**货物需求及技术要求**

**一、商务要求：**

|  |  |  |
| --- | --- | --- |
| **序号** | **商务条款名称** | **具体要求内容** |
| 1 | 付款方式 | 签订合同后，经采购人验收合格，一次性付清。 |
| 2 | 供货及安装地点 | 安庆职业技术学院 |
| 3 | 供货及安装期限 | 签订合同后10日历天内完成。 |

**二、技术要求一览表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 货物名称 | 技术参数要求 | 单位 | 数量 | 备注 |
| 1 | 日志审计一体机 | 1.硬件要求：1U设备，交流冗余电源，2个USB接口，1个RJ45串口,1个管理口，≥6个千兆电口，≥1个接口扩展槽位，4TB SATA硬盘，本项目授权支持100个日志源。 ★2.系统应支持各种设备、网络设备、数据库、Windows主机、Linux主机、Web服务器、虚拟化平台、网络流量设备、中间件、业务系统、文件等日志的接入，同时支持规则自适应日志接入，仅输入IP范围及端口即可自动匹配相应规则，完成日志自动接入。**（合同签订后供货前提供带有CNAS或CMA标识的第三方检测机构出具的检测报告复印件。）** 3.系统支持采集的设备厂家包括但不限于：NSFOCUS(绿盟科技)、Venustech(启明星辰)、Topsec(天融信)、DBAPPSecurit(安恒)、SANGFOR(深信服)、Hillstone(山石网科)、东软、瑞星、金山、网康、360网神、Dptech(迪普)、艾科网信、Imperva、Juniper(瞻博网络)、F5、Symantec(赛门铁克)、Deep Security(趋势科技)、MaAfee(迈克菲)、Fortinet(飞塔)、Windows、Linux/Unix、Cisco(思科)、HUAWEI(华为)、H3C(华三)、中兴、Apache、nginx 、IIS、WebLogic、Vmware、Kvm、Xen、OpenStack、Hyper-V、华为FusionSphere、Oracle、MySQL、PostgreSQL、SQL Server、Bind等。 4.日志管理：系统应支持范式化日志多级提取，系统应支持正则、KV、格式串等多种灵活的提取方式，系统应支持自动生成正则以高效的辅助提取。 5.支持规则自适应日志接入，支持将新接收的日志信息与系统内置规则、自定义规则进行匹配，将匹配度最高的规则与接收到的日志进行关联，完成自动接入。6.事件告警：系统应支持查询实时事件，支持自定义查询事件，支持模糊查询，系统应支持事件规则自定义，支持面向日志类型的规则配置。 ★7.资产管理：系统应支持对资产进行监控配置，包含资源监控、采集监控、采集限速等，支持展示资产的详细信息，点击关注资产，即可在资产列表中进行置顶。**（合同签订后供货前提供带有CNAS或CMA标识的第三方检测机构出具的检测报告复印件。）** 8.报表管理：系统应能支持自定义报表目录、LOGO等；系统应能够按照多种维度统计日志信息，系统应支持统计分析报表与多种文件格式导出，系统应能支持用户上传自定义报表模板。 9.用户管理：系统应支持支持用户自定义账号，系统应支持管理员、审计员、操作员多种权限设置，系统应支持来访IP限制，对暴力猜测IP地址进行锁定。 10.支持的数据采集方式包括但不限于SYSLOG、RSYSLOG、SNMP Trap、FTP、ODBC、JDBC、Net flow、WMI、二进制数据、专用Agent等方式采集日志。  ★12.免费原厂质保3年。**（响应文件中须提供承诺函，格式自拟）** | 台 | 1 |  |
