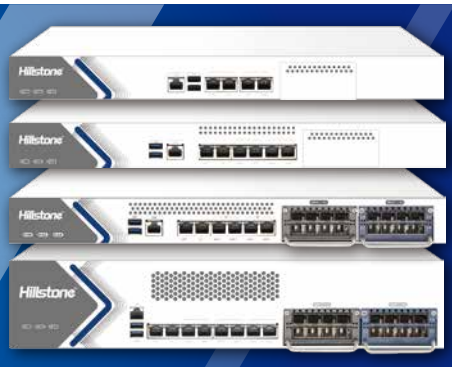
山石网科 Web 应用防火墙



山石网科 Web 应用防火墙 (以下简称：山石网科 WAF) 是新一代专业 Web 应用安全防护产品，专注于为网站及 Web 应用系统提供专业的应用层深度防御。广泛适用于政府、企业、金融、教育等行业中涉及 Web 应用安全防护的场景，满足如 PCI-DSS、等级保护、行业规范等政策法规的安全建设要求。

山石网科 WAF 充分考虑 WEB 应用系统可能存在的安全风险，通过对网络层、WEB 服务层、WEB 应用程序层、应用内容属性四个层面进行全方位安全分析与防御。针对各个层面不同的安全属性，分别采取相互独立的安全防御技术针对性防御，从整体上提升 WEB 应用的安全防御能力。

山石网科 WAF 采用双安全引擎等多种先进技术，能够有效抵御 SQL 注入攻击、跨站脚本（XSS）攻击、挂马、恶意扫描等常见 Web 攻击，支持敏感信息防泄露、网页防篡改、应用层 DDoS 防护等功能，最大限度的保障网站运行安全；同时，山石网科 WAF 支持 Web 应用加速、应用负载均衡、Bypass 和 HA 等功能，为 Web 应用提供全方位的防护解决方案。

产品亮点

深度 Web 安全防御，保障网站业务安全

山石网科WAF以用户网站为核心，通过对协议层、应用层、内容层等多层级进行针对性的安全分析与防御，可有效应对包括OWASP Top 10在内的SQL注入攻击、跨站脚本（XSS）攻击、缓冲区溢出攻击、扫描器扫描、网页挂马、盗链行为等各种Web安全威胁。

山石网科WAF采用白名单与黑名单安全引擎相结合的运作方式，实现异常流量快速阻断，增强对0day漏洞的防护能力，并且对非法请求进行深度检测，实现精准过滤，整体提升Web安全防御能力。

山石网科WAF通过采用威胁事件的数据挖掘与分析技术，实现对于攻击者的自动快速锁定与阻断，有效减低入侵风险；同时，提供敏感信息防泄露、网页防篡改、Web应用合规性检测、应用层DDoS攻击防护等功能，全面保障网站业务安全。

数字水印防篡改，保护原始网页内容

山石网科WAF可以定期抓取Web服务器的网页内容形成基线文件和缓存水印，当用户访问的页面发生篡改时，WAF向用户返回缓存的篡改前网页内容；同时WAF还提供被篡改页面的下载，可对服务器的篡改后页面进行计算机取证审计。

山石网科WAF支持“学习模式”和“保护模式”两种运行模式，在页面内容正常更新时采用“学习模式”，其他时间启用“保护模式”，有效区分恶意篡改行为和正常网站维护行为。

多种应用加速，使业务访问更高效

在提供Web安全防御的同时，山石网科WAF也高度重视用户的业务访问体验，提供了多种加速方案提升访问效率。山石网科WAF采用网页文件的高速

缓存技术，使客户访问端可直接在WAF本地获取文件，有效减少服务器交互数据，减轻Web服务器的处理负担；山石网科支持通过Web页面压缩、TCP连接复用等技术来提高传输效率，提升用户的访问体验；另外，山石网科WAF支持SSL卸载技术，可以代替Web服务器对流量进行加解密处理，在保证安全性的前提下，降低Web服务器的性能压力，提升网站的访问速度，节省运营成本。

人性化多维管理，使安全运维更简单

山石网科WAF具备丰富的安全监控与审计功能，可对网站访问情况进行实时统计和分析，实现基于安全事件级别的安全监控，将最具威胁的行为和最亟待处理的事件呈现出来。同时，可对自身状况及服务器性能状况进行监测和直观展现，可提供详尽的攻击事件日志记录，输出详细的图文式安全报表，还可及时通过邮件、SNMP、Syslog等多种方式进行告警，帮助管理员进行高效管理。

灵活可靠部署，保障 Web 业务可用性

山石网科WAF采用业界领先的透明代理技术，无需对现有网络进行改动，即可实现快速方便部署。为满足不同用户网络环境，山石网科WAF还支持镜像监听、反向代理、单臂部署、牵引部署模式等多种灵活部署方式，可应对各种复杂环境下的部署需求。

