Panduan Implementasi

Otomasi Keamanan untuk AWS WAF

Otomasi Keamanan untuk AWS WAF: Panduan Implementasi

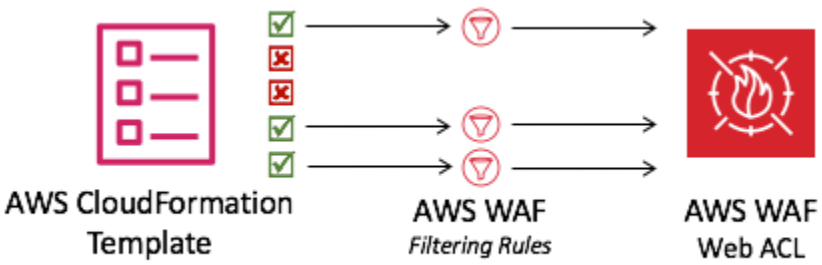
Table of Contents

Secara otomatis menyebarkan satu daftar kontrol akses web yang menyaring serangan berbasis web dengan Otomasi Keamanan di AWS WAF

Tanggal publikasi: September 2016 (pembaruan terakhir: Desember 2024)

AWS WAF Solusi Otomasi Keamanan untuk menerapkan seperangkat aturan yang telah dikonfigurasi sebelumnya untuk membantu Anda melindungi aplikasi Anda dari eksploitasi web umum. Layanan inti solusi ini AWS WAF, membantu melindungi aplikasi web dari teknik serangan yang dapat memengaruhi ketersediaan aplikasi, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan. Anda dapat menggunakan AWS WAF untuk menentukan aturan keamanan web yang dapat disesuaikan. Aturan ini mengontrol lalu lintas mana yang diizinkan atau diblokir ke aplikasi web dan antarmuka pemrograman aplikasi (APIs) yang digunakan pada AWS sumber daya seperti Amazon CloudFront, Application Load Balancer ALB (), dan Amazon Gateway. API Untuk jenis sumber daya yang didukung lainnya, lihat AWS WAFdi AWS WAF, AWS Firewall Manager, dan Panduan AWS Shield Advanced Pengembang.

Mengkonfigurasi AWS WAF aturan dapat menjadi tantangan dan memberatkan bagi organisasi besar dan kecil, terutama bagi mereka yang tidak memiliki tim keamanan khusus. Untuk menyederhanakan proses ini, Security Automations for AWS WAF solution secara otomatis menyebarkan satu daftar kontrol akses web (ACL) dengan seperangkat AWS WAF aturan yang dirancang untuk memfilter serangan berbasis web umum. Selama konfigurasi awal AWS CloudFormationtemplate solusi ini, Anda dapat menentukan fitur pelindung mana yang akan disertakan. Setelah Anda menerapkan solusi ini, AWS WAF periksa permintaan web ke distribusi atau CloudFront ALB distribusi yang ada, dan blokir jika berlaku.



Konfigurasi AWS WAF web ACL

Panduan implementasi ini membahas pertimbangan arsitektur, langkah konfigurasi, dan praktik terbaik operasional untuk menerapkan solusi ini di Amazon Web Services ()AWS Cloud. Ini mencakup tautan ke CloudFormation templat yang meluncurkan, mengonfigurasi, dan menjalankan AWS keamanan, komputasi, penyimpanan, dan layanan lain yang diperlukan untuk menerapkan solusi ini AWS, menggunakan praktik AWS terbaik untuk keamanan dan ketersediaan.

Informasi dalam panduan ini mengasumsikan pengetahuan kerja tentang AWS layanan seperti AWS WAF,, CloudFrontALBs, dan AWS Lambda. Ini juga membutuhkan pengetahuan dasar tentang serangan berbasis web umum dan strategi mitigasi.

> **Note**
>
> Pada versi 3.0.0, solusi ini mendukung versi terbaru AWS WAF layanan API (AWS WAF V2).

Panduan ini ditujukan untuk manajer TI, insinyur keamanan, DevOps insinyur, pengembang, arsitek solusi, dan administrator situs web.

> **Note**
>
> Sebaiknya gunakan solusi ini sebagai titik awal untuk menerapkan AWS WAF aturan. Anda dapat menyesuaikan kode sumber, menambahkan aturan kustom baru, dan memanfaatkan lebih banyak aturan AWS WAF terkelola berdasarkan kebutuhan Anda.

Gunakan tabel navigasi ini untuk menemukan jawaban atas pertanyaan-pertanyaan ini dengan cepat:

Jika kau mau.	Baca.
Ketahui biaya untuk menjalankan solusi ini. Total biaya untuk menjalankan solusi ini tergantung pada perlindungan yang diaktifkan dan jumlah data yang dicerna, disimpan, dan diproses.	Biaya
Pahami pertimbangan keamanan untuk solusi ini.	Keamanan

Jika kau mau.	Baca.
Ketahui mana Wilayah AWS yang didukung untuk solusi ini.	Didukung Wilayah AWS
Lihat atau unduh CloudFormation templat yang disertakan dalam solusi ini untuk secara otomatis menyebarkan sumber daya infrastru ktur (“tumpukan”) untuk solusi ini.	AWS CloudFormation Template
Gunakan AWS Support untuk membantu Anda menerapkan, menggunakan, atau memecahka n masalah solusi.	AWS Support
Akses kode sumber dan secara opsional gunakan AWS Cloud Development Kit (AWS CDK) untuk menyebarkan solusi	GitHubrepositori

Fitur dan manfaat

Otomatisasi Keamanan untuk AWS WAF solusi menyediakan fitur dan manfaat berikut.

Amankan aplikasi web Anda dengan grup Peraturan yang Dikelola AWS aturan

Peraturan yang Dikelola AWS untuk AWS WAF memberikan perlindungan terhadap kerentanan aplikasi umum atau lalu lintas yang tidak diinginkan lainnya. Solusi ini mencakup grup aturan reputasi IP AWSAWS Terkelola, grup aturan dasar terkelola, dan grup aturan khusus kasus penggunaan AWS terkelola. Anda memiliki opsi untuk memilih satu atau beberapa grup aturan untuk web AndaACL, hingga kuota unit ACL kapasitas web maksimum (WCU).

Menyediakan perlindungan banjir lapisan 7 dengan aturan kustom HTTP Banjir yang telah ditentukan

Aturan kustom HTTPFlood melindungi terhadap serangan web-layer Distributed Denial-of-Service (DDoS) untuk periode waktu yang ditentukan pelanggan. Anda dapat memilih salah satu opsi ini untuk mengaktifkan aturan ini:

- AWS WAF aturan berbasis tarif
- Pengurai log Lambda
- Pengurai log Amazon Athena

Opsi parser log Lambda atau parser log Athena memungkinkan Anda menentukan kuota permintaan kurang dari 100. Pendekatan ini dapat membantu Anda tidak mencapai kuota yang disyaratkan oleh aturan AWS WAF berbasis tarif. Untuk informasi selengkapnya, lihat Opsi pengurai log.

Anda juga dapat meningkatkan parser log Athena dengan menambahkan negara dan Uniform Resource Identifier (URI) ke kondisi pemfilteran. Pendekatan ini mengidentifikasi dan memblokir serangan HTTP banjir yang memiliki pola yang tidak terdugaURI. Untuk informasi lebih lanjut, lihat Gunakan negara dan URI di pengurai log HTTP Flood Athena.

Blokir eksploitasi kerentanan dengan aturan kustom Scanner & Probe yang telah ditentukan

Aturan kustom Scanners & Probe mem-parsing log akses aplikasi yang mencari perilaku mencurigakan, seperti jumlah kesalahan abnormal yang dihasilkan oleh asal. Kemudian memblokir alamat IP sumber yang mencurigakan untuk jangka waktu yang ditentukan pelanggan. Anda dapat memilih salah satu opsi ini untuk mengaktifkan aturan ini: Lambda log parser atau Athena log parser. Untuk informasi selengkapnya, lihat Opsi pengurai log.

Mendeteksi dan membelokkan intrusi dengan aturan kustom Bad Bot yang telah ditentukan

Aturan kustom Bad Bot menetapkan titik akhir honeypot, yang merupakan mekanisme keamanan yang dimaksudkan untuk memikat dan menangkis serangan yang dicoba. Anda dapat memasukkan titik akhir di situs web Anda untuk mendeteksi permintaan masuk dari pencakar konten dan bot buruk. Setelah terdeteksi, permintaan berikutnya dari asal yang sama akan diblokir. Untuk informasi selengkapnya, lihat Menyematkan tautan Honeypot di aplikasi web Anda.

Blokir alamat IP berbahaya dengan reputasi IP yang telah ditentukan sebelumnya mencantumkan aturan kustom

Reputasi IP mencantumkan aturan khusus memeriksa daftar reputasi IP pihak ketiga setiap jam untuk rentang IP baru yang akan diblokir. Daftar ini termasuk daftar Spamhaus Don't Route Or Peer (DROP) dan Extended DROP (EDROP), daftar IP Proofpoint Emerging Threats, dan daftar node keluar Tor.

Menyediakan konfigurasi IP manual dengan aturan kustom daftar IP yang diizinkan dan ditolak yang telah ditentukan

Aturan kustom daftar IP yang diizinkan dan ditolak memungkinkan Anda memasukkan alamat IP secara manual yang ingin Anda izinkan atau tolak. Anda juga dapat mengonfigurasi retensi IP pada daftar IP yang Diizinkan dan Ditolak untuk IPs kedaluwarsa pada waktu yang ditentukan.

Bangun dasbor pemantauan Anda sendiri

Solusi ini memancarkan CloudWatch metrik Amazon seperti permintaan yang diizinkan, permintaan yang diblokir, dan metrik relevan lainnya. Anda dapat membuat dasbor khusus untuk memvisualisasikan metrik ini dan mendapatkan wawasan tentang pola serangan dan perlindungan yang disediakan oleh. AWS WAF Untuk informasi selengkapnya, lihat Dasbor pemantauan Build.

Integrasi dengan Service Catalog AppRegistry dan Manajer Aplikasi AWS Systems Manager

Solusi ini mencakup AppRegistry sumber daya Service Catalog untuk mendaftarkan CloudFormation template solusi dan sumber daya dasarnya sebagai aplikasi di AWS Service Catalog AppRegistry dan AWS Systems Manager Application Manager. Dengan integrasi ini, Anda dapat mengelola sumber daya solusi secara terpusat.

Kasus penggunaan

Tanggal publikasi: September 2016 (pembaruan terakhir: Mei 2023)

Berikut ini adalah contoh kasus penggunaan untuk menggunakan solusi ini. Anda dapat menyesuaikan solusi ini dengan cara inovatif yang tidak terbatas pada daftar ini.

Otomatiskan pengaturan aturan AWS WAF

AWS WAF melindungi aplikasi web Anda dari serangan umum; Namun, pengaturan AWS WAF aturan bisa rumit dan memakan waktu. Untuk membantu Anda, solusi ini secara otomatis menerapkan seperangkat AWS WAF aturan ke akun Anda dengan CloudFormation templat. Dengan cara ini, Anda tidak perlu mengonfigurasi AWS WAF aturan sendiri, dan Anda dapat memulai dengan AWS WAF lebih cepat.

Kustomisasi lapisan 7 Perlindungan HTTP banjir

Solusi ini menyediakan tiga opsi untuk mengaktifkan perlindungan HTTP Banjir. Anda dapat memilih opsi yang sesuai dengan kebutuhan Anda untuk mendapatkan perlindungan terhadap DDoS serangan. Untuk informasi selengkapnya, lihat Menyediakan perlindungan banjir lapisan 7 dengan aturan kustom HTTP Banjir yang telah ditentukan sebelumnya di Fitur dan manfaat.

Manfaatkan kode sumber untuk menerapkan kustomisasi atau membangun otomatisasi keamanan Anda sendiri

Solusi ini memberikan contoh tentang cara menggunakan AWS WAF dan layanan lain untuk membangun otomatisasi keamanan di AWS Cloud. Kode sumber terbukanya GitHub memudahkan Anda untuk menerapkan penyesuaian atau membangun otomatisasi keamanan Anda sendiri yang sesuai dengan kebutuhan Anda.

Konsep dan definisi

Bagian ini menjelaskan konsep-konsep kunci dan mendefinisikan terminologi khusus untuk solusi ini.

ALBlog

Solusi ini menggunakan log untuk ALB sumber daya. Aturan Scanner & Probe Protection dalam solusi ini memeriksa log ini.

Pengurai log Athena

Amazon Athena adalah layanan analitik interaktif tanpa server yang dibangun di atas kerangka kerja sumber terbuka, mendukung format tabel terbuka dan file. Solusi ini menjalankan kueri Athena terjadwal untuk memeriksa AWS WAF, CloudFront, atau ALB mencatat jika pengguna memilih `yes - Amazon Athena log parser` saat mengaktifkan aturan Perlindungan HTTP Banjir atau aturan Perlindungan Pemindai & Probe.

AWS WAF aturan

AWS WAF Aturan mendefinisikan:

- Cara memeriksa HTTP (S) permintaan web
- Tindakan yang harus diambil berdasarkan permintaan jika sesuai dengan kriteria inspeksi

Anda mendefinisikan aturan hanya dalam konteks grup aturan atau webACL.

CloudFront log

Solusi ini menggunakan log untuk CloudFront sumber daya. Aturan Scanner & Probe Protection dalam solusi ini memeriksa log ini.

Set IP

Set IP menyediakan kumpulan alamat IP dan rentang alamat IP yang ingin Anda gunakan

bersama-sama dalam sebuah pernyataan aturan. Set IP adalah AWS sumber daya.

Pengurai log Lambda

Solusi ini menjalankan fungsi Lambda yang dipanggil oleh peristiwa pembuatan objek Amazon Simple Storage Service (Amazon S3). Fungsi Lamba memulai inspeksi AWS WAF, CloudFront, atau ALB mencatat jika pengguna memilih `yes – AWS Lambda log parser` saat mengaktifkan aturan Perlindungan HTTP Banjir atau aturan Scanner & Probe Protection.

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 berlaku untuk penggunaan grup aturan terkelola oleh Anda.

jenis sumber daya/titik akhir

Anda dapat mengaitkan AWS sumber daya dengan web ACLs untuk melindunginya. Sumber daya ini adalah CloudFront, API Gateway,, ALB AWS AppSync, Amazon Cognito, AWS App Runner, dan sumber daya Akses AWS Terverifikasi. Saat ini solusi ini Amazon mendukung CloudFront danALB.

WAFlog

Solusi ini menggunakan log yang dihasilkan oleh AWS WAF untuk sumber daya yang terkait dengan webACL. Aturan Perlindungan HTTP Banjir untuk solusi ini memeriksa log ini.

WCU

AWS WAF menggunakan daftar kontrol akses web (ACL) unit kapasitas (WCUs) untuk menghitung dan mengontrol sumber daya operasi yang diperlukan untuk menjalankan aturan, grup aturan, dan web AndaACLs. AWS WAF memberlakukan WCU kuota saat Anda mengonfigurasi grup aturan dan web Anda. ACLs WCUstidak mempengaruhi cara AWS WAF memeriksa lalu lintas web.

web ACL

Web ACL memberi Anda kontrol halus atas permintaan web HTTP (S) yang ditanggapi oleh sumber daya terlindungi Anda.

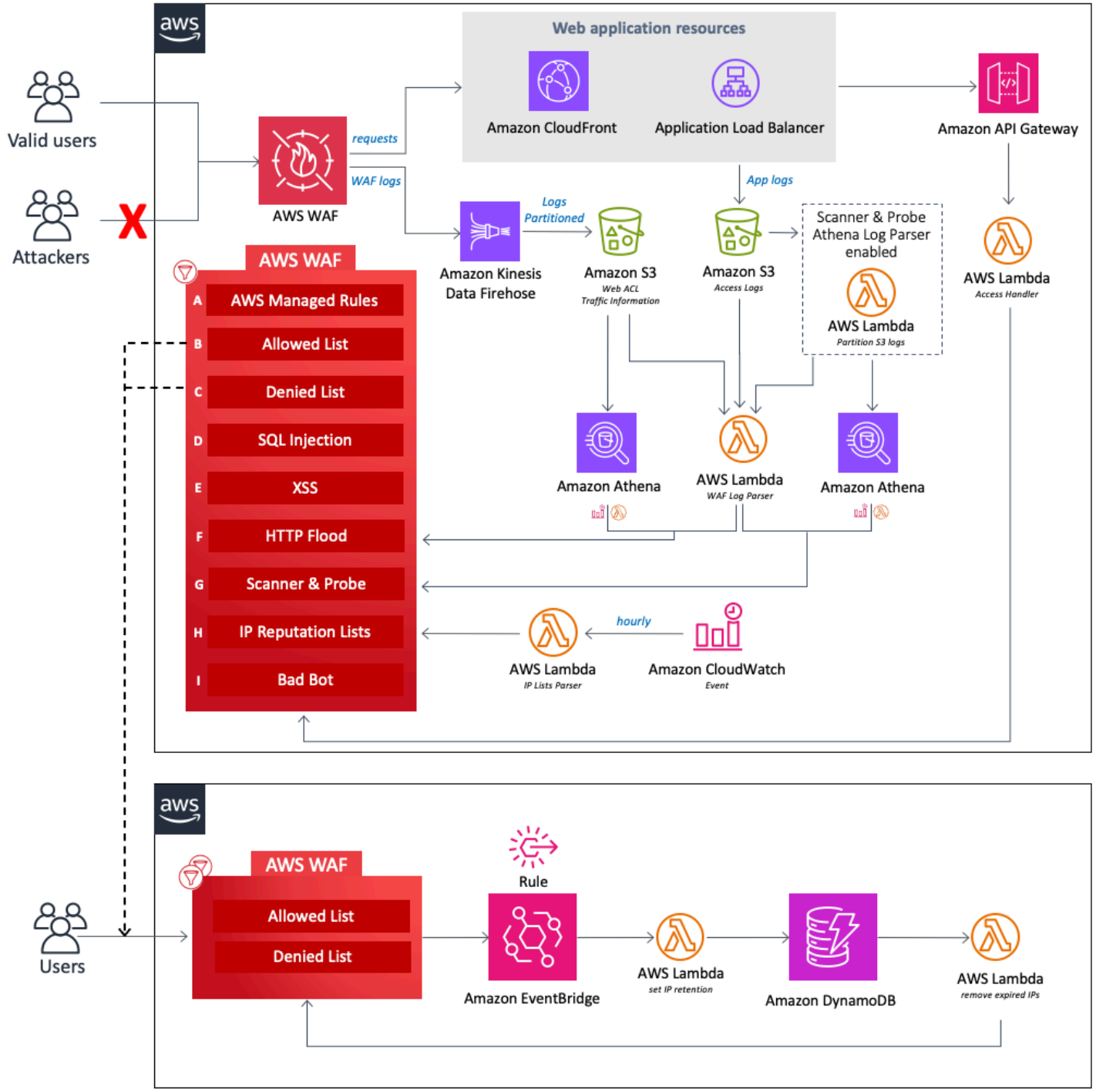
> **Note**
>
> Untuk referensi umum AWS istilah, lihat AWS Glosarium.

Gambaran umum arsitektur

Bagian ini menyediakan diagram arsitektur implementasi referensi untuk komponen yang digunakan dengan solusi ini.

Diagram arsitektur

Menerapkan solusi ini dengan parameter default menyebarkan komponen berikut di file Anda. Akun AWS



Otomasi Keamanan untuk AWS WAF arsitektur di AWS

Inti dari desain adalah AWS WAFwebACL, yang bertindak sebagai inspeksi pusat dan titik keputusan untuk semua permintaan yang masuk ke aplikasi web. Selama konfigurasi awal CloudFormation tumpukan, pengguna menentukan komponen pelindung mana yang akan diaktifkan. Setiap komponen beroperasi secara independen dan menambahkan aturan yang berbeda ke webACL.

Komponen solusi ini dapat dikelompokkan ke dalam bidang perlindungan berikut.

> **Note**
>
> Label grup tidak mencerminkan tingkat prioritas WAF aturan.

