AWS Whitepaper

AWS Praktik Terbaik untuk DDoS Ketahanan

AWS Praktik Terbaik untuk DDoS Ketahanan: AWS Whitepaper

Table of Contents

AWS Praktik Terbaik untuk DDoS Ketahanan

Tanggal publikasi: 9 Agustus 2023 () Revisi dokumen

Penting untuk melindungi bisnis Anda dari dampak serangan Distributed Denial of Service (DDoS), serta serangan siber lainnya. Menjaga kepercayaan pelanggan pada layanan Anda dengan menjaga ketersediaan dan daya tanggap aplikasi Anda adalah prioritas tinggi. Anda juga ingin menghindari biaya langsung yang tidak perlu ketika infrastruktur Anda harus skala sebagai respons terhadap serangan. Amazon Web Services (AWS) berkomitmen untuk menyediakan alat, praktik terbaik, dan layanan untuk melindungi Anda dari pelaku jahat di internet. Menggunakan layanan yang tepat dari AWS membantu memastikan ketersediaan, keamanan, dan ketahanan yang tinggi.

Dalam whitepaper ini, AWS memberi Anda DDoS panduan preskriptif untuk meningkatkan ketahanan aplikasi yang berjalan. AWS Ini termasuk arsitektur referensi DDoS -resilient yang dapat digunakan sebagai panduan untuk membantu melindungi ketersediaan aplikasi. Whitepaper ini juga menjelaskan berbagai jenis serangan, seperti serangan lapisan infrastruktur dan serangan lapisan aplikasi. AWS menjelaskan praktik terbaik mana yang paling efektif untuk mengelola setiap jenis serangan. Selain itu, layanan dan fitur yang sesuai dengan strategi DDoS mitigasi diuraikan, bersama dengan bagaimana masing-masing dapat digunakan untuk membantu melindungi aplikasi Anda.

Paper ini ditujukan untuk pengambil keputusan TI dan insinyur keamanan yang akrab dengan konsep dasar jaringan, keamanan, dan AWS. Setiap bagian memiliki tautan ke AWS dokumentasi yang memberikan detail lebih lanjut tentang praktik atau kemampuan terbaik.

AWS mendeteksi lebih dari satu juta DDoS serangan per tahun dan mengurangi ribuan setiap hari terhadap pelanggan kami. Menurut tim Response Shield kami (SRT), mayoritas pelanggan yang mengalami dampak bisnis dari DDoS serangan belum menerapkan rekomendasi dalam panduan ini.

Apakah Anda sudah Well-Architected?

Kerangka Kerja AWS Well-Architected membantu Anda memahami pro dan kontra dari keputusan yang Anda buat saat membangun sistem di cloud. Enam pilar dari Kerangka Kerja ini memungkinkan Anda mempelajari praktik terbaik arsitektural untuk merancang dan mengoperasikan sistem yang andal, aman, efisien, hemat biaya, dan berkelanjutan. Menggunakan AWS Well-Architected Tool, tersedia tanpa biaya di AWS Management Console(login diperlukan), Anda dapat meninjau beban kerja Anda terhadap praktik terbaik ini dengan menjawab serangkaian pertanyaan untuk setiap pilar.

Untuk panduan ahli dan praktik terbaik lainnya untuk arsitektur cloud Anda—penerapan arsitektur referensi, diagram, dan whitepaper, lihat Pusat Arsitektur.AWS

Pengantar serangan penolakan layanan

Serangan Denial of Service (DoS), atau peristiwa, adalah upaya yang disengaja untuk membuat situs web atau aplikasi tidak tersedia bagi pengguna, seperti dengan membanjirinya dengan lalu lintas jaringan. Penyerang menggunakan berbagai teknik yang mengkonsumsi sejumlah besar bandwidth jaringan atau mengikat sumber daya sistem lainnya, mengganggu akses untuk pengguna yang sah. Dalam bentuknya yang paling sederhana, penyerang tunggal menggunakan satu sumber untuk melakukan serangan DoS terhadap target, seperti yang ditunjukkan pada gambar berikut.

Diagram yang menggambarkan serangan DoS

Dalam serangan Distributed Denial of Service (DDoS), penyerang menggunakan beberapa sumber untuk mengatur serangan terhadap target. Sumber-sumber ini dapat mencakup kelompok terdistribusi komputer yang terinfeksi malware, router, perangkat IoT, dan titik akhir lainnya. Gambar berikut menunjukkan jaringan host yang dikompromikan yang berpartisipasi dalam serangan, menghasilkan banjir paket atau permintaan untuk membanjiri target.

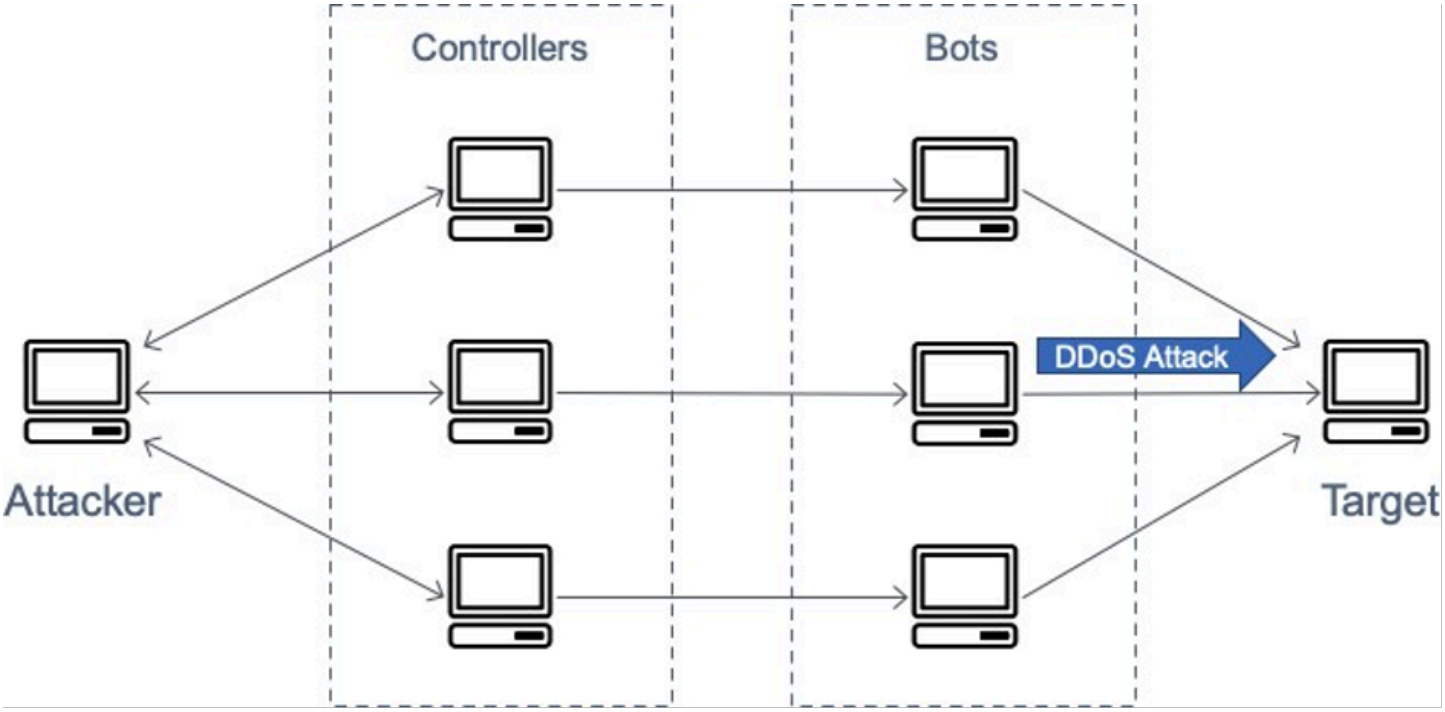


Diagram yang menggambarkan serangan DDoS

Ada tujuh lapisan dalam model Open Systems Interconnection (OSI), dan mereka dijelaskan dalam tabel berikut. DDoSserangan paling umum terjadi pada lapisan 3, 4, 6, dan 7.

- Serangan Layer 3 dan 4 sesuai dengan lapisan Network dan Transport OSI model. Dalam whitepaper ini, AWS mengacu pada ini secara kolektif sebagai serangan lapisan infrastruktur.
- Serangan Layer 6 dan 7 sesuai dengan lapisan Presentasi dan Aplikasi OSI model. Whitepaper ini membahas ini bersama-sama sebagai serangan lapisan aplikasi.

Paper ini membahas jenis serangan ini di bagian berikutnya.

Tabel 1 — OSI model

#	Lapisan	Unit	Deskripsi	Contoh vektor
7	Aplikasi	Data	Proses jaringan ke aplikasi	HTTPbanjir, banjir DNS permintaan
6	Presentasi	Data	Representasi dan enkripsi data	Penyalahgunaan Transport Layer Security (TLS)
5	Sesi	Data	Komunikasi antar host	N/A
4	Transportasi	Segmen	nd-to-end Koneksi E dan keandalan	Sinkronisasi (SYN) banjir
3	Jaringan	Paket	Penentuan jalur dan pengalama tan logis	Serangan refleksi Protokol Datagram Pengguna (UDP)
2	Tautan Data	Bingkai	Pengalamatan fisik	N/A

#	Lapisan	Unit	Deskripsi	Contoh vektor
1	Fisik	Bit	Media, sinyal, dan transmisi biner	N/A

Serangan lapisan infrastruktur

DDoSSerangan yang paling umum, User Datagram Protocol (UDP) serangan refleksi dan SYN banjir, adalah serangan lapisan infrastruktur. Seorang penyerang dapat menggunakan salah satu dari metode ini untuk menghasilkan volume besar lalu lintas yang dapat membanjiri kapasitas jaringan atau mengikat sumber daya pada sistem seperti server, firewall, sistem pencegahan intrusi ()IPS, atau penyeimbang beban. Meskipun serangan ini mudah diidentifikasi, untuk menguranginya secara efektif, Anda harus memiliki jaringan atau sistem yang meningkatkan kapasitas lebih cepat daripada banjir lalu lintas masuk. Kapasitas ekstra ini diperlukan untuk menyaring atau menyerap lalu lintas serangan yang membebaskan sistem dan aplikasi untuk menanggapi lalu lintas pelanggan yang sah.

UDPserangan refleksi

UDPserangan refleksi mengeksploitasi fakta bahwa UDP adalah protokol tanpa kewarganegaraan. Penyerang dapat membuat paket UDP permintaan yang valid yang mencantumkan alamat IP target serangan sebagai alamat IP UDP sumber. Penyerang sekarang telah memalsukan — menipu — IP sumber paket permintaanUDP. UDPPaket berisi IP sumber palsu dan dikirim oleh penyerang ke server perantara. Server ditipu untuk mengirimkan paket UDP responsnya ke IP korban yang ditargetkan daripada kembali ke alamat IP penyerang. Server perantara digunakan karena menghasilkan respons yang beberapa kali lebih besar dari paket permintaan, secara efektif memperkuat jumlah lalu lintas serangan yang dikirim ke alamat IP target.

Faktor amplifikasi adalah rasio ukuran respons terhadap ukuran permintaan, dan bervariasi tergantung pada protokol mana yang digunakan penyerang:, Protokol Waktu Jaringan ()DNS, Protokol Direktori Layanan Sederhana (NTP), Protokol Akses Direktori Ringan Tanpa Koneksi (SSDP), Memcached, Protokol Generator Karakter (CLDAP), atau Quote of the Day (CharGen). QOTD

Misalnya, faktor amplifikasi untuk DNS bisa 28 hingga 54 kali jumlah byte asli. Jadi, jika penyerang mengirimkan payload permintaan 64 byte ke DNS server, mereka dapat menghasilkan lebih dari 3400 byte lalu lintas yang tidak diinginkan ke target serangan. UDPSerangan refleksi bertanggung

jawab atas volume lalu lintas yang lebih besar dibandingkan dengan serangan lainnya. Gambar berikut menggambarkan taktik refleksi dan efek amplifikasi.

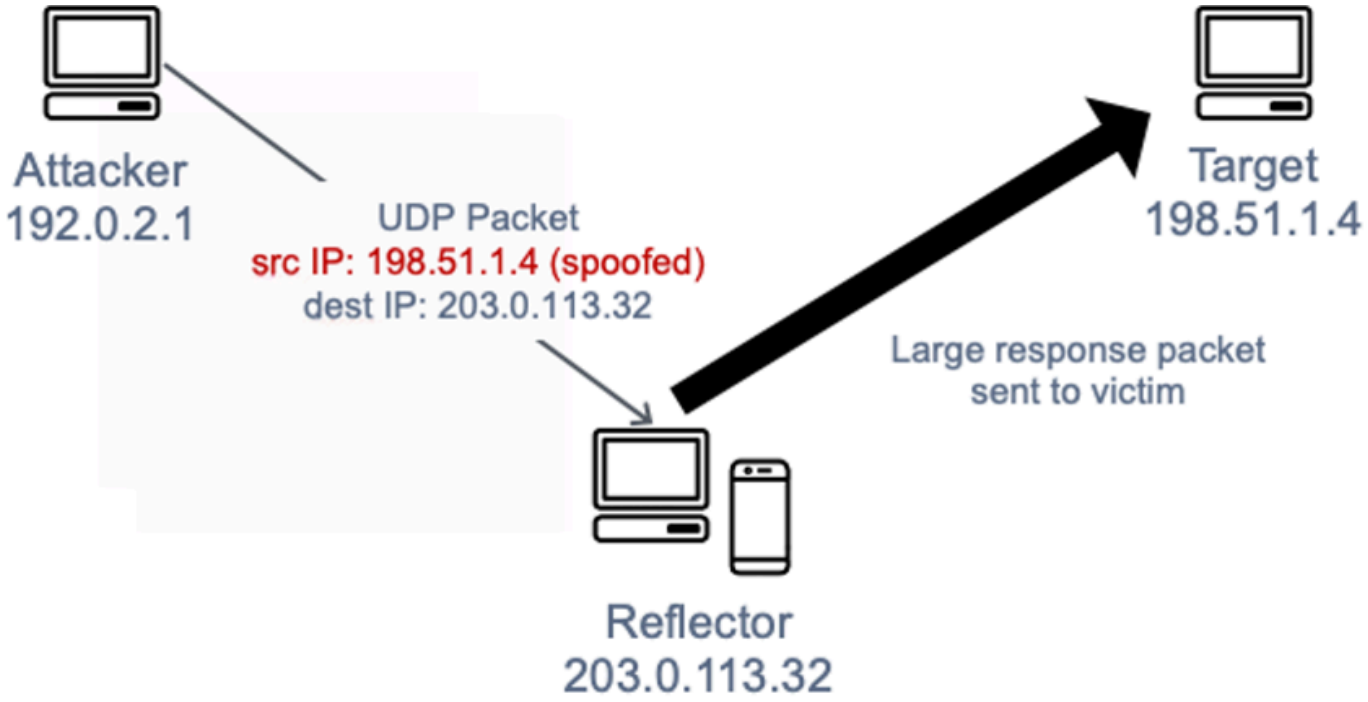


Diagram yang menggambarkan serangan UDP refleksi

Perlu dicatat bahwa serangan refleksi, sementara mereka memberikan penyerang dengan amplifikasi “gratis”, memerlukan kemampuan spoofing IP dan karena semakin banyak penyedia jaringan mengadopsi Validasi Alamat Sumber Di Mana Saja (SAVE) atau BCP38, kemampuan ini dihapus, mengharuskan penyedia DDoS layanan menghentikan serangan refleksi atau untuk pindah ke pusat data dan penyedia jaringan yang tidak menerapkan validasi alamat sumber.

