中国青年报社中青大厦办公区
网络建设二期项目

招 标 文 件

采购编号：HXJC2019HG/090

招　　标　　人：北京中青在线网络信息技术有限公司

招标代理机构：北京华夏京诚咨询有限公司

日　　　　期：2019 年 9 月 19 日

目　录

第一部分 投标邀请

北京华夏京诚咨询有限公司（以下简称“招标代理机构”）受**北京中青在线网络信息技术有限公司**（以下简称“招标人”）的委托，就**中国青年报社中青大厦办公区网络建设二期项目**组织国内公开招标，欢迎合格的投标人前来进行密封投标。

1.1 招标项目情况

1.1.1 项目名称：中国青年报社中青大厦办公区网络建设二期项目

1.1.2 采购编号：HXJC2019HG/090

1.1.3 项目预算：300 万元

最高投标限价：300 万元

项目资金来源：自筹资金

1.1.4 招标内容：

本次招标采购拟择优选择一家合格的供应商，根据招标人的技术需求，为招标人提供以下网络建设基础设备和服务：

（1）补充健全中国青年报社中青大厦办公区互联网出口安全防护设备，实现双路互联网接入线路稳定运行，保证出口网关安全稳定运行。

（2）购买中国青年报社中青大厦办公区网络二期建设所需交换机设备，实现办公区网络的冗余备份和办公区网络全覆盖。

（3）采购中国青年报社中青大厦办公区网络运维和安全管理系统，实现一期建设和本期建设的网络设施、网络安全可视化和自动化的统一管理。

（4）采购中国青年报社中青大厦办公区运维系统和安全管理系统所需硬件设备。

（5）采购中国青年报社中青大厦办公区两期网络集成运维服务。

具体内容及要求详见招标文件第三部分“采购内容及要求”。

1.2 投标人资格

1.2.1 具备《政府采购法》第 22 条规定的必须具备的如下条件：具有良好的商

业信誉和健全的财务会计制度；具有履行合同所必需的设备和专业技术能力；有依法缴纳税收和社会保障资金的良好记录；参加政府采购活动前三年内，在经营活动中没有重大违法记录，且在当地工商局企业信用查询中无重大违法记录。

1.2.2 截至投标文件递交截止时间前，供应商不能是被列入“信用中国”网站(www.creditchina.gov.cn)失信被执行人、重大税收违法案件当事人名单、以及“中国政府采购网”网站（www.ccgp.gov.cn）政府采购严重违法失信行为记录名单中被禁止参加1-3年政府采购活动的供应商（处罚期限尚未届满的）。

1.2.3 法定代表人为同一人或者存在直接控股、管理关系的不同供应商，不得共同参加本招标项目的投标。为本招标项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加本项目的投标。违反上述规定的相关投标均无效。

1.2.4 本项目不接受联合体投标，不允许将部分项目分包和转包。

1.3 招标文件发售

1.3.1 投标人必须向招标机构购买招标文件并登记备案，未向招标机构购买招标文件并登记备案的潜在投标人均无资格参加投标。

1.3.2 集中发售时间：自2019年9月20日至2019年9月26日，每天（法定节假日除外）上午9:00-11:30，下午13:30-16:00。

1.3.3 集中发售地点：北京市海淀区西直门北大街甲43号金运大厦B座802室（西直门文慧桥西南角）。

1.3.4 招标文件售价：人民币800元，招标文件售后不退。

1.3.5 投标人在购买招标文件时须向招标代理机构提供：

（1）营业执照（副本）复印件或法人证书复印件（加盖投标人公章）；

（2）法定代表人授权委托书原件（附授权代表身份证件复印件并加盖投标人公章）或法定代表人资格证明书原件（附法定代表人身份证件复印件）。

1.4 公告期限

公告期限为5个工作日。

1.5 开标

1.5.1 投标文件递交、截止的时间和地点

1.5.1.1 递交时间：2019 年 10 月 11 日下午 13:00-13:30。

1.5.1.2 截止时间：2019 年 10 月 11 日下午 13:30，超过截止时间递交投标文件将不予受理。

1.5.1.3 递交地点：北京市海淀区西直门北大街甲 43 号金运大厦 B 座 802 室（第二会议室）。

1.5.2 开标时间和地点

1.5.2.1 开标时间：2019 年 10 月 11 日下午 13:30，届时请各投标人派代表出席开标会议。

1.5.2.2 开标地点：北京市海淀区西直门北大街甲 43 号金运大厦 B 座 802 室（第二会议室）。

1.6 招标人相关情况

招标人名称：北京中青在线网络信息技术有限公司

招标人地址：北京市东城区海运仓 2 号

招标人联系方式：李伟 010-64098468

1.7 招标代理机构相关情况

开户名称：北京华夏京诚咨询有限公司

开户银行：中国民生银行北京西直门支行

银行账户：698882343

邮政编码：100044

联 系 人：李女士、王先生

电 话：（010）82582703-818/819

传　　真：010-82582703-876

电子邮箱：hxjczb@163.com

第二部分 投标人须知

投标人须认真阅读下列须知，并予以认真遵守。投标人不按招标文件要求提供投标文件和相关资料的，可能导致投标被拒绝。

2.1 投标人

2.1.1 合格投标人的条件

具备第一部分 1.2 规定资格的法人为合格投标人。

2.1.2 投标人委托

2.1.2.1 投标人代表为法定代表人的，投标时应出示其身份证原件和《法定代表人资格证明书》（式样见第五部分 5.2.8）；非法定代表人的，除出示其身份证原件外，还须持有《法定代表人资格证明书》和《法定代表人授权委托书》（式样见第五部分 5.2.9）。

2.1.2.2 投标人代表未按照 2.1.2.1 条款要求参加开标会议的，招标代理机构有权拒绝其投标。

2.1.3 投标费用

投标人自行承担参加投标有关的全部费用。

2.2 招标文件

2.2.1 招标文件

招标文件包括投标邀请、投标人须知、采购内容及要求、合同格式及主要条款、投标文件内容及式样等内容。

2.2.2 招标文件的澄清

2.2.2.1 投标人对招标文件如有疑点要求澄清，或认为有必要与招标人进行沟通时，应于开标日期 5 日之前以书面形式告知招标代理机构。如果招标人和招标代理机构认为需要答复的，在答复相关投标人的同时，分发给取得同一招标文件的所有投标人。

2.2.2.2 投标人已经参与投标，并于开标后对招标文件提出质疑的，其质疑为无效质疑。

2.2.3 招标文件的修改

2.2.3.1 在投标截止时间 15 日前，招标人可以采用补充通知的方式对招标文件进行必要的修改和补充。

2.2.3.2 对招标文件的修改，将以书面形式通知已购买招标文件的所有投标人。补充文件将作为招标文件的组成部分，对招标人和所有投标人均有约束力。

2.2.3.3 为使投标人有足够时间按招标文件的修改要求修正投标文件，招标人可酌情推迟投标的截止日期和开标日期，并将此变更通知所有投标人。

2.3 投标文件

2.3.1 投标文件的语言及计量单位

2.3.1.1 投标人提交的投标文件及投标人与招标人或招标代理机构之间所有来往函电文件均应采用中文简体。

2.3.1.2 投标人所提供的文件和资料，应采用中华人民共和国法定计量单位。

2.3.2 投标文件的组成

投标文件由投标函、资格证明文件及技术响应文件组成，具体内容按照第五部分投标文件内容及式样编制。

2.3.2.1 资格审查证明文件

（1）*营业执照副本复印件或法人证书复印件并加盖投标人公章；

（2）*税务登记证书复印件并加盖投标人公章（依据国家有关规定取消税务登记证书的投标人可不提供）；

（3）*投标截止日前 6 个月内任意一期缴纳增值税或企业所得税的凭据复印件并加盖投标人公章；

（4）*投标截止日前 6 个月内任意一期缴纳社会保险的凭据复印件并加盖投标人公章；

（5）*近三年度(2016 年、2017 年、2018 年)会计师事务所出具的年度财务审计

报告复印件并加盖投标人公章，或近三年度(2016 年、2017 年、2018 年)资产负债表和损益表（利润表）复印件并加盖投标人公章；若投标人为本年度新成立企业，仅需提供最近一期资产负债表和损益表；

（6）*投标截止日前三年内无重大违法行为的声明书；

2.3.2.2 符合性审查证明文件

（1）*投标函；

（2）*开标一览表；

（3）*投标报价明细表；

（4）*商务条款偏离表；

（5）*技术条款偏离表；

（6）*支付代理服务费承诺函；

（7）*法定代表人资格证明书；

（8）*法定代表人授权委托书（如果法定代表人不能参加投标的，应提供法定代表人授权委托书和法定代表人资格证明书）；

（9） 投标人基本情况表；

（10）近三年同类业绩情况表及证明材料；

（11）其他需要说明的事宜。

注：以上带“*”号标记的文件，除特殊说明外均为必须提供的材料，没有提供或没有按要求提供相关证明文件的，将视为未实质性响应招标文件要求。

2.3.2.3 技术响应文件包括但不限于如下内容：

（1）技术指标响应；

（2）技术实施方案；

（3）培训方案；

（4）质量保证和技术支持服务；

（5）需要补充的其他内容。

2.3.3 投标文件填写说明

2.3.3.1 投标人应详细阅读招标文件的全部内容。投标文件须对招标文件中的内

容做出实质性和完整的响应，如果投标文件填报的内容资料不详、不全，将导致投标被拒绝。

2.3.3.2 投标文件应严格按照招标文件的要求提交，并按规定的统一格式逐项填写，不准有空项；无相应内容可填的项应填写“无”、“没有相应指标”等明确的回答文字。投标文件未按规定提交或留有空项，将被视为不完全响应，其投标有可能被拒绝。

2.3.3.3 开标一览表为开标会议上唱标的内容，应按要求格式填写，不得自行增减内容。开标一览表应单独包装密封，随投标文件一并递交。

2.3.3.4 投标人须保证投标全部文件资料真实可靠，并接受评标委员会对任何文件资料进一步审查的要求。

2.3.4 投标文件报价说明

2.3.4.1 所有投标均以人民币“元”为计算单位报价。

2.3.4.2 **投标报价应包含完成中国青年报社中青大厦办公区网络建设二期项目网络基础设备采购、运输、安装、培训、维保等招标人委托任务的全部费用。招标人将不再支付其他任何费用。**

2.3.4.3 投标人按开标一览表及其他事项要求填写报价及有关内容。

2.3.4.4 投标人所报的各分项单价在合同履行过程中不可调整，不得以任何理由变更。任何包含价格调整要求的投标，将被视为非实质性响应予以拒绝。

2.3.4.5 招标人不接受任何选择性报价，投标文件中只能有一个投标报价，否则作为无效投标处理。

2.3.4.6 **评标委员会有权判定投标人明显低于成本的报价是无效报价。**

2.3.4.7 最低投标报价不作为中标的唯一保证。

2.3.4.8 **招标人对超出最高投标限价的投标报价将不予接受，该投标文件将被视为非实质性响应予以拒绝。**

2.3.5 投标保证金

本项目无须提交投标保证金。

2.3.6 投标文件的有效期

2.3.6.1 投标文件自开标日起90日内有效，有效期短于90日的投标文件将被拒绝。

2.3.6.2 特殊情况下，招标人可与投标人协商延长投标文件的有效期。如需延长投标文件有效期，将以书面形式进行。同时，按本须知规定的投标保证金的有效期也相应延长。

2.3.6.3 投标人可以拒绝接受延期要求而不影响保证金的退还。同意延长有效期的投标人除按招标人要求修改投标文件有效期外，不能修改投标文件的其它内容。

2.3.7 投标文件的签署及规定

组成投标文件的各项资料必须遵守以下条款：

2.3.7.1 投标人应填写全称，投标文件和单独封装递交的开标一览表都必须由法定代表人或授权代表签署，并加盖投标人公章。

2.3.7.2 **投标文件的正本必须用A4纸打印，须用不褪色的蓝、黑墨水签字，字迹清晰，易于辨认，并在封面右上角上注明“正本”字样。副本可以用正本的复印件，封面右上角注明“副本”字样。**

2.3.7.3 投标文件不得随意涂改和增删。如有修改，须由同一签署人在修改处签字并加盖投标人公章。

2.3.7.4 投标文件因字迹潦草或表达不清所引起的后果由投标人负责。

2.3.8 投标文件的装订要求

2.3.8.1 **投标文件应严格按照招标文件第五部分规定顺序和格式，统一编目编码、双面打印胶装成册，由于编排混乱导致投标文件被误读或查找不到，其责任由投标人承担。若投标人未按招标文件要求装订，评标委员会有权拒绝其投标文件。**

2.3.8.2 **投标文件一式5份，其中正本1份，副本4份，电子版1份（根据招标文件要求编制的投标文件电子版本，以U盘形式提交）。如果正本与副本内容不一致，以正本为准。**

2.4 投标文件的递交

2.4.1 投标文件的密封及标记

2.4.1.1 投标人应将投标文件密封包装，封口处应盖有投标人公章及法定代表人或授权代表的签字（封面式样见第五部分 5.4.1）。

2.4.1.2 为方便开标唱标，投标人应单独准备开标一览表原件 1 份密封包装，封口处应盖有投标人公章及法定代表人或授权代表的签字（封面式样见第五部分 5.4.2）。

2.4.1.3 投标文件应由专人送交，投标人应将投标文件按第二部分 2.4.1.1 和 2.4.1.2 中的规定进行密封和标记，按规定的时间、地点送达。

2.4.1.4 若投标人未按上述要求密封及加写标记，导致投标文件被误投或提前启封，其责任由投标人承担。

2.4.2 投标文件递交

2.4.2.1 投标人必须在招标文件规定的投标截止时间前派人到指定的地点，将投标文件送交至招标代理机构检查签收，在投标截止时间之后送达的投标文件将被拒收。

2.4.2.2 招标人如需调整投标截止时间，招标代理机构应以书面形式通知所有投标人。招标人和投标人的所有权利和义务均根据调整后的投标截止时间顺延。

2.4.2.3 投标人代表须按照招标文件 2.1.2 条款要求出示其身份证件原件和单独提供《法定代表人资格证明书》、《法定代表人授权委托书》，若未提供或核验不符，招标代理机构有权拒绝其投标。

