Laporan Resmi AWS

Praktik Terbaik AWS untuk Ketahanan DDoS

Praktik Terbaik AWS untuk Ketahanan DDoS: Laporan Resmi AWS

Table of Contents

AWS Praktik Terbaik AWS untuk Ketahanan DDoS

Tanggal publikasi: 21 September 2021 (Revisi Dokumen)

Abstrak

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

Dalam laporan resmi ini, AWS memberi Anda panduan DDoS preskriptif untuk meningkatkan ketahanan aplikasi yang berjalan di AWS. Ini termasuk arsitektur referensi yang tahan terhadap DDoS yang dapat digunakan sebagai panduan untuk membantu melindungi ketersediaan aplikasi. Laporan resmi ini juga menjelaskan jenis serangan yang berbeda-beda, 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 mitigasi DDoS akan diuraikan dan cara masing-masing dapat digunakan untuk membantu melindungi aplikasi Anda akan dijelaskan.

Laporan ini ditujukan untuk pengambil keputusan IT dan rekayasawan keamanan yang memahami konsep dasar jaringan, keamanan, dan AWS. Setiap bagiannya memiliki tautan ke dokumentasi AWS yang memberikan detail lebih lanjut tentang praktik terbaik atau kemampuan.

Pengantar: Serangan Denial of Service

Serangan Denial of Service (DoS) adalah percobaan yang disengaja untuk membuat situs web atau aplikasi tidak tersedia bagi pengguna, seperti dengan membanjiri lalu lintas jaringan. Penyerang menggunakan berbagai teknik yang mengonsumsi bandwidth jaringan dalam jumlah besar atau mengikat sumber daya sistem lainnya, sehingga 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.

Tabel 1: Diagram Serangan DoS

Dalam serangan DDoS, penyerang menggunakan beberapa sumber untuk mengatur serangan terhadap target. Sumber-sumber ini dapat mencakup grup terdistribusi yang terdiri dari komputer, router, perangkat IoT, dan titik akhir lainnya yang terinfeksi malware. Diagram berikut menunjukkan jaringan host yang mengalami kebocoran keamanan yang berpartisipasi dalam serangan, sehingga menghasilkan banjir paket atau permintaan untuk membanjiri target.

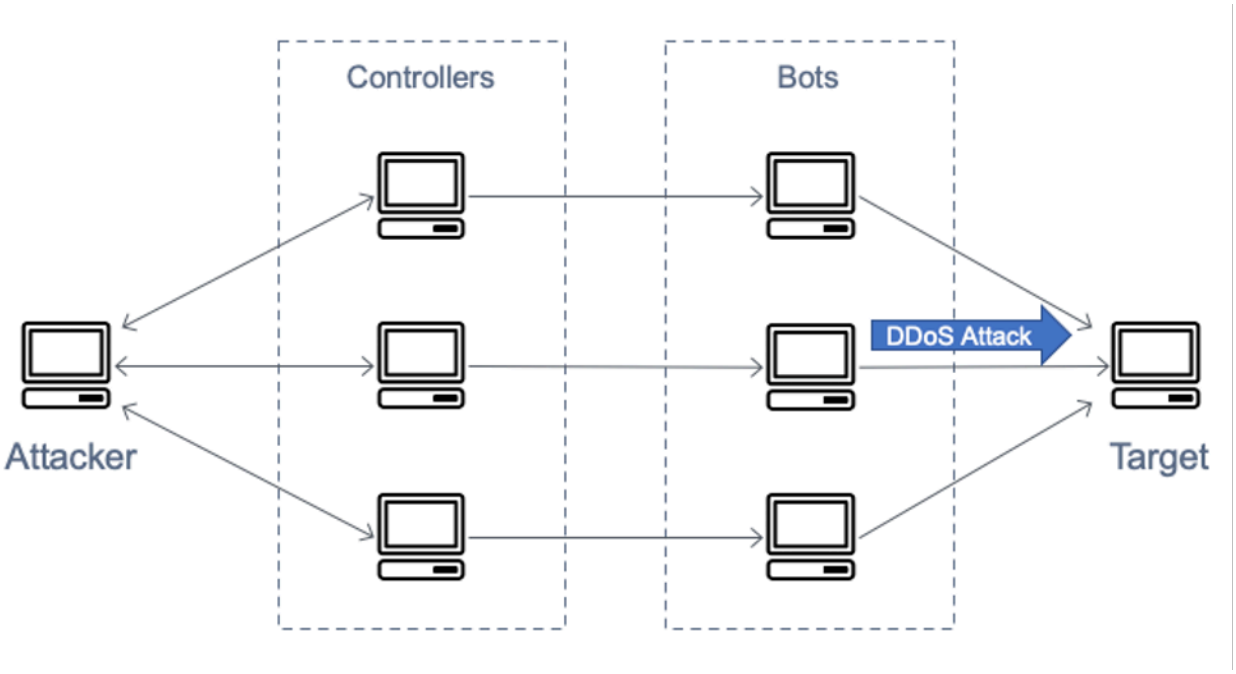

Diagram Serangan DDoS

Ada tujuh lapisan dalam model Open Systems Interconnection (OSI) dan lapisan ini dijelaskan dalam tabel Model Open Systems Interconnection (OSI) . Serangan DDoS paling umum terjadi pada lapisan tiga, empat, enam, dan tujuh. Serangan lapisan tiga dan empat adalah lapisan Jaringan

dan Pengangkutan model OSI. Dalam laporan ini, AWS menyebut hal ini secara kolektif sebagai serangan lapisan infrastruktur. Serangan lapisan enam dan tujuh adalah lapisan Presentasi dan Aplikasi model OSI. AWS akan membahas ini bersama-sama sebagai serangan lapisan aplikasi. Contoh jenis serangan ini dibahas dalam bagian berikut.

Model Open Systems Interconnection (OSI)

#	Lapisan	Unit	Deskripsi	Contoh Vektor
7	Aplikasi	Data	Proses jaringan ke aplikasi	Banjir HTTP, banjir permintaan DNS
6	Presentasi	Data	Representasi dan enkripsi data	Penyalahgunaan TLS
5	Sesi	Data	Komunikasi di antara host	T/A
4	Pengangkutan	Segmen	Koneksi dan keandalan ujung ke ujung	Banjir SYN
3	Jaringan	Paket	Penentuan jalur dan pengalamatan logis	Serangan refleksi UDP
2	Tautan Data	Frame	Pengalamatan fisik	T/A
1	Fisik	Bit	Transmisi media, sinyal, dan biner	T/A

Topik

- Serangan Lapisan Infrastruktur
- Serangan Lapisan Aplikasi

Serangan Lapisan Infrastruktur

Serangan DDoS yang paling umum, serangan refleksi User Datagram Protocol (UDP) dan banjir sinkronisasi (SYN) banjir, adalah serangan lapisan infrastruktur. Penyerang dapat menggunakan salah satu 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 dapat mudah diidentifikasi, untuk memitigasinya secara efektif, Anda harus memiliki jaringan atau sistem yang menaikkan skala kapasitas dengan lebih cepat daripada banjir lalu lintas yang masuk. Kapasitas tambahan ini diperlukan untuk memfilter atau menyerap lalu lintas serangan, sehingga membebaskan sistem dan aplikasi untuk merespons lalu lintas pelanggan yang sah.

