一、项目概述

1、项目名称：系统冗余架构加固项目

2、交付日期：合同签订后45天内

3、付款方式：交货验收合格并安装调试后，招标方根据医院付款流程，支付合同款项100%。

4、交付地点：招标人指定地点

5、项目建设需求

通过多年的信息化建设，医院已建成较为完善的信息系统软硬件平台，但由于病毒攻击、恶意攻击泛滥，应用软件漏洞层出不穷，使得医院的信息系统在安全防护方面仍面临较大的压力和挑战，存在较大的安全风险和安全漏洞。对于已经拥有较高信息化水平的医院来说，信息系统的安全性，信息系统的冗余性，网络架构的冗余性，网络环境的稳定性是保证业务顺利运行的关键。

随着IT信息化的更新与发展，为确保我院核心业务系统和应用、数据的安全，需要对医院外网区域、DMZ区域、外联区域进行安全加固，构建有效的网络安全管理架构，落实安全防护措施，在安全事故发生之前就进行预防和治理，从而减少和杜绝来自外部网络的安全威胁，真正有效、便捷地保障医院信息网络的安全可靠性。

同时10F华为的模块化机柜空间容量不足，需要扩容。

二、采购清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 采购内容 | 数量 | 单位 | 原厂免费质保 | 核心产品 |
| 1 | 上网行为管理 | 1 | 台 | ≥三年 | 否 |
| 2 | 网闸 | 2 | 台 | ≥三年 | 是 |
| 3 | 下一代防火墙 | 2 | 台 | ≥三年 | 是 |
| 4 | 日志审计 | 1 | 台 | ≥三年 | 否 |
| 5 | 堡垒机 | 1 | 台 | ≥三年 | 否 |
| 6 | 综合柜 | 1 | 台 | ≥三年 | 否 |
| 7 | 机柜 | 3 | 台 | ≥三年 | 否 |

三、技术要求

（一）上网行为管理

|  |  |
| --- | --- |
| 项目 | 功能要求说明 |
| 产品规格 | 产品不少于6个以太网电口，2个SFP+口，支持冗余电源，内存容量≥8G，硬盘容量≥128G SSD+960G SSDG，2U机箱。 |
| 网络层吞吐量≥12 Gbps，应用层吞吐量≥2.7 Gbps，带宽性能≥1.5 Gbps，支持用户数≥10000，每秒新建连接数≥2万,最大并发连接数≥80万。 |
| 部署方式 | 必须支持两台及两台以上设备同时做主机的部署模式； |
| VPN组网 | 支持IPSec VPN模块，支持与LDAP服务器、Radius服务器、硬件特征码绑定认证； |
| IPsec VPN支持多线路功能，通过配置主备线路组和流量分配模式的多线路选路策略。 |
| DNS代理 | 支持DNS代理，能够基于用户、域名、目标DNS，指定代理策略生效，代理策略可以设置为：重定向至DNS服务器、解析为IP、丢弃、重定向至指定线路； |
| 实时监控 | ▲支持首页分析显示接入用户人数、终端类型；带宽质量分析、实时流量排名；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行；（提供产品界面截图） |
| 排障工具 | 支持PPS异常、丢包异常、ARP异常、内网DOS攻击等异常情况实时监测，显示每日异常事件个数及情况； |
| 针对内网用户的web访问质量进行检测，对整体网络提供清晰的整体网络质量评级；（提供产品界面截图） |
| 用户管理 | ▲支持针对特权用户配置免认证key、免审计key、免控制key；（提供产品界面截图） |
| 第三方用户源 | 支持LDAP、Radius、POP3等第三方认证；支持ISA\lotus ldap\novell ldap\oracle、sql server、db2、mysql等数据库等第三方认证； |
| 指定用户必须用AD域账户登录操作系统，否则禁止上网； |
| 认证方式 | 支持终端用户账号绑定手机号码和微信号，绑定后可以通过手机验证码和微信扫码实现上网快捷登录认证。 |
| 支持通过OAuth认证协议对接，支持阿里钉钉，口袋助理，企业微信第三方账号授权认证； |
| 支持提供二维码和会议号，用户扫码或输入会议号认证上网；支持通过验证手机号码实名认证； |
| 终端资产管理 | 支持图形化查看当前内网IP使用情况，帮助管理员减少人工维护IP表的工作量； |
| 自动发现网络里面的终端，并获取IP、Mac、厂商、操作系统等信息，设备必须支持PC、移动设备、哑终端、专用设备的发现和型号识别：至少支持Windows、Linux、MAC、瘦客户机等PC；至少支持手机、平板等移动设备；至少支持服务器、交换机、无线控制器等网络设备；至少支持打印机、投影仪、电视、摄像头、门禁系统等哑终端；支持自定义终端类型（提供产品界面截图） |
| 对网络接入的终端进行可视化管理，展示终端详细信息、合规状态等，支持查看终端类型，以及终端详细信息（厂商，系统，端口等）； |
| 代理管理 | 支持代理控制功能，不允许使用外部HTTP代理，不允许使用外部Sock4/5代理，不允许在HTTP，SSL一些的标准端口上使用其他协议；（比如在80端口上传输非HTTP协议数据，在443端口上传输非HTTPS协议数据等） |
| 用户配额管理 | 基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中；用户指定应用上网流速超过预设阈值后，网关自动提醒该用户； |
| 网盘审计 | 支持网盘和笔记类应用访问内容和外发文件审计； |
| 上网行为日志 | 支持查询和导出基于指定时间段、用户和用户组的文件审计、邮件收发、访问网站、发帖/微博、搜索关键字等详细用户行为的报表； |
| 支持基于时间段、用户、用户组、终端类型和位置等维度的多种上网行为统计排行报表； |
| 日志管理 | 设备必须支持内置日志中心和独立日志中心；支持分级配置管理员日志查看权限，管理员登录日志中心只能查看指定用户组的上网行为日志； |
| 必须支持以USB-Key方式验证接入日志中心的管理员身份； |

