伊犁哈萨克自治州信息便民政务服务门户平台建设项目（二标段）

第一册

采购人：伊犁哈萨克自治州政务服务管理局

采购代理机构：新疆新之建工程咨询有限公司

发　出 日 期：2022 年 2 月

目　录

第1章　投标人须知

一　总 则

1.采购人、采购代理机构及投标人

1.1　采购人：是指依法开展政府采购活动的国家机关、事业单位、团体组织。

本项目的采购人见投标人须知资料表。

1.2　采购代理机构：是指在集中采购机构或从事采购代理业务的社会中介机构。本项目的采购代理机构见投标人须知资料表。

1.3　投标人：是指向采购人提供货物、工程或者服务的法人、非法人组织或者自然人。本项目的投标人及其投标货物须满足以下条件：

1.3.1　在中华人民共和国境内注册，能够独立承担民事责任，有生产或供应能力的本国供应商。

1.3.2　具备《中华人民共和国政府采购法》第二十二条关于供应商条件的规定，遵守本项目采购人本级和上级财政部门政府采购的有关规定。

1.3.3　以采购代理机构认可的方式获得了本项目的招标文件。

1.3.4　符合投标人须知资料表中规定的其他要求。

1.3.5　若投标人须知资料表中写明允许采购进口产品，投标人应保证所投产品可履行合法报通关手续进入中国关境内。

若投标人须知资料表中未写明允许采购进口产品，如投标人所投产品为进口产品，其投标将被认定为**投标无效**。

1.3.6　若投标人须知资料表中写明专门面向中小企业采购的，如投标人为非中小企业且所投产品为非中小企业产品，其投标将被认定为**投标无效**。

1.4　如投标人须知资料表中允许联合体投标，对联合体规定如下：

1.4.1　两个以上供应商可以组成一个投标联合体，以一个投标人的身份投标。

1.4.2　联合体各方均应符合《中华人民共和国政府采购法》第二十二条规定的条件。

1.4.3　采购人根据采购项目对投标人的特殊要求，联合体中至少应当有一方符合相关规定。

1.4.4　联合体各方应签订共同投标协议，明确约定联合体各方承担的工作和相应的责任，并将共同投标协议连同作为投标文件第一部分的内容提交。

1.4.5　大中型企业、其他自然人、法人或者非法人组织与小型、微型企业组成联合体共同参加投标，共同投标协议中应写明小型、微型企业的协议合同金额占到共同投标协议投标总金额的比例。

1.4.6　联合体中有同类资质的供应商按照联合体分工承担相同工作的，按照较低的资质等级确定联合体的资质等级。

1.4.7　以联合体形式参加政府采购活动的，联合体各方不得再单独参加或者与其他供应商另外组成联合体参加本项目投标，否则相关投标将被认定为**投标无效**。

1.4.8　对联合体投标的其他资格要求见投标人须知资料表。

1.5　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，其相关投标将被认定为**投标无效**。

1.6　为本项目提供过整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加本项目上述服务以外的其他采购活动。否则其投标将被认定为**投标无效**。

1.7　投标人在投标过程中不得向采购人提供、给予任何有价值的物品，影响其正常决策行为。一经发现，其将被认定为**投标无效**。

2.资金来源

2.1　本项目的采购人已获得足以支付本次招标后所签订的合同项下的资金（包括财政性资金和本项目采购中无法与财政性资金分割的非财政性资金）。

2.2　项目预算金额和分项或分包最高限价见投标人须知资料表。

2.3　投标人报价超过招标文件规定的预算金额或者分项、分包最高限价的，其投标将被认定为**投标无效**。

3.投标人资格要求

3.1　满足《中华人民共和国政府采购法》第二十二条规定;

3.2　落实政府采购政策需满足的资格要求：无;

3.3　本项目的特定资格要求：标项 1、2:

（1）投标人有效的独立法人资格的营业执照原件（或复印件并加盖公章）;

（2）法定代表人授权委托书原件、被授权人《居民身份证》原件(法定代表人参加提供身份证原件);

（3）新疆新之建工程咨询有限公司开具的投标保证金收据原件。

（4）须提供在“信用中国”、国家企业信用信息公示系统和“中国政府采购”网上未被列入失信被执行人、重大税收违法案件当事人名单以及政府采购严重违法失信行为记录名单的书面承诺并加盖公章。

（5）社保机构出具的投标人为被授权人和项目组成员（3 人以上）缴纳 2021 年下半年任意 3 个月的社保资金证明原件或有电子专用章的缴费清单（被授权人和项目组成员为退休人员的提供退休证原件）;

（6）税务机关出具的 2021 年下半年投标人依法纳税凭证原件或有电子专用章的完税证明;

（7）会计事务所出具的投标人 2020 年度财务审计报告原件或银行出具的资信证明原件;

（8）投标人参与政府采购活动前三年内在经营活动中无重大违法记录的书面声明函原件;

（9）涉密系统集成乙级及以上资质（标项 1、2 均需具备）、电子与智能化专业承包二级及以上资质（标项 2 需具备）原件（或复印件并加盖公章）。

4.投标费用

不论投标的结果如何，投标人应承担所有与准备和参加投标有关的费用。

二　招标文件

5.招标文件构成

5.1 招标文件分为三册共 7 章，内容如下:

第一册

第 1 章 投标人须知

第 2 章 投标文件格式

第二册

第 3 章 招标公告

第 4 章 投标人须知资料表

第 5 章 货物需求一览表及技术规格

第 6 章 评标方法和标准

第三册

第 7 章政府采购合同格式

5.2 如本文件的前后内容不一致，以最后描述为准。

5.3 投标人应认真阅读招标文件所有的事项、格式、条款和技术规范等。如投标人没有按照招标文件要求提交全部资料，或者投标文件没有对招标文件在各方面都做出实质性响应，可能导致其投标将被认定为**投标无效**。

6.招标文件的澄清与修改

6.1 为了保证对招标文件的澄清和修改满足法律的时限要求，任何要求对招标文件进行澄清的投标人，均应在投标截止期十五日前，以书面形式将澄清要求通知采购人或采购代理机构。

6.2 采购人可主动地或在解答投标人提出的澄清问题时对招标文件进行澄清或修改。采购代理机构将以发布澄清（更正）公告的方式，澄清或修改招标文件，澄清或修改内容作为招标文件的组成部分。

6.3 澄清或者修改的内容可能影响投标文件编制的，采购代理机构将以书面形式通知所有购买招标文件的潜在投标人，并对其具有约束力。投标人在收到上述通知后，应及时向采购代理机构回函确认。

7.投标截止时间的顺延

为使投标人准备投标时有足够的时间对招标文件的澄清或者修改部分进行研究，采购人将依法决定是否顺延投标截止时间。

三 投标文件的编制

8. 投标范围及投标文件中标准和计量单位的使用

8.1 项目有分包的，投标人可对招标文件其中某一个或几个分包货物进行投标，除非在投标人须知资料表中另有规定。

8.2 投标人应当对所投分包招标文件中“服务需求”所列的所有内容进行投标，如仅响应某一包中的部分内容，其该包投标将被认定为**投标无效**。

8.3 无论招标文件第 5 章货物需求一览表及技术规格中是否要求，投标人所投货物均应符合国家强制性标准。

8.4 除招标文件中有特殊要求外，投标文件中所使用的计量单位，应采用中华人民共和国法定计量单位。

9.投标文件构成

9.1 投标人应完整地按招标文件提供的投标文件格式及要求遍写投标文件，投标文件应包括“开标一览表及资格证明文件”和“商务及技术文件”两部分。两部分单独装订成册分别密封递交，电子版单独密封递交。投标人应承担封装失误产生的任何后果。

9.2 上述文件应按照招标文件规定的格式填写、签署和盖章。

10. 证明投标标的的合格性和符合招标文件规定的技术文件

10.1 投标人应提交证明文件，证明其投标内容符合招标文件规定。该证明文件是投标文件的一部分。

10.2 上款所述的证明文件，可以是文字资料、图纸和数据，它包括:

10.2.1 货物主要技术指标和性能的详细说明;

10.2.2 货物从买方开始使用至招标文件规定的保质期内正常、连续地使用所必须的备件和专用工具清单，包括备件和专用工具的货源及现行价格;

10.2.3 对照招标文件技术规格，逐条说明所提供货物及伴随的工程和服务已对招标文件的技术规格做出了实质性的响应，或申明与技术规格条文的偏差和例外。

10.3 投标人应注意采购人在技术规格中指出的工艺、材料和设备的参照品牌型号或分类号仅起说明作用，并没有任何限制性。投标人在投标中可以选用替代牌号或分类号，但这些替代要实质上相当于技术规格的要求。采购人、采购代理机构承诺不以上述参照品牌型号或分类号作为评标时判定其投标是否有效的标准。

11.投标报价

11.1 所有投标均以人民币报价。投标人的投标报价应遵守《中华人民共和国价格法》。同时，根据《中华人民共和国政府采购法》第二条的规定，为保证公平竞争，如有货物主体部分的赠与行为，其投标将被认定为**投标无效**。

11.2 投标人应在投标分项报价表上标明投标货物及相关服务的单价（如适用）和总价，并由法定代表人或其授权代表签署。

11.3 投标分项报价表上的价格应按下列方式填写:

11.3.1 投标货物（包括备品备件、专用工具等）的出厂价（包括已在中国国内的进口货物完税后的仓库交货价、展室交货价或货架交货价），投标货物安装、调试、检验、技术服务和培训等费用;

11.3.2 货物运至最终目的地的运输费和保险费用。

11.4 投标人所报的各分项投标单价在合同履行过程中是固定不变的，不得以任何理由予以变更。任何包含价格调整要求的投标，其投标将被认定为**投标无效**。

11.5 每种货物只能有一个投标报价。采购人不接受具有附加条件的报价。

12.投标保证金

12.1 投标人应提交投标人须知资料表中规定的投标保证金，并作为其投标的一部分。

12.2 投标人存在下列情形的，投标保证金不予退还:

（1）在投标有效期内，撤销投标的;

（2）中标后不按本须知第 30 条的规定与采购人签订合同的;

（3）中标后不按本须知第 31 条的规定提交履约保证金的;
（4）中标后不按本须知第 32 条的规定缴纳中标服务费的;
（5）存在其他违法违规行为的。

12.3 政府采购信用担保试点范围内的项目，接受符合财政部门规定的政府采购投标担保函原件。

12.4 投标人未按本须知第 12.1 和 12.3 条规定提交投标保证金的，其投标将被认定为**投标无效**。

12.4.1 采用电汇形式的，一般可以实时入账。

12.4.2 采用支票形式的，投标人则应充分考虑支票入账时间，以确保投标保证金能按时进入指定账户。根据银行信息交换和付款时间，支票从递交至实际入账一般需要 4-5 个工作日。如投标人未及时提交支票或支票不符合银行委托收款要求（如污损、折叠、胶装等），导致投标保证金不能按时进入指定账户的，将按照招标文件的第 22.2 条相关规定处理。

12.5 联合体投标的，可以由联合体中的一方或者共同提交投标保证金。以一方名义提交投标保证金的，对联合体各方均具有约束力。

12.6 投标保证金的退还

12.6.1 中标人应在与采购人签订合同之日起 5 个工作日内，及时联系保证金收受机构办理投标保证金无息退还手续。

12.6.2 未中标投标人的投标保证金将在中标通知书发出之日暨中标结果公告公布之日起 5 个工作日内无息退还。投标人应及时联系保证金收受机构办理退还投标保证金手续。

12.6.3 政府采购投标担保函不予退回。

12.7 因投标人自身原因导致无法及时退还的，采购人或采购代理机构将不承担相应责任。

13.投标有效期

13.1 投标应在投标人须知资料表中规定时间内保持有效。投标有效期不满足要求的投标，其投标将被认定为**投标无效**。

13.2 为保证有充分时间签订合同，采购人或采购代理机构可根据实际情况，在原投标有效期截止之前，要求投标人延长投标文件的有效期。接受该要求的投标人将不会被要求和允许修正其投标，且本须知中有关投标保证金的要求须在延长的有效期内继续有效。投标人可以拒绝延长投标有效期的要求，其投标保证金将及时无息退还。上述要求和答复都应以书面形式提交。

14.投标文件的签署及规定

14.1 投标人应按投标人须知资料表中的规定，准备和递交投标文件资格证明文件、商务和技术文件正本、副本和电子文档，每份资格证明文件、商务和技术文件封皮须清楚地标明“正本”或“副本”。若正本和副本不符，以正本为准。

14.2 投标文件的正本需打印或用不褪色墨水书写，并由投标人的法定代表人或经其正式委托代理人按招标文件规定在投标文件上签字并加盖单位印章。委托代理人须持有书面的“法定代表人授权委托书”（投标文件格式二），并将其附在投标文件中。如对投标文件进行了修改，则应由投标人的法定代表人或其委托代理人在每一修改处签字。投标

文件的副本可采用正本的复印件。

14.3 所有投标文件采用不可拆装的胶订方式装订，否则其投标将被认定为**投标无效**。

14.4 投标文件因字迹潦草、表达不清或装订不当所引起的后果由投标人负责。

四 投标文件的递交

15.投标文件的密封和标记

15.1 为方便开标及进行资格审查，投标人应将投标文件第一部分和第二部分的内容分开单独密封提交，并在封皮正面标明“第一部分开标一览表及资格证明文件”或“第二部分商务及技术文件”字样。

15.2 所有包装封皮和信封上均应：

（1）注明招标公告或投标邀请书中指明的项目名称、招标编号、投标人名称和“在（开标时间）之前不得启封”的字样。

（2）在封口处加盖投标人单位章，或由法定代表人（或其委托代理人）签字。

15.3 如果投标人未按上述要求密封的，将被拒绝接收。

15.4 资格证明文件密封装订在其他投标文件中，其投标将被认定为**投标无效**。

16.投标截止

16.1 投标人应在投标人须知资料表中规定的截止时间前，将投标文件递交到招标公告中规定的地点。

16.2 采购人和采购代理机构有权按本须知的规定，延迟投标截止时间。在此情况下，采购人、采购代理机构和投标人受投标截止时间制约的所有权利和义务均应延长至新的截止时间。

16.3 采购人和采购代理机构将拒绝接收在投标截止时间后送达的投标文件。

17.投标文件的接收、修改与撤回

17.1 在投标截止时间后送达的投标文件的，采购人和采购代理机构将拒绝接收。

17.2 采购人或者采购代理机构收到投标文件后，应当如实记载投标文件的送达时间和密封情况，并向投标人出具以下签收回执。

接收投标文件回执单

招标编号			
项目名称			
投标人名称			
递交时间		投标文件密封情况	
接收单位			
接收人签字:			

17.3 递交投标文件以后，如果投标人要进行修改或撤回投标，须提出书面申请并在投标截止时间前送达开标地点，投标人对投标文件的修改或撤回

通知应按本须知规定编制、密封、标记。

采购人和采购代理机构将予以接收，并视为投标文件的组成部分。

17.4 在投标截止期之后，采购人和采购代理机构不接受投标人主动对其投标文件做任何修改。

17.5 采购人和采购代理机构对所接收投标文件概不退回。

五 开标及评标

18. 开标

18.1 采购人和采购代理机构将按投标人须知资料表中规定的开标时间和地点组织公开开标并邀请所有投标人代表参加。

投标人不足 3 家的，不得开标。

18.2 开标时，由投标人或其推选的代表检查自己或所代表的投标文件的密封情况，经记录后，由采购人或采购代理机构当众拆封投标文件第一部分，宣读投标人名称、投标价格及招标文件规定的内容。对于投标人在投标截止期前递交的投标声明，在开标时当众宣读，评标时有效。未宣读投标价格、价格折扣等实质内容，评标时不予承认。

18.3 采购人或采购代理机构将对开标过程进行记录，由参加开标的各投标人代表和相关工作人员签字确认，并存档备查。

18.4 投标人代表对开标过程和开标记录有疑义，以及认为采购人、采购代理机构相关工作人员有需要回避的情形的，应当场提出询问或者回避申请。

19.资格审查及组建评标委员会

19.1 采购人或采购代理机构依据法律法规和招标文件中规定的内容，对投标人及其货物的资格进行审查，未通过资格审查的投标人不进入评标；通过资格审查的投标人少于不足三家的，不得评标。

19.2 采购人或采购代理机构将在开标前1个工作日至投标截止后1小时的期间内查询投标人的信用记录。投标人存在不良信用记录的，其投标将被认定为**投标无效**。

19.2.1 不良信用记录指：投标人在中国政府采购网（www.ccgp.gov.cn）被列入政府采购严重违法失信行为记录名单，或在“信用中国”网站（www.creditchina.gov.cn）被列入失信被执行人、重大税收违法案件当事人名单，以及存在《中华人民共和国政府采购法实施条例》第十九条规定的行政处罚记录。

以联合体形式参加投标的，联合体任何成员存在以上不良信用记录的，联合体投标将被认定为**投标无效**。

19.2.2 查询及记录方式：采购人或采购代理机构经办人将查询网页打印、签字并存档备查。投标人不良信用记录以采购人或采购代理机构查询结果为准。

在本招标文件规定的查询时间之后，网站信息发生的任何变更均不再作为评标依据。

投标人自行提供的与网站信息不一致的其他证明材料亦不作为资格审查依据。

19.3 按照《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》及本项目本级和上级财政部门的有关规定依法组建的评标委员会，负责评标工作。

20.投标文件符合性审查与澄清

20.1 符合性审查是指依据招标文件的规定，从投标文件的有效性和完整性对招标文件的响应程度进行审查，以确定是否对招标文件的实质性要求做出响应。

20.2 投标文件的澄清

20.2.1 在评标期间，评标委员会将以书面方式要求投标人对其投标文件中含义不明确、对同类问题表述不一致或者有明显文字和计算错误的内容，以及评标委员会认为投标人的报价明显低于其他通过符合性检查投标人的报价，有可能影响履约的情况作必要的澄清、说明或补正。投标人的澄清、说明或补正应在评标委员会规定的时间内以书面方式进行，并不得超出投标文件范围或者改变投标文件的实质性内容。

20.2.2 投标人的的澄清、说明或补正将作为投标文件的一部分。

20.3 投标文件报价出现前后不一致的，按照下列规定修正:

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

（二）大写金额和小写金额不一致的，以大写金额为准;

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

(四)总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价按照第20.2条的规定经投标人确认后产生约束力,投标人不确认的，其投标将被认定为**投标无效**。

对不同文字文本投标文件的解释发生异议的，以中文文本为准。

20.4 如一个分包内只有一种产品，不同投标人所投产品为同一品牌的，按如下方式处理:

20.4.1 如本项目使用综合评分法，提供相同品牌产品且通过资格审查、符合性审查的不同投标人，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，由采购人或者采购人委托评标委员会按照招标文件中评标办法规定的方式确定一个投标人获得中标人推荐资格；未规定的采取随机抽取方式确定，其他同品牌投标人不作为中标候选人。

20.5 如一个分包内包含多种产品的，采购人或采购代理机构将在投标人须知资料表中载明核心产品，多家投标人提供的核心产品品牌相同的，按第20.4条规定处理。

20.6 投标人所投产品如被列入财政部与国家主管部门颁发的节能产品目录或环境标志产品目录或无线局域网产品目录，应提供相关证明，在评标时予以优先采购，具体优先采购办法见第六章评标方法和标准。

如采购人所采购产品为政府强制采购的节能产品，投标人所投产品的品牌及型号必须为清单中有效期内产品并提供证明文件，否则其投标将被认定为**投标无效**。

21.投标偏离

评标委员会可以接受投标文件中不构成实质性偏离的不正规或不一致。

22.投标无效

22.1 在比较与评价之前，根据本须知的规定，评标委员会要审查每份投标文件是否实质上响应了招标文件的要求。实质上响应的投标应该是与招标文件要求的全部条款、条件和规格相符，没有重大偏离的投标。对关键条款的偏离，将被认定为**投标无效**。投标人不得通过修正或撤销不符合要求的偏离，从而使其投标成为实质上响应的投标。

评标委员会决定投标的响应性只根据招标文件要求、投标文件内容及财政主管部门指定相关信息发布媒体。

22.2 如发现下列情况之一的，其投标将被认定为**投标无效**:

（1） 未按招标文件规定的形式和金额提交投标保证金的;

（2） 未按照招标文件规定要求签署、盖章的;

（3） 未满足招标文件中技术条款的实质性要求;

（4） 与其他投标人串通投标，或者与招标人串通投标;

（5） 属于招标文件规定的其他**投标无效**情形;

（6） 评标委员会认为投标人的报价明显低于其他通过符合性检查投标人的报价，有可能影响履约的，且投标人未按照规定证明其报价合理性的;

（7） 投标文件含有采购人不能接受的附加条件的;

（8） 不符合法规和招标文件中规定的其他实质性要求的。

23.比较与评价

23.1 经符合性审查合格的投标文件，评标委员会将根据招标文件确定的评标方法和标准，对其技术部分和商务部分作进一步的比较和评价。

23.2 评标严格按照招标文件的要求和条件进行。根据实际情况，在投标人须知资料表中规定采用下列一种评标方法，详细评标标准见招标文件第六章:

（1） 综合评分法，是指投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为中标候选人的评标方法。

23.3 根据《政府采购促进中小企业发展暂行办法》（财库[2011]181 号）、《财政部 司法部关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68 号）和《三部门联合发布关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141 号）的规定，对满足价格扣除条件且在投标文件中提交了《投标人企业类型声明函》或省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件的投标人，其投标报价扣除 6%后参与评审。具体办法详见招标文件第 6 章。

24.废标

出现下列情形之一，将导致项目废标:

（1）符合专业条件的供应商或者对招标文件做实质性响应的供应商不足三家;

（2）出现影响采购公正的违法、违规行为的;

（3）投标人的报价均超过了采购预算，采购人不能支付的;

（4）因重大变故，采购任务取消的。

25.保密原则

25.1 评标将在严格保密的情况下进行。

25.2 政府采购评审专家应当遵守评审工作纪律，不得泄露评审文件、评审情况和评审中获悉的商业秘密。

六 确定中标

26.中标候选人的确定原则及标准

除第 28 条规定外，对实质上响应招标文件的投标人按下列方法进行排序，确定投标候选人:

（1）本项目采用综合评分法的，评标结果按评审后得分由高到低顺序排列。得分相同的，按修正和扣除后的投标报价由低到高顺序排列。得分与投标报价均相同的处理方式详见招标文件第 6 章。

27.确定中标候选人和中标人

评标委员会将根据评标标准，按投标人须知资料表中规定数量推荐中标候选人；或根据采购人的委托，直接确定中标人。

28.采购任务取消

因重大变故采购任务取消时，采购人有权拒绝任何投标人中标，且对受影响的投标人不承担任何责任。

29.中标通知书和招标结果通知书

29.1 在投标有效期内，中标人确定后，采购人或者采购代理机构发布中标公告，同时以书面形式向中标人发出中标通知书。

29.2 中标通知书是合同的组成部分。

29.3 招标结果通知书和中标通知书同时发出。招标结果通知书中将告知未通过资格审查的投标人未通过的原因；采用综合评分法评审的，还将告知未中标人本人的评审得分和排序。