Topik

Serangan Refleksi UDP

Serangan refleksi User Datagram Protocol (UDP) mengeksploitasi fakta bahwa UDP adalah protokol stateless. Penyerang dapat membuat paket permintaan UDP valid yang mencantumkan alamat IP target serangan sebagai alamat IP sumber UDP. Penyerang sekarang telah memalsukan-melakukan spoofing—IP sumber paket permintaan UDP. Paket UDP ini berisi IP sumber yang di-spoofing dan dikirim oleh penyerang ke server perantara. Server ditipu untuk mengirim paket respons UDP ke IP korban yang ditargetkan, bukan mengirim balik ke alamat IP penyerang. Server perantara digunakan karena menghasilkan respons yang beberapa kali lebih besar dari paket permintaan, sehingga secara efektif mengamplifikasi 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: DNS, NTP, SSDP, CLDAP, Memcached, CharGen, atau QOTD. Misalnya, faktor amplifikasi untuk DNS bisa 28 sampai 54 kali jumlah bita asli. Jadi, jika penyerang mengirimkan muatan permintaan 64 bita ke server DNS, mereka dapat menghasilkan lebih dari 3400 bita lalu lintas yang tidak diinginkan ke target serangan. Serangan refleksi UDP bertanggung jawab untuk volume lalu lintas yang lebih besar dibandingkan dengan serangan lainnya. Angka Serangan Refleksi UDP menggambarkan taktik refleksi dan efek amplifikasi.

Serangan Refleksi UDP

Serangan Banjir SYN

Ketika pengguna terhubung ke layanan Transmission Control Protocol (TCP), seperti server web, klien mereka mengirimkan paket sinkronisasi SYN. Server mengembalikan paket SYN-ACK dalam konfirmasi, dan terakhir klien merespons dengan paket konfirmasi (ACK), yang melengkapi handshake tiga arah yang diharapkan. Gambar berikut menunjukkan handshake yang biasa ini.

Handshake 3 arah SYN

Dalam serangan banjir SYN, klien berbahaya mengirimkan sejumlah besar paket SYN, tetapi tidak pernah mengirimkan paket ACK akhir untuk menyelesaikan handshake. Server dibiarkan menunggu respons terhadap koneksi TCP yang setengah terbuka dan akhirnya kehabisan kapasitas untuk menerima koneksi TCP baru. Hal ini dapat mencegah pengguna baru terhubung ke server. Serangan ini mencoba mengikat koneksi server yang tersedia sehingga sumber daya tidak tersedia untuk koneksi yang sah. Meskipun banjir SYN bisa mencapai hingga ratusan Gbps, tujuan serangan tersebut bukan untuk meningkatkan volume lalu lintas SYN.

Serangan Lapisan Aplikasi

Penyerang dapat menargetkan aplikasi itu sendiri dengan menggunakan serangan lapisan 7 atau lapisan aplikasi. Dalam serangan ini, yang mirip dengan serangan infrastruktur banjir SYN, penyerang mencoba membanjiri fungsi tertentu dari aplikasi untuk membuat aplikasi tidak tersedia atau tidak responsif terhadap pengguna yang sah. Terkadang hal 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 dimitigasi. Contoh serangan lapisan aplikasi termasuk banjir HTTP, serangan cache-busting, dan banjir XML-RPC WordPress.

Dalam serangan banjir HTTP, penyerang mengirimkan permintaan HTTP yang tampaknya berasal dari pengguna aplikasi web yang valid. Beberapa banjir HTTP menargetkan sumber daya tertentu, sementara banjir HTTP yang lebih kompleks mencoba meniru interaksi manusia dengan aplikasi. Hal ini dapat meningkatkan kesulitan dalam menggunakan teknik mitigasi umum seperti pembatasan laju permintaan.

Serangan cache-busting adalah jenis banjir HTTP yang menggunakan variasi dalam string kueri untuk menghindari caching jaringan pengiriman konten (CDN). Bukannya dapat mengembalikan hasil yang di-cache, CDN harus menghubungi server asal untuk setiap permintaan halaman, dan pengambilan asal ini menyebabkan beban tambahan pada server web aplikasi.

Dengan serangan banjir XML-RPC WordPress, yang juga dikenal sebagai banjir pingback WordPress, penyerang menargetkan situs web yang di-host di perangkat lunak manajemen konten WordPress. Penyerang menyalahgunakan fungsi API XML-RPC untuk menghasilkan banjir permintaan HTTP. Fitur pingback memungkinkan situs web yang di-host di WordPress (Situs A) memberi tahu situs WordPress 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 muncul di Agen Pengguna dalam header permintaan HTTP.

Ada bentuk lain dari lalu lintas berbahaya yang dapat memengaruhi ketersediaan aplikasi. Scraper bot mengotomatisasi percobaan untuk mengakses aplikasi web untuk mencuri konten atau mencatat informasi persaingan, seperti harga. Serangan brute force dan credential stuffing adalah percobaan terprogram untuk mendapatkan akses yang tidak sah ke area aplikasi yang aman. Serangan tersebut bukan sepenuhnya merupakan serangan DDoS; tetapi sifat otomatis serangan ini dapat terlihat mirip dengan serangan DDoS dan serangan ini dapat dimitigasi dengan menerapkan beberapa praktik terbaik yang sama yang akan dibahas dalam laporan ini.

Serangan lapisan aplikasi juga dapat menargetkan layanan Sistem Nama Domain (DNS). Yang paling umum dari serangan ini adalah banjir kueri DNS saat penyerang menggunakan banyak kueri DNS yang terbentuk dengan baik untuk menghabiskan sumber daya server DNS. Serangan ini juga dapat mencakup komponen cache-busting saat penyerang mengacak string subdomain untuk memintas cache DNS lokal dari setiap resolver tertentu. Akibatnya, resolver tidak dapat memanfaatkan kueri domain cache dan harus berulang kali menghubungi server DNS otoritatif, yang mengamplifikasi serangan.

Jika aplikasi web dikirim melalui Keamanan Lapisan Pengangkutan (TLS), penyerang juga dapat memilih untuk menyerang proses negosiasi TLS. TLS secara komputasional mahal sehingga penyerang, dengan menghasilkan beban kerja ekstra pada server untuk memproses data yang tidak dapat dibaca (atau tidak dapat dimengerti (ciphertext)) sebagai handshake yang sah, dapat mengurangi ketersediaan server. Dalam variasi serangan ini, penyerang menyelesaikan handshake TLS tetapi terus-menerus menegosiasikan ulang metode enkripsi. Seorang penyerang juga dapat mencoba menghabiskan sumber daya server dengan membuka dan menutup banyak sesi TLS.

Teknik Mitigasi

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

Semua AWS pelanggan bisa mendapatkan keuntungan dari perlindungan otomatis AWS Shield Standard tanpa biaya tambahan. AWS Shield Standard bertahan terhadap serangan DDoS lapisan jaringan dan pengangkutan yang paling umum dan sering terjadi yang menargetkan situs web atau aplikasi Anda. Perlindungan ini selalu aktif, dikonfigurasi sebelumnya, statis, dan tidak memberikan pelaporan atau analitik. Perlindungan ini ditawarkan pada semua layanan AWS dan di setiap Wilayah AWS. Di Wilayah AWS, serangan DDoS akan terdeteksi dan sistem Shield Standard akan secara otomatis menentukan acuan dasar lalu lintas, mengidentifikasi anomali, dan, jika perlu, membuat mitigasi. Anda dapat menggunakan AWS Shield Standard sebagai bagian dari arsitektur yang tahan terhadap DDoS untuk melindungi aplikasi web dan non-web.

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

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

- Akses ke kapasitas mitigasi internet dan DDoS di seluruh AWS Global Edge Network. Hal ini berguna dalam memitigasi serangan volumetrik yang lebih besar, yang dapat mencapai skala terabit.
- Sistem mitigasi DDoS AWS Shield terintegrasi dengan layanan edge AWS, sehingga memitigasi waktu mitigasi dari hitungan menit menjadi subdetik.
- Teknik mitigasi Banjir SYN stateless melakukan proksi dan verifikasi terhadap koneksi masuk sebelum meneruskannya ke layanan yang dilindungi. Hal ini memastikan bahwa hanya koneksi valid yang akan menjangkau aplikasi Anda sambil melindungi pengguna akhir Anda yang sah dari packet drop yang positif palsu.

