采购需求（01 包）

一、业务需求

以网络安全法、党委（党组）网络安全责任制和等级保护 2.0 为标准真正打造一套适应未来教育行业网络安全需求、覆盖等级保护 2.0 和网络安全法的各项要求，具备高水平网络安全治理（风险治理、资产治理、漏洞治理等）能力，建立以计算环境安全为基础，以区域边界安全、通信网络安全为保障，以安全管理中心为核心的信息安全整体保障体系，更加注重全方位主动防御、动态防御、整体防控和精准防护，最终提升对网络攻击预判和主动防御能力，防患于未然。保障业务和信息系统高效、准确、安全、稳定和持续运行，促进学校信息化长期稳定发展，为学校信息化提供可持续发展的信息网络安全技术和管理支撑。

通过持续加强网络安全保障体系建设，显著减少来自内外网的安全威胁、进一步保护数据安全、提升教学与学习体验、提高网络安全管理效率，有助于构建一个安全可信赖的数字化学习和工作环境，为高校的发展和创新提供有力的支撑。具体业务需求如下 ：

1、部署智能流量调度硬件设备，将校园网边界组网方式“由串改并”，形成更加安全的设备资源池，实现流量调度和流量编排等智能服务链。

2、部署零信任网关设备，替换现有的 SSL VPN 设备。通过身份持续动态认证和授权，提升数据保护水平，增强远程访问安全性。

3、部署流量分析及管控硬件设备。

4、升级网站群平台，增加或完善用户登录、密码校验、系统日志、敏感信息处理、非法链接检测、安全运维监控等平台功能。

采购清单

产品类型	产品名称	数量
网络与安全硬件	智能流量调度系统	1
网络与安全硬件	零信任解决方案	1
网络与安全硬件	流量分析及管控系统	1
软件及信息技术服务	网站群平台升级改造	1

二、技术指标要求

①指标按重要性分为“★”、“#”和“△”。★代表实质性指标，不满足该指标项将导致投标被拒绝，#代表重要指标，△则表示一般指标项。

②“证明材料要求”项填“是”的，投标人须提供包含相关指标项的证明材料，证明材料可以使用制造商官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖投标人公章，未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。

③除需求中明确要求投标人承诺的事项外，其他要求提供证明材料的指标中，提供投标人承诺作为应答的不予认定。

2.1 智能流量调度系统

序号	重要性	指标项	指标要求	证明材料要求
1	★	硬件参数	10GbE SFP+ 端口数≥48，并配置光模块； 40GbE QSFP+ 端数≥6，并配置光模块。	是
2	#		交换容量≥1.2Tbps； 包转发率≥1024Mpps； 冗余电源、冗余风扇。	否
3	#		内置服务链控制器,集成在系统中，内置相关一条智能服务链授权。	否
4	#		支持扩展外置控制器,双转发设备统一管控,实现单链双转发设备 HA 模式。	是
5	#	服务链功能	支持扩展控制器集群功能,支持多区域、多数据中心服务链统一管控； 支持图形化界面展示，包括转发设备的基础信息和当前流量策略的展示，服务链物理拓扑的展示；支持生成统计分析报表，包含服务链和服务节点的吞吐量、包速率等内容； 支持非对称服务链（自定义编排上/下行安全设备设备流量路径）模式，在此模式中，上行流量拓扑和下行流量拓扑可独立自由编排（如下行流量先经过安全设备，再经过功能设备；上行流量亦先经过上述安全设备，再经过功能设备）。	是
6	△		支持服务割接功能，服务节点 ON/OFF 开关一键上/下线。	否
7	△		支持服务编排功能，鼠标拖拽方式编排服务节点顺序。	否
8	△		支持服务映射功能，二到四层流量分类，引导不同流量经过不同服务节点。	否

9	△		服务映射支持 IPv6 策略，可基于 IPv6 地址进行流量分类。	否
10	#		单条服务链中可支持服务节点的 HA 功能，HA 组内的一个服务节点出现故障，另一个服务节点可自动接管相应流量； 可扩展支持服务链间的 HA 功能，当一条服务链中的服务节点出现故障，另一条服务链对应的服务节点可自动接管相应流量。	是
11	△		支持服务链流量镜像功能，包括服务链上行端口流入、流出方向，下行端口流入、流出方向，以及上述四个方向流量的任意组合。	否
12	△		支持服务节点流量镜像功能，包括服务节点上行端口的流入、流出方向，下行端口的流入、流出方向，以及上述四个方向流量的任意组合。	否
13	#		支持服务链流量阻断功能，匹配相关策略流量进行流量阻断； 支持服务链流量直通功能，匹配相关策略流量内外网直通； 支持服务节点直通策略，匹配相关策略流量跳开本服务节点。	是
14	△		支持接口、ICMP、丢包、模拟流量检查功能，服务节点异常自动下线；	否
15	△		支持基于 WEB 页面进行管理，支持导入和导出配置文件，实现快速配置恢复；	否
16	△		支持事件等级，事件分类，事件标签将不同告警进行有效区分。	否
17	#		支持多种自定义报警机制，用户可绑定用户微信、企业微信、钉钉、邮件、SYSLOG 获取实时自定义报警信息。	是
18	#	产品商务要求	相关产品通过信息技术应用创新产品适配性测试，并提供证书复印件（相关产品必须为本次所投产品，同时产品名称需包含 “服务链”、“流量调度”、“流量编排”、“流量汇聚”、“包代理”等关键字之一，否则视为无效）。	是
19	#		相关产品通过国家网络与信息系统安全产品质量监督检验中心的检测（相关产品必须为本次所投产品，同时产品名称需包含 “服务链”、“流量调度”、“流量编排”、“流量汇聚”、“包代理”等关键字之一，否则视为无效）。	是
20	#		智能流量调度系统提供相关产品软件著作权证书、提供相关证书（相关软件必须为本次所投产品，同时产品名称需包含 “服务链”、“流量调度”、“流量编排”、“流量汇聚”、“包代理”等关键字之一，否则视为无效；）。	是

