浙江大学医学院附属妇产科医院

2号楼、3号楼有线网络设施更新项目

1. **采购内容**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 商品类目 | 品牌型号或服务 | 技术要求 | 数量 | 起拍总价 |
| 1 | 2、3号楼网络汇聚交换机 | H3C S7504E | 单台配置要求：24端口万兆单模光接口、4端口40/100G单模光接口、双电源、双风扇、ADCampus Director授权许可，5年原厂7\*24小时免费保修。 | 4台 | ￥400,000.00 |
| 2 | 2、3号网络接入交换机 | H3C S5130S-52S-EI | 交单台配置要求：48个10/100/1000Base-T自适应以太网端口，4个万兆单模光口、5年原厂7\*24小时免费保修。 | 35台 | ￥245,000.00 |
| 3 | 外网核心交换机 | 华为 S7706 | 万兆光口≥24，千兆光口≥24，千兆电口≥48个，冗余电源，冗余主控、华为Agile Controller-DCN软件许可，5年原厂7\*24小时免费保修。 | 1台 | ￥130,000.00 |
| 4 | 外网汇聚交换机 | 华为 S6720S-26Q-EI-24S | 24个万兆多模光口，2个40G单模光口，5年原厂7\*24小时免费保修。 | 4台 | ￥120,000.00 |
| 5 | 外网接入交换机 | 华为S5720S-28X-LI-AC | 24个千兆电口+2个万兆光口，5年原厂7\*24小时免费保修。 | 50台 | ￥200,000.00 |
| 6 | VPN网关 | 深信服VPN-1000 | 内存大小：2G，硬盘容量：64G minisata SSD，电源：冗余电源，接口：4千兆电口+4千兆光口SFP。最大理论加密流量（Mbps）：250，最大理论并发用户数：1000，IPSec加密最大流量（Mbps）：110，设备整机理论最大吞吐量：500Mbps，设备整机理论最大并发会话数：60w。  3年原厂7\*24小时免费保修。 | 1台 | ￥70,000.00 |
| 7 | 堡垒机 | 深信服OSM-1000 | 软硬一体化机架式设备，规格：2U，内存大小≥8G，硬盘容量≥64GB SSD+2TB SATA，电源：单电源，接口：≥6千兆电口、≥2万兆光口SFP+，提供600个授权许可，支持licence扩容，3年原厂7\*24小时免费保修。 | 1台 | ￥70,000.00 |
| 8 | 网闸 | 奇安信G1500 | 系统吞吐量：2500Mbps  硬件配置：2U机箱，单电源；具有液晶面板  内网：6个10/100/1000Base-T端口，2个万兆SFP接口，1个Console口，2个USB口；  外网：6个10/100/1000Base-T端口，2个万兆SFP接口，1个Console口，2个USB口；  产品包含3年硬件维保 | 1台 | ￥145,000.00 |
| 9 | 防火墙 | H3C F1000-AK135 | 防火墙吞吐量：三层 5Gbps/七层 800Mbps；支持IPSec隧道：2000个，吞吐量：800M；支持SSL vpn并发用户:1000个，吞吐量：350M；支持L2TP/GRE隧道数：1000个；虚拟防火墙数量4个.接口：16千兆电口+2千兆光口SFP，IPS特征库、URL特征库、防病毒功能特征库授权升级 3年 | 2台 | ￥80,000.00 |
| 10 | 防火墙授权升级 | H3C AK-135 | IPS特征库、URL特征库、防病毒功能特征库授权升级 3年 | 3套 | ￥30,000.00 |
| 11 | 准入及桌面管理系统 | 盈高MSEP | 2U机架结构；标准配置单电源；标准配置6个1000MBASE-T接口； 6000 每秒事务数（TPS)：≥12000（次/秒），最大吞吐量：≥5Gbps，最大并发连接数：8000，支持终端用户认证数量3000点。产品包含3年硬件维保 | 1台 | ￥110,000.00 |

**二、技术需求**

1. 2,3号楼汇聚交换机（4台）

|  |  |
| --- | --- |
| **功能及技术指标** | **参数要求** |
| 业务插槽数 | 业务插槽数≥4 |
| 通风散热 | 前后通风，且风道可调，具备更强的机房适应能力 |
| 交换容量 | ≥15Tbps |
| ★整机包转发能力 | ≥3000Mpps |
| 关键部件热插拔 | 电源、接口模块、风扇等关键部件可热插拔 |
| ★网络自动化 | 支持网络自动化管理，可以将园区设备按核心、汇聚、接入进行分组，每个设备分组中多个设备对应一份配置，通过DHCP实现设备配置一次性完全下发，实现设备自动化上线。对于已有网络，新增设备，设备分组更换后，可以自动纳管并且进行设备配置的下发 |
| 支持通过图形界面方式规划网络拓扑，并展示设备自动上线过程。 |
| 支持将园区设备按核心、汇聚、接入进行分组，对于同种类型的设备更换，可通过新设备自动化上线纳管后，执行一键替换功能快速完成设备的更换，尽快恢复业务。要求提供第三方测试报告。 |
| 支持路由器、交换机、无线、安全、语音、存储、监控、服务器、打印机、UPS等设备进行管理，实现设备资源的集中化管理。管理员可以通过该功能根据业务需求创建设备组视图，并将所需设备加入该视图中，以便进行管理。 |
| 业务自动化 | 支持业务自动化管理通过统一的用户编排界面实现物联网终端接入时自动识别终端，并将接入终端按照业务应用自动划入到相应的VRF隔离域。 |
| 提供针对业务的虚拟Overlay网络（比如VXLAN网络）的管理，可以自动识别并导入端点设备，自动识别网络中的虚拟专用网络和隧道，并实现对虚拟网络的加入监控、移除监控、查看分层拓扑、查看业务拓扑、查看全网拓扑、查看详细信息和查看流量信息等功能。要求提供第三方测试报告。 |
| 故障诊断 | 支持故障诊断提供基于任务的性能监控，可定制监控任务，长期监控网络性能，可以形成日报、周报、月报等报表。支持定制性能阈值，可以为监控的性能指标设置两级阈值，当性能指标超过阈值时根据不同的阈值发送不同级别的告警。 |
| 提供单设备故障诊断和设备间连通性诊断功能，管理员通过诊断的设备IP地址，即可以在整个控制器平台搜索出告警信息、性能信息、网络配置等一系列相关信息，协助管理员快速进行故障定位，并且管理员可以通过诊断结果进行相应操作。要求提供界面截图。 |
| 接口要求 | 以太网支持千兆电口，千兆光口，万兆光口、万兆电口、40G接口 |
| 整机万兆光端口密度≥96, |
| 整机万兆电口密度≥96 |
| 整机40G端口密度≥32 |
| 单槽位能够同时提供万兆电口+40G接口/万兆光口+40G接口，提高槽位利用率 |
| 可靠性 | 支持冗余电源模块、冗余风扇模块 |
| 支持BFD，BFD for VRRP/BGP/IS-IS/OSPF/RSVP/LDP/RIP/静态路由。  BFD收敛时间<50ms |
| ★虚拟化 | 多虚一技术(N:1)，N≥4 |
| 支持远程端口扩展，作为控制设备（Controlling Bridge,CB）实现对端口扩展模块（Port Extender,PE）的集中控制  支持和配套的端口扩展模块虚拟成单一的逻辑设备，在管理层面实现单一节点管理；虚拟化能力≥30：1，即通过单一管理节点可实现超过30台物理设备的统一管理。 |
| SDN/OPENFLOW | 支持OPENFLOW功能，支持普通模式和Openflow 模式切换支持多控制器（EQUAL模式、主备模式）  支持多表流水线  支持Group table  支持Meter |
| VxLAN | 支持VxLAN 网关， |
| 跨三层互联技术 | 支持主流的MAC in IP技术，如EVI/EVN/OTV等，实现跨三层网络的二层互联 |
| 有线无线一体化 | 支持原生的无线AC功能，无需独立的AC板卡或带AC功能的接口板，即支持无线AP管理功能。 |
| 安全特性 | 支持IPv4 uRPF |
| 支持DHCP Snooping |
| 支持ARP防攻击 |
| 支持IP Source Guard |
| 支持CoPP |
| 支持广播风暴抑制 |
| 支持EAD |
| 支持端口隔离 |
| 支持IP+MAC+VLAN+PORT的绑定 |
| 支持报文过滤功能，黑洞路由、黑洞MAC |
| 支持IEEE 802.1ae介质访问控制安全技术 |
| 成熟度 | 提供产品工信部入网证 |
| 配置要求 | 每台台配置万兆多模光口≥24个，40/100G单模光口≥4个  每台配置40G QSFP+ 5m电缆1根  每台配置双电源、满配风扇 |

