
项目编号：310151000250411101566-51232647

上海市崇明区教育局
崇明区教育网学校网络万兆全光网
改造项目
招标文件

业主方：上海市崇明区教育局

集中采购机构：上海市崇明区政府采购中心

2025年06月18日

2025年06月18日

目 录

第一章： 投标邀请

第二章： 投标人须知

第三章： 项目需求

第四章： 合同主要条款指引

第五章： 评审办法

第六章： 投标文件清单及投标文件有关格式

附件：

第一章：投 标 邀 请

根据《中华人民共和国政府采购法》之规定，上海市崇明区政府采购中心受委托，对上海市崇明区教育局崇明区教育网学校网络万兆全光网改造项目进行国内公开招标采购，特邀请合格的供应商前来投标。

一、合格的投标人必须具备以下条件：

1、符合《中华人民共和国政府采购法》第二十二条规定的供应商，未被列入“信用中国”网站(www.creditchina.gov.cn)失信被执行人名单、重大税收违法案件当事人名单和中国政府采购网(www.ccgp.gov.cn)政府采购严重违法失信行为记录名单的供应商。

2、根据《上海市政府采购供应商登记及诚信管理办法》已登记入库的供应商。

3、其他资格要求：

(1) 具备电子与智能化工程专业承包二级及其以上资质；

(2) 《安全生产许可证》（非本市企业安全生产许可证需备案）；

(3) 参加投标的供应商应具有健全的财务会计制度、有依法缴纳税收和社会保障资金的良好记录，须提供《财务状况及税收、社会保障资金缴纳情况声明函》；

(4) 本项目不接受进口产品投标；

(5) 本项目**不允许**联合体投标；

(6) 单位负责人为同一人或者存在直接控股、管理关系的不同投标人，不得参加同一合同项下的政府采购活动，提供股东组成基本情况表。

二、项目概况：

1、项目名称：崇明区教育网学校网络万兆全光网改造项目

2、招标编号：310151000250411101566-51232647

3、项目主要内容、数量及简要规格描述或项目基本概况介绍：对校校通网络出口进行升级改造。同时需要同步推进关键系统的商密建设，以确保网络性能的提升、安全审计的加强以及教学效能的全面提高，详见项目需求。

4、交付地址：上海市崇明区教育局指定地点。

5、合同履行期限：本项目建设周期为合同签订之日起 60 天完成交付使用，设备自验收合格之日起质保期 3 年。

6、采购预算金额：540 万元。

7、采购项目需要落实的政府采购政策情况：推行节能产品政府采购、环境标志产品政府采购。促进中小企业、监狱企业、残疾人福利性单位发展。规范进口产品采购政策。

三、招标文件的获取：

1、下载（获取）招标文件开始日期：**2025-06-19**，下载（获取）招标文件结束日期：**2025-06-26**，上午下载（获取）时间：**00:00:00~12:00:00**，下午下载（获取）时间：**12:00:00~23:59:59**。凡愿参加投标的合格供应商可在上述时间内下载（获取）招标文件并按照招标文件要求参加投标。

2、注：投标人须保证获得招标文件需提交的资料和所填写内容真实、完整、有效、一致，如因投标人递交虚假材料或填写信息错误导致的与本项目有关的任何损失由投标人承担。

四、投标截止时间及开标时间：

1、投标截止时间：**2025-07-10 10:00:00**。

2、开标时间：**2025-07-10 10:00:00**。

五、投标地点和开标地点：

1、投标地点：**上海政府采购网** (<http://www.zfcg.sh.gov.cn/>) 电子招投标系统网上投标。

2、开标地点：

上海政府采购网 (<http://www.zfcg.sh.gov.cn/>)；

上海市崇明区城桥镇翠竹路 1501 号四楼开标室（具体安排，详见当日四楼大屏幕提示）。届时请投标人代表持投标时所使用的数字证书（CA 证书）参加开标。

3、开标所需携带其他材料：

可以无线上网的笔记本电脑。

六、发布公告的媒介：

以上信息若有变更我们会通过“上海政府采购网”通知，请供应商关注。

七、其他事项

根据上海市财政局《关于上海市政府采购信息管理平台招投标系统正式运行的通知》（沪财采[2014]27号）的规定，本项目招投标相关活动在上海市政府采购信息管理平台（简称：电子采购平台）（网址：<http://www.zfcg.sh.gov.cn/>）电子招投标系统进行。电子采购平台是由市财政局建设和维护。投标人应根据《上海市电子政府采购管理暂行办法》等有关规定和要求执行。投标人在电子采购平台的有关操作方法可以参照电子采购平台中相关内容和操作要求办理。投标人应在投标截止时间前尽早加密上传投标文件，电话通知项目联系人进行签收，并及时查看电子采购平台上的签收情况，打印签收回执，避免因临近投标截止时间上传造成无法在开标前完成签收的情形。未签收的投标文件视为投标未完成。

八、联系方式：

采购人：上海市崇明区教育局

地址：崇明区城桥镇崇明大道 8188 号 3 号楼 4 层

邮编：202150

联系人：吴剑峰

电话：021-33802508 2025年06月18日

集中采购机构：上海市崇明区政府采购中心

地址：崇明区城桥镇翠竹路 1501 号 417 室

邮编：202150

联系人：徐洁

2025年06月18日

电话：021-69696988-8576

传真：021-69699633

电子邮箱：cmcgzx@163.com

第二章：投 标 人 须 知

一、项目需求情况：

详见《项目需求》。

二、交付方式：

详见《项目需求》。

三、验收方式：

详见《项目需求》。

四、付款方式：“★”

合同签订之后且全部到货安装完毕后，付款合同总额的 50%；整体验收通过后付款合同总额的 40%；正式投入使用 3 个月后再付 10%。

五、时间安排

1、投标截止及开标时间 **2025-07-10 10:00:00**。

2、纸质投标文件递交地点：上海市崇明区城桥镇翠竹路 1501 号 4 楼开标室。
(具体开标室安排，详见当日四楼大屏幕提示)

3、开标地点：

上海政府采购网 (<http://www.zfcg.sh.gov.cn/>)；

上海市崇明区城桥镇翠竹路 1501 号 4 楼开标室。(具体安排，详见当日四楼大屏幕提示)。届时请投标人代表持投标时所使用的数字证书(CA 证书)参加开标。

六 “★”、最高限价：540 万元。投标人必须使用人民币进行投标报价。

七 “★”、投标人应在规定的投标截止时间前上传投标文件，逾期未上传至指定系统的投标文件，不予受理。

投标文件必须有投标单位法定代表人或被授权人签字并加盖公章，法定代表人亲自参加投标的，须提交法定代表人证明及法定代表人的身份证原件扫描件，法定代表人不能亲自参加投标的，则被授权人应同时提交法定代表人证明、授权委托书及被授权人的身份证原件扫描件。如不能提供前述证(文)件，则取消其投标资格，本次投标文件有效期为自开标之日起 90 日。[供应商须保证所提交的

投标文件、资料的内容真实、完整、有效、一致，如递交虚假的投标文件、资料或填写信息错误导致的与本项目有关的任何损失由供应商承担。]

八、投标文件中请注明联系人、电话、手机、传真、E-mail 等。

九“★”、本次采购采用公开招标形式，参与投标的供应商须同时具备以下条件：

1、符合《中华人民共和国政府采购法》第二十二条规定的供应商，未被列入“信用中国”网站(www.creditchina.gov.cn)失信被执行人名单、重大税收违法案件当事人名单和中国政府采购网(www.ccgp.gov.cn)政府采购严重违法失信行为记录名单的供应商。

2、根据《上海市政府采购供应商登记及诚信管理办法》已登记入库的供应商。

3、其他资格要求：

(1) 具备电子与智能化工程专业承包二级及其以上资质；

(2) 《安全生产许可证》（非本市企业安全生产许可证需备案）；

(3) 参加投标的供应商应具有健全的财务会计制度、有依法缴纳税收和社会保障资金的良好记录，须提供《财务状况及税收、社会保障资金缴纳情况声明函》；

(4) 本项目不接受进口产品投标；

(5) 本项目不允许联合体投标；

(6) 单位负责人为同一人或者存在直接控股、管理关系的不同投标人，不得参加同一合同项下的政府采购活动，提供股东组成基本情况表。

十、其它具体要求：

1、最终供应商应严格遵守安全生产方面的相应规则，如因供应商原因引起的各类安全事故一切由供应商负责。

2、采购人将在开标后、评标结束前，通过“信用中国”网站(www.creditchina.gov.cn)、中国政府采购网(www.ccgp.gov.cn)查询相关投标人信用记录，并对供应商信用记录进行甄别，对列入“信用中国”网站(www.creditchina.gov.cn)失信被执行人名单、重大税收违法案件当事人名单、中国政府采购网(www.ccgp.gov.cn)政府采购严重违法失信行为记录名单及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的供应商，将拒绝其参与政府采购活动。

两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商的身份

共同参加政府采购活动的，将对所有联合体成员进行信用记录查询，联合体成员存在不良信用记录的，视同联合体存在不良信用记录。

3、本招标文件未明确之处应按国家相应的规范、规程执行。

不能满足上述要求的，采购人将保留解除合同、拒付款项之权力。

十一 “★”、投标文件中不得出现任何选择性报价，否则一律视作无效投标。

十二、投标单位在制作纸质投标文件时，一式二份，其中一份正本、一份副本，请在封面首页注明“正本”或“副本”字样，投标单位应将纸质投标文件密封封装，并在封口骑缝处加盖投标单位公章。

十三、采购人将通过专家进行综合评审，充分考虑价格、方案等因素，选择性价比最优的供应商，具体评审办法详见第五章。

十四、本招标文件解释权归采购人及上海市崇明区政府采购中心所有，当供应商对本招标文件有歧义时，本中心将依据“公开、公平、公正”原则作出相应解释。

十五、供应商提交的投标文件以及供应商与采购人就有关采购的所有来往书面文件均应使用中文；如果投标文件中有外文文件或资料的，必须同时提供其中文翻译，以便核实；供应商所提供的所有技术性能规格及参数，必须与制造厂家公布或确认的内容保持一致。

十六、本招标文件中出现带“★”条款的，均为实质性条款。

十七、凡出现下列情况之一者，该投标视作无效投标：

- (1) 许可类证书超出有效期的或超出经营范围的；
- (2) 供应商投标报价超过（大于）最高限价的；
- (3) 投标文件无法定代表人签字，或签字人无法定代表人的有效授权书；
- (4) 公开投标时未提供有效资格证明文件的（如法人授权书、身份证等）；
- (5) 无详细的投标报价表；
- (6) 投标文件项目需求中的响应与事实不符或虚假投标的（须经全体评委一致认定。）；
- (7) 带“★”条款出现负偏离的；
- (8) 如符合带“★”参数的供应商少于3家的，本次招标按“实质性”响应少于3家处理，宣告招标采购失败；
- (9) 投标文件出现招标文件中规定无效投标的其它商务或技术条款的。

十八、询问与质疑

1、投标人对招标活动事项有疑问的，可以向招标人提出询问。询问可以采取电话、电子邮件、当面或书面等形式。对投标人的询问，招标人将依法及时作出答复，但答复的内容不涉及商业秘密或者依法应当保密的内容。

2、投标人认为招标文件、招标过程或中标结果使自己的合法权益受到损害的，可以在知道或者应知其权益受到损害之日起七个工作日内，以书面形式向招标人提出质疑。其中，对招标文件的质疑，应当在其收到招标文件之日（以采购云平台显示的报名时间为准）起七个工作日内提出；对招标过程的质疑，应当在各招标程序环节结束之日起七个工作日内提出；对中标结果的质疑，应当在中标公告期限届满之日起七个工作日内提出。

投标人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，超过次数的质疑将不予受理。以联合体形式参加政府采购活动的，其质疑应当由组成联合体的所有供应商共同提出。

3、投标人可以委托代理人进行质疑。代理人提出质疑应当提交投标人签署的授权委托书，并提供相应的身份证明。授权委托书应当载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。投标人为自然人的，应当由本人签字；投标人为法人或者其他组织的，应当由法定代表人、主要负责人签字或者盖章，并加盖公章。

4、投标人提出质疑应当提交质疑函和必要的证明材料。质疑函应当包括下列内容：

- （1）供应商的姓名或者名称、地址、邮编、联系人及联系电话；
- （2）质疑项目的名称、编号；
- （3）具体、明确的质疑事项和与质疑事项相关的请求；
- （4）事实依据；
- （5）必要的法律依据；
- （6）提出质疑的日期。

投标人为自然人的，应当由本人签字；投标人为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

质疑函应当按照财政部制定的范本填写，范本格式可通过中国政府采购网（<http://www.ccgp.gov.cn>）右侧的“下载专区”下载。

5、投标人提起询问和质疑，应当按照《政府采购质疑和投诉办法》（财政部令

第 94 号) 及《上海市政府采购中心供应商询问、质疑处理规程》的规定办理。质疑函或授权委托书的内容不符合《投标人须知》第十九条中第 3 条和第 4 条规定的, 招标人将当场一次性告知投标人需要补正的事项, 投标人超过法定质疑期未按要求补正并重新提交的, 视为放弃质疑。

质疑函的递交可以采取邮寄、快递或当面递交形式。

6、招标人将在收到投标人的书面质疑后七个工作日内作出答复, 并以书面形式通知提出质疑的投标人和其他有关投标人, 但答复的内容不涉及商业秘密或者依法应当保密的内容。

7、对投标人询问或质疑的答复将导致招标文件变更或者影响招标活动继续进行的, 招标人将通知提出询问或质疑的投标人, 并在原招标公告发布媒体上发布变更公告。

第三章：项目需求

随着教育信息化进程的不断加速，学校在教学、科研以及管理等多个场景中网络的依赖性日益增强。原有的网络出口由于带宽的限制和安全方面的不足，已经越来越难以满足当前日益增长的业务需求。为了打破这种发展的瓶颈，迫切需要对校校通网络出口进行不低于 80G，冷备不低于 40G 的升级改造。同时，还需要同步推进关键系统的商密建设，以确保网络性能的提升、安全审计的加强以及教学效能的全面提高。

本项目属于信创项目除网络建设以外，服务器采购须符合财政部工业和信息化部关于印发《通用服务器政府采购需求标准(2023 年版)》的要求。

商密建设需符合第三级密码应用要求。

一：设备及服务清单

类别	数量	单位	备注
校校通出口升级			
校校通网络出口防火墙	2	台	
校校通出口防火墙模块	4	只	
校校通网络出口安全网关	2	台	
校校通网络出口网关模块	4	只	
校校通网络出口冷备网关	1	台	
校校通网络出口冷备网关模块	2	只	
全网日志系统（含各校）	1	套	须适配本次所投日志存储服务器
日志存储服务器	3	台	
日志存储服务器模块	6	只	
七级应用镜像分流系统	2	台	
七级应用镜像分流系统光模块	6	只	
安装调试	1	项	
系统集成	1	项	日志系统需完成对各校网关设备进行日志对接
综合布线	1	项	
商密建设			
云加密机	1	台	国产化商密
云加密机光模块	2	只	
服务器密码机	1	台	国产化商密
密码机光模块	2	只	
签名验签服务器	1	台	国产化商密

签名验签光模块	2	只	
国密浏览器	1	套	商密配套
设备证书	1	套	商密配套
SSL 站点证书	1	套	商密配套
用户证书（含证书介质）	1	套	商密配套
国密门禁系统	1	套	商密配套
国密视频监控系统	1	套	商密配套
机房密评环境改造	1	项	含门禁与视频
认证中心商密改造	1	项	应用改造
数据中心商密改造	1	项	应用改造
国密堡垒机	1	套	50 资产
云日志系统	1	套	200 资产
云数据库审计	1	套	20 资产
安管平台	1	套	
云安全虚拟化系统	1	台	承载堡垒机，日志系统，数据库审计系统，安管平台的运行，
安装调试	1	项	
系统集成	1	项	需要对已建设的认证中心，数据中心进行系统商密改造。并协助第三方完成密码改造。
综合布线	1	项	
校园网高密 AP			
高密 AP	160	台	
安装调试	1	项	
系统集成	1	项	需集成到教育局已经建设的 AC 控制系统，或单独提供不少于 3000 点的 AC 管理系统并提供 API 接口
综合布线	1	项	
校园网万兆升级			
校园网核心交换机	20	台	
校园网核心交换机千兆万兆子卡	40	台	
校园网核心交换机电源模块适配器	40	台	
光纤配线器机框	20	台	
8 口光配件子卡	20	台	
光模块	160	只	
光模块	20	只	

校园网接入交换机	65	台	
校园网接入交换机光模块	120	只	
交换机箱	150	套	
校园网万兆防火墙	20	台	
校园网万兆防火墙光模块	40	只	
校园网万兆防火墙光模块	40	只	
安装调试	1	项	
系统集成	1	项	需集成到教育局已经建设的网络设备管理平台，或单独提供不少于 10000 点的设备管理系统并提供 API 接口
综合布线	1	项	

二：总体建设内容

校校通出口升级：通过升级出口防火墙、部署安全网关、增设冷备安全网关、构建全网日志系统以及配置高性能的日志存储服务器，显著提升校校通出口的网络吞吐能力和安全防护水平。确保教育资源的快速、稳定传输，并为师生提供更加安全、可靠的网络访问环境。

校园网万兆升级：对校园内部网络进行全面优化和升级。通过引入万兆网络设备，提升网络带宽和传输速度，满足日益增长的网络应用需求。为多媒体教学、在线协作、远程教育等应用场景提供更加流畅、高效的网络支持。

校园网高密 AP：将针对校园无线网络进行升级和优化。通过部署高性能、高密度的无线接入点（AP），提升校园三个助手网络的覆盖范围和信号质量，为师生提供更加便捷、稳定的无线网络访问体验。推动移动学习、无线办公等新型教学模式的发展和应用。

本项目包括网络基础设施层、设备管理层、用户安全及应用授权服务层。

基础设施层

本项目建立 20 所学校的万兆到汇聚层，同时扩容和更换校校通出口硬件带宽不低于 80G，冷备网关不低于 40G。

设备管理层

主要建设一套跨平台、跨厂商、跨地域的综合管理系统，支持多种数据采集方式，支持有线/无线网络设备、安全设备、服务器、数据库、中间件、虚拟化设备、存储设备、机房系统、应用系统等多厂商、多种类的资源监控，并且提供开放的接口，用户可以自行编制监控脚本，完成相应资源的监控；