30.签订合同

30.1 中标人应当自发出中标通知书之日起 30 日内，与采购人签订合同。

30.2 招标文件、中标人的投标文件及其澄清文件等，均为签订合同的依据。

30.3 中标人拒绝与采购人签订合同的，采购人可以按照评审报告推荐的中标候选人名单排序，确定下一中标候选人为中标人，也可以重新开展政府采购活动。

30.4 当出现法规规定的**中标无效或中标结果无效**情形时，采购人可与排名下一位的中标候选人另行签订合同，或依法重新开展采购活动。

31.履约保证金

31.1 中标人应按照投标人须知资料表规定向采购人缴纳履约保证金（如采用保函形式，格式见本章附件 1）。

31.2 政府采购利用担保试点范围内的项目，除 31.1 规定的情形外，中标人也可以按照财政部门的规定，向采购人提供合格的履约担保函（格式见本章附件 2）。

31.3 如果中标人没有按照上述履约保证金的规定执行，将视为放弃中标资格，中标人的投标保证金将不予退还。在此情况下，采购人可确定下一候选人为中标人，也可以重新开展采购活动。

32.中标服务费

中标人须按照投标须知资料表规定，向采购代理机构支付中标服务费。

33.政府采购信用担保

33.1 本项目是否属于信用担保试点范围见投标人须知资料表。

33.2 如属于政府采购信用担保试点范围内，中小型企业投标人可以自由按照财政部门的规定，采用投标担保、履约担保和融资担保。

33.2.1 投标人递交的投标担保函和履约担保函应符合本招标文件的规定。

33.2.2 中标人可以采取融资担保的形式为政府采购项目履约进行融资。

33.2.3 合格的政府采购专业信用担保机构名单见投标人须知资料表。

34.廉洁自律规定

34.1 采购代理机构工作人员不得以不正当手段获取政府采购代理业务，不得与采购人、供应商恶意串通操纵政府采购活动。

34.2 采购代理机构工作人员不得接受采购人或者供应商组织的宴请、旅游、娱乐，不得收受礼品、现金、有价证券等，不得向采购人或者供应商报销应当由个人承担的费用。

34.3 为强化采购代理机构内部监督机制，供应商可按投标人须知资料表中的监督电话和邮箱，反映采购代理机构的廉洁自律等问题。

35.人员回避

投标人认为采购人员及其相关人员有法律法规所列与其他供应商有利害关系的，可以向采购人或采购代理机构书面提出回避申请，并说明理由。

36.质疑与接收

36.1 投标人认为招标文件、招标过程和中标结果使自己的权益受到损害的，可以根据《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》和《政府采购质疑和投诉办法》的有关规定，依法向采购人或其委托的采购代理机构提出质疑。

36.2 质疑供应商应按照财政部制定的《政府采购质疑函范本》格式（可从财政部官方网站下载）和《政府采购质疑和投诉办法》的要求，在法定质疑期内以纸质形式提出质疑，针对同一采购程序环节的质疑应一次性提出。

超出法定质疑期的、重复提出的、分次提出的或内容、形式不符合《政府采购质疑和投诉办法》的，质疑供应商将依法承担不利后果。

36.3 采购代理机构质疑函接收部门、联系电话和通讯地址，见投标人须知资料表。

附件1：履约保证金保函（格式）

（中标后开具）

致：（*买方名称*）

_____号合同履约保函

本保函作为贵方与（*卖方名称*）（以下简称卖方）于_____年_____月_____日就_____项目（以下简称项目）项下提供（*货物名称*）（以下简称货物）签订的（*合同号*）号合同的履约保函。

（*出具保函的银行名称*）（以下简称银行）无条件地、不可撤销地具结保证本行、其继承人和受让人无追索地向贵方以（*货币名称*）支付总额不超过（*货币数量*），即相当于合同价格的_____%，并以此约定如下：

1. 只要贵方确定卖方未能忠实地履行所有合同文件的规定和双方此后一致 同意的修改、补充和变动，包括更改和/或修补贵方认为有缺陷的货物（以下简称违约），无论卖方有任何反对，本行将凭贵方关于卖方违约说明的书面通知，立即按贵方提出的累计总额不超过上述金额的款项和按贵方通知规定的方式付给贵方。

2. 本保函项下的任何支付应为免税和净值。对于现有或将来的税收、关税、收费、费用扣减或预提税款，不论这些款项是何种性质和由谁征收，都不应从本保函项下的支付中扣除。

3. 本保函的条款构成本行无条件的、不可撤销的直接责任。对即将履行的合同条款的任何变更、贵方在时间上的宽限、或由贵方采取的如果没有本款可能免除本行责任的任何其它行为，均不能解除或免除本行在本保函项下的责任。

4. 本保函在本合同规定的保证期期满前完全有效。

谨启

出具保函银行名称：_____

签字人姓名和职务：_____

签字人签名：_____

公章：_____

附件2：履约担保函格式

（采用政府采购信用担保形式时使用）

政府采购履约担保函（项目用）

编号:

_____（采购人）:

鉴于你方与_____（以下简称供应商）于___年__月__日签定编号为　　的《_____政府采购合同》（以下简称主合同），且依据该合同的约定，供应商应在____年____月___日前向你方交纳履约保证金，且可以履约担保函的形式交纳履约保证金。应供应商的申请，我方以保证的方式向你方提供如下履约保证金担保:

一、保证责任的情形及保证金额

（一）在供应商出现下列情形之一时，我方承担保证责任:

1. 将中标项目转让给他人，或者在投标文件中未说明，且未经采购招标机构人同意，将中标项目分包给他人的;

2. 主合同约定的应当缴纳履约保证金的情形:

（1）未按主合同约定的质量、数量和期限供应货物/提供服务/完成工程的;

（2）_____。

（二）我方的保证范围是主合同约定的合同价款总额的_____%数额为元（大写_____），币种为_____。（即主合同履约保证金金额）

二、保证的方式及保证期间

我方保证的方式为: 连带责任保证。

我方保证的期间为: 自本合同生效之日起至供应商按照主合同约定的供货/完工期限届满后_____日内。

如果供应商未按主合同约定向贵方供应货物/提供服务/完成工程的，由我方在保证金额内向你方支付上述款项。

三、承担保证责任的程序

1. 你方要求我方承担保证责任的，应在本保函保证期间内向我方发出书面索赔通知。索赔通知应写明要求索赔的金额，支付款项应到达的帐号。并附有证明供应商违约事实的证明材料。

如果你方与供应商因货物质量问题产生争议，你方还需同时提供部门出具的质量检测报告，或经诉讼（仲裁）程序裁决后的裁决书、调解书，本保证人即按照检测结果或裁决书、调解书决定是否承担保证责任。

2. 我方收到你方的书面索赔通知及相应证明材料，在_____工作日内进行核定后按照本保函的承诺承担保证责任。

四、保证责任的终止

1. 保证期间届满你方未向我方书面主张保证责任的，自保证期间届满次日起，我方保证责任自动终止。保证期间届满前，主合同约定的货物\工程\服务全部验收合格的，自验收合格日起，我方保证责任自动终止。

2. 我方按照本保函向你方履行了保证责任后，自我方向你方支付款项（支

付款项从我方账户划出）之日起，保证责任即终止。

3. 按照法律法规的规定或出现应终止我方保证责任的其它情形的，我方在本保函项下的保证责任亦终止。

4. 你方与供应商修改主合同，加重我方保证责任的，我方对加重部分不承担保证责任，但该等修改事先经我方书面同意的除外；你方与供应商修改主合同履行期限，我方保证期间仍依修改前的履行期限计算，但该等修改事先经我方书面同意的除外。

五、免责条款

1. 因你方违反主合同约定致使供应商不能履行义务的，我方不承担保证责任。

2. 依照法律法规的规定或你方与供应商的另行约定，全部或者部分免除供应商应缴纳的保证金义务的，我方亦免除相应的保证责任。

3. 因不可抗力造成供应商不能履行供货义务的，我方不承担保证责任。

六、争议的解决

因本保函发生的纠纷，由你我双方协商解决，协商不成的，通过诉讼程序解决，诉讼管辖地法院为_____法院。

七、保函的生效

本保函自我方加盖公章之日起生效。

保证人：（公章）

年　　月　　日

第2章　投标文件格式

第一部分 开标一览表及资格证明文件

1 、开标一览表（见投标文件格式一）;

2、法人或者非法人组织的营业执照等证明文件复印件（须加盖本单位章）或自然人的身份证明复印件;

3、法定代表人授权书（见投标文件格式二，自然人投标的无需提供）;

4、具有良好的商业信誉和健全的财务会计制度的证明文件;

6、社会保障资金的缴纳记录;

7、参加政府采购活动前 3 年内在经营活动中没有重大违法记录的书面声明;

8、投标人须知资料表要求的其他资格证明文件;

9、投标人所投产品为进口产品按照投标人须知资料表中规定提供制造厂家的授权书见投标文件格式四）

1　开标一览表（投标文件格式一）

开标一览表

项目名称:　　招标编号:　　包号:

报价单位：人民币**万元**

货物名称	投标总价	投标保证金	合同履约期限	交货地点	备注
	大写: 小写:				

投标人名称（单位盖章）：_____

法定代表人或委托代理(签字):_____

注:1、此表应按投标人须知的规定装订密封。

2、此表中，每包的投标总价应和投标分项报价表的总价相一致。

2 法人或者非法人组织的营业执照等证明文件或自然人的身份证明

说明：1.提供有效的营业执照等证明文件复印件，复印件上应加盖本单位章。

2. 投标人为自然人的，应提供身份证明的复印件。

3.联合体投标应提供联合体各方满足以上要求的证明文件。

3 法定代表人授权委托书(投标文件格式二，自然人投标的无需提供)

本授权书声明：注册于（国家或地区的名称）的（*投标人*）的在下面签字的（*法人代表姓名、职务*）代表我单位授权（*单位名称*）的在下面签字的（*被授权人的姓名、职务*）为我单位的合法代理人，就（*项目名称*）的（*合同名称*）投标，以我单位名义处理一切与之有关的事务。

本授权书于_____年_____月_____日签字生效,特此声明。

投标人（盖单位章）;_____
法定代表人（签字或签章）：_____
身份证号码:_____
委托代理人:_____
身份证号码:_____
详细通讯地址:_____
邮 政 编 码 :_____
传　　真:_____
电　　话:_____

4 具有良好的商业信誉和健全的财务会计制度的证明文件

说明:

1、如提供本单位上年度经会计师事务所出具的审计报告复印件须加盖本单位章。

2、如提供银行出具的证明文件。银行证明文件可提供原件，也可提供银行在开标日前三个月内开具证明文件的复印件。若提供的是复印件，招标采购单位保留审核原件的权利。银行出具的证明文件应能说明该投标人与银行之间业务往来正常，企业信誉良好等。

3、如果是联合体投标，联合体各方均需提供上述证明。

5 投标保证金缴纳凭证复印件或投标担保函

投标人可将本项目投标保证金支付的汇款凭证、支票、汇票或保证金收据（如有）的复印件作为缴纳凭证装订在本部分，复印件上应加盖本单位章；使用银行保函等其他投标担保函的，应将担保函正本，装订在本部分正本中；如采用政府采购信用担保形式的，应使用（投标文件格式三），将原件装订在本部分正本中。

政府采购投标担保函 （项目用）（投标文件格式三）

编号:

_____（采购人或采购代理机构）:

鉴于_____（以下简称“投标人”）拟参加编号为_____的_____项目（以下简称“本项目”）投标，根据本项目招标文件，供应商参加投标时应向你方交纳投标保证金，且可以投标担保函的形式交纳投标保证金。应供应商的申请，我方以保证的方式向你方提供如下投标保证金担保:

一、保证责任的情形及保证金额

（一）在投标人出现下列情形之一时，我方承担保证责任:

1. 中标后投标人无正当理由不与采购人或者采购代理机构签订《政府采购合同》；

2. 招标文件规定的投标人应当缴纳保证金的其他情形。

（二）我方承担保证责任的最高金额为人民币_____元（大写_____），即本项目的投标保证金金额。

二、保证的方式及保证期间

我方保证的方式为: 连带责任保证。

我方的保证期间为: 自本保函生效之日起____个月止。

三、承担保证责任的程序

1. 你方要求我方承担保证责任的，应在本保函保证期间内向我方发出书面索赔通知。索赔通知应写明要求索赔的金额，支付款项应到达的账号，并附有证明投标人发生我方应承担保证责任情形的事实材料。

2. 我方在收到索赔通知及相关证明材料后，在_____个工作日内进行审查，符合应承担保证责任情形的，我方应按照你方的要求代投标人向你方支付投标保证金。

四、保证责任的终止

1. 保证期间届满你方未向我方书面主张保证责任的，自保证期间届满次日起，我方保证责任自动终止。

2. 我方按照本保函向你贵方履行了保证责任后，自我方向你贵方支付款项（支付款项从我方账户划出）之日起，保证责任终止。

3. 按照法律法规的规定或出现我方保证责任终止的其它情形的，我方在本保函项下的保证责任亦终止。

五、免责条款

1. 依照法律规定或你方与投标人的另行约定，全部或者部分免除投标人投标保证金义务时，我方亦免除相应的保证责任。

2. 因你方原因致使投标人发生本保函第一条第（一）款约定情形的，我方不承担保证责任。

3. 因不可抗力造成投标人发生本保函第一条约定情形的，我方不承担保证责任。

4. 你方或其他有权机关对招标文件进行任何澄清或修改，加重我方保证责任的，我方对加重部分不承担保证责任，但该澄清或修改经我方事先书面同意的除外。

六、争议的解决

因本保函发生的纠纷，由你我双方协商解决，协商不成的，通过诉讼程序解决，诉讼管辖地法院为_____法院。

七、保函的生效

本保函自我方加盖公章之日起生效。

保证人：（公章）

年　　月　　日

6 社会保障资金的缴纳记录

说明：1.按照投标人须知资料表中的规定提供复印件。
2.复印件上应加盖本单位章。
3.如果是联合体投标，联合体各方均需提供上述证明。

7　参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明

说明：1.投标人应按照相关法规规定如实作出说明。

2．按照招标文件的规定加盖单位章（自然人投标的无需盖章，需要签字）。

3.如果是联合体投标，联合体各方均需提供上述证明。

8 投标人须知资料表要求的其他资格证明文件

说明：1.应提供投标人须知资料表要求的其他资格证明文件。

2.复印件上应加盖本单位章（自然人投标的无需盖章，需要签字）。

3. 如果是联合体投标，联合体各方需提供的满足招标文件要求的其他资格证明文件。

9 进口产品制造厂家的授权书 （投标文件格式四）

致：采购代理机构

我们（*制造商名称*）是按（*国家名称*）法律成立的一家制造商，主要营业地点设在（*制造商地址*）。兹指派按（*国家名称*）的法律正式成立的，主要营业地点设在（*经销商地址*）的（*经销商名称*）作为我方真正的合法的代理人进行下列有效的活动：

（1）代表我方办理贵方____（招标编号）___投标邀请要求提供的由我方制造的货物的有关事宜，并对我方具有约束力。

（2）作为制造商，我方保证以投标合作者来约束自己，并对该投标共同和分别承担招标文件中所规定的义务。

（3）我方兹授予____（经销商名称）____全权办理和履行上述我方为完成上述各点所必须的事宜，具有替换或撤销的全权。兹确认____（经销商名称）____或其正式授权代表依此合法地办理一切事宜。

（4）我方于_____年_____月_____日签署本文件，____（经销商名称）于____年_____月_____日接受此件，以此为证。

制造商名称：（盖章）_____

签字人职务和部门：_____

签字人姓名：_____

签字人签名：_____

第二部分　商务及技术文件

1、投标书（投标文件格式五）
2、投标保证金缴纳凭证复印件或投标担保函（见投标文件格式六）
3、投标分项报价表（投标文件格式七）
4、货物说明一览表（投标文件格式八）
5、技术规格偏离表（投标文件格式九）
6、商务条款偏离表（投标文件格式十）
7、符合《政府采购促进中小企业发展暂行办法》、《关于政府采购支持监狱企业发展有关问题的通知》和《三部门联合发布关于促进残疾人就业政府采购政策的通知》价格扣减条件的投标人须提交）
7-1《投标人企业（单位）类型声明函》（投标文件格式十一）
7-2《制造商投标人企业（单位）类型声明函》（投标文件格式十二）
7-3《残疾人福利性单位声明函》（投标文件格式十三）
8、投标人关联单位的说明（格式自拟）
9、投标文件还应包括投标人须知第10条的所有技术文件
10、所投产品近三年有销售业绩（需提供中标通知书或合同）
11、售后服务体系

1　投标书（投标文件格式五）

致：采购代理机构

根据贵方(*项目名称*)项目的投标邀请(*招标编号*)，签字代表(*姓名、职务*)经正式授权并代表投标人(*名称、地址*)提交下述文件正本___份、副本_____份及电子文档_____份，并以_____形式出具的金额为人民币_____元的投标保证金。

据此，签字代表宣布同意如下：

（1）附投标价格表中规定的应提供货物的投标总价详见开标一览表，其中由小型和微型企业制造产品的价格为_____（用文字和数字表示），占投标总价　　%。

（2）本投标有效期为自投标截止之日起_____个日历日。

（3）联合体中的大中型企业和其他自然人、法人或者非法人组织，与联合体中的小型、微型企业之间_____（存在、不存在）投资关系（如果是联合体的话）。

（4）已详细审查全部招标文件，包括所有补充通知（如果有的话），完全理解并同意放弃对这方面有不明、误解和质疑的权力。

（5）在规定的开标时间后，遵守招标文件中有关保证金的规定。

（6）我方不是为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，我方不是采购代理机构的附属机构。

（7）在领取中标通知书的同时按招标文件规定的形式，向贵方一次性支付中标服务费。

（8）按照贵方可能要求，提供与其投标有关的一切数据或资料，完全理解贵方不一定接受最低价的投标或收到的任何投标。

（9）按照招标文件的规定履行合同责任和义务。

与本投标有关的一切正式往来信函请寄：

地址_____　　传真_____

电话_____　　电子函件_____

法定代表人或其委托代理人签字----------

投标人名称（全称）----------

投标人开户银行（全称）_____

投标人银行帐号_____

投标人单位章----------

日期----------

2　投标保证金缴纳凭证复印件或投标担保函

投标人可将本项目投标保证金支付的汇款凭证、支票、汇票或保证金收据（如有）的复印件作为缴纳凭证装订在本部分，复印件上应加盖本单位章；使用银行保函等其他投标担保函的，应将担保函正本，装订在本部分正本中；如采用政府采购信用担保形式的，应使用政府采购投标担保函（投标文件格式六），将原件装订在本部分正本中。

政府采购投标担保函 （项目用）（投标文件格式六）

编号:

_____（采购人或采购代理机构）:

鉴于_____（以下简称“投标人”）拟参加编号为_____的_____项目（以下简称“本项目”）投标，根据本项目招标文件，供应商参加投标时应向你方交纳投标保证金，且可以投标担保函的形式交纳投标保证金。应供应商的申请，我方以保证的方式向你方提供如下投标保证金担保:

一、保证责任的情形及保证金额

（一）在投标人出现下列情形之一时，我方承担保证责任:

1. 中标后投标人无正当理由不与采购人或者采购代理机构签订《政府采购合同》；

2. 招标文件规定的投标人应当缴纳保证金的其他情形。

（二）我方承担保证责任的最高金额为人民币_____元（大写_____），即本项目的投标保证金金额。

二、保证的方式及保证期间

我方保证的方式为: 连带责任保证。

我方的保证期间为: 自本保函生效之日起____个月止。

三、承担保证责任的程序

1. 你方要求我方承担保证责任的，应在本保函保证期间内向我方发出书面索赔通知。索赔通知应写明要求索赔的金额，支付款项应到达的账号，并附有证明投标人发生我方应承担保证责任情形的事实材料。

2. 我方在收到索赔通知及相关证明材料后，在_____个工作日内进行审查，符合应承担保证责任情形的，我方应按照你方的要求代投标人向你方支付投标保证金。

四、保证责任的终止

1. 保证期间届满你方未向我方书面主张保证责任的，自保证期间届满次日起，我方保证责任自动终止。

2. 我方按照本保函向你贵方履行了保证责任后，自我方向你贵方支付款项（支付款项从我方账户划出）之日起，保证责任终止。

3. 按照法律法规的规定或出现我方保证责任终止的其它情形的，我方在本保函项下的保证责任亦终止。

五、免责条款

1. 依照法律规定或你方与投标人的另行约定，全部或者部分免除投标人投标保证金义务时，我方亦免除相应的保证责任。

2. 因你方原因致使投标人发生本保函第一条第（一）款约定情形的，我方不承担保证责任。

3. 因不可抗力造成投标人发生本保函第一条约定情形的，我方不承担保证责任。

4. 你方或其他有权机关对招标文件进行任何澄清或修改，加重我方保证责任的，我方对加重部分不承担保证责任，但该澄清或修改经我方事先书面同意的除外。

六、争议的解决

因本保函发生的纠纷，由你我双方协商解决，协商不成的，通过诉讼程序解决，诉讼管辖地法院为_____法院。

七、保函的生效

本保函自我方加盖公章之日起生效。

保证人：（公章）

年　　月　　日

3　投标分项报价表（投标文件格式七）

项目名称:　　招标编号:　　包号:　　报价单位：人民币万元

序号	名称	型号和规格	数量	原产地	制造商名称	单价	总价	备注
1.	货物名称							
2.	备品备件							
3.	专用工具							
4.	安装、调试、检验							
5.	培训							
6.	技术服务							
总价:								

法定代表人或其委托代理人签字:_____

投标人(盖单位章):_____

注:1.如果投标人认为需要，每种货物填写一份该表。

2.如果按单价计算的结果与总价不一致,以单价为准修正总价。

3.如果不提供详细分项报价将视为没有实质性响应招标文件。

4.上述各项的详细分项报价，应另页描述。

5.如果开标一览表（报价表）内容与投标文件中明细表内容不一致的，以开标一览表（报价表）内容为准。

4　货物说明一览表（投标文件格式八）

项目名称:　　招标编号:　　包号:

序号	货物名称	主要规格	数量	交货期	交货地点	其它

法定代表人或其委托代理人签字:_____

投标人(盖单位章):_____

注: 各项货物详细技术性能应另页描述。

5　技术规格偏离表（投标文件格式九）

项目名称:　　招标编号:　　包号:

序号	货物名称	招标文件条款号	招标规格	投标规格	偏离	说明

法定代表人或其委托代理人签字:_____

投标人(盖单位章):_____

6　商务条款偏离表（投标文件格式十）

项目名称:　　招标编号:　　包号:

序号	招标文件条款号	招标文件的商务条款	投标文件的商务条款	说明

法定代表人或其委托代理人签字:_____

投标人(盖单位章):_____

7-1 投标人企业（单位）类型声明函（投标文件格式十一）

本企业（单位）郑重声明下列事项（按照实际情况勾选或填空）：

1、□本企业（单位）为直接投标人提供本企业（单位）制造的货物。

（1）根据《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业[2011]300号）规定的划分标准，本企业为------（请填写：中型、小型、微型）企业。

（2） 本企业_____（请填写：是、不是）监狱企业。后附省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。

（3） 根据《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）。本单位_____（请填写：是、不是）残疾人福利性单位。

2、□本企业（单位）为代理商，提供其他------（请填写：中型、小型、微型）企业、监狱企业或残疾人福利性单位制造的货物。本条所称货物不包括使用大型企业注册商标的货物。（后附制造商企业（单位）类型声明函）

