中 标 通 知 书

致：浙江安易信科技有限公司

诸暨市第五人民医院机房网络信创安全设备采购项目(编号：诸暨博开 2024-11-04)，于 2024 年 12 月 19 日 14：30 时在诸暨市东旺路 39 号二楼评标室开标，根据招标文件评标办法等有关规定，经评审和公告，现确定你单位为该项目的中标单位，中标报价为：大写：叁拾捌万玖仟伍佰肆拾元整（小写：389540.00 元）。

请您单位在收到本通知书后，在规定时间内上门与用户单位签订采购合同，并在规定期限内正确履约。

采购单位：诸暨市第五人民医院

联 系 人：郦光焕 13588557068

2024 年 12 月 20 日

代理机构：诸暨博开项目管理有限公司

联 系 人：张爱超 13989573703

2024 年 12 月 20 日

注：1.本通知书由中标单位到诸暨博开项目管理有限公司领取发放。

诸暨市第五人民医院机房网络信创安全设备采购项目合同

合同编号：

甲方（甲方）：诸暨市第五人民医院　签订日期：2024 年 1 月 15 日

乙方（供货单位）：浙江安易信科技有限公司　签订地点：诸暨

根据《中华人民共和国民法典》《中华人民共和国政府采购法》等有关规定，以及 诸暨博开项目管理有限公司（编号：诸暨博开 20 24 — 11 — 04 号）采购文件相关要求，经法定程序采购，双方同意签订以下合同条款，以便双方共同遵守、履行合同。

一、采购项目

产品名称	技术要求	数量	单价（元）	合价（元）
信创防火墙	详见附件	2	93270	186540
信创日志审计		1	63710	63710
信创网闸		1	55840	55840
信创堡垒机		1	83450	83450
合计人民币（大写）：叁拾捌万玖仟伍佰肆拾元整　¥ 389540				

二、系统集成基本要求

1. 系统集成基本要求

乙方应对本项目提供完整解决方案，乙方的建议方案应符合本项目的网络结构和设备配置要求，应全面详细了解采购方对全部系统方案的整体要求，保证方案的合理性，并对具体实现方式做出有效建议，同时必须满足有关信息工程的建设条款和规范。

2. 系统集成的工作内容

（1）乙方负责协调所有硬件设备以及本项目所涉及的配套安全服务，以确保达到本项目对硬件、软件、平台及服务的功能要求。

（2）乙方需要根据诸暨市第五人民医院网络的整体规划，将在相应的安全设备、安全平台中配置相关安全策略、访问控制。

（3）乙方负责整个系统的联调、开通，确保达到本项目对整个系统的规范、功能要求。

三、项目建设要求

1. 项目组织及人员配备要求

(1) 乙方应充分考虑满足投标项目的建设要求，提出完整的项目管理、系统设计与开发、培训、项目施工、项目验收、售后服务方案。

(2) 乙方应根据对项目的理解作出项目的人员配置管理计划，包括组织结构、项目负责人、组成人员及分工职责；阐述项目建设中业主方和建设方的职责。

(3) 参与此项目的技术人员具有承担过相同类型项目经验，能够与用户进行良好的沟通，掌握相关领域的相关基础知识，具备相关产品集成、应用和开发的能力。

(4) 乙方应按照投标文件中提供本次项目实施的实施人员名单，以及整个项目实施工期的具体计划安排表实施。

2. 技术资料

（1）项目完结时乙方应提交的成果和整个项目过程电子文档，包括但不限于：系统详细设计；系统概要设计；需求分析报告；系统测试方案；安装维护手册；使用操作手册；培训资料。

（2）没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。

3. 知识产权

（1）乙方应保证所提供的产品或其任何一部分均不会侵犯任何第三方的知识产权。

（2）乙方应保证甲方在软件使用过程中免受第三方提出的侵权起诉。如发生此类纠纷，由乙方承担一切责任并负责解决。

4. 产权担保

乙方项目中涉及的建设内容的所有权完全属于乙方，在交付甲方后保证无任何抵押、查封、债务转移等产权瑕疵。

5. 转包或违法分包

本项目范围的软件，不得转让他人或违法分包他人供应，否则甲方有权解除合同，没收履约保证金并追究乙方的违约责任。

6. 保密义务

（1）双方应严格保守在合作过程中所了解的对方的商业及技术机密，否则应对由此造成的损失承担赔偿。

（2）任何一方不得出于除履行本合同以外的任何目的的披露、传播、复制或使用来自另一方的所有或者部分保密信息；不得在未经另一方书面明确同意的前提下向任何第三方披露本项目相关保密信息；本合同履行完毕后，任一方应当将所有涉及保密信息的载体交还另一方或自行做好管理。

（3）乙方应严格遵循甲方各项安全保密制度，所有信息数据迁移、处理等过程中严禁私自复制、传输，完成建设任务后，乙方使用的用户信息等敏感数据必须物理清除。

（4）乙方有义务保障平台的稳定性、账户的安全性，因平台崩溃、账户盗号或被攻击发布非法信息等引发的问题，所有经济责任及法律责任均由乙方承担。

（5）乙方应保障设备运作过程中采集到的所有数据及信息的安全性；保证数据及信息不外泄，不另作他用。如项目人员有变动，乙方需保障项目数据不外泄，如果因数据及信息外泄或另作他用而引发的第三方投诉、追诉、要求赔偿等纠纷而造成甲方损失的，所有经济损失全部由乙方负责承担。

