

第五章 采购需求

一、项目内容

序号	产品名称	单位	数量	控制单价(万元)	备注
1	超融合一体机集群（核心产品）	套	1	91.1	质保≥3 年
2	零信任安全网关（国密）	套	1	27.9	质保≥3 年

二、技术要求

1. 超融合一体机集群（核心产品）

指标项	指标要求
总体要求	1. 要求所投超融合产品的计算虚拟化软件、存储虚拟化软件、网络虚拟化软件为同一品牌且完全自主研发，需要提供产品软件著作权。
	2. 采用裸金属架构，无需绑定操作系统即可搭建超融合平台。
	#3. 为保证本次采购超融合设备能够扩容进我院现有超融合集群，本次采购超融合系统需能够跟我院现有超融合管理平台（深信服云计算管理平台 V6.0 ）纳入统一集群管理，需提供可统一管理说明函。
节点配置	1. 项目配置 5 个节点，每个节点配置≥2 颗 CPU，单颗处理器主频≥2.9GHz，核数≥16 核，配置≥32*32G DDR4 内存；配置≥2*240G SSD 系统盘；配置≥2*3.84T SATA SSD 缓存盘，配置≥4 块 16T SATA，配置≥4 个千兆电口，配置≥4 个万兆光口（满配模块），盘位数≥12，配置冗余电源。
	2. 提供配套存储交换机 2 台，交换机万兆光口≥12，千兆电口≥12（满配模块）
	3. 软硬件均支持 ECC 告警。支持提前发现内存 CE 故障，并且实现 100%异常自动隔离。支持内存 UE 故障检测告警，并在用户界面显示告警信息。
计算虚拟化软件	1. 配置并激活计算虚拟化软件，每个节点配置 2 颗 CPU 计算虚拟化软件授权。
	2. 考虑医院实际运维需求，要求当虚拟机卡死或蓝屏时虚拟机需具备自动检测功能并实现自动重启，无需人工干预，减少运维工作量。
	3. 为保证业务运行可靠性，要求支持 IO 重试，当存储出现故障，导致虚拟机无法读取存储数据时，自动挂起虚拟机，避免业务故障。
	4. 为保障业务系统可靠性，平台需定期升级保障平台稳定性，超融合平台需支持在线升级不影响业务；为保证升级时间与步骤可控，

	升级过程中支持对升级节点进行升级顺序编排、升级暂停。 #5. 提供基于 PowerShell 的 CLI 命令行功能，通过命令行可以进行管理计算虚拟化、存储虚拟化、网络虚拟化模块，并通过 PowerShell 脚本可简化用户运维操作。支持漏洞及版本信息巡检，推送补丁及升级信息，并支持补丁管理、更新、回滚。（提供产品相关证明材料） 6. 虚拟化管理平台具备监控功能，对资源池中 CPU、网络、磁盘使用率等指标进行实时的数据统计，当指标超过设置的阈值，可以通过多种方式（短信、邮箱）告知管理员进行排障。 #7. 支持平台中的集群资源环境一键检测，对硬件健康、平台底层的虚拟化的运行状态和配置，进行多个维度进行检查，提供快速定位问题功能，确保系统最佳状态。（提供产品相关证明材料） 8. 虚拟机资源告警项支持虚拟机 CPU 利用率、内存利用率，虚拟机单网口链接 session 数过高、虚拟机过期时间，并检测异常状态持续时间，支持检测虚拟机镜像文件损坏，备份失败，虚拟机与外部网络不通的监控告警，用户可自定义告警项并支持通过邮件和短信进行告警。
存储虚拟化软件	1. 配置并激活存储虚拟化软件，每个节点配置 2 颗 CPU 存储虚拟化软件授权； #2. 为保证亚健康硬盘的数据安全，支持主动将亚健康硬盘数据进行迁移修复，当硬盘的坏道数过多，系统能够自动将该盘的数据迁移至其他健康硬盘上。（提供产品相关证明材料） 3. 支持磁盘坏道检测功能，虚拟存储集群可以对数据盘进行坏道检测，发现坏道后可自动从另外一个副本读取数据，并对坏道数据进行修复。 4. 支持数据自动重建机制，当主机或者磁盘故障后，自动利用集群内空闲磁盘空间，将故障数据重新恢复，且重建速度最快可达 30min/TB 以上，快速恢复副本的完整性和冗余度，确保用户数据的可靠性和安全性。 5. 支持数据重建智能保护业务性能，可以对数据重建速度进行智能限速，避免数据重建过程中 IO 性能占用导致对业务的性能造成影响。 6. 支持存储分卷功能，以物理主机为单位划分为不同的存储卷，如高性能卷，大容量卷，全闪存卷等，可使对存储性能和容量要求不同的业务运行在不同的存储卷上。 #7. 支持数据重建优先级调整，可以查看数据重建任务列表信息，包括对象名称、对象类型、数据量和优先级等信息，可以点击操作中的优先级对数据重建进行优先重建，保证重要的业务优先恢复数据的安全性。（提供产品相关证明材料）
网络虚拟化软件	1. 配置并激活网络虚拟化软件，软件按照物理 CPU 数量方式进行授权，每个节点配置 2 颗 CPU 网络虚拟化软件授权； 2. 支持对 oracle、sqlserver、Weblogic 数据库及中间件监控，实现对数据库的语句的故障定位排错，执行时延分析。

