采购需求

一、项目名称

信息管理系统等级保护整改

二、项目概述

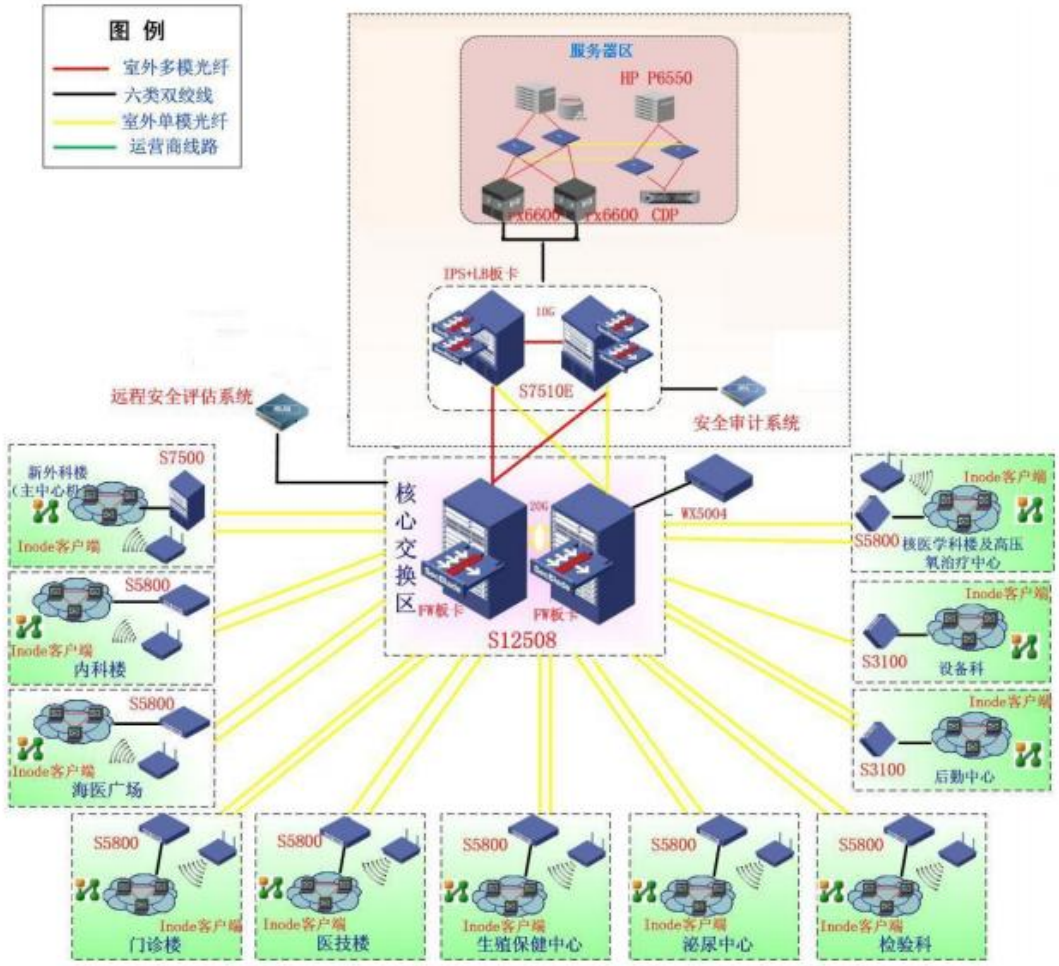
随着信息化应用水平的不断深入和提高，国家和海南医学院第一附属医院自身对信息安全的重视程度和相关要求也越来越高，在此背景下，受海南医学院第一附属医院的委托以《信息技术信息系统安全等级保护基本要求》和《信息技术信息系统安全等级保护测评要求》为基础，依据《信息安全技术信息系统安全等级保护测评过程指南》分别从安全技术类物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复五个层面和安全管理类安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理等五个方面，对海南医学院第一附属医院信息管理系统的安全保护现状进行了客观的访谈和检查。

为达到国家 GB/T 22239-2008《信息技术信息系统安全等级保护基本要求》相应的等级保护能力要求，需对海南医学院第一附属医院信息管理系统启动等级保护安全整改工作的建议与规划方案，以增强系统的安全防护能力，有效抵御内部和外部威胁，切实达到国家及行业信息安全等级保护相应要求，使海南医学院第一附属医院信息管理系统在现有运行环境下风险可控，能够为海南医学院第一附属医院客户及内部各部门提供安全、稳定的业务服务。保证海南医学院第一附属医院相关业务系统达到系统定级相应的等级保护能力要求。

三、项目需求

（以下参数中标注有“★”号的条款必须实质性响应，负偏离（不满足要求）将导致投标无效；“▲”号的条款为重要技术要求，响应程度将影响技术得分。）

（一）海南医学院第一附属医院目前网络结构



信息系统服务器部署在内网服务器区，在网络边界处部署 H3C 板卡防火墙实现基本的安全防护，配备绿盟审计系统实现网络审计，配备绿盟远程安全评估系统进行漏洞扫描，H3C S7510E 交换机上配备 LB 板卡但未启用；各业务科室的无线路由均隐藏 SSID 且绑定 MAC 地址。

（二）系统情况

医院信息管理系统由海南医学院第一附属医院负责建设，目前部署在外科楼十六层的信息中心主机房，由海南医学院第一附属医院信息中心负责技术支撑及运维。海南医学院第一附属医院是该系统的主管单位，同时也是定级的责任单位。该系统实现入院管理、院长查询、住院发药、综合维护、药房管理、药库管理、护士工作站管理、出院管理、门诊发药、门诊收费、手术管理等方面。该系统的保护等级为三级（S3A3G3）。

