

第五章 采购需求

一、项目名称：

石景山医院网络与存储系统升级扩容采购项目

二、项目背景

医院互联网出口 DMZ 区虚拟化平台承载医院互联网医疗业务相关应用服务器及前置服务器，虚拟化平台由 3 台联想 ThinkSystem SR665 节点服务器及 1 套联想 ThinkSystem DE4000H 存储系统组成，随着医院互联网医疗业务不断增加，相关应用服务器及前置服务器对于虚拟化平台的计算及存储资源需求不断增加，现有平台资源严重不足，亟待进行升级改造。

医院互联网出口未部署上网行为管理设备，易导致敏感医疗数据因无管控而泄露、非工作行为挤占带宽影响远程会诊等核心业务，同时难以拦截病毒木马等网络威胁，还会因缺乏行为日志记录无法满足合规审计要求，面临隐私安全、业务中断、安全入侵及监管处罚等多重风险。

医院没有部署漏洞扫描设备，难以主动发现网络系统、医疗软件及服务器中存在的安全漏洞（如系统补丁缺失、配置缺陷、软件漏洞等），无法提前排查潜在风险隐患，同时也难以满足网络安全等级保护等合规要求中对风险主动防控的相关规定，使医院网络安全防护体系存在明显短板。

医院网络系统设备上线运行超过 10 年，部分网络设备存在设备老化，性能不足等问题，亟待进行升级改造。

三、建设目标

通过本项目实施，实现医院 DMZ 区虚拟化平台内存资源及存储资源扩容；医院互联网出口部署上网行为管理设备，实现医护人员及患者上网的身份认证、流控控制及上网行为审计，保证医院互联网访问安全，确保远程会诊、在线挂号、检验结果查询等关键医疗业务的网络可靠性，满足《网络安全法》《数据安全法》及医疗行业等保要求，为安全事件溯源、合规审计提供可靠依据；医院部署漏洞扫描设备，主动、定期检测网络中的服务器、医疗业务系统等存在的安全漏洞，提前发现潜在风险并预警，避免黑客利用未修复漏洞发起攻击，满足网络安全等级保护、医疗行业数据安全等合规要求中对“主动防控风险”的规定；升级医院网络系统核心交换机、汇聚交换机及接入交

换机，提升网络系统性能及可靠性，保证医院业务系统稳定运行。

三、采购设备清单

序号	货物名称	数量	单位	是否核心产品
1	DMZ 区服务器内存	30	条	否
2	DMZ 区存储系统磁盘	16	块	否
3	上网行为管理	1	台	否
4	漏洞扫描系统	1	台	否
5	内网核心交换机	2	台	是
6	内网汇聚交换机	2	台	否
7	内网接入交换机	10	台	否

四、技术要求

4.1 DMZ 区服务器内存（30 条）

序号	重要性	指标项	指标要求	证明材料要求
1	★	内存规格	32GB TruDDR4 3200MHz (2Rx4 1.2V) RDIMM	否
2	★	使用机型	兼容联想 ThinkSystem SR665 服务器，系统可正常识别。	否
3	★	服务	内存扩容随主机年限保修，如主机保修年限不足1年，内存配件按1年保修。	否

4.2 DMZ 区存储系统磁盘（16 块）

序号	重要性	指标项	指标要求	证明材料要求
1	★	磁盘规格	DE Series 1.8TB 10K 2.5 英寸 HDD 2U24	否
2	★	使用机型	兼容联想 ThinkSystem DE4000H 磁盘阵列，系统可正常识别。	否
3	★	服务	内存扩容随主机年限保修，如主机保修年限不足1年，硬盘配件按1年保修。	否