2.2 零信任解决方案

序号	重要性	指标项	指标要求	证明材料要求

零信任控制中心				
1	★	硬件要求	100/1000MBase-T 端口数≥6； 千兆 SPF 光口数≥4，且配置光模块； 万兆 SPF+光口≥2，且配置光模块； 电源：交流冗余电源。	否
2	★	性能要求	最大并发≥12000； 新建用户数≥280/s； 用户授权数量≥10000 个。	否
3	△	网络部署	支持 IPV4/IPV6 双栈网络 IP 配置，可自主选择配置 LAN 口或 WAN 口；支持默认限制所有 IP 通过 WAN 口访问系统，支持通过配置 IP 白名单的方式来放通 WAN 口接入的特殊需求。	否
4	#	隧道资源发布	支持隧道模式，可以基于 TCP、UDP、ICMP 等协议代理访问业务资源，支持发布 IP、IP 范围、IP 段、具体域名及通配符域名等形式的服务器地址，满足常见办公业务的代理，收缩业务暴露面。支持同一个资源发布多个服务器地址；可自主选择优先使用长连接或短连接进行业务代理。提供截图证明并加盖制造商公章。	是
5	#	WEB 资源发布	支持基于 http 或 https 协议代理访问业务资源，支持发布 IP 或域名形式的后端服务器地址，可配置业务应用的具体访问 URL 路径。 后端服务器地址需支持多地址配置；WEB 应用的前端访问地址应支持多地址访问。存在前置代理设备的场景，支持从 XFF 字段获取源 IP；支持通过域名+URL 路径发布和授权应用；支持将 WEB 应用以免认证的形式发布，并且支持对免认证的 IP 地址进行限制，只允许指定 IP 免认证访问。提供截图证明并加盖制造商公章。	是
6	#	应用打开方式	支持配置点击工作台的业务应用即可直接拉起对应的 CS 程序进行访问，包括但不限于浏览器、远程桌面或其他指定程序，支持 Windows、macOS、统信 UOS、麒麟 kylin、Ubuntu 等主流操作系统；针对 Windows 系统，还应支持拉起 CS 应用时携带启动参数，自动访问管理员设定的地址。提供截图证明材料加盖制造商公章。	是
7	△	支持细粒度的资源发布	为有效抵御恶意软件和有针对性地攻击，WEB 资源发布时应支持到 URL 路径级别，且支持配置 URL 路径规则。黑名单模式下，用户只能访问不在黑名单内的路径；白名单模式下，用户只能访问白名单内的路径。且为了简化管理员配置，URL 黑白名单还应支持 * ？ 等通配符配置。	否
8	#	私有 DNS 解析	支持以私有 DNS 发布资源，无需额外购买 DNS 服务即可使用域名访问内网资源，支持管理员自主配置是否允许从具体网络区域（局域网/互联网）接入时使用此私有 DNS 解析地址。需提供产品功能截图及第三方权威检测机构出具的带 CNAS 标识的检测报告证明并加盖制造商公章。	是
9	△	应用授权	为方便维护人员管理应用权限，支持直接在应用授权界面为单一应用或某个应用分类分配用户授权，授权方式支持直接授权给用户所在的组织架构、用户关联的角色或用户	否

