项目概况

序号	内容	说明
1	项目背景	智慧校园经过高校信息化建设的不断摸索，逐渐的发展起来，目前已进入快速发展期。信息技术的飞速发展为高校信息化建设提供了机遇和条件，也不断暴露出很多新问题，如信息孤岛、信息安全等问题导致业务流程不通畅、用户使用不方便、系统应用推广难等等。 在智慧校园建设的过程中，网络安全一直是需要重要关注的方向。2022 年 6 月 22 日，西北工业大学发布《公开声明》称，该校遭受境外网络攻击。陕西省西安市公安局碑林分局随即发布《警情通报》，证实在西北工业大学的信息网络中发现了多款源于境外的木马程序样本，西安警方已对此正式立案调查。由此可见，高校作为国家科研数据研究的重要行业，必将面临国外安全组织的重点攻击。 在该事件中，美国国家安全局 TAO 部门的 S325 单位，通过层层掩护，构建了由 49 台跳板机和 5 台代理服务器组成的匿名网络，购买专用网络资源，架设攻击平台。S321 单位运用 40 余种不同的 NSA 专属网络攻击武器，持续对我国开展攻击窃密，窃取了关键网络设备配置、网管数据、运维数据等核心技术数据，窃密活动持续时间长，覆盖范围广。 由此可见，在使用高级攻击手段如 0day 漏洞等进行攻击时，之前网络安全设备存在被绕过的风险，从而导致内网重要数据被窃取。零信任安全体系作为新一代的“鉴白”安全体系，能够很好的解决该事件中发现的安全问题，也必将成为高校安全体系补充建设的首选。西南大学构建零信任统一接入平台建设势在必行。
2	执行依据	《中华人民共和国网络安全法》（2016.11） GB/T22239-2019 信息安全技术网络安全等级保护基本要求（2019.5）
3	需求分析及项目目标	国家近几年明确了网络安全创新能力的投入，目标构建完善的网络安全体系，聚焦事前防护、事中检测、事后处置、调查溯源等环节需要。而零信任作为“网络安全关键技术”之一，其业务能力栈覆盖从事前防护到调查溯源等环节，在 2019 年工信部《关于促进网络安全产业发展的指导意见》中明确了零信任作为新技术架构的推广的指导意见。对于学校来说，需要建立和保证信息安全的核心目标和安全基线，与零信任中明确业务资源权限、严格控制资源的被访问和授权、收集基础设施当前态势信息理念是吻合的。 （1）内外网全面实现随时随地安全办公：通过零信任架构收缩业务暴露面，避免业务直接暴露在互联网，满足出差、外勤、运维、外包、疫情隔离等利用 PC 端或移动端开展远程办公。不仅能够最大程度降低对用户体验的损害，确保用户能够方便地接入业务，还能有效阻断来自终端的风险，避免远程办公用户成为风险入口。同时，即使用户在学校内部接入办公，也不免存在通过钓鱼等攻击手段，被利用作为跳板进行内网横向攻击，所以内网接入办公也需要实现全面零信任的演进，在不更改现有安全设备部署方式、安全策略设置等要求，最小化改造实现基于身份建立完善的最小访问权限模型，数据中心业务之