SYNserangan banjir

Ketika pengguna terhubung ke layanan Transmission Control Protocol (TCP), seperti server web, klien mereka mengirim SYN paket. Server mengembalikan paket sinkronisasi-pengakuan (SYN-ACK), dan akhirnya klien merespons dengan paket pengakuan (ACK), yang melengkapi jabat tangan tiga arah yang diharapkan. Gambar berikut menggambarkan jabat tangan khas ini.

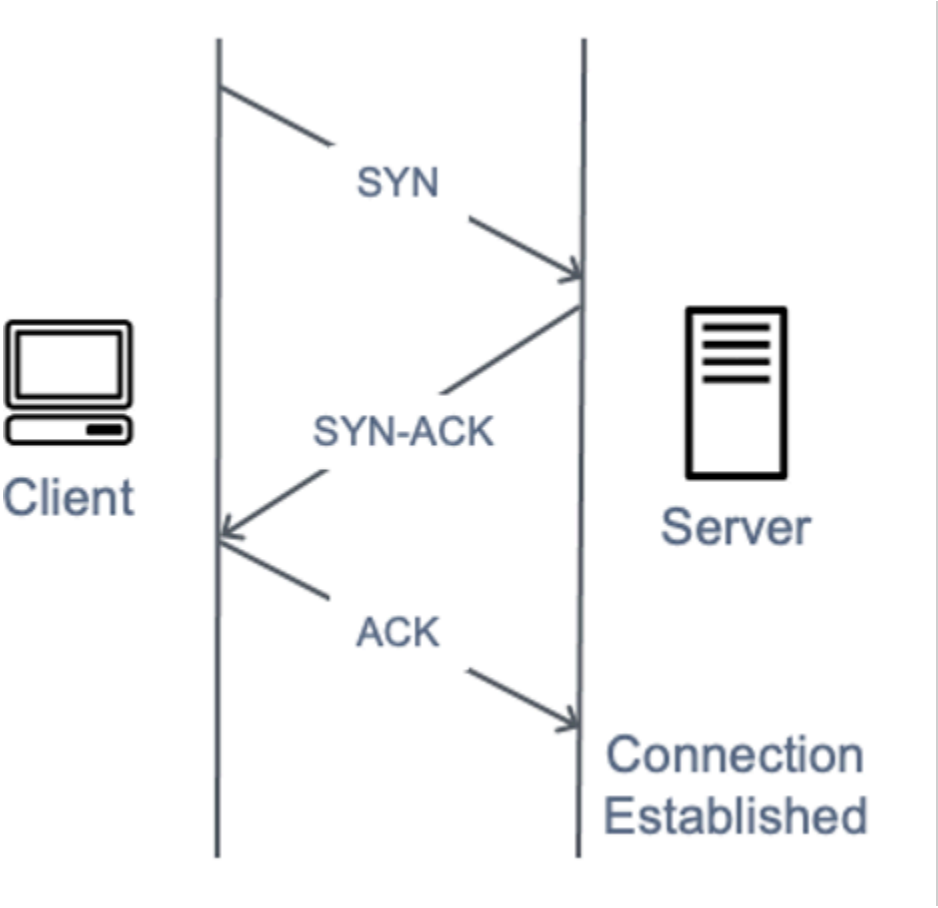


Diagram yang menggambarkan jabat tangan SYN tiga arah

Dalam serangan SYN banjir, klien jahat mengirim sejumlah besar SYN paket, tetapi tidak pernah mengirim ACK paket akhir untuk menyelesaikan jabat tangan. Server dibiarkan menunggu respons terhadap TCP koneksi setengah terbuka dan idenya adalah bahwa target akhirnya kehabisan kapasitas untuk menerima TCP koneksi baru yang mencegah pengguna baru terhubung ke server, namun dampak sebenarnya lebih bernuansa. Sistem operasi modern semuanya menerapkan SYN cookie secara default sebagai mekanisme untuk melawan kelelahan tabel status dari serangan SYN banjir. Setelah panjang SYN antrian mencapai ambang batas yang telah ditentukan sebelumnya, server merespons dengan SYN - ACK berisi nomor urut awal yang dibuat, tanpa membuat entri dalam antreannya. SYN Jika server kemudian menerima nomor pengakuan ACK yang ditambahkan dengan benar, server dapat menambahkan entri ke tabel statusnya dan melanjutkan seperti biasa. Dampak sebenarnya dari SYN banjir pada perangkat target cenderung kapasitas jaringan dan CPU kelelahan, namun perangkat stateful menengah seperti firewall (atau pelacakan koneksi grup EC2 keamanan) dapat mengalami kelelahan tabel TCP status dan menjatuhkan koneksi baru.

TCPrefleksi middlebox

Vektor serangan yang relatif baru ini pertama kali diungkapkan dalam whitepaper akademis pada Agustus 2021 yang menjelaskan bagaimana TCP ketidakpatuhan di firewall negara-bangsa dan yang tersedia secara komersial dapat mengakibatkan ini ditipu menjadi vektor amplifikasi. TCP Kami telah melihat serangan ini “di alam liar” sejak awal 2022 dan terus melihatnya hari ini. Faktor amplifikasi bervariasi karena cara yang berbeda di mana vendor telah menerapkan “fitur” ini, tetapi dapat melebihi amplifikasi Memcached. UDP

Serangan lapisan aplikasi

Seorang penyerang dapat menargetkan aplikasi itu sendiri dengan menggunakan lapisan 7 atau serangan lapisan aplikasi. Dalam serangan ini, mirip dengan serangan infrastruktur SYN banjir, penyerang mencoba membebani fungsi spesifik aplikasi untuk membuat aplikasi tidak tersedia atau tidak responsif terhadap pengguna yang sah. Terkadang ini dapat dicapai dengan volume permintaan yang sangat rendah yang hanya menghasilkan volume kecil lalu lintas jaringan. Hal ini dapat membuat serangan sulit untuk dideteksi dan dikurangi. Contoh serangan lapisan aplikasi termasuk HTTP banjir, serangan penghilang cache, dan - banjir. WordPress XML RPC

- Dalam serangan HTTP banjir, penyerang mengirimkan HTTP permintaan yang tampaknya berasal dari pengguna aplikasi web yang valid. Beberapa HTTP banjir menargetkan sumber daya tertentu, sementara HTTP banjir yang lebih kompleks mencoba meniru interaksi manusia dengan aplikasi tersebut. Hal ini dapat meningkatkan kesulitan menggunakan teknik mitigasi umum seperti pembatasan tingkat permintaan.
- Serangan cache-busting adalah jenis HTTP banjir yang menggunakan variasi dalam string kueri untuk menghindari caching jaringan pengiriman konten (). CDN Alih-alih dapat mengembalikan hasil cache, CDN harus menghubungi server asal untuk setiap permintaan halaman, dan pengambilan asal ini menyebabkan ketegangan tambahan pada server web aplikasi.
- Dengan serangan RPC banjir, juga dikenal sebagai banjir WordPress pingback, penyerang menargetkan situs web yang dihosting pada perangkat lunak manajemen WordPress konten. WordPress XML Penyerang menyalahgunakan RPC API fungsi XML- untuk menghasilkan banjir permintaan. HTTP Fitur pingback memungkinkan situs web yang dihosting di WordPress (Situs A) untuk memberi tahu WordPress situs yang berbeda (Situs B) melalui tautan yang telah dibuat Situs A ke Situs B. Situs B kemudian mencoba mengambil Situs A untuk memverifikasi keberadaan tautan. Dalam banjir pingback, penyerang menyalahgunakan kemampuan ini untuk menyebabkan Situs B menyerang Situs A. Jenis serangan ini memiliki tanda tangan yang jelas: "`WordPress:`" biasanya ada di User-Agent dari header permintaan. HTTP

Ada bentuk lain dari lalu lintas berbahaya yang dapat memengaruhi ketersediaan aplikasi. Scraper bot mengotomatiskan upaya untuk mengakses aplikasi web untuk mencuri konten atau merekam informasi kompetitif, seperti harga. Serangan brute force dan credential stuffing adalah upaya terprogram untuk mendapatkan akses tidak sah ke area aman aplikasi. Ini bukan DDoS serangan ketat, tetapi sifat otomatisnya dapat terlihat mirip dengan DDoS serangan dan mereka dapat dikurangi dengan menerapkan beberapa praktik terbaik yang sama untuk dibahas dalam paper ini.

Serangan lapisan aplikasi juga dapat menargetkan layanan Domain Name System (DNS). Yang paling umum dari serangan ini adalah banjir DNS kueri di mana penyerang menggunakan banyak DNS kueri yang terbentuk dengan baik untuk menghabiskan sumber daya server. DNS Serangan ini juga dapat mencakup komponen cache-busting di mana penyerang mengacak string subdomain untuk melewati cache lokal dari resolver yang diberikan. DNS Akibatnya, resolver tidak dapat memanfaatkan kueri domain cache dan sebaliknya harus berulang kali menghubungi DNS server otoritatif, yang memperkuat serangan.

Jika aplikasi web dikirimkan melalui Transport Layer Security (TLS), penyerang juga dapat memilih untuk menyerang TLS proses negosiasi. TLSmahal secara komputasi sehingga penyerang, dengan menghasilkan beban kerja tambahan di server untuk memproses data yang tidak dapat dibaca (atau tidak dapat dipahami (ciphertext)) sebagai jabat tangan yang sah, dapat mengurangi ketersediaan server. Dalam variasi serangan ini, penyerang menyelesaikan TLS jabat tangan tetapi terus-menerus menegosiasikan kembali metode enkripsi. Seorang penyerang dapat mencoba untuk menghabiskan sumber daya server dengan membuka dan menutup banyak TLS sesi.

Teknik mitigasi

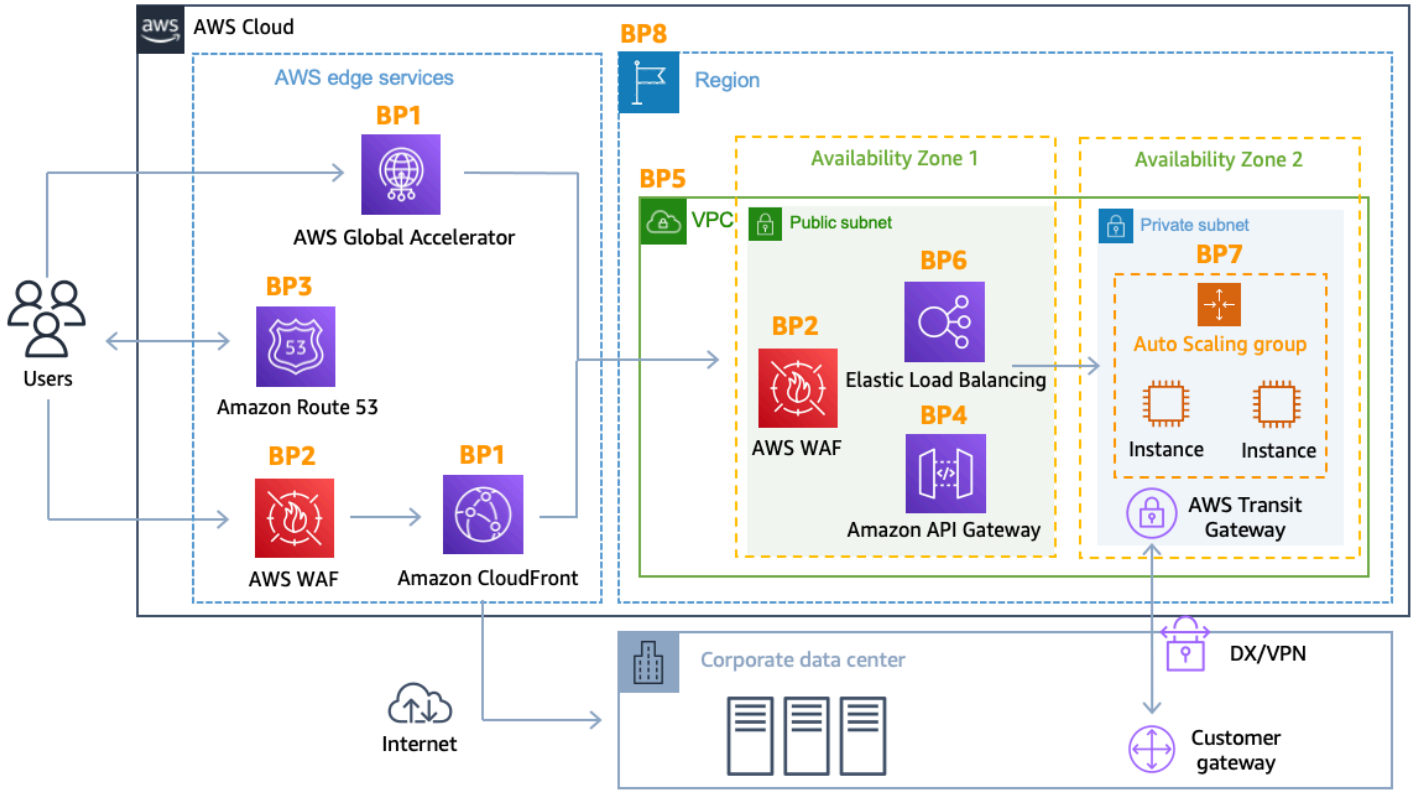
Beberapa bentuk DDoS mitigasi disertakan secara otomatis dengan AWS layanan. DDoSketahanan dapat ditingkatkan lebih lanjut dengan menggunakan AWS arsitektur dengan layanan tertentu, yang tercakup dalam bagian berikut, dan dengan menerapkan praktik terbaik tambahan untuk setiap bagian dari aliran jaringan antara pengguna dan aplikasi Anda.

