9 Amazon WAF 安全自动化

WAF Automation on Amazon Web Services

SLV1-SIC-Mgmt-NCD-WAF/VPC-AWS WAF Security Automations

行业：通用
技术：安全

一键部署 代码开源

1. 总体介绍

方案背景 在复杂的网络安全环境下，配置 Amazon WAF (Web 应用程序防火墙) 规则是一件繁琐而有难度的工作。因此，客户需要一套自动化方案，能按照最佳实践自动部署和更新 Amazon WAF，来过滤常见的 Web 攻击。

适用客户 适用于所有行业中在中国区域使用 Amazon WAF 的客户，主要行业包括电商、游戏、媒体等，他们通过 Web 对外提供服务，且访问量大。

适用场景 典型的应用场景是客户使用 Amazon WAF 为 Amazon ALB、Amazon API Gateway、Amazon AppSync 等服务过滤 Web 攻击。例如，为电商网站部署全面、自动的防网络攻击系统。

客户痛点 (1) Amazon WAF 配置工作复杂。随着网络攻击规模越来越大，风险越来越高，需要的 Amazon WAF 规则也越来越复杂。但客户在对网络安全更加重视的同时，也面临着 Amazon WAF 配置更加复杂、困难的现状。
(2) Amazon WAF 规则更新工作量大。Amazon WAF 规则需要根据网络攻击的变化及时更新，但客户自己分析日志、更新规则，不仅工作量大，而且难度高。
(3) 客户缺乏安全指导和最佳实践。很多客户没有专门的安全团队，需要安全最佳实践的支持和指导。

2. 客户价值

该方案可以快速、全面地满足客户使用 Amazon WAF 抵挡网络攻击的需求。

(1) 简单易用：客户只需要使用 Amazon CloudFormation 一键部署，就能获得完整而规范的 Amazon WAF 配置，节约部署 WAF 规则的工作量和时间。

(2) 自动更新：该方案会分析访问日志，根据攻击情况自动更新 WAF 规则，从而大大减少客户在安全更新、维护上的工作量。

(3) 应用最佳实践：该方案部署的 WAF 规则包括托管规则，客户也可以添加自定义规则，既遵循了最佳实践，又保留了灵活性。

3. 解决方案概要

方案概要 该方案自动部署一系列 Amazon WAF 规则，以过滤常见的基于 Web 的攻击。客户可以从预先配置的保护性功能中选择，这些功能用于定义 Amazon WAF Web 访问控制列表 (Web ACL) 中包含的规则。在部署完成后，Amazon WAF 检查请求，从而保护 Application Load Balancer (ALB)。可选择的功能主要包括：
(1) 亚马逊云科技的托管规则：通过托管核心规则提供保护，避免各种常见的应用程序漏洞被利用，或出现其他不必要的流量。
(2) 手动 IP 列表：客户可以手动添加限制或允许的 IP 地址。
(3) SQL 注入和 XSS：防止 URI、查询字符串或请求正文中常见的 SQL 注入或跨站脚本 (XSS) 攻击。
(4) HTTP 泛洪攻击：防止由来自特定 IP 地址的大量请求组成的攻击，例如 DDoS 攻击或暴力登录尝试。
(5) 扫描程序和探测器：解析应用程序访问日志，搜索可疑行为，然后在客户指定的时间段内阻止这些可疑的源 IP 地址。
(6) IP 声誉列表：通过 Amazon Lambda 函数每小时检查第三方 IP 声誉列表，并更新要阻止的 IP 列表。
(7) 不良 Bot：自动设置蜜罐，引诱并转移试图进行的攻击。

