第四章　采购人需求

第一节　技术参数

序号	设备名称	技术参数要求	数量	单位	备注
一、物理环境					
1	消防系统	气体消防、FM200,柜式七氟丙烷无管网系统 70 升装置，含光电感烟、感温探测器和声光报警器，气体灭火控制器、紧急启停按钮等	1	套	
2	机房动环监控系统	配置机房门禁、UPS、空调、配电系统、漏水、温度、湿度、视频监控检测系统	1	套	
3	机房基础环境改造	机房墙壁、吊顶防尘处理，基础装修改造，配置 1 拖 6 一体化机柜	1	套	
二、安全产品					
4	防火墙	1.采用非 X86 64 位多核高性能处理器和高速存储器；主控模块内存≥4G；2U 以下盒式设备； 2.★≥8 个千兆光口+16 个千兆电口；整机最大可扩展接口数量 8SPF+24GE； 3.扩展要求：≥2 个扩展槽位，可扩展 4GE Bypass 功能接口； 4.★最大并发连接数≥400 万；IPSec VPN 并发连接数≥2000；每秒新建连接数≥50K；整机大包吞吐量≥2.5Gbps；整机混合包吞吐量≥2G；整机 DPI 深度防御吞吐量≥2G；3DES 加密≥2G；AES256 加密≥2G；	2	台	专网边界 内外网边界

		5.可靠性要求：支持 VRRP 的链路备份支持双机集群式高可靠性技术，融合后可统一管理配置，对外单一节点，单 IP 并实现主备/主主方式转发； 6.支持基于 CPU、内存等硬件划分资源的完全虚拟化技术,可分配吞吐量、新建、并发，虚拟防火墙可独立重启、配置独立导出，虚拟防火墙数量≥16 个； 7.★免费支持高性能 IPSec、L2TP、GRE VPN、SSL VPN 功能；能够实现与 L2TP over IPSec 与安卓、ISO 系统自带 VPN 组件对接；提供客户端与安卓、IOS、Windows、Linux、MAC 对接，支持 BYOD 解决方案；配置≥15 并发 ssl vpn 授权许可。 8.支持链路负载均衡功能、服务器负责均衡功能； 9.支持 IPv6：IPV6 状态防火墙、IPV6 动态路由协议、IPV6 攻击防范； 10.单台配置：内置双交流电源及一块 500G 硬盘；含 3 年 AV 防病毒安全 License，含 3 年 IPS 特征库升级服务；			
5	内网网络改造	核心交换机： 1. 采用高可靠的模块化设计方式，要求所有接口板必须是分布式转发工作模式，业务模块插槽数≥3 个； 2. 交换容量≥19Tbps，包转发率≥2800Mpps； 3. ★支持千兆电口、千兆光口、10GE 端口、40G 端口、支持拓展 EPON OLT 接口板，提供官网截图或第三方检测报告； 4. ★支持多虚一技术，将两台物理设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理，跨物理设备的链路聚合，提供第三方测试报告； 5. ★支持一虚多技术，支持多虚一技术和一虚多技术的配合使用，提供第三方测试报告； 6. ★支持扩展硬件防火墙业务板插卡、网络流量统计分析业务板插卡(业务板订购信息须在产品原厂商官方网站上公布,并提供网址与截图作为证	2	台	

