**部署国家传染病智能监测预警前置软件网络安全加固及链路改造项目要求**

# 项目概述

为了满足医院国家疾病预防控制局和北京市疾病预防控制局北京市卫生健康委员会关于北京市部署国家传染病智能监测预警前置软件工作方案的通知要求，以及我院日益增长的内外网交互业务需要，我院计划对旧机房设备进行搬迁，并对内外网络安全边界进行加固改造，以满足传染病智能监测业务要求。

网络改造则侧重于提升医院网络架构的稳定性、安全性和扩展性，以满足部署国家传染病智能监测预警前置软件网络安全的需要和未来医院业务发展的需要。

# 采购需求

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 货物、服务名称 | 单位 | 数量 |
| 1 | 机房搬迁服务 | 项 | 1 |
| 2 | 网络梳理和改造服务 | 项 | 1 |
| 3 | 网闸 | 台 | 1 |
| 4 | 入侵防御系统 | 台 | 1 |
| 5 | 防毒墙 | 台 | 1 |
| 6 | 前置服务器 | 台 | 1 |

# 技术需求

## 机房搬迁服务

|  |  |
| --- | --- |
| **名称** | **技术参数及要求** |
| 机房搬迁服务 | 搬迁前调研与规划：对旧机房进行调研，制定搬迁方案和计划，同时规划详细的回退方案。 |
| 旧机房专线搬迁：协调相关部门，进行医保专线搬迁，确保搬迁过程中专线不受影响，并制定专线回退计划 |
| 设备搬迁：安排专业人员进行设备搬迁，确保设备安全、完整，同时制定设备回退计划， |
| 搬迁后系统重组与测试：在新机房进行系统重组和测试，确保系统正常运行，如发现问题，执行回退计划 |
| 搬迁工具提供：提供拆卸工具、运输车辆和托运工具等，确保搬迁过程顺利 |
| 搬迁人员：搬迁人员不少于4人 |
| 协助迁移后业务测试：协助业务人员进行系统测试，确保业务正常运行，如遇问题则配合回退计划 |
| 医保业务保障：为防止医保业务迁移过程中发生故障，要求提供实时备份系统，对医保数据进行备份。并保证一旦服务器发生故障，可以通过备份系统快速接管业务。提供针对此要求的服务承诺书，并加盖投标人公章 |

## 网络梳理和改造服务

|  |  |
| --- | --- |
| **名称** | **技术参数及要求** |
| 网络梳理和改造服务 | 全院网络架构梳理：梳理全院网络架构，确认整体结构和各核心位置，确保网络布局清晰、合理 |
| 设备互联链路和接口确认：确认设备之间的互联链路和接口，确保设备间通信顺畅 |
| 专线和互联网梳理：梳理专线和互联网接入，确认各接口接入位置信息，确保线路稳定可靠 |
| 整体拓扑图绘制：绘制全院网络拓扑图，方便后续维护和管理 |
| 全院交换机配置导出备份：导出并备份全院交换机配置，确保搬迁过程中配置不丢失,方便后续维护和管理 |
| 内外网交互网络规划设计：根据医院需求和现有架构，设计内外网交互网络方案，整理现有网络出口，进行出口收敛。明确内外网数据交互路径，确保内外网安全隔离 |
| 业务交互端口梳理：梳理业务交互端口，优化访问控制策略 |
| 安全咨询规划：结合网络结构，按照等级保护要求，给出安全规划建议 |
| 交付物：网络拓扑图，配置文件，互联接口信息表，安全规划方案 |