			本身，并展示应用直接授权的组织架构、授权角色或用户数量。	
10	△	应用访问权限自助申请	为符合单位合规性要求，管理员可自主编辑用户访问未授权应用时的告警内容；支持配置是否允许用户自助申请应用访问权限，启用后，管理员可以在控制台根据审批状态查看应用申请详情，包括但不限于：申请时间、用户名、所属组织架构、角色、应用名称、应用访问地址、申请理由、申请有效期等。应用管理员可对待审批的应用进行批准或驳回操作，支持批量操作。	否
11	△	浏览器兼容性	为了不改变用户原有使用习惯，保障用户的使用体验，需支持以下主流浏览器访问 WEB 资源： 1、支持 IE11 版本浏览器访问 WEB 资源； 2、支持 Chrome 78 及以上版本访问 WEB 资源； 3、支持 Edge、Firefox、Opera、Safari 等其他主流浏览器访问 WEB 资源； 4、支持微信内置浏览器、钉钉内置浏览器访问 WEB 资源； 5、支持 Android、iOS 各大手机厂商的自带浏览器访问 WEB 资源； 6、支持国产操作系统浏览器接入并访问 WEB 资源。	否
12	#	客户端国产终端兼容性	为了保障用户在国产化终端上的正常业务访问，零信任客户端应兼容主流国产硬件 CPU 的国产操作系统终端，需提供国产操作系统与零信任厂商的兼容性证明，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。提供相关兼容性证明材料加盖制造商公章。	是
13	#	VPN 客户端平滑升级	为方便用户快速切换使用新的远程接入方式，应支持直接用户在打开原 VPN 客户端时直接升级成零信任客户端来登录访问业务，管理员可以自行通过配置决定升级完成后是否卸载原 VPN 客户端，制造商出具承诺函加盖公章	是
14	△	内网 DNS 解析能力	内网 DNS 解析能力：应支持管理员自行配置内网 DNS 解析，以实现终端用户在零信任客户端登录后可以使用单位自建的内网 DNS 进行域名解析。支持配置内网 DNS 解析的域名白名单实现仅部分指定域名才能使用内网 DNS 解析，并支持额外排除部分域名地址。	否
15	#	CDN 接入及访问全局优化	支持配置企业的 CDN 作为零信任客户端下载地址，支持获取 CDN 加速前的访问 IP，并在日志中记录此 IP 为客户端 IP。需提供产品功能截图及第三方权威检测机构出具的带 CNAS 标识的检测报告证明并加盖制造商公章。支持优化 TCP 协议，增强隧道抗丢包、抗抖动特性，实现弱网环境的访问加速。支持将短隧道资源新建连接耗时优化至 ORTT，需提供产品功能截图，加盖制造商公章。	是
16	△	支持不同平台的终端同时在线	支持不同平台的终端同时在线，管理员可分别设置可同时在线的 PC 或移动终端个数，配置范围不小于 0-1000，当超过终端个数时，可以注销最早登录的终端，且被注销的终端有对应的注销提醒；管理员可设置允许终端在线数为	否

			0，以禁止用户通过此类终端接入访问。	
17	#	客户端自动选路	支持时延优先的选路模式，首次接入时客户端以最低时延线路接入访问业务，后续客户端进行周期性探测线路时延，可切换后智能切换至当前最优时延的线路上。多网关接入访问业务的场景，可以设定一个相对时延阈值，首次接入时客户端可在最低时延+相对时延阈值的范围内随机选择网关线路接入。后续客户端进行周期性探测线路时延，可切换后智能切换至当前最优时延的线路上。需提供产品功能截图及第三方权威检测机构出具的带 CNAS 标识的检测报告证明，加盖制造商公章。	是
18	#	多因素认证	为了进一步保障用户身份安全，需支持多因素认证，支持管理员结合已对接的主认证和辅认证类型进行设置，可自由选择采用首次认证+二次认证+终端认证+增强认证等方式。	是
19	#	自适应认证	为强化系统认证安全性，可配置在触发异常环境的条件时，用户需完成增强认证才可登录。可配置的异常环境包括但不限于：帐号首次登录、帐号在该终端首次登录、账号在该地点首次登录、账号在新地点登录、账号在非常用地点登录、闲置帐号登录、弱密码登录、异常时间登录等。需提供产品功能截图及第三方权威检测机构出具的带 CNAS 标识的检测报告证明并加盖制造商公章	是
20	△	默认登录认证方式	为使登录快速便捷，支持指定一个认证来源为默认登录认证方式，用户在登陆时，不需要选择认证方式，默认使用该认证服务器作为认证登录，便于用户快速登录，提升用户体验	否
21	△	单点登录	支持帐号密码代填的单点登录功能，支持智能识别登录页面的用户名和密码输入框，	否
22	#	动态业务访问控制	支持配置动态访问规则，可配置化的 ACL 规则引擎，可以灵活地将终端环境、用户身份、处置动作等进行配置，需提供产品功能截图及第三方权威检测机构出具的带 CNAS 标识的检测报告证明并加盖制造商公章。	是
23	#	CDN 接入能力	支持配置企业的 CDN 作为零信任客户端下载地址，以降低设备本身的非业务访问带宽压力，支持获取 CDN 加速前的访问 IP，并在日志中记录此 IP 为客户端 IP。需提供产品功能截图及第三方权威检测机构出具的带 CNAS 标识的检测报告证明并加盖制造商公章。	是
24	#	服务隐身	支持提供单包授权能力，支持 UDP+TCP 组合的单包授权技术，安全码支持共享码、一人一码和一次一码等多种模式，支持短信分发安全码。可以阻止用户登录上线并产生安全告警，可配置一次一码模式的 SPA 服务隐身机制，提供截图证明并加盖厂商公章。	是
25	#	虚拟 IP	支持以虚拟 IP 方式，访问真实的业务系统，以配合其他对 IP 有要求的安全设备工作，支持共享虚拟 IP 池模式，为用户组分配一个 IP 地址段；支持独享虚拟 IP 模式，可配置一个独享 IP 池，在独享 IP 池中为用户分配指定的虚拟 IP 地址，在独享资源池中给用户绑定的虚拟 IP 不会释放。支持当虚拟 IP 池分配超过一定比例时，零信任可向管理员发送邮件告警，此比例可由管理员自主配置。需提供产品功能截图及第三方权威检测机构出具的带 CNAS 标	是