		明文件加盖投标人公章）； 7. ★支持跨数据中心二层互联技术,提供官方网址链接与截图； 8. 支持 FCoE 接口、OLT 接口；支持 VXLAN 网关； 9. 支持 RIP、OSPF、BGP、ISIS、OSPFv3、ISISv6； 10. 支持命令行接口（CLI），Telnet，Console 口进行配置；支持 SNMPv1/v2/v3； 配置要求： 11. 每台配置冗余主控、冗余电源,24 个千兆电口、24 个千兆光口、8 个万兆光口，配置 4 个万兆多模光模块、12 个千兆单模光模块；			
		楼层接入： 1. 交换容量≥330Gbps，包转发率≥96Mpps； 2. 提供千兆电口≥24 个，千兆 SFP 光口≥4 个； 3.★ 实现 ERPS 功能，能够快速阻断环路，链路收敛时间≤50ms 要求提供权威机构颁发的测试报告 4. 支持基于端口、VLAN 下发 ACL； 5. 支持 IPv4 静态路由、RIP，支持 IPv6 静态路由，OSPF； 6. ★贵州多雷雨天气，为保证防雷，要求端口支持≥10KV 防雷，要求提供官网截图证明及链接并加盖鲜章； 7. ★支持 Smart Link，可以实现双上行组网，提供可靠的链路备份、负载分担和快速收敛，提供第三方测试报告； 8. ★支持 CPU 保护功能，能限制非法报文对 CPU 的攻击，保护交换机在各种环境下稳定工作，提供第三方测试报告； 9. 支持虚拟电缆检测 VCT；； 10.支持 Console/Telnet 命令行配置；支持 SNMP V1/V2c/V3 11.提供工信部入网许可证复印件； 12.配置 2 个单模模块	6	台	

6	堡垒机	1.标准 1U 硬件，千兆电口≥6 个,硬盘≥1T，1*RJ45 串口。 2.支持资产数≥100 个运维。 ★3.支持基于不同的用户设置不同的双因子认证模式,如 user1 用动态令牌、user2 用 USBkey、user3 手机 APP 动态口令认证（提供截图证明并加盖投标人公章）。 ★4.支持自动收集设备 IP、运维协议、端口号、账号、密码、与用户的权限关系，甚至可自动完成授权 （提供截图证明并加盖投标人公章）。 5.设备信息文件支持加密导出，导出的设备信息文件加密存储， 解密时须由 2 个管理员同时解密才能查看到设备信息文件内容。 6. 支持保存 RDP 磁盘映射传输的原始文件。 ★7.支持 DB2、oracle、mysql、sqlserver 主流数据库协议代理运维，可直接调用 本地 windows 系统的数据库客户端工具，支持自动登录、无需应用发布前置机（提供截图证明并加盖投标人公章）。 ★8.支持使用本地的 SecurCRT/Xshell/OpenSSH 工具通过 SSH 网关代理方式直接登录字符设备（提供截图证明并加盖投标人公章）。 9 支持在 mac 电脑里使用 navicat 工具通过堡垒机登录 mysql、oracle 等数据库服务器 10.审计日志：支持对 oracle/mysql/sqlserver/DB2 运维产生的 SQL 语句进行记录。 11.安全联动：支持和同品牌数据库审计系统进行联动，将通过 SSH/RDP 等加密方式操作数据库的行为整合到数据库审计中,实现数据库行为的统一集中查询、展 示、审计分析等。 12. 支持认证窗口的全局设置：可以选择启用哪种或者哪几种认证登录窗口。 13. 支持批量登录字符设备功能：能自动生成 SecurCRT/Xshell 工具的批量登录文件，实现在工具中批量登录多台设备。	1	台	

