**项目需求书**

**一、项目概况及总体要求**

为更好的贯彻落实国务院关于网络安全的重要指示精神，有效应对当前网络安全面临的严峻威胁与挑战，全力做好重要信息系统网络安全保卫工作，我院对重要信息系统每年开展等保测评工作时发现部分系统存在安全隐患，根据信息系统三级等保测评机构出具的《江苏大学附属医院2024年网络安全等级测评项目整改建议书》及市委网信办、市等保办对医院信息安全作出的安全隐患应及时整改的相关要求，结合我院目前在用的安全设备的实际状况，需采购以下安全设备作安全防护，保障医院信息系统的稳定运行。

**二、采购用途**

采购用途：□科研 □教学 □医疗 ☑管理 □后勤 □其他

用途说明：信息安全设备增加、扩容及安全整改，以满足医院信息系统的安全等级保护要求。**三、采购需求一览表（货物类）：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 货物名称 | 单位 | 数量 | 核心产品（是/否） |
| 1 | 外网防火墙 | 台 | 2 | 是 |
| 2 | 上网行为管理 | 台 | 1 | 否 |
| 3 | API防护系统 | 套 | 1 | 否 |
| 4 | 数据库审计设备 | 台 | 1 | 否 |
| 5 | 日志审计设备 | 台 | 1 | 否 |
| 6 | 漏洞扫描设备 | 台 | 1 | 否 |
| 7 | 流量分析系统 | 套 | 1 | 否 |
| 8 | 网闸扩容 | 套 | 1 | 否 |
| 9 | 应用负载设备扩容 | 台 | 1 | 否 |
| 10 | 杀毒软件扩容 | 套 | 1 | 否 |

**三、技术指标（按一览表中货物分别填写）**

**1. 外网防火墙（2台）**

|  |  |  |
| --- | --- | --- |
| 序号 | 功能项 | 指标要求 |
| 1 | 架构要求 | 要求采用自主知识产权的专用操作系统，应用多核并行处理技术保障产品处理性能，需提供官方检测机构出具关于“多核并行安全操作系统”的证书。 |
| 2 | 规格要求 | ★性能要求：网络层吞吐≥20G,应用层吞吐≥10G，全威胁吞吐≥1G  硬件配置：不少于8个千兆电口，2个万兆光口，1个RJ45串口，2个USB接口，冗余电源，配置IPS模块/AV模块/URL模块/防通报模块/防勒索模块/WEB防御模块 |
| 3 | 工作模式 | 要求支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。 |
| 4 | 硬件一虚多 | 要求支持虚拟防火墙功能，支持虚拟防火墙的创建和删除，具备独立的接口、会话管理、应用控制策略、NAT等资源。 |
| 5 | 链路状态检测 | 要求支持链路连通性检查功能，支持基于3种以上协议对链路连通性进行探测，探测协议至少包括DNS解析、ARP探测、PING和BFD等方式。 |
| 6 | IPv6 | 要求支持IPv4/IPv6双栈工作模式，以适应IPv6发展趋势。 |
| 7 | 要求支持基于应用、服务、时间、域名、IPv6对象等维度的访问控制。 |
| 8 | 认证方式 | 要求支持3种以上的用户认证方式,包含但不限于单点登录、本地账号密码、外部账号密码认证。 |
| 9 | 访问控制策略 | 要求支持基于网络区域、网络对象、MAC地址、服务、应用、域名等维度进行访问控制策略设置。 |
| 10 | 文件过滤 | 要求支持基于文件传输方式、文件类型等维度的管控策略配置。 |
| 11 | 防病毒 | 要求支持对SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP等协议进行病毒防御。 |
| 12 | 要求支持对压缩病毒文件进行检测和拦截，压缩层数支持15层及以上。 |
| 13 | ▲要求产品应具备独立的勒索病毒防护模块，非普通防病毒功能，支持对特定的业务进行勒索风险自动化评估，并依据评估结果自动生成防护策略。（需提供产品功能截图证明，需提供产品功能截图证明并出具关于“勒索病毒”的软件著作权证明功能有效性）。 |
| 14 | 入侵攻击防御 | 要求产品内置不低于15000种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则。 |
| 15 | 要求支持基于IMAP、FTP、RDP、VNC、SSH、TELNET、ORACLE、MYSQL、MSSQL等应用协议进行深度检测与防护。 |
| 16 | 要求支持僵尸主机检测功能，产品内置僵尸网络特征库超过120万种，可识别主机的异常外联行为。 |
| 17 | Web应用防御 | 要求内置超过4500种WEB应用攻击特征，支持对跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护。 |
| 18 | 要求产品支持服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁。 |
| 19 | 要求产品支持Cookie攻击防护功能，并通过日志记录Cookie被篡改。 |
| 20 | 账号安全 | 要求支持独立的账号安全防护模块，具备事前账号脆弱性、事中账号爆破、事后账号失陷的全生命周期安全防护，在设备界面可以详细展示账号安全相关信息，包括风险业务、风险等级、存在账号入口、存在弱口令、遭受口令爆破、异常账号登录。 |
| 21 | 策略有效性分析 | 要求支持安全策略有效性分析功能，分析内容至少包括策略冗余分析、策略匹配分析、风险端口风险等内容，提供安全策略优化建议。 |
| 22 | 策略生命周期管理 | 要求支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。 |
| 23 | 管理方式 | 要求支持Web管理、串口管理、SSH管理等多种不同方式。 |
| 24 | 业务资产管理 | 要求支持被动监测和主动扫描两种资产识别方式，可梳理离线资产、高危端口开放、冗余端口等安全风险；同时通过可视化的拓扑关系图，直观地展示资产和资产之间的访问关系、访问细节协议端口等信息； |
| 25 | 带外管理 | 要求支持带外管理,保障管理网络和业务网络相互隔离。（需提供产品功能截图证明） |
| 26 | 防通报 | ▲要求支持对威胁流量就近进行实时检测&拦截，实现失陷外联实时阻断，保护资产安全。支持云端未知威胁主动探测技术，实现5min内未知威胁情报全网设备下发。（需提供产品功能截图证明并提供具备CMA/CNAS标识的第三方检测报告） |
| 27 | 安全响应 | 本次所投防火墙支持与医院现有态势感知平台联动、在安全事件发生时可实现访问控制（指定源目IP、源目端口号及服务）及批量联动封锁（URL、域名、IPV4/IPV6，封锁时间可具体到天或永久封锁），来保证发生安全事件可快速进行响应处置； |
| 28 | ▲考虑到医院行业的特殊性及业务系统的重要性，为实现我院安全事件发生时可以快速闭环处置，防止事态进一步扩散：可跟医院现有的安全运营服务进行联动，将检测到的安全事件信息及安全日志实时传递给安全运营服务中台，发生安全事件时云端服务经理可第一时间接入进行处置闭环，对服务范围内发现的每一个高危可利用漏洞提供防护规则，防护率达到99%，针对违规外联等网络侧事件，实现一般事件遏制时间小于30min，重大事件遏制时间小于15min；（需提供相关证明材料） |
| 29 | 网管协议 | 要求产品支持SNMP V1/V2/V3/Trap等标准网络管理协议。 |

**2. 上网行为管理(1台)**

|  |  |  |
| --- | --- | --- |
| 序号 | 功能项 | 指标要求 |
| 1 | ★性能指标 | 要求网络层吞吐量（大包）：≥10Gb，应用层吞吐量：≥1.5Gb，带宽性能：≥1Gb，支持用户数：≥6000，每秒新建连接数：≥14000，最大并发连接数不少于： 600000。内存大小不少于8G，硬盘容量不少于1TB (全闪容量)，接口不少于6千兆电口、2万兆光口。 |
| 2 | 实时状态 | 要求支持首页分析显示接入用户人数、终端类型；带宽质量分析、实时流量排名；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行； |
| 3 | Web访问质量检测 | 要求针对内网用户的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； |
| 4 | 邮件管理 | 要求支持允许用户登录Webmail收邮件，而禁止发送Webmail邮件的功能； |
| 5 | 单点登录 | 要求支持radius、AD、POP3、Proxy、PPPOE、 H3C IMC/CAMS、锐捷 SAM、城市热点等系统进行认证单点登录，简化用户操作，可强制指定用户、指定IP段的用户必须使用单点登录； |
| 6 | 认证方式 | 要求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； |
| 7 | 要求支持账号密码+动态令牌（Authenticator APP）验证码身份认证，支持通过短信和密码绑定动态令牌 |
| 8 | P2P智能流控 | ▲要求支持通过抑制P2P的下行丢包，来减缓P2P的下行流量，从而解决网络出口在做流控后仍然压力较大的问题；（提供产品界面截图） |
| 9 | 业务访问审计 | 要求支持WEB/FTP/SMB类型业务的行为和内容审计，对上传/下载文件可选择只审计文件名或同时审计文件内容； |
| 10 | 网页访问管理 | 要求支持SSL中间人解密和客户端解密，确保数据传输的透明性与安全性； |
| 11 | 要求支持根据访问的URL和网页关键字进行网页过滤，支持设置拒绝以IP访问网页行为；支持根据文件类型限制HTTP、FTP方式上传、下载行为； |
| 12 | 流量管理 | 要求能够实时看到各级流控通道的状态：包括所属线路、瞬时速率、通道占用比例、用户数、保证带宽、最大带宽，启用状态等； |
| 13 | 终端资产识别 | ▲要求自动发现网络里面的终端，并获取IP、Mac、厂商、操作系统等信息，设备必须支持PC、移动设备、哑终端、专用设备的发现和型号识别：至少支持Windows、Linux、MAC、瘦客户机等PC；至少支持手机、平板等移动设备；至少支持服务器、交换机、无线控制器等网络设备；至少支持打印机、投影仪、电视、摄像头、门禁系统等哑终端；支持自定义终端类型（提供产品界面截图） |
| 14 | 上网合规检测 | ▲本次所投行为管理设备要求支持与医院现有态势感知平台联动、在访问不合规/发生异常操作时可实现上网提醒、批量冻结账号（支持IPV4/IPV6）来保证发生上网的合规性及安全性；（需提供证明截图） |
| 15 | 日志中心 | 要求设置内置、外置日志中心；支持分级配置管理员日志查看权限，支持以USB-Key方式验证接入日志中心的管理员身份； |