（6）不论本项目是否变更、解除、终止，本条款均有效。

四、供货时间、范围及要求

1. 供货及安装调试时间要求

乙方应协调主要部件对应的原厂工程师进行现场安装调试，合同签订后30个工作日内完成安装调试。

2. 乙方须保证提供货物为全新的、先进的、成熟的、完整的和安全可靠的，且货物的技术经济性能符合本项目采购要求。

3. 乙方应提供详细供货清单，清单中依次说明型号、数量、产地、生产厂家等内容。

4. 除有特别注明外，所列设备及数量为建设本项目必需但不一定是全部。对于属于整套系统运行和施工所必需的部件，即使在本项目采购中未列出或数目不足，乙方应在投标时应充分考虑并须在执行合同时无偿补足。

5. 成交乙方应提供所有安装和检修所需专用工具和消耗材料等，并提供详细供货清单。

6. 所有货物应根据甲方要求、指定位置进行规范安装。

五、质量标准和技术服务条件

1. 质量标准要求

（1）本项目的所有软、硬件(如电源适配器、线缆、软件、硬件模块等，包括未列出而系统实施又必需的软件、硬件)需配齐以构成一套完整实用系统，如有任何遗漏，由乙方免费补齐。

（2）乙方方案中的硬件设备如需使用特别接头、插座等，由乙方提供。

（3）所投设备需为原厂设备，符合国家技术规范和质量标准，通过国家有关部门检测合格的原产地设备，能够与甲方现有设备正常连接；设备安装调试完毕后，能在其功能范围内保障用户的系统安全、稳定运行。

（4）所投设备及主要部件均须非停产设备，并提供备件、附件和耗材的供应。

（5）本次采购的供货除包括上述设备外，还应包括随机的辅助设备、专用电线电缆、随机软件、技术资料（包括操作培训手册、产品使用指南、维修指南和含维修网点在内的服务手册等）、设备运行所必需的随机消耗材料，相应的技术服务与质量保证。

（6）验收条件：

开箱验收：清点设备装箱内容符合装箱单所列并符合招标文件要求和承诺书承诺；

开机验收：设备应通电开机后进行所规定时间的试验运行后方可验收。

（7）验收方式：设备安装、调试完成之后开始做验收准备工作，双方须按采购文件以及乙方的乙方按要求对设备逐个进行全面的技术指标和功能测试。所有系统测试完毕正常运行后可进行最终验收。

（8）对所有的设备等只能作为本项目使用，不得转借其他项目。

（9）本系统产生的任何照片、视频、文字等信息数据产权归甲方所有，不得擅自截留，用作商业开发利用。

（10）乙方供货产品必须是原厂商、正宗品牌、正规渠道的产品，不得用假冒及伪劣产品替代；如出现上述质量问题，甲方有权退货；如造成损失的，甲方可要求乙方给予赔偿。

（11）乙方须对甲方的技术人员培训。乙方须在投标文件中提供详细的培训计划，包括培训内容、培训时间、培训费用等。技术培训费用应包含在投标总价中。

2.技术服务要求

（1）乙方应确保其技术建议以及所提供的产品的完整性、实用性，保证全部系统及时投入正常运行。否则若出现因乙方提供的设备不满足要求、不合理，或者其所提供的技术支持和服务不全面，而导致系统无法实现或不能完全实现的状况，乙方负全部责任。

（2）如果产品在服务期内发生设备故障，乙方应及时予以响应（免费上门服务），否则甲方将自行采取必要的措施，由此产生的风险和费用由乙方承担。

（3）如遗漏了必须具备的设备、配件或服务，乙方有义务保证甲方系统的完整性，如项目实施过程中因缺少设备、配件或服务导致甲方系统无法正常运行，由乙方提供相应设备、配件，费用包含在合同总价中。

六、付款方式

合同签订后7日内，甲方支付合同金额40%的预付款，剩余款项待所有设备到货、安装、调试完成经验收合格后付清。乙方必须提供等额正式税务发票。如因乙方提交发票延迟造成的支付逾期，不视为甲方违约。

七、履约保证金

1、乙方在签订合同前需向甲方缴纳合同金额 1 % 即￥3895.40元的履约保证金。

2、履约保证金在甲方将项目验收合格后，无息退还给乙方。

3、如乙方未能履行合同规定的义务，甲方有权在履约保证金中取得补偿。

八、产品数量变更

合同履行过程中，甲方根据实际情况，需要增减与合同标的相同的产品（或服务），在不改变合同其他条款的前提下，可以与乙方协商签订补充合同，但所有补充合同的采购金额不得超过原合同采购金额的 10%，增减产品（或服务）的价格为相应中标产品（或服务）的价格，且事先须向诸暨市财政局审核备案。

九、售后服务

1. 乙方必须为本项目提供三年的免费售后维护服务，售后维护期从项目终验合格后开始计算。质保期内出现问题，15分钟内响应，1小时内到达现场，2小时内解决问题，如现场无法解决，需提供相同档次的备机供使用。要求乙方在乙方方案中有完整的服务方案，服务方式应包括远程电话支持、远程网络支持、现场服务支持等方式，服务响应时间参照前面所述标准。

2. 乙方应按照在投标文件中对质量保证及售后服务方案做出的承诺提供服务。

3. 乙方须做出无推诿承诺。无论由于哪一方产生的问题而使系统发生不正常情况时，在得到甲方通知后，须立即派遣工程师到场，全力协助系统集成商和其他乙方，使系统尽快恢复正常。

