu, dalam hitungan detik, yang AWS WAF harus dimasukkan dalam jumlah permintaannya, melihat ke belakang dari waktu saat ini. Misalnya, untuk pengaturan 120, ketika AWS WAF memeriksa tarif, itu menghitung permintaan untuk 2 menit segera sebelum waktu saat ini. Pengaturan yang valid adalah 60 (1 menit), 120 (2 menit), 300 (5 menit), dan 600 (10 menit), dan 300 (5 menit) adalah default.

Pengaturan ini tidak menentukan seberapa sering AWS WAF memeriksa tarif, tetapi seberapa jauh tampilannya setiap kali memeriksa. AWS WAF memeriksa tarif sering, dengan waktu yang independen dari pengaturan jendela evaluasi.

- Batas tarif - Jumlah maksimum permintaan yang sesuai dengan kriteria Anda yang AWS WAF seharusnya hanya melacak untuk jendela evaluasi yang ditentukan. Pengaturan batas terendah yang diizinkan adalah 100. Saat batas ini dilanggar, AWS WAF terapkan pengaturan tindakan aturan ke permintaan tambahan yang sesuai dengan kriteria Anda.

  AWS WAF menerapkan pembatasan tarif mendekati batas yang Anda tetapkan, tetapi tidak menjamin kecocokan batas yang tepat. Untuk informasi selengkapnya, lihat Peringatan aturan berbasis tarif.
- Agregasi permintaan — Kriteria agregasi yang digunakan di web meminta agar aturan berbasis tarif dihitung dan batas tarif. Batas tarif yang Anda tetapkan berlaku untuk setiap instance agregasi. Untuk detailnya, lihat Opsi dan kunci agregasi dan Contoh dan hitungan agregasi.
- Tindakan — Tindakan yang harus diambil atas permintaan yang dibatasi oleh tarif aturan. Anda dapat menggunakan tindakan aturan apa pun kecualiAllow. Ini ditetapkan pada tingkat aturan seperti biasa, tetapi memiliki beberapa batasan dan perilaku yang khusus untuk aturan berbasis tarif. Untuk informasi umum tentang tindakan aturan, lihatTindakan aturan. Untuk informasi khusus tentang pembatasan tarif, lihat Perilaku membatasi tingkat permintaan aturan berbasis tarif di bagian ini.
- Lingkup inspeksi dan pembatasan tarif — Anda dapat mempersempit cakupan permintaan yang dilacak pernyataan berbasis tarif dan batas tarif dengan menambahkan pernyataan cakupan ke bawah. Jika Anda menentukan pernyataan cakupan bawah, aturan hanya mengumpulkan, menghitung, dan membatasi permintaan yang cocok dengan pernyataan cakupan bawah. Jika Anda memilih opsi agregasi permintaan Hitung semua, maka pernyataan cakupan bawah diperlukan. Untuk informasi selengkapnya tentang pernyataan cakupan bawah, lihat. Pernyataan cakupan ke bawah
- (Opsional) Konfigurasi IP yang diteruskan - Ini hanya digunakan jika Anda menentukan alamat IP di header dalam agregasi permintaan Anda, baik sendiri atau sebagai bagian dari pengaturan kunci khusus. AWS WAF mengambil alamat IP pertama di header yang ditentukan dan menggunakannya sebagai nilai agregasi. Header umum untuk tujuan ini adalah`X-Forwarded-For`, tetapi Anda dapat menentukan header apa pun. Untuk informasi selengkapnya, lihat Alamat IP yang diteruskan.

Peringatan aturan berbasis tarif

AWS WAF Pembatasan tarif dirancang untuk mengontrol tingkat permintaan yang tinggi dan melindungi ketersediaan aplikasi Anda dengan cara yang paling efisien dan efektif. Ini tidak dimaksudkan untuk pembatasan tingkat permintaan yang tepat.

- AWS WAF memperkirakan tingkat permintaan saat ini menggunakan algoritme yang lebih mementingkan permintaan yang lebih baru. Karena itu, AWS WAF akan berlaku pembatasan tarif mendekati batas yang Anda tetapkan, tetapi tidak menjamin kecocokan batas yang tepat.
- Setiap kali AWS WAF memperkirakan tingkat permintaan, AWS WAF melihat kembali jumlah permintaan yang masuk selama jendela evaluasi yang dikonfigurasi. Karena ini dan faktor lain seperti penundaan propagasi, permintaan mungkin masuk dengan kecepatan yang terlalu tinggi hingga beberapa menit sebelum AWS WAF mendeteksi dan membatasi nilainya. Serupa. tingkat permintaan dapat berada di bawah batas untuk jangka waktu tertentu sebelum AWS WAF mendeteksi penurunan dan menghentikan tindakan pembatasan laju. Biasanya, penundaan ini di bawah 30 detik.
- Jika Anda mengubah setelan batas tarif apa pun dalam aturan yang sedang digunakan, perubahan akan mengatur ulang jumlah pembatasan tarif aturan. Ini dapat menjeda aktivitas pembatasan tarif aturan hingga satu menit. Pengaturan batas tarif adalah jendela evaluasi, batas tarif, pengaturan agregasi permintaan, konfigurasi IP yang diteruskan, dan ruang lingkup inspeksi.

Opsi dan kunci agregasi aturan berbasis tarif

Secara default, aturan berbasis tarif mengumpulkan dan membatasi permintaan berdasarkan alamat IP permintaan. Anda dapat mengonfigurasi aturan untuk menggunakan berbagai tombol agregasi dan kombinasi tombol lainnya. Misalnya, Anda dapat menggabungkan berdasarkan alamat IP yang diteruskan, pada metode HTTP, atau pada argumen kueri. Anda juga dapat menentukan kombinasi tombol agregasi, seperti alamat IP dan metode HTTP, atau nilai dari dua cookie yang berbeda.

> **Note**
>
> Semua komponen permintaan yang Anda tentukan dalam kunci agregasi harus ada dalam permintaan web untuk permintaan yang akan dievaluasi atau tarif dibatasi oleh aturan.

Anda dapat mengonfigurasi aturan berbasis tarif dengan opsi agregasi berikut.

- Alamat IP Sumber — Agregat hanya menggunakan alamat IP dari asal permintaan web.

Alamat IP sumber mungkin tidak berisi alamat klien asal. Jika permintaan web melewati satu atau lebih proxy atau penyeimbang beban, ini akan berisi alamat proxy terakhir.

- Alamat IP di header - Agregat hanya menggunakan alamat klien di header HTTP. Ini juga disebut sebagai alamat IP yang diteruskan.

  Dengan konfigurasi ini, Anda juga menentukan perilaku fallback untuk diterapkan ke permintaan web dengan alamat IP cacat di header. Perilaku fallback menetapkan hasil pencocokan untuk permintaan, agar cocok atau tidak cocok. Untuk tidak ada kecocokan, aturan berbasis tarif tidak menghitung atau membatasi nilai permintaan. Untuk kecocokan, aturan berbasis laju mengelompokkan permintaan bersama dengan permintaan lain yang memiliki alamat IP cacat di header yang ditentukan.

  Berhati-hatilah dengan opsi ini, karena header dapat ditangani secara tidak konsisten oleh proxy dan mereka juga dapat dimodifikasi untuk melewati inspeksi. Untuk informasi tambahan dan praktik terbaik, lihatAlamat IP yang diteruskan.
- Hitung semua — Hitung dan batasi nilai semua permintaan yang cocok dengan pernyataan cakupan bawah aturan. Opsi ini membutuhkan pernyataan cakupan ke bawah. Ini biasanya digunakan untuk membatasi serangkaian permintaan tertentu, seperti semua permintaan dengan label tertentu atau semua permintaan dari wilayah geografis tertentu.
- Kunci kustom - Agregat menggunakan satu atau lebih kunci agregasi kustom. Untuk menggabungkan salah satu opsi alamat IP dengan kunci agregasi lainnya, tentukan di sini di bawah kunci khusus.

  Kunci agregasi kustom adalah bagian dari opsi komponen permintaan web yang dijelaskan di. Minta opsi komponen

  Opsi utamanya adalah sebagai berikut. Kecuali jika dicatat, Anda dapat menggunakan opsi beberapa kali, misalnya, dua header atau tiga ruang nama label.

  - Namespace label — Gunakan namespace label sebagai kunci agregasi. Setiap nama label yang memenuhi syarat lengkap yang memiliki namespace label yang ditentukan berkontribusi pada instance agregasi. Jika Anda hanya menggunakan satu namespace label sebagai kunci kustom Anda, maka setiap nama label sepenuhnya mendefinisikan instance agregasi.

    Aturan berbasis tarif hanya menggunakan label yang telah ditambahkan ke permintaan dengan aturan yang dievaluasi sebelumnya di ACL web.

Untuk informasi tentang ruang nama label dan nama, lihat. AWS WAF sintaks label dan persyaratan penamaan

- Header — Gunakan header bernama sebagai kunci agregasi. Setiap nilai yang berbeda di header berkontribusi pada contoh agregasi.

  Header mengambil transformasi teks opsional. Lihat Opsi transformasi teks.

- Cookie — Gunakan cookie bernama sebagai kunci agregasi. Setiap nilai yang berbeda dalam cookie berkontribusi pada contoh agregasi.

  Cookie mengambil transformasi teks opsional. Lihat Opsi transformasi teks.

- Argumen kueri — Gunakan argumen kueri tunggal dalam permintaan sebagai kunci agregat. Setiap nilai yang berbeda untuk argumen kueri bernama berkontribusi pada contoh agregasi.

  Argumen kueri mengambil transformasi teks opsional. Lihat Opsi transformasi teks.

- Query string - Gunakan seluruh string query dalam permintaan sebagai kunci agregat. Setiap string kueri yang berbeda berkontribusi pada contoh agregasi. Anda dapat menggunakan jenis kunci ini sekali.

  String kueri mengambil transformasi teks opsional. Lihat Opsi transformasi teks.

- Jalur URI — Gunakan jalur URI dalam permintaan sebagai kunci agregat. Setiap jalur URI yang berbeda berkontribusi pada instance agregasi. Anda dapat menggunakan jenis kunci ini sekali.

  Jalur URI mengambil transformasi teks opsional. Lihat Opsi transformasi teks.

- Metode HTTP — Gunakan metode HTTP permintaan sebagai kunci agregat. Setiap metode HTTP yang berbeda berkontribusi pada instance agregasi. Anda dapat menggunakan jenis kunci ini sekali.

- Alamat IP — Agregat menggunakan alamat IP dari asal permintaan web dalam kombinasi dengan tombol lain.

  Ini mungkin tidak berisi alamat klien asal. Jika permintaan web melewati satu atau lebih proxy atau penyeimbang beban, ini akan berisi alamat proxy terakhir.

- Alamat IP di header — Agregat menggunakan alamat klien dalam header HTTP dalam kombinasi dengan tombol lain. Ini juga disebut sebagai alamat IP yang diteruskan.

  Berhati-hatilah dengan opsi ini, karena header dapat ditangani secara tidak konsisten oleh proxy dan mereka dapat dimodifikasi untuk melewati inspeksi. Untuk informasi tambahan dan praktik terbaik, lihatAlamat IP yang diteruskan.

Contoh dan hitungan agregasi aturan berbasis tarif

Saat aturan berbasis laju mengevaluasi permintaan web menggunakan kriteria agregasi Anda, setiap kumpulan nilai unik yang ditemukan aturan untuk kunci agregasi yang ditentukan menentukan instance agregasi unik.

- Beberapa kunci — Jika Anda telah menetapkan beberapa kunci kustom, nilai untuk setiap kunci berkontribusi pada definisi instance agregasi. Setiap kombinasi nilai yang unik mendefinisikan contoh agregasi.
- Kunci tunggal — Jika Anda telah memilih satu kunci, baik dalam kunci kustom atau dengan memilih salah satu pilihan alamat IP tunggal, maka setiap nilai unik untuk kunci mendefinisikan contoh agregasi.
- Hitung semua - tidak ada kunci - Jika Anda telah memilih opsi agregasi Hitung semua, maka semua permintaan yang dievaluasi aturan termasuk dalam contoh agregasi tunggal untuk aturan tersebut. Pilihan ini membutuhkan pernyataan cakupan ke bawah.

Aturan berbasis tarif menghitung permintaan web secara terpisah untuk setiap instance agregasi yang diidentifikasi.

Misalnya, asumsikan aturan berbasis tarif mengevaluasi permintaan web dengan alamat IP berikut dan nilai metode HTTP:

- Alamat IP 10.1.1.1, metode HTTP POST
- Alamat IP 10.1.1.1, metode HTTP GET
- Alamat IP 127.0.0.0, metode HTTP POST
- Alamat IP 10.1.1.1, metode HTTP GET

Aturan membuat instance agregasi yang berbeda sesuai dengan kriteria agregasi Anda.

- Jika kriteria agregasi hanya alamat IP, maka setiap alamat IP individu adalah contoh agregasi, dan AWS WAF menghitung permintaan secara terpisah untuk masing-masing. Contoh agregasi dan jumlah permintaan untuk contoh kami adalah sebagai berikut:
  - Alamat IP 10.1.1.1: hitungan 3
  - Alamat IP 127.0.0.0: hitung 1

- Jika kriteria agregasi adalah metode HTTP, maka setiap metode HTTP individu adalah contoh agregasi. Contoh agregasi dan jumlah permintaan untuk contoh kami adalah sebagai berikut:
  - Metode HTTP POST: hitung 2
  - Metode HTTP GET: hitung 2
- Jika kriteria agregasi adalah alamat IP dan metode HTTP, maka setiap alamat IP dan setiap metode HTTP akan berkontribusi pada contoh agregasi gabungan. Contoh agregasi dan jumlah permintaan untuk contoh kami adalah sebagai berikut:
  - Alamat IP 10.1.1.1, metode HTTP POST: hitungan 1
  - Alamat IP 10.1.1.1, metode HTTP GET: hitung 2
  - Alamat IP 127.0.0.0, metode HTTP POST: hitungan 1

Perilaku membatasi tingkat permintaan aturan berbasis tarif

Kriteria yang AWS WAF digunakan untuk menilai permintaan batas untuk aturan berbasis tarif adalah kriteria yang sama yang AWS WAF digunakan untuk menggabungkan permintaan untuk aturan tersebut. Jika Anda menentukan pernyataan cakupan bawah untuk aturan, AWS WAF hanya agregat, hitungan, dan batas nilai permintaan yang cocok dengan pernyataan cakupan bawah.

Kriteria pencocokan yang menyebabkan aturan berbasis laju menerapkan pengaturan tindakan aturannya ke permintaan web tertentu adalah sebagai berikut:

- Permintaan web cocok dengan pernyataan cakupan bawah aturan, jika ada yang didefinisikan.
- Permintaan web milik instance agregasi yang jumlah permintaannya saat ini melebihi batas aturan.

Bagaimana AWS WAF menerapkan tindakan aturan

Jika aturan berbasis laju menerapkan pembatasan laju pada permintaan, aturan tersebut akan menerapkan tindakan aturan dan, jika Anda telah menetapkan penanganan atau pelabelan khusus apa pun dalam spesifikasi tindakan Anda, aturan tersebut akan menerapkannya. Penanganan permintaan ini sama dengan cara aturan pencocokan menerapkan pengaturan tindakannya untuk mencocokkan permintaan web. Aturan berbasis tarif hanya menerapkan label atau melakukan tindakan lain pada permintaan yang membatasi tarif secara aktif.

Anda dapat menggunakan tindakan aturan apa pun kecualiAllow. Untuk informasi umum tentang tindakan aturan, lihatTindakan aturan.

Daftar berikut menjelaskan cara kerja pembatasan laju untuk setiap tindakan.

- Block— AWS WAF memblokir permintaan dan menerapkan perilaku pemblokiran khusus apa pun yang telah Anda tentukan.
- Count— AWS WAF menghitung permintaan, menerapkan header atau label khusus yang telah Anda tetapkan, dan melanjutkan evaluasi ACL web dari permintaan tersebut.

  Tindakan ini tidak membatasi tingkat permintaan. Itu hanya menghitung permintaan yang melebihi batas.
- CAPTCHAatau Challenge — AWS WAF menangani permintaan baik seperti Block atau sepertiCount, tergantung pada status token permintaan.

  Tindakan ini tidak membatasi tingkat permintaan yang memiliki token yang valid. Ini membatasi tingkat permintaan yang melebihi batas dan juga kehilangan token yang valid.
  - Jika permintaan tidak memiliki token yang valid dan belum kedaluwarsa, tindakan akan memblokir permintaan dan mengirimkan teka-teki CAPTCHA atau tantangan browser kembali ke klien.

    Jika pengguna akhir atau browser klien merespons dengan sukses, klien menerima token yang valid dan secara otomatis mengirimkan ulang permintaan asli. Jika pembatasan tarif untuk instance agregasi masih berlaku, permintaan baru ini dengan token yang valid dan belum kedaluwarsa akan memiliki tindakan yang diterapkan padanya seperti yang dijelaskan dalam bullet point berikutnya.
  - Jika permintaan memiliki token yang valid dan belum kedaluwarsa, Challenge tindakan CAPTCHA atau memverifikasi token dan tidak mengambil tindakan atas permintaan tersebut, mirip dengan tindakan tersebut. Count Aturan berbasis tarif mengembalikan evaluasi permintaan kembali ke ACL web tanpa mengambil tindakan penghentian apa pun, dan ACL web melanjutkan evaluasi permintaan tersebut.

  Untuk informasi tambahan, lihat CAPTCHAdan Challenge di AWS WAF.

Jika Anda menilai batas hanya alamat IP atau alamat IP yang diteruskan

Saat Anda mengonfigurasi aturan untuk membatasi hanya alamat IP untuk alamat IP yang diteruskan, instance aturan dapat membatasi hingga 10.000 alamat IP. Jika instance aturan mengidentifikasi lebih dari 10.000 alamat IP untuk menilai batas, itu hanya membatasi 10.000 pengirim tertinggi.

Dengan konfigurasi ini, Anda dapat mengambil daftar alamat IP yang saat ini dibatasi oleh aturan berbasis tarif. Jika Anda menggunakan pernyataan cakupan bawah, permintaan yang dibatasi tarif

hanya yang ada dalam daftar IP yang cocok dengan pernyataan cakupan bawah. Untuk informasi tentang mengambil daftar alamat IP, lihatDaftar alamat IP yang dibatasi oleh aturan berbasis tarif.

Contoh aturan berbasis tarif

Bagian ini menjelaskan contoh konfigurasi untuk berbagai kasus penggunaan aturan berbasis tarif umum.

Setiap contoh memberikan deskripsi kasus penggunaan dan kemudian menunjukkan solusi dalam daftar JSON untuk aturan yang dikonfigurasi khusus.

> **Note**
>
> Daftar JSON yang ditampilkan dalam contoh ini dibuat di konsol dengan mengonfigurasi aturan dan kemudian mengeditnya menggunakan editor Rule JSON.

Topik

- Nilai membatasi permintaan ke halaman login
- Nilai membatasi permintaan ke halaman login dari alamat IP apa pun, pasangan agen pengguna
- Batasi nilai permintaan yang tidak memiliki header tertentu
- Nilai membatasi permintaan dengan label tertentu
- Nilai batas permintaan untuk label yang memiliki namespace label tertentu

Nilai membatasi permintaan ke halaman login

Untuk membatasi jumlah permintaan ke halaman login di situs web Anda tanpa memengaruhi lalu lintas ke seluruh situs Anda, Anda dapat membuat aturan berbasis tarif dengan pernyataan cakupan bawah yang cocok dengan permintaan ke halaman login Anda dan dengan agregasi permintaan diatur ke Hitung semua.

Aturan berbasis tarif akan menghitung semua permintaan untuk halaman login dalam satu contoh agregasi dan menerapkan tindakan aturan ketika permintaan melebihi batas.

Daftar JSON berikut menunjukkan contoh konfigurasi aturan ini. Opsi hitung semua agregasi tercantum di JSON sebagai pengaturan. `CONSTANT` Contoh ini cocok dengan halaman login yang dimulai dengan`/login`.

```
{
```

```
  "Name": "test-rbr",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-rbr"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": 1000,
      "EvaluationWindowSec": 300,
      "AggregateKeyType": "CONSTANT",
      "ScopeDownStatement": {
        "ByteMatchStatement": {
          "FieldToMatch": {
            "UriPath": {}
          },
          "PositionalConstraint": "STARTS_WITH",
          "SearchString": "/login",
          "TextTransformations": [
            {
              "Type": "NONE",
              "Priority": 0
            }
          ]
        }
      }
    }
  }
}
```

Nilai membatasi permintaan ke halaman login dari alamat IP apa pun, pasangan agen pengguna

Untuk membatasi jumlah permintaan ke halaman login di situs web Anda untuk alamat IP, pasangan agen pengguna yang melebihi batas Anda, atur agregasi permintaan ke kunci Kustom dan berikan kriteria agregasi.

Daftar JSON berikut menunjukkan contoh konfigurasi aturan ini. Dalam contoh ini, kami telah menetapkan batas untuk 100 permintaan dalam periode lima menit per alamat IP, pasangan agen pengguna.

```
{
  "Name": "test-rbr",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-rbr"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": 100,
      "EvaluationWindowSec": 300,
      "AggregateKeyType": "CUSTOM_KEYS",
      "CustomKeys": [
        {
          "Header": {
            "Name": "User-Agent",
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
        },
        {
          "IP": {}
        }
      ],
      "ScopeDownStatement": {
        "ByteMatchStatement": {
          "FieldToMatch": {
            "UriPath": {}
          },
          "PositionalConstraint": "STARTS_WITH",
          "SearchString": "/login",
          "TextTransformations": [
            {
              "Type": "NONE",
              "Priority": 0
```

```
            }
          ]
        }
      }
    }
  }
}
```

Batasi nilai permintaan yang tidak memiliki header tertentu

Untuk membatasi jumlah permintaan yang tidak memiliki header tertentu, Anda dapat menggunakan opsi Hitung semua agregasi dengan pernyataan cakupan bawah. Konfigurasikan pernyataan scope-down dengan `NOT` pernyataan logis yang berisi pernyataan yang mengembalikan true hanya jika header ada dan memiliki nilai.

Daftar JSON berikut menunjukkan contoh konfigurasi aturan ini.

```
{
  "Name": "test-rbr",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-rbr"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": 1000,
      "AggregateKeyType": "CONSTANT",
      "EvaluationWindowSec": 300,
      "ScopeDownStatement": {
        "NotStatement": {
          "Statement": {
            "SizeConstraintStatement": {
              "FieldToMatch": {
                "SingleHeader": {
                  "Name": "user-agent"
                }
              },
              "ComparisonOperator": "GT",
```

```
              "Size": 0,
              "TextTransformations": [
                {
                  "Type": "NONE",
                  "Priority": 0
                }
              ]
            }
          }
        }
      }
    }
  }
}
```

Nilai membatasi permintaan dengan label tertentu

Anda dapat menggabungkan pembatasan tarif dengan aturan atau grup aturan apa pun yang menambahkan label ke permintaan, untuk membatasi jumlah permintaan dari berbagai kategori. Untuk melakukan ini, Anda mengonfigurasi ACL web Anda sebagai berikut:

- Tambahkan aturan atau grup aturan yang menambahkan label, dan konfigurasikan agar tidak memblokir atau mengizinkan permintaan yang ingin Anda beri batas nilai. Jika Anda menggunakan grup aturan terkelola, Anda mungkin perlu mengganti beberapa tindakan aturan grup aturan Count untuk mencapai perilaku ini.
- Tambahkan aturan berbasis tarif ke ACL web Anda dengan pengaturan nomor prioritas yang lebih tinggi dari aturan pelabelan dan grup aturan. AWS WAF mengevaluasi aturan dalam urutan numerik, mulai dari yang terendah, sehingga aturan berbasis tarif Anda akan berjalan setelah aturan pelabelan. Konfigurasikan batasan tarif Anda pada label menggunakan kombinasi pencocokan label dalam pernyataan cakupan bawah aturan dan agregasi label.

Contoh berikut menggunakan grup aturan Aturan AWS Terkelola daftar reputasi IP Amazon. Aturan grup aturan `AWSManagedIPDDoSList` mendeteksi dan memberi label permintaan yang IPnya diketahui aktif terlibat dalam aktivitas DDoS. Tindakan aturan dikonfigurasi Count dalam definisi grup aturan. Untuk informasi selengkapnya tentang grup aturan, lihatthe section called “Daftar reputasi IP Amazon”.

Daftar ACL JSON web berikut menggunakan grup aturan reputasi IP diikuti oleh aturan berbasis tingkat pencocokan label. Aturan berbasis laju menggunakan pernyataan scope-down untuk

memfilter permintaan yang telah ditandai oleh aturan grup aturan. Pernyataan aturan berbasis tingkat agregat dan nilai membatasi permintaan yang difilter oleh alamat IP mereka.

```
{
  "Name": "test-web-acl",
  "Id": ...
  "ARN": ...
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesAmazonIpReputationList",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesAmazonIpReputationList"
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesAmazonIpReputationList"
      }
    },
    {
      "Name": "test-rbr",
      "Priority": 1,
      "Statement": {
        "RateBasedStatement": {
          "Limit": 100,
          "EvaluationWindowSec": 300,
          "AggregateKeyType": "IP",
          "ScopeDownStatement": {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:amazon-ip-list:AWSManagedIPDDoSList"
            }
```

```
          }
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "test-rbr"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-web-acl"
  },
  "Capacity": 28,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:0000000000:webacl:test-web-acl:"
}
```

Nilai batas permintaan untuk label yang memiliki namespace label tertentu

Aturan tingkat umum dalam grup aturan terkelola Bot Control menambahkan label untuk bot dari berbagai kategori, tetapi mereka hanya memblokir permintaan dari bot yang tidak diverifikasi. Untuk informasi tentang aturan ini, lihatDaftar aturan Bot Control.

Jika Anda menggunakan grup aturan terkelola Kontrol Bot, Anda dapat menambahkan batasan tarif untuk permintaan dari bot terverifikasi individual. Untuk melakukan ini, Anda menambahkan aturan berbasis kecepatan yang berjalan setelah grup aturan Kontrol Bot dan agregat permintaan berdasarkan label nama bot mereka. Anda menentukan kunci agregasi namespace Label dan mengatur kunci namespace ke. `awswaf:managed:aws:bot-control:bot:name:` Setiap label unik dengan namespace yang ditentukan akan menentukan contoh agregasi. Misalnya, label `awswaf:managed:aws:bot-control:bot:name:axios` dan `awswaf:managed:aws:bot-control:bot:name:curl` masing-masing mendefinisikan contoh agregasi.

Daftar ACL JSON web berikut menunjukkan konfigurasi ini. Aturan dalam contoh ini membatasi permintaan untuk setiap instance agregasi bot tunggal menjadi 1.000 dalam periode dua menit.

```
{
```

```
  "Name": "test-web-acl",
  "Id": ...
  "ARN": ...
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesBotControlRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesBotControlRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesBotControlRuleSet": {
                "InspectionLevel": "COMMON"
              }
            }
          ]
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesBotControlRuleSet"
      }
    },
    {
      "Name": "test-rbr",
      "Priority": 1,
      "Statement": {
        "RateBasedStatement": {
          "Limit": 1000,
          "EvaluationWindowSec": 120,
          "AggregateKeyType": "CUSTOM_KEYS",
          "CustomKeys": [
            {
              "LabelNamespace": {
```

```
                "Namespace": "awswaf:managed:aws:bot-control:bot:name:"
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "test-rbr"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-web-acl"
  },
  "Capacity": 82,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:0000000000:webacl:test-web-acl:"
}
```

Daftar alamat IP yang dibatasi oleh aturan berbasis tarif

Jika aturan berbasis tarif Anda hanya agregat pada alamat IP atau alamat IP yang diteruskan, Anda dapat mengambil daftar alamat IP yang aturan saat ini membatasi tarif. AWS WAF menyimpan alamat IP ini dalam daftar kunci terkelola aturan.

> **Note**
>
> Opsi ini hanya tersedia jika Anda menggabungkan hanya alamat IP atau hanya alamat IP di header. Jika Anda menggunakan agregasi permintaan kunci kustom, Anda tidak dapat mengambil daftar alamat IP terbatas tarif, bahkan jika Anda menggunakan salah satu spesifikasi alamat IP di kunci kustom Anda.

Aturan berbasis laju menerapkan tindakan aturannya ke permintaan dari daftar kunci terkelola aturan yang cocok dengan pernyataan cakupan bawah aturan. Ketika aturan tidak memiliki pernyataan

cakupan bawah, itu menerapkan tindakan untuk semua permintaan dari alamat IP yang ada dalam daftar. Tindakan aturan secara Block default, tetapi dapat berupa tindakan aturan yang valid kecuali untukAllow. Jumlah maksimum alamat IP yang AWS WAF dapat membatasi nilai menggunakan instance aturan berbasis tarif tunggal adalah 10.000. Jika lebih dari 10.000 alamat melebihi batas tarif, AWS WAF batasi alamat dengan tarif tertinggi.

Anda dapat mengakses daftar kunci terkelola aturan berbasis laju menggunakan CLI, API, atau SDK mana pun. Topik ini mencakup akses menggunakan CLI dan API. Konsol tidak menyediakan akses ke daftar saat ini.

Untuk AWS WAF API, perintahnya adalah GetRateBasedStatementManagedKeys.

Untuk AWS WAF CLI, perintahnya adalah get-rate-based-statement -managed-keys.

Berikut ini menunjukkan sintaks untuk mengambil daftar alamat IP terbatas tingkat untuk aturan berbasis tarif yang digunakan dalam ACL web pada distribusi Amazon. CloudFront

```
aws wafv2 get-rate-based-statement-managed-keys --scope=CLOUDFRONT --region=us-east-1
 --web-acl-name=WebACLName --web-acl-id=WebACLId --rule-name=RuleName
```

Berikut ini menunjukkan sintaks untuk aplikasi regional, Amazon API Gateway REST API, Application Load Balancer, API AWS AppSync GraphQL, kumpulan pengguna Amazon Cognito, layanan AWS App Runner , atau instance Akses Terverifikasi. AWS

```
aws wafv2 get-rate-based-statement-managed-keys --scope=REGIONAL --region=region --web-
acl-name=WebACLName --web-acl-id=WebACLId --rule-name=RuleName
```

AWS WAF memantau permintaan web dan mengelola kunci secara independen untuk setiap kombinasi unik ACL web, grup aturan opsional, dan aturan berbasis tarif. Misalnya, jika Anda menentukan aturan berbasis laju di dalam grup aturan, dan kemudian menggunakan grup aturan di ACL web, AWS WAF memantau permintaan web dan mengelola kunci untuk ACL web tersebut, pernyataan referensi grup aturan, dan contoh aturan berbasis tarif. Jika Anda menggunakan grup aturan yang sama di ACL web kedua, AWS WAF memantau permintaan web dan mengelola kunci untuk penggunaan kedua ini sepenuhnya independen dari yang pertama.

Untuk aturan berbasis laju yang telah Anda tetapkan di dalam grup aturan, Anda perlu memberikan nama pernyataan referensi grup aturan dalam permintaan Anda, selain nama ACL web dan nama aturan berbasis laju di dalam grup aturan. Berikut ini menunjukkan sintaks untuk aplikasi regional di mana aturan berbasis laju didefinisikan di dalam grup aturan, dan grup aturan digunakan dalam ACL web.

```
aws wafv2 get-rate-based-statement-managed-keys --scope=REGIONAL --region=region --web-acl-name=WebACLName --web-acl-id=WebACLId --rule-group-rule-name=RuleGroupRuleName --rule-name=RuleName
```

Pernyataan aturan kelompok aturan

Pernyataan aturan kelompok aturan tidak bersarang.

Bagian ini menjelaskan pernyataan aturan grup aturan yang dapat Anda gunakan di ACL web Anda. Grup aturan unit kapasitas ACL web (WCU) ditetapkan oleh pemilik grup aturan pada saat pembuatan. Untuk informasi tentang WCU, lihatAWS WAF unit kapasitas ACL web (WCU).

Pernyataan kelompok aturan	Deskripsi	WCU
Grup aturan terkelola	Menjalankan aturan yang didefinisikan dalam grup aturan terkelola yang ditentukan. Anda dapat mempersempit cakupan permintaan yang dievaluasi oleh grup aturan dengan menambahkan pernyataan cakupan ke bawah. Anda tidak dapat membuat sarang pernyataan grup aturan terkelola di dalam jenis pernyataan lainnya.	Didefinisikan oleh grup aturan, ditambah WCU tambahan untuk pernyataan cakupan ke bawah.
Grup aturan	Menjalankan aturan yang didefinisikan dalam grup aturan yang Anda kelola. Anda tidak dapat menambahkan pernyataan cakupan bawah ke pernyataan referensi grup	Anda menentukan batas WCU untuk grup aturan saat Anda membuatnya.

Pernyataan kelompok aturan	Deskripsi	WCU
	aturan untuk grup aturan Anda sendiri. Anda tidak dapat membuat sarang pernyataan grup aturan di dalam jenis pernyataan lain	

Pernyataan grup aturan terkelola

Pernyataan aturan grup aturan terkelola menambahkan referensi dalam daftar aturan ACL web Anda ke grup aturan terkelola. Anda tidak melihat opsi ini di bawah pernyataan aturan Anda di konsol, tetapi ketika Anda bekerja dengan format JSON ACL web Anda, setiap grup aturan terkelola yang telah Anda tambahkan muncul di bawah aturan ACL web sebagai tipe ini.

Grup aturan terkelola adalah grup aturan Aturan AWS Terkelola, yang sebagian besar gratis untuk AWS WAF pelanggan, atau grup aturan AWS Marketplace terkelola. Anda secara otomatis berlangganan grup aturan Aturan AWS Terkelola berbayar saat Anda menambahkannya ke ACL web Anda. Anda dapat berlangganan grup aturan AWS Marketplace terkelola melalui AWS Marketplace. Untuk informasi selengkapnya, lihat Grup aturan terkelola.

Saat menambahkan grup aturan ke ACL web, Anda dapat mengganti tindakan aturan dalam grup ke Count atau ke tindakan aturan lain. Untuk informasi selengkapnya, lihat Opsi penggantian tindakan untuk grup aturan.

Anda dapat mempersempit cakupan permintaan yang AWS WAF mengevaluasi dengan grup aturan. Untuk melakukan ini, Anda menambahkan pernyataan cakupan ke bawah di dalam pernyataan grup aturan. Untuk informasi tentang pernyataan cakupan bawah, lihat. Pernyataan cakupan ke bawah Ini dapat membantu Anda mengelola bagaimana grup aturan memengaruhi lalu lintas Anda dan dapat membantu Anda memuat biaya yang terkait dengan volume lalu lintas saat Anda menggunakan grup aturan. Untuk informasi dan contoh penggunaan pernyataan scope-down dengan grup aturan terkelola AWS WAF Bot Control, lihat. AWS WAF Kontrol Bot

Tidak bersarang - Anda tidak dapat membuat jenis pernyataan ini di dalam pernyataan lain, dan Anda tidak dapat memasukkannya ke dalam grup aturan. Anda dapat memasukkannya langsung ke ACL web.

(Opsional) Pernyataan cakupan bawah — Jenis aturan ini menggunakan pernyataan cakupan bawah opsional, untuk mempersempit cakupan permintaan yang dievaluasi oleh grup aturan. Untuk informasi selengkapnya, lihat Pernyataan cakupan ke bawah.

WCU - Tetapkan untuk grup aturan saat pembuatan.

Di mana menemukan pernyataan aturan ini

- Konsol — Selama proses membuat ACL web, pada halaman Tambahkan aturan dan grup aturan, pilih Tambahkan grup aturan terkelola, lalu temukan dan pilih grup aturan yang ingin Anda gunakan.
- API — ManagedRuleGroupStatement

Pernyataan kelompok aturan

Pernyataan aturan grup aturan menambahkan referensi ke daftar aturan ACL web Anda ke grup aturan yang Anda kelola. Anda tidak melihat opsi ini di bawah pernyataan aturan Anda di konsol, tetapi ketika Anda bekerja dengan format JSON ACL web Anda, salah satu grup aturan Anda sendiri yang telah Anda tambahkan muncul di bawah aturan ACL web sebagai tipe ini. Untuk informasi tentang menggunakan grup aturan Anda sendiri, lihatMengelola grup aturan Anda sendiri.

Saat menambahkan grup aturan ke ACL web, Anda dapat mengganti tindakan aturan dalam grup ke Count atau ke tindakan aturan lain. Untuk informasi selengkapnya, lihat Opsi penggantian tindakan untuk grup aturan.

Tidak bersarang - Anda tidak dapat membuat jenis pernyataan ini di dalam pernyataan lain, dan Anda tidak dapat memasukkannya ke dalam grup aturan. Anda dapat memasukkannya langsung ke ACL web.

WCU - Tetapkan untuk grup aturan saat pembuatan.

Di mana menemukan pernyataan aturan ini

- Konsol — Selama proses membuat ACL web, pada halaman Tambahkan aturan dan grup aturan, pilih Tambahkan aturan dan grup aturan saya sendiri, grup Aturan, lalu tambahkan grup aturan yang ingin Anda gunakan.
- API — RuleGroupReferenceStatement

Penanganan komponen permintaan kebesaran di AWS WAF

AWS WAF tidak mendukung pemeriksaan konten yang sangat besar untuk badan komponen permintaan web, header, atau cookie. Layanan host yang mendasarinya memiliki batasan jumlah dan ukuran pada apa yang diteruskannya AWS WAF untuk diperiksa. Misalnya, layanan host tidak mengirim lebih dari 200 header ke AWS WAF, jadi untuk permintaan web dengan 205 header, tidak AWS WAF dapat memeriksa 5 header terakhir.

Ketika AWS WAF memungkinkan permintaan web untuk melanjutkan ke sumber daya Anda yang dilindungi, seluruh permintaan web dikirim, termasuk konten apa pun yang berada di luar batas hitungan dan ukuran yang AWS WAF dapat diperiksa.

Batas ukuran inspeksi komponen

Batas ukuran inspeksi komponen adalah sebagai berikut:

- **`Body`**dan **`JSON Body`** — Untuk Application Load Balancer dan AWS AppSync, AWS WAF dapat memeriksa 8 KB pertama dari badan permintaan. Untuk CloudFront, API Gateway, Amazon Cognito, App Runner, dan Akses Terverifikasi, secara default, AWS WAF dapat memeriksa 16 KB pertama, dan Anda dapat meningkatkan batas hingga 64 KB dalam konfigurasi ACL web Anda. Untuk informasi selengkapnya, lihat Mengelola batas ukuran inspeksi tubuh.
- **`Headers`**— AWS WAF dapat memeriksa paling banyak 8 KB pertama (8.192 byte) dari header permintaan dan paling banyak 200 header pertama. Konten tersedia untuk diperiksa AWS WAF hingga batas pertama yang tercapai.
- **`Cookies`**— AWS WAF dapat memeriksa paling banyak 8 KB pertama (8.192 byte) dari cookie permintaan dan paling banyak 200 cookie pertama. Konten tersedia untuk diperiksa AWS WAF hingga batas pertama yang tercapai.

Opsi penanganan ukuran besar untuk pernyataan aturan Anda

Saat Anda menulis pernyataan aturan yang memeriksa salah satu jenis komponen permintaan ini, Anda menentukan cara menangani komponen yang terlalu besar. Penanganan oversize memberi tahu AWS WAF apa yang harus dilakukan dengan permintaan web ketika komponen permintaan yang diperiksa aturan melebihi batas ukuran.

Opsi untuk menangani komponen kebesaran adalah sebagai berikut:

- Continue— Periksa komponen permintaan secara normal sesuai dengan kriteria inspeksi aturan. AWS WAF akan memeriksa isi komponen permintaan yang berada dalam batas ukuran.

- Match— Perlakukan permintaan web sebagai pencocokan pernyataan aturan. AWS WAF menerapkan tindakan aturan untuk permintaan tanpa mengevaluasinya terhadap kriteria inspeksi aturan.
- No match— Perlakukan permintaan web sebagai tidak cocok dengan pernyataan aturan tanpa mengevaluasinya terhadap kriteria inspeksi aturan. AWS WAF melanjutkan inspeksi permintaan web menggunakan sisa aturan di ACL web seperti yang akan dilakukan untuk aturan yang tidak cocok.

Di AWS WAF konsol, Anda harus memilih salah satu opsi penanganan ini. Di luar konsol, opsi default adalahContinue.

Jika Anda menggunakan Match opsi dalam aturan yang mengatur tindakannyaBlock, aturan akan memblokir permintaan yang komponen inspeksinya terlalu besar. Dengan konfigurasi lainnya, disposisi akhir permintaan tergantung pada berbagai faktor, seperti konfigurasi aturan lain di ACL web Anda dan pengaturan tindakan default ACL web.

Penanganan kebesaran dalam grup aturan yang tidak Anda miliki

Batasan ukuran dan jumlah komponen berlaku untuk semua aturan yang Anda gunakan di ACL web Anda. Ini termasuk aturan apa pun yang Anda gunakan tetapi tidak dikelola, di grup aturan terkelola dan dalam grup aturan yang dibagikan dengan Anda oleh akun lain.

Bila Anda menggunakan grup aturan yang tidak Anda kelola, grup aturan mungkin memiliki aturan yang memeriksa komponen permintaan terbatas tetapi tidak menangani konten berukuran besar seperti yang Anda butuhkan untuk ditangani. Untuk informasi tentang cara Aturan AWS Terkelola mengelola komponen yang terlalu besar, lihatAWS Daftar grup aturan Aturan Terkelola. Untuk informasi tentang grup aturan lain, tanyakan kepada penyedia grup aturan Anda.

Pedoman untuk mengelola komponen yang terlalu besar di ACL web Anda

Cara Anda menangani komponen oversize di ACL web Anda dapat bergantung pada sejumlah faktor seperti ukuran yang diharapkan dari konten komponen permintaan Anda, penanganan permintaan default ACL web Anda, dan bagaimana aturan lain di ACL web Anda cocok dan menangani permintaan.

Pedoman umum untuk mengelola komponen permintaan web berukuran besar adalah sebagai berikut:

- Jika Anda perlu mengizinkan beberapa permintaan dengan konten komponen yang terlalu besar, jika memungkinkan, tambahkan aturan untuk secara eksplisit hanya mengizinkan permintaan

tersebut. Prioritaskan aturan tersebut sehingga mereka berjalan sebelum aturan lain di ACL web yang memeriksa jenis komponen yang sama. Dengan pendekatan ini, Anda tidak akan dapat menggunakannya AWS WAF untuk memeriksa seluruh konten komponen kebesaran yang Anda izinkan untuk diteruskan ke sumber daya yang dilindungi.

- Untuk semua permintaan lainnya, Anda dapat mencegah byte tambahan lewat dengan memblokir permintaan yang melampaui batas:
  - Aturan dan grup aturan Anda — Dalam aturan yang memeriksa komponen dengan batas ukuran, konfigurasikan penanganan ukuran besar sehingga Anda memblokir permintaan yang melampaui batas. Misalnya, jika aturan Anda memblokir permintaan dengan konten header tertentu, setel penanganan ukuran besar agar sesuai dengan permintaan yang memiliki konten header yang terlalu besar. Sebagai alternatif, jika ACL web Anda memblokir permintaan secara default dan aturan Anda mengizinkan konten header tertentu, maka konfigurasikan penanganan ukuran besar aturan Anda agar tidak cocok dengan permintaan apa pun yang memiliki konten header yang terlalu besar.
  - Grup aturan yang tidak Anda kelola — Untuk mencegah grup aturan yang tidak Anda kelola mengizinkan komponen permintaan yang terlalu besar, Anda dapat menambahkan aturan terpisah yang memeriksa jenis komponen permintaan dan memblokir permintaan yang melampaui batas. Prioritaskan aturan di ACL web Anda sehingga berjalan sebelum grup aturan. Misalnya, Anda dapat memblokir permintaan dengan konten tubuh yang terlalu besar sebelum aturan inspeksi tubuh Anda dijalankan di ACL web. Prosedur berikut menjelaskan cara menambahkan jenis aturan ini.

Memblokir komponen permintaan web yang terlalu besar

Anda dapat menambahkan aturan di ACL web Anda yang memblokir permintaan dengan komponen yang terlalu besar.

Untuk menambahkan aturan yang memblokir konten berukuran besar

1. Saat Anda membuat atau mengedit ACL web Anda, dalam pengaturan aturan, pilih Tambahkan aturan, Tambahkan aturan dan grup aturan saya sendiri, Pembuat aturan, lalu Editor visual Aturan. Untuk panduan tentang membuat atau mengedit ACL web, lihatBekerja dengan ACL web.
2. Masukkan nama untuk aturan Anda, dan biarkan pengaturan Type pada aturan Regular.
3. Ubah pengaturan kecocokan berikut dari defaultnya:

a. Pada Pernyataan, untuk Inspect, buka dropdown dan pilih komponen permintaan web yang Anda butuhkan, baik Body, Header, atau Cookies.

b. Untuk jenis Match, pilih Ukuran lebih besar dari.

c. Untuk Ukuran, ketikkan angka yang setidaknya ukuran minimum untuk jenis komponen. Untuk header dan cookie, ketik8192. Dalam Application Load Balancer atau ACL AWS AppSync web, untuk badan, ketik. 8192 Untuk badan di CloudFront, API Gateway, Amazon Cognito, App Runner, atau ACL web Akses Terverifikasi, jika Anda menggunakan batas ukuran badan default, ketik. 16384 Jika tidak, ketikkan batas ukuran tubuh yang telah Anda tetapkan untuk ACL web Anda.

d. Untuk penanganan Oversize, pilih Match.

4. Untuk Tindakan, pilih Blokir.
5. Pilih Tambahkan aturan.
6. Setelah Anda menambahkan aturan, pada halaman prioritas aturan Set, pindahkan ke atas aturan atau grup aturan apa pun di ACL web Anda yang memeriksa jenis komponen yang sama. Ini memberi aturan baru pengaturan prioritas numerik yang lebih rendah, yang menyebabkan AWS WAF untuk mengevaluasinya terlebih dahulu. Untuk informasi selengkapnya, lihat Memproses urutan aturan dan kelompok aturan dalam ACL web.

Pencocokan pola ekspresi reguler di AWS WAF

AWS WAF mendukung sintaks pola yang digunakan oleh pustaka PCRE. `libpcre` Pustaka didokumentasikan di PCRE - Perl Compatible Regular Expressions.

AWS WAF tidak mendukung semua konstruksi perpustakaan. Misalnya, mendukung beberapa pernyataan lebar nol, tetapi tidak semua. Kami tidak memiliki daftar lengkap konstruksi yang didukung. Namun, jika Anda memberikan pola regex yang tidak valid atau menggunakan konstruksi yang tidak didukung, AWS WAF API akan melaporkan kegagalan.

AWS WAF tidak mendukung pola PCRE berikut:

- Referensi balik dan menangkap subexpressions
- Referensi subrutin dan pola rekursif
- Pola bersyarat
- Kata kerja kontrol mundur

- Direktif byte tunggal\ C
- Arahan pencocokan baris baru\ R
- Perintah pengaturan ulang pertandingan dimulai\ K
- Callout dan kode tertanam
- Pengelompokan atom dan kuantifier posesif

Set IP dan set pola regex di AWS WAF

AWS WAF menyimpan beberapa informasi yang lebih kompleks dalam set yang Anda gunakan dengan mereferensikannya dalam aturan Anda. Masing-masing set ini memiliki nama dan diberi Nama Sumber Daya Amazon (ARN) saat pembuatan. Anda dapat mengelola set ini dari dalam pernyataan aturan Anda dan Anda dapat mengakses dan mengelolanya sendiri, melalui panel navigasi konsol.

Anda dapat menggunakan set terkelola dalam grup aturan atau ACL web.

- Untuk menggunakan set IP, lihatPernyataan aturan kecocokan set IP.
- Untuk menggunakan set pola regex lihat. Pernyataan aturan kecocokan set pola regex

Ketidakkonsistenan sementara selama pembaruan

Saat Anda membuat atau mengubah ACL web atau AWS WAF sumber daya lainnya, perubahan membutuhkan sedikit waktu untuk menyebar ke semua area tempat sumber daya disimpan. Waktu propagasi bisa dari beberapa detik hingga beberapa menit.

Berikut ini adalah contoh inkonsistensi sementara yang mungkin Anda perhatikan selama propagasi perubahan:

- Setelah Anda membuat ACL web, jika Anda mencoba mengaitkannya dengan sumber daya, Anda mungkin mendapatkan pengecualian yang menunjukkan bahwa ACL web tidak tersedia.
- Setelah Anda menambahkan grup aturan ke ACL web, aturan grup aturan baru mungkin berlaku di satu area di mana ACL web digunakan dan tidak di area lain.
- Setelah mengubah setelan tindakan aturan, Anda mungkin melihat tindakan lama di beberapa tempat dan tindakan baru di tempat lain.
- Setelah Anda menambahkan alamat IP ke set IP yang digunakan dalam aturan pemblokiran, alamat baru mungkin diblokir di satu area sementara masih diizinkan di area lain.

Topik

Membuat dan mengelola set IP

Kumpulan IP menyediakan kumpulan alamat IP dan rentang alamat IP yang ingin Anda gunakan bersama dalam pernyataan aturan. IP set adalah AWS sumber daya.

Untuk menggunakan set IP dalam ACL web atau grup aturan, Anda terlebih dahulu membuat AWS sumber daya, `IPSet` dengan spesifikasi alamat Anda. Kemudian Anda mereferensikan set ketika Anda menambahkan pernyataan aturan set IP ke ACL web atau grup aturan.

Topik

Membuat set IP

Ikuti prosedur di bagian ini untuk membuat set IP baru.

> **Note**
>
> Selain prosedur di bagian ini, Anda memiliki opsi untuk menambahkan set IP baru saat Anda menambahkan aturan pencocokan IP ke ACL web atau grup aturan Anda. Memilih opsi itu mengharuskan Anda untuk memberikan pengaturan yang sama seperti yang diperlukan oleh prosedur ini.

Untuk membuat set IP

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.
2. Di panel navigasi, pilih set IP dan kemudian Buat set IP.
3. Masukkan nama dan deskripsi untuk set IP. Anda akan menggunakan ini untuk mengidentifikasi set ketika Anda ingin menggunakannya.

> **Note**
>
> Anda tidak dapat mengubah nama setelah Anda membuat set IP.

4. Untuk Region, pilih Global (CloudFront) atau pilih Region tempat Anda ingin menyimpan set IP. Anda dapat menggunakan set IP regional hanya di ACL web yang melindungi sumber daya regional. Untuk menggunakan set IP di ACL web yang melindungi CloudFront distribusi Amazon, Anda harus menggunakan Global ()CloudFront.
5. Untuk versi IP, pilih versi yang ingin Anda gunakan.
6. Di kotak teks alamat IP, masukkan satu alamat IP atau rentang alamat IP per baris, dalam notasi CIDR. AWS WAF mendukung semua rentang IPv4 dan IPv6 CIDR kecuali untuk. `/0` Untuk informasi lebih lanjut tentang notasi CIDR, lihat artikel Wikipedia Classless Inter-Domain Routing.

   Berikut ini adalah beberapa contohnya:

   - Untuk menentukan alamat IPv4 192.0.2.44, ketik 192.0.2.44/32.
   - Untuk menentukan alamat IPv6 2620:0:2 d 0:200:0:0:0:0:0, ketik 2620:0:2 d 0:200:0:0:0:0 /128.
   - Untuk menentukan kisaran alamat IPv4 dari 192.0.2.0 hingga 192.0.2.255, ketik 192.0.2.0/24.
   - Untuk menentukan kisaran alamat IPv6 dari 2620:0: 2 d 0:200:0: 0:0 hingga 2620:0:2 d 0:200: ffff:ffff:ffff:ffff, masukkan 2620:0:2 d 0:200: :/64.
7. Tinjau pengaturan untuk set IP, dan pilih Buat set IP.

Menghapus set IP

Ikuti panduan di bagian ini untuk menghapus set yang direferensikan.

Menghapus set yang direferensikan dan grup aturan

Saat Anda menghapus entitas yang dapat Anda gunakan di ACL web, seperti kumpulan IP, kumpulan pola regex, atau grup aturan, AWS WAF periksa untuk melihat apakah entitas saat ini sedang digunakan di ACL web. Jika menemukan bahwa itu sedang digunakan, AWS WAF memperingatkan Anda. AWS WAF hampir selalu dapat menentukan apakah suatu entitas sedang direferensikan oleh ACL web. Namun, dalam kasus yang jarang terjadi mungkin DNS Firewall tidak dapat melakukannya. Jika Anda perlu memastikan bahwa saat ini tidak ada yang menggunakan entitas, periksa di ACL

web Anda sebelum menghapusnya. Jika entitas adalah kumpulan yang direferensikan, periksa juga apakah tidak ada grup aturan yang menggunakannya.

Untuk menghapus set IP

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.
2. Di panel navigasi, pilih set IP.
3. Pilih set IP yang ingin Anda hapus dan pilih Hapus.

Membuat dan mengelola set pola regex

Kumpulan pola regex menyediakan kumpulan ekspresi reguler yang ingin Anda gunakan bersama dalam pernyataan aturan. Set pola Regex adalah AWS sumber daya.

Untuk menggunakan pola regex yang diatur dalam ACL web atau grup aturan, Anda terlebih dahulu membuat AWS sumber daya, `RegexPatternSet` dengan spesifikasi pola regex Anda. Kemudian Anda mereferensikan set saat Anda menambahkan pernyataan aturan set pola regex ke ACL web atau grup aturan. Set pola regex harus berisi setidaknya satu pola regex.

Jika set pola regex Anda berisi lebih dari satu pola regex, ketika digunakan dalam aturan, pencocokan pola digabungkan dengan logika. `OR` Artinya, permintaan web akan cocok dengan pernyataan aturan set pola jika komponen permintaan cocok dengan salah satu pola dalam set.

AWS WAF mendukung sintaks pola yang digunakan oleh pustaka PCRE `libpcre` dengan beberapa pengecualian. Pustaka didokumentasikan di PCRE - Perl Compatible Regular Expressions. Untuk informasi tentang AWS WAF dukungan, lihatPencocokan pola ekspresi reguler di AWS WAF.

Topik

- Membuat set pola regex
- Menghapus set pola regex

Membuat set pola regex

Ikuti prosedur di bagian ini untuk membuat set pola regex baru.

Untuk membuat set pola regex

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.
2. Di panel navigasi, pilih set pola Regex dan kemudian Buat set pola regex.
3. Masukkan nama dan deskripsi untuk set pola regex. Anda akan menggunakan ini untuk mengidentifikasinya ketika Anda ingin menggunakan set.

   > **Note**
   >
   > Anda tidak dapat mengubah nama setelah Anda membuat set pola regex.

4. Untuk Region, pilih Global (CloudFront) atau pilih Region tempat Anda ingin menyimpan set pola regex. Anda dapat menggunakan set pola regex regional hanya di ACL web yang melindungi sumber daya regional. Untuk menggunakan pola regex yang disetel di ACL web yang melindungi CloudFront distribusi Amazon, Anda harus menggunakan Global (). CloudFront
5. Dalam kotak teks Ekspresi reguler, masukkan satu pola regex per baris.

   Misalnya, ekspresi reguler `I[a@]mAB[a@]dRequest` cocok dengan string berikut:`IamABadRequest`,, `IamAB@dRequestI@mABadRequest`, dan`I@mAB@dRequest`.

   AWS WAF mendukung sintaks pola yang digunakan oleh pustaka PCRE `libpcre` dengan beberapa pengecualian. Pustaka didokumentasikan di PCRE - Perl Compatible Regular Expressions. Untuk informasi tentang AWS WAF dukungan, lihatPencocokan pola ekspresi reguler di AWS WAF.
6. Tinjau pengaturan untuk set pola regex, dan pilih Buat set pola regex.

Menghapus set pola regex

Ikuti panduan di bagian ini untuk menghapus set yang direferensikan.

Menghapus set yang direferensikan dan grup aturan

Saat Anda menghapus entitas yang dapat Anda gunakan di ACL web, seperti kumpulan IP, kumpulan pola regex, atau grup aturan, AWS WAF periksa untuk melihat apakah entitas saat ini sedang digunakan di ACL web. Jika menemukan bahwa itu sedang digunakan, AWS WAF memperingatkan Anda. AWS WAF hampir selalu dapat menentukan apakah suatu entitas sedang direferensikan oleh ACL web. Namun, dalam kasus yang jarang terjadi mungkin DNS Firewall tidak dapat melakukannya.

Jika Anda perlu memastikan bahwa saat ini tidak ada yang menggunakan entitas, periksa di ACL web Anda sebelum menghapusnya. Jika entitas adalah kumpulan yang direferensikan, periksa juga apakah tidak ada grup aturan yang menggunakannya.

Untuk menghapus set pola regex

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.
2. Di panel navigasi, pilih set pola Regex.
3. Pilih set pola regex yang ingin Anda hapus dan pilih Hapus.

Permintaan dan tanggapan web yang disesuaikan di AWS WAF

Anda dapat menambahkan permintaan web kustom dan perilaku penanganan respons ke tindakan AWS WAF aturan dan tindakan ACL web default. Pengaturan kustom Anda berlaku setiap kali tindakan yang dilampirkan berlaku.

Anda dapat menyesuaikan permintaan dan tanggapan web dengan cara berikut:

- DenganAllow,Count,CAPTCHA, dan Challenge tindakan, Anda dapat menyisipkan header khusus ke dalam permintaan web. Saat AWS WAF meneruskan permintaan web ke sumber daya yang dilindungi, permintaan berisi seluruh permintaan asli ditambah header khusus yang telah Anda masukkan. Untuk Challenge tindakan CAPTCHA dan tindakan, AWS WAF hanya berlaku kustomisasi jika permintaan melewati CAPTCHA atau inspeksi token tantangan.

- Dengan Block tindakan, Anda dapat menentukan respons kustom lengkap, dengan kode respons, header, dan isi. Sumber daya yang dilindungi merespons permintaan menggunakan respons khusus yang disediakan oleh AWS WAF. Respons kustom Anda menggantikan respons Block tindakan default. `403 (Forbidden)`

Pengaturan tindakan yang dapat Anda sesuaikan

Anda dapat menentukan permintaan atau respons khusus saat menentukan setelan tindakan berikut:

- Tindakan aturan. Untuk informasi, lihat Tindakan aturan.
- Tindakan default untuk ACL web. Untuk informasi, lihat Tindakan default ACL web.

Pengaturan tindakan yang tidak dapat Anda sesuaikan

Anda tidak dapat menentukan penanganan permintaan kustom dalam tindakan penggantian untuk grup aturan yang Anda gunakan di ACL web. Lihat Evaluasi aturan dan kelompok aturan ACL Web. Lihat juga Pernyataan grup aturan terkelola danPernyataan kelompok aturan.

Ketidakkonsistenan sementara selama pembaruan

Saat Anda membuat atau mengubah ACL web atau AWS WAF sumber daya lainnya, perubahan membutuhkan sedikit waktu untuk menyebar ke semua area tempat sumber daya disimpan. Waktu propagasi bisa dari beberapa detik hingga beberapa menit.

Berikut ini adalah contoh inkonsistensi sementara yang mungkin Anda perhatikan selama propagasi perubahan:

- Setelah Anda membuat ACL web, jika Anda mencoba mengaitkannya dengan sumber daya, Anda mungkin mendapatkan pengecualian yang menunjukkan bahwa ACL web tidak tersedia.
- Setelah Anda menambahkan grup aturan ke ACL web, aturan grup aturan baru mungkin berlaku di satu area di mana ACL web digunakan dan tidak di area lain.
- Setelah mengubah setelan tindakan aturan, Anda mungkin melihat tindakan lama di beberapa tempat dan tindakan baru di tempat lain.
- Setelah Anda menambahkan alamat IP ke set IP yang digunakan dalam aturan pemblokiran, alamat baru mungkin diblokir di satu area sementara masih diizinkan di area lain.

Batas penggunaan permintaan dan tanggapan kustom

AWS WAF mendefinisikan pengaturan maksimum untuk penggunaan permintaan dan tanggapan kustom Anda. Misalnya, jumlah maksimum header permintaan per ACL web atau grup aturan, dan jumlah maksimum header khusus untuk satu definisi respons kustom. Untuk informasi, lihat AWS WAF kuota.

Topik

- Penyisipan header permintaan khusus untuk tindakan non-pemblokiran
- Tanggapan khusus untuk Block tindakan
- Kode status yang didukung untuk respon kustom

Penyisipan header permintaan khusus untuk tindakan non-pemblokiran

Anda dapat menginstruksikan AWS WAF untuk menyisipkan header kustom ke dalam permintaan HTTP asli ketika tindakan aturan tidak memblokir permintaan. Dengan opsi ini, Anda hanya menambah permintaan. Anda tidak dapat memodifikasi atau mengganti bagian mana pun dari permintaan asli. Kasus penggunaan untuk penyisipan header khusus termasuk memberi sinyal pada aplikasi hilir untuk memproses permintaan secara berbeda berdasarkan header yang disisipkan, dan menandai permintaan untuk analisis.

Opsi ini berlaku untuk tindakan aturanAllow,, CountCAPTCHA, Challenge dan untuk tindakan default ACL web yang disetel keAllow. Untuk informasi selengkapnya tentang tindakan aturan, lihatTindakan aturan. Untuk informasi selengkapnya tentang tindakan ACL web default, lihatTindakan default ACL web.

Nama header permintaan kustom

AWS WAF awalan semua header permintaan yang disisipkan`x-amzn-waf-`, untuk menghindari kebingungan dengan header yang sudah ada dalam permintaan. Misalnya, jika Anda menentukan nama header`sample`, AWS WAF menyisipkan header`x-amzn-waf-sample`.

Header dengan nama yang sama

Jika permintaan sudah memiliki header dengan nama yang sama dengan yang AWS WAF disisipkan, AWS WAF timpa header. Jadi, jika Anda mendefinisikan header dalam beberapa aturan dengan nama yang identik, aturan terakhir untuk memeriksa permintaan dan menemukan kecocokan akan ditambahkan tajuknya, dan aturan sebelumnya tidak akan.

Header khusus dengan tindakan aturan yang tidak mengakhiri

Berbeda dengan Allow Count tindakan, tindakan tidak berhenti AWS WAF dari memproses permintaan web menggunakan sisa aturan di ACL web. Demikian pula, kapan CAPTCHA dan Challenge menentukan bahwa token permintaan valid, tindakan ini tidak berhenti AWS WAF memproses permintaan web. Jadi, jika Anda menyisipkan header khusus menggunakan aturan dengan salah satu tindakan ini, aturan selanjutnya mungkin juga menyisipkan header khusus. Untuk informasi selengkapnya tentang perilaku tindakan aturan, lihatTindakan aturan.

Misalnya, Anda memiliki aturan berikut, diprioritaskan dalam urutan yang ditunjukkan:

1. RuleA dengan Count tindakan dan header khusus bernama. `RuleAHeader`

2. RuleB dengan Allow tindakan dan header khusus bernama. `RuleBHeader`

Jika permintaan cocok dengan RuleA dan RuleB, AWS WAF masukkan header `x-amzn-waf-RuleAHeader` dan`x-amzn-waf-RuleBHeader`, lalu teruskan permintaan ke sumber daya yang dilindungi.

AWS WAF menyisipkan header khusus ke dalam permintaan web ketika selesai memeriksa permintaan. Jadi, jika Anda menggunakan penanganan permintaan kustom dengan aturan yang mengatur tindakanCount, header kustom yang Anda tambahkan tidak akan diperiksa oleh aturan berikutnya.

Contoh penanganan permintaan kustom

Anda menentukan penanganan permintaan kustom untuk tindakan aturan atau untuk tindakan default ACL web. Daftar berikut menunjukkan JSON untuk penanganan kustom yang ditambahkan ke tindakan default untuk ACL web.

```
{
 "Name": "SampleWebACL",
 "Scope": "REGIONAL",
 "DefaultAction": {
  "Allow": {
   "CustomRequestHandling": {
    "InsertHeaders": [
     {
      "Name": "fruit",
      "Value": "watermelon"
     },
     {
      "Name": "pie",
      "Value": "apple"
     }
    ]
   }
  }
 },
 "Description": "Sample web ACL with custom request handling configured for default
 action.",
 "Rules": [],
 "VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
```

```
  "MetricName": "SampleWebACL"
 }
}
```

Tanggapan khusus untuk Block tindakan

Anda dapat menginstruksikan AWS WAF untuk mengirim respons HTTP kustom kembali ke klien untuk tindakan aturan atau tindakan default ACL web yang disetel ke. Block Untuk informasi selengkapnya tentang tindakan aturan, lihatTindakan aturan. Untuk informasi selengkapnya tentang tindakan ACL web default, lihatTindakan default ACL web.

Saat menentukan penanganan respons khusus untuk suatu Block tindakan, Anda menentukan kode status, header, dan badan respons. Untuk daftar kode status yang dapat Anda gunakan AWS WAF, lihat bagian berikut,Kode status yang didukung untuk respon kustom.

Kasus penggunaan

Kasus penggunaan untuk tanggapan kustom meliputi yang berikut:

- Mengirim kode status non-default kembali ke klien.
- Mengirim header respons khusus kembali ke klien. Anda dapat menentukan nama header apa pun kecuali untuk`content-type`.
- Mengirim halaman kesalahan statis kembali ke klien.
- Mengarahkan klien ke URL yang berbeda. Untuk melakukan ini, Anda menentukan salah satu kode status `3xx` pengalihan, seperti `301 (Moved Permanently)` atau`302 (Found)`, dan kemudian tentukan header baru bernama `Location` dengan URL baru.

Interaksi dengan tanggapan yang Anda tentukan dalam sumber daya yang dilindungi

Respons kustom yang Anda tentukan untuk AWS WAF Block tindakan lebih diutamakan daripada spesifikasi respons apa pun yang Anda tentukan di sumber daya yang dilindungi.

Layanan host untuk AWS sumber daya yang Anda lindungi AWS WAF mungkin mengizinkan penanganan respons khusus untuk permintaan web. Contohnya meliputi hal berikut:

- Dengan Amazon CloudFront, Anda dapat menyesuaikan halaman kesalahan berdasarkan kode status. Untuk selengkapnya, lihat Menghasilkan respons kesalahan kustom di Panduan CloudFront Pengembang Amazon.

- Dengan Amazon API Gateway Anda dapat menentukan respons dan kode status untuk gateway Anda. Untuk selengkapnya, lihat Respons Gateway di API Gateway di Panduan Pengembang Amazon API Gateway.

Anda tidak dapat menggabungkan setelan respons AWS WAF kustom dengan setelan respons khusus di AWS sumber daya yang dilindungi. Spesifikasi respons untuk setiap permintaan web individu datang baik sepenuhnya dari AWS WAF atau sepenuhnya dari sumber daya yang dilindungi.

Untuk permintaan web yang AWS WAF memblokir, berikut ini menunjukkan urutan prioritas.

1. AWS WAF respons kustom - Jika AWS WAF Block tindakan mengaktifkan respons kustom, sumber daya yang dilindungi akan mengirimkan respons kustom yang dikonfigurasi kembali ke klien. Pengaturan respons apa pun yang mungkin telah Anda tetapkan di sumber daya yang dilindungi itu sendiri tidak berpengaruh.
2. Respons khusus yang ditentukan dalam sumber daya yang dilindungi — Jika tidak, jika sumber daya yang dilindungi memiliki pengaturan respons khusus yang ditentukan, sumber daya yang dilindungi menggunakan pengaturan tersebut untuk merespons klien.
3. AWS WAF Blockrespons default - Jika tidak, sumber daya yang dilindungi merespons klien dengan Block respons AWS WAF `403 (Forbidden)` default.

Untuk permintaan web yang AWS WAF memungkinkan, konfigurasi sumber daya yang dilindungi menentukan respons yang dikirim kembali ke klien. Anda tidak dapat mengonfigurasi setelan respons AWS WAF untuk permintaan yang diizinkan. Satu-satunya penyesuaian yang dapat Anda konfigurasikan AWS WAF untuk permintaan yang diizinkan adalah penyisipan header khusus ke dalam permintaan asli, sebelum meneruskan permintaan ke sumber daya yang dilindungi. Opsi ini dijelaskan di bagian sebelumnya,. Penyisipan header permintaan khusus untuk tindakan non-pemblokiran

Header respon kustom

Anda dapat menentukan nama header apa pun kecuali untuk`content-type`.

Badan respons khusus

Anda menentukan isi respons kustom dalam konteks ACL web atau grup aturan tempat Anda ingin menggunakannya. Setelah menentukan badan respons kustom, Anda dapat menggunakannya dengan referensi di tempat lain di ACL web atau grup aturan tempat Anda membuatnya. Dalam

pengaturan Block tindakan individual, Anda mereferensikan badan kustom yang ingin Anda gunakan dan Anda menentukan kode status dan header respons kustom.

Saat membuat respons khusus di konsol, Anda dapat memilih dari badan respons yang telah ditentukan atau Anda dapat membuat badan baru. Di luar konsol, Anda menentukan badan respons kustom di ACL web atau tingkat grup aturan, lalu mereferensikannya dari setelan tindakan dalam ACL web atau grup aturan. Hal ini ditunjukkan dalam contoh JSON di bagian berikut.

Contoh respon kustom

Contoh berikut mencantumkan JSON untuk grup aturan dengan pengaturan respons kustom. Badan respons kustom didefinisikan untuk seluruh grup aturan, kemudian direferensikan dengan kunci dalam tindakan aturan.

```
{
 "ARN": "test_rulegroup_arn",
 "Capacity": 1,

 "CustomResponseBodies": {
  "CustomResponseBodyKey1": {
   "Content": "This is a plain text response body.",
   "ContentType": "TEXT_PLAIN"
  }
 },

 "Description": "This is a test rule group.",
 "Id": "test_rulegroup_id",
 "Name": "TestRuleGroup",

 "Rules": [
  {
   "Action": {
    "Block": {
     "CustomResponse": {
      "CustomResponseBodyKey": "CustomResponseBodyKey1",
      "ResponseCode": 404,
      "ResponseHeaders": [
       {
        "Name": "BlockActionHeader1Name",
        "Value": "BlockActionHeader1Value"
       }
      ]
     }
```

```
    }
   },
   "Name": "GeoMatchRule",
   "Priority": 1,
   "Statement": {
    "GeoMatchStatement": {
     "CountryCodes": [
      "US"
     ]
    }
   },
   "VisibilityConfig": {
    "CloudWatchMetricsEnabled": true,
    "MetricName": "TestRuleGroupReferenceMetric",
    "SampledRequestsEnabled": true
   }
  }
 ],
 "VisibilityConfig": {
  "CloudWatchMetricsEnabled": true,
  "MetricName": "TestRuleGroupMetric",
  "SampledRequestsEnabled": true
 }
}
```

Kode status yang didukung untuk respon kustom

Untuk informasi rinci tentang kode status HTTP, lihat Kode Status oleh Internet Engineering Task Force (IETF) dan Daftar kode status HTTP di Wikipedia.

Berikut ini adalah kode status HTTP yang AWS WAF mendukung respons khusus.

- 2xx Successful
  - 200 – OK
  - 201 – Created
  - 202 – Accepted
  - 204 – No Content
  - 206 – Partial Content
- 3xx Redirection
  - 300 – Multiple Choices

  - 301 – Moved Permanently
  - 302 – Found
  - 303 –See Other
  - 304 – Not Modified
  - 307 – Temporary Redirect
  - 308 – Permanent Redirect
- 4xx Client Error
  - 400 – Bad Request
  - 401 – Unauthorized
  - 403 – Forbidden
  - 404 – Not Found
  - 405 – Method Not Allowed
  - 408 – Request Timeout
  - 409 – Conflict
  - 411 – Length Required
  - 412 – Precondition Failed
  - 413 – Request Entity Too Large
  - 414 – Request-URI Too Long
  - 415 – Unsupported Media Type
  - 416 – Requested Range Not Satisfiable
  - 421 – Misdirected Request
  - 429 – Too Many Requests
- 5xx Server Error
  - 500 – Internal Server Error
  - 501 – Not Implemented
  - 502 – Bad Gateway
  - 503 – Service Unavailable
  - 504 – Gateway Timeout
  - 505 – HTTP Version Not Supported

AWS WAF label pada permintaan web

Label adalah metadata yang ditambahkan ke permintaan web dengan aturan saat aturan cocok dengan permintaan. Setelah ditambahkan, label tetap tersedia berdasarkan permintaan sampai evaluasi ACL web berakhir. Anda dapat mengakses label dalam aturan yang berjalan nanti di evaluasi ACL web dengan menggunakan pernyataan pencocokan label. Lihat perinciannya di Pernyataan aturan pencocokan label.

Label pada permintaan web menghasilkan metrik CloudWatch label Amazon. Untuk daftar metrik dan dimensi, lihatLabel metrik dan dimensi. Untuk informasi tentang mengakses metrik dan ringkasan metrik melalui CloudWatch dan melalui konsol, lihat. AWS WAF Pemantauan dan penyetelan

Pelabelan kasus penggunaan

Kasus penggunaan umum untuk AWS WAF label meliputi yang berikut:

- Mengevaluasi permintaan web terhadap beberapa pernyataan aturan sebelum mengambil tindakan atas permintaan — Setelah kecocokan ditemukan dengan aturan di ACL web, AWS WAF terus evaluasi permintaan terhadap ACL web jika tindakan aturan tidak menghentikan evaluasi ACL web. Anda dapat menggunakan label untuk mengevaluasi dan mengumpulkan informasi dari beberapa aturan sebelum Anda memutuskan untuk mengizinkan atau memblokir permintaan. Untuk melakukannya, ubah tindakan untuk aturan yang ada Count dan konfigurasikan untuk menambahkan label ke permintaan yang cocok. Kemudian, tambahkan satu atau beberapa aturan baru untuk dijalankan setelah aturan Anda yang lain, dan konfigurasikan untuk mengevaluasi label dan mengelola permintaan sesuai dengan kombinasi pencocokan label.
- Mengelola permintaan web berdasarkan wilayah geografis — Anda dapat menggunakan aturan pencocokan geografis saja untuk mengelola permintaan web berdasarkan negara asal. Untuk menyempurnakan lokasi ke tingkat wilayah, Anda menggunakan aturan geo match dengan Count tindakan yang diikuti dengan aturan pencocokan label. Untuk informasi tentang aturan geo match, lihatPernyataan aturan kecocokan geografis.
- Menggunakan kembali logika di beberapa aturan — Jika Anda perlu menggunakan kembali logika yang sama di beberapa aturan, Anda dapat menggunakan label untuk sumber tunggal logika dan hanya menguji hasilnya. Bila Anda memiliki beberapa aturan kompleks yang menggunakan subset umum dari pernyataan aturan bersarang, menduplikasi aturan umum yang ditetapkan di seluruh aturan kompleks Anda dapat memakan waktu dan rawan kesalahan. Dengan label, Anda dapat membuat aturan baru dengan subset aturan umum yang menghitung permintaan yang cocok dan menambahkan label ke dalamnya. Anda menambahkan aturan baru ke ACL web Anda sehingga

berjalan sebelum aturan kompleks asli Anda. Kemudian, dalam aturan asli Anda, Anda mengganti subset aturan bersama dengan satu aturan yang memeriksa label.

Misalnya, Anda memiliki beberapa aturan yang hanya ingin Anda terapkan pada jalur masuk Anda. Daripada meminta setiap aturan menentukan logika yang sama untuk mencocokkan jalur login potensial, Anda dapat menerapkan satu aturan baru yang berisi logika itu. Minta aturan baru menambahkan label ke permintaan yang cocok untuk menunjukkan bahwa permintaan berada di jalur login. Di ACL web Anda, berikan aturan baru ini pengaturan prioritas numerik yang lebih rendah daripada aturan asli Anda sehingga berjalan terlebih dahulu. Kemudian, dalam aturan asli Anda, ganti logika bersama dengan cek keberadaan label. Untuk informasi tentang setelan prioritas, lihatMemproses urutan aturan dan kelompok aturan dalam ACL web.

- Membuat pengecualian pada aturan dalam grup aturan — Opsi ini sangat berguna untuk grup aturan terkelola, yang tidak dapat Anda lihat atau ubah. Banyak aturan grup aturan terkelola menambahkan label ke permintaan web yang cocok, untuk menunjukkan aturan yang cocok dan mungkin untuk memberikan informasi tambahan tentang kecocokan. Bila Anda menggunakan grup aturan yang menambahkan label ke permintaan, Anda dapat mengganti aturan grup aturan untuk menghitung kecocokan, lalu menjalankan aturan setelah grup aturan yang menangani permintaan web berdasarkan label grup aturan. Semua Aturan AWS Terkelola menambahkan label ke permintaan web yang cocok. Untuk detailnya, lihat deskripsi aturan diAWS Daftar grup aturan Aturan Terkelola.
- Menggunakan metrik label untuk memantau pola lalu lintas — Anda dapat mengakses metrik untuk label yang Anda tambahkan melalui aturan dan untuk metrik yang ditambahkan oleh grup aturan terkelola yang Anda gunakan di ACL web Anda. Semua grup aturan Aturan AWS Terkelola menambahkan label ke permintaan web yang mereka evaluasi. Untuk daftar metrik dan dimensi label, lihatLabel metrik dan dimensi. Anda dapat mengakses metrik dan ringkasan metrik melalui CloudWatch dan melalui halaman ACL web di konsol. AWS WAF Untuk informasi, lihat Pemantauan dan penyetelan.

Cara AWS WAF kerja pelabelan

Jika aturan cocok dengan permintaan web, jika aturan memiliki label yang ditentukan, AWS WAF tambahkan label ke permintaan di akhir evaluasi aturan. Aturan yang dievaluasi setelah aturan pencocokan di ACL web dapat cocok dengan label yang ditambahkan aturan.

Siapa yang menambahkan label ke permintaan

Komponen ACL web yang mengevaluasi permintaan dapat menambahkan label ke permintaan.

- Aturan apa pun yang bukan pernyataan referensi grup aturan dapat menambahkan label ke permintaan web yang cocok. Kriteria pelabelan adalah bagian dari definisi aturan, dan ketika permintaan web cocok dengan aturan, AWS WAF menambahkan label aturan ke permintaan. Untuk informasi, lihat the section called “Aturan yang menambahkan label”.
- Pernyataan aturan geo match menambahkan label negara dan wilayah ke permintaan apa pun yang diperiksa, terlepas dari apakah pernyataan tersebut menghasilkan kecocokan. Untuk informasi, lihat the section called “Pertandingan geografis”.
- Aturan AWS Terkelola untuk AWS WAF semua menambahkan label ke permintaan yang mereka periksa. Mereka menambahkan beberapa label berdasarkan kecocokan aturan di grup aturan dan mereka menambahkan beberapa berdasarkan AWS proses yang digunakan grup aturan terkelola, seperti pelabelan token yang ditambahkan saat Anda menggunakan grup aturan mitigasi ancaman cerdas. Untuk informasi tentang label yang ditambahkan oleh setiap grup aturan terkelola, lihatthe section called “AWS Daftar grup aturan Aturan Terkelola”.

Bagaimana AWS WAF mengelola label

AWS WAF menambahkan label aturan ke permintaan di akhir pemeriksaan aturan atas permintaan. Pelabelan adalah bagian dari aktivitas pencocokan aturan, mirip dengan tindakan.

Label tidak bertahan dengan permintaan web setelah evaluasi ACL web berakhir. Agar aturan lain cocok dengan label yang ditambahkan aturan Anda, tindakan aturan Anda tidak boleh menghentikan evaluasi permintaan web oleh ACL web. Tindakan aturan harus diatur keCount,CAPTCHA, atauChallenge. Ketika evaluasi ACL web tidak berakhir, aturan berikutnya di ACL web dapat menjalankan kriteria pencocokan label mereka terhadap permintaan. Untuk informasi selengkapnya tentang tindakan aturan, lihatTindakan aturan.

Akses ke label selama evaluasi ACL web

Setelah ditambahkan, label tetap tersedia pada permintaan selama AWS WAF mengevaluasi permintaan terhadap ACL web. Aturan apa pun di ACL web dapat mengakses label yang telah ditambahkan oleh aturan yang telah berjalan di ACL web yang sama. Ini termasuk aturan yang didefinisikan langsung di dalam ACL web dan aturan yang didefinisikan di dalam grup aturan yang digunakan dalam ACL web.

- Anda dapat mencocokkan label dalam kriteria pemeriksaan permintaan aturan Anda menggunakan pernyataan pencocokan label. Anda dapat mencocokkan dengan label apa pun yang dilampirkan pada permintaan. Untuk detail pernyataan, lihatPernyataan aturan pencocokan label.

- Pernyataan pencocokan geografis menambahkan label dengan atau tanpa kecocokan, tetapi hanya tersedia setelah pernyataan yang berisi aturan ACL web telah menyelesaikan evaluasi permintaan.
  - Anda tidak dapat menggunakan aturan tunggal, misalnya pernyataan logis, untuk menjalankan AND pernyataan geo match diikuti dengan pernyataan pencocokan label terhadap label geografis. Anda harus meletakkan pernyataan pencocokan label dalam aturan terpisah yang berjalan setelah aturan yang berisi pernyataan geo match.
  - Jika Anda menggunakan pernyataan geo match sebagai pernyataan scope-down di dalam pernyataan aturan berbasis tarif atau pernyataan referensi grup aturan terkelola, label yang ditambahkan oleh pernyataan geo match tidak tersedia untuk diperiksa oleh pernyataan aturan yang berisi. Jika Anda perlu memeriksa pelabelan geografis dalam pernyataan aturan berbasis tarif atau grup aturan, Anda harus menjalankan pernyataan geo match dalam aturan terpisah yang berjalan sebelumnya.

Akses ke informasi label di luar evaluasi ACL web

Label tidak bertahan dengan permintaan web setelah evaluasi ACL web berakhir, tetapi AWS WAF mencatat informasi label di log dan metrik.

- AWS WAF menyimpan CloudWatch metrik Amazon untuk 100 label pertama pada setiap permintaan tunggal. Untuk informasi tentang mengakses metrik label, lihat Pemantauan CloudWatch dengan Amazon dan. Label metrik dan dimensi
- AWS WAF merangkum metrik CloudWatch label di dasbor ikhtisar lalu lintas ACL web di konsol. AWS WAF Anda dapat mengakses dasbor di halaman ACL web apa pun. Untuk informasi selengkapnya, lihat Dasbor ikhtisar lalu lintas ACL web.
- AWS WAF merekam label di log untuk 100 label pertama berdasarkan permintaan. Anda dapat menggunakan label, bersama dengan tindakan aturan, untuk memfilter log yang AWS WAF merekam. Untuk informasi, lihat Pencatatan AWS WAF lalu lintas ACL web.

Evaluasi ACL web Anda dapat menerapkan lebih dari 100 label ke permintaan web dan cocok dengan lebih dari 100 label, tetapi AWS WAF hanya mencatat 100 label pertama dalam log dan metrik.

AWS WAF sintaks label dan persyaratan penamaan

Label adalah string yang terdiri dari awalan, ruang nama opsional, dan nama. Komponen label dibatasi dengan titik dua. Label memiliki persyaratan dan karakteristik sebagai berikut:

- Label peka huruf besar/kecil.
- Setiap namespace label atau nama label dapat memiliki hingga 128 karakter.
- Anda dapat menentukan hingga lima ruang nama dalam label.
- Komponen label dipisahkan oleh titik dua (`:`).
- Anda tidak dapat menggunakan string cadangan berikut di ruang nama atau nama yang Anda tentukan untuk label:`awswaf`,,,,`aws`,`waf`, `rulegroup` `webaclregexpatternset`, `ipset` dan. `managed`

Sintaks label

Label yang sepenuhnya memenuhi syarat memiliki awalan, ruang nama opsional, dan nama label. Prefiks mengidentifikasi grup aturan atau konteks ACL web aturan yang menambahkan label. Ruang nama dapat digunakan untuk menambahkan lebih banyak konteks untuk label. Nama label memberikan tingkat detail terendah untuk label. Ini sering menunjukkan aturan spesifik yang menambahkan label ke permintaan.

Awalan label bervariasi tergantung pada asalnya.

- Label Anda — Berikut ini menunjukkan sintaks label lengkap untuk label yang Anda buat di ACL web dan aturan grup aturan. Jenis entitas adalah `rulegroup` dan`webacl`.

  ```
  awswaf:<entity owner account id>:<entity type>:<entity name>:<custom
   namespace>:...:<label name>
  ```

  - Awalan namespace label: `awswaf:<entity owner account id>:<entity type>:<entity name>:`
  - Penambahan namespace khusus: `<custom namespace>:…:`

  Saat Anda menentukan label untuk aturan dalam grup aturan atau ACL web, Anda mengontrol string namespace kustom dan nama label. Sisanya dihasilkan untuk Anda oleh AWS WAF. AWS WAF secara otomatis awalan semua label dengan `awswaf` dan akun dan web ACL atau pengaturan entitas grup aturan.

- Label grup aturan terkelola - Berikut ini menunjukkan sintaks label lengkap untuk label yang dibuat oleh aturan dalam grup aturan terkelola.

```
awswaf:managed:<vendor>:<rule group name>:<custom namespace>:...:<label name>
```

  - Awalan namespace label: `awswaf:managed:<vendor>:<rule group name>:`
  - Penambahan namespace khusus: `<custom namespace>:…:`

  Semua grup aturan Aturan AWS Terkelola menambahkan label. Untuk informasi tentang grup aturan terkelola, lihatGrup aturan terkelola.

- Label dari AWS proses lain — Proses ini digunakan oleh grup aturan Aturan AWS Terkelola, sehingga Anda melihatnya ditambahkan ke permintaan web yang Anda evaluasi menggunakan grup aturan terkelola. Berikut ini menunjukkan sintaks label lengkap untuk label yang dibuat oleh proses yang dipanggil oleh kelompok aturan terkelola.

```
awswaf:managed:<process>:<custom namespace>:...:<label name>
```

  - Awalan namespace label: `awswaf:managed:<process>:`
  - Penambahan namespace khusus: `<custom namespace>:…:`

  Label jenis ini dicantumkan untuk grup aturan terkelola yang memanggil AWS proses. Untuk informasi tentang grup aturan terkelola, lihatGrup aturan terkelola.

Contoh label untuk aturan Anda

Contoh label berikut ditentukan oleh aturan dalam grup aturan bernama `testRules` milik akun, 111122223333.

```
awswaf:111122223333:rulegroup:testRules:testNS1:testNS2:LabelNameA
```

```
awswaf:111122223333:rulegroup:testRules:testNS1:LabelNameQ
```

```
awswaf:111122223333:rulegroup:testRules:LabelNameZ
```

Daftar berikut menunjukkan contoh spesifikasi label di JSON. Nama label ini menyertakan string namespace khusus sebelum nama label akhir.

```
Rule: {
    Name: "label_rule",
    Statement: {...}
    RuleLabels: [
        Name: "header:encoding:utf8",
        Name: "header:user_agent:firefox"
    ],
    Action: { Count: {} }
}
```

> **Note**
>
> Anda dapat mengakses jenis daftar ini di konsol melalui editor aturan JSON.

Jika Anda menjalankan aturan sebelumnya dalam grup aturan dan akun yang sama dengan contoh label sebelumnya, label yang dihasilkan dan memenuhi syarat adalah sebagai berikut:

```
awswaf:111122223333:rulegroup:testRules:header:encoding:utf8
```

```
awswaf:111122223333:rulegroup:testRules:header:user_agent:firefox
```

Contoh label untuk grup aturan terkelola

Berikut ini menunjukkan contoh label dari grup aturan Aturan AWS Terkelola dan proses yang mereka panggil.

```
awswaf:managed:aws:core-rule-set:NoUserAgent_Header
```

```
awswaf:managed:aws:sql-database:SQLiExtendedPatterns_QueryArguments
```

```
awswaf:managed:aws:atp:aggregate:attribute:compromised_credentials
```

```
awswaf:managed:token:accepted
```

AWS WAF aturan yang menambahkan label

Di hampir semua aturan, Anda dapat menentukan label dan AWS WAF akan menerapkannya pada permintaan yang cocok.

Jenis aturan berikut adalah satu-satunya pengecualian:

- Aturan berbasis tarif hanya memberi label saat pembatasan laju — Aturan berbasis tarif hanya menambahkan label ke permintaan web untuk instance agregasi tertentu sementara instance itu dibatasi oleh tarif. AWS WAF Untuk informasi tentang aturan berbasis tarif, lihat. Pernyataan aturan berbasis tarif
- Pelabelan tidak diperbolehkan dalam pernyataan referensi grup aturan — Konsol tidak menerima label untuk jenis aturan ini. Melalui API, menentukan label untuk salah satu jenis pernyataan menghasilkan pengecualian validasi. Untuk informasi tentang jenis pernyataan ini, lihat Pernyataan grup aturan terkelola danPernyataan kelompok aturan.

WCU — 1 WCU untuk setiap 5 label yang Anda tentukan di ACL web atau aturan grup aturan Anda.

Di mana menemukan ini

- Pembuat aturan di konsol — Di bawah pengaturan Tindakan aturan, di bawah Label.
- Jenis data API - `Rule` `RuleLabels`

Anda menentukan label dalam aturan dengan menentukan string namespace kustom dan nama untuk ditambahkan ke awalan namespace label. AWS WAF mendapatkan awalan dari konteks di mana Anda mendefinisikan aturan. Untuk informasi tentang ini, lihat informasi sintaks label di bawahAWS WAF sintaks label dan persyaratan penamaan.

AWS WAF aturan yang cocok dengan label

Anda dapat menggunakan pernyataan pencocokan label untuk mengevaluasi label permintaan web. Anda dapat mencocokkan dengan Label, yang memerlukan nama label, atau terhadap Namespace, yang memerlukan spesifikasi namespace. Untuk label atau namespace, Anda dapat secara opsional menyertakan ruang nama sebelumnya dan awalan dalam spesifikasi Anda. Untuk informasi umum tentang jenis pernyataan ini, lihatPernyataan aturan pencocokan label.

Awalan label mendefinisikan konteks grup aturan atau ACL web tempat aturan label didefinisikan. Dalam pernyataan pencocokan label aturan, jika string pencocokan label atau namespace Anda tidak menentukan awalan, AWS WAF gunakan awalan untuk aturan pencocokan label.

- Label untuk aturan yang didefinisikan langsung di dalam ACL web memiliki awalan yang menentukan konteks ACL web.
- Label untuk aturan yang berada di dalam grup aturan memiliki awalan yang menentukan konteks grup aturan. Ini bisa berupa grup aturan Anda sendiri atau grup aturan yang dikelola untuk Anda.

Untuk informasi tentang ini, lihat sintaks label di bawahAWS WAF sintaks label dan persyaratan penamaan.

> **Note**
>
> Beberapa grup aturan terkelola menambahkan label. Anda dapat mengambilnya melalui API dengan meneleponDescribeManagedRuleGroup. Label tercantum di AvailableLabels properti dalam tanggapan.

Jika Anda ingin mencocokkan aturan yang berada dalam konteks yang berbeda dari konteks aturan Anda, Anda harus memberikan awalan dalam string pencocokan Anda. Misalnya, jika Anda ingin mencocokkan label yang ditambahkan oleh aturan dalam grup aturan terkelola, Anda dapat menambahkan aturan di ACL web Anda dengan pernyataan pencocokan label yang string kecocokannya menentukan awalan grup aturan diikuti dengan kriteria kecocokan tambahan Anda.

Dalam string pencocokan untuk pernyataan pencocokan label, Anda menentukan label atau namespace:

- Label — Spesifikasi label untuk kecocokan terdiri dari bagian akhir label. Anda dapat menyertakan sejumlah ruang nama yang berdekatan yang segera mendahului nama label diikuti dengan nama. Anda juga dapat memberikan label yang sepenuhnya memenuhi syarat dengan memulai spesifikasi dengan awalan.

  Contoh spesifikasi:

  - `testNS1:testNS2:LabelNameA`
  - `awswaf:managed:aws:managed-rule-set:testNS1:testNS2:LabelNameA`

- Namespace — Spesifikasi namespace untuk kecocokan terdiri dari subset bersebelahan dari spesifikasi label tidak termasuk nama. Anda dapat menyertakan awalan dan Anda dapat menyertakan satu atau lebih string namespace.

  Contoh spesifikasi:

  - `testNS1:testNS2:`
  - `awswaf:managed:aws:managed-rule-set:testNS1:`

AWS WAF contoh kecocokan label

Bagian ini memberikan contoh spesifikasi kecocokan, untuk pernyataan aturan pencocokan label.

> **Note**
>
> Daftar JSON ini dibuat di konsol dengan menambahkan aturan ke ACL web dengan spesifikasi pencocokan label dan kemudian mengedit aturan dan beralih ke editor Rule JSON. Anda juga bisa mendapatkan JSON untuk grup aturan atau web ACL melalui API atau antarmuka baris perintah.

Topik

Cocokkan dengan label lokal

Daftar JSON berikut menunjukkan pernyataan pencocokan label untuk label yang telah ditambahkan ke permintaan web secara lokal, dalam konteks yang sama dengan aturan ini.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
```

```
            Scope: "LABEL",
            Key: "header:encoding:utf8"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

Jika Anda menggunakan pernyataan pencocokan ini di akun 111122223333, dalam aturan yang Anda tentukan untuk ACL web`testWebACL`, itu akan cocok dengan label berikut.

```
awswaf:111122223333:webacl:testWebACL:header:encoding:utf8
```

```
awswaf:111122223333:webacl:testWebACL:testNS1:testNS2:header:encoding:utf8
```

Itu tidak akan cocok dengan label berikut, karena string label tidak sama persis.

```
awswaf:111122223333:webacl:testWebACL:header:encoding2:utf8
```

Itu tidak akan cocok dengan label berikut, karena konteksnya tidak sama, jadi awalan tidak cocok. Ini benar bahkan jika Anda menambahkan grup aturan `productionRules` ke ACL web`testWebACL`, di mana aturan didefinisikan.

```
awswaf:111122223333:rulegroup:productionRules:header:encoding:utf8
```

Cocokkan dengan label dari konteks lain

Daftar JSON berikut menunjukkan aturan pencocokan label yang cocok dengan label dari aturan di dalam grup aturan yang dibuat pengguna. Awalan diperlukan dalam spesifikasi untuk semua aturan yang berjalan di ACL web yang bukan bagian dari grup aturan bernama. Spesifikasi label contoh ini hanya cocok dengan label yang tepat.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "LABEL",
```

```
            Key: "awswaf:111122223333:rulegroup:testRules:header:encoding:utf8"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

Cocokkan dengan label grup aturan terkelola

Ini adalah kasus khusus pencocokan dengan label yang berasal dari konteks lain selain aturan kecocokan. Daftar JSON berikut menunjukkan pernyataan pencocokan label untuk label grup aturan terkelola. Ini hanya cocok dengan label persis yang ditentukan dalam pengaturan kunci pernyataan pencocokan label.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "LABEL",
            Key: "awswaf:managed:aws:managed-rule-set:header:encoding:utf8"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

Cocokkan dengan namespace lokal

Daftar JSON berikut menunjukkan pernyataan pencocokan label untuk namespace lokal.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "NAMESPACE",
            Key: "header:encoding:"
        }
    },
```

```
    Labels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

Mirip dengan `Label` kecocokan lokal, jika Anda menggunakan pernyataan ini di akun 111122223333, dalam aturan yang Anda tentukan untuk web ACL`testWebACL`, itu akan cocok dengan label berikut.

```
awswaf:111122223333:webacl:testWebACL:header:encoding:utf8
```

Itu tidak akan cocok dengan label berikut, karena akunnya tidak sama, jadi awalan tidak cocok.

```
awswaf:444455556666:webacl:testWebACL:header:encoding:utf8
```

Awalan juga tidak cocok dengan label apa pun yang diterapkan oleh grup aturan terkelola, seperti berikut ini.

```
awswaf:managed:aws:managed-rule-set:header:encoding:utf8
```

Cocokkan dengan namespace grup aturan terkelola

Daftar JSON berikut menunjukkan pernyataan pencocokan label untuk namespace grup aturan terkelola. Untuk grup aturan yang Anda miliki, Anda juga perlu memberikan awalan agar cocok dengan namespace yang berada di luar konteks aturan.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "NAMESPACE",
            Key: "awswaf:managed:aws:managed-rule-set:header:"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
```

```
}
```

Spesifikasi ini cocok dengan label contoh berikut.

```
awswaf:managed:aws:managed-rule-set:header:encoding:utf8
```

```
awswaf:managed:aws:managed-rule-set:header:encoding:unicode
```

Itu tidak cocok dengan label berikut.

```
awswaf:managed:aws:managed-rule-set:query:badstring
```

AWS WAF mitigasi ancaman cerdas

Bagian ini mencakup fitur mitigasi ancaman cerdas terkelola yang disediakan oleh. AWS WAF Ini adalah perlindungan canggih dan khusus yang dapat Anda terapkan untuk melindungi dari ancaman seperti bot berbahaya dan upaya pengambilalihan akun.

> **Note**
>
> Fitur yang dijelaskan di sini menimbulkan biaya tambahan, di luar biaya dasar untuk menggunakan AWS WAF. Untuk informasi selengkapnya, silakan lihat Harga AWS WAF.

Panduan yang disediakan di bagian ini ditujukan untuk pengguna yang tahu secara umum cara membuat dan mengelola ACL AWS WAF web, aturan, dan grup aturan. Topik-topik tersebut dibahas di bagian sebelumnya dari panduan ini.

Topik

- Opsi untuk mitigasi ancaman cerdas
- Praktik terbaik untuk mitigasi ancaman cerdas
- AWS WAF token permintaan web
- AWS WAF Pencegahan penipuan pembuatan akun Kontrol Penipuan (ACFP)
- AWS WAF Pencegahan pengambilalihan akun Kontrol Penipuan (ATP)
- AWS WAF Kontrol Bot

- AWS WAF integrasi aplikasi klien
- CAPTCHAdan Challenge di AWS WAF

Opsi untuk mitigasi ancaman cerdas

Bagian ini memberikan perbandingan rinci tentang opsi untuk menerapkan mitigasi ancaman cerdas.

AWS WAF menawarkan jenis perlindungan berikut untuk mitigasi ancaman cerdas.

- AWS WAF Pencegahan penipuan pembuatan akun Kontrol Penipuan (ACFP) — Mendeteksi dan mengelola upaya pembuatan akun berbahaya di halaman pendaftaran aplikasi Anda. Fungsionalitas inti disediakan oleh grup aturan terkelola ACFP. Lihat informasi yang lebih lengkap di AWS WAF Pencegahan penipuan pembuatan akun Kontrol Penipuan (ACFP) dan AWS WAF Grup aturan pencegahan penipuan (ACFP) pembuatan akun Kontrol Penipuan.
- AWS WAF Pencegahan pengambilalihan akun Kontrol Penipuan (ATP) - Mendeteksi dan mengelola upaya pengambilalihan berbahaya pada halaman login aplikasi Anda. Fungsionalitas inti disediakan oleh grup aturan terkelola ATP. Lihat informasi yang lebih lengkap di AWS WAF Pencegahan pengambilalihan akun Kontrol Penipuan (ATP) dan AWS WAF Kelompok aturan pencegahan pengambilalihan akun Kontrol Penipuan (ATP).
- AWS WAF Kontrol Bot — Mengidentifikasi, memberi label, dan mengelola bot ramah dan berbahaya. Fitur ini menyediakan manajemen untuk bot umum dengan tanda tangan yang unik di seluruh aplikasi, dan juga untuk bot bertarget yang memiliki tanda tangan khusus untuk aplikasi. Fungsionalitas inti disediakan oleh grup aturan terkelola Bot Control. Lihat informasi yang lebih lengkap di AWS WAF Kontrol Bot dan AWS WAF Grup aturan Bot Control.
- SDK integrasi aplikasi klien — Validasi sesi klien dan pengguna akhir di halaman web Anda dan dapatkan AWS WAF token untuk digunakan klien dalam permintaan web mereka. Jika Anda menggunakan ACFP, ATP, atau Bot Control, terapkan SDK integrasi aplikasi dalam aplikasi klien Anda jika Anda bisa, untuk memanfaatkan sepenuhnya semua fitur grup aturan. Kami hanya merekomendasikan penggunaan grup aturan ini tanpa integrasi SDK sebagai tindakan sementara, ketika sumber daya penting perlu diamankan dengan cepat dan tidak ada cukup waktu untuk integrasi SDK. Untuk informasi tentang penerapan SDK, lihatAWS WAF integrasi aplikasi klien.
- Challengedan tindakan CAPTCHA aturan — Validasi sesi klien dan pengguna akhir dan dapatkan AWS WAF token untuk digunakan klien dalam permintaan web mereka. Anda dapat menerapkannya di mana saja yang Anda tentukan tindakan aturan, dalam aturan Anda, dan sebagai penggantian dalam grup aturan yang Anda gunakan. Tindakan ini menggunakan AWS WAF JavaScript pengantara untuk menginterogasi klien atau pengguna akhir, dan mereka

memerlukan aplikasi klien yang mendukung. JavaScript Untuk informasi selengkapnya, lihat CAPTCHAdan Challenge di AWS WAF.

Aturan Aturan AWS Terkelola mitigasi ancaman cerdas mengelompokkan ACFP, ATP, dan Kontrol Bot menggunakan token untuk deteksi lanjutan. Untuk informasi tentang fitur yang diaktifkan token dalam grup aturan, lihatMengapa Anda harus menggunakan SDK integrasi aplikasi dengan ACFP,Mengapa Anda harus menggunakan SDK integrasi aplikasi dengan ATP, danMengapa Anda harus menggunakan SDK integrasi aplikasi dengan Bot Control.

Opsi Anda untuk menerapkan mitigasi ancaman cerdas dijalankan dari penggunaan dasar tindakan aturan untuk menjalankan tantangan dan menegakkan akuisisi token, hingga fitur-fitur canggih yang ditawarkan oleh kelompok aturan Aturan Terkelola mitigasi AWS ancaman cerdas.

Tabel berikut memberikan perbandingan rinci dari opsi untuk fitur dasar dan lanjutan.

Topik

- Opsi untuk tantangan dan akuisisi token
- Opsi untuk kelompok aturan terkelola mitigasi ancaman cerdas
- Opsi untuk membatasi tarif dalam aturan berbasis tarif dan aturan Kontrol Bot yang ditargetkan

Opsi untuk tantangan dan akuisisi token

Anda dapat memberikan tantangan dan memperoleh token menggunakan SDK integrasi AWS WAF aplikasi atau tindakan aturan Challenge danCAPTCHA. Secara garis besar, tindakan aturan lebih mudah diterapkan, tetapi mereka menimbulkan biaya tambahan, mengganggu lebih banyak pengalaman pelanggan Anda, dan membutuhkan. JavaScript SDK memerlukan pemrograman dalam aplikasi klien Anda, tetapi mereka dapat memberikan pengalaman pelanggan yang lebih baik, mereka bebas untuk digunakan, dan mereka dapat digunakan dengan JavaScript atau di aplikasi Android atau iOS. Anda hanya dapat menggunakan SDK integrasi aplikasi dengan ACL web yang menggunakan salah satu grup aturan terkelola mitigasi ancaman cerdas berbayar, yang dijelaskan di bagian berikut.

Perbandingan opsi untuk tantangan dan akuisisi token

	Challenge tindakan aturan	CAPTCHAti ndakan aturan	JavaScript Tantangan SDK	Tantangan SDK Seluler
Apa itu	Tindakan aturan yang memberlak ukan akuisisi AWS WAF token dengan menghadir kan interstit ial tantangan senyap kepada klien browser	Tindakan aturan yang memberlak ukan akuisisi AWS WAF token dengan menghadir kan interstit ial tantangan visual atau audio kepada pengguna akhir klien	Lapisan integrasi aplikasi, untuk browser klien dan perangkat lain yang mengeksek usiJavaSc ript. Merender tantangan diam dan memperoleh token	Lapisan integrasi aplikasi, untuk aplikasi Android dan iOS. Secara native membuat tantangan diam dan memperoleh token
Pilihan bagus untuk...	Validasi senyap terhadap sesi bot dan penegakan akuisisi token untuk klien yang mendukung JavaScript	Pengguna akhir dan validasi diam terhadap sesi bot dan penegakan akuisisi token, untuk klien yang mendukung JavaScript	Validasi senyap terhadap sesi bot dan penegakan akuisisi token untuk klien yang mendukung JavaScript. SDK memberika n latensi terendah dan kontrol terbaik atas tempat skrip tantangan berjalan dalam aplikasi.	Validasi senyap terhadap sesi bot dan penegakan akuisisi token untuk aplikasi seluler asli di Android dan iOS. SDK memberika n latensi terendah dan kontrol terbaik atas tempat skrip tantangan berjalan dalam aplikasi.
Pertimbangan implementasi	Diimpleme ntasikan sebagai	Diimpleme ntasikan sebagai	Memerlukan salah satu grup aturan berbayar	Memerlukan salah satu grup aturan berbayar

	Challenge tindakan aturan	CAPTCHAti ndakan aturan	JavaScript Tantangan SDK	Tantangan SDK Seluler
	pengaturan tindakan aturan	pengaturan tindakan aturan	ACFP, ATP, atau Bot Control di ACL web. Membutuhkan pengkodean dalam aplikasi klien.	ACFP, ATP, atau Bot Control di ACL web. Membutuhkan pengkodean dalam aplikasi klien.
Pertimbangan runtime	Alur intrusif untuk permintaan tanpa token yang valid. Klien dialihkan ke interstitial AWS WAF tantangan. Menambahkan perjalanan pulang pergi jaringan dan memerlukan evaluasi kedua dari permintaan web.	Alur intrusif untuk permintaan tanpa token yang valid. Klien dialihkan ke interstitial AWS WAF CAPTCHA. Menambahkan perjalanan pulang pergi jaringan dan memerlukan evaluasi kedua dari permintaan web.	Bisa dijalankan di belakang layar. Memberi Anda lebih banyak kendali atas pengalaman tantangan.	Bisa dijalankan di belakang layar. Memberi Anda lebih banyak kendali atas pengalaman tantangan.
Membutuhkan JavaScript	Ya	Ya	Ya	Tidak
Klien yang didukung	Browser dan perangkat yang menjalankan Javascript	Browser dan perangkat yang menjalankan Javascript	Browser dan perangkat yang menjalankan Javascript	Perangkat Android dan iOS

	Challenge tindakan aturan	CAPTCHAti ndakan aturan	JavaScript Tantangan SDK	Tantangan SDK Seluler
Mendukung aplikasi satu halaman (SPA)	Hanya penegakan. Anda dapat menggunak an Challenge tindakan bersama dengan SDK, untuk memastikan bahwa permintaa n memiliki token tantangan yang valid. Anda tidak dapat menggunak an tindakan aturan untuk mengirimkan skrip tantangan ke halaman.	Hanya penegakan. Anda dapat menggunak an CAPTCHA tindakan bersama dengan SDK, untuk memastikan bahwa permintaa n memiliki token CAPTCHA yang valid. Anda tidak dapat menggunak an tindakan aturan untuk mengirimkan skrip CAPTCHA ke halaman.	Ya	N/A

	Challenge tindakan aturan	CAPTCHAti ndakan aturan	JavaScript Tantangan SDK	Tantangan SDK Seluler
Biaya tambahan	Ya, untuk setelan tindakan yang Anda tentukan secara eksplisit , baik dalam aturan yang Anda tetapkan atau sebagai penggantian tindakan aturan dalam grup aturan yang Anda gunakan. Tidak dalam semua kasus lainnya.	Ya, untuk setelan tindakan yang Anda tentukan secara eksplisit , baik dalam aturan yang Anda tetapkan atau sebagai penggantian tindakan aturan dalam grup aturan yang Anda gunakan. Tidak dalam semua kasus lainnya.	Tidak, tetapi membutuhkan salah satu grup aturan berbayar ACFP, ATP, atau Bot Control.	Tidak, tetapi membutuhkan salah satu grup aturan berbayar ACFP, ATP, atau Bot Control.

Untuk detail tentang biaya yang terkait dengan opsi ini, lihat informasi mitigasi ancaman cerdas di AWS WAF Harga.

Akan lebih mudah untuk menjalankan tantangan dan memberikan penegakan token dasar hanya dengan menambahkan aturan dengan CAPTCHA tindakan Challenge atau. Anda mungkin diminta untuk menggunakan tindakan aturan, misalnya jika Anda tidak memiliki akses ke kode aplikasi.

Namun, jika Anda dapat menerapkan SDK, Anda dapat menghemat biaya dan mengurangi latensi dalam evaluasi ACL web permintaan web klien, dibandingkan dengan menggunakan tindakan: Challenge

- Anda dapat menulis implementasi SDK Anda untuk menjalankan tantangan kapan saja dalam aplikasi Anda. Anda dapat memperoleh token di latar belakang, sebelum tindakan pelanggan apa pun yang akan mengirim permintaan web ke sumber daya Anda yang dilindungi. Dengan cara ini, token tersedia untuk dikirim dengan permintaan pertama klien Anda.

- Jika sebaliknya Anda memperoleh token dengan menerapkan aturan dengan Challenge tindakan, aturan dan tindakan memerlukan evaluasi dan pemrosesan permintaan web tambahan saat klien pertama kali mengirim permintaan dan kapan saja token kedaluwarsa. ChallengeTindakan memblokir permintaan yang tidak memiliki token yang valid dan belum kedaluwarsa, dan mengirimkan pengantara tantangan kembali ke klien. Setelah klien berhasil menanggapi tantangan, pengantara mengirim ulang permintaan web asli dengan token yang valid, yang kemudian dievaluasi untuk kedua kalinya oleh ACL web.

Opsi untuk kelompok aturan terkelola mitigasi ancaman cerdas

Kelompok aturan Aturan AWS Terkelola mitigasi ancaman cerdas menyediakan pengelolaan bot dasar, deteksi dan mitigasi bot yang canggih dan berbahaya, deteksi dan mitigasi upaya pengambilalihan akun, serta deteksi dan mitigasi upaya pembuatan akun yang curang. Grup aturan ini, dikombinasikan dengan SDKS integrasi aplikasi yang dijelaskan di bagian sebelumnya, memberikan perlindungan paling canggih dan kopling aman dengan aplikasi klien Anda.

Perbandingan opsi grup aturan terkelola

	ACFP	ATP	Bot Control tingkat umum	Tingkat target Bot Control
Apa itu	Mengelola permintaan yang mungkin merupakan bagian dari upaya pembuatan akun palsu pada halaman pendaftaran dan pendaftaran aplikasi. Tidak mengelola bot.	Mengelola permintaan yang mungkin merupakan bagian dari upaya pengambilalihan berbahaya pada halaman login aplikasi. Tidak mengelola bot. Lihat AWS WAF Kelompok aturan pencegahan pengambilalihan	Mengelola bot umum yang mengidentifikasi diri, dengan tanda tangan yang unik di seluruh aplikasi. Lihat AWS WAF Grup aturan Bot Control.	Mengelola bot bertarget yang tidak mengidentifikasi diri, dengan tanda tangan yang khusus untuk aplikasi. Lihat AWS WAF Grup aturan Bot Control.

	ACFP	ATP	Bot Control tingkat umum	Tingkat target Bot Control
	Lihat AWS WAF Grup aturan pencegahan penipuan (ACFP) pembuatan akun Kontrol Penipuan.	akun Kontrol Penipuan (ATP).		
Pilihan bagus untuk...	Pemeriksaan lalu lintas pembuatan akun untuk pembuatan akun penipuan menyerang upaya pembuatan tersebut dengan traversal nama pengguna dan banyak akun baru yang dibuat dari satu alamat IP.	Inspeksi lalu lintas login untuk pengambilalihan akun menyerang upaya login tersebut dengan traversal kata sandi dan banyak upaya login dari alamat IP yang sama. Ketika digunakan dengan token, juga menyediakan perlindungan agregat seperti pembatasan tingkat IP dan sesi klien untuk volume tinggi upaya login yang gagal.	Perlindungan bot dasar dan pelabelan lalu lintas bot otomatis yang umum.	Perlindungan yang ditargetkan terhadap bot canggih, termasuk pembatasan kecepatan pada tingkat sesi klien dan deteksi dan mitigasi alat otomatisasi browser seperti Selenium dan Dalang.

	ACFP	ATP	Bot Control tingkat umum	Tingkat target Bot Control
Menambahkan label yang menunjukkan hasil evaluasi	Ya	Ya	Ya	Ya
Menambahkan label token	Ya	Ya	Ya	Ya
Memblokir permintaan yang tidak memiliki token yang valid	Tidak termasuk. Lihat Memblokir permintaan yang tidak memiliki AWS WAF token yang valid.	Tidak termasuk. Lihat Memblokir permintaan yang tidak memiliki AWS WAF token yang valid.	Tidak termasuk. Lihat Memblokir permintaan yang tidak memiliki AWS WAF token yang valid.	Memblokir sesi klien yang mengirim 5 permintaan tanpa token.
Membutuhkan AWS WAF token `aws-waf-token`	Diperlukan untuk semua aturan. Lihat Mengapa Anda harus menggunakan SDK integrasi aplikasi dengan ACFP.	Diperlukan untuk banyak aturan. Lihat Mengapa Anda harus menggunakan SDK integrasi aplikasi dengan ATP.	Tidak	Ya
Mengakuisisi token AWS WAF `aws-waf-token`	Ya, ditegakkan oleh aturan `AllRequests`	Tidak	Tidak	Beberapa aturan menggunakan Challenge atau CAPTCHA mengatur tindakan, yang memperoleh token.

Untuk detail tentang biaya yang terkait dengan opsi ini, lihat informasi mitigasi ancaman cerdas di AWS WAF Harga.

Opsi untuk membatasi tarif dalam aturan berbasis tarif dan aturan Kontrol Bot yang ditargetkan

Level yang ditargetkan dari grup aturan Kontrol AWS WAF Bot dan pernyataan aturan AWS WAF berbasis tarif keduanya memberikan pembatasan tingkat permintaan web. Tabel berikut membandingkan dua opsi.

Perbandingan opsi untuk deteksi dan mitigasi berbasis tarif

	AWS WAF aturan berbasis tarif	AWS WAF Aturan yang ditargetkan Bot Control	
Bagaimana pembatasan tarif diterapkan	Bertindak atas kelompok permintaan yang datang pada tingkat yang terlalu tinggi. Anda dapat menerapkan tindakan apa pun kecuali untukAllow.	Menegakkan pola akses seperti manusia dan menerapkan pembatasan laju dinamis, melalui penggunaan token permintaan.	
Berdasarkan garis dasar lalu lintas historis?	Tidak	Ya	
Waktu yang dibutuhkan untuk mengumpulkan garis dasar lalu lintas bersejarah	N/A	Lima menit untuk ambang dinamis. N/A untuk token tidak ada.	
Kelambatan mitigasi	Biasanya 30-50 detik. Bisa sampai beberapa menit.	Biasanya kurang dari 10 detik. Bisa sampai beberapa menit.	

	AWS WAF aturan berbasis tarif	AWS WAF Aturan yang ditargetkan Bot Control	
Target mitigasi	Dapat dikonfigu rasi. Anda dapat mengelomp okkan permintaa n menggunakan pernyataan cakupan bawah dan dengan satu atau lebih kunci agregasi, seperti alamat IP, metode HTTP, dan string kueri.	Alamat IP dan sesi klien	
Tingkat volume lalu lintas diperlukan untuk memicu mitigasi	Sedang - bisa serendah 100 permintaan di jendela waktu yang ditentukan	Rendah - dimaksudk an untuk mendeteks i pola klien seperti pencakar lambat	
Ambang batas yang dapat disesuaikan	Ya	Tidak	

	AWS WAF aturan berbasis tarif	AWS WAF Aturan yang ditargetkan Bot Control	
Tindakan mitigasi default	Konsol default adalahBlock. Tidak ada pengatura n default di API; pengaturan diperluka n. Anda dapat mengatur ini ke tindakan aturan apa pun kecualiAllow.	Pengaturan tindakan aturan grup aturan adalah Challenge untuk token absen dan CAPTCHA untuk lalu lintas volume tinggi dari satu sesi klien. Anda dapat mengatur salah satu dari aturan ini ke tindakan aturan yang valid.	
Ketahanan terhadap serangan yang sangat terdistribusi	Medium - maksimum 10.000 alamat IP untuk alamat IP yang membatasi sendiri	Sedang - dibatasi hingga 50.000 total antara alamat IP dan token	
AWS WAF Penetapan Harga	Termasuk dalam biaya standar untuk AWS WAF.	Termasuk dalam biaya untuk tingkat yang ditargetkan dari mitigasi ancaman cerdas Kontrol Bot.	
Untuk informasi lebih lanjut	Pernyataan aturan berbasis tarif	AWS WAF Grup aturan Bot Control	

Praktik terbaik untuk mitigasi ancaman cerdas

Ikuti praktik terbaik di bagian ini untuk implementasi fitur mitigasi ancaman cerdas yang paling efisien dan hemat biaya.

- Implementasikan SDK integrasi aplikasi seluler — Terapkan integrasi aplikasi untuk mengaktifkan set lengkap fungsionalitas ACFP, ATP, atau Bot Control dengan cara yang seefektif mungkin. JavaScript Grup aturan terkelola menggunakan token yang disediakan oleh SDK untuk memisahkan lalu lintas klien yang sah dari lalu lintas yang tidak diinginkan di tingkat sesi. SDK integrasi aplikasi memastikan bahwa token ini selalu tersedia. Untuk detailnya, lihat berikut ini:
  - Mengapa Anda harus menggunakan SDK integrasi aplikasi dengan ACFP
  - Mengapa Anda harus menggunakan SDK integrasi aplikasi dengan ATP
  - Mengapa Anda harus menggunakan SDK integrasi aplikasi dengan Bot Control

  Gunakan integrasi untuk mengimplementasikan tantangan di klien Anda dan, untuk JavaScript, untuk menyesuaikan bagaimana teka-teki CAPTCHA disajikan kepada pengguna akhir Anda. Untuk detailnya, lihat AWS WAF integrasi aplikasi klien.

  Jika Anda menyesuaikan teka-teki CAPTCHA menggunakan JavaScript API dan Anda menggunakan tindakan CAPTCHA aturan di mana saja di ACL web Anda, ikuti panduan untuk menangani respons AWS WAF CAPTCHA di klien Anda di. Menangani respons CAPTCHA dari AWS WAF Panduan ini berlaku untuk aturan apa pun yang menggunakan CAPTCHA tindakan, termasuk yang ada di grup aturan terkelola ACFP dan tingkat perlindungan yang ditargetkan dari grup aturan terkelola Kontrol Bot.
- Batasi permintaan yang Anda kirim ke grup aturan ACFP, ATP, dan Kontrol Bot — Anda dikenakan biaya tambahan untuk menggunakan grup aturan Aturan Terkelola mitigasi AWS ancaman cerdas. Grup aturan ACFP memeriksa permintaan ke titik akhir pendaftaran dan pembuatan akun yang Anda tentukan. Grup aturan ATP memeriksa permintaan ke titik akhir login yang Anda tentukan. Grup aturan Bot Control memeriksa setiap permintaan yang mencapainya dalam evaluasi ACL web.

  Pertimbangkan pendekatan berikut untuk mengurangi penggunaan kelompok aturan ini:
  - Kecualikan permintaan dari inspeksi dengan pernyataan cakupan bawah dalam pernyataan grup aturan terkelola. Anda dapat melakukan ini dengan pernyataan nestable apa pun. Untuk informasi, lihat Pernyataan cakupan ke bawah.
  - Kecualikan permintaan dari inspeksi dengan menambahkan aturan sebelum grup aturan. Untuk aturan yang tidak dapat digunakan dalam pernyataan scope-down dan untuk situasi yang lebih kompleks, seperti pelabelan diikuti dengan pencocokan label, Anda mungkin ingin menambahkan aturan yang berjalan sebelum grup aturan. Untuk informasi selengkapnya, lihat Pernyataan cakupan ke bawah dan Dasar-dasar pernyataan aturan.

  - Jalankan kelompok aturan setelah aturan yang lebih murah. Jika Anda memiliki AWS WAF aturan standar lain yang memblokir permintaan karena alasan apa pun, jalankan sebelum grup aturan berbayar ini. Untuk informasi selengkapnya tentang aturan dan manajemen aturan, lihatDasar-dasar pernyataan aturan.
  - Jika Anda menggunakan lebih dari satu grup aturan terkelola mitigasi ancaman cerdas, jalankan dengan urutan berikut untuk menekan biaya: Kontrol Bot, ATP, ACFP.

  Untuk informasi harga terperinci, lihat AWS WAF Harga.

- Aktifkan tingkat perlindungan yang ditargetkan dari grup aturan Kontrol Bot selama lalu lintas web normal — Beberapa aturan tingkat perlindungan yang ditargetkan memerlukan waktu untuk menetapkan garis dasar untuk pola lalu lintas normal sebelum mereka dapat mengenali dan merespons pola lalu lintas yang tidak teratur atau berbahaya. Misalnya, `TGT_ML_*` aturan membutuhkan waktu hingga 24 jam untuk pemanasan.

  Tambahkan perlindungan ini ketika Anda tidak mengalami serangan dan beri mereka waktu untuk menetapkan garis dasar mereka sebelum mengharapkan mereka merespons serangan dengan tepat. Jika Anda menambahkan aturan ini selama serangan, setelah serangan mereda, waktu untuk menetapkan garis dasar biasanya dari dua kali lipat menjadi tiga kali lipat waktu normal yang diperlukan, karena kemiringan yang ditambahkan oleh lalu lintas serangan. Untuk informasi tambahan tentang aturan dan waktu pemanasan yang mereka butuhkan, lihatDaftar aturan.
- Untuk perlindungan penolakan layanan terdistribusi (DDoS), gunakan mitigasi DDoS lapisan aplikasi otomatis Shield Advanced - Grup aturan mitigasi ancaman cerdas tidak memberikan perlindungan DDoS. ACFP melindungi terhadap upaya pembuatan akun palsu ke halaman pendaftaran aplikasi Anda. ATP melindungi terhadap upaya pengambilalihan akun ke halaman login Anda. Bot Control berfokus pada penegakan pola akses seperti manusia menggunakan token dan pembatasan laju dinamis pada sesi klien.

  Saat Anda menggunakan Shield Advanced dengan mitigasi DDoS lapisan aplikasi otomatis diaktifkan, Shield Advanced secara otomatis merespons serangan DDoS yang terdeteksi dengan membuat, mengevaluasi, dan menerapkan mitigasi khusus atas nama Anda. AWS WAF Untuk informasi selengkapnya tentang Shield Advanced, lihatAWS Shield Advanced ikhtisar, danAWS Shield Advanced perlindungan lapisan aplikasi (lapisan 7).
- Sesuaikan dan konfigurasikan penanganan token — Sesuaikan penanganan token ACL web untuk pengalaman pengguna terbaik.
  - Untuk mengurangi biaya pengoperasian dan meningkatkan pengalaman pengguna akhir Anda, sesuaikan waktu kekebalan manajemen token Anda ke waktu terlama yang diizinkan oleh

persyaratan keamanan Anda. Ini membuat penggunaan teka-teki CAPTCHA dan tantangan diam seminimal mungkin. Untuk informasi, lihat Kedaluwarsa stempel waktu: waktu kekebalan token AWS WAF.

  - Untuk mengaktifkan berbagi token antar aplikasi yang dilindungi, konfigurasikan daftar domain token untuk ACL web Anda. Untuk informasi, lihat AWS WAF domain token dan daftar domain.

- Tolak permintaan dengan spesifikasi host arbitrer — Konfigurasikan sumber daya yang dilindungi agar `Host` header dalam permintaan web cocok dengan sumber daya yang ditargetkan. Anda dapat menerima satu nilai atau satu set nilai tertentu, misalnya `myExampleHost.com` dan`www.myExampleHost.com`, tetapi tidak menerima nilai arbitrer untuk host.
- Untuk Application Load Balancer yang berasal dari CloudFront distribusi, konfigurasikan CloudFront dan AWS WAF untuk penanganan token yang tepat — Jika Anda mengaitkan ACL web Anda ke Application Load Balancer dan Anda menerapkan Application Load Balancer sebagai asal distribusi, lihat. CloudFront Konfigurasi yang diperlukan untuk Application Load Balancer yang berasal CloudFront
- Uji dan sesuaikan sebelum menerapkan — Sebelum Anda menerapkan perubahan apa pun pada ACL web Anda, ikuti prosedur pengujian dan penyetelan dalam panduan ini untuk memastikan bahwa Anda mendapatkan perilaku yang Anda harapkan. Ini sangat penting untuk fitur-fitur berbayar ini. Untuk panduan umum, lihatMenguji dan menyetel perlindungan Anda AWS WAF. Untuk informasi khusus tentang grup aturan terkelola berbayar, lihatMenguji dan menerapkan ACFP,Menguji dan menerapkan ATP, danMenguji dan menerapkan Kontrol AWS WAF Bot.

AWS WAF token permintaan web

AWS WAF token adalah bagian integral dari perlindungan yang ditingkatkan yang ditawarkan oleh mitigasi ancaman AWS WAF cerdas. Token, kadang-kadang disebut sidik jari, adalah kumpulan informasi tentang sesi klien tunggal yang disimpan klien dan menyediakan setiap permintaan web yang dikirimkannya. AWS WAF menggunakan token untuk mengidentifikasi dan memisahkan sesi klien jahat dari sesi yang sah, bahkan ketika keduanya berasal dari satu alamat IP. Penggunaan token membebankan biaya yang dapat diabaikan untuk pengguna yang sah, tetapi mahal dalam skala untuk botnet.

AWS WAF menggunakan token untuk mendukung fungsionalitas tantangan browser dan pengguna akhir, yang disediakan oleh SDK integrasi aplikasi dan oleh tindakan aturan Challenge danCAPTCHA. Selain itu, token mengaktifkan fitur Kontrol AWS WAF Bot dan grup aturan terkelola pencegahan pengambilalihan akun.

AWS WAF membuat, memperbarui, dan mengenkripsi token untuk klien yang berhasil menanggapi tantangan diam dan teka-teki CAPTCHA. Ketika klien dengan token mengirim permintaan web, itu termasuk token terenkripsi, dan AWS WAF mendekripsi token dan memverifikasi isinya.

Topik

Bagaimana AWS WAF menggunakan token

AWS WAF menggunakan token untuk merekam dan memverifikasi jenis validasi sesi klien berikut:

- CAPTCHA — Teka-teki CAPTCHA membantu membedakan bot dari pengguna manusia. CAPTCHA dijalankan hanya oleh tindakan CAPTCHA aturan. Setelah berhasil menyelesaikan teka-teki, skrip CAPTCHA memperbarui stempel waktu CAPTCHA token. Untuk informasi selengkapnya, lihat CAPTCHAdan Challenge di AWS WAF.
- Tantangan — Tantangan berjalan diam-diam untuk membantu membedakan sesi klien reguler dari sesi bot dan membuatnya lebih mahal bagi bot untuk beroperasi. Ketika tantangan berhasil diselesaikan, skrip tantangan secara otomatis mendapatkan token baru dari AWS WAF jika diperlukan, dan kemudian memperbarui stempel waktu tantangan token.

  AWS WAF menjalankan tantangan dalam situasi berikut:

  - SDK integrasi aplikasi — SDK integrasi aplikasi berjalan di dalam sesi aplikasi klien Anda dan membantu memastikan bahwa upaya login hanya diizinkan setelah klien berhasil merespons tantangan. Untuk informasi selengkapnya, lihat AWS WAF integrasi aplikasi klien.
  - Challengetindakan aturan — Untuk informasi lebih lanjut, lihatCAPTCHAdan Challenge di AWS WAF.
  - CAPTCHA— Ketika pengantara CAPTCHA berjalan, jika klien belum memiliki token, skrip secara otomatis menjalankan tantangan terlebih dahulu, untuk memverifikasi sesi klien dan untuk menginisialisasi token.

Token diwajibkan oleh banyak aturan dalam kelompok aturan Aturan AWS Terkelola ancaman cerdas. Aturan menggunakan token untuk melakukan hal-hal seperti membedakan antara klien di tingkat sesi, untuk menentukan karakteristik browser, dan untuk memahami tingkat interaktivitas manusia pada halaman web aplikasi. Grup aturan ini memanggil manajemen AWS WAF token, yang menerapkan pelabelan token yang kemudian diperiksa oleh grup aturan.

- AWS WAF Pencegahan penipuan pembuatan akun Kontrol Penipuan (ACFP) — Aturan ACFP mengharuskan permintaan web dengan token yang valid. Untuk informasi lebih lanjut tentang aturan, lihatAWS WAF Grup aturan pencegahan penipuan (ACFP) pembuatan akun Kontrol Penipuan.
- AWS WAF Pencegahan pengambilalihan akun Kontrol Penipuan (ATP) — Aturan ATP yang mencegah volume tinggi dan sesi klien yang tahan lama memerlukan permintaan web yang memiliki token yang valid dengan stempel waktu tantangan yang belum kedaluwarsa. Untuk informasi selengkapnya, lihat AWS WAF Kelompok aturan pencegahan pengambilalihan akun Kontrol Penipuan (ATP).
- AWS WAF Kontrol Bot — Aturan yang ditargetkan dalam grup aturan ini membatasi jumlah permintaan web yang dapat dikirim klien tanpa token yang valid, dan mereka menggunakan pelacakan sesi token untuk pemantauan dan manajemen tingkat sesi. Jika diperlukan, aturan menerapkan tindakan Challenge dan CAPTCHA aturan untuk menegakkan akuisisi token dan perilaku klien yang valid. Untuk informasi selengkapnya, lihat AWS WAF Grup aturan Bot Control.

AWS WAF karakteristik token

Setiap token memiliki karakteristik sebagai berikut:

- Token disimpan dalam cookie bernama`aws-waf-token`.
- Token dienkripsi.
- Token sidik jari sesi klien dengan pengenal granular lengket yang berisi informasi berikut:
  - Stempel waktu respons sukses terbaru klien terhadap tantangan diam.
  - Stempel waktu respons sukses terbaru pengguna akhir terhadap CAPTCHA. Ini hanya ada jika Anda menggunakan CAPTCHA dalam perlindungan Anda.
  - Informasi tambahan tentang perilaku klien dan klien yang dapat membantu memisahkan klien sah Anda dari lalu lintas yang tidak diinginkan. Informasi tersebut mencakup berbagai pengenal klien dan sinyal sisi klien yang dapat digunakan untuk mendeteksi aktivitas otomatis. Informasi yang dikumpulkan tidak unik dan tidak dapat dipetakan ke individu manusia.

- Semua token menyertakan data dari interogasi browser klien, seperti indikasi otomatisasi dan inkonsistensi pengaturan browser. Informasi ini diambil oleh skrip yang dijalankan oleh Challenge tindakan dan oleh SDK aplikasi klien. Skrip secara aktif menginterogasi browser dan memasukkan hasilnya ke dalam token.
- Selain itu, saat Anda menerapkan SDK integrasi aplikasi klien, token menyertakan informasi yang dikumpulkan secara pasif tentang interaktivitas pengguna akhir dengan halaman aplikasi. Interaktivitas mencakup gerakan mouse, penekanan tombol, dan interaksi dengan bentuk HTML apa pun yang ada di halaman. Informasi ini membantu AWS WAF mendeteksi tingkat interaktivitas manusia dalam klien, untuk menantang pengguna yang tampaknya bukan manusia. Untuk informasi tentang integrasi sisi klien, lihatAWS WAF integrasi aplikasi klien.

Untuk alasan keamanan, AWS tidak memberikan deskripsi lengkap tentang isi AWS WAF token atau informasi rinci tentang proses enkripsi token.

Kedaluwarsa stempel waktu: waktu kekebalan token AWS WAF

AWS WAF menggunakan tantangan dan waktu kekebalan CAPTCHA untuk mengontrol seberapa sering sesi klien tunggal dapat disajikan dengan tantangan atau CAPTCHA. Setelah pengguna akhir berhasil merespons CAPTCHA, waktu kekebalan CAPTCHA menentukan berapa lama pengguna akhir tetap kebal dari disajikan dengan CAPTCHA lain. Demikian pula, waktu kekebalan tantangan menentukan berapa lama sesi klien tetap kebal dari tantangan lagi setelah berhasil menanggapi tantangan.

AWS WAF mencatat respons yang berhasil terhadap tantangan atau CAPTCHA dengan memperbarui stempel waktu yang sesuai di dalam token. Saat AWS WAF memeriksa token untuk tantangan atau CAPTCHA, itu mengurangi stempel waktu dari waktu saat ini. Jika hasilnya lebih besar dari waktu kekebalan yang dikonfigurasi, stempel waktu kedaluwarsa.

Anda dapat mengonfigurasi tantangan dan waktu kekebalan CAPTCHA di ACL web dan juga dalam aturan apa pun yang menggunakan tindakan aturan CAPTCHA atauChallenge.

- Pengaturan ACL web default untuk kedua waktu kekebalan adalah 300 detik.
- Anda dapat menentukan waktu kekebalan untuk aturan apa pun yang menggunakan CAPTCHA atau Challenge tindakan. Jika Anda tidak menentukan waktu kekebalan untuk aturan, itu mewarisi pengaturan dari ACL web.

- Untuk aturan di dalam grup aturan yang menggunakan Challenge tindakan CAPTCHA atau, jika Anda tidak menentukan waktu kekebalan untuk aturan tersebut, aturan tersebut akan mewarisi pengaturan dari setiap ACL web tempat Anda menggunakan grup aturan.
- SDK integrasi aplikasi menggunakan waktu kekebalan tantangan ACL web.

Nilai minimum untuk waktu kekebalan tantangan adalah 300 detik. Nilai minimum untuk waktu kekebalan CAPTCHA adalah 60 detik. Nilai maksimum untuk kedua waktu kekebalan adalah 259.200 detik, atau tiga hari.

Anda dapat menggunakan ACL web dan pengaturan waktu kekebalan tingkat aturan untuk menyetel CAPTCHA tindakanChallenge, atau perilaku manajemen tantangan SDK. Misalnya, Anda dapat mengonfigurasi aturan yang mengontrol akses ke data yang sangat sensitif dengan waktu kekebalan rendah, lalu menetapkan waktu kekebalan yang lebih tinggi di ACL web Anda untuk aturan lain dan SDK yang akan diwarisi.

Khususnya untuk CAPTCHA, memecahkan teka-teki dapat menurunkan pengalaman situs web pelanggan Anda, jadi menyetel waktu kekebalan CAPTCHA dapat membantu Anda mengurangi dampak pada pengalaman pelanggan sambil tetap memberikan perlindungan yang Anda inginkan.

Untuk informasi tambahan tentang menyetel waktu kekebalan untuk penggunaan tindakan Challenge dan CAPTCHA aturan Anda, lihatPraktik terbaik untuk menggunakan CAPTCHA dan Challenge tindakan.

Tempat mengatur waktu kekebalan AWS WAF token

Anda dapat mengatur waktu kekebalan di ACL web Anda dan dalam aturan Anda yang menggunakan tindakan Challenge dan CAPTCHA aturan.

Untuk informasi umum tentang mengelola ACL web dan aturannya, lihatBekerja dengan ACL web.

Tempat mengatur waktu kekebalan untuk ACL web

- Konsol — Saat Anda mengedit ACL web, di tab Aturan, edit dan ubah pengaturan di konfigurasi ACL CAPTCHA Web dan panel konfigurasi Tantangan ACL Web. Di konsol, Anda dapat mengonfigurasi ACL CAPTCHA web dan menantang waktu kekebalan hanya setelah Anda membuat ACL web.
- Di luar konsol - Tipe data ACL web memiliki CAPTCHA dan parameter konfigurasi tantangan, yang dapat Anda konfigurasi dan berikan untuk membuat dan memperbarui operasi di ACL web.

Di mana mengatur waktu kekebalan untuk suatu aturan

- Konsol — Saat membuat atau mengedit aturan dan menentukan Challenge tindakan CAPTCHA atau, Anda dapat mengubah pengaturan waktu kekebalan aturan.
- Di luar konsol — Tipe data aturan memiliki CAPTCHA dan parameter konfigurasi tantangan, yang dapat Anda konfigurasikan saat Anda menentukan aturan.

AWS WAF domain token dan daftar domain

Saat AWS WAF membuat token untuk klien, itu mengonfigurasinya dengan domain token. Saat AWS WAF memeriksa token dalam permintaan web, token tersebut menolak token sebagai tidak valid jika domainnya tidak cocok dengan domain mana pun yang dianggap valid untuk ACL web.

Secara default, AWS WAF hanya menerima token yang pengaturan domainnya sama persis dengan domain host dari sumber daya yang terkait dengan ACL web. Ini adalah nilai `Host` header dalam permintaan web. Di browser, Anda dapat menemukan domain ini di JavaScript `window.location.hostname` properti dan di alamat yang dilihat pengguna Anda di bilah alamat mereka.

Anda juga dapat menentukan domain token yang dapat diterima dalam konfigurasi ACL web Anda, seperti yang dijelaskan di bagian berikut. Dalam hal ini, AWS WAF menerima kedua kecocokan persis dengan header host dan cocok dengan domain dalam daftar domain token.

Anda dapat menentukan domain token AWS WAF untuk digunakan saat menyetel domain dan saat mengevaluasi token di ACL web. Domain yang Anda tentukan tidak dapat berupa sufiks publik seperti. `gov.au` Untuk domain yang tidak dapat Anda gunakan, lihat daftar https://publicsuffix.org/list/public_suffix_list.dat di bawah Daftar akhiran publik.

AWS WAF konfigurasi daftar domain token ACL web

Anda dapat mengonfigurasi ACL web untuk berbagi token di beberapa sumber daya yang dilindungi dengan menyediakan daftar domain token dengan domain tambahan yang AWS WAF ingin Anda terima. Dengan daftar domain token, AWS WAF masih menerima domain host sumber daya. Selain itu, ia menerima semua domain dalam daftar domain token, termasuk subdomain awalan mereka.

Misalnya, spesifikasi domain `example.com` dalam daftar domain token Anda cocok dengan `example.com` (dari`http://example.com/`),`api.example.com`, (dari`http://api.example.com/`), dan `www.example.com` (dari`http://www.example.com/`). Itu

tidak cocokexample.api.com, (darihttp://example.api.com/), atau apiexample.com (darihttp://apiexample.com/).

Anda dapat mengonfigurasi daftar domain token di ACL web Anda saat Anda membuat atau mengeditnya. Untuk informasi umum tentang mengelola ACL web, lihatBekerja dengan ACL web.

AWS WAF pengaturan domain token

AWS WAF membuat token atas permintaan skrip tantangan, yang dijalankan oleh SDK integrasi aplikasi dan tindakan CAPTCHA aturan Challenge dan.

Domain yang AWS WAF ditetapkan dalam token ditentukan oleh jenis skrip tantangan yang memintanya dan konfigurasi domain token tambahan apa pun yang Anda berikan. AWS WAF menetapkan domain dalam token ke pengaturan terpendek dan paling umum yang dapat ditemukan dalam konfigurasi.

- JavaScript SDK — Anda dapat mengonfigurasi JavaScript SDK dengan spesifikasi domain token, yang dapat menyertakan satu atau beberapa domain. Domain yang Anda konfigurasikan harus domain yang AWS WAF akan menerima, berdasarkan domain host yang dilindungi dan daftar domain token ACL web.

  Saat AWS WAF mengeluarkan token untuk klien, ia menetapkan domain token ke domain yang cocok dengan domain host dan merupakan yang terpendek, dari antara domain host dan domain dalam daftar yang dikonfigurasi. Misalnya, jika domain host `api.example.com` dan daftar domain token memilikiexample.com, AWS WAF gunakan `example.com` dalam token, karena cocok dengan domain host dan lebih pendek. Jika Anda tidak memberikan daftar domain token dalam konfigurasi JavaScript API, AWS WAF tetapkan domain ke domain host dari sumber daya yang dilindungi.

  Untuk informasi selengkapnya, lihat Menyediakan domain untuk digunakan dalam token.
- Mobile SDK — Dalam kode aplikasi Anda, Anda harus mengonfigurasi SDK seluler dengan properti domain token. Properti ini harus berupa domain yang AWS WAF akan menerima, berdasarkan domain host yang dilindungi dan daftar domain token ACL web.

  Saat AWS WAF mengeluarkan token untuk klien, ia menggunakan properti ini sebagai domain token. AWS WAF tidak menggunakan domain host dalam token yang dikeluarkan untuk klien SDK seluler.

  Untuk informasi selengkapnya, lihat `WAFConfiguration` `domainName` pengaturan diSpesifikasi SDK AWS WAF seluler.

- Challengetindakan — Jika Anda menentukan daftar domain token di ACL web, AWS WAF tetapkan domain token ke domain yang cocok dengan domain host dan merupakan yang terpendek, dari antara domain host dan domain dalam daftar. Misalnya, jika domain host `api.example.com` dan daftar domain token memilikiexample.com, AWS WAF gunakan `example.com` dalam token, karena cocok dengan domain host dan lebih pendek. Jika Anda tidak memberikan daftar domain token di ACL web, AWS WAF tetapkan domain ke domain host dari sumber daya yang dilindungi.

AWS WAF pelabelan token oleh bot dan grup aturan yang dikelola penipuan

Bagian ini menjelaskan label yang ditambahkan manajemen AWS WAF token ke permintaan web. Untuk informasi umum tentang label, lihatAWS WAF label pada permintaan web.

Saat Anda menggunakan salah satu grup aturan terkelola AWS WAF bot atau kontrol penipuan, grup aturan menggunakan manajemen AWS WAF token untuk memeriksa token permintaan web dan menerapkan pelabelan token ke permintaan. Untuk informasi tentang grup aturan terkelola, lihatAWS WAF Grup aturan pencegahan penipuan (ACFP) pembuatan akun Kontrol Penipuan,AWS WAF Kelompok aturan pencegahan pengambilalihan akun Kontrol Penipuan (ATP), danAWS WAF Grup aturan Bot Control.

> **Note**
>
> AWS WAF menerapkan label token hanya jika Anda menggunakan salah satu grup aturan terkelola mitigasi ancaman cerdas ini.

Manajemen token dapat menambahkan label berikut ke permintaan web.

Label sesi klien

Label `awswaf:managed:token:id:`*`identifier`* berisi pengenal unik yang digunakan manajemen AWS WAF token untuk mengidentifikasi sesi klien. Pengidentifikasi dapat berubah jika klien memperoleh token baru, misalnya setelah membuang token yang digunakannya.

> **Note**
>
> AWS WAF tidak melaporkan CloudWatch metrik Amazon untuk label ini.

Label status token: Awalan namespace label

Label status token melaporkan status token dan tantangan serta informasi CAPTCHA yang dikandungnya.

Setiap label status token dimulai dengan salah satu awalan namespace berikut:

- `awswaf:managed:token:` — Digunakan untuk melaporkan status umum token dan melaporkan status informasi tantangan token.
- `awswaf:managed:captcha:` — Digunakan untuk melaporkan status informasi CAPTCHA token.

Label status token: Nama label

Mengikuti awalan, sisa label memberikan informasi status token terperinci:

- `accepted` — Token permintaan hadir dan berisi yang berikut:
  - Tantangan yang valid atau solusi CAPTCHA.
  - Tantangan yang belum kedaluwarsa atau cap waktu CAPTCHA.
  - Spesifikasi domain yang valid untuk web ACL.

  Contoh: Label `awswaf:managed:token:accepted` menunjukkan bahwa token permintaan web memiliki solusi tantangan yang valid, stempel waktu tantangan yang belum kedaluwarsa, dan domain yang valid.
- `rejected` — Token permintaan ada tetapi tidak memenuhi kriteria penerimaan.

  Seiring dengan label yang ditolak, manajemen token menambahkan namespace dan nama label khusus untuk menunjukkan alasannya.
  - `rejected:not_solved` — Token tidak memiliki tantangan atau solusi CAPTCHA.
  - `rejected:expired` — Tantangan token atau cap waktu CAPTCHA telah kedaluwarsa, sesuai dengan waktu kekebalan token ACL web Anda yang dikonfigurasi.
  - `rejected:domain_mismatch` — Domain token tidak cocok untuk konfigurasi domain token ACL web Anda.
  - `rejected:invalid` — AWS WAF tidak bisa membaca token yang ditunjukkan.

  Contoh: Label `awswaf:managed:captcha:rejected` dan `awswaf:managed:captcha:rejected:expired` menunjukkan bahwa permintaan ditolak karena cap waktu CAPTCHA dalam token telah melebihi waktu kekebalan token CAPTCHA yang dikonfigurasi di ACL web.
- `absent` — Permintaan tidak memiliki token atau manajer token tidak dapat membacanya.

Contoh: Label `awswaf:managed:captcha:absent` menunjukkan bahwa permintaan tidak memiliki token.

Memblokir permintaan yang tidak memiliki AWS WAF token yang valid

Saat Anda menggunakan grup aturan Aturan AWS Terkelola ancaman cerdas `AWSManagedRulesACFPRuleSet` `AWSManagedRulesATPRuleSetAWSManagedRulesBotControlRuleSet`, dan, grup aturan akan memanggil manajemen AWS WAF token untuk mengevaluasi status token permintaan web dan memberi label permintaan yang sesuai.

> **Note**
>
> Pelabelan token hanya diterapkan pada permintaan web yang Anda evaluasi menggunakan salah satu grup aturan terkelola ini.

Untuk informasi tentang pelabelan yang diterapkan manajemen token, lihat bagian sebelumnya,. AWS WAF pelabelan token oleh bot dan grup aturan yang dikelola penipuan

Kelompok aturan terkelola mitigasi ancaman cerdas kemudian menangani persyaratan token sebagai berikut:

- `AWSManagedRulesACFPRuleSetAllRequests`Aturan dikonfigurasi untuk menjalankan Challenge tindakan terhadap semua permintaan, secara efektif memblokir semua yang tidak memiliki label `accepted` token.
- Permintaan `AWSManagedRulesATPRuleSet` blok yang memiliki label `rejected` token, tetapi tidak memblokir permintaan dengan label `absent` token.
- Tingkat perlindungan yang `AWSManagedRulesBotControlRuleSet` ditargetkan menantang klien setelah mereka mengirim lima permintaan tanpa label `accepted` token. Itu tidak memblokir permintaan individu yang tidak memiliki token yang valid. Tingkat perlindungan umum grup aturan tidak mengelola persyaratan token.

Untuk detail tambahan tentang kelompok aturan ancaman cerdas, lihatAWS WAF Grup aturan pencegahan penipuan (ACFP) pembuatan akun Kontrol Penipuan, AWS WAF Kelompok aturan pencegahan pengambilalihan akun Kontrol Penipuan (ATP) danAWS WAF Grup aturan Bot Control.

Untuk memblokir permintaan yang tidak memiliki token saat menggunakan Bot Control atau grup aturan terkelola ATP

Dengan Bot Control dan grup aturan ATP, dimungkinkan untuk permintaan tanpa token yang valid untuk keluar dari evaluasi grup aturan dan terus dievaluasi oleh ACL web.

Untuk memblokir semua permintaan yang tidak ada tokennya atau tokennya ditolak, tambahkan aturan untuk dijalankan segera setelah grup aturan terkelola menangkap dan memblokir permintaan yang tidak ditangani oleh grup aturan untuk Anda.

Berikut ini adalah contoh daftar JSON untuk ACL web yang menggunakan grup aturan terkelola ATP. Web ACL memiliki aturan tambahan untuk menangkap `awswaf:managed:token:absent` label dan menanganinya. Aturan mempersempit evaluasinya ke permintaan web yang masuk ke titik akhir login, agar sesuai dengan ruang lingkup grup aturan ATP. Aturan yang ditambahkan tercantum dalam huruf tebal.

```
{
  "Name": "exampleWebACL",
  "Id": "55555555-6666-7777-8888-999999999999",
  "ARN": "arn:aws:wafv2:us-east-1:111111111111:regional/webacl/
exampleWebACL/55555555-4444-3333-2222-111111111111",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesATPRuleSet",
      "Priority": 1,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesATPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesATPRuleSet": {
                "LoginPath": "/web/login",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
```

```
                "PasswordField": {
                  "Identifier": "/form/password"
                }
              },
              "ResponseInspection": {
                "StatusCode": {
                  "SuccessCodes": [
                    200
                  ],
                  "FailureCodes": [
                    401,
                    403,
                    500
                  ]
                }
              }
            }
          }
        ]
      }
    },
    "OverrideAction": {
      "None": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSManagedRulesATPRuleSet"
    }
  },
  {
    "Name": "RequireTokenForLogins",
    "Priority": 2,
    "Statement": {
      "AndStatement": {
        "Statements": [
          {
            "Statement": {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:token:absent"
              }
            }
          },
```

```
            {
              "ByteMatchStatement": {
                "SearchString": "/web/login",
                "FieldToMatch": {
                  "UriPath": {}
                },
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                 }
                ],
                "PositionalConstraint": "STARTS_WITH"
              }
            },
            {
              "ByteMatchStatement": {
                "SearchString": "POST",
                "FieldToMatch": {
                  "Method": {}
                },
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ],
                "PositionalConstraint": "EXACTLY"
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "RequireTokenForLogins"
      }
    }
  ],
  "VisibilityConfig": {
```

```
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "exampleWebACL"
  },
  "Capacity": 51,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:111111111111:webacl:exampleWebACL:"
}
```

Konfigurasi yang diperlukan untuk Application Load Balancer yang berasal CloudFront

Baca bagian ini jika Anda mengaitkan ACL web Anda ke Application Load Balancer dan Anda menggunakan Application Load Balancer sebagai asal distribusi. CloudFront

Dengan arsitektur ini, Anda perlu menyediakan konfigurasi tambahan berikut agar informasi token ditangani dengan benar.

- Konfigurasikan CloudFront untuk meneruskan `aws-waf-token` cookie ke Application Load Balancer. Secara default, CloudFront menghapus cookie dari permintaan web sebelum meneruskannya ke asal. Untuk menyimpan cookie token dengan permintaan web, konfigurasikan perilaku CloudFront cache untuk menyertakan hanya cookie token atau semua cookie. Untuk informasi tentang cara melakukannya, lihat Caching konten berdasarkan cookie di Panduan CloudFront Pengembang Amazon.
- Konfigurasikan AWS WAF sehingga mengenali domain CloudFront distribusi sebagai domain token yang valid. Secara default, CloudFront tetapkan `Host` header ke asal Application Load Balancer, dan AWS WAF menggunakannya sebagai domain sumber daya yang dilindungi. Browser klien, bagaimanapun, melihat CloudFront distribusi sebagai domain host, dan token yang dihasilkan untuk klien menggunakan CloudFront domain sebagai domain token. Tanpa konfigurasi tambahan, saat AWS WAF memeriksa domain sumber daya yang dilindungi terhadap domain token, itu akan mendapatkan ketidakcocokan. Untuk memperbaikinya, tambahkan nama domain CloudFront distribusi ke daftar domain token dalam konfigurasi ACL web Anda. Untuk informasi tentang cara melakukan ini, lihat AWS WAF konfigurasi daftar domain token ACL web.

AWS WAF Pencegahan penipuan pembuatan akun Kontrol Penipuan (ACFP)

Penipuan pembuatan akun adalah aktivitas ilegal online di mana penyerang mencoba membuat satu atau lebih akun palsu. Penyerang menggunakan akun palsu untuk kegiatan penipuan seperti

menyalahgunakan promosi dan mendaftar bonus, meniru seseorang, dan serangan cyber seperti phishing. Kehadiran akun palsu dapat berdampak negatif pada bisnis Anda dengan merusak reputasi Anda dengan pelanggan dan paparan penipuan keuangan.

Anda dapat memantau dan mengontrol upaya penipuan pembuatan akun dengan menerapkan fitur pencegahan AWS WAF penipuan pembuatan akun Kontrol Penipuan (ACFP). AWS WAF menawarkan fitur ini di grup aturan Aturan AWS Terkelola `AWSManagedRulesACFPRuleSet` dengan SDK integrasi aplikasi pendamping.

Grup aturan terkelola ACFP memberi label dan mengelola permintaan yang mungkin merupakan bagian dari upaya pembuatan akun berbahaya. Grup aturan melakukan ini dengan memeriksa upaya pembuatan akun yang dikirim klien ke titik akhir pendaftaran akun aplikasi Anda.

ACFP melindungi halaman pendaftaran akun Anda dengan memantau permintaan pendaftaran akun untuk aktivitas anomali dan dengan secara otomatis memblokir permintaan yang mencurigakan. Kelompok aturan menggunakan pengidentifikasi permintaan, analisis perilaku, dan pembelajaran mesin untuk mendeteksi permintaan penipuan.

- Inspeksi permintaan — ACFP memberi Anda visibilitas dan kontrol atas upaya pembuatan akun anomali dan upaya yang menggunakan kredensi curian, untuk mencegah pembuatan akun penipuan. ACFP memeriksa kombinasi email dan kata sandi terhadap basis data kredensialnya yang dicuri, yang diperbarui secara berkala karena kredensi baru yang bocor ditemukan di web gelap. ACFP mengevaluasi domain yang digunakan dalam alamat email, dan memantau penggunaan nomor telepon dan bidang alamat untuk memverifikasi entri dan untuk mendeteksi perilaku penipuan. ACFP mengumpulkan data berdasarkan alamat IP dan sesi klien, untuk mendeteksi dan memblokir klien yang mengirim terlalu banyak permintaan yang bersifat mencurigakan.
- Inspeksi respons — Untuk CloudFront distribusi, selain memeriksa permintaan pembuatan akun yang masuk, grup aturan ACFP memeriksa respons aplikasi Anda terhadap upaya pembuatan akun, untuk melacak tingkat keberhasilan dan kegagalan. Dengan menggunakan informasi ini, ACFP dapat memblokir sementara sesi klien atau alamat IP yang memiliki terlalu banyak upaya gagal. AWS WAF melakukan inspeksi respons secara asinkron, jadi ini tidak meningkatkan latensi dalam lalu lintas web Anda.

> **Note**
>
> Anda akan dikenakan biaya tambahan saat menggunakan grup aturan terkelola ini. Untuk informasi selengkapnya, silakan lihat Harga AWS WAF.

> **Note**
>
> Fitur ACFP tidak tersedia untuk kumpulan pengguna Amazon Cognito.

Topik

- AWS WAF Komponen ACFP
- Mengapa Anda harus menggunakan SDK integrasi aplikasi dengan ACFP
- Menambahkan grup aturan terkelola ACFP ke ACL web Anda
- Menguji dan menerapkan ACFP
- AWS WAF Contoh pencegahan penipuan pembuatan akun Kontrol Penipuan (ACFP)

AWS WAF Komponen ACFP

Komponen utama pencegahan AWS WAF penipuan pembuatan akun Kontrol Penipuan (ACFP) adalah sebagai berikut:

- **`AWSManagedRulesACFPRuleSet`**— Aturan dalam grup aturan Aturan AWS Terkelola ini mendeteksi, memberi label, dan menangani berbagai jenis aktivitas pembuatan akun penipuan. Grup aturan memeriksa permintaan `GET` teks/html HTTP yang dikirim klien ke titik akhir pendaftaran akun tertentu dan permintaan `POST` web yang dikirim klien ke titik akhir pendaftaran akun yang ditentukan. Untuk CloudFront distribusi yang dilindungi, grup aturan juga memeriksa respons yang dikirim distribusi kembali ke permintaan pembuatan akun. Untuk daftar aturan grup aturan ini, lihatAWS WAF Grup aturan pencegahan penipuan (ACFP) pembuatan akun Kontrol Penipuan. Anda menyertakan grup aturan ini di ACL web Anda menggunakan pernyataan referensi grup aturan terkelola. Untuk informasi tentang menggunakan grup aturan ini, lihatMenambahkan grup aturan terkelola ACFP ke ACL web Anda.

> **Note**
>
> Anda akan dikenakan biaya tambahan saat menggunakan grup aturan terkelola ini. Untuk informasi selengkapnya, silakan lihat Harga AWS WAF.

- Detail tentang halaman pendaftaran dan pembuatan akun aplikasi Anda — Anda harus memberikan informasi tentang halaman pendaftaran dan pembuatan akun Anda saat menambahkan grup `AWSManagedRulesACFPRuleSet` aturan ke ACL web Anda. Ini memungkinkan grup aturan mempersempit cakupan permintaan yang diperiksa dan memvalidasi permintaan web pembuatan akun dengan benar. Halaman pendaftaran harus menerima permintaan `GET` teks/html. Jalur pembuatan akun harus menerima `POST` permintaan. Grup aturan ACFP bekerja dengan nama pengguna yang dalam format email. Untuk informasi selengkapnya, lihat Menambahkan grup aturan terkelola ACFP ke ACL web Anda.
- Untuk CloudFront distribusi yang dilindungi, detail tentang bagaimana aplikasi Anda merespons upaya pembuatan akun — Anda memberikan detail tentang tanggapan aplikasi Anda terhadap upaya pembuatan akun, dan grup aturan ACFP melacak dan mengelola upaya pembuatan akun massal dari satu alamat IP atau sesi klien tunggal. Untuk informasi tentang mengonfigurasi opsi ini, lihatMenambahkan grup aturan terkelola ACFP ke ACL web Anda.
- JavaScript dan SDK integrasi aplikasi seluler — Terapkan SDK AWS WAF JavaScript dan seluler dengan implementasi ACFP Anda untuk mengaktifkan rangkaian lengkap kemampuan yang ditawarkan grup aturan. Banyak aturan ACFP menggunakan informasi yang disediakan oleh SDK untuk verifikasi klien tingkat sesi dan agregasi perilaku, yang diperlukan untuk memisahkan lalu lintas klien yang sah dari lalu lintas bot. Untuk informasi selengkapnya tentang SDK, lihat AWS WAF integrasi aplikasi klien.

Anda dapat menggabungkan implementasi ACFP Anda dengan yang berikut ini untuk membantu Anda memantau, menyetel, dan menyesuaikan perlindungan Anda.

- Logging dan metrik — Anda dapat memantau lalu lintas, dan memahami bagaimana grup aturan terkelola ACFP memengaruhi hal itu, dengan mengonfigurasi dan mengaktifkan log, pengumpulan data Amazon Security Lake, dan metrik CloudWatch Amazon untuk ACL web Anda. Label yang `AWSManagedRulesACFPRuleSet` menambah permintaan web Anda disertakan dalam data. Untuk informasi tentang opsi, lihat, Pencatatan AWS WAF lalu lintas ACL webPemantauan CloudWatch dengan Amazon, dan Apa itu Amazon Security Lake? .

Tergantung pada kebutuhan Anda dan lalu lintas yang Anda lihat, Anda mungkin ingin menyesuaikan `AWSManagedRulesACFPRuleSet` implementasi Anda. Misalnya, Anda mungkin ingin mengecualikan beberapa lalu lintas dari evaluasi ACFP, atau Anda mungkin ingin mengubah cara menangani beberapa upaya penipuan pembuatan akun yang diidentifikasi, menggunakan AWS WAF fitur seperti pernyataan cakupan bawah atau aturan pencocokan label.

- Aturan pencocokan label dan label — Untuk salah satu aturan di`AWSManagedRulesACFPRuleSet`, Anda dapat mengubah perilaku pemblokiran untuk menghitung, lalu mencocokkan dengan label yang ditambahkan oleh aturan. Gunakan pendekatan ini untuk menyesuaikan cara Anda menangani permintaan web yang diidentifikasi oleh grup aturan terkelola ACFP. Untuk informasi selengkapnya tentang pelabelan dan penggunaan pernyataan pencocokan label, lihat Pernyataan aturan pencocokan label danAWS WAF label pada permintaan web.
- Permintaan dan tanggapan khusus - Anda dapat menambahkan header khusus ke permintaan yang Anda izinkan dan Anda dapat mengirim tanggapan khusus untuk permintaan yang Anda blokir. Untuk melakukan ini, Anda memasangkan label yang cocok dengan permintaan AWS WAF kustom dan fitur respons. Untuk informasi selengkapnya tentang menyesuaikan permintaan dan tanggapan, lihatPermintaan dan tanggapan web yang disesuaikan di AWS WAF.

Mengapa Anda harus menggunakan SDK integrasi aplikasi dengan ACFP

Kami sangat menyarankan untuk menerapkan SDK integrasi aplikasi, untuk penggunaan grup aturan ACFP yang paling efisien.

- Fungsionalitas grup aturan lengkap — Aturan ACFP `SignalClientHumanInteractivityAbsentLow` hanya berfungsi dengan token yang diisi oleh integrasi aplikasi. Aturan ini mendeteksi dan mengelola interaktivitas manusia yang abnormal dengan halaman aplikasi. SDK integrasi aplikasi dapat mendeteksi interaktivitas manusia normal melalui gerakan mouse, penekanan tombol, dan pengukuran lainnya. Pengantara yang dikirim oleh tindakan aturan CAPTCHA dan tidak Challenge dapat menyediakan jenis data ini.
- Mengurangi latensi — Aturan grup Challenge aturan `AllRequests` menerapkan tindakan aturan untuk setiap permintaan yang belum memiliki token tantangan. Ketika ini terjadi, permintaan dievaluasi oleh kelompok aturan dua kali: sekali tanpa token, dan kemudian kedua kalinya setelah token diperoleh melalui Challenge tindakan pengantara. Anda tidak dikenakan biaya tambahan untuk hanya menggunakan `AllRequests` aturan, tetapi pendekatan ini menambahkan overhead ke lalu lintas web Anda dan menambahkan latensi ke pengalaman pengguna akhir Anda. Jika

Anda memperoleh token sisi klien menggunakan integrasi aplikasi, sebelum mengirim permintaan pembuatan akun, grup aturan ACFP mengevaluasi permintaan satu kali.

Untuk informasi selengkapnya tentang kemampuan grup aturan, lihatAWS WAF Grup aturan pencegahan penipuan (ACFP) pembuatan akun Kontrol Penipuan.

Untuk informasi tentang SDK, lihatAWS WAF integrasi aplikasi klien. Untuk informasi tentang AWS WAF token, lihatAWS WAF token permintaan web. Untuk informasi tentang tindakan aturan, lihatCAPTCHAdan Challenge di AWS WAF.

Menambahkan grup aturan terkelola ACFP ke ACL web Anda

Untuk mengonfigurasi grup aturan terkelola ACFP untuk mengenali aktivitas penipuan pembuatan akun di lalu lintas web Anda, Anda memberikan informasi tentang cara klien mengakses halaman pendaftaran Anda dan mengirim permintaan pembuatan akun ke aplikasi Anda. Untuk CloudFront distribusi Amazon yang dilindungi, Anda juga memberikan informasi tentang bagaimana aplikasi Anda merespons permintaan pembuatan akun. Konfigurasi ini merupakan tambahan dari konfigurasi normal untuk grup aturan terkelola.

Untuk deskripsi grup aturan dan daftar aturan, lihatAWS WAF Grup aturan pencegahan penipuan (ACFP) pembuatan akun Kontrol Penipuan.

> **Note**
>
> Basis data kredensyal curian ACFP hanya berisi nama pengguna dalam format email.

Panduan ini ditujukan untuk pengguna yang tahu secara umum cara membuat dan mengelola ACL AWS WAF web, aturan, dan grup aturan. Topik-topik tersebut dibahas di bagian sebelumnya dari panduan ini. Untuk informasi dasar tentang cara menambahkan grup aturan terkelola ke ACL web Anda, lihatMenambahkan grup aturan terkelola ke ACL web melalui konsol.

Ikuti praktik terbaik

Gunakan grup aturan ACFP sesuai dengan praktik terbaik di. Praktik terbaik untuk mitigasi ancaman cerdas

Untuk menggunakan grup **`AWSManagedRulesACFPRuleSet`** aturan di ACL web Anda

1. Tambahkan grup aturan AWS terkelola, `AWSManagedRulesACFPRuleSet` ke ACL web Anda, dan Edit pengaturan grup aturan sebelum menyimpan.

   > **Note**
   >
   > Anda akan dikenakan biaya tambahan saat menggunakan grup aturan terkelola ini. Untuk informasi selengkapnya, silakan lihat Harga AWS WAF.

2. Di panel konfigurasi grup Aturan, berikan informasi yang digunakan grup aturan ACFP untuk memeriksa permintaan pembuatan akun.

   a. Untuk Gunakan ekspresi reguler di jalur, aktifkan ini jika Anda ingin AWS WAF melakukan pencocokan ekspresi reguler untuk spesifikasi jalur halaman pendaftaran dan pembuatan akun Anda.

      AWS WAF mendukung sintaks pola yang digunakan oleh pustaka PCRE `libpcre` dengan beberapa pengecualian. Pustaka didokumentasikan di PCRE - Perl Compatible Regular Expressions. Untuk informasi tentang AWS WAF dukungan, lihatPencocokan pola ekspresi reguler di AWS WAF.

   b. Untuk jalur halaman Pendaftaran, berikan jalur titik akhir halaman pendaftaran untuk aplikasi Anda. Halaman ini harus menerima permintaan `GET` teks/html. Grup aturan hanya memeriksa permintaan `GET` teks/html HTTP ke titik akhir halaman pendaftaran yang Anda tentukan.

      > **Note**
      >
      > Pencocokan untuk titik akhir tidak peka huruf besar/kecil. Spesifikasi Regex tidak boleh berisi bendera, yang menonaktifkan pencocokan yang tidak `(?-i)` peka huruf besar/kecil. Spesifikasi string harus dimulai dengan garis miring `/` ke depan.

      Misalnya, untuk URL`https://example.com/web/registration`, Anda dapat memberikan spesifikasi jalur string`/web/registration`. Jalur halaman pendaftaran yang dimulai dengan jalur yang Anda berikan dianggap cocok. Misalnya `/web/registration` cocok dengan jalur pendaftaran`/web/registration`,`/web/registration/`,`/web/`

`registrationPage`, dan`/web/registration/thisPage`, tetapi tidak cocok dengan jalur `/home/web/registration` atau`/website/registration`.

> **Note**
>
> Pastikan bahwa pengguna akhir Anda memuat halaman pendaftaran sebelum mereka mengirimkan permintaan pembuatan akun. Ini membantu memastikan bahwa permintaan pembuatan akun dari klien menyertakan token yang valid.

c. Untuk jalur pembuatan Akun, berikan URI di situs web Anda yang menerima detail pengguna baru yang telah selesai. URI ini harus menerima `POST` permintaan.

> **Note**
>
> Pencocokan untuk titik akhir tidak peka huruf besar/kecil. Spesifikasi Regex tidak boleh berisi bendera, yang menonaktifkan pencocokan yang tidak `(?-i)` peka huruf besar/kecil. Spesifikasi string harus dimulai dengan garis miring `/` ke depan.

Misalnya, untuk URL`https://example.com/web/newaccount`, Anda dapat memberikan spesifikasi jalur string`/web/newaccount`. Jalur pembuatan akun yang dimulai dengan jalur yang Anda berikan dianggap cocok. Misalnya `/web/newaccount` cocok dengan jalur pembuatan akun`/web/newaccount`,`/web/newaccount/`,`/web/newaccountPage`, dan`/web/newaccount/thisPage`, tetapi tidak cocok dengan jalur `/home/web/newaccount` atau`/website/newaccount`.

d. Untuk pemeriksaan Permintaan, tentukan bagaimana aplikasi Anda menerima upaya pembuatan akun dengan memberikan jenis payload permintaan dan nama bidang dalam badan permintaan tempat nama pengguna, kata sandi, dan detail pembuatan akun lainnya disediakan.

> **Note**
>
> Untuk bidang alamat utama dan nomor telepon, berikan bidang sesuai urutan tampilannya di payload permintaan.

Spesifikasi nama bidang Anda tergantung pada jenis payload.

- Jenis payload JSON - Tentukan nama bidang dalam sintaks penunjuk JSON. Untuk informasi tentang sintaks JSON Pointer, lihat dokumentasi Internet Engineering Task Force (IETF) JavaScriptObject Notation (JSON) Pointer.

  Misalnya, untuk contoh payload JSON berikut, spesifikasi bidang nama pengguna adalah `/signupform/username` dan spesifikasi bidang alamat utama adalah`/signupform/addrp1`,`/signupform/addrp2`, dan. `/signupform/addrp3`

```
{
    "signupform": {
        "username": "THE_USERNAME",
        "password": "THE_PASSWORD",
        "addrp1": "PRIMARY_ADDRESS_LINE_1",
        "addrp2": "PRIMARY_ADDRESS_LINE_2",
        "addrp3": "PRIMARY_ADDRESS_LINE_3",
        "phonepcode": "PRIMARY_PHONE_CODE",
        "phonepnumber": "PRIMARY_PHONE_NUMBER"
    }
}
```

- Jenis payload FORM_ENCODED - Gunakan nama formulir HTML.

  Misalnya, untuk formulir HTML dengan elemen input pengguna dan kata sandi bernama `username1` dan`password1`, spesifikasi bidang nama pengguna adalah `username1` dan spesifikasi bidang kata sandi adalah`password1`.

e. Jika Anda melindungi CloudFront distribusi Amazon, maka di bawah pemeriksaan Response, tentukan bagaimana aplikasi Anda menunjukkan keberhasilan atau kegagalan dalam tanggapannya terhadap upaya pembuatan akun.

> **Note**
>
> Pemeriksaan respons ACFP hanya tersedia di ACL web yang melindungi distribusi. CloudFront

Tentukan satu komponen dalam respons pembuatan akun yang ingin diperiksa oleh ACFP. Untuk tipe komponen Body dan JSON, AWS WAF dapat memeriksa 65.536 byte pertama (64 KB) komponen.

Berikan kriteria inspeksi Anda untuk jenis komponen, seperti yang ditunjukkan oleh antarmuka. Anda harus memberikan kriteria keberhasilan dan kegagalan untuk diperiksa dalam komponen.

Misalnya, aplikasi Anda menunjukkan status upaya pembuatan akun dalam kode status respons, dan digunakan `200 OK` untuk sukses dan `401 Unauthorized` atau `403 Forbidden` untuk kegagalan. Anda akan mengatur pemeriksaan respons Jenis komponen ke kode Status, lalu di kotak teks Sukses masukkan `200` dan di kotak teks Kegagalan, masukkan `401` pada baris pertama dan `403` pada baris kedua.

Kelompok aturan ACFP hanya menghitung tanggapan yang sesuai dengan kriteria pemeriksaan keberhasilan atau kegagalan Anda. Aturan kelompok aturan bertindak pada klien sementara mereka memiliki tingkat keberhasilan yang terlalu tinggi di antara tanggapan yang dihitung, untuk mengurangi upaya pembuatan akun massal. Untuk perilaku yang akurat menurut aturan grup aturan, pastikan untuk memberikan informasi lengkap untuk upaya pembuatan akun yang berhasil dan gagal.

Untuk melihat aturan yang memeriksa respons pembuatan akun, cari `VolumetricIPSuccessfulResponse` dan `VolumetricSessionSuccessfulResponse` di daftar aturan di[AWS WAF Grup aturan pencegahan penipuan (ACFP) pembuatan akun Kontrol Penipuan](#).

3. Berikan konfigurasi tambahan apa pun yang Anda inginkan untuk grup aturan.

   Anda dapat membatasi cakupan permintaan yang diperiksa oleh grup aturan dengan menambahkan pernyataan cakupan bawah ke pernyataan grup aturan terkelola. Misalnya, Anda hanya dapat memeriksa permintaan dengan argumen kueri atau cookie tertentu. Grup aturan hanya akan memeriksa permintaan yang sesuai dengan kriteria dalam pernyataan cakupan bawah Anda dan yang dikirim ke jalur pendaftaran akun dan pembuatan akun yang Anda tentukan dalam konfigurasi grup aturan. Untuk informasi tentang pernyataan cakupan bawah, lihat. [Pernyataan cakupan ke bawah](#)

4. Simpan perubahan Anda ke ACL web.

Sebelum Anda menerapkan implementasi ACFP Anda untuk lalu lintas produksi, uji dan sesuaikan di lingkungan pementasan atau pengujian sampai Anda merasa nyaman dengan potensi dampak terhadap lalu lintas Anda. Kemudian uji dan atur aturan dalam mode hitungan dengan lalu lintas produksi Anda sebelum mengaktifkannya. Lihat bagian berikut untuk panduan.

Menguji dan menerapkan ACFP

Bagian ini memberikan panduan umum untuk mengonfigurasi dan menguji implementasi pencegahan AWS WAF penipuan pembuatan akun Kontrol Penipuan (ACFP) untuk situs Anda. Langkah-langkah spesifik yang Anda pilih untuk diikuti akan tergantung pada kebutuhan, sumber daya, dan permintaan web yang Anda terima.

Informasi ini merupakan tambahan dari informasi umum tentang pengujian dan penyetelan yang disediakan diMenguji dan menyetel perlindungan Anda AWS WAF.

> **Note**
>
> AWS Aturan Terkelola dirancang untuk melindungi Anda dari ancaman web umum. Bila digunakan sesuai dengan dokumentasi, grup aturan Aturan AWS Terkelola menambahkan lapisan keamanan lain untuk aplikasi Anda. Namun, grup aturan Aturan AWS Terkelola tidak dimaksudkan sebagai pengganti tanggung jawab keamanan Anda, yang ditentukan oleh AWS sumber daya yang Anda pilih. Lihat Model Tanggung Jawab Bersama untuk memastikan bahwa sumber daya Anda AWS dilindungi dengan benar.

> **Risiko lalu lintas produksi**
>
> Sebelum Anda menerapkan implementasi ACFP Anda untuk lalu lintas produksi, uji dan sesuaikan di lingkungan pementasan atau pengujian sampai Anda merasa nyaman dengan potensi dampak terhadap lalu lintas Anda. Kemudian uji dan atur aturan dalam mode hitungan dengan lalu lintas produksi Anda sebelum mengaktifkannya.

AWS WAF menyediakan kredensyal pengujian yang dapat Anda gunakan untuk memverifikasi konfigurasi ACFP Anda. Dalam prosedur berikut, Anda akan mengonfigurasi ACL web uji untuk menggunakan grup aturan terkelola ACFP, mengonfigurasi aturan untuk menangkap label yang ditambahkan oleh grup aturan, dan kemudian menjalankan upaya pembuatan akun menggunakan kredenal pengujian ini. Anda akan memverifikasi bahwa ACL web Anda telah mengelola upaya dengan benar dengan memeriksa CloudWatch metrik Amazon untuk upaya pembuatan akun.

Panduan ini ditujukan untuk pengguna yang tahu secara umum cara membuat dan mengelola ACL AWS WAF web, aturan, dan grup aturan. Topik-topik tersebut dibahas di bagian sebelumnya dari panduan ini.

Untuk mengkonfigurasi dan menguji implementasi pencegahan AWS WAF penipuan (ACFP) pembuatan akun Kontrol Penipuan

Lakukan langkah-langkah ini terlebih dahulu di lingkungan pengujian, kemudian dalam produksi.

1. Tambahkan grup aturan AWS WAF terkelola pencegahan penipuan (ACFP) pembuatan akun Kontrol Penipuan dalam mode hitung

   > **Note**
   >
   > Anda akan dikenakan biaya tambahan saat menggunakan grup aturan terkelola ini. Untuk informasi selengkapnya, silakan lihat Harga AWS WAF.

   Tambahkan grup aturan Aturan AWS Terkelola `AWSManagedRulesACFPRuleSet` ke ACL web baru atau yang sudah ada dan konfigurasikan agar tidak mengubah perilaku ACL web saat ini. Untuk detail tentang aturan dan label untuk grup aturan ini, lihatAWS WAF Grup aturan pencegahan penipuan (ACFP) pembuatan akun Kontrol Penipuan.

   - Saat Anda menambahkan grup aturan terkelola, edit dan lakukan hal berikut:
     - Di panel konfigurasi grup Aturan, berikan detail halaman pendaftaran dan pembuatan akun aplikasi Anda. Grup aturan ACFP menggunakan informasi ini untuk memantau aktivitas masuk. Untuk informasi selengkapnya, lihat Menambahkan grup aturan terkelola ACFP ke ACL web Anda.
     - Di panel Aturan, buka dropdown Override all rule actions dan pilih. Count Dengan konfigurasi ini, AWS WAF mengevaluasi permintaan terhadap semua aturan dalam grup aturan dan hanya menghitung kecocokan yang dihasilkan, sambil tetap menambahkan label ke permintaan. Untuk informasi selengkapnya, lihat Mengesampingkan tindakan aturan dalam grup aturan.

       Dengan penggantian ini, Anda dapat memantau dampak potensial dari aturan terkelola ACFP untuk menentukan apakah Anda ingin menambahkan pengecualian, seperti pengecualian untuk kasus penggunaan internal.
   - Posisikan grup aturan sehingga dievaluasi setelah aturan yang ada di ACL web, dengan pengaturan prioritas yang secara numerik lebih tinggi daripada aturan atau grup aturan apa pun yang sudah Anda gunakan. Untuk informasi selengkapnya, lihat Memproses urutan aturan dan kelompok aturan dalam ACL web.

Dengan cara ini, penanganan lalu lintas Anda saat ini tidak terganggu. Misalnya, jika Anda memiliki aturan yang mendeteksi lalu lintas berbahaya seperti injeksi SQL atau skrip lintas situs, mereka akan terus mendeteksi dan mencatatnya. Sebagai alternatif, jika Anda memiliki aturan yang memungkinkan lalu lintas non-berbahaya yang diketahui, mereka dapat terus mengizinkan lalu lintas itu, tanpa diblokir oleh grup aturan terkelola ACFP. Anda mungkin memutuskan untuk menyesuaikan urutan pemrosesan selama aktivitas pengujian dan penyetelan Anda.

2. Menerapkan SDK integrasi aplikasi

   Integrasikan AWS WAF JavaScript SDK ke dalam jalur pendaftaran akun dan pembuatan akun browser Anda. AWS WAF juga menyediakan SDK seluler untuk mengintegrasikan perangkat iOS dan Android. Untuk informasi selengkapnya tentang SDK integrasi, lihatAWS WAF integrasi aplikasi klien. Untuk informasi tentang rekomendasi ini, lihatMengapa Anda harus menggunakan SDK integrasi aplikasi dengan ACFP.

   > **Note**
   >
   > Jika Anda tidak dapat menggunakan SDK integrasi aplikasi, Anda dapat menguji grup aturan ACFP dengan mengeditnya di ACL web Anda dan menghapus penggantian yang Anda tempatkan pada aturan. `AllRequests` Ini memungkinkan pengaturan Challenge tindakan aturan, untuk memastikan bahwa permintaan menyertakan token tantangan yang valid.
   > Lakukan ini terlebih dahulu di lingkungan pengujian dan kemudian dengan sangat hati-hati di lingkungan produksi Anda. Pendekatan ini memiliki potensi untuk memblokir pengguna. Misalnya, jika jalur halaman pendaftaran Anda tidak menerima permintaan `GET` teks/html, konfigurasi aturan ini dapat secara efektif memblokir semua permintaan di halaman pendaftaran.

3. Aktifkan pencatatan dan metrik untuk ACL web

   Jika diperlukan, konfigurasikan pencatatan, pengumpulan data Amazon Security Lake, pengambilan sampel permintaan, dan CloudWatch metrik Amazon untuk ACL web. Anda dapat menggunakan alat visibilitas ini untuk memantau interaksi grup aturan terkelola ACFP dengan lalu lintas Anda.

   - Untuk informasi tentang pencatatan, lihatPencatatan AWS WAF lalu lintas ACL web.

- Untuk informasi tentang Amazon Security Lake, lihat Apa itu Amazon Security Lake? dan Mengumpulkan data dari AWS layanan di panduan pengguna Amazon Security Lake.
- Untuk informasi tentang CloudWatch metrik Amazon, lihatPemantauan CloudWatch dengan Amazon.
- Untuk informasi tentang pengambilan sampel permintaan web, lihatMelihat contoh permintaan web.

4. Kaitkan ACL web dengan sumber daya

   Jika ACL web belum dikaitkan dengan sumber daya pengujian, kaitkan. Untuk informasi, lihat Mengaitkan atau memisahkan ACL web dengan sumber daya AWS.

5. Pantau lalu lintas dan kecocokan aturan ACFP

   Pastikan lalu lintas normal Anda mengalir dan aturan grup aturan terkelola ACFP menambahkan label ke permintaan web yang cocok. Anda dapat melihat label di log dan melihat metrik ACFP dan label di metrik Amazon. CloudWatch Di log, aturan yang telah Anda ganti untuk dihitung dalam grup aturan muncul di `action` set to count, dan `ruleGroupList` dengan `overriddenAction` menunjukkan tindakan aturan yang dikonfigurasi yang Anda timpa.

6. Uji kemampuan pemeriksaan kredensi grup aturan

   Lakukan upaya pembuatan akun dengan menguji kredensi yang dikompromikan dan periksa apakah grup aturan cocok dengan mereka seperti yang diharapkan.

   a. Akses halaman pendaftaran akun sumber daya terlindungi Anda dan coba tambahkan akun baru. Gunakan pasangan kredensi AWS WAF uji berikut dan masukkan tes apa pun

      - Pengguna: `WAF_TEST_CREDENTIAL@wafexample.com`
      - Kata Sandi: `WAF_TEST_CREDENTIAL_PASSWORD`

      Kredensi pengujian ini dikategorikan sebagai kredenal yang dikompromikan, dan grup aturan terkelola ACFP akan menambahkan `awswaf:managed:aws:acfp:signal:credential_compromised` label ke permintaan pembuatan akun, yang dapat Anda lihat di log.

   b. Di log ACL web Anda, cari `awswaf:managed:aws:acfp:signal:credential_compromised` label di `labels` bidang pada entri log untuk permintaan pembuatan akun pengujian Anda. Untuk informasi tentang pencatatan, lihatPencatatan AWS WAF lalu lintas ACL web.

Setelah memverifikasi bahwa grup aturan menangkap kredensional yang dikompromikan seperti yang diharapkan, Anda dapat mengambil langkah-langkah untuk mengonfigurasi implementasinya sesuai kebutuhan untuk sumber daya yang dilindungi.

7. Untuk CloudFront distribusi, uji pengelolaan grup aturan atas upaya pembuatan akun massal

   Jalankan pengujian ini untuk setiap kriteria respons sukses yang Anda konfigurasikan untuk grup aturan ACFP. Tunggu setidaknya 30 menit di antara tes.

   a. Untuk setiap kriteria keberhasilan Anda, identifikasi upaya pembuatan akun yang akan berhasil dengan kriteria keberhasilan tersebut sebagai tanggapan. Kemudian, dari satu sesi klien, lakukan setidaknya 5 upaya pembuatan akun yang berhasil dalam waktu kurang dari 30 menit. Seorang pengguna biasanya hanya akan membuat satu akun di situs Anda.

      Setelah pembuatan akun pertama yang berhasil, `VolumetricSessionSuccessfulResponse` aturan harus mulai cocok dengan respons pembuatan akun lainnya, memberi label dan menghitungnya, berdasarkan penggantian tindakan aturan Anda. Aturan mungkin melewatkan satu atau dua yang pertama karena latensi.

   b. Di log ACL web Anda, cari `awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_` label di `labels` bidang pada entri log untuk permintaan web pembuatan akun pengujian Anda. Untuk informasi tentang pencatatan, lihatPencatatan AWS WAF lalu lintas ACL web.

   Tes ini memverifikasi bahwa kriteria keberhasilan Anda sesuai dengan tanggapan Anda dengan memeriksa bahwa jumlah yang berhasil dikumpulkan oleh aturan melampaui ambang batas aturan. Setelah Anda mencapai ambang batas, jika Anda terus mengirim permintaan pembuatan akun dari sesi yang sama, aturan akan terus cocok hingga tingkat keberhasilan turun di bawah ambang batas. Meskipun ambang batas terlampaui, aturan tersebut cocok dengan upaya pembuatan akun yang berhasil atau gagal dari alamat sesi.

8. Sesuaikan penanganan permintaan web ACFP

   Jika diperlukan, tambahkan aturan Anda sendiri yang secara eksplisit mengizinkan atau memblokir permintaan, untuk mengubah cara aturan ACFP akan menanganinya.

   Misalnya, Anda dapat menggunakan label ACFP untuk mengizinkan atau memblokir permintaan atau untuk menyesuaikan penanganan permintaan. Anda dapat menambahkan aturan

pencocokan label setelah grup aturan terkelola ACFP untuk memfilter permintaan berlabel untuk penanganan yang ingin Anda terapkan. Setelah pengujian, pertahankan aturan ACFP terkait dalam mode hitungan, dan pertahankan keputusan penanganan permintaan dalam aturan kustom Anda. Sebagai contoh, lihat Contoh ACFP: Respons khusus untuk kredensil yang dikompromikan.

9. Hapus aturan pengujian Anda dan aktifkan pengaturan grup aturan terkelola ACFP

   Tergantung pada situasi Anda, Anda mungkin telah memutuskan bahwa Anda ingin meninggalkan beberapa aturan ACFP dalam mode hitungan. Untuk aturan yang ingin Anda jalankan seperti yang dikonfigurasi di dalam grup aturan, nonaktifkan mode hitungan dalam konfigurasi grup aturan ACL web. Setelah selesai menguji, Anda juga dapat menghapus aturan pencocokan label pengujian.

10. Memantau dan menyetel

    Untuk memastikan bahwa permintaan web ditangani seperti yang Anda inginkan, pantau lalu lintas Anda dengan cermat setelah Anda mengaktifkan fungsionalitas ACFP yang ingin Anda gunakan. Sesuaikan perilaku sesuai kebutuhan dengan penggantian hitungan aturan pada grup aturan dan dengan aturan Anda sendiri.

Setelah Anda selesai menguji implementasi grup aturan ACFP Anda, jika Anda belum mengintegrasikan AWS WAF JavaScript SDK ke halaman pendaftaran akun dan pembuatan akun browser Anda, kami sangat menyarankan Anda melakukannya. AWS WAF juga menyediakan SDK seluler untuk mengintegrasikan perangkat iOS dan Android. Untuk informasi selengkapnya tentang SDK integrasi, lihatAWS WAF integrasi aplikasi klien. Untuk informasi tentang rekomendasi ini, lihatMengapa Anda harus menggunakan SDK integrasi aplikasi dengan ACFP.

AWS WAF Contoh pencegahan penipuan pembuatan akun Kontrol Penipuan (ACFP)

Bagian ini menunjukkan contoh konfigurasi yang memenuhi kasus penggunaan umum untuk implementasi pencegahan AWS WAF penipuan pembuatan akun Kontrol Penipuan (ACFP).

Setiap contoh memberikan deskripsi kasus penggunaan dan kemudian menunjukkan solusi dalam daftar JSON untuk aturan yang dikonfigurasi khusus.

> **Note**
>
> Anda dapat mengambil daftar JSON seperti yang ditunjukkan dalam contoh ini melalui unduhan ACL JSON web konsol atau editor JSON aturan, atau melalui `getWebACL` operasi di API dan antarmuka baris perintah.

Topik

Contoh ACFP: Konfigurasi sederhana

Daftar JSON berikut menunjukkan contoh ACL web dengan grup aturan terkelola pencegahan AWS WAF penipuan pembuatan akun Kontrol Penipuan (ACFP). Perhatikan tambahan `CreationPath` dan `RegistrationPagePath` konfigurasi, bersama dengan jenis payload dan informasi yang diperlukan untuk menemukan informasi akun baru di payload, untuk memverifikasinya. Grup aturan menggunakan informasi ini untuk memantau dan mengelola permintaan pembuatan akun Anda. JSON ini mencakup pengaturan ACL web yang dihasilkan secara otomatis, seperti namespace label dan URL integrasi aplikasi ACL web.

```
{
  "Name": "simpleACFP",
  "Id": "... ",
  "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/simpleACFP/... ",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesACFPRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesACFPRuleSet",
          "ManagedRuleGroupConfigs": [
```

```
        {
          "AWSManagedRulesACFPRuleSet": {
            "CreationPath": "/web/signup/submit-registration",
            "RegistrationPagePath": "/web/signup/registration",
            "RequestInspection": {
              "PayloadType": "JSON",
              "UsernameField": {
                "Identifier": "/form/username"
              },
              "PasswordField": {
                "Identifier": "/form/password"
              },
              "EmailField": {
                "Identifier": "/form/email"
              },
              "PhoneNumberFields": [
                {
                  "Identifier": "/form/country-code"
                },
                {
                  "Identifier": "/form/region-code"
                },
                {
                  "Identifier": "/form/phonenumber"
                }
              ],
              "AddressFields": [
                {
                  "Identifier": "/form/name"
                },
                {
                  "Identifier": "/form/street-address"
                },
                {
                  "Identifier": "/form/city"
                },
                {
                  "Identifier": "/form/state"
                },
                {
                  "Identifier": "/form/zipcode"
                }
              ]
            },
```

```
                "EnableRegexInPath": false
              }
            }
          ]
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "simpleACFP"
  },
  "Capacity": 50,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:111122223333:webacl:simpleACFP:"
}
```

Contoh ACFP: Respons khusus untuk kredensil yang dikompromikan

Secara default, pemeriksaan kredensil yang dilakukan oleh grup aturan `AWSManagedRulesACFPRuleSet` menangani kredenal yang dikompromikan dengan memberi label permintaan dan memblokirnya. Untuk detail tentang kelompok aturan dan perilaku aturan, lihatAWS WAF Grup aturan pencegahan penipuan (ACFP) pembuatan akun Kontrol Penipuan.

Untuk memberi tahu pengguna bahwa kredensi akun yang mereka berikan telah disusupi, Anda dapat melakukan hal berikut:

- Ganti **`SignalCredentialCompromised`** aturan ke Count — Ini menyebabkan aturan hanya menghitung dan memberi label permintaan yang cocok.
- Tambahkan aturan pencocokan label dengan penanganan khusus — Konfigurasikan aturan ini agar sesuai dengan label ACFP dan untuk melakukan penanganan kustom Anda.

Daftar ACL web berikut menunjukkan grup aturan terkelola ACFP dari contoh sebelumnya, dengan tindakan `SignalCredentialCompromised` aturan diganti untuk dihitung. Dengan konfigurasi ini, ketika grup aturan ini mengevaluasi permintaan web apa pun yang menggunakan kredensi yang dikompromikan, ia akan memberi label permintaan, tetapi tidak memblokirnya.

Selain itu, web ACL sekarang memiliki respons khusus bernama `aws-waf-credential-compromised` dan aturan baru bernama`AccountSignupCompromisedCredentialsHandling`. Prioritas aturan adalah pengaturan numerik yang lebih tinggi daripada grup aturan, sehingga berjalan setelah grup aturan dalam evaluasi ACL web. Aturan baru cocok dengan permintaan apa pun dengan label kredensi grup aturan yang disusupi. Saat aturan menemukan kecocokan, aturan tersebut menerapkan Block tindakan ke permintaan dengan badan respons khusus. Badan respons khusus memberikan informasi kepada pengguna akhir bahwa kredensialnya telah dikompromikan dan mengusulkan tindakan untuk diambil.

```
{
  "Name": "compromisedCreds",
  "Id": "... ",
  "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/compromisedCreds/...",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesACFPRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesACFPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesACFPRuleSet": {
                "CreationPath": "/web/signup/submit-registration",
                "RegistrationPagePath": "/web/signup/registration",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
                  "PasswordField": {
                    "Identifier": "/form/password"
```

```
            },
            "EmailField": {
              "Identifier": "/form/email"
            },
            "PhoneNumberFields": [
              {
                "Identifier": "/form/country-code"
              },
              {
                "Identifier": "/form/region-code"
              },
              {
                "Identifier": "/form/phonenumber"
              }
            ],
            "AddressFields": [
              {
                "Identifier": "/form/name"
              },
              {
                "Identifier": "/form/street-address"
              },
              {
                "Identifier": "/form/city"
              },
              {
                "Identifier": "/form/state"
              },
              {
                "Identifier": "/form/zipcode"
              }
            ]
          },
          "EnableRegexInPath": false
        }
      }
    ],
    "RuleActionOverrides": [
      {
        "Name": "SignalCredentialCompromised",
        "ActionToUse": {
          "Count": {}
        }
      }
```

```
          ]
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
      }
    },
    {
      "Name": "AccountSignupCompromisedCredentialsHandling",
      "Priority": 1,
      "Statement": {
        "LabelMatchStatement": {
          "Scope": "LABEL",
          "Key": "awswaf:managed:aws:acfp:signal:credential_compromised"
        }
      },
      "Action": {
        "Block": {
          "CustomResponse": {
            "ResponseCode": 406,
            "CustomResponseBodyKey": "aws-waf-credential-compromised",
            "ResponseHeaders": [
              {
                "Name": "aws-waf-credential-compromised",
                "Value": "true"
              }
            ]
          }
        }
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AccountSignupCompromisedCredentialsHandling"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
```

```
    "CloudWatchMetricsEnabled": true,
    "MetricName": "compromisedCreds"
  },
  "Capacity": 51,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:111122223333:webacl:compromisedCreds:",
  "CustomResponseBodies": {
    "aws-waf-credential-compromised": {
      "ContentType": "APPLICATION_JSON",
      "Content": "{\n  \"credentials-compromised\": \"The credentials you provided have
 been found in a compromised credentials database.\\n\\nTry again with a different
 username, password pair.\"\n}"
    }
  }
}
```

Contoh ACFP: Konfigurasi inspeksi respons

Daftar JSON berikut menunjukkan contoh ACL web dengan grup aturan terkelola pencegahan AWS WAF penipuan pembuatan akun Kontrol Penipuan (ACFP) yang dikonfigurasi untuk memeriksa tanggapan asal. Perhatikan konfigurasi inspeksi respons, yang menentukan kode status keberhasilan dan respons. Anda juga dapat mengonfigurasi pengaturan keberhasilan dan respons berdasarkan kecocokan JSON header, body, dan body. JSON ini mencakup pengaturan ACL web yang dihasilkan secara otomatis, seperti namespace label dan URL integrasi aplikasi ACL web.

> **Note**
>
> Pemeriksaan respons ATP hanya tersedia di ACL web yang melindungi CloudFront distribusi.

