招标公告

孝义市人民医院业务专网建设项目采购项目的潜在投标人应在全国公共资源交易平台（山西省-吕梁市）获取招标文件，并于 2021 年 7 月 20 日 09 点 30 分前提交投标文件。

一、项目基本情况

1．项目编号：孝政采字 2021-001 号

2．项目名称：孝义市人民医院业务专网建设项目

3．采购方式：公开招标

4．预算金额：2000000 元，其中：

第 1 包 1900000 元

第 2 包 100000 元。

5．采购需求：

本次采购项目共 2 包，其中：

（1）第 1 包为孝义市人民医院业务专网建设项目软硬件，技术参数如下：

序号	产品名称	技术参数	单位	数量
	入侵	1.要求所供设备为专业的 IPS 硬件设备，非防火墙类安全产品授权的 IPS 功能模块； 2.要求设备为标准机架式设备，1U，含交流冗余电源模块，2*USB 接口，1*RJ45 串口，2*GE 管理口，≥8*GE 接口（含 Bypass），≥3 个接口扩展槽位，≥1T 硬盘，网络层吞吐量≥12G,并发连接数≥300 万，每秒新建会话数≥10 万，含防病毒功能模块； 3.要求系统提供覆盖广泛的攻击特征库，可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测和阻断，攻击特征库数量至少为 8000 种以上； 4.要求系统支持多种抗逃避检测技术。系统应提供入侵行为特征的自定义接口，可根据用户需求定制相应的检测和阻断规则。系统应能够有效抵御 SQL 注入等多种常见的应用层安全威胁； 5.系统支持工控协议的相关漏洞攻击检测与防护，能够有效防护 Simens 等医疗工控设备的攻击； 6.要求系统提供 DoS/DDoS 攻击防护能力，支持 TCP/UDP/ICMP/ACK Flooding，以及 UDP/ICMP Smurfing 等常见的 DoS/DDoS 的攻击； 7.要求系统提供服务器异常告警功能，可以自学习服务器正常工作行为，并以此为基线检测处服务器非法外联行为； 8.要求系统提供敏感数据保护功能，能够识别、阻断通过自身的敏感数据信息（身份证号、银行卡、手机号等）；		

		9.要求系统支持监听（Monitor）、直通（Direct）两种工作模式，能够快速部署在各种网络环境中，应支持独立式多路 IPS 工作模式，各路 IPS 相互独立，可单独配置策略； 10.要求系统支持远程扫描、暴力破解、缓存区溢出、蠕虫病毒、木马后门、SQL 注入、跨站脚本等检测和防护，能够基于训练分类的协议识别； 11.要求系统支持流式和启发式防病毒功能，支持木马病毒、蠕虫病毒、宏病毒、脚本病毒等各种病毒的查杀；以及对 HTTP、FTP、POP3、SMTP 协议的病毒查杀，查杀邮件正文/附件、网页及下载文件中包含的病毒；支持 ZIP/ARJ/CAB/RAR/GZIP/BZIP2 等最多 10 层压缩文件的病毒查杀； 12.要求系统支持 IPv6/IPv4 双协议栈功能，能同时辨识 IPv4 和 IPv6 通讯流量。支持 IPv6 环境下攻击检测技术和基于 IPv6 地址格式的安全控制策略，为 IPv6 环境提供入侵防护； 13.要求系统支持 IP 碎片重组、TCP 流重组、流量状态追踪技术，基于智能、深入的协议分析，全面监测超过 100 种以上的应用层协议，能够有效检测运行在非标准端口的协议、木马，以及支持基于 Smart Tunnel 的应用协议，能够基于训练分类的协议识别； 14.要求系统支持僵尸网络防护、恶意 URL 访问防护及文件信誉防护，支持配置文件信誉检测白名单。 15.要求系统具备易用性，应提供策略模板，减少配置工作量，提高部署效率。		
2	WEB 应用防火墙	1.要求所供设备为专业的 Web 应用安全防护硬件设备，非防火墙类安全产品授权的 Web 安全防护功能模块； 2.1U，含交流单电源，2*USB 接口，1*RJ45 串口，1*RJ45 管理口，≥4*GE 电口(Bypass)，≥1 个接口扩展槽位。应用层吞吐量≥200M，事务处理能力（TPS）≥10000tps，最大并发连接数≥80000，硬盘≥1T； 3.要求系统支持透明部署，旁路部署及反向代理模式，支持牵引回注旁路部署。系统要求支持 Web 应用漏洞扫描防护、SQL 注入/XSS 防护、WEB 常规攻击防护、 URL ACL、ARP 欺骗防护、非法下载防护、非法上传防护、Web 内容安全防护、网页盗链、爬虫防护、HTTP 协议防护、扫描防护； 4.要求系统提供可配置的内置规则；且支持自定义规则，规则属性要求支持“检测方向（请求或响应）”、“检测对象、匹配操作、特征签名”等丰富要素； 5.要求支持云联动，最大程度获取暴露在互联网上的恶意 IP、僵尸网络、恶意文件特征等信息，在 WAF 上自动生成防护策略。 6.要求设备具备专业的 HTTP Flood 防护能力， WAF 可在服务器返回给客户端的数据包中，添加验证信息（包括	台	1

		httpCookie、urlCookie、ascii-image 以及 bmp-image 四种能力）。提供上述功能的配置实例； 7.要求支持 XML 防护，包括 XML 基础校验、Schema 校验以及 SOAP 校验。提供上述功能的配置实例； 8.要求支持误分析功能，提升检测精度，减少告警噪音。提供上述功能的配置实例。		
3	网闸	1.要求产品采用“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； 2.2U 机架式，内网机：≥2 个 SFP 插槽，≥6 个 10/100/1000BASE-T 接口，1 个 console 接口；2 个 USB 接口，最大可扩展至 6 个 SFP 插槽或 10 个 10/100/1000BASE-T 接口；外网机：≥2 个 SFP 插槽，≥6 个 10/100/1000BASE-T 接口，1 个 console 接口；2 个 USB 接口，最大可扩展至 6 个 SFP 插槽或 10 个 10/100/1000BASE-T 接口；吞吐量≥600 Mbps；最大并发连接数≥100,000； 3.要求带液晶屏，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，可检测上网代理、邮件代理、FTP 代理、数据库代理功能是否正常，面板可操控整机复位、关机，具有设备异常（如网络 IP 冲突、通讯异常等）监测报警功能； 4.要求必须通过内网主机系统来管理和配置网闸，必须采用硬件 USB 钥匙加密管理； 5.要求支持对文件内容智能语义分析并对包含指定内容的文件进行过滤； 5. 文件交换客户端支持扩展 windows 右键菜单发送文件、支持拖拽方式发送文件、客户端界面按钮选择文件三种方式发送文件。 6. 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，提供该功能的配置界面证明；	台	1
		1. 要求设备为标准机架式硬件，采用非 X86 多核架构。1U 机型，交流双电源，1 个 GE 管理口，≥15 个千兆电口（含 Bypass），≥8 个千兆 SFP 光口，≥4 个万兆 SFP+光口，≥1 个接口扩展槽位； 2. 防火墙吞吐量≥5G，最大并发连接数≥250 万，每秒新建连接数≥6 万。SSL VPN 并发用户≥1000；IPSec VPN 隧道数≥2000；本次提供 125 个 SSL VPN 并发用户授权，配置 IPS 功能模块； 3.支持一对一、多对一、多对多等多种形式的 NAT，实现 DNS、FTP、H.323 等多种 NAT ALG 功能。NAT 地址池支持动态探测和可用地址分配； 4.实现高性能 IPSec、L2TP、GRE VPN、SSL VPN 等功能。支持 IPsec VPN 隧道自动建立，无需流量触发； 5.支持与态势感知智能联动，设备实时上报威胁日志，当设备遭到攻		