4. 安全巡检服务：提供月度安全巡检服务。安全巡检服务是指定期对用户的网络设备、安全设备、重要业务系统、重要终端等进行的安全检测，检测内容包含漏洞扫描、基线核查、日志审查，检测完成后提供全面的巡检服务报告，给出存在的安全风险并提供对应的修复建议。

安全巡检服务包含以下内容：

（1）漏洞扫描：漏洞扫描评估主要是根据已有的安全漏洞知识库，模拟黑客的攻击方法，检测网络协议、网络服务、网络设备等各种信息资产所存在的安全隐患和漏洞。采用工具对网络扫描网络中的核心服务器及重要的网络设备，包括服务器、交换机、防火墙等，以对网络设备进行安全漏洞检测和分析。

（2）基线核查：采用扫描脚本的方式对操作系统、数据库、中间件等进行配置检查，检查项包含但不限于：账号策略、登录超时、特权用户、ssh配置、身份鉴别等。

（3）日志审查：检查安全设备日志，识别网络中发生的攻击事件、病毒事件、设备异常事件等，分析网络存在的安全风险隐患。

5. 乙方负责设备的安装调试，其中包括离线备份设备的安装及连接调试。还包括与已有设备的对接，并提供质保期内设备搬迁集成服务。

6. 乙方应提供详细的项目实施方案，说明项目的实施计划、实施过程、质量控制措施、成功保障措施、项目完成后交付的成果文档以及其它认为需要说明的内容。

7. 实施服务要求

（1）实施服务必须为设备原厂商提供。

（2）乙方在本项目实施期间，其技术团队必须全程常驻甲方指定地点，如发现乙方技术团队没有按照要求实施服务，甲方将单方面解除合同，履约保证金不予退还，并保留进一步追究相关法律责任权利。

十、违约责任

1、甲方无正当理由拒收产品（或服务），由甲方向乙方偿付合同总价的5%违约金。

2、甲方未能在合同规定期限内验收完毕的，每超过一天，付合同价的 0.5 %的违约 金给乙方。

3、如甲方未按约定支付款项的，应向乙方支付逾期利息，利率为合同订立时1年期贷款市场报价利率。

4、乙方不能交付产品（或服务），甲方有权扣留全部履约保证金；同时乙方向甲方支付合同款总价5%的违约金。

5、乙方逾期交付产品（或服务）的，每逾期1天，乙方向甲方偿付逾期部分产品（或服务）货款的 0.5 %的滞纳金，如乙方逾期15天，甲方有权解除合同，解除合同的通知自到达乙方时生效。

十一、其他约定事项

无。

十二、解决合同纠纷方式

其它未尽事宜或履行时发生争议，由双方本着诚实信用的原则协商解决，协商不成 功可选择：向 诸暨市 人民法院起诉。

十三、其它

1、本项目的招标文件、投标文件、中标通知书作为合同的附件，具有同等法律效力。

2、本合同自签订之日起生效。

3、本合同一式三份，甲乙双方各执一份，代理机构存档一份。

采购单位	供货单位
单位名称（盖章）诸暨市第五人民医院	单位名称（盖章）浙江安易信科技有限公司
单位地址：	单位地址：浙江省杭州市拱墅区万融城1幢1602室
法定代表人：	法定代表人：
委托代理人：	委托代理人：
联系电话：	联系电话：0571-86086995
传真号码：	传真号码：0571-86086995
邮政编码：	邮政编码：31100
	开户银行： 杭州银行西湖支行
	账 号：3301040160021045391

附件：

1.信创防火墙

技术指标	参数要求
基本要求	信创设备，此为信创防火墙设备，又是零信任设备，设备≥12个千兆电口（6对Bypass），≥4个千兆光口，≥1个CON口，≥2个USB 3.0口，≥1个管理口，≥1个HA口，≥1个业务扩展槽位，≥16G内存，≥1T硬盘，双电源。
	HTTP应用层吞吐量≥18Gbps，IPS吞吐量≥18Gbps，AV吞吐量≥5.5Gbps，并发连接数≥3000万，每秒新建连接数≥28万，IPSec隧道数≥10000，零信任并发在线用户数≥8000。
	配置3年IPS入侵防御、AV病毒过滤、TI威胁情报、APP应用识别、8个零信任许可、5个虚拟防火墙许可、云安全运维/订阅许可。
NAT	要求所投产品支持NATv6、NAT444、NAT64、DS-Lite、Full-Cone-NAT等地质转换技术，并可对SNAT\DNAT进行命中分析，帮助用户识别长期未命中的NAT规则。
	支持NAT扩展技术，突破传统单个公网IP地址64512个端口的瓶颈达到更大值。
策略管理	支持基于国家/地区维度进行流量控制等安全策略，支持垃圾策略清理，支持聚合策略以及策略导出。
	支持自学习生成策略功能，聚合流量并生成细化的策略规则，辅助用户更快速、更准确和更完整地配置安全策略。
	提供策略分析引擎，支持一键全局分析和单独策略的即时分析，至少支持检测出冗余策略、隐藏策略、冲突策略、可合并策略、空策略、过期策略，并提供问题策略的原因说明和优化建议
业务扩展	响应业务软件扩展，所投产品提供容器化服务，支持第三方容器镜像的加载
带宽限制	支持用户/IP流量限额策略，可基于流量七元组限制，可设置白名单，可设置带宽阈值
负载均衡	支持智能链路负载均衡技术，可动态探测链路响应速度并选择最优链路进行转发。支持DNS透明代理功能，可基于负载均衡算法代理内网用户进行DNS请求转发，避免单运营商DNS解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率。
IOT安全	支持自动发现IOT设备，对识别出的设备进行实时监控，然后根据配置对出现非法行为的设备进行阻断等操作。。
SD-WAN	能够支持全生命周期的SD-WAN整体解决方案，包括：自动化部署、链路双活、链路质量检测、隧道安全、控制器高可靠等功能。
云安全运维	支持通过云端SaaS管理平台为用户提供便捷、高质量以及低成本的增值安全服务，支持手机APP对设备进行监控：通过手机可以第一时间获知设备的基础信息，安全风险实时告警，帮助快速定位问题、安全可视化实时呈现。提供App下载URL，该APP不能是VPN客户端软件，该APP不限制使用用户数
入侵防御	基于状态、精准的高性能攻击检测和防御，支持针对HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS等20余种协议和应用的攻击检测和防御。
	具备16000种以上攻击特征库规则列表，至少支持基于协议类型、操作系统、攻击类型、流行程度、严重程度、特征ID等方式的查询。
病毒过滤	支持基于流模式的病毒过滤，可对SMB\IMAP等协议传输的病毒以及不少于5层压缩病毒文件进行检出，要求本地病毒特征库规模≥1000万，支持手动添加、删除病毒特征。
共享接入	支持识别和封堵私接主机，包括无线路由器等软硬件网络共享方式；可制定策略分别设置私接终端类型个数为阀值进行封堵
云沙箱平台对接	支持扩展云端沙箱技术，可将可疑文件提交云端沙箱进行安全模拟运行，并根据运行结果与防火墙实现联动。