	3. 支持部署虚拟分布式交换机、虚拟路由器、分布式防火墙。
	4. 在管理平台上可以通过拖拽虚拟设备图标和连线就能完成网络拓扑的构建，快速的实现整个业务逻辑，并且可以连接、开启、关闭虚拟网络设备，支持对整个平台虚拟设备实现统一的管理，提升运维管理的工作效率。
	5. 分布式防火墙基于监测虚机 IP 地址和端口进行东西向流量隔离控制，并提供实时拦截日志，以及支持“数据直通 ByPass”功能，方便出现问题快速定位问题。
	6. 主动探测业务系统，实时监控业务可用性，监控策略包括 HTTP、FTP、POP3、SMTP、自定义端口协议等，当业务出现故障时，通过多种方式（短信、邮箱）告知管理员进行排障。
产品资质和服务要求	#为保障产品的可靠性和生产商的技术开发能力，要求产品厂商提供《CCRC 信息安全服务-软件开发服务资质》一级及以上证书，提供证明材料并加盖公章。

2. 零信任网关（国密）

指标项	指标要求
基本要求	标准 1U 机架式设备，实配千兆电口 ≥ 6 个，千兆 SFP 接口 ≥ 4 个。最大加密流量 ≥ 480 Mbps，最大并发用户数 ≥ 1000 个，最大 https 并发连接数 ≥ 48000 个，最大 https 新建连接数 ≥ 192 个/秒；IPSEC 性能参数：加密最大流量 ≥ 165 Mbps，并发隧道数 ≥ 600 Tunnel，配置不少于 500 点并发授权。
兼容性要求	#本次提供设备需与我院现有零信任平台（深信服 SDP 安全网关软件 V2.0）可组集群，需提供说明函。
密码设定要求	#支持密码复杂度配置，支持设定密码不能包含用户名，支持设定密码不能与历史的密码相同，支持设定密码不能包含键盘连续排序。（提供产品相关证明材料）
CDN 加速	支持配置 CDN 下载加速功能，支持客户端的下载地址配置为企业的 CDN。
私有 DNS	支持私有 DNS 解析功能，支持在不额外购买 DNS 的情况下在内网使用域名访问内网资源。
资源授权	支持批量资源授权功能，支持将单个或多个应用授权给用户的组织架构、用户角色或最终用户。
增强认证	#支持增强认证，支持在账号首次登录、新终端登录、新地点登录、异常时间登陆情境下进行增强认证。（提供产品相关证明材料）
TCP 优化	支持对 TCP 协议的优化，支持在网络环境不佳的情况下业务的快速访问。
单包授权	支持 SPA 单包授权功能，支持 UDP+TCP 组合的单包授权技术，支持未授权客户无法扫描到服务端口场景实现。
一人一码	支持一人一码功能，支持绑定登陆用户和 SPA 安全码，支持在用户与 SPA 安全不一致时产生安全告警。
安全开发能力	#为保障产品的可靠性和生产商的技术开发能力，要求产品厂商提供《CCRC 信息安全服务-软件开发服务资质》一级及以上证书，