用户安全及应用授权服务层

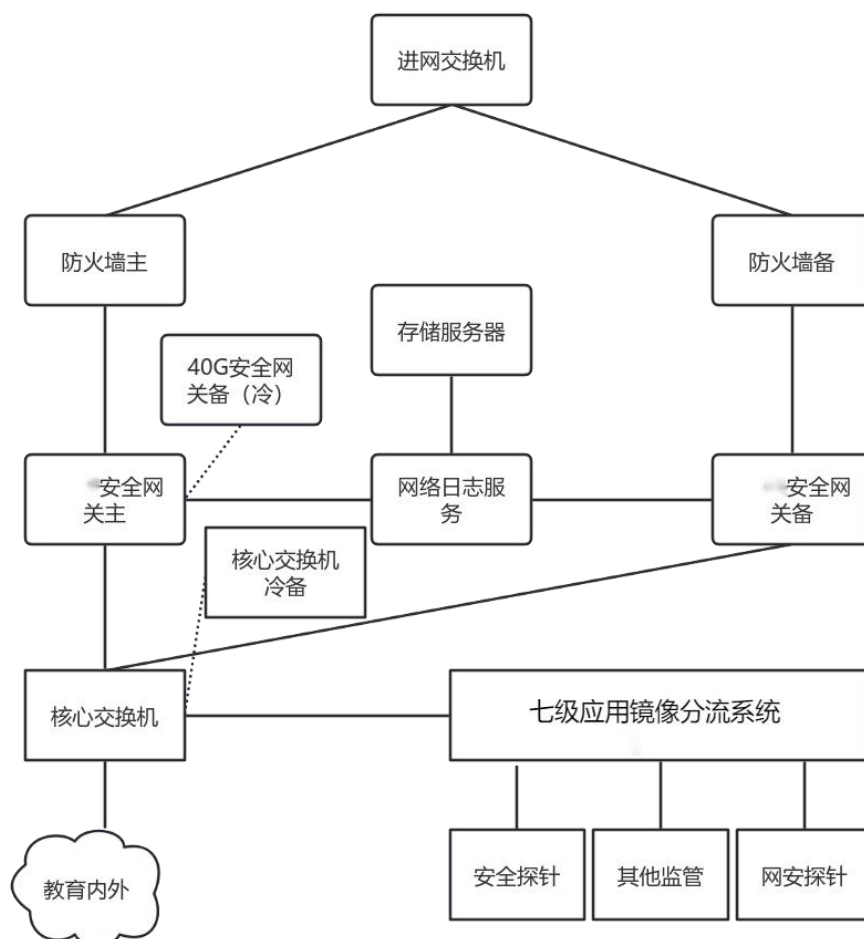
是在基座统一用户认证平台基础上,通过统一接口为校园网内网用户提供无感知认证和访客的临时认证系统（本期建设涵盖商密建设）;

系统提供了如终端发现，终端定位，推送杀毒软件，禁止高危端口，软件黑白名单等安全功能。

三：服务内容及需求

2.1校校通出口升级

校校通出口拓扑图



主要设备：

- 校校通网络出口防火墙 x2 台：主要负责入侵检测和入侵防御；
- 校校通网络出口安全网关 x2 台：主要负责流量控制，流量均衡，行为管

控，网安日志留存和威胁情报检测；

- 全网日志系统和日志存储（3 台）一套：主要用于留存全部学校和出口的的上网行为日志和行为分析，保存时间为 180 天；
- 核心交换机利旧
- 七级应用镜像分流系统为各监管部门提供镜像数据，TAP 系统为 10G 接口。

2.1.1 校校通网络出口防火墙性能要求：

名称	硬件规格/性能要求
防火墙	▲1：≤2U, 存储空间≥4T, 1个MGMT口，1个HA口, 冗余电源, 8个扩展槽位。 2：≥4个千兆电口 3：≥4个千兆光口 4：≥8个万兆光口 5：≥2个40G光口 6：防火墙吞吐≥80G 7：并发连接≥3000万 8：每秒新建连接≥52万 9：支持应用识别、入侵防御和病毒查杀功能

2.1.2 校校通网络出口防火墙技术要求：

功能类别	功能要求
路由交换	支持RIP、RIPng、OSPF、OSPFv3、BGP4、QinQ（VLAN VPN）、PIM-SM、PIM-DM、IPv6静态和动态组播路由；
链路聚合	支持根据源/目的MAC、源/目的IP、源/目的端口、五元组、端口轮询等条件进行链路聚合，提供不少于10种链路负载算法。
IP/MAC 绑定	支持IP/MAC绑定，支持跨三层绑定，支持IP/MAC绑定表导入导出，以便对IP/MAC绑定关系进行批量操作；
地址转换	支持源/目的NAT、双向NAT，支持源IP转换同一性；支持端口块地址转换和EIM地址转换，支持NAT64、NAT46、NAT66地址转换；
IPv4/IPv6 访问控制	支持一体化安全策略配置，可以通过一条策略实现五元组、源MAC、源地区、目的地区、域名、应用、服务、时间、长连接、并发会话、WEB认证、IPS、AV、URL过滤、高级威胁防护、WAF、邮件安全、数据过滤、文件过滤、僵尸蠕虫防御、审计、数据库防护、防代理、APT等功能配置, 简化用户管理；)
	支持IPv4和IPv6域名控制，支持对多级域名进行控制，域名对象支持通配符；
	提供策略命中、宽泛、冗余、冲突、包含检查及策略查询功能，支持五元组快速查询以及针对策略名、源/目的区域、源/目的地址、服务、对象、未命中时间等条件进行细粒度查询，支持重复对象分析；
	提供策略变更信息管理功能，支持查看变更策略、变更动作、变更时间、修改人、登陆IP，支持对变更前后的策略进行直观对比，并能一键还原配置；

应用识别	支持对P2P、数据库、移动应用、迅雷加密流量、向日葵/Teamview等远程控制软件、Modbus/IEC/OPC等工控物联网协议进行识别控制，支持自定义应用特征； 特征库数量：5000+
带宽管理	支持链路和四层通道嵌套的流量控制功能，可基于上下行区域、地址、地理对象、用户/用户组、服务/服务组、应用/应用组和时间等配置带宽策略，支持带宽策略优先级和针对IP、应用设置白名单；
连接控制	支持连接控制和监控，可对源/目的地理对象、应用制定连接限制策略，可展示被拦截的IP、地址对象、应用的限制条件、被拒次数、最近被拒时间等信息；
DDOS 防御	支持IP、ICMP、TCP、UDP、DNS、HTTP、HTTPS、SIP、NTP DDOS防护； 支持预定义和自定义策略模板； 支持阈值检查、源/目的限流、源认证、会话检查、报文大小限制、格式检查等方式综合进行SYN FLOOD、SYN-ACK FLOOD、FIN FLOOD、DNS REPLY FLOOD、NX防御、HTTP FLOOD、HTTP URI CC攻击、HTTP连接耗尽、NTP QUERY FLOOD、NTP REPLY FLOOD、SIP FLOOD、HTTPS FLOOD等攻击防护；
信息防泄漏	内置数据过滤功能，支持HTTP、FTP、POP3、SMTP等协议，可对预置身份证号、护照号、银行卡号、手机号等敏感信息和自定义关键字进行过滤，可对FTP命令和邮件标题、正文、附件、收发件人进行过滤； 内置文件过滤功能，支持识别超过300种文件类型，对无法识别文件、更改文件后缀、缺失文件后缀等常见规避手段处理过的文件内容进行检查；
邮件安全	内置邮件安全防护功能，支持邮件过滤、邮箱防暴力破解、收发件频率检测、邮件黑、白名单检测；
DNS 安全	支持独立的DNS安全模块，可对用户端进行DNS报文检查、DGA检测、DNS反射放大检测，可对服务端进行DNS报文检查、NX防御，DNS安全模块能自动生成动态非法地址表和动态非法域名表；能对域名请求和域名解析情况进行排名统计；
黑名单	内置静态黑名单功能，可设置多个对象条件，如：五元组信息、源MAC、地址范围、应用、用户，实现对特定报文进行快速过滤；支持封禁HTTP代理X-Forward-For字段IP 内置动态黑名单功能，可与URL过滤、病毒过滤、防代理、WAF功能实现联动封锁；支持静态和动态黑名单命中统计和监控；
支持现网集中管理平台	▲支持域组织架构图，安全域大屏可视化展示，安全域拓扑展示；支持域添加、编辑；支持域组织架构图的一键收缩；支持鼠标放大、拖动安全域；（提供功能截图） 支持设备远程管理，在设备管理列表中选择设备，通过调用浏览器登录远程设备进行管理；支持NAT后设备远程管理； 支持查看设备管理状态，支持设备语法包是否匹配的信息展示；支持设备规则库版本是否一致的信息展示；支持设备配置最后更新时间的信息展示；支持设备位置信息的显示； 支持平台下发访问控制策略与设备端策略进行对比合并； 支持全局策略及单台设备策略；支持创建策略模板，可将多个策略模板内容合并然后下发给所管理的域或一组设备；支持选择域一键创建策略模板；支持自动创建策略模板并自动与选择的域进行关联； 支持统计网络对象、服务对象未被引用的占比；支持策略分析的总览展示；支持对防火墙安全策略、网络对象、服务对象、区域的分析结果导出和查询；

配置维护	支持配置文件本地备份和回滚，支持>3个配置文件备份，支持配置定时保存，支持配置导入及明文/密文导出，支持对访问控制策略、NAT策略等关键配置进行部分导出和恢复；支持对配置命令及配置文件的操作行为进行审计；
升级维护	支持软件版本本地备份，可备份多个系统版本文件，支持对软件版本进行快速升级及回滚；
产品资质	▲具备网络关键设备和网络安全专用产品安全认证证书(提供证书复印件并原厂盖章) 具备信息安全产品分级评估(EAL4+)证明
	▲提供原厂售后服务承诺函。

2.1.3 校校通网络出口安全网关性能要求：

名称	硬件规格/性能要求
安全网关	▲满足≥100G带宽处理能力；每秒新建会话数≥60万/秒；PPS（包转发率）≥600万；终端用户数≥10000。（提供产品功能截图或产品公开彩页） ▲接口数量：≥2个千兆电口、10G光口≥4、≥2个100G光口；冗余电源；2U机架式设备。（提供产品功能截图或产品公开彩页）

2.1.4 校校通网络出口安全网关技术要求：

序号	功能类别	功能要求
1.	负载均衡功能	1. 链路负载均衡功能：根据目标地址、源地址、服务协议、时间等要素灵活的按照用户需求进行链路的负载均衡。（须提供该功能相应的系统截图及该功能文字描述或产品公开彩页） 2. 基于应用负载均衡：根据业务应用实现负载到不同的网络出口链路，例如：可以将微信路由到A运营商出口、腾讯会议路由到B运营商出口、迅雷路由到C运营商出口。（须提供该功能相应的系统截图及该功能文字描述或产品公开彩页） 3. 基于域名负载均衡：实现基于域名的负载均衡，例如：可以让www.baidu.com域名自动路由至A运营商出口，而www.youku.com网站自动路由至B运营商出口。（须提供该功能相应的系统截图及该功能文字描述或产品公开彩页） （以上条件均须提供该功能相应的系统截图及该功能文字描述或产品公开彩页）
2.	负载能力	支持不低于5条运营商出口线路之间的负载均衡。
3.	告警模式	如发生以下情况需通过微信进行告警： 运营商线路连接中断、单IP连接数过高、流量异常；
4.	工作模式	支持透明网桥模式、路由模式、NAT模式、旁路分析模式；支持路由、NAT、网桥和旁路分析的混合模式。（须提供该功能相应的系统截图及该功能文字描述）
5.	流量控制功能	1. 带宽限制功能：根据策略对特定用户群组、IP/IP组、应用协议或域名进行带宽限制。 2. 带宽保证功能：根据特定用户群组、IP/IP组、应用协议或域名进行带宽保证，当网络拥塞时候，可以保证这些IP或者应用优先传输。 3. 基于用户群组的策略：支持和单位园网认证&计费系统对接，根

		据认证计费的用户群组作带宽管理策略。 4. 基于单独IP的限速：支持针对内网单IP地址带宽限速。（须提供该功能相应的系统截图及该功能文字描述）
6.	共享检测功能	支持对单位内用户通过路由器共享等模式上网检测，自动发现共享上网用户，支持自动启动对于的策略对其进行限速或者阻断。（须提供该功能相应的系统截图及该功能文字描述）
7.	IPv6 的 NAT	支持IPv4到IPv6的NAT，支持NAT66。（须提供该功能相应的系统截图及该功能文字描述）
8.	QPS 管理	支持对DNS的QPS进行管理，可限制DNS访问每秒的次数，解决用户恶意频繁请求（须提供该功能相应的系统截图及该功能文字描述）
9.	端口镜像	▲支持有条件的端口镜像功能，例如将HTTP流量单独镜像至某一个网络接口、将某域名相关联流量单独镜像至某一个网络接口、镜像某一会话流的前N个数据包、基于时间维度进行。（须提供该功能相应的系统截图及该功能文字描述或产品公开彩页）
10.	认证功能	▲支持认证网关功能；支持IPv4、IPv6的认证；支持外置Portal、短信、Radius等认证方式；支持认证嗅探功能，可以在旁路或串接等模式下，深度分析radius、PPPOE、DHCP、华为5G网等报文，分析出如“账号和IP”、“IP和MAC”、“账号的贷款限制参数”、“IP和手机号码”等重要信息。 （以上条件均须提供该功能相应的系统截图及该功能文字描述或产品公开彩页）
11.	认证计费系统对接功能	1. 支持和单位认证计费系统对接，可以自动读取认证计费系统用户群组，根据用户群组作带宽管理功能、并发控制功能、DNS管控功能。 2. 与认证计费系统对接后，网络访问日志自动显示并记录IP地址对应的用户账号、姓名等信息。
12.	智能 DNS 功能	1. 支持根据源IP、目标IP、访问域名、所在线路等组合条件实现对域名访问的控制。 2. 支持对网内DNS流量进行重定向等管理； 3. 支持根据不同运营商源IP地址源解析域名。
13.	威胁情报关联	▲支持与威胁情报关联（威胁情报库不低于100万条），并支持对匹配流量进行阻断（须提供该功能相应的系统截图及该功能文字描述）。
14.	安全防护	支持“垃圾包”检测及过滤功能； 支持“IP分片”攻击检测及过滤功能； 支持对异常流量IP的实时查询、日志反查功能；
15.	SD-WAN 能力	支持SD-WAN的Tunnel，方便与其他单位外单位互联互通。支持Tunnel的负载均衡能力，支持集中管理100台以上SD-WAN设备。（须提供该功能相应的系统截图及该功能文字描述）
16.	IPv4/IPv6 转换	IPv6路由：可通过线路配置转发IPv6及IPv4路由（须提供该功能相应的系统截图及该功能文字描述）。
17.		IPv4转换IPv6：可通过配置IPv6前缀，将IPv4地址转换成IPv6地址。（须提供该功能相应的系统截图及该功能文字描述）
18.		IPv4/IPv6域名转换：系统可针对网站信息，解析对应的IPv4及IPv6地址地址，并记录路由至相关地址的次数。（须提供该功能相应的系统截图及该功能文字描述）
19.		IPv6流量分析：系统可查看IPv6的TOP应用流量、IPv6的会话记录、URL日志、异常分析日志等信息。（须提供该功能相应的系统截图及该功能文字描述）
		▲提供原厂售后服务承诺函。

2.1.5 校校通网络出口冷备网关性能要求：

名称	硬件规格/性能要求
安全网关（备）	满足 $\geq 40\text{G}$ 带宽处理能力
	接口数量： ≥ 4 个千兆光口、 ≥ 2 个40G光口；冗余电源；2U机架式设备。

2.1.6 校校通网络出口冷备网关技术要求：

名称	硬件规格/性能要求
安全网关（备）	（与主安全网关一致）

2.1.7 日志存储服务器性能须符合财政部工业和信息化部关于印发《通用服务器政府采购需求标准(2023 年版)》的要求：

一级指标	二级指标	指标要求
CPU 规格、功能、性能、安全要求	CPU 规格	C86架构；单CPU核数 ≥ 16 ；
		主频（基频） $\geq 2.5\text{ GHz}$ ；
		单 CPU 末级缓存容量： $\geq 32\text{ MB}$
	CPU 信息	供应商给出 CPU 信息，包含 CPU 型号、物理核心数、主频、末级缓存容量、线程数、热设计功耗及支持内存的最高速率、通道数和位宽
	实配 CPU 数量	2 颗
	CPU 计算处理功能要求	支持通用计算及虚拟化功能。处理器需集成整型计算单元、浮点计算单元、内存控制器、I/O 模块等，处理器与存储部件、网络部件、I/O 部件等组成计算系统，提供数据处理、网络接入等计算相关功能
	关键部件安全要求	CPU 须通过中国信息安全测评中心的安全可靠测评
	CPU 密码算法实现要求	CPU 芯片应符合 GM/T 0008 的相关规定，或芯片密码模块应符合 GB/T 37092 或 GM/T 0028 的相关规定
主板规格规格、功能	主板支持CPU和内存情况	供应商给出主板支持的 CPU 和内存的型号数量
	主板内存槽数量	主板支持的内存槽位数量 ≥ 16 条；
	主板存储接口	至少支持 SATA、SAS、M.2、U.2 等存储接口中的 1 种
	PCIe 插槽接口	支持 PCIe3.0 或以上扩展总线,PCIe 的接口速率与位宽需保证向下兼容。
	主板 PCIe 插槽数量及规格	PCIe 插槽应不少于 5 个（不含 Storage 专用插槽和 OCP 插槽）
	功能卡兼容性	内置或适配符合 PCIe 的功能卡，如：网络功能卡、存储功能卡及图形显示功能卡
	主板外部接口	至少支持 USB、显示、管理接口
内存规格规格、功能、性能	实配内存数量	实配内存 ≥ 2 条
	单内存模块容量	$\geq 16\text{GB}$
	内存规格	$\geq \text{DDR4}$
	内存速率	$\geq 3200\text{ MHz}$