威胁情报	支持与云端威胁情报中心联动，支持威胁情报与防火墙威胁事件、威胁日志检测结果加强与取证，用户可通过手动触发与自动触发将日志元素上送威胁情报平台进行上下文查询。
防雷击	为保障日常使用的稳定性，所投产品具备防雷击浪涌等级三级以上，通过浪涌（冲击）抗扰度（4KV）测试项目
Web防护	支持Web防护，可对高频访问限制、敏感目录扫描、SQL注入检查、XSS注入检查、外链检查、盗链检查、Iframe检测、CC防护等功能。支持WEB应用防护特征库数量超过10000种。
虚拟系统	支持虚拟系统功能，每个虚拟系统可自定义CPU资源、会话数、策略数、安全域数、源NAT数、目的NAT数、IPSEC VPN隧道数、会话限制规则数、IPS功能、URL功能、关键字类别、威胁日志等。
电磁兼容	所投产品满足电磁兼容性要求，
测试验证	中标后3天内提供投标型号的测试设备对招标要求的功能性能进行逐项测试验证，测试所产生的相关费用均由中标人承担，若无法在规定时间内提供测试设备或测试结果与招标要求不符，取消中标资格，中标人承担所有责任。
质保服务	提供原厂3年技术支持和保修服务，最终用户方为“诸暨市第五人民医院”，为保证货物是原厂家最新生产合法渠道货物，中标后提供原厂服务承诺函和原厂盖章授权函。

2.信创日志审计

指标项	指标内容
基本要求	信创设备，设备≥8个千兆电口，≥1个CON口，2个2个USB 3.0口，≥4T硬盘，≥16G内存，≥2个扩展槽。
	日志处理性能≥7000EPS，授权≥50个设备许可，可扩展至200个。
审计仪表盘	支持自定义仪表盘，可在一个仪表盘中选择多个对应的微件，可涵盖日志中的所有字段，仪表盘具有全屏监控功能，仪表盘中可直接导入事件统计中的各类图表，支持实时监控，支持配置实时监控策略，支持创建多个仪表盘
数据采集	支持Syslog、SNMP Trap、WMI、文件、数据库、SMB、二进制、插件扩展、Kafka、SOCKET、日志导入等
资产管理	支持资产主动发现。通过对网络进行资产扫描，可将发现的IP对象转资产或删除 支持资产被动发现。可将网络划分成多个安全域，系统能自动发现安全域中的IP对象并可以转资产或删除 支持添加、修改、删除资产；支持对资产的基本属性进行维护，并可以增加自定义属性 支持拓扑自动发现，可手动添加拓扑，并能够展示整体安全、事件分布、告警分布等 支持资产自定义分级分组、标签 支持在一个资产下添加多个日志源（日志采集的对象） 支持资产性能监控，如监控CPU、内存、磁盘使用率等资产指标 支持资产地图，可查看资产整体安全状态、性能指标信息以及关联日志源的日志信息
日志采集	支持采集的对象包括安全设备、网络设备、操作系统、数据库、中间件、应用系统、虚拟机等 支持主动、被动相结合的数据采集方式，支持通过Agent采集日志数据，支持通过Syslog、SNMP Trap、HTTP、TCP、telnet、JDBC、WMI、文件、Kafka等方式采集日志 支持日志标准化解析（范式化、归一化），将不同格式日志解析为多个字段，自动识别系统类型至少达到200种 支持日志自定义解析，系统自带图形化工具，可通过GROK、分隔符、JSON、XML、时间等自定义解析规则