		击，能够智能感知自动下发规则，及时拦截阻断。支持 AI 智能指纹识别，支持文件指纹识别，终端指纹识别，实现多样化的接入方式和认证策略，差异化的用户权限控制； 6.支持 Web 攻击防护功能，能够阻断 C&C 攻击、SQL 注入、XSS、http flood 等，识别黑链 URL，保障 WEB 站点可用性； 7.实现对黑客攻击、蠕虫/病毒、木马、恶意代码、间谍软件/广告软件等攻击的防御，实现缓冲区溢出、SQL 注入、IDS/IPS 逃逸等攻击的防御，实现攻击特征库的分类。可基于病毒特征进行检测，实现病毒库手动和自动升级，报文流处理模式，实现病毒日志和报表； 8.支持数据防泄露，对传输的文件和内容进行识别过滤，对内容与身份证、信用卡、银行卡、社会安全卡号等类型进行匹配； 9.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； 10.能够防范 DOS/DDOS 攻击： Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing、SYN Flood、ICMP Flood、UDP Flood、HTTP Flood（cc）攻击、ARP 欺骗、TCP 报文标志位不合法、超大 ICMP 报文、地址扫描的防范、端口扫描的防范、DNS Flood、ACK Flood、FIN Flood、分片 Flood、Tiny-Fragment； 11.支持 DDOS 攻击流量自学习功能，可设置自学习时间，自动分析并计算符合当前网络环境的 DDoS 攻击防范阈值，并自动生成 DDoS 防范策略； 12.实现对黑客攻击、蠕虫/病毒、木马、恶意代码、间谍软件/广告软件等攻击的防御，实现缓冲区溢出、SQL 注入、IDS/IPS 逃逸等攻击的防御，实现攻击特征库的分类。可基于病毒特征进行检测，实现病毒库手动和自动升级，报文流处理模式，实现病毒日志和报表； 13.支持国密 SM1/2/3/4 算法； 14.支持 SNMPv1、SNMPv2、SNMPv3、RMON 等网络管理协议，并且支持通过网管软件远程进行设备软件升级、配置等。		
		1. 要求设备为标准机架式硬件，采用非 X86 多核架构。1U 机型，交流双电源，1 个 GE 管理口，≥15 个千兆电口（含 Bypass），≥8 个千兆 SFP 光口，≥4 个万兆 SFP+光口，≥1 个接口扩展槽位； 2. 防火墙吞吐量≥5G，最大并发连接数≥250 万，每秒新建连接数≥6 万。SSL VPN 并发用户≥1000；IPSec VPN 隧道数≥2000；本次提供 125 个 SSL VPN 并发用户授权； 3.支持一对一、多对一、多对多等多种形式的 NAT，实现 DNS、FTP、H.323 等多种 NAT ALG 功能。NAT 地址池支持动态探测和可用地址分配； 4.实现高性能 IPSec、L2TP、GRE VPN、SSL VPN 等功能。支持 IPsec VPN 隧道自动建立，无需流量触发； 5.支持与态势感知智能联动，设备实时上报威胁日志，当设备遭到攻击，能够智能感知自动下发规则，及时拦截阻断。支持 AI 智能指纹		

		识别，支持文件指纹识别，终端指纹识别，实现多样化的接入方式和认证策略，差异化的用户权限控制； 6.支持 Web 攻击防护功能，能够阻断 C&C 攻击、SQL 注入、XSS、http flood 等，识别黑链 URL，保障 WEB 站点可用性； 7.实现对黑客攻击、蠕虫/病毒、木马、恶意代码、间谍软件/广告软件等攻击的防御，实现缓冲区溢出、SQL 注入、IDS/IPS 逃逸等攻击的防御，实现攻击特征库的分类。可基于病毒特征进行检测，实现病毒库手动和自动升级，报文流处理模式，实现病毒日志和报表； 8.支持数据防泄露，对传输的文件和内容进行识别过滤，对内容与身份证、信用卡、银行卡、社会安全卡号等类型进行匹配； 9.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； 10.能够防范 DOS/DDOS 攻击： Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing、SYN Flood、ICMP Flood、UDP Flood、HTTP Flood（cc）攻击、ARP 欺骗、TCP 报文标志位不合法、超大 ICMP 报文、地址扫描的防范、端口扫描的防范、DNS Flood、ACK Flood、FIN Flood、分片 Flood、Tiny-Fragment； 11.支持 DDOS 攻击流量自学习功能，可设置自学习时间，自动分析并计算符合当前网络环境的 DDoS 攻击防范阈值，并自动生成 DDoS 防范策略； 12.实现对黑客攻击、蠕虫/病毒、木马、恶意代码、间谍软件/广告软件等攻击的防御，实现缓冲区溢出、SQL 注入、IDS/IPS 逃逸等攻击的防御，实现攻击特征库的分类。可基于病毒特征进行检测，实现病毒库手动和自动升级，报文流处理模式，实现病毒日志和报表； 13.支持国密 SM1/2/3/4 算法； 14.支持 SNMPv1、SNMPv2、SNMPv3、RMON 等网络管理协议，并且支持通过网管软件远程进行设备软件升级、配置等。		
		1.要求所供设备为专业的 IPS 硬件设备，非防火墙类安全产品授权的 IPS 功能模块； 2.要求设备为标准机架式设备，1U，含交流冗余电源模块，2*USB 接口，1*RJ45 串口，2*GE 管理口，≥8*GE 接口（含 Bypass），≥2 个万兆 SFP+插槽（含万兆多模光模块），≥2 个接口扩展槽位；网络层吞吐量≥12G,并发连接数≥300 万，每秒新建会话数≥10 万； 3.要求系统提供覆盖广泛的攻击特征库，可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测和阻断，攻击特征库数量至少为 8000 种以上； 4.要求系统支持多种抗逃避检测技术。系统应提供入侵行为特征的自定义接口，可根据用户需求定制相应的检测和阻断规则。系统应能够有效抵御 SQL 注入等多种常见的应用层安全威胁； 5.系统支持工控协议的相关漏洞攻击检测与防护，能够有效防护		