1. 2,3号楼接入交换机（35台）

|  |  |
| --- | --- |
| 功能及技术指标 | 详细技术参数 |
| 交换容量 | ≥330Gbps（官网双重指标取小值，提供官网截图及链接，并加盖制造厂商章） |
| 转发性能 | ≥140Mpps（官网双重指标取小值，提供官网截图及链接，并加盖制造厂商章） |
| 接口类型 | 48个GE端口，4个万兆SFP+口 |
| ERPS | 实现ERPS功能，  能够快速阻断环路，  链路收敛时间≤50ms |
| CPU防护 | 实现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 |
| ★堆叠 | 最大堆叠台数>=9台 |
| 最大堆叠带宽>=40G（万兆上行主机） |
| 可要求堆叠带宽>=40G（万兆上行主机），并要求实配接口的基础上额外满配堆叠带宽所需的接口和互联模块 |
| 支持跨设备链路聚合，单一IP管理，分布式弹性路由 |
| 支持通过标准以太端口进行堆叠（万兆或千兆均支持） |
| 支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成MAC和IP地址的重配置，无需手动干预 |
| 支持远程堆叠 |
| VLAN特性 | 支持基于端口的VLAN，支持基于协议的VLAN； |
| 支持基于MAC的VLAN； |
| 最大VLAN数(不是VLAN ID)>=4094 |
| 镜像功能 | 支持本地端口镜像和远程端口镜像RSPAN； |
| 支持流镜像 |
| 同时支持N：M的端口镜像（M大于1） |
| 绿色节能 | 符合IEEE 802.3az（EEE）节能标准 |
| 端口定时down功能（Schedule job） |
| 支持端口休眠，关闭没有应用的端口，节省能源 |
| 成熟度 | 提供产品工信部入网证 |
| 配置要求 | 每台配置千兆电口≥48个,万兆多模光口≥4个 |

1. 外网核心交换机（1台）

|  |  |
| --- | --- |
| **功能及技术指标** | **参数要求** |
| ★业务插槽数 | 主控引擎≥2；整机业务板槽位数≥6 |
| 通风散热 | 为保证设备散热效果和可靠性，要求设备支持模块化风扇框，可热插拔，独立风扇框数≥2； |
| ★整机能力 | 交换容量≥15Tbps，包转发率≥2800Mpps，以官网最小值为准，提供官网截图及链接；支持每槽位带宽≥320Gbps，提供权威第三方测试报告; |
| 关键部件热插拔 | 电源、接口模块、风扇等关键部件可热插拔，支持颗粒化电源，整机电源槽位数≥3； |
| 接口要求 | 以太网支持千兆电口，千兆光口，万兆光口、万兆电口、40G接口 |
| 整机万兆光端口密度≥96, |
| 整机万兆电口密度≥96 |
| 整机40G端口密度≥32 |
| 单槽位能够同时提供万兆电口+40G接口/万兆光口+40G接口，提高槽位利用率 |
| 可靠性 | 支持冗余电源模块、冗余风扇模块 |
| 支持BFD，BFD for VRRP/BGP/IS-IS/OSPF/RSVP/LDP/RIP/静态路由。  BFD收敛时间<50ms |
| ▲虚拟化 | 多虚一技术(N:1) |
| 为了简化管理，支持纵向虚拟化技术，支持把交换机和AP虚拟为一台设备，支持两层子节点，且子节点接入交换机支持堆叠，提供权威第三方测试报告; |
| SDN/OPENFLOW | 支持真实业务流的实时检测技术，秒级快速故障定位，提供权威第三方测试报告； |
| VxLAN | 支持VxLAN 网关， |
| 跨三层互联技术 | 支持主流的MAC in IP技术，如EVI/EVN/OTV等，实现跨三层网络的二层互联 |
| 有线无线一体化 | 支持原生的无线AC功能，无需独立的AC板卡或带AC功能的接口板，即支持无线AP管理功能。 |
| 安全特性 | 支持IPv4 uRPF |
| 支持DHCP Snooping |
| 支持ARP防攻击 |
| 支持IP Source Guard |
| 支持CoPP |
| 支持广播风暴抑制 |
| 支持EAD |
| 支持端口隔离 |
| 支持IP+MAC+VLAN+PORT的绑定 |
| 支持报文过滤功能，黑洞路由、黑洞MAC |
| 支持IEEE 802.1ae介质访问控制安全技术 |
| 成熟度 | 提供产品工信部入网证 |
| 配置要求 | 实配：万兆多模光口≥24，千兆多模光口≥24，千兆电口≥48个，冗余电源，冗余主控 |