Anda dapat menggunakan AWS layanan yang beroperasi dari lokasi edge, seperti Amazon CloudFront, AWS Global Accelerator, dan Amazon Route 53 untuk membangun perlindungan ketersediaan komprehensif terhadap semua serangan lapisan infrastruktur yang diketahui. Layanan ini merupakan bagian dari AWS Global Edge Network, dan dapat meningkatkan DDoS ketahanan aplikasi Anda saat melayani semua jenis lalu lintas aplikasi dari lokasi tepi yang didistribusikan di seluruh dunia. Anda dapat menjalankan aplikasi Anda di mana pun Wilayah AWS, dan menggunakan layanan ini untuk melindungi ketersediaan aplikasi Anda dan mengoptimalkan kinerja aplikasi Anda untuk pengguna akhir yang sah.

Manfaat menggunakan Amazon CloudFront, Global Accelerator, dan Amazon Route 53 meliputi:

- Akses ke internet dan kapasitas DDoS mitigasi di seluruh AWS Global Edge Network. Ini berguna dalam mengurangi serangan volumetrik yang lebih besar, yang dapat mencapai skala terabit.
- AWS Shield DDoSSistem mitigasi terintegrasi dengan layanan AWS edge, mengurangi time-to-mitigate dari menit ke sub detik.
- Mitigasi Stateless SYN Flood memverifikasi koneksi masuk menggunakan SYN cookie sebelum meneruskannya ke layanan yang dilindungi. Ini memastikan bahwa hanya koneksi yang valid yang mencapai aplikasi Anda sekaligus melindungi pengguna akhir yang sah dari penurunan positif palsu.
- Sistem rekayasa lalu lintas otomatis yang membubarkan atau mengisolasi dampak serangan volumetrik DDoS besar. Semua layanan ini mengisolasi serangan pada sumber sebelum mencapai asal Anda, yang berarti lebih sedikit dampak pada sistem yang dilindungi oleh layanan ini.
- Pertahanan lapisan aplikasi untuk CloudFront bila digabungkan dengan AWS WAFitu tidak memerlukan perubahan arsitektur aplikasi saat ini (misalnya, di pusat data Wilayah AWS atau lokal).

Tidak ada biaya untuk transfer data masuk AWS dan Anda tidak membayar untuk lalu lintas DDoS serangan yang dikurangi oleh. AWS Shield Diagram arsitektur berikut mencakup layanan AWS Global Edge Network.



DDoS-arsitektur referensi tangguh

Arsitektur ini mencakup beberapa AWS layanan yang dapat membantu Anda meningkatkan ketahanan aplikasi web Anda terhadap seranganDDoS. Tabel berikut memberikan ringkasan layanan ini dan kemampuan yang dapat mereka berikan. AWS telah menandai setiap layanan dengan indikator praktik terbaik (BP1,BP2) untuk referensi yang lebih mudah dalam dokumen ini. Misalnya, bagian yang akan datang membahas kemampuan yang disediakan oleh Amazon CloudFront dan Global Accelerator yang mencakup indikator praktik terbaik. BP1

Tabel 2 - Ringkasan praktik terbaik

	AWS Tepi			Wilayah AWS		
	Menggunakan Amazon CloudFront (BP1) dengan	Menggunakan Global Accelerator () BP1	Menggunakan Amazon Route 53 (BP3)	Menggunakan Elastic Load Balancing (BP6) dengan	Menggunakan grup keamanan dan jaringan ACLs di	Menggunakan Auto BP7 Scaling Amazon Elastic

	AWS Tepi			Wilayah AWS		
	AWS WAF (BP2)			AWS WAF () BP2	Amazon VPC (BP5)	Compute Cloud (AmazonEC2) ()
Lapisan 3 (misalnya, UDP refleksi) mitigasi serangan	✓	✓	✓	✓	✓	✓
Layer 4 (misalnya, SYN banjir) mitigasi serangan	✓	✓	✓	✓		
Layer 6 (misalnya ,TLS) mitigasi serangan	✓	✓	✓	✓		
Kurangi permukaan serangan	✓	✓	✓	✓	✓	
Skala untuk menyerap lalu lintas lapisan aplikasi	✓	✓	✓	✓	✓	✓

	AWS Tepi			Wilayah AWS		
Lapisan 7 (lapisan aplikasi) mitigasi serangan	✓	✓(*)	✓	✓	✓(*)	✓(*)
Isolasi geografis dan penyebaran lalu lintas berlebih dan serangan yang lebih besar DDoS	✓	✓	✓			

✓ (*): Jika digunakan AWS WAF dengan Application Load Balancer

Cara lain untuk meningkatkan kesiapan Anda untuk merespons dan mengurangi DDoS serangan adalah dengan berlangganan. AWS Shield Advanced Manfaat menggunakan AWS Shield Advanced meliputi:

- Akses ke dukungan khusus 24x7 dari Tim AWS Shield Response (AWS SRT) untuk bantuan dalam mengurangi DDoS serangan yang memengaruhi ketersediaan aplikasi, termasuk fitur keterlibatan Proaktif opsional
- Ambang deteksi sensitif yang mengarahkan lalu lintas ke sistem DDoS mitigasi lebih awal dan dapat meningkatkan serangan time-to-mitigate terhadap Amazon EC2 (termasuk Load Balancer elastis) atau Network Load Balancer, saat digunakan dengan alamat IP Elastis
- Deteksi Layer 7 yang disesuaikan berdasarkan pola lalu lintas dasar aplikasi Anda saat digunakan AWS WAF
- DDoSMitigasi lapisan aplikasi otomatis di mana Shield Advanced merespons DDoS serangan yang terdeteksi dengan membuat, mengevaluasi, dan menerapkan aturan khusus AWS WAF

- Akses tanpa AWS WAF biaya tambahan untuk mitigasi DDoS serangan lapisan aplikasi (bila digunakan dengan Amazon CloudFront atau Application Load Balancer)
- Manajemen kebijakan keamanan terpusat tanpa AWS Firewall Managerbiaya tambahan.
- Perlindungan biaya yang memungkinkan Anda untuk meminta pengembalian dana terbatas dari biaya terkait penskalaan yang dihasilkan dari serangan. DDoS
- Perjanjian tingkat layanan yang ditingkatkan yang khusus untuk AWS Shield Advanced pelanggan.
- Grup perlindungan yang memungkinkan Anda menggabungkan sumber daya, menyediakan cara swalayan untuk menyesuaikan ruang lingkup deteksi dan mitigasi aplikasi Anda dengan memperlakukan beberapa sumber daya sebagai satu unit. Untuk informasi tentang grup perlindungan, lihat grup perlindungan Shield Advanced.
- DDoSmenyerang visibilitas dengan menggunakan CloudWatch metrik AWS Management ConsoleAPI,, dan alarm Amazon.

Layanan DDoS mitigasi opsional ini membantu melindungi aplikasi yang dihosting di mana pun. Wilayah AWS Layanan ini tersedia secara global untuk CloudFront, Route 53, dan Global Accelerator. Secara regional, Anda dapat melindungi Application Load Balancer, Classic Load Balancer, dan alamat IP Elastis yang memungkinkan Anda melindungi Network Load Balancer () atau instans NLBs Amazon. EC2

Untuk daftar lengkap AWS Shield Advanced fitur dan untuk informasi lebih lanjut tentang AWS Shield, lihat Cara AWS Shield kerja.

Praktik terbaik untuk DDoS mitigasi

Pada bagian berikut, masing-masing praktik terbaik yang direkomendasikan untuk DDoS mitigasi dijelaskan secara lebih mendalam. Untuk easy-to-implement panduan singkat tentang membangun lapisan DDoS mitigasi untuk aplikasi web statis atau dinamis, lihat Cara Membantu Melindungi Aplikasi Web Dinamis Terhadap DDoS Serangan dengan Menggunakan Amazon dan CloudFront Amazon Route 53.

Pertahanan lapisan infrastruktur (BP1,BP3,BP6,BP7)

Dalam lingkungan pusat data tradisional, Anda dapat mengurangi DDoS serangan lapisan infrastruktur dengan menggunakan teknik seperti kapasitas penyediaan berlebihan, menerapkan sistem mitigasi, atau menggosok lalu lintas dengan bantuan DDoS layanan mitigasi. DDoS Pada AWS, kemampuan DDoS mitigasi disediakan secara otomatis; tetapi Anda dapat mengoptimalkan

DDoS ketahanan aplikasi Anda dengan membuat pilihan arsitektur yang paling memanfaatkan kemampuan tersebut dan juga memungkinkan Anda untuk menskalakan lalu lintas berlebih.

Pertimbangan utama untuk membantu mengurangi DDoS serangan volumetrik termasuk memastikan bahwa kapasitas transit dan keragaman yang cukup tersedia dan melindungi sumber daya AWS , seperti EC2 contoh Amazon, terhadap lalu lintas serangan.

Beberapa jenis EC2 instans Amazon mendukung fitur yang dapat lebih mudah menangani volume lalu lintas yang besar, misalnya, antarmuka bandwidth jaringan hingga 100 Gbps dan jaringan yang disempurnakan. Ini membantu mencegah kemacetan antarmuka untuk lalu lintas yang telah mencapai instans AmazonEC2. Instans yang mendukung peningkatan jaringan memberikan kinerja input/output (I/O) yang lebih tinggi, bandwidth yang lebih tinggi, dan CPU pemanfaatan yang lebih rendah dibandingkan dengan implementasi tradisional. Ini meningkatkan kemampuan instance untuk menangani volume lalu lintas yang besar dan pada akhirnya membuat mereka sangat tangguh terhadap beban paket per detik (pps).

Untuk memungkinkan tingkat ketahanan yang tinggi ini, AWS rekomendasikan untuk menggunakan Instans EC2Khusus Amazon, atau instans Amazon dengan throughput jaringan lebih tinggi yang memiliki akhiran “N” dan dukungan untuk Jaringan yang Ditingkatkan dengan bandwidth Jaringan hingga 100 Gbps, misalnya, `c6gn.16xlarge` dan `c5n.18xlarge` atau EC2 instans logam (seperti). `c5n.metal`

Untuk informasi selengkapnya tentang EC2 instans Amazon yang mendukung 100 antarmuka jaringan Gigabit dan jaringan yang disempurnakan, lihat Jenis Instans Amazon EC2.

Modul yang diperlukan untuk jaringan yang disempurnakan dan set `enaSupport` atribut yang diperlukan disertakan dengan Amazon Linux 2 dan versi terbaru dari Amazon LinuxAMI. Oleh karena itu, jika Anda meluncurkan instance dengan perangkat keras virtual machine (HVM) versi Amazon Linux pada jenis instans yang didukung, jaringan yang disempurnakan sudah diaktifkan untuk instans Anda. Untuk informasi lebih lanjut, lihat Uji apakah jaringan yang disempurnakan diaktifkan dan Jaringan yang disempurnakan di Linux.

Amazon EC2 dengan Auto Scaling () BP7

Cara lain untuk mengurangi serangan infrastruktur dan lapisan aplikasi adalah dengan beroperasi dalam skala besar. Jika Anda memiliki aplikasi web, Anda dapat menggunakan penyeimbang beban untuk mendistribusikan lalu lintas ke sejumlah EC2 instans Amazon yang dilebih-lebihkan atau dikonfigurasi untuk menskalakan secara otomatis. Contoh ini dapat menangani lonjakan lalu lintas mendadak yang terjadi karena alasan apa pun, termasuk kerumunan flash atau serangan lapisan

DDoS aplikasi. Anda dapat menyetel CloudWatch alarm Amazon untuk memulai Auto Scaling agar secara otomatis menskalakan ukuran armada EC2 Amazon Anda sebagai respons terhadap peristiwa yang Anda tentukan, CPU seperti, I/O JaringanRAM, dan bahkan metrik khusus.

Pendekatan ini melindungi ketersediaan aplikasi ketika ada peningkatan volume permintaan yang tidak terduga. Saat menggunakan Amazon CloudFront, Application Load Balancer, Classic Load Balancer, atau Network Load Balancer dengan aplikasi Anda, TLS negosiasi ditangani oleh distribusi (Amazon) atau oleh penyeimbang beban. CloudFront Fitur-fitur ini membantu melindungi instans Anda agar tidak terkena dampak serangan TLS berbasis dengan penskalaan untuk menangani permintaan yang sah dan TLS serangan penyalahgunaan.

Untuk informasi selengkapnya tentang penggunaan Amazon CloudWatch untuk menjalankan Auto Scaling, lihat Memantau metrik CloudWatch Amazon untuk grup dan instans Auto Scaling Anda.

Amazon EC2 menyediakan kapasitas komputasi yang dapat diubah ukurannya sehingga Anda dapat dengan cepat meningkatkan atau menurunkan saat persyaratan berubah. Anda dapat menskalakan secara horizontal dengan menambahkan instance ke aplikasi secara otomatis dengan menskalakan ukuran grup EC2 Auto Scaling Amazon, dan Anda dapat menskalakan secara vertikal menggunakan jenis instans yang lebih besar. EC2

Dengan menggunakan Amazon RDS Proxy, Anda dapat mengizinkan aplikasi Anda untuk mengumpulkan dan berbagi koneksi database untuk meningkatkan kemampuan mereka dalam skala dan menangani lonjakan tak terduga dalam lalu lintas database. Anda juga dapat mengaktifkan auto-scaling penyimpanan untuk instans database AmazonRDS. Lihat Mengelola kapasitas secara otomatis dengan penskalaan otomatis RDS penyimpanan Amazon untuk informasi selengkapnya.

Elastic Load Balancing () BP6

DDoSSerangan besar dapat membanjiri kapasitas satu EC2 instans Amazon. Dengan Elastic Load Balancing (ELB), Anda dapat mengurangi risiko kelebihan beban aplikasi dengan mendistribusikan lalu lintas di banyak instance backend. Elastic Load Balancing dapat menskalakan secara otomatis, memungkinkan Anda untuk mengelola volume yang lebih besar ketika Anda memiliki lalu lintas ekstra yang tidak terduga, misalnya, karena kerumunan flash atau serangan. DDoS Untuk aplikasi yang dibangun di AmazonVPC, ada tiga jenis yang ELBs perlu dipertimbangkan, tergantung pada jenis aplikasi Anda: Application Load Balancer (ALB), Network Load Balancer () dan Classic Load Balancer NLB (). CLB

Untuk aplikasi web, Anda dapat menggunakan Application Load Balancer untuk merutekan lalu lintas berdasarkan konten dan hanya menerima permintaan web yang terbentuk dengan baik.

Application Load Balancer memblokir banyak DDoS serangan umum, seperti SYN banjir atau serangan UDP refleksi, melindungi aplikasi Anda dari serangan. Application Load Balancer secara otomatis menskalakan untuk menyerap lalu lintas tambahan ketika jenis serangan ini terdeteksi. Aktivitas penskalaan akibat serangan lapisan infrastruktur transparan bagi AWS pelanggan dan tidak memengaruhi tagihan Anda.