（三）安全责任制落实情况

单位配置有信息安全领导小组、信息系统负责部门及人员，明确了相关责任部门及人员的信息安全职责，但未制定信息系统建设发展规划文件，存在没有授权审批方面的制度等问题。不利于建立信息安全长效机制，落实信息安全措施，切实履行好信息安全保障责任。

（四）安全管理制度体系建设情况

单位安全管理制度体系建设仍有待进一步完善，当前制定了涵盖物理、网络、主机、应用、数据等方面的安全管理制度。但未制定信息安全总体方针文件，且部分制度存在结构与内容不全面，缺少各岗位操作规程文件（如安全管理员、网络管理员、系统管理员、主机审计员、数据库管理员、机房管理员以及安全审计员等），未定期对安全管理制度体系的合理性和适用性进行审定，不利于保障信息系统的有效运转和信息安全管理工作的开展。

（五）基础设施与网络环境

单位现已建有专用的信息中心主机房，位于外科楼十六层，采取了防雷、防盗、防火、防静电等措施，并配备了电子门禁系统和视频监控，对出入机房的人员进行严格的访问控制；机房配备了 UPS 设备、备用供电系统以及冗余电路，能够保证系统电力供应安全要求；相关申请审批单及运行维护记录保存完整，机房安全措施落实到位。

网络环境方面，单位在网络边界部署了防火墙作为基础防护，主要网络设备提供硬件冗余有效保障系统的高可用性；数据中心部署了 IPS。但重要服务器设备缺乏防毒墙的防护设备，存在一定的安全隐患。

（六）安全控制措施实施情况

在主机安全层面，管理员对服务器和数据库设置了较强的口令，但未定期更换口令；策略上存在的问题主要有未启用登录失败处理功能、未启用登录操作超时锁定功能、以及安全审计功能未开启或开启后未定期对日志记录进行分析、未采用双因子认证进行身份鉴别等；

在应用安全层面，系统具有身份鉴别功能和安全审计功能，在系统访问上做了严格的访问控制，起到了基本的安全防护作用，但系统缺乏口令复杂度设置和登录失败处理功能。另系统在通信完整性、保密性、抗抵赖上的功能也存在不足。

另外，通过扫描发现服务器存在高危漏洞，存在较大的安全风险。

（七）系统建设管理情况

当前信息系统已经建成投入使用，本系统明确了安全保护等级并到相关部门进行备案，建设阶段的重要过程文档有工程实施方案、验收报告及交付清单等；但系统建设方面的管理制度仍有缺失，主要体现在缺少工程实施、测试验收以及系统交付等方面的管理制度，不利于对信息系统的建设情况进行统一管理及整体把控。

（八）系统运维管理情况

本信息系统有专人负责日常运维管理，与本信息系统相关联的服务器、数据库、应用系统等均有指定专人或运维商进行统一管理。

在日常运维过程中，缺少相关岗位操作规程及部分记录文档等内容，对系统日常补丁升级、漏洞检查、安全审计记录、恶意代码防范等缺乏统一有效的监管，在系统变更、安全事件处置等方面的管理制度不够完善，制定了应急预案但未进行定期演练。

在数据保护方面，缺乏成文的备份恢复策略指导文件，不利于出现紧急事件时有序的进行应急处理。

综合上述评价结果，本信息系统的总体安全保护状况相对等级保护基本要求有一定的差距，需进一步完善。

（九）主要安全问题

（1）网络层面

1、未部署防毒墙等安全防护设备保护信息系统安全，可能增加被攻击者入侵的风险。

2、未采用两种或两种以上的组合鉴别技术对网络设备用户进行身份鉴别。

3、网络设备未启用登录失败处理功能。

4、部分设备采用明文传输协议 telnet 进行远程管理。

（2）主机层面

1、登录系统用户未采用两种或两种以上的身份鉴别技术对用户身份进行鉴别，采用单一认证方式时，如口令被窃取、监听或暴力破解，则可能被攻击者冒用身份。

2、操作系统和数据库未启用口令复杂度功能，未启用登录失败处理功能，攻击者在网络中任何可达位置对设备用户名、口令进行暴力猜解，造成身份冒用。

3、未对系统日志记录以及定期保存及分析，无法及时发现异常情况。

4、对服务器进行远程管理时，未采取加密措施。

5、系统管理、安全管理以及安全审计等特权用户权限未进行分离。

6、服务器及运维终端未支持恶意代码防范的统一管理，可能会受到木马、蠕虫等病毒的攻击。

（3）应用层面

1、登录系统用户未采用两种或两种以上的身份鉴别技术对用户身份进行鉴别，采用单一认证方式时，如口令被窃取、监听或暴力破解，则可能被攻击者冒用身份。

2、应用系统未提供登录失败处理功能，攻击者在网络中任何可达位置对应用系统用户名、口令进行暴力猜解，造成身份冒用。

（4）安全管理部分

安全管理制度，安全管理机构，人员安全管理，系统建设管理，系统运维管理五大层面建设不够全面和完善，必需的相关制度及其贯彻执行记录部分缺乏，存在一定的管理疏漏，易导致越权滥用、无作为及误操作等安全管理隐患。

1. 设备清单

序号	产品名称	技术要求	数量	单位
1	防毒墙	详见“2.1、防毒墙”中产品技术要求	2	台
2	入侵检测系统	详见“2.2、入侵检测系统”中产品技术要求	1	台
3	安全管理平台	详见“2.3、安全管理平台”中产品技术要求	1	台
4	账号集中管理与审计系统	详见“2.4、账号集中管理与审计系统”中产品技术要求	2	台
5	移动办公接入网关(SSL VPN)	详见“2.5、移动办公接入网关”中产品技术要求	1	台
6	安全服务	详见“2.6、安全服务”中技术要求	1	项

