# 安全网关

|  |  |  |  |
| --- | --- | --- | --- |
| **参数性质** | **序号** | **指标项** | **技术参数** |
| √ | 1.    | 性能要求 | 推荐带宽800Mbps；整机吞吐≥8Gbps；最大并发数≥300万；最大新建数≥10万/秒； |
| √ | 2 | 硬件要求 | 标准≥1U机架式；硬盘：≥500GB HDD；电源：双电源；千兆电口≥12个(含1对电口Bypass），管理电口≥1个，千兆光口≥12个，不带光模块 |
| 0 | 3.     | 部署模式 | 支持网关模式、网桥模式、旁路模式、虚拟网线工作模式、混合模式；部署模式切换无需重启设备 |
| 0 | 4.     | 4G支持 | 支持4G USB插卡接入，实现4G连接，与有线链路之间互为备份；并支持在4G接口上运行IPSec VPN  |
| 0 | 5.     | NAT | 支持IPv4/IPv6双栈协议的源地址转换、目的地址转换、双向NAT、NAT44、NAT66、NAT46、NAT64等地址转换 |
| 0 | 10.    | DNS | 可实现DNS透明代理；支持指定DNS或继承链路DNS配置，针对多链路支持基于优先级、权重、流量算法进行DNS负载 |
| 0 | 11.    | IPv6 | 支持IPv6/IPv4双栈；  |
| 0 | 12.    | 支持IPv6安全策略、包括审计策略、NAT策略、流量控制策略、会话控制策略、黑名单、白名单、认证策略等 |
| 0 | 13.    | 端口扫描 | 支持针对IP、端口进行端口扫描，可选择立即执行或定期执行；支持呈现扫描结果，包括端口、端口状态、端口服务、程序版本、操作系统、风险状态、设备类型和时间等信息，支持导出功 |
| 0 | 14.    | 其他防护 | 支持非法外联学习和防护特性，可有效保障服务器安全，可定义外联白名单地址和端口；支持通过流量自学习获得服务器合法的外联行为，检测流量中的异常访问流量，实现自动拦截；学习时长可选择1小时、12小时、一天、一周等。  |
| 0 | 15.    | 应用识别 | 应用特征不少于7000个，移动应用不少于2200个 |
| 0 | 16.    | 支持应用智能识别，有效识别迅雷和P2P行为，识别模式可选择严格、适中、宽松，支持排除扫描端口 |
| √ | 17.    | 用户认证 | 可实现本地WEB认证、微信认证、短信认证、portal server、免认证、SAM认证、单点认证、访客二维码认证、IC卡认证、APP认证、POP3认证、钉钉认证、企业微信认证、混合认证，以上参数提供Web配置界面截图 |
| 0 | 18.    | 防私接路由  | 支持防网络共享行为，针对私接路由器和非法无线热点行为进行识别和阻断 |
| 0 | 19.    | 支持自定义配置终端数量、冻结时间和添加信任列表；支持例外排除功能，可针对终端类型分别设置阀值数量。 |
| 0 | 20.    | 针对私接网络行为，惩罚方式包括但不限于无操作、阻断和限速，阻断和限速支持自定义惩罚时长 |
| 0 | 21.    | 代理上网 | 支持HTTP、SOCKS4、SOCKS5等方式代理上网，实现内部用户通过设备代理的方式接入互联网，可以隐藏真实IP，避免被探测和攻击 |
| 0 | 22.    | 广告推送 | 可实现广告对象设置，包含广告名称、广告描述、广告类型（本地自定义广告、第三方广告）、设备管理IP、位置、广告图片；同时针对广告推送策略进行针对性配置，包含推送间隔、动作、广告类型、设备管理IP、广告对象、用户、源地址、目的地址、时间 |
| 0 | 23.    | VPN | 支持标准IPSec VPN和快速IPSec VPN；同品牌设备快速IPSec VPN对接时加密算法等参数无需配置，自动生成，仅需配置保护子网、共享密钥、IP地址 |
| 0 | 24.    | 支持IPSec VPN、SSL VPN 、GRE VPN；支持手机、平板电脑等移动终端VPN接入，功能标配，无需增加功能授权即可使用 |
| √ | 25.    | 其他要求 | 中标后5日内，要求中标人部署设备到招标人现场进行参数符合性测试，对所有功能、参数指标进行逐一测试匹配，超过指定时间范围参加测试视为自动放弃中标资格；中标人完全满足后进行合同签订等其他后续流程。一旦发现中标供应商存在虚假应标行为，将立即废标该供货商，同时根据项目总体金额10%进行罚款，虚假应标供应商列入政府采购黑名单，并追究其相关责任 |
| 注：1.“参数性质”栏中划“0”表示此参数为一般性技术参数，划“√”表示此参数为重要技术参数。2．重要技术或服务参数（要求） 不接受负偏离。　 |

