WAF 防火墙设备指标及参数说明：

| 指标 | 功能参数 | | 数量 | 单位 | 备注 |
|---|---|---|---|---|---|
| 设备基本要求 | 专用的硬件和软件保障 | 采用专用硬件架构与专用安全操作系统，基于操作系统内核的完全检测技术；硬件设备可以机架安装。产品必须为专业性 WEB 应用防火墙硬件设备，而非下一代防火墙 \UTM 类设备集成的 WEB 防护功能；硬软件质保期≥ 3 年，需提供厂家质保证明文件 | 1 | 台 | |
| | 硬件模块化设计 | 硬件采用模块化设计，可以通过扩展卡来增减业务接口，而非软件 WAF。 | | | |
| | 端口数量和扩展能力 | 2U机架式结构；最大配置为 26 个接口；默认包括 2 个可插拔的扩展槽和 4 个 10/100/1000BASE-T 接口和 4 个 SFP插槽（其中 2 个 SFP+万兆插槽），2 个 10/100/1000BASE-T 接口（作为HA口和管理口）； | | | |
| | MTBF | 不少于 450000 小时 | | | |
| 性能要求 | 应用层吞吐率 | 3G | | | |
| | 最大吞吐能力 | 20G | | | |
| | 并发 TCP会话数 | 300 万 | | | |
| 网络部署 | 部署方式 | 无 IP 纯透明模式串联部署、旁路监测模式部署、负载均衡模式部署、反向代理模式部署。 | | | |
| | | 串联部署时防护口不占用 IP 地址。 | | | |
| | | 串联部署时服务器可以看到真实客户端源 IP，而不是 WAF的业务 IP 地址。 | | | |
| | 网络适应性 | 支持 VLAN划分，支持多 VLAN环境下 trunk 的部署。 | | | |
| | | 支持虚拟线无论任何网络环境可强制数据从一个接口转发到另一个接口。 | | | |
| | | 物理接口支持子接口 | | | |
| | | 支持链路聚合 (Channel) 部署，提高链路带宽；支持 Trunk 链路防护。 | | | |
| | | 支持自定义配置网络接口 MTU、双工模式、双工模式等属性。 | | | |
| | | 支持静态路由及策略路由配置。 | | | |
| | | 支持 ARP绑定 | | | |
| | | 支持静态 MAC地址表配置 | | | |
| | | 支持服务器健康检查，可以实时监测服务器的活跃状态；健康记录可定期备份 | | | |
| | | 支持 IPV6 协议。 | | | |
| | | 支持 IPV6 协议下邻居指定 | | | |
| | | 支持网络层防火墙功能，支持源 IP、源区域、目的 IP、目的区域等条件的访问控制。 | | | |
| 攻击防护 | HTTPS支持 | 支持 HTTP/HTTPS站点防护 | | | |
| | 协议合规检查 | 支持请求限制配置通过定义最大请求头长度、最大 content-length 、最大 body 长度、最大请求行长度、最大 header 行长度、最多 cookies 个数、最多 header 头个数、最 | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | 大 header 长度等来对请用户数据做合规性检查。 | | | |
| | WEB安全防护 | 支持 800+条以上的应用层规则。 | | | |
| | | 应能识别和阻断 SQL注入攻击 ,Cookie 注入攻击，命令注入攻击。 | | | |
| | | 应能识别和阻断跨站脚本 (XSS)攻击。 | | | |
| | | 支持 webshell 等后门上传防护、 支持对中国菜刀等工具对后门连接的阻断。 | | | |
| | | 支持对 appscan、 awvs 等扫描器的扫描防护 | | | |
| | | 支持远程文件包含、本地文件包含、目录遍历、信息泄露等攻击防护 | | | |
| | | 支持 HTTP参数污染攻击、 00 截断、 Struts2 命令执行等常见攻击防护 | | | |
| | | 支持爬虫防护且用户可以根据需要可以自定义爬虫 | | | |
| | | 支持暴力登录防护，用户可以根据需要配置需要防护暴力登录的界面 | | | |
| | | 支持盗链防护，且支持攻击源盗链例外配置，及目的服务器 URI 例外配置。 | | | |
| | | 应能识别和阻断跨站请求伪造 (CSRF)攻击 | | | |
| | | 支持 IP 黑白名单、 URL黑白名单控制。 | | | |
| | | 支持对身份证、信用卡、手机电话号码、座机电话号码、邮箱地址等敏感信息做检查，当检查到此类数据后可通过配置特殊字符予以替换隐藏，防止信息泄露。 | | | |
| | | 支持对 URL编码、多次编码等方式绕过 WAF的编码方式进行识别，防止绕过。 | | | |