2. 设备技术参数

2.1 防毒墙

序号	指标项	指标要求
1.	性能指标	★标准 2U 机架式设备，支持多核，提供端口不少于 4 个电口、4 个千兆光口，4 个万兆光口，具有 2 对 Bypass 功能，支持双机热备； 网络吞吐量不少于 3Gbps,Http 吞吐量不少于 10Gbps,SMTP 吞吐量不少于 1500 万邮件/小时。
2.	基础网络适应性	支持桥接、路由、NAT、虚拟线等网络部署模式
		支持 PPPOE 拨号设备接入，具备断线重连技术
		支持静态路由；ECMP 路由；OSPF、RIP、BGP 动态路由功能；支持 VLAN 间路由；支持 ISP 路由，并内置 ISP 地址列表；IGMP V1、V2、V3 组播路由协议
		支持基于源、目的 IP 的策略路由；支持基于协议、端口或应用的策略路由 ；支持主备路由，支持配置路由优先级
		支持端口镜像，将设备任一接口数据镜像到观察口，供用户分析
		支持端口聚合功能，实现带宽扩展
		支持 DNS 代理、DHCP client、DHCP server 代理
		支持双向 NAT 技术、静态 NAT 技术、动态 NAT 技术；支持多对一、一对多和一对一等多种方式的地址转换
		▲支持 IPV6 地址/地址组配置，且支持基于 IPV6 地址/地址组配置防火墙安全策略、防病毒策略、文件过滤策略、流量控制策略（提供界面截图）
		支持 IPV6 GRE 隧道技术，支持 IPv6 over 、IPv4 6to4、IPv6 over IPv4 ISATAP 技术；支持 NAT64、DNS64 翻译技术
		支持 IPV6 包过滤、策略路由、静态路由、HTTP 应用协议、自动获取 IPV6 地址
		支持多出口负载均衡，支持轮流、加权最少、权重轮流、最少连接等算法，支持多运营商智能选路
3.	防火墙	支持自定义安全策略，可基于 MAC 地址、IP 地址、端口、服务、应用、时间计划定义安全策略；能识别 2000+种应用
		支持检测 IP 地址盗用，并拦截盗用 IP 地址的主机经过设备的各种访问
		支持基于源 IP/目的 IP 配置并发连接数上限
		支持对 ARP FLOOD 攻击、ICMP FLOOD 攻击、UDP FLOOD 攻击、SYN FLLOD 攻击、DNS FLOOD 攻击、TearDrop 攻击、Smurf 攻击、LAND 攻击、WinNuk 攻击、ICMP 大包攻击进行防护
		支持会话超时时间自定义， 包括：TCP 连接建立、TCP 超时等待、UDP 超时等待
		支持根据源 IP 地址/目的 IP 地址查看会话连接排行； 支持多个维度监控当前所有会话，包括协议、源/目的地址、源/目的端口、状态；
		支持 IP-MAC 绑定，可自动扫描内网设备的 IP-MAC 地址；支持管理员手动配置；支持从外部文件导入 IP-MAC 地址列表；支持配置例外 IP 和例

		外端口；
4.	病毒木马防护	▲支持特征查杀引擎、机器学习引擎两种防病毒引擎，支持双引擎同时工作；（提供界面截图） 支持快速扫描和文件扫描两种工作模式切换（提供界面截图）
		支持多种文件类型的扫描及多重压缩文件扫描，最高支持 20 层解压
		支持本地库和云端扫描结合的方式；支持病毒库在线和离线更新
		支持基于 IP/IP 组、协议（HTTP、FTP、SMTP、POP3）配置防病毒策略；支持检测并报警、阻断、隔离三种响应处理方式；支持下载/删除隔离区恶意文件
		支持僵尸网络及恶意代码检测，如蠕虫病毒、后门木马、间谍软件等
		支持检测并拦截 HTTP、FTP 电子邮件等协议所携带的恶意代码，并记录拦截日志
		支持 400 万条以上的病毒库，并且可以自动或者手动升级
		提供长达 3 年的病毒特征库升级服务，云端机器学习病毒检测模型升级服务；支持定时升级、离线升级、在线升级；
		支持木马类型报告，提供超过 200 种木马的分析，包括木马文件名、类型、主要特征、分析步骤及结果、验证方法，措施建议和 Snort 规则
5.	网中网管控	▲支持对 WiFi 分享网络中移动终端进行检测，能检测到移动终端的系统类型包括安卓、苹果等，并对 WiFi 分享行为进行管控（提供界面截图）
6.	流量控制	支持基于用户/用户组、IP/IP 组、应用、时间计划的带宽控制策略
		▲支持配置保障通道和限制通道；支持限制同一用户组内单 IP 上下行带宽（提供界面截图）
		支持高、中、低三级通道优先级，支持动态调整带宽、利用空闲带宽
7.	反垃圾邮件	支持基于关键字的内容过滤，对 HTTP 上传，邮件主题、正文、附件名、发件人、收件人进行过滤
8.	信息泄露防护	支持基于文件类型的下载过滤，对 HTTP 上传、FTP 上传、邮件附件进行过滤，
		支持 web 内容过滤，支持自定义正则表达式过滤 web 请求内容/响应内容
9.	URL 过滤	▲支持基于源 IP/IP 组配置 URL 访问控制策略；内置成人类、赌博类、娱乐类等 63 类常见 URL 类型组，用户可快速完成配置；支持配置 URL 过滤策略优先级（提供界面截图）
		▲支持 URL 黑白名单，支持配置黑白名单优先级（提供界面截图）
		支持自定义恶意网站，具备恶意网站过滤功能
10.	系统管理	支持管理员角色三权分立，支持管理员用户名+密码/UKEY 双因子认证；支持按模块为管理员角色配置权限
		支持配置管理员密码安全策略，密码更换时间、密码最小长度等详细要求
		支持配置 IPV4/IPV6 可信管理主机
		支持 SNMP 协议；支持 NTP 协议
		支持图形化系统调试工具；内置抓包工具
		支持按系统备份历史记录回滚