		Simens 等医疗工控设备的攻击； 6.要求系统提供 DoS/DDoS 攻击防护能力，支持 TCP/UDP/ICMP/ACK Flooding，以及 UDP/ICMP Smurfing 等常见的 DoS/DDoS 的攻击。 7.要求系统提供服务器异常告警功能，可以自学习服务器正常工作行为，并以此为基线检测处服务器非法外联行为； 8.要求系统提供敏感数据保护功能，能够识别、阻断通过自身的敏感数据信息（身份证号、银行卡、手机号等）； 9.要求系统支持监听（Monitor）、直通（Direct）两种工作模式，能够快速部署在各种网络环境中，应支持独立式多路 IPS 工作模式，各路 IPS 相互独立，可单独配置策略； 10.要求系统支持远程扫描、暴力破解、缓存区溢出、蠕虫病毒、木马后门、SQL 注入、跨站脚本等检测和防护，能够基于训练分类的协议识别； 11.要求系统支持流式和启发式防病毒功能，支持木马病毒、蠕虫病毒、宏病毒、脚本病毒等各种病毒的查杀；以及对 HTTP、FTP、POP3、SMTP 协议的病毒查杀，查杀邮件正文/附件、网页及下载文件中包含的病毒；支持 ZIP/ARJ/CAB/RAR/GZIP/BZIP2 等最多 10 层压缩文件的病毒查杀； 12.要求系统支持 IPv6/IPv4 双协议栈功能，能同时辨识 IPv4 和 IPv6 通讯流量。支持 IPv6 环境下攻击检测技术和基于 IPv6 地址格式的安全控制策略，为 IPv6 环境提供入侵防护； 13.要求系统支持 IP 碎片重组、TCP 流重组、流量状态追踪技术，基于智能、深入的协议分析，全面监测超过 100 种以上的应用层协议，能够有效检测运行在非标准端口的协议、木马，以及支持基于 Smart Tunnel 的应用协议，能够基于训练分类的协议识别； 14.要求系统支持僵尸网络防护、恶意 URL 访问防护及文件信誉防护，支持配置文件信誉检测白名单； 15.要求系统具备易用性特点，应提供策略模板，减少配置工作量，提高部署效率。		
	WEB	1. 专业的 Web 应用安全防护硬件设备，非防火墙类安全产品授权的 Web 安全防护功能模块，具有完全自主知识产权的专用安全操作系统；2U,含交流冗余电源模块,2*USB 接口,1*RJ45 串口,2*GE 管理口，≥1T 硬盘，≥8 个千兆电口（4 路 Bypass），≥2 个万兆 SFP+光口，≥2 个扩展槽位。网络吞吐量≥6G，应用层吞吐量≥3G； 2. 系统要求支持透明部署，旁路部署及反向代理模式，支持牵引回注旁路部署。系统要求支持 Web 应用漏洞扫描防护、SQL 注入/XSS 防护、WEB 常规攻击防护、 URL ACL、ARP 欺骗防护、非法下载防护、非法上传防护、Web 内容安全防护、网页盗链、爬虫防护、HTTP 协议防护、扫描防护； 3. 系统提供可配置的内置规则；且支持自定义规则，规则属性要求支		

		持“检测方向（请求或响应）”、“检测对象、匹配操作、特征签名等丰富要素； 4. 系统可支持与 SaaS 扫描服务联动，在 WAF 上获取专家级、个性化的 WEB 漏洞扫描报告，并转化为 WAF 可执行的、有针对性的 WEB 安全防护策略。 5. 支持与威胁情报中心进行联动，实时获取最新的高危 IP 信誉库，在 WAF 上自动生成防护策略； 6. 要求设备具备专业的 HTTP Flood 防护能力， WAF 可在服务器返回给客户端的数据包中，添加验证信息（包括 httpCookie、urlCookie、ascii-image 以及 bmp-image 四种能力）； 7. 支持 XML 防护，包括 XML 基础校验、Schema 校验以及 SOAP 校验； 8. 支持误分析功能，提升检测精度，减少告警噪音。		
8	数据库审计系统	1.2U，含交流冗余电源模块，2*USB 接口，1*RJ45 串口，1*GE 管理口，≥6*GE 电口，≥1 个接口扩展槽位，≥2T SATA 硬盘。在线日志量 8 亿条以上，归档日志量 20 亿条以上，纯数据库网络吞吐量不低于 200Mbit/秒，并发会话数不小于 1000，SQL 处理性能不少于 10000 条/秒； 2. 支持数据库自动发现。设备无需添加、即插即用。支持主流数据库：Oracle、SQL Server、MySQL、DB2、PostgreSQL、sybase、Informix。会话的终端信息：IP、MAC、Port、工具名称（程序名）；会话的主机信息、IP、MAC、Port、数据库名（实例名）；会话的其它信息：登录时间、会话时长。提供该功能的配置界面证明； 3. 部署方式灵活，支持旁路部署、代理部署、分布式部署、虚拟化部署等。旁路部署模式下无须在被审计数据库系统上安装任何代理即可实现审计，数据单向流出，对应用系统无任何影响。支持在目标数据库安装 Agent 解决无法通过旁路镜像获取流量的场景，如同服务器部署数据库和应用系统、云环境、虚拟化环境场景下数据库的审计； 4. 审计要素：操作类型（DDL、DML、DCL 等）、操作时间、执行时长、操作成功与失败、操作对象（表、函数、存储过程名称）、SQL 语句。操作影响范围信息：查询、修改、删除操作的影响行数,以及返回行数； 5. 复杂 SQL 语句支持：准确审计长 SQL 语句；有效分割、准确审计多 SQL 语句；准确审计绑定变量的 SQL 语句。提供该功能的配置界面证明； 6. 数据库漏洞攻击监测：能对基于数据库漏洞进行攻击行为监测和告警，具备数据库漏洞攻击规则库； 7. SQL 注入检测：通过模式匹配的方式对 SQL 访问进行监测与告警,判断是否为可疑 SQL 注入；提供 SQL 注入特征库；	台	1

		8. 可疑行为识别：批量数据导出：对超过特定行数阀值的批量数据导出行为； 9. 高危操作：对超过特定行数阀值的批量数据修改、删除，或全表 Update、Delete 行为等新型语句的识别、SQL 注入行为的识别； 10. 基于数据库设置，从优先级和规则类别两个层面创建并查询审计规则。根据风险忽略、高风险、中风险、低风险四个层级逐级命中规则。风险操作支持多条规则逻辑关联，根据排列顺序区分优先级； 11. 支持 SQL 注入监测：根据 IP，sql 特征和正则表达式自定义 SQL 注入，支持数据库漏洞监测和审计语句统一管理； 12. 支持敏感语句告警策略。（黑白名单效果）；自定义添加敏感语句和信任语句（黑白名单效果）；根据风险操作、SQL 注入、漏洞攻击检测、语句管理等模块定义告警规则；支持高、中、低风险告警。支持系统资源监控与告警。根据不同的安全级别采用不同的响应方式，包括记录、告警；告警方式包括：邮件、短信、SYSLOG、SNMP； 13. 风险分析：根据敏感语句、sql 注入、漏洞攻击、风险操作等维度以时间维度统计数据库分析信息。语句分析：基于 SQL 语句的操作类型统计，支持失败 sql 统计、Top sql 统计；支持针对新型语句、语句审计模板检索。		
9	日志审计系统	1. 1U 标准式机架，交流冗余双电源，专用硬件平台和安全操作系统。1 个 RJ45 串口，2GE 管理口，≥4 个千兆电口，1CF 卡，支持多端口采集，≥3 个接口扩展槽位。1 块 4TB 硬盘，授权接入 140 个日志源，支持扩展；单台日志处理性能不低于 3000EPS。10 亿背景数据指定字段查询最快可在 5 秒内响应； 2.系统应基于大数据平台架构，具备海量数据收集与快速检索能力；系统应支持内置采集器，不依赖其他设备即可进行日志采集。提供该功能的配置界面证明； 3.系统支持的数据采集范围包括但不限于网络安全设备、交换设备、路由设备、操作系统、应用系统等； 4.系统支持的数据采集方式包括但不限于 SYSLOG、SNMP Trap、FTP、SFTP、JDBC、ODBC、Net flow、专用 Agent 等方式采集日志； 5.系统应支持手工注册资产，支持对资产进行修改/删除、批量导入/导出/添加/修改/删除等多种方式的管理。提供上述功能的配置实例； 6.系统应支持按类型、按日期(天)，手动、自动备份日志； 7.系统应支持设置日志存储备份策略，可设置备份周期、备份日志类型等；系统应支持日志备份远程服务器，如传送到 FTP 服务器； 8.系统应支持正则、KV、格式串等多种灵活的提取日志方式。提供上述功能的配置实例； 9.系统能够采集、保存原始日志数据，支持 NFS 网络文件共享方式扩展日志存储空间，保存时间至少半年；能够实现海量日志数据快速查	台	1