1. 外网汇聚交换机（4台）

|  |  |
| --- | --- |
| **功能及技术指标** | **参数要求** |
| 通风散热 |  |
| 整机能力 | 交换容量≥2.56TbpsTbps，包转发率≥480 Mpps |
| 关键部件热插拔 | 电源、接口模块、风扇等关键部件可热插拔，可插拔双电源，支持交流供电； |
| 接口要求 | 以太网支持千兆电口，千兆光口，万兆光口、万兆电口、40G接口，支持24个10GE SFP+，2个40GE QSFP+端口； |
| 可靠性 | 支持冗余电源模块、冗余风扇模块 |
| 支持BFD，BFD for VRRP/BGP/IS-IS/OSPF/RSVP/LDP/RIP/静态路由。  BFD收敛时间<50ms |
| ★虚拟化 | 多虚一技术(N:1) |
| 支持作为SVF Parent，将下联交换机纵向虚拟为一台设备管理，并支持2层Client架构 |
| SDN/OPENFLOW | 支持真实业务流的实时检测技术，秒级快速故障定位 |
| 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； |
| 跨三层互联技术 | 支持主流的MAC in IP技术，如EVI/EVN/OTV等，实现跨三层网络的二层互联 |
| 有线无线一体化 | 支持原生的无线AC功能，无需独立的AC板卡或带AC功能的接口板，即支持无线AP管理功能。 |
| 安全特性 | 支持IPv4 uRPF |
| 支持DHCP Snooping |
| 支持ARP防攻击 |
| 支持IP Source Guard |
| 支持CoPP |
| 支持广播风暴抑制 |
| 支持EAD |
| 支持端口隔离 |
| 支持IP+MAC+VLAN+PORT的绑定 |
| 支持报文过滤功能，黑洞路由、黑洞MAC |
| 支持IEEE 802.1ae介质访问控制安全技术 |
| 成熟度 | 提供产品工信部入网证 |
| 配置要求 | 实配：支持24个万兆多模光口，2个40GE 单模光端口，冗余电源 |

1. 外网接入交换机（50台）

|  |  |
| --- | --- |
| 功能及技术指标 | 详细技术参数 |
| 交换容量及性能 | 交换容量≥336Gbps，包转发率≥108Mpps，以官网最小值为准，提供官网截图及链接 |
| 接口类型 | 48个GE端口，4个万兆SFP+口 |
| 虚拟化 | 支持纵向虚拟化，作为纵向子节点零配置即插即用，提供官网截图或产品彩页 |
| ERPS | 实现ERPS功能，  能够快速阻断环路，  链路收敛时间≤50ms |
| CPU防护 | 实现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 |
| VLAN特性 | 支持基于端口的VLAN，支持基于协议的VLAN； |
| 支持基于MAC的VLAN； |
| 最大VLAN数(不是VLAN ID)>=4094 |
| 镜像功能 | 支持本地端口镜像和远程端口镜像RSPAN； |
| 支持流镜像 |
| 同时支持N：M的端口镜像（M大于1） |
| 绿色节能 | 符合IEEE 802.3az（EEE）节能标准 |
| 端口定时down功能（Schedule job） |
| 支持端口休眠，关闭没有应用的端口，节省能源 |
| 成熟度 | 提供产品工信部入网证 |
| 配置要求 | 每台配置千兆电口≥24个,万兆光口≥2个 |

1. VPN网关（1台）

|  |  |
| --- | --- |
| 功能指标 | 指标要求 |
| ★性能配置 | 专业VPN设备，非插卡或防火墙带VPN模块设备；规格：1U，内存大小：2G，硬盘容量： 64G SSD，电源：冗余电源，接口：4千兆电口。  最大理论加密流量（Mbps）：250，最大理论并发用户数：1000，IPSec加密最大流量（Mbps）：110，设备整机理论最大吞吐量：500Mbps，设备整机理论最大并发会话数：60w。 |
| 基本特性 | 专业VPN设备，采用标准SSL、TLS 协议，同时支持IPSec VPN、SSLVPN两种VPN，非插卡或防火墙带VPN模块设备。同时支持软件化交付 |
| 设备支持多种终端系统，如windows10、mac OS X El Capitan、ios9.x等及以下版本，使用包括IE11及以下版本或其他IE内核的浏览器，以及非IE内核浏览器，如Firefox，Safari，Google Chrome，Opera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 |
| 支持国产化终端使用，包括中标麒麟、银河麒麟、深度OS等操作系统来登录SSLVPN系统，并完整支持该操作系统下的各种IP层以上的B/S和C/S应用（提供截图证明，或至少2家国产系统厂商与VPN产品的兼容性认证报告） |
| 产品应支持的密码算法包括：AES、DES、3DES、DH、RSA、RC4、MD5、SHA1； |
| 易用性 | 产品应提供环境检测、自动修复工具，支持对Windows的环境兼容性一键检测能力，以及对检测结果进行一键修复的能力，避免由于用户操作系统环境存在问题影响SSL VPN的使用，减轻运维工作。（提供产品证明截图） |
| 支持断线重连自动技术，防止用户关闭浏览器或无线网正常切换时VPN隧道断开。支持客户端永久在线功能，对于无人值守的设备可以设定永久在线。 |
| ★终端安全 | 产品必须支持防中间人攻击，产品可在用户登录SSLVPN时智能判断存在中间人攻击行为，断开被攻击的连接，并可提示异常现象。（提供截图证明） |
| 支持客户端注销后自动清除所有缓存、Cookies、浏览器历主从认证账号绑定史记录、保存的表单信息，实现零痕迹访问。 |
| 支持VPN专线功能，可配置用户在接入SSL VPN的同时，断开与Internet其他连接 |
| 提供HTTPS驱动病毒查杀工具，支持对Windows环境下的HTTPS拦截监听的驱动病毒进行扫描查杀，避免因为HTTPS驱动病毒导致无法正常接入和使用SSL VPN（提供产品证明截图） |
| 支持主从认证账号绑定，必须实现SSL VPN账号与应用系统账号的唯一绑定，VPN资源中的系统只能以指定账号登陆，加强身份认证，防止登录SSL VPN后冒名登录应用系统 |
| ★身份认证 | 产品必须支持Local DB 、USB KEY、短信认证、硬件特征码、动态令牌、数字证书认证、LDAP、RADIUS、等认证方式；可针对用户/用户组设置认证方式的与、或组合； |
| 支持与阿里钉钉、企业微信APP等第三方OA认证对接，移动端通过OA访问企业自建H5应用时，会自动拉起VPN，实现其内置H5应用的安全接入（提供产品证明截图） |
| 设备内部必须支持自建CA中心，便于数字证书认证平台搭建；支持与第三方CA进行结合认证，支持CRL证书撤销列表；单台VPN设备可扩展同时支持5套以上CA根证书 |
| 高速性 | 支持HTP快速传输协议，大幅优化无线环境（CDMA、GPRS、WIFI、3G）、高丢包、高延等恶劣网络环境下传输速度及效率；支持根据网络境自动选择并切换至最优的传输协议（提供界面配置截图） |
| ★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。（提供界面配置截图） |
| 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 |
| 高管理要求 | 支持WebAPI接口，无需定制，可轻松被第三方系统集成，实现对VPN用户、资源、在线情况进行统一管理运维。 |
| 为满足我单位多数据量的保存，保障日志平台运行稳定且高可用性，必须支持外置数据中心。 |
| 稳定性、可扩展性 | 支持基于自组域简化部署VPN网络的方法，即当有多台设备处于VPN网络中时，通过连接任意节点的VPN设备，即相当于连入整个VPN网络； |
| 在负载均衡集群部署模式下，支持授权漂移，即当集群中一台设备宕机，该宕机设备中的并发授权自动迁移到其他正常的设备中，而无需额外购买授权。 |
| 支持设备自身的抗攻击防护，支持防Host头部攻击设置，用于防止Host头部攻击, 设备只允许通过符合设置规则的地址进行访问；支持防SWEET32攻击设置，用于防止SWEET32攻击。（提供产品证明截图） |
| ★产品及企业资质 | 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（提供证明材料）  为保障软件开发质量，要求厂商具有CMMI5级认证。（提供证书复印件） |

