|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 硬件规格 | 产品应采用1U专用机架式硬件设备，系统硬件为全内置封闭式结构,非NGFW、NGAF等下一代防火墙或UTM安全网关产品 |
| 标配4个10/100/1000自适应电口 (含两路Bypass接口)， 独立的1个管理口，1个HA接口，1个扩展插槽。 |
| 防雷击，必须通过国家无线电监测中心检测中心浪涌（冲击）抗扰度（4KV）测试项目，并出具国家无线电监测中心检测中心委托测试报告 |
| 性能参数 | 吞吐量不小于1.5G  基于HTTP的TCP并发大于10万  每秒事务处理能力(TPS)大于2万每秒  不小于1T硬盘 |
| 部署方式 | 透明桥部署：防护口不占用IP地址，实现完全透明部署，无需以先终结用户的TCP会话后再发起新的TCP会话到服务器方式处理，并支持路由不对称场景 |
| 透明代理部署：防护口不占用IP地址，实现应用层透明部署，支持TCP连接复用，并优化服务器会话处理改善服务器处理性能。 |
| 端口镜像部署：镜像服务器流量即可实现安全审计和告警，支持添加服务器网段防护 |
| 网关模式部署：通过WEB应用防火墙对外发布应用，隐藏真实服务器 |
| 负载均衡模式部署：实现对WEB服务器进行负载均衡 |
| 路由模式部署：可支持静态路由、动态路由分发，无缝路由切换 |
| 高可用性 | 支持全透明集群模式、主-主模式、主备模式、硬件BYPASS、软件BYPASS |
| 保护对象 | 支持多条链路数据的防护，可防护2路物理链路，防护网段数量不限 |
| 支持以域名和IP多种方式进行防护 |
| 支持ipv4/ipv6双协议栈 |
| WEB服务自发现 | 支持WEB站点服务自动侦测功能 |
| 支持识别VLAN信息 |
| 防御功能 | 能够识别恶意请求含：跨站脚本(XSS)、注入式攻击（包括SQL注入、命令注入 、Cookie 注入等）、跨站请求伪造等应用攻击行为 |
| 能够识别服务端响应内容导致的缺陷：敏感信息泄露、已有的网页后门、错误配置、目录浏览等缺陷 |
| 能基于访问行为特征进行分析，能识别防盗链、应用DOS攻击的能力 |
| 能识别网站中的网页木马程序，通过策略可防止木马网页被用户访问 |
| 内置主流Webshell特征库，对上传内容进行检查，防止恶意Weshell上传 |
| 支持丰富的自定义规则，可以针对多个条件组合，形成深度的WEB防护规则 |
| 支持服务器隐藏  可配置删除服务器响应头信息 |
| 支持Cookie安全机制，支持Cookie自学习  支持Cookie Httponly 支持Cookie防篡改、防劫持 |
| 智能攻击者锁定 | 支持智能识别攻击者，对网站连接发起攻击的IP地址进行自动锁定禁止访问被攻击的网站  可配置攻击者识别策略和算法  可配置攻击者锁定时间  可配置将攻击者直接加入网络黑名单  可展示攻击者发生的时间和攻击者所在的地理位置 |
| 防御动作 | 针对触发安全规则的行为进行阻断并发出告警页面 |
| 告警页面支持重定向至其它URL |
| 能将攻击者列入网络黑名单进行网络阻断该IP的访问 |
| 对攻击报文丢弃 |
| WEB访问行为合规 | 支持对访问流程的校验  可配置页面合规页面流程  可配置页面思考时间  发现访问违反合规的直接被拦截并产生告警日志 |
| CC防护功能 | 支持多种算法检测方法：对指定URL访问速率、对指定URL访问集中度检测  支持多种条件匹配算法：可基于URL、请求头字段、目标IP、请求方法等多种组合条件进行检测  检测对象支持IP或IP+URL算法，IP可支持X\_Forwarded-For字段解析，并支持自定义检测字段功能  支持挑战模式，客户端访问时WAF发起302重定向与js挑战验证是真实客户还是CC工具发起的访问  支持学习业务流量模型，在业务流量异常时开启CC防护，并支持启动配置阈值  支持基于地理位置的识别，可设置不同地理区域的检测算法  支持统计访问流量信息，进行人机对抗 |
