**高性能万兆入侵防御系统招标技术参数**

|  |  |
| --- | --- |
| **指标项** | **技术指标要求** |
| **硬件平台** | 标准2U机架式，冗余电源，1个RJ-45 Console口，2个10/100/1000 Base-T带外管理口，4个网络接口板扩展槽位，实配工作接口≥4个千兆电口，4个千兆光口，4个万兆接口，同时支持带外管理接口；具备≥2个USB接口，用于扩展外置bypass；工作电口均应支持内置硬件bypass，光口支持外接bypass设备 |
| **系统架构** | 系统采用多核硬件平台，提供多核并行操作系统证书，专业入侵防御设备，非防火墙或NGFW下一代防火墙通过功能模块扩展；。 |
| **扩展能力** | 系统支持无线防御扩展能力。 |
| 系统内置IT以上硬盘，用于日志存储和APT防御扩展。 |
| **性能要求** | 在开启IPS的情况下，最大吞吐量≥24Gbps。 |
| 在开启IPS的情况下，最大并发连接数≥500万。 |
| 每秒新建连接数≥20万/S。 |
| **入侵防御功能** | 系统入侵防御事件库事件数量≥5000条，特征库兼容CVE标准，具备兼容性认证证书； |
| 支持入侵防御事件库在线自动升级和手工导入，入侵事件特征库升级频率不少于一周一次；为了保证产品系统及入侵防御特征库的持续稳定更新升级，要求厂商通过CMMI3认证； |
| 系统支持无线攻击检测和防护功能扩展，可手工或自动识别和区分内部AP和外部AP，也可以手工或自动识别合法终端，并基于此设定无线准入策略，通过射频信号阻止非法AP、终端的接入。支持无线扫描、欺骗、DoS、破解等常见无线网络攻击行为的检测、告警、阻断功能，同时支持多种类型流氓AP的检测与阻断（提供相关界面截图）。 |
| 系统内置未知恶意代码检测引擎，能检测流经的http、ftp、邮件协议中包含的office文档、图片文档及压缩文档中的未知恶意文件,报警信息应包括源目的IP、协议类型、文件基本信息、检测方法、危险等级及文件的应用的详细信息（如邮件的发件人、收件人、标题等），方便跟踪恶意文件。 |
|
| 系统应支持单独的恶意样本检测规则升级功能，方便对恶意样本检测功能进行扩充。 |
| 系统应支持恶意样本自学习功能，除通过网络文件捕获外，还支持通过系统直接上传文件，自动识别黑白文件并提供简要信息。 |
| 系统应支持与恶意代码动态检测系统联动。系统将流经的http、ftp、邮件协议中包含的office文档、图片文档及压缩文档提交给APT检测系统，并可查询APT的检测结果。 |
| 系统应支持未知C&C通道（隐蔽通道）检测功能，能够提供C&C通道的危险级别、连接建立时间、连接持续时间、控制端IP地址和端口、受控端IP地址和端口等C&C通道信息。提供各种响应动作：阻断会话、临时阻断和抓包分析等。 |
| 可基于IP地址、网段、时间、VLAN、协议类型等条件设定IPS检测及响应方式。 |
| 支持虚拟IPS功能，不同的用户可以方便定制满足自身要求的检测模版 |
| 系统应具备网络准入控制能力，通过和终端管理系统联动，拒绝不安全主机连入网络。 |
| 系统支持威胁情报，通过通用接口获得第三方的威胁情报，提升防御能力。 |
| 系统支持特殊环境下的攻击源真实地址还原能力。 |
| 系统应具备终端与服务器环境感知能力，通过主动扫描和扫描结果导入获得终端环境情况。通过安全防护情况、漏洞修复情况、可信软件安全情况等确定的安全状态，当不满足安全要求时，可以对连接状态进行阻断，并可以设置终端白名单，能够查询终端安全状态情况（提供相关截图）。 |
| 系统应支持事件响应模版，能够批量修改事件响应动作，包括：事件级别、事件启用开关、动作、日志合并方式、日志开关、抓包取证。 |
| 系统应支持多种事件响应方式，满足客户的安全要求，需包括：重置、临时阻断、丢弃报文、丢弃会话等动作。 |
| 采用先进的模式匹配及协议分析技术实现对网络报文的分析； |
| 具备协议自动识别功能； |
| 支持检测规则自定义功能；自定义参数不低于100种。 |
| 系统应支持常见默认事件集，便于用户使用，默认事件集至少包括：全集、中高级事件、僵尸木马蠕虫事件集、WEB事件。 |
| 事件库应支持CVE和CNNVD兼容能力。 |
| 系统应支持QQ和MSN应用识别功能，支持黑白名单功能，阻止或允许部分帐号登录。 |
| 系统应支持密码穷举探测功能，提供应用的密码穷举行为探测和阻断。 |
| 系统应支持弱口令检测功能，支持网络协议及弱口令检测元素。  |
