AWS Guida decisionale

AWS WAF o AWS Shield?

AWS WAF o AWS Shield?: AWS Guida decisionale

Table of Contents

AWS WAF o AWS Shield?

Comprendi le differenze e scegli quella più adatta a te

Scopo	Per aiutarti a determinare se AWS WAF o AWS Shield soddisfa le tue esigenze di un servizio di sicurezza delle applicazioni web.
Ultimo aggiornamento	17 settembre 2024
Servizi coperti	• AWS WAF • AWS Shield

Introduzione

AWS WAF(Web Application Firewall) e AWS Shieldpuò aiutarti a proteggere le tue applicazioni Web da vari tipi di attacchi informatici, come attacchi Distributed Denial of Service (DDoS) e altre vulnerabilità delle applicazioni Web.

- AWS WAFsi concentra sulla protezione delle applicazioni Web dagli exploit Web comuni. AWS WAF Utilizzalo per creare regole di sicurezza web personalizzabili per filtrare il traffico dannoso, proteggere da attacchi come SQL injection e cross-site scripting (XSS) e integrarsi con altri. Servizi AWS
- AWS Shieldè un servizio di protezione DDo S gestito. Viene utilizzato AWS Shield per attivare il rilevamento sempre attivo e le mitigazioni automatiche e proteggere dai comuni attacchi DDo S a livello di rete e di trasporto.

Oltre AWS Shield a difenderti dagli attacchi su larga scala a livello di rete, con AWS Shield Advanced puoi associare un ACL AWS WAF web a una risorsa per fornire protezione a livello di applicazione. AWS WAF fornisce una protezione più granulare contro le vulnerabilità specifiche dell'applicazione. Utilizzate entrambi i servizi in tandem per una strategia di difesa a più livelli, proteggendo le applicazioni da una gamma più ampia di potenziali minacce su diversi livelli di rete.

Ecco una panoramica di alto livello delle principali differenze tra questi servizi.

Categoria	 AWS WAF	 AWS Shield
Scopo principale	Protegge dagli exploit sulle applicazioni web (come SQL injection o XSS)	Protegge dagli attacchi DDo S (come i flood SYN o UDP)
Strato di protezione	Livello di applicazione (L7)	Livelli di rete, trasporto e applicazione (L3/L4/L7)
Implementazione	Deve essere configurato in modo esplicito	AWS Shield Protezione standard inclusa per tutti gli account dei clienti
Personalizzazione	Altamente personalizzabile con regole personalizzate	Attiva o disattiva AWS Shield Advanced, con opzioni per attivare la mitigazione automatica delle protezioni di livello DDo S dell'applicazione
Regole gestite	Include regole AWS gestite e regole di terze parti	Non applicabile
Modello tariffario	Pay-as-you-go prezzi basati sul numero di regole e richieste	AWS Shield Standard incluso; AWS Shield Advanced comporta costi aggiuntivi
Squadra di risposta agli attacchi	Non applicabile	Disponibile con AWS Shield Advanced (team di risposta 24 ore su 24 DDo, 7 giorni su 7)
monitoraggio in tempo reale	Sì	Sì
Ispezione del traffico	A livello di richiesta	A livello di pacchetto

Differenze tra e AWS WAF AWS Shield

Esplora otto aree chiave di differenza tra AWS Shield e AWS WAF, che includono il livello di protezione, l'implementazione, la personalizzazione, le regole gestite, il modello di prezzo, il team di risposta agli attacchi, il monitoraggio in tempo reale e l'ispezione del traffico.

Layer of protection

AWS WAF

- Funziona a livello di applicazione (livello 7). Protegge le applicazioni Web filtrando e monitorando il HTTP/S traffico. AWS WAF difende da exploit web comuni come SQL injection, cross-site scripting (XSS) e cross-site request forgery (CSRF). È possibile creare regole personalizzate per bloccare le richieste dannose in base a vari criteri come indirizzi IP, stringhe di query e intestazioni.

AWS Shield

- Funziona principalmente a livello di rete (livello 3) e di trasporto (livello 4). È progettato per mitigare gli attacchi Distributed Denial of Service (DDoS) che mirano a sovraccaricare le risorse di rete, come SYN/ACK inondazioni, attacchi di riflessione UDP e attacchi volumetrici. AWS Shield assicura che il traffico di rete che raggiunge le risorse rimanga disponibile anche in caso di attacco. AWS AWS Shield funziona analizzando i modelli di traffico di rete e mitigando automaticamente le minacce identificate ai margini della AWS rete.

Deployment

AWS WAF

- Richiede un'impostazione e una configurazione esplicite. Può essere distribuito su più piattaforme Servizi AWS, tra cui Amazon CloudFront, Application Load Balancer (ALB), Amazon API Gateway e. AWS AppSync È necessario creare e associare il Web ACLs (Access Control Lists) alle risorse, definendo regole per consentire, bloccare o monitorare richieste Web specifiche. AWS WAF offre opzioni di implementazione personalizzabili, che consentono di adattare le politiche di sicurezza alle esigenze specifiche delle applicazioni.