Untuk informasi lebih lanjut tentang melindungi aplikasi web dengan Application Load Balancer, lihat Memulai dengan Application Load Balancers.

Untuk HTTPS aplikasi HTTP non-/, Anda dapat menggunakan Network Load Balancer untuk merutekan lalu lintas ke target (misalnya, EC2 instans Amazon) pada latensi sangat rendah. Salah satu pertimbangan utama dengan Network Load Balancer adalah bahwa setiap TCP SYN atau UDP lalu lintas yang mencapai penyeimbang beban pada pendengar yang valid akan diarahkan ke target Anda, tidak diserap, namun ini tidak berlaku untuk TLS -listeners yang mengakhiri koneksi. TCP Untuk Network Load Balancers dengan TCP pendengar, kami sarankan untuk menggunakan Global Accelerator untuk melindungi dari banjir. SYN

Anda dapat menggunakan Shield Advanced untuk mengonfigurasi DDoS perlindungan untuk alamat IP Elastis. Jika alamat IP Elastis ditetapkan per Availability Zone ke Network Load Balancer, Shield Advanced akan menerapkan DDoS perlindungan yang relevan untuk lalu lintas Network Load Balancer.

Untuk informasi selengkapnya tentang perlindungan TCP dan UDP aplikasi dengan Network Load Balancer, lihat Memulai dengan Network Load Balancer.

> **Note**
>
> Bergantung pada konfigurasi grup keamanan, diperlukan sumber daya yang menggunakan keamanan untuk mengelompokkan untuk menggunakan pelacakan koneksi untuk melacak informasi tentang lalu lintas, ini dapat memengaruhi kemampuan penyeimbang beban untuk memproses koneksi baru, karena jumlah koneksi yang dilacak terbatas.
> Konfigurasi grup keamanan yang berisi aturan masuk yang menerima lalu lintas dari alamat IP apa pun (misalnya, `0.0.0.0/0` atau`::/0`) tetapi tidak memiliki aturan yang sesuai untuk mengizinkan lalu lintas respons, menyebabkan grup keamanan menggunakan informasi pelacakan koneksi untuk memungkinkan lalu lintas respons dikirim. Jika terjadi DDoS serangan, jumlah maksimum koneksi yang dilacak dapat habis. Untuk meningkatkan DDoS ketahanan Application Load Balancer atau Classic Load Balancer yang menghadap publik, pastikan bahwa grup keamanan yang terkait dengan penyeimbang beban Anda dikonfigurasi

untuk tidak menggunakan pelacakan koneksi (koneksi yang tidak dilacak), sehingga arus lalu lintas tidak tunduk pada batas pelacakan koneksi.
Untuk ini, konfigurasikan grup keamanan Anda dengan aturan yang memungkinkan aturan masuk untuk menerima TCP aliran dari alamat IP apa pun (`0.0.0.0/0`atau`::/0`), dan tambahkan aturan yang sesuai ke arah keluar yang memungkinkan sumber daya ini mengirim lalu lintas respons (izinkan rentang keluar untuk alamat IP apa pun `0.0.0.0/0` atau`::/0`) untuk semua port (0-65535), sehingga lalu lintas respons diizinkan berdasarkan aturan grup keamanan, dan bukan pada informasi pelacakan. Dengan konfigurasi ini, Classic dan Application Load Balancer tidak tunduk pada batas pelacakan koneksi knalpot yang dapat memengaruhi pembuatan koneksi baru ke node penyeimbang beban, dan memungkinkannya untuk menskalakan berdasarkan peningkatan lalu lintas jika terjadi serangan. DDoS Informasi lebih lanjut tentang koneksi yang tidak dilacak dapat ditemukan di: Pelacakan koneksi grup keamanan: Koneksi tidak terlacak.
Menghindari pelacakan koneksi grup keamanan hanya membantu dalam kasus di mana DDoS lalu lintas berasal dari sumber yang diizinkan oleh grup keamanan — DDoS lalu lintas dari sumber yang tidak diizinkan dalam grup keamanan tidak memengaruhi pelacakan koneksi. Konfigurasi ulang grup keamanan Anda untuk menghindari pelacakan koneksi tidak diperlukan dalam kasus ini, misalnya, jika daftar izin grup keamanan Anda terdiri dari rentang IP yang dengannya Anda memiliki tingkat kepercayaan yang tinggi, seperti firewall perusahaan perusahaan atau jalan keluar tepercaya atauVPN. IPs CDNs

Gunakan lokasi AWS Edge untuk skala (BP1,BP3)

Akses ke koneksi internet yang berskala tinggi dan beragam dapat secara signifikan meningkatkan kemampuan Anda untuk mengoptimalkan latensi dan throughput kepada pengguna, untuk menyerap DDoS serangan, dan untuk mengisolasi kesalahan sekaligus meminimalkan dampak pada ketersediaan aplikasi Anda. AWS Lokasi edge menyediakan lapisan tambahan infrastruktur jaringan yang memberikan manfaat ini untuk aplikasi web apa pun yang menggunakan Amazon CloudFront, Global Accelerator, dan Amazon Route 53. Dengan layanan ini, Anda dapat secara komprehensif melindungi di tepi aplikasi Anda berjalan dari Wilayah AWS.

Pengiriman aplikasi web di tepi (BP1)

Amazon CloudFront adalah layanan yang dapat digunakan untuk mengirimkan seluruh situs web Anda termasuk konten statis, dinamis, streaming, dan interaktif. Koneksi persisten dan pengaturan variabel time-to-live (TTL) dapat digunakan untuk menurunkan lalu lintas dari asal Anda, bahkan jika

Anda tidak menyajikan konten yang dapat di-cache. Penggunaan CloudFront fitur-fitur ini mengurangi jumlah permintaan dan TCP koneksi kembali ke asal Anda, membantu melindungi aplikasi web Anda dari HTTP banjir.

CloudFront hanya menerima koneksi yang terbentuk dengan baik, yang membantu mencegah banyak DDoS serangan umum, seperti SYN banjir dan serangan UDP refleksi, mencapai asal Anda. DDoSSerangan juga secara geografis terisolasi dekat dengan sumbernya, yang mencegah lalu lintas berdampak pada lokasi lain. Kemampuan ini dapat sangat meningkatkan kemampuan Anda untuk terus melayani lalu lintas ke pengguna selama DDoS serangan besar. Anda dapat menggunakan CloudFront untuk melindungi asal di AWS atau di tempat lain di internet.

Jika Anda menggunakan Amazon Simple Storage Service (Amazon S3) untuk menyajikan konten statis di internet, AWS sarankan Anda menggunakan Amazon CloudFront untuk melindungi bucket Anda dengan memberikan manfaat berikut:

- Membatasi akses ke bucket Amazon S3 sehingga tidak dapat diakses publik.
- Memastikan bahwa pemirsa (pengguna) dapat mengakses konten di bucket hanya melalui CloudFront distribusi yang ditentukan—yaitu, mencegah mereka mengakses konten langsung dari bucket, atau melalui distribusi yang tidak diinginkan. CloudFront

Untuk mencapai hal ini, konfigurasikan CloudFront untuk mengirim permintaan yang diautentikasi ke Amazon S3, dan konfigurasikan Amazon S3 agar hanya mengizinkan akses ke permintaan yang diautentikasi dari. CloudFront CloudFront menyediakan dua cara untuk mengirim permintaan yang diautentikasi ke asal Amazon S3: kontrol akses asal OAC () dan identitas OAI akses asal (). Kami merekomendasikan penggunaan OAC karena mendukung:

- Semua bucket Amazon S3 secara keseluruhan Wilayah AWS, termasuk Wilayah keikutsertaan diluncurkan setelah Desember 2022
- Enkripsi sisi server Amazon S3 dengan (-) AWS KMS SSE KMS
- Permintaan dinamis (`PUT`dan`DELETE`) ke Amazon S3

Untuk informasi selengkapnya tentang OAC danOAI, lihat Membatasi akses ke asal Amazon S3.

Untuk informasi selengkapnya tentang melindungi dan mengoptimalkan kinerja aplikasi web dengan Amazon CloudFront, lihat Memulai dengan Amazon CloudFront.

Lindungi lalu lintas jaringan lebih jauh dari asal Anda menggunakan AWS Global Accelerator () BP1

Global Accelerator adalah layanan jaringan yang meningkatkan ketersediaan dan kinerja lalu lintas pengguna hingga 60%. Ini dilakukan dengan memasukkan lalu lintas di lokasi tepi yang paling dekat dengan pengguna Anda dan mengarutkannya melalui infrastruktur jaringan AWS global ke aplikasi Anda, apakah itu berjalan dalam satu atau beberapa. Wilayah AWS

Rute Akselerator Global TCP dan UDP lalu lintas ke titik akhir optimal berdasarkan kinerja yang paling Wilayah AWS dekat dengan pengguna. Jika ada kegagalan aplikasi, Global Accelerator menyediakan failover ke endpoint terbaik berikutnya dalam waktu 30 detik. Global Accelerator menggunakan kapasitas besar jaringan AWS global dan integrasi dengan Shield, seperti kemampuan SYN proxy stateless yang menantang upaya koneksi baru dan hanya melayani pengguna akhir yang sah, untuk melindungi aplikasi.

Anda dapat menerapkan arsitektur DDoS tangguh yang memberikan banyak manfaat yang sama dengan praktik terbaik Pengiriman Aplikasi Web di Edge, bahkan jika aplikasi Anda menggunakan protokol yang tidak didukung oleh CloudFront atau Anda mengoperasikan aplikasi web yang memerlukan alamat IP statis global.

Misalnya, Anda mungkin memerlukan alamat IP yang dapat ditambahkan pengguna akhir Anda ke daftar izin di firewall mereka dan tidak digunakan oleh AWS pelanggan lain. Dalam skenario ini Anda dapat menggunakan Global Accelerator untuk melindungi aplikasi web yang berjalan pada Application Load Balancer dan dalam hubungannya AWS WAF dengan juga mendeteksi dan mengurangi banjir permintaan lapisan aplikasi web.

Untuk informasi lebih lanjut tentang melindungi dan mengoptimalkan kinerja lalu lintas jaringan menggunakan Global Accelerator, lihat Memulai dengan Global Accelerator.

Resolusi nama domain di tepi (BP3)

Topik

- Menggunakan Route 53 untuk DNS ketersediaan
- Mengkonfigurasi Route 53 untuk perlindungan biaya dari serangan NXDOMAIN

Menggunakan Route 53 untuk DNS ketersediaan

Amazon Route 53 adalah layanan Domain Name System (DNS) yang sangat tersedia dan skalabel yang dapat digunakan untuk mengarahkan lalu lintas ke aplikasi web Anda. Ini mencakup fitur-fitur canggih seperti Arus Lalu Lintas, Pemeriksaan dan Pemantauan Kesehatan, Perutean Berbasis Latensi, dan Geo. DNS Fitur-fitur canggih ini memungkinkan Anda untuk mengontrol bagaimana layanan merespons DNS permintaan untuk meningkatkan kinerja aplikasi web Anda dan untuk menghindari pemadaman situs. Ini adalah satu-satunya AWS layanan yang memiliki ketersediaan pesawat data 100%SLA.

Amazon Route 53 menggunakan teknik seperti shuffle sharding dan anycast striping, yang dapat membantu pengguna mengakses aplikasi Anda bahkan jika DNS layanan ditargetkan oleh serangan. DDoS

Dengan shuffle sharding, setiap server nama dalam kumpulan delegasi Anda sesuai dengan serangkaian lokasi tepi dan jalur internet yang unik. Ini memberikan toleransi kesalahan yang lebih besar dan meminimalkan tumpang tindih antar pelanggan. Jika satu server nama dalam kumpulan delegasi tidak tersedia, pengguna dapat mencoba lagi dan menerima respons dari server nama lain di lokasi tepi yang berbeda.

Anycast striping memungkinkan setiap DNS permintaan dilayani oleh lokasi yang paling optimal, menyebarkan beban jaringan dan mengurangi latensi. DNS Ini memberikan respons yang lebih cepat bagi pengguna. Selain itu, Amazon Route 53 dapat mendeteksi anomali dalam sumber dan volume DNS kueri, dan memprioritaskan permintaan dari pengguna yang diketahui dapat diandalkan.

Untuk informasi selengkapnya tentang menggunakan Amazon Route 53 untuk merutekan pengguna ke aplikasi Anda, lihat Memulai dengan Amazon Route 53.

Mengkonfigurasi Route 53 untuk perlindungan biaya dari serangan **NXDOMAIN**

`NXDOMAIN`Serangan terjadi ketika penyerang mengirim banjir permintaan ke zona host untuk sub-domain yang tidak ada, seringkali melalui resolver “baik” yang dikenal. Tujuan dari serangan ini mungkin untuk mempengaruhi cache resolver rekursif dan/atau ketersediaan resolver otoritatif, atau bisa menjadi bentuk DNS pengintaian untuk mencoba menemukan catatan zona host. Menggunakan Route 53 untuk penyelesai otoritatif Anda mengurangi risiko ketersediaan/dampak kinerja, namun hasilnya dapat berupa peningkatan biaya yang signifikan dalam biaya Rute 53 bulanan. Untuk melindungi dari kenaikan biaya, manfaatkan harga Route 53 di mana DNS kueri gratis jika kedua hal berikut benar:

- Nama domain atau subdomain (`example.com`ataustore.example.com) dan tipe record (`A`) dalam kueri cocok dengan catatan alias.
- Target alias adalah AWS sumber daya selain catatan Route 53 lainnya.

Buat catatan wildcard, misalnya, `*.example.com` dengan tipe `A` (Alias) yang menunjuk ke AWS sumber daya seperti EC2 instance, Elastic Load Balancer CloudFront atau distribusi, sehingga ketika kueri dibuat, IP sumber daya akan dikembalikan dan Anda tidak akan dikenakan biaya `qwerty12345.example.com` untuk kueri.

Pertahanan lapisan aplikasi (BP1,BP2)

Banyak teknik yang dibahas sejauh ini dalam paper ini efektif dalam mengurangi dampak DDoS serangan lapisan infrastruktur terhadap ketersediaan aplikasi Anda. Untuk juga bertahan terhadap serangan lapisan aplikasi, Anda perlu menerapkan arsitektur yang memungkinkan Anda mendeteksi, menskalakan untuk menyerap, dan memblokir permintaan berbahaya secara khusus. Ini merupakan pertimbangan penting karena sistem DDoS mitigasi berbasis jaringan umumnya tidak efektif dalam mengurangi serangan lapisan aplikasi yang kompleks.

Mendeteksi dan memfilter permintaan web berbahaya (BP1,BP2)

Saat aplikasi berjalan AWS, Anda dapat memanfaatkan Amazon CloudFront (dan kemampuan HTTP caching) AWS WAF, dan perlindungan lapisan Shield Advanced Automatic Application untuk membantu mencegah permintaan yang tidak perlu mencapai asal Anda selama DDoS serangan lapisan aplikasi.