		支持对规则库手动升级，支持配置定时升级，支持自动升级；
		支持为不同 IP/IP 组定制用户认证页面
		支持配置向导，为用户提供常用功能配置指导；支持配置检查功能
		支持集中管理功能，监控所有设备状态；支持统一下发配置，统一更新规则库，日志上报功能
11.	日志审计	支持本地存储日志、syslog 多发日志；支持覆盖、暂停、报警三种日志满响应方式；支持配置日志入库归档周期
		▲支持系统登录日志、恢复与备份日志、重启关机日志、管理员操作日志、资源告警日志、防火墙日志、防病毒日志、信息泄露防护日志、DDOS 攻击防护日志、应用管控日志、URL 访问日志、用户认证日志、网中网检测日志（提供界面截图）
		支持用户自定义日志任务，支持分模块、基于时间、响应方式、协议、源地址/目的地址等维度导出 Excel 格式日志
		支持配置日志审计平台或者第三方日志服务器，提供强大的日志管理和日志审计功能（存储、审计、报表）
		支持导出流量统计报表，支持基于应用、协议、IP/用户等维度统计流量并排行
12.	报警	支持对入侵事件、攻击事件等进行报警，并记录报警数据
		支持对系统运行状态进行报警，如 CPU、内存、带宽超过阈值
		支持邮件、短信、SNMP Trap、声音报警等报警方式
13.	高可用性	支持主-主模式、主-备模式的双机热备
		支持物理设备状态监测，即主防毒墙出现断电或其他故障时，备防毒墙能及时发现并接管主防毒墙的工作
		支持会话状态、配置同步
		支持冗余心条线机制
		支持 VRRP 协议和 STP 协议
		支持链路状态检测的双机热备
		支持基于集群工作模式的负载均衡功能，使多台防毒墙能够协同工作均衡网络流量
		支持电源冗余电源；支持电源热插拔；支持业务接口卡热插拔
14.	产品资质（出具加盖厂商公章的复印件）	具备公安部颁发的《计算机信息系统安全专用产品销售许可证》
		▲具备中国人民解放军信息安全测评认证中心颁发的《军用信息安全产品认证证书》
15.	厂商资质（出具加盖厂商公章的复印件）	▲厂商具备 ISO20000、ISO27001 和 CMMI 5 级证书
		厂商具备中国信息安全认证中心（ISCCC）颁发的应急处理服务资质
		具备中国信息安全认证中心（ISCCC）颁发的信息系统安全集成一级资质
		具备中国信息安全评测中心颁发的信息安全服务资质证书
		为省级或省级以上计算机信息网络安全协会指定服务单位

2.2 入侵检测系统

序号	指标项	技术规格参数要求
1.	★性能指标	网络接口：1管理口，7检测口（4光4电）
		最大并发连接数：≥3800000
		最大吞吐量：≥5.4Gbps
2.	产品架构	机架式硬件，专业 IDS 入侵检测设备
		支持多网段、跨网段的多路混合部署
3.	入侵检测	内置攻击规则特征库，规则库规则列表≥8000种
		支持用户自定义特征规则
		支持入侵规避发现，能发现躲避或欺骗检测的行为，如 IP 碎片重组，TCP 流重组、协议端口重定位等等
		支持内置事件调整，可对事件种类、事件说明、事件级别重新编辑
		支持 SYN flood、TCP flood、UDP flood、ICMPflood 攻击检测
		支持多种告警方式，至少包含声音告警、邮件告警、短信告警、snmp trap 等
		▲系统携带的攻击特征库须获得 CVE-Compatible 兼容性认证，CVE 兼容性认证须提供证明文件。
4.	高级威胁检测	▲系统应提供基于信誉的僵尸网络检测能力，具备可以持续升级的信誉库，IDS 通过信誉库内的恶意网站 IP、C&C 服务器地址的信誉值执行相应的检测动作。须提供信誉库界面截图。
		系统应提供服务器异常告警功能，可以自学习服务器正常工作行为，并以此为基线检测处服务器非法外联行为，须提供界面截图。
		▲系统应提供敏感数据外发的检测功能，能够识别通过自身的敏感数据信息（身份证号、银行卡、手机号等），须提供界面截图。
5.	部署能力	系统应提供系统规则和用户规则模板，减少配置工作量，提高部署效率，需提供界面截图。
6.	产品资质（出具加盖厂商公章的复印件）	具备公安部颁发的《计算机信息系统安全专用产品销售许可证》
		具备国家保密科技测评中心颁发的《涉密信息系统产品检测证书》
		产品要求取得中国信息安全测评中心《信息技术产品安全测评证书（EAL3+）级)》
		投标 IDS 产品应具有 IPv6 Ready Logo 证书，提供有效证书的复印件
7.	厂商资质（出具加盖厂商公章的复印	▲厂商具备 ISO20000 和 ISO27001 证书
		厂商具备中国信息安全认证中心（ISCCC）颁发的应急处理服务资质
		具备中国信息安全认证中心（ISCCC）颁发的信息系统安全集成一级资质