1. 堡垒机（1台）

| 功能指标 | 指标要求 |
| --- | --- |
| ★系统部署 | 软硬一体化机架式设备，规格：2U，内存大小≥8G，硬盘容量≥64GB SSD+2TB SATA，电源：单电源，接口：≥6千兆电口、≥2万兆光口SFP+，可管理资源数≥600个，支持licence扩容 |
| 物理旁路单臂部署，以逻辑网关方式工作；不改变现有网络结构 |
| 系统各模块支持以B/S方式管理，采用https加密方式访问 |
| 支持协议 | 支持字符协议：SSHv1、SSHv2、TELNET；图形协议：RDP、VNC；文件传输协议：FTP、SFTP、RDP磁盘映射、RDP剪切板 |
| 支持通过协议前置机进行协议扩展，至少支持扩展KVM、Vmware、数据库、http/https、CS应用等 |
| 动作流 | ★支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登陆和审计接入（提供截图） |
| 用户管理 | 支持对用户指定限制登录IP、登录时间段（可循环，如每周一到周五9：00-17：00时）等规则，以确保可信用户登陆系统 |
| 用户登陆认证方式支持静态口令认证、手机动态口令认证、Usbkey（数字证书）认证、AD域认证、Radius认证等认证方式；并支持各种认证方式和静态口令组合认证（提供截图） |
| 内置三员角色的同时支持角色灵活自定义，可根据用户实际的管理特性或特殊的安全管理组织架构，划分管理角色的管理范畴 |
| 资源管理 | 支持unix资源、windows资源、网络设备资源、数据库资源、C/S资源、B/S资源 |
| 支持RDP安全模式（RDP、NLA、TLS、ANY）设置，以适应RDP-Tcp属性中的所有功能配置，包括加密级别为客户端兼容、低、高、符合FIPS标准等加密级别 |
| 运维授权 | 支持一对一、一对多、多对多授权，如将单个资产授权多个用户，一个用户授予多个资产，用户组向资产组授权 |
| 支持在授权基础上自定义访问审批流程，可设置一级或多级审批人，每级审批可指定通过投票数，需逐级审批通过才可最终发起运维操作 |
| ★支持自定义紧急运维流程开启或关闭，紧急运维开启时，运维人员可通过紧急运维流程直接访问目标设备，系统记录为紧急运维工单，审批人员可在事后查看或审批（提供截图） |
| 口令策略 | 可以配置口令长度，是否包含字母及字母的长度，是否包含数字及数字的长度，是否包含符号及符号的长度，口令时效性；口令策略还可以配置禁止包含的关键字 |
| 改密计划 | ★支持定期变更目标设备真实口令，支持自定义口令变更周期和口令强度。口令变更方式至少支持手动指定固定口令、通过密码表生成口令、依照设备挂载的口令策略生成随机口令、依照密码策略生成同一口令等方式（提供截图） |
| 访问控制 | 支持命令黑命单，对字符型设备（如linux/unix/网络设备）的高危命令执行进行阻断，如rm、shutdown、reboot等 |
| 支持命令审批规则，用户执行高危命令时需要管理员审批后才允许执行；命令审批规则可以指定运维人员、访问设备、设备账号及命令审批人 |
| 支持RDP协议的控制台登录控制 |
| 运维方式 | 支持web页面直接发起运维，无需安装任何控件，并同时支持调用SecureCRT、Xshell、Putty、WinSCP、FileZilla、RDP等客户端工具实现单点登陆，不改变运维人员操作习惯 |
| 审计日志 | 支持监控正在运维的会话，信息包括运维用户、运维客户端地址、资源地址、协议、开始时间等，并可以实时阻断 |
| 图形资源访问时，支持键盘、剪切板、窗口标题、文件传输记录，并且对图形资源的审计回放时，可以从某个键盘、剪切板、窗口标题、文件传输记录的指定位置开始回放（提供截图） |
| 支持运维审计日志在线播放，并且支持离线下载后使用专用离线播放器播放（提供截图） |
| 备份与维护 | 具有日志防溢出功能，当磁盘空间达到阈值时，可设置停止记录审计日志或日志回滚 |
| 支持系统配置还原，可以还原至任一备份点 |
| 管理能力 | cpu工作情况，内存使用情况，磁盘使用情况，网卡使用情况，系统数据库工作情况， WEB服务工作情况，其他关键组件工作情况等 |
| 支持日志数据的外置存储，支持NFS、ISCSI和Windows文件共享协议 |
| 客户端兼容 | 全面支持Windows、linux、国产麒麟系统、Android、IOS、Mac OS等客户端操作系统下的H5页面一站式运维，实现跨终端适应性BYOD（Bring Your Own Device）（提供截图） |
| 产品资质 | 公安部《计算机信息系统安全专用产品销售许可证》； |
| 中国网络安全审查技术与认证中心《IT产品信息安全认证证书》 |
| ★厂商资质  要求 | 厂商具有国家信息安全漏洞库（CNNVD）技术支撑单位等级证书（二级） |
| 厂商具有国家计算机网络应急技术处理协调中心颁发的网络安全应急服务支撑单位证书（国家级） |