- Sistem rekayasa lalu lintas otomatis yang mendispersi atau mengisolasi dampak serangan DDoS volumetrik besar. Semua layanan ini mengisolasi serangan di sumbernya sebelum mencapai asal Anda, yang berarti lebih sedikit dampak pada sistem yang dilindungi oleh layanan ini.
- Pertahanan lapisan aplikasi jika dikombinasikan dengan AWS WAF yang tidak memerlukan perubahan arsitektur aplikasi saat ini (misalnya, di Wilayah AWS atau pusat data on-premise).

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

Arsitektur ini mencakup beberapa layanan AWS yang dapat membantu Anda meningkatkan ketahanan aplikasi web Anda terhadap serangan DDoS. Tabel Ringkasan Praktik Terbaik menyediakan ringkasan layanan ini dan kemampuannya. AWS telah menandai setiap layanan dengan indikator praktik terbaik (BP1, BP2) untuk referensi yang lebih mudah dalam dokumen ini. Misalnya, bagian selanjutnya akan membahas kemampuan yang disediakan oleh Amazon CloudFront dan Global Accelerator yang mencakup indikator praktik terbaik BP1.

Tabel 2 - Ringkasan Praktik Terbaik

Edge AWS	Wilayah AWS					
	Menggunakan Amazon CloudFront (BP1) dengan AWS WAF (BP2)	Menggunakan Akselerator Global (BP1)	Menggunakan Amazon Route 53 (BP3)	Menggunakan Elastic Load Balancing (BP6) dengan AWS WAF (BP2)	Menggunakan Grup Keamanan dan ACL jaringan di Amazon VPC (BP5)	Menggunakan Amazon EC2 Auto Scaling (BP7)
Mitigasi serangan lapisan 3 (misalnya	✓	✓	✓	✓	✓	✓

Edge AWS	Wilayah AWS					
, refleksi UDP)						
Mitigasi serangan lapisan 4 (misalnya, banjir SYN)	✓	✓	✓	✓		
Mitigasi serangan lapisan 6 (misalnya, TLS)	✓	✓	✓	✓		
Mengurangi permukaan serangan	✓	✓	✓	✓	✓	
Menskalakan untuk menyerap lalu lintas lapisan aplikasi	✓	✓	✓	✓	✓	✓
Mitigasi serangan lapisan 7 (lapisan aplikasi)	✓	✓	✓	✓	✓	✓

Edge AWS	Wilayah AWS					
Isolasi geografis dan dispersi lalu lintas berlebih dan serangan DDoS yang lebih besar	✓	✓	✓			
✓(*): jika digunakan dengan AWS WAF bersama Application Load Balancer						

Cara lain untuk meningkatkan kesiapan Anda untuk merespons dan memitigasi serangan DDoS adalah dengan berlangganan AWS Shield Advanced.

Pelanggan menerima deteksi yang disesuaikan berdasarkan:

- Pola lalu lintas spesifik aplikasi Anda.
- Perlindungan terhadap serangan DDoS Lapisan 7 termasuk AWS WAF tanpa biaya tambahan.
- Akses ke dukungan khusus 24x7 dari AWS SRT.
- Manajemen terpusat kebijakan keamanan melalui AWS Firewall Manager.
- Perlindungan biaya untuk mencegah biaya penskalaan yang dihasilkan dari lonjakan penggunaan terkait DDoS.

Layanan mitigasi DDoS opsional ini membantu melindungi aplikasi yang di-host di Wilayah AWS mana pun. Layanan ini tersedia secara global untuk CloudFront, Route 53, dan Global Accelerator. Menggunakan Shield Advanced dengan alamat IP Elastis memungkinkan Anda melindungi instans Network Load Balancer (NLB) atau Amazon EC2.

Manfaat menggunakan AWS Shield Advanced meliputi:

- Akses ke AWS SRT untuk bantuan terkait memitigasi serangan DDoS yang memengaruhi ketersediaan aplikasi.
- Visibilitas serangan DDoS dengan menggunakan metrik dan alarm AWS Management Console, Amazon CloudWatch, API, dan Amazon.
- Akses ke riwayat semua peristiwa DDoS dari 13 bulan terakhir.
- Akses ke firewall aplikasi web AWS (AWS WAF), tanpa biaya tambahan untuk mitigasi serangan DDoS lapisan aplikasi (jika digunakan dengan Amazon CloudFront atau Application Load Balancer).
- Penentuan acuan dasar otomatis terhadap atribut lalu lintas web, jika digunakan dengan AWS WAF.
- Akses ke AWS Firewall Manager, tanpa biaya tambahan, untuk penegakan kebijakan otomatis.
- Ambang deteksi sensitif yang mengarahkan lalu lintas ke sistem mitigasi DDoS secara lebih awal dan dapat mempersingkat waktu mitigasi serangan terhadap Amazon EC2 atau Network Load Balancer, ketika digunakan dengan alamat IP Elastis.
- Perlindungan biaya yang memungkinkan Anda meminta pengembalian dana terbatas atas biaya terkait penskalaan yang dihasilkan dari serangan DDoS.
- Perjanjian tingkat layanan yang disempurnakan yang dikhususkan untuk pelanggan AWS Shield Advanced.
- Keterlibatan proaktif dari AWS SRT ketika peristiwa Shield terdeteksi.
- Grup perlindungan yang memungkinkan Anda menggabungkan sumber daya, sehingga menyediakan cara mandiri untuk menyesuaikan cakupan deteksi dan mitigasi untuk aplikasi Anda dengan memperlakukan beberapa sumber daya sebagai satu unit. Pengelompokan sumber daya meningkatkan keakuratan deteksi, meminimalkan positif palsu, memudahkan perlindungan otomatis sumber daya yang baru dibuat, dan mempercepat waktu untuk memitigasi serangan terhadap banyak sumber daya yang terdiri dari satu aplikasi. Untuk informasi tentang grup perlindungan, lihat Grup perlindungan Shield Advanced.

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

Topik

Praktik Terbaik untuk Mitigasi DDoS

Pada bagian berikut, masing-masing praktik terbaik yang direkomendasikan untuk mitigasi DDoS dijelaskan secara lebih mendalam. Untuk panduan yang cepat dan mudah diterapkan dalam membangun lapisan mitigasi DDoS untuk aplikasi web statis atau dinamis, lihat Cara Membantu Melindungi Aplikasi Web Dinamis terhadap Serangan DDoS.

Pertahanan Lapisan Infrastruktur (BP1, BP3, BP6, BP7)

Dalam lingkungan pusat data tradisional, Anda dapat memitigasi serangan DDoS lapisan infrastruktur dengan menggunakan teknik seperti kapasitas penyediaan yang berlebih, menerapkan sistem mitigasi DDoS, atau melakukan scrubbing lalu lintas dengan bantuan layanan mitigasi DDoS. Di AWS, kemampuan mitigasi DDoS disediakan secara otomatis; tetapi Anda dapat mengoptimalkan ketahanan DDoS aplikasi Anda dengan membuat pilihan arsitektur yang paling memanfaatkan kemampuan tersebut dan juga memungkinkan Anda menskalakan untuk lalu lintas yang berlebih.

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

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

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

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

Modul yang diperlukan untuk jaringan yang disempurnakan dan set atribut enaSupport yang diperlukan telah disertakan dengan Amazon Linux 2 dan versi terbaru AMI Amazon Linux. Oleh karena itu, jika Anda meluncurkan instans dengan Amazon Linux versi HVM pada jenis instans yang didukung, jaringan yang disempurnakan sudah diaktifkan untuk instans Anda. Untuk informasi selengkapnya, lihat Uji apakah jaringan yang disempurnakan diaktifkan . Untuk informasi selengkapnya tentang cara mengaktifkan jaringan yang disempurnakan, lihat Jaringan yang disempurnakan di Linux.

