附件6

配置要求

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **指标项** | **指标要求** | **证明材料要求** |
|  | 硬件要求 | 1U机箱 配置为6个10/100/1000BASE-T接口、2个SFP插槽、2个SFP+插槽；单电源； | 否 |
|  | 性能要求 | 防火墙吞吐率：8Gbps并发连接数：200万 | 否 |
|  | 工作模式 | 支持路由、交换、虚拟线、Listening、混合工作模式；  | 否 |
|  | 路由交换 | 支持根据入接口、源/目的IP地址/地址对象、源/目的端口、协议、用户、应用、选路算法、探测、度量值、权重等多种条件设置策略路由；  | 否 |
|  | IP/MAC绑定 | 支持IPv4/v6双栈IP/MAC静态和动态探测绑定，支持跨三层绑定，支持IP/MAC绑定表导入导出； | 否 |
|  | 链路聚合 | 支持手动和LACP链路聚合，可根据源/目的mac、源/目的IP、源/目的端口、五元组、端口轮询等条件提供不少于10种链路负载算法。**（提供配置界面截图证明，并加盖设备原厂商公章）**； | 是 |
|  | 访问控制 | 支持一体化安全策略配置，通过一条策略实现五元组、源MAC、域名、地理区域、应用、服务、时间、长连接、并发会话、WEB认证、IPS、AV、WAF、URL过滤、邮件安全、数据过滤、文件过滤、审计、APT等功能配置，简化用户管理 | 否 |
|  | 提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析，可在WEB界面显示检测结果；支持策略加速技术； | 否 |
|  | 提供策略命中、冗余、冲突、包含检查及策略查询功能，支持五元组快速查询以及针对策略名、源/目的区域、源/目的地址、服务、对象、未命中时间等条件进行细粒度查询；**（提供配置界面截图证明，并加盖设备原厂商公章）** | 是 |
|  | 应用控制 | 内置P2P应用、加密应用、数据库应用、等应用特征库；  | 否 |
|  | 带宽管理 | 支持链路和四层通道嵌套的流量控制功能，可基于上下行区域、地址、地理对象、用户/用户组、服务/服务组、应用/应用组和时间等配置带宽策略，支持带宽策略优先级和针对IP、应用设置白名单；**（提供配置界面截图证明，并加盖设备原厂商公章）** | 是 |
|  | 连接控制 | 支持对指定的源/目的地址对象、源/目的地理对象、应用制定连接限制策略，可控制所有或单IP会话总数及单IP新建连接数； | 否 |
|  | 文件过滤 | 内置文件过滤引擎，支持HTTP/FTP/SMTP/POP3等标准协议进行检测，识别可执行文件、office文件、视频文件、图片文件、帮助文件、压缩文件、数据文件等超过50种文档类型的文件过滤 | 否 |
|  | 内容过滤 | 内置内容过滤功能，可对FTP上传文件、下载文件、删除文件、重命名文件、创建目录、删除目录、列出目录等信令以及邮件发件人、收件人、主题、内容、附件等进行过滤；  | 否 |
|  | 黑名单 | 支持将五元组、源MAC、地址范围、应用、用户等加入静态黑名单，可与病毒过滤、防代理功能进行联动实现动态黑名单封锁，支持静态和动态黑名单命中统计和监控；**（提供配置界面截图证明，并加盖设备原厂商公章）** | 是 |
|  | 连接控制 | 支持连接控制和监控，可对源/目的地理对象、应用制定连接限制策略，可展示被拦截的IP、地址对象、应用的限制条件、被拒次数、最近被拒时间等信息； | 否 |
|  | 未知威胁 | 内置异常行为检测功能，通过统计智能学习算法，对特定地址对象建立监控策略，基于新建、并发、流量等数据与上一周期记录值进行比较判定是否异常，如果存在异常则报警；**（提供配置界面截图证明，并加盖设备原厂商公章）** | 是 |
|  | DDOS防御 | 支持针对IP、ICMP、TCP、UDP、DNS、HTTP、NTP等协议进行DDOS防护；  | 否 |
|  | 支持基于TCP协议的检测清洗，包括但不限于：TCP Flood、SYN Flood、FIN Flood、RST Flood、新建SESSION Flood、SESSION Flood等；支持SYN源认证技术，认证模式可设置为基本模式或者高级模式，以防止虚假源攻击；**（提供配置界面截图证明，并加盖设备原厂商公章）** | 是 |
|  | 支持基于NTP协议的检测清洗，包括NTP REQUEST FLOOD、NTP REPLY FLOOD等攻击检测，支持基于NTP请求限速、NTP响应限速、源认证、会话认证的防御策略；**（提供配置界面截图证明，并加盖设备原厂商公章）** | 是 |
|  | 支持静态白名单和动态黑名单功能； | 否 |
|  | 审计 | 支持独立审计策略，可对URL地址、网页标题、网页内容、邮件行为、邮件内容、FTP上传/下载行为及文件内容进行审计； | 否 |
|  | 提供完善的审计数据查询功能，可对用户访问网站、邮件收发、论坛微博、FTP、TELNET等上网行为以及用户上网流量时长等内容进行查询；**（提供配置界面截图证明，并加盖设备原厂商公章）** | 是 |
|  | 监控类型 | 支持对设备状态、威胁信息、接口流量、连接信息、应用流量、用户流量、服务器流量、网站类型流量、VPN流量、在线用户等对象进行监控展示； | 否 |
|  | 流量统计 | 支持根据应用对通过设备的数据进行统计，包括应用总流量排名和各个应用的协议名称、总流量、上行流量、下行流量、新建连接数、当前会话数以及流速； | 否 |
|  | 支持根据用户对通过设备的数据报文流量进行统计，包括用户总流量排名和各个用户的用户名、认证类型、上行流量、下行流量、新建会话数、当前会话数以及流速； | 否 |
|  | 支持根据服务器对通过设备的数据报文流量进行统计，包括各个服务器的服务器 IP、上行流量、下行流量、总流量以及新建会话数；**（提供配置界面截图证明，并加盖设备原厂商公章）** | 是 |
|  | 支持指定监控时间周期，包括：实时、最近1小时、最近1天、最近1月等； | 否 |
|  | 配置维护 | 支持多个配置文件并存，配置文件备份能力不少于4个；配置文件支持选择部分配置和全部配置导入导出； | 否 |
|  | 升级维护 | 支持主、备双系统以及多个系统版本文件并存，系统版本数量不少于5个； | 否 |
|  | 产品资质 | 《计算机信息系统安全专用产品销售许可证》**（提供有效证书的复印件，并加盖设备原厂商公章）** | 是 |
|  | 《信息安全产品自主原创证明》**（提供有效证书的复印件，并加盖设备原厂商公章）** | 是 |
|  | 《电信入网许可证》**（提供有效证书的复印件，并加盖设备原厂商公章）** | 是 |
|  | 近三年IDC报告防火墙市场占有率排名前三**（提供有效证明材料的复印件，并加盖设备原厂商公章）** | 是 |