	支持解析规则的批量导入/导出 支持日志源的自动发现，根据接收到的日志自动识别并创建日志源 支持日志源的自定义分级分组 支持不同设备相同IP的日志识别 支持自定义日志过滤策略，支持全局过滤、局部过滤，可选择对单个或多个日志源进行日志过滤 日志过滤支持字段过滤与指定时段过滤 支持对单个/多个日志源批量转发，支持定时转发，可通过Syslog、TCP和Kafka方式转发到第三方平台，并且支持转发原始日志和已解析日志 支持IP v4/IPv6采集。设备支持ipv6的地址管理、接收和查询，支持日志加密传输； 支持日志采集器限流功能；标准化字段多达95个字段；
日志分析	系统内置审计策略，内置审计策略至少600条 支持自定义审计策略 支持从审计策略模板直接创建策略，并可通过事件的任意字段制定规则创建策略 审计策略可以定义审计事件的名称、分类、级别以及命中后是否继续匹配其余审计策略 提供预置审计策略模板，包括：Windows主机类审计策略模板、Linux/Unix主机类审计策略模板、防火墙类审计策略模板、扫描器类审计策略模板、IDS/IPS类审计策略模板、防病毒类审计策略模板、数据库系统类审计策略模板、萨班斯审计策略模版、等级保护审计模板等 内置网站攻击、主机异常、账号异常、暴力破解、漏洞利用、权限异常等至少10种安全分析场景，内置关联规则至少400条 支持关联规则自定义设置功能，支持类型包括过滤规则、统计规则、序列规则、模式规则、多源日志关联和机器学习 支持跨设备的多事件关联分析，若日志满足系统内置或用户定义的关联规则，将产生关联事件 关联事件管理可以统一监控事件的命中情况，包括来源的设备、事件类型、最近命中时间以及命中总次数等 支持接收来自下级日志采集器转发的日志、安全事件和告警事件进行二次分析、关联 支持自定义数据字典，系统可从各类日志、事件中抽取相关片段准确和完整地映射至安全事件的标准字段，内置映射字段至少达到1000个 支持活动列表，可动态维持数据之间的关系映射，如账号与审计人员、IP与审计人员、是否是上班时间等 支持地理信息映射，根据其所选IP字段，映射到国家、省份、城市、安全域等
流量审计	支持对镜像流量的审计，审计内容包括mysql、pgsql、mongodb、redis、人大金仓、http等数据库和流量审计
日志检索	支持对解析后日志、安全事件、告警事件、原始日志等的查询 支持日志查询普通模式，可通过关键字等方式查询 支持日志查询高级模式，可通过多关键字、模糊、正则表达式等方式组合查询 支持将查询结果进行保存、导出 支持查询条件保存为查询模版，用于后续快捷调用
事件分析	对每台日志源的日志接入量呈阶段性统计展示
事件查询	查询模式支持普通模式和专家模式；两种模式均可以保存查询条件，方便之后查询使用； 普通模式支持常规字段查询和精细字段查询，查询后日志支持离线图形化分析； 专家模式支持表达式方式查询，用户可根据表达式快速、准确查询到日志信息
统计报表	支持生成综合报表、数据报表和统计报表 支持导出PDF、WORD、EXCEL、CSV报告 内置事件统计策略和图表，支持自定义事件统计策略和图表
告警管理	系统内置丰富审计类和关联类告警策略，并灵活支持自定义策略 对于告警的处理主要包括忽略、处理 具备告警合并和在一个时间段内抑制报警次数的能力

	可指定告警接收人员 告警方式包括短信、邮件、钉钉等
知识库	内置知识文章、事故案例、安全级别要求、典型日志事件介绍、日志审计配置指导等。并支持自定义创建增加知识库内容
系统管理	支持系统参数配置，包括自定义磁盘、CPU、内存等百分比告警阈值 支持系统基本配置，包括修改主机名称、网络接口IP、路由等，内置抓包、PING、端口测试等工具 支持设置日志存储备份策略，包括系统日志保存期（容量/天）、磁盘使用率百分比等 支持日志文件远程备份到外置存储节点，支持FTP、NFS、ISCSI、SMB等存储方式 支持数据容错，支持将错误日志重新入库 日志接收队列大小可配置，可存储因超过最大接收性能而未入库的日志 支持集群管理，支持审计中心、日志采集器的策略配置及下发 支持个性化管理，用户可自定义新的平台名称、导航栏名称、LOGO标识等
用户管理	用户支持三权分立设计模型 ，支持自定义权限角色 支持连续登录失败锁定用户，支持自定义失败次数、锁定时间、用户登录后超时时间 支持管理员访问控制，可设置指定IP、网段允许或拒绝管理员登录 支持自定义密码强度设置，可自定义用户密码强度要求，密码复杂度、长度 支持多因子认证，认证方式可为邮件、短信
部署要求	支持集中和分布式部署，系统全面支持IPV4/IPV6
资质证书	提供公安部-计算机信息系统安全专用产品销售许可证证书（增强级） 提供中国国家信息安全产品认证证书（增强级） 提供涉密信息系统产品检测证书
测试验证	中标后3天内提供投标型号的测试设备对招标要求的功能性能进行逐项测试验证，测试所产生的相关费用均由中标人承担，若无法在规定时间内提供测试设备或测试结果与招标要求不符，取消中标资格，中标人承担所有责任。
质保服务	提供原厂3年技术支持和保修服务，最终用户方为“诸暨市第五人民医院”，为保证货物是原厂家最新生产合法渠道货物，中标后提供原厂服务承诺函和原厂盖章授权函。