	内存通道	支持多个内存接口通道，每个通道可支持 1DPC 或 2DPC，当支持 2DPC 时，印制电路板上应具备插槽的序号标识，具体通道数应在随机文件中明确
	内存兼容性	适配 3 种及以上厂商的内存产品，且均不低于产品支持的内存规格
存储规格规格、功能、性能	硬盘规格	供应商给出服务器支持硬磁盘和固态盘类型及规格
	硬盘实配容量	系统盘：单盘容量 $\geq 1.2\text{TB}$ ；数据盘：单盘容量 $\geq 16\text{TB}$
	硬盘接口类型	系统盘：接口类型 $\geq \text{SATA } 3.0$ ；数据盘：接口类型 $\geq \text{SATA } 3.0$
	硬盘实配数量	系统盘：硬盘数量 ≥ 1 块；数据盘：硬盘数量 ≥ 10 块
	硬盘插槽数量及规格	规格：2.5 寸硬盘插槽；数量 ≥ 16 个
	固态存储兼容性	适配 3 种或以上厂商的固态存储产品，且均不低于产品支持的固态存储设备规格
RAID 卡规格规格、功能、性能	RAID 卡支持的接口数量	数量： ≥ 8
	RAID 卡 RAID 级别支持	RAID 模式支持：RAID 0/1/10/5/50/6/60
	RAID 卡缓存容量	实配 $\geq 2\text{GB}$
	RAID 卡 BBU 单元	RAID 实配持电池或电容备份单元
网络规格规格、功能、性能	网口速率和数量	光口卡：实配 ≥ 1 个双口万兆 SFP 卡，满配多模光模块 管理口：实配 ≥ 1 个千兆 RJ45 远程管理接口。
	板载网络接口	板载支持 ≥ 2 个 1GE 网口，且采用国产网络芯片，支持 NC-SI、网络唤醒、边带管理等功能
	网络功能	支持网络连接、网络访问、数据交换和网络管控功能
	网卡兼容性	网卡应适配 2 种或以上厂商产品
电源规格规格、功能、能耗	电源冗余模式	整机电源模块支持 1+1 冗余
	电源模块数量	电源数量满配，2U 服务器不少于 2 个电源模块
	电源功率	可保证服务器单路供电下满负荷运行。
	电源热插拔	整机电源模块应具备热插拔功能
	电源过流保护	支持过流及短路保护的功能
	电源能耗	在符合 GB/T 9813.3 的有关规定的基礎上，电源能耗技术参数符合 80 PLUS 标准中铂金/钛金级别同等标准
	电源线	根据现场实际需求提供国标电源线或 C13/C14 PDU 电源线。

整机规格规格、功能、可靠性、软件兼容性	外观和结构	a) 服务器的零部件应紧固无松动，可插拔部件应可靠连接，开关、按钮和其它控制部件应灵活可靠，布局应方便使用； b) 产品表面不应有明显的凹痕、划伤、裂缝、变形和污染等。表面涂层均匀，不应起泡、龟裂、脱落和磨损，金属零部件无锈蚀及其它机械损伤； c) 产品表面说明功能的文字、符号和标志应清晰、端正且牢固； d) 应在服务器的显著位置提供运行状态的指示功能，并在随机文件中明确具体含义； e) 机架、机箱的尺寸应符合通用机柜的安装要求，插入总线插座的电路板接口外形尺寸应符合有关总线标准的规定，将机箱固定在机柜上，机箱底面最大下垂变形不得干涉相邻机体； f) 高密度服务器应给出 CPU 个数与机柜高度； g) 服务器尺寸具体要求在随机文件中明确
	整机尺寸	供应商给出产品尺寸；设计应遵循标准化、系列化的要求；机箱的内部结构符合通用部件的安装需要
	机柜尺寸	供应商给出长度、高度和深度
	服务器导轨	实配免工具维护导轨，供应商给出导轨尺寸、安装方式等信息
	环境适应性	气候环境适应性应符合 GB/T9813.3 的有关规定，工作温度 10~35℃，贮存运输温度-40~55℃；工作相对湿度 35 ~80 ，贮存运输相对湿度 20%~93 （40℃）；大气压 86~106kPa
	机械环境适应性	机械环境适应性应符合 GB/T9813.3 的有关规定。
	显示接口	显示接口类型应不少于 1 种，如：VGA、DP、HDMI 等，至少包含 VGA 接口
	USB 接口	配备 USB 接口≥4 个，其中 USB3.0≥3 个
	噪声	符合 GB/T 9813.3 的有关规定，在产品说明中给出具体测试值。
	散热方式	支持风冷或液冷等散热方式
	外设兼容性要求	兼容多种主流生产商的外部设备，包括显示器、键盘、鼠标、闪存盘、移动硬盘、USB 光驱及 KVM 等，要求使用不同厂商的外部设备时，系统均能正常识别和安装驱动
	限用物质的限量要求	限用物质的限量应符合 GB/T 26572 的要求
	数据库兼容	兼容 3 个及以上厂商的数据库产品
	中间件兼容	兼容 3 个及以上厂商的中间件产品
	平台软件兼容	兼容 3 个及以上厂商的大数据平台
	虚拟化软件兼容	兼容 2 款及以上虚拟化软件

	整机可靠性	mtl 值 (MTBF 的不可接受值) 不得低于 200000h
	风扇可靠性	风扇寿命 $\geq$ 40000h
	部件可靠性	支持硬盘、电源、风扇热插拔(内置风扇除外)
	标志、包装、运输和贮存	符合 GB/T 9813.3 和商品包装政府采购需求标准的相关规定
管 理 系 统 功 能	BMC 固件基础功能	1) 支持 DHCP 设置网络功能; 2) 支持静态 IP 设置网络功能; 3) 支持设备日志记录, 包括但不限于登录日志、操作日志和报警日志等功能; 4) 支持日志信息导出和记录删除功能; 5) 支持通过管理接口向外输出准确的报警信息功能; 6) 设备的 BMC 管理软件应能够按报警的严重程度进行区分; 7) 支持 IPMI2.0、SNMP 或 Redfish 等接口功能; 8) 支持键盘、鼠标和视频的重定向、文本控制台的重定向、远程虚拟媒体、高可靠的硬件监控和管理功能; 9) 支持基于网络开启、关闭和重启设备的功能, 并查询当前设备开机运行状态; 10) 支持故障提示功能, 并可通过接口读取服务器故障信息; 11) 支持基于网络的固件更新功能, 包括 BMC 和 BIOS 等; 12) 支持基于网络安装操作系统的功能, 并可通过网络控制台访问设备; 13) 支持通过本地的硬盘或光驱等存储设备, 基于网络完成设备的操作系统安装功能; 14) 支持通过浏览器打开管理界面并登录功能; 15) 支持设置口令策略功能; 16) 支持访问权限设置功能, 并通过日志记录访问事件; 17) 支持对出厂默认的用户名及口令进行安全保护功能, 并提供默认口令修改提示; 18) 支持读取设备主板的工作环境温度功能; 19) 支持读取服务器 CPU 等核心器件的温度功能; 20) 支持通过外部管理工具进行 BMC 参数设置的功能, 并可基于网络通过外部管理工具对 BMC 进行管理; 21) 应支持固件版本查询、固件升级 22) 支持基于网络实现开关机和复位控制的功能; 23) BMC 启动时间应不超过 180s, 实现功能包括网络、IPMI、散热、传感器服务可用; 24) 支持 BMC 固件设置的恢复出厂功能

	BIOS 固件基础功能	1) 支持查看固件版本、内存信息、主板信息、处理器信息和系统时间信息功能； 2) 支持上电初始化界面显示 CPU 信息、内存信息、固件版本和部分快捷键信息功能； 3) 支持设置界面中英文显示切换功能； 4) 支持查看 PCIe 设备信息，SATA 设备信息功能； 5) 支持操作系统安装和引导功能，应并向操作系统提供计算机主板信息和服务接口； 6) 支持设置启动顺序，并按照设置的启动顺序启动功能； 7) 支持安全启动功能； 8) 支持设置口令、修改口令验证口令功能； 9) 支持 RAID 识别和启动功能； 10) 支持固件更新功能； 11) 支持 BIOS 固件设置的恢复出厂功能； 12) 支持网络引导启用和关闭功能。
	远程控制	支持远程关机和重新启动功能
固件安全要求	故障检测	1) 关键部件：CPU/内存/硬盘/电源/风扇支持故障报警功能； 2) 所有部件报警支持通过SNMP或IPMI方式对外提供。 3) 主机前面板提供故障诊断功能，具有对系统/内存/电源/风扇/温度/网络/硬盘等关键部件的故障诊断报警功能；能够分别提示硬盘故障、系统运行故障、风扇及温度故障、网络故障、内存故障和电源故障；
系统安全要求	弱口令字典检查	支持弱口令字典检查功能，出现在弱口令字典中的字符串不能被设置为用户口令
	白名单访问控制	支持基于时间、IP 或 MAC 白名单访问控制
	二次鉴别	支持二次鉴别功能。对于用户配置、权限配置、公钥导入等重要的管理操作，已登录用户应通过二次鉴别后，才能执行操作
	密码证书安全加密存储	支持对带外管理系统中的用户口令和证书等敏感信息进行加密存储，禁止使用私有的和业界已知不安全的密码算法
	敏感信息安全加密传输	支持使用安全的传输加密协议（如 SSH 或 HTTPS 等）传输用户的敏感信息
操作系统及驱动功能	操作系统及驱动的升级	支持通过网络、闪存盘对操作系统、驱动进行升级
	操作系统功能	a) 支持访问控制、安全审计、网络接入鉴别等功能； b) 操作系统其他功能应满足操作系统政府采购需求标准中加*的指标要求

信息安全要求	研发过程安全要求	供应商承诺，生产商已建立从需求、设计、开发、测试、维护端到端的开发流程管理机制，输出和保存开发流程中每个阶段的产品需求清单、设计文档、开发文档、测试记录等材料，保证各个流程可追溯
	漏洞管理	供应商承诺，制造商已建立漏洞全量视图，保证产品版本涉及到的所有漏洞(如驱动程序、BMC 软件等)都可以查看
	物理安全	安全要求应符合 GB 4943.1 的规定；配置机箱入侵检测，在外部打开机箱盖时提供报警功能
服务响应	服务响应要求	a) 提供电话、电子邮件、远程连接等多种形式的服务； b) 提供同城4h、异地12h技术响应服务，2个工作日解决问题，对于未能解决的问题和故障应提供可行的升级方案，并提供周转设备； c) 建立全国技术服务体系和服务团体，符合专业服务体系标准要求，提供原厂中文服务； d) 服务周期内提供产品的维修、换件和升级服务
	培训服务	供应商提供培训材料、产品手册、培训视频等培训相关内容
服务周期	服务周期	a) 产品免费服务周期(含换件和维修)应不小于3年； b) 设备停产后继续提供质量保障服务(含备品备件)，服务终止时间与最后一批设备交付时间间隔不低于6年； c) 产品停止服务时间应提前1年告知客户； d) 产品发布日期需在随机文件中明确
服务工具要求	工具要求	供应商提供设置服务器硬件、辅助操作系统安装等功能的辅助工具和管理软件。且随附软件应具有合法授权或版权
	驱动安装升级指引	供应商提供出厂安装的配件所需的驱动程序，形式包括但不限于驱动光盘、驱动下载链接等。其他配件应提供指引
	管理软件	具备资源管理、系统管理、性能监控、健康监控、基于网络控制、报警设置功能。
增值服务	厂家升级产品软件与扩容服务	供应商提供原厂级的部件/软件产品升级和扩容能力
	提供上门服务	供应商具备提供上门服务的能力(可收费)
供应链质量	抗干扰性	当产品部件出现供应风险时，应通知客户并提供风险应对方案确保产品的服务保障，必要时应停止相关受影响产品的销售。
	供应能力证明	供应商提供供应链稳定承诺书，确保产品的部件在产品服务周期内稳定供货。

2.1.8 全网日志系统技术要求：

大数据日志分析系统

序号	指标项	指标参数
1.	网络日志留存功能	▲会话行为留存：提供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、地理位置一共13个元素。同时采用1:1的日志输出，完整保留网络中的相关信息。虚拟身份留存：记录QQ、微信、邮件等帐号的登录时间，完成时间-IP-身份的映射，达到可以根据虚拟身份锁定IP和用户的目标。提供用户行为跟踪：包括用户上网URL日志、用户DNS解析日志等。 （以上条件均须提供该功能相应的系统截图及该功能文字描述或产品公开彩页）
2.	网络质量感知功能	▲支持单个协议时延、抖动等性能指标在时间维度的查询，内置识别协议数>1000。实现多个协议和用户的交叉查询，监测异常情况，上报预警或告警；实现业务性能指标的实时查看。包括但不限于：业务时延、服务时延、应用时延、平均时延、重传率、丢包数、请求数、失败响应数等指标分析维度。支持对服务器分析，包含连接数，最大时延ms，平均时延ms，流量等信息。支持国内时延，全球时延分析，包括区域名称，连接数，最大时延(ms)，平均时延(ms)，流量等信息。支持不同时间段内，多个或单个协议的时延对比，包括客户时延，服务时延，应用时延。 （以上条件均须提供该功能相应的系统截图及该功能文字描述或产品公开彩页）
3.	IPv6 流量可视化	提供整个系统IPv6流量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。
4.	IPv6 用户、协议排名分析	支持IPv6 TOP应用排序、多个应用协议进行趋势图分析对比，各个协议的IPV6地址排名等。支持IPV6 TOP用户排名、各个用户使用的协议、IPV6连接信息等。
5.	服务器资产管理	支持自动对服务器域名、IP、端口进行归纳，形成真实的网络访问情况，然后和单位备案服务器列表（白名单）进行对比，发现和备案名单不一致的资产情况。
6.	双非网站分析功能	▲支持对单位内提供HTTP或者HTTPS访问的域名进行统计，对内外网用户访问单位内服务器进行排名，同时发现单位内教育网IP使用单位外域名的情况。（须提供该功能相应的系统截图及该功能文字描述）
7.	单位内图书馆资源查询	对单位内用户访问单位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，为我单位购买图书馆资源提供依据；对单位内用户下载单位外图书馆次数作统计，提供下载排名，发现恶意下载用户。
8.	运维大屏	▲支持网络监测大屏展示，包括热点IP，SYN源，SYN目标，SSDP源，SSDP目标，NTP源，NTP目标，MSDS源，MSDS目标，ICMP源，ICMP目标，连接数，协议组，运营商，DNS服务器，热点域名，热点应用，未知应用端口，DNS用户，新增域名，威胁情报等信息。支持网络性能监测大屏展示，包括客户时延，服务时延，应用时延，游戏时延，所有协议，DNS时延，视频时延，社交时延，邮箱时延，目标时延，域名时延，运营商时延等信息。支持网络资产监控大屏展示，包括资产数，用户数，域名数，流量趋势，连接趋势，热点资产，热点用户，全球访问，国内访问，热点应用，热点域名，新增域名，热点端口，敏感端口，资产时延等信息。

		(以上条件均须提供该功能相应的系统截图及该功能文字描述或产品公开彩页)
9.	分析功能	支持用户画像功能: 提供内网任何IP的用户画像功能, 可以分析该用户访问的地理区域分布, 去往各个运营商比例, 该用户的TOP协议排名图, 用户访问流量趋势图, 用访问连接趋势图和该用户访问域名排名、身份信息等。
10.		支持异常流量分析功能: 查询某一阶段全网的流量、会话趋势, 精准定位到有问题的源、目的IP地址及协议。
11.		流量概况: 系统可以查看流量总体概况, 其中包括协议组流量、流量分布、连接数分布、上下行速率趋势、连接数趋势等信息或图示。
12.		TOP域名: 可根据时间段, 查询TOP访问域名, 其中包括访问域名的次数、访问端口、上下行流量、总流量等信息, 并可分析域名是否有威胁。
13.	自动化分析报表功能	▲支持日报, 周报, 月报。包括网络带宽分析, 应用访问分析, 流量流向分析, DNS分析, 安全分析等信息。支持通过邮箱发送流量告警, 报表, 流控登录日志, 日志硬盘状态等信息。 (以上条件均须提供该功能相应的系统截图及该功能文字描述)
14.	第三方平台支持能力	▲开放的数据平台, 支持接收第三方 NAT日志。可通过 Kafka 接口向第三方输出数据。支持NAT日志查询, 包括设备, 类型, 接口, 会话时间, 源地址:端口, 目标地址:端口, NAT地址:端口, 用户账号, 流量(上行/下行), 运营商 源位置, 目标位置等信息。支持阻断日志查询, 包括设备, 用户地址, MAC, 账号, 源端口, 目标地址, 目标端口, 时间, 协议名称, 运营商, 目标地理位置, 策略编号, 类型, 备注等信息。 (以上条件均须提供该功能相应的系统截图及该功能文字描述)
		▲提供原厂售后服务承诺函。

2.1.9 七级应用镜像分流系统性能要求:

名称	硬件规格/性能要求
七级应用镜像分流系统	标准1U机架式设备。 ▲实配10GE光口≥6个, 1GE电口≥8个, 1GE光口≥8个; 实配Console端口≥1个; 实配MGT端口≥1个 (以上条件均需提供产品功能截图或产品公开彩页)

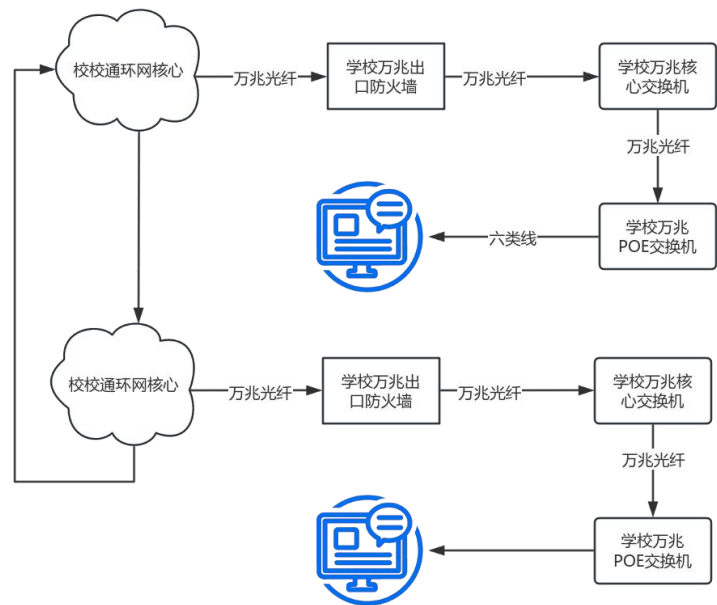
2.1.10 七级应用镜像分流系统技术要求:

1.	可靠性要求	操作系统双系统保活。 设备登录白名单访问限制。
2.	分发场景	支持自定义配置设备所有端口的模式类型, 所有的端口均可自定义为指定类型(镜像端口、监测端口、服务端口、设备间互联端口等)。 支持流量多路复制功能, 在设备物理端口数量范围内不限制复制数量, 多路复制具备线速性能, 满载不丢包。 支持端口流量汇聚, 可自定义汇聚策略进行流量的分发, 支持一对一、一对多、多对一及多对多映射关系。 支持流量去重功能, 能够根据条件要求将重复流量丢弃, 避免将重复流量输出至监控工具。

3.	策略分流功能	▲支持基于策略执行优先级的流量复制转发策略，策略条目数不低于65535。支持数据包截断，控制转发包长度，降低下游设备的性能压力。支持基于端口输入\输出双向的流量复制。支持基于IP五元组的流量复制策略。支持基于内网MAC组、VLAN、TTL的流量复制策略。支持基于首包接口、源接口的流量复制策略。支持基于域名的流量复制。支持基于时间的流量复制策略调度。支持基于指定输出接口的镜像/负载转发。支持输入/输出端口编组功能，可以将多个端口划分到一个“端口组”中，简化分流策略的配置过程，对选定的组内端口实现同策略管理。支持数据包标记功能，在分流输出时可以设置指定的VLAN ID值，且所有端口均应支持VLAN打标签功能。 （以上条件均须提供该功能相应的系统截图及该功能文字描述或产品公开彩页）
4.	应用协议分流功能	▲支持基于常规应用协议的流量镜像分发，降低下游设备性能压力。支持基于常规协议群组的流量镜像分发。支持基于自定义协议的流量镜像分发。支持基于自定义协议群组的流量镜像分发。 （以上条件均须提供该功能相应的系统截图及该功能文字描述）
5.	业务可视化	支持实时显示设备的输入/输出流量及PPS信息，并支持下钻统计流量协议信息，下钻统计网络趋势统计。 支持实时统计设备会话连接信息及用户信息，并支持按时间周期下钻统计连接数趋势及排名。 支持统计在线用户连接信息，通过三段时延（客户时延、服务时延、应用时延）分析当前用户网络连接质量情况。 支持端口模拟展示，并显示各端口连接状态、工作速率、流量速率、PPS值等信息。 支持按时间周期统计展示各端口的参数信息、实时/历史流速及PPS趋势统计。 支持按协议类型统计展示流量概况、输入/输出及分布情况的可视化图表。 支持按协议类型统计展示连接数趋势及分布情况的可视化图表。 支持按当前实时和峰值显示设备用户信息。 支持实时的设备授权信息，设备状态信息统计展示。
6.	遥测组网	支持SD-WAN组网，作为服务端接收远端流量。 支持SD-WAN组网，作为客户端发送流量给远端设备。
7.	业务管理能力	支持WEB网管和SSH命令行管理模式。 支持Syslog/SNMP Trap告警，支持设备日志功能。 支持内部时间源，支持NTP时钟同步。 支持按功能项的业务配置同步。 提供全功能许可服务能力License，无需额外购置。 授权期内支持软件业务能力更新迭代。
8.	安全要求	支持本地认证、Radius、LDAP等两种或两种以上的登录认证鉴别技术，对登录用户进行身份鉴别。 支持用户分级管理。 密码定期更新提示。
9.		▲提供原厂售后服务承诺函。

2.2校园网万兆升级建设

校园网万兆网络升级拓扑图



主要设备为：

- 20 台核心交换机：20 套核心交换部署在汲浜小学，陈家镇小学，竞存小学，横沙中学，圆沙小学，庙镇学校，长兴小学(前卫)，大公中学，堡镇中学，向化小学，大新中学，新海学校，东门中学(明志)，横沙小学，合兴小学，崇东中学，向化中学，长江学校，育才小学，海洪小学的校园网机房；
- 20 台万兆防火墙：主要用于校园网万兆出口到环网交换机使用。防火墙的 10G 上线模块连接校校通环网核心交换机。下行短距离 10G 模块连接核心交换机。
- 65 台接入交换机：20 所学校每校分配约 3-4 台（可根据实际情况调整），用于万兆接入各信息点。

2.2.1 校园网核心交换机性能要求

基本参数	▲交换容量≥4T，包转发速率≥1600Mpps，提供功能截图
	▲支持 10G 接口数≥24 个，QSFP28 100G 光接口≥2 个，提供功能截图证明。
	实配可拔插双模块化电源。

2.2.2 校园网核心交换机技术要求

功能要求	▲支持对下联交换机的即插即用实现零配置上线、互联光链路故障自动监测，下联交换机故障后零替换功能，提供功能截图证明。
------	---

	▲支持彩光技术，支持工作波长在 1271nm~1571nm 范围内的光模块，且各波长之间相互隔离，互不干扰，提供光模块参数功能截图证明。
	▲支持未来实现 10G 接口数≥80 个，千兆电口≥4 个的扩容，提供功能截图证明。
	产品尺寸适应业界主流机柜安装，要求设备高度≤2U，设备深度≤420mm。
	所投设备内置管理软件和业务模板，上电实现极速部署。
	支持 RIP，OSPF，BGP，RIPng，OSPFv3，BGP4+。
	支持多虚一技术，可将多台物理设备虚拟化为一台逻辑设备统一管理
	▲为充分利旧教育局现有基座网络综合运维管理平台，要求本次投标产品兼容现有基座网络综合管理平台，实现基座网络综合管理系统的整体功能升级及网络设备管理数量扩容。投标时需提供厂商兼容性承诺函，并加盖投标人公章。 若无法满足兼容性要求需额外提供以下设备： 提供独立一整套教育局综合网络管理管理平台并且可运行在信创环境下，实际配置可管理不少于 3000 颗无线 AP 的管理和 500 个交换机/虚拟机/数据库/操作系统的管理，并提供平台 API 接口。提供技术白皮书和加盖制造商公章承诺函证明。业主保留测试权力。
资质	提供工信部三层交换机进网许可证（标明是三层交换机入网证）。
▲提供原厂售后服务承诺函。	

2.2.3 校园网万兆防火墙性能要求

名称	硬件规格/性能要求
万兆防火墙	≥10个2.5G电口 ≥4个万兆光口

2.2.4 校园网万兆防火墙技术要求

序号	功能大项	功能小项	功能支持度
1	高可用性	主备系统保护	支持双系统备份，支持主备系统自动切换，切换时间小于500毫秒
		在线更新	支持在线更新协议特征库
			支持在线更新策略
			支持在线更新对象库文件
2	工作模式	网桥模式	支持网桥模式部署
		网关模式	支持网关模式部署，包括DHCP、NAT、DNAT、CGNAT等网关模式的应用功能
		旁路模式	支持旁路监听分析模式

		混合模式	支持路由、网桥、旁路分析的混合模式
3	应用协议识别	识别数量	支持常用协议总量大于1200种 1、支持对2~7层流量的识别能力，特别是针对第7层的应用识别能力，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---优酷、网络游戏---移动游戏等。 2、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（将持续新增至≥ 200种移动APP应用），现网协议识别率$\geq 95\%$ 3、支持常见AI应用协议，如ChatGPT、DeepSeek等
		协议识别	支持DPI、DFI、节点跟踪、主动探测、加密分析等多种技术。 1、对已经采用加密技术的P2P类应用比如BT、迅雷、Skype、eDonkey、Qvod、PPFilm、百度影音等精确识别。 2、可以区分迅雷、网际快车等下载工具的HTTP下载和IE浏览器下载 3、支持“迅雷增强识别”，大幅度改进对迅雷加密流量识别 4、支持“P2P智能识别”，大幅度改进P2P加密协议识别 5、支持“QUIC解密”，大幅度改进HTTP/3协议识别 6、协议精细分类且必须包含：移动浏览器（如iPhone手机上网）、应用商店（如安卓市场、手机报等）、云服务、网络支付（招商银行、兴业银行等）、移动游戏（手机游戏、iPad游戏）
		虚拟身份识别	支持虚拟身份的识别，如QQ号码、MSN账号、POP3账号、新浪微博、百度贴吧等
		特征库更新	支持在线状态下的特征库的更新升级
		识别准确率	现网识别准确率在95%以上
		业务识别率	现网业务识别率在95%以上
		自定义协议	支持自定义协议、自定义协议组
4	网络接入	多线路承载	支持虚拟LAN接口和WAN线路最大支持 >2000 条（2048条FreeBSD版本）；支持虚拟线路LAN+WAN线路最大支持4000条（仅限Linux版本）
		流量处理	支持VLAN、VLAN Trunk、QinQ、MPLS、GRE、Vxlan等以太网流量处理
			支持针对Gn接口数据包的解码，含GTP-C和GTP-U解码分析
		业务流向处理	支持基于端口判断业务上下行方向（接内/接外）
			支持基于设置内网IP地址端判断业务上下行方向
		PPPOE	支持网卡混合模式基于会话机制（TCP三次握手、UDP首包），自动判断业务流向
			支持自动检测链路状态，断线后自动拨号和支持计划定时重播

		VPN	支持L2TP, IPSec, 支持SD-WAN Tunnel等
		链路捆绑	支持物理静态链路捆绑
			支持LACP链路聚合
		MPLS	能部署在MPLS链路中, 并至少对具备2级标签的MPLS格式报文按应用进行识别、管理和统计
		NAT 网络地址转换	支持NAT功能
			支持静态NAT功能 (一对一NAT)
			支持基于NAPT功能
			支持CGNAT功能
			支持全锥型NAT功能
			支持UPnP功能
		VRRP 虚拟路由器冗余协议	支持VRRP功能
			VRRP支持IPv6
			支持VRRP v4和VRRP v6同时部署, 实现IPv4/IPv6双栈网络环境中的无缝切换
			支持接口线路工作状态和VRRP接口联动
			支持对多个VRRP物理网卡的状态进行检测, 并根据网卡状态自动调整VRRP抢占优先级
			支持自定义需要监测的逻辑线路, 并根据线路状态进行自动切换
		线路监测	WAN口支持PPPOE拨号功能, 自动检测链路状态, 断线后自动拨号和支持计划定时重拨
			每条WAN线路独立健康检查, 同时支持地址池, 地址池里的每个IP可以做健康新检查
			WAN线路监控检查支持心跳时延检测, 当心跳服务器时延超过阈值时, 即认为线路处于不健康状态
			支持WAN线路汇总统计功能, 选择多条WAN线路的总流量趋势进行统计
			支持WAN线路的批量导入和导出
			支持WAN线路独立对外ping的功能
			支持基于WAN/LAN线路的路由跟踪功能
			LAN线路支持Standby功能, 增加可靠性
		端口映射	支持端口映射, 可以设置映射内网ip的某个端口或者某段连续的端口 (如映射端口5000-6000) 到某个WAN接口, 或者某些WAN线路组成的线路群组上, 同一条策略里可以支持多个离散端口映射设置, 减少策略条数
			端口映射支持源IP过滤, 只允许指定的源IP地址进行端口映射的访问
		DHCP	支持DHCP SERVER功能

			支持基于VLAN条件分配IP地址
			支持同时启用多个DHCP SERVER
			支持DHCP SERVER域选项配置（Option字段）
			支持配置例外IP，指定IP群组内的IP地址不分配给终端
			支持下发无线控制器（AC）地址，可同时下发的地址数量为2，满足AP与AC主备策略的需求
			支持DHCPv6有状态地址分配
			支持DHCP中继功能
			DHCP中继支持IPv6，支持连接远程的DHCPv6服务器
			支持同时启用DHCP中继与DHCP服务功能
			DHCP中继支持VLAN条件，携带配置指定VLAN范围的DHCP请求才会匹配并转发至指定DHCP服务器
		PPPoE	支持PPPOE SERVER，单台最大支持在线用户不小于32000
		IPv6	支持对IPv6 2~7层流量的识别能力，特别是针对第7层的应用识别能力，能够识别主要应用协议
			支持IPv6 WAN，线路支持固定IP、DHCPv6、PPPoE IPv6等方式
			IPv6 LAN支持DHCPv6 PD(前缀代理)功能
			支持IPv6链路质量检测，检测链路的时延、丢包，并支持以检测结果为条件，设置阈值进行告警
			支持对IPv6的流量控制，对流量进行放行、阻断、通道限速等
			支持对IPv6路由，可以对IPv6的流量做路由策略
			支持IPv6到IPv4的映射，将IPv6的公网IP与内网IPv4的服务器做映射
			支持旁路或串接模式下，深度分析DHCPV6数据包，找到IP和MAC的对应关系，显示用户真实MAC
			支持IPv6地址属性识别，可以显示IPv6地址账号信息，以及进行限速
			支持静态NAT66功能
			支持动态IPv6 NAT
			支持IPv6的MAC管控
			支持内网IPv6的WEB认证
			支持DHCPv6有状态地址分配
			支持IPv6无状态地址分配
			支持V4到V6地址转换
			支持IPv6端口映射，将IPv6 WAN线路地址映射到内网IPv6服务器，满足外网IPv6主机访问内网IPv6私

			网地址主机的需求
		动态路由	支持OSPF、BGP等动态路由协议。
		ARP代理	支持ARP代理功能，使用物理网卡、VLAN、IP等条件策略，对匹配条件的ARP请求进行代理，并转发对应的流量数据，从而实现对东西向流量的分析与管控
		网卡抓包	支持对流经设备的原始数据包进行抓取与下载 支持指定网卡、流量方向、VLAN、协议类型、源/目IP地址、源/目端口、TCP标记、数据包类型等策略条件，对匹配条件的数据包进行抓取
5	对象库管理	对象库	支持自定义IP对象库（自定义IP群组），文件导入、导出、修改、搜索
			支持自定义域名对象库（自定义域名群组），文件导入、导出、修改、搜索
			支持第三方分类URL库，文件导入、导出、修改
			支持自定义IP地理位置库，文件导入、导出、修改、搜索
			支持IP_MAC绑定地址表，文件导入、导出、修改
			支持对象库容量大于十万条
6	智能路由	应用路由	支持基于5元组条件对流量做路由牵引
			支持基于域名条件对流量做路由牵引，跟踪DNS报文，获取指定域名的解析结果后，自动建立域名与IP的映射表，从而实现对域名的路由或NAT
			支持基于应用协议条件对流量做路由牵引
			支持基于应用分类（P2P下载、网络电视、网络游戏、Web视频和普通HTTP流量）条件对流量做路由牵引
			支持基于DSCP标签条件对流量做路由牵引
			支持基于对象库对象流量的路由牵引
			支持基于组合策略条件对流量做路由牵引
			支持对应用应用群组（自定义群组对象）条件对流量做路由牵引
			路由牵引时，WAN线路支持DNS代理功能，所有经过该WAN线路做NAT的DNS连接，其目标地址自动转换成线路的DNS地址，避免出现DNS解析异常的问题
		多线路流量牵引	支持虚拟LAN接口和WAN线路最大支持>2000条（2048条FreeBSD版本）；支持虚拟线路LAN+WAN线路最大支持4000条（仅限Linux版本）
7	负载均衡	负载模式	支持基于源IP、目的IP、源和目的IP、四元组、空闲带宽的负载均衡
			支持基于域名的负载均衡
			支持基于应用协议的负载均衡

			支持基于应用、域名混合模式的负载均衡
			支持基于对象库的负载均衡
			支持基于最大带宽负载，线路流量达到阈值后切换至其他线路
			支持负载均衡策略的生效时间设置
		多线路负载	支持虚拟LAN接口和WAN线路最大支持>2000条（2048条FreeBSD版本）；支持虚拟线路LAN+WAN线路最大支持4000条（仅限Linux版本）
		服务器负载	支持服务器负载均衡，最多可以支持100台服务器，16个服务器组
			服务器负载均衡支持根据源IP，源+目IP做HASH均衡，也支持加权轮询均衡算法
			服务器负载支持健康检测，检测方式包括ICMP与TCP
			服务器负载均衡支持域名负载
8	流量控制	控制对象参数	支持基于全局、链路、数据流向、共享用户、移动终端、应用协议/协议组和IP/IP群组的速率控制
		控制粒度	支持单条策略总控限速，可分别设置总控带宽。
			支持单条策略单IP限速，可分别设置单IP带宽。
			支持带宽控制颗粒度50 kbs（精细化控制限速颗粒度可达到1kbps）
		控制条件	支持基于IP五元组的流量控制
			支持基于VLAN的流量控制
			支持基于会话首包的流量控制方式
			支持基于应用协议和应用协议群组的流量控制；
			支持基于域名的流量控制；
			支持基于AD域账号/用户组的流量控制；
			支持基于对象库的流量控制；
			支持流量控制基于当日流量配额上限的控制；
			支持基于线路、数据流向、内网地址、外网地址、传输协议、应用协议、内网端口、外网端口、IP优先级等条件进行流量控制；
			支持基于策略对数据包的IP优先级（0-6，七个优先级）标记；
			支持基于时间在线IP数调度流量控制策略
			支持检测并控制网关“一拖N”行为功能；基于7层协议特征检测网关后面的私有IP地址信息，并能以“共享IP数”如“共享用户超过3人”为触发条件，对宿主IP进行两大类控制动作：流量控制和HTTP管控