**3. API防护系统(1台)**

|  |  |  |
| --- | --- | --- |
| 序号 | 功能项 | 指标要求 |
|  | 性能参数 | ★网卡要求不少于6个千兆以太网电口，不少于2路bypass,网络吞吐量≥2Gbps，应用层吞吐量≥1Gbps；并发TCP会话数：≥50万；HTTP新建连接速率: ≥于8000连接/秒；TPS处理性能：≥10000请求/秒 |
|  |
|  |
|  |
|  | 系统架构要求 | 部署方式：支持透明部署、反向代理部署、插件化部署和镜像部署； |
|  | 支持IPv4/IPv6双协议栈 |
|  | 动态防护能力 | 防扫描：可有效防止通过各类自动化扫描工具发起的漏洞扫描与探测，防护后无法扫描出高危漏洞； |
|  | 撞库防护：可有效防止攻击者通过自动化程序，发起撞库攻击或者暴力破解； |
|  | 恶意爬虫防护：可有效防止攻击者通过爬虫或其他自动化工具，搜刮网站上的页面、数据或敏感信息； |
|  | ▲浏览器真实性检测：能识别用户是否使用真实客户端浏览器，包括但不限于扫描器及其他高级自动化工具；（要求提供识别扫描器和自动化工具的截图） |
|  | 动态令牌功能：通过对当前访问页面内的合法请求授予在一定时间内有效的令牌，有效抵御网页后门及重放攻击等恶意行为，可设定令牌重复使用的次数、刷新令牌的频率、以及令牌的过期时间、配置指定路径的动态防护令牌可用次数； |
|  | 客户端指纹：自动在网页代码中插入JS检查代码，JS代码收集客户端环境信息，为每个客户端生成唯一的指纹标识。 |
|  | ▲客户端行为检测：能识别用户是否存在键盘鼠标行为，包括但不限于键盘行为事件、鼠标行为事件，从而识别是否是真人操作。（要求提供保护后的客户端行为截图） |
|  | Web应用安全防护能力 | 支持针对HTTP协议合规性检测，防范HTTP协议违规和异常攻击。 |
|  | 支持SQL注入、PHP代码注入、命令注入、跨站脚本（XSS）、跨站请求伪造（CSRF）等攻击防护。 |
|  | 支持Java反序列化攻击防护。 |
|  | 支持远程文件包含、本地文件包含、目录遍历、非法文件上传等攻击的防护。 |
|  | 支持对服务器信息泄露进行检测防护，支持对敏感信息进行隐藏。 |
|  | 支持网页防篡改功能，可以对指定的敏感页面进行缓存，并定期对网站页面与系统缓存的页面进行相似度比对，相似度高于设定阀值时，更新缓存，当相似度低于阀值时，产生告警，并只展示缓存的页面，即防止网页被篡改，同时减少管理员更新网站带来的误报问题。 |
|  | 支持Webshell等后门上传防护、支持对中国菜刀、冰蝎等工具对后门连接的阻断。 |
|  | 支持盗链防护。 |
|  | 支持丰富的自定义规则，可以针对多个条件组合，形成深度的WEB防护规则 |
|  | 支持WAF误报分析功能，以站点、路径、规则ID为聚合条件，根据命中次数进行排序，帮助管理人员分析和排查WAF误报的情况。 |
|  | 语义分析  支持语义分析引擎进行防护，至少具备SQL语义分析、XSS语义分析、JAVA OGNL语义分析三种语义分析技术，语义分析引擎支持威胁评分机制。 |
|  | 流量自学习  通过学习正常业务的URL参数的长度、参数类型、请求方法等数据，形成正常业务模型，从而提供精准的白名单防护策略，应对未知威胁 |
|  | 支持扩展的小程序安全防护能力 | 小程序合法性验证：验证请求是否由真实小程序客户端发起，防止假冒小程序的访问以及小程序运行环境威胁感知：要求防护系统具备小程序运行环境感知能力，包括电量和网络类型检测设备名称、设备厂商、手机电池电量、充电状态等设备基本信息、版本号、操作系统及版本、小程序版本、设备连接网络类型等信息。 |
|  | API资产管理 | API资产自动发现：支持自动识别API资产；自动对API资产路径进行评分，辅助应用人员确认该路径是否是API； |
|  | API资产确认和忽略：支持对自动发现的API信息进行手动确认和忽略，支持批量确认和忽略API信息； |
|  | API资产自动确认：支持对自动发现的API系统将自动确认到API列表中并分组，分组方式可指定分组和按域名分组。 |
|  | 自定义API接口规则：用户可以根据API的特征，自定义API规则，实现快速、精准识别，自定义参数包括：域名、端口、路径、请求方法、响应类型、请求参数。 |
|  | API接口样例采集：接口采样可视化展示，可对xml，json不同类型的接口进行请求和响应的数据展示，包括请求header和body, 响应header和body。 |
|  | API资产列表展现：支持展现已确认API及其详细信息，包括搜索、分组、方法、、状态、参数检测、风险类型、分类； |
|  | API资产列表信息配置：支持对API资产进行添加、编辑、删除、忽略等操作；支持批量对API资产进行移动、删除、忽略等操作；支持对API资产进行上线、下线操作，支持批量上下线操作； |
|  | API分组管理功能，实现对API分组、责任人的定义，支持API分组统计监控。 |
|  | 资产画像：实现对API的集中管理展示，监控API的运行情况，实现API资产管理、访问管理、活跃度管理、可用性管理，构建全API 访问视图。 |
|  | API 多租户分权：支持多租户，实现权限和数据隔离；为每个业务建立独立的用户账号；每个账号访问自己负责的域名、资产组，进行策略配置和资产管理；方便多业务部门协同管理。 |
|  | 支持把API参数自动学习的结果，一键应用到API合规参数检测中，对所学习的API参数取值范围和长度范围进行检测，检测内容包括：包括query参数最大个数、body参数最大个数、请求body最大大小、参数名称，参数位置，参数类型，取值范围，长度范围；对于超过阈值范围的请求参数进行告警。 |
|  | 威胁呈现能力 | 网站访问情况：提供网站访问情况的可视化报表，内容至少包括单个或多个网站的访问量、异常数量、请求趋势、响应状态码、来源客户端信息； |
|  | 支持针对API业务常用业务建立业务威胁模型，形成API业务威胁展示平台，建立的API威胁模型不少于2个，包括撞库、爬虫。 |
|  | 客户端来源呈现：提供访问网站来源客户端的可视化报表，内容至少包括客户端的IP地址、来源国家和城市、Referer、访问路径、User Agent、浏览器指纹等信息； |
|  | 支持风险接口流量识别，包括敏感信息泄漏、明文密码、弱密码、未鉴权、参数不合规 |
|  | 自动化工具识别报表：能够识别并标记对网站发起攻击的工具，识别自动化工具类型，并进行可视化呈现； |
|  | 系统维护功能 | 规则库升级：支持规则库在线升级和离线升级功能，可指定升级时间或选择只自动下载升级包后再手动升级。 |
|  | 过滤日志：包含时间、访问网址、来源IP地址、过滤规则及规则细节等； |
|  | 一键断网功能：支持一键断网功能，可指定站点，指定响应动作和设置定时器 |

