# 采购需求

**一、采购项目信息**

1.采购项目名称：郴州市第三人民医院网络接入控制系统项目

2.采购项目的数量及预算：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **数量** | **单位** | **预算金额（元）** |
| 1 | 网络接入控制系统 | 1 | 套 | 56000 |

1. **投标人资格条件**

1、符合《政府采购法》第二十二条规定的条件；

2、具有独立承担民事责任的能力（提供有效营业执照或事业法人登记证或社会团体法人登记证书等相关证明复印件）；

3、具有履行合同所必需的设备和专业技术能力的书面声明（提供《响应供应商资格声明函》）；

4、提供参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明（提供《响应供应商资格声明函》）；

5、供应商未被列入信用中国网站“记录失信被执行人或重大税收违法案件当事人名单或政府采购严重违法失信行为”记录名单；

6、本项目不接受联合体投标。

1. **采购内容**

要求终端准入及桌面管理产品具备出色的远程管理功能，且为功能一体化设计。设备为软硬件一体化设备，软件功能全开放，系统应当具备小型、轻量化的客户端插件，可以保证插件加载后，大部分单位电脑的流畅运行，并确保兼容老旧电脑（WINXP系统等）的安装和使用，产品至少包含1000个LICENSE授权，并支持后续升级扩容。★项目为核心要求项，所投产品必须满足。

