|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | | **指标项** | **功能描述** |
|  |  | 设备部署 | 与原出口防火墙同一品牌。 |
| ★设备性能要求 | | 专有硬件平台 | 硬件采用MIPS多核处理架构，多核核数≥24个 |
| 接口数量 | 设备高度≤2U，≥4个10/100/1000M自适应电口，≥4个SFP接口，每个接口可划分到不同安全域实现各接口间的安全隔离，独立的HA和管理接口，1个USB接口 |
| 热插拔电源 | 热插拔双冗余电源 |
| 热插拔风扇 | 支持可热插拔风扇，更换风扇不影响设备正常运行 |
| 设备性能 | 最大吞吐量≥32Gbps，IPSEC VPN≥18Gbps,最大并发连接数≥1200万，每秒新建连接 ≥50万，本次招标要求配置20000条IPSEC VPN隧道授权，8个SSL VPN并发授权，SSL VPN最大支持10000个并发用户。（为保证投标产品的真实性，要求提供官网详细参数链接与截图，并加盖原厂商公章） |
| 扩展性要求 | 4个扩展插槽，最大可扩展到40个千兆接口或16个万兆接口 |
| 支持扩展bypass接口，最大可扩展16个bypass接口 |
| 支持扩展POE接口，最大可扩展16个POE接口（要求提供板卡彩页介绍截图） |
| 网络适应性 | | 支持端口镜像 | 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（提供产品功能截图有效） |
| NAT功能 | 支持NAT扩展技术，突破传统单个公网IP地址64512个端口的瓶颈达到更大值（要求提供界面截图） |
| 支持NAT地址可用性探测，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（要求提供界面截图） |
| 路由协议 | 支持静态路由、等价路由、策略路由，以及BGP、RIPv1/v2、OSPF、ISIS等动态IPv4路由协议（非透传），策略路由支持基于指定IP地址、指定应用协议、指定时间表生效 |
| 防火墙 | | 地址簿设置 | 支持基于IP/掩码、地址范围设置地址簿，并支持排除地址设置 |
| web管理界面可显示地址簿成员的关联项，显示在哪些策略、源NAT会话限制、策略路由、QOS流控中被使用（提供产品功能截图有效） |
| ★抗DDoS攻击 | 支持抵御所列所有攻击类型，包括：DNS Query Flood、SYN Flood、UDP Flood、ICMP Flood等，动作支持记录、阻断两种模式（必须具备攻击防护软件自主知识产权证明） |
| ★ARP防护欺骗 | 为了防御ARP攻击和ARP病毒，支持免费 ARP广播及ARP客户端认证，本次招标要求配置10000台客户端授权。提供软、硬件协同防御ARP欺骗的界面截图或技术文档做证明（提供产品功能截图有效） |
| 策略管理 | 支持防火墙策略命中数统计和策略的冗余性检查功能,便于管理员维护防火墙策略（提供产品功能截图有效） |
| 应用协议智能识别 | 支持对3000+种应用的识别和控制（提供应用特征库数量截图有效） |
| 支持应用过滤器便于配置和维护，至少支持6个维度进行过滤，包括：名称、类别、子类、应用技术、风险界别、特性（提供产品功能截图有效） |
| ★负载均衡 | | 链路负载 | 支持SmartDNS功能；注：SMARTDNS功能实现当外部用户访问内部服务器时，联通用户解析到的域名IP为联通地址，电信用户解析到的域名IP为电信地址（提供产品功能截图有效） |
| 支持就近探测算法（根据SYN报文探测的响应时间和PING报文探测的响应时间等方法自动生成静态路由表，并将探测的响应时间生成日志）选择最优路径（要求提供界面截图） |
| 支持基于链路使用率和时延进行链路切换，提升出口的访问效率（提供产品功能截图有效） |
| 服务器负载功能 | 支持服务器的负载均衡，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（提供产品功能截图有效） |
| VPN功能 | | 用户认证 | 支持硬件USB-key的认证方式，支持用户名/密码+数字证书、数字证书等证书认证方式，支持匹配证书的CN、OU等主题名字检查（要求提供界面截图） |
| 客户端检测 | 支持对登录SSL VPN的用户端系统进行端点安全检查，至少包括文件路径、运行进程、安装服务、运行服务、防火墙设置等方面（要求提供界面截图） |
| 隐私数据清除 | 支持断开时自动清除cookie等隐私数据 |
| ★管理功能 | | 系统回滚 | 支持2个系统软件并存，并可在WEB界面上直接配置启动顺序，防止配置不当或系统故障造成的网络中断，充分保证系统的稳定性，支持不少于10个配置文件并存，并支持回滚。（提供产品功能截图有效） |
| 云沙箱平台对接 | 支持云端沙箱技术，可将可疑文件提交云端沙箱进行安全模拟运行，并根据运行结果与防火墙实现联动（提供云沙箱功能对接页面截图有效） |
| 云端SaaS管理平台对接 | 支持通过云端SaaS管理平台为用户提供便捷、高质量以及低成本的增值安全服务，要求通过手机 APP能够实时监控防火墙等设备的状态、网络流量、威胁等信息，及时获得告警，并提供丰富的报表和日志托管能力（提供云端平台网页截图及手机APP截图） |
| 流量包统计 | 支持按64字节、128字节、256字节、512字节等数据包流量统计（要求提供功能截图） |
| ★产品资质要求 | | 销售许可证 | 具备计算机信息系统安全专用产品销售许可证（万兆增强级） |
| CVE认证 | 具有下一代防火墙产品的CVE兼容性证书（非IPS产品） |
| 产品成熟度 | 连续三年入选过Gartner企业防火墙魔力象限，提供证明文件 |
| 信息安全产品认证证书 | 具备《中国国家信息安全产品认证证书》（万兆三级） |
| NSS LAB认证 | 下一代防火墙产品获得NSS LAB推荐级别认证，提供证明文件 |
| 防雷击 | 防雷击浪涌等级三级以上，通过国家无线电监测中心检测中心浪涌（冲击）抗扰度（4KV）测试项目，并出具国家无线电监测中心检测中心委托测试报告 |
| MAPP成员 | 要求加入微软安全响应中心发起的MAPP计划，作为该计划成员，可在微软发布每月安全公告之前获得微软产品的详细漏洞信息，为用户提供更及时的安全防护并提供微软官网截图 |
| 其他要求 | | 中标后测试 | 中标人在中标后7个工作日内需提供样机测试，并进行所承诺的所有功能测试，提供测试报告，如经测试发现与标书要求或投标文件不一致或投标单位有意拖延测试，则视为欺诈行为，招标人将不授予合同，投标单位将承担一切后果与责任 |
| 原厂质保 | 为保证服务质量，要求中标后提供原厂五年质保函。 |