采购编号：jsjzcg24-00040481

金山区政务外网租赁服务项目

招 标 文 件

采购人：上海市金山区行政服务中心

集中采购机构：上海市金山区政府采购中心

编制日期：2024-04-03

目　录

第一章 招标公告

一、项目基本情况

1、项目编号：**3101160002402221667 41-16074942**

2、项目名称：金山区政务外网租赁服务项目

3、预算资金：620 万元。

4、最高限价：本项目采购预算为 620 万元人民币。**超过最高限价的投标不予接受**。

5、项目主要内容、数量及简要规格描述或项目基本概况介绍：本项目主要针对金山区政务外网租赁服务进行招标工作。**具体项目内容、采购范围及所应达到的具体要求，以招标文件相应规定为准**。

6、服务期限：2024 年 6 月 1 日起至 2027 年 5 月 31 日。（本项目采用一次招标，三年沿用，合同一年一签的方式实施。采购人每年对中标供应商进行考核，考核合格、服务满意续签第二、第三年服务合同；若考核不合格、服务不满意，采购人有权终止服务合同，不再续签下一年的服务合同。）

7、服务地点：采购人指定地点。

8、本次招标不接受联合投标

9、代理机构内部编号：jsjzcg24-00040481

二、申请人资格要求

1、满足《中华人民共和国政府采购法》第二十二条规定；

2、落实政府采购政策需满足的资格要求；促进中小企业、监狱企业、残疾人福利性单位发展。

3、其他资质要求：

3.1 本项目面向大、中、小、微型等各类供应商采购；

3.2 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；

三、招标文件的获取

1、时间：**2024-04-03** 至 **2024-04-12** 每天上午 **00:00:00~12:00:00**，下午 **12:00:00~23:59:59**（北京时间，法定节假日除外）

2、地点：上海市政府采购网（http://www. zfcg.sh.gov.cn）

3、方式：网上获取

4、售价：0 元

5、凡愿参加投标的合格投标人应在上述规定的时间内按照规定获取招标文件，逾期不再办理。未按规定获取招标文件的投标将被拒绝。

四、提交投标文件截止时间、开标时间和地点

1、提交投标文件截止时间、开标时间：**2024-04-24 09:30:00**（北京时间）

2、开标地点：上海政府采购网（http://www.zfcg.sh.gov.cn）电子招投标系统远程开标

投标人使用数字证书（CA 证书）登录上海政府采购网（http://www.zfcg.sh.gov.cn）电子招投标系统，进入选定招标项目的虚拟开标室进行开标，投标人代表须于发起开标后 30 分钟内在虚拟开标室签到，在规定时间内未签到或签到失败的视为逾期送达，招标人将拒绝接收。

五、公告期限

自本公告发布之日起 5 个工作日

六、其他补充事宜

1、电子投标文件按电子招标系统设置要求。

2、参与本项目的供应商不需要到现场，项目为全程线上开标。

★3、纸质投标文件等材料递交

（1）递交时间：开标时间、投标截止时间（**2024-04-24 09:30:00**）前递交纸质投标文件（正本壹份，副本贰份）、无疑问回复函（原件）、法人委托授权书（原件）、被委托人身份证（复印件），密封包装备用（以网上递交的投标文件为准）。

（2）提交地址：上海市金山区金山大道 2000 号八号楼　上海市金山区政府采购中心门卫室

（3）提交方式：快递等。

4、投标人应在投标截止时间前尽早加密上传投标文件，以免因临近投标截止时间上传造成招标人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。

七、联系方式

1、采购人

采购人：上海市金山区行政服务中心

地址：上海市金山区龙山路 555 号

项目联系人：郑政

联系方式：021-57921546

2、采购代理机构

采购代理机构：上海市金山区政府采购中心

地址：上海市金山区金山大道 2000 号八号楼

项目联系人：张磊

联系方式：021-57921927

第二章 投标须知

前附（置）表

一、项目情况

1、项目名称：金山区政务外网租赁服务项目

2、采购编号：jsjzcg24-00040481

3、服务地点：采购人指定地点。

4、项目主要内容、数量及简要规格描述或项目基本概况介绍：本项目主要针对金山区政务外网租赁服务进行招标工作。**具体项目内容、采购范围及所应达到的具体要求，以招标文件相应规定为准**。

5、服务期限：2024 年 6 月 1 日起至 2027 年 5 月 31 日。（本项目采用一次招标，三年沿用，合同一年一签的方式实施。采购人每年对中标供应商进行考核，考核合格、服务满意续签第二、第三年服务合同；若考核不合格、服务不满意，采购人有权终止服务合同，不再续签下一年的服务合同。）

二、招标人

1、采购人

采购人：上海市金山区行政服务中心

地址：上海市金山区龙山路 555 号

项目联系人：郑政

联系方式：021-57921546

2、采购代理机构

采购代理机构：上海市金山区政府采购中心

地址：上海市金山区金山大道 2000 号八号楼

项目联系人：张磊

联系方式：021-57921927

三、申请人资格要求

1、满足《中华人民共和国政府采购法》第二十二条规定；

2、落实政府采购政策需满足的资格要求；促进中小企业、监狱企业、残疾人福利性单位发展。

3、其他资质要求：

3.1 本项目面向大、中、小、微型等各类供应商采购；

3.2 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；

四、招标有关事项

1、采购答疑会：不召开

1.1 要求对采购文件进行澄清的投标人均应在投标截止期 15 天以前，以书面形式通知采购人。

1.2 澄清文件通过“上海政府采购网”上发布，请供应商关注。

1.3 澄清仅此一次，逾期不再组织。

2、踏勘现场：不组织，投标人自行前往，踏勘现场。

3、投标有效期：90 天

4、投标保证金：本项目不收取投标保证金。

5、投标截止时间：详见采购邀请（采购公告）或延期公告（如有）

6、递交投标文件方式和网址

6.1 投标方式：由投标人在上海市政府采购信息管理平台的门户网站上海政府采购网（简称：电子采购平台）电子招投标系统提交。

6.2 投标网址：http://www.zfcg.sh.gov.cn

7、开标时间和开标地点：

7.1 开标时间：同投标截止时间

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

7.3 开标网址：上海市政府采购信息管理平台的门户网站上海政府采购网（简称：电子采购平台）电子招投标系统(网址：http://www.zfcg.sh.gov.cn)

8、评标委员会的组建：评标委员会由随机抽取构成：_5_人，其中采购人代表_1_人，专家_4_人；

9、评标方法：详见第五章

中标人推荐办法：采购人将根据评标委员会推荐的中标候选人及排序情况，依法确认本采购项目的中标人。

五、其它事项

1、付款方法：合同签订后支付合同价的 30%，项目建设完成后初验通过后支付 40%，一年整体运维验收通过后支付剩余 30%。

2、质量标准：按双方合同约定。

六、说明

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：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的“在线服务”专栏的有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，以免因临近投标截止时间上传造成招标人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。

投标须知

一. 总则

1 概述

1.1 根据《中华人民共和国政府采购法》、《中华人民共和国招标投标法》等有关法律、法规和规章的规定，本采购项目已具备采购条件。

1.2 本采购文件仅适用于《投标邀请》和《投标人须知》前附表中所述采购项目的招标采购。

1.3 采购文件的解释权属于《投标邀请》和《投标人须知》前附表中所述的采购人。

1.4 参与招标投标活动的所有各方，对在参与招标投标过程中获悉的国家、商业和技术秘密以及其它依法应当保密的内容，均负有保密义务，违者应对由此造成的后果承担全部法律责任。

1.5 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（网址：www.zfcg.sh.gov.cn）电子招投标系统进行。

2 定义

2.1“采购项目”系指《投标人须知》前附表中所述的采购项目。

2.2“服务”系指招标文件规定的投标人为完成采购项目所需承担的全部义务。

2.3“招标人”系指《投标人须知》前附表中所述的组织本次招标的集中采购机构和采购人。

2.4“投标人”系指从招标人处按规定获取招标文件，并按照招标文件向招标人提交投标文件的供应商。

2.5“中标人”系指中标的投标人。

2.6 “甲方”系指采购人

2.7“乙方”系指中标并向采购人提供服务的投标人。

2.8 招标文件中凡标有“★”的条款均系实质性要求条款。

2.9“电子采购平台”系指上海市政府采购信息管理平台的门户网站上海政府采购网（www.zfcg.sh.gov.cn）。是由市财政局建设和维护。

3 合格的投标人

3.1 符合《投标邀请》和《投标人须知》前附（置）表中规定的合格投标人所必须具备的资质条件和特定条件。

3.2《投标邀请》和《投标人须知》前附（置）表中规定接受联合体投标的，除应符合本章第 3.1 项要求外，还应遵守以下规定：

（1）联合体各方应按采购文件提供的格式签订联合体协议书，明确主投标人和各方权利义务；

（2）由同一专业的供应商组成的联合体，按照资质等级较低的供应商确定联合体资质等级；

（3）采购人根据采购项目的特殊要求规定投标人特定条件的，联合体各方中至少应当有一方符合采购规定的特定条件；

（4）联合体各方不得再以自己名义单独或参加其他联合体在同一采购项目中投标。

4 合格的服务

4.1 投标人所提供的服务应当没有侵犯任何第三方的知识产权、技术秘密等合法权利。

4.2 投标人提供的服务应当符合采购文件的要求，并且其质量完全符合国家标准、行业标准或地方标准。

5 投标费用

不论投标的结果如何，投标人均应自行承担所有与投标有关的全部费用，采购人在任何情况下均无义务和责任承担这些费用。

6 信息发布

本采购项目需要公开的有关信息，包括采购公告、采购文件澄清或修改公告、中标结果公示、未中标通知以及延长投标截止时间等与采购活动有关的通知，采购人均将通过“上海政府采购网”（http://www. zfcg. sh.gov.cn）公开发布。投标人在参与本采购项目招投标活动期间，请及时关注以上媒体上的相关信息，投标人因没有及时关注而未能如期获取相关信息，是投标人的风险，采购人对此不承担任何责任。

7 询问与质疑

7.1 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。

7.2 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，应当在其下载招标文件之日（以电子采购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。

7.3 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。

7.4 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。

7.5 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）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 7.3 条和第 7.4 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。

质疑函的递交应当采取当面递交形式。

7.6 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。

7.7 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。

8 公平竞争和诚实信用★

8.1 投标人在本招标项目的竞争中应自觉遵循公平竞争和诚实信用原则，不得存在腐败、欺诈或其他严重违背公平竞争和诚实信用原则、扰乱政府采购正常秩序的行为。“腐败行为”是指提供、给予任何有价值的东西来影响采购人员在采购过程或合同实施过程中的行为；“欺诈行为”是指为了影响采购过程或合同实施过程而提供虚假材料，谎报、隐瞒事实的行为，包括投标人之间串通投标等。

8.2 如果有证据表明投标人在本招标项目的竞争中存在腐败、欺诈或其他严重违背公平竞争和诚实信用原则、扰乱政府采购正常秩序的行为，招标人将拒绝其投标，并将报告政府采购监管部门查处；中标后发现的，中标人须参照《中华人民共和国消费者权益保护法》第55条之条文描述方式双倍赔偿采购人，且民事赔偿并不免除违法投标人的行政与刑事责任。

8.3 招标人将在**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。以上信用查询记录，招标人将打印查询结果页面后与其他采购文件一并保存。

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。

9 其他

本《投标人须知》的条款如与《投标邀请(采购公告)》、《项目采购需求》和《评标办法》就同一内容的表述不一致的，以《投标邀请》、《项目采购需求》和《评标办法》中规定的内容为准。

二. 采购文件

10 采购文件构成

10.1 采购文件由以下部分组成：

（1）投标邀请（采购公告）；

（2）投标人须知；

（3）政府采购政策功能；

（4）项目采购需求；

（5）评标办法；

（6）投标文件有关格式；

（7）合同格式

（8）本项目采购文件的澄清、答复、修改、补充内容（如有的话）。

10.2 投标人应仔细阅读采购文件的所有内容，并按照采购文件的要求提交投标文件。如果投标人没有按照采购文件要求提交全部资料，或者投标文件没有对采购文件在各方面作出实质性响应，则投标有可能被认定为无效标，其风险由投标人自行承担。

10.3 投标人应认真了解本次采购的具体工作要求、工作范围以及职责，了解一切可能影响投标报价的资料。一经中标，不得以不完全了解项目要求、项目情况等为借口而提出额外补偿等要求，否则，由此引起的一切后果由中标人负责。

10.4 投标人应按照采购文件规定的日程安排，准时参加项目招投标有关活动。

11 采购文件的澄清和修改

11.1 任何要求对采购文件进行澄清的投标人，均应在投标截止期 15 天以前，按《投标邀请》中的地址以书面形式（必须加盖投标人单位公章）通知采购人。

11.2 对在投标截止期 15 天以前收到的澄清要求，采购人需要对采购文件进行澄清、答复的；或者在投标截止前的任何时候，采购人需要对采购文件进行补充或修改的，采购人将会通过“上海政府采购网”以澄清或修改公告形式发布,并通过电子采购平台发送至已下载采购文件的供应商工作区。如果澄清或修改公告发布时间距投标截止时间不足 15 天的，则相应延长投标截止时间。延长后的具体投标截止时间以最后发布的澄清或修改公告中的规定为准。

11.3 澄清或修改公告的内容为采购文件的组成部分。当采购文件与澄清或修改公告就同一内容的表述不一致时，以最后发出的文件内容为准。

11.4 采购文件的澄清、答复、修改或补充都应由集中采购机构以澄清或修改公告形式发

布，除此以外的其他任何澄清、修改方式及澄清、修改内容均属无效，不得作为投标的依据，否则，由此导致的风险由投标人自行承担，采购人不承担任何责任。

11.5 采购人召开答疑会的，所有投标人应根据采购文件或者采购人通知的要求参加答疑会。投标人如不参加，其风险由投标人自行承担，采购人不承担任何责任。

12 踏勘现场

12.1 招标人组织踏勘现场的，所有投标人应按《投标人须知》前附表规定的时间、地点前往参加踏勘现场活动。投标人如不参加，其风险由投标人自行承担，招标人不承担任何责任。招标人不组织踏勘现场的，投标人可以自行决定是否踏勘现场，投标人需要踏勘现场的，招标人应为投标人踏勘现场提供一定方便，投标人进行现场踏勘时应当服从招标人的安排。

12.2 投标人踏勘现场发生的费用由其自理。

12.3 招标人在现场介绍情况时，应当公平、公正、客观，不带任何倾向性或误导性。

12.4 招标人在踏勘现场中口头介绍的情况，除招标人事后形成书面记录、并以澄清或修改公告的形式发布、构成招标文件的组成部分以外，其他内容仅供投标人在编制投标文件时参考，招标人不对投标人据此作出的判断和决策负责。

三. 投标文件

13 投标文件的构成

13.1 投标文件由商务响应文件（包括相关证明文件）和技术响应文件二部分构成。

13.2 商务响应文件（包括相关证明文件）和技术响应文件应具体包含的内容，以第四章《招标需求》规定为准。

14 投标的语言及计量单位

14.1 投标人提交的投标文件以及投标人与采购人就有关投标事宜的所有来往书面文件均应使用中文。除签名、盖章、专用名称等特殊情形外，以中文以外的文字表述的投标文件视同未提供。

14.2 投标计量单位，采购文件已有明确规定的，使用采购文件规定的计量单位；采购文件没有规定的，一律采用中华人民共和国法定计量单位（货币单位：人民币元）

15 投标有效期

15.1 投标文件应从开标之日起，在《投标须知前附表》规定的投标有效期内有效。投标有效期比采购文件规定短的属于非实质性响应，将被认定为**无效投标**。

15.2 在特殊情况下，在原投标有效期期满之前，采购人可书面征求投标人同意延长投标有效期。投标人可拒绝接受延期要求而不会导致投标保证金被没收。同意延长有效期的投标人需要相应延长投标保证金的有效期，但不能修改投标文件。

15.3 中标人的投标书作为项目合同的附件，其有效期至中标人全部合同义务履行完毕为止。

16 商务响应文件

16.1 商务响应文件由以下部分组成：

（1）投标函；

（2）资格条件响应表；

（3）实质性要求响应表；

（4）开标一览表（以电子采购平台设定为准）；

（5）商务响应表；

（6）相关证明文件（投标人应按照《招标需求》所规定的内容提交相关证明文件，以证明其有资格参加投标和中标后有能力履行合同）；

（7）投标人关于报价等的其他说明（如有的话）。

17 投标函

17.1 投标人应按照采购文件中提供的格式完整地填写《投标函》。

17.2 投标人不按照采购文件中提供的格式填写《投标函》，或者填写不完整的，评标时将按照第五章《评标办法》中的相关规定予以扣分。

17.3 投标文件中未提供《投标函》的，为**无效投标**。

18 开标一览表

18.1 投标人应按照采购文件和电子采购平台电子招投标系统提供的投标文件格式完整地填写开标一览表、报价明细表和报价构成表等，说明其拟提供货物名称及型号、品牌、数量、单位、质量保证期、交付期等。

18.2 开标一览表是为了便于采购人开标，开标一览表内容在开标时将当众公布。开标一

览表的内容应与投标报价明细表内容一致，不一致时以开标一览表内容为准。

18.3 投标人未按照招标文件的要求和电子采购平台电子招投标系统提供的投标文件格式完整地填写《开标一览表》、或者未提供《开标一览表》，导致其开标不成功的，其责任和风险由投标人自行承担。

19 投标报价

19.1 投标报价是履行合同的最终价格，除《项目采购需求》中另有说明外，投标报价应包括投标人为完成采购项目而提供服务的一切费用，包括投标人的各种成本、税金、管理费和利润。

19.2 投标人应按照采购文件和电子采购平台电子招投标系统提供的投标文件格式完整地填写开标一览表、报价明细表和报价构成表等，说明其拟提供服务的内容、数量、价格、时间、价格构成等。

19.3 除《项目采购需求》中说明并允许外，投标的每一种服务的单项报价以及采购项目的投标总价均只允许有一个报价，任何有选择的报价，采购人均将予以拒绝。

19.4 投标报价应是固定不变的，不得以任何理由予以变更。任何可变的或者附有条件的投标报价，采购人均将予以拒绝。

19.5 投标应以人民币报价。

20 资格条件及实质性要求响应表

投标人应当按照采购文件所提供格式，逐项填写并提交《资格条件及实质性要求响应表》，以证明其投标符合采购文件规定的所有合格投标人资格条件及实质性要求。

21 与评标有关的投标文件主要内容索引表

21.1 投标人应按照采购文件提供的格式完整地填写与评标有关的投标文件主要内容索引表。

21.2 与评标有关的投标文件主要内容索引表是为了便于评标。与评标有关的投标文件主要内容索引表与投标文件其他部分就同一内容的表述应当一致，不一致时以索引表内容为准。

22 技术响应文件

22.1 投标人应按照《项目采购需求》的要求编制并提交技术响应文件，对采购人的需求

全面完整地做出响应并编制服务方案，以证明其投标的服务符合采购文件规定。

22.2 技术响应文件可以是文字资料、表格、图纸和数据等各项资料，其内容应包括但不限于人力、物力等资源的投入以及服务内容、方式、手段、措施、质量保证及建议等。

23 相关证明文件

23.1 投标人应按照《项目采购需求》所规定的内容提交相关证明文件，以证明其有资格参加投标和中标后有能力履行合同。

24 投标保证金

24.1 投标保证金：本项目不收取投标保证金。

25 投标文件的编制和签署

25.1 投标人应按照采购文件和电子采购平台电子招投标系统要求的格式填写相关内容。

25.2 投标文件中凡采购文件要求签署、盖章之处，均应由投标人的法定代表人或法定代表人正式授权的代表签署和加盖公章。投标人应写明全称。如果是由法定代表人授权代表签署投标文件，则必须按采购文件提供的格式出具《法定代表人授权书》并将其附在投标文件中。投标文件若有修改错漏之处，须加盖投标人公章或者由法定代表人或法定代表人授权代表签字或盖章。投标文件因字迹潦草或表达不清所引起的后果由投标人自负。

25.3 投标人应按采购文件和电子采购平台电子招投标系统规定的内容、格式和顺序编制投标文件。凡采购文件提供有相应格式的，投标文件均应完整的按照采购文件提供的格式打印、填写并按要求在电子采购平台电子招投标系统上传。投标文件内容不完整、格式不符合导致投标文件被误读、漏读或者查找不到相关内容的，是投标人的责任，投标人需承担其投标在评标时因此被扣分甚至被认定为无效标的风险。

25.4 建设节约型社会是我国落实科学发展观的一项重大决策，也是政府采购应尽的义务和职责，需要政府采购各方当事人在采购活动中共同践行。目前，少数投标人制作的投标文件存在编写繁琐、内容重复的问题，既增加了制作成本，浪费了宝贵的资源，也增加了评审成本，影响了评审效率。为进一步落实建设节约型社会的要求，提请投标人在制作投标文件时注意下列事项：

（1）评标委员会主要是依据投标文件中技术、质量以及售后服务等指标来进行评定。因此，投标文件应根据采购文件的要求进行制作，内容简洁明了，编排合理有序，与采购文件内容无关或不符合采购文件要求的资料不要编入投标文件。

（2）投标文件应规范，应按照规定格式要求规范填写，扫描文件应清晰简洁、上传文

件应规范。

25.5 纸质投标文件

（1）投标人还应准备一份纸质投标文件正本和《投标人须知》前附表规定份数的副本。每份纸质投标文件封面上须清楚地标明“正本”或“副本”字样，正本和副本不符时以正本为准。

（2）纸质投标文件的正本需打印或用不褪色的墨水填写，投标文件正本除《投标人须知》中规定可提供复印件的以外均须提供原件。副本可以打印或用不褪色的墨水填写，也可以采用正本的完整复印件。

（3）纸质的投标文件纸张、封面和装订应力求简洁，不宜追求豪华装帧。

26 投标文件编制的响应性

26.1 投标人应按本网上投标系统规定的内容、格式和顺序编制投标文件。凡采购文件提供有格式的，投标文件均应完整的按照采购文件提供的格式打印、填写并按要求在网上投标系统上传。投标文件内容不完整、格式不符合导致投标文件被误读、漏读或者查找不到相关内容的，是投标人的责任，投标人需承担其投标在评标时因此被扣分甚至被认定为无效标的风险。

四 投标文件的递交

27 投标文件的的递交

27.1 投标人应在网上招标系统中按照要求填写和上传所有投标内容，并通过数字认证证书（CA 证书）加密方式提交投标文件，同时下载投标成功的投标回执。

27.2 投标人应充分考虑到期间网上投标会发生的故障和风险。对发生的任何故障和风险造成投标人内容不一致或利益受损或投标失败的，采购人不承担任何责任。

27.3 投标人还应提交将纸质投标文件正本和所有的副本，纸质的投标文件是为了便于采购人评标时使用，纸质投标文件的内容应与上传所有投标内容一致，不一致时以上传所有投标内为准。

28 投标截止时间

28.1 投标人必须在《投标邀请（采购公告）》规定的网上投标截止时间前将投标文件在电子采购平台电子招投标系统中上传并正式投标。

28.2 在采购人按《投标人须知》规定酌情延长投标截止期的情况下，采购人和投标人受

投标截止期制约的所有权利和义务均应延长至新的截止时间。

28.3 在投标截止时间后上传的任何投标文件，采购人均将拒绝接收。

28.4 投标人必须在《投标须知》前附表规定的投标截止时间前将纸质的投标文件送达《投标须知》前附表中规定的投标地点。

29 投标文件的修改与撤回

在投标截止时间之前，投标人可以对在电子采购平台电子招投标系统已提交的投标文件进行修改和撤回。有关事项应根据电子采购平台规定的要求办理。

五 开标

30 开标

30.1 采购人将按《投标邀请》或《延期公告》（如果有的话）中规定的时间和**地点**在电子采购平台上组织公开开标。

30.2 开标程序在电子采购平台进行，所有上传投标文件的供应商应登录电子采购平台参加开标。

30.3 投标截止，电子采购平台显示开标后，投标人进行签到操作，投标人签到完成后，由采购人解除电子采购平台对投标文件的加密。投标人应在规定时间内使用数字证书对其投标文件解密。投标人因自身原因未能签到或未能将其投标文件解密的，视为放弃投标。

30.4 投标文件解密后，电子采购平台根据投标文件中开标一览表的内容自动汇总生成开标记录表。

投标人应及时检查开标记录表的数据是否与其投标文件中的投标报价一览表一致，并作出确认。投标人因自身原因未作出确认的视为其确认开标记录表内容。投标人发现开标记录表与其投标文件开标一览表数据不一致的，应及时向开标人提出更正，开标人应核实开标记录表与投标文件中的开标一览表内容。

六 评标

31 评标委员会

31.1 采购人将依法组建评标委员会，评标委员会由采购人的代表和上海市政府采购评审专家组成，其中专家的人数不少于评标委员会成员总数的三分之二。

31.2 评标委员会负责对投标文件进行评审和比较，并向采购人推荐中标候选人。

32 投标文件的初审

32.1 开标后，采购人将协助评标委员会对投标文件进行初步审查，检查投标文件内容是否完整、编排是否有序、有无计算上的错误、是否提交了投标保证金、文件签署是否规范以及投标人资格是否符合要求等。

32.2 在详细评标之前，评标委员会要对投标人资格进行审核并审查每份投标文件是否实质性响应了采购文件的要求。实质性响应是指投标文件与采购文件要求的条款、投标人资格、条件和规格相符，没有采购文件所规定的无效投标情形。评标委员会只根据投标文件本身的内容来判定投标文件的响应性，而不寻求外部的证据。

32.3 没有实质性响应采购文件要求的投标文件不参加进一步的评审，投标人不得通过修正或撤销不符合要求的偏离或保留从而使其投标成为实质上响应的投标。

32.4 对于投标文件中不构成实质性偏差的小的不正规、不一致或不规范的内容，采购人可以接受，但这种接受不能影响评标时投标人之间的相对排序。

33 投标文件错误的修正

33.1 投标文件中如果有下列计算上或表达上的错误和矛盾，将按以下原则或方法进行修正：

（1）开标一览表内容与报价明细表及投标文件其它部分内容不一致的，以开标一览表内容为准；

（2）投标文件的大写金额和小写金额不一致的，以大写金额为准；

（3）总价与单价和数量的乘积不一致的，以单价计算结果为准，并修正总价；

（4）对投标文件中不同文字文本的解释发生异议的，以中文文本为准。

（5）其他错误和矛盾，按照不利于出错投标人的原则进行修正。

修正后的结果对投标人具有约束作用，投标人应接受并确认这种修正，否则，其投标将被作为无效投标处理。

34 投标文件的澄清

34.1 为有助于对投标文件审查、评价和比较，评标委员会可分别要求投标人对其投标文件中含义不明确、同类问题表述不一致等有关问题进行澄清。投标人应按照采购人通知的时间和地点委派授权代表向评标委员会作出说明或答复。

34.2 投标人对澄清问题的说明或答复，必要时还应以书面形式提交给采购人，并应由投

标人授权代表签字和加盖投标人公章。

34.3 投标人的澄清文件是其投标文件的组成部分。

34.4 投标人的澄清不得改变其投标文件的实质性内容。

35 投标文件的评价与比较

35.1 评标委员会只对被确定为实质上响应采购文件要求的投标文件进行评价和比较。

35.2 评标委员会根据《评标办法》中规定的方法进行评标，并向采购人提交书面评标报告和推荐中标候选人。

36 评标的有关要求

36.1 评标委员会应当公平、公正、客观，不带任何倾向性和启发性，评标委员会及有关工作人员不得私下与投标人接触。

36.2 评标过程严格保密。凡是属于审查、澄清、评价和比较有关的资料以及授标建议等，所有知情人均不得向投标人或其他无关的人员透露。

36.3 任何单位和个人都不得干扰、影响评标活动的正常进行。投标人在评标过程中所进行的试图影响评标结果的一切不符合法律或采购规定的活动，都可能导致其投标被**拒绝**

36.4 采购人和评标委员会均无义务向投标人进行任何有关评标的解释。

七 定标

37 确认中标人

除了《投标人须知》第 40 条规定的采购失败情况之外，采购人将根据评标委员会推荐的中标候选人及排序情况，依法确认本采购项目的中标人。

38 中标结果公示及中标和未中标通知

38.1 采购人确认中标人后，采购人将通过”上海政府采购网”http://www. zfcg. sh.gov.cn 对中标结果进行公示，公示期为一个工作日。

38.2 除了因发生有效的质疑或投诉导致中标结果改变以外，中标结果公示结束以后，采购人将及时向中标人发出《中标通知书》通知中标。《中标通知书》对采购人和投标人均具有法律约束力。

38.3 中标结果公示同时也是对其他未中标投标人的未中标通知。

39 投标文件的处理

所有在开标会上启封并唱出的投标文件都将作为档案保存, 不论中标与否，采购人均不退回投标文件。

40 采购失败

在投标截止时间结束后，参加投标的投标人不足三家的；或者在评标时，符合专业条件的投标人或对采购文件作出实质响应的投标人不足三家，评标委员会认为缺乏竞争性、确定为采购失败的，采购人将通过“上海政府采购网”http://www. zfcg. sh.gov.cn 发布采购失败公告。

八. 授予合同

41 合同授予

除了中标人无法履行合同义务之外，采购人将把合同授予根据《投标须知》第 37 条规定所确定的中标人。

42 采购人授标时更改数量的权利

采购人在授予合同时有权在±10％的幅度内对《采购需求》中规定的服务内容予以增加或减少，但对单价或其他的条款和条件不作任何改变。

43 签订合同

43.1 中标人与采购人应当在《中标通知书》发出之日起 30 日内签订政府采购合同。

44 其它投标注意事项

44.1 采购人和集中采购机构无义务向未中标单位解释未中标理由；

44.2 本采购文件解释权属采购人；

44.3 若发现供应商有不良行为的，将记录在案并上报有关部门。

45 网上投标咨询

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：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的“培训平台”和“联系我们”等专栏的有关内容和操作要求办理。

46 上传扫描文件要求

46.1 投标人应按照采购文件要求提交彩色扫描文件，并在网上投标系统中采用 PDF 模式上传其所有资料，文件格式参考第六章投标文件有关格式，含有公章、防伪标志和彩色底纹类文件（如投标函、营业执照、身份证、认证证书等）必须采用原件彩色扫描以清晰显示。如应上传、扫描、格式等原因导致评审时受影响，由投标人承担相应的责任。

46.2 采购人认为必要时，可以要求投标人提供文件原件进行核对，投标人必须按时提供。否则，视作为投标人放弃潜在中标资格并对该投标人进行调查，有欺诈行为的按有关规定进行处理。

47 网上投标说明

投标人参与网上投标，其主要流程如下：

47.1 下载采购文件：报名初审通过以后，投标人在“网上投标”栏目内选择要参与的投标项目，在采购文件下载有效期内下载采购文件。

47.2 投标文件上传：在投标截止时间前按照网上投标系统和采购文件要求上传投标内容，投标人用上海市电子签名认证证书对投标文件加密后上传到投标系统，**招标代理机构在采购平台进行签收并生成带数字签名的签收回执，投标单位应及时查看签收情况，并打印签收回执**。

第三章 政府采购政策功能

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。对列入财政部、国家发展改革委发布的“节能产品政府采购清单”且属于应当强制采购的节能（包括节水）产品，按照规定实行强制采购。对于列入财政部、国家发展改革委发布的“节能产品政府采购清单”的非强制采购节能产品；列入财政部、环保总局发布的“环境标志产品政府采购清单”的环境标志产品；对于参与投标的中小企业以及经县级以上人民政府民政部门认定、获得福利企业证书的企业，按照国家和上海市的有关政策规定，评标时在同等条件下享受优先待遇，实行优先采购。

上述“节能产品政府采购清单”、“环境标志产品政府采购清单”，在采购公告发布前已经过期的以及尚在公示期的均不得作为评标时的依据。

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。

政府采购对于非专门面向中小企业采购，对小型和微型企业，**投标人使用小型和微型企业产品的价格给予 10%的扣除，用扣除后的价格参与评审、投标人使用中型企业产品的视为中型企业**。如果政府采购非专门面向中小企业采购且接受联合体投标，联合协议中约定小型或微型企业的协议合同金额占到联合体协议合同总金额 30%以上的，给予联合体 4%的价格扣除，用扣除后的价格参与评审。联合体各方均为小型或微型企业的，联合体视同为小型、微型企业。组成联合体的大中型企业或者其他自然人、法人或其他组织，与小型、微型企业之间不得存在投资关系。

为进一步扩展政府采购的政策功能，不断增强政府采购服务中小微企业的能力，积极推进政府采购诚信体系建设，根据市财政局《关于本市开展政府采购融资担保试点工作的通知》（沪财企【2012】54 号）精神，自 2012 年 7 月 1 日起试点开展本市政府采购融资担保业务。中标供应商可自愿选择是否申请融资担保，详见上海市政府采购网 www.shzfcg.gov.cn 政府采购融资担保试点工作专栏中相关业务简介。

第四章 采购需求

一、项目概况

1.1 项目背景

本项目需按照《上海市电子政务外网建设和运行管理指南》中要求，深入贯彻网络强国战略思想，发挥信息化对经济社会发展的引领作用，高水平适应信息时代对政务网络基础设施的要求，做强电子政务“全市一张网”，支撑上海政务服务“一网通办”、城市运行“一网统管”现代化治理体系。采用数据平面和视频平面构建互为备份的“一网双平面”架构，故障时数据平面、视频平面可实现冗余保护，确保政务外网业务的灵活调度和稳定可靠运行。

1.2 现状介绍

金山区现网总体架构为“2+3+N”，“2”指2个区级核心节点，“3”指3个汇聚节点，“N”指N个区委办局、街镇和村居委等接入节点。区、镇两级电子政务外网遵循统一建设标准及运行管理规范。区级政务外网上联市级政务外网，下接街镇级政务网和各委办局政务网。