			识的检测报告证明。	
26	△	终端诊断工具	支持终端环境诊断排查，提供终端诊断工具，支持对当前终端的基本环境进行扫描和一键修复。	否
27	#	账号安全检查	支持疑似管理员测试帐号的残留检查；支持是否开启找回密码功能检查；支持疑似用户测试账号的检查。提供截图证明材料并加盖厂商公章。	是
零信任代理网关				
28	★	硬件要求	100/1000MBase-T 端口数≥4； 千兆 SPF 端口数≥4，并配置光模块； 万兆 SFP+端口数≥8 个，并配置光模块。	否
29	★	性能要求	吞吐量≥2.5Gbps； 最大并发用户≥25000； 最大 https 并发连接数≥20 万； https 新建连接数≥3000/s。	否
30	★	产品匹配	零信任代理网关必须与零信任控制中心为统一品牌并配套使用。	否
31	△	管理员帐号	1、支持新增/删除/修改管理员账号 2、支持管理员的随机密码 3、支持配置管理员过期时间和账号状态	否
32	#	管理员分级分权	支持新增/删除/修改管理组，内置审计管理员、安全管理员、系统管理员等管理组；通过管理组管理权限的配置，实现管理员分级分权。管理组支持按控制台模块分配权限，支持对模块配置[只读]、[完全控制]两种权限。提供证明截图材料并加盖制造商公章。	是
33	#	支持全面的日志记录	支持用户访问日志（用户、源 IP、URL、时间、get 请求、post 请求、端口）；支持管理员操作日志（含管理员、接入 IP、时间、管理行为、对象）；支持用户安全日志提取，审计中心应将具有异常登录行为的用户日志自动打标签为用户安全日志，用户安全日志包括但不限于：帐号安全（应包含帐号首次登录、异常时间登录、非常用地点登录、弱密码登录、爆破登录、闲置帐号登录、帐号在新终端登录等）、中间人攻击、SPA 安全（应包含 SPA 端口扫描、SPA 爆破攻击、SPA 敲门伪造、SPA 重放攻击、SPA 安全码泄漏等）、cookie 劫持等；支持将设备安全事件单独记录在设备安全日志中，事件类型包括但不限于：接口扫描、接口 webshell 攻击、接口参数爆破、接口越权调用等设备 API 防护日志。	是
34	#	流量镜像	支持将用户访问零信任系统的WEB资源访问流量解密后镜像给外部网络流量分析系统，如态势感知等设备，以完善系统的用户行为审计溯源能力，提升设备自身的安全性。	是
35	△	系统运维与设备安全	支持提供 SNMP 服务来对接运维监控设备，可在控制台下载 MIB 库，支持独立配置 SNMP 外发服务器地址。支持配置同 IP 用户连续登录错误超过上限时锁定 IP，并于指定时长后自动恢复	否

36	#	设备巡检报告	支持对设备自身的安全状态和策略配置进行巡检，对设备的整体状态进行打分，统计所有检查的正常项、异常项和告警项，并输出巡检报告，支持在设备上查看及下载巡检报告，报告应至少包含检测项、检查状态、存在的问题描述、建议改进措施等。	是
37	#	设备稳定性检查	应支持系统黑匣子及核心进程的状态检测。应支持 CPU 负载、内存负载、磁盘空间、网卡健康、硬盘健康、网卡日志、BIOS 固件等硬件相关状态的检测。应支持软件版本及补丁修复状态等检测。提供截图证明材料并加盖厂商公章。	是
38	#	设备管理端口安全检查	支持远程运维 SSH 端口开启检查；支持控制台接入 IP 限制情况检查；支持 SNMP 指定 IP 地址接入检查。	是
39	△	设备状态	支持查看当前设备运行状态，	否
40	#	产品资质	提供国家密码管理局商用密码检测中心出具的含有“访问控制系统”或“SDP”字样，符合 GM/T 0024 标准或 GM/T 0025 标准要求，以及符合 GM/T 0028《密码模块安全技术要求》第二级的《商用密码产品认证证书》。	是
41	#		提供国家版权局颁发的含有“主动防御”字样的《计算机软件著作权登记证书》。	是
42	#		为保障产品接入互联网的安全合规性，所投零信任产品型号应提供由工信部颁发的《电信设备进网许可证》	是