			支持同时基于应用协议和IP地址的优先级调度功能
			数据通道支持“子通道优先级”功能； 每个数据通道中均可设置多个优先级为1-16的“带宽保证”类的子通道，保证类子通道所配置的带宽，用时自动占用，不用则自动释放，真正达到基于应用层（应用协议）的“按需占用、无需干预、智能带宽”（向下支持网络层基于IP）
			支持“动态IP限速”功能（智能调控），可在启用此功能的链路中，针对单个IP设置“加速比”、“减速比”、“速度维持时间”等参数，百分比模式设置
			支持设置“带宽使用阈值”功能，可对具体链路设置“带宽使用下限”和“带宽使用上限”，百分比模式设置
			支持根据内网用户MAC做控制（IP或MAC做备注，选择用户组/地址池），表项最大支持2048
			支持对多个策略组进行调度，多个策略组可以同时生效
			支持策略嵌套，在同一条策略中，既可以针对特定对象（IP或应用）进行总的的数据通道控制，也可以单IP限速，同时可并列匹配“DSCP标记”等参数，实现策略的高度灵活性和简洁性
			支持两级策略匹配，先匹配策略组，后匹配策略，实现策略的高度灵活性、高效率，方便维护
			支持多条策略的一键“启用”、“禁用”和“删除”功能
		流量控制动作	支持流量阻断控制
			支持流量限速控制
			支持URL和DNS流量重定向控制
			提供控制速率前后对比
		IP黑名单	支持单独的IP黑名单设置，阻断其连接，IP黑名单也可以批量进行导入
			支持对IP黑名单内成员设置控制时长，到期后自动放行
9	智能控制功能	连接数控制	基于应用协议/协议组，支持针对内网每IP的TCP、UDP和总并发连接数控制
			支持限制内网IP到外网特定目标地址的每IP的TCP、UDP和总的应用并发连接数控制
			可根据数据链路、VLAN、外网地址、内网地址和应用协议/协议组、内网端口、外网端口等参数制定连接数控制策略
			支持针对“DNS连接”的控制/不控制选项
			支持针对“DNS连接”的控制时，被拒绝的连接可以在在指定时间内被释放
			可根据时间和在线IP数等参数启用相应策略
			可设置内网IP最大并发连接数，超过这个阈值的连接不再创建

		HTTP管控	支持HTTP协议的URL管控
			支持HTTPS协议的SNI（域名）管控
			支持IPv4和IPv6流量下的HTTP管控
			串接模式下，支持URL重定向
			旁路模式下，支持URL重定向
			支持Web信息提示
			支持（HTTP方式）文件类型的访问控制，控制用户通过HTTP方式访问或下载.exe、.rmvb、.mp3等类型的文件
			支持根据内网IP、文件类型、访问方法(GET或POST)和目标URL等参数设置控制策略
			可根据时间和在线IP数等参数启用相应策略
			执行阻断、URL重定向、TCP重置等管控时，支持记录并发送命中日志，内容包括：MAC地址、源IP、源端口、目标IP、目标端口、访问域名、执行动作、新域名（如果为跳转）
			支持策略“启用”和禁用功能
		智能DNS控制	可根据源IP、目标IP、访问域名、所在线路等组合条件实现对域名访问的控制
			域名控制方式支持阻断、劫持和重定向和QPS限制
			可以对DNS QPS做限制，可以在一条策略里做总限制，同时对单IP再做一个子项限制
			可根据源IP、目标IP、访问域名、所在线路等组合条件实现对域名访问的QPS速率做总量控制和单IP控制
			支持DNS QPS策略前后趋势图，可以显示一天，一周和一月趋势
			支持策略“启用”和禁用功能
		移动终端识别与控制	自动对移动终端型号进行识别，不依赖特征库
			移动终端信息统计，如访问IP、首次访问时间、最近访问时间
			对移动设备的网络访问进行控制和管理
			支持黑名单，当误识别时，将时别错误的终端类型放入黑名单，避免误识别
		共享检测	能够及时检测通过路由共享上网的PC个数
			支持禁止二级路由功能，可设置白名单，白名单中的IP不受限制
			可以根据PC终端个数做条件，对流量做控制
			可以根据QQ号，微信ID，邮箱等信息作为共享判断依据，并对流量做控制
10	流量镜像	本地流量镜像	支持基于IP五元组、VLAN的流量镜像

			支持基于应用协议的流量镜像；
			支持基于协议群组的流量镜像；
			支持基于域名和URL的流量镜像；
			支持端口镜像只镜像会话前N个包功能
			支持基于时间的流量镜像调度
		远程流量镜像	支持将镜像流量指定到SD-WAN线路封装和转发到指定的目的地；
			支持基于IP五元组、VLAN的流量镜像
			支持基于协议群组的流量镜像；
			支持基于域名和URL的流量镜像；
			支持端口镜像只镜像会话前N个包功能
			支持基于时间的流量镜像调度
		应用分流	流量按流量调度策略筛选后，支持将筛选后流量进行多出口复制，最多可达到15份无性能消耗的流量复制
			可提供“应用分流”前后的速率对比
11	SD-WAN	VPN隧道承载	支持SD-WAN 接入和承载方式；
			支持IPsec接入和承载方式；
			支持L2TP VPN接入和承载方式（包含客户端和服务端均支持）；
			支持GRE接入和承载方式；
		SD-WAN接入	SD-WAN客户端支持动态IP地址接入，及ADSL线路类型的接入
			支持分支点使用域名与总部服务器进行iWAN隧道建立
			支持分部与总部之间跨运营商组网，（举例：总部电信出口，分部联通接口）
			支持在IPv6环境中使用iWAN进行组网
			支持使用iWAN进行OSPF组网，实现分支与总部间路由的动态更新
			支持分段路由（SR）技术，支持标签转发和端到端加密，实现对多个分支下IP地址段重复时的互联互通
			支持在三层网络基础上建立二层以太网隧道，实现跨三层、跨地域的二层网络互连
			二层隧道支持TAG/UNTAG模式配置，支持VLAN范围转发
			支持总部设备集中身份认证
			支持iWAN Server负载均衡，对iWAN服务线路的上下行流量进行监控，当某一线路流量达到阈值时，

			将选择其他线路继续进行互联流量的传输
		隧道加密	支持国际通用隧道加密方式（DES、3DES、AES等）
			支持采用国密算法进行隧道加密（SMS4）
12	PPPOE	PPPoE服务	支持PPPOE SERVER，单台最大支持32768用户在线
			支持本地认证、radius认证、免认证功能
			PPPOE SERVER支持与Radius认证计费系统对接，并能接收Radius服务器下发的限速，踢掉在线用户等指令
			可针对用户上线发布公告，用户到期提醒和过期提示
			支持地址池数目>=64个
			支持用户批量操作如（添加，删除，禁用，启用、导出、导入，绑定账号的MAC）等
			支持PPPOE拨号日志，记录用户下线原因
			支持外部BRAS认证（PPPOE旁路功能）
		PPPoE代拨	支持PPPOE代拨，最少支持24K外网代拨账号，每个代拨账号可以支持1个或多个内网IP上网
			PPPOE代拨支持IPv6
			PPPOE代拨支持CMCC PORTAL协议，可以账号透传，也可以通过RADIUS获取代拨账号
			PPPOE代拨支持单账号最大在线IP数控制
			支持PPPOE代理，可根据服务名称代理，也可以根据账号名称代理，在线代理账号数>=3000
			支持PPPOE代理，PPPOE代理账号上线后，可以发送认证日志，日志信息包括账号和IP对应关系
13	认证功能	IP MAC绑定	支持针对IP和MAC地址的绑定认证
			支持IP_MAC地址表文件导入、导出、修改
		IP备注功能	支持IP备注功能，在展示IP用户时，自动关联备注信息
		认证策略	支持对时间、IP地址、VLAN等条件，制定不同的认证策略，认证策略可指定Portal类型（本地或第三方）、认证逻辑和认证方式等
			支持每日定时强制注销所有用户的功能
		认证方式	支持基于本地设置用户名和密码的认证
			支持基于手机号短信验证码的认证
			支持基于微信公众号认证，包括公众号网页认证及关注公众号认证等方式
			支持基于微信小程序的认证
			支持基于Radius的认证

			支持结合AD域和LDAP认证功能（可以同步AD域账号，实现基于AD域账号认证和账号控制）
			AD域免认证功能（域用户通过域账号登录域服务之后，系统根据用户域信息自动建立用户认证信息，用户无需再次进行WEB认证。）
			支持企业微信、钉钉、飞书、CAS、WiFiDog以及其他采用oAuth2的三方应用
			认证方式为微信、钉钉、飞书时，支持公共认证服务，扫码设备可以在不接入内网时，帮助被扫码设备完成认证
		认证逻辑	支持选择认证，选择某一种认证方式进行认证
			支持保障认证，一种认证方式失败后，自动验证另一种认证方式
			支持双因子认证，需同时通过两种方式进行认证
		免认证对象	支持设置免认证IP、免认证MAC及免认证应用协议
			支持设置需认证IP，只对网络中部分IP进行认证
		无感知认证	支持无感知认证，用户认证后记录MAC，记录下的MAC可以在指定时间内免登录
			支持漫游认证，实现跨地域（如总部和分公司）的无感知认证，用户首次认证后，移动至另一地点，不需要重复输入账号、密码等认证信息，达到无缝切换的效果。
			支持跨三层MAC获取和绑定
			MAC记忆支持配置三层交换MAC地址
		重定向	支持HTTPS访问时可重定向到WEB认证页面
		Portal 页面自定义	支持用户自定义页面定制化功能（用于客户推广业务）
			提供Portal页面预设模板，如公共Wi-Fi模板、教育模板等，提供模板类型不少于5个
			支持外置Portal认证，并支持CMCC Web Portal协议
		嗅探	支持在旁路或串接模式下，深度分析RADIUS数据包，找到账号和IP地址对应关系
			支持在旁路或串接模式下，深度分析RADIUS数据包，找到账号的带宽限制参数，自动对相应IP做限速
			支持在旁路或串接模式下，深度分析PPPOE数据包，找到账号和IP的对应关系，并且将嗅探到的账号和本地账号用户组关联，可匹配用户组相关策略
			支持在旁路或串接模式下，深度分析DHCP数据包，找到IP和MAC的对应关系，显示用户真实MAC
			支持在旁路或串接模式下，深度分析华为5G网，找到IP和手机号码的对应关系，并且将嗅探到的手机号码和本地账号用户组关联，可匹配用户组相关策略
			支持在旁路或串接模式下，深度分析RADIUS数据包，包括自定义设置端口进行嗅探

14	业务级质量测量	业务质量测量(NPM)	支持分析流量中每一条会话，进行基于应用级的质量测量。
			支持对每条会话监测客户时延，服务时延，应用时延的指标测量。（设备到客户端的网络时延），服务时延（设备到服务器的网络时延），应用时延（会话上下行首包时间差），最大包长（会话上下行最大包的长度）。
			支持每IP用户的实时连接应用的质量监测
			支持每IP用户对端服务应用的质量监测
			支持基于五元组进行业务质量分析；
			支持基于应用进行业务质量分析；
			支持基于域名进行业务质量分析；
		网络体检	支持对网络进行整体检测，可以输出网络应用协议流量大小，应用协议类型，流量组成、网站访问、连接数信息；
			支持IP、域名、连接数的统计和可视化等信息。
15	流量监控统计	实时流量分析	支持实时显示设备接入的流量信息（上行，下行，连接数），并支持最大值、最小值及平均值统计
			支持实时显示每个接口的流量信息（上行，下行，连接数）
			支持显示实时的在线IP用户数，以及近期（1周）的峰值信息
			支持实时显示接入流量的应用协议流量占比
			支持实时显示接入流量的应用协议连接数占比
			支持对应用协议类型进行下钻，显示指定协议的统计信息，包括流量趋势，流量大小，关联的IP用户等信息
			支持实时显示某个应用下的Top用户
			支持实时显示当前所有在线IP用户数
			支持按组织架构方式展示IP用户信息
			支持实时显示每个IP当前所有连接数信息（包括应用、协议、连接状态、首包接口、源目IP地址/端口、地理位置、策略路由、接口线路、连接时长、时延信息、上下行数据包、最大包长、MSS、上下行流量大小、上下行速率、HOST信息等）
			支持实时显示IP用户画像信息（按IP进行用户画像，关联MAC、移动终端、流量大小、连接数、应用协议、连接信息、对端服务信息、虚拟身份等信息进行关联）
			支持实时显示应用协议画像信息（按协议进行协议画像，关联协议访问的流量趋势，访问IP用户，连接排名，流量大小，连接数节点信息等进行关联分析和展示。）

			支持实时显示接入流量的TOP IP信息
			支持实时显示接入流量的TOP应用协议信息
			支持实时显示接入流量的TOP连接信息
			支持实时显示每一个IP流量速率和当前各个应用的速率明细
			支持实时显示接入流量的TOP域名信息，从DNS解析维度与应用（HTTP/HTTPS）访问维度对域名访问进行展示，每个维度包含：失败的会话数、应用时延优、良、中和差的会话数，总的时延数。其中，优、良、中、差评根据时延大小进行判断，同时支持自定义。
		流量统计分析	支持提供整个系统、各链路的流量和连接数统计图表
			支持提供最近10分钟流量、累计流量、并发连接数统计图表
			支持实时显示各协议组的当前速率、连接数等统计信息，自动刷新
			支持显示最近一天、最近一周和最近一月的流量趋势图表
			支持显示上行流量、下行流量、并发连接数的“三日对比”趋势图
			支持TOP应用排序
			支持TOP用户排序
			支持实时显示每一个IP流量速率和当前各个应用的速率明细（如同时在线60万IP用户）
			支持实时显示某个IP的当前速率及连接明细，以便于异常流量诊断
			支持对IP对应的身份信息，如QQ号码、MSN账号、POP3账号、微博账号等
			支持基于应用速率、流量和连接数等条件进行排序
			可提供在线并发连接、连接新建和删除速率等数据的趋势图表
			可提供在线IPv4与IPv6用户的统计趋势图表
			可选择两个或多个应用协议进行趋势图分析对比
			可提供“应用分流”前后的速率对比
			支持“移动终端”信息统计，包含手机类型、访问IP和时间等
			支持TOP连接排序，可以指定应用和IP条件进行IP（内网IP和外网IP均可）连接数排名统计，以快速定位攻击或被攻击IP
			支持通过趋势图方式显示网络数据包PPS（Packet Per Second）的趋势
			支持通过趋势图方式显示TCP SYN数据包和SYN + ACK数据包的PPS（Packet Per Second）的趋势

			支持显示流量所匹配具体的某条策略路由信息
			支持连接信息中的TCP会话状态的显示功能
			支持自动区分会话源目功能
16	威胁情报	威胁情报功能	系统内置数字货币、C&C节点、APT攻击、网站后门、钓鱼网址、僵尸网络等16种威胁情报，针对网络异常行为进行检测分析
			支持对威胁情报的命中监测，支持查看情报命中趋势、情报类型命中分布、以及源IP、目的IP、源MAC等信息
			支持对按照威胁情报类型，对命中情报的会话进行自动阻断
			支持白名单功能，加入白名单的IP和域名，不会命中情报，不会做相应的阻断等动作
		情报管理	情报库支持在线自动同步，支持离线上传
			情报库支持的情报条目不低于百万条
			支持对接第三方威胁情报
			支持的第三方威胁情报条目数不低于百万条（高级版不低于600万条）
17	入侵检测	入侵检测（IDS）功能	系统内置漏洞、木马、Web攻击等15大类常见网络威胁特征，快速检测发现网络中的异常行为
			支持根据入侵事件发生时间，规则名称/分类，源目IP等进行会话展示，并用可视化方式展示内网入侵事件趋势
			支持针对入侵事件检测日志进行查询，包括“时间”、“源IP”、“源IP”、“目的端口”、“目的IP”、“传输协议”、“规则名称”、“规则类型”、“严重性”等条件
			支持手动导入自定义规则
18	IP防护	IP防护	支持“内网伪IP”防护功能；检测并控制内网中毒设备伪装大量假IP攻击网络的行为
			支持“垃圾包”检测及过滤功能
			支持“IP分片”攻击检测及过滤功能
			支持对异常流量IP的实时查询、日志反查功能
19	告警功能	告警功能	支持基于策略的告警功能，可根据定义监控对象阈值，实时向外告警
			支持检测系统告警，如CPU、授权、总连接数、总IP数等
			支持检测网卡告警，如任意或指定网卡状态、流入/流出速率等
			支持检测WAN线路告警，如任意或指定WAN线路的流入/流出速率、状态变化、心跳时延等
			支持检测内网IP告警，如任意IP的连接数和会话应用
			支持检测应用协议告警，如指定应用协议的上、下行流量速率

			支持针对各接口Ping检测功能，根据检测时延设置阈值，实时向外告警
			告警发送方式支持微信公众号、企业微信、邮箱、钉钉等
20	设备日志	日志功能	支持对日志配置的管理和上报
			支持系统日志（在线/离线日志、操作日志、端口UP/DOWN日志、用户上下线日志、CGNAT日志等）
			支持告警日志，如网卡状态告警
			支持以SYSLOG格式向第三方设备输出日志，输出日志内容有：URL访问、QQ登陆退出事件，MSN登陆事件，DNS查询事件，POP3登陆事件，淘宝登录账号、新浪微博账号、腾讯微博账号登录事件、微信ID发现事件等日志
21	日志审计	会话日志	支持全量记录会话日志
			支持全量记录URL日志
			支持全量DNS会话日志
			支持记录虚拟身份（微信ID、QQ号）等信息
			支持记录威胁情报命中日志
			支持按照应用协议、URL关键字、端口号、运营商等信息进行检索和查询；
			TOP域名统计，可以统计时间段内域名访问排名。
22	维 护 和 管 理	设备管理	支持记录业务的性能日志；
			支持中英文Web管理界面
			支持HTTPS、SSH管理方式
			支持“DDNS”远程管理设备
			支持串口管理设备
			支持SNMP v1/v2c/v3版本
			管理接口支持配置IPv6地址
		系统检测	支持系统自检，集中检查系统硬件和软件运行情况
		设备升级	支持Web方式的升级维护
			支持定期自动检测当前系统是否为最新版本，并进行通知
		配置文件	配置文件导入、导出功能
			支持两台设备间配置自动同步，任意一台设备的配置发生变化，均会同步到另一台设备
		默认配置恢复	一键恢复出厂设置功能（命令控制台方式）
		账号管理	支持用户权限分级，如guest账号仅具有查询权限