1. 网闸（1台）

|  |  |
| --- | --- |
| 技术指标 | 指标要求 |
| ★品牌要求 | 考虑到产品的成熟度和稳定性，要求为国内主流网闸品牌，产品入围公安部组织测试的接入平台安全产品名单（投标时要求提供证明文件） |
| 性能指标 | 系统吞吐量：2500Mbps  硬件配置：2U机箱，单电源；具有液晶面板  产品包含3年硬件维保 |
| 硬件规格 | 系统采用2+1架构，自主研发的基于安全芯片的专用隔离部件，无操作系统，外部无法编程控制，全硬件交换, 原厂商参与《军用网络安全隔离交换产品通用要求》标准编制,要求提供相关证明文件 |
| 2U机箱  内网：6个10/100/1000Base-T端口，2个万兆SFP接口，1个Console口，2个USB口；  外网：6个10/100/1000Base-T端口，2个万兆SFP接口，1个Console口，2个USB口； |
| 内、外网分别具有独立的HA口，实现双机热备及负载均衡(提供证明截图) |
| 内、外网分别具有液晶屏，能够显示产品品牌、型号、CPU/内存占用率、网络接口状态等信息。(提供证明截图) |
| 支持双系统冗余架构，可通过WEB、console口进行主备系统切换，当主系统发生故障可切换至备系统进行工作； |
| 管理维护 | 内、外网分别具有独立的管理接口，而不是通过网络接口管理，也不是通过内网一个管理接口完成全部管理 |
| 支持用户名/密码+U-KEY、用户名/密码+数字证书等多种双因子认证方式；（提供证明截图以及U-key实物相片） |
| 支持带内管理，可通过业务口进行网闸管理工作；用户可自行选择是否启用带内管理功能（提供证明截图） |
| 支持集中监管平台，可对多台网闸进行统一监控，记录每台设备的系统资源运行情况；（提供证明截图） |
| 支持多种告警方式，如弹框告警、邮件告警、SNMPTrap、syslog告警等； |
| 支持设备健康状态追踪，通过可视化界面实时显示设备健康状态分布图；（提供证明截图） |
| 提供调制工具，其中包括：trace；ping；telnet；arp等 |
|  | 支持NFS、SMB、FTP等文件传输协议实现文件同步。支持不同文件传输协议之间的文件同步，如：NFS与SMB之间的文件同步 |
| 文件交换模块支持病毒检测功能，支持通过文件大小控制病毒查杀；(提供证明截图) |
| 支持多种同步模式： 完全一致、完全复制、首次复制+新增、源端移动、源端删除等多种模式。(提供证明截图) |
| 文件交换支持传送优先级，可根据文件大小、后缀名等多种方式进行优先级排序传输 |
| 客户端支持服务模式，当服务器异常重启，客户端可自行启动，无需人员干预；(提供证明截图) |
| 支持实时监控文件同步进度、同步状态、操作标识等同步信息，便于实时掌握文件传输过程；(提供证明截图) |
| 客户端提供实时异常诊断信息，便于管理维护；（提供能证明截图） |
| 支持文件名及后缀名过滤，同时支持文件类型识别过滤，即不基于后缀名的过滤。 |
| 支持客户端、无客户端多种部署方式实现数据库同步；(提供证明截图) |
| 无客户端方式同步由网闸主动发起并完成，不需要第三方软件支持（无需在数据库安全任何第三方软件），支持windows、linux、unix等多种数据库操作系统类型。 |
| 邮件模块支持病毒检测功能；支持通过文件大小控制病毒查杀；支持超长邮件限定是否接受； |
| 支持ORCLE、SQL Server数据库命令控制，可对数据库SQL语句进行过滤；（提供证明截图） |
| 数据库库名控制、数据库表控制，可以根据用户与数据库表对应关系，进行相应数据库操作过滤；（提供证明截图） |
| 支持任务运行时间控制(提供证明截图) |
| 支持透明模式、代理模式及混合模式(提供证明截图) |
| FTP访问模块支持病毒检测功能，支持通过文件大小控制病毒查杀； |
| 不仅支持传输文件扩展名过滤，而且可以根据文件内容识别进行文件类型过滤。 |
| 安全浏览模块支持病毒检测功能，支持通过内容长度控制病毒查杀；支持图片文件、媒体文件等文件类型病毒检查；可设定病毒扫描内容最大长度。(提供证明截图) |
| 支持TCP定制服务；支持源地址绑定、网络接口地址绑定功能；（提供功能截图） |
| 支持组播的定制服务 |
| 支持任务运行标记 |
| 支持SSL隧道访问模式，针对FTP访问模块、数据库访问模块、邮件访问、定制模块等模块，通过网闸实现访问客户端认证、授权及访问链路加密，保证客户端访问合法性及访问链路的安全性。认证方式支持用户名口令认证及证书认证；（提供功能截图） |
| 支持Socks4、Socks5版本代理功能； |
| 能够实现基于源地址、目的地址、源端口、目的端口的访问控制； |
| 安全审计 | 具有独立审计用户，支持标准Syslog、FTP日志审计方式，支持Syslog端口自定义 |
| 支持多种日志导出格式，html、txt、cvs； |
| 支持数据轨迹查询，可以查询、追溯摆渡数据的源与目的； |
| 支持根据时间、文件名、文件类型、数据库源表、目的表、IP、端口、等条件查询数据从源到目的的整体轨迹信息。（非基本日志信息） |
| 支持通过SecFOX安全管理系统实现的集中安全管理 |
| 支持数据轨迹查询，可以查询、追溯摆渡数据的源与目的； |
| 提供告警，支持声音告警、邮件告警、trap等告警方式； |
| 支持多种告警类型：病毒告警、攻击告警、硬件异常、系统异常、资源异常、配置变化、日志告警 |
| 攻击防御 | 支持双机热备及超过双机的多机热备功能 |
| 支持双机配置同步功能，可将主闸配置主动同步到备闸，方便配置管理（提供功能截图） |
| 支持多机（最多32台）负载均衡，支持负载分担、负载信息查看、自动切换、自动恢复等 |
| 支持端口和链路的冗余：无需其他设备支持和配合，实现了在一条链路故障时，业务能够切换到另一条链路上 |
| 支持双引擎病毒模块，可根据用户需求选择需要的病毒引擎； |
| ★产品资质（复印件） | 产品具备国家信息安全测评信息技术产品安全测评证书EAL3+； |
| 产品具备密码检测证书 |
| ★厂商资质（复印件） | 涉密信息系统集成甲级资质； |
| 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） |
| CCRC信息安全服务资质-安全运维服务资质一级证书； |
| 国测信息安全服务资质-安全开发类一级证书； |
| 厂商具备CCRC信息安全服务资质-安全运维服务资质证书 |
| 厂商为“信息安全等级保护关键技术国家工程实验室”理事单位； |
| 其他 | 中标后三个工作日内提供软件测试对以上所有产品功能逐一进行实测,满足所有招标要求方可签订合同，否则将追究相关责任。 |