2.4.3 投标文件的修改和撤回

2.4.3.1 投标人递交投标文件后，如果对投标文件提出修改、补充或撤回要求，应以书面形式在投标截止时间前送达招标代理机构。投标人提出的书面修改、补充或撤回投标文件要求须经招标代理机构签字确认接受，否则无效。

2.4.3.2 投标人对修改、补充的页面按照招标文件的要求签署、盖章，作为投标文件的组成部分密封后送达招标代理机构，同时应在封面上标明“投标后修改（并注明采购编号）”和“开标时启封”字样。

2.4.3.3 撤回投标文件必须递交有投标人法定代表人或授权代表签署的要求撤

回投标文件的书面请求，撤回投标文件的时间以书面请求送达至招标代理机构为准。

2.4.3.4 开标后，投标人不得撤回投标文件，否则投标保证金将不予退还。

2.5 开标

2.5.1 招标代理机构按招标文件规定的时间、地点组织开标会议，参加会议人员包括招标人代表、投标人代表、监标人和有关工作人员。监标人对开标全过程进行现场监督。

2.5.2 开标前由投标人代表和监标人检查投标文件的密封情况，未按招标文件要求密封的，将视为无效投标文件；密封合格的，由投标人代表和监标人确认并签字。

2.5.3 开标一览表由工作人员在会上现场拆封，并当场宣读开标一览表中所有信息。

2.5.4 招标代理机构填写开标记录，如投标人发现开标记录与投标文件不符时，应现场提出修改。开标记录应由投标人代表和监标人确认并签字。

2.5.5 投标人未参加开标的，视同认可开标结果。

2.5.6 开标结束后，招标人或者招标代理机构根据招标文件规定的资格条件，依法对投标人的资格进行审查，并如实记录审查结果。

2.5.7 资格审查主要按照招标文件**“2.3.2.1 资格审查证明文件”**相关要求进行审查。

2.5.8 通过资格审查的合格投标人不足 3 家的，不得评标。

2.6 评标

2.6.1 评标委员会

2.6.1.1 招标代理机构根据有关规定及项目特点组建评标委员会。评标委员会成员由招标人推荐专家，以及在财政部门的评标专家库中的专家组成，共计 5 人（含）以上单数，其中评标专家库中专家数量不少于成员总数的 2/3。

2.6.1.2 评标委员会负责具体评标事务，并独立履行下列职责：

（1）审查、评价投标文件是否符合招标文件的商务、技术等实质性要求；

（2）要求投标人对投标文件有关事项作出澄清或者说明；

（3）对投标文件进行比较和评价；

（4）确定中标候选人名单，以及根据招标人委托直接确定中标人；

（5）向招标人、招标代理机构或者有关部门报告评标中发现的违法行为。

2.6.1.3 招标代理机构应当采取必要措施，保证评标在严格保密的情况下进行。除招标人代表、评标现场组织人员外，招标人的其他工作人员以及与评标工作无关的人员不得进入评标现场。

2.6.1.4 有关人员对评标情况以及在评标过程中获悉的国家秘密、商业秘密负有保密责任。

2.6.2 评标原则

（1）坚持公平、公正、科学、规范的原则

（2）坚持反不正当竞争的原则

（3）坚持回避原则

与招投标单位或者其主要负责人有亲属关系、经济利益关系的人员；曾任项目主管部门或行政监督部门人员；或在招标、评标以及其他有关活动中有违法行为而受过行政处罚或刑事处罚的人员。以上人员均应予以回避。

（4）坚持保密原则

对评标过程和结果以及投标人的商业秘密有保密义务，开标之后，直至授予投标人合同为止，不得向投标人或其他与评标无关的人员透露。在评标期间，投标人企图影响招标人和评标委员会的任何活动，将导致投标被拒绝，并由其承担相应的法律责任。

2.6.3 评标方法

本项目采用综合评分法评标，即评标委员会按照招标文件规定的评分指标和标准进行综合评审。以评标总得分最高的投标人作为预中标人的评标方法。评分指标具体如下：

评分指标

序号	评分指标		评分标准	分值
	一级指标	二级指标		
1	商务部分（5 分）	同类业绩（5 分）	近三年投标人独立完成的同类项目，每提供 1 份有效的业绩资料得 1 分，满分 5 分。 有效的业绩资料要求详见招标文件“第五部分 投标文件内容及式样”中“5.2.10 近三年同类项目业绩情况表及证明材料”规定。	0-5 分
2	价格部分（30分）	满足招标文件要求且投标价格最低的投标报价为评标基准价，及报价得分为满分。投标报价得分=（评标基准价/投标报价）×30×100% 评标基准价=所有投标人中有效报价的最低价		0-30 分
3	技术部分（65 分）	技术指标响应程度（40分）	针对所投产品满足本招标文件“**3.2.2 设备系统及服务指标要求**”情况打分，完全符合招标文件要求的为满分 40 分。普通产品技术参数每有一项负偏离扣除 0.5 分，标有“★”号条款每有一项负偏离（未提供截图文件、测试报告、认证证书等证明文件的，按负偏离对待）扣除 1 分，最低为 0 分。	0-40分
		技术实施方案（15分）	提供的实施方案全面合理，技术方案针对性强，对项目总体架构、安全部署、网络等设计全面、科学合理且充分考虑甲方现有环境的设备配置，能跟现有设备进行安全联动和统一管理。 （优秀：9～15 分；良好：5～8 分；一般：0～4 分）	0-15分
		培训方案（5分）	内容全面、计划得当，措施有力，服务质量方面能够得到有效的保证。 （优秀：5分；良好：3～4分；一般：0～2分）	0-5分
		质量保证和技术支持服务（5分）	质量保证和技术支持服务详细、合理，满足项目需求。 （优秀：5分；良好：3～4分；一般：0～2分）	0-5分

注：业绩需附证明材料并加盖公章，复印件清晰可辨，否则不计分。

2.6.4 投标文件评审

2.6.4.1 开标后，评标委员会先对投标文件进行符合性审查。审查的主要内容为

投标文件中的资格证明文件、投标保证金等，并从投标文件的有效性、完整性和对招标文件的响应程度进行审查，以确定投标人是否具备投标资格并对招标文件做出实质性响应。

2.6.4.2 符合性审查有下列情况之一的，按照无效投标处理：

（1）未按招标文件要求提供带“*”号材料的；

（2）投标文件未按照招标文件的规定密封、签署、盖章的；

（3）不具备招标文件中对投标人的资格要求的；

（4）未按招标文件规定报价，以及经评标委员会判定投标人的报价为无效报价的；

（5）投标有效期不足 90 个日历日的；

（6）投标报价超过招标文件中规定的预算金额或者最高投标限价的；

（7）投标文件含有招标人不能接受的附加条件的；

（8）提供虚假文件的，或故意隐瞒不良业绩的；

（9）投标文件存在其他不符合招标文件的商务、技术等实质性要求；

（10）不符合法律、法规和招标文件中规定的其他实质性要求的。

2.6.4.3 评标委员会严格按照招标文件规定的评标标准和评标方法对通过符合性审查的投标文件作进一步评审。

2.6.4.4 评审过程中，投标文件报价出现前后不一致的，除招标文件另有规定外，按照下列规定修正：

（1）投标文件中开标一览表（报价表）内容与投标文件中相应内容不一致的，以开标一览表（报价表）为准；

（2）大写金额和小写金额不一致的，以大写金额为准；**单独封装的开标一览表与投标文件(正本)中的开标一览表不一致的，按投标无效处理。**

（3）单价金额小数点或者百分比有明显错位的，以开标一览表的总价为准，并修改单价；

（4）总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

（5）同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价经

投标人确认后产生约束力，确认需加盖投标人公章或由其法定代表人或其授权代表签字，投标人不确认的，其投标无效。

（6）上述原则对投标人具有约束力，投标人不同意的，其投标将被拒绝。

2.6.4.5 相同品牌投标人认定：

（1）多家投标人提供的核心产品品牌相同的，将被视为同品牌产品投标。

（2）提供相同品牌产品且通过符合性审查的不同投标人按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格。

2.6.5 投标文件的澄清

2.6.5.1 评标委员会有权以书面形式要求投标人对投标文件中含义不明确、对同类事项表述不一致、有明显文字或计算错误等问题作必要的澄清、说明或者补正。投标人必须按照要求的内容和时间，以书面形式予以澄清、说明或者补正，并由法定代表人或授权代表签字。投标人拒不按照要求进行澄清、说明或补正的，评标委员会可拒绝该投标。

2.6.5.2 **评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。**

2.6.5.3 投标人的投标澄清文件作为投标文件的一部分，不得超出投标文件的范围或改变投标文件的实质性内容，不得改变投标价格。

2.6.6 废标处理

出现下列情形之一的按废标处理，招标人将废标理由以书面形式通知所有投标人。

（1）符合条件的投标人或对招标文件做出实质性响应的投标人不足三家的；

（2）出现影响采购公正的违法、违规行为的；

（3）投标人的报价均超过了招标预算，招标人不能支付的；

（4）因重大变故，采购任务取消的。

2.7 确定中标

2.7.1 推荐中标候选人

2.7.1.1 评标委员会对投标文件进行综合评审后，根据总得分情况，由高到低排序，向招标人推荐合格的中标候选人，并提交书面评标报告。

2.7.1.2 如果中标候选人总得分相同时，按投标报价由低到高排序；总得分相同且投标报价也相同时，按技术部分得分由高到低排序。

2.7.2 确定中标人

2.7.2.1 招标代理机构应当在评标结束后 2 个工作日内将评标报告送交招标人。招标人应当在收到评标报告后 5 个工作日内，按照评标报告中推荐的中标候选人顺序确定中标人。

2.7.2.2 招标人将按排序先后确定中标人，如中标人放弃中标或因不可抗力的原因而不能履行合同，或者有其它不符合中标条件的，招标人仍按中标候选人的排序先后依次确定中标人。

2.7.2.3 中标人应在中标之后提供本招标文件要求提供的有关资料原件以备查。

2.7.3 中标通知

2.7.3.1 中标人确定后 2 个工作日之内，由招标代理机构在指定的信息发布媒体上公告中标结果。

2.7.3.2 招标代理机构以书面形式向中标人发出中标通知书。中标通知书是合同的一个组成部分，对招标人和中标人具有同等法律效力。

2.7.4 签订合同

2.7.4.1 中标通知书发出后，招标人不得违法改变中标结果，中标人无正当理由不得放弃中标。

2.7.4.2 招标人应当自中标通知书发出之日起 30 日内，按照招标文件和中标人投标文件的规定，与中标人签订书面合同。所签订的合同不得对招标文件确定的事项和中标人投标文件作实质性修改。

2.7.4.3 招标人不得向中标人提出任何不合理的要求作为签订合同的条件。

2.7.4.4 中标人应按中标通知书要求与招标人签订合同，否则按开标后撤回投标

处理。

2.7.4.5 招标文件及其补充文件、投标文件及评标过程中有关澄清文件等均为合同的附件。

2.7.5 质疑

2.7.5.1 投标人对中标公告有异议的，应当在公布之日起 7 个工作日内，以书面形式（原件）向招标代理机构提出质疑。提出质疑时需向招标代理机构提交如下材料纸质版原件：

（1）质疑函原件并加盖投标人公章；质疑函应当包括下列内容：

- 投标人名称、地址、邮编、联系人及联系电话；
- 质疑项目的名称、编号；
- 具体、明确的质疑事项和与质疑事项相关的请求；
- 事实依据；
- 必要的法律依据；
- 提出质疑的日期。

质疑函应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

（2）法定代表人授权委托书原件并加盖投标人公章。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，并由法定代表人、主要负责人签字或者盖章，并加盖公章。

（3）以上材料由授权代表送至招标代理机构处，联系信息如下：

地址：北京市海淀区西直门北大街甲 43 号金运大厦 B 座 802 室

联 系 人：李女士、王先生

电　　话：010-82582703-818/819

2.7.5.2 投标人在法定质疑期内需一次性提出针对同一采购程序环节的质疑。对同一采购程序环节提出的后续多次质疑将不被接受。

2.8 代理服务费

2.8.1 招标代理机构依据招标代理协议，向中标人收取代理服务费

代理服务费以中标金额为依据，按差额定率累进法计算，收费标准如下：

服务类型 / 费率 / 中标金额（万元）	货物招标	服务招标	工程招标
100 以下	1.5%	1.5%	1.0%
100-500	1.1%	0.8%	0.7%
500-1000	0.8%	0.45%	0.55%
1000-5000	0.5%	0.25%	0.35%
5000-10000	0.25%	0.1%	0.2%
10000-100000	0.05%	0.05%	0.05%
1000000 以上	0.01%	0.01%	0.01%

2.8.2 中标人应以转帐支票（北京地区）、银行汇款（京外地区）形式支付代理服务费，汇款时需注明**中国青年报社中青大厦办公区网络建设二期项目（项目编号：190335），备注“代理服务费”**。

2.9 保密和披露

2.9.1 投标人自领取招标文件之日起，须承诺承担本招标项目保密义务。

2.9.2 招标人有权将投标人提供的资料向有关人员披露。

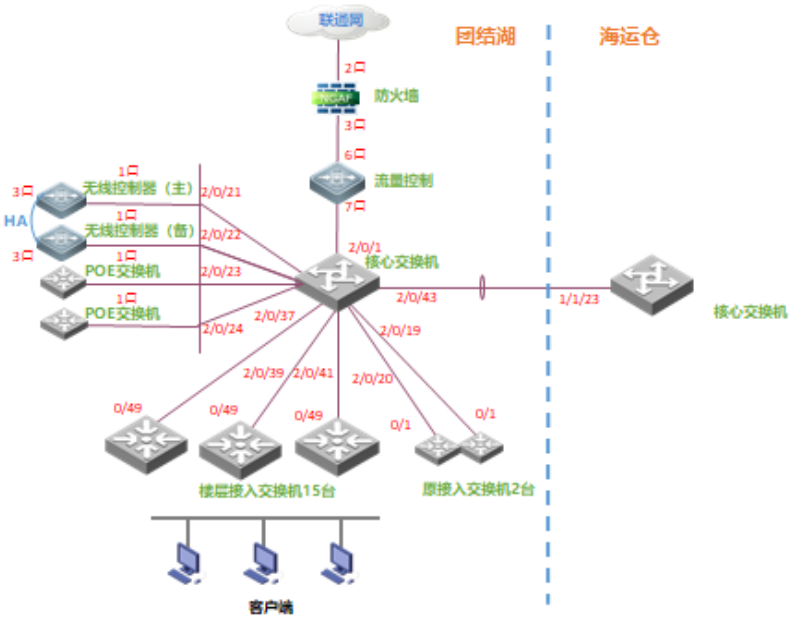
2.9.3 招标人有权在法律规定的情况下，向要求披露信息的第三方和有关人员，提供项目的相关资料。

