AWS Guia de decisão

AWS WAF ou AWS Shield?

AWS WAF ou AWS Shield?: AWS Guia de decisão

Table of Contents

AWS WAF ou AWS Shield?

Entenda as diferenças e escolha a mais adequada para você

Finalidade	Para ajudá-lo a determinar se AWS WAF ou AWS Shield atende às suas necessidades de um serviço de segurança de aplicativos web.
Última atualização	17 de setembro de 2024
Serviços cobertos	• AWS WAF • AWS Shield

Introdução

AWS WAF(Web Application Firewall) e AWS Shieldpode ajudá-lo a proteger seus aplicativos da web contra vários tipos de ataques cibernéticos, como ataques distribuídos de negação de serviço (DDoS) e outras vulnerabilidades de aplicativos da web.

- AWS WAFconcentra-se em proteger seus aplicativos da web contra explorações comuns da web. Use AWS WAF para criar regras de segurança web personalizáveis para filtrar tráfego malicioso, proteger contra ataques como injeção de SQL e cross-site scripting (XSS) e integrar-se a outros. Serviços da AWS
- AWS Shieldé um serviço DDo gerenciado de proteção S. Use AWS Shield para ativar a detecção sempre ativa e as mitigações automáticas, além de se proteger contra ataques DDo S comuns nas camadas de rede e transporte.

Enquanto AWS Shield se defende contra ataques em grande escala em nível de rede, com o AWS Shield Advanced, você pode associar uma ACL AWS WAF da web a um recurso para fornecer proteção na camada do aplicativo. AWS WAF fornece proteção mais granular contra vulnerabilidades específicas do aplicativo. Use os dois serviços em conjunto para uma estratégia de defesa em várias camadas, protegendo seus aplicativos de uma gama mais ampla de ameaças potenciais em diferentes camadas de rede.

Aqui está uma visão geral das principais diferenças entre esses serviços.

Categoria	AWS WAF	AWS Shield
Objetivo principal	Protege contra explorações em aplicativos da web (como injeção de SQL ou XSS)	Protege contra ataques DDo S (como inundações de SYN ou UDP)
Camada de proteção	Camada de aplicação (L7)	Camadas de rede, transporte e aplicação (L3/L4/L7)
Implantação	Deve ser configurado explicita mente	AWS Shield Proteção padrão incluída para todas as contas de clientes
Personalização	Altamente personalizável com regras personalizadas	Ative ou desative o AWS Shield Avançado, com opções para ativar a mitigação automática das proteções da camada DDo S do aplicativo
Regras gerenciadas	Inclui regras AWS gerenciad as e regras de terceiros	Não aplicável
Modelo de definição de preços	Pay-as-you-go preços com base no número de regras e solicitações	AWS Shield Padrão incluído; AWS Shield Avançado incorre em custo adicional
Equipe de resposta ao ataque	Não aplicável	Disponível com AWS Shield Advanced (equipe de resposta DDo S 24/7)
monitoramento em tempo real	Sim	Sim
Inspeção de tráfego	Nível de solicitação	Nível do pacote

Diferenças entre AWS WAF e AWS Shield

Explore oito áreas principais de diferença entre AWS Shield e AWS WAF, abrangendo camada de proteção, implantação, personalização, regras gerenciadas, modelo de preços, equipe de resposta a ataques, monitoramento em tempo real e inspeção de tráfego.

Layer of protection

AWS WAF

- Opera na camada de aplicação (camada 7). Ele protege os aplicativos da web filtrando e monitorando o HTTP/S tráfego. AWS WAF defende-se contra explorações comuns da Web, como injeção de SQL, scripts entre sites (XSS) e falsificação de solicitações entre sites (CSRF). Você pode criar regras personalizadas para bloquear solicitações maliciosas com base em vários critérios, como endereços IP, cadeias de caracteres de consulta e cabeçalhos.

AWS Shield

- Opera principalmente nas camadas de rede (camada 3) e transporte (camada 4). Ele foi projetado para mitigar ataques distribuídos de negação de serviço (DDoS) que visam sobrecarregar os recursos da rede, como SYN/ACK inundações, ataques de reflexão UDP e ataques volumétricos. AWS Shield garante que o tráfego de rede que chega aos seus AWS recursos permaneça disponível mesmo sob ataque. AWS Shield A proteção funciona analisando os padrões de tráfego da rede e mitigando automaticamente as ameaças identificadas na borda da AWS rede.

Deployment

AWS WAF

- Requer instalação e configuração explícitas. Ele pode ser implantado em vários Serviços da AWS, incluindo Amazon CloudFront, Application Load Balancer (ALB), Amazon API Gateway e. AWS AppSync Você deve criar e associar a web ACLs (listas de controle de acesso) aos seus recursos, definindo regras para permitir, bloquear ou monitorar solicitações específicas da web. AWS WAF oferece opções de implantação personalizáveis, permitindo que você adapte as políticas de segurança às necessidades específicas do seu aplicativo.