		询；系统必须具备日志范式化功能，实现对日志格式的统一化。		
10	堡垒机	1、标准机架式设备，2U，含交流冗余电源模块，2*USB 接口，1*RJ45 串口，1*GE 管理口，≥6*GE 电口，≥1 个接口扩展槽位，≥2T SATA 硬盘，授权管理≥300 台设备。字符会话并发数不少于 250 个，图形会话并发数不少于 500 个； 2、主帐号登录堡垒机应支持本地静态密码认证、LDAP 认证、RADIUS 认证、证书认证等身份认证方式。标配 OTP 动态令牌或手机令牌的认证方式，组合口令认证，实现双因子强身份鉴别，满足等保合规双因子身份鉴别要求。提供该功能的配置界面证明； 3、支持半自动登录目标设备：即第一次登录目标设备时运维人员需手工输入目标设备帐号和密码并允许堡垒机保存该帐号密码，运维人员在后期登录时即可实现自动登录目标设备。支持密钥登录方式：在登录目标服务器时，使用的是秘钥登录，而非密码。在既可以使用密码，又可以使用秘钥的环境，可以自由选择登录认证方式； 4、要求支持幽灵账号功能。支持主动对从账号进行关联分析，当发现攻击者植入的异常账号时，对相关管理员采取告警、记录及通知等操作； 5、要求支持闲置账号功能。能够提供对各从账号的运维使用率的分析功能，当发现使用率异常的从账号，对相关管理员采取告警、记录及通知等操作。提供上述功能的配置实例； 6、具备工单系统，支持运维工单流程，运维人员审批可提前申请工单，审批人员审批自由度大幅提高，不再受审批时间限制，解放运维人员和审批人员，提高工作效率； 7.为方便远程安全管理，满足等级保护身份认证及会话安全相关要求。运维审计系统支持和防火墙实现二合一单点登录。远程运维环境下通过防火墙 VPN 登录内网时只需输入运维审计系统账号即可直接快速登录到运维审计系统运维设备，无需输入 VPN 账号，再输入运维审计系统账号才可运维。提供该功能的配置界面证明。	台	1
		1.标准机架式设备，2U，含交流冗余电源，1*RJ45 串口，1*GE 管理口，≥6*GE 扫描口，≥4 个千兆 SFP 插槽，授权可扫描总数量不多于 512 个无限制范围的 IP 地址或域名； 2. 要求支持系统漏洞、网站安全漏洞整体态势的图表统计展示模式；支持漏洞整体态势分布的地图展示模式；可以通过参数配置切换展示模式。支持仪表盘展示，包括资产仪表盘、主机风险仪表盘、网站风险仪表盘、漏洞处置仪表盘、安全事件仪表盘； 3. 要求所提供产品支持检测的漏洞数大于 160000 条，兼容 CVE、CNCVE、CNNVD、CNVD、Bugtraq 等主流标准； 4. 支持总体漏洞分布态势展示，支持风险等级、风险评分、发现漏洞数量最多的系统和应用类型 TOP10、周和月度漏洞数量趋势、漏洞处置情况统计等；		

		5.要求系统内置针对 Unix、Windows 操作系统、网络设备和防火墙等不同的漏洞模板，同时支持自定义扫描范围和扫描策略；支持自动模板匹配； 6.为了满足国产化自主可控需求，要求产品支持扫描国产操作系统、应用及软件的安全漏洞； 7.要求产品支持扫描主流虚拟机管理系统的安全漏洞，包括 VMWareESX/ESXi 等，要求能够扫描大于 5000 条相关漏洞； 8.支持资产持续监控，发现资产新增、变更、减少的变化，给出资产稽查报告。支持资产稽查结果统计信息，支持资产稽查结果列表信息，支持资产变更的详细对比； 9.提供系统快照功能，当系统出现问题时，可以通过恢复快照，一次性将系统恢复到快照时的版本，并将用户数据一同恢复； 10.具备单独口令猜测扫描任务，支持多种口令猜测方式，包括利用 SMB、TELNET、FTP、SSH、POP3、TOMCAT、SQL SERVER、MYSQL、ORACLE、SYBASE、DB2、SNMP 等协议进行口令猜测，允许外挂用户提供的用户名字典、密码字典和用户名密码组合字典。		
		1.标准机架式 2U 设备，含交流冗余电源模块，≥2*CPU（10 核），≥128G 内存，≥256G SSD 系统盘，≥4*10TB SATA 硬盘，≥6 个千兆电口，≥3 个接口扩展槽位，接入能力≥2000EPS； 2.系统应基于大数据平台架构，具备海量数据收集与快速检索能力；系统应支持内置采集器，不依赖其他设备即可进行日志采集； 3.系统应支持手工注册资产，支持对资产进行修改/删除、批量导入/导出/添加/修改/删除等多种方式的管理； 4.系统应支持正则、KV、格式串等多种灵活的提取日志方式，便于实施，不需要更改 XML 配置文件或定制开发； 5.能够采集、保存原始日志数据，支持 NFS 网络文件共享方式扩展日志存储空间，保存时间至少半年；能够实现海量日志数据快速查询；系统必须具备日志范式化功能，实现对日志格式的统一化； 6.支持全网业务可视化，可以呈现全网业务对象的访问关系与被入侵业务的图形化展示。支持用户自定义的业务资产管理的可视化； 7.支持对安全事件信息的统一收集、分析和展示；可在产品界面直观展示单位关注安全事件，例如网络入侵情况、木马蠕虫传播情况、僵尸网络情况等； 8.具有强大的兼容性，可通过半自动化的页面，将监测数据传输到其他平台，传输数据可通过可视化界面自定义编辑；数据采集系统监听的风险数据需通过 TCP 协议传输到监测平台，采用多个 TCP 可靠接口传输数据，提供该功能的配置界面证明； 9.支持展示攻击链模型及每级事件关联的目标 IP 数;攻击链事件的时间范围随地图的时间控件变化。提供该功能的配置界面证明；		