（二）网闸

|  |  |
| --- | --- |
| 指标项 | 功能描述 |
| 产品架构 | 采用2+1模式，即系统由A网主机模块、B网主机模块和交换模块组成； |
| 设备性能 | 应用层吞吐≥700Mbps ，应用层并发连接≥10万条，视频并发数≥350路（2M码流） |
| 网络接口 | 内网接口至少满足：6个10/100/1000Base-T端口，4个SFP插槽,1个Console口，2个USB口；支持1个扩展槽位； |
| 外网接口至少满足：6个10/100/1000Base-T端口，4个SFP插槽,1个Console口，2个USB口；支持1个扩展槽位; |
| 硬件规格 | 2U机箱，冗余电源；支持液晶面板 |
| 适配平台 | 支持信创CPU芯片和操作系统； |
| 文件交换 | 支持FTP、SFTP、SMB、NFS等协议，同时可设置服务器加密方式，服务器编码方式等 |
| 灵活设置文件传输方向，同时工作模式支持源端移动、源端删除、增量更新、完全复制、延迟删除等多种模式 |
| 支持多种同步模式： 源端移动、源端删除、源端保留等模式； |
| 具备文件断点续传，同时支持文件并发数量设置，大幅度提升文件传输性能，充分利用硬件资源（提供产品功能截图证明） |
| 文件传输具备文件名过滤、文件类型过滤、文件内容过滤、文档重建、病毒过滤（提供产品功能截图证明） |
| 支持文件重构技术，可自动剔除文件中夹带的危险程序，可执行代码等 |
| 文件交换支持传送优先级，可根据文件大小、新旧、文件名、后缀、缓时传输等多种方式进行优先级排序传输(提供产品功能截图证明) |
| 数据库同步 | 至少支持Oracle、SQL Server、人大金仓、达梦等主流数据库同步； |
| 支持无客户端方式同步，无客户端方式同步由网闸主动发起并完成，不需要第三方软件支持（无需在数据库安全任何第三方软件，可以在网闸系统上完成数据库同步配置） |
| 支持一对一、一对多、多对一数据库同步，支持设定同步时间和同步周期； |
| 支持两台单向设备实现数据库的双向同步； |
| 支持数据库同步进度监控，支持数据库连接状态检测；（提供产品功能截图） |
| 数据库访问 | 支持对附件及其附件类型进行过滤控制，邮件内容过滤、文档重建、病毒过滤 |
| 至少支持MySQL、ORACLE、SQLServer、DB2、SYBASE、POSTGRESQL、达梦、神通、人大金仓等数据库的访问 |
| 支持数据库访问用户名过滤、数据库名、表控制等策略 |
| 视频模块 | 支持工业SCADA网络OPC协议、MODBUS协议、IEC104协议等 |
| 邮件访问 | 支持同步冲突策略，可自定义覆盖、丢弃冲突策略 |
| 支持SMTP、POP3、IMAP通用协议 |
| 安全浏览 | 支持FTP用户在线情况查看，包含但不限于用户地址、登陆日期、登陆时间等信息 |
| 安全FTP | 数据库库名控制、数据库表控制，可以根据用户与数据库表对应关系，进行相应数据库操作过滤，支持最大并发连接数、单个IP最大并发数设置，灵活限制数据通道是否在1024以下端口使用，支持病毒扫描文件大小限制、文件类型大小限制、关键字过滤文件大小限制 |
| 定制模块 | 支持模块定制 |
| 工控访问 | 支持双引擎病毒模块，可根据用户需求选择需要的病毒引擎； |
| 支持抗Dos攻击功能设置； |
| 安全管理 | 支持内、外网分别具有独立的管理接口，而不是通过内/外网一个管理接口完成全部管理； |
| 支持基于https的图形化安全管理；支持用户名/密码+U-KEY、用户名/密码+数字证书等双因子认证方式； |
| 支持带内管理，可通过业务口进行管理工作；用户可自行选择是否启用带内管理功能；（提供产品功能截图） |
