采购（技术及服务）需求

**哈尔滨工业大学VPN系统采购**

1. **采购标的需实现的功能或者目标：**

**通过建设VPN设备，实现目标如下：**

**（1）校园内网资源安全访问：实现安全接入访问校园内网数字化资源，并可结合校内统一认证系统，以身份为中心，远程安全接入平台。**

**（2）图书馆资源无感知访问：实现校外安全访问图书馆资源，解决校外访问电子资源的认证授信问题，支持所有主流操作系统及移动端。**

**（3）运维及敏感资源安全访问：通过SDP、MFA等技术为远程运维人员及敏感资源访问用户提供加密通道限制对运维对象及敏感资源安全访问。**

**（4）内外网统一访问控制：通过VPN系统将内部及图书电子资源访问需求集中至加密隧道，实现 "单点接入 - 全网防护"，收敛攻击面。构建 "连接前认证 - 连接中监控 - 连接后审计" 的全周期信任链，将传统基于 IP 的粗放授权转变为基于身份的精细管控。**

1. **采购标的明细（名称、数量、单位）：**

|  |  |  |
| --- | --- | --- |
| **标的名称** | **数量** | **单位** |
| **VPN系统** | **2** | **套** |

1. **需执行的相关政策合规要求、执行标准和规范要求：**

**提供网络安全产品相关证书**

1. **供应商资格要求**

**需符合《政府采购法》第二十二条要求。（具有独立承担民事责任的能力（法人/组织/自然人）、良好商业信誉与健全财务制度、履行合同所需的设备与技术能力、有依法缴纳税收和社会保障资金的良好记录，前三年内在经营活动中没有重大违法记录。）**

1. **项目技术/服务要求**

**本次采购VPN系统为2套,由2台VPN控制中心,2台VPN代理网关组成**

**（1）VPN控制中心：2台**

**★1.硬件参数：2U机架式设备，接口≥4千兆电口，≥4千兆光口，≥8万兆光口；最大并发用户数≥20000，每秒新建用户数≥2000。VPN集群实配并发接入授权数≥20000。**

**2.集群或主备模式下各节点控制中心的接入授权数可共享使用，单节点控制中心故障后，其设备上的接入授权会自动迁移到其他节点上，总授权数量不变。提供承诺函并加盖投标人公章。**

**3.产品需提供外置零信任分析中心进行交付，提供必要的计算及存储资源，支持安全报表、操作录屏、操作审计、日志存储与查询、基础统计分析、办公报表展示和大屏。提供承诺函并加盖投标人公章。**

**★4.产品须与学校统一身份认证系统进行对接，以实现业务系统的无感单点登录。提供功能截图并加盖投标人公章。**

**5.产品需支持发布web模式资源，支持通过HTTP或HTTPS协议访问业务资源。**

**6.产品需支持在客户端工作台上点击业务应用时，自动启动相应的CS程序，以便运维人员能够直接访问所需的资源，包括不限于浏览器、远程桌面或其他应用。支持主流的操作系统，如Windows、统信UOS、麒麟kylin、macOS等。提供功能截图并加盖投标人公章。**

