佛山市高明区人民医院
信息系统安全防护项目需求说明

1. 项目背景

随着等级保护 2.0 的发布，对于医院的信息化系统提出了新的要求，医院的信息系统建设在安全方面的建设力度是否满足未来发展的要求都是对现有信息系统建设能力储备的考量。本项目主要通过对网络结构、网络安全的风险分析，最大限度地消除医院网络环境目前存在的安全隐患及漏洞，提供完善安全防护，实现事前监测、事中防护、事后审计的体系化防护，并满足等级保护 2.0 的三级系统建设要求。

2. 项目主要清单

序号	细项名称	数量	单位
1	内外网隔离网闸	2	台
2	外网防火墙	1	台
3	医保网防火墙	1	台
4	政务网防火墙	1	台
5	服务器区防火墙	2	台
6	WEB 安全网关（WAF）	1	台
7	内网杀毒软件（含服务器杀毒） （1300 台 PC，130 台服务器）	1	项
8	大数据安全分析平台硬件	1	台
9	内外网分拆工程(网络设备及施工)	1	项
10	离线备份磁带库	1	套
11	综合安全服务 （含 2 人现场驻点 1 年服务）	1	项

3.各细项详细要求

3.1 内外网隔离网闸（2 台，双机热备）

指标项	指标要求
设备参数	网络层吞吐量≥500Mbps;千兆电口≥8 个; 并发连接数≥10 万;
部署模式	支持透明、代理及路由等工作模式
内置应用	产品内置各类应用支持模块。
文件交换	支持文件交换
数据库同步	支持数据库同步
数据库传输	支持数据库传输
FTP 访问	支持 FTP 访问
邮件传输	支持邮件传输
安全浏览	支持安全浏览
安全通道	支持安全通道
抗 DDoS 攻击	支持抗 DDoS 攻击
安全管理	支持安全管理
双机热备	支持双机热备
日志审计与状态监控	支持日志审计与状态监控

3.2 外网、医保网、政务网防火墙（各 1 台）

指标项	指标要求
设备参数	网络层吞吐量≥4G，应用层吞吐量≥1G，并发连接数≥100 万，HTTP 新建连接数≥2 万，
路由实现	实现静态路由、策略路由、RIP、OSPF、BGP 等路由协议。
攻击防护	实现安全区域划分，访问控制列表，配置对象及策略，动态包过滤，黑名单，MAC 和 IP 绑定功能，基于 MAC 的访问控制列表，802.1q VLAN 透传等功能。
会话控制	支持基于接口/安全域、地址、用户、服务、应用和时间的会话控制策略，包括总连接数控制、每秒总新建连接数控制、每 IP 总连接数控制、每 IP 新建连接数控制。
流量控制	支持带宽管理和流量控制功能。
入侵防御	支持并开通网络入侵检测及防御功能
防病毒	支持对文件感染型病毒、蠕虫病毒、脚本病毒、宏病毒、木马、恶意软件等过滤
DDoS 防护	能够防范 DOS/DDOS 攻击

3.3 服务器区防火墙（2 台）

指标项	指标要求
设备参数	性能参数：网络层吞吐量≥10G，应用层吞吐量≥4G，并发连接数≥220 万
部署方式	支持路由，单臂，网桥，虚拟网线，旁路以及混合部署方式；
路由支持	支持静态路由，策略路由；
防病毒	支持对文件感染型病毒、蠕虫病毒、脚本病毒、宏病毒、木马、恶意软件等过滤。
Web 应用安全防护	支持口令暴力破解防护，支持自定义爆破阈值设置； 具备识别与阻断外部扫描器发起的服务器恶意扫描行为，可对扫描器地址进行自定义封堵。
入侵防御	支持并开通网络入侵检测及防御功能
僵尸主机检测	支持在僵尸网络检测

3.4 WEB 安全网关（WAF）（1 台）

指标项	指标要求
设备参数	性能参数：网络层吞吐量≥4Gbps，HTTP 应用层吞吐量≥220Mbps，HTTP 新建连接数≥20000，HTTP 并发连接数≥1000000。
部署方式	支持复杂使用环境的接入要求。
HTTP 异常检测	支持 HTTP 异常检测
Web 应用防护	支持防护 SQL 注入、XSS 攻击、网页木马、网站扫描、Webshell、跨站请求伪造（CSRF）、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web 漏洞攻击等。 支持自定义 Web 应用防护规则，通过正则表达式自定义规则匹配方向、动作、字符串、危险等级、动作、攻击影响、描述等。
语义分析	支持语义引擎用于检测 Web 攻击，能针对不同类型的 Web 攻击如命令注入攻击防护等
业务学习	支持业务模型学习监督功能，通过智能分析引擎对业务流量进行分析学习，建立用户业务特征模型，解决因 WEB 应用中因代码不规范和安全检测功能冲突导致的业务误判问题。

