华为WAF2000&5000系列
Web应用防火墙

WAF2210

WAF2230

WAF5220

WAF5230

产品概述

华为Web应用防火墙是一款专业的Web应用安全防护产品，适用于PCI-DSS、等级保护、企业内控等规范中信息安全的合规建设，采用多种先进技术，提供Web应用实时深度防御、Web应用加速、敏感信息防泄露、网页防篡改等功能，能够抵御各类针对Web应用的外来攻击，最大限度的保障网站运行安全。

产品特点

首创双引擎架构

- 用户行为异常检测引擎（WebUBAD），快速识别正常行为，提供最优访问体验。
- 透明代理引擎（Transparent Proxy）实现HTTP协议完整还原，从根源上避免绕过及穿透攻击。
- CPU多核绑定技术，实现流量快速转发，兼顾WEB应用检测的复杂运算。

专利级检测算法与云安全中心强强联合

- 多项专利技术保障识别能力，精确识别OWASP Top 10等各种Web通用攻击。
- 独创行为状态链检测技术，有效应对盗链、跨站请求伪造等WEB特殊攻击。
- 云安全中心提供国内最为全面的内容管理系统（CMS）0day防护策略。

精细控制策略

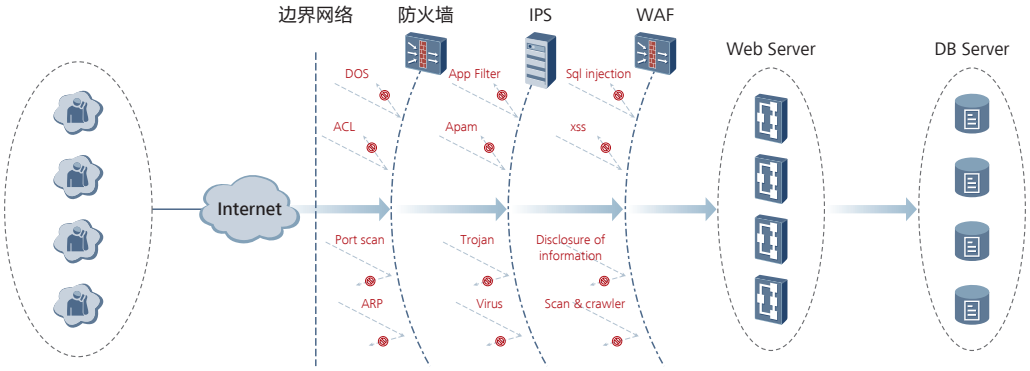
- 基于IP信用度的动态阻断策略，对高信用IP仅阻断带攻击的请求，对低信用度IP实现网络封锁。
- 基于URL粒度的安全规则实现WEB资源的差异化防护。
- 基于完整HTTP协议框架，可灵活定制各种复杂WEB防护特定策略。

纵深业务安全防御

- 基于HTTP应用的DDoS防护，有效应对应用层CC攻击对业务的冲击。
- 基于隐私信息保护技术，有效应对商业爬虫对商业数据的抓取行为。
- 基于用户行为分析，有效应对同行发起的恶意预定及抢购行为。

部署灵活运维简单

- 站点资源自动发现，真正即插即用。
- 策略自学习，自动生成最符合您业务的专属策略。
- 日志自挖掘，展现您最需关注的威胁。



华为企业ICT解决方案 悉您所需 为您所用

HUAWEI

功能概述

Web防护能力：华为WAF基于7层防护技术，深入理解应用层内容，在引入了安全白名单、安全黑名单等技术进行双引擎防护；对于应用层CC和恶意商业数据抓取等攻击，WAF可基于页面次数和时间算法统计进行防护；对于HTTP慢攻击或包分片攻击，WAF可对数据包完整重组后识别攻击。从而有效防御应用层攻击，且误报率和漏报率低，仅为0.0001%。

特征库黑名单：华为WAF内置了30余类的通用Web攻击特征，通过大量项目实践，精炼出580多个类别的攻击特征，全面覆盖了Web应用安全存在的主要安全威胁，防护各类SQL注入、跨站、挂马、扫描器扫描、敏感信息泄露、盗链行为等攻击，同时低误报率、低漏报率。

策略自学习建模及白名单防护技术：华为WAF采用自学习建模技术通过对访问流量的自学习和概率统计算法分析，结合白名单技术对网站的正常访问行为规律进行分析和总结，生成一套针对网站特性的安全白名单规则，对正常的请求直接进行放行，快速识别安全的请求。白名单比传统WAF的特征库防护的误报率更低，可有效防护0day攻击。

网页篡改监测：通过内置自学习功能获取Web站点的页面信息，对整个站点进行爬行，爬行后根据设置的文件类型（如html、css、xml、jpeg、png、gif、pdf、word、flash、excel、zip等类型）进行缓存，并生成唯一的数字水印，实时监测网站服务器的相关是否给非法更改，一旦发现被改则第一时间通知管理员，并形成详细的日志信息。与此同时，WAF系统将对外显示之前的正确页面，防止被篡改的内容被访问到。

Web应用加速：通过高速缓存和相关算法镜像及管理相关的静态内容，以及TCP连接复用，实现应用加速。

高可用性：华为WAF支持透明模式的HA/Bypass，平均无故障时间MTBF大于65000小时。

透明代理技术：华为WAF可实现快速方便的部署，无需对现有环境进行改动。

站点自动侦测：华为 WAF 对经过自身的流量自动学习，可获取 Web 应用服务器信息，如服务器 IP、TCP 端口、域名等信息。管理员不需要通过复杂的环境调研和现场确认，即可直接将自动发现 Web 应用服务器添加至 WAF 的保护站点中，即插即用，实现快速安全防护策略的部署。