3. 信创网闸

技术指标	招标要求
基础要求	信创设备， 2U，液晶屏，双电源，≥16G内存，≥256G SSD硬盘； 内网机：≥4个千兆光口，≥6个千兆电口，≥1个CON接口，≥2个USB接口； 外网机：≥4个千兆光口，≥6个千兆电口，≥1个CON接口，≥2个USB接口；
	性能：吞吐量≥600Mbps，并发连接数≥20万，数据库同步速率≥2000条/秒，并发视频路数≥240路D1视频，系统延迟<1ms； 授权：配置文件交换模块、数据库同步模块、视频交换模块、安全浏览模块、FTP代理模块、邮件代理模块、防病毒模块和入侵防御许可；
架构	产品采用“2+1”（即双主机系统+物理隔离数据通道控制系统）体系结构；通过嵌入式数据通道控制系统隔离外部网络，而不是采用DMA、SCSI、网卡等方式实现；采用特有控制逻辑和专用通讯协议完全控制数据的实时交换，确保可信网络（域）和非可信网络（域）之间任何连接的断开，彻底阻断TCP/IP协议及其他网络协议；
系统	支持双系统引导，通过管理平台控制系统启动顺序，当前系统出现异常时，自动切换到备份系统，并支持系统相互备份和自动还原功能。
系统监控	带液晶屏，液晶菜单可显示内外网机IP地址、CPU使用率和内存使用率等整机信息，具有设备异常（如网络IP冲突、通讯异常等）监测报警功能（提供物理结构图和功能图）
高可用	具备多网口链路聚合功能，可实现内网网口和外网网口链路备份，分发策略支持Layer2、Layer2+3、Layer3+4；

	具备HA双机热备功能，可通过独立的热备端口或普通业务端口实现双机热备。
	负载均衡功能，支持HTTP/HTTPS、邮件、文件同步等业务负载均衡，负载均衡算法至少支持轮询、最少连接数、原地址哈希、随机等
文件同步	文件同步支持FTP、SAMBA/NFS等文件传输协议。
	支持文件传输方向可控，实现单向或双向传输。支持病毒检测。
	支持对文件内容智能语义分析，对指定文件的内容关键字过滤，确保只有符合策略的数据文件才允许被同步。
	支持先镜像后增量、增量同步、镜像同步等多种同步模式。
	支持传输后删除源文件或源文件夹、删除同步等传输策略。
	支持目的文件发生变化时重新同步。
	支持目录内子目录同步，子目录级别不受限制。
	文件同步支持时间段的控制：时间段可以是一次性执行、某个时间段执行、周期循环执行三种方式。
数据库同步	持ORACLE、SYBASE、MySQL、SQL Server、DB2、PostgreSQL等主流数据库同步和支持信创达梦、人大金仓等数据库的同步。
	支持多种同步方式（如先镜像后增量、增量），同步模式支持单向和双向同步。
	支持同构数据库之间、异构数据库之间的数据同步，无需修改数据库表结构。
	支持表级、字段级同步。
	支持对指定字段和指定字段的指定内容允许同步或不允许同步。
	支持时间段的控制：时间段可以是一次性执行、某个时间段执行、周期循环执行三种方式，且同步数据的数量可选及自定义。
	支持数据库同步实时日志记录，提供日志审计、查询。
	支持数据库连接性测试及测试结果反馈功能，提升文件同步配置的易用性。
	支持灵活的数据库冲突处理策略，当关键字数据发生冲突时可选择：覆盖/丢弃。
	可分别控制insert、update、delete的数据传输。
文件交换	新增文件交换客户端（windows版本）。
	内置用户组织架构，能够批量导入，自动生成用户组织架构
	能够对接AD域服务器，自动获取域用户和组织架构
	具备文件发送审批功能，重要文件审批才能发送。
	文件客户端安全支持密码有效期、最大登录失败次数和锁定时长等策略。
	支持病毒查杀、文件大小、文件类型、文件内容检测，拒绝不合规文件传输。
	文件交换客户端支持下载目录自定义和管理功能。
	具备限制特定用户的文件传输大小，具备用户级的文件交换权限策略设置，如允许/禁止内网到外网或外网到内网的传输。
	文件发送/接收行为详细记录，包括发送/接收人、文件大小、文件名称等记录信息，审计支持下载还原文件，满足事后溯源要求，文件发送/接收具备进度条显示，便于文件发送或接收者能够直观了解文件发送/接收进度
视频网闸	支持SIP、RTSP等主流视频协议。
	支持视音频同时传输。
	支持基于动态端口传输的流媒体视频应用。
	支持视频管理服务器数据转发，视频管理服务器通道建立。
	支持视频SIP服务器数据转发，SIP管理服务器通道建立。能够严格区分视频数据流和控制信令流，根据策略配置可以控制视频数据的单向传输。
	支持主流视频监控厂商。
组播代理	支持ASM（任意信源）、SSM（指定信源）、SFM（过滤信源）三种类型的组播。

