

RayWAF 锐御

Web 应用防护系统

PRODUCT INTRODUCTION 产品介绍

Web 应用防护系统（RayWAF）是盛邦安全基于自主研发的 RayOS 开发的应用安全产品，全新一代智能 Web 应用防护系统以特征防护引擎为基础，结合智能语义分析引擎、机器学习引擎、主动防御引擎、威胁情报引擎、入侵防护引擎等 6 大全新安全引擎，构建“主动”+“被动”的纵深防御体系，不仅用于保护面向互联网的 Web 应用，还可以部署在内部 Web 应用服务器之前，对内部的业务访问进行访问控制和业务审计，防范来自内部的威胁，全面提高 Web 应用防护能力。

下一代Web应用防护系统框架图



KEY FEATURES 主要功能

态势监控

RayWAF 支持内置态势分析系统，无需与监控设备联动，可以对流量事件和攻击事件进行分析，并对关键的信息钻取，做可视化呈现。



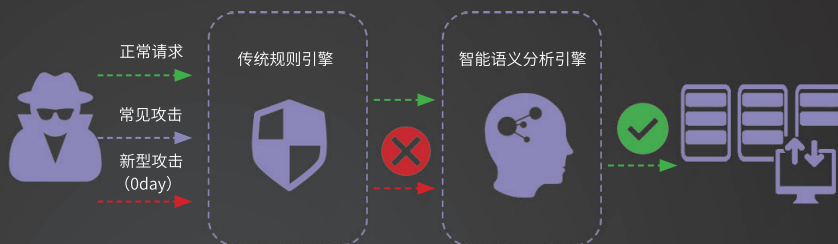
Web 攻击防御

OWASP-Top10

- | | |
|-----------------|-----------------|
| A1—注入 | AA6—敏感信息泄露 |
| A2—失效的身份认证和会话管理 | A7—攻击检测与防范不足 |
| A3—跨站脚本（XSS） | A8—跨站请求伪造（CSRF） |
| A4—失效的访问控制 | A9—使用含有已知漏洞的组件 |
| A5—安全配置错误 | A10—未受保护的 APIs |

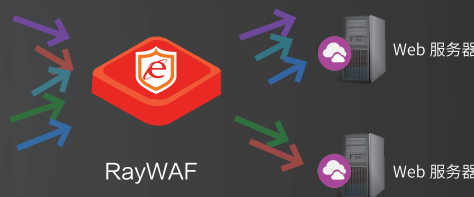
智能语义防护

智能语义分析引擎通过智能的分析算法模型，针对 SQL 以及 XSS 攻击进行检测与防御，与特征匹配的检测方式相比，智能语义分析技术具有准确率高、误报率低的特点，无需维护固定并庞大的特征库，有效提高了 Web 防护工作效率。



Web 负载均衡

RayWAF 支持 Web 负载均衡技术，通过内置的多种负载均衡算法，有效提高 Web 服务的响应速度和访问者的体验，通过 Web 负载均衡功能，能够提高 Web 应用系统的整体性能和扩展性能。



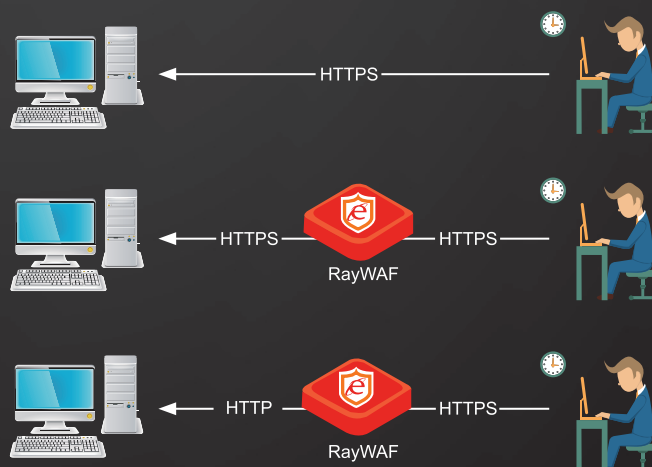
DDoS 防护

RayWAF 的防 DDoS 攻击模块采用主动监测加被动跟踪相互结合的防护技术，可辨识多种 DDoS 攻击，并启用特有的阻断方式，能够高效地完成对 DDoS 攻击的过滤和防护。针对互联网中常见的 DDoS 攻击手段，提供多种防护手段结合的方式，有效阻断攻击行为，从而确保服务器的安全和正常运转。

