询价公告

项目概况

江苏省南通中学校园网络及安防设备采购项目的潜在供应商应在南通市公共资源交易网获取采购文件，并于2022年6月10日10点00分（北京时间）前提交响应文件。

一、项目基本情况

项目编号：Z320601220116(XJ030)

项目名称：江苏省南通中学校园网络及安防设备采购项目

预算金额：80万元，最终报价超过采购预算的为无效响应文件。

采购需求：详见附件1

合同履行期限：详见项目需求，请仔细研究。

本项目不接受联合体。

二、申请人的资格要求：

1.满足《中华人民共和国政府采购法》第二十二条规定；

2.落实政府采购政策需满足的资格要求：无

3.本项目的特定资格要求：无

4.未被“信用中国”网站（www.creditchina.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重失信行为记录名单；

三、获取采购文件

时间：2022年 6月1日至2022年6 月10日（北京时间，法定节假日除外）

地点：南通市公共资源交易网

方式：自行下载

售价：免费

四、响应文件提交

截止时间：2022年6月10日10点00分（北京时间）

地点：南通市公共资源交易网

五、公告期限

自本公告发布之日起3个工作日。

六、其他补充事宜

  1、对项目需求部分的询问、质疑请向采购人提出，由采购人负责答复。对软件系统有关问题请向软件系统驻场技术人员提出。

2、供应商必须详细报出采购清单中各个子项的名称、品牌、规格型号、数量、单价，且各分项报价合计应当与投标报价总表报价合计相等。**请各供应商务必按照以上要求填报，否则作为无效投标处理。**

注：相关流程和要求，详情请查阅南通市政府采购网（南通市公共资源交易平台）-“办事指南—业务指南—政府采购”中《南通市公共资源交易平台政府采购询价方式供应商投标指引》。

七、凡对本次采购提出询问，请按以下方式联系。

1.采购人信息

名    称：江苏省南通中学

联系方式： 朱先生13901487016

2. 集中采购代理机构信息

名 称：南通市公共资源交易中心

地址：南通市工农南路150号

联系方式：见本项目联系方式

3.项目联系方式

网上询价项目负责人:陈女士（0513-59001963）；

软件系统驻场技术人员：0513-59001839。

**附件1：项目采购需求**

**项目需求**

**一、采购标的需实现的功能或者目标, 以及为落实政府采购政策需满足的要求**

项目名称：江苏省南通中学校园网络设备更新及等保安全监控设备采购项目

采购预算：80万元，最终报价超过采购预算的为无效响应文件。

成交方式：按项目成交

成交原则：

1、符合采购需求且报价最低；

2、网上报价为项目的总价，不得将项目拆分或选择性报价；

3、 成交人不得用以任何方式转包或分包本项目。

1. **采购标的需执行的国家相关标准、行业标准、地方标准或者其他标准、规范**

产品必须是全新、未使用过的原装合格正品，达到国家或行业规定的标准。

1. **采购标的需满足的质量、安全、技术规格、物理特性等要求**

（一）．南通中学校园网设备更新

1、目前现状

我校校园网经过了几次网络建设，目前已基本实现了有线网络和无线网络的全校覆盖。但是最早一批网络交换机购于2012年左右，已满10年，亟需更换新的交换机。另外由于无线网络技术的更新换代，部分老师办公室的无线AP还不支持新的WIFI6，为提高教师的教学备课效率，提升教师们网络使用体验。今年我们需要更换一批教师办公室区域的无线AP。