核心层：2个核心节点各部署了两台核心路由器，以满足设备互为备份的要求。两台设备之间互联链路的带宽100Gbps，与市政务外网之间带宽单端口速率达到40Gbps。

汇聚层：3个汇聚节点各部署了两台汇聚路由器，以满足设备互为备份的要求。两台设备之间互联链路的带宽100Gbps。汇聚节点向上通过100Gbps链路连接核心节点，

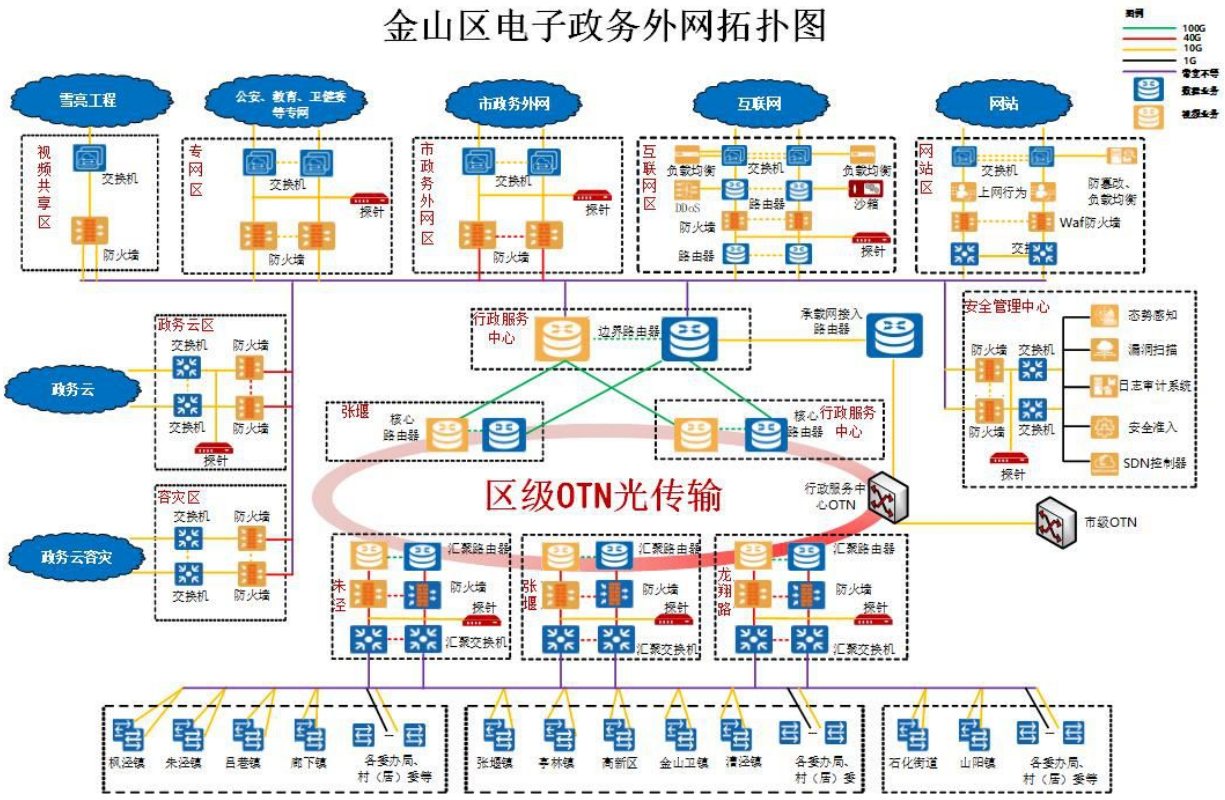
向下通过 1Gbps 链路或 10Gbps 链路连接区级各委办局、村居委，40G 链路至各街镇。

接入层：N 个接入节点通过 N*1Gbps 链路或 N*10Gbps 链路联接至汇聚节点。

边界出口：行政服务中心配备了 2 台核心边界路由器作为边界出口统一接入。在专网边界、市政务外网边界、管理区已建设 6 台交换机。现政务外网网络区域有互联网区域、市政务外网区域、专网区域、视频共享区域、政务云区域（DMZ 和内网区域）和容灾区域。

互联网区域提供全区政务外网用户的互联网访问；市政务外网区域提供区级和市级政务外网之间的互联互通；专网区域提供各委办局专线业务和政务网之间的联通；视频共享区提供视频会议和视频资源共享；政务云区域提供各委办局的网站和系统业务托管；容灾区域提供政务云区域的系统业务冗余和数据备份。

现网拓扑图如下：



1.3 建设目标

以满足未来电子政务发展需求为导向，建成一张标准统一、技术先进、管理智能、安全可靠、坚强有力的新型电子政务外网。充分利用现有资源，按照国家、上海市统一规划和标准规范，完成金山区电子政务外网骨干网升级改造，建立金山区电子政务外网“运维管理体系”和“安全防护体系”，实现金山区电子政务外网在网络架构、技术路线、网络资源、网络运维、网络安全等方面的统一管理，着力打造“四大能力”，为金山区实现跨部门跨层级的网络互通、数据共享、应用协同提供有利支撑，助力金山区实现城市治理能力现代化。

1.4 主要建设内容

本项目的主要建设内容为：政务外网网络系统建设和政

务外网安全体系建设，采购网络运行支撑服务和采购网络整体运维服务，采购安全稳定可靠易于管理的DNS域名解析服务，建设与业务网络相互独立的管理系统承载网。

1.4.1 政务外网网络系统建设服务

采用单波速率100G及以上的OTN技术建设光传输骨干环网；依据A、B双平面（视频网、数据网）的架构设计，建设带宽核心节点100G,核心节点与下级汇聚节点40-100G，同一汇聚节点内主备冗余设备之间40-100G，汇聚节点与下级接入节点N*1G或N*10G的区级政务外网业务网络；建设SDN管控融合平台，实现业务快速部署和流量智能调整能力；建设DNS网络设备，推进网络、平台、应用、终端等全面支持IPv6；整体业务网络需支持IPv4/IPv6双栈能力并满足对IPv6流量的线速转发。

1.4.2 政务外网安全体系建设服务

构建区电子政务外网的安全保障体系，实现政务外网的业务网络安全和安全管理中心的建设。业务网络安全依据区电子政务外网接入方式对网络安全边界进行划分，规划业务网各边界安全防护措施，确保全网受到安全保护、监测、管理，并满足信息系统安全等级保护2.0三级基本要求；建设安全管理中心具备通报预警、漏洞扫描、威胁情报共享台、日志审计、安全管理控制等功能，根据所承载的信息系统安全等级要求，实现网络传输数据的保密性和完整性保护。

还需升级完善配套的电子政务外网安全体系。网络安全

系统依据国家《电子政务外网安全建设规范》的思路建设，并符合《信息安全技术网络安全等级保护基本要求》（GBT22239-2019）规范的基本要求。在此基础上，结合当前电子政务外网的安全现状，从安全技术、安全运营管理、安全运维三个方面开展安全建设，打造运营平台化、管理一体化、态势可感知、事件可预警、事故可追溯、安全可闭环的电子政务外网安全体系。整体金山区电子政务外网机房需满足等级保护三级测评的要求。

本次网络安全部分的设计还需满足《上海市电子政务外网建设和运行管理指南（修订稿)》中对电子政务外网系统网络安全的要求，划分安全边界，安全部分的升级建设及服务主要包括互联网边界安全、市政务外网边界安全、政务云边界安全、单位用户接入边界安全和专网接入边界安全，并建立安全管理中心。

供应商需在设计中体现“一个中心、多重防护”即安全管理中心、区域边界安全、通信网络安全等方面通盘考虑方案设计深度和广度，能够满足安全体系在防御、事中、事后三个阶段监测、防御和追溯。

1.4.3 采购网络运行管理平台服务

建设网络运行管理平台，对基础资源、网络运行、运行日志、运行告警等监控，实现网络故障、传输流量、设备质量和服务质量等分析诊断；对各类网络设备、链路运行状态监控、故障定位与处理过程管控；建设资源管理、智能监控、

业务流程、运营分析和平台管理等应用平台；提供服务受理、变更管理、资源管理、性能管理、报告管理和服务质量管理控制等服务。

1.4.4 采购网络整体运维服务

根据保证政务外网系统稳定、安全、可靠、有效运行的要求，制定政务外网系统运行维护方案，并确保方案的有效执行；建立专业高效的运维服务体系，保障升级后的电子政务外网系统正常运行。提供日常监控维护、节点式管理、机房管理和日常维护、应急故障处理、节假日及重大活动保障和下沉式响应服用；提供政务外网系统信息安全服务，监测网络安全状态，发现各类安全事件，处置入侵攻击行为，快速恢复业务，消除或减轻影响。现场驻点服务团队运行管理服务的具体实施，提供 7×24 小时无推诿服务。

1.4.5 DNS 域名解析服务

助力 IPv6 改造，解决 IPv6 地址空间很大，地址不可识读的问题；对全过程进行集中管理；按照业务逻辑梳理 IPv6 地址，导入 IPv6 地址表，域名化内网地址，通过业务树状图方式管理 IPv6。

实现业务网络 DNS 权威解析及递归解析安全可控，并依靠 DDI 增值应用功能满足各场景的业务需求。另外系统还应该具备平滑升级及扩展能力，后续可以扩展至其他数据中心；系统还应满足维护、管理中文图形化集中管理需求；提供服务的设备应符合国家有关部门及网络安全战略相关规

范与要求，采用国产、具有自主知识产权、安全的设备。

1.5 主要服务内容

1.设施资源服务：包括机房资源服务、网络和安全设备资源服务等。

2.服务的实施：包括基础设施服务实施、运行保障服务实施。

3.保障服务：包括电子政务外网的资源监测、资源配置、资源优化、服务监控、事件处理、运维流程、日常巡检、备份恢复、灾备管理、应急预案管理、服务质量监督和报告等服务。

4.健全配套制度标准。投标企业可提供基于自身平台的相关标准、办法及建议，如：投标人可提供政务外网管理办法、运维制度、应急预案等。

5.建立健全满足政务外网监管需要的配套检测、监管手段（如：流量），及相应监测办法。

1.6 其他

网络服务内容应包含所有升级改造设备的安装、调试等，及项目范围内变更的配置服务等，以确保用户向中标供应商所服务的内容是满足招标文件技术要求，并可直接使用的机房、链路等。

安全、运维技术服务包含：通过建立专业高效的安全和运维服务体系，对升级后的金山区电子政务外网进行整体系统维护，保障网络系统的正常运行。

二、项目需求

2.1 进度要求

本项目须在合同签定之日起30个日历天内完成金山区电子政务外网的升级改造工作；需在2024年5月底前完成建设并进入运营服务期。

2.2 需求分析

2.2.1 光传输网络设计规范

2.2.1.1 光传输网设计

光传输网应具备与现有网络的兼容能力,具体要求如下:

核心节点之间的互联应采用高可用的组网架构,相邻核心节点之间开通两个不同路由的光传输通道,保证两点间多链路可达,对传输的业务进行冗余保护。OTN系统为80*100Gb/s环网，配置2*100Gb/s波道满足两组核心路由器双平面之间的承载需求。

汇聚节点之间应采用环形组网架构,每个汇聚节点到相邻的核心节点之间均开通两个不同路由的光传输通道。

采用单波100G速率，为各节点两个平面的路由器互联提供100G物理通道，并保留未来扩展性，提高网络的承载带宽。

核心节点间开通4个100G业务通道（工作2*100G业务通道，保护2*100G业务通道），承载核心节点间路由器互联

的 2*100GE 业务（视频 100GE，数据 100GE），各汇聚节点与核心节点分别各开通 2 个 100G 业务通道，承载各汇聚点到核心节点之间路由器互联的 2*100GE 业务（视频 100GE，数据 100GE）。各核心和汇聚节点数量，波道数量按需部署。

建设的 OTN 系统满足 OLP/OMSP 保护，同时建设的 OTN 系统节点可将网管信息传输至网管服务器。

2.2.2 业务网络设计规范

区政务外网业务网络应满足各接入单位网络汇聚接入及灵活互通的需求,具体要求如下:

1. 业务网络采用核心、汇聚、接入的三层架构设计;

2. 业务网络的核心、汇聚层应承载于政务外网光传输网络之上;

3. 业务网络采用 “一网双平面”的架构设计。数据平面承载网络数据流量,视频平面承载网络视频流量,两个平面在政务外网上逻辑隔离、独立运行,且互为冗余备份;

4. 应基于 TCP/IP 技术构建政务外网业务网络,采用支持 IPv4/IPv6 双栈技术的网络设备;

5. 业务网络应符合等保规范的要求;

6. 应保证不同应用在业务网络的相互独立,可选用 VLAN、VxLAN、VPN、网络切片等方式实现不同业务的隔离;

7. 应从多个维度考虑设备的安全自主可控,采用国产化、业界领先的网络和安全设备系统;

8. 应采用 SDN 技术,实现业务快速部署,流量工程和智能流量调整能力;

9. 应基于大数据分析技术和智能检测技术,对网络中不同业务的运行状态、服务质量,做到实时监控、主动运维;

2.2.2.1 核心节点设计

1. 核心层设备承担用户流量安全、高速、可靠转发的功能;

2. 核心节点设备选型应能满足面向未来业务发展平滑扩展的需要;

3. 核心节点应采用高冗余设计,保证核心网络的高可靠性。实际设计时,核心节点数应不少于 2 个,每个核心节点应部署不少于两台路由器设备,两台设备之间 100Gbps 链路互相冗余。不同核心节点之间应有多条冗余链路,核心节点之间互联带宽应不少于 100Gbps。

2.2.2.2 汇聚节点设计

1. 汇聚节点采用双归方式接入核心节点以提高网络可靠性。汇聚节点向上通过 100Gbps 链路连接核心节点,向下通过 N×1Gbps 链路或 N×10Gbps 链路连接区级各部门、街镇和村居;

2. 汇聚节点数应不少于 3 个,每个汇聚节点部署不少于两台路由器设备,两台设备之间互联链路的带宽带宽应不少于 100Gbps。

2.2.2.3 接入节点设计

区政务外网的接入节点通过N×1Gbps或N×10Gbps链路联接至汇聚节点。

各接入单位选择单设备单链路、单设备双链路,或双设备双链路作为上行方式（详见接入节点清单)。

2.2.2.4 DNS设计

DNS服务器应支持IPv4/IPv6域名查询(A/AAAA记录查询),且IPv6的DNS查询不影响IPv4的DNS查询。DNS服务器应支持AAAA请求递归查询。

域名解析服务器具备IPv6地址和IPv6网络接入能力,能够支持IPv6协议承载的域名解析请求的处理,即具备IPv6解析能力。

域名解析服务器IPv6域名解析性能包括IPv6域名解析时延和IPv6域名解析成功率,记录解析时延和解析的成功情况。

域名解析服务器需满足后期和市大数据中心DNS服务器的对接能力。

2.2.2.5 承载网设计

需在区级政务外网机房部署管理系统承载网,涉及的链路、设备板卡或接口等机房资源由投标方建设和提供。

区政务外网核心层的光传输环网设备,与相近的市级政务外网光传输环网设备互联,形成管理系统承载网的市、区互通。区级电子政务外网光传输网在与市电子政务外网光传输网互通时,应能通过电层客户侧接口对接。市、区两级政

务外网业务网络的互联互通应通过市级政务外网提供的接入设备完成。该接入设备与区政务外网的出口设备放置于同一机房,两者通过光纤直联。该接入设备宜通过N×10Gbps链路与市政务外网的汇聚交换机联接,宜通过N×1Gbps或N×10Gbps链路与区政务外网的出口设备联接。具体要求如下:

1.应支持IPv4/IPv6双栈技术,并可通过SRv6 隧道实现端到端直达。

2.应支持智能检测技术, 实现网络智能运维。

3.通过传输设备的电层客户侧接口(GE/10GE/100GE,FC等)直接对接。或者两方的传输设备,各自通过GE/10GE/100GE接口,联接至指定的路由器或交换机设备,在该设备上完成对接。

4.选用IS-IS/IS-ISv6、OSPF/OSPFv3、BGP(BGP4+)作为互联协议。

5.选用MPLS VPN、VLAN、VxLAN、EVPN、网络切片等技术实现不同政务业务子网的逻辑隔离。

6. 可选用OTN光传输网络进行市、区两级政务外网的对接。

7.应通过SDN技术实现智能路径计算和流量调优功能,网络和应用流量的精细化管理和分析。宜采用支持SR MPLS或SRv6技术的网络设备,宜支持SR BE、SR TE、SR Policy、SR的TI-LFA FRR、BFD for SR等协议和技术。

8.宜优先采用光传输设备的彩光技术对接(单个波长λ的波分侧信号80km内直接对接,两者采用同一波长,λ1~λ40可选),即区级政务外网的光传输环网设备线路侧彩光口(λ1),与市级政务外网的光传输环网设备线路侧彩光口(λ1)直接互联。或者可采用光传输设备的灰光技术对接(如OTU2灰光),即区级政务外网的光传输环网设备线路侧模块(OTU2灰光),与市级政务外网的光传输环网设备线路侧模块(OTU2灰光)直接互联。

2.2.3 网络设备清单

序号	名称	单位	数量	备注
1	OTN光传输网	套	1	核心节点
2	OTN 承载网	套	1	
3	核心路由器	台	4	
4	核心边界路由器	台	2	
5	汇聚路由器	台	6	汇聚节点
6	接入收敛汇聚交换机	台	6	
7	万兆接入交换机	台	28	接入节点
8	千兆接入交换机	台	364	
10	市政务外网边界交换机	台	2	各边界
11	专网边界交换机	台	2	
12	安全管理中心交换机	台	2	
13	政务网光纤资源	对	476	光纤资源
14	公务网光纤资源	对	28	
15	专线光纤资源	对	7	
16	SDN服务器	套	1	服务器区
17	DNS域名解析设备	台	2	

18	光模块	个	匹配相应网络和安全设备光模块和速率	各节点

2.2.4 接入节点清单

2.2.4.1 政务外网接入节点清单

政务网建设接入节点清单						
序号	区域	单位	地址	资源/对	万兆交换机	千兆交换机
1	综合大楼	行政大楼	龙山路 555 号（核心节点相连）	2	无需增加	无需增加
2			龙山路 555 号（行政楼 4 楼汇聚）	0	利旧	0
3		区政府大楼	金山大道 2000 号	0	利旧	0
4		规划展示馆大楼	金山大道 1800 号四楼	1	1	0
5		合欣大厦	龙山路 758 号 2 楼	0	1	0
6		城投大厦	浩源路 289 号 1 楼	2	1	0
7		工商联大厦	龙山路 299 号	1	1	0
8		晨光进修学院综合办公大楼	蒙山北路 611 号	1	1	0
9		老石化医院大楼	金一东路 391 号安保室	1	0	利旧
10		卫二路 428 号综合大楼	卫二路 428 号	1	0	利旧
11		卫二路老大院	卫二路 429 号	1	0	1
12		金文大厦	蒙山北路 280 号	0	2	0
13		财政大楼	蒙山北路 99 号 5 楼	2	1	0
14		税务大楼	浩源路 80 号 4 楼	1	0	1
15		蓝色收获大院	板桥东路 902 弄 48 号 1 楼	2	0	利旧
16		金一东路 391 号综合办公大楼	石化街道金一东路 391 号	2	0	利旧
17	院外委办局	金山医院	龙航路 1508 号	2	0	1
18		市政_环卫署	松南支路 49 号	1	0	1
19		市场公司	学府路 739 号	1	0	1
20		城市管理执法局	隆安东路 288	1	0	1
21		公安分局	蒙源路 110 号	1	0	1
22		检察院	浩源路 211 号	1	0	1
23		城市沙滩接入（原绿容局）	荔浦路 135 弄 47 号	1	0	1
24		房土局	二村 250 号	1	0	1
25		法院	金山大道 2288 号	1	0	1
26		海关	卫新路 11 号	1	0	1
27		园林管理所	卫一路 165 号	1	0	1
28		生态环境局	临桂路 2430 号	1	0	1

29		武装部	龙皓路 810 号	1	0	1
30		石化市场监督所	石化十二村 121 号	1	0	1
31		计量质量检测所	杭州湾大道 2525 号	1	0	1
32		文化资源配送	临潮三村 73 号	1	0	1
33		统战部	卫零路 809 号	1	0	1
34		国安分局	松卫南路 618 号	1	0	1
35		医保办	蒙山路 1536 号	1	0	1
36		科委	金一东路 11 号	1	利旧	0
37		工人文化宫	杭州湾大道 601 号	1	0	利旧
38		看守所	南阳湾路 1188 号	1	0	1
39		铁塔公司	卫零北路 168 弄 16 号	1	0	1
40		气象局	杭州湾大道 1228 弄 1 号	1	0	1
41		精神卫生中心	金石南路 1949 号	1	0	1
42		电力公司	金山大道 2522 号	1	0	1
43	漕泾镇	漕泾镇镇政府	上海市金山区漕泾镇漕廊公路 398 号	2	利旧	0
44		漕泾镇社区事务受理中心	漕泾镇中一西路 601 号	2	0	1
45		漕泾镇网格化	漕泾镇致富路 11 号	2	2	0
46		漕泾镇综治中心	漕泾镇新民路 15 号	1	0	1
47		漕泾镇社区卫生服务中心	漕泾镇中一东路 99 号	1	0	1
48		漕泾镇党建服务中心	漕泾镇中一西路 311 号	1	0	1
49		漕泾镇规土所	漕泾镇中心西街 250 号	1	0	1
50		漕泾镇经济管理事务中心	漕泾镇漕廊公路 458 号	1	0	1
51		漕泾镇财政所	漕泾镇新民路 8 号	1	0	1
52		漕泾镇绿化市容管理所	漕泾镇漕廊公路 518 号	1	0	1
53		漕泾镇文化体育服务中心	漕泾镇富漕路 239 号	1	0	1
54		漕泾镇农业技术推广服务站	漕泾镇漕廊公路 938 号	1	0	1
55		金山第二工业区	漕泾镇合展路 118 号	1	0	1
56		漕泾镇市场监督管理所	漕泾镇漕廊公路 18 号	1	0	1
57		漕泾镇水务站	漕泾镇漕廊公路 636 号	1	0	1
58		增丰村	上海市金山区漕泾镇增丰村 2058 号	1	0	1
59		东海村	上海市金山区漕泾镇东海村 2121 号	1	0	1
60		营房村	上海市金山区漕泾镇工农	1	0	1

			街 99 号			
61		沙积村	上海市金山区漕泾镇沙积村 2132 号	1	0	1
62		水库村	上海市金山区漕泾镇水泾路 1155 号	1	0	1
63		阮巷村	上海市金山区漕泾镇朱漕公路 2828 号	1	0	1
64		蒋庄村	上海市金山区漕泾镇蒋庄村 2058 号	1	0	1
65		护塘村	上海市金山区漕泾镇护塘村邓桥路 1518 号	1	0	1
66		金光村	上海市金山区漕泾镇漕廊公路 958 号	1	0	1
67		海涯村	上海市金山区漕泾镇漕廊公路 985 号 601 室	1	0	1
68		海渔村	上海市金山区漕泾镇海渔村 1180 号	1	0	1
69		花园居委	上海市金山区漕泾镇中心街 252 弄 2 号	1	0	1
70		建龙居委	上海市金山区漕泾镇中一东路 333 号	1	0	1
71		绿地居委	上海市金山区漕泾镇富漕路 461 弄 26 号	1	0	1
72	枫泾镇	枫泾镇镇政府	朱枫公路 9880 号	2	利旧	0
73		枫泾镇社区事务受理中心	枫泾镇枫杰路 51 号	2	0	2
74		兴塔社区分中心	金山区枫泾镇兰兴路 600 弄 568 号	2	0	2
75		枫泾镇网格化	朱枫公路 9880 号	0	2	0
76		枫泾镇社区卫生服务中心	枫杰路 28 号	1	0	1
77		枫泾镇党建服务中心	枫兰路 144 号	1	0	1
78		枫泾镇规土所	枫泾枫丽路 125 号	1	0	1
79		枫泾镇住房所	新枫路 121 弄 19 号	1	0	1
80		枫泾镇文化体育服务中心	朱枫公路 8666 号	1	0	1
81		枫泾镇绿容环境事务所	思古弄 30 号	1	0	1
82		枫泾镇水务站	枫思路 95 号	1	0	1
83		枫泾镇工业区管理委员会	亭枫公路 6728 号	1	0	1
84		新元村	新元村 5513 号	1	0	1

85		中洪村	中洪村 17 组 5087-1 号	1	0	1
86		俞汇村	俞汇村 1 组 1118 号	1	0	1
87		新春村	枫阳路 1811 弄 116 号	1	0	1
88		农兴村	枫湾路 531 号	1	0	1
89		长征村	万枫公路 5019 号	1	0	1
90		钱明村	钱明村王圩东路 5088 号	1	0	1
91		盛新村	盛新村 13 组 5120 号	1	0	1
92		新华村	枫南 6 组 6138 号	1	0	1
93		新义村	明星路 2115 号	1	0	1
94		菖梧村	菖梧村 6008 号	1	0	1
95		团新村	团新村 8 组 7002 号	1	0	1
96		新新村	新新村养义 6 组	1	0	1
97		五星村	五星村蒋浜 1068 号	1	0	1
98		双庙村	双庙村 5 组 4138 号	1	0	1
99		新黎村	兴寒路 2120 号	1	0	1
100		兴塔村	兴塔村 8 组 1062 号	1	0	1
101		贵泾村	兴坊路 698 号	1	0	1
102		下坊村	兴坊路 358 号	1	0	1
103		五一村	五一村 15 组 2121 号	1	0	1
104		卫星村	卫星村 5 组 5130 号	1	0	1
105		泖桥村	泖桥村 4 组 5003-1 号	1	0	1
106		韩坞村	韩坞村 2162 号	1	0	1
107		友好居委会	圣堂弄 18 号	1	0	1
108		新枫居委会	枫丽路 99 号	1	0	1
109		和平居委会	北大街 303 号	1	0	1
110		白牛居委会	白牛路 99 弄 3 号	1	0	1
111		枫阳居委会	泾波路 219 弄 59 号	1	0	1
112		枫岸华庭	枫湾路 500 弄 54 号	1	0	1
113		兴塔居委会	新金山路 386 号	1	0	1
114		新苑小区	金山区枫泾镇兰兴路 600 弄 568 号	1	0	1
115		枫香名苑	枫兰路 128 弄 44 号	1	0	1
116		桃源名庭	泾波路 1536 弄 41 号东 2 楼	1	0	1
117		枫泾镇居家养老	枫丽路 168 号 1 层	1	0	1
118		城建中心综合楼	枫泾镇泾波路 1694 号	1	0	1
119		兴塔社区卫生服务中心	金山枫泾镇镇兴塔兴新路 838 号	1	0	1
120		枫兰居居民区管理委员会	枫兰路 1069 号	1	0	1
121		枫美居居民区管理委员会	枫湾路 680 弄 8 号	1	0	1
122		枫泾镇两城管委会	枫翠路 562 号 2 楼	1	0	1

123	山阳镇	山阳镇镇政府	龙皓路 28 号	2	利旧	0
124		山阳镇社区事务受理中心	亭卫公路 1500 号三楼	2	0	2
125		山阳镇网格化	山阳镇龙皓路 110 号	2	2	0
126		山阳镇综治中心	山阳镇亭卫公路 1500 号南侧	1	0	1
127		山阳镇社区卫生服务中心	向阳西路 88 号	1	0	1
128		山阳镇绿化市容所	邓曙路 441 号西侧	1	0	1
129		上海湾区	亭卫公路 1000 号	1	0	1
130		山阳镇党建服务中心	亭卫公路 1358 号党建楼 1 层	1	0	1
131		向阳村	红旗东路 232 弄 48 号	1	0	利旧
132		九龙村	汀南路与朱山路交叉路口往东约 150 米	1	0	利旧
133		长兴村	长兴村 2009 号（长甸路与长兴南路交叉路口往北约 50 米）	1	0	利旧
134		华新村	工农路与山丰路交叉路口往北约 200 米	1	0	利旧
135		渔业村	亭卫南路 88 号	1	0	1
136		中兴村	中兴村 8056 号	1	0	利旧
137		东方村	金山大道 1388 号	1	0	利旧
138		杨家村	卫零北路 281 号南 80 米	1	0	利旧
139		新江村	亭卫南路临桂路东侧约 200 米	1	0	利旧
140		卫东村	卫零路 799 弄 66 号	1	0	利旧
141		三岛龙洲居委	蒙山路 1498 号	1	0	1
142		金海岸居委	龙胜东路 784 号	1	0	1
143		金世纪居委	金山大道 2335 号	1	0	1
144		戚家墩居委	隆安东路 161 号	1	0	1
145		金豪居委	卫清东路 2988 号 58 号	1	0	1
146		海云居委	海丰路 83 弄 1 号 3 楼	1	0	1
147		海趣居委	龙翔路 1128 弄	1	0	1
148		联江居委	同凯路 515 号西侧	1	0	1
149		康建居委	卫清东路 2835 弄 171 号 2 楼	1	0	1
150		山新居委	向阳西路 88 号南侧约 50 米	1	0	1
151		蓝色收获居委	板桥东路 902 弄 48 号 3 楼	0	0	1
152		海尚居委会	海盛路 515 号	1	0	1
153		海欣居委会	龙皓路 398 弄	1	0	1
154		红树林居委会	卫零北路 800 弄	1	0	1

155		金天地居委会	板桥西路 96 弄 46 号	1	0	1
156		金湾居委会	海芙路 275 号	1	0	1
157		金悦居委会	卫零北路 811 号	1	0	1
158		金韵居委会	卫零北路 333 弄	1	0	1
159		龙泽园居委会	龙翔路 785 号	1	0	1
160		万盛居委会	海汇街 500 弄	1	0	1
161		万皓居委会	龙皓路 1068 号 1 号写字楼三楼	1	0	1
162		海悦居委会筹建组	龙航路 718 号	1	0	1
163		旭辉居委会筹建组	海盛路 500 弄	1	0	1
164		香颂湾居委会筹建组	龙轩路 999 弄 35 号一楼	1	0	1
165		国宸府居委会筹建组	同凯路 228 弄 68 号 102	1	0	1
166		山阳城运中心（万达联勤）	龙皓路 962 号 2 楼	1	0	1
167		民兵训练基地	龙皓路 158 号	1	0	利旧
168		女子民兵哨所	沪杭公路 7085 号	1	0	利旧
169		光明府居委会	龙堰路 223 弄 14 号 2 层	1	0	1
170		山阳镇铂翠廷居委会	上海市金山区山阳镇龙堰路 999 弄 3 号 1 层	1	0	1
171		山阳镇海璟居委会	龙湾路 66 弄 15 号	1	0	1
172		海芙金邸居委会筹建组	上海市金山区山阳镇龙堰路 699 弄 5 号 1 层	1	0	1
173	廊下镇	廊下镇镇政府	廊下镇景乐路 228 号	2	利旧	0
174		廊下镇综治中心	新村路 195 号	1	0	1
175		廊下镇网格化	廊下镇景乐路 228 号	0	2	0
176		廊下镇社区卫生服务中心	漕廊公路 7887 号	1	0	1
177		廊下镇党建服务中心	景钱路 1688 弄 1708 号	1	0	1
178		廊下镇市场监管所	金廊公路 149 号	1	0	1
179		光明村	金石北路 985 号	1	0	1
180		景阳村	景阳村新建丰 1012 号	1	0	1
181		廊下居委会	益民路 56 号	1	0	1
182		南陆村	南陆村庄家 2002 号	1	0	1
183		南塘村	南塘村 6076-1 号	1	0	1
184		山塘村	山塘村 1053 号	1	0	1
185		万春村	漕廊公路 6825 弄 517 号（机房 519）	1	0	1
186		勇敢村	勇敢村 5078 号	1	0	1
187		友好村	友好村向化 5032 号	1	0	1
188		中丰村	中丰村 3088 号	1	0	1

189		中华村	中华村委会 5092 号	1	0	1
190		中联村	中联村 3013 号	1	0	1
191		中民村	中民村 5068 号	1	0	1
192		景展社区	春虹路 208 弄 29 号	1	0	1
193		特色民居	景钱路 1688 弄 666 号	1	0	1
194	吕巷镇	吕巷镇镇政府	金山区吕巷镇朱吕公路 6888 号	2	利旧	0
195		吕巷镇社区事务受理中心	吕巷镇溪南路 58 号	2	0	2
196		吕巷镇网格化	吕巷镇金张公路 4679 号	2	2	1
197		吕巷镇社区卫生服务中心	吕巷镇溪北路 74 号	1	0	1
198		吕巷镇党建服务中心	吕巷镇朱吕公路 6858 号 2 楼	1	0	1
199		吕巷镇规划建设和环境保护办	吕巷镇康兴路 106 弄 211-213 号	1	0	利旧
200		吕巷镇绿化市容管理所	吕巷镇郭家新村 132 号	1	0	1
201		吕巷镇农业技术推广服务站	吕巷镇南溪二村 68 号	1	0	1
202		吕巷镇经济园区	吕巷镇金张公路 4865 号	1	0	1
203		干巷街道	金山区吕巷镇龙士路 8 号	1	0	1
204		白漾村	金山区吕巷镇荣田路 688 号 1 层	1	0	1
205		龙跃村	金山区吕巷镇金张公路 1625 号	1	0	1
206		太平村	金山区吕巷镇吕新路 1782 号	1	0	1
207		和平村	金山区吕巷镇和平村 5 组 3000 号	1	0	1
208		蔷薇村	金山区吕巷镇吕青路 1002 号	1	0	1
209		夹漏村	金山区吕巷镇夹漏村 1068 号	1	0	1
210		姚家村	金山区吕巷镇姚家村 3088 号	1	0	1
211		荡田村	金山区吕巷镇荡田村 6 组 2088 号	1	0	1
212		颜圩村	金山区吕巷镇干林路 1318 号	1	0	1
213		马新村	金山区吕巷镇马新村 5080 号	1	0	1
214		吕巷街道	金山区吕巷镇溪南路 68	1	0	1