防扫描和信息保护	支持 HTTP 应用隐藏，支持过滤如 Server、X-powered-by 类型的 HTTP 响应报文头，支持替换服务器出错页面（5XX）和替换服务器出错页面（4XX）。

3.5 内网杀毒软件（含服务器杀毒）

（不少于 1300 台 PC，130 台服务器援权，不少于 3 年服务）

项目	指标	具体要求
平台环境要求	控制中心要求	控制中心支持级联方式和单一部署两种方式，控制中心根据客户端点数的增加支持横向扩展，操作系统支持 Windows Server 2008 R2/2012/2012 R2/2016 的 64 位版本（简体中文版）； 支持 CentOS 7、Redhat 7 等 Linux 系统；
		控制中心支持安装在虚拟机上；
	客户端要求	操作系统： Windows XP_SP3 及以上/Windows Vista/Windows 7/Windows 8/Windows 10； Windows Server 2008/Windows Server 2012/Windows Server 2016/Windows Server 2019
基础功能	终端许可管理	支持按照终端类型/分组统计及分配管理每个功能的终端授权使用数量。
	控制中心管理	支持控制中心迁移、数据备份、数据恢复；支持多升级服务器；
		支持根据分组、计算机名称、IP 地址、操作系统、在线状态等条件的组合筛选出符合条件的终端进行管理；
		支持与 NTP 时间服务器同步，可设置同步时间间隔，使终端时间保持和时间服务器相同。
		支持单个页面展示终端部署统计、终端安全趋势、终端状态（文件防护开启率、未安装补丁终端率、终端病毒更新率和终端版本更新率）、终端程序版本、终端在线统计、病毒库版本分布、安全更新和重要补丁安全趋势等信息，均可通过图形化展示。
		支持定时公告功能，可配置开机显示、周期显示和立即推送。

		支持对单个客户端进行维护，终端视角查看终端基本信息，包括计算机名、型号、IP、MAC 地址、工作组、域信息、本次开机时间、上次关机时间、应用功能、在线状态； 所功能应用策略情况； 硬件信息展示，包括 CPU、主板、内存、磁盘存储、显卡、显示器、声卡、网卡等信息； 实时进程信息展示，包括进程名称、PID、进程用户名、命令行、占用内存、CPU 占用、MD5 等信息； 网络信息展示，包括。
		支持通过高级筛选方式对终端概况进行筛选查看指定范围终端实时统计数据，支持“与或”组合筛选。
		支持自动分组，按 IP 地址、CPU 数量、MEM 容量、主机名、计算机工作组等参数进行自动动态调整分组。
		管理控制中心当登录账号输入密码错误次数超过锁定阈值后账号将被锁定，且可设置锁定时间，该时间内账号登录请求不被接受。同时应支持双因子认证登录方式，提高安全性。
		客户端主程序、病毒库版本支持按分组和多批次进行灰度更新，保持在低风险中完成终端能力更新。支持设置不同终端类型设置和每批次观察时长。当检测到新版本将从第一批次重新观察。
		支持在线更新病毒库、补丁库、威胁情报等数据，并且支持“按月、按周、按天、按小时”灵活设置更新时间。支持隔离网环境更新数据。
		支持文件下载分级缓存，支持下载文件限速和日志上传限速，可设置带宽最大使量和限速时间，避免过多占用网络带宽，影响业务办公。
		支持定义不同权限管理员角色，通过角色能够对有相同权限需求的用户进行授权，达到复用的能力；而对于没有复用的权限，可通过基于规则方式进行授权，支持角色层级管理，可至少达到 5 级新建角色。简化管理员对角色的管理成本，提高效率。
		支持终端用户和管理员是一套账号管理系统，简化账号管理复杂度，一个账号解决所有身份认证，既可以用于终端登录，也可以用于管理管理中心。
		支持控制中心迁移、数据备份、数据恢复；支持多升级服务器；
		支持自定义告警规则，例如系统一段时间内病毒和未知文件超过一定数量后会通过邮件发送给收件人查阅。支持邮件和阿里云平台的短信告警通知。
	客户端管理	支持终端密码保护功能，支持终端“防退出”密码保护、“防卸载”密码保护、防安装密码保护。支持设置自我保护功能，可有效防止客户端进程被恶意终止、注入、提高客户端进程、数据、配置的安全性。
		支持自定义定制客户端标题、皮肤、语言、产品 LOGO、企业 LOGO、认证弹窗 LOGO。
防病毒防护	病毒防护概况	病毒防护概况：终端基础信息、病毒库版本、发现病毒数、未处理病毒数、最后查杀时间、文件防护状态、引擎使用状态、扩展病毒库版本