# 日志审计分析平台

|  |  |  |  |
| --- | --- | --- | --- |
| **参数性质** | **序号** | **指标项** | **技术参数** |
| √ | 1.     | 硬件 | ≥标准1U硬件，硬盘：≥2T\*1 ， 电源：单电源， 网口：≥6个千兆工作管理口(1管理口+1HA口+4审计口)，≥1个console口； |
| √ | 2.     | 性能 | 授权资产数≥55个；每秒事务处理数≥2000个（条） |
| 0 | 3.     | 功能扩展 | 可实现日志转发，转发协议支持syslog转发、TCP转发、Kafka转发、文本转发、Http转发、APT沙箱报告转发，提供配置界面截图 |
| √ | 4.     | 日志转发与存储支持数字签名与加密模式，签名方式支持SM3和SHA256，加密方式支持AES和SM4，加密模式支持CBC和ECB，PADDING补码方式支持P7和P5；日志接收支持解密，提供配置界面截图 |
| 0 | 5.     | 日志解析可支持解析处理线程数、计数器间隔配置，同时对日志源资产重识别、地理信息识别、内网地理信息识别、内网段地理信息识别、源目标地址识别、时间威胁识别、活跃规则匹配进行启用与禁用控制；统计数据存储方式支持NutEngine，提供配置界面截图 |
| √ | 6.     | 日志存储 | 日志存储支持Lucene入库，能够对线程数、批量数、缓存数、索引最大内存数、合并因子、允许加载的reader数量、合并机制允许的最大文档数、检索垃圾清理、索引压缩、分词器进行配置，提供配置界面截图 |
| √ | 7.     | 人力资源安全管理 | 人力资源安全管理支持新增账户、删除账户、锁定账户、权限增加账户、权限删除账户、权限变更账户数据呈现，提供配置界面截图 |
| 0 | 8.     | 信息系统获取、开发和维护管理 | 信息系统获取、开发和维护管理支持配置变更设备资产、配置变更设备类型统计、配置变更设备IP分布、资源耗尽设备资产、错配置设备资产、损坏设备资产数据呈现，提供配置界面截图 |
| 0 | 9.     | 信息安全事故 | 信息安全事故支持TOP10 攻击源、TOP10攻击目标、TOP10攻击事件、TOP10 高风险来源、TOP10高风险目标、TOP10高风险事件数据呈现，提供配置界面截图 |
| 0 | 10.    | 符合性及系统程序管理 | 符合性支持来自第三方系统的策略违法、来自第三方系统的非法访问、到第三方系统的非法访问数据呈现；系统程序管理支持到第三方系统的病毒活动、到第三方系统的木马活动、到第三方系统的漏洞利用、到第三方系统的SQL注入、到第三方系统的跨站攻击、到第三方系统的DOS攻击，提供配置界面截图 |
| 0 | 11.    | WEB日常审计 | Web日常审计包含web访问概况（请求发生事件数、服务器事件分布、访问源事件分布、请求方法事件分布、状态码事件分布、请求URL事件分布）、web访问客户端分析（常见请求浏览器分布、常见请求操作系统分布、IE系列浏览器请求TOP源IP、Windows系列操作系统请求TOP源IP、Chrome浏览器请求TOP源IP、MAC操作系统请求TOP源IP）、web访问地区分析、web异常访问分析（异常请求时段分析、异常请求TOP、403请求TOP、404请求TOP），提供配置界面截图 |
| 0 | 12.    | WEB告警威胁分析 | 可通过图表形式呈现WEB告警威胁等级，包含低等级告警威胁发生事件数（威胁等级：3）、事件分布（低等级告警威胁源IP）、事件分布（低等级告警威胁服务器IP）、中等级告警威胁发生事件数（危险级别：4-6）、事件分布（中等级告警威胁源IP）、事件分布（中等级告警威胁服务器IP）、高等级告警威胁发生事件数（危险级别：7-10）、事件分布（高等级告警威胁源IP）、事件分布（高等级告警威胁服务器IP）； |
| 可通过图表形式呈现WEB告警威胁地区分析，包含告警威胁事件分布（来源国家）、告警威胁事件分布（来源地区）、告警威胁事件分布（来源城市）提供配置界面截图 |
| 0 | 13.    | 事件查询 | 可通过多种因素进行时间查询，包含组织架构、威胁等级（低、中、高）、事件类型（基本事件、聚合事件、关联事件、三维关联事件、原始事件）、分类（对象、技术方式、动作、设备类型、效果、时间特征）、地理（来源目的国家、来源目的地区、来源目的城市、来源目的县市）、协议（应用协议、传输协议、客户端程序、上下文、方法、响应码、HTTP Cookies）、表达式、设备（处理动作、危险等级、报文、域名、分类ID），应用协议支持UUCP、wins、sunmission、whoami、isakmp进行事件梳理，提供配置界面截图 |
| 0 | 14. | 活动列表 | 支持活动列表数据呈现，包含唯一标识、属性、扩展属性、有效期、最大缓存条目、最大持久条目数据，新建活动列表可对属性进行配置，包含传输协议、攻击子类型、机密性关联状态、机密性级别、机器码、机密签名、可靠性关联状态、可靠性级别、来源地理详细地址，提供配置界面截图 |
| √ | 15. | 远程仓库 | 可实现配置远程仓库，通过FTP、SAMBA、NFS、FILE、OSS 5种方式进行远程仓库新增，完成远程数据备份，提供配置界面截图 |
| √ | 16 | 制造商要求 | 制造商具备中国信息安全测评中心颁发的《国家信息安全测评信息安全服务资质证书》（安全工程类三级），提供佐证资料 |
| √ | 17 | 其他要求 | 中标后5日内，要求中标人部署设备到招标人现场进行参数符合性测试，对所有功能、参数指标进行逐一测试匹配，超过指定时间范围参加测试视为自动放弃中标资格；中标人完全满足后进行合同签订等其他后续流程。一旦发现中标供应商存在虚假应标行为，将立即废标该供货商，同时根据项目总体金额10%进行罚款，虚假应标供应商列入政府采购黑名单，并追究其相关责任 |
| 注：1.“参数性质”栏中划“0”表示此参数为一般性技术参数，划“√”表示此参数为重要技术参数。2．重要技术或服务参数（要求） 不接受负偏离。　 |

# 运维审计与风险控制系统

|  |  |  |
| --- | --- | --- |
| **参数性质** | **指标项** | **技术参数** |
| √ | 性能 | 授权资产数≥100个；并发字符连接最大数≥100个；并发图形连接最大数≥20个；  |
| √ | 硬件 | 标准≥1U工控机，硬盘：≥2T，单电源（额定功率60W），网络接口：≥千兆电管理口\*2，≥千兆业务电口\*4，USB口：≥USB2.0\*2，串口：≥RJ45串口\*1 ； |
| 0 | 部门层级管理 | 支持按部门组织架构（至少10个层级的部门）管理用户数据、资产数据、授权数据、审计数据，且数据相互隔离；可按部门层级分别设定各部门不同权限的管理员，如部门内的运维管理员、审计管理员、系统管理员等。每个部门管理员仅可管理本部门及下级部门的相关配置。 |
| 0 | 兼容客户端类型 | 单点登录支持调用多种本地客户端工具：字符：xshell、secureCRT、putty、MobaXterm，图形：mstsc、realvnc，文件传输：secureFX、flashFXP、filezilla、winscp、Xftp、MobaXterm，数据库：ssms、sqlwb、DBeaver、mysqlcli、DbVisualizer、MySQLWorkbench、MySQLFront、PLSQL、SQLPlus、db2cmd、QuestCentral、pgAdmin3、psSQL、Ksql、lsql、Dlsql、DMmanager、GbaseDataStudio、Toad、ToadForDB2、navicat系列，无需应用发布服务器。 |
| 0 | MAC兼容性 | 支持在Mac操作系统下调用navicat工具运维MySQL、Oracle等数据库资产。 |
| √ | 其他要求 | 中标后5日内，要求中标人部署设备到招标人现场进行参数符合性测试，对所有功能、参数指标进行逐一测试匹配，超过指定时间范围参加测试视为自动放弃中标资格；中标人完全满足后进行合同签订等其他后续流程。一旦发现中标供应商存在虚假应标行为，将立即废标该供货商，同时根据项目总体金额10%进行罚款，虚假应标供应商列入政府采购黑名单，并追究其相关责任 |
| 注：1.“参数性质”栏中划“0”表示此参数为一般性技术参数，划“√”表示此参数为重要技术参数。2．重要技术或服务参数（要求） 不接受负偏离。 |

