AWS 决策指南

AWS WAF 或者 AWS Shield？

AWS WAF 或者 AWS Shield？: AWS 决策指南

Table of Contents

AWS WAF 或者 AWS Shield？

了解差异并选择适合您的差异

目的	帮助您确定是否 AWS WAF 或 AWS Shield 满足您对 Web 应用程序安全服务的需求。
上次更新	2024 年 9 月 17 日
承保服务	• AWS WAF • AWS Shield

简介

AWS WAF（Web 应用程序防火墙），AWS Shield可以帮助您保护 Web 应用程序免受各种类型的网络攻击，例如分布式拒绝服务 (DDoS) 攻击和其他 Web 应用程序漏洞。

- AWS WAF重点是保护您的 Web 应用程序免受常见 Web 漏洞的侵害。用于 AWS WAF 创建可自定义的 Web 安全规则，以过滤恶意流量，防御 SQL 注入和跨站脚本 (XSS) 等攻击，并与其他规则集成。 AWS 服务
- AWS Shield是一项托管 DDo S 保护服务。 AWS Shield 用于开启全天候检测和自动缓解功能，并防范网络层和传输层常见的 DDo S 攻击。

虽然可以抵 AWS Shield 御大规模的网络级攻击，但使用 AWS Shield Advanced，您可以将 AWS WAF Web ACL 与资源关联，以便在应用层提供保护。 AWS WAF 针对特定于应用程序的漏洞提供了更精细的保护。同时使用这两种服务来制定多层防御策略，保护您的应用程序免受跨不同网络层的更广泛潜在威胁的侵害。

以下是这些服务之间主要区别的高级视图。

类别	 AWS WAF	 AWS Shield
主要目的	防止 Web 应用程序上的漏洞（例如 SQL 注入或 XSS）	防御 DDo S 攻击（例如 SYN 或 UDP 洪水）
保护层	应用层 (L7)	网络、传输层和应用层 (L3/L4/L7)
部署	必须明确设置	AWS Shield 所有客户账户均包含标准保护
自定义	使用自定义规则进行高度自定义	开启或禁用“ AWS Shield 高级”，并提供开启自动缓解应用层 DDo S 保护的选项
托管规则	包括 AWS 托管规则和第三方规则	不适用
定价模式	Pay-as-you-go 根据规则和请求数量定价	AWS Shield 包括标准版；AWS Shield 高级版会产生额外费用
攻击响应小组	不适用	适用于高 AWS Shield 级（24/7 DDo S 响应小组）
实时监控	支持	是
交通检查	请求级别	数据包级别

AWS WAF 和之间的区别 AWS Shield

探索 AWS Shield 和之间的八个关键区别 AWS WAF，包括保护层、部署、自定义、托管规则、定价模型、攻击响应团队、实时监控和流量检查。

Layer of protection

AWS WAF

- 在应用层（第 7 层）运行。它通过过滤和监控 HTTP/S 流量来保护 Web 应用程序。 AWS WAF 防御常见的 Web 漏洞，例如 SQL 注入、跨站脚本 (XSS) 和跨站请求伪造 (CSRF)。您可以创建自定义规则，根据 IP 地址、查询字符串和标头等各种标准阻止恶意请求。

AWS Shield

- 主要在网络层（第 3 层）和传输层（第 4 层）上运行。它旨在缓解旨在压倒网络资源的分布式拒绝服务 (DDoS) 攻击，例如 SYN/ACK 洪水、UDP 反射攻击和容量攻击。 AWS Shield 确保即使受到攻击，到达您的 AWS 资源的网络流量也仍然可用。 AWS Shield的保护工作原理是分析网络流量模式并自动缓解 AWS 网络边缘已识别的威胁。

Deployment

AWS WAF

- 需要明确的设置和配置。它可以部署在多个上 AWS 服务，包括亚马逊 CloudFront、Application Load Balancer (ALB)、Amazon API Gateway 和 AWS AppSync。您必须创建 Web ACLs （访问控制列表）并将其与您的资源关联，定义允许、阻止或监控特定 Web 请求的规则。 AWS WAF 提供可自定义的部署选项，允许您根据特定的应用程序需求定制安全策略。

