|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 部署位置 | 数量 | 详细需求 |
| 1 | 防火墙 | 互联网出口边界 | 2 | 1. 性能需求：网络层吞吐量≧16G，应用层吞吐量≧14G，并发连接数≧400万，网络入侵防御吞吐量≧3G，全威胁吞吐量≧2G，防病毒吞吐量≧3G，WEB应用防护吞吐量≧1.5G，IPSEC VPN隧道数≧2000SSL VPN并发用户数≧3000 。 2. 电源需求：冗余电源。 3.物理接口需求：千兆电口≧6个，万兆光口SFP+≧4个   4.售后服务需求：包含3年原厂设备维保服务，配置应用识别、IPS、AV、Web应用防护检测授权以及3年特征库升级服务 5.与现网态势感知系统联动实现风险IP一键封堵 |
| 2 | 防火墙 | 数据中心业务边界 | 2 | 1、性能参数：网络层吞吐量：≧35G，应用层吞吐量：≧20G，防病毒吞吐量：≧3.5G，IPS吞吐量：≧3G，全威胁吞吐量：≧2G，并发连接数：≧800万，HTTP新建连接数：≧18万，SSL VPN推荐用户数：≧35，SSL VPN最大用户数：≧120，SSL VPN最大理论加密流量：≧300M，IPSec VPN 最大接入数：≧4000，IPSec VPN吞吐量：≧1.2G硬件参数：规格：≧1U，内存大小：≧16G，硬盘容量：≧256G SSD，电源：冗余电源，接口：≧16千兆电口+6万兆光口SFP+。  2、网关杀毒升级许可；特征库升级服务；原厂维保服务：3年。 |
| 3 | 防火墙 | 终端接入边界 | 2 | 1.性能需求：网络层吞吐量≧8G，应用层吞吐量≧6G，并发连接数≧220万，网络入侵防御吞吐量≧1.5G，全威胁吞吐量≧1.5G，防病毒吞吐量≧1.5G，WEB应用防护吞吐量≧1G，IPSEC VPN隧道数≧2000 。 2.电源需求：冗余电源。 3.物理接口需求：千兆电口≧6个，万兆光口SFP+≧4个。 4.售后服务需求：包含3年原厂设备维保服务，配置应用识别、IPS、AV、Web应用防护检测授权以及3年特征库升级服务。 5.与现网态势感知系统联动实现风险IP一键封堵 |
| 4 | 内网准入系统 |  | 1 | 医院终端现状：硬件：院内共有终端1000余台：终端操作系统有WindowsXP、Windows7，Windows10，Windows 11等操作系统；  网络环境：医院网络环境采用主干万兆光纤建设，千兆网线到桌面  准入要求：提升终端防病毒能力和访问隔离，阻止病毒蔓延，保障信息安全。  增强内网安全管控，自动识别并阻断违规外网访问，定位和溯源违规行为。  加强终端接入安全，识别并隔离非法终端，确保新入网终端审批和审计合法。  实现终端访问精细化管理，遵循最小化权限和实名制原则，集中化管理权限，限制访问时间和权限，确保可溯源。  进行网络优化，通过QINQ技术实现终端微隔离，简化配置管理，减少维护工作量，核心设备仅需管理二层网络配置。  提高网络运行质量，实现实时监控，快速定位和解决问题，根除传统二层网络问题，提高运维效率，实现即插即用。  提高运维效率，精简配置，统一管理，精准定位故障，快速处理，实现策略自动下发和一键隔离。  实现资产可视化管理，对入网资产进行管控，实时展示资产位置和统计闲置资产，降低损耗。 |