Amazon EC2 dengan Auto Scaling (BP7)

Cara lain untuk memitigasi serangan lapisan infastruktur dan aplikasi adalah dengan beroperasi pada skala besar. Jika Anda memiliki aplikasi web, Anda dapat menggunakan penyeimbang beban untuk mendistribusikan lalu lintas ke sejumlah instans Amazon EC2 yang disediakan secara berlebih atau dikonfigurasi untuk diskalakan secara otomatis. Instans ini dapat menangani lonjakan lalu lintas mendadak yang terjadi karena alasan apa pun, termasuk flash crowd atau serangan DDoS lapisan aplikasi. Anda dapat mengatur alarm Amazon CloudWatch untuk memulai Auto Scaling agar secara otomatis menskalakan ukuran armada Amazon EC2 Anda sebagai respons terhadap peristiwa yang Anda tetapkan, seperti metrik CPU, RAM, I/O Jaringan, dan bahkan metrik Kustom. 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, negosiasi TLS ditangani oleh distribusi (Amazon CloudFront) atau oleh penyeimbang beban. Fitur-fitur ini membantu melindungi instans Anda agar tidak terkena dampak serangan berbasis TLS dengan menskalakan untuk menangani permintaan yang sah dan serangan penyalahgunaan TLS.

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

Amazon EC2 menyediakan kapasitas komputasi yang dapat diubah ukurannya sehingga Anda dapat dengan cepat menaikkan atau menurunkan skala seiring perubahan persyaratan. Anda dapat

menskalakan secara horizontal dengan menambahkan instans ke aplikasi secara otomatis dengan Menskalakan ukuran grup Amazon EC2 Auto Scaling, dan Anda dapat menskalakan secara vertikal dengan menggunakan jenis instans EC2 yang lebih besar.

Elastic Load Balancing (BP6)

Serangan DDoS besar dapat membanjiri kapasitas instans Amazon EC2 tunggal. Dengan Elastic Load Balancing (ELB), Anda dapat mengurangi risiko kelebihan beban aplikasi Anda dengan mendistribusikan lalu lintas di banyak instans backend. Elastic Load Balancing dapat menskalakan secara otomatis, sehingga memungkinkan Anda mengelola volume yang lebih besar ketika Anda memiliki lalu lintas ekstra yang tidak diantisipasi, misalnya, karena flash crowd atau serangan DDoS. Untuk aplikasi yang dibuat dalam Amazon VPC, ada tiga jenis ELB yang perlu dipertimbangkan, tergantung pada jenis aplikasi Anda: Application Load Balancer (ALB), Classic Load Balancer (CLB), dan Network Load Balancer (NLB).

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

Untuk informasi selengkapnya tentang melindungi aplikasi web dengan Application Load Balancer, lihat Mulai Menggunakan Application Load Balancer

Untuk aplikasi berbasis TCP, Anda dapat menggunakan Network Load Balancer untuk merutekan lalu lintas ke target (misalnya, instans Amazon EC2) pada latensi ultra-rendah. Salah satu pertimbangan utama dengan Network Load Balancer adalah bahwa setiap lalu lintas yang mencapai penyeimbang beban pada listener yang valid akan dialihkan ke target Anda, dan tidak diserap. Anda dapat menggunakan Shield Advanced untuk mengonfigurasi perlindungan DDoS untuk alamat IP Elastis. Ketika alamat IP Elastis ditetapkan per Zona Ketersediaan ke Network Load Balancer, Shield Advanced akan menerapkan perlindungan DDoS yang relevan untuk lalu lintas Network Load Balancer.

Untuk informasi selengkapnya tentang melindungi aplikasi TCP dengan Network Load Balancer, lihat Mulai menggunakan Network Load Balancer

Manfaatkan Lokasi Edge AWS untuk Skala (BP1, BP3)

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

Pengiriman Aplikasi Web di Edge (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 waktu untuk tayang (TTL) yang bervariasi dapat digunakan untuk mengeluarkan lalu lintas dari asal Anda, bahkan jika Anda tidak menyajikan konten yang dapat di-cache. Penggunaan fitur CloudFront ini mengurangi jumlah permintaan dan koneksi TCP yang kembali ke asal Anda, sehingga membantu melindungi aplikasi web Anda dari banjir HTTP. CloudFront hanya menerima koneksi yang terbentuk dengan baik, yang membantu mencegah banyak serangan DDoS umum, seperti banjir SYN dan serangan refleksi UDP, agar tidak mencapai asal Anda. Serangan DDoS juga terisolasi secara geografis di dekat sumbernya, yang mencegah lalu lintas berdampak pada lokasi lain. Kemampuan ini dapat sangat meningkatkan kemampuan Anda untuk terus menyajikan lalu lintas kepada pengguna selama serangan DDoS besar. Anda dapat menggunakan CloudFront untuk melindungi asal di AWS atau di tempat lain di internet.

Jika Anda menggunakan Amazon S3 untuk menyajikan konten statis di internet, AWS merekomendasikan Anda untuk menggunakan Amazon CloudFront untuk melindungi bucket Anda. Anda dapat menggunakan identitas akses asal (OAI) untuk memastikan bahwa pengguna hanya mengakses objek Anda dengan menggunakan URL CloudFront.

Untuk informasi selengkapnya tentang OAI, lihat Membatasi akses ke konten Amazon S3 dengan menggunakan identitas akses asal.

Untuk informasi selengkapnya tentang melindungi dan mengoptimalkan performa aplikasi web dengan Amazon CloudFront, lihat Mulai Menggunakan CloudFront.

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

Global Accelerator adalah layanan jaringan yang meningkatkan ketersediaan dan performa lalu lintas pengguna hingga 60%. Hal ini dilakukan dengan memasukkan lalu lintas di lokasi edge yang paling dekat dengan pengguna Anda dan merutekannya melalui infrastruktur jaringan global AWS ke aplikasi Anda, baik itu berjalan dalam satu atau beberapa Wilayah AWS.

Global Accelerator merutekan lalu lintas TCP dan UDP ke titik akhir yang optimal berdasarkan performa di Wilayah AWS yang terdekat dengan pengguna. Jika terjadi kegagalan aplikasi, Global Accelerator menyediakan failover ke titik akhir terbaik berikutnya dalam waktu 30 detik. Global Accelerator menggunakan kapasitas luas jaringan AWS global dan integrasi dengan Shield, seperti kemampuan proksi SYN stateless yang menahan percobaan koneksi baru dan hanya melayani pengguna akhir yang sah, untuk melindungi aplikasi.

Anda dapat menerapkan arsitektur yang tahan terhadap DDoS 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 ke daftar izinkan di firewall mereka dan tidak digunakan oleh pelanggan AWS lain. Dalam skenario ini, Anda dapat menggunakan Global Accelerator untuk melindungi aplikasi web yang berjalan di Application Load Balancer dan AWS WAF untuk juga mendeteksi dan memitigasi banjir permintaan lapisan aplikasi web.

Untuk informasi selengkapnya tentang melindungi dan mengoptimalkan performa lalu lintas jaringan menggunakan Global Accelerator, lihat Mulai menggunakan Global Accelerator.