3、□本企业（单位）为联合体一方，提供本企业（单位）制造的货物，由本企业（单位）承担工程、提供服务。本企业（单位）提供协议合同金额占到共同投标协议合同总金额的比例为_____。

本企业（单位）对上述声明的真实性负责。如有虚假，将依法承担相应责任。

投标人名称（盖单位章）：----------　---

日　期：----------

7-2　制造商企业（单位）类型声明函（投标文件格式十二）

本企业（单位）作为------单位的------ 项目的设备制造商，参加政府采购活动。根据《政府采购促进中小企业发展暂行办法》（财库[2011]181号），《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业[2011]300号）、《财政部、司法部关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68号）以及《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）的有关规定，作出如下声明:

本企业为------（请填写：中型、小型、微型）企业。

本企业_____（请填写：是、不是）监狱企业。后附省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。

本单位为_____（请填写：是、不是）残疾人福利性单位。

本企业（单位）提供本企业（单位）制造的货物。

本企业（单位）对上述声明的真实性负责。如有虚假，将依法承担相应责任。

本声明函经制造商和投标人共同盖章生效。

制造商名称（盖单位章）:

投标人名称（盖单位章）: ----------　---

日　期: ----------

7-3　残疾人福利性单位声明函（投标文件格式十三）

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）的规定，本单位为符合条件的残疾人福利性单位，且本单位参加------单位的------项目采购活动提供本单位制造的货物，或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

残疾人福利性单位名称（盖单位章）：----------

日　期：----------

8　投标人关联单位的说明

说明：投标人应当如实披露与本单位存在下列关联关系的单位名称：
（1）与投标人单位负责人为同一人的其他单位；
（2）与投标人存在直接控股、管理关系的其他单位。

9　投标文件还应包括投标人须知第10条的所有技术文件

第二册

第3章 招标公告

伊犁哈萨克自治州信息便民政务服务门户平台建设项目
公开招标公告（三次）

项目概况:伊犁哈萨克自治州信息便民政务服务门户平台建设项目的潜在供应商应在伊宁市解放路77号亚欧国际9层获取招标文件,并于2022年3月14日11:00前提交投标文件。

一、项目基本情况

项目编号:2140xzjP194-3

项目名称:伊犁哈萨克自治州信息便民政务服务门户平台建设项目

采购方式: 公开招标

预算金额（元）: 6790000

最高限价（元）: 6370000

采购需求:

标项名称:伊犁哈萨克自治州政务服务管理局机房设备

数量:不限

预算金额（元）:6790000

简要规格描述或项目基本概况介绍、用途: 详见采购文件

备注:

合同履约期限: 合同签订后30日内完成本次采购设备、调试及安装。

本项目（否）接受联合体投标。

二、申请人的资格要求:

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: 无;

3.本项目的特定资格要求: 标项1: 3.1、落实政府采购政策需满足的资格要求:（1）财政部、国家发展改革委、生态环境部、市场监管总局《关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库[2019]9号文）;（2）财政部、生态环境部《关于印发环境标志产品政府采购品目清单的通知》（财库[2019]18号文）;（3）财政部、发展改革委《关于印发节能产品政府采购品目清单的通知》（财库[2019]19号文）;（4）市场监管总局《市场监管总局关于发布参与实施政府采购节能产品、环境标志产品认证机构名录的公告》（2019年第16号）;（5）工信部等部委发布的《关于印发中小企业划型标准规定的通知》（工信部联企业[2011]300号）及《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）、关于转发《政府采购促进中小企业发展管理办法》的通知（兵财库〔2021〕7号）;（6）根据财政部、司法部关于政府采购支持监狱企业发展有关问题的通知（财库[2014]68号）, 财政部、民政部、中国残疾人联合会关于促进残疾人就业政府采购政策的通知（财库[2017]141号）, 监狱企业、残疾人福利性单位视同小型、微型企业, 享受。3.2本项目的特定资格要求:（1）投标人有效的独立法人资格的营业执照原件（或复印件并

加盖公章）；（2）法定代表人授权委托书原件、被授权人《居民身份证》原件(法定代表人参加提供身份证原件)；（3）新疆新之建工程咨询有限公司开具的投标保证金收据原件；（4）须提供在“信用中国”、国家企业信用信息公示系统和“中国政府采购”网上未被列入失信被执行人、重大税收违法案件当事人名单以及政府采购严重违法失信行为记录名单的书面承诺并加盖公章；（5）社保机构出具的投标人为被授权人和项目组成员（3人以上）缴纳2021年下半年任意3个月的社保资金证明原件或有电子专用章的缴费清单(被授权人和项目组成员为退休人员的提供退休证原件）；（6）税务机关出具的2021年下半年投标人依法纳税凭证原件或有电子专用章的完税证明；（7）会计事务所出具的投标人2020年度财务审计报告原件或银行出具的资信证明原件；（8）投标人参与政府采购活动前三年内在经营活动中无重大违法记录的书面声明函原件；（9）涉密系统集成乙级及以上资质、电子与智能化专业承包二级及以上资质原件(或复印件并加盖公章）

说明：其中（1）-（9）为资格审查时的必备条件，投标人必须按要求现场单独提供，如果提供不全(或密封在投标文件中）则视为对招标文件资格审查内容的不响应，投标将被拒绝。

三、获取招标文件

时间：2022年2月22日至2022年3月1日，每天上午10:00至14:00，下午15:30至19:00（北京时间，法定节假日除外）

地点：伊宁市解放路77号亚欧国际9层

方式：现场来人获取（供应商购买招标文件时请随身携带法定代表人授权委托书及被授权人的身份证、营业执照。所有购买招标文件的供应商需提供上述资料加盖企业公章的复印件两套交由采购代理公司存档。）

售价（元）：200

四、提交投标文件截止时间、开标时间和地点

提交投标文件截止时间：2022年3月14日 11:00（北京时间）

投标地点:伊宁市海棠路3号州财政局办公楼附楼1层州政府采购中心 一楼开标厅

开标时间：2022年3月14日 11:00

开标地点:伊宁市海棠路3号州财政局办公楼附楼1层州政府采购中心 一楼开标厅

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：无。

七、凡对本次招标提出询问，请按以下方式联系。

1.采购人信息

名　　称：伊犁哈萨克自治州政务服务管理局

地　　址：伊宁市边境经济合作区广东路52号

联系方式：0999-8024006

2.采购代理机构信息

名　　称：新疆新之建工程咨询有限公司

地　　址：伊宁市解放路77号亚欧国际九楼

联系方式：8039929

3.项目联系方式

项目联系人：韩绪
联系方式：18699906566

第4章投标人须知资料表

本表是本招标项目的具体资料，是对投标人须知的具体补充和修改，如有矛盾，应以本资料表为准。

条款号	内　　容
1.1	采购人：伊犁哈萨克自治州政务服务管理局 地　址：伊宁市边境经济合作区广东路52号 电　话：0999-8024006
1.2	采购代理机构：新疆新之建工程咨询有限公司 地址：伊宁市解放路77号亚欧国际九楼 业务联系人：韩绪 电话：18699906566 传真：0999-8039929
1.3.4	合格投标人的其他资格要求：详见招标公告申请人的资格要求
1.3.5	是否允许采购进口产品：否 *（是、否）*
1.3.6	是否为专门面向中小企业采购：否 *（是、否）*
1.4	是否允许联合体投标：否 *（是、否）*
1.4.8	联合体的其他资格要求：/
2.2	项目预算金额：880万元；2标段最高限价：637万元，**投标人报价不能超过最高限价，否则视为不响应招标文件，作废标处理。**
8.1	如投标商对多个包进行投标，可以中标/包
12.1	保证金形式：☐保函 ☑电汇 ☐支票 保证金数额：二标段10万元 保证金收款人：新疆新之建工程咨询有限公司伊犁分公司 开户银行：新疆伊犁农村商业银行股份有限公司 账　　号：812010312010136147390 行　　号：402898000017 社会信用代码:91654002MA786EFJ99
13.1	投标有效期：30日历日
14.1	第一部分投标文件：正本：1份、副本：4份； 第二部分投标文件：正本：1份、副本：4份； 除上述文件外，还须递交单独密封的《开标一览表》1份、投标文件电子文档1份（包括U盘1个） 电子文档内容包括正本扫描件，盖公章并扫描成PDF格式。
16.1	投标截止时间：2022年3月14日11:00
18.1	开标时间：2022年3月14日11:00 开标地点：伊宁市海棠路3号州财政局办公楼附楼1层
20.5	核心产品：/
23.2	评标方法：适用综合评标法
27	推荐中标候选供应商的数量：3名

27	招标人是否委托评标委员会直接确定中标人：__是__ *（是、否）*
31.1	履约保证金金额：合同总价的__/__*（不得超过政府采购合同金额的 10%）* 履约保证金形式：__/__ 提交履约保证金的时间：/
32	中标服务费：☑本项目中标服务费由中标人支付。 支付形式：__电汇__ 支付时间：__领取中标通知书时支付__
33.1	本项目是否属于信用担保试点范围：__否__ *（是、否）*
33.2	政府采购专业担保机构：/ 2. 本项目采购人本级和上级财政部门政府采购有关规定增加的担保机构：/
34.3	反腐倡廉监督电话/邮箱：__0999-8075070__
36.3	接收部门：__伊犁州财政局国库处__ 联系电话：__0999-8075070__ 通讯地址：__伊宁市海棠路 3 号__
适用于本投标人须知的额外增加的变动：	
1	投标人提供__有效书面__证明具有良好的商业信誉和健全的财务会计制度*（会计师事务所出具的上一年度财务审计报告或银行出具的说明投标人商业信誉或结算情况等事项的证明文件。）*
2	提供投标人的最近__3__个月的社保缴纳记录; 在法规范围内不需提供的，应做书面说明和证明文件。
3	进口产品制造商授权等是否作为资格要求：__否__*（是、否）*
4	根据货物特点，提出相应货物资格证书，如涉密资质、电子与智能化专业承包资质等法规要求的资格条件
5	**资格审查：开标时，供应商应在密封的投标文件之外随身携带招标公告申请人的资格要求的资料，以备开标时，采购人对其资格进行审查。 开标时必须按公告要求提交，如有缺项、未按要求提供的情况，视为投标人不响应本次招标，资格审查将不予通过。**
6	付款方式：付款方式合同另行约定；交货地点：采购人指定地点。
7	质量保证期：自验收合格交付采购人使用之日起 3 年（提供原厂商 3 年免费质保及升级服务）。

资格审查表

投标人名称	审查项目									结论
	在中华人民共和国境内注册	营业执照等证明	法定代表人授权委托书	具有良好的商业信誉和健全的财务会计制度的证明文件	社保缴纳记录	信用记录	*投标人须知资料表中要求的其他资格要求*	*进口产品制造商授权（如作为资格条件）*	招标公告中要求的资格条件	

第5章货物需求一览表及服务要求

一、项目概述

1、建设背景

政府网站集约化建设是国务院办公厅向各级人民政府提出的一项工作任务，根据国家和自治区有关文件精神，进一步加快政府网站集约化建设，将政府网站打造成整体联动、资源共享、权威准确、集中全面的政务信息数据平台，成为政府网站提升服务水平、提高主动服务精准服务能力的重要保障，并利用政府网站主动做好政策解读、积极回应社会关切、提高政务舆情回应实效、畅通群众投诉举报渠道，促进政府网站成为政府沟通民众的重要桥梁和纽带。

2017 年 5 月，国务院办公厅印发《政府网站发展指引的通知》（国办发〔2017〕47 号），要求参照指引制定政府网站管理办法，规范网站域名，严格开办流程，加强监管考核，推进资源集约，实现政府网站有序健康发展，对于政府网站集约化建设提出了详细的要求。2017 年 10 月，新疆维吾尔自治区人民政府办公厅印发《新疆政府门户网站建设与管理规范》（新政办发〔2017〕190 号），要求进一步加强和规范自治区各级政府网站的规划建设与应用管理工作，优化社会管理和公共服务，提升政府网上服务能力和水平。

2019 年 10 月，自治区开始建设自治区政府网站集约化平台和统一信息资源库，目前已经集约化了自治区政府网站主门户和直属部门机构政府网站，建设了自治区统一的政府网站技术平台，实现开设子站、栏目、频道等，主要提供信息内容、资源集约、技术安全、运维保障等功能。

2020 年自治区印发《新疆维吾尔自治区政府网站集约化平台管理办法（试行）》（新政办函〔2020〕115 号），根据文件要求为避免重复投资，加强信息资源整合，保障网站技术安全，进一步加强政府网站管理，引领自治区各级政府网站创新发展，现拟将伊犁哈萨克自治州（以下简称“伊犁州”）各级政府网站包括伊犁哈萨克自治州政府门户网站以及各县（市）政府网站基于新疆自治区政府网站集约

化平台环境进行建设。

2、建设目标

按照“统一组织领导、统一规划实施、统一标准规范、统一网络平台、统一安全管理”的原则，利用已建成的自治区政府网站统一集约化平台为支撑，通过统一的标准规范和管理规范的建设，对伊犁州各级政府网站（网站改版、数据迁移）进行集约化升级改造。做好建设后数据的校验工作的质量把控，确保历史数据建设完整性、一致性、有效性，总分平衡检查，记录条数检查，特殊样本数据的检查均无异常，最终实现网站建设的“四统一，两集中”，即统一标准体系、统一技术平台、统一安全防护、统一运维监管，集中管理信息数据，集中提供内容服务。

按照国家等保三级标准构建平台运行环境。制订安全管理制度和应急响应机制，确保环境安全、平台安全、数据安全、应用安全。配合进行每年的等保评测。保证信息系统在物理、网络安全运行、信息保密和管理等方面的总体要求，科学合理评估信息系统风险，协助合理确定安全保护等级，在此基础上科学规划设计一整套完整的安全体系改造加固方案。该安全体系需要全面保卫网络和基础设施、边界和外部接入、计算环境、支持性基础设施、数据和系统等方面内容，实现信息资源的机密、完整、可用、不可抵赖和可审计性，基本做到“进不来、拿不走、改不了、看不懂、跑不了、可审计、打不垮”。

3、建设内容

遵循新疆维吾尔自治区政府网站标准规范，结合伊犁哈萨克自治州实际情况，在新疆维吾尔自治区政府网站集约化平台上建设伊犁哈萨克自治州各级政府网站（包括伊犁哈萨克自治州政府门户网站以及各县（市、区）政府门户网站），并将信息资源导入自治区统一信息资源库平台，实现信息资源共享。以等保 2.0“一个中心三重防御”的保障理念，提出等保 2.0 安全保障体系方案，重点突出以安全管理中心建设，引入整体安全运营理念，整合推进安全保障技术体系及管理体系的完善， 构建优化以安全通信网络、安全区域边界、安全计算环境的多重防御架构，提供覆盖政务云整体的安全防护能力。

➢ 安全合规

政务云上运行的均为政府机关部门的业务应用，一部分业务是面向互联网公众，一部分业务是面向机关各部门之间，所以云安全方案设计首先应符合国家相关信息安全政策和标准，确保设计的政务云信息安全保障系统遵循国家法律且符合国家政策和国家标准。

➢ 能力异构

网络安全产品及能力需要遵循异构原则，一方面采用不同的安全能力，构建纵深防御体系，另一方面，采用不同厂家的安全设备或系统，保障信息系统的整体健壮性。为了保证所有安全设备的稳定性、可靠性，要求所有的安全设备品牌异构，品牌数不大于 4 家，不少于三家，并且所供产品品牌需满足行业市占率前三的要求;

➢ 功能全面

面向合规和业务需求，提供功能全面的安全产品，满足业务各阶段的安全需求。

➢ 技术先进

充分利用现有充分利用现有安全控制措施及最新技术，满足整个安全方案的交付，如 SDN、VXLAN、存储虚拟化、网络虚拟化技术等。所选的设备必须提供设备生产厂商授权，并提供原厂售后服务承诺函；要求所提供安全设备必须是厂商自主研发，有自己产品线及研发部门， 非 OEM 贴牌产品，要求提供设备生产厂商著作权和承诺函。一经发现弄虚作假行为直接不予中标，或做废标处理。同时相关单位及厂家列入合作黑名单;

➢ 安全服务化

在先进的技术背景下，能够与计算资源一样实现服务化交付，满足云计算整体服务化交付理念。

➢ 弹性扩展

云计算的特点是按需分配、资源弹性、自动化、重复模式，并以服务为中心的。因此，对于安全控制措施选择、部署、使用来讲必须满足上述特点，提供资源弹性、按需分配、自动化的安全服务，满足云计算平台的安全保障要求。

➢ 广泛开放

提供开放的安全生态，能够允许第三方安全产品快速融合到安全平台中，共同为云上租户打造一套完整的安全解决方案。

4、技术要求

（一）系统性能要求

1）软硬件要求

详见《伊犁哈萨克自治州信息便民政务服务门户平台建设项目规格技术参数》

2）性能技术要求

必须提升伊犁州信息便民政务服务门户平台的可靠性、安全性，同时能够提供统一管理、联动响应能力，降低运维复杂度。

（二）系统集成要求

基于伊犁州信息便民政务服务门户平台现状，针对现网中存在的网络隐患，提出合理的规划及具体优化建议，总体原则及要求如下:

1）总体原则

按照国家、自治区的标准规范，对伊犁州信息便民政务服务门户平台安全防护设备进行完善，并形成 “安全可视、统一管理、闭环

联动”的安全体系：

（1）对现有的网络边界安全设备进行完善，满足整体网络安全组网的要求，并能能够满足未来 3-5 年的信息化发展需求。

（2）采用服务器终端检测响应、联动防御的形式，实现对业务系统进行统一的运维管理，统一查杀，防病毒等操作。

（3）安全设备异构，实现信息便民政务服务门户平台的全网流量防护，对整体网络安全情况进行有效分析，判断是否进行了有效投资，体现 IT 价值。

2）交付能力要求

（1）集成单位需要了解《国务院办公厅关于加强政府网站信息内容建设的意见》等相关政策;

（2）集成单位具备大中型网络规划及维护能力;

（3）集成单位服务人员具备通信厂商专业认证能力，具备华为路由交换 HCNP、华三路由交换 H3CSE、思科路由交换 CCNP 等厂商认证能力;

（4）集成单位服务人员具备多厂商设备调试及维护能力，包含华为、华三、思科、锐捷、迪普、深信服等，设备安装需由原厂认证工程师安装调试。

3）服务时限要求

（1）要求提供 5×8 小时日常服务，7×24 小时应急响应。

（2）硬件故障问题，30 分钟响应，24 小时内完成故障判断并给出解决方案;

4）服务方式要求

（1）提供巡检服务，满足第（2）部分人员交付能力要求;

（2）每季度巡检：至少每季度提供一次设备巡检，并提交设备

巡检报告;

（3）每季度隐患分析，至少每季度提供一次隐患分析报告;

（4）中标产品厂家须提供具备中标产品服务认证工程师一名，三年免费的驻场服务。

二、项目需求及参数

1、设备需求

序号	名称	数量	单位	技术需求	异构要求（安全性考虑）
1	负载均衡	2	台	详见技术参数	要求与抗拒绝攻击、态势感知平台异构，不得同一品牌
2	抗拒绝服务攻击	2	台	详见技术参数	要求应用负载均衡、态势感知平台异构，不得同一品牌
3	边界防火墙	2	台	详见技术参数	要求与抗拒绝攻击、态势感知平台异构，不得同一品牌
4	入侵防御	2	台	详见技术参数	要求与态势感知、边界防火墙异构，不得同一品牌
5	VPN	1	台	详见技术参数	要求与入侵防御、网闸异构，不得同一品牌
6	区级纵向防火墙	2	台	详见技术参数	要求与抗拒绝攻击、态势感知平台异构，不得同一品牌
7	管理服务器	1	台	详见技术参数	
8	上网行为管理	1	台	详见技术参数	要求与抗拒绝攻击、态势感知平台异构，不得同一品牌
9	应用负载均衡	2	台	详见技术参数	要求与抗拒绝攻击、态势感知平台异构，不得同一品牌
10	日志审计	1	台	详见技术参数	要求与链路负载均衡、数据库审计异构，不得同一品牌
11	堡垒机	1	台	详见技术参数	要求与边界防火墙、漏洞扫描系统异构，不得同一品牌
12	漏洞扫描	1	台	详见技术参数	要求上网行为管理、态势感知平台异构，不得同一品牌
13	杀毒软件	1	套	详见技术参数	要求数据库审计、漏洞扫描系统异构，不得同一品牌
14	网管平台	1	套	详见技术参数	

15	态势感知	1	台	详见技术参数	要求与抗拒绝攻击、边界防火墙异构，不得同一品牌
16	数据库审计	1	台	详见技术参数	要求与杀毒软件、日志审计系统异构，不得同一品牌
17	全流量威胁分析探针	2	台	详见技术参数	要求与负载均衡、网闸异构，不得同一品牌
18	网闸	2	台	详见技术参数	要求与漏洞扫描系统、边界防火墙异构，不得同一品牌

2、产品规格详细技术参数

序号	设备名称	用　途	部署区域	数量	基本配置要求	异构要求（安全性考虑）
1	负载均衡	链路冗余	互联网接入域	2	4 层吞吐量（默认网口）：≥20G，四层并发连接数：≥8000000，4 层新建连接数 CPS：≥210000，7 层新建连接数 RPS：≥350000。 性能参数： 支持串接部署方式和旁路部署方式，支持三角传输模式。 提供针对多条出口线路的链路负载均衡功能，实现 inbound 和 outbound 流量的均衡调度，以及链路之间的冗余互备。 提供针对 L4/L7 内容交换的服务器负载均衡功能，可在单一设备上支持多个应用和服务器集群，可以根据多种算法和要求分配用户的请求。 提供针对多站点业务发布的全局负载均衡功能，通过智能 DNS 等机制实现内外网用户对多个数据中心的最优接入路径选择 ★单一设备可同时支持包括链路负载均衡、全局负载均衡和服务器负载均衡的功能。三种功能同时处于激活可使用状态，无需额外购买相应授权。（提供设备操作界面截图证明材料，并提供厂家授权免费开通功能声明并加盖公章） ★支持轮询、加权轮询、按主机加权轮询、加权最小连接、按主机加权最小连接、动态反馈、最快响应、加权最小流量、按主机加权最小流量、加权源 IP 哈希、带宽比例、哈希、首个可用、优先级等算法。（提供设备操作界面截图证明材料） 通过某种编程语言（如 lua）实现自定义的流量编排，对 IP、TCP、UDP、SSL、HTTP 和 HTTPS 等类型的流量进行分发、修改和统计等操作。（提供设备操作界面截图证明材料） ★支持静态 IP 和 PPPOE 两种线路接入方式。（提供设备操作界面截图证明材料） ★支持三明治架构，对防火墙、IPS、行为管理等网络设备进行流量负载均衡和故障切换，使以上网络设备获得 Active-Active 运行的能力。（提供实际的功能测试报告） 支持跨设备健康状态监视（透明监视），同时支持 IPv4 和 IPv6（提供设备操作界面截图证明材料） 支持基于五元组条件（源 IP 地址，源端口，目的 IP 地址，目的端口，传输层协议号）来进行出站访问的流量调度分发。 ★支持基于管理员自定义的时间计划来进行出站访问的流量调度分发。（提供设备操作界面截图证明材料）	要求与抗拒绝攻击、态势感知平台异构，不得同一品牌

