AWS 决策指南

AWS WAF 或 AWS Shield？

AWS WAF 或 AWS Shield？: AWS 決策指南

Table of Contents

AWS WAF 或 AWS Shield？

了解差異並挑選適合您的差異

用途	協助您判斷 AWS WAF 或 是否符合 AWS Shield 您對 Web 應用程式安全服務的需求。
上次更新	2024 年 9 月 17 日
涵蓋的服務	• AWS WAF • AWS Shield

簡介

AWS WAF (Web Application Firewall) 和 AWS Shield可協助您保護您的 Web 應用程式免受各種類型的網路攻擊，例如分散式阻斷服務 (DDoS) 攻擊和其他 Web 應用程式漏洞。

- AWS WAF 著重於保護您的 Web 應用程式免受常見的 Web 入侵。使用 AWS WAF 建立可自訂的 Web 安全規則來篩選惡意流量、防範 SQL Injection 和跨網站指令碼 (XSS) 等攻擊，以及與其他 整合 AWS 服務。
- AWS Shield 是受管 DDoS 保護服務。使用 AWS Shield 開啟永遠開啟偵測和自動緩解，並防止網路和傳輸層的常見 DDoS 攻擊。

雖然 AWS Shield 可以防禦大規模的網路層級攻擊，但您可以透過 AWS Shield 進階將 AWS WAF Web ACL 與 資源建立關聯，以在應用程式層提供保護。 AWS WAF 提供更精細的保護，防範應用程式特定的漏洞。將這兩種服務一起用於多層防禦策略，保護您的應用程式免受不同網路層中更廣泛的潛在威脅。

以下是這些服務之間主要差異的高階檢視。

類別	 AWS WAF	 AWS Shield
主要用途	防止 Web 應用程式（例如 SQL Injection 或 XSS) 上的入侵	防範 DDoS 攻擊（例如 SYN 或 UDP 洪水）
保護層	應用程式層 (L7)	網路、傳輸和應用程式層 (L3/L4/L7)
部署	必須明確設定	AWS Shield 包含所有客戶帳戶的標準保護
自訂	使用自訂規則高度自訂	開啟或停用 AWS Shield 進階，並可選擇開啟應用程式層 DDoS 保護的自動緩解
受管規則	包含 AWS 受管規則和第三方規則	不適用
定價方式	根據規則和請求數量的Pay-as-you-go定價	AWS Shield 包含標準； AWS Shield 進階會產生額外費用
攻擊回應團隊	不適用	適用於 AWS Shield 進階（全年無休 DDoS 回應團隊）
即時監控	是	是
流量檢查	請求層級	封包層級

AWS WAF 和 之間的差異 AWS Shield

探索 AWS Shield 和 之間的八個主要差異領域 AWS WAF，涵蓋保護層、部署、自訂、受管規則、定價模型、攻擊回應團隊、即時監控和流量檢查。

Layer of protection

AWS WAF

- 在應用程式層（第 7 層）操作。它透過篩選和監控 HTTP/S 流量來保護 Web 應用程式。 AWS WAF 防禦常見的 Web 入侵，例如 SQL Injection、跨網站指令碼 (XSS) 和跨網站請求偽造 (CSRF)。您可以建立自訂規則，根據 IP 地址、查詢字串和標頭等各種條件來封鎖惡意請求。

AWS Shield

- 主要在網路（第 3 層）和傳輸（第 4 層）層操作。它旨在緩解分散式阻斷服務 (DDoS) 攻擊，這些攻擊旨在使網路資源暴增，例如 SYN/ACK 洪水、UDP 反射攻擊和容積攻擊。 AWS Shield 可確保到達您 AWS 資源的網路流量即使在攻擊下仍然可用。 AWS Shield的保護透過分析網路流量模式並自動緩解 AWS 網路邊緣的已識別威脅來運作。

Deployment

AWS WAF

- 需要明確的設定和組態。它可以部署在多個 上 AWS 服務，包括 Amazon CloudFront、Application Load Balancer (ALB)、Amazon API Gateway 和 AWS AppSync。您必須建立 Web ACLs（存取控制清單）並將其與資源建立關聯，定義規則以允許、封鎖或監控特定 Web 請求。 AWS WAF 提供可自訂的部署選項，可讓您根據特定應用程式需求量身打造安全政策。