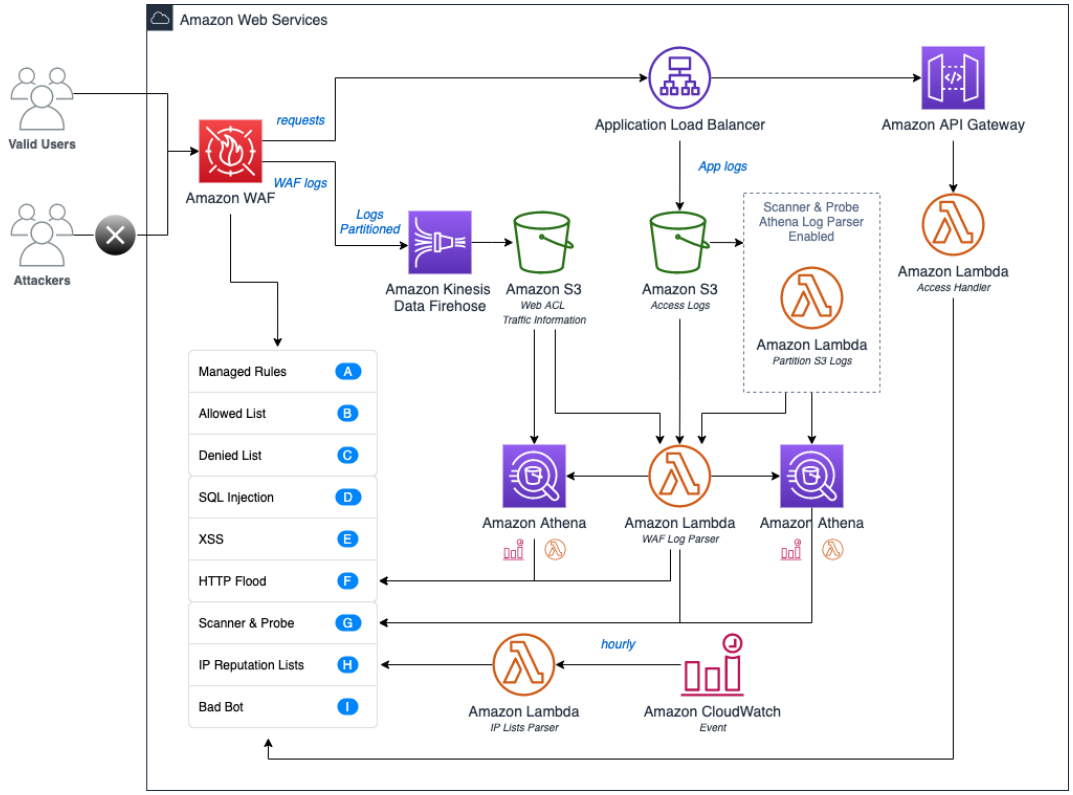
方案特点 该方案支持一键部署，应用安全最佳实践并自动更新。
(1) 简单易用，最佳实践：通过 Amazon CloudFormation 一键部署应用了安全最佳实践的 Amazon WAF 规则集。
(2) 功能全面，使用灵活：提供丰富的安全功能，并可以根据实际需求灵活选择是否启用。
(3) 分析日志，自动更新：该方案会分析应用日志、周期性检查第三方 IP 声誉列表，并自动更新 Amazon WAF 规则，在提高安全防护效果的同时减少安全管理人员的工作量。

部署前提 客户拥有亚马逊云科技中国区域的账户，并对账户中计划保护的 Application Load Balancer (ALB) 启用日志功能。

客户资源/能力评估 客户对 Amazon WAF 服务有基本的了解，有基本的安全领域知识。

成本因素 客户不需要为方案本身付费，只需要为使用到的亚马逊云科技的服务资源付费。运行此解决方案的总费用主要取决于接收、存储和处理的数据量、Amazon API Gateway 接收的请求数量，以及 Amazon Lambda 的调用数量。

4. 架构图



主要服务： Amazon API Gateway、Amazon Athena、Amazon CloudWatch、Amazon Kinesis Data Firehose、Amazon Lambda、Amazon S3、Amazon WAF

5. 资源和帮助

官网（中国）» https://www.amazonaws.cn/solutions/amazon-waf-security-automations/

部署手册 » https://s3.cn-north-1.amazonaws.com.cn/aws-dam-prod/china/Solutions/amazon_waf_security_automations/amazon-waf-security-automations-deployment-guide.pdf

GitHub » https://github.com/awslabs/aws-waf-security-automations

PartnerCast：利用 Amazon WAF 安全自动化解决方案轻松简化安全运维 » https://explore.skillbuilder.aws/learn/course/internal/view/elearning/12289/aws-partnercast-li-yongamazon-waf-an-quan-zi-dong-hua-jie-jue-fang-an-qing-song-jian-hua-an-quan-yun-wei-technical

博客：在多账户场景下将 Amazon WAF 安全自动化解决方案与 Amazon Firewall Manager 结合使用 » https://aws.amazon.com/cn/blogs/china/combine-amazon-waf-security-automation-solution-with-amazon-firewall-manager-in-multi-account-scenarios/

Campaign ID » SLV1-SIC-Mgmt-NCD-WAF/VPC-AWS WAF Security Automations

产 品 经 理 李思源（siyuanli@amazon.com）
项目负责人 李思源（siyuanli@amazon.com）
推广负责人 张濮（puzhang@amazon.com）

SO0006