**4. 数据库审计设备(1台)**

|  |  |  |
| --- | --- | --- |
| 序号 | 功能项 | 指标要求 |
| 1 | 硬件配置 | ★要求2U机架式，内存不少于32G，机械硬盘容量不少于4T，不少于6个千兆电口，不少于4个千兆光口，冗余电源，不少于2个扩展槽位，配置不少于20个云主机授权； |
| 2 | 性能要求 | ★要求吞吐：≥6Gbps，可审计流量：≥1Gbp，峰值SQL处理能力：≥40000条/s，日处理能力：≥3000万条； |
| 3 | 数据库协议类型 | 要求支持国内外≥40余种主流数据库协议，包括国产化/非国产化的关系型数据库、非关系型数据库等； |
| 4 | 要求支持Oracle、SQLServer、MySQL、DB2、Sybase、Informix、PostgreSQL、Teradata等数据库系统； |
| 5 | 要求支持Cache、Hive、Hana、clickhouse、Tibero、Solr、MongoDB、HBase、ElasticSearch、Redis等国际主流数据库系统； |
| 6 | 要求支持KingBase、DaMeng、Oscar、GBase、浪潮\_KDB、Highgo、GaussDB等国内主流数据库系统； |
| 7 | 审计规则组 | 要求内置多种数据库协议默认管控规则，包括Oracle、MySQL、SQLserver、PostgreSQL、Dameng、OSCAR、MongoDB、Sybase、DB2、Kingbase、SequoiaDB、Cassandra等多种协议分类，提供用户登录、高风险操作、SQL命令等出厂默认规则组，用户无需自定义可直接引用； |
| 8 | 内置默认审计规则 | 要求内置默认控制规则，包括用户登录、低中高风险操作、数据库DML、DCL、DDL等操作语句等规则定义，方便用户引用和制定控制规则； |
| 9 | 要求支持内置规则一键复制，可基于复制后的标准规则模板进行优化配置，满足用户精细化场景下审计需求； |
| 10 | 自定义审计规则 | 要求支持自定义控制规则，可定义控制规则告警级别、执行时间等；控制规则支持定义源目IP、源目端口、源目MAC、数据库名、数据库客户端、数据库用户名、SQL语句、返回码、SQL错误信息、数据库表名、返回结果集、影响字段、SQL模板等字段，结合与或非等逻辑运算进行规则设计； |
| 11 | 要求可将事件中的字段、自定义告警内容添加到告警描述中，使告警日志可读性更强，更易于理解和及时处置； |
| 12 | 双向审计 | 要求支持数据库请求和返回的双向审计，特别是SQL返回结果集、SQL语句响应时间、连接时长、表影响的字段、影响行数等内容； |
| 13 | 要求支持通过返回行数控制返回结果集审计大小，降低系统开销；可自行开启解析结果集，自定义配置结果集行数； |
| 14 | SQL操作审计 | 具备数据库操作类、表、视图、索引、触发器、游标、事务等各种对象的SQL操作审计； |
| 15 | 细粒度审计日志 | 要求系统支持详细的审计日志，审计字段包括访问数据库的时间、源目IP、源目端口、事件ID、源目MAC、应用协议、实名用户、规则名称、告警描述、数据库名、客户端程序、数据库用户名、SQL语句、返回码、SQL错误信息、影响行数、响应时间、返回结果集、业务URL、业务用户名、SQL操作类型、数据库表名、表影响字段、敏感类型等； |
| 16 | 一键加入规则 | 要求支持审计日志一键加入控制规则，一键加入基线； |
| 17 | 会话回放 | 要求支持查看会话回放，支持倍速回放，至少包括2倍速、3倍速、4倍速等，完整还原数据库操作情况； |
| 18 | 审计统计 | 要求支持审计字段统计功能，可按照所选审计字段查看统计数据和占比情况；默认显示Top100统计数据； |
| 19 | 二次分析 | 要求支持匹配查询条件后的查询结果分析，分析结果支持在线查看报表导出； |
| 20 | 主流业务协议审计查询 | 要求HTTP协议支持按HTTP访问域名、URL、请求类型、请求文件、Cookie、响应码等字段作为查询和统计的条件； |
| 21 | 要求Telnet协议支持按telnet命令、返回信息等字段作为查询和统计的条件； |
| 22 | 要求FTP协议支持按FTP用户名、操作命令、操作结果、传输文件名等字段作为查询和统计条件； |
| 23 | 复杂SQL审计能力 | 要求支持超长SQL语句审计，至少不低于5M；支持多层嵌套SQL语句的审计； |
| 24 | 要求准确审计绑定变量的SQL语句，分离式存储SQL语句保障数据库审计效率； |
| 25 | 要求有效分割、准确审计主流数据库协议的多SQL语句； |
| 26 | 端口重定向 | 要求支持端口重定向审计，在服务器端口变化动态协商为其他端口时同样能精确审计； |
| 27 | 实名审计 | 要求支持以用户名、源IP、部门、域名、主机名、邮箱、联系电话为条件的实名审计； |
| 28 | 业务关联审计 | 要求支持插件方式和非插件方式的业务关联审计，支持B/S业务系统三层关联审计，实现javaweb环境100%准确关联，包括但不限于Tomcat、Weblogic、Jboss服务器； |
| 29 | 白名单审计 | 要求支持白名单审计：系统使用审计白名单将非关注的内容进行过滤，降低性能消耗和存储空间占用； |
| 30 | 数据库自动发现 | 要求产品可精准识别流量中包含的数据库协议，自动发现网络中存在的数据库；展示包括其数据库类型、IP地址、端口号、发现日期，当前会话数、事务数等信息；可一键加入管理； |
| 31 | 数据库管理 | 要求支持展示加入管理数据库的数据库名、数据库类型、数据库IP端口、发现日期、今日会话数、今日事件数等； |
| 32 | SQL效率分析 | 要求以饼图展示正常SQL与慢SQL分布占比情况、TOP10慢SQL的详细分析：数据库用户名、源ip、SQL语句、SQL操作类型、SQL语句响应时间等要素； |
| 33 | SQL错误知识库 | 要求支持20000条以上数据库协议的SQL错误码，知识库至少体现SQL错误码、SQL错误信息、出错原因、解决办法等内容； |
| 34 | 弱口令扫描 | 要求支持对数据库的密码进行主动扫描，判断数据库的密码是否存在弱口令风险，扫描出的弱密码支持脱敏显示； |
| 35 | 应用流量监控 | 要求支持审计各个应用协议的流量大小和数据包数量，并以图表形式进行排名； |
| 36 | 要求支持自定义时间查看各个协议审计的流量趋势图，直观展示应用流量的监听情况； |
| 37 | 流量统计 | 要求柱状图的方式展示用户排名、协议排名、协议大类流量Top10；展示用户、协议、协议组的百分比、详细、总流量、上下行流量、平均速率、上下行平均速率、峰值速率、上下行峰值速率、总会话数、上下行会话数等详细信息； |
| 38 | 设备运行状态 | 要求支持首页直观展示产品的运行情况，比如并发连接数、每秒新建连接速率、版本号、运行时间以及CPU、内存、硬盘等资源占用情况； |
| 39 | 高危异常操作行为分析 | 要求统计图表展示数据库高危操作行为统计，可直观展示针对数据库删库、删表等高危风险操作，并展示受影响数据库详情； |
| 40 | 要求针对数据库的批量数据修改和泄露操作进行统计展示，协助用户判断潜在危害，点击柱状图可展示详情； |
| 41 | 攻击行为分析 | 要求支持以折线图的方式实时展示SQL注入风险发生趋势和数据库漏洞攻击趋势，并以表格的方式展示SQL和数据库漏洞攻击注入统计信息和攻击详情； |
| 42 | 要求以图表的形式展示当天存在疑似暴力破解行为的目标数据库分布；以图表的形式展示当天存在疑似暴力破解行为的目的IP告警事件数；展示当天疑似暴力破解次数统计，形成趋势图；图表的形式展示疑似暴力破解的详细告警信息； |
| 43 | 要求以图表的形式展示当天存在疑似撞库攻击的目标数据库分布；以图表的形式展示当天存在疑似撞库攻击的目的IP告警事件数；展示当天疑似撞库攻击次数统计，形成趋势图；以图表的形式展示疑似撞库攻击的详细告警信息； |
| 44 | 账号异常登录分析 | 要求数据库账号异常：以饼图的形式展示账户数最多的数据库TOP5分布数据； |
| 45 | 要求以饼状图的形式展示非工作时间登录数据库情况排行； |
| 46 | 事件趋势分析 | 要求以折线图的形式，展示5分钟、1小时、今天、近7天、近30天、近一年、自定义时间段，数据库操作事件趋势和告警趋势； |
| 47 | 敏感防护 | 要求支持对审计日志中敏感数据（身份证号、手机号、银行卡号等）进行掩码处理，进行隐私保护，敏感保护规则可自定义； |
| 48 | 敏感信息扫描 | 要求支持用户数据库中敏感信息的自动发现和手动添加，可定位敏感数据所在数据库名、实例名、表名、列名，并形成针对敏感信息的检测规则； |
| 49 | 危害分析 | 要求当审计事件在指定时间内累计发生次数或发生频率超过设定的阈值产生告警信息 |
| 50 | 一键巡检 | 要求支持系统本身主要运行功能服务模块的运行状态巡检，保证系统安全稳定运行； |
| 51 | AI智能问答 | 要求基于NLP算法和嵌入模型技术对用户问题进行语义理解，以交互式对话方式，支持智能分析用户意图、快速图文响应用户需求；内置数据检索分析、高危操作检索、数据泄漏事件查询、攻击事件分析等问题，可直接点击问题获取答案；支持按自然语言形式输入自定义问题，即可快速获取用户关心的数据，数据可以饼图、柱图、表格、文字等形式提供； |