			号			
215	石化街道	石化街道	卫零路 485 号	2	利旧	0
216		石化街道社区事务受理中心	卫零路 478 号	2	0	1
217		石化街道网格化	沪杭公路 7818 号	2	2	0
218		石化街道综治中心	象州路 50 号	1	0	1
219		石化街道社区卫生服务中心	象州路 12 号	1	0	1
220		石化街道房管所	南康路 128 号	1	0	1
221		消保委	蒙山路 915 号	1	0	利旧
222		石化街道文体中心	象州路 238 号	1	0	1
223		石化街道社会组织服务中心/石化街道拆违办	临潮二村 18 号	1	0	利旧
224		三村居委会	金零路 98 号三村 312 号 101 室	1	0	利旧
225		四村居委会	石化四村 400 号	1	0	利旧
226		柳城居委会	柳城路 161 号石化八村东区 824-1 号	1	0	利旧
227		七村居委会	柳城路 100 号 2 楼	1	0	利旧
228		九村居委会	富川路 15 号，九村 986 号	1	0	利旧
229		十村居委会	石化十村 19 号	1	0	利旧
230		合浦居委会	石化街道石化十一村 69 号 2 层	1	0	1
231		十二村居委会	石化十二村 111 号	1	0	利旧
232		十三村居委会	石化十三村 6 号 102 室	1	0	利旧
233		梅州居委会	梅州新村 B 公建 192 号 3 楼	1	0	利旧
234		海棠居委会	新城路 318 号	1	0	利旧
235		临蒙居委会	临潮一村 21 号底楼	1	0	利旧
236		临三居委会	临潮三村 55 号	1	0	利旧
237		滨一居委会	板桥西路 1230 号滨海三村 10 号	1	0	利旧
238		滨二居委会	板桥西路 1221 弄滨海二村 29 号	1	0	利旧
239		东礁一居委会	东礁三村 8 号	1	0	利旧
240		东礁二居委会	东礁四村 12 号 101 室	1	0	利旧
241		东村居委会	学府路 221 号	1	0	1
242		东泉居委会	龙胜路 151 弄 211 号	1	0	利旧
243		辰凯居委会	龙胜路 400 号辰凯花苑 18 号 2 楼	1	0	利旧
244		山鑫居委会	蒙山路 1090 弄 88 号 204 室	1	0	利旧

245		山龙居委会	山龙新村 130 号	1	0	利旧
246		卫清居委会	卫零路 548 弄振阳新村 4 号 101 室	1	0	利旧
247		桥园居委会	龙胜路 666 弄 27 号	1	0	利旧
248		紫卫居委会	蒙山路 1517 弄 76 号	1	0	利旧
249		合生居委会	龙胜路 69 弄 6 号	1	0	利旧
250		城运中心联勤	石化二村 250 号	1	0	利旧
251	亭林镇	亭林镇镇政府	华亭路 56 号	2	利旧	0
252		亭林镇社区事务受理中心	亭林镇亭升路 550 弄 33 号	2	0	2
253		亭林镇党建服务中心	华亭路 115 号	1	0	利旧
254		亭林镇综治中心	大通路 26 号	1	0	1
255		亭林镇武装部	寺平南路 16 号（武装部）	1	0	1
256		亭林镇农技站	新建新村 55 号	1	0	1
257		亭林镇住房保障所	寺平北路 68 号	1	0	1
258		亭林镇城管中队	南亭公路 6779 弄 17 号	1	0	1
259		亭林镇外经公司	兴工路 225 号	1	0	1
260		亭林镇绿容所	新建新村 30 号	1	0	1
261		亭林医院	寺平北路 80 号	1	0	1
262		松隐社区卫生服务中心	松隐大街 456 号	1	0	1
263		驳岸村	亭林镇驳岸村 11 组 7100 号	1	0	1
264		东新村	亭林镇亭朱公路 1955 号	1	0	1
265		浩光村	亭林镇松金公路 6088 号	1	0	1
266		红阳村	亭林镇红阳村 7 组 9093-30 号	1	0	1
267		后岗村	亭林镇后岗村前中 10 组 4128 号	1	0	1
268		金门村	亭林镇亭枫公路 1034 号	1	0	1
269		金明村	亭林镇金明村 5 组 2048 号	1	0	1
270		龙泉村	亭林镇南亭公路 5346 弄 9 号	1	0	1
271		南星村	亭林镇南星村 9 组 4110 号	1	0	1
272		亭北村	亭林镇亭北村 9 组 6088 号	1	0	1
273		亭东村	亭林镇亭东村亭虹路 308 号	1	0	1
274		亭西村	亭林镇亭西村 8 组 2020 号	1	0	1
275		新巷村	亭林镇新巷村 14 组 2087 号	1	0	1
276		油车村	亭林镇油车村 5088 号	1	0	1
277		周栅村	亭林镇周栅村松牌路 415	1	0	1

			号			
278		复兴居委会	亭林镇和平东路 85 号	1	0	1
279		中山居委会	亭林镇中山街 196 号	1	0	1
280		新建居委会	新建新村 29 号	1	0	1
281		寺平居委会	亭林镇寺平北路 165 弄 72 号	1	0	1
282		松隐居委会	亭林镇小康路 34 号	1	0	1
283		寺北居委会	亭林镇寺平北路 351 弄 213 号	1	0	1
284		隆亭居委会	亭林镇金展路 2146 弄 52 号	1	0	1
285		华城第一居委会	亭林镇林珍路 59 弄 98 号	1	0	1
286		华城第二居委会	亭林镇林珍路 58 弄 66 号	1	0	1
287		社会事业发展办公室	寺平南路 28 号	1	0	1
288		亭林名阳两城居委会	上海市金山区亭林镇林吉路 788 弄 26 号 1 层	1	0	1
289	张堰镇	张堰镇镇政府	康德路 328 号	2	利旧	0
290		张堰镇社区事务受理中心	张堰镇东贤路 951 号	2	0	1
291		张堰镇城运中心	康德路 328 号	0	2	0
292		张堰镇城建中心	金张公路 274 号	1	0	1
293		张堰镇综治中心	张漕公路 8 号	1	0	1
294		张堰镇党建服务中心	金张公路 281 号	1	0	1
295		旧港村	张旧公路 1038-2	1	0	1
296		桑园村	张旧公路 1802 号	1	0	1
297		鲁堰村	鲁堰村 2188 号	1	0	1
298		角里村	松金公路 2088 号	1	0	1
299		百家村	荡里路 55 弄 36 号	1	0	1
300		秦山村	张溪路 308 弄 8 号	1	0	1
301		建农村	建农路 1288 号	1	0	1
302		秦阳村	秦阳村 7001 号	1	0	1
303		秦望村	金张公路 506 号	1	0	1
304		富民居民区	富民新村 110 号	1	0	1
305		东风居民区	新华东路 67 号	1	0	1
306		解放居民区	政安弄 5 支弄 1 号	1	0	1
307		留溪居民区	张堰镇松金公路 2800 弄 85 号	1	0	1
308		综治中心留溪广场外口工作站	金山区张堰镇新建路 94 号 2 层	1	0	利旧
309		张堰镇社区卫生服务中心	上海市金山区张堰镇张漕公路 118 号	1	0	1

310		朱泾镇镇政府	人民路 310 号	2	利旧	0
311		妇幼保健院	南圩路 12 号	1	0	1
312		水产技术推广	朱泾镇临源街 655 号	1	0	1
313		矫正中心	沈浦泾路临仓小区东侧	1	0	利旧
314		朱泾镇城建办	万安街 750 号 4 号楼	1	0	1
315		公路署	临仓街 519 号	1	0	1
316		疾控中心	卫生路 94 号	1	0	1
317		农委信息中心	人民路 39 号	1	0	1
318		残联	朱泾镇文商路 99 号	1	0	1
319		婚姻登记所	朱泾镇临源街 620 号	1		1
320		老干部局	人民路 80 号	1	0	1
321		退管中心	金山朱泾镇临仓街 520 号	1	0	1
322		林业站	朱泾镇人民路 95 号	1	0	1
323		农校	南圩路 255 号	1	0	1
324		水务站	人民路 65 号	1	0	1
325		党校	健康路 236	1	0	利旧
326		水利管理所	秀州街 658 号	1	0	1
327		朱泾镇社区事务受理中心	人民路 360 号	2	0	1
328		朱泾镇网格化	临源街 750 号	2	2	0
329		朱泾镇安宁养老院	康健路 46 号	1	0	1
330	朱泾镇	朱泾镇综治中心	人民路 280 号	1	0	1
331		朱泾镇社区卫生服务中心	罗星南路 608 号	1	0	1
332		第六人民医院	朱泾镇健康路 147 号	2	0	1
333		朱泾镇党建服务中心	人民路 261 号	1	0	1
334		朱泾镇规土所	临源街 368 号	1	0	1
335		秀州村	秀州村胜利 5 组 3198 号	1	0	1
336		万联村	万枫公路 238 号	1	0	1
337		五龙村	金廊公路 5185 号	1	0	1
338		待泾村	待泾村蒋泾中心路 7088 号	1	0	1
339		新泾村	朱平公路 5198 号	1	0	1
340		大茫村	大茫村增产 14 组 6011 号	1	0	1
341		民主村	罗星南路 190 弄 455 号	1	0	1
342		长浜村	仙居路 818 号	1	0	1
343		慧农村	慧农村 5006 号	1	0	1
344		牡丹村	牡丹村 2088 号	1	0	1
345		温河村	新民 2 组 4002 号	1	0	1
346		社区生活服务中心	金龙新街 519 号二楼	1	0	1
347		钟楼居委	钟楼新村 45 号	1	0	1
348		凤翔居委	凤翔新村 46 号 101 室	1	0	1

349		北圩居委	临源街 1072 号 2 楼	1	0	1
350		南圩居委	南圩新村 144 号	1	0	1
351		临源居委	万安街 556 号 2 楼	1	0	1
352		临东居委	临源一村 171 号 101 室	1	0	1
353		罗星居委	罗星新村 27 号 102 室	1	0	1
354		东林居委	城中路 38 弄 82 号 101 室	1	0	1
355		西林居委	万安新村 22 号	1	0	1
356		新汇居委	朱泾镇公园路 129 弄 21 号 3 楼	1	0	1
357		广福居委	西粮库路 168 号	1	0	1
358		金龙居委	众安街 389 弄 2 号	1	0	1
359		浦银居委	浦银路 455 号	1	0	1
360		塘园居委	健康南路 518 弄 60-61 号	1	0	1
361		金汇居委	罗星南路 258 弄 55 号	1	0	1
362		红菱居委	秀州街 718 弄 2 号 3 楼	1	0	1
363		金来居委	金南街 501 弄 91 号 2 楼	1	0	1
364		众安居委	众安街 928 弄 1 号 4 楼	1	0	1
365		金山殡仪馆	金张公路 6605 号业务楼 2 楼	1	0	利旧
366		联勤工作站	朱泾镇金龙新街 370 号	1	0	利旧
367		金山资本管理集团有限公司	沈浦泾路 28 号	1	0	利旧
368		新天鸿居委会	金石北路 6800 弄 3018 号 2 层	1	0	1
369		供销社	朱泾镇金山东风南路 85 弄 25 号	1	0	利旧
370	金山卫	金山卫镇镇政府	老卫清路 288 号	2	利旧	0
371		金山卫镇社区事务受理中心	金山卫镇古城路 319 号	2	0	1
372		金山卫镇党群服务中心	金山卫镇古城路 295 号	0	0	1
373		金山卫镇网格化	西静路 660 号	2	2	0
374		金山卫镇综治中心	老卫清路 348 号	1	0	1
375		金山卫镇应急管理中心	老卫清路 239 号	1	0	1
376		金山卫镇规土所	南阳湾路 1839 号	1	0	1
377		绿容所	老卫清路 29 号	1	0	1
378		动迁安置办	金山卫镇老卫清路 580 号	1	0	利旧
379		水务站	金山卫镇老卫清路 116 号	1	0	1
380		农技站	金山大道 4258 号	1	0	1
381		钱圩劳动保障	建圩路 69 号	1	0	1
382		农建村	金山卫镇松金公路 218 号	1	0	1
383		金卫村	板桥西路 1338 号	1	0	1

384		卫城村	金山卫镇古城路 239 号	1	0	1
385		八一村	金山卫镇建昌路 1006 号	1	0	1
386		八二村	金山卫镇卫五北路 199 号	1	0	1
387		永久村	金山卫镇海金路 538 号	1	0	1
388		永联村	金山卫镇金石南路 805 号	1	0	1
389		横浦村	金山卫镇海秀路 555 弄 32 号	1	0	1
390		卫通村	金山卫镇卫通村 9 组 5011 号	1	0	1
391		张桥村	金石南路 1122 号	1	0	1
392		横召村	金山卫镇横召村 2138 号	1	0	1
393		星火村	钱鑫路 600 号	1	0	1
394		塔港村	塔港村 6027 号	1	0	1
395		八字村	金山卫镇八字村 7030 号	1	0	1
396		东门居委会	学府路 792 号	1	0	1
397		南门居委会	金山卫镇北泰路 318 弄 50 号	1	0	1
398		西门居委会	金山卫镇临江村路 59 号	1	0	1
399		北门居委会	金山卫镇龙轩路 2208 弄 90 号	1	0	1
400		钱圩居委会	金山卫镇建圩路 20 弄 38 号	1	0	1
401		金康居委会	南阳湾路 1288 弄 102 号	1	0	1
402		东平居委会	金山卫镇龙皓路 1738 弄 67 号	1	0	1
403		明卫居委会（筹）	明卫路 688 弄 18 号	1	0	1
404		金山第二工业区	金山卫镇秋实路 688 号	1	0	1
405		福利院	金山大道 3528 号行政楼 106	1	0	1
406		龙湾璟苑居委会	上海市金山区金山卫镇龙湾路 1885 弄 1 号 2 层	1	0	1
407	卫健委机房（金山卫社区卫生服务中心）	行政服务中心(容灾机房链路冗余）	西静路 367 号 3 号楼 3 层	1	无需增加	无需增加
				1	0	1
				1	无需增加	无需增加
				1	无需增加	无需增加
				1	无需增加	无需增加
				1	无需增加	无需增加
				1	无需增加	无需增加
				1	无需增加	无需增加
				1	无需增加	无需增加
408	高新区	高新区	工业区 2 号楼	2	利旧	0
409		高新区社区	金山工业区恒顺路 280 弄 15 号	2	0	1

410		高新区社区卫生服务中心	亭卫公路 6668 号	1	0	1
411		高新区网格化	金山工业区	0	2	0
412		高新区规土所	高林路 115 号	1	0	1
413		市场监督管理所	夏宁路 818 弄 52 号	1	0	1
414		拆违与城管办	朱漕公路 115 号	1	0	1
415		农技站	朱漕公路 2072-1 号	1	0	1
416		工业区发展公司	工业区大道 100 号	1	0	1
417		欢兴村村民委员会	烟漕路 2060 号	1	0	1
418		红光村村民委员会	朱漕路 655 号	1	0	1
419		高楼村村民委员会	高楼村 6 组 4011 号	1	0	1
420		桥湾村村民委员会	恒顺南路 98 弄 22 号	1	0	1
421		胥浦村村民委员会	胥浦村 1 组 4090 号	1	0	1
422		新街村村民委员会	新街村 4 组 1020 号	1	0	1
423		保卫村村民委员会	保卫处 6 组 3010 号	1	0	1
424		合兴村村民委员会	合兴村 1 组 1001 号	1	0	1
425		红叶居民委员会	珠港街 148 号	1	0	1
426		恒信居民委员会	恒顺路 215 弄 317 号	1	0	1
427		恒顺居民委员会	恒顺路 408 号	1	0	1
428		朱行居民委员会	高林路 115 号	1	0	1
429		恒康居民委员会	恒康路 256 号	1	0	1
430		金水湖居民委员会	博海路 99 弄 55 号	1	0	1
431		运河村	朱漕公路 328 弄 161 号	1	0	1
432		鑫港湾	月工路 888 号	1	0	1
433		残疾人“阳光家园”	亭朱公路 585 号	1	0	1
434		华云居民委员会	九工路 2055 弄 25 号	1	0	1
435	经济小区	杭州湾北岸产业园	金山区亭卫公路 6488 号北楼 13 层	1	0	1
436		二工区企业服务中心	上海市金山区金一东路 1 号(金山宾馆)南楼一层	1	0	1
437		临海经济小区	海汇街 108 弄 18 号	1	0	1
438		朱泾经济小区	上海市金山区朱泾镇临源街 553 号	1	0	1
439		珠龙小区	金山区朱泾镇罗星南路 585 号	1	0	1
440		枫泾经济小区	枫泾镇白牛路 660 弄 1 号	1	0	1
441		新农经济小区	朱泾镇罗星南路 208 号底楼	1	0	1
442		金城经济小区	山阳镇龙翔路 1142 号一楼	1	0	1
443		金石湾功能区	上海市金山区山阳镇浦卫公路 16299 弄 5 号楼 217 室	1	0	1

	总计：	476	28	364

2.2.4.2 政务内网接入节点清单

政务内网建设接入节点清单		
序号	单位	资源/对
1	检察院	1
2	税务局	1
3	党校	1
4	残联	1
5	老干部局	1
6	金山区统战部	1
7	教育局	1
8	环保局	1
9	规划局	1
10	科委	1
11	司法局	1
12	公安局	1
13	法院	1
15	人武部	1
16	城市管理监察大队	1
17	山阳政府双路由	1
18	廊下政府双路由	1
19	漕泾政府双路由	1
20	吕巷政府双路由	1
21	金卫政府双路由	1
22	亭林政府双路由	1
23	工业区管委会双路由	1
24	枫泾政府双路由	1
25	朱泾政府双路由	1
26	张堰政府双路由	1
27	石化街道双路由	1
28	医保中心	1
29	城投大厦	1
30	公服中心 10 家单位	自建
31	体育局、文旅局	自建
32	区融媒体中心	自建

33	建管委、房管局、水务局、绿化市容局	自建
34	民防办、退役军人事务局	自建
35	区纪委、巡察办	自建
36	金山发展公司	自建
37	二工区发展公司	自建
38	会议中心	自建
总计		28

2.2.4.3 专线接入节点清单

专线接入节点清单		
序号	单位	资源/对
1	税务局	1
		1
2	中国石化上海石油	1
3	档案局	1
4	卫健委机房 （金山卫社区）	1
		1
		1
5	教育局	1
总计		7

接入节点清单其中利旧设备和自建链路在服务期间发生故障时，供应商应及时提供技术支持或备品备件完成修复网络，服务期间不产生任何费用。另所有双链路实施的必须保证双路由通道，链路需铺设在不同管道，并提供承诺书。

三、服务内容及要求

3.1 设备技术要求

序号	名称	单位	数量	备注
1	OTN 光传输网	套	1	**详见设备技术要求 3.2**
2	OTN 承载网	套	1	**详见设备技术要求 3.2**
3	核心路由器	台	4	**详见设备技术要求 3.3**
4	核心边界路由器	台	2	**详见设备技术要求 3.4**
5	汇聚路由器	台	6	**详见设备技术要求 3.5**
6	接入收敛汇聚交换机	台	6	**详见设备技术要求 3.6**

7	万兆接入交换机	台	28	**详见设备技术要求 3.7**
8	千兆接入交换机	台	364	**详见设备技术要求 3.8**
9	市政务外网边界交换机	台	2	**详见设备技术要求 3.9**
10	无线/专网边界交换机	台	2	**详见设备技术要求 3.10**
11	安全管理中心交换机	台	2	**详见设备技术要求 3.11**
12	DNS 域名解析	台	2	**详见设备技术要求 3.12**
13	SDN 服务期	套	1	**详见设备技术要求 8.4**

3.2 OTN 光传输

指标项		功能描述
基本要求	系统组成	OTN系统组成包括OTN终端复用设备、OTN电交叉连接设备、OTN光交叉连接设备、OTN光电混合交叉连接设备、OA(光线路放大器)和色散补偿模块(DCM)(可选)组成。其中OA含光线路放大器、光监控通路(OSC)；DCM（可选）根据色散容忍范围和光放段/光复用段长度配置。
	接口能力	提供SDH STM-N(N=1/4/16/64/256)，ATM、以太网（FE、GE、10GE、40GE、100GE)、OTUk(k=1,2,2e,3,3e1,3e2,4)、FC(可选)、CPRI(1~9)等多种业务接口，及标准的OTN IrDI 互联接口，连接其它OTN设备。
	交叉能力	具备一个或者多个级别ODUk(k=0,1,2,2e,3,4，flex)电路调度。投标方应详细说明支持的交叉颗粒和类型，并提供分别基于ODU0、ODU1、ODU2、ODU2e、ODU3、ODU4、ODUflex交叉颗粒时设备所支持的最大无阻塞电交叉连接能力。
	交叉连接方向及类型	交叉连接方向应不少于线路到支路，支路到线路，线路到线路，支路到支路。连接类型支持单向、双向、广播和环回交叉。
	保护	具备交叉板冗余保护功能。
	通道保护能力	具备一个或者多个级别ODUk通道的保护和恢复协调能力,倒换时间在50ms以内。
设备功能	合分波器	合波器/分波器、梳状滤波器、光放大器、光监控信道等技术性能应满足《160/80x10Gbit/s波分复用系统技术规范》、《40/80x40Gbit/s波分复用系统技术规范》和《80x100Gbits波分复用系统技术规范》要求。
	波长转换器和TMUX	在OTN系统中没有进入光电交叉设备直接进行波长转换的，波长转换器和TMUX等设备的技术性能应满足《160/80x10Gbit/s波分复用系统技术规范》、《40/80x40Gbit/s波分复用系统技术规范》和《80x100Gbits波分复用系统技术规范》要求。
	电层业务调度类型和能力	具备MPLS-TP、以太网、VC等多种业务调度。投标方应详细说明投标设备支持的业务调度类型。
		设备应采用统一的、集中型多业务电层调度芯片或多个不同调度类型的集中调度模块，实现对多种业务的调度。

		VC交叉调度功能模块支持VC通道交叉处理能力，并支持高阶通道VC4级别的虚级联或连续级联功能，具体要求应符合YD/T 1022-1999和YDN 099-1998中的相应规定。
		应具备根据不同业务调度需求选择不同的业务处理流程，至少应包括： 流程一：ODUk交叉调度方式，业务经过ODUk接口适配处理模块封装映射后直接通过ODUk交叉调度模块调度； 流程二：业务经过VC交叉或分组交换后再经ODUk接口适配处理模块封装映射后接着通过线路接口处理模块处理； 流程三：业务通过分组交换或VC交叉模块调度后再经过ODUk接口适配处理模块封装后再通过大容量ODUk核心交叉调度模块统一调度。
	以太网业务类型	以太网点到点专线（E-LINE）业务功能和性能测试
		以太网专网（E-LAN）业务
		以太网根基多点（E-Tree）业务
	以太网交换处理基本功能	a) 传输链路带宽可配置
		b) 应实现转发/过滤以太网数据帧的功能，该功能应符合IEEE 802.1协议的规定
		c) 必须能够识别IEEE 802.1规定的数据帧，并根据VLAN信息转发/过滤数据帧；
		d) 提供自学习和静态配置两种可选方式维护MAC地址表
		e) 支持IEEE802.1生成树协议（STP）
		f) 支持多链路聚合（LAG）来实现灵活的高带宽和链路冗余，实现多链路聚合应符合IEEE 802.1AX
		g) 支持以太网端口流量控制。
	业务转发	应支持根据端口或者端口+VLAN静态转发（EPL或者EVPL），或者根据MAC或者VLAN+MAC动态学习转发（EPLAN或者EVPLAN），具体见YD/T 1948.3-2010 《传送网承载以太网（EoT）技术要求 第3部分：以太网业务框架》以及YD/T 1948.5-2011 《传送网承载以太网（EoT）技术要求 第5部分：以太网专线（EPL）业务和以太网虚拟专线（EVPL）业务》的规定。
	VLAN	应支持客户C-VLAN和运营商S-VLAN的透传、交换、添加、剥离处理，提供基于端口和基于VLAN进行转发的业务处理。
		对VLAN的处理符合IEEE 802.1ad的要求。
	MPLS-TP交换处理功能	基于PW/LSP标签进行业务转发，具体机制应符合YD/T 2374-2011第4.3节要求。
		支持将客户侧信号映射到PW和LSP中，具体机制应符合YD/T 2374-2011第5章要求。
		在以太网QoS的基础上，支持基于PW/LSP标签和优先级的流分类和各种QoS策略，包括流量监管、流量整形、拥塞控制和队列调度，具体机制应符合YD/T 2374-2011第8章规范。
		支持MPLS-TP层网络的OAM机制，包括故障检测和性能监测，具体机制应符合 YD/T 2374-2011第7章要求
网络保护		Pe-OTN网络中的光波长传送层、OTN传送层和分组传送层，各自支持相应的网络保护机制，并且不同层之间的网络保护机制相互独立。

		MPLS-TP传送层应支持YD/T 2374-2011的第6章规范的LSP 1:1和1+1线性保护和PW双归保护;
		Pe-OTN网络的SDH传送子层可选支持ITU-T G.841规范的SNCP和ITU-T G.842规范的共享环网保护，主要应用在Pe-OTN与基于SDH的MSTP互通组网场景下。
OAM		Pe-OTN设备支持MPLS-TP的OAM应分为PW OAM、LSP OAM、段层OAM（可选）、OTN层OAM（包括OPUk/ODUk/OTUk开销）。Pe-OTN网元还应支持以太网和STM-N的接入链路OAM机制
QoS		Pe-OTN网络的MPLS-TP分组传送子层或以太网传送子层应具备QoS 功能应包括流分类和流标记、流量监管、拥塞管理、队列调度、流量整形、连接允许功能等。投标方应说明投标设备都支持上述哪些QoS功能。
网络管理	拓扑管理	PE-OTN拓扑管理应在YD/T 1289.2-2003 6.1.2节基础上支持“网络拓扑视图”功能。网络拓扑视图包括对象显示和实时告警显示，各视图之间可无障碍切换，支持拓扑搜索和手工创建两种方式建立网络拓扑视图
	配置管理	a)支持各类业务配置管理功能
		b）应支持层间适配配置管理功能
		c)应支持各个层次的OAM配置管理
		d) 应支持各个层次的保护机制以及层间保护协调机制的配置管理
		e) MPLS-TP的配置管理要求应符合YD/T 2374-2011的第11.2.2节的规范
	告警管理	Pe-OTN网管系统应支持基本的故障管理功能，具体要求参见YD/T 1289.2-2003 6.1.4
	性能管理	PE-OTN网管性能管理功能应包括：性能监测参数、性能监测管理、性能数据上报管理、性能门限管理、性能数据查询、性能数据存储、性能趋势分析。具体要求参见YD/T 1289.2-2003 6.1.5节。
同步功能要求		应满足《OTN网络同步技术要求》相关要求。
资质要求		提供工信部设备入网证
		符合ISO9001和ISO9002系列标准的要求

3.3 核心路由器

指标项	指标要求
设备性能	满配置下交换容量≥130Tbps，转发性能≥25000Mpps，提供产品官网链接及网页截图、官方彩页材料作为证明材料
设备架构	设备支持双主控且满配，具备双主控双电源冗余，要求所有业务板卡及电源、风扇均可热插拔，提供产品官网链接及网页截图、官方彩页材料作为证明材料
	整机业务载板插槽≥14 个；单槽位最大支持 200G 线速转发不丢包，提供第三方测试报告作为证明材料
接口类型	设备支持 100GE、50GE、40GE、25GE、10GE、GE、FE、E1、POS、CPOS 等接口类型

	具备端口散列技术，可将 100GE 端口散列成 10GE 口或者 25GE 口进行使用，可灵活进行设备的端口容量和类型控制使用，提供第三方测试报告作为证明材料并加盖厂商公章或投标专用章
基本功能	具备 RIP、OSPF、IS-IS、BGP 等路由协议，具备 L2VPN、L3VPN、EVPN 等 VPN 技术，具备 LDP LSP、RSVP-TE、SR-TE 等 MPLS 技术
	具备 IPv4 静态路由、OSPF、IS-IS、BGP 等路由协议，VxLAN、GRE 等隧道技术；具备 IPv6 静态路由，BGP4+、OSPFv3、IS-ISv6 等动态路由协议，IPv4 over IPv6 隧道和 6PE，NAT44(4)、NAT64，静态 IPv6 DNS，指定 IPv6 DNS 服务器，TFTP IPv6 client
IPv6	具备 IPv6 路由协议，包括静态路由、OSPFv3、IS-ISv6、BGP4+等协议，支持 IPv6 终端的 接入、IPv6 访问控制列表和基于 IPv6 的策略路由；支持 IPv4 和 IPv6 双协议栈和 IPv4/IPv6 过渡技术
SR	具备 SRv6 TE policy 的流量统计功能，支持动态下发 EVPN IPv4 L3VPN over SRv6 TE policy 功能，实现 SRv6 承载 L3VPN 业务场景，提供第三方测试报告作为证明材料并加盖厂商公章或投标专用章
可靠性	具备基于硬件的 BFD 故障探测技术，误码倒换，IP/IPv6/LDP/TE/VPN/VPNv6 FRR 快速重路由，端口聚合，ECMP、UCMP，LDP，VRRP，NSR，关键部件冗余备份，组件可热拔插，平滑重启（GR），不中断转发（NSF），ISSU
QoS	具备多级 MPLS H-QoS，MPLS VPN、VLL 和 PWE3 的 QoS 调度，面向 TE 隧道的 QoS；具备通过网络切片或其它网络基础资源隔离技术，将网络划分为多个独立的逻辑业务平面以进行业务隔离，每个平面拥有独立的带宽资源，各独立平面间的带宽不能相互抢占
OAM	支持随业务流的智能检测技术，实现基于 IP 五元组筛选追踪业务流，对丢包、误码类故障进行实时检测，精准定位到故障点；支持 EFM、CFM、Y.1731、MPLS-TP OAM 技术，提供官方产品手册中对该功能的配置说明截图作为证明材料
可维护性	支持 Telemetry，可实现从设备高速采集数据的技术，设备通过推模式（Push Mode）周期性的向采集器上送设备的接口流量统计、CPU 或内存数据等信息，提升用户进行网络大数据分析能力；支持随流的性能检测技术，即不额外发送检测报文，对用户业务流进行直接的丢包、时延的监测，得到业务端到端或逐跳的丢包和时延信息，支持通过 telemetry 上送获得的性能数据；提供第三方测试报告或提供官方产品手册中对该功能的配置说明截图作为证明材料并加盖厂商公章或投标专用章
系统安全	支持 BGP 监控协议 BGP Monitoring Protocol（BMP）（RFC 7854），能够对网络中设备的 BGP 运行状态进行实时监控，实现针对网络的路由安全追踪，路由事件回溯和网络安全剖析
	支持 MACSec 加密技术，提供第三方测试报告作为证明材料并加盖厂商公章或投标专用章
系统管理	支持 Console、Telnet、SSH 等管理方式
资质要求	投标产品的关键芯片（包括 CPU、NP、TM、TCAM、FIC 及交换芯片等）采用自研国产化芯片，提供第三方测试报告作为证明材料并加盖厂商公章或投标专用章
配置要求	2 台区核心 A 路由器要求每台不少于 6 个 100GE 接口，1 个 100GE 堆叠线，1 个 100GE 单模模块；4 个 100GE 多模模块， 2 台路由器要求每台不少于 6 个 100GE 接口，10 个 10GE 接口，1 个 100GE 堆叠线，5 个 100GE 多模模块，10 个 10GE 多模模块
服务及质保要求	自验收合格之日起，含 3 年产品原厂标准维保服务，并提供原厂针对本项目的授权函和三年原厂售后服务承诺函

3.4 核心边界路由器

指标项	指标要求
设备性能	满配置下交换容量≥130Tbps，转发性能≥25000Mpps，提供产品官网链接及网页截图、官方彩页材料作为证明材料
设备架构	设备支持双主控且满配，具备双主控双电源冗余，要求所有业务板卡及电源、风扇均可热插拔，提供产品官网链接及网页截图、官方彩页材料作为证明材料
	整机业务载板插槽≥14 个；单槽位最大支持 200G 线速转发不丢包，提供第三方测试报告作为证明材料
接口类型	设备支持 100GE、50GE、40GE、25GE、10GE、GE、FE、E1、POS、CPOS 等接口类型
	具备端口散列技术，可将 100GE 端口散列成 10GE 口或者 25GE 口进行使用，可灵活进行设备的端口容量和类型控制使用，提供第三方测试报告作为证明材料并加盖厂商公章或投标专用章
基本功能	具备 RIP、OSPF、IS-IS、BGP 等路由协议，具备 L2VPN、L3VPN、EVPN 等 VPN 技术，具备 LDP LSP、RSVP-TE、SR-TE 等 MPLS 技术
	具备 IPv4 静态路由、OSPF、IS-IS、BGP 等路由协议，VxLAN、GRE 等隧道技术；具备 IPv6 静态路由，BGP4+、OSPFv3、IS-ISv6 等动态路由协议，IPv4 over IPv6 隧道和 6PE，NAT44(4)、NAT64，静态 IPv6 DNS，指定 IPv6 DNS 服务器，TFTP IPv6 client
IPv6	具备 IPv6 路由协议，包括静态路由、OSPFv3、IS-ISv6、BGP4+等协议，支持 IPv6 终端的 接入、IPv6 访问控制列表和基于 IPv6 的策略路由；具备 IPv4 和 IPv6 双协议栈和 IPv4/IPv6 过渡技术
SR	具备 SRv6 TE policy 的流量统计功能，具备动态下发 EVPN IPv4 L3VPN over SRv6 TE policy 功能，实现 SRv6 承载 L3VPN 业务场景，提供第三方测试报告作为证明材料并加盖厂商公章或投标专用章
可靠性	支持基于硬件的 BFD 故障探测技术，误码倒换，IP/IPv6/LDP/TE/VPN/VPNv6 FRR 快速重路由，端口聚合，ECMP、UCMP，LDP，VRRP，NSR，关键部件冗余备份，组件可热拔插，平滑重启（GR），不中断转发（NSF），ISSU
QoS	具备多级 MPLS H-QoS，MPLS VPN、VLL 和 PWE3 的 QoS 调度，面向 TE 隧道的 QoS；具备通过网络切片或其它网络基础资源隔离技术，将网络划分为多个独立的逻辑业务平面以进行业务隔离，每个平面拥有独立的带宽资源，各独立平面间的带宽不能相互抢占
OAM	支持随业务流的智能检测技术，实现基于 IP 五元组筛选追踪业务流，对丢包、误码类故障进行实时检测，精准定位到故障点；支持 EFM、CFM、Y.1731、MPLS-TP OAM 技术，提供官方产品手册中对该功能的配置说明截图作为证明材料
可维护性	支持 Telemetry，可实现从设备高速采集数据的技术，设备通过推模式（Push Mode）周期性的向采集器上送设备的接口流量统计、CPU 或内存数据等信息，提升用户进行网络大数据分析能力；支持随流的性能检测技术，即不额外发送检测报文，对用户业务流进行直接的丢包、时延的监测，得到业务端到端或逐跳的丢包和时延信息，支持通过 telemetry 上送获得的性能数据；提供第三方测试报告或提供官方产品手册中对该功能的配置说明截图作为证明材料并加盖厂商公章或投标专用章
系统安全	支持 BGP 监控协议 BGP Monitoring Protocol（BMP）（RFC 7854），能够对网络中设备的 BGP 运行状态进行实时监控，实现针对网络的路由安全追踪，路由事件回溯和网络安全剖析