## 网闸

|  |  |  |
| --- | --- | --- |
| 指标项 | 指标子项 | 指标要求 |
| 性能指标 | 性能 | 应用层系统吞吐≥500Mbps |
| 硬件规格 | 接口要求 | 内外网主机分别具有接口：10/100/1000Base-T端口≥6个、SFP插槽≥2个、扩展槽位≥1个、USB接口≥2、RJ45 Console口≥1； |
| 液晶屏 | #内、外网主机分别具有独立液晶屏，能够显示产品品牌、型号、CPU/内存占用率、网络接口状态等信息（提供证明截图，证明材料加盖投标人和厂商公章） |
| 功能模块 | 文件交换 | #文件交换具备无客户端模式，有客户端模式，服务端模式（提供功能截图，证明材料加盖投标人和厂商公章） |
| 文件交换可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。 |
| #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（提供证明截图，证明材料加盖投标人和厂商公章） |
| 数据库同步 | 数据库同步支持有客户端、无客户端方式同步； |
| #具备数据库数据防泄漏能力，可对数据库字段进行敏感信息脱敏过滤，支持正则表达式、关键字、枚举、数值区间、时间区间等方式来匹配关键字段内容，替换成指定内容进行数据脱敏（提供产品功能截图，证明材料加盖投标人和厂商公章）； |
| #支持MySQL、ORACLE、ORACLE\_RAC、SQLServer、DB2、SYBASE、POSTGRESQL等常见数据库，支持神通、达梦、人大金仓、南大通用等国产数据库同步(提供证明截图，证明材料加盖投标人和厂商公章) |
| 病毒防护 | #支持异构双引擎病毒模块，可根据用户需求选择需要的病毒引擎（提供证明截图，证明材料加盖投标人和厂商公章） |
| #支持云查杀模式，可联动云端文件鉴定中心，预判文件安全风险，防止恶意文件通过网闸进入内网，提供高中低不同级别阻断策略（提供证明截图，证明材料加盖投标人和厂商公章） |
| 资质要求 | EAL4+ | 具备中国信息安全测评中心颁发的：信息技术产品安全测评证书EAL |
| ISO28000 | 生产制造厂家具备iso28000质量管理体系认证证书 |
| 信息化建设能力 | 生产制造厂家信息化建设及数字化能力评价中心颁发的信息化建设及数字化能力评价证书一级 |
| 服务要求 | 服务要求 | #提供三年质保和售后服务，提供制造厂商授权书和售后服务承诺（加盖原厂公章） |

## 入侵防御系统

|  |  |  |
| --- | --- | --- |
| 指标项 | 指标子项 | 指标要求 |
| 性能要求 | 网络层吞吐量 | 最大吞吐量≥6Gbps |
| 应用（HTTP）吞吐量 | HTTP应用最大吞吐量≥4Gbps |
| IPS吞吐量 | 开启IPS功能的最大吞吐量≥1.2Gbps |
| 新建连接速率 | 每秒新建连接数≥5万 |
| 并发连接数 | 并发连接数≥180万 |
| 网络接口 | 6个千兆电口和4个千兆电口； |
| 攻击防护 | 网络攻击防护 | #所投产品必须支持基于不同安全区域防御SYN Flood、UDP Flood、ICMP Flood、IP Flood、Frag Flood、DNS Flood、HTTP Flood、NTP Query Flood 、NTP Reply Flood 和SIP Flood 攻击，并支持警告、丢弃、普通防护、增强防护、授权服务器防护等多种防护措施（提供证明截图，证明材料加盖投标人和厂商公章） |
| #所投产品必须支持基于Flood攻击和恶意扫描的的流量自学习能力，可自定义开始时间、学习时长、查看学习结果，并根据学习结果一键生成DDOS防护策略。（提供证明截图，证明材料加盖投标人和厂商公章） |
| 病毒防护 | #所投产品必须能够对HTTP/FTP/POP3/SMTP/IMAP/SMB/IPTUX七种协议进行病毒查杀；本地病毒库规模大于3000万，支持样本留存。所投产品必须支持病毒样本上传和页面消息推送功能。 |
| 所投产品必须支持对最多16级的压缩文件进行解压查杀 |
| #所投产品必须支持基于MD5的自定义病毒签名；支持设置例外特征，对特定的病毒特征不进行查杀（提供证明截图，证明材料加盖投标人和厂商公章） |
| 入侵防御 | #所投产品必须支持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL注入、WEB攻击等六种分类；漏洞防护支持日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于FTP、HTTP、IMAP、OTHER\_APP、POP3、SMB、SMTP等应用协议的漏洞防护（投标文件需要提供能够体现漏洞防护特征库分类信息、支持的执行动作以及支持的应用协议的截图，证明材料加盖原厂及投标人公章） |
| #所投产品必须支持间谍软件防护功能，同时将间谍软件特征库分类，至少包括木马后门、病毒蠕虫、僵尸网络等三种分类;支持在间谍软件签名库直接查阅攻击的名称、严重性、描述等信息；间谍软件防护支持日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于FTP、HTTP、IMAP、OTHER\_APP、POP3、SMB、SMTP等应用协议的间谍软件防护（提供证明截图，证明材料加盖投标人和厂商公章） |
| 产品资质 | 产品资质 | #所投产品具备中国网络安全审查技术与认证中心颁发的“网络关键设备和网络安全专用产品安全认证证书”(提供证明材料,加盖投标人和厂商公章) |
| 所投产品具备国家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”，证书级别为EAL4+，(提供证明材料,加盖投标人和厂商公章) |
| ISO28000 | 生产制造厂家具备iso28000质量管理体系认证证书,提供证明材料,加盖投标人和厂商公章 |
| 信息化建设能力 | 生产制造厂家信息化建设及数字化能力评价中心颁发的信息化建设及数字化能力评价证书一级(提供证明材料,加盖投标人和厂商公章) |
| 服务要求 | 服务要求 | #提供三年质保和售后服务，提供制造厂商授权书和售后服务承诺（加盖原厂公章） |

