采购内容及要求

一、项目概况

（一）建设背景

随着我校网络规模的快速扩张及数字化校园建设需求，现需采购一台专业DHCP服务器及一台DNS服务器，以解决当前网络架构中存在的核心隐患并提升整体服务水平。

目前，我校基础网络网络服务DNS依赖于单机的DNS设备；DHCP服务使用核心交换设备附带的简易DHCP功能。随着师生移动终端与物联网设备数量激增，DNS与DHCP原始架构负荷较大。其弊端集中表现为：DNS服务存在严重的单点故障风险，一旦该设备故障，将导致全校域名解析服务中断，严重影响教学、科研及日常办公；基础交换设备的DHCP功能在IP地址管理的精细化、可视化、安全性和稳定性上存在明显不足，会导致IP地址分配混乱、偶发冲突等问题，影响了用户的网络体验，并为校园网安全埋下隐患。

（二）建设目标

此次采购旨在构建面向校园全场景应用的、健壮、高效、可管可控的专业化网络基础服务平台。通过部署专业的DNS与DHCP核心网络服务设备，实现“地址自动化管理+智能解析调度+可视化运维+IPv6深度支持”的整体目标，为学校科研教学、校园管理、智慧校园应用提供长期可靠的基础技术支撑。

在DNS体系建设方面，新设备将与现有DNS设备进行融合部署，构建统一管理、高可靠解析架构。依托智能DNS的多链路调度能力，与互联网出口设备联动，实现IPv4/IPv6双栈环境下跨运营商链路的智能选路与流量优化，从而在多运营商带宽资源不均衡或出现某链路断路的情况下显著改善访问体验并保持解析不中断，保障校园网关键业务的持续、稳定运行。同时，借助域名解析系统的拨测能力，对境外学术资源访问质量进行监测与智能优化，提升国际教育与科研资源的访问效率和稳定性。通过DNS数据分析构建域名系统的可观测能力，实现对DNS解析异常的快速识别和精准定位，有效区分普通网络故障，缩短故障处理时间，增强网络核心服务的韧性与可用性。同时联动威胁域名情报库，实现对校园网内挖矿、勒索病毒、赌博等非法域名访问的精准拦截，确保威胁域名访问不出

校园网，也可做到精准溯源，保障校园网络安全。

在 IP 地址管理方面，引入专业化的 DHCP 设备，实现对 IPv4 与 IPv6 地址的统一规划与集中管理。通过系统层次化、语义化的 IPv6 编码规则，并提供直观的可视化管理界面、权限分级控制、使用记录追踪及 IP 地址全生命周期管理功能，显著减少人工干预和维护工作量，提高管理效率。通过定制开发，实现与现有认证计费系统协同对接，有效解决 IPv6 使用中可能出现的网速下降、访问不稳定等问题，并实现对终端分配多个运营 IPv6 地址，确保满足国家“去 NAT”要求下的多出口链路调度。同时，通过实时状态监控与结构化可视化展示，管理人员可以清晰掌握各网段、各类型终端的地址使用情况，减少配置错误和冲突风险，提升校园网运行的稳定性和管理效率。

在综合管理与运维能力上，与学校 “一网通办” 系统深度对接并开展定制化功能开发，实现域名与 IP 地址全生命周期、全流程在线管理，为智慧校园业务的自动化运转、规范化推进及审计可追溯提供坚实支撑。同时，搭建统一可视化大屏，面向网络中心、运维管理、应急保障等核心场景，集中展示网络运行状态、故障告警、地址使用率、IT 资产及安全风险等关键指标，全面达成网络运行的可视、可管、可控。

本次建设将使学校网络服务能力从“可用”迈向“稳定、安全、智能、可运营”。通过统一平台、集中管理、可视化展示和高可用架构，全面提升网络服务质量、科研教学体验、管理效率与运维水平，为未来 IPv6 深度应用、智慧校园建设和网络安全体系升级奠定坚实基础。

二、技术要求

（一）DNS 智能解析

1.CPU：国产化处理器；内存≥16GB；磁盘空间≥2TB*2；网口≥10 个 10/100/1000M 电口，≥2 个万兆光口；电源：提供交流冗余电源，支持热插拔；系统具备系统级、软件功能级冗余备份能力，QPS：不少于 100000，支持 HA 部署。