4.3 上网行为管理（1 台）

序号	重要性	指标项	指标要求	证明材料要求
1	★	基本要求	标准 1U 机架式设备，硬盘 ≥960GSSD，实配千兆电口 ≥6 个，万兆 SFP+ 接口 ≥4 个（含 4 个万兆多模光模块），配置冗余电源。网络层吞吐量 ≥10G，带宽性能 ≥1G，支持用户数 ≥6000 人，每秒新建连接数 ≥1.4 万，最大并发连接数 ≥60 万。实配不少于 3 年规则库升级服务。	否
2		IPv6 支持	产品支持 IPv4/IPv6 双栈工作模式，以适应 IPv6 发展趋势。	否
3		流量管控	支持从 IP、用户、应用、时间段、终端类型等不同维度对流量进行限制，以保证关键业务的运行。	否
4	#	信息统计	支持对用户人数、实时流量排行、终端类型分布、违规终端、违规用户等信息进行直接展示。（提供功能证明材料并加盖原厂公章）	是
5	#	访问质量	Web 访问质量检测，针对内网用户的 web 访问质量进行检测，对整体网络提供清晰的整体网络质量评级。（提供功能证明材料并加盖原厂公章）	是
6	#	终端识别	设备需支持 PC、移动终端、服务器、交换机、摄像头、门禁、投影仪等终端类型识别，并支持获取 IP、MAC 及操作系统信息。（提供功能证明材料并加盖原厂公章）	是
7		可视化	支持首页显示在线用户、流量分析、行为日志分析、应用流量排名、用户流量排名、资产类型分布、新设备发现趋势、TOP 违规检查项、TOP 违规用户、行为风险分析包括：泄密风险、终端接入、上网安全、系统状态、接入状态。	否
8		防路由私接	设备需具有防路由私接功能，支持设定白名单，针对私接路由支持设定冻结时间。	否
9		故障排查	支持网络故障排查，支持 PPS 异常、丢包异常、ARP 异常、内网 DOS 攻击等异常情况实时监测，显示每日异常事件个数及情况	否
10	#	应用识别库	设备内置应用识别规则库，支持超过 9000 种以上应用规则数、支持超过 6000 种以上的应用；支持根据标签选择应用，并支持给每个应用自定义标签；支持根据标签选择一类应用做控制；支持超过 900 种主流 Saas 应用，对 Saas 应用有默认分类标签，帮助客户统一配置策略。（提供功能证明材料并加盖原厂公章）	是
11	#	异常感知	支持 ARP 异常、内网 DOS 攻击、PPS 异常等网络故障排查每日异常事件个数进行统计。（提供功能证明材料并加盖原厂公章）	是

12		业务审计	支持针对重点业务系统进行单独审计，业务系统名称、IP、端口或域名支持自定义。	否
13		信息维护	支持从本地导入帐户/分组/IP/MAC/描述等相关信息。	否
14	#	其他要求	为保障产品的可靠性和生产商的技术开发能力，要求产品生产商提供《CCRC 信息安全服务-软件开发服务资质》一级及以上证书，提供证明材料并加盖原厂公章。	是
15	#	其他要求	为保障安全服务能力，要求产品生产商为网络安全应急服务支撑单位（甲级），提供证书复印件并加盖原厂公章。	是

4.4 漏洞扫描系统（1台）

序号	重要性	指标项	指标要求	证明材料要求
1	★	硬件要求	标准机架式硬件，1U，交流单电源， $\geq 1T$ 硬盘， $\geq 4*$ 千兆电口， $\geq 4*$ 千兆光口（不含光纤接口模块）， $\geq 2*$ USB 口， $\geq 1*$ 串口。	否
2			支持 IPv4 和 IPv6 环境的部署和扫描	否
3	★	基本要求	允许最大并发扫描 ≥ 60 个 IP 地址，允许最大并发任务 ≥ 10 个任务，授权可扫描总数量 ≥ 512 个无限制范围的 IP 地址或域名，三年特征库升级服务。	否
4	#		支持 web 扫描，可对 Web 应用提供专业的漏洞、挂马检测和分析。请提供证明截图并加盖原厂公章。	是
5	#		支持检测的漏洞数大于 300000 条，兼容 CVE、CNCVE、CNNVD、CNVD 等主流标准，并提供 CVE Compatible 证书。请提供证明截图并加盖原厂公章。	是
6		漏洞管理和分析	支持系统漏洞库和 Web 漏洞库通过多种维度对漏洞进行检索，包括：漏洞名称、漏洞 ID，CVE ID、BUGTRAQ ID、CNCVE ID、CNVD ID、CNNVD ID、MS 编号、风险等级、是否使用危险插件、是否支持漏洞验证，漏洞发布日期、漏洞分类信息。	否
7			内置不同的漏洞模板针对 Unix、Windows 操作系统、网络设备和防火墙等模板，同时支持用户自定义扫描范围和扫描策略；	否
8			支持数据库扫描模板，支持 Oracle、MySQL、MS SQL、DB2、Sybase、MongoDB 数据库漏洞检查，请提供功能截图。	否
9	#		支持复用已有任务配置用于新的扫描任务，请提供功能截图并加盖原厂公章。	是