| 支持跨网段管理，实现管理终端IP地址和端口的访问控制；管理员及审计员区分并独立，支持分权管理；具有独立审计用户，提供完善的日志审计功能 |
| 运维管理 | 支持设备运行状态检测、系统资源监控；支持通过界面能够查看到多核CPU使用率，进行设备的远程关闭及重启功能； |
| 支持提供调制工具，至少包括trace、ping、telnet、arp |
| 集中监控 | 支持集中监管平台，可对多台网闸进行统一监控，记录每台设备的系统资源运行情况； |

（三）下一代防火墙

|  |  |
| --- | --- |
| 指标项 | 功能描述 |
| 硬件规格要求 | 千兆电口≥16个，万兆光口≥6个，内存≥16G，硬盘容量≥256G SSD， |
| 产品性能要求 | 网络层吞吐量≥40G，应用层吞吐量≥25G，全威胁吞吐量≥2G，并发连接数≥420万，HTTP新建连接数≥19万。 |
| 工作模式 | 产品至少支持路由模式、透明模式、虚拟网线模式、旁路镜像模式部署方式。 |
| 路由特性 | 产品支持静态路由、策略路由和多播路由协议，并支持BGP、RIP、OSPF等动态路由协议。 |
| NAT功能 | 产品支持支持源地址转换SNAT，目的地址转换DNAT和双向NAT等功能， 支持一对一、一对多、多对一等形式的NAT。 |
| 产品支持各种应用协议的NAT 穿越，实现SQLNET、TFTP、RTSP、PPTP、FTP、H.323、SIP等多种NAT ALG功能。 |
| 访问控制 | 产品支持多维度安全策略设置，可基于时间、用户、应用、IP、域名等内容进行安全策略设置。 |
| 应用控制 | 产品支持对不少于9000种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。 |
| DDoS防护 | 产品支持对ICMP、UDP、DNS、SYN等协议进行DDOS防护。 |
| 防病毒 | 产品支持对SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP等协议进行病毒防御。 |
| 产品支持对多重压缩文件的病毒检测能力，支持不小于12层压缩文件病毒检测与处置。 |
| 产品支持勒索病毒检测与防御功能（需提供产品功能截图证明） |
| 入侵防御 | 产品支持对不少于9000种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。 |
| 产品支持僵尸主机检测功能，产品预定义特征库超过110万种，可识别主机的异常外联行为。 |
| 账号安全 | 产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生。 |
| 蜜罐联动 | 产品支持主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客指纹信息，并自动封锁高危IP。 |
| 策略生命周期管理 | 产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。 |
| 双机部署 | 产品支持主主、主备两种双机模式部署。 |
| 管理方式 | 产品至少支持Web管理、串口管理、SSH管理方式。 |
| 管理员账号权限管控 | 产品支持三权分立功能，根据管理员权限分为安全管理员、审计员、系统管理员三种角色。 |
| 双因素认证 | 产品支持管理员双因素认证功能，用户通过用户名、密码和Key等不同方式登陆产品管理界面。 |
| 产品资质 | 要求所投产品具备国家信息安全漏洞库兼容性资质证书，提供有效证书复印件。 |

