AWS Panduan keputusan

AWS WAF atau AWS Shield?

AWS WAF atau AWS Shield?: AWS Panduan keputusan

Table of Contents

AWS WAF atau AWS Shield?

Pahami perbedaannya dan pilih yang tepat untuk Anda

Tujuan	Untuk membantu Anda menentukan apakah AWS WAF atau AWS Shield memenuhi kebutuhan Anda akan layanan keamanan aplikasi web.
Terakhir diperbarui	September 17, 2024
Layanan yang tercakup	• AWS WAF • AWS Shield

Pengantar

AWS WAF(Web Application Firewall) dan AWS Shielddapat membantu Anda melindungi aplikasi web Anda terhadap berbagai jenis serangan siber, seperti serangan Distributed Denial of Service (DDoS) dan kerentanan aplikasi web lainnya.

- AWS WAFberfokus pada melindungi aplikasi web Anda dari eksploitasi web umum. Gunakan AWS WAF untuk membuat aturan keamanan web yang dapat disesuaikan untuk memfilter lalu lintas berbahaya, melindungi terhadap serangan seperti injeksi SQL dan skrip lintas situs (XSS), dan berintegrasi dengan yang lain. Layanan AWS
- AWS Shieldadalah layanan perlindungan DDo S terkelola. Gunakan AWS Shield untuk mengaktifkan deteksi selalu aktif dan mitigasi otomatis, dan melindungi terhadap serangan DDo S umum di jaringan dan lapisan transportasi.

Saat AWS Shield bertahan melawan serangan tingkat jaringan skala besar, dengan AWS Shield Advanced, Anda dapat mengaitkan ACL AWS WAF web dengan sumber daya untuk memberikan perlindungan pada lapisan aplikasi. AWS WAF memberikan perlindungan yang lebih terperinci terhadap kerentanan khusus aplikasi. Gunakan kedua layanan bersama-sama untuk strategi pertahanan berlapis-lapis, melindungi aplikasi Anda dari berbagai ancaman potensial yang lebih luas di berbagai lapisan jaringan.

Berikut adalah pandangan tingkat tinggi tentang perbedaan utama antara layanan ini.

Kategori	 AWS WAF	 AWS Shield
Tujuan Utama	Melindungi terhadap eksploitasi pada aplikasi web (seperti injeksi SQL atau XSS)	Melindungi terhadap serangan DDo S (seperti banjir SYN atau UDP)
Lapisan perlindungan	Lapisan aplikasi (L7)	Jaringan, transportasi, dan lapisan aplikasi (L3/L4/L7)
Deployment	Harus diatur secara eksplisit	AWS Shield Perlindungan standar disertakan untuk semua akun pelanggan
Kustomisasi	Sangat dapat disesuaikan dengan aturan khusus	Aktifkan atau nonaktifkan AWS Shield Advanced, dengan opsi untuk mengaktifkan mitigasi otomatis perlindungan lapisan DDo S aplikasi
Aturan Terkelola	Termasuk Aturan AWS Terkelola dan aturan pihak ketiga	Tidak berlaku
Model penentuan harga	Pay-as-you-go harga berdasarkan jumlah aturan dan permintaan	AWS Shield Standar termasuk; AWS Shield Advanced menimbulkan biaya tambahan
Tim Respons Serangan	Tidak berlaku	Tersedia dengan AWS Shield Advanced (Tim Respons 24/7 DDo S)
Pemantauan waktu nyata	Ya	Ya

Kategori	AWS WAF	AWS Shield
Inspeksi Lalu Lintas	Tingkat permintaan	Tingkat paket

Perbedaan antara AWS WAF dan AWS Shield

Jelajahi delapan area utama perbedaan antara AWS Shield dan AWS WAF, yang mencakup lapisan perlindungan, penyebaran, penyesuaian, aturan terkelola, model penetapan harga, tim respons serangan, pemantauan waktu nyata, dan inspeksi lalu lintas.