		10.攻击链查询支持按时间段（必选）、IP 范围，按地域，按资产组等查询； 11.支持直观地展示攻击的情况。可以对地图进行下钻，查看对应地域的攻击和被攻击 top5 ip 的情况，支持地图动态联动； 12.支持按攻击链的各个阶段进行主机失陷分析，失陷主机呈现内容包括：已失陷主机/高可疑主机/低可疑主机统计（过滤主机风险列表），攻击链分布，失陷主机分布趋势，攻击者 TOP5（下钻攻击者视角），受害者 TOP5（下钻受害者视角），主机风险列表（下钻主机失陷详情页面）； 13.支持与本次采购的漏洞扫描服务进行数据对接，支持在平台上对进行漏扫服务时下发系统扫描、网站扫描、网站收集的扫描任务。 14.对高危用户进行可视化展示，对高危用户的风险操作，攻击行为，违规行为，影响业务进行可视化展现，并按确定性分类为失陷用户，高危用户，可疑用户。提供该功能的配置界面证明； 15.具有安全事件处置管理能力，方式包括但不限于：事件处置、事件审批、事件归档等，提供该功能的配置界面证明； 16.支持基于规则的安全事件关联分析的能力，能够对不同的事件进行相关性分析，发掘潜在的信息，能够全面展现网络安全态势情况、动态提醒当前网络最新的安全威胁； 17.通以多维度资产管理，支持多维度资产分析视图，系统至少支持三种视图：地理视图、业务视图、组织架构视图。通过可视化图形展示当前网内资产安全概况，提供基于风险、脆弱性、威胁、资产、工单、情报预警、运维监控等仪表盘展示； 18.支持资产持续监控，发现资产新增、变更、减少的变化，给出资产稽查报告。支持资产稽查结果统计信息，支持资产稽查结果列表信息，支持资产变更的详细对比； 19.支持针对事件源/目的进行威胁情报追溯，依据情报显示的 IP 黑名单、高危漏洞数、关联域名威胁等级及关联恶意样本，确定事件的风险等级；支持追溯情报下钻呈现； 20.具有实时事件关联分析引擎，支持能力包括：采用 FLINK 技术框架。在性能上要求，事件分析上报不晚于事件发生的 5 分钟内； 21.支持大屏投放要求及分辨率兼容要求，且易于操作，展现形式多样，画面丰富，并且能够以地图、柱状图、饼状图等多种图形化方式展现网络安全态势情况，动态提醒当前网络最新的安全威胁； 22.通过访问关系学习展示用户、业务系统、网络大区之间访问关系，能够识别访问关系的 who,what,when,how；		
		1.业务插槽数≥3，为了便于扩容，需支持单块板卡包含 24 电口+20 个千兆光口+4 个万兆光口； 2.交换容量≥64Tbps, 转发能力≥22000Mpps； 3.支持主控引擎模块≥2，满足 1+1 冗余； 4.支持跨设备链路聚合，支持对广播、组播、单播报文的均匀分担，		

		聚合组数≥128 组，每组成员≥8 个； 5.支持双向 ACL，支持标准和扩展 ACL，支持 VLAN ACL； 6.支持静态路由，支持 RIPv1/v2，支持 OSPFv2，支持 IS-IS，支持 BGPv4； 7.支持双引擎快速倒换，主备切换时候板内转发无丢包 ，支持 NSF/GR for OSFP/BGP/IS-IS，支持热补丁功能，可在线进行补丁升级，支持 BFD，BFD for VRRP/BGP/IS-IS/OSPF/RSVP/LDP/RIP/静态路由； 8.支持多虚一技术(N:1)； 9.支持 OPENFLOW 1.3；支持普通模式和 Openflow 模式切换；支持多控制器（EQUAL 模式、主备模式）；支持多表流水线；支持 Group table；支持 Meter； 10.支持 IEEE 802.1ae 介质访问控制安全技术； 11.实配双主控，双电源，千兆电口≥24 个，千兆光口≥24 个，万兆光口≥8 个。		
14	汇聚交换机	1.交换容量≥590Gbps，包转发率≥220Mpps； 2.千兆电口≥24 个，万兆光口≥4 个； 3.实现 CPU 保护功能，能限制非法报文对 CPU 的攻击，保护交换机在各种环境下稳定工作； 4.支持跨设备链路聚合，单一 IP 管理，分布式弹性路由；支持通过标准以太端口进行堆叠；支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预； 5.支持基于端口的 VLAN，支持基于协议的 VLAN；支持基于 MAC 的 VLAN； 6.支持 IGMP Snooping v1/v2/v3，MLD Snooping v1/v2，支持 PIM Snooping，支持 PIM-DM，PIM-SM，PIM-SSM； 7.支持 IPv4/IPv6 静态路由，支持 RIP/RIPng，OSPFV1/V2/V3； 8.支持 RRPP（快速环网保护协议）、支持 Smartlink、支持 RSTP 功能、支持 MSTP 功能、支持 MSTP 功能； 9.支持 DHCP Client，支持 DHCP Snooping，支持 DHCP Relay，支持 DHCP Server，支持 DHCP Option82； 10.支持过流保护、过压保护和过热保护技术；支持电源和风扇的故障检测及告警； 11.支持云管理平台，无需自己搭建专业的管理服务器和软件，即可享用专业的网络管理和运维服务。提供该功能的配置界面证明。	台	2
		1.交换容量≥330Gbps，包转发率≥100Mpps； 2.千兆电口≥24 个，万兆光口≥4 个； 3.支持横向虚拟化，支持跨设备链路聚合，单一 IP 管理，分布式弹性路由；支持通过标准以太端口进行堆叠；支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预； 4.支持纵向虚拟化，将接入设备作为远程接口板加入主设备系统，在		

		纵向维度上将核心层设备和接入层设备虚拟为一台逻辑设备，实现简化管理，；简化网络层级，实现数据转发平面虚拟化，提供官网截图及链接； 5.支持基于端口的 VLAN，支持基于协议的 VLAN；支持基于 MAC 的 VLAN； 6.支持 DHCP client，DHCP Snooping，DHCP Snooping trust，DHCP Snooping option 82，DHCP Server； 7.支持 IPv4 静态路由、RIP V1/V2； 8.支持 RRPP（快速环网保护协议）、支持 RSTP 功能、支持 RSTP 功能、支持 MSTP 功能； 9.支持免费云平台管理，远程管理，提供官网截图及链接。		
16	网络监控平台	1.监控平台采用 B/S 架构，系统平台和管理对象模块分离；采用 JAVA+HTML5 开发；从数据安全及系统维护成本考虑，要求系统自带数据库并对数据做加密处理； 2.提供以周维度的健康状态视图，提供趋势管理能力，在一张图上列出问题最多的设备和指标、关键指标环比变化最大的线路和主机等信息； 3. 支持自动数据基线运维能力，根据自动采集的数据形成基线，不能以人工导入或者手工绘制方式实现，基线能按照用户要求随时重构； 4. 要求支持不少于 10 个并发用户同时登录系统并进行操作； 5.要求支持基于智维规则、手工触发方式调用分析策略的方式，实现异常事件的自动分析；提供对于异常指标进行及时提醒，并可给出指标意义、指标影响和常规处置建议；支持对高频告警信息的主动信息收集纳入告警处置经验，实现处置经验的主动收集； 6.本次项目节点授权数量：100 个（包含网络设备、安全设备、主机操作系统等）； 7.系统能支持各大设备厂商的各型号设备，支持多厂商设备组成的混合网络自动发现，提供端口关闭与启用操作，可以更改 VLAN ID；拓扑图的生成必须支持网络设备的 SNMP V1、V2、V3 这三个版本的混和生成，并能对 SNMP V3 设备进行管理； 8.要求系统提供配置模板。管理对象一旦添加，即可自动适配相关智维规则、告警规则、报表规则等，无需人工参与配置；系统能提供业务基线。支持自动学习被管对象业务运行规律，自动形成业务基准基线、高负载基线和低负载基线。设备运行一旦偏离高/低负载基线后即可进行异常提示； 9. 系统支持拓扑图自动布局，网络设备可实现星型排布、圆型排布、从上到下树形排布、从左到右树形排布多种自动排布方式；拓扑图设备间的连线除直线形式外，还可支持以折线、合并线等线型，并可将网络拓扑按照线路图、地域分布图、逻辑关系图等方式呈现； 10. 系统支持对于 Windows、HP	套	1