（四）日志审计

|  |  |
| --- | --- |
| 指标项 | 功能描述 |
| 性能参数 | 事件处理性能最高不低于10000EPS |
| 日志授权 | 至少包含100个日志授权； |
| 网络接口 | 4个千兆电口，1块RAID卡，2个扩展插槽 |
| 硬件规格 | 产品应为标准机架式设备，标准2U机箱，冗余电源； |
| 适配平台 | 支持信创CPU芯片和操作系统； |
| 审计对象 | 支持审计网络设备、安全设备、主机操作系统、数据库、中间件、应用系统的配置日志、运行日志、告警日志等； |
| 日志采集 | ▲支持通过Syslog、Syslog-NG、SNMP Trap、Netflow V5、JDBC、Agent代理、WMI、(S)FTP、NetBIOS、文件\文件夹读取、Kafka等方式完成各种日志的收集； (提供产品功能截图) |
| 与转发 | 支持按照Syslog-NG标准及自有格式进行转发，转发时包含原始日志源IP地址； |
| 资产管理 | 支持资产按多种维度进行分组、分域管理； |
| 支持对资产日志进行过滤，设置允许接收和拒绝接收日志，可对资产设置一定时间内未收到事件后主动告警。 |
| 支持自定义资产类型及资产属性；支持对资产自定义标签，对标签内容进行查询和管理； |
| 日志归一化 | 系统提供页面可视化编辑归一化策略，对页面查看的日志编辑归一化策略； |
| 支持对日志进行归一化处理并保留原始日志，方便用户对关键日志快速定位和事后取证； |
| 支持正则表达式、Key-Value、JSON日志解析，支持日志自动化辅助范化； (提供产品功能截图) |
| 支持对日志中的源和目的IP地址进行自动补全； |
| ▲系统可自动识别收集的日志并自动选择范化策略，针对匹配的多条范化策略，系统支持设置策略匹配优先级； (提供产品功能截图) |
| 日志交互式分析 | 系统具备全文检索的大数据处理能力，能够对事件进行非格式化的文本式处理； |
| 用户可自定义事件搜索查询条件，并可保存为策略； |
| 系统支持即席在线查询；用户可根据需要配置事件显示的字段内容等。查询结果可支持加密导出。 |
| ▲采用机器学习对原始日志进行聚类分析，能够对原始日志结构模式进行自动识别(无须范化)； (提供产品功能截图) |
| 支持图形化展示日志属性之间的聚合关系，支持手动选择日志属性，显示多维事件分析图； |
| 日志统计分析 | 可自定义统计场景，统计的字段条件和时间段以及过滤器等可自由设定； |
| 支持将统计结果保存为仪表板、报表和策略；(提供产品功能截图) |
| 日志综合展现 | 系统提供可编辑的自定义仪表板；可对仪表板的任一元素进行下钻，查看原始日志； |
| 可根据需要随时调整已创建的仪表板，编辑仪表板展示条件，调整位置、新增组件等； |
| 关联分析 | 支持基于规则的关联分析引擎，能够提供逻辑关联、统计关联和递归关联三种关联分析能力； |
| 支持单事件关联和多事件关联，能够针对多个不同类型不同来源的安全事件进行综合关联分析； |
| 关联规则支持规则嵌套和引用，通过多规则联合，可精确识别复杂安全事件和场景 |
| 支持分布式关联分析引擎，可以弹性扩展分析能力； |
| 告警管理 | 告警支持提供告警统计策略，选中某条策略，就能展示某个统计图表；支持告警归并，有效抑制重复告警，归并规则可自定义； |
| 报表管理 | ▲提供报表管理功能，根据时间、数据类型等生成报表，为管理员提供决策和分析的数据基础；（提供产品功能截图） |
| 支持提供安全运维报告，帮助运维人员快速生成日常日志分析和运维报告 |
| 备份归档 | 支持按周期的方式选择备份，支持原始日志与分析后日志分离，支持历史日志恢复导入；支持以FTP/SFTP方式将日志数据备份至外部存储空间，支持数据恢复 |