			支持设置账号的有效期，到期后账号自动失效
			支持设置账号的密码的复杂度选项（简单密码/复杂密码）
			支持“在线管理用户”显示及针对“非admin”强制下线功能
		IP备注	支持自定义“IP标注”功能
		系统告警	支持“系统告警”功能
			支持“系统告警”远程输出及记录文件导出功能
		上线向导	支持“上线向导”功能，协助用户快速上线
23	其他功能	第三方支持	支持和城市热点、深澜计费联动，可以实现基于账号的流量控制
			支持锐捷SAM的用户组信息对接
			支持天翼网校园APP账号识别
			支持huawei5g二次鉴权
		缓存牵引	支持缓存牵引，可以根据策略将视频或大流量下载用户牵引到指定的缓存，提升用户体验并节省带宽；
			支持对不同类型的文件牵引到不同的缓存服务器；
			最多可以支持多达128台缓存设备牵引；
24	产品服务	升级服务	年签名升级次数承诺总计8-15次
			对于用户要求识别的非加密类应用协议，承诺在72小时内完成特征库升级支持
			支持特征库独立升级，升级特征库时，不会中断网络
			支持逆向升级（版本回退）
			▲提供原厂售后服务承诺函。

2.2.5 校园网接入交换机性能要求

硬件	交换容量≥336Gbps，转发性能≥126Mpps。
	固化10/100/1000M以太网端口≥24个，1G/10G SFP+光接口≥4个。
	要求所投设备MAC地址≥16K。
	支持≥24个电口POE和POE+远程供电，整机POE功率输出≥370W。

2.2.6 校园网接入交换机技术要求

软件	▲投标产品面板自带一键查看PoE供电状态功能的PoE按钮，轻按即可查看设备当前的通信状态和供电状态，提供功能截图。
----	---

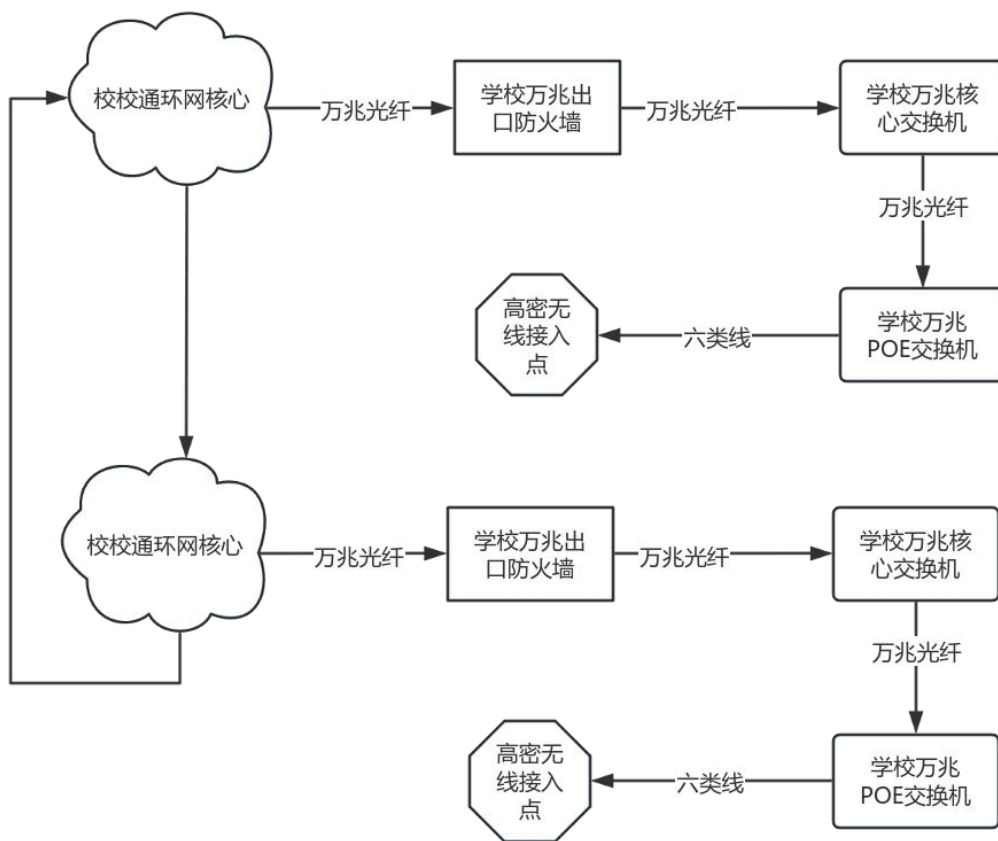
	支持IPv4和IPv6的静态路由、RIP/RIPng、OSPFv2/OSPFv3等三层路由协议。
	要求所投设备支持1对1、基于流、基于VLAN的镜像；支持RSPAN
	支持CPU保护功能，能限制非法报文对CPU的攻击，保护交换机在各种环境下稳定工作。
	▲支持专门基础网络保护机制，能够限制用户向网络中发送数据包的速率，对有攻击行为的用户进行隔离，保证设备和整网的安全稳定运行，提供功能截图。
资质	▲提供工信部设备进网许可证。
	▲提供原厂售后服务承诺函。

2.2.7 校园网光模块技术要求

指标项	招标技术参数规格要求
基本参数	支持本次投标 POE 接入交换机万兆单模互联
功能参数	光模块支持彩光，支持工作波长在 1271nm~1571nm 范围内
	▲提供原厂售后服务承诺函。

2.3校园网校园网高密AP建设

学校（高密 AP）拓扑图



主要设备为：

- 160 台高密 AP，选择三个助手试点校分配使用。

2.3.1 高密 AP 性能要求

射频	▲支持802.11ax协议；整机支持≥4条空间流；整机最大无线速率≥2.97Gbps。提供功能截图。
接口	至少支持1个1000M自适应以太网端口；至少支持1个2.5G SFP光口。

2.3.2 高密 AP 技术要求

环境与可靠性	▲由于放装AP部署在高空环境，难以时常清洁，为保障设备堆积灰尘仍可以正常运行，要求所投无线接入点符合国标GB/T 4208-2017即《外壳防护等级（IP代码）》，防尘防水等级至少达到IP41。提供第三方权威测试报告复印件证明。
安全	要求所投产品支持WPA3安全标准。提供Wi-Fi联盟出具的认证证书复印件。
资质	提供无线电发射设备型号核准复印件。产品型号需和核准型号保持一致。
软件能力	AP整机最大终端接入数≥256个。 支持Long GI配置。

	所投AP具有WLAN自动网优功能，不借助任何网络优化软件，仅通过AP配置进行无线网络优化，降低无线网络中的频段干扰。
	支持1024QAM调制解调方式。
	支持SSID隐藏，支持为每个SSID配置单独的认证方式、加密机制，VLAN属性。
	支持边缘智能感知（RIPT）。
	支持终端智能识别技术，可识别终端类型并上报。
	支持基于SSID、射频卡的接入用户数限制。
	支持基于终端数或流量的智能负载均衡，支持基于STA/SSID/AP的限速。
	支持胖模式（云模式）、瘦模式切换。
兼容性	▲因教育局没有无线控制器，要求投标产品能够支持并兼容教育局现有云管理平台管理，如无法被教育局现有云管理平台管理，要求提供一套无线管理平台管理本次投标设备，并且需支持并兼容管理崇明学校其他的无线设备，提供制造商承诺函，并保留测试要求。（提供的平台不收费）
	▲提供原厂售后服务承诺函。

2.4设备管理与系统升级建设

2.4.1 网络设备监控

所投标设备需对接到《崇明教育网络设备管理系统》。本系统支持学校计算机老师自主简易管理网络设备和系统拓扑查看。投标时需在投标方案里写明对接方式和对接后可使用功能，最大程度遵从 RFC 规范。（投标需提供完整的技术对接方案）

2.4.2 无线接入认证

无线高密需接入《崇明教育基座认证系统》。本系统需要支持与现有认证系统对接。（投标需提供完整的技术对接方案）

2.5国密改造建设

▲本次项目需对认证中心和组织中心进行密码等级保护建设和系统升级并协助其他第三方完成商密系统对接与改造。（投标需提供后期对接承诺函）

2.5.1 云加密机性能要求

名称	功能要求
云加密机	国产处理器，国产系统，2U，6个千兆电口，4个千兆光口，冗余电源，2个扩展槽位，国密 IPSEC VPN最大理论吞吐率：800Mbps 国密 IPSEC VPN最大理论隧道数：6000条 国密 SSL VPN最大理论吞吐率：300Mbps 国密 SSL VPN最大

	建议并发用户数：1800，包含400个SSL VPN的客户端并发许可；可扩展PC端可信接入模块、可扩展短信认证模块，可扩展入侵防御模块，可扩展应用过滤模块，可扩展PC端Windows系统病毒检查模块。
--	--

2.5.2 云加密机技术要求

功能类别	功能要求
产品要求	产品必须为专业性VPN硬件设备，而非下一代防火墙\UTM 类设备集成的VPN模块。
用户管理	支持静态用户名口令、数字证书、短信、硬件特征码绑定、图形码认证方式；（提供截图证明） 支持两种或两种以上组合认证方式；（提供截图证明） 支持国密USBKey的自适配功能，无需适配工作即可完成国密证书的认证； 支持用户名口令认证防暴力破解； 支持使用邮件、短信方式密码找回； 支持对用户口令复杂度和有效性设置； 支持Web方式单点登录，用户登录VPN后无需二次输入用户名口令即可登录应用系统； 支持用户自行修改单点登陆的账户信息； 支持Windows、iOS、Android、Linux、Mac客户端接入方式； 支持国产操作系统客户端接入方式，包括但不限于：麒麟、统信、深度、中科方德等； 支持使用RADIUS、TACACS、LDAP安全认证方式； 支持对接企业微信实现企业微信扫码认证； 支持对接谷歌软件令牌认证； ▲支持可信接入功能，能够对接接入主机的信息进行检查，包括域名、杀毒软件、必须安装的程序、必须运行的服务等；支持可信接入授权；（提供截图证明）
PKI 设置	支持内置CA，可以对证书进行生成、签发、废弃操作；（提供截图证明） 支持国际、国密算法证书； 支持DER/PEM/PKCS12等多种证书编码； 支持导入多个第三方CA根证书和CRL列表，可以对不同的CA用户证书进行身份认证； 支持通过HTTP协议定时下载同步CRL列表； 支持支持通过OCSP/LDAP等协议对CA证书进行在线认证；
SSLVPN	支持国密、国际算法； 支持压缩算法； 支持SSL VPN的防中间人攻击； 支持SSL VPN客户端和服务端双向认证； ▲支持SSL卸载功能；（提供截图证明） 支持USB Key为证书载体，支持国密、国际数字证书认证，保障接入身份可信； 支持Android及IOS移动应用中调用SSL VPN的SDK； 支持PC端、移动端客户端登录界面样式自定义设置，可设置客户端登录页背景、Logo、页脚、标题等；（提供截图证明） 支持WEB VPN功能； 支持Web VPN无客户端、支持IE、谷歌、360、火狐、搜狗等市面上主流无浏览器无插件接入； 支持Web VPN使用口令、数字证书、短信、LDAP、AD域、企业微信认证； 支持Web VPN与业务应用单点登录； ▲支持虚拟门户功能，支持虚拟门户中使用用户名口令、数字证书认证方式

	，支持虚拟门户双因子认证；（提供截图证明） 支持HTML、JSP、ASP、JAVA APPLET、ACTIVE、Cookies等各种Web应用； 支持对访问资源的健康检查； 支持对用户、用户组、用户角色可访问资源URL权限控制； 支持虚拟门户配置不同的登录界面、定制使用哪些功能模块、定制不同的认证方式、定制不同的公告信息等； 支持SSL VPN与企业门户无缝融合，即用户可以通过企业门户登录SSL VPN，并且SSL VPN能够自动跳转Portal页面到企业的某个网站； 支持拔KEY隧道自动中断，支持用户超时自动退出，超时时间可以设置； 支持会话功能，能够实时监控在线用户的登录时间、登录IP、在线时间、访问流量，登录设备等多种信息；
IPSecVPN	支持国际、国密1.0、国密1.1协议； 支持SM2、RSA非对称算法； 支持SM4、AES128、AES192、AES256等对称算法； 支持SM3、SHA256、SHA384、SHA512等摘要算法； 支持IKEv1、IKEv2、野蛮协商模式； 支持虚拟路由、隧道转发； 支持使用标准的X.509证书建立隧道； 支持网状、树型、星型等多种VPN网络拓扑； 支持GRE隧道； 支持使用IPsec VPN客户端接入，支持IPsec VPN客户端接入后配置访问权限； 支持使用域名进行隧道定义及协商； 支持使用天融信集中管理平台对IPSec隧道进行集中管理、策略下发； 支持L2tp VPN；
业务监控	▲支持设备的运行状态、设备资源状态、并发用户数、客户端类型分布、IPSEC隧道状态、用户流量、安全事件、中国任意省市区的接入用户数监控，并通过图表展示；（提供截图证明）
安全防护	支持基于源/目的IP地址、MAC地址、端口和协议、时间、用户、角色的访问控制； 支持基于状态检测的动态包过滤； 支持隧道内的访问控制； 支持动态端口协议：SIP、FTP、RTSP、SQL*NET、MMS、RPC、TFTP、PPTP； 支持动态地址转换和静态地址转换，支持多对一、一对多和一对一等多种方式的地址转换； 支持双向NAT，支持NAT 6to4、4to6、4to4、6to6； 支持流量控制，可对链路的速率、最大速率、优先级等进行设定；（提供截图证明） 支持SPA单包认证功能； ▲支持入侵防御功能；（提供截图证明） ▲支持入侵防御规则库更新；（提供截图证明） 支持入侵防御日志记录； ▲支持应用访问控制功能；（提供截图证明） ▲支持应用规则库更新；（提供截图证明） 支持应用访问控制日志记录；
网络管理	支持IPv6协议数据报通信； 支持链路聚合功能； 支持DDNS动态域名解析；（提供截图证明） 支持网络加速功能；通过网络加速功能动态地调整拥塞窗口大小和发送速率。（提供功能截图证明）
告警管理	支持邮件、声音、SNMP、控制台等报警方式；

	支持系统诊断管理；（提供截图证明）
日志管理	支持设备内置日志记录保存； 支持按照磁盘占用百分比及最大保留天数自动删除日志 支持日志详细记录用户行为，包括但不限于登陆IP、登陆时间、登陆成功失败情况等； 支持日志详细记录管理员行为，包括但不限于管理员账号名称、操作行为等
系统管理	支持对系统时间、信息设置，可通过管理页面对系统进行重启管理。 支持PING、TRACEROUTE、TCP、HTTP、DNS网络诊断。 支持管理员分权管理，根据不同管理可以管理不同的功能模块； 支持管理员对接外部Radius、LDAP、Tacacs服务器认证； 支持管理员密码复杂度、密码过期提醒、强制修改密码配置； 支持管理员最大在线数设置；
高可用性	支持双机热备模式部署，在双机热备模式下支持SSL VPN授权漂移功能； 支持集群管理，在SSLVPN负载均衡模式下VPN不需要借助其他负载产品可以完成负载分发工作；（提供功能截图证明）
产品资质	▲具备商用密码产品认证证书，满足GM/T 0023《IPSec VPN 网关产品规范》、GM/T 0025《SSL VPN 网关产品规范》和GM/T0028《密码模块安全技术要求》第二级要求。（提供证书复印件并原厂盖章）
	▲具备网络安全专用产品安全检测证书。（提供证书复印件并原厂盖章）
	▲具备EAL3增强级认证。（提供证书复印件并原厂盖章）
	具备IPv6 Ready Logo认证（提供证书复印件并原厂盖章）
	▲提供原厂售后服务承诺函。

2.5.3 服务器密码机性能要求

名称	硬件规格/性能要求
服务器密码机	2U, 国产处理器，国产系统，1个管理口，1个HA口，4个千兆电口，4个SFP插槽，32G内存，4TB企业级硬盘，冗余电源，2个扩展槽位，SM2算法密钥最大生成速率：5000对/秒 SM2算法最大签名速率：8000次/秒 SM2算法最大验签速率：4000次/秒 SM3算法最大校验吞吐率：1300Mbps SM4算法最大加解密吞吐率：2100Mbps。

2.5.4 服务器密码机技术要求

功能类别	功能要求
基本功能	通过数字签名可以保证信息传输的完整性、对发送者进行源认证以及防抵赖支持用户自行修改单点登陆的账户信息
	支持三层密钥结构：管理密钥、用户密钥/设备密钥/密钥加密密钥、会话密钥
	具备四路随机噪声源，采用由国家密码管理局批准使用的物理噪声源发生器芯片生成随机数
	▲符合GM/T 0018-2012《密码设备应用接口规范》标准，支持WINDOWS、LINUX系统平台，提供JAVA、C语言的接口，具备高兼容性（提供截图证明）
业务配置	支持白名单IP授权登录管理页面
	业务通信支持国际和国密协议
应用接口	支持多操作系统Linux、Windows；
	支持API接口描述，包括接口类别、接口实例，根据所选择的具体接口，显示该接口函数的名称、参数、以及示例demo；
密码算法	▲支持国密算法SM2/SM3/SM4；支持算法模式：ECB、CBC、CFB、OFB；支持杂凑算法：MD4、MD5、SHA1、SHA2；支持SM2和RSA的数字信封转换；支持会话密钥生成、导入、导出、协商及销毁；支持基于兑成算法的MAC消

	息鉴别码产生及验证；支持密钥的全生命周期管理：密钥的生成、存储、使用、备份、恢复、删除、销毁等功能（提供截图证明）
日志管理	支持配置管理日志、系统日志、业务日志审计，支持按日志类型、时间、级别、关键词等分类查询
	支持日志级别自定义配置
	支持将日志本地存储和第三方日志服务器传输，且传输日志可以通过对称算法进行加密
系统管理	支持三元管理
	支持手动与本地同步两种方式修改系统时间
	支持负载均衡模式多机并行
	可支持单机上扩展多块密码卡
	支持基于TFTP服务器、FTP服务器和本地方式升级设备的系统软件
	可展示与其建立连接的所有连接的基本信息，包括协议、本地IP/端口、连接IP/端口以及连接状态
	支持对配置文件的备份、下载、删除、恢复和上载； 具备系统密码服务的自监控能力，服务器密码机系统运行过程中进行自检测，系统运行异常将停止服务，并且上报服务状态，用户可以实时查看密码服务状态
产品资质	支持对部分配置本地和异地的批量导出和导入；
	▲具备商用密码产品认证证书，满足GM/T0030《服务器密码机技术规范》和GM/T0028《密码模块安全技术要求》第二级要求。（提供证书复印件并原厂盖章）
	▲具备网络安全专用产品安全检测证书。（提供证书复印件并原厂盖章）
	具备软件著作权证书。（提供证书复印件并原厂盖章）
	▲提供原厂售后服务承诺函。