**5. 日志审计设备(1台)**

|  |  |  |
| --- | --- | --- |
| 序号 | 功能项 | 指标要求 |
|  | 硬件指标 | ★要求软硬件一体化产品；2U机架式，不少于8个千兆电口，不少于4个万兆光口，不少于1个IPMI远程管理口，不少于1个console口，不少于6个USB接口，冗余电源，不少于64G内存，硬盘容量：系统盘不少于480G SSD系统盘，数据盘不少于16TB（配置Raid5），日志采集处理速度≥20000EPS，包含≥300个日志源授权； |
|  | 系统部署 | 要求支持单级部署；支持代理分布式部署采集日志；各级完全自制，独立管理本级日志；下级不需要把日志传到上级，上级可以直接远程查看、统计各级日志，节省网络带宽； |
|  | 系统性能 | 数据存储能力：要求压缩加密存储，压缩比不低10:1；日志存储不低于10000条/M；支持百亿级数据交互式多条件查询，百亿级数据查询响应时间小于10s； |
|  | 数据采集 | 要求支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于26类300种日志对象的日志数据采集； |
|  | 要求对于尚未支持的设备类型日志进行新增采集支持，在页面上传升级文件或增加配置文件即可； |
|  | 要求支持Syslog、SNMPTrap、Netflow、JDBC、WMI、FTP、SFTP、SCP、文件等方式进行数据采集；支持通过Agent采集日志数据； |
|  | 要求系统内置已支持设备种类清单，提供设备日志外发配置建议指导； |
|  | 要求支持日志归一化处理，将不同设备所产生的不同格式的难以理解的日志数据进行统一格式化处理，提炼出有用信息清晰、明确的展示给管理者； |
|  | 要求支持实时自动刷新每个日志源的实时日志列表，支持在实时日志界面通过选择过滤器来监视所关注的特定类型的日志； |
|  | 要求支持首页展示日志采集总量统计，可按不同日志源种类分类显示日志总量及大小，并支持导出； |
|  | 要求对于尚未支持的设备类型日志进行新增采集支持，在页面上传升级文件或增加配置文件即可；支持主动、被动相结合的数据采集方式； |
|  | 要求支持独立展示每个被采集源最近24小时的日志数量趋势，便于掌握设备的安全事件情况，支持独立展示每个设备日志的最新采集时间，便于了解设备日志的采集状态； |
|  | 要求支持对日志流量非常大但是日志重要程度低的syslog类型日志源进行限制接收速率，降低对系统资源的占用，保障重要日志的收集； |
|  | 要求支持对每个日志源设置过滤条件规则，自动过滤无用日志； |
|  | 要求支持日志转发给第三方系统平台，支持设置多个日志转发IP地址，支持转发格式化日志或仅转发原始日志； |
|  | 数据存储 | 要求支持对所管理设备的日志原始数据完整存储，支持数据本地集中存储、网络存储； |
|  | 要求支持根据设备重要程度设置独立设置每个被采集源的日志、报表数据存储时间为1个月、3个月、6个月和永久保存等参数； |
|  | 要求支持自定义存储位置，支持多盘并行存储，当磁盘满后自动切换存储位置，支持磁盘阵列、SAN、DAS等外部高性能存储； |
|  | 要求支持存储空间图像化、动态监控，超过阀值进行告警；支持从存储空间、存储时间多维度进行动态监控； |
|  | 要求支持日志备份功能，支持本地备份和FTP备份方式，支持自动备份和手动备份； |
|  | 数据查询 | 要求支持首页以全国地图、全球地图展示最近24小时日志访问源和访问目的的分布，能根据颜色区分访问来源和访问目的数据量大小，能够通过首页地图快速下钻查询指定区域的日志详细信息； |
|  | 要求支持实时日志查询，支持历史备份文件导入查询；支持等于、不等于、大于、小于、正则表达式等查询条件；支持多条件组合查询； |
|  | 要求支持对常用查询条件进行保存，可重复使用；支持查询条件缓存，通过快速调用系统右侧隐藏栏中缓存的查询条件，提升常用条件的检索速度； |
|  | 要求支持为不同类型日志设置不同的查询条件和显示条件；支持原始日志全文检索；查询结果可将归一化日志和原始日志同屏对比显示；支持展示日志查询情况，包括查询条件命中数、日志总量、查询耗时等信息； |
|  | 要求支持对重点日志源的关注设置，并可通过关注列表快速查看重点日志源的状态、当日日志量、采集日志总量、最近接收时间、业务组等基础信息； |
|  | 要求查询结果支持分页显示；支持查询结果格式化日志、原始日志导出； |
|  | 要求支持查询结果快速统计，可自定义统计主题规则，支持将多个主题添加为一个统计任务，以分、时、周、月、年定时执行自动统计，将统计结果报表发送到指定邮箱； |
|  | 要求支持基于时间轴展示日志数据分布，能够通过时间轴进行查询分析； |
|  | 要求支持多种运维管理工具，可对日志源进行HTTP、HTTPS、SSH、SCP、SFTP、FTP、MYSQL、ORACLE、SQLSERVER等操作； |
|  | 告警管理 | 要求支持首页展示当日告警情况统计；支持展示当日最新告警TOP10、TOP30和TOP50； |
|  | 要求内置系统运行相关告警规则，包括检测到新日志源、节点掉线、主动日志源长期不外发日志、存储上限告警、主机认证失败等，可启用/禁用规则； |
|  | 要求支持安全告警概况、安全告警趋势的统一展示，实时告警可根据级别、规则类型等进行分类； |
|  | 要求支持实时告警展示，可根据告警规则、告警级别两个维度进行实时告警监视，并可对刷新事件间隔进行设定； |
|  | 要求支持根据告警级别、告警规则类型、规则名称、时间范围、事件名称、设备IP、源IP、目的IP等方式快速检索安全事件告警，检索结果支持Excel等格式导出； |
|  | 要求支持基于时间轴展示告警数据分布，能够通过时间轴进行查询分析； |
|  | 要求支持在告警事件查询界面直接显示触发告警的关联日志，也支持点击跳转到日志查询界面； |
|  | 要求支持告警抑制规则设定，防止报警信息短时间内大量发送； |
|  | 告警响应方式 | 要求支持邮件、SnmpTrap、声音、声光、短信、一信通响应、数据库响应等多种告警方式，支持报警内容引用字段变量参数； |
|  | 要求可以针对不同类型、不同种类以及不同安全级别的安全事件制定不同的告警方式； |
|  | 统计报表管理 | 要求支持自动实现智能报表创建，每添加一个日志源，系统自动分析日志源类型进行相应报表创建，无需人工干预，报表和资产一一对应； |
|  | 要求报表需支持基于全国地图、全球地图进行访问源、访问目的追踪； |
|  | 要求支持自定义统计日志数据形成报表，支持统计分析报表以PDF、word、execl、html等方式导出；支持实时报表、计划报表； |
|  | 日志源管理 | 要求支持手动添加日志源，管理员可以对日志源进行查看、批量修改、添加、编辑、删除以及启\禁用的操作； |
|  | 要求支持按照日志源名称、IP地址、日志源类型、接受时间及状态等维度对日志源列表进行排序； |
|  | 要求支持为日志源指定类型、名称、IP地址、收集节点、收集方式、以及日志源启停状态等属性信息； |
|  | 要求支持日志源在线状态监测告警，实时监测日志源的可用性，可显示每个日志源采集日志的最近时间，实时展示每个日志源最近一天日志趋势变化； |
|  | 要求支持以业务角度将日志源进行分组，支持在日志查询时以业务组进行查询，支持在首页拓扑展示时以业务组进行展示； |
|  | 要求支持基于拓扑图的日志源相关数据信息快速查看；支持通过拓扑下钻查看对应日志源的日志、报表、告警数据； |
|  | 日志分析 | 要求系统内置常见安全事件关联分析规则； |
|  | 要求内置系统运行相关告警规则，包括检测到新日志源、节点掉线、主动日志源长期不外发日志、存储上限告警、主机认证失败等，可启用/禁用规则； |
|  | 要求支持基于策略的多日志源海量日志实时关联分析，发现安全事件实时告警； |
|  | 要求提供可视化关联分析规则编辑视图，可根据实际业务编辑关联分析规则； |
|  | 要求系统内置安全知识库，支持自定义增加安全知识内容，可在关联分析规则中关联知识； |
|  | 要求系统需内置多种维度的数据在线分析模型，在数据查询结果界面直接对查询结果数据进行多维度在线数据分析，分析结果实时展示，分析模型包括但不限于树图、散点图、关系图、折线图、时序图、柱状图等； |
|  | 知识库管理 | 要求知识库包含常见典型日志事件描述，支持自定义增加日志时间内容描述，支持在配置告警规则时关联知识库内规则； |

**6. 漏洞扫描设备(1台)**

|  |  |  |
| --- | --- | --- |
| 序号 | 功能项 | 指标要求 |
|  | 硬件要求 | ★标准机架式硬件，处理器：应采用通过中国信息安全测评中心安全可靠测评的国产处理器，主频不少于2.3GHz，不少于8核，交流冗余电源，不少于4T硬盘，不少于6\*千兆电口，不少于4\*千兆光口，≥2扩展槽位，不少于1个串口，支持无限IP授权，包含主机、弱口令、WEB功能模块。 |
|  | 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，漏洞发布日期、漏洞分类信息。 |
|  | ▲支持风险告警和风险闭环处理，可在集中告警平台灵活配置告警内容、告警方式、告警资产范围等，支持邮件和页面告警，支持单个或批量修改风险状态(提供界面截图)。 |
|  | 应具备单独口令猜测扫描任务，支持多种口令猜测方式，包括利用SMB、RDP、SSH、Telnet、SQL SERVER、MySQL 、Oracle、Sybase、DB2、MongoDB、Memcached、Redis 、PostgreSQL 、HighGo 、UXDB 、Kingbase 、STDB 、FTP、SFTP、ActiveMQ、POP3、Tomcat、SMTP、IMAP、Onvif、RTSP、 SNMP、SIP、Vmware ESXi、HTTP Digest、Weblogic、Elasticsearch、Websphere等协议进行口令猜测，允许外挂用户提供的用户名字典、密码字典和用户名密码组合字典。 |
|  | 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；支持自动模板匹配技术. |
|  | ▲支持自定义风险值计算标准配置，可对主机风险等级评定标准和网络风险等级评定标准进行自定义(提供界面截图)。 |
|  | 多权限用户管理 | 应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。 |
|  | 应支持多用户分级权限管理，可为每个用户角色分配账号、任务级的权限分配、允许登录的IP范围和允许扫描的IP范围等。 |
|  | 展示和报表 | ▲支持通过仪表盘直观展示资产风险值、漏洞总数、风险资产数/资产总数、扫描任务数、漏洞库新增漏洞TOP20，资产分类统计、资产风险等级分布、漏洞风险分布、风险TOP5、漏洞TOP5、风险数趋势图、整体风险值趋势(提供界面截图)。 |

