**南京理工大学紫金学院Web应用防护系统技术参数**

1. **项目介绍**

 为保障学校网站安全，**抵御来自应用层的威胁**，解决目前所面临的注入攻击、跨站攻击、脚本木马、缓冲区溢出、信息泄露、网页被篡改、防恶意扫描等安全问题。学校拟采购Web应用防护系统一套。

1. **技术要求**

|  |  |
| --- | --- |
| 系统架构 | 采用1U专用机架式硬件设备。专业WEB应用防护设备，非OEM、NGFW、NGAF等下一代防火墙或UTM安全网关产品。 |
| 接口数量 | 标配千兆电口≥6个；千兆光口≥4个。支持4进4出，4路同时防护 |
| 配套软件 | 提供10套投标品牌的可在WINDOWS平台上安装和运行的软件版WEB应用防护系统。（提供功能截图，加盖公章）。至少提供同品牌windows平台webshell检测工具一套搜索网站里面的网页木马，并生成统计报表。（提供功能截图，加盖公章） |
| 性能要求 | 吞吐量≥6000Mbps |
| 应用层（HTTP）吞吐量≥3000Mbps |
| 最大并发会话数≥200万 |
| HTTP请求速率≥36000次/秒 |
| 网络延迟≤0.04毫秒 |
| 不限防护网站数量 |
| 部署方式 | 支持纯透明部署，需即插即用（无需绑定域名、IP及端口号）即可防护（中标后一周内须通过现场测试验证） |
| 支持策略路由部署 |
| 透明部署时，在VLAN Trunk链路下，至少支持2条以上链路的检测与防御，并支持https协议解码。 |
| 支持端口汇聚（Trunk），显著提高设备间的吞吐能力（提供功能截图，加盖公章） |
| 支持IPv6到IPv4的协议转换（提供功能截图，加盖公章） |
| HTTPS支持 | 支持透明模式下的HTTPS协议防护，加载证书后由系统在本地完成HTTPS解密过滤再加密转发到后端服务器，服务器端无需做任何改动，实现双向加密。（提供功能截图，加盖公章） |
| 透明模式下支持上传证书格式：pem、der、pfx、p7b。（提供功能截图，加盖公章） |
| 透明模式下支持系统自动生成证书对HTTPS报文进行加密过滤（提供功能截图，加盖公章） |
| 支持非标准的443端口的HTTPS协议防护。（提供功能截图，加盖公章） |
| HTTPS证书管理 | 在线管理SSL证书，及时查看到期时间和证书域名内容，方便HTTPS的防护工作（提供功能截图，加盖公章） |
| 安全特性 | 能够同时支持IPv6/IPv4环境下的攻击检测和访问策略 |
| 支持隐藏Web服务器的类型名称 |
| 支持对恶意扫描行为开启防扫描功能，用户可自定义防护等级。 |
| 真实来源IP解析：支持解析通过代理服务器访问用户的真实IP地址，默认支持X-Real-IP或X-Forwarded-For字段的值作为真实来源IP地址，同时支持用户自定义字段名称。 |
| 支持任意碎片组包、支持超长报文组包设置，功能功能上可以对报文大小优先进行设置。（报文大小设置不低于30M）（提供功能截图，加盖公章） |
| 攻击防御手段 | 支持多虚拟web主机同时防护 |
| SQL注入攻击：攻击者通过输入数据库查询代码窃取或修改数据库中的数据 |
| XSS跨站攻击：跨站脚本攻击才利用网站漏洞攻击那些访问该站点的用户，常见目的是采取窃取该站点访问者相关的用户登陆或认证问博信息 |
| 关键文件下载：攻击者通过工具或特殊命令下载网站系统的数据库文件、配置文件信息 |
| 木马上传：攻击者利用黑客工具上传Webshell以达到控制服务器的目的 |
| 具有智能化阻断功能：基于智能用户行为识别的动态防护机制，识别并彻底阻断黑客的攻击行为（提供功能截图，加盖公章） |
| 关键字过滤：支持敏感关键字过滤功能，用户可自定义关键字内容（提供功能截图，加盖公章） |
| 配置备案检查功能：检测网站的ICP备案情况，对于通过备案网站优先放行，未通过备案才禁止访问。（提供功能截图，加盖公章） |
| 配置数据库防篡改功能，无需安装任何数据库代理插件。（提供功能截图，加盖公章） |
| 配置网页防篡改功能：支持FTP/SFTP连接方式的网页防篡改（提供功能截图，加盖公章） |
| 自动学习并构建网站的URL模型，禁止违反现有模型的尝试行为 |
| 攻击数据包：提供原始攻击数据包记录和下载导出功能（提供功能截图，加盖公章） |
| 配置防扫描功能：支持对恶意扫描行为开启防扫描功能，用户可自定义防护等级。（提供功能截图，加盖公章） |
| 网站统计功能：能统计每天不同时段后端防护网站各个时段的访问博次数、攻击次数并绘制成图表 |
| URL统计：统计被防护网站的URL每天的总访问次数，最后一次访问IP、访问时间与访问端口。（提供功能截图，加盖公章） |
| 弱密码记录：记录登陆过程中使用的弱密码（提供功能截图，加盖公章） |
| 来源区域访问控制 | 支持针对不同的来源区域，跳转到指定页面。来源区域可以为国家、地区、自定义地址组。（提供功能截图） |
| 支持指定页面的用户自定义。（提供功能截图，加盖公章） |
| 一键断网 | 支持微信一键断网及恢复和网页一键断网（提供功能截图，加盖公章） |
| 重保重防 | 支持重保重防期间设备自动提升网站防护等级（提供功能截图，加盖公章） |
| 交互式统计视图 | 可以生成攻击访问地域视图，可按国家、省份、市交互式呈现。统计客户端访问来自于哪些搜索引擎、搜索词以及访客排行，以便用户更好的了解自己网站的访问信息（提供功能截图，加盖公章） |
| 网站上线发布审核 | 一键禁止未备案或未通过信息化部门审核的Web应用（提供功能截图，加盖公章） |
| 网站统计 | 统计被防护网站每天的总访问量和总攻击数。（提供功能截图，加盖公章） |
| 报表功能 | 安全报表（入侵统计、按入侵类别统计、被攻击主机、攻击来源IP和地理位置、页面访问次数、网络接口流量趋势） |
| 报表中可以统计URL访问的次数，可记录最后访问者的浏览器类型者（提供功能截图，加盖公章） |
| Webshell提示：生成的报表中需提供对防护Web网站中已经存在Webshell文件的告警功能（提供功能截图，加盖公章） |
| 日志功能 | 系统日志、审计日志和安全防护日志（入侵记录、攻击源IP所处地理位置、页面统计、网络流量、防篡改日志、防CC日志） |
| 可基于时间、IP、端口、协议、动作、规则集、规则集类别、危害等级、请求方法等条件进行日志查询。 |
| 支持对外以syslog方式输出入侵记录日志、网站访问日志 |
| 管理功能 | 提供接入即防护的能力 |
| 针对高级用户，对于访问控制、防篡改等功能，支持灵活时间段的计划任务 |
| 支持基于HTTPS的B/S管理 |
| 行业占有率 | 所投产品厂商江苏省内≥10所教育行业案例（其中包含不少于3所211客户案例），提供成功客户名录（含联系人、电话、使用部门）及相关合同复印件证明资料。 |
| 售后服务 | 上述硬件平台、所有软件功能模块提供五年原厂保修和升级服务。 |