	件）	具备中国信息安全评测中心颁发的信息安全服务资质证书
		厂商须获得中国信息安全测评中心颁发的：信息安全服务资质证书-风险评估类（二级），提供证书复印件；
		产品厂商获得互联网安全研究中心颁发的应用安全联盟会员认证，提供会员证书复印件。
		▲产品厂商获得网络安全应急服务支撑单位证书（国家级），提供证书的复印件。
		厂商须获得中国信息安全测评中心颁发的：信息安全服务资质证书（安全工程类二级）、信息安全服务资质证书（安全开发类一级），须提供以上两个证书的复印件。

2.3 安全管理平台

序号	指标项	技术规格参数要求
1.	系统架构	开放式设计：平台化设计，功能模块插件化，用户可以自主选择需要的功能模块，或在现有平台上进行客户化定制
		分布组件：各功能组件之间采用网络方式进行通讯，各组件可以分布安装在不同的机器上，以支持大规模和灵活的部署
		采用业界主流的 B/S 方式，通过 SSL 加密通信
2.	性能参数	管理资产数量≥100 标准资产
		日志保存时间：3 个月
		最大日志记录条数为：1 亿条
		日志分析结果保存天数：365 天
		事件处理能力：3000 条/秒
3.	部署方式	单机部署：各组件集中式部署
		分布式部署：采集器和分析引擎支持分布式部署，可根据实际需要灵活扩容
		级联部署：下级 SOC 可将告警信息，日志信息汇报给上级 SOC
4.	资产管理	支持对资产属性的定义，资产属性包括：资产名称、资产类别、IP 地址、资产价值、厂商信息、资产版本、所属部门、所属区域、地理位置、责任人等信息
		支持对资产的新增，删除，修改，导出，导入等操作
		支持资产设备自动发现
		支持对资产进行多条件组合的检索查询
		支持资产漏洞导入，查看和漏洞统计

		支持资产风险值计算模型，可用风险值量化单设备风险和整个网络的风险情况
		▲支持资产健康度计算模型、可信度计算模型，可用健康值和可信值量化表示
5.	设备管控	支持对网络设备、安全设备、主机、服务器等设备的监控
		支持 CPU 使用率、内存使用率、磁盘使用率、进程信息、软件信息、网口流量信息等设备状态的监控，并可图形化展示
		支持 ssh，snmp，bdsec 接口进行设备管理，设备管理包括：重启、关机、时间同步、关闭服务、启动服务、策略备份、策略下发等。
6.	拓扑管理	▲可自动发现网络设备及其网络连接情况，获取最初的网络拓扑信息，并通过拓扑图展示(提供界面截图)
		★可在拓扑图上查看某个网元的基础信息（设备名称、设备类型、设备厂商、操作系统等），运行状况（cpu、硬盘、内存使用率等），事件情况（上报事件、发起事件、受影响事件等），告警情况
		可查看网元间网络连通情况，流量信息等
		可在拓扑图上对设备进行管控操作，包括关机、重启、时间同步等
		用户可手工编辑拓扑，包括节点属性编辑，网元连接线编辑，拓扑背景图更换，拓扑区域划分
		支持选择不同的地理域、设备类型、组织架构等维度信息，从不同维度查看拓扑图
		可通过拓扑图运维工具集中进行运维，运维工具包括 ping，traceroute 等
7.	业务管理	支持业务建模，录入业务系统信息，包括系统名称、责任人、相关设备、相关支撑服务等
		可定期对业务系统关键 URL 的可访问情况进行检查，可检测 URL 是否可达，访问延时等
		可根据业务建模自动生成三层业务拓扑图，用户可修改编辑业务拓扑图
		支持通过拓扑图直观展示故障业务系统的支撑服务告警情况，主机设备基本信息、事件信息、告警信息、漏洞信息等情况，帮助用户分析判断业务故障的原因
		支持业务异常数统计，内置业务健康度计算模型，可通过业务健康值和业务异常数图示化标识可能存在故障的系统
8.	IT 资源监控	▲可监控多种中间件，数据库的运行指标情况，包括 weblogic，tomcat，apache，iis 等中间件，包括 mysql，oracle，sqlserver，db2，sysbase 等数据库（提供界面截图）
		内置监控对象，对象模型，对象指标等一系列完整的指标体系，用户可选择监控对象后简单录入配置信息即可实现监控
		可通过扩展适配器的方式，与不同网管系统，运维平台对接，获取监控数据
9.	蜜罐管理	▲支持模拟开放服务端口，引诱攻击者入侵，并记录入侵行为数据（提供界面截图）

10.	自动巡检	▲支持用户按周或者按月制定周期巡检任务，系统可自动执行巡检脚本，完成设备连通性、运行状态、运行进程等项目的自动巡检，支持巡检报告导出（提供界面截图）
11.	应急管理	▲支持应急资源的录入与查询（提供界面截图）
		支持应急预案的制定
		支持应急事件录入与查询
		支持应急演练计划制定与查询
12.	等保测评	▲支持根据待评级的等保级别，列出对应等保级别所需满足的测评项目（提供界面截图）
		支持根据各测评项目检查情况录入或者选择对应的检查结果，支持根据结果生成测评整改分析报告，并可产生统计报表
13.	流量分析	支持通过动态推移图的方式直观展示实时流量情况
		支持按照不同维度对流量进行统计
		▲支持异常流量分析，内置基线学习引擎，学习多种维度的流量基线，用户可配置基线策略，通过基线策略和流量基线分析异常流量（提供界面截图）
14.	漏洞管理	▲支持对多个厂家多种型号的漏扫设备漏扫报告的导入，导入数据包括漏洞端口、漏洞级别、漏洞名称、ip 地址、漏洞类型、漏洞 CVE 号、漏洞 SID 号（提供界面截图）
		可根据漏洞生成漏洞报表，可利用漏洞数据产生预警和进行关联分析
15.	事件管理	支持 syslog、snmp trap、文件、wmi、opsec 协议的日志采集，支持网络设备、安全设备、服务器、数据库、中间件、应用系统等多种软硬件设备的日志采集
		日志采集策略设置，可过滤指定来源的日志
16.	关联分析	支持多维度多场景的关联分析，支持通过统一配置方式增加或者修改关联模型
		支持事件规则关联、情报关联、资产关联、流量关联、指标关联等多种组合关联
17.	风险分析	提供符合 bs7799/iso17799 标准的资产风险分析和风险计算方法，风险按照国际标准划分为 5 级
		用户可以从资产风险追踪到相关的高风险事件，有效判断资产风险的来源，并进行正确的处理
18.	行为及信息监控	▲支持通过部署行为监测探针，可获取终端的违规行为信息，包括违规终端 IP，违规行为类型，违规时间（提供界面截图）
		▲支持通过部署信息监测探针，可监测内网的敏感信息内容，当出现敏感信息后，系统将触发告警，告警信息包括，告警主机 IP，告警时间，敏感内容详情（提供界面截图）
19.	异常事件分析	▲支持按照事件数量、事件类型、事件目标、事件协议等维度，依照某一学习周期学习并生成基线（提供界面截图）