					★内置完备的 IP 地址库，无需手动导入并支持自动全网更新，可查看并编辑各国家、国内各省份的 IP 地址段和国内各大运营商 IP 地址段，并可灵活匹配 IP 地址库进行流量调度分发，实现链路负载功能（提供设备操作界面截图证明材料） ★支持基于应用协议的智能选路，能对网银、游戏、视频等流量进行调度（需提供设备功能界面截图证明） ★支持基于域名的流量调度，针对特定网站选择指定的链路转发。（提供设备操作界面截图证明材料） 支持 DNS 透明代理功能，可基于负载均衡算法代理内网用户进行 DNS 请求转发，避免单运营商 DNS 解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率。（提供设备操作界面截图证明材料） 支持 DNS 内网记录，包含 A、AAAA、CNAME、MX 和 TXT 等类型，可识别内网用户并对其 DNS 请求直接返回相应结果； 支持智能 DNS 解析功能，实现外网用户访问内网业务系统的最优路径选择。 链路健康检查与服务器健康检查联动，入站负载跟服务器负载结合的时候，如果后端服务器全挂，则入站负载时也认为该虚拟 IP（此时要求入站负载的虚拟 IP 与虚拟服务发布的 IP 组相同）也离线，从而达到联动效果。 支持基于链路负荷情况的繁忙保护机制，能根据链路的上行/下行带宽占用率情况执行对出站/入站流量的高级调度策略。（提供设备操作界面截图证明材料） ★SLB 能够通过健康检查来获取后端服务器状态，同时将服务可用性、设备 CPU、新建并发吞吐等数据上报 GSLB，设备之间的联动使得 GSLB 能根据链路和服务器两者的综合状态实现智能切换，为用户选择最优的数据中心和服务器分配方式。 ★支持跨数据中心集群和跨数据中心会话保持 支持多种链路检测方法，能够通过 PING、TCP、HTTP 等方式监控链路的连通性，当某一条链路故障时，可将访问流量切换到其它链路，保障用户业务的持久通畅。 ★支持链路负载投屏展示，能够分别基于链路监测、应用选路和 ISP 流量进行投屏展示分析。链路监测展示链路的健康状态、上下行带宽、总带宽、新建连接数、并发连接数和吞吐量；应用选路展示基于应用分类选择相应链路的示意图；ISP 展示基于运营商分类选择链路的示意图。（提供设备操作界面截图证明材料） 支持源 IP、Cookie（插入/被动/改写）、HTTP-Header、SSL Session ID 等多种会话保持机制，支持跨虚拟服务的会话保持。（提供设备操作界面截图证明材料） ★支持 cookie 加密，提升 cookie 安全性。（提供设备操作界面截图证明材料） ★支持防秒杀功能，即能够以 JSESSIONID 为标识限制用户访问速度，且不影响该用户访问非防护页面（提供设备操作界面截图证明材料） 支持大数据输出功能，输出必须包括客户端 IP、x-forwarded-For IP、访问时间、访问 IP、访问 URL、响应时间和资源大小。	

					（提供设备操作界面截图证明材料） 支持优先级算法下最少可用节点保障，优先级高的节点故障时会自动进行选举，保证优先级高节点的可用性。 支持常见的主动式健康检查功能，提供基于 SNMP、ICMP、TCP/UDP、FTP、HTTP、DNS、RADIUS，ORACLE/MSSQL/MYSQL 数据库等多种类型的探测判断机制，支持对 HTTPS 服务进行内容健康检查。 ★支持用户自定义方式的健康检查，支持多种编程语言（如 Python、Java 等），用户可根据节点运行的实际业务流程来编写代码，检查业务处理逻辑是否正常。（提供设备操作界面截图证明材料） ★支持外部监视器探测方式通过编写脚本执行命令使得节点智能恢复，当节点出现故障时，负载均衡能自动重启服务器上的相关进程或重启服务器，使其恢复正常状态并继续提供服务；如无法使其恢复正常，则将其从节点池中移除，保证业务正常访问。（提供设备操作界面截图证明材料） 支持银联 8583 等长连接负载，支持 8583 单工和双工的区分，对于非 HTTP 协议的长连接应用，可通过分析议特征来识别消息的开始和截止，以消息为对象进行七层负载均衡，而非传统基于连接的四层负载均衡。（提供设备操作界面截图证明材料）6.6 定制和 6.6R1 定制、705 定制、708 定制支持；708R3 版本默认支持 ★支持被动式健康检查，可根据对业务流量的观测采样，辅助判断应用服务器健康状况；对常规 HTTP 应用可配置基于反映 URL 失效的 HTTP 响应状态码的观测判断机制，对于复杂应用可配置基于 RST 关闭连接和零窗口等异常 TCP 传输行为的观测判断机制。（提供设备操作界面截图证明材料） ★支持面向服务器健康度的弹性调控机制，可通过监控业务流中的 TCP 传输异常来衡量服务器节点的有效性，尝试对性能不足的服务器临时开启过载保护，动态调节服务器的负载。（提供设备操作界面截图证明材料） ★支持主动探测方式与被动观测方式结合使用的服务器健康检查手段，以便适应各种复杂应用交互流程，保障业务系统的高可用性。（提供设备操作界面截图证明材料） 支持配置每台的服务器最大连接限制和新建连接限制，以及单个特定用户或者一个用户组中所有用户访问指定应用服务的并发连接总数限制，避免应用系统的服务器过载。 ★支持命令行配置，支持 Tab 键补全操作，支持界面全部模块通过命令行的模式配置，支持命令批量操作，支持配置导入导出命令行操作（提供设备操作界面截图证明材料） ★节点支持域名和 IP 两种形式，支持自定义 DNS 查询间隔。（提供设备操作界面截图证明材料） ★支持后端服务不可用时主动关闭连接，保证客户端访问的连续性（提供设备操作界面截图证明材料） ★支持 Loose Initiation 和 Loose Close 功能选项（支持非 SYN 建立会话的选择和任意 FIN 释放会话选择）（提供设备操作界面截图证明材料） ★对于超过服务器的连接数上限或者请求数上限的新建连接缓存起来放入队列中，后续分批逐步发送给服务器，而不是直接丢弃数据包（提供设备操作界面截图证明材料） ★服务器负载状态支持投屏展示，能够显示设备的电源状态、风扇转速、磁盘温度、CPU 温度、CPU 和内存占用	

					率、新建连接数、并发连接数、吞吐情况、SSL 新建和 SSL 吞吐数据、压缩优化和缓存优化数据；业务的健康状态、新建连接数、并发连接数、上下行流量、每秒请求数；节点池的调度算法、健康状态、新建连接数、并发连接数、上下行流量；（提供设备操作界面截图证明材料）； ★支持二个或四个以上的多重引导（提供设备操作界面截图证明材料）； IPv6 支持双栈模式，支持 NAT46、NAT64、NAT66、FTP ALG、DNS64 等协议转换 ★IPv6 改造方案能够解决天窗问题，支持一条策略匹配多个外链网站，同时外链和网站子链发生修改时支持自动识别并做主动修改，不允许通过人工解析配置的方式解决天窗问题 提供 IPv6 产品检测报告； 支持通过 syslog 的方式实现 IPv4/IPv6 协议转换日志功能，累积存储和查询 3 个月内数据；提供 IPv6/IPv4 协议翻译和互通的日志信息，包括源/目的 IP 地址和端口，被访问的 URL 等信息，并在需要的情况下，回溯查询用户信息 支持 HTTP 缓存功能，利用内存 Cache 缓存用户频繁访问的 web 内容，降低后台服务器的负载压力,提升用户访问的响应速度。 支持 TCP 连接复用功能，利用 HTTP 连接池机制，将来自客户端的多个请求合并成一个连接发送到服务器，减少服务器端的工作负荷，并提升业务效率。 支持 SSL 卸载功能，卸除服务器端的密集型运算任务，释放服务器计算资源，并提升 SSL 业务的处理速度； 支持 SSL 加密功能，可将普通流量加密以适配需要通过 SSL/TLS 协议才能访问的服务器； ★支持非对称式部署的 TCP 协议优化技术，提升远端用户访问应用服务的速度。无需在用户终端或应用服务器上安装任何插件和软件，不受操作系统类型、浏览器版本等兼容性因素限制，并且用户首次访问应用服务即可产生加速效果。(提供第三方评测报告,证明所投产品厂商可提供此类技术) ★支持图片优化技术，通过对图片格式的转换，减少传输流量，提升 web 页面加载速度。无需改动服务器端的图片源文件，可根据浏览器种类自动识别转换类型，将图片转换为对应支持的 WebP 或 JPEG 格式，优化加速效果。（提供设备操作界面截图证明材料） ★免费开通 HTTP 压缩、HTTP 缓存、TCP 连接复用、SSL 卸载等功能，无需额外购买相应授权。（提供厂家授权免费开通声明并加盖公章）。支持双机热备部署方式，可自动同步配置并提供连接会话的镜像功能，实现无缝故	

					障切换； 支持基于链路流量进行有效性判断，能够在预设时间内进行主动探测。 支持高可用集群 N+M 部署方式，单集群支持 16 台设备，可自动同步配置并提供连接会话的镜像功能，实现无缝故障切换； ★提供基于 VM 和容器两种方式的硬件一虚多。一台物理设备可从逻辑上划分为多台虚拟设备，各虚拟设备拥有独立的计算资源和网络资源，各虚拟设备可运行不同软件版本，虚拟设备重启或升级时不影响其他虚拟设备的正常运行，虚拟设备宕机可自动重启。 支持全中文管理界面和 HTTPS 方式登录、用户角色管理、多级授权管理。 支持设置管理地址白名单列表，远程维护支持设置是否允许 WAN/LAN ★IPv6 支持双栈模式，支持 NAT46、NAT64、NAT66 等协议转换（提供设备操作界面截图证明材料） ★内置智能告警系统，支持 E-mail、SNMP Trap 两种告警方式，管理员可基于业务安全所关注方面来选择告警触发事件与对应的告警方式，当业务网络环境中发生问题时（如服务器宕机、网络攻击、链路中断等故障场景），即会自动向管理员发送告警信息。（提供设备操作界面截图证明材料） ★设备内置数据中心，支持自动订阅和手动生成两种方式输出 PDF 格式的报表。报表可对链路和服务器的稳定性进行统计，可查询服务器的异常状态信息，并提供对故障原因的分析。 支持全局数据中心智能 DNS 统计，包括访问次数统计及按照 Local DNS 来源统计；支持统计虚拟服务和真实服务器的流量、访问次数、并发连接数。（提供设备操作界面截图证明材料） 支持标准的 RESTful 等形式的 API 接口，可提供 Python 和 Java 的 SDK 工具，可实现与第三方应用平台的集成与二次开发。（提供设备操作界面截图证明材料） 所投产品具备《计算机软件著作权登记证书》(提供复印件)	
2	抗拒绝服务攻击	DDoS 攻击防护	政务云业务域	2	★攻击流量处理能力≥10Gbps，攻击包处理能力≥148 万 pps； ★设备接口要求：不少于 2*USB 接口，不少于 1*RJ45 串口，不少于 2*GE 管理口，设备提供不少于 4 个万兆 SFP+，提供不少于 8 个千兆 SFP，不少于 4 个 GE 工作电口；设备总共提供不少于 4 个链路扩展板卡插槽（支持千兆和万兆网卡）。每个接口扩展槽位支持 4GE/4SFP/8GE/8SFP/2SFP+；提供 3 年原厂质保服务；64K 小包清洗能力不小于 296 万 pps；	要求应用负载均衡、态势感知平台异构，不得同一

					★提供无限 IP 防护能力；无限并发数限制； ★本次网络需要形成 HA 部署，实现会话同步、策略同步、主备切换等功能，满足本次项目双链路热备的安全防护需求； 1）支持对欺骗与非欺骗的 TCP、UDP、ICMP、(M)Stream Flood 及混合类型攻击的防护；设备具备针对 UDP53、TCP53 及 3DNS 提供专用的 DNS Query Flood 防护手段； 2）设备具备针对缓存 DNS 服务器及授权 DNS 服务器专用的 DNS 防护手段，至少 4 种；（提供厂商盖章的配置界面截图证明） 3）设备具备针对 HTTP Get Flood 攻击具备专门的防护手段；设备具备针对 HTTP Get Flood 攻击具备不少于 9 种专有防护手段，能够对 HTTP 进行解码。（提供厂商盖章的配置界面截图证明）； 4）设备具备对不同类型的 url 请求合法性进行验证，实行不同的防护策略。 5）产品能够有效防护 CC 攻击，并提供 etag、http cookies、url 验证、ascii 图片验证、bmp 图片验证、传奇游戏验证、FCS 检查和模式匹配检查防护算法以抵御不同程度的攻击，（提供厂商盖章的配置界面截图证明）； 6）支持和第三方（GENIE/Arbor 等）的 NETFLOW 异常流量检测设备联动，（提供厂商盖章的配置界面截图证明） 7）提供分组过滤功能，支持白名单、黑名单、ACL、高级模式匹配、URL 访问控制规则等多种分组过滤方式; 8）支持与专业 WEB 应用防护设备进行联动，为 WEB 应用提供细粒度拒绝服务攻击防护功能（提供功能界面截图并加盖公章并加盖公章）； 9）具备云平台，能够通过云服务 7X24 小时对设备进行远程维护、攻击事件响应及策略调整，并进行数据关联分析（提供功能界面截图并加盖公章和测试账号）； 10）具备多级部署能力，支持与上级异常流量清洗中心联动（提供功能界面截图并加盖公章）。 11）可扩展 DDoS 攻击云监护服务，厂商安全团队通过“云安全”平台 7×24 小时监测设备的状态和日志，一旦发现可疑事件并人工验证后，30 分钟内通过电话\短信\邮件等方式通知用户，协助用户优化防护策略，对 DDoS 攻击流量进行精确清洗，（提供云监控中心照片和监控平台界面图片），提供 DDoS 云监护服务的服务等级协议（SLA）说明书，详细说明服务形式、服务内容、测量标准、报告形式等。 12）支持使用 IP 信誉库对流量进行防护，并支持 IP 信誉查询，信誉库更新周期≤1 天 ，（提供厂商盖章的配置界面截图证明）。 13）提供界面手动及自动抓包功能，抓包参数定义范围至少包含如下几项：接口、协议、抓包数量、源 IP、目标 IP、源或目标 IP、最大包长、流量方向。 14）支持以中文图表形式输出流量报表、安全报表、综合报表；支持 HTML、RTF、PDF 等格式的报表生成，并支持通过 SYSLOG、SNMP、SFTP、SSH、邮件等多种方式输出；支持日报、周报、月报和年报，并且支持对设备、IP 群组、单台主机形式输出以上报表；提供完善的日志管理功能，包括日查询、删除、备份、生成报表等操，而且	品牌

					要支持自定义报表、自动生成报表等功能 15）管理界面友好、易用性强，可支持集中管理（提供功能界面截图并加盖公章）、本地管理、Https 远程管理等多种管理方式，并能实时显示攻击事件、流量、系统运行状况等信息，可扩展支持云平台管理； 16）支持与态势感知平台进行对接，针对恶意攻击 IP 实现一键封堵功能（提供产品功能截图并加盖公章）。 具备以下资质证书并加盖公章： 1.公安部颁发的《计算机信息系统安全专用产品销售许可证》 2.国家版权局颁发的《计算机软件著作权登记证》 以上功能需进行逐项测试，提供投标型号测试机并测试，满足所有功能方可签署合同，否则按照虚假应标处理。	
3	边界防火墙	区域边界隔离	互联网接入域	2	网络层吞吐量：≥20G，应用层吞吐量：≥8G，防病毒吞吐量：≥1.5G，IPS 吞吐量：≥1.3G，全威胁吞吐量：≥1G，并发连接数：≥220 万，HTTP 新建连接数：≥15 万，IPSec 最大隧道数：1000，IPSec VPN 吞吐量：≥400M。 硬件参数：规格：1U，内存大小：8G，硬盘容量：128G minisata SSD，电源：冗余电源，接口：不少于 6 千兆电口，不少于 2 万兆光口 SFP+。 产品采用多核并行处理架构，提供中国信息安全测评中心、公安部信息安全产品检测中心、中国软件评测中心、国家版权局之中任意一家机构出具的关于“多核并行安全操作系统”的证书或测试报告。 支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式。 支持静态路由，ECMP 等价路由。支持 RIPv1/v2，OSPFv2/v3，BGP 等动态路由协议。 支持基于 IP 地址、端口、地域、协议、应用等维度配置策略路由策略，支持多种负载均衡算法，包括加权、带宽比例、轮询、线路排序等。（需提供产品功能截图证明） ★支持多链路出站负载，支持基于源/目的 IP、源/目的端口、协议、ISP、应用类型以及国家地域来进行选路的策略路由选路功能。（提供产品界面截图） 访问控制规则支持基于源 / 目的 IP，源端口，源 / 目的区域，用户（组），应用/服务类型，时间组的细化控制方式;支持异常流量展示并支持查看异常流量过程和下载异常流量数据包；（需提供相关功能截图证明） ★支持识别管控的应用识别规则总数超过 9700 条，并支持自定义应用规则；（需提供相关功能截图证明） ★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。 支持 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing 攻击防护，支持 SYN Flood、IPv4 和 IPv6 ICMP Flood、UDP Flood、DNS Flood、ARP Flood 攻击防护，支持 IP 地址扫描，端口扫描防护，支持 ARP 欺骗防护功能、支持 IP 协议异常报文检测和 TCP 协议异常报文检测。 ★设备具备独立的入侵防护漏洞规则特征库，特征总数在 7000 条以上。 （提供产品界面截图） 支持对服务器和客户端的漏洞攻击防护。	要求与抗拒绝攻击、态势感知平台异构，不得同一品牌

					支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telnet、Weblogic、VNC）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能。 具备防护常见网络协议（SSH、FTP、RDP、VNC、Netbios）和数据库（MySQL、Oracle、MSSQL）的弱密码扫描功能。 ★可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则。（提供产品界面截图） ★设备具备独立的僵尸网络与病毒防护库，防护类型包括木马远控、恶意脚本、勒索病毒、僵尸网络、挖矿病毒等，特征总数在105万条以上，支持自定义僵尸网络规则库；（需提供相关功能截图证明） 支持DNS代理场景下重定向恶意域名。 ★支持蜜罐功能，定位内网感染僵尸网络病毒的真实主机IP地址；（需提供相关功能截图证明） 支持具备网络连接、终端进程、威胁情报举证识别同一失陷主机的能力。且通过流量中识别的恶意地址定位到具体的发起终端、文件，隔离恶意文件和记录处置情况； ★支持针对失陷主机推送杀毒通知和提供处置工具，并支持自定杀毒通知显示时间；（需提供相关功能截图证明） ★支持基于勒索病毒的攻击链提供勒索病毒防护配置向导，包含防护对象、勒索病毒常用端口、漏洞、弱口令的自定义定时识别及自动生成包含WEB应用防护、漏洞防护、内容安全、僵尸网络检测、慢速爆破防御等勒索病毒防护策略；（需提供相关功能截图证明） ★产品内置Web应用攻击检测引擎，支持文件包含攻击、抵御注入式攻击（包含SQL注入、系统命令注入）、信息泄露攻击、跨站脚本（XSS）、网站扫描、WEBSHELL后门攻击、跨站请求伪造、目录遍历攻击、WEB整站系统漏洞等应用层攻击行为，支持超过3000种Web服务器漏洞特征规则。（需提供产品功能截图证明） ★支持对HTTP异常请求协议检测和防护攻击，检测内容包含HTTP请求信息的方法及参数长度等。（需提供产品功能截图证明） 支持基于源IP、Referer、URL等多种组合条件对CC攻击进行检测，检测指标为检测时间和触发阀值。 ★具备识别与阻断外部扫描器发起的服务器恶意扫描行为，可对扫描器地址进行自定义封堵。（需提供产品功能截图证明） ★支持服务漏洞检测功能，基于服务器请求和响应内容识别服务器存在的系统安全漏洞和应用安全漏洞。（需提供产品功能截图证明） 支持内容敏感数据防泄露功能，对传输的文件和内容进行检测,支持对银行卡号、手机号码等类型数据防护。 ★支持网站防篡改功能，可防止攻击者非授权修改网站目录文件，提供不少于10套网页防篡改软件。（需提供产品功能截图证明） ★支持网页恶意链接检测功能，有效识别网页盗链/黑链的行为，避免用户网页资源被滥用。（需提供产品功能	

					截图证明） 支持基于业务安全和用户安全维度的风险展示； ★支持 Web 服务器自动侦测功能，根据 Web 服务器在线状态、端口使用状态、Web 服务器之间的互访关系生成业务资产列表，同时展示内网资产访问的风险等级。（需提供产品功能截图证明） 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） ★支持安全运营中心功能，可以对全网所有的服务器和主机的威胁进行全面评估，管理员通过一键便可完成对服务器和主机的资产更新识别、脆弱性评估、策略动作的合理化监测、当前服务器和用户的保护状态、当前的服务器和主机的风险状态及需要管理员待办的紧急事项等，可以自动化直观的展示最终的风险；（需提供相关功能截图证明） ★防火墙需具备未知威胁检测能力（提供国家版权局颁发的未知威胁检测软件著作权登记证书） 支持与防病毒系统平台的联动，实现管理员在防火墙平台通过终防病毒平台对其下属终端下发快速查杀任务、并根据查杀结果并进行处置；	
4	入侵防御	外部攻击防御	互联网接入域	2	★提供交流冗余电源模块，2*USB 接口，1 个 RJ45 串口，1 个 RJ45 管理口，提供不少于 4 个万兆 SFP+，不少于 4 个千兆 SFP，提供不少于 4 个千兆电口，设备提供不少于 2 个接口扩展槽位。 ★本次网络入侵防护系统形成 HA 部署，实现会话同步、策略同步、主备切换等功能，满足本次项目双链路热备的安全防护需求； 1）系统支持监听（Monitor）、直通（Direct）和管理（Mgt）三种安全区模式，能够快速部署在各种网络环境中。 2）支持独立式多路 IPS 工作模式，各路 IPS 相互独立，彼此之间没有数据交换，可单独配置策略。支持 IPv6/IPv4 双协议栈功能，能同时辨识 IPv4 和 IPv6 通讯流量。支持多种隧道模式，确保 IPv6 过渡时代的网络通畅。 3）支持 IPv6 环境下攻击检测技术和基于 IPv6 地址格式的安全控制策略，为 IPv6 环境提供入侵防护。支持 VLAN 802.1Q、BGP、MPLS、QinQ、PPPOE 等特殊封装协议，能够适应多种不同的网络环境。 1）系统支持基于信誉的僵尸网络防护能力，支持持续升级的信誉库，IPS 通过信誉库内的恶意网站 IP、C&C 服务器地址的信誉值执行相应的防护动作（提供功能界面截图并加盖公章）； 2）系统具备融合模式匹配、协议分析、异常检测、会话关联分析，以及抗 IDS/IPS 逃逸等多种技术，准确识别各种黑客入侵，为用户提供 2¯7 层深度入侵防御，提供对网络病毒、蠕虫、间谍软件、木马后门、刺探扫描、暴力破解、僵尸网络等恶意流量的检测和阻断，提供自定义攻击功能和零日攻击防护功能； 3）系统应具备攻击快照功能，详细记录触发告警的数据特征，以便做进一步的事件分析（提供功能界面截图并	