```
{
  "Name": "simpleACFP",
  "Id": "... ",
  "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/simpleACFP/... ",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesACFPRuleSet",
      "Priority": 0,
```

```
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesACFPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesACFPRuleSet": {
                "CreationPath": "/web/signup/submit-registration",
                "RegistrationPagePath": "/web/signup/registration",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
                  "PasswordField": {
                    "Identifier": "/form/password"
                  },
                  "EmailField": {
                    "Identifier": "/form/email"
                  },
                  "PhoneNumberFields": [
                    {
                      "Identifier": "/form/country-code"
                    },
                    {
                      "Identifier": "/form/region-code"
                    },
                    {
                      "Identifier": "/form/phonenumber"
                    }
                  ],
                  "AddressFields": [
                    {
                      "Identifier": "/form/name"
                    },
                    {
                      "Identifier": "/form/street-address"
                    },
                    {
                      "Identifier": "/form/city"
                    },
                    {
                      "Identifier": "/form/state"
                    },
```

```
                {
                  "Identifier": "/form/zipcode"
                }
              ]
            },
            "ResponseInspection": {
              "StatusCode": {
                "SuccessCodes": [
                  200
                ],
                "FailureCodes": [
                  401
                ]
              }
            },
            "EnableRegexInPath": false
          }
        }
      ]
    }
  },
  "OverrideAction": {
    "None": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
  }
 }
],
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "simpleACFP"
},
"Capacity": 50,
"ManagedByFirewallManager": false,
"LabelNamespace": "awswaf:111122223333:webacl:simpleACFP:"
}
```

AWS WAF Pencegahan pengambilalihan akun Kontrol Penipuan (ATP)

Pengambilalihan akun adalah aktivitas ilegal online di mana penyerang mendapatkan akses tidak sah ke akun seseorang. Penyerang mungkin melakukan ini dalam beberapa cara, seperti menggunakan kredensi curian atau menebak kata sandi korban melalui serangkaian upaya. Ketika penyerang mendapatkan akses, mereka mungkin mencuri uang, informasi, atau layanan dari korban. Penyerang mungkin berpose sebagai korban untuk mendapatkan akses ke akun lain yang dimiliki korban, atau untuk mendapatkan akses ke akun orang atau organisasi lain. Selain itu, mereka mungkin mencoba mengubah kata sandi pengguna untuk memblokir korban dari akun mereka sendiri.

Anda dapat memantau dan mengontrol upaya pengambilalihan akun dengan menerapkan fitur Pencegahan Pengambilalihan Akun Kontrol AWS WAF Penipuan (ATP). AWS WAF menawarkan fitur ini di grup aturan Aturan AWS Terkelola `AWSManagedRulesATPRuleSet` dan SDK integrasi aplikasi pendamping.

Grup aturan terkelola ATP memberi label dan mengelola permintaan yang mungkin merupakan bagian dari upaya pengambilalihan akun berbahaya. Grup aturan melakukan ini dengan memeriksa upaya login yang dikirim klien ke titik akhir login aplikasi Anda.

- Inspeksi permintaan — ATP memberi Anda visibilitas dan kontrol atas upaya login anomali dan upaya login yang menggunakan kredensi curian, untuk mencegah pengambilalihan akun yang dapat menyebabkan aktivitas penipuan. ATP memeriksa kombinasi email dan kata sandi terhadap basis data kredensialnya yang dicuri, yang diperbarui secara berkala karena kredensi baru yang bocor ditemukan di web gelap. ATP mengumpulkan data berdasarkan alamat IP dan sesi klien, untuk mendeteksi dan memblokir klien yang mengirim terlalu banyak permintaan yang bersifat mencurigakan.
- Inspeksi respons — Untuk CloudFront distribusi, selain memeriksa permintaan masuk masuk, grup aturan ATP memeriksa respons aplikasi Anda terhadap upaya login, untuk melacak tingkat keberhasilan dan kegagalan. Dengan menggunakan informasi ini, ATP dapat memblokir sementara sesi klien atau alamat IP yang memiliki terlalu banyak kegagalan login. AWS WAF melakukan inspeksi respons secara asinkron, jadi ini tidak meningkatkan latensi dalam lalu lintas web Anda.

> **Note**
>
> Anda akan dikenakan biaya tambahan saat menggunakan grup aturan terkelola ini. Untuk informasi selengkapnya, silakan lihat Harga AWS WAF.

> **Note**
>
> Fitur ATP tidak tersedia untuk kumpulan pengguna Amazon Cognito.

Topik

AWS WAF Komponen ATP

Komponen utama pencegahan pengambilalihan akun Kontrol AWS WAF Penipuan (ATP) adalah sebagai berikut:

- **`AWSManagedRulesATPRuleSet`**— Aturan dalam grup aturan Aturan AWS Terkelola ini mendeteksi, memberi label, dan menangani berbagai jenis aktivitas pengambilalihan akun. Grup aturan memeriksa permintaan `POST` web HTTP yang dikirim klien ke titik akhir login yang ditentukan. Untuk CloudFront distribusi yang dilindungi, grup aturan juga memeriksa respons yang dikirim distribusi kembali ke permintaan ini. Untuk daftar aturan grup aturan, lihatAWS WAF Kelompok aturan pencegahan pengambilalihan akun Kontrol Penipuan (ATP). Anda menyertakan grup aturan ini di ACL web Anda menggunakan pernyataan referensi grup aturan terkelola. Untuk informasi tentang menggunakan grup aturan ini, lihatMenambahkan grup aturan terkelola ATP ke ACL web Anda.

  > **Note**
  >
  > Anda akan dikenakan biaya tambahan saat menggunakan grup aturan terkelola ini. Untuk informasi selengkapnya, silakan lihat Harga AWS WAF.

- Detail tentang halaman login aplikasi Anda — Anda harus memberikan informasi tentang halaman login Anda ketika Anda menambahkan grup `AWSManagedRulesATPRuleSet` aturan ke ACL web Anda. Ini memungkinkan grup aturan mempersempit cakupan permintaan yang diperiksa dan memvalidasi penggunaan kredensil dengan benar dalam permintaan web. Grup aturan ATP

bekerja dengan nama pengguna yang dalam format email. Untuk informasi selengkapnya, lihat Menambahkan grup aturan terkelola ATP ke ACL web Anda.

- Untuk CloudFront distribusi yang dilindungi, detail tentang bagaimana aplikasi Anda merespons upaya login — Anda memberikan detail tentang tanggapan aplikasi Anda terhadap upaya login, dan grup aturan melacak dan mengelola klien yang mengirim terlalu banyak upaya login yang gagal. Untuk informasi tentang mengonfigurasi opsi ini, lihatMenambahkan grup aturan terkelola ATP ke ACL web Anda.
- JavaScript dan SDK integrasi aplikasi seluler — Terapkan SDK AWS WAF JavaScript dan seluler dengan implementasi ATP Anda untuk mengaktifkan rangkaian lengkap kemampuan yang ditawarkan grup aturan. Banyak aturan ATP menggunakan informasi yang disediakan oleh SDK untuk verifikasi klien tingkat sesi dan agregasi perilaku, yang diperlukan untuk memisahkan lalu lintas klien yang sah dari lalu lintas bot. Untuk informasi selengkapnya tentang SDK, lihat AWS WAF integrasi aplikasi klien.

Anda dapat menggabungkan implementasi ATP Anda dengan yang berikut ini untuk membantu Anda memantau, menyetel, dan menyesuaikan perlindungan Anda.

- Logging dan metrik — Anda dapat memantau lalu lintas, dan memahami bagaimana grup aturan terkelola ACFP memengaruhi hal itu, dengan mengonfigurasi dan mengaktifkan log, pengumpulan data Amazon Security Lake, dan metrik CloudWatch Amazon untuk ACL web Anda. Label yang `AWSManagedRulesATPRuleSet` menambah permintaan web Anda disertakan dalam data. Untuk informasi tentang opsi, lihat, Pencatatan AWS WAF lalu lintas ACL webPemantauan CloudWatch dengan Amazon, dan Apa itu Amazon Security Lake? .

  Tergantung pada kebutuhan Anda dan lalu lintas yang Anda lihat, Anda mungkin ingin menyesuaikan `AWSManagedRulesATPRuleSet` implementasi Anda. Misalnya, Anda mungkin ingin mengecualikan beberapa lalu lintas dari evaluasi ATP, atau Anda mungkin ingin mengubah cara menangani beberapa upaya pengambilalihan akun yang diidentifikasi, menggunakan AWS WAF fitur seperti pernyataan cakupan bawah atau aturan pencocokan label.
- Aturan pencocokan label dan label — Untuk salah satu aturan di`AWSManagedRulesATPRuleSet`, Anda dapat mengubah perilaku pemblokiran untuk menghitung, lalu mencocokkan dengan label yang ditambahkan oleh aturan. Gunakan pendekatan ini untuk menyesuaikan cara Anda menangani permintaan web yang diidentifikasi oleh grup aturan terkelola ATP. Untuk informasi selengkapnya tentang pelabelan dan penggunaan pernyataan pencocokan label, lihat Pernyataan aturan pencocokan label danAWS WAF label pada permintaan web.

- Permintaan dan tanggapan khusus - Anda dapat menambahkan header khusus ke permintaan yang Anda izinkan dan Anda dapat mengirim tanggapan khusus untuk permintaan yang Anda blokir. Untuk melakukan ini, Anda memasangkan label yang cocok dengan permintaan AWS WAF kustom dan fitur respons. Untuk informasi selengkapnya tentang menyesuaikan permintaan dan tanggapan, lihatPermintaan dan tanggapan web yang disesuaikan di AWS WAF.

Mengapa Anda harus menggunakan SDK integrasi aplikasi dengan ATP

Grup aturan terkelola ATP memerlukan token tantangan yang dihasilkan oleh SDK integrasi aplikasi. Token memungkinkan set lengkap perlindungan yang ditawarkan grup aturan.

Kami sangat menyarankan untuk menerapkan SDK integrasi aplikasi, untuk penggunaan grup aturan ATP yang paling efektif. Skrip tantangan harus dijalankan sebelum grup aturan ATP agar grup aturan mendapat manfaat dari token yang diperoleh skrip. Ini terjadi secara otomatis dengan SDK integrasi aplikasi. Jika Anda tidak dapat menggunakan SDK, Anda dapat mengkonfigurasi ACL web secara bergantian sehingga menjalankan tindakan CAPTCHA aturan Challenge atau terhadap semua permintaan yang akan diperiksa oleh grup aturan ATP. Menggunakan tindakan Challenge atau CAPTCHA aturan dapat dikenakan biaya tambahan. Untuk detail harga, lihat AWS WAF Harga.

Kemampuan grup aturan ATP yang tidak memerlukan token

Ketika permintaan web tidak memiliki token, grup aturan terkelola ATP mampu memblokir jenis lalu lintas berikut:

- Alamat IP tunggal yang membuat banyak permintaan login.
- Alamat IP tunggal yang membuat banyak permintaan login gagal dalam waktu singkat.
- Login mencoba dengan traversal kata sandi, menggunakan nama pengguna yang sama tetapi mengubah kata sandi.

Kemampuan grup aturan ATP yang membutuhkan token

Informasi yang diberikan dalam token tantangan memperluas kemampuan grup aturan dan keamanan aplikasi klien Anda secara keseluruhan.

Token menyediakan informasi klien dengan setiap permintaan web yang memungkinkan grup aturan ATP untuk memisahkan sesi klien yang sah dari sesi klien yang berperilaku buruk, bahkan ketika keduanya berasal dari satu alamat IP. Grup aturan menggunakan informasi dalam token untuk menggabungkan perilaku permintaan sesi klien untuk deteksi dan mitigasi yang disetel dengan baik.

Ketika token tersedia dalam permintaan web, grup aturan ATP dapat mendeteksi dan memblokir kategori klien tambahan berikut di tingkat sesi:

- Sesi klien yang gagal dalam tantangan diam yang dikelola SDK.
- Sesi klien yang melintasi nama pengguna atau kata sandi. Ini juga dikenal sebagai isian kredenal.
- Sesi klien yang berulang kali menggunakan kredensil curian untuk masuk.
- Sesi klien yang menghabiskan waktu lama mencoba masuk.
- Sesi klien yang membuat banyak permintaan login. Grup aturan ATP menyediakan isolasi klien yang lebih baik daripada aturan AWS WAF berbasis tarif, yang dapat memblokir klien berdasarkan alamat IP. Kelompok aturan ATP juga menggunakan ambang batas yang lebih rendah.
- Sesi klien yang membuat banyak permintaan login gagal dalam waktu singkat. Fungsionalitas ini tersedia untuk CloudFront distribusi Amazon yang dilindungi.

Untuk informasi selengkapnya tentang kemampuan grup aturan, lihatAWS WAF Kelompok aturan pencegahan pengambilalihan akun Kontrol Penipuan (ATP).

Untuk informasi tentang SDK, lihatAWS WAF integrasi aplikasi klien. Untuk informasi tentang AWS WAF token, lihatAWS WAF token permintaan web. Untuk informasi tentang tindakan aturan, lihatCAPTCHAdan Challenge di AWS WAF.

Menambahkan grup aturan terkelola ATP ke ACL web Anda

Untuk mengonfigurasi grup aturan terkelola ATP untuk mengenali aktivitas pengambilalihan akun di lalu lintas web Anda, Anda memberikan informasi tentang cara klien mengirim permintaan login ke aplikasi Anda. Untuk CloudFront distribusi Amazon yang dilindungi, Anda juga memberikan informasi tentang bagaimana aplikasi Anda merespons permintaan login. Konfigurasi ini merupakan tambahan dari konfigurasi normal untuk grup aturan terkelola.

Untuk deskripsi grup aturan dan daftar aturan, lihatAWS WAF Kelompok aturan pencegahan pengambilalihan akun Kontrol Penipuan (ATP).

> **Note**
>
> Database kredensyal yang dicuri ATP hanya berisi nama pengguna dalam format email.

Panduan ini ditujukan untuk pengguna yang tahu secara umum cara membuat dan mengelola ACL AWS WAF web, aturan, dan grup aturan. Topik-topik tersebut dibahas di bagian sebelumnya dari

panduan ini. Untuk informasi dasar tentang cara menambahkan grup aturan terkelola ke ACL web Anda, lihatMenambahkan grup aturan terkelola ke ACL web melalui konsol.

Ikuti praktik terbaik

Gunakan kelompok aturan ATP sesuai dengan praktik terbaik diPraktik terbaik untuk mitigasi ancaman cerdas.

Untuk menggunakan grup **`AWSManagedRulesATPRuleSet`** aturan di ACL web Anda

1. Tambahkan grup aturan AWS terkelola, `AWSManagedRulesATPRuleSet` ke ACL web Anda, dan Edit pengaturan grup aturan sebelum menyimpan.

   > **Note**
   >
   > Anda akan dikenakan biaya tambahan saat menggunakan grup aturan terkelola ini. Untuk informasi selengkapnya, silakan lihat Harga AWS WAF.

2. Di panel konfigurasi grup Aturan, berikan informasi yang digunakan grup aturan ATP untuk memeriksa permintaan login.

   a. Untuk Gunakan ekspresi reguler di jalur, aktifkan ini jika Anda ingin AWS WAF melakukan pencocokan ekspresi reguler untuk spesifikasi jalur halaman login Anda.

      AWS WAF mendukung sintaks pola yang digunakan oleh pustaka PCRE `libpcre` dengan beberapa pengecualian. Pustaka didokumentasikan di PCRE - Perl Compatible Regular Expressions. Untuk informasi tentang AWS WAF dukungan, lihatPencocokan pola ekspresi reguler di AWS WAF.

   b. Untuk jalur Login, berikan jalur titik akhir login untuk aplikasi Anda. Grup aturan hanya memeriksa `POST` permintaan HTTP ke titik akhir login yang Anda tentukan.

      > **Note**
      >
      > Pencocokan untuk titik akhir tidak peka huruf besar/kecil. Spesifikasi Regex tidak boleh berisi bendera, yang menonaktifkan pencocokan yang tidak `(?-i)` peka huruf besar/kecil. Spesifikasi string harus dimulai dengan garis miring `/` ke depan.

Misalnya, untuk URL`https://example.com/web/login`, Anda dapat memberikan spesifikasi jalur string`/web/login`. Jalur masuk yang dimulai dengan jalur yang Anda berikan dianggap cocok. Misalnya `/web/login` cocok dengan jalur login`/web/login`,`/web/login/`,`/web/loginPage`, dan`/web/login/thisPage`, tetapi tidak cocok dengan jalur login `/home/web/login` atau`/website/login`.

c. Untuk pemeriksaan Permintaan, tentukan bagaimana aplikasi Anda menerima upaya login dengan memberikan jenis payload permintaan dan nama bidang dalam badan permintaan tempat nama pengguna dan kata sandi disediakan. Spesifikasi nama bidang Anda tergantung pada jenis payload.

   - Jenis payload JSON - Tentukan nama bidang dalam sintaks penunjuk JSON. Untuk informasi tentang sintaks JSON Pointer, lihat dokumentasi Internet Engineering Task Force (IETF) JavaScriptObject Notation (JSON) Pointer.

     Misalnya, untuk contoh payload JSON berikut, spesifikasi bidang nama pengguna adalah `/login/username` dan spesifikasi bidang kata sandi adalah. `/login/password`

     ```
     {
         "login": {
             "username": "THE_USERNAME",
             "password": "THE_PASSWORD"
         }
     }
     ```

   - Jenis payload FORM_ENCODED - Gunakan nama formulir HTML.

     Misalnya, untuk formulir HTML dengan elemen masukan bernama `username1` dan`password1`, spesifikasi bidang nama pengguna adalah `username1` dan spesifikasi bidang kata sandi adalah`password1`.

d. Jika Anda melindungi CloudFront distribusi Amazon, maka di bawah pemeriksaan Response, tentukan bagaimana aplikasi Anda menunjukkan keberhasilan atau kegagalan dalam tanggapannya terhadap upaya login.

> **Note**
>
> Pemeriksaan respons ATP hanya tersedia di ACL web yang melindungi CloudFront distribusi.

Tentukan satu komponen dalam respons login yang Anda ingin ATP periksa. Untuk tipe komponen Body dan JSON, AWS WAF dapat memeriksa 65.536 byte pertama (64 KB) komponen.

Berikan kriteria inspeksi Anda untuk jenis komponen, seperti yang ditunjukkan oleh antarmuka. Anda harus memberikan kriteria keberhasilan dan kegagalan untuk diperiksa dalam komponen.

Misalnya, aplikasi Anda menunjukkan status upaya login dalam kode status respons, dan digunakan `200 OK` untuk sukses dan `401 Unauthorized` atau `403 Forbidden` untuk kegagalan. Anda akan mengatur pemeriksaan respons Jenis komponen ke kode Status, lalu di kotak teks Sukses masukkan `200` dan di kotak teks Kegagalan, masukkan `401` pada baris pertama dan `403` pada baris kedua.

Kelompok aturan ATP hanya menghitung respons yang sesuai dengan kriteria pemeriksaan keberhasilan atau kegagalan Anda. Aturan kelompok aturan bertindak pada klien sementara mereka memiliki tingkat kegagalan yang terlalu tinggi di antara tanggapan yang dihitung. Untuk perilaku yang akurat menurut aturan grup aturan, pastikan untuk memberikan informasi lengkap untuk upaya login yang berhasil dan gagal.

Untuk melihat aturan yang memeriksa respons login, cari `VolumetricIpFailedLoginResponseHigh` dan `VolumetricSessionFailedLoginResponseHigh` di daftar aturan di[AWS WAF Kelompok aturan pencegahan pengambilalihan akun Kontrol Penipuan (ATP)].

3. Berikan konfigurasi tambahan apa pun yang Anda inginkan untuk grup aturan.

   Anda dapat membatasi cakupan permintaan yang diperiksa oleh grup aturan dengan menambahkan pernyataan cakupan bawah ke pernyataan grup aturan terkelola. Misalnya, Anda hanya dapat memeriksa permintaan dengan argumen kueri atau cookie tertentu. Grup aturan hanya akan memeriksa `POST` permintaan HTTP ke titik akhir login yang Anda tentukan yang cocok dengan kriteria dalam pernyataan cakupan bawah Anda. Untuk informasi tentang pernyataan cakupan bawah, lihat. [Pernyataan cakupan ke bawah]

4. Simpan perubahan Anda ke ACL web.

Sebelum Anda menerapkan implementasi ATP Anda untuk lalu lintas produksi, uji dan sesuaikan di lingkungan pementasan atau pengujian hingga Anda merasa nyaman dengan potensi dampak

terhadap lalu lintas Anda. Kemudian uji dan atur aturan dalam mode hitungan dengan lalu lintas produksi Anda sebelum mengaktifkannya. Lihat bagian berikut untuk panduan.

Menguji dan menerapkan ATP

Bagian ini memberikan panduan umum untuk mengonfigurasi dan menguji implementasi pencegahan pengambilalihan akun Kontrol AWS WAF Penipuan (ATP) untuk situs Anda. Langkah-langkah spesifik yang Anda pilih untuk diikuti akan tergantung pada kebutuhan, sumber daya, dan permintaan web yang Anda terima.

Informasi ini merupakan tambahan dari informasi umum tentang pengujian dan penyetelan yang disediakan di[Menguji dan menyetel perlindungan Anda AWS WAF](#).

> **Note**
>
> AWS Aturan Terkelola dirancang untuk melindungi Anda dari ancaman web umum. Bila digunakan sesuai dengan dokumentasi, grup aturan Aturan AWS Terkelola menambahkan lapisan keamanan lain untuk aplikasi Anda. Namun, grup aturan Aturan AWS Terkelola tidak dimaksudkan sebagai pengganti tanggung jawab keamanan Anda, yang ditentukan oleh AWS sumber daya yang Anda pilih. Lihat Model Tanggung Jawab Bersama untuk memastikan bahwa sumber daya Anda AWS dilindungi dengan benar.

> **Risiko lalu lintas produksi**
>
> Sebelum Anda menerapkan implementasi ATP Anda untuk lalu lintas produksi, uji dan sesuaikan di lingkungan pementasan atau pengujian hingga Anda merasa nyaman dengan dampak potensial terhadap lalu lintas Anda. Kemudian uji dan atur aturan dalam mode hitungan dengan lalu lintas produksi Anda sebelum mengaktifkannya.

AWS WAF menyediakan kredensyal pengujian yang dapat Anda gunakan untuk memverifikasi konfigurasi ATP Anda. Dalam prosedur berikut, Anda akan mengonfigurasi ACL web uji untuk menggunakan grup aturan terkelola ATP, mengonfigurasi aturan untuk menangkap label yang ditambahkan oleh grup aturan, dan kemudian menjalankan upaya masuk menggunakan kredenal pengujian ini. Anda akan memverifikasi bahwa ACL web Anda telah mengelola upaya dengan benar dengan memeriksa CloudWatch metrik Amazon untuk upaya login.

Panduan ini ditujukan untuk pengguna yang tahu secara umum cara membuat dan mengelola ACL AWS WAF web, aturan, dan grup aturan. Topik-topik tersebut dibahas di bagian sebelumnya dari panduan ini.

Untuk mengonfigurasi dan menguji implementasi pencegahan pengambilalihan akun Kontrol AWS WAF Penipuan (ATP)

Lakukan langkah-langkah ini terlebih dahulu di lingkungan pengujian, kemudian dalam produksi.

1. Tambahkan grup aturan terkelola pencegahan pengambilalihan akun Kontrol AWS WAF Penipuan (ATP) dalam mode hitung

   > **Note**
   >
   > Anda akan dikenakan biaya tambahan saat menggunakan grup aturan terkelola ini. Untuk informasi selengkapnya, silakan lihat Harga AWS WAF.

   Tambahkan grup aturan Aturan AWS Terkelola `AWSManagedRulesATPRuleSet` ke ACL web baru atau yang sudah ada dan konfigurasikan agar tidak mengubah perilaku ACL web saat ini. Untuk detail tentang aturan dan label untuk grup aturan ini, lihatAWS WAF Kelompok aturan pencegahan pengambilalihan akun Kontrol Penipuan (ATP).

   - Saat Anda menambahkan grup aturan terkelola, edit dan lakukan hal berikut:
     - Di panel konfigurasi grup Aturan, berikan detail halaman login aplikasi Anda. Grup aturan ATP menggunakan informasi ini untuk memantau aktivitas masuk. Untuk informasi selengkapnya, lihat Menambahkan grup aturan terkelola ATP ke ACL web Anda.
     - Di panel Aturan, buka dropdown Override all rule actions dan pilih. Count Dengan konfigurasi ini, AWS WAF mengevaluasi permintaan terhadap semua aturan dalam grup aturan dan hanya menghitung kecocokan yang dihasilkan, sambil tetap menambahkan label ke permintaan. Untuk informasi selengkapnya, lihat Mengesampingkan tindakan aturan dalam grup aturan.

       Dengan penggantian ini, Anda dapat memantau dampak potensial dari aturan terkelola ATP untuk menentukan apakah Anda ingin menambahkan pengecualian, seperti pengecualian untuk kasus penggunaan internal.
   - Posisikan grup aturan sehingga dievaluasi setelah aturan yang ada di ACL web, dengan pengaturan prioritas yang secara numerik lebih tinggi daripada aturan atau grup aturan apa

pun yang sudah Anda gunakan. Untuk informasi selengkapnya, lihat Memproses urutan aturan dan kelompok aturan dalam ACL web.

Dengan cara ini, penanganan lalu lintas Anda saat ini tidak terganggu. Misalnya, jika Anda memiliki aturan yang mendeteksi lalu lintas berbahaya seperti injeksi SQL atau skrip lintas situs, mereka akan terus mendeteksi dan mencatatnya. Sebagai alternatif, jika Anda memiliki aturan yang memungkinkan lalu lintas non-berbahaya yang diketahui, mereka dapat terus mengizinkan lalu lintas itu, tanpa diblokir oleh grup aturan yang dikelola ATP. Anda mungkin memutuskan untuk menyesuaikan urutan pemrosesan selama aktivitas pengujian dan penyetelan Anda.

2. Aktifkan pencatatan dan metrik untuk ACL web

   Jika diperlukan, konfigurasikan pencatatan, pengumpulan data Amazon Security Lake, pengambilan sampel permintaan, dan CloudWatch metrik Amazon untuk ACL web. Anda dapat menggunakan alat visibilitas ini untuk memantau interaksi grup aturan terkelola ATP dengan lalu lintas Anda.

   - Untuk informasi tentang mengonfigurasi dan menggunakan logging, lihatPencatatan AWS WAF lalu lintas ACL web.
   - Untuk informasi tentang Amazon Security Lake, lihat Apa itu Amazon Security Lake? dan Mengumpulkan data dari AWS layanan di panduan pengguna Amazon Security Lake.
   - Untuk informasi tentang CloudWatch metrik Amazon, lihatPemantauan CloudWatch dengan Amazon.
   - Untuk informasi tentang pengambilan sampel permintaan web, lihatMelihat contoh permintaan web.

3. Kaitkan ACL web dengan sumber daya

   Jika ACL web belum dikaitkan dengan sumber daya pengujian, kaitkan. Untuk informasi, lihat Mengaitkan atau memisahkan ACL web dengan sumber daya AWS.

4. Pantau lalu lintas dan kecocokan aturan ATP

   Pastikan lalu lintas normal Anda mengalir dan aturan grup aturan terkelola ATP menambahkan label ke permintaan web yang cocok. Anda dapat melihat label di log dan melihat ATP dan metrik label di metrik Amazon CloudWatch . Di log, aturan yang telah Anda ganti untuk dihitung dalam grup aturan muncul di `action` set to count, dan `ruleGroupList` dengan `overriddenAction` menunjukkan tindakan aturan yang dikonfigurasi yang Anda timpa.

5. Uji kemampuan pemeriksaan kredensi grup aturan

   Lakukan upaya login dengan menguji kredensyal yang dikompromikan dan periksa apakah grup aturan cocok dengan mereka seperti yang diharapkan.

   a. Masuk ke halaman login sumber daya yang dilindungi menggunakan pasangan kredensi AWS WAF pengujian berikut:

      - Pengguna: `WAF_TEST_CREDENTIAL@wafexample.com`
      - Kata Sandi: `WAF_TEST_CREDENTIAL_PASSWORD`

      Kredensi pengujian ini dikategorikan sebagai kredenal yang dikompromikan, dan grup aturan terkelola ATP akan menambahkan `awswaf:managed:aws:atp:signal:credential_compromised` label ke permintaan login, yang dapat Anda lihat di log.

   b. Di log ACL web Anda, cari `awswaf:managed:aws:atp:signal:credential_compromised` label di `labels` bidang pada entri log untuk permintaan web login pengujian Anda. Untuk informasi tentang pencatatan, lihatPencatatan AWS WAF lalu lintas ACL web.

   Setelah memverifikasi bahwa grup aturan menangkap kredensional yang dikompromikan seperti yang diharapkan, Anda dapat mengambil langkah-langkah untuk mengonfigurasi implementasinya sesuai kebutuhan untuk sumber daya yang dilindungi.

6. Untuk CloudFront distribusi, uji manajemen kegagalan login grup aturan

   a. Jalankan pengujian untuk setiap kriteria respons kegagalan yang Anda konfigurasikan untuk grup aturan ATP. Tunggu setidaknya 10 menit di antara tes.

      Untuk menguji kriteria kegagalan tunggal, identifikasi upaya login yang akan gagal dengan kriteria tersebut dalam respons. Kemudian, dari satu alamat IP klien, lakukan setidaknya 10 upaya login yang gagal dalam waktu kurang dari 10 menit.

      Setelah 6 kegagalan pertama, aturan login volumetrik yang gagal akan mulai cocok dengan sisa upaya Anda, memberi label dan menghitungnya. Aturan mungkin melewatkan satu atau dua yang pertama karena latensi.

b. Di log ACL web Anda, cari `awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:high` label di `labels` bidang pada entri log untuk permintaan web login pengujian Anda. Untuk informasi tentang pencatatan, lihatPencatatan AWS WAF lalu lintas ACL web.

Pengujian ini memverifikasi bahwa kriteria kegagalan Anda cocok dengan tanggapan Anda dengan memeriksa bahwa jumlah login yang gagal melampaui ambang batas aturan. `VolumetricIpFailedLoginResponseHigh` Setelah Anda mencapai ambang batas, jika Anda terus mengirim permintaan login dari alamat IP yang sama, aturan akan terus cocok hingga tingkat kegagalan turun di bawah ambang batas. Sementara ambang batas terlampaui, aturan cocok dengan login yang berhasil atau gagal dari alamat IP.

7. Kustomisasi penanganan permintaan web ATP

   Jika diperlukan, tambahkan aturan Anda sendiri yang secara eksplisit mengizinkan atau memblokir permintaan, untuk mengubah cara aturan ATP akan menanganinya.

   Misalnya, Anda dapat menggunakan label ATP untuk mengizinkan atau memblokir permintaan atau untuk menyesuaikan penanganan permintaan. Anda dapat menambahkan aturan pencocokan label setelah grup aturan terkelola ATP untuk memfilter permintaan berlabel untuk penanganan yang ingin Anda terapkan. Setelah pengujian, pertahankan aturan ATP terkait dalam mode hitungan, dan pertahankan keputusan penanganan permintaan dalam aturan kustom Anda. Sebagai contoh, lihat Contoh ATP: Penanganan khusus untuk kredensi yang hilang dan dikompromikan.

8. Hapus aturan pengujian Anda dan aktifkan pengaturan grup aturan terkelola ATP

   Tergantung pada situasi Anda, Anda mungkin telah memutuskan bahwa Anda ingin meninggalkan beberapa aturan ATP dalam mode hitungan. Untuk aturan yang ingin Anda jalankan seperti yang dikonfigurasi di dalam grup aturan, nonaktifkan mode hitungan dalam konfigurasi grup aturan ACL web. Setelah selesai menguji, Anda juga dapat menghapus aturan pencocokan label pengujian.

9. Memantau dan menyetel

   Untuk memastikan bahwa permintaan web ditangani seperti yang Anda inginkan, pantau lalu lintas Anda dengan cermat setelah Anda mengaktifkan fungsionalitas ATP yang ingin Anda gunakan. Sesuaikan perilaku sesuai kebutuhan dengan penggantian hitungan aturan pada grup aturan dan dengan aturan Anda sendiri.

Setelah Anda selesai menguji implementasi grup aturan ATP, jika Anda belum melakukannya, kami sangat menyarankan Anda mengintegrasikan AWS WAF JavaScript SDK ke halaman login browser Anda, untuk meningkatkan kemampuan deteksi. AWS WAF juga menyediakan SDK seluler untuk mengintegrasikan perangkat iOS dan Android. Untuk informasi selengkapnya tentang SDK integrasi, lihatAWS WAF integrasi aplikasi klien. Untuk informasi tentang rekomendasi ini, lihatMengapa Anda harus menggunakan SDK integrasi aplikasi dengan ATP.

AWS WAF Contoh pencegahan pengambilalihan akun Kontrol Penipuan (ATP)

Bagian ini menunjukkan contoh konfigurasi yang memenuhi kasus penggunaan umum untuk implementasi pencegahan pengambilalihan akun Kontrol AWS WAF Penipuan (ATP).

Setiap contoh memberikan deskripsi kasus penggunaan dan kemudian menunjukkan solusi dalam daftar JSON untuk aturan yang dikonfigurasi khusus.

> **Note**
>
> Anda dapat mengambil daftar JSON seperti yang ditunjukkan dalam contoh ini melalui unduhan ACL JSON web konsol atau editor JSON aturan, atau melalui `getWebACL` operasi di API dan antarmuka baris perintah.

Topik

- Contoh ATP: Konfigurasi sederhana
- Contoh ATP: Penanganan khusus untuk kredensi yang hilang dan dikompromikan
- Contoh ATP: Konfigurasi inspeksi respons

Contoh ATP: Konfigurasi sederhana

Daftar JSON berikut menunjukkan contoh ACL web dengan grup aturan terkelola pencegahan pengambilalihan akun Kontrol AWS WAF Penipuan (ATP). Perhatikan konfigurasi halaman masuk tambahan, yang memberi grup aturan informasi yang dibutuhkan untuk memantau dan mengelola permintaan login Anda. JSON ini mencakup pengaturan ACL web yang dihasilkan secara otomatis, seperti namespace label dan URL integrasi aplikasi ACL web.

```
{
    "WebACL": {
        "LabelNamespace": "awswaf:111122223333:webacl:ATPModuleACL:",
```

```
        "Capacity": 50,
        "Description": "This is a test web ACL for ATP.",
        "Rules": [
            {
                "Priority": 1,
                "OverrideAction": {
                    "None": {}
                },
                "VisibilityConfig": {
                    "SampledRequestsEnabled": true,
                    "CloudWatchMetricsEnabled": true,
                    "MetricName": "AccountTakeOverValidationRule"
                },
                "Name": "DetectCompromisedUserCredentials",
                "Statement": {
                    "ManagedRuleGroupStatement": {
                        "VendorName": "AWS",
                        "Name": "AWSManagedRulesATPRuleSet",
                        "ManagedRuleGroupConfigs": [
                          {
                            "AWSManagedRulesATPRuleSet": {
                              "LoginPath": "/web/login",
                              "RequestInspection": {
                                "PayloadType": "JSON",
                                "UsernameField": {
                                  "Identifier": "/form/username"
                                },
                                "PasswordField": {
                                  "Identifier": "/form/password"
                                }
                              },
                              "EnableRegexInPath": false
                            }
                          }
                        ]
                    }
                }
            }
        ],
        "VisibilityConfig": {
            "SampledRequestsEnabled": true,
            "CloudWatchMetricsEnabled": true,
            "MetricName": "ATPValidationAcl"
        },
```

```
        "DefaultAction": {
            "Allow": {}
        },
        "ManagedByFirewallManager": false,
        "Id": "32q10987-65rs-4tuv-3210-98765wxyz432",
        "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
ATPModuleACL/32q10987-65rs-4tuv-3210-98765wxyz432",
        "Name": "ATPModuleACL"
    },
    "ApplicationIntegrationURL": "https://9z87abce34ea.us-
east-1.sdk.awswaf.com/9z87abce34ea/1234567a1b10/",
    "LockToken": "6d0e6966-95c9-48b6-b51d-8e82e523b847"
}
```

Contoh ATP: Penanganan khusus untuk kredensi yang hilang dan dikompromikan

Secara default, pemeriksaan kredenal yang dilakukan oleh grup aturan `AWSManagedRulesATPRuleSet` menangani permintaan web sebagai berikut:

- Kredensi hilang — Label dan blokir permintaan.
- Kredensi yang dikompromikan - Permintaan label tetapi jangan memblokir atau menghitungnya.

Untuk detail tentang kelompok aturan dan perilaku aturan, lihatAWS WAF Kelompok aturan pencegahan pengambilalihan akun Kontrol Penipuan (ATP).

Anda dapat menambahkan penanganan kustom untuk permintaan web yang memiliki kredensialnya hilang atau dikompromikan dengan melakukan hal berikut:

- Ganti **`MissingCredential`** aturan ke Count — Penggantian tindakan aturan ini menyebabkan aturan hanya menghitung dan memberi label permintaan yang cocok.
- Tambahkan aturan pencocokan label dengan penanganan kustom — Konfigurasikan aturan ini agar sesuai dengan kedua label ATP dan untuk melakukan penanganan kustom Anda. Misalnya, Anda dapat mengarahkan pelanggan ke halaman pendaftaran Anda.

Aturan berikut menunjukkan grup aturan terkelola ATP dari contoh sebelumnya, dengan tindakan `MissingCredential` aturan diganti untuk dihitung. Hal ini menyebabkan aturan menerapkan labelnya ke permintaan yang cocok, dan kemudian hanya menghitung permintaan, alih-alih memblokirnya.

```
"Rules": [
    {
        "Priority": 1,
        "OverrideAction": {
            "None": {}
        },
        "VisibilityConfig": {
            "SampledRequestsEnabled": true,
            "CloudWatchMetricsEnabled": true,
            "MetricName": "AccountTakeOverValidationRule"
        },
        "Name": "DetectCompromisedUserCredentials",
        "Statement": {
            "ManagedRuleGroupStatement": {
                "ManagedRuleGroupConfigs": [
                  {
                    "AWSManagedRulesATPRuleSet": {
                      "LoginPath": "/web/login",
                      "RequestInspection": {
                        "PayloadType": "JSON",
                        "UsernameField": {
                          "Identifier": "/form/username"
                        },
                        "PasswordField": {
                          "Identifier": "/form/password"
                        }
                      },
                      "EnableRegexInPath": false
                    }
                  }
                ]
                "VendorName": "AWS",
                "Name": "AWSManagedRulesATPRuleSet",
                "RuleActionOverrides": [
                  {
                    "ActionToUse": {
                      "Count": {}
                    },
                    "Name": "MissingCredential"
                  }
                ],
                "ExcludedRules": []
            }
```

```
        }
    }
],
```

Dengan konfigurasi ini, ketika grup aturan ini mengevaluasi permintaan web apa pun yang memiliki kredensialnya hilang atau dikompromikan, ia akan memberi label permintaan tersebut, tetapi tidak memblokirnya.

Aturan berikut memiliki pengaturan prioritas yang lebih tinggi secara numerik daripada kelompok aturan sebelumnya. AWS WAF mengevaluasi aturan dalam urutan numerik, mulai dari yang terendah, sehingga aturan ini akan dievaluasi setelah evaluasi kelompok aturan. Aturan dikonfigurasi agar sesuai dengan salah satu label kredensi dan untuk mengirim respons khusus untuk permintaan yang cocok.

```
"Name": "redirectToSignup",
      "Priority": 10,
      "Statement": {
        "OrStatement": {
          "Statements": [
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:atp:signal:missing_credential"
              }
            },
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:atp:signal:credential_compromised"
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {
          "CustomResponse": {
             your custom response settings
          }
        }
      },
      "VisibilityConfig": {
```

```
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "redirectToSignup"
      }
```

Contoh ATP: Konfigurasi inspeksi respons

Daftar JSON berikut menunjukkan contoh ACL web dengan grup aturan terkelola pencegahan pengambilalihan akun Kontrol AWS WAF Penipuan (ATP) yang dikonfigurasi untuk memeriksa tanggapan asal. Perhatikan konfigurasi inspeksi respons, yang menentukan kode status keberhasilan dan respons. Anda juga dapat mengonfigurasi pengaturan keberhasilan dan respons berdasarkan kecocokan JSON header, body, dan body. JSON ini mencakup pengaturan ACL web yang dihasilkan secara otomatis, seperti namespace label dan URL integrasi aplikasi ACL web.

> **Note**
>
> Pemeriksaan respons ATP hanya tersedia di ACL web yang melindungi CloudFront distribusi.

```
{
    "WebACL": {
        "LabelNamespace": "awswaf:111122223333:webacl:ATPModuleACL:",
        "Capacity": 50,
        "Description": "This is a test web ACL for ATP.",
        "Rules": [
            {
                "Priority": 1,
                "OverrideAction": {
                    "None": {}
                },
                "VisibilityConfig": {
                    "SampledRequestsEnabled": true,
                    "CloudWatchMetricsEnabled": true,
                    "MetricName": "AccountTakeOverValidationRule"
                },
                "Name": "DetectCompromisedUserCredentials",
                "Statement": {
                    "ManagedRuleGroupStatement": {
                        "VendorName": "AWS",
                        "Name": "AWSManagedRulesATPRuleSet",
                        "ManagedRuleGroupConfigs": [
```

```
                        {
                          "AWSManagedRulesATPRuleSet": {
                            "LoginPath": "/web/login",
                            "RequestInspection": {
                              "PayloadType": "JSON",
                              "UsernameField": {
                                "Identifier": "/form/username"
                              },
                              "PasswordField": {
                                "Identifier": "/form/password"
                              }
                            },
                            "ResponseInspection": {
                              "StatusCode": {
                                "SuccessCodes": [
                                  200
                                ],
                                "FailureCodes": [
                                  401
                                ]
                              }
                            },
                            "EnableRegexInPath": false
                          }
                        }
                      ]
                    }
                }
            }
        ],
        "VisibilityConfig": {
            "SampledRequestsEnabled": true,
            "CloudWatchMetricsEnabled": true,
            "MetricName": "ATPValidationAcl"
        },
        "DefaultAction": {
            "Allow": {}
        },
        "ManagedByFirewallManager": false,
        "Id": "32q10987-65rs-4tuv-3210-98765wxyz432",
        "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
ATPModuleACL/32q10987-65rs-4tuv-3210-98765wxyz432",
        "Name": "ATPModuleACL"
    },
```

```
    "ApplicationIntegrationURL": "https://9z87abce34ea.us-
east-1.sdk.awswaf.com/9z87abce34ea/1234567a1b10/",
    "LockToken": "6d0e6966-95c9-48b6-b51d-8e82e523b847"
}
```

AWS WAF Kontrol Bot

Dengan Bot Control, Anda dapat dengan mudah memantau, memblokir, atau menilai bot batas seperti pencakar, pemindai, perayap, monitor status, dan mesin pencari. Jika Anda menggunakan tingkat inspeksi yang ditargetkan dari grup aturan, Anda juga dapat menantang bot yang tidak mengidentifikasi diri sendiri, membuatnya lebih sulit dan lebih mahal bagi bot jahat untuk beroperasi di situs web Anda. Anda dapat melindungi aplikasi Anda menggunakan grup aturan terkelola Kontrol Bot sendiri, atau dalam kombinasi dengan grup aturan Aturan AWS Terkelola lainnya dan AWS WAF aturan kustom Anda sendiri.

Bot Control mencakup dasbor konsol yang menunjukkan berapa banyak lalu lintas Anda saat ini berasal dari bot, berdasarkan pengambilan sampel permintaan. Dengan grup aturan terkelola Bot Control ditambahkan ke ACL web Anda, Anda dapat mengambil tindakan terhadap lalu lintas bot dan menerima informasi terperinci dan real-time tentang lalu lintas bot umum yang datang ke aplikasi Anda.

> **Note**
>
> Anda akan dikenakan biaya tambahan saat menggunakan grup aturan terkelola ini. Untuk informasi selengkapnya, silakan lihat Harga AWS WAF.

Grup aturan terkelola Bot Control menyediakan tingkat perlindungan dasar dan umum yang menambahkan label ke bot pengenal diri, memverifikasi bot yang umumnya diinginkan, dan mendeteksi tanda tangan bot dengan kepercayaan tinggi. Ini memberi Anda kemampuan untuk memantau dan mengontrol kategori umum lalu lintas bot.

Grup aturan Bot Control juga menyediakan tingkat perlindungan yang ditargetkan yang menambahkan deteksi untuk bot canggih yang tidak mengidentifikasi diri. Perlindungan yang ditargetkan menggunakan teknik deteksi seperti interogasi browser, sidik jari, dan heuristik perilaku untuk mengidentifikasi lalu lintas bot yang buruk. Selain itu, perlindungan yang ditargetkan menyediakan analisis pembelajaran mesin opsional otomatis dari statistik lalu lintas situs web untuk mendeteksi aktivitas terkait bot. Saat Anda mengaktifkan pembelajaran mesin, AWS WAF

gunakan statistik tentang lalu lintas situs web, seperti stempel waktu, karakteristik browser, dan URL sebelumnya yang dikunjungi, untuk meningkatkan model pembelajaran mesin Kontrol Bot.

Untuk informasi selengkapnya tentang grup aturan terkelola Kontrol Bot, lihatAWS WAF Grup aturan Bot Control.

Saat AWS WAF mengevaluasi permintaan web terhadap grup aturan terkelola Bot Control, grup aturan menambahkan label ke permintaan yang dideteksi sebagai bot terkait, misalnya kategori bot dan nama bot. Anda dapat mencocokkan label ini dalam AWS WAF aturan Anda sendiri untuk menyesuaikan penanganan. Label yang dihasilkan oleh grup aturan terkelola Kontrol Bot disertakan dalam CloudWatch metrik Amazon dan log ACL web Anda.

Anda juga dapat menggunakan AWS Firewall Manager AWS WAF kebijakan untuk menyebarkan grup aturan terkelola Kontrol Bot di seluruh aplikasi Anda di beberapa akun yang merupakan bagian dari organisasi Anda. AWS Organizations

AWS WAF Komponen Kontrol Bot

Komponen utama implementasi Bot Control adalah sebagai berikut:

- **`AWSManagedRulesBotControlRuleSet`**— Grup aturan terkelola Bot Control yang aturannya mendeteksi dan menangani berbagai kategori bot. Grup aturan ini menambahkan label ke permintaan web yang dideteksi sebagai lalu lintas bot.

  > **Note**
  >
  > Anda akan dikenakan biaya tambahan saat menggunakan grup aturan terkelola ini. Untuk informasi selengkapnya, silakan lihat Harga AWS WAF.

  Grup aturan terkelola Bot Control menyediakan dua tingkat perlindungan yang dapat Anda pilih:

  - Umum - Mendeteksi berbagai bot pengenal diri, seperti kerangka kerja pengikisan web, mesin pencari, dan browser otomatis. Perlindungan Bot Control pada tingkat ini mengidentifikasi bot umum menggunakan teknik deteksi bot tradisional, seperti analisis data permintaan statis. Aturan memberi label lalu lintas dari bot ini dan memblokir yang tidak dapat mereka verifikasi.
  - Ditargetkan - Termasuk perlindungan tingkat umum dan menambahkan deteksi bertarget untuk bot canggih yang tidak mengidentifikasi diri. Perlindungan yang ditargetkan mengurangi aktivitas bot menggunakan kombinasi pembatasan kecepatan dan CAPTCHA dan tantangan browser latar belakang.

- **`TGT_`**— Aturan yang memberikan perlindungan yang ditargetkan memiliki nama yang dimulai dengan`TGT_`. Semua perlindungan yang ditargetkan menggunakan teknik deteksi seperti interogasi browser, sidik jari, dan heuristik perilaku untuk mengidentifikasi lalu lintas bot yang buruk.
- **`TGT_ML_`**— Aturan perlindungan yang ditargetkan yang menggunakan pembelajaran mesin memiliki nama yang dimulai dengan`TGT_ML_`. Aturan-aturan ini menggunakan analisis pembelajaran mesin otomatis dari statistik lalu lintas situs web untuk mendeteksi perilaku anomali yang menunjukkan aktivitas bot terdistribusi dan terkoordinasi. AWS WAF menganalisis statistik tentang lalu lintas situs web Anda seperti stempel waktu, karakteristik browser, dan URL sebelumnya yang dikunjungi, untuk meningkatkan model pembelajaran mesin Kontrol Bot. Kemampuan pembelajaran mesin diaktifkan secara default, tetapi Anda dapat menonaktifkannya dalam konfigurasi grup aturan Anda. Ketika pembelajaran mesin dinonaktifkan, AWS WAF tidak mengevaluasi aturan-aturan ini.

  Untuk detail termasuk informasi tentang aturan grup aturan, lihatAWS WAF Grup aturan Bot Control.

  Anda menyertakan grup aturan ini di ACL web Anda menggunakan pernyataan referensi grup aturan terkelola dan menunjukkan tingkat inspeksi yang ingin Anda gunakan. Untuk tingkat yang ditargetkan, Anda juga menunjukkan apakah akan mengaktifkan pembelajaran mesin. Untuk informasi selengkapnya tentang menambahkan grup aturan terkelola ini ke ACL web Anda, lihatMenambahkan grup aturan terkelola AWS WAF Bot Control ke ACL web Anda.

- Dasbor Kontrol Bot — Dasbor pemantauan bot untuk ACL web Anda, tersedia melalui tab Kontrol Bot ACL web. Gunakan dasbor ini untuk memantau lalu lintas Anda dan memahami berapa banyak yang berasal dari berbagai jenis bot. Ini bisa menjadi titik awal untuk menyesuaikan manajemen bot Anda, seperti yang dijelaskan dalam topik ini. Anda juga dapat menggunakannya untuk memverifikasi perubahan dan memantau aktivitas untuk berbagai bot dan kategori bot.
- JavaScript dan SDK integrasi aplikasi seluler — Anda harus menerapkan SDK seluler AWS WAF JavaScript dan seluler jika Anda menggunakan tingkat perlindungan yang ditargetkan dari grup aturan Kontrol Bot. Aturan yang ditargetkan menggunakan informasi yang disediakan oleh SDK dalam token klien untuk meningkatkan deteksi terhadap bot berbahaya. Untuk informasi selengkapnya tentang SDK, lihat AWS WAF integrasi aplikasi klien.
- Logging dan metrik - Anda dapat memantau lalu lintas bot Anda dan memahami bagaimana grup aturan terkelola Kontrol Bot mengevaluasi dan menangani lalu lintas Anda dengan mempelajari data yang dikumpulkan untuk ACL web Anda dengan log AWS WAF , Amazon Security Lake, dan Amazon. CloudWatch Label yang ditambahkan Bot Control ke permintaan web Anda

disertakan dalam data. Untuk informasi tentang opsi ini, lihatPencatatan AWS WAF lalu lintas ACL web,Pemantauan CloudWatch dengan Amazon, dan Apa itu Amazon Security Lake? .

Bergantung pada kebutuhan dan lalu lintas yang Anda lihat, Anda mungkin ingin menyesuaikan implementasi Kontrol Bot Anda. Berikut ini adalah beberapa opsi yang paling umum digunakan.

- Pernyataan cakupan bawah - Anda dapat mengecualikan beberapa lalu lintas dari permintaan web yang dievaluasi oleh grup aturan terkelola Bot Control dengan menambahkan pernyataan cakupan ke bawah di dalam pernyataan referensi grup aturan terkelola Bot Control. Sebuah pernyataan scope-down dapat berupa pernyataan aturan nestable. Ketika permintaan tidak cocok dengan pernyataan scope-down, AWS WAF mengevaluasinya sebagai tidak cocok dengan pernyataan referensi grup aturan tanpa mengevaluasinya terhadap kelompok aturan. Untuk informasi selengkapnya tentang pernyataan cakupan bawah, lihat. Pernyataan cakupan ke bawah

  Harga untuk grup aturan terkelola Bot Control naik dengan jumlah permintaan web yang AWS WAF mengevaluasi dengannya. Anda dapat membantu mengurangi biaya ini dengan menggunakan pernyataan cakupan bawah untuk membatasi permintaan yang dievaluasi oleh grup aturan. Misalnya, Anda mungkin ingin mengizinkan beranda dimuat untuk semua orang, termasuk bot, lalu menerapkan aturan grup aturan ke permintaan yang masuk ke API aplikasi Anda atau yang berisi jenis konten tertentu.
- Aturan pencocokan label dan label — Anda dapat menyesuaikan cara grup aturan Kontrol Bot menangani beberapa lalu lintas bot yang diidentifikasi menggunakan pernyataan aturan pencocokan AWS WAF label. Grup aturan Bot Control menambahkan label ke permintaan web Anda. Anda dapat menambahkan aturan pencocokan label setelah grup aturan Kontrol Bot yang cocok pada label Kontrol Bot dan menerapkan penanganan yang Anda butuhkan. Untuk informasi selengkapnya tentang pelabelan dan penggunaan pernyataan pencocokan label, lihat Pernyataan aturan pencocokan label danAWS WAF label pada permintaan web.
- Permintaan dan tanggapan khusus - Anda dapat menambahkan header khusus ke permintaan yang Anda izinkan dan Anda dapat mengirim tanggapan khusus untuk permintaan yang Anda blokir dengan memasangkan label yang cocok dengan fitur permintaan dan respons AWS WAF khusus. Untuk informasi selengkapnya tentang menyesuaikan permintaan dan tanggapan, lihatPermintaan dan tanggapan web yang disesuaikan di AWS WAF.

Mengapa Anda harus menggunakan SDK integrasi aplikasi dengan Bot Control

Sebagian besar perlindungan yang ditargetkan dari grup aturan terkelola Kontrol Bot memerlukan token tantangan yang dihasilkan oleh SDK integrasi aplikasi. Aturan yang tidak memerlukan token tantangan pada permintaan adalah perlindungan tingkat umum Kontrol Bot dan aturan pembelajaran

mesin tingkat yang ditargetkan. Untuk deskripsi tingkat perlindungan dan aturan dalam kelompok aturan, lihatAWS WAF Grup aturan Bot Control.

Kami sangat menyarankan untuk menerapkan SDK integrasi aplikasi, untuk penggunaan grup aturan Bot Control yang paling efektif. Skrip tantangan harus berjalan sebelum grup aturan Kontrol Bot agar grup aturan mendapat manfaat dari token yang diperoleh skrip.

- Dengan SDK integrasi aplikasi, skrip berjalan secara otomatis.
- Jika Anda tidak dapat menggunakan SDK, Anda dapat mengonfigurasi ACL web Anda sehingga menjalankan tindakan CAPTCHA aturan Challenge atau terhadap semua permintaan yang akan diperiksa oleh grup aturan Kontrol Bot. Menggunakan tindakan Challenge atau CAPTCHA aturan dapat dikenakan biaya tambahan. Untuk detail harga, lihat AWS WAF Harga.

Saat Anda menerapkan SDK integrasi aplikasi di klien Anda atau menggunakan salah satu tindakan aturan yang menjalankan skrip tantangan, Anda memperluas kemampuan grup aturan dan keamanan aplikasi klien Anda secara keseluruhan.

Token memberikan informasi klien dengan setiap permintaan web. Informasi tambahan ini memungkinkan grup aturan Kontrol Bot untuk memisahkan sesi klien yang sah dari sesi klien yang berperilaku buruk, bahkan ketika keduanya berasal dari satu alamat IP. Grup aturan menggunakan informasi dalam token untuk menggabungkan perilaku permintaan sesi klien untuk deteksi dan mitigasi yang disetel dengan baik yang diberikan oleh tingkat perlindungan yang ditargetkan.

Untuk informasi tentang SDK, lihatAWS WAF integrasi aplikasi klien. Untuk informasi tentang AWS WAF token, lihatAWS WAF token permintaan web. Untuk informasi tentang tindakan aturan, lihatCAPTCHAdan Challenge di AWS WAF.

Menambahkan grup aturan terkelola AWS WAF Bot Control ke ACL web Anda

Grup aturan terkelola Bot Control `AWSManagedRulesBotControlRuleSet` memerlukan konfigurasi tambahan untuk mengidentifikasi tingkat perlindungan yang ingin Anda terapkan.

Untuk deskripsi grup aturan dan daftar aturan, lihatAWS WAF Grup aturan Bot Control.

Panduan ini ditujukan untuk pengguna yang tahu secara umum cara membuat dan mengelola ACL AWS WAF web, aturan, dan grup aturan. Topik-topik tersebut dibahas di bagian sebelumnya dari panduan ini. Untuk informasi dasar tentang cara menambahkan grup aturan terkelola ke ACL web Anda, lihatMenambahkan grup aturan terkelola ke ACL web melalui konsol.

Ikuti praktik terbaik

Gunakan grup aturan Kontrol Bot sesuai dengan praktik terbaik diPraktik terbaik untuk mitigasi ancaman cerdas.

Untuk menggunakan grup **`AWSManagedRulesBotControlRuleSet`** aturan di ACL web Anda

1. Tambahkan grup aturan AWS terkelola, `AWSManagedRulesBotControlRuleSet` ke ACL web Anda. Untuk deskripsi grup aturan lengkap, lihatthe section called “Grup aturan Bot Control”.

   > **Note**
   >
   > Anda akan dikenakan biaya tambahan saat menggunakan grup aturan terkelola ini. Untuk informasi selengkapnya, silakan lihat Harga AWS WAF.

   Saat Anda menambahkan grup aturan, edit untuk membuka halaman konfigurasi untuk grup aturan.
2. Pada halaman konfigurasi grup aturan, di panel tingkat Inspeksi, pilih tingkat inspeksi yang ingin Anda gunakan.

   - Umum - Mendeteksi berbagai bot pengenal diri, seperti kerangka kerja pengikisan web, mesin pencari, dan browser otomatis. Perlindungan Bot Control pada tingkat ini mengidentifikasi bot umum menggunakan teknik deteksi bot tradisional, seperti analisis data permintaan statis. Aturan memberi label lalu lintas dari bot ini dan memblokir yang tidak dapat mereka verifikasi.
   - Ditargetkan - Termasuk perlindungan tingkat umum dan menambahkan deteksi bertarget untuk bot canggih yang tidak mengidentifikasi diri. Perlindungan yang ditargetkan mengurangi aktivitas bot menggunakan kombinasi pembatasan kecepatan dan CAPTCHA dan tantangan browser latar belakang.
     - **`TGT_`**— Aturan yang memberikan perlindungan yang ditargetkan memiliki nama yang dimulai dengan`TGT_`. Semua perlindungan yang ditargetkan menggunakan teknik deteksi seperti interogasi browser, sidik jari, dan heuristik perilaku untuk mengidentifikasi lalu lintas bot yang buruk.
     - **`TGT_ML_`**— Aturan perlindungan yang ditargetkan yang menggunakan pembelajaran mesin memiliki nama yang dimulai dengan`TGT_ML_`. Aturan-aturan ini menggunakan analisis pembelajaran mesin otomatis dari statistik lalu lintas situs web untuk mendeteksi perilaku anomali yang menunjukkan aktivitas bot terdistribusi dan terkoordinasi. AWS WAF

menganalisis statistik tentang lalu lintas situs web Anda seperti stempel waktu, karakteristik browser, dan URL sebelumnya yang dikunjungi, untuk meningkatkan model pembelajaran mesin Kontrol Bot. Kemampuan pembelajaran mesin diaktifkan secara default, tetapi Anda dapat menonaktifkannya dalam konfigurasi grup aturan Anda. Ketika pembelajaran mesin dinonaktifkan, AWS WAF tidak mengevaluasi aturan ini.

3. Jika Anda menggunakan tingkat perlindungan yang ditargetkan dan Anda tidak AWS WAF ingin menggunakan pembelajaran mesin (ML) untuk menganalisis lalu lintas web untuk aktivitas bot terdistribusi dan terkoordinasi, nonaktifkan opsi pembelajaran mesin. Pembelajaran mesin diperlukan untuk aturan Kontrol Bot yang namanya dimulai dengan`TGT_ML_`. Untuk detail tentang aturan ini, lihatDaftar aturan Bot Control.
4. Tambahkan pernyataan cakupan ke bawah untuk grup aturan, untuk memuat biaya penggunaannya. Pernyataan cakupan ke bawah mempersempit kumpulan permintaan yang diperiksa oleh kelompok aturan. Misalnya kasus penggunaan, mulailah dengan Contoh Kontrol Bot: Gunakan Kontrol Bot hanya untuk halaman login danContoh Kontrol Bot: Gunakan Kontrol Bot hanya untuk konten dinamis.
5. Berikan konfigurasi tambahan apa pun yang Anda butuhkan untuk grup aturan.
6. Simpan perubahan Anda ke ACL web.

Sebelum Anda menerapkan implementasi Kontrol Bot Anda untuk lalu lintas produksi, uji dan sesuaikan di lingkungan pementasan atau pengujian hingga Anda merasa nyaman dengan potensi dampak terhadap lalu lintas Anda. Kemudian uji dan atur aturan dalam mode hitungan dengan lalu lintas produksi Anda sebelum mengaktifkannya. Lihat bagian yang mengikuti untuk panduan.

Positif palsu dengan Kontrol AWS WAF Bot

Kami telah dengan hati-hati memilih aturan dalam grup aturan terkelola AWS WAF Bot Control untuk meminimalkan positif palsu. Kami menguji aturan terhadap lalu lintas global dan memantau dampaknya pada ACL web uji. Namun, masih mungkin untuk mendapatkan positif palsu karena perubahan pola lalu lintas. Selain itu, beberapa kasus penggunaan diketahui menyebabkan positif palsu dan akan memerlukan penyesuaian khusus untuk lalu lintas web Anda.

Situasi di mana Anda mungkin menemukan positif palsu termasuk yang berikut:

- Aplikasi seluler biasanya memiliki agen pengguna non-browser, yang diblokir `SignalNonBrowserUserAgent` aturan secara default. Jika Anda mengharapkan lalu lintas dari aplikasi seluler, atau lalu lintas sah lainnya dengan agen pengguna non-browser, Anda harus menambahkan pengecualian untuk mengizinkannya.

- Anda mungkin mengandalkan beberapa lalu lintas bot tertentu untuk hal-hal seperti pemantauan uptime, pengujian integrasi, atau alat pemasaran. Jika Bot Control mengidentifikasi dan memblokir lalu lintas bot yang ingin Anda izinkan, Anda perlu mengubah penanganan dengan menambahkan aturan Anda sendiri. Meskipun ini bukan skenario positif palsu untuk semua pelanggan, jika itu untuk Anda, Anda harus menanganinya sama seperti positif palsu.
- Grup aturan terkelola Bot Control memverifikasi bot menggunakan alamat IP dari. AWS WAF Jika Anda menggunakan Kontrol Bot dan Anda telah memverifikasi bot yang merutekan melalui proxy atau penyeimbang beban, Anda mungkin perlu mengizinkannya secara eksplisit menggunakan aturan khusus. Untuk informasi tentang cara membuat aturan kustom jenis ini, lihatAlamat IP yang diteruskan.
- Aturan Kontrol Bot dengan tingkat positif palsu global yang rendah mungkin sangat memengaruhi perangkat atau aplikasi tertentu. Misalnya, dalam pengujian dan validasi, kami mungkin tidak mengamati permintaan dari aplikasi dengan volume lalu lintas rendah atau dari browser atau perangkat yang kurang umum.
- Aturan Kontrol Bot yang memiliki tingkat positif palsu yang rendah secara historis mungkin telah meningkatkan positif palsu untuk lalu lintas yang valid. Ini mungkin karena pola lalu lintas baru atau atribut permintaan yang muncul dengan lalu lintas yang valid, menyebabkannya cocok dengan aturan yang tidak sebelumnya. Perubahan ini mungkin disebabkan oleh situasi seperti berikut:
  - Rincian lalu lintas yang diubah sebagai arus lalu lintas melalui peralatan jaringan, seperti penyeimbang beban atau jaringan distribusi konten (CDN).
  - Perubahan yang muncul dalam data lalu lintas, misalnya browser baru atau versi baru untuk browser yang ada.

Untuk informasi tentang cara menangani positif palsu yang mungkin Anda dapatkan dari grup aturan terkelola Kontrol AWS WAF Bot, lihat panduan di bagian berikut,Menguji dan menerapkan Kontrol AWS WAF Bot.

Menguji dan menerapkan Kontrol AWS WAF Bot

Bagian ini memberikan panduan umum untuk mengonfigurasi dan menguji implementasi Kontrol AWS WAF Bot untuk situs Anda. Langkah-langkah spesifik yang Anda pilih untuk diikuti akan tergantung pada kebutuhan, sumber daya, dan permintaan web yang Anda terima.

Informasi ini merupakan tambahan dari informasi umum tentang pengujian dan penyetelan yang disediakan diMenguji dan menyetel perlindungan Anda AWS WAF.

> **Note**
>
> AWS Aturan Terkelola dirancang untuk melindungi Anda dari ancaman web umum. Bila digunakan sesuai dengan dokumentasi, grup aturan Aturan AWS Terkelola menambahkan lapisan keamanan lain untuk aplikasi Anda. Namun, grup aturan Aturan AWS Terkelola tidak dimaksudkan sebagai pengganti tanggung jawab keamanan Anda, yang ditentukan oleh AWS sumber daya yang Anda pilih. Lihat Model Tanggung Jawab Bersama untuk memastikan bahwa sumber daya Anda AWS dilindungi dengan benar.

> **Risiko lalu lintas produksi**
>
> Sebelum Anda menerapkan implementasi Kontrol Bot Anda untuk lalu lintas produksi, uji dan sesuaikan di lingkungan pementasan atau pengujian hingga Anda merasa nyaman dengan potensi dampak terhadap lalu lintas Anda. Kemudian uji dan atur aturan dalam mode hitungan dengan lalu lintas produksi Anda sebelum mengaktifkannya.

Panduan ini ditujukan untuk pengguna yang tahu secara umum cara membuat dan mengelola ACL AWS WAF web, aturan, dan grup aturan. Topik-topik tersebut dibahas di bagian sebelumnya dari panduan ini.

Untuk mengkonfigurasi dan menguji implementasi Bot Control

Lakukan langkah-langkah ini terlebih dahulu di lingkungan pengujian, kemudian dalam produksi.

1. Tambahkan grup aturan terkelola Bot Control

   > **Note**
   >
   > Anda akan dikenakan biaya tambahan saat menggunakan grup aturan terkelola ini. Untuk informasi selengkapnya, silakan lihat Harga AWS WAF.

   Tambahkan grup AWS aturan terkelola `AWSManagedRulesBotControlRuleSet` ke ACL web baru atau yang sudah ada dan konfigurasikan agar tidak mengubah perilaku ACL web saat ini.

   - Saat Anda menambahkan grup aturan terkelola, edit dan lakukan hal berikut:

- Di panel tingkat Inspeksi, pilih tingkat inspeksi yang ingin Anda gunakan.
  - Umum - Mendeteksi berbagai bot pengenal diri, seperti kerangka kerja pengikisan web, mesin pencari, dan browser otomatis. Perlindungan Bot Control pada tingkat ini mengidentifikasi bot umum menggunakan teknik deteksi bot tradisional, seperti analisis data permintaan statis. Aturan memberi label lalu lintas dari bot ini dan memblokir yang tidak dapat mereka verifikasi.
  - Ditargetkan - Termasuk perlindungan tingkat umum dan menambahkan deteksi bertarget untuk bot canggih yang tidak mengidentifikasi diri. Perlindungan yang ditargetkan mengurangi aktivitas bot menggunakan kombinasi pembatasan kecepatan dan CAPTCHA dan tantangan browser latar belakang.
    - **`TGT_`**— Aturan yang memberikan perlindungan yang ditargetkan memiliki nama yang dimulai dengan`TGT_`. Semua perlindungan yang ditargetkan menggunakan teknik deteksi seperti interogasi browser, sidik jari, dan heuristik perilaku untuk mengidentifikasi lalu lintas bot yang buruk.
    - **`TGT_ML_`**— Aturan perlindungan yang ditargetkan yang menggunakan pembelajaran mesin memiliki nama yang dimulai dengan`TGT_ML_`. Aturan-aturan ini menggunakan analisis pembelajaran mesin otomatis dari statistik lalu lintas situs web untuk mendeteksi perilaku anomali yang menunjukkan aktivitas bot terdistribusi dan terkoordinasi. AWS WAF menganalisis statistik tentang lalu lintas situs web Anda seperti stempel waktu, karakteristik browser, dan URL sebelumnya yang dikunjungi, untuk meningkatkan model pembelajaran mesin Kontrol Bot. Kemampuan pembelajaran mesin diaktifkan secara default, tetapi Anda dapat menonaktifkannya dalam konfigurasi grup aturan Anda. Ketika pembelajaran mesin dinonaktifkan, AWS WAF tidak mengevaluasi aturan-aturan ini.

  Untuk informasi lebih lanjut tentang pilihan ini, lihat[AWS WAF Grup aturan Bot Control](#).
- Di panel Aturan, buka dropdown Override all rule actions dan pilih. Count Dengan konfigurasi ini, AWS WAF mengevaluasi permintaan terhadap semua aturan dalam grup aturan dan hanya menghitung kecocokan yang dihasilkan, sambil tetap menambahkan label ke permintaan. Untuk informasi selengkapnya, lihat [Mengesampingkan tindakan aturan dalam grup aturan](#).

  Dengan penggantian ini, Anda dapat memantau dampak potensial dari aturan Kontrol Bot pada lalu lintas Anda, untuk menentukan apakah Anda ingin menambahkan pengecualian untuk hal-hal seperti kasus penggunaan internal atau bot yang diinginkan.

- Posisikan grup aturan sehingga dievaluasi terakhir di ACL web, dengan pengaturan prioritas yang secara numerik lebih tinggi daripada aturan atau grup aturan lain yang sudah Anda gunakan. Untuk informasi selengkapnya, lihat Memproses urutan aturan dan kelompok aturan dalam ACL web.

  Dengan cara ini, penanganan lalu lintas Anda saat ini tidak terganggu. Misalnya, jika Anda memiliki aturan yang mendeteksi lalu lintas berbahaya seperti injeksi SQL atau skrip lintas situs, mereka akan terus mendeteksi dan mencatat permintaan tersebut. Sebagai alternatif, jika Anda memiliki aturan yang memungkinkan lalu lintas non-berbahaya yang diketahui, mereka dapat terus mengizinkan lalu lintas itu, tanpa diblokir oleh grup aturan yang dikelola Bot Control. Anda mungkin memutuskan untuk menyesuaikan urutan pemrosesan selama aktivitas pengujian dan penyetelan Anda, tetapi ini adalah cara yang baik untuk memulai.

2. Aktifkan pencatatan dan metrik untuk ACL web

   Jika diperlukan, konfigurasikan pencatatan, pengumpulan data Amazon Security Lake, pengambilan sampel permintaan, dan CloudWatch metrik Amazon untuk ACL web. Anda dapat menggunakan alat visibilitas ini untuk memantau interaksi grup aturan terkelola Kontrol Bot dengan lalu lintas Anda.

   - Untuk informasi tentang pencatatan, lihatPencatatan AWS WAF lalu lintas ACL web.
   - Untuk informasi tentang Amazon Security Lake, lihat Apa itu Amazon Security Lake? dan Mengumpulkan data dari AWS layanan di panduan pengguna Amazon Security Lake.
   - Untuk informasi tentang CloudWatch metrik Amazon, lihatPemantauan CloudWatch dengan Amazon.
   - Untuk informasi tentang pengambilan sampel permintaan web, lihatMelihat contoh permintaan web.

3. Kaitkan ACL web dengan sumber daya

   Jika ACL web belum dikaitkan dengan sumber daya, kaitkan. Untuk informasi, lihat Mengaitkan atau memisahkan ACL web dengan sumber daya AWS.

4. Pantau lalu lintas dan kecocokan aturan Kontrol Bot

   Pastikan lalu lintas mengalir dan aturan grup aturan terkelola Bot Control menambahkan label ke permintaan web yang cocok. Anda dapat melihat label di log dan melihat metrik bot dan label di metrik Amazon CloudWatch . Di log, aturan yang telah Anda ganti untuk dihitung dalam grup aturan muncul di `action` set to count, dan `ruleGroupList` dengan `overriddenAction` menunjukkan tindakan aturan yang dikonfigurasi yang Anda timpa.

> **Note**
>
> Grup aturan terkelola Bot Control memverifikasi bot menggunakan alamat IP dari. AWS WAF Jika Anda menggunakan Kontrol Bot dan Anda telah memverifikasi bot yang merutekan melalui proxy atau penyeimbang beban, Anda mungkin perlu mengizinkannya secara eksplisit menggunakan aturan khusus. Untuk informasi tentang cara membuat aturan kustom, lihatAlamat IP yang diteruskan. Untuk informasi tentang bagaimana Anda dapat menggunakan aturan untuk menyesuaikan penanganan permintaan web Kontrol Bot, lihat langkah berikutnya.

Tinjau penanganan permintaan web dengan hati-hati untuk setiap positif palsu yang mungkin perlu Anda kurangi dengan penanganan khusus. Untuk contoh positif palsu, lihatPositif palsu dengan Kontrol AWS WAF Bot.

5. Kustomisasi penanganan permintaan web Kontrol Bot

   Jika diperlukan, tambahkan aturan Anda sendiri yang secara eksplisit mengizinkan atau memblokir permintaan, untuk mengubah cara aturan Kontrol Bot akan menanganinya.

   Bagaimana Anda melakukan ini tergantung pada kasus penggunaan Anda, tetapi berikut ini adalah solusi umum:

   - Izinkan permintaan secara eksplisit dengan aturan yang Anda tambahkan sebelum grup aturan terkelola Kontrol Bot. Dengan ini, permintaan yang diizinkan tidak pernah mencapai grup aturan untuk dievaluasi. Ini dapat membantu menahan biaya penggunaan grup aturan terkelola Bot Control.
   - Kecualikan permintaan dari evaluasi Bot Control dengan menambahkan pernyataan scope-down di dalam pernyataan grup aturan terkelola Bot Control. Ini berfungsi sama dengan opsi sebelumnya. Ini dapat membantu menahan biaya penggunaan grup aturan terkelola Kontrol Bot karena permintaan yang tidak cocok dengan pernyataan cakupan bawah tidak pernah mencapai evaluasi grup aturan. Untuk informasi tentang pernyataan cakupan bawah, lihat. Pernyataan cakupan ke bawah

     Untuk contoh , lihat yang berikut ini:

     - Kecualikan rentang IP dari manajemen bot
     - Izinkan lalu lintas dari bot yang Anda kontrol

- Gunakan label Kontrol Bot dalam penanganan permintaan untuk mengizinkan atau memblokir permintaan. Tambahkan aturan pencocokan label setelah grup aturan terkelola Kontrol Bot untuk memfilter permintaan berlabel yang ingin Anda izinkan dari permintaan yang ingin Anda blokir.

  Setelah pengujian, pertahankan aturan Kontrol Bot terkait dalam mode hitungan, dan pertahankan keputusan penanganan permintaan dalam aturan kustom Anda. Untuk informasi tentang pernyataan pencocokan label, lihatPernyataan aturan pencocokan label.

  Untuk contoh jenis kustomisasi ini, lihat berikut ini:

  - Buat pengecualian untuk agen pengguna yang diblokir
  - Izinkan bot tertentu yang diblokir
  - Blokir bot terverifikasi

Untuk contoh tambahan, lihat AWS WAF Contoh Kontrol Bot.

6. Jika diperlukan, aktifkan pengaturan grup aturan terkelola Kontrol Bot

   Bergantung pada situasi Anda, Anda mungkin telah memutuskan bahwa Anda ingin meninggalkan beberapa aturan Kontrol Bot dalam mode hitungan atau dengan penggantian tindakan yang berbeda. Untuk aturan yang ingin Anda jalankan saat dikonfigurasi di dalam grup aturan, aktifkan konfigurasi aturan reguler. Untuk melakukannya, edit pernyataan grup aturan di ACL web Anda dan buat perubahan di panel Aturan.

AWS WAF Contoh Kontrol Bot

Bagian ini menunjukkan contoh konfigurasi yang memenuhi berbagai kasus penggunaan umum untuk implementasi AWS WAF Bot Control.

Setiap contoh memberikan deskripsi kasus penggunaan dan kemudian menunjukkan solusi dalam daftar JSON untuk aturan yang dikonfigurasi khusus.

> **Note**
>
> Daftar JSON yang ditampilkan dalam contoh ini dibuat di konsol dengan mengonfigurasi aturan dan kemudian mengeditnya menggunakan editor Rule JSON.

Topik

Contoh Kontrol Bot: Konfigurasi sederhana

Daftar JSON berikut menunjukkan contoh ACL web dengan grup aturan terkelola AWS WAF Bot Control. Perhatikan konfigurasi visibilitas, yang menyebabkan AWS WAF untuk menyimpan sampel permintaan dan metrik untuk tujuan pemantauan.

```
{
  "Name": "Bot-WebACL",
  "Id": "...",
  "ARN": "...",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "Bot-WebACL",
  "Rules": [
      {
        ...
      },
      {
         "Name": "AWS-AWSBotControl-Example",
         "Priority": 5,
         "Statement": {
```

```
            "ManagedRuleGroupStatement": {
               "VendorName": "AWS",
               "Name": "AWSManagedRulesBotControlRuleSet",
               "ManagedRuleGroupConfigs": [
                 {
                   "AWSManagedRulesBotControlRuleSet": {
                     "InspectionLevel": "COMMON"
                   }
                 }
               ],
               "RuleActionOverrides": [],
               "ExcludedRules": []
            },
            "VisibilityConfig": {
               "SampledRequestsEnabled": true,
               "CloudWatchMetricsEnabled": true,
               "MetricName": "AWS-AWSBotControl-Example"
             }
          }
      }
    ],
    "VisibilityConfig": {
      ...
    },
    "Capacity": 1496,
    "ManagedByFirewallManager": false
}
```

Contoh Kontrol Bot: Izinkan bot terverifikasi secara eksplisit

AWS WAF Bot Control tidak memblokir bot yang dikenal sebagai bot umum dan dapat diverifikasi. AWS Ketika Bot Control mengidentifikasi permintaan web sebagai berasal dari bot terverifikasi, ia menambahkan label yang memberi nama bot dan label yang menunjukkan bahwa itu adalah bot terverifikasi. Bot Control tidak menambahkan label lain, seperti label sinyal, untuk mencegah bot bagus yang diketahui diblokir.

Anda mungkin memiliki AWS WAF aturan lain yang memblokir bot terverifikasi. Jika Anda ingin memastikan bahwa bot terverifikasi diizinkan, tambahkan aturan khusus untuk mengizinkannya berdasarkan label Kontrol Bot. Aturan baru Anda harus berjalan setelah grup aturan terkelola Kontrol Bot, sehingga label tersedia untuk dicocokkan.

Aturan berikut secara eksplisit memungkinkan bot terverifikasi.

```
{
    "Name": "match_rule",
    "Statement": {
      "LabelMatchStatement": {
        "Scope": "LABEL",
        "Key": "awswaf:managed:aws:bot-control:bot:verified"
      }
    },
    "RuleLabels": [],
    "Action": {
      "Allow": {}
    }
}
```

Contoh Kontrol Bot: Blokir bot terverifikasi

Untuk memblokir bot terverifikasi, Anda harus menambahkan aturan untuk memblokirnya yang berjalan setelah grup aturan terkelola Kontrol AWS WAF Bot. Untuk melakukan ini, identifikasi nama bot yang ingin Anda blokir dan gunakan pernyataan pencocokan label untuk mengidentifikasi dan memblokirnya. Jika Anda hanya ingin memblokir semua bot yang diverifikasi, Anda dapat menghilangkan kecocokan terhadap label. `bot:name:`

Aturan berikut hanya memblokir bot yang `bingbot` diverifikasi. Aturan ini harus berjalan setelah grup aturan terkelola Bot Control.

```
{
    "Name": "match_rule",
    "Statement": {
      "AndStatement": {
        "Statements": [
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:bot-control:bot:name:bingbot"
            }
          },
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:bot-control:bot:verified"
            }
          }
```

```
        ]
      }
    },
    "RuleLabels": [],
    "Action": {
      "Block": {}
    }
  }
```

Aturan berikut memblokir semua bot yang diverifikasi.

```
{
    "Name": "match_rule",
    "Statement": {
      "LabelMatchStatement": {
        "Scope": "LABEL",
        "Key": "awswaf:managed:aws:bot-control:bot:verified"
      }
    },
    "RuleLabels": [],
    "Action": {
      "Block": {}
    }
}
```

Contoh Kontrol Bot: Izinkan bot tertentu yang diblokir

Mungkin saja bot diblokir oleh lebih dari satu aturan Kontrol Bot. Jalankan melalui prosedur berikut untuk setiap aturan pemblokiran.

Jika aturan Kontrol AWS WAF Bot memblokir bot yang tidak ingin Anda blokir, lakukan hal berikut:

1. Identifikasi aturan Kontrol Bot yang memblokir bot dengan memeriksa log. Aturan pemblokiran akan ditentukan dalam log di bidang yang namanya dimulai dengan`terminatingRule`. Untuk informasi tentang log ACL web, lihatPencatatan AWS WAF lalu lintas ACL web. Perhatikan label yang ditambahkan aturan ke permintaan.
2. Di ACL web Anda, timpa tindakan aturan pemblokiran untuk dihitung. Untuk melakukan ini di konsol, edit aturan grup aturan di ACL web dan pilih penggantian tindakan aturan Count untuk aturan tersebut. Ini memastikan bahwa bot tidak diblokir oleh aturan, tetapi aturan akan tetap menerapkan labelnya untuk permintaan yang cocok.

3. Tambahkan aturan pencocokan label ke ACL web Anda, setelah grup aturan terkelola Kontrol Bot. Konfigurasikan aturan agar sesuai dengan label aturan yang diganti dan untuk memblokir semua permintaan yang cocok kecuali bot yang tidak ingin Anda blokir.

   ACL web Anda sekarang dikonfigurasi sehingga bot yang ingin Anda izinkan tidak lagi diblokir oleh aturan pemblokiran yang Anda identifikasi melalui log.

Periksa lalu lintas dan log Anda lagi, untuk memastikan bahwa bot diizinkan masuk. Jika tidak, jalankan kembali prosedur di atas.

Misalnya, Anda ingin memblokir semua bot pemantauan kecuali untuk`pingdom`. Dalam hal ini, Anda mengganti `CategoryMonitoring` aturan untuk menghitung dan kemudian menulis aturan untuk memblokir semua bot pemantauan kecuali yang memiliki label nama bot. `pingdom`

Aturan berikut menggunakan grup aturan terkelola Bot Control tetapi mengesampingkan tindakan aturan `CategoryMonitoring` untuk dihitung. Aturan pemantauan kategori menerapkan labelnya seperti biasa untuk permintaan yang cocok, tetapi hanya menghitungnya alih-alih melakukan tindakan pemblokiran yang biasa.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
   "RuleActionOverrides": [
        {
          "ActionToUse": {
            "Count": {}
          },
          "Name": "CategoryMonitoring"
        }
      ],
```

```
      "ExcludedRules": []
    }
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "AWS-AWSBotControl-Example"
  }
}
```

Aturan berikut cocok dengan label pemantauan kategori yang ditambahkan `CategoryMonitoring` aturan sebelumnya ke permintaan web yang cocok. Di antara permintaan pemantauan kategori, aturan ini memblokir semua kecuali yang memiliki label untuk nama bot`pingdom`.

Aturan berikut harus berjalan setelah grup aturan terkelola Kontrol Bot sebelumnya dalam urutan pemrosesan ACL web.

```
{
      "Name": "match_rule",
      "Priority": 10,
      "Statement": {
        "AndStatement": {
          "Statements": [
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:bot-control:bot:category:monitoring"
              }
            },
            {
              "NotStatement": {
                "Statement": {
                  "LabelMatchStatement": {
                    "Scope": "LABEL",
                    "Key": "awswaf:managed:aws:bot-control:bot:name:pingdom"
                  }
                }
              }
            }
          ]
        }
      },
      "Action": {
```

```
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "match_rule"
      }
}
```

Contoh Kontrol Bot: Buat pengecualian untuk agen pengguna yang diblokir

Jika lalu lintas dari beberapa agen pengguna non-browser diblokir secara keliru, Anda dapat membuat pengecualian dengan menetapkan aturan Kontrol AWS WAF Bot yang menyinggung `SignalNonBrowserUserAgent` ke Hitung dan kemudian menggabungkan pelabelan aturan dengan kriteria pengecualian Anda.

> **Note**
>
> Aplikasi seluler biasanya memiliki agen pengguna non-browser, yang diblokir `SignalNonBrowserUserAgent` aturan secara default.

Aturan berikut menggunakan grup aturan terkelola Bot Control tetapi mengesampingkan tindakan aturan `SignalNonBrowserUserAgent` untuk Menghitung. Aturan sinyal menerapkan labelnya seperti biasa untuk permintaan yang cocok, tetapi hanya menghitungnya alih-alih melakukan tindakan blok yang biasa.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
```

```
   "RuleActionOverrides": [
        {
          "ActionToUse": {
            "Count": {}
          },
          "Name": "SignalNonBrowserUserAgent"
        }
      ],
      "ExcludedRules": []
    }
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "AWS-AWSBotControl-Example"
  }
}
```

Aturan berikut cocok dengan label sinyal yang ditambahkan `SignalNonBrowserUserAgent` aturan Kontrol Bot ke permintaan webnya yang cocok. Di antara permintaan sinyal, aturan ini memblokir semua kecuali yang memiliki agen pengguna yang ingin kami izinkan.

Aturan berikut harus berjalan setelah grup aturan terkelola Kontrol Bot sebelumnya dalam urutan pemrosesan ACL web.

```
{
    "Name": "match_rule",
    "Statement": {
      "AndStatement": {
        "Statements": [
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:bot-control:signal:non_browser_user_agent"
            }
          },
          {
            "NotStatement": {
              "Statement": {
                "ByteMatchStatement": {
                  "FieldToMatch": {
                    "SingleHeader": {
                      "Name": "user-agent"
```

```
                    }
                  },
                  "PositionalConstraint": "EXACTLY",
                  "SearchString": "PostmanRuntime/7.29.2",
                  "TextTransformations": [
                    {
                      "Priority": 0,
                      "Type": "NONE"
                    }
                  ]
                }
              }
            }
          }
        ]
      }
    },
    "RuleLabels": [],
    "Action": {
      "Block": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "match_rule"
    }
}
```

Contoh Kontrol Bot: Gunakan Kontrol Bot hanya untuk halaman login

Contoh berikut menggunakan pernyataan scope-down untuk menerapkan AWS WAF Bot Control hanya untuk lalu lintas yang datang ke halaman login situs web, yang diidentifikasi oleh jalur URI. `login` Jalur URI ke halaman login Anda mungkin berbeda dari contoh, tergantung pada aplikasi dan lingkungan Anda.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
   "ManagedRuleGroupConfigs": [
```

```
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "ByteMatchStatement": {
        "SearchString": "login",
        "FieldToMatch": {
          "UriPath": {}
        },
        "TextTransformations": [
          {
            "Priority": 0,
            "Type": "NONE"
          }
        ],
        "PositionalConstraint": "CONTAINS"
      }
    }
  }
}
```

Contoh Kontrol Bot: Gunakan Kontrol Bot hanya untuk konten dinamis

Contoh ini menggunakan pernyataan scope-down untuk menerapkan AWS WAF Bot Control hanya untuk konten dinamis.

Pernyataan scope-down mengecualikan konten statis dengan meniadakan hasil kecocokan untuk kumpulan pola regex:

- Set pola regex dikonfigurasi agar sesuai dengan ekstensi konten statis. Misalnya, spesifikasi set pola regex mungkin. `(?i)\.(jpe?g|gif|png|svg|ico|css|js|woff2?)$` Untuk informasi tentang kumpulan pola regex dan pernyataan, lihat. Pernyataan aturan kecocokan set pola regex

- Dalam pernyataan scope-down, kami mengecualikan konten statis yang cocok dengan menyarangkan pernyataan set pola regex di dalam pernyataan. `NOT` Untuk informasi tentang `NOT` pernyataan tersebut, lihatNOTpernyataan aturan.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
   "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
        "Statement": {
          "RegexPatternSetReferenceStatement": {
            "ARN": "arn:aws:wafv2:us-east-1:123456789:regional/regexpatternset/
excludeset/00000000-0000-0000-0000-000000000000",
            "FieldToMatch": {
              "UriPath": {}
            },
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
```

```
        }
      }
    }
  }
}
```

Contoh Kontrol Bot: Kecualikan rentang IP dari manajemen bot

Jika Anda ingin mengecualikan subset lalu lintas web dari manajemen Kontrol AWS WAF Bot, dan Anda dapat mengidentifikasi subset tersebut menggunakan pernyataan aturan, lalu kecualikan dengan menambahkan pernyataan cakupan ke bawah ke pernyataan grup aturan terkelola Kontrol Bot Anda.

Aturan berikut melakukan manajemen bot Kontrol Bot normal pada semua lalu lintas web kecuali untuk permintaan web yang berasal dari rentang alamat IP tertentu.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
        "Statement": {
          "IPSetReferenceStatement": {
```

```
            "ARN": "arn:aws:wafv2:us-east-1:123456789:regional/ipset/
friendlyips/00000000-0000-0000-0000-000000000000"
          }
        }
      }
    }
  }
}
```

Contoh Kontrol Bot: Izinkan lalu lintas dari bot yang Anda kontrol

Anda dapat mengonfigurasi beberapa bot pemantauan situs dan bot khusus untuk mengirim header khusus. Jika Anda ingin mengizinkan lalu lintas dari jenis bot ini, Anda dapat mengonfigurasinya untuk menambahkan rahasia bersama di header. Anda kemudian dapat mengecualikan pesan yang memiliki header dengan menambahkan pernyataan scope-down ke pernyataan grup aturan terkelola AWS WAF Bot Control.

Contoh aturan berikut mengecualikan lalu lintas dengan header rahasia dari inspeksi Bot Control.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
```

```
        "Statement": {
          "ByteMatchStatement": {
            "SearchString": "YSBzZWNyZXQ=",
            "FieldToMatch": {
              "SingleHeader": {
                "Name": "x-bypass-secret"
              }
            },
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ],
            "PositionalConstraint": "EXACTLY"
          }
        }
      }
    }
  }
}
```

Contoh Kontrol Bot: Tingkat inspeksi yang ditargetkan

Untuk tingkat perlindungan yang ditingkatkan, Anda dapat mengaktifkan tingkat inspeksi yang ditargetkan di grup aturan terkelola Kontrol AWS WAF Bot Anda.

Dalam contoh berikut, fitur pembelajaran mesin diaktifkan. Anda dapat memilih keluar dari perilaku ini dengan menyetel `EnableMachineLearning` ke`false`.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "TARGETED",
            "EnableMachineLearning": true
          }
```

```
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    }
  }
}
```

Contoh Kontrol Bot: Gunakan dua pernyataan untuk membatasi penggunaan tingkat inspeksi yang ditargetkan

Sebagai pengoptimalan biaya, Anda dapat menggunakan dua pernyataan grup aturan terkelola AWS WAF Bot Control di ACL web Anda, dengan tingkat inspeksi dan pelingkupan terpisah. Misalnya, Anda dapat mencakup pernyataan tingkat inspeksi yang ditargetkan hanya ke titik akhir aplikasi yang lebih sensitif.

Dua pernyataan dalam contoh berikut memiliki pelingkupan yang saling eksklusif. Tanpa konfigurasi ini, permintaan dapat menghasilkan dua evaluasi yang ditagih.

> **Note**
>
> Referensi `AWSManagedRulesBotControlRuleSet` beberapa pernyataan tidak didukung di editor visual di konsol. Sebagai gantinya, gunakan editor JSON.

```
{
  "Name": "Bot-WebACL",
  "Id": "...",
  "ARN": "...",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "Bot-WebACL",
  "Rules": [
      {
        ...
      },
```

```
    {
     "Name": "AWS-AWSBotControl-Common",
     "Priority": 5,
     "Statement": {
        "ManagedRuleGroupStatement": {
           "VendorName": "AWS",
           "Name": "AWSManagedRulesBotControlRuleSet",
           "ManagedRuleGroupConfigs": [
             {
               "AWSManagedRulesBotControlRuleSet": {
                 "InspectionLevel": "COMMON"
               }
             }
           ],
           "RuleActionOverrides": [],
           "ExcludedRules": []
        },
        "VisibilityConfig": {
           "SampledRequestsEnabled": true,
           "CloudWatchMetricsEnabled": true,
           "MetricName": "AWS-AWSBotControl-Common"
         },
         "ScopeDownStatement": {
            "NotStatement": {
              "Statement": {
                "ByteMatchStatement": {
                  "FieldToMatch": {
                    "UriPath": {}
                  },
                  "PositionalConstraint": "STARTS_WITH",
                  "SearchString": "/sensitive-endpoint",
                  "TextTransformations": [
                    {
                      "Type": "NONE",
                      "Priority": 0
                    }
                  ]
                }
              }
            }
         }
      }
    },
    {
```

```
      "Name": "AWS-AWSBotControl-Targeted",
      "Priority": 6,
      "Statement": {
         "ManagedRuleGroupStatement": {
            "VendorName": "AWS",
            "Name": "AWSManagedRulesBotControlRuleSet",
            "ManagedRuleGroupConfigs": [
              {
                "AWSManagedRulesBotControlRuleSet": {
                  "InspectionLevel": "TARGETED",
                  "EnableMachineLearning": true
                }
              }
            ],
            "RuleActionOverrides": [],
            "ExcludedRules": []
         },
         "VisibilityConfig": {
            "SampledRequestsEnabled": true,
            "CloudWatchMetricsEnabled": true,
            "MetricName": "AWS-AWSBotControl-Targeted"
          },
          "ScopeDownStatement": {
             "Statement": {
               "ByteMatchStatement": {
                 "FieldToMatch": {
                   "UriPath": {}
                 },
                 "PositionalConstraint": "STARTS_WITH",
                 "SearchString": "/sensitive-endpoint",
                 "TextTransformations": [
                   {
                     "Type": "NONE",
                     "Priority": 0
                   }
                 ]
               }
             }
          }
       }
     }
   ],
   "VisibilityConfig": {
     ...
```

```
    },
    "Capacity": 1496,
    "ManagedByFirewallManager": false
}
```

AWS WAF integrasi aplikasi klien

Gunakan API integrasi aplikasi AWS WAF klien untuk memasangkan perlindungan sisi klien dengan perlindungan ACL web AWS sisi server Anda, untuk membantu memverifikasi bahwa aplikasi klien yang mengirim permintaan web ke sumber daya yang dilindungi adalah klien yang dituju dan bahwa pengguna akhir Anda adalah manusia.

Gunakan integrasi klien untuk mengelola tantangan browser senyap dan teka-teki CAPTCHA, dapatkan token dengan bukti keberhasilan browser dan tanggapan pengguna akhir, dan untuk memasukkan token ini dalam permintaan ke titik akhir Anda yang dilindungi. Untuk informasi umum tentang AWS WAF token, lihatAWS WAF token permintaan web.

Gabungkan integrasi klien Anda dengan perlindungan ACL web yang memerlukan token yang valid untuk akses ke sumber daya Anda. Anda dapat menggunakan grup aturan yang memeriksa dan memantau token tantangan, seperti yang tercantum di bagian berikutnya, diIntegrasi ancaman cerdas dan Aturan AWS Terkelola, dan Anda dapat menggunakan tindakan CAPTCHA dan Challenge aturan untuk memeriksa, seperti yang dijelaskan dalamCAPTCHAdan Challenge di AWS WAF.

AWS WAF menyediakan dua tingkat integrasi untuk JavaScript aplikasi, dan satu untuk aplikasi seluler:

- Integrasi ancaman cerdas — Verifikasi aplikasi klien dan berikan akuisisi dan manajemen AWS token. Ini mirip dengan fungsi yang disediakan oleh tindakan AWS WAF Challenge aturan. Fungsionalitas ini sepenuhnya mengintegrasikan aplikasi klien Anda dengan grup aturan `AWSManagedRulesACFPRuleSet` terkelola, grup aturan `AWSManagedRulesATPRuleSet` terkelola, dan tingkat perlindungan yang ditargetkan dari grup aturan `AWSManagedRulesBotControlRuleSet` terkelola.

  API integrasi ancaman cerdas menggunakan tantangan browser AWS WAF senyap untuk membantu memastikan bahwa upaya login dan panggilan lain ke sumber daya Anda yang dilindungi hanya diizinkan setelah klien memperoleh token yang valid. API mengelola otorisasi token untuk sesi aplikasi klien Anda dan mengumpulkan informasi tentang klien untuk membantu menentukan apakah itu dioperasikan oleh bot atau oleh manusia.

> **Note**
>
> Ini tersedia untuk JavaScript dan untuk aplikasi seluler Android dan iOS.

- Integrasi CAPTCHA - Verifikasi pengguna akhir dengan teka-teki CAPTCHA yang disesuaikan yang Anda kelola dalam aplikasi Anda. Ini mirip dengan fungsionalitas yang disediakan oleh tindakan AWS WAF CAPTCHA aturan, tetapi dengan kontrol tambahan atas penempatan dan perilaku teka-teki.

  Integrasi ini memanfaatkan integrasi ancaman JavaScript cerdas untuk menjalankan tantangan diam dan memberikan AWS WAF token ke halaman pelanggan.

  > **Note**
  >
  > Ini tersedia untuk JavaScript aplikasi.

Topik

Integrasi ancaman cerdas dan Aturan AWS Terkelola

API integrasi ancaman cerdas bekerja dengan ACL web yang menggunakan grup aturan ancaman cerdas untuk mengaktifkan fungsionalitas penuh dari grup aturan terkelola lanjutan ini.

- AWS WAF Grup aturan terkelola pencegahan penipuan (ACFP) pembuatan akun Kontrol Penipuan. `AWSManagedRulesACFPRuleSet`

  Penipuan pembuatan akun adalah aktivitas ilegal online di mana penyerang membuat akun yang tidak valid dalam aplikasi Anda untuk tujuan seperti menerima bonus pendaftaran atau meniru seseorang. Grup aturan terkelola ACFP menyediakan aturan untuk memblokir, memberi label, dan mengelola permintaan yang mungkin merupakan bagian dari upaya pembuatan akun palsu. API memungkinkan verifikasi browser klien yang disetel dengan baik dan informasi interaktivitas

manusia yang digunakan aturan ACFP untuk memisahkan lalu lintas klien yang valid dari lalu lintas berbahaya.

Lihat informasi yang lebih lengkap di AWS WAF Grup aturan pencegahan penipuan (ACFP) pembuatan akun Kontrol Penipuan dan AWS WAF Pencegahan penipuan pembuatan akun Kontrol Penipuan (ACFP).

- AWS WAF Kelompok aturan terkelola pencegahan pengambilalihan akun Kontrol Penipuan (ATP). `AWSManagedRulesATPRuleSet`

  Pengambilalihan akun adalah aktivitas ilegal online di mana penyerang mendapatkan akses tidak sah ke akun seseorang. Grup aturan terkelola ATP menyediakan aturan untuk memblokir, memberi label, dan mengelola permintaan yang mungkin merupakan bagian dari upaya pengambilalihan akun berbahaya. API memungkinkan verifikasi klien yang disetel dengan baik dan agregasi perilaku yang digunakan aturan ATP untuk memisahkan lalu lintas klien yang valid dari lalu lintas berbahaya.

  Lihat informasi yang lebih lengkap di AWS WAF Kelompok aturan pencegahan pengambilalihan akun Kontrol Penipuan (ATP) dan AWS WAF Pencegahan pengambilalihan akun Kontrol Penipuan (ATP).

- Tingkat perlindungan yang ditargetkan dari grup aturan terkelola Kontrol AWS WAF Bot`AWSManagedRulesBotControlRuleSet`.

  Bot berjalan dari yang mengidentifikasi diri dan berguna, seperti kebanyakan mesin pencari dan crawler, hingga bot jahat yang beroperasi melawan situs web Anda dan tidak mengidentifikasi diri. Grup aturan terkelola Bot Control menyediakan aturan untuk memantau, memberi label, dan mengelola aktivitas bot di lalu lintas web Anda. Saat Anda menggunakan tingkat perlindungan yang ditargetkan dari grup aturan ini, aturan yang ditargetkan menggunakan informasi sesi klien yang disediakan API untuk mendeteksi bot berbahaya dengan lebih baik.

  Lihat informasi yang lebih lengkap di AWS WAF Grup aturan Bot Control dan AWS WAF Kontrol Bot.

Untuk menambahkan salah satu grup aturan terkelola ini ke ACL web Anda, lihat prosedurnya Menambahkan grup aturan terkelola ACFP ke ACL web AndaMenambahkan grup aturan terkelola ATP ke ACL web Anda, danMenambahkan grup aturan terkelola AWS WAF Bot Control ke ACL web Anda.

> **Note**
>
> Grup aturan terkelola saat ini tidak memblokir permintaan yang tidak memiliki token. Untuk memblokir permintaan yang tidak memiliki token, setelah Anda menerapkan API integrasi aplikasi, ikuti panduan diMemblokir permintaan yang tidak memiliki AWS WAF token yang valid.

Mengakses API integrasi aplikasi AWS WAF klien

API JavaScript integrasi umumnya tersedia, dan Anda dapat menggunakannya untuk browser Anda dan perangkat lain yang mengeksekusi JavaScript.

AWS WAF menawarkan SDK integrasi ancaman cerdas khusus untuk aplikasi seluler Android dan iOS.

- Untuk aplikasi seluler Android, AWS WAF SDK berfungsi untuk Android API versi 23 (Android versi 6) dan yang lebih baru. Untuk informasi tentang versi Android, lihat catatan rilis SDK Platform.
- Untuk aplikasi seluler iOS, AWS WAF SDK berfungsi untuk iOS versi 13 dan yang lebih baru. Untuk informasi tentang versi iOS, lihat Catatan Rilis iOS & iPadOS.

Untuk mengakses API integrasi melalui konsol

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.
2. Pilih Integrasi aplikasi di panel navigasi, lalu pilih tab yang Anda minati.

   - Integrasi ancaman cerdas tersedia untuk JavaScript dan aplikasi seluler.

     Tab berisi yang berikut:

     - Daftar ACL web yang diaktifkan untuk integrasi aplikasi ancaman cerdas. Daftar ini mencakup setiap ACL web yang menggunakan grup aturan `AWSManagedRulesACFPRuleSet` terkelola, grup aturan `AWSManagedRulesATPRuleSet` terkelola, atau tingkat perlindungan yang ditargetkan dari grup aturan `AWSManagedRulesBotControlRuleSet` terkelola. Saat menerapkan API ancaman cerdas, Anda menggunakan URL integrasi untuk ACL web yang ingin Anda integrasikan.
     - API yang dapat Anda akses. JavaScript API selalu tersedia. Untuk akses ke SDK seluler, hubungi dukungan di Kontak AWS.

- Integrasi CAPTCHA tersedia untuk JavaScript aplikasi.

  Tab berisi yang berikut:

  - URL integrasi untuk digunakan dalam integrasi Anda.
  - Kunci API yang telah Anda buat untuk domain aplikasi klien Anda. Penggunaan CAPTCHA API Anda memerlukan kunci API terenkripsi yang memberi klien hak untuk mengakses AWS WAF CAPTCHA dari domain mereka. Untuk setiap klien yang Anda integrasikan, gunakan kunci API yang berisi domain klien. Untuk informasi selengkapnya persyaratan ini dan tentang mengelola kunci ini, lihatMengelola kunci API untuk JS CAPTCHA API.

AWS WAF JavaScript integrasi

Anda dapat menggunakan API JavaScript integrasi untuk mengimplementasikan integrasi AWS WAF aplikasi di browser Anda dan perangkat lain yang mengeksekusi JavaScript.

Teka-teki CAPTCHA dan tantangan diam hanya dapat berjalan ketika browser mengakses titik akhir HTTPS. Klien browser harus berjalan dalam konteks aman untuk mendapatkan token.

- API ancaman cerdas memungkinkan Anda mengelola otorisasi token melalui tantangan browser sisi klien yang diam, dan menyertakan token dalam permintaan yang Anda kirim ke sumber daya yang dilindungi.
- API integrasi CAPTCHA menambah API ancaman cerdas, dan memungkinkan Anda menyesuaikan penempatan dan karakteristik teka-teki CAPTCHA dalam aplikasi klien Anda. API ini memanfaatkan API ancaman cerdas untuk memperoleh AWS WAF token untuk digunakan di halaman setelah pengguna akhir berhasil menyelesaikan teka-teki CAPTCHA.

Dengan menggunakan integrasi ini, Anda memastikan bahwa panggilan prosedur jarak jauh oleh klien Anda berisi token yang valid. Ketika API integrasi ini diterapkan pada halaman aplikasi Anda, Anda dapat menerapkan aturan mitigasi di ACL web Anda, seperti memblokir permintaan yang tidak berisi token yang valid. Anda juga dapat menerapkan aturan yang memberlakukan penggunaan token yang diperoleh aplikasi klien Anda, dengan menggunakan Challenge atau CAPTCHA tindakan dalam aturan Anda.

Daftar berikut menunjukkan komponen dasar dari implementasi tipikal API ancaman cerdas di halaman aplikasi web.

```
<head>
```

```
<script type="text/javascript" src="Web ACL integration URL/challenge.js" defer></
script>
</head>
<script>
const login_response = await AwsWafIntegration.fetch(login_url, {
    method: 'POST',
    headers: {
      'Content-Type': 'application/json'
    },
    body: login_body
  });
</script>
```

API integrasi CAPTCHA memungkinkan Anda menyesuaikan pengalaman teka-teki CAPTCHA pengguna akhir Anda. Integrasi CAPTCHA memanfaatkan integrasi ancaman JavaScript cerdas, untuk verifikasi browser dan manajemen token, dan menambahkan fungsi untuk mengonfigurasi dan merender teka-teki CAPTCHA.

Daftar berikut menunjukkan komponen dasar implementasi khas CAPTCHA JavaScript API di halaman aplikasi web.

```
<head>
    <script type="text/javascript" src="<Integration URL>/jsapi.js" defer></script>
</head>

<script type="text/javascript">
    function showMyCaptcha() {
        var container = document.querySelector("#my-captcha-container");

        AwsWafCaptcha.renderCaptcha(container, {
            apiKey: "...API key goes here...",
            onSuccess: captchaExampleSuccessFunction,
            onError: captchaExampleErrorFunction,
            ...other configuration parameters as needed...
        });
    }

    function captchaExampleSuccessFunction(wafToken) {
        // Use WAF token to access protected resources
        AwsWafIntegration.fetch("...WAF-protected URL...", {
            method: "POST",
            ...
        });
```

```
    }

    function captchaExampleErrorFunction(error) {
        /* Do something with the error */
    }
</script>

<div id="my-captcha-container">
    <!-- The contents of this container will be replaced by the captcha widget -->
</div>
```

Topik

- Menyediakan domain untuk digunakan dalam token
- Menggunakan JavaScript API dengan kebijakan keamanan konten
- Menggunakan JavaScript API ancaman cerdas
- Menggunakan JavaScript CAPTCHA API

Menyediakan domain untuk digunakan dalam token

Secara default, saat AWS WAF membuat token, ia menggunakan domain host dari sumber daya yang terkait dengan ACL web. Anda dapat memberikan domain tambahan untuk token yang AWS WAF dibuat untuk JavaScript API. Untuk melakukan ini, konfigurasikan variabel global`window.awsWafCookieDomainList`, dengan satu atau lebih domain token.

Saat AWS WAF membuat token, ia menggunakan domain terpendek yang paling tepat dari antara kombinasi domain di `window.awsWafCookieDomainList` dan domain host dari sumber daya yang terkait dengan ACL web.

Contoh pengaturan:

```
window.awsWafCookieDomainList = ['.aws.amazon.com']
```

```
window.awsWafCookieDomainList = ['.aws.amazon.com', 'abc.aws.amazon.com']
```

Anda tidak dapat menggunakan sufiks publik dalam daftar ini. Misalnya, Anda tidak dapat menggunakan `gov.au` atau `co.uk` sebagai domain token dalam daftar.

Domain yang Anda tentukan dalam daftar ini harus kompatibel dengan domain dan konfigurasi domain Anda yang lain:

- Domain haruslah yang AWS WAF akan menerima, berdasarkan domain host yang dilindungi dan daftar domain token yang dikonfigurasi untuk ACL web. Untuk informasi selengkapnya, lihat AWS WAF konfigurasi daftar domain token ACL web.
- Jika Anda menggunakan JavaScript CAPTCHA API, setidaknya satu domain di kunci API CAPTCHA Anda harus sama persis dengan salah satu domain token di dalamnya `window.awsWafCookieDomainList` atau harus domain puncak dari salah satu domain token tersebut.

  Misalnya, untuk domain token`mySubdomain.myApex.com`, kunci `mySubdomain.myApex.com` API sama persis dan kunci API `myApex.com` adalah domain apex. Salah satu kunci cocok dengan domain token.

  Untuk informasi selengkapnya tentang kunci API, lihatMengelola kunci API untuk JS CAPTCHA API.

Jika Anda menggunakan grup aturan `AWSManagedRulesACFPRuleSet` terkelola, Anda dapat mengonfigurasi domain yang cocok dengan domain di jalur pembuatan akun yang Anda berikan ke konfigurasi grup aturan. Untuk informasi selengkapnya tentang konfigurasi ini, silakan lihat Menambahkan grup aturan terkelola ACFP ke ACL web Anda.

Jika Anda menggunakan grup aturan `AWSManagedRulesATPRuleSet` terkelola, Anda dapat mengonfigurasi domain yang cocok dengan domain di jalur masuk yang Anda berikan ke konfigurasi grup aturan. Untuk informasi selengkapnya tentang konfigurasi ini, silakan lihat Menambahkan grup aturan terkelola ATP ke ACL web Anda.

Menggunakan JavaScript API dengan kebijakan keamanan konten

Jika Anda menerapkan kebijakan keamanan konten (CSP) ke sumber daya Anda, agar JavaScript implementasi Anda berfungsi, Anda perlu mengizinkan daftar domain AWS WAF apex. `awswaf.com` JavaScript SDK melakukan panggilan ke AWS WAF titik akhir yang berbeda, jadi izinkan daftar domain ini memberikan izin yang dibutuhkan SDK untuk beroperasi.

Berikut ini menunjukkan contoh konfigurasi untuk mengizinkan domain AWS WAF apex:

```
connect-src 'self' https://*.awswaf.com;
script-src 'self' https://*.awswaf.com;
script-src-elem 'self' https://*.awswaf.com;
```

Jika Anda mencoba menggunakan JavaScript SDK dengan sumber daya yang menggunakan CSP, dan Anda belum mengizinkan daftar AWS WAF domain, Anda akan menerima kesalahan seperti berikut:

```
Refused to load the script ...awswaf.com/<> because it violates the following Content
 Security Policy directive: “script-src ‘self’
```

Menggunakan JavaScript API ancaman cerdas

API ancaman cerdas menyediakan operasi untuk menjalankan tantangan diam terhadap browser pengguna, dan untuk menangani AWS WAF token yang memberikan bukti tantangan yang berhasil dan respons CAPTCHA.

Terapkan JavaScript integrasi terlebih dahulu di lingkungan pengujian, kemudian dalam produksi. Untuk panduan pengkodean tambahan, lihat bagian berikut.

Untuk menggunakan API ancaman cerdas

1. Instal API

   Jika Anda menggunakan CAPTCHA API, Anda dapat melewati langkah ini. Saat Anda menginstal CAPTCHA API, skrip secara otomatis menginstal API ancaman cerdas.

   a. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.
   b. Di panel navigasi, pilih Integrasi aplikasi. Pada halaman Integrasi aplikasi, Anda dapat melihat opsi tab.
   c. Pilih Integrasi ancaman cerdas
   d. Di tab, pilih ACL web yang ingin Anda integrasikan. Daftar ACL web hanya mencakup ACL web yang menggunakan grup aturan `AWSManagedRulesACFPRuleSet` terkelola, grup aturan `AWSManagedRulesATPRuleSet` terkelola, atau tingkat perlindungan yang ditargetkan dari grup aturan `AWSManagedRulesBotControlRuleSet` terkelola.
   e. Buka panel JavaScript SDK, dan salin tag skrip untuk digunakan dalam integrasi Anda.
   f. Dalam kode halaman aplikasi Anda, di `<head>` bagian, masukkan tag skrip yang Anda salin untuk ACL web. Inklusi ini menyebabkan aplikasi klien Anda secara otomatis mengambil token di latar belakang pada pemuatan halaman.

      ```
      <head>
      ```

```
    <script type="text/javascript" src="Web ACL integration URL/challenge.js”
 defer></script>
<head>
```

`<script>`Daftar ini dikonfigurasi dengan `defer` atribut, tetapi Anda dapat mengubah pengaturan `async` jika Anda menginginkan perilaku yang berbeda untuk halaman Anda.

2. (Opsional) Tambahkan konfigurasi domain untuk token klien — Secara default, saat AWS WAF membuat token, ia menggunakan domain host dari sumber daya yang terkait dengan ACL web. Untuk menyediakan domain tambahan untuk JavaScript API, ikuti panduan diMenyediakan domain untuk digunakan dalam token.
3. Kode integrasi ancaman cerdas Anda — Tulis kode Anda untuk memastikan bahwa pengambilan token selesai sebelum klien mengirimkan permintaannya ke titik akhir yang dilindungi. Jika Anda sudah menggunakan `fetch` API untuk melakukan panggilan, Anda dapat mengganti `fetch` pembungkus AWS WAF integrasi. Jika Anda tidak menggunakan `fetch` API, Anda dapat menggunakan `getToken` operasi AWS WAF integrasi sebagai gantinya. Untuk panduan pengkodean, lihat bagian berikut.
4. Tambahkan verifikasi token di ACL web Anda — Tambahkan setidaknya satu aturan ke ACL web Anda yang memeriksa token tantangan yang valid dalam permintaan web yang dikirim klien Anda. Anda dapat menggunakan grup aturan yang memeriksa dan memantau token tantangan, seperti level target grup aturan terkelola Kontrol Bot, dan Anda dapat menggunakan tindakan Challenge aturan untuk memeriksa, seperti yang dijelaskan dalamCAPTCHAdan Challenge di AWS WAF.

   Penambahan ACL web memverifikasi bahwa permintaan ke titik akhir yang dilindungi menyertakan token yang telah Anda peroleh dalam integrasi klien Anda. Permintaan yang menyertakan token yang valid dan belum kedaluwarsa lulus Challenge inspeksi dan tidak mengirim tantangan diam lain kepada klien Anda.
5. (Opsional) Blokir permintaan yang tidak memiliki token — Jika Anda menggunakan API dengan grup aturan terkelola ACFP, grup aturan terkelola ATP, atau aturan yang ditargetkan dari grup aturan Kontrol Bot, aturan ini tidak memblokir permintaan yang tidak memiliki token. Untuk memblokir permintaan yang tidak memiliki token, ikuti panduan diMemblokir permintaan yang tidak memiliki AWS WAF token yang valid.

Topik

- Spesifikasi API ancaman cerdas
- Cara menggunakan fetch pembungkus integrasi

- Cara menggunakan integrasi getToken

Spesifikasi API ancaman cerdas

Bagian ini mencantumkan spesifikasi untuk metode dan properti API mitigasi JavaScript ancaman cerdas. Gunakan API ini untuk ancaman cerdas dan integrasi CAPTCHA.

`AwsWafIntegration.fetch()`

Mengirim `fetch` permintaan HTTP ke server menggunakan implementasi AWS WAF integrasi.

`AwsWafIntegration.getToken()`

Mengambil AWS WAF token yang disimpan dan menyimpannya dalam cookie pada halaman saat ini dengan nama`aws-waf-token`, dan nilai ditetapkan ke nilai token.

`AwsWafIntegration.hasToken()`

Mengembalikan boolean yang menunjukkan apakah `aws-waf-token` cookie saat ini memegang token yang belum kedaluwarsa.

Jika Anda juga menggunakan integrasi CAPTCHA, lihat spesifikasinya di. Spesifikasi CAPTCHA API JavaScript

Cara menggunakan **`fetch`** pembungkus integrasi

Anda dapat menggunakan AWS WAF `fetch` pembungkus dengan mengubah `fetch` panggilan normal Anda ke `fetch` API di bawah `AwsWafIntegration` namespace. AWS WAF Pembungkus mendukung semua opsi yang sama dengan panggilan JavaScript `fetch` API standar dan menambahkan penanganan token untuk integrasi. Pendekatan ini umumnya merupakan cara paling sederhana untuk mengintegrasikan aplikasi Anda.

Sebelum implementasi pembungkus

Daftar contoh berikut menunjukkan kode standar sebelum menerapkan `AwsWafIntegration` `fetch` pembungkus.

```
const login_response = await fetch(login_url, {
     method: 'POST',
     headers: {
       'Content-Type': 'application/json'
```

```
    },
    body: login_body
  });
```

Setelah implementasi pembungkus

Daftar berikut menunjukkan kode yang sama dengan implementasi `AwsWafIntegration` `fetch` wrapper.

```
const login_response = await AwsWafIntegration.fetch(login_url, {
    method: 'POST',
    headers: {
      'Content-Type': 'application/json'
    },
    body: login_body
  });
```

Cara menggunakan integrasi **`getToken`**

AWS WAF mengharuskan permintaan Anda ke titik akhir yang dilindungi untuk menyertakan cookie yang diberi nama `aws-waf-token` dengan nilai token Anda saat ini.

`getToken`Operasi ini adalah panggilan API asinkron yang mengambil AWS WAF token dan menyimpannya dalam cookie pada halaman saat ini dengan nama`aws-waf-token`, dan nilai yang ditetapkan ke nilai token. Anda dapat menggunakan cookie token ini sesuai kebutuhan di halaman Anda.

Saat Anda menelepon`getToken`, itu melakukan hal berikut:

- Jika token yang belum kedaluwarsa sudah tersedia, panggilan akan segera mengembalikannya.
- Jika tidak, panggilan akan mengambil token baru dari penyedia token, menunggu hingga 2 detik hingga alur kerja akuisisi token selesai sebelum waktu habis. Jika waktu operasi habis, itu akan menimbulkan kesalahan, yang harus ditangani oleh kode panggilan Anda.

`getToken`Operasi ini memiliki operasi yang menyertainya`hasToken`, yang menunjukkan apakah `aws-waf-token` cookie saat ini memegang token yang belum kedaluwarsa.

`AwsWafIntegration.getToken()`mengambil token yang valid dan menyimpannya sebagai cookie. Sebagian besar panggilan klien secara otomatis melampirkan cookie ini, tetapi beberapa tidak. Misalnya, panggilan yang dilakukan di seluruh domain host tidak melampirkan cookie. Dalam

detail implementasi yang mengikuti, kami menunjukkan cara bekerja dengan kedua jenis panggilan klien.

`getToken`Implementasi dasar, untuk panggilan yang melampirkan **`aws-waf-token`** cookie

Daftar contoh berikut menunjukkan kode standar untuk mengimplementasikan `getToken` operasi dengan permintaan login.

```
const login_response = await AwsWafIntegration.getToken()
     .catch(e => {
         // Implement error handling logic for your use case
     })
     // The getToken call returns the token, and doesn't typically require special
 handling
     .then(token => {
         return loginToMyPage()
     })

 async function loginToMyPage() {
     // Your existing login code
 }
```

Kirim formulir hanya setelah token tersedia dari **`getToken`**

Daftar berikut menunjukkan cara mendaftarkan pendengar acara untuk mencegat kiriman formulir hingga token yang valid tersedia untuk digunakan.

```
<body>
   <h1>Login</h1>
   <p></p>
   <form id="login-form" action="/web/login" method="POST" enctype="application/x-www-
form-urlencoded">
     <label for="input_username">USERNAME</label>
     <input type="text" name="input_username" id="input_username"><br>
     <label for="input_password">PASSWORD</label>
     <input type="password" name="input_password" id="input_password"><br>
     <button type="submit">Submit<button>
   </form>

 <script>
   const form = document.querySelector("#login-form");

   // Register an event listener to intercept form submissions
```

```
   form.addEventListener("submit", (e) => {
       // Submit the form only after a token is available
       if (!AwsWafIntegration.hasToken()) {
           e.preventDefault();
           AwsWafIntegration.getToken().then(() => {
               e.target.submit();
           }, (reason) => { console.log("Error:"+reason) });
         }
     });
 </script>
 </body>
```

Melampirkan token saat klien Anda tidak melampirkan **`aws-waf-token`** cookie secara default

`AwsWafIntegration.getToken()`mengambil token yang valid dan menyimpannya sebagai cookie, tetapi tidak semua panggilan klien melampirkan cookie ini secara default. Misalnya, panggilan yang dilakukan di seluruh domain host tidak melampirkan cookie.

`fetch`Pembungkus menangani kasus ini secara otomatis, tetapi jika Anda tidak dapat menggunakan `fetch` pembungkus, Anda dapat menangani ini dengan menggunakan header khususx-aws-waf-token. AWS WAF membaca token dari header ini, selain membacanya dari `aws-waf-token` cookie. Kode berikut menunjukkan contoh pengaturan header.

```
const token = await AwsWafIntegration.getToken();
const result = await fetch('/url', {
    headers: {
        'x-aws-waf-token': token,
    },
});
```

Secara default, AWS WAF hanya menerima token yang berisi domain yang sama dengan domain host yang diminta. Setiap token lintas domain memerlukan entri yang sesuai dalam daftar domain token ACL web. Untuk informasi selengkapnya, lihat AWS WAF konfigurasi daftar domain token ACL web.

Untuk informasi tambahan tentang penggunaan token lintas domain, lihat aws-waf-bot-controlaws-samples/ -. api-protection-with-captcha

Menggunakan JavaScript CAPTCHA API

CAPTCHA JavaScript API memungkinkan Anda untuk mengkonfigurasi teka-teki CAPTCHA dan menempatkannya di tempat yang Anda inginkan dalam aplikasi klien Anda. API ini memanfaatkan

fitur JavaScript API ancaman cerdas untuk memperoleh dan menggunakan AWS WAF token setelah pengguna akhir berhasil menyelesaikan teka-teki CAPTCHA.

Terapkan JavaScript integrasi terlebih dahulu di lingkungan pengujian, kemudian dalam produksi. Untuk panduan pengkodean tambahan, lihat bagian berikut.

Untuk menggunakan API integrasi CAPTCHA

1. Instal API

   a. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   b. Di panel navigasi, pilih Integrasi aplikasi. Pada halaman Integrasi aplikasi, Anda dapat melihat opsi tab.

   c. Pilih integrasi CAPTCHA.

   d. Salin tag skrip JavaScript integrasi yang terdaftar untuk digunakan dalam integrasi Anda.

   e. Dalam kode halaman aplikasi Anda, di `<head>` bagian, masukkan tag skrip yang Anda salin. Inklusi ini membuat teka-teki CAPTCHA tersedia untuk konfigurasi dan penggunaan.

   ```
   <head>
       <script type="text/javascript" src="integrationURL/jsapi.js" defer></
   script>
   </head>
   ```

   `<script>`Daftar ini dikonfigurasi dengan `defer` atribut, tetapi Anda dapat mengubah pengaturan `async` jika Anda menginginkan perilaku yang berbeda untuk halaman Anda.

   Skrip CAPTCHA juga secara otomatis memuat skrip integrasi ancaman cerdas jika belum ada. Skrip integrasi ancaman cerdas menyebabkan aplikasi klien Anda secara otomatis mengambil token di latar belakang pada pemuatan halaman, dan menyediakan fungsionalitas manajemen token lain yang Anda butuhkan untuk penggunaan CAPTCHA API.

2. (Opsional) Tambahkan konfigurasi domain untuk token klien — Secara default, saat AWS WAF membuat token, ia menggunakan domain host dari sumber daya yang terkait dengan ACL web. Untuk menyediakan domain tambahan untuk JavaScript API, ikuti panduan diMenyediakan domain untuk digunakan dalam token.

3. Dapatkan kunci API terenkripsi untuk klien — CAPTCHA API memerlukan kunci API terenkripsi yang berisi daftar domain klien yang valid. AWS WAF menggunakan kunci ini

untuk memverifikasi bahwa domain klien yang Anda gunakan dengan integrasi disetujui untuk menggunakan AWS WAF CAPTCHA. Untuk membuat kunci API Anda, ikuti panduan diMengelola kunci API untuk JS CAPTCHA API.

4. Kode implementasi widget CAPTCHA Anda - Terapkan panggilan `renderCaptcha()` API di halaman Anda, di lokasi di mana Anda ingin menggunakannya. Untuk informasi tentang mengkonfigurasi dan menggunakan fungsi ini, lihat bagian berikut, Spesifikasi CAPTCHA API JavaScript dan Cara membuat teka-teki CAPTCHA.

   Implementasi CAPTCHA terintegrasi dengan API integrasi ancaman cerdas untuk manajemen token dan menjalankan panggilan pengambilan yang menggunakan token. AWS WAF Untuk panduan tentang penggunaan API ini, lihatMenggunakan JavaScript API ancaman cerdas.

5. Tambahkan verifikasi token di ACL web Anda — Tambahkan setidaknya satu aturan ke ACL web Anda yang memeriksa token CAPTCHA yang valid dalam permintaan web yang dikirim klien Anda. Anda dapat menggunakan tindakan CAPTCHA aturan untuk memeriksa, seperti yang dijelaskan dalamCAPTCHAdan Challenge di AWS WAF.

   Penambahan ACL web memverifikasi bahwa permintaan yang masuk ke titik akhir yang dilindungi menyertakan token yang telah Anda peroleh dalam integrasi klien Anda. Permintaan yang menyertakan token CAPTCHA yang valid dan belum kedaluwarsa lulus inspeksi tindakan CAPTCHA aturan dan tidak menghadirkan teka-teki CAPTCHA lain kepada pengguna akhir Anda.

Topik

- Spesifikasi CAPTCHA API JavaScript
- Cara membuat teka-teki CAPTCHA
- Menangani respons CAPTCHA dari AWS WAF
- Mengelola kunci API untuk JS CAPTCHA API

Spesifikasi CAPTCHA API JavaScript

Bagian ini mencantumkan spesifikasi untuk metode dan properti CAPTCHA API JavaScript . Gunakan CAPTCHA JavaScript API untuk menjalankan teka-teki CAPTCHA khusus di aplikasi klien Anda.

API ini dibangun di atas API ancaman cerdas, yang Anda gunakan untuk mengonfigurasi dan mengelola akuisisi dan penggunaan AWS WAF token. LihatSpesifikasi API ancaman cerdas.

`AwsWafCaptcha.renderCaptcha(container, configuration)`

Menyajikan teka-teki AWS WAF CAPTCHA kepada pengguna akhir dan, setelah berhasil, memperbarui token klien dengan validasi CAPTCHA. Ini hanya tersedia dengan integrasi CAPTCHA. Gunakan panggilan ini bersama dengan API ancaman cerdas untuk mengelola pengambilan token dan menyediakan token dalam `fetch` panggilan Anda. Lihat API ancaman cerdas diSpesifikasi API ancaman cerdas.

Berbeda dengan pengantara CAPTCHA yang AWS WAF mengirim, teka-teki CAPTCHA yang diberikan oleh metode ini menampilkan teka-teki segera, tanpa layar judul awal.

`container`

`Element`Objek untuk elemen kontainer target pada halaman. Ini biasanya diambil dengan menelepon `document.getElementById()` ataudocument.querySelector().

Diperlukan: Ya

Tipe: `Element`

konfigurasi

Objek yang berisi pengaturan konfigurasi CAPTCHA, sebagai berikut:

`apiKey`

Kunci API terenkripsi yang memungkinkan izin untuk domain klien. Gunakan AWS WAF konsol untuk membuat kunci API Anda untuk domain klien Anda. Anda dapat menggunakan satu kunci hingga lima domain. Untuk informasi, lihat Mengelola kunci API untuk JS CAPTCHA API.

Diperlukan: Ya

Tipe: `string`

`onSuccess: (wafToken: string) => void;`

Dipanggil dengan AWS WAF token yang valid ketika pengguna akhir berhasil menyelesaikan teka-teki CAPTCHA. Gunakan token dalam permintaan yang Anda kirim ke titik akhir yang Anda lindungi dengan ACL AWS WAF web. Token memberikan bukti dan stempel waktu penyelesaian teka-teki terbaru yang berhasil.

Diperlukan: Ya

`onError?: (error: CaptchaError) => void;`

Dipanggil dengan objek kesalahan ketika terjadi kesalahan selama operasi CAPTCHA.

Diperlukan: Tidak

`CaptchaError`definisi kelas - `onError` Handler menyediakan jenis kesalahan dengan definisi kelas berikut.

```
CaptchaError extends Error {
    kind: "internal_error" | "network_error" | "token_error" | "client_error";
    statusCode?: number;
}
```

- `kind`— Jenis kesalahan yang dikembalikan.
- `statusCode`— Kode status HTTP, jika tersedia. Ini digunakan oleh `network_error` jika kesalahan disebabkan oleh kesalahan HTTP.

`onLoad?: () => void;`

Dipanggil ketika teka-teki CAPTCHA baru dimuat.

Diperlukan: Tidak

`onPuzzleTimeout?: () => void;`

Dipanggil ketika teka-teki CAPTCHA tidak selesai sebelum kedaluwarsa.

Diperlukan: Tidak

`onPuzzleCorrect?: () => void;`

Dipanggil ketika jawaban yang benar diberikan untuk teka-teki CAPTCHA.

Diperlukan: Tidak

`onPuzzleIncorrect?: () => void;`

Dipanggil ketika jawaban yang salah diberikan untuk teka-teki CAPTCHA.

Diperlukan: Tidak

`defaultLocale`

Lokal default yang digunakan untuk teka-teki CAPTCHA. Instruksi tertulis untuk teka-teki CAPTCHA tersedia dalam bahasa Arab (ar-sa), bahasa Mandarin sederhana (Zh-CN),

Belanda (nl-NL), Inggris (en-US), Prancis (fr-Fr), Jerman (de-DE), Italia (IT-it), Jepang (Ja-jp), Portugis Brasil (Pt-BR), Spanyol (es-ES), dan Turki (Tr-tr). Instruksi audio tersedia untuk semua bahasa tertulis kecuali bahasa Mandarin dan Jepang, yang default ke bahasa Inggris. Untuk mengubah bahasa default, berikan bahasa internasional dan kode lokal, misalnya,`ar-SA`.

Default: Bahasa yang saat ini digunakan di browser pengguna akhir

Diperlukan: Tidak

Tipe: `string`

`disableLanguageSelector`

Jika diatur ke`true`, teka-teki CAPTCHA menyembunyikan pemilih bahasa.

Default: `false`

Diperlukan: Tidak

Tipe: `boolean`

`dynamicWidth`

Jika diatur ke`true`, teka-teki CAPTCHA mengubah lebar untuk kompatibilitas dengan lebar jendela browser.

Default: `false`

Diperlukan: Tidak

Tipe: `boolean`

`skipTitle`

Jika diatur ke`true`, teka-teki CAPTCHA tidak menampilkan judul puzzle Pecahkan teka-teki.

Default: `false`

Diperlukan: Tidak

Tipe: `boolean`

Cara membuat teka-teki CAPTCHA

Anda dapat menggunakan AWS WAF `renderCaptcha` panggilan di mana Anda ingin di antarmuka klien Anda. Panggilan mengambil teka-teki CAPTCHA dari AWS WAF, merendernya, dan mengirimkan hasilnya untuk verifikasi. AWS WAF Saat Anda melakukan panggilan, Anda menyediakan konfigurasi rendering teka-teki dan panggilan balik yang ingin Anda jalankan saat pengguna akhir menyelesaikan teka-teki. Untuk detail tentang opsi, lihat bagian sebelumnya,. Spesifikasi CAPTCHA API JavaScript

Gunakan panggilan ini bersama dengan fungsionalitas manajemen token dari API integrasi ancaman cerdas. Panggilan ini memberi klien Anda token yang memverifikasi keberhasilan penyelesaian teka-teki CAPTCHA. Gunakan API integrasi ancaman cerdas untuk mengelola token dan untuk menyediakan token dalam panggilan klien Anda ke titik akhir yang dilindungi dengan ACL AWS WAF web. Untuk informasi tentang API ancaman cerdas, lihatMenggunakan JavaScript API ancaman cerdas.

Contoh implementasi

Daftar contoh berikut menunjukkan implementasi CAPTCHA standar, termasuk penempatan URL AWS WAF integrasi di bagian`<head>`.

Daftar ini mengonfigurasi `renderCaptcha` fungsi dengan callback sukses yang menggunakan `AwsWafIntegration.fetch` pembungkus API integrasi ancaman cerdas. Untuk informasi tentang fungsi ini, lihatCara menggunakan `fetch` pembungkus integrasi.

```
<head>
    <script type="text/javascript" src="<Integration URL>/jsapi.js" defer></script>
</head>

<script type="text/javascript">
    function showMyCaptcha() {
        var container = document.querySelector("#my-captcha-container");

        AwsWafCaptcha.renderCaptcha(container, {
            apiKey: "...API key goes here...",
            onSuccess: captchaExampleSuccessFunction,
            onError: captchaExampleErrorFunction,
            ...other configuration parameters as needed...
        });
    }
```

```
    function captchaExampleSuccessFunction(wafToken) {
        // Captcha completed. wafToken contains a valid WAF token. Store it for
        // use later or call AwsWafIntegration.fetch() to use it easily.
        // It will expire after a time, so calling AwsWafIntegration.getToken()
        // again is advised if the token is needed later on, outside of using the
        // fetch wrapper.

        // Use WAF token to access protected resources
        AwsWafIntegration.fetch("...WAF-protected URL...", {
            method: "POST",
            headers: {
                "Content-Type": "application/json",
            },
            body: "{ ... }" /* body content */
        });
    }

    function captchaExampleErrorFunction(error) {
        /* Do something with the error */
    }
</script>

<div id="my-captcha-container">
    <!-- The contents of this container will be replaced by the captcha widget -->
</div>
```

Contoh pengaturan konfigurasi

Contoh daftar berikut menunjukkan `renderCaptcha` dengan pengaturan non-default untuk lebar dan pilihan judul.

```
        AwsWafCaptcha.renderCaptcha(container, {
            apiKey: "...API key goes here...",
            onSuccess: captchaExampleSuccessFunction,
            onError: captchaExampleErrorFunction,
            dynamicWidth: true,
            skipTitle: true
        });
```

Untuk informasi selengkapnya tentang opsi konfigurasi, lihatSpesifikasi CAPTCHA API JavaScript .

Menangani respons CAPTCHA dari AWS WAF

AWS WAF Aturan dengan CAPTCHA tindakan menghentikan evaluasi permintaan web yang cocok jika permintaan tidak memiliki token dengan stempel waktu CAPTCHA yang valid. Jika permintaan adalah panggilan `GET` teks/html, CAPTCHA tindakan kemudian melayani klien pengantara dengan teka-teki CAPTCHA. Ketika Anda tidak mengintegrasikan CAPTCHA JavaScript API, pengantara menjalankan teka-teki dan, jika pengguna akhir berhasil menyelesaikannya, secara otomatis mengirimkan kembali permintaan.

Saat Anda mengintegrasikan CAPTCHA JavaScript API dan menyesuaikan penanganan CAPTCHA Anda, Anda perlu mendeteksi respons CAPTCHA yang mengakhiri, menyajikan CAPTCHA kustom Anda, dan kemudian jika pengguna akhir berhasil memecahkan teka-teki, kirimkan kembali permintaan web klien.

Contoh kode berikut ini menunjukkan cara untuk melakukannya.

> **Note**
>
> Respons AWS WAF CAPTCHA tindakan memiliki kode status HTTP 405, yang kami gunakan untuk mengenali CAPTCHA respons dalam kode ini. Jika titik akhir Anda yang dilindungi menggunakan kode status HTTP 405 untuk mengkomunikasikan jenis respons lain untuk panggilan yang sama, kode contoh ini akan membuat teka-teki CAPTCHA untuk tanggapan tersebut juga.

```
<!DOCTYPE html>
<html>
<head>
    <script type="text/javascript" src="<Integration URL>/jsapi.js" defer></script>
</head>
<body>
    <div id="my-captcha-box"></div>
    <div id="my-output-box"></div>

    <script type="text/javascript">
    async function loadData() {
        // Attempt to fetch a resource that's configured to trigger a CAPTCHA
        // action if the rule matches. The CAPTCHA response has status=HTTP 405.
        const result = await AwsWafIntegration.fetch("/protected-resource");
```

```
        // If the action was CAPTCHA, render the CAPTCHA and return

        // NOTE: If the endpoint you're calling in the fetch call responds with HTTP
 405
        // as an expected response status code, then this check won't be able to tell
 the
        // difference between that and the CAPTCHA rule action response.

        if (result.status === 405) {
            const container = document.querySelector("#my-captcha-box");
            AwsWafCaptcha.renderCaptcha(container, {
                apiKey: "...API key goes here...",
                onSuccess() {
                    // Try loading again, now that there is a valid CAPTCHA token
                    loadData();
                },
            });
            return;
        }

        const container = document.querySelector("#my-output-box");
        const response = await result.text();
        container.innerHTML = response;
    }

    window.addEventListener("load", () => {
        loadData();
    });
    </script>
</body>
</html>
```

Mengelola kunci API untuk JS CAPTCHA API

Untuk mengintegrasikan AWS WAF CAPTCHA ke dalam aplikasi klien dengan JavaScript API, Anda memerlukan tag integrasi JavaScript API dan kunci API terenkripsi untuk domain klien tempat Anda ingin menjalankan teka-teki CAPTCHA Anda.

Integrasi aplikasi CAPTCHA untuk JavaScript menggunakan kunci API terenkripsi untuk memverifikasi bahwa domain aplikasi klien memiliki izin untuk menggunakan CAPTCHA API. AWS WAF Ketika Anda memanggil CAPTCHA API dari JavaScript klien Anda, Anda menyediakan kunci API dengan daftar domain yang menyertakan domain untuk klien saat ini. Anda dapat mencantumkan hingga 5 domain dalam satu kunci terenkripsi.

Persyaratan kunci API

Kunci API yang Anda gunakan dalam integrasi CAPTCHA harus berisi domain yang berlaku untuk klien tempat Anda menggunakan kunci tersebut.

- Jika Anda menentukan a `window.awsWafCookieDomainList` dalam integrasi ancaman cerdas klien Anda, maka setidaknya satu domain dalam kunci API Anda harus sama persis dengan salah satu domain token di dalamnya `window.awsWafCookieDomainList` atau itu harus menjadi domain puncak dari salah satu domain token tersebut.

  Misalnya, untuk domain token`mySubdomain.myApex.com`, kunci `mySubdomain.myApex.com` API sama persis dan kunci API `myApex.com` adalah domain apex. Salah satu kunci cocok dengan domain token.

  Untuk informasi tentang pengaturan daftar domain token, lihatMenyediakan domain untuk digunakan dalam token.
- Jika tidak, domain saat ini harus terkandung dalam kunci API. Domain saat ini adalah domain yang dapat Anda lihat di bilah alamat browser.

Domain yang Anda gunakan haruslah yang AWS WAF akan menerima, berdasarkan domain host yang dilindungi dan daftar domain token yang dikonfigurasi untuk ACL web. Untuk informasi selengkapnya, lihat AWS WAF konfigurasi daftar domain token ACL web.

Cara memilih Region untuk kunci API Anda

AWS WAF dapat menghasilkan kunci API CAPTCHA di Wilayah mana pun yang AWS WAF tersedia.

Sebagai aturan umum, Anda harus menggunakan Wilayah yang sama untuk kunci API CAPTCHA Anda seperti yang Anda gunakan untuk ACL web Anda. Namun, jika Anda mengharapkan audiens global untuk ACL web regional, Anda dapat memperoleh tag JavaScript integrasi CAPTCHA yang dicakup CloudFront dan kunci API yang dicakup CloudFront, dan menggunakannya dengan ACL web regional. Pendekatan ini memungkinkan klien memuat teka-teki CAPTCHA dari Wilayah yang paling dekat dengan mereka, yang mengurangi latensi.

Kunci API CAPTCHA yang dicakup ke Wilayah selain tidak didukung untuk digunakan CloudFront di beberapa Wilayah. Mereka hanya dapat digunakan di Wilayah yang mereka cakupkan.

Untuk menghasilkan kunci API untuk domain klien Anda

Untuk mendapatkan URL integrasi dan menghasilkan serta mengambil kunci API melalui konsol.

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.
2. Di panel navigasi, pilih Integrasi aplikasi.
3. Di panel, Web ACL yang diaktifkan untuk integrasi aplikasi, pilih Wilayah yang ingin Anda gunakan untuk kunci API Anda. Anda juga dapat memilih Wilayah di panel kunci API pada tab integrasi CAPTCHA.
4. Pilih tab Integrasi CAPTCHA. Tab ini menyediakan tag JavaScript integrasi CAPTCHA, yang dapat Anda gunakan dalam integrasi Anda, dan daftar kunci API. Keduanya tercakup ke Wilayah yang dipilih.
5. Di panel kunci API, pilih Generate key. Dialog generasi kunci muncul.
6. Masukkan domain klien yang ingin Anda sertakan dalam kunci. Anda dapat memasukkan hingga 5. Setelah selesai, pilih Generate key. Antarmuka kembali ke tab integrasi CAPTCHA, di mana kunci baru Anda terdaftar.

   Setelah dibuat, kunci API tidak dapat diubah. Jika Anda perlu membuat perubahan pada kunci, buat kunci baru dan gunakan itu sebagai gantinya.
7. (Opsional) Salin kunci yang baru dibuat untuk digunakan dalam integrasi Anda.

Anda juga dapat menggunakan REST API atau salah satu AWS SDK khusus bahasa untuk pekerjaan ini. Panggilan REST API adalah createApiKey dan ListApiKeys.

Untuk menghapus kunci API

Untuk menghapus kunci API, Anda harus menggunakan REST API atau salah satu AWS SDK khusus bahasa. Panggilan REST API adalah deleteApiKey. Anda tidak dapat menggunakan konsol untuk menghapus kunci.

Setelah Anda menghapus kunci, diperlukan waktu hingga 24 jam AWS WAF untuk melarang penggunaan kunci di semua wilayah.

AWS WAF integrasi aplikasi seluler

Anda dapat menggunakan SDK AWS WAF seluler untuk menerapkan SDK integrasi ancaman AWS WAF cerdas untuk aplikasi seluler Android dan iOS.

- Untuk aplikasi seluler Android, AWS WAF SDK berfungsi untuk Android API versi 23 (Android versi 6) dan yang lebih baru. Untuk informasi tentang versi Android, lihat catatan rilis SDK Platform.

- Untuk aplikasi seluler iOS, AWS WAF SDK berfungsi untuk iOS versi 13 dan yang lebih baru. Untuk informasi tentang versi iOS, lihat Catatan Rilis iOS & iPadOS.

Dengan SDK seluler, Anda dapat mengelola otorisasi token, dan menyertakan token dalam permintaan yang Anda kirim ke sumber daya yang dilindungi. Dengan menggunakan SDK, Anda memastikan bahwa panggilan prosedur jarak jauh ini oleh klien Anda berisi token yang valid. Selain itu, ketika integrasi ini diterapkan pada halaman aplikasi Anda, Anda dapat menerapkan aturan mitigasi di ACL web Anda, seperti memblokir permintaan yang tidak berisi token yang valid.

Untuk akses ke SDK seluler, hubungi dukungan di Kontak AWS.

> **Note**
>
> SDK AWS WAF seluler tidak tersedia untuk kustomisasi CAPTCHA.

Pendekatan dasar untuk menggunakan SDK adalah membuat penyedia token menggunakan objek konfigurasi, kemudian menggunakan penyedia token untuk mengambil token dari. AWS WAF Secara default, penyedia token menyertakan token yang diambil dalam permintaan web Anda ke sumber daya yang dilindungi.

Berikut ini adalah sebagian daftar implementasi SDK, yang menunjukkan komponen utama. Untuk contoh lebih detail, lihat Menulis kode Anda untuk SDK AWS WAF seluler.

iOS

```
let url: URL = URL(string: "Web ACL integration URL")!
 let configuration = WAFConfiguration(applicationIntegrationUrl: url, domainName:
 "Domain name")
 let tokenProvider = WAFTokenProvider(configuration)
 let token = tokenProvider.getToken()
```

Android

```
URL applicationIntegrationURL = new URL("Web ACL integration URL");
 String domainName = "Domain name";
 WAFConfiguration configuration =
 WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL).domainName(
```

```
WAFTokenProvider tokenProvider = new WAFTokenProvider(Application context,
configuration);
WAFToken token = tokenProvider.getToken();
```

Menginstal SDK AWS WAF seluler

Untuk akses ke SDK seluler, hubungi dukungan di Kontak AWS.

Terapkan SDK seluler terlebih dahulu di lingkungan pengujian, kemudian dalam produksi.

Untuk menginstal SDK AWS WAF seluler

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.
2. Di panel navigasi, pilih Integrasi aplikasi.
3. Di tab Integrasi ancaman cerdas, lakukan hal berikut:
   a. Di panel Web ACL yang diaktifkan untuk integrasi aplikasi, cari ACL web yang Anda integrasikan. Salin dan simpan URL integrasi ACL web untuk digunakan dalam implementasi Anda. Anda juga dapat memperoleh URL ini melalui panggilan API`GetWebACL`.
   b. Pilih jenis dan versi perangkat seluler, lalu pilih Unduh. Anda dapat memilih versi apa pun yang Anda suka, tetapi kami sarankan menggunakan versi terbaru. AWS WAF mengunduh `zip` file untuk perangkat Anda ke lokasi unduhan standar Anda.
4. Di lingkungan pengembangan aplikasi Anda, unzip file ke lokasi kerja pilihan Anda. Di direktori tingkat atas file zip, cari dan buka file. `README` Ikuti petunjuk dalam `README` file untuk menginstal SDK AWS WAF seluler untuk digunakan dalam kode aplikasi seluler Anda.
5. Program aplikasi Anda sesuai dengan panduan di bagian berikut.

Spesifikasi SDK AWS WAF seluler

Bagian ini mencantumkan objek SDK, operasi, dan pengaturan konfigurasi untuk versi SDK AWS WAF seluler terbaru yang tersedia. Untuk informasi terperinci tentang cara kerja penyedia token dan operasi untuk berbagai kombinasi pengaturan konfigurasi, lihatCara kerja SDK AWS WAF seluler.

`WAFToken`

Memegang AWS WAF token.

`getValue()`

Mengambil `String` representasi dari. `WAFToken`

`WAFTokenProvider`

Mengelola token di aplikasi seluler Anda. Terapkan ini menggunakan `WAFConfiguration` objek.

`getToken()`

Jika penyegaran latar belakang diaktifkan, ini mengembalikan token yang di-cache. Jika penyegaran latar belakang dinonaktifkan, ini membuat panggilan pemblokiran sinkron AWS WAF untuk mengambil token baru.

`onTokenReady(WAFTokenResultCallback)`

Menginstruksikan penyedia token untuk menyegarkan token dan memanggil panggilan balik yang disediakan saat token aktif siap. Penyedia token akan memanggil panggilan balik Anda di utas latar belakang saat token di-cache dan siap. Panggil ini saat aplikasi Anda pertama kali dimuat dan juga saat kembali ke status aktif. Untuk informasi selengkapnya tentang kembali ke status aktif, lihatthe section called “Mengambil token setelah aplikasi tidak aktif”.

Untuk aplikasi Android atau iOS, Anda dapat mengatur `WAFTokenResultCallback` ke operasi yang ingin dijalankan oleh penyedia token saat token yang diminta sudah siap. Implementasi Anda `WAFTokenResultCallback` harus mengambil parameter`WAFToken`,`SdkError`. Untuk aplikasi iOS, Anda dapat membuat fungsi inline secara bergantian.

`storeTokenInCookieStorage(WAFToken)`

Menginstruksikan `WAFTokenProvider` untuk menyimpan AWS WAF token yang ditentukan ke dalam manajer cookie SDK. Secara default, token hanya ditambahkan ke toko cookie saat pertama kali diperoleh dan saat di-refresh. Jika aplikasi menghapus penyimpanan cookie bersama karena alasan apa pun, SDK tidak secara otomatis menambahkan AWS WAF token kembali hingga penyegaran berikutnya.

`WAFConfiguration`

Memegang konfigurasi untuk implementasi`WAFTokenProvider`. Saat Anda menerapkan ini, Anda memberikan URL integrasi ACL web Anda, nama domain yang akan digunakan dalam

token, dan pengaturan non-default apa pun yang Anda inginkan untuk digunakan oleh penyedia token.

Daftar berikut menentukan pengaturan konfigurasi yang dapat Anda kelola dalam `WAFConfiguration` objek.

`applicationIntegrationUrl`

URL integrasi aplikasi. Dapatkan ini dari AWS WAF konsol atau melalui panggilan `getWebACL` API.

Diperlukan: Ya

Jenis: URL khusus aplikasi. Untuk iOS, lihat URL iOS. Untuk Android, lihat URL java.net.

`backgroundRefreshEnabled`

Menunjukkan apakah Anda ingin penyedia token menyegarkan token di latar belakang. Jika Anda menyetel ini, penyedia token akan menyegarkan token Anda di latar belakang sesuai dengan pengaturan konfigurasi yang mengatur aktivitas penyegaran token otomatis.

Diperlukan: Tidak

Tipe: `Boolean`

Nilai default: `TRUE`

`domainName`

Domain yang akan digunakan dalam token, yang digunakan dalam akuisisi token dan penyimpanan cookie. Misalnya, `example.com` atau `aws.amazon.com`. Ini biasanya domain host dari sumber daya Anda yang terkait dengan ACL web, tempat Anda akan mengirim permintaan web. Untuk grup aturan terkelola `ACFPAWSManagedRulesACFPRuleSet`, ini biasanya akan menjadi domain tunggal yang cocok dengan domain di jalur pembuatan akun yang Anda berikan dalam konfigurasi grup aturan. Untuk grup aturan terkelola `ATPAWSManagedRulesATPRuleSet`, ini biasanya akan menjadi domain tunggal yang cocok dengan domain di jalur login yang Anda berikan dalam konfigurasi grup aturan.

Sufiks publik tidak diizinkan. Misalnya, Anda tidak dapat menggunakan `gov.au` atau `co.uk` sebagai domain token.

Domain harus menjadi salah satu yang AWS WAF akan menerima, berdasarkan domain host yang dilindungi dan daftar domain token ACL web. Untuk informasi selengkapnya, lihat AWS WAF konfigurasi daftar domain token ACL web.

Diperlukan: Ya

Tipe: `String`

`maxErrorTokenRefreshDelayMsec`

Waktu maksimum dalam milidetik untuk menunggu sebelum mengulangi penyegaran token setelah upaya gagal. Nilai ini digunakan setelah pengambilan token gagal dan berulang kali dicoba`maxRetryCount`.

Diperlukan: Tidak

Tipe: `Integer`

Nilai default: `5000` (5 detik)

Nilai minimum yang diizinkan: `1` (1 milidetik)

Nilai maksimum yang diizinkan: `30000` (30 detik)

`maxRetryCount`

Jumlah maksimum percobaan ulang untuk dilakukan dengan backoff eksponensial ketika token diminta.

Diperlukan: Tidak

Tipe: `Integer`

Nilai default: Jika penyegaran latar belakang diaktifkan,`5`. Atau, `3`.

Nilai minimum yang diizinkan: `0`

Nilai maksimum yang diizinkan: `10`

`setTokenCookie`

Menunjukkan apakah Anda ingin pengelola cookie SDK menambahkan cookie token dalam permintaan Anda. Secara default, ini menambahkan cookie token ke semua permintaan. Manajer cookie menambahkan cookie token ke permintaan apa pun yang jalurnya berada di bawah jalur yang ditentukan dalam`tokenCookiePath`.

Diperlukan: Tidak

Tipe: `Boolean`

Nilai default: TRUE

`tokenCookiePath`

Digunakan kapan `setTokenCookie`TRUE. Menunjukkan jalur tingkat atas tempat Anda ingin pengelola cookie SDK menambahkan cookie token. Manajer menambahkan cookie token ke semua permintaan yang Anda kirim ke jalur ini dan ke semua jalur anak.

Misalnya, jika Anda menyetel ini`/web/login`, maka manajer menyertakan cookie token untuk semua yang dikirim ke `/web/login` dan jalur turunannya, seperti`/web/login/help`. Itu tidak termasuk token untuk permintaan yang dikirim ke jalur lain, seperti`/`,`/web`, atau`/web/order`.

Diperlukan: Tidak

Tipe: `String`

Nilai default: `/`

`tokenRefreshDelaySec`

Digunakan untuk penyegaran latar belakang. Jumlah waktu maksimum dalam hitungan detik antara token latar belakang menyegarkan.

Diperlukan: Tidak

Tipe: `Integer`

Nilai default: 88

Nilai minimum yang diizinkan: 88

Nilai maksimum yang diizinkan: `300` (5 menit)

Cara kerja SDK AWS WAF seluler

SDK seluler memberi Anda penyedia token yang dapat dikonfigurasi yang dapat Anda gunakan untuk pengambilan dan penggunaan token. Penyedia token memverifikasi bahwa permintaan yang Anda izinkan berasal dari pelanggan yang sah. Saat Anda mengirim permintaan ke AWS sumber daya yang Anda lindungi AWS WAF, Anda menyertakan token dalam cookie, untuk memvalidasi permintaan tersebut. Anda dapat menangani cookie token secara manual atau meminta penyedia token melakukannya untuk Anda.

Bagian ini mencakup interaksi antara kelas, properti, dan metode yang disertakan dalam SDK seluler. Untuk spesifikasi SDK, lihatSpesifikasi SDK AWS WAF seluler.

Pengambilan dan caching token

Saat membuat instance penyedia token di aplikasi seluler, Anda mengonfigurasi cara mengelola token dan pengambilan token. Pilihan utama Anda adalah cara mempertahankan token yang valid dan belum kedaluwarsa untuk digunakan dalam permintaan web aplikasi Anda:

- Penyegaran latar belakang diaktifkan - Ini adalah default. Penyedia token secara otomatis menyegarkan token di latar belakang dan menyimpannya dalam cache. Dengan penyegaran latar belakang diaktifkan, saat Anda menelepon`getToken()`, operasi mengambil token yang di-cache.

  Penyedia token melakukan penyegaran token pada interval yang dapat dikonfigurasi, sehingga token yang belum kedaluwarsa selalu tersedia di cache saat aplikasi aktif. Penyegaran latar belakang dijeda saat aplikasi Anda dalam keadaan tidak aktif. Untuk informasi tentang ini, lihatMengambil token setelah aplikasi tidak aktif.
- Penyegaran latar belakang dinonaktifkan — Anda dapat menonaktifkan penyegaran token latar belakang, dan kemudian mengambil token hanya sesuai permintaan. Token yang diambil sesuai permintaan tidak di-cache, dan Anda dapat mengambil lebih dari satu jika Anda mau. Setiap token independen dari token lain yang Anda ambil, dan masing-masing memiliki stempel waktu sendiri yang digunakan untuk menghitung kedaluwarsa.

  Anda memiliki pilihan berikut untuk pengambilan token saat penyegaran latar belakang dinonaktifkan:

  - **`getToken()`**— Saat Anda menelepon `getToken()` dengan penyegaran latar belakang dinonaktifkan, panggilan secara sinkron mengambil token baru dari. AWS WAF Ini adalah panggilan yang berpotensi memblokir yang dapat memengaruhi respons aplikasi jika Anda memanggilnya di utas utama.
  - **`onTokenReady(WAFTokenResultCallback)`**— Panggilan ini secara asinkron mengambil token baru dan kemudian memanggil panggilan balik hasil yang disediakan di utas latar belakang saat token siap.

Bagaimana penyedia token mencoba kembali pengambilan token yang gagal

Penyedia token secara otomatis mencoba kembali pengambilan token saat pengambilan gagal. Percobaan ulang awalnya dilakukan menggunakan backoff eksponensial dengan waktu tunggu coba

lagi mulai 100 ms. Untuk informasi tentang percobaan ulang eksponensial, lihat Error retries dan exponential backoff di. AWS

Ketika jumlah percobaan ulang mencapai konfigurasi`maxRetryCount`, penyedia token berhenti mencoba atau beralih ke mencoba setiap `maxErrorTokenRefreshDelayMsec` milidetik, tergantung pada jenis pengambilan token:

- **`onTokenReady()`**— Penyedia token beralih ke `maxErrorTokenRefreshDelayMsec` milidetik menunggu di antara upaya, dan terus mencoba mengambil token.
- Penyegaran latar belakang — Penyedia token beralih ke `maxErrorTokenRefreshDelayMsec` milidetik menunggu di antara upaya, dan terus mencoba mengambil token.
- **`getToken()`**Panggilan sesuai permintaan, saat penyegaran latar belakang dinonaktifkan — Penyedia token berhenti mencoba mengambil token dan mengembalikan nilai token sebelumnya, atau nilai nol jika tidak ada token sebelumnya.

Mengambil token setelah aplikasi tidak aktif

Penyegaran latar belakang hanya dilakukan saat aplikasi Anda dianggap aktif untuk jenis aplikasi Anda:

- iOS — Penyegaran latar belakang dilakukan saat aplikasi berada di latar depan.
- Android — Penyegaran latar belakang dilakukan saat aplikasi tidak ditutup, baik itu di latar depan atau latar belakang.

Jika aplikasi Anda tetap dalam status apa pun yang tidak mendukung penyegaran latar belakang lebih lama dari `tokenRefreshDelaySec` detik yang dikonfigurasi, penyedia token akan menjeda penyegaran latar belakang. Misalnya, untuk aplikasi iOS, jika `tokenRefreshDelaySec` 300 dan aplikasi ditutup atau masuk ke latar belakang selama lebih dari 300 detik, penyedia token berhenti menyegarkan token. Saat aplikasi kembali ke status aktif, penyedia token secara otomatis memulai ulang penyegaran latar belakang.

Saat aplikasi Anda kembali ke status aktif, hubungi `onTokenReady()` agar Anda dapat diberi tahu saat penyedia token telah mengambil dan menyimpan token baru dalam cache. Jangan hanya menelepon`getToken()`, karena cache mungkin belum berisi token yang valid saat ini.

Menulis kode Anda untuk SDK AWS WAF seluler

Bagian ini memberikan contoh kode untuk menggunakan SDK seluler.

Menginisialisasi penyedia token dan mendapatkan token

Anda memulai instance penyedia token Anda menggunakan objek konfigurasi. Kemudian Anda dapat mengambil token menggunakan operasi yang tersedia. Berikut ini menunjukkan komponen dasar dari kode yang diperlukan.

iOS

```
let url: URL = URL(string: "Web ACL integration URL")!
let configuration = WAFConfiguration(applicationIntegrationUrl: url, domainName:
 "Domain name")
let tokenProvider = WAFTokenProvider(configuration)

//onTokenReady can be add as an observer for
 UIApplication.willEnterForegroundNotification
self.tokenProvider.onTokenReady() { token, error in
 if let token = token {
 //token available
 }

 if let error = error {
 //error occurred after exhausting all retries
 }
}

//getToken()
let token = tokenProvider.getToken()
```

Android

Contoh Java:

```
String applicationIntegrationURL = "Web ACL integration URL";
//Or
URL applicationIntegrationURL = new URL("Web ACL integration URL");

String domainName = "Domain name";

WAFConfiguration configuration =
 WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL).domainName(
WAFTokenProvider tokenProvider = new WAFTokenProvider(Application context,
 configuration);
```

```
// implement a token result callback
WAFTokenResultCallback callback = (wafToken, error) -> {
 if (wafToken != null) {
 // token available
 } else {
 // error occurred in token refresh
 }
};

// Add this callback to application creation or activity creation where token will
 be used
tokenProvider.onTokenReady(callback);

// Once you have token in token result callback
// if background refresh is enabled you can call getToken() from same tokenprovider
 object
// if background refresh is disabled you can directly call getToken()(blocking call)
 for new token
WAFToken token = tokenProvider.getToken();
```

Contoh Kotlin:

```
import com.amazonaws.waf.mobilesdk.token.WAFConfiguration
import com.amazonaws.waf.mobilesdk.token.WAFTokenProvider

private lateinit var wafConfiguration: WAFConfiguration
private lateinit var wafTokenProvider: WAFTokenProvider

private val WAF_INTEGRATION_URL = "Web ACL integration URL"
private val WAF_DOMAIN_NAME = "Domain name"

fun initWaf() {
 // Initialize the tokenprovider instance
 val applicationIntegrationURL = URL(WAF_INTEGRATION_URL)
 wafConfiguration =
  WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL)
   .domainName(WAF_DOMAIN_NAME).backgroundRefreshEnabled(true).build()
 wafTokenProvider = WAFTokenProvider(getApplication(), wafConfiguration)

  // getToken from tokenprovider object
  println("WAF: "+ wafTokenProvider.token.value)

  // implement callback for where token will be used
```

```
  wafTokenProvider.onTokenReady {
   wafToken, sdkError ->
  run {
   println("WAF Token:" + wafToken.value)
  }
 }
}
```

Mengizinkan SDK menyediakan cookie token dalam permintaan HTTP Anda

Jika `setTokenCookie` ya`TRUE`, penyedia token menyertakan cookie token untuk Anda dalam permintaan web Anda ke semua lokasi di bawah jalur yang ditentukan`tokenCookiePath`. Secara default, `setTokenCookie` adalah `TRUE` dan `tokenCookiePath` adalah`/`.

Anda dapat mempersempit cakupan permintaan yang menyertakan cookie token dengan menentukan jalur cookie token, misalnya,`/web/login`. Jika Anda melakukan ini, periksa apakah AWS WAF aturan Anda tidak memeriksa token dalam permintaan yang Anda kirim ke jalur lain. Saat Anda menggunakan grup `AWSManagedRulesACFPRuleSet` aturan, Anda mengonfigurasi jalur pendaftaran dan pembuatan akun, dan grup aturan memeriksa token dalam permintaan yang dikirim ke jalur tersebut. Untuk informasi selengkapnya, lihat Menambahkan grup aturan terkelola ACFP ke ACL web Anda. Demikian pula, saat Anda menggunakan grup `AWSManagedRulesATPRuleSet` aturan, Anda mengonfigurasi jalur masuk, dan grup aturan memeriksa token dalam permintaan yang dikirim ke jalur tersebut. Untuk informasi selengkapnya, lihat Menambahkan grup aturan terkelola ATP ke ACL web Anda.

iOS

`setTokenCookie`Kapan`TRUE`, penyedia token menyimpan AWS WAF token dalam a `HTTPCookieStorage.shared` dan secara otomatis menyertakan cookie dalam permintaan ke domain yang Anda tentukan`WAFConfiguration`.

```
let request = URLRequest(url: URL(string: domainEndpointUrl)!)
//The token cookie is set automatically as cookie header
let task = URLSession.shared.dataTask(with: request) { data, urlResponse, error  in
}.resume()
```

Android

`setTokenCookieKapan`TRUE, penyedia token menyimpan AWS WAF token dalam `CookieHandler` instance yang dibagikan di seluruh aplikasi. Penyedia token secara otomatis menyertakan cookie dalam permintaan ke domain yang Anda tentukan`WAFConfiguration`.

Contoh Java:

```
URL url = new URL("Domain name");
//The token cookie is set automatically as cookie header
HttpsURLConnection connection = (HttpsURLConnection) url.openConnection();
connection.getResponseCode();
```

Contoh Kotlin:

```
val url = URL("Domain name")
//The token cookie is set automatically as cookie header
val connection = (url.openConnection() as HttpsURLConnection)
connection.responseCode
```

Jika Anda sudah menginisialisasi instance `CookieHandler` default, penyedia token akan menggunakannya untuk mengelola cookie. Jika tidak, penyedia token akan menginisialisasi `CookieManager` instance baru dengan AWS WAF token `CookiePolicy.ACCEPT_ORIGINAL_SERVER` dan kemudian mengatur instance baru ini sebagai instance default di`CookieHandler`.

Kode berikut menunjukkan cara SDK menginisialisasi pengelola cookie dan penangan cookie saat tidak tersedia di aplikasi Anda.

Contoh Java:

```
CookieManager cookieManager = (CookieManager) CookieHandler.getDefault();
if (cookieManager == null) {
 // Cookie manager is initialized with CookiePolicy.ACCEPT_ORIGINAL_SERVER
 cookieManager = new CookieManager();
 CookieHandler.setDefault(cookieManager);
}
```

Contoh Kotlin:

```
var cookieManager = CookieHandler.getDefault() as? CookieManager
if (cookieManager == null) {
 // Cookie manager is initialized with CookiePolicy.ACCEPT_ORIGINAL_SERVER
 cookieManager = CookieManager()
 CookieHandler.setDefault(cookieManager)
}
```

Menyediakan cookie token secara manual dalam permintaan HTTP Anda

Jika Anda menyetel `setTokenCookie` ke`FALSE`, maka Anda perlu memberikan cookie token secara manual, sebagai header permintaan HTTP Cookie, dalam permintaan Anda ke titik akhir yang dilindungi. Kode berikut menunjukkan bagaimana melakukan ini.

iOS

```
var request = URLRequest(url: wafProtectedEndpoint)
request.setValue("aws-waf-token=token from token provider", forHTTPHeaderField:
 "Cookie")
request.httpShouldHandleCookies = true
URLSession.shared.dataTask(with: request) { data, response, error in }
```

Android

Contoh Java:

```
URL url = new URL("Domain name");
HttpsURLConnection connection = (HttpsURLConnection) url.openConnection();
String wafTokenCookie = "aws-waf-token=token from token provider";
connection.setRequestProperty("Cookie", wafTokenCookie);
connection.getInputStream();
```

Contoh Kotlin:

```
val url = URL("Domain name")
val connection = (url.openConnection() as HttpsURLConnection)
val wafTokenCookie = "aws-waf-token=token from token provider"
connection.setRequestProperty("Cookie", wafTokenCookie)
connection.inputStream
```

CAPTCHAdan Challenge di AWS WAF

Anda dapat mengonfigurasi AWS WAF aturan untuk menjalankan Challenge tindakan CAPTCHA atau terhadap permintaan web yang sesuai dengan kriteria pemeriksaan aturan Anda. Anda juga dapat memprogram aplikasi JavaScript klien Anda untuk menjalankan teka-teki CAPTCHA dan tantangan browser secara lokal.

Teka-teki CAPTCHA dan tantangan diam hanya dapat berjalan ketika browser mengakses titik akhir HTTPS. Klien browser harus berjalan dalam konteks aman untuk mendapatkan token.

- CAPTCHA— Membutuhkan pengguna akhir untuk memecahkan teka-teki CAPTCHA untuk membuktikan bahwa manusia mengirim permintaan. Teka-teki CAPTCHA dimaksudkan untuk menjadi cukup mudah dan cepat bagi manusia untuk menyelesaikan dengan sukses dan sulit bagi komputer untuk menyelesaikan dengan sukses atau secara acak menyelesaikan dengan tingkat keberhasilan yang berarti.

  Dalam aturan ACL web, CAPTCHA biasanya digunakan ketika suatu Block tindakan akan menghentikan terlalu banyak permintaan yang sah, tetapi membiarkan semua lalu lintas lewat akan menghasilkan tingkat permintaan yang tidak diinginkan yang sangat tinggi, seperti dari bot. Untuk informasi tentang perilaku tindakan aturan, lihatBagaimana tindakan AWS WAFCAPTCHA dan Challenge aturan bekerja.

  Anda juga dapat memprogram implementasi teka-teki CAPTCHA di API integrasi aplikasi klien Anda. Ketika Anda melakukan ini, Anda dapat menyesuaikan perilaku dan penempatan teka-teki dalam aplikasi klien Anda. Untuk informasi selengkapnya, lihat AWS WAF integrasi aplikasi klien.
- Challenge— Menjalankan tantangan diam yang mengharuskan sesi klien untuk memverifikasi bahwa itu adalah browser, dan bukan bot. Verifikasi berjalan di latar belakang tanpa melibatkan pengguna akhir. Ini adalah opsi yang baik untuk memverifikasi klien yang Anda curigai tidak valid tanpa berdampak negatif pada pengalaman pengguna akhir dengan teka-teki CAPTCHA. Untuk informasi tentang perilaku tindakan aturan, lihatBagaimana tindakan AWS WAFCAPTCHA dan Challenge aturan bekerja.

  Tindakan Challenge aturan mirip dengan tantangan yang dijalankan oleh API integrasi ancaman cerdas klien, yang dijelaskan diAWS WAF integrasi aplikasi klien.

> **Note**
>
> Anda akan dikenakan biaya tambahan ketika Anda menggunakan tindakan CAPTCHA atau Challenge aturan di salah satu aturan Anda atau sebagai penggantian tindakan aturan dalam grup aturan. Untuk informasi selengkapnya, silakan lihat Harga AWS WAF.

Untuk deskripsi semua opsi tindakan aturan, lihatTindakan aturan.

Topik

- AWS WAF Teka-teki CAPTCHA
- Bagaimana tindakan AWS WAFCAPTCHA dan Challenge aturan bekerja
- Praktik terbaik untuk menggunakan CAPTCHA dan Challenge tindakan

AWS WAF Teka-teki CAPTCHA

AWS WAF menyediakan fungsionalitas CAPTCHA standar yang menantang pengguna untuk mengonfirmasi bahwa mereka adalah manusia. CAPTCHA adalah singkatan dari Completely Automated Public Turing Test untuk memberitahu komputer dan manusia terpisah. Teka-teki CAPTCHA dirancang untuk memverifikasi bahwa manusia mengirim permintaan dan untuk mencegah aktivitas seperti pengikisan web, isian kredenal, dan spam. Teka-teki CAPTCHA tidak dapat menyingkirkan semua permintaan yang tidak diinginkan. Banyak teka-teki telah dipecahkan menggunakan pembelajaran mesin dan kecerdasan buatan. Dalam upaya untuk menghindari CAPTCHA, beberapa organisasi melengkapi teknik otomatis dengan intervensi manusia. Meskipun demikian, CAPTCHA terus menjadi alat yang berguna untuk mencegah lalu lintas bot yang kurang canggih dan untuk meningkatkan sumber daya yang dibutuhkan untuk operasi skala besar.

AWS WAF secara acak menghasilkan teka-teki CAPTCHA dan memutarnya untuk memastikan bahwa pengguna disajikan dengan tantangan unik. AWS WAF secara teratur menambahkan jenis dan gaya teka-teki baru agar tetap efektif melawan teknik otomatisasi. Selain teka-teki, skrip AWS WAF CAPTCHA mengumpulkan data tentang klien untuk memastikan bahwa tugas diselesaikan oleh manusia dan untuk mencegah serangan replay.

Setiap teka-teki CAPTCHA mencakup seperangkat kontrol standar bagi pengguna akhir untuk meminta teka-teki baru, beralih antara teka-teki audio dan visual, mengakses instruksi tambahan, dan mengirimkan solusi teka-teki. Semua teka-teki termasuk dukungan untuk pembaca layar, kontrol keyboard, dan warna yang kontras.

Teka-teki AWS WAF CAPTCHA memenuhi persyaratan Pedoman Aksesibilitas Konten Web (WCAG). Untuk selengkapnya, lihat Tinjauan Panduan Aksesibilitas Konten Web (WCAG) di situs web World Wide Web Consortium (W3C).

Topik

Dukungan bahasa teka-teki CAPTCHA

Teka-teki CAPTCHA dimulai dengan instruksi tertulis dalam bahasa browser klien atau, jika bahasa browser tidak didukung, dalam bahasa Inggris. Teka-teki ini menyediakan opsi bahasa alternatif melalui menu tarik-turun.

Pengguna dapat beralih ke instruksi audio dengan memilih ikon headphone di bagian bawah halaman. Versi audio teka-teki memberikan instruksi lisan tentang teks yang harus diketik pengguna ke dalam kotak teks, dilapisi oleh kebisingan latar belakang.

Tabel berikut mencantumkan bahasa yang dapat Anda pilih untuk instruksi tertulis dalam teka-teki CAPTCHA dan dukungan audio untuk setiap pilihan.

AWS WAF Teka-teki CAPTCHA mendukung bahasa

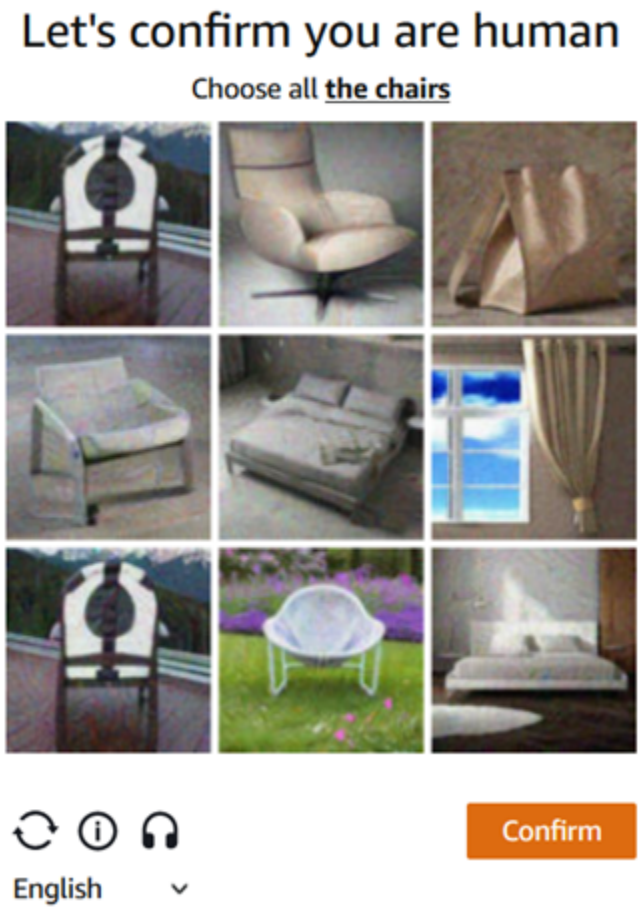
Dukungan instruksi tertulis	Kode lokal	Dukungan instruksi audio
Arab	AR-sa	Arab
Bahasa Mandarin Sederhana	Zh-CN	Audio dalam bahasa Inggris
Bahasa Belanda	Nl-NL	Bahasa Belanda
Bahasa Inggris	en-US	Bahasa Inggris
Prancis	FR-fr	Bahasa Prancis
Bahasa Jerman	De-de	Bahasa Jerman

Dukungan instruksi tertulis	Kode lokal	Dukungan instruksi audio
Bahasa Italia	It-itu	Bahasa Italia
Bahasa Jepang	Ja-JP	Audio dalam bahasa Inggris
Portugis Brasil	Pt-BR	Portugis Brasil
Bahasa Spanyol	ES-es	Bahasa Spanyol
Turki	TR-TR	Turki

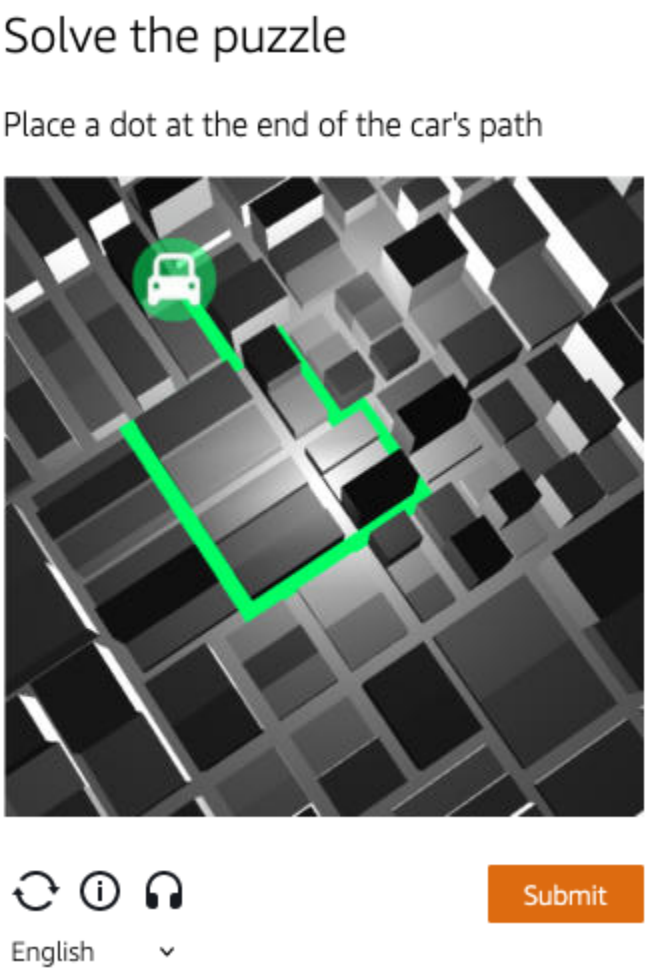
Contoh teka-teki CAPTCHA

Teka-teki CAPTCHA visual yang khas membutuhkan interaksi untuk menunjukkan bahwa pengguna dapat memahami dan berinteraksi dengan satu atau lebih gambar.

Tangkapan layar berikut menunjukkan contoh teka-teki kisi gambar. Teka-teki ini mengharuskan Anda untuk memilih semua gambar di grid yang menyertakan jenis objek tertentu.

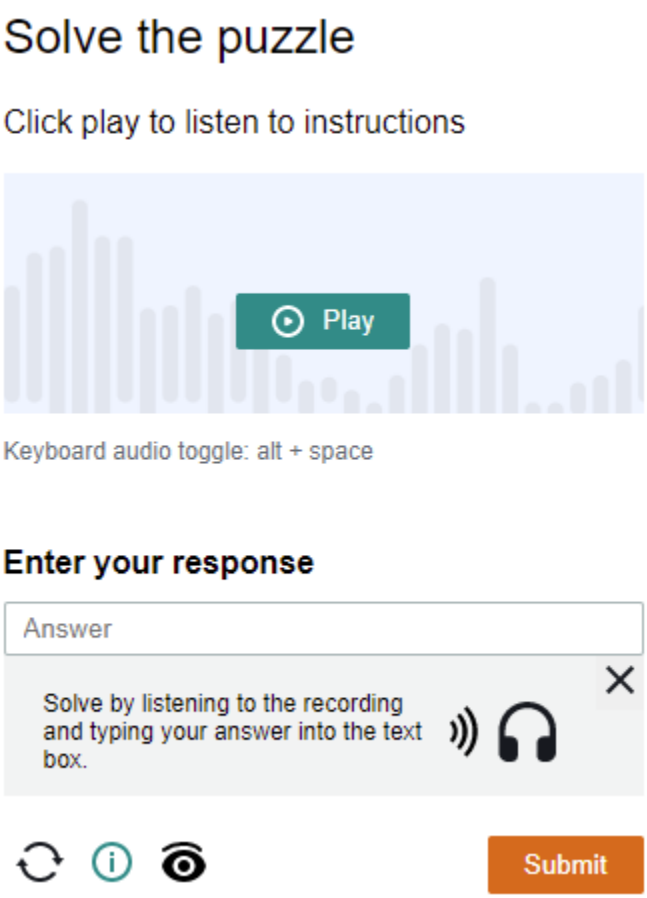


Tangkapan layar berikut menunjukkan contoh teka-teki yang mengharuskan Anda mengidentifikasi titik akhir jalur mobil dalam gambar.



Teka-teki audio memberikan kebisingan latar belakang yang dilapisi dengan instruksi lisan tentang teks yang harus diketik pengguna ke dalam kotak teks.

Tangkapan layar berikut menunjukkan tampilan untuk pilihan puzzle audio.



Bagaimana tindakan AWS WAFCAPTCHA dan Challenge aturan bekerja

AWS WAF CAPTCHAdan Challenge merupakan tindakan aturan standar, sehingga relatif mudah diterapkan. Untuk menggunakan salah satu dari mereka, Anda membuat kriteria inspeksi untuk aturan Anda yang mengidentifikasi permintaan yang ingin Anda periksa, lalu tentukan salah satu dari dua tindakan aturan. Untuk informasi umum tentang opsi tindakan aturan, lihatTindakan aturan.

Selain menerapkan tantangan diam dan teka-teki CAPTCHA dari sisi server, Anda dapat mengintegrasikan tantangan diam dalam aplikasi klien JavaScript iOS dan Android Anda, dan Anda dapat membuat teka-teki CAPTCHA di klien Anda. JavaScript Integrasi ini memungkinkan Anda untuk memberi pengguna akhir Anda kinerja yang lebih baik dan pengalaman teka-teki CAPTCHA, dan mereka dapat mengurangi biaya yang terkait dengan penggunaan tindakan aturan dan kelompok aturan mitigasi ancaman cerdas. Untuk informasi selengkapnya tentang opsi ini, lihat AWS WAF integrasi aplikasi klien. Untuk informasi harga, lihat Harga AWS WAF.

Topik

CAPTCHAdan perilaku Challenge tindakan

Ketika permintaan web cocok dengan kriteria inspeksi aturan dengan CAPTCHA atau Challenge tindakan, AWS WAF menentukan cara menangani permintaan sesuai dengan status token dan konfigurasi waktu imunitasnya. AWS WAF juga mempertimbangkan apakah permintaan dapat menangani teka-teki CAPTCHA atau pengantara skrip tantangan. Script dirancang untuk ditangani sebagai konten HTML, dan mereka hanya dapat ditangani dengan benar oleh klien yang mengharapkan konten HTML.

> **Note**
>
> Anda akan dikenakan biaya tambahan ketika Anda menggunakan tindakan CAPTCHA atau Challenge aturan di salah satu aturan Anda atau sebagai penggantian tindakan aturan dalam grup aturan. Untuk informasi selengkapnya, silakan lihat Harga AWS WAF.

Bagaimana tindakan menangani permintaan web

AWS WAF menerapkan CAPTCHA atau Challenge tindakan untuk permintaan web sebagai berikut:

- Token yang valid — AWS WAF menangani ini mirip dengan Count tindakan. AWS WAF menerapkan label dan kustomisasi permintaan apa pun yang telah Anda konfigurasikan untuk tindakan aturan, dan kemudian terus mengevaluasi permintaan menggunakan aturan yang tersisa di ACL web.
- Token yang hilang, tidak valid, atau kedaluwarsa — AWS WAF menghentikan evaluasi ACL web dari permintaan dan memblokirnya pergi ke tujuan yang dimaksudkan.

  AWS WAF menghasilkan respons yang dikirim kembali ke klien, sesuai dengan jenis tindakan aturan:

  - Challenge— AWS WAF termasuk yang berikut dalam tanggapan:
    - Header `x-amzn-waf-action` dengan nilai`challenge`.

> **Note**
>
> Header ini tidak tersedia untuk JavaScript aplikasi yang berjalan di browser klien. Untuk detailnya, lihat bagian berikut.

- Kode status HTTP`202 Request Accepted`.
- Jika permintaan berisi `Accept` header dengan nilai`text/html`, responsnya menyertakan pengantara JavaScript halaman dengan skrip tantangan.

- CAPTCHA— AWS WAF termasuk yang berikut dalam tanggapan:
  - Header `x-amzn-waf-action` dengan nilai`captcha`.

> **Note**
>
> Header ini tidak tersedia untuk JavaScript aplikasi yang berjalan di browser klien. Untuk detailnya, lihat bagian berikut.

  - Kode status HTTP`405 Method Not Allowed`.
  - Jika permintaan berisi `Accept` header dengan nilai`text/html`, responsnya mencakup pengantara JavaScript halaman dengan skrip CAPTCHA.

Untuk mengonfigurasi waktu kedaluwarsa token di ACL web atau level aturan, lihat. Kedaluwarsa stempel waktu: waktu kekebalan token AWS WAF

Header tidak tersedia untuk JavaScript aplikasi yang berjalan di browser klien

Saat AWS WAF menanggapi permintaan klien dengan CAPTCHA atau respons tantangan, itu tidak menyertakan header berbagi sumber daya lintas asal (CORS). Header CORS adalah seperangkat header kontrol akses yang memberi tahu browser web klien domain, metode HTTP, dan header HTTP mana yang dapat digunakan oleh aplikasi. JavaScript Tanpa header CORS, JavaScript aplikasi yang berjalan di browser klien tidak diberikan akses ke header HTTP sehingga tidak dapat membaca `x-amzn-waf-action` header yang disediakan di dan tanggapan. CAPTCHA Challenge

Apa yang dilakukan tantangan dan pengantara CAPTCHA

Ketika pengantara tantangan berjalan, setelah klien merespons dengan sukses, jika belum memiliki token, pengantara menginisialisasi satu untuk itu. Kemudian memperbarui token dengan stempel waktu pemecahan tantangan.

Ketika pengantara CAPTCHA berjalan, jika klien belum memiliki token, pengantara CAPTCHA memanggil skrip tantangan terlebih dahulu untuk menantang browser dan menginisialisasi token. Kemudian interstisial menjalankan teka-teki CAPTCHA. Ketika pengguna akhir berhasil menyelesaikan teka-teki, pengantara memperbarui token dengan cap waktu pemecahan CAPTCHA.

Dalam kedua kasus, setelah klien merespons dengan sukses dan skrip memperbarui token, skrip mengirimkan kembali permintaan web asli menggunakan token yang diperbarui.

Anda dapat mengonfigurasi cara AWS WAF menangani token. Untuk informasi, lihat AWS WAF token permintaan web.

CAPTCHAdan Challenge tindakan dalam log dan metrik

ChallengeTindakan CAPTCHA dan dapat berupa non-terminating, like, atau terminatingCount, like. Block Hasilnya tergantung pada apakah permintaan memiliki token yang valid dengan stempel waktu yang belum kedaluwarsa untuk tipe tindakan.

- Token yang valid — Saat tindakan menemukan token yang valid dan tidak memblokir permintaan, AWS WAF menangkap metrik dan log sebagai berikut:
  - Meningkatkan metrik untuk salah satu `CaptchaRequests` dan `RequestsWithValidCaptchaToken` atau `ChallengeRequests` dan. `RequestsWithValidChallengeToken`
  - Log pertandingan sebagai `nonTerminatingMatchingRules` entri dengan aksi CAPTCHA atauChallenge. Daftar berikut menunjukkan bagian log untuk jenis kecocokan ini dengan CAPTCHA tindakan.

```
    "nonTerminatingMatchingRules": [
    {
      "ruleId": "captcha-rule",
      "action": "CAPTCHA",
      "ruleMatchDetails": [],
      "captchaResponse": {
        "responseCode": 0,
        "solveTimestamp": 1632420429
      }
    }
  ]
```

- Token hilang, tidak valid, atau kedaluwarsa — Saat tindakan memblokir permintaan karena token yang hilang atau tidak valid, AWS WAF menangkap metrik dan log sebagai berikut:

- Menambah metrik untuk `CaptchaRequests` atau`ChallengeRequests`.
- Log kecocokan sebagai `CaptchaResponse` entri dengan kode `405` status HTTP atau sebagai `ChallengeResponse` entri dengan kode `202` status HTTP. Log menunjukkan apakah permintaan tidak ada token atau memiliki stempel waktu yang kedaluwarsa. Log juga menunjukkan apakah AWS WAF mengirim halaman pengantara CAPTCHA ke klien atau tantangan diam ke browser klien. Daftar berikut menunjukkan bagian log untuk jenis kecocokan ini dengan CAPTCHA tindakan.

```
"terminatingRuleId": "captcha-rule",
"terminatingRuleType": "REGULAR",
"action": "CAPTCHA",
"terminatingRuleMatchDetails": [],
...
"responseCodeSent": 405,
...
"captchaResponse": {
  "responseCode": 405,
  "solveTimestamp": 0,
  "failureReason": "TOKEN_MISSING"
}
```

Untuk informasi tentang AWS WAF log, lihatPencatatan AWS WAF lalu lintas ACL web.

Untuk informasi tentang AWS WAF metrik, lihatAWS WAF metrik dan dimensi.

Untuk informasi tentang opsi tindakan aturan, lihatTindakan aturan.

Praktik terbaik untuk menggunakan CAPTCHA dan Challenge tindakan

Ikuti panduan di bagian ini untuk merencanakan dan mengimplementasikan AWS WAF CAPTCHA atau tantangan.

Rencanakan CAPTCHA Anda dan tantang implementasi

Tentukan di mana menempatkan teka-teki CAPTCHA atau tantangan diam berdasarkan penggunaan situs web Anda, sensitivitas data yang ingin Anda lindungi, dan jenis permintaan. Pilih permintaan di mana Anda akan menerapkan CAPTCHA sehingga Anda menyajikan teka-teki sesuai kebutuhan, tetapi hindari menyajikannya di tempat yang tidak berguna dan dapat menurunkan pengalaman pengguna. Gunakan Challenge tindakan untuk menjalankan tantangan diam yang berdampak lebih

kecil pada pengguna akhir, tetapi tetap membantu memverifikasi bahwa permintaan tersebut berasal dari browser yang JavaScript diaktifkan.

Teka-teki CAPTCHA dan tantangan diam hanya dapat berjalan ketika browser mengakses titik akhir HTTPS. Klien browser harus berjalan dalam konteks aman untuk mendapatkan token.

Putuskan di mana menjalankan teka-teki CAPTCHA dan tantangan diam pada klien Anda

Identifikasi permintaan yang Anda tidak ingin terpengaruh oleh CAPTCHA, misalnya, permintaan untuk CSS atau gambar. Gunakan CAPTCHA hanya jika diperlukan. Misalnya, jika Anda berencana untuk memeriksa CAPTCHA saat login, dan pengguna selalu dibawa langsung dari login ke layar lain, memerlukan pemeriksaan CAPTCHA di layar kedua mungkin tidak diperlukan dan mungkin menurunkan pengalaman pengguna akhir Anda.

Konfigurasikan Challenge dan CAPTCHA gunakan sehingga AWS WAF hanya mengirimkan teka-teki CAPTCHA dan tantangan diam sebagai tanggapan atas permintaan. `GET text/html` Anda tidak dapat menjalankan teka-teki atau tantangan dalam menanggapi `POST` permintaan, permintaan preflight Cross-Origin Resource Sharing (CORS), atau jenis `OPTIONS` `GET` non-permintaan lainnya. Perilaku browser untuk jenis permintaan lain dapat bervariasi dan mungkin tidak dapat menangani pengantara dengan benar.

Ada kemungkinan bagi klien untuk menerima HTML tetapi masih tidak dapat menangani CAPTCHA atau menantang pengantara. Misalnya, widget pada halaman web dengan iFrame kecil mungkin menerima HTML tetapi tidak dapat menampilkan CAPTCHA atau memprosesnya. Hindari menempatkan tindakan aturan untuk jenis permintaan ini, sama seperti permintaan yang tidak menerima HTML.

Gunakan CAPTCHA atau Challenge untuk memverifikasi akuisisi token sebelumnya

Anda dapat menggunakan tindakan aturan semata-mata untuk memverifikasi keberadaan token yang valid, di lokasi di mana pengguna yang sah harus selalu memilikinya. Dalam situasi ini, tidak masalah apakah permintaan dapat menangani pengantara.

Misalnya, jika Anda menerapkan aplikasi JavaScript klien CAPTCHA API, dan menjalankan teka-teki CAPTCHA pada klien segera sebelum Anda mengirim permintaan pertama ke titik akhir yang dilindungi, permintaan pertama Anda harus selalu menyertakan token yang valid untuk tantangan dan CAPTCHA. Untuk informasi tentang integrasi aplikasi JavaScript klien, lihatAWS WAF JavaScript integrasi.

Untuk situasi ini, di ACL web Anda, Anda dapat menambahkan aturan yang cocok dengan panggilan pertama ini dan mengonfigurasinya dengan tindakan CAPTCHA aturan Challenge atau. Ketika

aturan cocok untuk pengguna akhir dan browser yang sah, tindakan akan menemukan token yang valid, dan karena itu tidak akan memblokir permintaan atau mengirim tantangan atau teka-teki CAPTCHA sebagai tanggapan. Untuk informasi selengkapnya tentang cara kerja tindakan aturan, lihatCAPTCHAdan perilaku Challenge tindakan.

Lindungi data non-HTML sensitif Anda dengan CAPTCHA dan Challenge

Anda dapat menggunakan CAPTCHA dan Challenge proteksi untuk data non-HTML yang sensitif, seperti API, dengan pendekatan berikut.

1. Identifikasi permintaan yang mengambil respons HTML dan yang dijalankan di dekat permintaan untuk data sensitif dan non-HTML Anda.
2. Tulis CAPTCHA atau Challenge aturan yang cocok dengan permintaan HTML dan yang cocok dengan permintaan untuk data sensitif Anda.
3. Sesuaikan pengaturan waktu Anda CAPTCHA dan Challenge kekebalan sehingga, untuk interaksi pengguna normal, token yang diperoleh klien dari permintaan HTML tersedia dan belum kedaluwarsa dalam permintaan mereka untuk data sensitif Anda. Untuk informasi penyetelan, lihatKedaluwarsa stempel waktu: waktu kekebalan token AWS WAF.

Ketika permintaan untuk data sensitif Anda cocok dengan Challenge aturan CAPTCHA atau, itu tidak akan diblokir jika klien masih memiliki token yang valid dari teka-teki atau tantangan sebelumnya. Jika token tidak tersedia atau stempel waktu kedaluwarsa, permintaan untuk mengakses data sensitif Anda akan gagal. Untuk informasi selengkapnya tentang cara kerja tindakan aturan, lihatCAPTCHAdan perilaku Challenge tindakan.

Gunakan CAPTCHA dan Challenge untuk menyesuaikan aturan yang ada

Tinjau aturan yang ada, untuk melihat apakah Anda ingin mengubah atau menambahkannya. Berikut ini adalah beberapa skenario umum yang perlu dipertimbangkan.

- Jika Anda memiliki aturan berbasis tarif yang memblokir lalu lintas, tetapi Anda menjaga batas tarif relatif tinggi untuk menghindari pemblokiran pengguna yang sah, pertimbangkan untuk menambahkan aturan berbasis tarif kedua setelah aturan pemblokiran. Berikan aturan kedua batas yang lebih rendah dari aturan pemblokiran dan tetapkan tindakan aturan ke CAPTCHA atauChallenge. Aturan pemblokiran masih akan memblokir permintaan yang datang pada tingkat yang terlalu tinggi, dan aturan baru akan memblokir sebagian besar lalu lintas otomatis pada tingkat yang lebih rendah. Untuk informasi tentang aturan berbasis tarif, lihat. Pernyataan aturan berbasis tarif

- Jika Anda memiliki grup aturan terkelola yang memblokir permintaan, Anda dapat mengalihkan perilaku untuk beberapa atau semua aturan dari Block ke CAPTCHA atauChallenge. Untuk melakukannya, dalam konfigurasi grup aturan terkelola, ganti setelan tindakan aturan. Untuk informasi tentang tindakan aturan utama, lihatPengesampingan tindakan aturan kelompok aturan.

Uji CAPTCHA Anda dan tantang implementasi sebelum Anda menerapkannya

Adapun semua fungsionalitas baru, ikuti panduan dithe section called “Menguji dan menyetel perlindungan Anda”.

Selama pengujian, tinjau persyaratan kedaluwarsa stempel waktu token Anda dan atur ACL web Anda dan konfigurasi waktu kekebalan tingkat aturan sehingga Anda mencapai keseimbangan yang baik antara mengontrol akses ke situs web Anda dan memberikan pengalaman yang baik bagi pelanggan Anda. Untuk informasi, lihat Kedaluwarsa stempel waktu: waktu kekebalan token AWS WAF.

Pencatatan AWS WAF lalu lintas ACL web

Anda dapat mengaktifkan logging untuk mendapatkan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Informasi yang dicatat mencakup waktu AWS WAF menerima permintaan web dari AWS sumber daya Anda, informasi terperinci tentang permintaan, dan detail tentang aturan yang cocok dengan permintaan tersebut. Anda dapat mengirim log ACL web ke grup CloudWatch log Amazon Logs, bucket Amazon Simple Storage Service (Amazon S3), atau aliran pengiriman Amazon Data Firehose.

Opsi pengumpulan dan analisis data lainnya

Selain pencatatan, Anda dapat mengaktifkan opsi berikut untuk pengumpulan dan analisis data:

- Amazon Security Lake - Anda dapat mengonfigurasi Security Lake untuk mengumpulkan data ACL web. Security Lake mengumpulkan data log dan peristiwa dari berbagai sumber untuk normalisasi, analisis, dan manajemen. Untuk informasi tentang opsi ini, lihat Apa itu Amazon Security Lake? dan Mengumpulkan data dari AWS layanan di panduan pengguna Amazon Security Lake.

  AWS WAF tidak mengenakan biaya untuk menggunakan opsi ini. Untuk informasi harga, lihat Harga Security Lake dan Cara penetapan harga Security Lake di panduan pengguna Amazon Security Lake.

- Permintaan pengambilan sampel — Anda dapat mengonfigurasi ACL web Anda untuk mengambil sampel permintaan web yang dievaluasi, untuk mendapatkan gambaran tentang jenis lalu lintas yang diterima aplikasi Anda. Untuk informasi tentang opsi ini, lihatMelihat contoh permintaan web.

> **Note**
>
> Konfigurasi pencatatan ACL web hanya memengaruhi AWS WAF log. Secara khusus, konfigurasi bidang yang disunting untuk pencatatan tidak berdampak pada pengambilan sampel permintaan atau pengumpulan data Security Lake. Pengumpulan data Security Lake dikonfigurasi sepenuhnya melalui layanan Security Lake. Satu-satunya cara untuk mengecualikan bidang dari permintaan sampel adalah dengan menonaktifkan pengambilan sampel untuk ACL web.

Topik

Harga untuk mencatat informasi lalu lintas ACL web

Anda dikenakan biaya untuk mencatat informasi lalu lintas ACL web sesuai dengan biaya yang terkait dengan setiap jenis tujuan log. Biaya ini merupakan tambahan dari biaya untuk menggunakan AWS WAF. Biaya Anda dapat bervariasi tergantung pada faktor-faktor seperti jenis tujuan yang Anda pilih dan jumlah data yang Anda log.

Berikut ini menyediakan tautan ke informasi harga untuk setiap jenis tujuan pencatatan:

- CloudWatch Log — Biaya adalah untuk pengiriman log yang dijual. Lihat Harga CloudWatch Log Amazon. Di bawah Tingkat Berbayar, pilih tab Log, lalu di bawah Log Terjual, lihat informasi untuk Pengiriman ke CloudWatch Log.
- Bucket Amazon S3 — Biaya Amazon S3 adalah biaya gabungan untuk pengiriman CloudWatch log penjual Log ke ember Amazon S3 dan untuk menggunakan Amazon S3.

- Untuk Amazon S3, lihat Harga Amazon S3.
- Untuk pengiriman CloudWatch log terjual Log ke Amazon S3, lihat Harga Log CloudWatch Amazon. Di bawah Tingkat Berbayar, pilih tab Log, lalu di bawah Vended Logs, lihat informasi untuk Pengiriman ke S3

- Firehose — Lihat Harga Amazon Data Firehose.

Untuk informasi tentang AWS WAF harga, lihat AWS WAF Harga.

AWS WAF tujuan pencatatan

Bagian ini menjelaskan opsi pencatatan yang dapat Anda pilih untuk AWS WAF log Anda. Setiap bagian menyediakan panduan untuk mengonfigurasi logging termasuk informasi tentang perilaku apa pun yang spesifik untuk jenis tujuan. Setelah mengonfigurasi tujuan pencatatan, Anda dapat memberikan spesifikasinya ke konfigurasi logging ACL web Anda untuk mulai masuk ke sana.

Topik

- Grup CloudWatch log Amazon Logs
- Bucket Layanan Penyimpanan Sederhana Amazon
- Aliran pengiriman Amazon Data Firehose

Grup CloudWatch log Amazon Logs

Topik ini memberikan informasi untuk mengirim log lalu lintas ACL web Anda ke grup CloudWatch log Log.

> **Note**
>
> Anda dikenakan biaya untuk logging selain biaya untuk menggunakan AWS WAF. Untuk informasi, lihat Harga untuk mencatat informasi lalu lintas ACL web.

Untuk mengirim log ke Amazon CloudWatch Logs, Anda membuat grup CloudWatch log Log. Saat Anda mengaktifkan login AWS WAF, Anda memberikan grup log ARN. Setelah Anda mengaktifkan pencatatan untuk ACL web Anda, AWS WAF mengirimkan log ke grup CloudWatch log Log di aliran log.

Saat Anda menggunakan CloudWatch Log, Anda dapat menjelajahi log untuk ACL web Anda di AWS WAF konsol. Di halaman ACL web Anda, pilih tab Wawasan log. Opsi ini merupakan tambahan dari wawasan logging yang disediakan untuk CloudWatch Log melalui CloudWatch konsol.

Konfigurasikan grup log untuk log ACL AWS WAF web di Wilayah yang sama dengan ACL web dan menggunakan akun yang sama seperti yang Anda gunakan untuk mengelola ACL web. Untuk informasi tentang mengonfigurasi grup CloudWatch log Log, lihat Bekerja dengan Grup Log dan Aliran Log.

Kuota untuk grup CloudWatch log Log

CloudWatch Log memiliki kuota maksimum default untuk throughput, dibagikan di semua grup log dalam suatu wilayah, yang dapat Anda minta untuk ditingkatkan. Jika persyaratan pencatatan Anda terlalu tinggi untuk pengaturan throughput saat ini, Anda akan melihat metrik pembatasan untuk `PutLogEvents` akun Anda. Untuk melihat limit di konsol Service Quotas dan meminta peningkatan, lihat kuota CloudWatch Log PutLogEvents .

Penamaan grup log

Nama grup log Anda harus dimulai dengan `aws-waf-logs-` dan dapat diakhiri dengan akhiran apa pun yang Anda suka, misalnya,`aws-waf-logs-testLogGroup2`.

Format ARN yang dihasilkan adalah sebagai berikut:

```
arn:aws:logs:Region:account-id:log-group:aws-waf-logs-log-group-suffix
```

Aliran log memiliki format penamaan berikut:

```
Region_web-acl-name_log-stream-number
```

Berikut ini menunjukkan contoh aliran log untuk web ACL `TestWebACL` di Wilayah`us-east-1`.

```
us-east-1_TestWebACL_0
```

Izin yang diperlukan untuk mempublikasikan log ke CloudWatch Log

Mengkonfigurasi pencatatan lalu lintas ACL web untuk grup CloudWatch log Log memerlukan pengaturan izin yang dijelaskan di bagian ini. Izin ditetapkan untuk Anda saat Anda menggunakan salah satu kebijakan terkelola akses AWS WAF penuh, `AWSWAFConsoleFullAccess` atau`AWSWAFFullAccess`. Jika Anda ingin mengelola akses berbutir halus ke pencatatan dan AWS

WAF sumber daya, Anda dapat mengatur sendiri izin tersebut. Untuk informasi tentang mengelola izin, lihat Manajemen akses untuk AWS sumber daya di Panduan Pengguna IAM. Untuk informasi tentang kebijakan yang AWS WAF dikelola, lihatAWS kebijakan terkelola untuk AWS WAF.

Izin ini memungkinkan Anda mengubah konfigurasi pencatatan ACL web, mengonfigurasi pengiriman CloudWatch log untuk Log, dan untuk mengambil informasi tentang grup log Anda. Izin ini harus dilampirkan ke pengguna yang Anda gunakan untuk mengelola AWS WAF.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[

            "wafv2:PutLoggingConfiguration",
            "wafv2:DeleteLoggingConfiguration"
         ],
         "Resource":[
            "*"
         ],
         "Effect":"Allow",
         "Sid":"LoggingConfigurationAPI"
      }
      {
         "Sid":"WebACLLoggingCWL",
         "Action":[
            "logs:CreateLogDelivery",
            "logs:DeleteLogDelivery",
            "logs:PutResourcePolicy",
            "logs:DescribeResourcePolicies",
            "logs:DescribeLogGroups"
         ],
         "Resource":[
            "*"
         ],
         "Effect":"Allow"
      }
   ]
}
```

Ketika tindakan diizinkan pada semua AWS sumber daya, itu ditunjukkan dalam kebijakan dengan `"Resource"` pengaturan`"*"`. Ini berarti bahwa tindakan diizinkan pada semua

AWS sumber daya yang didukung oleh setiap tindakan. Misalnya, tindakan hanya `wafv2:PutLoggingConfiguration` didukung untuk `wafv2` mencatat sumber daya konfigurasi.

Bucket Layanan Penyimpanan Sederhana Amazon

Topik ini memberikan informasi untuk mengirim log lalu lintas ACL web Anda ke bucket Amazon S3.

> **Note**
>
> Anda dikenakan biaya untuk logging selain biaya untuk menggunakan AWS WAF. Untuk informasi, lihat Harga untuk mencatat informasi lalu lintas ACL web.

Untuk mengirim log lalu lintas ACL web Anda ke Amazon S3, Anda menyiapkan bucket Amazon S3 dari akun yang sama seperti yang Anda gunakan untuk mengelola ACL web, dan Anda memberi nama bucket dimulai. `aws-waf-logs-` Saat mengaktifkan login AWS WAF, Anda memberikan nama bucket. Untuk informasi tentang membuat bucket logging, lihat Membuat Bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Anda dapat mengakses dan menganalisis log Amazon S3 Anda menggunakan layanan kueri interaktif Amazon Athena. Athena memudahkan untuk menganalisis data secara langsung di Amazon S3 menggunakan SQL standar. Dengan beberapa tindakan di dalamnya AWS Management Console, Anda dapat mengarahkan Athena ke data yang disimpan di Amazon S3 dan dengan cepat mulai menggunakan SQL standar untuk menjalankan kueri ad-hoc dan mendapatkan hasil. Untuk informasi selengkapnya, lihat Menanyakan AWS WAF log di panduan pengguna Amazon Athena. Untuk contoh tambahan kueri Amazon Athena, lihat waf-log-sample-athenaaws-samples/ -queries di situs web. GitHub

> **Note**
>
> AWS WAF mendukung enkripsi dengan bucket Amazon S3 untuk kunci jenis kunci Amazon S3 (SSE-S3) dan untuk (SSE-KMS). AWS Key Management Service AWS KMS keys AWS WAF tidak mendukung enkripsi untuk AWS Key Management Service kunci yang dikelola oleh AWS.

ACL web Anda mempublikasikan file log mereka ke bucket Amazon S3 dengan interval 5 menit. Setiap file log berisi catatan log untuk lalu lintas yang direkam dalam 5 menit sebelumnya.

Ukuran file maksimum untuk berkas log adalah 75 MB. Jika file log mencapai batas ukuran file dalam periode 5 menit, log berhenti menambahkan catatan ke dalamnya, menerbitkannya ke bucket Amazon S3, dan kemudian membuat file log baru.

Berkas log dikompresi. Jika Anda membuka file menggunakan konsol Amazon S3, Amazon S3 mendekompresi catatan log dan menampilkannya. Jika Anda mengunduh file log, Anda harus mendekompresnya untuk melihat catatan.

Sebuah file log tunggal berisi entri yang disisipkan dengan beberapa catatan. Untuk melihat semua file log untuk ACL web, cari entri yang digabungkan berdasarkan nama ACL web, Wilayah, dan ID akun Anda.

Persyaratan penamaan dan sintaks

Nama bucket Anda untuk AWS WAF logging harus dimulai dengan `aws-waf-logs-` dan dapat diakhiri dengan akhiran apa pun yang Anda inginkan. Misalnya, `aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX`.

Lokasi ember

Lokasi bucket menggunakan sintaks berikut:

```
s3://aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX/
```

ARN Bucket

Format bucket Amazon Resource Name (ARN) adalah sebagai berikut:

```
arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX
```

Lokasi bucket dengan awalan

Jika Anda menggunakan awalan dalam nama kunci objek untuk mengatur data yang disimpan di bucket, Anda dapat memberikan awalan dalam nama bucket logging Anda.

> **Note**
>
> Opsi ini tidak tersedia melalui konsol. Gunakan AWS WAF API, CLI, atau. AWS CloudFormation

Untuk informasi tentang menggunakan awalan di Amazon S3, lihat Mengatur objek menggunakan awalan di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Lokasi bucket dengan awalan menggunakan sintaks berikut:

```
s3://aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX/DOC-EXAMPLE-KEY-NAME-PREFIX/
```

Folder bucket dan nama file

Di dalam bucket Anda, dan mengikuti awalan apa pun yang Anda berikan, AWS WAF log Anda ditulis di bawah struktur folder yang ditentukan oleh ID akun Anda, Wilayah, nama ACL web, dan tanggal dan waktu.

```
AWSLogs/account-id/WAFLogs/Region/web-acl-name/YYYY/MM/dd/HH/mm
```

Di dalam folder, nama file log mengikuti format yang sama:

```
account-id_waflogs_Region_web-acl-name_timestamp_hash.log.gz
```

Spesifikasi waktu yang digunakan dalam struktur folder dan nama file log mematuhi spesifikasi format stempel waktu. YYYYMMddTHHmmZ

Berikut ini menunjukkan contoh file log di bucket Amazon S3 untuk bucket bernama. DOC-EXAMPLE-BUCKET Akun AWS adalah11111111111. Web ACL adalah TEST-WEBACL dan Wilayah adalahus-east-1.

```
s3://DOC-EXAMPLE-BUCKET/AWSLogs/11111111111/WAFLogs/us-east-1/
TEST-WEBACL/2021/10/28/19/50/11111111111_waflogs_us-east-1_TEST-
WEBACL_20211028T1950Z_e0ca43b5.log.gz
```

> **Note**
>
> Nama bucket Anda untuk AWS WAF logging harus dimulai dengan `aws-waf-logs-` dan dapat diakhiri dengan akhiran apa pun yang Anda inginkan.

Izin diperlukan untuk mempublikasikan log ke Amazon S3

Mengonfigurasi pencatatan lalu lintas ACL web untuk bucket Amazon S3 memerlukan pengaturan izin berikut. Izin ini ditetapkan untuk Anda saat Anda menggunakan salah satu kebijakan terkelola

akses AWS WAF penuh, `AWSWAFConsoleFullAccess` atau`AWSWAFFullAccess`. Jika Anda ingin mengelola akses berbutir halus ke pencatatan dan AWS WAF sumber daya, Anda dapat mengatur izin ini sendiri. Untuk informasi tentang mengelola izin, lihat Manajemen akses untuk AWS sumber daya di Panduan Pengguna IAM. Untuk informasi tentang kebijakan AWS WAF terkelola, lihatAWS kebijakan terkelola untuk AWS WAF.

Izin berikut memungkinkan Anda mengubah konfigurasi pencatatan ACL web dan mengonfigurasi pengiriman log ke bucket Amazon S3 Anda. Izin ini harus dilampirkan ke pengguna yang Anda gunakan untuk mengelola AWS WAF.

> **Note**
>
> Saat Anda menetapkan izin yang tercantum di bawah ini, Anda mungkin melihat kesalahan dalam AWS CloudTrail log yang menunjukkan akses ditolak, tetapi izin tersebut benar untuk AWS WAF pencatatan.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "wafv2:PutLoggingConfiguration",
            "wafv2:DeleteLoggingConfiguration"
         ],
         "Resource":[
            "*"
         ],
         "Effect":"Allow",
         "Sid":"LoggingConfigurationAPI"
      },
    {

       "Sid":"WebACLLogDelivery",

       "Action":[

          "logs:CreateLogDelivery",

          "logs:DeleteLogDelivery"
```

```
        ],

        "Resource": "*",

        "Effect":"Allow"

    },
      {
         "Sid":"WebACLLoggingS3",
         "Action":[
            "s3:PutBucketPolicy",
            "s3:GetBucketPolicy"
         ],
         "Resource": [
                "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET"
         ],
         "Effect":"Allow"
      }
   ]
}
```

Ketika tindakan diizinkan pada semua AWS sumber daya, itu ditunjukkan dalam kebijakan dengan `"Resource"` pengaturan`"*"`. Ini berarti bahwa tindakan diizinkan pada semua AWS sumber daya yang didukung oleh setiap tindakan. Misalnya, tindakan hanya `wafv2:PutLoggingConfiguration` didukung untuk `wafv2` mencatat sumber daya konfigurasi.

Secara default, ember Amazon S3 dan objek yang dikandungnya bersifat pribadi. Hanya pemilik bucket yang bisa mengakses bucket dan objek yang tersimpan di dalamnya. Namun, pemilik bucket dapat memberikan akses ke sumber daya dan pengguna lain dengan menulis kebijakan akses.

Jika pengguna yang membuat log memiliki bucket, layanan akan secara otomatis melampirkan kebijakan berikut ke bucket untuk memberikan izin log untuk memublikasikan log ke bucket:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryWrite",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
```

```
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET/AWSLogs/account-id/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "aws:SourceAccount": ["account-id"]
        },
        "ArnLike": {
          "aws:SourceArn": ["arn:aws:logs:region:account-id:*"]
        }
      }
    },
    {
      "Sid": "AWSLogDeliveryAclCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": ["account-id"]
        },
        "ArnLike": {
          "aws:SourceArn": ["arn:aws:logs:region:account-id:*"]
        }
      }
    }
  ]
}
```

> **Note**
>
> Nama bucket Anda untuk AWS WAF logging harus dimulai dengan `aws-waf-logs-` dan dapat diakhiri dengan akhiran apa pun yang Anda inginkan.

Jika pengguna yang membuat log tidak memiliki bucket, atau tidak memiliki `PutBucketPolicy` izin `GetBucketPolicy` dan untuk bucket, pembuatan log gagal. Dalam hal ini, pemilik bucket harus menambahkan kebijakan sebelumnya secara manual ke bucket dan menentukan ID pembuat log. Akun AWS Untuk informasi selengkapnya, lihat Bagaimana Cara Menambahkan Kebijakan Bucket

S3? di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon. Jika bucket menerima log dari beberapa akun, tambahkan entri `Resource` elemen ke pernyataan `AWSLogDeliveryWrite` kebijakan untuk setiap akun.

Misalnya, kebijakan bucket berikut memungkinkan Akun AWS `111122223333` untuk memublikasikan log ke bucket bernama`aws-waf-logs-`*`DOC-EXAMPLE-BUCKET`*:

```
{
    "Version": "2012-10-17",
    "Id": "AWSLogDeliveryWrite20150319",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
                "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET/
AWSLogs/111122223333/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": ["111122223333"]
                },
                "ArnLike": {
                    "aws:SourceArn": ["arn:aws:logs:us-east-1:111122223333:*"]
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET",
            "Condition": {
                "StringEquals": {
                "aws:SourceAccount": ["111122223333"]
                },
                "ArnLike": {
```

```
                "aws:SourceArn": ["arn:aws:logs:us-east-1:111122223333:*"]
                }
            }
        }
    ]
}
```

Izin untuk menggunakan AWS Key Management Service dengan kunci KMS

Jika tujuan pencatatan Anda menggunakan enkripsi sisi server dengan kunci yang disimpan di AWS Key Management Service (SSE-KMS) dan Anda menggunakan kunci terkelola pelanggan (kunci KMS), Anda harus memberikan AWS WAF izin untuk menggunakan kunci KMS Anda. Untuk melakukan ini, Anda menambahkan kebijakan kunci ke kunci KMS untuk tujuan yang Anda pilih. Ini memungkinkan AWS WAF logging untuk menulis file log Anda ke tujuan Anda.

Tambahkan kebijakan kunci berikut ke kunci KMS Anda untuk memungkinkan masuk AWS WAF ke bucket Amazon S3 Anda.