	病毒查杀日志	病毒防护日志包含：病毒查杀日志、查杀任务日志、攻击防护日志、系统防护日志、按分组、按终端、按时间。
	病毒防护报表	病毒报表支持病毒查杀趋势、扫描触发方式趋势、发现病毒趋势、终端感染趋势、病毒类型统计、病毒处理结果统计、病毒发现触、方式统计、趋势图表、按分组、按终端、按病毒名称。
	黑白名单	支持手动导入、导出黑白名单，添加黑白名单。支持通过文件导入添加黑白名单。
		支持通过文件数字签名添加黑白名单管理。
	病毒扫描	支持信任区设置，病毒扫描或实时防护时不扫描目录或文件。
		病毒扫描支持扫描所有文件和仅扫描程序及文档文件设置，支持对压缩包文件设置最大扫描层数和大小，当发现压缩包内存在病毒时，还需继续扫描压缩包内其他文件。
		支持对终端当扫描到感染型病毒、顽固木马时，自动进入深度查模式，可设置禁止终端用户管理路径或文件白名单、禁止终端用户管理扩展名白名单、扫描时不允许终端用户暂停或停止扫描任务。
		支持扫描资源占用设置，可设置不限制、均衡型、低资源三种模式。
	主动防御	支持对进程防护、注册表防护、驱动防护、U 盘安全防护、邮件防护、下载防护、IM 防护、局域网文件防护、网页安全防护、勒索软件防护。
	网络防护	支持自动阻止远程登录行为，防护黑客远程爆破和拦截恶意的远程登录。
		支持网络入侵拦截对流入本机的网络包数据和行为进行检测，根据策略在网络层拦截漏洞攻击、黑客入侵等威胁。
		支持僵尸网络攻击防护，对流出本机的网络包数据和行为进行检测，根据策略在网络层拦截后门攻击、C2 连接等威胁。
		支持防护对流出本机的网络包数据和行为进行检测，根据策略在网络层拦截后门攻击、C2 连接等威胁。
		支持 ARP 攻击防护根据策略检测和拦截局域网中的 ARP 欺骗攻击行为。
	终端病毒处理弹窗	客户端弹窗支持免打扰模式和智能模式，使用免打扰模式可以对不能弹窗的终端设备中避免弹窗。使用智能模式是智能调整弹窗，对已知的病毒自动处理，对未知的病毒提示处理。
	杀毒引擎	支持不少于三个杀毒引擎混合使用，提高病毒检出率。
补丁管理	补丁类型	支持对 Windows 操作系统、IE、.NET Framework、Office、Adobe Flash Player、Adobe Acrobat 和 Adobe Acrobat Reader DC、硬件驱动更新等软件进行补丁修复。
		支持按补丁类型和级别修复，补丁级别需包括：安全更新、重要补丁、功能补丁、可选补丁。支持仅安装指定补丁设置。
		支持精细配置按照操作系统版本修复漏洞，支持精细配置按照 Office 版本修复漏洞。
	补丁语言	补丁语言种类需支持中文，繁体中文，英文。

	灰度发布	支持管理员预先设置好灰度发布批次和漏洞修复策略（分时间段、按级别、排除有兼容性问题的补丁等），每当控制台更新补丁库，自动化编排完成漏洞修复——将全网终端划分为由小到大的多个批次，根据企业环境，自动先推送给第一个小批次分组，如无问题自动推送给下一个批次，直到推送给全网。如有问题，只需将有问题的补丁添加到排除列表和卸载已安装的终端即可。整个推送安装过程自动化编排，无需管理员过多参与，只需在有问题时添加排除列表和下发卸载补丁任务。
	漏洞修复设置	支持开启自动修复漏洞，包括开机时修复，并支持随机延迟执行、间隔修复和按时间段修复，可设置延迟时间、间隔修复时间和修复时间段。
		支持影响到编辑 Office 文档时提醒，可取消此次修复任务。
		允许终端用户手动修复漏洞，如果发现“修复内容”中设置的需要修复的漏洞和功能缺陷没有修复成功则提醒终端用户修复。
	补丁日志	支持展示终端信息、补丁号、补丁级别、补丁类型、安装日期、事件上报时间、事件类型、结果、详细描述。
		支持按终端统计补丁安装和生效情况，支持按照终端维度统计，统计每台终端的各个级别的补丁未安装数量，以及已安装、已安装未生效、已排除的总数量，并支持导出统计报表。
		支持按照补丁的维度统计补丁安装情况，包括补丁号、系统类型、补丁类型、补丁级别、补丁名称、补丁描述、发布日期、**漏洞 CVE 编号、漏洞 CNNVD 编号**、未安装、已安装、已安装未生效、已排除、未更新补丁库。并支持导出统计报表。
主机防火墙	支持主机防火墙功能，通过添加 IP、域名规则、支持允许/拒绝规则、支持任意流向拦截和允许，支持 TCP、UDP、TCP+UDP、ICMP、多播和组播，支持自定义端口范围、支持自定义目标 IP，支持输入 IP 范围。	
	支持根据需要来设置是否接管系统防火墙，支持根据规则的重要程度设置规则的优先级。	
	支持展示防火墙上报日志，展示终端基础信息、拦截规则名称、拦截时间、操作、协议、源地址，目的 IP/域名、源端口、目的端口。	
	为了避免规则过大，导致日志上报造成网络堵塞或撑满服务器，支持设置日志上报频率。	
基线核查	基线核查项	支持终端安全基线检查，可自定义基线检查项，可自定义终端端定性标准，通过基线检查分数设定，定义出高危、中危、低危和安全，同时产品内置等保 2.0 基线模板。
		支持系统状态基线核查，应包括：是否安装关键和重要系统补丁、是否安装防病毒软件、工作组命名检查、是否加入域、计算计命名检查、系统备份还原点检查、系统重要目录对 Everyone 或 Guests 来宾账户开放检查、空口令检查、操作系统是否开启 Hardware DEP Available 保护检查、系统隐藏用户检查、关键进程是否运行或禁止检查、禁止开放端口检查。