2、建设目标

可以实现校园网主干网络万兆连接，教师办公区域无线网络支持WIFI6。为教师教学服务，为教师云桌面系统实施提供强有力的网络支撑保障。

3、网络设备技术参数需求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 品牌 | 技术参数 | 总数量 |
| 1 | 面板AP | 锐捷  华为  H3C | 1）支持802.11ax标准，采用双路双频设计，面板型AP，支持嵌入86面板安装方式； 2）★整机4条空间流，整机最大接入速率≥1.775Gbps，5GHz单射频支持2\*2 MIMO，且单射频最大接入速率≥1.2Gbps，2.4GHz单射频支持2\*2 MIMO，且单射频最大接入速率≥0.574Gbps，提供官网截图； 3）★1个1G以太网口上联，4个1G以太网口下联，提供官网截图； 4）★为保证用电安全与电源的易获得性，同时支持802.3af/本地DC12V电源供电模式，提供官网截图； 5）★整机功耗小于10W，提供官网截图； 6）考虑安装后的美观度，面板AP外露墙体部分尺寸不得超过120mm\*86mm（长\*宽）； 7）为快速建立高度隔离的安全网络，设备应支持实现AP虚拟化功能，实现一台AP虚拟为多台AP，分别受不同AC设备独立管理，互不影响。不同虚拟 AP之间数据隔离，虚拟AP在AC上不占用AP License； 8）★提供无线电发射设备型号核准证复印件。 9）★为保障设备的兼容性、稳定性，要求学校现有无线控制器可以对本次项目新增无线AP设备进行统一管理，要求提供兼容性承诺函。 | 15 |
| 2 | 吸顶AP | 锐捷  华为  H3C | 1）★支持标准的802.11ax协议，采用双路双频设计，可同时工作在802.11ax和802.11a/b/g/n/ac模式；（提供官网截图） 2）★支持4条空间流，单频最大接入速率1.2Gbps，整机最大接入速率1.775Gbps；（提供官网截图） 3）发射功率≤20dBm； 4）1个10/100/1000Base-T以太网口，支持PoE供电； 5）工作温度支持-10°C～50°C； 6）★支持防盗锁孔；（提供官网截图） 7）支持IP41防护等级； 8）支持802.3af/本地电源DC48V两种供电模式，整机功耗小于12.95w；（提供官网截图） 9）设备布局紧凑，外观精巧，安装时能够紧贴墙面，边缘高度不大于30mm（长×宽×高）； 10）为保证网络出口稳定性，网络出口需要备份，所投无线接入点具备NAT功能。支持ALG (FTP ALG/DNS ALG)； 11）为快速建立高度隔离的安全网络，设备应支持实现AP虚拟化功能，实现一台AP虚拟为多台AP，分别受不同AC设备独立管理，互不影响。不同虚拟 AP之间数据隔离，虚拟AP在AC上不占用AP License； 12）所投AP内置探针功能，能够对覆盖范围的终端MAC信息进行检测。 13）★为保障设备的兼容性、稳定性，要求学校现有无线控制器可以对本次项目新增无线AP设备进行统一管理，要求提供兼容性承诺函。 | 20 |
| 3 | 24口接入交换机 | 锐捷  华为  H3C | 1）★交换容量≥336Gbps，转发性能≥108Mpps，固化10/100/1000M以太网端口≥24，1G/10G SFP+光接口≥4个； 2）要求所投产品端口浪涌抗扰度≥10KV（即具备10KV的防雷能力）； 3）支持静态路由、RIP/RIPng、OSPFv2/OSPFv3等三层路由协议，要求提供官网截图； 4）★支持专门基础网络保护机制，能够限制用户向网络中发送数据包的速率，对有攻击行为的用户进行隔离，保证设备和整网的安全稳定运行，要求提供官网截图； 5）★支持快速链路检测协议（RLDP），可快速检测链路的通断和光纤链路的单向性，并支持端口下的环路检测功能，要求提供官网截图及快速链路检测协议技术白皮书； 6）支持虚拟化功能，可将多台物理设备虚拟化为一台逻辑设备统一管理，并且链路故障的收敛时间≤50ms； 7）支持SNMP、CLI(Telnet/Console)、RMON、SSH、Syslog、NTP/SNTP、FTP、TFTP、Web； 8）★提供工信部三层交换机进网许可证。 | 4 |
| 4 | 24口POE交换机 | 锐捷  华为  H3C | 1）★交换容量≥336Gbps，转发性能≥51Mpps，固化10/100/1000M以太网端口≥24，1G SFP光接口≥4个； 2）★≥24个电口支持POE和POE+远程供电，整机POE功率输出≥370W； 3）★投标产品面板自带一键查看PoE供电状态功能的PoE按钮，轻按即可查看设备当前的通信状态和供电状态，提供所投产品官网截图； 4）要求所投产品端口浪涌抗扰度≥10KV（即具备10KV的防雷能力）； 5）支持静态路由、RIP/RIPng、OSPFv2/OSPFv3等三层路由协议，要求提供官网截图； 6）★支持专门基础网络保护机制，能够限制用户向网络中发送数据包的速率，对有攻击行为的用户进行隔离，保证设备和整网的安全稳定运行，要求提供官网截图； 7）★支持快速链路检测协议（RLDP），可快速检测链路的通断和光纤链路的单向性，并支持端口下的环路检测功能，要求提供官网截图及快速链路检测协议技术白皮书； 8）支持虚拟化功能，可将多台物理设备虚拟化为一台逻辑设备统一管理，并且链路故障的收敛时间≤50ms； 9）支持SNMP、CLI(Telnet/Console)、RMON、SSH、Syslog、NTP/SNTP、FTP、TFTP、Web； 10）★提供工信部三层交换机进网许可证。 | 3 |
| 5 | 48口接入交换机 | 锐捷  华为  H3C | 1）★交换容量≥432Gbps，转发性能≥144Mpps，固化10/100/1000M以太网端口≥48，1G/10G SFP+光接口≥4； 2）要求所投产品端口浪涌抗扰度≥10KV（即具备10KV的防雷能力）； 3）支持静态路由、RIP/RIPng、OSPFv2/OSPFv3等三层路由协议，要求提供官网截图； 4）★支持专门基础网络保护机制，能够限制用户向网络中发送数据包的速率，对有攻击行为的用户进行隔离，保证设备和整网的安全稳定运行，要求提供官网截图； 5）★支持快速链路检测协议（RLDP），可快速检测链路的通断和光纤链路的单向性，并支持端口下的环路检测功能，要求提供官网截图及快速链路检测协议技术白皮书； 6）支持虚拟化功能，可将多台物理设备虚拟化为一台逻辑设备统一管理，并且链路故障的收敛时间≤50ms； 7）支持SNMP、CLI(Telnet/Console)、RMON、SSH、Syslog、NTP/SNTP、FTP、TFTP、Web； 8）★提供工信部三层交换机进网许可证。 | 2 |
| 6 | 交换机万兆模块 | 锐捷  华为  H3C | 万兆LC接口模块（1310nm），10km，适用于SFP+接口 | 16 |

（二）南通中学校园网等保安全需求项目

1、目前现状

随着学校网站已由教育局统一管理，智慧校园项目已部署至政务云上，目前学校校园网安全主要侧重于终端安全的管理。为满足国家二级等保的要求，在去年已配置下一代防火墙和日志审计系统的基础上，为加强终端安全管理，还需要新增入侵防御系统1台，堡垒机1台，上网行为管理1台以及终端安全EDR。