Amazon CloudFront

Amazon CloudFront dapat membantu mengurangi beban server dengan mencegah lalu lintas non-web mencapai asal Anda. Untuk mengirim permintaan ke CloudFront aplikasi, koneksi harus dibuat dengan alamat IP yang valid melalui TCP jabat tangan yang lengkap, yang tidak dapat dipalsukan. Selain itu, CloudFront dapat secara otomatis menutup koneksi dari penyerang membaca lambat atau menulis lambat (misalnya, Slowloris).

CDNcaching

CloudFront memungkinkan Anda untuk menyajikan konten dinamis dan konten statis dari lokasi AWS tepi. Dengan menyajikan konten proxy yang dapat CDN di-cache dari cache, Anda mencegah permintaan mencapai asal Anda dari node cache tepi tertentu selama durasi caching. TTL

Sehubungan dengan keruntuhan permintaan untuk konten yang kedaluwarsa tetapi dapat di-cache, bahkan sangat singkat TTL berarti bahwa jumlah permintaan yang dapat diabaikan akan mencapai asal Anda selama banjir permintaan untuk konten tersebut. Selain itu mengaktifkan fitur seperti CloudFront Origin Shield dapat membantu mengurangi beban pada asal Anda — apa pun yang dapat Anda lakukan untuk meningkatkan rasio hit cache dapat berarti perbedaan antara serangan banjir permintaan yang berdampak dan tidak berdampak.

AWS WAF

Dengan menggunakan AWS WAF, Anda dapat mengonfigurasi daftar kontrol akses web (WebACLs) pada CloudFront distribusi global atau sumber daya regional untuk memfilter, memantau, dan memblokir permintaan berdasarkan tanda tangan permintaan. Untuk menentukan apakah akan mengizinkan atau memblokir permintaan, Anda dapat mempertimbangkan faktor-faktor seperti alamat IP atau negara asal, string atau pola tertentu dalam permintaan, ukuran bagian tertentu dari permintaan, dan keberadaan SQL kode atau skrip berbahaya. Anda juga dapat menjalankan CAPTCHA teka-teki dan tantangan sesi klien diam terhadap permintaan.

Keduanya AWS WAF dan CloudFront juga memungkinkan Anda untuk mengatur pembatasan geografis untuk memblokir atau mengizinkan permintaan dari negara yang dipilih. Ini dapat membantu memblokir atau membatasi serangan dari lokasi geografis di mana Anda tidak berharap untuk melayani pengguna. Dengan pernyataan aturan kecocokan geografis berbutir halus AWS WAF, Anda dapat mengontrol akses ke tingkat wilayah.

Anda dapat menggunakan pernyataan Scope-down untuk mempersempit cakupan permintaan yang dievaluasi aturan untuk menghemat biaya dan “label” pada permintaan web untuk mengizinkan aturan yang cocok dengan permintaan untuk mengkomunikasikan hasil kecocokan ke aturan yang dievaluasi nanti di web yang sama. ACL Pilih opsi ini untuk menggunakan kembali logika yang sama di beberapa aturan.

Anda juga dapat menentukan respons kustom lengkap, dengan kode respons, header, dan badan.

Untuk membantu mengidentifikasi permintaan berbahaya, tinjau log server web Anda atau gunakan AWS WAF pencatatan dan pengambilan sampel permintaan.Dengan mengaktifkan AWS WAF pencatatan, Anda mendapatkan informasi terperinci tentang lalu lintas yang dianalisis oleh Web. ACL AWS WAF mendukung penyaringan log, memungkinkan Anda untuk menentukan permintaan web mana yang dicatat dan permintaan mana yang dibuang dari log setelah inspeksi.

Informasi yang direkam dalam log mencakup waktu AWS WAF menerima permintaan dari AWS sumber daya Anda, informasi terperinci tentang permintaan, dan tindakan pencocokan untuk setiap aturan yang diminta.

Permintaan sampel memberikan detail tentang permintaan dalam tiga jam terakhir yang cocok dengan salah satu aturan Anda AWS WAF . Anda dapat menggunakan informasi ini untuk mengidentifikasi tanda tangan lalu lintas yang berpotensi berbahaya dan membuat aturan baru untuk menolak permintaan tersebut. Jika Anda melihat sejumlah permintaan dengan string kueri acak, pastikan untuk mengizinkan hanya parameter string kueri yang relevan dengan cache untuk aplikasi Anda. Teknik ini sangat membantu dalam mengurangi serangan cache busting terhadap asal Anda.

AWS WAF — Aturan berbasis tarif

AWS sangat merekomendasikan perlindungan terhadap banjir HTTP permintaan dengan menggunakan aturan berbasis tarif AWS WAF untuk secara otomatis memblokir alamat IP aktor jahat ketika jumlah permintaan yang diterima dalam jendela geser 5 menit melebihi ambang batas yang Anda tentukan. Alamat IP klien yang menyinggung akan menerima respons terlarang 403 (atau respons kesalahan blok yang dikonfigurasi) dan tetap diblokir hingga tingkat permintaan turun di bawah ambang batas.

Disarankan untuk aturan berbasis tingkat lapisan untuk memberikan perlindungan yang ditingkatkan sehingga Anda memiliki:

- Aturan berbasis tarif selimut untuk melindungi aplikasi Anda dari banjir besarHTTP.
- Satu atau lebih aturan berbasis tarif untuk melindungi spesifik URIs pada tingkat yang lebih ketat daripada aturan berbasis tarif selimut.

Misalnya Anda dapat memilih aturan berbasis tarif selimut (tidak ada pernyataan cakupan turun) dengan batas 500 permintaan dalam periode 5 menit, dan kemudian membuat satu atau lebih aturan berbasis tarif berikut dengan batas lebih rendah dari 500 (serendah 100 permintaan dalam periode 5 menit) menggunakan pernyataan cakupan bawah:

- Lindungi halaman web Anda dengan pernyataan cakupan ke bawah seperti "`if NOT uri_path contains '.'`" sehingga permintaan sumber daya tanpa ekstensi file dilindungi lebih lanjut. Ini juga melindungi homepage Anda (`/`) yang merupakan URI jalur yang sering ditargetkan.
- Lindungi titik akhir dinamis dengan pernyataan cakupan ke bawah seperti "" `if method exactly matches 'post' (convert lowercase)`
- Lindungi permintaan berat yang mencapai database Anda atau memanggil kata sandi satu kali (OTP) dengan cakupan ke bawah seperti "" `if uri_path starts_with '/login' OR uri_path starts_with '/signup' OR uri_path starts_with '/forgotpassword'`

Berbasis tarif dalam mode “Blok” adalah landasan defense-in-depth WAF konfigurasi Anda untuk melindungi dari banjir permintaan dan merupakan persyaratan agar permintaan perlindungan AWS Shield Advanced biaya disetujui. Kami akan memeriksa defense-in-depth WAF konfigurasi tambahan di bagian berikut.

AWS WAF — Reputasi IP

Untuk mencegah serangan berdasarkan reputasi alamat IP, Anda dapat membuat aturan menggunakan pencocokan IP atau menggunakan Aturan Terkelola untuk AWS WAF.

Grup aturan daftar reputasi IP Amazon mencakup aturan berdasarkan intelijen ancaman internal Amazon. Aturan-aturan ini mencari alamat IP yang merupakan bot, melakukan pengintaian terhadap AWS sumber daya, atau secara aktif terlibat dalam aktivitas. DDoS `AWSManagedIPDDoSList`Aturan, telah diamati memblokir lebih dari 90% dari permintaan banjir berbahaya.

Grup aturan daftar IP Anonim berisi aturan untuk memblokir permintaan dari layanan yang memungkinkan pengaburan identitas penampil. Ini termasuk permintaan dariVPNs, proxy, node Tor, dan platform cloud (tidak termasuk AWS).

Selain itu, Anda dapat menggunakan daftar reputasi IP pihak ketiga dengan menggunakan komponen parser Daftar IP dari Otomatisasi Keamanan untuk AWS WAF solusi.

AWS WAF - Mitigasi ancaman cerdas

Botnet adalah ancaman keamanan yang serius dan biasanya digunakan untuk melakukan kegiatan ilegal atau berbahaya seperti mengirim spam, mencuri data sensitif, memulai serangan ransomware, melakukan penipuan iklan melalui klik penipuan, atau meluncurkan serangan terdistribusi (). denial-of-service DDoS Untuk mencegah serangan bot, gunakan grup aturan terkelola AWS WAF Bot Control. Grup aturan ini menyediakan tingkat perlindungan dasar “Umum” yang menambahkan label ke bot pengenal diri, memverifikasi bot yang umumnya diinginkan, dan mendeteksi tanda tangan bot dengan kepercayaan tinggi dan tingkat perlindungan “Ditargetkan” yang menambahkan deteksi untuk bot tingkat lanjut yang tidak mengidentifikasi diri.

Perlindungan yang ditargetkan menggunakan teknik deteksi lanjutan seperti interogasi browser, sidik jari, dan heuristik perilaku untuk mengidentifikasi lalu lintas bot yang buruk dan kemudian menerapkan kontrol mitigasi seperti pembatasan laju dan dan tindakan aturan Tantangan. CAPTCHA Targeted juga menyediakan opsi pembatasan tarif untuk menegakkan pola akses seperti manusia dan menerapkan pembatasan laju dinamis melalui penggunaan token permintaan. Untuk detail

selengkapnya, lihat Grup aturan Kontrol AWS WAF Bot. Untuk mendeteksi dan mengelola upaya pengambilalihan berbahaya pada halaman login aplikasi Anda, Anda dapat menggunakan grup aturan pencegahan pengambilalihan akun Kontrol AWS WAF Penipuan (ATP). Grup aturan melakukan ini dengan memeriksa upaya login yang dikirim klien ke titik akhir login aplikasi Anda dan juga memeriksa respons aplikasi Anda terhadap upaya login, untuk melacak keberhasilan dan tingkat kegagalan.

Penipuan pembuatan akun adalah aktivitas ilegal online di mana penyerang mencoba membuat satu atau lebih akun palsu. Penyerang menggunakan akun palsu untuk kegiatan penipuan seperti menyalahgunakan promosi dan mendaftar bonus, meniru seseorang, dan serangan cyber seperti phishing. Kehadiran akun palsu dapat berdampak negatif pada bisnis Anda dengan merusak reputasi Anda dengan pelanggan dan paparan penipuan keuangan.

Anda dapat memantau dan mengontrol upaya penipuan pembuatan akun dengan menerapkan fitur pencegahan AWS WAF penipuan (ACFP) pembuatan akun Fraud Control. AWS WAF menawarkan fitur ini di grup Peraturan yang Dikelola AWS aturan `AWS ManagedRulesACFPRuleSet` dengan integrasi aplikasi pendampingSDKs.

Pelajari lebih lanjut tentang perlindungan ini dalam AWS WAF mitigasi ancaman cerdas.

Secara otomatis mengurangi DDoS peristiwa lapisan aplikasi (,,) BP1 BP2 BP6

Jika Anda berlangganan AWS Shield Advanced, Anda dapat mengaktifkan DDoSmitigasi lapisan aplikasi otomatis Shield Advanced. Fitur ini secara otomatis membuat, mengevaluasi, dan menerapkan AWS WAF aturan untuk mengurangi DDoS peristiwa layer 7 atas nama Anda.

AWS Shield Advanced menetapkan garis dasar lalu lintas untuk setiap sumber daya yang dilindungi yang terkait dengan Web. WAF ACL Lalu lintas yang secara signifikan menyimpang dari baseline yang ditetapkan ditandai sebagai peristiwa potensial. DDoS Setelah peristiwa terdeteksi, AWS Shield Advanced upaya untuk mengidentifikasi tanda tangan permintaan web yang merupakan peristiwa, dan jika tanda tangan diidentifikasi, AWS WAF aturan dibuat untuk mengurangi lalu lintas dengan tanda tangan itu.

Setelah aturan dievaluasi berdasarkan garis dasar historis dan dianggap aman, aturan tersebut ditambahkan ke grup aturan yang dikelola Shield, dan Anda dapat memilih apakah aturan diterapkan dalam mode hitungan atau blokir. Shield Advanced secara otomatis menghapus AWS WAF aturan setelah ditentukan bahwa suatu peristiwa telah sepenuhnya mereda.

Engage SRT (hanya pelanggan Shield Advanced)

Selain itu, saat berlangganan Shield Advanced, Anda dapat terlibat AWS SRT untuk membantu Anda membuat aturan guna mengurangi serangan yang merusak ketersediaan aplikasi Anda. Anda dapat memberikan akses AWS SRT terbatas ke akun Anda AWS Shield Advanced dan AWS WAF APIs. AWS SRTmengakses ini APIs untuk menempatkan mitigasi pada akun Anda hanya dengan otorisasi eksplisit Anda. Untuk informasi lebih lanjut, lihat Dukungan bagian dokumen ini.

Anda dapat menggunakan AWS Firewall Manager untuk mengonfigurasi dan mengelola aturan keamanan secara terpusat, seperti AWS Shield Advanced perlindungan dan AWS WAF aturan, di seluruh organisasi Anda. Akun AWS Organizations manajemen Anda dapat menunjuk akun administrator, yang diberi wewenang untuk membuat kebijakan Firewall Manager. Kebijakan ini memungkinkan Anda untuk menentukan kriteria, seperti jenis sumber daya dan tag, yang menentukan di mana aturan diterapkan. Ini berguna ketika Anda memiliki banyak akun dan ingin membakukan perlindungan Anda.

Untuk informasi lebih lanjut tentang:

- Peraturan yang Dikelola AWS untuk AWS WAF, lihat Peraturan yang Dikelola AWS untuk AWS WAF.
- Menggunakan pembatasan geografis untuk membatasi akses ke CloudFront distribusi Anda, lihat Membatasi distribusi geografis konten Anda.
- Menggunakan AWS WAF, lihat:
  - Memulai dengan AWS WAF
  - Mencatat informasi ACL lalu lintas web
  - Melihat contoh permintaan web
- Mengkonfigurasi aturan berbasis tarif, lihat Lindungi Situs Web dan Layanan Menggunakan Aturan Berbasis Tarif untuk. AWS WAF
- Cara mengelola penerapan aturan di seluruh AWS sumber daya Anda dengan Firewall Manager, lihat:
  - Memulai dengan AWS WAF kebijakan Firewall Manager.
  - Memulai kebijakan Firewall Manager Shield Advanced.

