华为WAF5000系列Web应用防火墙

网站作为商务贸易、客户交流、信息共享平台，承载着各类虚拟业务的运营，蕴含客户账号、交易记录等重要信息。与此同时，由于攻击技术门槛低以及可带来的巨大商业利益，网站已成为各国黑客的主要攻击目标。通常网络中会部署防火墙、IPS等安全产品，但是这类产品对于HTTP和HTTPS的Web应用层攻击往往无法察觉，不能起到理想的防护效果。专门针对Web应用防护的WAF(Web Application Firewall)产品应运而生。

华为WAF专注于7层防护，采用最为先进的双引擎技术，用户行为异常检测引擎、透明代理检测引擎相结合的安全防护机制实现各类SQL注入、跨站、挂马、扫描器扫描、敏感信息泄露、盗链行为等攻击防护，并有效防护0day攻击，支持网页防篡改。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。

同时，华为WAF支持Web应用加速，支持HA/Bypass部署配置以及维护。此外，华为WAF支持透明模式、旁路监听模式、反向代理模式等部署模式，广泛适用于“金融、运营商、政府、公安、教育、能源、税务、工商、社保、卫生、电子商务”等涉及Web应用的各个行业。

产品图

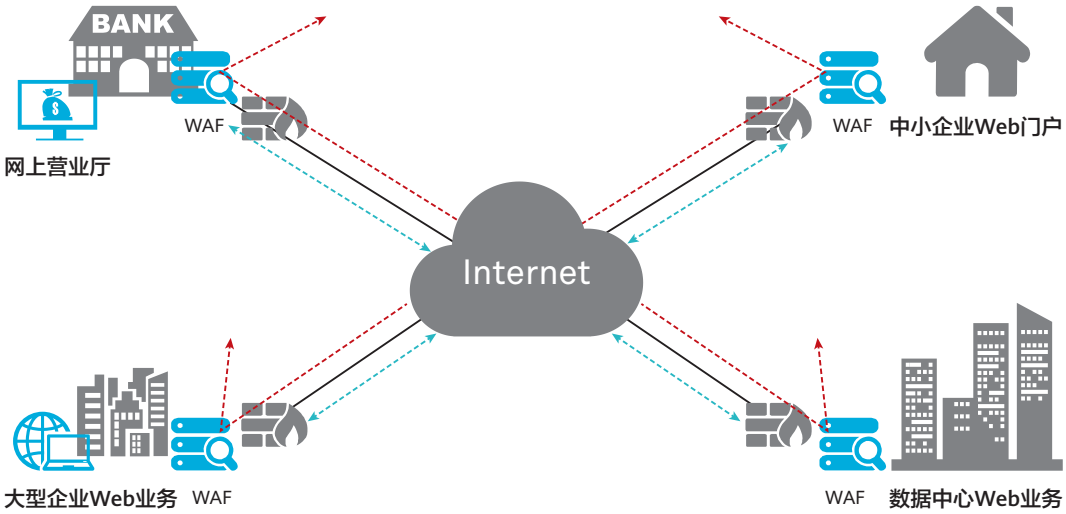
华为WAF5000系列Web应用防火墙包括四款硬件型号WAF5110、WAF5250、WAF5260和WAF5510，满足不同处理性能要求。此外，还支持WAF5000-V系列软件形态WAF产品。

华为WAF5000系列Web应用防火墙

HUAWEI

产品特点

华为WAF5000系列Web应用防火墙采用多种先进技术，对网络防火墙过滤后的流量进一步检测，帮助用户解决目前所面临的各类网站安全问题，如：注入攻击、跨站脚本攻击、恶意编码(网页木马)、缓冲区溢出、信息泄露、应用层DoS/DDoS攻击等。



华为WAF可有效拦截穿越网络防火墙的威胁事件

黑白名单

- 通过安全白名单检测引擎快速识别正常访问业务流量并快速转发，提供网站最优访问体验。
- 通过黑名单检测引擎实现HTTP协议完整还原，对疑似攻击流量深入检测，从根源上避免绕过及穿透攻击。
- 黑白名单双引擎架构协同工作，既能有效识别和阻断Web攻击又不影响正常的Web业务运营。