2、建设目标

学校校园网可以实现全网终端管理，可以快速发现问题，并能够方便定位问题所在以及快速解决终端各类安全问题。

3、等保安全设备技术参数需求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 品牌 | 技术参数 | 数量 |
| 1 | 入侵防御系统IPS | 深信服，山石网科，锐捷 | |  |  | | --- | --- | | **指标项** | **详细参数** | | ★**硬件规格** | 专业IPS设备，基于高性能硬件平台和专业安全操作系统； | | 标准机架，1T硬盘，1个扩展槽，USB接口≥2个，RJ45串口≥1个；本次配置≥4个千兆电口（2组bypass接口）,4个千兆光口； | | 吞吐量≥10Gbps ，最大并发连接数≥200万，每秒新建连接数≥55000； | | **入侵防御** | 支持针对HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS等20余种协议和应用的攻击检测和防御；支持HTTP Get、Head、Put、Post等多种协议方法检查； | | 支持自定义入侵防御特征：可依据IP、TCP、UDP、IGMP、ICMP等网络层的各项参数设置自定义特征；全面设置TCP/IP应用层的特征比对内容而不受通信协议限制；支持跨数据包检测机制，包括：比对位移(matching offset)、比对长度(matching depth)、比对距离(matching distance)、比对范围(within)；支持基于流的数据包(stream-based)比对技术； | | 提供12000多种特征的攻击检测和防御，特征库支持网络实时更新；（中标后签订合同前提供产品功能页面截图） | | 支持威胁详情URI和攻击数据解码；支持IPv6环境下入侵检测和防御；支持IPv6威胁日志显示和下载；支持SSL加密流量的检测和防御； | | **Web防护** | 系统具备对网站外链防护功能，可以对Web服务系统提供保护；系统具备对CC攻击的检测和防御能力，可以对Web服务系统提供保护；系统具备对跨站脚本攻击的检测和防御能力，可以对Web服务系统提供保护；系统具备对SQL注入攻击的检测和防御能力，可以对Web服务系统提供保护；（中标后签订合同前提供产品功能页面截图） | | 系统具备对Referer首部过滤，可以对Refer而白名单之外的HTTP请求进行过滤；系统具备对隐藏IFrame过滤功能，可以对页面中iFrame标签属性做检测；系统具备高频交易访问控制功能，可以对URL访问频率进行限制；（中标后签订合同前提供产品功能页面截图） | | **口令防护** | 支持对ftp、telnet、smtp、pop3、imap弱口令行为进行检测（中标后签订合同前提供产品功能页面截图）  支持对ftp、telnet、smtp、pop3、imap、sunrpc暴力破解行为检测（中标后签订合同前提供产品功能页面截图） | | **应用识别** | 基于应用特征、行为和关联信息的应用识别；可识别超过3000种以上应用程序；支持SSL加密应用识别与控制；能够准确识别IM、P2P下载、文件传输、邮件、在线游戏、股票软件、流媒体、非法信道等应用；支持针对Android、iOS等移动应用的识别；（中标后签订合同前提供产品功能页面截图） | | **高可用性** | 支持接口硬件Bypass；通过外置的组件，支持断电Bypass功能；  ★支持外置Bypass;  支持H-A部署；支持双机热备功能，在单台设备故障时，已建立的会话连接session可以自动切换到HA的另一台设备上，不会引起连接中断； | | **安全策略** | 支持在同一条安全策略设置源安全域、目的安全域、用户、服务、应用、入侵防护和反病毒的访问控制； 支持策略命中数统计功能，便于管理员维护策略；支持预定义和自定义安全策略；安全策略规则支持复制、粘贴和移动操作。支持安全策略的冗余检测；支持安全策略的命中数检测；支持安全策略的时间表有效性检测； | | 支持按照国家地理位置设置安全过滤策略，内置国家地理地址库信息； | | **系统管理** | 登陆管理支持HTTPS、SSH、Console等管理方式；支持Radius或Local方式进行管理员身份认证；支持多级管理权限设置功能，预定义系统管理员、操作员、审计员等管理角色；支持SNMP v1、v2c、V3；支持电子邮件、SNMP、SYSLOG及自定义等多种响应方式进行实时推送；同时支持TAP/L2/L3模式的混合部署。L3模式（支持NAT，PAT，路由等），可支持多条线路；需提供中文管理界面、中文化报表及管理接口；特征库可以通过人工或者自动方式进行入侵防御设备的升级，升级过程中不需重启设备。并能保持原有会话连接不中断； | | ★产品必须支持全功能CLI（SSH、TELNET、CONSOLE等方式）命令配置，以方便快速进行脚本操作和故障调试，且CLI配置必须支持中文输入；（中标后签订合同前提供产品功能页面截图） | | ★操作界面支持中英文切换，支持2个系统软件并存，避免单一操作系统故障影响业务，支持10个配置文件并存，便于快速恢复不同阶段的设备配置；（中标后签订合同前提供产品功能页面截图） | | ★提供手机APP的监控通告服务，服务内容包括：安全资讯、设备监控、告警信息、威胁日志等；（中标后签订合同前提供产品功能页面截图） | | **日志与报表** | 报表需要包含多视角,提供安全风险概览、安全风险详情、威胁类型、网络流量分析、系统运行状况不同维度报表。