AWS Guide de décision

AWS WAF ou AWS Shield ?

AWS WAF ou AWS Shield ?: AWS Guide de décision

Table of Contents

AWS WAF ou AWS Shield ?

Comprenez les différences et choisissez celui qui vous convient le mieux

Objectif	Pour vous aider à déterminer si AWS WAF un service de sécurité des applications Web AWS Shield répond à vos besoins.
Dernière mise à jour	17 septembre 2024
Services couverts	• AWS WAF • AWS Shield

Introduction

AWS WAF(Web Application Firewall) et AWS Shieldpeut vous aider à protéger vos applications Web contre différents types de cyberattaques, telles que les attaques par déni de service (DDoS) distribué et d'autres vulnérabilités des applications Web.

- AWS WAFmet l'accent sur la protection de vos applications Web contre les exploits Web courants. Utilisez-le AWS WAF pour créer des règles de sécurité Web personnalisables afin de filtrer le trafic malveillant, de vous protéger contre les attaques telles que l'injection SQL et les scripts intersites (XSS), et de les intégrer à d'autres. Services AWS
- AWS Shieldest un service de protection DDo S géré. Utilisez-le AWS Shield pour activer la détection permanente et les mesures d'atténuation automatiques, et pour vous protéger contre les attaques DDo S courantes au niveau du réseau et des couches de transport.

Tout en AWS Shield vous protégeant contre les attaques à grande échelle au niveau du réseau, avec AWS Shield Advanced, vous pouvez associer une ACL AWS WAF Web à une ressource afin de fournir une protection au niveau de la couche application. AWS WAF fournit une protection plus précise contre les vulnérabilités spécifiques aux applications. Utilisez les deux services en tandem pour une stratégie de défense à plusieurs niveaux, protégeant vos applications contre un plus large éventail de menaces potentielles sur les différentes couches du réseau.

Voici un aperçu général des principales différences entre ces services.

Catégorie	 AWS WAF	 AWS Shield
Objectif principal	Protège contre les exploits sur les applications Web (telles que l'injection SQL ou XSS)	Protège contre les attaques DDo S (telles que les inondations SYN ou UDP)
Couche de protection	Couche d'application (L7)	Couches réseau, transport et application (L3/L4/L7)
Déploiement	Doit être explicitement configuré	AWS Shield Protection standard incluse pour tous les comptes clients
Personnalisation	Hautement personnalisable avec des règles personnal isées	Activez ou désactivez le AWS Shield mode avancé, avec des options permettant d'activer l'atténuation automatique des protections de la couche d'application DDo S
Règles gérées	Inclut des règles AWS gérées et des règles tierces	Ne s’applique pas
Modèle de tarification	Pay-as-you-go tarification basée sur le nombre de règles et de demandes	AWS Shield Standard inclus ; le AWS Shield niveau avancé entraîne des frais supplémen taires
Équipe d'intervention en cas d'attaque	Ne s’applique pas	Disponible avec AWS Shield Advanced (équipe d'interve ntion DDo S 24/7)
Surveillance en temps réel	Oui	Oui
Inspection du trafic	Niveau de demande	Au niveau du paquet

Différences entre AWS WAF et AWS Shield

Explorez huit domaines clés qui font la différence entre AWS Shield et AWS WAF, concernant la couche de protection, le déploiement, la personnalisation, les règles gérées, le modèle de tarification, l'équipe de réponse aux attaques, la surveillance en temps réel et l'inspection du trafic.

Layer of protection

AWS WAF

- Fonctionne au niveau de la couche d'application (couche 7). Il protège les applications Web en filtrant et en surveillant HTTP/S le trafic. AWS WAF protège contre les exploits Web courants tels que l'injection SQL, le cross-site scripting (XSS) et le cross-site request forgery (CSRF). Vous pouvez créer des règles personnalisées pour bloquer les demandes malveillantes en fonction de divers critères tels que les adresses IP, les chaînes de requête et les en-têtes.

AWS Shield

- Fonctionne principalement au niveau des couches réseau (couche 3) et transport (couche 4). Il est conçu pour atténuer les attaques par déni de service (DDoS) distribué qui visent à submerger les ressources du réseau, telles que les SYN/ACK inondations, les attaques par réflexion UDP et les attaques volumétriques. AWS Shield garantit que le trafic réseau atteignant vos AWS ressources reste disponible même en cas d'attaque. AWS Shield fonctionne en analysant les modèles de trafic réseau et en atténuant automatiquement les menaces identifiées à la périphérie du AWS réseau.

Deployment

AWS WAF

- Nécessite une installation et une configuration explicites. Il peut être déployé sur plusieurs sites Services AWS, notamment Amazon CloudFront, Application Load Balancer (ALB), Amazon API Gateway et. AWS AppSync Vous devez créer et associer des sites Web ACLs (listes de contrôle d'accès) à vos ressources, en définissant des règles pour autoriser, bloquer ou surveiller des requêtes Web spécifiques. AWS WAF propose des options de déploiement personnalisables, vous permettant d'adapter les politiques de sécurité aux besoins spécifiques de vos applications.