2.3 流量分析及管控系统

序号	重要性	指标项	指标参数	证明材料要求
1	★	性能要求	吞吐量≥40Gbps； PPS（包转发率）≥1000 万。	是
2	★	配置要求	GE 电口数≥2； SFP 千兆光口≥4，并配置光模块； SFP+万兆接口≥4，并配置光模块； QSFP+40G 接口≥2，并配置光模块。	是
3	△	工作模式	支持透明网桥模式，支持路由模式，支持 NAT 模式，支持旁路分析模式，支持路由、NAT、网桥和旁路分析的混合模式。	是
4	△	协议识别能力	支持对 2～7 层流量的识别能力，能够识别主要应用协议，并逐级细分 P2P 下载、网络视频、网络电话、游戏、HTTP 协议的子类别和具体客户端名称，比如 HTTP 协议---Web 视频---土豆、网络游戏---移动游戏等；支持国内各类常见协议≥1000 种，其中大型游戏≥300 种，移动 APP 应用≥30 种，现网协议识别率 ≥95%。	是
5	△	流量可视化管理	可提供整个系统、各链路的流量和连接数统计图表；可提供近 10 分钟流量、累计流量、并发连接数统计图表； 支持 TOP 应用、用户排序。	否
6	△	会话日志	系统支持会话日志，包含设备编号、接口、访问时间、源地址、目标地址、NAT 地址、账号信息、域名、协议类型、7 层协议名称、流量、运营商、地理位置等元素。同时采用	是

			1:1 的日志输出，完整保留网络中的相关信息。	
7	△	校内图书馆资源查询	对校内用户访问校外图书馆资源进行统计，提供对图书馆资源流量和下载排名，为我校购买图书馆资源提供依据；对校内用户下载校外图书馆次数作统计，提供下载排名，发现恶意下载用户。	是
8	#	内容分析	支持网络贷、邪教网站、虚拟货币用户访问、使用分析及用户信息查询；可以统计网内用户使用的终端类型数目，终端使用分布、终端操作系统种类及数量。	是
9	#	IPv6 流量可视化	提供整个系统 IPv6 流量分别和连接分别统计图表,可以查看 IPv6 协议占整体流量比例；IPv6 最近一天、最近一周和最近一月的流量趋势图表，各协议组的当前速率、连接数等统计信息及条件排序。	是
10	#	网络应用性能监测	1、对网络中各种应用的时延进行检测，各种协议时延要求包括客户时延、服务时延、应用时延等； 2、支持用户导入本地资产备案名单文档；支持根据流量分析结果与用户导入的备案文档进行对比，自动分析出可信资产、灰色资产以及黑色资产；支持查看用户自有资产信息，包括：域名、服务器地址、群组名称、访问次数、上下行流量以及总流量等；支持资产域名所在区域以及访问量查询。	是
11	#	运维大屏展示	对网络各类应用时延，例如：网页时延、DNS 时延、社交时延、邮箱时延等进行动态监控，发现网络延时异常用户、应用等情况； 提供 TOP 域名、域名差量分析；DNS 重度用户、重度服务器分析；提供常用端口异常应用分析、文件下载分析等。	是
12	#	PPPoE 代拨功能	支持 PPPoE 代拨和 IPoE 代拨等多种代拨模式。	是

2.4 网站群平台升级改造

序号	重要性	指标项	指标要求	证明材料要求
1	★	整体要求	本项目需要基于现有网站群系统平台上进行平滑升级。包括功能优化、系统改造、数据迁移、使用培训等，提供对原有网站的文章、附件、视频、图片等格式的数据迁移服务。并完成相关系统对接、集成部署，数据迁移与整合、培训等。	是
2	★	运行环境要求	（1）平台需采用微服务架构，支持分布式集群，具有跨平台、跨数据库的通用性和移植性； （2）支持本地化部署；支持集群部署、管理机与发布机的分布式部署、物理隔离部署和远程分离式部署等多种部署方式； （3）支持麒麟、统信、龙蜥、欧拉等国产操作系统；支持海光、飞腾、鲲鹏、龙芯等信创硬件环境，以满足学校的部署需求； （4）支持 Oracle、SQL Server、MySQL 等关系型数据库和 Kingbase ES（人大金仓）、DM（达梦数据库）、GBase（南大通用）等国产数据库；支持 Tomcat、Apache、金蝶、东	是