（五）堡垒机

|  |  |
| --- | --- |
| 指标项 | 功能描述 |
| 系统部署 | 性能参数：包含运维授权数≥350，最大可扩展资产数≥1000，图形运维最大并发数≥200，字符运维最大并发数≥350。 |
| 硬件参数：规格：2U，内存≥8G，硬盘容量≥128GB SSD+2TB SATA，电源：单电源，接口：千兆电口≥6个+万兆光口SFP+≥2个，万兆多模光模块≥2个，LC-LC 5M≥2个； |
| 支持协议 | 字符协议：SSHv1、SSHv2、TELNET |
| 图形协议：RDP、VNC |
| 文件传输协议：FTP、SFTP、RDP磁盘映射、RDP剪切板 |
| 支持通过协议前置机进行协议扩展，至少支持扩展KVM、Vmware、数据库、http/https、CS应用 |
| 动作流 | 支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登陆和审计接入，提供截图证明； |
| 用户管理 | 支持批量导入、导出用户信息；支持用户手动添加、删除、编辑、设定角色、单独指定登陆认证方式、设定用户有效期 |
| 用户登陆认证方式支持静态口令认证、手机动态口令认证、Usbkey（数字证书）认证、AD域认证、Radius认证等认证方式；并支持各种认证方式和静态口令组合认证 |
| 支持从windows AD域抽取用户账号作为主账号，支持一次性抽取和周期性抽取两种方式 |
| 支持Windows AD域账号与堡垒主机账号周期比对，自动或手动删除或锁定失效的域账号 |
| 内置三员角色的同时支持角色灵活自定义，可根据用户实际的管理特性或特殊的安全管理组织架构，划分管理角色的管理范畴，提供截图证明并加盖厂商公章； |
| 支持对用户指定限制登录IP、登录时间段（可循环，如每周一到周五9：00-17：00时）等规则，以确保可信用户登陆系统 |
| 支持口令有效期设置，用户账号口令到期强制用户修改自身口令，口令强度必须符合密码策略要求 |
| 支持登陆控制台会话超时时间设置，用户在指定时间内无操作自动注销当前会话 |
| 支持设定访问锁定策略，达到限制主帐号密码输入错误次数和锁定时间的目的 |
| 支持以图形方式查看用户占比、在线用户数量、以及活跃用户 |
| 资源管理 | 支持unix资源、windows资源、网络设备资源、数据库资源、C/S资源、B/S资源 |
| 支持批量导入、导出资源信息；支持手动添加、删除、编辑、查询资源，支持变更默认运维端口 |
| ▲支持RDP安全模式（RDP、NLA、TLS、ANY）设置，以适应RDP-Tcp属性中的所有功能配置，包括加密级别为客户端兼容、低、高、符合FIPS标准等加密级别，提供截图证明 |
| 支持网络设备enable和unix主机su等身份切换的单点登录功能 |
| 支持以柱形图方式查看系统中不同资源所占比例 |
| 运维授权 | 支持一对一、一对多、多对多授权，如将单个资产授权多个用户，一个用户授予多个资产，用户组向资产组授权 |
| 支持跨部门的交叉授权操作，部门资源管理员可将本部门资源授权给其他部门用户，实现资源临时/长期跨部门访问 |
| 支持按授权名称、用户名称、用户账号、资源名称、资源地址、资源账号查询已授权信息 |
| 支持在授权基础上设定双人复核登陆，登录时必须经过第二人授权后才能登录，第二人可通过远程授权或同终端授权两种方式实现授权 |
| 支持在授权基础上自定义访问审批流程，可设置一级或多级审批人，每级审批可指定通过投票数，需逐级审批通过才可最终发起运维操作 |
| ▲支持自定义紧急运维流程开启或关闭，紧急运维开启时，运维人员可通过紧急运维流程直接访问目标设备，系统记录为紧急运维工单，审批人员可在事后查看或审批，提供截图证明 |
| 支持按加密格式导入、导出运维授权数据，方便授权关系备份以及授权数据迁移 |