AWS Shield

- Il est automatiquement intégré Services AWS et activé en permanence, ne nécessitant aucune configuration supplémentaire pour la protection de base. AWS Shield La norme est automatiquement incluse dans tout Comptes AWS, protégeant des ressources telles qu'Amazon EC2, Elastic Load Balancing (ELB) CloudFront, Amazon et Route 53. Pour améliorer la protection avec AWS Shield Advanced, vous devez l'activer explicitement pour des ressources spécifiques. Le déploiement est fluide et aucune configuration supplémentaire n'est nécessaire une fois AWS Shield activé.

Customization

AWS WAF

- Fournit des fonctionnalités de personnalisation étendues. Vous pouvez créer un site Web personnalisé ACLs (listes de contrôle d'accès) avec des règles qui définissent des conditions spécifiques pour autoriser, bloquer ou compter les requêtes Web en fonction des adresses IP, des en-têtes HTTP, des paramètres de chaîne de requête, etc. AWS WAF prend en charge les groupes de règles gérés par AWS ou par des tiers, qui peuvent être personnalisés davantage pour répondre aux besoins spécifiques de votre application. Vous pouvez également configurer des règles basées sur le débit afin de limiter le nombre de demandes provenant d'une seule adresse IP et de les intégrer AWS Lambda pour AWS WAF une inspection et une réponse avancées des demandes.

AWS Shield

- Offre des options de personnalisation limitées. Avec AWS Shield Standard, la protection est automatique et non configurable. AWS Shield La version avancée permet une certaine personnalisation, notamment en activant des métriques et des alertes avancées, en configurant des bilans de santé et en accédant à la AWS DDo S Response Team (DRT) pour une assistance personnalisée en matière d'atténuation. Cependant, il se concentre toujours sur la protection DDo S automatisée plutôt que sur les paramètres définis par l'utilisateur. Vous pouvez associer une ACL AWS WAF Web à des ressources pour activer la protection de la couche application.

Managed rules

AWS WAF

- Offre une gamme de règles gérées qui peuvent être appliquées aux applications Web pour se protéger contre les menaces Web courantes. Ces règles gérées sont préconfigurées par AWS ou par des fournisseurs de sécurité tiers et couvrent divers scénarios de sécurité tels que l'injection SQL, le cross-site scripting (XSS) et les adresses IP erronées connues. Vous pouvez vous abonner à ces groupes de règles gérés et les appliquer à votre site Web ACLs, en fournissant une out-of-the-box protection régulièrement mise à jour pour faire face aux nouvelles vulnérabilités et menaces. Les règles gérées peuvent être personnalisées et associées à des règles personnalisées pour adapter les politiques de sécurité aux besoins spécifiques des applications. AWS WAF fournit également des fonctionnalités intelligentes gérées d'atténuation des menaces. Il s'agit de protections avancées et spécialisées que vous pouvez mettre en œuvre pour vous protéger contre les menaces telles que les robots malveillants et les tentatives de prise de contrôle de compte.

AWS Shield

- Il est principalement axé sur la protection DDo S et ne propose pas de règles gérées traditionnelles. AWS Shield Standard applique automatiquement un ensemble de protections prédéfinies contre les attaques communes du réseau et de la couche de transport DDo S. AWS Shield Advanced améliore ces protections mais ne fournit pas de règles gérées personnalisables. Il propose plutôt des techniques d'atténuation plus avancées et un accès à l'équipe DDo S Response pour une assistance personnalisée.

Pricing model

AWS WAF

- Utilise un modèle de pay-as-you-go tarification. Vous êtes facturé en fonction du nombre de sites Web ACLs que vous créez, du nombre de règles que vous déployez au sein de chaque ACL et du nombre de demandes Web traitées par les règles. Ce modèle permet des coûts évolutifs en fonction de l'utilisation réelle, ce qui signifie que vous ne payez que pour les ressources dont vous avez besoin. Des frais supplémentaires s'appliquent aux groupes de règles gérés fournis par AWS ou par des fournisseurs tiers. AWS WAF fournit également des règles gérées pour le contrôle des bots et le contrôle de la fraude avec un modèle de tarification

par demande similaire. AWS WAF propose également une captcha/challenge fonctionnalité facturée en fonction du nombre de tentatives de captcha et de réponses aux défis fournies.

AWS Shield

- Dispose d'un modèle de tarification à plusieurs niveaux. AWS Shield Le standard est inclus sans frais supplémentaires avec tous Comptes AWS, offrant une protection DDo S de base. AWS Shield Advanced facture des frais basés sur un abonnement mensuel et des frais supplémentaires pour le transfert de données et l'atténuation au-delà d'un certain seuil. Cet abonnement inclut un accès 24 heures sur 24, 7 jours sur 7 à la AWS DDo S Response Team (DRT), des diagnostics avancés des attaques et une protection des coûts en cas d'attaque.