山石网科WAF还支持应用负载均衡功能，可将应用流量分配到不同的服务器上，加快访问速度，并有效避免单点故障问题。当作为串行安全设备部署时，山石网科WAF充分考虑Web业务连续性保障，提供软硬件Bypass功能，以及HA双机部署模式，保证应用访问不间断，增强运营可靠性。

功能规格

Web攻击防护

- 提供百余种攻击防护规则，能够有效的防御来自外部扫描和攻击，对OWASP TOP10风险有完整的解决方案。
- 具备注入攻击防御能力，可以对SQL注入、LDAP注入、SSI指令注入、Xpath注入、命令注入、远程文件包含以及其他注入进行防御。
- 系统具备跨站攻击防御能力，可以对跨站脚本（XSS）攻击和跨站请求伪造（CSRF）攻击进行防御。
- 系统具备特殊漏洞攻击防御能力，可以对针对Web服务器、Web框架、Web应用程序的漏洞攻击进行防御。
- 系统具备恶意软件防御能力，可以对Web Shell、木马攻击等进行防御。

协议规范性检查

- 通过HTTP协议规范性检查可以实现Web主动防御功能，如请求头长度限制、请求文件类型、请求编码类型限制等，从而障蔽了大部分非法的未知攻击行为。

抗Web扫描器扫描

- 系统具备Web访问控制能力，可以对扫描器的扫描行为、爬虫行为、目录遍历行为进行防御
- 能自动识别扫描器的扫描行为，并智能阻断如Nikto、Paros proxy、WebScarab、WebInspect、Whisker、libwhisker、Burpsuite、Wikto、Pangolin、Watchfire AppScan 、N-Stealth、Acunetix Web Vulnerability Scanner 等多种扫描器的扫描行为。

防止恶意言论提交

- 支持中文关键字解析技术，通过对用户提交信息进行过滤，有效的解决了用户提交政治敏感、违反法规相关的言论信息，从而保障网站的内容健康呈现。

Flood攻击检测和防御

- 支持常见的网络层Flood攻击检测及防御，包括Syn Flood、UDP Flood、ICMP Flood、代理攻击防护等
- 支持HTTP快速和慢速Flood攻击防御，对于检测到的攻击源头IP，可以设置黑名单进行阻断，并可以在线查看攻击内容。
- 可基于请求字段细粒度检测CC攻击，请求速率和请求集中度双重算法检测，有效应对CC慢速攻击，挑战模式识别人机访问减小误判概率，支持流量自学习建模和攻击者区域检测算法，完全隔离海外肉机，同时还能解决密码暴力猜解和商业爬虫行为。

防护盗链行为

- 支持多种盗链识别算法，能有效解决单一来源盗链、分布式盗链、网站数据恶意采集等信息盗取行为，从而确保网站的资源只能通过本站才能访问。

应用程序错误跟踪

- 能自动记录应用程序的出错信息，并能将应用程序出错信息进行分类汇总，为程序人员进行分析原因和修复程序提供了重要参考。
- 专注于动态应用程序的安全防护，考虑到门户网站对防篡改的要求，WAF内置了静态网页篡改防护与预警功能，防止篡改的页面显示到用户端并将篡改事件及时告警。

Cookie安全

- 支持Cookie自学习，防止Cookie被篡改或劫持
- 支持Cookie Http only机制。

Web访问行为合规

- 网站业务均需要逻辑上的合规判断，WAF根据业务逻辑顺序建立起一套业务合规性规则，对不符合业务合规性规则的访问行为进行拦截。

告警及防御

- 支持对触发规则行为仅告警。
- 支持针对触发安全规则的行为进行阻断。
- 支持告警页面重定向至其它URL。
- 支持邮件、Syslog、SNMP等告警方式。
- 支持将攻击者列入网络黑名单进行网络阻断该IP。

部署方式

- 支持透明串接部署，无需变更网络配置。
- 支持镜像监听部署，无需变更网络配置。
- 支持反向代理部署。
- 支持单臂部署。
- 支持牵引部署模式，含PBR回注和跨接回注。

高可用性

- 支持HA-AP模式双机热备功能。
- 支持断电Bypass功能，所有业务电口都支持硬件Bypass功能，业务光口可选支持硬件Bypass功能。

集中管理

- 支持通过山石网科HSM(安全管理中心)进行集中管理。
- 可以通过山石网科HSM进行批量升级。

Copyright © 2017，Hillstone Networks版权所有，保留所有权利。
Hillstone、Hillstone Networks标识、山石网科、StoneOS、StoneManager、Hillstone PnPVPN 均为Hillstone Networks所属商标。所有其他商标和注册商标均为其各自公司的财产。
本文所包含信息可能会有所修改，恕不另行通知，如需最新信息请浏览Hillstone Networks网站(www.hillstonenet.com.cn)。