AWS Shield

- 自动集成 AWS 服务 且始终处于开启状态，无需额外设置即可获得基本保护。 AWS Shield 标准版自动包含在所有资源中，可保护亚马逊 AWS 账户 EC2、Elastic Load Balancing (ELB) CloudFront、亚马逊和 Route 53 等资源。要使用 “ AWS Shield 高级” 增强保护，必须为特定资源明确启用该功能。部署是无缝的，开启后 AWS Shield 无需进行其他配置。

Customization

AWS WAF

- 提供广泛的自定义功能。您可以使用规则创建自定义 Web ACLs（访问控制列表），这些规则定义了基于 IP 地址、HTTP 标头、查询字符串参数等允许、阻止或计数 Web 请求的特定条件。 AWS WAF 支持来自 AWS 或第三方的托管规则组，可以对其进行进一步自定义以满足您的特

定应用程序需求。您还可以设置基于速率的规则来限制来自单个 IP 地址的请求数量，并 AWS WAF 与之集成， AWS Lambda 以进行高级请求检查和响应。

AWS Shield

- 提供有限的自定义选项。使用 AWS Shield 标准版，保护是自动且不可配置的。 AWS Shield Advanced 允许进行一些自定义，例如启用高级指标和警报、设置 Health Checks 以及访问 AWS DDo S Response Team (DRT) 以获得量身定制的缓解支持。但是，它的重点仍然是自动 DDo S 保护，而不是用户定义的设置。您可以将 AWS WAF Web ACL 与资源关联，以开启应用层保护。

Managed rules

AWS WAF

- 提供一系列可应用于 Web 应用程序的托管规则，以防范常见 Web 威胁。这些托管规则由 AWS 第三方安全供应商预先配置，涵盖各种安全场景，例如 SQL 注入、跨站点脚本 (XSS) 和已知的错误 IP 地址。您可以订阅这些托管规则组并将其应用到您的网站 ACLs，从而提供定期更新的 out-of-the-box保护，以应对新的漏洞和威胁。可以自定义托管规则并将其与自定义规则相结合，以根据特定的应用程序需求定制安全策略。 AWS WAF 还提供托管智能威胁缓解功能。您可以实施这些高级的专业保护，以防范恶意机器人和账户盗用尝试等威胁。

AWS Shield

- 主要侧重于 DDo S 保护，不提供传统的托管规则。 AWS Shield Standard 会自动应用一组预定义的保护，以防范常见的网络和传输层 DDo S 攻击。 AWS Shield 高级增强了这些保护，但不提供可自定义的托管规则。取而代之的是，它提供了更先进的缓解技术，并可以联系 DDo S Response Team以获得量身定制的帮助。

Pricing model

AWS WAF

- 使用定pay-as-you-go 价模型。根据您创建的 Web 数量、 ACLs 您在每个 ACL 中部署的规则数量以及规则处理的 Web 请求数量向您收费。这种模式允许根据实际使用情况调整成本，这意味着您只需为所需的资源付费。第三方供应商提供的 AWS 托管规则组需支付额外费用。 AWS WAF 还为机器人控制和欺诈控制提供了托管规则，其定价模型与每个请求的定价模式类似。

AWS WAF 还提供一项 captcha/challenge 功能，该功能按验证码尝试次数和提供的质疑响应次数收费。

AWS Shield

- 具有分层定价模型。 AWS Shield 所有产品均包含标准配置，不收取额外费用 AWS 账户，提供基本 DDo的 S 保护。 AWS Shield Advanced 会根据月度订阅收取费用，超过一定阈值的数据传输和缓解会产生额外费用。此订阅包括全天候访问 AWS DDo S Response Team (DRT)、高级攻击诊断和攻击期间的成本保护。