**7. 流量分析系统(1台)**

|  |  |  |
| --- | --- | --- |
| 序号 | 功能项 | 指标要求 |
|  | 硬件配置 | ★要求2U机架式，不少于7个千兆电口，不少于4个千兆光插槽，不少于128G内存，不少于16TB存储，冗余电源； |
|  | 性能指标 | ★要求整机吞吐：≥3G，最大并发连接数：≥600万； |
|  | 检测分析感知引擎 | ▲要求拥有独立的安全分析引擎，覆盖32个大类42000余种攻击行为；支持文件还原和病毒检测，病规模1000万以上；拥有漏洞扫描知识库包含9万条以上的漏洞规则，覆盖十万条毒库以上CVE漏洞记录；拥有独立的学术地址库，识别全球学术地址网站及其他资源库1300种以上；（提供截图证明） |
|  | 要求拥有独立的应用感知引擎，识别主流网络应用3800种以上，支持私有业务识别规则自定义，规则类型应支持：传输层协议类型匹配规则、端口匹配规则、包长匹配规则、字节匹配规则、字符串匹配规则、IP地址匹配规则、相同数据匹配规则、URL匹配规则、HTTPContent-Length匹配规则、缓冲区匹配规则、HTTP\_REF匹配规则、HTTP\_AGENT匹配规则、HTTP\_HDR匹配规则、HTTP匹配规则、IPV6地址匹配规则； |
|  | 要求支持基于syslog数据格式实现会话数据、TCP/UDP数据、业务性能数据、安全及资产告警数据的第三方共享功能，图形化接口配置，自定义数据发送，同时保存外发数据日志记录，实现统一管理； |
|  | 可视化态势分析 | 要求基于大数据技术架构,结合机器学习,事件关联、趋势预测等技术,具备对整体网络的安全攻击态势、外联风险态势、横向威胁态势、流量性能态势、资产态势五个模块的独立完整展示分析；支持按不同时段统一展示网络流量、性能与安全态势数据，支持消息中心语音弹窗提示流量、安全、性能等方面的全局信息，并且可以实时、分时查询； |
|  | 流量监控分析 | 要求支持流量智能关联；能对网络流量的应用/应用组/资产/资产组/国家/省市/外部地址/虚链路/学术/vlan等维度之间的数据跳转关联与多维度的Drill-Down分析；支持5级用户组的多维度动态关联下钻及用户组自定义管理；并支持7元组会话记录的自定义检索与传输层指标关联分析，会话记录数据包含记录时间/端口/MAC地址/持续时间/总字节数/总包个数/速率等25个以上关键指标； |
|  | 要求支持链路层、网络层、传输层协议流量监测；包括对TCP/UDP/IPv4/IPv6/ICMPv4/ICMPv6/Unicast/Broadcast/Multicast/ARP/RARP协议的流量平均速率、最大值、最小值、中值和标准差的统计，各层流量要能支持趋势图分析，在各层流量的趋势图分析中支持对任意时刻的流量进行TOPN的数据关联，确定网络流量来源、识别其所对应的应用类型、追踪其传输的目的地；支持流量概况展示，查看当前时间段内的资产数、流量大小和应用、用户、外部地址的TOP流量排名等数据的汇总统计； |
|  | 要求支持流量实时监控；显示时间粒度必须可支持到1秒，并可实时查看当前流量的应用、资产、外部地址；支持对网络连接数的分析，分析的类型必须包含并发流、新增流、老化流，并能对上述指标的变化趋势进行可视化展示，监测网络负载变化； |
|  | 数据抽离分析，支持整体网络中抽离逻辑数据并独立分析，并结合整体镜像流量统计分析；支持以虚链路为基本对象，可设定任意IP（组）到任意IP（组）的虚链路，产看该虚链路下TOPN应用/应用大类/资产/资产组/国际/国内/等的出入境流量及包数目的变化趋势； |
|  | 要求支持流量TOP10/20/50/100/1000等综合分析，对网络流量的应用/应用组/资产/资产组/国家/省市/外部地址/虚链路/VLAN/学术/源端口/目的端口等进行单独监测，基于IP、MAC、总流量、总流量所占百分比、出/入境流量所占百分比、连接数、趋势图、安全状态分析等信息实现流量综合分析； |
|  | 业务性能分析 | 要求支持HTTP/HTTPS、DNS、Oracle、MYSQL、DB2、MSSQL、REDIS、IMAP、POP3、SMTP、TELNET、RTSP、RTP、MMS、SIP、RTMP、FTP、SMB、ICMP等核心业务的性能监控，包括2-7层数据指标分析，如登录状态、登陆时间、三次握手时间、登陆交互流程等信息呈现； |
|  | 要求支持对HTTP/HTTPS网页、DNS域名、ORACLE/MYSQL数据库、SIP语音、POP邮件等主流业务访问服务的综合评分与基于服务质量的指标评价分析，包括建立连接时间、响应时间、连接成功率等关键性能指标；支持对业务的综合对比分析，按地区、按服务器角度对比分析； |
|  | 要求支持对HTTP/HTTPS网页访问服务的综合评分机制，包括页面载入时间、首字节加载时间、dns解析时间、建立连接时间、网页元素加载状态等，支持网页种每个元素的获取周期不同阶段监控，如域名解析、建立连接、发送请求、等待响应、接收数据5个阶段，响应头信息包含Cache-Control、Connection、Content-Encoding、Content-Length、Content-Type、Date、Expires、Last-Modified、Server，请求头信息包含Accept、Accept-Encoding、Accept-Language、Cookie、Host、User-Agent支持对业务的综合对比分析，按地区、按服务器角度对比分析；支持http访问信息还原分析，包括Image、Application、Text、Multipart、Video、Message、Audio等方式还原访问场景； |
|  | ▲要求支持绘制关键业务系统服务路径图，能够将组成业务系统的各个组件（客户端、中间设备、服务端）之间的逻辑关系以图形化的方式进行呈现，并且支持业务预览；支持对服务路径图上各链路的性能指标进行监控预警，可监控的关键性能指标至少包含：往返时延、丢包率、重置率、零窗口次数、拥塞率、建联失败率、创建会话数、节点丢包率；同时也可以在服务路径的链路上呈现总流量、连接数、出入包数和TCP性能的相关统计指标，TCP性能的相关统计指标包括链路的平均时延、平均丢包率、平均拥塞、平均零窗口、平均重置等；支持以进度条的方式查看对应时间范围内的节点链路告警情况；（提供截图证明） |
|  | 网络性能分析 | ▲要求支持TCP端到端的网络性能监控分析，以会话记录为对象，监测指标包括C2S和S2Ctcp、cwr、ece、urg:、ack、psh、rst、syn:、fin、纯ack、payload、重传、乱序、错误、sack、tcp报文总大小、payload报文大小、重传报文大小、乱序报文大小、错误报文大小、rst报文所占比、重传包个数所占比、重传包大小所占比、错误包个数所占比、错误包大小所占比、拥塞率、报文数占比、报文大小占比、rtt最大值、rtt最小值、平均rtt延时、三次握手建立时间、是否支持sack、超时引起的tcp重传报文个数、快速重传的tcp报文个数、最大数据段长度mss、windowscale、滑动窗口最大值、滑动窗口最小值、滑动窗口大小为0的次数、接收端窗口最大值、接收端窗口最小值、接收端窗口初始值、吞吐量、传输速率(个数)、传输速率等指标展示了解该会话TCP连接状态；（提供截图证明） |
|  | 要求支持UDP会话性能监控分析；以会话记录为对象，监测指标包括记录时间、源地址、源端口、目的地址、目的端口、间隔时延、传输速率、报文大小占比、报文总大小、报文校验错误总大小等指标展示了解该会话UDP连接状态； |
|  | 要求支持网络环路、IP冲突、广播风暴、链路断开、丢包率、链路利用率、端口状态检测功能，可实时显示异常信息； |
|  | 要求支持服务端/客户端的网络性能综合评价；能够按照自定义时间段，从时延查看最快/最慢的服务器/客户端TOP10；从传输字节与连接数查看最闲/最忙的服务器/客户端TOP10；从重传、拥塞、零窗口、重置等指标查看最优/最差的服务器/客户端TOP10等，了解受网络性能影响的服务器/客户端状态； |
|  | 威胁流量监控分析 | 要求支持以事件类型为统计主体、事件类型包括：DOS攻击、DOS威胁、网络扫描、端口扫描、管理员提权、用户提权、信息泄露、木马攻击、非标准协议、协议命令解码、远程过程调用、异常ping、缓冲区溢出、内存溢出、系统漏洞、应用程序漏洞、sql注入攻击、跨站攻击、web程序攻击、web文件攻击、可疑流量、可疑加密流量、违规访问、可疑域名、可疑文件等；支持对某一类型事件的分析，呈现该事件发生的趋势、安全事件详情分析（包括事件类型、开始时间、结束时间、内网IP数、告警总量、发生链路），每一次告警事件的详细信息（包括告警时间、五元组信息、告警名称、告警类型、告警级别等），对告警事件触发流量进行抓包，并支持数据包在线解码和下载，支持安全事件白名单； |
|  | 要求支持网络行为分析模型建模，基于数据包特征、行为异常、业务状态等离散数据完成自学习，建立对如主动外联、可疑ICMP传输、DNS数据夹带、畸形数据包通讯、可疑规律通讯、非标准协议传输等多种可疑网络行为的分析模型； |
|  | 要求实时检测网络中传输（下载/上传）的木马、病毒和恶意软件；支持HTTP、SMTP、FTP、NFS、SMB等协议，zip、exe、apk、rar、dll、sys、jpg、doc、xls、pdf等文件类型； |
|  | 要求支持基于数据包重组技术的文件还原，支持的协议主要包括http、smtp、ftp-data、smb、nfs等，支持还原的文件类型包括jpg、txt、zip、exe、rar、jsp、php和其它常见的文件类型； |
|  | 要求支持基于威胁情报的威胁检测，支持对受威胁资产数、威胁源数量、威胁流量的趋势变化进行分析；另外可以从受威胁资产角度和威胁源角度对威胁访问行为进行记录并打上威胁标签，同时统计相关流量； |
|  | 要求支持安全规则自定义，可以依据网络流量、访问行为等自写安全检测规则；协议规则类型参数包含IP：Payload，ICMP：itype、icode；TCP：FIN、SYN、RST、PSH、ACK、URG、CWR、ECE；HTTP：uri、user\_agent、methodGET/POST/PUT/HEAD/DELETE、protocol、cookie、host、header、accept、referer、start\_code、start\_msg、client\_body、content\_len、content\_type、connection、request\_line等；通过配置源目的IP、端口、特征字符在payload中出现和位置、数据包标志位、数据包频率等多项参数指标定义安全事件，同时提供对自定义规则实时动态加载和取消加载； |
|  | 全流量溯源分析 | ▲要求支持通讯数据的回溯分析；会话记录数据包含威胁情报/链路质量/拓扑路径/记录时间/源地址/源端口/目的地址/目的端口/源MAC地址/目的MAC地址/应用/开始时间/持续时间/总字节数/总包个数/包速率等40个以上关键字段；支持流记录的自定义检索，如特定源目的IP、应用协议、源目的端口等；流记录分析支持按表格、逻辑连接TOPO图、访问矩阵图多种形式查看；支持网络连接关系自动发现，形成网络逻辑连接关系图展示网络流量、端口、协议等信息；（提供截图证明） |
|  | 要求支持网络数据的关联分析；包括业务性能、网络性能、网络会话、安全事件数据的相互关联，在业务性能中查看关联会话记录，在会话记录中可以查看关联网络性能指标，在安全事件中查看关联原始数据包，在安全事件中查看关联会话记录； |
|  | 要求支持通讯数据的回溯分析；会话记录数据包含记录时间/源地址/源端口/目的地址/目的端口/源MAC地址/目的MAC地址/应用/开始时间/持续时间/总字节数/总包个数/包速率等25个以上关键字段；支持网络连接关系自动发现，形成网络逻辑连接关系图展示网络流量、端口、协议等信息； |
|  | 要求支持全流量存储，支持按照五元组、协议等实现关键流量的数据包的存储，采样方式支持不采样、时间采样、个数采样三种，采集协议支持取反；数据包支持基于ip/ip段、端口、协议、时间等条件独立或者条件组合采集或者过滤规则的应用； |
|  | 要求支持原始数据报文自定义离线保存与在线解码，对TCP数据包解码提供时序图分析功能，能够图形化的显示TCP会话中的数据交互传输过程，能够图形化显示数据传输中的时间间隔、载荷长度、时间差、标识位等信息，支持流追踪分析，以数据流视图、十六进制视图的形式双向、自定义节点方向呈现报文信息；支持报文指标统计，包含查看次数、文件大小、开始抓包时间、抓包所用时间、平均抓包速率、文件类型、封装类型、数据位速率、包总数、数据字节速率、平均包大小、数据大小、结束抓包时间等多项分析指标； |
|  | 资产分析 | 要求支持系统主动扫描探测内网资产，资产类型包括：终端、服务器、交换机、虚拟机、路由器、打印机、防火墙等16个资产大类1500多种资产类型的探测识别分析，支持资产黑名单与合法名单管理； |
|  | ▲要求支持资产群体画像分析，主要从资产分群画像、资产业务分群画像、流量分布画像、资产画像趋势分析4个维度对资产群体进行总体监测和分析；资产分群画像呈现的主要内容包括资产类型分布、资产风险分布、风险资产类型、风险厂商分布、高危漏洞分布、高危端口分布；资产业务分群画像呈现的主要内容包括：风险服务器资产分布、活跃服务器资产趋势、业务访问分析、业务体验分析、应用/协议访问分析；流量分布画像分析呈现的主要内容包括：资产访问分布统计、流量分布分析、数据包大小分布、数据包大小协议分布；资产画像趋势分析呈现的主要内容包括：资产的行为趋势、性能趋势、风险趋势；（提供截图证明） |
|  | ▲要求资产主机画像分析，通过构建资产静态指纹与动态指纹分析模型，综合评估资产优良等级，形成资产特有的行为属性标签、运维属性标签、风险属性标签；静态指纹包含资产名称、类型、厂商、系统、状态、时间记录、漏洞分布、服务与端口、高危端口、特征异变分析等类型；动态指纹包含行为属性、运维属性、风险属性三个分析类，行为有访问应用、常用域名、国际位置等信息；运维有网络性能指标，业务性能指标分析；风险属性有多维雷达图分析与该资产安全访问关联节点分析；同时从流量、应用、风险、区域四个方面呈现该资产趋势状态，支持安全日志、病毒日志、威胁日志、行为日志分析；（提供截图证明） |
|  | 要求支持对资产的漏洞信息进行高效扫描，支持60种以上漏洞类型，包括Bufferoverflow，Bruteforceattacks，Databases，Malware，DenialofService，Webserver等常见漏洞类型；支持windows/Linux/AIX/FreeBSD/CISCO/HP-UX等主流厂商产品的漏洞信息； |
|  | 要求系统内置了弱口令信息库，支持对资产的弱口令风险扫描，弱口令信息库支持自定义添加； |
|  | 回放分析 | 要求系统支持对数据包的回放，回放速度可调、回放状态可以监测；回放完毕，通过切换数据开关，在系统界面可选择只呈现回放数据包所产生的流量、安全、性能、回溯的相关数据；支持数据包回放记录的查看，包括任务下发时间、结束时间、文件个数、大小、回放状态等信息； |
|  | 告警推送 | 要求系统支持异常流量告警、网络性能异常告警、安全事件告警、系统状态告警等，支持短信、邮件、弹窗等方式呈现、推送，支持告警详情查看； |
|  | 报表 | 要求支持资产风险信息报表，输出内容包括：资产厂商分布TOPN、资产类型分布TOPN、端口TOPN、N天内资产数量情况、待确认资产TOPN、安全风险资产TOPN、漏洞资产TOPN、病毒资产TOPN、行为建模分析TOPN、超过N天未上线的设备数量、场景分析TOPN、流量TOPN、连接数TOPN、业务性能分析TOPN等信息，综合判定资产风险，提前预警告警规避损失； |
|  | 要求支持资产流量分析报表，最多可以定制五个维度的业务系统报告和网络流量分析报告报表内容，包括应用、资产、地域、外部地址、网络层、传输层、链路层等流量指标可供配置选择；支持日表、周表、月表、季表、年表等不同周期统计方式； |