- AWS Aturan Terkelola (A) - Komponen ini berisi grup aturan reputasi Peraturan yang Dikelola AWS IP, grup aturan dasar, dan grup aturan khusus kasus penggunaan. Kelompok aturan ini melindungi terhadap eksploitasi kerentanan aplikasi umum atau lalu lintas lain yang tidak diinginkan, termasuk yang dijelaskan dalam OWASPpublikasi, tanpa harus menulis aturan Anda sendiri.
- Daftar IP manual (B dan C) — Komponen ini membuat dua AWS WAF aturan. Dengan aturan ini, Anda dapat memasukkan alamat IP secara manual yang ingin Anda izinkan atau tolak. Anda dapat mengonfigurasi retensi IP dan menghapus alamat IP kedaluwarsa pada set IP yang diizinkan atau ditolak menggunakan EventBridge aturan Amazon dan AmazonDynamoDB. Untuk informasi selengkapnya, lihat Konfigurasi retensi IP pada set AWS WAF IP yang Diizinkan dan Ditolak.
- SQLInjection (D) dan XSS (E) - Komponen ini mengkonfigurasi dua AWS WAF aturan yang dirancang untuk melindungi terhadap SQL injeksi umum atau pola cross-site scripting (XSS) dalamURI, string kueri, atau badan permintaan.
- HTTPFlood (F) — Komponen ini melindungi terhadap serangan yang terdiri dari sejumlah besar permintaan dari alamat IP tertentu, seperti DDoS serangan web-layer atau upaya login brute-force. Dengan aturan ini, Anda menetapkan kuota yang menentukan jumlah maksimum permintaan masuk yang diizinkan dari satu alamat IP dalam periode lima menit default (dapat dikonfigurasi dengan parameter Jadwal Waktu Jalankan Kueri Athena). Setelah ambang batas ini dilanggar, permintaan tambahan dari alamat IP diblokir sementara. Anda dapat menerapkan aturan ini dengan menggunakan aturan AWS WAF berbasis laju, atau dengan memproses AWS WAF log menggunakan fungsi Lambda atau kueri Athena. Untuk informasi selengkapnya tentang pengorbanan yang terkait dengan opsi mitigasi HTTP banjir, lihat Opsi pengurai log.
- Scanner and Probe (G) - Komponen ini mem-parsing log akses aplikasi yang mencari perilaku mencurigakan, seperti jumlah kesalahan abnormal yang dihasilkan oleh asal. Kemudian memblokir alamat IP sumber yang mencurigakan untuk jangka waktu yang ditentukan pelanggan. Anda dapat menerapkan aturan ini menggunakan fungsi Lambda atau kueri Athena. Untuk informasi selengkapnya tentang pengorbanan yang terkait dengan opsi mitigasi pemindai dan probe, lihat opsi pengurai Log.
- Daftar Reputasi IP (H) - Komponen ini adalah fungsi `IP Lists Parser` Lambda yang memeriksa daftar reputasi IP pihak ketiga setiap jam untuk rentang baru yang akan diblokir. Daftar ini

termasuk daftar Spamhaus Don't Route Or Peer (DROP) dan Extended DROP (EDROP), daftar IP Proofpoint Emerging Threats, dan daftar node keluar Tor.

- Bad Bot (I) — Komponen ini secara otomatis menyiapkan honeypot, yang merupakan mekanisme keamanan yang dimaksudkan untuk memikat dan menangkis serangan yang dicoba. Honeypot solusi ini adalah titik akhir jebakan yang dapat Anda masukkan di situs web Anda untuk mendeteksi permintaan masuk dari pencakar konten dan bot buruk. Jika sumber mengakses honeypot, fungsi `Access Handler` Lambda mencegat dan memeriksa permintaan untuk mengekstrak alamat IP-nya, dan kemudian menambahkannya ke daftar blokir. AWS WAF

Masing-masing dari tiga fungsi Lambda kustom dalam solusi ini menerbitkan metrik runtime ke. CloudWatch Untuk informasi lebih lanjut tentang fungsi Lambda ini, lihat detail Komponen.

AWSPertimbangan desain Well-Architected

Solusi ini menggunakan praktik terbaik dari AWS Well-Architected Framework, yang membantu pelanggan merancang dan mengoperasikan beban kerja yang andal, aman, efisien, dan hemat biaya di cloud.

Bagian ini menjelaskan bagaimana prinsip-prinsip desain dan praktik terbaik dari Well-Architected Framework menguntungkan solusi ini.

Keunggulan operasional

Bagian ini menjelaskan bagaimana kami merancang solusi ini menggunakan prinsip dan praktik terbaik dari pilar keunggulan operasional.

- Solusi ini mendorong metrik untuk CloudWatch menyediakan observabilitas ke dalam infrastruktur, fungsi Lambda, Amazon Data Firehose, API Gateway, Amazon S3 bucket, dan komponen solusi lainnya.
- Kami mengembangkan, menguji, dan mempublikasikan solusi melalui pipeline AWS continuous integration and continuous delivery (CI/CD). Ini membantu pengembang mencapai hasil berkualitas tinggi secara konsisten.
- Anda dapat menginstal solusi dengan CloudFormation templat yang menyediakan semua sumber daya yang diperlukan di akun Anda. Untuk memperbarui atau menghapus solusi, Anda hanya perlu memperbarui atau menghapus template.

Keamanan

Bagian ini menjelaskan bagaimana kami merancang solusi ini menggunakan prinsip dan praktik terbaik pilar keamanan.

- Semua komunikasi antar-layanan menggunakan AWS Identity and Access Management(IAM) peran.
- Semua peran yang digunakan oleh solusi mengikuti akses hak istimewa paling sedikit. Dengan kata lain, mereka hanya berisi izin minimum yang diperlukan sehingga layanan dapat berfungsi dengan baik.
- Semua penyimpanan data, termasuk bucket Amazon S3 dan DynamoDB, memiliki enkripsi saat istirahat.

Keandalan

Bagian ini menjelaskan bagaimana kami merancang solusi ini menggunakan prinsip dan praktik terbaik dari pilar keandalan.

- Solusi ini menggunakan layanan AWS tanpa server sedapat mungkin (misalnya, Lambda, Firehose, Gateway, Amazon S3API, dan Athena) untuk memastikan ketersediaan dan pemulihan yang tinggi dari kegagalan layanan.
- Kami melakukan pengujian otomatis pada solusi untuk mendeteksi dan memperbaiki kesalahan dengan cepat.
- Solusinya menggunakan fungsi Lambda untuk pemrosesan data. Solusi ini menyimpan data di Amazon S3 dan DynamoDB, dan tetap ada di beberapa Zona Avaialbility secara default.

Efisiensi kinerja

Bagian ini menjelaskan bagaimana kami merancang solusi ini menggunakan prinsip dan praktik terbaik dari pilar efisiensi kinerja.

- Solusinya menggunakan arsitektur tanpa server untuk memastikan skalabilitas dan ketersediaan tinggi dengan biaya yang lebih rendah.
- Solusi ini meningkatkan kinerja database dengan memparitisi data dan mengoptimalkan kueri untuk mengurangi jumlah pemindaian data dan mencapai hasil yang lebih cepat.

- Solusinya secara otomatis diuji dan digunakan setiap hari. Arsitek solusi dan ahli materi pelajaran kami meninjau solusi untuk area untuk bereksperimen dan meningkatkan.

Optimalisasi Biaya

Bagian ini menjelaskan bagaimana kami merancang solusi ini menggunakan prinsip dan praktik terbaik dari pilar pengoptimalan biaya.

- Solusinya menggunakan arsitektur tanpa server, dan pelanggan hanya membayar untuk apa yang mereka gunakan.
- Lapisan komputasi solusi default ke Lambda, yang menggunakan model. pay-per-use
- Database dan kueri Athena dioptimalkan untuk mengurangi jumlah pemindaian data, sehingga mengurangi biaya.

Keberlanjutan

Bagian ini menjelaskan bagaimana kami merancang solusi ini menggunakan prinsip dan praktik terbaik pilar keberlanjutan.

- Solusinya menggunakan layanan terkelola dan tanpa server untuk meminimalkan dampak lingkungan dari layanan backend.
- Desain tanpa server solusi ini ditujukan untuk mengurangi jejak karbon dibandingkan dengan jejak server lokal yang terus beroperasi.

Detail arsitektur

Bagian ini menjelaskan komponen dan AWS layanan yang membentuk solusi ini dan detail arsitektur tentang bagaimana komponen ini bekerja sama.

AWS layanan dalam solusi ini

AWS layanan	Deskripsi	
AWS WAF	Inti. Menyebarkan AWS WAF webACL, grup Peraturan yang Dikelola AWS aturan, aturan khusus, dan set IP. Membuat AWS WAF API panggilan untuk memblokir serangan umum dan mengamankan aplikasi web.	
Amazon Data Firehose	Inti. Mengirimkan AWS WAF log ke ember Amazon S3.	
Amazon S3	Inti. Toko AWS WAF, CloudFront, dan ALB log.	
AWS Lambda	Inti. Menerapkan beberapa fungsi Lambda untuk mendukung aturan khusus.	
Amazon EventBridge	Inti. Membuat aturan acara untuk memanggil Lambda.	
Amazon Athena	Mendukung. Membuat kueri Athena dan kelompok kerja untuk mendukung pengurai log Athena.	

AWS layanan	Deskripsi	
AWS Glue	Mendukung. Membuat database dan tabel untuk mendukung parser log Athena.	
APIGerbang Amazon	Mendukung. Menciptakan titik akhir honeypot bot yang buruk.	
Amazon SNS	Mendukung. Mengirim pemberitahuan email Amazon Simple Notification Service (AmazonSNS) untuk mendukung retensi IP pada daftar yang diizinkan dan ditolak.	
AWS Systems Manager	Mendukung. Menyediakan pemantauan sumber daya tingkat aplikasi dan visualisasi operasi sumber daya dan data biaya.	

Opsi pengurai log

Seperti yang dijelaskan dalam ikhtisar Arsitektur, ada tiga opsi untuk menangani perlindungan HTTP banjir dan pemindai dan probe. Bagian berikut menjelaskan masing-masing opsi ini secara lebih rinci.

AWS WAF aturan berbasis tarif

Aturan berbasis tarif tersedia untuk perlindungan HTTP banjir. Secara default, aturan berbasis tarif mengumpulkan dan membatasi permintaan berdasarkan alamat IP permintaan. Solusi ini memungkinkan Anda untuk menentukan jumlah permintaan web yang memungkinkan IP klien dalam periode lima menit yang tertinggal dan terus diperbarui. Jika alamat IP melanggar kuota yang dikonfigurasi, AWS WAF blokir permintaan baru yang diblokir hingga tingkat permintaan kurang dari kuota yang dikonfigurasi.

Sebaiknya pilih opsi aturan berbasis tarif jika kuota permintaan lebih dari 2.000 permintaan per lima menit dan Anda tidak perlu menerapkan penyesuaian. Misalnya, Anda tidak mempertimbangkan akses sumber daya statis saat menghitung permintaan.

Anda selanjutnya dapat mengonfigurasi aturan untuk menggunakan berbagai tombol agregasi dan kombinasi tombol lainnya. Untuk informasi selengkapnya, lihat Opsi dan kunci agregasi.

Pengurai log Amazon Athena

Parameter template Perlindungan HTTP Banjir dan Pemindai & Probe Protection menyediakan opsi pengurai log Athena. Saat diaktifkan, berikan CloudFormation kueri Athena dan fungsi Lambda terjadwal yang bertanggung jawab untuk mengatur Athena untuk dijalankan, memproses hasil keluaran, dan memperbarui. AWS WAF Fungsi Lambda ini dipanggil oleh CloudWatch acara yang dikonfigurasi untuk dijalankan setiap lima menit. Ini dapat dikonfigurasi dengan parameter Athena Query Run Time Schedule.

Sebaiknya pilih opsi ini ketika Anda tidak dapat menggunakan aturan AWS WAF berbasis tarif dan Anda memiliki keakraban SQL untuk menerapkan penyesuaian. Untuk informasi selengkapnya tentang cara mengubah kueri default, lihat Lihat kueri Amazon Athena.

HTTPperlindungan banjir didasarkan pada pemrosesan log AWS WAF akses dan menggunakan file WAF log. Jenis log WAF akses memiliki jeda waktu yang lebih rendah, yang dapat Anda gunakan untuk mengidentifikasi asal HTTP banjir lebih cepat jika dibandingkan dengan CloudFront atau ALB mencatat waktu pengiriman. Namun, Anda harus memilih jenis CloudFront atau ALB log di parameter template Activate Scanner & Probe Protection untuk menerima kode status respons.

AWS Lambda pengurai log

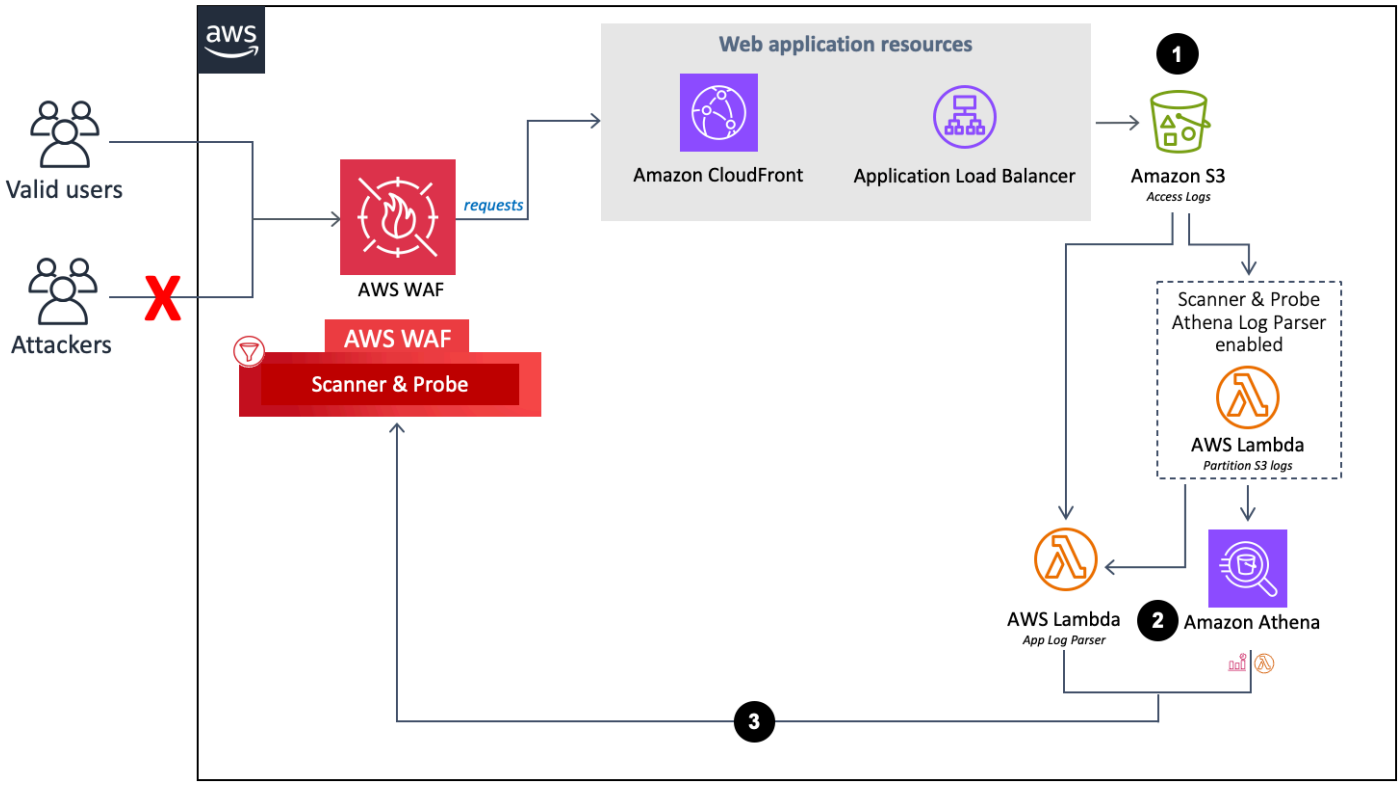
Parameter template HTTPFlood Protection dan Scanner & Probe Protection menyediakan opsi AWS Lambda Log Parser. Gunakan pengurai log Lambda hanya jika aturan AWS WAF berbasis tarif dan opsi pengurai log Amazon Athena tidak tersedia. Batasan yang diketahui dari opsi ini adalah bahwa informasi diproses dalam konteks file yang sedang diproses. Misalnya, IP mungkin menghasilkan lebih banyak permintaan atau kesalahan daripada kuota yang ditentukan, tetapi karena informasi ini dibagi menjadi file yang berbeda, setiap file tidak menyimpan cukup data untuk melebihi kuota.

Detail komponen

Seperti yang dijelaskan dalam diagram Arsitektur, empat komponen solusi ini menggunakan otomatisasi untuk memeriksa alamat IP dan menambahkannya ke daftar AWS WAF blok. Bagian berikut menjelaskan masing-masing komponen ini secara lebih rinci.

Log parser - Aplikasi

Pengurai log Aplikasi membantu melindungi dari pemindai dan probe.



Alur parser log aplikasi

1. Ketika CloudFront atau ALB menerima permintaan atas nama aplikasi web Anda, ia mengirimkan log akses ke bucket Amazon S3.
   a. (Opsional) Jika Anda memilih `Yes - Amazon Athena log parser` parameter template Aktifkan Perlindungan HTTP Banjir dan Aktifkan Pemindai & Probe Protection, fungsi Lambda memindahkan log akses dari folder aslinya `<customer-bucket>`/AWSLogs ke folder yang baru dipartisi `<customer-bucket>`/AWSLogs-partitioned/`<optional-prefix>` / year=`<YYYY>`/month=`<MM>` /day=`<DD>`/hour=`<HH>`/ saat tiba di Amazon S3.

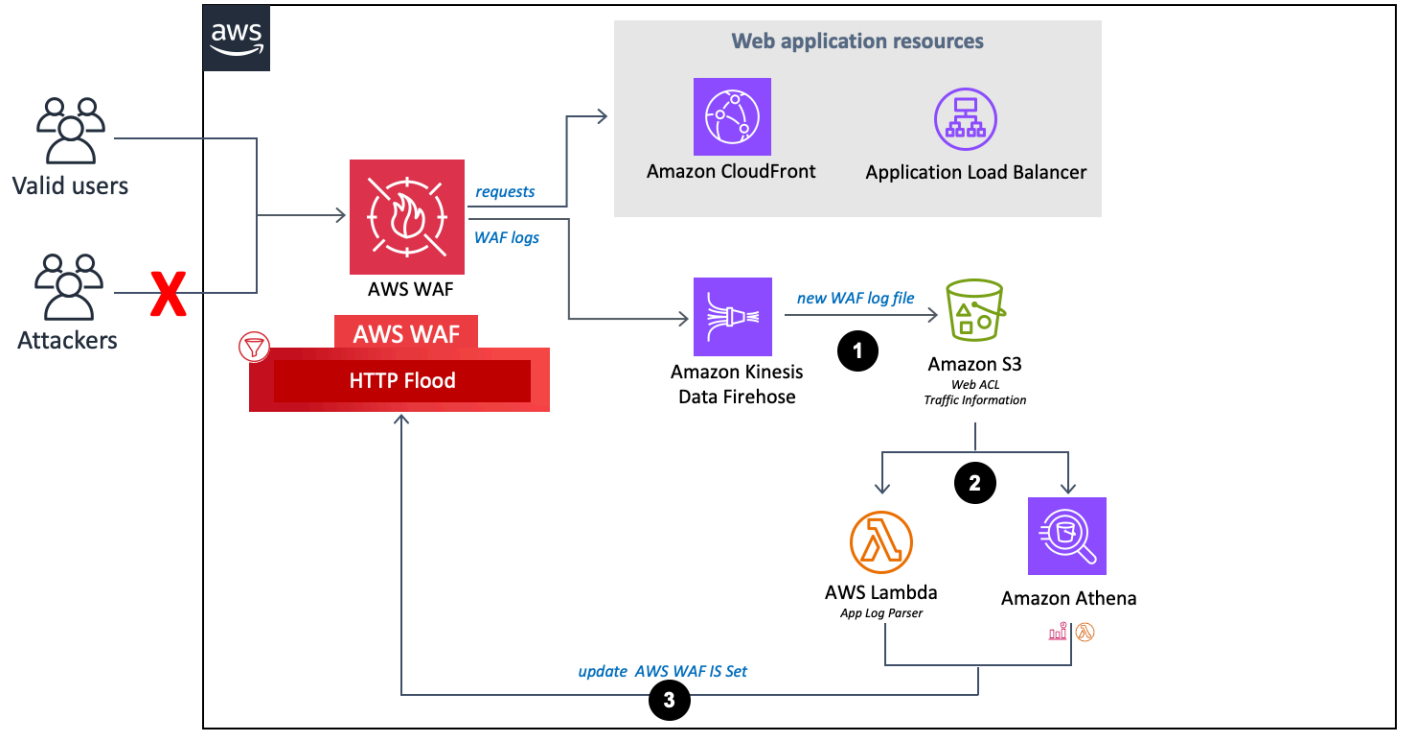
b. (Opsional) Jika Anda memilih `yes` untuk Simpan Data di parameter template lokasi S3 Asli, log tetap berada di lokasi aslinya dan disalin ke folder yang dipartisi, menduplikasi penyimpanan log Anda.

> **Note**
>
> Untuk pengurai log Athena, solusi ini hanya mempartisi log baru yang tiba di bucket Amazon S3 Anda setelah Anda menerapkan solusi ini. Jika Anda memiliki log yang ingin Anda partisi, Anda harus mengunggah log tersebut secara manual ke Amazon S3 setelah Anda menerapkan solusi ini.

2. Berdasarkan pilihan Anda untuk parameter template Activate HTTP Flood Protection dan Activate Scanner & Probe Protection, solusi ini memproses log menggunakan salah satu dari berikut ini:
   a. Lambda - Setiap kali log akses baru disimpan di bucket Amazon S3, fungsi `Log Parser` Lambda dimulai.
   b. Athena - Secara default, setiap lima menit kueri Scanner & Probe Protection Athena berjalan, dan output mendorong ke. AWS WAF Proses ini diprakarsai oleh sebuah CloudWatch peristiwa, yang memulai fungsi Lambda yang bertanggung jawab untuk menjalankan kueri Athena dan mendorong hasilnya ke dalam. AWS WAF
3. Solusi ini menganalisis data log untuk mengidentifikasi alamat IP yang menghasilkan lebih banyak kesalahan daripada kuota yang ditentukan. Solusinya kemudian memperbarui kondisi set AWS WAF IP untuk memblokir alamat IP tersebut untuk jangka waktu yang ditentukan pelanggan.