1. 防火墙（2台）

|  |  |
| --- | --- |
| **功能指标** | **指标要求** |
| 性能要求 | 防火墙吞吐量:三层 5Gbps/七层 800Mbps;支持IPSec隧道:2000个,吞吐量:800M;支持SSL vpn并发用户:1000个,吞吐量:350M;支持L2TP/GRE隧道数:100  接口：≥16千兆电口+2万兆光口SFP+。  3年AV 防病毒，3年应用特征库升级，3年IPS特征库升级，3年URL库升级 |
| 部署方式 | 支持路由、透明、虚拟网线、旁路镜像、混合等多种部署方式，适应复杂使用环境的接入要求。 |
| 路由功能 | 具备静态路由和多播路由，支持RIP、OSPF、BGP等路由协议。 |
| 支持基于IP地址、端口、地域、协议、应用等维度配置策略路由策略，支持多种负载均衡算法，包括加权、带宽比例、轮询、线路排序等。 |
| 地址转换 | 支持IPv4／IPv6下NAT地址转换，包括支持源地址转换SNAT，目的地址转换DNAT和双向地址转换双向NAT， 支持一对一、一对多、多对一等多种转换方式。 |
| 支持NAT ALG功能，包括支持FTP、RTSP、SQLNET、PPTP、TFTP、H.323、SIP应用协议的NAT穿越。 |
| 地域访问控制 | 支持基于对象、区域和地域维度设置安全访问控制策略，允许或拒绝特定国家或者地区的对象访问内部网络，保障业务重大时期安全可靠性。 |
| DDoS防御 | 支持SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood等泛洪类攻击防护，支持IP地址扫描和端口扫描攻击防护。 |
| 支持TearDrop 攻击、IP数据块分片传输、Land攻击、Smurf攻击、WinNuke攻击、超大ICMP数据攻击等异常报文攻击防护，支持IP协议异常报文和TCP协议异常报文攻击防护。 |
| SSL解密 | 支持对HTTPS协议加密会话进行解密分析，支持基于区域、对象、业务类型、服务器IP/端口设置解密策略。 |
| 防病毒 | 支持对HTTP、HTTPS、FTP、SMB、SMTP、POP3、IMAP协议进行病毒检测和查杀，支持最大10层的压缩文件查杀。 |
| 支持病毒排除设置，支持基于文件MD5值和文件下载URL设置病毒白名单； |
| 支持防火墙内置蜜罐功能，定位内网感染僵尸网络病毒的真实主机IP地址； |
| 具备勒索软件通信防护功能，提供具备CNAS（中国合格评定国家认可委员会）资质的第三方权威机构关于“勒索软件通信防护”产品功能检测报告。 |
| 入侵防御 | 产品内置IPS检测引擎，支持口令暴力破解、僵尸网络、恶意软件、服务器与终端漏洞攻击等检测和防护，支持超过5000种特征规则 |
| 具备僵尸网络检测功能，可基于僵尸网络检测引擎发现主机的异常外联行为，并提供威胁等级和非法外联次数作为举证。 |
| Web应用防御 | 产品内置Web应用攻击检测引擎，支持文件包含攻击、抵御注入式攻击（包含SQL注入、系统命令注入）、信息泄露攻击、跨站脚本（XSS）、网站扫描、WEBSHELL后门攻击、跨站请求伪造、目录遍历攻击、WEB整站系统漏洞等应用层攻击行为，支持超过2000种Web服务器漏洞特征规则。 |
| 支持内容敏感数据防泄露功能，对传输的文件和内容进行检测,支持对银行卡号、手机号码等类型数据防护。 |
| 支持windows/linux下网站防篡改功能，可防止攻击者非授权修改网站目录文件。 |
| 策略生命周期管理 | 支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便策略的管理和运维。 |
| 策略优化 | 支持对当前应用控制策略异常分析，包括策略风险访问、策略冗余、策略冲突、策略重合、端口放通过大等问题，并提供相关解决方案便于用户快速调优。 |
| 资产识别 | 支持Web服务器自动侦测功能，根据Web服务器在线状态、端口使用状态、Web服务器之间的互访关系生成业务资产列表，同时展示内网资产访问的风险等级。 |
| 攻击事件风险分析 | 支持针对业务攻击事件汇总，展示攻击事件类型TOP5及当前业务命中的全网实时热点事件，支持通过地图区域颜色深浅展示攻击者的分布与数量。 |

1. 防火墙安全授权（3套）

|  |  |
| --- | --- |
| 指标项 | 技术规格要求 |
| ★基础要求 | 华三AK135防火墙 IPS入侵防御特征库、防病毒功能特征库、应用识别特征库、URL特征库授权升级，3年升级服务 |