		支持设置基线偏离阈值，设置事件正常发生时间范围等条件，系统可根据条件检测异常事件
20.	报表管理	系统预置丰富的系统报表，充分满足用户的需求。报表支持多种格式的显示
		报表的生成方式分为手工报表和自动报表两种，手工报表可以直接支持生成，自动报表可以按照每小时、每天、每月、每年等周期的方式生成
		提供多种展现仪表盘，包括柱状图、折线图、饼状图、视网膜图、雷达图、热力图提供用户可定制 Top N 展示图表
21.	可视化分析	网络态势：支持展示基于 GIS 地图的攻击路径、攻击事件统计、威胁类型分布、设备产生日志总量趋势统计、整体安全风险系数、攻击事件列表等
		流量态势：支持展示基于 GIS 地图的流量热力图、外部源流量统计、协议类型统计、源和目的流量关系统计、资产总流量趋势统计、基于流量发现攻击事件列表等
		脆弱性态势：支持展示漏洞数量统计、漏洞类型统计、漏洞与资产关联关系统计、脆弱性利用分析等
22.	分布式采集器管理	▲支持分布式采集，通过传感器实现不同协议不同类型数据的统一传输，通过插件的方式实现采集方式的扩展（提供界面截图）
		支持传感器管理，实现对所有传感器运行状态的查看，和对传感器的启停控制
		支持插件管理，包括对各种采集插件的启停控制，状态查看，以及插件运行策略的设置
23.	合规检查	支持系统弱口令检查：检查系统或者应用是否存在弱口令，定期进行检查，并产生告警
		支持防病毒软件检查：定期检查系统是否有安装基线配置的防病毒软件，如果未安装，则产生告警
		支持软件安装记录检查：定期检查系统是否有私自安装非法软件，如果未安装，则产生告警
		支持软件卸载记录检查：定期检查系统是否私自卸载必须软件，如果检查到卸载记录，则产生告警
		支持系统进程与服务黑白名单检查：定期检查系统是否有启动非法进程，如果有启动，则产生告警
		支持网络连接异常监控：定期检查系统是否网络连接异常，如果连接异常，则产生告警
24.	黑客行为分析	反向拍照：可对攻击源进行反向拍照，获取攻击源的地域、操作系统等详细信息，以供后续取证
		攻击处理知识库：提供攻击事件的防范处理知识，帮助管理员快速解决问题
25.	联动功能	▲为了建立统一安全管理联动平台，与防毒墙必须同一品牌，提供原厂商联动证明原件
26.	产品要求	产品具备国家版权局颁发的软件著作权登记证书

	（出具加盖厂商公章的复印件）	获得公安部颁发的《计算机信息系统安全专用产品销售许可证》
		产品具备国家保密局涉密信息系统安全保密测评中心颁发的涉密信息系统产品检测证书
		产品具备 IPV6 认证
27.	厂商资质（出具加盖厂商公章的复印件）	▲厂商具备 ISO20000、ISO27001 和 CMMI 5 级证书
		厂商必须具备中国信息安全认证中心（ISCCC）颁发的应急处理服务资质
		具备中国信息安全认证中心（ISCCC）颁发的信息系统安全集成一级资质
		具备中国信息安全评测中心颁发的信息安全服务资质证书
		为省级或省级以上计算机信息网络安全协会指定服务单位

2.4 账号集中管理与审计系统

序号	指标项	技术规格要求
1.	产品架构	支持双机热备
		支持冗余网卡，允许将两张网卡绑定在一起使用，两张网卡同时使用一个 IP，当一张网卡有问题的时候另一张可以继续使用
		支持 VMware、KVM、XEN 等主流虚拟化平台以及第三方虚拟化平台部署
		支持 Docker 部署
2.	★性能指标	支持100许可；
		接口：4个百兆/千兆自适应电口；1个 Console 接口，2个 USB 接口
		审计日志存储空间≥1.5T；
		到目标设备的连接时间不大于2秒；
		MTBF 不少于6万小时；
3.	支持操作协议	终端命令操作：Telnet、SSH；
		远程桌面： RDP、VNC；
		文件上传和下载： FTP、SFTP；
4.	用户管理	用户帐号实名制：根据具体的维护人员添加唯一与其身份对应的用户，实现维护人员身份的唯一性管理
		可以设定活动、禁用两种用户帐号状态，当用户在一定时间内连续输错密码时，可以自动禁用该用户帐号
		▲支持静态密码、USBKEY 形式双因子认证；支持 AD 域、LDAP 域、Radius 网络认证方式；支持短信验证码、手机 APP 验证码、数字证书等动态口令认证；支持根据不同用户采用不同静态认证与动态认证的任意组合（提供界面截图）
		支持忘记密码后通过邮箱找回密码
		支持三权分立的原则和要求，审计员、管理员、运维人员职、权分离