# 漏洞扫描系统

|  |  |  |  |
| --- | --- | --- | --- |
| **参数性质** | **模块** | **指标项** | **技术参数** |
| √ | 硬件架构 | 性能要求 | 可扫描总数量≥128个无限制范围IP地址；并发任务数并发主机数：≥80；任务并发数≥10个 |
| √ | 硬件要求 | 标准机架式≥1U设备，硬盘≥2T\*1；电源规格：单电源、额定功率250W； 网络接口：管理口≥1个\*RJ45串口、千兆电口≥6个，USB口≥2个 ； |
| 0 | 功能要求 | 总体要求 | 产品要求界面友好，并有详尽的技术支持文档，所有图形界面的文字要求为中文。 |
| 0 | 系统为B/S架构，并采用SSL加密通信方式，用户可以通过浏览器远程访问设备，方便用户操作，支持多用户同时登录操作。 |
| 0 | 支持分布式部署方式，上级管理设备能够方便查看下级设备的状态信息。 |
| 0 | 分布式部署可以随机分配扫描引擎，也可指定扫描引擎 。 |
| 0 | 支持用户自定义系统名称、版权信息和系统的Logo信息，而无需进行定制化。 |
| 0 | 漏洞知识库支持自定义编辑，可编辑漏洞描述、修复建议、漏洞等级等内容，在扫描结果和导出报告中应展示编辑后的内容。 |
| 0 | 系统漏扫功能要求 | 厂商漏洞特征库大于200000条；漏洞知识库与CVE、CNNVD、Bugtraq、CNCVE、CNVD等国际、国内漏洞库标准兼容。 |
| 0 | 具备弱口令扫描功能，支持弱口令扫描协议数量≥22种，包括FTP、SMB、RDP、SSH、TELNET、SMTP、IMAP、POP3、Oracle、MySQL、MSSQL、DB2、REDIS、MongoDB、Sybase、Rlogin、RTSP、SIP、Onvif、Weblogic、Tomcat、SNMP等协议进行弱口令扫描，允许用户自定义用户、密码字典 。 |
| 0 | 同IP不同端口同漏洞的结果应明确给予端口标识。 |
| 0 | 扫描结果在产品界面中支持查看目标应用返回的软件版本，可以方便与漏洞描述对比进行漏洞验证 。 |
| 0 | 支持端口探测方式≥7种，如：TCP ACK、TCP SYN、TCP Connect、TCP Null、TCP Xmas、TCP Window、TCP Fin等。 |
| 注：1.“参数性质”栏中划“0”表示此参数为一般性技术参数，划“√”表示此参数为重要技术参数。2．重要技术或服务参数（要求） 不接受负偏离。 |

# 终端安全及防病毒系统

|  |  |  |
| --- | --- | --- |
| **参数性质** | **指标项** | **技术参数** |
| √ | 授权点数 | 本次招标要求终端PC防护≥30点，服务器防护≥10点；管理中心服务器配置：处理器≥8核，内存≥16G ，硬盘≥500G  |
| √ | 可视化大屏 | 能够进行可视化态势大屏展示，包括终端管控大屏和安全概况大屏，安全概况展示内容包括风险概况、安全威胁防护、风险类型排名、资产概况、终端风险排名、安全动态；终端管控包括资产状况、终端分组统计、设备系统分类、版本统计、标签统计、最新安装主机，提供产品配置界面截图 |
| 0 | 系统安全性模块 | 支持对CPU、内存、磁盘使用、网络IO达到配置阈值时告警。支持对CPU、内存达到一定阈值时客户端自动进行熔断。 |
| 0 | 支持自动收集终端资产：监听端口、运行程序、账号、软件、启动项、Web框架、Web服务、数据库、Web应用、系统安装包、JAR包、计划任务、环境变量等信息，支持从资产的维度和信息的维度去查看数据，并支持数据的导出。 |
| 0 | 内置1800+检测规则，可覆盖ATT&CK矩阵的14中攻击战术及131种攻击技术，建立完整而全面的ATT&CK战技术知识库，并支持已中英文两种语言展示；可精准检测并阻断基于ATT&CK的入侵攻击。 |
| 0 | 检测规则包含初始访问、执行、权限维持、权限提升、防御规避、凭据访问、信息发现、横向移动、数据收集、数据渗漏、命令与控制（C2）、影响等类型，并且可根据规则类型设置可信白名单。 |
| 0 | 支持“attack movie”功能，能够将自定义时间范围内（5分钟、30分钟、1小时、一天等）终端上发生的基于ATT&CK攻击技术的攻击事件以视频的形式进行回放，可视化展示攻击过程及演变历史。  |
| 0 | 支持网络分域访问，在服务端设置不同网络访问域，资产在同一时间只能访问任意一个网络域，支持资产自主切换不同网络访问域。  |
| √ | 支持登录防护，包括以系统账号为粒度的异常登录防护、支持4个任意维度（任意IP，任意域名，任意计算机名，任意时间）的系统登录访问策略设置。 |
| 0 | 提供专门的针对未知勒索病毒的行为检测防御引擎，基于文件读写、进程、命令、网络、注册表修改等行为对于未知勒索病毒进行发现和阻断。 |
| 0 | 防病毒模块 | 提供专门的挖矿风险评估工具。 |
| 0 | 提供专门的挖矿风险评估工具。 |
| 0 | 提供专门的挖矿实时防御工具 |
| 0 | 支持病毒立即处理，对于无法普通隔离的病毒文件进行处理并加入隔离区，或动态移动到信任区。 |
| 注：1.“参数性质”栏中划“0”表示此参数为一般性技术参数，划“√”表示此参数为重要技术参数。2．重要技术或服务参数（要求） 不接受负偏离。 |

