南京理工大学泰州科技学院

中国农业银行泰州分行

智慧校园网络基础设施改造工程项目

项目编号：2020.004-1

招 标 文 件

招标人：南京理工大学泰州科技学院（盖单位章）

2020年12月25日

根据《南京理工大学泰州科技学院物资采购管理办法》的规定，拟对“南京理工大学泰州科技学院中国农业银行泰州分行智慧校园网络基础设施改造工程项目” 进行国内公开招标，欢迎有兴趣并符合资格条件的供应商，在接受其所有条款要求的基础上参加投标。

**一、项目名称及内容**

1. 项目编号： 2020.004-1
2. 项目名称：智慧校园网络基础设施改造工程项目
3. 项目地点：江苏省泰州市梅兰东路8号
4. 项目单位：南京理工大学泰州科技学院
5. 项目概况：南京理工大学泰州科技学院中国农业银行泰州分行智慧校园网络基础设施改造工程项目，详见招标文件
6. 资金来源：非财政资金(自筹)
7. 项目预算：249.5万元
8. 最高限价：249.5万元
9. 项目类别：货物类（软硬件及工程服务）

**二、投标供应商资格**

1. 符合《中华人民共和国政府采购法》第二十二条规定；
2. 本项目不接受联合体投标；
3. 供应商存在以下不良信用记录情形之一的，不得推荐为中标候选供应商，不得确定为中标供应商：
   1. 供应商被人民法院列入失信被执行人的；
   2. 供应商或其法定代表人或拟派项目经理（项目负责人）被人民检察院列入行贿犯罪档案的；
   3. 供应商被工商行政管理部门列入企业经营异常名录的；
   4. 供应商被税务部门列入重大税收违法案件当事人名单的；
   5. 供应商被政府采购监管部门列入政府采购严重违法失信行为记录名单的。

**三、投标截止时间** ：2021年1月8日上午10:30前

**四、现场踏勘时间**: 2020年12月29日上午9:00-11:00，下午2:30-4:30。

踏勘联系人：陈老师 电话： 13905262961

**五、开标时间及地点**

1. 开标时间：2021年1月8日下午2:00
2. 开标地点：南京理工大学泰州科技学院评标室（明德楼4105）

**六、联系方法**

地 址：江苏省泰州市海陵区梅兰东路8号 资产与实验管理处(明德楼一楼4103)

招标联系：毛老师 电话：0523-86159939、13951170722

技术咨询：陈老师 电话： 13905262961

**七、其他事项说明**

1. 投标供应商可在学校官方网站直接下载招标文件。
2. 报名中有任何疑问或问题，请在工作时间（周一至周五，上午9:00-12:00，下午13:30-17:30，节假日休息） 咨询。
3. 投标人必须勘查现场，并在投标书提供详细的技术方案、施工方案、验收方案及售后服务与培训方案。同时在标书中必须提供技术偏离表和响应评分细则的索引目录表，便于现场评标。不参加现场踏勘，不可以参加本项目投标。
4. 项目付款方式：项目实施、试运行、竣工验收合格并经审计后付至审计价的90%，余款10%待1 年后付清。
5. 如对本招标文件有任何疑问或澄清要求，请在截止投标时间前2天（2021年1月6日16：00之前）联系采购人，否则视同理解和接受，投标供应商对招标文件、采购过程、中标结果的质疑，应当在法定质疑期内一次性提出针对同一采购程序环节的质疑。质疑请带营业执照、质疑函（盖单位公章），凭身份证至我校资产与实验室管理处进行规范质疑。

质疑联系人：毛老师 0523-86159939、13951170722

**招标需求**

# 项目概述

项目名称：智慧校园网络基础设施改造工程项目

项目编号：2020.004-1

项目内容：网络基础设备、网络安全设备、网络核心设备、虚拟化防护系统、VPN、运维管理平台及校园网络工程集成服务等。

项目预算：249.5万元

最高限价：249.5万元

# 项目建设目标

为保障南京理工大学泰州科技学院信息化建设工作顺利进行，在新数据中心机房重新搭建智慧校园应用基础设施平台，改造并升级原校园网三层架构，配置相应的网络安全产品，为智慧校园建设提供一个稳定、安全的网络环境。

本次项目采购2台智能DNS、2台核心交换机、3台汇聚设备、2台万兆防火墙作HA为网络出口，使网络冗余安全。防火墙上联接入电信、教育三条线路，改善学校网络带宽。原有的WAF防火墙，由于是对全校的Web网站进行防护，此次串联在数据中心汇聚交换机和核心之间，只针对服务器区进行防护，大大减轻了WAF的承载量。原有的流控设备，由于考虑到只具有千兆电口问题，影响到了核心与防火墙之间的万兆互联，因此这次去除，流控原有流量限制、网络隔离、开放外网权限等操作在防火墙上实现。而原先的宿舍楼、教学楼与数据中心汇聚交换机则保留不动，其他楼宇汇聚设备更新。数据中心区域新增1套虚拟化防护软件用于对虚拟机的安全防护；运维管理区增加 1台SSL VPN用于校外访问校内资源，并与今后智慧化校园平台对接；1台远程USB服务器设备，帮助解决虚拟化平台加密狗不够插的问题；1套IT运维管理系统用于对整个网络及服务器设备的监控。由于涉及新旧数据中心对接问题，增加1项新旧数据中心对接、虚拟服务器迁移、校园网整理运维的服务。详细设计要求招标项目建设具体指标（4.9校园网络项目集成服务）。

附1：原网络拓扑图如图1所示。

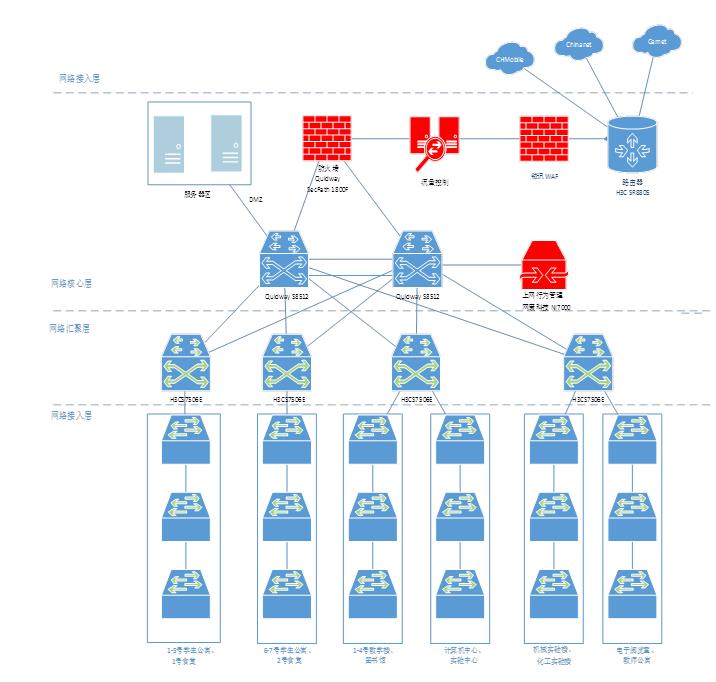
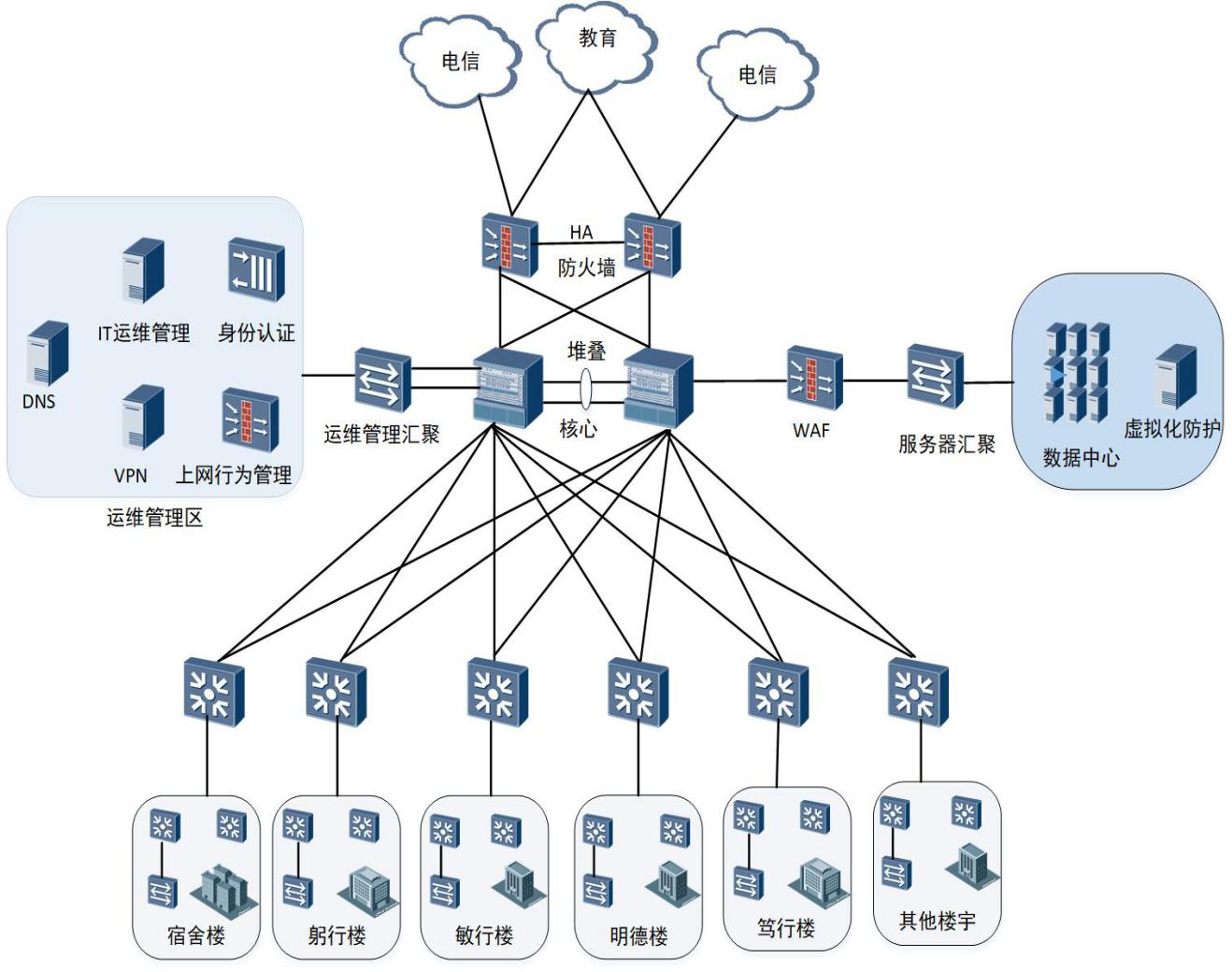