Resolusi Nama Domain di Edge (BP3)

Amazon Route 53 adalah layanan Sistem Nama Domain (DNS) yang sangat tersedia dan dapat diskalakan yang dapat digunakan untuk mengarahkan lalu lintas ke aplikasi web Anda. Ini mencakup fitur-fitur canggih seperti Traffic Flow, Health Checks dan Monitoring, Latency-Based Routing, dan Geo DNS. Fitur-fitur canggih ini memungkinkan Anda mengontrol bagaimana layanan merespons permintaan DNS untuk meningkatkan performa aplikasi web Anda dan untuk menghindari pemadaman situs.

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

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

Anycast striping memungkinkan setiap permintaan DNS dilayani oleh lokasi yang paling optimal mendispersi 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 kueri DNS, dan memprioritaskan permintaan dari pengguna yang diketahui dapat diandalkan.

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

Pertahanan Lapisan Aplikasi (BP1, BP2)

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

Deteksi dan Filter Permintaan Web Berbahaya (BP1, BP2)

Saat aplikasi berjalan di AWS, Anda dapat memanfaatkan Amazon CloudFront dan AWS WAF untuk membantu bertahan terhadap serangan DDoS lapisan aplikasi.

Amazon CloudFront memungkinkan Anda menyimpan konten statis dan menyajikannya dari lokasi edge AWS, yang dapat membantu mengurangi beban di asal Anda. Ini juga dapat membantu mengurangi beban server dengan mencegah lalu lintas non-web mencapai asal Anda. Selain itu, CloudFront dapat secara otomatis menutup koneksi dari penyerang slow reading atau slow writing (misalnya, Slowloris).

Dengan menggunakan AWS WAF, Anda dapat mengonfigurasi daftar kontrol akses web (ACL Web) pada distribusi CloudFront atau Application Load Balancer untuk memfilter dan memblokir permintaan berdasarkan tanda tangan permintaan. Setiap ACL Web terdiri dari aturan yang dapat Anda konfigurasikan ke kecocokan string atau kecocokan regex dengan satu atau beberapa atribut

permintaan, seperti Uniform Resource Identifier (URI), string kueri, metode HTTP, atau kunci header. Selain itu, dengan menggunakan aturan berbasis laju AWS WAF, Anda dapat secara otomatis memblokir alamat IP pelaku kejahatan saat permintaan yang cocok dengan aturan melebihi ambang batas yang Anda tetapkan.

Permintaan dari alamat IP klien yang melanggar akan menerima respons kesalahan 403 Forbidden dan akan tetap diblokir sampai laju permintaan turun di bawah ambang batas. Hal ini berguna untuk memitigasi serangan banjir HTTP yang menyamar sebagai lalu lintas web biasa. Untuk memblokir serangan berdasarkan reputasi alamat IP, Anda dapat membuat aturan menggunakan kondisi pencocokan IP atau menggunakan Managed Rules untuk AWS WAF yang ditawarkan oleh penjual di AWS Marketplace. AWS WAF secara langsung menawarkan AWS Managed Rules sebagai layanan terkelola, tempat Anda dapat memilih grup aturan reputasi IP. Grup aturan daftar reputasi IP Amazon berisi aturan yang didasarkan pada intelijen ancaman internal Amazon. Ini berguna jika Anda ingin memblokir alamat IP yang biasanya terkait dengan bot atau ancaman lainnya. Grup aturan daftar IP Anonim berisi aturan untuk memblokir permintaan dari layanan yang memungkinkan obfuskasi identitas pengakses (viewer). Ini termasuk permintaan dari VPN, proksi, node Tor, dan platform cloud (termasuk AWS). AWS WAF dan CloudFront juga memungkinkan Anda mengatur pembatasan geografis untuk memblokir atau mengizinkan permintaan dari negara tertentu. Ini dapat membantu memblokir serangan dari lokasi geografis yang penggunanya tidak diharapkan untuk Anda layani.

Untuk membantu mengidentifikasi permintaan berbahaya, tinjau log server web Anda atau gunakan fitur pencatatan log dan Sampel Permintaan AWS WAF. Dengan mengaktifkan pencatatan log AWS WAF, Anda mendapatkan informasi mendetail tentang lalu lintas yang dianalisis oleh ACL Web. AWS WAF mendukung pemfilteran log, sehingga memungkinkan Anda menentukan permintaan web mana yang dicatat dan permintaan mana yang dihapus dari log setelah pemeriksaan.

Informasi yang tercatat dalam log mencakup waktu saat AWS WAF menerima permintaan dari sumber daya AWS Anda, informasi mendetail tentang permintaan, dan tindakan pencocokan untuk setiap aturan yang diminta. Sampel Permintaan memberikan detail tentang permintaan dalam tiga jam terakhir yang cocok dengan salah satu aturan AWS WAF Anda. 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 memitigasi serangan cache-busting terhadap asal Anda.

Jika berlangganan AWS Shield Advanced, Anda dapat melibatkan Tim Respons AWS Shield (SRT) untuk membantu Anda membuat aturan untuk memitigasi serangan yang merugikan ketersediaan

aplikasi Anda. Anda dapat memberikan akses terbatas untuk AWS SRT ke API Shield Advanced dan AWS WAF di akun Anda. AWS SRT mengakses API ini untuk menerapkan mitigasi pada akun Anda hanya dengan otorisasi eksplisit Anda. Untuk informasi selengkapnya, lihat bagian Dukungan di dokumen ini.

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

Untuk informasi selengkapnya tentang:

- AWS Managed Rules untuk AWS WAF, lihat AWS Managed Rules untuk AWS WAF.
- Menggunakan pembatasan geografis untuk membatasi akses ke distribusi CloudFront Anda, lihat Membatasi distribusi geografis konten Anda.
- Menggunakan AWS WAF, lihat
  - Mulai menggunakan AWS WAF
  - Mencatat log informasi lalu lintas ACL web
  - Melihat sampel permintaan web
- Mengonfigurasi aturan berbasis laju, lihat Melindungi Situs Web dan Layanan Menggunakan Aturan Berbasis Laju untuk AWS WAF
- Cara mengelola deployment aturan AWS WAF di seluruh sumber daya AWS Anda dengan Firewall Manager, lihat
  - Mulai menggunakan kebijakan Firewall Manager AWS WAF.
  - Mulai menggunakan kebijakan Firewall Manager Shield Advanced.

Pengurangan Permukaan Serangan

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

Misalnya, jika Anda tidak mengharapkan pengguna 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.

Pada bagian berikut, AWS memberikan praktik terbaik untuk memandu Anda dalam mengurangi permukaan serangan dan membatasi ekspos internet pada aplikasi Anda.

Topik

Melakukan Obfuskasi Sumber Daya AWS (BP1, BP4, BP5)

Biasanya, pengguna dapat dengan cepat dan mudah menggunakan aplikasi tanpa memerlukan sumber daya AWS yang sepenuhnya terekspos ke internet. Misalnya, ketika Anda memiliki instans Amazon EC2 di belakang Elastic Load Balancing, instans itu sendiri mungkin tidak perlu diakses publik. Sebagai gantinya, Anda dapat memberi pengguna akses ke Elastic Load Balancing pada port TCP tertentu dan hanya mengizinkan Elastic Load Balancing untuk berkomunikasi dengan instans. Anda dapat mengaturnya dengan mengonfigurasi Grup Keamanan dan Daftar Kontrol Akses Jaringan (NACL) dalam Amazon Virtual Private Cloud (Amazon VPC) Anda. Amazon VPC memungkinkan Anda menyediakan bagian yang terisolasi secara logis dari AWS Cloud, tempat Anda dapat meluncurkan sumber daya AWS pada jaringan virtual yang ditentukan.