2.5.5 签名验签服务器性能要求

名称	硬件规格/性能要求
服务器密码机	2U, 国产处理器, 国产系统, 1个管理口, 1个HA口, 4个千兆电口, 4个SFP插槽, 32G内存, 4TB企业级硬盘, 冗余电源, 2个扩展槽位, SM2算法密钥最大生成速率: 5000对/秒 SM2算法最大签名速率: 8000次/秒 SM2算法最大验签速率: 4000次/秒 SM3算法最大校验吞吐率: 1300Mbps SM4算法最大加解密吞吐率: 2100Mbps SM2算法制作数字信封最大速率: 4000次/秒 SM2算法拆解数字信封最大速率: 3000次/秒

2.5.6 签名验签服务器技术要求

功能类别	功能要求
基本功能	通过数字签名可以保证信息传输的完整性、对发送者进行源认证以及防抵赖支持用户自行修改单点登陆的账户信息
	支持三层密钥结构：管理密钥、用户密钥/设备密钥/密钥加密密钥、会话密钥
	具备四路随机噪声源，采用由国家密码管理局批准使用的物理噪声源发生器芯片生成随机数
	▲符合GM/T 0018-2012《密码设备应用接口规范》标准，支持WINDOWS、LINUX系统平台，提供JAVA、C语言的接口，具备高兼容性（提供截图证明）

	明)
业务配置	支持白名单IP授权登录管理页面
	业务通信支持国际和国密协议
应用接口	支持多操作系统Linux、Windows;
	支持API接口描述, 包括接口类别、接口实例, 根据所选择的具体接口, 显示该接口函数的名称、参数、以及示例demo;
密码算法	▲支持国密算法SM2/SM3/SM4; 支持算法模式: ECB、CBC、CFB、OFB; 支持杂凑算法: MD4、MD5、SHA1、SHA2; 支持SM2和RSA的数字信封转换; 支持会话密钥生成、导入、导出、协商及销毁; 支持基于兑成算法的MAC消息鉴别码产生及验证; 支持密钥的全生命周期管理: 密钥的生成、存储、使用、备份、恢复、删除、销毁等功能(提供截图证明)
日志管理	支持配置管理日志、系统日志、业务日志审计, 支持按日志类型、时间、级别、关键词等分类查询
	支持日志级别自定义配置
	支持将日志本地存储和第三方日志服务器传输, 且传输日志可以通过对称算法进行加密
系统管理	支持三元管理
	支持手动与本地同步两种方式修改系统时间
	支持负载均衡模式多机并行
	可支持单机上扩展多块密码卡
	支持基于TFTP服务器、FTP服务器和本地方式升级设备的系统软件
	可展示与其建立连接的所有连接的基本信息, 包括协议、本地IP/端口、连接IP/端口以及连接状态
	支持对配置文件的备份、下载、删除、恢复和上载;
	具备系统密码服务的自监控能力, 服务器密码机系统运行过程中进行自检, 系统运行异常将停止服务, 并且上报服务状态, 用户可以实时查看密码服务状态
	支持对部分配置本地和异地的批量导出和导入;
产品资质	▲具备商用密码产品认证证书, 满足GM/T0030《服务器密码机技术规范》和GM/T0028《密码模块安全技术要求》第二级要求。(提供证书复印件并原厂盖章)
	▲具备网络安全专用产品安全检测证书。(提供证书复印件并原厂盖章)
	具备软件著作权证书。(提供证书复印件并原厂盖章)
	▲提供原厂售后服务承诺函。

2.5.7 国密门禁管理系统技术要求

名称	硬件规格/性能要求
国密门禁管理系统	(1) 采用C/S结构, 支持TCP/IP协议 (2) ▲标配国密二级加密卡, 具有符合0036要求的国密产品认证证书(签订合同前提供复印件加盖原厂公章); (3) ▲支持通过国密密码模块, 对逐条门禁记录进行完整性保护和对一段时间内产生的记录进行完整性保护;(提供截图证明) (4) ▲通过界面直接查看完整性记录情况。门禁完整性的设计采用的SM2算法, 可提供产品的进出记录完整性保护实现的代码片段;(提供截图证明) (5) ▲即插即用, 无需与密码机或签名验签服务器联调;(提供投标人承诺证明)

	(6) 可生成Excel表格将其记录存入其他硬盘，能使所有授权自动、有序地保留发生过的记录； (7) 各类信息分类显示，包括持卡人出入事件、报警事件、系统日志事件等，查询方式多种多样，可以按部门，进入时间，门的位置，人员编号等各种条件查询； (8) 支持数据导入、导入查询功能，在有大量的部门数据、人员数据时，可以通过数据导入添加部门及人员； (9) 在特定的读卡器刷卡统计考勤，每月生成统计表格，按时间段统计； (10) 具备扩容改造的后续手段。
--	---

2.5.8 国密门禁控制器技术要求

名称	硬件规格/性能要求
国密门禁控制器	(1) 电源供应：双电源，不小于DC12V @200mA； (2) 离线读卡量：≥500000张，离线事件记录：≥200000条； (3) 32位微处理器，内嵌Linux操作系统，并为非基于PC（含商用计算机和工控机）的工业级设备，具有高稳定性的模块化结构； (4) 具有≥4个按钮输入、≥4组锁继电器输出，防拆、电池、AC电源故障输入报警等；支持≥2个RS-485口，≥2个维根口，≥1个TCP/IP协议； (5) 通过3个LED灯分别显示设备状态，总线状态和电锁状态； (6) 总线采用高抗干扰的CAN总线； (7) 支持网络安全策略与数据通讯加密； (8) 在与文件服务器的联络中断时，门禁控制器可以独立工作

2.5.8 视频监控安全一体机技术要求

名称	硬件规格/性能要求
视频监控安全一体机	桌面式结构，产品支持8路视频接入；内置国密安全芯片，支持SM1/SM2/SM3/SM4算法，支持8路1080P视频接入，支持UDP协议，兼容H.264和H.265编码协议，支持对符合GB/T28181的视频流进行传输的完整性保护，支持对NVR存储的视频数据进行完整性保护。

2.6 企业及实施团队要求

投标人具备 ISO 27001 信息安全管理证书，ISO 20000 信息技术服务管理体系认证证书，需提供完整的、经验丰富的项目实施团队，并安排专属项目经理作为双方日常沟通的接口，确保项目的顺利实施和日常运转。

项目实施团队具备以下资质证书或相关证明，其中项目经理 1 名，具有一级建造师（通信与广电工程）以及高级工程师（计算机技术及应用）证书；技术负责人 1 名，具备信息安全工程师证书；项目组成员有 2 人及以上具备网络工程师

证书，有 2 人及以上具备注册信息安全专业证书。

2.7 售后服务要求

投标人需针对项目实际情况组建经验丰富的售后服务支持团队，并编制合理且完整的售后维护方案和应急响应预案。售后服务支持团队人员组织架构清晰。

服务响应时间：免费服务期内提供 7×24 小时运维保障服务，服务响应时间 ≤ 0.5 小时，系统故障修复时间 ≤ 2 小时，并提供无推诿承诺。

2.8 验收标准和方式

2.8.1 验收标准：

项目根据合同的规定完成后，业主方应及时进行根据合同的规定进行项目成果验收。中标供应商应当以书面形式向业主方递交验收通知书，业主方在收到验收通知书后的 10 个工作日内，确定具体日期，由双方按照本合同的规定完成项目的验收。

2.8.2 验收方式：

业主方根据合同的规定对项目验收合格后，业主方收取发票并签署初验及终验完工单。业主方法定代表人、项目负责人或其他授权代表签署验收单即视为验收合格。业主方未及时组织验收或验收合格后未按时签署验收单其他验收合格确认文件的，经中标供应商合理催告后三日内仍未完成的，视为验收通过。

四：其他约定

1. 本项目设备验收合格后质保期 3 年。

第四章：合同主要条款指引

包 1 合同模板：

[合同中心-合同名称]

合同统一编号： [合同中心-合同编码]

合同内部编号：

合同各方：

甲方： [合同中心-采购单位名称]

地址： [合同中心-采购单位所在地]

邮政编码： [合同中心-采购人单位邮编]

电话： [合同中心-采购单位联系人电话]

传真： [合同中心-采购人单位传真]

联系人： [合同中心-采购单位联系人]

[供应商信息-联合体]

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》之规定，本合同当事人在平等、自愿的基础上，经协商一致，同意按下述条款和条件签署本合同：

1. 乙方根据本合同的规定向甲方提供以下服务：

1. 1 乙方所提供的服务其来源应符合国家的有关规定，服务的内容、要求、服务质量等详见合同附件。

2. 合同价格、服务地点和服务期限

2. 1 合同价格

本合同价格为[合同中心-合同总价]元整（[合同中心-合同总价大写]）。

乙方为履行本合同而发生的所有费用均应包含在合同价中，甲方不再另行支付其它任何费用。

2. 2 服务地点

2. 3 服务期限

本服务的服务期限：**[合同中心-合同有效期]**。

3. 质量标准和要求

3. 1 乙方所提供的服务的质量标准按照国家标准、行业标准或制造厂家企业标准确定，上述标准不一致的，以严格的标准为准。没有国家标准、行业标准和企业标准的，按照通常标准或者符合合同目的的特定标准确定。

3. 2 乙方所交付的服务还应符合国家和上海市有关安全、环保、卫生之规定。

4. 权利瑕疵担保

4. 1 乙方保证对其交付的服务享有合法的权利。

4. 2 乙方保证在服务上不存在任何未曾向甲方透露的担保物权，如抵押权、质押权、留置权等。

4. 3 乙方保证其所交付的服务没有侵犯任何第三人的知识产权和商业秘密等权利。

4. 4 如甲方使用该服务构成上述侵权的，则由乙方承担全部责任。

5. 验收

5. 1 服务根据合同的规定完成后，甲方应及时进行根据合同的规定进行服务验收。乙方应当以书面形式向甲方递交验收通知书，甲方在收到验收通知书后的10个工作日内，确定具体日期，由双方按照本合同的规定完成服务验收。甲方有权委托第三方检测机构进行验收，对此乙方应当配合。

5. 2 如果属于乙方原因致使系统未能通过验收，乙方应当排除故障，并自行承担相关费用，同时进行试运行，直至服务完全符合验收标准。

5. 3 如果属于甲方原因致使系统未能通过验收，甲方应在合理时间内排除故障，再次进行验收。如果属于故障之外的原因，除本合同规定的不可抗力外，甲方不愿或未能在规定的时间内完成验收，则由乙方单方面进行验收，并将验收报告提

交甲方，即视为验收通过。

5. 4 甲方根据合同的规定对服务验收合格后，甲方收取发票并签署验收意见。

6. 保密

6. 1 如果甲方或乙方提供的内容属于保密的，应签订保密协议，甲乙双方均有保密义务。

7. 付款

7. 1 本合同以人民币付款（单位：元）。

7. 2 本合同款项按照以下方式支付。

7. 2. 1 付款内容：（分期付款）

7. 2. 2 付款条件：

[合同中心-支付方式名称]

合同签订之后且全部到货安装完毕后，付款合同总额的 50%；整体验收通过后付款合同总额的 40%；正式投入使用 3 个月后再付 10%。

8. 甲方（甲方）的权利义务

8. 1、甲方有权在合同规定的范围内享受，对没有达到合同规定的服务质量或标准的服务事项，甲方有权要求乙方在规定的时间内加急提供服务，直至符合要求为止。

8. 2 如果乙方无法完成合同规定的服务内容、或者服务无法达到合同规定的服务质量或标准的，造成的无法正常运行，甲方有权邀请第三方提供服务，其支付的服务费用由乙方承担；如果乙方不支付，甲方有权在支付乙方合同款项时扣除其相等的金额。

8. 3 由于乙方服务质量或延误服务的原因，使甲方有关或设备损坏造成经济损失的，甲方有权要求乙方进行经济赔偿。

8. 4 甲方在合同规定的服务期限内义务为乙方创造服务工作便利，并提供适合的工作环境，协助乙方完成服务工作。

8. 5 当或设备发生故障时，甲方应及时告知乙方有关发生故障的相关信息，以便乙方及时分析故障原因，及时采取有效措施排除故障，恢复正常运行。

8. 6 如果甲方因工作需要对原有进行调整, 应有义务并通过有效的方式及时通知乙方涉及合同服务范围调整的, 应与乙方协商解决。

9. 乙方的权利与义务

9. 1 乙方根据合同的服务内容和要求及时提供相应的服务, 如果甲方在合同服务范围外增加或扩大服务内容的, 乙方有权要求甲方支付其相应的费用。

9. 2 乙方为了更好地进行服务, 满足甲方对服务质量的要求, 有权利要求甲方提供合适的工作环境和便利。在进行故障处理紧急服务时, 可以要求甲方进行合作配合。

9. 3 如果由于甲方的责任而造成服务延误或不能达到服务质量的, 乙方不承担违约责任。

9. 4 由于因甲方工作人员人为操作失误、或供电等环境不符合合同设备正常工作要求、或其他不可抗力因素造成的设备损毁, 乙方不承担赔偿责任。

9. 5 乙方保证在服务中, 未经甲方许可不得使用含有可以自动终止或妨碍系统运作的软件和硬件, 否则, 乙方应承担赔偿责任。

9. 6 乙方在履行服务时, 发现存在潜在缺陷或故障时, 有义务及时与甲方联系, 共同落实防范措施, 保证正常运行。

9. 7 如果乙方确实需要第三方合作才能完成合同规定的服务内容和质量的, 应事先征得甲方的同意, 并由乙方承担第三方提供服务的费用。

9. 8 乙方保证在服务中提供更换的部件是全新的、未使用过的。如果或证实服务是有缺陷的, 包括潜在的缺陷或使用不符合要求的材料等, 甲方可以根据本合同第 10 条规定以书面形式向乙方提出补救措施或索赔。

10. 补救措施和索赔

10. 1 甲方有权根据质量检测部门出具的检验证书向乙方提出索赔。

10. 2 在服务期限内, 如果乙方对提供服务的缺陷负有责任而甲方提出索赔, 乙方应按照甲方同意的下列一种或多种方式解决索赔事宜:

(1) 根据服务的质量状况以及甲方所遭受的损失, 经过买卖双方商定降低服务的价格。

(2) 乙方应在接到甲方通知后七天内, 根据合同的规定负责采用符合规定的规格、质量和性能要求的新零件、部件和设备来更换在服务中有缺陷的部分或修补

缺陷部分，其费用由乙方负担。

(3) 如果在甲方发出索赔通知后十天内乙方未作答复，上述索赔应视为已被乙方接受。如果乙方未能在甲方发出索赔通知后十天内或甲方同意延长的期限内，按照上述规定的任何一种方法采取补救措施，甲方有权从应付的合同款项中扣除索赔金额，如不足以弥补甲方损失的，甲方有权进一步要求乙方赔偿。

11. 履约延误

11.1 乙方应按照合同规定的时间、地点提供服务。

11.2 如乙方无正当理由而拖延服务，甲方有权没收乙方提供的履约保证金，或解除合同并追究乙方的违约责任。

11.3 在履行合同过程中，如果乙方可能遇到妨碍按时提供服务的情况时，应及时以书面形式将拖延的事实、可能拖延的期限和理由通知甲方。甲方在收到乙方通知后，应尽快对情况进行评价，并确定是否同意延期提供服务。

12. 误期赔偿

12.1 除合同第13条规定外，如果乙方没有按照合同规定的时间提供服务，甲方可以应付的合同款项中扣除误期赔偿费而不影响合同项下的其他补救方法，赔偿费按每(天)赔偿延期服务的服务费用的百分之零点五(0.5%)计收，直至提供服务为止。但误期赔偿费的最高限额不超过合同价的百分之五(5%)。(一周按七天计算，不足七天按一周计算。)一旦达到误期赔偿的最高限额，甲方可考虑终止合同。

13. 不可抗力

13.1 如果合同各方因不可抗力而导致合同实施延误或不能履行合同义务的话，不应该承担误期赔偿或不能履行合同义务的责任。

13.2 本条所述的“不可抗力”系指那些双方不可预见、不可避免、不可克服的事件，但不包括双方的违约或疏忽。这些事件包括但不限于：战争、严重火灾、洪水、台风、地震、国家政策的重大变化，以及双方商定的其他事件。

13.3 在不可抗力事件发生后，当事方应尽快以书面形式将不可抗力的情况和原因通知对方。合同各方应尽可能继续履行合同义务，并积极寻求采取合理的措施

履行不受不可抗力影响的其他事项。合同各方应通过友好协商在合理的时间内达成进一步履行合同的协议。

14. 履约保证金

14.1 在本合同签署之前，乙方应向甲方提交一笔金额为元人民币的履约保证金。履约保证金应自出具之日起至全部服务按本合同规定验收合格后三十天内有效。在全部服务按本合同规定验收合格后 15 日内，甲方应一次性将履约保证金无息退还乙方。