					加盖公章）。 4）获得 CVE-Compatible 兼容性认证； 5）在透明模式下防止 SYN Flood 攻击（提供功能界面截图并加盖公章）； 6）支持 IP 碎片重组、TCP 流重组、流量状态追踪，智能协议分析技术； 7）提供对网络病毒、蠕虫、间谍软件、木马后门、刺探扫描、暴力破解、SQL 注入、跨站脚本攻击、僵尸网络等恶意流量的检测和阻断； 8）提供入侵行为和应用软件特征的自定义接口，可根据用户需求定制对其它流量的检测和阻断规则。支持白环境功能。 9）提供服务器异常告警功能，可以自学习服务器正常工作行为，并以此为基线检测处服务器非法外联行为（提供功能界面截图并加盖公章）。 10）提供关键文件保护功能，能够识别、阻断通过自身的关键文件，以防止非法外传行为（提供功能界面截图并加盖公章）。 11）支持用户以安全区、IP 地址（网段）、时间、用户、应用多维度的对流量进行管理和控制，包括限制应用上下行最大带宽、保证应用上下行最小带宽、保证带宽下的优先级排序以及每 IP 的进行应用流量控制， 12）能够提供网络数据传输速率控制设备及方法的证明（提供功能界面截图并加盖公章）； 13）支持攻击规则模板，可根据客户业务生成的固定场景下的攻击规则模板（提供功能界面截图并加盖公章）； 14）提供丰富的响应方式，包括：丢弃数据包、阻断会话、邮件报警、短信报警、控制台显示、声音报警、日志数据库记录、写入 XML 文件，运行用户自定义命令等； 15）提供基于告警设备、时间、IP 地址、事件类型、用户身份等条件的日志检索功能； 16）具备日志备份、清除和恢复功能， 17）具备递归查询功能； 18）支持日志缓存，日志归并功能； 19）支持自定义报表模板，提供定时自动发送报表功能， 20）支持在指定的时间内将生成的报表以 html、word、excel 等通用格式通过 FTP 或邮件发送给指定的管理员； 21）提供地址薄功能和过滤器模板功能 22）提供多种方式的管理界面，包括 HTTPS、CONSOLE、SSH、TELNET 等； 23）支持管理平台集中管理功能，可同时监控所有入侵保护系统和其他安全设备的运行状态，并支持对所有设备进行统一安全策略配置及统一版本升级； 24）支持分级部署和主辅管理； 25）提供实时在线升级、自动在线升级、离线升级、集中升级。	

					26）产品支持与态势感知平台进行对接（提供功能界面截图并加盖公章） 1）公安部销售许可证； 2）计算机软件著作权登记证； 3）CVE 兼容性证书；	
5	VPN	拨号用户接入	互联网接入域	1	包含 ≥200 用户授权，商密设备；最大理论加密流量（Mbps）：≥690；最大理论并发用户数：≥12000 IPSec 加密最大流量（Mbps）：≥450，设备整机理论最大吞吐量：≥2Gbps，设备整机理论最大并发会话数：≥250w 性能参数：最大理论加密流量（Mbps）≥350，最大理论并发用户数≥8000，IPSec 加密最大流量（Mbps）≥200，设备整机理论最大吞吐量≥1.2Gbps，设备整机理论最大并发会话数≥150W。内存大小≥8G，硬盘容量≥64GB SSD，电源：冗余电源，接口≥6 千兆电口+4 千兆光口 SFP。 支持 IPv6/IPv4 协议下的网关模式、单臂模式、双机模式、集群模式的部署。 专业 VPN 设备，采用标准 SSL、TLS 协议，同时支持 IPSec VPN、SSLVPN 两种 VPN，非插卡或防火墙带 VPN 模块设备。 ★支持 PC 终端使用包括 Windows10、Windows8、Windows7、Windows Vista、Windows xp、Mac OS、Linux 等主流操作系统的客户端来登录 SSLVPN 系统，并完整支持该操作系统下的各种 IP 层以上的 B/S 和 C/S 应用。（提供产品界面截图） ★产品应支持的密码算法包括：AES、DES、3DES、DH、RSA、RC4、MD5、SHA1、SM1、SM2、SM3、SM4（提供产品界面截图） ★可支持虚拟门户功能，在一台设备上配置不同的访问域名、IP 地址，以及不同的使用界面，实现一台设备为多个不同用户群体服务的的使用效果。（提供产品界面截图） 支持单点登录功能（SSO），支持移动用户登录 VPN 后再登录内部 B/S、C/S 应用系统时不需要二次重复认证。支持针对 B/S 单点登录用户名密码加密传输，保证安全。支持针对不同的访问资源设定不同的 SSO 用户名和密码，支持用户自行修改 SSO 账号。 ★产品应提供环境检测、自动修复工具，支持对 Windows 的环境兼容性一键检测能力，以及对检测结果进行一键修复的能力，避免由于用户操作系统环境存在问题影响 SSL VPN 的使用，减轻运维工作。（提供产品界面截图） ★产品必须支持防中间人攻击，产品可在用户登录 SSLVPN 时智能判断存在中间人攻击行为，断开被攻击的连接，并可提示异常现象。（可提供证明材料） 支持用户终端登录前、登陆后的安全性检测，检测范围包括：用户接入 IP、接入时间、接入线路 IP、进程、文件、注册表、操作系统、使用终端，可以检测出客户端是否安装指定的防火墙或杀毒软件。 支持客户端注销后自动清除所有缓存、Cookies、浏览器历史记录、保存的表单信息，实现零痕迹访问	要求与入侵防御、网闸异构，不得同一品牌

					支持 VPN 专线功能，可配置用户在接入 SSL VPN 的同时，断开与 Internet 其他连接 ★产品应提供 HTTPS 驱动病毒查杀工具,支持对 Windows 环境下的针对 HTTPS 拦截监听的驱动病毒进行扫描查杀，避免因为 HTTPS 驱动病毒导致无法正常接入和使用 SSL VPN。 支持设备自身的抗攻击防护，支持防 Host 头部攻击设置，用于防止 Host 头部攻击, 设备只允许通过符合设置规则的地址进行访问；支持防 SWEET32 攻击设置，用于防止 SWEET32 攻击。（提供配置截图） 产品应具有用户/用户组细粒度的权限分配功能：可以针对被访问资源的 IP 地址、端口、提供的服务、URL 地址等进行权限控制；针对同一 B/S 资源，可对不同用户做到细致到 URL 级别的授权。 ★支持主从认证账号绑定，必须实现 SSL VPN 账号与应用系统账号的唯一绑定，VPN 资源中的系统只能以指定账号登陆，加强身份认证，防止登录 SSL VPN 后冒名登录应用系统 支持关键文件保护功能，可针对特定应用关键文件进行锁定，防止用户进行篡改进行越权 针对服务器地址保护方面，可支持 SSLVPN 资源列表界面上的用户授权资源隐藏；针对 B/S 应用，可进行 URL 地址伪装，防止服务器真实 IP 地址泄露 产品必须支持 Local DB 、USB KEY、短信认证、硬件特征码、动态令牌、数字证书认证、LDAP、RADIUS、等认证方式。可针对用户/用户组设置认证方式的与、或组合，可进行用户名/密码、LDAP、USB KEY、硬件特征码、短信认证或动态令牌的五因素捆绑认证 设备内部必须支持自建 CA 中心，便于数字证书认证平台搭建； 支持与基于 PKI 体系的第三方 CA 进行结合认证 ，可根据 CA 某字段将通过 CA 认证的用户自动映射到指定用户组，方便进行权限授权配置；支持 CRL 证书撤销列表。 投标产品具有国家密码管理局颁发的《商用密码产品型号证书》，且型号与所投产品一致	
6	区级纵向防火墙	区域边界隔离	城域网接入域	2	网络层吞吐量：≥12Gbps，应用层吞吐量：≥750Mbps，并发连接数：≥2000000，新建连接数：≥80000，IPSec VPN 最大隧道数：1000，IPSec VPN 吞吐量：≥350Mbps。硬件参数：规格：1U，内存大小：≥4G，硬盘容量：≥64G minisata；SSD，接口：不少于 6 千兆电口，不少于 2 千兆光口 SFP，不少于 2 个万兆。 支持链路探测； 支持 ARP 代理和静态 ARP 绑定； 支持配置 DNS 及 DNS 代理，支持 DHCP 中继、DHCP 服务器； 支持 SNMP v1、v2、v3 网络管理协议，支持 SNMP Trap 配置； 支持 IPv4/v6 NAT 地址转换，支持多个内部地址映射到同一个公网地址、多个内部地址映射到多个公网地址、内部地址到公网地址一一映射、源地址和目的地址同时转换等多种方式； 支持外部网络主机访问内部服务器、支持 DNS 映射功能； 支持 IPv4/IPv6 双栈工作模式；	要求与抗拒绝攻击、态势感知平台异构，不得同一品牌

					支持 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing 攻击防护，支持 SYN Flood、IPv4/v6 ICMP Flood、UDP Flood、DNS Flood、ARP Flood 攻击防护； 支持 IP 地址扫描、端口扫描防护、ARP 欺骗防护功能、IP 协议异常报文检测和 TCP 协议异常报文检测； 支持 IPSec VPN 远程接入； 支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制，支持基于时间、地域、认证用户、子接口和 VLAN 等因素实现对象的流量控制； 访问控制规则支持从 IP、端口、服务、应用、时间维度进行细粒度的一体化设置与管控； ★访问控制规则支持失效规则识别，如规则内容存在冲突、规则生效时间已过期、规则超长时间未有匹配等情况；（需提供相关功能截图证明） ★访问控制规则支持数据模拟匹配，根据输入源的五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试；（需提供相关功能截图证明） 支持 URL 过滤和文件过滤功能，URL 过滤支持 GET，POST 请求过滤和 HTTPS 网站过滤，文件过滤支持文件上传和下载方式过滤； 支持针对 SMTP、POP3、IMAP 邮件协议的内容检测，如邮件附件病毒检测、邮件内容恶意链接检测，邮件异常账号检测等，支持根据邮件附件类型进行文件过滤；支持针对 HTTP、FTP 协议内容检测与病毒查杀； ★支持针对服务器的各种漏洞攻击防护，包括 Media 漏洞攻击、Network Device、Telnet 漏洞攻击、DNS 漏洞攻击、Tftp 漏洞攻击、FTP 漏洞攻击、Web 漏洞攻击、Mail 漏洞攻击、Database 漏洞、Scan 漏洞攻击、Shellcode 漏洞攻击、System 漏洞攻击；（需提供相关功能截图证明） ★支持针对客户端的各种漏洞攻击防护，包括 Application 漏洞攻击、File 漏洞攻击、Web Browse、Web Activex、Scan 漏洞攻击、Shellcode 漏洞攻击、System 漏洞攻击；（需提供相关功能截图证明） 支持后门软件、间谍软件、木马软件、蠕虫等恶意软件防护； 支持对常见应用服务（FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telne、Weblogic、VNC）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能； 支持 A/A，A/S 模式部署； 支持配置同步，会话同步和用户状态同步； 支持自定义维度查询流量统计、应用统计、内容安全、漏洞攻击防护、DOS 攻击、内容安全、应用控制、本机安全事件、用户登录/注销、系统操作等多种安全日志； 支持网页、PDF、EXCEL 等格式导出查询日志； 支持以安全策略模板方式快速部署安全策略，安全策略模板支持默认模板和自定义模板等多种格式，支持安全防护策略一体化配置，一条策略可同时对应用和用户进行安全防护设置，减少策略配置数目，提高管理易用性；	

					支持配置向导功能，快速实现设备初始运维部署； 支持内置规则库的手动/自动更新； 支持邮件、短信等多种告警方式； 支持安全设备集中管理，包括配置策略统一下发，规则库统一更新等功能； ★防火墙需具备未知威胁检测能力（提供国家版权局颁发的未知威胁检测软件著作权登记证书）	
7	管理服务器	配置、管理信息设备	安全管理域	1	CPU:2 颗 2.2GHz/12 核;内存：16GB*4;硬盘：480GB；SSD*2,1.2TB 10K HDD*4;RAID 卡：2 端口 RAID 卡(2G 缓存,含掉电保护)；网口：≥4*GE；电源：550W*2;导轨；面板；风扇；需提供符合管理平台的正版操作系统	
8	上网行为管理	用户行为审计，准入	委办局接入域	1	网络层吞吐量：≥8Gb，应用层吞吐量：≥1.1Gb，带宽性能：≥750Mb，IPSEC VPN 加密性能：≥150Mb，支持用户数：≥5000，包转发率：≥108Kpps，每秒新建连接数：≥ 12000，最大并发连接数：≥500000。 硬件参数：内存大小≥8G，硬盘容量≥1T SATA，接口≥6 千兆电口+4 万兆光口 SFP+。 必须支持两台及两台以上设备同时做主机的部署模式；旁路支持主主、主备模式部署。 ★支持部署在 IPv6 环境中，设备接口及部署模式均支持 ipv6 配置； 所有核心功能（上网认证、应用控制、流量控制、内容审计、日志报表等）都支持 IPv6；（提供产品界面截图） 必须具有 IPSec VPN 远程加密访问和连接的模块，并能提供 IPSec VPN 客户端授权远程接入访问。 支持首页分析显示接入用户人数、终端类型、认证方式。带宽质量分析、实时流量排名。泄密风险、违规访问、共享上网等行为风险情况。 针对内网用户的 web 访问质量进行检测，对整体网络提供清晰的整体网络质量评级；支持以列表形式展示访问质量差的用户名单；支持对单用户进行定向 web 访问质量检测（提供产品界面截图） 支持多种认证方式，包括本地用户名密码、第三方服务器、短信认证、二维码认证等 支持通过 OAuth 认证协议对接，支持阿里钉钉，口袋助理，企业微信第三方账号授权认证； 支持二维码认证，担保人扫描访客的二维码后对其网络访问授权；支持访客填写信息、担保人填写信息、免填写信息三种模式（提供产品界面截图） 可设置用户密码不能等于用户名。新密码不能与旧密码相同。可设置密码最小长度。可设置密码必须包括数字或字母或特殊字符。（提供产品界面截图）	要求与抗拒绝攻击、态势感知平台异构，不得同一品牌

					支持识别终端操作系统版本、系统补丁安装情况；支持识别终端硬盘指定目录下的文件情况；支持识别进程信息和注册表信息，防止间谍软件运行 支持终端准入功能，支持禁止不满足终端检查要求的用户访问互联网； ★支持 IP 管理功能，支持查看当前内网 IP 使用情况，帮助管理员减少人工维护 IP 表的工作量；（提供截图证明文件） 对网络接入的终端进行可视化和管理，展示终端详细信息、异常状态等； 支持检测 windows 重要补丁的安装情况，并反馈检测结果；（提供产品界面截图） 支持通过流量检查杀软是否运行，该方式不需安装准入插件（提供产品界面截图） 设备能够发现私接路由（或者共享软件等）共享网络的行为：支持自定义配置终端数量和冻结时间，和添加信任列表。 支持终端安全外联检查规则，终端行为包括但不限于拨号行为、双网卡行为、有 4G 网卡、有无线网卡行为、连接非法 wifi 行为、使用非法网关行为、连接外网行为、或自定义外联行为。检查到非法外联行为后，支持发送告警邮件、断网的违规处理配置；（提供产品界面截图） 支持”只能访问以下地址”和“不能访问以下地址”的配置；（提供产品界面截图） 支持外设管控。包括但不限于阻断终端用户使用外设，防止终端用户从内网拷贝信息；控制用户通过 USB 接口产生外联行为；允许用户使用某种符合规定的外设；支持填写硬件 ID 白名单（提供产品界面截图），并提供方法告诉管理员如何获取外设的 ID; 支持外设类型：存储设备、网络设备、蓝牙设备、摄像头、打印机 针对 SSL 加密的网站、论坛发帖、web 邮箱的内容进行关键字过滤和内容审计。审计 SSL 网页时，支持加密证书自动分发功能，用户点击网页上的工具即可一次性安装完成。解决管理员给每台 PC 单独安装证书的问题（要求提供产品界面截图） 支持业务审计，管理员需指定业务 IP 范围，系统即可自动识别开放的业务端口，里面的流量类型，并自动记录日志；审计用户主动访问业务产生的日志，审计业务主动连接外网产生的日志（所有功能必须提供产品界面截图） 必须支持流量父子；通道技术，且至少支持三级父子通道。 能够实时看到各级流控通道的状态：包括所属线路、瞬时速率、通道占用比例、用户数、保证带宽、最大带宽、	

					优先级，启用状态等。 支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率。 ★支持通过抑制 P2P 的上行流量，来减缓 P2P 的下行流量，从而解决网络出口在做流控后仍然压力较大的问题。（提供产品界面截图） 基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中（提供产品界面截图） 支持日志高性能模式处理，精简冗余日志。 管理员登录数据中心只能审计指定用户组的上网行为日志。 内置多套日志模板与各省市网安日志平台对接，至少支持以下平台：派博、任子行、网博、云辰、烽火、中新软件、兆物、新网程、美亚柏科、爱思等。 能够与同品牌终端检测响应产品实现联动，当检测到终端未安装终端检测响应产品产品时，禁止上网并提示需要安装终端检测响应产品软件；（提供截图证明文件） 具备国家版权局颁发的《上网行为管理软件》软件著作权证书	
9	应用负载均衡	业务冗余	政务云业务域	2	4 层吞吐量（默认网口）：≥20G，四层并发连接数：≥8000000，4 层新建连接数 CPS：≥210000，7 层新建连接数 RPS：≥350000。 硬件参数：规格：2U，内存大小≥16G，硬盘容量≥240G SSD，电源：冗余电源，接口≥6 千兆电口+2 万兆光口 SFP+。 支持串接部署方式和旁路部署方式，支持三角传输模式。 提供针对多条出口线路的链路负载均衡功能，实现 inbound 和 outbound 流量的均衡调度，以及链路之间的冗余互备。 提供针对 L4/L7 内容交换的服务器负载均衡功能，可在单一设备上支持多个应用和服务器集群，可以根据多种算法和要求分配用户的请求。 提供针对多站点业务发布的全局负载均衡功能，通过智能 DNS 等机制实现内外网用户对多个数据中心的最优接入路径选择 ★单一设备可同时支持包括链路负载均衡、全局负载均衡和服务器负载均衡的功能。三种功能同时处于激活可使	要求与抗拒绝攻击、态势感知平台异构，不得同一品牌

					用状态，无需额外购买相应授权。（提供设备操作界面截图证明材料，并提供厂家授权免费开通功能声明并加盖公章) ★支持轮询、加权轮询、按主机加权轮询、加权最小连接、按主机加权最小连接、动态反馈、最快响应、加权最小流量、按主机加权最小流量、加权源 IP 哈希、带宽比例、哈希、首个可用、优先级等算法。（提供设备操作界面截图证明材料) 通过某种编程语言（如 lua）实现自定义的流量编排，对 IP、TCP、UDP、SSL、HTTP 和 HTTPS 等类型的流量进行分发、修改和统计等操作。（提供设备操作界面截图证明材料) ★支持静态 IP 和 PPPOE 两种线路接入方式。（提供设备操作界面截图证明材料） ★支持三明治架构，对防火墙、IPS、行为管理等网络设备进行流量负载均衡和故障切换，使以上网络设备获得 Active-Active 运行的能力。（提供实际的功能测试报告）支持跨设备健康状态监视（透明监视），同时支持 IPv4 和 IPv6（提供设备操作界面截图证明材料） 支持基于五元组条件（源 IP 地址，源端口，目的 IP 地址，目的端口，传输层协议号）来进行出站访问的流量调度分发。 ★支持基于管理员自定义的时间计划来进行出站访问的流量调度分发。（提供设备操作界面截图证明材料） ★内置完备的 IP 地址库，无需手动导入并支持自动全网更新，可查看并编辑各国家、国内各省份的 IP 地址段和国内各大运营商 IP 地址段，并可灵活匹配 IP 地址库进行流量调度分发，实现链路负载功能（提供设备操作界面截图证明材料） ★支持基于 URL 的链路调度功能，内置不少于 1000 条的国外 URL 网址库，无需手动导入并支持自动更新，管理员可查看并进行编辑。可根据 URL 将访问国外网站的请求调度到指定线路。（提供设备操作界面截图证明材料） ★支持基于应用协议的智能选路，能对网银、游戏、视频等流量进行调度（需提供设备功能界面截图证明） ★支持基于域名的流量调度，针对特定网站选择指定的链路转发。（提供设备操作界面截图证明材料） 支持 DNS 透明代理功能，可基于负载均衡算法代理内网用户进行 DNS 请求转发，避免单运营商 DNS 解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率。（提供设备操作界面截图证明材料） 支持 DNS 内网记录，包含 A、AAAA、CNAME、MX 和 TXT 等类型，可识别内网用户并对其 DNS 请求直接返回相应结果; 支持智能 DNS 解析功能，实现外网用户访问内网业务系统的最优路径选择。 链路健康检查与服务器健康检查联动，入站负载跟服务器负载结合的时候，如果后端服务器全挂，则入站负载时也认为该虚拟 IP（此时要求入站负载的虚拟 IP 与虚拟服务发布的 IP 组相同）也离线，从而达到联动效果。 支持基于链路负荷情况的繁忙保护机制，能根据链路的上行/下行带宽占用率情况执行对出站/入站流量的高级调度策略。（提供设备操作界面截图证明材料）	

					★SLB 能够通过健康检查来获取后端服务器状态，同时将服务可用性、设备 CPU、新建并发吞吐等数据上报 GSLB，设备之间的联动使得 GSLB 能根据链路和服务器两者的综合状态实现智能切换，为用户选择最优的数据中心和服务器分配方式。 ★支持跨数据中心集群和跨数据中心会话保持 支持多种链路检测方法，能够通过 PING、TCP、HTTP 等方式监控链路的连通性，当某一条链路故障时，可将访问流量切换到其它链路，保障用户业务的持久通畅。 ★支持链路负载投屏展示，能够分别基于链路监测、应用选路和 ISP 流量进行投屏展示分析。链路监测展示链路的健康状态、上下行带宽、总带宽、新建连接数、并发连接数和吞吐量；应用选路展示基于应用分类选择相应链路的示意图；ISP 展示基于运营商分类选择链路的示意图。（提供设备操作界面截图证明材料） 支持源 IP、Cookie（插入/被动/改写）、HTTP-Header、SSL Session ID 等多种会话保持机制，支持跨虚拟服务的会话保持。（提供设备操作界面截图证明材料） ★支持 cookie 加密，提升 cookie 安全性。提供设备操作界面截图证明材料） ★支持防秒杀功能，即能够以 JSESSIONID 为标识限制用户访问速度，且不影响该用户访问非防护页面（提供设备操作界面截图证明材料） 支持大数据输出功能，输出必须包括客户端 IP、x-forwarded-For IP、访问时间、访问 IP、访问 URL、响应时间和资源大小。 （提供设备操作界面截图证明材料） ★支持优先级算法下最少可用节点保障，优先级高的节点故障时会自动进行选举，保证优先级高节点的可用性。 ★支持常见的主动式健康检查功能，提供基于 SNMP、ICMP、TCP/UDP、FTP、HTTP、DNS、RADIUS，ORACLE/MSSQL/MYSQL 数据库等多种类型的探测判断机制，支持对 HTTPS 服务进行内容健康检查。 ★支持用户自定义方式的健康检查，支持多种编程语言（如 Python、Java 等），用户可根据节点运行的实际业务流程来编写代码，检查业务处理逻辑是否正常。（提供设备操作界面截图证明材料） ★支持外部监视器探测方式通过编写脚本执行命令使得节点智能恢复，当节点出现故障时，负载均衡能自动重启服务器上的相关进程或重启服务器，使其恢复正常状态并继续提供服务；如无法使其恢复正常，则将其从节点池中移除，保证业务正常访问。（提供设备操作界面截图证明材料） 支持银联 8583 等长连接负载，支持 8583 单工和双工的区分，对于非 HTTP 协议的长连接应用，可通过分析议特征来识别消息的开始和截止，以消息为对象进行七层负载均衡，而非传统基于连接的四层负载均衡。（提供设备操作界面截图证明材料）6.6 定制和 6.6R1 定制、705 定制、708 定制支持；708R3 版本默认支持 ★支持被动式健康检查，可根据对业务流量的观测采样，辅助判断应用服务器健康状况；对常规 HTTP 应用可配置基于反映 URL 失效的 HTTP 响应状态码的观测判断机制，对于复杂应用可配置基于 RST 关闭连接和零窗口等异	