Serang pengurangan permukaan

Pertimbangan penting lainnya ketika merancang AWS solusi adalah membatasi peluang penyerang untuk menargetkan aplikasi Anda. Konsep ini dikenal sebagai pengurangan permukaan serangan. Sumber daya yang tidak terpapar ke internet lebih sulit diserang, yang membatasi opsi yang dimiliki penyerang untuk menargetkan ketersediaan aplikasi Anda.

Misalnya, jika Anda tidak mengharapkan pengguna untuk berinteraksi langsung dengan sumber daya tertentu, pastikan bahwa sumber daya tersebut tidak dapat diakses dari internet. Demikian pula, jangan menerima lalu lintas dari pengguna atau aplikasi eksternal pada port atau protokol yang tidak diperlukan untuk komunikasi.

Di bagian berikut, AWS berikan praktik terbaik untuk memandu Anda dalam mengurangi permukaan serangan dan membatasi eksposur internet aplikasi Anda.

Mengaburkan AWS sumber daya (,,) BP1 BP4 BP5

Biasanya, pengguna dapat dengan cepat dan mudah menggunakan aplikasi tanpa mengharuskan AWS sumber daya sepenuhnya terpapar ke internet.

Grup keamanan dan jaringan ACLs (BP5)

Amazon Virtual Private Cloud (AmazonVPC) memungkinkan Anda untuk menyediakan bagian yang terisolasi secara logis AWS Cloud di mana Anda dapat meluncurkan AWS sumber daya di jaringan virtual yang Anda tentukan.

Grup keamanan dan jaringan ACLs serupa karena memungkinkan Anda mengontrol akses ke AWS sumber daya di dalam AndaVPC. Tetapi grup keamanan memungkinkan Anda untuk mengontrol lalu lintas masuk dan keluar pada tingkat instans, sementara jaringan ACLs menawarkan kemampuan serupa di tingkat VPC subnet. Tidak ada biaya tambahan untuk menggunakan grup keamanan atau jaringanACLs.

Anda dapat memilih apakah akan menentukan grup keamanan saat meluncurkan instance atau mengaitkan instance dengan grup keamanan di lain waktu. Semua lalu lintas internet ke grup keamanan secara implisit ditolak kecuali Anda membuat aturan izin untuk mengizinkan lalu lintas.

Misalnya, jika Anda memiliki EC2 instans Amazon di belakang Elastic Load Balancer, instans itu sendiri tidak perlu diakses publik dan hanya bersifat pribadi. IPs Sebagai gantinya, Anda dapat memberikan akses Elastic Load Balancer ke port pendengar target yang diperlukan menggunakan

aturan Grup Keamanan yang memungkinkan akses ke 0.0.0.0/0 (untuk menghindari masalah pelacakan koneksi — lihat catatan di bawah) bersamaan dengan Daftar Kontrol Akses Jaringan (NACL) pada subnet grup target untuk mengizinkan hanya rentang IP Elastic Load Balancing untuk berkomunikasi dengan instance. Ini memastikan bahwa lalu lintas internet tidak dapat berkomunikasi secara langsung dengan EC2 instans Amazon Anda, yang membuatnya lebih sulit bagi penyerang untuk mempelajari dan memengaruhi aplikasi Anda.

Saat Anda membuat jaringanACLs, Anda dapat menentukan aturan izinkan dan tolak. Ini berguna jika Anda ingin secara eksplisit menolak jenis lalu lintas tertentu ke aplikasi Anda. Misalnya, Anda dapat menentukan alamat IP (sebagai CIDR rentang), protokol, dan port tujuan yang ditolak akses ke seluruh subnet. Jika aplikasi Anda hanya digunakan untuk TCP lalu lintas, Anda dapat membuat aturan untuk menolak semua UDP lalu lintas, atau sebaliknya. Opsi ini berguna saat merespons DDoS serangan karena memungkinkan Anda membuat aturan sendiri untuk mengurangi serangan ketika Anda mengetahui sumber IPs atau tanda tangan lainnya.

Jika Anda berlangganan AWS Shield Advanced, Anda dapat mendaftarkan alamat IP Elastis sebagai sumber daya yang dilindungi. DDoSserangan terhadap alamat IP Elastic yang telah terdaftar sebagai sumber daya yang dilindungi terdeteksi lebih cepat, yang dapat menghasilkan waktu yang lebih cepat untuk mengurangi. Ketika serangan terdeteksi, sistem DDoS mitigasi membaca jaringan ACL yang sesuai dengan alamat IP Elastis yang ditargetkan dan menegakkannya di perbatasan AWS jaringan, bukan di tingkat subnet. Ini secara signifikan mengurangi risiko dampak dari sejumlah DDoS serangan lapisan infrastruktur.

Untuk informasi selengkapnya tentang mengonfigurasi grup keamanan dan jaringan ACLs untuk mengoptimalkan DDoS ketahanan, lihat Cara Membantu Mempersiapkan DDoS Serangan dengan Mengurangi Permukaan Serangan Anda.

Untuk informasi selengkapnya tentang penggunaan Shield Advanced dengan alamat IP Elastic sebagai sumber daya yang dilindungi, lihat langkah-langkah untuk Berlangganan AWS Shield Advanced.

Melindungi asal Anda (BP1,BP5)

Jika Anda menggunakan Amazon CloudFront dengan asal yang ada di dalam AndaVPC, Anda mungkin ingin memastikan bahwa hanya CloudFront distribusi Anda yang dapat meneruskan permintaan ke asal Anda. Dengan Header Permintaan Edge-to-Origin, Anda dapat menambahkan atau mengganti nilai header permintaan yang ada saat CloudFront meneruskan permintaan ke asal Anda. Anda dapat menggunakan Header Kustom Asal, misalnya, `X-Shared-Secret` header, untuk membantu memvalidasi bahwa permintaan yang dibuat ke asal Anda dikirim. CloudFront

Untuk informasi selengkapnya tentang melindungi asal Anda dengan Header Kustom Asal, lihat Menambahkan header khusus ke permintaan asal dan Membatasi akses ke Application Load Balancers.

Untuk panduan tentang penerapan solusi sampel untuk secara otomatis memutar nilai Header Kustom Asal untuk pembatasan akses asal, lihat Cara meningkatkan keamanan CloudFront asal Amazon dengan AWS WAF dan Secrets Manager.

Atau, Anda dapat menggunakan AWS Lambdafungsi untuk memperbarui aturan grup keamanan secara otomatis agar hanya mengizinkan CloudFront lalu lintas. Ini meningkatkan keamanan asal Anda dengan membantu memastikan bahwa pengguna jahat tidak dapat melewati CloudFront dan AWS WAF saat mengakses aplikasi web Anda.

Untuk informasi selengkapnya tentang cara melindungi asal Anda dengan memperbarui grup keamanan secara otomatis, dan `X-Shared-Secret` tajuknya, lihat Cara Memperbarui Grup Keamanan Anda secara Otomatis untuk Amazon CloudFront dan AWS WAF Menggunakan AWS Lambda.

Namun, solusinya melibatkan konfigurasi tambahan dan biaya menjalankan fungsi Lambda. Untuk menyederhanakan ini, kami sekarang telah memperkenalkan daftar awalan AWS-managed untuk membatasi inboundHTTP/HTTPStraffic CloudFront ke asal Anda hanya dari alamat IP yang menghadap asal. CloudFront AWS Daftar awalan yang dikelola dibuat dan dikelola oleh AWS dan tersedia untuk digunakan tanpa biaya tambahan. Anda dapat mereferensikan daftar awalan terkelola CloudFront dalam aturan grup keamanan (AmazonVPC), tabel rute subnet, aturan grup keamanan umum dengan AWS Firewall Manager, dan AWS sumber daya lain yang dapat menggunakan daftar awalan terkelola.

Untuk informasi selengkapnya tentang menggunakan daftar awalan AWS-managed untuk Amazon CloudFront, lihat Batasi akses ke asal Anda menggunakan daftar awalan AWS-managed untuk Amazon. CloudFront

> **Note**
>
> Seperti yang dibahas di bagian lain dari dokumen ini, mengandalkan kelompok keamanan untuk melindungi asal Anda dapat menambahkan pelacakan koneksi grup keamanan sebagai potensi bottle-neck selama permintaan banjir. Kecuali Anda dapat memfilter permintaan berbahaya saat CloudFront menggunakan kebijakan caching yang memungkinkan caching, mungkin lebih baik mengandalkan Header Kustom Asal, yang dibahas sebelumnya, untuk membantu memvalidasi bahwa permintaan yang dibuat ke asal Anda dikirim CloudFront,

daripada menggunakan grup keamanan. Menggunakan header permintaan kustom dengan aturan pendengar Application Load Balancer mencegah pembatasan karena batas pelacakan yang dapat memengaruhi pembuatan koneksi baru ke penyeimbang beban, sehingga memungkinkan Application Load Balancer untuk menskalakan berdasarkan peningkatan lalu lintas jika terjadi serangan. DDoS

Melindungi API titik akhir () BP4

Ketika Anda harus mengekspos API ke publik, ada risiko bahwa API frontend dapat ditargetkan oleh serangan. DDoS Untuk membantu mengurangi risiko, Anda dapat menggunakan Amazon API Gateway sebagai pintu masuk ke aplikasi yang berjalan di Amazon EC2 AWS Lambda, atau di tempat lain. Dengan menggunakan Amazon API Gateway, Anda tidak memerlukan server Anda sendiri untuk API frontend dan Anda dapat mengaburkan komponen lain dari aplikasi Anda. Dengan mempersulit mendeteksi komponen aplikasi Anda, Anda dapat membantu mencegah AWS sumber daya tersebut ditargetkan oleh DDoS serangan.

Saat Anda menggunakan Amazon API Gateway, Anda dapat memilih dari dua jenis API titik akhir. Yang pertama adalah opsi default: API titik akhir yang dioptimalkan tepi yang diakses melalui distribusi Amazon. CloudFront Distribusi dibuat dan dikelola oleh API Gateway, sehingga Anda tidak memiliki kendali atasnya. Opsi kedua adalah menggunakan API titik akhir regional yang diakses dari titik yang sama Wilayah AWS di mana Anda REST API digunakan. AWS merekomendasikan agar Anda menggunakan jenis endpoint kedua dan mengaitkannya dengan CloudFront distribusi Amazon Anda sendiri. Ini memberi Anda kontrol atas CloudFront distribusi Amazon dan kemampuan untuk digunakan AWS WAF untuk perlindungan lapisan aplikasi. Mode ini memberi Anda akses ke kapasitas DDoS mitigasi skala di seluruh jaringan edge AWS global.

Saat menggunakan Amazon CloudFront dan AWS WAF dengan Amazon API Gateway, konfigurasikan opsi berikut:

- Konfigurasikan perilaku cache untuk distribusi Anda untuk meneruskan semua header ke titik akhir regional API Gateway. Dengan melakukan ini, CloudFront akan memperlakukan konten sebagai dinamis dan melewatkan caching konten.
- Lindungi API Gateway Anda dari akses langsung dengan mengonfigurasi distribusi untuk menyertakan header kustom asal x-api-key, dengan menetapkan nilai APIkunci di API Gateway.
- Lindungi backend dari kelebihan lalu lintas dengan mengonfigurasi batas standar atau burst rate untuk setiap metode di Anda. REST APIs

Untuk informasi selengkapnya tentang membuat APIs dengan Amazon API Gateway, lihat Amazon API Gateway Memulai.

Teknik operasional

Teknik mitigasi dalam paper ini membantu Anda merancang aplikasi yang secara inheren tahan terhadap serangan. DDoS Dalam banyak kasus, ini juga berguna untuk mengetahui kapan DDoS serangan menargetkan aplikasi Anda sehingga Anda dapat mengambil langkah-langkah mitigasi. Bagian ini membahas praktik terbaik untuk mendapatkan visibilitas ke dalam perilaku abnormal, peringatan dan otomatisasi, mengelola perlindungan dalam skala besar, dan terlibat AWS untuk dukungan tambahan.

Pengujian beban

Muat pengujian aplikasi Anda secara teratur menggunakan pedoman di whitepaper Aplikasi Pengujian Beban kami dengan tingkat lalu lintas yang diharapkan dan di atas yang diharapkan sehingga Anda dapat melihat seberapa efektif arsitektur Anda, bagaimana kebijakan Auto Scaling Anda berfungsi, dan bagaimana fungsi penanganan kesalahan Anda. Uji untuk peningkatan dan penurunan lalu lintas yang diharapkan tetapi juga untuk perilaku tipe “flash-crowd”. Tes ulang baik secara berkala atau sebelum rilis besar apa pun. Untuk pengujian DDoS simulasi lapisan 3 atau 4, seperti SYN banjir, ikuti Kebijakan Pengujian DDoS Simulasi kami.

Metrik dan alarm

Sebagai praktik terbaik, Anda harus menggunakan alat pemantauan infrastruktur dan aplikasi untuk memeriksa ketersediaan aplikasi Anda untuk memastikan aplikasi Anda tidak terpengaruh oleh suatu DDoS peristiwa, sebagai opsi Anda dapat mengonfigurasi aplikasi dan infrastruktur Pemeriksaan kesehatan Rute 53 untuk sumber daya untuk membantu meningkatkan deteksi DDoS peristiwa. Untuk informasi selengkapnya tentang pemeriksaan kesehatan, lihat AWS WAF, Firewall Manager dan Shield Advanced Developer Guide.

Ketika metrik operasional kunci menyimpang secara substansif dari nilai yang diharapkan, penyerang mungkin mencoba menargetkan ketersediaan aplikasi Anda. Keakraban dengan perilaku normal aplikasi Anda, berarti Anda dapat mengambil tindakan lebih cepat ketika Anda mendeteksi anomali. Amazon CloudWatch dapat membantu dengan memantau aplikasi yang Anda jalankan AWS. Misalnya, Anda dapat mengumpulkan dan melacak metrik, mengumpulkan dan memantau file log, mengatur alarm, dan secara otomatis merespons perubahan sumber daya Anda AWS .

Jika Anda mengikuti arsitektur referensi DDoS -resilient saat merancang aplikasi Anda, serangan lapisan infrastruktur umum akan diblokir sebelum mencapai aplikasi Anda. Jika Anda berlangganan

AWS Shield Advanced, Anda memiliki akses ke sejumlah CloudWatch metrik yang dapat menunjukkan bahwa aplikasi Anda sedang ditargetkan.