| | | 可对文件上传做控制，包括最多上传文件数、最大文件上传大小、可以通过对上传文件的扩展名、 MIME类型及允许请求体编码类型等做上传控制。 | | | |
| | | 可对文件做下载控制，包括最大下载文件大小、禁止下载文件的扩展名、 MIME类型等 | | | |
| | | 检测到攻击后支持阻断、只检测等动作且动作为阻断时用户可自定义阻断页面。 | | | |
| | | 支持 URI 策略例外，可针对服务器上 URL中的特殊 URI 地址做单独的策略控制。 | | | |
| | | 支持自学习建模功能，可以通过学习正常 URL参数的长度、参数类型、请求方法等数据特点创建白名单模型，如果参数违反白名单模型则认为是非法流量直接阻断。开启自学习建模功能后可生成自学习网站参数的自学习结果报告。 | | | |
| | | 支持虚拟补丁功能，支持导入 appscan 、w3af 等第三方扫描器的扫描结果生成 WAF的规则，对此类网站漏洞直接防护。 | | | |
| | | 可停用或启用任意一条规则，当触发规则后可以制定针对该条规则的动作，包括阻断记录日志、阻断不记录日志、继续、警告、临时或永久跳转到某一重定向页面等动作。 | | | |
| | | https 证书支持直接将证书内容填充到 waf 内使用，不用再上 | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | 传或者转换证书使用。 | | | |
| | 配置易用性 | 可以针对服务器 IP 地址进行防护，而不需要配置需要防护的网站域名。 | | | |
| | | 支持域名自学习，可以自动学习网络中网站服务器的 IP 地址及此地址下的域名。 | | | |
| | DDoS攻击防护 | 支持基线学习，可以自动学习用户 http 正常流量阈值模型，并给出推荐阈值配置项。 | | | |
| | | 对 ddos 流量支持检测清洗和强制防御两种模式，检测清洗根据是否到达阈值对流量进行清洗，强制清洗对所有流量直接进行流量清洗判断。 | | | |
| | | 支持针对每秒包数、每秒新建连接数、每秒并发连接数对 HTTP/HTTPS Flood 攻击做控制配置。 | | | |
| | | 支持对客户端在单位时间内的访问 URI 的次数做控制配置，防止特定 URI 路径被 HTTP Flood 恶意 ddos 攻击访问消耗服务器资源导致服务器拒绝服务。 | | | |
| | | 支持对 SLOW HEADER 和 SLOW POST 的等慢速 ddos 攻击的防护。 | | | |
| | | 支持对 HTTP/HTTPS Flood 攻击源的发包速度、源新建连接数、源并发连接数做源限速控制配置，且可以阻断攻击或者将攻击 IP 加入黑名单。 | | | |
| | | 支持对 HTTP/HTTPS Flood 攻击目的服务器的发包速度、源新建连接数、源并发连接数做目的限速控制配置，且可以阻断攻击或者将攻击 IP 加入黑名单。 | | | |
| | | 支持对 HTTP/HTTPS Flood 攻击做重定向或验证码验证，将异常流量加入黑名单。 | | | |
| | 网页防篡改 | 网关型网页防篡改，无需在服务器中安装任何插件，可以对动态网。<br>站及静态网站文件内容进行防篡改，当检测到篡改后可以实时恢复篡改内容。 | | | |
| | WEB漏洞扫描 | 支持多种 WEB 应用漏洞的安全扫描检测，如 SQL注入、跨站脚本、目录遍历等。 | | | |
| | | 支持自定义 WEB 漏洞扫描任务，支持对需要认证登录的 web 系统进行漏洞扫描，支持自定义每日、每周、每月等扫描周期设置。 | | | |
| | | 可导出 web 漏洞扫描报告，报告支 pdf,html,txt,xml 等格式导出。 | | | |
| | 负载均衡 | 支持多服务器的负载均衡，支持轮叫、加权轮叫、原地址散列、最小连接等多种负载均衡算法。 | | | |
| | | 能配合现有的负载均衡设备协同工作，支持任意部署，而不影响客户现有拓扑。 | | | |
| 数据分析 | 网络数据分析 | Web界面可以直观查看 WAF 扩展卡、接口、USB口、管理口、HA口及业务口的运行状态。 | | | |
| | | 可以查看使用业务接口的上下行实时流量。 | | | |
| | | 可以查看通过 WAF 的所有 IPV4 及 IPV6 客户端和服务器 IP 地 | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | 址及端口连接数及状态。 | | | |
| | | 可以实时查看设备新建连接数、并发连接数、每秒事务数及HTTP应用层吞吐率等数据并以可视化的方式展示。 | | | |
| | 设备运行数据分析 | 可以实时查看设备 CPU、内存、SSD固态硬盘等自身使用率情况。 | | | |