		身份鉴别应包括：密码使用期限、强制密码历史记录、最小密码长度、密码必须满足复杂性要求、使用还原加密存储密码、阻止 Microsoft 账户、账户锁定阈值、账户锁定持续时间、重置账号锁定计数器、启用屏幕保护程序。
		安全审计应包括：审核登录、审核其他登录/注销事件、审核策略更改、管理审核安全日志、审核账户锁定。
		访问控制应包括：Guest 账户状态、将本地账户使用空白密码限制为仅控制台登录、允许 Windows 自动边接到建议的开放式热点或与联系人共享的网络以及提供付费服务的热点、允许用户使用远程桌面服务、管理员账户状态、允许 ICMP 重定向覆盖 OSPF 生成的路由、检查是否关闭了默认共享、不显示上次登录、清除虚拟内存页面文件、重命名管理员账户、提示用户在密码过期之前更改密码、操作系统 UAC 用户账户控制是否开启至指定级别、设置活动但空闲的远程桌面服务会话的时间限制、TCP/IP 筛选。
		资源控制应包括：引用远程 DNS 或 NetBIOS 名称或地址、远程桌面服务、Remote Procedure Call (RPC) Locator (RpcLocator)、Remote Registry (RemoteRegistry)、Remote Desktop Configuration (SessionEnv)、Remote Desktop Services UserMode Port Redirector (UmRdpService)、Telnet 服务器、IE 受信任站点检查、Routing and Remote Access (RemoteAccess)、防火墙状态、服务管理事件和事件日志。
		支持关闭自动播放检查。
	基线报表	支持显示不通过检查项 TOP10 条形图统计，横坐标表示检查项名称，纵坐标表示不通过次数。
		支持以表格形式展示，显示内容包含检查项名称、检查范围（根据检查项分类划分）、不合规次数（该时段内该检查项不合规次数）。
		支持按分组名称、终端数量、该分组内的平均得分、该得分所属的安全级别。
		支持按终端统计列表内容：计算机名、分组名称、IP 地址、MAC 地址、终端类型、登录账号、该终端的核查次数、该终端的最新核查得分、该分数所属的安全级别。
终端管控	外设管理	支持对终端各种外设（USB 存储、硬盘、存储卡、光驱、打印机、扫描仪、摄像头、手机、平板等）、接口（USB 口、串口、并口、1394、PCMIA）设置使用权限，并支持生效时间设置。
		支持外设库管理，可统计终端外接的各种设备，包括厂商和设备类型、产品、数量、PID、VID 和设备来源。
		支持对支持对外设进行多维度的放行，包括设备名称、PID/VID、实例路径，通过添加实现例外或加黑。
	进程管理	支持对单点维护功能，可远程查看终端实时运行的进程，需要包含进程名称，进程用户、命令行（执行路径+执行参数）、内存占用、签名、产品名称、公司名称等，支持远程结束进程。 支持远程查看计算机各个网卡配置信息。
		支持终端进程红名单、黑名单、白名单功能。可设置核心进程必须运行，也可保护核心进程不被结束，违规并告警。

	知识库	支持统计终端的出口地址列表，搜集终端连接的无线信号信息统一展示，标识出 ssid 可连通互联网，可连通服务器的情况，汇总展示内网终端上报的进程信息，支持设置进程匹配规则，其它业务可直接调用创建好的进程规则或者进程分组。
	违规外联	支持对互联网出口地址探测，支持对违规的互联网出口进行发现、断开网络、终端锁屏、断网+锁屏处理。支持例外白名单添加。
	能耗管理	支持对终端节能管理，支持对长时间运行、定时关机、空闲节能、工作时间外开机等节能类型设定策略，支持仅提示、关机、注销、锁定、关闭显示器、锁定+关闭显示器、休眠和睡眠处理。并支持提示倒计时弹窗，可设置在终端取消后下一次提醒时间。
	网络防护	支持对网卡进行防护，支持阻止终端修改 IP 地址、使用动态 IP 地址、热点创建和 IPV6 地址使用等，可自定义提示内容和生效时间。