# APT攻击预警平台

|  |  |  |  |
| --- | --- | --- | --- |
| **参数性质** | **序号** | **指标项** | **技术参数** |
| √ | 1 | 性能要求 | ≥整机吞吐量500Mbps；≥1U标准机架式设备；电源：单电源 ；内存：≥8G；硬盘容量：2T\*1 ；接口数量：标配≥6个；接口类型：千兆RJ45网口\*2(管理口\*2)、千兆RJ45网口\*4； |
| 0 | 2 | 基础功能 | 可实现回连域名/IP进行展示，域名信息包含域名、首次发现时间、首次发现样本MD5、加入威胁情报、操作项，操作项中可查看风险列表，包含基本信息、客户端信息、服务端信息、ATT&CK、沙箱报告、建议与分析、处理内容，提供功能配置界面截图 |
| √ | 3 | 可实现白名单配置，包含WEB特征白名单（客户端IP、域名、WEB特性类别、WEB特征规则、HTTP方法）、IDS规则（规则ID、客户端IP、服务端IP、域名、资源路径、有效期）、文件白名单（MD5）、发件人域名白名单、发件人邮箱白名单（发件人邮箱）、域名白名单（域名匹配方式、域名、协议）、IP白名单（IP类型、IP、引擎类型），对特殊访问主体进行加白管理，提供配置界面截图。  |
| 　0 | 4 | 可实现资产管理，对资产名称、资产来源、资产类型、资产等级、资产健康度、告警次数、资产状态（活跃资产、离线资产、不活跃资产）、端口对应指纹名称、更新时间进行呈现，通过基本信息（资产IP、资产名称、MAC地址、资产重要性、资产类型、资产标签）、更多信息（资产编号、保密性、可用性、完整性）、操作系统信息（MAC OS、Windows2008、Windows Vista、Windows XP、统信）、应用信息进行资产整体情况定位，新增资产，提供功能配置界面截图 |
| 　0 | 5 | 流量代理agent模式可通过隧道模式（隧道类型gre、vxlan）、socket模式进行配置，提供功能配置界面截图 |
| √ | 6 | 可实现深度检测配置，同时对于深度检测特定规则开关、深度检测通用规则开关进行开关配置；特定规则检测模型包含后置判定集合插件、隧道工具插件、spc插件、pre插件、冰蝎检测2.0协商密钥、rsync前置修正、struct特性插件、shiro插件、数据安全插件、set插件、ssrf插件、msl插件、检测到冰蝎3.0通信流量、内存马插件、冰蝎4.0插件、cobaltStrike插件、向日葵插件、weevely插件、nacos插件，提供配置界面截图 |
| 0　 | 7 | 可进行DNS模型检测，包含DGA检测及隐蔽信道通信。DGA检测可通过度量周期、数据留存周期、长域名判定阈值、最小主域名长度、全数字模型长度阈值、交叉模型数字占比阈值、数字字母交叉长度阈值、随机模型随机步长、随机模型长域名随机阈值、数字随机模型随机步长、数字随机模型长域名随机阈值、随机性聚合域名告警阈值、高频访问同一域名阈值进行配置；隐蔽信道通信可通过度量周期、域名长度阈值、长域名判定阈值、最小数字占比阈值、数字字母交叉长度阈值、长域名随机阈值、短域名随机步长进行配置，提供配置界面截图 |
| 0 | 8.     | 暴力破解模型可通过状态、模型类型（通用规则处理类、加密规则处理类）、规则名称、协议、时间范围（60秒、120秒、180秒）、登录次数（成功此处、尝试次数、失败次数、累计次数）、聚合维度（IP维度、用户维度）、用户名检测机制（每次都计算、用户名或密码有一个变化、用户名和密码都变化、密码为空不检测、用户名大于等于二开始统计、用户名大于二且每次变化）、告警等级、攻击状态进行模型配置，通过可基于oscar、kingbase、SMB、RADMIN、MQTT、AFP、TITB、RSYNC、gbase、MEMCACHE协议进行暴力破解模型筛选，提供配置界面截图 |
| 0 | 9.     | 可实现自定义规则配置，规则内容可通过规则模式（普通模式、高级模式）、规则类型（特征匹配类、周期统计类、阻断规则）、Flowbits（set、isset、toggle、unset、isnoset）进行配置；会话信息可通过流量方向、流量状态（只触发已建立的TCP连接、不触发重建数据流、只触发重建数据流）配置，提供配置界面截图 |
| 0 | 10 | 风险事件管理 | 可通过运营模式、专业模式进行风险事件管理，运营模式可通过数据类型（聚合数据、原始数据）、风险级别、攻击状态（成功、尝试、失败、失陷）、风险类别、时间范围、客户端IP、服务端IP、客户网络、协议类型（TIDB）、攻击类型、安全事件（代码执行攻击事件、XXE注入攻击事件、键盘记录事件、暗网洋葱（Torweb）网络访问事件）、处理状态（未处理、处理中、处理完成、延迟处理、拒绝处理）、探测器、响应码、CVE、规则ID、域名、CNNVD、回放包ID、报文（模糊匹配URL/请求头/请求体/响应头/响应体/告警描述/告警描述/告警内容）在同一界面进行数据查询；专业模式通过外部渗透成功、外部扫描、内部横向扩散、恶意文件投递、数据窃取、脆弱性分析、发起回连行为模板进行风险查询分析；同时可基于目的IP城市、聚合标记、风险子类型、文件SHA1、HTTP源NATIP/DNS服务器IP、DGA算法类型、挖矿阶段进行针对性的匹配风险查询管理。提供配置界面截图文件 |
| 0 | 11 | 旁路阻断 | 可实现旁路阻断，可灵活配置旁路阻断策略，通过基于规则阻断及基于会话阻断方式进行旁路阻断异常流量，提供配置界面截图文件 |
| 0 | 12 | 场景化分析 | 可实现多种场景化分析能力，包含紧急事件分析、安全事件分析、攻击者视角分析、受害者视角分析、脆弱性分析、挖矿场景分析、勒索场景分析、主机威胁分析、失陷主机分析、情报时间分析、域名行为分析、流量回溯分析、钓鱼邮件分析、加密流量检测场景，每种场景化分析模块均有独立的呈现界面，提供功能配置界面截图 |
| 0 | 13.    | 拒绝服务攻击模型配置 | 可实现拒绝服务攻击模型配置，包含统计周期、单包长度阈值、统计周期内包数量阈值、攻击状态，提供配置界面截图 |
| 0 | 14.    | SSL流量检测 | 可实现SSL流量检测，对私钥别名、域名关联解析、服务器信息、私钥密码进行配置，同时支持对服务器私钥文件进行上，提供配置界面截图 |
| 0 | 15.    | 检测引擎管理 | 可实现多个检测引擎管理，包含WEB攻击、弱口令、邮件社工攻击、隧道通行。配置风险、入站情报、DGA域名请求进行检测引擎开关控制，提供配置界面截图 |
| 0 | 16 | 管理功能 | 可实现故障排查，通过网卡状态、镜像内容、服务管理、许可检查、配置核对、表分区检查、表检测、系统资源、日志分析、信息收集、运维管理完成问题排查，提供配置界面截图 |
| √ | 17 | 其他要求 | 中标后5日内，要求中标人部署设备到招标人现场进行参数符合性测试，对所有功能、参数指标进行逐一测试匹配，超过指定时间范围参加测试视为自动放弃中标资格；中标人完全满足后进行合同签订等其他后续流程。一旦发现中标供应商存在虚假应标行为，将立即废标该供货商，同时根据项目总体金额10%进行罚款，虚假应标供应商列入政府采购黑名单，并追究其相关责任 |
| 0 | 18 | 日志报表 | KAFKA服务器配置支持SASL认证和Kerberos认证；KAFKA数据传输支持明文或SSL加密 |
| 0 | 19 | 设备产生的数据重要程度至少分为3级，可自定义配置不同级别数据的清理比重 |
| 注：1.“参数性质”栏中划“0”表示此参数为一般性技术参数，划“√”表示此参数为重要技术参数。2．重要技术或服务参数（要求） 不接受负偏离。　 |