		间东西向流量可视可控。 （2）保障访问体验和运维效能：通过零信任架构的落地确保认证更可信，更便捷，访问速度快，性能好，支持大并发场景，技术产品能够全天候无间断工作，确保智慧校园运行的高效、稳定、可靠。同时考虑混合办公涉及大量的用户、终端、组织架构、业务等，能够结合学校自身的流程自动化系统，降低运维管理成本。 （3）全网最小化改动原则实现内部威胁控制：通过内网由传统的 ACL 区域隔离、同区域的授信后自有互访到基于身份的最小权限访问控制，业务东西向隔离，提升整体内部安全，限制数据泄露、病毒传播等危害。最大程度降低境外发起的入侵行为带来的核心数据丢失等网络安全风险。 （4）构建混合办公安全分析中心：依托零信任平台实现全网终端安全可视可控，将当前网络中的安全风险以可视化的方式直观和准入的展示给用户，提供具有可解释、可扩展、可持续优化、灵活的告警信息，通过主动运营和安全服务能力，实现快速定位问题、精准处置风险，以及在事后进行安全加固，进而提升整体安全防护能力。 （5）实现方案的先进性与示范性：以领先的零信任架构理念为建设思路，能够适配安全技术与措施不断演进发展，助力智慧校园安全建设在行业中处于领先示范地位，实现全面零信任架构演进。以此项目使得具有安全制度持续优化改善的机制和办法，能有执行零信任访问架构从规划到落地的全过程能力，构建出细粒度动态授权、策略自动优化的安全访问控制能力。
4	项目内容	1）零信任平台控制中心 1 台，提供包括统一认证、授权、策略管理与下发等功能，提供 8000 个并发授权，为保证一定的冗余度，设备支持并发用户数不低于 12000（个）； 2）零信任平台分析中心 1 套，提供访问行为分析和持续信任评估等能力，提供用户权限报表的统一导出，提供可视化管理平台，日志处理性能 EPS 不低于 3000； 3）零信任组件直连网关 1 台，主要负责内网访问控制，在逃生机制上支持多机热备、硬件 bypass 等特性，具备良好的业务兼容性，对流经的流量可进行解析和检测，具备 IPS 和 WAF 能力，网络层吞吐量不低于 150G，IPS 吞吐量不低于 40G； 4）零信任组件安全代理网关 1 台，主要负责外网访问控制，实现内网业务代理发布、建立可信加密隧道等，加密流量不低于 2.5Gbps，并发用户数不低于 12000（个）
5	项目范围	本次项目建设零信任统一接入平台覆盖西南交通大学全校内外网安全接入场景

采购标的数量

序号	设备名称	单位	数量
1	零信任平台控制中心	台	1

2	零信任平台分析中心	套	1
3	零信任组件直连网关	台	1
4	零信任组件安全代理网关	台	1

本次采购范围，包括以上货物的供应、运输、安装调试、培训及售后服务。具体采购内容及所应达到的具体要求，以本采购文件中商务、技术和服务的相应规定为准。

技术指标、功能需求

序号	名称	详细技术指标及功能需求
1	零信任平台控制中心	1. ★支持最大并发用户数≥12000，本次授权数量≥8000 个；内存≥16G，硬盘≥480GB SSD，电源：冗余电源，接口：千兆电口≥6 个、千兆光口 SFP≥4 个，万兆电口≥2 个。 2. ★控制中心支持与学校现网的金智统一身份认证平台进行认证登录对接且中标后用户将保留测试权利。（供应商提供承诺函原件并加盖供应商公章） 3. 支持主从式本地集群、分布式集群。 4. ●支持通过桌面悬浮球的方式，用户可一键切换内网或互联网。（提供现场演示/录播视频演示该功能） 5. 支持 IP 和端口级的应用配置，用户对不同 IP 发布相对应的应用。 6. 支持设置代理方式，隧道模式 和 WEB 模式。 7. ▲支持主流国产硬件 CPU 和国产操作系统，包括但不限于麒麟 V10×龙芯、麒麟 V10×龙芯 LoongArch、麒麟 V10×飞腾、麒麟 V10×鲲鹏、麒麟 V10×兆芯、麒麟 V10×海光、麒麟 V10×海思麒麟；统信 V20×龙芯（3A3000、3A4000）、统信 V20×龙芯（3A5000）、统信 V20×飞腾、统信 V20×鲲鹏、统信 V20×海光、统信 V20×兆芯等。（要求提供国产操作系统与零信任厂商兼容性证明） 8. ▲提供内置攻击工具进程黑名单，可基于内置的黑名单进行增减，黑名单进程可直接被引用，用于策略配置。（提供产品功能截图，并加盖投标人公章） 9. 支持 Android、iOS 的自带浏览器访问 WEB 资源，支持国产操作系统浏览器接入并访问 WEB 资源。 10. ▲支持与企业微信、钉钉等主流 APP 对接，实现与在企业微信或钉钉工作台上发布的 H5 微应用单点登录。（提供产品功能截图，并加盖投标人公章） 11. 支持设置用户与授信终端绑定。 12. 支持以下认证方式：本地账号密码认证、LDAP/AD 认证、OAuth2.0 标准协议的票据认证、CAS 标准协议、票据认证、证书认证、HTTP(S)短信认证、腾讯云短信网关、阿里云短信网关、标准 Radius 令牌认证、本地 OTP 动态令牌认证等认证方式、与企业微信、阿里钉钉、飞书结合实现扫码认证、通过飞书用户或个人微信企业号通过 H5 接入。 13. 支持在登录上线后，持续、动态检测终端环境安全，不符合后注销用户或锁定用户，便于及时定位并响应终端威胁。 14. ▲支持免辅助认证。用户勾选信任浏览器后，在该浏览器下有效期内不需