		14. 支持对设备进行按设备类型分组、按部门分组，支持设备批量导入/导出。 15. 支持对 RDP 屏幕文字内容、标题窗口、键盘输入的记录和搜索定位。			
7	日志审计	1. 支持审计 100 个日志源；平均处理能力（每秒日志解析能力 EPS）：5000EPS；电口≥4 个，1 个 console 口；内存≥16GB，磁盘≥4T ★2.用户支持双因子认证登录,双因子认证令牌支持绑定至具体用户。(提供截图证明并加盖投标人公章） 3.支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等 ★4. 注册用户资产时，提供自动发现识别能力 （提供截图证明并加盖投标人公章） ★5. 采用解决方案包上传对产品进行功能扩展，无需要代码开发，内置非法访问、可疑入侵、病毒爆发、设备异常、弱点针等不少于 50 种安全分析场景（提供截图证明并加盖投标人公章） 6.内置 SOX、ISO27001、WEB 安全等解决方案包 ； ★7. 支持 kafka 日志接收转发、大数据安全域同步、APT 沙箱报告转发等大数据联调功能（提供截图证明并加盖投标人公章）； 8. 支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作对象、技术方式、技术动作、技术效果、攻击类型、地理城市等参数进行过滤查询 ★9. 支持磁盘空间阈值告警，当磁盘使用率达到设定的阈值时可产生并外发告警（提供截图证明并加盖投标人公章）； ★10. 三维关联分析；支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件。（提供第三方检测报告） 11. 支持常见的虚拟机环境日志收集，包括 Xen、VMWare、Hyper-V 等。 ★12.支持资产拓扑图，资产拓扑支持按照实际的用户环境进行编辑发布	1	台	

		并可以和资产进行绑定。拓扑可以显示资产采集的事件数量被采集资产的状态等信息。（提供截图证明并加盖投标人公章）。 13. 支持如下应用的性能监控（Windows、Linux、Aix、FeeBSD、HP-UX/Tru64、Max OS、Sun Solaris）、数据库（mysql、oracle）、应用服务器（weblogic、tomcat）、web 服务器（apache） 14. 支持报表导出为 PDF 和 Word 格式文件			
8	数据库审计	1. 配置需求：标准机架式硬件架构，软硬件一体化系统；网口数量≥6*100/1000M 电口，硬盘存储：1TB SATA 企业级。 2. 处理能力：峰值事件处理能力≥5000 条语句/秒，日志存储≥8 亿条，吞吐能力≥2GB。 3. ★支持 Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、达梦等传统数据库的审计，支持后关系型数据库 Cache 的 5 种工具审计。 4. 系统包括审计引擎及管理后台软件、策略管理、告警管理、权限管理、系统日志、系统配置等功能，可同时支持审计多个不同类型的数据库,审计数据统一存储、查询、分析、统计。 5. 系统支持分布式部署方式，可支持防统方集中管理功能及上联接口，方便区域性管理及防护策略的落实。 6. ★支持后关系型数据库 Cache 的集成工具 terminal、portal、studio、Sqlmanager、MedTrak 工具的审计，其中 Portal 能审计到 sql 语句、查询 Global、返回结果，Terminal 能审计到 M 语句和返回结果。（提供截图证明并加盖投标人公章） 7. ★数据库安全功能：支持数据库绑定变量审计、函数审计(sum 求和函数等）；支持对 SQL 注入、跨站脚本攻击等 web 攻击的识别与告警；支持操作语句系列的组合审计规则，可根据某一客体的操作行为序列，连续操作了设定的语句序列时进行规则审计告警；支持重复操作的统计审计规	1	台	

		则，可根据在一定的时间内，重复某项操作达到设定的统计次数进行规则审计告警。（提供截图证明并加盖投标人公章） 8. 支持超长操作语句审计，针对传统型数据库，支持 3 万字节审计而不截断，支持对执行时间长达 48 小时操作的审计。 9. 支持端口重定向的审计。 10. 支持对 Telnet、FTP、POP3 协议审计，针对 FTP 能审计到内容。 11. 支持 B/S、C/S 应用系统三层架构 http 应用审计，可提取包括 IP、MAC、操作系统名称、操作系统账号、数据库账号、应用系统账号（工号）的身份信息，并可获取 XML 返回结果。 12. 支持带 COM、COM+、DCOM 组件的三层架构应用审计，可提取包括 IP、MAC、端口、操作系统名称、操作系统账号、数据库账号、应用系统账号（工号）的身份信息。 13. 在无需重启被审计数据库的情况下，支持对 MS SQLSserver 加密协议的审计，可正常审计到数据库账号、操作系统用户名、操作系统主机名等身份信息。 14. ★支持虚拟化平台环境的数据库审计，满足后续系统架构建设要求（提供截图证明并加盖投标人公章）			
9	上网行为管理	1.采用非 X86 架构，功能采用模块化结构设计； 2.设备固化千兆电口≥12 个、千兆光口≥12 个； 3.网络吞吐量≥5Gbps； 4.内置存储硬盘≥1TB，内置双电源； 5.支持路由模式、透明（网桥）模式、混合模式，部署模式切换无需重启设备； 6.支持静态路由、策略路由、 RIP、 OSPF、 ISP 路由，其中 ISP 路由支持自定义，并可提供基于应用的策略路由； 7.★支持 3G 扩展，支持电信、联通等主流 3G 网卡。支持 3G 接口的常			