图1 原校园网络拓扑结构图

附2：建设目标网络拓扑图，如图2所示。



**图2 新网络拓扑结构图**

# 项目建设内容

需求一览表：

| **序号** | **名称** | **性能及参数要求** | **质保** | **数量** |
| --- | --- | --- | --- | --- |
| 1 | 防火墙（万兆） | 2U机箱，4个通用扩展插槽，配置≥4个10/100/1000MBase-T电口，≥4个SFP口，≥2个万兆SFP+口。吞吐率(bps)≥**26G**，最大并发连接数≥600万，每秒新建连接数≥20万，支持IP Sec VPN隧道数≥20000条，支持并发SSL VPN用户许可≥10个，单台设备配置冗余电源。 | 质保三年 | 2 |
| 2 | 核心交换机 | 支持多级交换架构，能够配置独立的交换网板与独立的主控板，交换网板与主控板硬件槽位分离，业务插槽数≥10，交换容量≥512Tbps，转发能力≥96000Mpps，主控引擎模块≥2，满足1+1冗余，主控槽位与交换网板槽位宽度相同的全宽槽位，电源模块冗余。  单台交换机要求配置≥48个千兆电接口，配置≥24个千兆光接口，配置≥24个万兆光口。  共需配置千兆单模模块90个，千兆多模模块10个，万兆单模模块24个，万兆多模模块30个。 | 质保三年 | 2 |
| 3 | 汇聚交换机 | 业务插槽数≥6，交换容量≥76Tbps，转发能力≥8600Mpps，主控引擎模块≥2，满足1+1冗余，电源模块冗余  单台交换机要求配置冗余主控引擎，配置≥40个千兆光口，≥8个万兆光口 | 质保三年 | 2 |
| 4 | 汇聚交换机 | 业务插槽数≥6，交换容量≥76Tbps，转发能力≥8600Mpps，主控引擎模块≥2，满足1+1冗余，电源模块冗余  单台交换机要求配置冗余主控引擎，配置≥48个千兆光口，≥24个万兆光口。 | 质保三年 | 1 |
| 5 | 智能DNS设备 | ≥6个10/100/1000M电口，支持可扩展万兆光口，2块1TB硬盘，支持raid 0，1，配置支持热插拔双电源，DNS（QPS指标）单设备≥15万QPS，DHCP（LPS指标）单设备≥1200LPS，DHCP（IP地址容量）单设备≥100000，网络准入（并发上线数）≥200用户/秒，协议转换网关最大并发连接数≥8000000个；最大新建会话连接数≥50000个/秒；支持双栈DNS，DHCP和IPAM功能，集成权威/递归/转发/缓存等多种角色DNS服务、智能DNS解析、应用服务器宕机检测、DNS流量调度、DNS安全加固、DNS数据分析、终端服务端口扫描审计、全面支持IPv6。 | 质保三年 | 2 |
| 6 | 虚拟化防护 | 不限制虚拟机防护数量。  至少支持VMware等虚拟化平台安全防护，无需额外购买组件；  提供双主控，实现控制平面冗余；支持在线软件升级，使部署的更新和升级不会产生任何服务中断。吞吐量≥40G，并发连接数≥1000万，每秒新建连接≥22万，虚拟机不限作为保护对象。支持业务平台性能弹性扩展，根据将来业务发展需求，可扩展至吞吐量≥1Tbps，可扩展至最大并发连接数≥3亿，每秒新建连接数≥500万； | 质保三年 | 20 |
| 7 | SSL VPN | 性能指标：吞吐量1.5Gbps，并发会话数160万；支持 SSL VPN 并发用户≥2600个；SSL 最大加密流量400Mbps，IPSEC 最大加密流量220Mbps； 硬件指标：内存≥4G；硬盘 SSD ≥64G，千兆电口≥6个，千兆光口≥2个。配置SSLVPN接入授权≥800个。 | 质保三年 | 1 |
| 8 | IT运维管理软件 | 实现各种IT资源的统一监控与管理，提供网络拓扑的大屏展示功能，提供灵活的告警和通知策略，通过告警分析，准确定位故障源。提供30个主机设备许可，300网络设备许可 | 质保三年 | 1 |
| 9 | 校园网络项目集成服务 | 本次项目提供“交钥匙”工程，即为提供本次项目所涉及到的硬件实施部署、网络调试等，并配合校方将现有的网络系统、服务器系统、虚拟化平台迁移到此次项目平台中，另需结合机房现有环境、安全需求，根据校方要求，提供后续数据中心对接、联调服务等。  提供本项目使用的所有辅材。  本次项目提供项目经理1人，中途不允许更  换项目经理。本次项目中标方提供工程师驻场技术支持服务（日期从项目实施算起，为期一年），以确保此次项目的安全、稳定运行。  产品到货后提供生产厂家400电话对产品信息进行核实 | 质保三年 | 1 |
| 10 | 运维辅助设备 | 自动双面激光打印机，2台 | 质保  三年 | 2 |
| 网络服务器运维调试平板，2台 | 2 |
| 11 | 交换机 | 1U高度，24个10/100/1000Base-T千兆以太网端口交换机,包转发率: ≥108Mpps，交换容量: ≥336Gbps，支持4个万兆SFP+上联端口, ≥1个电源 | 质保三年 | 1 |
| 12 | 上网行为管理设备 | 原网康NI7000-SG由于产品授权已过期，升级原有产品3年授权，含3年服务 | 质保三年 | 1 |
| 13 | 远程USB服务器 | 不少于16个标准USB2.0接口，兼容USB3.0及USB1.0/USB1.1设备；  标准1U机架式安装，静音无风扇设计；  双网口，需独立MAC地址；双电源冗余输入； | 质保三年 | 1 |
| 14 | 服务器内存升级 | 原虚拟化服务器内存由原来的128G升级到256G，共3台。  原教务系统数据库服务器内存由原来的64GB升级到128GB，共2台。 | 质保三年 | 1 |

# 项目建设具体指标

## 4.1 防火墙

| **技术指标** | **指标要求** |
| --- | --- |
| 推举品牌 | 天融信、三石、华三、华为、绿盟、深信服 |
| 硬件规格 | 硬件平台采用先进的多核网络专用架构。硬件平台采用多核处理器，使用64位多核处理器 |
| 标准机架2U及以上，配置≥4个10/100/1000MBase-T电口，≥4个SFP口，≥2个万兆SFP+口，1 HA口，1个USB口，≥4个通用扩展插槽 |
| 性能 | ★吞吐率(bps)≥26G，最大并发连接数≥600万，每秒新建连接数≥20万，提供IPSec VPN隧道数≥20000条，支持并发SSL VPN用户许可≥10个； |
| 访问控制 | 支持基于用户、用户组的访问控制，用户认证要求支持Radius、LDAP、Windows AD域等方式；支持用户必须用AD域账户登录操作系统，否则禁止上网功能； |
| 支持策略命中数统计，便于维护策略。 |
| 内容过滤 | 支持内核级深度内容检测技术, 支持对网页关键字和JavaScript、ActiveX进行过滤, 支持对FTP上传和下载文件的控制 |
| 支持对收件人地址、发件人地址、主题、正文、附件名称通配符匹配、附件大小等进行匹配过滤 |
| 支持基于URL地址的关键字设置白名单和黑名单 |
| 支持将任意接口数据完全镜像到设备自身的其他接口用于抓包分析，支持基于源IP、目的IP、源端口、目的端口、网络协议（TCP、UDP、ICMP）等条件对镜像流量进行过滤，并且支持选择入方向、出方向及双向流量镜像 |
| 支持IPv4/IPv6双协议栈；  支持IPv4/IPv6，IPv6/IPv4协议转换；  支持IPv6动态路由； |
| 支持目的IP替换，支持记录所有日志或记录被替换目的IP的日志 |
| 支持WAP智能分流功能，通过HTTP request的URL内容将流量引向WAP网管或直接转发到互联网 |
| 应用协议智能识别 | 支持对1500+ 种应用的识别和控制，包括200+移动应用 |
| 支持将通过应用过滤器筛选出来的应用直接生成模板供用户统一管理使用 |
| 支持NAT444模式，支持导出NAT444静态映射表 |
| 支持NAT公网地址池中IP有效性检测，避免因NAT地址无法使用导致业务中断，提供产品界面截图有效 |
| ★功能虚拟化 | 支持配置文件、系统服务、路由、链路聚合、安全策略、NAT策略、带宽管理、认证策略、IPV6功能、URL过滤、病毒过滤、WAF、内容过滤、审计、报表、防代理等安全功能虚拟化（提供功能截图） |
| IPSEC VPN | 支持标准IPSec协议，能够与国内外知名知名厂商的VPN设备互联互通 |
| 支持3DES、DES、AES等多种加密算法 |
| SSL VPN | 必须支持对登录SSL VPN的用户端系统进行端点安全检查 |
| 支持基于手机短信的登录认证方式以及硬件USB-key的认证方式 |
| 支持自定义统计功能 |
| 资质 | 设备生产厂商具备中国信息安全测评中心颁发的《国家信息安全漏洞库（CNNVD）技术支撑单位等级证书》一级； |
| 设备生产厂商具备中国信息安全测评中心颁发的《国家信息安全漏洞库（CNNVD）技术支撑单位等级证书》一级； |
| 设备生产厂商具备国家计算机网络应急技术处理协调中心颁发的《网络安全应急服务支撑单位证书（国家级）》 |