					常 TCP 传输行为的观测判断机制。（提供设备操作界面截图证明材料） ★支持面向服务器健康度的弹性调控机制，可通过监控业务流中的 TCP 传输异常来衡量服务器节点的有效性，尝试对性能不足的服务器临时开启过载保护，动态调节服务器的负载。（提供设备操作界面截图证明材料） ★支持主动探测方式与被动观测方式结合使用的服务器健康检查手段，以便适应各种复杂应用交互流程，保障业务系统的高可用性。（提供设备操作界面截图证明材料） 支持配置每台的服务器最大连接限制和新建连接限制，以及单个特定用户或者一个用户组中所有用户访问指定应用服务的并发连接总数限制，避免应用系统的服务器过载。 ★支持命令行配置，支持 Tab 键补全操作，支持界面全部模块通过命令行的模式配置，支持命令批量操作，支持配置导入导出命令行操作（提供设备操作界面截图证明材料） ★节点支持域名和 IP 两种形式，支持自定义 DNS 查询间隔。（提供设备操作界面截图证明材料） ★支持后端服务不可用时主动关闭连接，保证客户端访问的连续性（提供设备操作界面截图证明材料） ★支持 Loose Initiation 和 Loose Close 功能选项（支持非 SYN 建立会话的选择和任意 FIN 释放会话选择）（提供设备操作界面截图证明材料） ★对于超过服务器的连接数上限或者请求数上限的新建连接缓存起来放入队列中，后续分批逐步发送给服务器，而不是直接丢弃数据包（提供设备操作界面截图证明材料） ★服务器负载状态支持投屏展示，能够显示设备的电源状态、风扇转速、磁盘温度、CPU 温度、CPU 和内存占用率、新建连接数、并发连接数、吞吐情况、SSL 新建和 SSL 吞吐数据、压缩优化和缓存优化数据；业务的健康状态、新建连接数、并发连接数、上下行流量、每秒请求数；节点池的调度算法、健康状态、新建连接数、并发连接数、上下行流量；（提供设备操作界面截图证明材料）； ★支持二个或四个以上的多重引导（提供设备操作界面截图证明材料）； IPv6 支持双栈模式，支持 NAT46、NAT64、NAT66、FTP ALG、DNS64 等协议转换 ★IPv6 改造方案能够解决天窗问题，支持一条策略匹配多个外链网站，同时外链和网站子链发生修改时支持自动识别并做主动修改，不允许通过人工解析配置的方式解决天窗问题 提供 IPv6 产品检测报告； 支持通过 syslog 的方式实现 IPv4/IPv6 协议转换日志功能，累积存储和查询 3 个月内数据；提供 IPv6/IPv4 协议翻译和互通的日志信息，包括源/目的 IP 地址和端口，被访问的 URL 等信息，并在需要的情况下，回溯查询用户信息 七层虚拟服务支持时间戳、TIME_WAIT 资源快速回收、节点失效关闭连接和重置无效连接功能（提供设备操作界面截图证明材料） 七层虚拟服务支持延迟 ACK、SACK 和 DSACK 功能（提供设备操作界面截图证明材料）	

					支持 HTTP 缓存功能，利用内存 Cache 缓存用户频繁访问的 web 内容，降低后台服务器的负载压力,提升用户访问的响应速度。 支持 HTTP 压缩功能，采用工业标准的 GZIP 或 Deflate 算法来压缩 HTTP 数据，从而减少传输数据量并降低带宽消耗，缩短客户端访问的下载等待时间。 支持 TCP 连接复用功能，利用 HTTP 连接池机制，将来自客户端的多个请求合并成一个连接发送到服务器，减少服务器端的工作负荷，并提升业务效率。 支持 SSL 卸载功能，卸除服务器端的密集型运算任务，释放服务器计算资源，并提升 SSL 业务的处理速度； 支持 SSL 加密功能，可将普通流量加密以适配需要通过 SSL/TLS 协议才能访问的服务器； ★支持非对称式部署的 TCP 协议优化技术，提升远端用户访问应用服务的速度。无需在用户终端或应用服务器上安装任何插件和软件，不受操作系统类型、浏览器版本等兼容性因素限制，并且用户首次访问应用服务即可产生加速效果。(提供第三方评测报告,证明所投产品厂商可提供此类技术) ★支持图片优化技术，通过对图片格式的转换，减少传输流量，提升 web 页面加载速度。无需改动服务器端的图片源文件，可根据浏览器种类自动识别转换类型，将图片转换为对应支持的 WebP 或 JPEG 格式，优化加速效果。（提供设备操作界面截图证明材料） ★免费开通 HTTP 压缩、HTTP 缓存、TCP 连接复用、SSL 卸载等功能，无需额外购买相应授权。（提供厂家授权免费开通声明并加盖公章）。支持双机热备部署方式，可自动同步配置并提供连接会话的镜像功能，实现无缝故障切换； 支持基于链路流量进行有效性判断，能够在预设时间内进行主动探测。 支持高可用集群 N+M 部署方式，单集群支持 16 台设备，可自动同步配置并提供连接会话的镜像功能，实现无缝故障切换； ★提供基于 VM 和容器两种方式的硬件一虚多。一台物理设备可从逻辑上划分为多台虚拟设备，各虚拟设备拥有独立的计算资源和网络资源，各虚拟设备可运行不同软件版本，虚拟设备重启或升级时不影响其他虚拟设备的正常运行，虚拟设备宕机可自动重启。 支持全中文管理界面和 HTTPS 方式登录、用户角色管理、多级授权管理。 支持设置管理地址白名单列表，远程维护支持设置是否允许 WAN/LAN ★支持 SNMP v1/v2c/v3，标准 MIB 库和自定义库，可接受第三方网管平台如 zabbix 的管理（提供设备操作界面截图证明材料） ★IPv6 支持双栈模式，支持 NAT46、NAT64、NAT66 等协议转换（提供设备操作界面截图证明材料） ★内置智能告警系统，支持 E-mail、SNMP Trap 两种告警方式，管理员可基于业务安全所关注方面来选择告警触发事件与对应的告警方式，当业务网络环境中发生问题时（如服务器宕机、网络攻击、链路中断等故障场景），	

					即会自动向管理员发送告警信息。（提供设备操作界面截图证明材料） ★设备内置数据中心，支持自动订阅和手动生成两种方式输出 PDF 格式的报表。报表可对链路和服务器的稳定性进行统计，可查询服务器的异常状态信息，并提供对故障原因的分析。 支持全局数据中心智能 DNS 统计，包括访问次数统计及按照 Local DNS 来源统计；支持统计虚拟服务和真实服务器的流量、访问次数、并发连接数。（提供设备操作界面截图证明材料） ★支持标准的 RESTful 等形式的 API 接口，可提供 Python 和 Java 的 SDK 工具，可实现与第三方应用平台的集成与二次开发。（提供设备操作界面截图证明材料） ★所投产品具备《计算机软件著作权登记证书》(提供复印件) ★所投产品具备国家强制性产品认证（CCC 认证）报告 ★所投产品具备国家工业和信息化部颁发的《电信设备进网许可证》(提供复印件)	
10	日志审计	安全运维	安全管理域	1	★提供不少于 2*USB 接口，1*RJ45 串口，2*GE 管理口，设备提供 不少于 4*千兆 SFP 插槽，不少于 6*GE 电口，不少于 1 个接口扩展槽位；不少于 1 个 RAID 卡，不少于 4TB SATA 硬盘。★系统硬盘容量应不低于 4TB，应支持定制扩容； 1）需提供原厂售后服务证明（加盖厂商公章）； 2）提供原厂商 3 年免费质保及升级服务； 1）系统应为标准式机架硬件设备，全内置封闭式结构，具有完全自主知识产权的专用安全操作系统 2）★系统应支持冗余双电源，避免电源硬件故障时设备宕机，提高设备可用性 3）系统应基于大数据平台架构，具备海量数据收集与快速检索能力 4）系统应基于 B/S 架构，支持 SSL 加密模式访问，可通过 web 方式直接对系统进行管理 5）系统应支持内置采集器，不依赖其他设备即可进行日志采集 6）系统支持的数据采集范围包括但不限于网络安全设备、交换设备、路由设备、操作系统、应用系统等 7）系统支持的数据采集方式包括但不限于 SYSLOG、SNMP/SNMP TRAP、FTP/SFTP、HTTP、API 接口、WebService、专用 Agent 等方式采集日志 8）系统应能实现海量日志数据的采集并保存原始日志数据 9）系统应能够对异构日志格式进行统一化处理并保存统一化处理后的日志数据 10）系统应能够实现对海量日志数据快速查询（提供功能界面截图并加盖公章） 11）系统应支持按类型、按日期(天)，手动、自动备份日志 12）系统应支持设置日志存储备份策略，可设置备份周期、备份日志类型等 13）系统应支持日志备份远程服务器，如传送到 FTP 服务器（提供功能界面截图并加盖公章） 14）系统应支持备份加密	要求与链路负载均衡、数据库审计异构，不得同一品牌

					15）系统应支持备份空间磁盘状态监控与主动告警 16）系统应支持备份日志导入查询 17）系统应支持实时日志查询、历史日志查询 18）系统应支持原始日志、范式化日志查询 19）系统应支持自定义查询规则 20）系统应支持查询实时事件，支持自定义查询事件，支持模糊查询 21）系统应支持事件规则自定义，支持面向日志类型的规则配置，支持通过插件方式实现日志类型的扩展 22）系统应支持周期性合并事件告警 23）系统应支持资产标签，且至少 6 种标签以上，根据标签可快速查询资产（提供功能界面截图并加盖公章） 24）系统应支持手工注册资产，支持对资产进行修改/删除、批量导入/导出/添加/修改/删除等多种方式的管理； 25）系统应支持从日志进行资产发现（提供功能界面截图并加盖公章） 26）系统应支持按资产查看资产日志、事件、资产告警 27）系统应能够按照多种维度统计日志信息 28）系统应支持统计分析报表与多种文件格式导出 29）系统应能支持用户上传自定义报表模板 30）系统应支持支持用户自定义账号 31）系统应支持管理员、审计员、操作员多种权限设置 32）系统应支持来访 IP 限制，对暴力猜测 IP 地址进行锁定 33）系统应支持自身日志记录并可查询、自身 CPU、内存和磁盘使用率可监控并以图形化方式动态显示； 34）系统应支持系统基本参数管理、基本配置管理。 1）公安部销售许可证 2）国家信息技术产品安全测评证书（EAL3+） 3）计算机软件著作权登记证书 4）涉密信息系统产品检测证书 5）中国国家信息安全产品认证证书	
11	堡垒机	安全运维	安全管理域	1	2U 机架式软硬一体设备，专用硬件平台和安全操作系统，双冗余电源。6 个千兆电口，1 个 Console 管理口，带液晶面板，2 个扩展槽（可扩展千兆光口、千兆电口、万兆光口），4T 硬盘。可管理设备授权数：无限。 支持在 IPV4,IPV6，IPV4 与 IPV6 网络环境下部署； 支持 NAT 地址映射部署，通过映射后的 IP 地址访问堡垒机进行管理和运维操作，支持从多个映射地址访问，适用于内外网隔离的复杂网络环境；	要求与边界防火墙、漏洞扫描系统异构，不得同一

					支持用户账号命名字母区分大小写、账号支持中文，账号长度最大支持 256 位字节（需提供截图）； 支持用户客户端 IP 和 MAC 限制，非法地址无法登录（需提供截图）； 支持改密的资源包括：Linux、Unix、Windows（采用 RPC 方式）、AIX 以及数据库 Oracle、SqlServer、PostgreSQL、MySql、DB2、Informix 、SYBASE（需提供截图）； ★必须支持数据库协议自动改密，改密类型支持：Oracle、PostgreSQL、MySql、DB2、Informix 、SYBASE，Mssql(2005,2008,2012)；（需提供截图） 必须支持以资源为视角进行用户访问授权，可在具体资源上直接进行用户角色绑定，提高授权关系绑定易用性和灵活性；（需提供截图） 支持限定配置中可指定用户通过指定的应用发布服务器对资源进行访问； 支持 WEB 界面上传改密脚本，通过自定义脚本模式实现新增改密类型，满足多种改密需求；（需提供截图） 支持管理员通过 WEB 界面自定义上传用户手册，保证使用手册及时更新； ★必须支持 Oracle、Postgresql、Sybase、MySQL、SQL server 数据库下行返回行数记录； 支持在 Oracle 数据库运维，运维人员对变量进行绑定，执行 SQL 后，堡垒机系统可审计对应 SQL 中唯一标识符的具体值，协助审计员分析安全事件。（需提供截图） 支持 RDP、VNC 图形操作过程中键盘输入操作记录和鼠标点击行为记录，并支持开启或关闭键盘输入审计功能； 支持 web 页面防跳转功能，进行 http/https 访问过程中，运维人员仅允许访问授权地址会话协议回放空闲时间过滤，应用发布图像操作回放支持操作空闲过滤（可设置无操作多长时间开始过滤）； ★必须支持审计查询关键字和结果显示支持多种编码(UTF-8,Big5,EUC-JP,EUC-KR,GB2312,GB18030,ISO-8859-2,KOI8-R,KS_C_5601_1987,Shift_JIS,Window-874)，由审计管理员自主选择；（需提供截图） 支持 SSH 协议服务端启用强加密算法 hmac-sha2-256,hmac-sha2-512，提升 SSH 协议安全性; 支持对剪贴板拷贝文件行为和文本信息内容的记录，并支持通过搜索文本内容关键字定位审计回放 自定义审计查询条件，包括：时间范围、用户、资源、资源账号、IP、关键字等条件; ★必须支持 C/S 客户端模式：提供 C/S 客户端功能，用于运维人员和管理员通过 C/S 客户端登录进行运维操作和管理操作，整个运维过程不依赖任何 Active 或 Java 控件；（需提供截图） 双因素认证：支持对不同用户设置不同认证方式组合的双因素认证（需提供截图）； 支持用户属性中手机号码和邮箱地址作为主账号身份登录； 支持用户以手机号码或邮箱地址作为用户身份登录；（需提供截图） ★必须支持扫描本地运维工具并进行配置保存，简化运维人员使用配置过程（需提供截图）； 支持调用运维人员终端电脑上的数据库工具，不改变运维人员使用习惯：SQLPlus、PLSQLDev、Toad for Oracle、	品牌

					Db2cmd（DB2）、Quest Central for DB2、Teradata SQL Assistant、SqlDbx Personal、SqlDbx Professional、pgAdmin3、Mysql Command、SSMS、Dbvisualizer、Navicat；（需提供截图） 支持以 Syslog 对外发送登录日志、业务管理日志和运维审计日志（需提供截图） ★必须支持运维用户可以设置自动运维操作定时/周期执行，实现网络设备配置的自动备份、供用户查看、下载（需提供截图）， 支持运维用户设置运维命令，在 Linux 类主机和网络设备自动执行并返回结果，供用户查看、下载（需提供截图）。 ★必须支持应用发布防跳转：通过应用发布只能访问已授权资源，无法通过应用工具新建未授权资源进行跳转连接（需提供截图）， 支持 web 页面或数据库防跳转功能，进行 http/https 访问过程中，运维人员仅允许访问授权地址（需提供截图）， 支持历史审计日志备份文件导入与历史审计日志查询；（需提供截图） 所投产品须提供以下证明文件： 所投产品须具备国家版权局《计算机软件著作权登记证书》； 所投产品须具备《计算机信息系统安全专用产品销售许可证 运维安全管理产品（增强级）》； 所投产品须具备中国信息安全认证中心颁发的《中国国家信息安全产品认证证书》；	
12	漏洞扫描	风险评估	安全管理域	1	★系统提供不少于 6 个 100/1000base-T 接口；提供不少于 1 个扩展插槽（支持扩展 4SFP/8SFP 接口）；设备提供 1 个 RJ45 管理串口； ★可扫描存活 IP 总数:无限 IP;最大扫描速度:不少于 20IP/分钟;最大存储任务数:不少于 1500 个； ★自主研发的安全产品，采用专用硬件平台及专用安全操作系统 ★提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与 CVE、CNCVE、CNNVD、CNVD 等主流标准兼容，并提供 CVE Compatible 证书；提供对主流操作系统、数据库、网络设备的漏洞检测功能；提供扫描过程中人工指定包括 SNMP、SMB、SSH 登陆口令的功能（提供功能界面截图并加盖公章）； 2）★支持扫描物联网设备的漏洞，需覆盖常见品牌摄像头、打印机、路由器，摄像头需支持扫描海康威视、宇视、大华、亚安、派尔高，打印机需支持扫描惠普、三星，路由器需支持扫描 TP-LINK、D-LINK、NETGEAR。支持扫描容器镜像存在的漏洞，支持扫描互联网上公开仓库中的镜像以及私有仓库中的镜像。支持专门针对已有攻击利用代码的漏洞检测，检测用户资产是否存在可利用的漏洞（提供功能界面截图并加盖公章）。 3）支持专门针对 DNS 服务的安全漏洞检测，包括 DNS 投毒等漏洞检测能力；支持“幽灵木马”检测（提供功能界面截图并加盖公章） 4）系统内置不同的策略模板如针对 Unix、Windows 操作系统等模板，同时允许用户定制扫描策略；支持对多个扫描任务并发执行 5）支持 Oracle、MySQL、MS SQL、DB2、Sybase 数据库漏洞检查。支持智能端口挖掘，可以智能发现非默认端口	要求上网行为管理、态势感知平台异构，不得同一品牌

					启动的服务（提供功能界面截图并加盖公章）。 6）提供端口扫描和弱口令猜测功能，可以智能发现非默认端口启动的服务，并调用相应扫描插件进行扫描（提供功能界面截图并加盖公章）； 7）★能够和 IPS 进行联动，通过平台进行反馈漏洞详情（提供功能界面截图并加盖公章）； 8）支持多任务自动调度，提供定期扫描与周期扫描功能（提供功能界面截图并加盖公章）； 9）可以智能发现非常规端口服务；评分标准可配置风险值计算标准；支持把资产管理和组织结构或者网络拓扑结构紧密结合，支持资产树等多种资产管理方式，支持通过资产树对指定主机展开漏洞扫描和配置核查任务，查看主机风险（提供功能界面截图并加盖公章）； 10）支持立即执行、定时执行、周期执行扫描任务，自定义的周期时间可精确至每*月第*个星期*的*点*分，请提供功能截图。支持断点续扫，可对已完成的扫描任务中没有被覆盖到的目标重新下发扫描任务（提供功能界面截图并加盖公章）。支持扫描时间段控制，只在指定时间段内执行任务，未完成任务在下一时间段自动继续执行，请提供功能截图 11）支持认证信息管理，可将系统登录信息、配置检查模板进行统一管理和配置，提供登录信息导入功能，无须每次下任务时进行配置（提供功能界面截图并加盖公章）。 12）支持和微软 WSUS 补丁系统的联动，能够在发给主机管理员的邮件中附带自动配置 WSUS 的注册表文件，方便进行自动化的补丁修补（提供功能界面截图并加盖公章）。 13）提供资产管理功能，支持通过 Excel 文件将地址导入到资产树；支持手动升级和在线自动升级、通过代理升级，至少每两周进行一次定期升级；提供创建系统还原点的备份恢复机制和操作审计功能（提供功能界面截图并加盖公章）； 14）支持集中管理；能够与 WAF 进行联动，形成漏洞管理闭环。（提供功能界面截图并加盖公章） 15）可与安全中心联动，实现分布式部署和集中任务下发、资产风险分析;产品支持集中告警平台，可以灵活配置告警内容、告警方式、告警资产范围等内容（提供功能界面截图并加盖公章）， 16）支持移动 APP 远程设备状态监控和管理（提供功能界面截图并加盖公章）。 17）漏洞分析报告提供在线浏览报告和离线打印报告；可以通过资产仪表盘直观展示资产的风险值、主机风险等级分布、资产风险趋势、资产风险分布等内容（提供功能界面截图并加盖公章）。 18）提供针对不同角色的默认模板，允许用户定制报告的内容、报告的格式等，报表详细描述漏洞信息并提供解决方案；提供历史数据查询、对比分析、趋势分析等功能；离线报告可以输出到 HTML、WORD、EXCEL（XML）等文件，报告可以直接下载或通过邮件直接发送给相应管理人员 1）计算机软件著作权登记证书,公安部销售许可证（增强级）；2）国家信息安全测评中心信息技术产品安全测评证书—EAL3+；3）涉密信息系统产品检测证书；4）中国国家信息安全产品认证证书（增强级）；5）CVE 兼容	

					性认证证书 1）以上 18 条功能参数需逐条满足并逐条测试功能，5 项资质需加盖原厂商公章证明文件 2）提供投标型号测试机并测试，满足所有功能方可签署合同，否则按照虚假应标进行处理。	
13	杀毒软件	病毒防御	安全管理域	1	200 服务器授权（可根据需要调整不同操作系统授权数） 无需安装任何其他软件和专用设备硬件，采用基于 X86 服务器或虚拟服务器即可完成平台部署；终端 Agent 软件可以通过软件安装或虚拟机模板的方式进行安装。 ★基于多维度轻量级的无特征检测技术，多引擎协同工作，包括：基于 AI 技术引擎、基于家族基因分析的特征检测引擎、基于虚拟执行和操作系统环境仿真技术的行为引擎、基于大数据分析平台的云查引擎。（提供产品界面截图） 支持本地查杀缓存，具备二级缓存机制：终端侧使用全盘文件缓存，加速本地二次扫描速度，减少对本地虚拟化环境的资源消耗；管理平台侧使用全网文件缓存，加速云查杀速度，减少通过互联网进行云查杀的带宽消耗 支持 agent 安装目录的文件保护，可以保护 agent 目录和文件实时监控驱动文件，可以保护 agent 的服务/进程/文件不被恶意删除，影响正常功能，导致用户的终端受到病毒入侵 ； 支持禁止黑客工具启动，包含：冰刃、xuetr、ProcessHacker、PCHunter、火绒剑、Mimikatz 的自启动，可以防止黑客攻击 支持对 zip， rar， jar， cab， 7z 等常见压缩文件的查杀，支持压缩文件查杀层级进行策略配置，最大可配置检查 10 层压缩文件； ★支持全网风险展示，包括但不限于未处理的勒索病毒数量、暴力破解数量、WebShell 后门数量、高危漏洞及其各自影响的终端数量（需提供产品截图证明） ★管理平台界面提供勒索病毒防护专区，提供针对勒索病毒的多维度防护机制；支持对勒索病毒的家族名、病毒名、加密文件后缀名的链接查询，或者通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具（需提供产品截图证明 ） ★提供挖矿病毒巡检工具，支持通过内存、进程和启动项来检索病毒相关信息（需提供产品截图证明） 支持对风险终端进行终端隔离，避免感染终端对内网其他主机的病毒传播； 支持对已隔离终端的恢复操作。 ★支持按照扫描网段、扫描方式、扫描协议、扫描端口对终端进行扫描，及时发现尚未纳入管控的终端（需提供产品截图证明） ★支持对安装了指定版本操作系统、特定应用软件、开放了高危端口的风险主机进行统计，具备对风险主机进行漏洞扫描、安装高危软件的主机列表信息统计导出、高危端口一键封堵的能力 （需提供产品截图证明） ★支持终端客户端软件的启用禁用，重启，支持在管理平台直接卸载客户端软件（需提供产品截图证明）	要求数据库审计、漏洞扫描系统异构，不得同一品牌