2.支持标准 DNS 协议，记录类型支持 A、AAAA、PTR、CNAME、MX、NS、TXT、SOA 等类型。

3.支持校内核心业务系统域名的安全防护，管理员在执行相关业务操作时，

可通过增强提示或禁止变更来规避误操作，以达到保护域名的效果。

4.递归查询支持 First/WRR、Only/WRR 等多种转发方式；支持对运营商 DNS 服务器进行健康检查，支持以 NS 域名方式作为转发目的。

5.▲具备智能 DNS 能力，业务系统健康监测方式不低于 15 种，支持 DNS 负载均衡算法不低于 9 种，包括但不限于动态就近性、多维度可用性算法、静态保持算法等实现最优解析，支持会话保持功能。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图）。

6.具备隧道攻击防护，可根据防护模式、阻断策略、双因子匹配、动态阻断有效期（秒）、监测统计周期（秒）、最大监测会话数、最大监测区数量等进行设置防护策略。

7.▲在智能 DNS 负载均衡调度场景下，支持配置业务解析失败应答策略包括但不限于动态兜底解析、静态兜底解析、无记录、无域名、丢弃等策略，提升异常场景下的容错率。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图）。

8.配置不少于 1 万条静态域名解析记录，压力测试单台设备的解析性能情况，在 QPS 解析性能参数达到 10 万时，要求：连续发起 10 次域名解析请求，每次解析延时不超过 1ms；日志查询检索时间是小于 10s；

9.▲可以监测防御 DDoS 反射攻击、源 IPDDoS 攻击、DNS 畸形包 DDoS 攻击、UDP Flood 攻击、TCP Flood 攻击、SYN Flood 攻击、ICMP Flood 攻击的 DNS DDoS 攻击，支持根据业务需求自定义限速阈值，并能提供相应的告警和攻击流量统计。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图）

10.对校内热点域名进行响应延迟探测，根据探测结果自动定期更新选路策略，优化整体访问质量和速度。

11.▲具备 SM3 国密算法进行 DNS 数据更新与存储。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图）

12.▲完成与我校现有 DNS 系统数据对接，集中下发 DNS 配置数据（现有 DNS 系统支持全 API 接口，可开发，但不能改变现有应用架构,现有 ZDNS T5100-SD，1U 硬件平台标准 DNS 设备，Intel 处理器，8G 内存，8 万 QPS，提供标准 API 接

口。)。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图）

13.▲DNS 节点支持实时同步云端威胁情报平台的威胁情报数据，数据同步支持加密，并能保证各 DNS 节点数据一致性。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图）

14.以上功能要求投标完成后三天内可由甲方组织测试验证，产品经过测试验证的视为满足，未经过测试验证的视为不满足，甲方可单方面终止合同。

15.数量 1 台；原厂软硬件质保 3 年

（二）DHCP 地址分配管理

1.CPU：国产化处理器；内存≥16GB；磁盘空间≥2TB*2；网口≥10 个 10/100/1000M 电口，≥2 个万兆光口；电源：提供交流冗余电源，支持热插拔；系统具备系统级、软件功能级冗余备份能力，LPS：不少于 1500，DHCP 容量:不低于 8 万，支持 HA 部署。

2.具备 IPV4/IPv6 DHCP Failover 技术，提供 DHCP 服务异地灾备的功能，当一台异常时另外一台支持一键接管全部租赁服务，支持调整 MCLT 和负载比例

3.具备对地址池进行分组，方便根据使用目的不同进行地址池归类管理支持对地址池进行分组，方便根据使用目的不同进行地址池归类管理，支持手动创建分组和基于自定义属性自动分组两种方式，并以可视化图形方式展示分组信息。

4.▲具备 IPv4-IPv6 双栈地址分配，可将 IPv4 地址嵌入 IPv6 地址中实现双栈地址对应，支持通过 IPv4 地址快速查找对应的 IPv6 地址。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图）

5.具备全局网络使用率、冲突地址条件、僵尸地址条件的自定义配置，可实时判断是否达到触发条件并告警。

6.▲具备创建 IPv6 地址规划方案，并绑定固定前缀，同时支持为不同的组织创建子方案并继承父方案空间规划；支持针对每个方案按位宽长度通过图形化拖拽方式规划连续的 IPv6 地址空间，每个空间用于标记业务类型；支持对每段地址空间配置对应的空间标识并为空间标识赋值，每个地址空间可配置多个空间

标识，空间标识象征具体业务。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图）。

7.具备创建 IPv4 地址规划方案，每个方案绑定唯一的地址前缀，可结合组织架构、业务等维度进行 IPv4 地址规划；支持创建多级子网规划，通过选择子网的目标子网掩码拆分规划子网，可按照业务需求选择需要规划的子网，并配置关联备注信息；支持通过在地址台账中引用通过规划方案形成的 IPv4 网络，快捷完成网络创建，并关联规划的备注信息。