10			支持对系统漏洞、web 漏洞进行综合分析，可输出同时包含漏洞扫描、弱口令检查结果的报表。	否
11			支持立即执行、定时执行、周期执行扫描任务，自定义的周期时间可精确至每*月第*个星期*的*点*分。	否
12			支持扫描时间段控制，只在指定时间段内执行任务，未完成任务在下一时间段自动继续执行。	否
13			提供高级漏洞检索模板，支持将符合筛选条件的漏洞自动加入到自定义漏洞模板中，及后续插件升级包中的漏洞也可以自动加入到模板中。	否
14	#		支持专门针对 DNS 服务的安全漏洞检测，包括 DNS 投毒等漏洞检测能力；支持“幽灵木马”检测，请提供功能截图并加盖原厂公章。	是
15		风险展示和报表	支持在线报表，在线查看任务参数、综述信息、主机信息、漏洞信息、脆弱账号以及参考标准，在线查看设备风险详情。	否
16	#		提供多种报表类型，包括综述报表和主机报表，请提供功能截图并加盖原厂公章。	是
17			报表能提供针对不同角色的默认模板，离线报告支持 HTML、WORD、EXCEL、PDF、XML 格式，报告可以直接下载或自动通过邮件直接发送给相应管理人员。	否
18		多权限用户管理	支持不同用户角色权限管理，区分系统管理员、普通管理员、审计管理员等角色，其中系统管理员和审计管理员可直接使用，普通管理员可以新增使用，不同管理员拥有不同的管理权限。	否
20	#	产品资质	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》，提供认证证明	是

4.5 内网核心交换机（2 台）

序号	重要性	指标项	指标要求	证明材料要求
1	★	转发性能	交换容量 $\geq 100\text{Tbps}$ ，包转发率 $\geq 76000\text{Mpps}$ ，以官网最小数值为准。	否
2	★	硬件规格	主控引擎 ≥ 2 ，整机业务板槽位数 ≥ 4 ，整机电源槽位数 ≥ 6 ，提供官网产品文档证明截图并提供官网链接。	是
3	#		为提升槽位使用率，主控引擎需支持业务端口，提供官网产品文档证明截图并提供官网链接。	是
4	#		采用厂商自研国产化芯片，提供权威第三方测试报告。	是

5		二层功能	支持 MAC 地址自动学习和老化、静态、动态、黑洞 MAC 表项、源 MAC 地址过滤、基于端口和 VLAN 的 MAC 地址学习限制。	否
6		三层功能	支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议、RIPng、OSPFv3、ISISv6、BGP4+等 IPv6 动态路由协议。	否
7		VXLAN	支持 VXLAN 功能，支持 VXLAN 网络的自动化部署。	否
8	#	安全性	支持 MACsec，端到端加密组网，提供权威第三方测试报告	是
9	#	可靠性	支持双活主控，故障倒换时间<5ms，提供权威第三方测试报告。	是
10		配置和维护	支持 Telemetry 技术。	否
11			支持 SNMP V1/V2/V3、Telnet、RMON、SSHV2。	否
12	★	实配	万兆以太网光接口≥48，千兆以太网电接口≥48，主控单元≥2，模块化电源≥2，10GE 高速堆叠线缆≥1。	否