**7.产品需支持对用户安全性登录配置进行检查，包括但不限于：支持用户登录防爆破、用户首次登录强制修改密码、用户上线风险通知、用户二次认证策略等。提供功能截图并加盖投标人公章。**

**8.产品需支持直接在应用授权管理界面为某个应用或某类应用分配用户授权，授权可以直接授权给用户所在的组织架构、角色或用户。**

**9.产品需支持将长期不登录/不使用的用户帐号识别为闲置帐号并自动锁定，管理员可自定义闲置账号时长阈值。提供功能截图并加盖投标人公章。**

**10.支持应用封装能力，通过封装的应用需支持单点登录功能，可为用户自动填入用户名、账号等信息，实现单点登录。**

**11.产品需支持在管理台查看用户状态，可以识别出存在安全风险的用户，如爆破锁定、异地登录等，可以手动解锁用户。**

**12.产品需支持查看当前在线用户，可以查看用户名、接入IP、组织架构、终端类型、浏览器类型等。**

**★13.控制中心支持实现跨数据中心组建集群的分布式集群功能，以实现通过互联网或内网在多数据中心不同网段下对控制中心数据和配置等进行自动同步。提供承诺函并加盖投标人公章。**

**14. 支持管理员选择是否允许用户通过短信验证码等方式自助找回密码,用户可以在PC端和手机端的登录页面上点击“忘记密码”来进行密码重置。**

**★15.简化原有VPN系统替换流程，自动弹出VPN升级提示并安装,若涉及到定制，应由投标人免费定制直至满足需求。提供承诺函并加盖投标人公章。**

**16.为提升运维人员对设备的维护和问题排查效率，产品需支持在命令面板上内嵌网络配置和排障命令，对网络进行测试以及故障排查。提供功能截图并加盖投标人公章。**

**17.在保障接入安全的前提下，为提高运维人员接入便捷性，支持在达到安全接入要求时为用户配置免除二次认证，支持配置的安全接入要求至少包括：授信终端环境、Windows域环境、自定义网络环境等。**

**18.产品需支持对自身的运行状态和策略配置情况进行巡检，对设备状态进行打分，统计检查的正常项/异常项/告警项，并支持管理员输出巡检报告。提供功能截图并加盖投标人公章。**

**19.与学校网络安全大数据平台对接，数据标准化采用统一日志格式（如 CEF、JSON），包含时间、用户ID、源IP、获取IP、目的IP、操作行为、客户端MAC地址、客户端主机名、资源方位路径等元数据，确保跨系统解析一致性。采用Kafka 等加密通道实时推送日志，防止传输过程中被篡改或窃听。**

**（2）VPN代理网关：2台**

**★1.设备最大加密流量≥1.3Gbps；2U机架式设备，接口数量≥4千兆电口，≥4千兆光口，≥8万兆光口。**

**2.产品需支持首次登录强制修改密码，支持设置密码有效期。**

**3.产品需支持对用户的访问日志进行全面的记录，包括用户、源IP、目的IP、时间、URL、源端口、目的端口、代理端口等。**

**4.支持将VPN流量镜像给学校的网络流量分析系统，提升流量分析效果，增强行为审计溯源能力。**

**5.代理网关部署时支持配置聚合网口，并可以将聚合网口设置为代理网关的网络部署IP地址。**

**6.产品需支持配置同一个IP地址用户连续登录错误超过上限时锁定IP地址，防止暴力破解，并于指定时间后自动恢复。**

**7.产品需支持检查设备的剩余日志空间；支持检查是否配置了虚拟IP。**

**8.产品需支持将接口参数爆破/webshell攻击/扫描/越权调用等非法安全行为事件记录在安全日志中。**

**9.产品需支持对用户安全日志进行提取，包括但不限于：cookie劫持、中间人攻击、帐号安全（包含异常时间/地点/弱密码/爆破/新终端登录）等。**

**10.产品需支持对自身运行状况进行自检，包括但不限于：磁盘空间、内存负载、网卡健康、网卡日志、BIOS固件等硬件相关状态的检测；核心进程状态检测；补丁修复状态等检测。提供功能截图并加盖投标人公章。**

**11.所含设备提供免费质保周期为5年。(硬件质保,软件升级)**

1. **项目实施要求**

**需求分析：明确项目需求和实施目标效果。**

**安装与调试：组织技术人员进行设备的安装和调试，确保设备正常运行。**

**测试与验收：对设备进行全面的测试，确保满足项目需求，并进行验收。**

**项目管理：建立完善的项目管理体系，明确项目进度、质量控制、风险管理等内容。**

**培训：供应商应为采购方提供相关设备的操作培训，确保采购方人员能够熟练使用设备。**

**设备提供免费质保周期为5年。(硬件质保,软件升级)**

**为学校VPN系统顺利割接,厂家须提供原厂工程师驻场45天。**

1. **验收方式**

**合同签订后30个工作日内交付所有功能并接受验收。**

**项目验收须达到如下要求：**

**（1）针对关键技术指标进行全面测试；**

**（2）提供加盖原厂售后服务承诺函，否则不予验收。**

1. **其他技术、服务相关要求。**

**厂家需提供2人/次相关产品本地化培训服务。**