| 系统应提供SQL注入攻击、XSS攻击的检测和防御功能，对Web服务系统提供保护； |
| 针对SQL注入和XSS攻击，设备应提供在线事件分析功能，提供攻击方法、攻击字段和攻击域、影响的数据库等。 |
| 系统应支持多种防web扫描能力，包括爬虫、CGI和漏洞扫描等，并支持设置至少4个不同级别的扫描容忍度/扫描敏感度（提供相关界面截图）。 |
| **部署方式** | 系统提供旁路部署及在线、旁路混合部署等部署方式。 |
| 系统支持IP地址转换（NAT）功能，包括：源地址转换、目的地址转换、静态地址转换。  |
| 系统支持桥组部署方式，并支持STP协议。 |
| 系统支持路由模式，至少包括：静态路由、策略路由、ISP和OSPF路由协议。 |
| 支持DHCP功能，包括DHCP服务器和DHCP中继功能。并可以作为客户端获得IP地址，满足客户自动化管理的需要。 |
| 系统支持端口聚合/链路捆绑协议，并提供手工方式和LACP两种配置方式。 |
| 系统支持完善的会话管理功能，可实时查看当前会话状态，支持根据源地址、目的地址、端口号或协议类型查询会话； |
| **防病毒功能** | 系统支持通过授权扩展支持对HTTP、FTP、SMTP、POP3、IMAP协议的病毒检测和过滤功能； |
| 系统支持通过授权扩展支持对HTTP、FTP、SMTP、POP3、IMAP协议的文件屏蔽功能，防止文件的下载和传输。 |
| 系统支持VLAN、VoIP数据流病毒过滤； |
| 系统支持双病毒引擎，异构病毒库提高病毒检测查杀能力（提供相关界面截图）。 |
| 系统支持对文件感染型病毒、蠕虫病毒、脚本病毒、宏病毒、木马、恶意软件等过滤，病毒库数量不少于70万。 |
| 系统支持HTTP协议和邮件协议防病毒，通过信息替换功能，用以通知用户病毒被阻断，管理员可以自行设置替换信息； |
| **系统成熟度** | 软件与防御特征库成熟，制造商为入侵防御系统国标起草单位。 |
| **内容防护** | 系统支持Web过滤功能，至少支持黑白名单、关键字过滤、禁止HTTP代理、URL分类过滤外，还支持Script、 Java Applet等过滤，并能通过统一模版设置，系统支持邮件内容过滤功能，有效防止恶意邮件及信息外泄。可根据邮件SMTP命令、发件人、主题、附件、IP及邮件大小进行过滤， |
| 系统支持邮件内容过滤功能，有效防止恶意邮件及信息外泄。可根据邮件SMTP命令、发件人、主题、附件、IP及邮件大小进行过滤， |
| 系统支持敏感信息防护功能，识别信息和文件中的关键字、身份证、手机号码、固定电话号码、银行卡、IP地址等敏感信息，并支持文件指纹识别和白名单功能。（提供相关界面截图） |
| **安全通告** | 入侵防御系统制造商需加入CSA云安全联盟与MAPP计划，及时时获得病毒、木马、钓鱼网站、僵尸网络、系统漏洞等样本信息，提供更及时的安全防护与安全通告服务。（提供相关证明） |
| **高可用性** | 系统支持双机热备和双机主备功能。 |
| 系统支持硬件BYPASS。在设备故障、重启及断电的情况下可保障网络畅通，能够手动配置BYPASS的启停。 |
| 系统支持重点资产和应用监控功能，当资产和应用出现异常时，通过syslog和邮件进行告警，并可以记录日志。 |
| **管理功能** | 系统支持WEB登录图像验证码功能，防止暴力破解。 |
| 系统支持设备集中管理功能，可同时监控IPS的运行状态，并支持对设备进行统一安全策略配置及进行版本升级（提供相关界面截图）。 |
| 系统支持定期修改密码功能。 |
| 支持场景分析功能，提供进行更深入的分析能力，至少包括僵尸木马蠕虫的分布式攻击场景分析。 |
| 系统支持本地日志及SYSLOG日志发送，支持向至少3个syslog服务器发送日志。 |
| 系统支持声音报警，通过设置事件级别、入侵事件级别和病毒事件进行声音报警。 |
| 系统支持报表个性化设置，通过自定义报表生成单位、报表生成人、单位logo和安全摘要信息等信息，快速生成符合单位特点的报告，减少工作量。 |
| 系统提供定期自定发送报表功能，通过邮件将html、doc、xls、CSV和pdf格式报表发送给管理员。 |
| 资质要求 | 计算机信息系统安全专用产品销售许可证（万兆、三级） |
| 涉密信息系统集成资质证书（甲级） |
| IPv6 Phase-2 证书且产品入围Gartner IPS魔力象限 |
| 产品架构成熟、应用广泛，入侵防御产品连续近三年IDC市场排名前三。 |