第三部分　项目内容及要求

3.1 项目概述

3.1.1 项目背景

按照共青团中央对新闻宣传大格局改革的部署，中国青年报社与原中青实业公司、共青团中央网络影视中心、中国青年网进行了机构合并与重组。合并重组后的中国青年报社在位于朝阳区东三环北路 19 号的中青大厦开辟了新的办公区，为满足办公区员工日常办公需要，中国青年报社将对办公区进行网络基础设施建设。



图一：中青大厦办公区临时网络结构图

按照中国青年报社中青大厦办公区投入使用时间安排，因投入使用前期准备时间紧张，招标人已对中青大厦办公区网络进行了一期建设，以满足最基本的办公需求(一期网络的结构图见图一)。目前已经采购并投入使用的设备有万兆核心交换机一台、千兆接入交换机 15 台、千兆光口接入交换机 1 台、千兆防火墙一台，此外，招标人还采购了整套无线解决方案搭建了中青大厦办公区的无线网络。

本次招标主要是完成网络完整性建设，首先是满足网络核心设备冗余备份；其次完成网络出口网关建设，完成负责均衡设备、防火墙设备、流量控制设备的采购和建设，并实现网关设备冗余备份功能；最后要完成网络管理功能的建设，要实现网络准

入、网络设备可视化管理、网络风险探测等功能。

3.1.2 项目概述

本次招标的招标主体单位是中国青年报社下属北京中青在线网络信息技术有限公司，具体网络建设由中国青年报社技术处负责。

为满足中国青年报社中青大厦办公区日常办公需要，在一期网络建设的基础上，按照中青大厦办公区网络需求进行二期建设项目的网络基础设备采购和建设。

本次网络建设一方面需要考虑中青大厦办公区的网络基础设施建设、网络安全建设、业务承载基础架构建设、与一期使用设备的兼容要求，另一方面还要考虑与中国青年报社海运仓办公区的业务安全互通，最终网络建成后需要能保障两个办公区各种业务安全稳定高效的运转。

中青大厦办公区网络设计的过程中需参考等级保护中要求的相关标准、贴合《中华人民共和国网络安全法》第 3-5 章节的相关内容、网络信息安全相关建设标准，为本次建设提供完善的网络安全建设解决方案。

3.2 项目具体要求

3.2.1 设备及服务采购清单

序号	货物名称	货物数量	货物说明	核心产品（是/否）
1	运维管理系统	1 套	具体配置见技术指标要求	否
2	负载均衡	2 台	具体配置见技术指标要求	否
3	安全网关	1 台	具体配置见技术指标要求	否
4	互联网日志审计系统	2 台	具体配置见技术指标要求	否
5	IDC 安全网关	1 台	具体配置见技术指标要求	否
6	专线安全网关	1 台	具体配置见技术指标要求	否
7	安全设备统一管理平台	1 台	具体配置见技术指标要求	否
8	安全分析系统	1 台	具体配置见技术指标要求	否
9	网络威胁探针	1 台	具体配置见技术指标要求	否
10	业务威胁探针	1 台	具体配置见技术指标要求	否
11	核心交换机	1 台	具体配置见技术指标要求	否
12	接入交换机 A	1 台	具体配置见技术指标要求	否
13	接入交换机 B	6 台	具体配置见技术指标要求	否
14	接入交换机 C	1 台	具体配置见技术指标要求	否
15	网络管理系统	1 套	具体配置见技术指标要求	否
16	服务器	4 台	具体配置见技术指标要求	否
17	网络融合集成运维服务	3 年	安全系统协调及售后支持服务	否

3.2.2 设备及服务技术指标要求

注：指标重要性分为“★”指标和一般无标示指标。★代表关键指标，无标识则表示一般指标项。

（1）运维管理系统

技术指标	指标要求
数量	1 套（150 节点）。
★定制开发需求	可根据甲方的实际需求进行部分功能的定制开发。
虚拟化部署	采用虚拟机镜像方式交付，不需要单独提供设备。
	支持私有云、公有云部署。
云平台支持	支持 Hypervisor 安全加固。
管理界面	支持 SSL 加密 WEB 方式、SSH 命令行方式管理设备。
	支持 MAC OS 系统 Safari 浏览器运维管理。
告警管理	告警方式支持邮件告警、页面告警。
云平台统一管理	基于唯一身份标识的全局云平台帐号，统一维护云平台管理，实现与各云平台的无缝连接。
密码托管	根据设定的周期，对设备资源账户实现定期自动修改，以提高设备账户口令的安全性。
账户导入导出	支持授权后设备账户导入、账户导出功能，方便批量处理，并且实现相应工具下实名制的查看。
组织结构	支持树型结构的多层次的用户分组管理；可建立和运维用户行政组织结构相同的网络组织结构。
云平台无缝管理	支持 Vmware ESX、Vmware Vcenter、Openstack、Xen Cloud、适配自主开发的云平台，可实现统一登录与无缝管理。
	支持虚拟机实例安全管理。
手机运维	支持 android、ios 系统 app 运维与管理。
告警规则	提供用户可灵活配置的告警规则。
	告警规则支持告警级别、告警分类和与设备资源绑定。
	告警动作支持会话阻断、邮件告警等。
数据中心	数据中心支持基于 ES 技术的大数据分析（全文模糊查询、正则表达式查询等）。
★服务要求	三年原厂服务并提供原厂服务承诺函。

（2）负载均衡

技术指标	指标要求
数量	2 台。
产品形态	需采用独立的专用硬件 AD 应用交付设备，而非通过添加功能模块的方式实现。
网络接口	千兆电口≥6 个；千兆光口≥2 个。
内存	系统内存≥4GB。
硬盘	提供 SSD 固态硬盘，硬盘容量≥240GB。
整机性能	吞吐量≥5Gbps； 并发连接数≥300 万； 四层新建连接数 CPS≥18 万； 七层新建连接数 RPS≥9 万。
★设备部署	设备需要和互联网出口其他设备进行联动切换，以保障单点故障后可以快速，ICMP 丢包数量≤5 个。
多合一功能集成	提供针对多条出口线路的链路负载均衡功能，实现 inbound 和 outbound 流量的均衡调度，以及链路之间的冗余互备。
★工作模式	可以设置 NAT 工作模式及 DR 工作模式，提供具备 CNAS 和 CMA 资质的第三方测评机构出具的测试报告，加盖原厂公章。
★上线保护	可以设置节点的最大请求速率增长幅度,包括:保持连接阈值、每秒新建链接阈值和每秒 HTTP 请求阈值，提供具备 CNAS 和 CMA 资质的第三方测评机构出具的测试报告，加盖原厂公章。
★会话保持机制	支持源 IP、Cookie（insert/passive）、HTTP-Header、SSL Session ID、URL 等多种会话保持机制，提供具备 CNAS 和 CMA 资质的第三方测评机构出具的测试报告，加盖原厂公章。
★ Smart_Rules 脚本语言	可以支持基于 LUA 的高级脚本语言实现客户端请求/服务端响应双向控制，提供具备 CNAS 和 CMA 资质的第三方测评机构出具的测试报告，加盖原厂公章。
★智能 DNS	可以支持智能 DNS 解析策略,包括:轮询、加权轮询、静态就近性、顺序优先、返回所有 IP、动态就近性、加权最小链接、加权最小流量、源/目地址哈希，提供具备 CNAS 和 CMA 资质的第三方测评机构出具的测试报告，加盖原厂公章。
★SSL 加速	可以支持软件的 SSL 卸载,支持客户端、服务器端双向数字证书认证,支持证书吊销列表联查,支持国密标准的证书，提供具备 CNAS 和 CMA 资质的第三方测评机构出具的测试报告，加盖原厂公章。
IPv6 功能	支持在不增加新域名 NS 记录和 A 记录的条件下解决 IPv6 改造过程中出现的天窗问题，保证客户端不做任何改动，实现平滑解决。
	IPv6 改造方案支持多种模式和部署方案，网络部署清晰可见，不允许通过引流或劫持等不可见的黑盒方式进行改造。
	IPv6 改造方案能够解决天窗问题，支持一条策略匹配多个外链网站，同时外链和网站子链发生修改时支持自动识别并做主动修改，不允许通过人工解析配

	置的方式解决天窗问题。
★服务器繁忙控制	支持配置的服务器上线保护期，包括恢复时间和温暖时间，提供具备 CNAS 和 CMA 资质的第三方测评机构出具的测试报告，加盖原厂公章。
服务器健康检查	支持常见的主动式健康检查功能，提供基于 SNMP、ICMP、TCP/UDP、FTP、HTTP、DNS、RADIUS，ORACLE/MSSQL/MYSQL 数据库等多种类型的探测判断机制。
★节点监视器	可以支持 TCP 主动探测和 TCP 被动探测方式监测服务器节点健康状态，提供具备 CNAS 和 CMA 资质的第三方测评机构出具的测试报告，加盖原厂公章。
★全球地址库	可以支持全球地址库在线更新，可以配置全球地址库的范围,并依据国家、运营商、省/州、城市精细划分，提供具备 CNAS 和 CMA 资质的第三方测评机构出具的测试报告，加盖原厂公章。
链路负载均衡	★支持静态 IP 和 PPPOE 两种线路接入方式,提供设备操作界面截图证明材料，并加盖厂商公章。
	★支持三明治架构，对防火墙、IPS、行为管理等网络设备进行流量负载均衡和故障切换，使以上网络设备获得 Active-Active 运行的能力，提供实际的功能测试报告，并加盖厂商公章。
	支持基于五元组条件（源 IP 地址，源端口，目的 IP 地址，目的端口，传输层协议号）来进行出站访问的流量调度分发。
	支持基于管理员自定义的时间计划来进行出站访问的流量调度分发。
	内置完备的 IP 地址库，无需手动导入并支持自动更新，可查看并编辑各国家、国内各省份的 IP 地址段和国内各大运营商 IP 地址段，并可灵活匹配 IP 地址库进行流量调度分发，实现链路负载功能。
	支持基于 URL 的链路调度功能，内置不少于 1000 条的国外 URL 网址库，无需手动导入并支持自动更新，管理员可查看并进行编辑。可根据 URL 将访问国外网站的请求调度到指定线路。
	支持 DNS 透明代理功能，可基于负载均衡算法代理内网用户进行 DNS 请求转发，避免单运营商 DNS 解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率。
	支持 DNS 内网记录，包含 A、AAAA、CNAME、MX 和 TXT 等类型，可识别内网用户并对其 DNS 请求直接返回相应结果； 支持智能 DNS 解析功能，实现外网用户访问内网业务系统的最优路径选择。
	支持基于链路负荷情况的繁忙保护机制，能根据链路的上行/下行带宽占用率情况执行对出站/入站流量的高级调度策略。
	可以支持 Ping、Ping-GW、TCP、HTTP/HTTPS、HTTP/HTTPS-EVC、FTP、DNS、POP3、SMTP、IMAP、MySQL、Radius、LDAP 健康检查，可以支持基于 LUA 脚本的健康检查，提供具备 CNAS 和 CMA 资质的第三方测评机构出具的测试报告，加盖原厂公章。

	★支持非对称式部署的 TCP 协议优化技术，提升远端用户访问应用服务的速度。无需在用户终端或应用服务器上安装任何插件和软件，不受操作系统类型、浏览器版本等兼容性因素限制，并且用户首次访问应用服务即可产生加速效果(提供第三方评测报告,证明所投产品厂商可提供此类技术，并加盖原厂公章)。
安全加固	支持四七层 DDoS 攻击防护：ICMP-Flood、SYN-Flood、UDP-Flood、DNS Query Flood、Script-Flood 、TCP 全连接攻击、并发连接耗尽攻击、SSL-Flood、HTTP Flood、CC 攻击、慢速攻击、Smurf 攻击、Fraggle 攻击、ARP/ND 等攻击防护。
运维管理	支持全中文管理界面和 HTTPS 方式登录、用户角色管理、多级授权管理。
	服务器负载状态支持投屏展示，能够显示设备的电源状态、风扇转速、磁盘温度、CPU 温度、CPU 和内存占用率、新建连接数、并发连接数、吞吐情况、SSL 新建和 SSL 吞吐数据、压缩优化和缓存优化数据；业务的健康状态、新建连接数、并发连接数、上下行流量、每秒请求数；节点池的调度算法、健康状态、新建连接数、并发连接数、上下行流量（需提供相关功能截图证明，并加盖厂商公章）。
★产品资质	所投产品具备《IPv6 Ready Phase-2 金色认证证书》(提供复印件，并加盖厂商公章)。
	所投产品为国产品牌非 OEM 设备。
	所投产品生产厂家通过 CMMI5 认证以保证产品代码质量与稳定性(提供复印件，并加盖厂商公章)。
	所投产品具备国家工业和信息化部颁发的《电信设备进网许可证》(提供复印件，并加盖厂商公章)。
服务要求	3 年原厂服务，提供原厂商服务承诺函。