```
{
    "Sid": "Allow AWS WAF to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "delivery.logs.amazonaws.com"
        ]
    },
    "Action": "kms:GenerateDataKey*",
    "Resource": "*"
}
```

Izin diperlukan untuk mengakses file log Amazon S3

Amazon S3 menggunakan daftar kontrol akses (ACL) untuk mengelola akses ke file log yang dibuat oleh log. AWS WAF Secara default, pemilik bucket memiliki izin `FULL_CONTROL` pada setiap file berkas log. Pemilik pengiriman log, jika berbeda dari pemilik bucket, tidak memiliki izin. Akun pengiriman log memiliki izin `READ` dan `WRITE`. Untuk informasi selengkapnya, lihat Ikhtisar Daftar Kontrol Akses (ACL) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Aliran pengiriman Amazon Data Firehose

Bagian ini memberikan informasi untuk mengirim log lalu lintas ACL web Anda ke aliran pengiriman Amazon Data Firehose.

> **Note**
>
> Anda dikenakan biaya untuk logging selain biaya untuk menggunakan AWS WAF. Untuk informasi, lihat Harga untuk mencatat informasi lalu lintas ACL web.

Untuk mengirim log ke Amazon Data Firehose, Anda mengirim log dari ACL web Anda ke aliran pengiriman Amazon Data Firehose yang Anda konfigurasikan di Firehose. Setelah Anda mengaktifkan logging, AWS WAF mengirimkan log ke tujuan penyimpanan Anda melalui titik akhir HTTPS Firehose.

Satu AWS WAF log setara dengan satu catatan Firehose. Jika Anda biasanya menerima 10.000 permintaan per detik dan mengaktifkan log penuh, Anda harus memiliki pengaturan 10.000 catatan per detik di Firehose. Jika Anda tidak mengonfigurasi Firehose dengan benar, tidak AWS WAF akan merekam semua log. Untuk informasi selengkapnya, lihat kuota Amazon Kinesis Data Firehose.

Untuk informasi tentang cara membuat aliran pengiriman Amazon Data Firehose dan meninjau log yang disimpan, lihat Apa itu Amazon Data Firehose?

Untuk informasi tentang membuat aliran pengiriman, lihat Membuat aliran pengiriman Amazon Data Firehose.

Mengonfigurasi aliran pengiriman Amazon Data Firehose untuk ACL web Anda

Konfigurasikan aliran pengiriman Amazon Data Firehose untuk ACL web Anda sebagai berikut.

- Buat menggunakan akun yang sama seperti yang Anda gunakan untuk mengelola ACL web.
- Buat di Wilayah yang sama dengan ACL web. Jika Anda menangkap log untuk Amazon CloudFront, buat firehose di Wilayah AS Timur (Virginia N.),. `us-east-1`
- Berikan firehose data nama yang dimulai dengan awalan`aws-waf-logs-`. Misalnya, `aws-waf-logs-us-east-2-analytics`.
- Konfigurasikan untuk direct put, yang memungkinkan aplikasi mengakses aliran pengiriman secara langsung. Di konsol Amazon Data Firehose, untuk setelan Sumber aliran pengiriman, pilih Direct PUT atau sumber lainnya. Melalui API, atur properti aliran pengiriman `DeliveryStreamType` ke`DirectPut`.

> **Note**
>
> Jangan gunakan `Kinesis stream` sebagai sumber Anda.

Izin yang diperlukan untuk memublikasikan log ke aliran pengiriman Amazon Data Firehose

Untuk memahami izin yang diperlukan untuk konfigurasi Firehose Data Kinesis, lihat Mengontrol Akses dengan Amazon Kinesis Data Firehose.

Anda harus memiliki izin berikut agar berhasil mengaktifkan pencatatan ACL web dengan aliran pengiriman Amazon Data Firehose.

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `wafv2:PutLoggingConfiguration`

Untuk informasi tentang peran terkait layanan dan `iam:CreateServiceLinkedRole` izin, lihat. Menggunakan peran terkait layanan untuk AWS WAF

Konfigurasi pencatatan ACL web

Anda dapat mengaktifkan dan menonaktifkan logging untuk ACL web kapan saja.

> **Note**
>
> Anda dikenakan biaya untuk logging selain biaya untuk menggunakan AWS WAF. Untuk informasi, lihat Harga untuk mencatat informasi lalu lintas ACL web.

Jika Anda tidak dapat menemukan catatan log di log Anda

Pada kesempatan langka, pengiriman AWS WAF log mungkin turun di bawah 100%, dengan log dikirim dengan upaya terbaik. AWS WAF Arsitektur memprioritaskan keamanan aplikasi Anda di atas semua pertimbangan lainnya. Dalam beberapa situasi, seperti ketika arus logging mengalami pembatasan lalu lintas, ini dapat mengakibatkan catatan dijatuhkan. Ini seharusnya tidak mempengaruhi lebih dari beberapa catatan. Jika Anda melihat sejumlah entri log yang hilang, hubungi AWS Support Pusat.

Dalam konfigurasi logging untuk ACL web Anda, Anda dapat menyesuaikan apa yang AWS WAF dikirim ke log.

- Redaksi bidang - Anda dapat menyunting bidang berikut dari catatan log untuk aturan yang menggunakan pengaturan kecocokan yang sesuai: jalur URI, String kueri, Header tunggal, dan metode HTTP. Bidang yang disunting muncul seperti `REDACTED` di log. Misalnya, jika Anda menyunting bidang string Query, di log, itu akan terdaftar sebagai `REDACTED` untuk semua aturan yang menggunakan pengaturan komponen pencocokan string Query. Redaksi hanya berlaku untuk komponen permintaan yang Anda tentukan untuk pencocokan dalam aturan, sehingga redaksi komponen header Tunggal tidak berlaku untuk aturan yang cocok di Header. Untuk daftar bidang log, lihatBidang log.

  > **Note**
  >
  > Pengaturan ini tidak berdampak pada pengambilan sampel permintaan. Dengan pengambilan sampel permintaan, satu-satunya cara untuk mengecualikan bidang adalah dengan menonaktifkan pengambilan sampel untuk ACL web.

- Pemfilteran log - Anda dapat menambahkan pemfilteran untuk menentukan permintaan web mana yang disimpan di log dan mana yang dijatuhkan. Anda memfilter pengaturan yang AWS WAF berlaku selama evaluasi permintaan web. Anda dapat memfilter pada pengaturan berikut:
  - Label yang sepenuhnya memenuhi syarat - Label yang sepenuhnya memenuhi syarat memiliki awalan, ruang nama opsional, dan nama label. Prefiks mengidentifikasi grup aturan atau konteks ACL web aturan yang menambahkan label. Untuk informasi tentang label, lihatAWS WAF label pada permintaan web.
  - Tindakan aturan - Anda dapat memfilter pada pengaturan tindakan aturan normal dan juga pada opsi `EXCLUDED_AS_COUNT` penggantian lama untuk aturan grup aturan. Untuk informasi tentang setelan tindakan aturan, lihatTindakan aturan. Untuk informasi tentang penggantian tindakan aturan saat ini dan lama untuk aturan grup aturan, lihat. Opsi penggantian tindakan untuk grup aturan
    - Filter tindakan aturan normal berlaku untuk tindakan yang dikonfigurasi dalam aturan dan juga tindakan yang dikonfigurasi menggunakan opsi saat ini untuk mengganti tindakan aturan grup aturan.
    - Filter `EXCLUDED_AS_COUNT` log tumpang tindih dengan filter log `Count` tindakan. `EXCLUDED_AS_COUNT`memfilter opsi saat ini dan lama untuk mengganti tindakan aturan grup aturan ke. Count

Mengaktifkan pencatatan untuk ACL web

Untuk mengaktifkan pencatatan untuk ACL web, Anda harus sudah mengonfigurasi tujuan pencatatan. Untuk informasi tentang pilihan tujuan Anda dan persyaratan untuk masing-masing, lihatAWS WAF tujuan pencatatan.

Untuk mengaktifkan pencatatan untuk ACL web

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.
2. Di panel navigasi, pilih Web ACL.
3. Pilih nama ACL web yang ingin Anda aktifkan untuk login. Konsol membawa Anda ke deskripsi ACL web, tempat Anda dapat mengeditnya.
4. Pada tab Logging, pilih Aktifkan logging.
5. Pilih jenis tujuan pencatatan, lalu pilih tujuan pencatatan yang Anda konfigurasikan. Anda harus memilih tujuan logging yang namanya dimulai dengan`aws-waf-logs-`.
6. (Opsional) Jika Anda tidak ingin beberapa bidang disertakan dalam log, edit. Pilih bidang yang akan disunting, lalu pilih Tambah. Ulangi seperlunya untuk menyunting bidang tambahan.

   > **Note**
   >
   > Pengaturan ini tidak berdampak pada pengambilan sampel permintaan. Dengan pengambilan sampel permintaan, satu-satunya cara untuk mengecualikan bidang adalah dengan menonaktifkan pengambilan sampel untuk ACL web.

7. (Opsional) Jika Anda tidak ingin mengirim semua permintaan ke log, tambahkan kriteria dan perilaku pemfilteran Anda. Di bawah Filter log, untuk setiap filter yang ingin Anda terapkan, pilih Tambahkan filter, lalu pilih kriteria pemfilteran Anda dan tentukan apakah Anda ingin menyimpan atau menghapus permintaan yang sesuai dengan kriteria. Ketika Anda selesai menambahkan filter, jika diperlukan, ubah perilaku logging Default.
8. Pilih Aktifkan logging.

> **Note**
>
> Bila Anda berhasil mengaktifkan logging, AWS WAF akan membuat peran service-linked dengan izin yang diperlukan untuk menulis log ke tujuan logging. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk AWS WAF.

Bidang log

Daftar berikut menjelaskan bidang log yang mungkin.

tindakan

Tindakan penghentian yang AWS WAF diterapkan pada permintaan. Ini menunjukkan baik allow, block, CAPTCHA, atau challenge. ChallengeTindakan CAPTCHA dan akan berakhir ketika permintaan web tidak berisi token yang valid.

argumen

String kueri.

CaptCharesponse

Status tindakan CAPTCHA untuk permintaan, diisi saat CAPTCHA tindakan diterapkan ke permintaan. Bidang ini diisi untuk CAPTCHA tindakan apa pun, baik penghentian atau non-penghentian. Jika permintaan memiliki CAPTCHA tindakan yang diterapkan beberapa kali, bidang ini diisi dari terakhir kali tindakan diterapkan.

CAPTCHATindakan menghentikan pemeriksaan permintaan web ketika permintaan tidak menyertakan token atau token tidak valid atau kedaluwarsa. Jika CAPTCHA tindakan dihentikan, bidang ini menyertakan kode respons dan alasan kegagalan. Jika tindakan tidak berakhir, bidang ini menyertakan stempel waktu pemecahan. Untuk membedakan antara tindakan terminating dan non-terminating, Anda dapat memfilter atribut yang tidak kosong `failureReason` di bidang ini.

ChallengeResponse

Status tindakan tantangan untuk permintaan, diisi saat Challenge tindakan diterapkan pada permintaan. Bidang ini diisi untuk Challenge tindakan apa pun, baik penghentian atau non-penghentian. Jika permintaan memiliki Challenge tindakan yang diterapkan beberapa kali, bidang ini diisi dari terakhir kali tindakan diterapkan.

ChallengeTindakan menghentikan pemeriksaan permintaan web ketika permintaan tidak menyertakan token atau token tidak valid atau kedaluwarsa. Jika Challenge tindakan dihentikan, bidang ini menyertakan kode respons dan alasan kegagalan. Jika tindakan tidak berakhir, bidang ini menyertakan stempel waktu pemecahan. Untuk membedakan antara tindakan terminating dan non-terminating, Anda dapat memfilter atribut yang tidak kosong `failureReason` di bidang ini.

clientIp

Alamat IP klien yang mengirim permintaan.

negeri

Negara sumber permintaan. Jika AWS WAF tidak dapat menentukan negara asal, ia menetapkan bidang ini ke`-`.

excludedRules

Digunakan hanya untuk aturan kelompok aturan. Daftar aturan dalam grup aturan yang telah Anda kecualikan. Tindakan untuk aturan ini diatur keCount.

Jika Anda mengganti aturan untuk dihitung menggunakan opsi tindakan aturan ganti, kecocokan tidak tercantum di sini. Mereka terdaftar sebagai pasangan aksi `action` dan`overriddenAction`.

exclusionType

Jenis yang menunjukkan bahwa aturan yang dikecualikan memiliki tindakanCount.

ruleId

ID aturan dalam kelompok aturan yang dikecualikan.

formatVersion

Versi format untuk log.

headers

Daftar header.

httpMethod

Metode HTTP dalam permintaan.

httpRequest

Metadata tentang permintaan.

httpSourceId

ID sumber daya terkait:

- Untuk CloudFront distribusi Amazon, ID adalah *distribution-id* dalam sintaks ARN:

  arn:*partition*cloudfront::*account-id*:distribution/*distribution-id*

- Untuk Application Load Balancer, ID adalah *load-balancer-id* dalam sintaks ARN:

  arn:*partition*:elasticloadbalancing:*region*:*account-id*:loadbalancer/app/*load-balancer-name/load-balancer-id*

- Untuk API REST Amazon API Gateway, ID adalah *api-id* dalam sintaks ARN:

  arn:*partition*:apigateway:*region*::/restapis/*api-id*/stages/*stage-name*

- Untuk AWS AppSync GraphQL API, ID adalah *GraphQLApiId* dalam sintaks ARN:

  arn:*partition*:appsync:*region*:*account-id*:apis/*GraphQLApiId*

- Untuk kumpulan pengguna Amazon Cognito, ID adalah *user-pool-id* dalam sintaks ARN:

  arn:*partition*:cognito-idp:*region*:*account-id*:userpool/*user-pool-id*

- Untuk AWS App Runner layanan, ID adalah *apprunner-service-id* dalam sintaks ARN:

  arn:*partition*:apprunner:*region*:*account-id*:service/*apprunner-service-name/apprunner-service-id*

httpSourceName

Sumber permintaan. Nilai yang memungkinkan: `CF` untuk Amazon CloudFront, `APIGW` untuk Amazon API Gateway, `ALB` untuk Application Load Balancer, `APPSYNC` untuk, untuk Amazon Cognito AWS AppSync, `COGNITOIDP` untuk App Runner`APPRUNNER`, `VERIFIED_ACCESS` dan untuk Akses Terverifikasi.

httpVersion

Versi HTTP.

Ja3sidik jari

Sidik jari JA3 dari permintaan tersebut.

> **Note**
>
> Pemeriksaan sidik jari JA3 hanya tersedia untuk CloudFront distribusi Amazon dan Application Load Balancer.

Sidik jari JA3 adalah hash 32 karakter yang berasal dari TLS Client Hello dari permintaan yang masuk. Sidik jari ini berfungsi sebagai pengenal unik untuk konfigurasi TLS klien. AWS WAF menghitung dan mencatat sidik jari ini untuk setiap permintaan yang memiliki cukup informasi TLS Client Hello untuk perhitungan.

Anda memberikan nilai ini ketika Anda mengonfigurasi kecocokan sidik jari JA3 dalam aturan ACL web Anda. Untuk informasi tentang membuat kecocokan dengan sidik jari JA3, lihat Sidik jari JA3 di Minta opsi komponen untuk pernyataan aturan.

label

Label pada permintaan web. Label ini diterapkan oleh aturan yang digunakan untuk mengevaluasi permintaan. AWS WAF mencatat 100 label pertama.

nonTerminatingMatchingAturan

Daftar aturan non-penghentian yang cocok dengan permintaan. Setiap item dalam daftar berisi informasi berikut.

tindakan

Tindakan yang AWS WAF diterapkan pada permintaan. Ini menunjukkan hitungan, CAPTCHA, atau tantangan. The CAPTCHA and Challenge non-terminating ketika permintaan web berisi token yang valid.

ruleId

ID aturan yang cocok dengan permintaan dan tidak mengakhiri.

ruleMatchDetails

Informasi terperinci tentang aturan yang cocok dengan permintaan. Bidang ini hanya diisi untuk pernyataan aturan pencocokan SQL injection dan cross-site scripting (XSS). Aturan pencocokan mungkin memerlukan kecocokan untuk lebih dari satu kriteria pemeriksaan, jadi detail kecocokan ini disediakan sebagai larik kriteria kecocokan.

Setiap informasi tambahan yang diberikan untuk setiap aturan bervariasi menurut faktor seperti konfigurasi aturan, jenis pencocokan aturan, dan detail pertandingan. Misalnya

untuk aturan dengan Challenge tindakan CAPTCHA atau, `captchaResponse` atau `challengeResponse` akan terdaftar. Jika aturan pencocokan ada dalam grup aturan dan Anda telah mengganti tindakan aturan yang dikonfigurasi, tindakan yang dikonfigurasi akan disediakan. `overriddenAction`

OversizeFields

Daftar bidang dalam permintaan web yang diperiksa oleh ACL web dan yang melebihi batas AWS WAF inspeksi. Jika bidang terlalu besar tetapi ACL web tidak memeriksanya, itu tidak akan tercantum di sini.

Daftar ini dapat berisi nol atau lebih dari nilai-nilai berikut:`REQUEST_BODY`,`REQUEST_JSON_BODY`,`REQUEST_HEADERS`, dan`REQUEST_COOKIES`. Untuk informasi selengkapnya tentang bidang oversize, lihatPenanganan komponen permintaan kebesaran di AWS WAF.

rateBasedRuleDaftar

Daftar aturan berbasis tarif yang bertindak atas permintaan. Untuk informasi tentang aturan berbasis tarif, lihat. Pernyataan aturan berbasis tarif

rateBasedRuleId

ID aturan berbasis tarif yang bertindak atas permintaan. Jika ini telah menghentikan permintaan, ID untuk `rateBasedRuleId` sama dengan ID untuk`terminatingRuleId`.

rateBasedRuleNama

Nama aturan berbasis tarif yang bertindak atas permintaan.

limitKey

Jenis agregasi yang digunakan aturan. Nilai yang mungkin adalah `IP` untuk asal permintaan web, `FORWARDED_IP` untuk IP yang diteruskan dalam header dalam permintaan, `CUSTOMKEYS` untuk pengaturan kunci agregat kustom. dan `CONSTANT` untuk menghitung semua permintaan bersama-sama, tanpa agregasi.

LimitValue

Digunakan hanya ketika tingkat dibatasi oleh satu jenis alamat IP. Jika permintaan berisi alamat IP yang tidak valid, `limitvalue` adalah`INVALID`.

maxRateAllowed

Jumlah maksimum permintaan yang diizinkan dalam jendela waktu yang ditentukan untuk contoh agregasi tertentu. Instans agregasi ditentukan oleh `limitKey` plus setiap spesifikasi kunci tambahan yang telah Anda berikan dalam konfigurasi aturan berbasis laju.

evaluationWindowSec

Jumlah waktu yang AWS WAF termasuk dalam permintaannya dihitung, dalam hitungan detik.

CustomValues

Nilai unik yang diidentifikasi oleh aturan berbasis tarif dalam permintaan. Untuk nilai string, log mencetak 32 karakter pertama dari nilai string. Tergantung pada jenis kunci, nilai-nilai ini mungkin hanya untuk kunci, seperti untuk metode HTTP atau string kueri, atau mereka mungkin untuk kunci dan nama, seperti untuk header dan nama header.

requestHeadersInserted

Daftar header dimasukkan untuk penanganan permintaan kustom.

requestId

ID permintaan, yang dihasilkan oleh layanan host yang mendasarinya. Untuk Application Load Balancer, ini adalah ID jejak. Untuk semua yang lain, ini adalah ID permintaan.

responseCodeSent

Kode respon dikirim dengan respon kustom.

ruleGroupId

ID dari grup aturan. Jika aturan memblokir permintaan, ID `ruleGroupID` untuk sama dengan ID untuk`terminatingRuleId`.

ruleGroupList

Daftar grup aturan yang bertindak atas permintaan ini, dengan informasi kecocokan.

terminatingRule

Aturan yang mengakhiri permintaan. Jika ini ada, itu berisi informasi berikut.

tindakan

Tindakan penghentian yang AWS WAF diterapkan pada permintaan. Ini menunjukkan baik allow, block, CAPTCHA, atau challenge. ChallengeTindakan CAPTCHA dan akan berakhir ketika permintaan web tidak berisi token yang valid.

ruleId

ID aturan yang cocok dengan permintaan.

ruleMatchDetails

Informasi terperinci tentang aturan yang cocok dengan permintaan. Bidang ini hanya diisi untuk pernyataan aturan pencocokan SQL injection dan cross-site scripting (XSS). Aturan pencocokan mungkin memerlukan kecocokan untuk lebih dari satu kriteria pemeriksaan, jadi detail kecocokan ini disediakan sebagai larik kriteria kecocokan.

Setiap informasi tambahan yang diberikan untuk setiap aturan bervariasi menurut faktor seperti konfigurasi aturan, jenis pencocokan aturan, dan detail pertandingan. Misalnya untuk aturan dengan Challenge tindakan CAPTCHA atau, `captchaResponse` atau `challengeResponse` akan terdaftar. Jika aturan pencocokan ada dalam grup aturan dan Anda telah mengganti tindakan aturan yang dikonfigurasi, tindakan yang dikonfigurasi akan disediakan. `overriddenAction`

terminatingRuleId

ID aturan yang mengakhiri permintaan. Jika tidak ada yang mengakhiri permintaan, nilainya adalah`Default_Action`.

terminatingRuleMatchDetail

Informasi terperinci tentang aturan penghentian yang cocok dengan permintaan. Aturan penghentian memiliki tindakan yang mengakhiri proses inspeksi terhadap permintaan web. Tindakan yang mungkin untuk aturan penghentian termasukAllow,, BlockCAPTCHA, danChallenge. Selama inspeksi permintaan web, pada aturan pertama yang cocok dengan permintaan dan yang memiliki tindakan AWS WAF penghentian, menghentikan inspeksi dan menerapkan tindakan. Permintaan web mungkin berisi ancaman lain, selain yang dilaporkan dalam log untuk aturan penghentian yang cocok.

Ini hanya diisi untuk pernyataan aturan pencocokan SQL injection dan cross-site scripting (XSS). Aturan pencocokan mungkin memerlukan kecocokan untuk lebih dari satu kriteria inspeksi, jadi detail kecocokan ini disediakan sebagai larik kriteria kecocokan.

terminatingRuleType

Jenis aturan yang mengakhiri permintaan. Nilai yang mungkin: RATE_BASED, REGULAR, GROUP, dan MANAGED_RULE_GROUP.

timestamp

Stempel waktu dalam milidetik.

uri

URI permintaan.

webaclId

GUID dari web ACL.

Contoh log

Example Aturan berbasis tingkat 1: Konfigurasi aturan dengan satu kunci, atur ke **`Header:dogname`**

```
{
  "Name": "RateBasedRule",
  "Priority": 1,
  "Statement": {
    "RateBasedStatement": {
      "Limit": 100,
      "AggregateKeyType": "CUSTOM_KEYS",
      "CustomKeys": [
        {
          "Header": {
            "Name": "dogname",
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
        }
      ]
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
```

```
        "MetricName": "RateBasedRule"
      }
    }
```

Example Aturan berbasis tarif 1: Entri log untuk permintaan yang diblokir oleh aturan berbasis tarif

```
{
   "timestamp":1683355579981,
   "formatVersion":1,
   "webaclId": ...,
   "terminatingRuleId":"RateBasedRule",
   "terminatingRuleType":"RATE_BASED",
   "action":"BLOCK",
   "terminatingRuleMatchDetails":[

   ],
   "httpSourceName":"APIGW",
   "httpSourceId":"EXAMPLE11:rjvegx5guh:CanaryTest",
   "ruleGroupList":[

   ],
   "rateBasedRuleList":[
      {
         "rateBasedRuleId": ...,
         "rateBasedRuleName":"RateBasedRule",
         "limitKey":"CUSTOMKEYS",
         "maxRateAllowed":100,
         "evaluationWindowSec":"120",
         "customValues":[
            {
               "key":"HEADER",
               "name":"dogname",
               "value":"ella"
            }
         ]
      }
   ],
   "nonTerminatingMatchingRules":[

   ],
   "requestHeadersInserted":null,
   "responseCodeSent":null,
   "httpRequest":{
```

```
      "clientIp":"52.46.82.45",
      "country":"FR",
      "headers":[
         {
            "name":"X-Forwarded-For",
            "value":"52.46.82.45"
         },
         {
            "name":"X-Forwarded-Proto",
            "value":"https"
         },
         {
            "name":"X-Forwarded-Port",
            "value":"443"
         },
         {
            "name":"Host",
            "value":"rjvegx5guh.execute-api.eu-west-3.amazonaws.com"
         },
         {
            "name":"X-Amzn-Trace-Id",
            "value":"Root=1-645566cf-7cb058b04d9bb3ee01dc4036"
         },
         {
            "name":"dogname",
            "value":"ella"
         },
         {
            "name":"User-Agent",
            "value":"RateBasedRuleTestKoipOneKeyModulePV2"
         },
         {
            "name":"Accept-Encoding",
            "value":"gzip,deflate"
         }
      ],
      "uri":"/CanaryTest",
      "args":"",
      "httpVersion":"HTTP/1.1",
      "httpMethod":"GET",
      "requestId":"Ed0AiHF_CGYF-DA="
   }
}
```

Example Aturan berbasis tingkat 2: Konfigurasi aturan dengan dua tombol, diatur ke dan **`Header:dognameHeader:catname`**

```
{
  "Name": "RateBasedRule",
  "Priority": 1,
  "Statement": {
    "RateBasedStatement": {
      "Limit": 100,
      "AggregateKeyType": "CUSTOM_KEYS",
      "CustomKeys": [
        {
          "Header": {
            "Name": "dogname",
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
        },
        {
          "Header": {
            "Name": "catname",
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
        }
      ]
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "RateBasedRule"
```

```
      }
    }
```

Example Aturan berbasis tarif 2: Entri log untuk permintaan yang diblokir oleh aturan berbasis tarif

```
{
   "timestamp":1633322211194,
   "formatVersion":1,
   "webaclId":...,
   "terminatingRuleId":"RateBasedRule",
   "terminatingRuleType":"RATE_BASED",
   "action":"BLOCK",
   "terminatingRuleMatchDetails":[

   ],
   "httpSourceName":"APIGW",
   "httpSourceId":"EXAMPLE11:rjvegx5guh:CanaryTest",
   "ruleGroupList":[

   ],
   "rateBasedRuleList":[
      {
         "rateBasedRuleId":...,
         "rateBasedRuleName":"RateBasedRule",
         "limitKey":"CUSTOMKEYS",
         "maxRateAllowed":100,
         "evaluationWindowSec":"120",
         "customValues":[
            {
               "key":"HEADER",
               "name":"dogname",
               "value":"ella"
            },
            {
               "key":"HEADER",
               "name":"catname",
               "value":"goofie"
            }
         ]
      }
   ],
   "nonTerminatingMatchingRules":[
```

```
    ],
    "requestHeadersInserted":null,
    "responseCodeSent":null,
    "httpRequest":{
       "clientIp":"52.46.82.35",
       "country":"FR",
       "headers":[
          {
             "name":"X-Forwarded-For",
             "value":"52.46.82.35"
          },
          {
             "name":"X-Forwarded-Proto",
             "value":"https"
          },
          {
             "name":"X-Forwarded-Port",
             "value":"443"
          },
          {
             "name":"Host",
             "value":"23llbyn8v3.execute-api.eu-west-3.amazonaws.com"
          },
          {
             "name":"X-Amzn-Trace-Id",
             "value":"Root=1-64556629-17ac754c2ed9f0620e0f2a0c"
          },
          {
             "name":"catname",
             "value":"goofie"
          },
          {
             "name":"dogname",
             "value":"ella"
          },
          {
             "name":"User-Agent",
             "value":"Apache-HttpClient/UNAVAILABLE (Java/11.0.19)"
          },
          {
             "name":"Accept-Encoding",
             "value":"gzip,deflate"
          }
       ],
```

```
      "uri":"/CanaryTest",
      "args":"",
      "httpVersion":"HTTP/1.1",
      "httpMethod":"GET",
      "requestId":"EdzmlH5OCGYF1vQ="
   }
}
```

Example Keluaran log untuk aturan yang dipicu pada deteksi SQLi (penghentian)

```
{
    "timestamp": 1576280412771,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:ap-southeast-2:111122223333:regional/webacl/
STMTest/1EXAMPLE-2ARN-3ARN-4ARN-123456EXAMPLE",
    "terminatingRuleId": "STMTest_SQLi_XSS",
    "terminatingRuleType": "REGULAR",
    "action": "BLOCK",
    "terminatingRuleMatchDetails": [
        {
            "conditionType": "SQL_INJECTION",
            "sensitivityLevel": "HIGH",
            "location": "HEADER",
            "matchedData": [
                "10",
                "AND",
                "1"
            ]
        }
    ],
    "httpSourceName": "-",
    "httpSourceId": "-",
    "ruleGroupList": [],
    "rateBasedRuleList": [],
    "nonTerminatingMatchingRules": [],
    "httpRequest": {
        "clientIp": "1.1.1.1",
        "country": "AU",
        "headers": [
            {
                "name": "Host",
                "value": "localhost:1989"
            },
```

```
            {
                "name": "User-Agent",
                "value": "curl/7.61.1"
            },
            {
                "name": "Accept",
                "value": "*/*"
            },
            {
                "name": "x-stm-test",
                "value": "10 AND 1=1"
            }
        ],
        "uri": "/myUri",
        "args": "",
        "httpVersion": "HTTP/1.1",
        "httpMethod": "GET",
        "requestId": "rid"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example Keluaran log untuk aturan yang dipicu pada deteksi SQLi (non-terminating)

```
{
    "timestamp":1592357192516
    ,"formatVersion":1
    ,"webaclId":"arn:aws:wafv2:us-east-1:123456789012:global/webacl/hello-
world/5933d6d9-9dde-js82-v8aw-9ck28nv9"
    ,"terminatingRuleId":"Default_Action"
    ,"terminatingRuleType":"REGULAR"
    ,"action":"ALLOW"
    ,"terminatingRuleMatchDetails":[]
    ,"httpSourceName":"-"
    ,"httpSourceId":"-"
    ,"ruleGroupList":[]
    ,"rateBasedRuleList":[]
    ,"nonTerminatingMatchingRules":
    [{
```

```
        "ruleId":"TestRule"
        ,"action":"COUNT"
        ,"ruleMatchDetails":
        [{
            "conditionType":"SQL_INJECTION"
            ,"sensitivityLevel": "HIGH"
            ,"location":"HEADER"
            ,"matchedData":[
                "10"
                ,"and"
                ,"1"]
            }]
    }]
    ,"httpRequest":{
        "clientIp":"3.3.3.3"
        ,"country":"US"
        ,"headers":[
            {"name":"Host","value":"localhost:1989"}
            ,{"name":"User-Agent","value":"curl/7.61.1"}
            ,{"name":"Accept","value":"*/*"}
            ,{"name":"myHeader","myValue":"10 AND 1=1"}
            ]
            ,"uri":"/myUri","args":""
            ,"httpVersion":"HTTP/1.1"
            ,"httpMethod":"GET"
            ,"requestId":"rid"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example Keluaran log untuk beberapa aturan yang dipicu di dalam grup aturan (Aturan-XSS berakhir dan Aturan-B tidak berakhir)

```
{
    "timestamp":1592361810888,
    "formatVersion":1,
    "webaclId":"arn:aws:wafv2:us-east-1:123456789012:global/webacl/hello-
world/5933d6d9-9dde-js82-v8aw-9ck28nv9"
    ,"terminatingRuleId":"RG-Reference"
```

```
    ,"terminatingRuleType":"GROUP"
    ,"action":"BLOCK",
    "terminatingRuleMatchDetails":
    [{
        "conditionType":"XSS"
        ,"location":"HEADER"
        ,"matchedData":["<","frameset"]
    }]
    ,"httpSourceName":"-"
    ,"httpSourceId":"-"
    ,"ruleGroupList":
    [{
        "ruleGroupId":"arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/hello-
world/c05lb698-1f11-4m41-aef4-99a506d53f4b"
        ,"terminatingRule":{
            "ruleId":"RuleA-XSS"
            ,"action":"BLOCK"
            ,"ruleMatchDetails":null
            }
        ,"nonTerminatingMatchingRules":
        [{
            "ruleId":"RuleB-SQLi"
            ,"action":"COUNT"
            ,"ruleMatchDetails":
            [{
                "conditionType":"SQL_INJECTION"
                ,"sensitivityLevel": "LOW"
                ,"location":"HEADER"
                ,"matchedData":[
                    "10"
                    ,"and"
                    ,"1"]
            }]
        }]
        ,"excludedRules":null
    }]
    ,"rateBasedRuleList":[]
    ,"nonTerminatingMatchingRules":[]
    ,"httpRequest":{
        "clientIp":"3.3.3.3"
        ,"country":"US"
        ,"headers":
        [
            {"name":"Host","value":"localhost:1989"}
```

```
            ,{"name":"User-Agent","value":"curl/7.61.1"}
            ,{"name":"Accept","value":"*/*"}
            ,{"name":"myHeader1","value":"<frameset onload=alert(1)>"}
            ,{"name":"myHeader2","value":"10 AND 1=1"}
            ]
        ,"uri":"/myUri"
        ,"args":""
        ,"httpVersion":"HTTP/1.1"
        ,"httpMethod":"GET"
        ,"requestId":"rid"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example Keluaran log untuk aturan yang dipicu untuk inspeksi badan permintaan dengan tipe konten JSON

AWS WAF saat ini melaporkan lokasi untuk inspeksi badan JSON sebagai`UNKNOWN`.

```
{
    "timestamp": 1576280412771,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:ap-southeast-2:123456789012:regional/webacl/test/111",
    "terminatingRuleId": "STMTest_SQLi_XSS",
    "terminatingRuleType": "REGULAR",
    "action": "BLOCK",
    "terminatingRuleMatchDetails": [
        {
            "conditionType": "SQL_INJECTION",
            "sensitivityLevel": "LOW",
            "location": "UNKNOWN",
            "matchedData": [
                "10",
                "AND",
                "1"
            ]
        }
    ],
    "httpSourceName": "ALB",
```

```
    "httpSourceId": "alb",
    "ruleGroupList": [],
    "rateBasedRuleList": [],
    "nonTerminatingMatchingRules": [],
    "requestHeadersInserted":null,
    "responseCodeSent":null,
    "httpRequest": {
        "clientIp": "1.1.1.1",
        "country": "AU",
        "headers": [],
        "uri": "",
        "args": "",
        "httpVersion": "HTTP/1.1",
        "httpMethod": "POST",
        "requestId": "null"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example Keluaran log untuk aturan CAPTCHA terhadap permintaan web dengan token CAPTCHA yang valid dan belum kedaluwarsa

Daftar log berikut adalah untuk permintaan web yang cocok dengan aturan dengan CAPTCHA tindakan. Permintaan web memiliki token CAPTCHA yang valid dan belum kedaluwarsa, dan hanya dicatat sebagai kecocokan CAPTCHA oleh AWS WAF, mirip dengan perilaku untuk tindakan tersebut. Count Pertandingan CAPTCHA ini dicatat di bawah. `nonTerminatingMatchingRules`

```
{
  "timestamp": 1632420429309,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/captcha-web-
acl/585e38b5-afce-4d2a-b417-14fb08b66c67",
  "terminatingRuleId": "Default_Action",
  "terminatingRuleType": "REGULAR",
  "action": "ALLOW",
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "123456789012:b34myvfw0b:pen-test",
  "ruleGroupList": [],
```

```
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [
    {
      "ruleId": "captcha-rule",
      "action": "CAPTCHA",
      "ruleMatchDetails": [],
      "captchaResponse": {
        "responseCode": 0,
        "solveTimestamp": 1632420429
      }
    }
  ],
  "requestHeadersInserted": [
    {
      "name": "x-amzn-waf-test-header-name",
      "value": "test-header-value"
    }
  ],
  "responseCodeSent": null,
  "httpRequest": {
    "clientIp": "72.21.198.65",
    "country": "US",
    "headers": [
      {
        "name": "X-Forwarded-For",
        "value": "72.21.198.65"
      },
      {
        "name": "X-Forwarded-Proto",
        "value": "https"
      },
      {
        "name": "X-Forwarded-Port",
        "value": "443"
      },
      {
        "name": "Host",
        "value": "b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com"
      },
      {
        "name": "X-Amzn-Trace-Id",
        "value": "Root=1-614cc24d-5ad89a09181910c43917a888"
      },
      {
```

```
        "name": "cache-control",
        "value": "max-age=0"
      },
      {
        "name": "sec-ch-ua",
        "value": "\"Chromium\";v=\"94\", \"Google Chrome\";v=\"94\", \";Not A Brand
\";v=\"99\""
      },
      {
        "name": "sec-ch-ua-mobile",
        "value": "?0"
      },
      {
        "name": "sec-ch-ua-platform",
        "value": "\"Windows\""
      },
      {
        "name": "upgrade-insecure-requests",
        "value": "1"
      },
      {
        "name": "user-agent",
        "value": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/94.0.4606.54 Safari/537.36"
      },
      {
        "name": "accept",
        "value": "text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9"
      },
      {
        "name": "sec-fetch-site",
        "value": "same-origin"
      },
      {
        "name": "sec-fetch-mode",
        "value": "navigate"
      },
      {
        "name": "sec-fetch-user",
        "value": "?1"
      },
      {
        "name": "sec-fetch-dest",
```

```
        "value": "document"
      },
      {
        "name": "referer",
        "value": "https://b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com/pen-
test/pets"
      },
      {
        "name": "accept-encoding",
        "value": "gzip, deflate, br"
      },
      {
        "name": "accept-language",
        "value": "en-US,en;q=0.9"
      },
      {
        "name": "cookie",
        "value": "aws-waf-token=51c71352-41f5-4f6d-b676-c24907bdf819:EQoAZ/J
+AAQAAAAA:t9wvxbw042wva7E2Y6lgud/
bS6YG0CJKVAJqaRqDZ140ythKW0Zj9wKB2O8lSkYDRqf1yONcVBFo5u0eYi0tvT4rtQCXsu
+KanAardW8go4QSLw4yoED59lgV7oAhGyCalAzE7ra29j+RvvZPsQyoQuDCrtoY/TvQyMTXIXzGPDC/rKBbg=="
      }
    ],
    "uri": "/pen-test/pets",
    "args": "",
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
    "requestId": "GINMHHUgoAMFxug="
  }
}
```

Example Keluaran log untuk aturan CAPTCHA terhadap permintaan web yang tidak memiliki token CAPTCHA

Daftar log berikut adalah untuk permintaan web yang cocok dengan aturan dengan CAPTCHA tindakan. Permintaan web tidak memiliki token CAPTCHA, dan diblokir oleh. AWS WAF

```
{
  "timestamp": 1632420416512,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/captcha-web-
acl/585e38b5-afce-4d2a-b417-14fb08b66c67",
  "terminatingRuleId": "captcha-rule",
```

```
  "terminatingRuleType": "REGULAR",
  "action": "CAPTCHA",
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "123456789012:b34myvfw0b:pen-test",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [],
  "requestHeadersInserted": null,
  "responseCodeSent": 405,
  "httpRequest": {
    "clientIp": "72.21.198.65",
    "country": "US",
    "headers": [
      {
        "name": "X-Forwarded-For",
        "value": "72.21.198.65"
      },
      {
        "name": "X-Forwarded-Proto",
        "value": "https"
      },
      {
        "name": "X-Forwarded-Port",
        "value": "443"
      },
      {
        "name": "Host",
        "value": "b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com"
      },
      {
        "name": "X-Amzn-Trace-Id",
        "value": "Root=1-614cc240-18b57ff33c10e5c016b508c5"
      },
      {
        "name": "sec-ch-ua",
        "value": "\"Chromium\";v=\"94\", \"Google Chrome\";v=\"94\", \";Not A Brand
\";v=\"99\""
      },
      {
        "name": "sec-ch-ua-mobile",
        "value": "?0"
      },
      {
```

```
        "name": "sec-ch-ua-platform",
        "value": "\"Windows\""
      },
      {
        "name": "upgrade-insecure-requests",
        "value": "1"
      },
      {
        "name": "user-agent",
        "value": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/94.0.4606.54 Safari/537.36"
      },
      {
        "name": "accept",
        "value": "text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9"
      },
      {
        "name": "sec-fetch-site",
        "value": "cross-site"
      },
      {
        "name": "sec-fetch-mode",
        "value": "navigate"
      },
      {
        "name": "sec-fetch-user",
        "value": "?1"
      },
      {
        "name": "sec-fetch-dest",
        "value": "document"
      },
      {
        "name": "accept-encoding",
        "value": "gzip, deflate, br"
      },
      {
        "name": "accept-language",
        "value": "en-US,en;q=0.9"
      }
    ],
    "uri": "/pen-test/pets",
    "args": "",
```

```
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
    "requestId": "GINKHEssoAMFsrg="
  },
  "captchaResponse": {
    "responseCode": 405,
    "solveTimestamp": 0,
    "failureReason": "TOKEN_MISSING"
  }
}
```

Menguji dan menyetel perlindungan Anda AWS WAF

Kami menyarankan Anda menguji dan menyetel perubahan apa pun pada ACL AWS WAF web Anda sebelum menerapkannya ke lalu lintas situs web atau aplikasi web Anda.

> ⚠ Risiko lalu lintas produksi
>
> Sebelum Anda menerapkan implementasi ACL web Anda untuk lalu lintas produksi, uji dan sesuaikan di lingkungan pementasan atau pengujian sampai Anda merasa nyaman dengan potensi dampak terhadap lalu lintas Anda. Kemudian uji dan atur aturan dalam mode hitungan dengan lalu lintas produksi Anda sebelum mengaktifkannya.

Bagian ini memberikan panduan untuk menguji dan menyetel ACL AWS WAF web Anda, aturan, grup aturan, set IP, dan set pola regex.

Bagian ini juga memberikan panduan umum untuk menguji penggunaan grup aturan yang dikelola oleh orang lain. Ini termasuk grup aturan Aturan AWS AWS Marketplace Terkelola, grup aturan terkelola, dan grup aturan yang dibagikan dengan Anda oleh akun lain. Untuk grup aturan ini, ikuti juga panduan apa pun yang Anda dapatkan dari penyedia grup aturan.

- Untuk grup aturan Aturan AWS Terkelola Kontrol Bot, lihat jugaMenguji dan menerapkan Kontrol AWS WAF Bot.
- Untuk grup aturan pencegahan pengambilalihan akun Aturan AWS Terkelola, lihat Menguji dan menerapkan ATP juga.
- Untuk grup aturan Aturan AWS Terkelola pencegahan penipuan pembuatan akun, lihat jugaMenguji dan menerapkan ACFP.

Ketidakkonsistenan sementara selama pembaruan

Saat Anda membuat atau mengubah ACL web atau AWS WAF sumber daya lainnya, perubahan membutuhkan sedikit waktu untuk menyebar ke semua area tempat sumber daya disimpan. Waktu propagasi bisa dari beberapa detik hingga beberapa menit.

Berikut ini adalah contoh inkonsistensi sementara yang mungkin Anda perhatikan selama propagasi perubahan:

- Setelah Anda membuat ACL web, jika Anda mencoba mengaitkannya dengan sumber daya, Anda mungkin mendapatkan pengecualian yang menunjukkan bahwa ACL web tidak tersedia.
- Setelah Anda menambahkan grup aturan ke ACL web, aturan grup aturan baru mungkin berlaku di satu area di mana ACL web digunakan dan tidak di area lain.
- Setelah mengubah setelan tindakan aturan, Anda mungkin melihat tindakan lama di beberapa tempat dan tindakan baru di tempat lain.
- Setelah Anda menambahkan alamat IP ke set IP yang digunakan dalam aturan pemblokiran, alamat baru mungkin diblokir di satu area sementara masih diizinkan di area lain.

Menguji dan menyetel langkah-langkah tingkat tinggi

Bagian ini menyediakan daftar periksa langkah-langkah untuk menguji perubahan pada ACL web Anda, termasuk aturan atau grup aturan apa pun yang digunakannya.

> **Note**
>
> Untuk mengikuti panduan di bagian ini, Anda perlu memahami cara membuat dan mengelola AWS WAF perlindungan seperti ACL web, aturan, dan grup aturan. Informasi itu tercakup dalam bagian sebelumnya dari panduan ini.

Untuk menguji dan menyetel ACL web Anda

Lakukan langkah-langkah ini terlebih dahulu di lingkungan pengujian, kemudian dalam produksi.

1. Bersiaplah untuk pengujian

   Persiapkan lingkungan pemantauan Anda, alihkan AWS WAF perlindungan baru Anda ke mode hitungan untuk pengujian, dan buat asosiasi sumber daya apa pun yang Anda butuhkan.

Lihat Mempersiapkan pengujian.

2. Pantau dan dengarkan lingkungan pengujian dan produksi

   Pantau dan sesuaikan AWS WAF perlindungan Anda terlebih dahulu di lingkungan pengujian atau pementasan, kemudian dalam produksi, hingga Anda puas bahwa mereka dapat menangani lalu lintas sesuai kebutuhan Anda.

   Lihat Pemantauan dan penyetelan.

3. Aktifkan perlindungan Anda dalam produksi

   Saat Anda puas dengan perlindungan pengujian Anda, alihkan ke mode produksi, bersihkan artefak pengujian yang tidak perlu, dan lanjutkan pemantauan.

   Lihat Mengaktifkan perlindungan Anda dalam produksi.

Setelah Anda selesai menerapkan perubahan Anda, lanjutkan memantau lalu lintas web Anda dan perlindungan dalam produksi untuk memastikan bahwa mereka bekerja seperti yang Anda inginkan. Pola lalu lintas web dapat berubah seiring waktu, jadi Anda mungkin perlu menyesuaikan perlindungan sesekali.

Mempersiapkan pengujian

Bagian ini menjelaskan cara mengatur untuk menguji dan menyetel AWS WAF perlindungan Anda.

> **Note**
>
> Untuk mengikuti panduan di bagian ini, Anda perlu memahami secara umum cara membuat dan mengelola AWS WAF perlindungan seperti ACL web, aturan, dan grup aturan. Informasi itu tercakup dalam bagian sebelumnya dari panduan ini.

Untuk mempersiapkan pengujian

1. Aktifkan pencatatan ACL web, CloudWatch metrik Amazon, dan pengambilan sampel permintaan web untuk ACL web

   Gunakan logging, metrik, dan sampling untuk memantau interaksi aturan ACL web dengan lalu lintas web Anda.

- Logging — Anda dapat mengonfigurasi AWS WAF untuk mencatat permintaan web yang dievaluasi oleh ACL web. Anda dapat mengirim log ke CloudWatch log, bucket Amazon S3, atau aliran pengiriman Amazon Data Firehose. Anda dapat menyunting bidang dan menerapkan pemfilteran. Untuk informasi selengkapnya, lihat Pencatatan AWS WAF lalu lintas ACL web.
- Amazon Security Lake - Anda dapat mengonfigurasi Security Lake untuk mengumpulkan data ACL web. Security Lake mengumpulkan data log dan peristiwa dari berbagai sumber untuk normalisasi, analisis, dan manajemen. Untuk informasi tentang opsi ini, lihat Apa itu Amazon Security Lake? dan Mengumpulkan data dari AWS layanan di panduan pengguna Amazon Security Lake.
- CloudWatch Metrik Amazon — Dalam konfigurasi ACL web Anda, berikan spesifikasi metrik untuk semua yang ingin Anda pantau. Anda dapat melihat metrik melalui AWS WAF dan CloudWatch konsol. Untuk informasi selengkapnya, lihat Pemantauan CloudWatch dengan Amazon.
- Pengambilan sampel permintaan web — Anda dapat melihat sampel semua permintaan web yang dievaluasi oleh ACL web Anda. Untuk informasi tentang pengambilan sampel permintaan web, lihatMelihat contoh permintaan web.

2. Atur perlindungan Anda ke mode Count

   Dalam konfigurasi ACL web Anda, alihkan apa pun yang ingin Anda uji ke mode hitung. Hal ini menyebabkan perlindungan pengujian merekam kecocokan terhadap permintaan web tanpa mengubah cara permintaan ditangani. Anda akan dapat melihat kecocokan dalam metrik, log, dan permintaan sampel Anda, untuk memverifikasi kriteria kecocokan dan untuk memahami apa efeknya pada lalu lintas web Anda. Aturan yang menambahkan label ke permintaan yang cocok akan menambahkan label terlepas dari tindakan aturan.

   - Aturan yang didefinisikan dalam ACL web — Edit aturan di ACL web dan atur tindakannya. Count
   - Grup aturan - Dalam konfigurasi ACL web Anda, edit pernyataan aturan untuk grup aturan dan, di panel Aturan, buka tarik-turun Ganti semua tindakan aturan dan pilih. Count Jika Anda mengelola ACL web di JSON, tambahkan aturan ke `RuleActionOverrides` pengaturan dalam pernyataan referensi grup aturan, dengan `ActionToUse` disetel ke. Count Contoh daftar berikut menunjukkan penggantian untuk dua aturan dalam grup aturan Aturan `AWSManagedRulesAnonymousIpList` AWS Terkelola.

     ```
     "ManagedRuleGroupStatement": {
     ```

```
    "VendorName": "AWS",
    "Name": "AWSManagedRulesAnonymousIpList",
      "RuleActionOverrides": [
        {
          "ActionToUse": {
            "Count": {}
          },
          "Name": "AnonymousIPList"
        },
        {
          "ActionToUse": {
            "Count": {}
          },
          "Name": "HostingProviderIPList"
        }
      ],
      "ExcludedRules": []
    }
  },
```

Untuk informasi selengkapnya tentang penggantian tindakan aturan, lihat. Mengesampingkan tindakan aturan dalam grup aturan

Untuk grup aturan Anda sendiri, jangan mengubah tindakan aturan di grup aturan itu sendiri. Aturan grup aturan dengan Count tindakan tidak menghasilkan metrik atau artefak lain yang Anda perlukan untuk pengujian Anda. Selain itu, mengubah grup aturan memengaruhi semua ACL web yang menggunakannya, sedangkan perubahan di dalam konfigurasi ACL web hanya memengaruhi ACL web tunggal.

- Web ACL — Jika Anda menguji ACL web baru, atur tindakan default untuk ACL web untuk mengizinkan permintaan. Ini memungkinkan Anda mencoba ACL web tanpa mempengaruhi lalu lintas dengan cara apa pun.

Secara umum, mode hitung menghasilkan lebih banyak kecocokan daripada produksi. Ini karena aturan yang menghitung permintaan tidak menghentikan evaluasi permintaan oleh ACL web, jadi aturan yang berjalan nanti di ACL web mungkin juga cocok dengan permintaan. Saat Anda mengubah tindakan aturan ke setelan produksinya, aturan yang mengizinkan atau memblokir permintaan akan menghentikan evaluasi permintaan yang cocok. Akibatnya, permintaan yang cocok umumnya akan diperiksa oleh aturan yang lebih sedikit di ACL web. Untuk informasi

selengkapnya tentang efek tindakan aturan pada evaluasi keseluruhan permintaan web, lihatTindakan aturan.

Dengan pengaturan ini, perlindungan baru Anda tidak akan mengubah lalu lintas web, tetapi akan menghasilkan informasi kecocokan dalam metrik, log ACL web, dan sampel permintaan.

3. Kaitkan ACL web dengan sumber daya

   Jika ACL web belum dikaitkan dengan sumber daya, kaitkan.

   Lihat Mengaitkan atau memisahkan ACL web dengan sumber daya AWS.

Anda sekarang siap untuk memantau dan menyetel ACL web Anda.

Pemantauan dan penyetelan

Bagian ini menjelaskan cara memantau dan menyetel AWS WAF perlindungan Anda.

> **Note**
>
> Untuk mengikuti panduan di bagian ini, Anda perlu memahami secara umum cara membuat dan mengelola AWS WAF perlindungan seperti ACL web, aturan, dan grup aturan. Informasi itu tercakup dalam bagian sebelumnya dari panduan ini.

Pantau lalu lintas web dan kecocokan aturan untuk memverifikasi perilaku ACL web. Jika Anda menemukan masalah, sesuaikan aturan Anda untuk memperbaiki dan kemudian memantau untuk memverifikasi penyesuaian.

Ulangi prosedur berikut sampai ACL web mengelola lalu lintas web Anda sesuai kebutuhan.

Untuk memantau dan menyetel

1. Pantau lalu lintas dan kecocokan aturan

   Pastikan lalu lintas mengalir dan aturan pengujian Anda menemukan permintaan yang cocok.

   Cari informasi berikut untuk perlindungan yang Anda uji:

   - Log — Mengakses informasi tentang aturan yang cocok dengan permintaan web:

  - Aturan Anda - Aturan di ACL web yang memiliki Count tindakan tercantum di bawah`nonTerminatingMatchingRules`. Aturan dengan Allow atau Block terdaftar sebagai`terminatingRule`. Aturan dengan CAPTCHA atau Challenge dapat berupa penghentian atau non-penghentian, dan terdaftar di bawah salah satu dari dua kategori, sesuai dengan hasil pencocokan aturan.
  - Grup aturan - Grup aturan diidentifikasi di `ruleGroupId` lapangan, dengan kecocokan aturan mereka dikategorikan sama dengan aturan mandiri.
  - Label - Label yang aturan telah diterapkan pada permintaan tercantum di `Labels` bidang.

  Untuk informasi selengkapnya, lihat Bidang log.

- CloudWatch Metrik Amazon — Anda dapat mengakses metrik berikut untuk evaluasi permintaan ACL web Anda.
  - Aturan Anda — Metrik dikelompokkan berdasarkan tindakan aturan. Misalnya, saat Anda menguji aturan dalam Count mode, kecocokannya terdaftar sebagai `Count` metrik untuk ACL web.
  - Grup aturan Anda — Metrik untuk grup aturan Anda tercantum di bawah metrik grup aturan.
  - Grup aturan yang dimiliki oleh akun lain — Metrik grup aturan umumnya hanya dapat dilihat oleh pemilik grup aturan. Namun, jika Anda mengganti tindakan aturan untuk aturan, metrik untuk aturan tersebut akan dicantumkan di bawah metrik ACL web Anda. Selain itu, label yang ditambahkan oleh grup aturan apa pun tercantum dalam metrik ACL web Anda

    Grup aturan dalam kategori ini adalahAWS Aturan Terkelola untuk AWS WAF,AWS Marketplace kelompok aturan terkelola,Grup aturan yang disediakan oleh layanan lain, dan grup aturan yang dibagikan dengan Anda oleh akun lain.
  - Label - Label yang ditambahkan ke permintaan web selama evaluasi tercantum dalam metrik label ACL web. Anda dapat mengakses metrik untuk semua label, terlepas dari apakah itu ditambahkan oleh aturan dan grup aturan Anda atau oleh aturan dalam grup aturan yang dimiliki akun lain.

  Untuk informasi selengkapnya, lihat Melihat metrik untuk ACL web Anda.

- Dasbor ikhtisar lalu lintas ACL Web — Akses ringkasan lalu lintas web yang telah dievaluasi oleh ACL web dengan membuka halaman ACL web di AWS WAF konsol dan membuka tab ikhtisar Lalu lintas.

  Dasbor ikhtisar lalu lintas menyediakan ringkasan hampir real-time dari CloudWatch metrik Amazon yang AWS WAF dikumpulkan saat mengevaluasi lalu lintas web aplikasi Anda.

Untuk informasi selengkapnya, lihat Dasbor ikhtisar lalu lintas ACL web.

- Permintaan web sampel — Akses informasi untuk aturan yang cocok dengan pengambilan sampel permintaan web. Informasi sampel mengidentifikasi aturan yang cocok dengan nama metrik untuk aturan di ACL web. Untuk grup aturan, metrik mengidentifikasi pernyataan referensi grup aturan. Untuk aturan di dalam grup aturan, sampel mencantumkan nama aturan yang cocok di`RuleWithinRuleGroup`.

  Untuk informasi selengkapnya, lihat Melihat contoh permintaan web.

2. Konfigurasikan mitigasi untuk mengatasi positif palsu

   Jika Anda menentukan bahwa aturan menghasilkan positif palsu, dengan mencocokkan permintaan web ketika seharusnya tidak, opsi berikut dapat membantu Anda menyetel perlindungan ACL web Anda untuk mengurangi.

   Mengoreksi kriteria inspeksi aturan

   Untuk aturan Anda sendiri, Anda sering hanya perlu menyesuaikan pengaturan yang Anda gunakan untuk memeriksa permintaan web. Contohnya termasuk mengubah spesifikasi dalam kumpulan pola regex, menyesuaikan transformasi teks yang Anda terapkan ke komponen permintaan sebelum pemeriksaan, atau beralih menggunakan alamat IP yang diteruskan. Lihat panduan untuk jenis aturan yang menyebabkan masalah, di bawahDasar-dasar pernyataan aturan.

   Memperbaiki masalah yang lebih kompleks

   Untuk kriteria inspeksi yang tidak Anda kendalikan dan untuk beberapa aturan kompleks, Anda mungkin perlu membuat perubahan lain, seperti menambahkan aturan yang secara eksplisit mengizinkan atau memblokir permintaan atau yang menghilangkan permintaan dari evaluasi oleh aturan bermasalah. Kelompok aturan terkelola paling sering membutuhkan jenis mitigasi ini, tetapi aturan lain juga bisa. Contohnya termasuk pernyataan aturan berbasis laju dan pernyataan aturan serangan injeksi SQL.

   Apa yang Anda lakukan untuk mengurangi positif palsu tergantung pada kasus penggunaan Anda. Berikut ini adalah pendekatan umum:

   - Tambahkan aturan mitigasi — Tambahkan aturan yang berjalan sebelum aturan baru dan yang secara eksplisit mengizinkan permintaan yang menyebabkan kesalahan positif. Untuk

informasi tentang urutan evaluasi aturan di ACL web, lihatMemproses urutan aturan dan kelompok aturan dalam ACL web.

Dengan pendekatan ini, permintaan yang diizinkan dikirim ke sumber daya yang dilindungi, sehingga mereka tidak pernah mencapai aturan baru untuk evaluasi. Jika aturan baru adalah grup aturan terkelola berbayar, pendekatan ini juga dapat membantu menahan biaya penggunaan grup aturan.

- Tambahkan aturan logis dengan aturan mitigasi — Gunakan pernyataan aturan logis untuk menggabungkan aturan baru dengan aturan yang mengecualikan positif palsu. Untuk informasi, lihat Pernyataan aturan logis.

  Misalnya, Anda menambahkan pernyataan kecocokan serangan injeksi SQL yang menghasilkan positif palsu untuk kategori permintaan. Buat aturan yang cocok dengan permintaan tersebut, lalu gabungkan aturan menggunakan pernyataan aturan logis sehingga Anda hanya cocok pada permintaan yang keduanya tidak cocok dengan kriteria positif palsu dan cocok dengan kriteria serangan injeksi SQL.

- Tambahkan pernyataan cakupan ke bawah — Untuk pernyataan berbasis tingkat dan pernyataan referensi grup aturan terkelola, kecualikan permintaan yang menghasilkan positif palsu dari evaluasi dengan menambahkan pernyataan cakupan ke bawah di dalam pernyataan utama.

  Permintaan yang tidak cocok dengan pernyataan scope-down tidak pernah mencapai kelompok aturan atau evaluasi berbasis tarif. Untuk informasi tentang pernyataan cakupan bawah, lihat. Pernyataan cakupan ke bawah Sebagai contoh, lihat Kecualikan rentang IP dari manajemen bot.

- Tambahkan aturan pencocokan label — Untuk grup aturan yang menggunakan pelabelan, identifikasi label yang diterapkan aturan bermasalah pada permintaan. Anda mungkin perlu mengatur aturan grup aturan dalam mode hitung terlebih dahulu, jika Anda belum melakukannya. Tambahkan aturan pencocokan label, diposisikan untuk dijalankan setelah grup aturan, yang cocok dengan label yang ditambahkan oleh aturan bermasalah. Dalam aturan pencocokan label, Anda dapat memfilter permintaan yang ingin Anda izinkan dari permintaan yang ingin Anda blokir.

  Jika Anda menggunakan pendekatan ini, saat Anda selesai menguji, pertahankan aturan bermasalah dalam mode hitungan di grup aturan, dan pertahankan aturan pencocokan label kustom Anda. Untuk informasi tentang pernyataan pencocokan label, lihatPernyataan aturan

pencocokan label. Sebagai contoh, lihat Izinkan bot tertentu yang diblokir dan Contoh ATP: Penanganan khusus untuk kredensi yang hilang dan dikompromikan.

- Mengubah versi grup aturan terkelola — Untuk grup aturan terkelola berversi, ubah versi yang Anda gunakan. Misalnya, Anda dapat beralih kembali ke versi statis terakhir yang berhasil Anda gunakan.

  Ini biasanya perbaikan sementara. Anda dapat mengubah versi untuk lalu lintas produksi saat melanjutkan pengujian versi terbaru di lingkungan pengujian atau pementasan, atau saat Anda menunggu versi yang lebih kompatibel dari penyedia. Untuk informasi tentang versi grup aturan terkelola, lihatGrup aturan terkelola.

Ketika Anda puas bahwa aturan baru cocok dengan permintaan yang Anda butuhkan, lanjutkan ke tahap pengujian berikutnya dan ulangi prosedur ini. Lakukan tahap akhir pengujian dan penyetelan di lingkungan produksi Anda.

Melihat metrik untuk ACL web Anda

Setelah mengaitkan ACL web dengan satu atau beberapa AWS sumber daya, Anda dapat melihat metrik yang dihasilkan untuk asosiasi tersebut dalam grafik Amazon CloudWatch .

Untuk informasi tentang AWS WAF metrik, lihatAWS WAF metrik dan dimensi. Untuk informasi tentang CloudWatch metrik, lihat Panduan CloudWatch Pengguna Amazon.

Untuk setiap aturan Anda di ACL web dan untuk semua permintaan yang diteruskan sumber daya terkait AWS WAF untuk ACL web, CloudWatch memungkinkan Anda melakukan hal berikut:

- Lihat data untuk jam sebelumnya atau tiga jam sebelumnya.
- Ubah interval antara titik data.
- Ubah perhitungan yang CloudWatch dilakukan pada data, seperti maksimum, minimum, rata-rata, atau jumlah.

> **Note**
>
> AWS WAF with CloudFront adalah layanan global dan metrik hanya tersedia ketika Anda memilih Wilayah AS Timur (Virginia N.) di. AWS Management Console Jika Anda memilih Wilayah lain, tidak ada AWS WAF metrik yang akan muncul di CloudWatch konsol.

Untuk melihat data untuk aturan di ACL web

1. Masuk ke AWS Management Console dan buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Jika perlu, ubah Wilayah ke wilayah tempat AWS sumber daya Anda berada. Untuk CloudFront, pilih Wilayah AS Timur (Virginia N.).
3. Di panel navigasi, di bawah Metrik, pilih Semua metrik dan kemudian cari di bawah tab Jelajahi. `AWS::WAFV2`
4. Pilih kotak centang untuk ACL web yang ingin Anda lihat datanya.
5. Ubah pengaturan yang berlaku:

   Statistik

   Pilih perhitungan yang CloudWatch dilakukan pada data.

   Rentang waktu

   Pilih apakah Anda ingin melihat data untuk jam sebelumnya atau tiga jam sebelumnya.

   Periode

   Pilih interval antara titik data dalam grafik.

   Aturan

   Pilih aturan yang ingin Anda lihat datanya.

   > **Note**
   >
   > Jika Anda mengubah nama aturan dan Anda ingin nama metrik aturan mencerminkan perubahan, Anda harus memperbarui nama metrik juga. AWS WAF tidak secara otomatis memperbarui nama metrik untuk aturan saat Anda mengubah nama aturan. Anda dapat mengubah nama metrik saat mengedit aturan di konsol, dengan menggunakan editor JSON aturan. Anda juga dapat mengubah kedua nama melalui API dan dalam daftar JSON apa pun yang Anda gunakan untuk menentukan ACL web atau grup aturan.

   Perhatikan hal berikut:

- Jika Anda baru-baru ini mengaitkan ACL web dengan AWS sumber daya, Anda mungkin perlu menunggu beberapa menit agar data muncul dalam grafik dan metrik agar ACL web muncul dalam daftar metrik yang tersedia.
- Jika Anda mengaitkan lebih dari satu sumber daya dengan ACL web, CloudWatch data akan mencakup permintaan untuk semuanya.
- Anda dapat mengarahkan kursor ke titik data untuk mendapatkan informasi lebih lanjut.
- Grafik tidak menyegarkan diri secara otomatis. Untuk memperbarui tampilan, pilih ikon segarkan
  ().

Untuk informasi selengkapnya tentang CloudWatch metrik, lihatPemantauan CloudWatch dengan Amazon.

Dasbor ikhtisar lalu lintas ACL web

Bagian ini menjelaskan dasbor ikhtisar lalu lintas ACL web di konsol. AWS WAF Setelah Anda mengaitkan ACL web dengan satu atau beberapa AWS sumber daya dan mengaktifkan metrik untuk ACL web, Anda dapat mengakses ringkasan lalu lintas web yang dievaluasi oleh ACL web dengan membuka tab ikhtisar Lalu lintas ACL web di konsol. AWS WAF Dasbor menyertakan ringkasan hampir real-time dari CloudWatch metrik Amazon yang AWS WAF dikumpulkan saat mengevaluasi lalu lintas web aplikasi Anda.

> **Note**
>
> Jika Anda tidak melihat apa pun di dasbor, pastikan metrik Anda diaktifkan untuk ACL web.

Tab ikhtisar lalu lintas ACL web berisi dasbor tab dengan kategori informasi berikut:

- Semua lalu lintas — Semua permintaan web yang dievaluasi oleh ACL web.

  Fokus dasbor adalah pada penghentian tindakan, tetapi Anda dapat melihat aturan kecocokan untuk hitungan di lokasi berikut:

  - 10 panel aturan teratas dari dasbor ini. Alihkan Beralih untuk menghitung tindakan untuk menampilkan kecocokan aturan hitungan.

  - Tab permintaan sampel dari halaman ACL web. Tab baru ini menyertakan grafik semua kecocokan aturan. Untuk informasi, lihat Melihat contoh permintaan web.
- Kontrol Bot — Permintaan web yang dievaluasi oleh ACL web menggunakan grup aturan terkelola Bot Control.

  Jika Anda tidak menggunakan grup aturan ini di ACL web Anda, tab ini menunjukkan hasil evaluasi pengambilan sampel lalu lintas web Anda terhadap aturan Kontrol Bot. Ini memberi Anda gambaran tentang lalu lintas bot yang diterima aplikasi Anda dan gratis.

  Kelompok aturan ini adalah bagian dari opsi mitigasi ancaman cerdas yang AWS WAF ditawarkan. Lihat informasi yang lebih lengkap di AWS WAF Kontrol Bot dan AWS WAF Grup aturan Bot Control.
- Pencegahan pengambilalihan akun — Web meminta agar ACL web mengevaluasi menggunakan grup aturan terkelola pencegahan pengambilalihan akun Kontrol AWS WAF Penipuan (ATP). Tab ini hanya tersedia jika Anda menggunakan grup aturan ini di ACL web Anda.

  Kelompok aturan ATP adalah bagian dari penawaran mitigasi ancaman AWS WAF cerdas. Lihat informasi yang lebih lengkap di AWS WAF Pencegahan pengambilalihan akun Kontrol Penipuan (ATP) dan AWS WAF Kelompok aturan pencegahan pengambilalihan akun Kontrol Penipuan (ATP).
- Pencegahan penipuan pembuatan akun — Web meminta agar ACL web mengevaluasi menggunakan grup aturan pencegahan AWS WAF penipuan pembuatan akun Kontrol Penipuan (ACFP) yang dikelola. Tab ini hanya tersedia jika Anda menggunakan grup aturan ini di ACL web Anda.

  Kelompok aturan ACFP adalah bagian dari penawaran mitigasi ancaman AWS WAF cerdas. Lihat informasi yang lebih lengkap di AWS WAF Pencegahan penipuan pembuatan akun Kontrol Penipuan (ACFP) dan AWS WAF Grup aturan pencegahan penipuan (ACFP) pembuatan akun Kontrol Penipuan.

Dasbor didasarkan pada metrik ACL web, dan grafik menyediakan akses ke CloudWatch metrik yang sesuai di. CloudWatch Untuk dasbor mitigasi ancaman cerdas, seperti Bot Control, metrik yang digunakan terutama adalah metrik label.

- Untuk daftar metrik yang AWS WAF menyediakan, lihatAWS WAF metrik dan dimensi.
- Untuk informasi tentang CloudWatch metrik, lihat Panduan CloudWatch Pengguna Amazon.

Dasbor memberikan ringkasan pola lalu lintas Anda untuk tindakan penghentian dan rentang tanggal yang Anda pilih. Dasbor mitigasi ancaman cerdas mencakup permintaan yang dievaluasi oleh grup aturan terkelola terkait, terlepas dari apakah grup aturan terkelola itu sendiri menerapkan tindakan penghentian. Misalnya, jika Block dipilih, dasbor pencegahan pengambilalihan Akun mencakup informasi untuk semua permintaan web yang dievaluasi oleh grup aturan terkelola ATP dan diblokir di beberapa titik selama evaluasi ACL web. Permintaan dapat diblokir oleh grup aturan terkelola ATP, dengan aturan yang dijalankan setelah grup aturan di ACL web, atau oleh tindakan default ACL web.

Melihat dasbor untuk ACL web

Ikuti prosedur di bagian ini untuk mengakses dasbor ACL web dan mengatur kriteria pemfilteran data. Jika Anda baru-baru ini mengaitkan ACL web dengan AWS sumber daya, Anda mungkin perlu menunggu beberapa menit agar data tersedia di dasbor.

Dasbor menyertakan permintaan untuk semua sumber daya yang Anda kaitkan dengan ACL web.

Untuk melihat dasbor ikhtisar lalu lintas untuk ACL web

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.
2. Di panel navigasi, pilih Web ACL dan kemudian cari ACL web yang Anda minati.
3. Pilih ACL web. Konsol membawa Anda ke halaman ACL web. Tab Ikhtisar lalu lintas dipilih secara default.
4. Ubah pengaturan Filter data sesuai kebutuhan.

    - Mengakhiri tindakan aturan — Pilih tindakan penghentian untuk disertakan di dasbor. Dasbor merangkum metrik untuk permintaan web yang memiliki salah satu tindakan yang dipilih yang diterapkan oleh evaluasi ACL web. Jika Anda memilih semua tindakan yang tersedia, dasbor menyertakan semua permintaan web yang dievaluasi. Untuk informasi tentang tindakan, lihatCara AWS WAF menangani tindakan kelompok aturan dan aturan di ACL web.
    - Rentang waktu - Pilih interval waktu untuk dilihat di dasbor. Anda dapat memilih untuk melihat kerangka waktu relatif terhadap sekarang, misalnya 3 jam terakhir atau minggu terakhir, dan Anda dapat memilih rentang waktu absolut dari kalender.
    - Zona waktu - Pengaturan ini berlaku saat Anda menentukan rentang waktu absolut. Anda dapat menggunakan zona waktu lokal browser Anda atau UTC (Coordinated Universal Time).

Tinjau informasi di tab yang Anda minati. Pilihan filter data berlaku untuk semua dasbor. Di panel grafik, Anda dapat mengarahkan kursor ke titik data atau area untuk melihat detail tambahan.

Countaturan tindakan

Anda dapat melihat informasi untuk menghitung kecocokan aksi di salah satu dari dua tempat.

- Di tab Ikhtisar lalu lintas ini, di dasbor Semua lalu lintas, temukan panel 10 aturan teratas dan alihkan tindakan Beralih untuk menghitung. Dengan sakelar ini aktif, panel menampilkan kecocokan aturan hitungan alih-alih mengakhiri kecocokan aturan.
- Di tab Permintaan sampel ACL web, lihat grafik semua kecocokan aturan dan tindakan untuk rentang waktu yang telah Anda tetapkan pada tab Ikhtisar lalu lintas. Untuk informasi tentang tab Permintaan sampel, lihatMelihat contoh permintaan web.

CloudWatch Metrik Amazon

Di panel grafik dasbor, Anda dapat mengakses CloudWatch metrik untuk data grafik. Pilih opsi di bagian atas panel grafik atau dari menu tarik-turun (elipsis vertikal) di dalam panel.

Menyegarkan dasbor

Dasbor tidak disegarkan secara otomatis. Untuk memperbarui tampilan, pilih

ikon penyegaran.

Contoh dasbor ikhtisar lalu lintas untuk ACL web

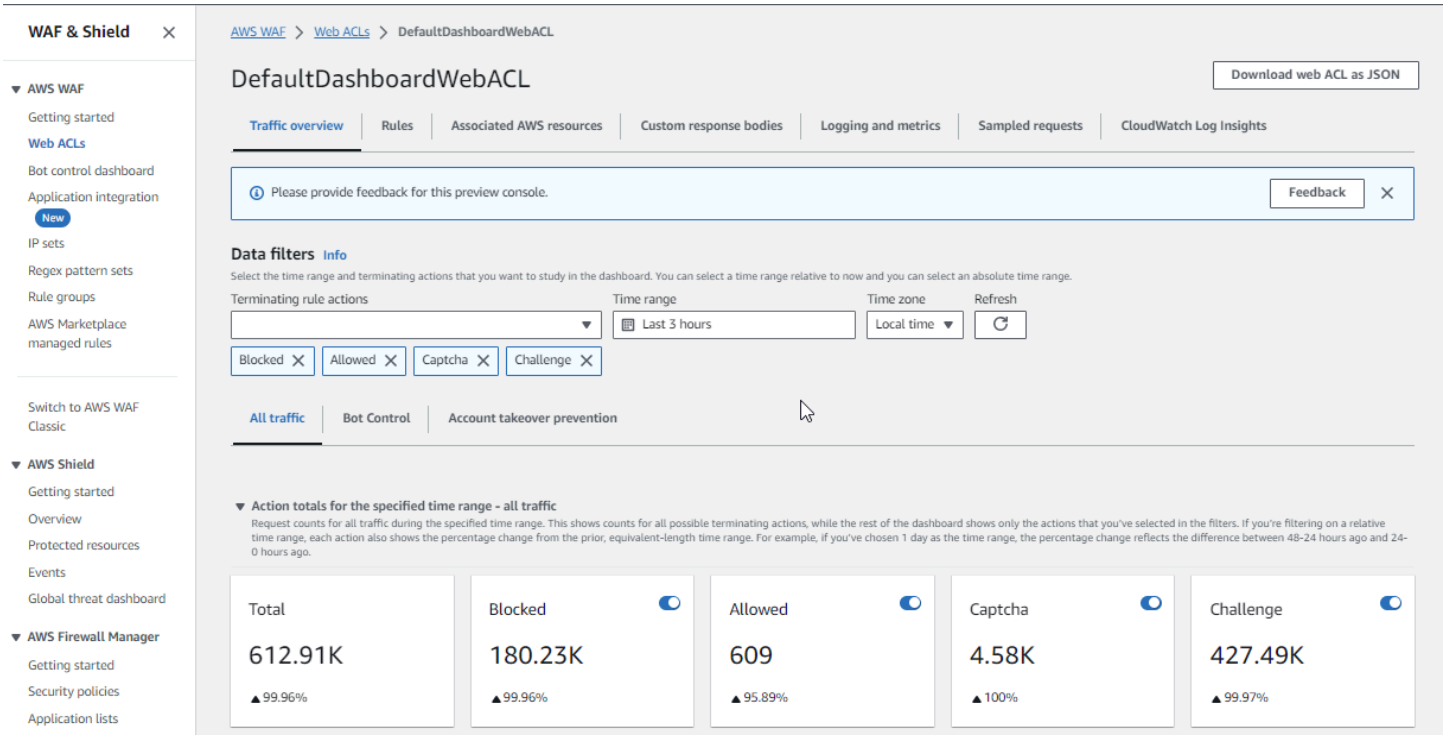
Bagian ini menunjukkan contoh layar dasbor ikhtisar lalu lintas untuk ACL web.

> **Note**
>
> Jika Anda sudah menggunakan AWS WAF untuk melindungi sumber daya aplikasi, Anda dapat melihat dasbor untuk ACL web apa pun di halamannya di AWS WAF konsol. Untuk informasi, lihat Melihat dasbor untuk ACL web.

Contoh layar: Filter data dan Semua tindakan dasbor lalu lintas dihitung

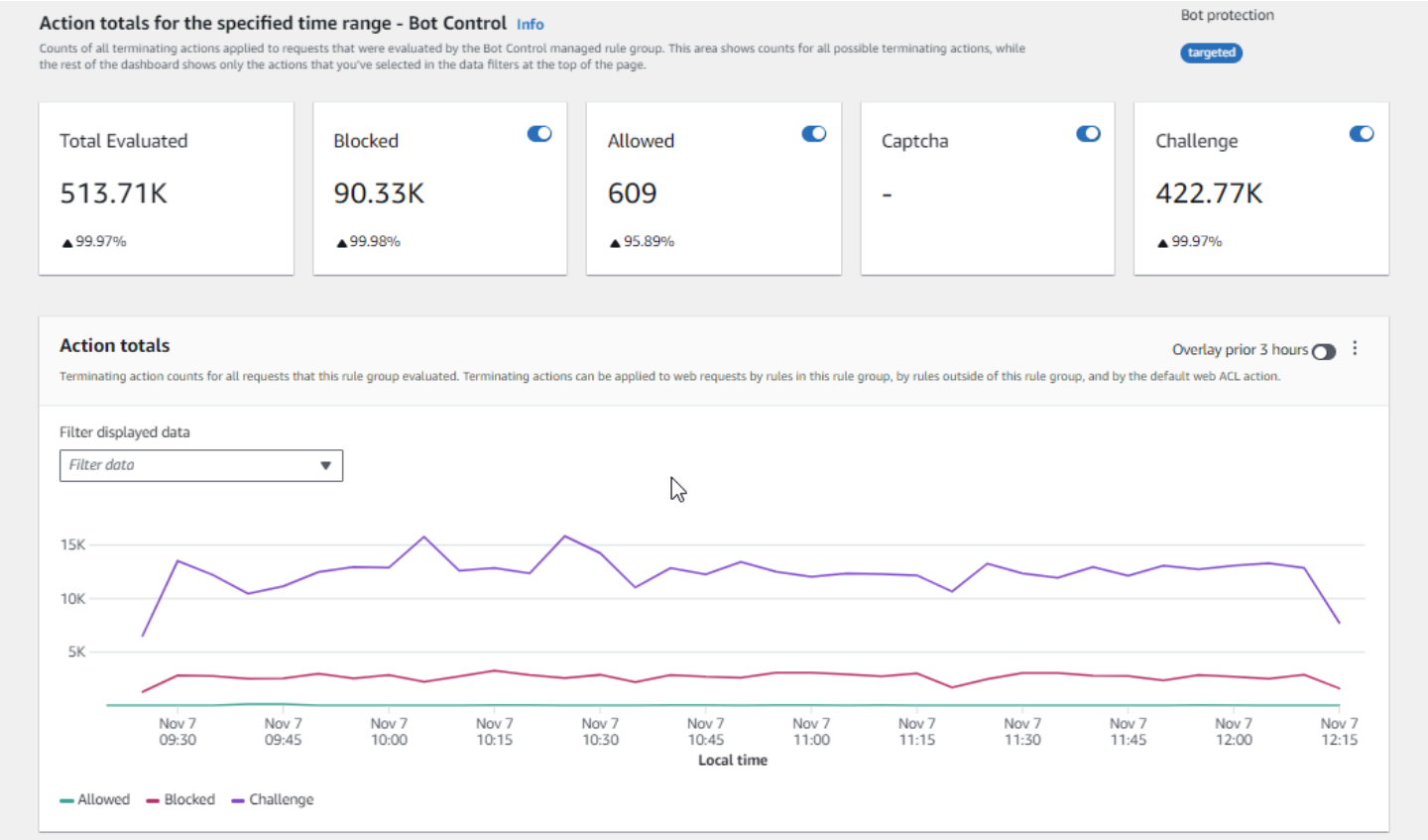
Tangkapan layar berikut menggambarkan ikhtisar lalu lintas untuk ACL web dengan tab Semua lalu lintas yang dipilih. Filter data diatur ke default: semua tindakan penghentian selama tiga jam terakhir.

Di dalam dasbor semua lalu lintas adalah total tindakan untuk berbagai tindakan penghentian. Setiap panel mencantumkan jumlah permintaan dan menampilkan panah atas/bawah yang menunjukkan perubahan sejak rentang waktu tiga jam sebelumnya.



Contoh layar: Jumlah tindakan dasbor Kontrol Bot

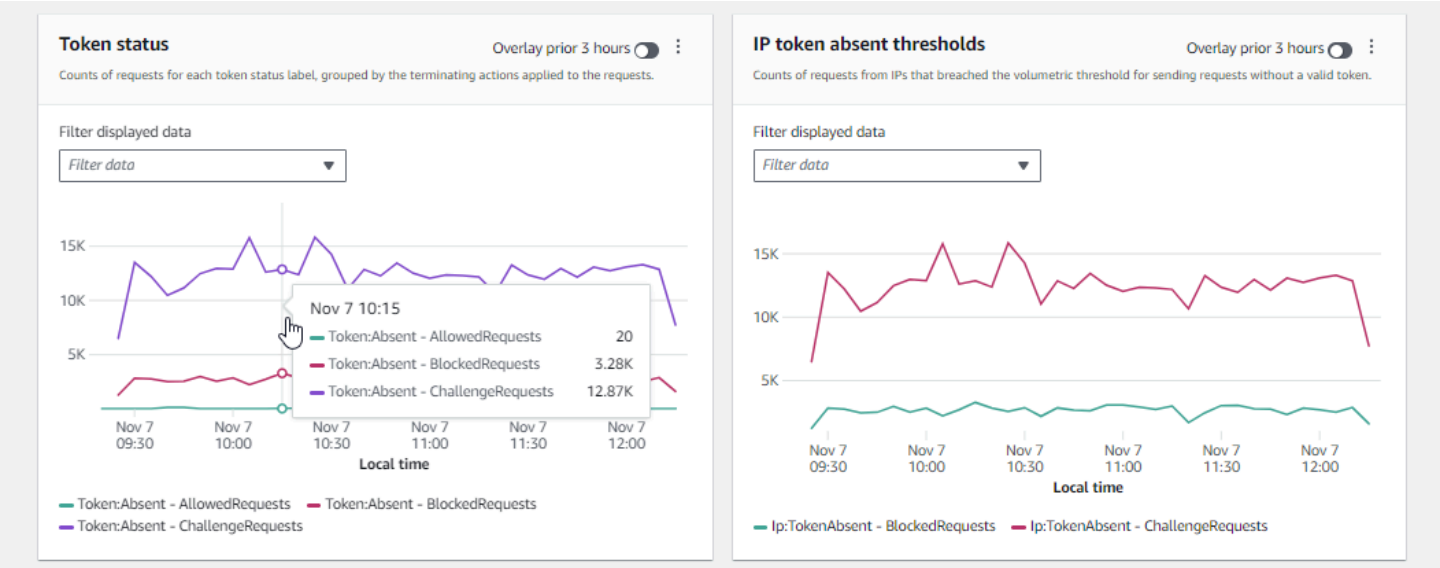
Tangkapan layar berikut menggambarkan jumlah tindakan untuk dasbor Kontrol Bot. Ini menunjukkan panel total yang sama untuk rentang waktu, tetapi jumlahnya hanya untuk permintaan yang dievaluasi oleh grup aturan Kontrol Bot. Lebih jauh ke bawah, di panel Total aksi, Anda dapat melihat jumlah tindakan di seluruh rentang waktu tiga jam yang ditentukan. Untuk rentang waktu ini, CAPTCHA tindakan tidak diterapkan pada permintaan apa pun yang dievaluasi oleh grup aturan.



Contoh layar: Grafik ringkasan status token dasbor Kontrol Bot

Tangkapan layar berikut menggambarkan dua grafik ringkasan yang tersedia di dasbor Kontrol Bot. Panel status Token menunjukkan jumlah untuk berbagai label status token, dipasangkan dengan tindakan aturan yang diterapkan pada permintaan. Panel ambang batas tidak ada token IP menunjukkan data untuk permintaan dari IP yang mengirim terlalu banyak permintaan tanpa token.

Melayang di atas area mana pun dalam grafik menampilkan detail informasi yang tersedia. Di panel status Token di tangkapan layar ini, mouse melayang di atas satu titik waktu, tanpa berada di garis grafik apa pun, sehingga konsol menampilkan data untuk semua baris pada saat itu.



Bagian ini hanya menampilkan beberapa ringkasan lalu lintas yang disediakan di dasbor ikhtisar lalu lintas ACL web. Untuk melihat dasbor untuk salah satu ACL web Anda, buka halaman ACL web di konsol. Untuk informasi tentang cara melakukan ini, lihat panduan diMelihat dasbor untuk ACL web.

Melihat contoh permintaan web

Bagian ini menjelaskan tab Permintaan Sampel ACL web di konsol. AWS WAF Di tab ini, Anda dapat melihat grafik dari semua aturan yang cocok untuk permintaan web yang AWS WAF telah diperiksa. Selain itu, jika Anda mengaktifkan sampling permintaan untuk ACL web, Anda dapat melihat tampilan tabel dari sampel permintaan web yang AWS WAF telah diperiksa. Anda juga dapat mengambil informasi permintaan sampel melalui panggilan API. `GetSampledRequests`

Contoh permintaan berisi hingga 100 permintaan yang cocok dengan kriteria aturan di ACL web dan 100 permintaan lainnya untuk permintaan yang tidak cocok dengan aturan apa pun dan tindakan default ACL web diterapkan. Permintaan dalam sampel berasal dari semua sumber daya yang dilindungi yang telah menerima permintaan untuk konten Anda dalam tiga jam sebelumnya.

Ketika permintaan web cocok dengan kriteria dalam aturan dan tindakan untuk aturan itu tidak mengakhiri evaluasi permintaan, AWS WAF terus memeriksa permintaan web menggunakan aturan berikutnya di ACL web. Karena itu, permintaan web dapat muncul beberapa kali. Untuk informasi tentang perilaku tindakan aturan, lihatTindakan aturan.

Untuk melihat grafik semua aturan dan permintaan sampel

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

2. Di panel navigasi, pilih Web ACL.
3. Pilih nama ACL web yang ingin Anda lihat permintaannya. Konsol membawa Anda ke deskripsi ACL web, tempat Anda dapat mengeditnya.
4. Di tab Permintaan sampel, Anda dapat melihat yang berikut:

   - Grafik semua aturan — Grafik ini menunjukkan aturan yang cocok dan tindakan aturan untuk semua evaluasi permintaan web yang dilakukan selama rentang waktu yang ditunjukkan.

     > **Note**
     >
     > Rentang waktu untuk grafik ini diatur di tab ikhtisar lalu lintas ACL web, di bagian Filter data. Untuk informasi, lihat Melihat dasbor untuk ACL web.

   - Tabel permintaan sampel - Tabel ini menampilkan data permintaan sampel selama 3 jam terakhir. Untuk setiap entri, tabel menampilkan data berikut:

     Nama metrik

     Nama CloudWatch metrik untuk aturan di ACL web yang cocok dengan permintaan. Jika permintaan web tidak cocok dengan aturan apa pun di ACL web, nilai ini adalah Default.

     > **Note**
     >
     > Jika Anda mengubah nama aturan dan Anda ingin nama metrik aturan mencerminkan perubahan, Anda harus memperbarui nama metrik juga. AWS WAF tidak secara otomatis memperbarui nama metrik untuk aturan saat Anda mengubah nama aturan. Anda dapat mengubah nama metrik saat mengedit aturan di konsol, dengan menggunakan editor JSON aturan. Anda juga dapat mengubah kedua nama melalui API dan dalam daftar JSON apa pun yang Anda gunakan untuk menentukan ACL web atau grup aturan.

     IP sumber

     Baik alamat IP tempat permintaan berasal atau, jika penampil menggunakan proxy HTTP atau Application Load Balancer untuk mengirim permintaan, alamat IP proxy atau Application Load Balancer.

URI

Bagian dari URL yang mengidentifikasi sumber daya, misalnya,`/images/daily-ad.jpg`.

Aturan di dalam kelompok aturan

Jika nama metrik mengidentifikasi pernyataan referensi grup aturan, ini mengidentifikasi aturan di dalam grup aturan yang cocok dengan permintaan.

Tindakan

Menunjukkan tindakan untuk aturan yang sesuai. Untuk informasi tentang kemungkinan tindakan aturan, lihatTindakan aturan.

Waktu

Waktu yang AWS WAF menerima permintaan dari sumber daya yang dilindungi.

Untuk menampilkan informasi tambahan tentang komponen permintaan web, pilih nama URI di baris permintaan.

Mengaktifkan perlindungan Anda dalam produksi

Ketika Anda telah menyelesaikan tahap akhir pengujian dan penyetelan di lingkungan produksi Anda, aktifkan perlindungan Anda dalam mode produksi.

Risiko lalu lintas produksi

Sebelum Anda menerapkan implementasi ACL web Anda untuk lalu lintas produksi, uji dan sesuaikan di lingkungan pengujian sampai Anda merasa nyaman dengan dampak potensial terhadap lalu lintas Anda. Juga uji dan sesuaikan dalam mode hitungan dengan lalu lintas produksi Anda sebelum mengaktifkan perlindungan Anda untuk lalu lintas produksi.

Note

Untuk mengikuti panduan di bagian ini, Anda perlu memahami secara umum cara membuat dan mengelola AWS WAF perlindungan seperti ACL web, aturan, dan grup aturan. Informasi itu tercakup dalam bagian sebelumnya dari panduan ini.

Lakukan langkah-langkah ini terlebih dahulu di lingkungan pengujian Anda, kemudian dalam produksi.

Aktifkan AWS WAF perlindungan Anda dalam produksi

1. Beralih ke perlindungan produksi Anda

   Perbarui ACL web Anda dan alihkan pengaturan Anda untuk produksi.

   a. Hapus aturan pengujian apa pun yang tidak Anda butuhkan

      Jika Anda menambahkan aturan pengujian yang tidak Anda perlukan dalam produksi, hapus aturan tersebut. Jika Anda menggunakan aturan pencocokan label apa pun untuk memfilter hasil aturan grup aturan terkelola, pastikan untuk membiarkannya tetap berlaku.

   b. Beralih ke tindakan produksi

      Ubah pengaturan tindakan untuk aturan baru Anda ke pengaturan produksi yang dimaksudkan.

      - Aturan yang didefinisikan dalam ACL web — Edit aturan di ACL web dan ubah tindakan mereka dari Count tindakan produksi mereka.
      - Grup aturan — Dalam konfigurasi ACL web grup aturan, alihkan aturan untuk menggunakan tindakannya sendiri atau biarkan mereka mengganti Count tindakan, sesuai dengan hasil aktivitas pengujian dan penyetelan Anda. Jika Anda menggunakan aturan pencocokan label untuk memfilter hasil aturan grup aturan, pastikan untuk membiarkan penggantian untuk aturan tersebut di tempatnya.

        Untuk beralih menggunakan tindakan aturan, dalam konfigurasi ACL web Anda, edit pernyataan aturan untuk grup aturan dan hapus Count penggantian untuk aturan tersebut. Jika Anda mengelola ACL web di JSON, dalam pernyataan referensi grup aturan, hapus entri untuk aturan dari daftar. `RuleActionOverrides`
      - Web ACL — Jika Anda mengubah tindakan default ACL web untuk pengujian Anda, alihkan ke pengaturan produksinya.

      Dengan pengaturan ini, perlindungan baru Anda akan mengelola lalu lintas web sesuai keinginan Anda.

Saat Anda menyimpan ACL web Anda, sumber daya yang terkait dengannya akan menggunakan pengaturan produksi Anda.

2. Memantau dan menyetel

   Untuk memastikan bahwa permintaan web ditangani seperti yang Anda inginkan, pantau lalu lintas Anda dengan cermat setelah Anda mengaktifkan fungsionalitas baru. Anda akan memantau metrik dan log untuk tindakan aturan produksi, alih-alih tindakan hitungan yang Anda pantau dalam pekerjaan penyetelan Anda. Terus pantau dan sesuaikan perilaku sesuai kebutuhan untuk beradaptasi dengan perubahan lalu lintas web Anda.

Cara AWS WAF bekerja dengan CloudFront fitur Amazon

Saat membuat ACL web, Anda dapat menentukan satu atau CloudFront beberapa distribusi yang AWS WAF ingin Anda periksa. AWS WAF mulai memeriksa dan mengelola permintaan web untuk distribusi tersebut berdasarkan kriteria yang Anda identifikasi di ACL web. CloudFront menyediakan beberapa fitur yang meningkatkan AWS WAF fungsionalitas. Bab ini menjelaskan beberapa cara yang dapat Anda konfigurasikan CloudFront untuk membuat CloudFront dan AWS WAF bekerja sama dengan lebih baik.

Topik

Menggunakan AWS WAF dengan halaman kesalahan CloudFront kustom

Secara default, ketika AWS WAF memblokir permintaan web berdasarkan kriteria yang Anda tentukan, ia mengembalikan kode status HTTP `403 (Forbidden)` ke CloudFront, dan CloudFront mengembalikan kode status tersebut ke penampil. Penampil kemudian menampilkan pesan default singkat dan jarang diformat mirip dengan berikut ini:

```
Forbidden: You don't have permission to access /myfilename.html on this server.
```

Anda dapat mengganti perilaku ini dalam aturan ACL AWS WAF web Anda dengan menentukan respons khusus. Untuk informasi selengkapnya tentang menyesuaikan perilaku respons menggunakan AWS WAF aturan, lihatTanggapan khusus untuk Block tindakan.

> **Note**
>
> Respons yang Anda sesuaikan menggunakan AWS WAF aturan lebih diutamakan daripada spesifikasi respons apa pun yang Anda tentukan di halaman kesalahan CloudFront kustom.

Jika Anda lebih suka menampilkan pesan kesalahan kustom melalui CloudFront, mungkin menggunakan format yang sama seperti situs web Anda lainnya, Anda dapat mengonfigurasi CloudFront untuk kembali ke penampil objek (misalnya, file HTML) yang berisi pesan kesalahan kustom Anda.

> **Note**
>
> CloudFront tidak dapat membedakan antara kode status HTTP 403 yang dikembalikan oleh asal Anda dan yang dikembalikan oleh AWS WAF ketika permintaan diblokir. Ini berarti bahwa Anda tidak dapat mengembalikan halaman kesalahan kustom yang berbeda berdasarkan penyebab yang berbeda dari kode status HTTP 403.

Untuk informasi selengkapnya tentang halaman kesalahan CloudFront kustom, lihat Menghasilkan respons kesalahan kustom di Panduan CloudFront Pengembang Amazon.

Menggunakan AWS WAF dengan CloudFront untuk aplikasi yang berjalan di server HTTP Anda sendiri

Saat menggunakannya AWS WAF CloudFront, Anda dapat melindungi aplikasi yang berjalan di server web HTTP apa pun, baik itu server web yang berjalan di Amazon Elastic Compute Cloud (Amazon EC2) atau server web yang Anda kelola secara pribadi. Anda juga dapat mengonfigurasi CloudFront untuk meminta HTTPS antara CloudFront dan server web Anda sendiri, serta antara pemirsa dan CloudFront.

Membutuhkan HTTPS antara CloudFront dan server web Anda sendiri

Untuk mewajibkan HTTPS antara CloudFront dan server web Anda sendiri, Anda dapat menggunakan fitur asal CloudFront kustom dan mengonfigurasi Kebijakan Protokol Asal dan

pengaturan Nama Domain Asal untuk asal tertentu. Dalam CloudFront konfigurasi Anda, Anda dapat menentukan nama DNS server bersama dengan port dan protokol yang CloudFront ingin Anda gunakan saat mengambil objek dari asal Anda. Anda juga harus memastikan bahwa sertifikat SSL/TLS di server asal kustom Anda cocok dengan nama domain asal yang telah Anda konfigurasikan. Ketika Anda menggunakan server web HTTP Anda sendiri di luar AWS, Anda harus menggunakan sertifikat yang ditandatangani oleh otoritas sertifikat pihak ketiga tepercaya (CA), misalnya, Comodo DigiCert, atau Symantec. Untuk informasi selengkapnya tentang mewajibkan HTTPS untuk komunikasi antara CloudFront dan server web Anda sendiri, lihat topik Memerlukan HTTPS untuk Komunikasi Antara CloudFront dan Asal Kustom Anda di Panduan CloudFront Pengembang Amazon.

Membutuhkan HTTPS antara penampil dan CloudFront

Untuk mewajibkan HTTPS antara pemirsa dan CloudFront, Anda dapat mengubah Kebijakan Protokol Penampil untuk satu atau beberapa perilaku cache dalam CloudFront distribusi Anda. Untuk informasi selengkapnya tentang penggunaan HTTPS antar pemirsa dan CloudFront, lihat topik Memerlukan HTTPS untuk Komunikasi Antar CloudFront Pemirsa dan di Panduan CloudFront Pengembang Amazon. Anda juga dapat membawa sertifikat SSL Anda sendiri sehingga pemirsa dapat terhubung ke CloudFront distribusi Anda melalui HTTPS menggunakan nama domain Anda sendiri, misalnya https://www.mysite.com. Untuk informasi selengkapnya, lihat topik Mengonfigurasi Nama Domain Alternatif dan HTTPS di Panduan CloudFront Pengembang Amazon.

Memilih metode HTTP yang CloudFront merespons

Saat Anda membuat distribusi CloudFront web Amazon, Anda memilih metode HTTP yang ingin CloudFront Anda proses dan teruskan ke asal Anda. Anda dapat memilih dari opsi berikut:

- **`GET`**, **`HEAD`** — Anda CloudFront hanya dapat menggunakan untuk mendapatkan objek dari asal Anda atau untuk mendapatkan header objek.
- **`GET`**,**`HEAD`**, **`OPTIONS`** — Anda CloudFront hanya dapat menggunakan untuk mendapatkan objek dari asal Anda, mendapatkan header objek, atau mengambil daftar opsi yang didukung server asal Anda.
- **`GET`**,**`HEAD`**,**`OPTIONS`**,**`PUT`**,**`POST`**,**`PATCH`**, **`DELETE`** — Anda dapat menggunakan CloudFront untuk mendapatkan, menambah, memperbarui, dan menghapus objek, dan untuk mendapatkan header objek. Selain itu, Anda dapat melakukan `POST` operasi lain seperti mengirimkan data dari formulir web.

Anda juga dapat menggunakan pernyataan aturan pencocokan AWS WAF byte untuk mengizinkan atau memblokir permintaan berdasarkan metode HTTP, seperti yang dijelaskan dalamPernyataan aturan kecocokan string. Jika Anda ingin menggunakan kombinasi metode yang CloudFront mendukung, seperti `GET` dan`HEAD`, maka Anda tidak perlu mengkonfigurasi AWS WAF untuk memblokir permintaan yang menggunakan metode lain. Jika Anda ingin mengizinkan kombinasi metode yang CloudFront tidak mendukung, seperti,, dan `GET` `HEAD``POST`, Anda dapat mengonfigurasi CloudFront untuk menanggapi semua metode, dan kemudian gunakan AWS WAF untuk memblokir permintaan yang menggunakan metode lain.

Untuk informasi selengkapnya tentang memilih metode yang CloudFront merespons, lihat Metode HTTP yang Diizinkan dalam topik Nilai yang Anda Tentukan Saat Membuat atau Memperbarui Distribusi Web di Panduan CloudFront Pengembang Amazon.

Keamanan dalam penggunaan AWS WAF layanan Anda

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

> **Note**
>
> Bagian ini memberikan panduan AWS keamanan standar untuk penggunaan AWS WAF layanan dan AWS sumber dayanya, seperti ACL AWS WAF web dan grup aturan.
> Untuk informasi tentang melindungi AWS sumber daya Anda menggunakan AWS WAF, lihat AWS WAF panduan lainnya.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan dari cloud dan keamanan di cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Efektivitas keamanan kami diuji dan diverifikasi secara rutin oleh auditor pihak ketiga sebagai bagian dari program kepatuhan AWS. Untuk mempelajari tentang program kepatuhan yang berlaku AWS WAF, lihat AWS Layanan dalam Lingkup berdasarkan Program Kepatuhan.
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor-faktor lain termasuk sensitivitas data Anda, persyaratan organisasi Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan AWS WAF. Topik berikut menunjukkan cara mengonfigurasi AWS WAF untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga belajar cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan AWS WAF sumber daya Anda.

Topik

Perlindungan data di AWS WAF

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di AWS WAF. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensyal dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.

- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi yang lebih lengkap tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan AWS WAF atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

AWS WAF entitas — seperti ACL web, grup aturan, dan set IP — dienkripsi saat istirahat, kecuali di Wilayah tertentu di mana enkripsi tidak tersedia, termasuk China (Beijing) dan China (Ningxia). Kunci enkripsi unik digunakan untuk setiap Wilayah.

Menghapus sumber daya AWS WAF

Anda dapat menghapus sumber daya yang Anda buat AWS WAF. Lihat panduan untuk setiap jenis sumber daya di bagian berikut.

- Menghapus ACL web
- Menghapus grup aturann
- Menghapus set IP
- Menghapus set pola regex

Identitas dan manajemen akses untuk AWS WAF

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya. AWS WAF IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan. AWS WAF

Pengguna layanan — Jika Anda menggunakan AWS WAF layanan untuk melakukan pekerjaan Anda, administrator Anda memberi Anda kredensyal dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak AWS WAF fitur untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara mengelola akses dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di AWS WAF, lihat Memecahkan masalah AWS WAF identitas dan akses.

Administrator layanan — Jika Anda bertanggung jawab atas AWS WAF sumber daya di perusahaan Anda, Anda mungkin memiliki akses penuh ke AWS WAF. Tugas Anda adalah menentukan AWS WAF fitur dan sumber daya mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep Basic IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM AWS WAF, lihatBagaimana AWS WAF bekerja dengan IAM.

Administrator IAM – Jika Anda adalah administrator IAM, Anda mungkin ingin belajar dengan lebih detail tentang cara Anda menulis kebijakan untuk mengelola akses ke AWS WAF. Untuk melihat contoh kebijakan AWS WAF berbasis identitas yang dapat Anda gunakan di IAM, lihat. Contoh kebijakan berbasis identitas untuk AWS WAF

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensyal identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensyal yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensyal Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensyal Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Menandatangani permintaan AWS API di Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat Autentikasi multi-faktor dalam Panduan Pengguna AWS IAM Identity Center dan Menggunakan autentikasi multi-faktor (MFA) dalam AWS dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensyal sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensyal yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensyal sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat Apakah itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup yang bernama IAMAdmins dan memberikan izin ke grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat Kapan harus membuat pengguna IAM (bukan peran) dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil peran IAM untuk sementara AWS Management Console dengan beralih peran. Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat Menggunakan peran IAM dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Sebagai contoh, ketika Anda memanggil suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan

hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.

- Peran layanan – Peran layanan adalah peran IAM yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
- Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensyal sementara untuk aplikasi yang berjalan pada instans EC2 dan membuat atau permintaan API. AWS CLI AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan dalam instans Amazon EC2 dalam Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, lihat Kapan harus membuat peran IAM (bukan pengguna) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasinya. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan yang dikelola atau kebijakan inline, lihat Memilih antara kebijakan yang dikelola dan kebijakan inline dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Daftar kontrol akses (ACL)

Daftar kontrol akses (ACL) mengendalikan prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, lihat Gambaran umum daftar kontrol akses (ACL) dalam Panduan Developer Amazon Simple Storage Service.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) — SCP adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur di organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organisasi dan SCP, lihat Cara kerja SCP dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Bagaimana AWS WAF bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses AWS WAF, pelajari fitur IAM yang tersedia untuk digunakan. AWS WAF

Fitur IAM yang dapat Anda gunakan dengan AWS WAF

Fitur IAM	AWS WAF dukungan
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Ya
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Ya
ACL	Tidak
ABAC (tanda dalam kebijakan)	Parsial
Kredensial sementara	Ya
Sesi akses teruskan (FAS)	Ya
Peran layanan	Ya
Peran terkait layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara AWS WAF dan AWS layanan lain bekerja dengan sebagian besar fitur IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk AWS WAF

Mendukung kebijakan berbasis identitas	Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Untuk melihat contoh kebijakan AWS WAF berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk AWS WAF

Kebijakan berbasis sumber daya dalam AWS WAF

Mendukung kebijakan berbasis sumber daya	Ya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai prinsipal dalam kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, administrator IAM di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke prinsipal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

AWS WAF menggunakan kebijakan berbasis sumber daya untuk mendukung pembagian grup aturan di seluruh akun. Anda membagikan grup aturan yang Anda miliki dengan AWS akun lain dengan menyediakan setelan kebijakan berbasis sumber daya ke panggilan AWS WAF API `PutPermissionPolicy` atau panggilan CLI atau SDK yang setara. Untuk informasi tambahan, termasuk contoh dan tautan ke dokumentasi untuk bahasa lain yang tersedia, lihat PutPermissionPolicydi Referensi AWS WAF API. Fungsionalitas ini tidak tersedia melalui cara lain, seperti konsol atau AWS CloudFormation.

Tindakan kebijakan untuk AWS WAF

Mendukung tindakan kebijakan	Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar AWS WAF tindakan dan izin untuk masing-masing tindakan, lihat Tindakan yang ditentukan oleh AWS WAF V2 di Referensi Otorisasi Layanan.

Tindakan kebijakan AWS WAF menggunakan awalan berikut sebelum tindakan:

```
wafv2
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

```
"Action": [
      "wafv2:action1",
      "wafv2:action2"
         ]
```

Anda juga dapat menentukan beberapa tindakan menggunakan wildcard (*). Misalnya, untuk menentukan semua tindakan AWS WAF yang dimulai dengan`List`, sertakan tindakan berikut:

```
"Action": "wafv2:List*"
```

Untuk melihat contoh kebijakan AWS WAF berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk AWS WAF

Tindakan yang memerlukan pengaturan izin tambahan

Beberapa tindakan memerlukan izin yang tidak dapat dijelaskan sepenuhnya dalam Tindakan yang ditentukan oleh AWS WAF V2 di Referensi Otorisasi Layanan. Bagian ini memberikan informasi izin tambahan.

Topik

- Izin untuk AssociateWebACL
- Izin untuk DisassociateWebACL
- Izin untuk GetWebACLForResource
- Izin untuk ListResourcesForWebACL

Izin untuk **`AssociateWebACL`**

Bagian ini mencantumkan izin yang diperlukan untuk mengaitkan ACL web ke sumber daya menggunakan tindakan. AWS WAF `AssociateWebACL`

Untuk CloudFront distribusi Amazon, alih-alih tindakan ini, gunakan CloudFront tindakan`UpdateDistribution`. Untuk selengkapnya, lihat UpdateDistributiondi Referensi Amazon CloudFront API.

API REST Amazon API Gateway

Memerlukan izin untuk memanggil API Gateway `SetWebACL` pada jenis sumber daya REST API dan memanggil AWS WAF `AssociateWebACL` ACL web.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "apigateway:SetWebACL"
    ],
    "Resource": [
        "arn:aws:apigateway:*::/restapis/*/stages/*"
    ]
}
```

Penyeimbang Beban Aplikasi

Memerlukan izin untuk memanggil `elasticloadbalancing:SetWebACL` tindakan pada jenis sumber daya Application Load Balancer dan memanggil AWS WAF `AssociateWebACL` ACL web.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
```

```
    "Effect": "Allow",
    "Action": [
        "elasticloadbalancing:SetWebACL"
    ],
    "Resource": [
        "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/app/*/*"
    ]
}
```

AWS AppSync GraphQL API

Memerlukan izin untuk memanggil AWS AppSync `SetWebACL` tipe sumber daya API GraphQL dan AWS WAF `AssociateWebACL` memanggil ACL web.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "appsync:SetWebACL"
    ],
    "Resource": [
        "arn:aws:appsync:*:account-id:apis/*"
    ]
}
```

Kolam pengguna Amazon Cognito

Memerlukan izin untuk memanggil `AssociateWebACL` tindakan Amazon Cognito pada jenis sumber daya kumpulan pengguna dan memanggil AWS WAF `AssociateWebACL` ACL web.

```
{
    "Sid": "AssociateWebACL1",
```

```
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}
```

AWS App Runner layanan

Memerlukan izin untuk memanggil `AssociateWebACL` tindakan App Runner pada jenis sumber daya layanan App Runner dan memanggil AWS WAF `AssociateWebACL` ACL web.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "apprunner:AssociateWebAcl"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
```

```
}
```

AWS Contoh Akses Terverifikasi

Memerlukan izin untuk memanggil `ec2:AssociateVerifiedAccessInstanceWebAcl` tindakan pada jenis sumber daya instans Akses Terverifikasi dan memanggil AWS WAF `AssociateWebACL` ACL web.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "ec2:AssociateVerifiedAccessInstanceWebAcl"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

Izin untuk **`DisassociateWebACL`**

Bagian ini mencantumkan izin yang diperlukan untuk memisahkan ACL web dari sumber daya menggunakan tindakan. AWS WAF `DisassociateWebACL`

Untuk CloudFront distribusi Amazon, alih-alih tindakan ini, gunakan CloudFront tindakan `UpdateDistribution` dengan ID ACL web kosong. Untuk selengkapnya, lihat UpdateDistributiondi Referensi Amazon CloudFront API.

API REST Amazon API Gateway

Memerlukan izin untuk memanggil API Gateway `SetWebACL` pada jenis sumber daya REST API. Tidak memerlukan izin untuk menelepon AWS WAF `DisassociateWebACL`.

```
{
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "apigateway:SetWebACL"
    ],
    "Resource": [
        "arn:aws:apigateway:*::/restapis/*/stages/*"
    ]
}
```

Penyeimbang Beban Aplikasi

Memerlukan izin untuk memanggil `elasticloadbalancing:SetWebACL` tindakan pada tipe sumber daya Application Load Balancer. Tidak memerlukan izin untuk menelepon AWS WAF `DisassociateWebACL`.

```
{
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "elasticloadbalancing:SetWebACL"
    ],
    "Resource": [
        "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/app/*/*"
    ]
}
```

AWS AppSync GraphQL API

Memerlukan izin untuk memanggil AWS AppSync `SetWebACL` tipe sumber daya GraphQL API. Tidak memerlukan izin untuk menelepon AWS WAF `DisassociateWebACL`.

```
{
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "appsync:SetWebACL"
    ],
    "Resource": [
        "arn:aws:appsync:*:account-id:apis/*"
    ]
```

```
}
```

Kolam pengguna Amazon Cognito

Memerlukan izin untuk memanggil `DisassociateWebACL` tindakan Amazon Cognito pada jenis sumber daya kumpulan pengguna dan untuk memanggil. AWS WAF `DisassociateWebACL`

```
{
    "Sid": "DisassociateWebACL1",
    "Effect": "Allow",
    "Action": "wafv2:DisassociateWebACL",
    "Resource": "*"
},
{
    "Sid": "DisassociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:DisassociateWebACL"
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}
```

AWS App Runner layanan

Memerlukan izin untuk memanggil `DisassociateWebACL` tindakan App Runner pada jenis sumber daya layanan App Runner dan untuk memanggil. AWS WAF `DisassociateWebACL`

```
{
    "Sid": "DisassociateWebACL1",
    "Effect": "Allow",
    "Action": "wafv2:DisassociateWebACL",
    "Resource": "*"
},
{
    "Sid": "DisassociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "apprunner:DisassociateWebAcl"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
```

```
    ]
}
```

AWS Contoh Akses Terverifikasi

Memerlukan izin untuk memanggil `ec2:DisassociateVerifiedAccessInstanceWebAcl` tindakan pada jenis sumber daya instans Akses Terverifikasi dan untuk memanggil AWS WAF `DisassociateWebACL`.

```
{
    "Sid": "DisassociateWebACL1",
    "Effect": "Allow",
    "Action": "wafv2:DisassociateWebACL",
    "Resource": "*"
},
{
    "Sid": "DisassociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "ec2:DisassociateVerifiedAccessInstanceWebAcl"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

Izin untuk **`GetWebACLForResource`**

Bagian ini mencantumkan izin yang diperlukan untuk mendapatkan ACL web untuk sumber daya yang dilindungi menggunakan tindakan. AWS WAF `GetWebACLForResource`

Untuk CloudFront distribusi Amazon, alih-alih tindakan ini, gunakan CloudFront tindakan`GetDistributionConfig`. Untuk selengkapnya, lihat GetDistributionConfigdi Referensi Amazon CloudFront API.

> **Note**
>
> `GetWebACLForResource`membutuhkan izin untuk meneleponGetWebACL. Dalam konteks ini, AWS WAF gunakan `GetWebACL` hanya untuk memverifikasi bahwa akun Anda memiliki izin yang diperlukan untuk mengakses ACL web yang `GetWebACLForResource` kembali. Ketika Anda meneleponGetWebACLForResource, Anda mungkin mendapatkan kesalahan

yang menunjukkan bahwa akun Anda tidak diizinkan untuk bekerja `wafv2:GetWebACL` pada sumber daya. AWS WAF tidak menambahkan jenis kesalahan ini ke riwayat AWS CloudTrail acara.

Amazon API Gateway REST API, Application Load Balancer, dan AWS AppSync GraphQL API

Memerlukan izin untuk menelepon AWS WAF `GetWebACLForResource` dan `GetWebACL` untuk ACL web.

```
{
    "Sid": "GetWebACLForResource",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
}
```

Kolam pengguna Amazon Cognito

Memerlukan izin untuk memanggil `GetWebACLForResource` tindakan Amazon Cognito pada jenis sumber daya kumpulan pengguna dan untuk memanggil AWS WAF `GetWebACLForResource` dan. `GetWebACL`

```
{
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "GetWebACLForResource2",
```

```
    "Effect": "Allow",
    "Action": [
        "cognito-idp:GetWebACLForResource"
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}
```

AWS App Runner layanan

Memerlukan izin untuk memanggil `DescribeWebAclForService` tindakan App Runner pada jenis sumber daya layanan App Runner dan untuk memanggil AWS WAF `GetWebACLForResource` dan. `GetWebACL`

```
{
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "GetWebACLForResource2",
    "Effect": "Allow",
    "Action": [
        "apprunner:DescribeWebAclForService"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
}
```

AWS Contoh Akses Terverifikasi

Memerlukan izin untuk memanggil `ec2:GetVerifiedAccessInstanceWebAcl` tindakan pada jenis sumber daya instans Akses Terverifikasi dan untuk memanggil AWS WAF `GetWebACLForResource` dan`GetWebACL`.

```
{
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "GetWebACLForResource2",
    "Effect": "Allow",
    "Action": [
        "ec2:GetVerifiedAccessInstanceWebAcl"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

Izin untuk **`ListResourcesForWebACL`**

Bagian ini mencantumkan izin yang diperlukan untuk mengambil daftar sumber daya yang dilindungi untuk ACL web menggunakan tindakan. AWS WAF `ListResourcesForWebACL`

Untuk CloudFront distribusi Amazon, alih-alih tindakan ini, gunakan CloudFront tindakan`ListDistributionsByWebACLId`. Untuk selengkapnya, lihat ListDistributionsByWebACLID di Referensi Amazon CloudFront API.

Amazon API Gateway REST API, Application Load Balancer, dan AWS AppSync GraphQL API

Memerlukan izin AWS WAF `ListResourcesForWebACL` untuk memanggil ACL web.

```
{
    "Sid": "ListResourcesForWebACL",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
```

```
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
}
```

Kolam pengguna Amazon Cognito

Memerlukan izin untuk memanggil `ListResourcesForWebACL` tindakan Amazon Cognito pada jenis sumber daya kumpulan pengguna dan untuk memanggil. AWS WAF `ListResourcesForWebACL`

```
{
    "Sid": "ListResourcesForWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "ListResourcesForWebACL2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}
```

AWS App Runner layanan

Memerlukan izin untuk memanggil `ListAssociatedServicesForWebAcl` tindakan App Runner pada jenis sumber daya layanan App Runner dan untuk memanggil. AWS WAF `ListResourcesForWebACL`

```
{
    "Sid": "ListResourcesForWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
```

```
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "ListResourcesForWebACL2",
    "Effect": "Allow",
    "Action": [
        "apprunner:ListAssociatedServicesForWebAcl"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
}
```

AWS Contoh Akses Terverifikasi

Memerlukan izin untuk memanggil `ec2:DescribeVerifiedAccessInstanceWebAclAssociations` tindakan pada jenis sumber daya instans Akses Terverifikasi dan untuk memanggil AWS WAF `ListResourcesForWebACL`.

```
{
    "Sid": "ListResourcesForWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "ListResourcesForWebACL2",
    "Effect": "Allow",
    "Action": [
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

Sumber daya kebijakan untuk AWS WAF

Mendukung sumber daya kebijakan	Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Untuk melihat daftar jenis AWS WAF sumber daya dan ARNnya, lihat Sumber daya yang ditentukan oleh AWS WAF V2 di Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang ditentukan oleh AWS WAF V2. Untuk mengizinkan atau menolak akses ke subset sumber AWS WAF daya, sertakan ARN sumber daya dalam elemen `resource` kebijakan Anda.

ARN sumber AWS WAF `wafv2` daya memiliki format berikut:

```
arn:partition:wafv2:region:account-id:scope/resource-type/resource-name/resource-id
```

Untuk informasi umum tentang spesifikasi ARN, lihat Nama Sumber Daya Amazon (ARN) di. Referensi Umum Amazon Web Services

Berikut daftar persyaratan yang khusus untuk ARN `wafv2` sumber daya:

- *`region`*: Untuk AWS WAF sumber daya yang Anda gunakan untuk melindungi CloudFront distribusi Amazon, setel ini ke`us-east-1`. Jika tidak, setel ini ke Wilayah yang Anda gunakan dengan sumber daya regional yang dilindungi.

- *scope*: Tetapkan cakupan `global` untuk digunakan dengan CloudFront distribusi Amazon atau `regional` untuk digunakan dengan sumber daya regional mana pun yang AWS WAF mendukung. Sumber daya regional adalah Amazon API Gateway REST API, Application Load Balancer, GraphQL API AWS AppSync , kumpulan pengguna Amazon Cognito, layanan, dan instance Akses Terverifikasi. AWS App Runner AWS
- *resource-type*: Tentukan salah satu nilai berikut:`webacl`,,,`rulegroup`, `ipset` atau. `regexpatternset` `managedruleset`
- *resource-name*: Tentukan nama yang Anda berikan AWS WAF sumber daya, atau tentukan wildcard (*) untuk menunjukkan semua sumber daya yang memenuhi spesifikasi lain di ARN. Anda harus menentukan nama sumber daya dan ID sumber daya atau menentukan wildcard untuk keduanya.
- *resource-id*: Tentukan ID AWS WAF sumber daya, atau tentukan wildcard (*) untuk menunjukkan semua sumber daya yang memenuhi spesifikasi lain di ARN. Anda harus menentukan nama sumber daya dan ID sumber daya atau menentukan wildcard untuk keduanya.

Misalnya, ARN berikut menentukan semua ACL web dengan cakupan regional untuk akun di Wilayah: `111122223333` `us-west-1`

```
arn:aws:wafv2:us-west-1:111122223333:regional/webacl/*/*
```

ARN berikut menentukan grup aturan bernama `MyIPManagementRuleGroup` dengan cakupan global untuk akun `111122223333` di Wilayah: `us-east-1`

```
arn:aws:wafv2:us-east-1:111122223333:global/rulegroup/MyIPManagementRuleGroup/1111aaaa-bbbb-cccc-dddd-example-id
```

Untuk melihat contoh kebijakan AWS WAF berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk AWS WAF

Kunci kondisi kebijakan untuk AWS WAF

Mendukung kunci kondisi kebijakan khusus layanan	Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi `AND` logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan `OR` operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tag yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, lihat Elemen kebijakan IAM: variabel dan tag dalam Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Selain itu, AWS WAF mendukung kunci kondisi berikut yang dapat Anda gunakan untuk memberikan pemfilteran halus untuk kebijakan IAM Anda:

- wafv2: LogDestinationResource

  Kunci kondisi ini mengambil spesifikasi Nama Sumber Daya Amazon (ARN) untuk tujuan pencatatan. Ini adalah ARN yang Anda sediakan untuk tujuan pencatatan saat Anda menggunakan panggilan REST API. `PutLoggingConfiguration`

  Anda dapat secara eksplisit menentukan ARN dan Anda dapat menentukan pemfilteran untuk ARN. Contoh berikut menentukan pemfilteran untuk ARN bucket Amazon S3 yang memiliki lokasi dan awalan tertentu.

  ```
  "Condition": { "ArnLike": { "wafv2:LogDestinationResource": "arn:aws:s3:::aws-waf-logs-suffix/custom-prefix/*" } }
  ```

- wafv2: LogScope

Kunci kondisi ini mendefinisikan sumber konfigurasi logging dalam string. Saat ini, ini selalu diatur ke default`Customer`, yang menunjukkan bahwa tujuan logging dimiliki dan dikelola oleh Anda.

Untuk melihat daftar kunci AWS WAF kondisi, lihat Kunci kondisi untuk AWS WAF V2 di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang ditentukan oleh AWS WAF V2.

Untuk melihat contoh kebijakan AWS WAF berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk AWS WAF

ACL di AWS WAF

Mendukung ACL	Tidak

Daftar kontrol akses (ACL) mengendalikan pengguna utama mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

ABAC dengan AWS WAF

Mendukung ABAC (tanda dalam kebijakan)	Parsial

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi ketika tag milik prinsipal cocok dengan tag yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi saat manajemen kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tag di elemen kondisi dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Apa itu ABAC? dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) dalam Panduan Pengguna IAM.

Menggunakan kredensyal sementara dengan AWS WAF

Mendukung penggunaan kredensial sementara	Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensyal sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensi sementara, lihat Layanan AWS yang bekerja dengan IAM di Panduan Pengguna IAM.

Anda menggunakan kredensyal sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensyal sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat Peralihan peran (konsol) dalam Panduan Pengguna IAM.

Anda dapat membuat kredensyal sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensyal sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda menghasilkan kredensyal sementara secara dinamis alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

Teruskan sesi akses untuk layanan AWS WAF

Mendukung sesi akses maju (FAS)	Ya

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan

izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.

Peran layanan untuk AWS WAF

Mendukung peran layanan	Ya

Peran layanan adalah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak AWS WAF fungsionalitas. Edit peran layanan hanya jika AWS WAF memberikan panduan untuk melakukannya.

Peran terkait layanan untuk AWS WAF

Mendukung peran terkait layanan	Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang membuat atau mengelola peran AWS WAF terkait layanan, lihat. Menggunakan peran terkait layanan untuk AWS WAF

Contoh kebijakan berbasis identitas untuk AWS WAF

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi AWS WAF sumber daya. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management

Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat menjalankan peran.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh AWS WAF, termasuk format ARN untuk setiap jenis sumber daya, lihat Kunci tindakan, sumber daya, dan kondisi untuk AWS WAF V2 di Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol AWS WAF
- Izinkan pengguna melihat izin mereka sendiri
- Berikan akses hanya-baca ke AWS WAF,, dan CloudFront CloudWatch
- Memberikan akses penuh ke AWS WAF, CloudFront, dan CloudWatch
- Berikan akses ke satu Akun AWS
- Berikan akses ke satu web ACL
- Berikan akses CLI ke ACL web dan grup aturan

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus AWS WAF sumber daya di akun Anda. Tindakan ini dikenai biaya untuk Akun AWS Anda. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat kebijakan yang dikelola AWS atau kebijakan yang dikelola AWS untuk fungsi pekerjaan di Panduan Pengguna IAM.

- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukan ini dengan menentukan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, juga dikenal sebagai izin hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk menerapkan izin, lihat Kebijakan dan izin di IAM di Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Syarat di Panduan Pengguna IAM.
- Menggunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda guna memastikan izin yang aman dan berfungsi – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat validasi kebijakan Analizer Akses IAM di Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk mewajibkan MFA saat operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi akses API yang dilindungi MFA di Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM di Panduan Pengguna IAM.

Menggunakan konsol AWS WAF

Untuk mengakses AWS WAF konsol, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang AWS WAF sumber daya di Anda Akun AWS. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebaliknya, izinkan akses hanya ke tindakan yang cocok dengan operasi API yang coba dilakukan.

Untuk memastikan bahwa pengguna dan peran dapat menggunakan AWS WAF konsol, lampirkan juga setidaknya kebijakan AWS WAF `AWSWAFConsoleReadOnlyAccess` AWS terkelola ke entitas. Untuk informasi tentang kebijakan terkelola ini, lihatAWS kebijakan terkelola: AWSWAFConsoleReadOnlyAccess. Untuk informasi selengkapnya tentang melampirkan kebijakan terkelola ke pengguna, lihat Menambahkan izin ke pengguna di Panduan Pengguna IAM.

Izinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan para pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
```

```
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Berikan akses hanya-baca ke AWS WAF,, dan CloudFront CloudWatch

Kebijakan berikut memberi pengguna akses hanya-baca ke AWS WAF sumber daya, distribusi CloudFront web Amazon, dan metrik Amazon. CloudWatch Ini berguna bagi pengguna yang memerlukan izin untuk melihat pengaturan dalam AWS WAF kondisi, aturan, dan ACL web untuk melihat distribusi mana yang terkait dengan ACL web, dan untuk memantau metrik dan sampel permintaan di. CloudWatch Pengguna ini tidak dapat membuat, memperbarui, atau menghapus AWS WAF sumber daya.

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Action": [
            "wafv2:Get*",
            "wafv2:List*",
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListDistributions",
            "cloudfront:ListDistributionsByWebACLId",
            "cloudwatch:ListMetrics",
            "cloudwatch:GetMetricStatistics",
            "ec2:DescribeRegions"
         ],
         "Effect": "Allow",
         "Resource": "*"
      }
   ]
}
```

Memberikan akses penuh ke AWS WAF, CloudFront, dan CloudWatch

Kebijakan berikut memungkinkan pengguna melakukan AWS WAF operasi apa pun, melakukan operasi apa pun pada distribusi CloudFront web, dan memantau metrik dan contoh permintaan di. CloudWatch Ini berguna untuk pengguna yang merupakan AWS WAF administrator.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Action": [
            "wafv2:*",
            "cloudfront:CreateDistribution",
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:UpdateDistribution",
            "cloudfront:ListDistributions",
            "cloudfront:ListDistributionsByWebACLId",
            "cloudfront:DeleteDistribution",
            "cloudwatch:ListMetrics",
            "cloudwatch:GetMetricStatistics",
            "ec2:DescribeRegions"
         ],
         "Effect": "Allow",
         "Resource": "*"
      }
   ]
}
```

Kami sangat menyarankan Anda mengonfigurasi otentikasi multi-faktor (MFA) untuk pengguna yang memiliki izin administratif. Untuk informasi selengkapnya, lihat Menggunakan Perangkat Multi-Factor Authentication (MFA) dengan Panduan Pengguna IAM. AWS

Berikan akses ke satu Akun AWS

Kebijakan ini memberikan izin berikut ke akun 444455556666:

- Akses penuh ke semua AWS WAF operasi dan sumber daya.
- Baca dan perbarui akses ke semua CloudFront distribusi, yang memungkinkan Anda mengaitkan ACL dan CloudFront distribusi web.
- Baca akses ke semua CloudWatch metrik dan statistik metrik, sehingga Anda dapat melihat CloudWatch data dan sampel permintaan di AWS WAF konsol.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "wafv2:*"
         ],
         "Resource": [
            "arn:aws:wafv2:us-east-1:444455556666:*"
         ]
      },
      {
         "Effect": "Allow",
         "Action": [
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListDistributions",
            "cloudfront:ListDistributionsByWebACLId",
            "cloudfront:UpdateDistribution",
            "cloudwatch:ListMetrics",
            "cloudwatch:GetMetricStatistics",
            "ec2:DescribeRegions"
         ],
         "Resource": [
            "*"
         ]
      }
   ]
}
```

Berikan akses ke satu web ACL

Kebijakan berikut memungkinkan pengguna melakukan AWS WAF operasi apa pun melalui konsol pada ACL web tertentu di akun444455556666.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "wafv2:*"
```

```
            ],
            "Resource": [
                "arn:aws:wafv2:us-east-1:444455556666:regional/webacl/
test123/112233d7c-86b2-458b-af83-51c51example",
            ]
        },
        {
            "Sid": "consoleAccess",
            "Effect": "Allow",
            "Action": [
                "wafv2:ListWebACLs",
                "ec2:DescribeRegions"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Berikan akses CLI ke ACL web dan grup aturan

Kebijakan berikut memungkinkan pengguna melakukan AWS WAF operasi apa pun melalui CLI pada ACL web tertentu dan grup aturan tertentu di akun. `444455556666`

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "wafv2:*"
         ],
         "Resource": [
        "arn:aws:wafv2:us-east-1:444455556666:regional/webacl/
test123/112233d7c-86b2-458b-af83-51c51example",
        "arn:aws:wafv2:us-east-1:444455556666:regional/rulegroup/
test123rulegroup/555555555-6666-1234-abcd-00d11example"
         ]
      }
   ]
}
```

Kebijakan berikut memungkinkan pengguna melakukan AWS WAF operasi apa pun melalui konsol pada ACL web tertentu di akun444455556666.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "wafv2:*"
            ],
            "Resource": [
                "arn:aws:wafv2:us-east-1:444455556666:regional/webacl/
test123/112233d7c-86b2-458b-af83-51c51example",
            ]
        },
        {
            "Sid": "consoleAccess",
            "Effect": "Allow",
            "Action": [
                "wafv2:ListWebACLs",
                "ec2:DescribeRegions"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS kebijakan terkelola untuk AWS WAF

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pemutakhiran akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat AWS kebijakan yang dikelola dalam Panduan Pengguna IAM.

AWS kebijakan terkelola: AWSWAFReadOnlyAccess

Kebijakan ini memberikan izin hanya-baca yang memungkinkan pengguna mengakses AWS WAF sumber daya dan sumber daya untuk layanan terintegrasi, seperti Amazon, Amazon API CloudFront Gateway, Application Load Balancer, AWS AppSync Amazon Cognito, dan Akses Terverifikasi. AWS App Runner AWS Anda dapat melampirkan kebijakan ini ke identitas IAM Anda. AWS WAF juga melampirkan kebijakan ini ke peran layanan yang memungkinkan AWS WAF untuk melakukan tindakan atas nama Anda.

Untuk detail tentang kebijakan ini, lihat AWSWAFReadOnlyAccessdi konsol IAM.

AWS kebijakan terkelola: AWSWAFFullAccess

Kebijakan ini memberikan akses penuh ke AWS WAF sumber daya dan sumber daya untuk layanan terintegrasi, seperti Amazon, Amazon API Gateway CloudFront, Application Load Balancer AWS AppSync, Amazon Cognito,, dan Akses Terverifikasi AWS App Runner. AWS Anda dapat melampirkan kebijakan ini ke identitas IAM Anda. AWS WAF juga melampirkan kebijakan ini ke peran layanan yang memungkinkan AWS WAF untuk melakukan tindakan atas nama Anda.

Untuk detail tentang kebijakan ini, lihat AWSWAFFullAccessdi konsol IAM.

AWS kebijakan terkelola: AWSWAFConsoleReadOnlyAccess

Kebijakan ini memberikan izin hanya-baca ke AWS WAF konsol, yang mencakup sumber daya untuk AWS WAF dan untuk layanan terintegrasi, seperti Amazon, Amazon API CloudFront Gateway, Application Load Balancer, AWS AppSync Amazon Cognito, dan Akses Terverifikasi. AWS App Runner AWS Anda dapat melampirkan kebijakan ini ke identitas IAM Anda. AWS WAF juga melampirkan kebijakan ini ke aiam/home#/policies/arn:aws:iam: :aws:policy/ $ peran layanan yang memungkinkan untuk melakukan tindakan atas nama Anda. AWSWAFConsoleFullAccess serviceLevelSummary AWS WAF

Untuk detail tentang kebijakan ini, lihat AWSWAFConsoleReadOnlyAccessdi konsol IAM.

AWS kebijakan terkelola: AWSWAFConsoleFullAccess

Kebijakan ini memberikan akses penuh ke AWS WAF konsol, yang mencakup sumber daya untuk AWS WAF dan untuk layanan terintegrasi, seperti Amazon, Amazon API Gateway CloudFront, Application Load Balancer AWS AppSync, Amazon Cognito, dan Akses Terverifikasi AWS App Runner. AWS Anda dapat melampirkan kebijakan ini ke identitas IAM Anda. AWS WAF juga melampirkan kebijakan ini ke peran layanan yang memungkinkan AWS WAF untuk melakukan tindakan atas nama Anda.

Untuk detail tentang kebijakan ini, lihat AWSWAFConsoleFullAccessdi konsol IAM.

AWS kebijakan terkelola: WAFV2 LoggingServiceRolePolicy

Kebijakan ini memungkinkan AWS WAF untuk menulis log ke Amazon Data Firehose. Kebijakan ini hanya digunakan jika Anda mengaktifkan login AWS WAF. Kebijakan ini dilampirkan pada peran terkait layanan. `AWSServiceRoleForWAFV2Logging` Untuk informasi selengkapnya tentang peran tertaut layanan, lihat Menggunakan peran terkait layanan untuk AWS WAF.

Untuk detail tentang kebijakan ini, lihat WAFV2 LoggingServiceRolePolicy di konsol IAM.

AWS WAF pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola AWS WAF sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman riwayat AWS WAF dokumen di. Riwayat dokumen

Kebijakan	Deskripsi perubahan	Tanggal
`WAFV2LoggingServiceRolePolicy` Kebijakan ini memungkinkan AWS WAF untuk menulis log ke Amazon Data Firehose. Ini hanya digunakan jika Anda mengaktifkan logging.	Menambahkan ID Pernyataan (Sids) ke setelan izin dalam peran terkait layanan yang dilampirkan kebijakan ini.	2024-06-03

Kebijakan	Deskripsi perubahan	Tanggal
Detail di konsol IAM: LoggingServiceRolePolicyWAFV2.		
`AWSServiceRoleForWAFV2Logging` Peran terkait layanan ini menyediakan kebijakan izin yang memungkinkan AWS WAF untuk menulis log ke Amazon Data Firehose. Detail di konsol IAM: AWSServiceRoleForWAFV2Logging.	Menambahkan ID Pernyataan (Sids) ke pengaturan izin.	2024-06-03
AWS WAF tambahan untuk mengubah pelacakan	AWS WAF mulai melacak perubahan untuk kebijakan terkelola `WAFV2LoggingServiceRolePolicy` dan peran terkait layanan. `AWSServiceRoleForWAFV2Logging`	2024-06-03
`AWSWAFFullAccess` Kebijakan ini memungkinkan AWS WAF untuk mengelola AWS sumber daya atas nama Anda di dalam AWS WAF dan dalam layanan terintegrasi. Detail di konsol IAM: AWSWAFFullAccess.	Izin yang diperluas untuk menambahkan instance Akses AWS Terverifikasi ke jenis sumber daya yang dapat Anda lindungi. AWS WAF	2023-06-17

Kebijakan	Deskripsi perubahan	Tanggal
`AWSWAFReadOnlyAccess` Kebijakan ini memungkinkan AWS WAF untuk mengelola AWS sumber daya atas nama Anda di dalam AWS WAF dan dalam layanan terintegrasi. Detail di konsol IAM: AWSWAFReadOnlyAccess.	Izin yang diperluas untuk menambahkan instance Akses AWS Terverifikasi ke jenis sumber daya yang dapat Anda lindungi. AWS WAF	2023-06-17
`AWSWAFConsoleFullAccess` Kebijakan ini memungkinkan AWS WAF untuk mengelola sumber daya AWS konsol dan AWS sumber daya lainnya atas nama Anda di dalam AWS WAF dan di layanan terintegrasi. Detail di konsol IAM: AWSWAFConsoleFullAccess.	Izin yang diperluas untuk menambahkan instance Akses AWS Terverifikasi ke jenis sumber daya yang dapat Anda lindungi. AWS WAF	2023-06-17

Kebijakan	Deskripsi perubahan	Tanggal
`AWSWAFConsoleReadOnlyAccess` Kebijakan ini memungkinkan AWS WAF untuk mengelola sumber daya AWS konsol dan AWS sumber daya lainnya atas nama Anda di dalam AWS WAF dan di layanan terintegrasi. Detail di konsol IAM: AWSWAFConsoleReadOnlyAccess.	Izin yang diperluas untuk menambahkan instance Akses AWS Terverifikasi ke jenis sumber daya yang dapat Anda lindungi. AWS WAF	2023-06-17
`AWSWAFFullAccess` Kebijakan ini memungkinkan AWS WAF untuk mengelola AWS sumber daya atas nama Anda di dalam AWS WAF dan dalam layanan terintegrasi. Detail di konsol IAM: AWSWAFFullAccess.	Izin yang diperluas untuk memperbaiki pengaturan akses untuk AWS App Runner layanan.	2023-06-06
`AWSWAFReadOnlyAccess` Kebijakan ini memungkinkan AWS WAF untuk mengelola AWS sumber daya atas nama Anda di dalam AWS WAF dan dalam layanan terintegrasi. Detail di konsol IAM: AWSWAFReadOnlyAccess.	Izin yang diperluas untuk memperbaiki pengaturan akses untuk AWS App Runner layanan.	2023-06-06

Kebijakan	Deskripsi perubahan	Tanggal
`AWSWAFConsoleFullAccess` Kebijakan ini memungkinkan AWS WAF untuk mengelola sumber daya AWS konsol dan AWS sumber daya lainnya atas nama Anda di dalam AWS WAF dan di layanan terintegrasi. Detail di konsol IAM: AWSWAFConsoleFullAccess.	Izin yang diperluas untuk memperbaiki pengaturan akses untuk AWS App Runner layanan.	2023-06-06
`AWSWAFConsoleReadOnlyAccess` Kebijakan ini memungkinkan AWS WAF untuk mengelola sumber daya AWS konsol dan AWS sumber daya lainnya atas nama Anda di dalam AWS WAF dan di layanan terintegrasi. Detail di konsol IAM: AWSWAFConsoleReadOnlyAccess.	Izin yang diperluas untuk memperbaiki pengaturan akses untuk AWS App Runner layanan.	2023-06-06

Kebijakan	Deskripsi perubahan	Tanggal
`AWSWAFFullAccess` Kebijakan ini memungkinkan AWS WAF untuk mengelola AWS sumber daya atas nama Anda di dalam AWS WAF dan dalam layanan terintegrasi. Detail di konsol IAM: AWSWAFFullAccess.	Izin yang diperluas untuk menambahkan AWS App Runner layanan ke jenis sumber daya yang dapat Anda lindungi. AWS WAF	2023-03-30
`AWSWAFReadOnlyAccess` Kebijakan ini memungkinkan AWS WAF untuk mengelola AWS sumber daya atas nama Anda di dalam AWS WAF dan dalam layanan terintegrasi. Detail di konsol IAM: AWSWAFReadOnlyAccess.	Izin yang diperluas untuk menambahkan AWS App Runner layanan ke jenis sumber daya yang dapat Anda lindungi. AWS WAF	2023-03-30
`AWSWAFConsoleFullAccess` Kebijakan ini memungkinkan AWS WAF untuk mengelola sumber daya AWS konsol dan AWS sumber daya lainnya atas nama Anda di dalam AWS WAF dan di layanan terintegrasi. Detail di konsol IAM: AWSWAFConsoleFullAccess.	Izin yang diperluas untuk menambahkan AWS App Runner layanan ke jenis sumber daya yang dapat Anda lindungi. AWS WAF	2023-03-30

Kebijakan	Deskripsi perubahan	Tanggal
`AWSWAFConsoleReadOnlyAccess` Kebijakan ini memungkinkan AWS WAF untuk mengelola sumber daya AWS konsol dan AWS sumber daya lainnya atas nama Anda di dalam AWS WAF dan di layanan terintegrasi. Detail di konsol IAM: AWSWAFConsoleReadOnlyAccess.	Izin yang diperluas untuk menambahkan AWS App Runner layanan ke jenis sumber daya yang dapat Anda lindungi. AWS WAF	2023-03-30
`AWSWAFFullAccess` Kebijakan ini memungkinkan AWS WAF untuk mengelola AWS sumber daya atas nama Anda di dalam AWS WAF dan dalam layanan terintegrasi. Detail di konsol IAM: AWSWAFFullAccess.	Izin yang diperluas untuk menambahkan kumpulan pengguna Amazon Cognito ke jenis sumber daya yang dapat Anda lindungi. AWS WAF	2022-08-25
`AWSWAFReadOnlyAccess` Kebijakan ini memungkinkan AWS WAF untuk mengelola AWS sumber daya atas nama Anda di dalam AWS WAF dan dalam layanan terintegrasi. Detail di konsol IAM: AWSWAFReadOnlyAccess.	Izin yang diperluas untuk menambahkan kumpulan pengguna Amazon Cognito ke jenis sumber daya yang dapat Anda lindungi. AWS WAF	2022-08-25

Kebijakan	Deskripsi perubahan	Tanggal
`AWSWAFConsoleFullAccess` Kebijakan ini memungkinkan AWS WAF untuk mengelola sumber daya AWS konsol dan AWS sumber daya lainnya atas nama Anda di dalam AWS WAF dan di layanan terintegrasi. Detail di konsol IAM: AWSWAFConsoleFullAccess.	Izin yang diperluas untuk menambahkan kumpulan pengguna Amazon Cognito ke jenis sumber daya yang dapat Anda lindungi. AWS WAF	2022-08-25
`AWSWAFConsoleReadOnlyAccess` Kebijakan ini memungkinkan AWS WAF untuk mengelola sumber daya AWS konsol dan AWS sumber daya lainnya atas nama Anda di dalam AWS WAF dan di layanan terintegrasi. Detail di konsol IAM: AWSWAFConsoleReadOnlyAccess.	Izin yang diperluas untuk menambahkan kumpulan pengguna Amazon Cognito ke jenis sumber daya yang dapat Anda lindungi. AWS WAF	2022-08-25

Kebijakan	Deskripsi perubahan	Tanggal
`AWSWAFFullAccess` Kebijakan ini memungkinkan AWS WAF untuk mengelola AWS sumber daya atas nama Anda di dalam AWS WAF dan dalam layanan terintegrasi. Detail di konsol IAM: AWSWAFFullAccess.	Memperbaiki pengaturan izin untuk pengiriman log untuk Amazon Simple Storage Service (Amazon S3) dan Amazon Logs. CloudWatc h Perubahan ini menyelesa ikan kesalahan akses ditolak yang terjadi selama konfigura si logging. Untuk informasi tentang mencatat lalu lintas ACL web Anda, lihatPencatata n AWS WAF lalu lintas ACL web.	2022-01-11
`AWSWAFConsoleFullA ccess` Kebijakan ini memungkinkan AWS WAF untuk mengelola sumber daya AWS konsol dan AWS sumber daya lainnya atas nama Anda di dalam AWS WAF dan di layanan terintegrasi. Detail di konsol IAM: AWSWAFConsoleFullAccess.	Memperbaiki pengaturan izin untuk pengiriman log untuk Amazon Simple Storage Service (Amazon S3) dan Amazon Logs. CloudWatch Perubahan ini menyelesaikan kesalahan akses yang terjadi selama konfigurasi logging. Untuk informasi tentang mencatat lalu lintas ACL web Anda, lihatPencatatan AWS WAF lalu lintas ACL web.	2022-01-11

Kebijakan	Deskripsi perubahan	Tanggal
`AWSWAFFullAccess` Kebijakan ini memungkinkan AWS WAF untuk mengelola AWS sumber daya atas nama Anda di dalam AWS WAF dan dalam layanan terintegrasi. Detail di konsol IAM: AWSWAFFullAccess.	Menambahkan izin baru untuk opsi logging diperluas. Perubahan ini memberikan AWS WAF akses ke tujuan pencatatan tambahan Amazon Simple Storage Service (Amazon S3) dan CloudWatch Amazon Logs. Untuk informasi tentang mencatat lalu lintas ACL web Anda, lihatPencatatan AWS WAF lalu lintas ACL web.	2021-11-15
`AWSWAFConsoleFullAccess` Kebijakan ini memungkinkan AWS WAF untuk mengelola sumber daya AWS konsol dan AWS sumber daya lainnya atas nama Anda di dalam AWS WAF dan di layanan terintegrasi. Detail di konsol IAM: AWSWAFConsoleFullAccess.	Menambahkan izin baru untuk opsi logging diperluas. Perubahan ini memberikan AWS WAF akses ke tujuan pencatatan tambahan Amazon Simple Storage Service (Amazon S3) dan CloudWatch Amazon Logs. Untuk informasi tentang mencatat lalu lintas ACL web Anda, lihatPencatatan AWS WAF lalu lintas ACL web.	2021-11-15
AWS WAF mulai melacak perubahan	AWS WAF mulai melacak perubahan untuk kebijakan yang AWS dikelola.	2021-3-01

Memecahkan masalah AWS WAF identitas dan akses

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan AWS WAF dan IAM.

Topik

Saya tidak berwenang untuk melakukan tindakan di AWS WAF

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya *`my-example-widget`* rekaan, tetapi tidak memiliki izin `wafv2:`*`GetWidget`* rekaan.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 wafv2:GetWidget on resource: my-example-widget
```

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya *`my-example-widget`* dengan menggunakan tindakan `wafv2:`*`GetWidget`*.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan yang tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran AWS WAF.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol tersebut untuk melakukan tindakan di AWS WAF. Namun, tindakan tersebut memerlukan

layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses AWS WAF sumber daya saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mempelajari apakah AWS WAF mendukung fitur-fitur ini, lihatBagaimana AWS WAF bekerja dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

Menggunakan peran terkait layanan untuk AWS WAF

AWS WAF menggunakan AWS Identity and Access Management peran terkait layanan (IAM). Peran terkait layanan adalah jenis unik peran IAM yang ditautkan langsung ke. AWS WAF Peran terkait layanan telah ditentukan sebelumnya oleh AWS WAF dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan AWS WAF lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. AWS WAF mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya AWS WAF dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin. Kebijakan izin tersebut tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran terkait layanan hanya setelah terlebih dahulu menghapus sumber daya terkait peran tersebut. Ini melindungi AWS WAF sumber daya Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat Layanan AWS yang bisa digunakan dengan IAM dan carilah layanan yang memiliki opsi Ya di kolom Peran Terkait Layanan. Pilih Ya bersama tautan untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

Izin peran terkait layanan untuk AWS WAF

AWS WAF menggunakan peran terkait layanan `AWSServiceRoleForWAFV2Logging` untuk menulis log ke Amazon Data Firehose. Peran ini hanya digunakan jika Anda mengaktifkan login AWS WAF. Untuk informasi tentang pencatatan, lihatPencatatan AWS WAF lalu lintas ACL web.

Peran terkait layanan ini dilampirkan pada kebijakan AWS terkelola. `WAFV2LoggingServiceRolePolicy` Untuk informasi selengkapnya tentang kebijakan terkelola, lihat AWS kebijakan terkelola: WAFV2 LoggingServiceRolePolicy.

Peran terkait layanan `AWSServiceRoleForWAFV2Logging` memercayai layanan `wafv2.amazonaws.com` untuk menjalankan peran.

Kebijakan izin peran memungkinkan AWS WAF untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan Amazon Data Firehose: `PutRecord` dan pada sumber daya aliran data `PutRecordBatch` Firehose dengan nama yang dimulai dengan. `aws-waf-logs-` Misalnya, `aws-waf-logs-us-east-2-analytics`.

- AWS Organizations tindakan: `DescribeOrganization` pada sumber daya organisasi Organisasi.

Lihat peran lengkap terkait layanan di konsol IAM:. AWSServiceRoleForWAFV2Logging

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, silakan lihat Izin Peran Tertaut Layanan di Panduan Pengguna IAM.

Membuat peran yang terhubung dengan layanan untuk AWS WAF

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda mengaktifkan AWS WAF login AWS Management Console, atau Anda membuat `PutLoggingConfiguration` permintaan di AWS WAF CLI atau AWS WAF API, AWS WAF membuat peran terkait layanan untuk Anda.

Anda harus memiliki `iam:CreateServiceLinkedRole` izin untuk mengaktifkan logging.

Jika Anda menghapus peran tertaut layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Saat Anda mengaktifkan AWS WAF pencatatan, AWS WAF buat peran terkait layanan untuk Anda lagi.

Mengedit peran terkait layanan untuk AWS WAF

AWS WAF tidak memungkinkan Anda untuk mengedit peran `AWSServiceRoleForWAFV2Logging` terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat menyunting penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit Peran Tertaut Layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk AWS WAF

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran tertaut layanan, kami menyarankan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Tetapi, Anda harus membersihkan sumber daya peran yang terhubung dengan layanan sebelum menghapusnya secara manual.

> **Note**
>
> Jika AWS WAF layanan menggunakan peran saat Anda mencoba menghapus sumber daya, maka penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus AWS WAF sumber daya yang digunakan oleh **`AWSServiceRoleForWAFV2Logging`**

1. Di AWS WAF konsol, hapus logging dari setiap ACL web. Untuk informasi selengkapnya, lihat Pencatatan AWS WAF lalu lintas ACL web.
2. Menggunakan API atau CLI, kirimkan `DeleteLoggingConfiguration` permintaan untuk setiap ACL web yang telah mengaktifkan logging. Untuk informasi lebih lanjut, lihat Referensi API AWS WAF.

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, CLI IAM, atau API CLI untuk menghapus peran tertaut layanan `AWSServiceRoleForWAFV2Logging`. Untuk informasi selengkapnya, lihat Menghapus Peran Terkait Layanan di Panduan Pengguna IAM.

Wilayah yang didukung untuk peran yang terhubung dengan layanan AWS WAF

AWS WAF mendukung penggunaan peran terkait layanan di semua wilayah tempat layanan tersedia. Untuk informasi lebih lanjut, lihat AWS WAF kuota dan titik akhir.

Penebangan dan pemantauan di AWS WAF

Pemantauan adalah bagian penting dari menjaga keandalan, ketersediaan, dan kinerja AWS WAF dan AWS solusi Anda. Anda harus mengumpulkan data pemantauan dari semua bagian AWS solusi Anda sehingga Anda dapat lebih mudah men-debug kegagalan multi-titik jika terjadi. AWS menyediakan beberapa alat untuk memantau AWS WAF sumber daya Anda dan menanggapi peristiwa potensial:

CloudWatch Alarm Amazon

Menggunakan CloudWatch alarm, Anda menonton satu metrik selama periode waktu yang Anda tentukan. Jika metrik melebihi ambang batas tertentu, CloudWatch kirimkan pemberitahuan ke topik atau AWS Auto Scaling kebijakan Amazon SNS. Untuk informasi selengkapnya, lihat Pemantauan CloudWatch dengan Amazon.

AWS CloudTrail log

CloudTrail menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di AWS WAF. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat AWS WAF, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan. Untuk informasi selengkapnya, lihat Logging panggilan API dengan AWS CloudTrail.

AWS WAF pencatatan lalu lintas ACL web

AWS WAF menawarkan pencatatan untuk lalu lintas yang dianalisis oleh ACL web Anda. Log mencakup informasi seperti waktu AWS WAF menerima permintaan dari AWS sumber daya Anda yang dilindungi, informasi terperinci tentang permintaan, dan pengaturan tindakan untuk aturan yang cocok dengan permintaan tersebut. Untuk informasi selengkapnya, lihat Pencatatan AWS WAF lalu lintas ACL web.

Validasi kepatuhan untuk AWS WAF

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar AWS yang berfokus pada keamanan dan kepatuhan.
- Arsitektur untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi yang memenuhi syarat HIPAA.

  > **Note**
  >
  > Tidak semua memenuhi Layanan AWS syarat HIPAA. Untuk informasi selengkapnya, lihat Referensi Layanan yang Memenuhi Syarat HIPAA.

- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber

daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.

- Amazon GuardDuty — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas yang mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan di AWS WAF

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang dan mengoperasikan aplikasi dan basis data yang melakukan secara otomatis pinda saat gagal/failover di antara zona-zona tanpa terputus. Zona Ketersediaan lebih sangat tersedia, lebih toleran kesalahan, dan lebih dapat diskalakan daripadai infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur AWS Global.

Keamanan infrastruktur dalam AWS WAF

Sebagai layanan terkelola, AWS WAF dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses AWS WAF melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani dengan menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan pengguna utama IAM. Atau Anda bisa menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

AWS WAF kuota

> **Note**
>
> Ini adalah versi terbaru dari AWS WAF. Untuk AWS WAF Klasik, lihatAWS WAF Klasik.

AWS WAF tunduk pada kuota berikut (sebelumnya disebut sebagai batas). Kuota ini sama untuk semua Wilayah yang AWS WAF tersedia. Setiap Wilayah tunduk pada kuota ini secara individual. Kuota tidak kumulatif di seluruh Wilayah.

AWS WAF memiliki kuota default pada jumlah maksimum entitas yang dapat Anda miliki per akun. Anda dapat meminta peningkatan kuota ini.

Sumber daya	Kuota default per akun per Wilayah
Jumlah maksimum ACL web	100
Jumlah maksimum kelompok aturan	100
Jumlah maksimum set IP	100
Jumlah maksimum permintaan per detik per web ACL	25.000
Jumlah maksimum header permintaan kustom per ACL web atau grup aturan	100
Jumlah maksimum header respons kustom per ACL web atau grup aturan	100
Jumlah maksimum badan respons kustom per ACL web atau grup aturan	50
Jumlah maksimum domain token dalam daftar domain token ACL web	10

Permintaan maksimum per detik (RPS) yang diizinkan untuk AWS WAF CloudFront aktif diatur oleh CloudFront dan dijelaskan dalam Panduan CloudFront Pengembang.

AWS WAF memiliki kuota tetap pada pengaturan entitas berikut per akun per Wilayah. Kuota-kuota ini tidak dapat diubah.

Sumber daya	Kuota per akun per Wilayah
Unit kapasitas ACL web maksimum (WCU) per ACL web*	5.000
WCU maksimum per grup aturan	5.000
Jumlah maksimum pernyataan referensi per kelompok aturan. Dalam kelompok aturan, pernyataan referensi dapat mereferensikan set IP atau set pola regex.	50
Jumlah maksimum pernyataan referensi per web ACL. Dalam ACL web, pernyataan referensi dapat mereferensikan grup aturan, kumpulan IP, atau kumpulan pola regex.	50
Jumlah maksimum alamat IP dalam notasi CIDR per set IP	10.000
Jumlah maksimum aturan berbasis tarif per web ACL	10
Jumlah maksimum aturan berbasis tarif per kelompok aturan	4
Tingkat permintaan minimum yang dapat ditentukan untuk aturan berbasis tarif	100
Jumlah maksimum alamat IP unik yang dapat dibatasi tarif per aturan berbasis tarif	10.000
Jumlah maksimum karakter dalam pernyataan kecocokan string	200
Jumlah maksimum karakter dalam setiap pola regex	200
Jumlah maksimum pola regex unik per set regex	10
Jumlah maksimum set regex	10
Ukuran maksimum badan permintaan web yang dapat diperiksa untuk Application Load AWS AppSync Balancer dan proteksi	8 KB

Sumber daya	Kuota per akun per Wilayah
Ukuran maksimum badan permintaan web yang dapat diperiksa CloudFront, API Gateway, Amazon Cognito, App Runner, dan perlindungan Akses Terverifikasi**	64 KB
Jumlah maksimum transformasi teks per pernyataan aturan	10
Ukuran maksimum konten badan respons khusus untuk satu definisi respons khusus	4 KB
Jumlah maksimum header kustom untuk satu definisi respons kustom	10
Jumlah maksimum header kustom untuk satu definisi permintaan kustom	10
Ukuran gabungan maksimum dari semua konten badan respons untuk grup aturan tunggal atau ACL web tunggal	50 KB

* Menggunakan lebih dari 1.500 WCU dalam ACL web menimbulkan biaya di luar harga ACL web dasar. Untuk informasi selengkapnya, lihat AWS WAF unit kapasitas ACL web (WCU) dan Harga AWS WAF.

** Secara default, batas pemeriksaan badan diatur ke 16 KB untukCloudFront, API Gateway, Amazon Cognito, App Runner, dan sumber daya Akses Terverifikasi, tetapi Anda dapat meningkatkannya untuk salah satu sumber daya ini dalam konfigurasi ACL web Anda, hingga maksimum yang tercantum. Untuk informasi selengkapnya, lihat Mengelola batas ukuran inspeksi tubuh.

AWS WAF memiliki kuota tetap berikut pada panggilan per akun per Wilayah. Kuota ini berlaku untuk total panggilan ke layanan melalui cara apa pun yang tersedia, termasuk konsol, CLI, REST API AWS CloudFormation, dan SDK. Kuota-kuota ini tidak dapat diubah.

Jenis panggilan	Kuota per akun per Wilayah
Jumlah maksimum panggilan ke `AssociateWebACL`	Satu permintaan setiap 2 detik

Jenis panggilan	Kuota per akun per Wilayah
Jumlah maksimum panggilan ke `DisassociateWebACL`	Satu permintaan setiap 2 detik
Jumlah maksimum panggilan ke `GetWebACLForResource`	Satu permintaan per detik
Jumlah maksimum panggilan ke `ListResourcesForWebACL`	Satu permintaan per detik
Jumlah maksimum panggilan ke individu `Get` atau `List` tindakan mana pun, jika tidak ada kuota lain yang ditentukan untuk itu	Lima permintaan per detik
Jumlah maksimum panggilan ke individu`Create`,, atau `Update` tindakan`Put`, jika tidak ada kuota lain yang ditentukan untuk itu	Satu permintaan per detik

Memigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF

Bagian ini memberikan panduan untuk memigrasikan aturan dan ACL web Anda dari AWS WAF Classic ke. AWS WAF AWS WAF dirilis pada November 2019. Jika Anda membuat sumber daya seperti aturan dan ACL web menggunakan AWS WAF Classic, Anda harus bekerja dengannya menggunakan AWS WAF Classic atau memigrasikannya ke versi terbaru ini.

Sebelum Anda memulai pekerjaan migrasi Anda, biasakan diri Anda AWS WAF dengan membacaAWS WAF.

Topik

- Mengapa bermigrasi ke AWS WAF?
- Cara kerja migrasi
- Peringatan dan batasan migrasi
- Migrasi ACL web dari Classic ke AWS WAFAWS WAF

Mengapa bermigrasi ke AWS WAF?

Versi terbaru AWS WAF menyediakan banyak perbaikan dibandingkan versi sebelumnya, sambil mempertahankan sebagian besar konsep dan terminologi yang biasa Anda gunakan.

Daftar berikut menjelaskan perubahan besar yang terbaru AWS WAF. Sebelum melanjutkan migrasi, luangkan waktu untuk meninjau daftar ini dan membiasakan diri dengan AWS WAF panduan lainnya.

- AWS Aturan Terkelola untuk AWS WAF — Grup aturan yang sekarang tersedia melalui Aturan AWS Terkelola memberikan perlindungan terhadap ancaman web umum. Sebagian besar kelompok aturan ini disertakan secara gratis AWS WAF. Untuk informasi selengkapnya, lihat AWS Daftar grup aturan Aturan Terkelola dan posting blog Mengumumkan Aturan AWS Terkelola untuk AWS WAF.
- AWS WAF API baru — API baru memungkinkan Anda mengonfigurasi semua AWS WAF sumber daya menggunakan satu set API. Untuk membedakan antara aplikasi regional dan global, API baru menyertakan `scope` pengaturan. Untuk informasi selengkapnya tentang API, lihat Tindakan AWS WAFV2 dan Jenis Data AWS WAFV2.

  Dalam API, SDK, CLI, dan AWS CloudFormation, AWS WAF Classic mempertahankan skema penamaannya dan versi terbaru ini AWS WAF disebut dengan tambahan `V2` atau`v2`, tergantung pada konteksnya.
- Kuota layanan yang disederhanakan (batas) - AWS WAF sekarang memungkinkan lebih banyak aturan per ACL web dan memungkinkan Anda untuk mengekspresikan pola regex yang lebih panjang. Untuk informasi selengkapnya, lihat AWS WAF kuota.
- Batas ACL web sekarang didasarkan pada kebutuhan komputasi — batas ACL Web sekarang didasarkan pada unit kapasitas ACL web (WCU). AWS WAF menghitung WCU untuk aturan sesuai dengan kapasitas operasi yang diperlukan untuk menjalankan aturan. WCU dari ACL web adalah jumlah dari WCU dari semua aturan dan kelompok aturan di ACL web.

  Untuk informasi umum tentang WCU, lihatBagaimana cara AWS WAF kerja. Untuk informasi tentang penggunaan WCU setiap aturan, lihatDasar-dasar pernyataan aturan.
- Penulisan aturan berbasis dokumen — Anda sekarang dapat menulis dan mengekspresikan aturan, grup aturan, dan ACL web dalam format JSON. Anda tidak perlu lagi menggunakan panggilan API individual untuk membuat kondisi yang berbeda dan kemudian mengaitkan kondisi dengan aturan. Ini sangat menyederhanakan cara Anda menulis dan memelihara kode Anda. Anda dapat mengakses format JSON ACL web Anda melalui konsol saat Anda melihat ACL web, dengan

memilih Unduh web ACL sebagai JSON. Ketika Anda membuat aturan Anda sendiri, Anda dapat mengakses representasi JSON dengan memilih Rule JSON editor.

- Rule nesting dan dukungan operasi logis penuh — Anda dapat menulis aturan gabungan yang kompleks dengan menggunakan pernyataan aturan logis dan dengan menggunakan nesting. Anda dapat membuat pernyataan seperti`[A AND NOT(B OR C)]`. Untuk informasi selengkapnya, lihat Pernyataan aturan logis.
- Aturan berbasis tarif yang ditingkatkan — Dalam versi terbaru AWS WAF, Anda dapat menyesuaikan jendela waktu yang dievaluasi aturan dan bagaimana aturan mengumpulkan permintaan. Anda dapat menyesuaikan agregasi menggunakan kombinasi sejumlah karakteristik permintaan web. Selain itu aturan berbasis tarif terbaru bereaksi lebih cepat terhadap perubahan lalu lintas. Untuk informasi selengkapnya, lihat Pernyataan aturan berbasis tarif.
- Dukungan rentang CIDR variabel untuk set IP - spesifikasi set IP sekarang memiliki lebih banyak fleksibilitas dalam rentang IP. Untuk IPv4, AWS WAF mendukung `/1` untuk. `/32` Untuk IPv6, AWS WAF mendukung `/1` untuk. `/128` Untuk informasi selengkapnya tentang set IP, lihatPernyataan aturan kecocokan set IP.
- Transformasi teks berantai — AWS WAF dapat melakukan beberapa transformasi teks terhadap konten permintaan web sebelum memeriksanya. Untuk informasi selengkapnya, lihat Opsi transformasi teks.
- Pengalaman konsol yang ditingkatkan — AWS WAF Konsol baru ini menampilkan pembuat aturan visual dan desain konsol yang lebih intuitif pengguna.
- Opsi yang diperluas untuk AWS WAF kebijakan Firewall Manager — Dalam pengelolaan Firewall Manager untuk ACL AWS WAF web, Anda sekarang dapat membuat satu set grup aturan yang AWS WAF memproses terlebih dahulu dan satu set grup aturan yang AWS WAF memproses terakhir. Setelah menerapkan AWS WAF kebijakan, pemilik akun lokal dapat menambahkan grup aturan mereka sendiri yang AWS WAF memproses di antara dua set ini. Untuk informasi selengkapnya tentang AWS WAF kebijakan Firewall Manager, lihatAWS WAF kebijakan.
- AWS CloudFormation dukungan untuk semua jenis pernyataan aturan — AWS WAF in AWS CloudFormation mendukung semua jenis pernyataan aturan yang didukung AWS WAF konsol dan API. Selain itu, Anda dapat dengan mudah mengonversi aturan yang Anda tulis dalam format JSON ke format YAMAL.

Cara kerja migrasi

Migrasi otomatis membawa sebagian besar konfigurasi ACL web AWS WAF Klasik Anda, meninggalkan beberapa hal yang perlu Anda tangani secara manual.

Berikut ini mencantumkan langkah-langkah tingkat tinggi untuk memigrasikan ACL web.

1. Migrasi otomatis membaca semua yang terkait dengan ACL web Anda yang ada, tanpa memodifikasi atau menghapus apa pun di Classic. AWS WAF Ini menciptakan representasi dari ACL web dan sumber daya terkait, kompatibel dengan AWS WAF. Ini menghasilkan AWS CloudFormation template untuk ACL web baru dan menyimpannya di ember Amazon S3.
2. Anda menyebarkan template ke dalam AWS CloudFormation, untuk membuat ulang ACL web dan sumber daya terkait di. AWS WAF
3. Anda meninjau ACL web, dan menyelesaikan migrasi secara manual, memastikan bahwa ACL web baru Anda memanfaatkan sepenuhnya kemampuan yang terbaru. AWS WAF
4. Anda secara manual mengalihkan sumber daya yang dilindungi ke ACL web baru.

Peringatan dan batasan migrasi

Migrasi tidak membawa semua pengaturan Anda, persis seperti yang Anda miliki di AWS WAF Classic. Beberapa hal, seperti aturan terkelola, tidak memetakan persis di antara dua versi. Pengaturan lain, seperti asosiasi ACL web dengan AWS sumber daya yang dilindungi, awalnya dinonaktifkan di versi baru sehingga Anda dapat menambahkannya saat Anda siap.

Daftar berikut menjelaskan peringatan migrasi dan menjelaskan langkah apa pun yang mungkin ingin Anda ambil sebagai tanggapan. Gunakan ikhtisar ini untuk merencanakan migrasi Anda. Langkah-langkah migrasi terperinci, nanti, memandu Anda melalui langkah-langkah mitigasi yang direkomendasikan.

- Akun tunggal — Anda hanya dapat memigrasikan sumber daya AWS WAF Klasik untuk akun apa pun ke AWS WAF sumber daya untuk akun yang sama.
- Aturan terkelola — Migrasi tidak membawa aturan terkelola apa pun dari AWS Marketplace penjual. Beberapa AWS Marketplace penjual memiliki aturan terkelola AWS WAF yang setara untuk Anda dapat berlangganan lagi. Sebelum Anda melakukannya, tinjau Aturan AWS Terkelola yang disediakan dengan versi terbaru AWS WAF. Sebagian besar gratis untuk AWS WAF pengguna. Untuk informasi tentang aturan terkelola, lihatGrup aturan terkelola.

- Asosiasi ACL Web — Migrasi tidak membawa asosiasi apa pun antara ACL web dan sumber daya yang dilindungi. Ini adalah desain, untuk menghindari mempengaruhi beban kerja produksi Anda. Setelah Anda memverifikasi bahwa semuanya dimigrasikan dengan benar, kaitkan ACL web baru dengan sumber daya Anda.
- Logging — Logging untuk ACL web yang dimigrasi dinonaktifkan secara default. Ini dengan desain. Aktifkan logging saat Anda siap untuk beralih dari AWS WAF Classic ke AWS WAF.
- AWS Firewall Manager grup aturan — Migrasi tidak menangani grup aturan yang dikelola oleh Firewall Manager. Anda dapat memigrasikan ACL web yang dikelola oleh Firewall Manager, tetapi migrasi tidak membawa grup aturan. Alih-alih menggunakan alat migrasi untuk ACL web ini, buat ulang kebijakan untuk yang baru AWS WAF di Firewall Manager.

  > **Note**
  >
  > Grup aturan yang dikelola Manajer Firewall untuk AWS WAF Classic adalah grup aturan Firewall Manager. Dengan versi baru AWS WAF, grup aturan adalah grup AWS WAF aturan. Secara fungsional, mereka sama.

- AWS WAF Otomatisasi Keamanan — Jangan mencoba memigrasi Otomasi AWS WAF Keamanan apa pun. Migrasi tidak mengonversi fungsi Lambda, yang mungkin digunakan oleh otomatisasi. Ketika solusi Otomasi AWS WAF Keamanan baru tersedia yang kompatibel dengan yang terbaru AWS WAF, terapkan kembali solusi itu.

Migrasi ACL web dari Classic ke AWS WAFAWS WAF

Untuk memigrasikan ACL web dan beralih ke ACL, lakukan migrasi otomatis, lalu selesaikan serangkaian langkah manual.

Topik

Migrasi ACL web: migrasi otomatis

Untuk secara otomatis memigrasikan konfigurasi ACL web dari Classic ke AWS WAFAWS WAF

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.
2. Pilih Beralih ke AWS WAF Klasik dan tinjau pengaturan konfigurasi Anda untuk ACL web. Catat pengaturan, dengan mempertimbangkan peringatan dan batasan yang dijelaskan di bagian sebelumnya,. Peringatan dan batasan migrasi
3. Dalam dialog informasi di bagian atas, cari kalimat yang dimulai dengan Migrasi ACL web dan pilih tautan ke wizard migrasi. Ini meluncurkan wizard migrasi.

   Jika Anda tidak melihat dialog informasi, Anda mungkin telah menutupnya sejak meluncurkan konsol AWS WAF Klasik. Di bilah navigasi, pilih Beralih ke baru AWS WAF lalu pilih Beralih ke AWS WAF Klasik, dan dialog informasi akan muncul kembali.
4. Pilih ACL web yang ingin Anda migrasikan.
5. Untuk konfigurasi Migrasi, sediakan bucket Amazon S3 yang akan digunakan untuk template. Anda memerlukan bucket Amazon S3 yang dikonfigurasi dengan benar untuk API migrasi, untuk menyimpan AWS CloudFormation template yang dihasilkannya.

   - Jika bucket dienkripsi, enkripsi harus menggunakan kunci Amazon S3 (SSE-S3). Migrasi tidak mendukung enkripsi dengan kunci AWS Key Management Service (SSE-KMS).
   - Nama bucket harus dimulai dengan`aws-waf-migration-`. Misalnya, `aws-waf-migration-my-web-acl`.
   - Bucket harus berada di Wilayah tempat Anda menerapkan template. Misalnya, untuk ACL web di`us-west-2`, Anda harus menggunakan bucket `us-west-2` Amazon S3 dan Anda harus menerapkan tumpukan templat. `us-west-2`
6. Untuk kebijakan bucket S3, sebaiknya pilih Auto apply kebijakan bucket yang diperlukan untuk migrasi. Atau, jika Anda ingin mengelola bucket sendiri, Anda harus menerapkan kebijakan bucket berikut secara manual:

   - Untuk CloudFront aplikasi Amazon global (`waf`):

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "apiv2migration.waf.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::<BUCKET_NAME>/AWSWAF/<CUSTOMER_ACCOUNT_ID>/
*"
        }
    ]
}
```

- Untuk aplikasi Amazon API Gateway atau Application Load Balancer regional ()`waf-regional`:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "apiv2migration.waf-regional.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::<BUCKET_NAME>/AWSWAF/<CUSTOMER_ACCOUNT_ID>/
*"
        }
    ]
}
```

7. Untuk Pilih cara menangani aturan yang tidak dapat dimigrasi, pilih salah satu untuk mengecualikan aturan yang tidak dapat dimigrasi, atau untuk menghentikan migrasi. Untuk informasi tentang aturan yang tidak dapat dimigrasikan, lihatPeringatan dan batasan migrasi.
8. Pilih Berikutnya.
9. Untuk Buat AWS CloudFormation templat, verifikasi pengaturan Anda, lalu pilih Mulai membuat AWS CloudFormation templat untuk memulai proses migrasi. Ini bisa memakan waktu beberapa menit, tergantung pada kompleksitas ACL web Anda.
10. Di Buat dan jalankan AWS CloudFormation tumpukan untuk menyelesaikan migrasi, Anda dapat memilih untuk pergi ke AWS CloudFormation konsol untuk membuat tumpukan dari template,

untuk membuat ACL web baru dan sumber dayanya. Untuk melakukan ini, pilih Buat AWS CloudFormation tumpukan.

Setelah proses migrasi otomatis selesai, Anda siap untuk melanjutkan ke langkah-langkah tindak lanjut manual. Lihat Migrasi ACL web: tindak lanjut manual.

Migrasi ACL web: tindak lanjut manual

Setelah migrasi otomatis selesai, tinjau ACL web yang baru dibuat dan isi komponen yang tidak dibawa migrasi untuk Anda. Prosedur berikut mencakup aspek manajemen ACL web yang tidak ditangani oleh migrasi. Untuk daftarnya, lihatPeringatan dan batasan migrasi.

Untuk menyelesaikan migrasi dasar - langkah manual

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.
2. Konsol harus secara otomatis menggunakan versi terbaru AWS WAF. Untuk memverifikasi ini, di panel navigasi, periksa apakah Anda dapat melihat opsi Beralih ke AWS WAF Klasik. Jika Anda melihat Beralih ke baru AWS WAF, pilih yang untuk beralih ke versi terbaru.
3. Di panel navigasi, pilih Web ACL.
4. Di halaman Web ACL, cari ACL web baru Anda dalam daftar untuk Wilayah tempat Anda membuatnya. Pilih nama ACL web untuk memunculkan pengaturan untuk ACL web.
5. Tinjau semua pengaturan untuk ACL web baru terhadap ACL web AWS WAF Klasik Anda sebelumnya. Secara default, pencatatan dan asosiasi sumber daya yang dilindungi dinonaktifkan. Anda mengaktifkannya saat Anda siap untuk beralih.
6. Jika ACL web AWS WAF Classic Anda memiliki aturan berbasis tarif dengan kondisi, kondisi tersebut tidak dibawa dalam migrasi. Anda dapat menambahkan kondisi ke aturan di ACL web baru.

    a. Di halaman pengaturan ACL web Anda, pilih tab Aturan.

    b. Temukan aturan berbasis tarif Anda dalam daftar, pilih, dan pilih Edit.

    c. Agar Kriteria menghitung permintaan terhadap batas tarif, pilih Hanya mempertimbangkan permintaan yang sesuai dengan kriteria dalam pernyataan aturan, lalu berikan kriteria tambahan Anda. Anda dapat menambahkan kriteria menggunakan pernyataan aturan apa pun yang dapat disarangkan, termasuk pernyataan logis. Untuk informasi tentang pilihan Anda, lihatPernyataan aturan berbasis tarif.

7. Jika ACL web AWS WAF Classic Anda memiliki grup aturan terkelola, penyertaan grup aturan tidak dibawa dalam migrasi. Anda dapat menambahkan grup aturan terkelola ke ACL web baru. Tinjau informasi tentang grup aturan AWS terkelola, termasuk daftar Aturan Terkelola yang tersedia dengan versi baru AWS WAF, atGrup aturan terkelola. Untuk menambahkan grup aturan terkelola, lakukan hal berikut:

   a. Di halaman pengaturan ACL web Anda, pilih tab Aturan ACL web.

   b. Pilih Tambahkan aturan, lalu pilih Tambahkan grup aturan terkelola.

   c. Perluas daftar untuk vendor pilihan Anda dan pilih grup aturan yang ingin Anda tambahkan. Untuk AWS Marketplace penjual, Anda mungkin perlu berlangganan grup aturan. Untuk informasi selengkapnya tentang menggunakan grup aturan terkelola di ACL web Anda, lihat Grup aturan terkelola danEvaluasi aturan dan kelompok aturan ACL Web.

Setelah Anda menyelesaikan proses migrasi dasar, kami sarankan Anda meninjau kebutuhan Anda dan mempertimbangkan opsi tambahan, untuk memastikan bahwa konfigurasi baru seefisien mungkin dan menggunakan opsi keamanan terbaru yang tersedia. Lihat Migrasi ACL web: pertimbangan tambahan.

Migrasi ACL web: pertimbangan tambahan

Tinjau ACL web baru Anda dan pertimbangkan opsi yang tersedia untuk Anda di yang baru AWS WAF untuk memastikan bahwa konfigurasinya seefisien mungkin dan menggunakan opsi keamanan terbaru yang tersedia.

Aturan AWS Terkelola Tambahan

Pertimbangkan untuk menerapkan Aturan AWS Terkelola tambahan di ACL web Anda untuk meningkatkan postur keamanan aplikasi Anda. Ini termasuk tanpa AWS WAF biaya tambahan. AWS Aturan Terkelola menampilkan jenis grup aturan berikut:

- Grup aturan dasar memberikan perlindungan umum terhadap berbagai ancaman umum, seperti menghentikan input buruk yang diketahui agar tidak masuk ke aplikasi Anda dan mencegah akses halaman admin.
- Kelompok aturan khusus kasus penggunaan memberikan perlindungan tambahan untuk banyak kasus penggunaan dan lingkungan yang beragam.
- Daftar reputasi IP memberikan intelijen ancaman berdasarkan IP sumber klien.

Untuk informasi selengkapnya, lihat AWS Aturan Terkelola untuk AWS WAF.

Pengoptimalan aturan dan pembersihan

Kunjungi kembali aturan lama Anda dan pertimbangkan untuk mengoptimalkannya dengan menulis ulang atau menghapus yang sudah ketinggalan zaman. Misalnya, jika di masa lalu, Anda menggunakan AWS CloudFormation template dari paper teknis untuk 10 Kerentanan Aplikasi Web Teratas OWASP, Mempersiapkan 10 Kerentanan Aplikasi Web Teratas OWASP AWS WAF dan Buku Putih Baru Kami, Anda harus mempertimbangkan untuk menggantinya dengan Aturan Terkelola. AWS Meskipun konsep yang ditemukan dalam dokumen masih berlaku dan dapat membantu Anda dalam menulis aturan Anda sendiri, aturan yang dibuat oleh template sebagian besar telah digantikan oleh Aturan AWS Terkelola.

CloudWatch Metrik dan alarm Amazon

Kunjungi kembali CloudWatch metrik Amazon Anda dan atur alarm sesuai kebutuhan. Migrasi tidak membawa CloudWatch alarm dan mungkin saja nama metrik Anda tidak seperti yang Anda inginkan.

Tinjau dengan tim aplikasi Anda

Bekerja dengan tim aplikasi Anda dan periksa postur keamanan Anda. Cari tahu bidang apa yang sering diuraikan oleh aplikasi dan tambahkan aturan untuk membersihkan input yang sesuai. Periksa kasus tepi dan tambahkan aturan untuk menangkap kasus ini jika logika bisnis aplikasi gagal memprosesnya.

Rencanakan peralihan

Rencanakan waktu sakelar dengan tim aplikasi Anda. Peralihan dari asosiasi ACL web lama ke yang baru dapat mengambil sedikit waktu untuk menyebar ke semua area di mana sumber daya Anda disimpan. Waktu propagasi bisa dari beberapa detik hingga beberapa menit. Selama waktu ini, beberapa permintaan akan diproses oleh ACL web lama dan lainnya akan diproses oleh ACL web baru. Sumber daya Anda akan dilindungi di seluruh sakelar, tetapi Anda mungkin melihat ketidakkonsistenan dalam penanganan permintaan saat sakelar sedang berlangsung.

Ketika Anda siap untuk beralih, ikuti prosedur diMigrasi ACL web: switchover.

Migrasi ACL web: switchover

Setelah Anda memverifikasi pengaturan ACL web baru Anda, Anda dapat mulai menggunakannya sebagai pengganti ACL web AWS WAF Klasik Anda.

Untuk mulai menggunakan ACL AWS WAF web baru Anda

1. Kaitkan ACL AWS WAF web dengan sumber daya yang ingin Anda lindungi, ikuti panduan diMengaitkan atau memisahkan ACL web dengan sumber daya AWS. Ini secara otomatis memisahkan sumber daya dari ACL web lama.

   Sakelar dapat memakan waktu dari beberapa detik hingga beberapa menit untuk merambat. Selama waktu ini, beberapa permintaan mungkin diproses oleh ACL web lama dan lainnya oleh ACL web baru. Sumber daya Anda akan dilindungi di seluruh sakelar, tetapi Anda mungkin melihat ketidakkonsistenan dalam penanganan permintaan hingga selesai.
2. Konfigurasikan logging untuk ACL web baru, mengikuti panduan diPencatatan AWS WAF lalu lintas ACL web.
3. (Opsional) Jika ACL web AWS WAF Klasik Anda tidak lagi terkait dengan sumber daya apa pun, pertimbangkan untuk menghapusnya sepenuhnya dari AWS WAF Klasik. Untuk informasi, lihat Menghapus ACL Web.

AWS WAF Klasik

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

AWS WAF Classic adalah firewall aplikasi web yang memungkinkan Anda memantau permintaan HTTP dan HTTPS yang diteruskan ke API Amazon API Gateway, Amazon, CloudFront atau Application Load Balancer. AWS WAF Classic juga memungkinkan Anda mengontrol akses ke konten Anda. Berdasarkan kondisi yang Anda tentukan, seperti alamat IP tempat permintaan berasal atau nilai string kueri, API Gateway, CloudFront atau Application Load Balancer merespons permintaan baik dengan konten yang diminta atau dengan kode status HTTP 403 (Terlarang). Anda juga dapat mengonfigurasi CloudFront untuk mengembalikan halaman kesalahan kustom saat permintaan diblokir.

Topik

Menyiapkan AWS WAF Klasik

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Topik ini menjelaskan langkah-langkah awal, seperti membuat akun pengguna, untuk mempersiapkan Anda menggunakan AWS WAF Classic. Anda tidak dikenakan biaya untuk ini. Anda hanya dikenakan biaya untuk AWS layanan yang Anda gunakan.

> **Note**
>
> Jika Anda pengguna baru AWS WAF, jangan ikuti langkah-langkah penyiapan ini untuk AWS WAF Classic. Sebagai gantinya, ikuti langkah-langkah untuk versi terbaru AWS WAF, atMenyiapkan akun Anda untuk menggunakan layanan.

Setelah Anda menyelesaikan langkah-langkah ini, lihat Memulai dengan AWS WAF Classic untuk melanjutkan memulai dengan AWS WAF Classic.

> **Note**
>
> AWS Shield Standard disertakan dengan AWS WAF Klasik dan tidak memerlukan pengaturan tambahan. Untuk informasi selengkapnya, lihat Bagaimana AWS Shield dan Shield Advanced bekerja.

Sebelum Anda menggunakan AWS WAF Klasik atau AWS Shield Advanced untuk pertama kalinya, selesaikan langkah-langkah di bagian ini.

Topik

- Mendaftar untuk Akun AWS

- Buat pengguna dengan akses administratif
- Unduh alat

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/signup.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan mengunjungi https://aws.amazon.com/ dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

   Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.
2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .
2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

  Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuknya, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.
2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

Unduh alat

AWS Management Console Termasuk konsol untuk AWS WAF Klasik, tetapi jika Anda ingin mengakses AWS WAF Classic secara terprogram, lihat berikut ini:

- Jika Anda ingin memanggil AWS WAF Classic API tanpa harus menangani detail tingkat rendah seperti merakit permintaan HTTP mentah, Anda dapat menggunakan SDK. AWS AWS SDK menyediakan fungsi dan tipe data yang merangkum fungsionalitas AWS WAF Classic dan layanan lainnya. AWS Untuk mengunduh AWS SDK, lihat halaman yang berlaku, yang juga mencakup prasyarat dan petunjuk pemasangan:
  - Java
  - JavaScript
  - .NET
  - Node.js
  - PHP
  - Python
  - Ruby

  Untuk daftar lengkap AWS SDK, lihat Alat untuk Amazon Web Services.
- Jika Anda menggunakan bahasa pemrograman yang AWS tidak menyediakan SDK, Referensi AWS WAF API mendokumentasikan operasi yang didukung AWS WAF Classic.
- The AWS Command Line Interface (AWS CLI) mendukung AWS WAF Klasik. Ini AWS CLI memungkinkan Anda mengontrol beberapa AWS layanan dari baris perintah dan mengotomatiskannya melalui skrip. Untuk informasi selengkapnya, lihat AWS Command Line Interface.
- AWS Tools for Windows PowerShell mendukung AWS WAF Klasik. Untuk informasi selengkapnya, lihat AWS Tools for PowerShell Referensi Cmdlet.

Bagaimana AWS WAF Classic bekerja

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Anda menggunakan AWS WAF Classic untuk mengontrol bagaimana API Gateway, Amazon, CloudFront atau Application Load Balancer merespons permintaan web. Anda mulai dengan membuat kondisi, aturan, dan daftar kontrol akses web (ACL web). Anda menentukan kondisi Anda, menggabungkan kondisi Anda ke dalam aturan, dan menggabungkan aturan menjadi ACL web.

> **Note**
>
> Anda juga dapat menggunakan AWS WAF Classic untuk melindungi aplikasi Anda yang di-host di wadah Amazon Elastic Container Service (Amazon ECS). Amazon ECS adalah layanan manajemen kontainer yang sangat skalabel dan cepat yang memudahkan untuk menjalankan, menghentikan, dan mengelola kontainer Docker di cluster. Untuk menggunakan opsi ini, Anda mengonfigurasi Amazon ECS untuk menggunakan Application Load Balancer yang diaktifkan AWS WAF Klasik untuk merutekan dan melindungi lalu lintas HTTP/HTTPS (lapisan 7) di seluruh tugas dalam layanan Anda. Untuk informasi selengkapnya, lihat topik Service Load Balancing di Amazon Elastic Container Service Developer Guide.

Kondisi

Kondisi menentukan karakteristik dasar yang Anda ingin AWS WAF Classic perhatikan dalam permintaan web:

- Skrip yang cenderung berbahaya. Penyerang menyematkan skrip yang dapat mengeksploitasi kerentanan dalam aplikasi web. Ini dikenal sebagai cross-site scripting.
- Alamat IP atau rentang alamat tempat permintaan berasal.
- Negara atau lokasi geografis tempat permintaan berasal.
- Panjang bagian tertentu dari permintaan, seperti string query.
- Kode SQL yang kemungkinan berbahaya. Penyerang mencoba mengekstrak data dari database Anda dengan menyematkan kode SQL berbahaya dalam permintaan web. Ini dikenal sebagai injeksi SQL.
- String yang muncul dalam permintaan, misalnya, nilai yang muncul di `User-Agent` header atau string teks yang muncul dalam string kueri. Anda juga dapat menggunakan ekspresi reguler (regex) untuk menentukan string ini.

Beberapa kondisi mengambil beberapa nilai. Misalnya, Anda dapat menentukan hingga 10.000 alamat IP atau rentang alamat IP dalam kondisi IP.

Aturan

Anda menggabungkan kondisi ke dalam aturan untuk secara tepat menargetkan permintaan yang ingin Anda izinkan, blokir, atau hitung. AWS WAF Klasik menyediakan dua jenis aturan:

Aturan reguler

Aturan reguler hanya menggunakan kondisi untuk menargetkan permintaan tertentu. Misalnya, berdasarkan permintaan terbaru yang Anda lihat dari penyerang, Anda dapat membuat aturan yang mencakup kondisi berikut:

- Permintaan datang dari 192.0.2.44.
- Berisi nilai `BadBot` di header `User-Agent`.
- Mereka tampaknya menyertakan kode seperti SQL dalam string kueri.

Ketika aturan menyertakan beberapa kondisi, seperti dalam contoh ini, AWS WAF Classic mencari permintaan yang cocok dengan semua kondisi—yaitu, itu `AND` adalah kondisi bersama-sama.

Tambahkan setidaknya satu kondisi ke aturan reguler. Aturan reguler tanpa kondisi tidak dapat cocok dengan permintaan apa pun, sehingga tindakan aturan (izinkan, hitung, atau blokir) tidak pernah dipicu.

Aturan berbasis tarif

Aturan berbasis tarif seperti aturan reguler dengan batas tarif tambahan. Aturan berbasis tarif menghitung permintaan yang datang dari alamat IP yang memenuhi ketentuan aturan. Jika permintaan dari alamat IP melebihi batas tarif dalam periode lima menit, aturan dapat memicu tindakan. Diperlukan waktu satu atau dua menit untuk memicu tindakan.

Ketentuan bersifat opsional untuk aturan berbasis tarif. Jika Anda tidak menambahkan kondisi apa pun dalam aturan berbasis tarif, batas tarif berlaku untuk semua alamat IP. Jika Anda menggabungkan kondisi dengan batas tarif, batas tarif berlaku untuk alamat IP yang sesuai dengan kondisi.

Misalnya, berdasarkan permintaan terbaru yang Anda lihat dari penyerang, Anda dapat membuat aturan berbasis kecepatan yang mencakup kondisi berikut:

- Permintaan datang dari 192.0.2.44.
- Berisi nilai `BadBot` di header `User-Agent`.

Dalam aturan berbasis laju ini, Anda juga menentukan batas laju. Dalam contoh ini, katakanlah Anda membuat batas tarif 1.000. Permintaan yang memenuhi kedua kondisi sebelumnya dan

melebihi 1.000 permintaan per lima menit memicu tindakan aturan (blokir atau hitung), yang didefinisikan dalam ACL web.

Permintaan yang tidak memenuhi kedua kondisi tidak dihitung terhadap batas tarif dan tidak terpengaruh oleh aturan ini.

Sebagai contoh kedua, misalkan Anda ingin membatasi permintaan ke halaman tertentu di situs web Anda. Untuk melakukan ini, Anda dapat menambahkan kondisi kecocokan string berikut ke aturan berbasis laju:

- Bagian dari permintaan untuk memfilter adalah`URI`.
- Jenis Pertandingan adalah`Starts with`.
- Nilai untuk dicocokkan adalah`login`.

Selanjutnya, Anda menentukan 1.000. `RateLimit`

Dengan menambahkan aturan berbasis tarif ini ke ACL web, Anda dapat membatasi permintaan ke halaman login Anda tanpa mempengaruhi sisa situs Anda.

ACL web

Setelah Anda menggabungkan kondisi Anda ke dalam aturan, Anda menggabungkan aturan menjadi ACL web. Di sinilah Anda menentukan tindakan untuk setiap aturan—izinkan, blokir, atau hitung—dan tindakan default:

Tindakan untuk setiap aturan

Jika permintaan web cocok dengan semua kondisi dalam aturan, AWS WAF Classic dapat memblokir permintaan atau mengizinkan permintaan diteruskan ke API Gateway API, CloudFront distribusi, atau Application Load Balancer. Anda menentukan tindakan yang ingin dilakukan AWS WAF Classic untuk setiap aturan.

AWS WAF Classic membandingkan permintaan dengan aturan di ACL web dalam urutan di mana Anda mencantumkan aturan. AWS WAF Classic kemudian mengambil tindakan yang terkait dengan aturan pertama yang cocok dengan permintaan. Misalnya, jika permintaan web cocok dengan satu aturan yang mengizinkan permintaan dan aturan lain yang memblokir permintaan, AWS WAF Classic akan mengizinkan atau memblokir permintaan tergantung pada aturan mana yang terdaftar terlebih dahulu.

Jika Anda ingin menguji aturan baru sebelum mulai menggunakannya, Anda juga dapat mengonfigurasi AWS WAF Classic untuk menghitung permintaan yang memenuhi semua

ketentuan dalam aturan. Seperti aturan yang mengizinkan atau memblokir permintaan, aturan yang menghitung permintaan dipengaruhi oleh posisinya dalam daftar aturan di ACL web. Misalnya, jika permintaan web cocok dengan aturan yang mengizinkan permintaan dan aturan lain yang menghitung permintaan, dan jika aturan yang mengizinkan permintaan dicantumkan terlebih dahulu, permintaan tersebut tidak dihitung.

Tindakan default

Tindakan default menentukan apakah AWS WAF Classic mengizinkan atau memblokir permintaan yang tidak cocok dengan semua kondisi di salah satu aturan di ACL web. Misalnya, Anda membuat ACL web dan hanya menambahkan aturan yang Anda tentukan sebelumnya:

- Permintaan datang dari 192.0.2.44.
- Berisi nilai `BadBot` di header `User-Agent`.
- Mereka tampaknya menyertakan kode SQL berbahaya dalam string kueri.

Jika permintaan tidak memenuhi ketiga kondisi dalam aturan dan jika tindakan default adalah`ALLOW`, AWS WAF Classic meneruskan permintaan ke API Gateway, CloudFront atau Application Load Balancer, dan layanan merespons dengan objek yang diminta.

Jika Anda menambahkan dua aturan atau lebih ke ACL web, AWS WAF Classic akan melakukan tindakan default hanya jika permintaan tidak memenuhi semua ketentuan di salah satu aturan. Misalnya, Anda menambahkan aturan kedua yang berisi satu kondisi:

- Permintaan yang berisi nilai `BIGBadBot` di `User-Agent` header.

AWS WAF Classic melakukan tindakan default hanya jika permintaan tidak memenuhi ketiga kondisi dalam aturan pertama dan tidak memenuhi satu syarat dalam aturan kedua.

Pada beberapa kesempatan, AWS WAF mungkin mengalami kesalahan internal yang menunda respons ke Amazon API Gateway, Amazon, CloudFront atau Application Load Balancer tentang apakah akan mengizinkan atau memblokir permintaan. Pada kesempatan itu biasanya CloudFront akan memungkinkan permintaan atau menyajikan konten. API Gateway dan Application Load Balancer biasanya akan menolak permintaan dan tidak menyajikan konten.

AWS WAF Harga klasik

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Dengan AWS WAF Classic, Anda hanya membayar untuk ACL web dan aturan yang Anda buat, dan untuk jumlah permintaan HTTP yang diperiksa AWS WAF Classic. Untuk informasi selengkapnya, lihat Harga AWS WAF Klasik.

Memulai dengan AWS WAF Classic

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Tutorial ini menunjukkan cara menggunakan AWS WAF Classic untuk melakukan tugas-tugas berikut:

- Mengatur AWS WAF Klasik.
- Buat daftar kontrol akses web (web ACL) menggunakan konsol AWS WAF Klasik, dan tentukan kondisi yang ingin Anda gunakan untuk memfilter permintaan web. Misalnya, Anda dapat menentukan alamat IP tempat permintaan berasal dan nilai dalam permintaan yang hanya digunakan oleh penyerang.
- Tambahkan kondisi ke aturan. Aturan memungkinkan Anda menargetkan permintaan web yang ingin Anda blokir atau izinkan. Permintaan web harus cocok dengan semua kondisi dalam aturan

sebelum AWS WAF Classic memblokir atau mengizinkan permintaan berdasarkan kondisi yang Anda tentukan.

- Tambahkan aturan ke ACL web Anda. Di sinilah Anda menentukan apakah Anda ingin memblokir permintaan web atau mengizinkannya berdasarkan kondisi yang Anda tambahkan ke setiap aturan.
- Tentukan tindakan default, baik blok atau izinkan. Ini adalah tindakan yang dilakukan AWS WAF Classic ketika permintaan web tidak cocok dengan aturan Anda.
- Pilih CloudFront distribusi Amazon yang Anda inginkan AWS WAF Classic untuk memeriksa permintaan web. Tutorial ini mencakup langkah-langkah hanya untuk CloudFront, tetapi proses untuk Application Load Balancer dan Amazon API Gateway API pada dasarnya adalah sama. AWS WAF Klasik untuk CloudFront tersedia untuk semua Wilayah AWS. AWS WAF Klasik untuk digunakan dengan API Gateway atau Application Load Balancer tersedia di Wilayah yang tercantum di titik akhir AWS layanan.

> **Note**
>
> AWS biasanya menagih Anda kurang dari US $0,25 per hari untuk sumber daya yang Anda buat selama tutorial ini. Ketika Anda selesai dengan tutorial, kami sarankan Anda menghapus sumber daya untuk mencegah timbulnya biaya yang tidak perlu.

Topik

Langkah 1: Mengatur AWS WAF Klasik

Jika Anda belum mengikuti langkah-langkah pengaturan umumMenyiapkan AWS WAF Klasik, lakukan sekarang.

Langkah 2: Buat Web ACL

Konsol AWS WAF Klasik memandu Anda melalui proses konfigurasi AWS WAF Classic untuk memblokir atau mengizinkan permintaan web berdasarkan kondisi yang Anda tentukan, seperti alamat IP tempat permintaan berasal atau nilai dalam permintaan. Pada langkah ini, Anda membuat ACL web.

Untuk membuat web ACL

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.

2. Jika ini adalah pertama kalinya Anda menggunakan AWS WAF Classic, pilih Go to AWS WAF Classic, lalu pilih Configure web ACL.

   Jika Anda pernah menggunakan AWS WAF Classic sebelumnya, pilih Web ACL di panel navigasi, lalu pilih Buat web ACL.

3. Pada halaman Nama web ACL, untuk nama Web ACL, masukkan nama.

   > **Note**
   >
   > Anda tidak dapat mengubah nama setelah membuat ACL web.

4. Untuk nama CloudWatch metrik, masukkan nama. Nama hanya dapat berisi karakter alfanumerik (A-Z, a-z, 0-9). Itu tidak bisa berisi ruang putih.

   > **Note**
   >
   > Anda tidak dapat mengubah nama setelah membuat ACL web.

5. Untuk Wilayah , pilih Wilayah. Jika Anda akan mengaitkan ACL web ini dengan CloudFront distribusi, pilih Global (CloudFront).

6. Agar AWS sumber daya dapat dikaitkan, pilih sumber daya yang ingin Anda kaitkan dengan ACL web Anda, lalu pilih Berikutnya.

Langkah 3: Buat kondisi kecocokan IP

Kondisi pencocokan IP menentukan alamat IP atau rentang alamat IP tempat permintaan berasal. Pada langkah ini, Anda membuat kondisi pencocokan IP. Pada langkah selanjutnya, Anda menentukan apakah Anda ingin mengizinkan permintaan atau memblokir permintaan yang berasal dari alamat IP yang ditentukan.

> **Note**
>
> Untuk informasi selengkapnya tentang kondisi pencocokan IP, lihatBekerja dengan kondisi pencocokan IP.

Untuk membuat kondisi kecocokan IP

1. Pada halaman Create conditions, untuk kondisi pencocokan IP, pilih Create condition.
2. Dalam kotak dialog Buat kondisi kecocokan IP, untuk Nama, masukkan nama. Nama hanya dapat berisi karakter alfanumerik (A-Z, a-z, 0-9) atau karakter khusus berikut: _-!” #`+*}, ./.
3. Untuk Alamat, masukkan 192.0.2.0/24. Rentang alamat IP ini, yang ditentukan dalam notasi CIDR, mencakup alamat IP dari 192.0.2.0 hingga 192.0.2.255. (Rentang alamat IP 192.0.2.0/24 dicadangkan untuk contoh, jadi tidak ada permintaan web yang berasal dari alamat IP ini.)

   AWS WAF Classic mendukung rentang alamat IPv4: /8 dan rentang apa pun antara /16 hingga /32. AWS WAF Classic mendukung rentang alamat IPv6: /24, /32, /48, /56, /64, dan /128. (Untuk menentukan alamat IP tunggal, seperti 192.0.2.44, masukkan 192.0.2.44/32.) Rentang lainnya tidak didukung.

   Untuk informasi lebih lanjut tentang notasi CIDR, lihat artikel Wikipedia Classless Inter-Domain Routing.
4. Pilih Buat.

Langkah 4: Buat kondisi geo match

Kondisi geo match menentukan negara atau negara tempat permintaan berasal. Pada langkah ini, Anda membuat kondisi geo match. Pada langkah selanjutnya, Anda menentukan apakah Anda ingin mengizinkan permintaan atau memblokir permintaan yang berasal dari negara yang ditentukan.

> **Note**
>
> Untuk informasi selengkapnya tentang kondisi geo match, lihatBekerja dengan kondisi kecocokan geografis.

Untuk membuat kondisi kecocokan geografis

1. Pada halaman Create conditions, untuk Geo match conditions, pilih Create condition.
2. Dalam kotak dialog Buat kondisi kecocokan geografis, untuk Nama, masukkan nama. Nama hanya dapat berisi karakter alfanumerik (A-Z, a-z, 0-9) atau karakter khusus berikut: _-!” #`+*}, ./.
3. Pilih jenis Lokasi dan negara. Saat ini, tipe Lokasi hanya bisa Negara.
4. Pilih Tambahkan lokasi.
5. Pilih Buat.

Langkah 5: Buat kondisi kecocokan string

Kondisi pencocokan string mengidentifikasi string yang Anda inginkan AWS WAF Classic untuk mencari dalam permintaan, seperti nilai yang ditentukan dalam header atau dalam string kueri. Biasanya, string terdiri dari karakter ASCII yang dapat dicetak, tetapi Anda dapat menentukan karakter apa pun dari heksadesimal 0x00 hingga 0xFF (desimal 0 hingga 255). Pada langkah ini, Anda membuat kondisi kecocokan string. Pada langkah selanjutnya, Anda menentukan apakah Anda ingin mengizinkan atau memblokir permintaan yang berisi string yang ditentukan.

> **Note**
>
> Untuk informasi selengkapnya tentang kondisi pencocokan string, lihatBekerja dengan kondisi kecocokan string.

Untuk membuat kondisi kecocokan string

1. Pada halaman Create conditions, untuk kondisi kecocokan String dan regex, pilih Create condition.
2. Dalam Buat kondisi kecocokan string kotak dialog, masukkan nilai berikut:

   Nama

   Masukkan nama. Nama hanya dapat berisi karakter alfanumerik (A-Z, a-z, 0-9) atau karakter khusus berikut: _-!” #`+*}, ./.

   Tipe

   Pilih String match.

   Bagian dari permintaan untuk memfilter

   Pilih bagian dari permintaan web yang Anda ingin AWS WAF Classic untuk memeriksa string tertentu.

   Untuk contoh ini, pilih Header.

   > **Note**
   >
   > Jika Anda memilih Body untuk nilai Bagian dari permintaan untuk difilter, AWS WAF Classic hanya memeriksa 8192 byte pertama (8 KB) karena hanya CloudFront meneruskan 8192 byte pertama untuk inspeksi. Untuk mengizinkan atau memblokir permintaan yang badannya lebih panjang dari 8192 byte, Anda dapat membuat kondisi batasan ukuran. (AWS WAF Klasik mendapatkan panjang badan dari header permintaan.) Untuk informasi selengkapnya, lihat Bekerja dengan kondisi kendala ukuran.

   Header (Diperlukan jika “Bagian dari permintaan untuk memfilter” adalah “Header”)

   Karena Anda memilih Header untuk Bagian dari permintaan untuk difilter, Anda harus menentukan header mana yang ingin Anda periksa AWS WAF Classic. Masukkan Agen Pengguna. (Nilai ini tidak peka huruf besar/kecil.)

Jenis kecocokan

Pilih di mana string yang ditentukan harus muncul di header User-Agent, misalnya, di awal, di akhir, atau di mana saja dalam string.

Untuk contoh ini, pilih Persis cocok, yang menunjukkan bahwa AWS WAF Classic memeriksa permintaan web untuk nilai header yang identik dengan nilai yang Anda tentukan.

Transformasi

Dalam upaya untuk mem-bypass AWS WAF Classic, penyerang menggunakan format yang tidak biasa dalam permintaan web, misalnya, dengan menambahkan spasi putih atau dengan pengkodean URL beberapa atau semua permintaan. Transformasi mengonversi permintaan web ke format yang lebih standar dengan menghapus spasi putih, dengan mendekode URL permintaan, atau dengan melakukan operasi lain yang menghilangkan banyak pemformatan yang tidak biasa yang biasa digunakan penyerang.

Anda hanya dapat menentukan satu jenis transformasi teks.

Untuk contoh ini, pilih None.

Nilai dikodekan base64

Ketika nilai yang Anda masukkan dalam Nilai yang cocok sudah dikodekan base64, pilih kotak centang ini.

Untuk contoh ini, jangan pilih kotak centang.

Nilai untuk dicocokkan

Tentukan nilai yang ingin Anda cari AWS WAF Classic di bagian permintaan web yang Anda tunjukkan di Bagian dari permintaan untuk difilter.

Untuk contoh ini, masukkan BadBot. AWS WAF Classic akan memeriksa `User-Agent` header dalam permintaan web untuk nilainya BadBot.

Panjang maksimum Nilai untuk dicocokkan adalah 50 karakter. Jika Anda ingin menentukan nilai yang dikodekan base64, Anda dapat memberikan hingga 50 karakter sebelum pengkodean.

3. Jika Anda ingin AWS WAF Classic memeriksa permintaan web untuk beberapa nilai, seperti `User-Agent` header yang berisi `BadBot` dan string kueri yang berisi`BadParameter`, Anda memiliki dua pilihan:

- Jika Anda ingin mengizinkan atau memblokir permintaan web hanya jika berisi kedua nilai (AND), Anda membuat satu kondisi kecocokan string untuk setiap nilai.
- Jika Anda ingin mengizinkan atau memblokir permintaan web saat berisi nilai atau keduanya (OR), Anda menambahkan kedua nilai ke kondisi pencocokan string yang sama.

Untuk contoh ini, pilih Buat.

Langkah 5A: Buat kondisi regex (opsional)

Kondisi ekspresi reguler adalah jenis kondisi pencocokan string dan serupa karena mengidentifikasi string yang Anda inginkan AWS WAF Classic untuk mencari dalam permintaan, seperti nilai yang ditentukan dalam header atau dalam string kueri. Perbedaan utama adalah bahwa Anda menggunakan ekspresi reguler (regex) untuk menentukan pola string yang Anda ingin AWS WAF Classic untuk mencari. Pada langkah ini, Anda membuat kondisi kecocokan regex. Pada langkah selanjutnya, Anda menentukan apakah Anda ingin mengizinkan atau memblokir permintaan yang berisi string yang ditentukan.

> **Note**
>
> Untuk informasi selengkapnya tentang kondisi pertandingan regex, lihat. Bekerja dengan kondisi kecocokan regex

Untuk membuat kondisi kecocokan regex

1. Pada halaman Create conditions, untuk kondisi String match dan regex, pilih Create condition.
2. Dalam Buat kondisi kecocokan string kotak dialog, masukkan nilai berikut:

   Nama

   Masukkan nama. Nama hanya dapat berisi karakter alfanumerik (A-Z, a-z, 0-9) atau karakter khusus berikut: _-!” #`+*}, ./.

   Tipe

   Pilih pertandingan Regex.

Bagian dari permintaan untuk memfilter

Pilih bagian dari permintaan web yang Anda ingin AWS WAF Classic untuk memeriksa string tertentu.

Untuk contoh ini, pilih Body.

> **Note**
>
> Jika Anda memilih Body untuk nilai Bagian dari permintaan untuk difilter, AWS WAF Classic hanya memeriksa 8192 byte pertama (8 KB) karena hanya CloudFront meneruskan 8192 byte pertama untuk inspeksi. Untuk mengizinkan atau memblokir permintaan yang badannya lebih panjang dari 8192 byte, Anda dapat membuat kondisi batasan ukuran. (AWS WAF Klasik mendapatkan panjang badan dari header permintaan.) Untuk informasi selengkapnya, lihat Bekerja dengan kondisi kendala ukuran.

Transformasi

Dalam upaya untuk mem-bypass AWS WAF Classic, penyerang menggunakan format yang tidak biasa dalam permintaan web, misalnya, dengan menambahkan spasi putih atau dengan pengkodean URL beberapa atau semua permintaan. Transformasi mengonversi permintaan web ke format yang lebih standar dengan menghapus spasi putih, dengan mendekode URL permintaan, atau dengan melakukan operasi lain yang menghilangkan banyak pemformatan yang tidak biasa yang biasa digunakan penyerang.

Anda hanya dapat menentukan satu jenis transformasi teks.

Untuk contoh ini, pilih None.

Pola regex agar sesuai dengan permintaan

Pilih Buat set pola regex.

Nama set pola baru

Masukkan nama dan kemudian tentukan pola regex yang ingin Anda cari AWS WAF Classic.

Selanjutnya, masukkan ekspresi reguler I [a@] mAb [a@] DreQuest. AWS WAF Classic akan memeriksa `User-Agent` header dalam permintaan web untuk nilai-nilai:

- iaMa BadRequest
- IamAb @dRequest
- Saya @mA BadRequest
- Saya @mAB @dRequest

3. Pilih Buat set pola dan tambahkan filter.
4. Pilih Buat.

Langkah 6: Buat kondisi kecocokan injeksi SQL

Kondisi pencocokan injeksi SQL mengidentifikasi bagian dari permintaan web, seperti header atau string kueri, yang Anda ingin AWS WAF Classic untuk memeriksa kode SQL berbahaya. Penyerang menggunakan kueri SQL untuk mengekstrak data dari database Anda. Pada langkah ini, Anda membuat kondisi kecocokan injeksi SQL. Pada langkah selanjutnya, Anda menentukan apakah Anda ingin mengizinkan permintaan atau memblokir permintaan yang tampaknya berisi kode SQL berbahaya.

> **Note**
>
> Untuk informasi selengkapnya tentang kondisi pencocokan string, lihatBekerja dengan kondisi kecocokan injeksi SQL.

Untuk membuat kondisi kecocokan injeksi SQL

1. Pada halaman Create conditions, untuk kondisi kecocokan injeksi SQL, pilih Create condition.
2. Dalam kotak dialog Create SQL injection match condition, masukkan nilai berikut:

   Nama

   Masukkan nama.

   Bagian dari permintaan untuk memfilter

   Pilih bagian dari permintaan web yang Anda ingin AWS WAF Classic untuk memeriksa kode SQL berbahaya.

   Untuk contoh ini, pilih Query string.

> **Note**
>
> Jika Anda memilih Body untuk nilai Bagian dari permintaan untuk difilter, AWS WAF Classic hanya memeriksa 8192 byte pertama (8 KB) karena hanya CloudFront meneruskan 8192 byte pertama untuk inspeksi. Untuk mengizinkan atau memblokir permintaan yang badannya lebih panjang dari 8192 byte, Anda dapat membuat kondisi batasan ukuran. (AWS WAF Klasik mendapatkan panjang badan dari header permintaan.) Untuk informasi selengkapnya, lihat Bekerja dengan kondisi kendala ukuran.

Transformasi

Untuk contoh ini, pilih URL decode.

Penyerang menggunakan format yang tidak biasa, seperti pengkodean URL, dalam upaya untuk melewati Classic. AWS WAF Opsi decode URL menghilangkan beberapa pemformatan itu dalam permintaan web sebelum AWS WAF Classic memeriksa permintaan.

Anda hanya dapat menentukan satu jenis transformasi teks.

3. Pilih Buat.
4. Pilih Berikutnya.

Langkah 7: (Opsional) buat kondisi tambahan

AWS WAF Klasik mencakup kondisi lain, termasuk yang berikut:

- Kondisi batasan ukuran - Mengidentifikasi bagian dari permintaan web, seperti header atau string kueri, yang Anda ingin AWS WAF Classic periksa panjangnya. Untuk informasi selengkapnya, lihat Bekerja dengan kondisi kendala ukuran.
- Kondisi pencocokan skrip lintas situs — Mengidentifikasi bagian dari permintaan web, seperti header atau string kueri, yang ingin Anda periksa AWS WAF untuk skrip berbahaya. Untuk informasi selengkapnya, lihat Bekerja dengan kondisi pencocokan skrip lintas situs.

Anda dapat secara opsional membuat kondisi ini sekarang, atau Anda dapat melompat keLangkah 8: Buat aturan dan tambahkan kondisi.

Langkah 8: Buat aturan dan tambahkan kondisi

Anda membuat aturan untuk menentukan kondisi yang ingin Anda cari AWS WAF Classic dalam permintaan web. Jika Anda menambahkan lebih dari satu kondisi ke aturan, permintaan web harus cocok dengan semua kondisi dalam aturan untuk AWS WAF Classic untuk mengizinkan atau memblokir permintaan berdasarkan aturan tersebut.

> **Note**
>
> Untuk informasi selengkapnya tentang aturan, lihatBekerja dengan aturan.

Untuk membuat aturan dan menambahkan kondisi

1. Pada halaman Buat aturan, pilih Buat aturan.
2. Dalam Buat aturan kotak dialog, masukkan nilai berikut:

   Nama

   Masukkan nama.

   CloudWatch nama metrik

   Masukkan nama untuk CloudWatch metrik yang akan dibuat oleh AWS WAF Classic dan akan dikaitkan dengan aturan. Nama hanya dapat berisi karakter alfanumerik (A-Z, a-z, 0-9). Itu tidak bisa berisi ruang putih.

   Jenis aturan

   Pilih salah satu Aturan reguler atau aturan berbasis Tarif. Aturan berbasis tarif identik dengan aturan reguler tetapi juga memperhitungkan berapa banyak permintaan yang datang dari alamat IP yang diidentifikasi dalam periode lima menit. Untuk informasi selengkapnya tentang jenis aturan, lihatBagaimana AWS WAF Classic bekerja. Untuk contoh ini, pilih`Regular rule`.

   Batas tarif

   Untuk aturan berbasis tarif, masukkan jumlah maksimum permintaan untuk mengizinkan dalam periode lima menit dari alamat IP yang sesuai dengan ketentuan aturan.
3. Untuk kondisi pertama yang ingin Anda tambahkan ke aturan, tentukan pengaturan berikut:

- Pilih apakah Anda ingin AWS WAF Classic mengizinkan atau memblokir permintaan berdasarkan apakah permintaan web cocok atau tidak sesuai dengan pengaturan dalam kondisi tersebut.

  Untuk contoh ini, pilih tidak.

- Pilih jenis kondisi yang ingin Anda tambahkan ke aturan: kondisi set kecocokan IP, kondisi set kecocokan string, atau kondisi set kecocokan injeksi SQL.

  Untuk contoh ini, pilih berasal dari alamat IP di.

- Pilih kondisi yang ingin Anda tambahkan ke aturan.

  Untuk contoh ini, pilih kondisi pencocokan IP yang Anda buat di tugas sebelumnya.

4. Pilih Tambahkan syarat.
5. Tambahkan kondisi geo match yang Anda buat sebelumnya. Tentukan nilai-nilai berikut ini:
   - Ketika sebuah permintaan
   - Berasal dari lokasi geografis di
   - Pilih kondisi geo match Anda.
6. Pilih Tambahkan kondisi lain.
7. Tambahkan kondisi kecocokan string yang Anda buat sebelumnya. Tentukan nilai-nilai berikut ini:
   - Ketika sebuah permintaan
   - cocokkan setidaknya satu filter dalam kondisi kecocokan string
   - Pilih kondisi kecocokan string Anda.
8. Pilih Tambahkan syarat.
9. Tambahkan kondisi kecocokan injeksi SQL yang Anda buat sebelumnya. Tentukan nilai-nilai berikut ini:
   - Ketika sebuah permintaan
   - mencocokkan setidaknya satu filter dalam kondisi kecocokan injeksi SQL
   - Pilih kondisi kecocokan injeksi SQL Anda.
10. Pilih Tambahkan syarat.
11. Tambahkan kondisi batasan ukuran yang Anda buat sebelumnya. Tentukan nilai-nilai berikut ini:

- Ketika sebuah permintaan
- cocokkan setidaknya satu filter dalam kondisi kendala ukuran
- Pilih kondisi kendala ukuran Anda.

12. Jika Anda membuat kondisi lain, seperti kondisi regex, tambahkan dengan cara yang sama.
13. Pilih Buat.
14. Untuk tindakan Default, pilih Izinkan semua permintaan yang tidak cocok dengan aturan apa pun.
15. Pilih Periksa dan buat.

Langkah 9: Tambahkan aturan ke ACL Web

Saat Anda menambahkan aturan ke ACL web, Anda menentukan pengaturan berikut:

- Tindakan yang Anda ingin AWS WAF Classic lakukan pada permintaan web yang cocok dengan semua kondisi dalam aturan: izinkan, blokir, atau hitung permintaan.
- Tindakan default untuk ACL web. Ini adalah tindakan yang Anda ingin AWS WAF Classic lakukan pada permintaan web yang tidak cocok dengan semua kondisi dalam aturan: izinkan atau blokir permintaan.

AWS WAF Classic mulai memblokir permintaan CloudFront web yang cocok dengan semua kondisi berikut (dan yang lain yang mungkin telah Anda tambahkan):

- Nilai `User-Agent` header adalah `BadBot`
- (Jika Anda membuat dan menambahkan kondisi regex) Nilai dari `Body` adalah salah satu dari empat string yang cocok dengan pola `I[a@]mAB[a@]dRequest`
- Permintaan berasal dari alamat IP dalam kisaran 192.0.2.0-192.0.2.255
- Permintaan berasal dari negara yang Anda pilih dalam kondisi geo match
- Permintaan tampaknya menyertakan kode SQL berbahaya dalam string kueri

AWS WAF Classic memungkinkan CloudFront untuk menanggapi permintaan apa pun yang tidak memenuhi ketiga kondisi ini.

Langkah 10: Bersihkan sumber daya Anda

Anda sudah berhasil menyelesaikan tutorial ini. Untuk mencegah akun Anda mendapatkan biaya AWS WAF Klasik tambahan, Anda harus membersihkan objek AWS WAF Klasik yang Anda buat. Atau, Anda dapat mengubah konfigurasi agar sesuai dengan permintaan web yang benar-benar ingin Anda izinkan, blokir, dan hitung.

> **Note**
>
> AWS biasanya menagih Anda kurang dari US $0,25 per hari untuk sumber daya yang Anda buat selama tutorial ini. Setelah selesai, kami sarankan Anda menghapus sumber daya untuk mencegah timbulnya biaya yang tidak perlu.

Untuk menghapus objek yang dikenakan biaya AWS WAF Classic

1. Putuskan hubungan ACL web Anda dari distribusi Anda CloudFront :

   a. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

      Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.

   b. Pilih nama ACL web yang ingin Anda hapus. Ini membuka halaman dengan detail ACL web di panel kanan.

   c. Di panel kanan, pada tab Aturan, buka AWS sumber daya menggunakan bagian ACL web ini. Untuk CloudFront distribusi yang Anda kaitkan dengan ACL web, pilih x di kolom Type.

