一、网络安全设备采购要求

本项目为交钥匙工程。包含本次系统集成所必需的辅助材料、系统调优、网络安全设备安装、平台搭建、链路改造等，负责并提供设备相关的网络设备的调试连接。根据招标方的需求及自身理解提交系统集成技术方案，技术方案应满足业务需求，具备可行性；

要求提供数据中心拓扑图和设备描述说明，针对目前招标方的设备系统提供本项目的实施技术方案。现场服务包括但不限于：医院现场环境及未来发展方向规划，网络调优，原有设备利旧规划；以及与其他相关系统的联调、数据迁移、现有业务拆分等；

要求提供原厂商现场培训服务，内容应包括：培训计划、培训课程表、培训内容（包括系统架构、硬件配置、软件配置、新建资源及管理使用等）；

配置本项目实施所需的全部软硬件，保证本项目所购软硬件均为原厂正规渠道。投标方应提供系统正常运行所需的一切相关设备及配件，提供交钥匙工程，包含方案的整体设计、设备采购、物流运输、安装及调试等所有相关工作；投标方所提供的设备产品，必须保证招标方在使用期间不受第三方可能提出侵犯其知识产权、商标权和其他知识产权的起诉或纠纷；

设备进场安装实施前，由原厂工程师提供原厂授权及售后服务承诺书原件进场实施，并且投标方须安排至少 1 名具有所投产品原厂技术服务认证资质的高级工程师根据医院要求可能存在的进行数据迁移及原系统的兼容，提供相关证书证明，以证明实施及运维能力。过程中如果发生数据丢失或者兼容性问题，所造成的损失由投标方承担，并据此提供书面承诺。核心技术要求如下：

1） 提供通信加密服务工具，加强通信加密与完整性保护

IPsec VPN 隧道配置：采用 IKEv2 协议协商密钥，密钥定期自动更换（默认 24 小时），同时启用哈希算法（SHA-256）验证数据完整性，防止数据被篡改；

敏感业务数据（如数据库同步、文件传输）额外叠加应用层加密，例如数据库同步采用 SSL 加密连接，文件传输使用 SFTP（SSH File Transfer Protocol）替代 FTP，禁用明文传输协议；

部署证书认证系统（PKI），为 VPN 设备、服务器颁发数字证书，基于证书进行身份认证，杜绝身份伪造攻击。

2） 提供网络边界防护，内置病毒防护系统

部署在网络边界（通常是内外网出入口）的硬件 / 软硬一体安全设备，专注于在网关层对网络流量中的病毒、木马、蠕虫、勒索软件等恶意代码进行实时检测、拦截与清除，区别于传统防火墙仅做 IP / 端口的网络层控制，它深入到应用层内容进行扫描，是企业边界防护的核心设备之一。

核心技术原理

特征码匹配：基于海量病毒特征库，快速识别已知恶意文件；需持续更新特征库应对新样本。

启发式分析：通过代码行为、结构特征判断可疑文件，可检测部分未知威胁。

沙箱（Sandbox）分析：在隔离环境中运行可疑文件，监控其行为（如修改系统、外联远控），精准识别零日漏洞与高级恶意软件。

深度包检测（DPI）：解析 HTTP、FTP、SMTP/POP3、IMAP 等协议流量，提取文件载荷进行扫描，支持多层压缩包、加壳文件的检测。

3） 提供应用负载调度服务工具系统

负载均衡是一种将网络流量或应用请求均匀分配到多个后端服务器的技术，用于提高系统可用性、稳定性和处理能力。

流量分发将客户端请求按策略分配到不同服务器，避免单点过载。

提高系统可用性自动检测后端服务器状态，故障时自动切换，实现高可用。

提升性能通过分担压力，提高整体响应速度和并发处理能力。

会话保持（粘性会话）让同一用户的请求始终落到同一台服务器，保证会话一致性。

SSL 卸载由负载均衡器处理 HTTPS 加密解密，减轻后端服务器负担。

健康检查定期检测后端服务状态，自动剔除异常节点。

内容缓存缓存静态资源，减少后端服务器请求量。

安全防护部分负载均衡器具备 WAF、DDoS 防护等功能。

4） 提供 Web 应用防护系统，加强对外发布业务防护

SQL 注入防护识别并阻断 SQL 注入攻击，防止攻击者通过恶意参数获取数据库内容。XSS 跨站脚本防护过滤包含恶意脚本的请求，避免用户浏览器被劫持或页面被篡改。文件上传攻击防护检查上传文件类型、

内容和恶意脚本，防止上传木马或恶意文件。WebShell 防护识别常见 WebShell 特征，阻止攻击者通过后门控制服务器。CC 攻击防护对异常高频访问进行识别和限流，保护网站不被恶意请求拖垮。爬虫与恶意机器人防护识别并拦截异常爬虫、扫描器和自动化攻击工具。敏感信息泄露防护防止服务器返回敏感信息（如错误堆栈、数据库信息）。API 防护对 REST API、JSON 接口进行校验，防止参数篡改和越权访问。基于规则的检测（特征识别）利用攻击特征库识别常见攻击模式，如 SQLi、XSS、命令执行等。行为分析通过分析访问频率、请求模式、会话行为等，识别异常访问。机器学习检测（高级 WAF）自动学习正常访问模式，对偏离基线的请求进行拦截。
深度包检测（DPI）解析 HTTP/HTTPS 流量，对请求头、请求体、参数、Cookie 等进行检查。主动防御对恶意请求进行阻断、重定向、验证码挑战或返回自定义页面。

5） 提供安全漏洞扫描系统

核心作用：自动发现资产、识别安全漏洞、输出整改报告，是等保、护网、企业安全运营的标配工具。

- 资产发现：自动扫描网段，梳理 IP、端口、服务、域名
- 漏洞检测：基于 POC/EXP、特征库、行为检测
- 弱口令扫描：SSH、RDP、FTP、数据库、后台管理账号
- 风险分级：高危 / 中危 / 低危 / 信息，按优先级修复
- 报表输出：等保合规报告、整改清单、趋势统计
- 任务管理：定时扫描、增量扫描、分组扫描、告警

6） 备份系统扩容

扩容后端容量数据备份代理（用于扩展定时备份功能备份一体机存储授权容量服务；含硬盘）企业级副本数据管理软件主模块服务，包含企业级副本数据管理软件的服务器端和客户端服务。可通过扩展前端容量或后端容量副本数据管理代理以及其它高级特性模块实现分级数据保护、开发测试数据验证、OLAP 应用及大数据应用数据抽取等数据服务功能。