FTP访问	支持文件名命名黑名单、扩展名类型黑名单过滤
	支持至少47种FTP命令黑白名单控制，如上传、下载、删除等；
	支持内容关键字过滤、文件类型过滤、命令过滤，支持导入内置命令或自定义编辑命令；
	支持对目的地址和端口进行访问控制；
安全浏览	支持HTTP内置七种请求类型（GET/POST/PUT/HEAD/DELETE/OPTIONS/TRACE）的黑白名单控制。
	支持自定义命令控制过滤。
	支持HTTP和HTTPS正向或者透明代理。
协议代理	支持TCP/UDP自定义代理访问并可自定义命令，对命令进行允许、拦截配置。
	支持TCP/UDP数据单向传输代理。
	支持1bit协议代理。可实现访问服务端只能回复1bit长度的信息，其他内容会被拦截，客户端发送则没有限制。
	支持邮件正向代理、邮件透明代理。可实现命令过滤拦截且不断开连接。
	支持SMB协议代理，可对Read、Write、Create等19个命令进行过滤。
	支持DNS代理。
	支持SNMP代理，set-request、get-response、get-request、get-next-request等命令进行过滤。
入侵检测	具有实时入侵检测机制，支持对BasicAttack、 SMTP、FTP、DNS、DOS/DDOS 攻击、PortScan 的检测。
安全管理	支持CPU、内存、硬盘状态实时监控。
	支持HTTPS的Web方式管理，实现了远程管理信息加密传输。
	支持必须由内网主机系统来管理和配置网闸，而不是采用低安全的管理方式，如采用内外网口分别管理和配置网闸；
	系统登录界面采用USBkey和用户名与密码双因子进行认证
	支持时间控制管理，可设置多个时间点来控制网闸网络服务的启动、终止；
防暴力破解限制	支持系统防爆处理，对管理员登陆有密码次数限制，密码输入错误，超过限定次数，自动锁定设备，阻止非法管理员再次登录。根据限定期限，可自动解除锁定。
接入方式	支持IPV4/IPV6双栈接入。
安全通道	支持映射模式、网关模式、路由模式、网桥模式功能。
	支持透明、代理及路由三种工作模式。
	源地址转换功能和虚拟IP技术，可对外部隐藏内网真实地址。
路由配置	支持IPV4静态路由，IPV6静态路由。
集中管理	支持标准的SNMP协议，可与网管平台无缝对接。
	支持集中管理，支持对多台设备进行统一管理。
日志空间管理	支持自定义日志空间大小，告警百分比，日志留存天数。
备份和恢复	支持备份、恢复功能，能对系统的各业务模块配置单独进行备份和恢复
时间配置	支持修改系统时间和日期，可设置时间与Internet时间服务器同步。
告警管理	支持针对网闸日志使用率超过磁盘限制的短信告警。
系统调试	支持针对指定网卡进行故障测试，测试工具包含traceroute、telnet、ping、arp、tcpdump等。
测试验证	中标后3天内提供投标型号的测试设备对招标要求的功能性能进行逐项测试验证，测试所产生的相关费用均由中标人承担，若无法在规定时间内提供测试设备或测试结果与招标要求不符，取消中标资格，中标人承担所有责任。

质保服务	提供原厂3年技术支持和保修服务，最终用户方为“诸暨市第五人民医院”，为保证货物是原厂家最新生产合法渠道货物，中标后提供原厂服务承诺函和原厂盖章授权函。

4.信创堡垒机

技术指标	指标要求
基本要求	信创设备，设备≥2U，≥8个千兆电口，≥4个千兆光口，≥1个CON口，≥2个USB口，2个扩展槽，≥16G内存，≥4T硬盘，冗余电源。字符并发数≥500，图形并发数≥300。
	授权：配置200个授权许可，可扩展到1200个。配置1个USBKEY和1个动态令牌用于双因素验证。
系统架构	支持单机部署、双机热备部署；
	采用https加密协议对系统进行管理，支持IPV4/IPV6网络环境下操作管理；
	系统内置SSL VPN模块功能，支持远程用户安全接入，SSL VPN用户名与密码策略系统完全一致，并支持配置、VPN传输协议、端口、虚拟地址段及VPN路由；
身份认证	系统支持用户多角色划分功能，如系统管理员、密码管理员、审计管理员、部门管理员、运维用户等，对各类角色需要进行细粒度的权限管理。也可自定义角色及权限范围，各角色功能定位明晰，不可越权；
	系统支持用户、资产按照部门进行划分，并支持多级部门（无级别限制）机构，各部门机构用户、资产隔离，可根据各级部门机构进行独立管理；
	系统对用户的身份认证需支持采用两种或两种以上组合方式进行身份验证：手机动态令牌认证、LDAP认证、AD域认证等自由组合认证；
	支持手机动态令牌身份认证，内置动态口令双因素认证，双因素系统内置在系统中，不需要使用其它的服务器（或虚拟机）进行安装，用户建立、令牌绑定等操作，在同一个管理界面中完成，客户端为手机APP/小程序方式查看令牌动态密码；
	支持运维用户账号密码强度校验和提示（长度至少8位；密码需含有数字、字母、特殊字符等）；
	支持强制定期修改运维人员账号密码功能，并可配置强制修改期限；
	支持认证方式全局设定、单一用户认证方式设定，支持多种认证方式组合
	支持创建运维用户随机密码功能，随机密码可通过邮件、短信等方式发送给指定运维用户；
资产管理	支持通过SSH/SFTP/VNC/RDP/HTTPS等协议实现运维对象（Windows、Linux、网络设备、数据库、安全设备、信创操作系统等）的资源添加及认证登录；
	支持通过应用发布的代理进行协议扩展，支持Radmin、Pcanywhere、 HTTP/HTTPS，可自定义其它访问协议及客户端支持；
	支持应用发布方式访问web资源越权访问提示及阻断功能；
	支持协议代理端口自定义；
	支持主机、网络设备、安全设备、数据库、IP地址、操作系统类型、协议端口、运维方式等资产信息及对应密码、密钥的收集录入配置；
	支持运维目标主机登录限制，同一台服务器可以只允许一个用户登录，防止已登录用户被登出；

