**附件：**

Web应用防护系统详细招标参数

WEB应用防护系统技术参数（**★**为必须满足的参数）

|  |  |  |
| --- | --- | --- |
| **指标项** | **指标子项** | **技术要求** |
| 系统架构 | 系统架构 | 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 |
| 软件架构 | 至少提供同品牌windows平台web应用防护软件十套，至少提供同品牌windows平台webshell检测工具一套（提供截图并加盖原厂公章） |
| 硬件架构 | 基本网络接口 | 电口\*6,2对千兆电口Bypass,可扩展千兆电/光口×4 |
| ★性能要求 | ★最大吞吐能力 | ≥2000Mbps-4000Mbps（扩展后） |
| ★最大HTTP吞吐能力 | ≥1000Mbps-2000Mbps（扩展后） |
| ★并发TCP会话数 | ≥120万 |
| ★HTTP请求速率 | ≥ 32000 次/秒 |
| ★网络延迟 | ≤ 0.05毫秒 |
| ★可防护IP数量 | 不限 |
| **部署能力** | **★部署模式** | **★**透明部署（基于透明网桥），需即插即用，无需做任何配置即可防护。支持旁路部署。 |
| **★**策略路由（支持流量牵引） |
| **★**支持反向代理部署 |
| **★**支持透明代理部署 |
| **检测引擎** | 高性能攻击特征检测引擎 |
| **★智能阻断** | 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 |
| **★URL自学习** | **★**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（提供界面截图） |
| **★**支持更新、修正现有URL模型（提供界面截图） |
| **安全特性** | **★IPv6** | ★IPv6协议通过和防护（提供界面截图） |
| **HTTP RFC符合性** | HTTP协议防护 |
| **HTTPS支持** | SSL加密会话分析 |
| **★真实来源IP解析**  （提供界面截图） | 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。 |
| **★内置规则**  （提供界面截图） | 系统提供完善的内置规则 |
| 支持用户自定义防护策略集，针对不同的来源/目的IP，目的URL选择不用的策略集。 |
| 提供高度灵活的自定义规则向导，适用于高级用户 |
| **★WEB应用漏洞扫描** | 能够对SQL注入、CGI、跨站脚本（XSS）进行应用层漏洞扫描 |
| **★碎片组包** | 支持任意碎片组包 |
| 支持超长报文组包（默认30M）（提供界面截图） |
| **编码还原** | ASCII编码的还原 |
| Unicode编码的还原 |
| 各种混淆编码的还原 |
| **★WEB基础架构防护** | **★**蠕虫、缓冲区溢出、CGI信息扫描、目录遍历等WEB通用攻击防护 |
| **★防扫描** | 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。（提供界面截图） |
| **★WEB应用安全防护** | SQL注入及XSS攻击防护 |
| 跨站请求伪造（CSRF）攻击防护 |
| 爬虫防护 |
| 恶意扫描防护 |
| Cookie安全 |
| 服务器信息伪装/过滤 |
| 缓冲区溢出 |
| HTTP请求类型过滤 |
| Webshell行为拦截 |
| **★智能木马检测**  （提供界面截图） | 能够智能识别木马上传行为，支持自定义上传文件的大小、后缀名。 |
| 用户可自定义对上传脚本文件的处理方式：直接拦截，智能识别。 |
| 支持木马上传日志，记录上传时间，源地址，目的地址，目的URL，拦截原因。支持将木马文件直接下载至本地进行人工分析。 |
| **★网页篡改防护** | 自动恢复对文件、目录的篡改 |
| 支持FTP/SFTP连接方式 |
| 支持文件、目录排除 |
| 设置检测优先级 |
| 支持多个防篡改用户 |
| 多操作系统支持：Windows、Linux、Unix、Solaris、AIX等操作系统 |
| 支持基于时间的计划任务 |
| **★数据库防篡改** | **★**支持数据库防篡改，无需安装任何数据库代理插件。（提供界面截图） |
| **★支持虚拟化功能** | 支持对虚拟机中的任意数量网站进行防护，使多个虚拟机共用一个IP地址 |
| **★内容安全** | 恶意代码过滤 |
| **★**支持敏感关键字过滤，用户可自定义关键字内容（提供界面截图） |
| **★弱密码记录** | **★**记录登陆过程中使用的弱密码（提供界面截图） |
| **★备案检查** | ★检测网站的备案情况，对于通过备案网站放行，未通过备案禁止访问（提供界面截图） |
| **★访问控制** | 基于规则的ACL |
| 来源IP的ACL |
| 目的IP的ACL |
| 目的URL的ACL |
| 支持基于时间的计划任务 |
| **主动阻断方式** | 丢弃数据包、阻断TCP连接、禁止恶意IP的后续访问 |
| **★防CC攻击防护**  （提供界面截图） | 来源IP攻击防护 |
| Rerferer攻击防护 |
| 特定URL攻击防护 |
| CC防护的访问控制（黑、白名单） |
| **★抗拒绝服务攻击** | **★**TCP/UDP Flood防护，基于最大上限阀值设置，而非DDOS特征库（提供界面截图） |
| **网络自适应能力** | **★802.1Q支持** | 支持VLAN解码，在Trunk线路上部署并提供防护（提供界面截图） |