	支持 MACSec 加密技术，提供第三方测试报告作为证明材料并加盖厂商公章或投标专用章
系统管理	支持 Console、Telnet、SSH 等管理方式
资质要求	投标产品的关键芯片（包括 CPU、NP、TM、TCAM、FIC 及交换芯片等）采用自研国产化芯片，提供第三方测试报告作为证明材料并加盖厂商公章或投标专用章
配置要求	不少于 6 个 100GE 接口（可自适应成 40GE 接口），10 个 10GE 接口，1 个 100GE 堆叠线，1 个 100GE 多模模块，1 个 100GE 单模模块，2 个 40GE 多模模块，10 个 10GE 多模模块
服务及质保要求	自验收合格之日起，含 3 年产品原厂标准维保服务，并提供原厂针对本项目的授权函和三年原厂售后服务承诺函

3.5 汇聚路由器

指标项	指标要求
设备性能	满配置下交换容量≥110Tbps，转发性能≥14000Mpps，提供产品官网链接及网页截图、官方彩页材料作为证明材料
设备架构	设备支持双主控且满配，具备双主控双电源冗余，要求所有业务板卡及电源、风扇均可热插拔，提供产品官网链接及网页截图、官方彩页材料作为证明材料
	整机业务载板插槽≥8 个，支持单槽位 200G 线速转发不丢包，提供第三方测试报告及相关板卡的功能、性能详细说明
接口类型	设备支持 100GE、50GE、40GE、25GE、10GE、GE、FE、E1、POS、CPOS 等接口类型
	具备端口散列技术，可将 100GE 端口散列成 10GE 口或者 25GE 口进行使用，可灵活进行设备的端口容量和类型控制使用，提供第三方测试报告作为证明材料
基本功能	具备 RIP、OSPF、IS-IS、BGP 等路由协议，具备 L2VPN、L3VPN、EVPN 等 VPN 技术，具备 LDP LSP、RSVP-TE、SR-TE 等 MPLS 技术
	具备 IPv4 静态路由、OSPF、IS-IS、BGP 等路由协议，VxLAN、GRE 等隧道技术；具备 IPv6 静态路由，BGP4+、OSPFv3、IS-ISv6 等动态路由协议，IPv4 over IPv6 隧道和 6PE，NAT44(4)、NAT64，静态 IPv6 DNS，指定 IPv6 DNS 服务器，TFTP IPv6 client
	IPv4、Ipv6 路由及转发表容量要求：支持 IPv4 路由表容量≥10M,IPv6 路由表容量≥5M，支持 IPv4 转发表容量≥4M,IPv6 转发表容量≥2M
IPV6 演进	具备 SRv6 TE policy 的 ping/tracert 功能 ,以实现设备基本运维能力 ,具备 SRv6 TE policy 的 FRR 功能，以实现设备可靠性，提供第三方测试报告作为证明材料并加盖厂商公章或投标专用章
可靠性	具备基于硬件的 BFD 故障探测技术，支持最小发包间隔 5ms
系统安全	支持 MACSec 加密技术，提供第三方测试报告作为证明材料
可维护性	支持对随流检测获取到的性能数据进行可视化的管理；支持设置告警阈值，对指标越限的链路、网元和端口进行告警
业务保障	具备 5 级 H-QoS 调度，支持通过基于时隙隔离的网络硬切片技术，开通具备独立带宽资源、不被抢占的逻辑网络，严格保证高优先级业务的 SLA 和安全性。提供第三方测试报告或提供官方产品手册中对该功能的配置说明截图作为证明材料并加盖厂商公章或投标专用章
资质要求	投标产品的关键芯片（包括 CPU、NP、TM、TCAM、FIC 及交换芯片等）采用自研国产化芯片，提供第三方测试报告作为证明材料并加盖厂商公章或投标专用章

配置要求	不少于 4 个 100GE 接口（可自适应成 40GE 接口），1 个 100GE 堆叠线，2 个 100GE 多模模块，1 个 40GE 多模模块
服务及质保要求	自验收合格之日起，含 3 年产品原厂标准维保服务，并提供原厂针对本项目的授权函和三年原厂售后服务承诺函

3.6 接入收敛汇聚交换机

指标项	指标要求
设备性能	交换容量≥200Tbps，包转发率≥10000Mpps，提供产品官网链接及网页截图、官方彩页材料作为证明材料
单板槽位	主控引擎与交换网板物理分离；主控引擎≥2；独立交换网板≥2；整机业务板槽位数≥4
硬件要求	为了适应机柜并排部署，采用机箱（包括业务板卡区）后出风风道设计
	为保证设备散热效果和可靠性，要求设备支持模块化风扇框，可热插拔，当单个风扇框发生故障时，有其他风扇正常运行，保证设备散热，独立风扇框数≥2
虚拟化技术	支持横向虚拟化技术，将多台设备虚拟为一台，支持长距离集群
VxLAN	支持 VxLAN 功能，支持 VxLAN 二层网关、三层网关，支持 BGP EVPN，支持分布式 Anycast 网关，支持 VxLAN Fabric 的自动化部署
IP 路由	支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6
配置要求	不少于 6 个 100GE 接口（可自适应到 40GE 接口），96 个 10GE 接口（可自适应到 GE 接口），1*40GE 堆叠线，1*40GE 多模模块，2 个独立交换网板，双主控，双电源
服务及质保要求	自验收合格之日起，含 3 年产品原厂标准维保服务，并提供原厂针对本项目的授权函和三年原厂售后服务承诺函

3.7 万兆接入交换机

指标项	指标要求
设备性能	交换容量≥400Gbps，包转发率≥140Mpps，提供产品官网链接及网页截图、官方彩页材料作为证明材料
电源	为了提高设备可靠性
端口类型	≥48 个千兆电口，≥4 个万兆 SFP+，2*10GE 单模模块；
三层功能	支持 RIP、RIPng、OSPF、OSPFv3 路由协议
安全	支持防止 DOS、ARP 攻击功能、ICMP 防攻击；支持端口隔离、端口安全、Sticky MAC；支持 IP、MAC、端口、VLAN 的组合绑定
虚拟化	支持纵向虚拟化
产品资质	提供工信部入网证
服务及质保要求	自验收合格之日起，含 3 年产品原厂标准维保服务。

3.8 千兆接入交换机

指标项	指标要求
设备性能	交换容量≥400Gbps，包转发率≥80Mpps，提供产品官网链接及网页截图、官方彩页材料作为证明材料
端口类型	≥48 个千兆电口，≥4 个千兆 SFP，2*GE 单模模块；
三层功能	支持 RIP、RIPng、OSPF、OSPFv3 路由协议
安全	支持防止 DOS、ARP 攻击功能、ICMP 防攻击；支持端口隔离、端口安全、Sticky MAC；支持 IP、MAC、端口、VLAN 的组合绑定
虚拟化	支持纵向虚拟化
产品资质	提供工信部入网证
服务及质保要求	自验收合格之日起，含 3 年产品原厂标准维保服务。

3.9 市政务外网边界交换机

指标项	指标要求
设备性能	交换容量≥2Tbps，包转发率≥700Mpps
设备配置	≥24 个万兆 SFP+，≥6 个 40GE QSFP+，1*40GE 堆叠线（2 台共 1 根）；1*40GE 多模模块；4*10GE 多模模块；2 块电源；
硬件	为了提高设备散热性能，支持可插拔风扇框
二层	支持 4K 个 VLAN，支持 Guest VLAN、Voice VLAN，支持基于 MAC/协议/IP 子网/策略/端口的 VLAN
三层	支持静态路由、RIP V1/2、OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6
用户管理	支持统一用户管理功能，支持 802.1X/MAC/Portal 等多种认证方式，支持 10000 认证用户同时在线
VxLAN	支持 VxLAN 功能，支持 BGP EVPN，支持分布式 Anycast 网关；支持控制器基于 WEB 界面进行 VxLAN Fabric 配置并下发给交换机
虚拟化	支持横向堆叠
管理维护	支持 SNMPv1/v2c/v3
安全	支持防 ARP 攻击、DOS 攻击、ICMP 防攻击、CPU 防攻击
可靠性	支持 G.8032 标准环网协议
资质	提供工信部入网证
服务及质保要求	自验收合格之日起，含 3 年产品原厂标准维保服务。

3.10 专网边界交换机

指标项	指标要求
设备性能	交换容量≥2Tbps，包转发率≥700Mpps
设备配置	≥24 个万兆 SFP+，≥6 个 40GE QSFP+，1*10GE 堆叠线，4*10GE 多模模块，2 块电源
硬件	为了提高设备散热性能，支持可插拔风扇框
二层	支持 4K 个 VLAN，支持 Guest VLAN、Voice VLAN，支持基于 MAC/协议/IP 子网/策略/端口的 VLAN
三层	支持静态路由、RIP V1/2、OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6
用户管理	支持统一用户管理功能，支持 802.1X/MAC/Portal 等多种认证方式，支持 10000 认证用户同时在线
VxLAN	支持 VxLAN 功能，支持 BGP EVPN，支持分布式 Anycast 网关；支持控制器基于 WEB 界面进行 VxLAN Fabric 配置并下发给交换机
虚拟化	支持横向堆叠
管理维护	支持 SNMPv1/v2c/v3
安全	支持防 ARP 攻击、DOS 攻击、ICMP 防攻击、CPU 防攻击
可靠性	支持 G.8032 标准环网协议
资质	提供工信部入网证
服务及质保要求	自验收合格之日起，含 3 年产品原厂标准维保服务。

3.11 安全管理中心交换机

指标项	指标要求
设备性能	交换容量≥2Tbps，包转发率≥700Mpps
设备配置	≥24 个万兆 SFP+，≥6 个 40GE QSFP+，1*10GE 堆叠线，4*10GE 多模模块，2 块电源
硬件	为了提高设备散热性能，支持可插拔风扇框
二层	支持 4K 个 VLAN，支持 Guest VLAN、Voice VLAN，支持基于 MAC/协议/IP 子网/策略/端口的 VLAN
三层	支持静态路由、RIP V1/2、OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6

用户管理	支持统一用户管理功能，支持 802.1X/MAC/Portal 等多种认证方式，支持 10000 认证用户同时在线
VxLAN	支持 VxLAN 功能，支持 BGP EVPN，支持分布式 Anycast 网关；支持控制器基于 WEB 界面进行 VxLAN Fabric 配置并下发给交换机
虚拟化	支持横向堆叠
管理维护	支持 SNMPv1/v2c/v3
安全	支持防 ARP 攻击、DOS 攻击、ICMP 防攻击、CPU 防攻击
可靠性	支持 G.8032 标准环网协议
资质	提供工信部入网证
服务及质保要求	自验收合格之日起，含 3 年产品原厂标准维保服务。

3.12 DNS 域名服务器

序号	指标项		参数要求
1	设备要求	IPv6 资质	设备要求具备 IPv6 解析功能，具备“IPV6 Ready Logo Certified”认证（须提供证明材料并加盖原厂商公章）
2	设备参数	网络接口	接口不少于 6 个千兆电口、2 个万兆光口，板载带外网管口支持 IPMI V2.0、板载冗余双电源模块（支持带外网管口镜像安装和远程开关机）
3		CPU、内存及硬盘	内存不低于 32G，硬盘容量不低于 1TB
4		LED 控制面板	具有按键可操作 LED 液晶状态指示屏，提供管理 IP 地址配置
5		软件操作系统	设备系统软件必须为完全自主研发、非开源软件修改，支持分层架构部署模式。（提供软件知识产权证书复印件并加盖原厂商公章）
6		解析服务性能	开启解析日志（Query log）时 DNS 解析服务性能不低于 15 万 QPS
7		安全防护性能	单台设备要求开启解析日志（Query log）时安全防护性能不低于 30 万 PPS/QPS（提供证明材料并加盖原厂商公章）
8		DHCP 性能	单台设备可扩展支持 DHCP 性能不低于 1000LPS
9	设备运维管理	HA 部署模式	设备支持 HA 模式，设备 HA 切换支持 1 秒级切换
10		Cluster 部署模式	设备支持 Cluster 模式。支持配置管理单独部署。在 cluster 模式下，各设备部署采用加密通讯方式。
11		Anycast 部署模式	设备支持 Anycast 部署模式，设备可实现在线实时扩容，保障业务的独立平稳运行。
12		重点域名监控	支持重点域名主动监控管理，管理重要的域名资产一旦发现与设定的域名/ip 地址对不同，及时日志、邮件告警。

13		域名定义启用生效时间	支持域名在指定时间启用服务和禁用，满足临时域名上线和收回的功能。
14		设备集中采用节点实 IP 地址管理模式	支持所有设备的统一集中管理，基于节点实 IP 地址统一的管理并下发配置，配置下发基于事务级同步方式，并能保证配置数据一致性。支持新增的节点设备加入某个集群可自动获得该集群的全部配置。
15		网络中断恢复后配置同步	任意节点网络异常时，不能下发的配置要在网络恢复后成功下发，保证配置的可靠下发。
16		配置管理	具备一键备份功能，用户可随时执行对系统的业务策略进行整体备份。同时可一键恢复，回退到用户配置的还原点，提供定时备份功能。
17		图形化管理	采用可视化全中文 WEB 操作界对所有服务节点进行集中管理 ，同时支持 SSH 协议进行管理。
18		登录用户认证管理	具备管理账户同认证系统 Radius、Tacas+、LDAP 联动。
19			支持多用户，并根据不同用户分配不同操作权限。管理账户可拥有直接最高管理权限。
20		登录安全控制	支持设置系统的白名单，仅白名单中的 IP 可登录系统，确保系统安全。
21			支持设定系统的服务 IP 和管理 IP，只允许用户通过服务 IP 使用 DNS 服务，通过管理 IP 访问管理界面对系统进行管理。支持设置账号有效期。支持登录 IP 白名单
22			支持对系统用户进行角色管理和细分权限设置，例如管理员角色可对所有集群和域进行配置，全域管理员角色可对所有域进行配置，域管理员角色只能对指定域进行配置。
23		日志管理	具备操作日志的完整记录与查询，包括登录日志、DNS 配置变更日志等。
24			具备自动定期备份系统配置到本地或远程服务器，并可使用配置文件进行恢复。
25		报表管理	具备丰富的图形报表展示功能，至少包括 DNS 请求流量、应答流量、授权流量、递归流量等业务数据，对于授权流量需支持按域进行展示。
26			具备 TOPN 排名、支持域的 TOP 排名、支持域名的 TOPN 排名、支持源 IP 的 TOP 排名。
27			对于被系统安全过滤的流量可通过图形报表展示，至少应包括各类异常报文、攻击报文及系统过滤流量等。
28			支持单位时间内请求客户端 MAC 地址的 TOPN 统计。
29			支持 LPS、网络流量和终端类型等按时段、图形化统计，并要求能生成和导出统计报告。
30	DDI 管理功能	权威功能	系统必须支持标准的 DNS 服务，支持正向解析、反向解析功能。支持对 NS、SOA、A、AAAA、MX、CNAME、SPF、PTR、TXT、SRV 等全面记录的解析。支持暂停、启用操作。
31			对授权记录管理支持暂停、启动操作；支持各种授权记录的批量操作。
32			具备 A、AAAA 记录同 PTR 的操作联动。
33			支持根据用户所属运营商线路返回权威域在对应运营商下的解析结果。

34			对授权记录管理支持暂停/启动操作，支持各种授权记录的批量操作。
35			智能化的访问调度，支持 DNS 多种负载均衡算法包括：来源就近算法、优先可用算法、返回备用 IP 算法、加权比率算法等。
36			提供运营商及各省市精确 IP 地址库，IP 地址库可以不断更新，以精确识别用户所属运营商。
37		递归功能	支持单独启用或停止递归功能。
38			支持本地递归查询和外网递归转发;提供全面的 DNS 记录类型的递归解析服务；支持指定请求类型过滤；支持指定解析类型重定向。
39			支持设置基于视图的递归请求的源地址。
40			支持指定域或者域名转发指定线路解析资源，同时可与源 IP 地址结合使用。
41			支持基于线路、用户、内容等单一或组合策略进行的调度功能。
42			提供智能 DNS 解析服务,根据不同区域的 DNS 请求,返回最佳解析结果;智能访问流量调度，根据不同访问的用户源，实现对终端访问多中心、多线路智能流量调度。
43			支持限速的转发功能。
44		缓存功能	缓存支持全局的 TTL 控制策略；支持对每个域的 TTL 控制策略；支持对每个域名的 TTL 控制策略；支持 TTL 优先级控制。
45			支持缓存智能更新,当热点域名缓存即将过期时,系统会预先进行更新。
46			支持按视图的域/域名/全局 DNS 转发功能；支持对转发服务器配置权重；支持对转发服务器进行健康检查；DNS 转发支持 ECS 配置。
47			支持异网业务地址解析，对非本地业务地址发起的 DNS 请求进行解析（如：8.8.8.8）。
48		健康检查	支持基于数据中心的 DNS 会话保持功能。
49			设备支持与 DNS 系统进行联动的健康检查功能，至少包括 ICMP、TCP、HTTP 内容、数据库等探测方式。
50			可以要求支持用户自定义模板，支持重点域名监控功能：对重点域名的资源记录进行监测，同时定义重点域名对应的 IP 地址群（经过人工校验后确认的数据），当有变化的时候，且变化后的内容不在给定的 IP 地址群中，则输出日志发告警并进行校验。
51		DHCP 功能	具备将地址池租赁地址转换为固定地址，方便快速进行 IP 和 MAC 的固定化使用。
52			具备 IP 地址动态分配、固定分配，提供灵活的租约管理。支持指定预留 IP 段，为 IP 地址规划提供便捷管理。
53			具备 DHCP 自动绑定功能,客户端初次分配 IP 地址后,后续再次接入时,获得同一 IP 地址分配。
54			具备 MAC 地址访问控制，支持 MAC 黑白名单。
55			提供 DHCP 指纹库，智能识别各种类型的终端。
56			设备具备 DHCP Failover 技术，提供 DHCP 服务异地备灾的功能，当一台异常时另外一台支持一键接管全部租赁服务。

57			支持基于 MAC、指纹信息、OPTION 设置 DHCP 访问控制策略，支持 DHCP 限速功能，针对 DHCP 特点对 Discover 类型请求限速。
58			DHCP 非法服务器探测：自动发现非法 DHCP 服务器并告警。
59			具备 DHCP 模板，可根据模板批量生成地址池，模板可指定地址池起止地址。支持地址池的批量导入、导出。
60		IP 地址管理功能	具备 IPv4、IPv6 双栈。
61			具备对单个 IP 地址探测;支持对 IP 地址段内的所有 IP 地址进行探测。
62			具备图形和列表展示，图形展示中，对指定 IP 段内的 IP 地址按照各种状态使用不同的颜色展示；列表展示中对每一个 IP 地址列出详细的属性。
63	高级安全防护	安全防护功能	产品应集成高性能专用 DNS 安全防护功能,提供内置安全模块 DNS 安全防护，以避免对 UDP 包产生瓶颈。
64			产品应集成高性能专用 DNS 安全防护功能，不接受内置防火墙实现的 DNS 安全防护，以避免对 UDP 包产生瓶颈。
65			具备按视图进行 DNS 请求类型过滤。
66			具备系统级的高级 ACL 安全防护。
67			具备对 IP 异常包、UDP 异常包、DNS 异常包进行识别和拦截。
68			具备对于源 IP 的流量限速，支持对于域名的流量限速，具备对于域的流量限速，支持对于递归流量的限速。
69			具备 DNS 缓存投毒防护。
70			具备 DDOS 攻击防护，具备 DDOS 攻击防护统计展示，至少包括攻击源 IP、域名、频次的展现
71			具备 DNSSEC 安全扩展,对所访问的站点地址有效性进行验证,提升 DNS 业务安全性；能够针对单个 IP 或一个地址段进行 DNS 响应速率限制。

四、网络安全设计要求

4.1 互联网区域设计

为了保证各委办局部门的移动办公、远程访问、现场执法等业务能安全接入到电子政务外网，也为了保证相关企事业单位和个人能利用互联网安全地接入到电子政务外网，金山区设置互联网区域并部署抗 DDoS 攻击、网络访问控制、入侵检测和防御、防病毒、APT 检测、日志审计等相关设备。

本次互联网区域已经进行过前期建设，对照市大数据中

心指南发现已经符合要求，互联网区域已建设的设备不在本次方案考虑范围。需建设探针设备的参数要求如下：

4.1.1 探针

数量	1 台
技术指标	参数指标要求
接口数量	不低于 6 个千兆电口，4 个千兆光口，2 个万兆光口
尺寸	2U
性能指标	应用层吞吐不低于 3G
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。
基础检测功能	具备报文检测引擎,可实现 IP 碎片重组、TCP 流重组、应用层协议识别与解析等, 具备多种的入侵攻击模式或恶意 URL 监测模式,可完成模式匹配并生成事件,可提取 URL 记录和 域名记录,在特征事件触发时可以基于五元组和二元组(IP 对)进行原始报文的录制。
监测识别规则库	能够识别应用类型超过 1100 种，应用识别规则总数超过 3000 条，具备亿万级别 URL 识别能力。漏洞利用规则特征库数量在 4000 条以上，漏洞利用特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，影响系统，对应 CVE 编号。
异常流量检测	支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括 3389、53、80/8080、21、69、443、25、110、143、22 等（需提供产品功能截图证明）。
深度监测能力	可提供网络流量的会话级视图,根据网络流量的正常行为轮廓特征建立正常流量模型,判别流量是否出现异常,对原始流记录进行异常检测,可发现网络蠕虫、网络水平扫描、网络垂直扫描、IP 地址扫描，端口扫描，ARP 欺骗，IP 协议异常报文检测和 TCP 协议异常报文等常见网络异常流量事件类型。
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（需提供产品功能截图证明）。 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；（要求对以上列出的攻击类型进行逐条响应并提供相应的功能界面截图证明，并加盖厂商公章）。 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。
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。 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。
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。
流量记录	能够对网络通信行为进行还原和记录，以供安全人员进行取证分析，还原内容包括：TCP 会话记录、Web 访问记录、SQL 访问记录、DNS 解析记录、文件传输行为、LDAP 登录行为。
抓包分析	支持通过设备对流量进行抓包分析，可定义抓包数量、接口、IP 地址、端口或自定义过滤表达式。
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。
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。
服务及质保要求	自验收合格之日起，含 3 年产品原厂标准维保服务，并提供原厂针对本项目的授权函和三年原厂售后服务承诺函

4.2 市政务外网区域设计

金山区电子政务外网需接入市政务外网，应设置安全边界，实现网络访问控制能力，阻断非法访问。市政务外网区域需实现网络访问控制、入侵检测和防御、防病毒、APT 检测、日志审计等功能。需建设相关设备参数配置不得低于如下标准：

4.2.1 防火墙(含入侵检测及防毒墙模块)

市政务外网防火墙		**2 台**
指标	**指标项**	**详细要求**
基本要求	系统结构	产品由专用的硬件平台、安全操作系统及功能软件构成。设备采用自主知识产权的专用安全操作系统，采用多核多平台并行处理机制；
	系统软件	系统具有良好的扩展性，支持扩展病毒防御、入侵防御、应用

		识别、网站分类库过滤、WAF、IPSEC VPN、SSLVPN 等功能，本次要求支持病毒防御和入侵防御模块。
系统性能	防火墙吞吐	防火墙吞吐量：100Gbps、应用层吞吐量：80Gbps、全威胁吞吐量：18Gbps、并发连接数：3000 万、HTTP 新建连接速率：70 万
硬件配置	机箱	设备不得超过 2U 标准高度；
	电源	设备配置模块化双冗余电源；
	接口配置	设备不少于 6 个端口扩展卡插槽，为了便于维护，所有扩展卡插槽均要求位于设备前面板；前面板具有独立的带外管理口与双机心跳口以及 2 个 USB 接口；配置 1T 硬盘和液晶屏。 本次配置 2 个 40GE（SFP+）含模块，4 个 SFP+含模块，4 个 SFP 含模块，6 个千兆电口。
网络接入	工作模式	支持路由、交换、虚拟线、Listening、混合工作模式；
	路由交换	支持静态路由、RIP、RIPNG、OSPFv2/v3、BGP、ISP 路由，内置移动、联通、电信、教育网、网通、长城宽带等 ISP 供应商地址列表，可通过 Web 界面选择不同的 ISP 供应商实现快速切换；
		支持 802.1q、QinQ 模式；
		支持根据入接口、源/目的 IP 地址/地址对象、源/目的端口、协议、用户、应用、选路算法、探测、度量值、权重等多种条件设置策略路由；
	链路聚合	支持手动和 LACP 链路聚合，可根据源/目的 mac、源/目的 IP、源/目的端口、五元组、端口轮询等条件提供不少于 10 种链路负载算法。
	IP/MAC 绑定	支持 IPv4/v6 双栈 IP/MAC 静态和动态探测绑定，支持跨三层绑定，支持 IP/MAC 绑定表导入导出；
	地址转换	支持一对一 SNAT、多对一 SNAT、一对一 DNAT、双向 NAT、NoNAT 等多种转换方式；支持 Sticky NAT 开关，使相同源 IP 的数据包经过地址转换后为其转换的源 IP 地址相同；
	DNS Doctoring	支持 DNS Doctoring 功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡（提供截图）；
访问控制	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信息源 MAC、域名、地理区域、应用、服务、时间、长连接、并发会话、WEB 认证、IPS、AV、URL 过滤、WAF、邮件安全、数据过滤、文件过滤、审计、防代理、APT 等功能配置,简化用户管理；
		访问控制策略执行动作支持允许、禁止及认证，对符合条件的流量进行 Web 认证，在策略中可设置用户 Web 认证的门户地址；
		提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析，可在 WEB 界面显示检测结果；（提

		供截图）支持策略加速技术；
		提供策略查询功能，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；
IPv6	双栈模式	支持 IPv4/IPv6 双栈工作模式；
	NAT	支持 NAT64,支持静态转换和前缀转换方式；支持 NAT66 地址转换，支持源地址转换；
	访问控制	支持 IPv6 安全控制策略设置，能针对 IPv6 的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置；
	安全防护	具备基于 IPv6 的病毒防御、入侵防御、URL 过滤、ADS、WAF、流量控制、连接限制、文件过滤、数据过滤、邮件安全等；（提供截图）
	功能虚拟化	支持配置文件、系统服务、路由、链路聚合、安全策略、NAT 策略、带宽管理、认证策略、IPV6 功能、URL 过滤、病毒过滤、WAF、内容过滤、审计、报表、防代理等安全功能虚拟化；
用户管控	认证方式	内置强大的用户身份管理系统，支持本地认证、外部认证及免认证等方式，支持 RADIUS、LDAP、TACACS 等第三方外部认证；
	用户管控	支持手动创建用户、批量导入导出用户、设备扫描方式创建用户；
		支持防暴力破解、密码复杂度、密码有效性设置，如认证失败次数及锁定时间、密码格式、密码长度、密码找回、首次登陆修改密码、密码定期修改、密码有效时间等设置；
		支持查看在线用户情况和用户流量，可显示用户流量、会话、新建连接列表及趋势图，支持用户流量排名；
		支持本地 CA 和第三方 CA，支持作为 CA 认证中心为其他人签发证书，也可采用第三方 CA 为其他人签发证书；支持标准 CRL 列表，支持 CRL 手工更新，同时支持 CRL 自动下载，通过 HTTP 或者 LDAP 方式定时自动下载更新 CRL 文件
应用管控	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	支持对指定的源/目的地址对象、源/目的地理对象、应用制定连接限制策略，可控制所有或单 IP 会话总数及单 IP 新建连接数；
		支持监控功能，显示被拦截的 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；
安全防护	入侵防御	支持独立的入侵防护规则特征库，特征总数在 5000 条以上，能对常见漏洞进行安全防护。
		规则库支持根据攻击类型、风险等级、流行程度、操作系统等进行分类，防护动作包括告警、阻断、记录攻击报文；
		支持针对地址、应用设置入侵防御白名单，支持攻击规则搜索以及自定义，可对自定义规则导入导出；

	未知威胁防御	内置异常行为检测功能，通过统计智能学习算法，对特定地址对象建立监控策略，基于新建、并发、流量等数据与上一周期记录值进行比较判定是否异常，如果存在异常则报警；（提供截图）
	DDOS 防御	支持针对 IP、ICMP、TCP、UDP、DNS、HTTP、NTP 等协议进行 DDOS 防护；支持预定义和自定义策略模板；
		支持基于 IP 协议的检测清洗，包括但不限于：IP Flood、IP Frag Flood、端口扫描、IP 地址扫描；
		支持基于 TCP 协议的检测清洗，包括但不限于：TCP Flood、SYN Flood、FIN Flood、RST Flood、新建 SESSION Flood、SESSION Flood 等；支持 SYN 源认证技术，认证模式可设置为基本模式或者高级模式，以防止虚假源攻击；
		支持基于 UDP 协议的检测清洗，包括对源、目的限速，对 UDP 最大及最小报文限制；同时支持 UDP 关联认证，要求所有去往服务器的 UDP 报文，必须首先与该服务器的 TCP 端口建立 TCP 连接，对源地址进行合法性认证；
		支持基于 DNS 协议的检测清洗，包括但不限于：DNS QUERY FLOOD、DNS REPLY FLOOD、DNS 投毒攻击、DNS 格式检查、DNS NX 异常比率检测等；支持 DNS QUERY 源认证、DNS REPLY 源认证&源限速&目的限速&域名限速等多种手提供段综合防护；
		支持基于 HTTP 协议的检测清洗，包括但不限于：HTTP Flood、HTTP 新建连接 Flood、HTTP 并发连接 Flood、HTTP URI CC 等攻击检测，同时支持对 HTTP slow-header 和 HTTP slow-post 设置最大传输时间以及异常会话数阈值，有效防御慢速攻击；
		支持基于 NTP 协议的检测清洗，包括 NTP REQUEST FLOOD、NTP REPLY FLOOD 等攻击检测，支持基于 NTP 请求限速、NTP 响应限速、源认证、会话认证的防御策略；
		支持静态白名单和动态黑名单功能；
		支持至少 2 种专业反病毒厂商的病毒特征库（提供至少 2 家专业防病毒厂商的合作文件复印件），病毒特征库规模超过 400 万
	升级维护	支持多个系统版本文件并存，系统版本数量不少于 5 个；
	系统诊断	支持在 WEB 界面进行网络诊断，支持 PING、TRACEROUTE、TCP、HTTP、DNS 诊断方式；
		支持在 WEB 界面进行网络抓包，支持设置接口、IP、协议、端口、包数等过滤条件，抓包文件支持导出；
	管理员	支持系统管理员能够通过本地认证及外部认证方式进行登录管理，外部认证失败时可转本地认证；支持管理员分权管理，可自定义管理员权限模板，所有功能模块组合可由管理员自由组合配置
显示监控	监控类型	支持对设备状态、威胁信息、接口流量、连接信息、应用流量、用户流量、服务器流量、网站类型流量、VPN 流量、在线用户等对象进行监控展示；

	流量统计	支持根据应用对通过设备的数据进行统计，包括应用总流量排名和各个应用的协议名称、总流量、上行流量、下行流量、新建连接数、当前会话数以及流速；
		支持根据用户对通过设备的数据报文流量进行统计，包括用户总流量排名和各个用户的用户名、认证类型、上行流量、下行流量、新建会话数、当前会话数以及流速；
		支持根据服务器对通过设备的数据报文流量进行统计，包括各个服务器的服务器 IP、上行流量、下行流量、总流量以及新建会话数；
		支持指定监控时间周期，包括：实时、最近 1 小时、最近 1 天、最近 1 月等；
	威胁统计	支持对病毒防御、入侵防御、WAF、ADS 攻击、APT 防御进行统计，支持按照威胁类型/攻击主机/受攻击主机三种维度结合威胁级别和时间进行统计排名。
服务及质保要求	投标方对投标产品提供 3 年产品原厂标准维保服务。	

4.2.2 探针

市政务外网探针	2 台
技术指标	参数指标要求
接口数量	不低于 6 个千兆电口，4 个千兆光口，2 个万兆光口
尺寸	2U
性能指标	应用层吞吐不低于 5G
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
基础检测功能	具备报文检测引擎,可实现 IP 碎片重组、TCP 流重组、应用层协议识别与解析等, 具备多种的入侵攻击模式或恶意 URL 监测模式,可完成模式匹配并生成事件,可提取 URL 记录和 域名记录,在特征事件触发时可以基于五元组和二元组(IP 对)进行原始报文的录制。
监测识别规则库	能够识别应用类型超过 1100 种，应用识别规则总数超过 3000 条，具备亿万级别 URL 识别能力。漏洞利用规则特征库数量在 4000 条以上，漏洞利用特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，影响系统，对应 CVE 编号
异常流量检测	支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括 3389、53、80/8080、21、69、443、25、110、143、22 等（需提供产品功能截图证明）
深度监测能力	可提供网络流量的会话级视图,根据网络流量的正常行为轮廓特征建立正常流量模型,判别流量是否出现异常,对原始流记录进行异常检测,可发现网络蠕虫、网络水平扫描、网络垂直扫描、IP 地址扫描，端口扫描，ARP 欺骗，IP 协议异常报文检测和 TCP 协议异常报文等常见网络异常流量事件类型;
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。（需提供产品功能截图证明）
	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	具备针对 B/S 架构应用抵御 SQL 注入、XSS、系统命令等注入型攻击；具备跨站请求伪造 CSRF 攻击检测；具备对 ASP,PHP,JSP 等主流脚本语言编写的 webshell 后门脚本上传的检测；具备其他类型的 Web 攻击，如文件包含，目录遍历，信息泄露攻击等的检测；（要求对以上列出的攻击类型进行逐条响应并提供相应的功能界面截图证明并加盖厂商公章） 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；
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。 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。
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。
流量记录	能够对网络通信行为进行还原和记录，以供安全人员进行取证分析，还原内容包括：TCP 会话记录、Web 访问记录、SQL 访问记录、DNS 解析记录、文件传输行为、LDAP 登录行为。
抓包分析	支持通过设备对流量进行抓包分析，可定义抓包数量、接口、IP 地址、端口或自定义过滤表达式。
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。
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。
服务及质保要求	自验收合格之日起，含 3 年产品原厂标准维保服务，并提供原厂针对本项目的授权函和三年原厂售后服务承诺函