## 4.2核心交换机

| **技术指标** | **指标要求** |
| --- | --- |
| 推举品牌 | 华为、华三、锐捷等 |
| 产品架构 | 支持多级交换架构，能够配置独立的交换网板与独立的主控板，交换网板与主控板硬件槽位分离 |
| 业务板卡与交换网板采用完全正交设计（槽位互相垂直），跨线卡业务流量通过正交连接器直接上交换网板，背板走线降低为零，极大规避信号衰减，具备平滑演进能力。 |
| 业务插槽数 | 支持业务插槽数≥8 |
| 整体性能 | ★交换容量≥512Tbps，转发能力≥96000Mpps（提供官网截图） |
| 主控引擎 | 主控引擎模块≥2，满足1+1冗余，主控槽位与交换网板槽位宽度相同的全宽槽位，提供更好的扩展性和可靠性 |
| 电源冗余 | 电源模块冗余 |
| 风扇冗余 | 风扇冗余，即使拔掉一个，设备也可以正常工作，可测试。 |
| 关键部件热插拔 | 主控交换卡、电源、接口模块、风扇、网板等关键部件可热插拔 |
| 接口要求 | 以太网支持千兆电口，千兆光口，万兆光口、万兆电口、40G端口、100G端口，提供官网链接 |
| 支持FCoE接口 |
| 链路聚合 | 聚合组数≥128组，每组成员≥8个 |
| 支持跨设备链路聚合 |
| 支持对广播、组播、单播报文的均匀分担 |
| 支持链路聚合+ECMP情况也可以对报文均匀分担，即等价路由的链路是由聚合链路组成情况下的报文分担 |
| ACL | 支持双向ACL，ACL≥4K |
| 支持端口ACL |
| 支持VLAN ACL |
| QOS | 每端口支持8个优先级队列，3个丢弃优先级，支持SP、WRR、SP+WRR三种队列调度算法 |
| 支持精细化的流量监管，粒度可达8K |
| 支持流量整形Shapping |
| 支持WRED拥塞避免 |
| 支持802.1p、TOS、DSCP、EXP优先级映射 |
| 可靠性 | 双引擎快速倒换，主备切换时候板内转发无丢包 |
| 支持NSF/GR for OSFP/BGP/IS-IS |
| 支持热补丁功能，可在线进行补丁升级 |
| 支持BFD，BFD for VRRP/BGP/IS-IS/OSPF/RSVP/LDP/RIP/静态路由。 |
| MAC | MAC表≥288K，提供测试报告证明 |
| 路由表 | 路由表≥256K |
| ARP | ARP表≥170K |
| 虚拟化 | 多虚一技术(N:1)，支持4框虚拟化技术,提供第三方权威机构检测报告 |
| 一虚多技术（1:N） |
| 支持多虚一技术和一虚多技术的配合使用 |
| 跨三层互联技术 | 支持主流的MAC in IP技术，如EVI/EVN/OTV等，实现跨三层网络的二层互联 |
| VxLAN | 支持VxLAN 网关，提供第三方权威机构检测报告 |
| IPv6 | 支持IPv6协议族，支持IPv6静态路由、RIPng、OSPFv3、IS-ISv6、BGP4+等IPV6路由协议，支持丰富的IPv4向IPv6过渡技术，包括：IPv6手工隧道、6to4隧道、ISATAP隧道、GRE隧道、IPv4兼容自动配置隧道等隧道技术 |
| 产品资质 | 为实现降低能源消耗、提高能源利用率、促进国家节能减排的目标。投标产品在设计、研发、生产、过程中符合国家节能标准。产品生产厂商需通过ISO 50001能源管理体系认证，要求提供证书复印件  产品生产厂商应具有健全的环保体系，建立有害物质的检测手段，严格管理产品采购和生产环节，禁止或控制有毒有害物质的使用。需通过QC 080000有害物质过程管理体系认证，要求提供证书复印件 |
| 配置要求 | 单台配置冗余主控，冗余风扇，2500W以上电源3块。  单台交换机要求配置48个千兆电接口，配置120个千兆光接口，配置24个万兆光口。  单台以太网板卡≥4个  两台交换机堆叠线缆一批，配置同品牌千兆单模模块90个，千兆多模模块10个，万兆单模模块24个，万兆多模模块30个。 |

## 4.3 汇聚交换机

| **技术指标** | **指标要求** |
| --- | --- |
| 推举品牌 | 华为、华三、锐捷等 |
| 基本要求 | 交换容量≥76Tbps、包转发率≥8640Mpps |
| 槽位数量≥8 |
| 机框通风散热需采用前后通风或左右通风方式，风道不拐弯设计，并提供设备散热通风图 |
| 多业务板卡支持 | 支持GEPON OLT及10G EPON OLT接口，提供官网配置手册截图和链接  支持1OG EPON 功能，支持1OG 对称和非对称 ONU提供工信部权威第三方测试报告 |
| VLAN特性 | 支持基于端口的VLAN，802.1q Vlan封装，最大Vlan数≥4096 |
| 产品性能 | MAC表≥1M、学习速率≥130K/S、IPv4 FIB表项≥3M、Ipv6 FIB表项≥1M、ARP表项≥180K、学习速率≥1.1K/S、ACL表项≥64K、端口缓存≤200ms，以上性能参数要求提供工信部权威第三方测试报告证明 |
| 产品功能 | 支持ERPS、RPR、OpenFlow、TRILL、Vxlan等功能，提供工信部权威第三方测试报告证明 |
| 带宽控制 | 支持带宽控制，控制粒度≤64Kbps |
| 虚拟化技术要求 | 支持N：1虚拟化：可将多台物理设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理，跨物理设备的链路聚合； |
| 支持1：N虚拟化：可将1台物理设备虚拟成多台逻辑设备，每台逻辑设备享有独立的硬件和软件资源，相互独立，互不影响； |
| 上述功能提供第三方测试报告证明 |
| 远程端口扩展能力 | 通过远程端口扩展，作为控制设备实现对端口扩展模块的集中控制，支持二级端口扩展设备级联，虚拟化后的设备支持基于Ipv4\Ipv6的VXLAN的二三层互通，提供工信部权威第三方测试报告 |
| 安全特性 | 支持IP+MAC+PORT任意组合的绑定，支持非法帧报文过滤，用户分级管理和口令保护，支持端口隔离，支持SSH，支持SNMPv3网管 |
| Macsec | 支持硬件级加密技术Macsec技术（802.1ae），上述功能提供官网截图证明 |
| IPv6 | 支持IPv6协议族，支持IPv6静态路由、RIPng、OSPFv3、IS-ISv6、BGP4+等IPV6路由协议，支持丰富的IPv4向IPv6过渡技术，包括：IPv6手工隧道、6to4隧道、ISATAP隧道、GRE隧道、IPv4兼容自动配置隧道等隧道技术 |
| 可靠性 | 支持VRRP，RRPP，Ethernet OAM（802.3ah），支持Graceful Restart for OSPF/BGP/IS-IS |
| 设备管理 | SNMP V1/V2/V3 |
| 配置要求 | 单台设备配置如下：  提供双电源、双引擎（集成4个25G/10G端口，支持做堆叠使用），配置不少于40个千兆光口，8个万兆光口。 |