AWS Shield

- Si integra automaticamente Servizi AWS ed è sempre attivo, non richiede alcuna configurazione aggiuntiva per la protezione di base. AWS Shield Standard è incluso automaticamente in tutti Account AWS e protegge risorse come Amazon EC2, Elastic Load Balancing (ELB) CloudFront, Amazon e Route 53. Per una protezione avanzata con AWS Shield Advanced, devi attivarla esplicitamente per risorse specifiche. L'implementazione è semplice e non è necessaria alcuna configurazione aggiuntiva una volta AWS Shield attivata.

Customization

AWS WAF

- Fornisce ampie funzionalità di personalizzazione. È possibile creare siti Web personalizzati ACLs (elenchi di controllo degli accessi) con regole che definiscono condizioni specifiche per consentire, bloccare o contare le richieste Web in base a indirizzi IP, intestazioni HTTP, parametri delle stringhe di query e altro ancora. AWS WAF supporta gruppi di regole gestiti da AWS o terze parti, che possono essere ulteriormente personalizzati per soddisfare le esigenze specifiche delle applicazioni. È inoltre possibile impostare regole basate sulla frequenza per limitare il numero di richieste da un singolo indirizzo IP e integrarle AWS WAF AWS Lambda per l'ispezione e la risposta avanzate delle richieste.

AWS Shield

- Offre opzioni di personalizzazione limitate. Con AWS Shield Standard, la protezione è automatica e non configurabile. AWS Shield Advanced consente alcune personalizzazioni, come l'abilitazione di metriche e avvisi avanzati, la configurazione di Health Checks e l'accesso allo AWS DDo S Response Team (DRT) per un supporto di mitigazione personalizzato. Tuttavia, la sua attenzione rimane sulla protezione DDo S automatizzata piuttosto che sulle impostazioni definite dall'utente. È possibile associare un ACL AWS WAF Web alle risorse per attivare la protezione a livello di applicazione.

Managed rules

AWS WAF

- Offre una gamma di regole gestite che possono essere applicate alle applicazioni Web per proteggersi dalle minacce Web comuni. Queste regole gestite sono preconfigurate da AWS fornitori di sicurezza di terze parti e coprono vari scenari di sicurezza come SQL injection,

cross-site scripting (XSS) e indirizzi IP noti non validi. È possibile sottoscrivere e applicare questi gruppi di regole gestite al Web ACLs, garantendo una out-of-the-box protezione regolarmente aggiornata per affrontare nuove vulnerabilità e minacce. Le regole gestite possono essere personalizzate e combinate con regole personalizzate per adattare le politiche di sicurezza alle esigenze specifiche delle applicazioni. AWS WAF fornisce anche funzionalità gestite e intelligenti di mitigazione delle minacce. Si tratta di protezioni avanzate e specializzate che è possibile implementare per proteggersi da minacce come bot dannosi e tentativi di acquisizione degli account.

AWS Shield

- Si concentra principalmente sulla protezione DDo S e non offre regole gestite tradizionali. AWS Shield Standard applica automaticamente una serie di protezioni predefinite contro gli attacchi di rete e di trasporto comuni al livello DDo S AWS Shield Advanced migliora queste protezioni ma non fornisce regole gestite personalizzabili. Offre invece tecniche di mitigazione più avanzate e l'accesso allo DDo S Response Team per un'assistenza personalizzata.

Pricing model

AWS WAF

- Utilizza un modello di pay-as-you-go prezzo. I costi vengono calcolati in base al numero di siti Web ACLs creati, al numero di regole distribuite in ogni ACL e al numero di richieste Web elaborate dalle regole. Questo modello consente costi scalabili in base all'utilizzo effettivo, il che significa che paghi solo per le risorse di cui hai bisogno. Si applicano costi aggiuntivi per i gruppi di regole gestiti forniti da AWS o da fornitori terzi. AWS WAF fornisce inoltre regole gestite per il controllo dei bot e il controllo delle frodi con un modello di prezzo per richiesta simile. AWS WAF offre anche una captcha/challenge funzionalità che viene addebitata in base al numero di tentativi di captcha e di risposte alle sfide inviate.

AWS Shield

- Ha un modello di prezzo a più livelli. AWS Shield Standard è incluso senza costi aggiuntivi in tutti Account AWS e fornisce una protezione DDo S di base. AWS Shield Advanced prevede una tariffa basata su un abbonamento mensile e costi aggiuntivi per il trasferimento e la mitigazione dei dati oltre una determinata soglia. Questo abbonamento include l'accesso 24

ore su 24, 7 giorni su 7, all' AWS DDoS Response Team (DRT), alla diagnostica avanzata degli attacchi e alla protezione dei costi durante gli attacchi.