AWS Shield

- 與 自動整合 AWS 服務 且一律開啟，無需額外設定即可提供基本保護。 AWS Shield Standard 會自動包含在所有 中 AWS 帳戶，以保護 Amazon EC2、Elastic Load Balancing (ELB)、Amazon CloudFront 和 Route 53 等資源。若要使用 AWS Shield 進階增強保護，您必須針對特定資源將其明確開啟。部署是無縫的，一旦開啟 AWS Shield ，就不需要額外的組態。

Customization

AWS WAF

- 提供廣泛的自訂功能。您可以使用規則建立自訂 Web ACLs（存取控制清單），這些規則定義了根據 IP 地址、HTTP 標頭、查詢字串參數等允許、封鎖或計數 Web 請求的特定條件。 AWS

WAF 支援來自 AWS 或第三方的受管規則群組，這些群組可以進一步自訂，以滿足您的特定應用程式需求。您也可以設定以速率為基礎的規則來限制來自單一 IP 地址的請求數量，並與 整合 AWS WAF AWS Lambda 以進行進階請求檢查和回應。

AWS Shield

- 提供有限的自訂選項。使用 AWS Shield 標準時，保護是自動且不可設定的。 AWS Shield 進階允許一些自訂，例如啟用進階指標和警示、設定運作狀態檢查，以及存取 AWS DDoS 回應團隊 (DRT) 以取得量身打造的緩解支援。不過，其重點仍是自動 DDoS 保護，而不是使用者定義的設定。您可以將 AWS WAF Web ACL 與 資源建立關聯，以開啟應用程式層保護。

Managed rules

AWS WAF

- 提供各種可套用至 Web 應用程式的受管規則，以防止常見的 Web 威脅。這些受管規則是由 AWS 或第三方安全廠商預先設定，涵蓋 SQL Injection、跨網站指令碼 (XSS) 和已知不良 IP 地址等各種安全案例。您可以訂閱並套用這些受管規則群組到您的 Web ACLs，提供out-of-the-box保護，並定期更新以解決新的漏洞和威脅。受管規則可以自訂並與自訂規則結合，以根據特定應用程式需求量身打造安全政策。 AWS WAF 也提供受管智慧型威脅緩解功能。這些是進階的專門保護，您可以實作這些保護，以防止惡意機器人和帳戶接管嘗試等威脅。

AWS Shield

- 主要專注於 DDoS 保護，並且不提供傳統的受管規則。 AWS Shield Standard 會自動套用一組預先定義的保護，以防範常見的網路和傳輸層 DDoS 攻擊。 AWS Shield Advanced 會增強這些保護，但不提供可自訂的受管規則。反之，它提供更進階的緩解技術和 DDoS 回應團隊的存取權，以取得量身打造的協助。

Pricing model

AWS WAF

- 使用pay-as-you-go定價模型。會根據您建立ACLs 數目、您在每個 ACL 內部署的規則數目，以及規則處理的 Web 請求數目，向您收費。此模型根據實際用量允許可擴展成本，這表示您只需支付所需的資源。由 AWS 或第三方廠商提供的受管規則群組需支付額外費用。 AWS WAF 也提

供 Bot Control 和詐騙控制的受管規則，每個請求定價模型皆類似。 AWS WAF 也提供 captcha/challenge 功能，該功能根據提供的 captcha 嘗試次數和挑戰回應收費。

AWS Shield

- 具有分層定價模型。 AWS Shield Standard 包含在所有 中，無需額外費用 AWS 帳戶，可提供基本的 DDoS 保護。 AWS Shield 進階會根據每月訂閱產生費用，並針對超過特定閾值的資料傳輸和緩解產生額外費用。此訂閱包括全年無休存取 AWS DDoS 回應團隊 (DRT)、進階攻擊診斷，以及在攻擊期間保護成本。