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

Grup Keamanan dan Daftar Kontrol Akses Jaringan (ACL Jaringan) (BP5)

Anda dapat memilih apakah akan menentukan grup keamanan saat meluncurkan instans atau mengaitkan instans dengan grup keamanan di lain waktu. Semua lalu lintas internet ke grup keamanan ditolak secara implisit kecuali jika Anda membuat aturan izinkan untuk mengizinkan lalu lintas. Misalnya, jika Anda memiliki aplikasi web yang menggunakan Elastic Load Balancing dan beberapa instans Amazon EC2, Anda dapat memutuskan untuk membuat satu grup keamanan untuk Elastic Load Balancing (grup keamanan Elastic Load Balancing) dan satu untuk instans (grup keamanan server aplikasi web). Anda kemudian dapat membuat aturan izinkan untuk mengizinkan lalu lintas internet ke grup keamanan ELB, dan aturan lain untuk mengizinkan lalu lintas dari grup keamanan ELB ke grup keamanan server aplikasi web. Hal ini memastikan bahwa lalu lintas internet tidak dapat berkomunikasi secara langsung dengan instans Amazon EC2 Anda, yang membuatnya lebih sulit bagi penyerang untuk mempelajari dan memengaruhi aplikasi Anda.

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

Jika Anda berlangganan AWS Shield Advanced, Anda dapat mendaftarkan alamat IP Elastis sebagai Sumber Daya Terproteksi. Serangan DDoS terhadap alamat IP Elastis yang telah terdaftar sebagai Sumber Daya Terproteksi akan terdeteksi lebih cepat, yang dapat menghasilkan waktu mitigasi yang lebih cepat. Ketika serangan terdeteksi, sistem mitigasi DDoS membaca ACL jaringan yang sesuai dengan IP Elastis yang ditargetkan dan memberlakukannya di batas jaringan AWS. Hal ini secara signifikan mengurangi risiko dampak dari sejumlah serangan DDoS lapisan infrastruktur.

Untuk informasi selengkapnya tentang mengonfigurasi Grup Keamanan dan ACL jaringan untuk mengoptimalkan ketahanan DDoS, lihat Cara Membantu Melakukan Persiapan untuk Serangan DDoS dengan Mengurangi Permukaan Serangan.

Untuk informasi selengkapnya tentang menggunakan Shield Advanced dengan alamat IP Elastis sebagai Sumber Daya Terproteksi, lihat langkah-langkah untuk Berlangganan AWS Shield Advanced.

Melindungi Asal Anda (BP1, BP5)

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

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

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

Sebagai alternatif, Anda dapat menggunakan fungsi AWS Lambda untuk memperbarui aturan grup keamanan secara otomatis agar hanya mengizinkan lalu lintas CloudFront. Hal 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, lihat header X-Shared-Secret, lihat Cara Memperbarui Grup Keamanan Anda Secara Otomatis untuk Amazon CloudFront dan AWS WAF Menggunakan AWS Lambda.

Melindungi Titik Akhir API (BP4)

Biasanya, ketika Anda harus mengekspos API ke publik, ada risiko bahwa frontend API 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 frontend API dan Anda dapat melakukan obfuskasi komponen lain dari aplikasi Anda. Dengan mempersulit deteksi terhadap komponen aplikasi Anda, Anda dapat membantu mencegah sumber daya AWS tersebut ditargetkan oleh serangan DDoS.

Saat menggunakan Amazon API Gateway, Anda dapat memilih dari dua jenis titik akhir API. Yang pertama adalah opsi default: titik akhir API yang dioptimalkan edge yang diakses melalui distribusi Amazon CloudFront. Namun, distribusi ini dibuat dan dikelola oleh API Gateway, jadi

Anda tidak memiliki kontrol atas distribusi tersebut. Opsi kedua adalah menggunakan titik akhir API regional yang diakses dari wilayah AWS yang sama, tempat API REST Anda digunakan. AWS merekomendasikan agar Anda menggunakan titik akhir jenis kedua dan menghubungkannya dengan distribusi Amazon CloudFront Anda sendiri. Hal ini memberi Anda kontrol atas distribusi Amazon CloudFront dan kemampuan untuk menggunakan AWS WAF untuk perlindungan lapisan aplikasi. Mode ini memberi Anda akses ke kapasitas mitigasi DDoS yang diskalakan di seluruh jaringan edge global AWS.

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 konten dinamis dan melewati proses caching konten.
- Lindungi API Gateway Anda terhadap akses langsung dengan mengonfigurasi distribusi untuk menyertakan header kustom asal `x-api-key`, dengan menetapkan nilai kunci API di API Gateway.
- Lindungi backend dari lalu lintas berlebih dengan mengonfigurasi batas laju standar atau burst untuk setiap metode di API REST Anda.

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

Teknik Operasional

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

Topik

Visibilitas

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

Jika Anda mengikuti arsitektur referensi yang tahan terhadap DDoS saat merancang aplikasi Anda, serangan lapisan infrastruktur umum akan diblokir sebelum mencapai aplikasi Anda. Jika berlangganan AWS Shield Advanced, Anda akan memiliki akses ke sejumlah metrik CloudWatch yang dapat menunjukkan bahwa aplikasi Anda sedang ditargetkan. Misalnya, Anda dapat mengonfigurasi alarm untuk memberi tahu Anda saat terjadi serangan DDoS yang sedang berlangsung, sehingga Anda dapat memeriksa kondisi aplikasi Anda dan memutuskan apakah akan melibatkan AWS SRT. Anda dapat mengonfigurasi metrik `DDoSDetected` untuk memberi tahu Anda jika serangan telah terdeteksi. Jika Anda ingin diberi tahu berdasarkan volume serangan, Anda juga dapat menggunakan metrik `DDoSAttackBitsPerSecond`, `DDoSAttackPacketsPerSecond`, atau `DDoSAttackRequestsPerSecond`. 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.

Sebuah serangan lapisan aplikasi dapat memicu banyak metrik Amazon CloudWatch. Jika Anda menggunakan AWS WAF, Anda dapat menggunakan CloudWatch untuk memantau dan mengaktifkan alarm pada jika ada kenaikan dalam permintaan yang telah Anda tetapkan di AWS WAF agar kemudian diizinkan, dihitung, atau diblokir. Hal ini memungkinkan Anda menerima pemberitahuan jika tingkat lalu lintas melebihi jumlah yang dapat ditangani aplikasi Anda. Anda juga dapat menggunakan metrik Amazon CloudFront, Amazon Route 53, Application Load Balancer, Network Load Balancer, Amazon EC2, dan Auto Scaling yang dilacak di CloudWatch untuk mendeteksi perubahan yang dapat menunjukkan serangan DDoS.

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

Tabel 3 - Metrik Amazon CloudWatch yang Direkomendasikan

Topik	Metrik	Deskripsi
AWS Shield Advanced	DDoSDetected	Menunjukkan peristiwa DDoS untuk Amazon Resource Name (ARN) tertentu.
AWS Shield Advanced	DDoSAttackBitsPerSecond	Jumlah bita yang diamati selama peristiwa DDoS untuk ARN tertentu. Metrik ini hanya tersedia untuk peristiwa DDoS lapisan 3/4.
AWS Shield Advanced	DDoSAttackPacketsPerSecond	Jumlah paket yang diamati selama peristiwa DDoS untuk ARN tertentu. Metrik ini hanya tersedia untuk peristiwa DDoS lapisan 3/4.
AWS Shield Advanced	DDoSAttackRequestsPerSecond	Jumlah permintaan yang diamati selama peristiwa DDoS untuk ARN tertentu. Metrik ini hanya tersedia untuk peristiwa DDoS lapisan 7 dan hanya dilaporkan untuk

Topik	Metrik	Deskripsi
		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 diteruskan. Ini hanya digunakan untuk permintaan yang melewati evaluasi grup aturan tanpa cocok dengan salah satu aturan grup aturan.
Amazon CloudFront	Permintaan	Jumlah permintaan HTTP/S.
Amazon CloudFront	TotalErrorRate	Persentase dari semua permintaan yang kode status HTTP-nya adalah 4xx atau 5xx.
Amazon Route 53	HealthCheckStatus	Status titik akhir pemeriksaan kondisi.
Application Load Balancer	ActiveConnectionCount	Jumlah total koneksi TCP bersamaan yang aktif dari klien ke penyeimbang beban, dan dari penyeimbang beban ke target.