	支持对运维对象的登录测试，支持运维人员与运维对象的批量关联；
	支持对B/S(HTTP/HTTPS)、C/S及数据库客户端程序进行集中管理及应用分发，支持Windwos2012/2016及信创麒麟操作系统作为应用发布服务器；
	支持资产扫描功能，可根据扫描地址（段）、扫描端口、归口部门等信息进行配置扫描，也可实时终止扫描任务，扫描后资产设备可进行一键提交归档，方便用户统一管理；
	支持对被管理Windows/Linux/网络设备的登录账号进行统一定期、周期修改密码，密码强度可进行配置，并可通过邮件/SFTP/FTP进行即时备份，密码备份文件进行加密处理；
	支持端口代理服务， 包括字符代理、ftp代理、Mysql、Redis；
	系统支持对LINUX系统账号进行自动收集及一键归档保存；
授权管理	支持对人员身份的有效时间段、来源IP进行验证；
	支持对连续登录失败人员账号进行锁定策略配置；且对锁定账号进行人员账号恢复、自动恢复等功能；
	支持对字符操作（SSH/TELNET协议）的指令/指令集进行控制，通过指令/指令集黑白名单实现对命令的有效管理，指令/指令集对运维账号、资产进行策略关联，命令输入支持正则表达式，可进行策略允许、指令阻断、会话阻断、申请确认等动作；
	支持管理员新建、查看、编辑、删除运维任务；运维任务支持手动、自动（定期）执行，运维任务包括脚本任务、命令等任务，输出的执行任务日志可导出；
工单管理	支持内置电子工单，运维人员可以在产品的web界面，手动填写工单，填写/选择的内容必须包括：标题、运维时间段、文件权限、描述、设备资源账号等；工单经审批通过后，运维人员可立即取得相应访问权限；
运维管理	支持最近常用设备、收藏及批量登录功能，便于用户的快速查询及登录，提高用户登录运维资产效率；
	支持Windows系统下的 IE/Chrome/火狐浏览器运维管理外，还支持信创操作系统下运行的浏览器运维和管理；
	支持运维用户终端无需安装和调用任何插件及客户端程序时，用户即可实现（RDP/VNC/SSH/TELNET）各种协议的登录运维；
	支持通过WEB页面调用XSHELL、SecureCRT、PUTTY等客户端登录目标运维设备；
	支持本地字符运维工具通过穿透堡垒机直连SSH/TELNET设备，且支持双因子认证；
	支持本地数据库运维工具通过堡垒机端口代理对mysql、redis的运维操作；
会话功能	支持启停应用发布防绕行限制，控制运维用户访问目标主机外的IP地址；
操作审计	支持对系统管理员操作（增/删/改等动作）进行详细的日志记录，日志记录结果具备较强的可读性；

	支持对字符协议（SSH/TELNET）的操作审计，支持基于运维人员账号、操作时间范围、目标运维对象、操作命令和输出结果进行关键字检索、定位和拖拽回放，支持多倍速、低倍速回放；
	支持对图形协议（RDP、VNC等）的操作审计，支持基于运维人员账号、操作时间范围、目标运维对象进行检索、定位、拖拽回放，支持多倍速、低倍速回放；
	支持对文件传输协议（FTP、SFTP）的操作提供上传/下载的记录审计，支持对运维人员账号、操作时间、目标运维对象、上传/下载行为、文件及文件名称进行审计；
	支持对重要字符命令和数据库命令进行实时审核，运维人员执行命令后，系统响应动作包括，指令审批、忽略指令、阻断会话、产生告警；支持的数据库命令包括ORACLE、MSSQL、Sybase、Mysql、DB2、Postgresql等数据库；
	支持B/S（应用发布客户端）、C/S运维数据库的操作审计记录；支持B/S（应用发布客户端）运维数据库的操作视频审计记录；支持通过WEB方式调用操作审计录像回放，支持正常、快进、慢进、鼠标拖拽播放；
	支持水印功能，在用户运维设备、在线审计回放后的录像文件操作时。水印标签包括用户名、真实姓名等属性信息；
	支持任意浏览器无插件安装下播放审计到的字符运维、图形运维审计记录；
异常告警	支持根据系统性能（CPU/内存/硬盘/SWAP使用率）阈值进行告警，告警方式可根据级别（高、中、低）进行消息、邮件、短信通知告警；
	支持根据系统访问量（用户在线数、SSH协议在线数、RDP协议在线数、VNC协议在线数、FTP协议在线数、SFTP协议在线数、TELNET协议在线数及应用在线数）阈值进行告警，告警方式可根据级别（高、中、低）进行消息、邮件、短信通知告警；
	支持客户端检测账号异常、ip变化等因素，启用后用户的ip地址发生变更将无法继续访问堡垒机，并进行告警；
界面配置	支持用户对界面的风格自定义，系统支持界面定制配置，配置包括用户登录背景、logo展示区等；
外发功能	支持syslog和snmp协议，syslog支持登录日志、运维日志、操作日志、命令日志等格式的上传，供外部日志采集系统使用；
API	支持系统各功能模块均可提供标准API接口调用及测试用例，供第三方平台调用；支持限定访问API接口的IP地址设置；
测试验证	中标后3天内提供投标型号的测试设备对招标要求的功能性能进行逐项测试验证，测试所产生的相关费用均由中标人承担，若无法在规定时间内提供测试设备或测试结果与招标要求不符，取消中标资格，中标人承担所有责任。
质保服务	提供原厂3年技术支持和保修服务，最终用户方为“诸暨市第五人民医院”，为保证货物是原厂家最新生产合法渠道货物，中标后提供原厂服务承诺函和原厂盖章授权函。

特别要求：乙方必须保证所有设备为原装正规渠道行货，序列号可查，所有产品均原包装到用户，当场开箱验货，同时提供该设备相关技术参数的说明。如不符合技术要求或甲方有疑问的，甲方有权要求由甲方指定的第三方提供检测报告，相关检测费用及由退货产生的一切后果由乙方承担。