全面检测

- 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。
- 内置全面的内容管理系统（CMS）0day防护策略，有效防护第三方CMS漏洞。
- 独创访问集中度和HTTP协议细粒度检测算法,精准防御应用层CC攻击。
- 内置国家级地址库，可根据地址位置进行在线封锁。

智能防护

- 站点服务自动发现，智能锁定防护对象。
- 策略自学习，智能调整成符合业务的安全策略。
- 智能防护锁缓解黑客持续化攻击。
- 自动生成多维度报表，展现最需关注的威胁。
- 规则库实时在线更新，有效应对新型Web攻击。
- 支持业内主流扫描器，自动生成虚拟补丁，快速修复网站漏洞。

系统可靠

- 多种部署模式，适应各种网络环境。

- 透明代理和反向代理下支持HA功能，实现配置同步。
- 支持设备系统、端口自检测功能，一旦出现故障自动切换到Bypass状态。

功能概述

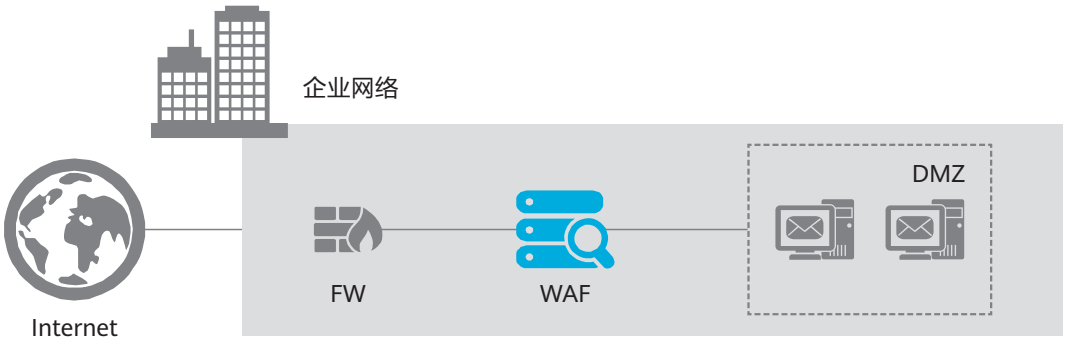
- **通用Web攻击防护：**内置30余类的通用Web攻击特征，通过大量项目实践，精炼出580多个类别的攻击特征，全面覆盖了Web应用安全存在的主要安全威胁，防护各类SQL注入、跨站、挂马、扫描器扫描、敏感信息泄露、盗链行为等攻击，同时低误报率、低漏报率。
- **网页篡改攻击防护：**通过内置自学习功能获取Web站点页面信息，对整个站点进行爬行，爬行后根据设置的文件类型（如html、css、xml、jpeg、png、gif、pdf、word、flash、excel、zip等类型）进行缓存，并生成唯一数字水印，实时监测网站服务器是否被非法更改，一旦检测到篡改行为立即通知管理员，并形成详细的日志信息。与此同时，WAF系统将对外显示之前的正确页面，防止被篡改内容的发布。
- **Web扫描器扫描防护：**支持自动识别扫描器的扫描行为，并智能阻断多种扫描行为。
- **CC攻击防护：**基于URL、请求头字段、目标IP、请求方法等多种组合条件进行检测，支持URL访问速率和指定URL访问集中度检测；华为 WAF支持真实攻击者IP识别，默认支持解析X-Forward-For头，并支持自定义方式；支持挑战模式。支持设置用户区域级检测算法，隔离海外或跨省攻击。
- **网页盗链行为防护：**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、网站数据恶意窃取等信息盗取行为，从而确保网站的资源只能通过本站才能访问。
- **敏感信息泄露防护：**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识别并依据策略采取相应措施。
- **恶意言论提交防护：**支持中文关键字解析技术，通过对用户提交信息进行过滤，有效解决匿名提交政治敏感、违反法律法规等恶意言论，保障网站内容健康呈现。
- **应用程序错误跟踪：**自动记录应用程序出错信息，并将出错信息进行分类汇总，为Web业务运维人员解决技术问题提供原因分析和修复建议。
- **合规检查主动防护：**通过HTTP协议规范性检查实现Web主动防御功能，如请求头长度限制、请求编码类型限制等屏蔽大部分非法未知攻击行为。
- **策略自学习建模及白名单防护：**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特征库防护误报率低，可有效防护0day攻击。
- **Web应用加速：**采用WebCache技术对防护网站进行加速，通过静态文件缓存技术，动态请求的TCP连接复用技术实现网站访问速度提升。
- **支持多种部署方式：**支持透明模式、反向代理模式、旁路监听模式、集群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。
- **高可靠性：**支持反向代理和透明模式下的HA/Bypass，平均无故障时间MTBF大于65000小时。
- **站点自动侦测：**对经过设备的流量自动学习，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。
- **站点访问审计：**支持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：**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。