# 数据库审计与风险控制系统

|  |  |  |
| --- | --- | --- |
| **参数性质** | **指标项** | **技术参数** |
| √ | 硬件 | ≥2U机架式；硬盘≥2TB\*1；内置300W交流双电源； ≥2个千兆电口管理口（admin口1个、HA口1个）；≥4个千兆业务电口;；;  |
| √ | 性能 | 整机吞吐≥1500Mbps；双向审计数据库流量≥210Mbps；峰值SQL事务处理能力≥30000条/秒；数据库实例数≥8个； |
| 0 | 部署方式 | 旁路部署模式下无须在被审计数据库系统上安装任何代理，仅通过镜像流量即可实现审计； |
| 0 | 在目标数据库安装Agent解决云环境、虚拟化环境内部流量无法镜像场景下数据库的审计； |
| 0 | 支持分布式部署，管理中心可实现统一配置、一键批量升级所有节点、统一报表生成、统一查询； |
| √ | 协议支持 | 支持Oracle（包括21C及其他版本）、MySQL、SQL Server、Sybase ASE、DB2、Informix、Cache、 PostgreSQL（14及其他版本）、Teradata、MariaDB、Hana、LibrA、Sybase IQ、TiDB、Vertica、PolarDB、PolarDB-X等主流数据库的审计； |
| √ | 支持达梦（DM8及其他版本）、南大通用(GBase）、高斯（GaussDB）、人大金仓（KingbaseV8、V7及其他版本）、K-DB、神舟通用（Oscar）、OceanBase等国产数据库的审计；  |
| √ | 支持MongoDB、HBase、Hive、Redis、Elasticsearch、Cassandra、HDFS、Impala、Graphbase、Greenplum、Spark SQL、SSDB、ArangoDB、Neo4j、OrientDB 等数据库的审计；  |
| 0 | 支持主流业务协议HTTP、Telnet、FTP的审计； |
| 0 | 可以通过导入证书的方式实现SQL Server 2005及其他版本采用了加密协议通讯的审计； |
| 0 | 可以通过导入证书的方式实现MySQL 5.7及其他版本采用了加密协议通讯的审计；  |
| 0 | 支持对各种协议自动识别编码及在web界面手工配置特定编码如GB13000、UTF-8、UTF-16等; |
| 0 | 审计功能 | 支持数据库操作表、视图、索引、存储过程等[各种对象的所有SQL操作审计](#_支持各种对象的SQL审计_1)； |
| 0 | 支持在双向审计场景下根据以往审计命中情况设置结果集存储策略，支持设置保存行数与最大保存长度; |
| 0 | 支持跨语句、跨多包的绑定变量名及绑定变量值审计； |
| 0 | 支持本地直连数据库场景下的审计，通过本地Agent捕获本地数据库客户端程序中实际响应的SQL指令，实现对本地运维人员的数据库操作行为的审计，支持主流数据库如Oracle、PostgreSQL、MySQL、SQLServer等； |
| 0 | 支持HDFS、HIVE、PostgreSQL、Spark SQL(Thrift)等场景下的kerberos认证加密流量的解析与审计；  |
| 0 | 支持超长SQL语句（最长4M）审计； |
| √ | 其他要求 | 中标后5日内，要求中标人部署设备到招标人现场进行参数符合性测试，对所有功能、参数指标进行逐一测试匹配，超过指定时间范围参加测试视为自动放弃中标资格；中标人完全满足后进行合同签订等其他后续流程。一旦发现中标供应商存在虚假应标行为，将立即废标该供货商，同时根据项目总体金额10%进行罚款，虚假应标供应商列入政府采购黑名单，并追究其相关责任 |
| 0 | 可维护性 | 内置运维终端，可实现日志查看与下载、监控日志、设备状态检测、查看系统资源使用、查看共享内存使用、查看Kafka消费情况、执行SQL语句、执行常用命令、特权运维；（需提供功能截图） |
| 注：1.“参数性质”栏中划“0”表示此参数为一般性技术参数，划“√”表示此参数为重要技术参数。2．重要技术或服务参数（要求） 不接受负偏离。 |

# 网络安全等级保护测评服务

|  |  |  |  |
| --- | --- | --- | --- |
| **参数性质** | **序号** | **服务指标** | **服务要求** |
| √ | 1 | 网络安全等级保护测评 | 1. 测评机构需具备公安部第三研究所颁发的“网络安全等级测评与检测评估机构服务认证证书”； |
| 0 | 2 | 2. 项目负责人需要具有等级测评师（高级）证书 ，根据《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）文件精神及《信息安全等级保护管理办法》的要求，根据《信息系统安全等级保护基本要求》（GB/T 22239-2019）、《信息安全技术网络安全等级保护定级指南》（GB/T 22240-2020），对下述信息系统实施信息安全等级保护工作。 |
| 0 | 3 | 3. 服务目标 |
| 在国家信息安全保障相关政策和标准指导下，通过对信息系统实施信息安全等级保护工作，全面提升信息系统的安全性及安全防护水平，使各级系统经改建后达到等级保护相应级别的安全防护要求。 |
| 测评系统等级：三级系统名称：不动产登记系统。 |
| √ | 4 | **4、服务内容** |
| 本次服务项目范围涉及到组织方开展等级保护工作的全过程，包括信息系统定级备案,系统差距分析测评、安全建设整改、等级测评等过程。 |
| **差距分析测评：**按照信息系统等级保护基本要求及测评流程，进行信息系统安全现状分析，明确信息系统目前采取的安全保护措施与信息安全等级保护相关国家标准和行业标准之间的差距，排查信息系统安全隐患和薄弱环节，查找信息系统安全建设整改需要解决的问题，确定安全需求，编制《差距分析报告》，并提交内容、格式完全符合公安部门正式测评报告要求的、未签字盖章的预测评报告。 |
|  **安全建设整改：**协助组织方进行安全建设整改工作。确保安全建设整改工作安全、科学、有效的进行，并达到国家相关标准的技术要求，切实、高效的提升信息系统安全防护水平。 |
|  **等级测评：**依据信息系统安全等级保护测评相关标准，运用各种管理和技术手段对信息系统安全等级进行等级测评，出具等级测评报告。**驻场安全服务：**安排具有通信工程师资质以上人员2人，现场维护、日常巡检、重要事件处理等服务。 |
| √ | 5 | **5、交付物** |
| 该项目提交的文档至少包括如下文件： |
| 1）《网络安全等级保护整改建议书》 |
| 2）《网络安全等级保护测评报告》 |
| 注：1.“参数性质”栏中划“0”表示此参数为一般性技术参数，划“√”表示此参数为重要技术参数。 |
|  2．重要技术或服务参数（要求） 不接受负偏离。　 |

