|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| **硬件规格** | 机架式硬件设备，基于高性能硬件平台和专业安全操作系统，多核处理器硬件架构；标配冗余双电源。 |
| 配置≥6个千兆电口（含两对bypass接口），≥4个GE接口，配置≥10个SFP口、6个SFP+口；提供RJ45串口≥1个、1个扩展槽位。 |
| **性能** | 网络吞吐量≥30Gbps，IPv6并发连接数≥1200万，IPS吞吐量≥20Gbps，AV吞吐量≥12Gbps，新建并发连接≥40万/s；IPSec隧道数≥20000个，并发SSL VPN用户≥8个。 |
| **网络适应性** | 支持透明、路由、混合、直连（虚拟线）模式 |
| 支持对3000+ 种应用的识别和控制 |
| 要求支持多系统引导，并可在WEB界面上直接配置启动顺序； |
| 支持静态路由、ISP路由，OSPF、BGP、RIP、ISIS、策略路由，策略路由支持基于应用协议的路由功能，根据应用类型进行路由选择 |
| 支持基于源地址、目的地址、生效时间、应用协议（http、https、mysql、ms-sql、sqlnet、sip等）限制新建连接、并发连接 |
| 支持将任意接口数据完全镜像到设备自身的其他接口用于抓包分析，支持基于源IP、目的IP、源端口、目的端口、网络协议（TCP、UDP、ICMP）等条件对镜像流量进行过滤，并且支持选择入方向、出方向及双向流量镜像。 |
| 支持出站负载均衡功能，能够自动探测多出口，选择最快的出口转发；支持基于多出口的DNS代理功能，可根据配置实现对不同外网线路的DNS服务器地址管理；支持入站SmartDNS,能自动判断访问者的IP地址并解析出对应的IP地址,提升网站访问速度；支持服务器负载均衡功能，提供加权轮询、加权最小连接数、加权散列等多种负载均衡方式；支持web界面实时显示所有服务器的状态和当前连接数 |
| 支持口令认证、短信认证、口令+短信方式的Web认证  |
| **NAT功能** | 支持多对一、多对多的NAT地址转换，且公网地址池可选择逐一使用和同时使用两种模式。 |
| 为解决公网IP地址资源问题，要求必须支持NAT的端口扩展技术，支持NAT full cone模式。 |
| 支持NAT公网地址池中IP有效性检测，避免因NAT地址无法使用导致业务中断。 |
| **攻击防护** | 支持SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood攻击防护，支持IP地址扫描，端口扫描防护，支持欺骗防护功能、支持IP协议异常报文检测和TCP协议异常报文检测。 |
| **入侵防御** | 具备12000种以上攻击特征库规则列表，并可自定义特征库（提供产品界面截图），设备具备CVE漏洞防护能力（提供兼容CVE证书），且厂商具备强大的漏洞和攻防研究能力。 |
| 支持缓冲区溢出、SQL注入和跨站脚本攻击的检测和防护,支持专业的Web Server防护功能，含CC攻击防护和外链防护等 |
| 支持旁路和在线两种模式，支持基于安全策略和安全域启用IPS功能，可在不同的攻击方向上启用IPS（至少支持流入\流出\双向等方向） |
| **病毒过滤** | 支持对HTTP、SMTP、POP3、IMAP4、FTP、SMB协议传输的文件进行病毒扫描，不少于300万病毒特征库，提供产品界面截图 |
| 支持用户手动添加MD5特征码到AV病毒库中，也可以手动清除该特征码 |
| **威胁情报** | 支持与云端威胁情报中心联动，支持热点情报推送到设备，并提供配置向导协助用户生成安全防护策略。 |
| 支持威胁情报与防火墙威胁事件、威胁日志检测结果加强与取证，用户可通过手动触发与自动触发将日志元素上送威胁情报平台进行上下文查询。 |
| **数据安全** | 支持HTTP、FTP、SMTP、POP3、IMAP、SMB等协议设置文件过滤，提供产品界面截图 |
| 支持基于文件类型、文件大小、文件名称进行数据传输安全控制，其中文件类型不少于100种 |
| 支持对网页关键字、Web外发信息、邮件过滤、应用行为控制等内容进行过滤 |
| 支持新浪微博、微信UID和QQ虚拟身份的识别及相关上网行为的审计记录 |
| **IPV6功能** | 支持IPV6邻居发现协议、IPV6 SNMP管理、IPV6路由配置、IPV6 DNS配置、IPV6策略配置、IPV6 ALG配置、IPV6 6TO4隧道配置、IPV6 4to6隧道配置、NAT-PT配置、NAT64和DNS64配置 |
| 支持对IPV6用户的会话日志监控、流量监控、应用监控功能，并且能够对IPV6用户进行自定义监控统计功能 |
| **VPN功能** | 支持标准IPSec VPN(IKEV1/V2)、GRE、L2TP(IPV4/IPV6)、Xauth等VPN连接;支持国密算法SM2/SM3/SM4;支持Android、iOS等移动设备的安全接入。 |
| 提供SSL VPN功能；必须支持对登录SSL VPN的用户端系统进行端点安全检查，至少包括指定文件、指定进程、系统补丁、浏览器版本、杀毒软件等方面，提供产品界面截图有效 |
| **管理功能** | 提供标准的SNMPV1/V2/V3协议管理方式；支持LLDP协议。 |
| 支持预定义和自定义报表模板，可自定义报表内容，报表内容包含网络及安全风险概况、网络流量详情、应用统计及风险详情、URL活动及风险详情、网络风险威胁详情和威胁说明等；报表格式支持PDF、HTML、WORD。 |
| 支持netflow进行流量信息采集和外发。 |
| 支持链路状态监控，可以查看链路的延迟、丢包率、抖动信息，可查看指定应用/应用组详情，支持选择多条链路进行对比分析 |
| 支持数据包路径检测工具通过在线检测、模拟检测等检测手段，WEB界面图形化展现数据包经过的每个防火墙功能模块的处理过程，以便快速定位异常功能模块，提供产品界面截图 |
| WEB界面支持在线抓包工具，可以根据源地址、目的地址、应用、协议、抓包时长等条件在线抓包，提供产品界面截图 |
| **资质要求** | 公安部颁发的《计算机信息系统安全专用产品销售许可证》提供证明文件。 |
| 具备中国网络安全审查技术与认证中心颁发的《网络关键设备和网络安全专用产品安全认证和中国国家信息安全产品认证二合一证书》（万兆），提供证明文件 |
| 具备信息产业部颁发的电信设备进网许可证，提供证明文件 |
| **售后服务** | 提供五年软硬件升级服务及原厂商的售后服务承诺函 |