4.3 专网区域

其它机构、部门专网有接入电子政务外网需求的，需要通过安全接入区接入电子政务外网，应建立专网区域。专网区域需实现网络访问控制、入侵检测和防御、防病毒、APT

检测、日志审计等功能。需建设相关设备参数配置不得低于如下标准：

4.3.1 防火墙(含入侵检测及防毒墙模块)

专网/其他边界防火墙	2 台
性能要求	招标技术要求
系统架构	采用专用多核硬件平台
硬件规格	万兆光口≥4 个，千兆电口≥6 个，千兆光口≥4 个，接口扩展槽位≥4 个，双电源，内置存储容量不少于 60G
性能	防火墙 1518 字节吞吐量≥20G bps，64 字节吞吐量≥10G bps 在同时开启防火墙、IPS、防病毒、APP 识别的情况下，整机 1518 字节吞吐量≥16G bps，64 字节吞吐量≥8G bps ；整机 HTTP 有效吞吐量≥10Gbps。
	HTTP 每秒新建≥ 60 万
	最大并发连接数≥260 万
虚拟化	支持基于硬件 Hypervisor 技术的底层虚拟化，各个虚拟防火墙之间完全隔离，可运行不同的防火墙版本，拥有完全独立的 CPU、内存、接口等资源。提供虚拟防火墙 Hypervisor 层资源配置管理界面截图。 每个虚拟防火墙均提供完整的安全功能，包括防火墙、入侵防御、防病毒、上网行为管理和流控、VPN、IPv4/IPv6 双栈等。
访问控制	支持基于接口/安全域、地址、用户、服务、应用和时间的防火墙访问控制策略，提供相关界面截图
	支持基于策略的流量统计和会话统计
	支持策略预编译技术，在大量防火墙访问控制策略情况下整机性能不受影响。
	支持详细的访问控制策略日志，每条匹配策略的会话均可记录其建立会话和拆除会话的日志；访问控制策略日志可本地记录或发送至 Syslog 服务器。提供策略配置界面截图及防火墙本地记录的策略建立会话及拆除会话的日志截图。
应用控制	支持并开通基于 DPI 和 DFI 技术的应用特征识别及行为控制，应用识别的种类不少于 1000 种
	支持针对应用动作、应用内容的细粒度控制，如设定允许登录的 QQ 帐号白名单、邮件关键字过滤等
	支持并开通 WEB 控制功能模块，包括 URL 访问分类管理、网页关键字过滤、http 文件下载类型管理等功能，提供相关页面截图。
	URL 分类库规模不少于 2000 万条
流量控制	支持并开通基于线路和多层通道嵌套的带宽管理和流量控制功能，提供至少四层管道嵌套的流控界面截图
	支持基于接口的上下行带宽管理
	支持高、中、低优先级通道设置
	支持基于应用、用户、源地址、目标地址、服务、时间的通道匹配
	支持带宽限制、带宽保障和弹性带宽

会话控制	支持基于接口/安全域、地址、用户、服务、应用和时间的会话控制策略，包括总连接数控制、每秒总新建连接数控制、每 IP 总连接数控制、每 IP 新建连接数控制。
入侵防御	具备并开通网络入侵检测及防御功能，入侵防御事件库事件数量不少于 5000 条
	具备基于接口/安全域、地址、用户、服务、应用和时间的入侵防御策略设定，每个入侵防御策略均可配置检测事件及响应方式。提供相关界面截图。
	具备协议自动识别功能；支持自定义事件功能；
WEB 防护	提供 SQL 注入攻击、XSS 攻击的检测和防御功能，对 Web 服务系统提供保护，要求相关技术具备自主研发专利，可在国家版权局网站查询，提供查询结果网页截图及专利号；
APT 防御	具备扩展 APT 检测模块，采用沙箱检测技术，对未知木马、病毒、恶意代码具有精确的检测效果，实现对未知威胁、高级持续威胁和 ODAY 攻击的有效防护。
	可对 exe、rtf、pdf、xls（x）、ppt（x）、doc（x）、pps（x）、swf、rar、zip 等常见的格式进行动态沙箱分析；可对 rtf、pdf、xls（x）、ppt（x）、doc（x）、pps（x）做 PE 内嵌检测，并且能指出文件偏移位置； 提供相关界面截图。
	内置多种沙箱环境与应用环境，使用反反沙箱、时光加速、机器学习等领先技术，确保恶意样本逃逸率大幅降低。
威胁情报防护	具备基于威胁情报云的动态防护功能，防火墙支持将用户对互联网的访问信息发送至威胁情报云进行实时情报查询及防护。提供防火墙配置界面及威胁情报云端界面截图。
防病毒	具备并开通对 HTTP、FTP、SMTP、POP3、IMAP 协议的病毒检测和过滤功能；
	具备基于接口/安全域、地址、用户、服务、应用和时间的防病毒策略设定。
	具备对文件感染型病毒、蠕虫病毒、脚本病毒、宏病毒、木马、恶意软件等过滤，病毒库数量不少于 1000 万。
	防病毒功能开启后，整机处理性能衰减不超过 30%
安全联动	支持与 IDS 设备的联动，可接收 IDS 产品发送的动态访问控制策略；提供相关界面截图；
	支持与终端管理系统的联动，可接收终端管理系统的主机状态列表，将不合规终端的访问重定向至终端管理指定页面；
网络特性	支持透明、路由、混合、旁路等部署模式；
	支持静态路由、动态路由（RIP、OSPF、BGP4）。
	支持基于入接口、源地址、目标地址、服务端口、应用类型、域名的策略路由。提供相关界面截图。
	支持并开通链路负载均衡，提供轮询、加权轮询、哈希等多种负载均衡算法，支持链路负载均衡的目的会话保持功能。
	支持并开通 IPSec VPN 和 L2TP VPN，投标产品实配 IPSec VPN 隧道数量不少于 5000 条。
	支持通过 ICMP、TCP、DNS 和 HTTP 协议实现对链路可用性的多重健康检查，。
	支持源 NAT、目的 NAT、静态 NAT，支持一对一、一对多和多对多等形式的 NAT

	支持各种应用协议的 NAT 穿越：FTP、TFTP、H.323、SQL*NET
	支持标准 DHCP 服务功能，支持 DHCP 条件下的 IP/MAC 绑定及 IP 地址排除等功能。
	支持 DNS 透明代理功能，可将指定范围内的 DNS 请求自动重定向至管理员指定的 DNS 服务器，且支持多台 DNS 服务器的负载均衡。提供相关界面截图。
	支持标准 DNS 服务器功能，支持多种 DNS 记录 ，包括 A ，NS，CNMAE，TXT，MX，PTR 记录。
高可用性	支持主-主和主-备模式，主备模式下支持基于设备优先级的主设备抢占功能。
	支持基于心跳信号丢失、链路断开等多种方式的 HA 切换条件及逻辑
	支持 HA 设备之间的会话自动同步，包括主主模式和主备模式，确保 HA 切换时业务不发生任何中断
	支持双路 HA 物理心跳线，确保 HA 运行稳定可靠
	支持 HA 设备之间的配置自动同步，确保用户只需在一台设备进行业务配置
系统管理	支持基于 WEB 和命令行的设备管理模式，WEB 界面和命令行模式下均可实现对设备所有功能的管理配置
	支持 SYSLOG 和 SNMP v3，SYSLOG 日志支持同时发给多个日志服务器
	支持威胁可视化技术和流量可视化技术，可提供详细的分析展示图表。
	支持整机威胁统计和展示，包括基于地理位置的威胁地图展示、基于威胁级别和威胁类型的统计分析、基于威胁事件源/目的主机的 TOP10 统计展示、基于具体威胁事件/威胁类型的 TOP10 统计展示等，统计展示的时间周期包括 1 小时/1 天/7 天/30 天。提供相关界面截图。
	支持基于流量的 TOP100 用户和 TOP100 应用的流量曲线图，流量曲线图的统计周期包括小时、天、7 天和 30 天。提供相关界面截图
	支持基于并发会话数量的 TOP100 用户和 TOP100 应用的并发数量曲线图，并发数量曲线图的统计周期包括小时、天、7 天和 30 天。提供相关界面截图
服务及质保要求	自验收合格之日起，含 3 年产品原厂标准维保服务，并提供原厂针对本项目的授权函和三年原厂售后服务承诺函

4.3.2 探针

专网/其他边界探针	**1 台**
技术指标	参数指标要求
接口数量	不低于 6 个千兆电口，4 个千兆光口，2 个万兆光口
尺寸	2U
性能指标	应用层吞吐不低于 2G
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。
基础检测功能	具备报文检测引擎,可实现 IP 碎片重组、TCP 流重组、应用层协议识别与解析等, 具备多种的入侵攻击模式或恶意 URL 监测模式,可完成模式匹配并生成事件,可提取 URL 记录和 域名记录,在特征事件触发

	时可以基于五元组和二元组(IP 对)进行原始报文的录制。
监测识别规则库	能够识别应用类型超过 1100 种，应用识别规则总数超过 3000 条，具备亿万级别 URL 识别能力。漏洞利用规则特征库数量在 4000 条以上，漏洞利用特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，影响系统，对应 CVE 编号。
异常流量检测	支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括 3389、53、80/8080、21、69、443、25、110、143、22 等。（需提供产品功能截图证明）
深度监测能力	可提供网络流量的会话级视图,根据网络流量的正常行为轮廓特征建立正常流量模型,判别流量是否出现异常,对原始流记录进行异常检测,可发现网络蠕虫、网络水平扫描、网络垂直扫描、IP 地址扫描，端口扫描，ARP 欺骗，IP 协议异常报文检测和 TCP 协议异常报文等常见网络异常流量事件类型。
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。（需提供产品功能截图证明）
	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	具备针对 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。（要求对以上列出的攻击类型进行逐条响应并提供相应的功能界面截图证明并加盖厂商公章） 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。
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。 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。
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。
流量记录	能够对网络通信行为进行还原和记录，以供安全人员进行取证分析，还原内容包括：TCP 会话记录、Web 访问记录、SQL 访问记录、DNS 解析记录、文件传输行为、LDAP 登录行为。
抓包分析	支持通过设备对流量进行抓包分析，可定义抓包数量、接口、IP 地址、端口或自定义过滤表达式。

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。
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。
服务及质保要求	自验收合格之日起，含 3 年产品原厂标准维保服务，并提供原厂针对本项目的授权函和三年原厂售后服务承诺函

4.4 汇聚层区域设计

对于各委办局、街镇等单位网络接入到金山区电子政务外网，应在电子政务外网用户层边界设置安全接入区，需实现网络访问控制、入侵检测和防御、防病毒、APT 检测、日志审计等功能。需建设相关设备参数配置不得低于如下标准：

4.4.1 防火墙(含入侵检测及防毒墙模块)

汇聚层防火墙	**6 台**
技术指标	指标要求
硬件规格	产品不少于 4 个千兆电口,4 个千兆光口,4 个万兆光口,2 个 40G (SPF+)接口
性能要求	网络层吞吐量≥80Gbps，应用层吞吐量≥35Gbps
部署方式	具备路由、透明、虚拟网线、旁路镜像、混合等多种部署方式，适应复杂使用环境的接入要求。
路由功能	支持静态路由和多播路由，支持 RIP、OSPF、BGP 等动态路由协议。
地址转换	支持 IPv4 / IPv6 下 NAT 地址转换，支持源地址转换 SNAT，目的地址转换 DNAT 和双向地址转换双向 NAT，支持 NAT64、NAT46 地址转换。
IPv6	支持 IPv4/IPv6 双栈工作模式，支持 IPv6 环境的应用控制策略设置，能针对 IPv6 的 IP 地址、服务端口、区域、服务/应用、时间等条件进行应用访问规则的设置。
VPN	IPSec VPN 支持智能选路功能，保障业务的高可靠性。（需提供产品功能截图证明）
地域访问控制	支持基于对象、区域和地域维度设置安全访问控制策略，允许或拒绝特定国家或者地区的对象访问内部网络，保障业务重大时期安全可靠性。（需提供产品功能截图证明）
流量控制	具备基于国家/地区的流量管理功能，提供具备 CNAS（中国合格评定国家认可委员会）资质的第三方权威机构关于“国家/地区的流量管理”产品功能检测报告。
DDoS 防御	具备 SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood 等泛洪类攻击防护，具备 IP 地址扫描和端口扫描攻击防护。

入侵防御	具备口令暴力破解、僵尸网络、恶意软件、服务器与终端漏洞攻击等检测和防护，支持超过 7000 种特征规则。
	具备僵尸网络检测功能，可基于僵尸网络检测引擎发现主机的异常外联行为，并提供威胁等级和非法外联次数作为举证。
防病毒	具备对 HTTP、HTTPS、FTP、SMB、SMTP、POP3、IMAP 协议进行病毒检测和查杀，支持最大 16 层的压缩文件查杀。（需提供产品功能截图证明）
	具备勒索软件通信防护功能，提供具备 CNAS（中国合格评定国家认可委员会）资质的第三方权威机构关于“勒索软件通信防护”产品功能检测报告。
	具备病毒排除设置，支持基于文件 MD5 值和文件下载 URL 设置病毒白名单。
策略生命周期管理	支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便策略的管理和运维。（需提供产品功能截图证明，并加盖原厂商公章）
双机部署	支持主主、主备两种双机模式部署。
安全报表	产品内置安全报表模板，可定义报表内容，包括网络整体安全状况、服务器安全风险分析、终端主机安全风险分析等。
用户管理权限	支持三权分立功能，根据用户权限分为安全管理员、审计员、系统管理员三种角色。
集中管理	产品支持接入集中管理平台实现多设备的统一管理，通过集中管理平台统一配置产品的安全策略，包括但不限于访问控制、入侵防御、防病毒、Web 应用防护等安全策略。
协同联动	支持上报网络活动产生的数据至本次规划部署的安全管理中心；并支持接收来自安全管理中心推送的处置策略，阻断攻击行为。（需提供产品功能截图证明，并加盖原厂商公章）
服务及质保要求	自验收合格之日起，含 3 年产品原厂标准维保服务，并提供原厂针对本项目的授权函和三年原厂售后服务承诺函

4.4.2 探针

汇聚层探针	**3 台**
技术指标	参数指标要求
接口数量	不低于 6 个千兆电口，4 个千兆光口，2 个万兆光口
尺寸	2U
性能指标	应用层吞吐不低于 5G
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。
基础检测功能	具备报文检测引擎,可实现 IP 碎片重组、TCP 流重组、应用层协议识别与解析等, 具备多种的入侵攻击模式或恶意 URL 监测模式,可完成模式匹配并生成事件,可提取 URL 记录和 域名记录,在特征事件触发时可以基于五元组和二元组(IP 对)进行原始报文的录制。
监测识别规则库	能够识别应用类型超过 1100 种，应用识别规则总数超过 3000 条，具备亿万级别 URL 识别能力。漏洞利用规则特征库数量在 4000 条以上，漏

	洞利用特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，影响系统，对应 CVE 编号。
异常流量检测	支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括 3389、53、80/8080、21、69、443、25、110、143、22 等。（需提供产品功能截图证明）
深度监测能力	可提供网络流量的会话级视图,根据网络流量的正常行为轮廓特征建立正常流量模型,判别流量是否出现异常,对原始流记录进行异常检测,可发现网络蠕虫、网络水平扫描、网络垂直扫描、IP 地址扫描，端口扫描，ARP 欺骗，IP 协议异常报文检测和 TCP 协议异常报文等常见网络异常流量事件类型。
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。（需提供产品功能截图证明）
	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	具备针对 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；具备对 ASP,PHP,JSP 等主流脚本语言编写的 webshell 后门脚本上传的检测；具备其他类型的 Web 攻击，如文件包含，目录遍历，信息泄露攻击等的检测。（要求对以上列出的攻击类型进行逐条响应并提供相应的功能界面截图证明并加盖厂商公章） 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。
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。 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。
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。
流量记录	能够对网络通信行为进行还原和记录，以供安全人员进行取证分析，还原内容包括：TCP 会话记录、Web 访问记录、SQL 访问记录、DNS 解析记录、文件传输行为、LDAP 登录行为。
抓包分析	支持通过设备对流量进行抓包分析，可定义抓包数量、接口、IP 地址、端口或自定义过滤表达式。
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。
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。

服务及质保要求	自验收合格之日起，含 3 年产品原厂标准维保服务，并提供原厂针对本项目的授权函和三年原厂售后服务承诺函

4.5 政务云区域设计

区级电子政务外网接入政务云时，应设置安全边界，实现网络访问控制能力，阻断非法访问。对于区级电子政务外网接入政务云，应在政务云边界设置安全接入区，需实现网络访问控制、入侵检测和防御、防病毒、APT 检测、日志审计等功能。需建设相关设备参数配置不得低于如下标准：

4.5.1 防火墙

区政务云防火墙	**2 台**
性能要求	招标技术要求
系统架构	采用专用多核硬件平台
硬件规格	配备千兆电口≥6 个，万兆光口≥4 个，40G 光口≥2 个，接口扩展槽位≥4 个，双电源，内置存储容量不少于 60G
性能	防火墙 1518 字节吞吐量≥70G bps，64 字节吞吐量≥20Gbps 在同时开启防火墙、IPS、防病毒、APP 识别的情况下，整机 1518 字节吞吐量≥60G bps,64 字节吞吐量≥16G bps ；整机 HTTP 有效吞吐量≥30Gbps
	HTTP 每秒新建≥ 160 万
	最大并发连接数≥650 万
访问控制	支持基于接口/安全域、地址、用户、服务、应用和时间的防火墙访问控制策略，提供相关界面截图
	支持基于策略的流量统计和会话统计
	支持策略预编译技术，在大量防火墙访问控制策略情况下整机性能不受影响。
	支持详细的访问控制策略日志，每条匹配策略的会话均可记录其建立会话和拆除会话的日志；访问控制策略日志可本地记录或发送至 Syslog 服务器。提供策略配置界面截图及防火墙本地记录的策略建立会话及拆除会话的日志截图。
应用控制	支持并开通基于 DPI 和 DFI 技术的应用特征识别及行为控制，应用识别的种类不少于 1000 种
	支持针对应用动作、应用内容的细粒度控制，如设定允许登录的 QQ 帐号白名单、邮件关键字过滤等
	支持并开通 WEB 控制功能模块，包括 URL 访问分类管理、网页关键字过滤、http 文件下载类型管理等功能，提供相关页面截图。
	URL 分类库规模不少于 2000 万条
	支持并开通基于线路和多层通道嵌套的带宽管理和流量控制功能，提供至少四层管道嵌套的流控界面截图

流量控制	支持基于接口的上下行带宽管理
	支持高、中、低优先级通道设置
	支持基于应用、用户、源地址、目标地址、服务、时间的通道匹配
	支持带宽限制、带宽保障和弹性带宽
会话控制	支持基于接口/安全域、地址、用户、服务、应用和时间的会话控制策略，包括总连接数控制、每秒总新建连接数控制、每 IP 总连接数控制、每 IP 新建连接数控制。
入侵防御	具备并开通网络入侵检测及防御功能，入侵防御事件库事件数量不少于 5000 条
	具备基于接口/安全域、地址、用户、服务、应用和时间的入侵防御策略设定，每个入侵防御策略均可配置检测事件及响应方式。提供相关界面截图。
	具备协议自动识别功能；支持自定义事件功能；
WEB 防护	提供 SQL 注入攻击、XSS 攻击的检测和防御功能，对 Web 服务系统提供保护，要求相关技术具备自主研发专利，可在国家版权局网站查询，提供查询结果网页截图及专利号；
威胁情报防护	具备基于威胁情报云的动态防护功能，防火墙支持将用户对互联网的访问信息发送至威胁情报云进行实时情报查询及防护。提供防火墙配置界面及威胁情报云端界面截图。
防病毒	具备并开通对 HTTP、FTP、SMTP、POP3、IMAP 协议的病毒检测和过滤功能；
	具备基于接口/安全域、地址、用户、服务、应用和时间的防病毒策略设定。
	具备对文件感染型病毒、蠕虫病毒、脚本病毒、宏病毒、木马、恶意软件等过滤，病毒库数量不少于 1000 万。
	防病毒功能开启后，整机处理性能衰减不超过 30%
网络特性	支持透明、路由、混合、旁路等部署模式；
	支持静态路由、动态路由（RIP、OSPF、BGP4）。
	支持基于入接口、源地址、目标地址、服务端口、应用类型、域名的策略路由。提供相关界面截图。
	支持并开通链路负载均衡，提供轮询、加权轮询、哈希等多种负载均衡算法，支持链路负载均衡的目的会话保持功能。
	支持并开通 IPSec VPN 和 L2TP VPN，投标产品实配 IPSec VPN 隧道数量不少于 5000 条。
	支持通过 ICMP、TCP、DNS 和 HTTP 协议实现对链路可用性的多重健康检查，。
	支持源 NAT、目的 NAT、静态 NAT，支持一对一、一对多和多对多等形式的 NAT
	支持各种应用协议的 NAT 穿越：FTP、TFTP、H.323、SQL*NET
	支持标准 DHCP 服务功能，支持 DHCP 条件下的 IP/MAC 绑定及 IP 地址排除等功能。
	支持 DNS 透明代理功能，可将指定范围内的 DNS 请求自动重定向至管理员指定的 DNS 服务器，且支持多台 DNS 服务器的负载均衡。提供相关界面截图。
	支持标准 DNS 服务器功能，支持多种 DNS 记录 ，包括 A ，NS，CNMAE，

	TXT，MX，PTR 记录。
高可用性	支持主-主和主-备模式，主备模式下支持基于设备优先级的主设备抢占功能。
	支持基于心跳信号丢失、链路断开等多种方式的 HA 切换条件及逻辑
	支持 HA 设备之间的会话自动同步，包括主主模式和主备模式，确保 HA 切换时业务不发生任何中断
	支持双路 HA 物理心跳线，确保 HA 运行稳定可靠
	支持 HA 设备之间的配置自动同步，确保用户只需在一台设备进行业务配置
系统管理	支持基于 WEB 和命令行的设备管理模式，WEB 界面和命令行模式下均可实现对设备所有功能的管理配置
	支持 SYSLOG 和 SNMP v3，SYSLOG 日志支持同时发给多个日志服务器
	支持基于流量的 TOP100 用户和 TOP100 应用的流量曲线图，流量曲线图的统计周期包括小时、天、7 天和 30 天。提供相关界面截图
	支持基于并发会话数量的 TOP100 用户和 TOP100 应用的并发数量曲线图，并发数量曲线图的统计周期包括小时、天、7 天和 30 天。提供相关界面截图
服务及质保要求	自验收合格之日起，含 3 年产品原厂标准维保服务，并提供原厂针对本项目的授权函和三年原厂售后服务承诺函

4.5.2 探针

区政务云探针	**1 台**
技术指标	参数指标要求
接口数量	不低于 6 个千兆电口，4 个千兆光口，2 个万兆光口
尺寸	2U
性能指标	应用层吞吐不低于 5G
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。
基础检测功能	具备报文检测引擎,可实现 IP 碎片重组、TCP 流重组、应用层协议识别与解析等, 具备多种的入侵攻击模式或恶意 URL 监测模式,可完成模式匹配并生成事件,可提取 URL 记录和 域名记录,在特征事件触发时可以基于五元组和二元组(IP 对)进行原始报文的录制。
监测识别规则库	能够识别应用类型超过 1100 种，应用识别规则总数超过 3000 条，具备亿万级别 URL 识别能力。漏洞利用规则特征库数量在 4000 条以上，漏洞利用特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，影响系统，对应 CVE 编号。
异常流量检测	支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括 3389、53、80/8080、21、69、443、25、110、143、22 等。（需提供产品功能截图证明）
深度监测能力	可提供网络流量的会话级视图,根据网络流量的正常行为轮廓特征建立正常流量模型,判别流量是否出现异常,对原始流记录进行异常检测,可发现网络蠕虫、网络水平扫描、网络垂直扫描、IP 地址扫描，端口扫描，ARP 欺骗,IP 协议异常报文检测和 TCP 协议异常报文等常见网络异常流量事件

	类型。
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。（需提供产品功能截图证明）
	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	具备针对 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；具备对 ASP,PHP,JSP 等主流脚本语言编写的 webshell 后门脚本上传的检测；具备其他类型的 Web 攻击，如文件包含，目录遍历，信息泄露攻击等的检测。（要求对以上列出的攻击类型进行逐条响应并提供相应的功能界面截图证明并加盖厂商公章） 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。
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。 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。
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。
流量记录	能够对网络通信行为进行还原和记录，以供安全人员进行取证分析，还原内容包括：TCP 会话记录、Web 访问记录、SQL 访问记录、DNS 解析记录、文件传输行为、LDAP 登录行为。
抓包分析	支持通过设备对流量进行抓包分析，可定义抓包数量、接口、IP 地址、端口或自定义过滤表达式。
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。
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。
服务及质保要求	自验收合格之日起，含 3 年产品原厂标准维保服务，并提供原厂针对本项目的授权函和三年原厂售后服务承诺函

4.6 安全管理中心设计

安全管理中心以态势感知平台为核心，包含通报预警平台、漏洞扫描系统、威胁情报共享平台、日志审计、安全管理控制系统等功能，符合《国家电子政务外网安全监测体系

技术规范与实施指南》、《政务网络安全监测平台总体技术要求》，并与现网已有日志管理中心系统做好接口对接。

1）通报预警平台

通过二级子账号、工单创建和派发流程，可以设定规则由系统在一定条件下自动创建，然后由管理员选择派发工单；对于没有及时完成的工单进行提醒，提醒方式支持站内消息、邮件等。二级单位自行进行处理，监管单位定时查看与通报。

2）漏洞扫描系统

通过主动扫描、安全设备、主机 agent 等来源发现漏洞，对主动扫描和主机 agent 等所发现的漏洞信息进行有效整合，形成网内标准的漏洞基础数据库。

3）威胁情报共享平台

从安全数据中分析、提取出来，用于在实际应用中发现安全问题，应包含失陷检测情报、文件信誉情报、安全预警通告情报等类型；

4）日志审计系统

通过采集政务外网互联网接入区、政务云和各类区域边界内的安全设备、终端设备、服务器等日志，以及下属委办上报的日志。并按照国家规定的标准格式上报日志数据，推送至智慧城市等数据共享交换平台。

5）安全管理控制系统

利用态势感知进行设备管理，策略管理，策略合规性检查，策略仿真，态势感知发现问题后将安全策略下发给边界防护类设备。

同时安全管理中心自身具备基本的安全防护能力，自身能够防护如 sql 注入、csrf 跨站请求攻击、xss 跨站脚本注入等常见的网络请求攻击行为。

采用模块化架构，具备扩展性，以审计监控技术主动实时采集多元多维的安全行为数据为核心和基础，并依据标准化数据接口，采集平台中边界检测和相关设备日志，构建安全数据中心，通过边界检测数据分析和行为数据分析互为验证，对平台中相关行为进行态势感知，防止平台数据被篡改、窃取以及平台瘫痪。相关设备参数配置不得低于如下标准：

4.6.1 态势感知模块

态势感知模块		**1 套**
技术指标		指标要求
态势感知模块	日志存储时长	180 天
	尺寸	2U
	硬盘容量	≥48T
	内存	≥256G
	接口数量	不低于 6 个千兆电口，4 个万兆光口
	电源	冗余电源
	综合安全态势大屏	具备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、设备运行态势，支持页面跳转到对应态势大屏，并具备大屏告警能力。
	横向威胁态势	具备图形化大屏展示横向威胁态势，包括业务与终端访问、发起威胁终端 TOP5、遭受威胁业务 TOP5、访问趋势图，并具备不同颜色标注横向攻击、违规访问、可疑行为、风险访问。
	资产	具备对全网资产总览分析，包括资产概览、服务器运行状态、资产统计，其中资产概览包括 7 天即将退库资产、全部资产数、核心资产数、资产组数、服务器数、终端数；服务器运行包括服务

		器离线 TOP5、服务器开放端口 TOP10、服务器应用 TOP5；资产统计包括资产组 TOP5、资产来源 TOP5、设备类型 TOP5、操作系统分布、7 天内即将退库资产。（需提供产品功能截图证明，并加盖原厂商公章）
	业务	具备感知业务/服务器资产，可定义 IP 地址、所属分支、主机名、责任人、责任人邮箱、所属业务、操作系统、服务与端口等信息，并支持基于流量支持识别操作系统、开放的服务与端口。
	安全域	▲支持安全域维度感知资产，可定义安全域名称、安全域属性、责任人、责任人邮箱、IP 范围、备注等信息，并支持导入导出 c 配置文件。（针对以上功能提供国家认证的机构检测报告证明，并加盖原厂商公章）
	脆弱性总览	具备页面展示业务脆弱性风险分布，不同严重级别业务分布，漏洞类型分布图，漏洞整体态势等，支持 7 天、30 天统计。
	弱密码	具备镜像流量检测 15 类以上常见协议的弱密码,包括 HTTP、FTP、LDAP、VMWARE、ORACLE、VNC 等类型协议，检测列表包含账号、密码、服务器、所属分支和业务、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；支持筛选管理员账号与是否登录成功，并支持导出弱密码报告。（针对以上功能提供国家认证的机构检测报告证明，并加盖原厂商公章）
	配置不当	支持检测业务服务器的配置不当，检测内容包括服务器、所属业务、所属分支、配置不当类型、风险等级、发现时间等；支持配置不当类型下钻，展示配置不当详情，提供解决方案和数据包举证，并支持导出配置不当报告。（需提供产品功能截图证明）
	风险业务视角	具备失陷(业务和用户)主机详细分析，包含攻击阶段分布、风险等级趋势、安全事件举证、遭受的外部攻击、存在的漏洞风险、行为画像（EBA）、开放端口等信息。攻击阶段包含存在漏洞、遭受攻击、C&C 通信、黑产牟利、内网探针、内网扩散、盗取数据；存在的漏洞风险包含漏洞风险、配置风险、明文传输、弱密码；行为画像 UEBA 包含外连、横向被访问、横向主动访问；具备对每个安全事件详细举证分析，包含风险危害、处置建议、专杀工具、安全知识库等。
	风险安全域视角	具备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。（针对以上功能提供国家认证的机构检测报告证明）
	威胁分析	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。
		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、隐蔽通信、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。

	挖矿专项检测	具备挖矿专项检测，可实时查看挖矿各个攻击阶段，包括感染挖矿病毒、与控制端建立通信、获取挖矿任务、尝试挖矿、挖矿成功等；并支持挖矿币种分布、挖矿风险态势、受影响主机等维度分析统计。（提供产品功能截图证明）
	日志检索	日志类型至少包含漏洞利用攻击、网站攻击、僵尸网络、业务弱点、DOS 攻击、邮件安全、文件安全、网络流量、DNS 日志、HTTP 日志、用户日志、数据库日志、文件审计日志、POP3 日志、SMTP、IMAP、LDAP、FTP、Telnet、第三方等各类日志，并可按照以上类型日志的各个关键字段搜索日志。
	主机安全风险报告	具备展示需要处理的风险主机与风险状况报告，报告内容包括业务与终端风险摘要、业务风险与终端详情分析，提供危害解释和参考解决方案；适用于日常处理安全问题的运维人员。
	等级保护管理服务	具备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。（针对以上功能提供国家认证的机构检测报告证明，并加盖原厂商公章）

4.6.2 通报预警模块

通报预警模块		**1 套**
技术指标		指标要求
通报预警模块	通报总览	具备通报事件统计，包括待通报数量、待认领数量处理中数量、已超时数量、已归档数量；具备通报分支统计，包括通报分支次数 TOP5、分支处理时长 TOP5、通报事件危害影响面，通报分支趋势等。
	自动研判	具备安全事件、漏洞隐患、攻击威胁自动研判，可基于安全等级，如已失陷、高可疑、低可疑、高危、中危、低危等条件；支持自定义工单邮件通报预警模板，可定义主题、附件、正文等内容。
	分支分权管理	具备分权管理，可自定义分支管理权限，分支管理员具备独立的管理页面，分支管理员只能管理和查看所分支所属的业务和终端的安全信息，具备完整的功能展示，包括监控中心、处置中心、分析中心、资产中心和报告中心；总部超级管理员支持查看全局的安全信息，并具备通过页面跳转各个分支的独立管理页面。（针对以上功能提供国家认证的机构检测报告证明，并加盖原厂商公章）

4.6.3 威胁情报共享模块

威胁情报分析		**1 套**
技术指标		指标要求
威胁情报共享模块	威胁情报总览	具备威胁情报总览展示，内置威胁情报数量不少于 120W，支持展示威胁情报命中数、今日命中数、命中威胁情报类别 TOP10、命中趋势、情报共享排行、活跃威胁情报 TOP20 等。（针对以上功能提供国家认证的机构检测报告证明，并加盖原厂商公章）
	威胁情报管理	具备自定义威胁情报，可定义域名、IP、URL、文件 MD5、确定性等级、威胁等级、事件类型、危害描述、处置建议等信息。
	威胁情	具备自定义威胁情报白名单，可自定义域名、URL、IP 和 MD5。

