**1.防火墙设备技术要求**

|  |  |
| --- | --- |
| **序号** | **内容** |
| 1 | SSD硬盘≥128GB；内存≥8GB；千兆电口≥8个；万兆光口SFP+≥2个。 |
| 2 | 网络层吞吐量≥10G；应用层吞吐量≥5GB；最大并发数≥200万；配置防病毒安全License≥3年；URL特征库升级服务≥3年；IPS特征库升级服务≥3年；应用识别特征库≥3年。 |
| 3 | 支持实现一对一、多对一、多对多等多种形式的NAT。 |
| 4 | 支持基于对包括但不限于操作系统、网络设备、办公软件、网页服务等保护对象的入侵防御策略，支持基于对漏洞、恶意文件、信息收集类攻击等的攻击分类的防护策略，支持WEB应用防护、僵尸网络及病毒防护，支持基于服务器、客户端的防护策略。 |
| 5 | 提供原厂硬件质保年限≥3年；软件升级服务≥3年；安全防护及基础库更新服务≥3年。 |
|  |  |

**2.VPN设备技术要求**

|  |  |
| --- | --- |
| **序号** | **内容** |
| 1 | SSD硬盘≥128GB；内存≥8GB；千兆网口≥6个；千兆光口SFP≥2个。支持单臂模式、路由模式部署； |
| 2 | 配备并发用户数≥100个（授权买断形式）；设备最大理论加密流量≥300Mbps；https并发连接数≥15000个；https新建连接数≥60个/秒； |
| 3 | 支持在触发异常环境的条件时，用户需完成增强认证才可登录。可配置的异常环境包括但不限于：帐号首次登录、帐号在该终端首次登录、闲置帐号登录、弱密码登录、异常时间登录、非常用地点登录等； |
| 4 | 支持单包授权能力（SPA），提供UDP+TCP组合的单包授权技术，未授权用户无法连接设备，无法扫描到服务端口。 |
| 5 | 加密机支持AES、DES、3DES、RC4、MD5、SHA1、RSA等多种算法。 |
| 6 | 支持国家商密专用的SM1、SM2、SM3、SM4算法。 |
| 7 | 提供原厂硬件质保年限≥3年；软件升级服务≥3年。 |