**国家传染病智能监测预警硬件采购项目**

1. **项目背景：**

我院为响应云南省疾控中心要求，为加快推动国家传染病智能监测预警前置软件部署应用有关工作，实现医疗机构传染病相关数据自动化交换，提高数据集成、风险识别、智能分析和及时预警能力，按照国家疾控局组织编制的《国家传染病智能监测预警前置软件服务器软硬件环境配置要求(试行)》部署实施硬件。

1. **产品清单**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **产品名称** | **单位** | **数量** | **限价** | **备注** |
| **1** | **前置服务器** | **台** | **1** | **72000元** | **核心产品** |
| 2 | VPN | 套 | 1 | 48000元 |  |
| 3 | 防火墙 | 套 | 1 | 30000元 |  |

**合计： 150000元**

1. **技术参数**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 机型 | 招标参数 | 数量 |
| 1 | 前置服务器 | 1、★国产自主品牌，配置2颗国产KH-40000处理器，持硬件加速国密SM2/SM3/SM4算法、每颗CPU核心数≥32核，每颗CPU主频≥2.0GHz，每颗CPU三级缓存≥64MB；  2、★配置≥256GB DDR4 3200MHz内存（8\*32），标配32个DDR4 RDIMM，最大可扩展至4TB  3、★配置≥3块960G企业级SSD硬盘，最大可扩展至≥12个3.5寸硬盘+4个2.5或3.5寸硬盘，内置2个M.2硬盘接口；  4、配置独立RAID卡，≥4G掉电保护智能缓存，支持RAID 0, 1, 10, 5, 50, 6, 60；  5、配置≥8个10/100/1000Mbps以太网口；≥4个USB接口，≥2个VGA接口；≥1个RJ-45管理接口；  6、配置2个≥1300W、1+1冗余热插拔白金电源模块 ；  7、最大支持10个PCIE4.0扩展（不含OCP及Raid卡插槽）；  8、★所投产品具备可靠性检验证书，要求MTBF≥200000小时（提供具备CNAS第三方检验证书），提供市场准入证书，包含所投产品国家3C认证，中国节能产品认证证书，中国环境标志产品认证证书； 同时要求所投产品通过传染病智能检测预警前置软件兼容性认证并提供证书；  9 、整机提供3年免费原厂质保和3年硬盘故障不返还服务。(提供原厂授权及售后服务承诺函并加盖公章)要求提供所投产品原厂400免费技术支持电话；厂家的售后服务经过CCCS钻石五星认证(客户联络中心标准体系认证)，提供证书扫描件； 投标服务器品牌在当地设有专业维修站（提供官网截图）。  10、★配置同品牌统一管理软件，可兼容管理多品牌存储、服务器、网络等X86和信创硬件设备及软件，提供加盖适配公司双方公章的兼容性认证证书（包括不限于华为、中科可控、浪潮、中兴、联想、五舟、长城、宁畅、烽火、麒麟、统信、新支点、中科方德、达梦、优炫、巨杉、东方通、中创等品牌的兼容性认证证书；同时提供支持Android 和IOS方式的运维APP，并提供APP 功能截图和软件著作权证书； | 1台 |
| 2 | VPN | 1、2U机箱，14个千兆电口，4个千兆光口，2个万兆光口，标配模块化双冗余电源，产品的CPU和操作系统均满足国产化要求。  2、国密 IPSEC VPN最大吞吐率：600Mbps，国密 IPSEC VPN最大隧道数：6000条，国密 SSL VPN最大吞吐率：200Mbps，国密 SSL VPN最大建议并发用户数：1000，标配50个SSL并发用户许可。  3、支持管理员分级分权管理，根据不同管理可以管理不同的功能模块；支持基于用户、用户组、用户角色进行授权，实现用户可访问资源、可信接入和客户端杀毒策略，保障医院基于不同用户，开放不同的权限，保障远程接入的安全；  4、★支持静态用户名口令、数字证书、短信、硬件特征码绑定、图形码方式；支持两种或两种以上组合认证方式，双因素的认证保障用户登录的安全；（提供截图证明）  5、支持可信接入功能，能够对接入主机的信息进行检查，包括域名、杀毒软件、必须安装的程序、必须运行的服务，支持可信接入分级授权；  6、支持内置CA，可以对证书进行生成、签发、废弃操作；支持国际、国密算法证书；  7、★支持DES、3DES、AES、MD5、SHA1、DH GROUP1/2/5、RSA 1024/2048等加密算法；支持国家商密专用的SM1、SM2、SM3、SM4算法；（提供截图证明）  8、支持设备的运行状态、设备资源状态、并发用户数、客户端类型分布、IPSEC隧道状态、用户流量、安全事件、中国任意省市区县的接入用户数监控，并通过图表展示；  9、★产品符合国密局制定的《IPsec技术规范》和《SSL VPN技术规范》，要求产品具备商用密码认证证书，提供证书复印件并加盖原厂公章  10、★为确保产品的稳定可靠，在使用过程中不会给业务系统带来安全风险，确保项目实施的顺利，要求厂商具备TL 9000质量管理体系认证证书（提供相关资质证书并加盖原厂公章） | 1套 |
| 3 | 防火墙 | 1、配置≥8个千兆电口、≥4个千兆光口,≥1个扩展槽位,防火墙吞吐≥4G，并发连接≥160万，每秒新建连接≥2万，应用层吞吐量≥2.2G，FW+IPS吞吐量≥750M，FW+AV吞吐量≥600M，全威胁吞吐量≥450M，IPSEC VPN吞吐≥400M，IPSEC VPN隧道数≥500。  2、配置IPSEC VPN功能模块、SDWAN功能模块，配置≥3年IPS攻击规则特征库升级许可，≥3年AV病毒特征库升级许可。  3、产品由专用的硬件平台、安全操作系统及功能软件构成。设备采用自主知识产权的专用安全操作系统，采用多核多平台并行处理机制（提供相应资质证明并加盖相应厂商公章）；  4、支持手动和LACP链路聚合，可根据源/目的MAC、源/目的IP、源/目的端口、五元组、端口轮询等条件提供不少于10种链路负载算法。  5、★支持对SD-WAN链路进行统一管理，并可自定义该链路的有效带宽值、查看当前链路状态以及触发链路过载保护机制；（提供相关截图证明并加盖相应厂商公章）  6、★支持对单条访问控制策略进行最大并发连接数和长连接的限制；（提供相关截图证明并加盖相应厂商公章）  7、规则库数量≥5000条，符合CVE标准规范，每条规则都注有中文名称，点击规则编号可显示出对应的详细规则描述，如CVE ID、风险等级、应用类型、漏洞描述、解决办法等  8、支持恶意代码防护功能，可针对HTTP、SMTP、POP3、FTP协议进行动态阻断；恶意代码特征库总数大于200万；  9、★产品完全自主研发，非OEM或贴牌其他厂商产品，满足医院对于自主可控的要求，提供中国信息安全测评中心颁发的防火墙产品《自主原创产品测评证书》并加盖厂商公章；  10、★本设备作为医院互联网出口边界防护设备，为保证投标人所投产品具备足够的安全防控能力，以及所投产品生产者的技术、资源、法律等方面的支持服务质量，投标人所投产品的制造厂商应具备中国电子信息行业联合会出具的《信息系统建设及服务能力评估资质》（CS4级）（提供相关资质证书并加盖原厂公章）。 | 1套 |