Topik	Metrik	Deskripsi
Application Load Balancer	ConsumedLCUs	Jumlah unit kapasitas penyeimbang beban (LCU) yang digunakan oleh penyeimbang beban Anda.
Application Load Balancer	HTTPCode_ELB_4XX_Count HTTPCode_ELB_5XX_Count	Jumlah kode kesalahan klien HTTP 4xx atau 5xx yang dihasilkan oleh penyeimbang beban.
Application Load Balancer	NewConnectionCount	Jumlah total koneksi TCP baru yang dibuat dari klien ke penyeimbang beban, dan dari penyeimbang beban ke target.
Application Load Balancer	ProcessedBytes	Jumlah bita diproses oleh penyeimbang beban.
Application Load Balancer	RejectedConnectionCount	Jumlah koneksi yang ditolak karena penyeimbang beban telah mencapai jumlah maksimum koneksi.
Application Load Balancer	RequestCount	Jumlah permintaan yang diproses.
Application Load Balancer	TargetConnectionErrorCount	Jumlah koneksi yang tidak berhasil dibuat antara penyeimbang beban dan target.
Application Load Balancer	TargetResponseTime	Waktu berlalu, dalam detik, setelah permintaan meninggal kan penyeimbang beban sampai respons dari target diterima.

Topik	Metrik	Deskripsi
Application Load Balancer	UnHealthyHostCount	Jumlah target yang dianggap tidak berkondisi baik.
Network Load Balancer	ActiveFlowCount	Jumlah total aliran (atau koneksi) TCP bersamaan dari klien ke target.
Network Load Balancer	ConsumedLCUs	Jumlah unit kapasitas penyeimbang beban (LCU) yang digunakan oleh penyeimbang beban Anda.
Network Load Balancer	NewFlowCount	Jumlah total aliran (atau koneksi) TCP baru yang dibuat dari klien ke target dalam periode waktu tertentu.
Network Load Balancer	ProcessedBytes	Jumlah total bita yang diproses oleh penyeimbang beban, termasuk header TCP/IP.
Global Accelerator	NewFlowCount	Jumlah total aliran (atau koneksi) TCP dan UDP baru yang dibuat dari klien ke titik akhir dalam periode waktu tertentu.
Global Accelerator	ProcessedBytesIn	Jumlah total bita masuk diproses oleh akselerator, termasuk header TCP/IP.
Auto Scaling	GroupMaxSize	Ukuran maksimum grup Auto Scaling.

Topik	Metrik	Deskripsi
Amazon EC2	CPUUtilization	Persentase unit komputasi EC2 yang dialokasikan yang saat ini sedang digunakan.
Amazon EC2	NetworkIn	Jumlah bita yang diterima oleh instans pada semua antarmuka jaringan.

Untuk informasi selengkapnya tentang penggunaan Amazon CloudWatch untuk mendeteksi serangan DDoS pada aplikasi Anda, lihat Mulai Menggunakan Amazon CloudWatch.

Untuk menjelajahi contoh dasbor yang dibuat menggunakan beberapa metrik dari tabel sebelumnya, lihat Sistem pemantauan acuan dasar kustom

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

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

Jika Anda berlangganan AWS Shield Advanced, dasbor layanan akan 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 Anda yang dilindungi beserta sejumlah dimensi. Ketika anomali terdeteksi, AWS Shield membuat sebuah peristiwa dan melaporkan dimensi lalu lintas, tempat anomali diamati. Dengan mitigasi yang diterapkan, hal ini melindungi sumber daya Anda agar tidak menerima lalu lintas berlebih dan lalu lintas yang cocok dengan tanda tangan peristiwa DDoS yang dikenal.

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

Metrik kontributor teratas jaringan memberikan wawasan terkait asal lalu lintas selama peristiwa yang terdeteksi. Anda dapat melihat kontributor volume tertinggi dan mengurutkan berdasarkan aspek seperti protokol, port sumber, dan flag TCP. Metrik kontributor teratas mencakup metrik untuk semua lalu lintas yang diamati pada sumber daya beserta berbagai dimensi. Hal ini menyediakan dimensi metrik tambahan yang dapat Anda gunakan untuk memahami lalu lintas jaringan yang dikirim ke sumber daya Anda selama peristiwa berlangsung.

Dasbor layanan juga mencakup detail tentang tindakan yang dilakukan secara otomatis untuk memitigasi serangan DDoS. Informasi ini memudahkan untuk menyelidiki anomali, mengeksplorasi dimensi lalu lintas, dan lebih memahami tindakan yang diambil oleh Shield Advanced untuk melindungi ketersediaan Anda.

Alat lain yang dapat membantu Anda mendapatkan visibilitas ke lalu lintas yang menargetkan aplikasi Anda adalah VPC Flow Logs. Pada jaringan tradisional, Anda dapat menggunakan log aliran jaringan untuk memecahkan masalah konektivitas dan keamanan serta memastikan bahwa aturan akses jaringan berfungsi seperti yang diharapkan. Dengan menggunakan VPC Flow Logs, Anda dapat menangkap informasi tentang lalu lintas IP yang menuju ke dan berasal dari antarmuka jaringan di VPC Anda.

Setiap catatan log aliran meliputi: alamat IP sumber dan tujuan, port sumber dan tujuan, protokol, dan jumlah paket dan bita yang ditransfer selama periode tangkapan data. Anda dapat menggunakan informasi ini untuk membantu mengidentifikasi anomali dalam lalu lintas jaringan dan mengidentifikasi vektor serangan tertentu. Misalnya, sebagian besar serangan refleksi UDP memiliki port sumber tertentu, seperti port sumber 53 untuk refleksi DNS. Ini adalah tanda tangan serangan yang jelas yang dapat Anda identifikasi dalam catatan log aliran. Sebagai respons, Anda dapat memilih untuk memblokir port sumber tertentu di tingkat instans atau membuat aturan ACL jaringan untuk memblokir seluruh protokol jika aplikasi Anda tidak memerlukannya.

Untuk informasi selengkapnya tentang menggunakan VPC Flow Logs untuk mengidentifikasi anomali jaringan dan vektor serangan DDoS, lihat VPC Flow Logs dan VPC Flow Logs – Catat Log dan Lihat Aliran Lalu Lintas Jaringan.

Manajemen visibilitas dan perlindungan di beberapa akun

Dalam skenario saat Anda beroperasi di beberapa akun AWS dan memiliki beberapa komponen untuk dilindungi, menggunakan teknik yang memungkinkan Anda beroperasi dalam skala besar dan menghemat biaya operasional akan meningkatkan kemampuan mitigasi Anda. Saat mengelola sumber daya yang dilindungi AWS Shield Advanced di beberapa akun, Anda dapat menyiapkan

pemantauan terpusat dengan menggunakan AWS Firewall Manager dan AWS Security Hub. Dengan Firewall Manager, Anda dapat membuat kebijakan keamanan yang memberlakukan kepatuhan perlindungan DDoS 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 terintegrasi secara otomatis dengan Firewall Manager, sehingga memungkinkan pelanggan Shield Advanced melihat temuan keamanan dalam satu dasbor, bersama peringatan keamanan dan status kepatuhan prioritas tinggi lainnya. Misalnya, ketika Shield Advanced mendeteksi lalu lintas beranomali yang mengarah ke sumber daya yang dilindungi di akun AWS mana pun yang termasuk dalam cakupan, temuan ini akan terlihat di konsol Security Hub. Jika dikonfigurasi, Firewall Manager dapat secara otomatis memastikan kepatuhan sumber daya ini dengan menjadikannya sebagai sumber daya yang dilindungi Shield Advanced, dan kemudian memperbarui Security Hub ketika sumber daya memiliki status patuh.