| **端口汇聚（Trunk）** | 支持端口汇聚（Trunk），显著提高设备间的吞吐能力（提供界面截图） |
| **路由配置** | 支持静态路由的配置 |
| **统计功能** | **网站统计** | 统计被防护网站每天的总访问量和总攻击数。 |
| **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。 |
| **★网站详情**  （提供界面截图） | 统计每天访问所有站点或某个站点的地域统计，并以地理热点分布图的形式体现。 |
| 统计每天访问所有站点或某个站点的浏览器类型和比例，并以图表方式体现。 |
| 统计每天访问所有站点或某个站点的操作系统类型和比例，并以图表方式体现。 |
| 统计每天访问所有站点或某个站点的来源页面的次数和比例。 |
| 统计每天访问者通过哪些搜索引擎访问到web防护系统后的站点，同时统计搜索引擎的次数和比例。 |
| 统计每天访问者在搜索引擎中通过哪些搜索词访问到web防护系统后的站点，同时统计次数和比例。 |
| 统计每天访问所有站点或某个站点的IP，及其浏览量和比例，以图表方式体现。 |
| 统计每天所有站点或某个站点每分钟的访问次数和攻击次数，以图表方式显示。 |
| **报表功能** | **★报表类型** | 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） |
| **★webshell提示** | 报表提供对防护Web网站中已经存在Webshell文件的告警功能（提供界面截图） |
| **报表查询** | 按事件类型、统计目标或周期类型条件进行统计 |
| **输出格式** | 支持将生成的报表以HTML、Word等通用格式输出 |
| **日志系统** | **日志类型** | 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） |
| **日志查询** | 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。 |
| **日志管理** | 日志导出、清空、自动磁盘日志清理 |
| **系统监控** | **监控类型** | 安全事件监控、访问情况监控、设备负载监控 |
| **系统信息** | 显示网络接口状态，引擎状态、系统CPU、内存及磁盘使用率 |
| **系统诊断和调试功能** | **维护工具** | 抓包工具，可抓取的网络原始报文，用于分析网络状况 |
| **配置备份与导入** | 支持系统配置的备份与导入功能 |
| **高可用性** | **HA双机** | 支持主从部署模式 |
| 支持链路是否正常的监控 |
| 支持本地端口是否正常的监控 |
| 支持双机配置自动同步 |
| **硬件BYPASS** | 内置bypass模块，设备故障直接切换到bypass模式 |
| **资质要求**  **（提供相关资质复印件，生产厂商盖章）** | **★涉密资质** | **★**获得国家保密局涉密信息系统安全保密测评中心颁发的符合国家保密标准BMB13－2004《涉及国家秘密的计算机信息系统入侵检测产品技术要求》的千兆《涉密信息系统产品检测证书》，并出具加盖厂商公章的复印件。 |
| **★**获得国家保密局涉密信息系统安全保密测评中心的《检测报告》，性能测试部分：背景流量达到1000Mbps下的检测报告，并出具加盖厂商公章的复印件。 |
| **★强制认证** | **★**获得中国信息安全认证中心颁发的符合ISCCC-IR-007:2011要求的《IT产品信息安全认证证书》，并出具加盖厂商公章的复印件 |
| **军用认证(优先考虑）** | **★获得中国人民解放军信息安全测评中心颁发的《军用信息安全产品认证证书》，产品为web应用防护系统，认证等级为：军B级，并出具加盖厂商公章的复印件** |
| **★销售许可证** | **★**获得公安部颁发的**web应用防火墙产品（增强级）**的《计算机信息系统安全专用产品销售许可证》，并出具加盖厂商公章的复印件 |
| **★**获得公安部计算机信息系统安全产品质量监督检验中心颁发的**web应用防火墙（增强级）**的检测报告，并出具加盖厂商公章的复印件 |
| **★应急支撑证书** | ★设备生产厂商具备CNCERT颁发《网络安全应急服务支撑单位证书》，并出具加盖厂商公章的复印件 |
| ★设备生产厂商至少为省级互联网应急中心网络安全信息通报成员单位，并出具加盖厂商公章的复印件 |
| **★厂商实力** | ★设备生产厂商应具有符合GB/T 19001-2008/ISO 9001:2008标准的《质量管理体系认证证书》，并出具加盖厂商公章的复印件 |
| ★设备生产厂商应具有漏洞发现能力，具备《中国国家信息安全漏洞库（CNNVD）技术支撑单位资质》，至少曾经获得中国信息安全测评中心颁发《中国国家漏洞库-信息安全漏洞提交证明》，不低于15份，并出具加盖厂商公章的复印件 |
| ★设备生产厂商应为CNVD技术组成员单位，出具CNVD官网截图证明及证书号并加盖厂商公章的复印件 |
| ★设备生产厂商具备中国信息安全测评中心颁发的《国家信息安全测评 信息安全服务资质证书》（安全工程类一级）资质，能力范围包括：安全风险评估、安全需求分析、安全方案设计、安全集成、安全监控和维护等，并出具加盖厂商公章的复印件 |
| ★设备生产厂商至少具有一名由国家计算机网络应急处理协调中心省级分中心或国家中心聘请的公共互联网络安全专家，并出具加盖厂商公章的复印件 |
| **售后服务支持** | **技术支持服务** | ★上述硬件平台、所有软件功能模块提供三年原厂保修和升级服务。  **★**为应对网络安全事件，投标方应成立WEB安全应急处置小组进行紧急响应，响应时间：7×24小时响应。 |