1. **采购方式**

询价

1. **服务要求**

1、本项目不面向中小企业采购

2、★签订合同前应当按采购人要求提供证明材料、证书、承诺函，且采购人有权要求中选方按照技术参数要求对其进行逐条核验，若核验不通过或未按采购人要求提供则视为虚假应标的行为，采购人有权取消合同，由此产生和造成的所有损失应当由中标人承担，并且采购人保留对中标人追究相关责任的权利。

3、本项目所有产品清单均属于同一标段采购项目。

1. **供货期**

1、中标供应商将采购方所需的货物，按照采购方要求的时间、地点进行配送，接到采购方供货通知后，按合同约定的时间完成供货。配送过程中应保证产品的完好无损，运输过程中产生的运费由中标供应商承担。

2、中标供应商需随货提供准确的交货清单等结算票据，与实际交付的产品一致，作为双方交货、验收、结算的依据。

1. **质保期**

中标供应商应提供符合国家标准及招标文件要求的产品，保证产品质量稳定可靠。提供三年质保。质保期内，在产品使用期间出现质量问题时，中标供应商必须免费更换符合国家标准及招标文件要求的产品。中标供应商应当按合同约定的时间赶到现场处理，所产生的一切费用及实施过程中的应预见和不可预见费用等由中标供应商承担。