2. Hapus kondisi dari aturan Anda:

   a. Di panel navigasi, pilih Aturan.

   b. Pilih aturan yang Anda buat selama tutorial.

   c. Pilih Edit aturan.

   d. Pilih x di sebelah kanan setiap judul kondisi.

   e. Pilih Perbarui.

3. Hapus aturan dari ACL web Anda, dan hapus ACL web:

   a. Di panel navigasi, pilih Web ACL.

b. Pilih nama ACL web yang Anda buat selama tutorial. Ini membuka halaman dengan detail ACL web di panel kanan.

c. Pada tab Aturan, pilih Edit web ACL.

d. Pilih x di sebelah kanan judul aturan.

e. Pilih Tindakan, lalu pilih Hapus web ACL.

4. Hapus aturan Anda:

a. Di panel navigasi, pilih Aturan.

b. Pilih aturan yang Anda buat selama tutorial.

c. Pilih Hapus.

d. Di kotak dialog Hapus, pilih Hapus lagi untuk mengonfirmasi.

AWS WAF Classic tidak mengenakan biaya untuk kondisi, tetapi jika Anda ingin menyelesaikan pembersihan, lakukan prosedur berikut untuk menghapus filter dari kondisi dan menghapus kondisi.

Untuk menghapus filter dan kondisi

1. Hapus rentang alamat IP dalam kondisi pencocokan IP Anda, dan hapus kondisi pencocokan IP:

a. Di panel navigasi konsol AWS WAF Klasik, pilih alamat IP.

b. Pilih kondisi pencocokan IP yang Anda buat selama tutorial.

c. Pilih kotak centang untuk rentang alamat IP yang Anda tambahkan.

d. Pilih Hapus alamat atau rentang IP.

e. Di panel Ketentuan kecocokan IP, pilih Hapus.

f. Di kotak dialog Hapus, pilih Hapus lagi untuk mengonfirmasi.

2. Hapus filter dalam kondisi kecocokan injeksi SQL Anda, dan hapus kondisi kecocokan injeksi SQL:

a. Di panel navigasi, pilih injeksi SQL.

b. Pilih kondisi kecocokan injeksi SQL yang Anda buat selama tutorial.

c. Pilih kotak centang untuk filter yang Anda tambahkan.

d. Pilih Hapus filter.

e. Di panel kondisi kecocokan injeksi SQL, pilih Hapus.

f. Di kotak dialog Hapus, pilih Hapus lagi untuk mengonfirmasi.

3. Hapus filter dalam kondisi kecocokan string Anda, dan hapus kondisi kecocokan string:

    a. Di panel navigasi, pilih String dan regex matching.

    b. Pilih kondisi kecocokan string yang Anda buat selama tutorial.

    c. Pilih kotak centang untuk filter yang Anda tambahkan.

    d. Pilih Hapus filter.

    e. Di panel Kondisi kecocokan String, pilih Hapus.

    f. Di kotak dialog Hapus, pilih Hapus lagi untuk mengonfirmasi.

4. Jika Anda membuatnya, hapus filter dalam kondisi pencocokan regex Anda, dan hapus kondisi pencocokan regex:

    a. Di panel navigasi, pilih String dan regex matching.

    b. Pilih kondisi pencocokan regex yang Anda buat selama tutorial.

    c. Pilih kotak centang untuk filter yang Anda tambahkan.

    d. Pilih Hapus filter.

    e. Di panel Ketentuan kecocokan Regex, pilih Hapus.

    f. Di kotak dialog Hapus, pilih Hapus lagi untuk mengonfirmasi.

5. Hapus filter dalam kondisi batasan ukuran Anda, dan hapus kondisi batasan ukuran:

    a. Di panel navigasi, pilih Kendala ukuran.

    b. Pilih kondisi batasan ukuran yang Anda buat selama tutorial.

    c. Pilih kotak centang untuk filter yang Anda tambahkan.

    d. Pilih Hapus filter.

    e. Di panel Kondisi batasan ukuran, pilih Hapus.

    f. Di kotak dialog Hapus, pilih Hapus lagi untuk mengonfirmasi.

Membuat dan mengonfigurasi Daftar Kontrol Akses Web (Web ACL)

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum

November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Daftar kontrol akses web (web ACL) memberi Anda kontrol halus atas permintaan web yang ditanggapi oleh API Amazon API Gateway, CloudFront distribusi Amazon, atau Application Load Balancer. Anda dapat mengizinkan atau memblokir jenis permintaan berikut:

- Berasal dari alamat IP atau berbagai alamat IP
- Berasal dari negara atau negara tertentu
- Berisi string tertentu atau mencocokkan pola ekspresi reguler (regex) di bagian permintaan tertentu
- Melebihi panjang yang ditentukan
- Tampaknya berisi kode SQL berbahaya (dikenal sebagai injeksi SQL)
- Tampaknya berisi skrip berbahaya (dikenal sebagai skrip lintas situs)

Anda juga dapat menguji kombinasi dari kondisi ini, atau memblokir atau menghitung permintaan web yang tidak hanya memenuhi persyaratan yang ditentukan, tetapi juga melebihi jumlah permintaan tertentu dalam periode 5 menit.

Untuk memilih permintaan yang ingin Anda izinkan untuk memiliki akses ke konten Anda atau yang ingin Anda blokir, lakukan tugas-tugas berikut:

1. Pilih tindakan default, izinkan atau blokir, untuk permintaan web yang tidak cocok dengan kondisi apa pun yang Anda tentukan. Untuk informasi selengkapnya, lihat Memutuskan tindakan default untuk ACL Web.
2. Tentukan kondisi di mana Anda ingin mengizinkan atau memblokir permintaan:
   - Untuk mengizinkan atau memblokir permintaan berdasarkan apakah permintaan tersebut tampaknya berisi skrip berbahaya, buat kondisi pencocokan skrip lintas situs. Untuk informasi selengkapnya, lihat Bekerja dengan kondisi pencocokan skrip lintas situs.
   - Untuk mengizinkan atau memblokir permintaan berdasarkan alamat IP asal mereka, buat kondisi pencocokan IP. Untuk informasi selengkapnya, lihat Bekerja dengan kondisi pencocokan IP.
   - Untuk mengizinkan atau memblokir permintaan berdasarkan negara asal mereka, buat kondisi kecocokan geografis. Untuk informasi selengkapnya, lihat Bekerja dengan kondisi kecocokan geografis.

- Untuk mengizinkan atau memblokir permintaan berdasarkan apakah permintaan melebihi panjang yang ditentukan, buat kondisi batasan ukuran. Untuk informasi selengkapnya, lihat Bekerja dengan kondisi kendala ukuran.
- Untuk mengizinkan atau memblokir permintaan berdasarkan apakah permintaan tampaknya berisi kode SQL berbahaya, buat kondisi kecocokan injeksi SQL. Untuk informasi selengkapnya, lihat Bekerja dengan kondisi kecocokan injeksi SQL.
- Untuk mengizinkan atau memblokir permintaan berdasarkan string yang muncul dalam permintaan, buat kondisi pencocokan string. Untuk informasi selengkapnya, lihat Bekerja dengan kondisi kecocokan string.
- Untuk mengizinkan atau memblokir permintaan berdasarkan pola regex yang muncul dalam permintaan, buat kondisi pencocokan regex. Untuk informasi selengkapnya, lihat Bekerja dengan kondisi kecocokan regex.

3. Tambahkan ketentuan ke satu atau lebih aturan. Jika Anda menambahkan lebih dari satu kondisi ke aturan yang sama, permintaan web harus cocok dengan semua kondisi untuk AWS WAF Classic untuk mengizinkan atau memblokir permintaan berdasarkan aturan. Untuk informasi selengkapnya, lihat Bekerja dengan aturan. Secara opsional, Anda dapat menggunakan aturan berbasis tarif alih-alih aturan reguler untuk membatasi jumlah permintaan dari alamat IP apa pun yang memenuhi ketentuan.
4. Tambahkan aturan ke ACL web. Untuk setiap aturan, tentukan apakah Anda ingin AWS WAF Classic mengizinkan atau memblokir permintaan berdasarkan kondisi yang Anda tambahkan ke aturan. Jika Anda menambahkan lebih dari satu aturan ke ACL web, AWS WAF Classic mengevaluasi aturan dalam urutan yang tercantum di ACL web. Untuk informasi selengkapnya, lihat Bekerja dengan ACL web.

   Saat Anda menambahkan aturan baru atau memperbarui aturan yang ada, diperlukan waktu hingga satu menit agar perubahan tersebut muncul dan aktif di seluruh ACL dan sumber daya web Anda.

Topik

- Bekerja dengan kondisi
- Bekerja dengan aturan
- Bekerja dengan ACL web

Bekerja dengan kondisi

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Kondisi menentukan kapan Anda ingin mengizinkan atau memblokir permintaan.

- Untuk mengizinkan atau memblokir permintaan berdasarkan apakah permintaan tersebut tampaknya berisi skrip berbahaya, buat kondisi pencocokan skrip lintas situs. Untuk informasi selengkapnya, lihat Bekerja dengan kondisi pencocokan skrip lintas situs.
- Untuk mengizinkan atau memblokir permintaan berdasarkan alamat IP asal mereka, buat kondisi pencocokan IP. Untuk informasi selengkapnya, lihat Bekerja dengan kondisi pencocokan IP.
- Untuk mengizinkan atau memblokir permintaan berdasarkan negara asal mereka, buat kondisi kecocokan geografis. Untuk informasi selengkapnya, lihat Bekerja dengan kondisi kecocokan geografis.
- Untuk mengizinkan atau memblokir permintaan berdasarkan apakah permintaan melebihi panjang yang ditentukan, buat kondisi batasan ukuran. Untuk informasi selengkapnya, lihat Bekerja dengan kondisi kendala ukuran.
- Untuk mengizinkan atau memblokir permintaan berdasarkan apakah permintaan tampaknya berisi kode SQL berbahaya, buat kondisi kecocokan injeksi SQL. Untuk informasi selengkapnya, lihat Bekerja dengan kondisi kecocokan injeksi SQL.
- Untuk mengizinkan atau memblokir permintaan berdasarkan string yang muncul dalam permintaan, buat kondisi pencocokan string. Untuk informasi selengkapnya, lihat Bekerja dengan kondisi kecocokan string.
- Untuk mengizinkan atau memblokir permintaan berdasarkan pola regex yang muncul dalam permintaan, buat kondisi pencocokan regex. Untuk informasi selengkapnya, lihat Bekerja dengan kondisi kecocokan regex.

Topik

- Bekerja dengan kondisi pencocokan skrip lintas situs
- Bekerja dengan kondisi pencocokan IP
- Bekerja dengan kondisi kecocokan geografis
- Bekerja dengan kondisi kendala ukuran
- Bekerja dengan kondisi kecocokan injeksi SQL
- Bekerja dengan kondisi kecocokan string
- Bekerja dengan kondisi kecocokan regex

Bekerja dengan kondisi pencocokan skrip lintas situs

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Penyerang terkadang memasukkan skrip ke dalam permintaan web dalam upaya untuk mengeksploitasi kerentanan dalam aplikasi web. Anda dapat membuat satu atau beberapa kondisi pencocokan skrip lintas situs untuk mengidentifikasi bagian-bagian permintaan web, seperti URI atau string kueri, yang ingin AWS WAF Classic periksa kemungkinan skrip berbahaya. Kemudian dalam proses, ketika Anda membuat ACL web, Anda menentukan apakah akan mengizinkan atau memblokir permintaan yang tampaknya berisi skrip berbahaya.

Topik

- Membuat kondisi pencocokan skrip lintas situs
- Nilai yang Anda tentukan saat membuat atau mengedit kondisi pencocokan skrip lintas situs
- Menambahkan dan menghapus filter dalam kondisi kecocokan skrip lintas situs
- Menghapus kondisi pencocokan skrip lintas situs

Membuat kondisi pencocokan skrip lintas situs

Saat Anda membuat kondisi pencocokan skrip lintas situs, Anda menentukan filter. Filter menunjukkan bagian dari permintaan web yang Anda ingin AWS WAF Classic untuk memeriksa skrip berbahaya, seperti URI atau string kueri. Anda dapat menambahkan lebih dari satu filter ke kondisi pencocokan skrip lintas situs, atau Anda dapat membuat kondisi terpisah untuk setiap filter. Inilah cara setiap konfigurasi memengaruhi perilaku AWS WAF Klasik:

- Lebih dari satu filter per kondisi pencocokan skrip lintas situs (disarankan) — Saat Anda menambahkan kondisi pencocokan skrip lintas situs yang berisi beberapa filter ke aturan dan menambahkan aturan ke ACL web, permintaan web harus cocok hanya dengan salah satu filter dalam kondisi pencocokan skrip lintas situs untuk AWS WAF Classic untuk mengizinkan atau memblokir permintaan berdasarkan kondisi tersebut.

  Misalnya, Anda membuat satu kondisi pencocokan skrip lintas situs, dan kondisi tersebut berisi dua filter. Satu filter menginstruksikan AWS WAF Classic untuk memeriksa URI untuk skrip berbahaya, dan yang lainnya menginstruksikan AWS WAF Classic untuk memeriksa string kueri. AWS WAF Classic mengizinkan atau memblokir permintaan jika tampaknya berisi skrip berbahaya baik di URI atau dalam string kueri.
- Satu filter per kondisi pencocokan skrip lintas situs — Saat Anda menambahkan kondisi pencocokan skrip lintas situs terpisah ke aturan dan menambahkan aturan ke ACL web, permintaan web harus cocok dengan semua kondisi untuk AWS WAF Classic untuk mengizinkan atau memblokir permintaan berdasarkan kondisi.

  Misalkan Anda membuat dua kondisi, dan setiap kondisi berisi salah satu dari dua filter dalam contoh sebelumnya. Saat Anda menambahkan kedua kondisi ke aturan yang sama dan menambahkan aturan ke ACL web, AWS WAF Classic mengizinkan atau memblokir permintaan hanya jika URI dan string kueri tampaknya berisi skrip berbahaya.

> **Note**
>
> Saat menambahkan kondisi pencocokan skrip lintas situs ke aturan, Anda juga dapat mengonfigurasi AWS WAF Classic untuk mengizinkan atau memblokir permintaan web yang tampaknya tidak mengandung skrip berbahaya.

Untuk membuat kondisi pencocokan skrip lintas situs

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Di panel navigasi, pilih Cross-site scripting.
3. Pilih Buat kondisi.
4. Tentukan pengaturan filter yang berlaku. Untuk informasi selengkapnya, lihat Nilai yang Anda tentukan saat membuat atau mengedit kondisi pencocokan skrip lintas situs.
5. Pilih Tambahkan filter lain.
6. Jika Anda ingin menambahkan filter lain, ulangi langkah 4 dan 5.
7. Setelah selesai menambahkan filter, pilih Buat.

Nilai yang Anda tentukan saat membuat atau mengedit kondisi pencocokan skrip lintas situs

Saat Anda membuat atau memperbarui kondisi pencocokan skrip lintas situs, Anda menentukan nilai berikut:

Nama

Nama kondisi pencocokan skrip lintas situs.

Nama hanya dapat berisi karakter A-Z, a-z, 0-9, dan karakter khusus: _-!” #`+*}, ./. Anda tidak dapat mengubah nama kondisi setelah Anda membuatnya.

Bagian dari permintaan untuk memfilter

Pilih bagian dari setiap permintaan web yang Anda ingin AWS WAF Classic untuk memeriksa skrip berbahaya:

Header

Header permintaan tertentu, misalnya, `Referer` header `User-Agent` atau. Jika Anda memilih Header, tentukan nama header di bidang Header.

Metode HTTP

Metode HTTP, yang menunjukkan jenis operasi yang diminta permintaan asal untuk dilakukan. CloudFront mendukung metode berikut:`DELETE`,`GET`,`HEAD`,`OPTIONS`,`PATCH`,`POST`, dan`PUT`.

String kueri

Bagian dari URL yang muncul setelah ? karakter, jika ada.

> **Note**
>
> Untuk kondisi pencocokan skrip lintas situs, kami sarankan Anda memilih Semua parameter kueri (hanya nilai) alih-alih String kueri untuk Bagian dari permintaan untuk memfilter.

URI

Jalur URI permintaan, yang mengidentifikasi sumber daya, misalnya,`/images/daily-ad.jpg`. Ini tidak termasuk string kueri atau komponen fragmen URI. Untuk selengkapnya, lihat Uniform Resource Identifier (URI): Generic Syntax.

Kecuali Transformasi ditentukan, URI tidak dinormalisasi dan diperiksa sama seperti AWS menerimanya dari klien sebagai bagian dari permintaan. Transformasi akan memformat ulang URI seperti yang ditentukan.

Tubuh

Bagian dari permintaan yang berisi data tambahan yang ingin Anda kirim ke server web Anda sebagai badan permintaan HTTP, seperti data dari formulir.

> **Note**
>
> Jika Anda memilih Body untuk nilai Bagian dari permintaan untuk difilter, AWS WAF Classic hanya memeriksa 8192 byte pertama (8 KB). Untuk mengizinkan atau memblokir permintaan yang badannya lebih panjang dari 8192 byte, Anda dapat membuat kondisi batasan ukuran. (AWS WAF Klasik mendapatkan panjang badan dari header permintaan.) Untuk informasi selengkapnya, lihat Bekerja dengan kondisi kendala ukuran.

Parameter kueri tunggal (hanya nilai)

Parameter apa pun yang telah Anda definisikan sebagai bagian dari string kueri. Misalnya, jika URL-nya adalah “www.xyz.com? UserName =abc& SalesRegion =seattle” Anda dapat menambahkan filter ke parameter atau. UserNameSalesRegion

Jika Anda memilih Parameter kueri tunggal (hanya nilai), Anda juga akan menentukan nama parameter Kueri. Ini adalah parameter dalam string kueri yang akan Anda periksa, seperti UserNameatau SalesRegion. Panjang maksimum untuk nama parameter Query adalah 30 karakter. Nama parameter kueri tidak peka huruf besar/kecil. Misalnya, Anda menentukan UserNamesebagai nama parameter Query, ini akan cocok dengan semua variasi UserName, seperti username dan UserName.

Semua parameter kueri (hanya nilai)

Mirip dengan Parameter kueri tunggal (hanya nilai), tetapi alih-alih memeriksa nilai parameter tunggal, AWS WAF Classic memeriksa semua nilai parameter dalam string kueri untuk kemungkinan skrip berbahaya. Misalnya, jika URL adalah “www.xyz.com? UserName =abc& SalesRegion =seattle,” dan Anda memilih Semua parameter kueri (hanya nilai), AWS WAF Classic akan memicu kecocokan jika nilai atau mengandung kemungkinan skrip berbahaya. UserNameSalesRegion

Header

Jika Anda memilih Header untuk Bagian dari permintaan untuk difilter, pilih header dari daftar header umum, atau masukkan nama header yang ingin Anda periksa AWS WAF Classic untuk skrip berbahaya.

Transformasi

Transformasi memformat ulang permintaan web sebelum AWS WAF Classic memeriksa permintaan. Ini menghilangkan beberapa format yang tidak biasa yang digunakan penyerang dalam permintaan web dalam upaya untuk melewati AWS WAF Classic.

Anda hanya dapat menentukan satu jenis transformasi teks.

Transformasi dapat melakukan operasi berikut:

Tidak ada

AWS WAF Classic tidak melakukan transformasi teks apa pun pada permintaan web sebelum memeriksanya agar string di Nilai cocok.

Mengkonversi ke lowercase

AWS WAF Klasik mengkonversi huruf besar (A-Z) ke huruf kecil (a-z).

Dekode HTML

AWS WAF Klasik menggantikan karakter yang dikodekan HTML dengan karakter yang tidak dikodekan:

- Mengganti `&quot;` dengan &
- Mengganti ` ` dengan ruang yang tidak pecah
- Mengganti `&lt;` dengan <
- Mengganti `&gt;` dengan >
- Mengganti karakter yang diwakili dalam format heksadesimal, `&#xhhhh;`, dengan karakter yang sesuai
- Mengganti karakter yang diwakili dalam format desimal, `&#nnnn;`, dengan karakter yang sesuai

Menormalkan ruang putih

AWS WAF Klasik menggantikan karakter berikut dengan karakter spasi (desimal 32):

- \ f, formfeed, desimal 12
- \ t, tab, desimal 9
- \ n, baris baru, desimal 10
- \ r, pengembalian pengangkutan, desimal 13
- \ v, tab vertikal, desimal 11
- spasi tanpa pindah baris, desimal 160

Selain itu, opsi ini menggantikan beberapa spasi dengan satu spasi.

Sederhanakan baris perintah

Untuk permintaan yang berisi perintah baris perintah sistem operasi, gunakan opsi ini untuk melakukan transformasi berikut:

- Menghapus karakter berikut: \ " ' ^
- Menghapus spasi sebelum karakter berikut: / (
- Mengganti karakter berikut dengan spasi: , ;
- Mengganti spasi ganda dengan satu spasi
- Mengonversi huruf besar (A-Z) ke huruf kecil (a-z)

Dekode URL

Memecahkan kode permintaan yang dikodekan URL.

Menambahkan dan menghapus filter dalam kondisi kecocokan skrip lintas situs

Anda dapat menambahkan atau menghapus filter dalam kondisi pencocokan skrip lintas situs. Untuk mengubah filter, tambahkan yang baru dan hapus yang lama.

Untuk menambah atau menghapus filter dalam kondisi pencocokan skrip lintas situs

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Di panel navigasi, pilih Cross-site scripting.
3. Pilih kondisi yang ingin Anda tambahkan atau hapus filter.
4. Untuk menambahkan filter, lakukan langkah-langkah berikut:
   a. Pilih Tambahkan filter.
   b. Tentukan pengaturan filter yang berlaku. Untuk informasi selengkapnya, lihat Nilai yang Anda tentukan saat membuat atau mengedit kondisi pencocokan skrip lintas situs.
   c. Pilih Tambahkan.
5. Untuk menghapus filter, lakukan langkah-langkah berikut:
   a. Pilih filter yang ingin Anda hapus.
   b. Pilih Hapus filter.

Menghapus kondisi pencocokan skrip lintas situs

Jika Anda ingin menghapus kondisi pencocokan skrip lintas situs, Anda harus terlebih dahulu menghapus semua filter dalam kondisi dan menghapus kondisi dari semua aturan yang menggunakannya, seperti yang dijelaskan dalam prosedur berikut.

Untuk menghapus kondisi pencocokan skrip lintas situs

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Di panel navigasi, pilih Cross-site scripting.

3. Di panel Kondisi pencocokan skrip lintas situs, pilih kondisi pencocokan skrip lintas situs yang ingin Anda hapus.
4. Di panel kanan, pilih tab Aturan terkait.

   Jika daftar aturan yang menggunakan kondisi pencocokan skrip lintas situs ini kosong, lanjutkan ke langkah 6. Jika daftar berisi aturan apa pun, catat aturannya, dan lanjutkan dengan langkah 5.
5. Untuk menghapus kondisi pencocokan skrip lintas situs dari aturan yang menggunakannya, lakukan langkah-langkah berikut:

   a. Di panel navigasi, pilih Aturan.

   b. Pilih nama aturan yang menggunakan kondisi pencocokan skrip lintas situs yang ingin Anda hapus.

   c. Di panel kanan, pilih kondisi pencocokan skrip lintas situs yang ingin Anda hapus dari aturan, dan pilih Hapus kondisi yang dipilih.

   d. Ulangi langkah b dan c untuk semua aturan yang tersisa yang menggunakan kondisi pencocokan skrip lintas situs yang ingin Anda hapus.

   e. Di panel navigasi, pilih Cross-site scripting.

   f. Di panel Kondisi pencocokan skrip lintas situs, pilih kondisi pencocokan skrip lintas situs yang ingin Anda hapus.
6. Pilih Hapus untuk menghapus kondisi yang dipilih.

Bekerja dengan kondisi pencocokan IP

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Jika Anda ingin mengizinkan atau memblokir permintaan web berdasarkan alamat IP tempat permintaan berasal, buat satu atau beberapa kondisi pencocokan IP. Kondisi pencocokan IP mencantumkan hingga 10.000 alamat IP atau rentang alamat IP tempat permintaan Anda berasal.

Kemudian dalam proses, ketika Anda membuat ACL web, Anda menentukan apakah akan mengizinkan atau memblokir permintaan dari alamat IP tersebut.

Topik

Membuat Kondisi Pencocokan IP

Jika Anda ingin mengizinkan beberapa permintaan web dan memblokir yang lain berdasarkan alamat IP tempat permintaan berasal, buat kondisi pencocokan IP untuk alamat IP yang ingin Anda izinkan dan kondisi pencocokan IP lainnya untuk alamat IP yang ingin Anda blokir.

> **Note**
>
> Saat menambahkan kondisi pencocokan IP ke aturan, Anda juga dapat mengonfigurasi AWS WAF Classic untuk mengizinkan atau memblokir permintaan web yang tidak berasal dari alamat IP yang Anda tentukan dalam kondisi tersebut.

Untuk membuat kondisi kecocokan IP

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Di panel navigasi, pilih alamat IP.
3. Pilih Buat kondisi.
4. Masukkan nama di bidang Nama.

   Nama hanya dapat berisi karakter alfanumerik (A-Z, a-z, 0-9) atau karakter khusus berikut: _-!” #` +*}, ./. Anda tidak dapat mengubah nama kondisi setelah Anda membuatnya.
5. Pilih versi IP yang benar dan tentukan alamat IP atau rentang alamat IP dengan menggunakan notasi CIDR. Berikut ini adalah beberapa contohnya:

   - Untuk menentukan alamat IPv4 192.0.2.44, ketik 192.0.2.44/32.

- Untuk menentukan alamat IPv6 0:0:0:0:0:ffff:c 000:22 c, ketik 0:0:0:0:0:0:ffff:c 000:22 c/128.
- Untuk menentukan kisaran alamat IPv4 dari 192.0.2.0 hingga 192.0.2.255, ketik 192.0.2.0/24.
- Untuk menentukan kisaran alamat IPv6 dari 2620:0: 2 d 0:200:0: 0:0 hingga 2620:0:2 d 0:200: ffff:ffff:ffff:ffff, masukkan 2620:0:2 d 0:200: :/64.

AWS WAF Classic mendukung rentang alamat IPv4: /8 dan rentang apa pun antara /16 hingga /32. AWS WAF Classic mendukung rentang alamat IPv6: /24, /32, /48, /56, /64, dan /128. Untuk informasi lebih lanjut tentang notasi CIDR, lihat entri Wikipedia Classless Inter-Domain Routing.

6. Pilih Tambahkan alamat atau rentang IP lain.
7. Jika Anda ingin menambahkan alamat atau rentang IP lain, ulangi langkah 5 dan 6.
8. Setelah selesai menambahkan nilai, pilih Create IP match condition.

Mengedit kondisi pencocokan IP

Anda dapat menambahkan rentang alamat IP ke kondisi pencocokan IP atau menghapus rentang. Untuk mengubah rentang, tambahkan yang baru dan hapus yang lama.

Untuk mengedit kondisi kecocokan IP

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Di panel navigasi, pilih alamat IP.
3. Di panel kondisi pencocokan IP, pilih kondisi pencocokan IP yang ingin Anda edit.
4. Untuk menambahkan rentang alamat IP:

   a. Di panel kanan, pilih Tambahkan alamat atau rentang IP.

   b. Pilih versi IP yang benar dan masukkan rentang alamat IP dengan menggunakan notasi CIDR. Berikut ini adalah beberapa contohnya:

      - Untuk menentukan alamat IPv4 192.0.2.44, masukkan 192.0.2.44/32.
      - Untuk menentukan alamat IPv6 0:0:0:0:0:ffff:c 000:22 c, masukkan 0:0:0:0:0:ffff:c 000:22 c/128.

- Untuk menentukan kisaran alamat IPv4 dari 192.0.2.0 hingga 192.0.2.255, masukkan 192.0.2.0/24.
- Untuk menentukan kisaran alamat IPv6 dari 2620:0: 2 d 0:200:0: 0:0 hingga 2620:0:2 d 0:200: ffff:ffff:ffff:ffff, masukkan 2620:0:2 d 0:200: :/64.

AWS WAF Classic mendukung rentang alamat IPv4: /8 dan rentang apa pun antara /16 hingga /32. AWS WAF Classic mendukung rentang alamat IPv6: /24, /32, /48, /56, /64, dan /128. Untuk informasi lebih lanjut tentang notasi CIDR, lihat entri Wikipedia Classless Inter-Domain Routing.

c. Untuk menambahkan lebih banyak alamat IP, pilih Tambahkan alamat IP lain dan masukkan nilainya.

d. Pilih Tambahkan.

5. Untuk menghapus alamat atau rentang IP:

a. Di panel kanan, pilih nilai yang ingin Anda hapus.

b. Pilih Hapus alamat atau rentang IP.

Menghapus kondisi pencocokan IP

Jika Anda ingin menghapus kondisi kecocokan IP, Anda harus terlebih dahulu menghapus semua alamat IP dan rentang dalam kondisi dan menghapus kondisi dari semua aturan yang menggunakannya, seperti yang dijelaskan dalam prosedur berikut.

Untuk menghapus kondisi kecocokan IP

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.

2. Di panel navigasi, pilih alamat IP.
3. Di panel kondisi pencocokan IP, pilih kondisi pencocokan IP yang ingin Anda hapus.
4. Di panel kanan, pilih tab Aturan.

   Jika daftar aturan yang menggunakan kondisi pencocokan IP ini kosong, lanjutkan ke langkah 6. Jika daftar berisi aturan apa pun, catat aturannya, dan lanjutkan dengan langkah 5.

5. Untuk menghapus kondisi kecocokan IP dari aturan yang menggunakannya, lakukan langkah-langkah berikut:

   a. Di panel navigasi, pilih Aturan.

   b. Pilih nama aturan yang menggunakan kondisi pencocokan IP yang ingin Anda hapus.

   c. Di panel kanan, pilih kondisi pencocokan IP yang ingin Anda hapus dari aturan, dan pilih Hapus kondisi yang dipilih.

   d. Ulangi langkah b dan c untuk semua aturan yang tersisa yang menggunakan kondisi pencocokan IP yang ingin Anda hapus.

   e. Di panel navigasi, pilih kondisi pencocokan IP.

   f. Di panel kondisi pencocokan IP, pilih kondisi pencocokan IP yang ingin Anda hapus.

6. Pilih Hapus untuk menghapus kondisi yang dipilih.

Bekerja dengan kondisi kecocokan geografis

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Jika Anda ingin mengizinkan atau memblokir permintaan web berdasarkan negara asal permintaan tersebut, buat satu atau beberapa kondisi kecocokan geografis. Kondisi geo match mencantumkan negara tempat permintaan Anda berasal. Kemudian dalam proses, ketika Anda membuat ACL web, Anda menentukan apakah akan mengizinkan atau memblokir permintaan dari negara-negara tersebut.

Anda dapat menggunakan kondisi pencocokan geografis dengan kondisi atau aturan AWS WAF Klasik lainnya untuk membuat pemfilteran canggih. Misalnya, jika Anda ingin memblokir negara tertentu, tetapi masih mengizinkan alamat IP tertentu dari negara tersebut, Anda dapat membuat aturan yang berisi kondisi geo match dan kondisi pencocokan IP. Konfigurasikan aturan untuk memblokir permintaan yang berasal dari negara tersebut dan tidak cocok dengan alamat IP yang disetujui. Sebagai contoh lain, jika Anda ingin memprioritaskan sumber daya untuk pengguna di

negara tertentu, Anda dapat menyertakan kondisi kecocokan geografis dalam dua aturan berbasis tarif yang berbeda. Tetapkan batas tarif yang lebih tinggi untuk pengguna di negara pilihan dan tetapkan batas tarif yang lebih rendah untuk semua pengguna lain.

> **Note**
>
> Jika Anda menggunakan fitur pembatasan CloudFront geografis untuk memblokir suatu negara agar tidak mengakses konten Anda, permintaan apa pun dari negara tersebut akan diblokir dan tidak diteruskan ke Classic. AWS WAF Jadi jika Anda ingin mengizinkan atau memblokir permintaan berdasarkan geografi ditambah kondisi AWS WAF Klasik lainnya, Anda tidak boleh menggunakan fitur pembatasan CloudFront geografis. Sebagai gantinya, Anda harus menggunakan kondisi kecocokan geografis AWS WAF Klasik.

Topik

Membuat kondisi geo match

Jika Anda ingin mengizinkan beberapa permintaan web dan memblokir yang lain berdasarkan negara asal permintaan tersebut, buat kondisi kecocokan geografis untuk negara yang ingin Anda izinkan dan kondisi kecocokan geografis lainnya untuk negara yang ingin Anda blokir.

> **Note**
>
> Saat menambahkan kondisi geo match ke aturan, Anda juga dapat mengonfigurasi AWS WAF Classic untuk mengizinkan atau memblokir permintaan web yang tidak berasal dari negara yang Anda tentukan dalam kondisi tersebut.

Untuk membuat kondisi geo match

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.

2. Di panel navigasi, pilih Geo match.
3. Pilih Buat kondisi.
4. Masukkan nama di bidang Nama.

   Nama hanya dapat berisi karakter alfanumerik (A-Z, a-z, 0-9) atau karakter khusus berikut: _-!” #` +*}, ./. Anda tidak dapat mengubah nama kondisi setelah Anda membuatnya.
5. Pilih Wilayah.
6. Pilih jenis Lokasi dan negara. Jenis lokasi saat ini hanya bisa Negara.
7. Pilih Tambahkan lokasi.
8. Pilih Buat.

Mengedit kondisi geo match

Anda dapat menambahkan negara ke atau menghapus negara dari kondisi geo match Anda.

Untuk mengedit kondisi kecocokan geografis

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Di panel navigasi, pilih Geo match.
3. Di panel Geo match conditions, pilih kondisi geo match yang ingin Anda edit.
4. Untuk menambahkan negara:
   a. Di panel kanan, pilih Tambahkan filter.
   b. Pilih jenis Lokasi dan negara. Jenis lokasi saat ini hanya bisa Negara.
   c. Pilih Tambahkan.
5. Untuk menghapus suatu negara:
   a. Di panel kanan, pilih nilai yang ingin Anda hapus.
   b. Pilih Hapus filter.

Menghapus kondisi geo match

Jika Anda ingin menghapus kondisi geo match, Anda harus terlebih dahulu menghapus semua negara dalam kondisi dan menghapus kondisi dari semua aturan yang menggunakannya, seperti yang dijelaskan dalam prosedur berikut.

Untuk menghapus kondisi kecocokan geografis

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Hapus kondisi geo match dari aturan yang menggunakannya:
   a. Di panel navigasi, pilih Aturan.
   b. Pilih nama aturan yang menggunakan kondisi geo match yang ingin Anda hapus.
   c. Di panel kanan, pilih Edit aturan.
   d. Pilih X di sebelah kondisi yang ingin Anda hapus.
   e. Pilih Perbarui.
   f. Ulangi untuk semua aturan yang tersisa yang menggunakan kondisi geo match yang ingin Anda hapus.
3. Hapus filter dari kondisi yang ingin Anda hapus:
   a. Di panel navigasi, pilih Geo match.
   b. Pilih nama kondisi geo match yang ingin Anda hapus.
   c. Di panel kanan, pilih kotak centang di sebelah Filter untuk memilih semua filter.
   d. Pilih filter Hapus.
4. Di panel navigasi, pilih Geo match.
5. Di panel Geo match conditions, pilih kondisi geo match yang ingin Anda hapus.
6. Pilih Hapus untuk menghapus kondisi yang dipilih.

Bekerja dengan kondisi kendala ukuran

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Jika Anda ingin mengizinkan atau memblokir permintaan web berdasarkan panjang bagian permintaan yang ditentukan, buat satu atau lebih kondisi batasan ukuran. Kondisi batasan ukuran mengidentifikasi bagian permintaan web yang ingin dilihat AWS WAF Classic, jumlah byte yang ingin dicari AWS WAF Classic, dan operator, seperti lebih besar dari (>) atau kurang dari (<). Misalnya, Anda dapat menggunakan kondisi batasan ukuran untuk mencari string kueri yang lebih panjang dari 100 byte. Kemudian dalam proses, ketika Anda membuat ACL web, Anda menentukan apakah akan mengizinkan atau memblokir permintaan berdasarkan pengaturan tersebut.

Perhatikan bahwa jika Anda mengonfigurasi AWS WAF Classic untuk memeriksa isi permintaan, misalnya, dengan mencari isi untuk string tertentu, AWS WAF Classic hanya memeriksa 8192 byte pertama (8 KB). Jika badan permintaan untuk permintaan web Anda tidak akan pernah melebihi 8192 byte, Anda dapat membuat kondisi batasan ukuran dan memblokir permintaan yang memiliki badan permintaan lebih besar dari 8192 byte.

Topik

Membuat kondisi kendala ukuran

Saat Anda membuat kondisi batasan ukuran, Anda menentukan filter yang mengidentifikasi bagian permintaan web yang Anda inginkan AWS WAF Classic untuk mengevaluasi panjangnya. Anda dapat menambahkan lebih dari satu filter ke kondisi batasan ukuran, atau Anda dapat membuat kondisi terpisah untuk setiap filter. Inilah cara setiap konfigurasi memengaruhi perilaku AWS WAF Klasik:

- Satu filter per kondisi kendala ukuran — Saat Anda menambahkan kondisi batasan ukuran terpisah ke aturan dan menambahkan aturan ke ACL web, permintaan web harus cocok dengan semua kondisi untuk AWS WAF Classic untuk mengizinkan atau memblokir permintaan berdasarkan kondisi.

  Misalnya, Anda membuat dua kondisi. Satu cocok dengan permintaan web yang string kuerinya lebih besar dari 100 byte. Yang lain cocok dengan permintaan web yang badan permintaannya lebih besar dari 1024 byte. Saat Anda menambahkan kedua kondisi ke aturan yang sama dan menambahkan aturan ke ACL web, AWS WAF Classic mengizinkan atau memblokir permintaan hanya jika kedua kondisi benar.
- Lebih dari satu filter per kondisi batasan ukuran — Saat Anda menambahkan kondisi batasan ukuran yang berisi beberapa filter ke aturan dan menambahkan aturan ke ACL web, permintaan web hanya perlu mencocokkan salah satu filter dalam kondisi batasan ukuran untuk AWS WAF Classic untuk mengizinkan atau memblokir permintaan berdasarkan kondisi tersebut.

  Misalkan Anda membuat satu kondisi, bukan dua, dan satu kondisi berisi dua filter yang sama seperti pada contoh sebelumnya. AWS WAF Classic memungkinkan atau memblokir permintaan jika string kueri lebih besar dari 100 byte atau badan permintaan lebih besar dari 1024 byte.

> **Note**
>
> Saat menambahkan kondisi batasan ukuran ke aturan, Anda juga dapat mengonfigurasi AWS WAF Classic untuk mengizinkan atau memblokir permintaan web yang tidak cocok dengan nilai dalam kondisi tersebut.

Untuk membuat kondisi kendala ukuran

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Di panel navigasi, pilih Kendala ukuran.
3. Pilih Buat kondisi.
4. Tentukan pengaturan filter yang berlaku. Untuk informasi selengkapnya, lihat Nilai yang Anda tentukan saat Anda membuat atau mengedit kondisi batasan ukuran.
5. Pilih Tambahkan filter lain.

6. Jika Anda ingin menambahkan filter lain, ulangi langkah 4 dan 5.
7. Setelah selesai menambahkan filter, pilih Buat kondisi batasan ukuran.

Nilai yang Anda tentukan saat Anda membuat atau mengedit kondisi batasan ukuran

Saat Anda membuat atau memperbarui kondisi batasan ukuran, Anda menentukan nilai berikut:

Nama

Masukkan nama untuk kondisi batasan ukuran.

Nama hanya dapat berisi karakter alfanumerik (A-Z, a-z, 0-9) atau karakter khusus berikut: _-!” #` +*}, ./. Anda tidak dapat mengubah nama kondisi setelah Anda membuatnya.

Bagian dari permintaan untuk memfilter

Pilih bagian dari setiap permintaan web yang Anda inginkan AWS WAF Classic untuk mengevaluasi panjangnya:

Header

Header permintaan tertentu, misalnya, `Referer` header `User-Agent` atau. Jika Anda memilih Header, tentukan nama header di bidang Header.

Metode HTTP

Metode HTTP, yang menunjukkan jenis operasi yang diminta permintaan asal untuk dilakukan. CloudFront mendukung metode berikut:`DELETE`,`GET`,`HEAD`,`OPTIONS`,`PATCH`,`POST`, dan`PUT`.

String kueri

Bagian dari URL yang muncul setelah ? karakter, jika ada.

URI

Jalur URI permintaan, yang mengidentifikasi sumber daya, misalnya,`/images/daily-ad.jpg`. Ini tidak termasuk string kueri atau komponen fragmen URI. Untuk selengkapnya, lihat Uniform Resource Identifier (URI): Generic Syntax.

Kecuali Transformasi ditentukan, URI tidak dinormalisasi dan diperiksa sama seperti AWS menerimanya dari klien sebagai bagian dari permintaan. Transformasi akan memformat ulang URI seperti yang ditentukan.

Tubuh

Bagian dari permintaan yang berisi data tambahan yang ingin Anda kirim ke server web Anda sebagai badan permintaan HTTP, seperti data dari formulir.

Parameter kueri tunggal (hanya nilai)

Parameter apa pun yang telah Anda definisikan sebagai bagian dari string kueri. Misalnya, jika URL-nya adalah “www.xyz.com? UserName =abc& SalesRegion =seattle” Anda dapat menambahkan filter ke parameter atau. UserNameSalesRegion

Jika Anda memilih Parameter kueri tunggal (hanya nilai), Anda juga akan menentukan nama parameter Kueri. Ini adalah parameter dalam string kueri yang akan Anda periksa, seperti UserName. Panjang maksimum untuk nama parameter Query adalah 30 karakter. Nama parameter kueri tidak peka huruf besar/kecil. Misalnya, Anda menentukan UserNamesebagai nama parameter Query, ini akan cocok dengan semua variasi UserName, seperti username dan UserName.

Semua parameter kueri (hanya nilai)

Mirip dengan Parameter kueri tunggal (hanya nilai), tetapi alih-alih memeriksa nilai parameter tunggal, AWS WAF Classic memeriksa nilai semua parameter dalam string kueri untuk batasan ukuran. Misalnya, jika URL adalah “www.xyz.com? UserName =abc& SalesRegion =seattle,” dan Anda memilih Semua parameter kueri (hanya nilai), AWS WAF Klasik akan memicu kecocokan nilai jika salah satu atau melebihi ukuran yang ditentukan. UserNameSalesRegion

Header (Hanya Ketika “Bagian dari permintaan untuk memfilter” adalah “Header”)

Jika Anda memilih Header untuk Bagian dari permintaan untuk difilter, pilih header dari daftar header umum, atau ketik nama header yang Anda inginkan AWS WAF Classic untuk mengevaluasi panjangnya.

Operator perbandingan

Pilih bagaimana Anda ingin AWS WAF Classic mengevaluasi panjang string kueri dalam permintaan web sehubungan dengan nilai yang Anda tentukan untuk Ukuran.

Misalnya, jika Anda memilih Lebih besar dari operator Perbandingan dan ketik 100 untuk Ukuran, AWS WAF Classic mengevaluasi permintaan web untuk string kueri yang lebih panjang dari 100 byte.

Ukuran

Masukkan panjang, dalam byte, yang Anda ingin AWS WAF Classic perhatikan dalam string kueri.

> **Note**
>
> Jika Anda memilih URI untuk nilai Bagian dari permintaan untuk difilter,/dalam URI dihitung sebagai satu karakter. Misalnya, jalur `/logo.jpg` URI memiliki panjang sembilan karakter.

Transformasi

Transformasi memformat ulang permintaan web sebelum AWS WAF Classic mengevaluasi panjang bagian permintaan yang ditentukan. Ini menghilangkan beberapa format yang tidak biasa yang digunakan penyerang dalam permintaan web dalam upaya untuk melewati AWS WAF Classic.

> **Note**
>
> Jika Anda memilih Body for Part dari permintaan untuk difilter, Anda tidak dapat mengonfigurasi AWS WAF Classic untuk melakukan transformasi karena hanya 8192 byte pertama yang diteruskan untuk diperiksa. Namun, Anda masih dapat memfilter lalu lintas berdasarkan ukuran badan permintaan HTTP dan menentukan transformasi None. (AWS WAF Klasik mendapatkan panjang badan dari header permintaan.)

Anda hanya dapat menentukan satu jenis transformasi teks.

Transformasi dapat melakukan operasi berikut:

Tidak ada

AWS WAF Classic tidak melakukan transformasi teks apa pun pada permintaan web sebelum memeriksa panjangnya.

Mengkonversi ke lowercase

AWS WAF Klasik mengkonversi huruf besar (A-Z) ke huruf kecil (a-z).

Dekode HTML

AWS WAF Klasik menggantikan karakter yang dikodekan HTML dengan karakter yang tidak dikodekan:

- Mengganti `&quot;` dengan &
- Mengganti ` ` dengan ruang yang tidak pecah
- Mengganti `<` dengan <
- Mengganti `>` dengan >
- Mengganti karakter yang diwakili dalam format heksadesimal, `&#xhhhh;`, dengan karakter yang sesuai
- Mengganti karakter yang diwakili dalam format desimal, `&#nnnn;`, dengan karakter yang sesuai

Menormalkan ruang putih

AWS WAF Klasik menggantikan karakter berikut dengan karakter spasi (desimal 32):

- \ f, formfeed, desimal 12
- \ t, tab, desimal 9
- \ n, baris baru, desimal 10
- \ r, pengembalian pengangkutan, desimal 13
- \ v, tab vertikal, desimal 11
- spasi tanpa pindah baris, desimal 160

Selain itu, opsi ini menggantikan beberapa spasi dengan satu spasi.

Sederhanakan baris perintah

Untuk permintaan yang berisi perintah baris perintah sistem operasi, gunakan opsi ini untuk melakukan transformasi berikut:

- Menghapus karakter berikut: \ " ' ^
- Menghapus spasi sebelum karakter berikut: / (
- Mengganti karakter berikut dengan spasi: , ;
- Mengganti spasi ganda dengan satu spasi
- Mengonversi huruf besar (A-Z) ke huruf kecil (a-z)

Dekode URL

Memecahkan kode permintaan yang dikodekan URL.

Menambahkan dan menghapus filter dalam kondisi batasan ukuran

Anda dapat menambahkan atau menghapus filter dalam kondisi batasan ukuran. Untuk mengubah filter, tambahkan yang baru dan hapus yang lama.

Untuk menambah atau menghapus filter dalam kondisi batasan ukuran

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Di panel navigasi, pilih Size constraint.
3. Pilih kondisi yang ingin Anda tambahkan atau hapus filter.
4. Untuk menambahkan filter, lakukan langkah-langkah berikut:
   a. Pilih Tambahkan filter.
   b. Tentukan pengaturan filter yang berlaku. Untuk informasi selengkapnya, lihat Nilai yang Anda tentukan saat Anda membuat atau mengedit kondisi batasan ukuran.
   c. Pilih Tambahkan.
5. Untuk menghapus filter, lakukan langkah-langkah berikut:
   a. Pilih filter yang ingin Anda hapus.
   b. Pilih Hapus filter.

Menghapus kondisi kendala ukuran

Jika Anda ingin menghapus kondisi batasan ukuran, Anda harus terlebih dahulu menghapus semua filter dalam kondisi dan menghapus kondisi dari semua aturan yang menggunakannya, seperti yang dijelaskan dalam prosedur berikut.

Untuk menghapus kondisi batasan ukuran

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.

2. Di panel navigasi, pilih Kendala ukuran.
3. Di panel Kondisi batasan ukuran, pilih kondisi batasan ukuran yang ingin Anda hapus.
4. Di panel kanan, pilih tab Aturan terkait.

   Jika daftar aturan yang menggunakan kondisi batasan ukuran ini kosong, lanjutkan ke langkah 6. Jika daftar berisi aturan apa pun, catat aturannya, dan lanjutkan dengan langkah 5.
5. Untuk menghapus kondisi batasan ukuran dari aturan yang menggunakannya, lakukan langkah-langkah berikut:

   a. Di panel navigasi, pilih Aturan.

   b. Pilih nama aturan yang menggunakan kondisi batasan ukuran yang ingin Anda hapus.

   c. Di panel kanan, pilih kondisi batasan ukuran yang ingin Anda hapus dari aturan, lalu pilih Hapus kondisi yang dipilih.

   d. Ulangi langkah b dan c untuk semua aturan yang tersisa yang menggunakan kondisi batasan ukuran yang ingin Anda hapus.

   e. Di panel navigasi, pilih Size constraint.

   f. Di panel Kondisi batasan ukuran, pilih kondisi batasan ukuran yang ingin Anda hapus.
6. Pilih Hapus untuk menghapus kondisi yang dipilih.

Bekerja dengan kondisi kecocokan injeksi SQL

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Penyerang terkadang menyisipkan kode SQL berbahaya ke dalam permintaan web sebagai upaya untuk mengekstrak data dari basis data Anda. Untuk mengizinkan atau memblokir permintaan web yang tampak berisi kode SQL berbahaya, buatlah satu atau beberapa injeksi SQL yang cocok

dengan kondisi. Kondisi kecocokan injeksi SQL mengidentifikasi bagian dari permintaan web, seperti jalur URI atau string kueri, yang ingin Anda periksa AWS WAF Classic. Kemudian dalam prosesnya, ketika Anda membuat ACL web, Anda menentukan apakah akan mengizinkan atau memblokir permintaan yang tampak berisi kode SQL berbahaya.

Topik

Membuat kondisi kecocokan injeksi SQL

Saat membuat kondisi kecocokan injeksi SQL, Anda menentukan filter, yang menunjukkan bagian permintaan web yang ingin AWS WAF Classic periksa untuk kode SQL berbahaya, seperti URI atau string kueri. Anda dapat menambahkan lebih dari satu filter ke kondisi kecocokan injeksi SQL, atau Anda dapat membuat kondisi terpisah untuk setiap filter. Inilah cara setiap konfigurasi memengaruhi perilaku AWS WAF Klasik:

- Lebih dari satu filter per kondisi kecocokan injeksi SQL (disarankan) - Saat Anda menambahkan kondisi kecocokan injeksi SQL yang berisi beberapa filter ke aturan dan menambahkan aturan ke ACL web, permintaan web hanya perlu mencocokkan salah satu filter dalam kondisi kecocokan injeksi SQL untuk AWS WAF Classic untuk mengizinkan atau memblokir permintaan berdasarkan kondisi tersebut.

  Misalnya, Anda membuat satu kondisi kecocokan injeksi SQL, dan kondisinya berisi dua filter. Satu filter menginstruksikan AWS WAF Classic untuk memeriksa URI untuk kode SQL berbahaya, dan yang lainnya menginstruksikan AWS WAF Classic untuk memeriksa string kueri. AWS WAF Classic memungkinkan atau memblokir permintaan jika tampaknya berisi kode SQL berbahaya baik di URI atau dalam string kueri.
- Satu filter per kondisi kecocokan injeksi SQL — Saat Anda menambahkan kondisi kecocokan injeksi SQL terpisah ke aturan dan menambahkan aturan ke ACL web, permintaan web harus cocok dengan semua kondisi untuk AWS WAF Classic untuk mengizinkan atau memblokir permintaan berdasarkan kondisi.

  Misalkan Anda membuat dua kondisi, dan setiap kondisi berisi salah satu dari dua filter dalam contoh sebelumnya. Saat Anda menambahkan kedua kondisi ke aturan yang sama dan

menambahkan aturan ke ACL web, AWS WAF Classic mengizinkan atau memblokir permintaan hanya ketika URI dan string kueri tampaknya berisi kode SQL berbahaya.

> **Note**
>
> Saat menambahkan kondisi kecocokan injeksi SQL ke aturan, Anda juga dapat mengonfigurasi AWS WAF Classic untuk mengizinkan atau memblokir permintaan web yang tampaknya tidak mengandung kode SQL berbahaya.

Untuk membuat kondisi kecocokan injeksi SQL

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Di panel navigasi, pilih injeksi SQL.
3. Pilih Buat kondisi.
4. Tentukan pengaturan filter yang berlaku. Untuk informasi selengkapnya, lihat Nilai yang Anda tentukan saat membuat atau mengedit kondisi kecocokan injeksi SQL.
5. Pilih Tambahkan filter lain.
6. Jika Anda ingin menambahkan filter lain, ulangi langkah 4 dan 5.
7. Setelah selesai menambahkan filter, pilih Buat.

Nilai yang Anda tentukan saat membuat atau mengedit kondisi kecocokan injeksi SQL

Saat Anda membuat atau memperbarui kondisi kecocokan injeksi SQL, Anda menentukan nilai berikut:

Nama

Nama kondisi kecocokan injeksi SQL.

Nama hanya dapat berisi karakter alfanumerik (A-Z, a-z, 0-9) atau karakter khusus berikut: _-!” #` +*}, ./. Anda tidak dapat mengubah nama kondisi setelah Anda membuatnya.

Bagian dari permintaan untuk memfilter

Pilih bagian dari setiap permintaan web yang Anda ingin AWS WAF Classic untuk memeriksa kode SQL berbahaya:

Header

Header permintaan tertentu, misalnya, `Referer` header `User-Agent` atau. Jika Anda memilih Header, tentukan nama header di bidang Header.

Metode HTTP

Metode HTTP, yang menunjukkan jenis operasi yang diminta permintaan asal untuk dilakukan. CloudFront mendukung metode berikut:`DELETE`,`GET`,`HEAD`,`OPTIONS`,`PATCH`,`POST`, dan`PUT`.

String kueri

Bagian dari URL yang muncul setelah `?` karakter, jika ada.

> **Note**
>
> Untuk kondisi kecocokan injeksi SQL, kami sarankan Anda memilih Semua parameter kueri (hanya nilai) alih-alih String kueri untuk Bagian dari permintaan untuk memfilter.

URI

Jalur URI permintaan, yang mengidentifikasi sumber daya, misalnya,`/images/daily-ad.jpg`. Ini tidak termasuk string kueri atau komponen fragmen URI. Untuk selengkapnya, lihat Uniform Resource Identifier (URI): Generic Syntax.

Kecuali Transformasi ditentukan, URI tidak dinormalisasi dan diperiksa sama seperti AWS menerimanya dari klien sebagai bagian dari permintaan. Transformasi akan memformat ulang URI seperti yang ditentukan.

Tubuh

Bagian dari permintaan yang berisi data tambahan yang ingin Anda kirim ke server web Anda sebagai badan permintaan HTTP, seperti data dari formulir.

> **Note**
>
> Jika Anda memilih Body untuk nilai Bagian dari permintaan untuk difilter, AWS WAF Classic hanya memeriksa 8192 byte pertama (8 KB). Untuk mengizinkan atau

memblokir permintaan yang badannya lebih panjang dari 8192 byte, Anda dapat membuat kondisi batasan ukuran. (AWS WAF Klasik mendapatkan panjang badan dari header permintaan.) Untuk informasi selengkapnya, lihat Bekerja dengan kondisi kendala ukuran.

Parameter kueri tunggal (hanya nilai)

Parameter apa pun yang telah Anda definisikan sebagai bagian dari string kueri. Misalnya, jika URL-nya adalah “www.xyz.com? UserName =abc& SalesRegion =seattle” Anda dapat menambahkan filter ke parameter atau. UserNameSalesRegion

Jika Anda memilih Parameter kueri tunggal (hanya nilai) Anda juga akan menentukan nama parameter Kueri. Ini adalah parameter dalam string kueri yang akan Anda periksa, seperti UserNameatau SalesRegion. Panjang maksimum untuk nama parameter Query adalah 30 karakter. Nama parameter kueri tidak peka huruf besar/kecil. Misalnya, Anda menentukan UserNamesebagai nama parameter Query, ini akan cocok dengan semua variasi UserName, seperti username dan UserName.

Semua parameter kueri (hanya nilai)

Mirip dengan Parameter kueri tunggal (hanya nilai), tetapi daripada memeriksa nilai parameter tunggal, AWS WAF Classic memeriksa nilai semua parameter dalam string kueri untuk kemungkinan kode SQL berbahaya. Misalnya, jika URL adalah “www.xyz.com? UserName =abc& SalesRegion =seattle,” dan Anda memilih Semua parameter kueri (hanya nilai), AWS WAF Classic akan memicu kecocokan jika nilai salah satu atau mengandung kemungkinan kode SQL berbahaya. UserNameSalesRegion

Header

Jika Anda memilih Header untuk Bagian dari permintaan untuk difilter, pilih header dari daftar header umum, atau masukkan nama header yang Anda ingin AWS WAF Classic untuk memeriksa kode SQL berbahaya.

Transformasi

Transformasi memformat ulang permintaan web sebelum AWS WAF Classic memeriksa permintaan. Ini menghilangkan beberapa format yang tidak biasa yang digunakan penyerang dalam permintaan web dalam upaya untuk melewati AWS WAF Classic.

Anda hanya dapat menentukan satu jenis transformasi teks.

Transformasi dapat melakukan operasi berikut:

Tidak ada

AWS WAF Classic tidak melakukan transformasi teks apa pun pada permintaan web sebelum memeriksanya agar string di Nilai cocok.

Mengkonversi ke lowercase

AWS WAF Klasik mengkonversi huruf besar (A-Z) ke huruf kecil (a-z).

Dekode HTML

AWS WAF Klasik menggantikan karakter yang dikodekan HTML dengan karakter yang tidak dikodekan:

- Mengganti `&quot;` dengan &
- Mengganti ` ` dengan ruang yang tidak pecah
- Mengganti `<` dengan <
- Mengganti `>` dengan >
- Mengganti karakter yang diwakili dalam format heksadesimal, `&#xhhhh;`, dengan karakter yang sesuai
- Mengganti karakter yang diwakili dalam format desimal, `&#nnnn;`, dengan karakter yang sesuai

Menormalkan ruang putih

AWS WAF Klasik menggantikan karakter berikut dengan karakter spasi (desimal 32):

- \ f, formfeed, desimal 12
- \ t, tab, desimal 9
- \ n, baris baru, desimal 10
- \ r, pengembalian pengangkutan, desimal 13
- \ v, tab vertikal, desimal 11
- spasi tanpa pindah baris, desimal 160

Selain itu, opsi ini menggantikan beberapa spasi dengan satu spasi.

Sederhanakan baris perintah

Untuk permintaan yang berisi perintah baris perintah sistem operasi, gunakan opsi ini untuk melakukan transformasi berikut:

- Menghapus karakter berikut: \ " ' ^

- Menghapus spasi sebelum karakter berikut: / (
- Mengganti karakter berikut dengan spasi: , ;
- Mengganti spasi ganda dengan satu spasi
- Mengonversi huruf besar (A-Z) ke huruf kecil (a-z)

Dekode URL

Mendekode permintaan yang dikodekan URL.

Menambahkan dan menghapus filter dalam kondisi kecocokan injeksi SQL

Anda dapat menambahkan atau menghapus filter dalam kondisi kecocokan injeksi SQL. Untuk mengubah filter, tambahkan yang baru dan hapus yang lama.

Untuk menambah atau menghapus filter dalam kondisi kecocokan injeksi SQL

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Di panel navigasi, pilih injeksi SQL.
3. Pilih kondisi yang ingin Anda tambahkan atau hapus filter.
4. Untuk menambahkan filter, lakukan langkah-langkah berikut:

   a. Pilih Tambahkan filter.
   b. Tentukan pengaturan filter yang berlaku. Untuk informasi selengkapnya, lihat Nilai yang Anda tentukan saat membuat atau mengedit kondisi kecocokan injeksi SQL.
   c. Pilih Tambahkan.
5. Untuk menghapus filter, lakukan langkah-langkah berikut:

   a. Pilih filter yang ingin Anda hapus.
   b. Pilih Hapus filter.

Menghapus kondisi kecocokan injeksi SQL

Jika Anda ingin menghapus kondisi kecocokan injeksi SQL, Anda harus terlebih dahulu menghapus semua filter dalam kondisi dan menghapus kondisi dari semua aturan yang menggunakannya, seperti yang dijelaskan dalam prosedur berikut.

Untuk menghapus kondisi kecocokan injeksi SQL

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Di panel navigasi, pilih injeksi SQL.
3. Di panel kondisi kecocokan injeksi SQL, pilih kondisi kecocokan injeksi SQL yang ingin Anda hapus.
4. Di panel kanan, pilih tab Aturan terkait.

   Jika daftar aturan yang menggunakan kondisi kecocokan injeksi SQL ini kosong, lanjutkan ke langkah 6. Jika daftar berisi aturan, catat aturan, dan lanjutkan dengan langkah 5.
5. Untuk menghapus kondisi kecocokan injeksi SQL dari aturan yang menggunakannya, lakukan langkah-langkah berikut:

   a. Di panel navigasi, pilih Aturan.
   b. Pilih nama aturan yang menggunakan kondisi kecocokan injeksi SQL yang ingin Anda hapus.
   c. Di panel kanan, pilih kondisi kecocokan injeksi SQL yang ingin Anda hapus dari aturan, dan pilih Hapus kondisi yang dipilih.
   d. Ulangi langkah b dan c untuk semua aturan yang tersisa yang menggunakan kondisi kecocokan injeksi SQL yang ingin Anda hapus.
   e. Di panel navigasi, pilih injeksi SQL.
   f. Di panel kondisi kecocokan injeksi SQL, pilih kondisi kecocokan injeksi SQL yang ingin Anda hapus.
6. Pilih Hapus untuk menghapus kondisi yang dipilih.

Bekerja dengan kondisi kecocokan string

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF.

Untuk versi terbaru AWS WAF, lihatAWS WAF.

Jika Anda ingin mengizinkan atau memblokir permintaan web berdasarkan string yang muncul dalam permintaan, buat satu atau beberapa kondisi pencocokan string. Kondisi pencocokan string mengidentifikasi string yang ingin Anda cari dan bagian dari permintaan web, seperti header tertentu atau string kueri, yang Anda ingin AWS WAF Classic untuk memeriksa string. Kemudian dalam proses, ketika Anda membuat ACL web, Anda menentukan apakah akan mengizinkan atau memblokir permintaan yang berisi string.

Topik

- Membuat kondisi kecocokan string
- Nilai yang Anda tentukan saat Anda membuat atau mengedit kondisi kecocokan string
- Menambahkan dan menghapus filter dalam kondisi kecocokan string
- Menghapus kondisi kecocokan string

Membuat kondisi kecocokan string

Saat Anda membuat kondisi pencocokan string, Anda menentukan filter yang mengidentifikasi string yang ingin Anda cari dan bagian dari permintaan web yang Anda ingin AWS WAF Classic untuk memeriksa string tersebut, seperti URI atau string kueri. Anda dapat menambahkan lebih dari satu filter ke kondisi kecocokan string, atau Anda dapat membuat kondisi pencocokan string terpisah untuk setiap filter. Inilah cara setiap konfigurasi memengaruhi perilaku AWS WAF Klasik:

- Satu filter per kondisi kecocokan string - Saat Anda menambahkan kondisi pencocokan string terpisah ke aturan dan menambahkan aturan ke ACL web, permintaan web harus cocok dengan semua kondisi untuk AWS WAF Classic untuk mengizinkan atau memblokir permintaan berdasarkan kondisi.

  Misalnya, Anda membuat dua kondisi. Satu cocok dengan permintaan web yang berisi nilai `BadBot` di `User-Agent` header. Yang lain cocok dengan permintaan web yang berisi nilai `BadParameter` dalam string kueri. Saat Anda menambahkan kedua kondisi ke aturan yang sama dan menambahkan aturan ke ACL web, AWS WAF Classic mengizinkan atau memblokir permintaan hanya jika berisi kedua nilai tersebut.
- Lebih dari satu filter per kondisi kecocokan string - Saat Anda menambahkan kondisi kecocokan string yang berisi beberapa filter ke aturan dan menambahkan aturan ke ACL web, permintaan

web hanya perlu mencocokkan salah satu filter dalam kondisi pencocokan string untuk AWS WAF Klasik untuk mengizinkan atau memblokir permintaan berdasarkan satu kondisi.

Misalkan Anda membuat satu kondisi, bukan dua, dan satu kondisi berisi dua filter yang sama seperti pada contoh sebelumnya. AWS WAF Classic memungkinkan atau memblokir permintaan jika berisi baik `BadBot` di `User-Agent` header atau `BadParameter` dalam string kueri.

> **Note**
>
> Saat menambahkan kondisi kecocokan string ke aturan, Anda juga dapat mengonfigurasi AWS WAF Classic untuk mengizinkan atau memblokir permintaan web yang tidak cocok dengan nilai dalam kondisi tersebut.

Untuk membuat kondisi kecocokan string

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Di panel navigasi, pilih String dan regex matching.
3. Pilih Buat kondisi.
4. Tentukan pengaturan filter yang berlaku. Untuk informasi selengkapnya, lihat Nilai yang Anda tentukan saat Anda membuat atau mengedit kondisi kecocokan string.
5. Pilih Tambahkan filter.
6. Jika Anda ingin menambahkan filter lain, ulangi langkah 4 dan 5.
7. Setelah selesai menambahkan filter, pilih Buat.

Nilai yang Anda tentukan saat Anda membuat atau mengedit kondisi kecocokan string

Saat Anda membuat atau memperbarui kondisi kecocokan string, Anda menentukan nilai berikut:

Nama

Masukkan nama untuk kondisi kecocokan string. Nama hanya dapat berisi karakter alfanumerik (A-Z, a-z, 0-9) atau karakter khusus berikut: _-!” #`+*}, ./. Anda tidak dapat mengubah nama kondisi setelah Anda membuatnya.

Tipe

Pilih String match.

Bagian dari permintaan untuk memfilter

Pilih bagian dari setiap permintaan web yang Anda inginkan AWS WAF Classic untuk memeriksa string yang Anda tentukan di Nilai yang cocok:

Header

Sebuah header permintaan tertentu, misalnya, `User-Agent` atau `Referer` header. Jika Anda memilih Header, tentukan nama header di bidang Header.

Metode HTTP

Metode HTTP, yang menunjukkan jenis operasi yang diminta permintaan asal untuk dilakukan. CloudFront mendukung metode berikut:`DELETE`,`GET`,`HEAD`,`OPTIONS`,`PATCH`,`POST`, dan`PUT`.

String kueri

Bagian dari URL yang muncul setelah `?` karakter, jika ada.

URI

Jalur URI permintaan, yang mengidentifikasi sumber daya, misalnya,`/images/daily-ad.jpg`. Ini tidak termasuk string kueri atau komponen fragmen URI. Untuk selengkapnya, lihat Uniform Resource Identifier (URI): Generic Syntax.

Kecuali Transformasi ditentukan, URI tidak dinormalisasi dan diperiksa sama seperti AWS menerimanya dari klien sebagai bagian dari permintaan. Transformasi akan memformat ulang URI seperti yang ditentukan.

Tubuh

Bagian dari permintaan yang berisi data tambahan yang ingin Anda kirim ke server web Anda sebagai badan permintaan HTTP, seperti data dari formulir.

> **Note**
>
> Jika Anda memilih Body untuk nilai Bagian dari permintaan untuk difilter, AWS WAF Classic hanya memeriksa 8192 byte pertama (8 KB). Untuk mengizinkan atau memblokir permintaan yang badannya lebih panjang dari 8192 byte, Anda dapat

membuat kondisi batasan ukuran. (AWS WAF Klasik mendapatkan panjang badan dari header permintaan.) Untuk informasi selengkapnya, lihat Bekerja dengan kondisi kendala ukuran.

Parameter kueri tunggal (hanya nilai)

Parameter apa pun yang telah Anda definisikan sebagai bagian dari string kueri. Misalnya, jika URL-nya adalah “www.xyz.com? UserName =abc& SalesRegion =seattle” Anda dapat menambahkan filter ke parameter atau. UserNameSalesRegion

Jika parameter duplikat muncul dalam string kueri, nilai dievaluasi sebagai “OR.” Artinya, salah satu nilai akan memicu kecocokan. Misalnya, di URL “www.xyz.com? SalesRegion =boston& SalesRegion =seattle”, “boston” atau “seattle” di Value to match akan memicu kecocokan.

Jika Anda memilih Parameter kueri tunggal (hanya nilai) Anda juga akan menentukan nama parameter Kueri. Ini adalah parameter dalam string kueri yang akan Anda periksa, seperti UserNameatau SalesRegion. Panjang maksimum untuk nama parameter Query adalah 30 karakter. Nama parameter kueri tidak peka huruf besar/kecil. Misalnya, Anda menentukan UserNamesebagai nama parameter Query, ini akan cocok dengan semua variasi UserName, seperti username dan UserName.

Semua parameter kueri (hanya nilai)

Mirip dengan Parameter kueri tunggal (hanya nilai), tetapi alih-alih memeriksa nilai parameter tunggal, AWS WAF Classic memeriksa nilai semua parameter dalam string kueri agar Nilai cocok. Misalnya, jika URL adalah “www.xyz.com? UserName =abc& SalesRegion =seattle,” dan Anda memilih Semua parameter kueri (hanya nilai), AWS WAF Klasik akan memicu kecocokan jika nilai salah satu UserNameatau SalesRegionditentukan sebagai Nilai yang cocok.

Header (Hanya Ketika “Bagian dari permintaan untuk memfilter” adalah “Header”)

Jika Anda memilih Header dari Bagian permintaan untuk memfilter pada daftar, pilih header dari daftar header umum, atau masukkan nama header yang ingin Anda periksa AWS WAF Classic.

Jenis kecocokan

Di bagian permintaan yang ingin Anda periksa AWS WAF Classic, pilih di mana string dalam Nilai yang cocok harus muncul agar sesuai dengan filter ini:

Contains

String muncul di mana saja di bagian permintaan yang ditentukan.

Berisi kata

Bagian yang ditentukan dari permintaan web harus menyertakan Nilai yang cocok, dan Nilai yang cocok harus hanya berisi karakter alfanumerik atau garis bawah (A-Z, a-z, 0-9, atau _). Selain itu, Nilai yang cocok harus berupa kata, yang berarti salah satu dari yang berikut:

- Nilai yang cocok persis sama dengan nilai bagian tertentu dari permintaan web, seperti nilai header.
- Nilai yang cocok adalah di awal bagian tertentu dari permintaan web dan diikuti oleh karakter selain karakter alfanumerik atau garis bawah (_), misalnya,. `BadBot;`
- Nilai yang cocok adalah di akhir bagian tertentu dari permintaan web dan didahului oleh karakter selain karakter alfanumerik atau garis bawah (_), misalnya,. `;BadBot`
- Nilai yang cocok berada di tengah bagian tertentu dari permintaan web dan didahului dan diikuti oleh karakter selain karakter alfanumerik atau garis bawah (_), misalnya,. `-BadBot;`

Persis cocok

String dan nilai bagian yang ditentukan dari permintaan identik.

Starts with

String muncul di awal bagian permintaan yang ditentukan.

Ends with

String muncul di akhir bagian permintaan yang ditentukan.

Transformasi

Transformasi memformat ulang permintaan web sebelum AWS WAF Classic memeriksa permintaan. Ini menghilangkan beberapa format yang tidak biasa yang digunakan penyerang dalam permintaan web dalam upaya untuk melewati AWS WAF Classic.

Anda hanya dapat menentukan satu jenis transformasi teks.

Transformasi dapat melakukan operasi berikut:

Tidak ada

AWS WAF Classic tidak melakukan transformasi teks apa pun pada permintaan web sebelum memeriksanya agar string di Nilai cocok.

Mengkonversi ke lowercase

AWS WAF Klasik mengkonversi huruf besar (A-Z) ke huruf kecil (a-z).

Dekode HTML

AWS WAF Klasik menggantikan karakter yang dikodekan HTML dengan karakter yang tidak dikodekan:

- Mengganti `&quot;` dengan &
- Mengganti ` ` dengan ruang yang tidak pecah
- Mengganti `<` dengan <
- Mengganti `>` dengan >
- Mengganti karakter yang diwakili dalam format heksadesimal, `&#xhhhh;`, dengan karakter yang sesuai
- Mengganti karakter yang diwakili dalam format desimal, `&#nnnn;`, dengan karakter yang sesuai

Menormalkan ruang putih

AWS WAF Klasik menggantikan karakter berikut dengan karakter spasi (desimal 32):

- \ f, formfeed, desimal 12
- \ t, tab, desimal 9
- \ n, baris baru, desimal 10
- \ r, pengembalian pengangkutan, desimal 13
- \ v, tab vertikal, desimal 11
- spasi tanpa pindah baris, desimal 160

Selain itu, opsi ini menggantikan beberapa spasi dengan satu spasi.

Sederhanakan baris perintah

Jika Anda khawatir penyerang menyuntikkan perintah baris perintah sistem operasi dan menggunakan pemformatan yang tidak biasa untuk menyamarkan beberapa atau semua perintah, gunakan pilihan ini untuk melakukan perubahan berikut:

- Menghapus karakter berikut: \ " ' ^
- Menghapus spasi sebelum karakter berikut: / (

- Mengganti karakter berikut dengan spasi: , ;
- Mengganti spasi ganda dengan satu spasi
- Mengonversi huruf besar (A-Z) ke huruf kecil (a-z)

Dekode URL

Mendekode permintaan yang dikodekan URL.

Nilai dikodekan base64

Jika nilai dalam Nilai yang cocok dikodekan base64, pilih kotak centang ini. Gunakan pengkodean base64 untuk menentukan karakter yang tidak dapat dicetak, seperti tab dan linefeed, yang disertakan penyerang dalam permintaan mereka.

Nilai untuk dicocokkan

Tentukan nilai yang ingin Anda cari AWS WAF Classic dalam permintaan web. Panjang maksimum adalah 50 byte. Jika Anda mengkodekan nilai base64, panjang maksimum 50-byte berlaku untuk nilai sebelum Anda menyandikannya.

Menambahkan dan menghapus filter dalam kondisi kecocokan string

Anda dapat menambahkan filter ke kondisi kecocokan string atau menghapus filter. Untuk mengubah filter, tambahkan yang baru dan hapus yang lama.

Untuk menambah atau menghapus filter dalam kondisi kecocokan string

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Di panel navigasi, pilih String dan regex matching.
3. Pilih kondisi yang ingin Anda tambahkan atau hapus filter.
4. Untuk menambahkan filter, lakukan langkah-langkah berikut:

   a. Pilih Tambahkan filter.

   b. Tentukan pengaturan filter yang berlaku. Untuk informasi selengkapnya, lihat Nilai yang Anda tentukan saat Anda membuat atau mengedit kondisi kecocokan string.

   c. Pilih Tambahkan.

5. Untuk menghapus filter, lakukan langkah-langkah berikut:

    a. Pilih filter yang ingin Anda hapus.

    b. Pilih Hapus Filter.

Menghapus kondisi kecocokan string

Jika Anda ingin menghapus kondisi kecocokan string, Anda harus terlebih dahulu menghapus semua filter dalam kondisi dan menghapus kondisi dari semua aturan yang menggunakannya, seperti yang dijelaskan dalam prosedur berikut.

Untuk menghapus kondisi kecocokan string

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

    Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.

2. Hapus kondisi kecocokan string dari aturan yang menggunakannya:

    a. Di panel navigasi, pilih Aturan.

    b. Pilih nama aturan yang menggunakan kondisi pencocokan string yang ingin Anda hapus.

    c. Di panel kanan, pilih Edit aturan.

    d. Pilih X di sebelah kondisi yang ingin Anda hapus.

    e. Pilih Perbarui.

    f. Ulangi untuk semua aturan yang tersisa yang menggunakan kondisi pencocokan string yang ingin Anda hapus.

3. Hapus filter dari kondisi yang ingin Anda hapus:

    a. Di panel navigasi, pilih String dan regex matching.

    b. Pilih nama kondisi kecocokan string yang ingin Anda hapus.

    c. Di panel kanan, pilih kotak centang di sebelah Filter untuk memilih semua filter.

    d. Pilih filter Hapus.

4. Di panel navigasi, pilih String dan regex matching.

5. Di panel Kondisi pencocokan String dan regex, pilih kondisi kecocokan string yang ingin Anda hapus.

6. Pilih Hapus untuk menghapus kondisi yang dipilih.

Bekerja dengan kondisi kecocokan regex

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Jika Anda ingin mengizinkan atau memblokir permintaan web berdasarkan string yang cocok dengan pola ekspresi reguler (regex) yang muncul dalam permintaan, buat satu atau beberapa kondisi pencocokan regex. Kondisi pencocokan regex adalah jenis kondisi pencocokan string yang mengidentifikasi pola yang ingin Anda cari dan bagian dari permintaan web, seperti header tertentu atau string kueri, yang Anda ingin AWS WAF Classic untuk memeriksa polanya. Kemudian dalam proses, ketika Anda membuat ACL web, Anda menentukan apakah akan mengizinkan atau memblokir permintaan yang berisi pola.

Topik

- Membuat kondisi kecocokan regex
- Nilai yang Anda tentukan saat membuat atau mengedit kondisi RegEx kecocokan
- Mengedit kondisi kecocokan regex

Membuat kondisi kecocokan regex

Saat membuat kondisi pencocokan regex, Anda menentukan kumpulan pola yang mengidentifikasi string (menggunakan ekspresi reguler) yang ingin Anda cari. Anda kemudian menambahkan set pola tersebut ke filter yang menentukan bagian dari permintaan web yang Anda ingin AWS WAF Classic untuk memeriksa set pola tersebut, seperti URI atau string kueri.

Anda dapat menambahkan beberapa ekspresi reguler ke satu set pola. Jika Anda melakukannya, ekspresi tersebut digabungkan dengan OR. Artinya, permintaan web akan cocok dengan pola yang ditetapkan jika bagian yang sesuai dari permintaan cocok dengan salah satu ekspresi yang terdaftar.

Saat menambahkan kondisi pencocokan regex ke aturan, Anda juga dapat mengonfigurasi AWS WAF Classic untuk mengizinkan atau memblokir permintaan web yang tidak cocok dengan nilai dalam kondisi tersebut.

AWS WAF Klasik mendukung sebagian besar Perl Compatible Regular Expressions (PCRE) standar. Namun, berikut ini tidak didukung:

- Referensi balik dan menangkap subexpressions
- Pernyataan lebar nol yang sewenang-wenang
- Referensi subrutin dan pola rekursif
- Pola bersyarat
- Kata kerja kontrol mundur
- Direktif byte tunggal\ C
- Arahan pencocokan baris baru\ R
- Perintah pengaturan ulang pertandingan dimulai\ K
- Callout dan kode tertanam
- Pengelompokan atom dan kuantifier posesif

Untuk membuat kondisi kecocokan regex

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Di panel navigasi, pilih String dan regex matching.
3. Pilih Buat kondisi.
4. Tentukan pengaturan filter yang berlaku. Untuk informasi selengkapnya, lihat Nilai yang Anda tentukan saat membuat atau mengedit kondisi RegEx kecocokan.
5. Pilih Buat set pola dan tambahkan filter (jika Anda membuat set pola baru) atau Tambahkan filter jika Anda menggunakan kumpulan pola yang ada.
6. Pilih Buat.

Nilai yang Anda tentukan saat membuat atau mengedit kondisi RegEx kecocokan

Saat Anda membuat atau memperbarui kondisi pencocokan regex, Anda menentukan nilai berikut:

Nama

Masukkan nama untuk kondisi kecocokan regex. Nama hanya dapat berisi karakter alfanumerik (A-Z, a-z, 0-9) atau karakter khusus berikut: _-!” #`+*}, ./. Anda tidak dapat mengubah nama kondisi setelah Anda membuatnya.

Tipe

Pilih pertandingan Regex.

Bagian dari permintaan untuk memfilter

Pilih bagian dari setiap permintaan web yang ingin Anda periksa oleh AWS WAF Classic untuk pola yang Anda tentukan di Nilai yang cocok:

Header

Header permintaan tertentu, misalnya, `Referer` header `User-Agent` atau. Jika Anda memilih Header, tentukan nama header di bidang Header.

Metode HTTP

Metode HTTP, yang menunjukkan jenis operasi yang diminta permintaan asal untuk dilakukan. CloudFront mendukung metode berikut:`DELETE`,`GET`,`HEAD`,`OPTIONS`,`PATCH`,`POST`, dan`PUT`.

String kueri

Bagian dari URL yang muncul setelah ? karakter, jika ada.

URI

Jalur URI permintaan, yang mengidentifikasi sumber daya, misalnya,`/images/daily-ad.jpg`. Ini tidak termasuk string kueri atau komponen fragmen URI. Untuk selengkapnya, lihat Uniform Resource Identifier (URI): Generic Syntax.

Kecuali Transformasi ditentukan, URI tidak dinormalisasi dan diperiksa sama seperti AWS menerimanya dari klien sebagai bagian dari permintaan. Transformasi akan memformat ulang URI seperti yang ditentukan.

Tubuh

Bagian dari permintaan yang berisi data tambahan yang ingin Anda kirim ke server web Anda sebagai badan permintaan HTTP, seperti data dari formulir.

> **Note**
>
> Jika Anda memilih Body untuk nilai Bagian dari permintaan untuk difilter, AWS WAF Classic hanya memeriksa 8192 byte pertama (8 KB). Untuk mengizinkan atau memblokir permintaan yang badannya lebih panjang dari 8192 byte, Anda dapat membuat kondisi batasan ukuran. (AWS WAF Klasik mendapatkan panjang badan dari header permintaan.) Untuk informasi selengkapnya, lihat Bekerja dengan kondisi kendala ukuran.

Parameter kueri tunggal (hanya nilai)

Parameter apa pun yang telah Anda definisikan sebagai bagian dari string kueri. Misalnya, jika URL-nya adalah “www.xyz.com? UserName =abc& SalesRegion =seattle” Anda dapat menambahkan filter ke parameter atau. UserNameSalesRegion

Jika parameter duplikat muncul dalam string kueri, nilai dievaluasi sebagai “OR.” Artinya, salah satu nilai akan memicu kecocokan. Misalnya, di URL “www.xyz.com? SalesRegion =boston& SalesRegion =seattle”, pola yang cocok dengan “boston” atau “seattle” di Value to match akan memicu kecocokan.

Jika Anda memilih Parameter kueri tunggal (hanya nilai) Anda juga akan menentukan nama parameter Kueri. Ini adalah parameter dalam string kueri yang akan Anda periksa, seperti UserNameatau SalesRegion. Panjang maksimum untuk nama parameter Query adalah 30 karakter. Nama parameter kueri tidak peka huruf besar/kecil. Misalnya, Anda menentukan UserNamesebagai nama parameter Query, ini akan cocok dengan semua variasi UserName, seperti username dan UserName.

Semua parameter kueri (hanya nilai)

Mirip dengan Parameter kueri tunggal (hanya nilai), tetapi alih-alih memeriksa nilai parameter tunggal, AWS WAF Classic memeriksa nilai semua parameter dalam string kueri untuk pola yang ditentukan dalam Nilai yang cocok. Misalnya, di URL “www.xyz.com? UserName =abc& SalesRegion =seattle”, pola di Value to match yang cocok dengan nilai di atau akan memicu kecocokan. UserNameSalesRegion

Header (Hanya Ketika “Bagian dari permintaan untuk memfilter” adalah “Header”)

Jika Anda memilih Header dari Bagian permintaan untuk memfilter pada daftar, pilih header dari daftar header umum, atau masukkan nama header yang ingin Anda periksa AWS WAF Classic.

Transformasi

Transformasi memformat ulang permintaan web sebelum AWS WAF Classic memeriksa permintaan. Ini menghilangkan beberapa format yang tidak biasa yang digunakan penyerang dalam permintaan web dalam upaya untuk melewati AWS WAF Classic.

Anda hanya dapat menentukan satu jenis transformasi teks.

Transformasi dapat melakukan operasi berikut:

Tidak ada

AWS WAF Classic tidak melakukan transformasi teks apa pun pada permintaan web sebelum memeriksanya agar string di Nilai cocok.

Mengkonversi ke lowercase

AWS WAF Klasik mengkonversi huruf besar (A-Z) ke huruf kecil (a-z).

Dekode HTML

AWS WAF Klasik menggantikan karakter yang dikodekan HTML dengan karakter yang tidak dikodekan:

- Mengganti `&quot;` dengan &
- Mengganti ` ` dengan ruang yang tidak pecah
- Mengganti `<` dengan <
- Mengganti `>` dengan >
- Mengganti karakter yang diwakili dalam format heksadesimal, `&#xhhhh;`, dengan karakter yang sesuai
- Mengganti karakter yang diwakili dalam format desimal, `&#nnnn;`, dengan karakter yang sesuai

Menormalkan ruang putih

AWS WAF Klasik menggantikan karakter berikut dengan karakter spasi (desimal 32):

- \ f, formfeed, desimal 12
- \ t, tab, desimal 9
- \ n, baris baru, desimal 10
- \ r, pengembalian pengangkutan, desimal 13

- \ v, tab vertikal, desimal 11
- spasi tanpa pindah baris, desimal 160

Selain itu, opsi ini menggantikan beberapa spasi dengan satu spasi.

Sederhanakan baris perintah

Jika Anda khawatir penyerang menyuntikkan perintah baris perintah sistem operasi dan menggunakan pemformatan yang tidak biasa untuk menyamarkan beberapa atau semua perintah, gunakan pilihan ini untuk melakukan perubahan berikut:

- Menghapus karakter berikut: \ " ' ^
- Menghapus spasi sebelum karakter berikut: / (
- Mengganti karakter berikut dengan spasi: , ;
- Mengganti spasi ganda dengan satu spasi
- Mengonversi huruf besar (A-Z) ke huruf kecil (a-z)

Dekode URL

Mendekode permintaan yang dikodekan URL.

Pola Regex agar sesuai dengan permintaan

Anda dapat memilih set pola yang ada, atau membuat yang baru. Jika Anda membuat yang baru, tentukan yang berikut ini:

Nama set pola baru

Masukkan nama dan kemudian tentukan pola regex yang ingin Anda cari AWS WAF Classic.

Jika Anda menambahkan beberapa ekspresi reguler ke set pola, ekspresi tersebut digabungkan dengan OR. Artinya, permintaan web akan cocok dengan pola yang ditetapkan jika bagian yang sesuai dari permintaan cocok dengan salah satu ekspresi yang terdaftar.

Panjang maksimum Nilai untuk dicocokkan adalah 70 karakter.

Mengedit kondisi kecocokan regex

Anda dapat membuat perubahan berikut pada kondisi pencocokan regex yang ada:

- Menghapus pola dari set pola yang ada
- Tambahkan pola ke set pola yang ada

- Menghapus filter ke kondisi kecocokan regex yang ada
- Tambahkan filter ke kondisi pencocokan regex yang ada (Anda hanya dapat memiliki satu filter dalam kondisi kecocokan regex. Oleh karena itu, untuk menambahkan filter, Anda harus menghapus filter yang ada terlebih dahulu.)
- Hapus kondisi kecocokan regex yang ada

> **Note**
>
> Anda tidak dapat menambah atau menghapus kumpulan pola dari filter yang ada. Anda harus mengedit set pola, atau menghapus filter dan membuat filter baru dengan set pola baru.

Untuk menghapus pola dari set pola yang ada

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Di panel navigasi, pilih String dan regex matching.
3. Pilih Lihat set pola regex.
4. Pilih nama set pola yang ingin Anda edit.
5. Pilih Edit.
6. Pilih X di sebelah pola yang ingin Anda hapus.
7. Pilih Simpan.

Untuk menambahkan pola ke set pola yang ada

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Di panel navigasi, pilih String dan regex matching.
3. Pilih Lihat set pola regex.
4. Pilih nama pola yang akan diedit.
5. Pilih Edit.

6. Masukkan pola regex baru.
7. Pilih + di sebelah pola baru.
8. Pilih Simpan.

Untuk menghapus filter dari kondisi kecocokan regex yang ada

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Di panel navigasi, pilih String dan regex matching.
3. Pilih nama kondisi dengan filter yang ingin Anda hapus.
4. Pilih kotak di sebelah filter yang ingin Anda hapus.
5. Pilih Hapus filter.

Untuk menghapus kondisi kecocokan regex

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Hapus filter dari kondisi regex. Lihat instruksi Untuk menghapus filter dari kondisi kecocokan regex yang ada untuk melakukan ini.)
3. Hapus kondisi pencocokan regex dari aturan yang menggunakannya:
   a. Di panel navigasi, pilih Aturan.
   b. Pilih nama aturan yang menggunakan kondisi pencocokan regex yang ingin Anda hapus.
   c. Di panel kanan, pilih Edit aturan.
   d. Pilih X di sebelah kondisi yang ingin Anda hapus.
   e. Pilih Perbarui.
   f. Ulangi untuk semua aturan yang tersisa yang menggunakan kondisi pencocokan regex yang ingin Anda hapus.
4. Di panel navigasi, pilih String dan regex matching.
5. Pilih tombol di sebelah kondisi yang ingin Anda hapus.

6. Pilih Hapus.

Untuk menambah atau mengubah filter ke kondisi kecocokan regex yang ada

Anda hanya dapat memiliki satu filter dalam kondisi kecocokan regex. Jika Anda ingin menambah atau mengubah filter, Anda harus terlebih dahulu menghapus filter yang ada.

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Hapus filter dari kondisi regex yang ingin Anda ubah. Lihat instruksi Untuk menghapus filter dari kondisi kecocokan regex yang ada untuk melakukan ini.)
3. Di panel navigasi, pilih String dan regex matching.
4. Pilih nama kondisi yang ingin Anda ubah.
5. Pilih Tambahkan filter.
6. Masukkan nilai yang sesuai untuk filter baru dan pilih Tambah.

Bekerja dengan aturan

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Aturan memungkinkan Anda secara tepat menargetkan permintaan web yang Anda ingin AWS WAF Classic izinkan atau blokir dengan menentukan kondisi yang tepat yang ingin Anda perhatikan oleh AWS WAF Classic. Misalnya, AWS WAF Classic dapat mengawasi alamat IP tempat permintaan berasal, string yang berisi permintaan dan di mana string muncul, dan apakah permintaan tampaknya berisi kode SQL berbahaya.

Topik

- Membuat aturan dan menambahkan kondisi
- Menambahkan dan menghapus kondisi dalam aturan
- Menghapus aturan
- AWS Marketplace kelompok aturan

Membuat aturan dan menambahkan kondisi

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Jika Anda menambahkan lebih dari satu kondisi ke aturan, permintaan web harus cocok dengan semua kondisi untuk AWS WAF Classic untuk mengizinkan atau memblokir permintaan berdasarkan aturan tersebut.

Untuk membuat aturan dan menambahkan kondisi

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Di panel navigasi, pilih Aturan.
3. Pilih Buat aturan.
4. Masukkan nilai berikut:

   Nama

   Masukkan nama.

   CloudWatch nama metrik

   Masukkan nama untuk CloudWatch metrik yang akan dibuat oleh AWS WAF Classic dan akan dikaitkan dengan aturan. Nama hanya dapat berisi karakter alfanumerik (A-Z, a-z, 0-9),

dengan panjang maksimum se128 dan panjang minimum satu. Itu tidak dapat berisi spasi putih atau nama metrik yang dicadangkan untuk AWS WAF Klasik, termasuk “Semua” dan “Default_Action.

Jenis aturan

Pilih salah satu `Regular rule` atau`Rate-based rule`. Aturan berbasis tarif identik dengan aturan reguler, tetapi juga memperhitungkan berapa banyak permintaan yang datang dari alamat IP dalam periode lima menit. Untuk informasi selengkapnya tentang jenis aturan ini, lihatBagaimana AWS WAF Classic bekerja.

Batas tarif

Untuk aturan berbasis tarif, masukkan jumlah maksimum permintaan untuk mengizinkan dalam periode lima menit dari alamat IP yang sesuai dengan ketentuan aturan. Batas tarif harus minimal 100.

Anda dapat menentukan batas tarif saja, atau batas dan kondisi tarif. Jika Anda hanya menentukan batas tarif, AWS WAF tempatkan batas pada semua alamat IP. Jika Anda menentukan batas dan kondisi tarif, AWS WAF tempatkan batas pada alamat IP yang sesuai dengan kondisi.

Ketika alamat IP mencapai ambang batas tingkat, AWS WAF menerapkan tindakan yang ditetapkan (blokir atau hitung) secepat mungkin, biasanya dalam 30 detik. Setelah tindakan dilakukan, jika lima menit berlalu tanpa permintaan dari alamat IP, AWS WAF setel ulang penghitung ke nol.

5. Untuk menambahkan kondisi ke aturan, tentukan nilai berikut:

   Ketika permintaan melakukan/tidak

   Jika Anda ingin AWS WAF Classic mengizinkan atau memblokir permintaan berdasarkan filter dalam suatu kondisi, pilih tidak. Misalnya, jika kondisi pencocokan IP mencakup rentang alamat IP 192.0.2.0/24 dan Anda ingin AWS WAF Classic mengizinkan atau memblokir permintaan yang berasal dari alamat IP tersebut, pilih tidak.

   Jika Anda ingin AWS WAF Classic mengizinkan atau memblokir permintaan berdasarkan kebalikan dari filter dalam suatu kondisi, pilih tidak. Misalnya, jika kondisi pencocokan IP mencakup rentang alamat IP 192.0.2.0/24 dan Anda ingin AWS WAF Classic mengizinkan atau memblokir permintaan yang tidak berasal dari alamat IP tersebut, pilih tidak.

mencocokkan/berasal dari

Pilih jenis kondisi yang ingin Anda tambahkan ke aturan:

- Kondisi pencocokan skrip lintas situs — pilih kecocokan setidaknya satu filter dalam kondisi pencocokan skrip lintas situs
- Ketentuan pencocokan IP - pilih yang berasal dari alamat IP di
- Kondisi kecocokan geografis — pilih yang berasal dari lokasi geografis di
- Kondisi batasan ukuran - pilih kecocokan setidaknya satu filter dalam kondisi batasan ukuran
- Kondisi kecocokan injeksi SQL - pilih kecocokan setidaknya satu filter dalam kondisi kecocokan injeksi SQL
- Kondisi pencocokan string - pilih kecocokan setidaknya salah satu filter dalam kondisi kecocokan string
- Kondisi pencocokan ekspresi reguler - pilih kecocokan setidaknya satu filter dalam kondisi pencocokan regex

nama kondisi

Pilih kondisi yang ingin Anda tambahkan ke aturan. Daftar hanya menampilkan kondisi dari jenis yang Anda pilih pada langkah sebelumnya.

6. Untuk menambahkan kondisi lain ke aturan, pilih Tambahkan kondisi lain, dan ulangi langkah 4 dan 5. Perhatikan hal berikut:

   - Jika Anda menambahkan lebih dari satu kondisi, permintaan web harus cocok dengan setidaknya satu filter di setiap kondisi agar AWS WAF Classic mengizinkan atau memblokir permintaan berdasarkan aturan tersebut
   - Jika Anda menambahkan dua kondisi pencocokan IP ke aturan yang sama, AWS WAF Classic hanya akan mengizinkan atau memblokir permintaan yang berasal dari alamat IP yang muncul di kedua kondisi pencocokan IP

7. Setelah selesai menambahkan kondisi, pilih Buat.

Menambahkan dan menghapus kondisi dalam aturan

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Anda dapat mengubah aturan dengan menambahkan atau menghapus kondisi.

Untuk menambah atau menghapus kondisi dalam aturan

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Di panel navigasi, pilih Aturan.
3. Pilih nama aturan di mana Anda ingin menambah atau menghapus kondisi.
4. Pilih Tambahkan aturan.
5. Untuk menambahkan kondisi, pilih Tambahkan kondisi dan tentukan nilai berikut:

   Ketika permintaan melakukan/tidak

   Jika Anda ingin AWS WAF Classic mengizinkan atau memblokir permintaan berdasarkan filter dalam suatu kondisi, misalnya, permintaan web yang berasal dari kisaran alamat IP 192.0.2.0/24, pilih tidak.

   Jika Anda ingin AWS WAF Classic mengizinkan atau memblokir permintaan berdasarkan kebalikan dari filter dalam suatu kondisi, pilih tidak. Misalnya, jika kondisi pencocokan IP mencakup rentang alamat IP 192.0.2.0/24 dan Anda ingin AWS WAF Classic mengizinkan atau memblokir permintaan yang tidak berasal dari alamat IP tersebut, pilih tidak.

   mencocokkan/berasal dari

   Pilih jenis kondisi yang ingin Anda tambahkan ke aturan:

- Kondisi pencocokan skrip lintas situs — pilih kecocokan setidaknya satu filter dalam kondisi pencocokan skrip lintas situs
- Ketentuan pencocokan IP - pilih yang berasal dari alamat IP di
- Kondisi kecocokan geografis — pilih yang berasal dari lokasi geografis di
- Kondisi batasan ukuran - pilih kecocokan setidaknya satu filter dalam kondisi batasan ukuran
- Kondisi kecocokan injeksi SQL - pilih kecocokan setidaknya satu filter dalam kondisi kecocokan injeksi SQL
- Kondisi pencocokan string - pilih kecocokan setidaknya salah satu filter dalam kondisi kecocokan string
- Kondisi pencocokan ekspresi reguler - pilih kecocokan setidaknya satu filter dalam kondisi pencocokan regex

nama kondisi

Pilih kondisi yang ingin Anda tambahkan ke aturan. Daftar hanya menampilkan kondisi dari jenis yang Anda pilih pada langkah sebelumnya.

6. Untuk menghapus kondisi, pilih X di sebelah kanan nama kondisi
7. Pilih Perbarui.

Menghapus aturan

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Jika Anda ingin menghapus aturan, Anda harus terlebih dahulu menghapus aturan dari ACL web yang menggunakannya dan menghapus kondisi yang termasuk dalam aturan.

Untuk menghapus aturan

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.

2. Untuk menghapus aturan dari ACL web yang menggunakannya, lakukan langkah-langkah berikut untuk masing-masing ACL web:

   a. Di panel navigasi, pilih Web ACL.

   b. Pilih nama ACL web yang menggunakan aturan yang ingin Anda hapus.

   c. Pilih tab Aturan.

   d. Pilih Edit web ACL.

   e. Pilih X di sebelah kanan aturan yang ingin Anda hapus, lalu pilih Perbarui.

3. Di panel navigasi, pilih Aturan.
4. Pilih nama aturan yang ingin Anda hapus.
5. Pilih Hapus.

AWS Marketplace kelompok aturan

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

AWS WAF Classic menyediakan grup AWS Marketplace aturan untuk membantu Anda melindungi sumber daya Anda. AWS Marketplace kelompok aturan adalah kumpulan ready-to-use aturan yang telah ditentukan sebelumnya, yang ditulis dan diperbarui oleh AWS dan perusahaan AWS mitra.

Beberapa grup AWS Marketplace aturan dirancang untuk membantu melindungi jenis aplikasi web tertentu seperti WordPress, Joomla, atau PHP. Kelompok AWS Marketplace aturan lain menawarkan

perlindungan luas terhadap ancaman yang diketahui atau kerentanan aplikasi web umum, seperti yang tercantum dalam OWASP Top 10.

Anda dapat menginstal grup AWS Marketplace aturan tunggal dari AWS mitra pilihan Anda, dan Anda juga dapat menambahkan aturan AWS WAF Klasik khusus Anda sendiri untuk meningkatkan perlindungan. Jika Anda tunduk pada kepatuhan peraturan seperti PCI atau HIPAA, Anda mungkin dapat menggunakan grup AWS Marketplace aturan untuk memenuhi persyaratan firewall aplikasi web.

AWS Marketplace kelompok aturan tersedia tanpa kontrak jangka panjang, dan tidak ada komitmen minimum. Saat Anda berlangganan grup aturan, Anda dikenakan biaya bulanan (prorata per jam) dan biaya permintaan berkelanjutan berdasarkan volume. Untuk informasi selengkapnya, lihat Harga AWS WAF Klasik dan deskripsi untuk setiap grup AWS Marketplace aturan AWS Marketplace.

Pembaruan otomatis

Tetap up to date pada lanskap ancaman yang terus berubah bisa memakan waktu dan mahal. AWS Marketplace grup aturan dapat menghemat waktu Anda saat menerapkan dan menggunakan AWS WAF Classic. Manfaat lainnya adalah bahwa AWS dan AWS mitra kami secara otomatis memperbarui grup AWS Marketplace aturan ketika kerentanan dan ancaman baru muncul.

Banyak mitra kami diberitahu tentang kerentanan baru sebelum pengungkapan publik. Mereka dapat memperbarui grup aturan mereka dan menyebarkannya kepada Anda bahkan sebelum ancaman baru diketahui secara luas. Banyak juga yang memiliki tim peneliti ancaman untuk menyelidiki dan menganalisis ancaman terbaru untuk menulis aturan yang paling relevan.

Akses ke aturan dalam grup AWS Marketplace aturan

Setiap kelompok AWS Marketplace aturan memberikan deskripsi komprehensif tentang jenis serangan dan kerentanan yang dirancang untuk melindunginya. Untuk melindungi kekayaan intelektual penyedia grup aturan, Anda tidak dapat melihat aturan individual dalam grup aturan. Pembatasan ini juga membantu mencegah pengguna jahat merancang ancaman yang secara khusus menghindari aturan yang dipublikasikan.

Karena Anda tidak dapat melihat aturan individual dalam grup AWS Marketplace aturan, Anda juga tidak dapat mengedit aturan apa pun dalam grup AWS Marketplace aturan. Namun, Anda dapat mengecualikan aturan tertentu dari grup aturan. Ini disebut “pengecualian grup aturan.” Tidak termasuk aturan tidak menghapus aturan tersebut. Sebaliknya, itu mengubah tindakan untuk aturan`COUNT`. Oleh karena itu, permintaan yang cocok dengan aturan yang dikecualikan dihitung tetapi tidak diblokir. Anda akan menerima metrik COUNT untuk setiap aturan yang dikecualikan.

Mengecualikan aturan dapat membantu saat memecahkan masalah grup aturan yang memblokir lalu lintas secara tidak terduga (positif palsu). Salah satu teknik pemecahan masalah adalah mengidentifikasi aturan spesifik dalam kelompok aturan yang memblokir lalu lintas yang diinginkan dan kemudian menonaktifkan (mengecualikan) aturan tertentu.

Selain mengecualikan aturan tertentu, Anda dapat menyempurnakan perlindungan dengan mengaktifkan atau menonaktifkan seluruh grup aturan, serta memilih tindakan grup aturan yang akan dilakukan. Untuk informasi selengkapnya, lihat Menggunakan grup AWS Marketplace aturan.

Kuota

Anda hanya dapat mengaktifkan satu grup AWS Marketplace aturan. Anda juga dapat mengaktifkan satu grup aturan kustom yang Anda buat menggunakan AWS Firewall Manager. Grup aturan ini dihitung terhadap kuota maksimum 10 aturan per ACL web. Oleh karena itu, Anda dapat memiliki satu grup AWS Marketplace aturan, satu grup aturan khusus, dan hingga delapan aturan khusus dalam satu ACL web.

Harga

Untuk penetapan harga grup AWS Marketplace aturan, lihat Harga AWS WAF Klasik dan deskripsi untuk setiap grup AWS Marketplace aturan AWS Marketplace.

Menggunakan grup AWS Marketplace aturan

Anda dapat berlangganan dan berhenti berlangganan dari grup AWS Marketplace aturan di konsol AWS WAF Klasik. Anda juga dapat mengecualikan aturan tertentu dari grup aturan.

Untuk berlangganan dan menggunakan grup AWS Marketplace aturan

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Di panel navigasi, pilih Marketplace.
3. Di bagian Produk pasar yang tersedia, pilih nama grup aturan untuk melihat detail dan informasi harga.
4. Jika Anda ingin berlangganan grup aturan, pilih Lanjutkan.

> **Note**
>
> Jika Anda tidak ingin berlangganan grup aturan ini, cukup tutup halaman ini di browser Anda.

5. Pilih Siapkan akun Anda.
6. Tambahkan grup aturan ke ACL web, sama seperti Anda akan menambahkan aturan individual. Untuk informasi selengkapnya, lihat Membuat Web ACL atau Mengedit ACL Web.

> **Note**
>
> Saat menambahkan grup aturan ke ACL web, tindakan yang Anda tetapkan untuk grup aturan (baik No override atau Override to count) disebut tindakan penggantian grup aturan. Untuk informasi selengkapnya, lihat Pengesampingan kelompok aturan.

Untuk berhenti berlangganan dari grup AWS Marketplace aturan

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Hapus grup aturan dari semua ACL web. Untuk informasi selengkapnya, lihat Mengedit ACL Web.
3. Di panel navigasi, pilih Marketplace.
4. Pilih Kelola langganan Anda.
5. Pilih Batalkan langganan di samping nama grup aturan tempat Anda ingin berhenti berlangganan.
6. Pilih Ya, batalkan langganan.

Untuk mengecualikan aturan dari grup aturan (pengecualian grup aturan)

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.

2. Jika belum diaktifkan, aktifkan pencatatan AWS WAF Klasik. Untuk informasi selengkapnya, lihat Logging informasi lalu lintas ACL Web. Gunakan log AWS WAF Klasik untuk mengidentifikasi ID aturan yang ingin Anda kecualikan. Ini biasanya aturan yang memblokir permintaan yang sah.
3. Di panel navigasi, pilih Web ACL.
4. Pilih nama ACL web yang ingin Anda edit. Ini membuka halaman dengan detail ACL web di panel kanan.

   > **Note**
   >
   > Grup aturan yang ingin Anda edit harus dikaitkan dengan ACL web sebelum Anda dapat mengecualikan aturan dari grup aturan tersebut.

5. Pada tab Aturan di panel kanan, pilih Edit web ACL.
6. Di bagian Pengecualian grup aturan, perluas grup aturan yang ingin Anda edit.
7. Pilih X di sebelah aturan yang ingin Anda kecualikan. Anda dapat mengidentifikasi ID aturan yang benar dengan menggunakan log AWS WAF Klasik.
8. Pilih Perbarui.

   Mengecualikan aturan tidak menghapus aturan tersebut dari grup aturan. Sebaliknya, itu mengubah tindakan untuk aturan`COUNT`. Oleh karena itu, permintaan yang cocok dengan aturan yang dikecualikan dihitung tetapi tidak diblokir. Anda akan menerima `COUNT` metrik untuk setiap aturan yang dikecualikan.

   > **Note**
   >
   > Anda dapat menggunakan prosedur yang sama ini untuk mengecualikan aturan dari grup aturan khusus yang telah Anda buat AWS Firewall Manager. Namun, daripada mengecualikan aturan dari grup aturan khusus menggunakan langkah-langkah ini, Anda juga dapat mengedit grup aturan khusus menggunakan langkah-langkah yang dijelaskan dalamMenambahkan dan menghapus aturan dari grup aturan AWS WAF Klasik.

Pengesampingan kelompok aturan

AWS Marketplace kelompok aturan memiliki dua kemungkinan tindakan: No override dan Override to count. Jika Anda ingin menguji grup aturan, setel tindakan ke Override untuk dihitung. Tindakan grup aturan ini mengesampingkan tindakan blok apa pun yang ditentukan oleh aturan individual

yang terdapat dalam grup. Artinya, jika tindakan grup aturan disetel ke Override to count, alih-alih berpotensi memblokir permintaan yang cocok berdasarkan tindakan aturan individual dalam grup, permintaan tersebut akan dihitung. Sebaliknya, jika Anda menetapkan tindakan grup aturan ke No override, tindakan aturan individual dalam grup akan digunakan.

Grup aturan pemecahan masalah AWS Marketplace

Jika Anda menemukan bahwa grup AWS Marketplace aturan memblokir lalu lintas yang sah, lakukan langkah-langkah berikut.

Untuk memecahkan masalah grup aturan AWS Marketplace

1. Kecualikan aturan khusus yang memblokir lalu lintas yang sah. Anda dapat mengidentifikasi aturan mana yang memblokir permintaan mana yang menggunakan log AWS WAF Klasik. Untuk informasi selengkapnya tentang mengecualikan aturan, lihatUntuk mengecualikan aturan dari grup aturan (pengecualian grup aturan).
2. Jika mengecualikan aturan tertentu tidak menyelesaikan masalah, Anda dapat mengubah tindakan untuk grup AWS Marketplace aturan dari No override ke Override untuk dihitung. Hal ini memungkinkan permintaan web untuk melewati, terlepas dari tindakan aturan individu dalam kelompok aturan. Ini juga memberi Anda CloudWatch metrik Amazon untuk grup aturan.
3. Setelah menyetel tindakan grup AWS Marketplace aturan ke Override untuk dihitung, hubungi tim dukungan pelanggan penyedia grup aturan untuk memecahkan masalah lebih lanjut. Untuk informasi kontak, lihat daftar grup aturan di halaman daftar produk AWS Marketplace.

Menghubungi dukungan pelanggan

Untuk masalah dengan AWS WAF Classic atau grup aturan yang dikelola oleh AWS, hubungi AWS Support. Untuk masalah dengan grup aturan yang dikelola oleh AWS mitra, hubungi tim dukungan pelanggan mitra tersebut. Untuk menemukan informasi kontak mitra, lihat daftar mitra di AWS Marketplace.

Membuat dan menjual grup AWS Marketplace aturan

Jika Anda ingin menjual grup AWS Marketplace aturan AWS Marketplace, lihat Cara Menjual Perangkat Lunak Anda di AWS Marketplace.

Bekerja dengan ACL web

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Saat menambahkan aturan ke ACL web, Anda menentukan apakah Anda ingin AWS WAF Classic mengizinkan atau memblokir permintaan berdasarkan kondisi dalam aturan. Jika Anda menambahkan lebih dari satu aturan ke ACL web, AWS WAF Classic mengevaluasi setiap permintaan terhadap aturan dalam urutan yang Anda daftarkan di ACL web. Ketika permintaan web cocok dengan semua kondisi dalam aturan, AWS WAF Classic segera mengambil tindakan yang sesuai—izinkan atau blok—dan tidak mengevaluasi permintaan terhadap aturan yang tersisa di ACL web, jika ada.

Jika permintaan web tidak cocok dengan aturan apa pun di ACL web, AWS WAF Classic akan mengambil tindakan default yang Anda tentukan untuk ACL web. Untuk informasi selengkapnya, lihat Memutuskan tindakan default untuk ACL Web.

Jika Anda ingin menguji aturan sebelum mulai menggunakannya untuk mengizinkan atau memblokir permintaan, Anda dapat mengonfigurasi AWS WAF Classic untuk menghitung permintaan web yang cocok dengan kondisi dalam aturan. Untuk informasi selengkapnya, lihat Menguji ACL web.

Topik

Memutuskan tindakan default untuk ACL Web

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Ketika Anda membuat dan mengkonfigurasi ACL web, keputusan pertama dan paling penting yang harus Anda buat adalah apakah tindakan default harus untuk AWS WAF Classic untuk mengizinkan permintaan web atau untuk memblokir permintaan web. Tindakan default menunjukkan apa yang Anda ingin AWS WAF Classic lakukan setelah memeriksa permintaan web untuk semua kondisi yang Anda tentukan, dan permintaan web tidak cocok dengan salah satu kondisi tersebut:

- Izinkan — Jika Anda ingin mengizinkan sebagian besar pengguna mengakses situs web Anda, tetapi Anda ingin memblokir akses ke penyerang yang permintaannya berasal dari alamat IP tertentu, atau yang permintaannya tampaknya berisi kode SQL berbahaya atau nilai yang ditentukan, pilih Izinkan untuk tindakan default.
- Blokir - Jika Anda ingin mencegah sebagian besar calon pengguna mengakses situs web Anda, tetapi Anda ingin mengizinkan akses ke pengguna yang permintaannya berasal dari alamat IP tertentu, atau yang permintaannya berisi nilai tertentu, pilih Blokir untuk tindakan default.

Banyak keputusan yang Anda buat setelah Anda memutuskan tindakan default bergantung pada apakah Anda ingin mengizinkan atau memblokir sebagian besar permintaan web. Misalnya, jika Anda ingin mengizinkan sebagian besar permintaan, maka kondisi pencocokan yang Anda buat umumnya harus menentukan permintaan web yang ingin Anda blokir, seperti berikut ini:

- Permintaan yang berasal dari alamat IP yang membuat jumlah permintaan yang tidak masuk akal
- Permintaan yang berasal dari negara tempat Anda tidak berbisnis atau sering menjadi sumber serangan
- Permintaan yang menyertakan nilai palsu di header User-Agent
- Permintaan yang tampaknya menyertakan kode SQL berbahaya

Membuat Web ACL

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Untuk membuat web ACL

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Jika ini adalah pertama kalinya Anda menggunakan AWS WAF Classic, pilih Go to AWS WAF Classic dan kemudian Configure Web ACL. Jika Anda pernah menggunakan AWS WAF Classic sebelumnya, pilih Web ACL di panel navigasi, lalu pilih Buat web ACL.
3. Untuk nama Web ACL, masukkan nama.

   > **Note**
   >
   > Anda tidak dapat mengubah nama setelah membuat ACL web.
4. Untuk nama CloudWatch metrik, ubah nama default jika berlaku. Nama hanya dapat berisi karakter alfanumerik (A-Z, a-z, 0-9), dengan panjang maksimum se128 dan panjang minimum satu. Itu tidak dapat berisi spasi putih atau nama metrik yang dicadangkan untuk AWS WAF Klasik, termasuk “Semua” dan “Default_Action.”

   > **Note**
   >
   > Anda tidak dapat mengubah nama setelah membuat ACL web.
5. Untuk Wilayah , pilih Wilayah.
6. Untuk AWS sumber daya, pilih sumber daya yang ingin Anda kaitkan dengan ACL web ini, lalu pilih Berikutnya.

7. Jika Anda telah membuat kondisi yang ingin digunakan AWS WAF Classic untuk memeriksa permintaan web Anda, pilih Berikutnya, lalu lanjutkan ke langkah berikutnya.

   Jika Anda belum membuat kondisi, lakukan sekarang. Untuk informasi selengkapnya, lihat topik berikut:

   - Bekerja dengan kondisi pencocokan skrip lintas situs
   - Bekerja dengan kondisi pencocokan IP
   - Bekerja dengan kondisi kecocokan geografis
   - Bekerja dengan kondisi kendala ukuran
   - Bekerja dengan kondisi kecocokan injeksi SQL
   - Bekerja dengan kondisi kecocokan string
   - Bekerja dengan kondisi kecocokan regex

8. Jika Anda telah membuat aturan atau grup aturan (atau berlangganan grup AWS Marketplace aturan) yang ingin Anda tambahkan ke ACL web ini, tambahkan aturan ke ACL web:

   a. Dalam daftar Aturan, pilih aturan.

   b. Pilih Tambahkan aturan ke web ACL.

   c. Ulangi langkah a dan b sampai Anda menambahkan semua aturan yang ingin Anda tambahkan ke ACL web ini.

   d. Pergi ke langkah 10.

9. Jika Anda belum membuat aturan, Anda dapat menambahkan aturan sekarang:

   a. Pilih Buat aturan.

   b. Masukkan nilai berikut:

      Nama

      Masukkan nama.

      CloudWatch nama metrik

      Masukkan nama untuk CloudWatch metrik yang akan dibuat oleh AWS WAF Classic dan akan dikaitkan dengan aturan. Nama hanya dapat berisi karakter alfanumerik (A-Z, a-z, 0-9), dengan panjang maksimum se128 dan panjang minimum satu. Itu tidak dapat berisi spasi putih atau nama metrik yang dicadangkan untuk AWS WAF Klasik, termasuk “Semua” dan “Default_Action.”

> **Note**
>
> Anda tidak dapat mengubah nama metrik setelah membuat aturan.

c. Untuk menambahkan kondisi ke aturan, tentukan nilai berikut:

Ketika permintaan melakukan/tidak

Jika Anda ingin AWS WAF Classic mengizinkan atau memblokir permintaan berdasarkan filter dalam suatu kondisi, misalnya, permintaan web yang berasal dari kisaran alamat IP 192.0.2.0/24, pilih tidak.

Jika Anda ingin AWS WAF Classic mengizinkan atau memblokir permintaan berdasarkan kebalikan dari filter dalam suatu kondisi, pilih tidak. Misalnya, jika kondisi pencocokan IP mencakup rentang alamat IP 192.0.2.0/24 dan Anda ingin AWS WAF Classic mengizinkan atau memblokir permintaan yang tidak berasal dari alamat IP tersebut, pilih tidak.

mencocokkan/berasal dari

Pilih jenis kondisi yang ingin Anda tambahkan ke aturan:

- Kondisi pencocokan skrip lintas situs — pilih kecocokan setidaknya satu filter dalam kondisi pencocokan skrip lintas situs
- Ketentuan pencocokan IP - pilih yang berasal dari alamat IP di
- Kondisi kecocokan geografis — pilih yang berasal dari lokasi geografis di
- Kondisi batasan ukuran - pilih kecocokan setidaknya satu filter dalam kondisi batasan ukuran
- Kondisi kecocokan injeksi SQL - pilih kecocokan setidaknya satu filter dalam kondisi kecocokan injeksi SQL
- Kondisi pencocokan string - pilih kecocokan setidaknya salah satu filter dalam kondisi kecocokan string
- Ketentuan pertandingan Regex — pilih kecocokan setidaknya satu filter dalam kondisi pertandingan regex

nama kondisi

Pilih kondisi yang ingin Anda tambahkan ke aturan. Daftar hanya menampilkan kondisi dari jenis yang Anda pilih dalam daftar sebelumnya.

d. Untuk menambahkan kondisi lain ke aturan, pilih Tambahkan kondisi lain, lalu ulangi langkah b dan c. Perhatikan hal berikut:

   - Jika Anda menambahkan lebih dari satu kondisi, permintaan web harus cocok dengan setidaknya satu filter di setiap kondisi agar AWS WAF Classic mengizinkan atau memblokir permintaan berdasarkan aturan tersebut.
   - Jika Anda menambahkan dua kondisi pencocokan IP ke aturan yang sama, AWS WAF Classic hanya akan mengizinkan atau memblokir permintaan yang berasal dari alamat IP yang muncul di kedua kondisi pencocokan IP.

e. Ulangi langkah 9 sampai Anda telah membuat semua aturan yang ingin Anda tambahkan ke ACL web ini.

f. Pilih Buat.

g. Lanjutkan dengan langkah 10.

10. Untuk setiap aturan atau grup aturan di ACL web, pilih jenis manajemen yang ingin disediakan AWS WAF Classic, sebagai berikut:

- Untuk setiap aturan, pilih apakah Anda ingin AWS WAF Classic mengizinkan, memblokir, atau menghitung permintaan web berdasarkan kondisi dalam aturan:
  - Izinkan - API Gateway, CloudFront atau Application Load Balancer merespons dengan objek yang diminta. Dalam kasus CloudFront, jika objek tidak berada di cache tepi, CloudFront teruskan permintaan ke asal.
  - Block — API Gateway, CloudFront atau Application Load Balancer merespons permintaan dengan kode status HTTP 403 (Forbidden). CloudFront juga dapat merespons dengan halaman kesalahan kustom. Untuk informasi selengkapnya, lihat Menggunakan AWS WAF Klasik dengan halaman kesalahan CloudFront kustom.
  - Hitungan — AWS WAF Klasik menambah penghitung permintaan yang sesuai dengan ketentuan dalam aturan, dan kemudian terus memeriksa permintaan web berdasarkan aturan yang tersisa di ACL web.

    Untuk informasi tentang penggunaan Count untuk menguji ACL web sebelum Anda mulai menggunakannya untuk mengizinkan atau memblokir permintaan web, lihatMenghitung permintaan web yang cocok dengan aturan di ACL web.
- Untuk setiap grup aturan, setel tindakan penggantian untuk grup aturan:
  - No override — Menyebabkan tindakan aturan individu dalam kelompok aturan yang akan digunakan.

- Ganti untuk menghitung — Mengganti tindakan blok apa pun yang ditentukan oleh aturan individual dalam grup, sehingga semua permintaan yang cocok hanya dihitung.

Untuk informasi selengkapnya, lihat Pengesampingan kelompok aturan.

11. Jika Anda ingin mengubah urutan aturan di ACL web, gunakan panah di kolom Order. AWS WAF Classic memeriksa permintaan web berdasarkan urutan aturan yang muncul di ACL web.
12. Jika Anda ingin menghapus aturan yang Anda tambahkan ke ACL web, pilih x di baris untuk aturan tersebut.
13. Pilih tindakan default untuk ACL web. Ini adalah tindakan yang dilakukan AWS WAF Classic ketika permintaan web tidak sesuai dengan kondisi di salah satu aturan di ACL web ini. Untuk informasi selengkapnya, lihat Memutuskan tindakan default untuk ACL Web.
14. Pilih Periksa dan buat.
15. Tinjau pengaturan untuk ACL web, dan pilih Konfirmasi dan buat.

Mengaitkan atau memisahkan ACL Web dengan API Amazon API Gateway, CloudFront distribusi, atau Application Load Balancer

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Untuk mengaitkan atau memisahkan ACL web, lakukan prosedur yang berlaku. Perhatikan bahwa Anda juga dapat mengaitkan ACL web dengan CloudFront distribusi saat membuat atau memperbarui distribusi. Untuk informasi selengkapnya, lihat Menggunakan AWS WAF Classic untuk Mengontrol Akses ke Konten Anda di Panduan CloudFront Pengembang Amazon.

Pembatasan berikut berlaku saat mengaitkan ACL web:

- Setiap API Gateway API, Application Load Balancer dan CloudFront distribusi dapat dikaitkan dengan hanya satu ACL web.

- Web ACL yang terkait dengan CloudFront distribusi tidak dapat dikaitkan dengan Application Load Balancer atau API Gateway API. ACL web dapat, bagaimanapun, dikaitkan dengan CloudFront distribusi lain.

Untuk mengaitkan ACL web dengan API Gateway API, CloudFront distribusi, atau Application Load Balancer

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Di panel navigasi, pilih Web ACL.
3. Pilih nama ACL web yang ingin Anda kaitkan dengan API Gateway API, CloudFront distribusi, atau Application Load Balancer. Ini membuka halaman dengan detail ACL web di panel kanan.
4. Pada tab Aturan, di bawah AWS sumber daya menggunakan ACL web ini, pilih Tambahkan asosiasi.
5. Saat diminta, gunakan daftar Resource untuk memilih API Gateway API, CloudFront distribusi, atau Application Load Balancer yang ingin Anda kaitkan dengan ACL web ini. Jika Anda memilih Application Load Balancer, Anda juga harus menentukan Region.
6. Pilih Tambahkan.
7. Untuk mengaitkan ACL web ini dengan API Gateway API tambahan, CloudFront distribusi, atau Application Load Balancer lainnya, ulangi langkah 4 hingga 6.

Untuk memisahkan ACL web dari API Gateway API, CloudFront distribusi, atau Application Load Balancer

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Di panel navigasi, pilih Web ACL.
3. Pilih nama ACL web yang ingin Anda putuskan dari API Gateway API, CloudFront distribusi, atau Application Load Balancer. Ini membuka halaman dengan detail ACL web di panel kanan.

4. Pada tab Aturan, di bawah AWS sumber daya yang menggunakan ACL web ini, pilih x untuk setiap API Gateway API, CloudFront distribusi, atau Application Load Balancer yang ingin Anda putuskan dari ACL web ini.

Mengedit ACL Web

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Untuk menambah atau menghapus aturan dari ACL web atau mengubah tindakan default, lakukan prosedur berikut.

Untuk mengedit ACL web

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Di panel navigasi, pilih Web ACL.
3. Pilih nama ACL web yang ingin Anda edit. Ini membuka halaman dengan detail ACL web di panel kanan.
4. Pada tab Aturan di panel kanan, pilih Edit web ACL.
5. Untuk menambahkan aturan ke ACL web, lakukan langkah-langkah berikut:
   a. Dalam daftar Aturan, pilih aturan yang ingin Anda tambahkan.
   b. Pilih Tambahkan aturan ke web ACL.
   c. Ulangi langkah a dan b sampai Anda menambahkan semua aturan yang Anda inginkan.
6. Jika Anda ingin mengubah urutan aturan di ACL web, gunakan panah di kolom Order. AWS WAF Classic memeriksa permintaan web berdasarkan urutan aturan yang muncul di ACL web.

7. Untuk menghapus aturan dari ACL web, pilih x di sebelah kanan baris untuk aturan itu. Ini tidak menghapus aturan dari AWS WAF Klasik, itu hanya menghapus aturan dari ACL web ini.
8. Untuk mengubah tindakan untuk aturan atau tindakan default untuk ACL web, pilih opsi yang disukai.

   > **Note**
   >
   > Saat menyetel tindakan untuk grup aturan atau grup AWS Marketplace aturan (sebagai lawan dari satu aturan), tindakan yang Anda tetapkan untuk grup aturan (baik No override atau Override to count) disebut tindakan penggantian. Lihat informasi yang lebih lengkap di Pengesampingan kelompok aturan

9. Pilih Simpan perubahan.

Menghapus ACL Web

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Untuk menghapus ACL web, Anda harus menghapus aturan yang disertakan dalam ACL web dan memisahkan semua CloudFront distribusi dan Application Load Balancers dari ACL web. Lakukan prosedur berikut.

Untuk menghapus ACL web

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Di panel navigasi, pilih Web ACL.

3. Pilih nama ACL web yang ingin Anda hapus. Ini membuka halaman dengan detail ACL web di panel kanan.
4. Pada tab Aturan di panel kanan, pilih Edit web ACL.
5. Untuk menghapus semua aturan dari ACL web, pilih x di sebelah kanan baris untuk setiap aturan. Ini tidak menghapus aturan dari AWS WAF Classic, itu hanya menghapus aturan dari ACL web ini.
6. Pilih Perbarui.
7. Putuskan hubungan ACL web dari semua CloudFront distribusi dan Application Load Balancer. Pada tab Aturan, di bawah AWS sumber daya yang menggunakan ACL web ini, pilih x untuk setiap API Gateway API, CloudFront distribusi, atau Application Load Balancer.
8. Pada halaman Web ACL, konfirmasikan bahwa ACL web yang ingin Anda hapus dipilih, lalu pilih Hapus.

Menguji ACL web

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Untuk memastikan bahwa Anda tidak sengaja mengonfigurasi AWS WAF Classic untuk memblokir permintaan web yang ingin Anda izinkan atau izinkan permintaan yang ingin Anda blokir, kami sarankan Anda menguji ACL web Anda secara menyeluruh sebelum Anda mulai menggunakannya di situs web atau aplikasi web Anda.

Topik

- Menghitung permintaan web yang cocok dengan aturan di ACL web
- Melihat contoh permintaan web yang diteruskan API Gateway CloudFront atau Application Load Balancer ke Classic AWS WAF

Menghitung permintaan web yang cocok dengan aturan di ACL web

Saat menambahkan aturan ke ACL web, Anda menentukan apakah Anda ingin AWS WAF Classic mengizinkan, memblokir, atau menghitung permintaan web yang cocok dengan semua kondisi dalam aturan tersebut. Kami menyarankan Anda memulai dengan konfigurasi berikut:

- Konfigurasikan semua aturan di ACL web untuk menghitung permintaan web
- Mengatur tindakan default untuk ACL web untuk mengizinkan permintaan

Dalam konfigurasi ini, AWS WAF Classic memeriksa setiap permintaan web berdasarkan kondisi dalam aturan pertama. Jika permintaan web cocok dengan semua kondisi dalam aturan itu, AWS WAF Classic menambah penghitung untuk aturan itu. Kemudian AWS WAF Classic memeriksa permintaan web berdasarkan kondisi dalam aturan berikutnya. Jika permintaan cocok dengan semua kondisi dalam aturan tersebut, AWS WAF Classic akan menambah penghitung untuk aturan tersebut. Ini berlanjut hingga AWS WAF Classic memeriksa permintaan berdasarkan kondisi di semua aturan Anda.

Setelah mengonfigurasi semua aturan di ACL web untuk menghitung permintaan dan mengaitkan ACL web dengan API Amazon API Gateway, CloudFront distribusi, atau Application Load Balancer, Anda dapat melihat jumlah yang dihasilkan dalam grafik Amazon. CloudWatch Untuk setiap aturan dalam ACL web dan untuk semua permintaan yang diteruskan oleh API Gateway, CloudFront atau Application Load Balancer ke Classic AWS WAF untuk CloudWatch ACL web, memungkinkan Anda:

- Lihat data untuk jam sebelumnya atau tiga jam sebelumnya,
- Ubah interval antara titik data
- Ubah perhitungan yang CloudWatch dilakukan pada data, seperti maksimum, minimum, rata-rata, atau jumlah

> **Note**
>
> AWS WAF Classic with CloudFront adalah layanan global dan metrik hanya tersedia jika Anda memilih Wilayah AS Timur (Virginia N.) di. AWS Management Console Jika Anda memilih wilayah lain, tidak ada metrik AWS WAF Klasik yang akan muncul di CloudWatch konsol.

Untuk melihat data untuk aturan di ACL web

1. Masuk ke AWS Management Console dan buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Di panel navigasi, di bawah Metrik, pilih WAF.
3. Pilih kotak centang untuk ACL web yang ingin Anda lihat datanya.
4. Ubah pengaturan yang berlaku:

   Statistik

   Pilih perhitungan yang CloudWatch dilakukan pada data.

   Rentang waktu

   Pilih apakah Anda ingin melihat data untuk jam sebelumnya atau tiga jam sebelumnya.

   Periode

   Pilih interval antara titik data dalam grafik.

   Aturan

   Pilih aturan yang ingin Anda lihat datanya.

   Perhatikan hal berikut:

   - Jika Anda baru saja mengaitkan ACL web dengan API Gateway API, CloudFront distribusi, atau Application Load Balancer, Anda mungkin perlu menunggu beberapa menit agar data muncul dalam grafik dan metrik agar ACL web muncul dalam daftar metrik yang tersedia.
   - Jika Anda mengaitkan lebih dari satu API Gateway API, CloudFront distribusi, atau Application Load Balancer dengan ACL web, CloudWatch data akan menyertakan semua permintaan untuk semua distribusi yang terkait dengan ACL web.
   - Anda dapat mengarahkan kursor mouse ke titik data untuk mendapatkan informasi lebih lanjut.
   - Grafik tidak menyegarkan diri secara otomatis. Untuk memperbarui tampilan, pilih ikon segarkan
     ().
5. (Opsional) Lihat informasi terperinci tentang permintaan individual yang diteruskan API Gateway CloudFront atau Application Load Balancer ke Classic. AWS WAF Untuk informasi

selengkapnya, lihat Melihat contoh permintaan web yang diteruskan API Gateway CloudFront atau Application Load Balancer ke Classic AWS WAF.

6. Jika Anda menentukan bahwa aturan mencegat permintaan yang tidak ingin dicegat, ubah pengaturan yang berlaku. Untuk informasi selengkapnya, lihat Membuat dan mengonfigurasi Daftar Kontrol Akses Web (Web ACL).

   Jika Anda puas bahwa semua aturan Anda hanya mencegat permintaan yang benar, ubah tindakan untuk setiap aturan Anda menjadi Izinkan atau Blokir. Untuk informasi selengkapnya, lihat Mengedit ACL Web.

Melihat contoh permintaan web yang diteruskan API Gateway CloudFront atau Application Load Balancer ke Classic AWS WAF

Di konsol AWS WAF Klasik, Anda dapat melihat contoh permintaan yang diteruskan API Gateway CloudFront atau Application Load Balancer ke Classic untuk AWS WAF diperiksa. Untuk setiap permintaan sampel, Anda dapat melihat data terperinci tentang permintaan, seperti alamat IP asal dan header yang disertakan dalam permintaan. Anda juga dapat melihat aturan mana yang cocok dengan permintaan, dan apakah aturan dikonfigurasi untuk mengizinkan atau memblokir permintaan.

Contoh permintaan berisi hingga 100 permintaan yang cocok dengan semua kondisi di setiap aturan dan 100 permintaan lainnya untuk tindakan default, yang berlaku untuk permintaan yang tidak cocok dengan semua kondisi dalam aturan apa pun. Permintaan dalam sampel berasal dari semua API Gateway API, lokasi CloudFront edge, atau Application Load Balancer yang telah menerima permintaan untuk konten Anda dalam 15 menit sebelumnya.

Untuk melihat contoh permintaan web yang diteruskan API Gateway; CloudFront atau Application Load Balancer ke Classic AWS WAF

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.

2. Di panel navigasi, pilih ACL web yang ingin Anda lihat permintaannya.
3. Di panel kanan, pilih tab Permintaan.

   Tabel permintaan Sampel menampilkan nilai-nilai berikut untuk setiap permintaan:

IP sumber

Entah alamat IP tempat permintaan berasal atau, jika penampil menggunakan proxy HTTP atau Application Load Balancer untuk mengirim permintaan, alamat IP proxy atau Application Load Balancer.

URI

Jalur URI permintaan, yang mengidentifikasi sumber daya, misalnya,`/images/daily-ad.jpg`. Ini tidak termasuk string kueri atau komponen fragmen URI. Untuk selengkapnya, lihat Uniform Resource Identifier (URI): Generic Syntax.

Aturan pertandingan

Mengidentifikasi aturan pertama di ACL web yang permintaan webnya cocok dengan semua kondisi. Jika permintaan web tidak cocok dengan semua kondisi dalam aturan apa pun di ACL web, nilai aturan Cocokkan adalah Default.

Perhatikan bahwa ketika permintaan web cocok dengan semua kondisi dalam aturan dan tindakan untuk aturan tersebut adalah Hitung, AWS WAF Classic terus memeriksa permintaan web berdasarkan aturan berikutnya di ACL web. Dalam hal ini, permintaan web dapat muncul dua kali dalam daftar permintaan sampel: sekali untuk aturan yang memiliki tindakan Hitung dan lagi untuk aturan berikutnya atau untuk tindakan default.

Tindakan

Menunjukkan apakah tindakan untuk aturan terkait adalah Izinkan, Blokir, atau Hitung.

Waktu

Waktu AWS WAF Classic menerima permintaan dari API Gateway, CloudFront atau Application Load Balancer Anda.

4. Untuk menampilkan informasi tambahan tentang permintaan, pilih panah di sisi kiri alamat IP untuk permintaan itu. AWS WAF Klasik menampilkan informasi berikut:

IP sumber

Alamat IP yang sama dengan nilai di kolom IP Sumber dalam tabel.

Negara

Kode negara dua huruf dari negara tempat permintaan itu berasal. Jika penampil menggunakan proxy HTTP atau Application Load Balancer untuk mengirim permintaan,

ini adalah kode negara dua huruf dari negara tempat proxy HTTP atau Application Load Balancer berada.

Untuk daftar kode negara dua huruf dan nama negara yang sesuai, lihat entri Wikipedia ISO 3166-1 alpha-2.

Metode

Metode permintaan HTTP untuk permintaan:`GET`,`HEAD`,`OPTIONS`,`PUT`, `POSTPATCH`, atau`DELETE`.

URI

URI yang sama dengan nilai di kolom URI dalam tabel.

Minta header

Header permintaan dan nilai header dalam permintaan.

5. Untuk menyegarkan daftar permintaan sampel, pilih Dapatkan sampel baru.

Bekerja dengan grup aturan AWS WAF Klasik untuk digunakan dengan AWS Firewall Manager

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Grup aturan AWS WAF Klasik adalah seperangkat aturan yang Anda tambahkan ke AWS Firewall Manager kebijakan AWS WAF Klasik. Anda dapat membuat grup aturan sendiri, atau Anda dapat membeli grup aturan terkelola dari AWS Marketplace.

> **Important**
>
> Jika Anda ingin menambahkan grup AWS Marketplace aturan ke kebijakan Firewall Manager, setiap akun di organisasi Anda harus terlebih dahulu berlangganan grup aturan tersebut.

Setelah semua akun berlangganan, Anda dapat menambahkan grup aturan ke kebijakan. Untuk informasi selengkapnya, lihat AWS Marketplace kelompok aturan.

Topik

- Membuat grup aturan AWS WAF Klasik
- Menambahkan dan menghapus aturan dari grup aturan AWS WAF Klasik

Membuat grup aturan AWS WAF Klasik

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Saat Anda membuat grup aturan AWS WAF Klasik untuk digunakan AWS Firewall Manager, Anda menentukan aturan mana yang akan ditambahkan ke grup.

Untuk membuat grup aturan (konsol)

1. Masuk ke akun AWS Management Console menggunakan AWS Firewall Manager administrator yang Anda atur di prasyarat, lalu buka konsol Firewall Manager di. https://console.aws.amazon.com/wafv2/fms

   > **Note**
   >
   > Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatLangkah 2: Buat akun administrator AWS Firewall Manager default.

2. Di panel navigasi, pilih Beralih ke AWS WAF Klasik.
3. Di panel navigasi AWS WAF Klasik, pilih Grup aturan.
4. Pilih Buat grup aturan.

> **Note**
>
> Anda tidak dapat menambahkan aturan berbasis laju ke grup aturan.

5. Jika Anda telah membuat aturan yang ingin ditambahkan ke grup aturan, pilih Gunakan aturan yang ada untuk grup aturan ini. Jika Anda ingin membuat aturan baru untuk ditambahkan ke grup aturan, pilih Buat aturan dan ketentuan untuk grup aturan ini.
6. Pilih Berikutnya.
7. Jika Anda memilih untuk membuat aturan, ikuti langkah-langkah untuk membuatnya diMembuat aturan dan menambahkan kondisi.

> **Note**
>
> Gunakan konsol AWS WAF Klasik untuk membuat aturan Anda.

Ketika Anda telah membuat semua aturan yang Anda butuhkan, lanjutkan ke langkah berikutnya.

8. Ketik nama grup aturan.
9. Untuk menambahkan aturan ke grup aturan, pilih aturan lalu pilih Tambah aturan. Pilih apakah akan mengizinkan, memblokir, atau menghitung permintaan yang sesuai dengan kondisi aturan. Untuk informasi lebih lanjut tentang pilihan, lihatBagaimana AWS WAF Classic bekerja.
10. Setelah selesai menambahkan aturan, pilih Buat.

Anda dapat menguji grup aturan Anda dengan menambahkannya ke AWS WAF WebACL dan menyetel tindakan WebACL ke Override to Count. Tindakan ini mengesampingkan tindakan apa pun yang Anda pilih untuk aturan yang terdapat dalam grup, dan hanya menghitung permintaan yang cocok. Untuk informasi selengkapnya, lihat Membuat Web ACL.

Menambahkan dan menghapus aturan dari grup aturan AWS WAF Klasik

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF.

Untuk versi terbaru AWS WAF, lihatAWS WAF.

Anda dapat menambahkan atau menghapus aturan dalam grup aturan AWS WAF Klasik.

Menghapus aturan dari grup aturan tidak menghapus aturan itu sendiri. Ini hanya menghapus aturan dari grup aturan.

Untuk menambah atau menghapus aturan dalam grup aturan (konsol)

1. Masuk ke akun AWS Management Console menggunakan AWS Firewall Manager administrator yang Anda atur di prasyarat, lalu buka konsol Firewall Manager di. https://console.aws.amazon.com/wafv2/fms

   > **Note**
   >
   > Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatLangkah 2: Buat akun administrator AWS Firewall Manager default.

2. Di panel navigasi, pilih Beralih ke AWS WAF Klasik.
3. Di panel navigasi AWS WAF Klasik, pilih Grup aturan.
4. Pilih grup aturan yang ingin Anda edit.
5. Pilih Edit grup aturan.
6. Untuk menambahkan aturan, lakukan langkah-langkah berikut:

   a. Pilih aturan, lalu pilih Tambahkan aturan ke grup aturan. Pilih apakah akan mengizinkan, memblokir, atau menghitung permintaan yang sesuai dengan kondisi aturan. Untuk informasi lebih lanjut tentang pilihan, lihatBagaimana AWS WAF Classic bekerja. Ulangi untuk menambahkan lebih banyak aturan ke grup aturan.

      > **Note**
      >
      > Anda tidak dapat menambahkan aturan berbasis laju ke grup aturan.

   b. Pilih Perbarui.
7. Untuk menghapus aturan, lakukan langkah-langkah berikut:

a. Pilih X di sebelah aturan yang akan dihapus. Ulangi untuk menghapus lebih banyak aturan dari grup aturan.

b. Pilih Perbarui.

Memulai AWS Firewall Manager untuk mengaktifkan aturan AWS WAF Klasik

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Anda dapat menggunakan AWS Firewall Manager untuk mengaktifkan AWS WAF aturan, aturan AWS WAF Klasik, AWS Shield Advanced perlindungan, dan grup keamanan Amazon VPC. Langkah-langkah untuk mengatur sedikit berbeda untuk masing-masing:

- Untuk menggunakan Firewall Manager untuk mengaktifkan aturan menggunakan versi terbaru AWS WAF, jangan gunakan topik ini. Sebagai gantinya, ikuti langkah-langkahnyaMemulai dengan AWS Firewall ManagerAWS WAF kebijakan.
- Untuk menggunakan Firewall Manager untuk mengaktifkan AWS Shield Advanced perlindungan, ikuti langkah-langkahnya. Memulai dengan AWS Firewall ManagerAWS Shield Advanced kebijakan
- Untuk menggunakan Firewall Manager untuk mengaktifkan grup keamanan Amazon VPC, ikuti langkah-langkahnya. Memulai AWS Firewall Manager kebijakan grup keamanan Amazon VPC

Untuk menggunakan Firewall Manager untuk mengaktifkan aturan AWS WAF Klasik, lakukan langkah-langkah berikut secara berurutan.

Topik

- Langkah 3: Buat grup aturan
- Langkah 4: Buat dan terapkan kebijakan AWS Firewall ManagerAWS WAF Klasik

Langkah 1: Selesaikan prasyarat

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Ada beberapa langkah wajib untuk mempersiapkan akun Anda AWS Firewall Manager. Langkah-langkah tersebut dijelaskan dalamAWS Firewall Manager prasyarat. Lengkapi semua prasyarat sebelum melanjutkan ke. Langkah 2: Buat aturan

Langkah 2: Buat aturan

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Pada langkah ini, Anda membuat aturan menggunakan AWS WAF Klasik. Jika Anda sudah memiliki aturan AWS WAF Klasik yang ingin Anda gunakan AWS Firewall Manager, lewati langkah ini dan bukaLangkah 3: Buat grup aturan.

> **Note**
>
> Gunakan konsol AWS WAF Klasik untuk membuat aturan Anda.

Untuk membuat aturan AWS WAF Klasik (konsol)

- Buat aturan Anda, lalu tambahkan kondisi Anda ke aturan Anda. Untuk informasi selengkapnya, lihat Membuat aturan dan menambahkan kondisi.

Anda sekarang siap untuk pergi keLangkah 3: Buat grup aturan.

Langkah 3: Buat grup aturan

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Kelompok aturan adalah seperangkat aturan yang mendefinisikan tindakan apa yang harus diambil ketika serangkaian kondisi tertentu terpenuhi. Anda dapat menggunakan grup aturan terkelola dari AWS Marketplace, dan Anda dapat membuat grup aturan sendiri. Untuk informasi tentang grup aturan terkelola, lihatAWS Marketplace kelompok aturan.

Untuk membuat grup aturan Anda sendiri, lakukan prosedur berikut.

Untuk membuat grup aturan (konsol)

1. Masuk ke akun AWS Management Console menggunakan AWS Firewall Manager administrator yang Anda atur di prasyarat, lalu buka konsol Firewall Manager di. https://console.aws.amazon.com/wafv2/fms
2. Di panel navigasi, pilih Kebijakan keamanan.
3. Jika Anda belum memenuhi prasyarat, konsol menampilkan instruksi tentang cara memperbaiki masalah apa pun. Ikuti instruksi, dan kemudian mulai langkah ini (buat grup aturan) lagi. Jika Anda telah memenuhi prasyarat, pilih Tutup.
4. Pilih Buat kebijakan.

   Untuk jenis Kebijakan, pilih AWS WAF Klasik.
5. Pilih Buat AWS Firewall Manager kebijakan dan tambahkan grup aturan baru.

6. Pilih Wilayah AWS, dan kemudian pilih Berikutnya.
7. Karena Anda sudah membuat aturan, Anda tidak perlu membuat kondisi. Pilih Berikutnya.
8. Karena Anda sudah membuat aturan, Anda tidak perlu membuat aturan. Pilih Berikutnya.
9. Pilih Buat grup aturan.
10. Untuk Nama, masukkan nama yang ramah.
11. Masukkan nama untuk CloudWatch metrik yang akan dibuat oleh AWS WAF Classic dan akan dikaitkan dengan grup aturan. Nama hanya dapat berisi karakter alfanumerik (A-Z, a-z, 0-9) atau karakter khusus berikut: _-!” #`+*}, ./. Itu tidak bisa berisi ruang putih.
12. Pilih aturan, lalu pilih Tambah aturan. Aturan memiliki setelan tindakan yang memungkinkan Anda memilih apakah akan mengizinkan, memblokir, atau menghitung permintaan yang cocok dengan kondisi aturan. Untuk tutorial ini, pilih Count. Ulangi menambahkan aturan sampai Anda telah menambahkan semua aturan yang Anda inginkan ke grup aturan.
13. Pilih Buat.

Anda sekarang siap untuk pergi keLangkah 4: Buat dan terapkan kebijakan AWS Firewall ManagerAWS WAF Klasik.

Langkah 4: Buat dan terapkan kebijakan AWS Firewall ManagerAWS WAF Klasik

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Setelah membuat grup aturan, Anda membuat AWS Firewall Manager AWS WAF kebijakan. AWS WAF Kebijakan Firewall Manager berisi grup aturan yang ingin Anda terapkan ke sumber daya Anda.

Untuk membuat AWS WAF kebijakan Firewall Manager (konsol)

1. Setelah Anda membuat grup aturan (langkah terakhir dalam prosedur sebelumnya,Langkah 3: Buat grup aturan), konsol akan menampilkan halaman ringkasan grup Aturan. Pilih Berikutnya.

2. Untuk Nama, masukkan nama yang ramah.
3. Untuk tipe Policy, pilih WAF.
4. Untuk Wilayah, pilih file Wilayah AWS. Untuk melindungi CloudFront sumber daya Amazon, pilih Global.

   Untuk melindungi sumber daya di beberapa wilayah (selain CloudFront sumber daya), Anda harus membuat kebijakan Firewall Manager terpisah untuk setiap Wilayah.
5. Pilih grup aturan untuk ditambahkan, lalu pilih Tambahkan grup aturan.
6. Kebijakan memiliki dua kemungkinan tindakan: Tindakan yang ditetapkan oleh grup aturan dan Hitungan. Jika Anda ingin menguji kebijakan dan grup aturan, setel tindakan ke Hitung. Tindakan ini mengesampingkan tindakan pemblokiran apa pun yang ditentukan oleh grup aturan yang terdapat dalam kebijakan. Artinya, jika tindakan kebijakan disetel ke Hitung, permintaan tersebut hanya dihitung dan tidak diblokir. Sebaliknya, jika Anda menetapkan tindakan kebijakan ke Tindakan yang ditetapkan oleh grup aturan, tindakan grup aturan dalam kebijakan akan digunakan. Untuk tutorial ini, pilih Count.
7. Pilih Berikutnya.
8. Jika Anda hanya ingin menyertakan akun tertentu dalam kebijakan, atau mengecualikan akun tertentu dari kebijakan, pilih Pilih akun yang akan disertakan/dikecualikan dari kebijakan ini (opsional). Pilih Sertakan hanya akun ini dalam kebijakan ini atau Kecualikan akun ini dari kebijakan ini. Anda hanya dapat memilih satu opsi. Pilih Tambahkan. Pilih nomor akun yang akan disertakan atau dikecualikan, lalu pilih OK.

   > **Note**
   >
   > Jika Anda tidak memilih opsi ini, Firewall Manager menerapkan kebijakan untuk semua akun di organisasi Anda AWS Organizations. Jika Anda menambahkan akun baru ke organisasi, Firewall Manager secara otomatis menerapkan kebijakan tersebut ke akun tersebut.
9. Pilih jenis sumber daya yang ingin Anda lindungi.
10. Jika Anda hanya ingin melindungi sumber daya dengan tag tertentu, atau mengecualikan sumber daya dengan tag tertentu, pilih Gunakan tag untuk menyertakan/mengecualikan sumber daya, masukkan tag, lalu pilih Sertakan atau Kecualikan. Anda hanya dapat memilih satu opsi.

    Jika Anda memasukkan lebih dari satu tag (dipisahkan dengan koma), dan jika sumber daya memiliki salah satu tag tersebut, itu dianggap cocok.

Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.

11. Pilih Buat dan terapkan kebijakan ini ke sumber daya yang ada dan yang baru.

    Opsi ini membuat ACL web di setiap akun yang berlaku dalam organisasi di AWS Organizations, dan mengaitkan ACL web dengan sumber daya yang ditentukan di akun. Opsi ini juga menerapkan kebijakan ke semua sumber daya baru yang sesuai dengan kriteria sebelumnya (jenis dan tag sumber daya). Atau, jika Anda memilih Buat tetapi tidak menerapkan kebijakan ini ke sumber daya yang ada atau yang baru, Firewall Manager membuat ACL web di setiap akun yang berlaku dalam organisasi, tetapi tidak menerapkan ACL web ke sumber daya apa pun. Anda harus menerapkan kebijakan ke sumber daya nanti.

12. Tinggalkan pilihan untuk Ganti ACL web terkait yang ada di pengaturan default.

    Ketika opsi ini dipilih, Firewall Manager menghapus semua asosiasi ACL web yang ada dari sumber daya dalam lingkup sebelum mengaitkan ACL web kebijakan baru dengan mereka.

13. Pilih Berikutnya.
14. Tinjau kebijakan baru. Untuk membuat perubahan apa pun, pilih Edit. Jika Anda puas dengan kebijakan ini, pilih Create policy (Buat kebijakan).

Tutorial: Membuat AWS Firewall Manager kebijakan dengan aturan hierarkis

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Dengan AWS Firewall Manager, Anda dapat membuat dan menerapkan kebijakan perlindungan AWS WAF Klasik yang berisi aturan hierarkis. Artinya, Anda dapat membuat dan menegakkan aturan tertentu secara terpusat, tetapi mendelegasikan pembuatan dan pemeliharaan aturan khusus akun kepada individu lain. Anda dapat memantau aturan (umum) yang diterapkan secara terpusat untuk setiap penghapusan atau kesalahan penanganan yang tidak disengaja, sehingga memastikan bahwa

aturan tersebut diterapkan secara konsisten. Aturan khusus akun menambahkan perlindungan lebih lanjut yang disesuaikan untuk kebutuhan masing-masing tim.

> **Note**
>
> Dalam versi terbaru AWS WAF, kemampuan ini dibangun dan tidak memerlukan penanganan khusus. Jika Anda belum menggunakan AWS WAF Classic, gunakan versi terbaru sebagai gantinya. Lihat Membuat AWS Firewall Manager kebijakan untuk AWS WAF.

Tutorial berikut menjelaskan cara membuat seperangkat aturan perlindungan hierarkis.

Topik

Langkah 1: Tentukan akun administrator Firewall Manager

Untuk menggunakannya AWS Firewall Manager, Anda harus menetapkan akun di organisasi Anda sebagai akun administrator Manajer Firewall. Akun ini dapat berupa akun manajemen atau akun anggota di organisasi.

Anda dapat menggunakan akun administrator Firewall Manager untuk membuat seperangkat aturan umum yang Anda terapkan ke akun lain di organisasi. Akun lain di organisasi tidak dapat mengubah aturan yang diterapkan secara terpusat ini.

Untuk menetapkan akun sebagai akun administrator Firewall Manager dan melengkapi prasyarat lain untuk menggunakan Firewall Manager, lihat instruksi di. AWS Firewall Manager prasyarat Jika Anda sudah menyelesaikan prasyarat, Anda dapat melompat ke langkah 2 dari tutorial ini.

Dalam tutorial ini, kami merujuk ke akun administrator sebagai**`Firewall-Administrator-Account`**.

Langkah 2: Buat grup aturan menggunakan akun administrator Firewall Manager

Selanjutnya, buat grup aturan menggunakan**`Firewall-Administrator-Account`**. Grup aturan ini berisi aturan umum yang akan Anda terapkan pada semua akun anggota yang diatur oleh kebijakan yang Anda buat di langkah berikutnya. Hanya **`Firewall-Administrator-Account`** dapat membuat perubahan pada aturan ini dan grup aturan kontainer.

Dalam tutorial ini, kita merujuk ke grup aturan kontainer ini sebagai**`Common-Rule-Group`**.

Untuk membuat grup aturan, lihat instruksi diMembuat grup aturan AWS WAF Klasik. Ingatlah untuk masuk ke konsol menggunakan akun administrator Firewall Manager (**`Firewall-Administrator-Account`**) saat mengikuti petunjuk ini.

Langkah 3: Buat kebijakan Firewall Manager dan lampirkan grup aturan umum

Menggunakan**`Firewall-Administrator-Account`**, buat kebijakan Firewall Manager. Saat membuat kebijakan ini, Anda harus melakukan hal berikut:

- Tambahkan **`Common-Rule-Group`** ke kebijakan baru.
- Sertakan semua akun di organisasi tempat Anda ingin **`Common-Rule-Group`** mendaftar.
- Tambahkan semua sumber daya yang ingin Anda **`Common-Rule-Group`** terapkan.

Untuk petunjuk cara membuat kebijakan, lihatMembuat AWS Firewall Manager kebijakan.

Ini menciptakan ACL web di setiap akun yang ditentukan dan **`Common-Rule-Group`** menambah masing-masing ACL web tersebut. Setelah Anda membuat kebijakan, ACL web ini dan aturan umum akan diterapkan ke semua akun yang ditentukan.

Dalam tutorial ini, kita merujuk ke web ACL ini sebagai**`Administrator-Created-ACL`**. Unik **`Administrator-Created-ACL`** sekarang ada di setiap akun anggota organisasi yang ditentukan.

Langkah 4: Tambahkan aturan khusus akun

Setiap akun anggota dalam organisasi sekarang dapat menambahkan aturan khusus akun mereka sendiri ke **`Administrator-Created-ACL`** yang ada di akun mereka. Aturan umum yang sudah ada **`Administrator-Created-ACL`** terus berlaku, bersama dengan aturan khusus akun yang

baru. AWS WAF memeriksa permintaan web berdasarkan urutan aturan yang muncul di ACL web. Ini berlaku untuk kedua **`Administrator-Created-ACL`** dan aturan khusus akun.

Untuk menambahkan aturan**`Administrator-Created-ACL`**, lihatMengedit ACL web.

Kesimpulan

Anda sekarang memiliki ACL web yang berisi aturan umum yang dikelola oleh akun administrator Firewall Manager serta aturan khusus akun yang dikelola oleh setiap akun anggota.

`Administrator-Created-ACL`Di setiap akun mereferensikan single**`Common-Rule-Group`**. Oleh karena itu, perubahan future oleh akun administrator Firewall Manager **`Common-Rule-Group`** akan segera berlaku di setiap akun anggota.

Akun anggota tidak dapat mengubah atau menghapus aturan umum di**`Common-Rule-Group`**.

Aturan khusus akun tidak memengaruhi akun lain.

Logging informasi lalu lintas ACL Web

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

> **Note**
>
> Anda tidak dapat menggunakan Amazon Security Lake untuk mengumpulkan data AWS WAF Klasik.

Anda dapat mengaktifkan logging untuk mendapatkan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Informasi yang terkandung dalam log mencakup waktu AWS WAF Classic menerima permintaan dari AWS sumber daya Anda, informasi rinci tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan.

Untuk memulai, Anda menyiapkan Amazon Kinesis Data Firehose. Sebagai bagian dari proses itu, Anda memilih tujuan untuk menyimpan log Anda. Selanjutnya, Anda memilih ACL web yang ingin Anda aktifkan untuk login. Setelah Anda mengaktifkan logging, AWS WAF mengirimkan log melalui firehose ke tujuan penyimpanan Anda.

Untuk informasi tentang cara membuat Amazon Kinesis Data Firehose dan meninjau log yang disimpan, lihat Apa itu Amazon Data Firehose? Untuk memahami izin yang diperlukan untuk konfigurasi Firehose Data Kinesis, lihat Mengontrol Akses dengan Amazon Kinesis Data Firehose.

Anda harus memiliki izin berikut agar berhasil mengaktifkan logging:

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `waf:PutLoggingConfiguration`

Untuk informasi selengkapnya tentang peran terkait layanan dan `iam:CreateServiceLinkedRole` izin, lihat. Menggunakan peran terkait layanan untuk Classic AWS WAF

Untuk mengaktifkan pencatatan untuk ACL web

1. Buat Amazon Kinesis Data Firehose menggunakan nama yang dimulai dengan aws-waf-logs awalan "-" Misalnya,. `aws-waf-logs-us-east-2-analytics` Buat firehose data dengan PUT sumber dan di wilayah tempat Anda beroperasi. Jika Anda menangkap log untuk Amazon CloudFront, buat firehose di US East (Virginia N.). Untuk informasi selengkapnya, lihat Membuat Aliran Pengiriman Firehose Data Amazon.

   > **Important**
   >
   > Jangan memilih `Kinesis stream` sebagai sumber Anda.
   > Satu log AWS WAF Klasik setara dengan satu catatan Firehose. Jika Anda biasanya menerima 10.000 permintaan per detik dan mengaktifkan log penuh, Anda harus memiliki pengaturan 10.000 catatan per detik di Firehose. Jika Anda tidak mengonfigurasi Firehose dengan benar, AWS WAF Classic tidak akan merekam semua log. Untuk informasi selengkapnya, lihat Kuota Amazon Kinesis Data Firehose.

2. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.

3. Di panel navigasi, pilih Web ACL.
4. Pilih nama ACL web yang ingin Anda aktifkan untuk login. Ini membuka halaman dengan detail ACL web di panel kanan.
5. Pada tab Logging, pilih Aktifkan logging.
6. Pilih Kinesis Data Firehose yang Anda buat pada langkah pertama. Anda harus memilih firehose yang dimulai dengan "aws-waf-logs-.”
7. (Opsional) Jika Anda tidak ingin bidang tertentu dan nilainya disertakan dalam log, edit bidang tersebut. Pilih bidang yang akan disunting, lalu pilih Tambah. Ulangi seperlunya untuk menyunting bidang tambahan. Bidang yang disunting muncul seperti `REDACTED` di log. Misalnya, jika Anda menyunting bidang cookie, bidang cookie di log akan menjadi`REDACTED`.
8. Pilih Aktifkan pencatatan.

> **Note**
>
> Jika Anda berhasil mengaktifkan logging, AWS WAF Classic akan membuat peran terkait layanan dengan izin yang diperlukan untuk menulis log ke Amazon Kinesis Data Firehose. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk Classic AWS WAF.

Untuk menonaktifkan pencatatan untuk ACL web

1. Di panel navigasi, pilih Web ACL.
2. Pilih nama ACL web yang ingin Anda nonaktifkan logging. Ini membuka halaman dengan detail ACL web di panel kanan.
3. Pada tab Logging, pilih Nonaktifkan logging.
4. Di kotak dialog, pilih Nonaktifkan logging.

Example Contoh log

```
{

 "timestamp":1533689070589,
```

```
"formatVersion":1,
"webaclId":"385cb038-3a6f-4f2f-ac64-09ab912af590",
"terminatingRuleId":"Default_Action",
"terminatingRuleType":"REGULAR",
"action":"ALLOW",
"httpSourceName":"CF",
"httpSourceId":"i-123",
"ruleGroupList":[
                        {
                         "ruleGroupId":"41f4eb08-4e1b-2985-92b5-e8abf434fad3",
                         "terminatingRule":null,
                         "nonTerminatingMatchingRules":[
                                                         {"action" : "COUNT",
                                                         "ruleId" :
"4659b169-2083-4a91-bbd4-08851a9aaf74"}
                                                        ],
                         "excludedRules":               [
                                                         {"exclusionType" :
"EXCLUDED_AS_COUNT",
                                                          "ruleId" :
"5432a230-0113-5b83-bbb2-89375c5bfa98"}
                                                        ]
                         }
                        ],

"rateBasedRuleList":[
                            {
                             "rateBasedRuleId":"7c968ef6-32ec-4fee-96cc-51198e412e7f",

                             "limitKey":"IP",
                             "maxRateAllowed":100

                            },
                            {
                             "rateBasedRuleId":"462b169-2083-4a93-bbd4-08851a9aaf30",
                             "limitKey":"IP",
                             "maxRateAllowed":100
                             }
                             ],

"nonTerminatingMatchingRules":[
                                       {"action" : "COUNT",
```

```
                                        "ruleId" : "4659b181-2011-4a91-
bbd4-08851a9aaf52"}
                                      ],

 "httpRequest":{
                       "clientIp":"192.10.23.23",

                       "country":"US",

                       "headers":[

                                  {
                                   "name":"Host",
                                   "value":"127.0.0.1:1989"
                                  },
                                  {
                                   "name":"User-Agent",
                                   "value":"curl/7.51.2"
                                  },
                                  {
                                   "name":"Accept",
                                   "value":"*/*"
                                  }
                                ],
                     "uri":"REDACTED",
                     "args":"usernam=abc",
                     "httpVersion":"HTTP/1.1",
                     "httpMethod":"GET",
                     "requestId":"cloud front Request id"
                     }
}
```

Berikut ini adalah penjelasan dari setiap item yang tercantum dalam log ini:

timestamp

Stempel waktu dalam milidetik.

formatVersion

Versi format untuk log.

webaclId

GUID dari web ACL.

terminatingRuleId

ID aturan yang mengakhiri permintaan. Jika tidak ada yang mengakhiri permintaan, nilainya adalah`Default_Action`.

terminatingRuleType

Jenis aturan yang mengakhiri permintaan. Nilai yang mungkin: RATE_BASED, REGULAR, dan GROUP.

tindakan

Tindakan . Nilai yang mungkin untuk aturan penghentian: ALLOW dan BLOCK. COUNT bukan nilai yang valid untuk aturan penghentian.

terminatingRuleMatchDetail

Informasi terperinci tentang aturan penghentian yang cocok dengan permintaan. Aturan penghentian memiliki tindakan yang mengakhiri proses inspeksi terhadap permintaan web. Tindakan yang mungkin untuk aturan penghentian adalah ALLOW dan BLOCK. Ini hanya diisi untuk pernyataan aturan pencocokan SQL injection dan cross-site scripting (XSS). Seperti semua pernyataan aturan yang memeriksa lebih dari satu hal, AWS WAF menerapkan tindakan pada pertandingan pertama dan berhenti memeriksa permintaan web. Permintaan web dengan tindakan penghentian dapat berisi ancaman lain, selain yang dilaporkan dalam log.

httpSourceName

Sumber permintaan. Nilai yang mungkin: CF (jika sumbernya adalah Amazon CloudFront), APIGW (jika sumbernya adalah Amazon API Gateway), dan ALB (jika sumbernya adalah Application Load Balancer).

httpSourceId

ID sumber. Kolom ini menunjukkan ID CloudFront distribusi Amazon terkait, REST API untuk API Gateway, atau nama untuk Application Load Balancer.

ruleGroupList

Daftar kelompok aturan yang bertindak atas permintaan ini. Dalam contoh kode sebelumnya, hanya ada satu.

ruleGroupId

ID dari grup aturan. Jika aturan memblokir permintaan, ID `ruleGroupID` untuk sama dengan ID untuk`terminatingRuleId`.

terminatingRule

Aturan dalam kelompok aturan yang mengakhiri permintaan. Jika ini adalah nilai non-null, itu juga berisi ruleid dan tindakan. Dalam hal ini, aksinya selalu BLOCK.

nonTerminatingMatchingAturan

Daftar aturan dalam grup aturan yang cocok dengan permintaan. Ini selalu aturan COUNT (aturan non-terminating yang cocok).

tindakan (Kelompok nonTerminatingMatching aturan)

Ini selalu COUNT (aturan non-terminating yang cocok).

RuleID nonTerminatingMatching (Grup Aturan)

ID aturan dalam grup aturan yang cocok dengan permintaan dan tidak mengakhiri. Artinya, aturan COUNT.

excludedRules

Daftar aturan dalam grup aturan yang telah Anda kecualikan. Tindakan untuk aturan ini diatur ke COUNT.

ExclusionType (grup ExcludeDrules)

Tipe yang menunjukkan bahwa aturan yang dikecualikan memiliki COUNT tindakan.

ruleID (grup ExcludeDrules)

ID aturan dalam grup aturan yang dikecualikan.

rateBasedRuleDaftar

Daftar aturan berbasis tarif yang bertindak atas permintaan.

rateBasedRuleId

ID aturan berbasis tarif yang bertindak atas permintaan. Jika ini telah menghentikan permintaan, ID untuk `rateBasedRuleId` sama dengan ID untuk`terminatingRuleId`.

limitKey

Bidang yang AWS WAF digunakan untuk menentukan apakah permintaan kemungkinan datang dari satu sumber dan dengan demikian tunduk pada pemantauan tarif. Nilai yang mungkin: IP.

maxRateAllowed

Jumlah maksimum permintaan, yang memiliki nilai identik di bidang yang ditentukan oleh`limitKey`, diizinkan dalam periode lima menit. Jika jumlah permintaan melebihi dan

`maxRateAllowed` predikat lain yang ditentukan dalam aturan juga terpenuhi, AWS WAF memicu tindakan yang ditentukan untuk aturan ini.

httpRequest

Metadata tentang permintaan.

clientIp

Alamat IP klien yang mengirim permintaan.

negeri

Negara sumber permintaan. Jika AWS WAF tidak dapat menentukan negara asal, ia menetapkan bidang ini ke`-`.

headers

Daftar header.

uri

URI permintaan. Contoh kode sebelumnya menunjukkan berapa nilainya jika bidang ini telah disunting.

args

String kueri.

httpVersion

Versi HTTP.

httpMethod

Metode HTTP dalam permintaan.

requestId

ID permintaan.

Daftar alamat IP yang diblokir oleh aturan berbasis tarif

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum

November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

AWS WAF Classic menyediakan daftar alamat IP yang diblokir oleh aturan berbasis tarif.

Untuk melihat alamat yang diblokir oleh aturan berbasis tarif

1. Masuk ke AWS Management Console dan buka AWS WAF konsol di https://console.aws.amazon.com/wafv2/.

   Jika Anda melihat Beralih ke AWS WAF Klasik di panel navigasi, pilih.
2. Di panel navigasi, pilih Aturan.
3. Di kolom Nama, pilih aturan berbasis tarif.

   Daftar ini menunjukkan alamat IP yang saat ini diblokir aturan.

Bagaimana AWS WAF Classic bekerja dengan CloudFront fitur Amazon

Note

Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Saat membuat ACL web, Anda dapat menentukan satu atau CloudFront beberapa distribusi yang ingin diperiksa oleh AWS WAF Classic. AWS WAF Classic mulai mengizinkan, memblokir, atau menghitung permintaan web untuk distribusi tersebut berdasarkan kondisi yang Anda identifikasi di ACL web. CloudFront menyediakan beberapa fitur yang meningkatkan fungsionalitas AWS WAF Klasik. Bab ini menjelaskan beberapa cara yang dapat Anda konfigurasikan CloudFront untuk membuat CloudFront dan AWS WAF Classic bekerja lebih baik bersama-sama.

Topik

Menggunakan AWS WAF Klasik dengan halaman kesalahan CloudFront kustom

Ketika AWS WAF Classic memblokir permintaan web berdasarkan kondisi yang Anda tentukan, ia mengembalikan kode status HTTP 403 (Forbidden) ke CloudFront. Selanjutnya, CloudFront mengembalikan kode status itu ke penampil. Penampil kemudian menampilkan pesan default singkat dan jarang diformat mirip dengan ini:

```
Forbidden: You don't have permission to access /myfilename.html on this server.
```

Jika Anda lebih suka menampilkan pesan kesalahan kustom, mungkin menggunakan format yang sama dengan situs web Anda lainnya, Anda dapat mengonfigurasi CloudFront untuk mengembalikan objek ke penampil (misalnya, file HTML) yang berisi pesan kesalahan kustom Anda.

> **Note**
>
> CloudFront tidak dapat membedakan antara kode status HTTP 403 yang dikembalikan oleh asal Anda dan kode yang dikembalikan oleh AWS WAF Classic saat permintaan diblokir. Ini berarti bahwa Anda tidak dapat mengembalikan halaman kesalahan kustom yang berbeda berdasarkan penyebab yang berbeda dari kode status HTTP 403.

Untuk informasi selengkapnya tentang halaman kesalahan CloudFront kustom, lihat Menyesuaikan Respons Kesalahan di Panduan CloudFront Pengembang Amazon.

Menggunakan AWS WAF Classic dengan CloudFront untuk aplikasi yang berjalan di server HTTP Anda sendiri

Saat menggunakan AWS WAF Classic with CloudFront, Anda dapat melindungi aplikasi yang berjalan di server web HTTP apa pun, baik itu server web yang berjalan di Amazon Elastic

Compute Cloud (Amazon EC2) atau server web yang Anda kelola secara pribadi. Anda juga dapat mengonfigurasi CloudFront untuk meminta HTTPS antara CloudFront dan server web Anda sendiri, serta antara pemirsa dan CloudFront.

Membutuhkan HTTPS Antara CloudFront dan Server Web Anda Sendiri

Untuk mewajibkan HTTPS antara CloudFront dan server web Anda sendiri, Anda dapat menggunakan fitur asal CloudFront kustom dan mengonfigurasi Kebijakan Protokol Asal dan pengaturan Nama Domain Asal untuk asal tertentu. Dalam CloudFront konfigurasi Anda, Anda dapat menentukan nama DNS server bersama dengan port dan protokol yang CloudFront ingin Anda gunakan saat mengambil objek dari asal Anda. Anda juga harus memastikan bahwa sertifikat SSL/TLS di server asal kustom Anda cocok dengan nama domain asal yang telah Anda konfigurasikan. Ketika Anda menggunakan server web HTTP Anda sendiri di luar AWS, Anda harus menggunakan sertifikat yang ditandatangani oleh otoritas sertifikat pihak ketiga tepercaya (CA), misalnya, Comodo DigiCert, atau Symantec. Untuk informasi selengkapnya tentang mewajibkan HTTPS untuk komunikasi antara CloudFront dan server web Anda sendiri, lihat topik Memerlukan HTTPS untuk Komunikasi Antara CloudFront dan Asal Kustom Anda di Panduan CloudFront Pengembang Amazon.

Membutuhkan HTTPS Antara Penampil dan CloudFront

Untuk mewajibkan HTTPS antara pemirsa dan CloudFront, Anda dapat mengubah Kebijakan Protokol Penampil untuk satu atau beberapa perilaku cache dalam CloudFront distribusi Anda. Untuk informasi selengkapnya tentang penggunaan HTTPS antar pemirsa dan CloudFront, lihat topik Memerlukan HTTPS untuk Komunikasi Antar CloudFront Pemirsa dan di Panduan CloudFront Pengembang Amazon. Anda juga dapat membawa sertifikat SSL Anda sendiri sehingga pemirsa dapat terhubung ke CloudFront distribusi Anda melalui HTTPS menggunakan nama domain Anda sendiri, misalnya https://www.mysite.com. Untuk informasi selengkapnya, lihat topik Mengonfigurasi Nama Domain Alternatif dan HTTPS di Panduan CloudFront Pengembang Amazon.

Memilih metode HTTP yang CloudFront merespons

Saat Anda membuat distribusi CloudFront web Amazon, Anda memilih metode HTTP yang ingin CloudFront Anda proses dan teruskan ke asal Anda. Anda dapat memilih dari opsi berikut:

- GET, HEAD - Anda CloudFront hanya dapat menggunakan untuk mendapatkan objek dari asal Anda atau untuk mendapatkan header objek.

- GET, HEAD, OPTIONS — Anda CloudFront hanya dapat menggunakan untuk mendapatkan objek dari asal Anda, mendapatkan header objek, atau mengambil daftar opsi yang didukung server asal Anda.
- GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE - Anda dapat menggunakan CloudFront untuk mendapatkan, menambah, memperbarui, dan menghapus objek, dan untuk mendapatkan header objek. Selain itu, Anda dapat melakukan operasi POST lainnya seperti mengirimkan data dari formulir web.

Anda juga dapat menggunakan kondisi pencocokan string AWS WAF Klasik untuk mengizinkan atau memblokir permintaan berdasarkan metode HTTP, seperti yang dijelaskan dalamBekerja dengan kondisi kecocokan string. Jika Anda ingin menggunakan kombinasi metode yang CloudFront mendukung, seperti `GET` dan`HEAD`, maka Anda tidak perlu mengkonfigurasi AWS WAF Classic untuk memblokir permintaan yang menggunakan metode lain. Jika Anda ingin mengizinkan kombinasi metode yang CloudFront tidak mendukung, seperti,, dan `GET HEADPOST`, Anda dapat mengonfigurasi CloudFront untuk merespons semua metode, lalu gunakan AWS WAF Classic untuk memblokir permintaan yang menggunakan metode lain.

Untuk informasi selengkapnya tentang memilih metode yang CloudFront merespons, lihat Metode HTTP yang Diizinkan dalam topik Nilai yang Anda Tentukan Saat Membuat atau Memperbarui Distribusi Web di Panduan CloudFront Pengembang Amazon.

Keamanan dalam AWS WAF Klasik

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan dari cloud dan keamanan di cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Efektivitas keamanan kami diuji dan diverifikasi secara rutin oleh auditor pihak ketiga sebagai bagian dari program kepatuhan AWS. Untuk mempelajari tentang program kepatuhan yang berlaku untuk AWS WAF Classic, lihat AWS Layanan dalam Lingkup berdasarkan Program Kepatuhan.
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor-faktor lain termasuk sensitivitas data Anda, persyaratan organisasi Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan AWS WAF Classic. Topik berikut menunjukkan cara mengonfigurasi AWS WAF Classic untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya AWS WAF Klasik Anda.

Topik

Perlindungan data dalam AWS WAF Klasik

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF.

Untuk versi terbaru AWS WAF, lihatAWS WAF.

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di AWS WAF Classic. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensyal dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi yang lebih lengkap tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan AWS WAF Classic atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan

supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

AWS WAF Entitas klasik—seperti ACL web, aturan, dan kondisi—dienkripsi saat istirahat, kecuali di Wilayah tertentu di mana enkripsi tidak tersedia, termasuk China (Beijing) dan China (Ningxia). Kunci enkripsi unik digunakan untuk setiap Wilayah.

Menghapus sumber daya AWS WAF Klasik

Anda dapat menghapus sumber daya yang Anda buat di AWS WAF Classic. Lihat panduan untuk setiap jenis sumber daya di bagian berikut.

- Menghapus ACL Web
- Menambahkan dan menghapus aturan dari grup aturan AWS WAF Klasik
- Menghapus aturan

Manajemen identitas dan akses untuk AWS WAF Classic

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Klasik. AWS WAF IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- Bagaimana AWS WAF Classic bekerja dengan IAM

- Contoh kebijakan berbasis identitas untuk Classic AWS WAF
- Memecahkan masalah Identitas dan AWS WAF akses klasik
- Menggunakan peran terkait layanan untuk Classic AWS WAF

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di AWS WAF Classic.

Pengguna layanan — Jika Anda menggunakan layanan AWS WAF Classic untuk melakukan pekerjaan Anda, administrator Anda memberi Anda kredensyal dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur AWS WAF Klasik untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di AWS WAF Classic, lihatMemecahkan masalah Identitas dan AWS WAF akses klasik.

Administrator layanan - Jika Anda bertanggung jawab atas sumber daya AWS WAF Klasik di perusahaan Anda, Anda mungkin memiliki akses penuh ke AWS WAF Classic. Tugas Anda adalah menentukan fitur dan sumber daya AWS WAF Klasik mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep Basic IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan AWS WAF Classic, lihatBagaimana AWS WAF Classic bekerja dengan IAM.

Administrator IAM - Jika Anda seorang administrator IAM, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke AWS WAF Classic. Untuk melihat contoh Kebijakan berbasis identitas AWS WAF klasik yang dapat Anda gunakan di IAM, lihat. Contoh kebijakan berbasis identitas untuk Classic AWS WAF

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensyal identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensyal yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensyal Google atau Facebook Anda adalah

contoh identitas federasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensyal Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Menandatangani permintaan AWS API di Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat Autentikasi multi-faktor dalam Panduan Pengguna AWS IAM Identity Center dan Menggunakan autentikasi multi-faktor (MFA) dalam AWS dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensyal sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses

Layanan AWS dengan menggunakan kredensyal yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensyal sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat Apakah itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup yang bernama IAMAdmins dan memberikan izin ke grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat Kapan harus membuat pengguna IAM (bukan peran) dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil peran IAM untuk sementara AWS Management Console dengan beralih peran. Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat Menggunakan peran IAM dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Sebagai contoh, ketika Anda memanggil suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.
  - Peran layanan – Peran layanan adalah peran IAM yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

  - Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensyal sementara untuk aplikasi yang berjalan pada instans EC2 dan membuat atau permintaan API. AWS CLI AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan dalam instans Amazon EC2 dalam Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, lihat Kapan harus membuat peran IAM (bukan pengguna) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasinya. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan

tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan yang dikelola atau kebijakan inline, lihat Memilih antara kebijakan yang dikelola dan kebijakan inline dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Daftar kontrol akses (ACL)

Daftar kontrol akses (ACL) mengendalikan prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, lihat Gambaran umum daftar kontrol akses (ACL) dalam Panduan Developer Amazon Simple Storage Service.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) — SCP adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur di organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organisasi dan SCP, lihat Cara kerja SCP dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Bagaimana AWS WAF Classic bekerja dengan IAM

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Sebelum Anda menggunakan IAM untuk mengelola akses ke AWS WAF Classic, pelajari fitur IAM apa yang tersedia untuk digunakan dengan AWS WAF Classic.

Fitur IAM yang dapat Anda gunakan dengan Classic AWS WAF

Fitur IAM	AWS WAF Dukungan klasik
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Ya
ACL	Tidak
ABAC (tanda dalam kebijakan)	Parsial
Kredensial sementara	Ya
Sesi akses teruskan (FAS)	Ya
Peran layanan	Ya
Peran terkait layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja AWS WAF Classic dan AWS layanan lainnya dengan sebagian besar fitur IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk Classic AWS WAF

Mendukung kebijakan berbasis identitas	Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Untuk melihat contoh kebijakan berbasis identitas AWS WAF Klasik, lihat. Contoh kebijakan berbasis identitas untuk Classic AWS WAF

Kebijakan berbasis sumber daya dalam Classic AWS WAF

Mendukung kebijakan berbasis sumber daya	Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai prinsipal dalam kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, administrator IAM di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke prinsipal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

Tindakan kebijakan untuk AWS WAF Classic

Mendukung tindakan kebijakan	Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar tindakan AWS WAF Klasik, lihat Tindakan yang ditentukan oleh AWS WAF dan Tindakan yang ditentukan oleh AWS WAF Regional dalam Referensi Otorisasi Layanan.

Tindakan kebijakan di AWS WAF Klasik menggunakan awalan berikut sebelum tindakan:

```
waf
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

```
"Action": [
```

```
      "waf:action1",
      "waf:action2"
         ]
```

Anda juga dapat menentukan beberapa tindakan menggunakan wildcard (*). Misalnya, untuk menentukan semua tindakan di AWS WAF Klasik yang dimulai dengan`List`, sertakan tindakan berikut:

```
"Action": "waf:List*"
```

Untuk melihat contoh kebijakan berbasis identitas AWS WAF Klasik, lihat. Contoh kebijakan berbasis identitas untuk Classic AWS WAF

Sumber daya kebijakan untuk AWS WAF Classic

Mendukung sumber daya kebijakan	Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Untuk melihat daftar tipe sumber daya AWS WAF Klasik dan ARNnya, lihat Sumber daya yang ditentukan oleh AWS WAF dan Sumber Daya yang ditentukan oleh AWS WAF Regional dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang ditentukan oleh AWS WAF dan Tindakan yang ditentukan

oleh Regional. AWS WAF Untuk mengizinkan atau menolak akses ke subset sumber daya AWS WAF Klasik, sertakan ARN sumber daya dalam elemen `resource` kebijakan Anda.

Di AWS WAF Classic, sumber dayanya adalah ACL dan aturan web. AWS WAF Classic juga mendukung kondisi seperti pencocokan byte, pencocokan IP, dan batasan ukuran.

Sumber daya dan kondisi ini memiliki Nama Sumber Daya Amazon (ARN) unik yang terkait dengannya, seperti yang ditunjukkan pada tabel berikut.

Nama di AWS WAF Konsol	Nama dalam AWS WAF SDK/CLI	Format ARN
Web ACL	`WebACL`	`arn:aws:waf::` *`account`*`:`*`webacl`*`/`*`ID`*
Aturan	`Rule`	`arn:aws:waf::` *`account`*`:`*`rule`*`/`*`ID`*
Kondisi kecocokan string	`ByteMatchSet`	`arn:aws:waf::` *`account`*`:`*`bytematchset`* `/`*`ID`*
Syarat pencocokan injeksi SQL	`SqlInjectionMatchSet`	`arn:aws:waf::` *`account`*`:`*`sqlinjectionset`* `/`*`ID`*
Kondisi kendala ukuran	`SizeConstraintSet`	`arn:aws:waf::` *`account`*`:`*`sizeconstraintset`* `/`*`ID`*
Syarat kecocokan IP	`IPSet`	`arn:aws:waf::` *`account`*`:`*`ipset`*`/`*`ID`*
Kondisi kecocokan skrip lintas situs	`XssMatchSet`	`arn:aws:waf::` *`account`*`:`*`xssmatchset`* `/`*`ID`*

Untuk mengizinkan atau menolak akses ke subset sumber daya AWS WAF Klasik, sertakan ARN sumber daya dalam elemen `resource` kebijakan Anda. ARN untuk AWS WAF Klasik memiliki format berikut:

```
arn:aws:waf::account:resource/ID
```

Ganti variabel *akun*, *sumber daya*, dan *ID* dengan nilai yang valid. Nilai yang valid dapat berupa sebagai berikut:

- *akun*: ID Anda Akun AWS. Anda harus menentukan nilai.
- *sumber daya*: Jenis sumber daya AWS WAF Klasik.
- *ID*: ID sumber daya AWS WAF Klasik, atau wildcard (*) untuk menunjukkan semua sumber daya dari jenis tertentu yang terkait dengan yang ditentukan Akun AWS.

Misalnya, ARN berikut menentukan semua ACL web untuk akun: 111122223333

```
arn:aws:waf::111122223333:webacl/*
```

Kunci kondisi kebijakan untuk AWS WAF Klasik

Mendukung kunci kondisi kebijakan khusus layanan	Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi `AND` logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan `OR` operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika

izin tersebut mempunyai tag yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, lihat Elemen kebijakan IAM: variabel dan tag dalam Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Untuk melihat daftar kunci kondisi AWS WAF Klasik, lihat Kunci kondisi untuk AWS WAF dan Sumber daya yang ditentukan oleh AWS WAF Regional dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang ditentukan oleh AWS WAF dan Tindakan yang ditentukan oleh AWS WAF Regional.

Untuk melihat contoh kebijakan berbasis identitas AWS WAF Klasik, lihat. Contoh kebijakan berbasis identitas untuk Classic AWS WAF

ACL dalam Klasik AWS WAF

Mendukung ACL	Tidak

Daftar kontrol akses (ACL) mengendalikan pengguna utama mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

ABAC dengan Klasik AWS WAF

Mendukung ABAC (tanda dalam kebijakan)	Parsial

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi ketika tag milik prinsipal cocok dengan tag yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi saat manajemen kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tag di elemen kondisi dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Apa itu ABAC? dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) dalam Panduan Pengguna IAM.

Menggunakan kredensyal sementara dengan Classic AWS WAF

Mendukung penggunaan kredensial sementara	Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensyal sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensyal sementara, lihat Layanan AWS yang bekerja dengan IAM di Panduan Pengguna IAM.

Anda menggunakan kredensyal sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensyal sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat Peralihan peran (konsol) dalam Panduan Pengguna IAM.

Anda dapat membuat kredensyal sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensyal sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda menghasilkan kredensyal sementara secara dinamis alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

Teruskan sesi akses untuk AWS WAF Classic

Mendukung sesi akses maju (FAS)	Ya

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah

tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.

Peran layanan untuk AWS WAF Klasik

Mendukung peran layanan	Ya

Peran layanan adalah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak fungsionalitas AWS WAF Klasik. Edit peran layanan hanya jika AWS WAF Classic memberikan panduan untuk melakukannya.

Peran terkait layanan untuk Classic AWS WAF

Mendukung peran terkait layanan	Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang membuat atau mengelola peran terkait layanan AWS WAF Klasik, lihat. Menggunakan peran terkait layanan untuk Classic AWS WAF

Contoh kebijakan berbasis identitas untuk Classic AWS WAF

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya AWS WAF Klasik. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat menjalankan peran.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh AWS WAF Classic, termasuk format ARN untuk setiap jenis sumber daya, lihat Tindakan, sumber daya, dan kunci kondisi untuk serta Kunci Tindakan, sumber daya, AWS WAF dan kondisi untuk AWS WAF Regional dalam Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol AWS WAF Klasik
- Izinkan pengguna melihat izin mereka sendiri

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya AWS WAF Klasik di akun Anda. Tindakan ini dikenai biaya untuk Akun AWS Anda. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat kebijakan yang dikelola AWS atau kebijakan yang dikelola AWS untuk fungsi pekerjaan di Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukan ini dengan menentukan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, juga dikenal sebagai izin hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk menerapkan izin, lihat Kebijakan dan izin di IAM di Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Syarat di Panduan Pengguna IAM.
- Menggunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda guna memastikan izin yang aman dan berfungsi – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat validasi kebijakan Analizer Akses IAM di Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk mewajibkan MFA saat operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi akses API yang dilindungi MFA di Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM di Panduan Pengguna IAM.

Menggunakan konsol AWS WAF Klasik

Untuk mengakses konsol AWS WAF Klasik, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya AWS WAF Klasik di Anda Akun AWS. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebaliknya, izinkan akses hanya ke tindakan yang cocok dengan operasi API yang coba dilakukan.

Pengguna yang dapat mengakses dan menggunakan AWS konsol juga dapat mengakses konsol AWS WAF Klasik. Tidak diperlukan izin tambahan.

Izinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan para pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
```

```
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Memecahkan masalah Identitas dan AWS WAF akses klasik

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan AWS WAF Classic dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di AWS WAF Klasik
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya AWS WAF Klasik saya

Saya tidak berwenang untuk melakukan tindakan di AWS WAF Klasik

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya *`my-example-widget`* rekaan, tetapi tidak memiliki izin `waf:`*`GetWidget`* rekaan.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 waf:GetWidget on resource: my-example-widget
```

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya *`my-example-widget`* dengan menggunakan tindakan `waf:`*`GetWidget`*.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan bahwa Anda tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke AWS WAF Classic.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di AWS WAF Classic. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya AWS WAF Klasik saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau pengguna di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi pengguna akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa hal berikut:

- Untuk mengetahui apakah AWS WAF Classic mendukung fitur-fitur ini, lihatBagaimana AWS WAF Classic bekerja dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Memberikan akses kepada pengguna eksternal yang sah (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara penggunaan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Perbedaan antara peran IAM dan kebijakan berbasis sumber daya di Panduan Pengguna IAM.

Menggunakan peran terkait layanan untuk Classic AWS WAF

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

AWS WAF Klasik menggunakan AWS Identity and Access Management peran terkait layanan (IAM). Peran terkait layanan adalah jenis peran IAM unik yang ditautkan langsung ke Classic. AWS WAF Peran terkait layanan telah ditentukan sebelumnya oleh AWS WAF Classic dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan AWS WAF Classic lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. AWS WAF Classic mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya AWS WAF Classic yang dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin. Kebijakan izin tersebut tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran terkait layanan hanya setelah terlebih dahulu menghapus sumber daya terkait peran tersebut. Ini melindungi sumber daya AWS WAF Klasik karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, silakan lihat Layanan AWS yang bisa digunakan dengan IAM dan carilah layanan yang memiliki opsi Ya di kolom Peran Terkait Layanan. Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Izin peran terkait layanan untuk Classic AWS WAF

AWS WAF Classic menggunakan peran terkait layanan berikut:

- `AWSServiceRoleForWAFLogging`
- `AWSServiceRoleForWAFRegionalLogging`

AWS WAF Classic menggunakan peran terkait layanan ini untuk menulis log ke Amazon Data Firehose. Peran ini hanya digunakan jika Anda mengaktifkan login AWS WAF. Untuk informasi selengkapnya, lihat Logging informasi lalu lintas ACL Web.

Peran `AWSServiceRoleForWAFLogging` dan peran `AWSServiceRoleForWAFRegionalLogging` terkait layanan mempercayai layanan berikut (masing-masing) untuk mengambil peran:

- `waf.amazonaws.com`

  `waf-regional.amazonaws.com`

Kebijakan izin peran memungkinkan AWS WAF Classic menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan: `firehose:PutRecord` dan `firehose:PutRecordBatch` di Amazon Data Firehose sumber daya aliran data dengan nama yang dimulai dengan "aws-waf-logs-." Misalnya, `aws-waf-logs-us-east-2-analytics`.

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi lebih lanjut, lihat Izin Peran Tertaut Layanan di Panduan Pengguna IAM.

Membuat peran terkait layanan untuk Classic AWS WAF

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda mengaktifkan AWS WAF Classic logging di AWS Management Console, atau Anda membuat `PutLoggingConfiguration` permintaan di AWS WAF Classic CLI atau Classic API, AWS WAF Classic akan membuat AWS WAF peran terkait layanan untuk Anda.

Anda harus memiliki `iam:CreateServiceLinkedRole` izin untuk mengaktifkan logging.

Jika Anda menghapus peran terkait layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Saat Anda mengaktifkan pencatatan AWS WAF AWS WAF Klasik, Classic akan membuat peran terkait layanan untuk Anda lagi.

Mengedit peran terkait layanan untuk Classic AWS WAF

AWS WAF Classic tidak memungkinkan Anda untuk mengedit `AWSServiceRoleForWAFLogging` dan peran `AWSServiceRoleForWAFRegionalLogging` terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat menyunting penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, silakan lihat Mengedit peran tertaut layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk Classic AWS WAF

Jika tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran tertaut layanan, sebaiknya Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Tetapi, Anda harus membersihkan sumber daya peran yang terhubung dengan layanan sebelum menghapusnya secara manual.

> **Note**
>
> Jika layanan AWS WAF Klasik menggunakan peran saat Anda mencoba menghapus sumber daya, maka penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus sumber daya AWS WAF Klasik yang digunakan oleh **`AWSServiceRoleForWAFLogging`** dan **`AWSServiceRoleForWAFRegionalLogging`**

1. Di konsol AWS WAF Klasik, hapus logging dari setiap ACL web. Untuk informasi selengkapnya, lihat Logging informasi lalu lintas ACL Web.
2. Menggunakan API atau CLI, kirimkan `DeleteLoggingConfiguration` permintaan untuk setiap ACL web yang telah mengaktifkan logging. Untuk informasi selengkapnya, lihat Referensi API AWS WAF Klasik.

Untuk menghapus peran terkait layanan secara manual menggunakan IAM

Gunakan konsol IAM, IAM CLI, atau IAM API untuk menghapus peran dan terkait layanan. `AWSServiceRoleForWAFLogging` `AWSServiceRoleForWAFRegionalLogging` Untuk informasi selengkapnya, silakan lihat Menghapus Peran Terkait Layanan di Panduan Pengguna IAM.

Wilayah yang Didukung untuk AWS WAF peran terkait layanan Klasik

AWS WAF Klasik mendukung penggunaan peran terkait layanan berikut ini. Wilayah AWS

Nama Wilayah	Identitas Wilayah	Support dalam AWS WAF Klasik
AS Timur (Virginia Utara)	`us-east-1`	Ya
AS Timur (Ohio)	`us-east-2`	Ya
AS Barat (California Utara)	`us-west-1`	Ya
AS Barat (Oregon)	`us-west-2`	Ya
Asia Pasifik (Mumbai)	`ap-south-1`	Ya

Nama Wilayah	Identitas Wilayah	Support dalam AWS WAF Klasik
Asia Pacific (Osaka)	ap-northeast-3	Ya
Asia Pasifik (Seoul)	ap-northeast-2	Ya
Asia Pacific (Singapore)	ap-southeast-1	Ya
Asia Pasifik (Sydney)	ap-southeast-2	Ya
Asia Pasifik (Tokyo)	ap-northeast-1	Ya
Kanada (Pusat)	ca-central-1	Ya
Eropa (Frankfurt)	eu-central-1	Ya
Eropa (Irlandia)	eu-west-1	Ya
Eropa (London)	eu-west-2	Ya
Eropa (Paris)	eu-west-3	Ya
Amerika Selatan (Sao Paulo)	sa-east-1	Ya

Pencatatan dan pemantauan di AWS WAF Classic

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Pemantauan adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja AWS WAF Classic dan AWS solusi Anda. Anda harus mengumpulkan data pemantauan dari semua bagian AWS solusi Anda sehingga Anda dapat lebih mudah men-debug kegagalan multi-titik jika terjadi. AWS menyediakan beberapa alat untuk memantau sumber daya AWS WAF Klasik Anda dan menanggapi peristiwa potensial:

CloudWatch Alarm Amazon

Menggunakan CloudWatch alarm, Anda menonton satu metrik selama periode waktu yang Anda tentukan. Jika metrik melebihi ambang batas tertentu, CloudWatch kirimkan pemberitahuan ke topik atau AWS Auto Scaling kebijakan Amazon SNS. Untuk informasi selengkapnya, lihat Pemantauan CloudWatch dengan Amazon.

AWS CloudTrail Log

CloudTrail menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di AWS WAF Classic. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat ke AWS WAF Classic, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan. Untuk informasi selengkapnya, lihat Logging panggilan API dengan AWS CloudTrail.

Validasi kepatuhan untuk Klasik AWS WAF

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar AWS yang berfokus pada keamanan dan kepatuhan.
- Arsitektur untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi yang memenuhi syarat HIPAA.

  > **Note**
  >
  > Tidak semua memenuhi Layanan AWS syarat HIPAA. Untuk informasi selengkapnya, lihat Referensi Layanan yang Memenuhi Syarat HIPAA.

- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS

dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).

- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan dalam Klasik AWS WAF

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang dan mengoperasikan aplikasi dan basis data yang melakukan secara otomatis pinda saat gagal/failover di antara zona-zona tanpa terputus. Zona Ketersediaan lebih sangat tersedia, lebih toleran kesalahan, dan lebih dapat diskalakan daripadai infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur AWS Global.

Keamanan infrastruktur di AWS WAF Classic

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

Sebagai layanan terkelola, AWS WAF Classic dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses AWS WAF Classic melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani dengan menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan pengguna utama IAM. Atau Anda bisa menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

AWS WAF Kuota klasik

> **Note**
>
> Ini adalah dokumentasi AWS WAF Klasik. Anda hanya boleh menggunakan versi ini jika Anda membuat AWS WAF sumber daya, seperti aturan dan ACL web, AWS WAF sebelum November 2019, dan Anda belum memigrasikannya ke versi terbaru. Untuk memigrasikan sumber daya Anda, lihatMemigrasi sumber daya AWS WAF Klasik Anda ke AWS WAF. Untuk versi terbaru AWS WAF, lihatAWS WAF.

AWS WAF Klasik tunduk pada kuota berikut (sebelumnya disebut sebagai batas).

AWS WAF Classic memiliki kuota default pada jumlah entitas per akun per Wilayah. Anda dapat meminta peningkatan untuk ini.

Sumber daya	Kuota default per akun per Wilayah
ACL web	50
Aturan	100

Sumber daya	Kuota default per akun per Wilayah
R ate-based-rules	5
Ketentuan per akun per Wilayah	Untuk semua kondisi kecuali regex match dan geo match, 100 dari setiap jenis kondisi. Misalnya, 100 kondisi batasan ukuran dan 100 kondisi kecocokan IP. Untuk kondisi regex dan geo match, lihat tabel berikut.
Permintaan per Detik	25.000 per ACL web*

*Kuota ini hanya berlaku untuk AWS WAF Classic pada Application Load Balancer. Kuota Requests per Second (RPS) untuk AWS WAF Classic on CloudFront sama dengan dukungan kuota RPS CloudFront yang dijelaskan dalam Panduan Pengembang. CloudFront

Kuota berikut pada entitas AWS WAF Klasik tidak dapat diubah.

Sumber daya	Kuota per akun per Wilayah
Grup aturan per web ACL	2:1 grup aturan yang dibuat pelanggan dan 1

Sumber daya	Kuota per akun per Wilayah
	AWS Marketplace grup aturan
Aturan per web ACL	10
Kondisi per aturan	10
Rentang alamat IP (dalam notasi CIDR) per kondisi kecocokan IP	10.000 Anda dapat memperbarui hingga 1.000 alamat sekaligus. Panggilan API `UpdateIPSet` menerima maksimal 1.000 alamat dalam satu permintaan.
Alamat IP diblokir per aturan berbasis tarif	10.000
Batas tarif aturan berbasis tarif minimum per periode 5 menit	100
Filter per syarat kecocokan pembuatan skrip lintas situs	10
Filter per syarat batasan ukuran	10
Filter per syarat kecocokan injeksi SQL	10
Filter per syarat kecocokan string	10
Dalam kondisi pencocokan string, jumlah karakter dalam nama header HTTP, ketika Anda telah mengonfigurasi AWS WAF Classic untuk memeriksa header dalam permintaan web untuk nilai yang ditentukan	40

Sumber daya	Kuota per akun per Wilayah
Dalam kondisi pencocokan string, jumlah karakter dalam nilai yang Anda ingin AWS WAF Classic cari	50
Ketentuan pertandingan Regex	10
Dalam kondisi pencocokan regex, jumlah karakter dalam pola yang ingin Anda cari AWS WAF Classic	70
Dalam kondisi kecocokan regex, jumlah pola per set pola	10
Dalam kondisi kecocokan regex, jumlah set pola per kondisi regex	1
Set pola	5
Ketentuan pertandingan geo	50
Lokasi per kondisi geo match	50

AWS WAF Classic memiliki kuota tetap berikut pada panggilan per akun per Wilayah. Kuota ini berlaku untuk total panggilan ke layanan melalui cara apa pun yang tersedia, termasuk konsol, CLI, REST API AWS CloudFormation, dan SDK. Kuota-kuota ini tidak dapat diubah.

Jenis panggilan	Kuota per akun per Wilayah
Jumlah maksimum panggilan ke `AssociateWebACL`	1 permintaan setiap 2 detik
Jumlah maksimum panggilan ke `DisassociateWebACL`	1 permintaan setiap 2 detik
Jumlah maksimum panggilan ke `GetWebACLForResource`	1 permintaan per detik
Jumlah maksimum panggilan ke `ListResourcesForWebACL`	1 permintaan per detik

Jenis panggilan	Kuota per akun per Wilayah
Jumlah maksimum panggilan ke `CreateWebACLMigrationStack`	1 permintaan per detik
Jumlah maksimum panggilan ke `GetChangeToken`	10 permintaan per detik
Jumlah maksimum panggilan ke `GetChangeTokenStatus`	1 permintaan per detik
Jumlah maksimum panggilan ke setiap `List` tindakan individu, jika tidak ada kuota lain yang ditentukan untuk itu	5 permintaan per detik
Jumlah maksimum panggilan ke setiap individu`Create`,`Put`, atau `Update` tindakan`Get`, jika tidak ada kuota lain yang ditentukan untuk itu	1 permintaan per detik

AWS Shield

Perlindungan terhadap serangan Distributed Denial of Service (DDoS) sangat penting untuk aplikasi Anda yang menghadap ke internet. Ketika Anda membangun aplikasi Anda AWS, Anda dapat menggunakan perlindungan yang AWS menyediakan tanpa biaya tambahan. Selain itu, Anda dapat menggunakan layanan perlindungan ancaman AWS Shield Advanced terkelola untuk meningkatkan postur keamanan Anda dengan kemampuan deteksi, mitigasi, dan respons DDoS tambahan.

AWS berkomitmen untuk memberi Anda alat, praktik terbaik, dan layanan untuk membantu memastikan ketersediaan, keamanan, dan ketahanan yang tinggi dalam pertahanan Anda terhadap aktor jahat di internet. Panduan ini disediakan untuk membantu pembuat keputusan TI dan teknisi keamanan memahami cara menggunakan Shield dan Shield Advanced untuk melindungi aplikasi mereka dari serangan DDoS dan ancaman eksternal lainnya dengan lebih baik.

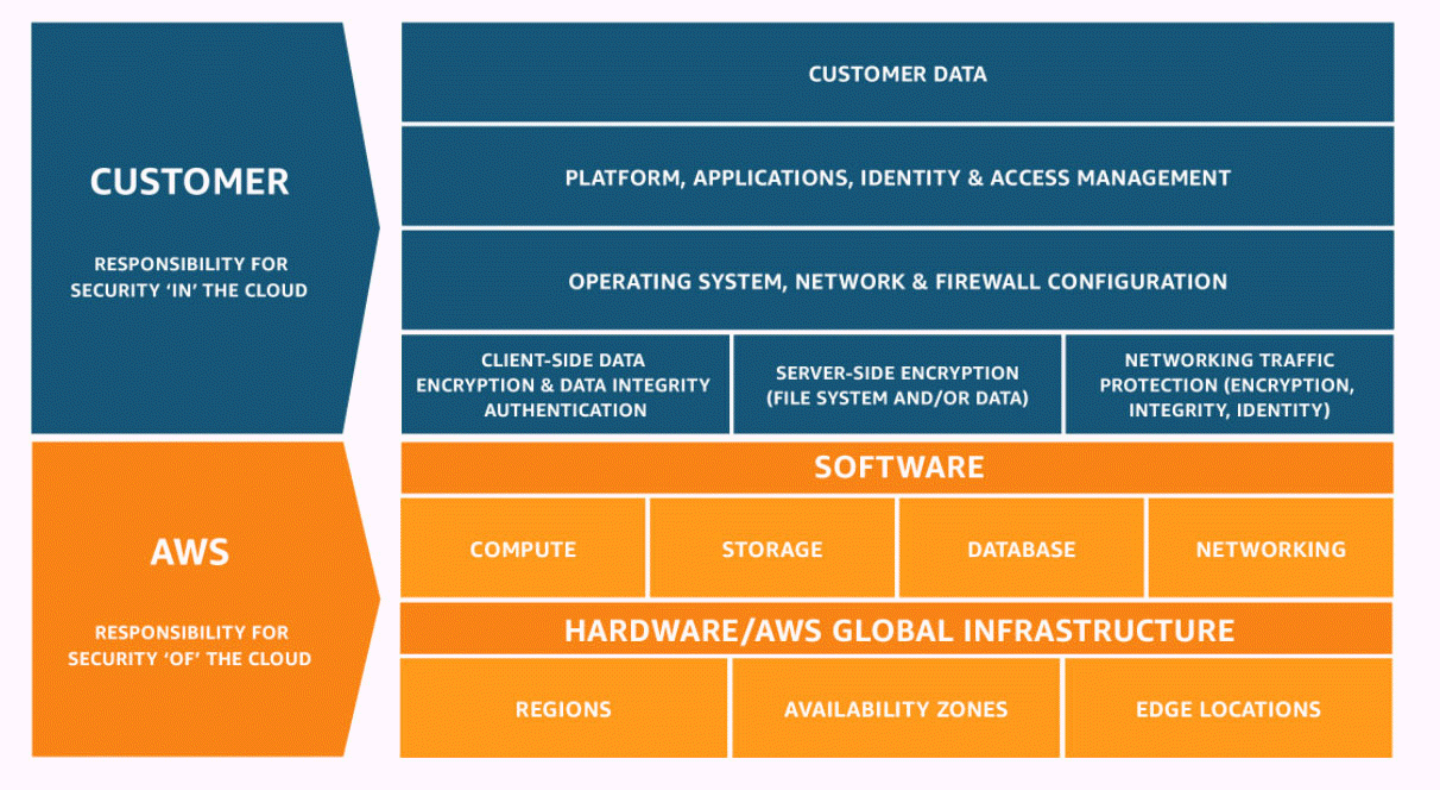
Saat Anda membangun aplikasi AWS, Anda menerima perlindungan otomatis AWS terhadap vektor serangan DDoS volumetrik umum, seperti serangan refleksi UDP dan banjir TCP SYN. Anda dapat memanfaatkan perlindungan ini untuk memastikan ketersediaan aplikasi yang Anda jalankan AWS dengan merancang dan mengonfigurasi arsitektur Anda untuk ketahanan DDoS.

Panduan ini memberikan rekomendasi yang dapat membantu Anda merancang, membuat, dan mengonfigurasi arsitektur aplikasi Anda untuk ketahanan DDoS. Aplikasi yang mematuhi praktik terbaik yang disediakan dalam panduan ini dapat memperoleh manfaat dari peningkatan kontinuitas ketersediaan ketika mereka ditargetkan oleh serangan DDoS yang lebih besar dan oleh rentang vektor serangan DDoS yang lebih luas. Selain itu, panduan ini menunjukkan cara menggunakan Shield Advanced untuk menerapkan postur perlindungan DDoS yang dioptimalkan untuk aplikasi penting Anda. Ini termasuk aplikasi yang telah Anda jamin tingkat ketersediaan tertentu bagi pelanggan Anda dan aplikasi yang memerlukan dukungan operasional AWS selama acara DDoS.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan dari cloud dan keamanan di cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Efektivitas keamanan kami diuji dan diverifikasi secara rutin oleh auditor pihak ketiga sebagai bagian dari program kepatuhan AWS. Untuk mempelajari tentang program kepatuhan yang berlaku untuk Shield Advanced, lihat AWS Layanan dalam Lingkup menurut Program Kepatuhan.

- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor-faktor lain termasuk sensitivitas data Anda, persyaratan organisasi Anda, serta undang-undang dan peraturan yang berlaku.



Bagaimana AWS Shield dan Shield Advanced bekerja

AWS Shield Standard dan AWS Shield Advanced memberikan perlindungan terhadap serangan Distributed Denial of Service (DDoS) untuk AWS sumber daya di jaringan dan lapisan transport (lapisan 3 dan 4) dan lapisan aplikasi (lapisan 7). Serangan DDoS adalah serangan di mana beberapa sistem yang dikompromikan mencoba membanjiri target dengan lalu lintas. Serangan DDoS dapat mencegah pengguna akhir yang sah mengakses layanan target dan dapat menyebabkan target crash karena volume lalu lintas yang luar biasa.

AWS Shield memberikan perlindungan terhadap berbagai vektor serangan DDoS yang diketahui dan vektor serangan zero-day. Deteksi dan mitigasi Shield dirancang untuk memberikan cakupan terhadap ancaman bahkan jika mereka tidak secara eksplisit diketahui oleh layanan pada saat deteksi. Shield Standard disediakan secara otomatis dan tanpa biaya tambahan saat Anda menggunakannya AWS.

Kelas serangan yang dideteksi Shield meliputi:

- Serangan volumetrik jaringan (lapisan 3) — Ini adalah sub kategori vektor serangan lapisan infrastruktur. Vektor-vektor ini mencoba untuk memenuhi kapasitas jaringan atau sumber daya yang ditargetkan, untuk menolak layanan kepada pengguna yang sah.
- Serangan protokol jaringan (lapisan 4) — Ini adalah sub kategori vektor serangan lapisan infrastruktur. Vektor-vektor ini menyalahgunakan protokol untuk menolak layanan ke sumber daya yang ditargetkan. Contoh umum dari serangan protokol jaringan adalah banjir TCP SYN, yang dapat menghabiskan status koneksi pada sumber daya seperti server, penyeimbang beban, atau firewall. Serangan protokol jaringan juga bisa bersifat volumetrik. Misalnya, banjir TCP SYN yang lebih besar mungkin bermaksud untuk memenuhi kapasitas jaringan sementara juga menghabiskan keadaan sumber daya yang ditargetkan atau sumber daya menengah.
- Serangan lapisan aplikasi (lapisan 7) — Kategori vektor serangan ini mencoba untuk menolak layanan kepada pengguna yang sah dengan membanjiri aplikasi dengan kueri yang valid untuk target, seperti banjir permintaan web.

Daftar Isi

- AWS Shield Advanced logika mitigasi untuk IP Elastis
- AWS Shield Advanced logika mitigasi untuk aplikasi web

AWS Shield Standard ikhtisar

AWS Shield adalah layanan perlindungan ancaman terkelola yang melindungi perimeter aplikasi Anda. Perimeter adalah titik masuk pertama untuk lalu lintas aplikasi yang datang dari luar AWS jaringan.

Untuk menentukan letak perimeter aplikasi Anda, pertimbangkan bagaimana pengguna mengakses aplikasi Anda dari internet. Jika titik masuk pertama ada di AWS Wilayah, maka perimeter aplikasi adalah Amazon Virtual Private Cloud (VPC) Anda. Jika pengguna diarahkan ke aplikasi Anda oleh Amazon Route 53, dan pertama-tama mengakses aplikasi menggunakan Amazon CloudFront atau AWS Global Accelerator, maka perimeter aplikasi dimulai di tepi AWS jaringan.