Misalnya, Anda dapat mengonfigurasi alarm untuk memberi tahu Anda ketika ada DDoS serangan yang sedang berlangsung, sehingga Anda dapat memeriksa kesehatan aplikasi Anda dan memutuskan apakah akan terlibat. AWS SRT Anda dapat mengonfigurasi `DDoSDetected` metrik untuk memberi tahu Anda jika serangan telah terdeteksi. Jika Anda ingin diperingatkan berdasarkan volume serangan, Anda juga dapat menggunakan`DDoSAttackBitsPerSecond`,`DDoSAttackPacketsPerSecond`, atau `DDoSAttackRequestsPerSecond` metrik. Anda dapat memantau metrik ini dengan mengintegrasikan CloudWatch dengan alat Anda sendiri atau dengan menggunakan alat yang disediakan oleh pihak ketiga, seperti Slack atau. PagerDuty

Serangan lapisan aplikasi dapat meningkatkan banyak CloudWatch metrik Amazon. Jika Anda menggunakan AWS WAF, Anda dapat menggunakan CloudWatch untuk memantau dan mengaktifkan alarm pada peningkatan permintaan yang telah Anda tetapkan AWS WAF untuk diizinkan, dihitung, atau diblokir. Ini memungkinkan Anda menerima pemberitahuan jika tingkat lalu lintas melebihi apa yang dapat ditangani aplikasi Anda. Anda juga dapat menggunakan Amazon CloudFront, Amazon Route 53, Application Load Balancer, Network Load Balancer, EC2 Amazon, dan metrik Auto Scaling yang CloudWatch dilacak untuk mendeteksi perubahan yang dapat mengindikasikan serangan. DDoS

Tabel berikut mencantumkan deskripsi CloudWatch metrik yang biasa digunakan untuk mendeteksi dan bereaksi terhadap DDoS serangan.

Tabel 3 - CloudWatch Metrik Amazon yang direkomendasikan

Topik	Metrik	Deskripsi
AWS Shield Advanced	`DDoSDetected`	Menunjukkan DDoS peristiwa untuk Nama Sumber Daya Amazon tertentu (ARN).
AWS Shield Advanced	`DDoSAttackBitsPerSecond`	Jumlah byte yang diamati selama suatu DDoS peristiwa untuk suatu peristiwa tertentuARN. Metrik ini hanya

Topik	Metrik	Deskripsi
		tersedia untuk DDoS peristiwa lapisan 3 atau 4.
AWS Shield Advanced	`DDoSAttackPacketsPerSecond`	Jumlah paket yang diamati selama DDoS acara tertentuARN. Metrik ini hanya tersedia untuk DDoS peristiwa lapisan 3 atau 4.
AWS Shield Advanced	`DDoSAttackRequestsPerSecond`	Jumlah permintaan yang diamati selama DDoS acara untuk spesifikARN. Metrik ini hanya tersedia untuk DDoS peristiwa lapisan 7 dan hanya dilaporkan untuk peristiwa lapisan 7 yang paling signifikan.
AWS WAF	`AllowedRequests`	Jumlah permintaan web yang diizinkan.
AWS WAF	`BlockedRequests`	Jumlah permintaan web yang diblokir.
AWS WAF	`CountedRequests`	Jumlah permintaan web yang dihitung.
AWS WAF	`PassedRequests`	Jumlah permintaan yang dilewati. Ini hanya digunakan untuk permintaan yang melalui evaluasi grup aturan tanpa mencocokkan aturan grup aturan mana pun.
Amazon CloudFront	`Requests`	Jumlah HTTP permintaan/S.

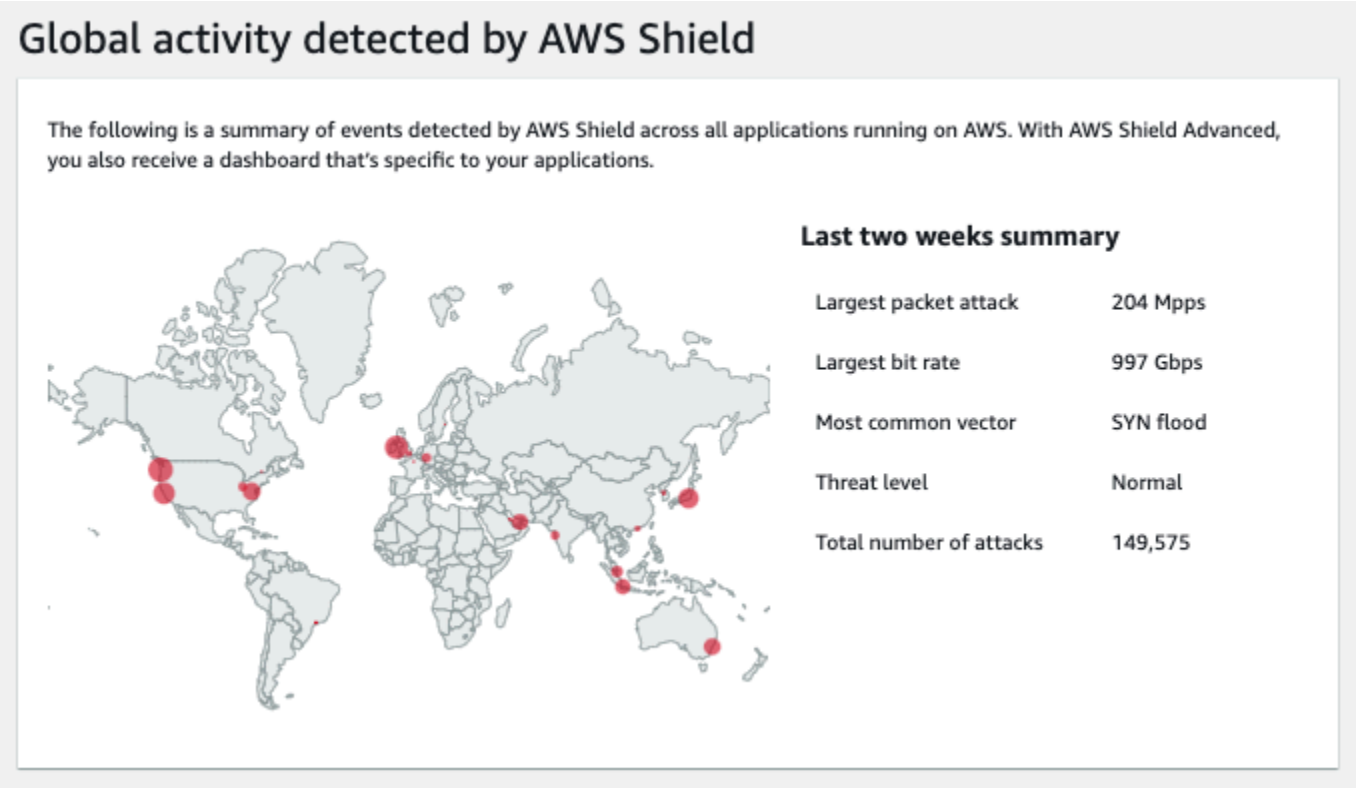
Topik	Metrik	Deskripsi
Amazon CloudFront	`TotalErrorRate`	Persentase semua permintaan yang kode HTTP statusnya `4xx` atau`5xx`.
Amazon Route 53	`HealthCheckStatus`	Status titik akhir pemeriksaan kesehatan.
Penyeimbang Beban Aplikasi	`ActiveConnectionCount`	Jumlah total TCP koneksi bersamaan yang aktif dari klien ke penyeimbang beban, dan dari penyeimbang beban ke target.
Penyeimbang Beban Aplikasi	`ConsumedLCUs`	Jumlah unit kapasitas load balancer (LCU) yang digunakan oleh load balancer Anda.
Penyeimbang Beban Aplikasi	`HTTPCode_ELB_4XX_Count` `HTTPCode_ELB_5XX_Count`	Jumlah HTTP `4xx` atau kode kesalahan `5xx` klien yang dihasilkan oleh penyeimbang beban.
Penyeimbang Beban Aplikasi	`NewConnectionCount`	Jumlah total TCP koneksi baru yang dibuat dari klien ke penyeimbang beban, dan dari penyeimbang beban ke target.
Penyeimbang Beban Aplikasi	`ProcessedBytes`	Jumlah total byte yang diproses oleh penyeimbang beban.
Penyeimbang Beban Aplikasi	`RejectedConnectionCount`	Jumlah koneksi yang ditolak karena penyeimbang beban telah mencapai jumlah koneksi maksimumnya.

Topik	Metrik	Deskripsi
Penyeimbang Beban Aplikasi	`RequestCount`	Jumlah permintaan yang diproses.
Penyeimbang Beban Aplikasi	`TargetConnectionErrorCount`	Jumlah koneksi yang tidak berhasil dibuat antara penyeimbang beban dan target.
Penyeimbang Beban Aplikasi	`TargetResponseTime`	Waktu berlalu, dalam hitungan detik, setelah permintaan meninggalkan penyeimbang beban hingga respons dari target diterima.
Penyeimbang Beban Aplikasi	`UnHealthyHostCount`	Jumlah target yang dianggap tidak sehat.
Network Load Balancer	`ActiveFlowCount`	Jumlah total TCP arus bersamaan (atau koneksi) dari klien ke target.
Network Load Balancer	`ConsumedLCUs`	Jumlah unit kapasitas load balancer (LCU) yang digunakan oleh load balancer Anda.
Network Load Balancer	`NewFlowCount`	Jumlah total TCP arus baru (atau koneksi) yang ditetapkan dari klien ke target dalam periode waktu tersebut.
Network Load Balancer	`ProcessedBytes`	Jumlah total byte yang diproses oleh penyeimbang beban, termasuk header TCP / IP.

Topik	Metrik	Deskripsi
Global Accelerator	`NewFlowCount`	Jumlah total baru TCP dan UDP arus (atau koneksi) yang dibuat dari klien ke titik akhir dalam periode waktu.
Global Accelerator	`ProcessedBytesIn`	Jumlah total byte masuk yang diproses oleh akselerator, termasuk TCP header /IP.
Auto Scaling	`GroupMaxSize`	Ukuran maksimum grup Auto Scaling.
Amazon EC2	`CPUUtilization`	Persentase unit EC2 komputasi yang dialokasikan yang saat ini digunakan.
Amazon EC2	`NetworkIn`	Jumlah bita yang diterima oleh instans di semua antarmuka jaringan.

Untuk informasi selengkapnya tentang menggunakan Amazon CloudWatch untuk mendeteksi DDoS serangan pada aplikasi Anda, lihat Memulai dengan Amazon CloudWatch.

AWS mencakup beberapa metrik dan alarm tambahan untuk memberi tahu Anda tentang serangan dan untuk membantu Anda memantau sumber daya aplikasi Anda. AWS Shield Konsol atau API memberikan ringkasan peristiwa per akun dan rincian tentang serangan yang telah terdeteksi.



Aktivitas global yang terdeteksi oleh AWS Shield

Selain itu, dasbor lingkungan ancaman global memberikan informasi ringkasan tentang semua DDoS serangan yang telah terdeteksi oleh AWS. Informasi ini mungkin berguna untuk lebih memahami DDoS ancaman di populasi aplikasi yang lebih besar selain tren serangan, dan membandingkannya dengan serangan yang mungkin telah Anda amati.

Jika Anda berlangganan AWS Shield Advanced, dasbor layanan menampilkan metrik deteksi dan mitigasi tambahan serta detail lalu lintas jaringan untuk peristiwa yang terdeteksi pada sumber daya yang dilindungi. AWS Shield mengevaluasi lalu lintas ke sumber daya terlindungi Anda di berbagai dimensi. Ketika anomali terdeteksi, AWS Shield buat peristiwa dan laporkan dimensi lalu lintas tempat anomali diamati. Dengan mitigasi yang ditempatkan, ini melindungi sumber daya Anda dari menerima kelebihan lalu lintas dan lalu lintas yang cocok dengan tanda tangan DDoS acara yang diketahui.

Metrik deteksi didasarkan pada aliran jaringan sampel atau AWS WAF log ketika web ACL dikaitkan dengan sumber daya yang dilindungi. Metrik mitigasi didasarkan pada lalu lintas yang diamati oleh sistem mitigasi Shield. DDoS Metrik mitigasi adalah pengukuran lalu lintas yang lebih tepat ke sumber daya Anda.

Metrik kontributor teratas jaringan memberikan wawasan tentang dari mana lalu lintas berasal selama peristiwa yang terdeteksi. Anda dapat melihat kontributor volume tertinggi dan mengurutkan berdasarkan aspek seperti protokol, port sumber, dan TCP bendera. Metrik kontributor teratas mencakup metrik untuk semua lalu lintas yang diamati pada sumber daya sepanjang berbagai dimensi. Ini memberikan dimensi metrik tambahan yang dapat Anda gunakan untuk memahami lalu lintas jaringan yang dikirim ke sumber daya Anda selama acara berlangsung. Perlu diingat bahwa untuk serangan lapisan 3 atau 4 non-refleksi, alamat IP sumber mungkin telah dipalsukan dan tidak dapat diandalkan.

Dasbor layanan juga mencakup detail tentang tindakan yang diambil secara otomatis untuk mengurangi seranganDDoS. Informasi ini memudahkan untuk menyelidiki anomali, menjelajahi dimensi lalu lintas, dan lebih memahami tindakan yang diambil oleh Shield Advanced untuk melindungi ketersediaan Anda.

Pencatatan log

Aktifkan pencatatan yang berguna di semua layanan sesuai dengan panduan Pencatatan dan pemantauan kami bagi pemilik aplikasi untuk memaksimalkan visibilitas dan membantu pemecahan masalah. Ini termasuk, tetapi tidak terbatas pada:

- AWS CloudTrail
- Log AWS WAF
- CloudFrontlog akses
- VPCLog Aliran (lihat Log dan Lihat Arus Lalu Lintas Jaringan) — sertakan `tcp-flags` bidang di bidang yang disertakan untuk memaksimalkan visibilitas
- ELBlog akses (ALB, CLB, NLB)
- Log HTTP akses server web
- Pencatatan keamanan sistem operasi
- Pencatatan aplikasi

Manajemen visibilitas dan perlindungan di beberapa akun

Dalam skenario ketika Anda beroperasi di beberapa Akun AWS dan memiliki beberapa komponen untuk dilindungi, menggunakan teknik yang memungkinkan Anda beroperasi dalam skala besar dan mengurangi overhead operasional meningkatkan kemampuan mitigasi Anda. Saat mengelola sumber daya yang AWS Shield Advanced dilindungi di beberapa akun, Anda dapat mengatur pemantauan

terpusat dengan menggunakan AWS Firewall Manager dan AWS Security Hub. Dengan Firewall Manager, Anda dapat membuat kebijakan keamanan yang memberlakukan kepatuhan DDoS perlindungan di semua akun Anda. Anda dapat menggunakan kedua layanan ini bersama-sama untuk mengelola sumber daya yang dilindungi di beberapa akun dan memusatkan pemantauan sumber daya tersebut.

Security Hub secara otomatis terintegrasi dengan Firewall Manager, memungkinkan pelanggan Shield Advanced untuk melihat temuan keamanan dalam satu dasbor, di samping peringatan keamanan prioritas tinggi lainnya dan status kepatuhan.