		▲支持批量定时修改设备密码，支持随机生成不同密码、随机生成相同密码以及手工指定相同密码的密码策略，并严格遵守密码强度设置，修改后的设备密码可以以邮件的方式发送给密码管理员（提供界面截图）
		用户帐号支持导入导出功能
5.	多级部门管理	▲支持多级部门管理功能，增加部门管理员和部门审计员，不同的用户和设备归属于不同的部门（子部门），不同部门的配置管理员只能针对自己部门及自己直属子部门设备进行访问权限设置，上级管理员可以对下级的管理员授权管理（提供界面截图）
6.	智能发现	▲能对 IP 地址段进行扫描，识别出该 IP 地址段内开放的应用类型、服务、端口等信息，支持一键添加管理功能（提供界面截图）
7.	审计内容	SSH、Telnet 字符命令界面操作审计
		FTP、SFTP 文件上传、下载、删除、改名等操作的审计
		VNC、RDP 远程桌面操作审计
		HTTP、HTTPS 操作审计
		支持 FTP/SFTP 方式文件上传的副本备份，可供审计员审计查看
		支持磁盘映射方式文件上传的副本备份，可供审计员审计查看
8.	数据库运维操作审计	审计包括访问起始和终止时间、用户名、用户 IP 地址、目标设备 IP、设备名称、数据库类型、操作内容等；支持操作内容录像回放
9.	安全策略	IP 策略：可以允许或拒绝指定的 IP 登录管理界面，还可以按照用户的需要指定用户或设备在一个指定 IP 或 IP 段下才可以对设备进行访问管理
		密码策略：可以指定密码有效期、密码复杂度设置
		防绕策略:可以指定 IP 或 IP 段进行防绕是否阻断与是否产生告警记录的选择
		时间策略：可以指定用户或设备在一个指定的时间段内有效。可以按照用户的需要定制时间白名单
10.	文件传输检测控制	▲支持文件上传下载（ftp/sftp)方式下对文件/文件夹标题及内容检测，及时发现敏感信息，对违规的下载或上传操作进行拦截或者产生后台告警，避免重要数据泄露（提供界面截图）
11.	图形用户行为审计	▲实现对远程桌面中的客户端操作动作进行识别分类等,能够识别文件的打开、删除、重命名，活动窗口的检测、菜单点击，键盘输入检测等动作。审计人员能够通过关键信息快速过滤和定位到目标位置，查看关键操作，提升审计效率（提供界面截图）
12.	工单管理	▲支持工单申请和下发,授权运维人员根据授权在指定时间内访问指定资源，申请内容包括设备 IP、设备账户、运维有效期、备注事由等，运维工单可以邮件方式通知管理员（提供界面截图）
13.	无感知应	▲可通过无感知应用发布的方式进行协议扩展,支持 B/S 和 C/S 方式的

	用发布	通用及专有的运维客户端程序，支持远程应用本地化展示、支持应用的单点登陆功能（提供界面截图）
14.	管理向导	▲通过设备管理向导完成设备从添加到授权的步骤;通过应用管理向导可以完成应用从录制配置文件到授权的步骤（提供界面截图）
15.	图形展示	▲首页访问关系图形展示，根据用户、设备、应用的不同颜色区分，通过连接图形直观展示用户对设备或应用的访问关系（提供界面截图）
16.	自动化运维	▲管理员可以根据设备/设备组、系统账号、时间、脚本内容（自定义），创建自动脚本任务；该任务到期自动执行，执行的结果自动发送给相关管理员（提供界面截图）
17.	报表管理	支持通过时间、用户、账号、源 IP、目标 IP、完成状态进行会话浏览排名统计
		支持应用浏览的排名统计和播放、下载
		提供拦截日志和防绕日志的查询和报表导出
		提供系统登陆日志、系统操作日志等自身审计日志和多种报表，给企业考核提供依据
18.	联动功能	为了建立统一安全管理联动平台，与安全管理平台必须同一品牌，提供原厂商联动证明原件
19.	产品资质（出具加盖厂商公章的复印件）	具备国家版权局颁发的《软件著作权登记证书》
		具备公安部颁发的《计算机信息系统安全专用产品销售许可证》
		具备国家保密科技测评中心颁发的《涉密信息系统产品检测证书》
		具备中国信息安全认证中心颁发的《IT 产品信息安全认证证书》（ISCCC）
		具备中国人民解放军信息安全测评认证中心颁发的《军用信息安全产品认证证书》
		具备中国质量认证中心颁发的《中国国家强制性产品认证证书》（CCC）
		具备中国质量认证中心颁发的《中国节能产品认证证书》
		产品具备 IPV6 金牌认证
20.	厂商资质（出具加盖厂商公章的复印件）	▲厂商具备 ISO20000、ISO27001 和 CMMI 5 级证书
		厂商必须具备中国信息安全认证中心（ISCCC）颁发的应急处理服务资质
		具备中国信息安全认证中心（ISCCC）颁发的信息系统安全集成一级资质
		具备中国信息安全评测中心颁发的信息安全服务资质证书
		为省级或省级以上计算机信息网络安全协会指定服务单位