（3）安全网关

技术指标	指标要求
数量	1 台。
整机吞吐量	≥10Gbps。
应用层吞吐量	≥2Gbps。
并发连接数	≥220W。
每秒新建连接数	≥12W。
设备接口	2U 机架设备,标配 10 个千兆电口，4 个千兆光口 。
部署方式	设备需要和互联网出口其他设备进行联动切换，以保障单点故障后可以快速，ICMP 丢包数量≤5 个。
★架构要求	设备需要与我单位现有安全网关实现双机热备，主设备宕机时可实现快速切换。
路由支持	支持静态路由，ECMP 等价路由； 支持 RIPv1/v2，OSPFv2/v3，BGP 等动态路由协议； 支持多链路出站负载，支持基于源/目的 IP、源/目的端口、协议、ISP、应用类型以及国家地域来进行选路的策略路由选路功能。
基础功能	支持连接会话展示，可针对具体的 IP 地址进行会话详情查询，支持封锁异常会话信息，并支持设置监听具体 IP 的会话记录； 支持根据国家/地区来进行地域访问控制。
内容安全	支持 URL 过滤和文件过滤功能,URL 过滤支持 GET,POST 请求过滤和 HTTPS 网站过滤，文件过滤支持文件上传和下载过滤； **★支持针对 SMTP、POP3、IMAP 邮件协议的内容检测，如邮件附件病毒检测、邮件内容恶意链接检测，邮件异常账号检测等，支持根据邮件附件类型进行文件过滤；支持针对 HTTP、FTP 协议内容检测与病毒查杀（需提供相关功能截图证明，并加盖厂商公章）。**
入侵防护功能	设备具备独立的入侵防护漏洞规则特征库，特征总数在 7000 条以上； 支持同防火墙访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联动封锁，支持自定义封锁时间； **★可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和**

	自动检测，发现问题后支持一键生成防护规则（需提供相关功能截图证明，并加盖厂商公章）。
僵尸主机检测	设备具备独立的热门威胁库，支持木马、勒索软件、蠕虫、挖矿病毒等种类，特征总数在 50 万条以上； 支持恶意域名重定向功能，用于 DNS 代理服务器场景下定位内网感染僵尸网络病毒的真实主机 IP 地址； 支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为（需提供相关功能截图证明，并加盖厂商公章）。
★设备联动	支持直接从安全分析系统产品上直接下发应用控制策略到安全网关（需提供相关功能截图证明，并加盖厂商公章）。
★厂商资质	厂商软件研发实力需通过 CMMI L5 认证，提供证明文件，并加盖原厂公章。
	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，提供证明文件，并加盖原厂公章。
★产品资质	电信设备进网许许可证（提供证明文件，并加盖原厂公章）。
★产品成熟度要求	厂商具备云安全成熟度模型 CSA-CMMI5 认证，提供证书复印件并加盖厂商公章。
★服务要求	三年原厂服务并提供原厂服务承诺函。

（4）互联网日志审计系统

技术指标	指标要求
数量	2 台。
支持带宽	≥700Mb。
用户规模	≥7000 人。
设备接口	6 个千兆电口； 2 个千兆光口。
硬盘	≥1TB。
BYPASS	支持。
★部署模式	设备需要和互联网出口其他设备进行联动切换，以保障单点故障后可以快速，ICMP 丢包数量≤5 个。
多主模式	必须支持两台及两台以上设备同时做主机的部署模式。
所有功能支持 IPv6	支持部署在 Ipv6 环境中，其所有功能（认证、应用控制、内容审计、报表等）都支持 Ipv6（提供产品界面截图，并加盖厂商公章）。
Web 访问质量监测	**★针对内网用户的 web 访问质量进行检测，对整体网络提供清晰的整体网络质量评级；** 支持以列表形式展示访问质量差的用户名单； 支持对单用户进行定向 web 访问质量检测（提供产品界面截图，并加盖厂商公章）。
首页可视化分析展示	支持首页分析显示接入用户人数、终端类型、认证方式； 带宽质量分析、实时流量排名； 泄密风险、违规访问、共享上网等行为风险情况。
用户密码强度	可设置用户密码不能等于用户名； 新密码不能与旧密码相同； 可设置密码最小长度； 可设置密码必须包括数字或字母或特殊字符（提供产品界面截图，并加盖厂商公章）。
多终端自定绑定	同一个账号，支持与指定数量的多个终端进行自动绑定。
共享接入管理（防共享）	设备能够发现私接路由（或者共享软件等）共享网络的行为： 1.支持自定义配置终端数量和冻结时间，和添加信任列表； 2.支持显示以 IP 或用户名的维度统计一段时间内的趋势图；

	3.支持例外排除功能：如指定例外条件 1 台 PC，2 个终端。当 PC 或终端数超过例外条件才会被判定为共享（提供产品界面截图，并加盖厂商公章）。
QQ 白名单	支持基于用户组、终端类型、位置的 QQ 白名单功能。
SSL 加密内容审计和过滤	针对 SSL 加密的网站、论坛发帖、web 邮箱的内容进行关键字过滤和内容审计。
动态流控	支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率。
P2P 智能流控	支持通过抑制 P2P 的上行流量，来减缓 P2P 的下行流量，从而解决网络出口在做流控后仍然压力较大的问题（提供产品界面截图，并加盖厂商公章）。
趋势报表	支持基于时间段/用户/用户组/终端类型/位置等多种维度的流速趋势报表、流控通道趋势报表、应用行为趋势报表、网站分类行为趋势报表等。
设备联动	支持和安全分析系统联动响应，实现将设备用户与安全事件关联； 支持通过浏览器推送用户提醒或冻结用户上网。
★产品资质要求	具有工信部颁发的《电信设备进网许可证》（提供证明文件并加盖原厂公章）。
	应为市场成熟产品，最近两年在国内 IDC 内容安全市场占有率排名都在前 3（提供证明文件并加盖原厂公章）。
	产品通过《网络关键设备和网络安全专用产品安全认证》，提供证书加盖原厂公章。
	具备《网络通讯安全审计产品（国标）销售许可证》，提供证书加盖原厂公章。
★厂商资质要求	公司研发体系通过国际认证 CMMI5（提供证明文件并加盖原厂公章）。
	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（提供证明文件，并加盖原厂公章）。
	厂商应是国家标准《信息安全技术信息系统安全审计产品技术要求和测试评价方法》的主要起草单位。
服务要求	三年原厂服务并提供原厂服务承诺函。

（5）IDC 安全网关

技术指标	指标要求
数量	1 台。
整机吞吐量	≥8Gbps。
并发连接数	≥200W。
每秒新建连接数	≥10W。
设备接口	2U 机架设备,标配 4 个千兆电口，8 个千兆光口 。
部署方式	支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式。
路由支持	支持静态路由，ECMP 等价路由； 支持 RIPv1/v2，OSPFv2/v3，BGP 等动态路由协议； 支持多链路出站负载，支持基于源/目的 IP、源/目的端口、协议、ISP、应用类型以及国家地域来进行选路的策略路由选路功能（需提供相关功能截图证明，并加盖原厂商公章）。
基础功能	支持连接会话展示，可针对具体的 IP 地址进行会话详情查询，支持封锁异常会话信息，并支持设置监听具体 IP 的会话记录； 支持根据国家/地区来进行地域访问控制（需提供相关功能截图证明，并加盖原厂商公章）。
内容安全	支持 URL 过滤和文件过滤功能，URL 过滤支持 GET，POST 请求过滤和 HTTPS 网站过滤，文件过滤支持文件上传和下载过滤； 支持针对 SMTP、POP3、IMAP 邮件协议的内容检测，如邮件附件病毒检测、邮件内容恶意链接检测，邮件异常账号检测等，支持根据邮件附件类型进行文件过滤；支持针对 HTTP、FTP 协议内容检测与病毒查杀（需提供相关功能截图证明，并加盖原厂商公章）。
入侵防护功能	设备具备独立的入侵防护漏洞规则特征库，特征总数在 7000 条以上； 支持同防火墙访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联动封

	锁，支持自定义封锁时间； **★可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则（需提供相关功能截图证明，并加盖原厂商公章）。**
僵尸主机检测	设备具备独立的热门威胁库，支持木马、勒索软件、蠕虫、挖矿病毒等种类，特征总数在 50 万条以上（需提供相关功能截图证明，并加盖原厂商公章）；支持恶意域名重定向功能，用于 DNS 代理服务器场景下定位内网感染僵尸网络病毒的真实主机 IP 地址； 支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为。
安全可视化	支持业务安全和用户安全的风险展示； 支持全网实时热点事件展示； 支持对检测到的攻击行为按照 IP 地址的地理位置信息进行威胁信息动态展示，实时监测和展示最新的攻击威胁信息。
设备联动	支持直接从安全分析系统产品上直接下发应用控制策略到安全网关。
★厂商资质	厂商软件研发实力需通过 CMMI L5 认证（提供证书复印件，并加盖原厂公章）。
	厂商需是 CSA 云安全联盟会员单位（提供证明文件，并加盖原厂公章）。
	厂商需是国家信息安全漏洞共享平台(CNVD)技术组成员（提供证明文件，并加盖原厂公章）。
	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（提供证明文件，并加盖原厂公章）。
★产品成熟度要求	厂商具备云安全成熟度模型CSA-CMMI5认证(提供证书复印件并加盖厂商公章)。
★服务要求	三年原厂服务并提供原厂服务承诺函。

（6）专线安全网关

技术指标	指标要求
数量	1 台。
整机吞吐量	≥3Gbps。
应用层吞吐量	≥500Mb。
并发连接数	≥150W。
每秒新建连接数	≥3W。
设备接口	1U 机架设备,标配 4 个千兆电口，2 个千兆光口 。
部署方式	支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式。
路由支持	支持静态路由，ECMP 等价路由； 支持 RIPv1/v2，OSPFv2/v3，BGP 等动态路由协议； 支持多播/组播路由协议； 支持路由异常告警功能。
基础功能	支持连接会话展示，可针对具体的 IP 地址进行会话详情查询，支持封锁异常会话信息，并支持设置监听具体 IP 的会话记录； 访问控制规则支持基于源 / 目的 IP，源端口，源 / 目的区域，用户（组），应用/服务类型，时间组的细化控制方式； 支持根据国家/地区来进行地域访问控制。
内容安全	支持 URL 过滤和文件过滤功能，URL 过滤支持 GET，POST 请求过滤和 HTTPS 网站过滤，文件过滤支持文件上传和下载过滤； 支持针对 SMTP、POP3、IMAP 邮件协议的内容检测，如邮件附件病毒检测、邮件内容恶意链接检测，邮件异常账号检测等，支持根据邮件附件类型进行文件过滤； 支持针对 HTTP、FTP 协议内容检测与病毒查杀（需提供相关功能截图证明，并加盖厂商公章） 。
入侵防护功能	设备具备独立的入侵防护漏洞规则特征库，特征总数在 7000 条以上； 支持同防火墙访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联动封锁，支持自定义封锁时间； **★可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则（需提供相关功能截图证明，并加盖厂商公章）。**
僵尸主机检测	设备具备独立的热门威胁库，支持木马、勒索软件、蠕虫、挖矿病毒等种类，特征总数在 50 万条以上； 支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为（需提供相关功能截图证明，并加盖厂商公章）； 支持通过云端的大数据分析平台，发现和展示整个僵尸网络的构成和分布，定位僵尸网络控制服务器的地址。

安全可视化	支持业务安全和用户安全的风险展示； 支持全网实时热点事件展示； 支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别，支持包含敏感数据业务的识别； 支持对检测到的攻击行为按照 IP 地址的地理位置信息进行威胁信息动态展示，实时监测和展示最新的攻击威胁信息； 支持在同一个界面对全网所有服务器和主机的安全状况进行风险评估，支持对当前所有业务的安全防护状态进行动态保护，支持对所有已被入侵和受控的设备进行风险检测与分析，针对风险可以实现快速响应与处置； 支持手动评估功能，自动展示最终的风险。
设备联动	支持直接从安全分析系统产品上直接下发应用控制策略到安全网关（需提供相关功能截图证明，并加盖厂商公章）。
★厂商资质	厂商软件研发实力需通过 CMMI L5 认证（提供证明文件，并加盖原厂公章）。
	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（提供证明文件，并加盖原厂公章）。
	厂商需是国家信息安全漏洞共享平台(CNVD)技术组成员（提供证明文件，并加盖原厂公章）。
★产品成熟度要求	厂商具备云安全成熟度模型 CSA-CMMI5 认证，提供证书复印件并加盖厂商公章。
★服务要求	三年原厂服务并提供原厂服务承诺函。

（7）安全设备统一管理平台

技术指标	指标要求
数量	1 台。
支持受控端管理数目	最大可管控 2000 个设备接入 。
网络接口	6 个千兆电口。
内置硬盘	1T SATA 盘。
设备型态	标准 1U。
★架构要求	平台底层采用超融合架构，支持平台中的集群资源环境一键检测，包括系统运行状态检测（系统服务检测、配置文件检测、系统分区检测、存储空间检测）、系统配置检测（系列号有效性检测、网口配置检测）、硬件健康监测（CPU 检测、内存检测、网卡检测、磁盘基本功能检测、RAID 检测），提供具备 CNAS 和 CMA 资质的第三方测评机构出具的测试报告，加盖厂商公章。
	平台底层采用超融合架构，支持数据数据重构功能，且重构速度可以达 30min/TB，提供具备 CNAS 和 CMA 资质的第三方测评机构出具的测试报告，加盖厂商公章。
	平台底层采用超融合架构，支持对 Oracle、SQL Server、Weblogic 数据库及中间件监控，实现对数据库的语句的故障定位排错，执行时延分析，提供具备 CNAS 和 CMA 资质的第三方测评机构出具的测试报告，加盖厂商公章。
单臂模式	设备必须支持单臂模式，以在不影响原有网络情况下同时能降低网络单点故障的发生概率。
软硬解耦	支持软硬件平台一体化交付，以及支持部署在 vmvare、深信服超融合等虚拟化平台。
可视化展示分支	具备可视化界面，以地图方式通过不同颜色展示全网分支机构健康、离线、告警状态，同时可展开省、市、区等多级分支。
设备自身管理	支持 Web、SSH。
远程接入分支	支持通过单点登录方式远程接入分支进行配置和管理，提供截图证明并加盖厂商公章。
分支详情展示	支持展示所有在线网点的网络吞吐带宽展示、当前用户流量信息、分支设备版本信息。
分支资源概况	支持即时查看受控设备状态，包括 CPU、内存、磁盘占用等。
分支版本监控	BBC 智能监控分支端设备 URL、应用识别库，若不是最新版本智能提醒升级。
网络告警	主机网口掉线、数据通信口不通、虚拟机与外部网络不通、直击网口丢包等。