3.6 大数据安全分析平台硬件

提供大数据安全管理平台扩容，包括平台软硬件；需支持与医院目前使用的 Ailpha 大数据安全态势感知平台无缝兼容。包括将现有医院 Ailpha 大数据安全态势感知平台迁至新硬件服务。

硬件参数要求：不少于 2 物理 CPU 24 核；内存 128GB/硬盘 24TB。

3.7 内外网分拆工程(网络设备及施工)

本次主要为重构医院外网网络，现在网络保留为医院内网。

拟在总院门诊 6 楼、妇幼各部署 2 台外网核心交换机。在总院门诊 66 楼，门诊 76 楼，门诊 86 楼，门诊 46 楼，门诊 16 楼，药库 26 楼，医技 5 楼，住院 1 号 1 楼，住院 1 号 6 楼，住院 1 号 12 楼，住院 2 号 4 楼、妇幼门诊 2 楼，妇幼住院 5 楼、文明院区等预留汇聚交换机。

本次终端布线预计 300 个点位，如不足 300 个点位侧以实际布线工程结算。工程完成后，需满足医院外网能独立运行。

序号	设备类型	描述	设备数量	单位
1	外网核心交换机	24 个万兆 SFP+,2 个 40GE QSFP+,含 1 个 170W 交流电源，QSFP+-40G-高速电缆-1m-(QSFP+38)-(CC8P0.254(S))-(QSFP+38 公)-室内用	4	台
2	外网汇聚交换机	48 个 10/100/1000BASE-T 以太网端口,4 个万兆 SFP+,交流供电	14	台
3	光纤模块	光模块-SFP+-10G-单模模块（1310m,10Km,LC）	满足运行需求	个
4	六类网线	六类网线	满足运行需求	箱
5	24 芯单模室外光纤	24 芯单模室外光纤（防鼠咬）	满足运行需求	米
6	8 芯单模室外光纤	8 芯单模室外光纤（防鼠咬）	满足运行需求	米
7	机柜	6U 机柜	1	个
8	水晶头	六类水晶头	满足运行需求	个
9	光纤跳线	3M 光纤跳线	满足运行需求	条
10	光纤配线架	24 口光纤配线架	满足运行需求	个
11	光纤配线架	12 口光纤配线架	满足运行需求	个
12	熔纤	光纤熔接	满足运行需求	个
13	辅材	PVC 线管、胶布等辅材	满足运行需求	项
14	技术服务	全院网络点布线	满足运行需求	个
15	光纤实施布线	光纤实施布线	满足运行需求	项
16	网管软件	20 个交换机许可	1	套

3.7.1 外网核心交换机

指标项	**详细指标**
交换容量	交换容量：2.56 Tbps/23.04Tbps
包转发率	包转发率：480 Mpps
端口	支持 24 个万兆 SFP+端口，2 个 40G QSFP+端口
	支持业务扩展插槽数≥1，扩展后最大可支持 6 个 40G QSFP+端口
	支持 24 个 10GE、6 个 40GE 端口线速转发
电源	为了提高设备可靠性，支持可插拔的双电源

指标项	详细指标
二层功能	支持 MAC 地址≥288K
	支持 ARP 表项≥44K
	支持 4K 个 VLAN，支持 Guest VLAN、Voice VLAN，支持基于 MAC/协议/IP 子网/策略/端口的 VLAN
	支持 1:1 和 N:1 VLAN 交换功能
路由	支持静态路由、RIP V1/2、URPF OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6
	支持 IPv4 FIB≥128K
	支持 IPv6 FIB≥64K
VxLAN	支持 VxLAN 功能，支持 VxLAN 二层网关、三层网关，支持 BGP EVPN，实现自动建立隧道
MPLS	支持 MPLS L3VPN、MPLS L2VPN(VPLS/VLL)、MPLS-TE、MPLS QoS
堆叠	支持堆叠，主机堆叠数不小于 9 台
纵向虚拟化	支持纵向虚拟化，作为父节点管理纵向子节点
	支持纵向虚拟化，作为纵向子节点零配置即插即用
QOS	支持报文的 802.1p 和 DSCP 优先级重新标记 支持 L2（Layer 2）~L4（Layer 4）包过滤功能，提供基于源 MAC 地址、目的 MAC 地址、源 IP 地址、目的 IP 地址、端口、协议、VLAN 的非法帧过滤功能
管理维护	支持以太网 OAM（802.3ah 和 802.1ag） 支持 SNMPv1/v2c/v3 支持网管系统、支持 WEB 网管特性 支持 sFlow
可靠性	支持 G.8032 标准环网协议