Attack response team

AWS WAF

- N'inclut pas d'équipe dédiée à la réponse aux attaques dans le cadre de son service. Il fournit plutôt des outils et des fonctionnalités qui vous permettent de créer, de gérer et d'ajuster les règles de sécurité elles-mêmes. Vous pouvez surveiller le trafic et apporter des modifications en temps réel à votre site Web en ACLs fonction de l'environnement des menaces, mais vous n'avez pas directement accès à une équipe d'assistance spécialisée pour atténuer les attaques.

AWS Shield

- Offre un accès à l'équipe AWS DDo S Response (DRT) dans le cadre de son service AWS Shield avancé. Le DRT est une équipe d'experts 24 heures sur 24, 7 jours sur 7, qui aide à atténuer les attaques et à y répondre en temps réel. En cas d'attaque DDo S, vous pouvez contacter le DRT pour obtenir des conseils et une assistance personnalisés afin de gérer et d'atténuer efficacement la menace. Cela inclut des conseils sur les meilleures pratiques, l'analyse des incidents et les réponses coordonnées afin de minimiser l'impact sur vos AWS ressources.

Real-time monitoring

AWS WAF

- Offre une surveillance en temps réel grâce à l'intégration AWS CloudWatch, ce qui vous permet de suivre des indicateurs tels que les demandes bloquées ou autorisées, les taux de demandes et l'efficacité de règles spécifiques. AWS WAF fournit une visibilité en temps quasi réel sur le trafic Web et les événements de sécurité via le AWS Management Console bloc opératoire APIs. Vous pouvez configurer des CloudWatch alarmes personnalisées en fonction de vos AWS WAF indicateurs afin de réagir rapidement aux menaces potentielles ou aux modèles de trafic inhabituels.

AWS Shield

- Fournit une surveillance en temps réel principalement via AWS Shield Advanced. Il s'intègre AWS CloudWatch pour fournir des métriques et des alertes en temps quasi réel liées aux attaques DDo S. Vous pouvez surveiller les diagnostics des attaques, les modèles de trafic et l'efficacité des mesures d'atténuation. AWS Shield Advanced propose également des rapports détaillés et une visibilité sur les vecteurs d'attaque et évolue automatiquement en réponse aux menaces, en fournissant des informations via le AWS Management Console.

Les deux services fournissent des tableaux de bord permettant de visualiser les modèles d'attaque et les tendances du trafic. AWS Shield se concentre sur les anomalies au niveau du réseau et les attaques volumétriques, tout en AWS WAF fournissant des informations plus approfondies sur les demandes de la couche applicative et sur l'efficacité des règles.

Traffic inspection

AWS WAF

- Inspecte le trafic au niveau de la couche application (couche 7), en analysant le contenu des HTTP/S demandes. Il évalue le trafic Web par rapport aux règles définies par l'utilisateur, en recherchant des modèles d'attaque spécifiques tels que l'injection SQL, les scripts intersites (XSS) ou d'autres charges utiles malveillantes dans le corps de la requête, les en-têtes ou les paramètres d'URL.

AWS Shield

- Se concentre sur la protection contre les attaques DDo S, principalement en inspectant le trafic au niveau des couches réseau (couche 3) et de transport (couche 4). Il n'inspecte pas le contenu du trafic de la couche application (HTTP/S), mais recherche plutôt les modèles typiques des attaques DDo S, tels que des volumes de trafic anormalement élevés ou une

utilisation abusive du protocole. AWS Shield atténue automatiquement ces menaces sans règles définies par l'utilisateur ni inspection basée sur le contenu, garantissant ainsi la disponibilité des personnes attaquées. Services AWS

Utiliser

AWS WAF

- Qu'est-ce que c'est AWS WAF ?

  Découvrez comment surveiller et protéger vos applications Web contre les exploits Web courants. AWS WAF

  Explorez le guide

- Analyse AWS WAF des journaux dans Amazon CloudWatch Logs

  Configurez la AWS WAF journalisation native dans CloudWatch les journaux Amazon et visualisez et analysez les données contenues dans les journaux.

  Lisez le blogue

- Visualisez AWS WAF les journaux avec un tableau de CloudWatch bord Amazon

  Utilisez Amazon CloudWatch pour surveiller et analyser AWS WAF l'activité à l'aide de CloudWatch métriques, de Contributor Insights et de Logs Insights.

  Lisez le blogue

AWS Shield

- Qu'est-ce que c'est AWS Shield ?

  Découvrez comment protéger vos applications Web contre les attaques DDo S courantes au niveau du réseau et des couches de transport. AWS Shield

  Explorez le guide

- Commencer à utiliser AWS Shield Advanced

  Commencez avec AWS Shield Advanced en utilisant la console AWS Shield Advanced.

  Explorez le guide

- AWS Shield Atelier avancé

  Protégez les ressources exposées à Internet contre les attaques DDo S, surveillez les attaques DDo S contre votre infrastructure et informez les équipes appropriées.

  Découvrez l'atelier

Historique du document

Le tableau suivant décrit les modifications importantes apportées à ce guide de décision. Pour recevoir des notifications concernant les mises à jour de ce guide, vous pouvez vous abonner à un flux RSS.

Modification	Description	Date
Publication initiale	Guide publié pour la première fois.	17 septembre 2024

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.