威胁日志内容至少包含CVE-ID、漏洞描述信息和解决方案；支持日志导出、搜索、日志聚合和过滤搜索；支持威胁日志名称中文显示。（中标后签订合同前提供产品功能页面截图） | | 设备配备大容量硬盘，支持日志报表本地化存储；预定义多种报表类型，支持PDF、word、HTML报表格式，一键生成报表，支持自定义报表；丰富的报表自定义内容，提供配置向导；支持定时自动发送报表、周期性报表输出，以通用格式邮件发送给管理员；支持威胁日志、NAT日志、会话日志、URL日志等日志；支持源、目的IP和威胁ID的日志白名单功能； | | **监控统计** | 支持全面的威胁监控，包括攻击名、严重程度、时间、地址、通信协议和解决建议等信息；支持基于用户/IP查看阻断次数以及应用阻断详情；支持用户应用流量、URL访问等统计分析；支持应用的多维度统计监控，包括应用风险、类别、特征、所用技术等；支持实时流量统计和分析功能；支持设备CPU、内存、温度、风扇等状态监控； | | **路由功能** | 支持静态路由；支持动态路由；支持源路由、源接口路由；支持基于源、目的、用户、应用、服务和时间表的策略路由； | | ★**资质要求** | 所投产品具有公安部颁发的《计算机信息系统安全专用产品销售许可证》，中标后签订合同前提供证明材料； | | 加入微软安全响应中心（Microsoft Security Response Center）发起的MAPP（Microsoft Active Protection Program）计划，作为该计划成员，可在微软发布每月安全公告之前获得微软产品的详细漏洞信息，为用户提供更及时的安全防护, 中标后签订合同前提供证明材料； | | 连续3年入围Gartner IDPS魔力象限或Gartner IDPS 市场指南，提供证明文件，中标后签订合同前提供证明材料； | | 所投产品具有中国信息安全测评中心颁发的《国家信息安全漏洞库兼容性资质证书》（千兆），中标后签订合同前提供证明材料； | | ★**其它** | 中标后三个工作日内，中标人须提供所投型号的产品进行上述功能要求的逐一测试验证，其中打星号参数为必须响应参数，测试中如发现虚假应标的行为将予以废标处理并保留对该厂商追究相关责任的权利，验证通过后签订采购合同。 | | 中标后签订合同前提供以上参数佐证材料并加盖制造商盖章资料及产品制造商3年质保函原件 | | 1 |
| 2 | 堡垒机 | 深信服、帕拉迪、山石网科 | |  |  |  | | --- | --- | --- | | **指标项** | **详细参数** | | | **可管理设备数** | ≥100个 | | | **连接数** | 最大图形并发连接数≥200，最大字符并发连接数≥600 | | | **网络接口** | ≥4个千兆自适应电口 | | | **硬盘容量** | 可用内置存储≥2TB | | | **电源要求** | 单电源 | | | **高可靠性**  **要求** | 支持web页面上配置网口bond绑定，bond模式支持平衡轮循环策略、主-备份策略、平衡策略、广播策略、IEEE802.3ad动态链路聚合、适配器传输负载均衡、适配器适应性负载均衡。  支持双机热备：支持系统配置以及审计日志实时同步；  支持集群部署：系统策略支持统一下发，后期升级扩容方式支持单节点扩容，无需进行软硬件的二次升级即可完成。 | | | **单点登录** | 图形终端协议（RDP、VNC、X11）字符终端协议（Telnet、SSH）文件传输协议（FTP、SFTP）数据库类型（Oracle、SQLDEVELOPER、Informix、DBACCES、Mysql、 SQL Server、Sybase：SCVIEW4、DB2等）WEB应用（HTTP、HTTPS）KVM、其它应用：AS400、REALVNC、PGADMIN、PCANYWHERE、RADMIN、DameWare、CiscoASDM、VMware vSphere Client等、支持IE代填、Google Chrome浏览器代填登录页面 | | | **★H5运维** | 最简单的运维方式，无平台限制，且无需额外安装插件、客户端和配置运维参数等，启用后即可直接在web也页面中进行所有的运维操作  H5-WEB运维水印：控制运维用户在Web运维时是否启用水印，可根据需求开关此功能（中标后签订合同前提供产品截图证明） | | | **文件传输控制** | RDP、FTP/SFTP、SCP文件上传下载控制：根据用户的需求设置细粒度的上传下载的单向控制权限，防止图形资产内、字符资产内数据遭未授权拷贝及下载。 | | | **系统自身安全性** | ★IP自动禁止功能 | 系统支持IP自动禁止功能，对连续登陆账号密码错误的来源IP自动屏蔽，可通过管理员解除屏蔽。（中标后签订合同前提供产品截图证明） | | 自身健康检测 | 支持对应用中心状态、审计状态和端口状态是否正常工作进行一键检查。 | | 安全客户端 | 持安全客户端隐身访问模式，无安全客户端或非授权安全客户端无法访问系统。 | | **用户帐**  **号管理** | 用户角色 | 系统角色需按法案要求进行划分，至少有系统管理员、密码管理员、配置管理员、审计管理员、普通用户等多种角色。 | | 身份认证 | 系统提供身份认证，自然人（员工帐户）登录系统时支持静态口令、Radius认证、LDAP、AD域、数字证书认证、动态令牌认证、USBKEY认证、指纹认证和Google手机动态令牌认证。 | | ★支持指纹认证：至少支持三个厂商的指纹认证。