| | 日志报表数据分析 | 日志支持以 syslog 和 welf 两种格式向远端日志服务器发送日志。 | | | |
| | | 日志传输可加密，且管理员可以配置加密密码。 | | | |
| | | 支持系统日志、管理员登录日志、调试日志的记录 | | | |
| | | 流量日志（访问日志）支持记录包括时间、客户端 IP、客户端端口、服务器 IP、服务器端口、协议类型、服务器 IP 地址、访问的 URL 地址、请求方法、服务器响应、接口及发送数据大小等相关信息。 | | | |
| | | 攻击日志支持记录包括时间、严重程度、客户端 IP、客户端端口、服务器 IP、服务器端口、协议类型、时间类型、触发规则 ID、解决建议、处理动作、攻击请求头等相关信息。 | | | |
| | | 支持防篡改日志及抗 DDOS日志的记录。 | | | |
| | | 日志支持多条件与查询，支持 CSV及 XML格式的日志导出，日志支持清空配置。 | | | |
| | | 支持每种攻击时间类型及次数的统计并以柱状图等形式直观展现。 | | | |
| | | 支持最近一小时、一天、三十天等多种条件内攻击源 IP 攻击次数及攻击分布 TOPN的统计。 | | | |
| 系统管理 | 系统管理 | 支持 SSL的 WEB界面、SSH、Console 多种方式管理。 | | | |
| | | 支持手工设置时间、本地同步时间、和 NTP服务器同步时间。 | | | |
| | | 支持 ping、TRACEROUTE、TCP、HTTP、DNS等多种故障诊断方式。 | | | |
| | | 支持 SNMP的 V1、V2、V3 管理，支持 SNMP陷阱主机功能。 | | | |
| | | 支持 WAF本机 DNS域名解析。 | | | |
| | | 支持 WAF配置文件导入、导出及恢复出厂配置。 | | | |
| | | 支持操作系统 WEB方式升级及命令行等方式的离线升级。 | | | |
| | | 支持规则库的在线升级和离线升级。 | | | |
| | | 支持攻击日志短信告警，可以将特定的攻击类型的攻击日志发送给指定手机接收。 | | | |
| | | 支持攻击日志邮件告警，可以定时将特定攻击类型的攻击日志间隔定一定时间后定时发送至指定邮箱。 | | | |
| | | 支持攻击报表邮件告警，可以定时将攻击报表间隔定一定时间后定时发送至指定邮箱。 | | | |
| | | 告警邮件支持明文传输、支持 starttls 认证传输、支持 ssl 的加密传输。 | | | |
| | 账号及认证管理 | 支持帐号创建、帐号授权、帐号属性修改、帐号删除等账号管理功能。 | | | |
| | | 支持用户身份认证，用户切换角色时，必须进行重新认证。 | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | 支持超时重新认证机制并能够定义用户认证尝试的最大允许失败次数。 | | | |
| | | 支持账号策略自定义，支持定义允许最大登录失败次数、密码错误账号锁定时间、最大在线管理员数、对其他非法在线管理员强制下线、防管理员账号暴力破解。 | | | |
| 高可用性 | 双机热备 | 支持双机热备，主备模式、主主负载均衡模式、连接保护模式(主主模式下一边断了，会话表会同步到另一边数据不丢包)。 | | | |
| | | 支持两台 WAF配置同步。 | | | |
| | | 支持同一台 WAF上下接口状态联动 (一个接口 down另外一个接口也同步 down) 。 | | | |
| | | 两台 WAF路由模式接入、两台 WAF纯透明交换模式接入。 | | | |
| | 硬件 Bypass 功能 | 支持开机及断电 bypass 模式，光口支持外置 bypass 模块。 | | | |
| 资质要求 | 厂商资质 | 中国信息安全测评中心颁发的《中国国家信息安全漏洞库（CNNVD）一级技术支撑单位》<br>国家互联网应急中心颁发的《网络安全应急服务支撑单位 -国家级》<br>中国信息安全认证中心颁发的《一级应急处理服务资质》<br>中国信息安全认证中心颁发的《一级风险评估服务资质》 | | | |
| | 产品资质 | 中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》 | | | |
| | | 国家保密科技测评中心颁发的 《涉密信息系统产品检测证书》(专业 WAF类) | | | |
| | | 中华人民共和国国家版权局颁发的《计算机软件著作权登记证书》 | | | |
| | | OWASP颁发的《 web 应用防火墙认证证书》 | | | |
| | | 国家信息安全测评信息技术产品安全测评证书（ EAL3+） | | | |