**4.4 汇聚交换机**

| **技术指标** | **指标要求** |
| --- | --- |
| 推举品牌 | 华为、华三、锐捷 |
| 基本要求 | 交换容量≥76Tbps、包转发率≥8640Mpps |
| 槽位数量≥8 |
| 机框通风散热需采用前后通风或左右通风方式，风道不拐弯设计，并提供设备散热通风图 |
| 多业务板卡支持 | 支持GEPON OLT及10G EPON OLT接口，提供官网配置手册截图和链接  支持1OG EPON 功能，支持1OG 对称和非对称 ONU提供工信部权威第三方测试报告 |
| VLAN特性 | 支持基于端口的VLAN，802.1q Vlan封装，最大Vlan数≥4096 |
| 产品性能 | MAC表≥1M、学习速率≥130K/S、IPv4 FIB表项≥3M、IPv6 FIB表项≥1M、ARP表项≥180K、学习速率≥1.1K/S、ACL表项≥64K、端口缓存≤200ms，以上性能参数要求提供工信部权威第三方测试报告证明 |
| 产品功能 | 支持ERPS、RPR、OpenFlow、TRILL、Vxlan等功能，提供工信部权威第三方测试报告证明 |
| 带宽控制 | 支持带宽控制，控制粒度≤64Kbps |
| 虚拟化技术要求 | 支持N：1虚拟化：可将多台物理设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理，跨物理设备的链路聚合； |
| 支持1：N虚拟化：可将1台物理设备虚拟成多台逻辑设备，每台逻辑设备享有独立的硬件和软件资源，相互独立，互不影响； |
| 上述功能提供第三方测试报告证明 |
| 远程端口扩展能力 | 通过远程端口扩展，作为控制设备实现对端口扩展模块的集中控制，支持二级端口扩展设备级联，虚拟化后的设备支持基于IPv4\IPv6的VXLAN的二三层互通，提供工信部权威第三方测试报告 |
| 安全特性 | 支持IP+MAC+PORT任意组合的绑定，支持非法帧报文过滤，用户分级管理和口令保护，支持端口隔离，支持SSH，支持SNMPv3网管 |
| Macsec | 支持硬件级加密技术Macsec技术（802.1ae），上述功能提供官网截图证明 |
| 可靠性 | 支持VRRP，RRPP，Ethernet OAM（802.3ah），支持Graceful Restart for OSPF/BGP/IS-IS |
| IPv6 | 支持IPv6协议族，支持IPv6静态路由、RIPng、OSPFv3、IS-ISv6、BGP4+等IPV6路由协议，支持丰富的IPv4向IPv6过渡技术，包括：IPv6手工隧道、6to4隧道、ISATAP隧道、GRE隧道、IPv4兼容自动配置隧道等隧道技术 |
| 设备管理 | SNMP V1/V2/V3 |
| 配置要求 | 单台设备配置如下：  提供双电源、双引擎（集成4个25G/10G端口，支持做堆叠使用），配置不少于48个千兆光口，24个万兆光口。 |

## 4.5 智能DNS设备

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
|
| 推举品牌 | 亚信、迪讯、微格 |
| 总体规格 | 提供一台DNS硬件设备，设备配置至少为，四核8进程，工业级内存16G，千兆电口≥6个，企业级存储介质1TB，提供不少于12万QPS的DNS解析授权。 |
| 磁盘空间 | 企业级硬盘，>=1TB，扩展支持RAID |
| 设备电源 | 支持并配置2U冗余电源 |
| 双机工作模式 | 支持HA双机部署、VRRP协议、DNS ANYCAST、集中管理等多种方式 |
| IP地址容量 | >=3万 |
| 双因子登录 | 支持双因子登录鉴别，支持动态令牌种子文件的导入，支持动态令牌+用户名/密码方式，防止密码重放性攻击（需提供界面截图，加盖投标人公章） |
| 权限控制 | 支持DNS ZONE授权，基于IP地址规划段授权，支持DNS资源记录锁定修改功能（需提供界面截图，加盖投标人公章） |
| 设备故障监控 | 支持实时显示设备CPU负载、空闲内存、磁盘使用、DNS QPS，DHCPv4 LPS，DHCPv6 LPS等设备参数（需提供界面截图，加盖投标人公章） |
| 巡检报告 | ★支持下载当前设备运行状态报告，简化设备巡检过程，巡检报告包括当前设备DNS/DHCP服务数据汇总、CPU/内存/网卡/硬盘等状态（需提供界面截图，加盖投标人公章） |
| CSRF防御 | 支持登录认证页面产生加密随机数，可以和Session会话进行对比分析，预防CSRF攻击 |
| TLS协议禁用 | 支持HTTPS访问禁用TLSv1协议，支持TLSv1.2或更高版本 |
| DNS服务 | 必须支持标准的DNS服务 |
| DNS参数定义 | 支持VIEW视图和ZONE区域的DNS参数继承，支持DNS参数定义（如allow-transfer、allow-recursion、allow-query、allow-notify、acl、Minimal Responses、check-names、RRSet-Order、Server TSIG key等参数） |
| 支持IPv6 | ★DNS解析服务支持IPv6，支持DNS64，提供IPv6 Ready核心协议认证复印件 |
| 生命周期管理 | 支持定义DNS HOST记录的使用到期时间，通知人邮箱。域名到期自动提醒及到期自动清除记录，自动发送邮件 |
| 解析排序 | 支持解析结果按照管理员设定的ISP所属网段返回，实现解析结果链路类型的负载应答控制（需提供界面截图，加盖投标人公章） |
| 智能解析 | 支持设定网通、电信、移动、教育、科技网等IP地址段，针对不同的地址段解析不同的IP，便于外部访问主页提高访问速度 |
| 业务宕机检测 | 支持ICMP，TCP/端口，HTTP URL，HTTPS URL，SNMP，TCP SYN，TCP CONNECT，UDP SCAN等多种检测方式（需提供界面截图，加盖投标人公章） |
| 支持DNS域名解析检测，通过设定预期结果进行解析比较，实现对重点域名进行检测（需提供界面截图，加盖投标人公章） |
| 宕机告警切换 | 支持业务健康性检测拓扑图实时监控，通过图形化界面直观呈现业务健康检测的结果，实时拓扑故障告警（需提供界面截图，加盖投标人公章） |
| 对于DNS宕机检测故障切换时，支持单记录自动切换，支持多记录同时自动切换，当业务节点故障排除后，自动启动策略切换回原来业务节点 |
| IPv6翻译转换 | 在WEB应用系统无需改动的前提下，进行设备的部署，实现WEB应用转换翻译功能，支持HTTP、HTTPS、POP3、SMTP等协议（需提供界面截图，加盖投标人公章） |
| 翻译溯源审计 | 支持代理转换日志溯源审计功能，包括用户访问时刻、用户使用的IP、访问的URL等信息，支持XFF协议 |
| 外链天窗处理 | 解决外链天窗问题，支持外链过滤器添加/删除/修改，支持网站页面静态和动态外部链接的识别和处理（需提供界面截图，加盖投标人公章） |
| DNS防火墙 | 支持禁止DNS ANY类型请求，支持防止DDOS攻击和放大攻击，支持基于IP或域名进行请求限速，支持自定义防火墙规则（需提供界面截图，加盖投标人公章） |
| 恶意域名过滤 | 支持DNS防火墙响应策略，支持恶意域名的识别和过滤，针对域名进行阻断，支持域名不存在/存在无响应/不启用策略/强制TCP/丢弃/域名劫持等操作（需提供界面截图，加盖投标人公章） |
| 域名一致性检测 | 针对域名劫持，支持对重点域名的资源记录进行监测，同时定义重点域名对应的IP地址群，当有变化的时候，且变化后的内容不在给定的IP地址群中，则输出日志，发送告警信息（需提供界面截图，加盖投标人公章） |
| 认证要求 | 产品具有销售许可证、软件著作权证书、3C认证证书、工信部电信设备进网许可证、安全漏洞覆盖测试证书等 |
| 具备IPv6 Ready第二阶段核心协议金牌认证证书、具备中国国家信息安全（ISCCC）产品认证证书、等保三级测评证书等 |