AWS Shield

- Integra-se automaticamente Serviços da AWS e está sempre ativo, sem necessidade de configuração adicional para proteção básica. AWS Shield O padrão é incluído automaticamente em tudo Contas da AWS, protegendo recursos como Amazon EC2, Elastic Load Balancing (ELB) CloudFront, Amazon e Route 53. Para melhorar a proteção com o AWS Shield Advanced, você deve ativá-lo explicitamente para recursos específicos. A implantação é perfeita e nenhuma configuração adicional é necessária depois AWS Shield de ativada.

Customization

AWS WAF

- Fornece amplos recursos de personalização. Você pode criar uma web personalizada ACLs (listas de controle de acesso) com regras que definem condições específicas para permitir, bloquear ou contar solicitações da web com base em endereços IP, cabeçalhos HTTP, parâmetros de sequência de caracteres de consulta e muito mais. AWS WAF oferece suporte a grupos de regras gerenciados de terceiros AWS ou de terceiros, que podem ser personalizados ainda mais para atender às necessidades específicas de seu aplicativo. Você também pode configurar regras baseadas em taxas para limitar o número de solicitações de um único endereço IP e integrá-las AWS WAF AWS Lambda para inspeção e resposta avançadas de solicitações.

AWS Shield

- Oferece opções limitadas de personalização. Com o AWS Shield Standard, a proteção é automática e não configurável. AWS Shield O Advanced permite algumas personalizações, como ativar métricas e alertas avançados, configurar Health Checks e acessar a AWS DDo S Response Team (DRT) para obter suporte personalizado de mitigação. No entanto, seu foco permanece na proteção DDo S automatizada, em vez de nas configurações definidas pelo usuário. Você pode associar uma ACL AWS WAF da web a recursos para ativar a proteção da camada de aplicação.

Managed rules

AWS WAF

- Oferece uma variedade de regras gerenciadas que podem ser aplicadas a aplicativos da Web para proteção contra ameaças comuns da Web. Essas regras gerenciadas são

pré-configuradas por fornecedores de segurança terceirizados AWS ou por fornecedores terceirizados e abrangem vários cenários de segurança, como injeção de SQL, scripts entre sites (XSS) e endereços IP incorretos conhecidos. Você pode se inscrever e aplicar esses grupos de regras gerenciadas à sua web ACLs, fornecendo out-of-the-box proteção que é atualizada regularmente para lidar com novas vulnerabilidades e ameaças. As regras gerenciadas podem ser personalizadas e combinadas com regras personalizadas para adaptar as políticas de segurança às necessidades específicas do aplicativo. AWS WAF também fornece recursos gerenciados e inteligentes de mitigação de ameaças. Essas são proteções avançadas e especializadas que você pode implementar para se proteger contra ameaças, como bots maliciosos e tentativas de apropriação de contas.

AWS Shield

- Focado principalmente na proteção DDo S e não oferece regras gerenciadas tradicionais. AWS Shield O padrão aplica automaticamente um conjunto de proteções predefinidas contra ataques comuns da camada DDo S de rede e transporte. AWS Shield O Advanced aprimora essas proteções, mas não fornece regras gerenciadas personalizáveis. Em vez disso, oferece técnicas de mitigação mais avançadas e acesso à equipe DDo S Response para assistência personalizada.

Pricing model

AWS WAF

- Usa um modelo pay-as-you-go de preços. Você é cobrado com base no número de web ACLs que você cria, no número de regras que você implanta em cada ACL e no número de solicitações da web processadas pelas regras. Esse modelo permite custos escaláveis com base no uso real, o que significa que você paga apenas pelos recursos necessários. Cobranças adicionais se aplicam a grupos de regras gerenciados fornecidos por AWS ou fornecedores terceirizados. AWS WAF também fornece regras gerenciadas para controle de bots e controle de fraudes com um modelo similar de preços por solicitação. AWS WAF também oferece um captcha/challenge recurso que é cobrado pelo número de tentativas de captcha e respostas de desafio fornecidas.

AWS Shield

- Tem um modelo de preços em camadas. AWS Shield O padrão está incluído sem custo adicional em tudo Contas da AWS, fornecendo proteção DDo S básica. AWS Shield O Advanced incorre em uma taxa com base em uma assinatura mensal e cobranças adicionais pela transferência e mitigação de dados além de um determinado limite. Essa assinatura inclui acesso 24 horas por dia, 7 dias por semana ao AWS DDo S Response Team (DRT), diagnóstico avançado de ataques e proteção de custos durante ataques.