	提供证明材料。
--	---------

三、服务标准要求

1. 配置管理

投标人需要在质保期内提供配置技术支持服务，在质保期内，有任何需求需要调整网络设备配置的，都需要及时安排人到现场进行技术支持。

2. 数据保密

投标人在履行服务中须对采购人的数据保密，不向任何第三方泄露、公布、扩散，如服务所必须则仅在项目人员内部使用，不得任意传播流通，数据内容包括但不限于信息系统架构、硬件及网络信息、业务信息及数据、电子及纸质资料等任何技术和非技术的信息，以及与现有、未来和预计的产品和服务相关的任何方案，保密期限为永久保密。

3. 网络安全

质保期内，投标人在重大活动开始前 3 天需要完成网络整体检查和骨干节点网络设备现场巡检工作，备份设备配置等工作。

4. 故障处理

投标人应确保所提供成果和技术服务的稳健性，投标人在提供技术服务过程中，应承担因其过失、疏忽或技术服务工作成果缺陷，而引发的信息系统故障或业务数据损失的责任，并按采购人要求积极负责排查故障原因，彻底解决故障问题。

四、项目管理要求

1、投标人需根据项目的采购、建设的要求，采用成熟的软硬件产品进行投标。产品必须满足本次项目的采购、建设的主要要求，并保证能对选用产品进行很好的集成。

2、投标人在中标并签署合同后，应完成采购文件中所规定的各项任务，包括：提供完善的系统建设方案、系统的安装调试、进行用户培训，并完成验收前期的各项准备工作。

3、投标人应向采购人提供产品或服务，承担方案中所有的集成责任。承诺与本项目的相关单位进行积极主动的合作。投标人必须服从采购人的统一协调，在系统方案设计、实施方案设计、设备供货、系统集成、技术支持、运行维护等

方面相互配合。

4、投标人在投标文件中需提供本项目的具体组织实施方案。方案中包括但不限于以下内容：需求分析，进度计划，保障措施，运输，安装，验收程序等。

（1）需求分析：根据采购人实际情况，深入理解项目建设要求。对现有的网络安全情况进行全面分析。

（2）实施计划：根据实施周期的要求，描绘项目目标、范围，合理安排实施人员，编制进度计划，投标人应对项目实施各阶段进行合理划分，并明确各阶段应完成的工作和提交的产品及文档，采购人将对项目实施进度进行评价。

（3）项目管理：提供采购人对项目管理的理解，内容包含进度管理、质量保证、文档要求、沟通管理、以及风险控制等内容。

（4）项目进度要求：90 个日历日内完成设备的供货、上架、安装、调试等工作。

5、项目服务团队：投标人应为本项目配备专门的服务团队，至少包括 1 名项目经理且具有信息系统项目管理师资质证书，1 名项目核心人员具有系统架构设计师资质证书，项目实施人员至少 3 名，实施人员中需具有 CISP 资质证书，网络工程师（中级）资质证书。团队人员项目期间不得随意更换，确因离职等原因，需要更换项目经理，应报送项目招标方同意备案后方可执行。