| 支持生成授权报表和可访问外部资源报表，报表详细展示用户和资源的授权关系，并提供EXCEL、WORD、PDF、HTML等格式导出 |
| 口令策略 | 可以配置口令长度，是否包含字母及字母的长度，是否包含数字及数字的长度，是否包含符号及符号的长度，口令时效性；口令策略还可以配置禁止包含的关键字 |
| 密码策略 | 支持密码策略设置，可自定义密码复杂程度，可设置密码中包含数字、字母、符号及禁用关键字等内容 |
| 支持密码文件备份功能，密码文件需密文保存，密码包及解密密钥分别发送给不同管理员保存，并使用专用的解密器才可打开 |
| 口令变更至少支持windows系统、网络设备、linux/unix系统、数据库 |
| 访问控制 | 支持命令黑命单，对字符型设备（包括但不限于linux、unix、网络设备）的高危命令执行进行阻断，包括但不限于rm、shutdown、reboot |
| ▲支持命令审批规则，用户执行高危命令时需要管理员审批后才允许执行；命令审批规则可以指定运维人员、访问设备、设备账号及命令审批人，提供截图证明 |
| 支持配置资源访问时间规则，即使授权范围内的资源，需在指定时间范围内才可发起访问，确保运维在可信时间范围 |
| 支持对文件传输类协议进行传输控制，包括但不限于RDP剪切板、mstsc磁盘映射、FTP/SFTP等的上行、下行控制 |
| 运维方式 | 支持web页面直接发起运维，无需安装任何控件，并同时支持调用SecureCRT、Xshell、Putty、WinSCP、FileZilla、RDP等客户端工具实现单点登陆，不改变运维人员操作习惯，提供截图证明并加盖厂商公章； |
| 审计日志 | 支持监控正在运维的会话，信息包括运维用户、运维客户端地址、资源地址、协议、开始时间等，并可以实时阻断 |
| 对字符命令方式的访问可以审计到所有交互内容，可以还原操作过程的命令输入和结果输出，并支持通过搜索操作语句或执行结果中关键字定位审计回放 |
| 图形资源访问时，支持键盘、剪切板、窗口标题、文件传输记录，并且对图形资源的审计回放时，可以从某个键盘、剪切板、窗口标题、文件传输记录的指定位置开始回放，提供截图证明 |
| 支持运维审计自查询功能，用户可查看自身的运维审计历史 |
| 支持提供系统内部操作审计，包括管理员和运维用户的登录、登出、对系统的配置操作、账号属性修改等系统管理操作 |
| 支持倍速播放、拖动、暂停、停止、重新播放等播放控制操作，并可以指定时间点定位播放位置 |
| 支持自定义报表，可记录审计报表模板，可生成图形报表，并提供EXCEL、WORD、PDF、HTML等格式导出 |
| 备份与维护 | 支持手动和自动定期备份配置信息，支持配置信息本地备份及异地FTP备份 |
| 支持系统配置还原，可以还原至任一备份点 |
| 具有日志防溢出功能，当磁盘空间达到阈值时，可设置停止记录审计日志或日志回滚 |
| 管理能力 | 支持NTP系统时间同步配置，保证系统拥有可靠的时间戳 |
| 支持日志数据的外置存储，支持NFS、ISCSI和Windows文件共享协议 |
| cpu工作情况，内存使用情况，磁盘使用情况，网卡使用情况，系统数据库工作情况， WEB服务工作情况，其他关键组件工作情况等 |
| 支持从 WEB管理界面重启、关闭设备 |
| 支持通过WEB界面进行系统升级 |
| 支持从WEB页面设置多端口绑定，防止单网卡或单网线故障发生 |
| 支持WEB页面配置双机热备（HA），保证系统可靠运行 |
| 客户端兼容 | 全面支持Windows、linux、国产麒麟系统、Android、IOS、Mac OS等网页端和客户端操作系统下的H5页面一站式运维，实现跨终端适应性BYOD（Bring Your Own Device），提供截图证明并加盖厂商公章； |