Pengurai log - AWS WAF

Jika Anda memilih `yes - AWS Lambda log parser` atau `yes - Amazon Athena log parser` untuk Aktifkan Perlindungan HTTP Banjir, solusi ini menyediakan komponen berikut, yang mengurai AWS WAF log untuk mengidentifikasi dan memblokir asal yang membanjiri titik akhir dengan tingkat permintaan yang lebih besar dari kuota yang Anda tentukan.

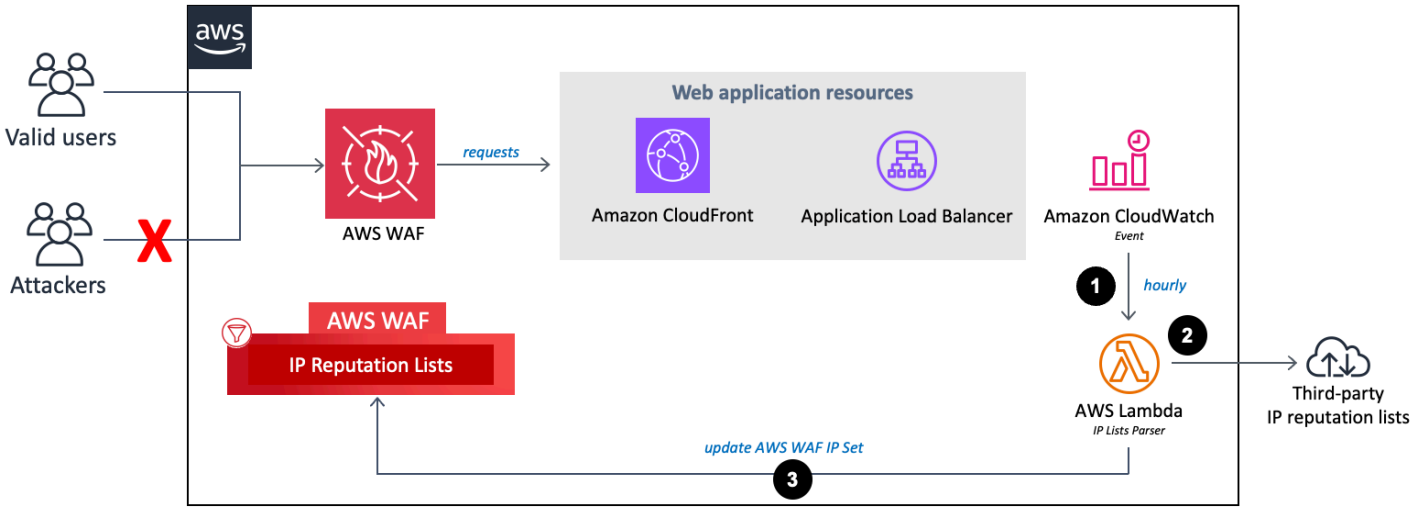


AWS WAF aliran pengurai log

1. Saat AWS WAF menerima log akses, log akan dikirim ke titik akhir Firehose. Firehose kemudian mengirimkan log ke bucket yang dipartisi di Amazon S3 bernama `<customer-bucket>/AWSLogs/ <optional-prefix>/year=<YYYY> /month=<MM>/day=<DD>/hour= <HH>/`
2. Berdasarkan pilihan Anda untuk parameter template Activate HTTP Flood Protection dan Activate Scanner & Probe Protection, solusi ini memproses log menggunakan salah satu dari berikut ini:
   a. Lambda: Setiap kali log akses baru disimpan di bucket Amazon S3, fungsi `Log Parser` Lambda dimulai.
   b. Athena: Secara default, setiap lima menit kueri pemindai dan probe Athena dijalankan dan output didorong ke. AWS WAF Proses ini diprakarsai oleh CloudWatch acara Amazon, yang kemudian memulai fungsi Lambda yang bertanggung jawab untuk mengeksekusi kueri Amazon Athena, dan mendorong hasilnya ke dalam. AWS WAF
3. Solusi ini menganalisis data log untuk mengidentifikasi alamat IP yang mengirim lebih banyak permintaan daripada kuota yang ditentukan. Solusinya kemudian memperbarui kondisi set AWS WAF IP untuk memblokir alamat IP tersebut untuk jangka waktu yang ditentukan pelanggan.

Pengurai daftar IP

Fungsi `IP Lists Parser` Lambda membantu melindungi terhadap penyerang yang dikenal yang diidentifikasi dalam daftar reputasi IP pihak ketiga.

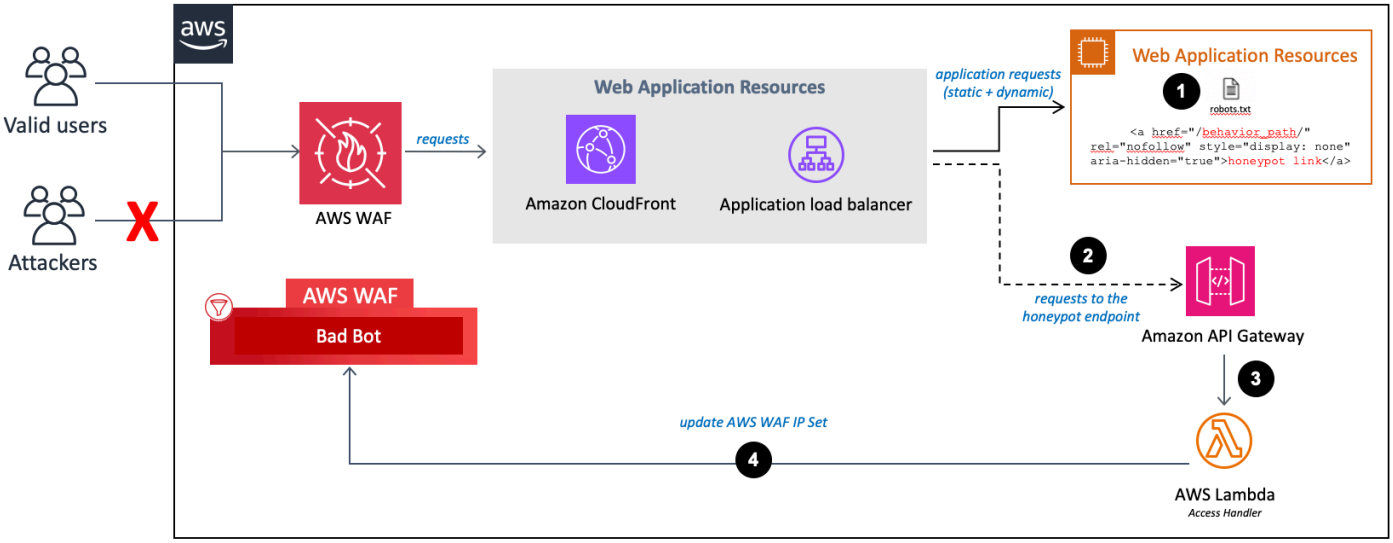


Reputasi IP mencantumkan aliran parser

1. CloudWatch Acara Amazon setiap jam memanggil fungsi Lambda`IP Lists Parser`.
2. Fungsi Lambda mengumpulkan dan mem-parsing data dari tiga sumber:
   - Spamhaus DROP dan daftar EDROP
   - Daftar IP Proofpoint Emerging Threats
   - Daftar node keluar Tor
3. Fungsi Lambda memperbarui daftar AWS WAF blok dengan alamat IP saat ini.

Penangan Akses

Fungsi `Access Handler` Lambda memeriksa permintaan ke titik akhir honeypot untuk mengekstrak alamat IP sumbernya.



Akses Handler dan titik akhir honeypot

1. Sematkan titik akhir honeypot di situs web Anda dan perbarui standar pengecualian robot Anda, seperti yang dijelaskan dalam Sematkan Tautan Honeypot di Aplikasi Web Anda (Opsional).
2. Ketika pengikis konten atau bot buruk mengakses titik akhir honeypot, itu memanggil fungsi Lambda. `Access Handler`
3. Fungsi Lambda mencegat dan memeriksa header permintaan untuk mengekstrak alamat IP dari sumber yang mengakses titik akhir perangkap.
4. Fungsi Lambda memperbarui kondisi set AWS WAF IP untuk memblokir alamat IP tersebut.

Rencanakan penyebaran Anda

Bagian ini menjelaskan biaya, keamananthe section called “Kuota”, dan pertimbangan lain sebelum menerapkan solusi.

Didukung Wilayah AWS

Bergantung pada nilai parameter input template yang Anda tentukan, solusi ini membutuhkan sumber daya yang berbeda. Sumber daya ini (tercantum dalam tabel berikut) mungkin tidak tersedia di semua Wilayah AWS. Oleh karena itu, Anda harus meluncurkan solusi ini Wilayah AWS di mana layanan ini tersedia. Untuk ketersediaan AWS layanan terbaru menurut Wilayah, lihat Daftar Layanan Wilayah AWS al.

	AWS WAF Web ACL	AWS Glue	Amazon Athena	Amazon Kinesis Data Firehose
Jenis titik akhir				
CloudFront	✓			
Application Load Balancer () ALB	✓			
Aktifkan Perlindungan HTTP Banjir				
ya - pengurai AWS Lambda log				✓
ya - Pengurai log Amazon Athena		✓	✓	✓
Aktifkan Scanner & Probe Protection				
ya - Pengurai log Amazon Athena		✓	✓	

> **Note**
>
> Jika Anda memilih `CloudFront` sebagai Endpoint Anda, Anda harus menerapkan solusi di Wilayah AS Timur (Virginia N.) (). `us-east-1`

Biaya

Anda bertanggung jawab atas biaya AWS layanan yang digunakan saat menjalankan otomatisasi keamanan untuk AWS WAF solusi. Total biaya untuk menjalankan solusi ini tergantung pada perlindungan yang diaktifkan dan jumlah data yang dicerna, disimpan, dan diproses.

Kami merekomendasikan membuat anggaran melalui AWS Cost Exploreruntuk membantu mengelola biaya. Untuk detail selengkapnya, lihat halaman web harga untuk setiap AWS layanan yang Anda gunakan dalam solusi ini.

Tabel berikut adalah contoh rincian biaya untuk menjalankan solusi ini di Wilayah AS Timur (Virginia N.) (tidak termasuk AWS Tingkat Gratis). Harga dapat berubah sewaktu-waktu.

Contoh 1: Aktifkan Perlindungan Daftar Reputasi, Perlindungan Bot Buruk, Pengurai AWS Lambda Log untuk Perlindungan HTTP Banjir, dan Perlindungan Pemindai & Probe

AWS layanan	Dimensi/Bulan	Biaya [USD]
Amazon Data Firehose	100 GB	~$2,90
Amazon S3	100 GB	~$2,30
AWS Lambda	128 MB: 3 fungsi, 1M pemanggilan, dan durasi rata-rata 500 milidetik per Lambda dijalankan 512 MB: 2 fungsi, 1M pemanggilan, dan durasi rata-rata 500 milidetik per Lambda run	~$5,40
APIGerbang Amazon	1M permintaan	~$3,40

AWS layanan	Dimensi/Bulan	Biaya [USD]
AWS WAF web ACL	1	$5.00
AWS WAF aturan	4	$4,00
AWS WAF permintaan	1M	$0,60
Jumlah		~ $23,60 per bulan

Contoh 2: Aktifkan Perlindungan Daftar Reputasi, Perlindungan Bot Buruk, Parser Log Amazon Athena untuk Perlindungan HTTP Banjir, dan Perlindungan Pemindai & Probe

AWS layanan	Dimensi/Bulan	Biaya [USD]
Amazon Data Firehose	100 GB	~$2,90
Amazon S3	100 GB	~$2,30
AWS Lambda	128 MB: 3 fungsi, 1M pemanggilan, dan durasi rata-rata 500 milidetik per Lambda dijalankan 512 MB: 2 fungsi, 7560 pemanggilan, dan durasi rata-rata 500 milidetik per Lambda run	~$1,26
APIGerbang Amazon	1M permintaan	~$3,40
Amazon Athena	1.2M CloudFront objek hits atau 1,2 juta ALB permintaan per hari yang menghasilkan catatan log ~ 500 byte per hit atau permintaan	~$4,32
AWS WAF web ACL	1	$5.00

AWS layanan	Dimensi/Bulan	Biaya [USD]
AWS WAF aturan	4	$4,00
AWS WAF permintaan	1M	$0,60
Jumlah		~ $23,78 per bulan

Contoh 3: Aktifkan Retensi IP untuk Set IP yang Diizinkan dan Ditolak

AWS layanan	Dimensi/Bulan	Biaya [USD]
Amazon DynamoDB	1K menulis dan penyimpanan data 1 MB	~ $0,00
AWS Lambda	128 MB: 1 fungsi, pemanggilan 2K, dan durasi rata-rata 500 milidetik per lari Lambda 512 MB: 1 fungsi, pemanggilan 2K, dan durasi rata-rata 500 milidetik per lari Lambda	~ $0,01
Amazon CloudWatch	Acara 2K	~ $0,00
AWS WAF Web ACL	1	$5.00
AWS WAF Aturan	2	$2,00
WASWAFpermintaan	1M	$0,60
Jumlah		~ $7,61 per bulan

Perkiraan biaya CloudWatch log

Beberapa AWS layanan yang digunakan dalam solusi ini, seperti Lambda, menghasilkan CloudWatch log. Log ini dikenakan biaya. Kami merekomendasikan menghapus atau mengarsipkan log untuk

mengurangi biaya. Untuk detail arsip log, lihat Mengekspor data log ke Amazon S3 di Panduan Pengguna CloudWatch Amazon Logs.

Jika Anda memilih untuk menggunakan pengurai log Athena saat penginstalan, solusi ini menjadwalkan kueri untuk dijalankan terhadap log akses AWS WAF atau aplikasi di bucket Amazon S3 Anda seperti yang dikonfigurasi. Anda dikenakan biaya berdasarkan jumlah data yang dipindai oleh setiap kueri. Solusinya menerapkan partisi ke log dan kueri untuk meminimalkan biaya. Secara default, solusi memindahkan log akses aplikasi dari lokasi Amazon S3 aslinya ke struktur folder yang dipartisi. Anda juga dapat mempertahankan yang asli, tetapi Anda akan dikenakan biaya untuk penyimpanan log duplikat. Solusi ini menggunakan grup kerja untuk mengelompokkan beban kerja, dan Anda dapat mengonfigurasi keduanya untuk mengelola akses kueri dan biaya. Lihat Estimasi biaya Athena untuk perhitungan perkiraan biaya sampel. Untuk informasi lebih lanjut, lihat Harga Amazon Athena.

Perkiraan biaya Athena

Jika Anda menggunakan opsi pengurai log Athena saat menjalankan aturan Perlindungan HTTP Banjir atau Perlindungan Pemindai & Probe, Anda akan dikenakan biaya untuk penggunaan Athena. Secara default, setiap kueri Athena berjalan setiap lima menit dan memindai data empat jam terakhir. Solusinya menerapkan partisi ke log dan kueri Athena untuk meminimalkan biaya. Anda dapat mengonfigurasi jumlah jam data yang dipindai kueri dengan mengubah nilai untuk parameter template Periode WAF Blok. Namun, meningkatkan jumlah data yang dipindai kemungkinan akan meningkatkan biaya Athena.

> **Tip**
>
> Berikut ini adalah contoh perhitungan biaya CloudFront log:
> Rata-rata, setiap CloudFront hit mungkin menghasilkan sekitar 500 byte data.
> Jika ada 1,2 juta CloudFront objek yang terkena per hari, maka akan ada 200K (1.2M/6) hit per empat jam, dengan asumsi bahwa data dicerna pada tingkat yang konsisten.
> Pertimbangkan pola lalu lintas Anda yang sebenarnya saat menghitung biaya Anda.
> `[500 bytes of data] * [200K hits per four hours] = [an average 100 MB (0.0001TB) data scanned per query]`
> Athena mengenakan biaya $5,00 per TB data yang dipindai.
> `[0.0001 TB] * [$5] = [$0.0005 per query scan]`
> Kueri Athena berjalan setiap lima menit, yaitu 12 kali per jam.
> `[12 runs] * [24 hours] = [288 runs per day]`

```
[$0.0005 per query scan] * [288 runs per day] * [30 days] = [$4.32
per month]
```

Biaya aktual bervariasi tergantung pada pola lalu lintas aplikasi Anda. Untuk informasi lebih lanjut, lihat Harga Amazon Athena.

Keamanan

Ketika Anda membangun sistem di atas AWS infrastruktur, tanggung jawab keamanan dibagi antara Anda dan AWS. Model tanggung jawab bersama ini mengurangi beban operasional Anda karena AWS mengoperasikan, mengelola, dan mengontrol komponen termasuk sistem operasi host, lapisan virtualisasi, dan keamanan fisik fasilitas tempat layanan beroperasi. Untuk informasi lebih lanjut tentang AWS keamanan, kunjungi AWS Cloud Keamanan.

Peran IAM

Dengan IAM peran, Anda dapat menetapkan akses terperinci, kebijakan, dan izin ke layanan dan pengguna di. AWS Cloud Solusi ini menciptakan IAM peran dengan hak istimewa paling sedikit, dan peran ini memberikan sumber daya solusi dengan izin yang diperlukan.

Data

Semua data yang disimpan dalam bucket Amazon S3 dan tabel DynamoDB memiliki enkripsi saat istirahat. Data dalam perjalanan dengan Firehose juga dienkripsi.

Kemampuan perlindungan

Aplikasi web rentan terhadap berbagai serangan. Serangan ini termasuk permintaan yang dibuat khusus yang dirancang untuk mengeksploitasi kerentanan atau mengendalikan server; serangan volumetrik yang dirancang untuk menjatuhkan situs web; atau bot dan pencakar buruk yang diprogram untuk mengikis dan mencuri konten web.

Solusi ini digunakan CloudFormation untuk mengonfigurasi AWS WAF aturan, termasuk Peraturan yang Dikelola AWS grup aturan dan aturan khusus, untuk memblokir serangan umum berikut:

- AWSAturan Terkelola — Layanan terkelola ini memberikan perlindungan terhadap kerentanan aplikasi umum atau lalu lintas lain yang tidak diinginkan. Solusi ini mencakup grup aturan reputasi IP AWS AWS Terkelola, grup aturan dasar terkelola, dan grup aturan khusus kasus penggunaan

AWS terkelola. Anda memiliki opsi untuk memilih satu atau beberapa grup aturan untuk web AndaACL, hingga kuota unit ACL kapasitas web maksimum (WCU).

- SQLInjeksi — Penyerang memasukkan SQL kode berbahaya ke dalam permintaan web untuk mengekstrak data dari database Anda. Kami merancang solusi ini untuk memblokir permintaan web yang berisi SQL kode yang berpotensi berbahaya.
- XSSPenyerang menggunakan kerentanan di situs web jinak sebagai kendaraan untuk menyuntikkan skrip situs klien berbahaya ke browser web pengguna yang sah. Kami merancang ini untuk memeriksa elemen permintaan masuk yang umum dieksplorasi untuk mengidentifikasi dan memblokir serangan. XSS
- HTTPbanjir — Server web dan sumber daya backend lainnya berisiko terkena DDoS serangan, seperti banjir. HTTP Solusi ini secara otomatis memanggil aturan berbasis tarif ketika permintaan web dari klien melebihi kuota yang dapat dikonfigurasi. Atau, Anda dapat menerapkan kuota ini dengan memproses AWS WAF log menggunakan fungsi Lambda atau kueri Athena.
- Pemindai dan probe — Sumber berbahaya memindai dan menyelidiki aplikasi web yang menghadap ke internet untuk kerentanan, dengan mengirimkan serangkaian permintaan yang menghasilkan kode kesalahan 4xx. HTTP Anda dapat menggunakan riwayat ini untuk membantu mengidentifikasi dan memblokir alamat IP sumber berbahaya. Solusi ini membuat fungsi Lambda atau kueri Athena yang secara otomatis mem-parsing CloudFront atau ALB mengakses log, menghitung jumlah permintaan buruk dari alamat IP sumber unik per menit, dan pembaruan AWS WAF untuk memblokir pemindaian lebih lanjut dari alamat yang mencapai kuota kesalahan yang ditentukan.
- Asal penyerang yang dikenal (daftar reputasi IP) - Banyak organisasi mempertahankan daftar reputasi alamat IP yang dioperasikan oleh penyerang yang dikenal, seperti spammer, distributor malware, dan botnet. Solusi ini memanfaatkan informasi dalam daftar reputasi ini untuk membantu Anda memblokir permintaan dari alamat IP berbahaya. Selain itu, solusi ini memblokir penyerang yang diidentifikasi oleh kelompok aturan reputasi IP berdasarkan intelijen ancaman internal Amazon.
- Bot dan pencakar — Operator aplikasi web yang dapat diakses publik perlu percaya bahwa klien yang mengakses konten mereka mengidentifikasi diri mereka secara akurat, dan bahwa mereka menggunakan layanan sebagaimana dimaksud. Namun, beberapa klien otomatis, seperti pencakar konten atau bot buruk, salah menggambarkan diri mereka sendiri untuk melewati batasan. Solusi ini membantu Anda mengidentifikasi dan memblokir bot dan pencakar yang buruk.