| 2 | 安全接入平台 | 一、性能参数：  设备具有CPU≥8C及以上处理器，32G及以上内存，4T及以上硬盘，6个千兆电口，2个万兆光口；标准2U设备。  二、基本参数：  1.支持并发用户数≥800。  三、部署模式：  1.支持软、硬件一体设备，必须为厂商自主研发产品，拥有自主知识产权。  四、协议支持：支持以下协议：  HTTP,HTTPS,UDP,TCP,ICMP,SSH,SNMP,Telnet,SSL,IPV4，IPV6。  五、产品指标要求：  ★1.产品需同时支持WEB VPN和SSL VPN模块。产品应在无需安装客户端或控件情况下，在后端进行业务发布方式即可访问学校电子图书资源、OA、科研、财务、教务系统等各类B/S业务系统。产品支持客户登录成功，可以通过点击对应访问图标的方式进行一键式访问。**（响应文件中提供产品功能截图证明）**  2.产品支持WEB终端。在不安装任何控件下，只需从浏览器就可使用如：RDP、SSH、VNC、Telnet等维护工具，同时支持对操作过程视频录制回放功能，方便对运维终端的溯源审计。  ★3.产品需支持限制应用仅能在对应操作系统展示及访问。**（响应文件中提供产品功能截图证明）**  ★4.支持微信、企业微信、钉钉、飞书扫码登录方式及其他三方扫码登录，支持SIM卡认证、Ukey数字证书认证、TOTP认证、人脸认证方式，可对webvpn系统内发布的web应用进行免密登录配置，并支持企业微信、钉钉、飞书的数据同步，同步方式可配置全量同步、反向同步等同步方式。**（响应文件中提供产品功能截图证明）**  5.产品需支持IPV4 /IPV6双栈接入访问，IPV4和IPV6互访。  6.产品需与门户系统、网上办事大厅等系统做深度融合，保证用户不受时间地点限制，内外网使用体验感完全一致。  7.产品需提供OAuth、CAS、SAML、DB、短信认证、AD、LDAP、RADIUS、MySQL、Oracle、SqlServer等认证方式。可针对用户支持密码、短信、邮件等多因素认证。  8.产品支持多种社交化认证方式，如微信、企业微信、钉钉扫码等。  9.产品提供不少于4路ISP网络接入到用户网络，实现不同ISP线路快速接入，并保障访问的源进源出能力。  ★10.支持与客户现有第三方APP进行SDK集成能力，且无需二次开发，可提供SDK文档，实现将vpn隧道能力集成给客户现有APP，用户登录自有APP后，即可具备vpn隧道能力。**（响应文件中提供第三方APP接口对接的功能截图证明）**  11.支持创建临时账号，管理员可设置账号类型为临时或永久，临时账号可选择使用日期，过期后自动失效。  12.支持终端绑定，管理员可设置PC端、移动端终端最大绑定数量，可设置PC端、移动端设备绑定数量取值范围。  ★13.支持在终端上启用水印，可展示内容包括账号、终端名称和登录时间，可以配置字体大小、字体透明度、文字方向和颜色。**（响应文件中提供产品功能截图证明）**  ★14.支持数据脱敏，对用户访问过程中，可对身份证、手机号、银行卡信息进行脱敏处理。**（响应文件中提供产品功能截图证明）**  15.支持创建内外网应用访问策略，内网IP支持配置IPv4、IPv6、IPv4段、IPv6段，执行范围支持以全局、所属用户组、用户的形式下发，应用范围支持以全局、应用组、应用、的形式下发；  ★16.支持对于第三方用户进行用户组切换，便于对第三方人员权限进行细粒度的划分，支持开启/关闭反同步功能。**（响应文件中提供产品功能截图证明）**  17.支持管理员角色和账号的创建，系统自带三权分立权限分配，包括：操作管理员、审计管理员和系统管理员。  ★18.支持对软件资产进行分类并预置软件分类，包括1）安全软件 2）游戏 3）下载工具 4）解压刻录 5）音乐软件 6）聊天软件 7）网络应用 8）办公软件 9）系统工具 10）财务软件等，方便的用户终端软件的统一管理。**（响应文件中提供产品功能截图证明）**  19.支持终端绑定，管理员可设置PC端、移动端终端最大绑定数量，可设置PC端、移动端设备绑定数量取值范围。  ★20.具备策略分发能力：支持基于用户的远程接入控制策略分发、支持基于用户角色的远程接入控制策略分发；支持用户认证管理：包括用户管理、用户鉴别信息、用户身份鉴别等；支持双机热备模式部署。**（合同签订后供货前提供带有CNAS或CMA标识的第三方检测机构出具的检测报告复印件。）**  ★21. 支持多种认证方式编排形成认证链：  （1）支持根据认证配置调用对应的认证因子进行认证，可对两个以上认证因子进行认证编排；**（响应文件中提供产品功能截图证明）**  （2）支持任意一种认证和按照优先级等级认证两种多因子认证方式；**（响应文件中提供产品功能截图证明）**  ★22.