		unix、Aix、Solaris、linux（redhat、CentOS、Suse（oracle）、Redflag）类型操作系统的管理，支持对于 CPU、内存、进程、日志、网络流量、磁盘性能的监控；提供该功能的配置界面证明； 11. 支持系统拓扑图，一张图可以展现所有主机承载的数据库、中间件和标准应用之间的实时状态监控，为主机监控提供全景视图。		
17	动环检测平台	1.千兆以太网口数≥4 个；并需提供 1 个 RJ-45 Console 管理口； 提供 USB 接口数≥2，用于外接硬件设备进行管理； 2.支持对接市电监测模块、三相电量仪、UPS、蓄电池、柴油发电机等动力系统，实现对机房动力系统的实时监测； 3.支持易部署上线，可以通过导航式部署快速上线传感器设备； 4.支持接入门禁、门磁、烟雾传感器、视频等，实现对机房安全状态的实时监测； 5.支持多种告警模式，包括电话告警、短信告警、声光告警、APP 告警、WEB 告警、阿里钉钉、微信告警，提供该功能的配置界面证明； 6.支持用电安全系统、空间节能系统、环境系统、消防系统、动力系统、安防系统，可同一平台直接添加所需子系统； 7.平台内置传感器库支持≥1000 种的传感器，能够支持对接主流的 UPS、精密空调及其他的各类监测/控制型传感器设备，满足机房设施管理的高可用性； 8.支持巡检策略设定，记录并存储巡检报告，比如平台定时对全部设备进行巡检，及时发现异常设备，消除隐患； 9.支持大屏展示，向管理人员展示整体机房整体运行状态，包括场景设备应用情况、用电安全、电力系统、温湿度情况、告警情况等信息，数据通过友好的大屏直观呈现展示，实现管理可视化。提供软件平台功能截图界面证明； 10.支持远端云守护功能，告警信息一段时间未处理，系统自动将告警信息发送到远端云平台，由厂商值守人员第一时间通知到运维人员； 11.提供一台 24 口 POE 交换机，交换机需支持二层广播自动发现控制器平台、配置静态 IP 地址三层发现控制器平台，DHCP 、Option43 方式发现控制器平台、DNS 域名发现控制器平台，且支持通过网管平台跨广域网、NAT 远程管理智能交换机。	套	1
18	监视器	显示尺寸：55″，背光类型：LED，物理分辨率：3840x2160； 亮度不低于 350cd/m2，对比度不低于 1200:1。视频输入端口支持：HDMI、VGA； 具备透雾增强、低照度增强功能、图像边缘修复技术及智能防灼屏技术； 水平可视角度 178°，垂直可视角度 178°； 工业级面板，适合 7*24 小时连续工作； 画面快速响应，真正无拖尾； 支持多种信号输入。	台	2

19	系统集成服务	1.资产梳理，对全院网络资产进行梳理，包括网络设备、安全设备、服务网、数据库等； 2.网络结构调整，根据分区分域的原则，按照等保2.0“一个中心三重防护”的要求，对网络结构进行调整，并配置相应安全防护策略； 3.配合对全院应用系统进行安全防护，且保证系统业务连续性； 4.对线路进行整理，整理后统一打标签； 5.配合完成对全院IP地址重新规划、更改、测试等工作； 6.提供并安装电子门禁、视频监控系统； 7.配合等保测评。	项	1
20	辅材	包括光纤、光模块、网线、机柜等	批	1

第一包采用综合评分法，评分细则如下：

技术部分：

排序	分值	评审内容	评审标准
1	10	整体设计方案	技术方案总体结构合理，架构编排得当，各章节主题阐述清晰，各部分技术设计详细，整体方案论述完整、准确、实用、可行，框架设计标准高，能体现较强的前瞻性、实用性、可扩展性，根据优秀程度，分出好、一般、差、未响应四个档次，分别得10 分、7 分、4分、0分；
2	5	设备安装调试与系统集成方案一	设备安装调试方案合理可行，针对项目的协调措施、技术难点解决方案等几个方面，应有具体落实措施和割接方案，确保医院业务系统稳定运行，根据优秀程度，分出好、一般、差、未响应四个档次，分别得5 分、4 分、3分、0分；
3	3	设备安装调试与系统集成方案二	对本项目的进度计划设置科学、合理，且满足项目建设进度需要，根据优秀程度，分出好、一般、差、未响应四个档次，分别得3 分、2分、1分、0分；
4	1	节能产品	货物（方案）中有最新公布的《节能产品政府采购品目清单》中强制采购产品以外的其他节能产品，每提供一项得0.2分，最高得1分。
5	1	环境标志产品	货物（方案）中有最新公布的《环境标志产品政府采购品目清单》中产品的，每提供一项得0.2分，最高得1分。
6	1	硬件设备技术参数及技术指标一	所供漏洞扫描设备（第11项）支持自定义风险值计算标准配置，可对主机风险等级评定标准和网络风险等级评定标准进行自定义。满足得1分，不满足不得分。
7	2	硬件设备技术参数及技术指标二	所供WEB应用防火墙（第2项、第7项）支持会话追踪功能。通过浏览器标识和会话标识实现对会话的跟踪，记录完整的黑客攻击过程，做到场景复现。满足得2分，不满足不得分。
8	2	硬件设备技术参数及技术指标三	所供入侵防护系统（第1项、第6项）支持基于SCADA、IEC 61850、IEC 60870-104等协议的相关漏洞攻击检测与防护。满足得2分，不满足不