2.5 移动办公接入网关

序号	指标项	技术规格

1	**部署方式参数**	支持网关模式、单臂模式部署两种方式；SSLVPN 加密速度≥480Mbps SSLVPN 每秒新建用户数≥400 防火墙吞吐量≥2.2Gbps 最大并发会话数目≥1600,000 网络接口≥6 个千兆电口、4 个≥千兆光口 尺寸≥2U;冗余电源
2	**安全性**	支持终端使用包括 IE6、7、8、10、11 或其他 IE 内核的浏览器，以及最新版本的非 IE 内核浏览器，如 Windows EDGE，Google Chrome，Firefox，Safari，Opera 最新版登录 SSLVPN 系统，登录后可完整支持各种 IP 层以上的 B/S 和 C/S 应用。（提供截图证明并加盖原厂公章）
3	**高性能**	支持启用多线路时，自动检测故障线路，并自动踢出故障线路；一旦线路恢复，可在一定时间内自动恢复。支持启用多线路时，自定义用户访问选路策略，包括按上/下行带宽，轮询，按优先级等方式。（提供截图证明并加盖原厂公章）
		▲支持利用网页进行动态寻址的方法，客户端无需安装插件、不依靠 IP 地址库、不依赖于第三方动态 IP 寻址、直接根据速度探测实现用户端接入线路的自动优选,用户通过访问寻址代理页面（简称 Webagent 页面），通过 Webagent 页面自动寻找 VPN 设备 IP(非 DDNS）,该方法不必单独注册域名或占用 IP 地址，大大降低了系统部署难度。（提供截图证明并加盖原厂公章）
		支持针对不同的 web 页面进行数据优化，支持动态压缩技术，基于数据流进行压缩，减少不必要的数据传输。（提供截图证明并加盖原厂公章）
		▲针对 B/S 资源支持 WebCache 技术，动态缓存页面元素，提高 Web 页面响应速度。支持流缓存技术，实现网关与网关、网关与移动客户端之间进行多磁盘、双向、基于分片数据包的字节流缓存加速，削减冗余数据，降低带宽压力的同时提高访问速度；支持共享流缓存功能，实现多分支网关在总部共享流缓存数据，提高流缓存效果（提供截图证明并加盖原厂公章）
4	**厂商资质**	提供中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》（提供证书复印件并加盖厂家公章） 提供产品 IPV6 Ready 认证证书(提供证书复印件并加盖厂家公章） ▲要求厂商具有 CMMI 5 级认证。（提供证书复印件并加盖厂家公章） ▲设备生产厂商需为国家密码管理局发布的《SSL VPN 技术规范》起草单位之一（提供相关证明并加盖厂家公章） ▲要求厂商是微软安全响应中心（Microsoft Security Response Center）发起的 MAPP（Microsoft Active Protection Program）计划成员，可在微软发布每月安全公告之前获得微软产品的详细漏洞信息，为用户提供更及时的安全防护。（提供相关证明并加盖厂家公章） 提供公安部信息安全产品检测中心颁发的《GA/T 686-2007 信息

		安全技术 虚拟专用网安全技术要求》三级或三级以上检测报告（三级以上为四级、五级）（提供证书复印件并加盖厂家公章）

2.6 安全服务

2.6.1 安全加固服务：针对安全扫描过程中发现的安全漏洞，在可控的范围下，对操作系统、数据库、中间件发现的安全漏洞进行加固。

2.6.2 应急体系建设和应急演练：根据国家和卫计委有关信息安全应急体系建设要求，结合医院实际情况，制定应急预案，并定期组织应急模拟演练，并做好应急演练总结。

2.6.3 应急响应服务：当用户单位遭受网络病毒/木马、黑客入侵、DOS 攻击等安全事件时，服务商在第一时间派出安全专家进行现场排查处理，保障业务系统的连续性，阻止和减小安全事件带来的负面影响。

2.6.4 安全培训服务：以实际业务运作为立足点，注重理论和实操结合，通过理论讲授、实验操作、问题讨论等方面，普及安全教育，提高安全意识，提高安全防范能力。主要内容包括网络安全的相关法律法规培训、各种网络攻击技术原理及防御培训、网络安全策略及安全管理培训、常用网络安全产品原理及应用培训等服务。

2.6.5 原厂服务：设备提供 3 年售后服务（软件升级、硬件质保）。必须提供 7×24 小时电话支持；应急服务紧急攻击事件 2 小时内响应，最大限度减少损失。提供两个名额的原厂培训（含参加认证考试）。

四、项目相关要求

1、工期或交货期

合同签订后 30 天内。

2、投标人必须提供详细的保修期内技术支持和服务方案，技术支持和服务方案包括（但不限于）：

1）整体工程提供不少于 3 年的免费维护，设备按原厂商标准提供维护。质保期内免费提供保证系统正常运行的全部备件及维护，免费提供系统运行所需软件的维护服务及最新版本。

2）提供不少于 3 年 5×8 小时上门保修，免费更换全部配件；提供 7×24

小时技术支持和服务，1 小时内作出实质性响应，对重大问题提供现场技术支持，4 小时内到达指定现场。

3、培训要求：

在项目建设过程中需对相关人员进行技术培训，在以后系统运行过程中亦需根据具体情况进行相应内容的培训，以保证系统的管理人员、技术人员和应用人员能够及时、准确地了解和熟练地运行系统。

4、投标人必须根据所投产品的技术参数、资质资料编写投标文件。在中标结果公示期间，采购人有权对中标候选人所投产品的资质证书等进行核查，如发现与其投标文件中的描述不一，代理机构将报政府采购主管部门严肃处理。

5、投标人必须如实地对招标文件中各项技术要求作出明确的逐项响应承诺，并对其真实性负责。

投标货物（含软件部分）的技术响应情况必须在《技术及资质响应表》中完整体现。

6、投标人的报价应包括本项目建设所有货物、运输、安装、集成、调试、试运行、服务、税等费用。