Kuota

Kuota layanan, juga disebut sebagai batas, adalah jumlah maksimum sumber daya layanan atau operasi untuk Anda Akun AWS.

Kuota untuk AWS layanan dalam solusi ini

Pastikan Anda memiliki kuota yang cukup untuk setiap layanan yang diterapkan dalam solusi ini. Untuk informasi lebih lanjut, lihat kuota AWS layanan. Untuk melihat kuota layanan untuk semua AWS layanan dalam dokumentasi tanpa berpindah halaman, lihat informasi di titik akhir Layanan dan halaman kuota di halaman sebagai gantinya. PDF

AWS WAF kuota

AWS WAF dapat memblokir maksimum 10.000 rentang alamat IP dalam notasi Classless Inter-Domain Routing (CIDR) per kondisi kecocokan IP. Setiap daftar yang dibuat oleh solusi ini tunduk pada kuota ini. Untuk informasi lebih lanjut, lihat AWS WAF kuota. Pada versi 3.0, solusi ini membuat dua set IP untuk dilampirkan ke setiap aturan, satu untuk IPv4 dan satu untukIPv6.

AWS WAF memungkinkan maksimum satu permintaan per detik, per akun, per Wilayah AWS API panggilan ke individu `CreatePut`, atau `Update` tindakan mana pun. Jika Anda melakukan API panggilan ini di luar solusi, Anda mungkin mengalami masalah API pelambatan. Untuk mencegah masalah ini, sebaiknya hindari menjalankan aplikasi lain yang melakukan API panggilan ini di akun dan Wilayah yang sama tempat solusi ini digunakan.

Pertimbangan deployment

Bagian berikut memberikan kendala dan pertimbangan untuk menerapkan solusi ini.

AWS WAF aturan

Web ACL yang dihasilkan solusi ini dirancang untuk menawarkan perlindungan komprehensif untuk aplikasi web. Solusinya menyediakan Peraturan yang Dikelola AWS seperangkat aturan khusus yang dapat Anda tambahkan ke webACL. Untuk memasukkan aturan, pilih `yes` parameter yang relevan saat meluncurkan CloudFormation tumpukan. Lihat Langkah 1. Luncurkan tumpukan untuk daftar parameter.

> **Note**
>
> out-of-boxSolusinya tidak mendukung AWS Firewall Manager. Jika Anda ingin menggunakan aturan di Firewall Manager, kami sarankan Anda untuk menerapkan penyesuaian pada kode sumbernya.

Pencatatan ACL lalu lintas web

Jika Anda membuat tumpukan di Wilayah AWS selain US East (Virginia N.) dan menetapkan Endpoint sebagai`CloudFront`, Anda harus mengatur Activate HTTP Flood Protection ke no atau. `yes - AWS WAF rate based rule`

Dua opsi lainnya (`yes - AWS Lambda log parser`dan`yes - Amazon Athena log parser`) memerlukan pengaktifan AWS WAF log di web ACL yang berjalan di semua lokasi AWS tepi, dan ini tidak didukung di luar US East (Virginia N.). Untuk informasi selengkapnya tentang pencatatan ACL lalu lintas Web, lihat panduan AWS WAF pengembang.

Penanganan kebesaran untuk komponen permintaan

AWS WAF tidak mendukung pemeriksaan konten berukuran besar untuk isi, header, atau cookie komponen permintaan web. Saat Anda menulis pernyataan aturan yang memeriksa salah satu jenis komponen permintaan ini, Anda dapat memilih salah satu opsi ini untuk memberi tahu AWS WAF apa yang harus dilakukan dengan permintaan ini:

- `yes`(lanjutkan) — Periksa komponen permintaan secara normal sesuai dengan kriteria inspeksi aturan. AWS WAF memeriksa isi komponen permintaan yang berada dalam batasan ukuran. Ini adalah opsi default yang digunakan dalam solusi.
- `yes - MATCH`— Perlakukan permintaan web sebagai pencocokan pernyataan aturan. AWS WAF menerapkan tindakan aturan untuk permintaan tanpa mengevaluasinya terhadap kriteria inspeksi aturan. Untuk aturan dengan `Block` tindakan, ini memblokir permintaan dengan komponen oversize.
- `yes – NO_MATCH`— Perlakukan permintaan web sebagai tidak cocok dengan pernyataan aturan, tanpa mengevaluasinya terhadap kriteria inspeksi aturan. AWS WAF melanjutkan inspeksi permintaan web dengan menggunakan sisa aturan di webACL, seperti yang akan dilakukan untuk aturan yang tidak cocok.

Untuk informasi selengkapnya, lihat Menangani komponen permintaan web yang terlalu besar di AWS WAF.

Beberapa penerapan solusi

Anda dapat menerapkan solusi beberapa kali di akun dan Wilayah yang sama. Anda harus menggunakan nama CloudFormation tumpukan unik dan nama bucket Amazon S3 untuk setiap penerapan. Setiap penyebaran unik dikenakan biaya tambahan dan tunduk pada AWS WAF kuota per akun, per Wilayah.

Terapkan solusinya

Solusi ini menggunakan AWS CloudFormation templat dan tumpukan untuk mengotomatiskan penerapannya. CloudFormation Template menentukan AWS sumber daya yang disertakan dalam solusi ini dan propertinya. CloudFormationTumpukan menyediakan sumber daya yang dijelaskan dalam template.

Ikhtisar proses penyebaran

Sebelum Anda meluncurkan CloudFormation template, tinjau pertimbangan arsitektur dan konfigurasi yang dibahas dalam panduan ini. Ikuti step-by-step petunjuk di bagian ini untuk mengonfigurasi dan menyebarkan solusi ke akun Anda.

Waktu untuk menyebarkan: Sekitar 15 menit.

> **Note**
>
> Jika sebelumnya Anda telah menerapkan solusi ini, lihat Memperbarui solusi untuk petunjuk pemutakhiran.

Prasyarat

- Konfigurasikan CloudFront distribusi
- Konfigurasikan sebuah ALB

Langkah 1. Luncurkan tumpukan

- Luncurkan CloudFormation template ke dalam Anda Akun AWS.
- Masukkan nilai untuk parameter yang diperlukan: Nama Tumpukan dan Nama Bucket Log Akses Aplikasi.
- Tinjau parameter template lainnya, dan sesuaikan jika perlu.

Langkah 2. Kaitkan web ACL dengan aplikasi web Anda

- Kaitkan distribusi CloudFront web Anda atau ALB (s) dengan web ACL yang dihasilkan oleh solusi ini. Anda dapat mengaitkan distribusi atau penyeimbang beban sebanyak yang Anda inginkan.

Langkah 3. Konfigurasikan pencatatan akses web

- Aktifkan pencatatan akses CloudFront web untuk distribusi atau ALB distribusi web Anda, dan kirim file log ke bucket Amazon S3 yang sesuai. Simpan log dalam folder yang cocok dengan awalan yang ditentukan pengguna. Jika tidak ada awalan yang ditentukan pengguna yang digunakan, simpan log ke Log (awalan AWS log default). `AWS Logs/` Lihat parameter Application Access Log Bucket Prefix pada Langkah 1. Luncurkan tumpukan untuk informasi lebih lanjut.

AWS CloudFormation template

Solusi ini mencakup satu AWS CloudFormation template utama dan dua template bersarang. Anda dapat mengunduh CloudFormation templat sebelum menerapkan solusi.

Tumpukan utama

View template

aws-waf-security-automations.template - Gunakan template ini sebagai titik masuk untuk meluncurkan solusi di akun Anda. Konfigurasi default menyebarkan AWS WAF web ACL dengan aturan yang telah dikonfigurasi sebelumnya. Anda dapat menyesuaikan template berdasarkan kebutuhan Anda.

ACLTumpukan web

View template

aws-waf-security-automations-webacl.template - Template bersarang ini menyediakan AWS WAF sumber daya termasuk webACL, IP, set, dan sumber daya terkait lainnya.

Tumpukan Firehose Athena

View template

aws-waf-security-automations-firehose-athena.template — Template bersarang ini menyediakan sumber daya yang terkait dengan, Athena, dan Firehose. AWS Glue Ini dibuat ketika Anda memilih pengurai log Scanner & Probe Athena atau parser log Flood HTTPLambda atau Athena.

Prasyarat

Solusi ini dirancang untuk bekerja dengan aplikasi web yang digunakan dengan CloudFront atau. ALB Jika Anda belum memiliki salah satu sumber daya ini yang dikonfigurasi, selesaikan tugas yang berlaku sebelum Anda meluncurkan solusi ini.

Konfigurasikan CloudFront distribusi

Selesaikan langkah-langkah berikut untuk mengonfigurasi CloudFront distribusi konten statis dan dinamis aplikasi web Anda. Lihat Panduan CloudFront Pengembang Amazon untuk petunjuk terperinci.

1. Buat distribusi aplikasi CloudFront web. Lihat Membuat Distribusi.
2. Konfigurasikan asal statis dan dinamis. Lihat Menggunakan berbagai asal dengan CloudFront distribusi.
3. Tentukan perilaku distribusi Anda. Lihat Nilai yang Anda tentukan saat membuat atau memperbarui distribusi.

> **Note**
>
> Jika Anda memilih `CloudFront` sebagai titik akhir Anda, Anda harus membuat WAFV2 sumber daya Anda di Wilayah AS Timur (Virginia N.).

Konfigurasikan sebuah ALB

Untuk mengonfigurasi ALB untuk mendistribusikan lalu lintas masuk ke aplikasi web Anda, lihat Membuat Application Load Balancer di Panduan Pengguna untuk Application Load Balancers.

Langkah 1. Luncurkan tumpukan

AWS CloudFormation Template otomatis ini menyebarkan solusi pada file. AWS Cloud

1. Masuk ke AWS Management Consoledan pilih Launch Solution untuk meluncurkan `waf-automation-on-aws.template` CloudFormation template.

Launch solution

2. Template diluncurkan di Wilayah AS Timur (Virginia N.) secara default. Untuk meluncurkan solusi ini secara berbeda Wilayah AWS, gunakan pemilih Wilayah di bilah navigasi konsol. Jika Anda memilih `CloudFront` sebagai titik akhir Anda, Anda harus menerapkan solusi di Wilayah AS Timur (Virginia N.) (`us-east-1`).

> **Note**
>
> Bergantung pada nilai parameter input yang Anda tentukan, solusi ini membutuhkan sumber daya yang berbeda. Sumber daya ini saat ini Wilayah AWS hanya tersedia secara spesifik. Oleh karena itu, Anda harus meluncurkan solusi ini Wilayah AWS di mana layanan ini tersedia. Untuk informasi selengkapnya, lihat Didukung Wilayah AWS.

3. Pada halaman Tentukan templat, verifikasi bahwa Anda memilih templat yang benar dan pilih Berikutnya.
4. Pada halaman Tentukan detail tumpukan, tetapkan nama ke AWS WAF konfigurasi Anda di bidang Nama tumpukan. Ini juga merupakan nama web ACL yang dibuat template.
5. Di bawah Parameter, tinjau parameter untuk templat dan modifikasi sesuai kebutuhan. Untuk memilih keluar dari fitur tertentu, pilih none atau no sebagaimana berlaku. Solusi ini menggunakan nilai default berikut.

Parameter	Default	Deskripsi
Nama tumpukan	*<requires input>*	Nama tumpukan tidak dapat berisi spasi. Nama ini harus unik di dalam Anda Akun AWS dan merupakan nama web ACL yang dibuat template.
Jenis Sumber Daya		
Titik akhir	`CloudFront`	Pilih jenis sumber daya yang digunakan.

Parameter	Default	Deskripsi
		Note Jika Anda memilih `CloudFront` sebagai titik akhir Anda, Anda harus meluncurkan solusi untuk membuat WAF sumber daya di Wilayah AS Timur (Virginia Utara) (`us-east-1`).
AWS Grup Aturan Reputasi IP Terkelola		

Parameter	Default	Deskripsi
Aktifkan Amazon IP Reputation List Managed Rule Group Protection	no	Pilih `yes` untuk mengaktifkan komponen yang dirancang untuk menambahkan Grup Aturan Terkelola Daftar reputasi IP Amazon ke webACL. Kelompok aturan ini 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. Yang dibutuhkan WCU adalah 25. Akun Anda harus memiliki WCU kapasitas yang cukup untuk menghindari kegagalan penyebaran ACL tumpukan web karena melebihi batas kapasitas. Untuk informasi selengkapnya, lihat daftar grup Peraturan yang Dikelola AWS aturan.

Parameter	Default	Deskripsi
Aktifkan Perlindungan Grup Aturan Terkelola Daftar IP Anonim	no	Pilih `yes` untuk mengaktifkan komponen yang dirancang untuk menambahkan Grup Aturan Terkelola Daftar IP Anonim ke webACL. Grup aturan ini memblokir permintaan dari layanan yang mengizinkan pengaburan identitas penampil. Ini termasuk permintaan dariVPNs, proxy, node Tor, dan penyedia hosting. 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. Yang dibutuhkan WCU adalah 50. Akun Anda harus memiliki WCU kapasitas yang cukup untuk menghindari kegagalan penyebaran ACL tumpukan web karena melebihi batas kapasitas. Untuk informasi selengkapnya, lihat daftar grup

Parameter	Default	Deskripsi
		Peraturan yang Dikelola AWS aturan.
AWS Grup Aturan Dasar Terkelola		
Aktifkan Aturan Inti Set Perlindungan Grup Aturan Terkelola	no	Pilih `yes` untuk mengaktifkan komponen yang dirancang untuk menambahkan Core Rule Set Managed Rule Group ke webACL. Kelompok aturan ini memberikan perlindungan terhadap eksploitasi berbagai kerentanan, termasuk beberapa risiko tinggi dan kerentanan yang umum terjadi. Pertimbangkan untuk menggunakan grup aturan ini untuk kasus AWS WAF penggunaan apa pun. Yang dibutuhkan WCU adalah 700. Akun Anda harus memiliki WCU kapasitas yang cukup untuk menghinda ri kegagalan penyebaran ACL tumpukan web karena melebihi batas kapasitas. Untuk informasi selengkap nya, lihat daftar grup Peraturan yang Dikelola AWS aturan.

Parameter	Default	Deskripsi
Aktifkan Perlindungan Admin Perlindungan Grup Aturan Terkelola	no	Pilih `yes` untuk mengaktifkan komponen yang dirancang untuk menambahkan Admin Protection Managed Rule Group ke webACL. Grup aturan ini 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 administr atif ke aplikasi Anda. Yang dibutuhkan WCU adalah 100. Akun Anda harus memiliki WCU kapasitas yang cukup untuk menghinda ri kegagalan penyebaran ACL tumpukan web karena melebihi batas kapasitas. Untuk informasi selengkap nya, lihat daftar grup Peraturan yang Dikelola AWS aturan.

Parameter	Default	Deskripsi
Aktifkan Perlindungan Kelompok Aturan Terkelola Masukan Buruk yang Diketahui	no	Pilih `yes` untuk mengaktifkan komponen yang dirancang untuk menambahkan Known Bad Inputs Managed Rule Group ke webACL. Grup aturan ini 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 administr atif ke aplikasi Anda. Yang dibutuhkan WCU adalah 100. Akun Anda harus memiliki WCU kapasitas yang cukup untuk menghinda ri kegagalan penyebaran ACL tumpukan web karena melebihi batas kapasitas. Untuk informasi selengkap nya, lihat daftar grup Peraturan yang Dikelola AWS aturan.
AWS Kelompok Aturan Khusus Kasus Penggunaan Terkelola		

Parameter	Default	Deskripsi
Aktifkan Perlindungan Grup Aturan Terkelola SQL Database	no	Pilih `yes` untuk mengaktifkan komponen yang dirancang untuk menambahkan SQLDatabase Managed Rule Group ke webACL. Kelompok aturan ini memblokir pola permintaan yang terkait dengan eksploitasi SQL database, seperti serangan SQL injeksi. Ini dapat membantu mencegah injeksi jarak jauh dari kueri yang tidak sah. Evaluasi grup aturan ini untuk digunakan jika aplikasi Anda berinteraksi dengan SQL database. Menggunakan aturan kustom SQL injeksi adalah opsional jika Anda sudah mengaktifkan grup SQL aturan AWS terkelola. Yang dibutuhkan WCU adalah 200. Akun Anda harus memiliki WCU kapasitas yang cukup untuk menghindari kegagalan penyebaran ACL tumpukan web karena melebihi batas kapasitas. Untuk informasi selengkapnya, lihat daftar grup Peraturan yang Dikelola AWS aturan.

Parameter	Default	Deskripsi
Aktifkan Perlindungan Grup Aturan Terkelola Sistem Operasi Linux	no	Pilih `yes` untuk mengaktifkan komponen yang dirancang untuk menambahkan Grup Aturan Terkelola Sistem Operasi Linux ke webACL. Grup aturan ini memblokir pola permintaan yang terkait dengan eksploitasi kerentanan khusus untuk Linux, termasuk serangan Local File Inclusion () khusus Linux. LFI Ini dapat membantu mencegah serangan yang mengekspos konten file atau menjalankan kode yang seharusnya tidak dapat diakses oleh penyerang. Evaluasi grup aturan ini jika ada bagian dari aplikasi Anda yang berjalan di Linux. Anda harus menggunakan grup aturan ini bersama dengan grup aturan sistem POSIX operasi. Yang dibutuhkan WCU adalah 200. Akun Anda harus memiliki WCU kapasitas yang cukup untuk menghindari kegagalan penyebaran ACL tumpukan web karena melebihi batas kapasitas.

Parameter	Default	Deskripsi
		Untuk informasi selengkap nya, lihat daftar grup Peraturan yang Dikelola AWS aturan.

Parameter	Default	Deskripsi
Aktifkan Perlindungan Grup Aturan Terkelola Sistem POSIX Operasi	no	Pilih `yes` untuk mengaktifkan komponen yang dirancang untuk menambahkan Aturan Inti Set Managed Rule Group Protection ke webACL. Grup aturan ini memblokir pola permintaan yang terkait dengan eksploitasi kerentanan khusus untuk POSIX dan POSIX -like sistem operasi, termasuk serangan. LFI Ini dapat membantu mencegah serangan yang mengekspos konten file atau menjalankan kode yang seharusnya tidak dapat diakses oleh penyerang. Evaluasi grup aturan ini jika ada bagian dari aplikasi Anda yang berjalan pada sistem operasi POSIX atau POSIX -like. Yang dibutuhkan WCU adalah 100. Akun Anda harus memiliki WCU kapasitas yang cukup untuk menghindari kegagalan penyebaran ACL tumpukan web karena melebihi batas kapasitas. Untuk informasi selengkapnya, lihat daftar grup Peraturan yang Dikelola AWS aturan.

Parameter	Default	Deskripsi
Aktifkan Perlindungan Grup Aturan Terkelola Sistem Operasi Windows	no	Pilih `yes` untuk mengaktifkan komponen yang dirancang untuk menambahkan Grup Aturan Terkelola Sistem Operasi Windows ke webACL. Grup aturan ini 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. Yang dibutuhkan WCU adalah 200. Akun Anda harus memiliki WCU kapasitas yang cukup untuk menghindari kegagalan penyebaran ACL tumpukan web karena melebihi batas kapasitas. Untuk informasi selengkapnya, lihat daftar grup

Parameter	Default	Deskripsi
		Peraturan yang Dikelola AWS aturan.

Parameter	Default	Deskripsi
Aktifkan Perlindungan Grup Aturan Terkelola PHP Aplikasi	no	Pilih `yes` untuk mengaktifkan komponen yang dirancang untuk menambahkan Grup Aturan Terkelola PHP Aplikasi ke webACL. Kelompok aturan ini memblokir pola permintaan yang terkait dengan eksploitasi kerentanan khusus untuk penggunaan bahasa PHP pemrograman, termasuk injeksi fungsi yang tidak PHP aman. Ini dapat membantu mencegah eksploitasi kerentanan yang memungkinkan penyerang menjalankan kode atau perintah dari jarak jauh yang tidak diizinkan. Evaluasi grup aturan PHP ini jika diinstal pada server mana pun yang berinteraksi dengan aplikasi Anda. Yang dibutuhkan WCU adalah 100. Akun Anda harus memiliki WCU kapasitas yang cukup untuk menghindari kegagalan penyebaran ACL tumpukan web karena melebihi batas kapasitas. Untuk informasi selengkapnya, lihat daftar grup

Parameter	Default	Deskripsi
		Peraturan yang Dikelola AWS aturan.
Aktifkan Perlindungan Grup Aturan Terkelola WordPress Aplikasi	no	Pilih `yes` untuk mengaktifkan komponen yang dirancang untuk menambahkan Grup Aturan Terkelola WordPress Aplikasi ke webACL. Grup aturan ini memblokir pola permintaan yang terkait dengan eksploitasi kerentanan khusus untuk WordPress situs. Evaluasi kelompok aturan ini jika Anda menjalankan WordPress. Kelompok aturan ini harus digunakan bersama dengan SQL database dan kelompok aturan PHP aplikasi. Yang dibutuhkan WCU adalah 100. Akun Anda harus memiliki WCU kapasitas yang cukup untuk menghinda ri kegagalan penyebaran ACL tumpukan web karena melebihi batas kapasitas. Untuk informasi selengkap nya, lihat daftar grup Peraturan yang Dikelola AWS aturan.
Aturan Kustom - Pemindai & Probe		

Parameter	Default	Deskripsi
Aktifkan Scanner & Probe Protection	`yes - AWS Lambda log parser`	Pilih komponen yang digunakan untuk memblokir pemindai dan probe. Lihat opsi pengurai Log untuk informasi selengkapnya tentang pengorbanan yang terkait dengan opsi mitigasi.