			得分。
9	2	硬件设备技术参数及技术指标四	漏洞扫描、防火墙、入侵防御、WEB 应用防火墙厂商具备 CNNVD（中国国家信息安全漏洞库）支撑单位资质，满足得 2 分；
10	1	硬件设备技术参数及技术指标五	漏洞扫描、防火墙、入侵防御、WEB 应用防火墙厂商管理体系符合 ISO/IEC 20000-1：2011 标准，满足得 1 分；
11	1	硬件设备技术参数及技术指标六	漏洞扫描、防火墙、入侵防御、WEB 应用防火墙厂商管理体系符合 ISO/IEC27001：2013 标准，满足得 1 分。
12	1	硬件设备技术参数及技术指标七	所供日志审计系统（第 9 项）设备具备中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书》，并获得 EAL3+级别及以上，满足得 1 分，不满足不得分。
13	2	硬件设备技术参数及技术指标八	所供态势感知平台（第 12 项）设备具备中国信息安全测评中心颁发的《国家信息安全漏洞库兼容性资质证书》、《国家信息安全测评信息技术产品安全测评证书》（EAL3+级别及以上），每提供一项得 1 分，最高得 2 分。
14	1	硬件设备技术参数及技术指标一	所供态势感知平台（第 12 项）厂商的安全开发能力获得国家权威机构认可，具备中国信息安全测评中心颁发的信息安全服务（安全开发类二级）资质，满足得 1 分，不满足不得分。
15	1	硬件设备技术参数及技术指标二	所供堡垒机（第 10 项）设备具备中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书》并获得 EAL3+以上级别，得 1 分，不提供者不得分。
16	1	现场演示一，投标人可现场搭建环境演示或远程搭建环境登录演示（不接受 PPT、视频等方式），演示内容符合功能参数要求，方可得分。 每个投标人的现场演示总时长为 30 分钟（含专家询问及投标人澄清所用时间），超时未完成的演示项目不得分。	入侵防护系统第 5 条：“系统支持工控协议的相关漏洞攻击检测与防护，能够有效防护 Simens 等医疗工控设备的攻击”；演示成功得 1 分，演示不成功或不演示不得分。
17	1	现场演示二，投标人可现场搭建环境演示或远程搭建环境登录演示（不接受 PPT、视频等方式），演示内容符合功能参数要求，方可得分。 每个投标人的现场演示总时长为 30 分钟（含专家询问及投标人澄清	WEB 应用防火墙第 6 条：“要求设备具备专业的 HTTP Flood 防护能力， WAF 可在服务器返回给客户端的数据包中，添加验证信息（包括 httpCookie、urlCookie、ascii-image 以及 bmp-image 四种能力）”；演示成功得 1 分，演示不成功或不演示不得分。

		所用时间），超时未完成的演示项目不得分。	
18	1	现场演示三，投标人可现场搭建环境演示或远程搭建环境登录演示（不接受 PPT、视频等方式），演示内容符合功能参数要求，方可得分。 每个投标人的现场演示总时长为 30 分钟（含专家询问及投标人澄清所用时间），超时未完成的演示项目不得分。	WEB 应用防火墙第 7 条：“支持 XML 防护，包括 XML 基础校验、Schema 校验以及 SOAP 校验”；演示成功得 1 分，演示不成功或不演示不得分。
19	1	现场演示四，投标人可现场搭建环境演示或远程搭建环境登录演示（不接受 PPT、视频等方式），演示内容符合功能参数要求，方可得分。 每个投标人的现场演示总时长为 30 分钟（含专家询问及投标人澄清所用时间），超时未完成的演示项目不得分。	WEB 应用防火墙第 8 条：“支持误分析功能，提升检测精度，减少告警噪音”；演示成功得 1 分，演示不成功或不演示不得分。
20	1	现场演示五，投标人可现场搭建环境演示或远程搭建环境登录演示（不接受 PPT、视频等方式），演示内容符合功能参数要求，方可得分。 每个投标人的现场演示总时长为 30 分钟（含专家询问及投标人澄清所用时间），超时未完成的演示项目不得分。	防火墙第 8 条：“支持数据防泄露，对传输的文件和内容进行识别过滤，对内容与身份证、信用卡、银行卡、社会安全卡号等类型进行匹配”；演示成功得 1 分，演示不成功或不演示不得分。
21	1	现场演示六，投标人可现场搭建环境演示或远程搭建环境登录演示（不接受 PPT、视频等方式），演示内容符合功能参数要求，方可得分。 每个投标人的现场演示总时长为 30 分钟（含专家询问及投标人澄清所用时间），超时未完	漏洞扫描第 7 条：“要求产品支持扫描主流虚拟机管理系统的安全漏洞，包括 VMWareESX/ESXi 等，要求能够扫描大于 5000 条相关漏洞”；演示成功得 1 分，演示不成功或不演示不得分。

		成的演示项目不得分。	
22	1	现场演示七，投标人可现场搭建环境演示或远程搭建环境登录演示（不接受 PPT、视频等方式），演示内容符合功能参数要求，方可得分。 每个投标人的现场演示总时长为 30 分钟（含专家询问及投标人澄清所用时间），超时未完成的演示项目不得分。	漏洞扫描第 9 条：“提供系统快照功能，当系统出现问题时，可以通过恢复快照，一次性将系统恢复到快照时的版本，并将用户数据一同恢复”；演示成功得 1 分，演示不成功或不演示不得分。
23	1	现场演示八，投标人可现场搭建环境演示或远程搭建环境登录演示（不接受 PPT、视频等方式），演示内容符合功能参数要求，方可得分。 每个投标人的现场演示总时长为 30 分钟（含专家询问及投标人澄清所用时间），超时未完成的演示项目不得分。	网络监控平台第 9 条：“系统支持拓扑图自动布局，网络设备可实现星型排布、圆型排布、从上到下树形排布、从左到右树形排布多种自动排布方式；拓扑图设备间的连线除直线形式外，还可支持以折线、合并线等线型，并可将网络拓扑按照线路图、地域分布图、逻辑关系图等方式呈现”；演示成功得 1 分，演示不成功或不演示不得分。
24	1	现场演示九，投标人可现场搭建环境演示或远程搭建环境登录演示（不接受 PPT、视频等方式），演示内容符合功能参数要求，方可得分。 每个投标人的现场演示总时长为 30 分钟（含专家询问及投标人澄清所用时间），超时未完成的演示项目不得分。	网络监控平台第 11 条：“支持系统拓扑图，一张图可以展现所有主机承载的数据库、中间件和标准应用之间的实时状态监控，为主机监控提供全景视图”；演示成功得 1 分，演示不成功或不演示不得分。
25	1	现场演示十，投标人可现场搭建环境演示或远程搭建环境登录演示（不接受 PPT、视频等方式），演示内容符合功能参数要求，方可得分。 每个投标人的现场演示总时长为 30 分钟（含专家询问及投标人澄清所用时间），超时未完成的演示项目不得分。	动环监控系统第 10 条：“支持远端云守护功能，告警信息一段时间未处理，系统自动将告警信息发送到远端云平台，由厂商值守人员第一时间通知到运维人员”。演示成功得 1 分，演示不成功或不演示不得分。

合计	44		

商务部分：

排序	分值	评审内容	评审标准
26	6	近 3 年类似业绩	合同案例是指在投标截止日期前三个年度内投标人与最终用户签订的合同，并且是网络安全产品类合同，要求必须提供与用户签订的合同首页、合同金额所在页、签字盖章页和发票扫描件作为证明。每提供一份符合认定标准的完整业绩得 2 分，最高得 6 分。（注：若经查验与投标文件要求不符，不计入得分。）
合计	6		