1. 终端安全管理系统（1台）

|  |  |
| --- | --- |
| 指标项 | 技术规格要求 |
| ★基础要求 | 具有独立的自主知识产权的一体式机架结构硬件产品，不接受PC SERVER系统架构。  必须为专用操作系统，非通用Linux系统或Windows系统。  支持多级级联架构，满足分级管理要求。 |
| 硬件指标 | 2U机架结构；标准配置单电源；标准配置6个1000MBASE-T接口； 6000 每秒事务数（TPS)：≥12000（次/秒），最大吞吐量：≥5Gbps，最大并发连接数：8000，支持终端用户认证数量3000点。 |
| 高可用性 | 必须具备HA模式，HA需支持主备机心跳IP检测及虚地址管理模式。  支持多级级联架构，满足分级管理要求。  支持负载均衡集群方式部署，支持超过10万点以上的终端点数。 |
| ★强制技术 | 支持基于策略路由技术的准入控制模式，入网设备在访问网内关键资源时，将被强制隔离、引导至认证管理页面。  可支持端口镜像准入技术，通过对交换机镜像数据的实时分析，能够及时发现并阻断非授权终端的接入。  单台准入设备可支持至少2个核心交换机进行策略路由准入控制。  （投标时提供功能截图） |
| 定向引导 | 支持终端入网IE重定向引导，当用户访问网页时能够自动转向到指定的页面或地址，并支持http代理及多重重定向引导。  可根据用户的实际环境自定义非80端口的Web服务端口号及用户重定向引导。  能通过浏览器完成身份认证、客户端安装、设备注册、安全检查、检查结果展现等全流程引导管理。 |
| 资产采集 | 自动采集各计算机的IP地址、计算机名、MAC地址、网卡型号和生产厂商、计算机所在域、操作系统、主要硬件、软件信息。  能够提供计算机信息综合查询报表。 |
| 硬件资产 | 能够对终端硬件初始记录、最新记录和变动记录形成报表，支持对硬件变动进行报警，并且能够查询变动的历史。 |
| 软件资产 | 1、支持对软件资产进行实时统计，能够灵活指定必须使用的软件资产和禁止安装的软件资产，支持对软件变动进行报警，并且能够查询变动的历史。  2、支持对终端违规安装的软件进行卸载; |
| ★IP地址资产 | 可通过矩阵图的方式自动进行网内IP地址的展示。  可通过颜色不同标识出该IP的状态：未分配、开机、关机。  IP使用历史记录：设备名称、设备IP、上线时间、离线时间、运行时长。  （投标时提供功能截图） |
| 软件使用管理 | 支持以软件为单位，审计使用的时间和次数。  支持以软件为单位，限制软件的打开和使用。 |
| Windows安全登录 | 可以与用户已有认证系统（UKey、LDAP等）相结合实现Windows系统安全登录与身份认证（替代Windows本地用户/密码认证模式）。 |
| 杀毒软件 | 支持至少18种杀毒软件的检查。  能够区分版本不合规、病毒库不合规，提供自动下载程序修复和网址引导修复。  （投标时提供功能截图） |
| 系统配置安全 | 能够建立终端设备的安全性评估任务，支持对帐户密码安全性、屏保设置、共享安全、系统服务、进程及服务等项目进行检查、评定，对存在安全风险的终端支持实时自动修复。  支持终端安全状况图形化展示，能够显示每台终端的详细风险信息并提供评估得分的统计报表。 |
| 重要进程管理 | 能够统计网内运行的所有进程，支持设置黑白名单指定禁止或允许的进程，支持进程MD5值识别方式，防止更改或伪造进程。 |
| 进程运行分析 | 能够对指定进程的运行情况进行跟踪并以表格方式展现分析结果 |
| 异常进程监控 | 能够对指定进程运行情况进行保护，防止进程被非法结束。 |
| 私设网站检查 | 可设置终端主动进行网段内私设WEB站点的扫描。  可扫描浏览器是否有上网的历史记录。 |
| 私设代理控制 | 1.管理员可设置策略禁止终端设置代理。  2.管理员可为被管控终端在管理系统后台设置指定代理、端口号，终端用户无感知。 |
| 流量控制检查 | 可对上传、下载流量、总流量、发包频率、TCP连接数、UDP监听端口数进行控制。 |
| 软件黑白名单 | 支持对终端应用进行控制管理，支持建立软件黑名单和白名单，强制终端只能在管理策略允许的范围内安装应用。 |
| 软件分发 | 能够支持可执行程序、MSI安装包或者文档数据文件自动下发与安装。  能够支持指定组范围、指定时间进行安装并提供程序打包工具。  能够自动统计分发成功率及软件安装成功率，支持进程、注册表、安装路径等多种参数判断方式。  支持根据操作系统不同分发不同升级包，提高软件分发功能对操作系统系统的适应性； |
| 远程协助方式 | 管理员计算机与被管理计算机采用专用tcp端口进行直接连接，远程协助时不占用服务器端口资源。  远程协助支持双向穿透NAT或VPN的远程屏幕控制。  （投标时提供功能截图） |
| ★远程协助功能 | 支持实时查看远端计算机的操作进程、服务、系统日志等信息。  支持对远端计算机进行关机、重启、断网等管理。  对远端计算机远程查看和远程控制，可根据管理需要灵活配置是否强制管理还是授权管理。  支持对远端计算机进行文件级远程管理，可在用户无感知的情况下远程创建、重命名、拷贝、删除文件。  远程查看、远程控制可以根据管理需要和网络状况，选择、配置适合管理员的窗口分辨率、显示比例、色彩、鼠标按键、光标等。  权限管理员支持限制操作管理员远程控制的权限，是否允许强制查看、控制和文件传输，允许指定必须申请管理的终端列表。  支持终端向管理员主动发起远程请求  （投标时提供功能截图） |
| 远程开机 | 支持远程开启计算机，支持定时、批量开启计算机。 |
| 网络适应性 | 支持各种网络环境的终端管理，包括同一网段、单方处于NAT子网中、双方各自处于不同的NAT子网中、处于VPN环境中。  支持自动穿透管理计算机的防火墙设置。 |
| 多方管理 | 支持一台计算机接受多台计算机同时维护管理。  支持一台计算机同时管理控制多台计算机。 |
| 外联行为控制 | 能够检测出通过代理等方式产生的外联行为并进行报警阻断，在内网设备带出外网的情况下同样能够检测出上述外联行为并进行违规行为上报或者阻断。  支持仅断开与网络连通的网卡  支持配置终端可访问的外网IP和域名  支持禁止DNS域名解析服务，并支持配置白名单。 |
| 违规访问控制 | 能够控制终端只能访问外网或只能访问内网，能够以策略方式按照区域、部门、组、ip段或单台设备设定内网访问范围。  能够对违规网络访问行为进行报警和阻断。  支持内网设备带出后在访问外网时自动进行阻断和违规行为上报。 |
| 网络代理使用管控 | 能够从网络协议层面检测网络代理的行为，支持基于网卡数据包的代理数据阻断功能，并支持报警、断网、锁屏等强制控制措施。  支持检测Windows的代理配置选项，检测不符合要求的代理配置情况，并支持自动清除、报警、断网、锁屏等强制控制措施。  代理行为的管制支持例外合法的代理地址。 |
| ★网络配置绑定 | 能够实时监测终端IP地址、MAC地址、DNS配置等相关网络信息，支持对应信息的实时绑定，当IP或MAC发生改变时能够强制恢复至修改前。  管理员可以授权部分用户修改IP地址； |
| ★外设管理 | 能够禁用终端设备的USB接口、光驱、软驱、打印机、调制解调器、串并口、1394、 红外、蓝牙及PCMCIA卡等外设接口。  能够单独禁用USB移动存储设备而不影响其他USB设备。  支持对手机的管控；通过外设使用控制策略，可以保证手机插入电脑后，不能把文件拷贝到手机 |
| 反ARP欺骗 | 支持网关、关键服务器等IP、MAC的静态绑定，从而免受ARP的欺骗攻击。能够实时检测ARP欺骗的病毒源，能够对有ARP攻击的终端设备进行隔离。 |
| 主机防火墙 | 能够提供基于协议、基于IP和端口、Ping共3种拦截方式。  能够设定允许或禁止主机访问的IP段、端口和协议。  能够设定允许或禁止某个IP段访问本地主机的端口和协议。 |
| 上网访问控制 | 能够基于URL关键字设定允许或禁止终端设备访问的网站，能够对违规访问设备进行报警或阻断。 |
| 可信主机访问 | 能够设置为例外可信设备，与其他安装客户端的设备通信。 |
| 移动介质授信管理 | 能够禁止未注册USB移动存储设备的随意接入。  必须支持新USB移动存储设备用户在线申请、注册，管理员在线审核，无需上交信息中心注册。  能够对指定的USB移动存储设备进行注册，设定所属部门和使用人，并进行加密、只读和可写的控制。  能够控制指定USB移动存储设备在外网无法使用。  能够针对区域、部门、组、IP段或单台设备控制指定USB移动存储设备的读写权限，能够对终端和USB移动存储设备进行一对一绑定。 |
| 移动介质安全管理 | 能够对USB移动存储设备中指定名称的文件进行允许或禁止访问的控制。  能够禁止访问USB移动存储设备中的可执行文件。  能够禁止USB移动存储设备的自动运行。 |
| 移动介质审计 | 能够对USB移动存储介质的插入和拔出行为进行审计。  能够指定审计的设备范围，能够指定审计的USB设备，能够指定审计的文件名称和操作类型，能够对通过USB设备进行的文件拷入、拷出行为进行审计，支持按照使用设备、文件路径、操作名称、操作时间进行报表的查询。 |
| 组策略管理 | 支持基于组策略的操作系统组件功能，如：禁用控制面板、禁止添加打印机、禁用任务管理器、阻止更改桌面背景、禁用注册表编辑器、阻止访问命令提示符等。  支持基于自定义工具定制组策略模板配置，可自动录制计算机的组策略配置信息，并可批量下发和批量执行。组策略模板执行的内容，在策略取消或停止后能自动回滚到执行前的配置状态。  支持定制windows组策略模板，支持批量下发，支持撤销。 |
| ★文档审计 | 能够记录终端用户日常的文档的操作行为，可以详细审计用户新建、拷贝、修改、移动、删除等操作行为。  支持软件过滤，只审计常用软件产生的文件变动行为。 |
| 邮件审计 | 能够对用户日常邮件的收发做有效审计，审计内容包括邮件地址、邮件标题、邮件内容以及附件等，方便事后追查。 |
| 网站审计 | 实时记录终端计算机访问过那些网站，并以柱状图、表单等图表方式形象的展现统计结果、访问量排行。  支持浏览器过滤，只审计常用浏览器产生的审计记录。 |
| 刻录审计 | 可以通过黑白名单方式进行审计或不审计指定光盘刻录机，同时可以对指定审计某种文件格式以及所在路径的文件。 |
| 屏幕录像审计 | 支持以截图的形式录制计算机的操作录像。  支持以视频的形式播放，支持快进、快退、暂停、播放速度调节。  支持自定义选择录制的帧率、图像质量。  支持上传和存储到第三方的文件服务器。  支持录像记录文件的定期自动清理功能。  支持基于桌面程序窗口的筛选录制，可实现只录制指定窗口的屏幕记录。 |
| 软件商店 | 1、建立企业软件商店，里面是企业提供的来源安全的软件，并且可以限制员工下载、安装涉及版权的软件，比如设定只有设计部门的员工才能安装CAD软件，确保正版软件的授权点不被其他人占用，规范正版软件的使用  2、管理员可对采购的软件进行订单和授权管理，支持将采购订单导出为软件正版化台账;  3、终端安装后，采集软件的下载、安装、使用情况，为采购计划提供参考。 |
| 正版化管理 | 收集全网电脑安装的商业软件，根据其序列号判断正版软件和盗版软件  支持读取offic、操作系统等软件的激活状态 |
| ★资质要求 | 公安部《信息安全产品检测报告》  公安部《计算机信息系统安全专用产品销售许可证》  国家保密科技测评中心《涉密信息系统产品检测证书（主机监控与审计产品）》 |
| 其他要求 | 验收时对产品进行上述功能要求的逐一测试，全部通过后才能执行合同验收工作，否则将作无条件退货处理，并保留对该厂商追究相关责任的权利。 |