		要进行辅助认证。有效期时长可设置 1-90 天。（提供产品功能截图，并加盖投标人公章） 15. 支持提供开放的 API，管理员可在控制台创建 API KEY，供第三方安全设备或单位自有安全分析平台对接，便于形成统一的安全体系。 16. ▲支持终端进程采集、自定义可信进程、进程信息可视、基于可信应用的访问控制策略。（提供产品功能截图，并加盖投标人公章） 17. 支持动态访问控制策略，可根据用户、应用配置规则使用范围，可基于 Windows、macOS、Linux、iOS、Android、麒麟、统信等操作系统单独配置策略 18. ▲为保证零信任产品的架构规范性，提供第三方检测/测评机构颁发的针对零信任 SDP 设备检测内容的相关认证证书。（提供相关证明材料，并加盖投标人公章） 19. ▲为保障产品的自身安全性，提供第三方检测/测评机构颁发的针对零信任系统检测内容的安全众测无漏洞证明文件或证书。（提供相关证明材料，并加盖投标人公章）
2	零信任平台分析中心	20. ★平台日志处理性能 EPS≥3000。 21. ▲支持告警适用对象可配置适用用户、排除用户、适用应用等条件。（提供产品功能截图，并加盖投标人公章） 22. 告警处置方式支持用户告警提示、用户下线、账号锁定等，系统内置不少于 5 个用户告警提示内容模板，允许管理员对告警内容进行自定义。 23. 支持告警列表，可展示已有告警策略的整体触发情况和具体详情，内容包括但不限于告警名称、处置状态、策略类型、告警条件类型、告警时间、用户名、组织结构、群主、IP 地址、终端名称、操作系统、授信状态、应用名称、应用服务器地址、处置人等。 24. ▲支持组织安全地图，可基于组织机构视角进行风险可视，查看特定组织架构内的用户数量、告警数量、告警处置情况。（提供产品功能截图，并加盖投标人公章） 25. ▲支持显示总体各应用的权限使用情况，并根据实际访问用户数、权限使用率进行排序。显示内容包括：应用名称、应用类型、访问模式、授权用户数、实际访问用户数、权限使用率、闲置权限数等。（提供产品功能截图，并加盖投标人公章） 26. 支持用户行为轨迹，记录用户访问过程，内容包括但不限于时间、操作者、操作行为、操作对象、客户端源 IP、IP 归属地、操作结果等。 27. ▲支持关键字搜索，可根据关键字对所有日志内容进行关键字搜索，快速定位安全问题。（提供产品功能截图，并加盖投标人公章） 28. 支持风险用户排行，可对 TOP5 的风险用户进行排行展示，内容包括但不限于用户名称、组织架构、告警概况、告警数量、处置情况等。 29. 支持告警排行，可对 TOP5 的告警进行排行展示，内容包括但不限于告警数量和告警名称。 30. 基于用户、终端、资产、访问行为的原始日志和风险告警，快速响应事中风险，事后的轨迹追溯和审计，实现安全风险的数字化，风险可视可控，不断闭环。
3	零信任组件直连网	31. ★网络层吞吐量≥150G，应用层吞吐量≥55G，IPS 吞吐量≥40G，并发连接数≥3500 万，HTTP 新建连接数≥120 万；内存≥192G，电源：冗余电源，