## 4.6 虚拟化安全软件

| **技术指标** | | **指标要求** |
| --- | --- | --- |
| 推举品牌 | | 山石、亚信、奇安信等 |
| 云环境适应性 | 虚拟化环境 | 支持VMware 等标准环境 |
| 云平台依赖性 | 无需安装额外插件或Agent |
| 耦合性 | 在网络侧解决安全防护问题，云平台和业务虚机零干扰 |
|  | 系统语言 | 支持中UI管理 |
| 构架设计 | 系统健壮性 | 管理，主控和业务处理分离的分布式架构，主控模块支持HA模式，业务服务模块采用多任务并行处理方式，支持自动Bypass功能，具有自动探测和修复能力 |
| 能实时监控系统各个模块组件的状态，能克隆备份管理模块，模块间采用非公有协议进行通信，具有可信主机访问控制列表，限制管理主机的IP地址和管理方式（针对Telnet，SSH，HTTP，HTTPS访问行为进行控制），提供产品界面截图有效 |
| 规模扩展性 | 一套产品最大可统一管理200台物理主机的安全防护，此次数量20颗物理CPU |
| 业务连续性保障 | 支持会话同步能力，安全防护可随虚机迁移而自动跟随，确保安全防护的持续性和业务连续性（可要求进行FTP/SSH方式的业务测试），支持在线升级方式，提供产品界面截图有效 |
| 网络环境适应性 | 虚拟化网络适应性 | 支持VMware VSS/VDS环境，支持OpenStack OVS环境 |
| 数据传输模式 | 支持标准长度的以太网帧传输，同时也支持超大帧（Jumbo Frame）传输 |
| 部署模式 | 支持透明旁路和串接两种模式，不改变原有网络的三层结构 |
| 引流控制 | 以虚机为对象，按需引流，安全防护功能仅在本地宿主机内的虚拟网络环境下完成，而无需将业务流量额外牵引至物理网络环境或别的宿主机中处理安全事务。 |
| 环境检查 | 可针对云平台的环境进行部署前的诊断和检查，为产品上线准入提供参考，提供产品界面截图有效 |
| 虚拟资产管理 | 虚拟机管理 | 自动同步云平台上所有虚拟机的名称，所属宿主机，网络适配器数量和IP |
| 自动更新虚拟机的启、停、增、减和修改等动作的变更结果 |
| 虚拟网络管理 | 自动同步云平台上所有业务网络信息，以及所连接的虚机数量和清单 |
| 自动更新虚拟网络的增、减和修改动作的变更结果 |
| 宿主机管理 | 自动发现云平台上所有宿主机IP和CPU信息，跟踪安全服务模块的部署情况 |
| 自动更新宿主机的启、停、增、减和修改等动作的变更结果 |
| 可视化 | 视图监控和统计能力 | 能发现统计云平台主要资产，并实时更新，提供流量、威胁、应用维度的TOP排名，支持对相关操作事务进展进行实时跟踪审计，支持对接入服务的虚拟机进行全方位的网络流量监控 |
| 交互模型图形化呈现 | 资产分布可视化，可将云内虚机和网络资产进行逻辑拓扑方式的呈现 |
| 账号角色维度可视化。在VDI场景下，可基于账号和角色名称的逻辑拓扑呈现 |
| 业务交互关系可视化。支持以逻辑拓扑图的方式展示可视化效果，拓扑图中可展示出虚拟机之间的互访关系，帮助管理员规范安全域划分，提供产品界面截图有效 |
| ★业务流向可视化。可将业务访问方向呈现在逻辑拓扑关系中，从而辨别出内-外/外-内的交互关系，提供产品界面截图有效 |
| 业务应用类型可视化。可将云平台内的虚机所产生的应用服务进行统计，并能在逻辑交互关系中定位和跟踪。。 |
| 业务流量可视化。可将云平台内的虚机所产生的网络流量进行全方位统计，并在逻辑交互关系中呈现。 |
| ★网络威胁可视化。可将云内产生的威胁事件通过逻辑交互关系进行可视化呈现，以此跟踪攻击源/受害者、威胁事件的发起源，受害者，扩散范围等情况，提供产品界面截图有效 |
| 视图操控方式 | 可基于IP地址，流量，防护状态，虚机和网络名称，应用类型，威胁名称/类型/安全级别等条件不同组合关系控制视图呈现效果 |
| 视图风格可与不同的管理员账号关联，支持鼠标的拖拽，缩放，以及右键对虚机/网络加防护的操作 |
| 云内风险评估报表 | 向用户提供云网络安全状况、网络流量和云内安全风险三个方面的运行情况评估，支持手工/定时周期式报表生成和输出能力。 |
| 基础防火墙功能 | 策略管理 | 提供在非NSX环境下，大二层网络内的东西向网络流量安全防护能力，且除产品自身外不需其他组件 |
| 提供在NSX环境下大二层网络内的东西向网络流量安全防护能力 |
| 支持L2-7层防火墙控制功能 |
| 安全防护功能基于白名单模式（即缺省所有数据阻断控制） |
| 支持策略助手功能，安全策略的配置可依据历史通讯数据，基于IP/端口/应用维度筛选和聚合条件匹配，半自动化的辅助管理员完成安全策略的精细化配置 |
| 基于虚机名称为对象的安全策略控制，且支持通配符方式定义动态地址簿 |
| 基于端口组名称为对象的安全策略控制 |
| 基于AD账户名称为对象的安全策略控制，可与Windows Active Directory联动 |
| 支持基于时间表的安全策略控制，支持对防火墙策略命中次数进行统计，支持会话、新建连接的限制，支持ALG功能，支持策略冗余检测，对策略重叠性检查 |
| 其他管理平台联动 | 支持与FireMon和Algosec统一安全策略管理平台联动，自动整理收敛配置 |
| 应用识别 | 技术特性 | 具备全新一代基于应用特征、行为和关联信息的应用识别 |
| 特征库 | 应用特征库不少于3000种，支持在线实时升级和线下手工升级 |
| 控制方式 | 可依据具体应用和应用类别维度的控制，并支持用户自定义应用 |
| 攻击防护 | DoS/DDoS识别防护能力 | 支持抵御所列所有攻击类型，包括：DNS Query Flood、SYN Flood、UDP Flood、ICMP Flood、Ping of Death、Smurf、WinNuke，TCP Split Handshake，动作支持记录、阻断两种模式。支持对不同安全域设定不同阈值和处理模式，提供产品界面截图有效，支持多种畸形报文攻击防护 |
| 网络行为检查 | ★支持端口扫描防护，支持指定虚机的ARP攻击防护（包括ARP欺骗和投毒），可通过可视化交互关系追踪攻击源和目标，提供产品界面截图有效 |
| 运维管理 | RESTAPI管理 | 支持通过RESTAPI接口进行配置和查看地址簿、病毒过滤、入侵防御、安全策略、接口配置，可向云平台提供深度整合的开发接口 |
| 故障排查 | 支持网络连通性的在线侦测功能，提供虚拟化网络在线抓包能力，并可导出pcap格式的抓包文件，为虚拟化环境下的运维提供有效助力，提供产品界面截图有效 |
| 审计功能 | 支持基于标准SYSLOG以及二进制的日志两种格式；且支持负载均衡方式的日志发送模式 |
| 支持SNMP监控、NTP功能、邮件告警功能 |
| 配置文件保存 | 支持不少于10个配置文件并存，并支持配置文件的中文备注 |
| 产品成熟度 | 产品上市时间≥3年 |
| 资质 | 资质 | 具有虚拟化微隔离系统著作权，以及相关测试报告；（需提供复印件证明） |
| 具备公安部办法的虚拟化云安全防火墙销售许可证三级；（需提供复印件证明） |
| 为保证产品兼容性所投产品品牌必须为VMware认证的partner。（提供VMware官网链接证明及截图。） |

4.7 SSL VPN

| **技术指标** | **指标要求** |
| --- | --- |
| 推举品牌 | 深信服、天融信、华为等 |
| 配置要求 | 吞吐量≥1.5Gbps，并发会话数≥160万；支持 SSL VPN 最大并发用户≥2600个；网口≥6个千兆电口+2个千兆光口，≥2U标准设备  配置SSL VPN接入同时在线用户数800个 |
| 部署方式 | 支持IPv6/IPv4协议下的网关模式、单臂模式、主备模式、集群模式的部署 |
| 基本特性 | WebVPN支持跨平台免插件访问，支持泛域名发布Web资源，简化资源发布和访问。 |
| 在windows系统上，能同时安装并运行多个VPN客户端，满足有多套VPN的客户同时登录VPN |
| ★产品应提供环境检测、自动修复工具，支持对Windows的环境兼容性一键检测能力，以及对检测结果进行一键修复的能力，避免由于用户操作系统环境存在问题影响SSL VPN的使用，减轻运维工作。（提高截图证明并加盖厂商公章） |
| 终端安全 | 产品必须支持防中间人攻击，支持用户终端登录前、登陆后的安全性检测。 |
| 支持客户端注销后自动清除所有缓存、Cookies、浏览器历史记录、保存的表单信息，实现零痕迹访问 |
| 支持VPN专线功能，可配置用户在接入SSL VPN的同时，断开与Internet其他连接 |
| 权限、服务器安全 | 产品应具有用户/用户组细粒度的权限分配功能：可以针对被访问资源的IP地址、端口、提供的服务、URL地址等进行权限控制；针对同一B/S资源，可对不同用户做到细致到URL级别的授权。 |
| 针对服务器地址保护方面，可支持SSLVPN资源列表界面上的用户授权资源隐藏；针对B/S应用，可进行URL地址伪装，防止服务器真实IP地址泄露 |
| 身份认证 | 产品必须支持Local DB 、USB KEY、短信认证、硬件特征码、动态令牌、数字证书认证、LDAP、RADIUS、等认证方式；可针对用户/用户组设置认证方式的与、或组合，可进行用户名/密码、LDAP、USB KEY、硬件特征码、短信认证或动态令牌的多因素捆绑认证 |
| 支持与阿里钉钉、企业级微信绑定，实现其内置OA的安全接入 |
| 设备内部必须支持自建CA中心，便于数字证书认证平台搭建；  支持与基于PKI体系的第三方CA进行结合认证 ，可根据CA某字段将通过CA认证的用户自动映射到指定用户组，方便进行权限授权配置；支持CRL证书撤销列表。  ★单台VPN设备可扩展同时支持5套以上CA根证书；（提供证明截图） |
| 支持主流的短信验证码认证对接（例如，腾讯云、阿里云短信网关认证）；  支持对接多个HTTP(S)辅助认证（HTTP(S)验证码认证、HTTP(S)令牌认证）；  支持用户、用户组主要认证完成后，继续通过辅助认证（HTTP(S)验证码认证、HTTP(S)令牌认证）； |
| 高速性 | 必须支持至少4条以上的外网多线路配置；并在设备单臂部署模式下，多线路接入前置网关，仅依靠SSLVPN设备同样可实现SSLVPN接入用户的多线路自动优选功能 |
| 支持HTP快速传输协议，大幅优化无线环境（CDMA、GPRS、WIFI、3G）、高丢包、高延等恶劣网络环境下传输速度及效率；支持根据网络境自动选择并切换至最优的传输协议（提供界面配置截图并加盖厂商公章） |
| 针对B/S资源支持WebCache技术，动态缓存页面元素，提高Web页面响应速度。支持流缓存技术，实现网关与网关、网关与移动客户端之间进行多磁盘、双向、基于分片数据包的字节流缓存加速，削减冗余数据，降低带宽压力的同时提高访问速度；支持共享流缓存功能，实现多分支网关在总部共享流缓存数据，提高流缓存效果（提供界面配置截图并加盖厂商公章） |
| 支持整体网关配置的本地及远程备份、恢复功能；支持SSLVPN配置的单独备份、恢复功能，并支持历史配置的回滚 |
| 稳定性、可扩展性 | 支持基于自组域简化部署VPN网络的方法，即当有多台设备处于VPN网络中时，通过连接任意节点的VPN设备，即相当于连入整个VPN网络。 |
| 产品必须支持经过集成的，基于Android IOS平台的第三方软件开发包（SDK），并实现基于Android IOS平台第三方应用软件（APP）。支持针对移动APP的VPN安全代码的自动封装，实现App应用的安全加固 |
| 远程应用 | 产品必须在Windows和MAC操作系统下支持远程应用发布功能 |
| 远程应用发布必须支持负载均衡策略，即当存在多台终端发布服务器时，可以根据服务器可用会话数、CPU、内存、I/O、综合性能等指标，智能的将用户分配到不同的终端服务器。 |
| 远程应用发布数据传输过程中使用SSLVPN协议加密，保证了数据传输的合法性和安全性； |
| 支持改写WindowsRDP协议，经改写的协议必须独立于OS运行环境，避免跨平台兼容性，针对图像数据，服务端必须支持有损压缩算法；服务端必须能够支持过滤动态内容（gif/flash/video）以减少传输流量，且根据客户需要配置。 |
| 资质要求 | 提供中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》，提供证书复印件 |
| 具备中国信息安全测评中心颁发的《信息技术产品安全测评证书》品类：VPN网关，级别：EAL3+，提供相应证明材料 |
| 提供公安部信息安全产品检测中心颁发的《GA/T 686-2007信息安全技术 虚拟专用网安全技术要求》三级或三级以上检测报告（三级以上为四级、五级），提供相应证明材料 |
| 厂商具备软件开发成熟度CMMI 5级认证，提供证书复印件、可查询链接及查询官网截图并加盖厂商公章 |
| 厂商应是国家互联网应急响应中心网络安全应急服务国家级支撑单位，提供证明材料、可查询链接并加盖厂商公章 |
| 服务要求 | **SSL VPN需与学校智慧化校园平台做对接，中标方无条件配合一切相关对接问题，接口必需对学校免费开放。** |