（中标后签订合同前提供产品截图证明） | | 系统内置PKI证书认证功能，用户只需配置USB-KEY即可实现证书登陆认证，实现双因素认证（USB-KEY+PIN码）。 | | 系统内置动态令牌认证，用户不需要额外部署认证服务器，通过配置动态令牌实现双因素认证；同时可支持Google手机动态令牌认证 | | 支持多因子认证自定义组合，可为不同用户组分配不同的认证策略，支持单因素，双因素和多因素的认证策略。 | | **设备及账号密码管理** | ★密函打印 | 支持将目标设备资产的账号密码进行密函打印导出（中标后签订合同前提供产品截图证明） | | 设备账号  自动改密 | 支持linux、unix、网络设备、windows2000/2003/2008的自动改密功能；无需通过插件、引擎或特殊端口对目标设备进行自动改密， | | 在系统完成密码修改之后，自动进行新密码登录测试，以便进一步校验密码修改结果 | | **扩展模块** | 移动运维 | 后期可扩展支持手机及平板等多硬件平台和安卓、IOS、PAD等多种操作系统的移动接入，同时可实现对接入行为的访问控制和行为控制。并能够实现完整审计。 | | 会同功能 | 支持三级会同功能，包含会话会同、密码会同、命令会同；支持会话会同到期后自动断开功能。支持会同生效时间，且支持以web弹窗的方式通知会同授权人。会同人收到会同请求时，刷新页面或登录时会在页面弹窗提示。 | | 协同监督 | 支持会话监督功能，运维人员具备运维会话发起功能，默认情况下不具备会话操作权限，需要向相应的人员进行申请协助，被邀请人同意后赋予操作权限发起人才具备对目标资产的操作权限，并产生相应的监督日志 | | **告警模块** | 图形操作告警 | 支持RDP会话针对操作行为告警（针对标题栏进行告警），可进行告警内容设置。 | | **统计报表** | 报表任  务周期 | 系统应具备在对系统制定报表任务时，可以配置时间周期，支持以图(柱、饼等)，统计、明细数据的方式表现。 | | **★资质要求** | 具备相关单点登录先进性的专利，提供实现一种安全的单点登录访问系统证明先进性证明，中标后签订合同前提供证明材料； | | | 产品成熟度，产品要求成熟度不低于9年，以软件著作权登记证首次颁发日期为准，中标后签订合同前提供证明材料； | | | 国产自研非OEM产品，所投产品必须具有公安部颁发的计算机信息系统安全专用产品销售许可证，具有中国国家信息安全产品认证证书，具备涉密信息系统产品检测证书，中标后签订合同前提供证明材料 | | | **★其它** | 中标后三个工作日内，中标人须提供所投型号的产品进行上述功能要求的逐一测试验证，其中打星号参数为必须响应参数，测试中如发现虚假应标的行为将予以废标处理并保留对该厂商追究相关责任的权利，验证通过后签订采购合同。 | | | 中标后签订合同前提供以上参数佐证材料并加盖制造商盖章资料及产品制造商3年质保函原件 | | | 1 |
| 3 | 上网行为管理 | 深信服，山石网科，锐捷 | |  |  | | --- | --- | | **指标项** | **详细参数** | | **性能要求** | 网络层吞吐量≥10G，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≥600000； | | **硬件要求** | 内存大小≥8G，硬盘容量≥64G SSD+960G SSD，接口≥6个千兆电口、≥2个万兆光口SFP+，单电源，1U设备； | | **部署方式** | 支持网关模式，网桥模式，旁路模式等多种部署模式； | | 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） | | **系统管理** | 支持统一平台设备下发升级包，一次下发，2 台设备连续同时升级成功。升级过程中会进行双机切换来保证业务不中断； | | **实时监控** | ★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；泄密风险、违规访问、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； | | **认证方式** | ★支持冻结认证失败次数超过最大值的用户，在冻结时间结束后恢复登录；（提供产品界面截图） | | 限制某个新用户只能在某个IP段、MAC段范围内登录； | | **应用管理** | ★1.对Saas应用有默认分类标签，帮助客户统一配置策略 2.必须支持超过200种主流网络会议/办公OA/教育学习应用;（提供产品界面截图） | | 支持基于用户组、终端类型、位置的QQ白名单功能； | | **网页审计** | ★支持网页内容审计后的网页快照功能；（提供产品界面截图） | | 审计SSL网页时，支持加密证书自动分发功能，用户点击网页上的工具即可一次性安装完成； | | 支持用户可以自定义产生根证书，导入包含秘钥的根证书； | | 支持基于时间段/用户/用户组/终端类型/位置等维度的多种上网行为统计排行报表，至少包括7种； | | 支持查询和导出基于指定时间段/用户/用户组的文件审计、邮件收发、访问网站、即时通讯、发帖/微博、搜索关键字等详细用户行为的报表； | | ★针对单用户的行为分析（包括：应用流速趋势、应用流量排行、域名流量排行、应用时长排行、域名时长排行、行为汇总排行等）;（提供产品界面截图） | | **邮件管理** | 