Layer of protection

AWS WAF

- Beroperasi pada layer aplikasi (Layer 7). Ini melindungi aplikasi web dengan memfilter dan memantau HTTP/S lalu lintas. AWS WAF bertahan terhadap eksploitasi web umum seperti injeksi SQL, cross-site scripting (XSS), dan cross-site request forgery (CSRF). Anda dapat membuat aturan khusus untuk memblokir permintaan berbahaya berdasarkan berbagai kriteria seperti alamat IP, string kueri, dan header.

AWS Shield

- Beroperasi terutama pada lapisan jaringan (Layer 3) dan transport (Layer 4). Ini dirancang untuk mengurangi serangan Distributed Denial of Service (DDoS) yang bertujuan untuk membanjiri sumber daya jaringan, seperti SYN/ACK banjir, serangan refleksi UDP, dan serangan volumetrik. AWS Shield memastikan bahwa lalu lintas jaringan yang mencapai AWS sumber daya Anda tetap tersedia bahkan di bawah serangan. AWS Shield perlindungan bekerja dengan menganalisis pola lalu lintas jaringan dan secara otomatis mengurangi ancaman yang diidentifikasi di tepi AWS jaringan.

Deployment

AWS WAF

- Membutuhkan pengaturan dan konfigurasi eksplisit. Ini dapat digunakan di beberapa Layanan AWS, termasuk Amazon CloudFront, Application Load Balancer (ALB), Amazon API Gateway, dan. AWS AppSync Anda harus membuat dan mengaitkan web ACLs (Daftar Kontrol Akses) dengan sumber daya Anda, menentukan aturan untuk mengizinkan, memblokir, atau memantau permintaan web tertentu. AWS WAF menawarkan opsi penerapan yang dapat disesuaikan, memungkinkan Anda menyesuaikan kebijakan keamanan dengan kebutuhan aplikasi spesifik Anda.

AWS Shield

- Terintegrasi secara otomatis dengan Layanan AWS dan selalu aktif, tidak memerlukan pengaturan tambahan untuk perlindungan dasar. AWS Shield Standar secara otomatis disertakan dengan semua Akun AWS, melindungi sumber daya seperti Amazon EC2, Elastic Load Balancing (ELB), Amazon CloudFront, dan Route 53. Untuk perlindungan yang ditingkatkan dengan AWS Shield Advanced, Anda harus mengaktifkannya secara eksplisit untuk sumber daya tertentu. Penerapan mulus, dan tidak ada konfigurasi tambahan yang diperlukan setelah AWS Shield dihidupkan.

Customization

AWS WAF

- Memberikan kemampuan kustomisasi yang luas. Anda dapat membuat web kustom ACLs (Daftar Kontrol Akses) dengan aturan yang menentukan kondisi tertentu untuk mengizinkan, memblokir, atau menghitung permintaan web berdasarkan alamat IP, header HTTP, parameter string kueri, dan banyak lagi. AWS WAF mendukung kelompok aturan terkelola dari AWS atau pihak ketiga, yang dapat disesuaikan lebih lanjut agar sesuai dengan kebutuhan aplikasi spesifik Anda. Anda juga dapat mengatur aturan berbasis tarif untuk membatasi jumlah permintaan dari satu alamat IP dan mengintegrasikan AWS WAF dengan inspeksi dan respons AWS Lambda permintaan lanjutan.

AWS Shield

- Menawarkan opsi penyesuaian terbatas. Dengan AWS Shield Standar, perlindungan otomatis dan tidak dapat dikonfigurasi. AWS Shield Advanced memungkinkan beberapa penyesuaian, seperti mengaktifkan metrik dan peringatan lanjutan, menyiapkan Pemeriksaan Kesehatan, dan mengakses Tim Respons AWS DDo S (DRT) untuk dukungan mitigasi yang disesuaikan.

Namun, fokusnya tetap pada perlindungan DDo S otomatis daripada pengaturan yang ditentukan pengguna. Anda dapat mengaitkan ACL AWS WAF web dengan sumber daya untuk mengaktifkan perlindungan lapisan aplikasi.