3.7.2 外网汇聚交换机

指标项	指标要求
交换容量	交换容量≥400Gbps
包转发率	包转发率≥144Mpps

端口类型	48 个千兆电口，4 个万兆 SFP+
二层功能	支持 MAC 地址≥16K
	支持 ARP 表项≥4K
	支持 4K 个 VLAN，支持 Voice VLAN，基于端口的 VLAN，基于 MAC 的 VLAN，基于协议的 VLAN 支持 Smart link
	支持 1:1 和 N:1 VLAN Mapping 功能
三层功能	支持 RIP、RIPng、OSPF、OSPFv3 路由协议
	支持 IPv4 FIB 表项≥4K
堆叠	支持智能 iStack 堆叠，将多台支持堆叠特性的交换机组合在一起，从逻辑上虚拟为一台交换机
组播	支持 IGMP v1/v2/v3 Snooping 支持 VLAN 内组播转发和组播多 VLAN 复制 支持捆绑端口的组播负载分担 支持可控组播 基于端口的组播流量统计
安全	支持防止 DOS、ARP 攻击功能、ICMP 防攻击 支持端口隔离、端口安全、Sticky MAC 支持 IP、MAC、端口、VLAN 的组合绑定
	支持 DHCPv6 Snooping，DAI，SAVI 等安全特性
可靠性	支持以太网环网保护协议 ERPS，故障倒换时间小于 50ms
虚拟化	支持纵向虚拟化，作为纵向子节点零配置即插即用
QOS	支持对端口接收报文速率和发送报文速率进行限制 支持 SP、WRR、SP+WRR 等队列调度算法 支持报文的 802.1p 和 DSCP 优先级重新标记
管理维护	支持 SNMP v1/v2/v3、Telnet、RMON 支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理
	支持 Telemetry 技术，配合网络分析组件通过智能故障识别算法对网络数据进行分析，精准展现网络实时状态，并能及时有效地定界故障以及定位故障发生原因，发现影响用户体验的网络问题，精准保障用户体验

3.7.3 网管软件

指标项	详细指标
管理规模要求	系统应支持大规模设备管理能力，可最多管理 20,000 台网元。
管理范围要求	系统应支持多种设备的管理，包括交换机、路由器、防火墙、WLAN、服务器、存储、操作系统、数据库、WEB 应用、摄像头、GPON 设备。

系统架构要求	系统使用 B/S 架构，支持使用 WEB 浏览器进行界面展示。
系统安全性要求	系统提供分权分域功能，为不同的用户、角色分配不同的设备管理范围和操作权限。
	系统应支持本地、RADIUS 和 LDAP 用户认证管理，实现用户的集中管理。
	系统提供系统日志、操作日志、安全日志。
系统开放性要求	系统提供三种北向接口（SNMP、FTP 及 Restful 接口），可通过北向接口向上层系统提供告警、性能以及资源数据。
	系统应支持多种南向接口类型，包括 SNMP、STelnet、FTP（服务端）、SFTP（客户端/服务端）、IPMI、HTTP（客户端）/HTTPS（REST/Redfish 客户端、服务端）、LwM2M、WebSocket、SocketPing、ICMP、WebPing、WebTrace、SSDP 接口，方便管理多种设备类型。
资源管理要求	支持将添加后的资源（如服务器、网络设备、存储设备等）进行分类和分组管理，用户通过配置不同的分组类型和分组将资源划分为不同类型以及不同分组。
	直观展示网络设备之间或者服务器设备之间的链路连接，并支持对链路进行发现、监控和配置。
	提供统一的设备远程上下电平台，对接入的服务器和存储设备可实现一键式上下电操作。
拓扑管理要求	系统应支持过滤显示拓扑视图、查看全景图等功能，用户可以及时监控所关注的拓扑节点状态和了解拓扑视图全貌。
	系统应支持用户在拓扑视图上添加图形、文本和容器等对拓扑对象进行可视化的组织、标记和描述，以方便运维管理。
	系统应支持刷新、导出拓扑视图，用户可以获取拓扑对象的最新状态，并查找和二次编辑拓扑对象，实现拓扑变化情况可视化管理。
	系统应支持创建自定义拓扑，用户可以将自己重点关注或管辖范围内的网元添加到自定义拓扑，以进行精准监控，实现高效运维。
故障管理要求	系统应提供多领域、多厂商数据采集能力，包括从下层第三方系统采集网元的告警信息，并将告警集中显示在告警面板中。
	提供了多样化的告警过滤方式，帮助运维人员快速筛选所关注的告警，提高监控效率。
	系统应支持灵活的告警规则配置，将海量的告警进行关联和压缩，减少告警噪声，实现精准监控。
	系统应提供紧急、严重、次要、提示四个等级来表达告警的紧急程度，帮助运维人员快速识别告警的重要程度，以采取相应的处理策略。
性能管理要求	系统支持对设备的关键性能指标进行监控，并对采集到的性能数据进行统计，方便用户对设备性能进行管理。
	支持通过设置不同的性能阈值，生成 4 级不同级别的告警：紧急、重要、次要、提示。
	支持查看指定设备、指定指标的历史性能数据，以了解设备历史性能趋势。
	支持监控设备的实时性能数据，了解设备的运行状态，以便确认设备是否存在异常，支持将查询结果导出到 excel 文件。
报表管理要求	支持用户拖拽式自定义报表内容，运用钻取、旋转、切片等操作，实现业务数据的灵活展现和统计汇总，提供自助式数据同比、环比、TOPN 等分析功能。
	支持根据用户设定的周期自动生成报表，可以通过 Email 发送，也可以手动导出