4.8 IT运维管理软件

| **技术指标** | **指标要求** |
| --- | --- |
| 推举品牌 | 网瑞达、华为、华三等 |
| 种类和范围 | 1.支持监控多种网络资源：有线设备、无线设备、安全设备、服务器、动环设备、存储设备、标准应用、中间件、数据库以及虚拟化；  2.支持多厂商：思科、华三、华为、神州数码、锐捷、中兴、迈普、戴尔、IBM、惠普、联想、微软、浪潮、Oracle、VMware等； |
| 指标种类 | 1. 支持用户自定义任何可以采集的指标并进行监控； |
| 指标管理 | 1.支持对指标项进行全局设置（是否采集、是否监控、是否记录、采集周期）和个性化设置，个性化设置优先级高于全局设置；  2.支持对指标项原始数据进行全量存储、分片索引；  3.支持对指标项的历史数据进行图表展现、批量导出； |
| 识别与发现方式 | 1.支持多种资源添加方式  2.支持通过ICMP、SNMP(v1,v2c,v3)、WMI等多种协议对资源进行自动扫描；  3.支持定期进行计划任务扫描以便及时发现新加入网络的资源；  4.支持自动发现资源信息变更，包括设备型号、描述、接口信息等；  5.支持无agent监控基础应用、中间件、数据库；  6.提供网络检测小工具，例如PING检测、Traceroute追踪、Telnet/SSH等，要求提供系统截图并加盖厂商公章； |
| 可自动识别和发现的资源信息 | 1.支持自动获取有线设备的名称、类型、制造商、型号、接口、SN号、软硬件版本、固件版本、堆叠信息；  2.支持自动获取无线控制器(AC)的名称、制造商、型号、接口、在线AP、离线AP；  3.支持自动获取无线接入点(AP)的名称、IP、MAC、所属控制器IP、上联交换机IP、上联交换机接口、终端数量；  4.支持自动获取AP下连接终端的IP地址、MAC地址、连接AP名称、无线工作模式、信号质量、频率、信道号、出入流量、出入速率、连接时长；  5.支持自动获取服务器名称、制造商、型号、操作系统；  6.支持自动获取虚拟化资源之间的映射关系；  7.支持自动获取虚拟化平台中物理主机的厂商、型号、存储等信息；  8.支持自动获取存储设备的名称、厂商、型号、磁盘、LUN、RAID； |
| 资源管理和操作 | 1.支持资源列表的自定义视图；  2.支持对资源监控的批量开启/关闭；  3.支持直接在WEB页面展示有线设备的MAC/ARP表  （恢复）5.支持开启/关闭有线设备接口；  6.支持自定义有线设备接口的位置描述；  7.支持自定义AP的位置描述；  8.支持重启AP； |
| 自定义Portal | 1.支持自定义Portal，将用户关注或常用的内容添加至Portal（统计图、排行、拓扑等）；  2.支持提供Portal的默认模板；  3.支持拖拽方式调整Portal布局；  4.支持自定多个Portal进行全屏轮播展示；  5.支持自适应不同分辨率下的屏幕； |
| 拓扑 | 1.支持自动计算设备间的连接关系  2.支持NDP、CDP、MSTP、STP、LLDP等协议、支持复杂网络下融合MAC，ARP，XDP多元信息的网络拓扑自动发现算法计算拓扑  3.支持以不同颜色实时显示设备和链路的运行状态、历史流量数据；  4.支持自定义拓扑节点和链路的展现方式  5.支持层级拓扑，子拓扑中设备状态可透传至父拓扑；支持导出拓扑的矢量图； |
| 真实面板 | 1.支持根据设备真实形态绘制的设备面板，设备接口、指示灯均与真实面板一致；  2.提供各厂商不同型号交换机、路由器、AC、防火墙、服务器的真实面板，可根据用户需求快速扩充新的展示面板图；  3.支持直接在真实面板上开/关接口、查看接口状态、当前流量、历史流量图；  4.支持展现板卡面板，并分层展现堆叠设备； |
| 告警策略 | 1.支持通过系统内阈值触发告警，支持通过设备日志触发告警，支持通过第三方系统推送触发告警；  2.支持系统针对各类指标项预定义合理的全局告警阈值；  3.支持对特定的资源设定个性化阈值，个性化阈值优先级高于全局告警阈值；  4.支持持续性告警，可设置某事件持续发生一段时间后产生告警；  5.支持频率告警，可设置某事件在某段时间内发生次数达到阈值时产生告警；  6.支持复合告警，由两个子条件组成，每个子条件中可设置不同告警类型和告警资源；当两个子条件同时满足时触发告警  7.支持将所有告警在统一的界面展示，可通过资源、时间、类型、等级、状态、告警内容查询告警；  8.支持告警状态的自动恢复、手工恢复，支持对已发生的告警进行标记以便日后处理； |
| 告警通知 | 1.支持微信、短信、邮件、首页闪烁提示等方式进行告警通知，自带微信告警服务平台，只需关注即可使用；  2.支持根据不同的告警类型和对象选择不同的告警接收者； |
| 告警分析 | 1.支持告警频率分析，对不同资源的告警次数及告警类型进行统计，评估资源故障率，要求提供系统截图并加盖厂商公章；  2.支持告警原因分析，自动分析关联告警，提取关键根源告警信息，实现告警收敛，避免大量告警淹没关键信息，并提供故障处理建议； |