Parameter	Default	Deskripsi
Nama Bucket Log Akses Aplikasi	*<requires input>*	Jika Anda yes memilih parameter Activate Scanner & Probe Protection, masukkan nama bucket Amazon S3 (baru atau yang sudah ada) tempat Anda ingin menyimpan log akses untuk CloudFront distribus i atau ALB distribusi Anda. Jika Anda menggunakan bucket Amazon S3 yang sudah ada, bucket tersebut harus berada di tempat yang sama Wilayah AWS di mana Anda menerapkan template. CloudFormation Anda harus menggunakan bucket yang berbeda untuk setiap penerapan solusi. Untuk menonaktifkan perlindungan ini, abaikan parameter ini. **Note** Aktifkan pencatata n akses CloudFront web untuk distribus i web atau ALB (s) Anda untuk mengirim file log ke bucket Amazon S3 ini. Simpan log dalam awalan yang sama

Parameter	Default	Deskripsi
		yang ditentukan dalam tumpukan (awalan `AWS Logs/` default). Lihat parameter Application Access Log Bucket Prefix untuk informasi selengkapnya.

Parameter	Default	Deskripsi
Awalan Bucket Log Akses Aplikasi	`AWS Logs/`	Jika Anda `yes` memilih parameter Activate Scanner & Probe Protection, Anda dapat memasukkan awalan yang ditentukan pengguna opsional untuk bucket log akses aplikasi di atas. Jika Anda memilih `CloudFront` untuk parameter Endpoint, Anda dapat memasukkan awalan seperti. `yourprefix/` Jika Anda memilih `ALB` untuk parameter Endpoint, Anda harus menambahkan `AWS Logs/` ke awalan Anda seperti. `yourprefix/AWSLogs/` Gunakan `AWS Logs/` (default) jika tidak ada awalan yang ditentukan pengguna. Untuk menonaktifkan perlindungan ini, abaikan parameter ini.

Parameter	Default	Deskripsi
Apakah pencatatan akses bucket dihidupkan?	no	Pilih yes apakah Anda memasukkan nama bucket Amazon S3 yang ada untuk parameter Nama Bucket Log Akses Aplikasi dan pencatatan akses server untuk bucket sudah diaktifkan. Jika Anda memilihno, solusinya mengaktifkan pencatatan akses server untuk bucket Anda. Jika Anda memilih no parameter Activate Scanner & Probe Protection, abaikan parameter ini.
Ambang Kesalahan	50	Jika Anda memilih yes parameter Activate Scanner & Probe Protection, masukkan permintaan buruk maksimum yang dapat diterima per menit, per alamat IP. Jika Anda memilih no parameter Activate Scanner & Probe Protection, abaikan parameter ini.

Parameter	Default	Deskripsi
Simpan Data di Lokasi S3 Asli	no	Jika Anda memilih `yes - Amazon Athena log parser` parameter Activate Scanner & Probe Protection, solusinya menerapkan partisi ke file log akses aplikasi dan kueri Athena. Secara default, solusi memindahkan file log dari lokasi aslinya ke struktur folder yang dipartisi di Amazon S3. Pilih `yes` apakah Anda juga ingin menyimpan salinan log di lokasi aslinya. Ini akan menduplikasi penyimpanan log Anda. Jika Anda tidak memilih `yes - Amazon Athena log parser` parameter Activate Scanner & Probe Protection, abaikan parameter ini.
Aturan Kustom - HTTP Banjir		
Aktifkan Perlindungan HTTP Banjir	`yes - AWS WAF rate-based rule`	Pilih komponen yang digunakan untuk memblokir serangan HTTP banjir. Lihat opsi pengurai Log untuk informasi selengkapnya tentang pengorbanan yang terkait dengan opsi mitigasi.

Parameter	Default	Deskripsi
Ambang Permintaan Default	`100`	Jika Anda `yes` memilih parameter Activate HTTP Flood Protection, masukkan permintaan maksimum yang dapat diterima per lima menit, per alamat IP. Jika Anda memilih `yes - AWS WAF rate-based rule` parameter Activate HTTP Flood Protection, nilai minimum yang dapat diterima adalah`100`. Jika Anda memilih `yes - AWS Lambda log parser` atau `yes – Amazon Athena log parser` untuk parameter Activate HTTP Flood Protection, itu bisa berupa nilai apa pun. Untuk menonaktifkan perlindungan ini, abaikan parameter ini.

Parameter	Default	Deskripsi
Permintaan Ambang Batas berdasarkan Negara	<optional input>	Jika Anda `yes - Amazon Athena log parser` memilih parameter Activate HTTP Flood Protection, Anda dapat memasukkan ambang batas berdasarkan negara mengikuti JSON format ini`{"TR":50,"ER":150}` . Solusinya menggunakan ambang batas ini untuk permintaan yang berasal dari negara yang ditentukan. Solusinya menggunakan parameter Ambang Permintaan Default untuk permintaan yang tersisa. **Note** Jika Anda menentukan parameter ini, negara akan secara otomatis disertakan dalam grup kueri Athena, bersama dengan IP dan bidang kelompok berdasarkan opsional lainnya yang dapat Anda pilih dengan parameter Kueri Grup Berdasarkan Permintaan di Flood HTTP Athena Query.

Parameter	Default	Deskripsi
		Jika Anda memilih untuk menonaktifkan perlindungan ini, abaikan parameter ini.
Kelompokkan Berdasarkan Permintaan di HTTP Flood Athena Query	None	Jika Anda memilih `yes - Amazon Athena log parser` parameter Activate HTTP Flood Protection, Anda dapat memilih bidang grup-menurut untuk menghitung permintaan per IP dan bidang grup-menurut yang dipilih. Misalnya, jika Anda memilih`URI`, solusi menghitung permintaan per IP dan`URI`. Jika Anda memilih untuk menonaktifkan perlindungan ini, abaikan parameter ini.

Parameter	Default	Deskripsi
WAFPeriode Blok	`240`	Jika Anda memilih `yes - AWS Lambda log parser` atau `yes – Amazon Athena log parser` untuk parameter Activate Scanner & Probe Protectio n atau Activate HTTP Flood Protection, masukkan periode (dalam hitungan menit) untuk memblokir alamat IP yang berlaku. Untuk menonaktifkan penguraian log, abaikan parameter ini.
Jadwal Waktu Jalankan Query Athena (Menit)	5	Jika Anda memilih `yes – Amazon Athena log parser` parameter Activate Scanner & Probe Protectio n atau Activate HTTP Flood Protection, Anda dapat memasukkan interval waktu (dalam hitungan menit) di mana kueri Athena berjalan. Secara default, kueri Athena berjalan setiap 5 menit. Jika Anda memilih untuk menonaktifkan perlindungan ini, abaikan parameter ini.
Aturan Kustom - Bot Buruk		

Parameter	Default	Deskripsi
Aktifkan Perlindungan Bot Buruk	`yes`	Pilih `yes` untuk mengaktifkan komponen yang dirancang untuk memblokir bot buruk dan pencakar konten.
ARNIAMperan yang memiliki akses tulis ke CloudWatch log di akun Anda	<optional input>	Berikan opsional ARN IAM peran yang memiliki akses tulis ke CloudWatch log di akun Anda. Sebagai contoh: `ARN: arn:aws:iam::account_id:role/myrolename` . Lihat Menyiapkan CloudWatch logging untuk REST API in API Gateway untuk petunjuk tentang cara membuat peran. Jika Anda membiarkan parameter ini kosong (default) , solusi akan membuat peran baru untuk Anda.

Parameter	Default	Deskripsi
Ambang Permintaan Default	100	Jika Anda `yes` memilih parameter Activate HTTP Flood Protection, masukkan permintaan maksimum yang dapat diterima per lima menit, per alamat IP. Jika Anda memilih `yes - AWS WAF rate-based rule` parameter Activate HTTP Flood Protection, nilai minimum yang dapat diterima adalah 100. Jika Anda memilih `yes - AWS Lambda log parser` atau `yes – Amazon Athena log parser` untuk parameter Activate HTTP Flood Protection, itu bisa berupa nilai apa pun. Untuk menonaktifkan perlindungan ini, abaikan parameter ini.
Aturan Kustom - Daftar Reputasi IP Pihak Ketiga		
Aktifkan Perlindungan Daftar Reputasi	`yes`	Pilih `yes` untuk memblokir permintaan dari alamat IP pada daftar reputasi pihak ketiga (daftar yang didukung termasuk Spamhaus, Emerging Threats, dan Tor exit node).

Parameter	Default	Deskripsi
Aturan Kustom Legacy		

Parameter	Default	Deskripsi
Aktifkan Perlindungan SQL Injeksi	`yes`	Pilih `yes` untuk mengaktifkan komponen yang dirancang untuk memblokir serangan SQL injeksi umum. Pertimbangkan untuk mengaktifkannya jika Anda tidak menggunakan kumpulan aturan inti AWS terkelola atau grup aturan SQL database AWS terkelola. Anda dapat memilih salah satu opsi (`yes`(lanjutkan),`yes - MATCH`, atau`yes - NO_MATCH`) yang AWS WAF ingin Anda tangani permintaan besar melebihi 8 KB (8192 byte). Secara default, `yes` memeriksa isi komponen permintaan yang berada dalam batasan ukuran sesuai dengan kriteria pemeriksaan aturan. Untuk informasi selengkapnya, lihat Menangani komponen permintaan web yang terlalu besar. Pilih no untuk menonaktifkan fitur ini. **Note** CloudFormation Tumpukan menambahkan opsi

Parameter	Default	Deskripsi
		penanganan ukuran besar yang dipilih ke aturan perlindungan SQL injeksi default dan menerapka nnya ke dalam aturan perlindun gan injeksi Anda. Akun AWS Jika Anda menyesuaikan aturan di luar CloudForm ation, perubahan Anda akan ditimpa setelah pembaruan tumpukan.

Parameter	Default	Deskripsi
Tingkat Sensitivitas untuk Perlindungan SQL Injeksi	`LOW`	Pilih tingkat sensitivitas yang ingin Anda gunakan AWS WAF untuk memeriksa serangan SQL injeksi. `HIGH`mendeteksi lebih banyak serangan, tetapi mungkin menghasilkan lebih banyak kesalahan positif. `LOW`umumnya merupakan pilihan yang lebih baik untuk sumber daya yang sudah memiliki perlindungan lain terhadap serangan SQL injeksi atau yang memiliki toleransi rendah untuk positif palsu. Untuk informasi selengkap nya, lihat AWS WAF menambahkan tingkat sensitivitas untuk pernyataa n aturan SQL injeksi dan SensitivityLevelproperti di Panduan AWS CloudForm ation Pengguna. Jika Anda memilih untuk menonaktifkan perlindun gan SQL injeksi, abaikan parameter ini.

Parameter	Default	Deskripsi
		Note CloudFormation Tumpukan menambahkan tingkat sensitivitas yang dipilih ke aturan perlindungan SQL injeksi default dan menerapkannya ke dalam aturan Anda Akun AWS. Jika Anda menyesuaikan aturan di luar CloudFormation, perubahan Anda akan ditimpa setelah pembaruan tumpukan.

Parameter	Default	Deskripsi
Aktifkan Perlindungan Skrip Lintas Situs	`yes`	Pilih `yes` untuk mengaktifkan komponen yang dirancang untuk memblokir XSS serangan umum. Pertimbangkan untuk mengaktifkannya jika Anda tidak menggunakan kumpulan aturan inti AWS terkelola. Anda juga dapat memilih salah satu opsi (`yes`(lanjutkan),`yes - MATCH`, atau`yes - NO_MATCH`) yang AWS WAF ingin Anda tangani permintaan besar melebihi 8 KB (8192 byte). Secara default, `yes` gunakan `Continue` opsi, yang memeriksa konten komponen permintaan yang berada dalam batasan ukuran sesuai dengan kriteria pemeriksaan aturan. Untuk informasi selengkapnya, lihat penanganan Oversize untuk komponen permintaan. Pilih no untuk menonaktifkan fitur ini. **Note** CloudFormation Tumpukan menambahkan opsi penanganan ukuran besar yang dipilih ke

Parameter	Default	Deskripsi
		aturan skrip lintas situs default dan menerapkannya ke dalam file Anda. Akun AWS Jika Anda menyesuaikan aturan di luar CloudForm ation, perubahan Anda akan ditimpa setelah pembaruan tumpukan.
Pengaturan Retensi IP yang Diizinkan dan Ditolak		
Periode Retensi (Menit) untuk Set IP yang Diizinkan	`-1`	Jika Anda ingin mengaktifkan retensi IP untuk set IP yang Diizinkan, masukkan nomor (`15`atau lebih besar) sebagai periode retensi (menit). Alamat IP yang mencapai periode retensi kedaluwar sa, dan solusi menghapus nya dari set IP. Solusinya mendukung periode retensi minimal 15 menit. Jika Anda memasukkan nomor antara `0` dan`15`, solusinya memperlak ukannya sebagai`15`. Biarkan sebagai `-1` (default) untuk mematikan retensi IP.

Parameter	Default	Deskripsi
Periode Retensi (Menit) untuk Set IP Ditolak	`-1`	Jika Anda ingin mengaktifkan retensi IP untuk kumpulan IP Ditolak, masukkan nomor (`15`atau lebih besar) sebagai periode retensi (menit). Alamat IP yang mencapai periode retensi kedaluwarsa, dan solusi menghapusnya dari set IP. Solusinya mendukung periode retensi minimal 15 menit. Jika Anda memasukkan nomor antara `0` dan`15`, solusinya memperlakukannya sebagai`15`. Biarkan sebagai `-1` (default) untuk mematikan retensi IP.
Email untuk menerima pemberitahuan setelah kedaluwarsa Set IP yang Diizinkan atau Ditolak	<optional input>	Jika Anda mengaktifkan parameter periode retensi IP (lihat dua parameter sebelumnya) dan ingin menerima pemberitahuan email saat alamat IP kedaluwarsa, masukkan alamat email yang valid. Jika Anda tidak mengaktifkan retensi IP atau ingin menonaktifkan notifikasi email, biarkan kosong (default).
Pengaturan Lanjutan		

Parameter	Default	Deskripsi
Periode Retensi (Hari) untuk Grup Log	`365`	Jika Anda ingin mengaktif kan retensi untuk Grup CloudWatch Log, masukkan nomor (1atau lebih besar) sebagai periode penyimpan an (hari). Anda dapat memilih periode retensi antara satu hari (1) dan sepuluh tahun (`3650`). Secara default log akan kedaluwarsa setelah satu tahun. Setel `-1` untuk menyimpan log tanpa batas waktu.

6. Pilih Berikutnya.
7. Pada halaman Configure stack options, Anda dapat menentukan tag (pasangan nilai kunci) untuk sumber daya di tumpukan Anda dan menetapkan opsi tambahan. Pilih Berikutnya.
8. Pada halaman Tinjau dan buat, tinjau dan konfirmasikan pengaturan. Pilih kotak yang mengakui bahwa template akan membuat IAM sumber daya dan kemampuan tambahan apa pun yang diperlukan.
9. Pilih Kirim untuk menyebarkan tumpukan.

   Melihat status tumpukan di AWS CloudFormation konsol di kolom Status. Anda akan menerima status CREATE _ COMPLETE dalam waktu sekitar 15 menit.

> **Note**
>
> Selain,, dan `Access Handler` AWS Lambda fungsi `Log Parser` `IP Lists Parser`, solusi ini mencakup fungsi `helper` dan `custom-resource` Lambda, yang berjalan hanya selama konfigurasi awal atau ketika sumber daya diperbarui atau dihapus.
> Saat menggunakan solusi ini, Anda akan melihat semua fungsi di AWS Lambda konsol, tetapi hanya tiga fungsi solusi utama yang aktif secara teratur. Jangan menghapus dua fungsi lainnya; mereka diperlukan untuk mengelola sumber daya terkait.

Untuk melihat detail tentang sumber daya tumpukan, pilih tab Output. Ini termasuk BadBotHoneypotEndpointnilai, yang merupakan titik akhir honeypot API Gateway. Ingat nilai ini karena Anda akan menggunakannya di Sematkan tautan Honeypot di aplikasi web Anda.

Langkah 2. Kaitkan web ACL dengan aplikasi web Anda

Perbarui CloudFront distribusi atau ALB (s) Anda untuk mengaktifkan AWS WAF dan mencatat menggunakan sumber daya yang Anda buat di Langkah 1. Luncurkan tumpukan.

1. Masuk ke konsol AWS WAF tersebut.
2. Pilih web ACL yang ingin Anda gunakan.
3. Pada tab AWS Sumber daya terkait, pilih Tambahkan AWS sumber daya.
4. Di bawah Jenis sumber daya, pilih CloudFront distribusi atauALB.
5. Pilih sumber daya dari daftar, lalu pilih Tambah untuk menyimpan perubahan Anda.

Langkah 3. Konfigurasikan pencatatan akses web

Konfigurasikan CloudFront atau Anda ALB untuk mengirim log akses web ke bucket Amazon S3 yang sesuai sehingga data ini tersedia untuk fungsi Log Parser Lambda.

Menyimpan log akses web dari CloudFront distribusi

1. Masuk ke CloudFront konsol Amazon.
2. Pilih distribusi aplikasi web Anda, dan pilih Pengaturan Distribusi.
3. Di tab Umum, pilih Edit.
4. Untuk AWS WAF Web ACL, pilih ACL solusi web yang dibuat (parameter nama Stack).
5. Untuk Logging, pilih On.
6. Untuk Bucket for Logs, pilih bucket S3 yang ingin Anda gunakan untuk menyimpan log akses web. Ini bisa berupa bucket S3 baru atau yang sudah ada yang digunakan di tumpukan utama dan memiliki izin CloudFront untuk menulis log. Daftar drop-down menyebutkan ember yang terkait dengan arus. Akun AWS Untuk informasi selengkapnya, lihat Memulai CloudFront distribusi dasar di Panduan CloudFront Pengembang Amazon.

7. Atur awalan log ke awalan yang digunakan untuk menerapkan solusi. Anda dapat menemukan awalan di tumpukan utama, tab Parameter, AppAccessLogBucketPrefixParam(defaultAWS Logs/).
8. Pilih Ya, edit untuk menyimpan perubahan Anda.

Untuk informasi selengkapnya, lihat Mengonfigurasi dan menggunakan log standar (log akses) di Panduan CloudFront Pengembang Amazon.

Menyimpan log akses web dari Application Load Balancer

1. Masuk ke konsol Amazon Elastic Compute Cloud (AmazonEC2).
2. Di panel navigasi, pilih Load Balancers.
3. Pilih aplikasi web AndaALB.
4. PadaDeskripsitab, pilihEdit atribut.
5. Pilih Aktifkan log akses.
6. Untuk lokasi S3, ketik nama bucket S3 yang ingin Anda gunakan untuk menyimpan log akses web. Ini bisa berupa bucket S3 baru atau yang sudah ada yang digunakan di tumpukan utama dan memiliki izin untuk Application Load Balancer untuk menulis log.
7. Atur awalan log ke awalan yang digunakan untuk menerapkan solusi. Anda dapat menemukan awalan di tumpukan utama, tab Parameter, AppAccessLogBucketPrefixParam(defaultAWS Logs/).
8. Pilih Simpan.

Untuk informasi selengkapnya, lihat Akses Log untuk Application Load Balancer Anda di Panduan Pengguna Elastic Load Balancing.