支持基于场景的安全策略编排，并以场景化进行保存，快速调用，如登录认证场景（内外网登录策略、威胁IP二次认证策略、账号撞库策略）、web应用访问场景、隧道管控场景（已知应用统计、未知应用标记、访问僵尸应用初始策略、数据采样）等；支持基于多场景安全策略评估结果联动控制，如在web应用访问场景中触发的安全策略评估结果，可以自动提供给用户登录场景进行调用。**（响应文件中提供产品功能截图证明）**  ★23、支持网络管控，包括违规外联管控和禁用WIFI连接，支持配置可连接的WIFI白名单。**（响应文件中提供产品功能截图证明）**  六、信息安全要求  1.产品能够有效阻止外部工具对内部业务系统的扫描探测，并针对所发布的浏览器应用进行URL地址伪装，防止服务器真实IP地址泄露，免遭恶意攻击，保障内部系统安全；  2.产品支持DES、3DES、SHA、RSA等商用密码以及SM2、SM3、SM4国密算法保障传输安全；  3.产品客户端支持不依赖虚拟网卡方式建立隧道，从而减少系统的兼容性问题；  4.支持访问白名单机制，把不在访问策略范围内的资源直接通过原有路径进行访问；  5.支持地址轮询，通过多个IP轮询访问电子资源，有效规避电子资源方将系统IP地址识别为恶意地址。  七、动态感知要求  ★1.产品提供态势感知大屏，智能化统计安全数据。支持把这些信息统一通过数据接口实时传输给其他态势感知平台或者数据安全监控平台或者大屏幕系统，以便做更全面的用户行为分析和数据安全分析。**（响应文件中提供产品功能截图证明）**  八、兼容性/用户端侧要求  1.产品支持主流浏览器访问：chrome、firefox、360、qq、ie11、edg等；  2.产品支持手机、笔记本电脑、台式电脑等终端使用；  3.产品支持当前市面上主流的终端操作系统，如：Windows 7/8/10，Mac，ios，Android。  九、系统管理要求：  1.产品支持多级管理员管理，超级管理员可以设定多个不同权限的管理员，并且支持管理员只读和读写全选的切换；  2.支持管理员查看针对某个账户的一次成功登陆鉴权访问，查看策略执行过程；  3.支持详细的账户控制策略，包括但不限于：登录时间策略、登录密码复杂度、多因子配置；  4.支持便捷的用户管理，可以和现网系统对接，做用户导入及对应同步更新。  十、日志审计要求  1.产品日志支持独立审计功能；  2.支持用户概览、应用概览、登录审计、异常审计分析日志的图表化PDF报表导出，包括且不限于：饼状图、柱状图、折线图、列表图等；  3.产品日志提供详细记录用户访问信息（用户、主机IP、访问内容、访问时间）、管理员日志（管理员、主机IP、时间、管理行为、对象）、系统日志、告警日志；可根据用户名、主机IP等信息进行用户行为查询；可提供用户组/用户流量排行及查询、资源流量排行及查询、资源活跃程度、用户活跃程度等记录。  ★4.支持日志审计功能：包括审计数据生成、审计日志存储、审计日志管理。**（合同签订后供货前提供带有CNAS或CMA标识的第三方检测机构出具的检测报告复印件。）**  十一、服务要求  1.质保期内提供免费统一认证、门户、办事大厅等对接服务。  2.针对本次系统中存在的bug、缺陷、信息安全漏洞，不论在保期内、外，供应商均应免费持续提供修正与消缺服务。  十二、应急处理措施  ★1.产品支持根据学校实际需求在不改动架构的情况下，结合疫情和师生实际使用情况做调整，如果学生同时在线人数超过800以上，承诺将并发量临时调整至3000，有效期一个月。**（响应文件中供应商提供承诺函。）**  ★2.供应商须承诺在质保期内，如果硬件设备出现意外故障，承诺在48小时内免费给学校更换一台新设备。**（响应文件中供应商提供承诺函。）**  ★十三、免费原厂质保3年。**（响应文件中供应商提供承诺函。）** | 台 | 1 |  |
