**关于南京医科大学附属口腔医院身份准入系统**

**征集潜在供应商的调研公告**

南京医科大学附属口腔医院拟对以下项目进行摸底、调研，公开征集潜在供应商。欢迎符合要求的供应商前来报名。

**项目名称：身份准入系统**

**数量：1套**

**项目基本情况介绍：**

南京医科大学附属口腔医院拟采购身份准入系统一套，通过控制终端违规外联和外部用户入网认证，保障医院重要数据不丢失，防止业务敏感数据泄露，推动数据外发可视。

**资质要求：**

供应商应具有独立法人资格，营业执照。提供有效的证书复印件加盖公章

**请仔细阅读本项目技术参数要求，并提供以下书面材料一式四份。**

1. 本公司满足本项目全部技术参数要求，无疑问。

或

本公司对本项目技术参数有正/负偏离，并附下表表述。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 指标 | 原技术指标 | 正/负偏离 | 原因 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

2、本公司对本项目技术参数有疑问，并附下表表述，标明原技术参数，建议修改内容并阐明原因。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 指标 | 原技术指标 | 建议修改 | 原因 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

1. 质检报告情况汇总表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 质检报告名称 | CMA或CANS或国际权威检测机构或其他 | 依据标准 | 质检报告结果（合格/不合格） |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

1. 该项目人员配置

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 姓名 | 所属工种 | 证书 |
| 1 |  |  |  |
| 2 |  |  |  |

1. 与本项目类似的成功案例（合同或中标通知书复印件）
2. 与本项目相关的公司资质证书专利等证明材料。
3. 报价一览表

|  |  |
| --- | --- |
| **项目名称** | **南京医科大学附属口腔医院 项目** |
| **序号** | **货物名称** | **品牌规格型号** | **数量** | **单价（元）** | **总价（元）** |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
|  |  |  |  |  |  |
| **合计金额** | **人民币（大写） 元整****（¥ 元整）** |
| **供货时间** | **签定合同后（ ）日历天内** |
| **实施期** |  |
| **质保期** |  |