离线告警	分支设备离线 。
授权告警	分支设备序列号过期、序列号状态异常、虚拟网络设备序列号过期等。
硬件告警	主机 CPU、磁盘利用率高，虚拟网络设备 CPU、磁盘利用率高等。
安全告警	全网分支网络安全告警，如系统漏洞、攻击、木马等安全风险。
日志查看	内置日志中心，详细记录管理员操作日志，管理员也可自行设定过滤规则来查看所需日志信息。
上网行为日志	支持同步受控端数据中心的日志到同一个外置数据中心，支持对内网中所有受控端日志的统计、排行和导出。
受控端设备日志查看	管理员通过 BBC 远程接入可以查看任何一台受控设备的实时及历史日志信息。
★厂商资质	厂商软件研发实力需通过 CMMI L5 认证（提供证明文件并加盖原厂公章）。
★服务要求	三年原厂服务并提供原厂服务承诺函。

（8）安全分析系统

技术指标	指标要求
数量	1 台。
尺寸	2U 架构。
硬盘容量	32TB。
CPU	16 核心。
内存	96G 内存。
接口数量	4 个千兆电口、1 个串口、3 个 USB 口。
电源	冗余电源。
综合安全态势大屏	支持大屏展示综合安全态势，包括资产态势、脆弱性态势、网络攻击态势、安全事件态势、外连态势、横向威胁态势，支持页面跳转到对应态势大屏。
安全事件态势	支持大屏展示安全事件态势，包括安全事件、事件等级分布、安全事件态势、安全事件 TOP5、威胁面最大的事件 TOP10、事件类型 TOP5、风险业务/终端 TOP5。
脆弱性态势	支持大屏展示业务脆弱性态势，包括漏洞风险态势、漏洞类型 TOP5、高危漏洞 TOP5、业务总览、脆弱性业务 TOP5、实时脆弱性监测（需提供截图证明并加盖原厂商公章）。
业务风险外连态势	支持大屏展示业务外连态势，包括外连风险总览、外连威胁 TOP10、外连态势、外连地区 TOP5、实时威胁监控，并支持国际、国内地图自主切换。
网络攻击态势	支持大屏展示网络攻击态势，包括攻击者、攻击总数、残余攻击、被攻击服务器、被攻击服务器 TOP5、攻击态势，并支持攻击全景地图展示。
★访问关系梳理大屏	支持大屏展示正常横向访问和正常外连监控，正常横向访问监控包括被访问最多的业务 TOP5、最活跃终端 TOP5、应用 TOP5、实时访问监控等，正常外连监控包括外连最多的业务 TOP5、外连最多终端 TOP5、外连态势、外连国家 TOP5,并支持国际、国内地图切换（需提供截图证明并加盖原厂商公章）。
多视角大屏展示	支持不同视角展示全网态势，包括综合安全态势、分支安全态势、安全事件态势、网络攻击态势、外连风险态势、横向威胁态势、脆弱性态势、资产态势等 8 个独立的大屏展示功能，并支持大屏轮播（需提供截图证明并加盖原厂商公章）。
分支	支持分支维度感知资产，可定义分支名称、责任人、责任人邮箱、设备、地理位置地图，地图可选择在线地图、离线地址或本地导入地图。
弱密码	支持镜像流量检测业务系统中的弱密码，检测列表包含账号、密码、服务器、所属分析和业务、最近登录源 IP、类型、最近发现时间等信息，密码星号显示需超级管理员才可查看，并支持储存数据包内容。
Web 明文传输	支持镜像流量检测 web 流量中是否存在可截获的口令信息，检测列表包含对应域名/URL、服务器 IP，所属分支和业务，数据包举证等信息，避免因明文传输导致信息泄露的风险。
漏洞报告	支持基于流量实时漏洞功能，漏洞分析类型包含配置错误漏洞、OpenSSH 漏洞、目录遍历漏洞、OpenLDAP 等操作系统、数据库、Web 应用等，页面上支持展示

	业务脆弱性风险分布、漏洞类型分析、漏洞态势与危害和处置建议，并支持导出脆弱性感知报告。
风险安全域视角	支持安全域维度展示安全风险，包含安全域列表、安全域评分、事件类型 TOP5、IP 地址、IP 类型、风险等级、关键风险、状态等信息（需提供截图证明并加盖原厂商公章）。
威胁分析	外部威胁感知展示包含高危攻击、残余攻击、暴力破解、成功的事中攻击、邮件威胁、文件威胁、外部风险访问；
	横向威胁感知展示包含横向威胁总览、横向攻击、违规访问、可疑行为、风险；其中横向风险总览包含发起与遭受横向威胁主机 TOP5，发起视角包含发起者 IP、发起者类型、所属分析、所属业务/终端组、横向威胁类型、遭受者数、遭受者类型、日志数（需提供截图证明并加盖原厂商公章）；
	★外连威胁感知包含对外威胁总览、对外攻击、APTC&C 通信、可疑行为、隐蔽通、违规访问、服务器风险访问；其中外连威胁总监包括外连威胁主机类型分布、存在外连威胁 IP TOP5、外连目标地区（国外）TOP5、外连威胁类型分布、非正常时间段外连主机 TOP5、外连威胁趋势。
访问关系分析	访问关系可视包含横向访问关系可视、外连可视，横向访问关系可视包含基于访问次数和流量大小被访问最多业务 TOP5、最活跃终端 TOP5，外连可视包含外连最多的业务 TOP5、外连最多终端 TOP5、外连趋势等；
	服务器外连支持 7 天、30 天服务器外连流量趋势，外连地域分布，其中流量可区分请求流量与响应流量，并支持流量请求响应比分析。
★潜伏威胁黄金眼	支持基于可视化的形式展示威胁的影响面，通过大数据分析和关联检索技术，能够直观的看到失陷主机的威胁影响面，同时基于列表模式展示攻击、违规访问、风险访问、可疑行为、正常访问等详细信息； 支持攻击溯源功能，分析出首次失陷、疑似入口点、首次遭受攻击等信息；帮助管理人员及时了解威胁的影响，并找到攻击入口点（需提供截图证明并加盖原厂商公章）。
综合风险报告	支持完整展示网络的安全态势和详情的综合风险报告，报告内容包括平台说明、安全风险概括、业务与终端安全详情分析、安全规划建设建议等。
★等级保护管理服务	支持对等级保护建设整改过程中系统定级、差距评估、备案、整改、测评过程中产生的文档结论进行统计归档，并使用可视化的统一界面进行展现与管理，最大程度发挥安全措施的保护能力（提供证明文件，并加盖厂商公章）。
UEBA	支持对业务服务器内网横向被访问、横向主动访问、外连等建立行为基线，其中包括访问流量趋势、访问次数趋势、自定义非正常时间段、常见访问源网段、访问源主机、应用 TOP5、目的端口 TOP5 等（需提供截图证明并加盖原厂商公章）。
SIEM	具备独立的 SIEM 管理模块，支持接入第三方安全设备、网络设备、DHCP 服务器、蜜罐、中间件等日志接入和解析功能，并支持导入正则文件解析主流设备日志，支持 syslog、wmi、https 接入方式；
	支持暴力破解、新增/修改/删除账号/账号提权、高危操作等内置关联分析规则，

	并支持规则启用与禁用。
★安全组件接入展示	支持接入防火墙、上网行为管理、终端 EDR、WAC 无线控制器、DAS 数据库审计和潜伏威胁探针等设备,并支持在页面中显示安全组件接入的数量和状态（需提供功能截图证明并加盖原厂商公章） 。
★EDR 组件联动	支持与同品牌终端 EDR 组件联动响应，禁止攻击流量出站或入站，并支持一键扫描和主机隔离，防止风险扩展（需提供功能截图证明并加盖原厂商公章）。
★防火墙设备联动	支持与同品牌防火墙进行联动响应，支持平台下发安全策略到防火墙上，阻断攻击流量（需提供功能截图证明并加盖原厂商公章）。
★WAC 设备联动	支持与无线控制器进行联动响应，同步无线接入用户信息，实现与安全事件关联，同时支持下发安全策略冻结无线用户账号（需提供功能截图证明并加盖原厂商公章）。
★SSL VPN 设备联动	支持与同品牌 SSL VPN 设备同步用户用户信息，包括用户登录、登出、分配 IP、访问资源记录的日志数据，实现远程接入用户与安全事件关联分析，分析出异常用户，以 VPN 用户为可视化视角，呈现风险问题、风险程度、内网资源访问情况等。支持同步管理员操作日志，满足审计要求（需提供截图证明并加盖原厂商公章）。
★上网行为设备联动	支持与同品牌上网行为管理设备进行联动响应，同步上网行为管理设备认证用户，实现与安全事件关联； 支持通过浏览器推送用户提醒或冻结用户上网（需提供截图证明并加盖原厂商公章）。
接入设备管理	分析平台可对安全探针进行统一的升级管理，支持配置向导功能，通过系统检测功能，检测设备基础配置、设备资源、设备接入情况、设备流量等是否有异常，并导出上架检测报告，同时支持监控探针和各类安全组件的运行状态，包含日志传输模式、日志传输量、最近同步信息等，其中安全组件需包括 EDR、上网行为管理、无线控制器、VPN 等设备（需提供截图证明并加盖原厂商公章）。
平台级联	支持上下级平台级联，下级平台可上报资产信息、安全事件、脆弱性风险到上级平台，并支持展示级联状态，最近上报时间等信息。
开放共享	平台支持通过 RESTful API 接口对平台数据资源的“开放”与“共享”，第三方平台可获取受监控 IP 组、资产信息、风险业务与终端、漏洞详情、弱密码和明文传输等信息，实现数据更大价值。
★厂商综合实力	厂商具备云安全成熟度模型 CSA-CMMI5 认证，提供证书复印件并加盖厂商公章。
★厂商资质	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（提供证明文件，并加盖原厂公章）。
	厂商需是国家信息安全漏洞共享平台(CNVD)技术组成员（提供证明文件，并加盖原厂公章）。
★服务要求	三年原厂服务并提供原厂服务承诺函。

（9）网络威胁探针

技术指标	指标要求
数量	1 台。
★品牌要求	与安全分析系统为同一品牌。
接口数量	4 个千兆电口、4 个千兆光口。
性能指标	1.5Gbps。
部署模式	旁路部署，支持探针同时接入多个镜像口，每个口相互独立不影响。
资产发现	具备主动发送少量探测报文，发现潜在的服务器（影子资产）以及学习服务器的基础信息，如：操作系统、开放的端口号等。
异常会话检测	可实现对外联行为分析、间歇会话连接分析、加密通道分析、异常域名分析、上下行流量分析等在内 的多场景网络异常通信行为分析能力。
高级检测	**★支持 5 种类型日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求（需提供截图证明并加盖原厂商公章）；**
	支持 DNS 审计日志，主要用于平台 dns flow 分析引擎进行安全分析； HTTP 审计日志，主要用于平台 http flow 分析引擎进行安全分析； SMB 审计日志，主要用于平台 SMB flow 分析引擎进行安全分析； 同步 SMTP、POP3、IMAP 审计日志，主要用于平台 Mail flow 分析引擎进行安全分析，同步 AD 域协议审计日志，主要用于平台 AD 域分析引擎进行安全分析。
Web 应用安全检测能力	支持 HTTP 1.0/1.1，HTTPS 协议的安全威胁检测； 支持针对 B/S 架构应用抵御 SQL 注入、XSS、系统命令等注入型攻击； 支持跨站请求伪造 CSRF 攻击检测； 支持对 ASP,PHP,JSP 等主流脚本语言编写的 webshell 后门脚本上传的检测； 支持其他类型的 Web 攻击，如文件包含，目录遍历，信息泄露攻击等的检测； 产品应具备独立的 Web 应用检测规则库，Web 应用检测规则总数在 3000 条以上； 支持敏感数据泄密功能检测能力，支持敏感信息自定义，支持根据文件类型和敏感关键字进行信息过滤； 支持对被 Web 网站是否被挂黑链进行检测。
僵尸网络检测	**★支持对终端种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为（需提供截图证明并加盖原厂商公章）；** 具备独立的僵尸主机识别特征库，恶意软件识别特征总数在 35 万条以上； 对于未知威胁具备同云端安全分析引擎进行联动的能力，上报可疑行为并在云端进行沙盒检测，并下发威胁特征。
违规访问检测	能够针对 IP，IP 组，服务，端口，访问时间等策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单（哪些访问逻辑是正常的）和黑名单（哪些访问逻辑肯定是异常的）两种方式。
集中管控	支持安全感知平台对接入探针的统一升级，可展示当前所有接入探针的规则库日期、是否过期等，并支持禁用指定探针的升级（需提供截图证明并加盖原厂

	商公章）。
部署	支持旁路部署，对镜像流量进行监听； 可以多台采集器同时部署于客户网络不同位置并将数据传输到同一套分析平台。
产品资质	要求安全感知平台具备公安颁发的安全管理平台销售许可证； 要求具备国家版权局颁发的软件著作权登记证书。
★厂商资质	厂商软件研发实力需通过 CMMI L5 认证（提供证明文件，并加盖原厂公章）。
	国家信息安全漏洞共享平台(CNVD)技术组成员； （提供证明文件，并加盖原厂公章）。
	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（提供证明文件，并加盖原厂公章）。
★厂商综合实力	厂商需是国家信息安全漏洞共享平台(CNVD)技术组成员（提供证明文件，并加盖原厂公章）。
★服务要求	三年原厂服务并提供原厂服务承诺函。