	报白名单	
	情报信息	具备情报信息展示，包含情报名称、情报来源、最近更新时间、情报内容，并可上报下达上下级平台。

4.6.4 漏洞扫描模块

漏洞扫描模块安全	**1 套**
功能指标	指标要求
扫描设备数	2U 设备，6 个千兆电口，4 个千兆光口 支持添加 200 个资产； 漏洞扫描不限制 IP 数； 单个扫描任务最多包含 65534 个 IP 地址（16 位掩码）； 最大并发扫描 IP 数≥110 个 IP 或域名；
部署与访问方式	支持 SSL 加密对数据传输等进行处理,HTTPS 方式,采用 B/S 架构操作，支持 IPv6
检查方式	基线检查和变更检查支持远程检查、SSH、TELNET、SMB。
	支持指定登录用户名和口令进行本地漏扫检查。
	基线检查和变更检查支持离线检查、跳转机跳转。
基线核查范围	基线检查支持系统类型包括主机类:Windows、Unix、Solaris、HP-Unix、AIX、Linux 等；网络设备：华为、H3C、Cisco、Juniper、中兴等；防火墙：华为、天融信、H3C、Fortigate、Cisco、Juniper、迪普防火墙等；数据库：Mysql、DB2、Oracle、Sqlserver、Sybase 等；中间件：Tomcat、IIS、Webservices、Apache、Weblogic、Resin、Nginx 等；虚拟化平台：VMware ESXi、VMware Center、XenServer。
脆弱性查看	在安全基线违规列表中，选择某个违规信息，具备查看该违规的详细信息和解决方案。
	变更检查支持检查重要文件、文件夹、注册表、启动项、进程等详细信息以及变更状态。
	具备根据实际情况设置任意检查结果作为变更基线，后续变更任务将以当前基线作为变更与否的比较标准，具备与自身或其他设备的同类型变更项进行比对，检查设备间核心配置项的异同之处。（需提供产品功能截图证明）
漏洞扫描	具备扫描识别出运行的服务和端口，内置漏洞库 58000 条以上。具备 CVE、CNVD、CNNVD、BugTraq 等，拥有完备的知识体系。
	具备扫描主流虚拟机管理系统的安全漏洞，如：VMWare ESXi、Xen 等
WEB 漏扫	具备常见的 WEB 应用弱点检测，具备主流安全漏洞扫描，如：SQL 注入、跨站脚本攻击、网页木马、系统命令执行漏洞、信息泄露、资源位置预测漏洞、目录遍历漏洞、配置不当漏洞、弱密码、内容欺骗漏洞、外链、暗链等类型漏洞；支持 WEB1.0，WEB2.0 扫描；具备对网站资产管理，快捷网站扫描。
任务管理	具备漏洞扫描、WEB 扫描、弱口令、安全基线检查、变更检查的五合一任务，五者也可任意组合执行任务。（需提供产品功能截图证明）
告警监控	以列表的方式展示告警，支持告警策略自定义、告警声音设置。
	支持告警复核。（针对已确认的告警进行系统自动检查，通过系统执行相关任务精确确认告警是否已经清除）

4.6.5 安全管理控制模块

安全管理中心		1 套
技术指标		指标要求
安全管理控制模块	深度检测引擎升级	具备安全日志分析引擎、DnsFlow 行为分析引擎、HttpFLow 分析引擎、NetFLow 分析引擎、MailFLow 分析引擎、SmbFLow 分析引擎、威胁情报分析关联引擎、第三方安全检测引擎、文件威胁检测引擎等，支持定期自动升级或离线手动升级。
	平台级联	具备上下级平台级联功能，可支持资产信息、安全事件、脆弱性风险上报，其中资产信息包含受监控内部 IP 组、业务/服务器、终端、分析；安全事件包含已失陷事件、高可疑事件、低可疑事件；脆弱性风险包含漏洞风险、配置风险、弱密码和明文传输，并支持页面展示下级平台的当前状态、上报内容、最近上报时间等。
	防火墙、上网行为设备联动	▲具备与现网内互联网接入区部署的防火墙和上网行为进行联动响应，支持平台下发安全策略到防火墙上，阻断攻击流量。（要求提供相关截图证明和厂商承诺函，并加盖原厂商公章）
	SSLVPN 设备联动	具备与现网内 SSL VPN 设备联动，同步用户信息，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，定位异常用户。（需提供截图证明和厂商承诺函，并加盖原厂商公章）
	策略自动填充	支持资产类型、事件类型、风险等级自动化编排响应策略，可联动组件包括防火墙、上网行为管理 AC 等；其中资产类型可选择终端、服务器或指定范围的 IP 资产；风险等级选择可选择已失陷、高可疑、低可疑；事件类型包括有害程序、网络攻击、信息破坏等，事件类型数量不少于 20 种。（需提供产品功能截图证明，并加盖原厂商公章）
	处置策略转换	支持将自定义的安全事件处置策略转换成自动响应策略，解决同类型事件手动重复配置问题，减轻运维工作量（需提供产品功能截图证明）。
	开放共享	支持通过 RESTful API 接口形成对平台数据资源的“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。

4.7 安全准入系统

金山区需建设一套安全准入系统，产品主要功能包括边界定位控制管理、IoT 设备控制、人员认证管理、设备规范管理、攻击威胁检测定位、操作行为管理、视角报表管理、分布部署管理等功能，并适应当前国产化终端的安全管理，主要对接入的电脑终端、移动终端及交换机进行准入控制管理。

4.7.1 准入控制设备

安全准入系统	1 台

指标项		功能描述
基本要求	系统要求	投标产品需符合公安部终端接入控制标准（GA/T 1105-2013）（提供相关证明材料）
		具有独立自主知识产权，须为标准机架式硬件产品。具有独立自主知识产权的准入控制技术。（提供自主知识产权证明文件）
	性能要求	不少于 2 个 1000MBASE-T 接口、4 个万兆光口；每秒事务数(TPS)：≥22000（次/秒），最大吞吐量：≥4.5Gbps，最大并发连接数：30000（条）；
	IPv6 支持	具备在 IPv4 和 IPv6 双栈环境下的终端准入控制、重定向、认证、安检、修复等。
	高可用性	准入设备必须具备 HA 模式。 提供第三方监控平台。
	语言支持	具备终端入网时客户端和 WEB 页面显示进行中英文双语切换。
准入架构	终端发现	能够实时监测并发现接入内网的 PC、移动终端、其他 IP 设备等终端。 对自动发现的终端能够按照类别自动归类，以方便网络终端的统计管理。能够通过自定义将不同的设备分组到不同的大类中，实现客制化的设备类型管理。支持分类不少于 32 个大类， 64 小类/大类。
	准入技术	准入设备具备基于多厂商 Virtual Gateway 的 VLAN 隔离技术，实现无客户端下端口级准入控制。（提供功能截图并加盖原厂商公章） 准入设备具备基于策略路由技术的准入控制模式，入网设备在访问网内关键资源时，将被强制隔离、引导至认证管理页面； 具备交换机接口动态 VLAN 下发、端口隔离模式的网络边界管理。 具备通过 MAC 旁路认证进行 ACL 下发的准入控制。
	802.1x 特性支持	支持根据账户指配下发的 VLAN/ACL。 通过 802.1x 认证进行 VLAN 切换后，可以在 30 秒内重新进行 IP 地址获取，避免切换 VLAN 后需要等待较长时间才能够访问网络。 终端（PC 和哑终端）认证通过后，当需要对终端进行下线、切换 VLAN/ACL 等动作时，准入系统可以通过动态授权（CoA）的方式立即执行，而不需要等待重认证周期。（提供功能截图并加盖原厂商公章） 支持系统自带客户端。 支持域计算机单点登录，在 802.1x 环境下，管理员将终端加入了域管理，终端用户第一次使用时准入客户端可以帮助用户进行 802.1x 认证，以便终端可以和 AD 域服务器进行账号验证，避免第一次无法登录的问题。

		支持 Linux GUI 认证，提供常见主流 Linux（包括：ubuntu、Readhat 等）802.1x 客户端，可以通过客户端进行 802.1x 认证。 支持自定义 Radius 属性下发。支持针对指定特征的终端（MAC），ASM 在其接入时给交换机下发特定的 Radius 属性，使得支持 Radius 属性的交换机对该终端做出特定动作。
	多路支持	单台准入设备可支持至少 4 路策略路由准入控制。 单台准入设备可支持至少 4 个镜像口进行准入控制。 单台准入控制设备支持至少 2 种准入技术组合使用，以增强环境的兼容性。
	定向引导	支持终端入网 IE 浏览器重定向引导，当用户访问网页时能够自动转向到指定的页面或地址，并支持 http 代理及多重重定向引导。 可根据用户的实际环境自定义非 80 端口的 Web 服务端口号及用户重定向引导。 支持使用域名进行终端入网重定向，可以实现准入服务器 IP 地址变动的环境下。 能通过浏览器完成身份认证、控件安装、设备注册、安全检查、检查结果展现等全流程引导管理。 具有 Mac OS、Linux、iOS、Android 等系统专属客户端，支持认证引导和准入管理。（提供功能截图并加盖原厂商公章）
边界管理	**IP/MAC 绑定**	支持 IP/MAC/端口三者强制绑定。 支持在 DHCP 环境下的 IP、MAC 绑定功能。
	NAT 设备	具有 NAT 识别和检测机制能够及时发现网内私接的小路由器、无线 AP、随身 WIFI 等 NAT 设备，帮助清查通过网中网隐藏的真实网络终端。 对通过 NAT 入网的计算机可以实现准入控制、安全评估和修复等流程化管理。
	Hub 管理	具备对连接 HUB 的交换机端口采用多种策略进行 VLAN 切换（提供功能截图并加盖原厂商公章）
网络管理	**网络设备管理**	具备对：交换机、路由器、防火墙等，按照类别进行添加归类管理和展示。 具备设备管理模板的定义功能，能够通过 SNMP、SSH、TELNET 等方式自动、批量添加网络设备。
	终端网络拓扑	能够在拓扑图上选取设备查看其基本状态信息、设备型号、所处位置、子节点、路由表、ARP 表等信息。 具备在界面上提供对该网络设备进行 TELNET、SSH 等管理。 能够在网络拓扑图上由用户自定义显示的节点类型，方便用户通过不同方式查看拓扑连接。 网络拓扑图具备按照网络设备归属的部门进行拓扑图展示。管理员

		在拓扑图上只能查看和管理有权限的设备。
	交换机管理	具备可网管型交换机面板图形化展现各接口状态。 用户可以根据网络安全要求自定义交换机管理端口号,准入设备可以具备使用自定义的 Telnet 和 SSH 端口进行交换机管理。 通过交换机面板显示可以直观查看每个端口下连接的设备类型、数量，可以直接进行端口关闭操作。（提供功能截图并加盖原厂商公章）
	DHCP 地址释放	支持 DHCP 通过管理服务器手动操作,主动进行某台主机的 IP 地址释放。实现 IP 地址充分利用。
移动终端管理	**终端识别**	具备当前主流智能终端设备的安全准入控制,能够自动识别主流手机、智能终端等设备，并自动进行分类。
	移动终端入网	提供独立的智能终端入网引导界面的自主定制功能。 能够提供移动终端入网的设备注册功能。 支持指纹入网认证。
认证管理	**联动认证**	能够全面结合用户已有的认证或业务系统，可以与 RADIUS、LDAP、邮件、AD、WEB 系统做联动认证。
	AD域单点登录	能够与用户现有的 AD 域相结合，当用户登录到 AD 域后，无需二次认证即可入网，避免多次认证的繁琐流程。 可对用户入网后进行是否 AD 域登录进行检查。 当启用 AD 域单点时，可以校验终端是否登录到了正确的企业 AD 域，对于登录了其他伪造的 AD 域的情况可以进行有效的防护。
	证书认证	在进行 Ukey 认证时，支持多个合法的根证书。终端用户认证时，自动进行根证书的匹配。 支持采用软证书认证。 支持 802.1x 客户端认证时使用 Ukey 进行认证。
	接入审核	能够针对不同的角色或设备状态有选择的开启入网审核功能,待审核的用户或设备必须经过管理员审批才能入网。
	认证控制	支持某类（角色）账户只能在指定的时间段、IP 段认证入网。（提供功能截图并加盖原厂商公章）
	自助账号申请	支持用户在认证页面自行进行账号的申请。 用户可自行提交用户名、密码、姓名、电话、部门、E-Mail 等信息。管理员审核通过后，用户即可使用该账号进行认证。有效解决用户账号和密码创建和分发的困难。
来宾管理	**来宾角色**	能够提供来宾角色选择，能够设定来宾设备的访问权限和入网时长。
	二维码认证	已入网员工可以通过扫描来宾终端上二维码，放行来宾用户入网。

终端安全管理	安全检查库	准入设备须提供系统安全配置、用户行为规范等类别检查项，至少提供 30 种以上安全检查项。
	系统补丁	准入设备具有完整的补丁管理子系统，无需第三方补丁服务器支持，自身即可以提供完整的流程化补丁管理，包括同步更新、补丁分发表等功能。 准入设备能够对补丁进行分级，分为：严重、重要、中等的类别。能够在终端的浏览器页面显示入网终端的补丁检查情况。 准入系统自身能够支持 office 系列补丁库、补丁检查和补丁分发安装。 增强型补丁检查与修复。支持对 Win10、Office 进行补丁修复 支持分流补丁服务。为了避免补丁修复造成带宽影响，准入系统支持自建独立的补丁存储服务器，终端修复补丁时可以指定到补丁存储服务器进行修复。
	防病毒软件	支持主流的 20 种以上的杀毒软件检查，包括微软 MSE、可牛、Avast 等，支持杀毒软件版本、病毒库和运行情况的检查，能够在页面显示出检查结果。
	终端安全加固	支持 Guest 来宾帐户、WSUS 更新配置、密码策略设置、屏幕保护设置、弱口令帐户、网卡绑定、系统共享资源进行检查加固。
	计算机健康性检测	支持对终端的磁盘使用率、垃圾文件、IE 主页、网络监听端口等安全性配置进行检查和修复。
	自定义安全检查	通过检测终端文件、指定文件版本、大小、MD5，注册表的项、注册表值，进程、服务状态进行检查。通过安装包运行、访问站点、开关服务、关闭进程、执行文件、删除文件、修改注册表进行修复。可以灵活的对终端进行安全检查和修复。（提供功能截图并加盖原厂商公章）
	终端安全修复	能够提供多种修复方式，用户自行修复、自动修复。
Linux 系统管理	通用 Linux	命令行客户端，支持 RedHat 或 CentOS 5.x~7.x， OpenSUSE 10.x~最新版， ubuntu 10.x~ubuntu 16.x，ArchLinux 等，支持 x86 架构的 32 位和 64 位 libc 库版本为 2.4 及以上所有 Linux 发行版本。支持 NAT 穿越。 图形化客户端，支持 32 位和 64 位麒麟操作系统，支持记住用户名密码，支持心跳保活，支持开机自启动。
	国产化 Linux	支持龙芯平台，支持麒麟平台。（提供功能截图并加盖原厂商公章） 支持系统时间检查、网络监听端口检查、计算机名称检查、磁盘使用检查、主机防火墙检测、IP/MAC 绑定检查、系统服务检查、操作系统版本检查、必须安装软件检查、必须运行进程检查、禁止安装软件检查、禁止运行进程检查、软件白名单检查、弱口令帐户检查、密码策略设置检查、自定义安检项。

资源管理	**软件检查**	通过安全检查检测终端软件安装、使用状态。 为终端指定修复的安装包或访问的网络站点。 软件产品授权，支持进行 windows、office、WPS 产品授权信息进行检查。
	IP 地址管理	提供 IP 地址分配矩阵图。 可以通过组织架构为维度查看 IP 地址分配矩阵图。
运维管理	**移动终端管理**	支持移动终端专用平台管理页面，方便使用平板、智能手机进行准入设备基本操作。 可实现设备快速定位、设备审核、实时报警监控、小助手确认码生成、准入控制器管理、平台基本信息、关机与重启。（提供功能截图并加盖原厂商公章）
	网络诊断工具	支持通过 Web 管理界面进行 ping、抓包、traceroute、nslookup 等功能，并可以设置命令参数进行相关调试。
报警报表管理	**安全管理报表**	能够支持自定义多个不同的报表模板。 准入设备后台提供每日入网报告、每周入网报告、每月入网报告。
	报警信息	支持系统报警、网络报警、终端报警等报警类型，超过 20 种以上自定义报警类型。 支持报警信息通过 Syslog、邮件、短信进行输出。
第三方产品联动		支持与主流上网行为管理系统深度联动，构建内网准入、准出的全面安全管理体系。（提供相关证明材料）
产品服务要求		投标产品需在三年售后服务内满足接入终端授权数量不少于 18000 个点
		提供原厂商针对本项目的至少三年的售后服务承诺函。

4.8 等级保护测评

本项目网络建设及交付验收必须符合国家有关法律法规、符合网络安全等级保护(三级)相关要求。本项目建设完成后投标方需开展该项目等级保护定级、备案和测评工作，并交付等级保护测评报告给招标方，测评整改过程中所产生的设备购买、线路调整、加固实施等费用由投标方负责。如投标方未整改相关工作,导致未能通过测评,招标方有权暂停或终止购买服务。投标方在服务期内需每年开展等级保护

测评工作，并交付等级保护测评报告给招标方。投标方须提供加盖投标人公章的承诺函作为证明材料。

五、环境要求

核心、汇聚机房的供配电系统、空调系统，在防静电、防雷、消防，防水等方面的建设，必须符合《信息安全技术网络安全等级保护测评要求》（GB/T 28448-2019）的规范要求。

供应商需根据组网需求合理选择网络节点，同时提供汇聚层及以上节点的机房平面布置图。

● 机房选址

政务外网核心、汇聚机房地选择在具有防震、防风和防雨等能力的建筑内。机房场地应避免设在建筑物的顶层或地下室，以及用水设备的下层或隔壁。核心、汇聚采用两个或两个以上节点配置，且每个节点必须配置 2 台核心、汇聚设备。有条件的区域，应采用物理地址不同的机房安装核心、汇聚设备。如因条件限制，核心、汇聚设备安装在同一机房，必须保证机房有 2 路（或以上）市电接入，核心、汇聚设备从不同列头柜引电，不同列头柜不使用同一开关。

供应商需承诺提供满足政务外网长期稳定运行要求的机房。

● 机房管理

政务外网核心、汇聚机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员；

● 机房环境

政务外网核心、汇聚机房应合理规划设备安装位置，应预留足够的空间作安装、维护及操作之用。房间装修必需使用阻燃材料，耐火等级符合国家相关标准规定。机房门大小应满足系统设备安装时运输需要。机房墙壁及天花板应进行表面处理，防止尘埃脱落，机房应安装防静电活动地板。

机房安装防雷和接地线，设置防雷保安器，防止感应雷，要求防雷接地和机房接地分别安装，且相隔一定的距离；机房设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。应配备空调系统，以保持房间恒湿、恒温的工作环境；在机房供电线路上配置稳压器和过电压防护设备；提供短期的备用电力供应，UPS 应该满足在断电情况下工作 2 小时的运行要求。宜配置冗余或并行的电力电缆线路为计算机系统供电；建立备用供电系统。铺设线缆要求电源线和通信线缆隔离铺设，避免互相干扰。对关键设备和磁介质实施电磁屏蔽。

● 设备与介质管理

政务外网各级机房必须采用有效的区域监控、防盗报警系统，阻止非法用户的各种临近攻击。

六、扩容服务要求

在一个服务周期内(1 年),当电子政务外网接入规模(招

标具体点位基础上10%以内的接入点位的新增)、网络出口或者链路资源等无法满足招标方使用要求时,投标人需无条件对现有网络进行优化扩容,一并做好机房等配套资源的扩容。在第二年和第三年内接入点位的新增,可根据投标方案、可行性方案及合同签订等情况按实次年结算。

七、项目实施要求

7.1 网络架构设计

供应商作为项目实施的主要组织者，需要对项目实施进行组织、协调。包括组织主设备、配套设备、配套材料（设备机柜、抗震机座、电力线、网线、光纤、蛇形套管、交流电源盒等）的采购；提供机房必要的装机条件（包括机房环境、电源、空调等)；负责整个项目实施的组织、协调及管理：制定详细的实施方案，安排、协调项目参与各方的工作，监督管理整个实施方案的执行。组织调测及验收。

供应商提供的电子政务外网组网架构应满足总体架构要求，同时提供详细网络拓扑图，包括节点位置、网元数量、设备配置及性能参数等信息。

7.2 网络割接要求

请供应商针对本次服务内容提供业务割接方案，并且进行实施。同时需要提供以下说明：

1）请说明本项目网络割接和调整以及进行相应的项目实施内容。

2）根据网络方案说明各节点的网络割接和调整步骤以

及具体工程实施计划，进行相应的工程实施。

3）网络割接调整时需要考虑对在线业务的中断性影响，争取将影响控制在最小，争取平滑割接。配合采购人部署业务应用线路的 IP 地址数量满足割接要求，并能与现有政务云业务应用系统 IP 地址相匹配，不影响采购人业务连续性，并提供承诺书。

7.3 IPv6

金山区电子政务外网业务网络应遵循《推进互联网协议第六版（IPv6）规模部署行动计划》的标准和要求，供应商所提供设备应均支持 IPv4/IPv6 双栈技术及 IPv6 线速转发。全网部署端到端双栈技术实现互通，并启用基于 IPv6 的路由协议。

7.4 QoS

金山区电子政务外网的 QoS 总体设计原则如下：

1）采用轻载方式保障网络服务质量，建议链路月平均日峰值利用率不超过 50%；

2）采用 DiffServ 作为网络突发拥塞时 QoS 保证方式；

3）识别用户侧流量，调度重要业务进 PQ 队列，调度普通业务进默认队列尽力转发。

供应商应根据上述原则,结合业务提出详细的 QoS 方案。

7.5 IP 地址

1） 供应商应根据网络结构和设备配置，给出本工程 IP 地址需求。

2）供应商应对本工程网络编址提出实施方案，以实现最佳的网络内地址分配及业务流量分布。

7.6 路由协议和路由策略

政务外网路由策略的总体要求为：

1）政务外网应实现业务网络路由和用户路由分离。IGP负责承载设备之间的互联链路、Loopback、网管等的承载网路由；BGP负责承载区政务外网和接入部门网络、数据中心等的用户路由。管理上层次分明，从而避免用户路由震荡影响业务网络路由，保证局部的变动不影响上层路由配置和全局路由配置。

2）区级政务外网业务网络路由和用户路由可以由IGP统一承载。当具备条件时，也可以与市级政务外网保持一致，进行业务网络路由和用户路由的分离。

3）路由设计应能反映出整个网络的层次结构，并与自治域、各节点子网的IP地址分配相结合，做到合理的路由聚合，减少路由表的长度，减轻路由更新给设备带来的负荷，提高路由稳定性。

4）在同一AS内，应根据网络流量分担、分布与路由备份需要，统一规划路由Metric值，实现路由策略。

5）合理规划IGP区域。对于新建网络，在单管理域设备数量较少时，可以配置为单区域。

供应商应根据上述要求给出详细的路由策略设计。供应商对路由协议的设计要求保证网络的连通性、可达性，路由

策略应实现网内流量流向的分担、备份和链路利用的均匀性，同时对于网络维护，路由策略应具备良好的可控性与可维护性。

供应商应给出域内路由协议的链路权值设置方案，并给出网络处于稳定状态时的选路结果。

根据路由组织方案，供应商应给出域间路由协议控制路由分布的实施方案。

供应商的路由策略方案应保证全网具备良好的路由稳定性和可扩展性且易于维护。

八、SDN 和运行管理系统

本项目需引入基于 SDN 软件定义网络技术的网络管理系统，实现网络资源的灵活管理，保障应用高效部署、稳定运行。网络管理系统需要提供整网综合管理能力，实现网络资源、用户和业务的融合管理，提供基本的网络资源管理、拓扑管理、故障管理、性能管理、用户管理，采用 SDN 技术，实现业务快速部署，流量工程和智能流量调整能力；应基于智能检测技术，对网络中不同业务的运行状态、服务质量，做到实时监控、主动运维。

8.1 运维管理

（1）拓扑集中监视

提供统一拓扑发现功能，全网监控，可以实时监控所有设备的运行状况，并根据网络运行环境变化提供合适的方式对网络参数进行配置修改，保证网络以最优性能正常运行，

拓扑功能包括：拓扑自动发现：将网元自动添加到拓扑视图中，同时可以发现网元间的链路。可以控制拓扑的图层显示，比如拓扑上的所有链接，只显示光纤，其他不显示。

拓扑业务状态显示：传送的 client 路径、路由器的 VPN 等业务，可以在拓扑中展现业务状态。

（2）告警管理

支持对全网设备的故障、运行状态进行实时监控、历史统计并提供协助排障的手段，故障管理功能支持如下功能：

支持多种告警级别：支持紧急、重要、次要、提示等基本的告警级别，每个级别的告警都用不同的颜色显示，告警颜色用户可以自定义。

告警多种通知方式：当告警发生后，管理系统可以发出告警声音，不同基本的告警声音不同，用户可以自定义告警音。同时支持告警外发能力，比如手机短信和 Email 等。

告警统计：能按照用户所设的统计条件对告警信息进行统计。统计条件包括告警名称、告警级别、告警功能分类、告警发生时间、告警状态、告警源等，也可以是以上各项的组合。

（3）设备配置文件管理

提供网络设备丰富的配置管理能力，网络管理员需要定期备份设备的配置文件，跟踪设备配置变化，从而保证一旦发生网络故障时，可以使用历史配置备份将网络设备立刻恢复正常。

设备配置文件的批量备份和恢复等集中管理 设备配置变化，主动备份配置文件 灵活的设备配置文件比较功能，包括指定设备的运行配置和启动配置的比较、不同设备间的配置文件比较等，管理员能够快速查看设备配置差异，迅速定位导致问题的配置命令。

（4）管理数据可靠

网管服务器数据库存储文件有两种，一种用来存储数据，另一种用来存储该数据库运行的日志信息。为保证数据安全，应定期进行数据库的备份。

数据备份：备份数据库到本地服务器或者远程服务器。包括立即备份和定时备份。

（5）业务网管功能

通过网管软件提供端到端的 VPN 专线运营的可视化业务管理能力，简化业务管理，提供业务配置、管理效率。跨域管理，从 VPN 到 IP 承载，到物理层快速定位，以及网络级的可视化管理，故障定位等功能。

（6）关键业务管理功能

支持图形化界面的端到端 VPN 专线业务配置能力：VPN 专线是电子政务网的重要业务，网管需要支持简单的图形界面，对路由器的隧道、VPN 的端到端图形化配置、管理和故障诊断。

VPN 端到端的故障定位功能：需要支持 VPN 端到端以及隧道内部的故障定位。

提供统一的简化的故障告警管理：通过告警管理功能，可以统一查看所有设备的告警信息，包括接入和 IP 的故障信息，可以查看告警影响的业务，支持故障定位功能。

8.2 网络性能及质量检测

（1）网络性能展示

网管系统提供性能视图直观展示设备状态数据，方便监控设备关键状态，及时发现设备的异常状态并处理，保证设备的正常运行。同时支持以拓扑图方式显示被管网元及其之间连接的状态，用户可通过浏览拓扑视图实时了解整个网络的组网情况和监控运行状态。

（2）基于 TWAMP Light 关键业务质量检测与排障

网管系统支持业界标准的 TWAMP 测试,通过 TWAMP Light 免探针的方式，在关键节点部署业务质量检测，测试网络实施时延、丢包、抖动网络参数。采用业务流图形化监控，10E-3 精度，7*24 实时性能数据，快速定位，理清责任界限。

（3）iFIT 免探针关键业务真实流性能监测

采用测试会话报文的性能测试结果，有时仍无法代表业务的真实流性能，比如：测试报文采用 UDP 封装而非 TCP 封装、DSCP 值不一样等等。路由器提供了 iFIT 功能，基于 IP 真实业务流报文的性能测试，可以单向的端到端或逐跳测试 IP 真实业务流的网络时延、抖动、丢包，适用于针对关键业务流中的质差流 7*24 小时的周期性持续不间断监控。

8.3 业务自动发布

VPN 是政务外网的最重要的业务，对于 VPN 业务来说，如果采用传统的手工方法需要配置命令行，建立隧道，配置 VRF 实例等过程，不仅对人的要求高而且容易因为人为因素配置错误影响客户单位的业务。因此，本项目需在网管平台部署 SDN 控制器，实现基于 SDN 的 VPN 业务自动发放，具体要求如下：

1）VPN 的创建图形化，参数模板化，通过层次化、可视化网络管理，提供完善的多层管理能力，实时获取网络承载关系，可视化操作，无须记忆命令行端到端可视化 VPN 及传输业务发放，利用业务模板创建业务，提升业务发放效率；

2）提供模板配置功能，在配置 VPN 的业务时，可以选择之前预定义的模板，快速设置业务参数，提高配置效率；

3）提供隧道和 VPN 等业务导入功能，可以从 excel 中配置业务参数，直接导入到管理系统中，进行业务参数检查后可以直接进行业务下发；

4）提供批量部署隧道的功能，选择网元和组网规则后，自动计算所有的隧道业务并统一下发配置，提高隧道部署效率；

5）提供端到端的业务管理，可以查看整个业务的业务状态，可以查看业务的路由信息，可以对路由进行调整。可以查看 VPN 业务的承载关系，了解资源使用情况；

6）提供业务的复制功能，可以快速发放业务，提高业务的部署效率；

7）VPN 隧道的可视化。从网络设计可以了解，电子政务网区分了不同的业务平面，并调整了网络的路径选择，使得不同级别的用户 VPN 需要通过不同的平面接入，隧道路径的可视化，能够使得 VPN 业务开通时，让管理维护人员确认流量是否按照规划的业务平面路径转发；

8）VPN 专线的开通，需要设置速率参数，如 CAR 参数，QOS 参数。网管提供图形化界面管理配置这些信息。此外，电子政务网还需要考虑能够可视化查看到当前各个用户单位 VPN 线路的状态，例如当前的端口速率，流量，SLA 信息等，提前预测网络状态。

8.4 SDN 技术要求

SDN 控制器	**1 套**
功能及技术指标	**参数要求**
部署环境	部署方式：支持物理主机、虚拟机部署 服务器: 支持含国产操作系统、ARM 架构 CPU
实配授权	本次实配 20 网元授权，路由器设备管理、控制、分析以及 MPLS 网络优化功能授权。
系统架构	SDN 控制器应该包含管理、控制和分析集成的统一云化架构。
	SDN 控制器应该支持统一的 Portal 来访问所有的 SDN 组件，包括设备管理，业务发放，网络优化，网络监控。提供功能截图或官网链接作为证明材料，并加盖厂商公章或投标专用章
	SDN 控制器应提供统一的用户认证机制，使用所有的 SDN 功能组件时不需要多次重复登录
	SDN 控制器应该在一个业务窗口中提供统一的业务监控能力，支持业务 DASHBOARD，支持业务相关告警，历史性能曲线和 OAM 工具，无需跳转到其他系统
	SDN 控制器应支持异地容灾能力,主备控制器之间的需要支持数据库同步机制
	SDN 控制器应该具备网络的全生命周期的管理能力，至少包括以下功能： Zore Touch 设备部署、自动的业务发放、MPLS 网络优化和最优路径计算、网络流量监控与分析、网络 SLA 以及 E2E 业务性能分析、网络保障、配置管理、故障管理
网络发现与基础配置管理能力	SDN 控制器应该支持通过 LLDP 等协议自动发现网络设备及链接关系 ,并生成全网的网络拓扑
	SDN 控制器应该支持通过 BGP-LS 等协议自动发现网络的逻辑拓扑

	SDN 控制器应该支持实时更新网络的拓扑变化
	▲SDN 控制器应该支持 zero touch 功能，自动发现网络中新安装的路由器，自动生成并向新路由器部署基本配置（LSR ID，IP 地址，IGP，协议...），自动添加新路由器并构建物理拓扑。提供功能截图或官网链接作为证明材料并加盖厂商公章或投标专用章
MPLS 网络优化与路径计算	SDN 控制器应至少支持 64k 隧道和 128k LSP
	SDN 控制器应能够同时管理 RSVP-TE LSP 和 SR-TE LSP
	SDN 控制器应支持根据实时采集的网络状态和性能数据，执行全局重新优化
	SDN 控制器支持使用链路亲和属性作为最优 LSP 计算的约束条件，SDN 控制器支持使用跳数限制作为最优 LSP 计算的约束条件，SDN 控制器支持使用链路 SRLG 属性作为最优 LSP 计算的约束条件，提供功能截图或官网链接作为证明材料
流量动态调整	支持根据实时采集的网络状态和性能数据，执行全局重新优化
	当隧道实时带宽变化率超过阈值后,SDN 控制器支持自动 LSP 重新优化，提供功能截图或官网链接作为证明材料并加盖厂商公章或投标专用章
	支持通过图形化界面手动启动局部流量调优能力，提供功能截图或官网链接作为证明材料
自动业务发放与管理	SDN 控制器应该支持 E2E 配置以下业务类型:RSVP-TE/SR-TE、 L3VPN、EVPN、VLL、VPLS SDN 控制器应该支持 L3VPN 驱动创建 SR-TE+VXLAN 混合隧道
	SDN 控制器支持模型驱动的 VPN 业务部署，以定义网络业务到设备配置的映射；SDN 控制器支持创建 QoS 模板，支持对设备或接口批量部署 QoS 模板，支持 SAI QoS 模板与 VPN 业务的快速部署
	SDN 控制器支持基于模版创建隧道，设置隧道带宽，时延，Hot-standby 等；SDN 控制器支持创建业务时通过 Auto-select 或 Binding 的方式实现业务和隧道的绑定
	SDN 控制器支持业务创建时自动地创建一条满足业务 SLA（时延）要求的路径的隧道的能力，而不需要提前建立好隧道。SDN 控制器支持业务创建时自动地创建一条满足业务 SLA（带宽）要求的路径的隧道的能力，不需要提前建立好隧道。提供功能截图或官网链接作为证明材料并加盖厂商公章或投标专用章
网络监控与分析	SDN 控制器应当支持通过 SNMP\NetStream 实时采集网络性能信息
	SDN 控制器应当支持通过实时采集网络性能信息，SDN 控制器应当支持动态采集链路、隧道数据时延信息，提供功能截图或官网链接作为证明材料
	SDN 控制器应当支持提供网络性能的统计报告及可视化呈现，包括丢包、时延、抖动、带宽利用率等 SDN 控制器应当支持提供基于 QoS 队列/VPN 业务性能和质量的统计报告及可视化呈现，包括丢包、时延、抖动
	SDN 控制器应当支持当性能超过阈值限制时产生警报 SDN 控制器应当支持提供 TopN 流量统计报告，并主动报告异常业务，TOP N 链路带宽使用情况
	自验收合格之日起，含 3 年产品原厂标准维保服务，并提供原厂针对本项目的授权函和三年原厂售后服务承诺函