					★支持对在线终端下发实时通知消息（需提供产品截图证明） 支持对来自 Internet、E-mail 或是光盘、移动存储、网络等各种入口渠道病毒进行实时检测； ★可实时监控文件的状态，在文件读、写、执行或者进入主机时主动进行扫描，支持根据用户性能偏好设置高、中、低 3 种防护级别（需提供产品截图证明） WebShell 文件的检查综合利用文件信誉库、静态分析、机器学习、运行行为分析对文件进行判断。 支持配置 WebShell 检测开启或关闭； 支持配置 WebShell 定时扫描任务，配置参数包括：扫描周期（每日、每周、每月）、扫描时间精确到分、发现威胁处置方式（自动隔离、仅上报不隔离）； ★支持展示终端检测到的 WebShell 事件及事件详情，包括：恶意文件名称，事件等级，受感染的文件，发现时间，检测引擎，文件类型，文件名，文件 Hash 值，文件大小，文件创建时间，检测依据； 基于 Agent 的 RDP 和 SSH 登录日志检测的暴力破解入侵检测； 支持单个攻击源和分布式攻击源的暴力破解检测； 支持开启暴力破解实时检测，自动封堵攻击源的 IP 地址，封停时间支持配置；（提供产品界面截图） ★支持展示终端检测到的暴力破解事件及事件详情，包括：攻击源、攻击类型、检测引擎、最后攻击时间、攻击方法、攻击内容、攻击历史； （提供产品界面截图） 支持对暴力破解事件攻击源 IP 加入黑名单，已加入黑名单的 IP 无法访问网内所有终端； 支持对指定终端/终端组进行终端基线合规性检查，对不合规的检查项提供设置建议； 针对 Windows 系统提供如下安全基线合规检查：身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范； 支持 windows 系统永恒之蓝漏洞（MS17-010）的检测； ★针对 Linux 系统提供如下安全基线合规检查：身份鉴别、访问控制、安全审计、 SSH 策略检测、入侵防范、恶意代码防范；（提供产品界面截图） 支持可视化展示终端的基线合规检查结果。 ★支持基于威胁情报的病毒特征值和域名全网终端搜索，可定位出全网终端该病毒的感染情况（需提供产品截图证明） ★支持管理平台向终端下发脚本（.bat，.sh 和.ps1）执行文件，方便管理人员对终端进行脚本下发 （需提供产品截图证明） 提供对业务系统之间、业务系统内不同应用角色之间、业务系统内相同应用角色之间的访问控制策略配置； ★支持基于 IP、IP 组、服务和角色四个维度进行配置项设置，并且支持对配置项的备份以及恢复操作（需提供	

					产品截图证明） 支持图形化显示业务系统、服务器及流量详情；服务器详情支持展示服务器的资源状态（CPU 占有率、内存占有率和磁盘率）、流量分布 Top5、该服务器开放的服务；流量线详情支持展示该流量线对应的微隔离策略；图形化显示服务器间流量关系，包括访问详情、流量趋势等。 ★支持与同厂商的网络防火墙进行安全联动，管理员可以在同厂商的网络防火墙管理界面下发快速查杀任务，并查看任务状态，结果并进行处置，支持在管理平台查询和统计联动信息 （需提供产品截图证明） ★支持未安装终端安全客户端的终端无法上网，有效推广终端安全客户端的部署 （需提供产品截图证明） 具备公安部颁发的销售许可证 具备版权局颁发的软件著作权证书	
14	网管平台	自动化运维	安全管理域	1	网络设备管理授权 100 点； 1.要求资源拓扑、告警、性能等功能模块支持多服务器分布式虚拟化部署，可实现负载分担，满足大规模网络环境的统一管理。 2.用户分权管理：可以为不同的管理员设置不同的用户名、密码，并限制管理员的管理权限和管理范围，实现用户分权管理； 3.多平台支持：支持 Windows、Linux 平台、麒麟等国产操作系统，及 MS SQL、Oracle、达梦等数据库，支持 B/S 架构； 4.支持自定义用户主页：管理员可以首页中通过拖拽，自定义需要在首页展示页面，同时支持 Widget 扩展； 5.自动发现拓扑：自动发现网络中的所有网络设备，并在拓扑中显示出来，支持拓扑图自定义修改，包括设备、链路等（提供截图）； 6.支持 IP 拓扑、二层拓扑、自定义拓扑视图（支持网络区域的任意划分、命名、拖拽、折叠和展开）、全景拓扑、Vxlan 拓扑、邻居拓扑、LLDP-MED 拓扑、流量拓扑、数据中心拓扑、数据中心机架拓扑、IRF 拓扑、MDC 虚拟网络拓扑、MDC 和 IRF 组合拓扑等多种拓扑类型；二层拓扑支持多协议，包括 Bridge、NDP、CDP、MSTP、STP、LLDP、DISMAN-PING 等二层协议，支持聚合链路，支持第三方的设备；拓扑可融合链路状态、设备告警等多种信息（提供截图）； 7.支持设备与用户统一管理：支持网络管理与用户管理联动，如通过点击拓扑楼层接入交换机图标，可查看该设备所有接入用户帐户信息，查询在线用户列表、强制用户下线、下发消息、总在线用户数统计、不安全用户数统计等； 8.支持设备与流量分析统一管理：支持网络管理平台实现设备管理与流量分析联动，如通过点击拓扑某链路可查看该链路的关键应用流量分布、关键用户流量使用等； 9.故障管理：支持对全网设备告警的实时监控和统一浏览；支持多种提醒方式，如告警实时提醒（告警板）、告	

					警音响提示；支持多种转发方式，比如转 E-mail，转短信，转上级网管或其它网管等。支持告警分析，可以屏蔽重复告警、闪断告警，支持告警自动确认功能； 10.告警智能分析，包括告警分类关联分析、告警多源关联分析、告警拓扑根源分析、告警网络影响度分析； 11.性能管理：支持基于任务的性能监控，可定制监控任务，长期监控网络性能，可以形成日报、周报、月报等报表。支持定制性能阈值，可以为监控的性能指标设置两级阈值，当性能指标超过阈值时根据不同的阈值发送不同级别的告警； 12.提供直观的设备的面板视图：支持设备面板的显示、定时刷新、面板缩放功能，通过面板管理，网络管理人员可以直观地看到设备、板卡、端口的工作状态；并提供基于设备面板的设备、单板、端口配置功能； 13.支持视图定制、切换：平台提供有网络基础管理视图、分级管理视图、快捷业务视图、桌面视图。视图切换方便。极大提高菜单易用性。创建操作员时可以指定有权限的视图和默认登录视图（提供截图）；	
15	态势感知	威胁预警	安全管理域	1	最大支持网络层 8G 网络流量的实时接收采集，应用层 >=5G 的实时采集。最大并发连接数 >=100W，每秒新建链接数≥8W，文件处理性能≥25W/天。 免费三年特征库等相关软件升级服务。 产品应使用高性能硬件架构，集流量采集、沙箱检测、大数据分析、展示于一体。 2U 机架式平台和安全操作系统系统，双冗余电源；配置 96G 内存，48T 存储，4 个千兆电口，具有 7 个接口扩展槽位（可扩展千兆光口、千兆电口、万兆光口）。 支持旁路部署、集群部署 应同时支持流量镜像接入与 syslog 日志接入。 支持网络威胁感知，基于基础检测日志进行威胁分析，基础日志包括入侵检测日志、恶意样本日志、恶意域名日志；各种日志提供单独的视角展示；能够展示、查询各种日志的元数据。 攻击者、被攻击者视角支持展示对应的的地理位置或资产信息、对应的被攻击者、攻击者数量、事件日志数量、样本日志数量、攻击发生时间范围（首次攻击时间、最后攻击时间），支持展示扫描探测、渗透入侵、获取权限、命令控制、传播破坏阶段的日志数量，对应数量可以进行跳转至对应数据以助于进一步分析；支持基于时间、被攻击者数、日志数量进行排序；支持全文检索日志。 产品提供事件日志视角供用户分析网络攻击，支持展示攻击阶段：扫描、攻击尝试、攻击成功、失陷辅助用户判断对应攻击的处理紧急程度；支持基于攻击者 IP、被攻击者 IP、事件名称进行合并，用以快速发现威胁总类；支持配置数据定时刷新 5s、10s、15s；支持基于资产范围、日志状态、攻击方向、攻击阶段等多维信息进行帅选，支持全文检索、模糊匹配，支持添加查询条件到模板，以助于快速检索。 针对攻击事件需支持进行有效性分析，可以展示 HTTP 会话的请求头、请求体、响应头、响应体，可以查看该事件的知识库包括：事件性质判定指引、事件处理建议等信息。支持访问被攻击路径、联动阻断下载报文等分析、	要求与抗拒绝攻击、边界防火墙异构，不得同一品牌

					处理操作。 产品支持检测并展示网络中传输的恶意样本文件，支持查看样本沙箱检测报告，支持中文展示文件恶意类型及关键恶意行为。 产品支持恶意域名检测，展示域名的威胁类型、攻击组织等信息，页面支持一键云查威胁情报 应提供不少于 7 种的专业模型视角：攻击者视角、被攻击者视角、事件视角、样本视角、恶意 URL 视角、威胁情报视角、脆弱性分析视角等多维度的专业视角，并可进行线索分析钻取能力。 支持内网安全和外部攻击两个主线分析维度，内网提供：WEB 攻击、扫描探测、异常行为、暴力破解、僵木蠕分析五个场景；内网提供：WEB 攻击、扫描探测、异常行为、暴力破解四个场景 内网/外网 WEB 攻击：分析内网横向/外网针对内部服务器 web 攻击行为，支持逐个事件进行有效性分析；支持快速关联攻击 IP 的攻击范围、方式的关联图，支持快速关联被攻击 IP 的受攻击范围和方式的关联图。 内网/外网扫描探测：分析内网横向/外网扫描探测行为，可下钻到扫描主机的详细扫描行为，支持快速关联扫描 IP 的扫描范围、方式的关联图，支持快速关联被扫描 IP 的受攻击范围和方式的关联图。 内网/外网异常行为：分析内网横向/外网异常行为，可下钻到访问主机的详细访问行为，支持快速关联访问 IP 的访问范围、方式的关联图，支持快速关联被访问 IP 的受攻击范围和方式的关联图。 内网/外网暴力破解行为：分析内网横向/外网暴力行为，可展示破解结果是否成功，可下钻到破解主机的详细登录行为，支持切换到基础登录日志，支持快速关联破解 IP 的攻击范围、方式的关联图，支持快速关联被攻击 IP 的受攻击范围和方式的关联图。 内网僵木蠕分析：支持检测内网主机会连后门、横向传播等威胁 支持基于旁路网络流量发现内部的脆弱性，包括弱口令、漏洞和高危端口。 支持根据登录成功的流量判断脆弱口令，支持 telnet、mysql、ftp、tds、smtp、pop3、imap 协议脆弱口令检测，支持自定义脆弱口令以防止常用复杂口令被爆破。 支持监测网络环境中在公网开放的高危端口，并记录高危端口连接记录。 支持监测内部主机存在的漏洞，并记录存在对应的攻击行为。 支持对网络资产进行感知分析，可配置多级资产分组，编辑资产分组范围，支持自动发现网络资产配置，可编辑资产的类型、标签、系统、位置、服务等信息。 支持公网私用配置，可将非私有地址配置成内部资产，并可自定义资产的地理位置。 支持发现失陷资产，支持基于 SMB 攻击行为、蠕虫传播行为、其他内网攻击以及用户手动确认攻击成功事件分析失陷主机，可以查看主机失陷判定事件的判定性质和处理流程。 支持对单资产进行分析，基于时间轴展示资产受到攻击的全部事件。 提供威胁情报视角，展示命中情报的数座数据，支持 IOC 一键云查，支持自定义威胁情报，可下载、导入情报库	

					模板；支持基于时间轴展示威胁情报总览情况。 单机内扩展的未知样本检测能力支持 callback 情报信息的提取并自动应用到已知检测模块。 ★必须能够与同品牌 IPS、WAF 产品进行联动阻断，可通过目的主机信息、异常访问事件、告警级别、命中威胁情报等参数配置自动化阻断规则，可配置阻断时长信息。（需提供截图证明） 提供事件帮助知识库，可根据事件名称查看对应事件的详细信息，包括事件名称、安全类型、事件描述、CVE、CNCVE、CNNVD、漏洞发现时间、影响系统、影响设备、软件指纹信息、事件性质判定、事件处理流程等信息。 支持配置白名单，可添加 IP、域名、MD5、事件名称，在各视角、有效性分析页面可以进行一键加白；支持指定 IP 和事件关联加白。 全局态势：统计汇总外部攻击情况和内部攻击情况，外部攻击至少包括 web 攻击、扫描探测、异常行为、暴力破解等；内部攻击至少包括 web 攻击、扫描探测、异常行为、暴力破解、僵木蠕等；支持根据时间显示攻击情况，当天、本周、近 7 天。 能够展示资产相关信息，内容包括资产信息、资产类型、活跃资产；3D 展示攻击情况，明确地理攻击方向，支持根据资产分组进行筛选展示攻击信息。 威胁情报态势：可显示基于威胁情报整体攻击趋势图；可在屏幕上对 IP、MD5、URL 进行云端威胁情报查询；界面包含威胁行为分析、情报 TOP5、链接域名 TOP5、情报总数等；分类统计展示 TOP4 的情报类型数据；支持根据资产分组进行筛选展示攻击信息。 ★沙箱监测态势：支持流程化展示样本监测情况，展示还原样本数量统计、静态检测样本统计、动态检测样本统计、告警率统计；可实时展示沙箱操作系统的调用分配情况，展示检测的样本总数，其中包括安全样本数量和恶意样本统计数量；可根据资产分组进行筛选展示攻击信息。（需提供截图证明） 外部攻击态势：展示信息包含攻击日志总数统计、基本信息、攻击行为分析、攻击类型分析、攻击事件列表、攻击源 TOP5、被攻击者 TOP5；攻击类型分析包括 web 攻击、扫描探测、可疑行为、高危端口等；展示攻击源的位置、情报标签和攻击次数，展示被攻击这的资产信息和次数；以平面地图展示攻击情况，明确地理攻击方向，攻击路线可支持下钻；客人根据当天、本周、近 7 天的时间范围显示攻击情况。 可根据资产分组进行筛选展示攻击信息。 资产态势：从资产维度展示相关信息，包含服务器、终端、网络设备、安全设备，并统计活跃情况；从资产维护展示攻击事件，包括攻击者信息、被攻击资产信息、攻击事件等。 横向攻击态势：统计展示从内部横向发现的攻击，包含攻击事件统计、失陷主机 TOP5、内部攻击 IP TOP5、事件攻击列表、内部攻击关系等；内部攻击关系包含资产攻击资产、内网 IP 攻击资产、资产攻击内部 IP、内部 IP 攻击内部 IP，可以通过攻击关系图展示；可根据当天、本周、近 7 天时间范围显示攻击情况，可根据资产分组进行筛选展示攻击信息。	

					所投产品须提供以下证明文件： 应标产品具备独立的高级可持续威胁安全监测产品的销售许可证（增强级） 应标产品具备国家版权局软件著作权登记证书 应标产品具备国家信息安全漏洞库兼容性资质证书	
16	数据库审计	安全审计	安全管理域	1	不少于 6 个 10/100/1000M Base-TX 接口；不少于 4 个 SFP 千兆光口；内置存储 2T*2 硬盘，1 个硬盘扩展槽位；抓包速度≥1000M，入库速度≥35000 条/秒，日处理事件≥2 亿条，可审计数据库流量≥ 800M，数据库审计授权个数：无限。 审计系统采用独立硬件；数据库审计授权个数：无限。 ★支持对 Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Teradata、Cache 等数据库进行审计(需提供功能截图)； 支持 MongoDB、Redis、Hbase、hive、ES 等数据库进行审计（需提供功能截图）； 支持 FTP、Rlogin、Radius、NFS、X11 等协议审计(需提供功能截图)。 支持对邮件协议的审计，包括 pop3、smtp 及 IMAP 等。 ★系统应内置规则集，对数据库 DML、DCL、DDL 等语句及 FTP、Telnet 等协议中的命令进行归类，便于用户定制审计策略。(需提供功能截图)； 提供对数据库返回码的实时说明，帮助管理员快速对返回码进行识别(需提供功能截图)； 审计策略支持数据库客户端软件名称、数据库名、数据库表名、数据库字段名、数据库返回码作为响应条件(需提供功能截图)； 审计策略支持数据库客户端软件名称、数据库名、数据库表名、数据库字段名、数据库返回码作为响应条件（非正则表达式方式）； 审计策略支持时间、源 IP、目的 IP、协议、端口、登陆账号、命令作为响应条件 支持对数据库绑定变量方式访问的审计； ★支持频次告警，某一操作在周期时间内达到设定的次数阀值即可告警，周期事件和次数可按需配置，需提供截图证明； 支持数据库并发会话数、并发进程数、并发用户数、并发游标数、并发事务数、数据库锁等超过限制的审计 (需提供功能截图)； 支持数据库操作类、表、视图、索引、触发器、存储过程、域、Schema、游标、事物等各种对象的 SQL 操作审计。 支持 Telnet 协议的审计，能够审计用户名、操作命令、命令响应时间、返回码等； 支持对 FTP 协议的审计，能够审计用户名、命令、文件、命令响应时间、返回码等； ★支持文件内容关键字审计，当网络中传输的文件包含关键字时，可进行告警，对于压缩包中包含关键字的文件	要求与杀毒软件、日志审计系统异构，不得同一品牌

					可准确定位压缩包中路径。（需提供截图证明） ★数据库审计支持用户环境中的数据库和资源账号、表名的自动发现，方便用户使用；（需提供截图证明）； 数据库审计支持用户数据库中敏感信息的自动发现，方便针对敏感信息配置针对性的审计策略，（需提供截图证明）； 敏感信息发现支持探测器和正则表达式两种方式，探测器至少包含：姓名、地名、银行卡、身份证、IP 地址、密码等多种探测器，（需提供截图证明）； 支持用户操作轨迹图展示，轨迹图维度可自定义，包括：资源账号、源 ip、客户端程序名、命令、表名、错误码等，可根据昨天、最近七天、最近 30 天以及自定义时间进行轨迹显示，可显示关联数量，可在某一维度中进行筛选，提供截图证明。 支持敏感信息掩码，用户可以针对姓名、身份证号、手机号、银行卡号、住址以及自定义信息进行敏感信息掩码配置，防止敏感信息在审计系统中进行泄露。需提供截图证明。 ★支持基于场景的操作异常分析；可直观展现数据库异常、异常账号的访问、同账号多 IP 登录、上下班操作量对比异常、操作响应时间分析；需提供截图证明。 支持疑似暴力破解、疑似撞库攻击场景的操作异常分析；行为周期与阀值可按需定义；需提供截图证明。 支持按数据库名、数据库表名、字段值、数据库登陆账号、数据库操作命令、数据库返回码、SQL 响应时间、数据库返回行数作为查询和统计条件。 查询需支持返回全部符合条件的结果，无上限限制；需提供截图证明。 可支持 sql 语句关键字查询，查询结果包含该关键字的 sql 语句；需提供截图证明。 系统应内置统计分析模板，统计模板包括且不限于：趋势分析、统计分析、性能分析等，且支持自定义模板，自定义条件包括源 IP、目的 IP、资源账号、客户端名称、协议等 10 几种。(需提供功能截图) 支持生成 Word、PDF、x1s、HTML、WPS 格式的报表导出。 提供管理员权限设置和分权管理，提供三权分立功能，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能； 能够对连续失败登陆进行自动锁定，锁定时间可设置； 提供审计数据管理功能，能够实现对审计数据的自动备份、删除； 提供系统升级功能，能够通过升级包的方式实现升级； 提供磁盘存储容量不足、磁盘 Raid 故障等自动邮件报警； 审计系统上存在大量敏感信息，必须对审计管理员进行强度更高的认证，管理员登陆支持硬件令牌认证； 提供 CPU、内存、磁盘、网口、运行时间、运行状态等信息的监视功能； 系统支持一键自检功能，可以检查系统当前运行状态，检查内容包括：系统信息、进程信息、数据库信息、授权	

					信息、用户信息等 17 项内容，协助管理员迅速定位系统异常，减少日常维护工作量。需提供功能截图证明； 提供审计策略和配置的导入导出； 系统告警，系统可以针对引擎状态变化、关键进程异常、登录异常、权限异常、系统资源超限、流量超限、HA 状态变化、磁盘空间不足等各类系统自身异常进行实时页面告警，帮助管理员及时发现系统异常； 记录审计事件、界面告警、Syslog 告警、SNMP trap 告警、邮件告警、短信告警等多种响应方式； 支持与同品牌 Web 应用防火墙（WAF）的联动，可对 WAF 上报的应用系统攻击实现场景还原展示；需提供截图。 支持与同品牌 APT 检测产品的联动，对于网络传输的文件不仅可以审计，还支持恶意代码检测，报告可疑的攻击文件。需提供截图证明。 ★所投产品必须提供以下证明文件（如有缺少视为严重劣势项）： 产品具有中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》（增强级）。 产品具有中国信息安全认证中心颁发的强制认证证书（增强级）。 产品具有中国国家保密局测评中心颁发的《涉密信息系统产品检测证书》。 具有国家版权局颁发的《计算机软件著作权登记证书》。 《中国信息安全测评中心的信息技术产品安全测评证书》EAL3。	
17	全流量威胁分析探针	安全检测	安全管理域	2	★采用 2U 专用硬件平台，采用具有完全自主知识产权的专用安全操作系统，稳定可靠，提供交流冗余电源。 ★系统提供不少于 2 个 USB 接口，1 个 RJ45 串口，2 个千兆管理口，内存不少于 16G，设备提供不少于 4 个万兆 SFP+光口，提供不少于 4 个千兆 SFP，提供不少于 4 个 GE 电口；设备整体提供不少于 4 个接口扩展槽位（可扩展 4GE/4SFP/8GE/8SFP/2SPF+/4SPF+）；检测能力不少于 2Gbps，最大并发 TCP 会话数不少于 200 万，每秒新增 TCP 会话数不少于 4 万；应覆盖多种攻击特征，可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测，攻击特征库数量至少为 9700 种以上；支持自定义 TCP/UDP 端口扫描检测模型，结合模型对流量进行检测和告警；内置 WEB 应用机器学习检测模型，支持对 sqli，xss，exec，phprce，ptravel 和 jeli 攻击类型进行分类检测和告警，告警信息至少包括机器学习告警类型和威胁事件名称；内置恶意文件检测引擎，支持对可执行文件、文档、压缩包和网页脚本进行恶意代码检测和告警，告警信息中至少包含恶意文件类型、恶意文件家族信息和恶意文件变种信息。 系统应支持 VLAN 802.1Q、BGP、MPLS、QinQ、PPPOE 等封装协议，能够适应多种不同的网络环境。 1）支持导入 HTTPS 证书，对流量进行解密和还原。须提供 HTTPS 证书功能截图 2）支持常见应用的识别不低于 3000 种 3）支持流量白名单，过滤掉不关注资产流量，白名单类型应包括 IP、端口、邮箱、域名。（提供功能截图并加盖厂商公章） 4）支持自定义 TCP/UDP 端口扫描检测模型，结合模型对流量进行检测和告警。	要求与负载均衡、数据库审计异构，不得同一品牌