（10）业务威胁探针

技术指标	指标要求
数量	1 台。
★品牌要求	与安全分析系统为同一品牌。
接口数量	4 个千兆电口、2 个千兆光口。
性能指标	1Gbps。
部署模式	旁路部署，支持探针同时接入多个镜像口，每个口相互独立不影响。
资产发现	具备主动发送少量探测报文，发现潜在的服务器（影子资产）以及学习服务器的基础信息，如：操作系统、开放的端口号等。
异常会话检测	可实现对外联行为分析、间歇会话连接分析、加密通道分析、异常域名分析、上下行流量分析等在内 的多场景网络异常通信行为分析能力。
高级检测	**★支持 5 种类型日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求（需提供截图证明并加盖原厂商公章）。**
	支持 DNS 审计日志，主要用于平台 dns flow 分析引擎进行安全分析； HTTP 审计日志，主要用于平台 http flow 分析引擎进行安全分析； SMB 审计日志，主要用于平台 SMB flow 分析引擎进行安全分析； 同步 SMTP、POP3、IMAP 审计日志，主要用于平台 Mail flow 分析引擎进行安全分析，同步 AD 域协议审计日志，主要用于平台 AD 域分析引擎进行安全分析。
Web 应用安全检测能力	支持 HTTP 1.0/1.1，HTTPS 协议的安全威胁检测； 支持针对 B/S 架构应用抵御 SQL 注入、XSS、系统命令等注入型攻击； 支持跨站请求伪造 CSRF 攻击检测； 支持对 ASP,PHP,JSP 等主流脚本语言编写的 webshell 后门脚本上传的检测； 支持其他类型的 Web 攻击，如文件包含，目录遍历，信息泄露攻击等的检测； 产品应具备独立的 Web 应用检测规则库，Web 应用检测规则总数在 3000 条以上； 支持敏感数据泄密功能检测能力，支持敏感信息自定义，支持根据文件类型和敏感关键字进行信息过滤； **★支持对被 Web 网站是否被挂黑链进行检测。**
僵尸网络检测	**★支持对终端种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为（需提供截图证明并加盖原厂商公章）；** 具备独立的僵尸主机识别特征库，恶意软件识别特征总数在 35 万条以上； 对于未知威胁具备同云端安全分析引擎进行联动的能力，上报可疑行为并在云端进行沙盒检测，并下发威胁特征。
违规访问检测	能够针对 IP，IP 组，服务，端口，访问时间等策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单（哪些访问逻辑是正常的）和黑名单（哪些访问逻辑肯定是异常的）两种方式。
集中管控	支持安全感知平台对接入探针的统一升级，可展示当前所有接入探针的规则库日期、是否过期等，并支持禁用指定探针的升级；（需提供截图证明并加盖原

	厂商公章）。
部署	支持旁路部署，对镜像流量进行监听； 可以多台采集器同时部署于客户网络不同位置并将数据传输到同一套分析平台。
产品资质	要求安全感知平台具备公安颁发的安全管理平台销售许可证（提供证明文件，并加盖原厂公章）； 要求具备国家版权局颁发的软件著作权登记证书。
★厂商资质	厂商软件研发实力需通过 CMMI L5 认证（提供证明文件，并加盖原厂公章）；
	国家信息安全漏洞共享平台(CNVD)技术组成员（提供证明文件，并加盖原厂公章）。
	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（提供证明文件，并加盖原厂公章）。
★厂商综合实力	厂商需是国家信息安全漏洞共享平台(CNVD)技术组成员（提供证明文件，并加盖原厂公章）。
★服务要求	三年原厂服务并提供原厂服务承诺函。

（11）核心交换机

功能及技术指标	参数要求
数量	1 台。
★业务插槽数	业务插槽数≥6。
★整机交换容量	≥19Tbps（官网双重指标取小值，提供官网截图）。
★整机包转发性能	≥2800Mpps（官网双重指标取小值，提供官网截图）。
主控引擎	主控引擎模块≥2，满足 1+1 冗余。
端口密度	整机万兆端口密度≥288 个； 整机 40GE 端口密度≥144 个； 整机 100GE 端口密度≥24 个。
★虚拟化	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，提供第三方测试报告证明并加盖原厂公章。
	N:1 虚拟化:可将 4 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，提供第三方测试报告证明并加盖原厂公章。
	支持多虚一技术和一虚多技术的配合使用，提供第三方测试报告证明并加盖原厂公章。
★网络安全一体化	支持防火墙、流量分析、IPS、流量控制、负载均衡、无线控制器等多业务模块，以满足后续控制、管理的要求；要求上述功能在官方网站可以查询，并提供官方截图。
有线无线一体化	支持 AC 板卡；
	支持有线无线一体化的终端准入认证。
★资质认证	提供工信部入网证，提供产品检测报告。
★配置要求	1.配置双主控，冗余电源； 2.配置≥48 个万兆光口； 3.实配虚拟化功能； 4.配置 10 个电模块。
★服务要求	三年原厂服务并提供原厂服务承诺函。

（12）交换机 A

功能及技术指标	参数要求
数量	1 台。
★整机交换容量	≥330Gbps（官网双重指标取小值，提供官网截图）。
★整机转发性能	≥90Mpps（官网双重指标取小值，提供官网截图）。
★接口类型	固化≥24 个 100/1000M SFP 光口及 8 个千兆 Combo 口，≥4 个万兆 SFP+端口。
VLAN 特性	最大 VLAN 数(不是 VLAN ID) ≥4094。
路由协议	支持 IPv4 静态路由、RIP V1/V2、OSPF； 支持 IPv6 静态路由、RIPng； 支持 IPv4 和 IPv6 环境下的策略路由。
堆叠	最大堆叠台数≥9 台； 最大堆叠带宽≥80G； 支持跨设备链路聚合，单一 IP 管理，分布式弹性路由； 支持通过标准以太端口进行堆叠（万兆或千兆均支持）； 支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预； 支持远程堆叠。
链路聚合	支持最多 8 个端口聚合；支持最多 128 个聚合组；支持 LACP。
安全特性	支持 802.1x、portal 认证功能，支持组播功能，并提供权威机构测试报告，并加盖原厂公章。
★资质认证	提供工信部入网证，提供产品检测报告。
★配置要求	1.每台单电源配置； 2.上行光模块：每台配置 4 个万兆多模光模块。
★服务要求	三年原厂服务并提供原厂服务承诺函。

（13）交换机 B

功能及技术指标	参数要求
数量	6 台。
★整机交换容量	≥330Gbps（官网双重指标取小值，提供官网截图）。
★整机转发性能	≥130Mpps（官网双重指标取小值，提供官网截图）。
★接口要求	固化≥48 个千兆电端口，≥2 个万兆光端口，≥2 个万兆电端口（提供设备前面板图片）。
VLAN 特性	最大 VLAN 数(不是 VLAN ID)≥4094； 支持 QinQ，灵活 QinQ。
三层路由功能	支持 IPv4/v6 静态路由、RIP、RIPng、OSPF 功能。
★链路聚合	支持 GE/10GE 端口聚合，最多 8 个端口聚合； 支持动态聚合； 支持跨设备聚合； 单机支持 14 个端口聚合组，跨设备最大 128 个聚合组。
安全特性	支持 IP+MAC+PORT 的绑定；
	支持 DHCP Snooping，防止欺骗的 DHCP 服务器；
	支持 ARP 检测来抵御 ARP 欺骗攻击；
	支持 CPU 防护；
	支持 802.1x 认证，支持集中式 MAC 地址认证；支持 Portal 认证。
★虚拟化技术	支持堆叠，主机堆叠数≥9 台； 实现单一 IP 管理； 支持跨设备链路聚合； 支持通过标准以太网接口进行堆叠； 支持本地堆叠和远程堆叠，堆叠距离≥10KM。
管理及维护	支持 SNMP V1/V2/V3、RMON、SSHV2。
	支持虚电缆检测功能(VCT)，快速准确定位网络中故障电缆的短路或断路点。
★资质认证	提供工信部入网证书，提供产品检测报告。
★配置要求	1.每台配置 4 个万兆多模光模块。
★服务要求	三年原厂服务并提供原厂服务承诺函。

（14）交换机 C

功能及技术指标	参数要求
数量	1 台。
★设备整机性能	交换容量≥590Gbps，包转发率≥250Mpps。
★接口要求	固化≥48 个千兆电端口，≥4 个万兆光端口，≥1 个扩展插槽（支持万兆电、万兆光、40G）。
★电源	模块化双电源（提供产品结构图证明）。
★风扇	模块化双风扇，前/后通风，风道可调（提供产品结构图证明）。
★多业务	主机支持多业务插卡(防火墙插卡，并可实现 FW、IPS，LB 等安全特性，提供官网截图）。
Macsec	支持 802.1ae Macsec 安全加密，实现 MAC 层安全加密，包括用户数据加密、数据帧完整性检查及数据源真实性校验。无需软件授权。
VLAN 特性	支持基于端口的 VLAN，支持基于协议的 VLAN； 支持基于 MAC 的 VLAN； 最大 VLAN 数(不是 VLAN ID) ≥4094。
链路聚合	支持最多 8 个 GE 口或 4 个 10 GE 端口聚合； 支持最多 128 个聚合组； 支持 LACP。
镜像功能	支持本地端口镜像和远程端口镜像 RSPAN； 支持流镜像； 同时支持 N：M 的端口镜像(M 大于 1)。
路由协议	支持 IPv4 静态路由、RIP V1/V2、OSPF、BGP； 支持 IPv6 静态路由、RIPng、OSPFv3、BGP4+； 支持 IPv4 和 IPv6 环境下的策略路由； 支持 IPv6 手动隧道、6to4 隧道和 ISATAP 隧道。
VxLAN	支持二层 VxLAN； 支持 VxLAN 网关； **★支持 VXLAN 路由交换，提供官网截图。**
★资质认证	提供工信部入网证书，提供产品检测报告。
★配置要求	1.配置双风扇模块，冗余电源； 2.每台配备 4 个万兆多模光模块。
★服务要求	三年原厂服务并提供原厂服务承诺函。

（15）网络管理系统

功能及技术指标	参数要求
数量	1 套。
分布式部署	要求资源拓扑、告警、性能等功能模块支持多服务器分布式虚拟化部署，可实现负载分担。
用户分权管理	可以为不同的管理员设置不同的用户名、密码，并限制管理员的管理权限和管理范围，实现用户分权管理。
多平台支持	支持 Windows、Linux 平台及 MS SQL、Oracle 数据库，支持 B/S 架构。
支持自定义用户主页	管理员可以首页中通过拖拽，自定义需要在首页展示页面。
自动发现拓扑	自动发现网络中的所有网络设备，并在拓扑中显示出来，支持拓扑图自定义修改，包括设备、链路等。
	支持 IP 拓扑、二层拓扑、邻居拓扑、网络拓扑视图（支持网络区域的任意划分、命名、拖拽、折叠和展开）、业务拓扑、STP 拓扑、MSTP 拓扑等多种拓扑类型；二层拓扑支持多协议，包括 Bridge、NDP、CDP、MSTP、STP、LLDP、DISMAN-PING 等二层协议，支持聚合链路，支持第三方的设备；拓扑可融合链路状态、设备告警等多种信息。。
	支持数据中心拓扑，包括机房拓扑、机架拓扑等。
支持设备与用户统一管理	支持网络管理与用户管理联动，如通过点击拓扑楼层接入交换机图标，可查看该设备所有接入用户帐户信息，查询在线用户列表、强制用户下线、下发消息、总在线用户数统计、不安全用户数统计等。
支持设备与流量分析统一管理	支持网络管理平台实现设备管理与流量分析联动，如通过点击拓扑某链路可查看该链路的关键应用流量分布、关键用户流量使用等。
故障管理	支持对全网设备告警的实时监控和统一浏览；支持多种提醒方式，如告警实时提醒（告警板）、告警音响提示；支持多种转发方式，比如转 E-mail，转短信，转上级网管或其它网管等。支持告警分析，可以屏蔽重复告警、闪断告警，支持告警自动确认功能。
	告警智能分析，包括告警分类关联分析、告警多源关联分析、告警拓扑根源分析、告警网络影响度分析。
性能管理	支持基于任务的性能监控，可定制监控任务，长期监控网络性能，可以形成日报、周报、月报等报表。支持定制性能阈值，可以为监控的性能指标设置两级阈值，当性能指标超过阈值时根据不同的阈值发送不同级别的告警。
提供直观的设备的面板视图	提供直观的设备的面板视图：支持设备面板的显示、定时刷新、面板缩放功能，通过面板管理，网络管理人员可以直观地看到设备、板卡、端口的工作状态。
	支持虚拟网络资源管理、虚拟网络拓扑展示、虚拟网络告警管理、虚拟网络性能监控、虚拟交换机配置管理、虚拟网络配置迁移管理。

IP 地址自动扫描	实现网络 IP 地址自动扫描、统计、分配和管理，同时允许用户手工分配和管理 IP 地址，以达到更加灵活的分配管理。结合 IP 地址段的管理功能，将整个网络的 IP，划入各个不同的 IP 地址段，分别进行管理，并给出详细直观的 IP 分配情况统计图表，使管理员能清楚的了解和掌握整个网络的 IP 使用情况。
IP 地址绑定、监控	支持 IP/MAC 绑定，对绑定的 IP/MAC 进行监控，如果该 MAC 地址对应的机器更换了 IP 地址，或者其它机器冒用了本 IP 地址，则系统会立即发送相关告警，通知管理员发生了 IP 使用违规现象，从而管理员能够及时采取措施应对。通过 IP/MAC 绑定，能有效的防治网络 IP 地址使用冲突或盗用的现象。
非法接入设备监控	对接入设备 MAC 地址进行监控，如果其它 MAC 地址接入到该接口，或者该 MAC 从其它设备接口接入网络，系统会立即发送相关告警，通知管理员发生了 MAC 接入违规现象，从而管理员能够及时采取措施应对。通过 MAC/接口绑定，能有效的防止网络中非法设备接入的现象。
全网 VLAN 管理	全网 VLAN 管理功能可以在全网范围内增加、修改和删除 VLAN，并能够方便地对 VLAN 内的设备进行管理，对 access 端口、trunk 端口、hybrid 端口和 VLAN 进行批量配部署。
VLAN 拓扑	VLAN 拓扑功能以可视的方式对网络中的 VLAN 资源进行管理，查看拓扑视图中所有设备节点和链路是否允许某个特定 VLAN 通过。
网络资产自动发现	在设备增加到网络资产管理的同时，系统还会自动发现该设备上可以管理的配件信息，并将这些配件加入到网络资产中进行管理，网管员可以根据不同的查询条件查询网络资产信息，对资产信息进行审计。
支持多种图表展示	提供多种报表样式，包括普通的行列报表、主/子报表、图形摘要报表、交叉表、TopN 和 BottomN 报表。支持多种图形展示：包括条形图、饼图、曲线图、甘特图、面积图、圆环图、三维梯形图、三维曲面图、XY 散点图、雷达图、气泡图、股票图、漏斗图等。
报表导出	可以直接打印或传真报表，也可以选择将报表导出。导出的格式包括 Microsoft Word（RTF）、Microsoft Excel、HTML、PDF、XML、CSV、TXT 等。
支持管理第三方设备	新设备注册，告警注册，新性能指标注册，新 Syslog 解析注册，Mib 编译，第三方设备配置管理-CLI 下发，配置管理-配置备份、软件升级（使用 TCL/Expect /Perl 模板自定制），第三方设备管理系统集成。
★配置要求	配置 25 个网络管理节点授权。
★服务要求	三年原厂服务并提供原厂服务承诺函。