Shield memberikan manfaat deteksi dan mitigasi DDoS untuk semua aplikasi yang berjalan AWS, tetapi keputusan yang Anda buat saat mendesain arsitektur aplikasi akan memengaruhi tingkat ketahanan DDoS Anda. Ketahanan DDoS adalah kemampuan aplikasi Anda untuk terus beroperasi dalam parameter yang diharapkan selama serangan.

Semua AWS pelanggan mendapat manfaat dari perlindungan otomatis Shield Standard, tanpa biaya tambahan. Shield Standard bertahan terhadap serangan DDoS lapisan jaringan dan transport yang paling umum dan sering terjadi yang menargetkan situs web atau aplikasi Anda. Meskipun Shield Standard membantu melindungi semua AWS pelanggan, Anda mendapatkan manfaat khusus dengan zona yang dihosting Amazon Route 53, CloudFront distribusi Amazon, dan akselerator AWS Global Accelerator standar. Sumber daya ini menerima perlindungan ketersediaan komprehensif terhadap semua serangan jaringan dan lapisan transportasi yang diketahui.

AWS Shield Advanced ikhtisar

AWS Shield Advanced adalah layanan terkelola yang membantu Anda melindungi aplikasi Anda dari ancaman eksternal, seperti serangan DDoS, bot volumetrik, dan upaya eksploitasi kerentanan. Untuk tingkat perlindungan yang lebih tinggi terhadap serangan, Anda dapat berlangganan AWS Shield Advanced.

Saat Anda berlangganan Shield Advanced dan menambahkan perlindungan ke sumber daya Anda, Shield Advanced menyediakan perlindungan serangan DDoS yang diperluas untuk sumber daya tersebut. Perlindungan yang Anda terima dari Shield Advanced dapat bervariasi tergantung pada

pilihan arsitektur dan konfigurasi Anda. Gunakan informasi dalam panduan ini untuk membangun dan melindungi aplikasi tangguh menggunakan Shield Advanced, dan untuk meningkatkan ketika Anda membutuhkan bantuan ahli.

Langganan dan biaya Shield Advanced AWS WAF

Langganan Shield Advanced Anda menanggung biaya penggunaan AWS WAF kemampuan standar untuk sumber daya yang Anda lindungi dengan Shield Advanced. AWS WAF Biaya standar yang ditanggung oleh perlindungan Shield Advanced Anda adalah biaya per ACL web, biaya per aturan, dan harga dasar per juta permintaan untuk pemeriksaan permintaan web, hingga 1.500 WCU, dan hingga ukuran badan default.

Mengaktifkan mitigasi DDoS lapisan aplikasi otomatis Shield Advanced menambahkan grup aturan ke ACL web Anda yang menggunakan 150 unit kapasitas ACL web (WCU). WCU ini dihitung terhadap penggunaan WCU di ACL web Anda. Lihat informasi selengkapnya di Mitigasi DDoS lapisan aplikasi otomatis Shield Advanced, Grup aturan Shield Advanced, dan AWS WAF unit kapasitas ACL web (WCU).

Langganan Anda ke Shield Advanced tidak mencakup AWS WAF penggunaan sumber daya yang tidak Anda lindungi menggunakan Shield Advanced. Ini juga tidak mencakup AWS WAF biaya non-standar tambahan untuk sumber daya yang dilindungi. Contoh biaya non-standar adalah AWS WAF biaya untuk Kontrol Bot, untuk tindakan CAPTCHA aturan, untuk ACL web yang menggunakan lebih dari 1.500 WCU, dan untuk memeriksa badan permintaan di luar ukuran tubuh default. Daftar lengkap disediakan di halaman AWS WAF harga.

Untuk informasi selengkapnya dan contoh harga, lihat Harga dan AWS WAF Harga Shield.

Penagihan langganan Shield Advanced

Jika Anda seorang Reseller AWS Saluran, bicarakan dengan tim akun Anda untuk informasi dan panduan. Informasi penagihan ini untuk pelanggan yang bukan AWS Channel Reseller.

Untuk yang lainnya, pedoman berlangganan dan penagihan berikut berlaku:

- Untuk akun yang merupakan anggota AWS Organizations organisasi, AWS menagih langganan Shield Advanced terhadap akun pembayar untuk organisasi, terlepas dari apakah akun pembayar itu sendiri berlangganan.
- Saat Anda berlangganan beberapa akun yang berada dalam keluarga akun penagihan AWS Organizations konsolidasi yang sama, satu harga langganan mencakup semua akun berlangganan dalam keluarga. Organisasi harus memiliki semua Akun AWS dan semua sumber daya mereka.

- Saat Anda berlangganan beberapa akun untuk beberapa organisasi, Anda masih dapat membayar satu biaya berlangganan di semua organisasi, akun, dan sumber daya yang menyediakan Anda memiliki semuanya. Hubungi manajer akun atau AWS dukungan Anda dan minta pengabaian biaya pada biaya AWS Shield Advanced berlangganan untuk semua kecuali satu organisasi.

Untuk informasi dan contoh harga terperinci, lihat AWS Shield Harga.

Topik

AWS Shield Advanced sumber daya yang dilindungi

> **Note**
>
> Perlindungan Shield Advanced hanya diaktifkan untuk sumber daya yang telah Anda tentukan secara eksplisit di Shield Advanced atau yang Anda lindungi melalui kebijakan AWS Firewall Manager Shield Advanced. Shield Advanced tidak secara otomatis melindungi sumber daya Anda.

Anda dapat menggunakan Shield Advanced untuk pemantauan dan perlindungan lanjutan dengan jenis sumber daya berikut:

- CloudFront Distribusi Amazon. Untuk penerapan CloudFront berkelanjutan, Shield Advanced melindungi distribusi pementasan apa pun yang terkait dengan distribusi primer yang dilindungi.
- Amazon Route 53 zona yang dihosting.
- AWS Global Accelerator akselerator standar.
- Alamat IP Elastis Amazon EC2. Shield Advanced melindungi sumber daya yang terkait dengan alamat IP Elastic yang dilindungi.
- Instans Amazon EC2, melalui asosiasi ke alamat IP Elastis Amazon EC2.
- Berikut ini penyeimbang beban Elastic Load Balancing (ELB):
  - Penyeimbang Beban Aplikasi.

- Penyeimbang Beban Klasik.
- Network Load Balancer, melalui asosiasi ke alamat IP Elastis Amazon EC2.

Untuk informasi tambahan tentang perlindungan untuk jenis sumber daya ini, lihatAWS Shield Advanced perlindungan berdasarkan jenis sumber daya.

AWS Shield Advanced kemampuan dan opsi

AWS Shield Advanced berlangganan mencakup kemampuan dan opsi berikut. Ini melengkapi kemampuan deteksi dan mitigasi DDoS yang sudah Anda terima. AWS

- AWS WAF integrasi - Shield Advanced menggunakan ACL AWS WAF web, aturan, dan grup aturan sebagai bagian dari perlindungan lapisan aplikasinya. Untuk informasi lebih lanjut tentang AWS WAF, lihatBagaimana cara AWS WAF kerja.

> **Note**
>
> Langganan Shield Advanced Anda menanggung biaya penggunaan AWS WAF kemampuan standar untuk sumber daya yang Anda lindungi dengan Shield Advanced. AWS WAF Biaya standar yang ditanggung oleh perlindungan Shield Advanced Anda adalah biaya per ACL web, biaya per aturan, dan harga dasar per juta permintaan untuk pemeriksaan permintaan web, hingga 1.500 WCU, dan hingga ukuran badan default. Mengaktifkan mitigasi DDoS lapisan aplikasi otomatis Shield Advanced menambahkan grup aturan ke ACL web Anda yang menggunakan 150 unit kapasitas ACL web (WCU). WCU ini dihitung terhadap penggunaan WCU di ACL web Anda. Lihat informasi selengkapnya di Mitigasi DDoS lapisan aplikasi otomatis Shield Advanced, Grup aturan Shield Advanced, dan AWS WAF unit kapasitas ACL web (WCU).
>
> Langganan Anda ke Shield Advanced tidak mencakup AWS WAF penggunaan sumber daya yang tidak Anda lindungi menggunakan Shield Advanced. Ini juga tidak mencakup AWS WAF biaya non-standar tambahan untuk sumber daya yang dilindungi. Contoh biaya non-standar adalah AWS WAF biaya untuk Kontrol Bot, untuk tindakan CAPTCHA aturan, untuk ACL web yang menggunakan lebih dari 1.500 WCU, dan untuk memeriksa badan permintaan di luar ukuran tubuh default. Daftar lengkap disediakan di halaman AWS WAF harga.
>
> Untuk informasi selengkapnya dan contoh harga, lihat Harga dan AWS WAF Harga Shield.

- Mitigasi DDoS lapisan aplikasi otomatis — Anda dapat mengonfigurasi Shield Advanced untuk merespons secara otomatis untuk mengurangi serangan lapisan aplikasi (lapisan 7) terhadap sumber daya yang dilindungi. Dengan mitigasi otomatis, Shield Advanced memberlakukan pembatasan AWS WAF tarif pada permintaan dari sumber DDoS yang dikenal, dan secara otomatis menambahkan dan mengelola AWS WAF perlindungan khusus sebagai respons terhadap serangan DDoS yang terdeteksi. Anda dapat mengonfigurasi mitigasi otomatis untuk menghitung atau memblokir permintaan web yang merupakan bagian dari serangan.

  Untuk informasi selengkapnya, lihat Mitigasi DDoS lapisan aplikasi otomatis Shield Advanced.

- Deteksi berbasis kesehatan — Anda dapat menggunakan pemeriksaan kesehatan Amazon Route 53 dengan Shield Advanced untuk menginformasikan deteksi dan mitigasi peristiwa. Pemeriksaan Kesehatan memantau aplikasi Anda sesuai dengan spesifikasi Anda, melaporkan sehat ketika spesifikasi Anda terpenuhi dan tidak sehat ketika tidak. Menggunakan pemeriksaan kesehatan dengan Shield Advanced membantu mencegah kesalahan positif dan memberikan deteksi dan mitigasi yang lebih cepat ketika sumber daya yang dilindungi tidak sehat. Anda dapat menggunakan deteksi berbasis kesehatan untuk semua jenis sumber daya kecuali zona yang dihosting Route 53. Keterlibatan proaktif Shield Advanced hanya tersedia untuk sumber daya yang mengaktifkan deteksi berbasis kesehatan.

  Untuk informasi selengkapnya, lihat Deteksi berbasis kesehatan menggunakan pemeriksaan kesehatan.

- Grup perlindungan — Anda dapat menggunakan grup perlindungan untuk membuat pengelompokan logis sumber daya yang dilindungi, untuk meningkatkan deteksi dan mitigasi grup secara keseluruhan. Anda dapat menentukan kriteria keanggotaan dalam grup perlindungan sehingga sumber daya yang baru dilindungi secara otomatis disertakan. Sumber daya yang dilindungi dapat menjadi milik beberapa kelompok perlindungan.

  Untuk informasi selengkapnya, lihat AWS Shield Advanced kelompok perlindungan.

- Peningkatan visibilitas ke dalam peristiwa dan serangan DDoS — Shield Advanced memberi Anda akses ke metrik dan laporan real-time tingkat lanjut untuk visibilitas ekstensif ke dalam peristiwa dan serangan terhadap sumber daya Anda yang dilindungi. AWS Anda dapat mengakses informasi ini melalui Shield Advanced API dan konsol, dan melalui CloudWatch metrik Amazon.

  Untuk informasi selengkapnya, lihat Visibilitas ke acara DDoS.

- Manajemen terpusat perlindungan Shield Advanced oleh AWS Firewall Manager — Anda dapat menggunakan Firewall Manager untuk secara otomatis menerapkan perlindungan Shield Advanced ke akun dan sumber daya baru Anda dan untuk menerapkan AWS WAF aturan ke

ACL web Anda. Firewall Manager Shield Kebijakan perlindungan lanjutan disertakan tanpa biaya tambahan untuk pelanggan Shield Advanced. Anda juga dapat memusatkan aktivitas pemantauan Shield Advanced untuk akun Anda dengan menggunakan Firewall Manager dengan topik Amazon Simple Notification Service (SNS) atau. AWS Security Hub

Untuk informasi selengkapnya tentang menggunakan Firewall Manager untuk mengelola perlindungan Shield Advanced, lihat AWS Firewall Manager danAWS Shield Advanced kebijakan. Untuk informasi tentang harga Firewall Manager, lihat AWS Firewall Manager Harga.

- AWS Shield Response Team (SRT) — SRT memiliki pengalaman mendalam dalam melindungi AWS, Amazon.com, dan anak perusahaannya. Sebagai AWS Shield Advanced pelanggan, Anda dapat menghubungi SRT kapan saja untuk mendapatkan bantuan selama serangan DDoS yang memengaruhi ketersediaan aplikasi Anda. Anda juga dapat bekerja dengan SRT untuk membuat dan mengelola mitigasi kustom untuk sumber daya Anda. Untuk menggunakan layanan SRT, Anda juga harus berlangganan paket Business Support atau paket Enterprise Support.

  Untuk informasi selengkapnya, lihat Dukungan Shield Response Team (SRT).

- Keterlibatan proaktif — Dengan keterlibatan proaktif, Tim Respons Shield (SRT) menghubungi Anda secara langsung jika pemeriksaan kesehatan Amazon Route 53 yang Anda kaitkan dengan sumber daya yang dilindungi menjadi tidak sehat selama acara yang terdeteksi oleh Shield Advanced. Ini memberi Anda keterlibatan yang lebih cepat dengan para ahli ketika ketersediaan aplikasi Anda mungkin terpengaruh oleh serangan yang dicurigai.

  Untuk informasi selengkapnya, lihat Mengkonfigurasi keterlibatan proaktif.

- Peluang perlindungan biaya — Shield Advanced menawarkan beberapa perlindungan biaya terhadap lonjakan AWS tagihan Anda yang mungkin diakibatkan oleh serangan DDoS terhadap sumber daya Anda yang dilindungi. Ini dapat mencakup cakupan untuk lonjakan biaya penggunaan Shield Advanced data transfer out (DTO). Shield Advanced memberikan perlindungan biaya apa pun dalam bentuk kredit layanan Shield Advanced.

  Untuk informasi selengkapnya, lihat Meminta kredit di AWS Shield Advanced.

Memutuskan apakah akan berlangganan AWS Shield Advanced dan menerapkan perlindungan tambahan

Tinjau skenario di bagian ini untuk membantu menentukan akun mana yang akan berlangganan AWS Shield Advanced dan di mana menerapkan perlindungan tambahan. Dengan Shield Advanced, Anda membayar satu biaya berlangganan bulanan untuk semua akun yang dibuat di bawah akun

penagihan gabungan, ditambah biaya penggunaan berdasarkan GB data yang ditransfer keluar. Untuk informasi tentang harga Shield Advanced, lihat AWS Shield Advanced Harga.

Untuk melindungi aplikasi dan sumber dayanya dengan Shield Advanced, Anda berlangganan akun yang mengelola aplikasi ke Shield Advanced dan kemudian Anda menambahkan perlindungan ke sumber daya aplikasi. Untuk informasi tentang berlangganan akun dan melindungi sumber daya, lihatMemulai dengan AWS Shield Advanced.

Langganan dan biaya Shield Advanced AWS WAF

Langganan Shield Advanced Anda menanggung biaya penggunaan AWS WAF kemampuan standar untuk sumber daya yang Anda lindungi dengan Shield Advanced. AWS WAF Biaya standar yang ditanggung oleh perlindungan Shield Advanced Anda adalah biaya per ACL web, biaya per aturan, dan harga dasar per juta permintaan untuk pemeriksaan permintaan web, hingga 1.500 WCU, dan hingga ukuran badan default.

Mengaktifkan mitigasi DDoS lapisan aplikasi otomatis Shield Advanced menambahkan grup aturan ke ACL web Anda yang menggunakan 150 unit kapasitas ACL web (WCU). WCU ini dihitung terhadap penggunaan WCU di ACL web Anda. Lihat informasi selengkapnya di Mitigasi DDoS lapisan aplikasi otomatis Shield Advanced, Grup aturan Shield Advanced, dan AWS WAF unit kapasitas ACL web (WCU).

Langganan Anda ke Shield Advanced tidak mencakup AWS WAF penggunaan sumber daya yang tidak Anda lindungi menggunakan Shield Advanced. Ini juga tidak mencakup AWS WAF biaya non-standar tambahan untuk sumber daya yang dilindungi. Contoh biaya non-standar adalah AWS WAF biaya untuk Kontrol Bot, untuk tindakan CAPTCHA aturan, untuk ACL web yang menggunakan lebih dari 1.500 WCU, dan untuk memeriksa badan permintaan di luar ukuran tubuh default. Daftar lengkap disediakan di halaman AWS WAF harga.

Untuk informasi selengkapnya dan contoh harga, lihat Harga dan AWS WAF Harga Shield.

Penagihan langganan Shield Advanced

Jika Anda seorang Reseller AWS Saluran, bicarakan dengan tim akun Anda untuk informasi dan panduan. Informasi penagihan ini untuk pelanggan yang bukan AWS Channel Reseller.

Untuk yang lainnya, pedoman berlangganan dan penagihan berikut berlaku:

- Untuk akun yang merupakan anggota AWS Organizations organisasi, AWS menagih langganan Shield Advanced terhadap akun pembayar untuk organisasi, terlepas dari apakah akun pembayar itu sendiri berlangganan.

- Saat Anda berlangganan beberapa akun yang berada dalam keluarga akun penagihan AWS Organizations konsolidasi yang sama, satu harga langganan mencakup semua akun berlangganan dalam keluarga. Organisasi harus memiliki semua Akun AWS dan semua sumber daya mereka.
- Saat Anda berlangganan beberapa akun untuk beberapa organisasi, Anda masih dapat membayar satu biaya berlangganan di semua organisasi, akun, dan sumber daya yang menyediakan Anda memiliki semuanya. Hubungi manajer akun atau AWS dukungan Anda dan minta pengabaian biaya pada biaya AWS Shield Advanced berlangganan untuk semua kecuali satu organisasi.

Untuk informasi dan contoh harga terperinci, lihat AWS Shield Harga.

Mengidentifikasi aplikasi untuk melindungi

Pertimbangkan untuk menerapkan perlindungan Shield Advanced untuk aplikasi di mana Anda memerlukan salah satu dari berikut ini:

- Ketersediaan terjamin untuk pengguna aplikasi.
- Akses cepat ke ahli mitigasi DDoS jika aplikasi dipengaruhi oleh serangan DDoS.
- Kesadaran AWS bahwa aplikasi mungkin terpengaruh oleh serangan DDoS dan pemberitahuan serangan dari AWS dan eskalasi ke tim keamanan atau operasi Anda.
- Prediktabilitas biaya cloud Anda, termasuk ketika serangan DDoS memengaruhi penggunaan layanan Anda. AWS

Jika aplikasi atau sumber dayanya memerlukan salah satu hal di atas, pertimbangkan untuk membuat langganan untuk akun terkait.

Mengidentifikasi sumber daya untuk melindungi

Untuk setiap akun berlangganan, pertimbangkan untuk menambahkan perlindungan Shield Advanced ke setiap sumber daya yang memiliki karakteristik berikut:

- Sumber daya melayani pengguna eksternal di internet.
- Sumber daya terpapar ke internet dan juga merupakan bagian dari aplikasi penting. Pertimbangkan setiap sumber daya yang terbuka, terlepas dari apakah Anda berniat untuk diakses oleh pengguna di internet.
- Sumber daya dilindungi oleh ACL AWS WAF web.

Untuk mempelajari lebih lanjut tentang membuat dan mengelola perlindungan untuk sumber daya Anda, lihatPerlindungan sumber daya di AWS Shield Advanced.

Selain itu, ikuti rekomendasi dalam panduan ini untuk membantu memastikan bahwa Anda merancang aplikasi Anda untuk ketahanan DDoS dan bahwa Anda telah mengonfigurasi fitur Shield Advanced dengan benar untuk perlindungan optimal.

Contoh serangan DDoS

AWS Shield Advanced memberikan perlindungan yang diperluas terhadap berbagai jenis serangan.

Daftar berikut menjelaskan beberapa jenis serangan umum:

Serangan refleksi User Datagram Protocol (UDP)

Dalam serangan refleksi UDP, penyerang dapat menipu sumber permintaan dan menggunakan UDP untuk mendapatkan respons besar dari server. Lalu lintas jaringan tambahan yang diarahkan ke alamat IP palsu dan diserang dapat memperlambat server yang ditargetkan dan mencegah pengguna akhir yang sah mengakses sumber daya yang dibutuhkan.

Banjir TCP SYN

Tujuan dari serangan banjir TCP SYN adalah untuk menghabiskan sumber daya yang tersedia dari sistem dengan meninggalkan koneksi dalam keadaan setengah terbuka. Ketika pengguna terhubung ke layanan TCP seperti server web, klien mengirimkan paket TCP SYN. Server mengembalikan pengakuan, dan klien mengembalikan pengakuannya sendiri, menyelesaikan jabat tangan tiga arah. Dalam banjir TCP SYN, pengakuan ketiga tidak pernah dikembalikan, dan server dibiarkan menunggu respons. Ini dapat mencegah pengguna lain terhubung ke server.

Banjir kueri DNS

Dalam banjir kueri DNS, penyerang menggunakan beberapa kueri DNS untuk menghabiskan sumber daya server DNS. AWS Shield Advanced dapat membantu memberikan perlindungan terhadap serangan banjir kueri DNS pada server DNS Route 53.

Serangan banjir/cache-busting HTTP (lapisan 7)

Dengan banjir HTTP, termasuk `GET` dan `POST` banjir, penyerang mengirimkan beberapa permintaan HTTP yang tampaknya berasal dari pengguna nyata aplikasi web. Serangan penghilang cache adalah jenis banjir HTTP yang menggunakan variasi dalam string kueri permintaan HTTP yang mencegah penggunaan konten cache yang terletak di tepi dan memaksa

konten untuk disajikan dari server web asal, menyebabkan ketegangan tambahan dan berpotensi merusak pada server web asal.

Bagaimana AWS Shield mendeteksi peristiwa

AWS mengoperasikan sistem deteksi tingkat layanan untuk AWS jaringan dan AWS layanan individu, untuk memastikan bahwa mereka tetap tersedia selama serangan DDoS. Selain itu, sistem deteksi tingkat sumber daya memantau setiap AWS sumber daya individu untuk memastikan bahwa lalu lintas menuju sumber daya tetap dalam parameter yang diharapkan. Kombinasi ini melindungi AWS sumber daya dan AWS layanan yang ditargetkan, dengan menerapkan mitigasi yang menjatuhkan paket buruk yang diketahui, menyoroti lalu lintas yang berpotensi berbahaya, dan memprioritaskan lalu lintas dari pengguna akhir.

Peristiwa yang terdeteksi muncul di ringkasan peristiwa Shield Advanced, detail serangan, dan CloudWatch metrik Amazon baik sebagai nama vektor serangan DDoS atau `Volumetric` seolah-olah evaluasi didasarkan pada volume lalu lintas, bukan tanda tangan. Untuk informasi lebih lanjut tentang dimensi vektor serangan yang tersedia dalam `DDoSDetected` CloudWatch metrik, lihat AWS Shield Advanced metrik

Topik

- Logika deteksi untuk ancaman lapisan infrastruktur
- Logika deteksi untuk ancaman lapisan aplikasi
- Logika deteksi untuk beberapa sumber daya dalam aplikasi

Logika deteksi untuk ancaman lapisan infrastruktur

Logika deteksi yang digunakan untuk melindungi AWS sumber daya yang ditargetkan terhadap serangan DDoS di lapisan infrastruktur (lapisan 3 dan lapisan 4) tergantung pada jenis sumber daya dan apakah sumber daya dilindungi. AWS Shield Advanced

Deteksi untuk Amazon CloudFront dan Amazon Route 53

Ketika Anda melayani aplikasi web Anda dengan CloudFront dan Route 53, semua paket ke aplikasi diperiksa oleh sistem mitigasi DDoS sepenuhnya inline, yang tidak memperkenalkan latensi yang dapat diamati. Serangan DDoS terhadap CloudFront distribusi dan zona host Route 53 dikurangi secara real time. Perlindungan ini berlaku terlepas dari apakah Anda menggunakannya AWS Shield Advanced.

Ikuti praktik terbaik penggunaan CloudFront dan Route 53 sebagai titik masuk aplikasi web Anda sedapat mungkin untuk deteksi dan mitigasi peristiwa DDoS tercepat.

Deteksi untuk AWS Global Accelerator dan layanan regional

Deteksi tingkat sumber daya melindungi akselerator dan sumber daya AWS Global Accelerator standar yang diluncurkan di AWS Wilayah, seperti Classic Load Balancer, Application Load Balancer, dan alamat IP Elastis (EIP). Jenis sumber daya ini dipantau untuk peningkatan lalu lintas yang mungkin menunjukkan adanya serangan DDoS yang memerlukan mitigasi. Setiap menit, lalu lintas ke setiap AWS sumber daya dievaluasi. Jika lalu lintas ke sumber daya meningkat, pemeriksaan tambahan dilakukan untuk mengukur kapasitas sumber daya.

Shield melakukan pemeriksaan standar berikut:

- Instans Amazon Elastic Compute Cloud (Amazon EC2), EIP yang dilampirkan ke instans Amazon EC2 — Shield mengambil kapasitas dari sumber daya yang dilindungi. Kapasitas tergantung pada jenis instans target, ukuran instans, dan faktor lain seperti apakah instance menggunakan jaringan yang disempurnakan.
- Classic Load Balancers dan Application Load Balancers — Shield mengambil kapasitas dari node load balancer yang ditargetkan.
- EIP yang terpasang pada Network Load Balancers — Shield mengambil kapasitas dari penyeimbang beban yang ditargetkan. Kapasitas tidak tergantung pada konfigurasi grup penyeimbang beban target.
- AWS Global Accelerator akselerator standar - Shield mengambil kapasitas, yang didasarkan pada konfigurasi titik akhir.

Evaluasi ini terjadi di berbagai dimensi lalu lintas jaringan, seperti port dan protokol. Jika kapasitas sumber daya yang ditargetkan terlampaui, Shield menempatkan mitigasi DDoS. Mitigasi yang ditempatkan oleh Shield akan mengurangi lalu lintas DDoS, tetapi mungkin tidak menghilangkannya. Shield juga dapat menempatkan mitigasi jika sebagian kecil dari kapasitas sumber daya terlampaui pada dimensi lalu lintas yang konsisten dengan vektor serangan DDoS yang diketahui. Shield menempatkan mitigasi ini dengan waktu terbatas untuk hidup (TTL), yang diperpanjang selama serangan sedang berlangsung.

> **Note**
>
> Mitigasi yang ditempatkan oleh Shield akan mengurangi lalu lintas DDoS, tetapi mungkin tidak menghilangkannya. Anda dapat menambahkan Shield dengan solusi seperti AWS

Network Firewall atau firewall on-host seperti iptables untuk mencegah aplikasi Anda memproses lalu lintas yang tidak valid untuk aplikasi Anda atau tidak dihasilkan oleh pengguna akhir yang sah.

Perlindungan Shield Advanced menambahkan hal berikut ke aktivitas deteksi Shield yang ada:

- Ambang batas deteksi yang lebih rendah — Shield Advanced menempatkan mitigasi pada setengah dari kapasitas yang dihitung. Ini dapat memberikan mitigasi yang lebih cepat untuk serangan yang meningkat perlahan dan mitigasi serangan yang memiliki tanda tangan volumetrik yang lebih ambigu.
- Perlindungan serangan intermiten — Shield Advanced menempatkan mitigasi dengan waktu hidup yang meningkat secara eksponensial (TTL), berdasarkan frekuensi dan durasi serangan. Ini membuat mitigasi di tempat lebih lama ketika sumber daya sering ditargetkan dan ketika serangan terjadi dalam ledakan singkat.
- Deteksi berbasis kesehatan — Saat Anda mengaitkan pemeriksaan kesehatan Route 53 dengan sumber daya yang dilindungi Shield Advanced, status pemeriksaan kesehatan digunakan dalam logika deteksi. Selama peristiwa yang terdeteksi, jika pemeriksaan kesehatan sehat, Shield Advanced membutuhkan keyakinan yang lebih besar bahwa acara tersebut adalah serangan sebelum melakukan mitigasi. Jika sebaliknya pemeriksaan kesehatan tidak sehat, Shield Advanced mungkin menempatkan mitigasi bahkan sebelum kepercayaan telah ditetapkan. Fitur ini membantu menghindari kesalahan positif dan memberikan reaksi lebih cepat terhadap serangan yang memengaruhi aplikasi Anda. Untuk informasi tentang pemeriksaan kesehatan dengan Shield Advanced, lihatDeteksi berbasis kesehatan menggunakan pemeriksaan kesehatan.

Logika deteksi untuk ancaman lapisan aplikasi

AWS Shield Advanced menyediakan deteksi lapisan aplikasi web untuk CloudFront distribusi Amazon yang dilindungi dan Application Load Balancer. Saat Anda melindungi jenis sumber daya ini dengan Shield Advanced, Anda dapat mengaitkan ACL AWS WAF web dengan perlindungan Anda untuk mengaktifkan deteksi lapisan aplikasi web. Shield Advanced menggunakan data permintaan untuk ACL web terkait dan membuat garis dasar lalu lintas untuk aplikasi Anda. Deteksi lapisan aplikasi web bergantung pada integrasi asli antara Shield Advanced dan AWS WAF. Untuk mempelajari lebih lanjut tentang perlindungan lapisan aplikasi, termasuk mengaitkan ACL AWS WAF web ke sumber daya yang dilindungi Shield Advanced, lihat. AWS Shield Advanced perlindungan lapisan aplikasi (lapisan 7)

Untuk deteksi lapisan aplikasi web, Shield Advanced memantau lalu lintas aplikasi dan membandingkannya dengan baseline bersejarah yang mencari anomali. Pemantauan ini mencakup total volume dan komposisi lalu lintas. Selama serangan DDoS, kami mengharapkan volume dan komposisi lalu lintas berubah, dan Shield Advanced membutuhkan penyimpangan yang signifikan secara statistik untuk menyatakan suatu peristiwa.

Shield Advanced melakukan pengukurannya terhadap jendela waktu historis. Pendekatan ini mengurangi pemberitahuan positif palsu dari perubahan volume lalu lintas yang sah atau dari perubahan lalu lintas yang sesuai dengan pola yang diharapkan, seperti penjualan yang ditawarkan pada waktu yang sama setiap hari.

> **Note**
>
> Hindari kesalahan positif dalam perlindungan Shield Advanced Anda dengan memberikan waktu kepada Shield Advanced untuk menetapkan garis dasar yang mewakili pola lalu lintas normal dan sah. Shield Advanced mulai mengumpulkan informasi untuk baseline saat Anda mengaitkan ACL web dengan sumber daya yang dilindungi. Kaitkan ACL web dengan sumber daya terlindungi Anda setidaknya 24 jam sebelum acara yang direncanakan yang dapat menyebabkan pola yang tidak biasa dalam lalu lintas web Anda. Deteksi lapisan aplikasi web Shield Advanced paling akurat ketika telah mengamati 30 hari lalu lintas normal.

Waktu yang dibutuhkan Shield Advanced untuk mendeteksi suatu peristiwa dipengaruhi oleh seberapa banyak perubahan yang diamati dalam volume lalu lintas. Untuk perubahan volume yang lebih rendah, Shield Advanced mengamati lalu lintas untuk jangka waktu yang lebih lama, untuk membangun keyakinan bahwa suatu peristiwa sedang terjadi. Untuk perubahan volume yang lebih tinggi, Shield Advanced mendeteksi dan melaporkan peristiwa dengan lebih cepat.

Aturan berbasis kecepatan di ACL web Anda, baik yang ditambahkan oleh Anda atau oleh fitur mitigasi lapisan aplikasi otomatis Shield Advanced, dapat mengurangi serangan sebelum mencapai tingkat yang dapat dideteksi. Untuk informasi selengkapnya tentang mitigasi DDoS lapisan aplikasi otomatis, lihat. Mitigasi DDoS lapisan aplikasi otomatis Shield Advanced

> **Note**
>
> Anda dapat merancang aplikasi Anda untuk skala dalam menanggapi peningkatan lalu lintas atau beban untuk memastikan bahwa itu tidak terpengaruh oleh banjir permintaan yang lebih kecil. Dengan Shield Advanced, sumber daya Anda yang dilindungi dilindungi oleh

perlindungan biaya. Ini membantu melindungi Anda dari kenaikan tak terduga dalam tagihan cloud Anda yang mungkin terjadi sebagai akibat dari serangan DDoS. Untuk mempelajari lebih lanjut tentang perlindungan biaya Shield Advanced, lihatMeminta kredit di AWS Shield Advanced.

Logika deteksi untuk beberapa sumber daya dalam aplikasi

Anda dapat menggunakan grup AWS Shield Advanced perlindungan untuk membuat koleksi sumber daya yang dilindungi yang merupakan bagian dari aplikasi yang sama. Anda dapat memilih sumber daya yang dilindungi untuk ditempatkan dalam grup atau menunjukkan bahwa semua sumber daya dari jenis yang sama harus diperlakukan sebagai satu grup. Misalnya, Anda dapat membuat grup dari semua Application Load Balancers. Saat Anda membuat grup perlindungan, deteksi Shield Advanced mengumpulkan semua lalu lintas untuk sumber daya yang dilindungi dalam grup. Ini berguna jika Anda memiliki banyak sumber daya yang masing-masing memiliki sejumlah kecil lalu lintas, tetapi dengan volume agregat yang besar. Anda juga dapat menggunakan grup perlindungan untuk mempertahankan baseline aplikasi, untuk kasus penyebaran biru-hijau di mana lalu lintas ditransfer antara sumber daya yang dilindungi.

Anda dapat memilih untuk mengumpulkan lalu lintas dalam grup perlindungan Anda dengan salah satu cara berikut:

- Jumlah — Agregasi ini menggabungkan semua lalu lintas lintas di seluruh sumber daya dalam grup perlindungan. Anda dapat menggunakan agregasi ini untuk memastikan bahwa sumber daya yang baru dibuat memiliki garis dasar yang ada dan untuk mengurangi sensitivitas deteksi, yang dapat membantu mencegah positif palsu.
- Mean — Agregasi ini menggunakan rata-rata semua lalu lintas di seluruh grup perlindungan. Anda dapat menggunakan agregasi ini untuk aplikasi di mana lalu lintas lintas sumber daya seragam, seperti penyeimbang beban.
- Max — Agregasi ini menggunakan lalu lintas tertinggi dari sumber daya apa pun dalam grup perlindungan. Anda dapat menggunakan agregasi ini ketika ada beberapa tingkatan aplikasi dalam grup perlindungan. Misalnya, Anda mungkin memiliki grup perlindungan yang menyertakan CloudFront distribusi, asal Application Load Balancer-nya, dan target instans Amazon EC2 Application Load Balancer.

Anda juga dapat menggunakan grup perlindungan untuk meningkatkan kecepatan di mana Shield Advanced menempatkan mitigasi, untuk serangan yang menargetkan beberapa IP Elastis yang

menghadap ke internet atau akselerator standar. AWS Global Accelerator Ketika satu sumber daya dalam grup perlindungan ditargetkan, Shield Advanced membangun kepercayaan untuk sumber daya lain dalam grup. Ini menempatkan deteksi Shield Advanced dalam keadaan waspada dan dapat mengurangi waktu yang diperlukan untuk membuat mitigasi tambahan.

Untuk mempelajari lebih lanjut tentang kelompok perlindungan, lihatAWS Shield Advanced kelompok perlindungan.

Bagaimana AWS Shield mengurangi peristiwa

Logika mitigasi yang melindungi aplikasi Anda dapat bervariasi tergantung pada arsitektur aplikasi Anda. Saat Anda melindungi aplikasi web dengan Amazon CloudFront dan Amazon Route 53, Anda mendapat manfaat dari mitigasi yang khusus untuk kasus penggunaan web dan DNS dan yang melindungi semua lalu lintas untuk layanan. Jika titik masuk aplikasi Anda adalah sumber daya yang berjalan di AWS Region, logika mitigasi bervariasi tergantung pada layanan, jenis sumber daya, dan penggunaan Anda. AWS Shield Advanced

AWS Sistem mitigasi DDoS dikembangkan oleh para insinyur Shield dan terintegrasi erat dengan layanan. AWS Para insinyur mempertimbangkan aspek arsitektur Anda seperti kapasitas dan kesehatan sumber daya yang ditargetkan. Shield engineer terus memantau kemanjuran dan kinerja sistem mitigasi DDoS dan mampu merespons dengan cepat ketika ancaman baru ditemukan atau diantisipasi.

Anda dapat merancang aplikasi Anda untuk skala dalam menanggapi peningkatan lalu lintas atau beban, untuk membantu memastikan bahwa itu tidak terpengaruh oleh banjir permintaan yang lebih kecil. Jika Anda menggunakan Shield Advanced untuk melindungi sumber daya Anda, Anda menerima cakupan terhadap kenaikan tak terduga dalam tagihan cloud Anda yang mungkin terjadi sebagai akibat dari serangan DDoS.

Mitigasi infrastruktur

Untuk serangan lapisan infrastruktur, sistem mitigasi AWS Shield DDoS hadir di perbatasan AWS jaringan dan di AWS lokasi tepi. Penempatan berbagai tingkat kontrol keamanan di seluruh AWS infrastruktur menyediakan defense-in-depth untuk aplikasi cloud Anda.

Shield memelihara sistem mitigasi DDoS di semua titik masuknya dari internet. Ketika Shield mendeteksi serangan DDoS, untuk setiap titik masuknya, ia mengalihkan lalu lintas melalui sistem mitigasi DDoS di lokasi yang sama. Ini tidak memperkenalkan latensi tambahan yang dapat diamati, dan menyediakan kapasitas mitigasi lebih dari 100 TeraBits Per Detik (Tbps) di semua AWS Wilayah

dan semua lokasi tepi. Shield melindungi ketersediaan sumber daya Anda tanpa mengalihkan lalu lintas ke pusat scrubbing eksternal atau jarak jauh, yang dapat meningkatkan latensi.

- Di perbatasan AWS jaringan, untuk AWS layanan atau sumber daya apa pun, sistem mitigasi DDoS mengurangi serangan lapisan infrastruktur yang berasal dari internet. Sistem melakukan mitigasi ketika diberi sinyal oleh deteksi Shield atau oleh seorang insinyur di Tim Respons Shield (SRT).
- Di lokasi AWS tepi, sistem mitigasi DDoS terus memeriksa setiap paket yang diteruskan ke distribusi Amazon CloudFront dan zona yang dihosting Amazon Route 53, terlepas dari asalnya. Bila diperlukan, sistem menerapkan mitigasi yang dirancang khusus untuk lalu lintas web dan DNS. Manfaat tambahan menggunakan Amazon CloudFront dan Amazon Route 53 untuk melindungi aplikasi web Anda adalah serangan DDoS segera dikurangi, tanpa memerlukan sinyal dari deteksi Shield.

Mitigasi lapisan aplikasi

Shield Advanced menyediakan mitigasi lapisan aplikasi web untuk CloudFront distribusi Amazon dan Application Load Balancer di mana Anda telah mengaktifkan perlindungan Shield Advanced. Ketika Anda mengaktifkan perlindungan, Anda mengaitkan ACL AWS WAF web dengan sumber daya, untuk mengaktifkan deteksi lapisan aplikasi web. Selain itu, Anda memiliki opsi untuk mengaktifkan mitigasi lapisan aplikasi otomatis, yang menginstruksikan Shield Advanced untuk mengelola perlindungan untuk Anda selama serangan DDoS.

Shield hanya menyediakan mitigasi khusus untuk serangan lapisan aplikasi pada sumber daya yang telah Anda aktifkan Shield Advanced dan mitigasi lapisan aplikasi otomatis. Dengan mitigasi otomatis, Shield Advanced memberlakukan pembatasan AWS WAF tarif pada permintaan dari sumber DDoS yang dikenal, dan secara otomatis menambahkan dan mengelola AWS WAF perlindungan khusus sebagai respons terhadap serangan DDoS yang terdeteksi. Untuk informasi rinci tentang mitigasi jenis ini, lihat. Bagaimana Shield Advanced mengelola mitigasi otomatis

Aturan berbasis kecepatan di ACL web Anda, baik yang ditambahkan oleh Anda atau ditambahkan oleh fitur mitigasi lapisan aplikasi otomatis Shield Advanced, dapat mengurangi serangan sebelum mencapai tingkat yang dapat dideteksi. Untuk informasi lebih lanjut tentang deteksi, lihatLogika deteksi untuk ancaman lapisan aplikasi.

Fitur mitigasi

Fitur utama mitigasi AWS Shield DDoS adalah sebagai berikut:

- Validasi paket — Ini memastikan bahwa setiap paket yang diperiksa sesuai dengan struktur yang diharapkan dan valid untuk protokolnya. Validasi protokol yang didukung termasuk IP, TCP (termasuk header dan opsi), UDP, ICMP, DNS, dan NTP.
- Access Control Lists (ACL) dan shapers — ACL mengevaluasi lalu lintas terhadap atribut tertentu dan menjatuhkan lalu lintas yang cocok atau memetakannya ke pembentuk. Pembentuk membatasi laju paket untuk lalu lintas yang cocok, menjatuhkan paket berlebih untuk memuat volume yang mencapai tujuan. AWS Shield Deteksi dan Shield Response Team (SRT) teknisi dapat menyediakan alokasi tarif khusus untuk lalu lintas yang diharapkan dan alokasi tingkat yang lebih ketat untuk lalu lintas dengan atribut yang cocok dengan vektor serangan DDoS yang diketahui. Atribut yang ACL dapat cocok termasuk port, protokol, bendera TCP, alamat tujuan, negara sumber, dan pola arbitrer dalam payload paket.
- Skor kecurigaan — Ini menggunakan pengetahuan bahwa Shield memiliki lalu lintas yang diharapkan untuk menerapkan skor ke setiap paket. Paket yang lebih dekat dengan pola lalu lintas yang diketahui baik diberi skor kecurigaan yang lebih rendah. Pengamatan atribut lalu lintas buruk yang diketahui dapat meningkatkan skor kecurigaan untuk sebuah paket. Ketika perlu untuk menilai paket batas, Shield menjatuhkan paket dengan skor kecurigaan yang lebih tinggi terlebih dahulu. Ini membantu Shield untuk mengurangi serangan DDoS yang diketahui dan zero-day sambil menghindari kesalahan positif.
- Proxy TCP SYN — Ini memberikan perlindungan terhadap banjir TCP SYN dengan mengirimkan cookie TCP SYN untuk menantang koneksi baru sebelum mengizinkannya lolos ke layanan yang dilindungi. Proxy TCP SYN yang disediakan oleh mitigasi Shield DDoS adalah tanpa kewarganegaraan, yang memungkinkannya untuk mengurangi serangan banjir TCP SYN terbesar yang diketahui tanpa mencapai kelelahan status. Ini dicapai dengan mengintegrasikan dengan AWS layanan untuk menyerahkan status koneksi alih-alih mempertahankan proxy berkelanjutan antara klien dan layanan yang dilindungi. Proxy TCP SYN saat ini tersedia di Amazon dan CloudFront Amazon Route 53.
- Distribusi tingkat — Ini terus menyesuaikan nilai pembentuk per lokasi berdasarkan pola masuknya lalu lintas ke sumber daya yang dilindungi. Ini mencegah pembatasan laju lalu lintas pelanggan yang mungkin tidak masuk ke AWS jaringan secara merata.

AWS Shield logika mitigasi untuk CloudFront dan Rute 53

Mitigasi Shield DDoS terus memeriksa lalu lintas untuk dan Route 53. CloudFront Layanan ini beroperasi dari jaringan lokasi AWS edge yang didistribusikan secara global yang memberi Anda akses luas ke kapasitas mitigasi DDoS Shield dan mengirimkan aplikasi Anda dari infrastruktur yang lebih dekat dengan pengguna akhir Anda.

- CloudFront— Mitigasi Shield DDoS hanya memungkinkan lalu lintas yang valid untuk aplikasi web untuk melewati layanan. Ini memberikan perlindungan otomatis terhadap banyak vektor DDoS umum, seperti serangan refleksi UDP.

  CloudFront mempertahankan koneksi persisten ke asal aplikasi Anda, banjir TCP SYN secara otomatis dikurangi melalui integrasi dengan fitur proxy Shield TCP SYN, dan Transport Layer Security (TLS) dihentikan di edge. Fitur gabungan ini memastikan bahwa asal aplikasi Anda hanya menerima permintaan web yang terbentuk dengan baik dan dilindungi dari serangan DDoS lapisan bawah, banjir koneksi, dan penyalahgunaan TLS.

  CloudFront menggunakan kombinasi arah lalu lintas DNS dan perutean anycast. Teknik-teknik ini meningkatkan ketahanan aplikasi Anda dengan mengurangi serangan yang dekat dengan sumbernya, memberikan isolasi kesalahan, dan memastikan akses ke kapasitas untuk mengurangi serangan terbesar yang diketahui.
- Route 53 — Mitigasi Shield hanya memungkinkan permintaan DNS yang valid untuk mencapai layanan. Shield mengurangi banjir kueri DNS menggunakan penilaian kecurigaan yang memprioritaskan kueri baik yang diketahui dan tidak memprioritaskan kueri yang berisi atribut serangan DDoS yang mencurigakan atau diketahui.

  Route 53 menggunakan sharding shuffle untuk menyediakan satu set unik dari empat alamat IP resolver ke setiap zona yang dihosting, untuk IPv4 dan IPv6. Setiap alamat IP sesuai dengan subset yang berbeda dari lokasi Route 53. Setiap subset lokasi terdiri dari server DNS otoritatif yang hanya sebagian tumpang tindih dengan infrastruktur di subset lainnya. Ini memastikan bahwa jika kueri pengguna gagal karena alasan apa pun, itu akan berhasil disajikan pada percobaan ulang.

  Route 53 menggunakan perutean anycast untuk mengarahkan kueri DNS ke lokasi tepi terdekat, berdasarkan kedekatan jaringan. Anycast juga menggemari lalu lintas DDoS ke banyak lokasi tepi, yang mencegah serangan berfokus pada satu lokasi.

Selain kecepatan mitigasi, CloudFront dan Route 53 menyediakan akses luas ke kapasitas Shield yang didistribusikan secara global. Untuk memanfaatkan kemampuan ini, gunakan layanan ini sebagai titik masuk aplikasi web dinamis atau statis Anda.

Untuk mempelajari lebih lanjut tentang menggunakan CloudFront dan Route 53 untuk melindungi aplikasi web, lihat Cara Membantu Melindungi Aplikasi Web Dinamis Terhadap Serangan DDoS dengan Menggunakan Amazon CloudFront dan Amazon Route 53. Untuk mempelajari lebih lanjut tentang isolasi kesalahan pada Rute 53, lihat Studi Kasus dalam Isolasi Kesalahan Global.

AWS Shield logika mitigasi untuk Wilayah AWS

Sumber daya yang diluncurkan di AWS Wilayah dilindungi oleh sistem mitigasi AWS Shield DDoS yang ditempatkan oleh deteksi tingkat sumber daya Shield. Sumber daya regional termasuk IP Elastis (EIP), Penyeimbang Beban Klasik, dan Penyeimbang Beban Aplikasi.

Sebelum menempatkan mitigasi, Shield mengidentifikasi sumber daya yang ditargetkan dan kapasitasnya. Shield menggunakan kapasitas untuk menentukan total lalu lintas maksimum yang mitigasi harus memungkinkan untuk diteruskan ke sumber daya. Daftar kontrol akses (ACL) dan pembentuk lain dalam mitigasi dapat mengurangi volume yang diizinkan untuk beberapa lalu lintas, misalnya lalu lintas yang cocok dengan vektor serangan DDoS yang diketahui atau yang tidak diharapkan datang dalam volume besar. Ini selanjutnya membatasi jumlah lalu lintas yang memungkinkan mitigasi untuk serangan refleksi UDP atau untuk lalu lintas TCP yang memiliki bendera TCP SYN atau FIN.

Shield menentukan kapasitas dan menempatkan mitigasi secara berbeda untuk setiap jenis sumber daya.

- Untuk instans Amazon EC2, atau EIP yang dilampirkan ke instans Amazon EC2, Shield menghitung kapasitas berdasarkan jenis instans dan atribut instans lainnya, seperti apakah instans telah mengaktifkan jaringan yang ditingkatkan.
- Untuk Application Load Balancer atau Classic Load Balancer, Shield menghitung kapasitas secara individual untuk setiap node yang ditargetkan dari load balancer. Mitigasi serangan DDoS untuk sumber daya ini disediakan oleh kombinasi mitigasi Shield DDoS dan penskalaan otomatis oleh penyeimbang beban. Ketika Shield Response Team (SRT) terlibat dalam serangan terhadap Application Load Balancer atau sumber daya Classic Load Balancer Klasik, mereka mungkin mempercepat penskalaan sebagai tindakan perlindungan tambahan.
- Shield menghitung kapasitas untuk beberapa AWS sumber daya didasarkan pada kapasitas yang tersedia dari AWS infrastruktur yang mendasarinya. Jenis sumber daya ini termasuk Network Load Balancers (NLBs) dan sumber daya yang mengarahkan lalu lintas melalui Gateway Load Balancers atau. AWS Network Firewall

> **Note**
>
> Lindungi Network Load Balancer Anda dengan melampirkan EIP yang dilindungi oleh Shield Advanced. Anda dapat bekerja dengan SRT untuk membangun mitigasi kustom yang didasarkan pada lalu lintas yang diharapkan dan kapasitas aplikasi yang mendasarinya.

Saat Shield menempatkan mitigasi, batas tarif awal yang ditentukan Shield dalam logika mitigasi diterapkan secara merata ke setiap sistem mitigasi Shield DDoS. Misalnya, jika Shield menempatkan mitigasi dengan batas 100.000 paket per detik (pps), awalnya akan memungkinkan 100.000 pps di setiap lokasi. Kemudian, Shield terus mengumpulkan metrik mitigasi untuk menentukan rasio lalu lintas yang sebenarnya, dan menggunakan rasio untuk menyesuaikan batas tarif untuk setiap lokasi. Ini mencegah positif palsu dan memastikan bahwa mitigasi tidak terlalu permisif.

AWS Shield logika mitigasi untuk AWS Global Accelerator akselerator standar

Mitigasi Shield hanya mengizinkan lalu lintas yang valid untuk mencapai titik akhir pendengar akselerator standar Global Accelerator. Akselerator standar digunakan secara global, dan mereka memberi Anda alamat IP yang dapat Anda gunakan untuk merutekan lalu lintas ke AWS sumber daya di Wilayah mana pun AWS . Batas tarif yang diberlakukan Shield untuk mitigasi Global Accelerator didasarkan pada kapasitas sumber daya tempat akselerator standar mengarahkan lalu lintas. Shield menempatkan mitigasi ketika total lalu lintas melebihi tingkat yang ditentukan, dan juga ketika sebagian kecil dari tingkat itu terlampaui untuk vektor DDoS yang diketahui.

Saat mengonfigurasi akselerator standar, Anda menentukan grup titik akhir untuk setiap AWS Wilayah tempat Anda akan merutekan lalu lintas untuk aplikasi Anda. Ketika Shield menempatkan mitigasi, Shield menghitung kapasitas setiap grup endpoint dan memperbarui batas tarif di setiap sistem mitigasi Shield DDoS yang sesuai. Tarif bervariasi untuk setiap lokasi, berdasarkan asumsi yang dibuat oleh Shield tentang bagaimana lalu lintas akan merutekan dari internet ke AWS sumber daya Anda. Kapasitas untuk grup endpoint dihitung sebagai jumlah sumber daya dalam grup dikalikan dengan kapasitas terendah untuk sumber daya apa pun dalam grup. Secara berkala, Shield menghitung ulang kapasitas aplikasi Anda dan memperbarui batas tarif sesuai kebutuhan.

> **Note**
>
> Menggunakan panggilan lalu lintas untuk mengubah persentase lalu lintas yang diarahkan ke grup endpoint tidak mengubah cara Shield menghitung atau mendistribusikan batas tarif ke sistem mitigasi DDoS-nya. Jika Anda menggunakan panggilan lalu lintas, konfigurasikan grup titik akhir Anda untuk mencerminkan satu sama lain dalam hal jenis dan kuantitas sumber daya. Ini membantu memastikan bahwa kapasitas yang dihitung oleh Shield mewakili sumber daya yang melayani lalu lintas untuk aplikasi Anda.

Untuk informasi selengkapnya tentang grup titik akhir dan panggilan lalu lintas di Global Accelerator, lihat Grup titik akhir dalam akselerator standar. AWS Global Accelerator

AWS Shield Advanced logika mitigasi untuk IP Elastis

Saat Anda melindungi Elastic IP (EIP) AWS Shield Advanced, Shield Advanced meningkatkan mitigasi yang ditempatkan Shield selama acara DDoS. Sistem mitigasi Shield Advanced DDoS mereplikasi konfigurasi Network ACL (NACL) untuk subnet publik yang terkait dengan EIP. Misalnya, jika NACL Anda dikonfigurasi untuk memblokir semua lalu lintas UDP, Shield Advanced menggabungkan aturan tersebut ke dalam mitigasi yang ditempatkan Shield.

Fungsionalitas tambahan ini dapat membantu Anda menghindari risiko ketersediaan karena lalu lintas yang tidak valid untuk aplikasi Anda. Anda juga dapat menggunakan NACL untuk memblokir alamat IP sumber individual atau rentang CIDR alamat IP sumber. Ini bisa menjadi alat mitigasi yang berguna untuk serangan DDoS yang tidak didistribusikan. Ini juga memungkinkan Anda dengan mudah mengelola daftar izin Anda sendiri atau untuk memblokir alamat IP yang seharusnya tidak berkomunikasi dengan aplikasi Anda, tanpa bergantung pada intervensi oleh AWS para insinyur.

AWS Shield Advanced logika mitigasi untuk aplikasi web

AWS Shield Advanced digunakan AWS WAF untuk mengurangi serangan lapisan aplikasi web. AWS WAF sudah termasuk dengan Shield Advanced tanpa biaya tambahan.

Perlindungan lapisan aplikasi standar

Bila Anda melindungi CloudFront distribusi Amazon atau Application Load Balancer dengan Shield Advanced, Anda dapat menggunakan Shield Advanced untuk mengaitkan ACL AWS WAF web dengan sumber daya yang dilindungi, jika Anda belum memiliki salah satu yang terkait. Jika Anda belum mengonfigurasi ACL web, Anda dapat menggunakan wizard konsol Shield Advanced untuk membuatnya dan menambahkan aturan berbasis kecepatan ke dalamnya. Aturan berbasis tarif membatasi jumlah permintaan per jendela waktu lima menit untuk setiap alamat IP, memberikan perlindungan dasar terhadap banjir permintaan lapisan aplikasi web. Anda dapat mengonfigurasi tarif, mulai serendah 100. Untuk informasi selengkapnya, lihat Shield Advanced Application Layer AWS WAF Web ACL dan aturan berbasis tarif.

Anda juga dapat menggunakan AWS WAF layanan ini untuk mengelola web ACL. Melalui AWS WAF, Anda dapat memperluas konfigurasi ACL web untuk melakukan hal-hal seperti memeriksa komponen permintaan web tertentu untuk kecocokan atau pola string, menambahkan permintaan kustom dan penanganan respons, dan mencocokkan dengan geolokasi asal permintaan. Untuk informasi selengkapnya tentang AWS WAF aturan, lihatAWS WAF aturan.

Mitigasi lapisan aplikasi otomatis

Untuk perlindungan yang ditingkatkan, aktifkan mitigasi lapisan aplikasi otomatis Shield Advanced. Dengan opsi ini, Shield Advanced mempertahankan aturan pembatasan AWS WAF laju untuk permintaan dari sumber DDoS yang dikenal dan menyediakan mitigasi khusus untuk serangan DDoS yang terdeteksi.

Ketika Shield Advanced mendeteksi serangan terhadap sumber daya yang dilindungi, ia mencoba mengidentifikasi tanda tangan serangan yang mengisolasi lalu lintas serangan dari lalu lintas normal ke aplikasi Anda. Shield Advanced mengevaluasi tanda tangan serangan yang diidentifikasi terhadap pola lalu lintas historis untuk sumber daya yang diserang, serta untuk sumber daya lain yang terkait dengan ACL web yang sama.

Jika Shield Advanced menentukan bahwa tanda tangan serangan hanya mengisolasi lalu lintas yang terlibat dalam serangan DDoS, itu mengimplementasikan tanda tangan dalam AWS WAF aturan di dalam ACL web terkait. Anda dapat menginstruksikan Shield Advanced untuk menempatkan mitigasi yang hanya menghitung lalu lintas yang cocok dengannya, atau yang memblokirnya, dan Anda dapat mengubah pengaturan kapan saja. Ketika Shield Advanced menentukan bahwa aturan mitigasi tidak lagi diperlukan, ia menghapusnya dari ACL web. Untuk informasi selengkapnya tentang mitigasi peristiwa lapisan aplikasi, lihat. Mitigasi DDoS lapisan aplikasi otomatis Shield Advanced

Untuk informasi selengkapnya tentang mitigasi lapisan aplikasi Shield Advanced, lihat. AWS Shield Advanced perlindungan lapisan aplikasi (lapisan 7)

Contoh arsitektur tangguh DDoS dasar

Ketahanan DDoS adalah kemampuan arsitektur aplikasi Anda untuk menahan serangan Distributed Denial of Service (DDoS) sambil terus melayani pengguna akhir yang sah. Aplikasi yang sangat tangguh dapat tetap tersedia selama serangan dengan dampak minimal pada metrik kinerja seperti kesalahan atau latensi. Bagian ini menunjukkan beberapa contoh arsitektur umum dan menjelaskan cara menggunakan kemampuan deteksi dan mitigasi DDoS yang disediakan oleh dan AWS Shield Advanced untuk meningkatkan ketahanan DDoS mereka.

Contoh arsitektur di bagian ini menyoroti AWS layanan yang memberikan manfaat ketahanan DDoS terbesar untuk aplikasi yang Anda gunakan. Manfaat dari layanan yang disorot meliputi:

- Akses ke kapasitas jaringan terdistribusi secara global — Layanan Amazon CloudFront, AWS Global Accelerator, dan Amazon Route 53 memberi Anda akses ke internet dan kapasitas mitigasi DDoS di seluruh jaringan edge AWS global. Ini berguna dalam mengurangi serangan volumetrik yang lebih besar, yang dapat mencapai skala terabit. Anda dapat menjalankan aplikasi Anda

di AWS Wilayah mana pun dan menggunakan layanan ini untuk melindungi ketersediaan dan mengoptimalkan kinerja untuk pengguna sah Anda.

- Perlindungan terhadap lapisan aplikasi web vektor serangan DDoS — Serangan DDoS lapisan aplikasi web paling baik dikurangi menggunakan kombinasi skala aplikasi dan firewall aplikasi web (WAF). Shield Advanced menggunakan log inspeksi permintaan web AWS WAF untuk mendeteksi anomali yang dapat dikurangi secara otomatis atau melalui keterlibatan dengan Tim Respons AWS Shield (SRT). Mitigasi otomatis tersedia melalui aturan AWS WAF berbasis tarif yang diterapkan dan juga melalui mitigasi DDoS lapisan aplikasi otomatis Shield Advanced.

Selain meninjau contoh-contoh ini, tinjau dan ikuti praktik terbaik yang berlaku di Praktik Terbaik untuk AWS Ketahanan DDoS.

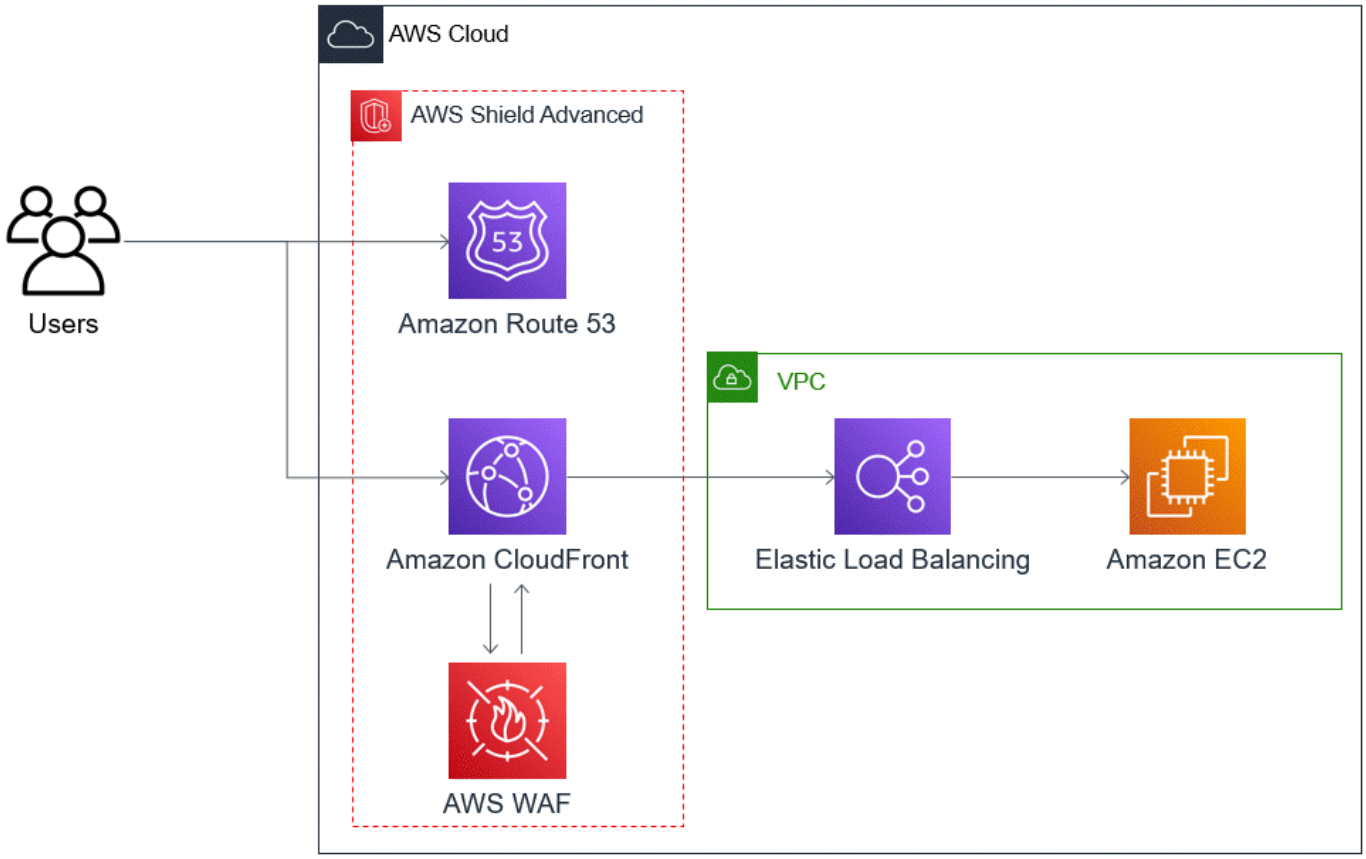
Contoh ketahanan DDoS untuk aplikasi web umum

Anda dapat membangun aplikasi web di AWS Wilayah mana pun dan menerima perlindungan DDoS otomatis dari kemampuan deteksi dan mitigasi yang AWS disediakan di Wilayah.

Contoh ini adalah untuk arsitektur yang mengarahkan pengguna ke aplikasi web menggunakan sumber daya seperti Classic Load Balancers, Application Load Balancers, Network Load Balancers, solusi AWS Marketplace, atau lapisan proxy Anda sendiri. Anda dapat meningkatkan ketahanan DDoS dengan memasukkan zona yang dihosting Amazon Route 53, CloudFront distribusi Amazon, dan ACL web antara sumber daya AWS WAF aplikasi web ini dan pengguna Anda. Penyisipan ini dapat mengaburkan asal aplikasi, melayani permintaan lebih dekat ke pengguna akhir Anda, dan mendeteksi dan mengurangi banjir permintaan lapisan aplikasi. Aplikasi yang menyajikan konten statis atau dinamis kepada pengguna Anda dengan CloudFront dan Route 53 dilindungi oleh sistem mitigasi DDoS terintegrasi dan sepenuhnya inline yang mengurangi serangan lapisan infrastruktur secara real time.

Dengan peningkatan arsitektur ini, Anda kemudian dapat melindungi zona yang dihosting Route 53 dan CloudFront distribusi Anda dengan Shield Advanced. Saat Anda melindungi CloudFront distribusi, Shield Advanced meminta Anda untuk mengaitkan ACL AWS WAF web dan membuat aturan berbasis kecepatan untuknya, dan memberi Anda opsi untuk mengaktifkan mitigasi DDoS lapisan aplikasi otomatis atau keterlibatan proaktif. Keterlibatan proaktif dan mitigasi DDoS lapisan aplikasi otomatis menggunakan pemeriksaan kesehatan Route 53 yang Anda kaitkan dengan sumber daya. Untuk mempelajari selengkapnya tentang opsi ini, lihat Perlindungan sumber daya di AWS Shield Advanced.

Diagram referensi berikut menggambarkan arsitektur tangguh DDoS ini untuk aplikasi web.



Manfaat yang diberikan pendekatan ini untuk aplikasi web Anda meliputi:

- Perlindungan terhadap serangan DDoS lapisan infrastruktur yang sering digunakan (lapisan 3 dan lapisan 4), tanpa penundaan deteksi. Selain itu, jika sumber daya sering ditargetkan, Shield Advanced menempatkan mitigasi untuk jangka waktu yang lebih lama. Shield Advanced juga menggunakan konteks aplikasi yang disimpulkan dari Network ACL (NACLS) untuk memblokir lalu lintas yang tidak diinginkan di hulu. Ini mengisolasi kegagalan lebih dekat ke sumbernya, meminimalkan efek pada pengguna yang sah.
- Perlindungan terhadap banjir TCP SYN. Sistem mitigasi DDoS yang terintegrasi denganCloudFront, Route 53, dan AWS Global Accelerator menyediakan kemampuan proxy TCP SYN yang menantang upaya koneksi baru dan hanya melayani pengguna yang sah.
- Perlindungan terhadap serangan lapisan aplikasi DNS, karena Route 53 bertanggung jawab untuk melayani tanggapan DNS otoritatif.
- Perlindungan terhadap banjir permintaan lapisan aplikasi web. Aturan berbasis tarif yang Anda konfigurasikan di ACL AWS WAF web Anda memblokir IP sumber saat mereka mengirim lebih banyak permintaan daripada yang diizinkan aturan.

- Mitigasi DDoS lapisan aplikasi otomatis untuk CloudFront distribusi Anda, jika Anda memilih untuk mengaktifkan opsi ini. Dengan mitigasi DDoS otomatis, Shield Advanced mempertahankan aturan berbasis tarif di ACL AWS WAF web terkait distribusi yang membatasi volume permintaan dari sumber DDoS yang diketahui. Selain itu, ketika Shield Advanced mendeteksi peristiwa yang memengaruhi kesehatan aplikasi Anda, secara otomatis akan membuat, menguji, dan mengelola aturan mitigasi di ACL web.
- Keterlibatan proaktif dengan Tim Respons Shield (SRT), jika Anda memilih untuk mengaktifkan opsi ini. Ketika Shield Advanced mendeteksi peristiwa yang memengaruhi kesehatan aplikasi Anda, SRT merespons dan secara proaktif terlibat dengan tim keamanan atau operasi Anda menggunakan informasi kontak yang Anda berikan. SRT menganalisis pola dalam lalu lintas Anda dan dapat memperbarui AWS WAF aturan Anda untuk memblokir serangan.

Contoh ketahanan DDoS untuk aplikasi TCP dan UDP

Contoh ini menunjukkan arsitektur tangguh DDoS untuk aplikasi TCP dan UDP di Wilayah AWS yang menggunakan instans Amazon Elastic Compute Cloud (Amazon EC2) atau alamat Elastic IP (EIP).

Anda dapat mengikuti contoh umum ini untuk meningkatkan ketahanan DDoS untuk jenis aplikasi berikut:

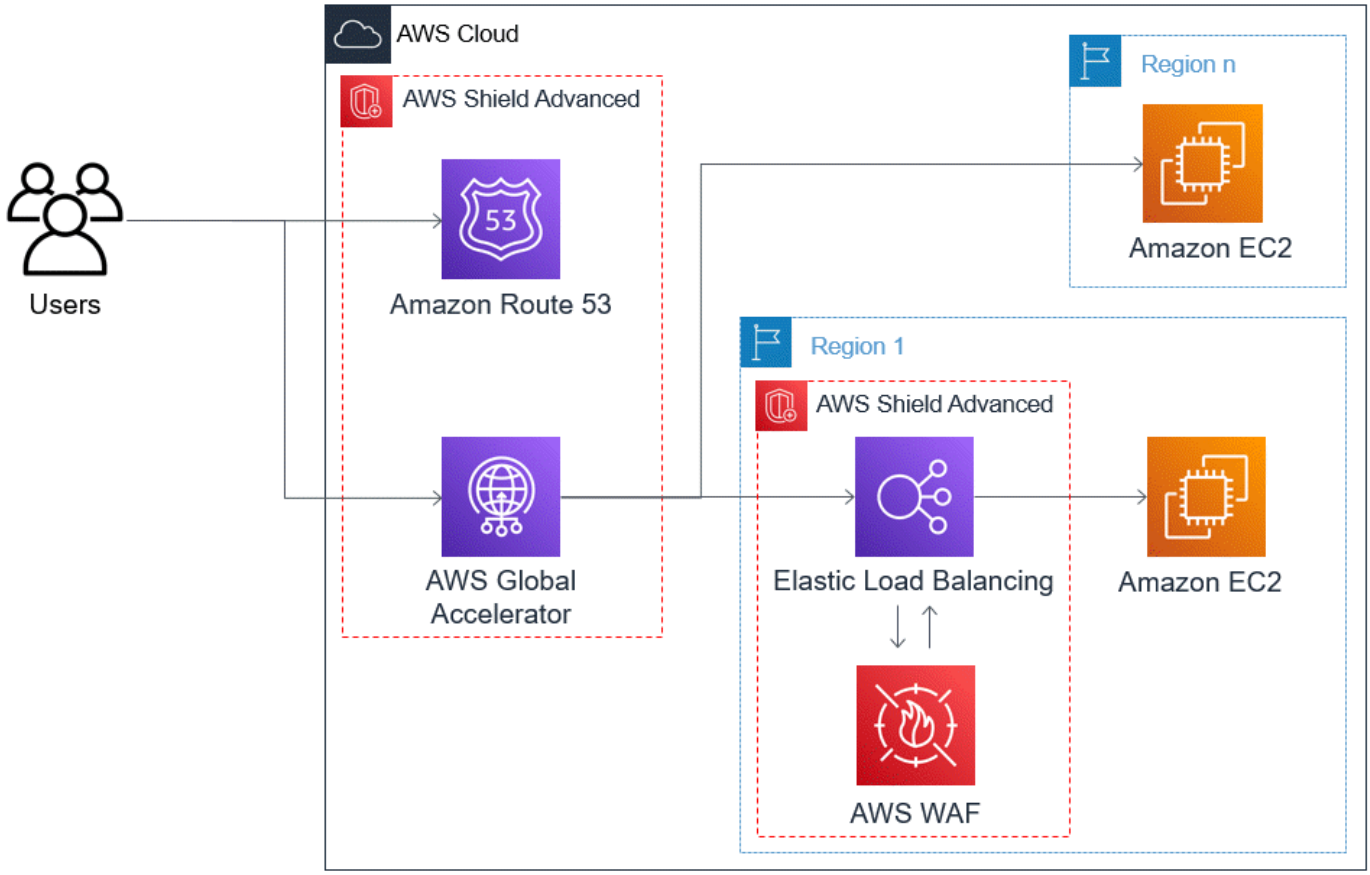
- Aplikasi TCP atau UDP. Misalnya, aplikasi yang digunakan untuk game, IoT, dan voice over IP.
- Aplikasi web yang memerlukan alamat IP statis atau yang menggunakan protokol yang CloudFront tidak didukung Amazon. Misalnya, aplikasi Anda mungkin memerlukan alamat IP yang dapat ditambahkan pengguna ke daftar izin firewall mereka, dan yang tidak digunakan oleh AWS pelanggan lain.

Anda dapat meningkatkan ketahanan DDoS untuk jenis aplikasi ini dengan memperkenalkan Amazon Route 53 dan. AWS Global Accelerator Layanan ini dapat mengarahkan pengguna ke aplikasi Anda dan mereka dapat menyediakan aplikasi Anda dengan alamat IP statis yang dirutekan di seluruh jaringan edge AWS global. Akselerator standar Global Accelerator dapat meningkatkan latensi pengguna hingga 60%. Jika Anda memiliki aplikasi web, Anda dapat mendeteksi dan mengurangi banjir permintaan lapisan aplikasi web dengan menjalankan aplikasi pada Application Load Balancer, dan kemudian melindungi Application Load Balancer dengan ACL web. AWS WAF

Setelah membuat aplikasi, lindungi zona yang dihosting Route 53, akselerator standar Akselerator Global, dan Penyeimbang Beban Aplikasi apa pun dengan Shield Advanced. Saat Anda melindungi Application Load Balancers, Anda dapat mengaitkan ACL AWS WAF web dan membuat aturan

berbasis kecepatan untuk mereka. Anda dapat mengonfigurasi keterlibatan proaktif dengan SRT untuk akselerator standar Akselerator Global dan Penyeimbang Beban Aplikasi Anda dengan mengaitkan pemeriksaan kesehatan Route 53 yang baru atau yang sudah ada. Untuk mempelajari lebih lanjut tentang opsi, lihatPerlindungan sumber daya di AWS Shield Advanced.

Diagram referensi berikut menggambarkan contoh arsitektur tangguh DDoS untuk aplikasi TCP dan UDP.



Manfaat yang diberikan pendekatan ini untuk aplikasi Anda meliputi:

- Perlindungan terhadap lapisan infrastruktur terbesar yang diketahui (lapisan 3 dan lapisan 4) serangan DDoS. Jika volume serangan menyebabkan kemacetan di hulu AWS, kegagalan akan diisolasi lebih dekat ke sumbernya dan akan memiliki efek yang diminimalkan pada pengguna sah Anda.
- Perlindungan terhadap serangan lapisan aplikasi DNS, karena Route 53 bertanggung jawab untuk melayani tanggapan DNS otoritatif.

- Jika Anda memiliki aplikasi web, pendekatan ini memberikan perlindungan terhadap banjir permintaan lapisan aplikasi web. Aturan berbasis tarif yang Anda konfigurasikan di ACL AWS WAF web Anda memblokir IP sumber saat mereka mengirim lebih banyak permintaan daripada yang diizinkan aturan.
- Keterlibatan proaktif dengan Tim Respons Shield (SRT), jika Anda memilih untuk mengaktifkan opsi ini untuk sumber daya yang memenuhi syarat. Ketika Shield Advanced mendeteksi peristiwa yang memengaruhi kesehatan aplikasi Anda, SRT merespons dan secara proaktif terlibat dengan tim keamanan atau operasi Anda menggunakan informasi kontak yang Anda berikan.

Contoh kasus penggunaan Shield Advanced

Anda dapat menggunakan Shield Advanced untuk melindungi sumber daya Anda dalam berbagai jenis skenario. Namun, dalam beberapa kasus Anda harus menggunakan layanan lain atau menggabungkan layanan lain dengan Shield Advanced untuk menawarkan perlindungan terbaik. Berikut ini adalah contoh cara menggunakan Shield Advanced atau AWS layanan lain untuk membantu melindungi sumber daya Anda.

Tujuan	Layanan yang disarankan	Dokumentasi layanan terkait
Melindungi aplikasi web dan RESTful API terhadap serangan DDoS	Shield Advanced melindungi CloudFront distribusi Amazon dan Application Load Balancer	Dokumentasi Elastic Load Balancing, Dokumentasi Amazon CloudFront
Melindungi aplikasi berbasis TCP terhadap serangan DDoS	Shield Advanced melindung i akselerator AWS Global Accelerator standar; dilampirk an ke alamat IP Elastis	AWS Global Accelerator Dokumentasi, dokumentasi Elastic Load Balancing
Lindungi server game berbasis UDP dari serangan DDoS	Shield Advanced melindung i instans Amazon EC2 yang dilampirkan ke alamat IP Elastis	Dokumentasi Cloud Komputasi Elastis Amazon

Misalnya, jika Anda menggunakan Shield Advanced untuk melindungi alamat IP Elastis, Shield Advanced melindungi sumber daya apa pun yang terkait dengannya. Selama serangan, Shield Advanced secara otomatis menyebarkan ACL jaringan Anda ke perbatasan jaringan. AWS Ketika

ACL jaringan Anda berada di perbatasan jaringan, Shield Advanced dapat memberikan perlindungan terhadap peristiwa DDoS yang lebih besar. Biasanya, ACL jaringan diterapkan di dekat instans Amazon EC2 Anda dalam VPC Amazon Anda. ACL jaringan dapat mengurangi serangan hanya sebesar yang dapat ditangani oleh VPC dan instans Amazon Anda. Jika antarmuka jaringan yang dilampirkan ke instans Amazon EC2 Anda dapat memproses hingga 10 Gbps, volume lebih dari 10 Gbps akan melambat dan mungkin memblokir lalu lintas ke instance itu. Selama serangan, Shield Advanced mempromosikan ACL jaringan Anda ke AWS perbatasan, yang dapat memproses beberapa terabyte lalu lintas. ACL jaringan Anda mampu memberikan perlindungan untuk sumber daya Anda jauh di luar kapasitas tipikal jaringan Anda. Untuk informasi selengkapnya tentang ACL jaringan, lihat ACL jaringan.

Memulai dengan AWS Shield Advanced

Tutorial ini memandu Anda untuk memulai AWS Shield Advanced menggunakan konsol Shield Advanced.

> **Note**
>
> Shield Advanced membutuhkan langganan, sementara AWS Shield Standard tidak. Perlindungan yang disediakan oleh Shield Standard tersedia gratis untuk semua AWS pelanggan.

Shield Advanced menyediakan deteksi DDoS tingkat lanjut dan perlindungan mitigasi untuk serangan lapisan jaringan (lapisan 3), lapisan transport (lapisan 4), dan lapisan aplikasi (lapisan 7). Untuk informasi selengkapnya tentang Shield Advanced, lihatAWS Shield Advanced ikhtisar.

Komunitas AWS teknis telah menerbitkan contoh proses otomatis untuk mengonfigurasi Shield Advanced menggunakan infrastruktur sebagai alat kode (IAc), AWS CloudFormation dan Terraform. Anda dapat menggunakan AWS Firewall Manager solusi ini jika akun Anda adalah bagian dari organisasi di AWS Organizations dan jika Anda melindungi jenis sumber daya apa pun kecuali Amazon Route 53 atau AWS Global Accelerator. Untuk menjelajahi opsi ini, lihat repositori kode di aws-samples/ aws-shield-advanced-one-click-deployment dan tutorial di One-click deployment dari Shield Advanced.

> **Note**
>
> Penting bagi Anda untuk mengonfigurasi sepenuhnya Shield Advanced sebelum acara Distributed Denial of Service (DDoS). Selesaikan konfigurasi untuk membantu memastikan bahwa aplikasi Anda dilindungi dan bahwa Anda siap untuk merespons jika aplikasi Anda dipengaruhi oleh serangan DDoS.

Lakukan langkah-langkah berikut secara berurutan untuk memulai menggunakan Shield Advanced.

Daftar Isi

Berlangganan AWS Shield Advanced

Anda harus berlangganan Shield Advanced untuk setiap Akun AWS yang ingin Anda lindungi. Anda tidak perlu berlangganan Shield Standard.

Penagihan langganan Shield Advanced

Jika Anda seorang Reseller AWS Saluran, bicarakan dengan tim akun Anda untuk informasi dan panduan. Informasi penagihan ini untuk pelanggan yang bukan AWS Channel Reseller.

Untuk yang lainnya, pedoman berlangganan dan penagihan berikut berlaku:

- Untuk akun yang merupakan anggota AWS Organizations organisasi, AWS menagih langganan Shield Advanced terhadap akun pembayar untuk organisasi, terlepas dari apakah akun pembayar itu sendiri berlangganan.

- Saat Anda berlangganan beberapa akun yang berada dalam keluarga akun penagihan AWS Organizations konsolidasi yang sama, satu harga langganan mencakup semua akun berlangganan dalam keluarga. Organisasi harus memiliki semua Akun AWS dan semua sumber daya mereka.
- Saat Anda berlangganan beberapa akun untuk beberapa organisasi, Anda masih dapat membayar satu biaya berlangganan di semua organisasi, akun, dan sumber daya yang menyediakan Anda memiliki semuanya. Hubungi manajer akun atau AWS dukungan Anda dan minta pengabaian biaya pada biaya AWS Shield Advanced berlangganan untuk semua kecuali satu organisasi.

Untuk informasi dan contoh harga terperinci, lihat AWS Shield Harga.

Sederhanakan langganan dengan AWS Firewall Manager

Jika akun Anda adalah bagian dari organisasi, kami sarankan Anda menggunakan AWS Firewall Manager jika Anda bisa, untuk mengotomatiskan langganan dan perlindungan Anda untuk organisasi. Firewall Manager mendukung semua jenis sumber daya yang dilindungi kecuali untuk Amazon Route 53 dan AWS Global Accelerator. Untuk menggunakan Firewall Manager, lihat AWS Firewall Manager danMemulai dengan AWS Firewall ManagerAWS Shield Advanced kebijakan.

Jika Anda tidak menggunakan Firewall Manager, untuk setiap akun dengan sumber daya untuk melindungi, berlangganan, dan menambahkan perlindungan menggunakan prosedur berikut.

Untuk berlangganan akun AWS Shield Advanced

1. Masuk ke AWS Management Console dan buka konsol AWS WAF & Shield di https://console.aws.amazon.com/wafv2/.
2. Di bilah AWS Shieldnavigasi, pilih Memulai. Pilih Berlangganan ke Shield Advanced.
3. Di halaman Berlangganan Shield Advanced, baca setiap jangka waktu perjanjian, lalu pilih semua kotak centang untuk menunjukkan bahwa Anda menerima persyaratan. Untuk akun dalam keluarga penagihan konsolidasi, Anda harus menyetujui persyaratan untuk setiap akun.

> **Important**
>
> Ketika Anda berlangganan, untuk berhenti berlangganan Anda harus menghubungi. AWS Support
> Untuk menonaktifkan autorenewal untuk langganan Anda, Anda harus menggunakan operasi Shield API atau perintah CLI UpdateSubscriptionupdate-subscription.

Pilih Berlangganan ke Shield Advanced. Ini berlangganan akun Anda ke Shield Advanced dan mengaktifkan layanan.

Akun Anda berlangganan. Lanjutkan melalui langkah-langkah berikut untuk melindungi sumber daya akun Anda dengan Shield Advanced.

> **Note**
>
> Shield Advanced tidak secara otomatis melindungi sumber daya Anda setelah berlangganan. Anda harus menentukan sumber daya yang Anda inginkan Shield Advanced untuk melindungi konfigurasi perlindungan.

Tambahkan sumber daya untuk melindungi dan mengonfigurasi perlindungan

Shield Advanced hanya melindungi sumber daya yang Anda tentukan, baik melalui Shield Advanced atau dalam kebijakan Firewall Manager Shield Advanced. Itu tidak secara otomatis melindungi sumber daya akun berlangganan.

Jika Anda menggunakan kebijakan AWS Firewall Manager Shield Advanced untuk perlindungan, Anda tidak perlu melakukan langkah ini. Anda mengonfigurasi kebijakan dengan jenis sumber daya yang akan dilindungi, dan Firewall Manager secara otomatis menambahkan perlindungan ke sumber daya yang berada dalam cakupan kebijakan.

Jika Anda tidak menggunakan Firewall Manager, ikuti prosedur berikut untuk setiap akun yang memiliki sumber daya untuk dilindungi.

Untuk memilih sumber daya yang akan dilindungi menggunakan Shield Advanced

1. Pilih Tambahkan sumber daya untuk melindungi dari halaman konfirmasi langganan prosedur sebelumnya, atau dari halaman Sumber daya atau Ikhtisar yang dilindungi.
2. Di halaman Pilih sumber daya untuk dilindungi dengan Shield Advanced, di Tentukan Wilayah dan jenis sumber daya, berikan spesifikasi Wilayah dan tipe sumber daya untuk sumber daya yang ingin Anda lindungi. Anda dapat melindungi sumber daya di beberapa Wilayah dengan memilih Semua Wilayah dan Anda dapat mempersempit pilihan ke sumber daya global dengan

memilih Global. Anda dapat membatalkan pilihan jenis sumber daya apa pun yang tidak ingin Anda lindungi. Untuk informasi tentang perlindungan untuk jenis sumber daya Anda, lihatAWS Shield Advanced perlindungan berdasarkan jenis sumber daya.

3. Pilih Muat sumber daya. Shield Advanced mengisi bagian Pilih Sumber Daya dengan AWS sumber daya yang sesuai dengan kriteria Anda.
4. Di bagian Pilih Sumber Daya, Anda dapat memfilter daftar sumber daya dengan memasukkan string untuk dicari di daftar sumber daya.

   Pilih sumber daya yang ingin Anda lindungi.
5. Di bagian Tag, jika Anda ingin menambahkan tag ke perlindungan Shield Advanced yang Anda buat, tentukan tag tersebut. Untuk informasi tentang menandai AWS sumber daya, lihat Bekerja dengan Editor Tag.
6. Pilih Lindungi dengan Shield Advanced. Ini menambahkan perlindungan Shield Advanced ke sumber daya.

Lanjutkan melalui layar wizard konsol untuk menyelesaikan konfigurasi perlindungan sumber daya Anda.

Topik

- Konfigurasikan perlindungan DDoS lapisan aplikasi (lapisan 7) dengan AWS WAF
- Konfigurasikan deteksi berbasis kesehatan untuk perlindungan Anda
- Konfigurasikan alarm dan notifikasi
- Tinjau dan selesaikan konfigurasi perlindungan Anda

Konfigurasikan perlindungan DDoS lapisan aplikasi (lapisan 7) dengan AWS WAF

Untuk melindungi sumber daya lapisan aplikasi, Shield Advanced menggunakan ACL AWS WAF web dengan aturan berbasis kecepatan sebagai titik awal. AWS WAF adalah firewall aplikasi web yang memungkinkan Anda memantau permintaan HTTP dan HTTPS yang diteruskan ke sumber daya lapisan aplikasi Anda, dan memungkinkan Anda mengontrol akses ke konten Anda berdasarkan karakteristik permintaan. Aturan berbasis tarif membatasi volume lalu lintas berdasarkan kriteria agregasi permintaan Anda, memberikan perlindungan DDoS dasar untuk aplikasi Anda. Lihat informasi yang lebih lengkap di Bagaimana cara AWS WAF kerja dan Pernyataan aturan berbasis tarif.

Anda juga dapat secara opsional mengaktifkan mitigasi DDoS lapisan aplikasi otomatis Shield Advanced, untuk memiliki permintaan batas tarif Shield Advanced dari sumber DDoS yang dikenal dan secara otomatis memberikan perlindungan khusus insiden untuk Anda.

> **Important**
>
> Jika Anda mengelola perlindungan Shield Advanced AWS Firewall Manager dengan menggunakan kebijakan Shield Advanced, Anda tidak dapat mengelola perlindungan lapisan aplikasi di sini. Anda harus mengelolanya dalam kebijakan Firewall Manager Shield Advanced Anda.

Langganan dan biaya Shield Advanced AWS WAF

Langganan Shield Advanced Anda menanggung biaya penggunaan AWS WAF kemampuan standar untuk sumber daya yang Anda lindungi dengan Shield Advanced. AWS WAF Biaya standar yang ditanggung oleh perlindungan Shield Advanced Anda adalah biaya per ACL web, biaya per aturan, dan harga dasar per juta permintaan untuk pemeriksaan permintaan web, hingga 1.500 WCU, dan hingga ukuran badan default.

Mengaktifkan mitigasi DDoS lapisan aplikasi otomatis Shield Advanced menambahkan grup aturan ke ACL web Anda yang menggunakan 150 unit kapasitas ACL web (WCU). WCU ini dihitung terhadap penggunaan WCU di ACL web Anda. Lihat informasi selengkapnya di Mitigasi DDoS lapisan aplikasi otomatis Shield Advanced, Grup aturan Shield Advanced, dan AWS WAF unit kapasitas ACL web (WCU).

Langganan Anda ke Shield Advanced tidak mencakup AWS WAF penggunaan sumber daya yang tidak Anda lindungi menggunakan Shield Advanced. Ini juga tidak mencakup AWS WAF biaya non-standar tambahan untuk sumber daya yang dilindungi. Contoh biaya non-standar adalah AWS WAF biaya untuk Kontrol Bot, untuk tindakan CAPTCHA aturan, untuk ACL web yang menggunakan lebih dari 1.500 WCU, dan untuk memeriksa badan permintaan di luar ukuran tubuh default. Daftar lengkap disediakan di halaman AWS WAF harga.

Untuk informasi selengkapnya dan contoh harga, lihat Harga dan AWS WAF Harga Shield.

Untuk mengonfigurasi perlindungan lapisan 7 DDoS untuk Wilayah

Shield Advanced memberi Anda opsi untuk mengonfigurasi mitigasi lapisan 7 DDoS untuk setiap Wilayah tempat sumber daya pilihan Anda berada. Jika Anda menambahkan perlindungan di beberapa wilayah, wizard memandu Anda melalui prosedur berikut untuk setiap Wilayah.

1. Halaman Configure layer 7 DDoS protections mencantumkan setiap sumber daya yang belum terkait dengan ACL web. Untuk masing-masing, pilih ACL web yang ada atau buat ACL web baru. Untuk sumber daya apa pun yang sudah memiliki ACL web terkait, Anda dapat mengubah ACL web dengan terlebih dahulu memisahkan yang sekarang. AWS WAF Untuk informasi selengkapnya, lihat Mengaitkan atau memisahkan ACL web dengan sumber daya AWS.

   Untuk ACL web yang belum memiliki aturan berbasis kecepatan, wizard konfigurasi meminta Anda untuk menambahkannya. Aturan berbasis tarif membatasi lalu lintas dari alamat IP ketika mereka mengirim permintaan volume tinggi. Aturan berbasis tarif membantu melindungi aplikasi Anda dari banjir permintaan web dan dapat memberikan peringatan tentang lonjakan lalu lintas mendadak yang mungkin mengindikasikan potensi serangan DDoS. Tambahkan aturan berbasis tarif ke ACL web dengan memilih Tambahkan aturan batas tingkat dan kemudian berikan batas tarif dan tindakan aturan. Anda dapat mengonfigurasi perlindungan tambahan di ACL web melalui. AWS WAF

   Untuk informasi tentang penggunaan ACL web dan aturan berbasis tarif dalam perlindungan Shield Advanced Anda, termasuk opsi konfigurasi tambahan untuk aturan berbasis tarif, lihat. Shield Advanced Application Layer AWS WAF Web ACL dan aturan berbasis tarif

2. Untuk mitigasi DDoS lapisan aplikasi Otomatis, jika Anda ingin Shield Advanced secara otomatis mengurangi serangan DDoS terhadap sumber daya lapisan aplikasi Anda, pilih Aktifkan dan kemudian pilih AWS WAF tindakan aturan yang ingin digunakan Shield Advanced dalam aturan kustomnya. Pengaturan ini berlaku untuk semua ACL web untuk sumber daya yang Anda kelola dalam sesi wizard ini.

   Dengan mitigasi DDoS lapisan aplikasi otomatis, Shield Advanced mempertahankan aturan berbasis kecepatan di ACL AWS WAF web sumber daya yang membatasi volume permintaan dari sumber DDoS yang dikenal. Selain itu, Shield Advanced membandingkan pola lalu lintas saat ini dengan garis dasar lalu lintas bersejarah untuk mendeteksi penyimpangan yang mungkin mengindikasikan serangan DDoS. Ketika Shield Advanced mendeteksi serangan DDoS, ia merespons dengan membuat, mengevaluasi, dan menerapkan aturan khusus untuk merespons. AWS WAF Anda menentukan apakah aturan kustom menghitung atau memblokir serangan atas nama Anda.

   > **Note**
   >
   > Mitigasi DDoS lapisan aplikasi otomatis hanya berfungsi dengan ACL web yang dibuat menggunakan versi terbaru (v2). AWS WAF

Untuk informasi selengkapnya tentang mitigasi DDoS lapisan aplikasi otomatis Shield Advanced, termasuk peringatan dan praktik terbaik untuk menggunakan fitur ini, lihat. Mitigasi DDoS lapisan aplikasi otomatis Shield Advanced

3. Pilih Berikutnya. Wisaya konsol maju ke halaman deteksi berbasis kesehatan.

Konfigurasikan deteksi berbasis kesehatan untuk perlindungan Anda

Konfigurasikan Shield Advanced untuk menggunakan deteksi berbasis kesehatan untuk meningkatkan daya tanggap dan akurasi dalam deteksi dan mitigasi serangan. Pemeriksaan kesehatan yang dikonfigurasi dengan baik sangat penting untuk deteksi kejadian yang akurat. Anda dapat mengonfigurasi deteksi berbasis kesehatan untuk semua jenis sumber daya kecuali untuk zona yang dihosting Route 53.

Untuk menggunakan deteksi berbasis kesehatan, tentukan pemeriksaan kesehatan untuk sumber daya Anda di Route 53, lalu kaitkan pemeriksaan kesehatan dengan perlindungan Shield Advanced Anda. Penting bahwa pemeriksaan kesehatan yang Anda konfigurasikan secara akurat mencerminkan kesehatan sumber daya. Untuk informasi dan contoh untuk mengonfigurasi pemeriksaan kesehatan yang akan digunakan dengan Shield Advanced, lihatDeteksi berbasis kesehatan menggunakan pemeriksaan kesehatan.

Pemeriksaan kesehatan diperlukan untuk dukungan keterlibatan proaktif Shield Response Team (SRT). Untuk informasi tentang keterlibatan proaktif, lihatMengkonfigurasi keterlibatan proaktif.

> **Note**
>
> Pemeriksaan kesehatan harus dilaporkan sehat saat Anda mengaitkannya dengan perlindungan Shield Advanced Anda.

Untuk mengonfigurasi deteksi berbasis kesehatan

1. Di bawah Pemeriksaan Kesehatan Terkait, pilih ID pemeriksaan kesehatan yang ingin Anda kaitkan dengan perlindungan.

> **Note**
>
> Jika Anda tidak melihat pemeriksaan kesehatan yang Anda butuhkan, buka konsol Route 53 dan verifikasi pemeriksaan kesehatan dan ID-nya. Untuk selengkapnya, lihat Membuat dan Memperbarui Pemeriksaan Kesehatan.

2. Pilih Berikutnya. Wisaya konsol maju ke halaman alarm dan notifikasi.

Konfigurasikan alarm dan notifikasi

Anda dapat mengonfigurasi notifikasi Amazon Simple Notification Service secara opsional untuk CloudWatch alarm Amazon yang terdeteksi dan aktivitas aturan berbasis kecepatan. Anda dapat menggunakannya untuk menerima pemberitahuan saat Shield mendeteksi peristiwa pada sumber daya yang dilindungi atau ketika batas kecepatan yang dikonfigurasi dalam aturan berbasis laju terlampaui.

Untuk informasi tentang CloudWatch metrik Shield Advanced, lihatAWS Shield Advanced metrik. Untuk informasi tentang Amazon SNS, lihat Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

Untuk mengkonfigurasi alarm dan notifikasi

1. Pilih topik Amazon SNS yang ingin Anda notifikasi. Anda dapat menggunakan satu topik Amazon SNS untuk semua sumber daya yang dilindungi dan aturan berbasis tarif, atau Anda dapat memilih topik yang berbeda, yang disesuaikan dengan organisasi Anda. Misalnya, Anda dapat membuat topik SNS untuk setiap tim yang bertanggung jawab atas respons insiden untuk kumpulan sumber daya tertentu.
2. Pilih Berikutnya. Wisaya konsol maju ke halaman tinjauan perlindungan sumber daya.

Tinjau dan selesaikan konfigurasi perlindungan Anda

Untuk meninjau dan mengonfigurasi pengaturan

1. Di halaman Tinjau dan konfigurasikan mitigasi dan visibilitas DDoS, tinjau pengaturan Anda. Untuk melakukan modifikasi, pilih Edit di area yang ingin Anda modifikasi. Ini akan membawa Anda kembali ke halaman terkait di wizard konsol. Buat perubahan, lalu pilih Berikutnya di

halaman berikutnya hingga Anda kembali ke halaman Tinjauan dan konfigurasikan halaman mitigasi dan visibilitas DDoS.

2. Pilih Selesai konfigurasi. Halaman Sumber daya yang dilindungi mencantumkan sumber daya Anda yang baru dilindungi.

Konfigurasikan AWS dukungan SRT

Shield Response Team (SRT) adalah insinyur keamanan yang berspesialisasi dalam respons acara DDoS. Anda dapat menambahkan izin yang memungkinkan SRT mengelola sumber daya atas nama Anda selama acara DDoS. Selain itu, Anda dapat mengonfigurasi SRT untuk terlibat secara proaktif dengan Anda jika pemeriksaan kesehatan Route 53 yang terkait dengan sumber daya yang dilindungi tidak sehat selama peristiwa yang terdeteksi. Kedua penambahan ini pada perlindungan Anda memungkinkan respons yang lebih cepat terhadap peristiwa DDoS.

> **Note**
>
> Untuk menggunakan layanan dari Shield Response Team (SRT), Anda harus berlangganan paket Business Support atau paket Enterprise Support.

SRT dapat memantau data AWS WAF permintaan dan log selama peristiwa lapisan aplikasi untuk mengidentifikasi lalu lintas anomali. Mereka dapat membantu menyusun AWS WAF aturan khusus untuk mengurangi sumber lalu lintas yang menyinggung. Sesuai kebutuhan, SRT mungkin membuat rekomendasi arsitektur untuk membantu Anda menyelaraskan sumber daya Anda dengan rekomendasi dengan AWS lebih baik.

Untuk informasi lebih lanjut tentang SRT, lihatDukungan Shield Response Team (SRT).

Untuk memberikan izin ke SRT

1. Di halaman Ikhtisar AWS Shield konsol, di bawah Konfigurasi dukungan AWS SRT, pilih Edit akses SRT. Halaman akses Edit AWS Shield Response Team (SRT) terbuka.
2. Untuk pengaturan akses SRT pilih salah satu opsi:

   - Jangan berikan SRT akses ke akun saya — Shield menghapus izin apa pun yang sebelumnya Anda berikan kepada SRT untuk mengakses akun dan sumber daya Anda.
   - Buat peran baru bagi SRT untuk mengakses akun saya — Shield membuat peran yang mempercayai prinsip layanan`drt.shield.amazonaws.com`, yang mewakili SRT, dan

melampirkan kebijakan terkelola padanya. `AWSShieldDRTAccessPolicy` Kebijakan terkelola memungkinkan SRT melakukan AWS Shield Advanced dan panggilan AWS WAF API atas nama Anda dan mengakses AWS WAF log Anda. Untuk informasi selengkapnya tentang kebijakan terkelola, lihat AWS kebijakan terkelola: AWSShieldDRTAccessPolicy.

- Pilih peran yang ada untuk SRT untuk mengakses akun saya — Untuk opsi ini, Anda harus mengubah konfigurasi peran di AWS Identity and Access Management (IAM) sebagai berikut:
  - Lampirkan kebijakan yang dikelola `AWSShieldDRTAccessPolicy` ke peran. Kebijakan terkelola ini memungkinkan SRT melakukan AWS Shield Advanced dan panggilan AWS WAF API atas nama Anda dan mengakses AWS WAF log Anda. Untuk informasi selengkapnya tentang kebijakan terkelola, lihat AWS kebijakan terkelola: AWSShieldDRTAccessPolicy. Untuk informasi tentang melampirkan kebijakan terkelola ke peran Anda, lihat Melampirkan dan Melepaskan Kebijakan IAM.
  - Ubah peran untuk mempercayai kepala layanan`drt.shield.amazonaws.com`. Ini adalah prinsip layanan yang mewakili SRT. Untuk informasi selengkapnya, lihat IAM JSON Policy Elements: Principal.

3. Pilih Simpan untuk menyimpan perubahan Anda.

Untuk informasi selengkapnya tentang memberikan SRT akses ke perlindungan dan data Anda, lihat. Mengkonfigurasi akses untuk Shield Response Team (SRT)

Untuk mengaktifkan keterlibatan proaktif SRT

1. Di halaman Ikhtisar AWS Shield konsol, di bawah Keterlibatan proaktif dan kontak, di area kontak, pilih Edit.

   Di halaman Edit kontak, berikan informasi kontak untuk orang yang Anda ingin SRT hubungi untuk keterlibatan proaktif.

   Jika Anda memberikan lebih dari satu kontak, dalam Catatan, tunjukkan keadaan di mana setiap kontak harus digunakan. Sertakan penunjukan kontak primer dan sekunder, dan berikan jam ketersediaan dan zona waktu untuk setiap kontak.

   Contoh catatan kontak:

   - Ini adalah hotline yang memiliki staf 24x7x365. Silakan bekerja dengan analis yang merespons dan mereka akan mendapatkan orang yang tepat pada panggilan.
   - Silakan hubungi saya jika hotline tidak merespons dalam waktu 5 menit.

2. Pilih Simpan.

   Halaman Ikhtisar mencerminkan informasi kontak yang diperbarui.

3. Pilih Edit fitur keterlibatan proaktif, pilih Aktifkan, lalu pilih Simpan untuk mengaktifkan keterlibatan proaktif.

Untuk informasi selengkapnya tentang keterlibatan proaktif, lihatMengkonfigurasi keterlibatan proaktif.

Buat dasbor DDoS CloudWatch dan atur alarm CloudWatch

Anda dapat memantau aktivitas DDoS potensial menggunakan Amazon CloudWatch, yang mengumpulkan data mentah dari Shield Advanced dan memprosesnya menjadi metrik hampir real-time yang dapat dibaca. Anda dapat menggunakan statistik CloudWatch untuk mendapatkan perspektif tentang kinerja aplikasi atau layanan web Anda. Untuk informasi selengkapnya tentang penggunaan CloudWatch, lihat Apa yang ada CloudWatch di Panduan CloudWatch Pengguna Amazon.

- Untuk instruksi untuk membuat CloudWatch dasbor, lihatPemantauan CloudWatch dengan Amazon.
- Untuk deskripsi metrik Shield Advanced yang dapat ditambahkan ke dasbor, lihat. AWS Shield Advanced metrik

Shield Advanced melaporkan metrik sumber daya CloudWatch lebih sering selama peristiwa DDoS daripada saat tidak ada acara yang sedang berlangsung. Shield Advanced melaporkan metrik satu menit sekali selama acara, dan kemudian sekali tepat setelah acara berakhir. Meskipun tidak ada peristiwa yang sedang berlangsung, Shield Advanced melaporkan metrik sekali sehari, pada waktu yang ditetapkan ke sumber daya. Laporan berkala ini membuat metrik tetap aktif dan tersedia untuk digunakan di CloudWatch alarm kustom Anda.

Ini melengkapi tutorial untuk memulai dengan Shield Advanced. Untuk memanfaatkan sepenuhnya perlindungan yang Anda pilih, lanjutkan menjelajahi fitur dan opsi Shield Advanced. Untuk memulai, biasakan diri Anda dengan opsi Anda untuk melihat dan menanggapi acara di Visibilitas ke acara DDoS danMenanggapi peristiwa DDoS.

Dukungan Shield Response Team (SRT)

Shield Response Team (SRT) menyediakan dukungan tambahan untuk pelanggan Shield Advanced. SRT adalah insinyur keamanan yang berspesialisasi dalam respons acara DDoS. Sebagai lapisan dukungan tambahan untuk AWS Support rencana Anda, Anda dapat bekerja secara langsung dengan SRT, memanfaatkan keahlian mereka sebagai bagian dari alur kerja respons acara Anda. Untuk informasi tentang opsi dan panduan konfigurasi, lihat topik berikut.

> **Note**
>
> Untuk menggunakan layanan dari Shield Response Team (SRT), Anda harus berlangganan paket Business Support atau paket Enterprise Support.

Kegiatan dukungan SRT

Tujuan utama dalam keterlibatan dengan SRT adalah untuk melindungi ketersediaan dan kinerja aplikasi Anda. Bergantung pada jenis acara DDoS dan arsitektur aplikasi Anda, SRT dapat mengambil satu atau beberapa tindakan berikut:

- AWS WAF analisis log dan aturan — Untuk sumber daya yang menggunakan ACL AWS WAF web, SRT dapat menganalisis AWS WAF log Anda untuk mengidentifikasi karakteristik serangan dalam permintaan web aplikasi Anda. Dengan persetujuan Anda selama keterlibatan, SRT dapat menerapkan perubahan pada ACL web Anda untuk memblokir serangan yang telah mereka identifikasi.
- Membangun mitigasi jaringan kustom — SRT dapat menulis mitigasi kustom untuk Anda untuk serangan lapisan infrastruktur. SRT dapat bekerja dengan Anda untuk memahami lalu lintas yang diharapkan untuk aplikasi Anda, untuk memblokir lalu lintas yang tidak terduga, dan untuk mengoptimalkan batas tarif paket per detik. Untuk informasi selengkapnya, lihat Mengkonfigurasi mitigasi kustom dengan Shield Response Team (SRT).
- Rekayasa lalu lintas jaringan — SRT bekerja sama dengan tim AWS jaringan untuk melindungi pelanggan Shield Advanced. Bila diperlukan, AWS dapat mengubah bagaimana lalu lintas internet tiba di AWS jaringan untuk mengalokasikan lebih banyak kapasitas mitigasi untuk aplikasi Anda.
- Rekomendasi arsitektur — SRT dapat menentukan bahwa mitigasi terbaik untuk serangan memerlukan perubahan arsitektur agar lebih selaras dengan praktik AWS terbaik, dan mereka akan membantu mendukung penerapan praktik ini. Untuk selengkapnya, lihat Praktik AWS Terbaik untuk Ketahanan DDoS.

Topik

Mengkonfigurasi akses untuk Shield Response Team (SRT)

Anda dapat memberikan izin kepada Tim Respons Shield (SRT) untuk bertindak atas nama Anda, mengakses AWS WAF log, dan melakukan panggilan ke AWS WAF API AWS Shield Advanced dan mengelola perlindungan. Selama peristiwa DDoS lapisan aplikasi, SRT dapat memantau AWS WAF permintaan untuk mengidentifikasi lalu lintas anomali dan membantu menyusun AWS WAF aturan khusus untuk mengurangi sumber lalu lintas yang menyinggung.

Selain itu, Anda dapat memberikan SRT akses ke data lain yang telah Anda simpan di bucket Amazon S3, seperti tangkapan paket atau log dari Application Load Balancer, CloudFront Amazon, atau dari sumber pihak ketiga.

> **Note**
>
> Untuk menggunakan layanan dari Shield Response Team (SRT), Anda harus berlangganan paket Business Support atau paket Enterprise Support.

Untuk mengelola izin untuk SRT

1. Di halaman Ikhtisar AWS Shield konsol, di bawah Konfigurasi dukungan AWS SRT, pilih Edit akses SRT. Halaman akses Edit AWS Shield Response Team (SRT) terbuka.
2. Untuk pengaturan akses SRT pilih salah satu opsi:

   - Jangan berikan SRT akses ke akun saya — Shield menghapus izin apa pun yang sebelumnya Anda berikan kepada SRT untuk mengakses akun dan sumber daya Anda.
   - Buat peran baru bagi SRT untuk mengakses akun saya — Shield membuat peran yang mempercayai prinsip layanan`drt.shield.amazonaws.com`, yang mewakili SRT, dan melampirkan kebijakan terkelola padanya. `AWSShieldDRTAccessPolicy` Kebijakan terkelola memungkinkan SRT melakukan AWS Shield Advanced dan panggilan AWS WAF

API atas nama Anda dan mengakses AWS WAF log Anda. Untuk informasi selengkapnya tentang kebijakan terkelola, lihat AWS kebijakan terkelola: AWSShieldDRTAccessPolicy.

- Pilih peran yang ada untuk SRT untuk mengakses akun saya — Untuk opsi ini, Anda harus mengubah konfigurasi peran di AWS Identity and Access Management (IAM) sebagai berikut:
  - Lampirkan kebijakan yang dikelola `AWSShieldDRTAccessPolicy` ke peran. Kebijakan terkelola ini memungkinkan SRT melakukan AWS Shield Advanced dan panggilan AWS WAF API atas nama Anda dan mengakses AWS WAF log Anda. Untuk informasi selengkapnya tentang kebijakan terkelola, lihat AWS kebijakan terkelola: AWSShieldDRTAccessPolicy. Untuk informasi tentang melampirkan kebijakan terkelola ke peran Anda, lihat Melampirkan dan Melepaskan Kebijakan IAM.
  - Ubah peran untuk mempercayai kepala layanan`drt.shield.amazonaws.com`. Ini adalah prinsip layanan yang mewakili SRT. Untuk informasi selengkapnya, lihat IAM JSON Policy Elements: Principal.

3. Untuk (Opsional): Berikan akses SRT ke bucket Amazon S3, jika Anda perlu berbagi data yang tidak ada di log ACL web AWS WAF Anda, konfigurasikan ini. Misalnya, Application Load Balancer mengakses log, log Amazon CloudFront , atau log dari sumber pihak ketiga.

   > **Note**
   >
   > Anda tidak perlu melakukan ini untuk log ACL AWS WAF web Anda. SRT mendapatkan akses ke mereka ketika Anda memberikan akses ke akun Anda.

   a. Konfigurasikan bucket Amazon S3 sesuai dengan pedoman berikut:

      - Lokasi bucket harus Akun AWS sama dengan yang Anda berikan kepada SRT akses umum, pada langkah sebelumnya akses AWS Shield Response Team (SRT).
      - Ember dapat berupa plaintext atau SSE-S3 dienkripsi. Untuk informasi selengkapnya tentang enkripsi Amazon S3 SSE-S3, lihat Melindungi Data Menggunakan Enkripsi Sisi Server dengan Kunci Enkripsi Terkelola Amazon S3 (SSE-S3) di Panduan Pengguna Amazon S3.

        SRT tidak dapat melihat atau memproses log yang disimpan dalam bucket yang dienkripsi dengan kunci yang disimpan di (). AWS Key Management Service AWS KMS

b. Di Shield Advanced (Opsional): Berikan akses SRT ke bagian bucket Amazon S3, untuk setiap bucket Amazon S3 tempat data atau log Anda disimpan, masukkan nama bucket dan pilih Tambahkan Bucket. Anda dapat menambahkan hingga 10 ember.

   Ini memberi SRT izin berikut pada setiap bucket:`s3:GetBucketLocation`,, `s3:GetObject` dan. `s3:ListBucket`

   Jika Anda ingin memberikan izin SRT untuk mengakses lebih dari 10 bucket, Anda dapat melakukannya dengan mengedit kebijakan bucket tambahan dan secara manual memberikan izin yang tercantum di sini untuk SRT.

   Berikut ini menunjukkan contoh daftar kebijakan.

```
{
    "Sid": "AWSDDoSResponseTeamAccessS3Bucket",
    "Effect": "Allow",
    "Principal": {
        "Service": "drt.shield.amazonaws.com"
    },
    "Action": [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket"
    ],
    "Resource": [
        "arn:aws:s3:::bucket-name",
        "arn:aws:s3:::bucket-name/*"
    ]
}
```

4. Pilih Simpan untuk menyimpan perubahan Anda.

Anda juga dapat mengotorisasi SRT melalui API dengan membuat peran IAM, melampirkan kebijakan padanya, dan kemudian meneruskan peran tersebut AWSShieldDRTAccessPolicy ke operasi AssociateDrTrole.

Mengkonfigurasi keterlibatan proaktif

Dengan keterlibatan proaktif, Tim Respons Shield (SRT) menghubungi Anda secara langsung ketika ketersediaan atau kinerja aplikasi Anda terpengaruh karena kemungkinan serangan. Kami merekomendasikan model keterlibatan ini karena memberikan respons SRT tercepat dan

memungkinkan SRT untuk memulai pemecahan masalah bahkan sebelum mereka menjalin kontak dengan Anda.

Keterlibatan proaktif tersedia untuk kejadian lapisan jaringan dan lapisan transportasi pada alamat IP Elastis dan akselerator AWS Global Accelerator standar, dan untuk banjir permintaan web pada distribusi Amazon dan Application Load Balancer. CloudFront Keterlibatan proaktif hanya tersedia untuk perlindungan sumber daya Shield Advanced yang memiliki pemeriksaan kesehatan Amazon Route 53 terkait. Untuk informasi tentang mengelola dan menggunakan pemeriksaan kesehatan, lihatDeteksi berbasis kesehatan menggunakan pemeriksaan kesehatan.

Selama acara yang terdeteksi oleh Shield Advanced, SRT menggunakan status pemeriksaan kesehatan Anda untuk menentukan apakah acara tersebut memenuhi syarat untuk keterlibatan proaktif. Jika demikian, SRT akan menghubungi Anda sesuai dengan panduan kontak yang Anda berikan dalam konfigurasi keterlibatan proaktif Anda.

Anda dapat mengonfigurasi hingga sepuluh kontak untuk keterlibatan proaktif, dan Anda dapat memberikan catatan untuk memandu SRT dalam menjangkau Anda. Kontak keterlibatan proaktif Anda harus tersedia untuk terlibat dengan SRT selama acara. Jika Anda tidak memiliki pusat operasi 24/7, Anda dapat memberikan kontak pager dan menunjukkan preferensi kontak ini di catatan kontak Anda.

Keterlibatan proaktif mengharuskan Anda melakukan hal berikut:

- Anda harus berlangganan paket Business Support atau paket Enterprise Support.
- Anda harus mengaitkan pemeriksaan kesehatan Amazon Route 53 dengan sumber daya apa pun yang ingin Anda lindungi dengan keterlibatan proaktif. SRT menggunakan status pemeriksaan kesehatan Anda untuk membantu menentukan apakah suatu peristiwa memerlukan keterlibatan proaktif, jadi penting bahwa pemeriksaan kesehatan Anda secara akurat mencerminkan keadaan sumber daya Anda yang dilindungi. Untuk informasi dan panduan lebih lanjut, lihatDeteksi berbasis kesehatan menggunakan pemeriksaan kesehatan.
- Untuk sumber daya yang terkait dengan ACL AWS WAF web, Anda harus membuat ACL web menggunakan AWS WAF (v2), yang merupakan versi terbaru dari. AWS WAF
- Anda harus menyediakan setidaknya satu kontak untuk SRT untuk digunakan untuk keterlibatan proaktif selama acara. Jaga informasi kontak Anda lengkap dan up to date.

Untuk mengaktifkan keterlibatan proaktif SRT

1. Di halaman Ikhtisar AWS Shield konsol, di bawah Keterlibatan proaktif dan kontak, di area kontak, pilih Edit.

   Di halaman Edit kontak, berikan informasi kontak untuk orang yang Anda ingin SRT hubungi untuk keterlibatan proaktif.

   Jika Anda memberikan lebih dari satu kontak, dalam Catatan, tunjukkan keadaan di mana setiap kontak harus digunakan. Sertakan penunjukan kontak primer dan sekunder, dan berikan jam ketersediaan dan zona waktu untuk setiap kontak.

   Contoh catatan kontak:

   - Ini adalah hotline yang memiliki staf 24x7x365. Silakan bekerja dengan analis yang merespons dan mereka akan mendapatkan orang yang tepat pada panggilan.
   - Silakan hubungi saya jika hotline tidak merespons dalam 5 menit.
2. Pilih Simpan.

   Halaman Ikhtisar mencerminkan informasi kontak yang diperbarui.
3. Pilih Edit fitur keterlibatan proaktif, pilih Aktifkan, lalu pilih Simpan untuk mengaktifkan keterlibatan proaktif.

Menghubungi Tim Respons Shield (SRT)

Anda dapat menghubungi Shield Response Team (SRT) dengan salah satu cara berikut:

Kasus Support

Anda dapat membuka case di bawah AWS Shielddi konsol AWS Support Center.

Untuk panduan cara membuat kasus dukungan, lihat AWS Support Pusat.

Pilih tingkat keparahan yang sesuai dengan situasi Anda dan berikan detail kontak Anda. Dalam deskripsi, berikan sedetail mungkin. Berikan informasi tentang sumber daya yang dilindungi yang menurut Anda mungkin terpengaruh, dan kondisi pengalaman pengguna akhir Anda saat ini. Misalnya, jika pengalaman pengguna Anda terdegradasi atau bagian dari aplikasi Anda saat ini tidak tersedia, berikan informasi tersebut.

- Untuk dugaan serangan DDoS - Jika ketersediaan atau kinerja aplikasi Anda saat ini dipengaruhi oleh kemungkinan serangan DDoS, pilih tingkat keparahan dan opsi kontak berikut:
  - Untuk tingkat keparahan, pilih tingkat keparahan tertinggi yang tersedia untuk paket dukungan Anda:
    - Untuk dukungan Bisnis ini adalah Sistem produksi turun: < 1 jam.
    - Untuk dukungan Enterprise, ini adalah sistem penting Bisnis turun: < 15 menit.
  - Untuk opsi kontak, pilih Telepon atau Obrolan dan berikan detail Anda. Menggunakan metode kontak langsung memberikan respons tercepat.

Keterlibatan proaktif

Dengan keterlibatan AWS Shield Advanced proaktif, SRT menghubungi Anda secara langsung jika pemeriksaan kesehatan Amazon Route 53 yang terkait dengan sumber daya yang dilindungi menjadi tidak sehat selama peristiwa yang terdeteksi. Untuk informasi selengkapnya tentang metrik ini, lihat Mengkonfigurasi keterlibatan proaktif.

Mengkonfigurasi mitigasi kustom dengan Shield Response Team (SRT)

Untuk IP Elastis (EIP) dan akselerator AWS Global Accelerator standar, Anda dapat bekerja dengan Shield Response Team (SRT) untuk mengonfigurasi mitigasi kustom. Ini berguna jika Anda mengetahui logika spesifik yang harus ditegakkan ketika mitigasi ditempatkan. Misalnya, Anda mungkin ingin hanya mengizinkan lalu lintas dari negara tertentu, menerapkan batas tarif tertentu, mengonfigurasi validasi opsional, melarang fragmen, atau hanya mengizinkan lalu lintas yang cocok dengan pola tertentu dalam muatan paket.

Contoh mitigasi kustom umum meliputi:

- Pencocokan pola — Jika Anda mengoperasikan layanan yang berinteraksi dengan aplikasi sisi klien, Anda dapat memilih untuk mencocokkan pola yang diketahui yang unik untuk aplikasi tersebut. Misalnya, Anda dapat mengoperasikan layanan game atau komunikasi yang mengharuskan pengguna akhir untuk menginstal perangkat lunak tertentu yang Anda distribusikan. Anda dapat memasukkan angka ajaib di setiap paket yang dikirim oleh aplikasi ke layanan Anda. Anda dapat mencocokkan hingga 128 byte (terpisah atau bersebelahan) dari muatan dan header paket TCP atau UDP yang tidak terfragmentasi. Pertandingan dapat dinyatakan dalam notasi heksadesimal sebagai offset spesifik dari awal payload paket atau offset dinamis mengikuti nilai yang diketahui. Misalnya, mitigasi dapat mencari byte `0x01` dan kemudian mengharapkan `0x12345678` sebagai empat byte berikutnya.

- Khusus DNS - Jika Anda mengoperasikan layanan DNS otoritatif Anda sendiri menggunakan layanan seperti Global Accelerator atau Amazon Elastic Compute Cloud (Amazon EC2), Anda dapat meminta mitigasi khusus yang memvalidasi paket untuk memastikan bahwa mereka adalah kueri DNS yang valid dan menerapkan penilaian kecurigaan yang mengevaluasi atribut yang spesifik untuk lalu lintas DNS.

Untuk menanyakan tentang bekerja dengan SRT untuk membangun mitigasi khusus, buat kasus dukungan di bawah. AWS Shield Untuk mempelajari lebih lanjut tentang membuat AWS Support kasus, lihat Memulai dengan AWS Support.

Perlindungan sumber daya di AWS Shield Advanced

Anda dapat menambahkan dan mengonfigurasi AWS Shield Advanced perlindungan untuk sumber daya Anda. Anda dapat mengelola perlindungan untuk satu sumber daya dan Anda dapat mengelompokkan sumber daya yang dilindungi ke dalam koleksi logis untuk manajemen acara yang lebih baik. Anda juga dapat melacak perubahan pada perlindungan Shield Advanced Anda menggunakan AWS Config.

Topik

AWS Shield Advanced perlindungan berdasarkan jenis sumber daya

Shield Advanced melindungi AWS sumber daya di jaringan dan lapisan transportasi (lapisan 3 dan 4) dan di lapisan aplikasi (lapisan 7). Anda dapat melindungi beberapa sumber daya secara langsung dan lainnya melalui asosiasi dengan sumber daya yang dilindungi. Shield Advanced mendukung IPv4, dan tidak mendukung IPv6.

Bagian ini memberikan informasi tentang perlindungan Shield Advanced untuk setiap jenis sumber daya.

> **Note**
>
> Shield Advanced hanya melindungi sumber daya yang telah Anda tentukan baik di Shield Advanced atau melalui kebijakan AWS Firewall Manager Shield Advanced. Itu tidak secara otomatis melindungi sumber daya Anda.

Anda dapat menggunakan Shield Advanced untuk pemantauan dan perlindungan lanjutan dengan jenis sumber daya berikut:

- CloudFront Distribusi Amazon. Untuk penerapan CloudFront berkelanjutan, Shield Advanced melindungi distribusi pementasan apa pun yang terkait dengan distribusi primer yang dilindungi.
- Amazon Route 53 zona yang dihosting.
- AWS Global Accelerator akselerator standar.
- Alamat IP Elastis Amazon EC2. Shield Advanced melindungi sumber daya yang terkait dengan alamat IP Elastic yang dilindungi.
- Instans Amazon EC2, melalui asosiasi ke alamat IP Elastis Amazon EC2.
- Berikut ini penyeimbang beban Elastic Load Balancing (ELB):
  - Penyeimbang Beban Aplikasi.
  - Penyeimbang Beban Klasik.
  - Network Load Balancer, melalui asosiasi ke alamat IP Elastis Amazon EC2.

Anda tidak dapat menggunakan Shield Advanced untuk melindungi jenis sumber daya lainnya. Misalnya, Anda tidak dapat melindungi akselerator perutean AWS Global Accelerator khusus atau Gateway Load Balancer.

Anda dapat memantau dan melindungi hingga 1.000 sumber daya untuk setiap jenis sumber daya per Akun AWS. Misalnya, dalam satu akun, Anda dapat melindungi 1.000 alamat IP Elastis Amazon EC2, 1.000 CloudFront distribusi, dan 1.000 Application Load Balancer. Anda dapat meminta peningkatan jumlah sumber daya yang dapat Anda lindungi dengan Shield Advanced melalui konsol Service Quotas di https://console.aws.amazon.com/servicequotas/.

Melindungi instans Amazon EC2 dan Network Load Balancer dengan Shield Advanced

Anda dapat melindungi instans Amazon EC2 dan Network Load Balancer dengan terlebih dahulu melampirkan sumber daya ini ke alamat IP Elastic, lalu melindungi alamat IP Elastis di Shield Advanced.

Saat Anda melindungi alamat IP Elastic, Shield Advanced mengidentifikasi dan melindungi sumber daya yang dilampirkan. Shield Advanced secara otomatis mengidentifikasi jenis sumber daya yang dilampirkan ke alamat IP Elastis dan menerapkan deteksi dan mitigasi yang sesuai untuk sumber daya tersebut. Ini termasuk mengonfigurasi ACL jaringan yang khusus untuk alamat IP Elastis. Untuk informasi selengkapnya tentang penggunaan alamat IP Elastis dengan AWS sumber daya Anda, lihat panduan berikut: Dokumentasi Amazon Elastic Compute Cloud atau dokumentasi Elastic Load Balancing.

Selama serangan, Shield Advanced secara otomatis menyebarkan ACL jaringan Anda ke perbatasan jaringan. AWS Ketika ACL jaringan Anda berada di perbatasan jaringan, Shield Advanced dapat memberikan perlindungan terhadap peristiwa DDoS yang lebih besar. Biasanya, ACL jaringan diterapkan di dekat instans Amazon EC2 Anda dalam VPC Amazon Anda. ACL jaringan dapat mengurangi serangan hanya sebesar yang dapat ditangani oleh VPC dan instans Amazon Anda. Misalnya, jika antarmuka jaringan yang dilampirkan ke instans Amazon EC2 Anda dapat memproses hingga 10 Gbps, maka volume lebih dari 10 Gbps akan melambat dan mungkin memblokir lalu lintas ke instance itu. Selama serangan, Shield Advanced mempromosikan ACL jaringan Anda ke AWS perbatasan, yang dapat memproses beberapa terabyte lalu lintas. ACL jaringan Anda mampu memberikan perlindungan untuk sumber daya Anda jauh di luar kapasitas tipikal jaringan Anda. Untuk informasi selengkapnya tentang ACL jaringan, lihat ACL jaringan.

Beberapa alat penskalaan, seperti AWS Elastic Beanstalk, tidak membiarkan Anda secara otomatis melampirkan alamat IP Elastis ke Network Load Balancer. Untuk kasus-kasus tersebut, Anda perlu melampirkan alamat IP Elastis secara manual.

AWS Shield Advanced perlindungan lapisan aplikasi (lapisan 7)

Untuk melindungi sumber daya lapisan aplikasi Anda dengan Shield Advanced, Anda mulai dengan mengaitkan ACL AWS WAF web dengan sumber daya dan menambahkan satu atau beberapa aturan berbasis kecepatan ke dalamnya. Anda juga dapat mengaktifkan mitigasi DDoS lapisan aplikasi otomatis, yang menyebabkan Shield Advanced secara otomatis membuat dan mengelola aturan ACL web atas nama Anda sebagai respons terhadap serangan DDoS.

Saat Anda melindungi sumber daya lapisan aplikasi dengan Shield Advanced, Shield Advanced menganalisis lalu lintas dari waktu ke waktu untuk menetapkan dan mempertahankan garis dasar. Shield Advanced menggunakan baseline ini untuk mendeteksi anomali dalam pola lalu lintas yang

mungkin mengindikasikan serangan DDoS. Titik di mana Shield Advanced mendeteksi serangan tergantung pada lalu lintas yang dapat diamati oleh Shield Advanced sebelum serangan dan pada arsitektur yang Anda gunakan untuk aplikasi web Anda. Variasi arsitektur yang dapat memengaruhi perilaku Shield Advanced mencakup jenis instance yang Anda gunakan, ukuran instans, dan apakah tipe instans mendukung jaringan yang disempurnakan. Anda juga dapat mengonfigurasi Shield Advanced untuk secara otomatis menempatkan mitigasi untuk serangan lapisan aplikasi.

Langganan dan biaya Shield Advanced AWS WAF

Langganan Shield Advanced Anda menanggung biaya penggunaan AWS WAF kemampuan standar untuk sumber daya yang Anda lindungi dengan Shield Advanced. AWS WAF Biaya standar yang ditanggung oleh perlindungan Shield Advanced Anda adalah biaya per ACL web, biaya per aturan, dan harga dasar per juta permintaan untuk pemeriksaan permintaan web, hingga 1.500 WCU, dan hingga ukuran badan default.

Mengaktifkan mitigasi DDoS lapisan aplikasi otomatis Shield Advanced menambahkan grup aturan ke ACL web Anda yang menggunakan 150 unit kapasitas ACL web (WCU). WCU ini dihitung terhadap penggunaan WCU di ACL web Anda. Lihat informasi selengkapnya di Mitigasi DDoS lapisan aplikasi otomatis Shield Advanced, Grup aturan Shield Advanced, dan AWS WAF unit kapasitas ACL web (WCU).

Langganan Anda ke Shield Advanced tidak mencakup AWS WAF penggunaan sumber daya yang tidak Anda lindungi menggunakan Shield Advanced. Ini juga tidak mencakup AWS WAF biaya non-standar tambahan untuk sumber daya yang dilindungi. Contoh biaya non-standar adalah AWS WAF biaya untuk Kontrol Bot, untuk tindakan CAPTCHA aturan, untuk ACL web yang menggunakan lebih dari 1.500 WCU, dan untuk memeriksa badan permintaan di luar ukuran tubuh default. Daftar lengkap disediakan di halaman AWS WAF harga.

Untuk informasi selengkapnya dan contoh harga, lihat Harga dan AWS WAF Harga Shield.

Topik

- Deteksi dan mitigasi
- Shield Advanced Application Layer AWS WAF Web ACL dan aturan berbasis tarif
- Mitigasi DDoS lapisan aplikasi otomatis Shield Advanced

Deteksi dan mitigasi

Bagian ini menjelaskan faktor-faktor yang mempengaruhi deteksi dan mitigasi peristiwa lapisan aplikasi oleh Shield Advanced.

Pemeriksaan kondisi

Pemeriksaan kesehatan yang secara akurat melaporkan kesehatan keseluruhan aplikasi Anda memberi Shield Advanced informasi tentang kondisi lalu lintas yang dialami aplikasi Anda. Shield Advanced membutuhkan lebih sedikit informasi yang menunjuk ke potensi serangan ketika aplikasi Anda melaporkan tidak sehat dan memerlukan lebih banyak bukti serangan jika aplikasi Anda melaporkan sehat.

Sangat penting untuk mengkonfigurasi pemeriksaan kesehatan Anda sehingga mereka secara akurat melaporkan kesehatan aplikasi. Untuk informasi dan panduan lebih lanjut, lihatDeteksi berbasis kesehatan menggunakan pemeriksaan kesehatan.

Garis dasar lalu lintas

Garis dasar lalu lintas memberikan informasi Shield Advanced tentang karakteristik lalu lintas normal untuk aplikasi Anda. Shield Advanced menggunakan garis dasar ini untuk mengenali kapan aplikasi Anda tidak menerima lalu lintas normal., sehingga dapat memberi tahu Anda dan, seperti yang dikonfigurasi, mulai merancang dan menguji opsi mitigasi untuk melawan potensi serangan. Untuk informasi tambahan tentang cara Shield Advanced menggunakan garis dasar lalu lintas untuk mendeteksi potensi peristiwa, lihat bagian ikhtisar. Logika deteksi untuk ancaman lapisan aplikasi

Shield Advanced membuat garis dasarnya dari informasi yang disediakan oleh ACL web yang terkait dengan sumber daya yang dilindungi. ACL web harus dikaitkan dengan sumber daya setidaknya selama 24 jam dan hingga 30 hari sebelum Shield Advanced dapat menentukan baseline aplikasi dengan andal. Waktu yang diperlukan dimulai saat Anda mengaitkan ACL web, baik melalui Shield Advanced atau melalui AWS WAF.

Untuk informasi selengkapnya tentang menggunakan ACL web dengan perlindungan lapisan aplikasi Shield Advanced, lihat. Shield Advanced Application Layer AWS WAF Web ACL dan aturan berbasis tarif

Aturan berbasis tarif

Aturan berbasis tarif dapat membantu mengurangi serangan. Mereka juga dapat mengaburkan serangan, dengan menguranginya sebelum menjadi masalah yang cukup besar untuk muncul melawan garis dasar lalu lintas normal atau dalam pelaporan status pemeriksaan kesehatan.

Sebaiknya gunakan aturan berbasis tarif di ACL web Anda saat Anda melindungi sumber daya aplikasi dengan Shield Advanced. Meskipun mitigasi mereka dapat mengaburkan serangan potensial, mereka adalah garis pertahanan pertama yang berharga, membantu memastikan bahwa

aplikasi Anda tetap tersedia untuk pelanggan sah Anda. Lalu lintas yang dideteksi oleh aturan berbasis tarif dan batas tarif terlihat dalam metrik Anda AWS WAF .

Selain aturan berbasis tarif Anda sendiri, jika Anda mengaktifkan mitigasi DDoS lapisan aplikasi otomatis, Shield Advanced menambahkan grup aturan ke ACL web Anda yang digunakan untuk mengurangi serangan. Dalam grup aturan ini, Shield Advanced selalu memiliki aturan berbasis kecepatan yang membatasi volume permintaan dari alamat IP yang dikenal sebagai sumber serangan DDoS. Metrik untuk lalu lintas yang dikurangi aturan Shield Advanced tidak tersedia untuk Anda lihat.

Untuk informasi selengkapnya tentang aturan berbasis tarif, lihat. Pernyataan aturan berbasis tarif Untuk informasi tentang aturan berbasis tarif yang digunakan Shield Advanced untuk mitigasi DDoS lapisan aplikasi otomatis, lihat. Grup aturan Shield Advanced

Untuk informasi selengkapnya tentang Shield Advanced dan AWS WAF metrik, lihatPemantauan CloudWatch dengan Amazon.

Shield Advanced Application Layer AWS WAF Web ACL dan aturan berbasis tarif

Untuk melindungi sumber daya lapisan aplikasi dengan Shield Advanced, Anda mulai dengan mengaitkan ACL AWS WAF web dengan sumber daya. AWS WAF adalah firewall aplikasi web yang memungkinkan Anda memantau permintaan HTTP dan HTTPS yang diteruskan ke sumber daya lapisan aplikasi Anda, dan memungkinkan Anda mengontrol akses ke konten Anda berdasarkan karakteristik permintaan. Anda dapat mengonfigurasi ACL web untuk memantau dan mengelola permintaan berdasarkan faktor-faktor seperti di mana permintaan berasal, isi string kueri dan cookie, dan tingkat permintaan yang berasal dari satu alamat IP. Minimal, perlindungan Shield Advanced Anda mengharuskan Anda untuk mengaitkan ACL web dengan aturan berbasis tarif, yang membatasi tingkat permintaan untuk setiap alamat IP.

Jika ACL web terkait tidak memiliki aturan berbasis kecepatan yang ditentukan, Shield Advanced meminta Anda untuk menentukan setidaknya satu. Aturan berbasis tarif secara otomatis memblokir lalu lintas dari IP sumber ketika melebihi ambang batas yang Anda tentukan. Mereka membantu melindungi aplikasi Anda dari banjir permintaan web dan dapat memberikan peringatan tentang lonjakan lalu lintas yang tiba-tiba yang mungkin mengindikasikan potensi serangan DDoS.

> **Note**
>
> Aturan berbasis tarif merespons dengan sangat cepat lonjakan lalu lintas yang dipantau oleh aturan tersebut. Karena itu, aturan berbasis kecepatan dapat mencegah tidak hanya serangan, tetapi juga deteksi serangan potensial oleh deteksi Shield Advanced. Perdagangan

ini mendukung pencegahan daripada visibilitas lengkap ke pattenr serangan. Sebaiknya gunakan aturan berbasis kecepatan sebagai garis pertahanan pertama Anda terhadap serangan.

Dengan ACL web Anda di tempat, jika serangan DDoS terjadi, Anda menerapkan mitigasi dengan menambahkan dan mengelola aturan di ACL web. Anda dapat melakukan ini secara langsung, dengan bantuan dari Shield Response Team (SRT), atau secara otomatis melalui mitigasi DDoS lapisan aplikasi otomatis.

Important

Jika Anda juga menggunakan mitigasi DDoS lapisan aplikasi otomatis, lihat praktik terbaik untuk mengelola ACL web Anda di. Praktik terbaik untuk menggunakan mitigasi otomatis

Perilaku aturan berbasis tarif default

Saat Anda menggunakan aturan berbasis tarif dengan konfigurasi defaultnya, evaluasi lalu lintas AWS WAF secara berkala untuk jendela waktu 5 menit sebelumnya. AWS WAF memblokir permintaan dari alamat IP apa pun yang melebihi ambang batas aturan hingga tingkat permintaan turun ke tingkat yang dapat diterima. Saat Anda mengonfigurasi aturan berbasis tarif melalui Shield Advanced, konfigurasikan ambang batas tarifnya ke nilai yang lebih besar dari tingkat lalu lintas normal yang Anda harapkan dari satu IP sumber dalam jangka waktu lima menit.

Anda mungkin ingin menggunakan lebih dari satu aturan berbasis tarif di ACL web. Misalnya, Anda dapat memiliki satu aturan berbasis tarif untuk semua lalu lintas yang memiliki ambang batas tinggi ditambah satu atau lebih aturan tambahan yang dikonfigurasi agar sesuai dengan bagian tertentu dari aplikasi web Anda dan yang memiliki ambang batas yang lebih rendah. Misalnya, Anda mungkin mencocokkan URI `/login.html` dengan ambang batas yang lebih rendah, untuk mengurangi penyalahgunaan terhadap halaman login.

Anda dapat mengonfigurasi aturan berbasis laju untuk menggunakan jendela waktu evaluasi yang berbeda dan untuk menggabungkan permintaan dengan sejumlah komponen permintaan, seperti nilai header, label, dan argumen kueri. Untuk informasi selengkapnya, lihat Pernyataan aturan berbasis tarif.

Untuk informasi dan panduan tambahan, lihat posting blog keamanan Tiga aturan AWS WAF berbasis tarif yang paling penting.

Opsi konfigurasi yang diperluas melalui AWS WAF

Konsol Shield Advanced memungkinkan Anda menambahkan aturan berbasis tarif dan mengonfigurasinya dengan pengaturan dasar dan default. Anda dapat menentukan opsi konfigurasi tambahan dengan mengelola aturan berbasis tarif. AWS WAF Misalnya, Anda dapat mengonfigurasi aturan untuk mengumpulkan permintaan berdasarkan kunci seperti alamat IP yang diteruskan, string kueri, dan label. Anda juga dapat menambahkan pernyataan cakupan ke bawah aturan untuk menyaring beberapa permintaan dari evaluasi dan pembatasan tarif. Untuk informasi selengkapnya, lihat Pernyataan aturan berbasis tarif. Untuk informasi tentang penggunaan AWS WAF untuk mengelola pemantauan permintaan web dan aturan manajemen, lihatMembuat web ACL.

Mitigasi DDoS lapisan aplikasi otomatis Shield Advanced

Anda dapat mengonfigurasi Shield Advanced untuk merespons secara otomatis untuk mengurangi serangan lapisan aplikasi (lapisan 7) terhadap sumber daya lapisan aplikasi Anda yang dilindungi, dengan menghitung atau memblokir permintaan web yang merupakan bagian dari serangan. Opsi ini merupakan tambahan untuk perlindungan lapisan aplikasi yang Anda tambahkan melalui Shield Advanced dengan ACL AWS WAF web dan aturan berbasis tarif Anda sendiri.

Saat mitigasi otomatis diaktifkan untuk sumber daya, Shield Advanced mempertahankan grup aturan di ACL web terkait sumber daya tempat ia mengelola aturan mitigasi atas nama sumber daya. Grup aturan berisi aturan berbasis kecepatan yang melacak volume permintaan dari alamat IP yang dikenal sebagai sumber serangan DDoS.

Selain itu, Shield Advanced membandingkan pola lalu lintas saat ini dengan garis dasar lalu lintas bersejarah untuk mendeteksi penyimpangan yang mungkin mengindikasikan serangan DDoS. Shield Advanced merespons serangan DDoS yang terdeteksi dengan membuat, mengevaluasi, dan menerapkan AWS WAF aturan kustom tambahan dalam grup aturan.

Daftar Isi

  - Bagaimana Shield Advanced mengelola mitigasi saat serangan mereda
  - Apa yang terjadi ketika Anda menonaktifkan mitigasi otomatis
- Grup aturan Shield Advanced
- Mengelola mitigasi lapisan aplikasi DDoS otomatis
  - Melihat konfigurasi mitigasi DDoS lapisan aplikasi otomatis untuk sumber daya
  - Mengaktifkan dan menonaktifkan mitigasi DDoS lapisan aplikasi otomatis
  - Mengubah tindakan yang digunakan untuk mitigasi DDoS lapisan aplikasi otomatis
  - Menggunakan AWS CloudFormation dengan mitigasi DDoS lapisan aplikasi otomatis

Peringatan untuk menggunakan mitigasi otomatis

Daftar berikut menjelaskan peringatan mitigasi DDoS lapisan aplikasi otomatis Shield Advanced, dan menjelaskan langkah-langkah yang mungkin ingin Anda ambil sebagai tanggapan.

- Mitigasi DDoS lapisan aplikasi otomatis hanya berfungsi dengan ACL web yang dibuat menggunakan versi terbaru (v2). AWS WAF
- Shield Advanced membutuhkan waktu untuk menetapkan garis dasar lalu lintas normal dan historis aplikasi Anda, yang dimanfaatkannya untuk mendeteksi dan mengisolasi lalu lintas serangan dari lalu lintas normal, untuk mengurangi lalu lintas serangan. Waktu untuk menetapkan baseline adalah antara 24 jam dan 30 hari sejak Anda mengaitkan ACL web dengan sumber daya aplikasi yang dilindungi. Untuk informasi tambahan tentang garis dasar lalu lintas, lihat. Deteksi dan mitigasi
- Mengaktifkan mitigasi DDoS lapisan aplikasi otomatis menambahkan grup aturan ke ACL web Anda yang menggunakan 150 unit kapasitas ACL web (WCU). WCU ini dihitung terhadap penggunaan WCU di ACL web Anda. Untuk informasi selengkapnya, lihat Grup aturan Shield Advanced, dan AWS WAF unit kapasitas ACL web (WCU).
- Grup aturan Shield Advanced menghasilkan AWS WAF metrik, tetapi tidak tersedia untuk dilihat. Ini sama dengan grup aturan lain yang Anda gunakan di ACL web tetapi tidak dimiliki, seperti grup aturan Aturan AWS Terkelola. Untuk informasi selengkapnya tentang AWS WAF metrik, lihatAWS WAF metrik dan dimensi. Untuk informasi tentang opsi perlindungan Shield Advanced ini, lihatMitigasi DDoS lapisan aplikasi otomatis Shield Advanced.
- Untuk ACL web yang melindungi beberapa sumber daya, mitigasi otomatis hanya menerapkan mitigasi khusus yang tidak berdampak negatif terhadap sumber daya yang dilindungi.

- Waktu antara dimulainya serangan DDoS dan ketika Shield Advanced menempatkan aturan mitigasi otomatis kustom bervariasi dengan setiap peristiwa. Beberapa serangan DDoS mungkin berakhir sebelum aturan kustom diterapkan. Serangan lain mungkin terjadi ketika mitigasi sudah ada, dan mungkin dikurangi dengan aturan tersebut sejak awal acara. Selain itu, aturan berbasis tarif di grup aturan ACL dan Shield Advanced web dapat mengurangi lalu lintas serangan sebelum terdeteksi sebagai peristiwa yang mungkin terjadi.
- Untuk Application Load Balancer yang menerima lalu lintas apa pun melalui jaringan pengiriman konten (CDN), seperti Amazon CloudFront, kemampuan mitigasi otomatis lapisan aplikasi dari Shield Advanced untuk sumber daya Application Load Balancer tersebut akan berkurang. Shield Advanced menggunakan atribut lalu lintas klien untuk mengidentifikasi dan mengisolasi lalu lintas serangan dari lalu lintas normal ke aplikasi Anda, dan CDN mungkin tidak mempertahankan atau meneruskan atribut lalu lintas klien asli. Jika Anda menggunakan CloudFront, kami sarankan untuk mengaktifkan mitigasi otomatis pada distribusi. CloudFront
- Mitigasi DDoS lapisan aplikasi otomatis tidak berinteraksi dengan kelompok perlindungan. Anda dapat mengaktifkan mitigasi otomatis untuk sumber daya yang ada di grup perlindungan, tetapi Shield Advanced tidak secara otomatis menerapkan mitigasi serangan berdasarkan temuan kelompok perlindungan. Shield Advanced menerapkan mitigasi serangan otomatis untuk sumber daya individu.

Praktik terbaik untuk menggunakan mitigasi otomatis

Patuhi panduan yang disediakan di bagian ini saat Anda menggunakan mitigasi otomatis.

Manajemen perlindungan umum

Ikuti panduan ini untuk merencanakan dan menerapkan perlindungan mitigasi otomatis Anda.

- Kelola semua perlindungan mitigasi otomatis Anda baik melalui Shield Advanced atau, jika Anda menggunakannya AWS Firewall Manager untuk mengelola pengaturan mitigasi otomatis Shield Advanced, melalui Firewall Manager. Jangan mencampur penggunaan Shield Advanced dan Firewall Manager untuk mengelola perlindungan ini.
- Kelola sumber daya serupa menggunakan ACL web dan pengaturan perlindungan yang sama, dan kelola sumber daya yang berbeda menggunakan ACL web yang berbeda. Ketika Shield Advanced mengurangi serangan DDoS pada sumber daya yang dilindungi, ia mendefinisikan aturan untuk ACL web yang terkait dengan sumber daya dan kemudian menguji aturan terhadap lalu lintas semua sumber daya yang terkait dengan ACL web. Shield Advanced hanya akan menerapkan

aturan jika aturan tersebut tidak berdampak negatif terhadap sumber daya terkait. Untuk informasi selengkapnya, lihat Bagaimana Shield Advanced mengelola mitigasi otomatis.

- Untuk Application Load Balancer yang memiliki semua lalu lintas internet mereka diproksi melalui CloudFront distribusi Amazon, hanya aktifkan mitigasi otomatis pada distribusi. CloudFront CloudFront Distribusi akan selalu memiliki jumlah atribut lalu lintas asli terbesar, yang dimanfaatkan Shield Advanced untuk mengurangi serangan.

Pengoptimalan deteksi dan mitigasi

Ikuti panduan ini untuk mengoptimalkan perlindungan yang diberikan mitigasi otomatis terhadap sumber daya yang dilindungi. Untuk ikhtisar deteksi dan mitigasi lapisan aplikasi, lihat. Deteksi dan mitigasi

- Konfigurasikan pemeriksaan kesehatan untuk sumber daya yang dilindungi dan gunakan untuk mengaktifkan deteksi berbasis kesehatan di perlindungan Shield Advanced Anda. Untuk panduan, lihat Deteksi berbasis kesehatan menggunakan pemeriksaan kesehatan.
- Aktifkan mitigasi otomatis dalam Count mode hingga Shield Advanced menetapkan garis dasar untuk lalu lintas normal dan bersejarah. Shield Advanced membutuhkan dari 24 jam hingga 30 hari untuk menetapkan baseline.

  Menetapkan dasar pola lalu lintas normal membutuhkan hal-hal berikut:

  - Asosiasi ACL web dengan sumber daya yang dilindungi. Anda dapat menggunakan AWS WAF langsung untuk mengaitkan ACL web Anda atau Anda dapat meminta Shield Advanced mengaitkannya saat Anda mengaktifkan perlindungan lapisan aplikasi Shield Advanced dan menentukan ACL web yang akan digunakan.
  - Arus lalu lintas normal ke aplikasi Anda yang dilindungi. Jika aplikasi Anda tidak mengalami lalu lintas normal, seperti sebelum aplikasi diluncurkan atau jika tidak memiliki lalu lintas produksi untuk jangka waktu yang lama, data historis tidak dapat dikumpulkan.

Manajemen ACL web

Ikuti panduan ini untuk mengelola ACL web yang Anda gunakan dengan mitigasi otomatis.

- Jika Anda perlu mengganti ACL web yang terkait dengan sumber daya yang dilindungi, buat perubahan berikut secara berurutan:
  1. Di Shield Advanced, nonaktifkan mitigasi otomatis.
  2. Di AWS WAF, pisahkan ACL web lama dan kaitkan ACL web baru.

3. Di Shield Advanced, aktifkan mitigasi otomatis.

   Shield Advanced tidak secara otomatis mentransfer mitigasi otomatis dari ACL web lama ke yang baru.

- Jangan hapus aturan grup aturan apa pun dari ACL web Anda yang namanya dimulai dengan`ShieldMitigationRuleGroup`. Jika Anda menghapus grup aturan ini, Anda menonaktifkan perlindungan yang disediakan oleh mitigasi otomatis Shield Advanced untuk setiap sumber daya yang terkait dengan ACL web. Selain itu, diperlukan Shield Advanced beberapa waktu untuk menerima pemberitahuan perubahan dan memperbarui pengaturannya. Selama waktu ini, halaman konsol Shield Advanced akan memberikan informasi yang salah.

  Untuk informasi selengkapnya tentang grup aturan, lihatGrup aturan Shield Advanced.
- Jangan mengubah nama aturan grup aturan yang namanya dimulai dengan`ShieldMitigationRuleGroup`. Melakukannya dapat mengganggu perlindungan yang diberikan oleh mitigasi otomatis Shield Advanced melalui ACL web.
- Saat Anda membuat aturan dan grup aturan, jangan gunakan nama yang dimulai dengan`ShieldMitigationRuleGroup`. String ini digunakan oleh Shield Advanced untuk mengelola mitigasi otomatis Anda.
- Dalam pengelolaan aturan ACL web Anda, jangan tetapkan pengaturan prioritas 10.000.000. Shield Advanced menetapkan pengaturan prioritas ini ke aturan grup aturan mitigasi otomatis saat menambahkannya.
- Pertahankan `ShieldMitigationRuleGroup` aturan yang diprioritaskan sehingga berjalan ketika Anda menginginkannya sehubungan dengan aturan lain di ACL web Anda. Shield Advanced menambahkan aturan grup aturan ke ACL web dengan prioritas 10.000.000, untuk menjalankan aturan Anda yang lain. Jika Anda menggunakan wizard AWS WAF konsol untuk mengelola ACL web Anda, sesuaikan pengaturan prioritas sesuai kebutuhan setelah Anda menambahkan aturan ke ACL web.
- Jika Anda menggunakan AWS CloudFormation untuk mengelola ACL web Anda, Anda tidak perlu mengelola `ShieldMitigationRuleGroup` aturan grup aturan. Ikuti bimbingan diMenggunakan AWS CloudFormation dengan mitigasi DDoS lapisan aplikasi otomatis.

Konfigurasi diperlukan untuk mengaktifkan mitigasi otomatis

Anda mengaktifkan mitigasi otomatis Shield Advanced sebagai bagian dari perlindungan DDoS lapisan aplikasi untuk sumber daya Anda. Untuk informasi tentang melakukan ini melalui konsol, lihatKonfigurasikan perlindungan DDoS lapisan aplikasi.

Fungsionalitas mitigasi otomatis mengharuskan Anda melakukan hal berikut:

- Kaitkan ACL web dengan sumber daya — Ini diperlukan untuk perlindungan lapisan aplikasi Shield Advanced. Anda dapat menggunakan ACL web yang sama untuk beberapa sumber daya. Kami merekomendasikan melakukan ini hanya untuk sumber daya yang memiliki lalu lintas serupa. Untuk informasi tentang ACL web, termasuk persyaratan untuk menggunakannya dengan beberapa sumber daya, lihatBagaimana cara AWS WAF kerja.
- Aktifkan dan konfigurasikan mitigasi DDoS lapisan aplikasi otomatis Shield Advanced — Saat Anda mengaktifkan ini, Anda menentukan apakah Anda ingin Shield Advanced memblokir atau menghitung permintaan web secara otomatis yang ditentukan sebagai bagian dari serangan DDoS. Shield Advanced menambahkan grup aturan ke ACL web terkait dan menggunakannya untuk mengelola responsnya secara dinamis terhadap serangan DDoS pada sumber daya. Untuk informasi tentang opsi tindakan aturan, lihatTindakan aturan.
- (Opsional, tetapi disarankan) Tambahkan aturan berbasis tarif ke ACL web — Secara default, aturan berbasis tarif menyediakan sumber daya Anda dengan perlindungan dasar terhadap serangan DDoS dengan mencegah alamat IP individual mengirim terlalu banyak permintaan dalam waktu singkat. Untuk informasi tentang aturan berbasis tarif, termasuk opsi dan contoh agregasi permintaan kustom, lihat. Pernyataan aturan berbasis tarif

Bagaimana Shield Advanced mengelola mitigasi otomatis

Topik di bagian menjelaskan bagaimana Shield Advanced menangani perubahan konfigurasi Anda untuk mitigasi DDoS lapisan aplikasi otomatis dan cara menangani serangan DDoS saat mitigasi otomatis diaktifkan.

Topik

- Apa yang terjadi ketika Anda mengaktifkan mitigasi otomatis
- Bagaimana Shield Advanced merespons serangan DDoS dengan mitigasi otomatis
- Bagaimana Shield Advanced mengelola pengaturan tindakan aturan
- Bagaimana Shield Advanced mengelola mitigasi saat serangan mereda
- Apa yang terjadi ketika Anda menonaktifkan mitigasi otomatis

Apa yang terjadi ketika Anda mengaktifkan mitigasi otomatis

Shield Advanced melakukan hal berikut ketika Anda mengaktifkan mitigasi otomatis:

- Jika diperlukan, tambahkan grup aturan untuk penggunaan Shield Advanced — Jika ACL AWS WAF web yang Anda kaitkan dengan sumber daya belum memiliki AWS WAF aturan grup aturan yang didedikasikan untuk mitigasi DDoS lapisan aplikasi otomatis, Shield Advanced menambahkannya.

  Nama aturan grup aturan dimulai dengan`ShieldMitigationRuleGroup`. Grup aturan selalu berisi aturan berbasis tingkat bernama`ShieldKnownOffenderIPRateBasedRule`, yang membatasi volume permintaan dari alamat IP yang dikenal sebagai sumber serangan DDoS. Untuk detail tambahan tentang grup aturan Shield Advanced dan aturan ACL web yang mereferensikannya, lihatGrup aturan Shield Advanced.
- Mulai merespons serangan DDoS terhadap sumber daya — Shield Advanced secara otomatis merespons serangan DDoS untuk sumber daya yang dilindungi. Selain aturan berbasis tarif, yang selalu ada, Shield Advanced menggunakan grup aturannya untuk menerapkan AWS WAF aturan khusus untuk mitigasi serangan DDoS. Shield Advanced menyesuaikan aturan ini dengan aplikasi Anda dan serangan yang dialami aplikasi Anda, dan mengujinya terhadap lalu lintas historis sumber daya sebelum menerapkannya.

Shield Advanced menggunakan aturan grup aturan tunggal di ACL web apa pun yang Anda gunakan untuk mitigasi otomatis. Jika Shield Advanced telah menambahkan grup aturan untuk sumber daya lain yang dilindungi, itu tidak menambahkan grup aturan lain ke ACL web.

Mitigasi DDoS lapisan aplikasi otomatis tergantung pada keberadaan kelompok aturan untuk mengurangi serangan. Jika grup aturan dihapus dari ACL AWS WAF web karena alasan apa pun, penghapusan menonaktifkan mitigasi otomatis untuk semua sumber daya yang terkait dengan ACL web.

Bagaimana Shield Advanced merespons serangan DDoS dengan mitigasi otomatis

Bila Anda mengaktifkan mitigasi otomatis pada sumber daya yang dilindungi, aturan berbasis laju di `ShieldKnownOffenderIPRateBasedRule` grup aturan Shield Advanced merespons secara otomatis volume lalu lintas yang meningkat dari sumber DDoS yang diketahui. Pembatasan kecepatan ini diterapkan dengan cepat dan bertindak sebagai pertahanan garis depan terhadap serangan.

Ketika Shield Advanced mendeteksi serangan, ia melakukan hal berikut:

1. Mencoba mengidentifikasi tanda tangan serangan yang mengisolasi lalu lintas serangan dari lalu lintas normal ke aplikasi Anda. Tujuannya adalah untuk menghasilkan aturan mitigasi DDoS

berkualitas tinggi yang, ketika ditempatkan, hanya memengaruhi lalu lintas serangan dan tidak memengaruhi lalu lintas normal ke aplikasi Anda.

2. Mengevaluasi tanda tangan serangan yang diidentifikasi terhadap pola lalu lintas historis untuk sumber daya yang diserang serta untuk sumber daya lain yang terkait dengan ACL web yang sama. Shield Advanced melakukan ini sebelum menerapkan aturan apa pun sebagai respons terhadap acara tersebut.

   Bergantung pada hasil evaluasi, Shield Advanced melakukan salah satu hal berikut:

   - Jika Shield Advanced menentukan bahwa tanda tangan serangan hanya mengisolasi lalu lintas yang terlibat dalam serangan DDoS, itu mengimplementasikan tanda tangan dalam AWS WAF aturan dalam grup aturan mitigasi Shield Advanced di ACL web. Shield Advanced memberikan aturan ini setelan tindakan yang telah Anda konfigurasikan untuk mitigasi otomatis sumber daya - salah satu atauCount. Block
   - Jika tidak, Shield Advanced tidak menempatkan mitigasi.

Selama serangan, Shield Advanced mengirimkan notifikasi yang sama dan memberikan informasi acara yang sama seperti untuk perlindungan lapisan aplikasi Shield Advanced dasar. Anda dapat melihat informasi tentang peristiwa dan serangan DDoS, dan tentang mitigasi Shield Advanced untuk serangan, di konsol acara Shield Advanced. Untuk informasi, lihat Visibilitas ke acara DDoS.

Jika Anda telah mengonfigurasi mitigasi otomatis untuk menggunakan tindakan Block aturan dan Anda mengalami kesalahan positif dari aturan mitigasi yang telah diterapkan Shield Advanced, Anda dapat mengubah tindakan aturan menjadi. Count Untuk informasi tentang cara ini, lihatMengubah tindakan yang digunakan untuk mitigasi DDoS lapisan aplikasi otomatis.

Bagaimana Shield Advanced mengelola pengaturan tindakan aturan

Anda dapat mengatur tindakan aturan untuk mitigasi otomatis Anda ke atau. Block Count

Saat Anda mengubah setelan tindakan aturan mitigasi otomatis untuk sumber daya yang dilindungi, Shield Advanced memperbarui semua setelan aturan untuk sumber daya. Ini memperbarui aturan apa pun yang saat ini ada untuk sumber daya di grup aturan Shield Advanced dan menggunakan setelan tindakan baru saat membuat aturan baru.

Untuk sumber daya yang menggunakan ACL web yang sama, jika Anda menentukan tindakan yang berbeda, Shield Advanced menggunakan setelan Block tindakan untuk aturan berbasis laju grup aturan. `ShieldKnownOffenderIPRateBasedRule` Shield Advanced membuat dan mengelola aturan lain dalam grup aturan atas nama sumber daya tertentu yang dilindungi, dan menggunakan

setelan tindakan yang telah Anda tentukan untuk sumber daya tersebut. Semua aturan dalam grup aturan Shield Advanced di ACL web diterapkan pada lalu lintas web dari semua sumber daya terkait.

Mengubah pengaturan tindakan dapat memakan waktu beberapa detik untuk menyebar. Selama waktu ini, Anda mungkin melihat pengaturan lama di beberapa tempat di mana grup aturan sedang digunakan, dan pengaturan baru di tempat lain.

Anda dapat mengubah pengaturan tindakan aturan untuk konfigurasi mitigasi otomatis di halaman peristiwa konsol, dan melalui halaman konfigurasi lapisan aplikasi. Untuk informasi tentang halaman acara, lihatMenanggapi peristiwa DDoS. Untuk informasi tentang halaman konfigurasi, lihatKonfigurasikan perlindungan DDoS lapisan aplikasi.

Bagaimana Shield Advanced mengelola mitigasi saat serangan mereda

Ketika Shield Advanced menentukan bahwa aturan mitigasi yang digunakan untuk serangan tertentu tidak lagi diperlukan, itu akan menghapusnya dari grup aturan mitigasi Shield Advanced.

Penghapusan aturan mitigasi tidak selalu bertepatan dengan akhir serangan. Shield Advanced memantau pola serangan yang dideteksi pada sumber daya Anda yang dilindungi. Ini mungkin secara proaktif bertahan terhadap terulangnya serangan dengan tanda tangan tertentu dengan menjaga aturan yang telah dikerahkan terhadap kejadian awal serangan itu di tempat. Sesuai kebutuhan, Shield Advanced meningkatkan jendela waktu agar aturan tetap berlaku. Dengan cara ini, Shield Advanced dapat mengurangi serangan berulang dengan tanda tangan tertentu sebelum memengaruhi sumber daya Anda yang dilindungi.

Shield Advanced tidak pernah menghapus aturan berbasis kecepatan`ShieldKnownOffenderIPRateBasedRule`, yang membatasi volume permintaan dari alamat IP yang dikenal sebagai sumber serangan DDoS.

Apa yang terjadi ketika Anda menonaktifkan mitigasi otomatis

Shield Advanced melakukan hal berikut saat Anda menonaktifkan mitigasi otomatis untuk sumber daya:

- Berhenti merespons serangan DDoS secara otomatis — Shield Advanced menghentikan aktivitas respons otomatisnya untuk sumber daya.
- Menghapus aturan yang tidak diperlukan dari grup aturan Shield Advanced — Jika Shield Advanced mempertahankan aturan apa pun dalam grup aturan terkelolanya atas nama sumber daya yang dilindungi, aturan tersebut akan menghapusnya.

- Menghapus grup aturan Shield Advanced, jika tidak lagi digunakan — Jika ACL web yang Anda kaitkan dengan sumber daya tidak terkait dengan sumber daya lain yang mengaktifkan mitigasi otomatis, Shield Advanced menghapus aturan grup aturannya dari ACL web.

Grup aturan Shield Advanced

Shield Advanced mengelola aktivitas mitigasi otomatis menggunakan aturan dalam grup aturan yang dimiliki dan dikelola untuk Anda. Shield Advanced mereferensikan grup aturan dengan aturan di ACL web yang telah Anda kaitkan dengan sumber daya yang dilindungi.

Aturan grup aturan di ACL web Anda

Aturan grup aturan Shield Advanced di ACL web Anda memiliki properti berikut:

- Nama – `ShieldMitigationRuleGroup_`*`account-id`*`_`*`web-acl-id`*`_`*`unique-identifier`*
- Unit kapasitas ACL Web (WCU) - 150. WCU ini dihitung terhadap penggunaan WCU di ACL web Anda.

Shield Advanced membuat aturan ini di ACL web Anda dengan pengaturan prioritas 10.000.000, sehingga berjalan setelah aturan dan grup aturan Anda yang lain di ACL web. AWS WAF menjalankan aturan di ACL web dari pengaturan prioritas numerik terendah di atas. Selama pengelolaan ACL web Anda, pengaturan prioritas ini mungkin berubah.

Fungsionalitas mitigasi otomatis tidak menggunakan AWS WAF sumber daya tambahan apa pun di akun Anda, selain WCU yang digunakan oleh grup aturan di ACL web Anda. Misalnya, grup aturan Shield Advanced tidak dihitung sebagai salah satu grup aturan akun Anda. Untuk informasi tentang batas akun di AWS WAF, lihatAWS WAF kuota.

Aturan dalam kelompok aturan

Dalam grup aturan Shield Advanced yang direferensikan, Shield Advanced mempertahankan aturan berbasis kecepatan`ShieldKnownOffenderIPRateBasedRule`, yang membatasi volume permintaan dari alamat IP yang dikenal sebagai sumber serangan DDoS. Aturan ini berfungsi sebagai garis pertahanan pertama terhadap serangan apa pun, karena selalu ada dalam kelompok aturan dan tidak bergantung pada analisis pola lalu lintas untuk menahan serangan. Tindakan aturan ini diatur ke tindakan yang Anda pilih untuk mitigasi otomatis, seperti aturan lain dalam grup aturan. Untuk informasi tentang aturan berbasis tarif, lihat. Pernyataan aturan berbasis tarif

> **Note**
>
> Aturan berbasis tarif `ShieldKnownOffenderIPRateBasedRule` beroperasi secara independen dari deteksi peristiwa Shield Advanced. Sementara mitigasi otomatis diaktifkan, tingkat aturan ini membatasi alamat IP yang dikenal sebagai sumber serangan DDoS. Untuk alamat IP ini, pembatasan laju aturan dapat mencegah serangan dan juga mencegah serangan muncul di informasi deteksi Shield Advanced. Trade off ini mendukung pencegahan daripada visibilitas lengkap ke dalam pola serangan.

Selain aturan berbasis tarif permanen yang dijelaskan di atas, grup aturan berisi aturan apa pun yang saat ini digunakan Shield Advanced untuk mengurangi serangan DDoS. Shield Advanced menambahkan, memodifikasi, dan menghapus aturan ini sesuai kebutuhan. Untuk informasi, lihat Bagaimana Shield Advanced mengelola mitigasi otomatis.

Metrik

Grup aturan menghasilkan AWS WAF metrik, tetapi karena grup aturan ini dimiliki oleh Shield Advanced, metrik ini tidak tersedia untuk dilihat. Untuk informasi selengkapnya, lihat AWS WAF metrik dan dimensi.

Mengelola mitigasi lapisan aplikasi DDoS otomatis

Gunakan panduan di bagian ini untuk mengelola konfigurasi mitigasi DDoS lapisan aplikasi otomatis Anda. Untuk informasi tentang cara kerja mitigasi otomatis, lihat topik sebelumnya.

> **Note**
>
> Ikuti praktik terbaik yang dijelaskan diPraktik terbaik untuk menggunakan mitigasi otomatis.

Topik

- Melihat konfigurasi mitigasi DDoS lapisan aplikasi otomatis untuk sumber daya
- Mengaktifkan dan menonaktifkan mitigasi DDoS lapisan aplikasi otomatis
- Mengubah tindakan yang digunakan untuk mitigasi DDoS lapisan aplikasi otomatis
- Menggunakan AWS CloudFormation dengan mitigasi DDoS lapisan aplikasi otomatis

Melihat konfigurasi mitigasi DDoS lapisan aplikasi otomatis untuk sumber daya

Anda dapat melihat konfigurasi mitigasi DDoS lapisan aplikasi otomatis untuk sumber daya di halaman Sumber daya yang dilindungi dan di halaman perlindungan individual.

Untuk melihat konfigurasi mitigasi DDoS lapisan aplikasi otomatis

1. Masuk ke AWS Management Console dan buka konsol AWS WAF & Shield di https://console.aws.amazon.com/wafv2/.
2. Di panel AWS Shield navigasi, pilih Sumber daya yang dilindungi. Dalam daftar sumber daya yang dilindungi, kolom Mitigasi DDoS lapisan aplikasi otomatis menunjukkan apakah mitigasi otomatis diaktifkan dan, jika diaktifkan, tindakan yang akan digunakan Shield Advanced dalam mitigasinya.

   Anda juga dapat memilih sumber daya lapisan aplikasi apa pun untuk melihat informasi yang sama yang tercantum di halaman perlindungan untuk sumber daya.

Mengaktifkan dan menonaktifkan mitigasi DDoS lapisan aplikasi otomatis

Prosedur berikut menunjukkan cara mengaktifkan atau menonaktifkan respons otomatis untuk sumber daya yang dilindungi.

Untuk mengaktifkan atau menonaktifkan mitigasi DDoS lapisan aplikasi otomatis untuk satu sumber daya

1. Masuk ke AWS Management Console dan buka konsol AWS WAF & Shield di https://console.aws.amazon.com/wafv2/.
2. Di panel AWS Shield navigasi, pilih Sumber daya yang dilindungi.
3. Di tab Protections, pilih sumber daya lapisan aplikasi yang ingin Anda aktifkan mitigasi otomatis. Halaman perlindungan terbuka untuk sumber daya.
4. Di halaman perlindungan sumber daya, pilih Edit.
5. Di halaman Konfigurasi lapisan 7 mitigasi DDoS untuk sumber daya global - opsional, untuk Mitigasi DDoS lapisan aplikasi otomatis, pilih opsi yang ingin Anda gunakan untuk mitigasi otomatis. Opsi di konsol adalah sebagai berikut:

   - Pertahankan pengaturan saat ini — Jangan membuat perubahan pada pengaturan mitigasi otomatis dari sumber daya yang dilindungi.

- Aktifkan - Aktifkan mitigasi otomatis untuk sumber daya yang dilindungi. Saat Anda memilih ini, pilih juga tindakan aturan yang Anda inginkan untuk digunakan mitigasi otomatis dalam aturan ACL web. Untuk informasi tentang setelan tindakan aturan, lihatTindakan aturan.

  Jika sumber daya yang dilindungi belum memiliki riwayat lalu lintas aplikasi normal, aktifkan mitigasi otomatis dalam Count mode hingga Shield Advanced dapat membuat baseline. Shield Advanced mulai mengumpulkan informasi untuk baseline ketika Anda mengaitkan ACL web dengan sumber daya yang dilindungi, dan dapat memakan waktu 24 jam hingga 30 hari untuk menetapkan garis dasar lalu lintas normal yang baik.
- Nonaktifkan - Nonaktifkan mitigasi otomatis untuk sumber daya yang dilindungi.

6. Berjalanlah melalui sisa halaman sampai Anda selesai dan simpan konfigurasi.

Di halaman Perlindungan, pengaturan mitigasi otomatis diperbarui untuk sumber daya.

Mengubah tindakan yang digunakan untuk mitigasi DDoS lapisan aplikasi otomatis

Anda dapat mengubah tindakan yang digunakan Shield Advanced untuk respons otomatis lapisan aplikasinya di beberapa lokasi di konsol:

- Konfigurasi mitigasi otomatis — Ubah tindakan saat Anda mengonfigurasi mitigasi otomatis untuk sumber daya Anda. Untuk prosedurnya, lihat bagian sebelumnya. Mengaktifkan dan menonaktifkan mitigasi DDoS lapisan aplikasi otomatis
- Halaman detail acara — Ubah tindakan di halaman detail acara, saat Anda melihat informasi acara di konsol. Untuk informasi, lihat AWS Shield Advanced rincian acara.

Jika Anda memiliki dua sumber daya terlindungi yang berbagi ACL web, dan Anda menetapkan tindakan Count untuk satu dan Block yang lain, Shield Advanced akan menetapkan tindakan untuk aturan berbasis laju grup aturan. `ShieldKnownOffenderIPRateBasedRule` Block

Menggunakan AWS CloudFormation dengan mitigasi DDoS lapisan aplikasi otomatis

Pahami cara menggunakan AWS CloudFormation untuk mengelola perlindungan dan ACL AWS WAF web Anda.

Mengaktifkan atau menonaktifkan mitigasi DDoS lapisan aplikasi otomatis

Anda dapat mengaktifkan dan menonaktifkan mitigasi DDoS lapisan aplikasi otomatis melalui AWS CloudFormation, menggunakan sumber daya. `AWS::Shield::Protection` Efeknya sama seperti

ketika Anda mengaktifkan atau menonaktifkan fitur melalui konsol atau antarmuka lainnya. Untuk informasi tentang AWS CloudFormation sumber daya, lihat AWS::Shield::Protectiondi panduan AWS CloudFormation pengguna.

Mengelola ACL web yang digunakan dengan mitigasi otomatis

Shield Advanced mengelola mitigasi otomatis untuk sumber daya yang dilindungi menggunakan aturan grup aturan di ACL AWS WAF web sumber daya yang dilindungi. Melalui AWS WAF konsol dan API, Anda akan melihat aturan yang tercantum dalam aturan ACL web Anda, dengan nama yang dimulai dengan`ShieldMitigationRuleGroup`. Aturan ini didedikasikan untuk mitigasi DDoS lapisan aplikasi otomatis Anda dan dikelola untuk Anda oleh Shield Advanced dan. AWS WAF Lihat informasi yang lebih lengkap di Grup aturan Shield Advanced dan Bagaimana Shield Advanced mengelola mitigasi otomatis.

Jika Anda menggunakannya AWS CloudFormation untuk mengelola ACL web, jangan tambahkan aturan grup aturan Shield Advanced ke template ACL web Anda. Saat Anda memperbarui ACL web yang digunakan dengan perlindungan mitigasi otomatis, AWS WAF secara otomatis mengelola aturan grup aturan di ACL web.

Anda akan melihat perbedaan berikut dibandingkan dengan ACL web lain yang Anda kelola melalui AWS CloudFormation:

- AWS CloudFormation tidak akan melaporkan penyimpangan apa pun dalam status stack drift antara konfigurasi ACL web yang sebenarnya, dengan aturan grup aturan Shield Advanced, dan template ACL web Anda, tanpa aturan. Aturan Shield Advanced tidak akan muncul di daftar sebenarnya untuk sumber daya dalam detail drift.

  Anda akan dapat melihat aturan grup aturan Shield Advanced di listingan ACL web yang Anda ambil AWS WAF, seperti melalui AWS WAF konsol atau AWS WAF API.
- Jika Anda memodifikasi template ACL web dalam tumpukan, AWS WAF dan Shield Advanced secara otomatis mempertahankan aturan mitigasi otomatis Shield Advanced di ACL web yang diperbarui. Perlindungan mitigasi otomatis yang disediakan oleh Shield Advanced tidak terganggu oleh pembaruan Anda ke ACL web.

Jangan mengelola aturan Shield Advanced di template ACL AWS CloudFormation web Anda. Template ACL web tidak boleh mencantumkan aturan Shield Advanced. Ikuti praktik terbaik untuk manajemen ACL web diPraktik terbaik untuk menggunakan mitigasi otomatis.

Deteksi berbasis kesehatan menggunakan pemeriksaan kesehatan

Anda dapat mengonfigurasi Shield Advanced untuk menggunakan deteksi berbasis kesehatan untuk meningkatkan respons dan akurasi dalam deteksi dan mitigasi serangan. Anda dapat menggunakan opsi ini dengan jenis sumber daya apa pun kecuali untuk zona yang dihosting Route 53.

Untuk mengonfigurasi deteksi berbasis kesehatan, Anda menentukan pemeriksaan kesehatan untuk sumber daya Anda di Route 53, memverifikasi apakah pelaporan tersebut sehat, lalu mengaitkannya dengan perlindungan Shield Advanced Anda. Untuk informasi tentang pemeriksaan kesehatan Route 53, lihat Cara Amazon Route 53 memeriksa kesehatan sumber daya Anda dan Membuat, memperbarui, dan menghapus pemeriksaan kesehatan di Panduan Pengembang Amazon Route 53.

> **Note**
>
> Pemeriksaan kesehatan diperlukan untuk dukungan keterlibatan proaktif Shield Response Team (SRT). Untuk informasi tentang keterlibatan proaktif, lihatMengkonfigurasi keterlibatan proaktif.

Pemeriksaan Kesehatan mengukur kesehatan sumber daya Anda berdasarkan persyaratan yang Anda tentukan. Status pemeriksaan kesehatan memberikan masukan penting ke mekanisme deteksi Shield Advanced, memberikan sensitivitas yang lebih besar terhadap status aplikasi spesifik Anda saat ini.

Anda dapat mengaktifkan deteksi berbasis kesehatan untuk semua jenis sumber daya kecuali untuk zona yang dihosting Route 53.

- Sumber daya lapisan jaringan dan transport (lapisan 3/lapisan 4) - Deteksi berbasis kesehatan meningkatkan akurasi deteksi dan mitigasi peristiwa lapisan jaringan dan lapisan transportasi untuk Network Load Balancer, alamat IP Elastis, dan akselerator standar Global Accelerator. Saat Anda melindungi jenis sumber daya ini dengan Shield Advanced, Shield Advanced dapat memberikan mitigasi untuk serangan yang lebih kecil dan mitigasi serangan yang lebih cepat, bahkan ketika lalu lintas berada dalam kapasitas aplikasi.

  Ketika Anda menambahkan deteksi berbasis kesehatan, selama periode ketika pemeriksaan kesehatan terkait tidak sehat, Shield Advanced dapat menempatkan mitigasi lebih cepat dan bahkan pada ambang batas yang lebih rendah.
- Sumber daya lapisan aplikasi (lapisan 7) — Deteksi berbasis kesehatan meningkatkan akurasi deteksi banjir permintaan web untuk CloudFront distribusi dan Application Load Balancer. Ketika

Anda melindungi jenis sumber daya ini dengan Shield Advanced, Anda menerima peringatan deteksi banjir permintaan web ketika ada penyimpangan signifikan secara statistik dalam volume lalu lintas yang dikombinasikan dengan perubahan signifikan dalam pola lalu lintas, berdasarkan karakteristik permintaan.

Dengan deteksi berbasis kesehatan, ketika pemeriksaan kesehatan Route 53 terkait tidak sehat, Shield Advanced membutuhkan penyimpangan yang lebih kecil untuk mengingatkan dan melaporkan kejadian lebih cepat. Sebaliknya, ketika pemeriksaan kesehatan Route 53 terkait sehat, Shield Advanced membutuhkan penyimpangan yang lebih besar untuk waspada.

Daftar Isi

Praktik terbaik untuk menggunakan pemeriksaan kesehatan dengan Shield Advanced

Ikuti praktik terbaik di bagian ini saat Anda membuat dan menggunakan pemeriksaan kesehatan dengan Shield Advanced.

- Rencanakan pemeriksaan kesehatan Anda dengan mengidentifikasi komponen infrastruktur yang ingin Anda pantau. Pertimbangkan jenis sumber daya berikut untuk pemeriksaan kesehatan:
  - Sumber daya kritis.
  - Sumber daya apa pun yang Anda inginkan sensitivitas lebih tinggi dalam deteksi dan mitigasi Shield Advanced.

  - Sumber daya yang Anda inginkan untuk Shield Advanced menjangkau Anda secara proaktif. Keterlibatan proaktif diinformasikan oleh status pemeriksaan kesehatan Anda.

  Contoh sumber daya yang mungkin ingin Anda pantau termasuk CloudFront distribusi Amazon, penyeimbang beban yang menghadap ke internet, dan instans Amazon EC2.

- Tentukan pemeriksaan kesehatan yang secara akurat mencerminkan kesehatan asal aplikasi Anda dengan pemberitahuan sesedikit mungkin.
  - Tulis pemeriksaan kesehatan sehingga hanya tidak sehat ketika aplikasi Anda tidak tersedia atau tidak berkinerja dalam parameter yang dapat diterima. Anda bertanggung jawab untuk menentukan dan memelihara pemeriksaan kesehatan berdasarkan persyaratan spesifik aplikasi Anda.
  - Gunakan pemeriksaan kesehatan sesedikit mungkin sambil tetap melaporkan kesehatan aplikasi Anda secara akurat. Misalnya, beberapa alarm dari beberapa area aplikasi Anda yang semuanya melaporkan masalah yang sama dapat menambah overhead ke aktivitas respons Anda tanpa menambahkan nilai informasi.
  - Gunakan pemeriksaan kesehatan terhitung untuk memantau kesehatan aplikasi menggunakan kombinasi CloudWatch metrik Amazon. Misalnya, Anda dapat menghitung kesehatan gabungan berdasarkan latensi server aplikasi Anda dan tingkat kesalahan 5xx mereka, yang menunjukkan bahwa server asal tidak memenuhi permintaan.
  - Buat dan publikasikan indikator kesehatan aplikasi Anda sendiri ke metrik CloudWatch khusus sesuai kebutuhan dan gunakan dalam pemeriksaan kesehatan yang dihitung.
- Terapkan dan kelola pemeriksaan kesehatan Anda untuk meningkatkan deteksi dan mengurangi aktivitas pemeliharaan yang tidak perlu.
  - Sebelum Anda mengaitkan pemeriksaan kesehatan dengan perlindungan Shield Advanced, pastikan itu dalam keadaan sehat. Mengaitkan pemeriksaan kesehatan yang melaporkan tidak sehat dapat mengubah mekanisme deteksi Shield Advanced untuk sumber daya Anda yang dilindungi.
  - Pastikan pemeriksaan kesehatan Anda tersedia untuk digunakan oleh Shield Advanced. Jangan menghapus pemeriksaan kesehatan di Route 53 yang Anda gunakan untuk perlindungan Shield Advanced.
  - Gunakan lingkungan pementasan dan pengujian hanya untuk menguji pemeriksaan kesehatan Anda. Hanya pertahankan asosiasi pemeriksaan kesehatan untuk lingkungan yang memerlukan kinerja dan ketersediaan tingkat produksi. Jangan menjaga asosiasi pemeriksaan kesehatan di Shield Advanced untuk lingkungan pementasan dan pengujian.

Metrik yang biasa digunakan untuk pemeriksaan kesehatan

Bagian ini mencantumkan CloudWatch metrik Amazon yang biasa digunakan dalam pemeriksaan kesehatan untuk mengukur kesehatan aplikasi selama peristiwa penolakan layanan terdistribusi (DDoS). Untuk informasi selengkapnya tentang CloudWatch metrik untuk setiap jenis sumber daya, lihat daftar yang mengikuti tabel.

Topik

Metrik digunakan untuk memantau kesehatan aplikasi

Sumber Daya	Metrik	Deskripsi
Route 53	`HealthCheckStatus`	Status titik akhir pemeriksaan kesehatan.
CloudFront	`5xxErrorRate`	Persentase semua permintaan yang kode status HTTP adalah 5xx. Ini menunjukkan serangan yang memengaruhi aplikasi.
Penyeimbang Beban Aplikasi	`HTTPCode_ELB_5XX_Count`	Jumlah kode kesalahan klien HTTP 5xx yang dihasilkan oleh penyeimbang beban.
Penyeimbang Beban Aplikasi	`RejectedConnectionCount`	Jumlah koneksi yang ditolak karena load balancer mencapai jumlah koneksi maksimumnya.
Penyeimbang Beban Aplikasi	`TargetConnectionErrorCount`	Jumlah koneksi yang tidak berhasil dibuat antara penyeimbang beban dan target.

Sumber Daya	Metrik	Deskripsi
Penyeimbang Beban Aplikasi	`TargetResponseTime`	Waktu berlalu dalam hitungan detik setelah permintaan meninggalkan penyeimbang beban dan ketika menerima respons dari target.
Penyeimbang Beban Aplikasi	`UnHealthyHostCount`	Jumlah target yang dianggap tidak sehat.
Amazon EC2	`CPUUtilization`	Persentase unit komputasi EC2 yang dialokasikan yang saat ini digunakan.

CloudWatch Metrik Amazon untuk setiap jenis sumber daya

Untuk informasi tambahan tentang metrik yang tersedia untuk sumber daya yang dilindungi, lihat bagian berikut di panduan sumber daya:

- Amazon Route 53 - Memantau sumber daya Anda dengan pemeriksaan kesehatan Amazon Route 53 dan Amazon CloudWatch di Panduan Pengembang Amazon Route 53.
- Amazon CloudFront - Pemantauan CloudFront dengan Amazon CloudWatch di Panduan CloudFront Pengembang Amazon.
- Application Load Balancer — CloudWatch metrik untuk Application Load Balancer Anda di Panduan Pengguna untuk Application Load Balancer.
- Network Load Balancer — CloudWatch metrik untuk Network Load Balancer Anda di Panduan Pengguna untuk Network Load Balancer.
- AWS Global Accelerator — Menggunakan Amazon CloudWatch dengan AWS Global Accelerator di Panduan AWS Global Accelerator Pengembang.
- Amazon Elastic Compute Cloud — Buat daftar CloudWatch metrik yang tersedia untuk instans Anda di https://docs.aws.amazon.com/ 2/latest/ /. AWSEC UserGuide
- Auto Scaling Amazon EC2 — Metrik CloudWatch pemantauan untuk grup dan instans Auto Scaling di Panduan Pengguna Auto Scaling Amazon EC2.

Mengelola asosiasi pemeriksaan kesehatan

Anda akan mendapat manfaat maksimal dari menggunakan pemeriksaan kesehatan dengan Shield Advanced jika pemeriksaan kesehatan hanya melaporkan sehat ketika aplikasi Anda berjalan dalam parameter yang dapat diterima dan hanya melaporkan tidak sehat jika tidak. Gunakan panduan di bagian ini untuk mengelola asosiasi pemeriksaan kesehatan Anda di Shield Advanced.

> **Note**
>
> Shield Advanced tidak secara otomatis mengelola pemeriksaan kesehatan Anda.

Berikut ini diperlukan untuk menggunakan pemeriksaan kesehatan dengan Shield Advanced:

- Pemeriksaan kesehatan harus dilaporkan sehat saat Anda mengaitkannya dengan perlindungan Shield Advanced Anda.
- Pemeriksaan kesehatan harus relevan dengan kesehatan sumber daya Anda yang dilindungi. Anda bertanggung jawab untuk menentukan dan memelihara pemeriksaan kesehatan yang secara akurat melaporkan kesehatan aplikasi Anda, berdasarkan persyaratan spesifik aplikasi Anda.
- Pemeriksaan kesehatan harus tetap tersedia untuk digunakan oleh perlindungan Shield Advanced. Jangan menghapus pemeriksaan kesehatan di Route 53 yang Anda gunakan untuk perlindungan Shield Advanced.

Topik

Mengaitkan pemeriksaan kesehatan dengan sumber daya Anda

Prosedur berikut menunjukkan cara mengaitkan pemeriksaan kesehatan Amazon Route 53 dengan sumber daya yang dilindungi.

> **Note**
>
> Sebelum Anda mengaitkan pemeriksaan kesehatan dengan perlindungan Shield Advanced, pastikan itu dalam keadaan sehat. Untuk selengkapnya, lihat Memantau status pemeriksaan kesehatan dan mendapatkan notifikasi di Panduan Pengembang Amazon Route 53.

Untuk mengaitkan pemeriksaan kesehatan

1. Masuk ke AWS Management Console dan buka konsol AWS WAF & Shield di https://console.aws.amazon.com/wafv2/.
2. Di panel AWS Shield navigasi, pilih Sumber daya yang dilindungi.
3. Pada tab Perlindungan, pilih sumber daya yang ingin Anda kaitkan dengan pemeriksaan kesehatan.
4. Pilih Konfigurasi perlindungan.
5. Pilih Berikutnya hingga Anda masuk ke halaman Konfigurasikan deteksi DDoS berbasis pemeriksaan kesehatan - opsional.
6. Di bawah Pemeriksaan Kesehatan Terkait, pilih ID pemeriksaan kesehatan yang ingin Anda kaitkan dengan perlindungan.

   > **Note**
   >
   > Jika Anda tidak melihat pemeriksaan kesehatan yang Anda butuhkan, buka konsol Route 53 dan verifikasi pemeriksaan kesehatan dan ID-nya. Untuk selengkapnya, lihat Membuat dan Memperbarui Pemeriksaan Kesehatan.

7. Berjalanlah melalui sisa halaman sampai Anda menyelesaikan konfigurasi. Pada halaman Perlindungan, asosiasi pemeriksaan kesehatan Anda yang diperbarui terdaftar untuk sumber daya.
8. Pada halaman Perlindungan, periksa apakah pemeriksaan kesehatan Anda yang baru terkait dilaporkan sehat.

   Anda tidak dapat berhasil mulai menggunakan pemeriksaan kesehatan di Shield Advanced saat pemeriksaan kesehatan melaporkan tidak sehat. Melakukan hal itu menyebabkan Shield Advanced mendeteksi positif palsu pada ambang batas yang sangat rendah dan juga dapat berdampak negatif pada kemampuan Tim Respons Shield (SRT) untuk menyediakan keterlibatan proaktif untuk sumber daya.

Jika pemeriksaan kesehatan yang baru terkait melaporkan tidak sehat, lakukan hal berikut:

a. Lepaskan pemeriksaan kesehatan dari perlindungan Anda di Shield Advanced.

b. Kunjungi kembali spesifikasi pemeriksaan kesehatan Anda di Amazon Route 53 dan verifikasi kinerja dan ketersediaan aplikasi Anda secara keseluruhan.

c. Ketika aplikasi Anda bekerja dalam parameter Anda untuk kesehatan yang baik dan pemeriksaan kesehatan Anda dilaporkan sehat, coba lagi untuk mengaitkan pemeriksaan kesehatan di Shield Advanced.

Prosedur asosiasi pemeriksaan kesehatan selesai ketika Anda telah membentuk asosiasi pemeriksaan kesehatan baru Anda dan dilaporkan sehat di Shield Advanced.

Memutuskan pemeriksaan kesehatan dari sumber daya Anda

Prosedur berikut menunjukkan cara memisahkan pemeriksaan kesehatan Amazon Route 53 dari sumber daya yang dilindungi.

Untuk memisahkan pemeriksaan kesehatan

1. Masuk ke AWS Management Console dan buka konsol AWS WAF & Shield di https://console.aws.amazon.com/wafv2/.
2. Di panel AWS Shield navigasi, pilih Sumber daya yang dilindungi.
3. Pada tab Proteksi, pilih sumber daya yang ingin Anda lepaskan dari pemeriksaan kesehatan.
4. Pilih Konfigurasi perlindungan.
5. Pilih Berikutnya hingga Anda masuk ke halaman Konfigurasikan deteksi DDoS berbasis pemeriksaan kesehatan - opsional.
6. Di bawah Pemeriksaan Kesehatan Terkait, pilih opsi kosong, terdaftar sebagai -.
7. Berjalanlah melalui sisa halaman sampai Anda menyelesaikan konfigurasi.

Pada halaman Proteksi, bidang pemeriksaan kesehatan untuk sumber daya Anda diatur ke -, yang menunjukkan tidak ada asosiasi pemeriksaan kesehatan.

Status asosiasi pemeriksaan kesehatan

Anda dapat melihat status pemeriksaan kesehatan yang terkait dengan perlindungan di halaman sumber daya yang Dilindungi konsol AWS WAF & Shield dan pada halaman detail setiap sumber daya.

- Sehat — Pemeriksaan kesehatan tersedia dan dilaporkan sehat.
- Tidak sehat — Pemeriksaan kesehatan tersedia dan melaporkan tidak sehat.
- Tidak tersedia — Pemeriksaan kesehatan tidak tersedia untuk digunakan oleh Shield Advanced.

Untuk menyelesaikan pemeriksaan kesehatan yang tidak tersedia

Buat dan gunakan pemeriksaan kesehatan baru. Jangan mencoba mengaitkan pemeriksaan kesehatan lagi setelah status tidak tersedia di Shield Advanced.

Untuk panduan terperinci tentang mengikuti langkah-langkah ini, lihat topik sebelumnya.

1. Di Shield Advanced, lepaskan pemeriksaan kesehatan dari sumber daya.
2. Di Route 53, buat pemeriksaan kesehatan baru untuk sumber daya dan catat ID-nya. Untuk selengkapnya, lihat Membuat dan Memperbarui Pemeriksaan Kesehatan di Panduan Pengembang Amazon Route 53.
3. Di Shield Advanced, kaitkan pemeriksaan kesehatan baru dengan sumber daya.

Contoh pemeriksaan kesehatan

Bagian ini menunjukkan contoh pemeriksaan kesehatan yang dapat Anda gunakan dalam pemeriksaan kesehatan yang dihitung. Pemeriksaan kesehatan yang dihitung menggunakan sejumlah pemeriksaan kesehatan individu untuk menentukan status gabungan. Status setiap pemeriksaan kesehatan individu didasarkan pada kesehatan titik akhir atau pada keadaan CloudWatch metrik Amazon. Anda menggabungkan pemeriksaan kesehatan ke dalam pemeriksaan kesehatan yang dihitung dan kemudian mengkonfigurasi pemeriksaan kesehatan Anda yang dihitung untuk melaporkan kesehatan berdasarkan status kesehatan gabungan dari pemeriksaan kesehatan individu. Sesuaikan sensitivitas pemeriksaan kesehatan yang Anda hitung sesuai dengan kebutuhan Anda untuk kinerja dan ketersediaan aplikasi.

Untuk informasi tentang pemeriksaan kesehatan yang dihitung, lihat Memantau pemeriksaan kesehatan lainnya (pemeriksaan kesehatan terhitung) di Panduan Pengembang Amazon Route

53. Untuk informasi tambahan, lihat posting blog Perbaikan Route 53 — Pemeriksaan Kesehatan Terhitung dan Pemeriksaan Latensi.

Topik

- CloudFront Distribusi Amazon
- Penyeimbang beban
- Alamat IP elastis Amazon EC2 (EIP)

CloudFront Distribusi Amazon

Contoh berikut menjelaskan pemeriksaan kesehatan yang dapat digabungkan menjadi pemeriksaan kesehatan yang dihitung untuk CloudFront distribusi:

- Pantau titik akhir dengan menentukan nama domain ke jalur distribusi yang menyajikan konten dinamis. Respons yang sehat akan mencakup kode respons HTTP 2xx dan 3xx.
- Pantau keadaan CloudWatch alarm yang mengukur kesehatan CloudFront asal. Misalnya, Anda dapat mempertahankan CloudWatch alarm pada metrik Application Load Balancer`TargetResponseTime`, dan membuat pemeriksaan kesehatan yang mencerminkan status alarm. Pemeriksaan kesehatan bisa menjadi tidak sehat ketika waktu respons, antara permintaan meninggalkan penyeimbang beban dan ketika penyeimbang beban menerima respons dari target, melebihi ambang batas yang dikonfigurasi dalam alarm.
- Pantau status CloudWatch alarm yang mengukur persentase permintaan yang kode status HTTP responsnya adalah 5xx. Jika tingkat kesalahan 5xx CloudFront distribusi lebih tinggi dari ambang batas yang ditentukan dalam CloudWatch alarm, status pemeriksaan kesehatan ini akan beralih ke tidak sehat.

Penyeimbang beban

Contoh berikut menjelaskan pemeriksaan kesehatan yang dapat digunakan dalam pemeriksaan kesehatan yang dihitung untuk Application Load Balancer, Network Load Balancer, atau akselerator standar Global Accelerator.

- Pantau keadaan CloudWatch alarm yang mengukur jumlah koneksi baru yang dibuat oleh klien ke penyeimbang beban. Anda dapat mengatur ambang alarm untuk jumlah rata-rata koneksi baru pada tingkat tertentu lebih tinggi dari rata-rata harian Anda. Metrik untuk setiap jenis sumber daya adalah sebagai berikut:
  - Application Load Balancer: `NewConnectionCount`

  - Network Load Balancer: `ActiveFlowCount`
  - Akselerator Global: `NewFlowCount`
- Untuk Application Load Balancer dan Network Load Balancer, pantau keadaan alarm CloudWatch yang mengukur jumlah load balancer yang dianggap sehat. Anda dapat mengatur ambang alarm baik di Availability Zone atau pada jumlah minimum host sehat yang dibutuhkan penyeimbang beban Anda. Metrik yang tersedia untuk sumber daya penyeimbang beban adalah sebagai berikut:
  - Application Load Balancer: `HealthyHostCount`
  - Network Load Balancer: `HealthyHostCount`
- Untuk Application Load Balancer, pantau status CloudWatch alarm yang mengukur jumlah kode respons HTTP 5xx yang dihasilkan oleh target penyeimbang beban. Untuk Application Load Balancer, Anda dapat menggunakan metrik `HTTPCode_Target_5XX_Count` dan mendasarkan ambang alarm pada jumlah semua kesalahan 5xx untuk penyeimbang beban.

Alamat IP elastis Amazon EC2 (EIP)

Contoh pemeriksaan kesehatan berikut dapat digabungkan menjadi pemeriksaan kesehatan yang dihitung untuk alamat IP elastis Amazon EC2:

- Pantau titik akhir dengan menentukan alamat IP ke alamat IP Elastis. Pemeriksaan kesehatan akan tetap sehat selama koneksi TCP dapat dibuat dengan sumber daya di belakang alamat IP.
- Pantau status CloudWatch alarm yang mengukur persentase unit komputasi Amazon EC2 yang dialokasikan yang saat ini digunakan pada instans. Anda dapat menggunakan metrik Amazon EC2 `CPUUtilization` dan mendasarkan ambang alarm pada apa yang Anda anggap sebagai tingkat pemanfaatan CPU yang tinggi untuk aplikasi Anda, seperti 90%.

Mengelola perlindungan sumber daya di AWS Shield Advanced

Gunakan panduan di bagian ini untuk mengelola perlindungan Shield Advanced untuk sumber daya Anda.

> **Note**
>
> Shield Advanced hanya melindungi sumber daya yang telah Anda tentukan di Shield Advanced atau melalui kebijakan AWS Firewall Manager Shield Advanced. Itu tidak secara otomatis melindungi sumber daya Anda.

Jika Anda menggunakan kebijakan AWS Firewall Manager Shield Advanced, Anda tidak perlu mengelola perlindungan untuk sumber daya yang berada dalam cakupan kebijakan. Firewall Manager secara otomatis mengelola perlindungan untuk akun dan sumber daya yang berada dalam cakupan kebijakan, sesuai dengan konfigurasi kebijakan. Untuk informasi selengkapnya, lihat AWS Shield Advanced kebijakan.

Topik

- Menambahkan AWS Shield Advanced perlindungan ke AWS sumber daya
- Mengkonfigurasi perlindungan AWS Shield Advanced
- Menghapus AWS Shield Advanced perlindungan dari sumber AWS daya

Menambahkan AWS Shield Advanced perlindungan ke AWS sumber daya

Ikuti panduan di bagian ini untuk menambahkan perlindungan Shield Advanced ke satu atau beberapa sumber daya.

Untuk menambahkan perlindungan untuk sumber AWS daya

1. Masuk ke AWS Management Console dan buka konsol AWS WAF & Shield di https://console.aws.amazon.com/wafv2/.
2. Di panel navigasi, di bawah AWS Shield pilih Sumber daya yang dilindungi.
3. Pilih Tambahkan sumber daya untuk dilindungi.
4. Di halaman Pilih sumber daya untuk dilindungi dengan Shield Advanced, di Tentukan Wilayah dan jenis sumber daya, berikan spesifikasi Wilayah dan tipe sumber daya untuk sumber daya yang ingin Anda lindungi. Anda dapat melindungi sumber daya di beberapa Wilayah dengan memilih Semua Wilayah dan Anda dapat mempersempit pilihan ke sumber daya global dengan memilih Global. Anda dapat membatalkan pilihan jenis sumber daya apa pun yang tidak ingin Anda lindungi. Untuk informasi tentang perlindungan untuk jenis sumber daya Anda, lihatAWS Shield Advanced perlindungan berdasarkan jenis sumber daya.
5. Pilih Muat sumber daya. Shield Advanced mengisi bagian Pilih Sumber Daya dengan AWS sumber daya yang sesuai dengan kriteria Anda.
6. Di bagian Pilih Sumber Daya, Anda dapat memfilter daftar sumber daya dengan memasukkan string untuk dicari di daftar sumber daya.

   Pilih sumber daya yang ingin Anda lindungi.

7. Di bagian Tag, jika Anda ingin menambahkan tag ke perlindungan Shield Advanced yang Anda buat, tentukan tag tersebut. Untuk informasi tentang menandai AWS sumber daya, lihat Bekerja dengan Editor Tag.
8. Pilih Protect dengan Shield Advanced. Ini menambahkan perlindungan Shield Advanced ke sumber daya.

Mengkonfigurasi perlindungan AWS Shield Advanced

Anda dapat mengubah pengaturan untuk AWS Shield Advanced perlindungan Anda kapan saja. Untuk melakukan ini, telusuri opsi untuk perlindungan yang Anda pilih dan ubah pengaturan yang perlu Anda ubah.

Untuk mengelola sumber daya yang dilindungi

1. Masuk ke AWS Management Console dan buka konsol AWS WAF & Shield di https://console.aws.amazon.com/wafv2/.
2. Di panel AWS Shield navigasi, pilih Sumber daya yang dilindungi.
3. Di tab Proteksi, pilih sumber daya yang ingin Anda lindungi.
4. Pilih Konfigurasi perlindungan dan opsi spesifikasi sumber daya yang Anda inginkan.
5. Berjalanlah melalui setiap opsi perlindungan sumber daya, buat perubahan sesuai kebutuhan.

Konfigurasikan perlindungan DDoS lapisan aplikasi

Untuk perlindungan terhadap serangan terhadap Amazon CloudFront dan sumber daya Application Load Balancer, Anda dapat menambahkan ACL AWS WAF web dan menambahkan aturan berbasis kecepatan. Untuk informasi tentang ini, lihatShield Advanced Application Layer AWS WAF Web ACL dan aturan berbasis tarif.

Anda juga dapat mengaktifkan mitigasi DDoS lapisan aplikasi otomatis Shield Advanced. Untuk informasi tentang cara AWS WAF kerja, lihatAWS WAF. Untuk informasi tentang fitur mitigasi otomatis, lihat. Mitigasi DDoS lapisan aplikasi otomatis Shield Advanced

> **Important**
>
> Jika Anda mengelola perlindungan Shield Advanced dengan AWS Firewall Manager menggunakan kebijakan Shield Advanced, Anda tidak dapat mengelola perlindungan lapisan aplikasi di sini. Untuk semua sumber daya lainnya, kami menyarankan agar, setidaknya,

Anda melampirkan ACL web ke setiap sumber daya, bahkan jika ACL web tidak berisi aturan apa pun.

> **Note**
>
> Saat Anda mengaktifkan mitigasi DDoS lapisan aplikasi otomatis untuk sumber daya, jika diperlukan, operasi secara otomatis menambahkan peran terkait layanan ke akun Anda untuk memberi Shield Advanced izin yang diperlukan untuk mengelola perlindungan ACL web Anda. Untuk informasi, lihat Menggunakan peran terkait layanan untuk Shield Advanced.

Untuk mengkonfigurasi perlindungan DDoS lapisan aplikasi

1. Di halaman Configure layer 7 DDoS protections, jika sumber daya belum dikaitkan dengan ACL web, Anda dapat memilih ACL web yang ada atau membuat sendiri.

   Untuk membuat ACL web, ikuti langkah-langkah berikut:

   a. Pilih Buat web ACL.

   b. Masukkan nama. Anda tidak dapat mengubah nama setelah membuat ACL web.

   c. Pilih Buat.

   > **Note**
   >
   > Jika sumber daya sudah dikaitkan dengan ACL web, Anda tidak dapat mengubah ke ACL web yang berbeda. Jika Anda ingin mengubah ACL web, Anda harus terlebih dahulu menghapus ACL web terkait dari sumber daya. Untuk informasi selengkapnya, lihat Mengaitkan atau memisahkan ACL web dengan sumber daya AWS.

2. Jika ACL web tidak memiliki aturan berbasis tarif yang ditentukan, Anda dapat menambahkannya dengan memilih aturan Tambah batas tingkat dan kemudian melakukan langkah-langkah berikut:

   a. Masukkan nama.

   b. Masukkan batas tarif. Ini adalah jumlah maksimum permintaan yang diizinkan dalam periode lima menit dari alamat IP tunggal sebelum tindakan aturan berbasis tarif diterapkan ke alamat IP. Ketika permintaan dari alamat IP jatuh di bawah batas, tindakan dihentikan.

c. Tetapkan tindakan aturan untuk menghitung atau memblokir permintaan dari alamat IP saat jumlah permintaannya melebihi batas. Aplikasi dan penghapusan tindakan aturan mungkin berlaku satu atau dua menit setelah tingkat permintaan alamat IP berubah.

d. Pilih Tambahkan aturan.

3. Untuk mitigasi DDoS lapisan aplikasi Otomatis, pilih apakah Anda ingin Shield Advanced untuk secara otomatis mengurangi serangan DDoS atas nama Anda, sebagai berikut:

   - Untuk mengaktifkan mitigasi otomatis, pilih Aktifkan, lalu pilih tindakan AWS WAF aturan yang ingin digunakan Shield Advanced dalam aturan kustomnya. Pilihan Anda adalah Count danBlock. Untuk informasi tentang tindakan AWS WAF aturan ini, lihatTindakan aturan. Untuk informasi tentang cara Shield Advanced mengelola setelan tindakan ini, lihatBagaimana Shield Advanced mengelola pengaturan tindakan aturan.
   - Untuk menonaktifkan mitigasi otomatis, pilih Nonaktifkan.
   - Agar pengaturan mitigasi otomatis tidak berubah untuk sumber daya yang Anda kelola, biarkan pilihan default Simpan pengaturan saat ini.

   Untuk informasi tentang mitigasi DDoS lapisan aplikasi otomatis Shield Advanced, lihat. Mitigasi DDoS lapisan aplikasi otomatis Shield Advanced

4. Pilih Berikutnya.

Buat alarm dan notifikasi

Prosedur berikut menunjukkan cara mengelola CloudWatch alarm untuk sumber daya yang dilindungi.

> **Note**
>
> CloudWatch menimbulkan biaya tambahan. Untuk CloudWatch harga, lihat CloudWatch Harga Amazon.

Untuk membuat alarm dan notifikasi

1. Di halaman perlindungan Buat alarm dan pemberitahuan - opsional, konfigurasikan topik SNS untuk alarm dan pemberitahuan yang ingin Anda terima. Untuk sumber daya yang tidak Anda

inginkan notifikasi, pilih Tidak ada topik. Anda dapat menambahkan topik Amazon SNS atau membuat topik baru.

2. Untuk membuat topik Amazon SNS, ikuti langkah-langkah ini:

   a. Dalam daftar dropdown, pilih Buat topik SNS.

   b. Masukkan nama topik.

   c. Secara opsional masukkan alamat email tempat pesan Amazon SNS akan dikirim, lalu pilih Tambahkan email. Anda dapat memasukkan lebih dari satu.

   d. Pilih Buat.

3. Pilih Berikutnya.

Menghapus AWS Shield Advanced perlindungan dari sumber AWS daya

Anda dapat menghapus AWS Shield Advanced perlindungan dari AWS sumber daya Anda kapan saja.

> **Important**
>
> Menghapus sumber AWS daya tidak menghapus sumber daya dari AWS Shield Advanced. Anda juga harus menghapus perlindungan pada sumber daya dari AWS Shield Advanced, seperti yang dijelaskan dalam prosedur ini.

Hapus AWS Shield Advanced perlindungan dari sumber AWS daya

1. Masuk ke AWS Management Console dan buka konsol AWS WAF & Shield di https://console.aws.amazon.com/wafv2/.
2. Di panel AWS Shield navigasi, pilih Sumber daya yang dilindungi.
3. Di tab Perlindungan, pilih sumber daya yang perlindungannya ingin Anda hapus.
4. Pilih Hapus perlindungan.

   - Jika Anda memiliki CloudWatch alarm Amazon yang dikonfigurasi untuk perlindungan, Anda diberi opsi untuk menghapus alarm bersama dengan perlindungan. Jika Anda memilih untuk tidak menghapus alarm pada saat ini, Anda dapat menghapusnya nanti menggunakan CloudWatch konsol.

> **Note**
>
> Untuk perlindungan yang memiliki pemeriksaan kesehatan Amazon Route 53 yang dikonfigurasi, jika Anda menambahkan perlindungan lagi nanti, perlindungan masih termasuk pemeriksaan kesehatan.

Langkah-langkah sebelumnya menghapus AWS Shield Advanced perlindungan dari sumber daya tertentu AWS . Mereka tidak membatalkan AWS Shield Advanced langganan Anda. Anda akan terus dikenakan biaya untuk layanan ini. Untuk informasi tentang AWS Shield Advanced langganan Anda, hubungi AWS Support Pusat.

Menghapus CloudWatch alarm dari perlindungan Shield Advanced

Untuk menghapus CloudWatch alarm dari perlindungan Shield Advanced, lakukan salah satu hal berikut:

- Hapus perlindungan seperti yang dijelaskan dalamMenghapus AWS Shield Advanced perlindungan dari sumber AWS daya. Pastikan untuk memilih kotak centang di samping Hapus juga alarm Deteksi DDoS terkait.
- Hapus alarm menggunakan CloudWatch konsol. Nama alarm yang akan dihapus dimulai dengan DDoS DetectedAlarmForProtection.

AWS Shield Advanced kelompok perlindungan

Gunakan grup perlindungan untuk membuat koleksi logis dari sumber daya Anda yang dilindungi dan mengelola perlindungan mereka sebagai grup. Untuk informasi tentang mengelola perlindungan sumber daya, lihatMengkonfigurasi perlindungan AWS Shield Advanced.

> **Note**
>
> Mitigasi DDoS lapisan aplikasi otomatis tidak berinteraksi dengan kelompok perlindungan. Anda dapat mengaktifkan mitigasi otomatis untuk sumber daya yang ada di grup perlindungan, tetapi Shield Advanced tidak secara otomatis menerapkan mitigasi serangan berdasarkan temuan kelompok perlindungan. Shield Advanced menerapkan mitigasi serangan otomatis untuk sumber daya individu.

AWS Shield Advanced kelompok perlindungan memberi Anda cara swalayan untuk menyesuaikan ruang lingkup deteksi dan mitigasi dengan memperlakukan beberapa sumber daya yang dilindungi sebagai satu unit. Pengelompokan sumber daya dapat memberikan sejumlah manfaat.

- Meningkatkan akurasi deteksi.
- Kurangi pemberitahuan acara yang tidak dapat ditindaklanjuti.
- Meningkatkan cakupan tindakan mitigasi untuk memasukkan sumber daya yang dilindungi yang juga mungkin terpengaruh selama suatu acara.
- Mempercepat waktu untuk mitigasi serangan dengan beberapa target serupa.
- Memfasilitasi perlindungan otomatis sumber daya yang dilindungi yang baru dibuat.