**注：如有配件及耗材需同时提供报价**

**单位名称（公章）：**

**法定代表人（授权代表）签名：**

 **联系电话（手机）：**

 **年 月 日**

**七、时 间：**2022年9月8日(星期四)上午9:00

（请各供应商委派技术人员参会）

**地 点：**江苏省口腔医院新综合楼十三楼1301会议室

信息中心： 陈主任 联系方式：69593126

采购中心： 李老师 联系方式：69593106

注： 1. 提供虚假文件一经查实将终止其参与资格。

 2. 资料一式四份，加盖单位公章并装订成册，概不退还。

**附件：身份准入系统具体技术参数要求**

|  |  |
| --- | --- |
| **指标项** | **技术规格要求** |
| 性能参数 | ★提供不少于1台身份准入设备，网络层吞吐量≥10Gb，应用层吞吐量≥1.5Gb，准入终端数≥3000，包转发率≥132Kpps，内存大小≥8G，硬盘容量≥64G SSD+960G SSD，千兆电口≥6个，万兆光口SFP+≥2个，提供3年URL&应用识别规则库升级，3年产品质保，3年软件升级 |
| 部署方式 | 支持网关模式，网桥模式，旁路模式、主主、主备模式部署，必须支持两台及两台以上设备同时做主机的部署模式；  |
| ★支持部署在IPv6环境中，设备接口及部署模式均支持ipv6配置，所有核心功能（上网认证、应用控制、流量控制、内容审计、日志报表等）都支持IPv6；（提供产品界面截图） |
| DNS代理 | 支持DNS代理，能够基于用户、域名、目标DNS，指定代理策略生效，代理策略可以设置为：重定向至DNS服务器、解析为IP、丢弃、重定向至指定线路； |
| 管理员账号 | 支持SSL加密WEB方式、SSH命令行方式管理设备，可设置四类管理员，分别为系统管理员、安全管理员、审计管理员，以及多种权限的超级管理员； |
| 支持管理员账号登录允许尝试次数可配，并支持管理员用户登录进行双因素认证，密码认证加邮件验证码；管理员账号支持TACACS+/RADIUS/LDAP协议外部认证； |
| 支持审计管理员的操作日志、系统日志等； |
| 实时监控 | ★支持首页分析显示接入用户人数、终端类型；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；带宽质量分析、实时流量排名；泄密风险、工作效率、共享上网等行为风险情况；（提供产品界面截图）； |
| 支持查看当前设备的线路状态，线路带宽利用率以及当前策略的引流流量分布和实时的引流策略，支持设置线路流控策略; |
| 排障工具 | 提供图形化排障工具，便于管理员排查策略错误等故障; |
| 支持针对用户认证的故障进行分析，给出错误详情以及排查建议； |
| 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； |
| 用户管理 | 支持从本地导入和扫描导入，支持以CSV格式文件导入帐户/分组/IP/MAC/描述/密码等信息； |
| 支持为用户添加自定义属性（职位、临时项目组、邮件组等），能够根据用户属性自动归类并可以针对用户属性配置上网权限策略、流控策略，审计策略等; |
| 同一个账号，支持与指定数量的多个终端进行自动绑定； |
| 支持针对特权用户配置免认证key、免审计key、免控制key； |
| 认证方式 | 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； |
| 支持终端用户账号绑定手机号码和微信号，绑定后可以通过手机验证码和微信扫码实现上网快捷登录认证； |
| ★支持通过OAuth认证协议对接，支持阿里钉钉，口袋助理，企业微信第三方账号授权认证；（提供产品界面截图） |
| 支持802.1x认证，支持对接本地和AD域用户源，支持在旁路模式部署下准入生效； |
| 支持绑定MAC免认证入网，打开客户端自动认证上线，支持强制初次上线修改密码，保障批量创建账号后的使用安全性; |
| 支持未认证前推送认证客户端下载页面，减轻客户端分发工作量; |
| 支持强制初次上线修改密码，保障批量创建账号后的使用安全性; |
| 支持根据MAC识别新增终端，用户新终端认证自动触发审批流程，需要管理员审批后才可认证入网; |
| 终端资产管理 | 支持图形化查看当前内网IP使用情况，帮助管理员减少人工维护IP表的工作量； |
| 设备必须支持能自动发现网络中通过无线上网的热点和移动终端的IP和终端类型，支持移动终端型号识别；  |
| 支持以图表方式显示移动终端接入趋势； |
| 终端安全检查 | 支持20款以上主流杀毒软件的运行情况、软件版本、病毒库更新时间检查，对不满足检查要求的终端可重定向页面修复、弹窗提示、限制权限、禁止上网； |
| 支持检查终端是否登录域、是否登录到指定域，对不满足检查要求的终端可弹窗提示、限制权限、禁止上网； |
| 支持检查终端的Windows系统是否属于指定版本范围，对不满足检查要求的终端可弹窗提示、禁止上网； |
| 支持检查终端是否运行指定进程，对不满足检查要求的终端可弹窗提示、禁止上网，可强制中止违规进程； |
| 支持检查终端指定路径是否存在指定文件，对不满足检查要求的终端可弹窗提示、禁止上网，可强制删除违规文件； |
| 支持检查终端注册表是否存在指定项，对不满足检查要求的终端可弹窗提示、禁止上网，可强制删除指定项； |
| 外联检查 | 支持检查终端是否使用无线网卡，对不满足检查要求的终端强制断网，支持向管理员告警，并弹窗提示用户; |
| 支持检查终端是否连接非法WIFI（可设置合法WIFI白名单），对不满足检查要求的终端强制断网，支持向管理员告警，并弹窗提示用户; |
| 支持检查终端是否使用4G网卡，对不满足检查要求的终端强制断网，支持向管理员告警，并弹窗提示用户; |
| 支持检查终端是否使用非法网关（可设置合法网关白名单），对不满足检查要求的终端强制断网，支持向管理员告警，并弹窗提示用户; |
| 支持自定义测试地址，检查终端是否能PING通，对不满足检查要求的终端强制断网，支持向管理员告警，并弹窗提示用户; |
| ★告警事件中增加违规外联告警选项，用于对违规外联行为使用进行预警;（提供产品界面截图） |
| 运维工具外联审计 | ★支持SSH/RDP协议，可对连接开始时间，连接结束时间，传输的流量大小进行审计;（提供产品界面截图） |
| 支持运维类应用的外发附件审计，包括Xshell，Pshell，MobaXterm，SecureCRT； |
| 外设管控与移动存储审计 | 支持便携设备、存储设备、网络设备、蓝牙设备、摄像头、打印机的使用管控; |
| 支持对终端上U盘和移动硬盘接入设置可读写、拒绝、可读、告警; |
| 支持允许特定的外设（包括U盘/存储设备）在终端上使用，并提供批量获取硬件ID的工具; |
| 代理管理 | ★不允许使用外部HTTP代理，不允许使用外部Sock4/5代理，不允许在HTTP,SSL一些的标准端口上使用其他协议（提供产品界面截图） |
| 多线路支持 | 必须支持将多条外网线路虚拟映射到设备上，实现对多线路的分别流控 |
| 流控策略 | ★支持基于用户组、位置、终端类型、URL类型配置流量管控策略，可灵活配置流控单位是IP还是用户名（提供产品界面截图） |
| 网盘审计 | 支持网盘/笔记类应用访问内容和外发文件审计； |
| 离线上网审计 | ★在非内网环境下通过客户端引流实现网页审计、邮件审计、应用审计、流量和时长审计，支持windows终端（提供产品界面截图） |
| 离线终端审计 | 在非内网环境下实现客户端应用审计、U盘审计、IM审计，外发行为日志留存在终端本地，终端接入内网后同步到设备日志中心; |
| 离线终端管控 | ★在非内网环境下，已配置的外设管控、外联管控、访问控制策略保持生效;（提供产品界面截图） |
| 日志管理 | 设备必须支持内置数据中心和独立数据中心； |
| 支持分级配置管理员日志查看权限，管理员登录数据中心只能查看指定用户组的行为日志； |
| 必须支持以USB-Key方式验证接入数据中心的管理员身份； |
| 日志中心所有导出都有对应管理员操作日志、系统日志的日志清理中记录数据删除日志、规则库升级有对应升级日志； |
| 等保合规自检 | 可以对接等保合规自检平台，设备自检后将结果发送给平台，快速输出等级保护合规自检报告； |
| 产品资质 | 公安部颁发的：《终端接入控制（一级）安全专用产品销售许可证》  |
| 产商资质 | 售后服务体系通过ISO9001认证 |