4.6 内网汇聚交换机（2 台）

序号	重要性	指标项	指标要求	证明材料要求
1	★	转发性能	交换容量≥2.56T/25.6T，包转发率≥1260Mpps，以官网最小数值为准。	否
2	★	硬件规格	万兆 SFP+≥24 个，40/100GE QSFP28≥6 个。	否
3			标准 1U 设备，支持电源模块≥2 个，风扇模块≥4 个。	否
4	#		采用厂商自研国产化芯片，提供权威第三方测试报告。	是
5	#	ID 指示灯	维护人员可以在后台点亮后去机房直接找到相对于设备，便于快速定位设备位置，提供官网产品文档证明截图并提供官网链接。	是
6		三层功能	支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议。	否
7			支持 RIPng、OSPFv3、ISISv6、BGP4+等 IPv6 动态路由协议。	否
8		VXLAN	支持 VXLAN 功能，支持 BGP EVPN，支持分布式 Anycast 网关。	否
9	★	实配	万兆 SFP+≥24 个，40/100GE QSFP28≥6 个，10G 单模光模块≥4，电源模块≥2，10GE 高速堆叠线缆≥1。	否

4.7 内网接入交换机（10 台）

序号	重要性	指标项	指标要求	证明材料要求
1	★	硬件规格	交换容量 $\geq 670\text{Gbps}$, 包转发率 $\geq 200\text{Mpps}$, 以官网最小数值为准。	否
2	★		10/100/1000Base-T 以太网端口 ≥ 48 个, 万兆 SFP+口 ≥ 4 个。	否
3	#		支持专用堆叠口, 不占用业务口带宽, 堆叠带宽(双向) $\geq 48\text{Gbps}$, 提供官网产品文档证明截图并提供官网链接。	是
4	#		采用厂商自研国产化芯片, 提供权威第三方测试报告。	是
5		二层功能	支持 4K VLAN, 支持 Voice VLAN、支持 MUX VLAN、VLAN Stacking、VLAN Mapping。	否
6		三层功能	支持静态路由、路由策略、策略路由。	否
7			支持 RIP、RIPng、OSPFv2、OSPFv3、VRRPv4、VRRPv6。	否
8	#	ID 指示灯	维护人员可以在后台点亮后去机房直接找到相对于设备, 便于快速定位设备位置, 提供官网产品文档证明截图并提供官网链接。	是
9	★	实配	10/100/1000Base-T 以太网端口 ≥ 48 个, 万兆 SFP+口 ≥ 4 个, 10GE 多模光模块 ≥ 4 , 10GE 高速堆叠线缆 ≥ 1 。	否

五、服务要求:

1、保修服务要求:

★1. 1DMZ 区服务器内存及 DMZ 区存储系统磁盘要求同医院现有服务器和磁盘阵列主机一同维保, 并享有原设备维保等级和维保服务内容, 需提供供应商售后服务承诺函。

#2. 2 所有设备提供至少三年免费原厂保修服务及软件升级, 提供原厂售后服务承诺函原件。

2、运维服务要求:

(1) 在系统验收通过后, 供应商提供至少三年期的系统维护, 软硬件原厂维保, 保证 7x24 小时提供服务;

(2) 日常报修: 接到通知后电话远程解决, 如无法解决, 2 小时内到达现场,

工作时间为 7*24 小时（每周 7 天，每天 24 小时）；

（3）巡检维护：在维护期内每月到现场进行巡检维护，提交巡检报告；

（4）升级更新：免费系统升级。供应商按设备原生产厂商指定的更新、升级要求，对运行的产品软件系统等进行更新、升级维护。

3、人员要求：

（1）投标人承担本项目工作的项目经理同时具备①高级信创集成项目管理师证书；②中国信息安全测评中心颁发的 CISP 证书；③近 3 年（2022 年至本项目招标公告之日起）实施主导过核心产品项目案例。

（2）除项目经理外，团队其他成员具备信息系统项目管理师（高级）认证不少于 1 人。具备高级信创集成项目管理师证书人员不少于 1 人。

4、交付时间：自合同签订之日起 3 个月内完成安装、调试并交付使用。

5. 交付地点：北京市石景山医院指定地点。