8.5 网络运行管理平台要求

网络运行管理平台	1 套
开放性	系统负荷 SOA 架构，标准模块接口，方便二次开发。
主要功能	资源拓扑，告警管理，设备管理，监控配置，统计报表呈现与配置，告警转发及后处理，系统管理。
网元类型	覆盖所有主流操作系统，网络设备，防火墙，数据库，中间件。
指标采集	用户可根据需求随时通过配置模式添加定制化采样，无需对软件进行二次开发。
Agentless or agent 探针	支持 SNMP get，ssh，telnet，wmi，perform，http，ftp，tl1，snmp trap，socket，jdbc 等多种标准探针接口。
可操作性	具有远程用户支持与控制功能。
事件管理	事件压缩，事件过滤，事件关联。
集中监控界面	网元拓扑，告警查询，性能查询，统计报表。可定制化界面。
趋势分析	性能统计报表，告警统计报表，业务报表。
可用性	包括网络管理软件、分布式系统监控功能、事件处理和自动化管理。
配置	包括软件分发管理和自动信息仓储管理。
安全性	具有跨平台的用户管理功能和全面的企业安全管理功能。
OSS	多协议 GATEWAY，易于与其它系统对接。
SLA 定义	针对用户运维，定制化 SLA 标准。
性能处理能力	支持 5w 条/分钟的性能数据采集处理能力
告警信息处理能力	支持 15w 条/分钟的告警信息处理能力
网管平台级联	支持网管平台通过级联方式对接，上级网管能对下级网管进行融合管理。
服务及质保要求	自验收合格之日起，含 3 年产品原厂标准维保服务，并提供原厂针对本项目的授权函和三年原厂售后服务承诺函

8.6 网络整体运维服务

按照金山区行政服务中心根据系统稳定、安全、可靠、有效运行所提出的要求和指标，及时制定、修改和完善系统运行维护方案，并确保系统运行维护方案有效执行。

在系统的安全性、稳定性和可靠性确保前提下，充分考虑系统运行状况优化和发展。

建立符合金山区电子政务外网实际情况的，具备专业和可操作性的 ITSS 信息技术服务架构，形成标准可靠可行的运维服务体系。

提供无推诿服务，即供应商应提供特殊措施，无论由于

哪一方产生的问题而使系统发生不正常情况时，应全力协助各类资源和相关部门，使系统尽快恢复正常。

提供节点式管理，核心、汇聚节点重点全方位响应服务和技术支持；提供下沉式服务，服务覆盖范围到所有接入层，提供接入层的网络响应服务和技术支持。

服务期内，供应商应承担金山区电子政务外网及互联网区域的网络运维工作。运维范围包含现网所有网络设备及网络节点，包含此次升级改造中所有新购设备、新建软件系统平台和节点，包含服务期内新增的所有网络、安全设备及节点。供应商应提供专业运维团队，提供7×24小时电话支持，5×8小时现场驻点运维服务等相关运维服务。驻场地点由采购人指定，专职团队至少包含项目经理1名，必须具备高级工程师职称证书或一级建造师证书（通信与广电工程专业），除项目经理外，专职团队应至少包含工程师（A）2名，必须具备CCNP、CCIE、HCNP、HCIE其中一类证书，工程师(B)1名，必须具备信息安全认证工程师资格。重保或两会重要期间，需每日提供夜间值班不少于1人，双休日日班应不少于2人，夜间值班需在甲方指定服务地点，并根据实际情况安排好人员支援和储备。运维团队应具备主动发现问题、主动处理故障的运维能力，全面负责金山区电子政务外网所有网络故障的排查和处理工作，根据网络故障安全等级，一般故障应在5分钟内响应，2小时内到达现场（如需到达现场处置的），4小时内恢复；重大故障应即时进行响应，半小时内

到达现场，2 小时内恢复，故障处理应出具处理报告，并经用户方签字确认。运维团队应做好日常巡检工作，每日对主要设备进行一次日常巡检，每季度对主要设备进行一次详细检查，巡检须出具检查报告，经评估需要整改的内容，由运维团队承担整改工作。运维团队应做好日常网络资产统计、配置管理、事件管理工作，资产信息应形成报表、定期更新，配置文件宜采用信息化手段定期备份。运维团队应负责与其他外联网络、线路的工作人员协调、对接工作。

8.6.1 网络接入服务

供应商承担金山区电子政务外网网络接入服务，根据政务外网管理办法要求，涉及需要接入区级政务外网的单位，供应商运维团队应对接接入单位网络接入需求，并出具接入方案，经金山采购人审核批准后实施，在已完成光缆接入的前提下，一个工作日内完成网络接入工作。对于其他专网、专线、无线网络、应用系统、VPN 用户等的接入需求，供应商运维团队应做好需求对接，出具安全可行的接入方案，经采购人审核批准后实施。

8.6.2 网络变更服务

服务期内，供应商应提供网络变更服务。针对金山区电子政务外网系统存在的网络变更调整，如网络构架变更、设备变更、链路变更、放置地点变更、部署位置变更、配置变更、策略变更等，供应商应负责对接变更需求，出具合理的变更方案，经采购人审核批准后，由供应商负责实施。

8.6.3 网络优化服务

服务期内，供应商应提供网络优化服务。供应商应对金山区电子政务外网的网络结构、网络配置、网络管理、管理工具、管理制度提出优化建议和优化方案，经采购人审核批准后实施，确保金山区电子政务外网的通畅、安全，尤其是保障区政务外网和互联网、无线网、市政务外网及各专网之间高速数据传输。

8.6.4 网络安全服务

服务期内，供应商应提供网络安全服务。安全服务应包含但不仅限于金山区电子政务外网的网络安全防护、入侵检测、流量控制、行为管理、安全准入、漏洞扫描、日志审计、风险预警、态势感知、趋势分析、安全通报、风险处理、事件处置等服务内容。供应商运维团队应安排专业安全人员负责安全服务工作，对全网安全情况实时监控、定期检查、全面分析；对可能存在的网络安全风险主动发现、充分评估、预先感知、提前预警、做好防护；对已经发生的网络安全事件及时处置、及时反馈、总结分析、做好整改。原则上每年至少提供采购人两次安全、应急演练服务。服务期内，供应商应全力配合采购人完成所有安全测评、安全检查、政务外网考核、上级演练等工作。

8.6.5 网络监测服务

服务期内，供应商应提供网络监测服务。供应商应提供包含网络安全、网络管理、运行监测等一系列全网监测、运

行管理系统及统一管理演示界面（统一运管监测门户），并具备展示能力。根据监测数据情况，可形成相应的报表、报告，对全网各单位的网络运行情况和所有设备的健康情况、流量情况应能够从多个维度进行分析、研判，形成并提交周报、月报、季度报、年报。区级网络安全监测系统或监测探针应按国家《政务网络安全监测平台总体技术要求》要求与市级安全监测平台进行所需数据的级联对接，形成市区两级协同联动的运行监测体系。

8.6.6 备品备件和质保服务

服务期内，供应商对所有新购设备应提供原厂质保服务；核心层、汇聚层、街镇主接入及网络边界的利旧设备，由采购人负责购买质保服务；所有在用的底层接入交换机及光模块，应由供应商提供备品备件服务，交换机不少于 5 台，10G 和 40G 光模块各不少于 5 个，并存放至甲方指定地点，在需要替换时负责实施工作。

8.6.7 重要活动保障服务

供应商应根据采购人的实际需求，在春节、国庆、护网、两会、党代会、进博会等重保期间，安排相应的技术力量，为采购人做好风险评估、安全防护和现场保障工作。

8.6.8 技术支持和培训服务

服务期间，供应商应对采购人相关人员进行全面培训和技术支持，培训内容应包含但不仅限于涉及项目建设的网络构架、运行原理、设备知识、平台功能和操作培训等，并以

操作手册、远程服务、现场支持等方式为采购人提供相应的技术支持服务。

8.6.9 其他服务

供应商应无条件提供与金山区电子政务外网的运行维护、安全保障、监测管理、应急处置、技术支持等方面的其他服务。

8.7 下沉式服务

8.7.1 下沉式服务范围要求

金山区电子政务外网核心、汇聚、接入层，接入层的政务外网接入设备的使用故障、技术支持等；具体接入下联单位节点详见项目需求中的现有节点清单。

8.7.2 下沉式服务主要内容

除了网络系统核心、汇聚，供应商需专门提供并分组安排运维团队人员，对政务外网各接入节点提供日常技术支持与快速响应；

积极主动配合各委办局相关信息技术负责人快速落地与政务外网服务相关的业务需求，了解各个委办局在政务外网业务需求以及数据在网络中流向。

定期或不定期对各个委办局进行抽样调查政务外网服务满意度，听取各方意见和建议，收集需求后综合分析并作出改进和优化。

通过工单系统通知及时处理各单位故障报修或技术支持等需求。工单处理完毕后完成用户满意度反馈。

8.7.3 下沉式服务响应要求

1、建立基于 7*24 小时不间断的 SLA 服务级别设计，原则上远程实时响应，现场 2 小时内响应，故障解决时间不超过 T+1 日,重要故障或核心故障 T+0 日。

2、除故障响应和技术支持响应之外，还需提供每月接入设备的巡检，做好巡检记录，并排除隐患。

九、培训要求

供应商应根据本项目的特点制定培训方案并提供培训，使采购人相关人员在培训后能够独立使用系统，而不必依赖供应商现场指导。培训课程涵盖电子政务外网的使用和管理培训，供应商负责安排专业培训讲师授课，并提供全套培训教材和培训课程计划表。

1)培训总则

供应商至少满足本章要求的培训服务。

所提供的培训课程表随响应文件一起提交。

培训授课人是经过厂商认证的工程师。

供应商为所有被培训人员提供培训用文字资料和讲义等相关用品。所有的资料是中文书写。

培训工作应在合同生效后安排。

每年安排一次针对各委办局信息系统基于电子政务外网建设的培训。

2)培训内容与课程要求

供应商应对项目中所有产品的基本知识、系统或参数配

置、管理维护等提供相应的培训。供应商详细列明相应的培训课程内容、人数和时间安排。

3)培训费用

供应商应将所有培训费用（含培训教材费）及各项支出计入资源服务费用中，不单独报价。

十、人员要求

供应商应为金山区电子政务外网单独建立管理组织，配置相应团队。项目投入人员需提供社保缴纳证明，如有退休人员须提供返聘合同扫描件。

1.项目经理：

对服务项目过程实行全面管理，执行检查控制协调项目的各项工作。

项目经理必须具备高级工程师职称证书或一级建造师证书（通信与广电工程专业）。

应从事大型网络、机房维护等相关工作至少5年以上实际经验，从事项目经理或项目负责人至少5年以上实际经验。

2.服务工程师：

服务工程师包含现场驻点运维工程师和二线支持团队，二线支持团队对一线运维进行远程技术与指导，紧急情况下处理应急事件、疑难问题和个案调查处理。并根据需要到现场进行响应、值守。

服务工程师需提供相关证书（或者类似证书）。

服务工程师中至少 2 名需具备 CCNP、CCIE、HCNP、HCIE 其中一类证书。

服务工程师中至少 1 名需具备信息安全认证工程师资格。

服务工程师中至少 3 名需从事网络、机房维护等相关工作至少 3 年以上实际经验。

十一、考核要求

11.1 升级改造服务期的验收标准

升级改造服务期的网络质量验收标准如下：

（1）核心层至汇聚层延迟不大于 2ms，丢包率小于等于 1%。

（2）核心层至区政务外网各出口边界路由器延迟不大于 2ms，丢包率小于等于 1%。

（3）核心层至各接入区汇聚交换机的网络延时不超过 2ms，丢包率小于等于 1%。

（4）区政务外网接入交换机访问区政务外网各出口边界路由器延迟不大于 2ms，丢包率小于等于 1%。

（5）各链路带宽承载能力应达到最大值的 80%，错报率小于 1%。

升级改造要符合《上海市电子政务外网建设和运行管理指南》的要求。

11.2 运营维护服务期考核要求

运营维护服务期，每年年底采购人组织对供应商进行考

核评估，考核内容主要包括网络可靠性、网络可用性、网络安全性与服务质量，考核内如详见下表。

分类	考核项目	内容	分数	得分	备注
网络可靠性	网络可用率不低99.99%		15分		网络可用率=（一个月总时长-电路不可用总时长）×100%/一个月总时长 电路不可用总时长为电路中断时间的累加。电路不可用总时长是以采购人发现电路中断，并向供应商报障的时间开始计算，在供应商把恢复的电路交还与采购人时停止计算。采购人将不能把以下中断时间计算为“电路不可用总时长”： （1）当供应商交还恢复的电路，而采购人人员不能实时验收电路时，不论电路是否被接收，“电路不可用总时长”也会被终止计算；（2）当电路中断是因为采购人拥有或操控的设备的故障，或在供应商提供服务以外的设备或设施的故障；（3）在供应商预先通知并得到采购人允许的情况下发生的电路终断；（4）不可抗力影响。
网络可用性	业务开通及变更	有线路资源	10分		6小时内完成开通；
		有管道资源无光纤资源	5分		10个工作日内开通
		无资源	5分		30个工作日内开通
	应急响应及抢修	在规定时间内应急响应	5分		响应时间≤20min
		在规定时间内到达故障现场	5分		重大故障1小时/严重故障2小时内/一般故障4小时
		故障在规定时限内抢	10分		重大故障2小时/严重故障4小时内/一般

		通			故障 24 小时
		事故报告	5 分		故障处理后 3 个工作日内及时分析原因并出具事故报告。
安全性	安全评测	提供等保 2.0 三级测评承诺函	10 分		投标方需在服务期内每年开展等级保护测评工作（三级），并交付给招标方。投标方需提供加盖投标人公章的承诺函作为证明材料。
服务质量	日常运维	驻场保障	5 分		安排工程师提供网络驻场保障服务。
	巡查巡检	日常巡检	5 分		每日对重要节点进行日常维护巡检服务。
		详细巡检	5 分		每季度对重要节点进行详细巡检服务。
		巡检报告	5 分		定期以书面或电子邮件形式反馈工作周期内的工作情况，包括：故障汇总、巡检情况、ping 测情况和资源变动情况等。
	重保	/	5 分		在春节、国庆、护网、两会、党代会、进博会等重保期间，供应商应安排相应的技术力量，为采购人做好现场保障工作。
	机房	机房运维	5 分		机房环境应做到防尘、防水，地面清洁，设备布局合理，布线规范。定期做好机房巡检工作，并做好记录。机房维护人员应熟知用电常识和用电应急处理步骤，严格管理机房所有出入人员，并做好记录。

考核评分 85 分及以上为 A，70-85 分为 B，60-69 分为 C，60 分以下为 D。考评结果为 A 则采购人全额支付当期服务费；如考评结果为 B，则采购人有权扣除当期服务费 1%；如考评结果为 C，则采购人有权扣除当期服务的 3%；如考评结果为 D，则采购人有权扣除当期服务的 5%，并无条件终止服务，更换服务提供商。

服务期内，采购人有权要求对下一个考核周期的考核内容进行调整，调整内容由采购人会同供应商共同细化，以备忘录形式加以约定。

十二、投标文件的编制要求

投标文件由商务响应文件（包括相关证明文件）和技术响应文件二部分构成，包括（但不限于）下列内容：

1. 商务响应文件

1.1 商务响应文件由以下部分组成（但不局限于）：

（1）投标函；

（2）资格条件响应表；

（3）实质性要求响应表；

（4）开标一览表（以电子采购平台设定为准）；

（5）报价分类明细表（相关报价表格详见第六章《投标文件有关格式》；

（6）商务响应表；

（7）投标单位的情况简介；

（8）法定代表人授权委托书（原件）和投标人代表的身份证复印件（复印件，加盖投标人公章）；

（9）中小企业声明函（原件）；

（10）投标人关于商务等的其他说明（如有的话）；

项目要求按上述内容编制商务标书，如有需说明的其他事项，一律写入“投标人关于报价等的其他说明”内。

2. 技术响应文件

2.1 技术响应文件由以下部分组成（但不局限于）：

（1）与评标有关的投标文件主要内容索引表

（2）项目需求理解

（3）技术方案

（4）网络割接方案

（5）项目管理与实施

（6）培训方案

（7）项目经理

（8）服务团队

（9）投标设备重要性能指标

（10）项目运维售后方案

（11）备品备件

（12）类似业绩

（13）照《项目采购需求》要求提供的其他技术性资料以及投标人需要说明的其他事项。

第五章　评标办法与程序

一、资格审查

招标人将依据法律法规和招标文件的《投标人须知》、《资格条件响应表》，对投标人进行资格审查。确定符合资格的投标人不少于 3 家的，将组织评标委员会进行评标。

二、投标无效情形

2.1 投标文件不符合《资格条件响应表》以及《实质性要求响应表》所列任何情形之一的，将被认定为无效投标。

2.2 单位负责人或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，参加同一包件或者未划分包件的同一项目投标的，相关投标均无效。

2.3 除上述以及政府采购法律法规、规章、《投标人须知》所规定的投标无效情形外，投标文件有其他不符合招标文件要求的均作为评标时的考虑因素，而不导致投标无效。

三、评标方法与程序

3.1 评标方法

根据《中华人民共和国政府采购法》及政府采购相关规定，结合项目特点，本项目采用“综合评分法”评标，总分为 100 分。

3.2 评标委员会

（1）本项目具体评标事务由评标委员会负责，评标委员会由 **5 人**组成，其中采购人代表 **1 名**，其余为政府采购评审专家。招标人将按照相关规定，从上海市政府采购评审专家库中随机抽取评审专家。

（2）评标委员会成员应坚持客观、公正、审慎的原则，依据投标文件对招标文件响应情况、投标文件编制情况等，按照《投标评分细则》逐项进行综合、科学、客观评分。

3.3 评标程序

（1）符合性审查。评标委员会应当对符合资格的投标人的投标文件进行符合性审查，以确定其是否满足招标文件的实质性要求。

（2）澄清有关问题。对投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评标委员会应当以书面形式要求投标人作出必要的澄清、说明或者纠正。投标人的澄清、说明或者补正应当采用书面形式，由其授权的代表签字，不得超出投标文件的范围或者改变投标文件的实质性内容，也不得通过澄清而使进行澄清的投标人在评标中更

加有利。

（3）比较与评分。评标委员会按招标文件规定的《投标评分细则》，对符合性审查合格的投标文件进行评分。

（4）推荐中标候选供应商名单。各评委按照评标办法对每个投标人进行独立评分，再计算平均分值，评标委员会按照每个投标人最终平均得分的高低依次排名，推荐得分最高者为第一中标候选人，依此类推。如果供应商最终得分相同，则按报价由低到高确定排名顺序，如果报价仍相同，则由评标委员会按照少数服从多数原则投票表决。

四、评审细则

4.1 投标价格分按照以下方式进行计算：

（1）价格评分：报价分＝价格分值×（评标基准价/评审价）

（2）评标基准价：是经符合性审查合格（技术、商务基本符合要求，无重大缺、漏项）满足招标文件要求且投标价格最低的投标报价。

（3）评审价：投标报价无缺漏项的，投标报价即评审价；投标报价有缺漏项的，按照其他投标人相同项的最高报价计算其缺漏项价格，经过计算的缺漏项价格不超过其投标报价10%的，其投标报价也即评审价，缺漏项的费用视为已包括在其投标报价中，经过计算的缺漏项价格超过其投标报价 10%的，**其投标无效**。

（4）本项目非专门面向中小企业采购，对小型和微型企业投标人的投标价格给予 10%的扣除，用扣除后的价格参与评审。中小企业投标应提供《中小企业声明函》

（5）**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竞标。如果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。**

4.2 投标文件其他评分因素及分值设置等详见《投标评分细则》

投标评分细则（100 分）

序号	评审内容	权重	评分细则
1	报价	10	价格权重×（评标基准价/评标价）×100 **本项目小微企业报价给予 10%的扣除，用扣除后的价格参加评审。**
2	项目需求理解	8	根据对本项目的建设背景、建设目标、建设内容、重点难点分析、整体设计思路等的理解程度等进行综合评分。 对本项目需求理解充分，所述建设目标符合采购需求，建设内容完整全面，重点难点分析到位，设计思路清晰可行得 7-8 分； 对本项目需求有基本了解，所述建设目标基本符合采购需求，建设内容大致全面，能基本分析出项目重点难点，设计思路不够清晰，得 4-6 分； 对本项目需求理解不全面，所述建设目标基本符合采购需求，建设内容不够全面，重点难点的把握不够精确，得 1-3 分； 未提交项目需求理解，或提交的需求理解完全不匹配本项目实际情况，得 0 分。
3	技术方案	20	根据技术方案进行针对性、合理性、实用性的设计，能否符合业主方实际使用需求，描述是否详细、准确；系统建设目标是否清晰，是否能全面覆盖项目总体需求；系统功能设计是否完整，能否充分满足系统建设需求，是否完全满足招标文件技术要求；方案是否科学合理、安全严密、具有一定的前瞻性等综合评定。 综合评定好的得 16-20 分； 综合评定较好的得 10-15 分； 综合评定一般的得 0-9 分。
4	网络割接方案	8	本项目对业务迁移连续性有很高的要求，投标方应针对本次服务内容提供符合金山区政务外网现网要求的无缝业务割接方案，需对现状进行分析，体现割接的针对性、合理性、稳定性和可靠性，此外方案需要有进一步论证实施等内容。投标人应在上个合同周期（2024 年 5 月 31 日到期）到期前，确保能完成全网建设实施。 根据投标方以上方案的完整性、科学性、可操作性，满足业务连续性要求情况等方面进行综合打分。 割接方案完整、科学、可操作性好的得 7-8 分； 割接方案较好的得 4-6 分； 割接方案一般的得 0-3 分。
5	项目管理与实施	8	根据投标方所提供的项目组织的合理性、过程管理的规范性、质量保证措施、风险管理的有效性及技术文档和管理文档的完整性，进行综合评分。 综合评定好的得 7-8 分； 综合评定较好的得 4-6 分； 综合评定一般的得 0-3 分。

6	培训方案	8	根据投标方是否提供完善的、与项目切实有关的培训方案进行综合评分。 综合评定好的得 7-8 分； 综合评定较好的得 4-6 分； 综合评定一般的得 0-3 分。
7	项目经理	5	对服务项目过程实行全面管理，执行检查控制协调项目的各项工作。 项目经理必须具备高级工程师职称证书或一级建造师证书（通信与广电工程专业）；应从事大型网络、机房维护等相关工作至少 5 年以上实际经验；从事项目经理或项目负责人至少 5 年以上实际经验。 配置较好的得 3-5 分；配置一般的得 1-2 分。 **需提供相关佐证材料及社保缴纳明细证明（近六个月中任意一个月，2023 年 11 月 1 日至本项目开标截止日），如退休须提供返聘合同扫描件。未提供的不得分。**
8	服务团队	8	服务工程师包含现场驻点运维工程师和二线支持团队，二线支持团队对一线运维进行远程技术与指导，紧急情况下处理应急事件、疑难问题和个案调查处理。并根据需要到现场进行响应、值守。 服务工程师需提供相关证书（或者类似证书）。 服务工程师中至少 2 名需具备 CCNP、CCIE、HCNP、HCIE 其中一类证书。 服务工程师中至少 1 名需具备信息安全认证工程师资格。 服务工程师中至少 3 名需从事网络、机房维护等相关工作至少 3 年以上实际经验。 配置较好的得 6-8 分；配置一般的得 1-5 分。 **需提供相关佐证材料及社保缴纳明细证明（近六个月中任意一个月，2023 年 11 月 1 日至本项目开标截止日），如有人员退休须提供返聘合同扫描件。未提供的不得分。**
9	投标设备重要性能指标	6	针对采购文件的采购需求，投标设备有▲项重要参数负偏离的，每项扣 2 分，扣完为止。
10	项目运维售后方案	8	根据投标人提供运维售后方案，包括： 故障响应时间；重要通讯保障；巡检巡修服务；对运维售后服务要求的吻合度。综合评定 综合评定好的得 7-8 分； 综合评定较好的得 4-6 分； 综合评定一般的得 0-3 分。

11	备品备件	6	所有在用的底层接入交换机及光模块，应由供应商提供备品备件服务，交换机不少于 5 台，10G 和 40G 光模块各不少于 5 个，并存放至采购人指定地点，根据投标人提供的备品备件清单进行综合评定。 综合评定好的得 5-6 分； 综合评定较好的得 3-4 分； 综合评定一般的得 0-2 分。
12	类似业绩	5	近三年（2021 年 1 月 1 日起签署合同）以来类似项目业绩： 有效的类似项目业绩由评标委员会根据投标人提供的业绩在业务内容、技术特点等方面与本项目的类似程度进行认定。 有一个有效业绩得 1 分，每增加一个有效业绩加 1 分，最高得分为 5 分。 **（需提供项目合同或中标通知书复印件加盖公章）**

第六章　投标文件有关格式

一．商务响应文件有关格式

投标函

致：_____（招标人名称）

根据贵方_____（项目名称、招标编号）采购的招标公告及投标邀请，_____（姓名和职务）被正式授权代表投标人_____（投标人名称、地址），向贵方在网上投标系统中提交投标文件 1 份 。

据此函，投标人兹宣布同意如下：

1、按招标文件规定，我方的投标总价为 _____（大写）元人民币。

2、我方已详细研究了全部招标文件，包括招标文件的澄清和修改文件（如果有的话）、参考资料及有关附件，我们已完全理解并接受招标文件的各项规定和要求，对招标文件的合理性、合法性不再有异议。

3、投标有效期为自开标之日起 _____日。

4、如我方中标，投标文件将作为本项目合同的组成部分，直至合同履行完毕止均保持有效，我方将按招标文件及政府采购法律、法规的规定，承担完成合同的全部责任和义务。

5、如果我方有招标文件规定的不予退还投标保证金的任何行为，我方的投标保证金可被贵方没收。

6、我方同意向贵方提供贵方可能进一步要求的与本投标有关的一切证据或资料。

7、我方完全理解贵方不一定要接受最低报价的投标或其他任何投标。

8、我方已充分考虑到投标期间网上投标会发生的故障和风险，并对可能发生任何故障和风险造成的投标内容不一致、利益受损或投标失败，承担全部责任。

9、我方同意网上投标内容均以网上投标系统开标时的开标记录表内容为准。我方授权代表将对开标记录进行校核及勘误，授权代表不进行校核及勘误的，由我方承担全部责任。

10、为便于贵方公正、择优地确定中标人及其投标货物和服务，我方就本次投标有关事项郑重声明如下：

（1）我方向贵方提交的所有投标文件、资料都是准确的和真实的。

（2）我方不是采购人的附属机构。

（3）我方近期有关投标型号货物的生产、供货、售后服务以及性能等方面的重大决策

和事项：_____

_____，

_____。

（4）我方最近三年内因违法行为被通报或者被处罚的情况：

_____，

_____。

（5）以上事项如有虚假或隐瞒，我方愿意承担一切后果，并不再寻求任何旨在减轻或免除法律责任的辩解。

地址：

电话、传真：

邮政编码：

开户银行：

银行账号：

投标人授权代表签名：

投标人名称（公章）：

日期：　　年　　月　　日

资格条件响应表

序号	项目内容	要求	响应内容说明(是/否)	详细内容所在投标文件页次	备注
1	法定基本条件	符合《中华人民共和国政府采购法》第二十二条规定的条件： 1、营业执照（或事业单位、社会团体法人证书)、税务登记证（若为多证合一的仅需提供营业执照） 2、具有健全的财务会计制度、依法缴纳税收和社会保障资金的良好记录的声明。 3、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的书面声明函，截止至开标日成立不足 3 年的供应商可提供自成立以来无重大违法记录的书面声明。 4、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	投标人资质	符合招标文件规定的合格投标人资质条件：无。			
3	中小企业	本项目面向大、中、小、微型等各类供应商采购			
4	联合投标	本项目不允许联合投标。			
5	法定代表人授权	1、在投标文件由法定代表人授权代表签字（或盖章）的情况下，应按招标文件规定格式提供法定代表人授权委托书； 2、按招标文件要求提供被授权人身份证。			

投标人授权代表签字：_____

投标人（公章）：_____

日期：_____年_____月_____日

实质性要求响应表

序号	项目内容	要求	响应内容说明(是/否)	详细内容所在投标文件页次	备注
1	投标文件内容、密封、签署等要求	1、投标文件按招标文件规定格式要求提供《投标函》、《开标一览表》、《资格条件响应表》以及《实质性要求响应表》并在标明签字和盖章页签字和盖章。 2、纸质投标文件按招标文件要求密封，电子投标文件须经电子加密（投标文件上传成功后，系统即自动加密）。			
2	投标有效期	不少于 90 天。			
3	质量标准	按双方合同约定。			
4	服务期限	2024 年 6 月 1 日起至 2027 年 5 月 31 日。（本项目采用一次招标，三年沿用，合同一年一签的方式实施。采购人每年对中标供应商进行考核，考核合格、服务满意续签第二、第三年服务合同；若考核不合格、服务不满意，采购人有权终止服务合同，不再续签下一年的服务合同。）			
5	付款条件	合同签订后支付合同价的 30%，项目建设完成后初验通过后支付 40%，一年整体运维验收通过后支付剩余 30%。			
6	合同转让与分包	合同不得转让，分包应符合招标文件规定：对非本专业项目，可进行专业分包，但不得将合同约定的全部事项一并委托给他人。除乙方投标文件中已说明的委托专项服务事项外，中标后一律不得对外分包。			
7	公平竞争和诚实信用	不得存在腐败、欺诈或其他严重违背公平竞争和诚实信用原则、扰乱政府采购正常秩序的行为。			
8	招标文件中标有★的实质性条款	招标文件中凡标有“★”的条款均系实质性要求条款。			

投标人授权代表签字：_____

投标人（公章）：_____

日 期：_____年_____月_____日

开标一览表

金山区政务外网租赁服务项目包 1

项目名称	服务期限	投标总价（大写）	最终报价（总价、元）

说明：（1）所有价格均用人民币表示，单位为元，精确到个数位。

（2）投标人应按照《采购需求》和《投标人须知》的要求报价。

（3）开标一览表内容与投标文件其它部分内容不一致时以开标一览表内容为准。

投标人授权代表签字：_____

投标人（公章）：_____

日期：_____年_____月_____日

报价分类明细表

序号	费用项目名称	费用
1		
2		
3		
4		

说明：

1、所有价格均系用人民币表示，单位为元，精确到个位数。

2、投标人应按照《采购需求》和《投标人须知》的要求报价。

3、投标人根据报价分类费用情况编制报价构成表并随本表一起提供。

4、报价分类明细合价应与开标一览表报价相等。

投标人授权代表签字：_____

投标人（公章）：_____

日期：_____年_____月_____日

商务响应表

项目名称：　　采购编号：

项目	采购文件要求	是否响应	投标人的承诺或说明
服务期限	2024 年 6 月 1 日起至 2027 年 5 月 31 日。（本项目采用一次招标，三年沿用，合同一年一签的方式实施。采购人每年对中标供应商进行考核，考核合格、服务满意续签第二、第三年服务合同；若考核不合格、服务不满意，采购人有权终止服务合同，不再续签下一年的服务合同。）		
服务地址	采购人指定地点。		
质量标准	按双方合同约定。		
付款条件	合同签订后支付合同价的 30%，项目建设完成后初验通过后支付 40%，一年整体运维验收通过后支付剩余 30%。		
投标有效期	90 天。		
转让与分包	本项目合同不得转让。		
投标报价	投标报价要求为唯一的，不能有两个或多个报价的。		

投标人授权代表签字：_____

投标人（公章）：_____

日期：　　年　　月　　日

投标人基本情况简介

（一）基本情况：

1、单位名称：

2、地址：

3、邮编：

4、电话/传真：

5、成立日期或注册日期：

6、行业类型：

（二）基本经济指标（到上年度 12 月 31 日止）：

1、实收资本：

2、资产总额：

3、负债总额：

4、营业收入：

5、净利润：

6、上交税收：

7、在册人数

（三）其他情况：

1、专业人员分类及人数：

2、企业资质证书情况：

3、近三年内因违法违规受到行业及相关机构通报批评以上处理的情况：

4、其他需要说明的情况：

我方承诺上述情况是真实、准确的，我方同意根据招标人进一步要求出示有关资料予以证实。

附：

1、营业执照（或事业单位、社会团体法人证书）、税务登记证（若为多证合一的仅需提供营业执照），（复印件，加盖投标人公章）；

2、具有健全的财务会计制度、依法缴纳税收和社会保障资金的良好记录的声明；

3、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的书面声明函，截止至开标日成立不足 3 年的供应商可提供自成立以来无重大违法记录的书面声明；

4、供应商书面声明。

投标人授权代表签字：_____

投标人（公章）：_____

日期：_____年_____月_____日

依法缴纳税收和社会保障资金、没有重大违法记录

声　明

本公司具有依法缴纳税收和社会保障资金的良好记录，且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。

特此声明。

本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日期：_____年___月___日

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：

供应商书面声明

致：（招标人名称）

我公司承诺已自查，在参加本项目政府采购活动中未违反《中华人民共和国政府采购法实施条例》第十八条“单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动”。

特此声明

附件：投标人股东名录及所占股东比例（国家企业信用系统公示系统）

投标人授权代表签字：_____

投标人（公章）：_____

日期：_____年_____月_____日

法定代表人资格证明书

单位名称：_____

地址：_____

姓名：_____性别：_____年龄：_____ 职务：_____

系 _____（单位）的法定代表人。

特此证明。

投标人：（盖章）

日期：　　年　　月　　日

法人授权委托书

致：_____

本授权委托书声明：

我 _____（姓名）系注册于 _____（投标人注册地）_____（投标人）的法定代表人，现授权委托_____（姓名）为我公司代表，以本公司的名义参加_____项目的投标活动。被授权人在本项目投标、开标、评标及合同谈判和签约过程中所签署的一切文件和处理与之有关的一切事务，本公司及我本人均予以承认。

