附件1

**安全等级保护设备采购需求说明**

1. 基本情况

根据《中华人民共和国计算机信息系统安全保护条例》规定，随着信息技术的快速发展，为维护国家安全和社会稳定，维护信息网络安全，计算机信息系统实行安全等级保护。

为贯彻落实“国家信息安全等级保护制度，遵循相关标准规范，开展信息安全等级保护定级备案、建设整改和等级测评等工作”的方针政策，切实提高我院自身信息安全防护能力，拟按照国家信息安全等级保护制度要求，对我院信息系统安全等级保护建设。

二、安全设备采购清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **基础参数** | **单位** | **数量** |
| **1** | 数据中心边界防火墙 | 交流主机,防火墙吞吐量≥20Gbps，最大并发连接数≥800万，每秒新建连接数≥20万，千兆电口≥12；千兆光口≥8,万兆光口≥4,单台配置IPS、AV、url、云沙箱授权≥3年，硬盘存储≥240GB-SATA | 2 | 台 |
| **2** | 备份一体机 | 备份一体机系统，4U，36盘位；2颗8核CPU处理器；6\*32GB DDR4内存；2\*600GB SAS系统盘，12\*8TB SATA数据盘；2\*GE+2\*10GE光口（含2\*10GE多模光模块）；数据存储管理软件-CDM软件-标准保护功能license授权-后端容量65TB. | 1 | 台 |
| **3** | 入侵检测系统 | 交流主机,IPS检测吞吐量≥8Gbit/s,每秒新建连接数≥25万,最大并发连接数≥1000万,业务口配置 ≥8\*GE COMBO+4\*GE光口+ 4\*GE电口+ 6\*10GE SFP+,单台配置IPS特征库升级≥3年、AV特征库升级≥3年、URL远程查询升级服务≥3年，支持本地硬盘存储日志信息和查看报表，容量不少于240G，配置双电源模块，电源支持热插拔。 | 1 | 台 |
| **4** | 安全运维区防火墙 | 交流主机,防火墙吞吐量≥20Gbps，最大并发连接数≥800万，每秒新建连接数≥20万，千兆电口≥12；千兆光口≥8,万兆光口≥4,单台配置IPS、AV、url、云沙箱授权≥3年，硬盘存储≥240GB-SATA | 2 | 台 |
| **5** | 漏洞扫描系统 | 交流主机，GE电接口≥6，扩展槽≥1个,交流电源，支持Web漏洞扫描、系统漏洞扫描、数据库漏洞扫描、基线安全检查与口令猜解的功能，漏洞库升级服务时间≥3年 | 1 | 台 |
| **6** | 网闸  (需要与现有的网闸[网御SIS-3000-Z4101-HA]做双机运行模式） | 标准2U机箱，标配双电源；配备液晶屏和整机健康监控声光报警装置。整机吞吐：700M。标配设备管理系统；  内网接口：标配1个千兆电接口，1个千兆电管理接口，1个千兆电HA接口。3个千兆电扩展接口，4个千兆SFP扩展插槽。  外网接口：标配1个千兆电网络接口，1个千兆电管理接口，1个千兆电 HA接口。3个千兆电扩展接口，4个千兆SFP扩展插槽。  产品服务：三年硬件保修、5×8技术支持服务。 | 1 | 台 |
| **7** | 防病毒系统 | 1、需同时满足业务网络和办公网络使用；  提供不少于300个用户原厂授权；  防病毒软件具备个人防火墙功能，有效阻止各种恶意威胁；  2、能够实时监控并清除来自各种途径的病毒、木马、蠕虫、恶意软件、勒索软件、黑客工具等；  3、扫描策略必须包含清除、隔离、删除、更名、不子处理以及拒绝访问等处理措施；  4、具备病毒爆发防御功能:当最新病毒爆发时，可在病毒代码未完成之前自动对企业网络中的病毒传播端口、共享等进行关闭，切断病毒传播途径，预防最新病毒的攻击；  5、具备Web信誉评估功能，包含HTTPS通信扫描，结合云安全架构自动识别并屏蔽恶意站点，阻止病毒自动更新；  6、具备外接沙盒设备和威胁发现设备的联动能力，可自动提交可疑恶意文件，并可接收分析结果；  7、必须具备防勒索软件防护功能；  8、支持客户端更新代理，支持将任意客户端设置为更新代理，其他客户端从更新代理更新病毒码、策略，避免影响网络使用；  9、能够有效防御高级持续威胁(APT) 的攻击，通过联动机制禁止客户机对命令与控制服务器的外联；  10、支持拦截恶意URL功能，检测并阻止恶意的URL链接，并支持URL地址黑白名单；  11、支持云安全扫描和传统病毒码扫描两种运行方式；  12、防病毒中央控管系统具备整体防病赤系统的实时集中监控功能，能支持病毒源  头查询机制，通过日志查找病毒源头；  13、防病毒中央控管系统具备整个防病毒系统集中的病毒代码、扫描引擎、防病毒预  防策略、专杀工具升级；  14、防病毒中央控管系统具备整个防病毒系统策略统-配置管理，能根据不同的防病毒需求进行随意分组、并分别制定和实施不同的防病毒策略； | 1 | 项 |
| **8** | 系统集成 |  | 1 | 项 |