更多的防护类型，满足企业级 DDoS 应用需求		
丰富的场景检测规则	丰富的 DDoS 类型	应用层处理特性
内置 5 个检测级别，可供不同的场景选择	洪水攻击防护 畸形报文防护 资源消耗攻击防护 反射攻击防护 CC 攻击 僵尸网络攻击	HTTP GET Flood HTTP POST Flood HTTP Slow Header HTTP Slow Body DNS Flood CC
丰富的组合策略，覆盖网络层到应用层的 DDoS 防护		

HTTPS 防护

RayWAF 针对 SSL 加密应用，根据业务模型提供 HTTPS 卸载和 HTTPS 加速应用，以提供最佳的客户体验并降低服务器负载。针对大型网站应用，配置专业的 SSL 加速卡，在保护客户数据安全性的同时不会影响业务的应用。



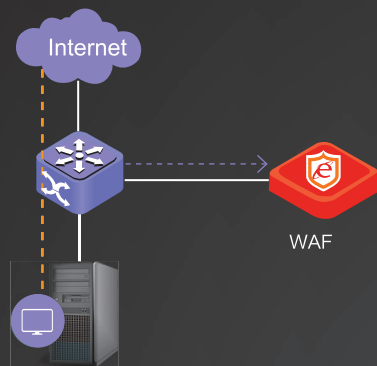
图：WAF 作为 HTTPS 卸载 / 加速应用

MULTIPLE DEPLOYMENT MODE

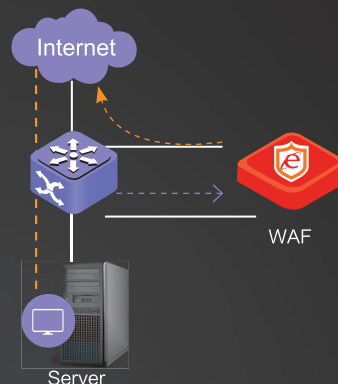
多种部署方案

Web 应用往往是组织内的重要业务系统，稳定性要求较高，对于安全产品的部署模式有着多种多样的需求。RayWAF 能够与客户的网络架构高度融合，支持镜像监测模式、镜像阻断防护模式、透明防护模式、反向代理防护模式等多种防护方式，符合客户的 IT 管理要求。

1、镜像监测



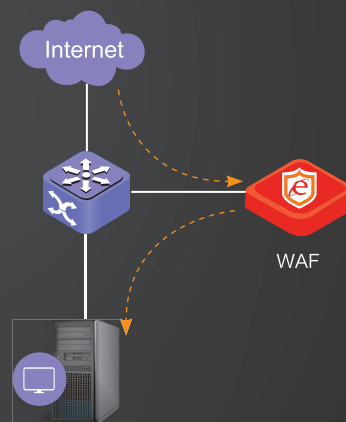
2、镜像阻断防护



3、透明防护



4、反向代理防护



ADVANTAGES

亮点优势

系统联动防护

RayWAF 与盛邦安全烽火台网站监控预警平台以及一体化漏洞评估系统形成联动，打造从漏洞扫描到攻击防御，从事前到事中、事后的完整解决方案。RayWAF 与 Web 资产治理平台形成联动，从管理到边界构建综合的资产治理方案，实现 Web 资产的安全自动化运营。

旁路镜像主动防御

支持旁路阻断部署模式，既保证了业务系统的稳定性，减少由串接导致的安全风险，又能起到对攻击进行阻断的安全作用。

IPv4/IPv6 双栈防护

RayWAF 可满足各类双栈部署环境，同时双向支持 IPv4 及 IPv6 协议栈，帮助用户轻松组建实验网络或从 IPv4 到 IPv6 的平稳过渡。

威胁情报防御

以云端 + 本地的威胁情报检测方式，通过智能融合，顺序匹配与加权匹配等算法模型，可将多个威胁情报数据进行聚合，并且保持与情报源之间的高频率更新互动，保证威胁判断依据的新鲜度和准确度。