（16）服务器

设备名称	配置	台数
服务器	机架2U E5-2620V4(8核16线程主频2.1)X1 32G 600G SAS10K X3阵列卡 raid5 双电源 导轨 自带操作系统	4台

（17）网络融合集成运维服务

指标项	指标要求
★漏洞分析与管理服务	服务概述：依据相关规范使用专业的国产漏洞扫描工具对信息系统进行全面漏洞扫描工作，并将扫描结果进行系统化管理，清晰掌握信息系统上的漏洞信息，让漏洞修复与管理工作有的放矢。
	服务频率：服务年限以招标文件为准；漏洞扫描次数不限；管理漏洞个数不限。
	资产梳理：梳理需要保护的业务系统，IP，域名并形成资产信息梳理表，并录入系统；
	漏洞扫描：针对通用web漏洞扫描、系统漏洞扫描、数据库漏洞扫描；针对检测网站源码、数据库备份文件、SVN文件、系统重要配置、日志文件向外网泄漏行为进行信息泄漏检测。针对受保护的业务资产提供弱口令的探测服务，内置包含通用性字典弱口令探测，行业性字典弱口令探测。
	漏洞管理：自动化持续跟踪漏洞情况，清晰直观地展示漏洞的修复情况，遗留情况以及漏洞对比情况，使得服务使用方可做到漏洞的可视、可管、可控。
	服务交付物：每月提交《漏洞分析与管理服务报告》
流行威胁通告与排查	结合最新威胁情报，及时对流行威胁进行评估、风险通告预警。
	安全专家排查是否对用户资产造成威胁，通知用户协助及时修复或调整安全策略。
★主动响应服务	根据事件发生的根因、影响范围，针对性给出安全加固方案
	安全服务工程师通过现象深入分析安全事件的成因，发现用户网络中存在的薄弱点，通过技术手段和方法溯源攻击路径；
	针对勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进行根除，快速恢复业务，消除或减轻影响。
	通过结合主动发现、主动处置、被动响应流程，对僵尸网络、病毒、后门、黑链等各类安全事件的处置服务
服务可视	通过安全服务平台，可随时查看业务资产安全状态。
	在线展示所有事件监测结果、防御过程和防御结果。
	本项目使用服务工具支持将收集的安全日志上传到安全服务平台上，并支持在该平台上对服务工具进行管理。
★服务频率	7*24小时持续专家服务，威胁发现及时响应。
服务交付物	《威胁预警报告》、《威胁处置报告》、《威胁管理报告》；
	报告支持每月或每季度或自定义时间导出

★应急响应	针对安全事件发生时，及时，准确的解决安全事件，化解安全危机、将安全事件的风险及损失降到最低。安全事件是指在客户信息系统中出现的影响业务正常运行的任何异常事件。例如：破坏系统的完整性、系统资源拒绝服务、通过渗透或者入侵的方式来对系统进行非法访问，系统资源的滥用以及任何可能对系统造成损害的行为等。
	（1）内容：在甲方遇到突发安全事件的时候，采取适当的响应策略及时遏制安全事件的影响，恢复业务到正常服务状态，保存证据和追查来源等。例如：勒索病毒、信息窃取、拒绝服务攻击、网络流量异常等。
	（2）过程：7*24 小时现场响应，重大节日如甲方需要，提供现场保障
	（3）服务期限，合同签订后 3 年。
★7×24，实时技术支持服务（现场服务）	对于报社的服务请求，整个服务过程有全程记录和跟踪，保证报社的每个服务请求都能够及时，高效的得到处理。如需现场服务，工程师应根据问题的紧急度按需及时到场服务。
★7×24 远程问题处理服务	接到网络或系统故障申报后，将首先进行远程故障分析与处理，及时排除故障。远程问题处理包括电话支持服务和远程接入服务。
设备迁移服务	需按照报社的需求在服务器期内对所维护的软硬件设备进行一次免费安装调试服务（包括硬件的迁移服务、软件的重新部署服务）。
★漏洞扫描服务	采用扫描工具对报社的信息系统进行安全扫描，发现漏洞，提供扫描报告，并根据扫描报告给出整改建议。包括：服务器、网络设备、安全设备和应用系统（每年 4 次，形成报告）。
系统安全加固	根据操作系统安全评估及漏洞扫描、安全检测、日志分析和配置检测中发现的问题，对服务器、网络设备、数据库系统等安全漏洞进行修补，加强安全配置、安全加固处理（根据漏洞扫描服务的结果每年 2-4 次）。
病毒监测、查杀及网络防病毒维护	定期对防病毒产品进行日志检查，定期对防病毒软件中出现的实施报警和定期扫描的报警信息进行监控和处理 。针对已感染系统，进行完整、系统的病毒查杀，并确保查杀效果满足网络要求（每年 12 次，每月不少于 1 次，形成报告）。
★运维巡检服务	网络设备、安全产品日常运维；网络及安全设备日志收集与分析；对网络病毒、蠕虫进行检测和查杀；服务器、操作系统及应用系统日志收集与分析（每年不少于 12 次，形成运维巡检报告）。
服务要求	签订合同后投标人需提供 3 年上门服务，并出具服务承诺函加盖公章。

3.2.3 交货方式、日期及地点

交货方式：工程设备货到现场，并通过最终验收，视为交货成功。

交货日期：合同生效后 20 天内。

交货地点：朝阳区东三环北路 19 号（中青大厦）

3.2.4 人员要求

要求投标人在项目实施时，需要至少固定 3 名项目实施人员

3.2.5 验收要求

（1）到货验收

在投标人将货物送到招标人指定地点后，双方应开箱检查产品的包装是否良好、数量是否正确，是否配件齐全、是否有合格证书，并由招标人签署产品签收证明。

（2）实施验收

招标人于设备安装调试完毕达到招标文件要求所需功能后 7 个工作日内完成产品初验，由招标人、投标人双方共同提供产品验收标准，产品符合要求，即为产品验收合格。初验完成产品试运行 1 个月，若产品运行正常，则由招标人、投标人双方共同签署项目终验报告，即为终验完成。终验后，投标人在质保期内仍需对货物的内在质量承担责任。

3.2.6 运输、保险及包装

（1）本项目的所有设备应包装坚固,以适合长途运输、多次搬运作业，并且投标人要根据设备的不同特性和要求采取防护措施，以防潮、雨、锈、震和腐蚀，保证其安全无损地到达安装现场。

由于包装不良所发生的损失，由于采用不充分或不妥善的防护措施而造成的任何货物毁损或丢失，由投标人承担赔偿责任。

（2）每包装箱内包含一份详细的装箱清单、产品说明书或使用手册。

（3）每包装箱上清楚写明箱号及设备接收人的详细地址、名称及发运人名称。

（4）设备包装费用、运输费用由投标人承担。

3.2.7 质量保证和技术支持服务

（1）质量保证：投标人承诺所提供的设备质量与其所提供的相关文件（包括但不限于产品说明书、产品保修单等文件）所宣称的质量一致。

（2）产品服务：投标人承诺为招标人提供免费 3 年原厂软件版本和硬件保修服务，服务期后投标人有责任继续为甲方提供软硬件维修、更换服务，并只收取成本费。

（3）相关技术支持服务：投标人承诺为招标人提供 7x24 小时技术支持热线、电子邮件及传真服务。在使用投标人提供的产品时如遇到问题时，招标人可拨打电话、发电子邮件或传真至投标人寻求帮助,投标人在收到邮件或传真后，须在 24 小时内进行答复，提供相关技术支持服务。招标人终生享受 7x24 小时技术支持热线服务。

（4）上门服务：投标人针承诺对本项目提供 3 年的 7*24 小时上门服务。

3.2.8 保密服务

投标人承诺对于招标人计算机网络应用系统相关的一切信息，包括但不限于：招标人网络系统软硬件的构成；运行状况与各种数据；安全测试结果等，永久保密。

3.2.9 技术培训要求

投标人应承诺项目实施结束后，需对甲方指定人员进行现场培训：包含但不限于产品使用培训。

第四部分　合同格式及主要条款

合同编号：

设备采购合同

签约日期：2019 年 X 月

签约地点：北京

销 售 合 同

本合同由以下双方经友好协商，本着平等互利的原则,于 2019 年 X 月于北京签订：

甲方：

地址：

法人代表：

联系人：

邮政编码：

联系电话：

传真号码：

乙方：

地址：

法人代表：

联系人：

邮政编码：

联系电话：

传真号码：

根据甲方实际需求与乙方订立本采购合同。

一、 **销售清单**

单位：元（人民币）

总报价如下：

XXX	
XXX	
XXX	
合计	

1.付款方式

合同总额为 XXXXX 即人民币：XXXXX（**大写**）

1.1 货物到现场安装就位，系统通过验收合格之日起 7 个工作日内，乙方须向甲方提供真实合法、等额正式的增值税专用发票，甲方在收到发票后的 7 日内以银行汇款、电汇等方式支付卖方合同金额的全部款项。

1.2 合同款项的付款日期以甲方支付款项的日期为准。甲方在每笔合同款项电汇后，视为甲方完成相应的付款义务。此日期即本合同第 7 条计算迟付货款违约金时间的根据。

甲方开票信息如下：

单位名称	
税号	
地址、电话	
开户行及账号	

乙方银行账号信息如下：

单位名称	
开户行及账号	

2.运输、保险及包装

2.1 本合同的所有工程设备应包装坚固,以适合长途运输、多次搬运作业，并且乙方要根据设备的不同特性和要求采取防护措施，以防潮、雨、锈、震和腐蚀，保证其安全无损地到达安装现场。由于包装不良所发生的损失，由于采用不充分或不妥善的防护措施而造成的任何货物毁损或丢失，乙方应负责赔偿由此而产生的一切损失。

2.2 每包装箱内包含一份详细的装箱清单，产品说明书和/或使用手册。

2.3 每包装箱上应清楚写明箱号及设备接收人的详细地址、名称及发运人名称。

2.4 工程设备包装费、运输费用由乙方承担

3.交货方式、日期及地点

交货方式：工程设备货到现场，并通过最终验收，视为交货成功。

交货日期：合同生效后_____ 天内。

交货地点：朝阳区东三环北路 19 号（中青大厦）

4.双方责任与义务

4.1 甲方责任：

4.1.1 甲方必须按时足额向乙方支付合同款项；

4.1.2 无不可抗力事件发生，甲方不得拒收乙方交付的符合合同约定质量标准的产品；

4.1.3 甲方必须如实提供最终用户信息；

最终用户：北京中青在线网络信息技术有限公司

4.2 乙方责任：

4.2.1 乙方必须按时完整地向甲方交付符合合同约定质量的产品；

4.2.2 乙方必须按本合同第 6 条约定向甲方提供技术支持；

5.验收

甲方购买乙方的产品应由乙方提供安装服务，在乙方将货物送到甲方指定地点后，双方应开箱检查产品的包装是否良好、数量是否正确，并由甲方签署产品签收证明。甲方应于设备安装调试完毕达到所需功能后 7 个工作日内完成产品初验，由甲乙双方共同提供产品验收标准，产品符合要求，即为产品验收合格。初验完成产品试运行 1 个月，若产品运行正常，则由甲乙双方共同签署项目终验报告，即为终验完成。终验后，乙方在质保期内仍需对货物的内在质量承担责任。

6.质量保证和技术支持服务

6.1 **质量保证：**乙方承诺所提供的工程设备质量与**其所提供的相关文件（包括但不限于产品说明书、产品保修单等文件）所宣称的质量一致；**

6.2 **产品服务：**乙方承诺为甲方提供免费 3 年原厂软件版本和硬件保修服务，服务期后乙方有责任继续为甲方提供软硬件维修、更换，并只收取成本费。

6.2.1 **7X24 小时产品技术热线服务:**甲方在使用乙方提供的产品时如遇到问题可终生享受乙方技术支持热线服务。

6.2.2 **电子邮件回复服务:**甲方对于网络监控问题，若当前产品不能提供具体控制措施，请发电子邮件至 ，在收到邮件后，乙方将在 24 小时内提供相关的技术支持。

6.2.3 **传真回复服务**:甲方可以将遇到的问题随时通过传真的方式提交给乙方的专门技术支持传真： ，并于 2 个工作日内得到答复。

6.2.4 **上门服务：乙方针对本项目提供 3 年的 7*24 小时上门服务。**

7.违约责任：

7.1 乙方需在签订合同后 1 个月内按照招标文件项目具体要求部分中的产品指标，在甲方指定地点进行现场测试，现场测试不通过的，甲方有权解除合同。乙方应向甲方支付合同总金额 10%的违约金。

7.2 甲方必须依照本合同支付货款，如逾期，每逾期一周（不足一周按一周计算）应向乙方支付合同总金额 4‰的违约金，但违约金累计总额不超过合同总金额的 10%。

7.3 乙方不能按期、按质交货，如逾期，每逾期一周（不足一周按一周计算），应向甲方支付合同总金额 4‰的违约金，但违约金累计总额不超过合同总金额的 10%。

7.4 乙方如违反本合同第 6 条（质量保证和技术支持服务）约定之义务，乙方应对此给甲方造成的损失进行赔偿。

7.5 若有特殊原因须单方面解除合同，应提前 30 日取得另一方的谅解及书面同意，否则，任何一方擅自解除合同，除应承担给对方所造成的经济损失外，还应赔偿对方相当于合同总金额 20%的违约金。