			方通等多种中间件。	
3	#	系统升级要求	（1）升级现有系统的功能模块，增加智能审核、纠错、脱敏功能，加强信息监管。增加“三审三校”、错别字监测、敏感信息扫描和脱敏处理等功能。完善信息的审核流程，强化网站内容发布前的监管审核，增加内容纠错和自动提醒功能；开放敏感词库接口，可定期对敏感信息批量更新。 （2）增加文章审核中心入口；支持流程管理，内嵌简单流程；文章日志中展示推送来源日志；支持可视化模板引用功能；支持可视化模板复用功能。 （3）提供统一的图片资源管理，支持全院各部系/部门图片资源共享，为授权用户进行查看和使用。支持批量上传、下载、移动、复制图片到指定目录功能；支持按标签、评分、类型、大小、日期等不同维度进行筛选；支持图片批量管理功能，如归档、收藏、下载、删除。 （4）提供专业的流媒体管理系统，包括多种格式的视频文件上传、转码、管理、播放等，支持视频总览，支持视频库最新视频文件的封面/标题、标签、部门、用户、创建时间等，授权用户可进行视频分类管理下载、编辑、复制链接引用等；提供视频文件的快速检索。 （5）完成现有网站历史文章的信息安全检测、整改，清除安全隐患。升级改造完成后，通过大数据、自然语言处理、知识图谱等技术,对全校外部网站已发布的内容进行信息安全扫描检测，有效防范因文本错敏引发的各类问题。 （6）提供二次开发 Web service 接口，便于学校进行二次开发、功能扩充以及与其它信息系统的整合。 （7）提供全面的系统安全策略实施，包括系统完善的用户及权限管理、用户身份认证策略以防非法用户入侵。 （8）系统必须具备安全性、易用性、可操作性强，操作流程清晰简洁，用户界面美观大方。 （9）所有系统须符合国家软件工程、信息系统工程最新标准或规范，符合学校信息编码标准，数据接口等要向用户全面开放。 （10）易于安装和维护，运行质量高，开放性好，便于移动、扩展。	是
4	#	安全要求	投标人应能够提供多种安全防护和入侵监测报警服务，提供从平台环境、内容采编发、内容安全监测、用户登录、认证加密、传输协议、系统保障、安全访问、防 SQL 注入、网页防篡改、前后台数据加密等多种安全措施、产品及服务，满足信息安全等级保护综合管理相关要求；包括但不限于：防 SQL 注入、网页防篡改、网络监控、用户认证、安全访问等，全面提升网站管理效率，优化网站访问速度，保障全校网站的高质量运行。	是
	#	性能要求	Web 发布服务器在并发用户数≤200 时，页面响应≤1 秒；	是

5			系统的响应速度在 50 用户并发访问时，页面响应时间≤1 秒;网页数量>20000,站内关键词检索时间不超过 10ms。	
6	#	兼容性要求	兼容主流浏览器，至少支持 IE，Edge、Chrome、Firefox 和 Safari 的当前版本，保证内外网用户和网站所有网页均通过以上浏览器及其低版本兼容性测试。	是

三、服务要求

序号	指标项	指标要求	证明材料要求
1	投标人服务标准	提供 5 年免费的备品备件保障方案，在设备报修后，设备及其整机相关备件应在 4 小时内送达，并负责安装调试，项目实施过程中产生的辅材辅料费等费用由投标人承担。冗余电源。投标人提供 365 天*24 小时应急服务响应，建立完善的故障应 急响应机制，并具有处理各种故障的能力。故障响应时间指标如下：（1）重大故障，系统在运行中出现瘫痪、服务中断等重大故障，工程师及时到达现场，并评估故障、制定技术处理方案，支持现场应急处理，保证 4 小时内恢复系统运行。设备出现硬件故障情况下，在 4 小时内进行维修或更换，彻底排除设备故障，恢复系统运行。如设备暂时无法修复，提供不低于原设备性能的替换设备，用于支撑系统正常运行，直至原设备修复。 （2）主要故障 系统在运行中出现的直接影响服务、导致系统性能或服务部分退化的故障，系统性能下降但不影响正常业务运作。工程师立即处理，评估系统运行情况，并制定技术处理方案，支持现场处理。在 4 小时内恢复系统正常运行状态，6 小时内彻底排除故障。在有硬件故障情况下，启用现场备件库，进行维修或更换，彻底恢复系统运行。 （3）日常简单故障系统在运行中出现的对系统功能和性能影响不大,关键业务不受影响的故障。 工程师立即响应，提供现场技术支持。	是
2	厂商服务标准	提供本次投标软、硬件产品的 5 年免费保修；5 年特征库、威胁情况库、云解析等免费升级的原厂服务承诺函； 原厂为硬件及系统提供 365 天*24 小时的免费远程技术支持，提供热线受理、远程问题处理、故障响应、现场备件更换等电话技术支持服务。	是
3	培训标准	投标人需承诺提供本项目采购设备的不少于 6 人/天的制造商认证的工程师安装配置等实操培训课程，场地、交通等与培训相关的费用均由投标人承担。投标人需提供承诺函。	是
4	集成标准	此项目为交钥匙工程，投标人负责对项目涉及的软、硬件设备进行系统集成安装、调试，配合采购人完善细化实施方案。相关的费用均由投标人承担，投标人应出具相关服务承诺函。 项目实施期间涉及到的一切辅材辅料及配件，如网线、光纤跳线、堆叠线、PDU 等，一律由投标人负责，相关的费用由投标人承担。 投标人负责完成项目集成实施期间，机房的环境清洁、线缆整理、打线标等。 投标人须做好设备管理，承担项目验收前的设备安全责任，包括设备不被损坏、不丢	否