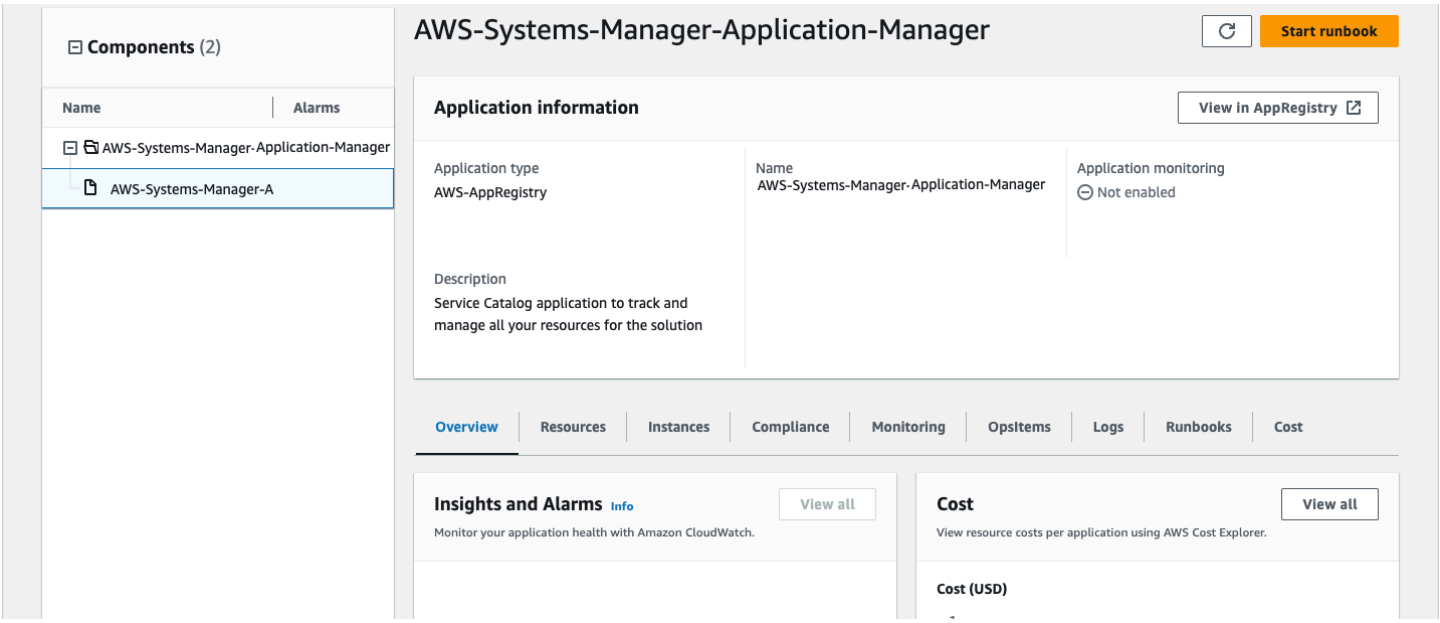
Pantau solusinya dengan AppRegistry

Solusinya mencakup AppRegistry sumber daya Service Catalog untuk mendaftarkan CloudFormation template dan sumber daya yang mendasarinya sebagai aplikasi di Service Catalog AppRegistry dan AWS Systems Manager Application Manager.

AWS Systems Manager Application Manager memberi Anda tampilan tingkat aplikasi ke dalam solusi ini dan sumber dayanya sehingga Anda dapat:

- Pantau sumber dayanya, biaya untuk sumber daya yang digunakan di seluruh tumpukan dan Akun AWS, dan log yang terkait dengan solusi ini dari lokasi pusat.
- Lihat data operasi untuk sumber daya solusi ini dalam konteks aplikasi. Misalnya, status penerapan, CloudWatch alarm, konfigurasi sumber daya, dan masalah operasional.

Gambar berikut menggambarkan contoh tampilan aplikasi untuk tumpukan solusi di Application Manager.



Tumpukan solusi di Manajer Aplikasi

Aktifkan Wawasan CloudWatch Aplikasi

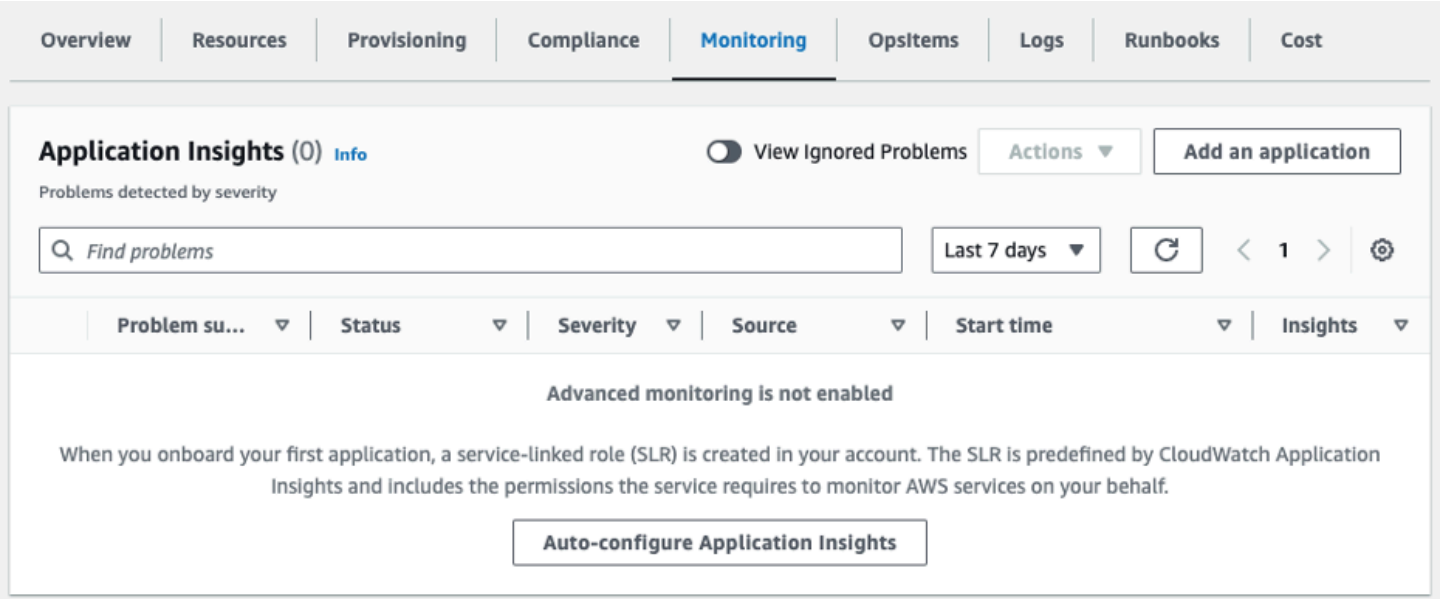
1. Masuk ke konsol Systems Manager.
2. Pada panel navigasi, pilih Manajer Aplikasi.

3. Di Aplikasi, cari nama aplikasi untuk solusi ini dan pilih.

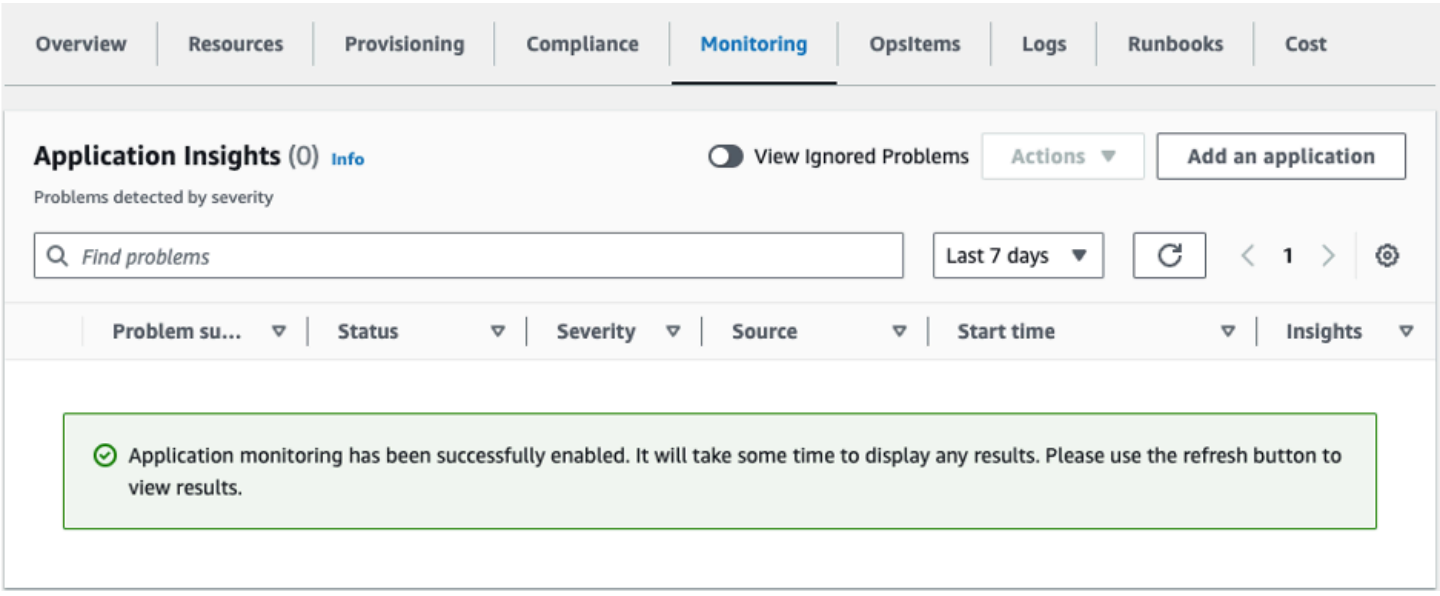
   Nama aplikasi akan memiliki App Registry di kolom Sumber Aplikasi, dan akan memiliki kombinasi nama solusi, Wilayah, ID akun, atau nama tumpukan.

4. Di pohon Komponen, pilih tumpukan aplikasi yang ingin Anda aktifkan.

5. Di tab Monitoring, di Application Insights, pilih Konfigurasi Otomatis Wawasan Aplikasi.



Pemantauan untuk aplikasi Anda sekarang diaktifkan dan kotak status berikut muncul:

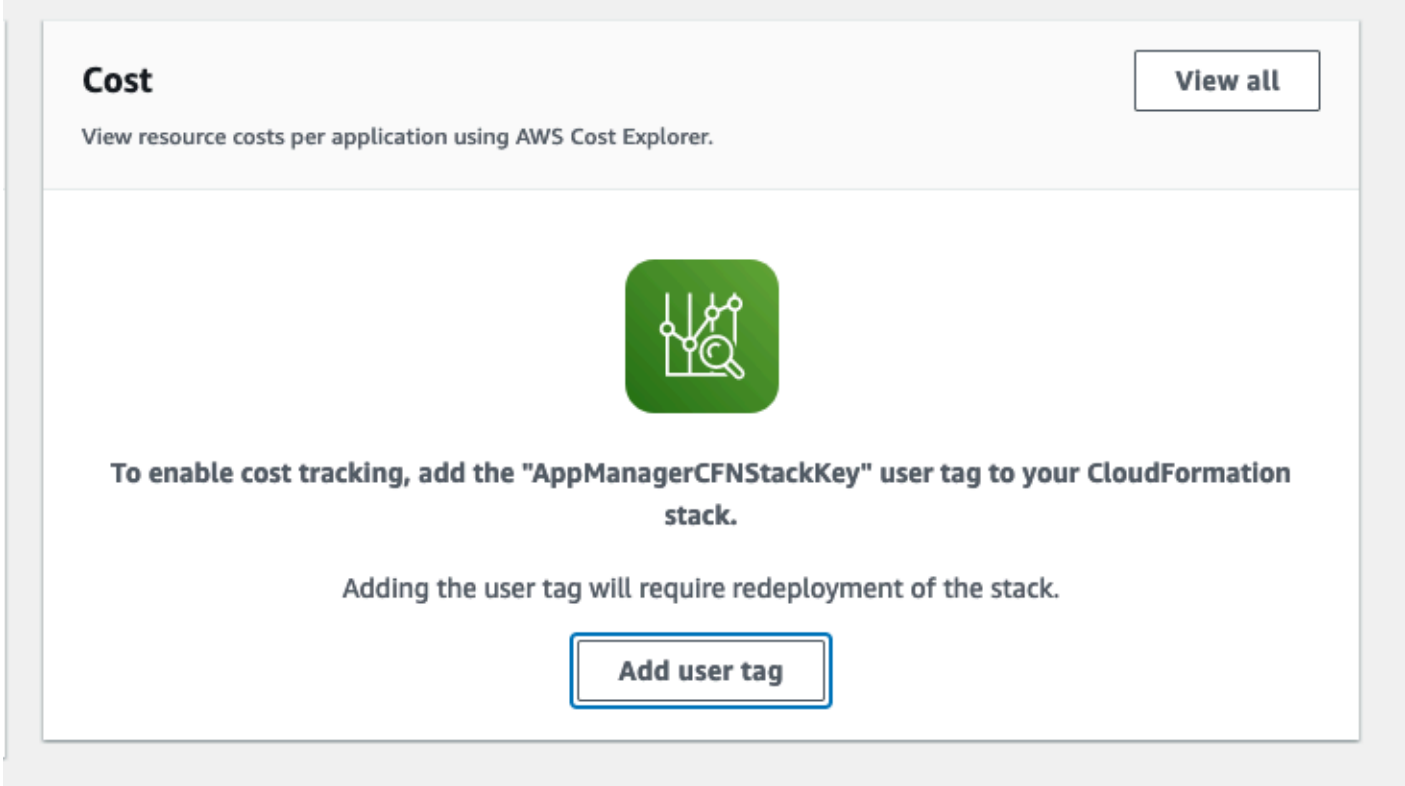


Konfirmasikan tag biaya yang terkait dengan solusi

Setelah Anda mengaktifkan tag alokasi biaya yang terkait dengan solusi, Anda harus mengonfirmasi tag alokasi biaya untuk melihat biaya untuk solusi ini. Untuk mengonfirmasi tag alokasi biaya:

1. Masuk ke konsol Systems Manager.
2. Pada panel navigasi, pilih Manajer Aplikasi.
3. Di Aplikasi, pilih nama aplikasi untuk solusi ini dan pilih.

   Nama aplikasi akan memiliki App Registry di kolom Sumber Aplikasi, dan akan memiliki kombinasi nama solusi, Wilayah, ID akun, atau nama tumpukan.
4. Di tab Ikhtisar, di Biaya, pilih Tambahkan tag pengguna.



5. Pada halaman Tambahkan tag pengguna, masukkan`confirm`, lalu pilih Tambahkan tag pengguna.

Proses aktivasi dapat memakan waktu hingga 24 jam untuk menyelesaikan dan data tag muncul.

Aktifkan tag alokasi biaya yang terkait dengan solusi

Setelah Anda mengaktifkan Cost Explorer, Anda harus mengaktifkan tag alokasi biaya yang terkait dengan solusi ini untuk melihat biaya untuk solusi ini. Tag alokasi biaya hanya dapat diaktifkan dari akun manajemen untuk organisasi. Untuk mengaktifkan tag alokasi biaya:

1. Masuk ke konsol AWS Billing and Cost Management dan Manajemen Biaya.
2. Di panel navigasi, pilih Tag Alokasi Biaya.
3. Pada halaman Tag alokasi biaya, filter untuk AppManager CFNStackKey tag, lalu pilih tag dari hasil yang ditampilkan.
4. Pilih Aktifkan.

AWS Cost Explorer

Anda dapat melihat ikhtisar biaya yang terkait dengan komponen aplikasi dan aplikasi dalam konsol Manajer Aplikasi melalui integrasi dengan AWS Cost Explorer, yang harus diaktifkan terlebih dahulu. Cost Explorer membantu Anda mengelola biaya dengan memberikan tampilan biaya dan penggunaan AWS sumber daya Anda dari waktu ke waktu. Untuk mengaktifkan Cost Explorer untuk solusinya:

1. Masuk ke konsol Manajemen AWS Biaya.
2. Di panel navigasi, pilih Cost Explorer untuk melihat biaya dan penggunaan solusi dari waktu ke waktu.

Perbarui solusinya

Jika sebelumnya Anda menerapkan solusi, ikuti prosedur ini untuk memperbarui CloudFormation tumpukan solusi untuk mendapatkan versi terbaru dari kerangka kerja solusi. Sebelum Anda memperbarui tumpukan, baca Perbarui pertimbangan dengan cermat.

1. Masuk ke konsol AWS CloudFormation tersebut.
2. Pilih Tumpukan di menu navigasi kiri.
3. Pilih `aws-waf-security-automations` CloudFormation tumpukan yang ada.
4. Pilih Perbarui.
5. Pilih Ganti template saat ini.
6. Di bawah Tentukan template:
   a. Pilih Amazon S3 URL.
   b. Salin tautan dari `aws-waf-security-automations.template` AWS CloudFormation.
   c. Tempel tautan di kotak Amazon S3 URL.
   d. Verifikasi bahwa templat yang benar URL ditampilkan di kotak URL teks Amazon S3.
   e. Pilih Berikutnya.
   f. Pilih Selanjutnya sekali lagi.
7. Di bawah Parameter, tinjau parameter untuk templat dan modifikasi seperlunya. Lihat Langkah 1. Luncurkan tumpukan untuk detail tentang parameter.
8. Pilih Berikutnya.
9. Pada Konfigurasikan halaman opsi stack, pilih Berikutnya.
10. Pada halaman Ulasan, tinjau dan konfirmasikan pengaturan.
11. Pilih kotak yang mengakui bahwa templat dapat membuat IAM sumber daya.
12. Pilih Lihat set perubahan dan verifikasi perubahan.
13. Pilih Perbarui tumpukan untuk menyebarkan tumpukan.

Anda dapat melihat status tumpukan di AWS CloudFormation konsol di kolom Status. Anda akan melihat status UPDATE _ COMPLETE dalam waktu sekitar 15 menit.

Perbarui pertimbangan

Bagian berikut memberikan kendala dan pertimbangan untuk memperbarui solusi ini.

Pembaruan jenis sumber daya

Anda harus menerapkan tumpukan baru untuk memperbarui parameter Endpoint setelah membuat tumpukan. Jangan mengubah parameter Endpoint saat memperbarui tumpukan.

WAFV2meng-upgrade

Mulai dari versi 3.0, solusi ini mendukung AWS WAF V2. Kami mengganti semua API panggilan AWS WAF Klasik dengan APIpanggilan AWS WAF V2. Ini menghapus dependensi pada Node.js dan menggunakan runtime Python up-to-date paling banyak. Untuk terus menggunakan solusi ini dengan fitur dan peningkatan terbaru, Anda harus menerapkan versi 3.0 atau lebih tinggi sebagai tumpukan baru.

Kustomisasi pada pembaruan tumpukan

out-of-boxSolusinya menerapkan seperangkat AWS WAF aturan dengan konfigurasi default ke dalam tumpukan Anda Akun AWS . CloudFormation Kami tidak menyarankan untuk menerapkan penyesuaian pada aturan yang diterapkan oleh solusi. Pembaruan tumpukan menimpa perubahan ini. Jika Anda memerlukan aturan yang disesuaikan, sebaiknya buat aturan terpisah di luar solusi.

> **Note**
>
> Jika Anda memutakhirkan dari versi 3.0 atau 3.1 ke versi 3.2 atau yang lebih baru dari solusi ini, dan Anda telah memasukkan alamat IP secara manual ke dalam kumpulan IP yang diizinkan atau ditolak, Anda akan berisiko kehilangan alamat IP tersebut. Untuk mencegah hal itu terjadi, buat salinan alamat IP di set IP yang diizinkan atau ditolak sebelum memutakhirkan solusi. Kemudian setelah Anda menyelesaikan upgrade, tambahkan alamat IP kembali ke set IP sesuai kebutuhan. Lihat perintah get-ip-setdan update-ip-setCLIperintah. Jika Anda sudah menggunakan versi 3.2 atau yang lebih baru, abaikan langkah ini.

Copot pemasangan solusinya

Untuk menghapus instalan solusi, hapus CloudFormation tumpukan:

1. Masuk ke konsol AWS CloudFormation tersebut.

2. Pilih tumpukan induk solusi. Semua tumpukan solusi lainnya akan dihapus secara otomatis.
3. Pilih Hapus.

> **Note**
>
> Menghapus instalan solusi akan menghapus semua AWS sumber daya yang digunakan oleh solusi kecuali untuk bucket Amazon S3. Jika beberapa set IP gagal dihapus karena tingkat melebihi masalah pelambatan yang disebabkan oleh AWAWAFAPIkuota, hapus set IP tersebut secara manual, lalu hapus tumpukan tersebut.

Gunakan solusinya

Bagian ini memberikan petunjuk terperinci untuk menggunakan solusi setelah Anda menerapkan solusi.

Ubah set IP yang diizinkan dan ditolak (opsional)

Setelah menerapkan CloudFormation tumpukan solusi ini, Anda dapat secara manual memodifikasi set IP yang diizinkan dan ditolak untuk menambah atau menghapus alamat IP seperlunya.

1. Masuk ke konsol AWS WAF tersebut.
2. Di panel navigasi kiri, pilih Set IP.
3. Pilih set IP untuk Daftar yang Diizinkan dan tambahkan alamat IP dari sumber tepercaya.
4. Pilih set IP untuk Daftar Ditolak dan tambahkan alamat IP yang ingin Anda blokir.

Sematkan tautan Honeypot di aplikasi web Anda (opsional)

Jika Anda memilih `yes` parameter Activate Bad Bot Protection di Langkah 1. Luncurkan tumpukan, CloudFormation template membuat titik akhir perangkap ke honeypot produksi interaksi rendah. Perangkap ini dimaksudkan untuk mendeteksi dan mengalihkan permintaan masuk dari pencakar konten dan bot buruk. Pengguna yang valid tidak akan mencoba mengakses titik akhir ini.

Namun, pencakar konten dan bot, seperti malware yang memindai kerentanan keamanan dan menggores alamat email, mungkin mencoba mengakses titik akhir perangkap. Dalam skenario ini, fungsi `Access Handler` Lambda memeriksa permintaan untuk mengekstrak asalnya, dan kemudian memperbarui AWS WAF aturan terkait untuk memblokir permintaan berikutnya dari alamat IP tersebut.

