附件：

| **序号** | **设备名称** | **数量（套）** | **实现功能** | **性能要求** |
| --- | --- | --- | --- | --- |
| 1 | 外网防火墙 | 2 | 对内网用户与外网进行数据交互时进行安全防护 | 防火墙吞吐量≥10Gbps ≥6个千兆电口  ≥2个千兆光口  ≥1个扩展槽  防病毒＋IPS功能  三年软硬件维保。 |
| 2 | 外网高级威胁检测 | 1 | 1.对网络中传输的文件进行分离和检测 2.对各种WEB攻击进行检测 3.对邮件社工类攻击进行检测 | 网络吞吐≥5Gbps  ≥4个千兆电口  三年软硬件维保 |
| 3 | 上网行为管理 | 1 | 对接院内上网用户进行行为审计与管理 | 适用带宽≥600M 适用用户数≥1000人 网络吞吐量≥6G ≥6个千兆电接口  ≥6个千兆光接口  三年软硬件维保 |
| 4 | 外网终端安全管理 | 1 | 对外网终端设备进行安全防护 | ≥300个WindowsPC资源授权点数，含杀毒+漏洞管理+资产管理+终端发现+威胁详情服务+虚拟化管理+终端管控+安全检查功能  ≥20个Windows server资源授权点数，含含杀毒+漏洞管理功能  ≥10个Linux服务器资源授权点数，含杀毒功能  三年病毒库升级 |
| 5 | 网闸 | 1 | 对内外网网络进行物理隔离，增强内外网通信安全 | 系统吞吐≥600Mbps 外网接口≥6个千兆电接口  内网接口≥6个千兆电接口  三年软硬件维保 |
| 6 | 数据中心防火墙 | 2 | 对内网访问服务器相关业务进行网络过滤与安全防护 | 防火墙吞吐量≥20Gbps ≥8个千兆电口  ≥2个千兆光口  ≥1个扩展槽  IPS功能  三年软硬件维保 |
| 7 | 数据库审计 | 1 | 对访问数据库的所有操作行为进行审计记录 | 最大日处理≥5000W条SQL明细 入库速度：≥8000(条/秒) 峰值事务处理能力：≥20000(条/秒)  ≥6个千兆电口  三年软硬件维保 |
| 8 | 日志审计 | 1 | 对网络中服务器，交换机安全设备等相关设备日志进行审计收集 | 日志源授权点数：≥150点  ≥6个千兆电口  三年软硬件维保 |
| 9 | 堡垒机 | 1 | 对服务器运维操作进行相关审计 | 资源授权点数：≥150  ≥6个千兆电口  三年软硬件维保 |
| 10 | 态势感知 | 1 | 对医院网络整体状态进行感知与管理，结合威胁情报对内网全流量、日志进行分析告警 | ≥256G内存  ≥960G SSD  ≥SATA存储48T  冗余电源  ≥4个千兆电口  ≥2个万兆光口  三年软硬件维保 |
| 11 | 态势探针 | 1 | 对全网镜像数据进行抓取发送给态势感知进行相关分析 | ≥6个千兆电口  ≥2个千兆光口  全流量吞吐率≥1Gbps  三年软硬件维保 |
| 12 | 终端安全管理 | 1 | 对内外网终端设备进行安全防护 | ≥500个WindowsPC资源授权点数，含杀毒+漏洞管理+资产管理+终端发现+威胁详情服务+虚拟化管理+终端管控+安全检查功能  ≥50个Windows server资源授权点数，含含杀毒+漏洞管理功能  ≥50个Linux服务器资源授权点数，含杀毒功能  三年病毒库升级 |
| 13 | 业务保障运维管理系统 | 1 | 通过业务网络镜像数据分析，智能梳理系统间访问关系、终端与服务的数据交互行为分析，建立终端用户体验感知、业务性能瓶颈发现、故障根因诊断定位，保障业务服务连续性；实现快速发现问题、帮助查明业务系统存在的问题，帮助快速定位问题原因，缩短业务系统故障恢复周期；帮助发现系统瓶颈，提高业务系统响应体验，提升信息系统的使用满意度，提升业务服务连续性和系统的稳定性，极大降低业务系统故障。 | CPU ≥12核心 24线程；内存 ≥32G；容量≥ 1TB;千兆电口≥3，万兆光口口≥2个，三年维保 |
| 14 | 威胁监测与主动响应 | 1 | 1）安全巡检：包括安全设备巡检（防火墙、IPS、杀毒、态势感知 等）、机房巡检（通风、温度、湿度）、应用巡检（数据库日志、中间件日志）。  2）漏洞扫描：包括系统主机、web 应用、网络设备、存疑漏洞进行人工验证等。  3）告警分析：包括主机告警、应用告警、安全设备告警、告警处置记录等。  4）安全规则优化：包括防火墙、态势感知、准入、IPS、杀毒等。  5）基线检查，包括主机系统、中间件、数据库等。  6）弱口令检查，包括 web 应用、中间件、主机。  7）应急响应：包括对突发性事件进行应急响应，防止事件加大一步扩散。 并协助专业应急响应人员，分析事件产生的原因。 | ≥1年/4次上门现场服务  每年至少开展两次网络安全培训；服务周期内，每季度提供一次渗透测试服务；重要时期，提供网络安全驻场保障服务；网络安全检查期间，提供网络安全技术支持。 |
| 15 | 堆叠交换机 | 4 | 数据中心交换机冗余，保障业务稳定性 | ≥24个千兆电口  ≥4个万兆光口  支持堆叠功能  三年软硬件维保 |
| 16 | 机房动力电源整改 | 1 | 保障机房所有设备在市电无法供应时，四个小时内业务不间断。 | 需现场查看 |