（六）综合柜

|  |  |
| --- | --- |
| 指标项 | 功能描述 |
| 品牌一致性 | ★UPS、空调、配电机柜为同一品牌。本次为综合柜扩容，需要与医院现有华为品牌兼容，投标人需在投标文件中提供相关承诺。 |
| 一体化设计 | UPS、配电、监控、空调一体化集成在一个综合柜，设备柜在综合柜两侧灵活扩展 |
| 电源制式 | 380~415V/3PH/50HZ |
| 防雷等级 | 不低于CLASSII/C级，8/20μs。 |
| 防护等级IP | 机柜整体防护等级不小于IP20 |
| 安装方式 | 支持水泥地面直接安装及架空地板安装 |
| 污染等级 | 满足B类使用环境 |
| 机柜门 | 1）机柜采用前后封闭设计，前后门单开，前门配置双层玻璃，以便内部设备可视，并降低设备运行声音。 |
| 2）机柜的前门、后门及侧板均可锁定，用提供的专用钥匙打开。 |
| 3）前后门开启角度不小于120°。 |
| 4）机柜应配备自动弹门装置，方便紧急情况下自动弹开，提供消防联动和应急散热的功能。 |
| 调平支脚 | 机柜采用不小于直径为40mm调平支脚调节机柜的水平度，可支持调节高度范围至少满足：10～55mm。 |
| 滚轮 | 机柜采用四个万向滚轮，单个滚轮动态承重不小于350kg,静态承载不小于500kg。 |
| 整体要求 | 各配电单元：UPS、配电盒、电源指示均模块化设计，机架安装便于维护 |
| 配电模块 | 包含UPS输入、UPS输出、UPS维修旁路开关、防雷保护开关；尺寸≤6U，配电模块至少需要12路IT输出 |
| 防雷器 | 配电柜配置电源防雷器（浪涌保护器/电涌保护器/过电压抑制器）,其泄放电流能力根据招标要求，响应时间≤25ns，残压≤1.2kV(C级)，≤2.0kV(B级)，防雷器配置前端断路器保护。 |
| UPS类型 | 机架式安装 |
| UPS输入电压范围 | 电压输入范围单相80~280V AC或三相138V AC～485V AC |
| UPS容量 | ≥10kVA |
| UPS配置 | 1+1冗余设计 |
| UPS输出功率因数 | 不低于0.9 |
| UPS防雷 | 满足6kV/5kA防雷设计，并提供EMC测试报告证明 |
| UPS效率 | 不小于94.5% |
| UPS过载能力 | 在125%的额定负载时，可至少持续5min |
| 内机安装方式 | 机架式安装 |
| 空调配置 | 1+1冗余设计 |
| 制冷量 | 风冷空调，制冷量不小于12.5kW |
| 制冷量调节范围 | 至少满足20%~100% |
| 压缩机 | 直流变频制冷 |
| 电源制式 | 220V/1Ph,50Hz |
| 送风方式 | 水平送风 |
| 空调风量 | 不小于2600m3/h |
| 制冷剂 | R410A，制冷剂预充注 |
| 外机安装方式 | 落地或挂墙 |
| 除湿 | 低载无凝露设计，可以使低负载（最低10%）、高湿环境中冷通道的湿度维持在20%～80% |
| 冷凝水排水 | 配置强排水泵，兼容上下排水 |
| 走管方式 | 支持上走管或下走管，空调内外机接口管路免焊接设计 |
| 监控采集器 | 1U，机架安装,提供机房动环提供统一北向接口，便于接入统一网管系统或远程WEB界面监控 |
| 漏水监控 | 对模块内有水源的地方进行非定位式漏水检测 |
| 烟雾监控 | 实时监测模块内的烟雾状态； |
| 温湿度监控 | 对模块内环境的温湿度进行检测 |
| 门锁 | 前后门智能门锁，支持本地钥匙打开可检测门状态，并支持远程开门。 |
| 监控显示屏 | 统一监控屏，可实现对模块所有动环进行监控；10英寸以上，电容屏，支持多点触控 |
| 近端通信 | 单个模块支持近端wifi功能，可通过平板电脑或手机APP软件实现本地监控 |
| 厂商资质要求 | 1）ISO 9001国际质量体系认证 |
| 3）ISO 27001信息安全管理体系认证 |