Attack response team

AWS WAF

- 服务中不包括专门的攻击响应小组。相反，它提供了允许您自己创建、管理和调整安全规则的工具和功能。您可以监控流量并 ACLs根据威胁形势对网络进行实时更改，但您无法直接联系专门的支持团队来缓解攻击。

AWS Shield

- 作为其 AWS Shield 高级服务的一部分，提供对 AWS DDo S 响应小组 (DRT) 的访问权限。DRT 是一个全天候专家团队，可协助进行实时攻击缓解和响应。遭受 DDo S 攻击时，您可以联系 DRT 寻求定制建议和支持，以有效管理和缓解威胁。这包括有关最佳实践、事件分析和协调响应的指导，以最大限度地减少对 AWS 资源的影响。

Real-time monitoring

AWS WAF

- 通过与集成提供实时监控 AWS CloudWatch，允许您跟踪诸如已阻止或允许的请求、请求率以及特定规则的有效性等指标。 AWS WAF 通过 AWS 管理控制台 或提供对网络流量和安全事件的近乎实时的可见性 APIs。您可以根据自己的 AWS WAF 指标设置自定义 CloudWatch 警报，以快速响应潜在威胁或异常流量模式。

AWS Shield

- 主要通过 AWS Shield 高级提供实时监控。它与集成 AWS CloudWatch ，提供与 DDo S 攻击相关的近乎实时的指标和警报。您可以监控攻击诊断、流量模式和缓解措施的有效性。 AWS Shield Advanced 还提供详细的报告和攻击向量的可见性，并自动扩展以应对威胁，通过提供见解 AWS 管理控制台。

这两项服务都提供用于可视化攻击模式和流量趋势的仪表板。 AWS Shield的监控侧重于网络级异常和容量攻击，同时 AWS WAF 提供对应用层请求和规则有效性的更深入见解。

Traffic inspection

AWS WAF

- 检查应用层（第 7 层）的流量，分析 HTTP/S 请求的内容。它根据用户定义的规则评估 Web 流量，检查请求正文、标头或 URL 参数中是否存在特定的攻击模式，例如 SQL 注入、跨站脚本 (XSS) 或其他恶意负载。

AWS Shield

- 重点是防御 DDo S 攻击，主要检查网络（第 3 层）和传输（第 4 层）层的流量。它不检查应用层流量 (HTTP/S) 的内容，而是查找 DDo S 攻击的典型模式，例如异常高的流量或协议滥用。 AWS Shield 无需用户定义的规则或基于内容的检查即可自动缓解这些威胁，从而确保受到攻击的可用性。 AWS 服务

使用

AWS WAF

- 什么是 AWS WAF？

  了解 AWS WAF 如何使用监控和保护您的 Web 应用程序免受常见 Web 漏洞的侵害。

  浏览指南

- 分析 Amazon AWS WAF 日志中的 CloudWatch 日志

  设置对 Amazon AWS WAF 日志的原生 CloudWatch 日志记录，并可视化和分析日志中的数据。

  阅读博客

- 使用 Amazon CloudWatch 控制面板可视化 AWS WAF 日志

  使用 Amazon CloudWatch 通过 CloudWatch 指标、贡献者见解和日志见解来监控和分析 AWS WAF 活动。

  阅读博客

AWS Shield

- 什么是 AWS Shield？

  了解 AWS Shield 如何使用保护 Web 应用程序免受网络和传输层常见的 DDo S 攻击。

  浏览指南

- AWS Shield 高级版入门

  使用 AWS Shield 高级控制台开始使用 AWS Shield 高级。

  浏览指南

- AWS Shield 高级研讨会

  保护暴露在互联网上的资源免 DDo受 S 攻击，监控针对您的基础设施的 DDo S 攻击，并通知相应的团队。

  探索工作坊

文档历史记录

下表描述了本决策指南的重要更改。要获取有关本指南更新的通知，您可以订阅 RSS feed。

变更	说明	日期
初次发布	指南首次出版。	2024 年 9 月 17 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。