	Excel、PDF 格式的报表。
网络资源管理要求	系统应支持一站式网络设备（包含交换机、路由器、防火墙、AC 等设备）仪表盘，通过设备、部件、仿真面板、运行状态等关键信息的集成显示，帮助运维人员快速全方位了解设备。
网络报表模板要求	系统应支持网络设备类型、设备 CPU 利用率、内存使用率统计、接口流量、链路流量、端口使用率等统计报表
配置文件管理要求	系统提供全网设备的配置文件管理，可以提供即时和周期的配置文件备份，支持对已备份的配置文件进行基线化、恢复和比较。
配置工具要求	系统应支持用户自定义配置模板或者导入规划表方式批量下发设备配置。
网络质量检测	系统应支持主动在网络设备之间发送诊断报文，测量线路上的丢包率、时延、抖动等关键性能指标。
	系统默认提供 ICMP Echo、ICMP Jitter、UDP Echo、UDP Jitter、DNS、DHCP 等常用测试 用例。
网络流量分析	系统应支持实时监控全网流量，提供多维度 TOPN 流量分析报告，帮助用户及时发现网络中异常流量、了解网络带宽的使用情况。
	系统应支持钻取式流量分析能力，用户可通过选择查看条件，查看需要关注的流量信息。系统提供了链路接口流量、应用流量、主机流量、会话流量、设备流量等维度的 TOPN 流量分析能力。
WLAN 网络管理要求	系统应支持对接主流规划工具，可快速导入网规数据，仿真楼栋、楼层、障碍物规划，实现信号覆盖可视。
	系统应支持 WLAN 网络 DASHBOARD 运维，包括概览、TOP AP 统计、流量趋势、用户趋势、TOP 区域统计等。
	系统应支持 WIDS 管理，探测无线网络中的非法设备/客户端、干扰源和攻击，并通过告警通知运维人员。
	系统应支持一键式故障检测，从终端、空口、AP、AC、连通性、AAA、DHCP 七个维度识别问题并提供故障原因和修复建议。
	系统应至少提供 AP 在线时长报表、在线用户趋势报表、AP 接口统计报表、用户明细报表等 WLAN 运维报表等报表，为网络运维提供优化依据。
操作系统监控	系统应支持查看操作系统状态、名称、IP 地址、子网、OS 版本、物理内存、厂商等。
	系统应支持详细展示操作系统的基本信息（名称、IP 地址、发行版本、OS 版本、内核版本等）、告警信息、分区列表、进程列表和网卡列表信息、协议参数。
	系统应支持监控操作系统的系统连通性、CPU 利用率、内存利用率、磁盘利用率、磁盘分区利用率以及网络连接数。
数据库监控	系统应支持查看数据库状态、名称、IP 地址、子网、端口、类型、驱动名称、DB 版本、厂商等。
	系统应支持详细展示数据库的基本信息（状态、名称、IP 地址、子网、端口、类型、驱动名称等）、告警信息、协议参数。
	系统应支持监控数据库的系统连通性、连接响应时间、连接数、连接数已使用百分比、内存使用信息以及命中率信息。
WEB 应	系统应支持查看 Web 应用状态、名称、IP 地址、子网、端口、类型、版本等。

用监控	系统应支持详细展示 Web 应用的基本信息（状态、名称、IP 地址、类型等）、告警信息、协议参数。
	系统应支持监控 Web 应用的系统连通性以及响应时间。