Managed rules

AWS WAF

- Menawarkan berbagai aturan terkelola yang dapat diterapkan pada aplikasi web untuk melindungi terhadap ancaman web umum. Aturan terkelola ini telah dikonfigurasi sebelumnya oleh AWS atau vendor keamanan pihak ketiga dan mencakup berbagai skenario keamanan seperti injeksi SQL, skrip lintas situs (XSS), dan alamat IP buruk yang diketahui. Anda dapat berlangganan dan menerapkan grup aturan terkelola ini ke web Anda ACLs, memberikan out-of-the-box perlindungan yang diperbarui secara berkala untuk mengatasi kerentanan dan ancaman baru. Aturan terkelola dapat disesuaikan dan dikombinasikan dengan aturan khusus untuk menyesuaikan kebijakan keamanan dengan kebutuhan aplikasi tertentu. AWS WAF juga menyediakan fitur mitigasi ancaman cerdas yang dikelola. Ini adalah perlindungan canggih dan khusus yang dapat Anda terapkan untuk melindungi dari ancaman seperti bot berbahaya dan upaya pengambilalihan akun.

AWS Shield

- Terutama berfokus pada perlindungan DDo S, dan tidak menawarkan aturan terkelola tradisional. AWS Shield Standar secara otomatis menerapkan satu set perlindungan yang telah ditentukan terhadap jaringan umum dan serangan lapisan DDo S transport. AWS Shield Advanced meningkatkan perlindungan ini tetapi tidak menyediakan aturan terkelola yang dapat disesuaikan. Sebaliknya, ia menawarkan teknik mitigasi yang lebih maju dan akses ke Tim Respons DDo S untuk bantuan yang disesuaikan.

Pricing model

AWS WAF

- Menggunakan model pay-as-you-go penetapan harga. Anda dikenakan biaya berdasarkan jumlah web yang ACLs Anda buat, jumlah aturan yang Anda terapkan dalam setiap ACL, dan jumlah permintaan web yang diproses oleh aturan. Model ini memungkinkan biaya yang dapat diskalakan berdasarkan penggunaan aktual, artinya Anda hanya membayar sumber daya

yang Anda butuhkan. Biaya tambahan berlaku untuk grup aturan terkelola yang disediakan oleh AWS atau vendor pihak ketiga. AWS WAF juga menyediakan aturan terkelola untuk kontrol Bot dan kontrol penipuan dengan model harga per permintaan yang serupa. AWS WAF juga menawarkan captcha/challenge fitur yang dibebankan oleh jumlah upaya captcha dan tanggapan tantangan yang disajikan.

AWS Shield

- Memiliki model harga berjenjang. AWS Shield Standar disertakan tanpa biaya tambahan dengan semua Akun AWS, memberikan perlindungan DDo S dasar. AWS Shield Advanced dikenakan biaya berdasarkan langganan bulanan dan biaya tambahan untuk transfer data dan mitigasi di luar ambang batas tertentu. Langganan ini mencakup akses 24/7 ke AWS DDo S Response Team (DRT), diagnostik serangan lanjutan, dan perlindungan biaya selama serangan.

Attack response team

AWS WAF

- Tidak termasuk tim respons serangan khusus sebagai bagian dari layanannya. Sebagai gantinya, ia menyediakan alat dan fitur yang memungkinkan Anda membuat, mengelola, dan menyesuaikan aturan keamanan sendiri. Anda dapat memantau lalu lintas dan membuat perubahan real-time ke web Anda ACLs berdasarkan lanskap ancaman, tetapi Anda tidak memiliki akses langsung ke tim dukungan khusus untuk mitigasi serangan.

AWS Shield

- Menawarkan akses ke AWS DDo S Response Team (DRT) sebagai bagian dari layanan AWS Shield Lanjutannya. DRT adalah tim ahli 24/7 yang membantu mitigasi dan respons serangan waktu nyata. Saat berada di bawah serangan DDo S, Anda dapat menghubungi DRT untuk mendapatkan saran dan dukungan khusus untuk mengelola dan mengurangi ancaman secara efektif. Ini termasuk panduan tentang praktik terbaik, analisis insiden, dan tanggapan terkoordinasi untuk meminimalkan dampak pada AWS sumber daya Anda.