		失等。本项目到货日期为合同签订后的 15 个工作日内，项目实施周期及交付期为合同签订后的一个月之内。	

采购需求（02 包）

一、业务需求

以网络安全法、党委（党组）网络安全责任制和等级保护 2.0 为标准真正打造一套适应未来教育行业网络安全需求、覆盖等级保护 2.0 和网络安全法的各项要求，具备高水平网络安全治理（风险治理、资产治理、漏洞治理等）能力，建立以计算环境安全为基础，以区域边界安全、通信网络安全为保障，以安全管理中心为核心的信息安全整体保障体系，更加注重全方位主动防御、动态防御、整体防控和精准防护，最终提升对网络攻击预判和主动防御能力，防患于未然。保障业务和信息系统高效、准确、安全、稳定和持续运行，促进学校信息化长期稳定发展，为学校信息化提供可持续发展的信息网络安全技术和管理支撑。

通过持续加强网络安全保障体系建设，显著减少来自内外网的安全威胁、进一步保护数据安全、提升教学与学习体验、提高网络安全管理效率，有助于构建一个安全可信赖的数字化学习和工作环境，为高校的发展和创新提供有力的支撑。具体业务需求如下 ：

1、部署智能流量调度硬件设备，将校园网边界组网方式“由串改并”，形成更加安全的设备资源池，实现流量调度和流量编排等智能服务链。

2、部署零信任网关设备，替换现有的 SSL VPN 设备。通过身份持续动态认证和授权，提升数据保护水平，增强远程访问安全性。

3、部署智能 DNS 解析服务系统，提高用户上网、学校相关业务的可用性，实现 DNS 安全防护、分析监控、日志存储、DNS 智能调度等功能。

4、部署流量分析及管控硬件设备。

5、升级网站群平台，增加或完善用户登录、密码校验、系统日志、敏感信息处理、非法链接检测、安全运维监控等平台功能。

采购清单

产品类型	产品名称	数量
网络与安全硬件	智能 DNS	2

二、技术指标要求

①指标按重要性分为“★”、“#”和“△”。★代表实质性指标，不满足该指标项将导致投标被拒绝，#代表重要指标，△则表示一般指标项。

②“证明材料要求”项填“是”的，投标人须提供包含相关指标项的证明材料，证明材料可以使用制造商官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖投标人公章，未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。

③除需求中明确要求投标人承诺的事项外，其他要求提供证明材料的指标中，提供投标人承诺作为应答的不予认定。

2.1 DNS 解析服务及安全防护设备

序号	重要性	指标项	指标要求	证明材料要求
1	★	硬件及性能要求	内存≥16G； 冗余电源； 支持 LCD； 千兆电口数≥8； 万兆光口数≥2，并配置光模块； 硬盘容量≥1T； 开启解析日志情况下，单台设备 DNS 服务器每秒查询次数 QPS≥80000。	是
2	△	管理功能	支持所有设备节点的统一集中管理，通过 HTTPS/HTTP 方式登录统一的管理平台上完成所有服务的配置。	否
3	△	解析功能	支持常用的记录类型，包括但不限于 A,AAAA,CNAME,MX,NS,PTR,TXT,SRV,SPF 等，对配置的记录支持设置有效期限	否
4	△		支持标准的 DNS 服务，支持正向解析、反向解析功能。	否
5	#		支持基于 ICMP、UDP、TCP_SYN、TCP、HTTP、HTTPS 等的应用健康检测模板定制。	是
6	△		支持递归场景中可以根据时间、域名库、源地址、链路带宽的使用情况、带宽比例进行灵活的递归调度。	否
7	△		系统必须全面支持 IPv6 所采用的系统必须支持 IPv4	否