## 4.9校园网络项目集成服务

| **技术指标** | **指标要求** |
| --- | --- |
| 人员要求 | 项目经理1名  项目实施人员至少3名  后续驻场人员1名 |
| 网络梳理 | 中心机房网络拓扑梳理、设备信息统计、网络地址信息统计，提供相应纸质文档和电子文档 |
| 网络中心机房与各教学楼、办公楼等网络互连信息梳理，涉及交换机接口信息、网络地址规划信息；旧数据中心服务器设备、网络设备迁移至新数据中心，需重新划分网段，并对服务器设备、网络设备网络地址进行变更，调试所有相关设备，使其正常运行，并提供迁移梳理后的相应纸质文档和电子文档材料 |
| 每个楼的楼层弱电间网络拓扑梳理、设备信息统计、网络地址信息统计，提供相应纸质文档和电子文档 |
| 每个办公室、教室、实验室到楼层弱电间网络信息统计、设备接口信息统计，提供相应纸质文档和电子文档 |
| 对于当前网络设备配置问题和线缆问题进行排查及解决，涉及硬件问题的列出设备运行状况及解决方案建议，提供纸质文档和电子文档 |
| 所有信息统计汇总及相关设备配置信息梳理，例如网络拓扑、信息点位置等，提供相应纸质文档和电子文档 |
| 网络规划 | 对于当前校内网络信息具体网络地址段落规划，例如分为设备管理段、教室段、办公室段、数据中心段，并涉及到相关的教室办公室、路由器、打印机等，并提供分配的网段后续的预留地址，提供相应纸质文档和电子文档 |
| 优化出口路由策略，最大化利用现有运营商线路，确保每个IP正常访问本校购买的图书等数据资源（如万方、知网等数字资源网站）。 |
| 对于当前校内教育公网地址、运营商公网地址重新规划，提高校内网络安全，提供相应纸质文档和电子文档 |
| 旧机房所有连接至核心的所有线缆均割接至新机房核心交换机，提供相应光纤、网线割接规划表。 |
| 对校内网络设备用途规划例如接入、汇聚、核心等区域规划，并按照新规划重新变更网络结构，提供变更后网络拓扑和规划图 |
| 基于当前网络设备及网络要求情况，对网络设备配置进行调整并对原配置进行备份，满足当前网络使用需求；提供原网络设备配置文件和新配置文件 |
| 网络访问策略制定及防火墙安全配置，如区域访问安全策略、网络流量带宽、端口限制策略等 |
| 网络地址重新规划，可能会引起个教学楼、办公室网络故障，开学期间会报修比较频繁，因此需提供细致的网络相关使用、管理操作培训，确保教学办公正常运行，并提供相应纸质文档和电子文档 |
| 新旧数据中心对接 | 割接前现场勘察实地情况，提供搬迁后的硬件设备机柜拓扑图及各设备供电功率信息表 |
| 线缆割接：  1、原三楼数据中心机房教学区光缆（单模）与新数据中心接入接配线架光缆做熔接，共120芯，采用直熔方式，并提供相应辅材。  2、从新数据中心接入间到冷池配线柜，做光纤（单模）对接，配置相应长度光缆，配上光纤盘及耦合器（品牌要求德特威勒，与新数据中心现有品牌一致，光纤盘要求米白色，耦合器颜色要求黄色），共156对（312芯）；做超6类网线对接，配置相应长度超6类网线48根，并配置相应的网线接口模块（品牌要求德特威勒，与新数据中心现有品牌一致）  提供相应光纤、网线割接规划表及配套辅材线缆等。 |
| 现有服务器、存储等设备搬迁和统计，现有虚拟化平台所有系统迁移至新虚拟化平台，并提供相关备份措施，将现有环境进行网线接口梳理打印，配合校方进行机器关机下架，搬迁至新数据中心，提供相应统计信息和接口信息的纸质文档和电子文档。 |
| 网络设备配套拆卸，板卡、模块、电源线等配件标签整理规范，统计信息，形成纸质文档和电子文档 |
| 搬迁后按规划上架设备，待所有设备上架无误后加电自检，在自检过程中出现错误，按规范进行排错，配合学校人员修改服务器及存储相应配置，使其能够在新网络环境中运行，并将事件整理成文档 |
| 配合校方进行网络验证、系统验证，如重要系统出现故障，则以割接前的备份进行恢复 |
| 线路整改工程 | 学校公共机房共23间，每间铺设两对光纤线路上联接入到新数据中心配线间，再由配线间接入到冷池配线机柜，配置相应配线架（**品牌要求德特威勒，与数据中心现有品牌一致**）及其他辅材、光电转换模块等。 |
| 驻场工程师资质要求 | ★要求对IIS、Tomcat、数据库、DNS、DHCP、Nginx等网络服务精通；对Window、Linux等操作系统精通；该工程师必须同时具备中级网络工程师认证（例如CCNP/HCNP等认证及以上）和虚拟化工程师认证（例如VMware VCP等认证及以上）能力，提供该工程师的相关证书和一年及以上公司的社保缴费证明； |

**注：以上设备必须支持IPV6,软硬件设备都必须支持等保2.0。**

4.10运维辅助设备

|  |  |  |
| --- | --- | --- |
| **设备名** | **技术指标** | **指标要求** |
| 自动双面激光打印机 | 功能 | 打印；扫描；复印 |
| 技术类型 | 黑白激光 |
| 幅面 | A4 |
| 连接方式 | 有线，USB |
| 自动双面打印 | 含输稿器，支持自动双面打印 |
| 复印分辨率 | 600x600dpi |
| 扫描分辨率 | 硬件： 高达300x300dpi(彩色和黑白，ADF)，高达600x600dpi(彩色、平板)，高达1200x1200dpi(黑白、平板) |
| 打印分辨率 | 黑白(最佳)： 高达1200x1200dpi； 黑白(正常)： 高达600×600d、1200(1200dpi品质) |
| 内存 | 256MB |
| 数量 | ２台 |
| 网络服务器运维调试终端平板 | 类型 | 二合一平板 |
| 运行内存 | >=16GB |
| 存储容量 | >=512GB SSD |
| 处理器 | >=i7-1065G7 4核 |
| 屏幕 | 12.3英寸 PixelSense显示屏 |
| 显示分辨率 | 2736\*1824dpi |
| 操作系统 | Windows 10 |
| 触控 | 支持触控笔，10点触控 |
| 数量 | 2套 |

4.11 交换机

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 推举品牌 | 华为、华三、锐捷等 |
| 交换容量 | 交换容量≥330Gbps |
| 包转发率 | 包转发率≥108Mpps |
| 端口类型 | ≥24个千兆电口，≥支持4个万兆SFP |
| 二层功能 | 支持MAC地址≥8K |
| 支持ARP表项≥2K |
| 支持4K个VLAN，支持Voice VLAN，基于端口的VLAN，基于MAC的VLAN，基于协议的VLAN  支持VLAN内端口隔离  支持Smart link |
| 支持端口聚合，每个聚合组至少8个端口,支持跨设备链路聚合。 |
| 路由功能 | 支持静态路由，RIP、RIPng |
| 安全功能 | 支持防止DOS、ARP攻击功能、ICMP防攻击  支持端口隔离、端口安全、Sticky MAC  支持DHCP Relay、DHCP Server、DHCP Snooping 支持AAA认证，支持Radius、HWTACACS、NAC等多种方式 |
| 支持基于第二层、第三层和第四层的ACL  支持IP/Port/MAC的绑定功能 |
| 可靠性 | 支持G.8032开放环网协议 |
| 管理维护 | 支持SNMP v1/v2/v3、Telnet、RMON  支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理  支持集群管理 |
| 节能 | 支持802.3az能效以太网节能环保 |

4.12 上网行为管理设备

|  |  |
| --- | --- |
| 产品要求 | 原网康NI7000-SG由于产品授权已过期，升级原有产品3年授权，含3年服务，**因原厂商支持购买3年授权可免费升级硬件服务，本次升级硬件到对应档次产品。** |
| 参数 | 提供替换主机（型号：NI7000-S）一台，标准2U机箱，标配主机带1个Console口 、1个HA接口，1个管理网口，4个千兆电口，4个千兆光SFP接口，另有2个扩展板卡插槽，1T机械硬盘存储，冗余电源。建议5G带宽以下网络环境使用；最大并发连接数为350万;最大新建连接数为10万/秒；  主机含3年软件版本与协议库升级服务  主机含3年的Web安全防护服务使用授权（含杀毒，恶意URL防护，威胁情报订阅服务）；  主机含3年硬件维保及远程技术支持服务（400电话支持、Email支持）。 |

4.13 远程USB服务器

|  |  |
| --- | --- |
| 产品要求 | 远程USB服务器通过IP来绑定加密狗，且USB端口数可以大大扩容，用来解决我校虚拟化平台服务器USB端口数量过少，加密狗不够插，虚拟机漂移后找不到加密狗的问题。 |
| 推举品牌 | 阿谱斯、淄博洛克、盛讯美恒等 |
| 参数 | 不少于16个标准USB2.0接口，兼容USB3.0及USB1.0/USB1.1设备  每个USB端口电流不低于800毫安；  标准1U机架式安装，静音无风扇设计；  双网口，需独立MAC地址；双电源冗余输入；  USB端口带指示灯显示  每个USB端口可独立控制加电/断电  需支持windows及Linux操作系统（Windows 64位操作系统驱动必须带数字签名）  需兼容所有USB类型设备，包括HID人机交互设备、通信类设备，如智能手机、单板，存储类设备以及同步设备如摄像头等；以及U盾Ukey加密狗加密锁等所有类型USB设备；  支持分组，每个USB端口设备可绑定到不同虚拟机IP地址；（支持虚拟机飘移），重新分组后，立即生效，不能重启设备；  支持VPN  支持SSL,TLS加密传输；  支持客户端主机重启后自动连接  支持网络断开恢复后自动重联  支持服务端强制断开已经连接的设备  支持端口连接数据量与速度显示  客户端能显示每个USB端口连接设备的PID,VIP串号等信息；  支持vmware vsphere、redhat KVM、fusionsphere等虚拟化技术；  需提供命令接口供程序进行自动化调用；  通过FCC/CE认证；  带微软WHQL认证； |