7.6 本合同自签订之日起具有法律效力，双方必须全面履行，因故变更时双方协商依法另立协议，若有违约，按合同违约条款处理。

7.7 其他责任参照《中华人民共和国合同法》及相关法律法规。

8.保密条款

8.1 保密内容：

指与甲方计算机网络应用系统相关的一切信息，包括但不限于：甲方网络系统软硬件的构成；运行状况与各种数据；安全测试结果等。以及乙方产品的技术、性能、合同价格等技术、商业秘密。

8.2 保密义务：

在双方合作期间及合作终止后，乙方有义务不向任何第三方披露本协议项下的保密信息内容。乙方承诺将上述保密信息的接触范围在乙方内部限制在指定范围内，并由严格的内控制度加以保证。未经甲方同意，乙方不得以任何方式复制保密信息，不得对甲方网络系统软件进行修改、改动、工程化、反汇编、改造成其他作品形式或进行分解。

8.3 对于双方信息，甲乙双方应该永久保密。

9.不可抗力

9.1 甲方或乙方因不可抗力迟延或不能履行其在本合同项下部分或全部义务的，不承担违约责任，但遭受不可抗力影响的一方应在通讯可能的条件下立即书面通知另一方，并提交不可抗力发生及持续的证明文件，同时及时采取措施减少因不可抗力造成的损失。

9.2 因一方迟延履行遭受不可抗力情形的，不适用本条，不能免责。

9.3 本合同所指不可抗力，是指本合同签订后发生的，不能预见、不能避免并且不能克服的客观情况，包括地震、自然灾害、战争、传染性疾病的蔓延等客观情况。

10.争议的解决：

凡因执行本合同所发生的争议，或与本合同有关的一切争议，双方应通过友好协商解决。如果协商不能解决，任何一方可向北京仲裁委员会申请仲裁。

11.其他：

本合同一式肆份，甲乙双方各执贰份，自双方签字盖章之日起生效。合同如有未尽事宜，须经双方共同协商，作出补充规定，补充规定与本合同具有同等效力。

甲方： 乙方：

法人代表：（签字）：

甲方（盖章）

日 期：

法人代表：（签字）：

乙方（盖章）

日 期：

第五部分　投标文件内容及式样

标注正本
或副本

中国青年报社中青大厦办公区网络建设二期项目

投 标 文 件

采购编号：HXJC2019HG/090

投标人名称：_____（盖章）

法定代表人或其委托代理人：_____（签字）

日　　期：____年__月__日

5.1 资格审查证明文件

5.1.1 营业执照副本复印件或法人证书复印件并加盖投标人公章

5.1.2 税务登记证书复印件并加盖投标人公章（依据国家有关规定取消税务登记证书的投标人可不提供）

5.1.3 投标截止日前 6 个月内任意一期缴纳增值税或企业所得税的凭据复印件并加盖投标人公章

5.1.4 投标截止日前 6 个月内任意一期缴纳社会保险的凭据复印件并加盖投标人公章

5.1.5 近三年度(2016 年、2017 年、2018 年)会计师事务所出具的年度财务审计报告复印件并加盖投标人公章，或近三年度(2016 年、2017 年、2018 年)资产负债表和损益表（利润表）复印件并加盖投标人公章；若投标人为本年度新成立企业，仅需提供最近一期资产负债表和损益表

5.1.6 投标截止日前三年内无重大违法行为的声明书

声 明 书

致招标人、招标代理机构：

我公司在参加本次招标采购活动前，做出以下郑重声明：

一、参加本次政府采购活动前三年内，在经营活动中没有重大违法记录。

二、在本次政府采购活动前三年内，我公司在中国政府采购网等政府采购信息发布平台及当地工商局企业信用查询系统中，无任何重大违法记录。

若发现我方上述声明与事实不符，愿按照政府采购相关规定接受相关处罚。

特此声明。

投标人名称（盖章）：_____

法定代表人或授权代表签字：_____

日　期：____年__月__日

5.2 符合性审查证明文件

5.2.1 投标函式样

投 标 函

致招标人、招标代理机构：

*投标人名称*授权下述签字人*姓名、职务或职称*为全权代表，参加贵方组织的中国青年报社中青大厦办公区网络建设二期项目（采购编号：HXJC2019HG/090）招标的有关活动。

在此，签字代表宣布：

1. 我方提交投标文件正本 1 份、副本 4 份及电子文件（U 盘）1 份。

2. 我方提交单独密封的开标一览表 1 份。

3. 开标一览表中的报价为我方要求的合理报酬，没有特殊理由不予以变更。

4. 我方保证递交的所有文件是真实的、准确的，符合本项目招标公告和招标文件对投标人的资格要求。

5. 我方完全理解招标文件的全部条款，并同意放弃对这方面有不明及误解的权力。

6. 我方承诺本投标文件的有效期为自开标日起 90 个日历日。

7. 我方同意按照贵方可能要求提供与此次投标有关的一切数据或资料，完全理解评标委员会不以最低投标报价作为定标依据。

8. 若我方中标，保证按照投标文件履行合同责任和义务。

9. 与本投标有关的一切正式往来信函请寄：

地址：_____

邮编：_____ 电话（办公室）：_____

移动电话：_____ 传真：_____

电子邮箱：_____

投标人名称(盖章)：_____

法定代表人或授权代表(签字)：_____

日 期：____年___月___日

5.2.2 开标一览表式样

开标一览表

项目名称：中国青年报社中青大厦办公区网络建设二期项目

采购编号：HXJC2019HG/090

投标人名称	投标报价 （元）	供货期	质保期 （年）	其他投标声明 （若有）
	小写： **大写：**	合同签订后_____。		

注：

1．此表内容在开标时当众宣读。

2．此表除在正本、副本中提交外，还应单独密封一份在信封内，信封上注明“开标一览表”字样，投标时递交。法定代表人或授权代表应在包装封口处签字并加盖投标人公章。

投标人名称（盖章）：_____

法定代表人或授权代表签字：_____

日　期：____年__月__日

5.2.3 投标报价明细表式样

投标报价明细表

项目名称：中国青年报社中青大厦办公区网络建设二期项目

采购编号：HXJC2019HG/090

序号	报价内容	制造商名称	品牌型号	产地	单位	数量	单价	小计	测算说明
1	……								
2									
3									
4									
	总计								

投标人名称（盖章）：_____

法定代表人或授权代表（签字）：_____

日　期：_____年___月___日

注：

1.此表可拓展，未按要求提供该表的将视为没有实质性响应招标文件。

2.所有价格系用人民币表示。

3.对于投标人免费提供的项目，投标人要先填写该项目的实际价格，在旁边注明免费及此项不计入总价或合计价。

5.2.4 商务条款偏离表式样

商务条款偏离表

项目名称：中国青年报社中青大厦办公区网络建设二期项目

采购编号：HXJC2019HG/090

序号	招标文件条款号	商务条款要求	投标应答	偏离说明

我方确认，除上述偏离外，完全接受招标文件中的其他商务条款。

投标人名称（盖章）：_____

法定代表人或授权代表签字：_____

日　期：____年__月__日

注：

1.此表只需列明有偏离的商务条款。

2.有偏离的商务条款须在该表中逐一列明，并在“投标应答”栏填写具体应答内容，在“偏离说明”中说明偏离具体情形。若无偏离请在“投标应答”中填写“无偏离”。

3.未声明部分将被视为已接受招标文件要求，签约时未经招标人同意不得改变。

4.投标人可根据其投标内容进一步细化上述表格，并可增添其它表格或说明以便进一步明确投标内容。

5.2.5 技术条款偏离表式样

技术条款偏离表

项目名称：中国青年报社中青大厦办公区网络建设二期项目

采购编号：HXJC2019HG/090

序号	招标文件条款号	技术条款要求	投标应答	偏离说明

我方确认，除上述偏离外，完全接受招标文件中的其他技术条款。

投标人名称（盖章）：_____

法定代表人或授权代表签字：_____

日　期：____年__月__日

注：

1.**此表需对本招标文件“3.2.2 设备及服务技术指标要求”技术条款逐项应答**。

2.有偏离的技术条款须在“投标应答”栏填写“有偏离”，在“偏离说明”中辅以详细解释。若无偏离请在“投标应答”中填写“无偏离”。

3.未声明部分将被视为已接受招标文件要求，签约时未经招标人同意不得改变。

.投标人可根据其投标内容进一步细化上述表格，并可增添其它表格或说明以便进一步明确投标内容。

5.2.6 支付代理服务费承诺函式样

支付代理服务费承诺函

致：北京华夏京诚咨询有限公司

我单位在贵公司组织的**中国青年报社中青大厦办公区网络建设二期项目（采购编号：HXJC2019HG/090）**招标中若中标，保证按招标文件的要求支付代理服务费。

特此承诺！

承诺方全称（盖章）：_____

地址：_____

电话：_____传真：_____

电邮：_____邮编：_____

承诺方授权代表签字：_____

日　期：____年__月__日

附：开票信息

（以下两项信息勾选一项并按要求填写）

□我单位为小规模纳税人，如获中标，请在我单位支付代理服务费后，按以下信息开具增值税普通发票：

付款单位名称：_____

纳税人识别号：_____

□我单位为一般纳税人，如获中标，请在我单位支付代理服务费后，按以下信息开具增值税专用发票：

付款单位名称：_____

纳税人识别号：_____

地　址：_____

电　话：_____

开户行全称：_____

账　号：_____

以上信息真实有效，如我单位相关信息在此期间内发生变更，我单位负责及时通知贵公司。由于填写错误、不清晰、我单位信息变更未及时告知贵公司而引起的开票延误等后果由我单位自行承担。

（注：投标人公章请勿加盖在银行账号上。）

5.2.7 法定代表人资格证明书式样

法定代表人资格证明书

投标人名称：_____

单位性质：_____

地　　址：_____

成立时间：_____ 年_____ 月_____ 日

经营期限：_____

姓名：_____ 性别：_____ 年龄：_____职务：_____

系_____（投标人名称）的法定代表人。

特此证明。

（须附法定代表人身份证件复印件）

投标人名称（盖章）：_____

日期：____年__月__日

注：此证明书除在正本、副本中提交外，还应在投标时单独递交 1 份原件。

5.2.8 法定代表人授权委托书式样

（如果法定代表人不能参加投标的，应提供法定代表人授权委托书和法定代表人资格证明书）

法定代表人授权委托书

本人_____（姓名）系_____（投标人名称）的法定代表人，现委托____（姓名）为我方代理人。代理人根据授权，以我方名义签署、澄清、说明、补正、递交、撤回、修改**中国青年报社中青大厦办公区网络建设二期项目（采购编号：HXJC2019HG/090）**投标文件、签订合同和处理有关事宜，其法律后果由我方承担。

本授权委托书自授权之日起生效。代理人无转委托权。代理人无转委托权。

（须附授权代表身份证件复印件）

投标人名称（盖章）：_____

法定代表人（签字或盖章）：_____

身份证号码：_____

授权代表（签字）：_____

身份证号码：_____

日期：____年__月__日

注：此委托书除在正本、副本中提交外，还应在投标时单独递交 1 份原件。

5.2.9 投标人基本情况表式样

投标人基本情况表

1．名称及概况：

（1）投标人名称：_____

（2）地址：_____

传真/电话号码：_____邮政编码：_____

（3）成立和/或注册日期：_____

（4）实收资本：_____

（5）开立基本账户银行的名称、地址、账号、税号：

_____

_____

2．针对本项目提供的人员情况：

姓名	职务	学历	职称	本项目中承担工作	从事过的同类项目及承担工作

注：须提供学历及执业资格、职称证明等相关复印件（加盖单位公章）

3．针对本项目提供的设备、设施情况（根据项目具体情况酌情提供）：

主要设备、设施名称	型号规格	数量	技术参数

4．近三年的营业额

年度	国内	国外	盈亏情况
2016			□盈利 □亏损
2017			□盈利 □亏损
2018			□盈利 □亏损

5．质量认证、行业资质等相关认证情况：

_____

_____

6．其他情况：

（组织机构、技术力量等）_____

兹证明上述声明是真实、正确的，并提供了全部能提供的资料和数据，我们同意遵照贵方要求出示有关证明文件。

投标人名称（盖章）：_____

法定代表人或授权代表签字：_____

日　期：____年__月__日

5.2.10 近三年同类业绩情况及证明材料

近三年同类业绩情况表

项目名称	委托单位	合同金额（万元）	委托日期
备注			

注：

1.同类业绩是指近三年投标人独立完成的项目，是否属于同类业绩由评标委员会根据投标人提供的业绩资料确定。

2.近三年指 2016 年 1 月 1 日（以签约时间为准）至投标截止日期前。

3.此表后须附同类项目业绩的合同协议书复印件等证明材料，合同协议书复印件必须具有与用户签订的合同首页、标的页、合同金额所在页及签字盖章页复印件作为证明。

4. 有效的证明材料应逐页加盖投标人公章。

5.2.11 其他需要说明的事宜

5.3 技术响应文件

（根据招标文件第二部分“2.3.2.3 条款”的要求编制，格式可自拟）

5.4 投标文件包装封面

5.4.1 投标文件包装封面式样

采购编号: HXJC2019HG/090

项目名称: 中国青年报社中青大厦办公区网络建设二期项目

投 标 文 件

（于 2019 年 月 日 时 分前不得启封）

投标人名称（盖章）:

通讯地址: 邮政编码:

注:

1. 正本、副本、电子文件 U 盘合并封装递交。
2. 法定代表人或授权代表应在包装封口处签字并加盖公章。

5.4.2 开标一览表信封封面式样

采购编号: HXJC2019HG/090

项目名称: 中国青年报社中青大厦办公区网络建设二期项目

开标一览表

（于 2019 年 月 日 时 分前不得启封）

投标人名称（盖章）:

通讯地址: 邮政编码:

注:

1. 开标一览表单独封装递交。
2. 法定代表人或授权代表应在包装封口处签字并加盖公章。