14.2 履约保证金可以采用支票或者甲方认可的银行出具的保函。乙方提交履约保证金所需的有关费用均由其自行承担。

14.3 如乙方未能履行本合同规定的任何义务，则甲方有权从履约保证金中得到补偿。履约保证金不足弥补甲方损失的，乙方仍需承担赔偿责任。

15. 争端的解决

15.1 合同各方应通过友好协商，解决在执行本合同过程中所发生的或与本合同有关的一切争端。如从协商开始十天内仍不能解决，可以向同级政府采购监管部门提请调解。

15.2 调解不成则提交上海仲裁委员会根据其仲裁规则和程序进行仲裁。

15.3 如仲裁事项不影响合同其它部分的履行，则在仲裁期间，除正在进行仲裁的部分外，本合同的其它部分应继续执行。

16. 违约终止合同

16.1 在甲方对乙方违约而采取的任何补救措施不受影响的情况下，甲方可在下列情况下向乙方发出书面通知书，提出终止部分或全部合同。

(1) 如果乙方未能在合同规定的期限或甲方同意延长的期限内提供部分或全部服务。

(2) 如果乙方未能履行合同规定的其它义务。

16.2 如果乙方在履行合同过程中有不正当竞争行为，甲方有权解除合同，并按《中华人民共和国反不正当竞争法》之规定由有关部门追究其法律责任。

17. 破产终止合同

17.1 如果乙方丧失履约能力或被宣告破产，甲方可在任何时候以书面形式通知

乙方终止合同而不给乙方补偿。该终止合同将不损害或影响甲方已经采取或将要采取任何行动或补救措施的权利。

18. 合同转让和分包

18.1 除甲方事先书面同意外，乙方不得转让和分包其应履行的合同义务。

19. 合同生效

19.1 本合同在合同各方签字盖章并且甲方收到乙方提供的履约保证金后生效。

19.2 本合同一式份，甲乙双方各执一份。一份送同级政府采购监管部门备案。

20. 合同附件

20.1 本合同附件包括： 招标(采购)文件、投标（响应）文件

20.2 本合同附件与合同具有同等效力。

20.3 合同文件应能相互解释，互为说明。若合同文件之间有矛盾，则以最新的文件为准。

21. 合同修改

21.1 除了双方签署书面修改协议，并成为本合同不可分割的一部分之外，本合同条件不得有任何变化或修改。

签约各方：

甲方（盖章）：

法定代表人或授权委托人（签章）：

[供应商法定代表人-联合体]

合同签订点:网上签约

第五章：评 审 办 法

一、主要政策

根据政府采购法，政府采购应当有助于实现国家的经济和社会发展政策目标，包括保护环境，扶持不发达地区和少数民族地区，促进中小企业发展等。

列入财政部、发展改革委发布的《节能产品政府采购品目清单》中强制采购类别的产品，按照规定实行强制采购；列入财政部、发展改革委、生态环境部发布的《节能产品政府采购品目清单》和《环境标志产品政府采购品目清单》中优先采购类别的产品，按规定实行优先采购。

中小企业按照《政府采购促进中小企业发展管理办法》享受中小企业扶持政策，对预留份额项目专门面向中小企业采购，对非预留份额采购项目按照规定享受价格扣除优惠政策。中小企业投标应提供《中小企业声明函》。享受扶持政策获得政府采购合同的，小微企业不得将合同分包给大中型企业，中型企业不得将合同分包给大型企业。

在政府采购活动中，监狱企业和残疾人福利性单位视同小型、微型企业，监狱企业应当提供由省级以上监狱管理局、戒毒管理局(含新疆生产建设兵团)出具的属于监狱企业的证明文件，残疾人福利性单位应当提供《残疾人福利性单位声明函》。

如果有国家或者上海市规定政府采购应当强制采购或优先采购的其他产品和服务，按照其规定实行强制采购或优先采购。

非预留份额专门面向中小企业采购的项目或包件，对小微企业报价给予 10% 的扣除，用扣除后的价格参与评审；非预留份额专门面向中小企业采购且接受联合体投标或者允许分包的项目或包件，对于联合协议或者分包意向协议中约定小微企业的合同份额占到合同总金额 30% 以上的投标人，给予其报价 5% 的扣除，用扣除后的价格参与评审。以联合体形式参加政府采购活动，联合体各方均为中小企业的，联合体视同中小企业。其中，联合体各方均为小微企业的，联合体视同小微企业。组成联合体或者接受分包的小微企业与联合体内其他企业、分包企业之间存在直接控股、管理关系的，不享受价格扣除优惠政策。符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。中小企业投标应提供《中

小企业声明函》。

二、评审办法

本项目评审采用综合评分法。满分为 100 分（不包括附加分）。本项目评标委员会由 5 人组成，由上海市政府采购专家咨询库中随机抽取产生。

中标候选人推荐办法：评标委员会成员对所有的投标文件进行独立评审、评价、打分，得出每一投标人的评语、评分。在专家评分后，供应商的最终得分按照如下方法计算：将所有专家的分值进行加和除以专家数量。按供应商最终得分的高低依次排名，推荐出中标候选人，若得分相同的，按投标报价由低到高顺序排名。得分且投标报价相同的，则由评标委员会按照少数服从多数原则投票表决。

三、评标程序

首先由评标委员会根据本项目的采购公告和招标文件的相关要求进行符合性检查，符合性检查合格的投标人方可进入商务分和技术分的评审，符合性检查不合格的投标人不能进入商务分和技术分的评审，应作为无效投标处理。

四、评分细则

评价因素	分值	评审办法	主/客观分
投标报价	10	以满足招标文件要求（指带★参数）且投标价格最低的报价为评审基准，其报价分为满分。 其他投标人的报价分=（评审基准价/报价）×10	/
重要技术规格及技术要求响应	36	根据投标人所投产品的产品性能、技术规格、参数指标，结合投标人产品材料的提供情况进行评审：投标文件需提供完整产品说明及证明材料，对“▲”重要技术参数指标进行逐条响应，未提供证明材料的则视为负偏离。 “▲”重要技术参数指标每有一项负偏离扣 1 分，扣完为止。（附“▲”指标的偏离表，打“▲”指标的响应证明文件在偏离表中列明所在投标文件中的页码，不提供本项不得分）	客观分
实施团队	10	1. 项目经理需具有一级建造师（通信与广电工程）以及高级工程师（计算机技术及应用）证书，并提供证明材料。满足得 4 分，不满足得 0 分。 2. 项目组成员具备以下资质证书或相关证明，并提供证明材料，未提供或不满足的不得分： 1) 项目技术负责人具备信息安全工程师证书，满足得 2 分，不满足得 0 分； 2) 项目组成员有 2 人及以上具备网络工程师证书，满足得 2 分，不满足得 0 分；	客观分

		3) 项目组成员有 2 人及以上具备注册信息安全专业证书, 满足得 2 分, 不满足得 0 分。	
实施方案	5	根据投标人项目实施方案中对采购需求的理解、现场环境的分析, 提出的相应的实施总体计划和流程安排的科学性、合理性、针对性, 进行综合评分; 优秀得 5 分, 好得 4 分, 较好得 3 分, 一般得 2 分; 差得 1 分, 未提供的不得分。	主观分
	4	根据投标人项目实施方案中提供各个学校相关系统的前端点位布置图和总体网络架构图, 深化设计图纸及资料齐全精准、完整科学可行性强、有针对性完成采购人实际施工需要, 进行综合评分; 优秀得 4 分, 好得 3 分, 一般得 2 分; 差得 1 分, 未提供的不得分。	主观分
	6	根据投标人集成施工后, 是否能够科学充分合规计划安排项目验收, 进行综合评分; 优秀得 6 分, 好得 5 分, 较好得 4 分, 一般得 3 分, 差得 2 分, 很差得 1 分, 未提供的不得分。	主观分
	6	根据投标人项目对接方案(第三章 2.4.1 网络设备监控的对接方案)的可行性、完整性、合理性进行综合评分) 优秀得 6 分, 好得 5 分, 较好得 4 分, 一般得 3 分, 差得 2 分, 很差得 1 分, 未提供的不得分。	主观分
	6	根据投标人项目对接方案(第三章 2.4.2 无线接入认证的对接方案)的可行性、完整性、合理性进行综合评分) 优秀得 6 分, 好得 5 分, 较好得 4 分, 一般得 3 分, 差得 2 分, 很差得 1 分, 未提供的不得分。	主观分
售后服务	8	根据售后维护方案、售后服务支持团队、应急响应预案、服务响应时间(是否在免费服务期内提供 7×24 小时运维保障服务, 服务响应时间≤0.5 小时, 系统故障修复时间≤2 小时, 并提供无推诿承诺)进行综合打分; 优秀得 8 分, 较好得 7 分, 一般得 5 分, 不合理得 2 分; 不合理且不完整得 1 分; 未提供的不得分。	主观分
资质	5	根据投标人的企业管理能力、产品质量保证能力等进行评分: 1) 拥有 ISO 27001 信息安全管理体认证证书的, 得 3 分。 2) 拥有 ISO 20000 信息技术服务管理体系认证证书的, 得 2 分。 注: 不提供证明材料不得分。	客观分
业绩	4	2022 年 1 月 1 日以来同类业绩, 提供 2 项及以上者, 得 4 分; 提供 1 项者, 得 2 分; 未提供者不得分。(须提供合同关键页, 否则不得分, 关键页包括项目名称、金额、签字盖章页等。可提供框架合同或单项合同, 仅提供订单视作为未提供证明材料, 数量以合同数量计算) 是否属于有效的类似项目由评标委员会根据投标人提供的项目承接情况在业务内容、技术特点	客观分

		等方面与本项目类似程度进行认定。	
总分	100		

本评分细则满分 100 分，平均分保留小数点后两位。

说明：

- 1、投标人不得以低于成本的报价竞标。如果评标委员会发现投标人的报价明显低于其他投标报价,使得投标报价可能低于其成本的,将要求该投标人作书面说明并提供相关证明材料。投标人不能合理说明或不能提供相关证明材料的,评标委员会将认定该投标人以低于成本报价竞标,其投标作无效投标处理。
- 2、投标人对评分细则中相应部分没有承诺的,评委可按评分细则中最低分进行打分。
- 3、如符合带“★”参数的供应商少于 3 家的,本次招标按“实质性”响应少于 3 家处理,宣告招标采购失败。
- 4、评标委员会推荐一名专家担任评标组长,负责起草评标结论。

第六章：投标文件清单及投标文件有关格式

一、投标文件清单

- 1、 投标文件编制说明、企业介绍；
- 2、 承诺函（后附格式）；
- 3、 开标一览表（后附格式）；
- 4、 报价明细表；
- 5、 法定代表人证明（后附格式）；
- 6、 法定代表人授权书（后附格式）；
- 7、 各类证照扫描件（包括：如营业执照、资质证件、股东组成等）；
- 8、 中小企业声明函（后附格式）；
- 9、 残疾人福利性单位声明函（后附格式）；
- 10、 《财务状况及税收、社会保障资金缴纳情况声明函》（后附格式）；
- 11、 项目方案；
- 12、 偏离表（标注“▲”项单独制成表格）；
- 13、 项目组成人员（后附格式）；
- 14、 同类项目业绩（后附格式）。

注：投标文件应包括但不仅限于以上所列内容。

二、附件：投标文件有关格式

承诺函

致：上海市崇明区教育局：

上海市崇明区政府采购中心：

1. 在考察本项目现实情况并仔细阅读招标文件并充分理解、考虑到可能存在的风险因素后，我们愿意按开标一览表中所报的单价、费率的价格和计算程序进行价款计算并定为合同价款。该总价已包括了业主要求完成的所有采购任务。一旦我公司中标，除非业主要求更改，将最终作为结算价，一次包死，不予调整。（采购量变更的除外）

2. 我们保证在签定合同后、承诺的日历天内（包括星期日、假期及恶劣天气）或按合同而延长的时间内完成上述任务。

3. 我们已注意到招标文件中的各项要求，我们承诺将完全考虑和接收业主提出的所有条件，并已在费用和措施中予以充分考虑。

4. 我们理解贵方不一定接受我方的投标，亦不会要求贵方解释选择或否决任何投标的原因。

5. 我方理解贵方不支付我方在投标中的任何费用。

6. 我方保证所提交的一切资料均真实、合法、有效。

7. 与本项目有关的、由国家、市、县各级各部门发布的各类法律、法规、规定及其他文书，我方将予以遵守，如有违反，愿意承担由此引发的各类法律责任。

投标单位名称：_____（公章）

地 址：_____

法人或被授权人签字：_____

日 期： 年 月 日

开标一览表

项目名称：崇明区教育网学校网络万兆全光网改造项目

项目编号：310151000250411101566-51232647

最高限价：540 万元

人民币元

崇明区教育网学校网络万兆全光网改造项目包 1

项目名称	总价（人民币元）	备注	最终报价(总价、元)

说明：

投标文件有效期：自开标之日起_____日

投标人是否为福利企业：_____

投标单位名称：_____（公章）

法人或被授权人签字：_____

日期： 年 月 日

法定代表人证明书

致：_____

兹证明_____（姓名），性别_____年龄_____身份证号码_____，担任我公司_____（职务），系本公司的法定代表人。

致

礼！

投标单位名称：_____（公章）

日期： 年 月 日

（请附法定代表人的身份证 正面原件扫描件）	（请附法定代表人的身份证 反面原件扫描件）
----------------------------------	----------------------------------

法定代表人授权书

本授权书声明：注册于_____的_____公司的
在下面签字的_____（法定代表人姓名、职务）代表本公司授权
（单位）的在下面签字的_____（被授权人的姓名、职务）为
本公司的合法代理人，全权委托其前往上海市崇明区政府采购中心办理
_____（采购项目名称编号）投标活动，并代表
我方全权办理针对上述项目的投标、开标、投标文件澄清、签约等一切具体事务
和签署相关文件。我方对被授权人的签名事项负全部责任。

在贵中心收到我方撤销授权的书面通知以前，本授权书一直有效。被授权人
在授权书有效期内签署的所有文件不因授权的撤销而失效。除我方书面撤销授权
外，本授权书自投标截止之日起直至我方的投标有效期结束前始终有效。

被授权人无转委托权，特此委托。

授权人签字：_____

授权人身份证号码：_____

代理人（被授权人）签字：_____

代理人（被授权人）身份证号码：_____

单位名称（公章）：_____

日 期： 年 月 日

（请附被授权人的身份证
正面原件扫描件）

（请附被授权人的身份证
反面原件扫描件）

公司股东组成基本情况表

企业名称： 注册资金：
注册地址： 实际经营地址：

序号	股东名称 (姓名)	投资者法人代表	企业代码或身份证号	联系电话	持股比例	备注
1						
2						
3						
4						
5						
6						
7						
8						

说明：企业股东超过 10 个的，仅需填列前 10 大股东即可。

填报人： 联系电话： 填报时间：

公司声明：本公司填写的《股东组成基本情况表》真实、有效，如有虚假，则本公司同意按照虚假报价处理。

年 月 日

中小企业声明函

本公司(联合体)郑重声明,根据《政府采购促进中小企业发展管理办法》(财库〔2020〕46号)的规定,本公司(联合体)参加上海市崇明区教育局的崇明区教育网学校网络万兆全光网改造项目采购活动,服务全部由符合政策要求的中小企业承接。相关企业(含联合体中的中小企业、签订分包意向协议的中小企业)的具体情况如下:

1. 崇明区教育网学校网络万兆全光网改造项目,属于软件和信息技术服务业;承接企业为(企业名称),从业人员 人,营业收入为 万元,资产总额为 万元,属于(中型企业、小型企业、微型企业);

以上企业,不属于大企业的分支机构,不存在控股股东为大企业的情形,也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假,将依法承担相应责任。

企业名称(盖章):

日期:

说明:(1)本声明函所称中小企业,是指在中华人民共和国境内依法设立,依据国务院批准的中小企业划分标准确定的中型企业、小型企业和微型企业,但与大企业的负责人为同一人,或者与大企业存在直接控股、管理关系的除外。符合中小企业划分标准的个体工商户,在政府采购活动中视同中小企业。事业单位、团体组织等非企业性质的政府采购供应商,不属于中小企业划型标准确定的中小企业,不得按《关于印发中小企业划型标准规定的通知》规定声明为中小微企业,也不适用《政府采购促进中小企业发展管理办法》。

(2)本声明函所称服务由中小企业承接,是指提供服务的人员为中小企业依照《中华人民共和国劳动合同法》订立劳动合同的从业人员,否则不享受中小企业扶持政策。

(3)从业人员、营业收入、资产总额填报上一年度数据,无上一年度数据的新成立企业可不填报。

(4)成交供应商为中小企业的,本声明函将随成交结果同时公告。

(5)投标人未按照上述格式正确填写《中小企业声明函》的,视为未提供《中小企业声明函》,不享受中小企业扶持政策。

注:行业划型标准:

(十二)软件和信息技术服务业。从业人员300人以下或营业收入10000万元以下的为中小微型企业。其中,从业人员100人及以上,且营业收入1000万元及以上的为中型企业;从业人员10人及以上,且营业收入50万元及以上的为小型企业;从业人员10人以下或营业收入50万元以下的为微型企业。

残疾人福利性单位声明函

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）的规定，本单位安置残疾人____人，占本单位在职职工人数比例____%，符合残疾人福利性单位条件，且本单位参加____单位的____项目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

单位名称（盖章）：

日 期：

说明：根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》享受政府采购支持政策的残疾人福利性单位应当同时满足以下条件：

- （1）安置的残疾人占本单位在职职工人数的比例不低于 25%（含 25%），并且安置的残疾人人数不少于 10 人（含 10 人）；
- （2）依法与安置的每位残疾人签订了一年以上（含一年）的劳动合同或服务协议；
- （3）为安置的每位残疾人按月足额缴纳了基本养老保险、基本医疗保险、失业保险、工伤保险和生育保险等社会保险费；
- （4）通过银行等金融机构向安置的每位残疾人，按月支付了不低于单位所在区县适用的经省级人民政府批准的月最低工资标准的工资；
- （5）提供本单位制造的货物、承担的工程或者服务（以下简称产品），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

中标人为残疾人福利性单位的，本声明函将随中标结果同时公告。

如投标人不符合残疾人福利性单位条件，无需填写本声明。

财务状况及税收、社会保障资金 缴纳情况声明函

我方（供应商名称）符合《中华人民共和国政府采购法》第二十二条第一款第（二）项、第（四）项规定条件，具体包括：

1. 具有健全的财务会计制度；
2. 有依法缴纳税收和社会保障资金的良好记录。

特此声明。

我方对上述声明的真实性负责。如有虚假，将依法承担相应责任。

供应商名称（公章）

日期：

项目组成人员

岗位	姓名	职称	主要经历、经验及担任过项目

同类项目业绩

序号	用户名称	项目名称	日期	采购金额	联系电话	备注

注意：须提供 2022 年 1 月 1 日以来合同关键页，否则不得分，关键页包括项目名称、金额、签字盖章页等，否则将不予认可

投标单位名称：_____（公章）

法人或被授权人签字：_____

日 期： 年 月 日