**机房改造**

|  |  |  |  |
| --- | --- | --- | --- |
| **参数性质** | **序号** | **产品名称** | **规格/配置/功能要求** |
| 0 | 1 | 机柜系统 | 1.600\*800\*2000mm机柜 |
| 0 | 2 | 2.含机柜加重底座1套 壁厚5.0mm |
| 0 | 3 | 3.底座尺寸：宽度600mm 深度800mm 高度可调 |
| 0 | 4 | 4.包含运输、就位、安装调试 |
| 0 | 5 | 5.含机柜配电单元：支持2:1双回路输入供电、1:1单回路输入供电，单侧10回路N+1输出模式. |
| 0 | 1 | 风冷直膨式精密空调机组 | 1.上送风；总冷量≥12.5kW、显冷量≥11.3kW、风量≥2800m3/h、能效比≥3（回风温度24℃，回风相对湿度50%）,投标时提供相应佐证； |
| 0 | 2 | 2.输入电压范围：380V(－15%~＋15%)； 频率：50Hz±2Hz； |
| 0 | 3 | 3.适应环境：温度：室内0℃~+35℃；室外 -15℃~+45℃；湿度：20%~80%RH； |
| 0 | 4 | 4.温度调节范围：+18℃~+28℃；温度调节精度：±1℃； |
| 0 | 5 | 5.湿度调节范围：40%~60%RH；湿度调节精度：±5%RH；温、湿度波动超限应能发出报警信号； |
| 0 | 6 | 6.机房专用空调应能应解决机房的高显热量负荷，在24℃、50%RH工况下：显热比 ≥0.90；,投标时提供相应佐证； |
| 0 | 7 | 7.机房专用空调系统应具有高可靠性，要求机组平均无故障时间MTBF≥10万小时；,投标时提供相应佐证； |
| 0 | 8 | 8.机组的室内风机系统应能够方便的从机组正面取出进行现场维修,提高系统的可维护性。室内主风机应采用后倾离心式风机送风系统，保证在增大机外余压的情况下送风风量不减少； |
| 0 | 9 | 9.机组加热性能：加热量≥6kW； |
| 0 | 10 | 10.机组加湿性能：采用电极式加湿，加湿电极方便拆卸清洗，加湿量≥2.8kg/h； |
| 0 | 11 | 11.冷凝风机采用无级调速，高效节能； |
| 0 | 12 | 12.蒸发器选用亲水铝箔和高效内螺纹盘管，提高换热效率； |
| 0 | 13 | 13.每台机组都应具有独立的控制系统、显示器、加热器、加湿器、独立的温湿度传感器。以保证每台机组的正常运行及高精度运行； |
| 0 | 14 | 14.系统应具有三遥性能（遥测、遥信、遥控）。 |
| 0 | 15 | 15.系统应具备通信接RS232/RS485接口，能接入动力环境监控系统中； |
| 0 | 16 | 16.机房专用空调机组的风冷型室外机组应提供冷凝风扇变速控制器，能根据冷凝器管道内部压力变化自动调节冷凝风扇的运转速度； |
| 0 | 17 | 17.具有不小于4.3寸的真彩色全中文大触摸屏，控制系统具有多级密码保护功能，具备联动与群控功能，并可共享温湿度设定值；,投标时提供相应佐证； |
| 0 | 18 | 18.本次投标厂家需获得空调行业《CRAA产品认证证书》。 |
| 0 | 19 | 19.本次投标精密空调需获得《中国节能产品认证证书》。 |
| 0 | 20 | 20.含室外机低温组件 |
| 0 | 21 | 21.含氮气、冷媒及制作、室外机电缆、室外机信号线缆、液管、气管、氟利昂、氮气、氧气、弯头、直接、护套、包带、焊条、乙炔、管路支架、延长组件、回油弯、反向弯等安装相关辅材 |
| 0 | 22 | 22.含空调输入电缆，YJV-5\*6 mm²国标线缆。 |
| 0 | 23 | 25.空调上下水管道：PVC上水管1套、PPR下水管1套 |
| 0 | 24 | 26.按空调尺寸定制，底座满足静态承重≧2000kg，盐雾测试72小时。 |
| 0 | 1 | 机房供配电等电位系统 | 1.包含机房内等电位环带1项 |
| 0 | 2 | 2.包含机房内等电位散流带1项 |
| 0 | 3 | 3.包含机房内等电位系统支架1项 |
| 0 | 4 | 4.包含机房接地子线30米 |
| 0 | 5 | 5.包含机房接地母线100米 |
| 0 | 6 | 6.包含室内等电位系统安装连接、接地子线制作连接、接地母线制作连接 |
| 0 | 7 | 7.含接地子线与室内设备壳体、金属构件等连接，规格：BVR6mm²。国标 |
| 0 | 8 | 8.含接地母线与楼体可靠接地连接，规格：BVR35mm²。国标 |
| 0 | 1 | UPS电源 | 1.UPS容量为20kVA，数量1台，单套满载延时要求＞2小时；采用在线UPS电源； |
| 0 | 2 | 2.UPS主机应采用先进的DSP数字控制技术，有效提升了产品性能和系统可靠性，并实现更高功率密度的集成和小型化。 |
| 0 | 3 | 3.UPS主机输入功率因数校正（PFC）采用数字化控制的功率因数校正技术，使输入功率因数高达0.99以上，以避免对电网环境的污染，达到节能，降低了系统的投资成本的目的。 |
| 0 | 4 | 4.UPS主机逆变器采用三电平技术，保证可靠性的同时提高系统效率，投标时提供拓扑原理图证明，加盖UPS厂家的公章； |
| 0 | 5 | 5.UPS主机具有独立旁路功能，确保主路系统出现异常或故障时，旁路系统仍能正常输出，确保负载不间断供电；投标时提供的产品使用说明书里面必须有相关的图文设置说明，加盖UPS厂家的公章； |
| 0 | 6 | 6.采用全数字化充电器，电池电压和电流可任意设置，充电电流最大不低于12A（三单机型充电电流最大10A），投标时提供的产品使用说明书里面必须有相关的图文说明，加盖UPS厂家的公章； |
| 0 | 7 | 7.UPS主机同时能兼容铅酸电池和铁锂电池，以满足用户不同的应用场景，投标时提供详细的设置说明，并加盖UPS厂家的公章； |
| 0 | 8 | 8.UPS主机应面板设定功能：可以通过面板设置UPS输出电压，输出频率，ECO模式、电池节数、并机模式，投标时提供的产品使用说明书里面必须有相关的图文设置说明，加盖UPS厂家的公章； |
| 0 | 9 | 9.UPS主机应具有LCD显示和LED状态显示， 可以显示：输入电压/频率、输出电压/频率、有功功率、视在功率、电池节数、电池电压、电池容量百分比、历史纪录等，投标时提供的产品使用说明书里面必须有相关的图文操作说明，加盖UPS厂家的公章； |