**8. 网闸扩容(1台)**

|  |  |  |
| --- | --- | --- |
| 序号 | 功能项 | 指标要求 |
|  | 系统基本架构 | 要求“2+1”系统结构，内外端机为TCP/IP网络协议的终点，阻断TCP/IP协议的直接贯通；内外端机之间采用专用硬件和专用协议进行连接，不可编程；网闸以软硬件结合的方式，有效地隔断内外网络间直接的连接，防止信息无限制交换； |
|  | 安全体系结构 | 要求控制台管理系统部署于内端机上，采用专有协议对设备进行管理，无法通过外端机直接连接到隔离系统； |
|  | 要求只能通过内端机上的管理口对网闸进行配置，不允许使用任何数据通讯口进行管理包括ssh后台管理；可避免内外端机由于被黑客从通讯口入侵，导致隔离网闸被黑客完全控制的现象； |
|  | 安全操作系统 | 要求采用安全操作系统、增强型内核，能够对两个主机系统提供多层次、高强度的安全防护，保护其重要进程、文件、数据不受黑客侵袭； |
|  | 要求操作系统基于Linux内核设计开发，全面加固强化安全防护能力；采用对象互斥和线程守护技术，保护主要进程的安全性和稳定性；不采用通用的指令库和函数库，只提供有限的内部调试用指令函数； |
|  | 要求内置IDS特征库，集成抗DDOS和病毒查杀功能，可抵御各类黑客入侵、拒绝服务攻击和病毒木马威胁，保证网闸系统自身的安全； |
|  | 硬件架构 | 要求硬件架构由内端机、外端机、专有隔离硬件三部分组成；内端机和外端机各自具有独立主板、独立总线、独立的存储和运算单元；内端机和外端机之间非网线、USB线、SCSI线等线缆直连，基于光隔离技术专有硬件进行隔离和数据交换； |
|  | 产品规格 | ★要求2U机架式结构，内端机不少于6个10/100/1000Base-T接口，2个SFP插槽，1个扩展槽位，外端机不少于6个10/100/1000Base-T接口，2个SFP插槽，1个扩展槽位；内外端双侧液晶屏；网络吞吐量：≥1Gbps；并发连接数：≥20万； |
|  | 安全邮件功能 | 要求提供安全的邮件访问，支持POP3、SMTP协议；支持邮件主机地址过滤、附件过滤；支持发件地址、收件地址过滤；支持内容过滤包括URL和关键字；支持情景模式，能够设置指定时间段允许进行邮件信息交换； |
|  | 要求代理、透明和路由工作模式下均支持POP3和SMTP协议内部命令及命令参数控制策略； |
|  | 文件传输功能 | 要求支持FTP文件传输协议，支持主动被动两种模式；支持FTP命令参数控制支持对传输文件的类型过滤；支持内容过滤；支持情景模式，能够设置时间段允许文件传输； |
|  | 要求代理、透明和路由工作模式下均支持FTP协议内部命令及命令参数控制策略； |
|  | 文件同步功能 | 要求设备支持有客户端和无客户端两种文件同步方式；无客户端方式无需在用户服务器上安装任何插件，网闸不开放任何服务端口； |
|  | 要求支持Samba、FTP、HTTP等多种通信协议；支持手动文件同步和自动文件同步；支持文件内容过滤；支持文件类型黑白名单传输控制；支持windows平台和linux平台；同步传输方向可控，双向或单向；支持一对多或多对一文件同步；支持目录内子目录同步，至多支持32级目录；支持中文文件名或目录同步； |
|  | 要求支持文件变动实时同步、定时同步、系统资源空闲智能同步等多种同步方式； |
|  | 要求支持同步删除和同步覆盖策略配置，并能将同步删除和同步覆盖的文件备份到指定文件夹； |
|  | 要求支持文件同步容错策略和告警策略，同步出错能够自动重传并能够设置重传次数，出现异常同步状况能够终止同步弹出告警提示并记录日志； |
|  | 数据库访问功能 | 要求提供对多种主流数据库,如：MYSQL、SQLSERVER、ORACLE、DB2、SYBASE等系统的安全访问；支持SQL语句控制；支持情景模式，能够设定特定时间允许访问数据库； |
|  | 要求代理、透明和路由工作模式下均支持数据库内部命令及命令参数控制策略； |
|  | 数据库同步功能 | 要求设备支持有客户端和无客户端两种数据据库同步方式；无客户端方式无需在用户服务器上安装任何插件，网闸不开放任何服务端口； |
|  | 要求有客户端方式可提供专用文件同步客户端安装在用户服务器上，提供安全的数据库同步服务； |
|  | 要求提供多种主流数据库系统如：ORACLE、SQLSERVER、MYSQL、SYBASE、DB2等之间的同步； |
|  | 要求支持达梦、人大金仓等国产数据同步； |
|  | 要求支持客户端与网闸数据摆渡通道数据特征绑定，确保只有授权的合法数据表记录可以通过网闸； |
|  | 要求数据库同步传输不使用通用数据库服务端口例如1433、1521、3306等，保障数据库同步传输的安全性；支持同构、异构数据库之间的同步，同步可具体设置到字段级别；支持全表复制，支持多种增量同步方式，可分别定义增加、删除、修改的同步方式； |
|  | 要求支持二进制普通文件、图片、文本文件及BLOB大字段同步；支持数据一对一、一对多、多对多的单向或双向交换和同步；支持灵活的数据冲突检测机制，当同步的数据记录发成冲突时，可以灵活处理出现冲突的数据记录； |
|  | 要求数据库同步高可靠性，即使发生网络故障，已变化数据也不会丢失；无需修改数据库表结构，不涉及到代码修改及二次开发； |
|  | 视频监控 | 要求采用复杂对称多处理（RSMP）技术，成倍提升处理能力，使网闸能够满足高并发、高质量、多路视频数据交换要求； |
|  | 要求根据策略配置可以控制视频数据的单向传输；内置视频监控模块，提供视频代理功能，兼容主流视频传输及控制协议H.323、H.264、MMS、RSTP、SIP等； |
|  | 要求至少支持13家视频厂商的流媒体视频平台；支持视频平台级联，基于国标SIP协议提供上下级异构厂商视频厂商的平台级联，完成上级对下级视频平台的视频流调用； |
|  | 要求支持对平台级联通信过程中的视频信令进行黑白名单控制；支持情景模式，能够设置视频监控允许传输的时间； |
|  | OPC工控应用 | 要求可扩展支持DCS/SCADA网络与办公网络之间的OPC应用数据的传输； |
|  | 要求支持同步、异步监测数据的传输，只需要绑定固定的一个起始端口即可满足动态的数据端口的数据传输；支持OPC读写指令控制，提供所有指令可读或可写模板；支持情景模式，能够设置OPC工控应用允许通信的时间； |
|  | ModBus工控应用 | 要求可扩展支持DCS/SCADA网络与办公网络之间的ModBus应用数据的传输； |
|  | 要求支持ModBus控制协议解析及内部命令控制，支持协议功能码控制，例如读写线圈、读写寄存器的控制； |
|  | WINCC工控应用 | 要求可扩展支持DCS/SCADA网络与办公网络之间西门子WINCC应用数据的传输； |
|  | 要求支持西门子控制协议解析及内部命令控制，支持协议功能码控制，例如只允许读取，不允许写入控制操作； |
|  | TCP单向无反馈传输 | 要求支持TCP应用层数据单向传输的控制，保证TCP应用数据的0反馈，以满足二次防护对数据传输的安全性需求； |
|  | 组播应用 | 要求设备支持多任务的组播代理功能，可穿透三层交换机网络进行部署； |
|  | 要求支持任意源组播、指定源组播、过滤源组播三种安全处理模式，支持对信源地址的黑白名单控制； |
|  | 自定义功能 | 要求支持自定义的TCP、UDP协议的数据隔离交换，以用户定制的命令、参数等协议解析方式来解析自定义应用的通信内容，支持16进制数据格式的定制； |
|  | 要求用户自定义应用无需对自定义协议软件进行二次修改开发；提供二次开发，可以根据需求开发新的专用协议处理过滤功能；支持情景模式，能够控制自定义应用的访问时间； |
|  | 双机热备 | ★要求支持与原有网络中的网闸进行热备，达到与原有设备双机切换功能； |