智能识别 SSL 网关应用层真实 IP：华为 WAF 能识别 SSL 网关前端的真实客户端地址，便于管理员根据真实客户端地址进行访问控制。

访问审计：华为WAF支持对所有的Web请求进行审计分析记录，提供详细的访问日志分析，以图表的形势展现Web服务的业务访问情况。同时，通过对访问记录的深度分析，可发掘潜在安全威胁，对于攻击防护遗漏的请求，仍然可以起到追根索源的目的。

实时安全告警与响应：华为WAF内置邮件与短信告警接口，检测到入侵攻击行为时可自动将告警信息发送到管理员邮箱或管理员手机中。

支持多种部署方式：华为WAF支持透明代理模式、旁路监听模式、反向代理模式、网关模式等多种部署模式，可根据用户网络环境使用不同的部署模式，实现灵活部署，满足不同用户需求。

详细安全日志：能够详细的记录HTTP协议相关的任何攻击信息，如请求的URL、POST内容、响应头部、页面内容等，为安全事件分析、安全事件追溯以及安全取证等提供了最为直接的依据。

技术规格

型号	WAF 2210	WAF 2230	WAF 5220	WAF 5230
接口规格				
专用管理口	2×GE(RJ45)（1×管理口，1×HA 口）	2×GE(RJ45)（1×管理口，1×HA 口）	2×GE(RJ45)（1×管理口，1×HA 口）	2×GE(RJ45)（1×管理口，1×HA 口）
工作口	4×GE(RJ45)	4×GE(RJ45)	4×GE(RJ45) 4×GE (SFP)	4×GE(RJ45) 2×10GE(SFP)
关键特性				
特征库黑名单	系统内置了 30 余类的通用 Web 攻击特征，精炼出 580 多个类别的攻击特征，全面覆盖了 Web 应用安全存在的主要安全威胁，防护各类 SQL 注入、跨站、挂马、扫描器扫描、敏感信息泄露、盗链行为等攻击，低误报率、低漏报率。			
抗 Web 扫描器扫描	自动识别扫描器扫描行为，并智能阻断如 Nikto、Paros proxy、Web Scarab、Web Inspect、Whisker、libwhisker、Burp suite、Wikto、Pangolin、Watch fire 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、邮箱等个人信息等。			
防护盗链行为	支持多种盗链识别算法，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。			
策略自学习建模及白名单防护技术	对网站的正常访问行为规律进行分析及总结，并生成一套针对网站特性的安全白名单规则，对正常的请求直接进行放行，提升了访问性能。白名单比传统 WAF 的特征库防护的误报率更低，可有效防护 0day 攻击。			
静态网页篡改防护	系统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。			
应用层 DDOS 攻击防护	基于 URL 级别的访问频率统计，并通过访问行为建模检测出 CC 攻击的来源，对 CC 攻击者采取限时锁定措施从而有效措施来自外网的 CC 攻击行为，该功能还可有效解决因验证码技术落后而导致的口令爆破问题。			
Web 应用加速	采用 Web Cache 技术、静态文件缓存技术，动态请求的 TCP 连接复用技术实现网站访问速度的提升。			
高可用性	支持透明模式的 HA/Bypass，平均无故障时间 MTBF 大于 65000 小时。			
透明代理技术	无需对现有环境进行改动，实现快速方便的部署。			
站点自动侦测	对经过 WAF 的流量自动学习，可获取 Web 应用服务器信息，如服务器 IP、TCP 端口、域名等信息。管理员不需要通过复杂的环境调研和现场确认，即可直接将需要防护的 Web 应用服务器添加至 WAF 的保护站点中。			
智能识别 SSL 网关应用层真实 IP	能识别 SSL 网关前端的真实客户端地址，便于管理员根据真实客户端地址进行访问控制。			
访问审计	对网站的访问情况进行统计分析呈现即时访问量趋势图、用户最关注的网页、访问者最集中的地市区域等信息，便于分析网站的业务模块的访问情况，并为业务功能的价值提供评价参考。			
实时安全告警与响应	系统内置邮件与短信告警接口，可自动将告警信息发送到管理员的邮箱或手机中。			
支持多种部署方式	支持透明代理模式、旁路监听模式、反向代理模式、网关模式等多种部署模式，实现灵活部署，满足不同用户需求。			
整机规格				
尺寸（W×D×H）mm	460×440×44	460×440×44	460×440×88	580×440×88
电源	AC：100～240V 50/60Hz 单电源	AC：100～240V 50/60Hz 单电源	AC：100～240V 50/60Hz 1+1 冗余电源	AC：100～240V 50/60Hz 1+1 冗余电源
最大功率	250W	250W	300W	460W
工作环境	温度： 5~40℃（41~104°F） 湿度：20%～90% 不结露	温度： 5~40℃（41~104°F） 湿度：20%～90% 不结露	温度： 5~40℃（41~104°F） 湿度：20%～90% 不结露	温度： 5~40℃（41~104°F） 湿度：20%～90% 不结露
MTBF	大于 65000 小时	大于 65000 小时	大于 65000 小时	大于 65000 小时