4.14服务器内存升级

|  |  |
| --- | --- |
| 产品要求 | 原虚拟化服务器内存由原来的128G升级到256G，共3台。  原教务系统数据库服务器内存由原来的64GB升级到128GB，共2台。 |
| 参数 | 1.原虚拟化平台服务器为ThinkServer RD640，共3台。  原配置内存型号为：8\*16GB R-ECC 1866 DDR3  内存插槽为20个。  现要求升级服务器内存，单台服务器上所有内存型号参数相同，每台由原来的128GB升级到256GB。  服务要求：**完成虚拟化服务器的内存升级，确保内存添加后虚拟化平台的正常运行。**  2.原教务系统数据库服务器为浪潮NF8465M4，共2台  原配置内存型号为DDR4，每台内存共64GB  现要求升级服务器内存，单台服务器上所有内存型号参数相同，每台服务器升级到128GB内存  服务要求：**完成数据库服务器的内存升级，确保内存添加后原服务器的正常运行。** |

**4.14 售后服务要求**

* 1. 所有产品三年免费维保，提供现场、电话、传真、电子邮件、互联网等多种方式的维护服务。
  2. 需保证在半小时内对学校所提出的维护要求做出响应，并在做出响应1小时内派出工作人员进行故障排除，投标供应商在投标文件中提供相应的书面承诺函。
  3. 中标供应商需提供免费上门安装调试系统服务。在系统部署完成后、正式使用前，中标供应商提供系统安全测试报告，同时需提供相应配置的详细说明书，现场对学校相关人员做不少于2天的技术培训。
  4. 中标供应商必须全程跟踪项目实施进度，同时有需要与智慧校园建设项目配合的地方需无条件全力配合。
  5. 中标供应商必须制定项目实施计划，精确编排实施进程表，有序实施。

**评标办法前附表**

**表4.1 初步评审表**

|  | **评审因素** | **评审标准** |
| --- | --- | --- |
| 形式评审标准 | 投标人名称 | 与营业执照、资质证书一致 |
| 投标文件签字盖章 | （1）招标文件中有单位名称和法定代表人或其委托代理人签字落款的投标文件必须逐页加盖单位公章，并由法定代表人或其委托代理人逐页手签或加盖法人印章。  （2）除上述文件以外的其他投标文件组成部分必须加盖骑缝章（骑缝章必须覆盖所有投标文件），或由法定代表人或其委托代理人逐页手签。  （3）投标文件凡出现投标人单位落款的地方应盖单位公章，如使用投标专用章、业务专用章的，应提供公章对投标专用章授权说明。  （4）所有投标文件应统一密封在坚固、易于密封、搬运的密封箱/袋中。密封袋/箱由投标单位用自制封条在开口处密封，封条上加盖骑缝公章和法定代表人或授权代理人签字或盖章。 |
| 报价唯一 | 只能有一个有效报价 |
| 资格评审标准 | 独立法人 | 投标人必须在中华人民共和国境内依法注册、具有独立法人资格，有一定注册资本；须提供营业执照、组织机构代码和税务登记证复印件；如投标人已办理“三证合一”，则只须提供三证合一后的营业执照复印件，且营业范围包含本次投标内容。 |
| 一般纳税人 | 投标人须为增值税一般纳税人，能够开具增值税专用发票。须提供盖有“增值税一般纳税人”章的税务登记证副本复印件或提供税务机关颁发的增值税一般纳税人资格认定文件复印件或投标人提供承诺书。 |
| 服务能力 | 投标人须具备完整的售后服务体系、具有快速响应维护能力，可负责质保期内外的服务工作，须提供书面承诺书。 |
| 资信能力 | 资信能力证明材料，如资信等级证书、信用等级证书、资信证明等文件复印件。 |
| 质保承诺函 | 投标人须提供所投产品的授权函和三年质保承诺函原件。 |
| 联合体 | 本项目不接受联合体投标。 |
| 其他要求 | (1) 投标人须提供近三个月任意一个月份(不含投标当月)的财务状况报告（资产负债表和利润表）或由会计师事务所出具的近两年中任意一个年度的审计报告和所附已审财务报告的复印件；  (2) 投标人须提供近三个月中任意一个月份(不含投标当月)的依法缴纳税收的相关材料（提供相关主管部门证明或银行代扣证明）复印件；  (3) 投标人须提供投标代表人近三个月 (不含投标当月)的依法缴纳社会保障资金的相关材料（提供相关主管部门证明或银行代扣证明）复印件；  上述第（1）、（2）、（3）三项，如投标人遇国家相关政策规定而不具备的，必须提供相关政策规定或相关单位出具的有效证明复印件。 |
| 不得存在的情形 | 投标人不得存在下列情形之一：  (1) 为招标人不具有独立法人资格的附属机构（单位）；  (2) 为本招标项目提供招标代理服务的；  (3) 被责令停业的；  (4) 被暂停或取消投标资格的；  (5) 财产被接管或冻结的；  (6) 在最近三年内有骗取中选或严重违约或重大工程质量问题的。  (7) 单位负责人为同一人或者存在控股、管理关系的不同单位，不得同时参加本招标项目投标。  (8) 法律法规限定的其他情形； |

**评分标准**

评标委员会将按照招标文件的有关规定和有关法律法规的规定，本着公平、公正、科学、择优的原则，对初步审查合格的投标进行以下各方面的综合评议。每个评委独立评分，所有评委评分的算术平均值, 加上以招标文件规定的方法计算出的价格分，即为每个投标人的最终得分。除价格分外，评委评分可保留1位小数，评标最终得分保留2位小数。

|  |  |  |  |
| --- | --- | --- | --- |
| 评估因素 | 价格 | 技术方案 | 商务 |
| 评估权重 | 30 | 40 | 30 |

**投标人资格要求**

1、符合《中华人民共和国政府采购法》第二十二条的规定；

2、投标人具有独立法人资格，提供有效的营业执照、税务登记证、组织机构代码证或三证一体证明文件；

3、投标人必须具有独立完成本次采购货物的供货、安装、调试、集成及相关服务的能力，中标后不允许分包、转包。

**评分标准**

|  |  |  |
| --- | --- | --- |
| **项目** | **子项** | **评分标准** |
| 价格(30分) | 价格（30分） | 评标基准价为所有有效投标人的有效报价的算术平均值，与基准价相比较，有效报价与基准价相等的投标人其报价得分为30分；有效报价每超出基准价的l％扣0.5分，每低于基准价的l％扣0.3分，最多扣5分。 |
| 技术方案  (40分) | 技术参数（26分） | 设备技术参数全部满足招标要求的得满分26分，有一项负偏离扣一分，打★号为关键指标项，有一项负偏离扣2分，扣完为止。 |
| 实施人员要求（2分） | 本项目提供专职项目经理1人，3年内主持过相关项目（提供支撑材料），施工过程中不得换人，提供至少一年社保证明，得1分。  投入本项目的人员具备：网络工程师（CCNP或CCIE）及以上相关技能认证得1分。 |
| 技术方案及现场技术讲解（12分） | 评委根据投标人现场技术讲解（8-10分钟）项目人员组成及实施方案等评分，最优的得该项最高分，其他酌情评分：  项目实施方案12分：评委根据投标人现场讲解本次项目采购软硬件设备安装调试方案、新旧对接方案、校园网地址整改方案、施工组织及时间进度方案以及配套软件系统，并结合机房现有网络情况的联调方案等的科学性、完整性、合理性等情况评分，最优的得9～12分，一般得5～8分，其他得1～4分。 |
| 商务  (30分) | 企业资质（10分） | 投标人提供信用评级机构出具的信用评级报告AAA级得2分，AA级的得1分，其他不得分；  投标人具有主流网络厂商认证的专家级网络工程师（如CCNP、HCNP等同级别证书），并提供近三个月社保证明，每提供一名得1分，最多2分；  并提供最高级网络工程师（如CCIE、HCIE等同级别证书），提供近六个月社保证明，每提供一名得2分,最多2分；  投标人具有ITSS运维资质证书的得1分，提供复印件并加盖单位公章，原件备查。  投标人具有信息安全服务资质认证证书的得1分，提供复印件并加盖单位公章，原件备查。  投标人具有ISO9001质量认证证书的得1分，提供复印件并加盖单位公章，原件备查。  投标人具有ISO20000信息技术服务管理体系认证证书的得1分，提供复印件并加盖单位公章，原件备查。 |
| 企业案例（12分） | 项目经验（数据中心机房建设相关类、非单一产品项目）：2016年1月1日以来供应商完成类似项目集成案例，提供合同,且单项合同（合同应能反映相关信息）金额≥100万的成功案例，每个案例提供完整合同复印件、验收报告的得2分，最多得12分（不提供验收报告的案例不得分），原件备查。 |
| 服务及培训（8分） | （1）项目培训方案1分：评委根据投标人提供培训方案的内容、价值等评分，最优的得1分，其他酌情评分;  （2）项目验收方案1分：评委根据软硬件设备测试方案、系统联调验收方案等评分，最优的得1分，其他酌情评分。  （3）根据投标人提供的售后服务方案，提供有针对性的符合用户需求的售后服务内容，由评委在各投标人之间横向比较，综合评价优秀得2分，良好得1分，未提供方案不得分。  （4）投标人提供售后服务三年，不加分，每超过1年加1分，最高得2分。  （5）提供每季度的巡检报告，以及相关优化建议和日常运维中的注意事项。**提供机房设备运维5万以上案例，提供合同复印件，原件备查**，合同应能反映相关信息，每一份合同得1分，最多得2分。 |