**9.** **应用负载设备扩容(1台)**

|  |  |  |
| --- | --- | --- |
| 序号 | 功能项 | 指标要求 |
|  | ★产品形态 | 要求采用独立的专用硬件AD应用交付设备，而非通过添加功能模块的方式实现 |
|  | 硬件规格 | 要求千兆电口不少于6个；千兆光口不少于2个；系统内存不少于8GB；提供SSD固态硬盘，硬盘容量不少于128GB；冗余电源； |
|  | ★整机性能 | 要求吞吐量≥5 Gbps；并发会话数≥800万；四层新建能力（CPS）≥15 万；七层新建能力（RPS）≥15万; |
|  | 多合一功能集成 | 要求单一设备可同时支持包括链路负载均衡、全局负载均衡和服务器负载均衡的功能。三种功能同时处于激活可使用状态，无需额外购买相应授权； |
|  | 链路负载均衡 | 要求支持静态IP和PPPOE两种线路接入方式； |
|  | ▲要求支持基于URL的链路调度功能，内置不少于10万条的国外URL网址库，无需手动导入并支持自动更新，管理员可查看。可根据URL将访问国外网站的请求调度到指定线路；（提供国家信息安全测评中心、公安部信息安全产品检测中心、中国泰尔实验室任一家国家权威机构相关证明材料或提供封面具有“CMA”或“CNAS”标识的检测报告） |
|  | 要求支持DNS透明代理功能，可基于负载均衡算法代理内网用户进行DNS请求转发，避免单运营商DNS解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率； |
|  | 服务器负载均衡 | 要求支持轮询、加权轮询、按主机加权轮询、加权最小连接、按主机加权最小连接、动态反馈、最快响应时间、加权最小流量、最小流量、最少连接、主机-最小流量、主机-最少连接调度、动态反馈、按主机加权最小流量、源IP源端口哈希、源IP哈希、URI哈希和HOST哈希等； |
|  | 要求支持优先级算法下最少可用节点保障，保证优先级高节点的可用性； |
|  | 要求通过某种编程语言（如lua）实现自定义的流量编排，对IP、TCP、UDP、SSL、HTTP和HTTPS等类型的流量进行分发、修改和统计等操作，具备对可编程脚本语法的校验功能，能够识别出脚本语言是否正确，定位到具体的错误语句； |
|  | 要求支持对虚拟服务、节点设置上行和下行流量限制，方便用户管控服务的压力； |
|  | 全局负载均衡 | ▲要求支持标准的DNS服务，支持正向解析和反向解析功能，支持常用的记录类型，包括A、AAAA、CNAME、DNAME、MX、NS、TXT、PTR、SRV、DS、CAA、HINFO和NAPTR等；（提供国家信息安全测评中心或公安部信息安全产品检测中心出具的相关证明材料或提供封面具有“CMA”或“CNAS”标识的检测报告） |
|  | 要求支持Anycast方式发布DNS VIP地址，可实现跨数据中心的DNS高可用； |
|  | ▲要求内置互联网公开的根服务器(包括Ipv4和ipv6)，并且可自定义根服务器，支持一键恢复默认值；（提供国家信息安全测评中心或公安部信息安全产品检测中心出具的相关证明材料或提供封面具有“CMA”或“CNAS”标识的检测报告） |
|  | ▲要求支持通过Web页面进行智能DNS解析规则测试；（提供国家信息安全测评中心或公安部信息安全产品检测中心出具的相关证明材料或提供封面具有“CMA”或“CNAS”标识的检测报告） |
|  | 要求SLB能够通过健康检查来获取后端服务器状态，同时将服务可用性、设备CPU、新建并发吞吐等数据上报GSLB，设备之间的联动使得GSLB能根据链路和服务器两者的综合状态实现智能切换，为用户选择最优的数据中心和服务器分配方式； |
|  | 要求支持设置允许递归的访问控制列表信息，避免递归查询带来的性能消耗，同时防止递归放大攻击； |
|  | SSL卸载 | 要求设备支持制作RSA2048算法的CSR证书请求和导入； |
|  | 要求管理页面可查看证书算法、证书有效期开始和结束的时间等所有证书信息； |
|  | 高可用性 | 要求支持会话保持表项与连接表项独立同步功能，可根据使用需要定义同步的会话保持表； |
|  | 要求支持基于vlan链路的零流量状态来进行高可用故障切换； |
|  | ★要求支持与原有网络中的负载均衡设备进行热备，达到与原有设备双机切换功能； |
|  | 运维管理 | 要求支持全中文管理界面HTTPS方式登录、SSH命令行方式管理、用户角色管理、多级授权管理，HTTPS登陆时可设置TLS协议版本SSH登陆时可设置加密算法、SSH MAC算法和SSH密钥交换算法； |
|  | 要求支持大数据输出功能，输出必须包括客户端IP、x-forwarded-For IP、访问时间、访问IP、访问URL、响应时间和资源大小； |
|  | 要求支持启用RAS事件告警，当设备PCIE或内存出现硬件故障时发送RAS告警； |
|  | 要求支持设备巡检功能，被检测设备无需访问互联网，实现离线巡检，并且可针对安全巡检、功能巡检以及健康巡检等多场景进行需要巡检的模块； |

**10.杀毒软件扩容（1套）**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 功能项 | | 指标要求 |
|  | 授权扩容 | | ★在我院现有云主机安全防护平台上扩容授权的方式增加不少于50台云主机的安全防护授权，授权功能包括：主机防病毒防护，主机防火墙，主机入侵防御。能对接本院现有云安全管理中心，实现统一管理。 |
|  | 安装部署要求 | | 要求系统支持两种安装部署模式，需要安装客户端的轻代理模式和无需安装客户端的无代理模式，两种模式可以混合使用 |
|  | 轻代理模式客户端要求支持Windows、RHEL、CentOS、Oracle Linux、SUSE、Ubuntu、Debian等操作系统。 |
|  | 要求系统提供Windows和Linux批量化安装部署脚本，主机分组、安全策略、更新源等脚本内容参数支持用户按需选择，并自动生成。 |
|  | ▲无代理模式要求支持VMware vSphere， 新华三CAS（提供华三认证证明材料）、深信服等云平台 |
|  | ▲要求无代理部署支持宿主机及虚拟机的防护，vmware环境无代理方案可不依赖于NSX进行部署。 |
|  | 要求系统控制台支持横向扩容，支持多节点集群化部署，保证系统高可用性。控制台离线，客户端仍可进行安全防护。 |
|  | 要求支持接入外置企业级数据库，防止因数据库异常导致数据丢失，安全策略无法下发，包括且不限于SQL Server， Oracle，Postgresql等。 |
|  | 主机管理要求 | | 要求支持通过网络掩码或 IP 范围查找未安装客户端的计算机，并且将发现的IP解析为主机名方便管理 |
|  | 要求支持Linux、windows客户端在同一页面进行集中管理 |
|  | 主机防病毒功能 | 扫描模式 | 要求支持本地扫描和云扫描，支持实时扫描（文件落地即扫描）、预设扫描、手动扫描和快速扫描；如发现特殊情况 （如业务高峰期），可支持终止操作。 |
|  | 勒索病毒 | 要求支持通过行为监控的方式，如检测可疑活动和未经授权的更改，防止勒索软件感染，并提供针对勒索软件事件专有历史纪录和勒索软件统计的监控组件 |
|  | 挖矿病毒 | ▲要求支持挖矿行为监控及告警，支持提供主机“银狐木马”专杀工具 |
|  | 处理措施 | 要求提供多种病毒的处理措施：包括不限于清除、删除、拒绝访问、隔离、不处理等，并针对不同的恶意软件类型，定制处理措施。 |
|  | 未知威胁查杀 | 要求支持和外部沙箱实现集成，同步沙箱的检测结果，检测未知威胁并处理 |
|  | 恶意站点拦截 | 要求具备web信誉库，通过Web信誉支持阻止主机访问恶意站点，支持恶意站点自定义 |
|  | 主机防火墙 | 网络访问控制 | 要求支持网络访问控制功能，自定义防火墙策略，支持IP、MAC地址、端口，支持协议：TCP、 UDP、 ICMP、ICMPv6 、IGMP、IDP等，支持IPv4、IPv6、ARP、RARP等 |
|  | 侦查扫描检测 | 要求支持检测扫描器、黑客工具对主机的探测侦察，支持扫描IP的阻断周期设置 |
|  | 入侵防御及漏洞防护 | 入侵防御 | 要求支持网络入侵攻击的防护，包含支持防护SQL注入,Cookie 注入，命令注入，跨站脚本(XSS)，跨站请求伪造(CSRF)，WebShell攻击防护等， |
|  | 要求内置入侵防御的规则库，支持关联ATT&CK框架的技术ID，便于了解网络入侵技战术点。 |
|  | 漏洞防护 | 要求通过流量检测技术，实现漏洞利用的攻击防护，支持操作系统、数据库、邮件服务、办公软件、中间件、Web应用、应用等类型的漏洞 |
|  | 漏洞扫描 | 要求提供操作系统和应用漏洞扫描功能，根据扫描结果自动下发对应的防护规则 |
|  | 定制规则 | 要求支持0Day漏洞暴露后，快速定制入侵防御规则，包括不限于签名、特征码、XML等方式，进行0day的快速防护，同时可支持配置优先级、检测或阻止模式、严重性等 |
|  | 虚拟补丁规则 | ▲要求支持虚拟补丁规则自定义，内置虚拟补丁规则不少于8000条 |
|  | 主机加固 | 资产清点 | 要求支持对主机的基本信息、账号、应用、安装包、启动项、端口、web服务、数据库、计划任务、内核模块等资产类别进行清点 |
|  | 漏洞扫描 | 要求支持对Windows、Linux系统及系统中的Web服务、数据库及其他应用的漏洞进行扫描，给出编号、漏洞名称、危险程度、CVE编号及修复参考建议；并支持高价值漏洞、POC检测以及漏洞处置优先级(VPT) |