| 3 | 下一代防火墙 | ★1、对天融信下一代防火墙NGFW4000-UF提供设备1年的软件升级及原厂维保服务；**（响应文件中提供原厂服务承诺并加盖供应商公章，承诺函格式自拟）** 2、提供1年硬件整机保修服务，在硬件质保期内，对硬件产品整机给予保修； 3、提供设备1年的应用识别库和专业防病毒升级授权； 4、提供1年电话咨询及远程调试服务，在服务期内，由天融信原厂工程师提供电话咨询及远程技术协助服务； 5、提供1年上门现场支持服务，在服务期内，对采购人使用过程中遇到的问题，如用户咨询及远程技术协助不能解决，将派遣天融信原厂工程师赴现场解决技术问题，为采购人提供现场技术支持；  ★6、每季度需要现场巡检一次，并提供巡检报告。**（响应文件中供应商提供承诺函。）** | 项 | 1 |  |
| 4 | 数据库审计 | ★1、对天融信数据库审计TA-DB提供设备1年的原厂维保服务；**（响应文件中提供原厂服务承诺并加盖供应商公章，承诺函格式自拟）**  2、提供1年硬件整机保修服务，在硬件质保期内，对硬件产品整机给予保修； 3、提供1年电话咨询及远程调试服务，在服务期内，由天融信原厂工程师提供电话咨询及远程技术协助服务； 4、提供1年上门现场支持服务，在服务期内，对于采购人使用过程中遇到的问题，如采购人咨询及远程技术协助不能解决，将派遣天融信原厂工程师赴现场解决技术问题，为用户提供现场技术支持；  ★5、每季度需要现场巡检一次，并提供巡检报告。**（响应文件中供应商提供承诺函。）** | 项 | 1 |  |
| 5 | 堡垒机 | ★1、对天融信堡垒机TopSAG提供设备1年的原厂维保服务；**（响应文件中提供原厂服务承诺并加盖供应商公章，承诺函格式自拟）** 2、提供1年硬件整机保修服务，在硬件质保期内，对硬件产品整机给予保修； 3、提供1年电话咨询及远程调试服务，在服务期内，由天融信原厂工程师提供电话咨询及远程技术协助服务； 4、提供1年上门现场支持服务，在服务期内，对于采购人使用过程中遇到的问题，如采购人咨询及远程技术协助不能解决，将派遣天融信原厂工程师赴现场解决技术问题，为用户提供现场技术支持。  ★5、每季度需要现场巡检一次，并提供巡检报告。**（响应文件中供应商提供承诺函。）** | 项 | 1 |  |
| 6 | 上网行为管理 | ★1.对深信服上网行为管理AC-1000-E440提供1年软件升级及产品质保服务；**（（响应文件中提供原厂服务承诺并加盖供应商公章，承诺函格式自拟）** 2.提供1年硬件整机保修服务，在硬件保修期内，对硬件产品整机给予保修； 3.提供1年软件升级服务，在软件升级服务期内，对软件内核进行版本升级及更新； 4.提供1年电话咨询及远程调试服务，在服务期内，由经过技术认证的工程师提供电话咨询及远程技术协助服务； 5.提供1年上门现场支持服务，在服务期内，对于采购人使用过程中遇到的问题，如采购人咨询及远程调试不能解决，将派遣经过技术认证的工程师赶赴现场解决技术问题，为采购人进行现场技术支持。  ★6、每季度需要现场巡检一次，并提供巡检报告。**（响应文件中供应商提供承诺函。）** | 项 | 1 |  |
| 7 | 入侵防御 | 提供学校现有IPS设备以下服务（山石网科SG-6000-S2060）**（响应文件中提供原厂服务承诺并加盖供应商公章，承诺函格式自拟）** 1、原厂硬件质保1年； 2、软件免费升级服务1年； 3、IPS特征库免费升级服务1年； 4、AV特征库免费升级服务1年；  5、提供1年上门现场支持服务，在服务期内，对于采购人使用过程中遇到的问题，如采购人咨询及远程调试不能解决，将派遣经过技术认证的工程师赶赴现场解决技术问题，为采购人进行现场技术支持。  ★6、每季度需要现场巡检一次，并提供巡检报告。**（响应文件中供应商提供承诺函。）** | 项 | 1 |  |
| **服务要求：**  **1、响应人的响应文件必须标明所投货物的品牌与参数，保证原厂正品供货。**  **2、应根据采购人的要求进行培训，直到熟练使用。**  **3、响应人免费提供7\*24小时电话或电子邮件服务及7\*8小时现场服务。对于现场服务，谈判响应人须在接到采购人报修，24小时内派遣工程技术人员到达提供现场服务。** | | | | | |

**三、验收**

成交人和采购人双方共同实施验收工作，结果和验收报告经双方确认后生效。