**系统集成及综合布线系统技术要求：**

1、系统集成服务(1项)

|  |  |
| --- | --- |
| 指标 | 技术规格要求 |
| 系统集成服务 | 1. 提供本项目质保期内所有设备的安装、调试以及售后服务。质保期内，投标单位应安排原厂认证网络工程师提供现场技术支持服务，负责医院网络系统技术保障（日常巡检、技术支持、故障处理）等服务。 2. 医院网络的稳定关系到医院的业务正常运营，必须确保在接到用户电话后，工作时间5 x 8小时10分钟内到达现场并承诺一般故障在30分钟内解决；重大故障及时提供备机30分钟内恢复运行并在48小时内修复完成。非工作时间10分钟响应、30分钟到现场并承诺一般故障在30分钟内解决；重大故障及时提供备机30分钟内恢复运行并在48小时内修复完成。**投标单位必须在投标文件中明确说明如何提供上述技术支持服务。** 3. 本项目是“交钥匙工程”，投标单位需了解我院的网络现状，必须确保医院核心交换机、汇聚交换机以及接入交换机的上联及下行的光纤链路能够满足交换机所配的光纤模块支持的最高速率，达到本项目设计的最终效果，否则不予以验收，因光纤或跳线等问题而所产生的整改费用有投标单位自行负责。 |

2、综合布线服务(1项)

|  |  |
| --- | --- |
| 指标 | 技术规格要求 |
| 综合布线服务 | 1、投标单位必须具备专业的综合布线施工资质，满足《综合布线系统工程设计规范》，编号为GB 50311-2007的国家标准。  2、负责2、3号楼弱电间以及数据中心容灾机房的综合布线整改，包括设计、施工以及售后服务。  3、本项目是“交钥匙工程”，投标单位需了解我院弱电井综合布线系统的现状，达到本项目设计的最终效果，否则不予以验收，因更换配线架或跳线等问题而所产生的整改费用有投标单位自行负责。与本项目所提供设备有关的配套材料如光纤跳线、双绞线6类跳线、电源PDU以及综合布线系统所涉及的所有室内外光纤、六类双绞线(需要重新布设六类线的信息点每个信息点所需的六类线按照100米长度计算）总共涉及到约1500个信息点、桥架、PVC管、配线架、理线架、信息点模块、机柜、墙柜等都有中标方提供，我院不在另行支付其他费用。投标商需在网络设备交货时一并提供本次综合布线系统升级所需的所有材料。  4、中标人在中标公告公示期满后七天内签订合同，交换机、综合布线系统材料签订合同后三十天内完成供货。由于本次综合布线项目属于在原有的网络系统上升级，又要考虑到不能影响医院正常的业务系统，院方将根据医院的实际情况分批安排施工，以夜间和周末施工为主，**工期跨度约5个月**（院方有权根据实际情况延长施工周期），待综合布线系统全部施工完毕后方可对本项目进行整体验收。  5、布线系统采用的线缆、配线架等材料需符合国家标准，推荐品牌：兰贝、一舟、东方线缆等品牌。 |

**三、商务需求**

1. 中标后五个工作日内须提供所投设备原厂商针对本项目的售后服务承诺函原件;及软件功能授权说明。
2. 本项目的系统软硬件产品的详细指标，投标人必须对指标要求有明确的响应，针对采购要求如实描述是否偏离。参数加★的条款为核心偏离项，若不满足，则为无效投标。

3、本项目用户方为浙江大学医学院附属妇产科医院，可以通过该产品序列号在生产厂商官方网站或生产厂商 400/800 电话中进行验证，并可查询该产品维保期限，一经发现水货和串货的产品，立即终止合同。

4、验收：中标人在合同签订后30天、内须完成设备到货，调试和系统集成工作后全部完成后，可申请初验，经采购人审核通过后出具验收报告。