支持根据源地址和目的地址过滤外发邮件；必须支持https网页全解密和按网站类别分类进行解密配置； | | **排障工具** | ★支持针对用户认证的故障进行分析，给出错误详情以及处置建议；（提供产品界面截图） | | ★支持针对上网权限策略进行检测分析，查看各个应用是否匹配相关策略；（提供产品界面截图） | | **流量管理** | 支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率；空闲值可自定义； | | ★支持通过抑制P2P的上行流量，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） | | ★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、优先级，启用状态等;（提供产品界面截图） | | **产品及厂商资质** | 提供公安部颁发的《网络通讯安全审计产品 销售许可证》复印件； | | 厂商的研发体系需通过国际认证CMMI5； | | 厂商具备中国网络安全审查技术与认证中心的信息安全软件开发服务资质，提供有效证书复印件； | | 厂商需具有国家应急中心应急支撑单位CNCERT证书（国家级）； | | 1 |
| 4 | 终端安全管理系统EDR | 深信服，奇安信，火绒 | |  |  | | --- | --- | | **指标项** | **详细参数** | | **产品形态** | 产品可以纯软件交付，包含管理控制中心软件及终端客户端软件，其中管理控制中心可云化部署；同时也支持硬件管理平台交付； | | **Windows PC 客户端支持** | Windows XP/Windows Vista/Windows 7/Windows 8/Windows 8.1/Windows 10 ； | | **管理可视化** | 采用B/S架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能； | | **多维度威胁展示** | ★支持全网风险展示，包括但不限于未处理的勒索病毒数量、暴力破解数量、WebShell后门数量、高危漏洞及其各自影响的终端数量；（需提供产品截图证明） | | **云端威胁分析** | ★支持跳转链接至云端安全威胁响应系统，针对已发生的病毒的基本信息，影响分析（客户情况、影响行业、区域分布）、威胁分析和处理建议;（需提供产品截图证明 ） | | **策略配置管理** | ★支持安全策略一体化配置，通过单一策略即可实现不同安全功能的配置，包括：终端病毒查杀的文件扫描配置、文件实时监控的参数配置、WebShell检测和威胁处置方式、暴力破解的威胁处置方式和Windows白名单信任目录； | | **资产管理** | ★支持全网视角的终端资产统一清点，清点信息包括操作系统、应用软件、监听端口和主机账户，其中操作系统、应用软件和监听端口支持从资产和终端两个视角进行统计和展示；（需提供产品截图证明） | | 支持收集并展示单个终端的基本信息，包括：主机名、在线/离线状态、IPv4地址、MAC地址、操作系统、终端agent版本、病毒库版本、最近登录时间、最近登录的用户名；终端信息变更能自动更新； | | **终端日志报表** | 支持根据统计周期、终端名称、IP地址，补丁信息和漏洞等级等多维度的入侵检测日志，杀毒扫描日志，微隔离日志，合规检测日志，管理员操作日志，运维日志，联动日志等的日志查询和检测； | | **管理员管理** | 支持配置不同的权限角色，支持超级管理员、普通管理员（管理）、审计管理员（查看）三种权限，并配置可管辖的终端范围，支持管理员账号限制IP登录；支持管理员账号采用用户名密码和USBKey双因素认证； | | **威胁检测** | 具备基于人工智能的检测引擎，支持无特征检测技术，有效应对恶意代码及其变种； | | **勒索病毒专防** | ★基于勒索病毒攻击过程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御；（需提供产品截图证明） | | ★支持监控诱饵文件，诱饵文件可被实时监控，当勒索病毒对该文件进行修改或加密操作时进行拦截；（需提供产品截图证明） | | **挖矿病毒巡检** | ★提供挖矿病毒巡检工具，支持通过内存、进程和启动项来检索病毒相关信息；（需提供产品截图证明） | | **威胁同步处置** | 构建全网文件信誉库，当一台终端发现某一病毒文件，全网可进行感知并进行针对性查杀，支持处置病毒时选择是否在其它终端上同步处置； | | **广告弹窗拦截** | ★支持对主流70+款软件进行广告弹窗拦截，让办公环境更纯净；支持在客户端查看拦截效果，包括拦截内容、拦截次数等； | | **远程桌面控制** | ★支持远程控制管控终端桌面的功能，便于管理员能够及时对存在故障的终端进行维护； | | **USB设备管控** | 支持分组的USB存储是管控防护启用，不允许指定终端分组下的终端使用USB存储设备；支持对USB存储设备设置基于设备ID的白名单，允许白名单设备使用； | | **上网行为管理的联动响应** | ★支持与同厂商的上网行为管理平台进行安全联动，支持管理员在上网行为管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息；（需提供产品截图证明） | | **资质** | 提供公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》网络版防病毒产品（一级品）资质证书； | | 厂商软件研发实力需通过CMMI L5认证； | | 厂商应是国家互联网应急响应中心网络安全应急服务国家级支撑单位； | | 300 |