1. 存储设备采购清单

我院目前存储设备情况：

（1）SQL数据库服务器2台；FC光纤交换机（华为OceanStor SNS2224）1台；OceanStor 5500 V5存储1台。

（2）Oracle数据库服务器2台；FC光纤交换机（华为OceanStor SNS2624）2台；OceanStor 5210V5存储1台。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **产品名称** | **产品规格** | **数量** | **备注** |
| 1 | 数据库区-FC光纤交换机 | OceanStor SNS3664-64端口(24端口激活,含24\*16Gb多模SFP)-双电源(交流) | 1 |  |
| 2 | 仲裁服务器 | CPU：2\*C4215R(3.2GHz-8Core)，内存：2\*32G，硬盘：2\*600G SAS，1\*RAID卡，网口：4\*GE+2\*10GE(含光模块)，1U滑轨 | 2 | 采用GE仲裁网络 |
| 3 | 5500 V5存储-双活存储(新增) | 双控，384GB缓存，25Gbps，2\*4端口 SmartIO I/O模块(SFP+,16Gb FC),2\*4端口 1Gb ETH I/O模块(RJ45)，硬盘：5\*960G SSD+6\*1.8T SAS+6\*6T NL SAS，1\*4U硬盘框，软件高级包许可(含存储多路径软件、精简配置、双活许可、快照许可等) | 1 | 跟原有5500 V5做双活 |
| 4 | 5210 V5存储-双活存储(新增) | 双控，128GB缓存，25Gbps，8\*1Gb ETH+4\*10Gb ETH(含多模SFP+)+2\*4端口 SmartIO I/O模块(SFP+,16Gb FC)，硬盘：4\*1.92T SSD+9\*1.2T SAS+9\*4T NL SAS，1\*4U硬盘框，软件高级包许可(含存储多路径软件、精简配置、双活许可、快照许可等) | 1 | 跟原有5210 V5做双活 |
| 5 | 5500 V5存储-双活许可 | 双活License许可，2\*4端口 1Gb ETH I/O模块(Base-T) | 1 | 原有存储需要配置双活许可才可以做双活 |
| 6 | 5210 V5存储-双活许可 | 双活License许可 | 1 |
| 7 | 服务 | 存储容灾规划设计与实施服务 | 1 |  |
| 数据备份服务 | 1 |  |

1. 其他要求

（1）对于增购、扩容的设备必须为全新原厂原装产品，并能兼容于现有设备；需能完成安装调试并正常使用。

（2）对于增购、扩容设备需与现有的服务器应用计算资源池融合，保障不影响现有业务系统运行，达到实现扩容效果。