Attack response team

AWS WAF

- Non include un team dedicato alla risposta agli attacchi come parte del suo servizio. Fornisce invece strumenti e funzionalità che consentono di creare, gestire e modificare autonomamente le regole di sicurezza. È possibile monitorare il traffico e apportare modifiche in tempo reale al Web in ACLs base al panorama delle minacce, ma non si ha accesso diretto a un team di supporto specializzato per la mitigazione degli attacchi.

AWS Shield

- Offre l'accesso allo AWS DDo S Response Team (DRT) come parte del servizio AWS Shield Advanced. Il DRT è un team di esperti attivo 24 ore su 24, 7 giorni su 7, che fornisce assistenza nella mitigazione e nella risposta agli attacchi in tempo reale. In caso di attacco DDo S, puoi contattare il DRT per consigli e supporto personalizzati per gestire e mitigare la minaccia in modo efficace. Ciò include linee guida sulle migliori pratiche, analisi degli incidenti e risposte coordinate per ridurre al minimo l'impatto sulle AWS risorse.

Real-time monitoring

AWS WAF

- Offre un monitoraggio in tempo reale grazie all'integrazione con AWS CloudWatch, che consente di tenere traccia di metriche come le richieste bloccate o consentite, le frequenze delle richieste e l'efficacia di regole specifiche. AWS WAF fornisce una visibilità quasi in tempo reale sul traffico web e sugli eventi di sicurezza tramite la Console di gestione AWS sala operatoria. APIs Puoi impostare CloudWatch allarmi personalizzati in base alle tue AWS WAF metriche per rispondere rapidamente a potenziali minacce o schemi di traffico insoliti.

AWS Shield

- Fornisce il monitoraggio in tempo reale principalmente tramite Advanced AWS Shield . Si integra AWS CloudWatch per fornire metriche e avvisi quasi in tempo reale relativi agli attacchi

S. DDo È possibile monitorare la diagnostica degli attacchi, i modelli di traffico e l'efficacia delle mitigazioni. AWS Shield Advanced offre inoltre report dettagliati e visibilità sui vettori di attacco e si ridimensiona automaticamente in risposta alle minacce, fornendo informazioni approfondite tramite. Console di gestione AWS

Entrambi i servizi forniscono dashboard per visualizzare i modelli di attacco e le tendenze del traffico. AWS Shield si concentra sulle anomalie a livello di rete e sugli attacchi volumetrici, mentre fornisce informazioni più approfondite sulle richieste a livello di applicazione e sull'efficacia delle regole. AWS WAF

Traffic inspection

AWS WAF

- Ispeziona il traffico a livello di applicazione (livello 7), analizzando il contenuto delle richieste. HTTP/S Valuta il traffico web rispetto a regole definite dall'utente, verificando modelli di attacco specifici come SQL injection, cross-site scripting (XSS) o altri payload dannosi all'interno del corpo della richiesta, delle intestazioni o dei parametri URL.

AWS Shield

- Si concentra sulla protezione dagli attacchi DDo S, principalmente ispezionando il traffico a livello di rete (livello 3) e di trasporto (livello 4). Non ispeziona il contenuto del traffico a livello applicativo (HTTP/S), ma cerca piuttosto schemi tipici degli attacchi DDo S, come volumi di traffico insolitamente elevati o uso improprio del protocollo. AWS Shield mitiga automaticamente queste minacce senza regole definite dall'utente o ispezioni basate sui contenuti, garantendo la disponibilità delle minacce sotto attacco. Servizi AWS

Utilizzo

AWS WAF

- Che cos'è? AWS WAF

  Scopri come puoi utilizzarle AWS WAF per monitorare e proteggere le tue applicazioni web dagli exploit web più comuni.

  Esplora la guida

- Analisi dei AWS WAF log in Amazon Logs CloudWatch

  Configura AWS WAF la registrazione nativa CloudWatch nei log di Amazon e visualizza e analizza i dati nei log.

  Leggi il blog

- Visualizza i AWS WAF log con una dashboard Amazon CloudWatch

  Usa Amazon CloudWatch per monitorare e analizzare le AWS WAF attività utilizzando CloudWatch metriche, Contributor Insights e Logs Insights.

  Leggi il blog

AWS Shield

- Che cos'è AWS Shield?

  Scopri come puoi utilizzarle AWS Shield per proteggere le tue applicazioni Web dai comuni attacchi DDo S a livello di rete e di trasporto.

  Esplora la guida

- Guida introduttiva ad AWS Shield Advanced

  Inizia a usare AWS Shield Advanced utilizzando la console AWS Shield Advanced.

  Esplora la guida

- AWS Shield Workshop avanzato

  Proteggi le risorse esposte a Internet dagli attacchi DDo S, monitora gli attacchi DDo S contro la tua infrastruttura e avvisa i team appropriati.

  Esplora il workshop

Cronologia dei documenti

La tabella seguente descrive le modifiche importanti a questa guida decisionale. Per ricevere notifiche sugli aggiornamenti di questa guida, puoi iscriverti a un feed RSS.

Modifica	Descrizione	Data
Pubblicazione iniziale	Guida pubblicata per la prima volta.	17 settembre 2024

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.