3.8 离线备份磁带库

技术指标项目	技术指标参数
磁带库整体要求	智能化磁带库，冗余设计，采用具有完全知识产权的产品，原厂生产，非 OEM 或贴牌产品
磁带库支持的磁带机驱动器技术	支持目前主流的 LTO8 磁带机技术
磁带库最大磁带机数量	>=24（单台磁带库非级联时最大磁带机数量）
磁带库最大槽位数量	>= 400
配置的磁带机驱动器类型	LTO8 FC 8Gb 磁带机
单台磁带机非压缩数据传输速率	>= 300MB/S
磁带机配置数量	>=2 台
配置的数据磁带类型	LTO8 数据磁带
单盘磁带非压缩存储容量	>= 12TB
数据磁带配置数量	>=25（含磁带标签）
LTO 通用清洗带数量	>=1
磁带库实际槽位	>=25（可以根据 25 槽位的倍数增加，最大可配置到 400 槽）；
磁带库分区及混合磁带介质管理功能	支持磁带库分区以及混合磁带介质管理功能，且不需要额外主机和软件实现此功能
磁带库最大分区数量	>= 12
系统连接方式	8Gb FC SAN
磁带库放置方式	落地式，可安装标准服务器机柜
磁带库扩展	支持多单元堆叠扩展模式
机械臂可靠性	平均无故障磁带装载次数 >= 2,000,000 次
平均故障修复时间(MTTR)	<=30 分钟
电源可靠性	必须要求配置 2N 全冗余电源系统，电源和风扇模块可以在线插拔和更换
磁带机磁头可靠性	平均无故障时间>=60,000 小时
远程管理功能	与操作面板完全一致的图形化管理界面，可以实时显示磁带库内部的操作情况，如磁带加、卸载次数、磁带读、写的数据量、磁带机的温度等参数
内置支持存储管理协议 SMI-S，便于 SRM 存储资源管理软件管理	要求在不额外配置外置的软硬件的前提下，直接支持该功能。
系统兼容性	必须支持主流的 UNIX 操作系统如 IBM AIX、HP UX 等，以及主流的备份软件 Symantec NBU、CommVault、IBM TSM、HP DataProtector

3.9 综合安全服务（含 2 人现场驻点 1 年服务）

序号	服务内容	内容简述	时间（年）	服务频率
1	渗透测试服务	通过真实模拟黑客使用的工具、分析方法来对网站进行模拟攻击，并结合智能工具扫描结果，由高级工程师进行深入的手工测试和分析，识别工具弱点扫描无法发现的问题。	1	1 次
2	安全漏洞检测服务	提供漏洞扫描工具对服务范围内各种软硬件设备进行网络层、系统层、数据库、应用层面的扫描与分析，扫描设备检测规则库及知识库应涵盖 CVE、 CNCVE、 CNVD、CNNVD 等标准。	1	4 次
3	协助安全加固	根据安全评估结果的具体情况，制定加固建议，协助进行安全加固处理，合理加强服务目标的安全性。	1	1 次
4	漏洞跟踪管理服务	漏洞监测及加固期间，提供漏洞跟踪管理工具，自动跟踪漏洞趋势，漏洞修复情况展示，实现漏洞闭环处置。	1	4 次
5	安全巡检数据分析服务	对医院的安全情况、安全设备运行状况进行定期现场检查，掌握医院存在的安全隐患，及时落实修补措施，并提供巡检报告。	1	4 次
6	业务系统运行质量分析服务	提供业务系统运行质量分析工具，系统数量不限，支持业务拓扑自动发现、业务响应时效、业务响应质量等分析维度，服务工具由供应商提供；提供《应用系统运行质量分析报告》	1	12 次
7	全网资产梳理服务	提供资产梳理工具，对全网信息资产进行全面排查梳理，包括服务器、PC、打印机、扫描仪、网络设备等等。输出《资产分析表》	1	2 次
8	敏感文件泄露监测服务	对企业、单位网站发布的文件中是否含有用户信息等敏感文件进行监测，包括 excel 、txt 等类型的文件。	1	2 次
9	Web 应用系统可用性检测服务	定期检测 Web 应用系统的可用性情况，监测站点的 DNS 解释是否正常	1	2 次
10	应急响应服务	在发生安全事件后进行 7×24 小时应急响应，快速协助进行系统恢复，尽可能降低安全事件对系统的正常运营所造成的影响，同时对安全事件进行分析，查找事件原因，对其中存在的安全隐患进行规避。	1	4 次
11	安全事件通	根据目前的信息安全形势，实时提供应用	1	不限

	告	安全相关漏洞的安全通告以及解决方案。		
12	安全培训服务	安全知识培训及其他项目实施中必要的培训。	1	1 次
13	安全人员驻场值守服务	**提供 2 名网络安全驻场人员，驻点办公地点为医院信息科，驻点时间与信息科上班时间一致，节假日需安排值班**，具备安全数据监测分析驻场服务经验，进行网络安全监控、风险分析、问题处理。驻场经理应该同时具备 PMP 认证、CISP 认证、CISAW, 等保专业从业人员认证，协同驻场人员应具备 NISP 或 CISP 认证。	1	2 人
14	勒索病毒保险	针对勒索病毒场景，当信息系统遭受勒索病毒攻击被加密时，根据保单约定责任范围赔偿如应急响应费用、数据修复费用、勒索损失等。	1	1 年

4. 需注明各项售后服务情况

本项目为连贯一个集体，供应商必须提供一套完整实施方案，包括外内网拆分工程实施方案，整体网络安全设备的规则整理设置，调优等方案。综合安全服务为项目验收后 1 年，其他为验收后提供 3 年所投产品质保服务（质保服务含硬件保修、软件升级维护、策略库升级维护服务）。