## 防毒墙

|  |  |  |
| --- | --- | --- |
| 指标项 | 指标子项 | 指标要求 |
| 硬件参数 | 硬件规格 | 至少具备6个千兆电口（含2对BYPASS），2个扩展板卡插槽。硬盘容量至少1TB，支持液晶屏信息显示。 |
| 性能指标 | 网络吞吐量≥2Gbps |
| 恶意代码监测吞吐量≥1Gbps |
| 恶意代码过滤吞吐量≥600Mbps |
| 最大并发数≥80万 |
| 网络功能 | 部署模式 | 支持串行（多路）、并行（多路）、串并混合部署。 |
| 网络接入 | 支持透明接入、非对称路由、端口汇聚、HA环境等网络结构，支持IPv4\IPv6双栈网络环境。 |
| BYPASS功能 | #具备掉电自动BYPASS；WEB界面BYPASS开启、关闭操作；端口震荡自动BYPASS。（提供证明截图，证明材料加盖投标人和厂商公章） |
| 管理协议 | 支持SNMPv2c/v3、SNMP Trap、syslog、radius。 |
| 数据镜像 | #提供网桥过滤后的流量镜像输出功能。（提供证明截图，证明材料加盖投标人和厂商公章） |
| 恶意代码防护 | 防病毒多引擎 | #支持单引擎应用，双引擎同时应用，支持协议层引擎选择应用。（提供证明截图，证明材料加盖投标人和厂商公章） |
| 活跃型恶意代码 | 支持蠕虫传播、木马通讯、勒索活动、APT通讯、WEB攻击、安全漏洞、恶意IP、可疑URL、恶意域名威胁类型。 |
| 协议层病毒过滤 | #支持HTTP、FTP、POP3、SMTP、IMAP、SMB协议标准端口或非标准端口自动过滤。（提供证明截图，证明材料加盖投标人和厂商公章） |
| 威胁库管理 | 支持系统威胁规则库管理，包括规则启用、动作处置等。 |
| 日志与报告 | 安全报告 | 自定义安全报告、定时任务邮件发送。 |
| 风险分析报告 | #支持风险分析报告自定义生成、威胁类型的风险参数设定、定时任务邮件发送。（提供证明截图，证明材料加盖投标人和厂商公章） |
| 设备管理 | 用户管理 | 支持账户三权分立、双因子登录、密码复杂度设定、账户超时设定、账户锁定设定、密码到期提醒。 |
| 资质要求 |  | 生产制造厂家具备ISO9001质量管理体系认证证书,提供证明材料,加盖投标人和厂商公章 |
|  | 生产制造厂家信息化建设及数字化能力评价中心颁发的信息化建设及数字化能力评价证书一级,提供证明材料,加盖投标人和厂商公章 |
| 服务要求 | 服务要求 | #提供三年质保和售后服务，提供制造厂商授权书和售后服务承诺（加盖原厂公章） |

## 前置服务器

|  |  |  |
| --- | --- | --- |
| **分类** | **指标项** | **指标要求** |
| 硬件 | 形态 | 2U机架式服务器机箱 |
| CPU | 采用国产自研CPU,物理核数≥64核 |
| 内存 | ≥256GB |
| 存储空间 | ≥1TB，存储介质类型SSD |
| 网卡 | 配置双网卡，四个千兆电口，两个万兆光口 |
| NPU支持 | 支持扩容NPU卡 |
| 软件 | 操作系统 | 预装国产化操作系统软件：麒麟、欧拉、统信等 |
| 数据库 | 预装国产化数据库软件：OpenGauss或同等架构的数据库 |
| 质保服务 | | 包含一年期软件紧急故障保障与重装服务，硬件原厂质保三年，提供硬件厂家原厂授权书和售后服务承诺函（加盖原厂公章） |