服务部分：

排序	分值	评审内容	评审标准
27	1	人力资源保障一	有且准确提供本项目售后服务总负责人的姓名、职务、详细的地址和联系方式的得 1 分，否则不得分；
28	3	人力资源保障二	项目负责人（须提供个人社保证明）具有中国信息安全测评中心颁发的注册信息安全工程师（CISP）证书，得 3 分，不提供者不得分。
29	8	服务保障	售后服务方案合理、措施得力，写明售后服务响应方式、售后服务的保障内容等，根据服务保障方案的优秀程度，分出好、一般、差、未响应四个档次，分别得 8 分、6 分、4 分、0 分；
30	8	培训	对培训内容、培训方案、培训团队构成、培训计划进行评价比较，根据优秀程度，分出好、一般、差、未响应四个档次，分别得 8 分、6 分、4 分、0 分
合计	20		

报价部分：

价格分统一采用低价优先法，即满足招标文件要求且最后价格最低的供应商的价格为评标基准价，其价格分为满分 30 分。其他投标供应商的价格分统一按照下列公式计算：

投标报价得分＝（评标基准价/投标报价）×30%×100

（2）第 2 包为孝义市人民医院业务专网建设项目测评服务，要求对孝义市人民医院 HIS 系统，依据《信息安全技术　　网络安全等级保护基本要求》（GB/T　　22239—2019）中第三级系统的要求，从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全人员管理、安全建设管理、安全运维管理层面开展测评工作，并出具相应的信息系统安全等级测评报告。采购范围以本招标文件中商务、技术和服务的相应规定为准。第 2 包采用经评审最低价法。

6．合同履行期限：

第 1 包：合同签订后 1 个月内全部供货安装完毕。

第 2 包：合同自签署之日起，有效期一年。

7．本项目（是/否）接受联合体：否

二、参与投标的供应商应具备的资格条件

1．满足《中华人民共和国政府采购法》第二十二条规定：

（一）具有独立承担民事责任的能力；

（二）具有良好的商业信誉和健全的财务会计制度；

（三）具有履行合同所必需的设备和专业技术能力；

（四）有依法缴纳税收和社会保障资金的良好记录；

（五）参加政府采购活动前三年内，在经营活动中没有重大违法记录；

（六）法律、行政法规规定的其他条件。

2．落实政府采购政策需满足的资格要求：无

3．本项目的特定资格要求：

第 1 包：无

第 2 包：投标人须在《全国网络安全等级保护测评机构推荐目录》内，具有国家网络安全等级保护工作协调小组办公室颁发的《网络安全等级保护测评机构推荐证书》。

三、电子投标须知

1．本项目采用电子投标方式，获取招标文件、提交投标文件，需提前在全国公共资源交易平台（山西省-吕梁市）主体库注册，并办理 CA 数字证书。

全国公共资源交易平台（山西省-吕梁市）网址：

http://www.llsggzyjyzx.cn/

主体库注册网址：

http://124.165.206.19:25006/register_directions.jspx

山西省公共资源 CA 交叉互认平台网址：

http://218.26.178.22:8011/dcjchr/index.html

在吕梁以外地区办理的 CA 数字证书须提前联系吕梁市公共资源交易中心技术人员进行激活后方可使用。

吕梁市公共资源交易中心技术支持电话：

0358-8487004、0358-8487010

2．供应商注册主体库、报名参加采购项目、下载获取招标文件、制作投标文件、加密投标文件及提交投标文件时，应严格遵守《吕梁市公共资源系统用户手册》等规范。

吕梁市公共资源电子交易平台教程网址：

http://124.165.206.19:25006/downCl.jspx

四、获取招标文件

1．获取时间：2021 年 6 月 28 日 00 时 00 分至 2021 年 7 月 9 日 00 时 00 分

2．获取方式：在获取招标文件截止时间前，登录全国公共资源交易平台（山西省-吕梁市）免费下载，此为获取招标文件的唯一途径。

3．获取网址：

http://www.llsggzyjyzx.cn/

http://124.165.206.19:25006/login.jspx

五、提交投标文件

1．截止时间：2021 年 7 月 20 日 9 点 30 分（自招标文件开始发出之日起至投标人提交投标文件截止之日止，不得少于 20 日）

2．提交方式：登录全国公共资源交易平台（山西省-吕梁市）上传

3．提交要求：所提交的投标文件须进行加密，到截止时间未按时提交投标文件的供应商按自动放弃投标处理。

4．提交网址：

http://www.llsggzyjyzx.cn/

http://124.165.206.19:25006/login.jspx

六、签到、开标及投标文件解密

1．签到时间：2021 年 7 月 20 日 9 点 00 分至 9 点 30 分

2．开标时间：2021 年 7 月 20 日 9 点 30 分

3．投标文件解密时间：2021 年 7 月 20 日 9 点 30 分至 10 点 00 分

4．签到地点、开标地点、投标文件解密地点：孝义市市民服务中心三层 310 开标室

5．电子签到需要时间操作，参加投标的供应商必须提前入场。

6．参加投标的供应商在开标时须携带公司 CA 数字证书及法定代表人（负责人）的 CA 数字证书，由委托代理人参加的还需携带委托代理人的 CA 数字证书，在规定时间、规定地点进行电子签到，并解密投标文件，到开标时间未完成签到的投标无效。

7．在吕梁以外地区办理的 CA 数字证书须提前联系吕梁市公共资源交易中心技术人员进行激活后方可使用，否则无法完成签到。

联系电话：0358-8487004、0358-8487010

8．参加投标的供应商在开标解密投标文件时，与上传提交投标文件前进行加密时，必须使用同一个 CA 数字证书。

9．参加投标的供应商在开标时必须自行携带能使用 CA 数字证书登录全国公共资源交易平台（山西省-吕梁市）的电脑终端设备（须安装 IE11 浏览器和 CA 数字证书驱动）。

七、公告期限

自本公告发布之日起 7 个工作日。

八、其他补充事宜

1．通过孝义市政府网站可预览招标文件内容，但从孝义市政府网站获取的招标文件无法用于制作投标文件，本项目招标文件应以从全国公共资源交易平台（山西省-吕梁市）下载获取的为准。

预览网址：

http://www.xiaoyi.gov.cn/xxgk/fdzdgknr/ggzyjy/zfcg/

2．对与本项目有关的通知，集采机构将在招标公告刊登的媒体上以公告的形式发布。自招标公告发布起至提交投标文件截止时间前，各潜在投标人应随时关注山西政府采购网、全国公共资源交易平台（山西省-吕梁市）、孝义市人民政府网站发布的本项目相关内容，且本项目相关内容仅在山西政府采购网、全国公共资源交易平台（山西省-吕梁市）、孝义市人民政府网站以公告形式公示，集采机构不再以其他方式通知，如因自身原因未及时关注而导致投标失败，其后果自行承担。

3．本招标文件所表述的时间均为北京时间。

九、凡对本次采购提出询问，请按以下方式联系

1．采购人信息

名称：孝义市人民医院

地址：孝义市新义街

联系人：任刚

联系方式：15698679656

2．采购代理机构信息

名称：孝义市政府采购中心

地址：孝义市迎宾路与时代大道路口市民服务中心三层

联系方式：0358-7875303

3．项目联系方式

项目联系人：王辉

电话：15035826084

4．全国公共资源交易平台（山西省-吕梁市）技术咨询电话：

0358-8487010、0358-8487004