Misalnya, ketika Shield Advanced mendeteksi lalu lintas anomali yang ditujukan untuk sumber daya yang dilindungi di dalam lingkup mana pun Akun AWS , temuan ini akan terlihat di konsol Security Hub. Jika dikonfigurasi, Firewall Manager dapat secara otomatis membawa sumber daya ke dalam kepatuhan dengan membuatnya sebagai sumber daya yang dilindungi Shield Advanced, dan kemudian memperbarui Security Hub saat sumber daya dalam status sesuai.

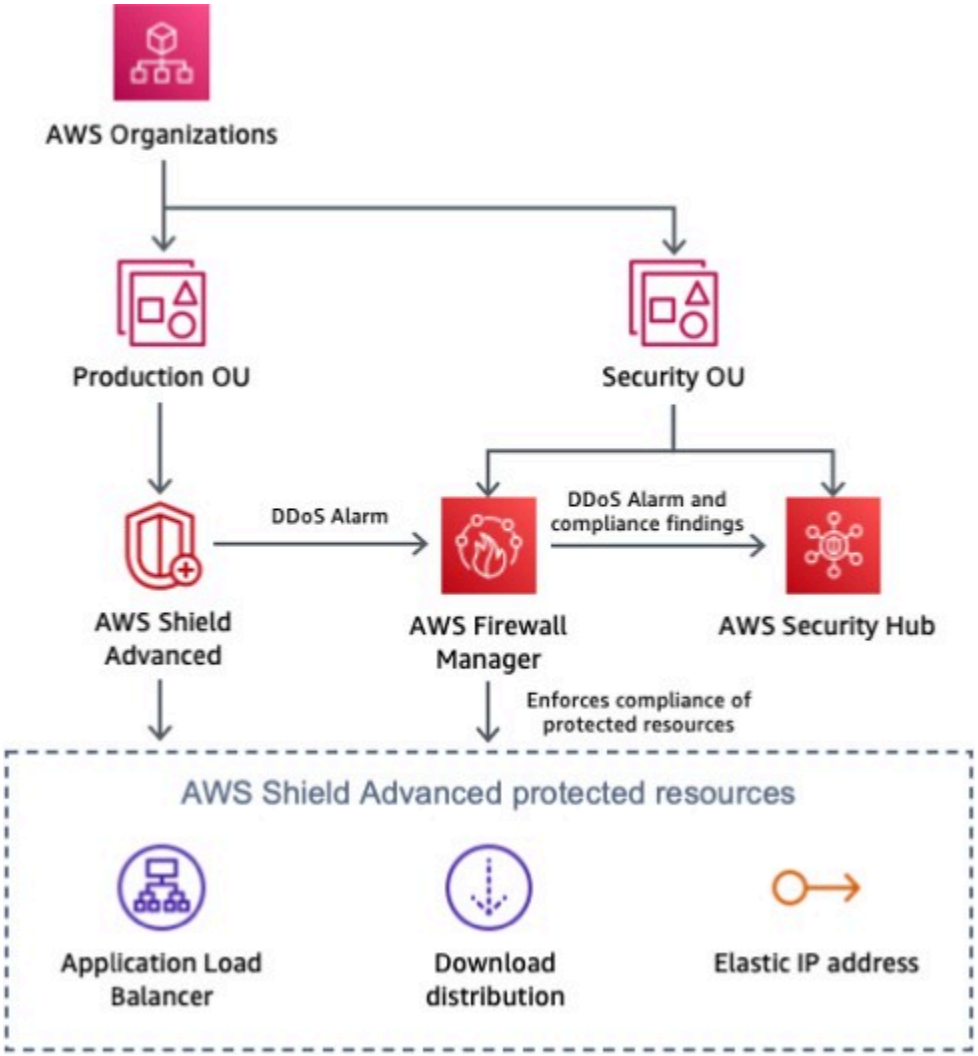


Diagram arsitektur yang menunjukkan pemantauan sumber daya AWS Shield yang dilindungi dengan Firewall Manager dan Security Hub

Untuk informasi selengkapnya tentang pemantauan pusat sumber daya yang dilindungi Shield, lihat Mengatur pemantauan terpusat untuk DDoS peristiwa dan memulihkan sumber daya yang tidak sesuai secara otomatis.

Strategi respons insiden dan runbook

Mengembangkan strategi respons insiden DDoS serangan dan membangun proses respons insiden keamanan di sekitarnya sangat penting bagi semua organisasi. Pendekatan yang disarankan adalah memodelkan buku NIST pedoman respons Anda berdasarkan langkah-langkah yang disarankan seperti mengumpulkan bukti, mengurangi, memulihkan, dan melakukan analisis pasca-insiden. Misalnya, buku pedoman respons untuk DoS atau DDoS serangan aplikasi web disediakan sebagai contoh. Sumber daya tambahan tersedia di Panduan Respons Insiden AWS Keamanan.

Dukungan

Jika Anda mengalami serangan, Anda juga bisa mendapatkan keuntungan dari dukungan AWS dalam menilai ancaman dan meninjau arsitektur aplikasi Anda, atau Anda mungkin ingin meminta bantuan lain. Penting untuk membuat rencana respons untuk DDoS serangan sebelum peristiwa yang sebenarnya. Praktik terbaik yang diuraikan dalam paper ini dimaksudkan sebagai tindakan proaktif yang Anda terapkan sebelum meluncurkan aplikasi, tetapi DDoS serangan terhadap aplikasi Anda mungkin masih terjadi. Tinjau opsi di bagian ini untuk menentukan sumber daya dukungan yang paling cocok untuk skenario Anda. Tim akun Anda dapat mengevaluasi kasus penggunaan dan aplikasi Anda, dan membantu dengan pertanyaan atau tantangan spesifik yang Anda miliki.

Jika Anda menjalankan beban kerja produksi AWS, pertimbangkan untuk berlangganan Business Support, yang memberi Anda akses 24/7 ke Cloud Support Engineers yang dapat membantu mengatasi DDoS masalah serangan. Jika Anda menjalankan beban kerja kritis misi, pertimbangkan Enterprise Support yang menyediakan kemampuan untuk membuka kasus kritis dan menerima respons tercepat dari Senior Cloud Support Engineer.

Jika Anda berlangganan AWS Shield Advanced dan juga berlangganan Business Support atau Enterprise Support, Anda dapat mengonfigurasi keterlibatan proaktif Shield. Ini memungkinkan Anda untuk mengonfigurasi pemeriksaan kesehatan, mengaitkan dengan sumber daya Anda, dan memberikan informasi kontak operasi 24/7. Ketika Shield mendeteksi tanda-tanda DDoS dan pemeriksaan kesehatan aplikasi Anda menunjukkan tanda-tanda degradasi, AWS SRT akan secara

proaktif menghubungi Anda. Ini adalah model keterlibatan yang kami rekomendasikan karena memungkinkan waktu AWS SRT respons tercepat dan memberdayakan AWS SRT untuk memulai pemecahan masalah bahkan sebelum kontak dibuat dengan Anda.

Untuk informasi selengkapnya, lihat Bandingkan AWS Support Paket.

Fitur keterlibatan proaktif mengharuskan Anda mengonfigurasi pemeriksaan kesehatan Route 53 yang secara akurat mengukur kesehatan aplikasi Anda dan dikaitkan dengan sumber daya yang dilindungi oleh Shield Advanced. Setelah pemeriksaan kesehatan Route 53 dikaitkan di konsol Shield, sistem deteksi Shield Advanced menggunakan status pemeriksaan kesehatan sebagai indikator kesehatan aplikasi Anda. Fitur deteksi berbasis kesehatan di Shield Advanced akan memastikan bahwa Anda diberi tahu dan mitigasi ditempatkan lebih cepat ketika aplikasi Anda tidak sehat. AWS SRTakan menghubungi Anda untuk memecahkan masalah apakah aplikasi yang tidak sehat sedang ditargetkan oleh DDoS serangan dan menempatkan mitigasi tambahan sesuai kebutuhan.

Menyelesaikan konfigurasi keterlibatan proaktif termasuk menambahkan detail kontak di konsol Shield. AWS SRTakan menggunakan informasi ini untuk menghubungi Anda. Anda dapat mengonfigurasi hingga sepuluh kontak, dan memberikan catatan tambahan jika Anda memiliki persyaratan atau preferensi kontak tertentu. Proaktif

kontak keterlibatan harus memegang peran 24/7, seperti pusat operasi keamanan atau individu yang segera tersedia.

Anda dapat mengaktifkan keterlibatan proaktif untuk semua sumber daya atau untuk sumber daya produksi kunci tertentu di mana waktu respons sangat penting. Ini dicapai dengan menetapkan pemeriksaan kesehatan hanya untuk sumber daya ini.

Anda juga dapat melakukan eskalasi AWS SRT dengan membuat AWS Support case menggunakan AWS Support konsol (login diperlukan), atau Support API jika Anda memiliki peristiwa DDoS terkait yang memengaruhi ketersediaan aplikasi Anda.

Kesimpulan

Praktik terbaik yang diuraikan dalam paper ini dapat membantu Anda membangun arsitektur DDoS tangguh yang melindungi ketersediaan aplikasi Anda dengan mencegah banyak infrastruktur umum dan serangan lapisan aplikasi. DDoS Sejauh mana Anda mengikuti praktik terbaik ini ketika Anda merancang aplikasi Anda akan memengaruhi jenis, vektor, dan volume DDoS serangan yang dapat Anda mitigasi. Anda dapat menggabungkan ketahanan tanpa berlangganan layanan mitigasi. DDoS Dengan memilih untuk berlangganan, AWS Shield Advanced Anda mendapatkan dukungan tambahan, visibilitas, mitigasi, dan fitur perlindungan biaya yang selanjutnya melindungi arsitektur aplikasi yang sudah tangguh.

Kontributor

Kontributor dokumen ini meliputi:

- Rodrigo Ferroni, Spesialis Keamanan AWS TAM
- Dmitriy Novikov, Arsitek Solusi AWS
- Achraf Souk, Arsitek Solusi AWS
- Joanna Knox, Teknik AWS Support
- Anuj Butail, Arsitek Solusi AWS
- Harith Gaddamanugu, Spesialis Tepi SA AWS

Bacaan lebih lanjut

Untuk informasi tambahan, lihat:

- Pedoman Pelaksanaan AWS WAF (AWS Whitepaper)
- NIS301 — re:Inforce 2023: Bagaimana intelijen AWS ancaman menjadi aturan firewall terkelola (video) YouTube
- NET314- re:invent 2022: Membangun aplikasi yang DDoS tangguh menggunakan (video) AWS Shield YouTube
- SEC321- Re: Invent 2020: Maju dari kurva dengan eskalasi Tim DDoS Respons (video) YouTube
- William Hill: DDoS Perlindungan Kinerja Tinggi dengan AWS - 2020 (YouTubevideo)
- SEC407 - re:Invent 2019: defense-in-depth Pendekatan untuk membangun aplikasi web (video) YouTube
- Praktik Terbaik untuk DDoS Mitigasi pada AWS — 2018 (video) YouTube
- SID324— Re: Invent 2017: Mengotomatiskan DDoS Respons di Cloud (video) YouTube
- CTD304 - re:Invent 2017: Perjalanan Dow Jones & Wall Street Journal untuk Mengelola Lonjakan Lalu Lintas Sementara (video) YouTube
- Mengurangi DDoS & Ancaman Lapisan Aplikasi (video) YouTube
- CTD310 - Re: Invent 2017: Hidup di Tepi, Lebih Aman Dari yang Anda Pikirkan! Membangun Kuat dengan Amazon (YouTube video)
- CloudFront, AWS Shield, dan AWS WAF (YouTube video)

Revisi dokumen

Untuk diberitahu tentang pembaruan pada whitepaper ini, berlangganan feed. RSS

Perubahan	Deskripsi	Tanggal
Pembaruan Whitepaper	Ditambahkan OAC untuk CloudFront dan perlindungan biaya DNS wildcard. Diskusi yang diperluas tentang teknik operasional, caching, aturan berbasis tarif, dan kelompok aturan terkelola. Ditambahkan lokal ke dalam diagram arsitektur, duplikasi dihapus, dan teks yang diklarifikasi untuk menghilangkan ambiguitas.	9 Agustus 2023
Pembaruan Whitepaper	Direvisi untuk kejelasan; Diperbarui untuk menyertakan rekomendasi dan fitur terbaru: Pelacakan koneksi grup keamanan dan DDoS mitigasi lapisan aplikasi otomatis Shield Advanced.	13 April 2022
Pembaruan Whitepaper	Diperbarui untuk menyertakan rekomendasi dan fitur terbaru. AWS Global Accelerator ditambahkan sebagai bagian dari perlindungan komprehensif di tepi. AWS Firewall Manager untuk pemantauan terpusat untuk DDoS acara dan memulihkan sumber daya	September 21, 2021

	yang tidak sesuai secara otomatis.	
Pembaruan Whitepaper	Diperbarui untuk memperjelas penghilangan cache di bagian Deteksi dan Filter Permintaan Web Berbahaya (BP1,BP2), dan ELB dan ALB penggunaan di bagian Skala untuk Menyerap (BP6). Diagram yang diperbarui dan Tabel 2, ditandai “Pilihan Wilayah.” sebagaiBP8. BP7Bagian yang diperbarui dengan detail lebih lanjut.	18 Desember 2019
Pembaruan Whitepaper	Diperbarui untuk memasukkan AWS WAF logging sebagai praktik terbaik.	Desember 1, 2018
Pembaruan Whitepaper	Diperbarui untuk menyertakan AWS Shield, AWS WAF fitur AWS Firewall Manager, dan praktik terbaik terkait.	1 Juni 2018
Pembaruan Whitepaper	Menambahkan panduan arsitektur preskriptif dan diperbarui untuk disertakan. AWS WAF	1 Juni 2016
Publikasi awal	Whitepaper diterbitkan.	1 Juni 2015

Pemberitahuan

Pelanggan bertanggung jawab untuk membuat penilaian independen mereka sendiri atas informasi dalam dokumen ini. Dokumen ini: (a) hanya untuk tujuan informasi, (b) mewakili penawaran dan praktik AWS produk saat ini, yang dapat berubah tanpa pemberitahuan, dan (c) tidak membuat komitmen atau jaminan apa pun dari AWS dan afiliasinya, pemasok, atau pemberi lisensinya. AWS produk atau layanan disediakan “sebagaimana adanya” tanpa jaminan, representasi, atau kondisi apa pun, baik tersurat maupun tersirat. Tanggung jawab dan kewajiban AWS kepada pelanggannya dikendalikan oleh AWS perjanjian, dan dokumen ini bukan bagian dari, juga tidak mengubah, perjanjian apa pun antara AWS dan pelanggannya.

AWS Glosarium

Untuk AWS terminologi terbaru, lihat AWS glosarium di Referensi.Glosarium AWS

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