|  |  |  |
| --- | --- | --- |
| **指标类型** | | **指标要求** |
| **★配置要求** | | 至少包含1000个LICENSE，并支持后续升级。1U机架式，6个千兆电口、2个USB 2.0接口、1个VGA接口，1个扩展槽。 |
| **架构要求** | | 标准采用B/S架构，便利易操作管理设计；  支持VPN/拨号接入、分支机构联动管理；  服务器系统采用Linux操作系统；  提供断电保护机制，确保异常时网络不受影响。 |
| **★性能要求** | | 客户端插件支持X32\X64平台的Win2003/XP/Vista/WIN7/WIN8/WIN10操作系统；客户端插件支持银河麒麟、UOS ARM版以及中标麒麟操作系统。 |
| **安全要求** | | 平台与客户端之间通讯、策略下发、文件分发等交互全程采用https加密协议和定制端口（非443）； |
| **平台要求** | | 产品控制平台管理账户支持三权分立，具有系统管理员、系统审计员、系统操作员管理账号；  系统支持能够根据管理需要自定义添加账号；  支持Syslog日志服务器对接设置，可传输系统登录、系统操作、终端用户登陆、终端用户修复、移动用户登陆、移动用户修复、高级用户登录、来宾用户登录等日志信息； |
| **准入技术要求** | | 准入技术支持VLAN安全网关、策略路由、DHCP、端口复制、透明网桥、Web-portal等方式；  可对网络划分不同的网络访问区域，至少能够划分安全用户访问区域、来宾用户访问区域、隔离用户访问区域，各访问区域可以根据实际需要进行修改； |
| **准入实施要求** | | 支持无客户端违规外联检测的功能；  支持阻断跨NAT路由器下未安装插件的计算机；  能够与终端的安全测评结果联动，根据测评结果进行终端的阻断与放行处理； |
| **网络拓扑** | | 支持对交换机及路由器等网络设备进行自动发现及展现，展示出网内拓扑情况；违规接入的终端可在拓扑图中通过上联交换机进行颜色报警或提示； |
| **IP地址管理** | | 支持以IP地址池的方式图形化查看网络内的已占用、未占用、长期离线和非法入侵IP，可在地址池中的各地址添加备注，并有报警和图表展示功能。 |
| **★国产操作系统管控** | | 支持银河麒麟V10 ARM MIPS、统信UOSV20 ARM MIPS版操作系统的登录认证、资产收集、U盘管控和进程黑名单管理以及非法外联报警。 |
| **设备信息** | | 支持通过全局设备感知技术自动发现网络中的PC、移动终端、智能设备和哑终端，可详细展示设备的IP、MAC、主机名、操作系统、设备更新时间、在线状态和准入可控状态；并可对设备进行信任、隔离等操作，支持批量操作。 |
| **★远程协助** | | 集成多种桌面支持工具，包括：远程对话、远程文件传输、远程执行、远程重启、远程截屏等功能；支持客户端主动/被动进行远程连接。远程控制不依赖于用户是否登录，也可以通过远程控制进行用户的注销和切换。管理端在控制用户端时，可以远程关闭用户端键鼠，实现完全控制，远程桌面管理发起时，应保证画面的实时性，实现操作和响应画面传输在1秒之内完成，支持全局热键远程执行的应用；  远程会话功能支持文字交互，支持强制与请求交互两种远程控制方式； |
| **例外设置** | | 支持针对特殊终端的白名单放行处理，无须安装插件测评即可入网；放行依据包括IP地址、MAC地址、IP地址段； |
| **违规外联管理** | **事前预防管理** | 禁止使用无线网卡；  禁用3G无线上网卡；  禁止手机代理上网；  禁止使用无线热点；  禁止使用其它网卡；（支持对虚拟网卡的单独设置）  IP/MAC绑定，可设置允许修改DNS；  禁止使用调制解调器。 |
| **事中阻断报警处理** | 能够及时发现终端发生违规外联或具备外联的能力；  违规外联后能够对违规终端进行报警提示操作，支持自定义终端报警内容；  触发报警后，支持对终端进行放置隔离区、锁定屏幕、关闭计算机等应急处理措施；  触发报警后，支持向管理员发送报警短信、报警邮件功能；  触发报警关闭计算机时，支持进行关机前的缓冲时间设置；  支持内网网段自定义功能，可自由调整内网IP范围。 |
| **事后报表统计管理** | 支持对违规外联行为的事后数据统计汇总行为，汇总分析结果支持通过趋势图的形式进行展示；  支持对报警信息的导出、打印功能。 |
| **安全测评** | | 支持安全测评项目的在线一键检测及一键全部修复功能； |
| **USB禁止使用** | | 支持对存储类USB设备进行禁用，不影响非存储类USB外设使用；  支持对USB接口使用进行只读或读写权限设置，禁止通过USB接口向外拷贝数据。 |
| **USB使用申请** | | 终端使用USB时可以主动发起申请操作，申请通过前不允许使用USB存储介质； |
| **★USB使用审计** | | 支持对USB存储介质的插拔行为进行记录；  支持对USB存储介质内的文件操作行为进行详细记录。 |
| **终端安全规范** | | 支持禁用终端所有USB存储设备、蓝牙设备、打印机、便携式设备、光驱介质使用；  支持禁用终端所有无线网卡、3G无线上网卡、手机代理上网、无线热点、调制解调器、其它网卡（含虚拟网卡，除与服务器连接应用的网卡）外联设备； |
| 支持IP/MAC绑定（可设定允许修改DNS）； |
| **终端行为审计** | | 支持针对终端的行为安全审计功能，包括上网行为、用户行为、文件操作等行为，具体包括终端浏览网站审计、终端应用程序审计、终端文件操作审计、终端USB插拔审计、终端USB文件操作审计功能。 |
| **水印信息** | | 支持屏幕水印防护，内容包含用户名、所属部门、用户真实姓名、IP地址、MAC地址、计算机名称、终端时间等，同时支持自定义水印内容； |
| **报表分析** | | 在线状态报表：通过在线状态分析功能，可以对入网终端的在线情况进行分析，包括在线终端、离线终端、长期离线终端的按日期分析功能，并支持按部门分别统计以上终端的分析内容，同时，支持以上数据按照汇总数据与详情数据的分别展示，支持对以上数据的高级查询、导出、打印等操作； |
| **资质证明** | | 具备公安部计算机信息系统安全专用产品销售许可证及检测报告  生产厂商具备软件开发成熟度CMMI5认证 |
|
|
|
|
|
|

1. **售后服务要求**

1、所提供的网络准入控制系统要求提供3年免费升级及维护服务，保修期内，所有软件、硬件系统维护均为免费。

2、供应商需设置售后服务机构，并配置服务人员。故障报修的响应时间为7X24小时。若电话中无法解决，6小时内到达现场进行维护。

3、保修期内，所有硬件设备维修服务均为上门服务，由此产生的费用均不再收取。

4、需提供系统扩充、升级方面的技术支持服务。

5、如产品过保，则厂家需根据需要提供有偿维保服务，包括但不限于有偿上门、维修、升级维护，采购建议等。