Gunakan salah satu prosedur berikut untuk menyematkan tautan honeypot untuk permintaan dari CloudFront distribusi atau. ALB

Buat CloudFront Asal untuk Honeypot Endpoint

Gunakan prosedur ini untuk aplikasi web yang digunakan dengan CloudFront distribusi. Dengan CloudFront, Anda dapat menyertakan `robots.txt` file untuk membantu mengidentifikasi pencakar

konten dan bot yang mengabaikan standar pengecualian robot. Selesaikan langkah-langkah berikut untuk menyematkan tautan tersembunyi dan kemudian secara eksplisit melarangnya di file Anda. `robots.txt`

1. Masuk ke konsol AWS CloudFormation tersebut.
2. Pilih tumpukan yang Anda bangun di Langkah 1. Luncurkan tumpukan
3. Pilih tab Output.
4. Dari BadBotHoneypotEndpointkunci, salin titik akhirURL. Ini berisi dua komponen yang Anda butuhkan untuk menyelesaikan prosedur ini:
   - Nama host endpoint (misalnya,`xxxxxxxxxx.execute-api.region.amazonaws.com`)
   - Permintaan URI (`/ProdStage`)
5. Masuk ke CloudFront konsol Amazon.
6. Pilih distribusi yang ingin Anda gunakan.
7. Pilih Pengaturan Distribusi.
8. Pada tab Origins, pilih Create Origin.
9. Di bidang Nama Domain Asal, tempel komponen nama host dari titik akhir URL yang Anda salin di Langkah 2. Kaitkan Web ACL dengan aplikasi web Anda.
10. Di Origin Path, tempel permintaan URL yang juga Anda salin di Langkah 2. Kaitkan Web ACL dengan aplikasi web Anda.
11. Terima nilai default untuk bidang lainnya.
12. Pilih Buat.
13. Pada tab Behaviors, pilih Create Behavior.
14. Buat perilaku cache baru dan arahkan ke asal baru. Anda dapat menggunakan domain khusus, seperti nama produk palsu yang mirip dengan konten lain di aplikasi web Anda.
15. Sematkan tautan titik akhir ini di konten Anda yang mengarah ke honeypot. Sembunyikan tautan ini dari pengguna manusia Anda. Sebagai contoh, tinjau contoh kode berikut:

```
<a href="/behavior_path" rel="nofollow" style="display: none" aria-
hidden="true">honeypot link</a>
```

> **Note**
>
> Anda bertanggung jawab untuk memverifikasi nilai tag apa yang berfungsi di lingkungan situs web Anda. Jangan gunakan `rel="nofollow"` jika lingkungan Anda tidak

mengamatinya. Untuk informasi selengkapnya tentang konfigurasi tag meta robot, lihat panduan pengembang Google.

16. Ubah `robots.txt` file di root situs web Anda untuk secara eksplisit melarang tautan honeypot, sebagai berikut:

```
User-agent: <*>
        Disallow: /<behavior_path>
```

Sematkan titik akhir Honeypot sebagai tautan eksternal

Gunakan prosedur ini untuk aplikasi web yang digunakan dengan fileALB.

1. Masuk ke konsol AWS CloudFormation tersebut.
2. Pilih tumpukan yang Anda bangun di Langkah 1. Luncurkan tumpukan.
3. Pilih tab Output.
4. Dari BadBotHoneypotEndpointkunci, salin titik akhirURL.
5. Sematkan tautan titik akhir ini di konten web Anda. Gunakan lengkap URL yang Anda salin di Langkah 2. Kaitkan Web ACL dengan aplikasi web Anda. Sembunyikan tautan ini dari pengguna manusia Anda. Sebagai contoh, tinjau contoh kode berikut:

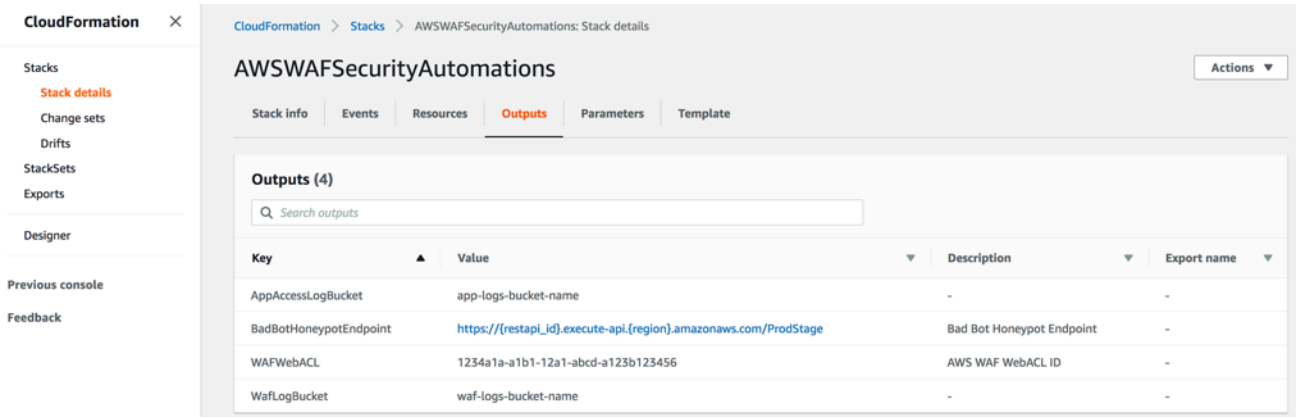
```
<a href="<BadBotHoneypotEndpoint value>" rel="nofollow" style="display: none" aria-
hidden="true"><honeypot link></a>
```

> **Note**
>
> Prosedur ini digunakan `rel=nofollow` untuk menginstruksikan robot untuk tidak mengakses URL honeypot. Namun, karena tautan disematkan secara eksternal, Anda tidak dapat menyertakan `robots.txt` file untuk secara eksplisit melarang tautan tersebut. Anda bertanggung jawab untuk memverifikasi tag apa yang berfungsi di lingkungan situs web Anda. Jangan gunakan `rel="nofollow"` jika lingkungan Anda tidak mengamatinya.

Gunakan file parser log Lambda JSON

Gunakan JSON file parser log Lambda untuk perlindungan Banjir HTTP

Jika Anda `Yes - AWS Lambda log parser` memilih parameter template Activate HTTP Flood Protection, solusi ini akan membuat file konfigurasi bernama *`<stack_name>`*`-waf_log_conf.json` dan mengunggahnya ke bucket Amazon S3 yang digunakan untuk menyimpan AWS WAF file log. Untuk menemukan nama bucket, lihat WafLogBucketvariabel dalam CloudFormation output. Gambar berikut menunjukkan contoh.



Output tumpukan

Jika Anda mengedit dan menimpa *`<stack_name>`*`-waf_log_conf.json` file di Amazon S3, fungsi `Log Parser` Lambda mempertimbangkan nilai baru saat memproses file log baru. AWS WAF Berikut ini adalah contoh file konfigurasi:

```
{
  "general": {
     "requestThreshold": 2000,
     "blockPeriod": 240,
     "ignoredSufixes": [".css", ".js", ".jpg", "png", ".gif"]
   },
  "uriList": {
     "/search": {
         "requestThreshold": 500,
         "blockPeriod": 600
     }
   }
}
```

HTTPfile konfigurasi banjir

Parameter meliputi:

- Umum:
  - Ambang permintaan (wajib) - Permintaan maksimum yang dapat diterima per lima menit, per alamat IP. Solusi ini menggunakan nilai yang Anda tentukan saat menyediakan atau memperbarui tumpukan. CloudFormation
  - Periode blok (wajib) — Periode (dalam menit) untuk memblokir alamat IP yang berlaku. Solusi ini menggunakan nilai yang Anda tentukan saat menyediakan atau memperbarui tumpukan. CloudFormation
  - Sufiks yang diabaikan - Permintaan yang mengakses jenis sumber daya ini tidak dihitung untuk meminta ambang batas. Secara default, daftar ini kosong.
- URIlist — Gunakan ini untuk menentukan ambang permintaan kustom dan periode blok untuk spesifikURLs. Secara default, daftar ini kosong.

Ketika WAF log tiba di WafLogBucket, mereka akan diproses oleh fungsi Lambda log parser menggunakan konfigurasi dalam file konfigurasi Anda. Solusinya menulis hasilnya ke file keluaran bernama `<stack_name>-waf_log_out.json` dalam ember yang sama. Jika file output berisi daftar alamat IP yang diidentifikasi sebagai penyerang, solusi menambahkannya ke set WAF IP untuk HTTPFlood, dan mereka diblokir untuk mengakses aplikasi Anda. Jika file output tidak memiliki alamat IP, periksa apakah file konfigurasi Anda valid atau apakah batas tarif telah melebihi sesuai dengan file konfigurasi.

Gunakan JSON file parser log Lambda untuk perlindungan pemindai dan probe

Jika Anda memilih `Yes - AWS Lambda log parser` parameter template Activate Scanner & Probe Protection, solusi ini akan membuat file konfigurasi bernama `<stack_name>-app_log_conf.json` dan mengunggahnya ke bucket Amazon S3 yang ditentukan yang digunakan untuk CloudFront menyimpan atau file log Application Load Balancer.

Jika Anda mengedit dan menimpa `<stack_name>-app_log_conf.json` di Amazon S3, fungsi `Log Parser` Lambda mempertimbangkan nilai baru saat memproses file log baru. AWS WAF Berikut ini adalah contoh file konfigurasi:

```
{
    "general": {
        "errorThreshold": 50,
        "blockPeriod": 240,
        "errorCodes": ["400", "401", "403", "404", "405"]
    },
    "uriList": {
        "/login": {
            "errorThreshold": 5,
            "blockPeriod": 600
        },
        "/api/feedback": {
            "errorThreshold": 10,
            "blockPeriod": 240
        }
    }
}
```

File konfigurasi pemindai dan Probe

Parameter meliputi:

- Umum:
  - Ambang kesalahan (wajib) - Permintaan buruk maksimum yang dapat diterima per menit, per alamat IP. Solusi ini menggunakan nilai yang Anda tentukan saat menyediakan atau memperbarui tumpukan. CloudFormation
  - Periode blok (wajib) — Periode (dalam menit) untuk memblokir alamat IP yang berlaku. Solusi ini menggunakan nilai yang Anda tentukan saat menyediakan atau memperbarui tumpukan. CloudFormation
  - Kode kesalahan - Kode status Teturn dianggap kesalahan. Secara default, daftar menganggap kode HTTP status berikut sebagai kesalahan:`400 (Bad Request)`,`401 (Unauthorized)`,`403 (Forbidden)`,`404 (Not Found)`, dan`405 (Method Not Allowed)`.

- URIlist — Gunakan ini untuk menentukan ambang permintaan kustom dan periode blok untuk spesifik. URLs Secara default, daftar ini kosong.

Ketika log akses aplikasi tiba di AppAccessLogBucket, fungsi `Log Parser` Lambda memprosesnya menggunakan konfigurasi dalam file konfigurasi Anda. Solusinya menulis hasilnya ke file keluaran bernama *`<stack_name>`*`-app_log_out.json` dalam ember yang sama. Jika file output berisi daftar alamat IP yang diidentifikasi sebagai penyerang, solusi menambahkannya ke set WAF IP untuk Scanner & Probe dan memblokir mereka dari mengakses aplikasi Anda. Jika file output tidak memiliki

alamat IP, periksa apakah file konfigurasi Anda valid atau apakah batas tarif telah terlampaui sesuai dengan file konfigurasi.

Gunakan negara dan URI dalam HTTP banjir Athena log parser

Anda dapat mengelompokkan IPs menurut negara dan URI di kueri Athena untuk mendeteksi dan memblokir serangan HTTP banjir yang memiliki pola yang tidak URI terduga. Untuk melakukannya, pilih salah satu opsi (`Country`,`URI`,`Country and URI`) untuk parameter Kueri Grup Berdasarkan Permintaan di HTTP Flood Athena saat meluncurkan tumpukan.

Anda juga dapat memasukkan ambang permintaan berdasarkan negara menggunakan parameter Request Threshold by Country. Misalnya, `{"TR": 50,"ER":150}`. Solusinya menggunakan ambang batas ini pada permintaan yang berasal dari negara-negara tertentu ini. Solusinya menggunakan ambang batas default pada permintaan dari negara lain.

> **Note**
>
> Jika Anda menentukan ambang batas menurut negara, solusinya secara otomatis menyertakan negara dalam klausa grup kueri Athena. Untuk informasi selengkapnya, lihat tabel parameter di Langkah 1. Luncurkan tumpukan.

Solusi menghitung ambang permintaan dalam periode lima menit secara default. Ini dapat dikonfigurasi dengan parameter Athena Query Run Time Schedule (Minute).

> **Note**
>
> Kueri Athena menghitung ambang batas per menit dengan membagi ambang permintaan dengan periode waktu. Sebagai contoh:
> Ambang permintaan (ambang batas default atau ambang batas menurut negara): 100
> Jadwal Waktu Jalankan Query Athena: 5
> Permintaan ambang per menit: 20 = 100/ 5

Lihat kueri Amazon Athena

Jika Anda memilih `Yes - Amazon Athena log parser` parameter template Activate HTTP Flood Protection atau Activate Scanner & Probe Protection, solusi ini membuat dan menjalankan

kueri Athena untuk CloudFront or ALB (`ScannersProbesLogParser`) atau AWS WAF logs (`HTTPFloodLogParser`), mem-parsing output, dan memperbarui sesuai dengan itu. AWS WAF

Untuk meningkatkan kinerja dan menjaga biaya tetap rendah, partisi solusi mencatat berdasarkan stempel waktu dalam nama file. Solusinya secara dinamis menghasilkan kueri Athena untuk menggunakan kunci partisi (tahun, bulan, hari, dan jam). Secara default, kueri berjalan setiap lima menit. Anda dapat mengonfigurasi jadwal lari mereka dengan mengubah nilai parameter template Athena Query Run Time Schedule (Minute). Setiap kueri yang dijalankan memindai empat hingga lima jam terakhir data secara default. Anda dapat mengonfigurasi jumlah data yang dipindai kueri dengan mengubah nilai parameter template Periode WAF Blok. Solusi ini juga menempatkan kueri dalam kelompok kerja terpisah untuk mengelola akses kueri dan biaya.

> **Note**
>
> Verifikasi bahwa Athena dikonfigurasi untuk mengakses file. AWS AWS Glue Data Catalog Solusi ini membuat katalog data log akses AWS Glue dan mengonfigurasi kueri Athena untuk memproses data. Jika Athena tidak dikonfigurasi dengan benar, kueri tidak berjalan. Untuk informasi lebih lanjut, lihat Upgrade ke yang terbaru AWSAWS Glue Data Catalog step-by-step.

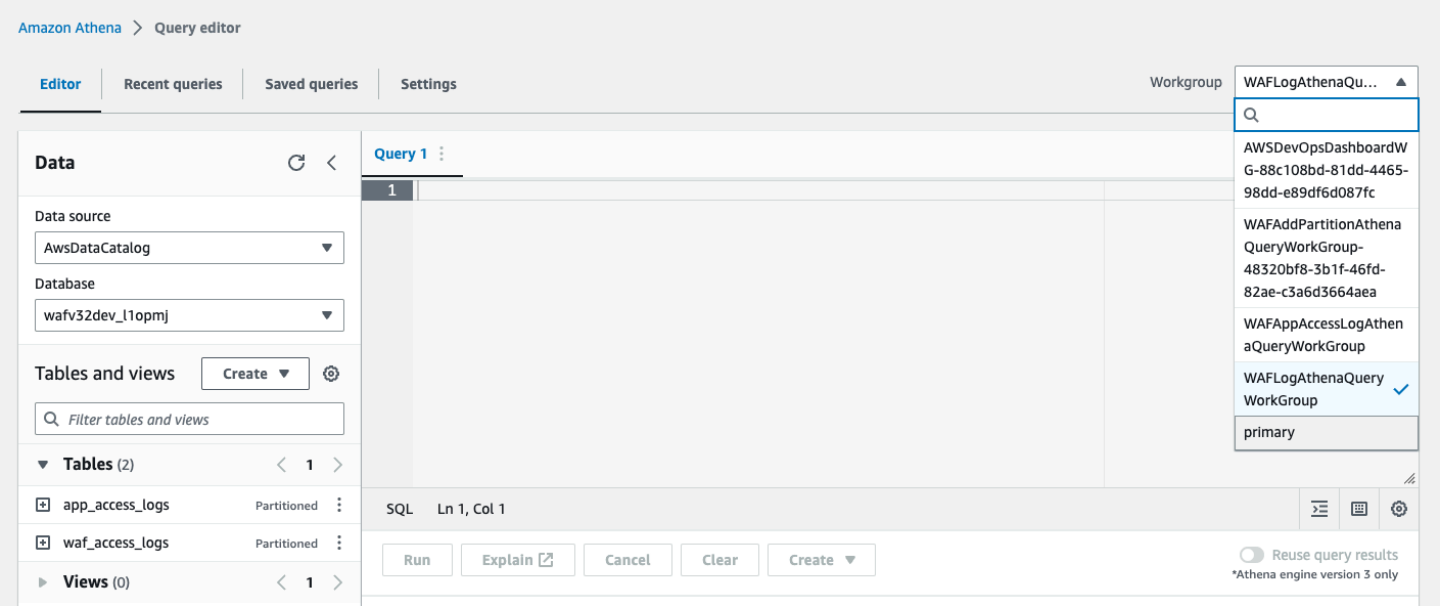
Gunakan prosedur berikut untuk melihat kueri ini:

Lihat kueri WAF log

1. Masuk ke konsol Amazon Athena.
2. Pilih Luncurkan editor kueri.
3. Pilih database untuk solusi ini.
4. Pilih WAFLogAthenaQueryWorkGroupdari daftar dropdown.

> **Note**
>
> Workgroup ini hanya ada jika Anda memilih `Yes - Amazon Athena log parser` parameter template Activate HTTP Flood Protection.

5. Pilih Beralih untuk mengganti workgroup.



6. Pilih tab Riwayat.
7. Pilih dan buka SELECT kueri dari daftar.

Lihat kueri log akses aplikasi

1. Masuk ke konsol Amazon Athena.
2. Pilih tab Workgroup.
3. Pilih WAFAppAccessLogAthenaQueryWorkGroupdari daftar.

> **Note**
>
> Workgroup ini hanya ada jika Anda memilih `Yes - Amazon Athena log parser` parameter template Activate Scanner & Probe Protection.

4. Pilih Switch workgroup.
5. Pilih tab Kueri terbaru.
6. Pilih dan buka SELECT kueri dari daftar.

Lihat menambahkan kueri partisi Athena

1. Masuk ke konsol Amazon Athena.

2. Pilih tab Workgroup.
3. Pilih WAFAddPartitionAthenaQueryWorkGroupdari daftar.

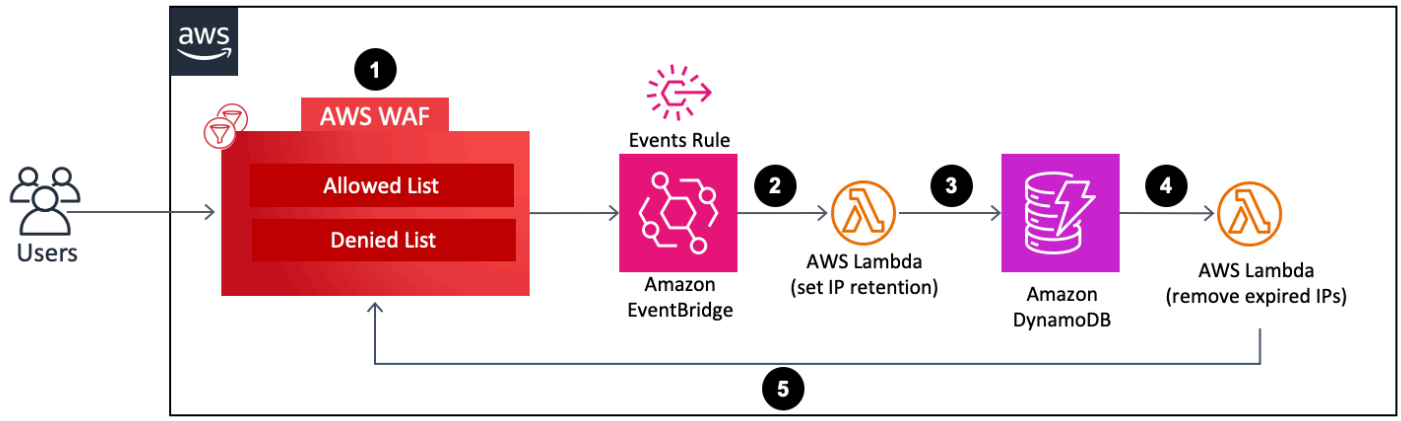
> **Note**
>
> Workgroup ini hanya ada jika Anda memilih `Yes - Amazon Athena log parser` parameter template Activate HTTP Flood Protection dan/atau Activate Scanner & Probe Protection.

4. Pilih Switch workgroup.
5. Pilih tab Riwayat.
6. Pilih dan buka `ALTER TABLE` kueri dari daftar. Kueri ini dijalankan setiap jam untuk menambahkan partisi per jam baru ke tabel Athena.

Konfigurasikan retensi IP pada set AWS WAF IP yang Diizinkan dan Ditolak

Anda dapat mengonfigurasi retensi IP pada set AWS WAF IP yang Diizinkan dan Ditolak yang dibuat oleh solusi. Bagian berikut menjelaskan cara kerjanya dan memberikan langkah-langkah untuk mengaturnya.