| 0 | 10 | 10.为避免误操作，UPS的开、关机采用双键组合的形式来实现开关机，投标时提供的产品使用说明书里面必须有相关的图文操作说明，加盖UPS厂家的公章； |
| 0 | 11 | 11.集交流输入过、欠压保护，输出过载、短路保护，逆变器过热保护、电池欠压预警保护和电池过充电保护等多功能保护于一体，极大地保证了系统运行的稳定性和可靠性。 |
| 0 | 12 | 12.可实现远程网络监控，支持RS232，RS485,SNMP等多种通信协议，配置WIFI/GRPS模块后可实现手机APP实时查看UPS参数 |
| 0 | 13 | 13.UPS主机应具有自老化功能，测试现场不需要外接负载就可以带载测试，投标时提供详细的设置说明，并支持现场验证，加盖UPS厂家公章； |
| 0 | 14 | 14.UPS主机系列应该获得泰尔、节能、抗震、CE等第三方权威机构出具有效期的认证和报告,加盖UPS厂家的公章。 |
| 0 | 15 | 15.含订制直流电缆1套 |
| 0 | 16 | 16.含UPS输入电缆1套 |
| 0 | 17 | 17.含UPS输出电缆1套 |
| 0 | 18 | 18.含原厂配套电池架1套 |
| 0 | 1 | 蓄电池 | 1.UPS采用12V免维护铅酸蓄电池，蓄电池设计寿命7-10年以上； |
| 0 | 2 | 2.蓄电池应通过抗震检测，其抗震等级应不低于9级，并提供同系列产品检测报告复印件。 |
| 0 | 3 | 3.蓄电池应具有泰尔检测认证及检测报告，并提供同系列产品检测报告复印件。 |
| 0 | 4 | 4.蓄电池连接件压降应低于7mV，需提供需提供检测报告复印件证明。 |
| 0 | 5 | 5.蓄电池在大电流放电后，极柱不应熔断，其外观不出现异常。 |
| 0 | 6 | 6.蓄电池在-30℃~+65℃时封口剂应无裂纹及溢留。 |
| 0 | 7 | 7.蓄电池密封反应效率不低于96.8%，需提供检测报告复印件证明。 |
| 0 | 8 | 8.蓄电池在30天过度放电结束后，容量恢复值应＞99%，需提供检测报告复印件。 |
| 0 | 9 | 9.蓄电池安全阀要求：开阀压力：1-20kPa；闭阀压力：1-20kPa，需提供检测报告复印件证明。 |
| 0 | 10 | 10.蓄电池在环境温度25±5℃的条件下，储存24h，通过安全阀向蓄电池充气在内外压差为50Kpa时并持续不少于5s时，能够不破裂、不开胶、压力释放后壳体无残余变形； |
| 0 | 11 | 11.电池内阻：蓄电池最大内阻＜4mΩ，同组蓄电池内阻偏差＜15%，需提供检测报告复印件证明 |
| 0 | 12 | 12.端电压均衡性：开路电压压差不应超出40mV，进入浮充状态24h后端电压差不应超出40mV，放电状态端电压差不应超出0.4V，需提供检测报告复印件证明。 |
| 0 | 13 | 13.再充电性能：恒压充电24h的再充电能力因素＞94%，需提供检测报告复印件证明。 |
| 0 | 14 | 14.蓄电池充满电后，在25℃±5℃环境中，以（2.45V±0.1V）/单体的恒定电压（不限流）连续充电168h。每隔24h记录一次充电电流值和蓄电池端子温度值。 计算浮充电流在任一24h之内的增长率△I和充电结束时蓄电池温度t：△I不应大于30％，t不应大于40℃，需提供检测报告复印件证明 |
| 0 | 15 | 15.同组蓄电池在25℃环境中，同组蓄电池10h率容量试验时，最大实际容量与最小实际容量差值≤5%，需提供检测报告复印件证明。 |
| 0 | 16 | 16.蓄电池与UPS主机充电器断开后，应能检测出连接线的开路状态，提供充电器与电池之间连接线开路的智能检测的第三方认证资料，**并加盖厂家公章。** |
| 0 | 17 | 17.UPS电源就位安装调试、UPS电池就位组装、UPS蓄电池就位安装调试、UPS输入输出电缆敷设连接 |
| 0 | 1 | 机房装修 | 1.包含机房地面防尘处理30m² |
| 0 | 2 | 2.包含机房棚面、梁面防尘处理30m² |
| 0 | 3 | 3.包含机房吊顶微孔铝天花30m² |
| 0 | 4 | 4.包含机房吊顶吊件及铝角30m² |
| 0 | 5 | 5.LED平板灯6套 |
| 0 | 6 | 6.灯电源线40米 |
| 0 | 7 | 7.存在感应器3套 |
| 0 | 8 | 8.防盗窗及窗口封堵2个 |
| 0 | 9 | 9.墙面大白（防火涂料）70m² |
| 0 | 10 | 10.封闭金属桥架30米 |
| 0 | 11 | 11.含陶瓷抗静电活动地板30m² |
| 0 | 12 | 12.膨胀栓，自攻钉，扎带，胶布、吊筋、射钉、切片等及其他装修辅材 |
| 0 | 13 | 13.含墙面涂刷、吊顶安装、吊筋、线管敷设、桥架敷设、地板拆除、地板恢复 |
| 0 | 1 | 动力环境监控系统 | 1.具备12个DI接口，4个DO接口，以及10个RS485接口 |
| 0 | 2 | 2.一体化环境监控主机要求能独立自成系统（含应用软件）， 具有数据采集、数据处理、协议转换、联动控制、报警管理、存储等功能，内嵌 WEB 服务，支持远程 IE 访问；友好的人机界面，满足用户个性化需求。内置 WEB 服务为系统管理人员提供远程设置、远程监控、远程维护及远程报警等专业管理功能；网络中断时动环采集单元仍可独立运行、存储数据及联动控制。数据采集终端将采集的数据和处理后的结果、报警信息等上传至集中监控层； |
| 0 | 3 | 3.具备本地化管理功能，无需借助上端动环监控软件平台，采集器自带组态图形化、列表等多种形式进行数据监测呈现，所有的显示模块（含导航栏）、数据监测组态页面及内容均可由用户自定义，支持机房能耗数据（PUE）展示；满足不同应用场景不同需求。 |
| 0 | 4 | 4.支持3D组态、支持本地TTS语音播报，支持联动及权限管理。注意：如采集器选用带HDMI接口+触控屏显示，则无法显示3D界面。 |
| 0 | 5 | 5.含机房监控软件1套 |
| 0 | 6 | 6.含工业电源1套 AC220V转DC12V/4A，带电池充电功能，提供2路DC输出。如机房可提供DC48V电源，则使用DC48V转DC12V/4A电源 |
| 0 | 7 | 7.电话短信模块短信模块1套,S80-A3-VSVW04-A01,LTE全网段 |