（三）校园监控

1.目前现状:东门传达室原显示屏已经使用12年以上 需更换需要在东门传达室增加监控大屏，几个食堂根据要求增加40个摄像头。

2.建设目标

在传达室建成9个46寸监控大屏，更好地监控整个校园，保证校园安全。食堂在关键点位增加40个摄像头确保饮食安全

3. 监控设备清单技术参数需求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 品牌 | 技术参数 | 总数量 |
| 1 | LED拼接屏 | 海康 大华 宇视 | LCD显示单元为：46“超窄边液晶屏；物理分辨率达到1920×1080，响应时间≤8ms。  LCD显示单元物理拼缝≤3.5mm，亮度达到610cd/㎡，对比度达到1200:1，图像显示清晰度≥950TVL，亮度鉴别等级为11级。（提供公安部出具的检验报告复印件）  LCD显示单元通过CCC、CE、CB、FCC检测认证，并提供CCC、CE、CB、FCC认证证书。  LCD显示单元具备能效等级为1级的CQC节能认证证书、CEC环境I型认证证书。  ★液晶显示单元内置图像处理芯片，能够实时分析显示内容资料，实现在影片、汇报和监控三种场景模式下智能切换。（提供封面具有CMA、ilac-MRA、CNAS标志的权威检测机构的检测报告复印件）  ★无需额外配置分配器或矩阵，液晶显示单元本身支持VGA、DVI、HDMI和DP四种信号中任意一种信号输入，均能通过HDMI或者DP环出，且信号环通级数达到35级，最后一级显示无噪点。（提供封面具有CMA、ilac-MRA、CNAS标志的权威检测机构的检测报告复印件）  ★拼接屏具有解析总数据量不超过3840 x 2160的任意分辨率信源的功能。（提供封面具有CMA、ilac-MRA、CNAS标志的权威检测机构的检测报告复印件）  ★拼接屏具有实时分析当前画面亮度分布比例，自动调整亮度值的功能，具有动态调节画面对比度，可提高暗阶画面亮度，增强暗画面显示细节的功能。（提供封面具有CMA、ilac-MRA、CNAS标志的权威检测机构的检测报告复印件）  ★为保护环境要求，液晶拼接屏需满足中国电器电子产品有害物质限制使用的要求，并提供中国质量认证中心产品认证证书。  ★LCD产品制造商作为起草单位参与国家标准GA/T 1084-2020《大型活动用拼接显示系统通用规范》的起草  LCD显示单元支持U盘点播，内置MPEG、JPEG和RealMedia解码器，支持点播U盘、移动硬盘中的视频、图片、音频或文本资源。视频：支持TS、3g2、avi、mkv、mov、mp4、mpg、tp等文件。音频：支持mp3、wma、m4a、wav、aac等文件。图片：支持jpg、bmp、png等文件。文本：支持txt文件。 | 9 |
| 2 | LCD拼接屏底座 | 海康 大华 宇视 |  | 1 |
| 3 | 高清线 | 绿联 秋叶原 海康 | 10米HDMI | 10 |
| 4 | 解码器 | 海康 大华 宇视 | 采用嵌入式架构，专用Linux系统，使用DSP解码。为了设备稳定可靠运行，不得采用工控机或者PC机的X86架构。  具有10个HDMI输出接口、1个VGA输入接口、1个DVI输入接口、2个USB口、1个语音对讲输入、1个语音对讲输出、10个音频输出、8个报警输入、8个报警输出、1个RS485接口、5个CVBS输出接口（通过转接头实现）、1个RS232接口，2个千兆网口、2个光口。样机采用AC220V电源供电。  具有1个电源指示灯、1个VGA信号接入指示灯和1个DVI信号接入指示灯  ★支持对输入的视频画面进行90°、180°、270°旋转显示。（提供封面具有CNAS认证标识的公安部报告证明。）  ★设备接入具有智能行为分析功能的摄像机，可解码显示智能行为分析信息，包括移动侦测、越界入侵、区域入侵、起身离开等，并上传报警信息。（提供封面具有CNAS认证标识的公安部报告证明。）  ★支持前端接入智能摄像机，直连前端人脸检测设备，可实时展示人脸检测结果，包括年龄、性别、是否戴眼镜等人脸属性信息；属性直接叠加画面显示。（提供封面具有CNAS认证标识的公安部报告证明。）  ★支持黑白名单功能，可设置256个黑白名单；当设置白名单时，只允许白名单IP访问设备；当设置黑名单时，黑名单内IP无法访问设备（提供封面具有CNAS认证标识的公安部报告证明。）  ★输入信号接入解码器后上墙显示，支持YUV422上墙显示；（提供封面具有CNAS认证标识的公安部报告证明。）  ★支持PC 软件客户端、WEB 浏览器客户端、平台客户端、IPAD、可视化触控平台方式访问管理。（提供封面具有CNAS认证标识的公安部报告证明）  ★设备可通过RTSP协议、ONVIF协议接入前端设备的视频流。为保证前期项目兼容性，需要能接入海康威视私有协议（SDK）。（提供封面具有CNAS认证标识的公安部报告证明。）（！！！括号部分删除使用。写入标底此句话斟酌使用，其中海康私有协议具有强控标性，但容易被质疑，解释可以说前期项目中有海康产品！！！） | 1 |
| 5 | 摄像头 | 海康 大华 宇视 | 具有400万像素CMOS传感器。  最大分辨率2560x1440。（公安部检验报告证明）  需具有20路取流路数能力，以满足更多用户同时在线访问摄像机视频。（公安部检验报告证明）  ★最低照度彩色：0.0008lx，黑白：0.0001lx，灰度等级不小于11级。（公安部检验报告证明）  红外补光距离不小于85米。（公安部检验报告证明）  需支持三码流技术，可同时输出三路码流，主码流最高2560x1440@30fps，第三码流最大2560x1440@30fps，子码流704x576@30fps。（公安部检验报告证明）  在2560x1440@25fps下，清晰度不小于1400TVL。（公安部检验报告证明）  支持H.264、H.265、MJPEG视频编码格式，且具有HighProfile编码能力。（公安部检验报告证明）  信噪比不小于55dB。（公安部检验报告证明）  需支持8行字符显示，字体颜色可设置，需具有图片叠加到视频画面功能。（公安部检验报告证明）  需具有黑白名单功能，其中白名单可添加不小于10个IP地址。（公安部检验报告证明）  需具备人脸检测、区域入侵检测、越界检测、虚焦检测、进入区域、离开区域、徘徊、人员聚集、逆行、场景变更等功能。（公安部检验报告证明）  可开启或关闭智能后检索功能。（公安部检验报告证明）  需具有电子防抖、ROI感兴趣区域、SVC可伸缩编码、自动增益、背光补偿、数字降噪、强光抑制、走廊模式、视频水印等功能。（公安部检验报告证明）  摄像机能够在-30~60摄氏度，湿度小于93%环境下稳定工作。（公安部检验报告证明）  设备与客户端之间用100米网线进行传输，数据包丢包率小于0.1%。（公安部检验报告证明）  不低于IP67防尘防水等级。（公安部检验报告证明）  需支持DC12V供电，且在不小于DC12V±30%范围内变化时可以正常工作。（公安部检验报告证明）  设备工作状态时，支持空气放电8kV，接触放电6kV，通讯端口支持6kV峰值电压。（公安部检验报告证明）  同一静止场景相同图像质量下，设备在H.265编码方式时，开启智能编码功能和不开启智能编码相比，码率节约1/2。（公安部检验报告证明） | 40 |
| 6 | 网络线 | 海康 一舟 普鲁斯特 |  | 8 |
| 7 | 系统集成费 |  |  |  |