| 篡改监控 | 系统提供防篡改功能，能够防止被篡改内容被浏览者访问到,一旦检测到被篡改，实时发送告警信息给管理员。 |
| 安全审计 | 能详细记录攻击事件的HTTP请求头信息，含请求的URL、UserAgent、POST内容，cookie等所有的请求头内容 |
| 能详细记录服务器响应头信息，服务器响应内容 |
| 日志分析 | 根据产生的安全日志进行智能分析，提高人工分析效率，减小规则误判概率 |
| 报表方式 | 支持自定义报表、定时报表、支持各类导出格式（WORD,PDF等） |
| 报表可自动发至管理员邮箱 |
| 告警方式 | 支持Syslog、手机短信、邮件等多种告警方式 |
| 访问审计 | 具备审计网站正常访问流量的能力，提供按小时，日期、月份生成报表 |
| 能记录、查询所有用户对网站的访问情况 |
| 能分析出访问量最大的URL，IP地址 |
| 能分析出访问流量最大的文件类型 |
| 加速功能 | 系统内嵌应用加速模块，通过对各类静态页面及部分脚本高速缓存，提高访问速度。 |
| 支持响应内容压缩，并支持对压缩的响应内容识别 |
| SSL透明代理 | 支持HTTPS服务器的防护，可支持第三方认证机构颁发的证书链，WEB应用防火墙前端与后端均为HTTPS加密链路，实现HTTPS应用系统的防御 |
| 部署在SSL网关后面，能够解析到真实的访问者IP，并能对真实的IP进行防护和阻断 |
| 负载均衡 | 工作在网关模式，对保护的多台负载WEB服务器，达到平均分发、按比例分发、热备等多种负载均衡模式。 |
| 设备管理 | 配置变更时不影响在线业务 |
| 支持HTTPS方式进行设备管理 |
| 设备管理采用管理员与审计员分离 |
| 操作界面支持全中文界面 |
| 防篡改软件系统功能 | 支持windows/Unix/Linux/Solarie/AIX/HP-UNI等主流操作系统。支持IIS、Apache、Weblogic、Tomcat、WebSphere等WEB发布类型。B/S架构，可以支持多客户端管理。支持管理用户密码复杂度策略设置。核心技术采用基于文件过滤驱动保护技术。 |
| 支持各类网页文件的保护，包括静态和动态网页以及各类文件信息。 |
| 支持自定义保护策略名称，提供产品截图有效。 |
| 支持仅监控保护功能。 |
| 系统需支持用户权限分级,可以设立多个基于设备的受控管理员。 |
| 支持对指定文件夹以及子文件夹的保护，避免上传非法文件及木马等恶意文件或插入恶意代码。 |
| 系统支持管理设备图形化展示，提供产品截图有效。 |
| 系统配置完成后，系统后台运行，支持断线检测。 |
| 系统支持在断线情况下对网页文件目录的防护功能。 |
| 系统支持黑白名单设置功能，提供进程黑白名单设置。 |
| 支持NFS网络文件系统防篡改保护。 |
| 支持NAS等网络存储防篡改保护。 |
| 支持docker容器应用的防篡改保护。 |
| 支持设备性能实时监控，实时告警，并图形化展示。 |
| 支持设备网络健康性监控，实时告警，并图形化展示。 |
| 防篡改保护进程被意外终止后，依然可以进行网页防护。 |
| 支持对系统关键文件目录的隐藏功能。 |
| 支持用户在监控端手动启停保护功能，并需经过身份认证。 |
| 可在管理平台对web服务器进行网络故障诊断，提供产品截图有效。 |
| 支持对系统服务进行监控功能。 |
| 提供管理中心和网页防篡改授权许可，系统注册最终用户须为采购单位，提供三年特征库升级服务 |