Attack response team

AWS WAF

- 不包含專用攻擊回應團隊做為其服務的一部分。反之，它提供了工具和功能，可讓您自行建立、管理和調整安全規則。您可以監控流量並根據威脅態勢對 Web ACLs 進行即時變更，但您無法直接存取專門的支援團隊以緩解攻擊。

AWS Shield

- 在進階服務中提供對 AWS DDoS 回應團隊 (DRT) 的 AWS Shield 存取權。DRT 是一個全年無休的專家團隊，可協助即時緩解攻擊和回應。在 DDoS 攻擊下，您可以聯絡 DRT 以取得自訂建議和支援，以有效地管理和緩解威脅。這包括最佳實務、事件分析和協調回應的指引，以將對 AWS 資源的影響降至最低。

Real-time monitoring

AWS WAF

- 透過與 AWS CloudWatch 整合來提供即時監控，可讓您追蹤指標，例如封鎖或允許的請求、請求率，以及特定規則的有效性。 透過 AWS 管理主控台 或 APIs AWS WAF 提供近乎即時的 Web 流量和安全事件可見性。您可以根據您的 AWS WAF 指標設定自訂 CloudWatch 警示，以快速回應潛在威脅或不尋常的流量模式。

AWS Shield

- 主要透過 AWS Shield 進階提供即時監控。它與 AWS CloudWatch 整合，可提供與 DDoS 攻擊相關的近乎即時指標和提醒。您可以監控攻擊診斷、流量模式和緩解措施的有效性。 AWS Shield Advanced 也提供詳細的報告和對攻擊向量的可見性，並自動擴展以回應威脅，透過 提供洞見 AWS 管理主控台。

這兩種服務都提供儀表板，以視覺化攻擊模式和流量趨勢。 AWS Shield的監控著重於網路層級異常和容積攻擊，同時 AWS WAF 提供應用程式層請求和規則有效性的更深入洞見。

Traffic inspection

AWS WAF

- 檢查應用程式層 （第 7 層） 的流量，分析 HTTP/S 請求的內容。它會根據使用者定義的規則評估 Web 流量，檢查特定攻擊模式，例如 SQL Injection、跨網站指令碼 (XSS) 或請求內文、標頭或 URL 參數中的其他惡意承載。

AWS Shield

- 專注於防範 DDoS 攻擊，主要檢查網路 （第 3 層） 和傳輸 （第 4 層） 層的流量。它不會檢查應用程式層流量 (HTTP/S) 的內容，而是尋找 DDoS 攻擊的典型模式，例如異常高流量或通訊協定濫用。 AWS Shield 會自動緩解這些威脅，無需使用者定義的規則或內容型檢查，以確保 AWS 服務 受到攻擊的可用性。

使用

AWS WAF

- 什麼是 AWS WAF？

  了解如何使用 AWS WAF 來監控和保護您的 Web 應用程式免受常見的 Web 入侵。

  探索指南

- 分析 Amazon CloudWatch AWS WAF Logs 中的日誌

  將原生 AWS WAF 記錄設定為 Amazon CloudWatch logs，並將日誌中的資料視覺化和分析。

  閱讀部落格

- 使用 Amazon CloudWatch 儀表板視覺化 AWS WAF 日誌

  使用 Amazon CloudWatch 透過 CloudWatch 指標、Contributor Insights 和 Logs Insights 來監控和分析 AWS WAF 活動。

  閱讀部落格

AWS Shield

- 什麼是 AWS Shield？

  了解如何使用 AWS Shield 來保護 Web 應用程式免受網路和傳輸層的常見 DDoS 攻擊。

  探索指南

- 進階入門 AWS Shield

  使用 AWS Shield 進階主控台開始使用 AWS Shield 進階。

  探索指南

- AWS Shield 進階研討會

  保護網際網路暴露的資源免受 DDoS 攻擊、監控對基礎設施的 DDoS 攻擊，並通知適當的團隊。

  探索研討會

文件歷史記錄

下表說明此決策指南的重要變更。如需有關本指南更新的通知，您可以訂閱 RSS 摘要。

變更	描述	日期
初次出版	指南首先發佈。	2024 年 9 月 17 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。