典型应用

华为WAF一般部署在传统防火墙后端，Web服务器前端，支持透明模式、旁路监听模式、反向代理模式等部署模式。需要说明的是，WAF5000-V系列软件WAF仅支持反向代理部署模式。

对企业DMZ区进行专业Web防护

将华为WAF5000系列WAF产品部署在企业核心交换机和接入交换机之间，可对企业DMZ区的Web业务起到很好的防护作用。当企业有多个DMZ区的服务器需要防护时，也可将WAF部署在传统防火墙和核心交换机之间实现防护。

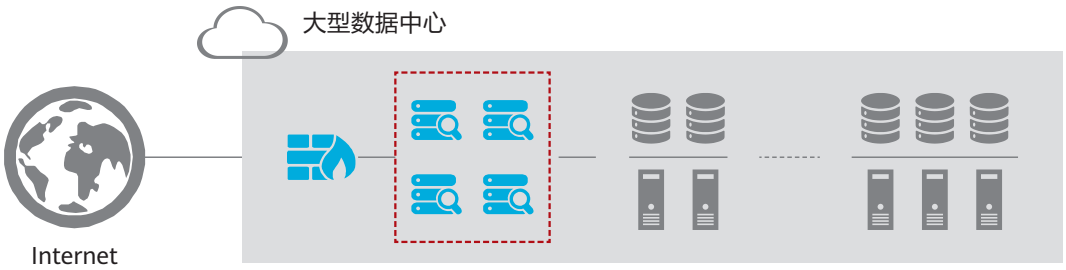


企业DMZ区防护典型组网

此外，为了应对复杂的网络部署环境，当客户网络流量较大或者不希望采用串接方式时，华为WAF5000系列产品支持反向代理特性，可旁挂于核心交换机或者路由器。

大型数据中心WAF集群防护

对于大型数据中心等网络流量大的场景，华为WAF5000系列产品支持集群部署。多台WAF负载均衡，同时配合交换机的链路捆绑技术，实现多台WAF流量负载。



WAF集群Web业务防护典型组网

产品规格

产品型号	WAF 5110	WAF 5250	WAF 5260	WAF 5510	WAF5000-V
接口规格					
专用管理口	2*GE电口 (管理口*1，HA口*1)	2*GE电口 (管理口*1，HA口*1)	2*GE电口 (管理口*1，HA口*1)	2*GE电口 (管理口*1，HA口*1)	NA
工作口	4*GE电口，2组硬件BYPASS模块	4*GE电口，2组硬件BYPASS模块	4*GE电口，2组硬件BYPASS模块 4*GE光口，不含硬件BYPASS模块	2*10GE光口，1组硬件BYPASS模块	NA
支持扩展卡(硬件WAF)/支持虚拟化平台(软件WAF)	不支持	不支持	插卡式8*GE电业务口，4组硬件BYPASS模块 插卡式4*GE电业务口，4*GE光业务口，含2组电口硬件BYPASS模块 插卡式4*GE光业务口，2组硬件BYPASS模块 插卡式8*GE光业务口，不含硬件BYPASS模块 (4选2)	插卡式8*GE电业务口，4组硬件BYPASS模块 插卡式4*GE电业务口，4*GE光业务口，含2组电口硬件BYPASS模块 插卡式4*GE光业务口，2组硬件BYPASS模块 插卡式8*GE光业务口，不含硬件BYPASS模块 插卡式2*10GE光业务口，含1组硬件BYPASS模块 插卡式4*10GE光业务口，不含硬件BYPASS模块 (6选3)	• Linux KVM，Kernel版本2.6.32以上 • XEN 4.5及以上(opensource Xen，Citrix的不支持) • VMware ESXi 5.5及以上
关键特性					
黑白名单双引擎架构	白名单与黑名单安全引擎相结合的工作方式，实现了正常请求快速识别与转发，未知请求进行深度清洗的安全策略，实现安全性与可用性的最佳结合。实现正常用户与攻击者相分离的效果，保障网站安全的同时增强了用户体验的效果。				
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。				