8.具备通过 SNMP 凭证以网络扫描的方式发现网络中的所有的网络设备；支持 SSH 凭证用于联动网络设备下发绑定/阻断策略；支持查看网络设备的终端接口信息包括 MAC 地址、终端类型、IP 地址、接口、VLAN 等信息同时可进行即时刷新。

9.具备与 AD、深澜、城市热点等第三方系统进行对接，允许信息同步至所有地址当中；支持与主流网络设备联动，对终端实现交换机阻断和端口绑定，且支持黑名单管理。

10.▲具备 DDI（DNS/DHCP/IPAM)拓展能力，能够在 DNS 设备异常后通过升级 License 服务接管 DNS 服务。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图）

11.具备通过配置下发能够实现 DHCP 地址的创建、分配、续租功能、支持 DHCP 固定、地址池、保留、僵尸地址等管理、支持 IPv4 及 IPv6 的 DHCP Failover 部署方式、支持通过 Excel 批量导入网络、IP、地址池等信息、支持语义模板方式按位宽规划网络。

12.▲具备为终端同时分配来自多家运营商的 IPv6 地址，并实现多出口链路的智能调度与优化，保障网络访问的连续性与最优性能。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图）

13.以上功能要求投标完成后三天内可由甲方组织测试验证，产品经过测试验证的视为满足，未经过测试验证的视为不满足，甲方可单方面终止合同。

14.数量 1 台；原厂软硬件质保 3 年

（三）零信任服务要求

1.支持 IPV4/IPV6 双栈网络 IP 配置，支持默认限制所有 IP 通过 WAN

口访问系统。

2.支持通过隧道模式和WEB模式发布资源,其中WEB模式支持透明代理、智能改写等模式。

3.▲支持针对发布的WEB应用开启WEB水印，水印内容至少包括：用户名+当前年月日。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图)。

4.零信任客户端支持多种终端操作系统兼容，包括但不限于：Windows7/10/11、MacOS10/11/12、Ubuntu、Android、iOS、麒麟V10系统、统信V20系统，提供国产化系统厂商相互兼容性证明。

5.支持配置一个帐号在PC端和移动端分别绑定N个终端数量，可设置的数量范围为1~100；支持配置一个终端仅允许一个用户绑定；支持多因素认证,其中异常环境下需完成增强认证才可登录;支持自动锁定闲置账号(时长可自定义配置)。

6.支持通过组织架构、角色等方式进行本地用户管理；支持与外部用户管理服务器进行对接；支持批量导入/导出用户；配置不少于10万条弱密码规则。

7.支持限定操作系统、接入IP、指定杀毒软件、用户登录时间等变量动控制态业务访问。

8.支持Web应用商店功能，可配置需认证/不经过认证访问Web应用商店。

9.支持UDP+TCP单包授权机制，UDP+TCP方式默认不开放端口；支持共享码和一人一码两种模式。

10.▲支持以私有DNS发布对外访问资源，支持管理员自主配置是否允许从具体网络区域（校园网网/互联网）接入时使用此私有DNS解析地址。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图）

11.支持PC终端登录零信任客户端后,在特定的网络域下只能主动访问

网络域对应的 IP、IP 范围、IP 段、域名，且只能被限定的 IP、IP 范围、IP 段访问。

12.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。

13.支持对设备自身的安全状态和策略配置进行巡检，并输出巡检报告，支持下载。

14.支持通过 OPEN API 的方式将零信任系统的能力开放给第三方业务系统进行调用配置。

15.▲支持 iOS、安卓、鸿蒙 Next 手机 APP 集成零信任 SDK，支持通过管理平台上传原包应用进行自动封装。支持为已经集成零信任 SDK 并发布到安卓或 iOS 应用市场的公有化生态应用配置策略，使其具有零信任接入能力及数据防泄漏能力。提供生产厂家确认的、相应的功能证明材料（包括但不限于测试报告、官网和功能截图）

16.配置≥100 个零信任并发用户授权。

17.在满足加密流量≥300Mbps，最大并发用户数≥400 的情况下，提供具备的硬件环境：≥8 个 10/100/1000 电口，≥2 万兆光口 SFP，内存大小≥16G，硬盘容量≥128G SSD。

18.原厂质保 3 年。