**（注：投标参数必须完全响应不允许负偏离，出现负偏离的作无效投标处理）**

**投标技术参数要求的技术白皮书证明材料在签订合同时提供，不能提供的作废标处理。**

网络设备，等保设备，监控设备中的建议品牌，只是建议所采购产品（设备）的档次。投标人可以选择建议品牌，也可以选择建议品牌以外的品牌，但所选品牌档次须等于或高于建议品牌档次。投标人所投品牌非建议品牌的，其档次不得低于建议品牌，同时投标人应当在投标时提供以下资料：①由地级市及以上技术检测机构针对本次招标采购而出具的符合本项目招标要求的投标产品检测报告；②技术白皮书；③生产许可证。①②③项出具材料为复印件的，则需加盖厂家红章。当三分之二评委认定所选品牌档次低于建议品牌档次的，将作无效响应处理。

1. **采购标的数量、采购项目交付或者实施的时间和地点**

1、 采购标的数量：设备清单

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 名称 | 规格型号 | 单位 | 数量 | 单价 | 总价 | 品牌 |
| 1 | 面板AP |  | 只 | 15 |  |  |  |
| 2 | 吸顶AP |  | 只 | 20 |  |  |  |
| 3 | 24口接入交换机 |  | 台 | 4 |  |  |  |
| 4 | 24口接入交换机 |  | 台 | 3 |  |  |  |
| 5 | 48口接入交换机 |  | 台 | 2 |  |  |  |
| 6 | 交换机万兆模块 |  | 只 | 16 |  |  |  |
| 7 | 入侵防御系统 | IPS | 套 | 1 |  |  |  |
| 8 | 堡垒机 | 安全运维审计系统 | 套 | 1 |  |  |  |
| 9 | 上网行为管理 | AC | 套 | 1 |  |  |  |
| 10 | 终端安全管理系统 | EDR | 套 | 1 |  |  |  |
| 11 | LED拼接屏 | 46寸 | 套 | 9 |  |  |  |
| 12 | LCD拼接屏底座 |  | 套 | 1 |  |  |  |
| 13 | 高清线 |  | 根 | 10 |  |  |  |
| 14 | 解码器 |  | 套 | 1 |  |  |  |
| 15 | 摄像头 |  | 套 | 40 |  |  |  |
| 16 | 网络线 |  | 箱 | 8 |  |  |  |
| 17 | 系统集成费 |  |  |  |  |  |  |

2、交货期（服务时间）：成交供应商须在合同签订后45个工作日内完成整个项目，保证所有系统均能正常使用。

3、交货（服务）地点：南通市崇川区中学堂街9号，江苏省南通中学。

1. **采购标的需满足的服务标准、期限、效率等要求**

1、中标人应当在中标通知书发出之日起15日内，按照招标文件确定的事项与采购人签订政府采购合同。

2、投标参数必须完全响应不允许负偏离，出现负偏离的作无效投标处理。

3、投标时上传所投设备的原厂质保服务承诺函（加盖厂商公章），原件在签订合同时提供，不能提供的作废标处理。

4、所有设备原厂三年质保。

5、中标供应商须提供安装、调试、培训、维护等服务，所有设备在质保期内提供免费维护维修及技术支持。保修期以外提供免费维护和技术支持，维修只收材料成本费。设备发生故障时，接到用户通知需2小时内上门，48小时内解决问题。

1. **采购标的验收标准**

在接到供应商以书面形式提出验收申请后，在5个工作日内及时组织相关专业技术人员，必要时邀请采购中心、质检等部门共同参与验收，并出具验收报告，作为支付货款的依据。

1. **付款方式**

1、合同签订生效后，学校预付中标单位合同总金额的30%；   
2、中标单位安装调试完毕且学校验收合格后，学校支付中标单位至合同总金额的95%;   
3、验收合格满一年后，支付合同总金额剩余5%。

**八、本项目不接受进口产品投标**