代理人无转委托权，特此委托。

本授权委托书在签署日至本合同签署之日期间始终保持有效。

附：被授权人身份证复印件。

投标人：_____（公章）

法定代表人：_____（签字）

被授权人身份证复印件粘贴处：

被授权人：_____（签字）

签署日期：_____年___月___日

中小企业声明函（工程、服务）

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 _____（单位名称） 的_____ （项目名称） 采购活动，工程的施工单位全部为符合政策要求的中小企业（或者：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._____（标的名称），属于 __软件和信息技术服务业__；承建（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）；

2._____（标的名称），属于 _____；承建（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：

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。

注：各行业划型标准：

（一）农、林、牧、渔业。营业收入 20000 万元以下的为中小微型企业。其中，营业收入 500 万元及以上的为中型企业，营业收入 50 万元及以上的为小型企业，营业收入 50 万元以下的为微型企业。

（二）工业。从业人员 1000 人以下或营业收入 40000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 300 万元及以上的为小型企业；从业人员 20 人以下或营业收入 300 万元以下的为微型企业。

（三）建筑业。营业收入 80000 万元以下或资产总额 80000 万元以下的为中小微型企业。其中，营业收入 6000 万元及以上，且资产总额 5000 万元及以上的为中型企业；营业收入 300 万元及以上，且资产总额 300 万元及以上的为小型企业；营业收入 300 万元以下或资产总额 300 万元以下的为微型企业。

（四）批发业。从业人员 200 人以下或营业收入 40000 万元以下的为中小微型企业。其中，从业人员 20 人及以上，且营业收入 5000 万元及以上的为中型企业；从业人员 5 人及以上，且营业收入 1000 万元及以上的为小型企业；从业人员 5 人以下或营业收入 1000 万元以下的为微型企业。

（五）零售业。从业人员 300 人以下或营业收入 20000 万元以下的为中小微型企业。其中，从业人员 50 人及以上，且营业收入 500 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 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（六）交通运输业。从业人员 1000 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 3000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 200 万元及以上的为小型企业；从业人员 20 人以下或营业收入 200 万元以下的为微型企业。

（七）仓储业。从业人员 200 人以下或营业收入 30000 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 20 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 20 人以下或营业收入 100 万元以下的为微型企业。

（八）邮政业。从业人员 1000 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 20 人以下或营业收入 100 万元以下的为微型企业。

（九）住宿业。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 2000 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 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十）餐饮业。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 2000 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 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十一）信息传输业。从业人员 2000 人以下或营业收入 100000 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 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（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。

（十三）房地产开发经营。营业收入 200000 万元以下或资产总额 10000 万元以下的为中小微型企业。其中，营业收入 1000 万元及以上，且资产总额 5000 万元及以上的为中型企业；营业收入 100 万元及以上，且资产总额 2000 万元及以上的为小型企业；营业收入 100 万元以下或资产总额 2000 万元以下的为微型企业。

（十四）物业管理。从业人员 1000 人以下或营业收入 5000 万元以下的为中小微型企业。其中，从业人员 300 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 100 人及以上，且营业收入 500 万元及以上的为小型企业；从业人员 100 人以下或营业收入 500 万元以下的为微型企业。

（十五）租赁和商务服务业。从业人员 300 人以下或资产总额 120000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且资产总额 8000 万元及以上的为中型企业；从业人员 10 人及以上，且资产总额 100 万元及以上的为小型企业；从业人员 10 人以下或资产总额 100 万元以下的为微型企业。

（十六）其他未列明行业。从业人员 300 人以下的为中小微型企业。其中，从业人员 100 人及以上的为中型企业；从业人员 10 人及以上的为小型企业；从业人员 10 人以下的为微型企业。

业绩一览表

项目名称：　　采购编号：

序号	年份	项目名称	项目概述	合同号	证明人	在标书中的页次

说明：

合同复印件需加盖公章。

投标人授权代表签字：_____

投标人（公章）：_____

日期：　　年　　月　　日

无疑问回复函

_____（采购单位）：

_____（采购代理单位）：

在仔细阅读了贵单位关于“_____”（项目名称）的采购文件、等其他资料后：

我公司确认对本项目采购文件、评标办法、技术规格及要求等其他资料所述条款及内容无疑义；

我公司确认采购文件显示的信息的准确性、完整性和有效性。

投标人名称（盖章）：

出具日期：　　年　　月　　日

说明：请各投标人仔细阅读招标文件及其他资料，如无疑义，请将本确认函加盖投标人公章，在递交纸质投标文件的同时递交。

二. 技术响应文件有关格式

与评标有关的投标文件主要内容索引表

项目名称：　　采购编号：

序号	响应项目	主要内容概述	详细内容所在投标文件页次	备注
1	报价			
2	项目需求理解			
3	技术方案			
4	网络割接方案			
5	项目管理与实施			
6	培训方案			
7	项目经理			
8	服务团队			
9	投标设备重要性能指标			
10	项目运维售后方案			
11	备品备件			
12	类似业绩			

说明：上述具体内容要求可以参照本项目评标方法之评分标准。

项目经理情况表

项目名称：　　采购编号：

姓名		出生年月		文化程度		毕业时间	
毕业院校和专业			从事本类项目工作年限			联系方式	
职业资格			技术职称			聘任时间	
主要工作经历： 主要管理服务项目： 主要工作特点： 主要工作业绩： 胜任本项目的理由：							
更换项目经理的方案							
更换项目经理的前提和客观原因： 更换项目经理的原则： 替代项目经理应达到的能力和资格：							

供应商授权代表签字：

供应商（公章）：

日期：_____年_____月_____日

人员配置汇总表

项目名称：　　采购编号：

项目组成员姓名	年龄	在项目组中的岗位	职业资格	备注

投标人授权代表签字：

投标人（公章）：

日期：

重要参数偏离表

序号	设备名称	招标要求	偏离内容	说明
1	安全管理中心	▲支持与现网内互联网接入区部署的防火墙和上网行为进行联动响应，支持平台下发安全策略到防火墙上，阻断攻击流量。（要求提供相关截图证明和厂商承诺函，并加盖原厂商公章） ▲支持安全域维度感知资产，可定义安全域名称、安全域属性、责任人、责任人邮箱、IP 范围、备注等信息，并支持导入导出 csv 配置文件。（针对以上功能提供国家认证的机构检测报告证明，并加盖原厂商公章）		
2	SDN 服务器	▲SDN 控制器应该支持 zero touch 功能，自动发现网络中新安装的路由器，自动生成并向新路由器部署基本配置（LSR ID，IP 地址，IGP，协议...），自动添加新路由器并构建物理拓扑。提供功能截图或官网链接作为证明材料并加盖厂商公章或投标专用章		

第七章　合同条款及格式

包 1 合同模板：

金山区政务外网租赁服务

合同

甲　　方：上海市金山区行政服务中心

乙　　方：[合同中心-供应商银行名称]

签订时间：[合同中心-签订时间]

金山区政务外网租赁项目服务合同

合同编号： [合同中心-合同编码]

合同双方：

甲方（委托人）： 上海市金山区行政服务中心
地址： 上海市金山区龙山路 555 号
邮政编码： 200540
电话： [合同中心-采购单位联系人电话]
联系人： [合同中心-采购单位联系人]
联系人邮箱：

乙方（受托人）： [合同中心-供应商名称]
地址： [合同中心-供应商所在地]
邮政编码： [合同中心-供应商单位邮编]
电话： [合同中心-供应商联系人电话]
联系人： [合同中心-供应商联系人]
联系人邮箱：
开户银行： [合同中心-供应商银行名称_1]
帐号： [合同中心-供应商银行账号]

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，在平等互惠、互相扶持、共同发展的基础上，甲方和乙方双方经过充分协商，共同签订本合同。乙方向甲方提供合同规定的服务，甲方向乙方支付服务的款项。双方按本合同约定的条款享受权利、履行义务并承担责任。

第一条　项目基本情况

甲方向乙方购买政务外网租赁服务，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、服务质量等详见招标文件和投标文件。

本项目涉及使用的设备由乙方提供，在服务期内，甲方享有完整的使用权。

第二条　服务时间及服务范围

1、 服务时间：服务期限为 1 年（自 2024 年 6 月 1 日起至 2025 年 5 月 31 日止）。[合同中心-合同有效期]

2、 服务地点：由甲方指定服务地点。

3、 技术服务质量要求:乙方所提供的服务需通过等级保护测评、服务和质量验收要求，达到合同执行考核标准，具体要求参照第三条条款相关内容。

第三条　合同文件的组成和解释顺序

1、 本合同书

2、 甲乙双方签订的增补协议

3、 本项目招标文件或采购文件中的采购需求

4、 本项目招标文件或采购文件中的合同条款

5、 乙方的本项目投标文件或响应文件

6、 其他合同文件（可行性论证文件）

上述文件互相补充和解释，如有不明确或不一致之处，按照上述文件次序在先者为准。同一层次合同文件有矛盾的，以时间

较后的为准。

第四条　服务内容与质量标准

1.　技术服务内容

1)　部署满足金山区政务外网升级改造服务要求的基础设施。包括但不限于为政务外网服务提供的机房资源、电力资源、光纤资源、网络资源、安全资源等必须的基础设施。

2)　乙方须配合甲方及其用户进行部署前的测试、基础设施服务的实施及部署后的调试。

3)　乙方须提供网络运行管理平台服务,满足市大数据中心下发的《上海市电子政务外网运行管理系统对接规范》，按照甲方要求，提供电子政务外网的资源监测、资源配置、资源优化、服务监控、事件处理、运维流程、日常巡检、备份恢复、灾备管理、应急预案管理、服务质量监督和报告等服务，提供与市大数据中心运行管理平台的纵向接口对接能力。

4)　乙方须提供安全监测平台服务,满足市大数据中心下发的《上海市电子政务外网安全监测平台技术规范》，按照甲方要求，提供通报预警、漏洞扫描、威胁情报共享台、日志审计、安全管理控制等功能，确保全网受到安全保护、监测、管理，并满足《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）第三级安全测评通用要求，提供与市大数据中心安全监测平台的纵向接口对接能力。

5)　乙方须健全配套制度标准。乙方可提供基于自身平台的相关标准、办法及建议，如：可提供政务外网管理办法、运维制

度、应急预案等。

6) 乙方需开展电子政务外网等级保护测评三级工作，并交付一份等级保护测评报告至甲方。

2. 运行维护服务

乙方须建立专职的运行维护团队，提供7×24小时电话支持，5×8小时现场驻点运维服务等相关运维服务。驻场地点甲方指定为金山区行政服务中心东4楼机房，专职团队至少包含项目经理1名，必须具备高级工程师职称证书或一级建造师证书，除项目经理外，专职团队应至少包含工程师2名，必须具备CCNP、CCIE、HCNP、HCIE其中一类证书，工程师1名，必须具备信息安全认证工程师资格。

3. 日常运行服务

1) 网络接入服务

乙方承担金山区政务外网网络接入服务，涉及有新的点位接入区级电子政务外网的，乙方应做好需求对接，并出具接入方案，经甲方审核批准后实施。在有链路资源的前提下，乙方一个工作日内完成网络接入工作；有管道资源无光纤资源的前提下，十个工作日内完成网络接入工作；无链路资源的前提下，三十个工作日内完成网络接入工作。对于其它专网、专线、无线网络、应用系统、VPN用户等的接入需求，乙方应做好需求对接，出具安全可行的接入方案，经甲方审核批准后实施。乙方应确保网络接入实施服务需在网络运行管理平台工单上闭环留档。

2) 网络变更服务

乙方应提供网络变更服务。针对金山区电子政务外网系统存在的网络变更调整，如网络构架变更、设备变更、链路变更、放置地点变更、部署位置变更、配置变更、策略变更等，乙方应负责对接变更需求，出具合理的变更方案，并在网络运行管理平台上工单申请，经甲方审核批准后，由乙方负责实施并反馈，在运网络行管理平台上记录留档。

3) 网络优化服务

乙方应提供网络优化服务。乙方应对金山区电子政务外网的网络结构、网络配置、网络管理、管理工具、管理制度提出优化建议和优化方案，经甲方审核批准后实施，确保金山区电子政务外网的通畅、安全，尤其是保障区政务外网和互联网、无线网、市政务外网及各专网之间高速数据传输。

4) 网络安全服务

乙方应提供网络安全服务。安全服务应包含但不仅限于金山区电子政务外网的网络安全防护、入侵检测、流量控制、行为管理、安全准入、漏洞扫描、日志审计、风险预警、态势感知、趋势分析、安全通报、风险处理、事件处置等服务内容。运维团队应安排专业安全人员负责安全服务工作，对全网安全情况实时监控、定期检查、全面分析；对可能存在的网络安全风险主动发现、充分评估、预先感知、提前预警、做好防护；对已经发生的网络安全事件及时处置、及时反馈、总结分析、做好整改。

原则上服务期内至少提供甲方两次安全、应急演练服务。服务期内，乙方应全力配合甲方完成所有安全测评、安全检查、政

务外网考核、上级演练等工作。

5)　网络监测服务

乙方应提供网络监测服务。乙方应提供包含网络安全、网络管理、运行监测等一系列全网监测、运行管理系统及统一管理演示界面（统一运管监测门户），并具备展示能力。根据监测数据情况，乙方应形成相应的报表、报告，对全网各单位的网络运行情况和所有设备的健康情况、流量情况应能够从多个维度进行分析、研判，形成并及时向甲方提交日报、周报、月报、季度报、年报。

6)　备品备件和质保服务

乙方对所有新购设备应提供原厂质保服务；所有在用的底层接入交换机，应由乙方提供备品备件服务，并在需要替换时负责实施工作。

7)　应急响应服务

乙方应建立运维服务应急响应体系，作为运维体系中的重要环节，通过应急响应体系的建立，面对突发事件，运维团队的响应可以做到有条不紊，快速高效的解决突然的运维事件。

8)　重要活动保障服务

乙方应根据甲方的实际需求，在春节、国庆、护网、两会、党代会、进博会等重保期间，安排相应的技术力量，为甲方做好风险评估、安全防护和现场保障工作，必要时候需安排人员在甲方指定定点夜班值守。

9)　技术支持和培训服务

乙方应对甲方相关人员进行全面培训和技术支持，培训内容应包含但不仅限于涉及项目建设的网络构架、运行原理、设备知识、平台功能和操作培训等，并以操作手册、远程服务、现场支持等方式为甲方提供相应的技术支持服务。

10） 其它服务

乙方应无条件提供与金山区电子政务外网的运行维护、安全保障、监测管理、应急处置、技术支持等方面的其它服务。

4. 技术服务的方式

1）提供无推诿服务，即乙方应提供特殊措施，无论由于哪一方产生的问题而使系统发生不正常情况时，应全力协助各类资源和相关部门，使系统尽快恢复正常。

2）提供节点式管理，核心、汇聚节点重点全方位响应服务和技术支持；提供下沉式服务，服务覆盖范围到所有接入层，提供接入层的网络响应服务和技术支持。

3)乙方所提供的网络设备产品及系统软件维护及维保做出服务承诺。

4）乙方提供专业运维团队现场运维，根据实际情况安排好人员支援和储备，运维团队应具备主动发现问题、主动处理故障的运维能力，全面负责金山区电子政务外网所有网络故障的排查和处理工作，根据网络故障安全等级，一般故障应在 10 分钟内响应，4 小时内到达现场，24 小时内恢复；严重故障应即时进行响应，2 小时内到达现场，4 小时内恢复；重大故障应即时进行响应，30 分钟内到达现场，1 小时内恢复，故障处理应出具处理

报告，并经甲方签字确认。乙方应对多次重复或较大影响用户面的故障出具详细事故报告，并提出整改意见。

5. 质量标准

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，按地方标准、相关管理办法执行。若上述均无，按照通常标准或者符合合同目的的特定标准确定。

6. 服务考核

服务期内，合同服务期限到期前30天甲方组织对乙方进行考核评估，考核内容主要包括网络可靠性、网络可用性、网络安全性与服务质量，考核内如详见下表。

分类	考核项目	内容	分数	得分	备注
网络可靠性	网络可用率不低99.99%		15分		网络可用率=（一个月总时长-电路不可用总时长）×100%/一个月总时长 电路不可用总时长为电路中断时间的累加。电路不可用总时长是以采购人发现电路中断，并向供应商报障的时间开始计算，在供应商把恢复的电路交还与采购人时停止计算。采购人将不能把以下中断时间计算为“电路不可用总时长”： （1）当供应商交还恢复的电路，而采购人人员不能实时验收电路时，不论电路是否被接收，“电路不可用总时长”也会被终止计算；（2）当电路中断是因为采购人拥有或操控的设备的故障，或在供应商提供服务以外的设备或设施的故障；（3）在供应商预先通知并得到采购人允许的情况下发生的电路终断；（4）不可抗力影响。
网络	业务开通及	有线路资源	10分		6小时内完成开通；

可用性	变更	有管道资源无光纤资源	5 分		10 个工作日内开通
		无资源	5 分		30 个工作日内开通
	应急响应及抢修	在规定时间内应急响应	5 分		响应时间≤20min
		在规定时间内到达故障现场	5 分		重大故障 1 小时/严重故障 2 小时内/一般故障 4 小时。
		故障在规定时限内抢通	10 分		重大故障 2 小时/严重故障 4 小时内/一般故障 24 小时。
		事故报告	5 分		故障处理后 3 个工作日内及时分析原因并出具事故报告。
安全性	安全评测	提供等保 2.0 三级测评承诺函	10 分		投标方需在服务期内每年开展等级保护测评工作（三级），并交付给招标方。投标方需提供加盖投标人公章的承诺函作为证明材料。
服务质量	日常运维	驻场保障	5 分		安排工程师提供网络驻场保障服务。
	巡查巡检	日常巡检	5 分		每日对重要节点进行日常维护巡检服务。
		详细巡检	5 分		每季度对重要节点进行详细巡检服务。
		巡检报告	5 分		定期以书面或电子邮件形式反馈工作周期内的工作情况，包括：故障汇总、巡检情况、ping 测情况和资源变动情况等。
	重保	/	5 分		在春节、国庆、护网、两会、党代会、进博会等重保期间，供应商应安排相应的技术力量，为采购人做好现场保障工作。
	机房	机房运维	5 分		机房环境应做到防尘、防水，地面清洁，设备布局合理，布线规范。定期做好机房巡检工作，并做好记录。机房维护人员应熟知用电常识和用电应急处理步骤，严格管理机房所有出入人员，并做好记录。

考核评分 85 分及以上为 A，70-85 分为 B，60-69 分为 C，60 分以下为 D。考评结果为 A 则甲方全额支付当期服务费；如考评结果为 B，则甲方有权扣除合同服务费用总额 1%；如考评结果为 C，则甲方有权扣除合同服务费用总额的 3%；如考评结果为 D，

则甲方有权扣除合同服务费用总额的5%，并无条件解除本合同，更换服务提供商。

服务期内，采购人有权要求对下一个考核周期的考核内容进行调整，调整内容由采购人会同供应商共同细化，以备忘录形式加以约定。

第五条　　服务费用及支付方式

1.　本项目服务费用总额：

（含税价）：人民币大写__[合同中心-合同总价大写]_，小写__[合同中心-合同总价]__元。

本合同费用总额已包括甲方就乙方履行本合同事宜所应支付的全部费用及税费（包括但不限于营业税、增值税等）。

在一个服务周期内(1 年),当电子政务外网接入规模(招标具体点位基础上 10%以内的接入点位的新增)、网络出口或者链路资源等无法满足招标方使用要求时,投标人需无条件对现有网络进行优化扩容,一并做好机房等配套资源的扩容。

除另有约定外，甲方无需就本合同项下委托事项向乙方支付上述费用之外的任何其它费用及税费（包括但不限于营业税、增值税等）。

2.　服务费支付方式：

服务费支付由甲方以人民币电汇或转账方式付至乙方书面指定的账户，并由乙方在付款前向甲方出具合法、正规、有效发票。

1)　甲方分期向乙方支付合同费用:合同签订后支付合同价的 30%，项目建设完成后初验通过后支付 40%，一年整体运维验收通过后支付剩余 30%。

2)　因涉及财政拨款时间调整,乙方须同意甲方按实际财政拨付时间调整付款时间，该调整付款时间不应被视为甲方违约。甲方对付款时间进行调整的,应在财政拨款到位后合理时间内进行付款。

第六条　知识产权

1.　乙方应保证所提供的服务或其任何一部分均不会侵犯任何第三方的专利权、商标权或著作权或其它知识产权。若有，乙方应负责与第三方解决纠纷，若因此导致甲方损失的，甲方有权要求乙方赔偿甲方因此遭受的全部损失,包括但不限于直接损失、间接损失、诉讼费、律师费等。

2.　双方确定,乙方利用甲方提供的技术资料和工作条件所完成的服务成果的所有权利（包括知识产权）归甲方所有。乙方负有保密义务。

第七条　无产权瑕疵条款

乙方保证所提供的服务的所有权和知识产权完全属于乙方且无任何抵押、查封等产权瑕疵。如有产权瑕疵的，视为乙方违约。乙方应负担由此而产生的一切损失。

第八条　甲方的权利和义务

1.　甲方有权对合同规定范围内乙方的服务行为进行监督和检查，拥有监管权。有权定期核对乙方提供服务所配备的人员

数量。甲方对乙方不符合本合同要求的部分有权下达整改通知书，并要求乙方限期整改。乙方拒不整改或者整改后仍不能满足本合同要求的，甲方有权利终止本合同，并要求乙方承担由此造成的损失。

2. 甲方最终用户的政务外网业务接入到乙方的各机房环境后，甲方有权对乙方提供的政务外网的部署位置、环境、性能和安全情况进行测试，并要求乙方配合完成。

3. 根据本合同规定，按时向乙方支付应付服务费用。

4. 国家法律、法规所规定由甲方承担的其它责任。

第九条 乙方的权利和义务

1. 乙方应当履行本合同规定的委托服务范围内的服务义务，履行对本项目的管理责任。

2. 乙方接受甲方的监督,及时向甲方通告本项目服务范围内有关服务的重大事项，及时配合处理投诉。

3. 乙方应当按照《上海市电子政务外网管理办法》及甲方相关服务需求对承载甲方及甲方最终用户的政务外网业务进行管理，提供政务外网正常运行服务，并与甲方一起，接受行业管理部门及政府有关部门的管理、审查和检查。

4. 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,达到合同规定的服务质量的,应事先征得甲方书面同意，并由乙方承担第三方提供服务的费用,且乙方应当确保第三方遵守不低于本合同下乙方应当遵守的保密义务,由第三方完成的部分，乙方与第三方承担连带责任。

5. 乙方应协助甲方建立健全配套制度标准，包括：运行维护制度、应急预案、安全保障制度、运行监管办法等。

6. 如因乙方及乙方有关人员在从事提供本合同项下的服务中给甲方或第三方造成人员人身伤害或财产损失的，乙方应依法承担赔偿责任。

7. 在乙方提供运行维护服务期间，乙方应负责政务外网的具体管理、运行监控、安全防护等工作，按甲方需求定期向甲方提供书面报告。

8. 乙方在服务期内提出退出要求，需至少提前9个月向甲方书面提出退出申请，经甲方同意后需提供9个月的延续服务，乙方应无条件免费配合完成移交工作；在服务期满后，如乙方不再提供政务外网运行服务，乙方应无条件配合甲方完成相关业务和基础设施的迁移和切换工作，切换期最长不超过 6 个月。

第十条 安全

1. 安全能力要求。乙方应保证政务外网的运行要求通过第三方安全测评。若乙方不能达到为党政部门提供相应安全能力水平服务的资质要求，甲方有权终止合同，退出服务，并要求乙方承担由此产生的全部损失。

2. 安全责任划分。乙方向甲方提供电子政务外网服务，乙方责任边界为政务外网、互联网及市政务外网等各网络边界。

3. 保密与所有权。

1) 甲方提供给乙方的数据、设备等资源，以及政务外网业务运行过程中收集、产生的数据和文档等都属甲方所有。乙方应

保证甲方对这些资源的访问、利用、支配等权利。

2) 甲方提供给乙方的各种文档资料,及双方共同完成的涉及甲方的相关资料都归甲方所有,乙方应在合同终止时归还给甲方。甲方对所拥有的文件和资料具有不受限的权利。

3) 乙方应将甲方的数据、政务外网业务运行过程中收集、产生的数据和文档等作为保密内容对待,未经甲方及其最终用户许可(书面授权),乙方不得访问、修改、披露、利用、转移、转让、销毁甲方的数据。在服务合同终止时,应按甲方要求做好数据、文档等资源的移交和清除工作。

4) 乙方及其相关方为履行本合同在甲方指定场所工作期间需按照甲方的保密管理要求开展工作,具体要求甲方在乙方及其相关方进入指定场所前将书面告知。无论本合同以何种事由终止或者解除,乙方及其相关方的保密义务自获得保密信息之日起持续有效。

4. 应急响应。一旦发生信息安全事件,乙方应立即按照预先制定的《应急响应方案》执行应急响应措施。乙方应每年对《应急响应方案》进行风险评估,并根据评估结果更新《应急响应方案》。乙方应按照《应急响应方案》开展应急响应演练活动。

第十一条 违约责任

1. 甲乙双方必须遵守本合同并执行合同中的各项规定,保证本合同的正常履行。

2. 如因乙方工作人员在履行职务过程中的疏忽、失职、过错等故意或者过失原因给甲方造成损失或侵害,包括但不限于甲

方本身的财产损失、由此而导致的甲方对任何第三方的法律责任等，乙方对此均应承担全部的赔偿责任。

3. 金山区政务外网采用闭环管理,乙方在招标过程中承诺的服务内容和性能指标,在实际运行过程中不能满足或出现问题的，甲方有权根据问题严重程度进行相应处罚。

第十二条 不可抗力事件处理

1. 在合同有效期内,任何一方因不可抗力事件导致不能履行合同,则合同履行期可延长,其延长期与不可抗力影响期相同。

2. 不可抗力事件发生后,应立即书面通知对方,并寄送有关权威机构出具的证明。

3. 不可抗力事件延续30天以上，双方应通过友好协商，确定是否继续履行合同。

4. 受不可抗力影响的一方,应当尽可能地采取必要的行为和适当的措施减轻不可抗力对本合同的履行所造成的影响,若因没有采取适当措施致使另一方损失扩大的,该方不得就扩大损失的部分要求免责或赔偿。

5. 一方在迟延履行本合同时,发生了不可抗力的情况,迟延方的合同义务不能免除。

第十三条 解决合同纠纷的方式

1. 在执行本合同中发生的或与本合同有关的争端,双方应通过友好协商解决，经协商在30天内不能达成协议时，任何一方均可以向甲方所在地有管辖权的法院起诉。

2. 在诉讼期间,除争议事项外,双方应继续行使其在本合

同项下的其它权利，履行其在本合同项下的其它义务。

第十四条　其它

1. 本合同由甲乙双方于签字并盖章后生效。

2. 本合同一式肆份，甲方执贰份，乙方执贰份，具有同等法律效力。

3. 本合同中双方的地址、传真等联系方式为各自文书、信息送达地址，同时也作为双方争议发生时的各自法律文书送达地址（包括原审、二审、再审、执行及仲裁等），变更须提前书面通知对方。

4. 双方同意，附件为本合同不可分割的部分。若附件与合同正文有任何冲突，以合同正文为准。

5. 超出本合同约定的增量部分甲乙双方另行签订补充合同。

【以下无正文】

【本页为《2023 年金山区政务外网升级改造服务合同》签章页，无正文】

甲方：上海市金山区行政服务中心（盖章）

法定代表人（授权代表）：___[合同中心-采购单位联系人_1]____

地址：上海市金山区龙山路 555 号

签约日期：[合同中心-签订时间_1]

乙方：[合同中心-供应商名称_1]（盖章）

法定代表人（授权代表）：__[合同中心-供应商法人姓名]([合同中心-供应商法人性别])___

地址：[合同中心-供应商所在地_1]

签约日期：[合同中心-签订时间_2]

保 密 协 议

甲方：上海市金山区行政服务中心

乙方：[合同中心-供应商名称_2]

甲方工作内容可能涉及人员隐私等敏感或机密信息，为保护国家和个人的秘密信息，维护国家安全和社会稳定，依据《中华人民共和国保守国家秘密法》、《科学技术保密规定》等相关法规规定，双方就乙方在履行服务期间保守甲方秘密，同时维护公司合作伙伴的技术和商业秘密，签订下列条款共同遵守：

第一条双方确认，乙方在甲方服务期间，因履行服务合同或者主要是利用甲方的物质技术条件、业务信息等产生的发明创造、技术秘密和国家秘密等，有关的知识产权均属于甲方享有。甲方可以在其业务范围内充分自由地利用这些发明创造、技术秘密和国家秘密，进行生产、经营或者向第三方转让。乙方应当依甲方的要求，提供一切必要的信息和采取一切必要的行动，包括申请、注册、登记等，协助甲方取得和行使有关的知识产权。

第二条乙方在甲方服务期间所完成的、与甲方业务相关的发明创造、技术秘密、公司秘密和国家秘密，乙方主张由其本人享有知识产权的，应当及时向甲方申明。经甲方核实，认为确属于非职责成果的，由乙方享有知识产权，甲方不得在未经乙方明确授权的前提下利用这些成果进行生产、经营，亦不得自行向第三方转让。

乙方没有申明的，推定其属于职责成果，甲方可以使用这些成果进行生产、经营或者向第三方转让。即使日后证明实际上是非职责成果的，乙方亦不得要求甲方承担任何经济责任和法律责任。

乙方申明后，甲方对成果的权属有异议的，可以通过协商解决；协商不成的，通过当地仲裁委员会仲裁解决。

第三条乙方在甲方服务期间，须指定乙方代表和乙方派遣人员，该人员须与乙方签定相关保密协议，乙方须以书面通知的形式告知甲方，经甲方同意后，方可进驻甲方履行服务。

第四条乙方在甲方服务期间，必须遵守甲方规定的任何成文或不成文的保密规章、制度，履行与其工作职责相应的保密职责。

甲方的保密规章、制度没有规定或者规定不明确之处，乙方亦应本着谨慎、诚实的态度，采取任何必要、合理的措施，维护其于服务期间知悉或者持有的任何属于甲方或者虽属于第

三方但甲方承诺有保密义务的技术秘密、政务服务办公室秘密和国家秘密，以保持其机密性。

保密资料的接触范围严格限制在因本协议规定目的而需接触保密资料的各自负责任的代表的范围内。

第四条除了履行职务的需要之外，乙方承诺，未经甲方同意，不得以泄露、公布、发布、出版、传授、转让或者其他任何方式使任何第三方（包括按照保密制度的规定不得知悉该项秘密的甲方的其他职员）知悉属于甲方或者虽属于他人但甲方承诺有保密义务的技术秘密或其他商业秘密信息，也不得在履行职务之外使用这些秘密信息。

第五条乙方同意，乙方服务期满之后仍对其在甲方服务期间接触、知悉的属于甲方或者虽属于第三方但甲方承诺有保密义务的技术秘密、公司秘密和国家秘密信息，承担如同服务期间一样的保密义务和不保存、不使用、不外泄有关秘密信息的义务，而无论乙方因何种原因与甲方终止服务。

乙方服务期满之后承担保密义务的期限为自服务终止之日 3 年内。

第六条乙方承诺，在履行职责时，由于乙方的原因，造成甲方的技术秘密、相关信息和国家秘密等秘密信息的泄漏，乙方应当承担全部的法律责任和经济赔偿责任。

第七条乙方在履行职责时，不得擅自使用任何属于他人的技术秘密、公司秘密和国家秘密，亦不得擅自实施可能侵犯他人知识产权的行为。

若乙方违反上述承诺而导致甲方遭受第三方的侵仅指控时，乙方应当承担全部的法律责任和经济赔偿责任。

第八条乙方在履行职责时，按照甲方的明确要求或者为了完成甲方明确交付的具体工作任务必然导致侵犯他人知识产权的，若甲方遭受第三方的侵权指控，应诉费用和侵权赔偿不得由乙方承担或部分承担。

第九条乙方因工作上的需要所持有或保管的一切记录着甲方秘密信息的文件、资料、图表、笔记、报告、信件、传真、磁带、磁盘、光盘、软盘、录像带、幻灯片、仪器以及其他任何形式的载体，均归甲方所有，而无论这些秘密信息有无商业上的价值。

第十条乙方应当于服务终止时，或者于甲方提出请求时，返还全部属于甲方的财物，包括记载着甲方秘密信息的一切载体。

但当记录着秘密信息的栽体是由乙方自备的，且秘密信息可以从载体上消除或复制出来时，可以由甲方将秘密信息复制到甲方享有所有权的其他载体上，并把原载体上的秘密信息消除。此种情况乙方无须将载体返还，甲方也无须给予乙方经济补偿。

第十一条本协议提及的秘密，包括但不限于：人员信息、数据、技术方案、工程设计、业务流程、技术指标、计算机软件、数据库、研究开发记录、技术报告、检测报告、系统数据、评测结果、图纸、操作手册、技术文档、相关的函电，等等。

第十二条本协议中所称的服务期间，以甲乙双方签订合同为标志，并以该合同的有效期间为服务期间。

第十三条如乙方受甲方委派为第三方提供外包服务，乙方对甲方的保密责任和义务同样有效，作用范围自动延伸到外包服务工作的全过程。

第十四条因本协议而引起的纠纷，如果协商解决不成，任何一方均有权提交当地仲裁委员会仲裁。

第十五条本协议自双方签字或盖章完成之日起生效，本协议一式四份，双方各执两份，具有同等法律效力。

第十六条本协议如与双方以前的口头或书面协议有抵触，以本协议为准。本协议的修改必须采用双方同意的书面形式。

甲方（签字/盖章）：[合同中心-采购单位名称]　　乙方（签字/盖章）：[合同中心-供应商名称_3]

地址：[合同中心-采购单位所在地]　　地址：[合同中心-供应商所在地_2]

联系电话：__[合同中心-采购单位联系人电话_1]_　　联系电话：_[合同中心-供应商联系人电话_1]__

传真：__[合同中心-采购人单位传真]__　　传真：__[合同中心-供应商单位传真]__

邮政编码：_[合同中心-采购人单位邮编]__　　邮政编码：_[合同中心-采购人单位邮编_1]__

[合同中心-签订时间_3]　　[合同中心-签订时间_4]