机器学习防护

RayWAF 下一代智能 Web 应用防护系统使用机器学习技术针对流量中的 Web 访问流量，将网站目录结构、请求方法、条件参数及流量明细等全部相关信息自动生成至本地并建立模型，针对模型进行自动化防护，降低安全误报。

主动防御，发现潜在威胁

利用主动防御引擎，基于潜在威胁建立主动防御体系，让用户知悉恶意攻击来源及动向；及时告警人为与自动化攻击，并发现潜在的攻击行为。同时根据本地信誉库，即时应对来自各方的安全威胁，调整防护策略，形成防护闭环。

蜜罐防护

集成蜜罐系统配合传统的特征防护构建“主动 + 被动”防护体系，通过伪装，数据诱捕以及威胁数据分析三种能力，精准定位攻击行为与攻击溯源。

机器人防护

通过验证码 + 动态令牌 + 限速技术，有效对抗各类自动化攻击与交易欺诈行为，防止黑产对企业内网以及在线业务的破坏，保障业务的安全运行和用户个人数据安全。

失陷主机防护

通过有效识别阻断失陷主机的外联行为，为用户提供了应对该类攻击行为的有效防护手段。

扫描陷阱防护

基于隐蔽陷阱，识别捕获爬虫和遍历行为，主动拦截黑客攻击，防御恶意扫描。

智能封禁防护

以实时模式和行为分析为基础，采用独有的智能封禁算法，有效防御高频攻击行为。

入侵防御防护

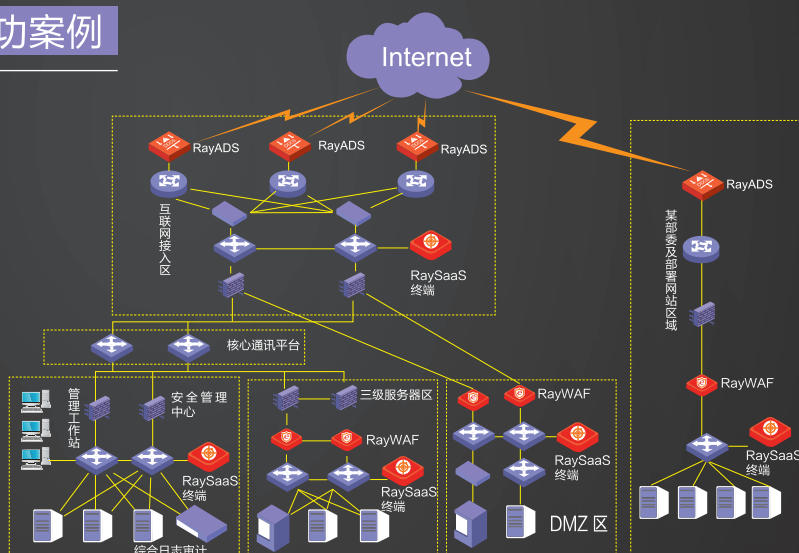
通过核心技术将引擎、协议分析和攻击检测进行结合，轻松应对多协议攻击行为。

SUCCESSFUL STORY 成功案例

某部委

需求分析：

- 服务器运行安全，不被攻击破坏；
- 门户网站内容安全，不被恶意篡改；
- 员工身份证及账号信息安全，不被窃取；
- 服务器稳定运行，资源不被非法占用。



方案概述：

某部委项目中，RayWAF 部署在各个服务器区域边界，在实现 Web 应用安全防护的基础上，一方面通过内置防篡改管理中心与服务器终端防篡改配合，实现篡改的发现与恢复功能；另一方面，通过与云端监控平台的联动进行灾情预警与动态的策略调整，形成一套闭合完整的安全解决方案。RayWAF 提供的功能主要有：

- 屏蔽恶意代码攻击，数据库注入及其他 Web 攻击；
- 避免网页篡改行为；
- 防止敏感数据泄露；
- 清洗 DDoS 攻击。

核心价值：

- 通过更靠近服务器的部署位置，提供有效的服务器安全；
- 识别拦截针对服务器的攻击行为，保障服务器自身安全；
- 提供必要的服务器负载均衡功能，保障服务器稳定可用；
- 识别保护服务器上传的敏感信息，保障服务器内容安全。