Attack response team

AWS WAF

- Não inclui uma equipe dedicada de resposta a ataques como parte de seu serviço. Em vez disso, ele fornece ferramentas e recursos que permitem que você mesmo crie, gerencie e ajuste as regras de segurança. Você pode monitorar o tráfego e fazer alterações em tempo real na sua web ACLs com base no cenário de ameaças, mas não tem acesso direto a uma equipe de suporte especializada para mitigação de ataques.

AWS Shield

- Oferece acesso ao AWS DDo S Response Team (DRT) como parte de seu serviço AWS Shield Avançado. A DRT é uma equipe de especialistas 24 horas por dia, 7 dias por semana, que auxilia na mitigação e resposta a ataques em tempo real. Quando estiver sob um ataque DDo S, você pode entrar em contato com o DRT para obter aconselhamento e suporte personalizados para gerenciar e mitigar a ameaça de forma eficaz. Isso inclui orientação sobre as melhores práticas, análise de incidentes e respostas coordenadas para minimizar o impacto em seus AWS recursos.

Real-time monitoring

AWS WAF

- Oferece monitoramento em tempo real por meio da integração com AWS CloudWatch, permitindo que você acompanhe métricas como solicitações bloqueadas ou permitidas, taxas de solicitações e a eficácia de regras específicas. AWS WAF fornece visibilidade quase em tempo real do tráfego da web e dos eventos de segurança por meio do Console de gerenciamento da AWS ou APIs. Você pode configurar CloudWatch alarmes personalizados

com base em suas AWS WAF métricas para responder rapidamente a possíveis ameaças ou padrões de tráfego incomuns.

AWS Shield

- Fornece monitoramento em tempo real principalmente por meio do AWS Shield Advanced. Ele se integra AWS CloudWatch para fornecer métricas e alertas quase em tempo real relacionados aos ataques DDo S. Você pode monitorar diagnósticos de ataques, padrões de tráfego e a eficácia das mitigações. AWS Shield O Advanced também oferece relatórios detalhados e visibilidade dos vetores de ataque e escala automaticamente em resposta às ameaças, fornecendo informações por meio do Console de gerenciamento da AWS.

Ambos os serviços fornecem painéis para visualizar padrões de ataque e tendências de tráfego. AWS Shield O monitoramento da se concentra em anomalias em nível de rede e ataques volumétricos, ao mesmo tempo em que AWS WAF fornece insights mais profundos sobre as solicitações da camada de aplicação e a eficácia das regras.

Traffic inspection

AWS WAF

- Inspeciona o tráfego na camada do aplicativo (camada 7), analisando o conteúdo das HTTP/S solicitações. Ele avalia o tráfego da web em relação às regras definidas pelo usuário, verificando padrões de ataque específicos, como injeção de SQL, cross-site scripting (XSS) ou outras cargas maliciosas no corpo da solicitação, nos cabeçalhos ou nos parâmetros de URL.

AWS Shield

- Concentra-se na proteção contra ataques DDo S, inspecionando principalmente o tráfego nas camadas de rede (camada 3) e transporte (camada 4). Ele não inspeciona o conteúdo do tráfego da camada de aplicação (HTTP/S), mas procura padrões típicos de ataques DDo S, como volumes de tráfego excepcionalmente altos ou uso indevido do protocolo. AWS Shield mitiga automaticamente essas ameaças sem regras definidas pelo usuário ou inspeção baseada em conteúdo, garantindo a disponibilidade de Serviços da AWS quem está sob ataque.

Use

AWS WAF

- O que é AWS WAF?

  Saiba como você pode usar AWS WAF para monitorar e proteger seus aplicativos da Web contra explorações comuns da Web.

  Explore o guia

- Análise de AWS WAF registros no Amazon CloudWatch Logs

  Configure o AWS WAF registro nativo CloudWatch nos registros da Amazon e visualize e analise os dados nos registros.

  Leia o blog

- Visualize AWS WAF registros com um painel da Amazon CloudWatch

  Use CloudWatch a Amazon para monitorar e analisar AWS WAF atividades usando CloudWatch métricas, Contributor Insights e Logs Insights.

  Leia o blog

AWS Shield

- O que é AWS Shield?

  Saiba como você pode usar AWS Shield para proteger seus aplicativos da web contra ataques DDo S comuns nas camadas de rede e transporte.

  Explore o guia

- Começando com o AWS Shield Advanced

  Comece a usar o AWS Shield Advanced usando o console AWS Shield Advanced.

  Explore o guia

- AWS Shield Workshop avançado

  Proteja os recursos expostos à Internet contra ataques DDo S, monitore DDo os ataques S contra sua infraestrutura e notifique as equipes apropriadas.

  Explore o workshop

Histórico do documento

A tabela a seguir descreve as mudanças importantes nesse guia de decisão. Para receber notificações sobre atualizações deste guia, você pode assinar um feed RSS.

Alteração	Descrição	Data
Publicação inicial	Guia publicado pela primeira vez.	17 de setembro de 2024

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.