		在线和按需上线模式，并支持在 3G 接口上运行 IPSec VPN，（提供 web 配置界面截图并加盖投标人公章）； 8.支持基于带宽和优先级的多链路负载均衡，可支持链路过载保护； 9.支持主流 P2P、 IM、在线视频、网络游戏、网络炒股等应用识别； 10.支持智能和快速识别模式配置，当网络流量过大时，可切换“优先应用识别模式”或“优先保障性能模式”； 11.支持自定义关键字对象，在应用控制的时候可选择“包含”、“不包含”、“等于”、“不等于”四种匹配模式，匹配类型包含关键字和数字； 12.★支持即时通讯应用管控的精细化管理，可管控微信的“位置分享”、“朋友圈”、“附近的人”、“摇一摇”、“漂流瓶”、“收发文件”、“收发消息”、“登陆注销”等行为，（提供 web 配置界面截图并加盖投标人公章）； 13.★支持基于某个用户的 QQ、微信、淘宝等虚拟账号关联汇总，可对某个用户一天的上网行为轨迹以时间轴方式进行呈现，（提供 web 配置界面截图并加盖投标人公章）； 14.支持收集网站访问日志，记录用户所有访问网站行为；支持收集搜索引擎日志，记录用户的搜索内容；支持收集 IM 通讯软件日志，记录用户登陆、注销、收发消息、收发文件等行为；支持收集邮件日志，记录邮件发件人、收件人、主题、正文、附件等信息； 15.支持通道化的 QoS，支持基于源地址、用户、服务、应用、时间进行带宽控制，并支持配置保障带宽、限制带宽、带宽借用、每 IP 带宽、带宽优先级等 QoS 动作，时间选择支持基于日计划、周计划、单次计划等； 16.★支持 4 级层次化 QoS、支持多级用户/用户组嵌套，（提供 web 配置界面截图并加盖投标人公章）； 17.支持微信认证； 18.★支持对指定 URL 的文件内容进行缓存加速,需缓存文件可手动上传			

		及更新；可查看缓存可用空间和命中次数，（提供 web 配置界面截图并加盖投标人公章）； 19.web 管理界面支持 Ping、 Traceroute、 TCP Syn 诊断工具，可支持基于接口、协议、 IP 地址、端口、应用进行网络抓包，并可下载导出分析； 配置要求： 21.每台配置 3 年特征库升级服务授权；			
10	终端安全管理	1、终端安全一体化 功能一体化：集终端防病毒和安全管控于一体的终端安全管理系统 平台一体化：完美兼容 Windows、Linux、国产操作系统 数据一体化：结合云端大数据和威胁情报，有效感知本地安全态势 2、病毒防御多维化 多引擎技术：拥有领先的云查杀引擎、系统修复引擎、QEX 脚本查杀引擎、启发式引擎、QVM 人工智能引擎，有效查杀已知和未知病毒 立体化主防：具备隔离防护、5 层入口防护、7 层系统防护及 8 层应用防护等主动防御技术 智能自学习：通过海量病毒样本数据自学习，QVM-II 人工智能引擎无需频繁更新特征库、病毒检出率仍远超传统查杀引擎 安全管控智能化 资产管理：自动识别全网终端资产信息，实时监控系统状态并告警，保障业务连续性 安全策略管理：通过非法外联、外设管理、进程控制、主机防火墙、桌面安全加固等多元化方式，提升终端安全等级 漏洞补丁管理：对全网终端漏洞进行扫描并关联，根据终端分组或操作系统类型错峰下发补丁 网络安全准入：支持旁路应用准入、802.1x 准入及其它多种准入技术，	1	套	