					5）支持自定义 TCP 端口扫描检测模型，支持配置参数包括检测阈值、检测周期、复位时间，提供默认配置。检测产生的告警信息至少包括扫描类型和扫描事件名称。（提供功能截图并加盖厂商公章） 6）支持自定义 UDP 端口扫描检测模型，支持配置参数包括检测阈值、检测周期、复位时间，提供默认配置。检测产生的告警信息至少包括扫描类型和扫描事件名称。（提供功能截图并加盖厂商公章） 7）内置 WEB 应用机器学习检测模型，支持对 sqli，xss，exec，phprce，ptravel 和 jeli 攻击类型进行分类检测和告警，告警信息至少包括机器学习告警类型和威胁事件名称。（提供功能截图并加盖厂商公章） 8）WEB 类告警详情中包含请求和响应信息，在请求和响应信息中能标记规则匹配中的字段信息，便于运维人员快速进行确认攻击事件。（提供功能截图并加盖厂商公章） 9）支持 WEB 类的攻击结果进行判定 10）内置恶意文件检测引擎，支持对可执行文件、文档、压缩包和网页脚本进行恶意代码检测和告警，告警信息中至少包含恶意文件类型、恶意文件家族信息和恶意文件变种信息。（提供功能截图并加盖厂商公章） 支持与威胁情报联动，可进行实时流量匹配检测和告警，支持对恶意 IP、恶意域名、恶意 URL 和恶意文件进行检测。（提供功能截图并加盖厂商公章） 11）内置基于统计学特征和操作码序列训练的检测模型，支持对 asp、jsp、php 文件类型进行检测和告警 12）内置基于 webshell 通信特点以及流量特征构建决策模型，支持对 asp 文件、php 文件、jsp 文件和图片马进行检测和告警 13）支持自定义 TCP/UDP 行为检测模型，通过自定义内部资产对流量中的异常行为（包括内部向外部发起、内部对内部发起）进行检测和告警，告警信息包含检测类型和威胁事件名称。须提供告警截图(包含告警类型和威胁事件名称) 14）支持自定义 TCP 行为模型，配置参数至少包括检测阈值、检测周期、复位时间、IP 对象。（提供功能截图并加盖厂商公章） 15）支持自定义 UDP 行为模型，配置参数至少包括检测阈值、检测周期、复位时间、IP 对象。（提供功能截图并加盖厂商公章） 16）支持展示威胁告警信息，展示的告警分类包括入侵检测告警、WEB 应用告警、恶意文件告警、威胁情报告警。 17）入侵检测告警字段至少包括：告警时间、攻击 IP、攻击端口、受害 IP、受害端口、告警类型、事件名称、威胁等级、详情。 18）WEB 应用告警字段至少包括：告警时间、攻击 IP、攻击端口、受害 IP、受害端口、告警类型、事件名称、URI、威胁等级、详情。 19）恶意文件告警字段至少包括：告警时间、攻击 IP、攻击端口、受害 IP、受害端口、传输协议、应用层协议、文件类型、文件名、文件 md5、详情。	

					20）威胁情报告警字段至少包括：告警时间、攻击 IP、攻击端口、受害 IP、受害端口、告警类型、事件名称、命中的威胁情报、详情。 21）应具备元数据提取、存储和检索的能力。 22）支持元数据存储和展示，元数据类型至少包括 TCP&UDP 日志、HTTP 日志、EMAIL 日志、FTP 日志、DNS 日志、ICMP 日志、文件还原日志。（提供功能截图并加盖厂商公章）和日志截图 23）支持对入侵检测告警、WEB 应用告警、威胁情报告警和恶意文件告警中的攻击 IP 和受害 IP 发送阻断报文，进行旁路阻断。（提供功能截图并加盖厂商公章） 24）支持自定义一键封堵，配置策略包括 IP 类型（配置选项包括源 ip/源端口/目的 ip/ 目的端口）、域名类型、生效时间和失效时间。（提供功能截图并加盖厂商公章） 25）支持与大数据平台联动：提供 API 接口，由大数据平台通过接口下发一键封堵断策略，探针执行封堵动作并将封堵日志信息发送给大数据平台。（提供功能截图并加盖厂商公章） 26）支持对采集的全部流量进行存储、检索和下载，检索条件包括源 IP、目的 IP、源端口、目的端口、起止时间。（提供功能截图并加盖厂商公章） 27）支持自定义规则抓取和留存可疑原始流量，自定义规则支持对原始流量的 payload 进行匹配。自定义规则内容至少包括：源 IP/源端口、目的 IP/目的端口、匹配类型（二进制、字符串、正则表达式）、匹配特征、会话数量、过期时间。须提供自定义规则配置功能截图 28）支持从流量中识别资产信息和展示，识别的信息至少包括资产 IP、资产 MAC、服务端口号、服务协议、设备类型、地理位置、操作系统、资产状态、资产描述、资产关联账号。（提供功能截图并加盖厂商公章） 29）支持配置策略的备份，备份数据至少包括全部配置、引擎参数、接口参数和白名单。（提供功能截图并加盖厂商公章） 30）支持备份策略恢复，恢复的类型包括全部配置、引擎参数配置，接口参数配置和白名单配置。（提供功能截图并加盖厂商公章） 具备二次开发能力，支持第三方通过探针的标准接口进行新的业务开发。 1）以上 31 条功能参数需逐条满足并逐条测试功能； 2）提供投标型号测试机并测试，满足所有功能方可签署合同，否则按照虚假应标进行处理。	
18	网闸	安全隔离	政务云业务区	2	标准 2U 机架式安全设备，配置冗余电源，内网接口：不少于 1 个 CONSOLE 口、6 个 10M/100M/1000M 电口（其中包含 1 个管理口、1 个 HA 口）、4 个 SFP 插槽、4 个 SFP+插槽、2 个 USB 口，管理口与业务口相互独立。外网接口：不少于 1 个 CONSOLE 口、6 个 10M/100M/1000M 电口（其中包含 1 个管理口、1 个 HA 口）、4 个 SFP 插槽、4 个 SFP+插槽、2 个 USB 口，管理口与业务口相互独立。吞吐不少于 12000Mbps；并发不少于 60 万；延时小于 1ms。	要求与漏洞扫描系统、边界防火墙异构，不得同一

					产品重点要求：内外网主机系统分别支持双系统引导，并可在 WEB 界面上直接配置启动顺序，在 A 系统发生故障时，可以随时切换到 B 系统；且支持系统(包括配置)备份； 支持多种访问控制，比如 IP 地址和端口访问控制，连续端口范围控制等；实现对多种（如 MySql、SqlServer、Oracle、DB2、Sybase）主流数据库系统的安全访问；支持 Oracle、SQL Server、Sybase、Db2、MySQL 等主流数据库；数据库同步客户端支持 Windows、Linux 等主流平台；支持 NFS、SMBFS 等文件系统；文件服务器可以是 Windows、Linux/Unix 等系统平台； 设备提供液晶面板实时显示设备工作状态及配置信息。（提供设备面板照片证明，并加盖原厂公章） 采用“2+1”系统架构，即由两个主机系统和一个隔离交换专用硬件组成；隔离交换矩阵基于专用芯片实现，保证数据在搬移的时间内，内、外网隔离卡与内、外网系统为断开状态。 ★内外网主机系统分别支持双系统引导，并可在 WEB 界面上直接配置启动顺序，在 A 系统发生故障时，可以随时切换到 B 系统；且支持系统(包括配置)备份；（提供产品功能界面截图证明，并加盖原厂公章） 支持接口冗余模式设置包括：轮询、热备、链路聚合协议（提供产品功能界面截图证明，并加盖原厂公章） 支持纯 IPv6 网络环境，能够在纯 IPv6 网络环境下正常工作（提供《公安部计算机信息系统安全产品质量监督检验中心检测报告》或其他相关证明，并加盖原厂公章） ★支持 WEB 认证方式和专用客户端两种认证方式；（提供产品功能界面截图证明，并加盖原厂公章），对用户的客户端版本和进程进行检查，进行准入控制；（提供产品功能界面截图证明，并加盖原厂公章） 支持 NFS、SMBFS 等文件系统；文件服务器可以是 Windows、Linux/Unix 等系统平台； 支持文件传输方向可控，实现单向或双向传输； 支持文件格式特征过滤；并能提供文件类型判断工具以帮助用户识别不常见文件类型（提供产品功能界面截图证明，并加盖原厂公章） 重名策略，接收端客户端支持对重名文件的控制策略，提供“覆盖”、“丢弃”、“重命名”等重名策略。（提供产品功能界面截图证明，并加盖原厂公章） 支持 Oracle、SQL Server、Sybase、Db2、MySQL 等主流数据库；数据库同步客户端支持 Windows、Linux 等主流平台； ★支持灵活的数据库冲突处理策略，当关键字数据发生冲突时可选择：覆盖/丢弃；（提供产品功能界面截图证明，并加盖原厂公章） 支持数据容错处理，当数据同步失败时，用户可以查询、恢复、删除未能正常传输的数据。（提供产品功能界面截图证明，并加盖原厂公章） ★支持客户端与网闸间的数字证书方式的身份认证；（提供产品功能界面截图证明，并加盖原厂公章）支持数据库同步客户端的双机热备技术，为用户提供更高的冗余技术支持；（提供产品功能界面截图证明，并加盖原厂公	品牌

					章） 实现对多种（如 MySql、SqlServer、Oracle、DB2、Sybase）主流数据库系统的安全访问； 提供数据库访问用户的过滤和控制； 支持数据库 SQL 语句过滤功能。（提供产品功能界面截图证明，并加盖原厂公章） 支持用户身份认证（提供产品功能界面截图证明，并加盖原厂公章） 实现安全的 FTP 访问，支持对访问用户、访问协议命令、上传下载文件类型等访问过滤控制； 支持访问时段策略；时间可以设置为一次性或者周循环方式 支持用户身份认证（提供产品功能界面截图证明，并加盖原厂公章） 支持基于 SMTP 协议的邮件发送和 POP3 协议的邮件接收； 支持邮件主题及正文的关键字过滤，以及收件人、发件人地址黑白名单 支持对邮件附件大小进行控制；支持附件类型过滤； 邮件收发支持时段访问控制；时间段可以是一次性执行、周循环两种方式 支持用户身份认证（提供产品功能界面截图证明，并加盖原厂公章） 支持访问源地址、目的地址、目的端口的访问控制； 支持页面关键字过滤，支持 MIME 类型过滤； 支持网页下载文件类型过滤；支持 URL 过滤； 支持上网时段控制策略，时间策略可以是一次性或者周循环模式； 支持用户身份认证（提供产品功能界面截图证明，并加盖原厂公章） 支持 HTTP 请求头部大小限制（提供产品功能界面截图证明，并加盖原厂公章） 实现特定 TCP、UDP 协议的数据隔离交换，可合作定制开发针对特定协议的安全检测，实现如黑白名单控制、关键字过滤等 支持源地址、目的地址、目的端口的访问控制。 支持用户身份认证（提供产品功能界面截图证明，并加盖原厂公章） 支持 HTTP/HTTPS/FTP/SMTP/POP3 等应用协议; 支持 H323/H323_GK 等多媒体协议； 支持多种访问控制，比如 IP 地址和端口访问控制，连续端口范围控制等； 支持时间策略访问控制。 支持 SYN、UDP FLOOD 阈值设置（提供产品功能界面截图证明，并加盖原厂公章） 支持 DCS/SCADA 网络与管理网络之间的 OPC 应用数据的传输； 支持用户身份认证（提供产品功能界面截图证明，并加盖原厂公章）	

					支持视频服务器认证，有效保证非法视频服务器不能接入用户的内部网络 支持用户认证，包括口令、证书等认证方式；并支持用户在线时段控制；（提供产品功能界面截图证明，并加盖原厂公章） 内置近 30 种视频厂商协议模板，可简化配置、调试步骤（提供产品功能界面截图证明，并加盖原厂公章） 支持集群部署（提供产品功能界面截图证明，并加盖原厂公章） 支持视频功能类型过滤，包括实时点播、历史回放、录像下载、云台控制、回放控制、录像检索、设备查询等（提供产品功能界面截图证明，并加盖原厂公章） 支持视频格式过滤，包括 G.711、G.729、H.264、H.263、MP4、PS 等（提供产品功能界面截图证明，并加盖原厂公章） 业务状态监控功能，实时提供业务是否可用、连接会话、流量统计等信息（提供产品功能界面截图证明，并加盖原厂公章） 采用自有知识产权的病毒防范引擎（提供相关专利证明，并加盖原厂公章）； 采用专用国产知名病毒库。（提供相关证明，并加盖原厂公章） ★支持 HTTPS 的 Web 方式管理，实现了远程管理信息加密传输；（提供《公安部计算机信息系统安全产品质量监督检验中心检测报告》证明，并加盖原厂公章） 内/外网主机系统分别具有独立管理接口，而不是采用低安全的管理方式，如通过业务口管理或通过内网唯一管理接口完成全部管理等； 支持配置文件以加密的方式导出（提供产品功能界面截图证明，并加盖原厂公章） 通过独立的热备接口实现双机热备； 支持抢占模式；（提供产品功能界面截图证明，并加盖原厂公章） 支持配置同步；（提供产品功能界面截图证明，并加盖原厂公章） 支持主、备状态实时展示；（提供产品功能界面截图证明，并加盖原厂公章） 支持中文日志显示，并能实现内外网主机日志同步（提供产品功能界面截图证明，并加盖原厂公章） 支持 FTP 方式上传日志；（提供产品功能界面截图证明，并加盖原厂公章） 支持 SNMP v1、v2、v3 版本，并支持 trap 方式。（提供产品功能界面截图证明，并加盖原厂公章） 提供在线用户状态监控，能够对在线用户列表及在线用户时长进行统计（提供产品功能界面截图及检测报告证明，并加盖原厂公章） 所投产品须提供以下证明文件： 具备公安部《计算机信息系统安全专用产品销售许可证》（网络隔离-增强级）； 具备《公安部计算机信息系统安全产品质量监督检验中心检测报告》（网络隔离-增强级）；	

					具备保密局《涉密信息系统产品检测证书》； 具有国家版权局颁发给产品的《计算机软件著作权登记证书》； 具备《中国国家信息安全产品认证证书》（3C）二级； 具备公安部安全与警用电子产品质量监测中心出具的 GB28181 测试报告,并能提供报告；	
备注					以上产品中具备特征库升级的产品须提供免费三年特征库升级服务。 厂商必须自主研发，有自己产品线及研发部门，非 OEM 贴牌产品，提供著作权和承诺函。 包含三年硬件质保服务及相关软件升级服务； 设备支持接入伊犁电子政务外网现有的安全集中管理平台。	

第6章　评标方法和标准

本项目将按照招标文件第一章投标人须知中“五 开标及评标”、“六 确定中标”及本章的规定评标。

序号	评审项目	标准分	评分标准
经济部分评分 30 分			
1	投标报价	30 分	1.投标报价超过采购预算的，投标无效，未超过采购预算的投标报价按以下公式进行计算 报价得分=(评标基准价/报价) × 30 % × 100 采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格为满分(保留小数点后两位) 2.如果在评标过程中，评标委员会发现投标人的报价明显低于其他投标人的报价或者明显低于上限价的有理由怀疑其投标报价可能低于其成本的，应当要求该投标人做出书面说明并提供相关证明材料。投标人不能合理说明或者不能提供相关证明材料的，评标委员会将视作该投标人以低于成本报价投标，经评标委员会小组认为无效的投标报价，经济标按零分计。
技术部分评分 50 分			
1	技术参数响应	25	1、所投产品配置需符合招标文件要求。配置不详，数不清，缺漏项的，每处扣 1 分，扣完为止。 2、★技术参数有负偏离的，一项扣除 2 分，扣完为高 25 分，最低 0 分。

2	重要技术方案功能设计满足响应	14	以下重要技术功能，需要投标人提供相关举证资料，未提供或不满足一项扣除对应分数；最高 14 分，最低 0 分。 1.边界防火墙需支持安全运营中心功能，可以对所有的服务器主机威胁进行全面评估，发现本地安全事件后，支持冻结终端网络访问权限，向终端推送病毒查杀通知，以免病毒大面积扩散，影响更多主机。可自定义设置通知页面时间，页面需支持定制。（提供视频演示或证明材料）得 **3** 分。 2.为了避免出现安全短板，上网行为管理设备需能够与杀毒软件产品实现联动，当检测到终端未安装杀毒软件时，禁止访问网络并提示需要安装杀毒终端软件；（提供证明材料）；得 **3** 分。 3、为保障入侵防御能力，网络入侵防御系统的系统攻击特征库规则数量大于 9000 条得 **3** 分，7000 条至 9000 条之间得 1 分，不足 7000 条不得分。 4、为保障漏洞发现能力，漏洞扫描系统的漏洞知识库信息数量大于 20 万条得 **3** 分，18 万至 20 万条之间得 1 分，不足 18 万条不得分。 5.网闸产品具备公安部安全与警用电子产品质量监测中心出具的 GB28181 测试报告，并能提供报告；得 **2** 分。
3	产品培训	2	投标人须提供详细、完整的产品培训方案，质量优得 2 分，较差或未提供不得分。
4	方案合理性	6	投标人须提供详细的技术设计方案，方案需满足采购人实际需求，并且体现原有业务系统进行兼容和对接。技术方案质量优得 4-6 分，一般得 1-3 分，方案不符合采购人需求或者无法结合实际业务，不得分。

5	售后服务承诺及方案	3	为保证售后服务响应及时性，提供 7*24 小时售后服务，并提供本地化服务，满足以下要求: 1.厂商或投标代理商需提供所购设备的安装、调试及培训，需出具售后服务承诺函。 2.投标人须提供完整的售后服务方案,包含售后服务体系介绍、技术服务与支持内容、应急响应机制等。 以上均出具，专家评价为优得 3 分，一般得 1-2 分，差或者未提供不得分。
商务部分评分 20 分			
1	投标人商业信誉	6	投标人需提供 2019 年以来类似项目的验收综合评价，每提供一项证明材料且评价良好以上得 2 分，此项最高得 6 分（未提供盖章的证明材料不得分）
2	制造商授权书	6	带*标志的产品提供制造商授权书，每提供一项厂家授权书的 1.5 分，满分 6 分。（授权书需制造商加盖鲜章，否则不得分）
3	投标人履约能力	2	根据投标人经营管理水平高低,需从企业内部规程管理制度、人员管理制度、财务管理制度等方面横向进行比较，评为优得 2 分，评为一般得 1 分，评为差不得分
4	投标人类似项目业绩	4	投标人自 2019 年起，每提供 1 个类似项目业绩的得 1 分，本项最多得 4 分（须提供加盖投标人鲜章的项目合同和验收报告证明材料复印件）
5	标函质量	2	标书质量及是否响应招标文件
合　计		100 分	

注：1.根据《政府采购促进中小企业发展暂行办法》（财库[2011]181号）、《财政部 司法部关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68号）和《三部门联合发布关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）的规定，对满足价格扣除条件且在投标文件中提交了《投标人企业类型声明函》、《残疾人福利性单位声明函》或省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件的投标人，其投标报价扣除 6 %后参与评审。对于同时属于小微企业、监狱企业或残疾人福利性单位的，不重复进行投标报价扣除。

2.联合协议中约定，小型、微型企业和监狱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，可给予联合体 6 %的价格扣除。

联合体各方均为小型、微型企业和监狱企业的，联合体视同为小型、微型企业和监狱企业。

3.投标人所投产品如被列入财政部与国家主管部门颁发的节能产品目录或环境标志产品目录或无线局域网产品目录，应提供相关证明，在评标时予以优先采购，具体优惠措施为：（节能清单部分产品的价格/投标报价）×3%×价格项满分值

4.如采购人所采购产品为政府强制采购的节能产品，投标人所投产品的品牌及型号必须为清单中有效期内产品并提供证明文件，否则其投标将被认定为**投标无效**。

5.对创新产品或创新性企业的优惠措施为： /

6.同品牌处理办法：

如采用综合评标法，则： 评审后得分最高的同品牌投标人获得第一的中标候选人。

7.中标候选人并列式时的处理方式：

如采用综合评标法，则：得分相同的，按投标报价由低到高顺序排列。得分且投标报价相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

一、商务符合性审查表

审查事项		投标人名称及审查情况		
招标文件条款（投标人须知、投标人须知资料表条款号）	**本项目要求**			
中小企业投标要求（1.3.6）	本项目*不适用*			
联合体投标规定（1.4）	本项目*不接受*联合体投标			
投标人的关联性（1.5）	在同一标包内，单位负责人为非同一人或者不存在直接控股、管理关系的不同供应商。			
未发现影响采购人决策行为（1.5）	投标人在投标过程中未向采购人提供、给予任何有价值的物品，影响其正常决策行为。			
满足投标范围的完整性要求（8.1）	投标人对所投分包招标文件中所列的所有内容进行投标。			
未包含价格调整要求（11.4）	投标人所报的各分项投标报价在合同履行过程中是固定不变的，不得以任何理由予以变更。			
投标保证金（12.1）	符合招标文件要求			
投标有效期满足要求（13.1）	自提交投标文件截止之日起 30 日历日内			
投标文件的装订方式（14.3）	所有投标文件采用不可拆装的胶订方式装订			
投标文件的签署和盖章符合要求（14.2、14.4）	按照招标文件规定要求签署、盖章。			
接受价格的算术修正（20.3）	投标文件报价出现前后不一致的，应按照招标文件规定的顺序修正。修正后的报价经投标人确认后产生约束力。			

符合强制采购节能产品要求（20.6）	本项目*不适用*			
未发现串通投标（22.2）	未与其他投标人串通投标，或者与招标人串通投标。			
报价说明可以接受（22.2）	投标人的报价明显低于其他通过符合性检查投标人的报价，有可能影响履约的，投标人能按照规定证明其报价合理性。			
无采购人不能接受的附加条件（22.2）	投标文件未含有采购人不能接受的附加条件。			
结论				

第三册

第7章 政府采购合同

请参照货物类政府采购合同参考范本订立采购合同。