Kelompok perlindungan dapat membantu mengurangi positif palsu dalam situasi seperti swap biru/hijau, di mana sumber daya bergantian antara mendekati nol beban dan terisi penuh. Contoh lain adalah ketika Anda sering membuat dan menghapus sumber daya sambil mempertahankan tingkat beban yang dibagikan di antara anggota grup. Untuk situasi seperti ini, pemantauan sumber daya individu dapat menyebabkan positif palsu, sementara memantau kesehatan kelompok sumber daya tidak.

Anda dapat mengonfigurasi grup perlindungan untuk menyertakan semua sumber daya yang dilindungi, semua sumber daya dari jenis sumber daya tertentu, atau sumber daya yang ditentukan secara individual. Sumber daya yang baru dilindungi yang memenuhi kriteria kelompok perlindungan Anda secara otomatis disertakan dalam grup perlindungan Anda. Sumber daya yang dilindungi dapat menjadi milik beberapa kelompok perlindungan.

Mengelola kelompok AWS Shield Advanced perlindungan

Gunakan panduan di bagian ini untuk mengelola konfigurasi grup perlindungan Anda.

Membuat grup perlindungan Shield Advanced

Untuk membuat grup perlindungan

1. Masuk ke AWS Management Console dan buka konsol AWS WAF & Shield di https://console.aws.amazon.com/wafv2/.
2. Di panel AWS Shield navigasi, pilih Sumber daya yang dilindungi.
3. Pilih tab Grup perlindungan, lalu pilih Buat grup perlindungan.

4. Di halaman Buat grup perlindungan, berikan nama untuk grup Anda. Anda akan menggunakan nama ini untuk mengidentifikasi grup dalam daftar sumber daya yang dilindungi. Anda tidak dapat mengubah nama grup perlindungan setelah Anda membuatnya.
5. Untuk kriteria pengelompokan Perlindungan, pilih kriteria yang Anda inginkan untuk digunakan Shield Advanced untuk mengidentifikasi sumber daya yang dilindungi untuk disertakan dalam grup. Buat pilihan tambahan Anda berdasarkan kriteria yang Anda pilih.
6. Untuk Agregasi, pilih cara Anda ingin Shield Advanced menggabungkan data sumber daya untuk grup untuk mendeteksi, mengurangi, dan melaporkan peristiwa.

   - Jumlah — Gunakan total lalu lintas di seluruh grup. Ini adalah pilihan yang baik untuk kebanyakan kasus. Contohnya termasuk alamat IP Elastis untuk instans Amazon EC2 yang menskalakan secara manual atau otomatis.
   - Mean — Gunakan rata-rata lalu lintas di seluruh grup. Ini adalah pilihan yang baik untuk sumber daya yang berbagi lalu lintas secara seragam. Contohnya termasuk akselerator dan penyeimbang beban.
   - Maks — Gunakan lalu lintas tertinggi dari setiap sumber daya. Ini berguna untuk sumber daya yang tidak berbagi lalu lintas, dan untuk sumber daya yang berbagi lalu lintas dengan cara yang tidak seragam. Contohnya termasuk CloudFront distribusi Amazon dan sumber daya asal untuk CloudFront distribusi.
7. Pilih Simpan untuk menyimpan grup perlindungan Anda dan kembali ke halaman Sumber daya yang dilindungi.

Di halaman Shield Events, Anda dapat melihat peristiwa untuk grup perlindungan dan menelusuri untuk melihat informasi tambahan untuk sumber daya yang dilindungi yang ada di grup.

Memperbarui grup perlindungan Shield Advanced

Untuk memperbarui grup perlindungan

1. Masuk ke AWS Management Console dan buka konsol AWS WAF & Shield di https://console.aws.amazon.com/wafv2/.
2. Di panel AWS Shield navigasi, pilih Sumber daya yang dilindungi.
3. Di tab Grup perlindungan, pilih kotak centang di samping grup perlindungan yang ingin Anda ubah.
4. Di halaman grup perlindungan, pilih Edit. Buat perubahan Anda pada pengaturan grup perlindungan.

5. Pilih Simpan untuk menyimpan perubahan Anda.

Menghapus grup perlindungan Shield Advanced

Untuk menghapus grup perlindungan

1. Masuk ke AWS Management Console dan buka konsol AWS WAF & Shield di https://console.aws.amazon.com/wafv2/.
2. Di panel AWS Shield navigasi, pilih Sumber daya yang dilindungi.
3. Di tab Grup perlindungan, pilih kotak centang di samping grup perlindungan yang ingin Anda hapus.
4. Di halaman grup perlindungan, pilih Hapus dan konfirmasikan tindakan.

Melacak perubahan perlindungan sumber daya di AWS Config

Anda dapat merekam perubahan pada AWS Shield Advanced perlindungan sumber daya Anda menggunakan AWS Config. Anda kemudian dapat menggunakan informasi ini untuk mempertahankan riwayat perubahan konfigurasi untuk tujuan audit dan pemecahan masalah.

Untuk merekam perubahan perlindungan, aktifkan AWS Config untuk setiap sumber daya yang ingin Anda lacak. Untuk informasi selengkapnya, lihat Memulai AWS Config di Panduan Pengguna AWS Config .

Anda harus mengaktifkan AWS Config untuk setiap Wilayah AWS yang berisi sumber daya yang dilacak. Anda dapat mengaktifkan AWS Config secara manual, atau Anda dapat menggunakan AWS CloudFormation templat “Aktifkan AWS Config” di Template AWS CloudFormation StackSets Sampel di Panduan AWS CloudFormation Pengguna.

Jika Anda mengaktifkan AWS Config, Anda akan dikenakan biaya seperti yang dijelaskan pada halaman AWS Config Harga.

> **Note**
>
> Jika Anda sudah AWS Config mengaktifkan Wilayah dan sumber daya yang diperlukan, Anda tidak perlu melakukan apa pun. AWS Config log mengenai perubahan perlindungan pada sumber daya Anda mulai terisi secara otomatis.

Setelah mengaktifkan AWS Config, gunakan Wilayah AS Timur (Virginia N.) di AWS Config konsol untuk melihat riwayat perubahan konfigurasi untuk sumber daya AWS Shield Advanced global.

Lihat sejarah perubahan untuk sumber daya AWS Shield Advanced regional melalui AWS Config konsol di AS Timur (Virginia N.), AS Timur (Ohio), AS Barat (Oregon), AS Barat (California N.), Eropa (Irlandia), Eropa (Frankfurt), Asia Pasifik (Tokyo), dan Asia Pasifik (Sydney).

Visibilitas ke acara DDoS

AWS Shield memberikan visibilitas ke dalam kategori acara dan kegiatan acara berikut:

- Global — Semua pelanggan dapat mengakses pandangan agregat aktivitas ancaman global selama dua minggu terakhir. Anda dapat melihat informasi ini di bawah halaman dasbor Memulai dan Ancaman Global AWS Shield konsol. Untuk informasi selengkapnya, lihat AWS Shield aktivitas global dan akun.
- Akun — Semua pelanggan dapat mengakses ringkasan acara untuk akun mereka selama tahun sebelumnya. Anda dapat melihat informasi ini di bawah halaman Memulai AWS Shield konsol. Untuk informasi selengkapnya, lihat AWS Shield aktivitas global dan akun.

Saat Anda berlangganan Shield Advanced dan menambahkan perlindungan ke sumber daya Anda, Anda mendapatkan akses ke informasi tambahan tentang peristiwa dan serangan DDoS pada sumber daya yang dilindungi:

- Acara pada sumber daya yang dilindungi — Shield Advanced memberikan informasi terperinci untuk setiap acara melalui halaman Acara AWS Shield konsol. Untuk informasi selengkapnya, lihat AWS Shield Advanced acara.
- Metrik peristiwa untuk sumber daya yang dilindungi — Shield Advanced menerbitkan CloudWatch metrik Amazon deteksi, mitigasi, dan kontributor teratas untuk semua sumber daya yang dilindungi. Anda dapat menggunakan metrik ini untuk mengonfigurasi CloudWatch dasbor dan alarm. Untuk informasi selengkapnya, lihat AWS Shield Advanced metrik.
- Visibilitas peristiwa lintas akun untuk sumber daya yang dilindungi — Jika Anda menggunakannya AWS Firewall Manager untuk mengelola perlindungan Shield Advanced, Anda dapat mengaktifkan visibilitas ke dalam perlindungan di beberapa akun dengan menggunakan Firewall Manager yang digabungkan dengannya. AWS Security Hub Untuk informasi selengkapnya, lihat Visibilitas acara di seluruh akun.

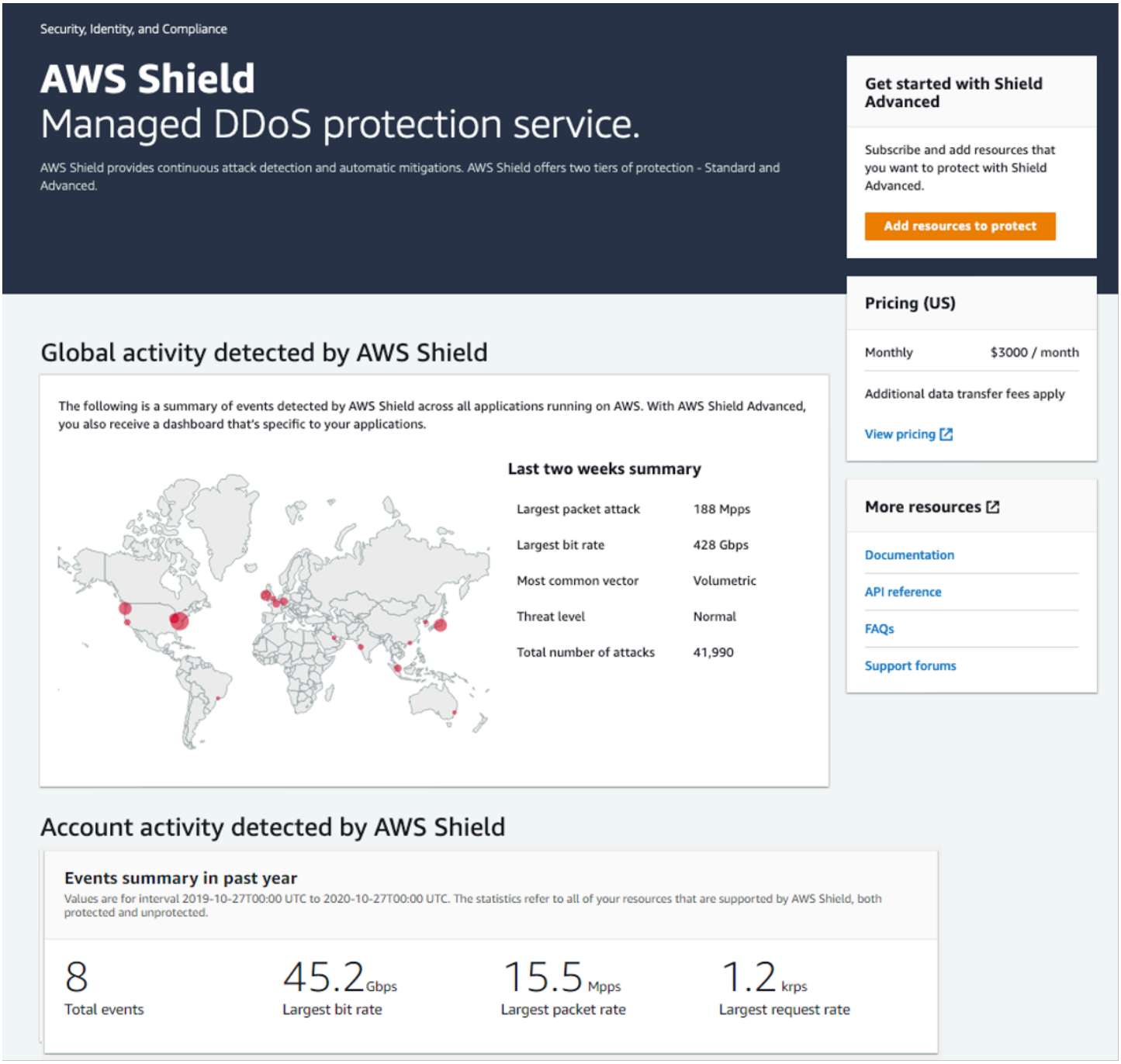
Jika Anda mengaktifkan mitigasi DDoS lapisan aplikasi otomatis untuk perlindungan lapisan aplikasi,

Topik

AWS Shield aktivitas global dan akun

Anda dapat mengakses tampilan agregat aktivitas ancaman global dan ringkasan peristiwa per akun di halaman dasbor Memulai AWS Shield konsol dan ancaman global.

Screenshot berikut menunjukkan contoh halaman Memulai.



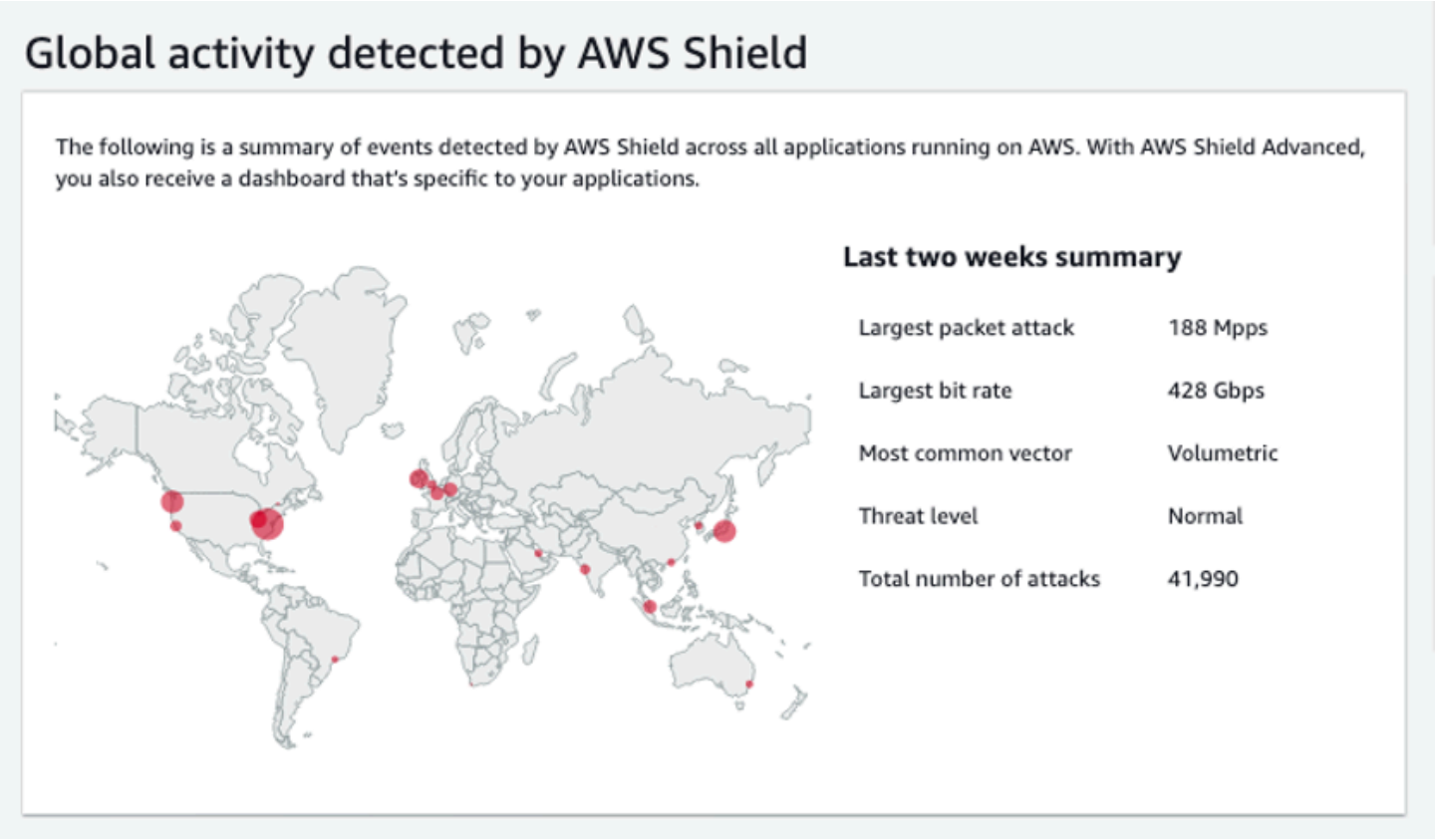
Untuk mengakses AWS Shield konsol

- Masuk ke AWS Management Console dan buka konsol AWS WAF & Shield di https://console.aws.amazon.com/wafv2/.

Anda tidak perlu berlangganan Shield Advanced untuk mengakses aktivitas global dan informasi ringkasan acara akun.

Aktivitas global

Informasi ini tersedia melalui AWS Shield konsol Dasbor ancaman global dan halaman Memulai. Screenshot berikut menunjukkan contoh panel aktivitas global.



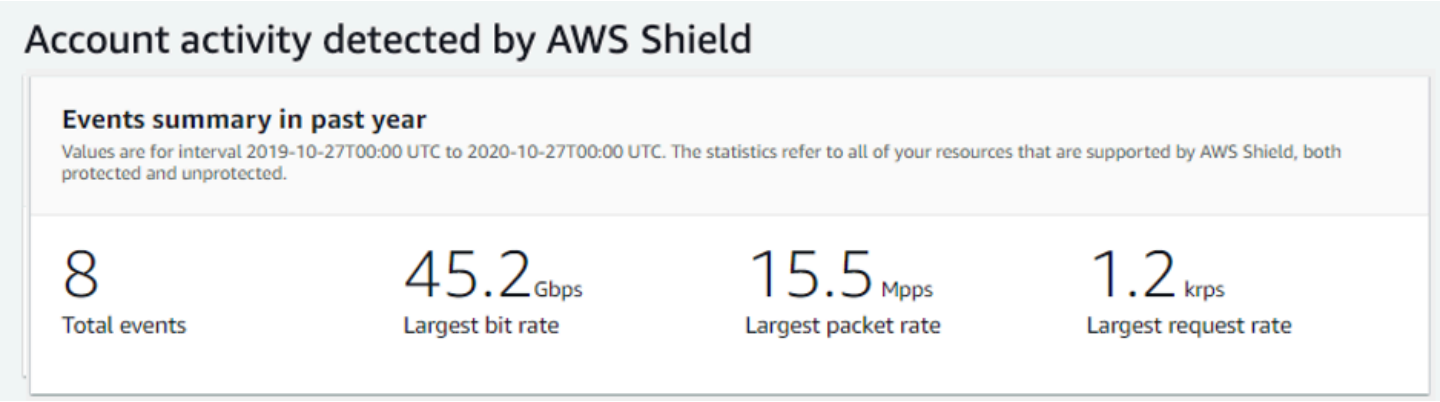
Aktivitas global menggambarkan peristiwa DDoS yang diamati di semua AWS pelanggan. Sekali per jam, AWS perbarui informasi untuk dua minggu sebelumnya. Di panel konsol, Anda dapat melihat hasilnya, dipartisi berdasarkan AWS Wilayah dan ditampilkan pada peta panas dunia. Di sebelah peta, Shield menampilkan informasi ringkasan seperti serangan paket terbesar, bit rate terbesar, vektor paling umum, jumlah total serangan, dan tingkat ancaman. Tingkat ancaman adalah penilaian aktivitas global saat ini dibandingkan dengan apa yang AWS biasanya diamati. Nilai tingkat ancaman default adalah Normal. AWS secara otomatis memperbarui nilai ke Tinggi untuk aktivitas DDoS yang ditinggikan.

Dasbor ancaman Global juga menyediakan metrik deret waktu dan memberi Anda kemampuan untuk mengubah antara durasi waktu. Untuk melihat riwayat serangan DDoS yang signifikan, Anda dapat menyesuaikan dasbor untuk tampilan dari hari terakhir hingga dua minggu terakhir. Metrik deret waktu memberikan tampilan bit rate, laju paket, atau tingkat permintaan terbesar untuk semua peristiwa yang terdeteksi oleh AWS Shield untuk aplikasi yang berjalan AWS selama jendela waktu yang Anda pilih.

Aktivitas akun

Informasi ini tersedia di halaman Memulai AWS Shield konsol.

Screenshot berikut menunjukkan contoh panel aktivitas akun.



Aktivitas akun menjelaskan peristiwa DDoS yang terdeteksi Shield untuk sumber daya Anda yang memenuhi syarat untuk perlindungan oleh Shield Advanced. Setiap hari, Shield membuat metrik ringkasan untuk tahun yang berakhir pada pukul 00:00 UTC pada hari sebelumnya, dan kemudian menampilkan total peristiwa, bit rate terbesar, tarif paket terbesar, dan tingkat permintaan terbesar.

- Metrik peristiwa total mencerminkan setiap kali Shield mengamati atribut mencurigakan dalam lalu lintas yang ditujukan untuk aplikasi Anda. Atribut mencurigakan dapat mencakup lalu lintas yang lebih tinggi dari volume normal, lalu lintas yang tidak sesuai dengan profil historis aplikasi Anda, atau lalu lintas yang tidak cocok dengan heuristik yang ditentukan oleh Shield untuk lalu lintas aplikasi yang valid.
- Bit rate terbesar dan statistik laju paket terbesar tersedia untuk setiap sumber daya.
- Statistik tingkat permintaan terbesar hanya tersedia untuk CloudFront distribusi Amazon dan Application Load Balancer yang memiliki ACL web terkait AWS WAF .

> **Note**
>
> Anda juga dapat mengakses ringkasan peristiwa tingkat akun melalui operasi AWS Shield API DescribeAttackStatistics.

AWS Shield Advanced acara

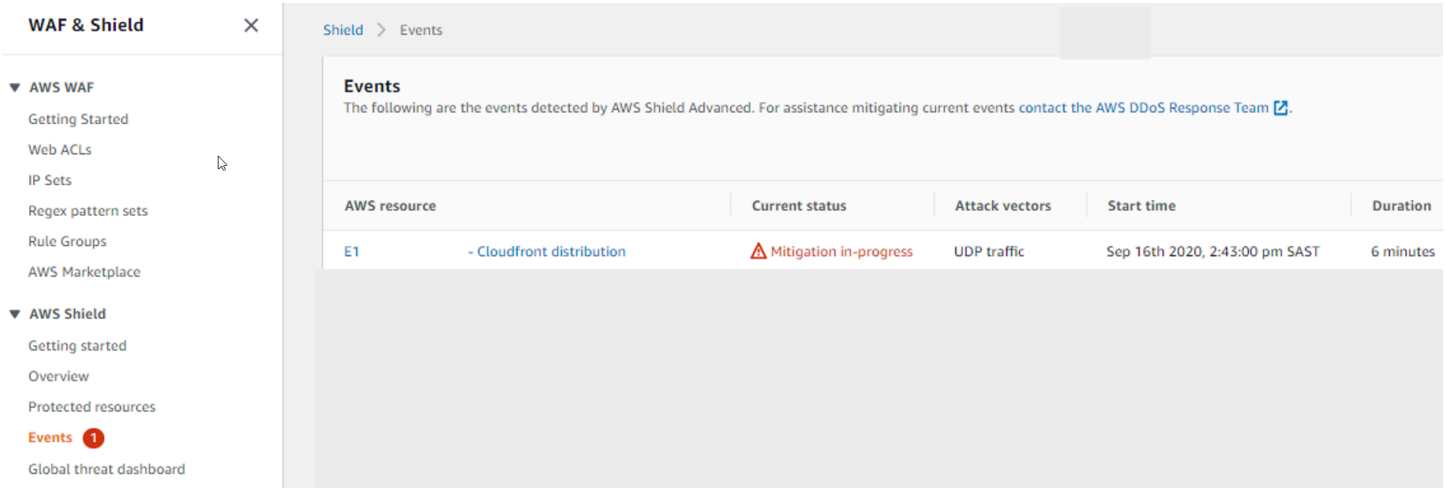
Saat berlangganan Shield Advanced, dan melindungi sumber daya, Anda mendapatkan akses ke fitur visibilitas tambahan untuk sumber daya. Ini termasuk pemberitahuan peristiwa yang hampir real-time yang terdeteksi oleh Shield Advanced dan informasi tambahan tentang peristiwa dan mitigasi yang terdeteksi.

> **Note**
>
> Informasi acara Anda di konsol Shield Advanced didasarkan pada metrik Shield Advanced. Untuk informasi tentang metrik Shield Advanced, lihat AWS Shield Advanced metrik

AWS Shield mengevaluasi lalu lintas ke sumber daya terlindungi Anda di berbagai dimensi. Ketika anomali terdeteksi, Shield Advanced membuat peristiwa terpisah untuk setiap sumber daya yang terpengaruh.

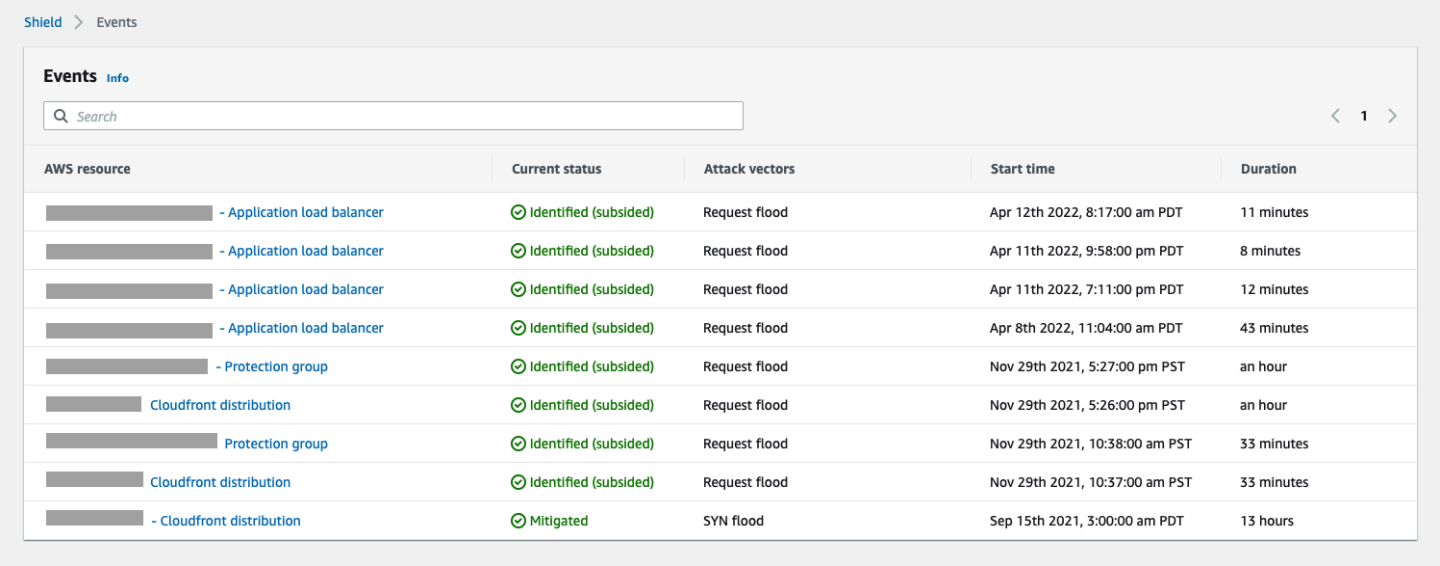
Anda dapat mengakses ringkasan dan detail acara melalui halaman Acara di konsol Shield. Halaman Acara tingkat atas memberikan ikhtisar peristiwa saat ini dan masa lalu.

Tangkapan layar berikut menunjukkan contoh halaman Acara dengan satu acara yang sedang berlangsung. Acara aktif ini juga ditandai di panel navigasi kiri.



Shield Advanced mungkin juga secara otomatis menempatkan mitigasi terhadap serangan, tergantung pada jenis lalu lintas dan perlindungan yang dikonfigurasi. Mitigasi ini dapat melindungi sumber daya Anda dari menerima kelebihan lalu lintas atau lalu lintas yang cocok dengan tanda tangan serangan DDoS yang dikenal.

Tangkapan layar berikut menunjukkan contoh daftar Acara di mana semua peristiwa telah dikurangi oleh Shield Advanced atau telah mereda dengan sendirinya.



Lindungi sumber daya Anda sebelum acara

Tingkatkan akurasi deteksi peristiwa dengan melindungi sumber daya dengan Shield Advanced saat mereka menerima lalu lintas normal yang diharapkan, sebelum mereka terkena serangan DDoS.

Untuk melaporkan peristiwa secara akurat untuk sumber daya yang dilindungi, Shield Advanced harus terlebih dahulu menetapkan dasar pola lalu lintas yang diharapkan untuknya.

- Shield Advanced melaporkan peristiwa lapisan infrastruktur untuk sumber daya setelah dilindungi setidaknya selama 15 menit.
- Shield Advanced melaporkan peristiwa lapisan aplikasi web untuk sumber daya setelah dilindungi setidaknya selama 24 jam. Keakuratan deteksi untuk peristiwa lapisan aplikasi adalah yang terbaik setelah Shield Advanced mengamati lalu lintas yang diharapkan selama 30 hari.

Untuk mengakses informasi peristiwa di AWS Shield konsol

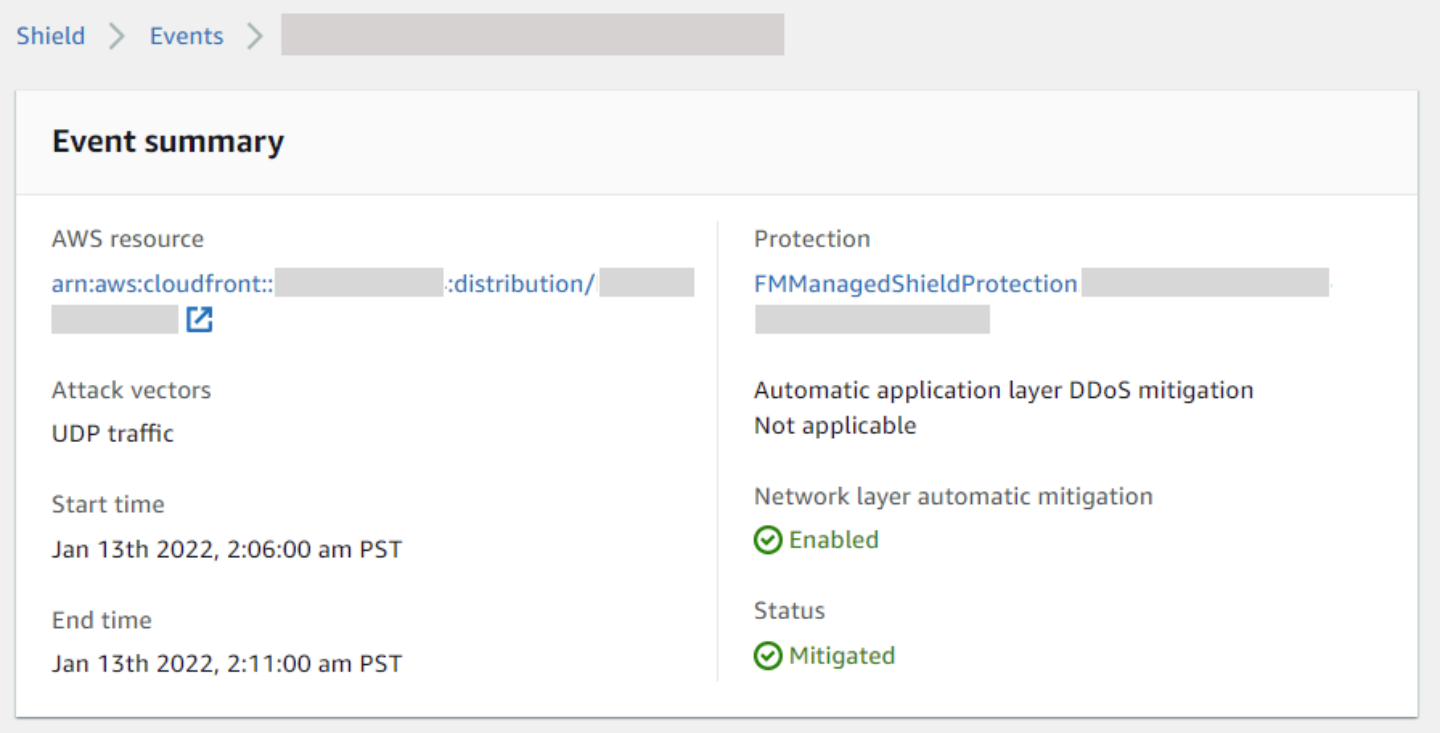
1. Masuk ke AWS Management Console dan buka konsol AWS WAF & Shield di https://console.aws.amazon.com/wafv2/.
2. Di panel AWS Shield navigasi, pilih Acara. Konsol menampilkan halaman Acara.
3. Dari halaman Acara, Anda dapat memilih acara apa pun dalam daftar untuk melihat informasi ringkasan dan detail tambahan untuk acara tersebut.

Topik

AWS Shield Advanced ringkasan acara

Anda dapat melihat ringkasan dan informasi detail untuk suatu acara di halaman konsol acara. Untuk membuka halaman acara, pilih nama AWS sumber dayanya dari daftar halaman Acara.

Tangkapan layar berikut menunjukkan contoh ringkasan acara untuk acara lapisan jaringan.



Informasi ringkasan halaman acara mencakup yang berikut ini.

- Status saat ini — Nilai yang menunjukkan status acara dan tindakan yang dilakukan Shield Advanced pada acara tersebut. Nilai status berlaku untuk lapisan infrastruktur (lapisan 3 atau 4) dan lapisan aplikasi (lapisan 7) peristiwa.
  - Diidentifikasi (sedang berlangsung) dan Diidentifikasi (mereda) — Ini menunjukkan bahwa Shield Advanced mendeteksi suatu peristiwa, tetapi sejauh ini belum mengambil tindakan terhadapnya. Diidentifikasi (mereda) menunjukkan bahwa lalu lintas mencurigakan yang terdeteksi Shield telah berhenti tanpa intervensi.

  - Mitigasi sedang berlangsung dan Dimitigasi — Ini menunjukkan bahwa Shield Advanced mendeteksi suatu peristiwa dan telah mengambil tindakan terhadapnya. Mitigated juga digunakan ketika sumber daya yang ditargetkan adalah CloudFront distribusi Amazon atau zona yang dihosting Amazon Route 53, yang memiliki mitigasi inline otomatis mereka sendiri.
- Vektor serangan — Vektor serangan DDoS seperti banjir TCP SYN dan heuristik deteksi Shield Advanced seperti banjir permintaan. Ini bisa menjadi indikator serangan DDoS.
- Waktu mulai - Tanggal dan waktu titik data lalu lintas anomali pertama terdeteksi.
- Durasi atau waktu akhir — Menunjukkan waktu yang telah berlalu antara waktu mulai peristiwa dan titik data anomali terakhir yang diamati yang diamati Shield Advanced. Sementara sebuah acara sedang berlangsung, nilai-nilai ini akan terus meningkat.
- Perlindungan — Menamai perlindungan Shield Advanced yang terkait dengan sumber daya, dan menyediakan tautan ke halaman perlindungannya. Ini tersedia di halaman acara individu.
- Mitigasi DDoS lapisan aplikasi otomatis — Digunakan untuk perlindungan lapisan aplikasi, untuk menunjukkan apakah mitigasi DDoS lapisan aplikasi otomatis Shield Advanced diaktifkan untuk sumber daya. Jika diaktifkan, ini menyediakan tautan untuk mengakses dan mengelola konfigurasi. Ini tersedia di halaman acara individu.
- Mitigasi otomatis lapisan jaringan - Menunjukkan apakah sumber daya memiliki mitigasi otomatis pada lapisan jaringan. Jika sumber daya memiliki komponen lapisan jaringan, itu akan mengaktifkan ini. Informasi ini tersedia di halaman acara individu.

Untuk sumber daya yang sering ditargetkan, Shield dapat meninggalkan mitigasi di tempat setelah kelebihan lalu lintas telah mereda, untuk mencegah kejadian berulang lebih lanjut.

> **Note**
>
> Anda juga dapat mengakses ringkasan peristiwa untuk sumber daya yang dilindungi melalui operasi AWS Shield API. ListAttacks

AWS Shield Advanced rincian acara

Anda dapat melihat detail tentang deteksi, mitigasi, dan kontributor teratas peristiwa di bagian bawah halaman konsol untuk acara tersebut. Bagian ini dapat mencakup campuran lalu lintas yang sah dan berpotensi tidak diinginkan, dan dapat mewakili lalu lintas yang diteruskan ke sumber daya yang dilindungi dan lalu lintas yang diblokir oleh mitigasi Shield.

- Deteksi dan mitigasi — Memberikan informasi tentang peristiwa yang diamati dan mitigasi yang diterapkan terhadapnya. Untuk informasi tentang mitigasi acara, lihat. Menanggapi peristiwa DDoS
- Kontributor teratas — Mengkategorikan lalu lintas yang terlibat dalam acara tersebut, dan mencantumkan sumber utama lalu lintas yang telah diidentifikasi Shield untuk setiap kategori. Untuk peristiwa lapisan aplikasi, gunakan informasi kontributor teratas untuk mendapatkan gambaran umum tentang sifat suatu peristiwa, tetapi gunakan AWS WAF log untuk keputusan keamanan Anda. Untuk informasi selengkapnya, lihat bagian berikut.

Informasi acara Anda di konsol Shield Advanced didasarkan pada metrik Shield Advanced. Untuk informasi tentang metrik Shield Advanced, lihat AWS Shield Advanced metrik

Metrik mitigasi tidak disertakan untuk sumber daya Amazon atau CloudFront Amazon Route 53, karena layanan ini dilindungi oleh sistem mitigasi yang selalu diaktifkan dan tidak memerlukan mitigasi untuk sumber daya individual.

Bagian detail bervariasi sesuai dengan apakah informasi tersebut untuk lapisan infrastruktur atau peristiwa lapisan aplikasi.

Detail acara lapisan aplikasi

Anda dapat melihat detail tentang deteksi, mitigasi, dan kontributor teratas peristiwa lapisan aplikasi di bagian bawah halaman konsol untuk acara tersebut. Bagian ini dapat mencakup campuran lalu lintas yang sah dan berpotensi tidak diinginkan, dan dapat mewakili lalu lintas yang diteruskan ke sumber daya yang dilindungi dan lalu lintas yang diblokir oleh mitigasi Shield Advanced.

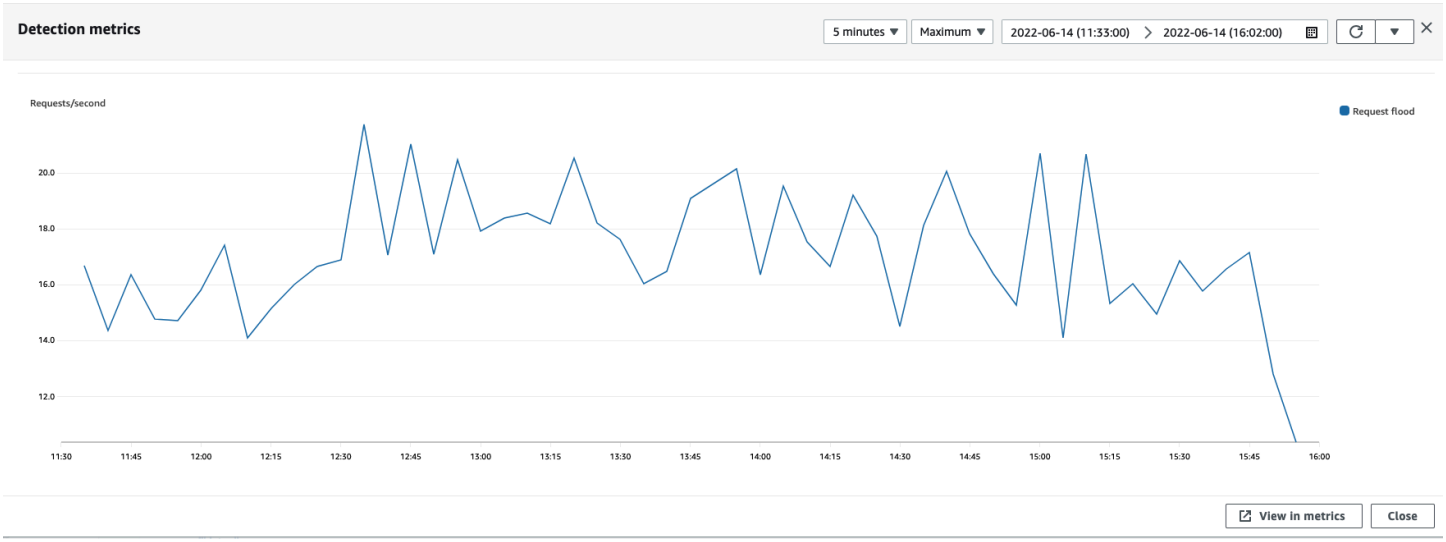
Detail mitigasi adalah untuk aturan apa pun di ACL web yang terkait dengan sumber daya, termasuk aturan yang diterapkan secara khusus sebagai respons terhadap serangan dan aturan berbasis kecepatan yang didefinisikan dalam ACL web. Jika Anda mengaktifkan mitigasi DDoS lapisan aplikasi otomatis untuk aplikasi, metrik mitigasi menyertakan metrik untuk aturan tambahan tersebut. Untuk informasi tentang perlindungan lapisan aplikasi ini, lihatAWS Shield Advanced perlindungan lapisan aplikasi (lapisan 7).

Deteksi dan mitigasi

Untuk peristiwa lapisan aplikasi (lapisan 7), tab Deteksi dan mitigasi menunjukkan metrik deteksi yang didasarkan pada informasi yang diperoleh dari log. AWS WAF Metrik mitigasi didasarkan pada AWS WAF aturan di ACL web terkait yang dikonfigurasi untuk memblokir lalu lintas yang tidak diinginkan.

Untuk CloudFront distribusi Amazon, Anda dapat mengonfigurasi Shield Advanced untuk menerapkan mitigasi otomatis untuk Anda. Dengan sumber daya lapisan aplikasi apa pun, Anda dapat memilih untuk menentukan aturan mitigasi Anda sendiri di ACL web Anda dan Anda dapat meminta bantuan dari Tim Respons Shield (SRT). Untuk informasi tentang opsi ini, lihat Menanggapi peristiwa DDoS.

Tangkapan layar berikut menunjukkan contoh metrik deteksi untuk peristiwa lapisan aplikasi yang mereda setelah beberapa jam.



Lalu lintas peristiwa yang mereda sebelum aturan mitigasi berlaku tidak direpresentasikan dalam metrik mitigasi. Hal ini dapat menyebabkan perbedaan antara lalu lintas permintaan web yang ditampilkan dalam grafik deteksi dan metrik izinkan dan blok yang ditunjukkan dalam grafik mitigasi.

Kontributor teratas

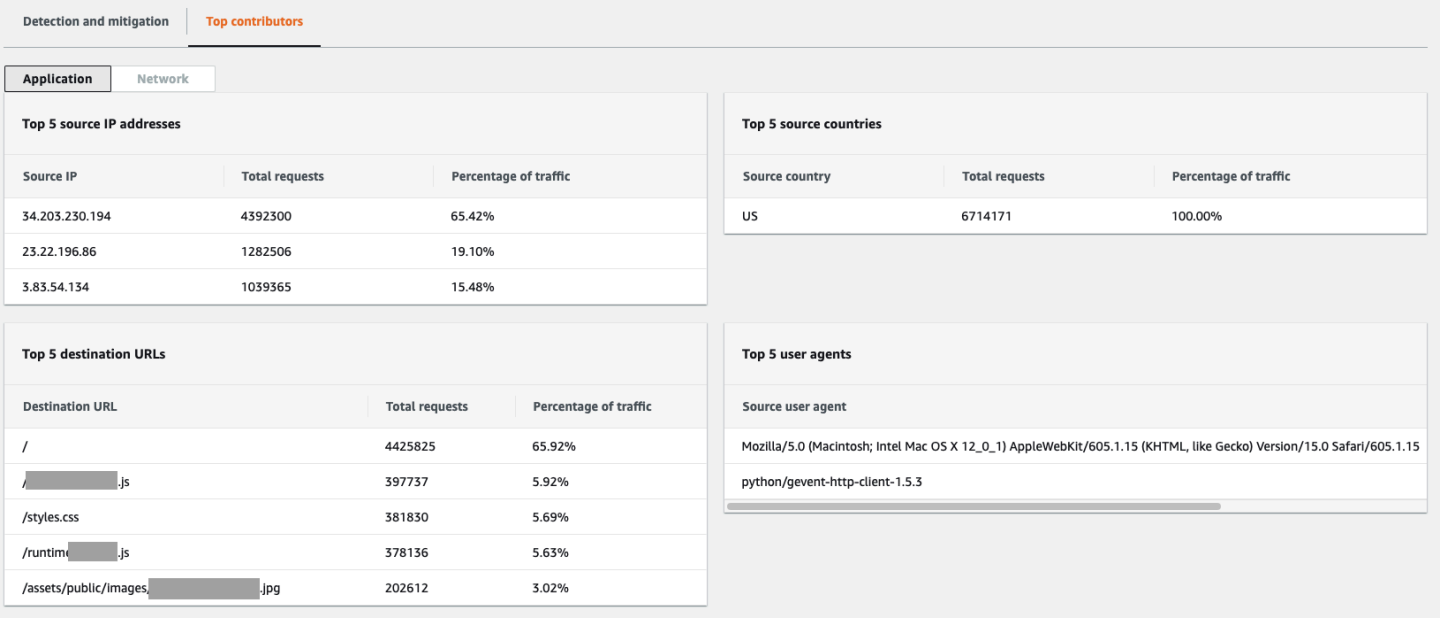
Tab kontributor teratas untuk peristiwa lapisan aplikasi menampilkan 5 kontributor teratas yang telah diidentifikasi Shield untuk acara tersebut, berdasarkan log AWS WAF yang telah diambil. Shield mengkategorikan informasi kontributor teratas berdasarkan dimensi seperti IP sumber, negara sumber, dan URL tujuan.

> **Note**
>
> Untuk informasi paling akurat tentang lalu lintas yang berkontribusi pada peristiwa lapisan aplikasi, gunakan AWS WAF log.

Gunakan informasi kontributor teratas lapisan aplikasi Shield hanya untuk mendapatkan gambaran umum tentang sifat serangan, dan jangan mendasarkan keputusan keamanan Anda padanya. Untuk peristiwa lapisan aplikasi, AWS WAF log adalah sumber informasi terbaik untuk memahami kontributor serangan dan untuk merancang strategi mitigasi Anda.

Informasi kontributor teratas Shield tidak selalu sepenuhnya mencerminkan data dalam log. AWS WAF Saat menyerap log, Shield memprioritaskan pengurangan dampak terhadap kinerja sistem daripada mengambil kumpulan data lengkap dari log. Hal ini dapat mengakibatkan hilangnya granularitas dalam data yang tersedia untuk Shield untuk analisis. Dalam kebanyakan kasus, sebagian besar informasi tersedia, tetapi mungkin saja data kontributor teratas condong ke tingkat tertentu untuk serangan apa pun.

Tangkapan layar berikut menunjukkan contoh tab Kontributor teratas untuk acara lapisan aplikasi.



Informasi kontributor didasarkan pada permintaan untuk lalu lintas yang sah dan berpotensi tidak diinginkan. Peristiwa volume yang lebih besar dan peristiwa di mana sumber permintaan tidak didistribusikan secara tinggi cenderung memiliki kontributor teratas yang dapat diidentifikasi. Serangan yang didistribusikan secara signifikan dapat memiliki sejumlah sumber, sehingga sulit untuk mengidentifikasi kontributor utama serangan tersebut. Jika Shield Advanced tidak mengidentifikasi kontributor signifikan untuk kategori tertentu, Shield Advanced akan menampilkan data sebagai tidak tersedia.

Detail peristiwa lapisan infrastruktur

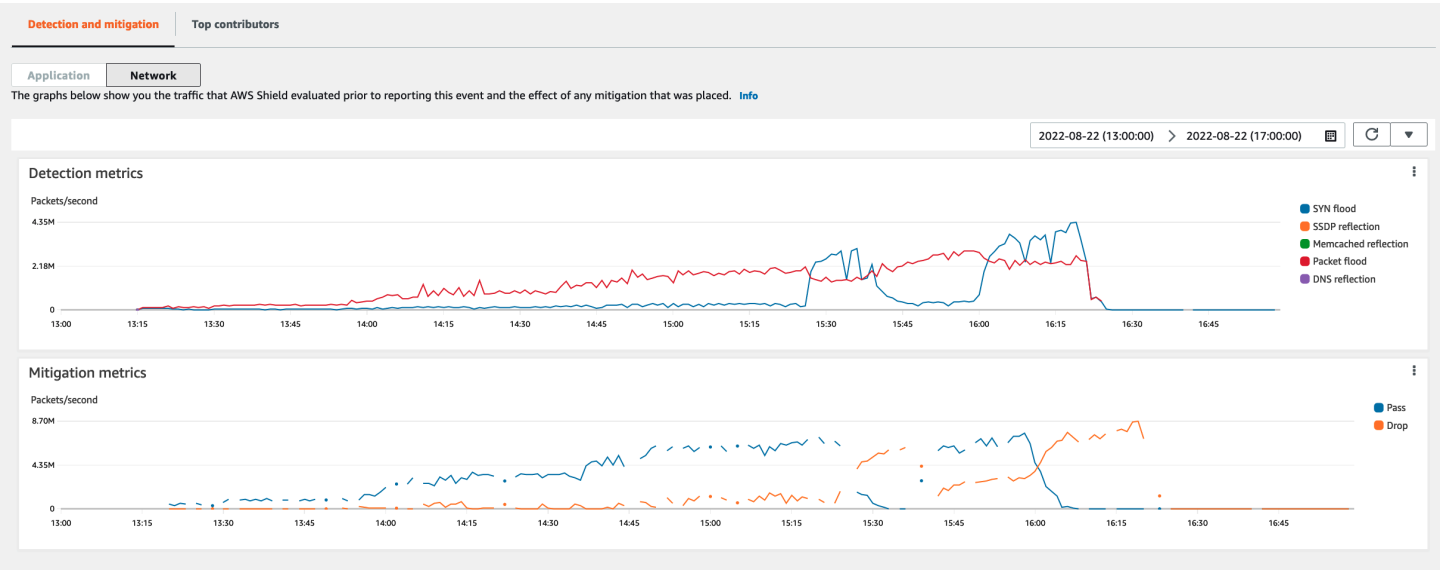
Anda dapat melihat detail tentang deteksi, mitigasi, dan kontributor teratas peristiwa lapisan infrastruktur di bagian bawah halaman konsol untuk acara tersebut. Bagian ini dapat mencakup campuran lalu lintas yang sah dan berpotensi tidak diinginkan, dan dapat mewakili lalu lintas yang diteruskan ke sumber daya yang dilindungi dan lalu lintas yang diblokir oleh mitigasi Shield.

Deteksi dan mitigasi

Untuk peristiwa lapisan infrastruktur (lapisan 3 atau 4), tab Deteksi dan mitigasi menunjukkan metrik deteksi yang didasarkan pada aliran jaringan sampel dan metrik mitigasi yang didasarkan pada lalu lintas yang diamati oleh sistem mitigasi. Metrik mitigasi adalah pengukuran lalu lintas yang lebih tepat ke sumber daya Anda.

Shield secara otomatis membuat mitigasi untuk jenis sumber daya yang dilindungi Elastic IP (EIP), Classic Load Balancer (CLB), Application Load Balancer (ALB), dan akselerator standar. AWS Global Accelerator Metrik mitigasi untuk alamat EIP dan akselerator AWS Global Accelerator standar menunjukkan jumlah paket yang dilewatkan dan dijatuhkan.

Tangkapan layar berikut menunjukkan contoh Deteksi dan mitigasi tab untuk peristiwa lapisan infrastruktur.

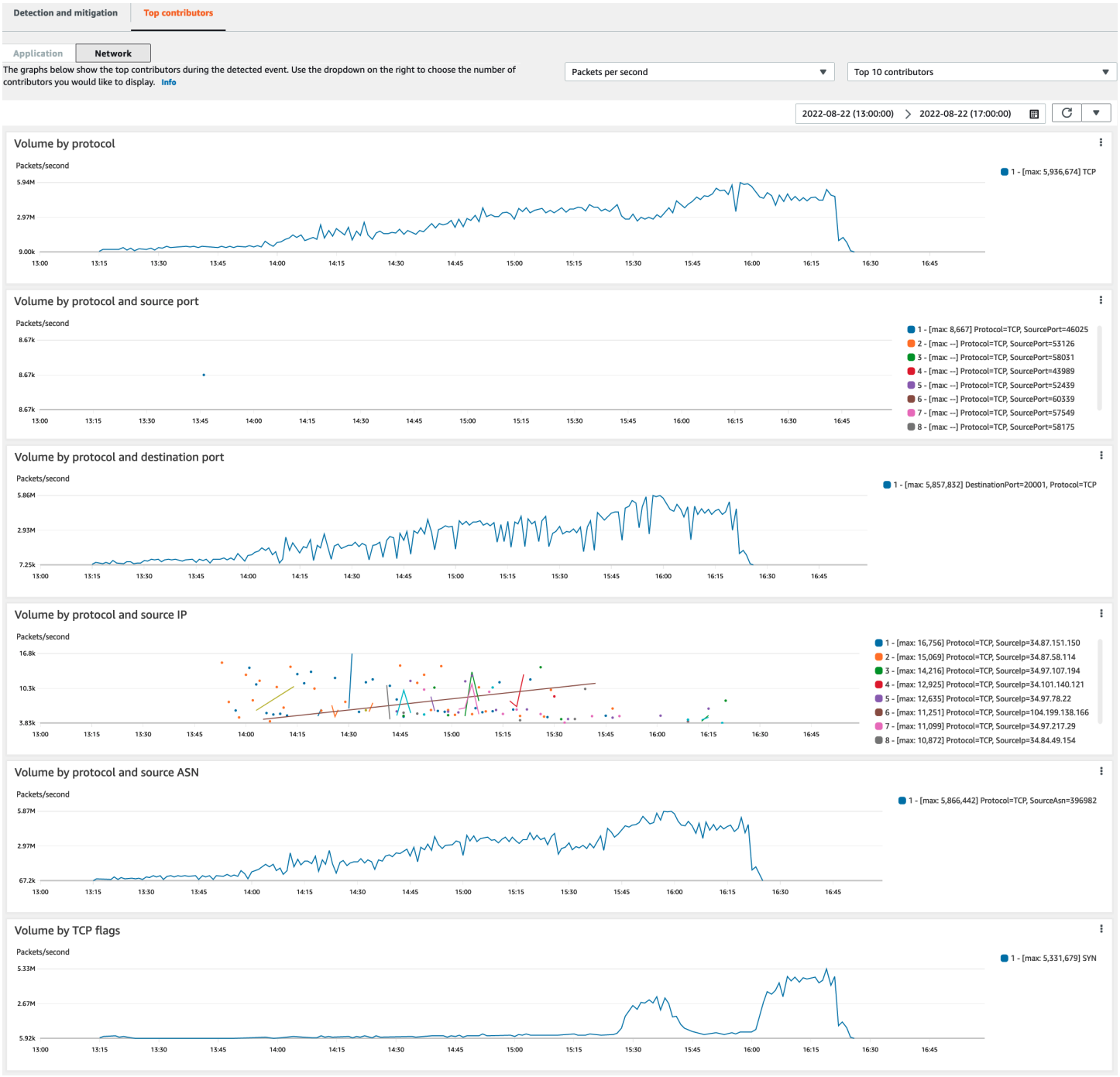


Lalu lintas peristiwa yang mereda sebelum Shield menempatkan mitigasi tidak direpresentasikan dalam metrik mitigasi. Hal ini dapat menyebabkan perbedaan antara lalu lintas yang ditunjukkan dalam grafik deteksi dan metrik pass and drop yang ditunjukkan dalam grafik mitigasi.

Kontributor teratas

Tab kontributor teratas untuk peristiwa lapisan infrastruktur mencantumkan metrik hingga 100 kontributor teratas pada beberapa dimensi lalu lintas. Rinciannya mencakup properti lapisan jaringan untuk dimensi apa pun di mana setidaknya lima sumber lalu lintas yang signifikan dapat diidentifikasi. Contoh sumber lalu lintas adalah sumber IP dan sumber ASN.

Tangkapan layar berikut menunjukkan contoh tab Kontributor teratas untuk peristiwa lapisan infrastruktur.



Metrik kontributor didasarkan pada aliran jaringan sampel untuk lalu lintas yang sah dan berpotensi tidak diinginkan. Peristiwa volume yang lebih besar dan peristiwa di mana sumber lalu lintas tidak didistribusikan sangat mungkin memiliki kontributor teratas yang dapat diidentifikasi. Serangan yang didistribusikan secara signifikan dapat memiliki sejumlah sumber, sehingga sulit untuk mengidentifikasi kontributor utama serangan tersebut. Jika Shield tidak mengidentifikasi kontributor signifikan untuk metrik atau kategori tertentu, Shield akan menampilkan data sebagai tidak tersedia.

Dalam serangan DDoS lapisan infrastruktur, sumber lalu lintas mungkin dipalsukan atau dipantulkan. Sumber palsu sengaja dipalsukan oleh penyerang. Sumber yang dipantulkan adalah sumber nyata dari lalu lintas yang terdeteksi, tetapi itu bukan peserta yang bersedia dalam serangan itu. Misalnya, penyerang mungkin menghasilkan banjir lalu lintas yang besar dan diperkuat ke target dengan mencerminkan serangan layanan di internet yang biasanya sah. Dalam hal ini, informasi sumber mungkin valid sementara itu bukan sumber serangan yang sebenarnya. Faktor-faktor ini dapat membatasi kelangsungan hidup teknik mitigasi yang memblokir sumber berdasarkan header paket.

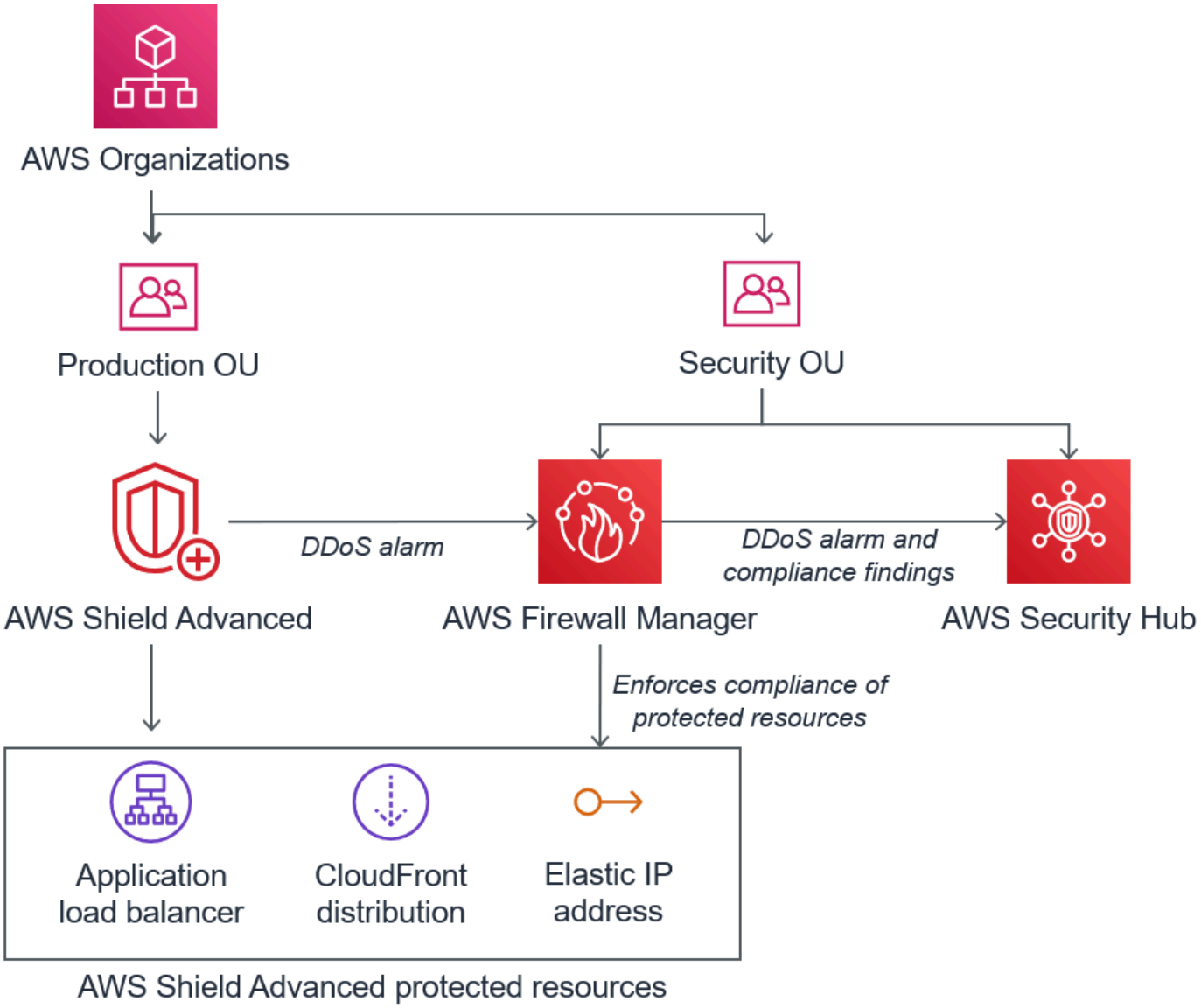
Visibilitas acara di seluruh akun

Anda dapat menggunakan AWS Firewall Manager dan AWS Security Hub mengelola dan memantau sumber daya yang AWS Shield Advanced dilindungi di beberapa akun.

Dengan Firewall Manager, Anda dapat membuat kebijakan keamanan Shield Advanced yang melaporkan dan memberlakukan kepatuhan perlindungan DDoS di semua akun Anda. Firewall Manager memantau sumber daya Anda yang dilindungi, termasuk menambahkan perlindungan ke sumber daya baru yang masuk ke dalam cakupan kebijakan Shield Advanced.

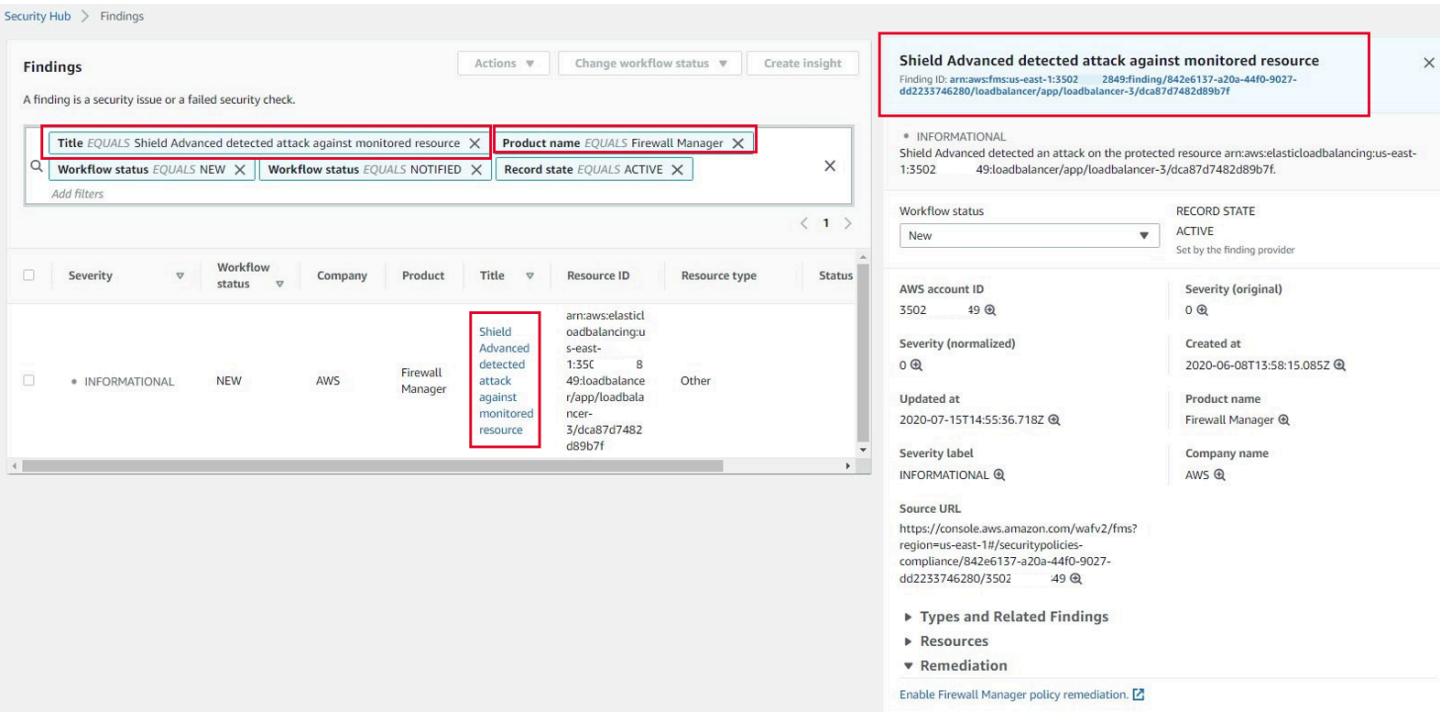
Anda dapat mengintegrasikan Firewall Manager AWS Security Hub untuk mendapatkan satu dasbor yang melaporkan peristiwa DDoS yang terdeteksi oleh temuan kepatuhan Shield Advanced dan Firewall Manager, saat Firewall Manager mengidentifikasi sumber daya yang tidak sesuai dengan kebijakan keamanan Shield Advanced Anda.

Gambar berikut menggambarkan arsitektur khas untuk memantau sumber daya yang dilindungi Shield Advanced dengan Firewall Manager dan Security Hub.



Saat mengintegrasikan Firewall Manager dengan Security Hub, Anda dapat melihat temuan keamanan di satu tempat, di samping peringatan dan informasi status kepatuhan lainnya untuk aplikasi yang Anda jalankan. AWS

Tangkapan layar berikut menyoroti informasi yang dapat Anda lihat untuk acara Shield Advanced di dalam konsol Security Hub saat Anda memiliki integrasi jenis ini.



Untuk mempelajari cara mengintegrasikan Firewall Manager dan Security Hub dengan Shield Advanced untuk memusatkan pemantauan peristiwa dan kepatuhan di seluruh akun Anda yang dilindungi, lihat blog AWS keamanan Mengatur pemantauan terpusat untuk peristiwa DDoS dan memulihkan sumber daya yang tidak sesuai secara otomatis.

Menanggapi peristiwa DDoS

AWS secara otomatis mengurangi serangan jaringan dan transport layer (layer 3 dan layer 4) Distributed Denial of Service (DDoS). Jika Anda menggunakan Shield Advanced untuk melindungi instans Amazon EC2, selama serangan Shield Advanced secara otomatis menyebarkan ACL jaringan VPC Amazon Anda ke perbatasan jaringan. AWS Hal ini memungkinkan Shield Advanced untuk memberikan perlindungan terhadap peristiwa DDoS yang lebih besar. Untuk informasi selengkapnya tentang ACL jaringan, lihat ACL jaringan.

Untuk lapisan aplikasi (lapisan 7) serangan DDoS, AWS upaya untuk mendeteksi dan memberi tahu AWS Shield Advanced pelanggan melalui CloudWatch alarm. Secara default, itu tidak secara otomatis menerapkan mitigasi, untuk menghindari pemblokiran lalu lintas pengguna yang valid secara tidak sengaja.

Untuk sumber daya lapisan aplikasi (lapisan 7), Anda memiliki opsi berikut yang tersedia untuk merespons serangan.

- Berikan mitigasi Anda sendiri — Anda dapat menyelidiki dan mengurangi serangan Anda sendiri. Untuk informasi, lihat Memitigasi serangan DDoS lapisan aplikasi secara manual.
- Hubungi dukungan — Jika Anda adalah pelanggan Shield Advanced, Anda dapat menghubungi AWS Support Pusat untuk mendapatkan bantuan terkait mitigasi. Kasus kritis dan mendesak diarahkan langsung ke ahli DDoS. Untuk informasi, lihat Menghubungi pusat dukungan selama serangan DDoS lapisan aplikasi.

Selain itu, sebelum serangan terjadi, Anda dapat secara proaktif mengaktifkan opsi mitigasi berikut:

- Mitigasi otomatis pada CloudFront distribusi Amazon — Dengan opsi ini, Shield Advanced mendefinisikan dan mengelola aturan mitigasi untuk Anda di ACL web Anda. Untuk informasi tentang mitigasi lapisan aplikasi otomatis, lihat. Mitigasi DDoS lapisan aplikasi otomatis Shield Advanced
- Keterlibatan proaktif — Ketika AWS Shield Advanced mendeteksi serangan lapisan aplikasi besar terhadap salah satu aplikasi Anda, SRT dapat secara proaktif menghubungi Anda. SRT melakukan triase acara DDoS dan menciptakan mitigasi. AWS WAF SRT menghubungi Anda dan, dengan persetujuan Anda, dapat menerapkan AWS WAF aturan. Untuk informasi selengkapnya tentang metrik ini, lihat Mengkonfigurasi keterlibatan proaktif.

Menghubungi pusat dukungan selama serangan DDoS lapisan aplikasi

Jika Anda seorang AWS Shield Advanced pelanggan, Anda dapat menghubungi AWS Support Pusat untuk mendapatkan bantuan terkait mitigasi. Kasus kritis dan mendesak diarahkan langsung ke ahli DDoS. Dengan AWS Shield Advanced, kasus kompleks dapat ditingkatkan ke AWS Shield Response Team (SRT), yang memiliki pengalaman mendalam dalam melindungi, Amazon.com AWS, dan anak perusahaannya. Untuk informasi lebih lanjut tentang SRT, lihatDukungan Shield Response Team (SRT).

Untuk mendapatkan dukungan Shield Response Team (SRT), hubungi AWS Support Pusat. Waktu respons untuk kasus Anda bergantung pada tingkat keparahan yang Anda pilih dan waktu respons, yang didokumentasikan pada halaman AWS Support Paket.

Pilih opsi berikut:

- Jenis kasus: Technical Support
- Layanan: Distributed Denial of Service (DDoS)
- Kategori: Inbound ke AWS

- Keparahan: Pilih opsi yang sesuai

Saat berdiskusi dengan perwakilan kami, jelaskan bahwa Anda adalah AWS Shield Advanced pelanggan yang mengalami kemungkinan serangan DDoS. Perwakilan kami akan mengarahkan panggilan Anda ke ahli DDoS yang sesuai. Jika Anda membuka kasus dengan AWS Support Center menggunakan jenis layanan Distributed Denial of Service (DDoS), Anda dapat berbicara langsung dengan pakar DDoS melalui obrolan atau telepon. Insinyur dukungan DDoS dapat membantu Anda mengidentifikasi serangan, merekomendasikan perbaikan AWS arsitektur Anda, dan memberikan panduan dalam penggunaan AWS layanan untuk mitigasi serangan DDoS.

Untuk serangan lapisan aplikasi, SRT dapat membantu Anda menganalisis aktivitas yang mencurigakan. Jika Anda mengaktifkan mitigasi otomatis untuk sumber daya Anda, SRT dapat meninjau mitigasi yang secara otomatis ditempatkan Shield Advanced terhadap serangan tersebut. Bagaimanapun, SRT dapat membantu Anda meninjau dan mengurangi masalah. Mitigasi yang direkomendasikan SRT sering memerlukan SRT untuk membuat atau memperbarui daftar kontrol akses AWS WAF web (ACL web) di akun Anda. SRT akan membutuhkan izin Anda untuk melakukan pekerjaan ini.

> **Important**
>
> Kami menyarankan bahwa sebagai bagian dari mengaktifkan AWS Shield Advanced, Anda mengikuti langkah-langkah Mengkonfigurasi akses untuk Shield Response Team (SRT) untuk secara proaktif memberikan SRT dengan izin yang mereka butuhkan untuk membantu Anda selama serangan. Memberikan izin sebelumnya membantu mencegah penundaan jika terjadi serangan yang sebenarnya.

SRT membantu Anda melakukan triase serangan DDoS untuk mengidentifikasi tanda tangan dan pola serangan. Dengan persetujuan Anda, SRT membuat dan menyebarkan AWS WAF aturan untuk mengurangi serangan.

Anda juga dapat menghubungi SRT sebelum atau selama kemungkinan serangan untuk meninjau mitigasi dan mengembangkan dan menerapkan mitigasi khusus. Misalnya, jika Anda menjalankan aplikasi web dan hanya membutuhkan port 80 dan 443 terbuka, Anda dapat bekerja dengan SRT untuk mengkonfigurasi ACL web untuk “mengizinkan” hanya port 80 dan 443.

Anda mengotorisasi dan menghubungi SRT di tingkat akun. Artinya, jika Anda menggunakan Shield Advanced dalam kebijakan Firewall Manager Shield Advanced, pemilik akun, bukan administrator

Firewall Manager, harus menghubungi SRT untuk mendapatkan dukungan. Administrator Firewall Manager dapat menghubungi SRT hanya untuk akun yang mereka miliki.

Memitigasi serangan DDoS lapisan aplikasi secara manual

Jika Anda menentukan bahwa aktivitas di halaman peristiwa untuk sumber daya Anda mewakili serangan DDoS, Anda dapat membuat AWS WAF aturan sendiri di ACL web Anda untuk mengurangi serangan. Ini adalah satu-satunya pilihan yang tersedia jika Anda bukan pelanggan Shield Advanced. AWS WAF sudah termasuk tanpa AWS Shield Advanced biaya tambahan. Untuk informasi tentang membuat aturan di ACL web Anda, lihatAWS WAF daftar kontrol akses web (ACL web).

Jika Anda menggunakan AWS Firewall Manager, Anda dapat menambahkan AWS WAF aturan Anda ke AWS WAF kebijakan Firewall Manager.

Untuk secara manual mengurangi potensi serangan lapisan aplikasi DDoS

1. Buat pernyataan aturan di ACL web Anda dengan kriteria yang cocok dengan perilaku yang tidak biasa. Untuk memulainya, konfigurasikan mereka untuk menghitung permintaan yang cocok. Untuk informasi tentang mengonfigurasi ACL web dan pernyataan aturan, lihat Evaluasi aturan dan kelompok aturan ACL Web dan. Menguji dan menyetel perlindungan Anda AWS WAF

   > **Note**
   >
   > Selalu uji aturan Anda terlebih dahulu dengan awalnya menggunakan tindakan aturan Count alih-alihBlock. Setelah Anda merasa nyaman bahwa aturan baru Anda mengidentifikasi permintaan yang benar, Anda dapat memodifikasinya untuk memblokir permintaan.

2. Pantau jumlah permintaan untuk menentukan apakah Anda ingin memblokir permintaan yang cocok. Jika volume permintaan terus sangat tinggi dan Anda yakin bahwa aturan Anda menangkap permintaan yang menyebabkan volume tinggi, ubah aturan di ACL web Anda untuk memblokir permintaan.
3. Lanjutkan memantau halaman acara untuk memastikan bahwa lalu lintas Anda ditangani seperti yang Anda inginkan.

AWS menyediakan template yang telah dikonfigurasi untuk membantu Anda memulai dengan cepat. Template mencakup seperangkat AWS WAF aturan yang dapat Anda sesuaikan dan gunakan untuk

memblokir serangan berbasis web yang umum. Untuk informasi selengkapnya, lihat Otomasi AWS WAF Keamanan.

Meminta kredit di AWS Shield Advanced

Jika Anda berlangganan AWS Shield Advanced dan mengalami serangan DDoS yang meningkatkan pemanfaatan sumber daya yang dilindungi Shield Advanced, Anda dapat meminta kredit layanan Shield Advanced untuk biaya yang terkait dengan peningkatan pemanfaatan, sejauh tidak dikurangi oleh Shield Advanced.

> **Note**
>
> Anda dapat menerapkan kredit apa pun yang diterima melalui proses ini hanya untuk penggunaan Shield Advanced. Kredit Shield Advanced tidak tersedia untuk digunakan dengan layanan lain.

Kredit hanya tersedia untuk jenis biaya berikut:

- Shield Transfer data lanjutan keluar
- Permintaan Amazon CloudFront HTTP/HTTPS
- CloudFront transfer data keluar
- Kueri Amazon Route 53
- AWS Global Accelerator transfer data akselerator standar
- Unit kapasitas penyeimbang beban untuk Application Load Balancer
- Biaya instans untuk instans Amazon Elastic Compute Cloud (Amazon EC2) yang dilindungi yang dibuat oleh kebijakan auto-scaling sebagai respons terhadap serangan

Prasyarat untuk meminta kredit

Agar memenuhi syarat untuk menerima kredit, sebelum serangan dimulai, Anda harus melakukan hal berikut:

- Anda harus menambahkan perlindungan Shield Advanced ke sumber daya yang ingin Anda minta kreditnya. Sumber daya yang dilindungi yang ditambahkan selama serangan tidak memenuhi syarat untuk perlindungan biaya.

> **Note**
>
> Mengaktifkan Shield Advanced pada Anda Akun AWS tidak secara otomatis mengaktifkan perlindungan Shield Advanced untuk sumber daya individu.

Untuk informasi selengkapnya tentang cara melindungi AWS sumber daya menggunakan Shield Advanced, lihatMenambahkan AWS Shield Advanced perlindungan ke AWS sumber daya.

- Untuk sumber daya yang berlaku CloudFront dan Application Load Balancer yang dilindungi, Anda harus mengaitkan ACL AWS WAF web dan menerapkan aturan berbasis tarif di ACL web dalam mode. Block Untuk informasi tentang AWS WAF aturan berbasis tarif, lihat. Pernyataan aturan berbasis tarif Untuk informasi tentang cara mengaitkan ACL web dengan AWS sumber daya, lihatAWS WAF daftar kontrol akses web (ACL web).
- Anda harus telah menerapkan praktik terbaik yang sesuai dalam Praktik AWS Terbaik untuk Ketahanan DDoS untuk mengonfigurasi aplikasi Anda dengan cara yang meminimalkan biaya selama serangan DDoS.

Cara mengajukan kredit

Agar memenuhi syarat untuk kredit, Anda harus mengirimkan permintaan kredit Anda dalam jangka waktu 15 hari segera setelah bulan penagihan di mana serangan terjadi.

Untuk mengajukan kredit, kirimkan kasus penagihan melalui AWS Support Pusat. Sertakan yang berikut ini dalam permintaan Anda:

- Kata-kata “Konsesi DDoS” di baris subjek
- Tanggal dan waktu setiap acara atau gangguan ketersediaan yang Anda minta kredit
- AWS Layanan dan sumber daya spesifik yang terpengaruh

Setelah Anda mengirimkan permintaan, AWS Shield Response Team (SRT) akan memvalidasi apakah serangan DDoS terjadi dan, jika demikian, apakah ada sumber daya yang dilindungi yang diskalakan untuk menyerap serangan DDoS. Jika AWS menentukan bahwa sumber daya yang dilindungi diskalakan untuk menyerap serangan DDoS, AWS akan mengeluarkan kredit untuk bagian lalu lintas yang AWS menentukan disebabkan oleh serangan DDoS. Kredit berlaku selama 12 bulan.

Keamanan dalam penggunaan AWS Shield layanan Anda

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

> **Note**
>
> Bagian ini memberikan panduan AWS keamanan standar untuk penggunaan Anda atas AWS Shield layanan dan AWS sumber dayanya, seperti perlindungan Shield Advanced. Untuk informasi tentang melindungi AWS sumber daya Anda menggunakan Shield dan Shield Advanced, lihat AWS Shield panduan lainnya.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan dari cloud dan keamanan di cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Efektivitas keamanan kami diuji dan diverifikasi secara rutin oleh auditor pihak ketiga sebagai bagian dari program kepatuhan AWS. Untuk mempelajari tentang program kepatuhan yang berlaku untuk Shield, lihat AWS Layanan dalam Lingkup berdasarkan Program Kepatuhan.
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor-faktor lain termasuk sensitivitas data Anda, persyaratan organisasi Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Shield. Topik berikut menunjukkan cara mengonfigurasi Shield untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Shield Anda.

Topik

- Ketahanan dalam Shield
- Keamanan infrastruktur dalam AWS Shield

Perlindungan data di Shield

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di AWS Shield. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensyal dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi yang lebih lengkap tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Shield atau lainnya Layanan AWS

menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Entitas Shield — seperti proteksi — dienkripsi saat istirahat, kecuali di Wilayah tertentu di mana enkripsi tidak tersedia, termasuk China (Beijing) dan China (Ningxia). Kunci enkripsi unik digunakan untuk setiap Wilayah.

Manajemen identitas dan akses untuk AWS Shield

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Shield. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Shield.

Pengguna layanan — Jika Anda menggunakan layanan Shield untuk melakukan pekerjaan Anda, administrator Anda memberi Anda kredensyal dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur Shield untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang

tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Shield, lihatMemecahkan masalah AWS Shield identitas dan akses.

Administrator layanan — Jika Anda bertanggung jawab atas sumber daya Shield di perusahaan Anda, Anda mungkin memiliki akses penuh ke Shield. Tugas Anda adalah menentukan fitur dan sumber daya Shield mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep Basic IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan Shield, lihatBagaimana AWS Shield bekerja dengan IAM.

Administrator IAM - Jika Anda administrator IAM, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Shield. Untuk melihat contoh kebijakan berbasis identitas Shield yang dapat Anda gunakan di IAM, lihat. Contoh kebijakan berbasis identitas untuk AWS Shield

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensyal identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensyal yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensyal Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensyal Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Menandatangani permintaan AWS API di Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat Autentikasi multi-faktor dalam Panduan Pengguna AWS IAM Identity Center dan Menggunakan autentikasi multi-faktor (MFA) dalam AWS dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensyal sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensi yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensyal sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat Apakah itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial

sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup yang bernama IAMAdmins dan memberikan izin ke grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat Kapan harus membuat pengguna IAM (bukan peran) dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil peran IAM untuk sementara AWS Management Console dengan beralih peran. Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat Menggunakan peran IAM dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.

- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Sebagai contoh, ketika Anda memanggil suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.
  - Peran layanan – Peran layanan adalah peran IAM yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
  - Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada instans EC2 dan membuat atau permintaan API. AWS CLI AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara.

Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan dalam instans Amazon EC2 dalam Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, lihat Kapan harus membuat peran IAM (bukan pengguna) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasinya. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan

terkelola adalah kebijakan mandiri yang dapat dilampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan yang dikelola atau kebijakan inline, lihat Memilih antara kebijakan yang dikelola dan kebijakan inline dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Daftar kontrol akses (ACL)

Daftar kontrol akses (ACL) mengendalikan prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, lihat Gambaran umum daftar kontrol akses (ACL) dalam Panduan Developer Amazon Simple Storage Service.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber

daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.

- Kebijakan kontrol layanan (SCP) — SCP adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur di organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organisasi dan SCP, lihat Cara kerja SCP dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Bagaimana AWS Shield bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Shield, pelajari fitur IAM yang tersedia untuk digunakan dengan Shield.

Fitur IAM yang dapat Anda gunakan dengan AWS Shield

Fitur IAM	Dukungan Shield
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak

Fitur IAM	Dukungan Shield
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Ya
ACL	Tidak
ABAC (tanda dalam kebijakan)	Parsial
Kredensial sementara	Ya
Sesi akses teruskan (FAS)	Ya
Peran layanan	Ya
Peran terkait layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Shield dan AWS layanan lainnya dengan sebagian besar fitur IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk Shield

Mendukung kebijakan berbasis identitas	Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan

berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Untuk melihat contoh kebijakan berbasis identitas Shield, lihat. Contoh kebijakan berbasis identitas untuk AWS Shield

Kebijakan berbasis sumber daya dalam Shield

Mendukung kebijakan berbasis sumber daya	Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai prinsipal dalam kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, administrator IAM di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke prinsipal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

Tindakan kebijakan untuk Shield

Mendukung tindakan kebijakan	Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar tindakan Shield, lihat Tindakan yang ditentukan oleh AWS Shield dalam Referensi Otorisasi Layanan.

Tindakan kebijakan di Shield menggunakan awalan berikut sebelum tindakan:

```
shield
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

```
"Action": [
      "shield:action1",
      "shield:action2"
         ]
```

Anda juga dapat menentukan beberapa tindakan menggunakan wildcard (*). Misalnya, untuk menentukan semua tindakan di Shield yang dimulai`List`, sertakan tindakan berikut:

```
"Action": "shield:List*"
```

Untuk melihat contoh kebijakan berbasis identitas Shield, lihat. Contoh kebijakan berbasis identitas untuk AWS Shield

Sumber daya kebijakan untuk Shield

Mendukung sumber daya kebijakan	Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Untuk melihat daftar jenis sumber daya Shield dan ARNnya, lihat Sumber daya yang ditentukan oleh AWS Shield dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan yang dapat menentukan ARN setiap sumber daya, lihat Tindakan yang ditentukan AWS Shield. Untuk mengizinkan atau menolak akses ke subset sumber daya Shield, sertakan ARN sumber daya dalam elemen `resource` kebijakan Anda.

Di AWS Shield, sumber daya adalah perlindungan dan serangan. Sumber daya ini memiliki Amazon Resource Name (ARN) yang unik dan terkait dengan sumber daya, seperti yang ditunjukkan di tabel berikut.

Nama di AWS Shield Konsol	Nama dalam AWS Shield SDK/CLI	Format ARN
Peristiwa atau serangan	`AttackDetail`	`arn:aws:shield:: account:attack/ID`
Perlindungan	`Protection`	`arn:aws:shield:: account:protection/ ID`

Untuk mengizinkan atau menolak akses ke subset sumber daya Shield, sertakan ARN sumber daya dalam elemen `resource` kebijakan Anda. ARN untuk Shield memiliki format berikut:

```
arn:partition:shield::account:resource/ID
```

Ganti *akun*, *sumber daya*, dan variabel *ID* dengan nilai yang valid. Nilai yang valid dapat berupa sebagai berikut:

- *akun*: ID Anda Akun AWS. Anda harus menentukan nilai.
- *sumber daya*: Jenis sumber daya Shield, baik `attack` atau`protection`.
- *ID*: ID sumber daya Shield, atau wildcard (*) untuk menunjukkan semua sumber daya dari jenis tertentu yang terkait dengan yang ditentukan Akun AWS.

Misalnya, ARN berikut menentukan semua perlindungan untuk akun: `111122223333`

```
arn:aws:shield::111122223333:protection/*
```

Sumber daya ARN of Shield memiliki format berikut:

```
arn:partition:shield:region:account-id:scope/resource-type/resource-name/resource-id
```

Untuk informasi umum tentang spesifikasi ARN, lihat Nama Sumber Daya Amazon (ARN) di. Referensi Umum Amazon Web Services

Berikut daftar persyaratan yang khusus untuk ARN `wafv2` sumber daya:

- *region*: Untuk sumber daya Shield yang Anda gunakan untuk melindungi CloudFront distribusi Amazon, setel ini ke`us-east-1`. Jika tidak, atur ini ke Wilayah yang Anda gunakan dengan sumber daya regional yang dilindungi.
- *scope*: Tetapkan cakupan `global` untuk digunakan dengan CloudFront distribusi Amazon atau `regional` untuk digunakan dengan sumber daya regional mana pun yang AWS WAF mendukung. Sumber daya regional adalah Amazon API Gateway REST API, Application Load Balancer, GraphQL API AWS AppSync , kumpulan pengguna Amazon Cognito, layanan, dan instance Akses Terverifikasi. AWS App Runner AWS
- *resource-type*: Tentukan salah satu nilai berikut: `attack` untuk peristiwa atau serangan, untuk perlindungan. `protection`
- *resource-name*: Tentukan nama yang Anda berikan pada resource Shield, atau tentukan wildcard (*) untuk menunjukkan semua resource yang memenuhi spesifikasi lain di ARN. Anda harus menentukan nama sumber daya dan ID sumber daya atau menentukan wildcard untuk keduanya.

- *resource-id*: Tentukan ID sumber daya Shield, atau tentukan wildcard (*) untuk menunjukkan semua sumber daya yang memenuhi spesifikasi lain di ARN. Anda harus menentukan nama sumber daya dan ID sumber daya atau menentukan wildcard untuk keduanya.

Misalnya, ARN berikut menentukan semua ACL web dengan cakupan regional untuk akun di Wilayah: `111122223333` `us-west-1`

```
arn:aws:wafv2:us-west-1:111122223333:regional/webacl/*/*
```

ARN berikut menentukan grup aturan bernama `MyIPManagementRuleGroup` dengan cakupan global untuk akun `111122223333` di Wilayah: `us-east-1`

```
arn:aws:wafv2:us-east-1:111122223333:global/rulegroup/MyIPManagementRuleGroup/1111aaaa-bbbb-cccc-dddd-example-id
```

Untuk melihat contoh kebijakan berbasis identitas Shield, lihat. Contoh kebijakan berbasis identitas untuk AWS Shield

Kunci kondisi kebijakan untuk Shield

Mendukung kunci kondisi kebijakan khusus layanan	Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi `AND` logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan `OR` operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tag yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, lihat Elemen kebijakan IAM: variabel dan tag dalam Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Untuk melihat daftar kunci kondisi Shield, lihat Kunci kondisi untuk AWS Shield Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang ditentukan oleh AWS Shield.

Untuk melihat contoh kebijakan berbasis identitas Shield, lihat. Contoh kebijakan berbasis identitas untuk AWS Shield

ACL di Shield

Mendukung ACL	Tidak

Daftar kontrol akses (ACL) mengendalikan pengguna utama mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

ABAC dengan Shield

Mendukung ABAC (tanda dalam kebijakan)	Parsial

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi ketika tag milik prinsipal cocok dengan tag yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi saat manajemen kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tag di elemen kondisi dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Apa itu ABAC? dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) dalam Panduan Pengguna IAM.

Menggunakan kredensyal sementara dengan Shield

Mendukung penggunaan kredensial sementara	Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensyal sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensi sementara, lihat Layanan AWS yang bekerja dengan IAM di Panduan Pengguna IAM.

Anda menggunakan kredensyal sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensil sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat Peralihan peran (konsol) dalam Panduan Pengguna IAM.

Anda dapat membuat kredensyal sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensyal sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda menghasilkan kredensyal sementara secara dinamis alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

Teruskan sesi akses untuk Shield

Mendukung sesi akses maju (FAS)	Ya

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.

Peran layanan untuk Shield

Mendukung peran layanan	Ya

Peran layanan adalah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak fungsionalitas Shield. Edit peran layanan hanya jika Shield memberikan panduan untuk melakukannya.

Peran terkait layanan untuk Shield

Mendukung peran terkait layanan	Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang membuat atau mengelola peran terkait layanan Shield, lihat. Menggunakan peran terkait layanan untuk Shield Advanced

Contoh kebijakan berbasis identitas untuk AWS Shield

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Shield. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat menjalankan peran.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Shield, termasuk format ARN untuk setiap jenis sumber daya, lihat Kunci tindakan, sumber daya, dan kondisi AWS Shield di Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol Shield
- Izinkan pengguna melihat izin mereka sendiri
- Berikan akses baca ke perlindungan Shield Advanced
- Berikan akses hanya-baca ke Shield,, dan CloudFront CloudWatch
- Memberikan akses penuh ke Shield, CloudFront, dan CloudWatch

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Shield di akun Anda. Tindakan ini dikenai biaya untuk Akun AWS Anda. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat kebijakan yang dikelola AWS atau kebijakan yang dikelola AWS untuk fungsi pekerjaan di Panduan Pengguna IAM.

- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukan ini dengan menentukan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, juga dikenal sebagai izin hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk menerapkan izin, lihat Kebijakan dan izin di IAM di Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Syarat di Panduan Pengguna IAM.
- Menggunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda guna memastikan izin yang aman dan berfungsi – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat validasi kebijakan Analizer Akses IAM di Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk mewajibkan MFA saat operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi akses API yang dilindungi MFA di Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM di Panduan Pengguna IAM.

Menggunakan konsol Shield

Untuk mengakses AWS Shield konsol, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Shield di Anda Akun AWS. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebaliknya, izinkan akses hanya ke tindakan yang cocok dengan operasi API yang coba dilakukan.

Pengguna yang dapat mengakses dan menggunakan AWS konsol juga dapat mengakses AWS Shield konsol. Tidak diperlukan izin tambahan.

Izinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan para pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

Berikan akses baca ke perlindungan Shield Advanced

AWS Shield memungkinkan akses sumber daya lintas akun, tetapi tidak memungkinkan Anda membuat perlindungan sumber daya lintas akun. Anda hanya dapat membuat perlindungan untuk sumber daya dari dalam akun yang memiliki sumber daya tersebut.

Berikut ini adalah contoh kebijakan yang memberikan izin untuk `shield:ListProtections` tindakan pada semua sumber daya. Shield tidak mendukung identifikasi sumber daya tertentu menggunakan ARN resource (juga disebut sebagai izin tingkat sumber daya) untuk beberapa tindakan API, jadi Anda menentukan karakter wildcard (*). Ini hanya memungkinkan akses ke sumber daya yang dapat Anda ambil melalui tindakan. `ListProtections`

```
{
    "Version": "2016-06-02",
    "Statement": [
        {
            "Sid": "ListProtections",
            "Effect": "Allow",
            "Action": [
                "shield:ListProtections"
            ],
            "Resource": "*"
        }
    ]
}
```

Berikan akses hanya-baca ke Shield,, dan CloudFront CloudWatch

Kebijakan berikut memberi pengguna akses hanya-baca ke Shield dan sumber daya terkait, termasuk sumber CloudFront daya Amazon, dan metrik Amazon. CloudWatch Ini berguna bagi pengguna yang memerlukan izin untuk melihat pengaturan di perlindungan dan serangan Shield dan untuk memantau metrik di. CloudWatch Pengguna ini tidak dapat membuat, memperbarui, atau menghapus sumber daya Shield.

```
{
        "Version": "2012-10-17",
        "Statement": [
```

```
            {
                "Sid": "ProtectedResourcesReadAccess",
                "Effect": "Allow",
                "Action": [
                    "cloudfront:List*",
                    "elasticloadbalancing:List*",
                    "route53:List*",
                    "cloudfront:Describe*",
                    "elasticloadbalancing:Describe*",
                    "route53:Describe*",
                    "cloudwatch:Describe*",
                    "cloudwatch:Get*",
                    "cloudwatch:List*",
                    "cloudfront:GetDistribution*",
                    "globalaccelerator:ListAccelerators",
                    "globalaccelerator:DescribeAccelerator"
                ],
                "Resource": [
                    "arn:aws:elasticloadbalancing:*:*:*",
                    "arn:aws:cloudfront::*:*",
                    "arn:aws:route53:::hostedzone/*",
                    "arn:aws:cloudwatch:*:*:*:*",
                    "arn:aws:globalaccelerator::*:*"
                ]
            },
            {
                "Sid": "ShieldReadOnly",
                "Effect": "Allow",
                "Action": [
                    "shield:List*",
                    "shield:Describe*",
                    "shield:Get*"
                ],
                "Resource": "*"
            }
    ]
}
```

Memberikan akses penuh ke Shield, CloudFront, dan CloudWatch

Kebijakan berikut memungkinkan pengguna melakukan operasi Shield apa pun, melakukan operasi apa pun pada distribusi CloudFront web, dan memantau metrik dan contoh permintaan di. CloudWatch Ini berguna untuk pengguna yang merupakan administrator Shield.

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "ProtectedResourcesReadAccess",
                "Effect": "Allow",
                "Action": [
                    "cloudfront:List*",
                    "elasticloadbalancing:List*",
                    "route53:List*",
                    "cloudfront:Describe*",
                    "elasticloadbalancing:Describe*",
                    "route53:Describe*",
                    "cloudwatch:Describe*",
                    "cloudwatch:Get*",
                    "cloudwatch:List*",
                    "cloudfront:GetDistribution*",
                    "globalaccelerator:ListAccelerators",
                    "globalaccelerator:DescribeAccelerator"
                ],
                "Resource": [
                    "arn:aws:elasticloadbalancing:*:*:*",
                    "arn:aws:cloudfront::*:*",
                    "arn:aws:route53:::hostedzone/*",
                    "arn:aws:cloudwatch:*:*:*:*",
                    "arn:aws:globalaccelerator::*:*"
                ]
            },
            {
                "Sid": "ShieldFullAccess",
                "Effect": "Allow",
                "Action": [
                    "shield:*"
                ],
                "Resource": "*"
            }
      ]
}
```

Kami sangat menyarankan Anda mengonfigurasi otentikasi multi-faktor (MFA) untuk pengguna yang memiliki izin administratif. Untuk informasi selengkapnya, lihat Menggunakan Perangkat Multi-Factor Authentication (MFA) dengan Panduan Pengguna IAM. AWS

AWS kebijakan terkelola untuk AWS Shield

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS dalam Panduan Pengguna IAM.

AWS kebijakan terkelola: AWSShieldDRTAccessPolicy

AWS Shield menggunakan kebijakan terkelola ini ketika Anda memberikan izin kepada Tim Respons Shield (SRT) untuk bertindak atas nama Anda. Kebijakan ini memberikan SRT akses terbatas ke AWS akun Anda, untuk membantu mitigasi serangan DDoS selama peristiwa tingkat keparahan tinggi. Kebijakan ini memungkinkan SRT untuk mengelola AWS WAF aturan dan perlindungan Shield Advanced dan mengakses log Anda AWS WAF .

Untuk informasi tentang pemberian izin kepada SRT untuk beroperasi atas nama Anda, lihat. Mengkonfigurasi akses untuk Shield Response Team (SRT)

Untuk detail tentang kebijakan ini, lihat AWSShieldDRTAccessPolicydi konsol IAM.

AWS kebijakan terkelola: AWSShieldServiceRolePolicy

Shield Advanced menggunakan kebijakan terkelola ini ketika Anda mengaktifkan mitigasi DDoS lapisan aplikasi otomatis, untuk menetapkan izin yang diperlukan untuk mengelola sumber daya untuk akun Anda. Kebijakan ini memungkinkan Shield Advanced untuk membuat dan menerapkan AWS WAF aturan dan grup aturan di ACL web yang telah Anda kaitkan dengan sumber daya yang dilindungi, untuk merespons serangan DDoS secara otomatis.

Anda tidak dapat melampirkan AWSShieldServiceRolePolicy ke entitas IAM Anda. Shield melampirkan kebijakan ini ke peran terkait layanan untuk `AWSServiceRoleForAWSShield` memungkinkan Shield melakukan tindakan atas nama Anda.

Shield Advanced memungkinkan penggunaan kebijakan ini saat Anda mengaktifkan mitigasi DDoS lapisan aplikasi otomatis. Untuk informasi selengkapnya tentang penggunaan kebijakan ini, lihatMitigasi DDoS lapisan aplikasi otomatis Shield Advanced.

Untuk informasi tentang peran terkait layanan AWSServiceRoleForAWSShield yang menggunakan kebijakan ini, lihat Menggunakan peran terkait layanan untuk Shield Advanced

Untuk detail tentang kebijakan ini, lihat AWSShieldServiceRolePolicydi konsol IAM.

Pembaruan Shield ke kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Shield sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman riwayat dokumen Shield di. Riwayat dokumen

Kebijakan	Deskripsi perubahan	Tanggal
`AWSShieldServiceRolePolicy` Kebijakan ini memungkinkan Shield mengakses dan mengelola AWS sumber daya agar dapat secara otomatis merespons serangan DDoS lapisan aplikasi atas nama Anda. Detail di konsol IAM: AWSShieldServiceRolePolicy	Menambahkan kebijakan ini untuk menyediakan Shield Advanced dengan izin yang diperlukan untuk fungsionalitas mitigasi DDoS lapisan aplikasi otomatis. Untuk informasi tentang fitur ini, lihatMitigasi DDoS lapisan aplikasi otomatis Shield Advanced.	1 Desember 2021
Peran terkait layanan `AWSServiceRoleForAWSShield` menggunakan		

Kebijakan	Deskripsi perubahan	Tanggal
kebijakan ini. Untuk informasi , lihat Menggunakan peran terkait layanan untuk Shield Advanced.		
Shield mulai melacak perubahan	Shield mulai melacak perubahan untuk kebijakan AWS terkelolanya.	3 Maret 2021

Memecahkan masalah AWS Shield identitas dan akses

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Shield dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di Shield
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Shield saya