（七）机柜

|  |  |
| --- | --- |
| 指标项 | 功能描述 |
| 模块整体深度 | ≤1350mm |
| IT机柜（宽×高） | 600cm x 2000cm（含通道）\*2套 |
| 材质 | 优质碳素冷轧钢板和镀锌板 |
| 静载 | 机柜静态承载能力≥1500kg（提供第三方检测报告） |
| 密闭通道门 | 双层玻璃门，确保隔热，防止凝露 |
| 走线设计 | 模块输入电缆支持上进线，模块内部电缆支持上走线。 |
| 机柜侧板 | 机柜所有面板可支持单独拆卸和拼装功能 |
| 并柜 | 机柜采用专用的机柜并柜连接件，应支持无需拆卸机柜门情况下实现机柜并柜功能。 |
| 机柜门 | 1）机柜采用前后封闭设计，前后门单开，前门配置双层玻璃，以便内部设备可视，并降低设备运行声音。 |
| 2）机柜的前门、后门及侧板均可锁定，用提供的专用钥匙打开。 |
| 3）前后门开启角度不小于120°。 |
| 4）机柜应配备自动弹门装置，方便紧急情况下自动弹开，提供消防联动和应急散热的功能。 |
| 调平支脚 | 机柜采用不小于直径为40mm调平支脚调节机柜的水平度，可支持调节高度范围至少满足：10～55mm。 |
| 滚轮 | 机柜采用四个万向滚轮，单个滚轮动态承重不小于350kg,静态承载不小于500kg。 |

四、售后服务要求（以下售后服务要求内容的费用均包含在投标总价中，招标人不再另行支付其他费用）

1、★提供不少于三年原厂维护服务。

2、响应时间：7\*24小时电话及现场响应，包括法定节假日。

3、非工作日，当系统出现严重故障，投标人按7\*24\*2小时响应服务，派工程师到现场响应服务。

4、提供热线支持服务及远程故障诊断服务。

5、提供不少于三年备件支持服务。

6、提供原厂备件及支持服务。

7、技术咨询：使用中遇到操作、工作流程不清晰、系统维护等技术上问题时，提供咨询服务，技术人员将负责详细解答。

8、系统定期优化：定期（每年不少于1次）为招标人进行系统优化，对服务器端的系统性能进行例行检查和优化工作。

9、软件版本升级：质保期内有新版本软件推出时，进行现有模块功能的版本升级。

五、★投标人需为所有投标货物制造厂家，或具备合法代理资质的经营销售企业（提供投标截止日在有效期内的制造厂家授权书或代理证明文件）；

六、商务要求

1. 交付日期：合同签订后45天内
2. 交付地点：招标人指定地点
3. 付款方式：

付款方式：交货验收合格并安装调试后，招标方根据医院付款流程，支付合同款项100%。

4. 最高限价

人民币270.00万元

5. 资格条件

（1）具有合法经营资质的独立法人、其他组织；

（2）未被“信用中国”网站（www.creditchina.gov.cn）列入失信被执行人名单、重大税收违法案件当事人名单，且未被中国政府采购网（www.ccgp.gov.cn）列入政府采购严重违法失信行为记录名单；

（3）本项目不接受联合体投标。