**四、服务需求**

*1、中标供应商在供货时，必须提交生产厂商出具的书面质保证明材料，保证该设备为原厂全新产品且由原厂提供不低于伍年的免费维保服务，包括但不限于设备免费硬件维保服务、软件升级服务、电话技术支持服务以及定期上门巡检服务等。*

*2、中标供应商应在中标一周内提供所投运维管理软件到用户现场环境测试, 对招标参数的每项指标均进行功能有效性验证，以确保产品实际质量及交付功能满足需求，以上招标要求的各项指标验证测试,经确认无误后签订合同。若测试结果与投标文件中提供的技术偏离表不一致,用户方有权追究其责任。*

*3、中标供应商在项目实施过程中不得影响全院正常工作，不得更改医院现有网络架构，必须在保证医院业务不受影响的前提下完成本项目的事实。*

*4、中标供应商必须为本项目中所有的设备提供全年7×24小时驻场服务，明确到人，晚班值班人员不得无故离岗、脱岗。*

*5、中标供应商按要求提供完整的项目建设档案，包括施工方案、竣工和技术文档、使用说明等；*必*须按医院三级等保整改报告相关要求部署安装本项目里相关设备，并配合医院完成本次等保测评工作，否则不予验收。*

6、中标供应商所提供的设备必须为全新生产，设备到货后，用户方将与供应商及生产厂商代表三方共同对设备进行非破坏性拆解验收，如发现设备内部有长时间使用、维修痕迹以及主要零部件生产日期过久等异常现象而供应商对此不能做出合理解释的话，则用户方将终止合同、并报政府采购监督管理相关部门进行处理， 供应商应承担相应违约法律责任。

7、中标供应商提供 7\*24 小时售后服务，须确定专人接受采购人故障申告。接到申告，0.5小时内到达现场，并在到达现场后4小时内将故障修复。4小时内不能修复的，启动备品备件的调用，设备修复后予以恢复。

8、要求中标供应商提供本项目的相关设备的巡检服务，次数不低于每月一次例行巡检，并出具一份设备巡检报告。配合用户根据运行环境和要求调整性能参数，并根据用户系统变化情况及时调整优化，供应商必须配合采购人完成内外网接入整改工作。对重大的技术问题，供应商应协调组织技术专家小组进行会诊，以确保系统的正常运行。

9、在重大活动时，根据采购人要求，中标供应商派出资深工程师做好现场技术保障。

10、中标供应商提供关于本项目的培训方案，投标人在产品安装调试时，对采购人的技术人员进行现场安装调试培训，讲解产品的结构、安装步骤、调试方法和系统配置等。

11、本项目为交钥匙工程，采购人不再承担任何配套费用。对本次采购的所有软硬件、配件、辅件在到货检查及质保期内应确保货物的正常使用，出现故障等情形必须按同型号无偿更换，提供免费上门维修。免费质保期内，不能修复时中标供应商必须免费提供同种规格配件进行更换，如不能提供同种规格型号的配件，用其它型号配件代替时，需经采购人同意，且不补差价。免费质保期后产品实行终身有偿维修，并且保证在设备的设计使用寿命周期内，能够及时提供原厂正宗的零备件，中标供应商只收取材料费，以确保设备的正常运行。投标人必须承诺后续服务、硬件的配件和软件的选件能以不高于本次采购的价格（或折扣率）购买。

**五、项目实施要求**

项目实施方案需包含项目组织、进度计划、项目风险管理、应急措施网络规划设计等，内容详实，措施得当，阶段划分合理。

（1）成立项目组

首先成立专业的项目组。项目组负责项目的具体施工、测试、验收等工作，并对施工进度与质量负责。按照项目实施的标准流程在招标方要求的时间内完成交付。

（2）制定详细的项目建设计划

项目启动后，需要立即组织项目相关的所有人员熟悉本项目相关的所有细节，熟悉项目的具体内容，制定详细的施工计划与进度表。项目计划文档至少包含如下内容：

1. 项目施工人员名单，确定联络人，项目组人员的具体分工与职责；
2. 实施过程需要的工具与设备；
3. 具体的施工计划与详细的进度表；
4. 具体的施工方案文档编写与汇总，每个节点都需要提供施工方案文档；
5. 阶段性的验收报告；
6. 施工过程中意外情况的处理；
7. 培训的时间、内容、规模等；
8. 明确具体的安全策略、测试方法、验收标准、完工文档等。

（3）工程勘察

提前与招标方确认好施工时间，在正式施工前提前进行勘察，勘察后编写《工程勘察纪要》，确定设备的安装和集成详细部署方案。

（4）发货与进场施工

按照招标方要求的时间发货，安装施工人员负责综合布线与设备上架，完成设备互联调试工作，编写实施文档等工作。

（5）项目施工质量管理

为了保证施工质量，需要制定质量管理计划、质量控制标准、质量保证措施、沟通管理计划、变更管理计划等。

（6）项目风险管理

在工程实施过程中，需要进行风险管理。风险管理内容至少包含风险识别、风险预警、风险量化、风险对策实施控制等。

（7）应急措施

针对施工过程中的突发情况，需要提前准备应急措施，应对如何在施工时受到意外事件影响而进行恢复。

（8）服务质量控制方案

在实施期间双方将本着友好合作的态度完成各自的职责。需要制定成熟可行的方案以保证招标方在整个项目施工过程中任意阶段（比如安装阶段、验收阶段、日常维护阶段）对服务质量不满意的情况下，能够得到及时的响应与改善。

（9）项目培训

为了保证项目的质量与运行、维护需要，对产品和系统使用的相关人员进行系统的技术培训。

**六、项目集成要求**

（1）负责完成产品免费到货、安装到指定地点和位置，并完成具体的系统安装调试至全部系统投入上线稳定运行。

（2）提供项目实施所需的线缆等辅材。

（3）负责完成项目相关的数据中心容灾网络与数据中心现有网络环境和相关设备的梳理、整合、对接部署、系统调试、网络与安全策略调整、联调优化等服务。

（4）负责完成相关安全设备的安装部署、操作系统的安装、配合应用的部署、有关服务器的配置调整与联调部署服务。

（5）负责完成有关设备迁移、系统迁移、应用迁移、数据迁移、数据备份与恢复、业务部署等技术服务。

**七、项目验收要求**

（1）验收工作由招标人组织实施，由招标人、中标人及原厂商共同完成。

（2）中标人保质保量、按整体解决方案如期完成全部工作，满足项目的全部建设要求。

（3）中标人应按照招标人要求，移交本包实施过程中的各类文档，并经过招标人验收签字。文档包括以下材料:设备及集成系统交付清单；用户使用手册(含设备及集成系统配置清单、用户操作手册、维护手册、安装手册等)；基础测试分析报告（含集成测试大纲、测试结果记录，要有测试负责人得签字或测试单位盖章）；项目施工过程文档、实施总报告等。

（4）中标人应就安装、调试、集成工作，采取文档讲解、会议研讨、培训、在日常工作中进行传帮带等方式，完成对招标人的知识转移工作。

**八、投标人履约能力评价的要求**

（1）中标人应按照招标人要求，具有国家认监委认可的机构颁发的有效期内的ISO9001,ISO27001，IS020000，ISO22301认证证书。

（2）中标人应按照招标人要求，项目负责人具有信息系统项目管理师、注册信息安全专业人员CISP证书。

（3）中标人应按照招标人要求，项目组成员中（除项目负责人外）提供1名软件设计师、2名系统集成项目管理工程师、1名CISAW信息安全保障人员，1名网络工程师（中级及以上），1名ITSS IT服务项目经理。

（4）中标人应按照招标人要求，具备自2020年6月以来类似项目案例。

**八、商务条款**

1.项目工期：签订合同后30天。

2.交付地点：江苏省镇江市解放路438号江苏大学附属医院

3.付款方式：合同签订生效后2个月内，甲方向乙方支付合同总金额的30%，项目竣工验收合格后2个月内,甲方向乙方支付合同总金额的50%。尾款支付时间：20%尾款在设备能够正常使用，且乙方能够履行本合同约定义务的情况下，填写付款证明，自入库之日起1年后2个月内付清，如因乙方发票不能及时提供而影响设备入库手续，则付款以入库日期顺延。