Saya tidak berwenang untuk melakukan tindakan di Shield

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya *`my-example-widget`* rekaan, tetapi tidak memiliki izin `shield:`*`GetWidget`* rekaan.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 shield:GetWidget on resource: my-example-widget
```

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya *`my-example-widget`* dengan menggunakan tindakan `shield:`*`GetWidget`*.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan bahwa Anda tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Shield.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di Shield. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Shield saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau pengguna di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi pengguna akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa hal berikut:

- Untuk mengetahui apakah Shield mendukung fitur ini, lihatBagaimana AWS Shield bekerja dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.

- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Memberikan akses kepada pengguna eksternal yang sah (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara penggunaan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Perbedaan antara peran IAM dan kebijakan berbasis sumber daya di Panduan Pengguna IAM.

Menggunakan peran terkait layanan untuk Shield Advanced

AWS Shield Advanced menggunakan AWS Identity and Access Management peran terkait layanan (IAM). Peran terkait layanan adalah jenis unik peran IAM yang ditautkan langsung ke Shield Advanced. Peran terkait layanan telah ditentukan sebelumnya oleh Shield Advanced dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan Shield Advanced lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Shield Advanced mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya Shield Advanced yang dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Ini melindungi sumber daya Shield Advanced karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, silakan lihat Layanan AWS yang bisa digunakan dengan IAM dan carilah layanan yang memiliki opsi Ya di kolom Peran Terkait Layanan. Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Izin Peran Tertaut Layanan untuk Shield Advanced

Shield Advanced menggunakan peran terkait layanan bernama. AWSServiceRoleForAWSShield Peran ini memungkinkan Shield Advanced untuk mengakses dan mengelola AWS sumber daya agar dapat secara otomatis merespons serangan DDoS lapisan aplikasi atas nama Anda. Untuk informasi selengkapnya tentang fungsi ini, lihatMitigasi DDoS lapisan aplikasi otomatis Shield Advanced.

Peran AWSServiceRoleForAWSShield terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `shield.amazonaws.com`

Kebijakan izin peran yang diberi nama AWSShieldServiceRolePolicy memungkinkan Shield Advanced menyelesaikan tindakan berikut pada semua AWS sumber daya:

- `wafv2:GetWebACL`
- `wafv2:UpdateWebACL`
- `wafv2:GetWebACLForResource`
- `wafv2:ListResourcesForWebACL`
- `cloudfront:ListDistributions`
- `cloudfront:GetDistribution`

Ketika tindakan diizinkan pada semua AWS sumber daya, ini ditunjukkan dalam kebijakan sebagai`"Resource": "*"`. Ini hanya berarti bahwa peran terkait layanan dapat mengambil setiap tindakan yang ditunjukkan pada semua AWS sumber daya yang didukung tindakan tersebut. Misalnya, tindakan hanya `wafv2:GetWebACL` didukung untuk sumber daya ACL `wafv2` web.

Shield Advanced hanya membuat panggilan API tingkat sumber daya untuk sumber daya yang dilindungi yang telah Anda aktifkan fitur perlindungan lapisan aplikasi dan untuk ACL web yang terkait dengan sumber daya yang dilindungi tersebut.

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi lebih lanjut, lihat Izin Peran Tertaut Layanan di Panduan Pengguna IAM.

Membuat Peran Tertaut Layanan untuk Shield Advanced

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda mengaktifkan mitigasi DDoS lapisan aplikasi otomatis untuk sumber daya di AWS Management Console, the, atau API AWS CLI AWS , Shield Advanced membuat peran terkait layanan untuk Anda.

Jika Anda menghapus peran terkait layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Saat Anda mengaktifkan mitigasi DDoS lapisan aplikasi otomatis untuk sumber daya, Shield Advanced akan membuat peran terkait layanan untuk Anda lagi.

Mengedit Peran Tertaut Layanan untuk Shield Advanced

Shield Advanced tidak mengizinkan Anda mengedit peran AWSServiceRoleForAWSShield terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin merujuk peran tersebut. Namun, Anda dapat mengedit deskripsi peran ini menggunakan IAM. Untuk informasi selengkapnya, silakan lihat Mengedit peran tertaut layanan dalam Panduan Pengguna IAM.

Menghapus Peran Tertaut Layanan untuk Shield Advanced

Jika tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran tertaut layanan, sebaiknya Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Tetapi, Anda harus membersihkan sumber daya peran yang terhubung dengan layanan sebelum menghapusnya secara manual.

> **Note**
>
> Jika Shield Advanced menggunakan peran saat Anda mencoba menghapus sumber daya, maka penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus sumber daya Shield Advanced yang digunakan oleh AWSServiceRoleForAWSShield

Untuk semua sumber daya Anda yang memiliki perlindungan DDoS lapisan aplikasi yang dikonfigurasi, nonaktifkan mitigasi DDoS lapisan aplikasi otomatis. Untuk petunjuk konsol, lihatKonfigurasikan perlindungan DDoS lapisan aplikasi.

Untuk menghapus peran terkait layanan secara manual menggunakan IAM

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran AWSServiceRoleForAWSShield terkait layanan. Untuk informasi selengkapnya, silakan lihat Menghapus Peran Terkait Layanan di Panduan Pengguna IAM.

Wilayah yang Didukung untuk Peran Tertaut Layanan Lanjutan Shield

Shield Advanced mendukung penggunaan peran terkait layanan di semua Wilayah tempat layanan tersedia. Untuk informasi selengkapnya, lihat Titik akhir dan kuota Shield Advanced.

Pencatatan dan pemantauan di Shield

Pemantauan adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja Shield dan AWS solusi Anda. Anda harus mengumpulkan data pemantauan dari semua bagian AWS solusi Anda sehingga Anda dapat lebih mudah men-debug kegagalan multi-titik jika terjadi. AWS menyediakan beberapa alat untuk memantau sumber daya Shield Anda dan menanggapi peristiwa potensial:

CloudWatch Alarm Amazon

Menggunakan CloudWatch alarm, Anda menonton satu metrik selama periode waktu yang Anda tentukan. Jika metrik melebihi ambang batas tertentu, CloudWatch kirimkan pemberitahuan ke topik atau AWS Auto Scaling kebijakan Amazon SNS. Untuk informasi selengkapnya, lihat Pemantauan CloudWatch dengan Amazon.

AWS CloudTrail Log

CloudTrail menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Shield. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat untuk Shield, alamat IP dari mana permintaan itu dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan. Untuk informasi selengkapnya, lihat Logging panggilan API dengan AWS CloudTrail.

Validasi kepatuhan untuk Shield

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar AWS yang berfokus pada keamanan dan kepatuhan.
- Arsitektur untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi yang memenuhi syarat HIPAA.

  > **Note**
  >
  > Tidak semua memenuhi Layanan AWS syarat HIPAA. Untuk informasi selengkapnya, lihat Referensi Layanan yang Memenuhi Syarat HIPAA.

- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber

daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.

- Amazon GuardDuty — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan dalam Shield

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang dan mengoperasikan aplikasi dan basis data yang melakukan secara otomatis pinda saat gagal/failover di antara zona-zona tanpa terputus. Zona Ketersediaan lebih sangat tersedia, lebih toleran kesalahan, dan lebih dapat diskalakan daripadai infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur AWS Global.

Keamanan infrastruktur dalam AWS Shield

Sebagai layanan terkelola, AWS Shield dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses Shield melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.

- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani dengan menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan pengguna utama IAM. Atau Anda bisa menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

AWS Shield Advanced kuota

AWS Shield Advanced memiliki kuota default pada jumlah entitas per Wilayah. Anda dapat meminta peningkatan kuota ini.

Sumber daya	Kuota bawaan
Jumlah maksimum sumber daya yang dilindungi untuk setiap jenis sumber daya yang AWS Shield Advanced menawarkan perlindungan untuk, per akun.	1.000
Jumlah maksimum grup perlindungan, per akun.	100
Jumlah maksimum sumber daya yang dilindungi individu yang dapat Anda sertakan secara khusus dalam grup perlindungan. Di API, ini berlaku untuk `Members` yang Anda tentukan saat Anda menyetel grup `Pattern` perlindun ganARBITRARY . Di konsol, ini berlaku untuk sumber daya yang Anda pilih untuk pengelompokan perlindungan Pilih dari sumber daya yang dilindungi.	1.000

AWS Firewall Manager

AWS Firewall Manager menyederhanakan tugas administrasi dan pemeliharaan Anda di beberapa akun dan sumber daya untuk berbagai perlindungan, termasuk AWS WAF, grup keamanan AWS Shield Advanced Amazon VPC dan ACL jaringan, serta Amazon Route 53 Resolver AWS Network Firewall DNS Firewall. Dengan Firewall Manager, Anda mengatur perlindungan hanya sekali dan layanan secara otomatis menerapkannya di seluruh akun dan sumber daya Anda, bahkan saat Anda menambahkan akun dan sumber daya baru.

Firewall Manager memberikan manfaat ini:

- Membantu melindungi sumber daya di seluruh akun
- Membantu melindungi semua sumber daya dari jenis tertentu, seperti semua CloudFront distribusi Amazon
- Membantu melindungi semua sumber daya dengan tag tertentu
- Secara otomatis menambahkan perlindungan ke sumber daya yang ditambahkan ke akun Anda
- Memungkinkan Anda berlangganan semua akun anggota dalam AWS Organizations organisasi AWS Shield Advanced, dan secara otomatis berlangganan akun dalam lingkup baru yang bergabung dengan organisasi
- Memungkinkan Anda menerapkan aturan grup keamanan ke semua akun anggota atau subset akun tertentu dalam suatu AWS Organizations organisasi, dan secara otomatis menerapkan aturan tersebut ke akun dalam lingkup baru yang bergabung dengan organisasi
- Memungkinkan Anda menggunakan aturan Anda sendiri, atau membeli aturan terkelola AWS Marketplace

Firewall Manager sangat berguna ketika Anda ingin melindungi seluruh organisasi Anda daripada sejumlah kecil akun dan sumber daya tertentu, atau jika Anda sering menambahkan sumber daya baru yang ingin Anda lindungi. Firewall Manager juga menyediakan pemantauan terpusat serangan DDoS di seluruh organisasi Anda.

Topik

- Memulai dengan AWS Firewall Manager kebijakan
- Bekerja dengan AWS Firewall Manager kebijakan
- Bekerja dengan kumpulan sumber daya di Firewall Manager
- Melihat informasi kepatuhan untuk suatu AWS Firewall Manager kebijakan
- AWS Firewall Manager temuan
- Keamanan dalam penggunaan AWS Firewall Manager layanan Anda
- AWS Firewall Manager kuota

AWS Firewall Manager harga

Biaya yang dikeluarkan oleh AWS Firewall Manager adalah untuk layanan yang mendasarinya, seperti AWS WAF dan. AWS Config Untuk informasi selengkapnya, lihat Harga AWS Firewall Manager.

AWS Firewall Manager prasyarat

Topik ini menunjukkan kepada Anda bagaimana bersiap-siap untuk mengelola AWS Firewall Manager. Anda menggunakan satu akun administrator Manajer Firewall untuk mengelola semua kebijakan keamanan Firewall Manager untuk organisasi Anda AWS Organizations. Kecuali jika disebutkan, lakukan langkah-langkah prasyarat menggunakan akun yang akan Anda gunakan sebagai administrator Firewall Manager.

Sebelum Anda menggunakan Firewall Manager untuk pertama kalinya, lakukan langkah-langkah berikut secara berurutan.

Topik

- Langkah 1: Bergabung dan konfigurasikan AWS Organizations
- Langkah 2: Buat akun administrator AWS Firewall Manager default
- Langkah 3: Aktifkan AWS Config
- Langkah 4: Untuk kebijakan pihak ketiga, berlangganan AWS Marketplace dan konfigurasikan setelan pihak ketiga
- Langkah 5: Untuk kebijakan Network Firewall dan DNS Firewall, aktifkan berbagi sumber daya
- Langkah 6: Untuk digunakan AWS Firewall Manager di Wilayah yang dinonaktifkan secara default

Langkah 1: Bergabung dan konfigurasikan AWS Organizations

Untuk menggunakan Firewall Manager, akun Anda harus menjadi anggota organisasi dalam AWS Organizations layanan tempat Anda ingin menggunakan kebijakan Firewall Manager Anda.

> **Note**
>
> Untuk informasi tentang Organizations, lihat Panduan AWS Organizations Pengguna.

Untuk menetapkan AWS Organizations keanggotaan dan konfigurasi yang diperlukan

1. Pilih akun yang akan digunakan sebagai administrator Firewall Manager untuk organisasi di Organizations.
2. Jika akun yang Anda pilih belum menjadi anggota organisasi, mintalah bergabung. Ikuti panduan di Mengundang Akun AWS untuk bergabung dengan organisasi Anda.
3. AWS Organizations memiliki dua set fitur yang tersedia: fitur penagihan terkonsolidasi dan semua fitur. Untuk menggunakan Firewall Manager, organisasi Anda harus diaktifkan untuk semua fitur. Jika organisasi Anda dikonfigurasi hanya untuk penagihan gabungan, ikuti panduan di Mengaktifkan Semua Fitur di Organisasi Anda.

Langkah 2: Buat akun administrator AWS Firewall Manager default

Prosedur ini menggunakan akun dan organisasi yang Anda pilih dan konfigurasikan pada langkah sebelumnya.

Hanya akun manajemen organisasi yang dapat membuat akun administrator default Firewall Manager. Akun administrator pertama yang Anda buat adalah akun admin default. Akun administrator default dapat mengelola firewall pihak ketiga dan memiliki cakupan administratif penuh. Saat Anda mengatur akun administrator default, Firewall Manager secara otomatis menetapkannya sebagai administrator yang AWS Organizations didelegasikan untuk Firewall Manager. Ini memungkinkan Firewall Manager untuk mengakses informasi tentang unit organisasi (OU) dalam organisasi. Anda dapat menggunakan OU untuk menentukan cakupan kebijakan Firewall Manager Anda. Untuk informasi selengkapnya tentang pengaturan cakupan kebijakan, lihat panduan untuk masing-masing jenis kebijakan di bawah iniMembuat AWS Firewall Manager kebijakan. Untuk informasi selengkapnya tentang Organizations and management account, lihat Mengelola AWS Akun di Organisasi Anda.

Pengaturan yang diperlukan untuk akun manajemen organisasi

Akun manajemen organisasi harus memiliki pengaturan berikut untuk onboard organisasi ke Firewall Manager dan membuat administrator default:

- Itu harus menjadi anggota organisasi di AWS Organizations mana Anda ingin menerapkan kebijakan Firewall Manager Anda.

Untuk mengatur akun administrator default

1. Masuk ke Firewall Manager AWS Management Console menggunakan akun AWS Organizations manajemen yang ada.
2. Buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2.
3. Pada panel navigasi, silakan pilih Pengaturan.
4. Ketik ID AWS akun akun yang Anda pilih untuk digunakan sebagai administrator Firewall Manager.

   > **Note**
   >
   > Administrator default memiliki ruang lingkup administratif penuh. Cakupan administratif penuh berarti bahwa akun ini dapat menerapkan kebijakan ke semua akun dan unit organisasi (OU) dalam organisasi, mengambil tindakan di semua Wilayah, dan mengelola semua jenis kebijakan Manajer Firewall.

5. Pilih Buat akun administrator untuk membuat akun.

Untuk informasi selengkapnya tentang mengelola akun administrator Manajer Firewall, lihatBekerja dengan AWS Firewall Manager administrator.

Langkah 3: Aktifkan AWS Config

Untuk menggunakan Firewall Manager, Anda harus mengaktifkan AWS Config.

> **Note**
>
> Anda dikenakan biaya untuk AWS Config pengaturan Anda, sesuai dengan AWS Config harga. Untuk informasi selengkapnya, lihat Memulai dengan AWS Config.

> **Note**
>
> Agar Firewall Manager memantau kepatuhan kebijakan, AWS Config harus terus mencatat perubahan konfigurasi untuk sumber daya yang dilindungi. Dalam AWS Config konfigurasi Anda, frekuensi perekaman harus diatur ke Continuous, yang merupakan pengaturan default.

AWS Config Untuk mengaktifkan Firewall Manager

1. Aktifkan AWS Config untuk setiap akun AWS Organizations anggota Anda, termasuk akun administrator Firewall Manager. Untuk informasi selengkapnya, lihat Memulai dengan AWS Config.
2. Aktifkan AWS Config untuk setiap Wilayah AWS yang berisi sumber daya yang ingin Anda lindungi. Anda dapat mengaktifkan AWS Config secara manual, atau Anda dapat menggunakan AWS CloudFormation templat “Aktifkan AWS Config” di Template AWS CloudFormation StackSets Sampel.

   Jika Anda tidak ingin mengaktifkan AWS Config semua sumber daya, maka Anda harus mengaktifkan yang berikut ini sesuai dengan jenis kebijakan Firewall Manager yang Anda gunakan:

   - Kebijakan WAF - Aktifkan Config untuk CloudFront jenis sumber daya Distribusi, Application Load Balancer ElasticLoadBalancing(pilih V2 dari daftar), API Gateway, WAF WebACL, WAF Regional WebACL, dan WAFv2 WebACL. Untuk memungkinkan AWS Config untuk melindungi CloudFront distribusi, Anda harus berada di Wilayah AS Timur (Virginia N.). Wilayah lain tidak memiliki CloudFront pilihan.
   - Kebijakan Shield - Aktifkan Config untuk jenis sumber daya Shield Protection, Protection, ShieldRegional Application Load Balancer, EC2 EIP, WAF WebACL, WAF Regional WebACL, dan WAFv2 WebACL.
   - Kebijakan grup keamanan - Aktifkan Config untuk jenis sumber daya EC2, Instans EC2 SecurityGroup, dan EC2. NetworkInterface
   - Kebijakan ACL Jaringan - Aktifkan Config untuk jenis sumber daya Amazon EC2 Subnet dan jaringan Amazon EC2 ACL.
   - Kebijakan Network Firewall - Aktifkan Config untuk jenis sumber daya,, EC2 VPC NetworkFirewall FirewallPolicy NetworkFirewallRuleGroup, EC2, EC2, dan InternetGateway EC2 Subnet. RouteTable

- Kebijakan DNS Firewall - Aktifkan Config untuk jenis sumber daya EC2 VPC.
- Kebijakan firewall pihak ketiga - Aktifkan Config untuk jenis sumber daya Amazon EC2 VPC, Amazon EC2, Amazon EC2, Amazon InternetGateway EC2 Subnet, dan Amazon RouteTable EC2 VPcendPoint.

> **Note**
>
> Jika Anda mengonfigurasi AWS Config perekam untuk menggunakan peran IAM kustom, Anda perlu memastikan kebijakan IAM memiliki izin yang tepat untuk merekam jenis sumber daya wajib kebijakan Firewall Manager. Tanpa izin yang tepat, sumber daya yang diperlukan mungkin tidak direkam yang mencegah Firewall Manager melindungi sumber daya Anda dengan benar. Firewall Manager tidak memiliki visibilitas ke dalam kesalahan konfigurasi izin ini. Untuk informasi tentang menggunakan IAM dengan AWS Config, lihat IAM untuk. AWS Config

Langkah 4: Untuk kebijakan pihak ketiga, berlangganan AWS Marketplace dan konfigurasikan setelan pihak ketiga

Lengkapi prasyarat berikut untuk memulai kebijakan firewall pihak ketiga Firewall Manager.

Fortigate Cloud Native Firewall (CNF) sebagai prasyarat kebijakan Layanan

Untuk menggunakan Fortigate CNF untuk Firewall Manager

1. Berlangganan Fortigate Cloud Native Firewall (CNF) sebagai layanan Layanan di Marketplace. AWS
2. Pertama, daftarkan penyewa di portal produk Fortigate CNF. Kemudian Tambahkan akun administrator Firewall Manager Anda di bawah penyewa Anda di portal produk Fortigate CNF. Untuk informasi lebih lanjut, lihat dokumentasi Fortigate CNF.

Untuk informasi tentang bekerja dengan kebijakan Fortigate CNF, lihat. Fortigate Cloud Native Firewall (CNF) sebagai kebijakan Layanan

Prasyarat kebijakan Firewall Generasi Berikutnya Palo Alto Networks Cloud

Untuk menggunakan Palo Alto Networks Cloud NGFW untuk Firewall Manager

1. Berlangganan layanan Palo Alto Networks Cloud Next Generation Firewall Pay-As-You-Go di Marketplace. AWS
2. Selesaikan langkah-langkah penerapan Palo Alto Networks Cloud NGFW yang tercantum dalam panduan Deploy Palo Alto Networks Cloud NGFW untuk AWS dengan AWS Firewall Manager topik di Palo Alto Networks Cloud Next Generation Firewall untuk panduan penerapan. AWS

Untuk informasi tentang bekerja dengan kebijakan Palo Alto Networks Cloud NGFW, lihat. Kebijakan Palo Alto Networks Cloud NGFW

Langkah 5: Untuk kebijakan Network Firewall dan DNS Firewall, aktifkan berbagi sumber daya

Untuk mengelola kebijakan Firewall Manager Network Firewall dan DNS Firewall, Anda harus mengaktifkan sharing with AWS Organizations in AWS Resource Access Manager. Ini memungkinkan Firewall Manager untuk menerapkan perlindungan di seluruh akun Anda saat Anda membuat jenis kebijakan ini.

Untuk mengaktifkan berbagi dengan AWS Organizations in AWS Resource Access Manager

- Ikuti panduan di Aktifkan Berbagi dengan AWS Organizations di Panduan AWS Resource Access Manager Pengguna.

Jika Anda mengalami masalah dengan berbagi sumber daya, lihat panduan diBerbagi sumber daya untuk kebijakan Network Firewall dan DNS Firewall.

Langkah 6: Untuk digunakan AWS Firewall Manager di Wilayah yang dinonaktifkan secara default

Untuk menggunakan Firewall Manager di Wilayah yang dinonaktifkan secara default, Anda harus mengaktifkan Region untuk akun manajemen AWS organisasi dan akun administrator default Firewall Manager. Untuk informasi tentang Wilayah yang dinonaktifkan secara default dan cara mengaktifkannya, lihat Mengelola Wilayah AWS di Referensi AWS Umum.

Untuk mengaktifkan Wilayah yang dinonaktifkan

- Untuk akun manajemen Organizations dan akun administrator default Firewall Manager, ikuti panduan di Mengaktifkan Wilayah di Referensi AWS Umum.

Setelah mengikuti langkah-langkah ini, Anda dapat mengonfigurasi Firewall Manager untuk mulai melindungi sumber daya Anda. Untuk informasi selengkapnya, lihat Memulai dengan AWS Firewall ManagerAWS WAF kebijakan.

Bekerja dengan AWS Firewall Manager administrator

Dengan AWS Firewall Manager Anda dapat memiliki satu atau beberapa administrator yang dapat mengelola sumber daya firewall organisasi Anda. Jika ingin menggunakan beberapa administrator Firewall Manager di organisasi, Anda dapat menerapkan kondisi cakupan administratif ke setiap administrator untuk menentukan sumber daya yang dapat mereka kelola. Ini memberi Anda fleksibilitas untuk memiliki peran administrator yang berbeda dalam organisasi Anda, dan membantu Anda mempertahankan prinsip akses yang paling tidak istimewa. Misalnya, Anda dapat meminta satu administrator mengelola satu set unit organisasi (OU) untuk organisasi Anda, sambil mendelegasikan administrator lain untuk mengelola hanya jenis kebijakan Firewall Manager tertentu. Untuk informasi selengkapnya tentang Organizations and management account, lihat Mengelola AWS Akun di Organisasi Anda.

Untuk jumlah maksimum administrator yang dapat Anda miliki per organisasi, lihat AWS Firewall Manager kuota

Memulai menggunakan administrator Firewall Manager

Sebelum Anda mulai menggunakan administrator Firewall Manager, Anda harus melengkapi prasyarat yang tercantum di dalamnya. AWS Firewall Manager prasyarat Dalam prasyarat, Anda akan melakukan onboard organisasi ke AWS Organizations Firewall Manager dan membuat akun administrator default untuk Firewall Manager. Akun administrator default memiliki kemampuan untuk mengelola firewall pihak ketiga dan memiliki ruang lingkup administratif penuh.

Ruang lingkup administratif

Lingkup administratif mendefinisikan sumber daya yang dapat dikelola oleh administrator Firewall Manager. Setelah akun AWS Organizations manajemen mengonboard organisasi ke Firewall Manager, akun manajemen dapat membuat administrator Firewall Manager tambahan dengan cakupan administratif yang berbeda. Akun AWS Organizations manajemen dapat memberikan

ruang lingkup administratif penuh atau terbatas kepada administrator. Cakupan penuh memberi administrator akses penuh ke semua jenis sumber daya sebelumnya. Lingkup terbatas mengacu pada pemberian izin administratif hanya sebagian dari sumber daya sebelumnya. Kami menyarankan Anda hanya memberikan administrator izin yang mereka butuhkan untuk melakukan tugas peran mereka. Anda dapat menerapkan kombinasi kondisi lingkup administratif ini ke administrator:

- Akun atau OU di organisasi Anda tempat administrator dapat menerapkan kebijakan.
- Wilayah tempat administrator dapat melakukan tindakan.
- Jenis kebijakan Firewall Manager yang dapat dikelola administrator.

Peran administrator

Ada dua jenis peran administrator di Firewall Manager: administrator default, dan administrator Firewall Manager.

- Administrator default - Akun manajemen organisasi membuat akun administrator default Firewall Manager saat mereka melakukan onboard organisasi mereka ke Firewall Manager saat menyelesaikan. AWS Firewall Manager prasyarat Administrator default dapat mengelola firewall pihak ketiga dan memiliki cakupan administratif penuh, tetapi sebaliknya pada tingkat rekan yang sama dengan administrator lain, jika Anda memilih untuk memiliki beberapa administrator.
- Administrator Firewall Manager - Administrator Firewall Manager dapat mengelola sumber daya yang ditetapkan oleh akun AWS Organizations manajemen untuk mereka dalam konfigurasi ruang lingkup administratifnya. Untuk jumlah maksimum administrator yang dapat Anda miliki per organisasi, lihatAWS Firewall Manager kuota. Setelah membuat akun administrator Firewall Manager, layanan memeriksa dengan AWS Organizations untuk melihat apakah akun tersebut sudah menjadi administrator yang didelegasikan untuk Firewall Manager dalam organisasi. Jika tidak, maka Firewall Manager memanggil Organizations untuk menetapkan akun sebagai administrator yang didelegasikan untuk Firewall Manager. Untuk informasi tentang administrator yang didelegasikan Organizations, lihat AWS Organizations terminologi dan konsep di Panduan Pengguna.AWS Organizations

Administrator yang ada

Jika Anda adalah pelanggan Firewall Manager yang sudah ada dan telah menetapkan administrator, maka administrator yang ada ini akan menjadi administrator default Firewall Manager. Seharusnya tidak ada dampak pada aliran Anda yang ada. Jika Anda ingin menambahkan lebih banyak administrator, Anda dapat melakukannya dengan mengikuti prosedur dalam Bab ini.

Membuat, memperbarui, dan mencabut akun administrator Firewall Manager

Prosedur dalam topik berikut menjelaskan cara membuat, memperbarui, dan mencabut akun administrator Firewall Manager. Hanya akun manajemen organisasi yang dapat membuat dan memperbarui akun administrator Firewall Manager. Hanya administrator Firewall Manager individu yang dapat mencabut akun administrator mereka sendiri.

Membuat akun administrator Firewall Manager

Prosedur berikut menjelaskan cara membuat akun administrator Firewall Manager menggunakan konsol Firewall Manager.

Untuk membuat akun administrator Firewall Manager

1. Masuk ke Firewall Manager AWS Management Console menggunakan akun AWS Organizations manajemen yang ada.
2. Buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2.
3. Pada panel navigasi, silakan pilih Pengaturan.
4. Pilih Buat akun administrator.
5. Di panel Detail, untuk ID AWS akun ketik AWS ID akun anggota yang ingin Anda tambahkan sebagai administrator Firewall Manager.
6. Untuk lingkup Administratif, pilih salah satu opsi berikut:

   - Lengkap — Ini memberi administrator kemampuan untuk menerapkan kebijakan ke semua akun dan unit organisasi (OU) dalam organisasi, mengambil tindakan di semua Wilayah, dan menerapkan semua jenis kebijakan Firewall Manager, kecuali untuk firewall pihak ketiga. Hanya administrator default yang dapat membuat dan mengelola firewall pihak ketiga. Berhati-hatilah jika memberikan tingkat izin ini kepada administrator. Dengan semangat hak istimewa yang paling sedikit, kami sarankan hanya memberikan izin kepada administrator yang mereka butuhkan untuk melakukan tugas peran mereka.
   - Dibatasi — Jika menerapkan cakupan Terbatas, maka di Konfigurasi lingkup administratif, konfigurasikan akun dan unit organisasi, Wilayah, dan jenis kebijakan yang dapat dikelola akun.

     Untuk Akun dan unit organisasi, pilih opsi sebagai berikut:

- Jika Anda ingin menerapkan kebijakan ke semua akun atau unit organisasi di organisasi Anda, pilih Sertakan semua akun di AWS organisasi saya.
- Jika Anda ingin menerapkan kebijakan hanya untuk akun atau akun tertentu yang berada di unit AWS Organizations organisasi tertentu (OU), pilih Sertakan hanya akun dan unit organisasi yang ditentukan, lalu tambahkan akun dan OU yang ingin Anda sertakan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.
- Jika Anda ingin menerapkan kebijakan untuk semua kecuali satu set akun atau unit AWS Organizations organisasi (OU) tertentu, pilih Kecualikan akun dan unit organisasi yang ditentukan, dan sertakan semua akun lainnya, lalu tambahkan akun dan OU yang ingin Anda kecualikan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.

Untuk Wilayah, pilih opsi sebagai berikut:

- Jika Anda ingin mengizinkan administrator melakukan tindakan di semua Wilayah yang tersedia, pilih Sertakan semua Wilayah.
- Jika Anda ingin administrator melakukan tindakan hanya di Wilayah tertentu, pilih Sertakan hanya Wilayah yang ditentukan, lalu tentukan Wilayah yang ingin Anda sertakan.

> **Note**
>
> Untuk menyertakan Wilayah yang dinonaktifkan secara default, Anda harus mengaktifkan Wilayah untuk akun manajemen AWS Organizations organisasi dan akun administrasi default. Untuk informasi tentang mengaktifkan Wilayah untuk akun, lihat Mengaktifkan Wilayah di. Referensi Umum Amazon Web

Untuk jenis Kebijakan, pilih opsi sebagai berikut:.

- Jika Anda ingin mengizinkan administrator mengelola semua jenis kebijakan, pilih Sertakan semua jenis kebijakan.
- Jika Anda ingin administrator mengelola hanya jenis kebijakan tertentu, pilih Sertakan hanya jenis kebijakan yang ditentukan, lalu tentukan jenis kebijakan yang ingin Anda sertakan.

7. Pilih Buat akun administrator untuk membuat akun administrator. Setelah dibuat, Firewall Manager memanggil AWS Organizations untuk melihat apakah administrator sudah menjadi administrator yang didelegasikan untuk organisasi Anda. Jika tidak, Firewall Manager akan

menunjuk akun sebagai administrator yang didelegasikan. Untuk informasi tentang administrator yang didelegasikan di Organizations, lihat AWS Organizations terminologi dan konsep di Panduan Pengguna.AWS Organizations

Jika Anda menerapkan lingkup administratif terbatas, Firewall Manager secara otomatis mengevaluasi sumber daya baru apa pun terhadap pengaturan Anda. Misalnya, jika Anda hanya menyertakan akun tertentu, Firewall Manager tidak menerapkan kebijakan tersebut ke akun baru mana pun. Sebagai contoh lain, jika Anda menyertakan OU, ketika Anda menambahkan akun ke OU atau ke salah satu OU anaknya, Firewall Manager secara otomatis menyertakan akun dalam lingkup administratif.

Memperbarui akun administrator Firewall Manager

Prosedur berikut menjelaskan cara memperbarui akun administrator Firewall Manager menggunakan konsol Firewall Manager.

> **Note**
>
> Untuk memperbarui cakupan administrator agar menyertakan Wilayah yang dinonaktifkan secara default, Anda harus mengaktifkan Wilayah untuk akun manajemen AWS Organizations organisasi dan akun administrasi default. Untuk informasi tentang mengaktifkan Wilayah untuk akun, lihat Mengaktifkan Wilayah di. Referensi Umum Amazon Web

Untuk memperbarui akun administrator (konsol)

1. Masuk ke Firewall Manager AWS Management Console menggunakan akun AWS Organizations manajemen yang ada.
2. Buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2.
3. Pada panel navigasi, silakan pilih Pengaturan.
4. di tabel administrator Firewall Manager, pilih akun yang ingin Anda perbarui.
5. Pilih Edit untuk mengubah detail akun administrator. Anda tidak dapat mengubah ID akun.
6. Pilih Simpan untuk menyimpan perubahan Anda.

Mencabut akun administrator

Prosedur berikut menjelaskan cara mencabut akun administrator Firewall Manager. Jika Anda adalah administrator default, sebelum Anda dapat mencabut akun Anda semua akun administrator Firewall Manager dalam organisasi Anda harus terlebih dahulu mencabut akun mereka sendiri. Untuk mencabut akun administrator, ikuti prosedur di bawah ini

Untuk mencabut akun administrator (konsol)

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Di panel akun Administrator, pilih Cabut akun administrator untuk mencabut akun Anda.

> **Important**
>
> Bila Anda mencabut hak istimewa administrator dari akun administrator, semua kebijakan Firewall Manager yang dibuat oleh akun tersebut akan dihapus.

Mengubah akun administrator default

Anda hanya dapat menetapkan satu akun di organisasi sebagai akun administrator Firewall Manager default. Akun administrator default mengikuti prinsip first in, last out. Untuk menetapkan akun administrator default yang berbeda, setiap akun administrator individu harus terlebih dahulu mencabut akun mereka sendiri. Kemudian, administrator default yang ada dapat mencabut akun mereka sendiri, yang juga akan melepaskan organisasi dari Firewall Manager. Ketika administrator mencabut akun mereka, semua kebijakan Firewall Manager yang dibuat oleh akun tersebut akan dihapus. Untuk menetapkan akun administrator default baru, Anda kemudian harus masuk ke Firewall Manager dengan akun AWS Organizations manajemen untuk menunjuk akun administrator baru. Untuk mengubah akun administrator default untuk organisasi, lakukan prosedur berikut.

Untuk mengubah akun administrator default

1. Masuk ke Firewall Manager AWS Management Console menggunakan akun AWS Organizations manajemen yang ada.

2. Buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2.
3. Pada panel navigasi, silakan pilih Pengaturan.
4. Ketik ID akun yang Anda pilih untuk digunakan sebagai administrator Firewall Manager.

> **Note**
>
> Akun ini diberikan izin untuk membuat dan mengelola kebijakan Firewall Manager di semua akun dalam organisasi Anda.

5. Pilih Buat akun administrator.
6. Ketik AWS ID akun yang Anda pilih untuk digunakan sebagai administrator Firewall Manager.

> **Note**
>
> Akun ini diberikan ruang lingkup administratif penuh. Cakupan administratif penuh berarti bahwa akun ini dapat menerapkan kebijakan ke semua akun dan unit organisasi (OU) dalam organisasi, mengambil tindakan di semua Wilayah, dan mengelola semua jenis kebijakan Manajer Firewall.

7. Pilih Buat akun administrator untuk membuat akun administrator default.

Mendiskualifikasi perubahan pada akun administrator

Beberapa perubahan pada akun administrator dapat mendiskualifikasi dari akun administrator yang tersisa.

Bagian ini menjelaskan perubahan yang dapat mendiskualifikasi akun administrator, dan bagaimana AWS dan Firewall Manager menangani perubahan ini.

Akun dihapus dari organisasi di AWS Organizations

Jika akun AWS Firewall Manager administrator dihapus dari organisasi di AWS Organizations, akun administrator tidak dapat lagi mengelola kebijakan untuk organisasi. Firewall Manager mengambil salah satu tindakan berikut:

- Akun tanpa kebijakan — Jika akun administrator Firewall Manager tidak memiliki kebijakan Firewall Manager, Firewall Manager mencabut akun administrator.

- Kebijakan Akun dengan Firewall Manager — Jika akun administrator Firewall Manager memiliki kebijakan Firewall Manager, Firewall Manager mengirimkan email untuk memberi tahu Anda tentang situasi dan untuk memberikan opsi yang dapat Anda ambil, dengan bantuan perwakilan akun AWS penjualan Anda.

Akun ditutup

Jika Anda menutup akun yang Anda gunakan untuk AWS Firewall Manager administrator, AWS dan Firewall Manager menangani penutupan sebagai berikut:

- AWS mencabut akses administrator akun dari Firewall Manager dan Firewall Manager menonaktifkan kebijakan apa pun yang dikelola oleh akun administrator. Perlindungan yang diberikan oleh kebijakan tersebut dihentikan di seluruh organisasi.
- AWS menyimpan data kebijakan Firewall Manager untuk akun selama 90 hari sejak tanggal efektif penutupan akun administrator. Selama periode 90 hari ini, Anda dapat membuka kembali akun yang ditutup.
  - Jika Anda membuka kembali akun yang ditutup selama periode 90 hari, AWS menetapkan kembali akun sebagai administrator Manajer Firewall dan memulihkan data kebijakan Manajer Firewall untuk akun tersebut.
  - Jika tidak, pada akhir periode 90 hari, AWS secara permanen menghapus semua data kebijakan Firewall Manager untuk akun tersebut.

Memulai dengan AWS Firewall Manager kebijakan

Anda dapat menggunakan AWS Firewall Manager untuk mengaktifkan sejumlah jenis kebijakan keamanan yang berbeda. Langkah-langkah untuk mengatur sedikit berbeda untuk masing-masing.

Topik

- Memulai dengan AWS Firewall ManagerAWS WAF kebijakan
- Memulai dengan AWS Firewall ManagerAWS Shield Advanced kebijakan
- Memulai AWS Firewall Manager kebijakan grup keamanan Amazon VPC
- Memulai dengan AWS Firewall Manager kebijakan ACL jaringan Amazon VPC
- Memulai dengan AWS Firewall ManagerAWS Network Firewall kebijakan
- Memulai kebijakan AWS Firewall Manager DNS Firewall

- Memulai dengan kebijakan AWS Firewall Manager Palo Alto Networks Cloud Next Generation Firewall
- Memulai dengan kebijakan AWS Firewall Manager Fortigate CNF

Memulai dengan AWS Firewall ManagerAWS WAF kebijakan

AWS Firewall Manager Untuk mengaktifkan AWS WAF aturan di seluruh organisasi Anda, lakukan langkah-langkah berikut secara berurutan.

Topik

- Langkah 1: Selesaikan prasyarat
- Langkah 2: Buat dan terapkan AWS WAF kebijakan
- Langkah 3: Bersihkan

Langkah 1: Selesaikan prasyarat

Ada beberapa langkah wajib untuk mempersiapkan akun Anda AWS Firewall Manager. Langkah-langkah tersebut dijelaskan dalamAWS Firewall Manager prasyarat. Lengkapi semua prasyarat sebelum melanjutkan ke. Langkah 2: Buat dan terapkan AWS WAF kebijakan

Langkah 2: Buat dan terapkan AWS WAF kebijakan

AWS WAF Kebijakan Firewall Manager berisi grup aturan yang ingin Anda terapkan ke sumber daya Anda. Firewall Manager membuat Firewall Manager web ACL di setiap akun tempat Anda menerapkan kebijakan. Manajer akun individu dapat menambahkan aturan dan grup aturan ke ACL web yang dihasilkan, selain grup aturan yang Anda tentukan di sini. Untuk informasi tentang AWS WAF kebijakan Firewall Manager, lihatAWS WAF kebijakan.

Untuk membuat AWS WAF kebijakan Firewall Manager (konsol)

Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

1. Di panel navigasi, pilih Kebijakan keamanan.
2. Pilih Buat kebijakan.
3. Untuk jenis Kebijakan, pilih AWS WAF.

4. Untuk Wilayah, pilih Wilayah AWS. Untuk melindungi CloudFront distribusi Amazon, pilih Global.

   Untuk melindungi sumber daya di beberapa Wilayah (selain CloudFront distribusi), Anda harus membuat kebijakan Firewall Manager terpisah untuk setiap Wilayah.

5. Pilih Selanjutnya.

6. Untuk nama Kebijakan, masukkan nama deskriptif. Firewall Manager menyertakan nama kebijakan dalam nama ACL web yang dikelola. Nama ACL web telah `FMManagedWebACLV2-` diikuti dengan nama kebijakan yang Anda masukkan di sini`-`, dan stempel waktu pembuatan ACL web, dalam milidetik UTC. Misalnya, `FMManagedWebACLV2-MyWAFPolicyName-1621880374078`.

   > **Important**
   >
   > Nama ACL web tidak dapat berubah setelah pembuatan. Jika memperbarui nama kebijakan, Firewall Manager tidak akan memperbarui nama ACL web terkait. Agar Firewall Manager membuat ACL web dengan nama yang berbeda, Anda harus membuat kebijakan baru.

7. Di bawah Aturan kebijakan, untuk grup aturan Pertama, pilih Tambahkan grup aturan. Perluas grup aturan AWS terkelola. Untuk set aturan Inti, alihkan Tambahkan ke ACL web. Untuk masukan buruk yang AWS diketahui, alihkan Add to web ACL. Pilih Tambahkan aturan.

   Untuk grup aturan terakhir, pilih Tambahkan grup aturan. Perluas grup aturan AWS terkelola dan untuk daftar reputasi IP Amazon, alihkan Tambahkan ke web ACL. Pilih Tambahkan aturan.

   Di bawah Grup aturan pertama, pilih Set aturan inti dan pilih Pindah ke bawah. AWS WAF mengevaluasi permintaan web terhadap grup aturan masukan buruk yang AWS diketahui sebelum mengevaluasi terhadap set aturan Core.

   Anda juga dapat membuat grup AWS WAF aturan Anda sendiri jika Anda mau, menggunakan AWS WAF konsol. Setiap grup aturan yang Anda buat muncul di bawah grup aturan Anda di halaman Jelaskan kebijakan: Tambahkan grup aturan.

   Grup AWS WAF aturan pertama dan terakhir yang Anda kelola melalui Firewall Manager memiliki nama yang dimulai dengan `PREFMManaged-` atau`POSTFMManaged-`, masing-masing, diikuti dengan nama kebijakan Firewall Manager, dan stempel waktu pembuatan grup aturan, dalam milidetik UTC. Misalnya, `PREFMManaged-MyWAFPolicyName-1621880555123`.

8. Biarkan tindakan default untuk ACL web di Izinkan.

9. Biarkan tindakan Kebijakan secara default, untuk tidak secara otomatis memulihkan sumber daya yang tidak sesuai. Anda dapat mengubah opsi nanti.
10. Pilih Selanjutnya.
11. Untuk cakupan Kebijakan, Anda menyediakan setelan untuk akun, jenis sumber daya, dan penandaan yang mengidentifikasi sumber daya yang ingin Anda terapkan kebijakan. Untuk tutorial ini, tinggalkan pengaturan Akun AWSdan Resources, dan pilih satu atau beberapa jenis sumber daya.
12. Untuk Sumber Daya, Anda dapat mempersempit cakupan kebijakan menggunakan penandaan, dengan menyertakan atau mengecualikan sumber daya dengan tag yang Anda tentukan. Anda dapat menggunakan inklusi atau pengecualian, dan bukan keduanya. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.

    Jika Anda memasukkan lebih dari satu tag, sumber daya harus memiliki semua tag untuk disertakan atau dikecualikan.

    Tag sumber daya hanya dapat memiliki nilai non-null. Jika Anda menghilangkan nilai untuk tag, Firewall Manager menyimpan tag dengan nilai string kosong: “”. Tag sumber daya hanya cocok dengan tag yang memiliki kunci yang sama dan nilai yang sama.
13. Pilih Selanjutnya.
14. Untuk tag Kebijakan, tambahkan tag pengenal apa pun yang ingin Anda tambahkan ke sumber daya kebijakan Manajer Firewall. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.
15. Pilih Selanjutnya.
16. Tinjau pengaturan kebijakan baru dan kembali ke halaman mana pun yang Anda perlukan untuk penyesuaian apa pun.

    Periksa untuk memastikan bahwa tindakan Kebijakan disetel ke Identifikasi sumber daya yang tidak mematuhi aturan kebijakan, tetapi jangan diperbaiki secara otomatis. Ini memungkinkan Anda untuk meninjau perubahan yang akan dibuat kebijakan Anda sebelum Anda mengaktifkannya.
17. Jika Anda puas dengan kebijakan ini, pilih Create policy (Buat kebijakan).

    Di panel AWS Firewall Manager kebijakan, kebijakan Anda harus dicantumkan. Ini mungkin akan menunjukkan Pending di bawah judul akun dan itu akan menunjukkan status pengaturan remediasi otomatis. Pembuatan kebijakan dapat memakan waktu beberapa menit. Setelah Status tertunda diganti dengan jumlah akun, Anda dapat memilih nama kebijakan untuk

menjelajahi status kepatuhan akun dan sumber daya. Untuk informasi, lihat Melihat informasi kepatuhan untuk suatu AWS Firewall Manager kebijakan

Langkah 3: Bersihkan

Untuk menghindari biaya asing, hapus kebijakan dan sumber daya yang tidak perlu.

Untuk menghapus kebijakan (konsol)

1. Pada halaman AWS Firewall Manager kebijakan, pilih tombol radio di sebelah nama kebijakan, lalu pilih Hapus.
2. Di kotak Hapus konfirmasi, pilih Hapus semua sumber kebijakan, lalu pilih Hapus lagi.

   AWS WAF menghapus kebijakan dan sumber daya terkait, seperti ACL web, yang dibuat di akun Anda. Perubahan mungkin memakan waktu beberapa menit untuk menyebar ke semua akun.

Memulai dengan AWS Firewall ManagerAWS Shield Advanced kebijakan

Anda dapat menggunakan AWS Firewall Manager untuk mengaktifkan AWS Shield Advanced perlindungan di seluruh organisasi Anda.

> **Important**
>
> Firewall Manager tidak mendukung Amazon Route 53 atau AWS Global Accelerator. Jika Anda perlu melindungi sumber daya ini dengan Shield Advanced, Anda tidak dapat menggunakan kebijakan Firewall Manager. Sebaliknya, ikuti instruksi diMenambahkan AWS Shield Advanced perlindungan ke AWS sumber daya.

Untuk menggunakan Firewall Manager untuk mengaktifkan perlindungan Shield Advanced, lakukan langkah-langkah berikut secara berurutan.

Topik

- Langkah 1: Selesaikan prasyarat
- Langkah 2: Buat dan terapkan kebijakan Shield Advanced
- Langkah 3: (Opsional) memberi wewenang kepada Tim Respons Shield (SRT)
- Langkah 4: Konfigurasikan notifikasi Amazon SNS dan alarm Amazon CloudWatch

Langkah 1: Selesaikan prasyarat

Ada beberapa langkah wajib untuk mempersiapkan akun Anda AWS Firewall Manager. Langkah-langkah tersebut dijelaskan dalamAWS Firewall Manager prasyarat. Lengkapi semua prasyarat sebelum melanjutkan ke. Langkah 2: Buat dan terapkan kebijakan Shield Advanced

Langkah 2: Buat dan terapkan kebijakan Shield Advanced

Setelah menyelesaikan prasyarat, Anda membuat kebijakan Shield AWS Firewall Manager Advanced. Kebijakan Firewall Manager Shield Advanced berisi akun dan sumber daya yang ingin Anda lindungi dengan Shield Advanced.

> **Important**
>
> Firewall Manager tidak mendukung Amazon Route 53 atau AWS Global Accelerator. Jika Anda perlu melindungi sumber daya ini dengan Shield Advanced, Anda tidak dapat menggunakan kebijakan Firewall Manager. Sebagai gantinya, ikuti instruksi diMenambahkan AWS Shield Advanced perlindungan ke AWS sumber daya.

Untuk membuat kebijakan lanjutan Firewall Manager Shield (konsol)

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

   > **Note**
   >
   > Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

2. Di panel navigasi, pilih Kebijakan keamanan.
3. Pilih Buat kebijakan.
4. Untuk jenis Kebijakan, pilih Shield Advanced.

   Untuk membuat kebijakan Shield Advanced, akun administrator Firewall Manager Anda harus berlangganan Shield Advanced. Jika Anda tidak berlangganan, Anda diminta untuk melakukannya. Untuk informasi tentang biaya berlangganan, lihat AWS Shield Advanced Harga.

> **Note**
>
> Anda tidak perlu berlangganan secara manual setiap akun anggota ke Shield Advanced. Firewall Manager melakukan ini untuk Anda saat membuat kebijakan. Setiap akun harus tetap berlangganan Firewall Manager dan Shield Advanced untuk terus melindungi sumber daya di akun.

5. Untuk Wilayah, pilih file Wilayah AWS. Untuk melindungi CloudFront sumber daya Amazon, pilih Global.

   Untuk melindungi sumber daya di beberapa Wilayah (selain CloudFront sumber daya), Anda harus membuat kebijakan Firewall Manager terpisah untuk setiap Wilayah.
6. Pilih Selanjutnya.
7. Untuk Nama, masukkan nama deskriptif.
8. (Khusus Wilayah Global) Untuk kebijakan Wilayah Global, Anda dapat memilih apakah Anda ingin mengelola mitigasi DDoS lapisan aplikasi otomatis Shield Advanced. Untuk tutorial ini, biarkan pilihan ini pada pengaturan default Ignore.
9. Untuk tindakan Kebijakan, pilih opsi yang tidak otomatis diperbaiki.
10. Pilih Selanjutnya.
11. Akun AWS Kebijakan ini berlaku untuk memungkinkan Anda mempersempit cakupan kebijakan Anda dengan menentukan akun untuk disertakan atau dikecualikan. Untuk tutorial ini, pilih Sertakan semua akun di bawah organisasi saya.
12. Pilih jenis sumber daya yang ingin Anda lindungi.

    Firewall Manager tidak mendukung Amazon Route 53 atau AWS Global Accelerator. Jika Anda perlu melindungi sumber daya ini dengan Shield Advanced, Anda tidak dapat menggunakan kebijakan Firewall Manager. Sebagai gantinya, ikuti panduan Shield Advanced diMenambahkan AWS Shield Advanced perlindungan ke AWS sumber daya.
13. Untuk Sumber Daya, Anda dapat mempersempit cakupan kebijakan menggunakan penandaan, dengan menyertakan atau mengecualikan sumber daya dengan tag yang Anda tentukan. Anda dapat menggunakan inklusi atau pengecualian, dan bukan keduanya. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.

    Jika Anda memasukkan lebih dari satu tag, sumber daya harus memiliki semua tag untuk disertakan atau dikecualikan.

Tag sumber daya hanya dapat memiliki nilai non-null. Jika Anda menghilangkan nilai untuk tag, Firewall Manager menyimpan tag dengan nilai string kosong: “”. Tag sumber daya hanya cocok dengan tag yang memiliki kunci yang sama dan nilai yang sama.

14. Pilih Selanjutnya.
15. Untuk tag Kebijakan, tambahkan tag pengenal apa pun yang ingin Anda tambahkan ke sumber daya kebijakan Manajer Firewall. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.
16. Pilih Selanjutnya.
17. Tinjau pengaturan kebijakan baru dan kembali ke halaman mana pun yang Anda perlukan untuk penyesuaian apa pun.

    Periksa untuk memastikan bahwa tindakan Kebijakan disetel ke Identifikasi sumber daya yang tidak mematuhi aturan kebijakan, tetapi jangan diperbaiki secara otomatis. Ini memungkinkan Anda untuk meninjau perubahan yang akan dibuat kebijakan Anda sebelum Anda mengaktifkannya.
18. Jika Anda puas dengan kebijakan ini, pilih Create policy (Buat kebijakan).

    Di panel AWS Firewall Manager kebijakan, kebijakan Anda harus dicantumkan. Ini mungkin akan menunjukkan Pending di bawah judul akun dan itu akan menunjukkan status pengaturan remediasi otomatis. Pembuatan kebijakan dapat memakan waktu beberapa menit. Setelah Status tertunda diganti dengan jumlah akun, Anda dapat memilih nama kebijakan untuk menjelajahi status kepatuhan akun dan sumber daya. Untuk informasi, lihat Melihat informasi kepatuhan untuk suatu AWS Firewall Manager kebijakan

Lanjutkan ke Langkah 3: (Opsional) memberi wewenang kepada Tim Respons Shield (SRT).

Langkah 3: (Opsional) memberi wewenang kepada Tim Respons Shield (SRT)

Salah satu AWS Shield Advanced keuntungannya adalah dukungan dari Shield Response Team (SRT). Ketika Anda mengalami potensi serangan DDoS, Anda dapat menghubungi AWS Support Pusat. Jika perlu, Support Center meningkatkan masalah Anda ke SRT. SRT membantu Anda menganalisis aktivitas yang mencurigakan dan membantu Anda dalam mengurangi masalah. Mitigasi ini sering melibatkan pembuatan atau pembaruan AWS WAF aturan dan ACL web di akun Anda. SRT dapat memeriksa AWS WAF konfigurasi Anda dan membuat atau memperbarui AWS WAF aturan dan ACL web untuk Anda, tetapi tim memerlukan otorisasi Anda untuk melakukannya. Kami merekomendasikan bahwa sebagai bagian dari pengaturan AWS Shield Advanced, Anda secara

proaktif memberikan SRT dengan otorisasi yang diperlukan. Memberikan otorisasi sebelumnya membantu mencegah penundaan mitigasi jika terjadi serangan yang sebenarnya.

Anda mengotorisasi dan menghubungi SRT di tingkat akun. Artinya, pemilik akun, bukan administrator Firewall Manager, harus melakukan langkah-langkah berikut untuk mengotorisasi SRT untuk mengurangi potensi serangan. Administrator Firewall Manager dapat mengotorisasi SRT hanya untuk akun yang mereka miliki. Demikian juga, hanya pemilik akun yang dapat menghubungi SRT untuk mendapatkan dukungan.

> **Note**
>
> Untuk menggunakan layanan SRT, Anda harus berlangganan paket Business Support atau paket Enterprise Support.

Untuk mengotorisasi SRT untuk mengurangi potensi serangan atas nama Anda, ikuti instruksi di. Dukungan Shield Response Team (SRT) Anda dapat mengubah akses dan izin SRT kapan saja dengan menggunakan langkah yang sama.

Lanjutkan ke Langkah 4: Konfigurasikan notifikasi Amazon SNS dan alarm Amazon CloudWatch .

Langkah 4: Konfigurasikan notifikasi Amazon SNS dan alarm Amazon CloudWatch

Anda dapat melanjutkan dari langkah ini tanpa mengonfigurasi notifikasi CloudWatch atau alarm Amazon SNS. Namun, mengonfigurasi alarm dan notifikasi ini secara signifikan meningkatkan visibilitas Anda ke kemungkinan peristiwa DDoS.

Anda dapat memantau sumber daya yang dilindungi untuk potensi aktivitas DDoS menggunakan Amazon SNS. Untuk menerima pemberitahuan kemungkinan serangan, buat topik Amazon SNS untuk setiap Wilayah.

Untuk membuat topik Amazon SNS di Firewall Manager (konsol)

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

> **Note**
>
> Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

2. Di panel navigasi, di bawah AWS FMS, pilih Pengaturan.
3. Pilih Buat topik baru.
4. Masukkan nama topik.
5. Masukkan alamat email tempat pesan Amazon SNS akan dikirim, lalu pilih Tambahkan alamat email.
6. Pilih Perbarui konfigurasi SNS.

Konfigurasikan CloudWatch alarm Amazon

Shield Deteksi catatan lanjutan, mitigasi, dan metrik kontributor teratas CloudWatch yang dapat Anda pantau. Untuk informasi lebih lanjut, lihatAWS Shield Advanced metrik. CloudWatch menimbulkan biaya tambahan. Untuk CloudWatch harga, lihat CloudWatch Harga Amazon.

Untuk membuat CloudWatch alarm, ikuti petunjuk di Menggunakan CloudWatch Alarm Amazon. Secara default, Shield Advanced mengonfigurasi CloudWatch untuk mengingatkan Anda setelah hanya satu indikator peristiwa DDoS potensial. Jika diperlukan, Anda dapat menggunakan CloudWatch konsol untuk mengubah pengaturan ini agar mengingatkan Anda hanya setelah beberapa indikator terdeteksi.

> **Note**
>
> Selain alarm, Anda juga dapat menggunakan CloudWatch dasbor untuk memantau potensi aktivitas DDoS. Dasbor mengumpulkan dan memproses data mentah dari Shield Advanced menjadi metrik hampir real-time yang dapat dibaca. Anda dapat menggunakan statistik di Amazon CloudWatch untuk mendapatkan perspektif tentang kinerja aplikasi atau layanan web Anda. Untuk informasi selengkapnya, lihat Apa yang ada CloudWatch di Panduan CloudWatch Pengguna Amazon.
> Untuk petunjuk tentang membuat CloudWatch dasbor, lihatPemantauan CloudWatch dengan Amazon. Untuk informasi tentang metrik Shield Advanced tertentu yang dapat ditambahkan ke dasbor, lihatAWS Shield Advanced metrik.

Setelah menyelesaikan konfigurasi Shield Advanced, biasakan diri Anda dengan opsi untuk melihat acara diVisibilitas ke acara DDoS.

Memulai AWS Firewall Manager kebijakan grup keamanan Amazon VPC

AWS Firewall Manager Untuk mengaktifkan grup keamanan Amazon VPC di seluruh organisasi Anda, lakukan langkah-langkah berikut secara berurutan.

Topik

- Langkah 1: Selesaikan prasyarat
- Langkah 2: Buat grup keamanan untuk digunakan dalam kebijakan Anda
- Langkah 3: Buat dan terapkan kebijakan grup keamanan umum

Langkah 1: Selesaikan prasyarat

Ada beberapa langkah wajib untuk mempersiapkan akun Anda AWS Firewall Manager. Langkah-langkah tersebut dijelaskan dalamAWS Firewall Manager prasyarat. Lengkapi semua prasyarat sebelum melanjutkan ke. Langkah 2: Buat grup keamanan untuk digunakan dalam kebijakan Anda

Langkah 2: Buat grup keamanan untuk digunakan dalam kebijakan Anda

Pada langkah ini, Anda membuat grup keamanan yang dapat Anda terapkan di seluruh organisasi menggunakan Firewall Manager.

> **Note**
>
> Untuk tutorial ini, Anda tidak akan menerapkan kebijakan grup keamanan Anda ke sumber daya di organisasi Anda. Anda hanya akan membuat kebijakan dan melihat apa yang akan terjadi jika Anda menerapkan grup keamanan kebijakan ke sumber daya Anda. Anda melakukan ini dengan menonaktifkan remediasi otomatis pada kebijakan.

Jika Anda sudah memiliki grup keamanan umum yang ditentukan, lewati langkah ini dan pergi keLangkah 3: Buat dan terapkan kebijakan grup keamanan umum.

Untuk membuat grup keamanan untuk digunakan dalam kebijakan grup keamanan umum Firewall Manager

- Buat grup keamanan yang dapat Anda terapkan ke semua akun dan sumber daya di organisasi Anda, ikuti panduan di bawah Grup Keamanan untuk VPC Anda di Panduan Pengguna Amazon VPC.

  Untuk informasi tentang opsi aturan grup keamanan, lihat Referensi Aturan Grup Keamanan.

Anda sekarang siap untuk pergi keLangkah 3: Buat dan terapkan kebijakan grup keamanan umum.

Langkah 3: Buat dan terapkan kebijakan grup keamanan umum

Setelah menyelesaikan prasyarat, Anda membuat kebijakan grup keamanan AWS Firewall Manager umum. Kebijakan grup keamanan umum menyediakan grup keamanan yang dikendalikan secara terpusat untuk seluruh AWS organisasi Anda. Ini juga mendefinisikan Akun AWS dan sumber daya yang diterapkan kelompok keamanan. Selain kebijakan grup keamanan umum, Firewall Manager mendukung kebijakan grup keamanan audit konten, untuk mengelola aturan grup keamanan yang digunakan di organisasi Anda, dan penggunaan kebijakan grup keamanan audit, untuk mengelola grup keamanan yang tidak digunakan dan berlebihan. Untuk informasi selengkapnya, lihat Kebijakan kelompok keamanan.

Untuk tutorial ini, Anda membuat kebijakan grup keamanan umum dan mengatur tindakannya agar tidak secara otomatis memperbaiki. Ini memungkinkan Anda untuk melihat apa efek kebijakan tersebut tanpa membuat perubahan pada AWS organisasi Anda.

Untuk membuat kebijakan grup keamanan umum Firewall Manager (konsol)

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Manajer Firewall, lihatAWS Firewall Manager prasyarat.

   > **Note**
   >
   > Untuk informasi tentang menyiapkan akun administrator Manajer Firewall, lihatAWS Firewall Manager prasyarat.

2. Di panel navigasi, pilih Kebijakan keamanan.

3. Jika Anda belum memenuhi prasyarat, konsol menampilkan instruksi tentang cara memperbaiki masalah apa pun. Ikuti petunjuknya, lalu kembali ke langkah ini, untuk membuat kebijakan grup keamanan umum.
4. Pilih Buat kebijakan.
5. Untuk jenis Kebijakan, pilih Grup keamanan.
6. Untuk jenis kebijakan grup Keamanan, pilih Grup keamanan umum.
7. Untuk Wilayah, pilih file Wilayah AWS.
8. Pilih Selanjutnya.
9. Untuk nama Kebijakan, masukkan nama deskriptif.
10. Aturan kebijakan memungkinkan Anda memilih bagaimana grup keamanan dalam kebijakan ini diterapkan dan dipelihara. Untuk tutorial ini, biarkan opsi tidak dicentang.
11. Pilih Tambahkan grup keamanan utama, pilih grup keamanan yang Anda buat untuk tutorial ini, dan pilih Tambahkan grup keamanan.
12. Untuk tindakan Kebijakan, pilih Identifikasi sumber daya yang tidak mematuhi aturan kebijakan, tetapi jangan memulihkan secara otomatis.
13. Pilih Selanjutnya.
14. Akun AWS terpengaruh oleh kebijakan ini memungkinkan Anda untuk mempersempit ruang lingkup kebijakan Anda dengan menentukan akun untuk disertakan atau dikecualikan. Untuk tutorial ini, pilih Sertakan semua akun di bawah organisasi saya.
15. Untuk jenis Sumber Daya, pilih satu atau beberapa jenis, sesuai dengan sumber daya yang telah Anda tetapkan untuk AWS organisasi Anda.
16. Untuk Sumber Daya, Anda dapat mempersempit cakupan kebijakan menggunakan penandaan, dengan menyertakan atau mengecualikan sumber daya dengan tag yang Anda tentukan. Anda dapat menggunakan inklusi atau pengecualian, dan bukan keduanya. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.

    Jika Anda memasukkan lebih dari satu tag, sumber daya harus memiliki semua tag untuk disertakan atau dikecualikan.

    Tag sumber daya hanya dapat memiliki nilai non-null. Jika Anda menghilangkan nilai untuk tag, Firewall Manager menyimpan tag dengan nilai string kosong: “”. Tag sumber daya hanya cocok dengan tag yang memiliki kunci yang sama dan nilai yang sama.
17. Pilih Selanjutnya.

18. Untuk tag Kebijakan, tambahkan tag pengenal apa pun yang ingin Anda tambahkan ke sumber daya kebijakan Manajer Firewall. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.
19. Pilih Selanjutnya.
20. Tinjau pengaturan kebijakan baru dan kembali ke halaman mana pun yang Anda perlukan untuk penyesuaian apa pun.

    Periksa untuk memastikan bahwa tindakan Kebijakan disetel ke Identifikasi sumber daya yang tidak sesuai dengan aturan kebijakan, tetapi jangan diperbaiki secara otomatis. Ini memungkinkan Anda untuk meninjau perubahan yang akan dibuat kebijakan Anda sebelum Anda mengaktifkannya.
21. Jika Anda puas dengan kebijakan ini, pilih Create policy (Buat kebijakan).

    Di panel AWS Firewall Manager kebijakan, kebijakan Anda harus dicantumkan. Ini mungkin akan menunjukkan Pending di bawah judul akun dan itu akan menunjukkan status pengaturan remediasi otomatis. Pembuatan kebijakan dapat memakan waktu beberapa menit. Setelah Status tertunda diganti dengan jumlah akun, Anda dapat memilih nama kebijakan untuk menjelajahi status kepatuhan akun dan sumber daya. Untuk informasi, lihat Melihat informasi kepatuhan untuk suatu AWS Firewall Manager kebijakan
22. Setelah selesai menjelajah, jika Anda tidak ingin menyimpan kebijakan yang Anda buat untuk tutorial ini, pilih nama kebijakan, pilih Hapus, pilih Bersihkan sumber daya yang dibuat oleh kebijakan ini. , dan akhirnya pilih Hapus.

Untuk informasi selengkapnya tentang kebijakan grup keamanan Firewall Manager, lihatKebijakan kelompok keamanan.

Memulai dengan AWS Firewall Manager kebijakan ACL jaringan Amazon VPC

AWS Firewall Manager Untuk mengaktifkan ACL jaringan di seluruh organisasi Anda, lakukan langkah-langkah di bagian ini secara berurutan.

Untuk informasi tentang ACL jaringan, lihat Mengontrol lalu lintas ke subnet menggunakan ACL jaringan di Panduan Pengguna Amazon VPC.

Topik

- Langkah 1: Selesaikan prasyarat

Langkah 1: Selesaikan prasyarat

Ada beberapa langkah wajib untuk mempersiapkan akun Anda AWS Firewall Manager. Langkah-langkah tersebut dijelaskan dalamAWS Firewall Manager prasyarat. Lengkapi semua prasyarat sebelum melanjutkan ke. Langkah 2: Buat kebijakan ACL jaringan

Langkah 2: Buat kebijakan ACL jaringan

Setelah menyelesaikan prasyarat, Anda membuat kebijakan ACL jaringan Firewall Manager. Kebijakan ACL jaringan menyediakan definisi ACL jaringan yang dikontrol secara terpusat untuk seluruh organisasi Anda. AWS Ini juga mendefinisikan Akun AWS dan subnet yang diterapkan ACL jaringan.

Untuk informasi tentang kebijakan ACL jaringan Manajer Firewall, lihatKebijakan ACL jaringan.

Untuk informasi umum tentang kebijakan ACL jaringan Firewall Manager, lihatKebijakan ACL jaringan.

> **Note**
>
> Untuk tutorial ini, Anda tidak akan menerapkan kebijakan ACL jaringan Anda ke subnet di organisasi Anda. Anda hanya akan membuat kebijakan dan melihat apa yang akan terjadi jika Anda menerapkan ACL jaringan kebijakan ke subnet Anda. Anda melakukan ini dengan menonaktifkan remediasi otomatis pada kebijakan.

Untuk membuat kebijakan ACL jaringan Firewall Manager (konsol)

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Manajer Firewall, lihatAWS Firewall Manager prasyarat.

   > **Note**
   >
   > Untuk informasi tentang menyiapkan akun administrator Manajer Firewall, lihatAWS Firewall Manager prasyarat.

2. Di panel navigasi, pilih Kebijakan keamanan.
3. Jika Anda belum memenuhi prasyarat, konsol menampilkan instruksi tentang cara memperbaiki masalah apa pun. Ikuti instruksi, lalu kembali ke langkah ini, untuk membuat kebijakan ACL jaringan.
4. Pilih Buat kebijakan.
5. Untuk Wilayah, pilih file Wilayah AWS.
6. Untuk jenis Kebijakan, pilih ACL Jaringan.
7. Pilih Selanjutnya.
8. Untuk nama Kebijakan, masukkan nama deskriptif.
9. Untuk aturan kebijakan ACL Jaringan, tentukan aturan pertama dan terakhir untuk lalu lintas masuk dan keluar.

   Anda menentukan aturan ACL jaringan di Firewall Manager mirip dengan cara Anda mendefinisikannya melalui Amazon VPC. Satu-satunya perbedaan adalah, alih-alih menetapkan nomor aturan sendiri, Anda menetapkan urutan untuk menjalankan setiap set aturan, dan kemudian Firewall Manager menetapkan nomor untuk Anda ketika Anda menyimpan kebijakan. Anda dapat menentukan hingga 5 aturan masuk, dibagi dengan cara apa pun antara pertama dan terakhir, dan Anda dapat menentukan hingga 5 aturan keluar.

   Untuk panduan yang menentukan aturan ACL jaringan, lihat Menambahkan dan menghapus aturan ACL jaringan di Panduan Pengguna Amazon VPC.

   Aturan yang Anda tentukan dalam kebijakan Firewall Manager menentukan konfigurasi aturan minimum yang harus dimiliki ACL jaringan agar sesuai dengan kebijakan ACL jaringan. Misalnya, aturan masuk ACL jaringan tidak dapat mematuhi kebijakan kecuali aturan tersebut dimulai sebagai aturan pertama masuk kebijakan, dalam urutan yang sama seperti yang ditentukan dalam kebijakan. Untuk informasi selengkapnya, lihat Kebijakan ACL jaringan.
10. Untuk tindakan Kebijakan, pilih Identifikasi sumber daya yang tidak mematuhi aturan kebijakan, tetapi jangan memulihkan secara otomatis.
11. Pilih Selanjutnya.
12. Akun AWS terpengaruh oleh kebijakan ini memungkinkan Anda untuk mempersempit ruang lingkup kebijakan Anda dengan menentukan akun untuk disertakan atau dikecualikan. Untuk tutorial ini, pilih Sertakan semua akun di bawah organisasi saya.

    Jenis sumber daya untuk kebijakan ACL jaringan selalu subnet.

13. Untuk Sumber Daya, Anda dapat mempersempit cakupan kebijakan menggunakan penandaan, dengan menyertakan atau mengecualikan sumber daya dengan tag yang Anda tentukan. Anda dapat menggunakan inklusi atau pengecualian, dan bukan keduanya. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.

    Jika Anda memasukkan lebih dari satu tag, sumber daya harus memiliki semua tag untuk disertakan atau dikecualikan.

    Tag sumber daya hanya dapat memiliki nilai non-null. Jika Anda menghilangkan nilai untuk tag, Firewall Manager menyimpan tag dengan nilai string kosong: “”. Tag sumber daya hanya cocok dengan tag yang memiliki kunci yang sama dan nilai yang sama.

14. Pilih Selanjutnya.

15. Untuk tag Kebijakan, tambahkan tag pengenal apa pun yang ingin Anda tambahkan ke sumber daya kebijakan Manajer Firewall. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.

16. Pilih Selanjutnya.

17. Tinjau pengaturan kebijakan baru dan kembali ke halaman mana pun yang Anda perlukan untuk penyesuaian apa pun.

    Periksa untuk memastikan bahwa tindakan Kebijakan disetel ke Identifikasi sumber daya yang tidak sesuai dengan aturan kebijakan, tetapi jangan diperbaiki secara otomatis. Ini memungkinkan Anda untuk meninjau perubahan yang akan dibuat kebijakan Anda sebelum Anda mengaktifkannya.

18. Jika Anda puas dengan kebijakan ini, pilih Create policy (Buat kebijakan).

    Di panel AWS Firewall Manager kebijakan, kebijakan Anda harus dicantumkan. Ini mungkin akan menunjukkan Pending di bawah judul akun dan itu akan menunjukkan status pengaturan remediasi otomatis. Pembuatan kebijakan dapat memakan waktu beberapa menit. Setelah Status tertunda diganti dengan jumlah akun, Anda dapat memilih nama kebijakan untuk menjelajahi status kepatuhan akun dan sumber daya. Untuk informasi, lihat Melihat informasi kepatuhan untuk suatu AWS Firewall Manager kebijakan

19. Setelah selesai menjelajah, jika Anda tidak ingin menyimpan kebijakan yang Anda buat untuk tutorial ini, pilih nama kebijakan, pilih Hapus, pilih Bersihkan sumber daya yang dibuat oleh kebijakan ini. , dan akhirnya pilih Hapus.

Untuk informasi selengkapnya tentang kebijakan ACL jaringan Firewall Manager, lihatKebijakan ACL jaringan.

Memulai dengan AWS Firewall ManagerAWS Network Firewall kebijakan

AWS Firewall Manager Untuk mengaktifkan firewall AWS Network Firewall di seluruh organisasi Anda, lakukan langkah-langkah berikut secara berurutan. Untuk informasi tentang kebijakan Firewall Manager Network Firewall, lihatAWS Network Firewall kebijakan.

Topik

- Langkah 1: Lengkapi prasyarat umum
- Langkah 2: Buat grup aturan Network Firewall untuk digunakan dalam kebijakan Anda
- Langkah 3: Buat dan terapkan kebijakan Network Firewall

Langkah 1: Lengkapi prasyarat umum

Ada beberapa langkah wajib untuk mempersiapkan akun Anda AWS Firewall Manager. Langkah-langkah tersebut dijelaskan dalamAWS Firewall Manager prasyarat. Lengkapi semua prasyarat sebelum melanjutkan ke langkah berikutnya.

Langkah 2: Buat grup aturan Network Firewall untuk digunakan dalam kebijakan Anda

Untuk mengikuti tutorial ini, Anda harus terbiasa dengan AWS Network Firewall dan tahu cara mengkonfigurasi grup aturan dan kebijakan firewall.

Anda harus memiliki setidaknya satu grup aturan di Network Firewall yang akan digunakan dalam AWS Firewall Manager kebijakan Anda. Jika Anda belum membuat grup aturan di Network Firewall, lakukan sekarang. Untuk informasi tentang menggunakan Network Firewall, lihat Panduan AWS Network Firewall Pengembang.

Langkah 3: Buat dan terapkan kebijakan Network Firewall

Setelah menyelesaikan prasyarat, Anda membuat kebijakan Network Firewall AWS Firewall Manager . Kebijakan Network Firewall menyediakan firewall yang dikontrol secara AWS Network Firewall terpusat untuk seluruh AWS organisasi Anda. Ini juga mendefinisikan Akun AWS dan sumber daya yang diterapkan firewall.

Untuk informasi selengkapnya tentang cara Firewall Manager mengelola kebijakan Network Firewall, lihatAWS Network Firewall kebijakan.

Untuk membuat kebijakan Firewall Manager Network Firewall (konsol)

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Manajer Firewall, lihatAWS Firewall Manager prasyarat.

   > **Note**
   >
   > Untuk informasi tentang menyiapkan akun administrator Manajer Firewall, lihatAWS Firewall Manager prasyarat.

2. Di panel navigasi, pilih Kebijakan keamanan.
3. Jika Anda belum memenuhi prasyarat, konsol akan menampilkan instruksi tentang cara memperbaiki masalah apa pun. Ikuti petunjuknya, lalu kembali ke langkah ini, untuk membuat kebijakan Network Firewall.
4. Pilih Buat kebijakan keamanan.
5. Untuk jenis Kebijakan, pilih AWS Network Firewall.
6. Untuk Wilayah, pilih file Wilayah AWS.
7. Pilih Selanjutnya.
8. Untuk nama Kebijakan, masukkan nama deskriptif.
9. Konfigurasi kebijakan memungkinkan Anda untuk menentukan kebijakan firewall. Ini adalah proses yang sama dengan yang Anda gunakan di AWS Network Firewall konsol. Anda menambahkan grup aturan yang ingin digunakan dalam kebijakan Anda dan memberikan tindakan stateless default. Untuk tutorial ini, konfigurasikan kebijakan ini seperti yang Anda lakukan pada kebijakan firewall di Network Firewall.

   > **Note**
   >
   > Remediasi otomatis terjadi secara otomatis untuk kebijakan AWS Firewall Manager Network Firewall, sehingga Anda tidak akan melihat opsi untuk memilih untuk tidak melakukan perbaikan otomatis di sini.

10. Pilih Selanjutnya.

11. Untuk titik akhir Firewall, pilih Beberapa titik akhir firewall. Opsi ini menyediakan ketersediaan tinggi untuk firewall Anda. Saat Anda membuat kebijakan, Firewall Manager membuat subnet firewall di setiap Availability Zone tempat Anda memiliki subnet publik untuk dilindungi.
12. Untuk konfigurasi AWS Network Firewall rute, pilih Monitor agar Firewall Manager memantau VPC Anda untuk pelanggaran konfigurasi rute dan beri tahu Anda dengan saran remediasi untuk membantu Anda mematuhi rute. Secara opsional, jika Anda tidak ingin konfigurasi rute Anda dipantau oleh Firewall Manager dan menerima peringatan ini, pilih Nonaktif.

> **Note**
>
> Pemantauan memberi Anda detail tentang sumber daya yang tidak sesuai karena konfigurasi rute yang salah, dan menyarankan tindakan remediasi dari Firewall Manager API. `GetViolationDetails` Misalnya, Network Firewall memberi tahu Anda jika lalu lintas tidak dirutekan melalui titik akhir firewall yang dibuat oleh kebijakan Anda.

> **Warning**
>
> Jika Anda memilih Monitor, Anda tidak dapat mengubahnya menjadi Off di masa mendatang untuk kebijakan yang sama. Anda harus membuat kebijakan baru.

13. Untuk jenis lalu lintas, pilih Tambahkan ke kebijakan firewall untuk merutekan lalu lintas melalui gateway internet.
14. Akun AWS terpengaruh oleh kebijakan ini memungkinkan Anda untuk mempersempit cakupan kebijakan Anda dengan menentukan akun untuk disertakan atau dikecualikan. Untuk tutorial ini, pilih Sertakan semua akun di bawah organisasi saya.

    Jenis sumber daya untuk kebijakan Network Firewall selalu VPC.
15. Untuk Sumber Daya, Anda dapat mempersempit cakupan kebijakan menggunakan penandaan, dengan menyertakan atau mengecualikan sumber daya dengan tag yang Anda tentukan. Anda dapat menggunakan inklusi atau pengecualian, dan bukan keduanya. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.

    Jika Anda memasukkan lebih dari satu tag, sumber daya harus memiliki semua tag untuk disertakan atau dikecualikan.

Tag sumber daya hanya dapat memiliki nilai non-null. Jika Anda menghilangkan nilai untuk tag, Firewall Manager menyimpan tag dengan nilai string kosong: “”. Tag sumber daya hanya cocok dengan tag yang memiliki kunci yang sama dan nilai yang sama.

16. Pilih Selanjutnya.
17. Untuk tag Kebijakan, tambahkan tag pengenal apa pun yang ingin Anda tambahkan ke sumber daya kebijakan Manajer Firewall. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.
18. Pilih Selanjutnya.
19. Tinjau pengaturan kebijakan baru dan kembali ke halaman mana pun yang Anda perlukan untuk penyesuaian apa pun.

    Periksa untuk memastikan bahwa tindakan Kebijakan disetel ke Identifikasi sumber daya yang tidak sesuai dengan aturan kebijakan, tetapi jangan diperbaiki secara otomatis. Ini memungkinkan Anda untuk meninjau perubahan yang akan dibuat kebijakan Anda sebelum Anda mengaktifkannya.
20. Jika Anda puas dengan kebijakan ini, pilih Create policy (Buat kebijakan).

    Di panel AWS Firewall Manager kebijakan, kebijakan Anda harus dicantumkan. Ini mungkin akan menunjukkan Pending di bawah judul akun dan itu akan menunjukkan status pengaturan remediasi otomatis. Pembuatan kebijakan dapat memakan waktu beberapa menit. Setelah Status tertunda diganti dengan jumlah akun, Anda dapat memilih nama kebijakan untuk menjelajahi status kepatuhan akun dan sumber daya. Untuk informasi, lihat Melihat informasi kepatuhan untuk suatu AWS Firewall Manager kebijakan
21. Setelah selesai menjelajah, jika Anda tidak ingin menyimpan kebijakan yang Anda buat untuk tutorial ini, pilih nama kebijakan, pilih Hapus, pilih Bersihkan sumber daya yang dibuat oleh kebijakan ini. , dan akhirnya pilih Hapus.

Untuk informasi selengkapnya tentang kebijakan Firewall Manager Network Firewall, lihatAWS Network Firewall kebijakan.

Memulai kebijakan AWS Firewall Manager DNS Firewall

AWS Firewall Manager Untuk mengaktifkan Amazon Route 53 Resolver DNS Firewall di seluruh organisasi Anda, lakukan langkah-langkah berikut secara berurutan. Untuk informasi tentang kebijakan Firewall Manager DNS Firewall, lihatKebijakan Firewall DNS Resolver Amazon Route 53.

Topik

Langkah 1: Lengkapi prasyarat umum

Ada beberapa langkah wajib untuk mempersiapkan akun Anda AWS Firewall Manager. Langkah-langkah tersebut dijelaskan dalamAWS Firewall Manager prasyarat. Lengkapi semua prasyarat sebelum melanjutkan ke langkah berikutnya.

Langkah 2: Buat grup aturan DNS Firewall untuk digunakan dalam kebijakan Anda

Untuk mengikuti tutorial ini, Anda harus terbiasa dengan Amazon Route 53 Resolver DNS Firewall dan tahu cara mengkonfigurasi grup aturannya.

Anda harus memiliki setidaknya satu grup aturan di DNS Firewall yang akan digunakan dalam AWS Firewall Manager kebijakan Anda. Jika Anda belum membuat grup aturan di DNS Firewall, lakukan sekarang. Untuk informasi tentang menggunakan DNS Firewall, lihat Amazon Route 53 Resolver DNS Firewall di Panduan Pengembang Amazon Route 53.

Langkah 3: Buat dan terapkan kebijakan DNS Firewall

Setelah menyelesaikan prasyarat, Anda membuat kebijakan DNS Firewall. AWS Firewall Manager Kebijakan DNS Firewall menyediakan sekumpulan asosiasi grup aturan DNS Firewall yang dikontrol secara terpusat untuk seluruh organisasi Anda. AWS Ini juga mendefinisikan Akun AWS dan sumber daya yang diterapkan firewall.

Untuk informasi selengkapnya tentang cara Firewall Manager mengelola asosiasi grup aturan DNS Firewall, lihatKebijakan Firewall DNS Resolver Amazon Route 53.

Untuk membuat kebijakan Firewall Manager DNS Firewall (konsol)

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Manajer Firewall, lihatAWS Firewall Manager prasyarat.
2. Di panel navigasi, pilih Kebijakan keamanan.

3. Jika Anda belum memenuhi prasyarat, konsol akan menampilkan instruksi tentang cara memperbaiki masalah apa pun. Ikuti petunjuknya, lalu kembali ke langkah ini, untuk membuat kebijakan DNS Firewall.
4. Pilih Buat kebijakan keamanan.
5. Untuk jenis Kebijakan, pilih Amazon Route 53 Resolver DNS Firewall.
6. Untuk Wilayah, pilih file Wilayah AWS.
7. Pilih Selanjutnya.
8. Untuk nama Kebijakan, masukkan nama deskriptif.
9. Konfigurasi kebijakan memungkinkan Anda menentukan asosiasi grup aturan DNS Firewall yang ingin Anda kelola dari Firewall Manager. Anda menambahkan grup aturan yang ingin Anda gunakan dalam kebijakan Anda. Anda dapat menentukan asosiasi untuk mengevaluasi terlebih dahulu untuk VPC Anda dan satu untuk mengevaluasi terakhir. Untuk tutorial ini, tambahkan satu atau dua asosiasi kelompok aturan, tergantung pada kebutuhan Anda.
10. Pilih Selanjutnya.
11. Akun AWS terpengaruh oleh kebijakan ini memungkinkan Anda untuk mempersempit ruang lingkup kebijakan Anda dengan menentukan akun untuk disertakan atau dikecualikan. Untuk tutorial ini, pilih Sertakan semua akun di bawah organisasi saya.

    Jenis sumber daya untuk kebijakan DNS Firewall selalu VPC.
12. Untuk Sumber Daya, Anda dapat mempersempit cakupan kebijakan menggunakan penandaan, dengan menyertakan atau mengecualikan sumber daya dengan tag yang Anda tentukan. Anda dapat menggunakan inklusi atau pengecualian, dan bukan keduanya. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.

    Jika Anda memasukkan lebih dari satu tag, sumber daya harus memiliki semua tag untuk disertakan atau dikecualikan.

    Tag sumber daya hanya dapat memiliki nilai non-null. Jika Anda menghilangkan nilai untuk tag, Firewall Manager menyimpan tag dengan nilai string kosong: “”. Tag sumber daya hanya cocok dengan tag yang memiliki kunci yang sama dan nilai yang sama.
13. Pilih Selanjutnya.
14. Untuk tag Kebijakan, tambahkan tag pengenal apa pun yang ingin Anda tambahkan ke sumber daya kebijakan Manajer Firewall. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.
15. Pilih Selanjutnya.

16. Tinjau pengaturan kebijakan baru dan kembali ke halaman mana pun yang Anda perlukan untuk penyesuaian apa pun.

    Periksa untuk memastikan bahwa tindakan Kebijakan disetel ke Identifikasi sumber daya yang tidak sesuai dengan aturan kebijakan, tetapi jangan diperbaiki secara otomatis. Ini memungkinkan Anda untuk meninjau perubahan yang akan dibuat kebijakan Anda sebelum Anda mengaktifkannya.

17. Jika Anda puas dengan kebijakan ini, pilih Create policy (Buat kebijakan).

    Di panel AWS Firewall Manager kebijakan, kebijakan Anda harus dicantumkan. Ini mungkin akan menunjukkan Pending di bawah judul akun dan itu akan menunjukkan status pengaturan remediasi otomatis. Pembuatan kebijakan dapat memakan waktu beberapa menit. Setelah Status tertunda diganti dengan jumlah akun, Anda dapat memilih nama kebijakan untuk menjelajahi status kepatuhan akun dan sumber daya. Untuk informasi, lihat Melihat informasi kepatuhan untuk suatu AWS Firewall Manager kebijakan

18. Setelah selesai menjelajah, jika Anda tidak ingin menyimpan kebijakan yang Anda buat untuk tutorial ini, pilih nama kebijakan, pilih Hapus, pilih Bersihkan sumber daya yang dibuat oleh kebijakan ini. , dan akhirnya pilih Hapus.

Untuk informasi selengkapnya tentang kebijakan Firewall Manager DNS Firewall, lihatKebijakan Firewall DNS Resolver Amazon Route 53.

Memulai dengan kebijakan AWS Firewall Manager Palo Alto Networks Cloud Next Generation Firewall

Untuk mengaktifkan kebijakan Palo Alto Networks Cloud Next Generation Firewall (NGFW), lakukan langkah-langkah berikut secara berurutan. AWS Firewall Manager Untuk informasi tentang kebijakan Palo Alto Networks Cloud NGFW, lihat. Kebijakan Palo Alto Networks Cloud NGFW

Topik

- Langkah 1: Lengkapi prasyarat umum
- Langkah 2: Lengkapi prasyarat kebijakan Palo Alto Networks Cloud NGFW
- Langkah 3: Buat dan terapkan kebijakan Palo Alto Networks Cloud NGFW

Langkah 1: Lengkapi prasyarat umum

Ada beberapa langkah wajib untuk mempersiapkan akun Anda AWS Firewall Manager. Langkah-langkah tersebut dijelaskan dalamAWS Firewall Manager prasyarat. Lengkapi semua prasyarat sebelum melanjutkan ke langkah berikutnya.

Langkah 2: Lengkapi prasyarat kebijakan Palo Alto Networks Cloud NGFW

Ada beberapa langkah wajib tambahan yang harus Anda selesaikan untuk menggunakan kebijakan Palo Alto Networks Cloud NGFW. Langkah-langkah tersebut dijelaskan dalamPrasyarat kebijakan Firewall Generasi Berikutnya Palo Alto Networks Cloud. Lengkapi semua prasyarat sebelum melanjutkan ke langkah berikutnya.

Langkah 3: Buat dan terapkan kebijakan Palo Alto Networks Cloud NGFW

Setelah menyelesaikan prasyarat, Anda membuat kebijakan AWS Firewall Manager Palo Alto Networks Cloud NGFW.

Untuk informasi selengkapnya tentang kebijakan Firewall Manager untuk Palo Alto Networks Cloud NGFW, lihat. Kebijakan Palo Alto Networks Cloud NGFW

Untuk membuat kebijakan Firewall Manager untuk Palo Alto Networks Cloud NGFW (konsol)

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Manajer Firewall, lihatAWS Firewall Manager prasyarat.

   > **Note**
   >
   > Untuk informasi tentang menyiapkan akun administrator Manajer Firewall, lihatAWS Firewall Manager prasyarat.

2. Di panel navigasi, pilih Kebijakan keamanan.
3. Pilih Buat kebijakan.
4. Untuk jenis Kebijakan, pilih Palo Alto Networks Cloud NGFW. Jika Anda belum berlangganan layanan Palo Alto Networks Cloud NGFW di AWS Marketplace, Anda harus melakukannya terlebih dahulu. Untuk berlangganan AWS Marketplace, pilih Lihat detail AWS Marketplace.

5. Untuk model Deployment, pilih model Terdistribusi atau model Terpusat. Model penerapan menentukan cara Firewall Manager mengelola titik akhir untuk kebijakan tersebut. Dengan model terdistribusi, Firewall Manager mempertahankan titik akhir firewall di setiap VPC yang berada dalam cakupan kebijakan. Dengan model terpusat, Firewall Manager mempertahankan satu titik akhir dalam VPC inspeksi.
6. Untuk Wilayah, pilih file Wilayah AWS. Untuk melindungi sumber daya di beberapa Wilayah, Anda harus membuat kebijakan terpisah untuk setiap Wilayah.
7. Pilih Selanjutnya.
8. Untuk nama Kebijakan, masukkan nama deskriptif.
9. Dalam konfigurasi kebijakan, pilih kebijakan firewall Palo Alto Networks Cloud NGFW untuk dikaitkan dengan kebijakan ini. Daftar kebijakan firewall Palo Alto Networks Cloud NGFW berisi semua kebijakan firewall Palo Alto Networks Cloud NGFW yang terkait dengan penyewa Palo Alto Networks Cloud NGFW Anda. Untuk informasi tentang membuat dan mengelola kebijakan firewall Palo Alto Networks Cloud NGFW, lihat panduan Deploy Palo Alto Networks Cloud NGFW untuk AWS Firewall Manager topik di Palo Alto Networks Cloud NGFW untuk AWS panduan penerapan. AWS
10. Untuk pencatatan Palo Alto Networks Cloud NGFW - opsional, pilih jenis log Palo Alto Networks Cloud NGFW mana yang akan dicatat untuk kebijakan Anda. Untuk informasi tentang jenis log Palo Alto Networks Cloud NGFW, lihat Mengkonfigurasi Logging untuk Palo Alto Networks Cloud NGFW AWS di Palo Alto Networks Cloud NGFW untuk panduan penerapan. AWS

    Untuk tujuan log, tentukan kapan Firewall Manager harus menulis log ke.
11. Pilih Selanjutnya.
12. Di bawah Konfigurasi titik akhir firewall pihak ketiga lakukan salah satu hal berikut, tergantung pada apakah Anda menggunakan model penyebaran terdistribusi atau terpusat untuk membuat titik akhir firewall Anda:

    - Jika Anda menggunakan model penerapan terdistribusi untuk kebijakan ini, di bawah Availability Zones, pilih Availability Zones untuk membuat endpoint firewall. Anda dapat memilih Availability Zones berdasarkan nama Availability Zone atau dengan Availability Zone ID.
    - Jika Anda menggunakan model penerapan terpusat untuk kebijakan ini, dalam konfigurasi AWS Firewall Manager titik akhir di bawah konfigurasi VPC Inspeksi, masukkan ID AWS akun pemilik VPC inspeksi, dan ID VPC VPC inspeksi.

- Di Availability Zones, pilih Availability Zones untuk membuat endpoint firewall. Anda dapat memilih Availability Zones berdasarkan nama Availability Zone atau dengan Availability Zone ID.

13. Pilih Selanjutnya.
14. Untuk cakupan Kebijakan, berdasarkan kebijakan Akun AWS ini berlaku untuk, pilih opsi sebagai berikut:

    - Jika Anda ingin menerapkan kebijakan ke semua akun di organisasi Anda, tinggalkan pilihan default, Sertakan semua akun di AWS organisasi saya.
    - Jika Anda ingin menerapkan kebijakan hanya untuk akun atau akun tertentu yang berada di unit AWS Organizations organisasi tertentu (OU), pilih Sertakan hanya akun dan unit organisasi yang ditentukan, lalu tambahkan akun dan OU yang ingin Anda sertakan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.
    - Jika Anda ingin menerapkan kebijakan untuk semua kecuali satu set akun atau unit AWS Organizations organisasi (OU) tertentu, pilih Kecualikan akun dan unit organisasi yang ditentukan, dan sertakan semua akun lainnya, lalu tambahkan akun dan OU yang ingin Anda kecualikan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.

    Anda hanya dapat memilih salah satu opsi.

    Setelah menerapkan kebijakan, Firewall Manager secara otomatis mengevaluasi akun baru apa pun terhadap pengaturan Anda. Misalnya, jika Anda hanya menyertakan akun tertentu, Firewall Manager tidak menerapkan kebijakan tersebut ke akun baru mana pun. Sebagai contoh lain, jika Anda menyertakan OU, ketika Anda menambahkan akun ke OU atau ke salah satu OU anaknya, Firewall Manager secara otomatis menerapkan kebijakan tersebut ke akun baru.

    Jenis sumber daya untuk kebijakan Network Firewall adalah VPC.

15. Untuk Sumber Daya, Anda dapat mempersempit cakupan kebijakan menggunakan penandaan, dengan menyertakan atau mengecualikan sumber daya dengan tag yang Anda tentukan. Anda dapat menggunakan inklusi atau pengecualian, dan bukan keduanya. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.

    Jika Anda memasukkan lebih dari satu tag, sumber daya harus memiliki semua tag untuk disertakan atau dikecualikan.

Tag sumber daya hanya dapat memiliki nilai non-null. Jika Anda menghilangkan nilai untuk tag, Firewall Manager menyimpan tag dengan nilai string kosong: “”. Tag sumber daya hanya cocok dengan tag yang memiliki kunci yang sama dan nilai yang sama.

16. Untuk akses lintas akun Grant, pilih Unduh AWS CloudFormation template. Ini mengunduh AWS CloudFormation template yang dapat Anda gunakan untuk membuat AWS CloudFormation tumpukan. Tumpukan ini menciptakan AWS Identity and Access Management peran yang memberikan izin lintas akun Firewall Manager untuk mengelola sumber daya Palo Alto Networks Cloud NGFW. Untuk informasi tentang tumpukan, lihat Bekerja dengan tumpukan di AWS CloudFormation Panduan Pengguna.
17. Pilih Selanjutnya.
18. Untuk tag Kebijakan, tambahkan tag pengenal apa pun yang ingin Anda tambahkan ke sumber daya kebijakan Manajer Firewall. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.
19. Pilih Selanjutnya.
20. Tinjau pengaturan kebijakan baru dan kembali ke halaman mana pun yang Anda perlukan untuk penyesuaian apa pun.

    Periksa untuk memastikan bahwa tindakan Kebijakan disetel ke Identifikasi sumber daya yang tidak sesuai dengan aturan kebijakan, tetapi jangan diperbaiki secara otomatis. Ini memungkinkan Anda untuk meninjau perubahan yang akan dibuat kebijakan Anda sebelum Anda mengaktifkannya.
21. Jika Anda puas dengan kebijakan ini, pilih Create policy (Buat kebijakan).

    Di panel AWS Firewall Manager kebijakan, kebijakan Anda harus dicantumkan. Ini mungkin akan menunjukkan Pending di bawah judul akun dan itu akan menunjukkan status pengaturan remediasi otomatis. Pembuatan kebijakan dapat memakan waktu beberapa menit. Setelah Status tertunda diganti dengan jumlah akun, Anda dapat memilih nama kebijakan untuk menjelajahi status kepatuhan akun dan sumber daya. Untuk informasi, lihat Melihat informasi kepatuhan untuk suatu AWS Firewall Manager kebijakan

Untuk informasi selengkapnya tentang kebijakan Firewall Manager Palo Alto Networks Cloud NGFW, lihat. Kebijakan Palo Alto Networks Cloud NGFW

Memulai dengan kebijakan AWS Firewall Manager Fortigate CNF

Fortigate Cloud Native Firewall (CNF) sebagai Layanan adalah layanan firewall pihak ketiga yang dapat Anda gunakan untuk kebijakan Anda. AWS Firewall Manager Dengan Fortigate CNF for Firewall Manager, Anda dapat membuat dan menyebarkan sumber daya dan kumpulan kebijakan Fortigate CNF secara terpusat di semua akun Anda. AWS Untuk menggunakan AWS Firewall Manager untuk mengaktifkan kebijakan CNF Fortigate, lakukan langkah-langkah berikut secara berurutan. Untuk informasi lebih lanjut tentang kebijakan Fortigate CNF, lihat. Fortigate Cloud Native Firewall (CNF) sebagai kebijakan Layanan

Topik

Langkah 1: Lengkapi prasyarat umum

Ada beberapa langkah wajib untuk mempersiapkan akun Anda AWS Firewall Manager. Langkah-langkah tersebut dijelaskan dalamAWS Firewall Manager prasyarat. Lengkapi semua prasyarat sebelum melanjutkan ke langkah berikutnya.

Langkah 2: Lengkapi prasyarat kebijakan Fortigate CNF

Ada langkah-langkah wajib tambahan yang harus Anda selesaikan untuk menggunakan kebijakan Fortigate CNF. Langkah-langkah tersebut dijelaskan dalamFortigate Cloud Native Firewall (CNF) sebagai prasyarat kebijakan Layanan. Lengkapi semua prasyarat sebelum melanjutkan ke langkah berikutnya.

Langkah 3: Buat dan terapkan kebijakan Fortigate CNF

Setelah menyelesaikan prasyarat, Anda membuat kebijakan Fortigate CNF. AWS Firewall Manager

Untuk informasi selengkapnya tentang kebijakan Firewall Manager untuk Fortigate CNF, lihat. Fortigate Cloud Native Firewall (CNF) sebagai kebijakan Layanan

Untuk membuat kebijakan Firewall Manager untuk Fortigate CNF (konsol)

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk

informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

> **Note**
>
> Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

2. Di panel navigasi, pilih Kebijakan keamanan.
3. Pilih Buat kebijakan.
4. Untuk jenis Kebijakan, pilih Fortigate CNF. Jika Anda belum berlangganan layanan Fortigate CNF di AWS Marketplace, Anda harus melakukannya terlebih dahulu. Untuk berlangganan AWS Marketplace, pilih Lihat detail AWS Marketplace.
5. Untuk model Deployment, pilih model Terdistribusi atau model Terpusat. Model penerapan menentukan cara Firewall Manager mengelola titik akhir untuk kebijakan tersebut. Dengan model terdistribusi, Firewall Manager mempertahankan titik akhir firewall di setiap VPC yang berada dalam cakupan kebijakan. Dengan model terpusat, Firewall Manager mempertahankan satu titik akhir dalam VPC inspeksi.
6. Untuk Wilayah, pilih Wilayah AWS. Untuk melindungi sumber daya di beberapa Wilayah, Anda harus membuat kebijakan terpisah untuk setiap Wilayah.
7. Pilih Selanjutnya.
8.
9. Dalam konfigurasi kebijakan, pilih kebijakan firewall Fortigate CNF untuk dikaitkan dengan kebijakan ini. Daftar kebijakan firewall Fortigate CNF berisi semua kebijakan firewall Fortigate CNF yang terkait dengan penyewa Fortigate CNF Anda. Untuk informasi tentang membuat dan mengelola kebijakan firewall Fortigate CNF, lihat dokumentasi Fortigate CNF.
10. Pilih Selanjutnya.
11. Di bawah Konfigurasi titik akhir firewall pihak ketiga lakukan salah satu hal berikut, tergantung pada apakah Anda menggunakan model penyebaran terdistribusi atau terpusat untuk membuat titik akhir firewall Anda:

    - Jika Anda menggunakan model penerapan terdistribusi untuk kebijakan ini, di bawah Availability Zones, pilih Availability Zones untuk membuat endpoint firewall. Anda dapat memilih Availability Zones berdasarkan nama Availability Zone atau dengan Availability Zone ID.

- Jika Anda menggunakan model penerapan terpusat untuk kebijakan ini, dalam konfigurasi AWS Firewall Manager titik akhir di bawah konfigurasi VPC Inspeksi, masukkan ID AWS akun pemilik VPC inspeksi, dan ID VPC VPC inspeksi.
  - Di Availability Zones, pilih Availability Zones untuk membuat endpoint firewall. Anda dapat memilih Availability Zones berdasarkan nama Availability Zone atau dengan Availability Zone ID.

12. Pilih Selanjutnya.
13. Untuk cakupan Kebijakan, berdasarkan kebijakan Akun AWS ini berlaku untuk, pilih opsi sebagai berikut:

    - Jika Anda ingin menerapkan kebijakan ke semua akun di organisasi Anda, tinggalkan pilihan default, Sertakan semua akun di AWS organisasi saya.
    - Jika Anda ingin menerapkan kebijakan hanya untuk akun atau akun tertentu yang berada di unit AWS Organizations organisasi tertentu (OU), pilih Sertakan hanya akun dan unit organisasi yang ditentukan, lalu tambahkan akun dan OU yang ingin Anda sertakan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.
    - Jika Anda ingin menerapkan kebijakan untuk semua kecuali satu set akun atau unit AWS Organizations organisasi (OU) tertentu, pilih Kecualikan akun dan unit organisasi yang ditentukan, dan sertakan semua akun lainnya, lalu tambahkan akun dan OU yang ingin Anda kecualikan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.

    Anda hanya dapat memilih salah satu opsi.

    Setelah menerapkan kebijakan, Firewall Manager secara otomatis mengevaluasi akun baru apa pun terhadap pengaturan Anda. Misalnya, jika Anda hanya menyertakan akun tertentu, Firewall Manager tidak menerapkan kebijakan tersebut ke akun baru mana pun. Sebagai contoh lain, jika Anda menyertakan OU, ketika Anda menambahkan akun ke OU atau ke salah satu OU anaknya, Firewall Manager secara otomatis menerapkan kebijakan tersebut ke akun baru.

    Jenis sumber daya untuk kebijakan CNF Fortigate adalah VPC.

14. Untuk Sumber Daya, Anda dapat mempersempit cakupan kebijakan menggunakan penandaan, dengan menyertakan atau mengecualikan sumber daya dengan tag yang Anda tentukan. Anda dapat menggunakan inklusi atau pengecualian, dan bukan keduanya. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.

Jika Anda memasukkan lebih dari satu tag, sumber daya harus memiliki semua tag untuk disertakan atau dikecualikan.

Tag sumber daya hanya dapat memiliki nilai non-null. Jika Anda menghilangkan nilai untuk tag, Firewall Manager menyimpan tag dengan nilai string kosong: “”. Tag sumber daya hanya cocok dengan tag yang memiliki kunci yang sama dan nilai yang sama.

15. Untuk akses lintas akun Grant, pilih Unduh AWS CloudFormation template. Ini mengunduh AWS CloudFormation template yang dapat Anda gunakan untuk membuat AWS CloudFormation tumpukan. Tumpukan ini menciptakan AWS Identity and Access Management peran yang memberikan izin lintas akun Firewall Manager untuk mengelola sumber daya CNF Fortigate. Untuk informasi tentang tumpukan, lihat Bekerja dengan tumpukan di AWS CloudFormation Panduan Pengguna. Untuk membuat tumpukan, Anda memerlukan ID akun dari portal Fortigate CNF.
16. Pilih Selanjutnya.
17. Untuk tag Kebijakan, tambahkan tag pengenal apa pun yang ingin Anda tambahkan ke sumber daya kebijakan Manajer Firewall. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.
18. Pilih Selanjutnya.
19. Tinjau pengaturan kebijakan baru dan kembali ke halaman mana pun yang Anda perlukan untuk penyesuaian apa pun.

    Periksa untuk memastikan bahwa tindakan Kebijakan disetel ke Identifikasi sumber daya yang tidak mematuhi aturan kebijakan, tetapi jangan diperbaiki secara otomatis. Ini memungkinkan Anda untuk meninjau perubahan yang akan dibuat kebijakan Anda sebelum Anda mengaktifkannya.
20. Jika Anda puas dengan kebijakan ini, pilih Create policy (Buat kebijakan).

    Di panel AWS Firewall Manager kebijakan, kebijakan Anda harus dicantumkan. Ini mungkin akan menunjukkan Pending di bawah judul akun dan itu akan menunjukkan status pengaturan remediasi otomatis. Pembuatan kebijakan dapat memakan waktu beberapa menit. Setelah Status tertunda diganti dengan jumlah akun, Anda dapat memilih nama kebijakan untuk menjelajahi status kepatuhan akun dan sumber daya. Untuk informasi, lihat Melihat informasi kepatuhan untuk suatu AWS Firewall Manager kebijakan

Untuk informasi selengkapnya tentang kebijakan Firewall Manager Fortigate CNF, lihat. Fortigate Cloud Native Firewall (CNF) sebagai kebijakan Layanan

Bekerja dengan AWS Firewall Manager kebijakan

AWS Firewall Manager menyediakan jenis kebijakan berikut. Untuk setiap jenis kebijakan, Anda menentukan:

- AWS WAFkebijakan — Firewall Manager mendukung AWS WAF dan kebijakan AWS WAF Klasik. Untuk kedua versi, Anda menentukan sumber daya mana yang dilindungi oleh kebijakan.
  - Jenis AWS WAF kebijakan mengambil kumpulan grup aturan untuk dijalankan pertama dan terakhir di ACL web. Kemudian, di akun tempat Anda menerapkan ACL web, pemilik akun dapat menambahkan aturan dan grup aturan untuk dijalankan di antara dua set.
  - Jenis kebijakan AWS WAF Klasik membutuhkan satu grup aturan untuk dijalankan di ACL web.
- Kebijakan Shield Advanced — Jenis kebijakan ini menerapkan perlindungan Shield Advanced di seluruh organisasi untuk jenis sumber daya yang Anda tentukan.
- Kebijakan grup keamanan Amazon VPC — Jenis kebijakan ini memberi Anda kendali atas grup keamanan yang digunakan di seluruh organisasi dan memungkinkan Anda menerapkan seperangkat aturan dasar di seluruh organisasi.
- Kebijakan daftar kontrol akses jaringan (ACL) Amazon VPC — Jenis kebijakan ini memberi Anda kontrol atas ACL jaringan yang digunakan di seluruh organisasi Anda dan memungkinkan Anda menerapkan kumpulan dasar ACL jaringan di seluruh organisasi Anda.
- Kebijakan Network Firewall — Jenis kebijakan ini menerapkan AWS Network Firewall perlindungan untuk VPC organisasi Anda.
- Kebijakan Amazon Route 53 Resolver DNS Firewall — Kebijakan ini menerapkan perlindungan DNS Firewall ke VPC organisasi Anda.
- Kebijakan firewall pihak ketiga — Jenis kebijakan ini menerapkan perlindungan firewall pihak ketiga. Firewall pihak ketiga tersedia dengan berlangganan melalui konsol AWS Marketplace di AWS Marketplace.
  - Kebijakan Palo Alto Networks Cloud NGFW - Jenis kebijakan ini menerapkan perlindungan Palo Alto Networks Cloud Next Generation Firewall (NGFW) dan aturan Palo Alto Networks Cloud NGFW ke VPC organisasi Anda.
  - Fortigate Cloud Native Firewall (CNF) sebagai kebijakan Layanan — Jenis kebijakan ini menerapkan Fortigate Cloud Native Firewall (CNF) sebagai perlindungan Layanan. Fortigate CNF adalah solusi yang berpusat pada cloud yang memblokir ancaman Zero-Day dan

mengamankan infrastruktur cloud dengan pencegahan ancaman canggih terdepan di industri, firewall aplikasi web pintar (WAF), dan perlindungan API.

Kebijakan Firewall Manager khusus untuk jenis kebijakan individual. Jika ingin menerapkan beberapa jenis kebijakan di seluruh akun, Anda dapat membuat beberapa kebijakan. Anda dapat membuat lebih dari satu kebijakan untuk setiap jenis.

Jika Anda menambahkan akun baru ke organisasi yang Anda buat AWS Organizations, Firewall Manager secara otomatis menerapkan kebijakan tersebut ke sumber daya di akun tersebut yang berada dalam cakupan kebijakan.

Pengaturan umum untuk AWS Firewall Manager kebijakan

AWS Firewall Manager kebijakan terkelola memiliki beberapa pengaturan dan perilaku umum. Untuk semua, Anda menentukan nama dan menentukan cakupan kebijakan, dan Anda dapat menggunakan penandaan sumber daya untuk mengontrol cakupan kebijakan. Anda dapat memilih untuk melihat akun dan sumber daya yang tidak sesuai tanpa mengambil tindakan korektif atau secara otomatis memulihkan sumber daya yang tidak sesuai.

Untuk informasi tentang cakupan kebijakan, lihatAWS Firewall Manager ruang lingkup kebijakan.

Membuat AWS Firewall Manager kebijakan

Langkah-langkah untuk membuat kebijakan bervariasi antara jenis kebijakan yang berbeda. Pastikan untuk menggunakan prosedur untuk jenis kebijakan yang Anda butuhkan.

> **Important**
>
> AWS Firewall Manager tidak mendukung Amazon Route 53 atau AWS Global Accelerator. Jika Anda ingin melindungi sumber daya ini dengan Shield Advanced, Anda tidak dapat menggunakan kebijakan Firewall Manager. Sebagai gantinya, ikuti instruksi diMenambahkan AWS Shield Advanced perlindungan ke AWS sumber daya.

Topik

- Membuat AWS Firewall Manager kebijakan untuk AWS WAF
- Membuat AWS Firewall Manager kebijakan untuk AWS WAF Classic
- Membuat AWS Firewall Manager kebijakan untuk AWS Shield Advanced

- Membuat kebijakan grup keamanan AWS Firewall Manager umum
- Membuat kebijakan grup keamanan audit AWS Firewall Manager konten
- Membuat kebijakan grup keamanan audit AWS Firewall Manager penggunaan
- Membuat kebijakan ACL AWS Firewall Manager jaringan
- Membuat AWS Firewall Manager kebijakan untuk AWS Network Firewall
- Membuat AWS Firewall Manager kebijakan untuk Amazon Route 53 Resolver DNS Firewall
- Membuat AWS Firewall Manager kebijakan untuk Palo Alto Networks Cloud NGFW
- Membuat AWS Firewall Manager kebijakan untuk Fortigate Cloud Native Firewall (CNF) sebagai Layanan

Membuat AWS Firewall Manager kebijakan untuk AWS WAF

Dalam AWS WAF kebijakan Firewall Manager, Anda dapat menggunakan grup aturan terkelola, yang dibuat AWS dan dipelihara oleh AWS Marketplace penjual untuk Anda. Anda juga dapat membuat dan menggunakan grup aturan Anda sendiri. Untuk informasi selengkapnya tentang grup aturan, lihatAWS WAF kelompok aturan.

Jika Anda ingin menggunakan grup aturan Anda sendiri, buat grup tersebut sebelum Anda membuat AWS WAF kebijakan Firewall Manager. Untuk panduan, lihat Mengelola grup aturan Anda sendiri. Untuk menggunakan aturan kustom individual, Anda harus menentukan grup aturan Anda sendiri, menentukan aturan Anda di dalamnya, dan kemudian menggunakan grup aturan dalam kebijakan Anda.

Untuk informasi tentang AWS WAF kebijakan Firewall Manager, lihatAWS WAF kebijakan.

Untuk membuat kebijakan Firewall Manager untuk AWS WAF (konsol)

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

   > **Note**
   >
   > Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

2. Di panel navigasi, pilih Kebijakan keamanan.
3. Pilih Buat kebijakan.
4. Untuk jenis Kebijakan, pilih AWS WAF.
5. Untuk Wilayah, pilih Wilayah AWS. Untuk melindungi CloudFront distribusi Amazon, pilih Global.

   Untuk melindungi sumber daya di beberapa Wilayah (selain CloudFront distribusi), Anda harus membuat kebijakan Firewall Manager terpisah untuk setiap Wilayah.
6. Pilih Selanjutnya.
7. Untuk nama Kebijakan, masukkan nama deskriptif. Firewall Manager menyertakan nama kebijakan dalam nama ACL web yang dikelolanya. Nama ACL web telah `FMManagedWebACLV2-` diikuti dengan nama kebijakan yang Anda masukkan di sini`-`, dan stempel waktu pembuatan ACL web, dalam milidetik UTC. Misalnya, `FMManagedWebACLV2-MyWAFPolicyName-1621880374078`.
8. Untuk inspeksi badan permintaan Web, secara opsional mengubah batas ukuran tubuh. Untuk informasi tentang batas ukuran inspeksi badan, termasuk pertimbangan harga, lihat Mengelola batas ukuran inspeksi tubuh di Panduan AWS WAF Pengembang.
9. Di bawah Aturan kebijakan, tambahkan grup aturan yang AWS WAF ingin Anda evaluasi pertama dan terakhir di ACL web. Untuk menggunakan versi grup aturan AWS WAF terkelola, alihkan Aktifkan pembuatan versi. Manajer akun individual dapat menambahkan aturan dan grup aturan di antara grup aturan pertama Anda dan grup aturan terakhir Anda. Untuk informasi selengkapnya tentang menggunakan grup AWS WAF aturan dalam kebijakan Firewall Manager AWS WAF, lihatAWS WAF kebijakan.

   (Opsional) Untuk menyesuaikan cara ACL web Anda menggunakan grup aturan, pilih Edit. Berikut ini adalah pengaturan kustomisasi umum:

   - Untuk grup aturan terkelola, ganti tindakan aturan untuk beberapa atau semua aturan. Jika Anda tidak menentukan tindakan penggantian untuk aturan, evaluasi menggunakan tindakan aturan yang ditentukan di dalam grup aturan. Untuk informasi tentang opsi ini, lihat Opsi penggantian tindakan untuk grup aturan di Panduan AWS WAF Pengembang.
   - Beberapa grup aturan terkelola mengharuskan Anda untuk menyediakan konfigurasi tambahan. Lihat dokumentasi dari penyedia grup aturan terkelola Anda. Untuk informasi khusus tentang grup aturan Aturan AWS Terkelola, lihat AWS Aturan Terkelola untuk AWS WAF di Panduan AWS WAF Pengembang.

   Setelah selesai dengan pengaturan, pilih Simpan aturan.

10. Tetapkan tindakan default untuk ACL web. Ini adalah tindakan yang diambil AWS WAF ketika permintaan web tidak cocok dengan aturan apa pun di ACL web. Anda dapat menambahkan header kustom dengan tindakan Izinkan, atau respons khusus untuk tindakan Blokir. Untuk informasi selengkapnya tentang tindakan ACL web default, lihatTindakan default ACL web. Untuk informasi tentang menyetel permintaan dan tanggapan web kustom, lihatPermintaan dan tanggapan web yang disesuaikan di AWS WAF.
11. Untuk konfigurasi Logging, pilih Aktifkan logging untuk mengaktifkan logging. Logging memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Pilih tujuan Logging, lalu pilih tujuan logging yang Anda konfigurasikan. Anda harus memilih tujuan logging yang namanya dimulai dengan`aws-waf-logs-`. Untuk informasi tentang mengonfigurasi tujuan AWS WAF pencatatan, lihatMengonfigurasi pencatatan untuk kebijakan AWS WAF.
12. (Opsional) Jika Anda tidak ingin bidang tertentu dan nilainya disertakan dalam log, edit bidang tersebut. Pilih bidang yang akan disunting, lalu pilih Tambah. Ulangi seperlunya untuk menyunting bidang tambahan. Bidang yang disunting muncul seperti `REDACTED` di log. Misalnya, jika Anda menyunting bidang URI, bidang URI di log akan menjadi`REDACTED`.
13. (Opsional) Jika Anda tidak ingin mengirim semua permintaan ke log, tambahkan kriteria dan perilaku pemfilteran Anda. Di bawah Filter log, untuk setiap filter yang ingin Anda terapkan, pilih Tambahkan filter, lalu pilih kriteria pemfilteran Anda dan tentukan apakah Anda ingin menyimpan atau menghapus permintaan yang sesuai dengan kriteria. Ketika Anda selesai menambahkan filter, jika diperlukan, ubah perilaku logging Default. Untuk informasi lebih lanjut, lihat Konfigurasi pencatatan ACL web dalam Panduan Pengembang AWS WAF .
14. Anda dapat menentukan daftar domain Token untuk mengaktifkan berbagi token antara aplikasi yang dilindungi. Token digunakan oleh CAPTCHA dan Challenge tindakan dan oleh SDK integrasi aplikasi yang Anda terapkan saat Anda menggunakan grup aturan Aturan AWS Terkelola untuk pencegahan pengambilalihan akun Kontrol AWS WAF Penipuan (ATP) dan AWS WAF Kontrol Bot.

    Sufiks publik tidak diizinkan. Misalnya, Anda tidak dapat menggunakan `gov.au` atau `co.uk` sebagai domain token.

    Secara default, AWS WAF menerima token hanya untuk domain sumber daya yang dilindungi. Jika Anda menambahkan domain token dalam daftar ini, AWS WAF menerima token untuk semua domain dalam daftar dan untuk domain sumber daya terkait. Untuk informasi lebih lanjut, lihat AWS WAF konfigurasi daftar domain token ACL web dalam Panduan Pengembang AWS WAF .

Anda hanya dapat mengubah CAPTCHA ACL web dan menantang waktu kekebalan saat Anda mengedit ACL web yang ada. Anda dapat menemukan pengaturan ini di bawah halaman detail Kebijakan Manajer Firewall. Untuk informasi tentang pengaturan ini, lihat Kedaluwarsa stempel waktu: waktu kekebalan token AWS WAF. Jika Anda memperbarui konfigurasi Asosiasi, CAPTCHA, Tantangan, atau pengaturan daftar domain Token dalam kebijakan yang ada, Firewall Manager akan menimpa ACL web lokal Anda dengan nilai baru. Namun, jika Anda tidak memperbarui konfigurasi Asosiasi kebijakan, CAPTCHA, Tantangan, atau pengaturan daftar domain Token, nilai di ACL web lokal Anda akan tetap tidak berubah. Untuk informasi tentang opsi ini, lihat CAPTCHAdan Challenge di AWS WAF di Panduan AWS WAF Pengembang.

15. Di bawah manajemen ACL Web, jika Anda ingin Firewall Manager mengelola ACL web yang tidak terkait, aktifkan Kelola ACL web yang tidak terkait. Dengan opsi ini, Firewall Manager membuat ACL web di akun dalam cakupan kebijakan hanya jika ACL web akan digunakan oleh setidaknya satu sumber daya. Jika sewaktu-waktu akun masuk ke cakupan kebijakan, Firewall Manager secara otomatis membuat ACL web di akun jika setidaknya satu sumber daya akan menggunakan ACL web. Setelah mengaktifkan opsi ini, Firewall Manager melakukan pembersihan satu kali dari ACL web yang tidak terkait di akun Anda. Proses pembersihan bisa memakan waktu beberapa jam. Jika sumber daya meninggalkan cakupan kebijakan setelah Firewall Manager membuat ACL web, Firewall Manager memisahkan sumber daya dari ACL web, tetapi tidak akan membersihkan ACL web yang tidak terkait. Firewall Manager hanya membersihkan ACL web yang tidak terkait saat Anda pertama kali mengaktifkan pengelolaan ACL web yang tidak terkait dalam suatu kebijakan.
16. Untuk tindakan Kebijakan, jika Anda ingin membuat ACL web di setiap akun yang berlaku dalam organisasi, tetapi belum menerapkan ACL web ke sumber daya apa pun, pilih Identifikasi sumber daya yang tidak mematuhi aturan kebijakan, tetapi jangan memulihkan secara otomatis dan jangan memilih Kelola ACL web yang tidak terkait. Anda dapat mengubah opsi ini nanti.

    Jika Anda ingin menerapkan kebijakan secara otomatis ke sumber daya dalam lingkup yang ada, pilih Remediasi otomatis sumber daya yang tidak sesuai. Jika Kelola ACL web yang tidak terkait dinonaktifkan, opsi Auto remediate setiap sumber daya yang tidak sesuai akan membuat ACL web di setiap akun yang berlaku dalam organisasi dan mengaitkan ACL web dengan sumber daya di akun. Jika Kelola ACL web yang tidak terkait diaktifkan, opsi Auto remediate semua sumber daya yang tidak sesuai hanya membuat dan mengaitkan ACL web di akun yang memiliki sumber daya yang memenuhi syarat untuk diasosiasikan ke ACL web.

    Saat memilih Remediasi otomatis sumber daya yang tidak sesuai, Anda juga dapat memilih untuk menghapus asosiasi ACL web yang ada dari sumber daya dalam lingkup, untuk ACL web

yang tidak dikelola oleh kebijakan Firewall Manager aktif lainnya. Jika Anda memilih opsi ini, Firewall Manager terlebih dahulu mengaitkan ACL web kebijakan dengan sumber daya, lalu menghapus asosiasi sebelumnya. Jika sumber daya memiliki asosiasi dengan ACL web lain yang dikelola oleh kebijakan Firewall Manager aktif yang berbeda, pilihan ini tidak memengaruhi asosiasi tersebut.

17. Pilih Selanjutnya.
18. Untuk kebijakan Akun AWS ini berlaku, pilih opsi sebagai berikut:

    - Jika Anda ingin menerapkan kebijakan ke semua akun di organisasi Anda, tinggalkan pilihan default, Sertakan semua akun di AWS organisasi saya.
    - Jika Anda ingin menerapkan kebijakan hanya untuk akun atau akun tertentu yang berada di unit AWS Organizations organisasi tertentu (OU), pilih Sertakan hanya akun dan unit organisasi yang ditentukan, lalu tambahkan akun dan OU yang ingin Anda sertakan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.
    - Jika Anda ingin menerapkan kebijakan untuk semua kecuali satu set akun atau unit AWS Organizations organisasi (OU) tertentu, pilih Kecualikan akun dan unit organisasi yang ditentukan, dan sertakan semua akun lainnya, lalu tambahkan akun dan OU yang ingin Anda kecualikan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.

    Anda hanya dapat memilih salah satu opsi.

    Setelah menerapkan kebijakan, Firewall Manager secara otomatis mengevaluasi akun baru apa pun terhadap pengaturan Anda. Misalnya, jika Anda hanya menyertakan akun tertentu, Firewall Manager tidak menerapkan kebijakan tersebut ke akun baru mana pun. Sebagai contoh lain, jika Anda menyertakan OU, ketika Anda menambahkan akun ke OU atau ke salah satu OU anaknya, Firewall Manager secara otomatis menerapkan kebijakan tersebut ke akun baru.
19. Untuk jenis Sumber Daya, pilih jenis sumber daya yang ingin Anda lindungi.
20. Untuk Sumber Daya, Anda dapat mempersempit cakupan kebijakan menggunakan penandaan, dengan menyertakan atau mengecualikan sumber daya dengan tag yang Anda tentukan. Anda dapat menggunakan inklusi atau pengecualian, dan bukan keduanya. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.

    Jika Anda memasukkan lebih dari satu tag, sumber daya harus memiliki semua tag untuk disertakan atau dikecualikan.

Tag sumber daya hanya dapat memiliki nilai non-null. Jika Anda menghilangkan nilai untuk tag, Firewall Manager menyimpan tag dengan nilai string kosong: “”. Tag sumber daya hanya cocok dengan tag yang memiliki kunci yang sama dan nilai yang sama.

21. Pilih Selanjutnya.
22. Untuk tag Kebijakan, tambahkan tag pengenal apa pun yang ingin Anda tambahkan ke sumber daya kebijakan Manajer Firewall. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.
23. Pilih Selanjutnya.
24. Tinjau pengaturan kebijakan baru dan kembali ke halaman mana pun yang Anda perlukan untuk penyesuaian apa pun.

    Jika Anda puas dengan kebijakan ini, pilih Create policy (Buat kebijakan). Di panel AWS Firewall Manager kebijakan, kebijakan Anda harus dicantumkan. Ini mungkin akan menunjukkan Pending di bawah judul akun dan itu akan menunjukkan status pengaturan remediasi otomatis. Pembuatan kebijakan dapat memakan waktu beberapa menit. Setelah Status tertunda diganti dengan jumlah akun, Anda dapat memilih nama kebijakan untuk menjelajahi status kepatuhan akun dan sumber daya. Untuk informasi, lihat Melihat informasi kepatuhan untuk suatu AWS Firewall Manager kebijakan

Membuat AWS Firewall Manager kebijakan untuk AWS WAF Classic

Untuk membuat kebijakan Firewall Manager untuk AWS WAF Classic (konsol)

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

   > **Note**
   >
   > Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

2. Di panel navigasi, pilih Kebijakan keamanan.
3. Pilih Buat kebijakan.
4. Untuk jenis Kebijakan, pilih AWS WAF Klasik.

5. Jika Anda telah membuat grup aturan AWS WAF Klasik yang ingin ditambahkan ke kebijakan, pilih Buat AWS Firewall Manager kebijakan dan tambahkan grup aturan yang ada. Jika Anda ingin membuat grup aturan baru, pilih Buat kebijakan Firewall Manager dan tambahkan grup aturan baru.
6. Untuk Wilayah, pilih Wilayah AWS. Untuk melindungi CloudFront sumber daya Amazon, pilih Global.

   Untuk melindungi sumber daya di beberapa Wilayah (selain CloudFront sumber daya), Anda harus membuat kebijakan Firewall Manager terpisah untuk setiap Wilayah.
7. Pilih Selanjutnya.
8. Jika Anda membuat grup aturan, ikuti instruksi diMembuat grup aturan AWS WAF Klasik. Setelah Anda membuat grup aturan, lanjutkan dengan langkah-langkah berikut.
9. Masukkan nama kebijakan.
10. Jika Anda menambahkan grup aturan yang ada, gunakan menu tarik-turun untuk memilih grup aturan yang akan ditambahkan, lalu pilih Tambahkan grup aturan.
11. Kebijakan memiliki dua kemungkinan tindakan: Tindakan yang ditetapkan oleh grup aturan dan Hitungan. Jika Anda ingin menguji kebijakan dan grup aturan, setel tindakan ke Hitung. Tindakan ini mengesampingkan tindakan blok apa pun yang ditentukan oleh aturan dalam grup aturan. Artinya, jika tindakan kebijakan disetel ke Hitung, permintaan tersebut hanya dihitung dan tidak diblokir. Sebaliknya, jika Anda menetapkan tindakan kebijakan ke Tindakan yang ditetapkan oleh grup aturan, tindakan aturan grup aturan akan digunakan. Pilih tindakan yang sesuai.
12. Pilih Selanjutnya.
13. Untuk kebijakan Akun AWS ini berlaku, pilih opsi sebagai berikut:

    - Jika Anda ingin menerapkan kebijakan ke semua akun di organisasi Anda, tinggalkan pilihan default, Sertakan semua akun di AWS organisasi saya.
    - Jika Anda ingin menerapkan kebijakan hanya untuk akun atau akun tertentu yang berada di unit AWS Organizations organisasi tertentu (OU), pilih Sertakan hanya akun dan unit organisasi yang ditentukan, lalu tambahkan akun dan OU yang ingin Anda sertakan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.
    - Jika Anda ingin menerapkan kebijakan untuk semua kecuali satu set akun atau unit AWS Organizations organisasi (OU) tertentu, pilih Kecualikan akun dan unit organisasi yang ditentukan, dan sertakan semua akun lainnya, lalu tambahkan akun dan OU yang ingin Anda

kecualikan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.

Anda hanya dapat memilih salah satu opsi.

Setelah menerapkan kebijakan, Firewall Manager secara otomatis mengevaluasi akun baru apa pun terhadap pengaturan Anda. Misalnya, jika Anda hanya menyertakan akun tertentu, Firewall Manager tidak menerapkan kebijakan tersebut ke akun baru mana pun. Sebagai contoh lain, jika Anda menyertakan OU, ketika Anda menambahkan akun ke OU atau ke salah satu OU anaknya, Firewall Manager secara otomatis menerapkan kebijakan tersebut ke akun baru.

14. Pilih jenis sumber daya yang ingin Anda lindungi.
15. Untuk Sumber Daya, Anda dapat mempersempit cakupan kebijakan menggunakan penandaan, dengan menyertakan atau mengecualikan sumber daya dengan tag yang Anda tentukan. Anda dapat menggunakan inklusi atau pengecualian, dan bukan keduanya. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.

    Jika Anda memasukkan lebih dari satu tag, sumber daya harus memiliki semua tag untuk disertakan atau dikecualikan.

    Tag sumber daya hanya dapat memiliki nilai non-null. Jika Anda menghilangkan nilai untuk tag, Firewall Manager menyimpan tag dengan nilai string kosong: “”. Tag sumber daya hanya cocok dengan tag yang memiliki kunci yang sama dan nilai yang sama.
16. Jika Anda ingin menerapkan kebijakan secara otomatis ke sumber daya yang ada, pilih Buat dan terapkan kebijakan ini ke sumber daya yang ada dan yang baru.

    Opsi ini membuat ACL web di setiap akun yang berlaku dalam suatu AWS organisasi dan mengaitkan ACL web dengan sumber daya di akun. Opsi ini juga menerapkan kebijakan ke semua sumber daya baru yang sesuai dengan kriteria sebelumnya (jenis dan tag sumber daya). Atau, jika Anda memilih Buat kebijakan tetapi tidak menerapkan kebijakan ke sumber daya yang ada atau yang baru, Firewall Manager membuat ACL web di setiap akun yang berlaku dalam organisasi, tetapi tidak menerapkan ACL web ke sumber daya apa pun. Anda harus menerapkan kebijakan ke sumber daya nanti. Pilih opsi yang sesuai.
17. Untuk Ganti ACL web terkait yang ada, Anda dapat memilih untuk menghapus asosiasi ACL web apa pun yang saat ini ditentukan untuk sumber daya dalam lingkup, lalu menggantinya dengan asosiasi ke ACL web yang Anda buat dengan kebijakan ini. Secara default, Firewall Manager tidak menghapus asosiasi ACL web yang ada sebelum menambahkan yang baru. Jika Anda ingin menghapus yang sudah ada, pilih opsi ini.

18. Pilih Selanjutnya.
19. Tinjau kebijakan baru. Untuk membuat perubahan, pilih Edit. Jika Anda puas dengan kebijakan tersebut, pilih Buat dan terapkan kebijakan.

Membuat AWS Firewall Manager kebijakan untuk AWS Shield Advanced

Untuk membuat kebijakan Firewall Manager untuk Shield Advanced (konsol)

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

   > **Note**
   >
   > Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

2. Di panel navigasi, pilih Kebijakan keamanan.
3. Pilih Buat kebijakan.
4. Untuk jenis Kebijakan, pilih Shield Advanced.

   Untuk membuat kebijakan Shield Advanced, Anda harus berlangganan Shield Advanced. Jika Anda tidak berlangganan, Anda diminta untuk melakukannya. Untuk informasi tentang biaya berlangganan, lihat AWS Shield Advanced Harga.
5. Untuk Wilayah, pilih file Wilayah AWS. Untuk melindungi CloudFront distribusi Amazon, pilih Global.

   Untuk pilihan Wilayah selain Global, untuk melindungi sumber daya di beberapa Wilayah, Anda harus membuat kebijakan Firewall Manager terpisah untuk setiap Wilayah.
6. Pilih Selanjutnya.
7. Untuk Nama, masukkan nama deskriptif.
8. Hanya untuk kebijakan Wilayah Global, Anda dapat memilih apakah Anda ingin mengelola mitigasi DDoS lapisan aplikasi otomatis Shield Advanced. Untuk informasi tentang fitur Shield Advanced ini, lihatMitigasi DDoS lapisan aplikasi otomatis Shield Advanced.

Anda dapat memilih untuk mengaktifkan atau menonaktifkan mitigasi otomatis, atau Anda dapat memilih untuk mengabaikannya. Jika Anda memilih untuk mengabaikannya, Firewall Manager tidak mengelola mitigasi otomatis sama sekali untuk perlindungan Shield Advanced. Untuk informasi selengkapnya tentang opsi kebijakan ini, lihatMitigasi DDoS lapisan aplikasi otomatis.

9. Di bawah manajemen ACL Web, jika Anda ingin Firewall Manager mengelola ACL web yang tidak terkait, aktifkan Kelola ACL web yang tidak terkait. Dengan opsi ini, Firewall Manager membuat ACL web di akun dalam cakupan kebijakan hanya jika ACL web akan digunakan oleh setidaknya satu sumber daya. Jika sewaktu-waktu akun masuk ke cakupan kebijakan, Firewall Manager secara otomatis membuat ACL web di akun jika setidaknya satu sumber daya akan menggunakan ACL web. Setelah mengaktifkan opsi ini, Firewall Manager melakukan pembersihan satu kali dari ACL web yang tidak terkait di akun Anda. Proses pembersihan bisa memakan waktu beberapa jam. Jika sumber daya meninggalkan cakupan kebijakan setelah Firewall Manager membuat ACL web, Firewall Manager tidak akan memisahkan sumber daya dari ACL web. Untuk menyertakan ACL web dalam pembersihan satu kali, Anda harus terlebih dahulu memisahkan sumber daya dari ACL web secara manual dan kemudian mengaktifkan Kelola ACL web yang tidak terkait.
10. Untuk tindakan Kebijakan, sebaiknya buat kebijakan dengan opsi yang tidak secara otomatis memulihkan sumber daya yang tidak sesuai. Ketika Anda menonaktifkan remediasi otomatis, Anda dapat menilai efek dari kebijakan baru Anda sebelum Anda menerapkannya. Ketika Anda puas bahwa perubahan adalah apa yang Anda inginkan, maka edit kebijakan dan ubah tindakan kebijakan untuk mengaktifkan remediasi otomatis.

    Jika Anda ingin menerapkan kebijakan secara otomatis ke sumber daya dalam lingkup yang ada, pilih Remediasi otomatis sumber daya yang tidak sesuai. Opsi ini menerapkan perlindungan Shield Advanced untuk setiap akun yang berlaku dalam AWS organisasi dan setiap sumber daya yang berlaku di akun.

    Hanya untuk kebijakan Wilayah Global, jika Anda memilih Remediasi otomatis sumber daya yang tidak sesuai, Anda juga dapat memilih agar Firewall Manager secara otomatis mengganti asosiasi ACL web AWS WAF Klasik yang ada dengan asosiasi baru ke ACL web yang dibuat menggunakan versi terbaru (v2). AWS WAF Jika Anda memilih ini, Firewall Manager menghapus asosiasi dengan ACL web versi sebelumnya dan membuat asosiasi baru dengan ACL web versi terbaru, setelah membuat ACL web kosong baru di akun dalam lingkup apa pun yang belum memilikinya untuk kebijakan tersebut. Untuk informasi selengkapnya tentang metrik ini, lihat Ganti ACL web AWS WAF Klasik dengan ACL web versi terbaru.
11. Pilih Selanjutnya.

12. Untuk kebijakan Akun AWS ini berlaku, pilih opsi sebagai berikut:

    - Jika Anda ingin menerapkan kebijakan ke semua akun di organisasi Anda, pertahankan pilihan default, Sertakan semua akun di AWS organisasi saya.
    - Jika Anda ingin menerapkan kebijakan hanya untuk akun atau akun tertentu yang berada di unit AWS Organizations organisasi tertentu (OU), pilih Sertakan hanya akun dan unit organisasi yang ditentukan, lalu tambahkan akun dan OU yang ingin Anda sertakan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.
    - Jika Anda ingin menerapkan kebijakan untuk semua kecuali satu set akun atau unit AWS Organizations organisasi (OU) tertentu, pilih Kecualikan akun dan unit organisasi yang ditentukan, dan sertakan semua akun lainnya, lalu tambahkan akun dan OU yang ingin Anda kecualikan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.

    Anda hanya dapat memilih salah satu opsi.

    Setelah menerapkan kebijakan, Firewall Manager secara otomatis mengevaluasi akun baru apa pun terhadap pengaturan Anda. Misalnya, jika Anda hanya menyertakan akun tertentu, Firewall Manager tidak menerapkan kebijakan tersebut ke akun baru mana pun. Sebagai contoh lain, jika Anda menyertakan OU, ketika Anda menambahkan akun ke OU atau ke salah satu OU anaknya, Firewall Manager secara otomatis menerapkan kebijakan tersebut ke akun baru.

13. Pilih jenis sumber daya yang ingin Anda lindungi.

    Firewall Manager tidak mendukung Amazon Route 53 atau AWS Global Accelerator. Jika Anda perlu menggunakan Shield Advanced untuk melindungi sumber daya dari layanan ini, Anda tidak dapat menggunakan kebijakan Firewall Manager. Sebagai gantinya, ikuti panduan Shield Advanced di[Menambahkan AWS Shield Advanced perlindungan ke AWS sumber daya](#).

14. Untuk Sumber Daya, Anda dapat mempersempit cakupan kebijakan menggunakan penandaan, dengan menyertakan atau mengecualikan sumber daya dengan tag yang Anda tentukan. Anda dapat menggunakan inklusi atau pengecualian, dan bukan keduanya. Untuk informasi selengkapnya tentang tag, lihat [Bekerja dengan Editor Tag](#).

    Jika Anda memasukkan lebih dari satu tag, sumber daya harus memiliki semua tag untuk disertakan atau dikecualikan.

Tag sumber daya hanya dapat memiliki nilai non-null. Jika Anda menghilangkan nilai untuk tag, Firewall Manager menyimpan tag dengan nilai string kosong: “”. Tag sumber daya hanya cocok dengan tag yang memiliki kunci yang sama dan nilai yang sama.

15. Pilih Selanjutnya.
16. Untuk tag Kebijakan, tambahkan tag pengenal apa pun yang ingin Anda tambahkan ke sumber daya kebijakan Manajer Firewall. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.
17. Pilih Selanjutnya.
18. Tinjau pengaturan kebijakan baru dan kembali ke halaman mana pun yang Anda perlukan untuk penyesuaian apa pun.

    Jika Anda puas dengan kebijakan ini, pilih Create policy (Buat kebijakan). Di panel AWS Firewall Manager kebijakan, kebijakan Anda harus dicantumkan. Ini mungkin akan menunjukkan Pending di bawah judul akun dan itu akan menunjukkan status pengaturan remediasi otomatis. Pembuatan kebijakan dapat memakan waktu beberapa menit. Setelah Status tertunda diganti dengan jumlah akun, Anda dapat memilih nama kebijakan untuk menjelajahi status kepatuhan akun dan sumber daya. Untuk informasi, lihat Melihat informasi kepatuhan untuk suatu AWS Firewall Manager kebijakan

Membuat kebijakan grup keamanan AWS Firewall Manager umum

Untuk informasi tentang cara kerja kebijakan grup keamanan umum, lihatKebijakan kelompok keamanan umum.

Untuk membuat kebijakan grup keamanan umum, Anda harus memiliki grup keamanan yang sudah dibuat di akun administrator Manajer Firewall yang ingin Anda gunakan sebagai yang utama untuk kebijakan Anda. Anda dapat mengelola grup keamanan melalui Amazon Virtual Private Cloud (Amazon VPC) atau Amazon Elastic Compute Cloud (Amazon EC2). Untuk selengkapnya, lihat Bekerja dengan Grup Keamanan di Panduan Pengguna Amazon VPC.

Untuk membuat kebijakan grup keamanan umum (konsol)

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

> **Note**
>
> Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

2. Di panel navigasi, pilih Kebijakan keamanan.
3. Pilih Buat kebijakan.
4. Untuk jenis Kebijakan, pilih Grup keamanan.
5. Untuk jenis kebijakan grup Keamanan, pilih Grup keamanan umum.
6. Untuk Wilayah, pilih file Wilayah AWS.
7. Pilih Selanjutnya.
8. Untuk nama Kebijakan, masukkan nama ramah.
9. Untuk aturan Kebijakan, lakukan hal berikut:

   a. Dari opsi aturan, pilih batasan yang ingin Anda terapkan pada aturan grup keamanan dan sumber daya yang berada dalam cakupan kebijakan. Jika Anda memilih Mendistribusikan tag dari grup keamanan utama ke grup keamanan yang dibuat oleh kebijakan ini, Anda juga harus memilih Identifikasi dan laporkan ketika grup keamanan yang dibuat oleh kebijakan ini menjadi tidak sesuai.

   > **Important**
   >
   > Firewall Manager tidak akan mendistribusikan tag sistem yang ditambahkan oleh AWS layanan ke dalam grup keamanan replika. Tag sistem dimulai dengan `aws:` awalan. Selain itu, Firewall Manager tidak akan memperbarui tag grup keamanan yang ada atau membuat grup keamanan baru jika kebijakan tersebut memiliki tag yang bertentangan dengan kebijakan tag organisasi. Untuk informasi tentang kebijakan tag, lihat Kebijakan tag di Panduan AWS Organizations Pengguna.

   Jika Anda memilih Mendistribusikan referensi grup keamanan dari grup keamanan utama ke grup keamanan yang dibuat oleh kebijakan ini, Firewall Manager hanya mendistribusikan referensi grup keamanan jika mereka memiliki koneksi peering aktif di Amazon VPC. Untuk informasi tentang opsi ini, lihat Pengaturan aturan kebijakan.

b. Untuk grup keamanan utama, pilih Tambahkan grup keamanan, lalu pilih grup keamanan yang ingin Anda gunakan. Firewall Manager mengisi daftar grup keamanan dari semua instance Amazon VPC di akun administrator Firewall Manager.

   Secara default, jumlah maksimum grup keamanan primer per kebijakan adalah 3. Untuk informasi tentang pengaturan ini, lihat AWS Firewall Manager kuota.

c. Untuk tindakan Kebijakan, sebaiknya buat kebijakan dengan opsi yang tidak otomatis diperbaiki. Ini memungkinkan Anda untuk menilai efek dari kebijakan baru Anda sebelum Anda menerapkannya. Ketika Anda puas bahwa perubahan adalah apa yang Anda inginkan, maka edit kebijakan dan ubah tindakan kebijakan untuk mengaktifkan remediasi otomatis sumber daya yang tidak sesuai.

10. Pilih Selanjutnya.
11. Untuk kebijakan Akun AWS ini berlaku, pilih opsi sebagai berikut:

    - Jika Anda ingin menerapkan kebijakan ke semua akun di organisasi Anda, tinggalkan pilihan default, Sertakan semua akun di AWS organisasi saya.
    - Jika Anda ingin menerapkan kebijakan hanya untuk akun atau akun tertentu yang berada di unit AWS Organizations organisasi tertentu (OU), pilih Sertakan hanya akun dan unit organisasi yang ditentukan, lalu tambahkan akun dan OU yang ingin Anda sertakan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.
    - Jika Anda ingin menerapkan kebijakan untuk semua kecuali satu set akun atau unit AWS Organizations organisasi (OU) tertentu, pilih Kecualikan akun dan unit organisasi yang ditentukan, dan sertakan semua akun lainnya, lalu tambahkan akun dan OU yang ingin Anda kecualikan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.

    Anda hanya dapat memilih salah satu opsi.

    Setelah menerapkan kebijakan, Firewall Manager secara otomatis mengevaluasi akun baru apa pun terhadap pengaturan Anda. Misalnya, jika Anda hanya menyertakan akun tertentu, Firewall Manager tidak menerapkan kebijakan tersebut ke akun baru mana pun. Sebagai contoh lain, jika Anda menyertakan OU, ketika Anda menambahkan akun ke OU atau ke salah satu OU anaknya, Firewall Manager secara otomatis menerapkan kebijakan tersebut ke akun baru.
12. Untuk jenis Sumber Daya, pilih jenis sumber daya yang ingin Anda lindungi.

Jika memilih instans EC2, Anda dapat memilih untuk menyertakan semua antarmuka jaringan elastis di setiap instans Amazon EC2 atau hanya antarmuka default di setiap instans. Jika Anda memiliki lebih dari satu elastic network interface dalam instans Amazon EC2 dalam lingkup, memilih opsi untuk menyertakan semua antarmuka memungkinkan Firewall Manager menerapkan kebijakan tersebut ke semuanya. Jika Anda mengaktifkan remediasi otomatis, jika Firewall Manager tidak dapat menerapkan kebijakan tersebut ke semua antarmuka jaringan elastis dalam instans Amazon EC2, kebijakan tersebut menandai instans sebagai tidak sesuai.

13. Untuk Sumber Daya, Anda dapat mempersempit cakupan kebijakan menggunakan penandaan, dengan menyertakan atau mengecualikan sumber daya dengan tag yang Anda tentukan. Anda dapat menggunakan inklusi atau pengecualian, dan bukan keduanya. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.

    Jika Anda memasukkan lebih dari satu tag, sumber daya harus memiliki semua tag untuk disertakan atau dikecualikan.

    Tag sumber daya hanya dapat memiliki nilai non-null. Jika Anda menghilangkan nilai untuk tag, Firewall Manager menyimpan tag dengan nilai string kosong: “”. Tag sumber daya hanya cocok dengan tag yang memiliki kunci yang sama dan nilai yang sama.
14. Untuk sumber daya VPC Bersama, jika Anda ingin menerapkan kebijakan ke sumber daya di VPC bersama, selain VPC yang dimiliki akun, pilih Sertakan sumber daya dari VPC bersama.
15. Pilih Selanjutnya.
16. Tinjau setelan kebijakan untuk memastikan setelan tersebut sesuai dengan yang Anda inginkan, lalu pilih Buat kebijakan.

Firewall Manager membuat replika grup keamanan utama di setiap instans VPC Amazon yang terdapat dalam akun dalam lingkup hingga kuota maksimum VPC Amazon per akun yang didukung. Firewall Manager mengaitkan grup keamanan replika ke sumber daya yang berada dalam cakupan kebijakan untuk setiap akun dalam lingkup. Untuk informasi selengkapnya tentang cara kerja kebijakan ini, lihatKebijakan kelompok keamanan umum.

Membuat kebijakan grup keamanan audit AWS Firewall Manager konten

Untuk informasi tentang cara kerja kebijakan grup keamanan audit konten, lihatKebijakan grup keamanan audit konten.

Untuk beberapa pengaturan kebijakan audit konten, Anda harus menyediakan grup keamanan audit untuk Firewall Manager untuk digunakan sebagai templat. Misalnya, Anda mungkin memiliki grup keamanan audit yang berisi semua aturan yang tidak diizinkan di grup keamanan mana pun. Anda harus membuat grup keamanan audit ini menggunakan akun administrator Firewall Manager Anda, sebelum Anda dapat menggunakannya dalam kebijakan Anda. Anda dapat mengelola grup keamanan melalui Amazon Virtual Private Cloud (Amazon VPC) atau Amazon Elastic Compute Cloud (Amazon EC2). Untuk selengkapnya, lihat Bekerja dengan Grup Keamanan di Panduan Pengguna Amazon VPC.

Untuk membuat kebijakan grup keamanan audit konten (konsol)

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

   > **Note**
   >
   > Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

2. Di panel navigasi, pilih Kebijakan keamanan.
3. Pilih Buat kebijakan.
4. Untuk jenis Kebijakan, pilih Grup keamanan.
5. Untuk jenis kebijakan grup Keamanan, pilih Audit dan penegakan aturan grup keamanan.
6. Untuk Wilayah, pilih file Wilayah AWS.
7. Pilih Selanjutnya.
8. Untuk nama Kebijakan, masukkan nama ramah.
9. Untuk aturan Kebijakan, pilih opsi aturan kebijakan terkelola atau kustom yang ingin Anda gunakan.

   a. Untuk Mengonfigurasi aturan kebijakan audit terkelola, lakukan hal berikut:

      i. Untuk Mengonfigurasi aturan grup keamanan yang akan diaudit, pilih jenis aturan grup keamanan yang ingin diterapkan oleh kebijakan audit Anda.

ii. Jika Anda ingin melakukan hal-hal seperti aturan audit berdasarkan protokol, port, dan pengaturan rentang CIDR yang ada di grup keamanan Anda, pilih Audit aturan grup keamanan yang terlalu permisif dan pilih opsi yang Anda inginkan.

Untuk pemilihan Aturan memungkinkan semua lalu lintas, Anda dapat memberikan daftar aplikasi khusus untuk menunjuk aplikasi yang ingin Anda audit. Untuk informasi tentang daftar aplikasi kustom dan cara menggunakannya dalam kebijakan Anda, lihat Daftar terkelola danMenggunakan daftar terkelola.

Untuk pilihan yang menggunakan daftar protokol, Anda dapat menggunakan daftar yang ada dan Anda dapat membuat daftar baru. Untuk informasi tentang daftar protokol dan cara menggunakannya dalam kebijakan Anda, lihat Daftar terkelola danMenggunakan daftar terkelola.

iii. Jika Anda ingin mengaudit risiko tinggi berdasarkan akses mereka ke rentang CIDR yang dicadangkan atau tidak dicadangkan, pilih Audit aplikasi berisiko tinggi dan pilih opsi yang Anda inginkan.

Pilihan berikut ini saling eksklusif: Aplikasi yang hanya dapat mengakses rentang CIDR yang dipesan dan Aplikasi diizinkan untuk mengakses rentang CIDR yang tidak dipesan. Anda dapat memilih paling banyak salah satu dari mereka dalam kebijakan apa pun.

Untuk pilihan yang menggunakan daftar aplikasi, Anda dapat menggunakan daftar yang ada dan Anda dapat membuat daftar baru. Untuk informasi tentang daftar aplikasi dan cara menggunakannya dalam kebijakan Anda, lihat Daftar terkelola danMenggunakan daftar terkelola.

iv. Gunakan pengaturan Overrides untuk secara eksplisit mengganti setelan lain dalam kebijakan. Anda dapat memilih untuk selalu mengizinkan atau selalu menolak aturan grup keamanan tertentu, terlepas dari apakah aturan tersebut mematuhi opsi lain yang telah Anda tetapkan untuk kebijakan tersebut.

Untuk opsi ini, Anda menyediakan grup keamanan audit sebagai aturan yang diizinkan atau templat aturan yang ditolak. Untuk grup keamanan audit, pilih Tambahkan grup keamanan audit, lalu pilih grup keamanan yang ingin Anda gunakan. Firewall Manager mengisi daftar grup keamanan audit dari semua instance VPC Amazon di akun administrator Firewall Manager. Kuota maksimum default untuk jumlah grup keamanan audit untuk suatu kebijakan adalah satu. Untuk informasi tentang peningkatan kuota, lihatAWS Firewall Manager kuota.

b. Untuk Mengonfigurasi aturan kebijakan kustom, lakukan hal berikut:

   i. Dari opsi aturan, pilih apakah hanya mengizinkan aturan yang ditentukan dalam kelompok keamanan audit atau menolak semua aturan. Untuk informasi tentang pilihan ini, lihatKebijakan grup keamanan audit konten.

   ii. Untuk grup keamanan audit, pilih Tambahkan grup keamanan audit, lalu pilih grup keamanan yang ingin Anda gunakan. Firewall Manager mengisi daftar grup keamanan audit dari semua instance VPC Amazon di akun administrator Firewall Manager. Kuota maksimum default untuk jumlah grup keamanan audit untuk suatu kebijakan adalah satu. Untuk informasi tentang peningkatan kuota, lihatAWS Firewall Manager kuota.

   iii. Untuk tindakan Kebijakan, Anda harus membuat kebijakan dengan opsi yang tidak otomatis diperbaiki. Ini memungkinkan Anda untuk menilai efek dari kebijakan baru Anda sebelum Anda menerapkannya. Ketika Anda puas bahwa perubahan adalah apa yang Anda inginkan, edit kebijakan dan ubah tindakan kebijakan untuk mengaktifkan remediasi otomatis sumber daya yang tidak sesuai.

10. Pilih Selanjutnya.

11. Untuk kebijakan Akun AWS ini berlaku, pilih opsi sebagai berikut:

    - Jika Anda ingin menerapkan kebijakan ke semua akun di organisasi Anda, tinggalkan pilihan default, Sertakan semua akun di AWS organisasi saya.
    - Jika Anda ingin menerapkan kebijakan hanya untuk akun atau akun tertentu yang berada di unit AWS Organizations organisasi tertentu (OU), pilih Sertakan hanya akun dan unit organisasi yang ditentukan, lalu tambahkan akun dan OU yang ingin Anda sertakan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.
    - Jika Anda ingin menerapkan kebijakan untuk semua kecuali satu set akun atau unit AWS Organizations organisasi (OU) tertentu, pilih Kecualikan akun dan unit organisasi yang ditentukan, dan sertakan semua akun lainnya, lalu tambahkan akun dan OU yang ingin Anda kecualikan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.

    Anda hanya dapat memilih salah satu opsi.

    Setelah menerapkan kebijakan, Firewall Manager secara otomatis mengevaluasi akun baru apa pun terhadap pengaturan Anda. Misalnya, jika Anda hanya menyertakan akun tertentu, Firewall Manager tidak menerapkan kebijakan tersebut ke akun baru mana pun. Sebagai contoh lain, jika

Anda menyertakan OU, ketika Anda menambahkan akun ke OU atau ke salah satu OU anaknya, Firewall Manager secara otomatis menerapkan kebijakan tersebut ke akun baru.

12. Untuk jenis Sumber Daya, pilih jenis sumber daya yang ingin Anda lindungi.
13. Untuk Sumber Daya, Anda dapat mempersempit cakupan kebijakan menggunakan penandaan, dengan menyertakan atau mengecualikan sumber daya dengan tag yang Anda tentukan. Anda dapat menggunakan inklusi atau pengecualian, dan bukan keduanya. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.

    Jika Anda memasukkan lebih dari satu tag, sumber daya harus memiliki semua tag untuk disertakan atau dikecualikan.

    Tag sumber daya hanya dapat memiliki nilai non-null. Jika Anda menghilangkan nilai untuk tag, Firewall Manager menyimpan tag dengan nilai string kosong: “”. Tag sumber daya hanya cocok dengan tag yang memiliki kunci yang sama dan nilai yang sama.
14. Pilih Selanjutnya.
15. Tinjau setelan kebijakan untuk memastikan setelan tersebut sesuai dengan yang Anda inginkan, lalu pilih Buat kebijakan.

Firewall Manager membandingkan grup keamanan audit dengan grup keamanan dalam lingkup di AWS organisasi Anda, sesuai dengan setelan aturan kebijakan Anda. Anda dapat meninjau status kebijakan di konsol AWS Firewall Manager kebijakan. Setelah kebijakan dibuat, Anda dapat mengeditnya dan mengaktifkan remediasi otomatis untuk menerapkan kebijakan grup keamanan audit Anda. Untuk informasi selengkapnya tentang cara kerja kebijakan ini, lihatKebijakan grup keamanan audit konten.

Membuat kebijakan grup keamanan audit AWS Firewall Manager penggunaan

Untuk informasi tentang cara kerja kebijakan grup keamanan audit penggunaan, lihatPenggunaan kebijakan grup keamanan audit.

Untuk membuat kebijakan grup keamanan audit penggunaan (konsol)

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

> **Note**
>
> Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

2. Di panel navigasi, pilih Kebijakan keamanan.
3. Pilih Buat kebijakan.
4. Untuk jenis Kebijakan, pilih Grup keamanan.
5. Untuk jenis kebijakan grup Keamanan, pilih Audit dan pembersihan grup keamanan yang tidak terkait dan berlebihan.
6. Untuk Wilayah, pilih file Wilayah AWS.
7. Pilih Selanjutnya.
8. Untuk nama Kebijakan, masukkan nama ramah.
9. Untuk aturan Kebijakan, pilih salah satu atau kedua opsi yang tersedia.

   - Jika Anda memilih Grup keamanan dalam cakupan kebijakan ini harus digunakan oleh setidaknya satu sumber daya, Firewall Manager menghapus grup keamanan apa pun yang ditentukan tidak digunakan. Ketika aturan ini diaktifkan, Firewall Manager menjalankannya terakhir saat Anda menyimpan kebijakan.

     Untuk detail tentang cara Firewall Manager menentukan penggunaan dan waktu remediasi, lihatPenggunaan kebijakan grup keamanan audit.

     > **Note**
     >
     > Bila Anda menggunakan jenis kebijakan grup keamanan audit penggunaan ini, hindari membuat beberapa perubahan pada status asosiasi grup keamanan dalam lingkup dalam waktu singkat. Melakukannya dapat menyebabkan Firewall Manager melewatkan acara terkait.

   Secara default, Firewall Manager menganggap grup keamanan tidak sesuai dengan aturan kebijakan ini segera setelah tidak digunakan. Anda dapat secara opsional menentukan beberapa menit bahwa grup keamanan dapat tidak digunakan sebelum dianggap tidak sesuai, hingga 525.600 menit (365 hari). Anda dapat menggunakan pengaturan ini untuk memberi Anda waktu untuk mengaitkan grup keamanan baru dengan sumber daya.

> **Important**
>
> Jika Anda menentukan jumlah menit selain nilai default nol, Anda harus mengaktifkan hubungan tidak langsung di AWS Config. Jika tidak, kebijakan grup keamanan audit penggunaan Anda tidak akan berfungsi sebagaimana dimaksud. Untuk informasi tentang hubungan tidak langsung di AWS Config, lihat Hubungan Tidak Langsung di AWS Config dalam Panduan AWS Config Pengembang.

- Jika Anda memilih Grup keamanan dalam cakupan kebijakan ini harus unik, Firewall Manager menggabungkan grup keamanan yang berlebihan, sehingga hanya satu yang terkait dengan sumber daya apa pun. Jika Anda memilih ini, Firewall Manager menjalankannya terlebih dahulu saat Anda menyimpan kebijakan.

10. Untuk tindakan Kebijakan, sebaiknya buat kebijakan dengan opsi yang tidak otomatis diperbaiki. Ini memungkinkan Anda untuk menilai efek dari kebijakan baru Anda sebelum Anda menerapkannya. Ketika Anda puas bahwa perubahan adalah apa yang Anda inginkan, maka edit kebijakan dan ubah tindakan kebijakan untuk mengaktifkan remediasi otomatis sumber daya yang tidak sesuai.
11. Pilih Selanjutnya.
12. Untuk kebijakan Akun AWS ini berlaku, pilih opsi sebagai berikut:

    - Jika Anda ingin menerapkan kebijakan ke semua akun di organisasi Anda, tinggalkan pilihan default, Sertakan semua akun di AWS organisasi saya.
    - Jika Anda ingin menerapkan kebijakan hanya untuk akun atau akun tertentu yang berada di unit AWS Organizations organisasi tertentu (OU), pilih Sertakan hanya akun dan unit organisasi yang ditentukan, lalu tambahkan akun dan OU yang ingin Anda sertakan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.
    - Jika Anda ingin menerapkan kebijakan untuk semua kecuali satu set akun atau unit AWS Organizations organisasi (OU) tertentu, pilih Kecualikan akun dan unit organisasi yang ditentukan, dan sertakan semua akun lainnya, lalu tambahkan akun dan OU yang ingin Anda kecualikan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.

    Anda hanya dapat memilih salah satu opsi.

Setelah menerapkan kebijakan, Firewall Manager secara otomatis mengevaluasi akun baru apa pun terhadap pengaturan Anda. Misalnya, jika Anda hanya menyertakan akun tertentu, Firewall Manager tidak menerapkan kebijakan tersebut ke akun baru mana pun. Sebagai contoh lain, jika Anda menyertakan OU, ketika Anda menambahkan akun ke OU atau ke salah satu OU anaknya, Firewall Manager secara otomatis menerapkan kebijakan tersebut ke akun baru.

13. Untuk Sumber Daya, Anda dapat mempersempit cakupan kebijakan menggunakan penandaan, dengan menyertakan atau mengecualikan sumber daya dengan tag yang Anda tentukan. Anda dapat menggunakan inklusi atau pengecualian, dan bukan keduanya. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.

    Jika Anda memasukkan lebih dari satu tag, sumber daya harus memiliki semua tag untuk disertakan atau dikecualikan.

    Tag sumber daya hanya dapat memiliki nilai non-null. Jika Anda menghilangkan nilai untuk tag, Firewall Manager menyimpan tag dengan nilai string kosong: “”. Tag sumber daya hanya cocok dengan tag yang memiliki kunci yang sama dan nilai yang sama.
14. Pilih Selanjutnya.
15. Jika Anda belum mengecualikan akun administrator Manajer Firewall dari cakupan kebijakan, Firewall Manager meminta Anda untuk melakukannya. Melakukan hal ini akan membuat grup keamanan di akun administrator Firewall Manager, yang Anda gunakan untuk kebijakan grup keamanan umum dan audit, di bawah kendali manual Anda. Pilih opsi yang Anda inginkan dalam dialog ini.
16. Tinjau setelan kebijakan untuk memastikan setelan tersebut sesuai dengan yang Anda inginkan, lalu pilih Buat kebijakan.

Jika Anda memilih untuk mewajibkan grup keamanan unik, Firewall Manager memindai grup keamanan redundan di setiap instans VPC Amazon dalam lingkup. Kemudian, jika Anda memilih untuk mewajibkan setiap grup keamanan digunakan oleh setidaknya satu sumber daya, Firewall Manager memindai grup keamanan yang tetap tidak digunakan selama menit yang ditentukan dalam aturan. Anda dapat meninjau status kebijakan di konsol AWS Firewall Manager kebijakan. Untuk informasi selengkapnya tentang cara kerja kebijakan ini, lihatPenggunaan kebijakan grup keamanan audit.

Membuat kebijakan ACL AWS Firewall Manager jaringan

Untuk informasi tentang cara kerja kebijakan ACL jaringan, lihatKebijakan ACL jaringan.

Untuk membuat kebijakan ACL jaringan, Anda harus tahu cara menentukan ACL jaringan untuk digunakan dengan subnet VPC Amazon Anda. Untuk selengkapnya, lihat Mengontrol lalu lintas ke subnet menggunakan ACL jaringan dan Bekerja dengan ACL jaringan di Panduan Pengguna Amazon VPC.

Untuk membuat kebijakan ACL jaringan (konsol)

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

   > **Note**
   >
   > Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

2. Di panel navigasi, pilih Kebijakan keamanan.
3. Pilih Buat kebijakan.
4. Untuk jenis Kebijakan, pilih ACL Jaringan.
5. Untuk Wilayah, pilih file Wilayah AWS.
6. Pilih Selanjutnya.
7. Untuk nama Kebijakan, masukkan nama deskriptif.
8. Untuk aturan Kebijakan, tentukan aturan yang ingin selalu dijalankan di ACL jaringan yang dikelola Firewall Manager untuk Anda. ACL jaringan memantau dan menangani lalu lintas masuk dan keluar, jadi dalam kebijakan Anda, Anda menentukan aturan untuk kedua arah.

   Untuk kedua arah, Anda menentukan aturan yang ingin selalu Anda jalankan terlebih dahulu dan aturan yang ingin selalu Anda jalankan terakhir. Di ACL jaringan yang dikelola Firewall Manager, pemilik akun dapat menentukan aturan khusus untuk dijalankan di antara aturan pertama dan terakhir ini.
9. Untuk tindakan Kebijakan, jika Anda ingin mengidentifikasi subnet dan ACL jaringan yang tidak sesuai, tetapi belum mengambil tindakan korektif apa pun, pilih Identifikasi sumber daya yang tidak mematuhi aturan kebijakan, tetapi jangan memulihkan secara otomatis. Anda dapat mengubah opsi ini nanti.

Jika Anda ingin menerapkan kebijakan secara otomatis ke subnet dalam lingkup yang ada, pilih Remediasi otomatis sumber daya yang tidak sesuai. Dengan opsi ini, Anda juga menentukan apakah akan memaksa remediasi ketika perilaku penanganan lalu lintas aturan kebijakan bertentangan dengan aturan kustom yang ada di ACL jaringan. Terlepas dari apakah Anda memaksa remediasi, Firewall Manager melaporkan aturan yang bertentangan dalam pelanggaran kepatuhannya.

10. Pilih Selanjutnya.
11. Untuk kebijakan Akun AWS ini berlaku, pilih opsi sebagai berikut:

    - Jika Anda ingin menerapkan kebijakan ke semua akun di organisasi Anda, tinggalkan pilihan default, Sertakan semua akun di AWS organisasi saya.
    - Jika Anda ingin menerapkan kebijakan hanya untuk akun atau akun tertentu yang berada di unit AWS Organizations organisasi tertentu (OU), pilih Sertakan hanya akun dan unit organisasi yang ditentukan, lalu tambahkan akun dan OU yang ingin Anda sertakan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.
    - Jika Anda ingin menerapkan kebijakan untuk semua kecuali satu set akun atau unit AWS Organizations organisasi (OU) tertentu, pilih Kecualikan akun dan unit organisasi yang ditentukan, dan sertakan semua akun lainnya, lalu tambahkan akun dan OU yang ingin Anda kecualikan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.

    Anda hanya dapat memilih salah satu opsi.

    Setelah menerapkan kebijakan, Firewall Manager secara otomatis mengevaluasi akun baru apa pun terhadap pengaturan Anda. Misalnya, jika Anda hanya menyertakan akun tertentu, Firewall Manager tidak menerapkan kebijakan tersebut ke akun baru yang berbeda. Sebagai contoh lain, jika Anda menyertakan OU, ketika Anda menambahkan akun ke OU atau ke salah satu OU anaknya, Firewall Manager secara otomatis menerapkan kebijakan tersebut ke akun baru.
12. Untuk tipe Sumber Daya, pengaturan ditetapkan di Subnet.
13. Untuk Sumber Daya, Anda dapat mempersempit cakupan kebijakan menggunakan penandaan, dengan menyertakan atau mengecualikan sumber daya dengan tag yang Anda tentukan. Anda dapat menggunakan inklusi atau pengecualian, dan bukan keduanya. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.

Jika Anda memasukkan lebih dari satu tag, sumber daya harus memiliki semua tag untuk disertakan atau dikecualikan.

Tag sumber daya hanya dapat memiliki nilai non-null. Jika Anda menghilangkan nilai untuk tag, Firewall Manager menyimpan tag dengan nilai string kosong: “”. Tag sumber daya hanya cocok dengan tag yang memiliki kunci yang sama dan nilai yang sama.

14. Pilih Selanjutnya.
15. Tinjau setelan kebijakan untuk memastikan setelan tersebut sesuai dengan yang Anda inginkan, lalu pilih Buat kebijakan.

Firewall Manager membuat kebijakan dan mulai memantau dan mengelola ACL jaringan dalam lingkup sesuai dengan pengaturan Anda. Untuk informasi selengkapnya tentang cara kerja kebijakan ini, lihatKebijakan ACL jaringan.

Membuat AWS Firewall Manager kebijakan untuk AWS Network Firewall

Dalam kebijakan Firewall Manager Network Firewall, Anda menggunakan grup aturan yang Anda kelola AWS Network Firewall. Untuk informasi tentang mengelola grup aturan, lihat grup AWS Network Firewall aturan di Panduan Pengembang Firewall Jaringan.

Untuk informasi tentang kebijakan Firewall Manager Network Firewall, lihatAWS Network Firewall kebijakan.

Untuk membuat kebijakan Firewall Manager untuk AWS Network Firewall (konsol)

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

   > **Note**
   >
   > Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

2. Di panel navigasi, pilih Kebijakan keamanan.
3. Pilih Buat kebijakan.

4. Untuk jenis Kebijakan, pilih AWS Network Firewall.
5. Di bawah Jenis manajemen Firewall, pilih cara Anda ingin Firewall Manager mengelola firewall kebijakan. Pilih dari salah satu pilihan berikut:

   - Distributed - Firewall Manager membuat dan memelihara titik akhir firewall di setiap VPC yang ada dalam lingkup kebijakan.
   - Terpusat - Firewall Manager membuat dan memelihara titik akhir dalam satu VPC inspeksi.
   - Impor firewall yang ada - Firewall Manager mengimpor firewall yang ada dari Network Firewall menggunakan kumpulan sumber daya. Untuk informasi tentang kumpulan sumber daya, lihatBekerja dengan kumpulan sumber daya di Firewall Manager.
6. Untuk Wilayah, pilih file Wilayah AWS. Untuk melindungi sumber daya di beberapa Wilayah, Anda harus membuat kebijakan terpisah untuk setiap Wilayah.
7. Pilih Selanjutnya.
8. Untuk nama Kebijakan, masukkan nama deskriptif. Firewall Manager menyertakan nama kebijakan dalam nama firewall Network Firewall dan kebijakan firewall yang dibuatnya.
9. Dalam konfigurasi AWS Network Firewall kebijakan, konfigurasikan kebijakan firewall seperti yang Anda lakukan di Network Firewall. Tambahkan grup aturan stateless dan stateful Anda dan tentukan tindakan default kebijakan. Anda dapat secara opsional menyetel urutan evaluasi aturan stateful kebijakan dan tindakan default, serta konfigurasi logging. Untuk informasi tentang manajemen kebijakan firewall Network Firewall, lihat kebijakan AWS Network Firewall firewall di Panduan AWS Network Firewall Pengembang.

   Saat Anda membuat kebijakan Firewall Manager Network Firewall, Firewall Manager membuat kebijakan firewall untuk akun yang berada dalam cakupan. Manajer akun individu dapat menambahkan grup aturan ke kebijakan firewall, tetapi mereka tidak dapat mengubah konfigurasi yang Anda berikan di sini.
10. Pilih Selanjutnya.
11. Lakukan salah satu hal berikut, tergantung pada jenis manajemen Firewall yang Anda pilih pada langkah sebelumnya:

    - Jika Anda menggunakan tipe manajemen firewall terdistribusi, dalam konfigurasi AWS Firewall Manager titik akhir di bawah lokasi titik akhir Firewall, pilih salah satu opsi berikut:
      - Konfigurasi endpoint khusus - Firewall Manager membuat firewall untuk setiap VPC dalam cakupan kebijakan, di Availability Zone yang Anda tentukan. Setiap firewall berisi setidaknya satu titik akhir firewall.

    - Di Availability Zones, pilih Availability Zones untuk membuat endpoint firewall. Anda dapat memilih Availability Zones berdasarkan nama Availability Zone atau dengan Availability Zone ID.
    - Jika Anda ingin menyediakan blok CIDR untuk Firewall Manager untuk digunakan untuk subnet firewall di VPC Anda, semuanya harus/28 blok CIDR. Masukkan satu blok per baris. Jika Anda menghilangkan ini, Firewall Manager memilih alamat IP untuk Anda dari yang tersedia di VPC.

      > **Note**
      >
      > Remediasi otomatis terjadi secara otomatis untuk kebijakan AWS Firewall Manager Network Firewall, sehingga Anda tidak akan melihat opsi untuk memilih untuk tidak melakukan perbaikan otomatis di sini.

  - Konfigurasi endpoint otomatis - Firewall Manager secara otomatis membuat titik akhir firewall di Availability Zones dengan subnet publik di VPC Anda.
    - Untuk konfigurasi endpoint Firewall, tentukan bagaimana Anda ingin endpoint firewall dikelola oleh Firewall Manager. Sebaiknya gunakan beberapa titik akhir untuk ketersediaan tinggi.
- Jika Anda menggunakan tipe manajemen firewall terpusat, dalam konfigurasi AWS Firewall Manager titik akhir di bawah konfigurasi VPC Inspeksi, masukkan ID AWS akun pemilik VPC inspeksi, dan ID VPC dari VPC inspeksi.
  - Di Availability Zones, pilih Availability Zones untuk membuat endpoint firewall. Anda dapat memilih Availability Zones berdasarkan nama Availability Zone atau dengan Availability Zone ID.
  - Jika Anda ingin menyediakan blok CIDR untuk Firewall Manager untuk digunakan untuk subnet firewall di VPC Anda, semuanya harus/28 blok CIDR. Masukkan satu blok per baris. Jika Anda menghilangkan ini, Firewall Manager memilih alamat IP untuk Anda dari yang tersedia di VPC.

    > **Note**
    >
    > Remediasi otomatis terjadi secara otomatis untuk kebijakan AWS Firewall Manager Network Firewall, sehingga Anda tidak akan melihat opsi untuk memilih untuk tidak melakukan perbaikan otomatis di sini.

- Jika Anda menggunakan jenis manajemen firewall firewall impor yang ada, dalam kumpulan Sumber daya tambahkan satu atau beberapa kumpulan sumber daya. Kumpulan sumber daya menentukan firewall Firewall Jaringan yang ada yang dimiliki oleh akun organisasi yang ingin Anda kelola secara terpusat dalam kebijakan ini. Untuk menambahkan kumpulan sumber daya ke kebijakan, Anda harus terlebih dahulu membuat kumpulan sumber daya menggunakan konsol atau PutResourceSetAPI. Untuk informasi tentang kumpulan sumber daya, lihatBekerja dengan kumpulan sumber daya di Firewall Manager. Untuk informasi selengkapnya tentang mengimpor firewall yang ada dari Network Firewall, lihat mengimpor firewall yang ada.

12. Pilih Selanjutnya.
13. Jika kebijakan Anda menggunakan jenis manajemen firewall terdistribusi, di bawah Manajemen rute, pilih apakah Firewall Manager akan memantau dan memperingatkan lalu lintas yang harus dialihkan melalui titik akhir firewall masing-masing atau tidak.

> **Note**
>
> Jika Anda memilih Monitor, Anda tidak dapat mengubah pengaturan ke Off di kemudian hari. Pemantauan berlanjut hingga Anda menghapus kebijakan.

14. Untuk jenis Lalu Lintas, secara opsional tambahkan titik akhir lalu lintas yang ingin Anda rutekan lalu lintas untuk inspeksi firewall.
15. Untuk Izinkan lalu lintas lintas lintas AZ yang diperlukan, jika Anda mengaktifkan opsi ini maka Firewall Manager memperlakukan perutean yang sesuai yang mengirimkan lalu lintas keluar dari Availability Zone untuk diperiksa, untuk Availability Zone yang tidak memiliki endpoint firewall sendiri. Availability Zone yang memiliki endpoint harus selalu memeriksa lalu lintas mereka sendiri.
16. Pilih Selanjutnya.
17. Untuk cakupan Kebijakan, berdasarkan kebijakan Akun AWS ini berlaku untuk, pilih opsi sebagai berikut:

    - Jika Anda ingin menerapkan kebijakan ke semua akun di organisasi Anda, tinggalkan pilihan default, Sertakan semua akun di AWS organisasi saya.
    - Jika Anda ingin menerapkan kebijakan hanya untuk akun atau akun tertentu yang berada di unit AWS Organizations organisasi tertentu (OU), pilih Sertakan hanya akun dan unit organisasi yang ditentukan, lalu tambahkan akun dan OU yang ingin Anda sertakan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.

- Jika Anda ingin menerapkan kebijakan untuk semua kecuali satu set akun atau unit AWS Organizations organisasi (OU) tertentu, pilih Kecualikan akun dan unit organisasi yang ditentukan, dan sertakan semua akun lainnya, lalu tambahkan akun dan OU yang ingin Anda kecualikan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.

Anda hanya dapat memilih salah satu opsi.

Setelah menerapkan kebijakan, Firewall Manager secara otomatis mengevaluasi akun baru apa pun terhadap pengaturan Anda. Misalnya, jika Anda hanya menyertakan akun tertentu, Firewall Manager tidak menerapkan kebijakan tersebut ke akun baru mana pun. Sebagai contoh lain, jika Anda menyertakan OU, ketika Anda menambahkan akun ke OU atau ke salah satu OU anaknya, Firewall Manager secara otomatis menerapkan kebijakan tersebut ke akun baru.

18. Jenis sumber daya untuk kebijakan Network Firewall adalah VPC.
19. Untuk Sumber Daya, Anda dapat mempersempit cakupan kebijakan menggunakan penandaan, dengan menyertakan atau mengecualikan sumber daya dengan tag yang Anda tentukan. Anda dapat menggunakan inklusi atau pengecualian, dan bukan keduanya. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.

    Jika Anda memasukkan lebih dari satu tag, sumber daya harus memiliki semua tag untuk disertakan atau dikecualikan.

    Tag sumber daya hanya dapat memiliki nilai non-null. Jika Anda menghilangkan nilai untuk tag, Firewall Manager menyimpan tag dengan nilai string kosong: “”. Tag sumber daya hanya cocok dengan tag yang memiliki kunci yang sama dan nilai yang sama.
20. Pilih Selanjutnya.
21. Untuk tag Kebijakan, tambahkan tag pengenal apa pun yang ingin Anda tambahkan ke sumber daya kebijakan Manajer Firewall. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.
22. Pilih Selanjutnya.
23. Tinjau pengaturan kebijakan baru dan kembali ke halaman mana pun yang Anda perlukan untuk penyesuaian apa pun.

    Jika Anda puas dengan kebijakan ini, pilih Create policy (Buat kebijakan). Di panel AWS Firewall Manager kebijakan, kebijakan Anda harus dicantumkan. Ini mungkin akan menunjukkan Pending di bawah judul akun dan itu akan menunjukkan status pengaturan remediasi otomatis.

Pembuatan kebijakan dapat memakan waktu beberapa menit. Setelah Status tertunda diganti dengan jumlah akun, Anda dapat memilih nama kebijakan untuk menjelajahi status kepatuhan akun dan sumber daya. Untuk informasi, lihat Melihat informasi kepatuhan untuk suatu AWS Firewall Manager kebijakan

Membuat AWS Firewall Manager kebijakan untuk Amazon Route 53 Resolver DNS Firewall

Dalam kebijakan Firewall Manager DNS Firewall, Anda menggunakan grup aturan yang Anda kelola di Amazon Route 53 Resolver DNS Firewall. Untuk informasi tentang mengelola grup aturan, lihat Mengelola grup aturan dan aturan di DNS Firewall di Panduan Pengembang Amazon Route 53.

Untuk informasi tentang kebijakan Firewall Manager DNS Firewall, lihatKebijakan Firewall DNS Resolver Amazon Route 53.

Untuk membuat kebijakan Firewall Manager untuk Amazon Route 53 Resolver DNS Firewall (konsol)

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

   > **Note**
   >
   > Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

2. Di panel navigasi, pilih Kebijakan keamanan.
3. Pilih Buat kebijakan.
4. Untuk jenis Kebijakan, pilih Amazon Route 53 Resolver DNS Firewall.
5. Untuk Wilayah, pilih file Wilayah AWS. Untuk melindungi sumber daya di beberapa Wilayah, Anda harus membuat kebijakan terpisah untuk setiap Wilayah.
6. Pilih Selanjutnya.
7. Untuk nama Kebijakan, masukkan nama deskriptif.
8. Dalam konfigurasi kebijakan, tambahkan grup aturan yang ingin dievaluasi oleh DNS Firewall terlebih dahulu dan terakhir di antara asosiasi grup aturan VPC Anda. Anda dapat menambahkan hingga dua grup aturan ke kebijakan.

Saat Anda membuat kebijakan Firewall Manager DNS Firewall, Firewall Manager membuat asosiasi grup aturan, dengan prioritas asosiasi yang Anda berikan, untuk VPC dan akun yang berada dalam cakupan. Manajer akun individu dapat menambahkan asosiasi grup aturan di antara asosiasi pertama dan terakhir Anda, tetapi mereka tidak dapat mengubah asosiasi yang Anda tentukan di sini. Untuk informasi selengkapnya, lihat Kebijakan Firewall DNS Resolver Amazon Route 53.

9. Pilih Berikutnya.
10. Untuk kebijakan Akun AWS ini berlaku, pilih opsi sebagai berikut:

    - Jika Anda ingin menerapkan kebijakan ke semua akun di organisasi Anda, tinggalkan pilihan default, Sertakan semua akun di AWS organisasi saya.
    - Jika Anda ingin menerapkan kebijakan hanya untuk akun atau akun tertentu yang berada di unit AWS Organizations organisasi tertentu (OU), pilih Sertakan hanya akun dan unit organisasi yang ditentukan, lalu tambahkan akun dan OU yang ingin Anda sertakan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.
    - Jika Anda ingin menerapkan kebijakan untuk semua kecuali satu set akun atau unit AWS Organizations organisasi (OU) tertentu, pilih Kecualikan akun dan unit organisasi yang ditentukan, dan sertakan semua akun lainnya, lalu tambahkan akun dan OU yang ingin Anda kecualikan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.

    Anda hanya dapat memilih salah satu opsi.

    Setelah menerapkan kebijakan, Firewall Manager secara otomatis mengevaluasi akun baru apa pun terhadap pengaturan Anda. Misalnya, jika Anda hanya menyertakan akun tertentu, Firewall Manager tidak menerapkan kebijakan tersebut ke akun baru mana pun. Sebagai contoh lain, jika Anda menyertakan OU, ketika Anda menambahkan akun ke OU atau ke salah satu OU anaknya, Firewall Manager secara otomatis menerapkan kebijakan tersebut ke akun baru.
11. Jenis sumber daya untuk kebijakan DNS Firewall adalah VPC.
12. Untuk Sumber Daya, Anda dapat mempersempit cakupan kebijakan menggunakan penandaan, dengan menyertakan atau mengecualikan sumber daya dengan tag yang Anda tentukan. Anda dapat menggunakan inklusi atau pengecualian, dan bukan keduanya. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.

Jika Anda memasukkan lebih dari satu tag, sumber daya harus memiliki semua tag untuk disertakan atau dikecualikan.

Tag sumber daya hanya dapat memiliki nilai non-null. Jika Anda menghilangkan nilai untuk tag, Firewall Manager menyimpan tag dengan nilai string kosong: “”. Tag sumber daya hanya cocok dengan tag yang memiliki kunci yang sama dan nilai yang sama.

13. Pilih Selanjutnya.
14. Untuk tag Kebijakan, tambahkan tag pengenal apa pun yang ingin Anda tambahkan ke sumber daya kebijakan Manajer Firewall. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.
15. Pilih Selanjutnya.
16. Tinjau pengaturan kebijakan baru dan kembali ke halaman mana pun yang Anda perlukan untuk penyesuaian apa pun.

    Jika Anda puas dengan kebijakan ini, pilih Create policy (Buat kebijakan). Di panel AWS Firewall Manager kebijakan, kebijakan Anda harus dicantumkan. Ini mungkin akan menunjukkan Pending di bawah judul akun dan itu akan menunjukkan status pengaturan remediasi otomatis. Pembuatan kebijakan dapat memakan waktu beberapa menit. Setelah Status tertunda diganti dengan jumlah akun, Anda dapat memilih nama kebijakan untuk menjelajahi status kepatuhan akun dan sumber daya. Untuk informasi, lihat Melihat informasi kepatuhan untuk suatu AWS Firewall Manager kebijakan

Membuat AWS Firewall Manager kebijakan untuk Palo Alto Networks Cloud NGFW

Dengan kebijakan Firewall Manager untuk Palo Alto Networks Cloud Next Generation Firewall (Palo Alto Networks Cloud NGFW), Anda menggunakan Firewall Manager untuk menyebarkan sumber daya Palo Alto Networks Cloud NGFW, dan mengelola tumpukan aturan NGFW secara terpusat di semua akun Anda. AWS

Untuk informasi tentang kebijakan Firewall Manager Palo Alto Networks Cloud NGFW, lihat. Kebijakan Palo Alto Networks Cloud NGFW Untuk informasi tentang cara mengkonfigurasi dan mengelola Palo Alto Networks Cloud NGFW untuk Firewall Manager, lihat Palo Alto Networks Palo Alto Networks Cloud NGFW pada dokumentasi. AWS

Prasyarat

Ada beberapa langkah wajib untuk mempersiapkan akun Anda AWS Firewall Manager. Langkah-langkah tersebut dijelaskan dalamAWS Firewall Manager prasyarat. Lengkapi semua prasyarat sebelum melanjutkan ke langkah berikutnya.

Untuk membuat kebijakan Firewall Manager untuk Palo Alto Networks Cloud NGFW (konsol)

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

   > **Note**
   >
   > Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

2. Di panel navigasi, pilih Kebijakan keamanan.
3. Pilih Buat kebijakan.
4. Untuk jenis Kebijakan, pilih Palo Alto Networks Cloud NGFW. Jika Anda belum berlangganan layanan Palo Alto Networks Cloud NGFW di AWS Marketplace, Anda harus melakukannya terlebih dahulu. Untuk berlangganan AWS Marketplace, pilih Lihat detail AWS Marketplace.
5. Untuk model Deployment, pilih model Terdistribusi atau model Terpusat. Model penerapan menentukan cara Firewall Manager mengelola titik akhir untuk kebijakan tersebut. Dengan model terdistribusi, Firewall Manager mempertahankan titik akhir firewall di setiap VPC yang berada dalam cakupan kebijakan. Dengan model terpusat, Firewall Manager mempertahankan satu titik akhir dalam VPC inspeksi.
6. Untuk Wilayah, pilih file Wilayah AWS. Untuk melindungi sumber daya di beberapa Wilayah, Anda harus membuat kebijakan terpisah untuk setiap Wilayah.
7. Pilih Selanjutnya.
8. Untuk nama Kebijakan, masukkan nama deskriptif.
9. Dalam konfigurasi kebijakan, pilih kebijakan firewall Palo Alto Networks Cloud NGFW untuk dikaitkan dengan kebijakan ini. Daftar kebijakan firewall Palo Alto Networks Cloud NGFW berisi semua kebijakan firewall Palo Alto Networks Cloud NGFW yang terkait dengan penyewa Palo Alto Networks Cloud NGFW Anda. Untuk informasi tentang membuat dan mengelola kebijakan firewall Palo Alto Networks Cloud NGFW, lihat panduan Deploy Palo Alto Networks Cloud NGFW

untuk AWS Firewall Manager topik di Palo Alto Networks Cloud NGFW untuk AWS panduan penerapan. AWS

10. Untuk pencatatan Palo Alto Networks Cloud NGFW - opsional, pilih jenis log Palo Alto Networks Cloud NGFW mana yang akan dicatat untuk kebijakan Anda. Untuk informasi tentang jenis log Palo Alto Networks Cloud NGFW, lihat Mengkonfigurasi Logging untuk Palo Alto Networks Cloud NGFW AWS di Palo Alto Networks Cloud NGFW untuk panduan penerapan. AWS

    Untuk tujuan log, tentukan kapan Firewall Manager harus menulis log ke.

11. Pilih Selanjutnya.
12. Di bawah Konfigurasi titik akhir firewall pihak ketiga lakukan salah satu hal berikut, tergantung pada apakah Anda menggunakan model penyebaran terdistribusi atau terpusat untuk membuat titik akhir firewall Anda:

    - Jika Anda menggunakan model penerapan terdistribusi untuk kebijakan ini, di bawah Availability Zones, pilih Availability Zones untuk membuat endpoint firewall. Anda dapat memilih Availability Zones berdasarkan nama Availability Zone atau dengan Availability Zone ID.
    - Jika Anda menggunakan model penerapan terpusat untuk kebijakan ini, dalam konfigurasi AWS Firewall Manager titik akhir di bawah konfigurasi VPC Inspeksi, masukkan ID AWS akun pemilik VPC inspeksi, dan ID VPC VPC inspeksi.
        - Di Availability Zones, pilih Availability Zones untuk membuat endpoint firewall. Anda dapat memilih Availability Zones berdasarkan nama Availability Zone atau dengan Availability Zone ID.
13. Jika Anda ingin menyediakan blok CIDR untuk Firewall Manager untuk digunakan untuk subnet firewall di VPC Anda, semuanya harus/28 blok CIDR. Masukkan satu blok per baris. Jika Anda menghilangkan ini, Firewall Manager memilih alamat IP untuk Anda dari yang tersedia di VPC.

    > **Note**
    >
    > Remediasi otomatis terjadi secara otomatis untuk kebijakan AWS Firewall Manager Network Firewall, sehingga Anda tidak akan melihat opsi untuk memilih untuk tidak melakukan perbaikan otomatis di sini.

14. Pilih Selanjutnya.
15. Untuk cakupan Kebijakan, berdasarkan kebijakan Akun AWS ini berlaku untuk, pilih opsi sebagai berikut:

- Jika Anda ingin menerapkan kebijakan ke semua akun di organisasi Anda, tinggalkan pilihan default, Sertakan semua akun di AWS organisasi saya.
- Jika Anda ingin menerapkan kebijakan hanya untuk akun atau akun tertentu yang berada di unit AWS Organizations organisasi tertentu (OU), pilih Sertakan hanya akun dan unit organisasi yang ditentukan, lalu tambahkan akun dan OU yang ingin Anda sertakan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.
- Jika Anda ingin menerapkan kebijakan untuk semua kecuali satu set akun atau unit AWS Organizations organisasi (OU) tertentu, pilih Kecualikan akun dan unit organisasi yang ditentukan, dan sertakan semua akun lainnya, lalu tambahkan akun dan OU yang ingin Anda kecualikan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.

Anda hanya dapat memilih salah satu opsi.

Setelah menerapkan kebijakan, Firewall Manager secara otomatis mengevaluasi akun baru apa pun terhadap pengaturan Anda. Misalnya, jika Anda hanya menyertakan akun tertentu, Firewall Manager tidak menerapkan kebijakan tersebut ke akun baru mana pun. Sebagai contoh lain, jika Anda menyertakan OU, ketika Anda menambahkan akun ke OU atau ke salah satu OU anaknya, Firewall Manager secara otomatis menerapkan kebijakan tersebut ke akun baru.

16. Jenis sumber daya untuk kebijakan Network Firewall adalah VPC.
17. Untuk Sumber Daya, Anda dapat mempersempit cakupan kebijakan menggunakan penandaan, dengan menyertakan atau mengecualikan sumber daya dengan tag yang Anda tentukan. Anda dapat menggunakan inklusi atau pengecualian, dan bukan keduanya. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.

    Jika Anda memasukkan lebih dari satu tag, sumber daya harus memiliki semua tag untuk disertakan atau dikecualikan.

    Tag sumber daya hanya dapat memiliki nilai non-null. Jika Anda menghilangkan nilai untuk tag, Firewall Manager menyimpan tag dengan nilai string kosong: “”. Tag sumber daya hanya cocok dengan tag yang memiliki kunci yang sama dan nilai yang sama.
18. Untuk akses lintas akun Grant, pilih Unduh AWS CloudFormation template. Ini mengunduh AWS CloudFormation template yang dapat Anda gunakan untuk membuat AWS CloudFormation tumpukan. Tumpukan ini menciptakan AWS Identity and Access Management peran yang

memberikan izin lintas akun Firewall Manager untuk mengelola sumber daya Palo Alto Networks Cloud NGFW. Untuk informasi tentang tumpukan, lihat Bekerja dengan tumpukan di AWS CloudFormation Panduan Pengguna.

19. Pilih Selanjutnya.
20. Untuk tag Kebijakan, tambahkan tag pengenal apa pun yang ingin Anda tambahkan ke sumber daya kebijakan Manajer Firewall. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.
21. Pilih Selanjutnya.
22. Tinjau pengaturan kebijakan baru dan kembali ke halaman mana pun yang Anda perlukan untuk penyesuaian apa pun.

    Jika Anda puas dengan kebijakan ini, pilih Create policy (Buat kebijakan). Di panel AWS Firewall Manager kebijakan, kebijakan Anda harus dicantumkan. Ini mungkin akan menunjukkan Pending di bawah judul akun dan itu akan menunjukkan status pengaturan remediasi otomatis. Pembuatan kebijakan dapat memakan waktu beberapa menit. Setelah Status tertunda diganti dengan jumlah akun, Anda dapat memilih nama kebijakan untuk menjelajahi status kepatuhan akun dan sumber daya. Untuk informasi, lihat Melihat informasi kepatuhan untuk suatu AWS Firewall Manager kebijakan

Membuat AWS Firewall Manager kebijakan untuk Fortigate Cloud Native Firewall (CNF) sebagai Layanan

Dengan kebijakan Firewall Manager untuk Fortigate CNF, Anda dapat menggunakan Firewall Manager untuk menyebarkan dan mengelola sumber daya Fortigate CNF di semua akun Anda. AWS

Untuk informasi tentang kebijakan Firewall Manager Fortigate CNF, lihat. Fortigate Cloud Native Firewall (CNF) sebagai kebijakan Layanan Untuk informasi tentang cara mengkonfigurasi Fortigate CNF untuk digunakan dengan Firewall Manager, lihat dokumentasi Fortinet.

Prasyarat

Ada beberapa langkah wajib untuk mempersiapkan akun Anda AWS Firewall Manager. Langkah-langkah tersebut dijelaskan dalamAWS Firewall Manager prasyarat. Lengkapi semua prasyarat sebelum melanjutkan ke langkah berikutnya.

Untuk membuat kebijakan Firewall Manager untuk Fortigate CNF (konsol)

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

   > **Note**
   >
   > Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

2. Di panel navigasi, pilih Kebijakan keamanan.
3. Pilih Buat kebijakan.
4. Untuk jenis Kebijakan, pilih Fortigate Cloud Native Firewall (CNF) sebagai Layanan. Jika Anda belum berlangganan layanan Fortigate CNF di AWS Marketplace, Anda harus melakukannya terlebih dahulu. Untuk berlangganan AWS Marketplace, pilih Lihat detail AWS Marketplace.
5. Untuk model Deployment, pilih model Terdistribusi atau model Terpusat. Model penerapan menentukan cara Firewall Manager mengelola titik akhir untuk kebijakan tersebut. Dengan model terdistribusi, Firewall Manager mempertahankan titik akhir firewall di setiap VPC yang berada dalam cakupan kebijakan. Dengan model terpusat, Firewall Manager mempertahankan satu titik akhir dalam VPC inspeksi.
6. Untuk Wilayah, pilih file Wilayah AWS. Untuk melindungi sumber daya di beberapa Wilayah, Anda harus membuat kebijakan terpisah untuk setiap Wilayah.
7. Pilih Selanjutnya.
8. Untuk nama Kebijakan, masukkan nama deskriptif.
9. Dalam konfigurasi kebijakan, pilih kebijakan firewall Fortigate CNF untuk dikaitkan dengan kebijakan ini. Daftar kebijakan firewall Fortigate CNF berisi semua kebijakan firewall Fortigate CNF yang terkait dengan penyewa Fortigate CNF Anda. Untuk informasi tentang membuat dan mengelola penyewa Fortigate CNF, lihat dokumentasi Fortinet.
10. Pilih Selanjutnya.
11. Di bawah Konfigurasi titik akhir firewall pihak ketiga lakukan salah satu hal berikut, tergantung pada apakah Anda menggunakan model penyebaran terdistribusi atau terpusat untuk membuat titik akhir firewall Anda:

- Jika Anda menggunakan model penerapan terdistribusi untuk kebijakan ini, di bawah Availability Zones, pilih Availability Zones untuk membuat endpoint firewall. Anda dapat memilih Availability Zones berdasarkan nama Availability Zone atau dengan Availability Zone ID.
- Jika Anda menggunakan model penerapan terpusat untuk kebijakan ini, dalam konfigurasi AWS Firewall Manager titik akhir di bawah konfigurasi VPC Inspeksi, masukkan ID AWS akun pemilik VPC inspeksi, dan ID VPC VPC inspeksi.
  - Di Availability Zones, pilih Availability Zones untuk membuat endpoint firewall. Anda dapat memilih Availability Zones berdasarkan nama Availability Zone atau dengan Availability Zone ID.

12. Jika Anda ingin menyediakan blok CIDR untuk Firewall Manager untuk digunakan untuk subnet firewall di VPC Anda, semuanya harus/28 blok CIDR. Masukkan satu blok per baris. Jika Anda menghilangkan ini, Firewall Manager memilih alamat IP untuk Anda dari yang tersedia di VPC.

> **Note**
>
> Remediasi otomatis terjadi secara otomatis untuk kebijakan AWS Firewall Manager Network Firewall, sehingga Anda tidak akan melihat opsi untuk memilih untuk tidak melakukan perbaikan otomatis di sini.

13. Pilih Selanjutnya.
14. Untuk cakupan Kebijakan, berdasarkan kebijakan Akun AWS ini berlaku untuk, pilih opsi sebagai berikut:

- Jika Anda ingin menerapkan kebijakan ke semua akun di organisasi Anda, tinggalkan pilihan default, Sertakan semua akun di AWS organisasi saya.
- Jika Anda ingin menerapkan kebijakan hanya untuk akun atau akun tertentu yang berada di unit AWS Organizations organisasi tertentu (OU), pilih Sertakan hanya akun dan unit organisasi yang ditentukan, lalu tambahkan akun dan OU yang ingin Anda sertakan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.
- Jika Anda ingin menerapkan kebijakan untuk semua kecuali satu set akun atau unit AWS Organizations organisasi (OU) tertentu, pilih Kecualikan akun dan unit organisasi yang ditentukan, dan sertakan semua akun lainnya, lalu tambahkan akun dan OU yang ingin Anda

kecualikan. Menentukan OU adalah setara dengan menentukan semua akun di OU dan di salah satu OU turunan, termasuk setiap OU turunan dan akun yang ditambahkan di lain waktu.

Anda hanya dapat memilih salah satu opsi.

Setelah menerapkan kebijakan, Firewall Manager secara otomatis mengevaluasi akun baru apa pun terhadap pengaturan Anda. Misalnya, jika Anda hanya menyertakan akun tertentu, Firewall Manager tidak menerapkan kebijakan tersebut ke akun baru mana pun. Sebagai contoh lain, jika Anda menyertakan OU, ketika Anda menambahkan akun ke OU atau ke salah satu OU anaknya, Firewall Manager secara otomatis menerapkan kebijakan tersebut ke akun baru.

15. Jenis sumber daya untuk kebijakan Network Firewall adalah VPC.
16. Untuk Sumber Daya, Anda dapat mempersempit cakupan kebijakan menggunakan penandaan, dengan menyertakan atau mengecualikan sumber daya dengan tag yang Anda tentukan. Anda dapat menggunakan inklusi atau pengecualian, dan bukan keduanya. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.

    Jika Anda memasukkan lebih dari satu tag, sumber daya harus memiliki semua tag untuk disertakan atau dikecualikan.

    Tag sumber daya hanya dapat memiliki nilai non-null. Jika Anda menghilangkan nilai untuk tag, Firewall Manager menyimpan tag dengan nilai string kosong: “”. Tag sumber daya hanya cocok dengan tag yang memiliki kunci yang sama dan nilai yang sama.
17. Untuk akses lintas akun Grant, pilih Unduh AWS CloudFormation template. Ini mengunduh AWS CloudFormation template yang dapat Anda gunakan untuk membuat AWS CloudFormation tumpukan. Tumpukan ini menciptakan AWS Identity and Access Management peran yang memberikan izin lintas akun Firewall Manager untuk mengelola sumber daya CNF Fortigate. Untuk informasi tentang tumpukan, lihat Bekerja dengan tumpukan di AWS CloudFormation Panduan Pengguna. Untuk membuat tumpukan, Anda memerlukan ID akun dari portal Fortigate CNF.
18. Pilih Selanjutnya.
19. Untuk tag Kebijakan, tambahkan tag pengenal apa pun yang ingin Anda tambahkan ke sumber daya kebijakan Manajer Firewall. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.
20. Pilih Selanjutnya.
21. Tinjau pengaturan kebijakan baru dan kembali ke halaman mana pun yang Anda perlukan untuk penyesuaian apa pun.

Jika Anda puas dengan kebijakan ini, pilih Create policy (Buat kebijakan). Di panel AWS Firewall Manager kebijakan, kebijakan Anda harus dicantumkan. Ini mungkin akan menunjukkan Pending di bawah judul akun dan itu akan menunjukkan status pengaturan remediasi otomatis. Pembuatan kebijakan dapat memakan waktu beberapa menit. Setelah Status tertunda diganti dengan jumlah akun, Anda dapat memilih nama kebijakan untuk menjelajahi status kepatuhan akun dan sumber daya. Untuk informasi, lihat Melihat informasi kepatuhan untuk suatu AWS Firewall Manager kebijakan

Menghapus kebijakan AWS Firewall Manager

Anda dapat menghapus kebijakan Firewall Manager dengan melakukan langkah-langkah berikut.

Untuk menghapus kebijakan (konsol)

1. Di panel navigasi, pilih Kebijakan keamanan.
2. Pilih opsi di samping kebijakan yang ingin Anda hapus.
3. Pilih Hapus.

> **Note**
>
> Saat Anda menghapus kebijakan grup keamanan umum Manajer Firewall, untuk menghapus grup keamanan replika kebijakan, pilih opsi untuk membersihkan sumber daya yang dibuat oleh kebijakan tersebut. Jika tidak, setelah primer dihapus, replika tetap dan memerlukan manajemen manual di setiap instance VPC Amazon.

> **Important**
>
> Saat Anda menghapus kebijakan Firewall Manager Shield Advanced, kebijakan tersebut akan dihapus, tetapi akun Anda tetap berlangganan Shield Advanced.

AWS Firewall Manager ruang lingkup kebijakan

Ruang lingkup kebijakan menentukan di mana kebijakan tersebut berlaku. Anda dapat menerapkan kebijakan yang dikontrol secara terpusat ke semua akun dan sumber daya dalam organisasi Anda

di AWS Organizations, atau ke subset akun dan sumber daya Anda. Untuk petunjuk tentang cara menyetel cakupan kebijakan, lihatMembuat AWS Firewall Manager kebijakan.

Opsi cakupan kebijakan di AWS Firewall Manager

Saat Anda menambahkan akun atau sumber daya baru ke organisasi Anda, Firewall Manager secara otomatis menilainya terhadap setelan Anda untuk setiap kebijakan dan menerapkan kebijakan berdasarkan setelan ini. Misalnya, Anda dapat memilih untuk menerapkan kebijakan ke semua akun kecuali nomor akun dalam daftar tertentu; Anda juga dapat memilih untuk menerapkan kebijakan hanya pada sumber daya yang memiliki semua tag dalam daftar.

Akun AWS dalam ruang lingkup

Pengaturan yang Anda berikan untuk menentukan kebijakan yang Akun AWS terpengaruh menentukan akun mana di AWS organisasi Anda yang akan menerapkan kebijakan tersebut. Anda dapat memilih untuk menerapkan kebijakan dengan salah satu cara berikut:

- Ke semua akun di organisasi Anda
- Untuk hanya daftar spesifik nomor akun dan unit AWS Organizations organisasi (OU) yang disertakan
- Untuk semua kecuali daftar spesifik nomor akun yang dikecualikan dan unit AWS Organizations organisasi (OU)

Untuk selengkapnya AWS Organizations, lihat Panduan AWS Organizations Pengguna.

Sumber daya dalam ruang lingkup

Sama halnya dengan pengaturan untuk akun dalam cakupan, setelan yang Anda sediakan untuk sumber daya menentukan jenis sumber daya dalam lingkup mana yang akan diterapkan kebijakan tersebut. Anda dapat memilih salah satu dari yang berikut ini:

- Semua sumber daya
- Sumber daya yang memiliki semua tag yang Anda tentukan
- Semua sumber daya kecuali yang memiliki semua tag yang Anda tentukan

Anda hanya dapat menentukan tag sumber daya dengan nilai non-null. Jika Anda tidak memberikan apa pun untuk nilainya, Firewall Manager menyimpan tag dengan nilai string kosong: “”. Tag sumber daya hanya cocok dengan tag yang memiliki kunci yang sama dan nilai yang sama.

Untuk informasi selengkapnya tentang menandai sumber daya Anda, lihat Bekerja dengan Editor Tag.

Manajemen lingkup kebijakan di AWS Firewall Manager

Ketika kebijakan diberlakukan, Firewall Manager mengelolanya terus menerus dan menerapkannya ke sumber baru Akun AWS dan sumber daya saat ditambahkan, sesuai dengan ruang lingkup kebijakan.

Bagaimana Firewall Manager mengelola Akun AWS dan sumber daya

Jika akun atau sumber daya keluar dari cakupan karena alasan apa pun, AWS Firewall Manager tidak secara otomatis menghapus perlindungan atau menghapus sumber daya yang dikelola Manajer Firewall kecuali Anda memilih kotak centang Hapus perlindungan secara otomatis dari sumber daya yang meninggalkan cakupan kebijakan.

> **Note**
>
> Opsi secara otomatis menghapus perlindungan dari sumber daya yang meninggalkan cakupan kebijakan tidak tersedia AWS Shield Advanced atau kebijakan AWS WAF Klasik.

Memilih kotak centang ini akan mengarahkan AWS Firewall Manager untuk secara otomatis membersihkan sumber daya yang dikelola Manajer Firewall untuk akun saat akun tersebut meninggalkan cakupan kebijakan. Misalnya, Firewall Manager akan memisahkan ACL web yang dikelola Manajer Firewall dari sumber daya pelanggan yang dilindungi saat sumber daya pelanggan meninggalkan cakupan kebijakan.

Untuk menentukan sumber daya mana yang harus dihapus dari perlindungan saat sumber daya pelanggan meninggalkan cakupan kebijakan, Firewall Manager mengikuti pedoman berikut:

- Perilaku default:
  - Aturan AWS Config terkelola terkait dihapus. Perilaku ini tidak tergantung pada kotak centang.
  - Setiap daftar kontrol akses AWS WAF web terkait (ACL web) yang tidak berisi sumber daya apa pun akan dihapus. Perilaku ini tidak tergantung pada kotak centang.
  - Setiap sumber daya yang dilindungi yang keluar dari ruang lingkup tetap terkait dan dilindungi. Misalnya, Application Load Balancer atau API dari API Gateway yang terkait dengan ACL web tetap terkait dengan ACL web, dan proteksi tetap ada.

- Dengan kotak centang Hapus perlindungan secara otomatis dari sumber daya yang meninggalkan cakupan kebijakan dipilih:
  - Aturan AWS Config terkelola terkait dihapus. Perilaku ini tidak tergantung pada kotak centang.
  - Setiap daftar kontrol akses AWS WAF web terkait (ACL web) yang tidak berisi sumber daya apa pun akan dihapus. Perilaku ini tidak tergantung pada kotak centang.
  - Setiap sumber daya yang dilindungi yang keluar dari cakupan secara otomatis dipisahkan dan dihapus dari perlindungan Firewall Manager ketika meninggalkan cakupan kebijakan. Misalnya, untuk kebijakan grup keamanan, akselerator Elastic Inference atau instans Amazon EC2 secara otomatis dipisahkan dari grup keamanan yang direplikasi saat meninggalkan cakupan kebijakan. Grup keamanan yang direplikasi dan sumber dayanya secara otomatis dihapus dari perlindungan.

Daftar terkelola

Daftar aplikasi dan protokol terkelola merampingkan konfigurasi dan pengelolaan kebijakan grup keamanan audit AWS Firewall Manager konten Anda. Anda menggunakan daftar terkelola untuk menentukan protokol dan aplikasi yang diizinkan dan dilarang oleh kebijakan Anda. Untuk informasi tentang kebijakan grup keamanan audit konten, lihatKebijakan grup keamanan audit konten.

Anda dapat menggunakan jenis daftar terkelola berikut dalam kebijakan grup keamanan audit konten:

- Daftar aplikasi Firewall Manager dan daftar protokol — Firewall Manager mengelola daftar ini.
  - Daftar aplikasi termasuk `FMS-Default-Public-Access-Apps-Allowed` dan`FMS-Default-Public-Access-Apps-Denied`, yang menggambarkan aplikasi yang umum digunakan yang harus diizinkan atau ditolak kepada masyarakat umum.
  - Daftar protokol termasuk`FMS-Default-Protocols-Allowed`, daftar protokol yang umum digunakan yang harus diizinkan untuk masyarakat umum. Anda dapat menggunakan daftar apa pun yang dikelola Firewall Manager, tetapi Anda tidak dapat mengedit atau menghapusnya.
- Daftar aplikasi kustom dan daftar protokol — Anda mengelola daftar ini. Anda dapat membuat daftar dari kedua jenis dengan pengaturan yang Anda butuhkan. Anda memiliki kontrol penuh atas daftar terkelola kustom Anda sendiri, dan Anda dapat membuat, mengedit, dan menghapusnya sesuai kebutuhan.

> **Note**
>
> Saat ini, Firewall Manager tidak memeriksa referensi ke daftar terkelola kustom saat Anda menghapusnya. Ini berarti Anda dapat menghapus daftar aplikasi terkelola kustom atau daftar protokol bahkan ketika sedang digunakan oleh kebijakan aktif. Hal ini dapat menyebabkan kebijakan berhenti berfungsi. Hapus daftar aplikasi atau daftar protokol hanya setelah Anda memverifikasi bahwa itu tidak direferensikan oleh kebijakan aktif apa pun.

Daftar terkelola adalah AWS sumber daya. Anda dapat menandai daftar terkelola kustom. Anda tidak dapat menandai daftar terkelola Firewall Manager.

Pembuatan versi daftar terkelola

Daftar terkelola kustom tidak memiliki versi. Saat Anda mengedit daftar kustom, kebijakan yang mereferensikan daftar secara otomatis menggunakan daftar yang diperbarui.

Daftar terkelola Firewall Manager berversi. Tim layanan Firewall Manager menerbitkan versi baru sesuai kebutuhan, untuk menerapkan praktik keamanan terbaik ke daftar.

Saat Anda menggunakan daftar terkelola Firewall Manager dalam kebijakan, Anda memilih strategi pembuatan versi sebagai berikut:

- Versi terbaru yang tersedia — Jika Anda tidak menentukan setelan versi eksplisit untuk daftar, kebijakan Anda akan secara otomatis menggunakan versi terbaru. Ini adalah satu-satunya opsi yang tersedia melalui konsol.
- Versi eksplisit — Jika Anda menentukan versi untuk daftar, kebijakan Anda akan menggunakan versi tersebut. Kebijakan Anda tetap terkunci ke versi yang Anda tentukan hingga Anda mengubah setelan versi. Untuk menentukan versi, Anda harus menentukan kebijakan di luar konsol, misalnya melalui CLI atau salah satu SDK.

Untuk informasi selengkapnya tentang memilih setelan versi untuk daftar, lihatMenggunakan daftar terkelola dalam kebijakan grup keamanan audit konten.

Menggunakan daftar terkelola dalam kebijakan grup keamanan audit konten

Saat membuat kebijakan grup keamanan audit konten, Anda dapat memilih untuk menggunakan aturan kebijakan audit terkelola. Beberapa pengaturan untuk opsi ini memerlukan daftar aplikasi terkelola atau daftar protokol. Contoh pengaturan ini termasuk protokol yang diizinkan dalam aturan grup keamanan dan aplikasi dapat mengakses internet.

Pembatasan berikut berlaku untuk setiap setelan kebijakan yang menggunakan daftar terkelola:

- Anda dapat menentukan paling banyak satu daftar terkelola Firewall Manager untuk pengaturan apa pun. Secara default, Anda dapat menentukan paling banyak satu daftar kustom. Batas daftar kustom adalah kuota lunak, sehingga Anda dapat meminta kenaikan untuk itu. Untuk informasi selengkapnya, lihat AWS Firewall Manager kuota.
- Di konsol, jika Anda memilih daftar terkelola Firewall Manager, Anda tidak dapat menentukan versinya. Kebijakan akan selalu menggunakan versi terbaru dari daftar. Untuk menentukan versi, Anda harus menentukan kebijakan di luar konsol, misalnya melalui CLI atau salah satu SDK. Untuk informasi tentang pembuatan versi untuk daftar terkelola Firewall Manager, lihat. Pembuatan versi daftar terkelola

Untuk informasi tentang membuat kebijakan grup keamanan audit konten melalui konsol, lihatMembuat kebijakan grup keamanan audit konten.

Membuat daftar aplikasi terkelola kustom

Untuk membuat daftar aplikasi terkelola kustom

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

   > **Note**
   >
   > Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

2. Di panel navigasi, pilih Daftar aplikasi.
3. Di halaman Daftar aplikasi, pilih Buat daftar aplikasi.

4. Di halaman Buat daftar aplikasi, beri nama daftar Anda. Jangan gunakan awalan `fms-` karena ini dicadangkan untuk Firewall Manager.
5. Tentukan aplikasi baik dengan memberikan protokol dan nomor port atau dengan memilih aplikasi dari drop down Type. Beri nama spesifikasi aplikasi Anda.
6. Pilih Tambahkan yang lain sesuai kebutuhan dan isi informasi aplikasi sampai Anda menyelesaikan daftar Anda.
7. (Opsional) Terapkan tag ke daftar Anda.
8. Pilih Simpan untuk menyimpan daftar Anda dan kembali ke halaman Daftar aplikasi.

Membuat daftar protokol terkelola kustom

Untuk membuat daftar protokol terkelola kustom

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

   > **Note**
   >
   > Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

2. Di panel navigasi, pilih Daftar protokol.
3. Di halaman daftar Protokol, pilih Buat daftar protokol.
4. Di halaman pembuatan daftar protokol, beri nama daftar Anda. Jangan gunakan awalan `fms-` karena ini dicadangkan untuk Firewall Manager.
5. Tentukan protokol.
6. Pilih Tambahkan yang lain sesuai kebutuhan dan isi informasi protokol sampai Anda menyelesaikan daftar Anda.
7. (Opsional) Terapkan tag ke daftar Anda.
8. Pilih Simpan untuk menyimpan daftar Anda dan kembali ke halaman daftar Protokol.

Melihat daftar terkelola

Untuk melihat daftar aplikasi atau daftar protokol

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

   > **Note**
   >
   > Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

2. Di panel navigasi, pilih Daftar aplikasi atau daftar Protokol.

   Halaman menampilkan semua daftar jenis yang dipilih yang tersedia untuk Anda gunakan. Daftar yang dikelola Firewall Manager memiliki Y di ManagedListkolom.

3. Untuk melihat detail daftar, pilih namanya. Halaman detail menampilkan konten daftar dan tag apa pun.

   Untuk daftar terkelola Firewall Manager, Anda juga dapat melihat versi yang tersedia dengan memilih drop-down Versi.

Menghapus daftar terkelola kustom

Anda dapat menghapus daftar terkelola kustom. Anda tidak dapat mengedit atau menghapus daftar yang dikelola oleh Firewall Manager.

> **Note**
>
> Saat ini, Firewall Manager tidak memeriksa referensi ke daftar terkelola kustom saat Anda menghapusnya. Ini berarti Anda dapat menghapus daftar aplikasi terkelola kustom atau daftar protokol bahkan ketika sedang digunakan oleh kebijakan aktif. Hal ini dapat menyebabkan kebijakan berhenti berfungsi. Hanya hapus daftar aplikasi atau daftar protokol setelah Anda memverifikasi bahwa itu tidak direferensikan oleh kebijakan aktif apa pun.

Untuk menghapus daftar aplikasi atau protokol terkelola kustom

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

   > **Note**
   >
   > Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

2. Pastikan daftar yang ingin Anda hapus tidak digunakan dalam kebijakan grup keamanan audit Anda dengan melakukan hal berikut:

   a. Di panel navigasi, pilih Kebijakan keamanan.

   b. Di halaman AWS Firewall Manager kebijakan, pilih dan edit grup keamanan audit Anda, dan hapus referensi apa pun ke daftar kustom yang ingin Anda hapus.

      Jika Anda menghapus daftar terkelola kustom yang digunakan dalam kebijakan grup keamanan audit, kebijakan yang menggunakannya dapat berhenti berfungsi.

3. Di panel navigasi, pilih Daftar aplikasi atau daftar Protokol, tergantung pada jenis daftar yang ingin Anda hapus.
4. Di halaman daftar, pilih daftar kustom yang ingin Anda hapus dan pilih Hapus.

AWS WAF kebijakan

Dalam AWS WAF kebijakan Firewall Manager, Anda menentukan grup AWS WAF aturan yang ingin Anda gunakan di seluruh sumber daya Anda. Saat menerapkan kebijakan, Firewall Manager membuat ACL web di akun dalam cakupan kebijakan tergantung pada cara Anda mengonfigurasi pengelolaan ACL web dalam kebijakan Anda. Di ACL web yang dibuat oleh kebijakan, manajer akun individual dapat menambahkan aturan dan grup aturan, selain grup aturan yang Anda tentukan melalui Firewall Manager.

Bagaimana Firewall Manager mengelola ACL web

Firewall Manager membuat ACL web berdasarkan cara Anda mengonfigurasi setelan Kelola ACL web yang tidak terkait dalam kebijakan Anda, atau `optimizeUnassociatedWebACL` setelan dalam tipe SecurityServicePolicyDatadata di API.

Jika Anda mengaktifkan pengelolaan ACL web yang tidak terkait, Firewall Manager membuat ACL web di akun dalam cakupan kebijakan hanya jika ACL web akan digunakan oleh setidaknya satu sumber daya. Jika sewaktu-waktu akun masuk ke cakupan kebijakan, Firewall Manager secara otomatis membuat ACL web di akun jika setidaknya satu sumber daya akan menggunakan ACL web. Saat Anda mengaktifkan pengelolaan ACL web yang tidak terkait, Firewall Manager melakukan pembersihan satu kali dari ACL web yang tidak terkait di akun Anda. Selama pembersihan, Firewall Manager melewatkan ACL web apa pun yang telah Anda modifikasi setelah pembuatannya, misalnya, jika Anda menambahkan grup aturan ke ACL web atau memodifikasi pengaturannya. Proses pembersihan bisa memakan waktu beberapa jam. Jika sumber daya meninggalkan cakupan kebijakan setelah Firewall Manager membuat ACL web, Firewall Manager memisahkan sumber daya dari ACL web, tetapi tidak akan membersihkan ACL web yang tidak terkait. Firewall Manager hanya membersihkan ACL web yang tidak terkait saat Anda pertama kali mengaktifkan pengelolaan ACL web yang tidak terkait dalam suatu kebijakan.

Jika Anda tidak mengaktifkan opsi ini, Firewall Manager tidak mengelola ACL web yang tidak terkait, dan Firewall Manager secara otomatis membuat ACL web di setiap akun yang berada dalam cakupan kebijakan.

Pengambilan sampel dan metrik CloudWatch

AWS Firewall Manager memungkinkan pengambilan sampel dan CloudWatch metrik Amazon untuk ACL web dan grup aturan yang dibuat untuk kebijakan. AWS WAF

Struktur penamaan ACL web

Ketika Firewall Manager membuat ACL web untuk kebijakan, itu menamai web `FMManagedWebACLV2-`*`policy name`*`-`*`timestamp`* ACL. Stempel waktu dalam milidetik UTC. Misalnya, `FMManagedWebACLV2-MyWAFPolicyName-1621880374078`.

> **Note**
>
> Jika sumber daya yang dikonfigurasi dengan mitigasi DDoS lapisan aplikasi otomatis lanjutan masuk ke dalam cakupan AWS WAF kebijakan, Firewall Manager tidak akan dapat mengaitkan ACL web yang dibuat oleh AWS WAF kebijakan ke sumber daya.

Kelompok aturan dalam AWS WAF kebijakan

ACL web yang dikelola oleh AWS WAF kebijakan Firewall Manager berisi tiga set aturan. Set ini memberikan tingkat prioritas yang lebih tinggi untuk aturan dan kelompok aturan di ACL web:

- Grup aturan pertama, yang ditentukan oleh Anda dalam AWS WAF kebijakan Firewall Manager. AWS WAF mengevaluasi kelompok aturan ini terlebih dahulu.
- Aturan dan grup aturan yang ditentukan oleh manajer akun di ACL web. AWS WAF mengevaluasi aturan atau kelompok aturan yang dikelola akun berikutnya.
- Grup aturan terakhir, yang ditentukan oleh Anda dalam AWS WAF kebijakan Firewall Manager. AWS WAF mengevaluasi kelompok aturan ini terakhir.

Dalam masing-masing set aturan ini, AWS WAF mengevaluasi aturan dan kelompok aturan seperti biasa, sesuai dengan pengaturan prioritas mereka dalam set.

Dalam kumpulan grup aturan pertama dan terakhir kebijakan, Anda hanya dapat menambahkan grup aturan. Anda dapat menggunakan grup aturan AWS terkelola, yang Aturan Terkelola dan AWS Marketplace penjual membuat dan memelihara untuk Anda. Anda juga dapat mengelola dan menggunakan grup aturan Anda sendiri. Untuk informasi selengkapnya tentang semua opsi ini, lihatAWS WAF kelompok aturan.

Jika Anda ingin menggunakan grup aturan Anda sendiri, Anda membuatnya sebelum membuat AWS WAF kebijakan Firewall Manager. Untuk panduan, lihat Mengelola grup aturan Anda sendiri. Untuk menggunakan aturan kustom individual, Anda harus menentukan grup aturan Anda sendiri, menentukan aturan Anda di dalamnya, dan kemudian menggunakan grup aturan dalam kebijakan Anda.

Grup AWS WAF aturan pertama dan terakhir yang Anda kelola melalui Firewall Manager memiliki nama yang dimulai dengan `PREFMManaged-` atau`POSTFMManaged-`, masing-masing, diikuti dengan nama kebijakan Firewall Manager, dan stempel waktu pembuatan grup aturan, dalam milidetik UTC. Misalnya, `PREFMManaged-MyWAFPolicyName-1621880555123`.

Untuk informasi tentang cara AWS WAF mengevaluasi permintaan web, lihatEvaluasi aturan dan kelompok aturan ACL Web.

Untuk prosedur membuat AWS WAF kebijakan Firewall Manager, lihatMembuat AWS Firewall Manager kebijakan untuk AWS WAF.

Firewall Manager memungkinkan pengambilan sampel dan CloudWatch metrik Amazon untuk grup aturan yang Anda tetapkan untuk kebijakan tersebut. AWS WAF

Pemilik akun individu memiliki kontrol penuh atas metrik dan konfigurasi pengambilan sampel untuk setiap aturan atau grup aturan yang mereka tambahkan ke ACL web terkelola kebijakan.

Mengonfigurasi pencatatan untuk kebijakan AWS WAF

Anda dapat mengaktifkan pencatatan terpusat untuk AWS WAF kebijakan Anda untuk mendapatkan informasi terperinci tentang lalu lintas yang dianalisis oleh ACL web Anda dalam organisasi Anda. Informasi dalam log mencakup waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi terperinci tentang permintaan, dan tindakan untuk aturan yang dicocokkan oleh setiap permintaan dari semua akun dalam lingkup. Anda dapat mengirim log ke aliran data Amazon Data Firehose atau bucket Amazon Simple Storage Service (S3). Untuk informasi tentang AWS WAF pencatatan, lihat Pencatatan AWS WAF lalu lintas ACL web di Panduan AWS WAF Pengembang.

> **Note**
>
> AWS Firewall Manager mendukung opsi ini untuk AWS WAFV2, bukan untuk AWS WAF Klasik.

Topik

- Tujuan pencatatan
- Mengaktifkan pencatatan log
- Menonaktifkan log

Tujuan pencatatan

Bagian ini menjelaskan tujuan pencatatan yang dapat Anda pilih untuk mengirim log AWS WAF kebijakan Anda. Setiap bagian menyediakan panduan untuk mengonfigurasi pencatatan log untuk jenis tujuan dan informasi tentang semua perilaku yang spesifik untuk jenis destinasi. Setelah mengonfigurasi tujuan pencatatan, Anda dapat memberikan spesifikasinya ke AWS WAF kebijakan Firewall Manager Anda untuk mulai masuk ke sana.

Firewall Manager tidak memiliki visibilitas ke kegagalan log setelah membuat konfigurasi logging. Anda bertanggung jawab untuk memverifikasi bahwa pengiriman log berfungsi seperti yang Anda inginkan.

> **Note**
>
> Firewall Manager tidak mengubah konfigurasi logging yang ada di akun anggota organisasi Anda.

Topik

Aliran data Amazon Data Firehose

Topik ini memberikan informasi untuk mengirim log lalu lintas ACL web Anda ke aliran data Amazon Data Firehose.

Saat mengaktifkan pencatatan Amazon Data Firehose, Firewall Manager mengirimkan log dari ACL web kebijakan Anda ke Amazon Data Firehose tempat Anda mengonfigurasi tujuan penyimpanan. Setelah Anda mengaktifkan logging, AWS WAF mengirimkan log untuk setiap ACL web yang dikonfigurasi, melalui titik akhir HTTPS dari Kinesis Data Firehose ke tujuan penyimpanan yang dikonfigurasi. Sebelum Anda menggunakannya, uji aliran pengiriman Anda untuk memastikan bahwa itu memiliki throughput yang cukup untuk mengakomodasi log organisasi Anda. Untuk informasi selengkapnya tentang cara membuat Amazon Kinesis Data Firehose dan meninjau log yang disimpan, lihat Apa itu Amazon Data Firehose?

Anda harus memiliki izin berikut agar berhasil mengaktifkan logging dengan Kinesis:

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `wafv2:PutLoggingConfiguration`

Saat Anda mengonfigurasi tujuan pencatatan Amazon Data Firehose pada AWS WAF kebijakan, Firewall Manager akan membuat ACL web untuk kebijakan tersebut di akun administrator Manajer Firewall sebagai berikut:

- Firewall Manager membuat ACL web di akun administrator Firewall Manager terlepas dari apakah akun tersebut berada dalam cakupan kebijakan.

- ACL web telah mengaktifkan pencatatan, dengan nama log`FMManagedWebACLV2-Logging`*`policy name`*`-`*`timestamp`*, di mana stempel waktu adalah waktu UTC ketika log diaktifkan untuk ACL web, dalam milidetik. Misalnya, `FMManagedWebACLV2-LoggingMyWAFPolicyName-1621880565180`. Web ACL tidak memiliki kelompok aturan dan tidak ada sumber daya terkait.
- Anda dikenakan biaya untuk ACL web sesuai dengan AWS WAF pedoman harga. Untuk informasi selengkapnya, silakan lihat Harga AWS WAF.
- Firewall Manager menghapus ACL web saat Anda menghapus kebijakan.

Untuk informasi tentang peran terkait layanan dan `iam:CreateServiceLinkedRole` izin, lihat. Menggunakan peran terkait layanan untuk AWS WAF

Untuk informasi selengkapnya tentang membuat aliran pengiriman, lihat Membuat Aliran Pengiriman Firehose Data Amazon.

Bucket Amazon Simple Storage Service

Topik ini memberikan informasi untuk mengirim log lalu lintas ACL web Anda ke bucket Amazon S3.

Bucket yang Anda pilih sebagai tujuan pencatatan harus dimiliki oleh akun administrator Firewall Manager. Untuk informasi tentang persyaratan pembuatan bucket Amazon S3 untuk persyaratan pencatatan dan penamaan bucket, lihat Layanan Penyimpanan Sederhana Amazon di Panduan AWS WAF Pengembang.

Konsistensi akhirnya

Saat Anda mengubah AWS WAF kebijakan yang dikonfigurasi dengan tujuan pencatatan Amazon S3, Firewall Manager memperbarui kebijakan bucket untuk menambahkan izin yang diperlukan untuk pencatatan. Saat melakukannya, Firewall Manager mengikuti model last-writer-wins semantik dan konsistensi data yang diikuti Amazon Simple Storage Service. Jika Anda secara bersamaan membuat beberapa pembaruan kebijakan ke tujuan Amazon S3 di konsol Firewall Manager atau melalui PutPolicyAPI, beberapa izin mungkin tidak disimpan. Untuk informasi selengkapnya tentang model konsistensi data Amazon S3, lihat model konsistensi data Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Izin untuk mempublikasikan log ke bucket Amazon S3

Mengonfigurasi pencatatan lalu lintas ACL web untuk bucket Amazon S3 dalam kebijakan memerlukan AWS WAF setelan izin berikut. Firewall Manager secara otomatis melampirkan izin ini

ke bucket Amazon S3 saat mengonfigurasi Amazon S3 sebagai tujuan pencatatan untuk memberikan izin layanan untuk memublikasikan log ke bucket. Jika Anda ingin mengelola akses berbutir halus ke sumber daya logging dan Firewall Manager, Anda dapat mengatur sendiri izin ini. Untuk informasi tentang mengelola izin, lihat Manajemen akses untuk AWS sumber daya di Panduan Pengguna IAM. Untuk informasi tentang kebijakan AWS WAF terkelola, lihatAWS kebijakan terkelola untuk AWS WAF.

```
{
    "Version": "2012-10-17",
    "Id": "AWSLogDeliveryForFirewallManager",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryAclCheckFMS",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::aws-waf-DOC-EXAMPLE-BUCKET"
        },
        {
            "Sid": "AWSLogDeliveryWriteFMS",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET/policy-id/
AWSLogs/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
}
```

Untuk mencegah masalah deputi lintas layanan yang membingungkan, Anda dapat menambahkan kunci konteks kondisi `aws:SourceAccount`global `aws:SourceArn`dan global ke kebijakan bucket Anda. Untuk menambahkan kunci ini, Anda dapat mengubah kebijakan yang dibuat oleh Manajer Firewall untuk Anda saat mengonfigurasi tujuan pencatatan, atau jika Anda menginginkan kontrol

berbutir halus, Anda dapat membuat kebijakan sendiri. Jika Anda menambahkan kondisi ini ke kebijakan tujuan pencatatan, Firewall Manager tidak akan memvalidasi atau memantau perlindungan deputi yang membingungkan. Untuk informasi umum tentang masalah wakil yang bingung, lihat Masalah wakil yang bingung di Panduan Pengguna IAM.

Saat Anda menambahkan `sourceArn` properti `sourceAccount` add, itu akan meningkatkan ukuran kebijakan bucket. Jika Anda menambahkan daftar panjang `sourceArn` properti `sourceAccount` add, berhati-hatilah agar tidak melebihi kuota ukuran kebijakan bucket Amazon S3.

Contoh berikut menunjukkan cara mencegah masalah deputi yang membingungkan dengan menggunakan kunci konteks kondisi `aws:SourceAccount` global `aws:SourceArn` dan global dalam kebijakan bucket Anda. Ganti *`member-account-id`*dengan ID akun anggota di organisasi Anda.

```
{
   "Version":"2012-10-17",
   "Id":"AWSLogDeliveryForFirewallManager",
   "Statement":[
      {
         "Sid":"AWSLogDeliveryAclCheckFMS",
         "Effect":"Allow",
         "Principal":{
            "Service":"delivery.logs.amazonaws.com"
         },
         "Action":"s3:GetBucketAcl",
         "Resource":"arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET",
         "Condition":{
            "StringEquals":{
               "aws:SourceAccount":[
                  "member-account-id",
                  "member-account-id"
               ]
            },
            "ArnLike":{
               "aws:SourceArn":[
                  "arn:aws:logs:*:member-account-id:*",
                  "arn:aws:logs:*:member-account-id:*"
               ]
            }
         }
      },
      {
```

```
         "Sid":"AWSLogDeliveryWriteFMS",
         "Effect":"Allow",
         "Principal":{
            "Service":"delivery.logs.amazonaws.com"
         },
         "Action":"s3:PutObject",
         "Resource":"arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET/policy-id/AWSLogs/*",
         "Condition":{
            "StringEquals":{
               "s3:x-amz-acl":"bucket-owner-full-control",
               "aws:SourceAccount":[
                    "member-account-id",
                  "member-account-id"
               ]
            },
            "ArnLike":{
               "aws:SourceArn":[
                  "arn:aws:logs:*:member-account-id-1:*",
                  "arn:aws:logs:*:member-account-id-2:*"
               ]
            }
         }
      }
   ]
}
```

Enkripsi sisi server untuk bucket Amazon S3

Anda dapat mengaktifkan enkripsi sisi server Amazon S3 atau menggunakan kunci yang dikelola AWS Key Management Service pelanggan di bucket S3 Anda. Jika Anda memilih untuk menggunakan enkripsi Amazon S3 default di bucket Amazon S3 AWS WAF untuk log, Anda tidak perlu mengambil tindakan khusus apa pun. Namun, jika Anda memilih untuk menggunakan kunci enkripsi yang disediakan pelanggan untuk mengenkripsi data Amazon S3 Anda saat istirahat, Anda harus menambahkan pernyataan izin berikut ke kebijakan kunci Anda: AWS Key Management Service

```
{
            "Sid": "Allow Logs Delivery to use the key",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
```

```
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*"
}
```

Untuk informasi tentang penggunaan kunci enkripsi yang disediakan pelanggan dengan Amazon S3, lihat Menggunakan enkripsi sisi server dengan kunci yang disediakan pelanggan (SSE-C) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Mengaktifkan pencatatan log

Prosedur berikut menjelaskan cara mengaktifkan logging untuk AWS WAF kebijakan di konsol Firewall Manager.

Untuk mengaktifkan pencatatan untuk AWS WAF kebijakan

1. Sebelum Anda dapat mengaktifkan logging, Anda harus mengonfigurasi sumber daya tujuan pencatatan Anda sebagai berikut:

   - Amazon Kinesis Data Streams - Buat Amazon Data Firehose menggunakan akun administrator Firewall Manager Anda. Gunakan nama yang dimulai dengan awalan`aws-waf-logs-`. Misalnya, `aws-waf-logs-firewall-manager-central`. Buat firehose data dengan PUT sumber dan di Wilayah yang Anda operasikan. Jika Anda menangkap log untuk Amazon CloudFront, buat firehose di US East (Virginia N.). Sebelum Anda menggunakannya, uji aliran pengiriman Anda untuk memastikan bahwa itu memiliki throughput yang cukup untuk mengakomodasi log organisasi Anda. Untuk informasi selengkapnya, lihat Membuat aliran pengiriman Amazon Data Firehose.
   - Bucket Layanan Penyimpanan Sederhana Amazon - Buat bucket Amazon S3 sesuai dengan pedoman dalam topik Layanan Penyimpanan Sederhana Amazon di Panduan AWS WAF Pengembang. Anda juga harus mengonfigurasi bucket Amazon S3 Anda dengan izin yang tercantum di. Izin untuk mempublikasikan log ke bucket Amazon S3

2. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk

informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

> **Note**
>
> Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

3. Di panel navigasi, pilih Kebijakan Keamanan.
4. Pilih AWS WAF kebijakan yang ingin Anda aktifkan pencatatan. Untuk informasi lebih lanjut tentang AWS WAF catatan, lihat Pencatatan AWS WAF lalu lintas ACL web.
5. Pada tab Detail kebijakan, di bagian Aturan kebijakan, pilih Edit.
6. Untuk konfigurasi Logging, pilih Aktifkan logging untuk mengaktifkan logging. Logging memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda. Pilih tujuan Logging, lalu pilih tujuan logging yang Anda konfigurasikan. Anda harus memilih tujuan pencatatan yang namanya dimulai dengan`aws-waf-logs-`. Untuk informasi tentang mengonfigurasi tujuan AWS WAF pencatatan, lihatMengonfigurasi pencatatan untuk kebijakan AWS WAF.
7. (Opsional) Jika Anda tidak ingin bidang tertentu dan nilainya disertakan dalam log, edit bidang tersebut. Pilih bidang yang akan disunting, lalu pilih Tambah. Ulangi seperlunya untuk menyunting bidang tambahan. Bidang yang disunting muncul seperti `REDACTED` di log. Misalnya, jika Anda menyunting bidang URI, bidang URI di log akan menjadi`REDACTED`.
8. (Opsional) Jika Anda tidak ingin mengirim semua permintaan ke log, tambahkan kriteria dan perilaku pemfilteran Anda. Di bawah Filter log, untuk setiap filter yang ingin Anda terapkan, pilih Tambahkan filter, lalu pilih kriteria pemfilteran Anda dan tentukan apakah Anda ingin menyimpan atau menghapus permintaan yang sesuai dengan kriteria. Ketika Anda selesai menambahkan filter, jika diperlukan, ubah perilaku logging Default. Untuk informasi lebih lanjut, lihat Konfigurasi pencatatan ACL web dalam Panduan Pengembang AWS WAF .
9. Pilih Selanjutnya.
10. Tinjau pengaturan Anda, lalu pilih Simpan untuk menyimpan perubahan pada kebijakan.

Menonaktifkan log

Prosedur berikut menjelaskan cara menonaktifkan logging untuk AWS WAF kebijakan di konsol Firewall Manager.

Untuk menonaktifkan pencatatan untuk AWS WAF kebijakan

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

   > **Note**
   >
   > Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

2. Di panel navigasi, pilih Kebijakan Keamanan.
3. Pilih AWS WAF kebijakan yang ingin Anda nonaktifkan pencatatan.
4. Pada tab Detail kebijakan, di bagian Aturan kebijakan, pilih Edit.
5. Untuk status konfigurasi Logging, pilih Dinonaktifkan.
6. Pilih Selanjutnya.
7. Tinjau pengaturan Anda, lalu pilih Simpan untuk menyimpan perubahan pada kebijakan.

AWS Shield Advanced kebijakan

Dalam AWS Shield kebijakan Firewall Manager, Anda memilih sumber daya yang ingin Anda lindungi. Saat Anda menerapkan kebijakan dengan remediasi otomatis diaktifkan, untuk setiap sumber daya dalam lingkup yang belum dikaitkan dengan ACL AWS WAF web, Firewall Manager mengaitkan ACL web kosong. AWS WAF ACL web kosong digunakan untuk tujuan pemantauan Shield. Jika Anda kemudian mengaitkan ACL web lain ke sumber daya, Firewall Manager menghapus asosiasi ACL web kosong.

> **Note**
>
> Ketika sumber daya yang berada dalam cakupan AWS WAF kebijakan masuk ke dalam cakupan kebijakan Shield Advanced yang dikonfigurasi dengan mitigasi DDoS lapisan aplikasi otomatis, Firewall Manager menerapkan perlindungan Shield Advanced hanya setelah mengaitkan ACL web yang dibuat oleh kebijakan. AWS WAF

Cara AWS Firewall Manager mengelola ACL web yang tidak terkait dalam kebijakan Shield

Anda dapat mengonfigurasi apakah Firewall Manager mengelola ACL web yang tidak terkait untuk Anda melalui setelan Kelola ACL web yang tidak terkait dalam kebijakan Anda, atau `optimizeUnassociatedWebACLs` setelan dalam tipe SecurityServicePolicyDatadata di API. Jika Anda mengaktifkan pengelolaan ACL web yang tidak terkait dalam kebijakan Anda, Firewall Manager akan membuat ACL web di akun dalam cakupan kebijakan hanya jika ACL web akan digunakan oleh setidaknya satu sumber daya. Jika sewaktu-waktu akun masuk ke cakupan kebijakan, Firewall Manager secara otomatis membuat ACL web di akun jika setidaknya satu sumber daya akan menggunakan ACL web.

Saat Anda mengaktifkan pengelolaan ACL web yang tidak terkait, Firewall Manager melakukan pembersihan satu kali dari ACL web yang tidak terkait di akun Anda. Proses pembersihan bisa memakan waktu beberapa jam. Jika sumber daya meninggalkan cakupan kebijakan setelah Firewall Manager membuat ACL web, Firewall Manager tidak memisahkan sumber daya dari ACL web. Jika Anda ingin Firewall Manager membersihkan ACL web, Anda harus terlebih dahulu memisahkan sumber daya dari ACL web secara manual, lalu mengaktifkan opsi kelola ACL web yang tidak terkait dalam kebijakan Anda.

Jika Anda tidak mengaktifkan opsi ini, Firewall Manager tidak mengelola ACL web yang tidak terkait, dan Firewall Manager secara otomatis membuat ACL web di setiap akun yang berada dalam cakupan kebijakan.

Cara AWS Firewall Manager mengelola perubahan cakupan dalam kebijakan Shield

Akun dan sumber daya dapat keluar dari cakupan kebijakan AWS Firewall Manager Shield Advanced karena sejumlah perubahan, seperti perubahan pengaturan cakupan kebijakan, perubahan tag pada sumber daya, dan penghapusan akun dari organisasi. Untuk informasi umum tentang pengaturan cakupan kebijakan, lihatAWS Firewall Manager ruang lingkup kebijakan.

Dengan kebijakan AWS Firewall Manager Shield Advanced, jika akun atau sumber daya keluar dari cakupan, Firewall Manager berhenti memantau akun atau sumber daya.

Jika akun keluar dari cakupan dengan dihapus dari organisasi, akun akan terus berlangganan Shield Advanced. Karena akun tidak lagi menjadi bagian dari keluarga penagihan konsolidasi, akun tersebut akan dikenakan biaya berlangganan Shield Advanced yang diprorata. Di sisi lain, akun yang keluar dari ruang lingkup tetapi tetap berada di organisasi tidak dikenakan biaya tambahan.

Jika sumber daya keluar dari cakupan, itu terus dilindungi oleh Shield Advanced dan terus dikenakan biaya transfer data Shield Advanced.

Mitigasi DDoS lapisan aplikasi otomatis

Bila Anda menerapkan kebijakan Shield Advanced ke CloudFront distribusi Amazon atau Application Load Balancers, Anda memiliki opsi untuk mengonfigurasi mitigasi DDoS lapisan aplikasi otomatis Shield Advanced dalam kebijakan.

Untuk informasi tentang mitigasi otomatis Shield Advanced, lihat. Mitigasi DDoS lapisan aplikasi otomatis Shield Advanced

Mitigasi DDoS lapisan aplikasi otomatis Shield Advanced memiliki persyaratan sebagai berikut:

- Mitigasi DDoS lapisan aplikasi otomatis hanya berfungsi dengan CloudFront distribusi Amazon dan Application Load Balancer.

  Jika menerapkan kebijakan Shield Advanced ke CloudFront distribusi Amazon, Anda dapat memilih opsi ini untuk kebijakan Shield Advanced yang Anda buat untuk Wilayah Global. Jika menerapkan perlindungan pada Application Load Balancers, Anda dapat menerapkan kebijakan tersebut ke Wilayah mana pun yang didukung oleh Firewall Manager.
- Mitigasi DDoS lapisan aplikasi otomatis hanya berfungsi dengan ACL web yang dibuat menggunakan versi terbaru (v2). AWS WAF

  Karena itu, jika Anda memiliki kebijakan yang menggunakan ACL web AWS WAF Klasik, Anda perlu mengganti kebijakan tersebut dengan kebijakan baru, yang secara otomatis akan menggunakan versi terbaru AWS WAF, atau meminta Firewall Manager membuat ACL web versi baru untuk kebijakan yang ada dan beralih ke menggunakannya. Untuk informasi lebih lanjut tentang opsi, lihat Ganti ACL web AWS WAF Klasik dengan ACL web versi terbaru.

Konfigurasi mitigasi otomatis

Opsi mitigasi DDoS lapisan aplikasi otomatis untuk Kebijakan Firewall Manager Shield Advanced menerapkan fungsionalitas mitigasi otomatis Shield Advanced ke akun dan sumber daya dalam cakupan kebijakan Anda. Untuk informasi rinci tentang fitur Shield Advanced ini, lihatMitigasi DDoS lapisan aplikasi otomatis Shield Advanced.

Anda dapat memilih agar Firewall Manager mengaktifkan atau menonaktifkan mitigasi otomatis untuk CloudFront distribusi atau Application Load Balancer yang berada dalam cakupan kebijakan, atau Anda dapat memilih agar kebijakan mengabaikan pengaturan mitigasi otomatis Shield Advanced:

- Aktifkan - Jika Anda memilih untuk mengaktifkan mitigasi otomatis, Anda juga menentukan apakah mitigasi aturan Shield Advanced harus menghitung atau memblokir permintaan web yang cocok. Firewall Manager akan menandai sumber daya dalam lingkup sebagai tidak sesuai jika tidak mengaktifkan mitigasi otomatis, atau menggunakan tindakan aturan yang tidak cocok dengan yang Anda tentukan untuk kebijakan tersebut. Jika Anda mengonfigurasi kebijakan untuk remediasi otomatis, Firewall Manager akan memperbarui sumber daya yang tidak sesuai kebutuhan.
- Nonaktifkan - Jika Anda memilih untuk menonaktifkan mitigasi otomatis, Firewall Manager akan menandai sumber daya dalam lingkup sebagai tidak sesuai jika mitigasi otomatis diaktifkan. Jika Anda mengonfigurasi kebijakan untuk remediasi otomatis, Firewall Manager akan memperbarui sumber daya yang tidak sesuai kebutuhan.
- Abaikan — Jika Anda memilih untuk mengabaikan mitigasi otomatis, Firewall Manager tidak akan mempertimbangkan setelan mitigasi otomatis apa pun dalam kebijakan Shield saat melakukan aktivitas remediasi untuk kebijakan tersebut. Pengaturan ini memungkinkan Anda untuk mengontrol mitigasi otomatis melalui Shield Advanced, tanpa pengaturan tersebut ditimpa oleh Firewall Manager. Pengaturan ini tidak berlaku untuk sumber daya Classic Load Balancer atau IP Elastic yang dikelola melalui Shield Advanced, karena Shield Advanced saat ini tidak mendukung mitigasi otomatis L7 untuk sumber daya tersebut.

Ganti ACL web AWS WAF Klasik dengan ACL web versi terbaru

Mitigasi DDoS lapisan aplikasi otomatis hanya berfungsi dengan ACL web yang dibuat menggunakan versi terbaru (v2). AWS WAF

Untuk menentukan versi ACL web untuk kebijakan Shield Advanced Anda, lihatMenentukan versi AWS WAF yang digunakan oleh kebijakan Shield Advanced.

Jika Anda ingin menggunakan mitigasi otomatis dalam kebijakan Shield Advanced, dan kebijakan Anda saat ini menggunakan AWS WAF Classic web ACL, Anda dapat membuat kebijakan Shield Advanced baru untuk menggantikan kebijakan Anda saat ini, atau Anda dapat menggunakan opsi yang dijelaskan di bagian ini untuk mengganti ACL web versi sebelumnya dengan ACL web baru (v2) di dalam kebijakan Shield Advanced Anda saat ini. Kebijakan baru selalu membuat ACL web menggunakan versi terbaru. AWS WAF Jika Anda mengganti seluruh kebijakan, saat Anda menghapusnya, Anda dapat meminta Firewall Manager menghapus semua ACL web versi sebelumnya juga. Bagian lainnya menjelaskan opsi Anda untuk mengganti ACL web di dalam kebijakan yang ada.

Saat Anda mengubah kebijakan Shield Advanced yang ada untuk CloudFront sumber daya Amazon, Firewall Manager dapat secara otomatis membuat ACL web kosong AWS WAF (v2) baru untuk kebijakan tersebut, di akun dalam lingkup apa pun yang belum memiliki ACL web v2. Saat Firewall Manager membuat ACL web baru, jika kebijakan sudah memiliki ACL web AWS WAF Klasik di akun yang sama, Firewall Manager mengonfigurasi ACL web versi baru dengan setelan tindakan default yang sama dengan ACL web yang ada. Jika tidak ada ACL web AWS WAF Klasik yang ada, Firewall Manager menetapkan tindakan default ke Allow ACL web baru. Setelah Firewall Manager membuat ACL web baru, Anda dapat menyesuaikannya sesuai kebutuhan melalui AWS WAF konsol.

Bila Anda memilih salah satu opsi konfigurasi kebijakan berikut, Firewall Manager membuat ACL web baru (v2) untuk akun dalam lingkup yang belum memilikinya:

- Saat Anda mengaktifkan atau menonaktifkan mitigasi DDoS lapisan aplikasi otomatis. Pilihan ini saja hanya menyebabkan Firewall Manager membuat ACL web baru, dan tidak menggantikan asosiasi ACL web AWS WAF Klasik yang ada pada sumber daya dalam cakupan kebijakan.
- Bila Anda memilih tindakan kebijakan remediasi otomatis dan Anda memilih opsi untuk mengganti ACL web AWS WAF Klasik dengan AWS WAF (v2) ACL web. Anda dapat memilih untuk mengganti ACL web versi sebelumnya terlepas dari pilihan konfigurasi Anda untuk mitigasi DDoS lapisan aplikasi otomatis.

  Saat Anda memilih opsi penggantian, Firewall Manager membuat ACL web versi baru sesuai kebutuhan, lalu melakukan hal berikut untuk sumber daya dalam cakupan kebijakan:
  - Jika sumber daya dikaitkan dengan ACL web dari kebijakan Firewall Manager aktif lainnya, Firewall Manager meninggalkan asosiasi sendirian.
  - Untuk kasus lain, Firewall Manager menghapus asosiasi apa pun dengan ACL web AWS WAF Klasik dan mengaitkan sumber daya dengan ACL web kebijakan AWS WAF (v2).

Anda dapat memilih untuk meminta Firewall Manager mengganti ACL web versi sebelumnya dengan ACL web versi baru saat Anda mau. Jika sebelumnya Anda telah menyesuaikan ACL web AWS WAF Klasik kebijakan, Anda dapat memperbarui ACL web versi baru ke setelan yang sebanding sebelum Anda memilih agar Firewall Manager melakukan langkah penggantian.

Anda dapat mengakses salah satu versi ACL web untuk kebijakan melalui konsol versi yang sama untuk AWS WAF atau Classic. AWS WAF

Firewall Manager tidak menghapus ACL web AWS WAF Klasik yang diganti sampai Anda menghapus kebijakan itu sendiri. Setelah ACL web AWS WAF Klasik tidak lagi digunakan oleh kebijakan, Anda dapat menghapusnya jika mau.

Menentukan versi AWS WAF yang digunakan oleh kebijakan Shield Advanced

Anda dapat menentukan versi kebijakan Lanjutan Firewall Manager Shield yang digunakan dengan melihat kunci parameter dalam aturan AWS Config terkait layanan kebijakan. AWS WAF Jika AWS WAF versi yang digunakan adalah yang terbaru, kunci parameter menyertakan `policyId` dan`webAclArn`. Jika versi sebelumnya, AWS WAF Classic, kunci parameter termasuk `webAclId` dan`resourceTypes`.

AWS Config Aturan hanya mencantumkan kunci untuk ACL web yang saat ini digunakan kebijakan dengan sumber daya dalam cakupan.

Untuk menentukan versi kebijakan Firewall Manager Shield Advanced yang digunakan AWS WAF

1. Mengambil ID kebijakan untuk kebijakan Shield Advanced:

    a. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

    b. Di panel navigasi, pilih Kebijakan Keamanan.

    c. Pilih Wilayah untuk kebijakan. Untuk CloudFront distribusi, ini`Global`.

    d. Temukan kebijakan yang Anda inginkan dan salin nilai ID Policy-nya.

    Contoh ID kebijakan:`1111111-2222-3333-4444-a55aa5aaa555`.

2. Buat nama AWS Config aturan kebijakan dengan menambahkan ID kebijakan ke string`FMManagedShieldConfigRule`.

    Contoh nama AWS Config aturan:`FMManagedShieldConfigRule1111111-2222-3333-4444-a55aa5aaa555`.

3. Cari parameter untuk AWS Config aturan terkait untuk kunci bernama `policyId` dan`webAclArn`:

    a. Buka AWS Config konsol di https://console.aws.amazon.com/config/.

    b. Di panel navigasi, pilih Aturan.

    c. Temukan nama AWS Config aturan kebijakan Firewall Manager Anda dalam daftar dan pilih. Halaman aturan terbuka.

    d. Di bawah Rincian aturan, di bagian Parameter, lihat tombol. Jika Anda menemukan kunci bernama `policyId` dan`webAclArn`, kebijakan menggunakan ACL web yang dibuat

menggunakan versi terbaru. AWS WAF Jika Anda menemukan kunci bernama `webAclId` dan`resourceTypes`, kebijakan menggunakan ACL web yang dibuat menggunakan versi sebelumnya, AWS WAF Classic.

Kebijakan kelompok keamanan

Anda dapat menggunakan kebijakan grup AWS Firewall Manager keamanan untuk mengelola grup keamanan Amazon Virtual Private Cloud untuk organisasi Anda AWS Organizations. Anda dapat menerapkan kebijakan grup keamanan yang dikontrol secara terpusat ke seluruh organisasi Anda atau ke subset tertentu dari akun dan sumber daya Anda. Anda juga dapat memantau dan mengelola kebijakan grup keamanan yang digunakan di organisasi Anda, dengan kebijakan grup keamanan audit dan penggunaan.

Firewall Manager terus mempertahankan kebijakan Anda dan menerapkannya ke akun dan sumber daya saat ditambahkan atau diperbarui di seluruh organisasi Anda. Untuk selengkapnya AWS Organizations, lihat Panduan AWS Organizations Pengguna.

Untuk informasi tentang grup keamanan Amazon Virtual Private Cloud, lihat Grup Keamanan untuk VPC Anda di Panduan Pengguna Amazon VPC.

Anda dapat menggunakan kebijakan grup keamanan Firewall Manager untuk melakukan hal berikut di seluruh AWS organisasi Anda:

- Terapkan grup keamanan umum ke akun dan sumber daya tertentu.
- Audit aturan kelompok keamanan, untuk menemukan dan memulihkan aturan yang tidak patuh.
- Audit penggunaan kelompok keamanan, untuk membersihkan kelompok keamanan yang tidak terpakai dan berlebihan.

Bagian ini mencakup cara kerja kebijakan grup keamanan Firewall Manager dan memberikan panduan untuk menggunakannya. Untuk prosedur untuk membuat kebijakan grup keamanan, lihatMembuat AWS Firewall Manager kebijakan.

Kebijakan kelompok keamanan umum

Dengan kebijakan grup keamanan umum, Firewall Manager menyediakan asosiasi grup keamanan yang dikendalikan secara terpusat ke akun dan sumber daya di seluruh organisasi Anda. Anda menentukan di mana dan bagaimana menerapkan kebijakan di organisasi Anda.

Anda dapat menerapkan kebijakan grup keamanan umum ke jenis sumber daya berikut:

- Contoh Amazon Elastic Compute Cloud (Amazon EC2)
- Antarmuka Jaringan Elastis
- Penyeimbang Beban Aplikasi
- Classic Load Balancer

Untuk panduan cara membuat kebijakan grup keamanan umum menggunakan konsol, lihatMembuat kebijakan grup keamanan umum.

VPC bersama

Dalam pengaturan cakupan kebijakan untuk kebijakan grup keamanan umum, Anda dapat memilih untuk menyertakan VPC bersama. Pilihan ini mencakup VPC yang dimiliki oleh akun lain dan dibagikan dengan akun dalam lingkup. VPC yang memiliki akun dalam lingkup selalu disertakan. Untuk informasi tentang VPC bersama, lihat Bekerja dengan VPC bersama di Panduan Pengguna VPC Amazon.

Peringatan berikut berlaku untuk menyertakan VPC bersama. Ini adalah tambahan dari peringatan umum untuk kebijakan kelompok keamanan diPeringatan dan batasan kebijakan kelompok keamanan.

- Firewall Manager mereplikasi grup keamanan utama ke dalam VPC untuk setiap akun dalam lingkup. Untuk VPC bersama, Firewall Manager mereplikasi grup keamanan utama satu kali untuk setiap akun dalam lingkup tempat VPC dibagikan. Ini dapat menghasilkan beberapa replika dalam satu VPC bersama.
- Saat membuat VPC bersama baru, Anda tidak akan melihatnya terwakili dalam detail kebijakan grup keamanan Firewall Manager hingga setelah Anda membuat setidaknya satu sumber daya di VPC yang berada dalam cakupan kebijakan.
- Saat Anda menonaktifkan VPC bersama dalam kebijakan yang mengaktifkan VPC bersama, di VPC bersama, Firewall Manager menghapus grup keamanan replika yang tidak terkait dengan sumber daya apa pun. Firewall Manager meninggalkan grup keamanan replika yang tersisa di tempatnya, tetapi berhenti mengelolanya. Penghapusan grup keamanan yang tersisa ini memerlukan manajemen manual di setiap instance VPC bersama.

Kelompok keamanan utama

Untuk setiap kebijakan grup keamanan umum, Anda AWS Firewall Manager menyediakan satu atau beberapa grup keamanan utama:

- Grup keamanan utama harus dibuat oleh akun administrator Firewall Manager dan dapat berada di instans VPC Amazon apa pun di akun.
- Anda mengelola grup keamanan utama melalui Amazon Virtual Private Cloud (Amazon VPC) atau Amazon Elastic Compute Cloud (Amazon EC2). Untuk selengkapnya, lihat Bekerja dengan Grup Keamanan di Panduan Pengguna Amazon VPC.
- Anda dapat memberi nama satu atau beberapa grup keamanan sebagai pendahuluan untuk kebijakan grup keamanan Firewall Manager. Secara default, jumlah grup keamanan yang diizinkan dalam kebijakan adalah satu, tetapi Anda dapat mengirimkan permintaan untuk meningkatkannya. Untuk informasi, lihat AWS Firewall Manager kuota.

Pengaturan aturan kebijakan

Anda dapat memilih satu atau beberapa perilaku kontrol perubahan berikut untuk grup keamanan dan sumber daya kebijakan grup keamanan umum Anda:

- Identifikasi dan laporkan setiap perubahan yang dibuat oleh pengguna lokal ke grup keamanan replika.
- Putuskan hubungan kelompok keamanan lain dari AWS sumber daya yang berada dalam lingkup kebijakan.
- Mendistribusikan tag dari grup utama ke grup keamanan replika.

> **Important**
>
> Firewall Manager tidak akan mendistribusikan tag sistem yang ditambahkan oleh AWS layanan ke dalam grup keamanan replika. Tag sistem dimulai dengan `aws:` awalan. Selain itu, Firewall Manager tidak akan memperbarui tag grup keamanan yang ada atau membuat grup keamanan baru jika kebijakan tersebut memiliki tag yang bertentangan dengan kebijakan tag organisasi. Untuk informasi tentang kebijakan tag, lihat Kebijakan tag di Panduan AWS Organizations Pengguna.

- Mendistribusikan referensi grup keamanan dari grup utama ke grup keamanan replika.

  Ini memungkinkan Anda untuk dengan mudah membuat aturan referensi grup keamanan umum di semua sumber daya dalam lingkup ke instance yang terkait dengan VPC grup keamanan yang

ditentukan. Saat Anda mengaktifkan opsi ini, Firewall Manager hanya menyebarkan referensi grup keamanan jika grup keamanan mereferensikan grup keamanan rekan di Amazon Virtual Private Cloud. Jika grup keamanan replika tidak mereferensikan grup keamanan sejawat dengan benar, Firewall Manager menandai grup keamanan yang direplikasi ini sebagai tidak sesuai. Untuk informasi tentang cara mereferensikan grup keamanan rekan di Amazon VPC, lihat Memperbarui grup keamanan Anda untuk mereferensikan grup keamanan rekan di Panduan Peering VPC Amazon.

Jika Anda tidak mengaktifkan opsi ini, Firewall Manager tidak menyebarkan referensi grup keamanan ke grup keamanan replika. Untuk informasi tentang mengintip VPC di Amazon VPC, lihat Panduan Peering VPC Amazon.

Pembuatan dan manajemen kebijakan

Saat Anda membuat kebijakan grup keamanan umum, Firewall Manager mereplikasi grup keamanan utama ke setiap instans VPC Amazon dalam cakupan kebijakan, dan mengaitkan grup keamanan yang direplikasi ke akun dan sumber daya yang berada dalam cakupan kebijakan. Saat Anda memodifikasi grup keamanan utama, Firewall Manager menyebarkan perubahan ke replika.

Saat menghapus kebijakan grup keamanan umum, Anda dapat memilih apakah akan membersihkan sumber daya yang dibuat oleh kebijakan tersebut. Untuk grup keamanan umum Firewall Manager, sumber daya ini adalah grup keamanan replika. Pilih opsi pembersihan kecuali Anda ingin mengelola setiap replika secara manual setelah kebijakan dihapus. Untuk sebagian besar situasi, memilih opsi pembersihan adalah pendekatan yang paling sederhana.

Bagaimana replika dikelola

Grup keamanan replika dalam instans VPC Amazon dikelola seperti grup keamanan Amazon VPC lainnya. Untuk selengkapnya, lihat Grup Keamanan untuk VPC Anda di Panduan Pengguna Amazon VPC.

Kebijakan grup keamanan audit konten

Gunakan kebijakan grup keamanan audit AWS Firewall Manager konten untuk mengaudit dan menerapkan tindakan kebijakan pada aturan yang digunakan dalam grup keamanan organisasi Anda. Kebijakan grup keamanan audit konten berlaku untuk semua grup keamanan yang dibuat pelanggan yang digunakan di AWS organisasi Anda, sesuai dengan cakupan yang Anda tetapkan dalam kebijakan.

Untuk panduan cara membuat kebijakan grup keamanan audit konten menggunakan konsol, lihatMembuat kebijakan grup keamanan audit konten.

Jenis sumber daya lingkup kebijakan

Anda dapat menerapkan kebijakan grup keamanan audit konten ke jenis sumber daya berikut:

- Contoh Amazon Elastic Compute Cloud (Amazon EC2)
- Antarmuka Jaringan Elastis
- Grup keamanan Amazon VPC

Kelompok keamanan dipertimbangkan dalam lingkup kebijakan jika mereka secara eksplisit berada dalam ruang lingkup atau jika mereka terkait dengan sumber daya yang berada dalam ruang lingkup.

Opsi aturan kebijakan

Anda dapat menggunakan aturan kebijakan terkelola atau aturan kebijakan khusus untuk setiap kebijakan audit konten, tetapi tidak keduanya.

- Aturan kebijakan terkelola — Dalam kebijakan dengan aturan terkelola, Anda dapat menggunakan daftar aplikasi dan protokol untuk mengontrol aturan mana yang diaudit oleh Manajer Firewall dan menandai sebagai patuh atau tidak patuh. Anda dapat menggunakan daftar yang dikelola oleh Firewall Manager. Anda juga dapat membuat dan menggunakan daftar aplikasi dan protokol Anda sendiri. Untuk informasi tentang jenis daftar ini dan opsi manajemen Anda untuk daftar kustom, lihatDaftar terkelola.
- Aturan kebijakan khusus — Dalam kebijakan dengan aturan kebijakan khusus, Anda menentukan grup keamanan yang ada sebagai grup keamanan audit untuk kebijakan Anda. Anda dapat menggunakan aturan grup keamanan audit sebagai templat yang mendefinisikan aturan yang diaudit oleh Manajer Firewall dan menandai sebagai patuh atau tidak sesuai.

Audit kelompok keamanan

Anda harus membuat grup keamanan audit menggunakan akun administrator Firewall Manager Anda, sebelum Anda dapat menggunakannya dalam kebijakan Anda. Anda dapat mengelola grup keamanan melalui Amazon Virtual Private Cloud (Amazon VPC) atau Amazon Elastic Compute Cloud (Amazon EC2). Untuk selengkapnya, lihat Bekerja dengan Grup Keamanan di Panduan Pengguna Amazon VPC.

Grup keamanan yang Anda gunakan untuk kebijakan grup keamanan audit konten digunakan oleh Firewall Manager hanya sebagai referensi perbandingan untuk grup keamanan yang berada dalam cakupan kebijakan. Firewall Manager tidak mengaitkannya dengan sumber daya apa pun di organisasi Anda.

Cara Anda menentukan aturan dalam grup keamanan audit bergantung pada pilihan Anda di setelan aturan kebijakan:

- Aturan kebijakan terkelola — Untuk pengaturan aturan kebijakan terkelola, Anda menggunakan grup keamanan audit untuk mengganti setelan lain dalam kebijakan, untuk secara eksplisit mengizinkan atau menolak aturan yang mungkin memiliki hasil kepatuhan lainnya.
  - Jika Anda memilih untuk selalu mengizinkan aturan yang ditetapkan dalam grup keamanan audit, aturan apa pun yang cocok dengan aturan yang ditentukan dalam grup keamanan audit dianggap sesuai dengan kebijakan, terlepas dari pengaturan kebijakan lainnya.
  - Jika Anda memilih untuk selalu menolak aturan yang ditetapkan dalam grup keamanan audit, aturan apa pun yang cocok dengan aturan yang ditetapkan dalam grup keamanan audit dianggap tidak sesuai dengan kebijakan, terlepas dari pengaturan kebijakan lainnya.
- Aturan kebijakan khusus — Untuk pengaturan aturan kebijakan khusus, grup keamanan audit memberikan contoh apa yang dapat diterima atau tidak dapat diterima dalam aturan grup keamanan dalam lingkup:
  - Jika Anda memilih untuk mengizinkan penggunaan aturan, semua grup keamanan dalam lingkup hanya boleh memiliki aturan yang berada dalam rentang yang diizinkan dari aturan grup keamanan audit kebijakan. Dalam hal ini, aturan kelompok keamanan kebijakan memberikan contoh tentang apa yang dapat diterima untuk dilakukan.
  - Jika Anda memilih untuk menolak penggunaan aturan, semua grup keamanan dalam ruang lingkup hanya boleh memiliki aturan yang tidak berada dalam rentang yang diizinkan dari aturan grup keamanan audit kebijakan. Dalam hal ini, kelompok keamanan kebijakan memberikan contoh tentang apa yang tidak dapat diterima untuk dilakukan.

Pembuatan dan manajemen kebijakan

Saat membuat kebijakan grup keamanan audit, remediasi otomatis harus dinonaktifkan. Praktik yang disarankan adalah meninjau efek pembuatan kebijakan sebelum mengaktifkan remediasi otomatis. Setelah meninjau efek yang diharapkan, Anda dapat mengedit kebijakan dan mengaktifkan remediasi otomatis. Ketika remediasi otomatis diaktifkan, Firewall Manager memperbarui atau menghapus aturan yang tidak sesuai dalam grup keamanan dalam lingkup.

Kelompok keamanan yang terpengaruh oleh kebijakan grup keamanan audit

Semua grup keamanan di organisasi Anda yang dibuat pelanggan memenuhi syarat untuk berada dalam cakupan kebijakan grup keamanan audit.

Grup keamanan replika tidak dibuat oleh pelanggan sehingga tidak memenuhi syarat untuk secara langsung berada dalam lingkup kebijakan grup keamanan audit. Namun, mereka dapat diperbarui sebagai hasil dari kegiatan remediasi otomatis kebijakan. Grup keamanan utama kebijakan grup keamanan umum dibuat oleh pelanggan dan dapat berada dalam lingkup kebijakan grup keamanan audit. Jika kebijakan grup keamanan audit membuat perubahan pada grup keamanan utama, Firewall Manager secara otomatis menyebarkan perubahan tersebut ke replika.

Penggunaan kebijakan grup keamanan audit

Gunakan kebijakan grup keamanan audit AWS Firewall Manager penggunaan untuk memantau organisasi Anda untuk grup keamanan yang tidak digunakan dan berlebihan dan secara opsional melakukan pembersihan. Bila Anda mengaktifkan remediasi otomatis untuk kebijakan ini, Firewall Manager melakukan hal berikut:

1. Mengkonsolidasikan grup keamanan yang berlebihan, jika Anda telah memilih opsi itu.
2. Menghapus grup keamanan yang tidak digunakan, jika Anda memilih opsi itu.

Anda dapat menerapkan kebijakan grup keamanan audit penggunaan ke jenis sumber daya berikut:

- Grup keamanan Amazon VPC

Untuk panduan cara membuat kebijakan grup keamanan audit penggunaan menggunakan konsol, lihatMembuat kebijakan grup keamanan audit penggunaan.

Bagaimana Firewall Manager mendeteksi dan memulihkan grup keamanan yang berlebihan

Agar kelompok keamanan dianggap berlebihan, mereka harus memiliki aturan yang persis sama dan berada dalam instance VPC Amazon yang sama.

Untuk memulihkan kumpulan grup keamanan yang berlebihan, Firewall Manager memilih salah satu grup keamanan dalam set yang akan disimpan, dan kemudian mengaitkannya ke semua sumber daya yang terkait dengan grup keamanan lain di set. Firewall Manager kemudian memisahkan grup keamanan lain dari sumber daya yang terkait dengannya, yang membuat mereka tidak digunakan.

> **Note**
>
> Jika Anda juga memilih untuk menghapus grup keamanan yang tidak digunakan, Firewall Manager melakukannya selanjutnya. Hal ini dapat mengakibatkan penghapusan kelompok keamanan yang berada di set redundan.

Bagaimana Firewall Manager mendeteksi dan memulihkan grup keamanan yang tidak digunakan

Firewall Manager menganggap grup keamanan tidak digunakan jika kedua hal berikut benar:

- Grup keamanan tidak digunakan oleh instans Amazon EC2 atau antarmuka elastis network Amazon EC2.
- Firewall Manager belum menerima item konfigurasi untuk itu dalam jumlah menit yang ditentukan dalam periode waktu aturan kebijakan.

Periode waktu aturan kebijakan memiliki pengaturan default nol menit, tetapi Anda dapat meningkatkan waktu hingga 365 hari (525.600 menit), untuk memberi diri Anda waktu untuk mengaitkan grup keamanan baru dengan sumber daya.

> **Important**
>
> Jika Anda menentukan jumlah menit selain nilai default nol, Anda harus mengaktifkan hubungan tidak langsung di AWS Config. Jika tidak, kebijakan grup keamanan audit penggunaan Anda tidak akan berfungsi sebagaimana dimaksud. Untuk informasi tentang hubungan tidak langsung di AWS Config, lihat Hubungan Tidak Langsung AWS Config di Panduan AWS Config Pengembang.

Firewall Manager memulihkan grup keamanan yang tidak digunakan dengan menghapusnya dari akun Anda sesuai dengan pengaturan aturan Anda, jika memungkinkan. Jika Firewall Manager tidak dapat menghapus grup keamanan, ia menandainya sebagai tidak sesuai dengan kebijakan. Firewall Manager tidak dapat menghapus grup keamanan yang direferensikan oleh grup keamanan lain.

Waktu remediasi bervariasi sesuai dengan apakah Anda menggunakan pengaturan periode waktu default atau pengaturan kustom:

- Periode waktu ditetapkan ke nol, default — Dengan pengaturan ini, grup keamanan dianggap tidak digunakan segera setelah tidak digunakan oleh instans Amazon EC2 atau elastic network interface.

  Untuk pengaturan periode waktu nol ini, Firewall Manager segera memperbaiki grup keamanan.
- Periode waktu lebih besar dari nol — Dengan pengaturan ini, grup keamanan dianggap tidak digunakan saat tidak digunakan oleh instans Amazon EC2 atau elastic network interface dan Firewall Manager belum menerima item konfigurasi untuk itu dalam jumlah menit yang ditentukan.

  Untuk pengaturan periode waktu bukan nol, Firewall Manager memulihkan grup keamanan setelah tetap dalam keadaan tidak digunakan selama 24 jam.

Spesifikasi akun default

Saat Anda membuat kebijakan grup keamanan audit penggunaan melalui konsol, Firewall Manager secara otomatis memilih Kecualikan akun yang ditentukan dan menyertakan semua akun lainnya. Layanan kemudian menempatkan akun administrator Firewall Manager dalam daftar untuk dikecualikan. Ini adalah pendekatan yang disarankan, dan memungkinkan Anda untuk secara manual mengelola grup keamanan milik akun administrator Firewall Manager.

Praktik terbaik untuk kebijakan grup keamanan

Bagian ini mencantumkan rekomendasi untuk mengelola grup keamanan yang digunakan AWS Firewall Manager.

Kecualikan akun administrator Manajer Firewall

Saat Anda menetapkan cakupan kebijakan, kecualikan akun administrator Manajer Firewall. Saat Anda membuat kebijakan grup keamanan audit penggunaan melalui konsol, ini adalah opsi default.

Mulailah dengan remediasi otomatis dinonaktifkan

Untuk kebijakan grup keamanan audit konten atau penggunaan, mulailah dengan remediasi otomatis dinonaktifkan. Tinjau informasi detail kebijakan untuk menentukan efek yang akan ditimbulkan oleh remediasi otomatis. Ketika Anda puas bahwa perubahan adalah apa yang Anda inginkan, edit kebijakan untuk mengaktifkan remediasi otomatis.

Hindari konflik jika Anda juga menggunakan sumber luar untuk mengelola grup keamanan

Jika Anda menggunakan alat atau layanan selain Firewall Manager untuk mengelola grup keamanan, berhati-hatilah untuk menghindari konflik antara pengaturan Anda di Firewall Manager

dan pengaturan di sumber luar Anda. Jika Anda menggunakan remediasi otomatis dan konflik pengaturan, Anda dapat membuat siklus remediasi yang bertentangan yang menghabiskan sumber daya di kedua sisi.

Misalnya, Anda mengonfigurasi layanan lain untuk mempertahankan grup keamanan untuk sekumpulan AWS sumber daya, dan Anda mengonfigurasi kebijakan Firewall Manager untuk mempertahankan grup keamanan yang berbeda untuk beberapa atau semua sumber daya yang sama. Jika Anda mengonfigurasi kedua sisi untuk melarang grup keamanan lain dikaitkan dengan sumber daya dalam lingkup, pihak tersebut akan menghapus asosiasi grup keamanan yang dikelola oleh pihak lain. Jika kedua belah pihak dikonfigurasi dengan cara ini, Anda dapat berakhir dengan siklus disasosiasi dan asosiasi yang saling bertentangan.

Selain itu, katakan bahwa Anda membuat kebijakan audit Firewall Manager untuk menerapkan konfigurasi grup keamanan yang bertentangan dengan konfigurasi grup keamanan dari layanan lain. Remediasi yang diterapkan oleh kebijakan audit Firewall Manager dapat memperbarui atau menghapus grup keamanan tersebut, membuatnya tidak sesuai dengan layanan lainnya. Jika layanan lain dikonfigurasi untuk memantau dan secara otomatis memperbaiki masalah yang ditemukannya, itu akan membuat ulang atau memperbarui grup keamanan, membuatnya lagi tidak sesuai dengan kebijakan audit Manajer Firewall. Jika kebijakan audit Firewall Manager dikonfigurasi dengan remediasi otomatis, kebijakan tersebut akan memperbarui atau menghapus grup keamanan luar, dan seterusnya.

Untuk menghindari konflik seperti ini, buat konfigurasi yang saling eksklusif, antara Firewall Manager dan sumber luar mana pun.

Anda dapat menggunakan penandaan untuk mengecualikan grup keamanan luar dari remediasi otomatis berdasarkan kebijakan Firewall Manager Anda. Untuk melakukan ini, tambahkan satu atau beberapa tag ke grup keamanan atau sumber daya lain yang dikelola oleh sumber luar. Kemudian, ketika Anda menentukan cakupan kebijakan Firewall Manager, dalam spesifikasi sumber daya Anda, kecualikan sumber daya yang memiliki tag atau tag yang telah Anda tambahkan.

Demikian pula, di alat atau layanan luar Anda, kecualikan grup keamanan yang dikelola Manajer Firewall dari aktivitas manajemen atau audit apa pun. Jangan mengimpor sumber daya Firewall Manager atau gunakan penandaan khusus Manajer Firewall untuk mengecualikannya dari manajemen luar.

Praktik terbaik untuk penggunaan kebijakan grup keamanan audit

Ikuti panduan ini saat Anda menggunakan kebijakan grup keamanan audit penggunaan.

- Hindari membuat beberapa perubahan pada status asosiasi grup keamanan dalam waktu singkat, seperti dalam jendela 15 menit. Melakukannya dapat menyebabkan Firewall Manager melewatkan beberapa atau semua peristiwa terkait. Misalnya, jangan cepat mengasosiasikan dan memisahkan grup keamanan dengan elastic network interface.

Peringatan dan batasan kebijakan kelompok keamanan

Bagian ini mencantumkan peringatan dan batasan untuk menggunakan kebijakan grup keamanan Firewall Manager:

- Memperbarui grup keamanan untuk antarmuka jaringan elastis Amazon EC2 yang dibuat menggunakan jenis layanan Fargate tidak didukung. Namun, Anda dapat memperbarui grup keamanan untuk antarmuka jaringan elastis Amazon ECS dengan jenis layanan Amazon EC2.
- Firewall Manager tidak mendukung grup keamanan untuk antarmuka jaringan elastis Amazon EC2 yang dibuat oleh Amazon Relational Database Service.
- Memperbarui antarmuka jaringan elastis Amazon ECS hanya dimungkinkan untuk layanan Amazon ECS yang menggunakan pengontrol penyebaran pembaruan bergulir (Amazon ECS). Untuk pengontrol penyebaran Amazon ECS lainnya seperti CODE_DEPLOY atau pengontrol eksternal, Firewall Manager saat ini tidak dapat memperbarui antarmuka jaringan elastis.
- Dengan grup keamanan untuk antarmuka jaringan elastis Amazon EC2, perubahan pada grup keamanan tidak langsung terlihat oleh Firewall Manager. Firewall Manager biasanya mendeteksi perubahan dalam beberapa jam, tetapi deteksi dapat ditunda hingga enam jam.
- Firewall Manager tidak mendukung pembaruan grup keamanan di antarmuka jaringan elastis untuk Network Load Balancer.
- Dalam kebijakan grup keamanan umum, jika VPC bersama kemudian tidak dibagikan dengan akun, Firewall Manager tidak akan menghapus grup keamanan replika di akun.
- Dengan kebijakan grup keamanan audit penggunaan, jika Anda membuat beberapa kebijakan dengan pengaturan waktu tunda khusus yang semuanya memiliki cakupan yang sama, kebijakan pertama dengan temuan kepatuhan adalah kebijakan yang melaporkan temuan.

Kasus penggunaan kebijakan grup keamanan

Anda dapat menggunakan kebijakan grup keamanan AWS Firewall Manager umum untuk mengotomatiskan konfigurasi firewall host untuk komunikasi antara instans Amazon VPC. Bagian ini mencantumkan arsitektur VPC Amazon standar dan menjelaskan cara mengamankan masing-

masing menggunakan kebijakan grup keamanan umum Firewall Manager. Kebijakan grup keamanan ini dapat membantu Anda menerapkan seperangkat aturan terpadu untuk memilih sumber daya di akun yang berbeda dan menghindari konfigurasi per akun di Amazon Elastic Compute Cloud dan Amazon VPC.

Dengan kebijakan grup keamanan umum Firewall Manager, Anda dapat menandai hanya antarmuka jaringan elastis EC2 yang Anda perlukan untuk komunikasi dengan instance di VPC Amazon lainnya. Contoh lain di VPC Amazon yang sama kemudian lebih aman dan terisolasi.

Kasus penggunaan: Memantau dan mengendalikan permintaan ke Application Load Balancers dan Classic Load Balancer

Anda dapat menggunakan kebijakan grup keamanan umum Firewall Manager untuk menentukan permintaan penyeimbang beban dalam ruang lingkup yang harus disajikan. Anda dapat mengonfigurasi ini melalui konsol Firewall Manager. Hanya permintaan yang mematuhi aturan masuk grup keamanan yang dapat mencapai penyeimbang beban Anda, dan penyeimbang beban hanya akan mendistribusikan permintaan yang memenuhi aturan keluar.

Kasus penggunaan: VPC Amazon publik yang dapat diakses Internet

Anda dapat menggunakan kebijakan grup keamanan umum Firewall Manager untuk mengamankan VPC Amazon publik, misalnya, untuk mengizinkan hanya port masuk 443. Ini sama dengan hanya mengizinkan lalu lintas HTTPS masuk untuk VPC publik. Anda dapat menandai sumber daya publik dalam VPC (misalnya, sebagai “PublicVPC”), lalu menyetel cakupan kebijakan Manajer Firewall ke hanya sumber daya dengan tag tersebut. Firewall Manager secara otomatis menerapkan kebijakan ke sumber daya tersebut.

Kasus penggunaan: Instans VPC Amazon Publik dan Pribadi

Anda dapat menggunakan kebijakan grup keamanan umum yang sama untuk sumber daya publik seperti yang direkomendasikan dalam kasus penggunaan sebelumnya untuk instans VPC Amazon publik yang dapat diakses internet. Anda dapat menggunakan kebijakan grup keamanan umum kedua untuk membatasi komunikasi antara sumber daya publik dan sumber daya pribadi. Tandai sumber daya dalam instance VPC Amazon publik dan pribadi dengan sesuatu seperti "PublicPrivate" untuk menerapkan kebijakan kedua kepada mereka. Anda dapat menggunakan kebijakan ketiga untuk menentukan komunikasi yang diizinkan antara sumber daya pribadi dan perusahaan lain atau instans VPC Amazon pribadi. Untuk kebijakan ini, Anda dapat menggunakan tag pengenal lain pada sumber daya pribadi.

Kasus penggunaan: Hub dan ucapkan instans VPC Amazon

Anda dapat menggunakan kebijakan grup keamanan umum untuk menentukan komunikasi antara instans VPC Amazon hub dan instance VPC Amazon. Anda dapat menggunakan kebijakan kedua untuk menentukan komunikasi dari setiap instance VPC Amazon spoke ke hub Amazon VPC instance.

Kasus penggunaan: Antarmuka jaringan default untuk instans Amazon EC2

Anda dapat menggunakan kebijakan grup keamanan umum untuk hanya mengizinkan komunikasi standar, misalnya layanan pembaruan SSH dan Patch/OS internal, dan untuk melarang komunikasi tidak aman lainnya.

Kasus penggunaan: Identifikasi sumber daya dengan izin terbuka

Anda dapat menggunakan kebijakan grup keamanan audit untuk mengidentifikasi semua sumber daya dalam organisasi Anda yang memiliki izin untuk berkomunikasi dengan alamat IP publik atau yang memiliki alamat IP milik vendor pihak ketiga.

Kebijakan daftar kontrol akses jaringan (ACL) Amazon VPC

Bagian ini mencakup cara kerja kebijakan ACL AWS Firewall Manager jaringan dan memberikan panduan untuk menggunakannya. Untuk panduan membuat kebijakan ACL jaringan menggunakan konsol, lihatMembuat kebijakan ACL jaringan.

Untuk informasi tentang daftar kontrol akses jaringan (ACL) Amazon VPC, lihat Mengontrol lalu lintas ke subnet menggunakan ACL jaringan di Panduan Pengguna Amazon VPC.

Anda dapat menggunakan kebijakan ACL jaringan Firewall Manager untuk mengelola daftar kontrol akses jaringan (ACL) Amazon Virtual Private Cloud (Amazon VPC) untuk organisasi Anda. AWS Organizations Anda menentukan pengaturan aturan ACL jaringan kebijakan dan akun serta subnet tempat Anda ingin pengaturan diberlakukan. Firewall Manager terus menerapkan pengaturan kebijakan Anda ke akun dan subnet saat ditambahkan atau diperbarui di seluruh organisasi Anda. Untuk informasi tentang cakupan kebijakan dan AWS Organizations, lihat AWS Firewall Manager ruang lingkup kebijakan dan Panduan AWS Organizations Pengguna.

Saat Anda menentukan kebijakan ACL jaringan Manajer Firewall, selain pengaturan kebijakan Firewall Manager standar, seperti nama dan cakupan, Anda memberikan yang berikut ini:

- Aturan pertama dan terakhir untuk penanganan lalu lintas masuk dan keluar. Firewall Manager memberlakukan keberadaan dan urutan ini di ACL jaringan yang berada dalam cakupan kebijakan,

atau melaporkan ketidakpatuhan. Akun individual Anda dapat membuat aturan khusus untuk dijalankan di antara aturan pertama dan terakhir kebijakan.

- Apakah akan memaksa remediasi ketika remediasi akan mengakibatkan konflik manajemen lalu lintas antara aturan dalam jaringan ACL. Ini hanya berlaku jika remediasi diaktifkan untuk kebijakan.

Aturan dan penandaan ACL jaringan Firewall Manager

Bagian ini menjelaskan spesifikasi aturan kebijakan ACL jaringan dan ACL jaringan yang dikelola oleh Firewall Manager.

Menandai pada jaringan terkelola ACL

Firewall Manager menandai ACL jaringan terkelola dengan `FMManaged` tag yang memiliki nilai. `true` Firewall Manager hanya melakukan remediasi pada ACL jaringan yang memiliki setelan tag ini.

Aturan yang Anda tetapkan dalam kebijakan

Dalam spesifikasi kebijakan ACL jaringan Anda, Anda menentukan aturan yang ingin Anda jalankan pertama dan terakhir untuk lalu lintas masuk dan aturan yang ingin Anda jalankan pertama dan terakhir untuk lalu lintas keluar.

Secara default, Anda dapat menentukan hingga 5 aturan masuk, untuk digunakan dalam kombinasi aturan pertama dan terakhir dalam kebijakan. Demikian pula, Anda dapat menentukan hingga 5 aturan keluar. Untuk informasi lebih lanjut tentang batasan ini, lihatKuota lembut. Untuk informasi tentang batasan umum pada ACL jaringan, lihat Kuota VPC Amazon pada ACL jaringan di Panduan Pengguna Amazon VPC.

Anda tidak menetapkan nomor aturan ke aturan kebijakan. Sebagai gantinya, Anda menentukan aturan dalam urutan yang Anda inginkan untuk dievaluasi, dan Firewall Manager menggunakan urutan tersebut untuk menetapkan nomor aturan di ACL jaringan yang dikelola.

Selain itu, Anda mengelola spesifikasi aturan ACL jaringan kebijakan karena Anda akan mengelola aturan dalam ACL jaringan melalui Amazon VPC. Untuk informasi tentang manajemen ACL jaringan di Amazon VPC, lihat Mengontrol lalu lintas ke subnet menggunakan ACL jaringan dan Bekerja dengan ACL jaringan di Panduan Pengguna Amazon VPC.

Aturan dalam jaringan terkelola ACL

Firewall Manager mengonfigurasi aturan dalam ACL jaringan yang dikelola dengan menempatkan aturan pertama dan terakhir kebijakan sebelum dan sesudah aturan kustom apa pun yang ditentukan oleh manajer akun individual. Firewall Manager mempertahankan urutan aturan kustom. ACL jaringan dievaluasi dimulai dengan aturan bernomor terendah.

Ketika Firewall Manager pertama kali membuat ACL jaringan, ia mendefinisikan aturan dengan penomoran berikut:

- Aturan pertama: 1, 2,... — Didefinisikan oleh Anda dalam kebijakan ACL jaringan Firewall Manager.

  Firewall Manager menetapkan nomor aturan mulai dari 1 dengan penambahan 1, dengan aturan yang diurutkan seperti yang Anda pesan dalam spesifikasi kebijakan.
- Aturan kustom: 5.000, 5,100,... — Dikelola oleh manajer akun individu melalui Amazon VPC.

  Firewall Manager menetapkan nomor untuk aturan ini mulai dari 5.000 dan bertambah 100 untuk setiap aturan berikutnya.
- Aturan terakhir:... 32,765, 32,766 — Ditentukan oleh Anda dalam kebijakan ACL jaringan Firewall Manager.

  Firewall Manager menetapkan nomor aturan yang berakhir pada angka setinggi mungkin, 32766 dengan penambahan 1, dengan aturan yang diurutkan seperti yang Anda pesan dalam spesifikasi kebijakan.

Setelah inisialisasi ACL jaringan, Firewall Manager tidak mengontrol perubahan yang dilakukan akun individual di ACL jaringan terkelolanya. Akun individu dapat mengubah ACL jaringan tanpa mengeluarkannya dari kepatuhan, dengan ketentuan aturan kustom apa pun tetap diberi nomor di antara aturan pertama dan terakhir kebijakan, dan aturan pertama dan terakhir mempertahankan urutan yang ditentukan. Sebagai praktik terbaik, saat mengelola aturan khusus, patuhi penomoran yang dijelaskan di bagian ini.

Bagaimana Firewall Manager memulai manajemen ACL jaringan untuk subnet

Firewall Manager memulai pengelolaan jaringan ACL untuk subnet ketika mengaitkan subnet dengan jaringan ACL yang Firewall Manager telah dibuat dan ditandai dengan set to. `FMManaged` `true`

Kepatuhan terhadap kebijakan ACL jaringan mengharuskan ACL jaringan subnet untuk menempatkan aturan pertama kebijakan terlebih dahulu, dalam urutan yang ditentukan dalam kebijakan, aturan terakhir yang diposisikan terakhir, berurutan, dan aturan kustom lainnya yang

ditempatkan di tengah. Persyaratan ini dapat dipenuhi oleh ACL jaringan yang tidak dikelola bahwa subnet sudah dikaitkan dengan atau oleh ACL jaringan terkelola.

Ketika Firewall Manager menerapkan kebijakan ACL jaringan ke subnet yang terkait dengan ACL jaringan yang tidak dikelola, Firewall Manager memeriksa hal-hal berikut secara berurutan, berhenti ketika mengidentifikasi opsi yang layak:

1. ACL jaringan terkait sudah sesuai — Jika ACL jaringan yang saat ini terkait dengan subnet sesuai, maka Firewall Manager meninggalkan asosiasi itu dan tidak memulai manajemen ACL jaringan untuk subnet.

   Firewall Manager tidak mengubah atau mengelola ACL jaringan yang tidak dimilikinya, tetapi selama itu sesuai, Firewall Manager membiarkannya di tempatnya dan hanya memantaunya untuk kepatuhan kebijakan.
2. Tersedia ACL jaringan terkelola yang sesuai — Jika Firewall Manager sudah mengelola ACL jaringan yang sesuai dengan konfigurasi yang diperlukan, maka ini adalah opsi. Jika remediasi diaktifkan, Firewall Manager mengaitkan subnet ke subnet tersebut. Jika remediasi dinonaktifkan, Firewall Manager menandai subnet yang tidak sesuai dan menawarkan penggantian asosiasi ACL jaringan sebagai opsi remediasi.
3. Buat ACL jaringan terkelola baru yang sesuai — Jika remediasi diaktifkan, Firewall Manager membuat ACL jaringan baru dan mengaitkannya dengan subnet. Jika tidak, Firewall Manager menandai subnet yang tidak sesuai dan menawarkan opsi remediasi untuk membuat ACL jaringan baru dan mengganti asosiasi ACL jaringan.

Jika langkah-langkah ini gagal, Firewall Manager melaporkan ketidakpatuhan untuk subnet.

Firewall Manager mengikuti langkah-langkah ini ketika subnet pertama kali masuk ke ruang lingkup dan ketika ACL jaringan subnet yang tidak dikelola tidak sesuai.

Bagaimana Firewall Manager memulihkan ACL jaringan terkelola yang tidak sesuai

Bagian ini menjelaskan cara Firewall Manager memulihkan ACL jaringan terkelolanya ketika mereka tidak sesuai dengan kebijakan. Firewall Manager hanya memperbaiki ACL jaringan terkelola—dengan tag disetel ke. `FMManaged` `true` Untuk ACL jaringan yang tidak dikelola oleh Firewall Manager, lihatManajemen ACL jaringan awal.

Remediasi mengembalikan lokasi relatif dari aturan pertama, kustom, dan terakhir dan mengembalikan pemesanan untuk aturan pertama dan terakhir. Selama remediasi, Firewall Manager

tidak akan selalu memindahkan aturan ke nomor aturan yang digunakan dalam inisialisasi ACL jaringan. Untuk pengaturan nomor awal dan deskripsi kategori aturan ini, lihatManajemen ACL jaringan awal.

Untuk menetapkan aturan dan urutan aturan yang sesuai, Firewall Manager mungkin perlu memindahkan aturan di dalam ACL jaringan. Sebisa mungkin, Firewall Manager mempertahankan perlindungan ACL jaringan dengan mempertahankan urutan aturan yang sesuai seperti yang dilakukan. Misalnya, mungkin sementara menduplikasi aturan ke lokasi baru, dan kemudian melakukan penghapusan berurutan aturan asli, menjaga lokasi relatif selama proses.

Pendekatan ini melindungi pengaturan Anda, tetapi juga membutuhkan ruang di ACL jaringan untuk aturan sementara. Jika Firewall Manager mencapai batas untuk aturan dalam ACL jaringan, itu akan menghentikan remediasi. Ketika ini terjadi, ACL jaringan tetap tidak sesuai dan Firewall Manager melaporkan alasannya.

Jika akun menambahkan aturan khusus ke ACL jaringan yang dikelola oleh Firewall Manager, dan aturan tersebut mengganggu remediasi Firewall Manager, Firewall Manager menghentikan aktivitas remediasi apa pun di ACL jaringan dan melaporkan konflik tersebut.

Remediasi paksa

Jika Anda memilih remediasi otomatis untuk kebijakan tersebut, Anda juga menentukan apakah akan memaksa remediasi untuk aturan pertama atau aturan terakhir.

Ketika Firewall Manager menghadapi konflik dalam penanganan lalu lintas antara aturan kustom dan aturan kebijakan, itu mengacu pada pengaturan remediasi paksa yang sesuai. Jika remediasi paksa diaktifkan, Firewall Manager menerapkan remediasi, terlepas dari konflik. Jika opsi ini tidak diaktifkan, Firewall Manager menghentikan remediasi. Dalam kedua kasus tersebut, Firewall Manager melaporkan konflik aturan dan menawarkan opsi remediasi.

Persyaratan dan batasan jumlah aturan

Selama remediasi, Firewall Manager mungkin sementara menduplikasi aturan untuk memindahkannya tanpa mengubah perlindungan yang mereka berikan.

Untuk aturan masuk atau keluar, jumlah aturan terbesar yang mungkin diperlukan oleh Manajer Firewall untuk melakukan remediasi adalah sebagai berikut:

```
2 * (the number of rules defined in the policy for the traffic direction)
+
```

```
the number of custom rules defined in the network ACL for the traffic direction
```

ACL jaringan dan kebijakan ACL jaringan terikat oleh batas aturan yang dapat berubah. Jika Firewall Manager mencapai batas dalam upaya remediasi, ia berhenti mencoba untuk memulihkan dan melaporkan ketidakpatuhan.

Untuk memberi ruang bagi Firewall Manager untuk melakukan aktivitas remediasi, Anda dapat meminta peningkatan batas. Sebagai alternatif, Anda dapat mengubah konfigurasi dalam kebijakan atau jaringan ACL untuk mengurangi jumlah aturan yang digunakan.

Untuk informasi tentang batas ACL jaringan, lihat Kuota VPC Amazon pada ACL jaringan di Panduan Pengguna Amazon VPC.

Ketika remediasi gagal

Saat memperbarui ACL jaringan, jika Firewall Manager perlu berhenti karena alasan apa pun, itu tidak mengembalikan perubahan, tetapi sebaliknya meninggalkan ACL jaringan dalam keadaan sementara. Jika Anda melihat aturan duplikat di ACL jaringan yang memiliki `FMManaged` tag yang disetel `ketrue`, Firewall Manager mungkin sedang memperbaiki itu. Perubahan mungkin sebagian selesai untuk suatu periode, tetapi karena pendekatan yang dilakukan Firewall Manager untuk remediasi, ini tidak akan mengganggu lalu lintas atau mengurangi perlindungan untuk subnet terkait.

Ketika Firewall Manager tidak sepenuhnya memulihkan ACL jaringan yang tidak sesuai, ia melaporkan ketidakpatuhan untuk subnet terkait dan menyarankan kemungkinan opsi remediasi.

Mencoba lagi setelah remediasi gagal

Dalam kebanyakan kasus, jika Firewall Manager gagal menyelesaikan perubahan remediasi ke ACL jaringan, pada akhirnya akan mencoba kembali perubahan tersebut.

Pengecualian untuk ini adalah ketika remediasi mencapai batas jumlah aturan ACL jaringan atau batas jumlah ACL jaringan VPC. Firewall Manager tidak dapat melakukan aktivitas remediasi yang mengambil AWS sumber daya melebihi pengaturan batasnya. Dalam kasus ini, Anda perlu mengurangi jumlah atau menambah batas untuk melanjutkan. Untuk informasi tentang batasan, lihat kuota VPC Amazon pada ACL jaringan di Panduan Pengguna Amazon VPC.

Pelaporan kepatuhan ACL jaringan Firewall Manager

Firewall Manager memantau dan melaporkan kepatuhan untuk semua ACL jaringan yang dilampirkan ke subnet dalam lingkup.

Secara umum, ketidakpatuhan terjadi untuk situasi seperti urutan aturan yang salah atau konflik dalam perilaku penanganan lalu lintas antara aturan kebijakan dan aturan khusus. Pelaporan ketidakpatuhan mencakup pelanggaran kepatuhan dan opsi remediasi.

Firewall Manager melaporkan pelanggaran kepatuhan untuk kebijakan ACL jaringan dengan cara yang sama seperti jenis kebijakan lainnya. Untuk informasi tentang pelaporan kepatuhan, lihatMelihat informasi kepatuhan untuk suatu AWS Firewall Manager kebijakan.

Ketidakpatuhan selama pembaruan kebijakan

Setelah Anda mengubah kebijakan ACL jaringan, hingga Firewall Manager memperbarui ACL jaringan yang berada dalam cakupan kebijakan, Firewall Manager menandai ACL jaringan tersebut tidak sesuai. Firewall Manager melakukan ini bahkan jika ACL jaringan mungkin, secara tegas, mematuhi.

Misalnya, jika Anda menghapus aturan dari spesifikasi kebijakan, sementara ACL jaringan dalam cakupan masih memiliki aturan tambahan, definisi aturannya mungkin masih mematuhi kebijakan. Namun, karena aturan tambahan adalah bagian dari aturan yang dikelola oleh Firewall Manager, Firewall Manager melihatnya sebagai pelanggaran pengaturan kebijakan saat ini. Ini berbeda dengan cara Manajer Firewall melihat aturan khusus yang Anda tambahkan ke ACL jaringan terkelola Manajer Firewall.

Praktik terbaik untuk menggunakan kebijakan ACL jaringan Firewall Manager

Bagian ini mencantumkan rekomendasi untuk bekerja dengan kebijakan ACL jaringan Firewall Manager dan ACL jaringan terkelola.

Lihat **`FMManaged`** tag untuk mengidentifikasi ACL jaringan yang dikelola oleh Firewall Manager

ACL jaringan yang dikelola Firewall Manager memiliki `FMManaged` tag yang disetel ke`true`. Gunakan tag ini untuk membantu membedakan ACL jaringan kustom Anda sendiri dari yang Anda kelola melalui Firewall Manager.

Jangan mengubah nilai **`FMManaged`** tag pada ACL jaringan

Firewall Manager menggunakan tag ini untuk mengatur dan menentukan status manajemennya dengan ACL jaringan.

Jangan mengubah asosiasi untuk subnet yang memiliki ACL jaringan terkelola Firewall Manager

Jangan secara manual mengubah asosiasi antara subnet Anda dan ACL jaringan apa pun yang dikelola oleh Firewall Manager. Melakukannya dapat menonaktifkan kemampuan Firewall Manager untuk mengelola perlindungan untuk subnet tersebut. Anda dapat mengidentifikasi ACL jaringan yang dikelola oleh Firewall Manager dengan mencari pengaturan `FMManaged` tag. `true`

Untuk menghapus subnet dari manajemen kebijakan Firewall Manager, gunakan pengaturan cakupan kebijakan Manajer Firewall untuk mengecualikan subnet. Misalnya, Anda dapat menandai subnet dan kemudian mengecualikan tag tersebut dari cakupan kebijakan. Untuk informasi selengkapnya, lihat AWS Firewall Manager ruang lingkup kebijakan.

Saat Anda memperbarui ACL jaringan terkelola, jangan mengubah aturan yang dikelola oleh Firewall Manager

Di ACL jaringan yang dikelola oleh Firewall Manager, pisahkan aturan kustom Anda dari aturan kebijakan dengan mengikuti skema penomoran yang dijelaskan dalam. Aturan dan penandaan ACL jaringan Firewall Manager Hanya menambah atau memodifikasi aturan yang memiliki angka antara 5.000 dan 32.000.

Hindari menambahkan terlalu banyak aturan untuk batas akun Anda

Selama remediasi ACL jaringan, Firewall Manager biasanya meningkatkan jumlah aturan ACL jaringan sementara. Untuk menghindari masalah ketidakpatuhan, pastikan Anda memiliki cukup ruang untuk aturan yang Anda gunakan. Untuk informasi selengkapnya, lihat Bagaimana Firewall Manager memulihkan ACL jaringan terkelola yang tidak sesuai.

Mulailah dengan remediasi otomatis dinonaktifkan

Mulailah dengan remediasi otomatis dinonaktifkan, lalu tinjau informasi detail kebijakan untuk menentukan efek yang akan ditimbulkan oleh remediasi otomatis. Ketika Anda puas bahwa perubahan adalah apa yang Anda inginkan, edit kebijakan untuk mengaktifkan remediasi otomatis.

Peringatan kebijakan ACL jaringan Firewall Manager

Bagian ini mencantumkan peringatan dan batasan untuk menggunakan kebijakan ACL jaringan Firewall Manager.

- Waktu pembaruan lebih lambat dibandingkan dengan kebijakan lain — Firewall Manager umumnya menerapkan kebijakan ACL jaringan dan perubahan kebijakan lebih lambat dibandingkan dengan kebijakan Firewall Manager lainnya, karena keterbatasan dalam tingkat di mana API ACL jaringan

Amazon EC2 dapat memproses permintaan. Anda mungkin memperhatikan bahwa perubahan kebijakan membutuhkan waktu lebih lama daripada perubahan serupa dengan kebijakan Firewall Manager lainnya, khususnya saat Anda pertama kali menambahkan kebijakan.

- Untuk perlindungan subnet awal, Firewall Manager lebih memilih kebijakan yang lebih lama — Ini hanya berlaku untuk subnet yang belum dilindungi oleh kebijakan ACL jaringan Firewall Manager. Jika subnet masuk ke dalam cakupan lebih dari satu kebijakan ACL jaringan pada saat yang sama, maka Firewall Manager menggunakan kebijakan tertua untuk melindungi subnet.
- Alasan kebijakan untuk berhenti melindungi subnet — Kebijakan yang mengelola ACL jaringan untuk subnet mempertahankan manajemen sampai salah satu hal berikut terjadi:
  - Subnet keluar dari cakupan kebijakan.
  - Kebijakan ini dihapus.
  - Anda secara manual mengubah asosiasi subnet ke ACL jaringan yang dikelola oleh kebijakan Firewall Manager yang berbeda dan cakupannya subnet.

Menghapus kebijakan ACL jaringan Firewall Manager

Saat Anda menghapus kebijakan ACL jaringan Manajer Firewall, Firewall Manager mengubah nilai `FMManaged` tag `false` pada semua ACL jaringan yang telah dikelola untuk kebijakan tersebut.

Selain itu, Anda dapat memilih apakah akan membersihkan sumber daya yang dibuat oleh kebijakan. Jika Anda memilih membersihkan, Firewall Manager mencoba langkah-langkah berikut secara berurutan:

1. Kembalikan asosiasi ke aslinya — Firewall Manager mencoba mengaitkan subnet kembali ke ACL jaringan yang dikaitkan dengannya sebelum Firewall Manager mulai mengelolanya.
2. Hapus aturan pertama dan terakhir dari ACL jaringan — Jika tidak dapat mengubah asosiasi, Firewall Manager mencoba menghapus aturan pertama dan terakhir kebijakan, hanya menyisakan aturan khusus di ACL jaringan yang terkait dengan subnet.
3. Jangan lakukan apa pun pada aturan atau asosiasi — Jika tidak dapat melakukan salah satu dari hal-hal di atas, Firewall Manager meninggalkan jaringan ACL dan asosiasinya sebagaimana adanya.

Jika Anda tidak memilih opsi pembersihan, Anda harus mengelola setiap ACL jaringan secara manual setelah kebijakan dihapus. Untuk sebagian besar situasi, memilih opsi pembersihan adalah pendekatan yang paling sederhana.

AWS Network Firewall kebijakan

Anda dapat menggunakan kebijakan AWS Firewall Manager Network Firewall untuk mengelola AWS Network Firewall firewall untuk VPC Amazon Virtual Private Cloud di seluruh organisasi. AWS Organizations Anda dapat menerapkan firewall yang dikontrol secara terpusat ke seluruh organisasi Anda atau ke subset tertentu dari akun dan VPC Anda.

Network Firewall menyediakan perlindungan pemfilteran lalu lintas jaringan untuk subnet publik di VPC Anda. Firewall Manager membuat dan mengelola firewall berdasarkan jenis manajemen firewall yang ditentukan oleh kebijakan Anda. Firewall Manager menyediakan model manajemen firewall berikut:

- Didistribusikan - Untuk setiap akun dan VPC yang berada dalam cakupan kebijakan, Firewall Manager membuat firewall Network Firewall dan menyebarkan titik akhir firewall ke subnet VPC, untuk memfilter lalu lintas jaringan.
- Terpusat - Firewall Manager membuat firewall Network Firewall tunggal dalam satu VPC Amazon.
- Impor firewall yang ada - Firewall Manager mengimpor firewall yang ada untuk pengelolaan dalam satu kebijakan Firewall Manager. Anda dapat menerapkan aturan tambahan ke firewall impor yang dikelola oleh kebijakan Anda untuk memastikan bahwa firewall Anda memenuhi standar keamanan Anda.

> **Note**
>
> Kebijakan Firewall Manager Network Firewall adalah kebijakan Firewall Manager yang Anda gunakan untuk mengelola perlindungan Firewall Jaringan untuk VPC Anda di seluruh organisasi Anda.
> Perlindungan Network Firewall ditentukan dalam sumber daya dalam layanan Network Firewall yang disebut kebijakan firewall.

Untuk informasi tentang menggunakan Network Firewall, lihat Panduan AWS Network Firewall Pengembang.

Bagian berikut mencakup persyaratan untuk menggunakan kebijakan Firewall Manager Network Firewall dan menjelaskan cara kerja kebijakan. Untuk prosedur pembuatan kebijakan, lihatMembuat AWS Firewall Manager kebijakan untuk AWS Network Firewall.

Anda harus mengaktifkan berbagi sumber daya

Kebijakan Firewall Jaringan membagikan grup aturan Firewall Jaringan di seluruh akun di organisasi Anda. Agar ini berfungsi, Anda harus mengaktifkan berbagi sumber daya AWS Organizations. Untuk informasi tentang cara mengaktifkan berbagi sumber daya, lihatBerbagi sumber daya untuk kebijakan Network Firewall dan DNS Firewall.

Anda harus memiliki grup aturan Network Firewall yang ditentukan

Ketika Anda menentukan kebijakan Network Firewall baru, Anda menentukan kebijakan firewall sama seperti yang Anda lakukan ketika Anda menggunakan AWS Network Firewall secara langsung. Anda menentukan grup aturan stateless untuk ditambahkan, tindakan stateless default, dan grup aturan stateful. Grup aturan Anda harus sudah ada di akun administrator Manajer Firewall agar Anda dapat memasukkannya ke dalam kebijakan. Untuk informasi tentang membuat grup aturan Firewall Jaringan, lihat grup AWS Network Firewall aturan.

Bagaimana Firewall Manager membuat titik akhir firewall

Jenis manajemen Firewall dalam kebijakan Anda menentukan cara Firewall Manager membuat firewall. Kebijakan Anda dapat membuat firewall terdistribusi, firewall terpusat, atau Anda dapat mengimpor firewall yang ada:

- Didistribusikan - Dengan model penerapan terdistribusi, Firewall Manager membuat titik akhir untuk setiap VPC yang berada dalam cakupan kebijakan. Anda dapat menyesuaikan lokasi titik akhir dengan menentukan Availability Zones untuk membuat endpoint firewall, atau Firewall Manager dapat secara otomatis membuat endpoint di Availability Zones dengan subnet publik. Jika Anda memilih Availability Zones secara manual, Anda memiliki opsi untuk membatasi kumpulan CIDR yang diizinkan per Availability Zone. Jika Anda memutuskan untuk membiarkan Firewall Manager secara otomatis membuat endpoint, Anda juga harus menentukan apakah layanan akan membuat endpoint tunggal atau beberapa endpoint firewall dalam VPC Anda.
  - Untuk beberapa titik akhir firewall, Firewall Manager menyebarkan titik akhir firewall di setiap Availability Zone di mana Anda memiliki subnet dengan gateway internet atau rute endpoint firewall yang dibuat oleh Manajer Firewall di tabel rute. Ini adalah opsi default untuk kebijakan Network Firewall.
  - Untuk titik akhir firewall tunggal, Firewall Manager menyebarkan titik akhir firewall di satu Availability Zone di subnet mana pun yang memiliki rute gateway internet. Dengan opsi ini, lalu lintas di zona lain perlu melintasi batas zona agar dapat disaring oleh firewall.

> **Note**
>
> Untuk kedua opsi ini, harus ada subnet yang terkait dengan tabel rute yang memiliki rute IPv4/PrefixList di dalamnya. Firewall Manager tidak memeriksa sumber daya lainnya.

- Terpusat - Dengan model penyebaran terpusat, Firewall Manager membuat satu atau lebih titik akhir firewall dalam VPC inspeksi. VPC inspeksi adalah VPC pusat tempat Firewall Manager meluncurkan endpoint Anda. Saat Anda menggunakan model penerapan terpusat, Anda juga menentukan Availability Zone untuk membuat endpoint firewall. Anda tidak dapat mengubah VPC inspeksi setelah membuat kebijakan. Untuk menggunakan VPC inspeksi yang berbeda, Anda harus membuat kebijakan baru.
- Impor firewall yang ada - Saat Anda mengimpor firewall yang ada, Anda memilih firewall yang akan dikelola dalam kebijakan Anda dengan menambahkan satu atau beberapa kumpulan sumber daya ke kebijakan Anda. Kumpulan sumber daya adalah kumpulan sumber daya, dalam hal ini firewall yang ada di Network Firewall, yang dikelola oleh akun di organisasi Anda. Sebelum menggunakan kumpulan sumber daya dalam kebijakan, Anda harus terlebih dahulu membuat kumpulan sumber daya. Untuk informasi tentang kumpulan sumber daya Firewall Manager, lihatBekerja dengan kumpulan sumber daya di Firewall Manager.

  Ingatlah pertimbangan berikut saat bekerja dengan firewall yang diimpor:

  - Jika firewall yang diimpor menjadi tidak sesuai, Firewall Manager akan mencoba menyelesaikan pelanggaran secara otomatis, kecuali dalam keadaan berikut:
    - Jika ada ketidakcocokan antara tindakan default stateful atau stateless kebijakan Firewall Manager Firewall Firewall.
    - Jika grup aturan dalam kebijakan firewall firewall yang diimpor memiliki prioritas yang sama dengan grup aturan dalam kebijakan Firewall Manager.
    - Jika firewall yang diimpor menggunakan kebijakan firewall yang terkait dengan firewall, itu bukan bagian dari kumpulan sumber daya kebijakan. Hal ini dapat terjadi karena firewall dapat memiliki tepat satu kebijakan firewall, tetapi kebijakan firewall tunggal dapat dikaitkan dengan beberapa firewall.
    - Jika grup aturan yang sudah ada sebelumnya milik kebijakan firewall firewall yang diimpor yang juga ditentukan dalam kebijakan Firewall Manager diberikan prioritas yang berbeda.
  - Jika Anda mengaktifkan pembersihan sumber daya dalam kebijakan, Firewall Manager menghapus grup aturan yang telah ada dalam kebijakan impor FMS dari firewall dalam lingkup kumpulan sumber daya.

- Firewall yang dikelola oleh Firewall Manager mengimpor jenis manajemen firewall yang ada hanya dapat dikelola oleh satu kebijakan pada satu waktu. Jika kumpulan sumber daya yang sama ditambahkan ke beberapa kebijakan firewall jaringan impor, firewall dalam kumpulan sumber daya akan dikelola oleh kebijakan pertama yang ditambahkan kumpulan sumber daya dan akan diabaikan oleh kebijakan kedua.
- Firewall Manager saat ini tidak melakukan streaming konfigurasi kebijakan pengecualian. Untuk informasi tentang kebijakan pengecualian aliran, lihat Kebijakan pengecualian Streaming di Panduan AWS Network Firewall Pengembang.

Jika Anda mengubah daftar Availability Zone untuk kebijakan yang menggunakan manajemen firewall terdistribusi atau terpusat, Firewall Manager akan mencoba membersihkan titik akhir apa pun yang dibuat di masa lalu, tetapi saat ini tidak dalam cakupan kebijakan. Firewall Manager akan menghapus titik akhir hanya jika tidak ada rute tabel rute yang mereferensikan titik akhir di luar cakupan. Jika Firewall Manager menemukan bahwa ia tidak dapat menghapus titik akhir ini, itu akan menandai subnet firewall sebagai tidak sesuai dan akan terus mencoba untuk menghapus titik akhir hingga saat aman untuk dihapus.

Bagaimana Firewall Manager mengelola subnet firewall Anda

Subnet firewall adalah subnet VPC yang dibuat oleh Firewall Manager untuk titik akhir firewall yang menyaring lalu lintas jaringan Anda. Setiap titik akhir firewall harus digunakan dalam subnet VPC khusus. Firewall Manager membuat setidaknya satu subnet firewall di setiap VPC yang berada dalam cakupan kebijakan.

Untuk kebijakan yang menggunakan model penyebaran terdistribusi dengan konfigurasi titik akhir otomatis, Firewall Manager hanya membuat subnet firewall di Availability Zones yang memiliki subnet dengan rute gateway internet, atau subnet dengan rute ke titik akhir firewall yang dibuat oleh Firewall Manager untuk kebijakan mereka. Untuk informasi selengkapnya, lihat VPC dan subnet di Panduan Pengguna Amazon VPC.

Untuk kebijakan yang menggunakan model terdistribusi atau terpusat tempat Anda menentukan Availability Zones Firewall Manager mana yang membuat titik akhir firewall, Firewall Manager membuat titik akhir di Availability Zone tertentu terlepas dari apakah ada sumber daya lain di Availability Zone.

Saat pertama kali menentukan kebijakan Network Firewall, Anda menentukan cara Firewall Manager mengelola subnet firewall di masing-masing VPC yang berada dalam cakupan. Anda tidak dapat mengubah pilihan ini nanti.

Untuk kebijakan yang menggunakan model penerapan terdistribusi dengan konfigurasi titik akhir otomatis, Anda dapat memilih di antara opsi berikut:

- Menyebarkan subnet firewall untuk setiap Availability Zone yang memiliki subnet publik. Ini adalah perilaku default. Ini memberikan ketersediaan tinggi perlindungan penyaringan lalu lintas Anda.
- Menyebarkan subnet firewall tunggal dalam satu Availability Zone. Dengan pilihan ini, Firewall Manager mengidentifikasi zona di VPC yang memiliki subnet publik paling banyak dan membuat subnet firewall di sana. Titik akhir firewall tunggal menyaring semua lalu lintas jaringan untuk VPC. Ini dapat mengurangi biaya firewall, tetapi tidak terlalu tersedia dan memerlukan lalu lintas dari zona lain untuk melintasi batas zona agar dapat disaring.

Untuk kebijakan yang menggunakan model penerapan terdistribusi dengan konfigurasi titik akhir kustom atau model penerapan terpusat, Firewall Manager membuat subnet di Availability Zone tertentu yang berada dalam cakupan kebijakan.

Anda dapat menyediakan blok VPC CIDR untuk Firewall Manager untuk digunakan untuk subnet firewall atau Anda dapat meninggalkan pilihan alamat endpoint firewall hingga Firewall Manager untuk menentukan.

- Jika Anda tidak menyediakan blok CIDR, Firewall Manager menanyakan VPC Anda untuk alamat IP yang tersedia untuk digunakan.
- Jika Anda memberikan daftar blok CIDR, Firewall Manager mencari subnet baru hanya di blok CIDR yang Anda berikan. Anda harus menggunakan blok /28 CIDR. Untuk setiap subnet firewall yang dibuat oleh Firewall Manager, ia berjalan di daftar blok CIDR Anda dan menggunakan yang pertama yang ditemukan yang berlaku untuk Availability Zone dan VPC dan memiliki alamat yang tersedia. Jika Firewall Manager tidak dapat menemukan ruang terbuka di VPC (dengan atau tanpa batasan), layanan tidak akan membuat firewall di VPC.

Jika Firewall Manager tidak dapat membuat subnet firewall yang diperlukan di Availability Zone, itu menandai subnet sebagai tidak sesuai dengan kebijakan. Sementara zona dalam keadaan ini, lalu lintas untuk zona harus melintasi batas zona untuk disaring oleh titik akhir di zona lain. Ini mirip dengan skenario subnet firewall tunggal.

Bagaimana Firewall Manager mengelola sumber daya Network Firewall Anda

Saat Anda menentukan kebijakan di Firewall Manager, Anda memberikan perilaku pemfilteran lalu lintas jaringan dari kebijakan AWS Network Firewall firewall standar. Anda menambahkan grup aturan

Network Firewall stateless dan stateful dan menentukan tindakan default untuk paket yang tidak cocok dengan aturan stateless. Untuk informasi tentang cara bekerja dengan kebijakan firewall AWS Network Firewall, lihat kebijakan AWS Network Firewall firewall.

Untuk kebijakan terdistribusi dan terpusat, saat Anda menyimpan kebijakan Network Firewall, Firewall Manager membuat kebijakan firewall dan firewall di setiap VPC yang berada dalam cakupan kebijakan. Firewall Manager menamai sumber daya Network Firewall ini dengan menggabungkan nilai-nilai berikut:

- String tetap, baik `FMManagedNetworkFirewall` atau`FMManagedNetworkFirewallPolicy`, tergantung pada jenis sumber daya.
- Nama kebijakan Firewall Manager. Ini adalah nama yang Anda tetapkan saat membuat kebijakan.
- ID kebijakan Manajer Firewall. Ini adalah ID AWS sumber daya untuk kebijakan Firewall Manager.
- ID VPC Amazon. Ini adalah ID AWS sumber daya untuk VPC tempat Firewall Manager membuat kebijakan firewall dan firewall.

Berikut ini menunjukkan contoh nama untuk firewall yang dikelola oleh Firewall Manager:

```
FMManagedNetworkFirewallEXAMPLENameEXAMPLEFirewallManagerPolicyIdEXAMPLEVPCId
```

Berikut ini menunjukkan contoh nama kebijakan firewall:

```
FMManagedNetworkFirewallPolicyEXAMPLENameEXAMPLEFirewallManagerPolicyIdEXAMPLEVPCId
```

Setelah Anda membuat kebijakan, akun anggota di VPC tidak dapat mengganti pengaturan kebijakan firewall atau grup aturan Anda, tetapi akun tersebut dapat menambahkan grup aturan ke kebijakan firewall yang telah dibuat oleh Manajer Firewall.

Cara Firewall Manager mengelola dan memantau tabel rute VPC untuk kebijakan Anda

> **Note**
>
> Manajemen tabel rute saat ini tidak didukung untuk kebijakan yang menggunakan model penerapan terpusat.

Ketika Firewall Manager membuat endpoint firewall Anda, itu juga membuat tabel rute VPC untuk mereka. Namun, Firewall Manager tidak mengelola tabel rute VPC Anda. Anda harus mengonfigurasi

tabel rute VPC Anda untuk mengarahkan lalu lintas jaringan ke titik akhir firewall yang dibuat oleh Firewall Manager. Menggunakan penyempurnaan perutean masuk Amazon VPC, ubah tabel perutean Anda untuk merutekan lalu lintas melalui titik akhir firewall baru. Perubahan Anda harus menyisipkan titik akhir firewall di antara subnet yang ingin Anda lindungi dan lokasi luar. Perutean yang tepat yang perlu Anda lakukan tergantung pada arsitektur Anda dan komponennya.

Saat ini, Firewall Manager memungkinkan pemantauan rute tabel rute VPC Anda untuk setiap lalu lintas yang ditujukan ke gateway internet, yang melewati firewall. Firewall Manager tidak mendukung gateway target lain seperti gateway NAT.

Untuk informasi tentang mengelola tabel rute untuk VPC Anda, lihat Mengelola tabel rute untuk VPC Anda di Panduan Pengguna Amazon Virtual Private Cloud. Untuk informasi tentang mengelola tabel rute untuk Network Firewall, lihat Konfigurasi tabel rute untuk AWS Network Firewall Panduan AWS Network Firewall Pengembang.

Saat Anda mengaktifkan pemantauan kebijakan, Firewall Manager terus memantau konfigurasi rute VPC dan memberi tahu Anda tentang lalu lintas yang melewati pemeriksaan firewall untuk VPC tersebut. Jika subnet memiliki rute endpoint firewall, Firewall Manager mencari rute berikut:

- Rute untuk mengirim lalu lintas ke titik akhir Network Firewall.
- Rute untuk meneruskan lalu lintas dari titik akhir Network Firewall ke gateway internet.
- Rute masuk dari gateway internet ke titik akhir Network Firewall.
- Rute dari subnet firewall.

Jika subnet memiliki rute Network Firewall tetapi ada routing asimetris di Network Firewall dan tabel rute gateway internet Anda, Firewall Manager melaporkan subnet sebagai tidak sesuai. Firewall Manager juga mendeteksi rute ke gateway internet di tabel rute firewall yang dibuat oleh Firewall Manager, serta tabel rute untuk subnet Anda, dan melaporkannya sebagai tidak sesuai. Rute tambahan dalam tabel rute subnet Network Firewall dan tabel rute gateway internet Anda juga dilaporkan sebagai tidak sesuai. Bergantung pada jenis pelanggaran, Firewall Manager menyarankan tindakan remediasi untuk membawa konfigurasi rute ke kepatuhan. Firewall Manager tidak menawarkan saran dalam semua kasus. Misalnya, jika subnet pelanggan Anda memiliki titik akhir firewall yang dibuat di luar Firewall Manager, Firewall Manager tidak menyarankan tindakan remediasi.

Secara default, Firewall Manager akan menandai setiap lalu lintas yang melintasi batas Availability Zone untuk inspeksi sebagai tidak sesuai. Namun, jika Anda memilih untuk secara otomatis membuat

satu titik akhir di VPC Anda, Firewall Manager tidak akan menandai lalu lintas yang melintasi batas Availability Zone sebagai tidak sesuai.

Untuk kebijakan yang menggunakan model penerapan terdistribusi dengan konfigurasi titik akhir kustom, Anda dapat memilih apakah lalu lintas yang melintasi batas Availability Zone dari Availability Zone tanpa titik akhir firewall ditandai sebagai sesuai atau tidak sesuai.

> **Note**
>
> - Firewall Manager tidak menyarankan tindakan remediasi untuk rute non-IPv4, seperti IPv6 dan rute daftar awalan.
> - Panggilan yang dilakukan menggunakan panggilan `DisassociateRouteTable` API dapat memakan waktu hingga 12 jam untuk mendeteksi.
> - Firewall Manager membuat tabel rute Network Firewall untuk subnet yang berisi titik akhir firewall. Firewall Manager mengasumsikan bahwa tabel rute ini hanya berisi gateway internet yang valid dan rute default VPC. Setiap rute tambahan atau tidak valid dalam tabel rute ini dianggap tidak sesuai.

Ketika Anda mengonfigurasi kebijakan Firewall Manager, jika Anda memilih mode Monitor, Firewall Manager memberikan rincian pelanggaran dan remediasi sumber daya tentang sumber daya Anda. Anda dapat menggunakan tindakan remediasi yang disarankan ini untuk memperbaiki masalah rute di tabel rute Anda. Jika Anda memilih mode Off, Firewall Manager tidak memantau konten tabel rute untuk Anda. Dengan opsi ini, Anda mengelola sendiri tabel rute VPC Anda. Untuk informasi selengkapnya tentang pelanggaran sumber daya ini, lihat[Melihat informasi kepatuhan untuk suatu AWS Firewall Manager kebijakan](#).

> **Warning**
>
> Jika Anda memilih Monitor di bawah konfigurasi AWS Network Firewall rute saat membuat kebijakan, Anda tidak dapat menonaktifkannya untuk kebijakan tersebut. Namun, jika Anda memilih Off, Anda dapat mengaktifkannya nanti.

Mengonfigurasi pencatatan untuk kebijakan AWS Network Firewall

Anda dapat mengaktifkan pencatatan terpusat untuk kebijakan Network Firewall Anda untuk mendapatkan informasi terperinci tentang lalu lintas dalam organisasi Anda. Anda dapat memilih

pencatatan aliran untuk menangkap arus lalu lintas jaringan, atau pencatatan peringatan untuk melaporkan lalu lintas yang cocok dengan aturan dengan tindakan aturan yang disetel ke `DROP` atau`ALERT`. Untuk informasi selengkapnya tentang AWS Network Firewall pencatatan, lihat Mencatat lalu lintas jaringan dari AWS Network Firewall Panduan AWS Network Firewall Pengembang.

Anda mengirim log dari firewall Network Firewall kebijakan Anda ke bucket Amazon S3. Setelah Anda mengaktifkan logging, AWS Network Firewall kirimkan log untuk setiap Network Firewall yang dikonfigurasi dengan memperbarui pengaturan firewall untuk mengirimkan log ke bucket Amazon S3 pilihan Anda dengan awalan cadangan, AWS Firewall Manager . `<policy-name>-<policy-id>`

> **Note**
>
> Awalan ini digunakan oleh Firewall Manager untuk menentukan apakah konfigurasi logging ditambahkan oleh Firewall Manager, atau apakah itu ditambahkan oleh pemilik akun. Jika pemilik akun mencoba menggunakan awalan cadangan untuk pencatatan kustom mereka sendiri, itu akan ditimpa oleh konfigurasi logging dalam kebijakan Firewall Manager.

Untuk informasi selengkapnya tentang cara membuat bucket Amazon S3 dan meninjau log yang disimpan, lihat Apa itu Amazon S3? di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Untuk mengaktifkan pencatatan, Anda harus memenuhi persyaratan berikut:

- Amazon S3 yang Anda tentukan dalam kebijakan Firewall Manager harus ada.
- Anda harus memiliki izin berikut:
  - `logs:CreateLogDelivery`
  - `s3:GetBucketPolicy`
  - `s3:PutBucketPolicy`
- Jika bucket Amazon S3 yang merupakan tujuan pencatatan Anda menggunakan enkripsi sisi server dengan kunci yang disimpan AWS Key Management Service, Anda harus menambahkan kebijakan berikut ke AWS KMS kunci yang dikelola pelanggan agar Firewall Manager masuk ke grup log Log Anda: CloudWatch

```
{
    "Effect": "Allow",
    "Principal": {
```

```
        "Service": "delivery.logs.amazonaws.com"
    },
    "Action": [
        "kms:Encrypt*",
        "kms:Decrypt*",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:Describe*"
    ],
    "Resource": "*"
}
```

Perhatikan bahwa hanya bucket di akun administrator Firewall Manager yang dapat digunakan untuk logging AWS Network Firewall pusat.

Saat Anda mengaktifkan logging terpusat pada kebijakan Network Firewall, Firewall Manager mengambil tindakan ini di akun Anda:

- Firewall Manager memperbarui izin pada bucket S3 yang dipilih untuk memungkinkan pengiriman log.
- Firewall Manager membuat direktori di bucket S3 untuk setiap akun anggota dalam lingkup kebijakan. Log untuk setiap akun dapat ditemukan di`<bucket-name>/<policy-name>-<policy-id>/AWSLogs/<account-id>`.

Untuk mengaktifkan logging untuk kebijakan Network Firewall

1. Buat bucket Amazon S3 menggunakan akun administrator Firewall Manager Anda. Untuk informasi selengkapnya, lihat Membuat bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.
2. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

> **Note**
>
> Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

3. Di panel navigasi, pilih Kebijakan Keamanan.
4. Pilih kebijakan Network Firewall yang ingin Anda aktifkan untuk login. Untuk informasi selengkapnya tentang AWS Network Firewall pencatatan, lihat Mencatat lalu lintas jaringan dari AWS Network Firewall Panduan AWS Network Firewall Pengembang.
5. Pada tab Detail kebijakan, di bagian Aturan kebijakan, pilih Edit.
6. Untuk mengaktifkan dan menggabungkan log, pilih satu atau beberapa opsi di bawah konfigurasi Logging:
   - Aktifkan dan agregat log aliran
   - Aktifkan dan agregat log peringatan
7. Pilih bucket Amazon S3 tempat Anda ingin log Anda dikirimkan. Anda harus memilih bucket untuk setiap jenis log yang Anda aktifkan. Anda dapat menggunakan bucket yang sama untuk kedua jenis log.
8. (Opsional) Jika Anda ingin pencatatan yang dibuat akun anggota khusus diganti dengan konfigurasi logging kebijakan, pilih Ganti konfigurasi logging yang ada.
9. Pilih Selanjutnya.
10. Tinjau pengaturan Anda, lalu pilih Simpan untuk menyimpan perubahan pada kebijakan.

Untuk menonaktifkan logging untuk kebijakan Network Firewall

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

   > **Note**
   >
   > Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

2. Di panel navigasi, pilih Kebijakan Keamanan.
3. Pilih kebijakan Network Firewall yang ingin Anda nonaktifkan logging.
4. Pada tab Detail kebijakan, di bagian Aturan kebijakan, pilih Edit.
5. Di bawah Status konfigurasi Logging, batalkan pilihan Aktifkan dan agregat log aliran serta Aktifkan dan agregat log peringatan jika dipilih.

6. Pilih Selanjutnya.
7. Tinjau pengaturan Anda, lalu pilih Simpan untuk menyimpan perubahan pada kebijakan.

Kebijakan Firewall DNS Resolver Amazon Route 53

Anda dapat menggunakan kebijakan AWS Firewall Manager DNS Firewall untuk mengelola asosiasi antara grup aturan Amazon Route 53 Resolver DNS Firewall dan VPC Amazon Virtual Private Cloud di seluruh organisasi Anda. AWS Organizations Anda dapat menerapkan grup aturan yang dikontrol secara terpusat ke seluruh organisasi, atau ke subset tertentu dari akun dan VPC Anda.

DNS Firewall menyediakan penyaringan dan pengaturan lalu lintas DNS keluar untuk VPC Anda. Anda membuat koleksi aturan pemfilteran yang dapat digunakan kembali di grup aturan DNS Firewall dan Anda mengaitkan grup aturan ke VPC Anda. Saat menerapkan kebijakan Firewall Manager, untuk setiap akun dan VPC yang berada dalam cakupan kebijakan, Firewall Manager membuat asosiasi antara setiap grup aturan DNS Firewall dalam kebijakan dan setiap VPC yang berada dalam cakupan kebijakan, menggunakan pengaturan prioritas asosiasi yang Anda tentukan dalam kebijakan Manajer Firewall.

Untuk informasi tentang menggunakan DNS Firewall, lihat Amazon Route 53 Resolver DNS Firewall di Panduan Pengembang Amazon Route 53.

Bagian berikut mencakup persyaratan untuk menggunakan kebijakan Firewall Manager DNS Firewall dan menjelaskan cara kerja kebijakan. Untuk prosedur pembuatan kebijakan, lihatMembuat AWS Firewall Manager kebijakan untuk Amazon Route 53 Resolver DNS Firewall.

Anda harus mengaktifkan berbagi sumber daya

Kebijakan DNS Firewall membagikan grup aturan DNS Firewall di seluruh akun di organisasi Anda. Agar ini berfungsi, Anda harus mengaktifkan berbagi sumber daya AWS Organizations. Untuk informasi tentang cara mengaktifkan berbagi sumber daya, lihatBerbagi sumber daya untuk kebijakan Network Firewall dan DNS Firewall.

Anda harus memiliki grup aturan DNS Firewall yang ditentukan

Saat menentukan kebijakan DNS Firewall baru, Anda menentukan grup aturan sama seperti yang Anda lakukan saat menggunakan Amazon Route 53 Resolver DNS Firewall secara langsung. Grup aturan Anda harus sudah ada di akun administrator Manajer Firewall agar Anda dapat memasukkannya ke dalam kebijakan. Untuk informasi tentang membuat grup aturan DNS Firewall, lihat Grup dan aturan DNS Firewall.

Anda menentukan asosiasi kelompok aturan prioritas terendah dan tertinggi

Asosiasi grup aturan DNS Firewall yang Anda kelola melalui kebijakan Firewall Manager DNS Firewall berisi asosiasi prioritas terendah dan asosiasi prioritas tertinggi untuk VPC Anda. Dalam konfigurasi kebijakan Anda, ini muncul sebagai grup aturan pertama dan terakhir.

DNS Firewall memfilter lalu lintas DNS untuk VPC dengan urutan sebagai berikut:

1. Grup aturan pertama, yang ditentukan oleh Anda dalam kebijakan Firewall Manager DNS Firewall. Nilai yang valid adalah antara 1 dan 99.
2. Grup aturan DNS Firewall yang dikaitkan oleh manajer akun individu melalui DNS Firewall.
3. Grup aturan terakhir, yang ditentukan oleh Anda dalam kebijakan Firewall Manager DNS Firewall. Nilai yang valid adalah antara 9.901 dan 10.000.

Menghapus grup aturann

Untuk menghapus grup aturan dari kebijakan Firewall Manager DNS Firewall, Anda harus melakukan langkah-langkah berikut:

1. Hapus grup aturan dari kebijakan Firewall Manager DNS Firewall Anda.
2. Hapus berbagi grup aturan di AWS Resource Access Manager. Untuk membatalkan pembagian grup aturan yang Anda miliki, Anda harus menghapusnya dari pembagian sumber daya. Anda dapat melakukan ini menggunakan AWS RAM konsol atau AWS CLI. Untuk informasi tentang membatalkan pembagian sumber daya, lihat Memperbarui bagian sumber daya AWS RAM di Panduan AWS RAM Pengguna.
3. Hapus grup aturan menggunakan konsol DNS Firewall atau AWS CLI.

Bagaimana Firewall Manager memberi nama asosiasi grup aturan yang dibuatnya

Saat Anda menyimpan kebijakan DNS Firewall, jika Anda mengaktifkan autoremediation, Firewall Manager akan membuat asosiasi DNS Firewall antara grup aturan yang Anda berikan dalam kebijakan dan VPC yang berada dalam cakupan kebijakan. Firewall Manager menamai asosiasi ini dengan menggabungkan nilai-nilai berikut:

- String tetap,`FMManaged_`.
- ID kebijakan Manajer Firewall. Ini adalah ID AWS sumber daya untuk kebijakan Firewall Manager.

Berikut ini menunjukkan contoh nama untuk firewall yang dikelola oleh Firewall Manager:

```
FMManaged_EXAMPLEDNSFirewallPolicyId
```

Setelah Anda membuat kebijakan, jika pemilik akun di VPC mengganti pengaturan kebijakan firewall atau asosiasi grup aturan Anda, maka Firewall Manager akan menandai kebijakan tersebut sebagai tidak patuh dan mencoba mengusulkan tindakan perbaikan. Pemilik akun dapat mengaitkan grup aturan DNS Firewall lainnya ke VPC yang berada dalam lingkup kebijakan DNS Firewall. Setiap asosiasi yang dibuat oleh pemilik akun individu harus memiliki pengaturan prioritas antara asosiasi grup aturan pertama dan terakhir Anda.

Kebijakan Palo Alto Networks Cloud NGFW

Palo Alto Networks Cloud Next Generation Firewall (NGFW) adalah layanan firewall pihak ketiga yang dapat Anda gunakan untuk kebijakan Anda. AWS Firewall Manager Dengan Palo Alto Networks Cloud NGFW for Firewall Manager, Anda dapat membuat dan menyebarkan sumber daya dan aturan Palo Alto Networks Cloud NGFW secara terpusat di semua akun Anda. AWS

Untuk menggunakan Palo Alto Networks Cloud NGFW dengan Firewall Manager, pertama-tama Anda berlangganan layanan Palo Alto Networks Cloud NGFW Pay-As-You-Go di Marketplace. AWS Setelah berlangganan, Anda melakukan serangkaian langkah di layanan Palo Alto Networks Cloud NGFW untuk mengonfigurasi akun Anda dan pengaturan Cloud NGFW. Kemudian, Anda membuat kebijakan Firewall Manager Cloud FMS untuk menyebarkan dan mengelola sumber daya dan aturan Palo Alto Networks Cloud NGFW secara terpusat di semua akun di Organizations Anda. AWS

Untuk prosedur pembuatan kebijakan Firewall Manager, lihatMembuat AWS Firewall Manager kebijakan untuk Palo Alto Networks Cloud NGFW. Untuk informasi tentang cara mengkonfigurasi dan mengelola Palo Alto Networks Cloud NGFW untuk Firewall Manager, lihat Palo Alto Networks Palo Alto Networks Cloud NGFW pada dokumentasi. AWS

Fortigate Cloud Native Firewall (CNF) sebagai kebijakan Layanan

Fortigate Cloud Native Firewall (CNF) sebagai Layanan adalah layanan firewall pihak ketiga yang dapat Anda gunakan untuk kebijakan Anda. AWS Firewall Manager Fortigate CNF adalah layanan firewall generasi berikutnya yang memudahkan Anda untuk melindungi jaringan cloud Anda dan mengelola kebijakan keamanan Anda. Dengan Fortigate CNF for Firewall Manager, Anda dapat membuat dan menyebarkan sumber daya dan kumpulan kebijakan Fortigate CNF secara terpusat di semua akun Anda. AWS

Untuk menggunakan Fortigate CNF dengan Firewall Manager, pertama-tama Anda berlangganan Fortigate Cloud Native Firewall (CNF) sebagai Layanan di Marketplace. AWS Setelah berlangganan, Anda melakukan serangkaian langkah di layanan Fortigate CNF untuk mengonfigurasi kumpulan kebijakan global Anda dan pengaturan lainnya. Kemudian, Anda membuat kebijakan Firewall Manager untuk menyebarkan dan mengelola sumber daya CNF Fortigate secara terpusat di semua akun di Organizations Anda. AWS

Untuk prosedur pembuatan kebijakan Fortigate CNF Firewall Manager, lihat. Membuat AWS Firewall Manager kebijakan untuk Fortigate Cloud Native Firewall (CNF) sebagai Layanan Untuk informasi tentang cara mengkonfigurasi dan mengelola Fortigate CNF untuk digunakan dengan Firewall Manager, lihat dokumentasi Fortigate CNF.

Berbagi sumber daya untuk kebijakan Network Firewall dan DNS Firewall

Untuk mengelola kebijakan Firewall Manager Network Firewall dan DNS Firewall, Anda harus mengaktifkan berbagi sumber daya dengan AWS Organizations in AWS Resource Access Manager. Ini memungkinkan Firewall Manager untuk menerapkan perlindungan di seluruh akun Anda saat Anda membuat jenis kebijakan ini.

Untuk mengaktifkan berbagi sumber daya, ikuti petunjuk di Aktifkan Berbagi dengan AWS Organizations di Panduan AWS Resource Access Manager Pengguna.

Masalah dengan berbagi sumber daya

Anda mungkin mengalami masalah dengan berbagi sumber daya, baik saat Anda menggunakannya AWS RAM untuk mengaktifkannya, atau saat Anda mengerjakan kebijakan Firewall Manager yang memerlukannya.

Contoh masalah ini meliputi:

- Saat Anda mengikuti petunjuk untuk mengaktifkan berbagi, di AWS RAM konsol, pilihan Aktifkan berbagi dengan AWS Organizations berwarna abu-abu dan tidak tersedia untuk dipilih.
- Saat Anda bekerja di Firewall Manager pada kebijakan yang memerlukan pembagian sumber daya, kebijakan tersebut ditandai sebagai tidak sesuai dan Anda melihat pesan yang menunjukkan bahwa berbagi sumber daya atau AWS RAM tidak diaktifkan.

Jika Anda mengalami masalah dengan berbagi sumber daya, gunakan prosedur berikut untuk mencoba mengaktifkannya.

Coba lagi untuk mengaktifkan berbagi sumber daya

- Coba lagi untuk mengaktifkan berbagi menggunakan salah satu opsi berikut:
  - (Opsi) Melalui AWS RAM konsol, ikuti petunjuk di Aktifkan Berbagi dengan AWS Organizations di Panduan AWS Resource Access Manager Pengguna.
  - (Opsi) Menggunakan AWS RAM API, panggil`EnableSharingWithAwsOrganization`. Lihat dokumentasi di EnableSharingWithAwsOrganization.

Bekerja dengan kumpulan sumber daya di Firewall Manager

Kumpulan AWS Firewall Manager sumber daya adalah kumpulan sumber daya, seperti firewall, yang dapat Anda kelompokkan bersama dan kelola dalam kebijakan Firewall Manager. Kumpulan sumber daya memungkinkan anggota di organisasi Anda memiliki kontrol terperinci atas sumber daya apa yang harus dikelola dalam kebijakan. Untuk menggunakan kumpulan sumber daya, buat set sumber daya di konsol atau menggunakan PutResourceSetAPI, lalu tambahkan set sumber daya ke kebijakan Firewall Manager Anda.

Anda dapat membuat dan mengelola kumpulan sumber daya untuk jenis kebijakan sumber daya dan keamanan berikut:

Jenis sumber daya	Jenis kebijakan keamanan Firewall Manager
AWS Network Firewall - firewall	Kebijakan Network Firewall - Gunakan kumpulan sumber daya untuk mengimpor firewall yang ada dari Network Firewall. Untuk informasi tentang penggunaan kumpulan sumber daya dalam kebijakan Network Firewall, lihat langkah Mengimpor firewall yang ada dalam prosedurMembuat AWS Firewall Manager kebijakan untuk AWS Network Firewall.

Bagian berikut mencakup persyaratan untuk membuat dan menghapus kumpulan sumber daya.

Topik

- Pertimbangan saat bekerja dengan set sumber daya di Firewall Manager
- Membuat set sumber daya
- Menghapus kumpulan sumber daya

Pertimbangan saat bekerja dengan set sumber daya di Firewall Manager

Perhatikan pertimbangan berikut saat bekerja dengan kumpulan sumber daya

Referensi ke sumber daya yang tidak ada

Saat menambahkan sumber daya ke kumpulan sumber daya, Anda membuat referensi ke sumber daya menggunakan Amazon Resource Name (ARN). Firewall Manager memvalidasi bahwa Amazon Resource Name (ARN) adalah format yang benar, tetapi Firewall Manager tidak memeriksa apakah sumber daya yang direferensikan ada. Jika sumber daya belum ada melewati validasi ARN, Firewall Manager menyertakan referensi sumber daya dalam kumpulan sumber daya. Jika sumber daya baru dengan ARN yang sama kemudian dibuat, Firewall Manager menerapkan grup aturan dari kebijakan terkait kumpulan sumber daya ke sumber daya baru.

Sumber daya yang dihapus

Ketika sumber daya dalam kumpulan sumber daya dihapus, referensi ke sumber daya tetap berada di set sumber daya hingga dihapus oleh administrator Manajer Firewall.

Sumber daya yang dimiliki oleh akun anggota yang meninggalkan AWS Organizations organisasi

Jika akun anggota meninggalkan organisasi, referensi apa pun ke sumber daya yang dimiliki oleh akun anggota tersebut akan tetap berada dalam kumpulan sumber daya tetapi tidak akan lagi dikelola oleh kebijakan apa pun yang terkait dengan kumpulan sumber daya tersebut.

Asosiasi dengan berbagai kebijakan

Kumpulan sumber daya dapat dikaitkan dengan beberapa kebijakan, tetapi tidak semua jenis kebijakan mendukung beberapa kebijakan yang mengelola sumber daya yang sama. Lihat dokumentasi untuk jenis kebijakan spesifik Anda untuk informasi tentang skenario yang tidak didukung.

Membuat set sumber daya

Untuk membuat kumpulan sumber daya (konsol)

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

   > **Note**
   >
   > Untuk informasi tentang menyiapkan akun administrator Firewall Manager, lihatAWS Firewall Manager prasyarat.

2. Di panel navigasi, pilih Set sumber daya.

3. Pilih Buat kumpulan sumber daya.
4. Untuk nama set Sumber Daya, masukkan nama deskriptif.
5. (Opsional) masukkan Deskripsi untuk kumpulan sumber daya.
6. Pilih Berikutnya.
7. Untuk Pilih sumber daya, pilih ID AWS akun lalu pilih Pilih sumber daya untuk menambahkan sumber daya yang dimiliki dan dikelola oleh akun ini ke kumpulan sumber daya. Setelah Anda memilih sumber daya, pilih Tambah untuk menambahkan sumber daya ke kumpulan sumber daya.
8. Pilih Berikutnya.
9. Untuk tag set Sumber Daya, tambahkan tag pengenal apa pun yang Anda inginkan untuk kumpulan sumber daya. Untuk informasi selengkapnya tentang tag, lihat Bekerja dengan Editor Tag.
10. Pilih Berikutnya.
11. Tinjau kumpulan sumber daya baru. Untuk membuat perubahan, pilih Edit di area yang ingin Anda ubah. Ini mengembalikan Anda ke langkah yang sesuai di wizard pembuatan. Bila Anda puas dengan kumpulan sumber daya, pilih Buat kumpulan sumber daya.

Menghapus kumpulan sumber daya

Sebelum Anda dapat menghapus kumpulan sumber daya, kumpulan sumber daya harus dipisahkan dari semua kebijakan menggunakan kumpulan sumber daya. Anda dapat memisahkan grup sumber daya di halaman detail kebijakan menggunakan konsol, atau dengan PutPolicyAPI.

Untuk menghapus kumpulan sumber daya (konsol)

1. Di panel navigasi, pilih Set sumber daya.
2. Pilih opsi di sebelah kumpulan sumber daya yang ingin Anda hapus.
3. Pilih Hapus.

Melihat informasi kepatuhan untuk suatu AWS Firewall Manager kebijakan

Bagian ini memberikan panduan untuk melihat status kepatuhan akun dan sumber daya yang berada dalam cakupan AWS Firewall Manager kebijakan. Untuk informasi tentang kontrol yang

diterapkan AWS untuk menjaga keamanan dan kepatuhan cloud, lihatValidasi kepatuhan untuk Firewall Manager.

> **Note**
>
> Agar Firewall Manager memantau kepatuhan kebijakan, AWS Config harus terus mencatat perubahan konfigurasi untuk sumber daya yang dilindungi. Dalam AWS Config konfigurasi Anda, frekuensi perekaman harus diatur ke Continuous, yang merupakan pengaturan default.

> **Note**
>
> Untuk mempertahankan status kepatuhan yang tepat dalam sumber daya yang dilindungi, hindari berulang kali mengubah status perlindungan Firewall Manager, baik secara otomatis maupun manual. Firewall Manager menggunakan informasi dari AWS Config untuk mendeteksi perubahan konfigurasi sumber daya. Jika perubahan diterapkan cukup cepat, AWS Config dapat kehilangan jejak beberapa dari mereka, yang dapat mengakibatkan hilangnya informasi tentang kepatuhan atau remediasi status di Firewall Manager.
> Jika Anda melihat bahwa sumber daya yang Anda lindungi dengan Firewall Manager memiliki status kepatuhan atau remediasi yang salah, pertama-tama pastikan Anda tidak menjalankan proses apa pun yang mengubah atau mengatur ulang perlindungan Firewall Manager Anda, lalu segarkan AWS Config pelacakan untuk sumber daya dengan mengevaluasi kembali aturan konfigurasi terkait di. AWS Config

Untuk semua AWS Firewall Manager kebijakan, Anda dapat melihat status kepatuhan untuk akun dan sumber daya yang berada dalam cakupan kebijakan. Akun atau sumber daya sesuai dengan kebijakan Firewall Manager jika pengaturan dalam kebijakan tercermin dalam pengaturan untuk akun atau sumber daya. Setiap jenis kebijakan memiliki persyaratan kepatuhannya sendiri, yang dapat Anda sesuaikan saat menentukan kebijakan. Untuk beberapa kebijakan, Anda juga dapat melihat informasi pelanggaran terperinci untuk sumber daya dalam lingkup, untuk membantu Anda memahami dan mengelola risiko keamanan dengan lebih baik.

Untuk melihat informasi kepatuhan untuk suatu kebijakan

1. Masuk ke akun administrator AWS Management Console menggunakan Firewall Manager Anda, lalu buka konsol Firewall Manager dihttps://console.aws.amazon.com/wafv2/fmsv2. Untuk

informasi tentang menyiapkan akun administrator Manajer Firewall, lihatAWS Firewall Manager prasyarat.

> **Note**
>
> Untuk informasi tentang menyiapkan akun administrator Manajer Firewall, lihatAWS Firewall Manager prasyarat.

2. Di panel navigasi, pilih Kebijakan keamanan.
3. Pilih kebijakan. Di tab Akun dan sumber daya pada halaman kebijakan, Firewall Manager mencantumkan akun di organisasi Anda, dikelompokkan berdasarkan akun yang berada dalam cakupan kebijakan dan akun yang berada di luar cakupan.

   Panel Akun dalam cakupan kebijakan mencantumkan status kepatuhan untuk setiap akun. Status Compliant menunjukkan bahwa kebijakan telah berhasil diterapkan ke semua sumber daya dalam lingkup untuk akun. Status Noncompliant menunjukkan bahwa kebijakan belum diterapkan ke satu atau beberapa sumber daya dalam cakupan untuk akun tersebut.
4. Pilih akun yang tidak patuh. Di halaman akun, Firewall Manager mencantumkan ID dan jenis untuk setiap sumber daya yang tidak sesuai dan alasan sumber daya tersebut melanggar kebijakan.

   > **Note**
   >
   > Untuk tipe sumber daya `AWS::EC2::NetworkInterface` (ENI) dan`AWS::EC2::Instance`, Firewall Manager mungkin menampilkan sejumlah sumber daya yang tidak sesuai. Untuk mencantumkan sumber daya tambahan yang tidak sesuai, perbaiki sumber daya yang awalnya ditampilkan untuk akun.
5. Jika jenis kebijakan Firewall Manager adalah kebijakan grup keamanan audit konten, Anda dapat mengakses informasi pelanggaran terperinci untuk sumber daya.

   Untuk melihat detail pelanggaran, pilih sumber daya.

   > **Note**
   >
   > Sumber daya yang menurut Firewall Manager tidak sesuai sebelum penambahan halaman pelanggaran sumber daya terperinci mungkin tidak memiliki detail pelanggaran.

Di halaman sumber daya, Firewall Manager mencantumkan detail spesifik tentang pelanggaran, sesuai dengan jenis sumber daya.

- **`AWS::EC2::NetworkInterface`**(ENI) — Firewall Manager menampilkan informasi tentang grup keamanan yang tidak dipatuhi oleh sumber daya. Pilih grup keamanan untuk melihat detail lebih lanjut tentangnya.
- **`AWS::EC2::Instance`**— Firewall Manager menampilkan ENI yang terpasang pada instans EC2 yang tidak sesuai. Ini juga menampilkan informasi tentang grup keamanan yang tidak dipatuhi oleh sumber daya. Pilih grup keamanan untuk melihat detail lebih lanjut tentangnya.
- **`AWS::EC2::SecurityGroup`**— Firewall Manager menampilkan rincian pelanggaran berikut:
  - Aturan grup keamanan yang tidak sesuai — Aturan yang melanggar, termasuk protokol, jangkauan port, rentang IP CIDR, dan deskripsi.
  - Aturan yang direferensikan — Aturan grup keamanan audit yang melanggar aturan kelompok keamanan yang tidak patuh, dengan detailnya.
  - Alasan pelanggaran — Penjelasan tentang temuan ketidakpatuhan.
  - Tindakan remediasi — Tindakan yang disarankan untuk diambil. Jika Firewall Manager tidak dapat menentukan tindakan remediasi yang aman, bidang ini kosong.
- **`AWS::EC2::Subnet`**— Ini digunakan untuk kebijakan ACL jaringan dan Network Firewall.

  Firewall Manager menampilkan subnet ID, VPC ID, dan Availability Zone. Jika berlaku, Firewall Manager menyertakan informasi tambahan tentang pelanggaran. Komponen deskripsi pelanggaran berisi deskripsi tentang keadaan sumber daya yang diharapkan, keadaan saat ini, tidak patuh, dan jika tersedia, deskripsi tentang apa yang menyebabkan perbedaan tersebut.

  Pelanggaran Network Firewall

  - Pelanggaran manajemen rute — Untuk kebijakan Network Firewall yang menggunakan mode Monitor, Firewall Manager menampilkan informasi subnet dasar, serta rute yang diharapkan dan aktual di subnet, gateway internet, dan tabel rute subnet Network Firewall. Firewall Manager memberi tahu Anda bahwa ada pelanggaran jika rute sebenarnya tidak sesuai dengan rute yang diharapkan dalam tabel rute.
  - Tindakan remediasi untuk pelanggaran manajemen rute — Untuk kebijakan Network Firewall yang menggunakan mode Monitor, Firewall Manager menyarankan kemungkinan tindakan remediasi pada konfigurasi rute yang memiliki pelanggaran.

Misalnya, subnet diharapkan mengirim lalu lintas melalui titik akhir firewall, tetapi subnet saat ini mengirimkan lalu lintas langsung ke gateway internet. Ini adalah pelanggaran manajemen rute. Remediasi yang disarankan dalam kasus ini mungkin merupakan daftar tindakan yang diperintahkan. Yang pertama adalah rekomendasi untuk menambahkan rute yang diperlukan ke tabel rute subnet Network Firewall untuk mengarahkan lalu lintas keluar ke gateway internet dan mengarahkan lalu lintas masuk untuk tujuan di dalam VPC ke. `local` Rekomendasi kedua adalah mengganti rute gateway internet atau rute Network Firewall yang tidak valid di tabel rute subnet untuk mengarahkan lalu lintas keluar ke titik akhir firewall. Rekomendasi ketiga adalah menambahkan rute yang diperlukan ke tabel rute gateway internet untuk mengarahkan lalu lintas masuk ke titik akhir firewall.

- **`AWS::EC2::InternetGateway`**— Ini digunakan untuk kebijakan Network Firewall yang mengaktifkan mode Monitor.
  - Pelanggaran manajemen rute — Gateway internet tidak sesuai jika gateway internet tidak terkait dengan tabel rute, atau jika ada rute yang tidak valid di tabel rute gateway internet.
  - Tindakan remediasi untuk pelanggaran manajemen rute — Firewall Manager menyarankan kemungkinan tindakan remediasi untuk memperbaiki pelanggaran manajemen rute.

  Example 1 — Pelanggaran manajemen rute dan saran remediasi

  Gateway internet tidak terkait dengan tabel rute. Tindakan remediasi yang disarankan mungkin merupakan daftar tindakan yang diperintahkan. Tindakan pertama adalah membuat tabel rute. Tindakan kedua adalah mengaitkan tabel rute dengan gateway internet. Tindakan ketiga adalah menambahkan rute yang diperlukan ke tabel rute gateway internet.

  Example 2 — Pelanggaran manajemen rute dan saran remediasi

  Gateway internet dikaitkan dengan tabel rute yang valid, tetapi rute dikonfigurasi dengan tidak benar. Remediasi yang disarankan mungkin merupakan daftar tindakan yang diperintahkan. Saran pertama adalah menghapus rute yang tidak valid. Yang kedua adalah menambahkan rute yang diperlukan ke tabel rute gateway internet.
- **`AWS::NetworkFirewall::FirewallPolicy`**— Ini digunakan untuk kebijakan Network Firewall. Firewall Manager menampilkan informasi tentang kebijakan firewall Network Firewall yang telah dimodifikasi dengan cara yang membuatnya tidak patuh. Informasi tersebut menyediakan kebijakan firewall yang diharapkan dan kebijakan yang ditemukan di akun pelanggan, sehingga Anda dapat membandingkan nama grup aturan stateless dan stateful dan pengaturan prioritas, nama tindakan kustom, dan pengaturan tindakan stateless default.

Komponen deskripsi pelanggaran berisi deskripsi tentang keadaan sumber daya yang diharapkan, keadaan saat ini, tidak patuh, dan jika tersedia, deskripsi tentang apa yang menyebabkan perbedaan tersebut.

- **`AWS::EC2::VPC`**— Ini digunakan untuk kebijakan DNS Firewall. Firewall Manager menampilkan informasi tentang VPC yang berada dalam lingkup kebijakan Firewall Manager DNS Firewall, dan itu tidak sesuai dengan kebijakan tersebut. Informasi yang diberikan mencakup kelompok aturan yang diharapkan yang diharapkan terkait dengan VPC dan kelompok aturan yang sebenarnya. Komponen deskripsi pelanggaran berisi deskripsi tentang keadaan sumber daya yang diharapkan, keadaan saat ini, tidak patuh, dan jika tersedia, deskripsi tentang apa yang menyebabkan perbedaan tersebut.

AWS Firewall Manager temuan

AWS Firewall Manager menciptakan temuan untuk sumber daya yang tidak sesuai dan untuk serangan yang dideteksinya, dan mengirimkannya ke AWS Security Hub. Untuk informasi tentang temuan Security Hub, lihat Temuan di AWS Security Hub.

Saat Anda menggunakan Security Hub dan Firewall Manager, Firewall Manager secara otomatis mengirimkan temuan Anda ke Security Hub. Untuk informasi tentang memulai Security Hub, lihat Menyiapkan AWS Security Hub di Panduan AWS Security Hub Pengguna.

> **Note**
>
> Firewall Manager hanya memperbarui temuan untuk kebijakan yang berada di bawah pengelolaannya dan sumber daya yang dipantau.
> Firewall Manager tidak menyelesaikan temuan untuk hal berikut:
>
> - Kebijakan yang telah dihapus.
> - Sumber daya yang telah dihapus.
> - Sumber daya yang telah keluar dari cakupan kebijakan Firewall Manager, misalnya karena perubahan tag atau perubahan definisi kebijakan.

Bagaimana cara melihat temuan Firewall Manager saya?

Untuk melihat temuan Firewall Manager Anda di Security Hub, ikuti panduan di Bekerja dengan Temuan di Security Hub dan buat filter menggunakan setelan berikut:

- Atribut diatur ke Nama Produk.
- Operator diatur ke EQUALS.
- Nilai diatur ke`Firewall Manager`. Pengaturan ini peka huruf besar/kecil.

Bisakah saya menonaktifkan ini?

Anda dapat menonaktifkan integrasi AWS Firewall Manager temuan dengan Security Hub melalui konsol Security Hub. Pilih Integrasi di bilah navigasi, lalu di panel Firewall Manager, pilih Nonaktifkan Integrasi. Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS Security Hub.

AWS Firewall Manager menemukan jenis

- AWS WAF temuan kebijakan
- AWS Shield Advanced temuan kebijakan
- Temuan kebijakan umum kelompok keamanan
- Temuan kebijakan audit konten kelompok keamanan
- Temuan kebijakan audit penggunaan kelompok keamanan
- Temuan kebijakan Amazon Route 53 Resolver DNS Firewall

AWS WAF temuan kebijakan

Anda dapat menggunakan AWS WAF kebijakan Firewall Manager untuk menerapkan grup AWS WAF aturan ke sumber daya Anda AWS Organizations. Untuk informasi selengkapnya, lihat Bekerja dengan AWS Firewall Manager kebijakan.

Sumber daya tidak ada ACL web terkelola Firewall Manager.

AWS Sumber daya tidak memiliki asosiasi ACL web AWS Firewall Manager terkelola sesuai dengan kebijakan Firewall Manager. Anda dapat mengaktifkan remediasi Firewall Manager pada kebijakan untuk memperbaikinya.

- Keparahan - 80
- Pengaturan status - LULUS/GAGAL
- Pembaruan - Jika Firewall Manager melakukan tindakan remediasi, itu akan memperbarui temuan dan tingkat keparahannya akan lebih rendah dari `HIGH` ke`INFORMATIONAL`. Jika Anda melakukan remediasi, Firewall Manager tidak akan memperbarui temuan.

Firewall Manager web yang dikelola ACL memiliki grup aturan yang salah dikonfigurasi.

Grup aturan dalam ACL web yang dikelola oleh Firewall Manager tidak dikonfigurasi dengan benar, sesuai dengan kebijakan Firewall Manager. Ini berarti bahwa ACL web tidak memiliki grup aturan yang diperlukan oleh kebijakan tersebut. Anda dapat mengaktifkan remediasi Firewall Manager pada kebijakan untuk memperbaikinya.

- Keparahan - 80
- Pengaturan status - LULUS/GAGAL
- Pembaruan - Jika Firewall Manager melakukan tindakan remediasi, itu akan memperbarui temuan dan tingkat keparahannya akan lebih rendah dari `HIGH` ke`INFORMATIONAL`. Jika Anda melakukan remediasi, Firewall Manager tidak akan memperbarui temuan.

AWS Shield Advanced temuan kebijakan

Untuk informasi tentang AWS Shield Advanced kebijakan, lihatKebijakan kelompok keamanan.

Sumber daya tidak memiliki perlindungan Shield Advanced.

AWS Sumber daya yang seharusnya memiliki perlindungan Shield Advanced, menurut kebijakan Firewall Manager, tidak memilikinya. Anda dapat mengaktifkan remediasi Firewall Manager pada kebijakan, yang akan memungkinkan perlindungan untuk sumber daya.

- Keparahan - 60
- Pengaturan status - LULUS/GAGAL
- Pembaruan - Jika Firewall Manager melakukan tindakan remediasi, itu akan memperbarui temuan dan tingkat keparahannya akan lebih rendah dari `HIGH` ke`INFORMATIONAL`. Jika Anda melakukan remediasi, Firewall Manager tidak akan memperbarui temuan.

Shield Advanced mendeteksi serangan terhadap sumber daya yang dipantau.

Shield Advanced mendeteksi serangan terhadap AWS sumber daya yang dilindungi. Anda dapat mengaktifkan remediasi Firewall Manager pada kebijakan.

- Keparahan - 70
- Pengaturan status - Tidak ada
- Pembaruan - Firewall Manager tidak memperbarui temuan ini.

Temuan kebijakan umum kelompok keamanan

Untuk informasi tentang kebijakan umum grup keamanan, lihatKebijakan kelompok keamanan.

Sumber daya memiliki grup keamanan yang salah dikonfigurasi.

Firewall Manager telah mengidentifikasi sumber daya yang tidak memiliki asosiasi grup keamanan yang dikelola Manajer Firewall yang seharusnya dimiliki, sesuai dengan kebijakan Firewall Manager. Anda dapat mengaktifkan remediasi Firewall Manager pada kebijakan, yang membuat asosiasi sesuai dengan setelan kebijakan.

- Keparahan - 70
- Pengaturan status - LULUS/GAGAL
- Pembaruan - Firewall Manager memperbarui temuan ini.

Grup keamanan replika Firewall Manager tidak sinkron dengan grup keamanan utama.

Grup keamanan replika Firewall Manager tidak sinkron dengan grup keamanan utamanya, sesuai dengan kebijakan grup keamanan umum mereka. Anda dapat mengaktifkan remediasi Firewall Manager pada kebijakan, yang menyinkronkan grup keamanan replika dengan yang utama.

- Keparahan - 80
- Pengaturan status - LULUS/GAGAL
- Pembaruan - Firewall Manager memperbarui temuan ini.

Temuan kebijakan audit konten kelompok keamanan

Untuk informasi tentang kebijakan audit konten grup keamanan, lihatKebijakan kelompok keamanan.

Grup keamanan tidak sesuai dengan grup keamanan audit konten.

Kebijakan audit konten grup keamanan Firewall Manager telah mengidentifikasi grup keamanan yang tidak patuh. Ini adalah grup keamanan yang dibuat pelanggan yang berada dalam cakupan kebijakan audit konten dan tidak mematuhi pengaturan yang ditentukan oleh kebijakan dan grup keamanan auditnya. Anda dapat mengaktifkan remediasi Firewall Manager pada kebijakan, yang mengubah grup keamanan yang tidak patuh agar sesuai.

- Keparahan - 70

- Pengaturan status - LULUS/GAGAL
- Pembaruan - Firewall Manager memperbarui temuan ini.

Temuan kebijakan audit penggunaan kelompok keamanan

Untuk informasi tentang kebijakan audit penggunaan grup keamanan, lihatKebijakan kelompok keamanan.

Firewall Manager menemukan grup keamanan yang berlebihan.

Audit penggunaan grup keamanan Firewall Manager telah mengidentifikasi grup keamanan yang berlebihan. Ini adalah grup keamanan dengan aturan identik yang ditetapkan sebagai grup keamanan lain dalam instance Amazon Virtual Private Cloud yang sama. Anda dapat mengaktifkan remediasi otomatis Firewall Manager pada kebijakan audit penggunaan, yang menggantikan grup keamanan yang berlebihan dan dengan satu grup keamanan.

- Keparahan — 30
- Pengaturan status - Tidak ada
- Pembaruan — Firewall Manager tidak memperbarui temuan ini.

Firewall Manager menemukan grup keamanan yang tidak digunakan.

Audit penggunaan grup keamanan Firewall Manager telah mengidentifikasi grup keamanan yang tidak digunakan. Ini adalah grup keamanan yang tidak direferensikan oleh kebijakan grup keamanan umum Firewall Manager. Anda dapat mengaktifkan remediasi otomatis Firewall Manager pada kebijakan audit penggunaan, yang menghapus grup keamanan yang tidak digunakan.

- Keparahan — 30
- Pengaturan status - Tidak ada
- Pembaruan — Firewall Manager tidak memperbarui temuan ini.

Temuan kebijakan Amazon Route 53 Resolver DNS Firewall

Untuk informasi tentang kebijakan DNS Firewall, lihatKebijakan Firewall DNS Resolver Amazon Route 53.

Sumber daya tidak memiliki perlindungan DNS Firewall

VPC tidak memiliki asosiasi grup aturan DNS Firewall yang ditentukan dalam kebijakan Firewall Manager DNS Firewall. Temuan ini mencantumkan grup aturan yang ditentukan oleh kebijakan.

- Keparahan - 80

Keamanan dalam penggunaan AWS Firewall Manager layanan Anda

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

> **Note**
>
> Bagian ini memberikan panduan AWS keamanan standar untuk penggunaan Anda atas AWS Firewall Manager layanan dan AWS sumber dayanya, seperti kebijakan Firewall Manager Network Firewall dan kebijakan grup keamanan.
> Untuk informasi tentang melindungi AWS sumber daya Anda menggunakan Firewall Manager, lihat panduan Firewall Manager lainnya.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Efektivitas keamanan kami diuji dan diverifikasi secara rutin oleh auditor pihak ketiga sebagai bagian dari program kepatuhan AWS. Untuk mempelajari tentang program kepatuhan yang berlaku untuk Firewall Manager, lihat AWS Layanan dalam Lingkup berdasarkan Program Kepatuhan.
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor-faktor lain termasuk sensitivitas data Anda, persyaratan organisasi Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Firewall Manager. Topik berikut menunjukkan cara mengonfigurasi Firewall

Manager untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Firewall Manager Anda.

Topik

Perlindungan data di Firewall Manager

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di AWS Firewall Manager. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensyal dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.

- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi yang lebih lengkap tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Firewall Manager atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Entitas Firewall Manager — seperti kebijakan — dienkripsi saat istirahat, kecuali di Wilayah tertentu di mana enkripsi tidak tersedia, termasuk China (Beijing) dan China (Ningxia). Kunci enkripsi unik digunakan untuk setiap Wilayah.

Identity and Access Management untuk AWS Firewall Manager

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Firewall Manager. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- Bagaimana AWS Firewall Manager bekerja dengan IAM
- Contoh kebijakan berbasis identitas untuk AWS Firewall Manager
- AWS kebijakan terkelola untuk AWS Firewall Manager
- Memecahkan masalah AWS Firewall Manager identitas dan akses
- Menggunakan peran terkait layanan untuk Firewall Manager

- Pencegahan confused deputy lintas layanan

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Firewall Manager.

Pengguna layanan — Jika Anda menggunakan layanan Firewall Manager untuk melakukan pekerjaan Anda, administrator Anda memberi Anda kredensyal dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur Firewall Manager untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Firewall Manager, lihatMemecahkan masalah AWS Shield identitas dan akses.

Administrator layanan — Jika Anda bertanggung jawab atas sumber daya Firewall Manager di perusahaan Anda, Anda mungkin memiliki akses penuh ke Firewall Manager. Tugas Anda adalah menentukan fitur dan sumber daya Firewall Manager mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep Basic IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan Firewall Manager, lihatBagaimana AWS Shield bekerja dengan IAM.

Administrator IAM - Jika Anda seorang administrator IAM, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Firewall Manager. Untuk melihat contoh kebijakan berbasis identitas Manajer Firewall yang dapat Anda gunakan di IAM, lihat. Contoh kebijakan berbasis identitas untuk AWS Shield

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensyal identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensyal yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensyal Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensyal Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Menandatangani permintaan AWS API di Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat Autentikasi multi-faktor dalam Panduan Pengguna AWS IAM Identity Center dan Menggunakan autentikasi multi-faktor (MFA) dalam AWS dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensyal sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensi yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensyal sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat Apakah itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup yang bernama IAMAdmins dan memberikan izin ke grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat Kapan harus membuat pengguna IAM (bukan peran) dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil peran IAM untuk sementara AWS Management Console dengan beralih peran. Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat Menggunakan peran IAM dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Sebagai contoh, ketika Anda memanggil suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna IAM atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.
  - Peran layanan – Peran layanan adalah peran IAM yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

  - Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada instans EC2 dan membuat atau permintaan API. AWS CLI AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan dalam instans Amazon EC2 dalam Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, lihat Kapan harus membuat peran IAM (bukan pengguna) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasinya. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan

tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan yang dikelola atau kebijakan inline, lihat Memilih antara kebijakan yang dikelola dan kebijakan inline dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Daftar kontrol akses (ACL)

Daftar kontrol akses (ACL) mengendalikan prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, lihat Gambaran umum daftar kontrol akses (ACL) dalam Panduan Developer Amazon Simple Storage Service.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) — SCP adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur di organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organisasi dan SCP, lihat Cara kerja SCP dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Bagaimana AWS Firewall Manager bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Firewall Manager, pelajari fitur IAM apa yang tersedia untuk digunakan dengan Firewall Manager.

Fitur IAM yang dapat Anda gunakan AWS Firewall Manager

Fitur IAM	Dukungan Firewall Manager
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Tidak
ACL	Tidak
ABAC (tanda dalam kebijakan)	Ya
Kredensial sementara	Ya
Sesi akses teruskan (FAS)	Ya
Peran layanan	Parsial
Peran terkait layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Firewall Manager dan AWS layanan lainnya dengan sebagian besar fitur IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk Firewall Manager

Mendukung kebijakan berbasis identitas	Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Untuk melihat contoh kebijakan berbasis identitas Manajer Firewall, lihat. Contoh kebijakan berbasis identitas untuk AWS Firewall Manager

Contoh kebijakan berbasis identitas untuk Firewall Manager

Untuk melihat contoh kebijakan berbasis identitas Manajer Firewall, lihat. Contoh kebijakan berbasis identitas untuk AWS Firewall Manager

Kebijakan berbasis sumber daya dalam Firewall Manager

Mendukung kebijakan berbasis sumber daya	Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai prinsipal dalam kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan

kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, administrator IAM di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke prinsipal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

Tindakan kebijakan untuk Firewall Manager

Mendukung tindakan kebijakan	Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar tindakan Firewall Manager, lihat Tindakan yang ditentukan oleh AWS Firewall Manager dalam Referensi Otorisasi Layanan.

Tindakan kebijakan di Firewall Manager menggunakan awalan berikut sebelum tindakan:

```
fms
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

```
"Action": [
      "fms:action1",
      "fms:action2"
         ]
```

Anda juga dapat menentukan beberapa tindakan menggunakan wildcard (*). Sebagai contoh, untuk menentukan semua tindakan yang dimulai dengan kata `Describe`, sertakan tindakan berikut:

```
"Action": "fms:Describe*"
```

Untuk melihat contoh kebijakan berbasis identitas Manajer Firewall, lihat. Contoh kebijakan berbasis identitas untuk AWS Firewall Manager

Sumber daya kebijakan untuk Firewall Manager

Mendukung sumber daya kebijakan	Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Untuk melihat daftar jenis sumber daya Firewall Manager dan ARNnya, lihat Sumber daya yang ditentukan oleh AWS Firewall Manager dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan yang dapat menentukan ARN setiap sumber daya, lihat Tindakan yang ditentukan AWS Firewall Manager.

Untuk melihat contoh kebijakan berbasis identitas Manajer Firewall, lihat. Contoh kebijakan berbasis identitas untuk AWS Firewall Manager

Kunci kondisi kebijakan untuk Firewall Manager

Mendukung kunci kondisi kebijakan khusus layanan	Tidak

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi `AND` logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan `OR` operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tag yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, lihat Elemen kebijakan IAM: variabel dan tag dalam Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Untuk melihat daftar kunci kondisi Firewall Manager, lihat Kunci kondisi untuk AWS Firewall Manager Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang ditentukan oleh AWS Firewall Manager.

Untuk melihat contoh kebijakan berbasis identitas Manajer Firewall, lihat. Contoh kebijakan berbasis identitas untuk AWS Firewall Manager

ACL di Firewall Manager

Mendukung ACL	Tidak

Daftar kontrol akses (ACL) mengendalikan pengguna utama mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

ABAC dengan Firewall Manager

Mendukung ABAC (tanda dalam kebijakan)	Ya

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi ketika tag milik prinsipal cocok dengan tag yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi saat manajemen kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tag di elemen kondisi dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Apa itu ABAC? dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) dalam Panduan Pengguna IAM.

Menggunakan kredensyal sementara dengan Firewall Manager

Mendukung penggunaan kredensial sementara	Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensyal sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensyal sementara, lihat Layanan AWS yang bekerja dengan IAM di Panduan Pengguna IAM.

Anda menggunakan kredensyal sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensyal sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat Peralihan peran (konsol) dalam Panduan Pengguna IAM.

Anda dapat membuat kredensyal sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensyal sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda menghasilkan kredensyal sementara secara dinamis alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

Teruskan sesi akses untuk Firewall Manager

Mendukung sesi akses maju (FAS)	Ya

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.

Peran layanan untuk Firewall Manager

Mendukung peran layanan	Parsial

Peran layanan adalah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak fungsionalitas Firewall Manager. Edit peran layanan hanya jika Firewall Manager memberikan panduan untuk melakukannya.

Memilih peran IAM di Firewall Manager

Untuk menggunakan tindakan *PutNotificationChannel*API di Firewall Manager, Anda harus memilih peran untuk mengizinkan Firewall Manager mengakses Amazon SNS sehingga layanan dapat mempublikasikan pesan Amazon SNS atas nama Anda. Untuk informasi selengkapnya, lihat PutNotificationChanneldi Referensi AWS Firewall Manager API.

Berikut ini menunjukkan contoh pengaturan izin topik SNS. Untuk menggunakan kebijakan ini dengan peran kustom Anda sendiri, ganti ganti Nama Sumber Daya `AWSServiceRoleForFMS` Amazon (ARN) dengan `SnsRoleName` ARN.

```
{
  "Sid": "AWSFirewallManagerSNSPolicy",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::account ID:role/aws-service-role/
fms.amazonaws.com/AWSServiceRoleForFMS"
  },
  "Action": "sns:Publish",
  "Resource": "SNS topic ARN"
}
```

Untuk informasi selengkapnya tentang tindakan dan sumber daya Firewall Manager, lihat topik AWS Identity and Access Management panduan Tindakan yang Ditentukan oleh AWS Firewall Manager

Peran terkait layanan untuk Firewall Manager

Mendukung peran terkait layanan	Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang pembuatan atau manajemen peran terkait layanan, lihat Layanan AWS yang berfungsi dengan IAM. Cari layanan dalam tabel yang memiliki `Yes` di kolom Peran terkait layanan. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Contoh kebijakan berbasis identitas untuk AWS Firewall Manager

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Firewall Manager. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian akan dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Firewall Manager, termasuk format ARN untuk setiap jenis sumber daya, lihat Tindakan, sumber daya, dan kunci kondisi untuk AWS Firewall Manager dalam Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol Firewall Manager
- Mengizinkan pengguna melihat izin mereka sendiri
- Berikan akses baca ke grup keamanan Firewall Manager Anda

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Firewall Manager di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi

selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.

- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan IAM Access Analyzer dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi akses API yang dilindungi MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan dalam IAM dalam Panduan Pengguna IAM.

Menggunakan konsol Firewall Manager

Untuk mengakses AWS Firewall Manager konsol, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Firewall Manager di situs Anda Akun AWS. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat

daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, izinkan akses hanya ke tindakan yang sesuai dengan operasi API yang coba mereka lakukan.

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan konsol Firewall Manager, lampirkan juga Firewall Manager *ConsoleAccess* atau kebijakan *ReadOnly* AWS terkelola ke entitas. Untuk informasi selengkapnya, lihat Menambah izin untuk pengguna dalam Panduan Pengguna IAM.

Mengizinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
```

```
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Berikan akses baca ke grup keamanan Firewall Manager Anda

Firewall Manager memungkinkan akses sumber daya lintas akun, tetapi tidak memungkinkan Anda membuat perlindungan sumber daya lintas akun. Anda hanya dapat membuat perlindungan untuk sumber daya dari dalam akun yang memiliki sumber daya tersebut.

Berikut ini adalah contoh kebijakan yang memberikan izin untuk`fms:Get`,`fms:List`, dan `ec2:DescribeSecurityGroups` tindakan pada semua sumber daya.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "fms:Get*",
                "fms:List*",
                "ec2:DescribeSecurityGroups"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS kebijakan terkelola untuk AWS Firewall Manager

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pemutakhiran akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat AWS kebijakan yang dikelola dalam Panduan Pengguna IAM.

AWS kebijakan terkelola: **`AWSFMAdminFullAccess`**

Gunakan kebijakan `AWSFMAdminFullAccess` AWS terkelola untuk mengizinkan administrator mengakses AWS Firewall Manager sumber daya, termasuk semua jenis kebijakan Manajer Firewall. Kebijakan ini tidak menyertakan izin untuk menyiapkan notifikasi Amazon Simple Notification Service. AWS Firewall Manager Untuk informasi tentang cara mengatur akses untuk Amazon Simple Notification Service, lihat Menyiapkan akses untuk Amazon Simple Notification Service.

Untuk daftar kebijakan dan detailnya, lihat konsol IAM di AWSFMAdminFullAccess. Sisa bagian ini memberikan gambaran umum tentang pengaturan kebijakan.

Pernyataan izin

Kebijakan ini dikelompokkan ke dalam pernyataan berdasarkan kumpulan izin.

- AWS Firewall Manager resource kebijakan - Memungkinkan izin administratif penuh ke sumber daya AWS Firewall Manager, termasuk semua jenis kebijakan Firewall Manager.
- Menulis AWS WAF log ke Amazon Simple Storage Service - Memungkinkan Firewall Manager untuk menulis dan membaca AWS WAF log di Amazon S3.
- Buat peran terkait layanan — Memungkinkan administrator membuat peran terkait layanan, yang memungkinkan Firewall Manager mengakses sumber daya di layanan lain atas nama Anda. Izin ini memungkinkan pembuatan peran terkait layanan hanya untuk digunakan oleh Firewall Manager. Untuk informasi tentang cara Firewall Manager menggunakan peran terkait layanan, lihat. Menggunakan peran terkait layanan untuk Firewall Manager
- AWS Organizations— Memungkinkan administrator untuk menggunakan Firewall Manager untuk organisasi di AWS Organizations. Setelah mengaktifkan akses tepercaya untuk Firewall Manager

di AWS Organizations, anggota akun admin dapat melihat temuan di seluruh organisasi mereka. Untuk informasi tentang menggunakan AWS Organizations dengan AWS Firewall Manager, lihat Menggunakan AWS Organizations dengan AWS layanan lain di Panduan AWS Organizations Pengguna.

Kategori izin

Berikut ini mencantumkan jenis izin dalam kebijakan dan izin yang diberikannya.

- `fms`— Bekerja dengan AWS Firewall Manager sumber daya.
- `waf`dan `waf-regional` — Bekerja dengan kebijakan AWS WAF Klasik.
- `elasticloadbalancing`— Associate AWS WAF web ACLsto Elastic Load Balancers.
- `firehose`— Lihat informasi tentang AWS WAF log.
- `organizations`— Bekerja dengan sumber daya AWS Organizations.
- `shield`— Lihat status berlangganan AWS Shield kebijakan.
- `route53resolver`— Bekerja dengan Route 53 Private DNS untuk grup aturan VPC dalam kebijakan DNS Pribadi Route 53 untuk VPC.
- `wafv2`Bekerja dengan AWS WAFV2 kebijakan.
- `network-firewall`Bekerja dengan AWS Network Firewall kebijakan.
- `ec2`— Lihat kebijakan Availability Zone dan Regions.
- `s3`— Lihat informasi tentang AWS WAF log.

AWS kebijakan terkelola: **`FMSServiceRolePolicy`**

Kebijakan ini memungkinkan AWS Firewall Manager untuk mengelola AWS sumber daya atas nama Anda di Firewall Manager dan dalam layanan terintegrasi. Kebijakan ini dilampirkan pada peran terkait layanan. `AWSServiceRoleForFMS` Untuk informasi selengkapnya tentang peran tertaut layanan, lihat Menggunakan peran terkait layanan untuk Firewall Manager.

Untuk detail kebijakan, lihat konsol IAM di ServiceRolePolicyFMS.

AWS kebijakan terkelola: AWSFMAdminReadOnlyAccess

Memberikan akses hanya-baca ke semua sumber daya AWS Firewall Manager.

Untuk daftar kebijakan dan detailnya, lihat konsol IAM di AWSFMAdminReadOnlyAccess. Sisa bagian ini memberikan gambaran umum tentang pengaturan kebijakan.

Kategori izin

Berikut ini mencantumkan jenis izin dalam kebijakan dan informasi yang memungkinkan akses hanya baca.

- `fms`— AWS Firewall Manager sumber daya.
- `waf`dan `waf-regional` — Kebijakan AWS WAF klasik.
- `firehose`— AWS WAF log.
- `organizations`— Sumber daya AWS Organisasi.
- `shield`— AWS Shield kebijakan.
- `route53resolver`— Rute 53 DNS Pribadi untuk grup aturan VPC dalam kebijakan DNS Pribadi Route 53 untuk VPC.
- `wafv2`— Grup AWS WAFV2 aturan Anda dan grup aturan Aturan AWS Terkelola yang tersedia di AWS WAFV2.
- `network-firewall`— kelompok AWS Network Firewall aturan dan metadata kelompok aturan.
- `ec2`— AWS Network Firewall kebijakan Availability Zone dan Regions.
- `s3`— AWS WAF log.

AWS kebijakan terkelola: AWSFMMemberReadOnlyAccess

Memberikan akses hanya-baca ke AWS Firewall Manager sumber daya anggota. Untuk daftar kebijakan dan detailnya, lihat konsol IAM di AWSFMMemberReadOnlyAccess.

Firewall Manager memperbarui kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Firewall Manager sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman riwayat dokumen Firewall Manager di. Riwayat dokumen

Perubahan	Deskripsi	Tanggal
FMS ServiceRolePolicy - Kebijakan yang diperbarui	Menambahkan izin untuk mengelola ACL jaringan.	2024-04-22

Perubahan	Deskripsi	Tanggal
	Lihat kebijakan yang diperbarui di konsol IAM: ServiceRolePolicyFMS.	
FMS ServiceRolePolicy - Kebijakan yang diperbarui	Menambahkan izin yang memungkinkan Firewall Manager untuk menjelaskan apakah AWS Config aturan yang ditentukan sesuai. Lihat kebijakan yang diperbarui di konsol IAM: ServiceRolePolicyFMS.	2023-04-21
FMS ServiceRolePolicy - Kebijakan yang diperbarui	Menambahkan izin yang memungkinkan Firewall Manager mendeskripsikan instans Amazon EC2 dan atribut antarmuka jaringan. Lihat kebijakan yang diperbarui di konsol IAM: ServiceRolePolicyFMS.	2022-11-15
AWSFMAdminReadOnlyAccess— Kebijakan yang diperbarui	Menambahkan izin untuk mendukung AWS WAFV2, Shield, Network Firewall, DNS Firewall, grup keamanan Amazon VPC, kebijakan. Lihat kebijakan yang diperbarui di konsol IAM: AWSFMAdminReadOnlyAccess.	2022-11-02

Perubahan	Deskripsi	Tanggal
AWSFMAdminFullAccess— Kebijakan yang diperbarui	Menambahkan izin untuk mendukung AWS WAFV2, Shield, Network Firewall, DNS Firewall, grup keamanan Amazon VPC, kebijakan. Izin Amazon SNS yang dihapus. Lihat kebijakan yang diperbarui di konsol IAM: AWSFMAdminFullAccess.	2022-10-21
`FMSServiceRolePolicy` — Izin baru untuk kebijakan firewall AWS Firewall Manager pihak ketiga	Perubahan ini memungkinkan Firewall Manager untuk membuat dan menghapus titik akhir VPC Amazon EC2 yang terkait dengan kebijakan firewall pihak ketiga.	2022-03-30
`FMSServiceRolePolicy` — Izin baru untuk kebijakan AWS Network Firewall	Menambahkan izin baru untuk mendukung penerapan firewall untuk kebijakan Network Firewall. Izin baru memungkinkan pengambilan informasi tentang Availability Zone untuk akun yang berada dalam cakupan kebijakan.	2022-02-16

Perubahan	Deskripsi	Tanggal
`FMSServiceRolePolicy` — Izin baru untuk kebijakan AWS Shield	Menambahkan izin baru untuk mengambil tag untuk sumber daya AWS WAF regional dan AWS WAF global. Menambahkan izin AWS WAF regional untuk mengambil ACL web menggunakan ARN sumber daya. Menambahkan izin untuk mendukung mitigasi DDoS lapisan aplikasi otomatis Shield.	2022-01-07
`FMSServiceRolePolicy` — Izin baru untuk kebijakan AWS Shield	Menambahkan izin baru untuk mengambil tag untuk sumber daya Elastic Load Balancing.	2021-11-18
`FMSServiceRolePolicy` — Izin baru untuk grup keamanan dan kebijakan AWS Network Firewall	Menambahkan izin baru untuk mengaktifkan pencatatan terpusat untuk AWS Network Firewall kebijakan. Selain itu, izin Amazon EC2 hanya-baca ditambahkan untuk mendukung perubahan pada layanan Config yang AWS Firewall Manager memengaruhi sumber daya kueri untuk kebijakan grup keamanan.	2021-09-29

Perubahan	Deskripsi	Tanggal
`FMSServiceRolePolicy` — Format ARN untuk sumber daya AWS WAF	Memperbarui `FMSServiceRolePolicy` untuk menstandarisasi format ARN untuk sumber daya. AWS WAF Format ARN yang diperbarui adalah `arn:aws:waf:*:*:*` dan. `arn:aws:waf-regional:*:*:*`	2021-08-12
`FMSServiceRolePolicy` - Wilayah tambahan di China	AWS Firewall Manager telah diaktifkan `FMSServiceRolePolicy` untuk wilayah BJS dan ZHY di China.	2021-08-12
`FMSServiceRolePolicy` — Update ke kebijakan yang ada	Menambahkan izin baru AWS Firewall Manager untuk memungkinkan mengelola Amazon Route 53 Resolver DNS Firewall. Perubahan ini memungkinkan Firewall Manager untuk mengkonfigurasi asosiasi Amazon Route 53 Resolver DNS Firewall. Ini memungkinkan Anda untuk menggunakan Firewall Manager untuk memberikan perlindungan DNS Firewall untuk VPC Anda di seluruh organisasi Anda. AWS Organizations	2021-03-17

Perubahan	Deskripsi	Tanggal
Firewall Manager mulai melacak perubahan	Firewall Manager mulai melacak perubahan untuk kebijakan yang AWS dikelola.	2021-03-02

Memecahkan masalah AWS Firewall Manager identitas dan akses

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Firewall Manager dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di Firewall Manager
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Firewall Manager saya

Saya tidak berwenang untuk melakukan tindakan di Firewall Manager

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya *`my-example-widget`* rekaan, tetapi tidak memiliki izin `fms:`*`GetWidget`* rekaan.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fms:GetWidget on resource: my-example-widget
```

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya *`my-example-widget`* dengan menggunakan tindakan `fms:`*`GetWidget`*.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan yang tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Firewall Manager.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di Firewall Manager. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Firewall Manager saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau pengguna di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi pengguna akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa hal berikut:

- Untuk mengetahui apakah Firewall Manager mendukung fitur-fitur ini, lihatBagaimana AWS Shield bekerja dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.

- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Memberikan akses kepada pengguna eksternal yang sah (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara penggunaan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Perbedaan antara peran IAM dan kebijakan berbasis sumber daya di Panduan Pengguna IAM.

Menggunakan peran terkait layanan untuk Firewall Manager

AWS Firewall Manager menggunakan AWS Identity and Access Management peran terkait layanan (IAM). Peran terkait layanan adalah jenis unik peran IAM yang ditautkan langsung ke Firewall Manager. Peran terkait layanan telah ditentukan sebelumnya oleh Firewall Manager dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan Firewall Manager lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Firewall Manager mendefinisikan izin dari peran terkait layanan, dan kecuali ditentukan lain, hanya Firewall Manager yang dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin. Kebijakan izin tersebut tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran terkait layanan hanya setelah terlebih dahulu menghapus sumber daya terkait peran tersebut. Ini melindungi sumber daya Firewall Manager Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat Layanan AWS yang bisa digunakan dengan IAM dan carilah layanan yang memiliki opsi Ya di kolom Peran Terkait Layanan. Pilih Ya bersama tautan untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

Izin peran terkait layanan untuk Firewall Manager

AWS Firewall Manager menggunakan nama peran terkait layanan AWSServiceRoleForFMS untuk memungkinkan Firewall Manager memanggil AWS layanan atas nama Anda untuk pengelolaan kebijakan firewall dan sumber daya AWS Organizations akun. Kebijakan ini melekat pada peran yang AWS dikelolaAWSServiceRoleForFMS. Untuk informasi selengkapnya tentang peran terkelola, lihatAWS kebijakan terkelola: FMSServiceRolePolicy.

Peran AWSServiceRoleForFMS terkait layanan mempercayai layanan untuk mengambil peran tersebut. `fms.amazonaws.com`

Kebijakan izin peran memungkinkan Firewall Manager untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- `waf`- Kelola ACL web AWS WAF Klasik, izin grup aturan, dan asosiasi ACL web di akun Anda.
- `ec2`- Kelola grup keamanan pada antarmuka jaringan elastis dan instans Amazon EC2. Kelola ACL jaringan di subnet VPC Amazon.
- `vpc`- Kelola subnet, tabel rute, tag, dan titik akhir di Amazon VPC.
- `wafv2`- Kelola ACL AWS WAF web, izin grup aturan, dan asosiasi ACL web di akun Anda.
- `cloudfront`- Buat ACL web untuk melindungi CloudFront distribusi.
- `config`- Kelola AWS Config aturan yang dimiliki Manajer Firewall di akun Anda.
- `iam`- Kelola peran terkait layanan ini, dan buat peran wajib dan AWS WAF Shield terkait layanan jika mengonfigurasi kebijakan logging untuk dan Shield. AWS WAF
- `organization`- Buat peran terkait layanan yang dimiliki oleh Firewall Manager untuk mengelola AWS Organizations sumber daya yang digunakan oleh Firewall Manager.
- `shield`- Kelola AWS Shield perlindungan dan konfigurasi mitigasi L7 untuk sumber daya di akun Anda.
- `ram`- Mengelola berbagi AWS RAM sumber daya untuk grup aturan DNS Firewall dan grup aturan Network Firewall.
- `network-firewall`- Kelola AWS Network Firewall sumber daya milik Manajer Firewall dan sumber daya VPC Amazon yang bergantung pada akun Anda.
- `route53resolver`- Kelola asosiasi Firewall DNS Firewall milik Manajer Firewall di akun Anda.

Lihat kebijakan selengkapnya di konsol IAM: ServiceRolePolicyFMS.

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, silakan lihat Izin Peran Tertaut Layanan di Panduan Pengguna IAM.

Membuat peran terkait layanan untuk Firewall Manager

Anda tidak perlu membuat peran terkait layanan secara manual. Ketika Anda mengaktifkan Firewall Manager masuk AWS Management Console, atau Anda membuat `PutLoggingConfiguration`

permintaan di Firewall Manager CLI atau Firewall Manager API, Firewall Manager membuat peran terkait layanan untuk Anda.

Anda harus memiliki `iam:CreateServiceLinkedRole` izin untuk mengaktifkan logging.

Jika Anda menghapus peran tertaut layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Saat Anda mengaktifkan pencatatan Firewall Manager, Firewall Manager membuat peran terkait layanan untuk Anda lagi.

Mengedit peran terkait layanan untuk Firewall Manager

Firewall Manager tidak mengizinkan Anda mengedit peran AWSServiceRoleForFMS terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat menyunting penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit Peran Tertaut Layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk Firewall Manager

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, kami merekomendasikan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Tetapi, Anda harus membersihkan sumber daya peran yang terhubung dengan layanan sebelum menghapusnya secara manual.

> **Note**
>
> Jika layanan Firewall Manager menggunakan peran saat Anda mencoba menghapus sumber daya, maka penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus peran terkait layanan menggunakan IAM

Gunakan konsol IAM, IAM CLI, atau IAM API untuk menghapus peran terkait layanan. AWSServiceRoleForFMS Untuk informasi selengkapnya, silakan lihat Menghapus Peran Terkait Layanan di Panduan Pengguna IAM.

Wilayah yang Didukung untuk peran terkait layanan Firewall Manager

Firewall Manager mendukung penggunaan peran terkait layanan di semua wilayah tempat layanan tersedia. Untuk informasi selengkapnya, lihat titik akhir dan kuota Firewall Manager.

Pencegahan confused deputy lintas layanan

Masalah deputi yang bingung adalah masalah keamanan di mana entitas yang tidak memiliki izin untuk melakukan tindakan dapat memaksa entitas yang lebih istimewa untuk melakukan tindakan. Pada tahun AWS, peniruan lintas layanan dapat mengakibatkan masalah wakil yang membingungkan. Peniruan identitas lintas layanan dapat terjadi ketika satu layanan (layanan yang dipanggil) memanggil layanan lain (layanan yang dipanggil). Layanan pemanggilan dapat dimanipulasi menggunakan izinnya untuk bertindak pada sumber daya pelanggan lain dengan cara yang seharusnya tidak dilakukannya kecuali bila memiliki izin untuk mengakses. Untuk mencegah hal ini, AWS menyediakan alat yang membantu Anda melindungi data untuk semua layanan dengan pengguna utama layanan yang telah diberi akses ke sumber daya di akun Anda.

Sebaiknya gunakan kunci konteks kondisi `aws:SourceAccount`global `aws:SourceArn`dan dalam kebijakan sumber daya untuk membatasi izin yang AWS Firewall Manager memberikan layanan lain ke sumber daya. Gunakan `aws:SourceArn` jika Anda hanya ingin satu sumber daya dikaitkan dengan akses lintas layanan. Gunakan `aws:SourceAccount` jika Anda ingin mengizinkan sumber daya apa pun di akun tersebut dikaitkan dengan penggunaan lintas layanan.

Cara paling efektif untuk melindungi dari masalah confused deputy adalah dengan menggunakan kunci konteks kondisi global `aws:SourceArn` dengan ARN lengkap sumber daya. Jika Anda tidak mengetahui ARN lengkap sumber daya atau jika Anda menentukan beberapa sumber daya, gunakan kunci kondisi konteks `aws:SourceArn` global dengan karakter wildcard (`*`) untuk bagian ARN yang tidak diketahui. Misalnya, `arn:aws:fms:*:`*`account-id`*`:*`.

Jika `aws:SourceArn` nilainya tidak berisi ID akun, seperti ARN bucket Amazon S3, Anda harus menggunakan kedua kunci konteks kondisi global untuk membatasi izin.

Nilai `aws:SourceArn` harus menjadi AWS akun AWS Firewall Manager administrator.

Contoh berikut menunjukkan bagaimana Anda dapat menggunakan kunci konteks kondisi `aws:SourceArn` global di Firewall Manager untuk mencegah masalah deputi yang membingungkan.

Contoh berikut menunjukkan cara mencegah masalah deputi yang membingungkan dengan menggunakan kunci konteks kondisi `aws:SourceArn` global dalam kebijakan kepercayaan peran Manajer Firewall. Ganti *`Region`* dan *`account-id`* dengan informasi Anda sendiri.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "servicename.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": [
          "arn:aws:fms:Region:account-id:${*}",
          "arn:aws:fms:Region:account-id:policy/*"]
      },
      "StringEquals": {
        "aws:SourceAccount": "account-id"
      }
    }
  }
}
```

Pencatatan dan pemantauan di Firewall Manager

Pemantauan adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja Firewall Manager dan AWS solusi Anda. Anda harus mengumpulkan data pemantauan dari semua bagian AWS solusi Anda sehingga Anda dapat lebih mudah men-debug kegagalan multi-titik jika terjadi. AWS menyediakan beberapa alat untuk memantau sumber daya Firewall Manager Anda dan menanggapi peristiwa potensial:

CloudWatch Alarm Amazon

Menggunakan CloudWatch alarm, Anda menonton satu metrik selama periode waktu yang Anda tentukan. Jika metrik melebihi ambang batas tertentu, CloudWatch kirimkan pemberitahuan ke topik atau AWS Auto Scaling kebijakan Amazon SNS. Untuk informasi selengkapnya, lihat Pemantauan CloudWatch dengan Amazon.

AWS CloudTrail Log

CloudTrail menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Firewall Manager. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat untuk Firewall Manager, alamat IP dari mana permintaan itu dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan. Untuk informasi selengkapnya, lihat Logging panggilan API dengan AWS CloudTrail.

Validasi kepatuhan untuk Firewall Manager

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar AWS yang berfokus pada keamanan dan kepatuhan.
- Arsitektur untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi yang memenuhi syarat HIPAA.

  > **Note**
  >
  > Tidak semua memenuhi Layanan AWS syarat HIPAA. Untuk informasi selengkapnya, lihat Referensi Layanan yang Memenuhi Syarat HIPAA.

- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber

daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.

- Amazon GuardDuty — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan di Firewall Manager

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang dan mengoperasikan aplikasi dan basis data yang melakukan secara otomatis pinda saat gagal/failover di antara zona-zona tanpa terputus. Zona Ketersediaan lebih sangat tersedia, lebih toleran kesalahan, dan lebih dapat diskalakan daripadai infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur AWS Global.

Keamanan infrastruktur dalam AWS Firewall Manager

Sebagai layanan terkelola, AWS Firewall Manager dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses Firewall Manager melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.

- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani dengan menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan pengguna utama IAM. Atau Anda bisa menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

AWS Firewall Manager kuota

AWS Firewall Manager tunduk pada kuota berikut (sebelumnya disebut sebagai batas).

AWS Firewall Manager memiliki kuota default yang mungkin dapat Anda tingkatkan dan kuota tetap.

Kebijakan grup keamanan dan kebijakan ACL jaringan yang dikelola oleh Firewall Manager tunduk pada kuota VPC Amazon standar. Untuk informasi selengkapnya, lihat Kuota VPC Amazon di Panduan Pengguna Amazon VPC.

Setiap kebijakan Firewall Manager Network Firewall membuat firewall Network Firewall dengan kebijakan firewall terkait dan grup aturannya. Sumber daya Network Firewall ini tunduk pada kuota yang tercantum pada AWS Network Firewall kuota dalam Panduan Pengembang Network Firewall.

Kuota lembut

AWS Firewall Manager memiliki kuota default pada jumlah entitas per Wilayah. Anda dapat meminta peningkatan kuota ini.

Semua jenis kebijakan

Sumber Daya	Kuota default per Wilayah
Akun per organisasi di AWS Organizations	Bervariasi. Undangan yang dikirim ke akun dihitung terhadap kuota ini. Hitungan tersebut dikembali kan jika akun yang

Sumber Daya	Kuota default per Wilayah
	diundang menolak, akun pengelola an membatalkan undangan, atau undangan kedaluwar sa.
Kebijakan Firewall Manager per organisasi di AWS Organizations.	50. Spesifikasi Wilayah `Global` dan `US East (N. Virginia) Region` mengacu pada Wilayah yang sama, jadi batas ini berlaku untuk total kebijakan gabungan untuk keduanya.
Unit organisasi dalam lingkup per kebijakan Firewall Manager.	20
Akun dalam lingkup kebijakan Firewall Manager jika Anda secara eksplisit menyertakan dan mengecualikan akun individual.	200
Akun dalam lingkup kebijakan Firewall Manager jika Anda tidak secara eksplisit menyertakan atau mengecualikan akun individual.	2.500
Tag yang menyertakan atau mengecualikan sumber daya sesuai kebijakan Firewall Manager.	8
Jumlah set sumber daya per akun.	20
Jumlah sumber daya per set sumber daya.	100
Jumlah set sumber daya per kebijakan Firewall Manager.	5

AWS WAF kebijakan

Sumber Daya	Kuota default per Wilayah
AWS WAF grup aturan per akun administrator Firewall Manager.	100
AWS WAF Grup aturan klasik per akun administrator Firewall Manager.	10
Kelompok aturan per AWS WAF kebijakan.	50

Kebijakan kelompok keamanan umum

Sumber Daya	Kuota default per Wilayah.
Kelompok keamanan utama per kebijakan.	3
Instans VPC Amazon dalam cakupan per kebijakan per akun, termasuk VPC bersama.	100

Kebijakan grup keamanan audit konten

Sumber Daya	Kuota default per Wilayah
Audit kelompok keamanan per kebijakan.	1
Aplikasi per daftar aplikasi.	50
Daftar aplikasi terkelola khusus untuk aturan yang memungkinkan semua lalu lintas.	1
Daftar aplikasi terkelola kustom per aturan kebijakan.	1
Daftar aplikasi terkelola khusus per akun.	10
Protokol per daftar protokol.	5
Daftar protokol terkelola khusus untuk setelan apa pun dalam kebijakan.	1

Sumber Daya	Kuota default per Wilayah
Daftar protokol terkelola khusus per akun.	10

Kebijakan ACL jaringan

Sumber Daya	Kuota default per Wilayah
Jumlah aturan masuk per kebijakan ACL jaringan, digunakan untuk aturan pertama atau terakhir. Misalnya, Anda dapat memiliki 5 aturan masuk pertama dan 0 terakhir, atau 2 pertama dan 3 terakhir, tetapi Anda tidak dapat memiliki 4 aturan pertama dan 2 terakhir.	5
Jumlah aturan keluar per kebijakan ACL jaringan, digunakan untuk aturan pertama atau terakhir. Misalnya, Anda dapat memiliki 5 aturan keluar pertama dan 0 terakhir, atau 2 pertama dan 3 terakhir, tetapi Anda tidak dapat memiliki 4 yang pertama dan 2 terakhir.	5

Kebijakan DNS Firewall

Sumber Daya	Kuota default per Wilayah
Grup aturan DNS Firewall per kebijakan DNS Firewall.	2

Kuota keras

Kuota per wilayah berikut yang terkait dengan tidak AWS Firewall Manager dapat diubah.

Semua jenis kebijakan

Sumber Daya	Kuota per Wilayah
Jumlah maksimum administrator Firewall Manager yang dapat Anda miliki dalam suatu AWS Organizations organisasi. Anda harus memiliki	10

Sumber Daya	Kuota per Wilayah
satu administrator default, dan sebanyak sembilan administrator Firewall Manager tambahan.	

AWS WAF kebijakan

Sumber Daya	Kuota per Wilayah
Total unit kapasitas ACL web (WCU) untuk kelompok aturan dalam suatu AWS WAF kebijakan.	5.000

AWS WAF Kebijakan klasik

Sumber Daya	Kuota per Wilayah
AWS WAF Kelompok aturan klasik per kebijakan.	2:1 grup aturan yang dibuat pelanggan dan 1 grup AWS Marketplace aturan.
AWS WAF Aturan klasik per Firewall Manager AWS WAF Classic grup aturan.	10

Kebijakan audit konten grup keamanan

Sumber Daya	Kuota per Wilayah
Daftar aplikasi terkelola Firewall Manager untuk pengaturan apa pun dalam kebijakan.	1
Daftar protokol terkelola Firewall Manager untuk setelan apa pun dalam kebijakan.	1

Kebijakan Network Firewall

Sumber Daya	Kuota per Wilayah
Jumlah VPC yang dapat diperbaiki secara otomatis untuk satu kebijakan.	1.000
Jumlah CIDR IPV4 yang dapat Anda berikan untuk satu kebijakan.	50

Pemantauan AWS WAF, AWS Firewall Manager, dan AWS Shield Advanced

Pemantauan adalah bagian penting untuk menjaga keandalan, ketersediaan, dan kinerja layanan Anda.

> **Note**
>
> Untuk informasi tentang memantau sumber daya Shield Advanced Anda dan mengidentifikasi kemungkinan peristiwa DDoS menggunakan Shield Advanced, lihatAWS Shield.

Saat Anda mulai memantau layanan ini, Anda harus membuat rencana pemantauan yang mencakup jawaban atas pertanyaan-pertanyaan berikut:

- Apa tujuan pemantauan Anda?
- Sumber daya apa yang akan Anda pantau?
- Seberapa sering Anda akan memantau sumber daya ini?
- Alat pemantauan apa yang akan Anda gunakan?
- Siapa yang akan melakukan tugas pemantauan?
- Siapa yang harus diberi tahu saat terjadi kesalahan?

Langkah berikutnya adalah menetapkan dasar untuk performa normal di lingkungan Anda, dengan mengukur kinerja di berbagai waktu dan dengan kondisi beban yang berbeda. Saat Anda memantau AWS WAF, Firewall Manager, Shield Advanced dan layanan terkait, menyimpan data pemantauan historis sehingga Anda dapat membandingkannya dengan data kinerja saat ini, mengidentifikasi pola kinerja normal dan anomali kinerja, dan merancang metode untuk mengatasi masalah.

Untuk AWS WAF, Anda harus memantau item berikut minimal untuk menetapkan garis dasar:

- Jumlah permintaan web yang diizinkan
- Jumlah permintaan web yang diblokir

Topik

- Pemantauan CloudWatch dengan Amazon
- Logging panggilan API dengan AWS CloudTrail

Alat-alat pemantauan

AWS menyediakan berbagai alat yang dapat Anda gunakan untuk memantau AWS WAF dan AWS Shield Advanced. Anda dapat mengonfigurasi beberapa alat ini untuk melakukan pemantauan untuk Anda, sementara alat lain memerlukan intervensi manual. Kami menyarankan agar Anda mengautomasi tugas pemantauan sebanyak mungkin.

Alat pemantauan otomatis

Anda dapat menggunakan alat pemantauan otomatis berikut untuk menonton AWS WAF AWS Shield Advanced dan melaporkan ketika ada sesuatu yang salah:

- Dasbor ikhtisar lalu lintas ACL Web — Akses ringkasan lalu lintas web yang dievaluasi oleh ACL web dengan membuka halaman ACL web di AWS WAF konsol dan membuka tab Ikhtisar lalu lintas.

  Dasbor ikhtisar lalu lintas menyediakan ringkasan hampir real-time dari CloudWatch metrik Amazon yang AWS WAF dikumpulkan saat mengevaluasi lalu lintas web aplikasi Anda. Anda dapat melihat ringkasan untuk semua lalu lintas web Anda dan untuk lalu lintas yang dievaluasi oleh kelompok aturan mitigasi ancaman cerdas.

  Untuk informasi selengkapnya, lihat Dasbor ikhtisar lalu lintas ACL web atau buka dasbor di konsol.
- CloudWatch Alarm Amazon — Tonton satu metrik selama periode waktu yang Anda tentukan, dan lakukan satu atau beberapa tindakan berdasarkan nilai metrik relatif terhadap ambang batas tertentu selama beberapa periode waktu. Tindakan ini adalah pengiriman notifikasi ke topik Amazon Simple Notification Service (Amazon SNS) atau kebijakan Amazon EC2 Auto Scaling. Alarm memanggil tindakan untuk perubahan status berkelanjutan saja. CloudWatch alarm tidak akan memanggil tindakan hanya karena mereka berada dalam keadaan tertentu; negara harus telah berubah dan dipertahankan untuk sejumlah periode tertentu. Untuk informasi selengkapnya, lihat Memantau CloudFront Aktivitas Menggunakan CloudWatch.

  > **Note**
  >
  > CloudWatch metrik dan alarm tidak diaktifkan untuk. AWS Firewall Manager

Anda tidak hanya dapat menggunakannya CloudWatch untuk memantau AWS WAF dan Shield metrik Advanced seperti yang dijelaskan dalamPemantauan CloudWatch dengan Amazon, Anda juga harus menggunakannya CloudWatch untuk memantau aktivitas sumber daya yang dilindungi. Untuk informasi selengkapnya, lihat hal berikut:

- Memantau CloudFront Aktivitas Menggunakan CloudWatch di Panduan CloudFront Pengembang Amazon
- Pencatatan dan pemantauan di Amazon API Gateway di Panduan Pengembang API Gateway
- CloudWatch Metrik untuk Application Load Balancer Anda di Panduan Pengguna Elastic Load Balancing
- Pemantauan dan Logging di Panduan AWS AppSync Pengembang
- Pencatatan dan pemantauan di Amazon Cognito di Panduan Pengembang Amazon Cognito
- Melihat log Pelari Aplikasi yang dialirkan ke CloudWatch Log dan Melihat metrik layanan Pelari Aplikasi yang dilaporkan dalam Panduan Pengembang CloudWatchAWS App Runner

- Amazon CloudWatch Logs — Pantau, simpan, dan akses file log Anda dari AWS CloudTrail atau sumber lain. Untuk informasi selengkapnya, lihat Apa itu CloudWatch Log Amazon? .
- CloudWatch Acara Amazon - Otomatiskan AWS layanan Anda dan tanggapi peristiwa sistem secara otomatis. Acara dari AWS layanan dikirimkan ke CloudWatch Acara dalam waktu dekat, dan Anda dapat menentukan tindakan otomatis yang akan diambil saat acara cocok dengan aturan yang Anda tulis. Untuk informasi selengkapnya, lihat Apa itu CloudWatch Acara Amazon?
- AWS CloudTrail Pemantauan Log - Bagikan file log antar akun, pantau file CloudTrail log secara real time dengan mengirimkannya ke CloudWatch Log, menulis aplikasi pemrosesan log di Java, dan validasi bahwa file log Anda tidak berubah setelah pengiriman oleh. CloudTrail Untuk informasi selengkapnya, lihat Logging panggilan API dengan AWS CloudTrail dan Bekerja dengan File CloudTrail Log di Panduan AWS CloudTrail Pengguna.
- AWS Config— Lihat konfigurasi AWS sumber daya di AWS akun Anda, termasuk bagaimana sumber daya terkait satu sama lain dan bagaimana mereka dikonfigurasi di masa lalu sehingga Anda dapat melihat bagaimana konfigurasi dan hubungan berubah dari waktu ke waktu.

Alat pemantauan manual

Bagian penting lainnya dari pemantauan AWS WAF dan AWS Shield Advanced melibatkan pemantauan secara manual item-item yang tidak tercakup oleh CloudWatch alarm. Anda dapat melihat AWS Management Console dasbor AWS WAF, Shield Advanced CloudWatch,, dan lainnya

untuk melihat keadaan AWS lingkungan Anda. Kami menyarankan Anda juga memeriksa file log untuk ACL dan aturan web Anda.

- Misalnya, untuk melihat AWS WAF dasbor:
  - Pada tab Permintaan halaman ACL AWS WAF Web, lihat grafik total permintaan dan permintaan yang cocok dengan setiap aturan yang telah Anda buat. Untuk informasi selengkapnya, lihat Melihat contoh permintaan web.
- Lihat halaman CloudWatch beranda untuk hal-hal berikut:
  - Alarm dan status saat ini
  - Grafik alarm dan sumber daya
  - Status kondisi layanan

  Selain itu, Anda dapat menggunakan CloudWatch untuk melakukan hal berikut:
  - Membuat dasbor yang disesuaikan untuk memantau layanan yang penting bagi Anda.
  - Data metrik grafik untuk memecahkan masalah dan mengungkap tren.
  - Cari dan telusuri semua metrik AWS sumber daya Anda.
  - Membuat dan mengedit alarm agar diberi tahu tentang masalah.

Pemantauan CloudWatch dengan Amazon

Anda dapat memantau permintaan web dan ACL web serta aturan menggunakan Amazon CloudWatch, yang mengumpulkan dan memproses data mentah dari AWS WAF dan AWS Shield Advanced menjadi metrik yang dapat dibaca, mendekati waktu nyata. Anda dapat menggunakan statistik di Amazon CloudWatch untuk mendapatkan perspektif tentang kinerja aplikasi atau layanan web Anda. Untuk informasi selengkapnya, lihat Apa yang ada CloudWatch di Panduan CloudWatch Pengguna Amazon.

> **Note**
>
> CloudWatch metrik dan alarm tidak diaktifkan untuk Firewall Manager.

Anda dapat membuat CloudWatch alarm Amazon yang mengirimkan pesan Amazon SNS saat alarm berubah status. Alarm mengawasi satu metrik selama periode waktu yang Anda tentukan, dan melakukan satu atau beberapa tindakan berdasarkan nilai metrik relatif terhadap ambang batas tertentu selama beberapa periode waktu. Tindakan ini adalah notifikasi yang dikirim ke topik Amazon

SNS atau kebijakan Penskalaan Otomatis. Alarm memanggil tindakan untuk perubahan status berkelanjutan saja. CloudWatch alarm tidak memanggil tindakan hanya karena mereka berada dalam keadaan tertentu; negara harus telah berubah dan dipertahankan untuk sejumlah periode tertentu.

Topik

Melihat metrik dan dimensi

Metrik dikelompokkan pertama oleh namespace layanan, dan kemudian oleh berbagai kombinasi dimensi dalam setiap namespace. AWS Firewall Manager tidak merekam metrik.

- AWS WAF Namespace adalah `AWS/WAFV2`
- Namespace Shield Advanced adalah `AWS/DDoSProtection`

> **Note**
>
> AWS WAF melaporkan metrik satu menit sekali.
> Shield Advanced melaporkan metrik satu menit sekali selama acara dan lebih jarang di lain waktu.

Gunakan prosedur berikut untuk melihat metrik untuk AWS WAF dan AWS Shield Advanced.

Untuk melihat metrik menggunakan konsol CloudWatch

1. Masuk ke AWS Management Console dan buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Jika perlu, ubah Wilayah ke wilayah tempat AWS sumber daya Anda berada. Untuk CloudFront, pilih Wilayah AS Timur (Virginia N.).
3. Di panel navigasi, di bawah Metrik, pilih Semua metrik dan kemudian cari di bawah tab Browse untuk layanan.

Untuk melihat metrik menggunakan CLI AWS

- Untuk AWS/WAFV2, pada command prompt gunakan perintah berikut:

```
aws cloudwatch list-metrics --namespace "AWS/WAFV2"
```

  Untuk Shield Advanced, pada command prompt gunakan perintah berikut:

```
aws cloudwatch list-metrics --namespace "AWS/DDoSProtection"
```

AWS WAF metrik dan dimensi

AWS WAF melaporkan metrik satu menit sekali. AWS WAF menyediakan metrik dan dimensi di `AWS/WAFV2` namespace.

Anda dapat melihat informasi ringkasan untuk AWS WAF metrik melalui AWS WAF konsol, di tab ikhtisar lalu lintas ACL web. Untuk informasi lebih lanjut, buka konsol atau lihatDasbor ikhtisar lalu lintas ACL web.

Anda dapat melihat metrik berikut untuk ACL web, aturan, grup aturan, dan label.

- Aturan Anda — Metrik dikelompokkan berdasarkan tindakan aturan. Misalnya, saat Anda menguji aturan dalam Count mode, kecocokannya terdaftar sebagai `Count` metrik untuk ACL web.
- Grup aturan Anda — Metrik untuk grup aturan Anda tercantum di bawah metrik grup aturan.
- Grup aturan yang dimiliki oleh akun lain — Metrik grup aturan umumnya hanya dapat dilihat oleh pemilik grup aturan. Namun, jika Anda mengganti tindakan aturan untuk aturan, metrik untuk aturan tersebut akan dicantumkan di bawah metrik ACL web Anda. Selain itu, label yang ditambahkan oleh grup aturan apa pun tercantum dalam metrik ACL web Anda

  Grup aturan dalam kategori ini adalahAWS Aturan Terkelola untuk AWS WAF,AWS Marketplace kelompok aturan terkelola,Grup aturan yang disediakan oleh layanan lain, dan grup aturan yang dibagikan dengan Anda oleh akun lain.
- Label - Label yang ditambahkan ke permintaan web selama evaluasi tercantum dalam metrik label ACL web. Anda dapat mengakses metrik untuk semua label, terlepas dari apakah itu ditambahkan oleh aturan dan grup aturan Anda atau oleh aturan dalam grup aturan yang dimiliki akun lain.

Topik

Web ACL, grup aturan, dan metrik dan dimensi aturan

Web ACL, grup aturan, dan metrik aturan

Metrik	Deskripsi
`AllowedRequests`	Jumlah permintaan web yang diizinkan. Kriteria pelaporan: Ada nilai bukan nol. Statistik yang valid: Jumlah
`BlockedRequests`	Jumlah permintaan web yang diblokir. Kriteria pelaporan: Ada nilai bukan nol. Statistik yang valid: Jumlah
`CountedRequests`	Jumlah permintaan web yang dihitung. Kriteria pelaporan: Ada nilai bukan nol. Permintaan web yang dihitung adalah permintaan yang cocok dengan setidaknya salah satu aturan. Penghitungan permintaan biasanya digunakan untuk pengujian. Statistik yang valid: Jumlah
`CaptchaRequests`	Jumlah permintaan web yang memiliki kontrol CAPTCHA diterapkan. Kriteria pelaporan: Ada nilai bukan nol.

Metrik	Deskripsi
	Permintaan web CAPTCHA adalah permintaan yang cocok dengan aturan yang memiliki pengatura n CAPTCHA tindakan. Metrik ini mencatat semua permintaan yang cocok, terlepas dari apakah mereka memiliki token CAPTCHA yang valid. Statistik yang valid: Jumlah
`RequestsWithValidCaptchaTok en`	Jumlah permintaan web yang memiliki kontrol CAPTCHA diterapkan dan yang memiliki token CAPTCHA yang valid. Kriteria pelaporan: Ada nilai bukan nol. Statistik yang valid: Jumlah
`CaptchasAttempted`	Jumlah solusi yang diajukan oleh pengguna akhir dalam menanggapi tantangan teka-teki CAPTCHA. Kriteria pelaporan: Ada nilai bukan nol. Statistik yang valid: Jumlah
`CaptchasSolved`	Jumlah solusi puzzle CAPTCHA yang dikirimkan yang berhasil memecahkan teka-teki. Kriteria pelaporan: Ada nilai bukan nol. Statistik yang valid: Jumlah

Metrik	Deskripsi
`ChallengeRequests`	Jumlah permintaan web yang memiliki kontrol tantangan diterapkan. Kriteria pelaporan: Ada nilai bukan nol. Permintaan web tantangan adalah permintaan yang cocok dengan aturan yang memiliki pengaturan Challenge tindakan. Metrik ini mencatat semua permintaan yang cocok, terlepas dari apakah mereka memiliki token tantangan yang valid. Statistik yang valid: Jumlah
`RequestsWithValidChallengeToken`	Jumlah permintaan web yang memiliki kontrol tantangan diterapkan dan yang memiliki token tantangan yang valid. Kriteria pelaporan: Ada nilai bukan nol. Statistik yang valid: Jumlah
`PassedRequests`	Jumlah permintaan yang dilewati. Ini hanya digunakan untuk permintaan yang melalui evaluasi grup aturan tanpa mencocokkan aturan grup aturan mana pun. Kriteria pelaporan: Ada nilai bukan nol. Permintaan yang diteruskan adalah permintaan yang tidak cocok dengan aturan apa pun di grup aturan. Statistik yang valid: Jumlah

Web ACL, grup aturan, dan dimensi aturan

Dimensi	Deskripsi
`Region`	Diperlukan untuk semua jenis sumber daya yang dilindungi kecuali untuk CloudFront distribusi Amazon.
`Rule`	Salah satu dari yang berikut: • Nama metrik dari`Rule`. • ALL, yang mewakili semua aturan dalam WebACL atau. `RuleGroup` • `Default_Action` (hanya bila digabungkan dengan `WebACL` dimensi), yang mewakili tindakan yang ditetapkan untuk setiap permintaan yang evaluasinya tidak dihentikan oleh tindakan aturan di ACL web.
`RuleGroup`	Nama metrik dari`RuleGroup` .
`WebACL`	Nama metrik dari`WebACL`.
`Country`	Negara asal permintaan. Ini adalah penunjukan dua karakter dari standar Organisasi Internasional untuk Standardisasi (ISO) 3166. Misalnya, AS untuk Amerika Serikat dan UA untuk Ukraina. Jika permintaan memiliki `X-Forwarded-For` header, AWS WAF gunakan itu untuk menentuka n pengaturan ini. Jika tidak, AWS WAF gunakan negara IP klien. Penentuan ini tidak tergantung pada logika apa pun yang Anda gunakan dalam aturan Anda untuk menentukan negara asal. AWS WAF menentukan lokasi MaxMind IP menggunakan database GeoIP.

Dimensi	Deskripsi
`Attack`	Jenis serangan yang AWS WAF diidentifikasi dalam permintaan, berdasarkan aturan dan kelompok aturan yang Anda gunakan di ACL web Anda. Aturan Anda dan aturan dalam kelompok aturan AWS terkelola dasar dapat mengidentifikasi jenis serangan. Misalnya, kecocokan aturan cross-site scripting (XSS) mengidentifikasi jenis serangan XSS, dan aturan berbasis kecepatan mengidentifikasi jenis serangan volumetrik. Jenis serangan biasanya menunjukkan jenis aturan yang mengakhiri evaluasi permintaan web.
`Device`	Jenis perangkat klien yang mengirim permintaan, diperoleh dari `user-agent` header permintaan web.
`ManagedRuleGroup`	Nama metrik dari`ManagedRuleGroup` .
`ManagedRuleGroupRule`	Aturan dalam `ManagedRuleGroup` yang cocok.

Label metrik dan dimensi

Metrik untuk label yang ditambahkan ke permintaan selama evaluasi menurut aturan Anda dan oleh grup aturan terkelola yang Anda gunakan di ACL web Anda. Untuk informasi, lihat Label pada permintaan web.

Untuk setiap permintaan web tunggal, AWS WAF menyimpan metrik untuk paling banyak 100 label. Evaluasi ACL web Anda dapat menerapkan lebih dari 100 label dan cocok dengan lebih dari 100 label, tetapi hanya 100 label pertama yang tercermin dalam metrik.

Metrik label

Metrik	Deskripsi
`AllowedRequests`	Jumlah label pada permintaan web yang memiliki pengaturan tindakan Allow diterapkan. Label dapat

Metrik	Deskripsi
	ditambahkan kapan saja selama evaluasi permintaan web. Kriteria pelaporan: Ada nilai bukan nol. Statistik yang valid: Jumlah
`BlockedRequests`	Jumlah label pada permintaan web yang memiliki pengaturan tindakan Block diterapkan. Label dapat ditambahkan kapan saja selama evaluasi permintaan web. Kriteria pelaporan: Ada nilai bukan nol. Statistik yang valid: Jumlah
`CountedRequests`	Jumlah label yang ditambahkan ke permintaan web oleh aturan grup aturan yang memiliki pengaturan Count tindakan. Metrik ini hanya tersedia untuk pemilik grup aturan, untuk aturan di dalam grup aturan. Untuk kasus lain, metrik label hitungan digulung ke dalam tindakan penghentian yang diterapkan pada permintaan, seperti Allow atau. Block Kriteria pelaporan: Ada nilai bukan nol. Statistik yang valid: Jumlah
`CaptchaRequests`	Jumlah label pada permintaan web yang memiliki CAPTCHA tindakan penghentian diterapkan. Label dapat ditambahkan kapan saja selama evaluasi permintaan web. Kriteria pelaporan: Ada nilai bukan nol. Statistik yang valid: Jumlah

Metrik	Deskripsi
`ChallengeRequests`	Jumlah label pada permintaan web yang memiliki Challenge tindakan penghentian diterapkan. Label dapat ditambahkan kapan saja selama evaluasi permintaan web. Kriteria pelaporan: Ada nilai bukan nol. Statistik yang valid: Jumlah
`AllowRuleMatch`	Jumlah aturan yang cocok yang menghasilkan label terkait dan mengakhiri evaluasi permintaan dengan tindakanAllow. Kriteria pelaporan: Ada nilai bukan nol. Statistik yang valid: Jumlah
`BlockRuleMatch`	Jumlah aturan yang cocok yang menghasilkan label terkait dan mengakhiri evaluasi permintaan dengan Block tindakan. Kriteria pelaporan: Ada nilai bukan nol. Statistik yang valid: Jumlah
`CountRuleMatch`	Jumlah aturan yang cocok yang menghasilkan label terkait dan menerapkan Count tindakan. Satu permintaan dapat menghasilkan beberapa contoh metrik ini, jika beberapa aturan dikonfigurasi dengan label dan tindakan yang sama. Kriteria pelaporan: Ada nilai bukan nol. Statistik yang valid: Jumlah

Metrik	Deskripsi
`CaptchaRuleMatch`	Jumlah aturan yang cocok yang menghasilkan label terkait dan mengakhiri evaluasi permintaan dengan CAPTCHA tindakan. Kriteria pelaporan: Ada nilai bukan nol. Statistik yang valid: Jumlah
`ChallengeRuleMatch`	Jumlah aturan yang cocok yang menghasilkan label terkait dan mengakhiri evaluasi permintaan dengan Challenge tindakan. Kriteria pelaporan: Ada nilai bukan nol. Statistik yang valid: Jumlah
`CaptchaRuleMatchWithValidToken`	Jumlah aturan yang cocok yang menghasilkan label terkait dan menerapkan tindakan non-penghentianCAPTCHA. Satu permintaan dapat menghasilkan beberapa contoh metrik ini, jika beberapa aturan dikonfigurasi dengan label dan tindakan yang sama. Kriteria pelaporan: Ada nilai bukan nol. Statistik yang valid: Jumlah

Metrik	Deskripsi
`ChallengeRuleMatchWithValidToken`	Jumlah aturan yang cocok yang menghasilkan label terkait dan menerapkan tindakan non-penghentianChallenge. Satu permintaan dapat menghasilkan beberapa contoh metrik ini, jika beberapa aturan dikonfigurasi dengan label dan tindakan yang sama. Kriteria pelaporan: Ada nilai bukan nol. Statistik yang valid: Jumlah

Dimensi label

Dimensi	Deskripsi
`Region`	Diperlukan untuk semua jenis sumber daya yang dilindungi kecuali untuk CloudFront distribusi Amazon.
`WebACL`	Nama metrik dari`WebACL`.
`RuleGroup`	Nama metrik dari`RuleGroup` . Digunakan untuk metrik`CountedRequests` .
`LabelNamespace`	Awalan namespace label yang ditambahkan ke permintaan.
`Label`	Nama label yang ditambahkan ke permintaan.
`Context`	Grup aturan terkelola yang berfungsi sebagai konteks penambahan label. Misalnya, konteks untuk label manajemen token seperti `awswaf:managed:token:accepted` adalah grup aturan AWS WAF terkelola yang menggunakan manajemen token pada permintaan, seperti Bot Control atau grup

Dimensi	Deskripsi
	aturan terkelola ATP. Dimensi ini tidak berlaku untuk semua label.

Metrik dan dimensi visibilitas bot gratis

Bila Anda tidak menggunakan Kontrol Bot di ACL web Anda, AWS WAF terapkan grup aturan terkelola Kontrol Bot ke pengambilan sampel permintaan web Anda, tanpa biaya tambahan. Ini dapat memberikan gambaran tentang lalu lintas bot yang datang ke sumber daya Anda yang dilindungi. Untuk informasi tentang Kontrol Bot, lihatAWS WAF Grup aturan Bot Control.

Metrik visibilitas bot gratis

Metrik	Deskripsi
`SampleAllowedRequest`	Jumlah permintaan sampel yang memiliki Allow tindakan. Kriteria pelaporan: Ada nilai bukan nol. Statistik yang valid: Jumlah
`SampleBlockedRequest`	Jumlah permintaan sampel yang memiliki Block tindakan. Kriteria pelaporan: Ada nilai bukan nol. Statistik yang valid: Jumlah
`SampleCaptchaRequest`	Jumlah permintaan sampel yang memiliki CAPTCHA tindakan. Kriteria pelaporan: Ada nilai bukan nol. Statistik yang valid: Jumlah
`SampleChallengeRequest`	Jumlah permintaan sampel yang memiliki Challenge tindakan. Kriteria pelaporan: Ada nilai bukan nol.

Metrik	Deskripsi
	Statistik yang valid: Jumlah
`SampleCountRequest`	Jumlah permintaan sampel yang memiliki Count tindakan. Kriteria pelaporan: Ada nilai bukan nol. Statistik yang valid: Jumlah

Dimensi visibilitas bot gratis

Dimensi	Deskripsi
`Region`	Diperlukan untuk semua jenis sumber daya yang dilindungi kecuali untuk CloudFront distribusi Amazon.
`WebACL`	Nama metrik dari`WebACL`.
`BotCategory`	Nama kategori bot yang terdeteksi, berdasarkan label permintaan web.
`VerificationStatus`	Nama status verifikasi bot yang terdeteksi, berdasark an label permintaan web.
`Signal`	Nama sinyal bot yang terdeteksi, berdasarkan label permintaan web.

AWS Shield Advanced metrik

Shield Advanced menerbitkan metrik CloudWatch deteksi, mitigasi, dan kontributor teratas Amazon untuk semua sumber daya yang dilindunginya. Metrik ini meningkatkan kemampuan Anda untuk memantau sumber daya Anda dengan memungkinkan untuk membuat dan mengonfigurasi CloudWatch dasbor dan alarm untuk mereka.

Konsol Shield Advanced menyajikan ringkasan dari banyak metrik yang direkam. Untuk informasi, lihat Visibilitas ke acara DDoS.

Jika Anda mengaktifkan mitigasi DDoS lapisan aplikasi otomatis untuk perlindungan lapisan aplikasi,

Lokasi pelaporan metrik

Shield Advanced melaporkan metrik di Wilayah AS Timur (Virginia Utara), `us-east-1` untuk hal berikut:

- Layanan global Amazon CloudFront dan Amazon Route 53.
- Kelompok perlindungan. Untuk informasi tentang grup perlindungan, lihatAWS Shield Advanced kelompok perlindungan.

Untuk jenis sumber daya lainnya, Shield Advanced melaporkan metrik di Wilayah sumber daya.

Waktu pelaporan metrik

Shield Advanced melaporkan metrik ke Amazon CloudWatch pada AWS sumber daya lebih sering selama peristiwa DDoS daripada saat tidak ada acara yang sedang berlangsung. Shield Advanced melaporkan metrik satu menit sekali selama acara, dan kemudian sekali tepat setelah acara berakhir.

Meskipun tidak ada peristiwa yang sedang berlangsung, Shield Advanced melaporkan metrik sekali sehari, pada waktu yang ditetapkan ke sumber daya. Laporan berkala ini membuat metrik tetap aktif dan tersedia untuk digunakan di CloudWatch alarm dan dasbor khusus.

Rekomendasi alarm

Kami menyarankan Anda membuat alarm untuk memberi tahu Anda tentang keadaan yang memerlukan perhatian. Sebagai titik awal, Anda dapat membuat alarm untuk setiap sumber daya yang dilindungi yang melaporkan saat metrik `DDoSDetected` deteksi bukan nol. Nilai bukan nol dalam metrik ini tidak selalu menyiratkan bahwa serangan DDoS sedang berlangsung, tetapi kami sarankan untuk melihat lebih dekat status sumber daya saat metrik berada dalam keadaan ini.

Untuk banjir permintaan, kami menyarankan Anda membuat alarm untuk pemeriksaan komposit yang juga mempertimbangkan faktor-faktor seperti kesehatan aplikasi dan volume permintaan web. Anda dapat memilih untuk alarm pada tiga metrik lainnya yang melaporkan volume lalu lintas untuk berbagai dimensi vektor serangan. Dengan mempertimbangkan kapasitas aplikasi Anda dan mengkhawatirkan ketika lalu lintas mendekati batasan aplikasi Anda, Anda dapat membuat seperangkat aturan yang memberi tahu Anda sesuai kebutuhan, tanpa terlalu banyak kebisingan yang tidak diinginkan.

Topik

Metrik deteksi

Shield Advanced menyediakan metrik dan dimensi di `AWS/DDoSProtection` namespace.

Metrik deteksi

Metrik	Deskripsi
`DDoSDetected`	Menunjukkan apakah peristiwa DDoS sedang berlangsung untuk Amazon Resource Name (ARN) tertentu. Metrik ini memiliki nilai bukan nol selama suatu peristiwa.
`DDoSAttackBitsPerSecond`	Jumlah bit yang diamati selama acara DDoS untuk Amazon Resource Name (ARN) tertentu. Metrik ini hanya tersedia untuk peristiwa DDoS lapisan jaringan dan transport (lapisan 3 dan lapisan 4). Metrik ini memiliki nilai bukan nol selama suatu peristiwa. Unit: Bits
`DDoSAttackPacketsPerSecond`	Jumlah paket yang diamati selama acara DDoS untuk Amazon Resource Name (ARN) tertentu. Metrik ini hanya tersedia untuk peristiwa DDoS lapisan jaringan dan transport (lapisan 3 dan lapisan 4). Metrik ini memiliki nilai bukan nol selama suatu peristiwa.

Metrik	Deskripsi
	Unit: Paket
DDoSAttackRequestsPerSecond	Jumlah permintaan yang diamati selama acara DDoS untuk Amazon Resource Name (ARN) tertentu. Metrik ini hanya tersedia untuk peristiwa DDoS layer 7. Metrik dilaporkan hanya untuk peristiwa lapisan 7 yang paling signifikan. Metrik ini memiliki nilai bukan nol selama suatu peristiwa. Unit: Permintaan

Shield Advanced memposting DDoSDetected metrik tanpa dimensi lain. Metrik deteksi yang tersisa mencakup AttackVector dimensi yang sesuai dengan jenis serangan, dari daftar berikut:

- ACKFlood
- ChargenReflection
- DNSReflection
- GenericUDPReflection
- MemcachedReflection
- MSSQLReflection
- NetBIOSReflection
- NTPReflection
- PortMapper
- RequestFlood
- RIPReflection
- SNMPReflection
- SSDPReflection
- SYNFlood
- UDPFragment

- `UDPTraffic`
- `UDPReflection`

Metrik mitigasi

Shield Advanced menyediakan metrik dan dimensi di `AWS/DDoSProtection` namespace.

Metrik mitigasi

Metrik	Deskripsi
`VolumePacketsPerSecond`	Jumlah paket per detik yang dijatuhkan atau dilewatkan oleh mitigasi yang digunakan sebagai respons terhadap peristiwa yang terdeteksi. Unit: paket

Dimensi mitigasi

Dimensi	Deskripsi
`ResourceArn`	Amazon Resource Name (ARN)
`MitigationAction`	Hasil dari mitigasi yang diterapkan. Nilai yang mungkin adalah `Pass` atau`Drop`.

Metrik kontributor teratas

Shield Advanced menyediakan metrik di `AWS/DDoSProtection` namespace.

Metrik kontributor teratas

Metrik	Deskripsi
`VolumePacketsPerSecond`	Jumlah paket per detik untuk kontributor teratas. Unit: paket

Metrik	Deskripsi
VolumeBitsPerSecond	Jumlah bit per detik untuk kontributor teratas. Unit: bit

Shield Advanced memposting metrik kontributor teratas berdasarkan kombinasi dimensi yang menjadi ciri kontributor acara. Anda dapat menggunakan salah satu kombinasi dimensi berikut untuk salah satu metrik kontributor teratas:

- ResourceArn, Protocol
- ResourceArn, Protocol, SourcePort
- ResourceArn, Protocol, DestinationPort
- ResourceArn, Protocol, SourceIp
- ResourceArn, Protocol, SourceAsn
- ResourceArn, TcpFlags

Dimensi kontributor teratas

Dimensi	Deskripsi
ResourceArn	Nama Sumber Daya Amazon (ARN).
Protocol	Nama protokol IP, salah satu TCP atauUDP.
SourcePort	Sumber TCP atau port UDP.
DestinationPort	Port TCP atau UDP tujuan.
SourceIp	Alamat IP sumber.
SourceAsn	Nomor sistem otonom sumber (ASN).
TcpFlags	Kombinasi flag hadir dalam paket TCP, dipisahka n oleh tanda hubung (). - Bendera yang dipantau adalahACK,,FIN,RST. SYN Nilai dimensi ini selalu

Dimensi	Deskripsi
	muncul diurutkan menurut abjad. Misalnya,`ACK-FIN-RST-SYN` ,`ACK-SYN`, dan`FIN-RST`.

AWS Firewall Manager pemberitahuan

AWS Firewall Manager tidak merekam metrik, jadi Anda tidak dapat membuat CloudWatch alarm Amazon khusus untuk Firewall Manager. Namun, Anda dapat mengonfigurasi notifikasi Amazon SNS untuk mengingatkan Anda tentang potensi serangan. Untuk membuat notifikasi Amazon SNS di Firewall Manager, lihat. Langkah 4: Konfigurasikan notifikasi Amazon SNS dan alarm Amazon CloudWatch

Logging panggilan API dengan AWS CloudTrail

AWS WAF, AWS Shield Advanced, dan AWS Firewall Manager terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan. CloudTrail menangkap subset panggilan API untuk layanan ini sebagai peristiwa, termasuk panggilan dari konsol, AWS WAF Shield Advanced atau Firewall Manager dan dari panggilan kode ke API, AWS WAF Shield Advanced, atau Firewall Manager. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail peristiwa secara terus menerus ke bucket Amazon S3, termasuk peristiwa untuk, AWS WAF Shield Advanced, atau Firewall Manager. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat untuk layanan ini, alamat IP tempat permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, termasuk cara mengonfigurasi dan mengaktifkannya, lihat Panduan AWS CloudTrail Pengguna.

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas peristiwa yang didukung terjadi di AWS WAF, Shield Advanced, atau Firewall Manager, aktivitas tersebut direkam dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di situs Anda Akun AWS. Untuk informasi selengkapnya, lihat Melihat Acara dengan Riwayat CloudTrail Acara.

Untuk catatan peristiwa yang sedang berlangsung di Anda Akun AWS, termasuk acara untuk AWS WAF, Shield Advanced, atau Firewall Manager, buat jejak. Jejak memungkinkan CloudTrail untuk

mengirimkan file log ke bucket Amazon S3. Secara default, ketika Anda membuat jejak pada konsol tersebut, jejak diterapkan ke semua Wilayah . Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- Gambaran umum untuk Membuat Jejak
- CloudTrail Layanan dan Integrasi yang Didukung
- Mengkonfigurasi Notifikasi Amazon SNS untuk CloudTrail
- Menerima File CloudTrail Log dari Beberapa Wilayah dan Menerima File CloudTrail Log dari Beberapa Akun

AWS WAF informasi di AWS CloudTrail

Semua AWS WAF tindakan dicatat oleh AWS CloudTrail dan didokumentasikan dalam Referensi AWS WAF API. Misalnya, panggilan ke`ListWebACL`,`UpdateWebACL`, dan `DeleteWebACL` menghasilkan entri dalam file CloudTrail log.

Setiap entri peristiwa atau log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut ini:

- Apakah permintaan dibuat dengan kredensil pengguna root
- Baik permintaan tersebut dibuat dengan kredensial keamanan sementara untuk peran atau pengguna gabungan
- Apakah permintaan itu dibuat oleh AWS layanan lain

Untuk informasi selengkapnya, lihat Elemen CloudTrailUserIdentity.

Contoh: entri file AWS WAF log

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. AWS CloudTrail file log berisi satu atau lebih entri log. Peristiwa merepresentasikan satu permintaan dari sumber apa pun dan menyertakan informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, sehingga file tersebut tidak muncul dalam urutan tertentu.

Berikut ini adalah contoh entri CloudTrail log untuk operasi ACL AWS WAF web.

Contoh: entri CloudTrail log untuk `CreateWebACL`


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T03:43:07Z"
      }
    }
  },
  "eventTime": "2019-11-06T03:44:21Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "CreateWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "defaultAction": {
      "block": {}
    },
    "description": "foo",
    "rules": [
      {
        "name": "foo",
```

```
        "priority": 1,
        "statement": {
          "geoMatchStatement": {
            "countryCodes": [
              "AF",
              "AF"
            ]
          }
        },
        "action": {
          "block": {}
        },
        "visibilityConfig": {
          "sampledRequestsEnabled": true,
          "cloudWatchMetricsEnabled": true,
          "metricName": "foo"
        }
      }
    ],
    "visibilityConfig": {
      "sampledRequestsEnabled": true,
      "cloudWatchMetricsEnabled": true,
      "metricName": "foo"
    }
  },
  "responseElements": {
    "summary": {
      "name": "foo",
      "id": "ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b",
      "description": "foo",
      "lockToken": "67551e73-49d8-4363-be48-244deea72ea9",
      "aRN": "arn:aws:wafv2:us-east-1:112233445566:global/webacl/foo/
ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b"
    }
  },
  "requestID": "c51521ba-3911-45ca-ba77-43aba50471ca",
  "eventID": "afd1a60a-7d84-417f-bc9c-7116cf029065",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```


Contoh: entri CloudTrail log untuk `GetWebACL`

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AssumedRole",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin/admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AssumedRole",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T19:17:20Z"
      }
    }
  },
  "eventTime": "2019-11-06T19:18:28Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "GetWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "webacl"
  },
  "responseElements": null,
  "requestID": "f2db4884-4eeb-490c-afe7-67cbb494ce3b",
  "eventID": "7d563cd6-4123-4082-8880-c2d1fda4d90b",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

Contoh: entri CloudTrail log untuk `UpdateWebACL`


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T19:17:20Z"
      }
    }
  },
  "eventTime": "2019-11-06T19:20:56Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "UpdateWebACL",
  "awsRegion": ""us-east-1,
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b",
    "defaultAction": {
      "block": {}
    },
    "description": "foo",
    "rules": [
      {
        "name": "foo",
        "priority": 1,
```

```
        "statement": {
          "geoMatchStatement": {
            "countryCodes": [
              "AF"
            ]
          }
        },
        "action": {
          "block": {}
        },
        "visibilityConfig": {
          "sampledRequestsEnabled": true,
          "cloudWatchMetricsEnabled": true,
          "metricName": "foo"
        }
      }
    ],
    "visibilityConfig": {
      "sampledRequestsEnabled": true,
      "cloudWatchMetricsEnabled": true,
      "metricName": "foo"
    },
    "lockToken": "67551e73-49d8-4363-be48-244deea72ea9"
  },
  "responseElements": {
    "nextLockToken": "a6b54c01-7975-4e6d-b7d0-2653cb6e231d"
  },
  "requestID": "41c96e12-9790-46ab-b145-a230f358f2c2",
  "eventID": "517a10e6-4ca9-4828-af90-a5cff9756594",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

Contoh: entri CloudTrail log untuk `DeleteWebACL`

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin/session-name",
    "accountId": "112233445566",
```

```
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T19:17:20Z"
      }
    }
  },
  "eventTime": "2019-11-06T19:25:17Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "DeleteWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b",
    "lockToken": "a6b54c01-7975-4e6d-b7d0-2653cb6e231d"
  },
  "responseElements": null,
  "requestID": "71703f89-e139-440c-96d4-9c77f4cd7565",
  "eventID": "2f976624-b6a5-4a09-a8d0-aa3e9f4e5187",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```


Contoh: entri file log AWS WAF klasik

AWS WAF Klasik adalah versi sebelumnya AWS WAF. Untuk informasi, lihat AWS WAF Klasik.

Entri log menunjukkan`CreateRule`,, `GetRuleUpdateRule`, dan `DeleteRule` operasi:

```
{
  "Records": [
   {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:14Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "CreateRule",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
        "name": "0923ab32-7229-49f0-a0e3-66c81example",
        "changeToken": "l9434322-8685-4ed2-9c5b-9410bexample",
        "metricName": "0923ab32722949f0a0e366c81example"
      },
      "responseElements": {
        "rule": {
          "metricName": "0923ab32722949f0a0e366c81example",
          "ruleId": "12132e64-6750-4725-b714-e7544example",
          "predicates": [

          ],
          "name": "0923ab32-7229-49f0-a0e3-66c81example"
        },
        "changeToken": "l9434322-8685-4ed2-9c5b-9410bexample"
      },
      "requestID": "4e6b66f9-d548-11e3-a8a9-73e33example",
      "eventID": "923f4321-d378-4619-9b72-4605bexample",
      "eventType": "AwsApiCall",
      "apiVersion": "2015-08-24",
      "recipientAccountId": "777777777777"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
```

```
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:22Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "GetRule",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
        "ruleId": "723c2943-82dc-4bc1-a29b-c7d73example"
      },
      "responseElements": null,
      "requestID": "8e4f3211-d548-11e3-a8a9-73e33example",
      "eventID": "an236542-d1f9-4639-bb3d-8d2bbexample",
      "eventType": "AwsApiCall",
      "apiVersion": "2015-08-24",
      "recipientAccountId": "777777777777"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:13Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "UpdateRule",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
        "ruleId": "7237b123-7903-4d9e-8176-9d71dexample",
        "changeToken": "32343a11-35e2-4dab-81d8-6d408example",
        "updates": [
          {
```

```
            "predicate": {
              "type": "SizeConstraint",
              "dataId": "9239c032-bbbe-4b80-909b-782c0example",
              "negated": false
            },
            "action": "INSERT"
          }
        ]
      },
      "responseElements": {
        "changeToken": "32343a11-35e2-4dab-81d8-6d408example"
      },
      "requestID": "11918283-0b2d-11e6-9ccc-f9921example",
      "eventID": "00032abc-5bce-4237-a8ee-5f1a9example",
      "eventType": "AwsApiCall",
      "apiVersion": "2015-08-24",
      "recipientAccountId": "777777777777"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:28Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "DeleteRule",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
        "changeToken": "fd232003-62de-4ea3-853d-52932example",
        "ruleId": "3e3e2d11-fd8b-4333-8b03-1da95example"
      },
      "responseElements": {
        "changeToken": "fd232003-62de-4ea3-853d-52932example"
      },
      "requestID": "b23458a1-0b2d-11e6-9ccc-f9928example",
      "eventID": "a3236565-1a1a-4475-978e-81c12example",
      "eventType": "AwsApiCall",
```

```
      "apiVersion": "2015-08-24",
      "recipientAccountId": "777777777777"
    }
  ]
}
```

AWS Shield Advanced informasi di CloudTrail

AWS Shield Advanced mendukung pencatatan tindakan berikut sebagai peristiwa dalam file CloudTrail log:

- ListAttacks
- DescribeAttack
- CreateProtection
- DescribeProtection
- DeleteProtection
- ListProtections
- CreateSubscription
- DescribeSubscription
- GetSubscriptionState

Setiap peristiwa atau entri log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut:

- Apakah permintaan dibuat dengan kredensi pengguna root
- Apakah permintaan dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat Elemen CloudTrail UserIdentity.

Contoh: Shield Advanced log file entri

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili

permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, sehingga file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `DeleteProtection` dan `ListProtections` tindakan.


```
[
 {
   "eventVersion": "1.05",
   "userIdentity": {
     "type": "IAMUser",
     "principalId": "123456789098765432123l",
     "arn": "arn:aws:iam::123456789012:user/SampleUser",
     "accountId": "123456789012",
     "accessKeyId": "1AFGDT647FHU83JHFI81H",
     "userName": "SampleUser"
   },
   "eventTime": "2018-01-10T21:31:14Z",
   "eventSource": "shield.amazonaws.com",
   "eventName": "DeleteProtection",
   "awsRegion": "us-east-1",
   "sourceIPAddress": "AWS Internal",
   "userAgent": "aws-cli/1.14.10 Python/3.6.4 Darwin/16.7.0 botocore/1.8.14",
   "requestParameters": {
     "protectionId": "12345678-5104-46eb-bd03-agh4j8rh3b6n"
   },
   "responseElements": null,
   "requestID": "95bc0042-f64d-11e7-abd1-1babdc7aa857",
   "eventID": "85263bf4-17h4-43bb-b405-fh84jhd8urhg",
   "eventType": "AwsApiCall",
   "apiVersion": "AWSShield_20160616",
   "recipientAccountId": "123456789012"
 },
 {
   "eventVersion": "1.05",
   "userIdentity": {
     "type": "IAMUser",
     "principalId": "123456789098765432123",
     "arn": "arn:aws:iam::123456789012:user/SampleUser",
```

```
      "accountId": "123456789012",
      "accessKeyId": "1AFGDT647FHU83JHFI81H",
      "userName": "SampleUser"
    },
    "eventTime": "2018-01-10T21:30:03Z",
    "eventSource": "shield.amazonaws.com",
    "eventName": "ListProtections",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "aws-cli/1.14.10 Python/3.6.4 Darwin/16.7.0 botocore/1.8.14",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "6accca40-f64d-11e7-abd1-1bjfi8urhj47",
    "eventID": "ac0570bd-8dbc-41ac-a2c2-987j90j3h78f",
    "eventType": "AwsApiCall",
    "apiVersion": "AWSShield_20160616",
    "recipientAccountId": "123456789012"
  }
]
```


AWS Firewall Manager informasi di CloudTrail

AWS Firewall Manager mendukung pencatatan tindakan berikut sebagai peristiwa dalam file CloudTrail log:

- AssociateAdminAccount
- DeleteNotificationChannel
- DeletePolicy
- DisassociateAdminAccount
- PutNotificationChannel
- PutPolicy
- GetAdminAccount
- GetComplianceDetail
- GetNotificationChannel
- GetPolicy
- ListComplianceStatus
- ListPolicies

Setiap peristiwa atau entri log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut:

- Apakah permintaan dibuat dengan kredensi pengguna root
- Apakah permintaan dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat Elemen CloudTrail UserIdentity.

Contoh: entri file log Firewall Manager

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, sehingga file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `GetAdminAccount` --> tindakan.

```
 {
                "eventVersion": "1.05",
                "userIdentity": {
                                "type": "AssumedRole",
                                "principalId": "123456789098765432123",
                                "arn": "arn:aws:sts::123456789012:assumed-role/Admin/
SampleUser",
                                "accountId": "123456789012",
                                "accessKeyId": "1AFGDT647FHU83JHFI81H",
                                "sessionContext": {
                                                "attributes": {
                                                                "mfaAuthenticated":
 "false",
                                                                "creationDate":
 "2018-04-14T02:51:50Z"
                                                },
                                                "sessionIssuer": {
```

```
                                                                "type": "Role",
                                                                "principalId":
"123456789098765432123 1",
                                                                "arn":
"arn:aws:iam::123456789012:role/Admin",
                                                                "accountId":
"123456789012",
                                                                "userName": "Admin"
                                                                 }
                                                    }
                                },
                "eventTime": "2018-04-14T03:12:35Z",
                "eventSource": "fms.amazonaws.com",
                "eventName": "GetAdminAccount",
                "awsRegion": "us-east-1",
                "sourceIPAddress": "72.21.198.65",
                "userAgent": "console.amazonaws.com",
                "requestParameters": null,
                "responseElements": null,
                "requestID": "ae244f41-3f91-11e8-787b-dfaafef95fc1",
                "eventID": "5769af1e-14b1-4bd1-ba75-f023981d0a4a",
                "eventType": "AwsApiCall",
                "apiVersion": "2018-01-01",
                "recipientAccountId": "123456789012"
    }
```

Menggunakan AWS WAF dan AWS Shield Advanced API

Bagian ini menjelaskan cara membuat permintaan ke AWS WAF dan Shield Advanced API untuk membuat dan mengelola set kecocokan, aturan, dan ACL web AWS WAF serta langganan dan perlindungan Anda di Shield Advanced. Bagian ini akan memperkenalkan Anda dengan komponen permintaan, isi tanggapan, dan cara mengotentikasi permintaan.

Topik

Menggunakan AWS SDK

Jika Anda menggunakan bahasa yang AWS menyediakan SDK, gunakan SDK daripada mencoba mengerjakan API. SDK membuat otentikasi lebih sederhana, terintegrasi dengan mudah dengan lingkungan pengembangan Anda, dan menyediakan akses mudah ke dan perintah AWS WAF Shield Advanced. Untuk informasi selengkapnya tentang AWS SDK, lihat Unduh alat di topikMenyiapkan akun Anda untuk menggunakan layanan.

Membuat permintaan HTTPS ke AWS WAF atau Shield Advanced

AWS WAF dan Permintaan Shield Advanced adalah permintaan HTTPS, seperti yang didefinisikan oleh RFC 2616. Seperti permintaan HTTP lainnya, permintaan ke AWS WAF atau Shield Advanced berisi metode permintaan, URI, header permintaan, dan badan permintaan. Respons berisi kode status HTTP, header respons, dan terkadang badan respons.

Permintaan URI

URI permintaan selalu berupa garis miring tunggal,/.

Header HTTP

AWS WAF dan Shield Advanced memerlukan informasi berikut di header permintaan HTTP:

Host (Diperlukan)

Titik akhir yang menentukan di mana sumber daya Anda dibuat. Untuk informasi tentang titik akhir, lihat titik akhir AWS layanan. Misalnya, nilai `Host` header AWS WAF untuk CloudFront distribusi adalah`waf.amazonaws.com:443`.

x-amz-date atau Tanggal (Wajib)

Tanggal yang digunakan untuk membuat tanda tangan yang terdapat di `Authorization` header. Tentukan tanggal dalam format standar ISO 8601, dalam waktu UTC, seperti yang ditunjukkan pada contoh berikut:

```
x-amz-date: 20151007T174952Z
```

Anda harus menyertakan `x-amz-date` atau `Date`. (Beberapa pustaka klien HTTP tidak mengizinkan Anda mengatur `Date` header). Saat `x-amz-date` header hadir, AWS WAF abaikan `Date` header apa pun saat mengautentikasi permintaan.

Cap waktu harus dalam waktu 15 menit dari waktu AWS sistem ketika permintaan diterima. Jika tidak, permintaan gagal dengan kode `RequestExpired` kesalahan untuk mencegah orang lain memutar ulang permintaan Anda.

Otorisasi (Diperlukan)

Informasi yang diperlukan untuk otentikasi permintaan. Untuk informasi selengkapnya tentang membuat header ini, lihatMengautentikasi permintaan.

X-Amz-Target (Diperlukan)

Rangkaian `AWSWAF_` atau`AWSShield_`, versi API tanpa tanda baca, periode (`.`), dan nama operasi, misalnya:

`AWSWAF_20150824.CreateWebACL`

Tipe Konten (Bersyarat)

Menentukan bahwa jenis konten adalah JSON serta versi JSON, seperti yang ditunjukkan pada contoh berikut:

```
Content-Type: application/x-amz-json-1.1
```

Kondisi: Diperlukan untuk `POST` permintaan.

Panjang Konten (Bersyarat)

Panjang pesan (tanpa header) menurut RFC 2616.

Kondisi: Diperlukan jika badan permintaan itu sendiri berisi informasi (sebagian besar toolkit menambahkan header ini secara otomatis).

Berikut ini adalah contoh header untuk permintaan HTTP untuk membuat web ACL di AWS WAF:

```
POST / HTTP/1.1
Host: waf.amazonaws.com:443
X-Amz-Date: 20151007T174952Z
Authorization: AWS4-HMAC-SHA256
               Credential=AccessKeyID/20151007/us-east-2/waf/aws4_request,
               SignedHeaders=host;x-amz-date;x-amz-target,

 Signature=145b1567ab3c50d929412f28f52c45dbf1e63ec5c66023d232a539a4afd11fd9
X-Amz-Target: AWSWAF_20150824.CreateWebACL
Accept: */*
Content-Type: application/x-amz-json-1.1; charset=UTF-8
Content-Length: 231
Connection: Keep-Alive
```

Badan permintaan HTTP

Banyak AWS WAF tindakan Shield Advanced API mengharuskan Anda untuk menyertakan data berformat JSON di badan permintaan.

Contoh permintaan berikut menggunakan pernyataan JSON sederhana untuk memperbarui `IPSet` untuk menyertakan alamat IP 192.0.2.44 (diwakili dalam notasi CIDR sebagai 192.0.2.44/32):

```
POST / HTTP/1.1
Host: waf.amazonaws.com:443
X-Amz-Date: 20151007T174952Z
Authorization: AWS4-HMAC-SHA256
               Credential=AccessKeyID/20151007/us-east-2/waf/aws4_request,
               SignedHeaders=host;x-amz-date;x-amz-target,

 Signature=145b1567ab3c50d929412f28f52c45dbf1e63ec5c66023d232a539a4afd11fd9
X-Amz-Target: AWSWAF_20150824.UpdateIPSet
Accept: */*
Content-Type: application/x-amz-json-1.1; charset=UTF-8
```

```
Content-Length: 283
Connection: Keep-Alive

{
   "ChangeToken": "d4c4f53b-9c7e-47ce-9140-0ee5ffffffff",
   "IPSetId": "69d4d072-170c-463d-ab82-0643ffffffff",
   "Updates": [
      {
         "Action": "INSERT",
         "IPSetDescriptor": {
            "Type": "IPV4",
            "Value": "192.0.2.44/32"
         }
      }
   ]
}
```

Tanggapan HTTP

Semua tindakan API Lanjutan AWS WAF dan Shield menyertakan data berformat JSON dalam respons.

Berikut adalah beberapa header penting dalam respons HTTP dan bagaimana Anda harus menanganinya dalam aplikasi Anda, jika berlaku:

HTTP/1.1

Header ini diikuti oleh kode status. Kode status 200 menunjukkan operasi yang berhasil.

Jenis: String

x-amzn- RequestId

Nilai yang dibuat oleh AWS WAF atau Shield Advanced yang secara unik mengidentifikasi permintaan Anda, misalnya,. `K2QH8DN0U907N97FNA2GDLL80BVV4KQNSO5AEMVJF66Q9ASUAAJG` Jika Anda memiliki masalah dengan AWS WAF, AWS dapat menggunakan nilai ini untuk memecahkan masalah.

Jenis: String

Content-Length

Panjang badan respons dalam byte.

Jenis: String

Tanggal

Tanggal dan waktu yang ditanggapi AWS WAF atau Shield Advanced, misalnya, Rabu, 07 Okt 2015 12:00:00 GMT.

Jenis: String

Tanggapan kesalahan

Jika permintaan menghasilkan kesalahan, respons HTTP berisi nilai-nilai berikut:

- Dokumen kesalahan JSON sebagai badan respons
- Content-Type
- Kode status HTTP 3xx, 4xx, atau 5xx yang berlaku

Berikut ini adalah contoh dokumen kesalahan JSON:

```
HTTP/1.1 400 Bad Request
x-amzn-RequestId: b0e91dc8-3807-11e2-83c6-5912bf8ad066
x-amzn-ErrorType: ValidationException
Content-Type: application/json
Content-Length: 125
Date: Mon, 26 Nov 2012 20:27:25 GMT

{"message":"1 validation error detected: Value null at 'TargetString' failed to satisfy
 constraint: Member must not be null"}
```

Mengautentikasi permintaan

Jika Anda menggunakan bahasa yang AWS menyediakan SDK, sebaiknya gunakan SDK. Semua AWS SDK sangat menyederhanakan proses penandatanganan permintaan dan menghemat banyak waktu jika dibandingkan dengan menggunakan atau AWS WAF Shield Advanced API. Selain itu, SDK terintegrasi dengan mudah dengan lingkungan pengembangan Anda dan menyediakan akses mudah ke perintah terkait.

AWS WAF dan Shield Advanced mengharuskan Anda mengautentikasi setiap permintaan yang Anda kirim dengan menandatangani permintaan. Untuk menandatangani permintaan, Anda

menghitung tanda tangan digital menggunakan fungsi hash kriptografi, yang mengembalikan nilai hash berdasarkan input. Input termasuk teks permintaan Anda dan kunci akses rahasia Anda. Fungsi hash mengembalikan nilai hash yang Anda sertakan dalam permintaan sebagai tanda tangan Anda. Tanda tangan adalah bagian header `Authorization` dari permintaan Anda.

Setelah menerima permintaan Anda, AWS WAF atau Shield Advanced menghitung ulang tanda tangan menggunakan fungsi hash yang sama dan masukan yang Anda gunakan untuk menandatangani permintaan. Jika tanda tangan yang dihasilkan cocok dengan tanda tangan dalam permintaan, AWS WAF atau Shield Advanced memproses permintaan. Jika tidak, permintaan ditolak.

AWS WAF dan Shield Advanced mendukung otentikasi menggunakan AWS Signature Version 4. Proses untuk menghitung tanda tangan dapat dibagi menjadi tiga tugas:

Tugas 1: Buat Permintaan Canonical

Buat permintaan HTTP Anda dalam format kanonik seperti yang dijelaskan dalam Tugas 1: Buat Permintaan Kanonik Untuk Tanda Tangan Versi 4 di. Referensi Umum Amazon Web

Tugas 2: Buat String untuk Ditandatangani

Buat string yang akan Anda gunakan sebagai salah satu nilai input untuk fungsi hash kriptografi Anda. String, yang disebut string untuk ditandatangani, adalah gabungan dari nilai-nilai berikut:

- Nama algoritma hash
- Tanggal permintaan
- String lingkup kredensi
- Permintaan kanonik dari tugas sebelumnya

String lingkup kredensi itu sendiri adalah rangkaian informasi tanggal, wilayah, dan layanan.

Untuk `X-Amz-Credential` parameternya, tentukan yang berikut ini:

- Kode untuk titik akhir yang Anda kirimi permintaan, `us-east-2`
- `waf`untuk singkatan layanan

Sebagai contoh:

```
X-Amz-Credential=AKIAIOSFODNN7EXAMPLE/20130501/us-east-2/waf/
aws4_request
```

Tugas 3: Buat Tanda Tangan

Buat tanda tangan untuk permintaan Anda dengan menggunakan fungsi hash kriptografi yang menerima dua string input:

- String Anda untuk ditandatangani, dari Tugas 2.
- Kunci turunan. Kunci turunan dihitung dengan memulai secret access key Anda dan menggunakan string cakupan kredensial untuk membuat serangkaian kode autentikasi pesan berbasis hash (HMAC).

Informasi terkait

Sumber daya terkait berikut dapat membantu Anda ketika bekerja dengan layanan ini.

Sumber daya berikut tersedia untuk AWS WAF, AWS Shield Advanced, dan AWS Firewall Manager.

- Pedoman Pelaksanaan AWS WAF — Publikasi teknis dengan rekomendasi terkini untuk diterapkan AWS WAF untuk melindungi aplikasi web yang ada dan yang baru.
- AWS forum diskusi — Forum berbasis komunitas untuk mendiskusikan pertanyaan teknis yang terkait dengan ini dan layanan lainnya. AWS
- AWS WAF Forum Diskusi — Forum berbasis komunitas bagi pengembang untuk mendiskusikan pertanyaan teknis yang berkaitan dengan. AWS WAF
- Shield Advanced Discussion Forum — Forum berbasis komunitas bagi pengembang untuk mendiskusikan pertanyaan teknis terkait dengan Shield Advanced.
- AWS WAF informasi produk — Halaman web utama untuk informasi tentang AWS WAF, termasuk fitur, harga, dan banyak lagi.
- Informasi produk Shield Advanced — Halaman web utama untuk informasi tentang Shield Advanced, termasuk fitur, harga, dan lainnya.

Sumber daya berikut tersedia untuk Amazon Web Services.

- Kelas & Lokakarya - Tautan ke kursus berbasis peran dan khusus, selain laboratorium mandiri untuk membantu mempertajam keterampilan Anda AWS dan mendapatkan pengalaman praktis.
- AWS Pusat Pengembang — Jelajahi tutorial, unduh alat, dan pelajari tentang acara AWS pengembang.
- AWS Alat Pengembang - Tautan ke alat pengembang, SDK, toolkit IDE, dan alat baris perintah untuk mengembangkan dan mengelola aplikasi. AWS
- Memulai Pusat Sumber Daya — Pelajari cara menyiapkan Akun AWS, bergabung dengan AWS komunitas, dan meluncurkan aplikasi pertama Anda.
- Hands-On Tutorial - Ikuti step-by-step tutorial untuk meluncurkan aplikasi pertama Anda. AWS
- AWS Whitepaper — Tautan ke daftar lengkap AWS whitepaper teknis, yang mencakup topik-topik seperti arsitektur, keamanan, dan ekonomi dan ditulis oleh AWS Solutions Architects atau pakar teknis lainnya.

- AWS Support Pusat — Hub untuk membuat dan mengelola AWS Support kasus Anda. Juga termasuk tautan ke sumber daya bermanfaat lainnya, seperti forum, FAQ teknis, status kesehatan layanan, dan. AWS Trusted Advisor
- AWS Support— Halaman web utama untuk informasi tentang AWS Support, saluran dukungan respons cepat untuk membantu Anda membangun dan menjalankan aplikasi di cloud. one-on-one
- Hubungi Kami – Titik kontak pusat untuk pertanyaan tentang tandaihan AWS , akun, peristiwa, penyalahgunaan, dan masalah lainnya.
- AWS Ketentuan Situs — Informasi terperinci tentang hak cipta dan merek dagang kami; akun, lisensi, dan akses situs Anda; dan topik lainnya.

Riwayat dokumen

Halaman ini mencantumkan perubahan signifikan pada dokumentasi ini.

Fitur layanan terkadang diluncurkan secara bertahap ke AWS Wilayah tempat layanan tersedia. Kami memperbarui dokumentasi ini hanya untuk rilis pertama. Kami tidak memberikan informasi tentang ketersediaan Wilayah atau mengumumkan peluncuran Wilayah berikutnya. Untuk informasi tentang ketersediaan fitur layanan wilayah dan untuk berlangganan pemberitahuan tentang pembaruan, lihat Apa yang Baru dengan AWS? .

Perubahan	Deskripsi	Tanggal
Klarifikasi cara kerja penguraian tubuh JSON	Cakupan yang diperbarui untuk inspeksi tubuh JSON untuk memperjelas cara AWS WAF menangani penguraian dan perilaku mundur penguraian tubuh.	Juni 25, 2024
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	Memperbarui set aturan sistem operasi Linux.	Juni 6, 2024
AWS WAF perubahan kebijakan terkelola	Diperbarui `WAFV2LoggingServiceRolePolicy` dan `AWSServiceRoleForWAFV2Logging` untuk menambahkan ID Pernyataan (Sids) ke pengaturan izin.	3 Juni 2024
AWS WAF pelacakan perubahan kebijakan terkelola	AWS WAF mulai melacak perubahan untuk kebijakan terkelola `WAFV2LoggingServiceRolePolicy` dan peran terkait layanan. `AWSServiceRoleForWAFV2Logging`	3 Juni 2024

Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	Grup aturan terkelola Bot Control, ATP, dan ACFP sekarang berversi dan akan memberikan notifikasi SNS untuk pembaruan versi, sama seperti Aturan Terkelola berversi lainnya. AWS	29 Mei 2024
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan sistem operasi POSIX, `AWSManagedRulesUnixRuleSet` .	28 Mei 2024
CAPTCHAdan Challenge tindakan	Menambahkan klarifikasi bahwa klien browser memerlukan HTTPS untuk menjalankan teka-teki CAPTCHA dan tantangan diam.	24 Mei 2024
Integrasi dengan Amazon Security Lake	Anda sekarang dapat menggunakan Security Lake untuk mengumpulkan data lalu lintas ACL web. Untuk selengkapnya, lihat Mengumpulkan data dari AWS layanan di panduan pengguna Amazon Security Lake.	22 Mei 2024
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan set aturan inti (CRS).	21 Mei 2024
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan database SQLi.	14 Mei 2024

Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui input buruk yang diketahui dan grup aturan sistem operasi POSIX.	8 Mei 2024
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan sistem operasi Windows.	3 Mei 2024
AWS WAF contoh kode Android Kotlin SDK seluler	Menambahkan kode contoh untuk integrasi Android berbasis Kotlin.	2 Mei 2024
AWS WAF metrik menambahkan dimensi dan metrik baru	AWS WAF menambahkan dimensi baru untuk `ManagedRuleSetRule` metrik aturan dan metrik baru untuk tindakan aturan yang cocok untuk metrik label.	2 Mei 2024
AWS Firewall Manager mendukung kebijakan ACL jaringan	Firewall Manager sekarang mendukung pengelolaan daftar kontrol akses jaringan Amazon VPC (ACL) melalui kebijakan ACL jaringan Firewall Manager.	April 25, 2024
AWS Firewall Manager pembaruan kebijakan keamanan	Pembaruan `FMSServiceRolePolicy` untuk menambahkan izin untuk mengelola ACL jaringan.	April 22, 2024
Daftar metrik pemeriksaan kesehatan yang diperbarui	Kami menghapus beberapa metrik dari daftar metrik yang biasa digunakan dalam pemeriksaan kesehatan.	April 16, 2024

Pembaruan untuk kebijakan grup keamanan Firewall Manager	Kami telah memperbarui kebijakan grup keamanan audit penggunaan kami dan meningkatkan dokumenta si. Lihat bagian kebijakan audit penggunaan dan bagian tentang praktik dan batasan terbaik.	April 2, 2024
Contoh Kontrol Bot yang Diperbarui	Menambahkan contoh yang menggambarkan tingkat inspeksi yang ditargetkan dan memperbarui contoh yang ada untuk mencerminkan praktik terbaik.	Maret 27, 2024
Contoh ATP yang diperbarui	Contoh tambahan yang menggambarkan konfigura si inspeksi respons dan memperbarui contoh yang ada untuk mencerminkan praktik terbaik.	Maret 27, 2024
Contoh ACFP yang diperbarui	Ditambahkan contoh yang menggambarkan konfigurasi inspeksi respon.	Maret 27, 2024
Perbarui batas aliran CloudWatch log Amazon Logs	AWS WAF tidak lagi memiliki batas ACL per web untuk menerbitkan log ke aliran log CloudWatch Log.	Maret 27, 2024

AWS Shield Advanced perlindungan lapisan aplikasi (lapisan 7)	Panduan praktik umum dan terbaik yang diperbarui untuk deteksi dan mitigasi lapisan aplikasi, penggunaan ACL web, aturan berbasis tarif, dan mitigasi DDoS lapisan aplikasi otomatis.	Maret 14, 2024
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan reputasi IP.	Maret 13, 2024
Perubahan batas ukuran inspeksi tubuh	AWS WAF sekarang mendukung batas ukuran inspeksi tubuh yang lebih besar untuk beberapa sumber daya regional.	7 Maret 2024
Jendela evaluasi yang dapat dikonfigurasi untuk aturan berbasis AWS WAF tarif	Anda sekarang dapat mengonfigurasi jendela waktu yang digunakan aturan berbasis tarif untuk menghitung permintaan, menjadi 1, 2, 5, atau 10 menit. Defaultnya adalah 5, yang merupakan satu-satunya pilihan sebelum rilis ini.	Februari 28, 2024

Informasi pencatatan yang diperluas untuk CAPTCHA dan Challenge	Tingkat `captchaResponse` dan `challengeResponse` bidang teratas sekarang diisi dengan tindakan terakhir yang akan diterapkan pada permintaan, baik penghenti an atau non-penghentian. Sebelum ini, bidang-bidang ini diisi hanya untuk menghenti kan tindakan.	Februari 22, 2024
JavaScript Manajemen kunci CAPTCHA API	Anda sekarang dapat menghapus kunci CAPTCHA JS API melalui API. AWS WAF	Februari 6, 2024
AWS WAF CAPTCHA teka-teki audio	Versi audio dari teka-teki CAPTCHA sekarang mendukung beberapa bahasa.	Februari 6, 2024
AWS WAF tantangan dan pelabelan token CAPTCHA	Manajemen token sekarang menambahkan label untuk token CAPTCHA dan telah meningkatkan pelabelan token untuk token tantangan.	20 Desember 2023
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan masukan buruk yang diketahui.	Desember 16, 2023
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan masukan buruk yang diketahui.	14 Desember 2023
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan set aturan inti (CRS).	6 Desember 2023

Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan berikut: Kontrol AWS WAF Bot.	5 Desember 2023
AWS Config Prasyarat Firewall Manager yang diperbarui	Jika Anda menggunakan peran IAM kustom alih-alih peran yang dikelola Manajer Firewall AWS Config, Anda harus memastikan bahwa kebijakan izin Anda mengizinkan AWS Config perekam merekam sumber daya Firewall Manager.	17 November 2023
AWS WAF dasbor konsol	Kami mengoreksi panduan untuk melihat semua aturan dan sampel permintaan untuk ACL web di konsol. AWS WAF	17 November 2023
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan Kontrol Bot.	14 November 2023
AWS WAF konsol memiliki dasbor ACL web baru	Halaman ACL web di AWS WAF konsol memiliki dasbor ikhtisar lalu lintas web baru.	14 November 2023
Grup aturan terkelola ATP yang diperbarui	Informasi label yang dikoreksi untuk aturan `VolumetricIpFailedLoginResponseHigh` dan `VolumetricSessionFailedLoginResponseHigh` .	13 November 2023

Grup aturan terkelola ACFP yang diperbarui	Informasi label yang dikoreksi untuk aturan `VolumetricIPSuccessfulResponse` dan `VolumetricSessionSuccessfulResponse`.	13 November 2023
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan set aturan inti (CRS).	November 2, 2023
Mitigasi DDoS lapisan aplikasi otomatis Shield Advanced	Shield Advanced sekarang mempertahankan aturan berbasis kecepatan dalam grup aturan mitigasi otomatis yang membatasi volume permintaan dari alamat IP yang dikenal sebagai sumber serangan DDoS.	31 Oktober 2023
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan set aturan inti (CRS).	30 Oktober 2023
Grup aturan terkelola Bot Control menghapus label sinyal untuk permintaan CSP	Grup aturan terkelola Bot Control menghapus label sinyal yang menunjukkan penyedia layanan cloud (CSP).	Oktober 28, 2023
Label sinyal grup aturan terkelola Bot Control untuk permintaan CSP	Label sinyal grup aturan terkelola Bot Control menyertakan label yang menunjukkan penyedia layanan cloud (CSP).	Oktober 27, 2023

Informasi izin AWS WAF IAM yang diperbarui	Untuk AWS WAF tindakan yang mengelola asosiasi ACL web, bagian tindakan kebijakan sekarang mencantumkan persyaratan izin untuk setiap jenis sumber daya aplikasi web.	25 Oktober 2023
Manajemen Firewall Manager dari ACL web yang dimodifikasi	Saat Anda mengaktifkan pengelolaan ACL web yang tidak terkait, Firewall Manager tidak menyertakan ACL web yang dimodifikasi dalam pembersihan satu kali sumber daya yang tidak digunakan.	19 Oktober 2023
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan sistem operasi POSIX, `AWSManagedRulesUnixRuleSet` .	12 Oktober 2023
AWS WAF metrik menambahkan dimensi	AWS WAF menambahkan dimensi baru untuk melihat metrik ACL web.	12 Oktober 2023
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan set aturan inti (CRS).	11 Oktober 2023
Perbarui ke spesifikasi SDK AWS WAF seluler	Menambahkan `storeTokenInCookieStorage` operasi ke `WAFTokenProvider` .	11 Oktober 2023

Penerapan pengecualian Aturan AWS Terkelola untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF merilis dua versi statis dari grup aturan masukan buruk yang diketahui dan memperbarui versi default untuk menunjuk ke versi statis terbaru.	4 Oktober 2023
AWS WAF Entitas HTML memecahkan kode transform asi teks	Memperluas fungsionalitas transformasi teks decode entitas HTML.	4 Oktober 2023
Menambahkan opsi baru ke kebijakan umum grup keamanan Firewall Manager	Firewall Manager sekarang dapat mendistribusikan referensi grup keamanan ke grup keamanan replika.	3 Oktober 2023
AWS WAF menambahkan inspeksi sidik jari JA3	Anda sekarang dapat melakukan pencocokan yang tepat terhadap sidik jari JA3 permintaan web, untuk CloudFront distribusi Amazon dan Application Load Balancers.	26 September 2023
Pembaruan pengaturan aturan kebijakan grup keamanan Firewall Manager	Firewall Manager sekarang mendukung referensi grup keamanan dari grup keamanan utama ke grup keamanan replika.	25 September 2023

Mitigasi DDoS lapisan aplikasi otomatis Shield Advanced yang diperbarui	Firewall Manager sekarang mendukung sumber daya Application Load Balancer untuk kebijakan Shield Advanced yang dikonfigurasi dengan mitigasi DDoS lapisan aplikasi otomatis.	14 September 2023
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan berikut: Kontrol AWS WAF Bot.	September 6, 2023
AWS WAF Kontrol Bot	Tingkat perlindungan yang ditargetkan dari grup aturan terkelola Kontrol Bot sekarang memeriksa penggunaan kembali token antara alamat IP. Ini juga sekarang menyediakan analisis opsional, pembelajaran mesin statistik lalu lintas untuk mendeteksi beberapa aktivitas terkait bot.	September 6, 2023
Perbarui ke spesifikasi SDK AWS WAF seluler	Menurunkan nilai min, maks, dan default untuk `tokenRefreshDelaySec` dari min 300, max 600, dan default 300 ke min 88, max 300, dan default 88.	5 September 2023
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan Kontrol AWS WAF Bot.	Agustus 30, 2023

Mitigasi DDoS lapisan aplikasi otomatis Shield Advanced	Menambahkan panduan untuk menggunakan AWS CloudFormation untuk mengelola ACL web yang Anda gunakan dengan mitigasi DDoS lapisan aplikasi otomatis.	Agustus 30, 2023
Opsi kebijakan grup keamanan audit konten Firewall Manager baru	Menambahkan opsi baru untuk mengaudit grup aturan yang terlalu permisif, dan deskripsi prosedur konsol yang ditingkat kan.	29 Agustus 2023
Opsi Firewall Manager Shield dan AWS WAF kebijakan baru	Jika Anda mengaktifkan pengelolaan ACL web yang tidak terkait di dan AWS WAF Shield, Firewall Manager hanya membuat ACL web di akun dalam cakupan kebijakan hanya jika ACL web akan digunakan oleh setidaknya satu sumber daya.	9 Agustus 2023
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan set aturan inti (CRS).	26 Juli 2023
Agregasi aturan berbasis tarif pada jalur URI	Sekarang Anda dapat menentukan jalur URI di kunci agregasi kustom untuk aturan berbasis laju.	Juli 19, 2023

Opsi aturan AWS WAF kebijakan baru di AWS Firewall Manager	AWS Firewall Manager menambahkan dukungan untuk mengonfigurasi batas ukuran inspeksi badan permintaan AWS WAF web.	Juli 18, 2023
AWS WAF perubahan kebijakan terkelola	Memperbarui `AWSWAFFullAccessPolicy` `AWSWAFConsoleFullAccess` ,`AWSWAFReadOnlyAccess` ,, dan `AWSWAFConsoleReadOnlyAccess` untuk menambahkan Akses AWS Terverifikasi ke jenis sumber daya yang dapat Anda lindungi AWS WAF.	Juni 17, 2023
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF menambahkan grup aturan`AWSManagedRulesACFPRuleSet` .	13 Juni 2023
Pembaruan untuk pencegahan pengambilalihan akun Kontrol AWS WAF Penipuan (ATP)	Anda sekarang dapat menentukan titik akhir login untuk grup aturan terkelola ATP menggunakan ekspresi reguler.	13 Juni 2023
Informasi baru untuk JavaScript CAPTCHA API	Bagian baru menjelaskan cara menyajikan teka-teki CAPTCHA khusus saat AWS WAF menanggapi permintaan dengan CAPTCHA.	13 Juni 2023

Grup aturan terkelola ACFP baru	Gunakan grup aturan baru `AWSManagedRulesACFPRuleSet` untuk mendeteksi dan memblokir upaya pembuatan akun penipuan.	13 Juni 2023
Pencegahan AWS WAF penipuan pembuatan akun Kontrol Penipuan Baru (ACFP)	Anda dapat mendeteksi dan memblokir upaya pembuatan akun penipuan dengan grup aturan terkelola pencegahan AWS WAF penipuan pembuatan akun Kontrol Penipuan (ACFP) yang baru. `AWSManagedRulesACFPRuleSet` Dengan CloudFront distribusi yang dilindungi, Anda juga dapat menggunakan ACFP untuk memblokir upaya pembuatan akun baru dari klien yang baru-baru ini mengirimkan terlalu banyak upaya pembuatan akun yang gagal.	13 Juni 2023
AWS WAF perubahan kebijakan terkelola	Diperbarui `AWSWAFFullAccessPolicy` `AWSWAFConsoleFullAccess` ,`AWSWAFReadOnlyAccess` ,, dan `AWSWAFConsoleReadOnlyAccess` untuk memperbaiki pengaturan akses untuk AWS App Runner layanan.	6 Juni 2023

Menambahkan batasan untuk kebijakan grup keamanan Firewall Manager	Jika VPC bersama kemudian tidak dibagikan, Firewall Manager tidak akan menghapus grup keamanan replika di akun terkait.	Juni 2, 2023
Komponen AWS WAF permintaan baru: Header order	Anda sekarang dapat mencocokkan dengan daftar yang diurutkan dari nama-nama header dalam permintaan.	30 Mei 2023
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	Memperbarui set aturan sistem operasi Linux.	22 Mei 2023
Memperbarui organisasi bagian AWS WAF aturan	Daftar pernyataan aturan sekarang dikelompokkan berdasarkan jenis pernyataan.	16 Mei 2023
Topik yang dipindahkan: Daftar alamat IP yang dibatasi tarifnya	Topik untuk daftar alamat IP yang dibatasi oleh aturan berbasis tarif sekarang berada di bawah topik aturan berbasis tarif.	16 Mei 2023
Opsi yang diperluas untuk aturan berbasis tarif	Anda sekarang dapat menilai batas permintaan web berdasarkan kunci agregasi selain alamat IP, dan Anda dapat menggabungkan menggunakan kombinasi tombol. Anda juga dapat menilai batas semua permintaan yang cocok dengan pernyataan cakupan bawah, tanpa agregasi lebih lanjut.	16 Mei 2023

Kuota Firewall Manager meningkat	Meningkatkan jumlah kebijakan Firewall Manager per organisasi AWS Organizations dari 20 menjadi 50. Peningkatan jumlah maksimum kelompok keamanan primer per kebijakan dari satu menjadi tiga. Mengubah jumlah maksimum WCU dari kuota lunak menjadi kuota keras.	5 Mei 2023
Peningkatan WCU maksimum per kelompok aturan	Anda sekarang dapat menggunakan hingga 5.000 unit kapasitas ACL web (WCU) per grup aturan tanpa meminta peningkatan dari dukungan. Batas baru ini tidak dapat ditingkatkan.	1 Mei 2023
AWS WAF Lokasi bucket log Amazon S3 dengan awalan	AWS WAF sekarang memungkinkan awalan dalam nama bucket log Amazon S3.	1 Mei 2023
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan set aturan inti (CRS).	28 April 2023
Menambahkan dukungan untuk instans Akses AWS Terverifikasi ke AWS WAF	Anda sekarang dapat mengaitkan ACL AWS WAF web dengan instance Akses Terverifikasi. Perubahan ini hanya tersedia di versi terbaru AWS WAF dan bukan di AWS WAF Classic.	28 April 2023

Bab yang direvisi tentang bekerja dengan beberapa administrator Firewall Manager	Sekarang Anda dapat menunjuk beberapa administrator Firewall Manager untuk membuat dan mengelola sumber daya firewall organisasi Anda.	24 April 2023
AWS Firewall Manager pembaruan kebijakan terkelola	Diperbarui`FMSServiceRolePolicy` .	April 21, 2023
Integrasi aplikasi JavaScript klien baru untuk CAPTCHA	Anda sekarang dapat menyesuaikan penempatan dan karakteristik teka-teki CAPTCHA di aplikasi JavaScript klien Anda.	20 April 2023
Integrasi aplikasi diubah namanya menjadi integrasi ancaman cerdas	Kami mengganti nama fungsionalitas yang ada untuk integrasi aplikasi klien menjadi integrasi ancaman cerdas, untuk membantu membedakan antara itu dan integrasi aplikasi CAPTCHA baru untuk. JavaScript	20 April 2023
Harga variabel untuk web ACL WCU di luar 1.500	Menggunakan lebih dari 1.500 unit kapasitas ACL web (WCU) di ACL web Anda menimbulkan biaya tambahan, yang disesuaikan secara otomatis karena penggunaan ACL WCU web Anda meningkat dan menurun. Maksimum ACL web adalah 5.000 WCU.	11 April 2023

Peningkatan WCU maksimum per web ACL	Anda sekarang dapat menggunakan hingga 5.000 unit kapasitas ACL web (WCU) per ACL web tanpa meminta peningkatan dari dukungan. Batas baru ini tidak dapat ditingkatkan.	11 April 2023
Batas ukuran inspeksi tubuh untuk ACL CloudFront web	Untuk ACL web yang melindungi CloudFront distribusi Amazon, Anda dapat meningkatkan batas ukuran pemeriksaan tubuh hingga 64 KB dalam konfigurasi ACL web Anda.	11 April 2023
Peningkatan ukuran inspeksi tubuh untuk CloudFront	Batas ukuran inspeksi AWS WAF tubuh maksimum untuk CloudFront distribusi Amazon ditingkatkan dari 8 KB menjadi 64 KB. Batas ukuran inspeksi default untuk CloudFront adalah 16 KB.	11 April 2023
Opsi aturan AWS WAF kebijakan baru di AWS Firewall Manager	AWS Firewall Manager menambahkan dukungan untuk pencegahan pengambil alihan akun Kontrol AWS WAF Penipuan (ATP) dan grup aturan Aturan AWS Terkelola Kontrol AWS WAF Bot, tujuan pencatatan Amazon S3, penggantian tindakan aturan, dan tindakan aturan`CAPTCHA`, `Challenge` dan daftar domain token.	April 7, 2023

Firewall Manager mendukung bucket Amazon S3 sebagai tujuan logging untuk logging AWS WAF	Sekarang Anda dapat menggunakan bucket Amazon S3 sebagai tujuan pencatatan dalam kebijakan Anda. AWS WAF	April 7, 2023
AWS WAF perubahan kebijakan terkelola	Diperbarui `AWSWAFFullAccessPolicy` `AWSWAFConsoleFullAccess` ,`AWSWAFReadOnlyAccess` ,, dan `AWSWAFConsoleReadOnlyAccess` untuk menambahkan AWS App Runner layanan ke jenis sumber daya yang dapat Anda lindungi AWS WAF.	30 Maret 2023
Menambahkan peringatan tentang penggunaan tag dalam kebijakan grup keamanan	Firewall Manager tidak akan memperbarui tag grup keamanan yang ada atau membuat grup keamanan baru jika kebijakan tersebut memiliki tag yang bertentangan dengan kebijakan tag organisasi.	Maret 28, 2023
Memperbarui informasi peran layanan	Memperbarui cara menggunakan peran layanan dengan Firewall Manager.	8 Maret 2023

Informasi yang dikoreksi tentang bagaimana aturan berbasis tarif melakukan pembatasan tarif	Rate based rules dengan scope-down statement hanya rate limit request yang cocok dengan pernyataan scope-down aturan. Kami menyatakan bahwa pembatasan berlaku untuk semua permintaan untuk alamat IP terbatas tarif apa pun.	1 Maret 2023
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan aplikasi PHP.	27 Februari 2023
Menambahkan dukungan AWS App Runner untuk AWS WAF	Anda sekarang dapat mengaitkan ACL AWS WAF web dengan AWS App Runner layanan. Perubahan ini hanya tersedia di versi terbaru AWS WAF dan bukan di AWS WAF Classic.	23 Februari 2023
Memperbarui panduan IAM untuk AWS Firewall Manager	Panduan yang diperbarui untuk menyelaraskan dengan praktik terbaik IAM. Untuk informasi selengkapnya, lihat Praktik terbaik keamanan di IAM.	16 Februari 2023
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan `AWSManagedRulesATPRuleSet` untuk menambahkan inspeksi respons login di ACL web yang melindungi CloudFront distribusi Amazon.	15 Februari 2023

AWS WAF Pemeriksaan respons masuk pencegahan pengambilalihan akun Kontrol Penipuan (ATP)	Untuk CloudFront distribusi yang dilindungi, Anda sekarang dapat menggunakan ATP untuk memblokir upaya login baru dari klien yang baru-baru ini mengirimkan terlalu banyak upaya login yang gagal.	15 Februari 2023
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	Memperbarui set aturan inti.	Januari 25, 2023
Praktik terbaik untuk mitigasi ancaman cerdas	Menambahkan bagian dengan praktik terbaik untuk menerapkan Kontrol Bot, ATP, dan fitur mitigasi ancaman cerdas lainnya.	Januari 22, 2023
Cara memeriksa header pseudo HTTP/2	Menambahkan bagian yang memetakan header pseudo HTTP/2 ke komponen permintaan web yang sesuai.	20 Januari 2023
Memperbarui panduan IAM untuk Klasik AWS WAF	Panduan yang diperbarui untuk menyelaraskan dengan praktik terbaik IAM. Untuk informasi selengkapnya, lihat Praktik terbaik keamanan di IAM.	Januari 3, 2023
Memperbarui panduan IAM untuk AWS WAF	Panduan yang diperbarui untuk menyelaraskan dengan praktik terbaik IAM. Untuk informasi selengkapnya, lihat Praktik terbaik keamanan di IAM.	Januari 3, 2023

Memperbarui panduan IAM untuk AWS Shield	Panduan yang diperbarui untuk menyelaraskan dengan praktik terbaik IAM. Untuk informasi selengkapnya, lihat Praktik terbaik keamanan di IAM.	Januari 3, 2023
Memperbarui kebijakan Amazon Route 53 Resolver DNS Firewall	Menambahkan informasi tentang menghapus grup aturan Amazon Route 53 Resolver DNS Firewall.	Desember 29, 2022
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	Memperbarui set aturan sistem operasi Linux.	Desember 15, 2022
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	Memperbarui set aturan inti.	Desember 5, 2022
Firewall Manager menambahkan dukungan untuk Fortigate Cloud Native Firewall (CNF) sebagai kebijakan Layanan	Firewall Manager sekarang mendukung kebijakan Fortigate CNF.	Desember 2, 2022
AWS Config Persyaratan dihapus untuk kebijakan DNS Firewall	Untuk kebijakan DNS Firewall, Anda sekarang hanya perlu mengaktifkan Config untuk jenis sumber daya EC2 VPC.	17 November 2022
AWS Firewall Manager pembaruan kebijakan terkelola	Diperbarui`FMSServiceRolePolicy` .	15 November 2022
Perluasan pilihan bahasa untuk teka-teki AWS WAF CAPTCHA	Teka-teki CAPTCHA sekarang menawarkan instruksi tertulisnya dalam berbagai bahasa. Instruksi di dalam setiap teka-teki audio masih disediakan dalam bahasa Inggris saja.	11 November 2022

Kuota Firewall Manager baru untuk kumpulan sumber daya	Menambahkan kuota baru untuk set sumber daya.	8 November 2022
Tambahkan dukungan untuk kumpulan sumber daya	Anda dapat membuat kumpulan sumber daya untuk mengelompokkan sumber daya yang akan dikelola dalam kebijakan Firewall Manager.	8 November 2022
Tambahkan dukungan untuk mengimpor firewall dari Network Firewall	Sekarang Anda dapat mengimpor dan mengelola firewall yang ada dalam kebijakan Network Firewall menggunakan kumpulan sumber daya.	8 November 2022
AWS Firewall Manager pembaruan kebijakan terkelola	Diperbarui`AWSFMAdminReadOnlyAccess` .	2 November 2022
Pernyataan geo match sekarang menambahkan label ke permintaan negara dan wilayah	Anda sekarang dapat mengelola asal permintaan geografis di tingkat wilayah dengan menggabungkan pencocokan geografis dengan pencocokan label.	31 Oktober 2022
Mengganti nama bagian tingkat atas: Perlindungan terkelola	Bagian ini sekarang bernama mitigasi ancaman AWS WAF cerdas, yang sejalan dengan halaman pemasaran kami.	27 Oktober 2022
Tingkat perlindungan baru yang ditargetkan dalam grup aturan terkelola Bot Control	Grup aturan terkelola Bot Control sekarang menawarkan aturan tambahan yang ditargetkan untuk deteksi dan mitigasi bot canggih. Tingkat perlindungan ini tersedia dengan biaya tambahan.	27 Oktober 2022

Bagian baru tentang AWS WAF token	Pahami cara AWS WAF menggunakan token untuk mitigasi ancaman cerdas.	27 Oktober 2022
Menambahkan catatan penting tentang memperbarui kebijakan Firewall Manager Network Firewall	Saat Anda memperbarui kebijakan Manajer Firewall, semua kebijakan Firewall Jaringan yang dibuat oleh kebijakan tersebut akan diperbarui dengan konfigurasi kebijakan Firewall Manager kebijakan Firewall Firewall.	27 Oktober 2022
Tindakan menimpa dalam grup aturan	Anda sekarang dapat mengganti tindakan aturan dalam grup aturan ke setelan tindakan aturan apa pun. Seperti halnya penggantian Count tindakan sebelumnya, Anda dapat menerapkan penggantian Anda ke semua aturan dalam grup aturan dan aturan individual.	27 Oktober 2022
AWS WAF opsi tindakan Challenge aturan baru	Anda dapat mengonfigurasi aturan untuk menggunakanChallenge, untuk memverifikasi bahwa permintaan sedang dikirim oleh browser.	27 Oktober 2022
AWS WAF memungkinkan berbagi token di beberapa aplikasi yang dilindungi	Anda dapat mengaktifkan penggunaan token di beberapa aplikasi yang dilindungi dengan mengonfigurasi daftar domain token untuk ACL web Anda.	27 Oktober 2022

Semua spesifikasi header tidak peka huruf besar/kecil	Mengubah spesifikasi semua header menjadi tidak peka huruf besar/kecil. Ini cocok dengan perilaku header tunggal.	26 Oktober 2022
AWS Firewall Manager perubahan kebijakan terkelola	Koreksi ke`AWSFMAdmi nFullAccess` .	21 Oktober 2022
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	Memperbarui grup aturan input buruk yang diketahui.	20 Oktober 2022
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	Memperbarui grup aturan input buruk yang diketahui.	5 Oktober 2022
Perbarui ke spesifikasi SDK AWS WAF seluler	Menurunkan nilai default `tokenRefreshDelaySec` dari 600 (10 menit) menjadi 300 (5 menit).	30 September 2022
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	Memperbaiki nama label yang disediakan dalam dokumentasi ini untuk kelompok aturan berikut: Sistem operasi POSIX, aplikasi PHP, WordPress aplikasi.	19 September 2022
Opsi aturan AWS WAF kebijakan baru di AWS Firewall Manager	AWS Firewall Manager sekarang mendukung permintaan dan tanggapan web yang disesuaikan untuk tindakan web default dalam AWS WAF kebijakan.	9 September 2022
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan berikut: Reputasi IP.	30 Agustus 2022

AWS WAF perubahan kebijakan terkelola	Memperbarui `AWSWAFFullAccessPolicy` `AWSWAFConsoleFullAccess` ,`AWSWAFReadOnlyAccess` ,, dan `AWSWAFConsoleReadOnlyAccess` untuk menambahkan kumpulan pengguna Amazon Cognito ke jenis sumber daya yang dapat Anda lindungi. AWS WAF	Agustus 25, 2022
AWS WAF Pencegahan pengambilalihan akun Kontrol Penipuan (ATP)	Anda sekarang dapat menggunakan fungsionalitas pencegahan pengambil alihan akun Kontrol AWS WAF Penipuan (ATP) dengan distribusi Amazon CloudFront .	Agustus 24, 2022
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan berikut: Masukan buruk yang diketahui.	22 Agustus 2022
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan berikut:`AWSManagedRulesATPRuleSet` .	Agustus 11, 2022
Menambahkan dukungan untuk kumpulan pengguna Amazon Cognito AWS WAF	Anda sekarang dapat mengaitkan ACL AWS WAF web dengan kumpulan pengguna Amazon Cognito. Perubahan ini hanya tersedia di versi terbaru AWS WAF dan bukan di AWS WAF Classic.	Agustus 11, 2022

Menambahkan bagian tentang penerapan untuk grup aturan Aturan Terkelola berversi AWS	Menambahkan bagian baru yang mendokumentasikan penerapan untuk grup aturan Aturan Terkelola berversi. AWS Bagian ini mencakup informasi tentang bagaimana versi default diberi nama selama penerapan kandidat rilis.	Juli 29, 2022
Persyaratan yang diperbarui untuk mengonfigurasi logging untuk kebijakan Network Firewall	Persyaratan tambahan untuk kebijakan Network Firewall yang menggunakan bucket Amazon S3 terenkripsi sebagai tujuan log.	26 Juli 2022
Opsi tingkat sensitivitas untuk pernyataan aturan SQLi	Anda sekarang dapat meningkatkan sensitivitas pernyataan aturan injeksi SQL Anda. Ini tidak mengubah perilaku pernyataan yang ada, yang tingkat sensitivitasnya pada defaultLOW.	15 Juli 2022
Menambahkan opsi konfigurasi kebijakan Firewall Jaringan	Firewall Manager sekarang mendukung urutan evaluasi stateful dan tindakan default dalam konfigurasi kebijakan firewall Network Firewall.	14 Juli 2022
Pembaruan pengaturan aturan kebijakan grup keamanan Firewall Manager	Firewall Manager sekarang mendukung distribusi tag dari grup keamanan utama ke grup keamanan replika.	Juli 7, 2022

Pembaruan untuk AWS Shield panduan	Memperluas informasi dalam panduan Shield untuk menjelaskan cara Shield melakukan mitigasi peristiwa.	Juni 24, 2022
Panduan terbaru untuk pengujian dan penyetelan perlindungan AWS WAF	Panduan umum untuk pengujian dan penyetelan AWS WAF diperbarui dan sekarang menjadi topik tingkat atas.	Juni 20, 2022
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan berikut: Set aturan inti (CRS).	9 Juni 2022
Manajer Firewall Baru membingungkan panduan wakil	Menambahkan panduan tentang cara mencegah masalah wakil yang membingungkan untuk Firewall Manager.	1 Juni 2022
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan berikut: Set aturan inti (CRS).	24 Mei 2022
Komponen AWS WAF permintaan baru: Headers dan Cookies	Anda sekarang dapat memeriksa cookie dalam permintaan web dan Anda dapat memeriksa semua header dalam permintaa n web, selain hanya satu header.	29 April 2022

AWS WAF penanganan untuk komponen permintaan bodi, header, dan cookie yang terlalu besar	Sekarang Anda dapat menentukan bagaimana AWS WAF menangani badan permintaan yang terlalu besar, header, dan cookie di dalam aturan Anda yang memeriksa komponen ini. Aturan yang telah Anda buat yang memeriksa komponen ini memiliki perilaku yang cocok dengan Continue opsi baru untuk penanganan ukuran besar.	29 April 2022
AWS WAF Perubahan kebijakan log Amazon S3	Memperbarui kebijakan dan contoh izin log Amazon S3.	12 April 2022
Opsi mitigasi DDoS lapisan aplikasi otomatis sekarang tersedia AWS Shield Advanced untuk Application Load Balancer	Shield Advanced sekarang mendukung mitigasi DDoS lapisan aplikasi otomatis untuk Application Load Balancer, sehingga tersedia untuk semua perlindun gan lapisan aplikasi. Anda dapat mengonfigurasi Shield Advanced untuk secara otomatis menghitung atau memblokir permintaan web yang merupakan bagian dari serangan lapisan aplikasi DDoS pada sumber daya yang dilindungi.	8 April 2022
Menambahkan indikator setelan versi default saat ini untuk grup aturan terkelola	Daftar versi grup aturan terkelola sekarang menunjukk an versi mana yang merupakan default saat ini.	8 April 2022

Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan berikut: Kontrol AWS WAF Bot.	April 6, 2022
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan berikut: Masukan buruk yang diketahui.	31 Maret 2022
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan berikut: Masukan buruk yang diketahui.	Maret 30, 2022
Firewall Manager menambahkan dukungan untuk Palo Alto Networks Cloud Next Generation Firewall (NGFW)	Firewall Manager sekarang mendukung Palo Alto Networks Cloud Next Generation Firewall (NGFW).	Maret 30, 2022
Tambahkan dukungan untuk Palo Alto Networks Cloud NGFW ke AWS Firewall Manager	AWS Firewall Manager sekarang mendukung kebijakan Palo Alto Networks Cloud Next Generation Firewall (NGFW).	Maret 30, 2022
Pembaruan untuk AWS Shield panduan	Memperluas informasi dalam panduan Shield untuk menjelaskan bagaimana Shield melakukan deteksi peristiwa dan untuk memberikan contoh arsitektur tangguh DDoS.	16 Maret 2022

Pembaruan untuk AWS Shield panduan	Memperluas informasi dalam panduan Shield dan meningkatkan organisasi berbagai bagian. Perubahan utama ada di bagian panduan Shield berikut: Dukungan Shield Response Team (SRT), Perlindungan sumber daya AWS Shield Advanced, dan Visibilitas ke dalam peristiwa DDoS.	28 Februari 2022
Firewall Manager sekarang mendukung model penyebaran terpusat Network Firewall	Menambahkan prosedur baru yang menjelaskan cara mengonfigurasi kebijakan yang menggunakan model penyebaran terdistribusi dan terpusat.	Februari 24, 2022
Firewall Manager menambahkan dukungan untuk model penyebaran AWS Network Firewall terpusat	Sekarang Anda dapat mengonfigurasi AWS Network Firewall kebijakan Anda untuk menggunakan model penyebaran terdistribusi atau terpusat. Dengan model penerapan terdistribusi, Firewall Manager membuat dan memelihara titik akhir firewall di setiap VPC yang berada dalam cakupan kebijakan. Dengan model penyebaran terpusat, Firewall Manager membuat dan memelihara titik akhir firewall dalam satu VPC inspeksi.	Februari 24, 2022

Tambahkan dukungan untuk pembuatan versi grup aturan AWS WAF terkelola AWS Firewall Manager	AWS Firewall Manager sekarang mendukung pembuatan versi grup aturan AWS WAF terkelola dalam kebijakan Firewall Manager AWS WAF .	18 Februari 2022
AWS Firewall Manager perubahan kebijakan terkelola	Perbarui ke`FMSServiceRolePolicy` .	16 Februari 2022
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan berikut: Daftar reputasi IP.	Februari 15, 2022
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF menambahkan grup aturan pencegahan pengambilalihan akun Kontrol AWS WAF Penipuan (ATP). `AWSManagedRulesATPRuleSet`	Februari 11, 2022
Perubahan pada organisasi AWS WAF panduan	Menambahkan bagian tingkat atas baru untuk perlindungan terkelola. Memindahkan bagian CAPTCHA dari bawah aturan ke bagian perlindungan terkelola yang baru. Memindahkan bagian label dari bawah aturan ke bagian tingkat atasnya sendiri.	Februari 11, 2022

AWS WAF integrasi aplikasi klien	Gunakan API klien AWS WAF JavaScript dan seluler untuk mengintegrasikan aplikasi klien Anda dengan grup aturan Aturan AWS Terkelola mitigasi ancaman cerdas untuk deteksi yang disempurnakan.	Februari 11, 2022
AWS WAF Pencegahan pengambilalihan akun Kontrol Penipuan (ATP)	Anda dapat mendeteksi dan memblokir upaya pengambil alihan akun dengan grup aturan terkelola pencegaha n pengambilalihan akun Kontrol AWS WAF Penipuan (ATP) yang baru. `AWSManage dRulesATPRuleSet`	Februari 11, 2022
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan berikut: Masukan buruk yang diketahui.	28 Januari 2022
AWS WAF perubahan kebijakan terkelola	Diperbarui `AWSWAFFul lAccessPolicy` dan `AWSWAFConsoleFullA ccess` untuk memperbaiki izin logging.	11 Januari 2022
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan berikut: set aturan inti (CRS), database SQLi.	10 Januari 2022

Firewall Manager mendukung mitigasi DDoS lapisan aplikasi otomatis Shield Advanced	Firewall Manager Shield Kebijakan lanjutan untuk CloudFront sumber daya Amazon sekarang menyertakan dukungan untuk mitigasi DDoS lapisan aplikasi otomatis.	7 Januari 2022
AWS Firewall Manager perubahan kebijakan terkelola	Perbarui ke`FMSServiceRolePolicy` .	7 Januari 2022
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan berikut: Masukan buruk yang diketahui.	Desember 17, 2021
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan berikut: Masukan buruk yang diketahui.	Desember 11, 2021
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan berikut: Masukan buruk yang diketahui.	Desember 10, 2021
AWS Shield Advanced Peran terkait layanan baru	Ditambahkan `AWSServiceRoleForAWSShield` untuk mendukung fungsi mitigasi DDoS lapisan aplikasi otomatis.	1 Desember 2021
Kebijakan AWS Shield terkelola baru	Ditambahkan `AWSShieldServiceRolePolicy` untuk mendukung fungsi mitigasi DDoS lapisan aplikasi otomatis.	1 Desember 2021

Opsi mitigasi DDoS lapisan aplikasi otomatis sekarang tersedia dengan untuk AWS Shield Advanced CloudFront	Shield Advanced sekarang mendukung mitigasi DDoS lapisan aplikasi otomatis untuk distribusi Amazon. CloudFront Anda dapat mengkonfigurasi Shield Advanced untuk secara otomatis menghitung atau memblokir permintaan web yang merupakan bagian dari serangan DDoS lapisan aplikasi pada CloudFront distribusi.	1 Desember 2021
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan berikut: set aturan inti (CRS), sistem operasi Windows, sistem operasi Linux, dan daftar reputasi IP.	23 November 2021
AWS Firewall Manager perubahan kebijakan terkelola	Perbarui ke`FMSServiceRolePolicy` .	18 November 2021
Opsi logging yang diperluas untuk AWS WAF	Sekarang Anda dapat mencatat lalu lintas ACL web ke grup CloudWatch log Amazon Logs atau bucket Amazon Simple Storage Service (Amazon S3). Opsi ini merupakan tambahan dari opsi yang ada untuk masuk ke aliran pengiriman Amazon Data Firehose.	15 November 2021

AWS WAF perubahan kebijakan terkelola	Diperbarui `AWSWAFFullAccessPolicy` dan `AWSWAFConsoleFullAccess` untuk mendukung tujuan pencatatan tambahan.	15 November 2021
AWS WAF opsi tindakan CAPTCHA aturan baru	Anda dapat mengonfigurasi aturan untuk menjalankan CAPTCHA terhadap permintaan web dan, sesuai kebutuhan, mengirim masalah CAPTCHA ke klien.	November 8, 2021
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan set aturan inti (CRS).	27 Oktober 2021
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	Semua grup aturan Aturan AWS Terkelola sekarang mendukung pelabelan. Deskripsi aturan mencakup spesifikasi label.	25 Oktober 2021
Firewall Manager mendukung pemfilteran log Network Firewall	AWS Firewall Manager sekarang mendukung penyaringan log untuk kebijakan Network Firewall.	4 Oktober 2021
AWS Firewall Manager perubahan kebijakan terkelola	Perbarui ke`FMSServiceRolePolicy` .	29 September 2021
Menambahkan pernyataan pertandingan regex	Anda sekarang dapat mencocokkan permintaan web dengan ekspresi reguler tunggal.	22 September 2021

Aturan berbasis tarif di dalam AWS WAF grup aturan	Anda sekarang dapat menentukan aturan berbasis tingkat di dalam AWS WAF grup aturan. Pada tahun AWS Firewall Manager, kemampuan ini didukung penuh untuk AWS WAF kebijakan.	13 September 2021
Firewall Manager mendukung penyaringan AWS WAF log	AWS Firewall Manager sekarang mendukung penyaringan log untuk AWS WAF kebijakan.	31 Agustus 2021
Secara otomatis menghapus perlindungan out-of-scope sumber daya di AWS Firewall Manager	AWS Firewall Manager memungkinkan Anda untuk secara otomatis menghapus perlindungan dari sumber daya yang meninggalkan cakupan kebijakan.	25 Agustus 2021
AWS Firewall Manager perubahan kebijakan terkelola	Perbarui ke`FMSServiceRolePolicy` .	Agustus 12, 2021
Menambahkan versi ke grup aturan terkelola	Penyedia grup aturan terkelola sekarang dapat membuat versi grup aturan mereka.	9 Agustus 2021
Ubah persyaratan AWS Firewall Manager administrator	Anda dapat menggunakan akun manajemen organisasi sebagai akun administrator Firewall Manager. Ini telah dianulir.	2 Agustus 2021
Peningkatan kuota Firewall Manager	Meningkatkan jumlah instans VPC Amazon yang dapat Anda miliki dalam cakupan kebijakan Firewall Manager dari 10 menjadi 100.	28 Juli 2021

AWS Firewall Manager dukungan untuk pemantauan tabel AWS Network Firewall rute	AWS Firewall Manager sekarang mendukung pemantauan tabel rute, dan memberikan rekomendasi tindakan remediasi kepada administrator keamanan untuk AWS Network Firewall kebijakan dengan rute yang salah konfigurasi.	8 Juli 2021
AWS WAF opsi transformasi teks tambahan	Opsi yang diperluas untuk transformasi teks, yang dapat Anda terapkan ke komponen permintaan web sebelum memeriksanya.	24 Juni 2021
Penamaan yang dimodifikasi untuk sumber daya AWS WAF kebijakan Firewall Manager	Penamaan untuk ACL web, grup aturan, dan pencatatan yang dikelola Manajer Firewall untuk AWS WAF kebijakan Anda telah berubah.	26 Mei 2021
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF menambahkan dukungan untuk pelabelan ke daftar reputasi IP dan sufiks yang dihapus pada nama aturan untuk daftar reputasi IP Amazon.	4 Mei 2021

Tambahkan dukungan untuk Administrator AWS Organizations Delegasi	Saat Anda mengatur akun AWS Firewall Manager administrator, Firewall Manager sekarang menetapkan akun sebagai administrator yang AWS Organizations didelegasikan untuk Firewall Manager. Dengan perubahan ini, saat Anda mengatur akun administrator Manajer Firewall, Anda harus memberikan akun anggota selain akun manajemen organisasi. Perubahan ini tidak memengaruhi pengaturan yang ada.	30 April 2021
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF menambahkan grup aturan Kontrol AWS WAF Bot.	1 April 2021
Tetapkan tindakan aturan individual ke Count dalam grup aturan	Sekarang Anda dapat mengatur tindakan aturan individual dalam grup aturanCount. Informasi untuk penggantian yang ada, yang berada di tingkat grup aturan, telah diperbaiki.	1 April 2021
Pernyataan cakupan bawah untuk grup aturan terkelola	Anda sekarang dapat menggunakan pernyataan scope-down dengan grup aturan terkelola dengan cara yang sama seperti yang Anda bisa dengan pernyataan berbasis rate.	1 April 2021

Pemfilteran log	Anda sekarang dapat memfilter lalu lintas ACL web yang Anda log berdasarkan tindakan aturan dan label.	1 April 2021
AWS WAF label pada permintaan web	Anda dapat mengonfigurasi aturan untuk menambahkan label ke permintaan web yang cocok dan mencocokkan label yang ditambahkan oleh aturan lain.	1 April 2021
AWS WAF Kontrol Bot	Anda dapat memantau dan mengontrol lalu lintas bot dengan fitur Kontrol AWS WAF Bot baru, yang menggabungkan grup aturan terkelola Kontrol Bot dengan pelabelan permintaan web, pernyataan cakupan bawah, dan penyaringan log.	1 April 2021
Firewall Manager mendukung kebijakan Amazon Route 53 Resolver DNS Firewall	AWS Firewall Manager mendukung manajemen pusat Amazon Route 53 Resolver DNS Firewall outbound DNS traffic filtering untuk VPC Anda.	31 Maret 2021

Permintaan khusus dan penanganan respons	Anda dapat menyertakan header khusus untuk permintaan web yang AWS WAF tidak diblokir dan Anda dapat mengirim tanggapan khusus untuk permintaan web yang AWS WAF memblokir. Ini tersedia untuk tindakan default ACL web dan pengaturan tindakan aturan.	29 Maret 2021
AWS Firewall Manager perubahan kebijakan terkelola	Perbarui ke`FMSServiceRolePolicy` .	17 Maret 2021
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan berikut: set aturan inti (CRS), perlindungan admin, input buruk yang diketahui, dan sistem operasi Linux.	3 Maret 2021
AWS Shield pelacakan perubahan kebijakan terkelola	Shield mulai melacak perubahan untuk kebijakan AWS terkelolanya.	3 Maret 2021
AWS Firewall Manager pelacakan perubahan kebijakan terkelola	Firewall Manager mulai melacak perubahan untuk kebijakan yang AWS dikelola.	2 Maret 2021
AWS WAF pelacakan perubahan kebijakan terkelola	AWS WAF mulai melacak perubahan untuk kebijakan AWS terkelolanya.	1 Maret 2021

Periksa badan permintaan web sebagai JSON yang diurai	Menambahkan opsi untuk memeriksa badan permintaan web sebagai JSON yang diurai dan difilter. Ini merupakan tambahan dari opsi yang ada untuk memeriksa badan permintaan web sebagai teks biasa.	12 Februari 2021
Firewall Manager mendukung AWS Network Firewall kebijakan	AWS Firewall Manager mendukung manajemen pusat penyaringan lalu lintas AWS Network Firewall jaringan untuk VPC Anda.	17 November 2020
Tambahkan dukungan untuk grup AWS Shield Advanced perlindungan	Anda sekarang dapat mengelompokkan sumber daya yang dilindungi ke dalam grup logis dan mengelola perlindungan mereka secara kolektif.	13 November 2020
Menambahkan dukungan AWS AppSync untuk AWS WAF	Anda sekarang dapat mengaitkan ACL AWS WAF web dengan AWS AppSync GraphQL API Anda. Perubahan ini hanya tersedia di versi terbaru AWS WAF dan bukan di AWS WAF Classic.	1 Oktober 2020
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui set aturan sistem operasi Windows.	23 September 2020

Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui aturan menetapkan aplikasi PHP dan sistem operasi POSIX.	16 September 2020
AWS Shield Konsol yang diperbarui	AWS Shield menawarkan opsi konsol baru, dengan pengalaman pengguna yang lebih baik. Panduan konsol dalam dokumentasi adalah untuk konsol baru.	1 September 2020
Firewall Manager memperbarui kebijakan grup keamanan umum	AWS Firewall Manager Kebijakan grup keamanan umum sekarang mendukung jenis sumber daya Application Load Balancers dan Classic Load Balancers melalui implementasi konsol. Opsi baru tersedia di pengaturan cakupan Kebijakan kebijakan umum.	11 Agustus 2020
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui set aturan inti.	7 Agustus 2020
Firewall Manager mendukung konfigurasi AWS WAF logging	AWS Firewall Manager sekarang mendukung konfigurasi logging terpusat untuk AWS WAF kebijakan.	30 Juli 2020

Tentukan lokasi alamat IP dalam permintaan web	Menambahkan opsi untuk menggunakan alamat IP dari header HTTP yang Anda tentukan, alih-alih menggunakan asal permintaan web. Header alternatif umumnya `X-Forwarded-For` (XFF), tetapi Anda dapat menentukan nama header apa pun. Anda dapat menggunakan opsi ini untuk pencocokan set IP, pencocokan geografis, dan agregasi jumlah aturan berbasis laju.	9 Juli 2020
Firewall Manager memperbarui kebijakan grup keamanan audit konten	AWS Firewall Manager telah memperluas fungsionalitas untuk kebijakan grup keamanan audit konten termasuk opsi aturan terkelola, yang menggunakan daftar aplikasi dan protokol terkelola, dan detail untuk pelanggaran sumber daya.	7 Juli 2020
Daftar terkelola Firewall Manager	AWS Firewall Manager sekarang mendukung aplikasi terkelola dan daftar protokol. Firewall Manager mengelola beberapa daftar dan Anda dapat membuat dan mengelola sendiri.	7 Juli 2020

Firewall Manager mendukung VPC bersama dalam kebijakan grup keamanan umum	AWS Firewall Manager sekarang mendukung penggunaan kebijakan grup keamanan umum di VPC bersama. Anda dapat melakukan ini selain menggunakannya di VPC yang dimiliki oleh akun dalam lingkup.	26 Mei 2020
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	Menambahkan dokumenta si untuk setiap aturan dalam Aturan AWS Terkelola untuk AWS WAF.	20 Mei 2020
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui grup aturan sistem operasi Linux.	19 Mei 2020
Tambahkan dukungan untuk memigrasi sumber daya AWS WAF Klasik ke AWS WAF (v2)	Sekarang Anda dapat menggunakan konsol atau API untuk mengekspor sumber daya AWS WAF Klasik untuk migrasi ke versi terbaru AWS WAF.	27 April 2020

Menambahkan dukungan untuk unit AWS Organizations organisasi dalam lingkup kebijakan	AWS Firewall Manager sekarang mendukung penggunaan unit AWS Organizations organisasi (OU) untuk menentukan ruang lingkup kebijakan. Anda dapat menggunakan OU untuk memasukkan atau mengecualikan akun dari ruang lingkup, selain menyertakan atau mengecualikan akun tertentu. Menentukan OU sama dengan menentukan semua akun di OU dan di salah satu OU anaknya, termasuk OU anak dan akun yang ditambahkan di lain waktu.	6 April 2020
Tambahkan dukungan untuk AWS WAF (v2) ke AWS Firewall Manager	AWS Firewall Manager sekarang mendukung versi terbaru AWS WAF, selain versi sebelumnya, AWS WAF Klasik.	31 Maret 2020
Memperbarui ke kebijakan grup keamanan AWS Firewall Manager umum	AWS Firewall Manager Kebijakan grup keamanan umum sekarang memiliki opsi untuk menerapkan kebijakan ke semua antarmuka jaringan elastis dalam instans Amazon EC2 dalam cakupan Anda. Anda masih dapat memilih untuk hanya menerapkan kebijakan ke default elastic network interface.	11 Maret 2020

Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF menambahkan grup `AWSManagedRulesAnonymousIpList` aturan.	6 Maret 2020
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF memperbarui WordPress aplikasi dan grup `AWSManagedRulesCommonRuleSet` aturan.	3 Maret 2020
Menambahkan pemeriksaan kesehatan Amazon Route 53 ke opsi AWS Shield Advanced perlindungan	Shield Advanced sekarang mendukung penggunaan asosiasi pemeriksaan kesehatan Amazon Route 53, untuk meningkatkan akurasi deteksi dan mitigasi ancaman.	14 Februari 2020
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF telah memperbarui grup aturan Database SQL untuk menambahkan pemeriksaan URI pesan.	23 Januari 2020
Opsi baru Firewall Manager untuk kebijakan audit penggunaan grup keamanan	Firewall Manager memiliki opsi baru untuk kebijakan audit penggunaan grup keamanan. Anda sekarang dapat menetapkan jumlah menit minimum grup keamanan harus tetap tidak digunakan sebelum dianggap tidak patuh. Secara default, pengaturan menit ini adalah nol.	Januari 14, 2020

Firewall Manager opsi baru untuk AWS WAF kebijakan	Firewall Manager memiliki opsi baru untuk AWS WAF kebijakan. Sekarang Anda dapat memilih untuk menghapus semua asosiasi ACL web yang ada dari sumber daya dalam lingkup sebelum mengaitkan ACL web baru kebijakan tersebut dengan mereka.	Januari 14, 2020
Aturan AWS Terkelola yang Diperbarui untuk AWS WAF	AWS Aturan Terkelola untuk AWS WAF telah memperbarui transformasi teks untuk aturan dalam Kumpulan Aturan Inti dan grup aturan Database SQL.	20 Desember 2019
AWS Firewall Manager terintegrasi dengan AWS Security Hub	AWS Firewall Manager sekarang menciptakan temuan untuk sumber daya yang di luar kepatuhan dan untuk serangan dan mengirimkannya ke AWS Security Hub.	18 Desember 2019

Rilis AWS WAF versi 2	Versi baru dari panduan AWS WAF pengembang. Anda dapat mengelola ACL web atau grup aturan dalam format JSON. Kemampuan yang diperluas mencakup pernyataan aturan logis, penyarangan pernyataan aturan, dan dukungan CIDR penuh untuk alamat IP dan rentang alamat. Aturan tidak lagi AWS sumber daya, tetapi hanya ada dalam konteks ACL web atau grup aturan. Untuk pelanggan yang sudah ada, versi layanan sebelumnya sekarang disebut AWS WAF Klasik. Dalam API, SDK, dan CLI, AWS WAF Classic mempertahankan skema penamaannya dan versi terbaru ini AWS WAF disebut dengan tambahan “V2" atau “v2", tergantung pada konteksnya. AWS WAF tidak dapat mengakses AWS sumber daya yang dibuat di AWS WAF Classic. Untuk menggunakan sumber daya tersebut AWS WAF, Anda perlu memigrasikannya.	25 November 2019
AWS Grup aturan Aturan Terkelola untuk AWS WAF	Menambahkan grup aturan Aturan AWS Terkelola. Ini gratis untuk AWS WAF pelanggan.	25 November 2019

AWS Firewall Manager dukungan untuk grup keamanan Amazon Virtual Private Cloud	Menambahkan dukungan untuk grup keamanan Amazon VPC ke Firewall Manager.	10 Oktober 2019
AWS Firewall Manager dukungan untuk AWS Shield Advanced	Menambahkan dukungan untuk Shield Advanced ke Firewall Manager.	15 Maret 2019
Tutorial: Membuat kebijakan hierarkis	Ditambahkan tutorial tentang membuat kebijakan hierarkis di AWS Firewall Manager.	11 Februari 2019
Kontrol tingkat aturan dalam kelompok aturan	Anda sekarang dapat mengecualikan aturan individual dari grup AWS Marketplace aturan, serta grup aturan Anda sendiri.	12 Desember 2018
AWS Shield Advanced dukungan untuk akselerator AWS Global Accelerator standar	Shield Advanced sekarang dapat melindungi akselerator AWS Global Accelerator standar.	26 November 2018
AWS WAF dukungan untuk Amazon API Gateway	AWS WAF sekarang melindungi API Amazon API Gateway.	25 Oktober 2018
Wizard memulai AWS perisai lanjutan yang diperluas	Wizard baru memberikan kesempatan untuk membuat aturan berbasis tarif dan Acara Amazon CloudWatch .	31 Agustus 2018
AWS WAF pencatatan log	Aktifkan pencatatan untuk mendapatkan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web Anda.	31 Agustus 2018

Support untuk parameter kueri dalam kondisi	Saat membuat kondisi, Anda sekarang dapat mencari permintaan untuk parameter tertentu.	5 Juni 2018
Shield advanced untuk memulai wizard	Memperkenalkan proses baru yang disederhanakan untuk berlangganan Shield AWS Advanced.	5 Juni 2018
Rentang CIDR yang diizinkan diperluas	Saat membuat kondisi pencocokan IP, AWS WAF sekarang mendukung rentang alamat IPv4: /8 dan rentang apa pun antara /16 hingga /32.	5 Juni 2018

Pembaruan sebelum 2018

Tabel berikut menjelaskan perubahan penting dalam setiap rilis Panduan AWS WAF Pengembang yang dibuat sebelum 2018.

Perubahan	Versi API	Deskripsi	Tanggal Rilis
Perbarui	2016-08-24	AWS Marketplace kelompok aturan	November, 2017
Perbarui	2016-08-24	Dukungan Shield Advanced untuk alamat IP Elastis	November, 2017
Perbarui	2016-08-24	Dasbor ancaman global	November, 2017
Perbarui	2016-08-24	Tutorial situs web tahan DDoS	Oktober, 2017

Perubahan	Versi API	Deskripsi	Tanggal Rilis
Perbarui	2016-08-24	Kondisi geo dan regex	Oktober, 2017
Perbarui	2016-08-24	Aturan berbasis tarif	Juni, 2017
Perbarui	2016-08-24	Reorganisasi	April, 2017
Perbarui	2016-08-24	Menambahkan informasi tentang perlindungan DDOS dan dukungan untuk Application Load Balancers.	Selasa, 07 Nopember 2016
Fitur Baru	2015-08-24	Sekarang Anda dapat mencatat semua panggilan API Anda ke AWS WAF through AWS CloudTrail, AWS layanan yang merekam panggilan API untuk akun Anda dan mengirimkan file log ke bucket S3 Anda. CloudTrail log dapat digunakan untuk mengaktif kan analisis keamanan, melacak perubahan pada AWS sumber daya Anda, dan membantu dalam audit kepatuhan. Mengintegrasikan AWS WAF dan CloudTrail memungkinkan Anda menentukan permintaan mana yang dibuat ke AWS WAF API, alamat IP sumber dari mana setiap permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan banyak lagi. Jika Anda sudah menggunakan AWS CloudTrail, Anda akan mulai melihat panggilan AWS WAF API di CloudTrail log Anda. Jika Anda belum mengaktifkan CloudTrail akun Anda, Anda dapat mengaktifkannya CloudTrail dari AWS Management Console. Tidak ada biaya tambahan untuk mengaktifkan CloudTrail, tetapi tarif standar untuk Amazon S3 dan penggunaan Amazon SNS berlaku.	April 28, 2016

Perubahan	Versi API	Deskripsi	Tanggal Rilis
Fitur Baru	2015-08-24	Anda sekarang dapat menggunakan AWS WAF untuk mengizinkan, memblokir, atau menghitung permintaan web yang tampaknya berisi skrip berbahaya, yang dikenal sebagai cross-site scripting atau XSS. Penyerang terkadang memasukkan skrip berbahaya ke dalam permintaan web dalam upaya untuk mengeksploitasi kerentanan dalam aplikasi web. Untuk informasi selengkapnya, lihat Pernyataan aturan serangan skrip lintas situs.	29 Maret 2016
Fitur Baru	2015-08-24	Dengan rilis ini, AWS WAF menambahkan fitur berikut: • Anda dapat mengonfigurasi AWS WAF untuk mengizinkan, memblokir, atau menghitung permintaan web berdasarkan panjang bagian permintaan yang ditentukan, seperti string kueri atau URI. Untuk informasi selengkapnya, lihat Pernyataan aturan batasan ukuran. • Anda dapat mengonfigurasi AWS WAF untuk mengizinkan, memblokir, atau menghitung permintaan web berdasarkan konten di badan permintaan. Ini adalah bagian dari permintaan yang berisi data tambahan yang ingin Anda kirimkan ke server web Anda sebagai isi permintaan HTTP, seperti data dari formulir. Fitur ini berlaku untuk kondisi pencocokan string, kondisi kecocokan injeksi SQL, dan kondisi batasan ukuran baru yang disebutkan dalam bullet pertama. Untuk informasi selengkapnya, lihat Spesifikasi dan penanganan komponen permintaan web.	27 Januari 2016

Perubahan	Versi API	Deskripsi	Tanggal Rilis
Fitur Baru	2015-08-24	Anda sekarang dapat menggunakan AWS WAF konsol untuk memilih CloudFront distribusi yang ingin Anda kaitkan dengan ACL web. Untuk informasi selengkap nya, lihat Mengaitkan atau Memisahkan ACL Web dan Distribusi. CloudFront	November 16, 2015
Rilis Awal	2015-08-24	Panduan ini adalah perilisan pertama dari Panduan Developer AWS WAF .	Oktober 6, 2015

AWS Glosarium

Untuk AWS terminologi terbaru, lihat AWS glosarium di Referensi.Glosarium AWS

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.