			和 IPv6 双栈。	
8	△	威胁情报及域名安全	支持双因子认证功能，与目前在用的统一身份对接，支持的认证源类型包括：LDAP、RADIUS、CAS、OAuth 。	是
9	#		能够支持防御 DNS SERVFAIL 攻击，客户端通过发起大量错误域名攻击触发递归无响应从而导致服务器性能拥塞，该设备能够自主识别该类攻击特征，进行攻击防护。	是
10	△		支持隧道攻击防护：支持对 DNS 请求类型、请求内容、及其规则特点的识别，配置相关参数（数据包大小、阈值频率、防护周期、TXT 类型防护启用、TXT 阈值频率、TXT 防护周期等）对 DNS 协议数据进行深度检测，对异常通信数据及时发现并阻断。	否
11	#		支持对全网发现的所有威胁事件统计，威胁事件分类包括但不限于：传统的僵尸网络病毒、后门木马、蠕虫病毒、检测 DDoS 木马等，利用高危漏洞样本的攻击、勒索软件等；威胁事件统计包括不限于发现时间，包含域名，严重级别等。	是
12	#		提供威胁解析识别+阻断的完整威胁防御链，能够将威胁访问在内网进行处置，保障内部网络环境的安全。支持对挖矿行为进行拦截，并对拦截记录进行日志记录、统计分析，定位到挖矿者源 IP。可以通过同厂商威胁情报平台提供在线更新服务。	是
13	△		威胁情报中心平台支持全球情报资讯查询，可按时间搜索，包括资讯标题、发布时间、资讯描述、参考链接。	是
14	#	云解析	基于全球 BGP+Anycast 网络，全球节点部署（节点覆盖国内主要的运营商：联通、电信、移动、教育网、等运营商策略），提供快速、安全、稳定的域名解析服务。	是
15	#		支持 IPv4 和 IPv6 智能解析，在 IPv4 和 IPv6 双栈环境下基于运营商、国家、省份、地市、权重等解析策略。提供对内置地址库的在线更新，并且由同厂商的云资源平台提供在线更新服务。	是
16	△		针对重点域名提供保障方案，并针对重点域名的实名信息修改、NS 记录修改提供详细的针对性解决方案，落实具体每一步操作流程的生效时间及情况，确保重点域名做任何变动均在安全范围内，保障重点域名的安全。	是
17	△		支持 A、AAAA、MX、CNAME、TXT、NS、URL 转发、SRV 等记录类型。	否
18	#	厂商资质	所投全部产品具备软件著作权，并具有相应证明文件，具有自主知识产权。	是
19	△		所投 DNS 产品具备公安部颁布的网络安全专用产品安全检测证书。	是

20	#		制造商通过 ISO9001 认证以及 ISO27001 认证，并具有对应认证证书	是

三、服务要求

序号	指标项	指标要求	证明材料要求
1	投标人服务标准	提供 5 年免费的备品备件保障方案，在设备报修后，设备及其整机相关备件应在 4 小时内送达，并负责安装调试，项目实施过程中产生的辅材辅料费等费用由投标人承担。冗余电源。投标人提供 365 天*24 小时应急服务响应，建立完善的故障应 急响应机制，并具有处理各种故障的能力。故障响应时间指标如下：（1）重大故障，系统在运行中出现瘫痪、服务中断等重大故障，工程师及时到达现场，并评估故障、制定技术处理方案，支持现场应急处理，保证 4 小时内恢复系统运行。设备出现硬件故障情况下，在 4 小时内进行维修或更换，彻底排除设备故障，恢复系统运行。如设备暂时无法修复，提供不低于原设备性能的替换设备，用于支撑系统正常运行，直至原设备修复。 （2）主要故障 系统在运行中出现的直接影响服务、导致系统性能或服务部分退化的故障，系统性能下降但不影响正常业务运作。工程师立即处理，评估系统运行情况，并制定技术处理方案，支持现场处理。在 4 小时内恢复系统正常运行状态，6 小时内彻底排除故障。在有硬件故障情况下，启用现场备件库，进行维修或更换，彻底恢复系统运行。 （3）日常简单故障系统在运行中出现的对系统功能和性能影响不大,关键业务不受影响的故障。 工程师立即响应，提供现场技术支持。	是
2	厂商服务标准	提供本次投标软、硬件产品的 5 年免费保修；5 年特征库、威胁情况库、云解析等免费升级的原厂服务承诺函； 原厂为硬件及系统提供 365 天*24 小时的免费远程技术支持，提供热线受理、远程问题处理、故障响应、现场备件更换等电话技术支持服务。	是
3	培训标准	投标人需承诺提供本项目采购设备的不少于 6 人/天的制造商认证的工程师安装配置等实操培训课程，场地、交通等与培训相关的费用均由投标人承担。投标人需提供承诺函。	是
4	集成标准	此项目为交钥匙工程，投标人负责对项目涉及的软、硬件设备进行系统集成安装、调试，配合采购人完善细化实施方案。相关的费用均由投标人承担，投标人应出具相关服务承诺函。 项目实施期间涉及到的一切辅材辅料及配件，如网线、光纤跳线、堆叠线、PDU 等，一律由投标人负责，相关的费用由	否

		投标人承担。 投标人负责完成项目集成实施期间，机房的环境清洁、线缆整理、打线标等。 投标人须做好设备管理，承担项目验收前的设备安全责任，包括设备不被损坏、不丢失等。本项目到货日期为合同签订后的 15 个工作日内，项目实施周期及交付期为合同签订后的一个月之内。	