产品型号	WAF 5110	WAF 5250	WAF 5260	WAF 5510	WAF5000-V
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。				
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	硬件WAF支持透明代理模式、旁路监听模式、反向代理模式、集群模式等多种部署模式，实现灵活部署，满足不同用户需求。软件WAF仅支持反向代理部署模式。				
整机规格					
产品形态	1U	2U	2U	2U	NA
尺寸(W×D×H)cm	44×26×4.4	44×47×8.8	44×62×8.8	44×60×8.8	NA
电源	AC： 100～240V 50/60Hz 单电源	AC： 100～240V 50/60Hz 1+1冗余电源， 可热插拔	AC： 100～240V 50/60Hz 1+1冗余电源， 可热插拔	AC： 100～240V 50/60Hz 1+1冗余电源， 可热插拔	NA
最大功率	250W	300W	300W	300W	NA
工作环境	温度： 5～40°C（41～104°F） 湿度：20%～90% 不结露				NA
MTBF	大于65000小时				NA

订购信息

编码	描述
硬件WAF	
WAF5110	WAF5110交流典配
WAF5250	WAF5250交流典配（2*300W交流,滑轨）
WAF5260	WAF5260交流典配（2*350W交流,滑轨）
WAF5510	WAF5260交流典配（2*760W交流,滑轨）
接口卡	
WAF-8GE-4BY	8*GE电业务口，4组硬件BYPASS模块
WAF-4GE-4GEF-2BY	4*GE电业务口，4*GE光业务口，含2组电口硬件BYPASS模块
WAF-4GEF-2BY	4*GE光业务口，2组硬件BYPASS模块
WAF-8GEF	8*GE光业务口，不含硬件BYPASS模块
WAF-2XGEF-1BY	2*10GE光业务口，含1组硬件BYPASS模块
WAF-4XGEF	4*10GE光业务口，不含硬件BYPASS模块
License	
LIC-HARDAV-1Y-WAF	硬件WAF特征库升级服务时间续购12个月
软件WAF	
WAF5000-V-4-1Y	WAF5000-V（防护4站点）软件1年订阅费
WAF5000-V-4-3Y	WAF5000-V（防护4站点）软件3年订阅费
WAF5000-V-8-1Y	WAF5000-V（防护8站点）软件1年订阅费
WAF5000-V-8-3Y	WAF5000-V（防护8站点）软件3年订阅费
WAF5000-V-16-1Y	WAF5000-V（防护16站点）软件1年订阅费
WAF5000-V-16-3Y	WAF5000-V（防护16站点）软件3年订阅费
WAF5000-V-32-1Y	WAF5000-V（防护32站点）软件1年订阅费
WAF5000-V-32-3Y	WAF5000-V（防护32站点）软件3年订阅费
LIC-SITE-1Y-WAF	增加一个防护站点软件1年订阅费
LIC-SITE-3Y-WAF	增加一个防护站点软件3年订阅费