Cara kerjanya



Retensi IP pada Set WAF IP yang Diizinkan dan Ditolak

1. Saat pengguna memperbarui (menambah atau menghapus alamat IP) set WAF IP yang Diizinkan atau Ditolak, tindakan ini AWS WAF `UpdateIPSet` API memanggil panggilan dan membuat acara.
2. Aturan EventBridge peristiwa Amazon mendeteksi peristiwa berdasarkan pola peristiwa yang telah ditentukan sebelumnya, dan memanggil fungsi Lambda untuk mengatur periode retensi untuk semua alamat IP yang ada di set IP setelah pembaruan.
3. Fungsi Lambda memproses peristiwa, mengekstrak data yang relevan ke retensi IP (seperti nama set IP, ID, ruang lingkup, alamat IP), dan memasukkannya ke dalam tabel DynamoDB. Ini juga menyisipkan `ExpirationTime` atribut untuk setiap item DynamoDB. Solusi menghitung waktu kedaluwarsa dengan menambahkan periode retensi yang ditentukan pengguna ke waktu acara. Tabel memiliki DynamoDB Streams dan Time to Live () diaktifkan. TTL TTLAtributnya adalah`ExpirationTime`.
4. Ketika item mencapai waktu kedaluwarsa, TTL dipanggil dan DynamoDB menghapus item dari tabel setelah waktu kedaluwarsa. Setelah penghapusan item, item yang dihapus ditambahkan ke aliran DynamoDB, yang memanggil fungsi Lambda untuk pemrosesan hilir.
5. Fungsi Lambda memperoleh informasi tentang item yang dihapus dari aliran DynamoDB dan membuat AWS WAF API panggilan untuk menghapus alamat IP kedaluwarsa yang disertakan dalam item dari set IP target. AWS WAF

Aktifkan retensi IP

Ikuti langkah-langkah berikut untuk mengaktifkan retensi IP:

1. Di tumpukan Cloudformation yang Anda terapkan atau perbarui, masukkan Periode Retensi IP (Menit) untuk Set IP yang Diizinkan dan Periode Retensi IP (Menit) untuk Set IP yang Ditolak. Periode retensi minimum adalah 15 menit. Solusinya memperlakukan angka apa pun antara `0` dan `15` as`15`. Untuk informasi selengkapnya tentang konfigurasi penerapan, lihat Langkah 1. Luncurkan tumpukan.
2. Masukkan alamat email jika Anda ingin menerima pemberitahuan email ketika alamat IP kedaluwarsa dihapus dari kumpulan AWS WAF IP. Jika Anda memilih untuk menerima pemberitahuan email, Anda harus mengonfirmasi langganan menggunakan tautan di email yang Anda terima setelah solusi berhasil diterapkan. Untuk informasi selengkapnya tentang konfigurasi penerapan, lihat Langkah 1. Luncurkan tumpukan.

3. Perbarui set AWS WAF IP dengan menambahkan atau menghapus alamat IP. Ini memulai proses retensi IP dan membuat item DynamoDB, termasuk daftar kedaluwarsa IP. Daftar kedaluwarsa ini terdiri dari alamat IP yang ada di set AWS WAF IP setelah Anda memperbaruinya.
4. Setelah item DynamoDB mencapai waktu kedaluwarsa dan dihapus dari tabel, solusi menghapus alamat IP yang termasuk dalam daftar kedaluwarsa IP item dari set IP. WAF

> **Note**
>
> Bergantung pada waktu ketika DynamoDB menghapus item yang kedaluwarsa TTL oleh, operasi penghapusan sebenarnya dari alamat IP kedaluwarsa dari kumpulan IP dapat bervariasi. AWS WAF Penghapusan TTL DynamoDB terutama tergantung pada ukuran dan tingkat aktivitas tabel. Harapkan penundaan dalam operasi AWS WAF penghapusan karena potensi penundaan dalam operasi penghapusan DynamoDB. Secara umum, solusi menghapus alamat IP kedaluwarsa dari set AWS WAF IP tak lama setelah penghapusan DynamoDB. TTL Untuk informasi selengkapnya, lihat DynamoDB Time to Live TTL () di Panduan Pengembang Amazon DynamoDB.

Bangun dasbor pemantauan

AWS merekomendasikan agar Anda mengonfigurasi sistem pemantauan dasar khusus untuk setiap titik akhir kritis. Untuk informasi tentang membuat dan menggunakan tampilan metrik yang disesuaikan, lihat CloudWatchDasbor — Buat & Gunakan Tampilan Metrik yang Disesuaikan dan Menggunakan dasbor Amazon CloudWatch .

Screenshot dasbor berikut menunjukkan contoh sistem pemantauan baseline kustom.

Dasbor menampilkan metrik berikut:

- Permintaan yang Diizinkan vs Diblokir - Menunjukkan jika Anda menerima lonjakan akses yang diizinkan (dua kali akses puncak normal) atau akses yang diblokir (periode apa pun yang mengidentifikasi lebih dari 1K permintaan yang diblokir). CloudWatch mengirimkan peringatan ke saluran Slack. Anda dapat menggunakan metrik ini untuk melacak DDoS serangan yang diketahui (ketika permintaan diblokir meningkat) atau versi baru serangan (ketika permintaan diizinkan untuk mengakses sistem).

  > **Note**
  >
  > Catatan: Solusinya menyediakan metrik ini.

- BytesDownloaded vs Unggah - Membantu mengidentifikasi kapan DDoS serangan menargetkan layanan yang biasanya tidak menerima sejumlah besar akses ke sumber daya buang (misalnya, komponen mesin pencari mengirim MBs informasi untuk satu set parameter permintaan tertentu).
- ELBSpillover and Queue length — Membantu memverifikasi apakah DDoS serangan menyebabkan kerusakan pada infrastruktur dan penyerang melewati CloudFront atau AWS WAF lapisan, dan menyerang sumber daya yang tidak terlindungi secara langsung.

- ELBJumlah Permintaan — Membantu mengidentifikasi kerusakan pada infrastruktur. Metrik ini menunjukkan apakah penyerang melewati lapisan perlindungan, atau jika Anda harus meninjau aturan CloudFront cache untuk meningkatkan tingkat hit cache.
- ELBTuan Rumah Sehat — Anda dapat menggunakan ini sebagai metrik pemeriksaan kesehatan sistem lain.
- ASGCPUPemanfaatan — Membantu mengidentifikasi apakah penyerang melewati CloudFront, AWS WAF, dan Elastic Load Balancing. Anda juga dapat menggunakan metrik ini untuk mengidentifikasi kerusakan serangan.

Tangani positif XSS palsu

Solusi ini mengonfigurasi AWS WAF aturan yang memeriksa elemen permintaan masuk yang umum dieksplorasi untuk mengidentifikasi dan memblokir serangan. XSS Pola deteksi ini kurang efektif jika beban kerja Anda memungkinkan pengguna yang sah untuk menulis dan mengirimkanHTML, misalnya, menggunakan editor teks kaya dalam sistem manajemen konten. Dalam skenario ini, pertimbangkan untuk membuat aturan pengecualian yang melewati XSS aturan default untuk URL pola tertentu yang menerima masukan teks kaya, dan menerapkan mekanisme alternatif untuk melindungi yang dikecualikanURLs.

Selain itu, beberapa format gambar atau data khusus dapat menyebabkan kesalahan positif karena mengandung pola yang menunjukkan potensi XSS serangan dalam HTML konten. Misalnya, SVG file mungkin berisi `<script>` tag. Jika Anda mengharapkan jenis konten ini dari pengguna yang sah, sesuaikan XSS aturan Anda secara sempit untuk mengizinkan HTML permintaan yang menyertakan format data lain ini.

Selesaikan langkah-langkah berikut untuk memperbarui XSS aturan untuk mengecualikan URLs yang diterima HTML sebagai input. Lihat Panduan WAF Pengembang Amazon untuk petunjuk terperinci.

1. Masuk ke konsol AWS WAF tersebut.
2. Buat kecocokan string atau kondisi regex.
3. Konfigurasikan pengaturan filter untuk memeriksa URI dan mencantumkan nilai yang ingin Anda terima terhadap XSS aturan.
4. Edit XSSAturan solusi ini dan tambahkan kondisi baru yang Anda buat.

   Misalnya, untuk mengecualikan semua URLs dalam daftar, pilih yang berikut untuk Ketika permintaan:

- tidak
- mencocokkan setidaknya satu dari filer dalam kondisi kecocokan string
- XSSDaftar Izinkan

Pemecahan Masalah

Jika Anda memerlukan bantuan dengan solusi ini, hubungi AWS Support untuk membuka kasus dukungan untuk solusi ini.

Kontak AWS Support

Jika Anda memiliki Support AWS Developer, AWSBusiness Support, atau AWSEnterprise Support, Anda dapat menggunakan Support Center untuk mendapatkan bantuan ahli dengan solusi ini. Bagian berikut memberikan petunjuk.

Buat kasus

1. Buka Support Center.
2. Pilih Buat kasus.

Bagaimana kami bisa membantu?

1. Pilih Teknis.
2. Untuk Layanan, pilih WAFatau AWS WAF.
3. Untuk Kategori, pilih Otomatisasi WAF Keamanan atau Otomasi Keamanan untuk. AWS WAF
4. Untuk Keparahan, opsi yang paling cocok dengan kasus penggunaan Anda.
5. Saat Anda memasuki Layanan, Kategori, dan Tingkat Keparahan, antarmuka mengisi tautan ke pertanyaan pemecahan masalah umum. Jika Anda tidak dapat menyelesaikan pertanyaan Anda dengan tautan ini, pilih Langkah selanjutnya: Informasi tambahan.

Informasi tambahan

1. Untuk Subjek, masukkan teks yang merangkum pertanyaan atau masalah Anda.
2. Untuk Deskripsi, jelaskan masalah ini secara rinci.
3. Pilih Lampirkan file.
4. Lampirkan informasi yang AWS Support diperlukan untuk memproses permintaan.

Bantu kami menyelesaikan kasus Anda lebih cepat

1. Masukkan informasi yang diminta.
2. Pilih Langkah selanjutnya: Selesaikan sekarang atau hubungi kami.

Selesaikan sekarang atau hubungi kami

1. Tinjau solusi Selesaikan sekarang.
2. Jika Anda tidak dapat menyelesaikan masalah Anda dengan solusi ini, pilih Hubungi kami, masukkan informasi yang diminta, dan pilih Kirim.

Panduan pengembang

Bagian ini menyediakan kode sumber untuk solusinya.

Kode sumber

Kunjungi GitHubrepositori kami untuk mengunduh templat dan skrip untuk solusi ini, dan untuk berbagi penyesuaian Anda dengan orang lain.

Referensi

Bagian ini mencakup informasi tentang fitur opsional untuk mengumpulkan metrik unik untuk solusi ini, petunjuk ke sumber daya terkait, dan daftar pembangun yang berkontribusi pada solusi ini.

Pengumpulan data anonim

Solusi ini mencakup opsi untuk mengirim metrik operasional ke AWS. Kami menggunakan data ini untuk lebih memahami bagaimana pelanggan menggunakan solusi ini dan layanan serta produk terkait. Ketika dihidupkan, solusi mengumpulkan informasi berikut dikumpulkan dan mengirimkannya ke AWS selama penyebaran awal template: CloudFormation

- ID Solusi — Pengidentifikasi AWS solusi
- Unique ID (UUID) - Pengidentifikasi unik yang dibuat secara acak untuk setiap penerapan solusi ini
- Stempel waktu - Stempel waktu pengumpulan data
- Konfigurasi solusi - Fitur diaktifkan dan parameter ditetapkan selama peluncuran awal
- Siklus Hidup - Berapa lama pelanggan menggunakan solusi ini (berdasarkan penghapusan tumpukan)
- Data pengurai log:
  - Jumlah alamat IP dalam set IP Scanner & Probe dan IP HTTPFlood diatur untuk memblokir
  - Jumlah permintaan yang diproses dan diblokir
- IP mencantumkan data parser:
  - Jumlah alamat IP dalam kumpulan IP Daftar Reputasi
  - Jumlah permintaan yang diproses dan diblokir
- Akses data penangan:
  - Jumlah alamat IP dalam set IP Bad Bot
  - Jumlah permintaan yang diproses dan diblokir
- Data retensi IP - Jumlah alamat IP kedaluwarsa yang dihapus dari kumpulan IP yang Diizinkan atau Ditolak

AWS memiliki data yang dikumpulkan melalui survei ini. Pengumpulan data tunduk pada Kebijakan AWS Privasi. Untuk memilih keluar dari fitur ini, selesaikan langkah-langkah berikut sebelum meluncurkan AWS CloudFormation template.

1. Unduh `aws-waf-security-automations.template` AWS CloudFormationke hard drive lokal Anda.
2. Buka CloudFormation template dengan editor teks.
3. Ubah bagian pemetaan CloudFormation template dari:

```
Solution:
  Data:
   SendAnonymizedUsageData: "Yes"
```

   ke:

```
Solution:
  Data:
   SendAnonymizedUsageData: "No"
```

4. Masuk ke AWS CloudFormation konsol.
5. Pilih Buat tumpukan.
6. Pada halaman Buat tumpukan, Tentukan templat bagian, pilih Unggah file templat.
7. Di bawah Unggah file templat, pilih Pilih file dan pilih templat yang diedit dari drive lokal Anda.
8. Pilih Berikutnya dan ikuti langkah-langkah di Langkah 1. Luncurkan tumpukan.

Sumber daya terkait

AWS Whitepaper terkait

- AWS Praktik Terbaik untuk DDoS Ketahanan

Posting Blog AWS Keamanan Terkait

- Cara Mencegah Hotlinking dengan Menggunakan, AWS WAF Amazon CloudFront, dan Referer Checking

Daftar Reputasi IP Pihak Ketiga

- Situs web Daftar Spamhaus DROP

- Daftar IP Proofpoint Emerging Threats
- Daftar node keluar Tor

Kontributor

- Heitor Vital
- Lee Atkinson
- Ben Potter
- Vlad Vlasceanu
- Aijun Peng
- Chaitanya Deolankar
- Shu Jackson
- William Quan

Revisi

Tanggal	Perubahan
September 2016	Rilis awal
Januari 2017	Klarifikasi tentang batas alamat IP dalam solusi ini.
Maret 2017	Panduan tambahan tentang membuat perilaku cache; diperbarui URLs untuk posting Blog AWS Keamanan.
Juni 2017	Menambahkan ALB dukungan dan batas produk yang diperbarui.
November 2017	Menambahkan dukungan aturan berbasis tarif untuk perlindungan HTTP banjir; tautan tambahan untuk menyimpan log akses sumber daya.
Januari 2018	Konten yang diperbarui tentang ketersediaan regional AWS WAF untuk Application Load Balancers.
Desember 2018	Menambahkan IPv6 Support, memperluas CIDR rentang, dan menambahkan dashboard pemantauan.
April 2019	AWS WAF log integrasi, integrasi Amazon Athena, dan menambahkan parser log yang dapat dikonfigurasi.
Desember 2019	Menambahkan informasi tentang dukungan untuk pembaruan Node.js.
Februari 2020	Perbaikan bug dan pembaruan ke RequestTh reshold parameter.

Tanggal	Perubahan
Juni 2020	Menambahkan optimasi biaya Athena menggunakan partisi; README instruksi yang diperbarui; memperbaiki potensi masalah DoS dalam header Bad Bots. X-Forward-For
Juli 2020	Ditingkatkan dari layanan AWS WAF API Klasik ke AWS WAF V2.
November 2020	Versi rilis 3.1.0: klarifikasi tentang aturan Perlindungan HTTP Banjir dan Perlindungan Pemindai & Probe untuk Wilayah tertentu; mengganti tipe jalur S3 dengan gaya yang dihosting virtual; menambahkan variabel partisi ke semuaARNs; untuk informasi lebih lanjut, lihat file.md di repositori. CHANGELOG GitHub
September 2021	Versi rilis 3.2.0: Menambahkan dukungan retensi IP pada Set IP yang Diizinkan dan Ditolak; perbaikan bug. Untuk informasi lebih lanjut, lihat CHANGELOGfile.md di GitHub repositori.
Agustus 2022	Versi rilis 3.2.1: Menambahkan dukungan pada penanganan WAF kebesaran untuk komponen permintaan; menambahkan dukungan pada tingkat WAF sensitivitas untuk pernyataan aturan SQL injeksi. Untuk informasi lebih lanjut, lihat CHANGELOGfile.md di GitHub repositori.
September 2022	Dokumentasi yang diperbarui untuk kustomisa si di luar CloudFormation tumpukan solusi.

Tanggal	Perubahan
Desember 2022	Versi rilis 3.2.2: Menambahkan integrasi dengan Service Catalog AppRegistry dan Manajer Aplikasi AWS Systems Manager. Untuk informasi lebih lanjut, lihat CHANGELOG file.md di GitHub repositori.
Desember 2022	Versi rilis 3.2.3: Tambahkan wilayah sebagai awalan ke nama grup atribut aplikasi untuk menghindari konflik dengan nama yang dimulai dengan. AWS Untuk informasi lebih lanjut, lihat CHANGELOGfile.md di GitHub repositori.
Februari 2023	Versi rilis 3.2.4: Pytest yang ditingkatkan dan permintaan untuk mengurangi. CVE Untuk informasi lebih lanjut, lihat CHANGELOGfile.md di GitHub repositori.
Maret 2023	Dokumentasi yang diperbarui untuk meningkat kan solusi dari versi 3.0 atau 3.1 ke 3.2 atau yang lebih baru yang telah mengizinkan atau menolak alamat IP.
April, 2023	Versi rilis 3.2.5: Dampak yang dikurangi yang disebabkan oleh pengaturan default baru untuk Kepemilikan Objek Amazon S3 (ACLsdino naktifkan) untuk semua bucket Amazon S3 baru. Untuk informasi lebih lanjut, lihat CHANGELOGfile.md di GitHub repositori.
Mei 2023	Versi rilis 4.0.0: Menambahkan dukungan untuk grup Peraturan yang Dikelola AWS aturan baru dan aturan kustom yang diperbarui. Untuk informasi lebih lanjut, lihat CHANGELOGfile.md di GitHub repositori.

Tanggal	Perubahan
Mei 2023	Versi rilis 4.0.1: `.gitignore` File yang diperbarui untuk menyelesaikan masalah file yang hilang. Untuk informasi lebih lanjut, lihat CHANGELOGfile.md di GitHub repositori.
September 2023	Versi rilis 4.0.2: Kode refactored untuk meningkatkan kualitas. Kerentanan paket permintaan yang ditambal. Untuk informasi lebih lanjut, lihat CHANGELOGfile.md di GitHub repositori.
Oktober 2023	Versi rilis 4.0.3: Versi paket yang diperbarui untuk mengatasi kerentanan keamanan. Untuk informasi lebih lanjut, lihat CHANGELOGfile.md di GitHub repositori.
November 2023	Pembaruan dokumentasi: Menambahkan Support AWS Developer dan menggabungkan Contact AWS Support ke bagian Troublesh ooting.
November 2023	Pembaruan dokumentasi: Menambahkan tag biaya Konfirmasi yang terkait dengan solusi ke AppRegistry bagian Memantau solusi dengan AWS Service Catalog.
April 2024	Pembaruan dokumentasi: Petunjuk yang diklarifikasi untuk menambahkan bucket S3 di langkah penerapan 3.
September 2024	Versi rilis 4.0.4: Versi paket yang diperbarui untuk mengatasi kerentanan keamanan. Untuk informasi lebih lanjut, lihat CHANGELOGfile.md di GitHub repositori.

Tanggal	Perubahan
Oktober 2024	Versi rilis 4.0.5: Puisi Digunakan untuk manajemen ketergantungan. Mengganti logger Python asli dengan logger aws_lambda_powertools. Untuk informasi lebih lanjut, lihat CHANGELOGfile.md di GitHub repositori.
Desember 2024	Versi rilis 4.0.6: Perbarui lambda ke python 3.12. Untuk informasi lebih lanjut, lihat CHANGELOGfile.md di GitHub repositori.

Pemberitahuan

Panduan implementasi ini disediakan hanya untuk tujuan informasi. Ini mewakili penawaran dan praktik AWS produk saat ini pada tanggal penerbitan dokumen ini, yang dapat berubah tanpa pemberitahuan. Pelanggan bertanggung jawab untuk membuat penilaian independen mereka sendiri atas informasi dalam dokumen ini dan setiap penggunaan AWS produk atau layanan, yang masing-masing disediakan “sebagaimana adanya” tanpa jaminan dalam bentuk apa pun, baik tersurat maupun tersirat. Dokumen ini tidak membuat jaminan, representasi, komitmen kontrak, kondisi atau jaminan apa pun dariAWS, afiliasinya, pemasok, atau pemberi lisensinya. Tanggung jawab dan kewajiban AWS kepada pelanggannya dikendalikan oleh perjanjian AWS, dan dokumen ini bukan bagian dari, juga tidak mengubah, perjanjian apa pun antara AWS dan pelanggannya.

Otomatisasi Keamanan untuk AWS WAF solusi dilisensikan berdasarkan ketentuan Lisensi Apache Versi 2.0.

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.