Untuk informasi selengkapnya tentang pemantauan terpusat sumber daya yang dilindungi Shield, lihat Siapkan pemantauan terpusat untuk peristiwa DDoS dan perbaiki sumber daya yang tidak patuh secara otomatis.

Dukungan

Jika Anda mengalami serangan, Anda juga dapat memperoleh manfaat dari dukungan AWS dalam menilai ancaman dan meninjau arsitektur aplikasi Anda, atau Anda sebaiknya meminta bantuan lain. Penting untuk membuat rencana respons untuk serangan DDoS sebelum peristiwa yang sebenarnya terjadi. Praktik terbaik yang diuraikan dalam laporan ini dimaksudkan untuk menjadi tindakan proaktif yang Anda terapkan sebelum meluncurkan aplikasi, tetapi serangan DDoS terhadap aplikasi Anda mungkin masih terjadi. Tinjau opsi di bagian ini untuk menentukan sumber daya dukungan yang paling sesuai untuk skenario Anda. Tim akun Anda dapat mengevaluasi kasus penggunaan dan aplikasi Anda, dan membantu terkait pertanyaan atau tantangan tertentu yang Anda miliki.

Jika Anda menjalankan beban kerja produksi di AWS, pertimbangkan untuk berlangganan Business Support, yang memberi Anda akses 24/7 ke Rekayasawan Dukungan Cloud yang dapat membantu masalah serangan DDoS. Jika Anda menjalankan beban kerja yang sangat penting, pertimbangkan Enterprise Support yang menyediakan kemampuan untuk melaporkan kasus kritis dan menerima respons tercepat dari Rekayasawan Dukungan Cloud Senior.

Jika berlangganan AWS Shield Advanced dan juga berlangganan Business Support atau Enterprise Support, Anda dapat mengonfigurasi keterlibatan proaktif Shield. Hal ini memungkinkan Anda

mengonfigurasi pemeriksaan kondisi, mengaitkan ke sumber daya Anda, dan memberikan informasi kontak operasi 24/7. Ketika Shield mendeteksi tanda-tanda DDoS dan pemeriksaan kondisi aplikasi Anda menunjukkan tanda-tanda penurunan, AWS SRT akan secara proaktif menghubungi Anda. Ini adalah model keterlibatan kami yang direkomendasikan karena memungkinkan waktu respons AWS SRT tercepat dan memberdayakan AWS SRT untuk memulai pemecahan masalah bahkan sebelum menghubungi Anda.

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

Menyelesaikan konfigurasi keterlibatan proaktif termasuk menambahkan detail kontak di konsol Shield. AWS SRT akan menggunakan informasi ini untuk menghubungi Anda. Anda dapat mengonfigurasi hingga 10 kontak dan memberikan catatan tambahan jika Anda memiliki persyaratan atau preferensi kontak tertentu. Kontak keterlibatan proaktif harus memegang peran dengan waktu kerja 24/7, seperti pusat operasi keamanan atau individu yang selalu siaga.

Anda dapat mengaktifkan keterlibatan proaktif untuk semua sumber daya atau untuk sumber daya produksi utama tertentu yang sangat mementingkan waktu respons. Hal ini dilakukan dengan menetapkan pemeriksaan kondisi hanya ke sumber daya ini.

Anda juga dapat mengeskalasikan ke AWS SRT dengan membuat kasus AWS Support menggunakan konsol AWS Support atau API Support jika Anda memiliki peristiwa terkait DDoS yang memengaruhi ketersediaan aplikasi Anda.

Kesimpulan

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

Kontributor

Kontributor dokumen ini meliputi:

- Jeffrey Lyon, Kepala Operasi Teknis (Lead of Technical Operations), Perlindungan Perimeter AWS
- Rodrigo Ferroni, TAM Spesialis Keamanan AWS (AWS Security Specialist TAM)
- Dmitriy Novikov, Arsitek Solusi AWS (AWS Solutions Architect)
- Achraf Souk, Arsitek Solusi AWS (AWS Solutions Architect)
- Yoshihisa Nakatani, Arsitek Solusi AWS (AWS Solutions Architect)

Sumber daya

Bacaan Lebih Lanjut:

- Praktik Terbaik untuk Mitigasi DDoS AWS
- Panduan untuk Menerapkan AWS WAF
- SID324 – re:Invent 2017: Mengotomatisasi Respons DDoS di Cloud
- CTD304 - re:Invent 2017: Perjalanan Dow Jones & Wall Street Journal untuk Mengelola Lonjakan Lalu Lintas Sambil Mengurangi Ancaman DDoS & Lapisan Aplikasi
- CTD310 - re:Invent 2017: Beroperasi di Edge, Lebih Aman dari yang Anda Pikirkan! Membangun dengan Kuat Menggunakan Amazon CloudFront, AWS Shield, dan AWS WAF
- SEC407 - re:Invent 2019: Pendekatan pertahanan yang mendalam untuk membangun aplikasi web
- SEC321 - re:Invent 2020: Menjadi yang terdepan dengan eskalasi Tim Respons DDoS
- William Hill: Perlindungan DDoS performa tinggi dengan AWS

Revisi Dokumen

Untuk mendapatkan notifikasi tentang pembaruan laporan resmi ini, sebaiknya berlangganan umpan RSS.

perubahan-riwayat-pembaruan	deskripsi-riwayat-pembaruan	tanggal-riwayat-pembaruan
Pembaruan laporan resmi	Memperbarui untuk menyertakan rekomendasi dan fitur terbaru. AWS Global Accelerator ditambahkan sebagai bagian dari perlindungan komprehensif di edge. AWS Firewall Manager untuk pemantauan terpusat peristiwa DDoS dan perbaikan otomatis sumber daya yang tidak mematuhi aturan.	21 September 2021
Pembaruan laporan resmi	Memperbarui untuk memperjelas cache busting di bagian Mendeteksi dan Memfilter Permintaan Web Berbahaya (BP1, BP2), serta penggunaan ELB dan ALB di bagian Menskalakan untuk Menyerap (BP6). Memperbarui diagram dan Tabel 2, menandai “Pilihan Wilayah”. sebagai BP8. Memperbarui bagian BP7 dengan detail lebih lanjut.	18 Desember 2019
Pembaruan laporan resmi	Memperbarui untuk menyertakan pencatatan log AWS WAF sebagai praktik terbaik.	1 Desember 2018

Pembaruan laporan resmi	Memperbarui untuk menyertakan AWS Shield, fitur AWS WAF, AWS Firewall Manager, dan praktik terbaik terkait.	1 Juni 2018
Pembaruan laporan resmi	Menambahkan panduan arsitektur preskriptif dan memperbarui untuk menyertakan AWS WAF.	1 Juni 2016
Publikasi awal	Laporan resmi dipublikasikan.	1 Juni 2015

Pemberitahuan

Pelanggan bertanggung jawab untuk membuat penilaian independen mereka sendiri atas informasi dalam dokumen ini. Dokumen ini: (a) hanya disediakan sebagai informasi, (b) berisi penawaran produk dan praktik AWS saat ini, yang dapat berubah tanpa pemberitahuan, dan (c) tidak menjadi komitmen atau jaminan apa pun dari AWS dan afiliasi, pemasok, atau pemberi lisensinya. Produk atau layanan AWS disediakan “sebagaimana adanya” tanpa jaminan, representasi, atau ketentuan apa pun, baik tersurat maupun tersirat. 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.