五、售后服务要求

1、设备 3 年免费维保内，投标人每月度为采购人提供设备巡检服务，并提供智能信息化运维管理系统用于记录巡检服务工作内容，以便采购人清晰了解巡检服务绩效；

2、设备 3 年免费维保内，投标人每季度为采购人提供设备安全加固服务，并提供智能信息化运维管理系统用于记录安全加固工作内容，以便采购人清晰了解安全加固服务绩效；

3、硬件若任何因安装工艺、材料和产品部件、质量造成的设备或部件损坏，进行无偿更换和维修；若经修缮后仍存在质量问题，则该项保修期应予顺延。保修期内发生故障的设备如无法在 24 小时内修复，应提供备用设备以保证系统的连续稳定运行，并在 5 个工作日内修复故障设备或更换新设备，5 个工作日内不能解决的，由投标人提供替代设备保障系统正常运行，在无相同型号的同种设备

时，应当更换同类设备中较高型号的产品。

六、 服务承诺

投标人应在投标文件中将服务承诺单列一章，服务承诺应包括对服务内容的响应程度，如服务的频次、提供服务人员的能力与经验情况、敏感时期的保障措施、投标人可免费提供的其他特色服务等。

★1、投标人应保证项目建设期间系统稳定运行。为保证本项目实施有序进行，若投标人取得中标资格，应自行完成所有协调第三方软件系统开发公司协助进行防火墙切换的工作，以满足本项目实施需要，所产生的费用均包含在投标总价中，采购人不再支付任何费用。

★2、若投标人取得中标资格应制定符合网络安全等级保护第三级相关要求的项目实施方案，并根据采购人现有网络安全设施进行兼容集成，采购人有权组织网络安全专家对投标人制定的项目实施方案进行论证，直到投标人提交的项目实施方案符合网络安全等级保护第三级相关要求为止，由此所产生的费用均包含在投标总价中，采购人不再为此支付任何费用。

注：投标人应提供加盖单位公章的承诺书签原件，否则其投标将作为无效投标被否决。

七、其他服务要求

1. 对于技术规格中标注“#”“★”号的技术参数，投标人须在投标文件中按照招标文件技术规格的要求提供技术应答的证明材料，并加盖投标人公章。其中技术支持资料指包含但不限于产品功能截图、白皮书、检测报告、资质等相关证明材料。”

如投标人技术响应与技术支持资料（或证明材料）不一致，将以技术支持资料（或证明材料）为准。对于投标人提供的投标文件技术应答未按本条款要求提供投标产品技术支持资料（或证明材料）的，评标委员会可能会认为该技术应答不符合招标文件要求。由此产生的评标风险，由投标人承担。

2. 投标人需为本项目成立独立于其它项目的专门工作组，项目实施计划需详细的描述项目的进程，并明确了资源配置和项目各阶段应该完成的内容。

3. 投标人在中标后，实施过程中应具备完善的实施方案与应急处理方案，避免因项目实施所造成的业务中断。

4. 投标人有责任提供包括设备安装手册、用户使用手册、设备维护手册、技术白皮书、技术授权书、软件系统用户使用手册等在内的完备准确的技术资料。

5. 在设备安装和系统实施期间，由投标人和医院的技术人员共同组成项目实施小组，负责项目实施。

6. 在设备投入使用后，质保期内如采购人需要进行设备升级和扩容，投标人有义务协助采购人完成相关工作，并向医院提供必要的技术支持。

7. 投标人必须向招标方承诺技术二线支持，为网络、安全系统中主要设备、软件和系统的功能扩充提供技术支持。

8. 投标人和设备原厂商必须保证其在国内的售后服务与技术支持工作。所有以上承诺的服务要求在医院提出后，应急响应服务应满足 3 分钟快速响应，60 分钟到达用户现场的要求。

9. 为保证投标人熟悉和了解采购人的网络环境及物理环境，从而确保方案设计的合理性和可行性，保证项目的顺利实施，投标人须在投标前需自行联系采购方进行现场勘查。