山石网科 Web 应用防火墙

WAF | W1066 / W1160 / W1260 / W2460 / W3660

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 采用双安全引擎等多种先进技术，有效抵御 SQL 注入、跨站、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、跨站脚本、缓冲区溢出、扫描器扫描、网页挂马、盗链行为等 30 余类 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，通过对网站流量进行自学习建模生成白名单安全规则，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、HTTPS 防护、应用层 DDoS 攻击防护等功能，全面保障网站业务安全。

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。首先，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。其次，通过动态请求的 TCP 连接复用技术，实现 TCP 协议加速功能，使数据传输速度大幅提升。另外，网页流量较大会增加传输时间，山石网科 WAF 支持在线内容压缩功能，将服务器返回的内容进行压缩传输，提升业务访问速度。

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，还可及时通过邮件或短信方式进行告警，帮助管理员进行高效管理。

山石网科 WAF 具备独特的自动服务发现功能，可对 Web 网站服务进行监测和自动发现，避免人工配置失误，不需复杂环境调研即可实现快速安全防护策略的部署，真正做到即插即用。在做策略调整时，山石网科 WAF 可将海量告警日志进行自动统计分析，一键完成策略智能适应，减少人工分析成本。

灵活可靠部署，保障 Web 业务可用性

产品亮点

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 还支持反向代理、旁路监测、路由模式、网关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。

关键指标

Web 应用防火墙

指 标	SG-6000-W1066	SG-6000-W1160	SG-6000-W1260	SG-6000-W2460	SG-6000-W3660
					
吞吐量	1G	4G	4G	4G	10G
最大并发连接数	80,000	150,000	250,000	300,000	550,000
每秒新建连接数	4000	30,000	35,000	40,000	40,000
应用层吞吐	800M	1.5G	1.6G	1.8G	5G
管理口	1 个管理口、1 个 HA 口 1 个 RS232 串口	1 个管理口、1 个 HA 口 1 个 RS232 串口	1 个管理口、1 个 HA 口 1 个 RS232 串口	1 个管理口、1 个 HA 口 1 个 RS232 串口	1 个管理口、1 个 HA 口 1 个 RS232 串口
标配网口	4GE 电口	4GE 电口	4GE 电口 +4SFP 光口	4GE 电口	2SFP+ 万兆光口
标配 BYPASS	2 组 BYPASS 电接口	2 组 BYPASS 电接口	2 组 BYPASS 电接口	2 组 BYPASS 电接口	1 组 BYPASS 光接口
扩展模块槽	无	1 个通用扩展槽	2 个通用扩展槽	1 个通用扩展槽	1 个通用扩展槽
扩展模块选项	无	IOC-4SFP-W	IOC-8GE-B-W、IOC-4GE-B-4SFP-W、IOC-2SFP-B-W、IOC-8SFP-W、IOC-2SFP+-B-W、IOC-4SFP-B-W	IOC-4GE-B-W、IOC-4SFP-W、IOC-2SFP-B-W	IOC-4SFP-W、 IOC-2SFP-B-W
电源	AC: 100~240V 50~60Hz 单电源	AC: 100~240V 50~60Hz 双冗余热插拔电源	AC: 100~240V 50~60Hz 双冗余热插拔电源	AC: 100~240V 50~60Hz 双冗余热插拔电源	AC: 100~240V 50~60Hz 双冗余热插拔电源
最大功率	250W	300W	350W	460W	460W
尺寸 (W × D × H, mm)	1U(440x400x44)	2U(440x470x88)	2U(440x580x88)	2U(440x580x88)	2U(440x580x88)
工作环境	温度 5~40℃（41~104° F） 湿度 20~90%RH 海拔－ 20~3500 米（－ 60~10000 英尺）				
MTBF	大于 65000 小时				

功能规格

防护30余类Web通用攻击

- 系统内置了30余类的通用Web攻击特征有效的防御来自外部的如SQL注入、文件注入、命令注入、配置注入、LDAP注入、跨站脚本等，部署WAF后自动障蔽相应的Web攻击行为，对OWASP TOP10有完整的解决方案。

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

- 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。

防护敏感信息泄露

- 具备双向内容检测的能力，能识别服务器页面内容的敏感信息，防止敏感信息泄露，如服务器出错信息，数据库连接文件信息，Web服务器配置信息，网页中的连续出现的身份证、手机、邮箱等个人信息均可被WAF识别并依据策略采取相应的措施

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。

CC攻击防护

- 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。

静态网页篡改防护

- 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，同时支持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，不符合业务合规则则拦截。