| 0 | 8 | 8.含温湿度传感器（RS485）2个 RS485通讯接口，显示：内置LCD显示测量值 ，测湿范围:0～100％RH ，精度:±3%RH ，测温范围:-20～70℃，精度:±0.5℃(25℃) |
| 0 | 9 | 9.含烟雾感应器2个 光电式感烟探测器,工作电压：12VDC；消耗电流：小于18mA；工作温度：-10℃～50℃；报警输出：常开/常闭可选，接点容量DC28V 100mA。 |
| 0 | 10 | 10.含不定位漏水检测传感器1台 现场采用不定位漏水检测时配置仅DI通讯 |
| 0 | 11 | 11.不定位漏水引出线1根 不定位漏水引出线（3米/根），配套不定位漏水感应线使用 |
| 0 | 12 | 12.5米不定位漏水感应线1根 5米不定位漏水感应线，直径5mm，材料为导电聚合物+金属导线 |
| 0 | 13 | 13.不定位漏水终止端1个 不定位漏水终止端，配套不定位漏水感应线使用 |
| 0 | 14 | 14.声光报警器1个 额定工作电压：12VDC，工作电压范围：9-15V，额定工作电流范围：60-85mA，声压范围：102±3Db，工作温度范围：-20℃~+60℃，外壳尺寸：122×72×42mm |
| 0 | 15 | 15.双门门禁控制器1个 ,可管理2个门的单向；支持刷卡、密码；5000人，3000条记录；DC12V供电（需要另配工业电源）；通过MC4.0一体化数据采集器进行人员添加和发卡授权、采集指纹和下载指纹等 |
| 0 | 16 | 16.接入控制器标准安装箱 尺寸：421mm(L)x256mm(W)x87mm(H) |
| 0 | 17 | 17.指纹密码ID读卡器 1个，尺寸：183mm(L)x80mm(W)x42mm(H)，供电：DC 12V，读卡类型：指纹/ID卡/MF卡，键盘：微动开关键盘，屏幕：彩屏 |
| 0 | 18 | 18.出门按钮 长86x宽86x厚20(mm)，适用于各种门禁系统。 |
| 0 | 19 | 19.电插锁 适用于木门、玻璃门、金属门、防火门等；工作电压：DC12V/0.45A（启动） |
| 0 | 20 | 20.硬盘录像机 1台，硬件规格：3U标准机架式，2个HDMI，2个VGA,HDMI+VGA组内同源，4盘位，可满配8T硬盘，2个千兆网口，2个USB2.0接口、1个USB3.0接口，1个eSATA接口，报警IO：16进8出，支持RAID0、1、5、10，支持全局热备盘，软件性能：输入带宽：320M，8路H.264、H.265混合接入，最大支持16×1080P解码，支持H.265、H.264解码，Smart 2.0/整机热备/ANR/智能检索/智能回放/车牌检索/人脸检索/热度图/客流量统计/分时段回放/超高倍速回放/双系统备份， |
| 0 | 21 | 21.24口交换机 1台 |
| 0 | 22 | 22.半球摄像机 4台 |
| 0 | 23 | 23.8T硬盘 4块 空气填充；接口：SATA 6Gb/s；转速7200rpm；256MB缓存；最大持续传输速率210MB/s；开机小时数8760；平均故障间隔时间1,000,000小时；启动电流（12V）:2.0；平均工作功率9W；电压公差：5V±5%，12V±10%；工作温度5~70℃。 |
| 0 | 24 | 24.防盗报警系统 1套 |
| 0 | 1 | 七氟丙烷气体灭火系统 | 1.GQQ40、2.5 |
| 0 | 2 | 2.含整套系统含长短途运费、安装、搬运、调试、测试、就位、线材及其他辅材 |
| 0 | 3 | 3.含七氟丙烷药剂40KG 规格：分子量170.03，临界度102.8，临界压力2.98MPa；包装规格：可回收钢瓶。质量指标：杯状燃烧器灭火浓度5.8；质量浓度0.4kg/m3，纯度≥99.6%，水份PPM≤10，酸度PPM≤0.01。 |
| 0 | 4 | 4.自动泄压装置1套 XZ0.25/1.1 |
| 0 | 5 | 5.点型光电感烟探测器2只，工作电压：DC24V，通过二总线；工作电流：监视≤300UA，报警≤1.3mA；线制：二总线，无极性，与控制器ZX+，ZX-二总线连接；探测器的状态灯在监控状态下闪亮，在报警状态下常亮；编码方式：采用手持编址器进行电子编码；使用环境：温度：-10℃～+55℃；湿度：5％～95％RH，无凝水； |
| 0 | 6 | 6.点型感温火灾探测器2只，工作电压：DC24V，通过二总线；工作电流：监视≤300uA报警≤1.3mA；线制：二总线，无极性，与控制器ZX+，ZX-二总线连接；报警温度：62℃；探测器的状态灯在监控状态下闪亮，在报警状态下常亮；编码方式：采用手持编址器进行电子编码；双状态灯指示，从360°的任何方位可视；使用环境：温度：-10℃～+50℃；湿度：5％～95％RH，无凝水。 |
| 0 | 7 | 7.探测器底座2只 J-EI6018 |
| 0 | 8 | 8.声光报警器1个 用于气体灭火防护区的现场声光报警，安装在防护区的出入口等现场区域，编码电路内置微处理器(CPU)，无极性二总线；接入WT8700气体灭火控制器的气体回路，占一个地址。 |
| 0 | 9 | 9.警铃1个 |
| 0 | 10 | 10.紧急启停按钮1个 内置微处理器(CPU)，总线型设备，无极性二总线；接入气体灭火控制器的气体回路，占一个地址；紧急启动和紧急停止指示；具有一个两态电子锁，用于手动操作控制分区状态；具有误操作玻璃防护装置。 |
| 0 | 11 | 11.放气指示灯1个 用于气体灭火喷洒的现场光指示，安装在防护区的出入口。编码电路内置微处理器(CPU)，无极性二总线；接入气体灭火控制器的气体回路，占一个地址。 |
| 0 | 12 | 12.手/自动转换开关1个 |
| 0 | 13 | 13.气体灭火控制器1区 内置微处理器(CPU)，总线型设备，无极性二总线；接入气体灭火控制器的气体回路，占一个地址；两个状态指示灯：分别指示手动和自动状态两个动作指示灯：紧急启动和紧急停止指示；具有一个两态电子锁，用于手动操作控制分区状态；具有误操作玻璃防护装置。 |
| 0 | 1 | 网络迁移、综合布线改造、机房割接 | 含网线测线，网线寻线，线缆整理，铝合金固线器，机房内线缆改造，临时标签及永久线缆标签标识，网络设备上架、含施工辅材。 |
| 注：1.“参数性质”栏中划“0”表示此参数为一般性技术参数，划“√”表示此参数为重要技术参数。 |
| 1. 重要技术或服务参数（要求） 不接受负偏离。
 |