		对不满足安全性检查的终端不予接入网络,并引导到修复区进行安全修复 本次配置含 1 控制台，300 个终端，10 个服务器端			
11	备份一体机	1. 产品提供软件著作权登记证书，计算机信息系统安全专用产品销售许可证及涉密信息系统产品检测证书。提供相关证明材料。 2. ★ linux 嵌入式备份设备，标配 1 颗 8 核存储专用处理器，支持自适应 1+1 冗余电源，配置≥32G 高速缓存，2 个千兆网络接口。硬件 RAID，支持企业级 SAS 与 SATA 混插,设备系统和软件安装嵌入在 2 块 120GB SSD 固态硬盘上,不占用自身硬盘的存储空间。本次配置 5 块 6TB 企业级硬盘； 3. 支持自动监控备份节点服务状态，当备份节点出现故障时，会自动将受故障影响的备份任务分配到正常工作的备份节点上执行.。支持 Web 请求负载均衡,对于并发的大批量 Web 请求,会自动分发给不同的备份节点,提升性能。支持备份任务负载均衡，高并发的数据备份任务在调用存储系统和重删服务分配存储节点和重删节点时，实现负载均衡，确保海量数据备份、高并发备份的性能。 5. ★配置 SAP HANA、MongoDB、Postgresql、SQL Server、MySQL、Sybase、Oracle、Exchange Server、DB2 与 Lotus Domino、达梦、神舟、人大金仓数据库等在线备份保护，提供四种以上数据库厂商兼容证明材料； 6. ★支持 Oracle10、11、12、18、19 等版本 Oracle 单机、Oracle RAC、HA 等架构的实时备份，支持按任意版本恢复，支持任意时间点数据恢复(要求提供软件功能截图并加盖投标人公章)； 7. 当生产服务器出现故障时，可通过容灾服务器在线接管生产服务器业务，确保应用连续性；当生产服务器修复正常后，可以支持将接管后的容灾服务器的数据恢复到生产服务器； 8、支持对 Vmware vSphere ESX/ESXi 虚拟化平台的备份，支持对 Vmware vCenter 管理的虚拟化平台的备份，支持并发配置备份策略、并发备份和	1	套	

		并发恢复。(要求提供软件功能截图并加盖投标人公章) 9. 配置不限制客户端数量通过 API 接口直接对 Vmware vSphere ESXi、Microsoft Hyper-V、RHEV、XenServer、浪潮 InCloud Sphere、Fusion Sphere、H3Cloud、CAS、Openstack、云宏主流国内外虚拟化应用无代理定时备份保护功能授权; 10. 采用 https（SSL）加密登录方式。具备系统管理员、审计管理员、安全管理员三权角色分立。(要求提供软件功能截图并加盖投标人公章)			
12	集群软件	利用现有服务器，将服务器组建虚拟化集群	1	套	
13	数据库迁移	现有数据库及应用系统迁移至集群平台内	1	次	
三、安全集成与服务					
14	安全集成服务	整合本次设计采购的各安全设备和系统,协调各系统和设备厂商完成产品部署实施与上线运行。	1	次	
15	管理制度建设	依据等保三级管理体系的要求，补充完善医院的管理制度体系。	1	次	
16	系统加固服务	由专业安服人员对测评范围内的设备、主机等资产提供安全加固服务。	1	次	
17	安全培训	本次整改过程方法论和主要安全系统使用维护培训。	1	次	