	关	接口：千兆电口≥8 个、千兆光口 SFP≥8 个、万兆光口 SFP+≥8 个。 32. 支持链路连通性检查功能，支持基于 3 种以上协议对链路连通性进行探测，探测协议至少包括 DNS 解析、ARP 探测、PING 和 BFD 等方式。 33. 支持多维度流量控制功能，支持基于 IP 地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求。 34. ▲为保证识别勒索访问流量，要求支持勒索软件通信防护功能。（提供具备 CMA 或者 CNAS 认证的第三方机构出具的产品检测报告，并加盖投标人公章） 35. 持对不少于 9000 种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。 36. ●要求产品内置不低于 10000 种漏洞规则，支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持 CC 攻击防护功能。（提供现场演示/录制视频演示该功能） 37. 支持应用控制策略有效性检测，及时发现如策略冲突、策略生效时间过期、策略未匹配情况，保障策略持续优化。 38. ▲支持从零信任控制中心平台接收认证前应用管理配置，包括是否开放应用、开放的应用端口、是否全部开放等。（提供产品功能截图，并加盖投标人公章） 39. ●支持僵尸主机检测功能，内置僵尸网络特征库超过 128 万种，可识别主机的异常外联行为。（提供现场演示/录制视频演示该功能） 40. 接收零信任控制中心下发的用户管控范围、认证地址，实现用户认证、准入等操作；通过设置安全策略，实现内网隐藏；上报内网访问应用日志、安全日志到零信任分析中心平台供分析等。 41. ●为防止外区域恶意流量攻击，要求支持针对多个区域实现批量快速管控恶意流量的功能。（提供现场演示/录制视频演示该功能） 42. 针对终端安全风险汇总展示，按照已失陷、高风险、中风险、低风险不同等级展示内网终端整体安全状况，并给出解决建议实现风险快速处置。 43. ▲为保障用户账号安全，要求产品支持账号安全保护功能，提供国家版权局颁发的软件著作权证书。（提供证书，并加盖投标人公章）
4	零信任组件安全代理网关	44. ★加密流量≥2.5Gbps，最大并发用户数≥25000，https 并发连接数（个）≥200000,https 新建连接数(个/秒)≥3000;内存≥32G,硬盘≥480GB SSD,电源：冗余电源，接口：千兆电口≥4 个、千兆光口 SFP≥4 个、万兆光口 SFP+≥4 个。 45. 支持单臂模式、路由模式部署。 46. 支持接入 IP 限制，从浏览器、SSH 或 SNMP 等方式接入管理台时，都必须在上述 IP 白名单范围内接入。 47. ▲支持首次登录强制修改密码，支持配置密码最长使用周期。（提供产品功能截图，并加盖投标人公章） 48. ▲支持开启 SSH 进行远程运维，且开启后会定期关闭 SSH，以免运维人员进行远程运维后，忘记关闭 SSH，带来潜在风险。（提供产品功能截图，并加盖投标人公章） 49. 支持配置邮箱服务器，告警事件支持邮件通知管理员。 50. 支持当前设备配置自动同步、支持从备份配置中恢复。 51. 支持常规的网络配置和排障命令，方便运维人员对设备进行维护，网络测

		试以及故障排查。

服务要求

序号	服务要求项目	指标符号	服务要求标准
1	技术文件	★	应提供全套、完整的书面技术资料，包括仪器说明书、操作手册、简单维修说明等。
2	设备安装、调试和验收	★	在合同生效后应向用户提供详细的安装要求并提供技术咨询；设备到达用户所在地，在接到用户通知后一周内进行安装调试，直至通过验收。
3	技术培训	★	供应商应提供完整的培训服务，包括内容、人员、时间、地点、频次等。在用户所在地对设备使用者进行设备操作和维护进行培训，使被培训人员达到能够熟练使用。
4	投标人服务标准	★	投标人承诺所有硬件不少于三年保修、厂家自主软件三年保修升级。

说明：★代表实质性指标，不满足该指标项将导致投标被拒绝。

商务要求（实质性要求）

（一）履约时间：第一期付款后 30 天内交货。

（二） 履约地点：西南交通大学犀浦校区图书馆 B145。

（三）付款方式：1.分期付款

第一期：合同生效且供应商提交履约保证金后，预付合同金额的 20%；

第二期：项目验收合格后，支付合同金额的 80%。

2. 每次付款前，供应商应出具等额增值税普通发票，发票与合同的银行账户信息应保持一致。

（四）验收方法和标准：

1、货物到达现场后，供应商应在采购人在场情况下当面开包，共同清点、检查外观，作出验货记录，双方签字确认后开始安装调试。

2、中标（成交）供应商应保证货物到达采购人所在地完好无损，如有缺漏、损坏，由供应商负责调换、补齐或赔偿。

3、中标（成交）供应商应提供完备的技术资料、装箱单、授权文件或生产厂商提供的原厂正品出货证明材料（非装箱清单组成材料）等，并派遣专业技术人员进行现场部署调试。验收合格条件如下：

（1）产品技术参数与采购合同一致，性能指标达到规定的标准；

（2）产品技术资料、装箱单、授权文件等资料齐全；

（3）在产品（系统）试运行期间所出现的问题得到解决，并运行正常；

（4）在规定时间内完成交货并验收，并经采购人确认。

4、产品在部署调试并试运行符合要求后，才作为最终验收。

5、采购人对供应商交付的产品（包括质量、技术参数等）进行确认，并出具书面验收意见。