Real-time monitoring

AWS WAF

- Menawarkan pemantauan real-time dengan mengintegrasikan dengan AWS CloudWatch, memungkinkan Anda untuk melacak metrik seperti permintaan yang diblokir atau diizinkan, tarif permintaan, dan efektivitas aturan tertentu. AWS WAF menyediakan visibilitas hampir real-time ke lalu lintas web dan peristiwa keamanan melalui Konsol Manajemen AWS atau APIs. Anda dapat mengatur CloudWatch alarm khusus berdasarkan AWS WAF metrik Anda untuk merespons dengan cepat potensi ancaman atau pola lalu lintas yang tidak biasa.

AWS Shield

- Menyediakan pemantauan real-time terutama melalui AWS Shield Advanced. Ini terintegrasi dengan AWS CloudWatch untuk memberikan metrik dan peringatan mendekati waktu nyata yang terkait dengan serangan S. DDo Anda dapat memantau diagnostik serangan, pola lalu lintas, dan efektivitas mitigasi. AWS Shield Advanced juga menawarkan laporan terperinci dan visibilitas ke dalam vektor serangan dan skala secara otomatis sebagai respons terhadap ancaman, memberikan wawasan melalui. Konsol Manajemen AWS

Kedua layanan menyediakan dasbor untuk memvisualisasikan pola serangan dan tren lalu lintas. AWS Shield Pemantauan berfokus pada anomali tingkat jaringan dan serangan volumetrik, sekaligus AWS WAF memberikan wawasan yang lebih dalam tentang permintaan lapisan aplikasi dan efektivitas aturan.

Traffic inspection

AWS WAF

- Memeriksa lalu lintas di lapisan aplikasi (Layer 7), menganalisis konten HTTP/S permintaan. Ini mengevaluasi lalu lintas web terhadap aturan yang ditentukan pengguna, memeriksa pola serangan tertentu seperti injeksi SQL, skrip lintas situs (XSS), atau muatan berbahaya lainnya dalam badan permintaan, header, atau parameter URL.

AWS Shield

- Berfokus pada perlindungan terhadap serangan DDo S, terutama memeriksa lalu lintas di lapisan jaringan (Layer 3) dan transport (Layer 4). Ini tidak memeriksa isi lalu lintas lapisan aplikasi (HTTP/S), melainkan mencari pola khas serangan DDo S, seperti volume lalu lintas yang luar biasa tinggi atau penyalahgunaan protokol. AWS Shield secara otomatis mengurangi ancaman ini tanpa aturan yang ditentukan pengguna atau inspeksi berbasis konten, memastikan ketersediaan serangan. Layanan AWS

Gunakan

AWS WAF

- Apa itu AWS WAF?

  Pelajari cara Anda dapat menggunakan AWS WAF untuk memantau dan melindungi aplikasi web Anda dari eksploitasi web umum.

  Jelajahi panduannya

- Menganalisis AWS WAF Log di CloudWatch Log Amazon

  Siapkan AWS WAF pencatatan asli ke CloudWatch log Amazon dan visualisasikan serta analisis data di log.

  Baca blognya

- Visualisasikan AWS WAF log dengan dasbor Amazon CloudWatch

  Gunakan Amazon CloudWatch untuk memantau dan menganalisis AWS WAF aktivitas menggunakan CloudWatch metrik, Wawasan Kontributor, dan Wawasan Log.

  Baca blognya

AWS Shield

- Apa itu AWS Shield?

  Pelajari bagaimana Anda dapat menggunakan AWS Shield untuk melindungi aplikasi web Anda terhadap serangan DDo S umum di jaringan dan lapisan transportasi.

  Jelajahi panduannya

- Memulai dengan AWS Shield Advanced

  Memulai AWS Shield Advanced dengan menggunakan konsol AWS Shield Advanced.

  Jelajahi panduannya

- AWS Shield Lokakarya lanjutan

  Lindungi sumber daya yang terpapar internet dari serangan DDo S, pantau serangan DDo S terhadap infrastruktur Anda, dan beri tahu tim yang sesuai.

  Jelajahi lokakarya

Riwayat dokumen

Tabel berikut menjelaskan perubahan penting pada panduan keputusan ini. Untuk pemberitahuan tentang pembaruan panduan ini, Anda dapat berlangganan umpan RSS.

Perubahan	Deskripsi	Tanggal
Publikasi awal	Panduan pertama kali diterbitkan.	September 17, 2024

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