内蒙古中涛工程项目管理有限公司

公 开 招 标 文 件

项目名称：内蒙古自治区教育招生考试中心采购网络安全设备、网络设备、安全及密码设备

项目编号：NMGZCS-G-H-220922

2022年11月

第一章 投标邀请

内蒙古中涛工程项目管理有限公司受内蒙古自治区教育招生考试中心委托，采用公开招标方式组织采购网络安全设备、网络设备、安全及密码设备。欢迎符合资格条件的投标人参加投标。

一.项目概述

1.名称与编号

项目名称：网络安全设备、网络设备、安全及密码设备

批准文件编号：项目流水号[2022]23765号

招标文件编号：NMGZCS-G-H-220922

2.内容及分包情况（技术规格、参数及要求）

包号	货物、服务和工程名称	采购需求	预算金额（元）
1	网络安全设备	详见招标文件	2,600,000.00
2	安全及密码设备	详见招标文件	2,990,000.00
3	网络设备	详见招标文件	1,080,000.00

二.投标人的资格要求

1. 投标人应符合《中华人民共和国政府采购法》第二十二条规定的条件。

2.到提交投标文件的截止时间，投标人未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。（以通过查询“信用中国”网站和“中国政府采购网”网站的信用记录内容为准。）

3. 其他资质要求：

合同包1（网络安全设备）：无

合同包2（安全及密码设备）：无

合同包3（网络设备）：无

三.获取招标文件的时间、地点、方式

获取招标文件的期限：详见招标公告；

获取招标文件的地点：详见招标公告；

获取招标文件的方式：投标人可从内蒙古自治区政府采购网查阅采购信息、预览招标文件。登录内蒙古自治区政府采购网获取招标文件。

其他要求：

本项目采用“不见面开标”模式进行开标（投标人无需到达开标现场，开标当日在投标截止时间前登录“内蒙古自治区政府采购网--政府采购云平台”参加远程开标）。请投标人使用投标客户端严格按照招标文件的相关要求制作和上传电子投标文件，并按照相关要求参加开标。

四.招标文件售价

本次招标文件的售价为 无 元人民币。

五.递交投标（响应）文件截止时间、开标时间及地点

递交投标（响应）文件截止时间：详见招标公告

投标地点：详见招标公告

开标时间：详见招标公告

开标地点：详见招标公告

六.联系方式

采购代理机构名称：内蒙古中涛工程项目管理有限公司

地址： 内蒙古自治区呼和浩特市新城区兴安南路5号兴业成大厦12楼

邮政编码：010010

联系人： 内蒙古中涛工程项目管理有限公司

联系电话： 0471-4216299

账户名称：系统自动生成的缴交账户名称

开户行：详见投标人须知

账号：详见投标人须知

采购单位名称：内蒙古自治区教育招生考试中心

地址： 呼和浩特市赛罕区乌兰察布东街甲81号

邮政编码：

联系人： 李老师
联系电话： 0471-3261710

内蒙古中涛工程项目管理有限公司

第二章 投标人须知

一.前附表

序号	条款名称	内容及要求
1	分包情况	共3包
2	采购方式	公开招标
3	开标方式	不见面开标
4	评标方式	现场网上评标
5	评标办法	合同包1（网络安全设备）：综合评分法 合同包2（安全及密码设备）：综合评分法 合同包3（网络设备）：综合评分法
6	获取招标文件时间（同招标文件提供期限）	详见招标公告
7	保证金缴纳截止时间（同递交投标文件截止时间）	详见招标公告
8	电子投标文件递交	电子投标文件在投标截止时间前递交至内蒙古自治区政府采购网--政府采购云平台
9	投标文件数量	（1）加密的电子投标文件 1 份（需在投标截止时间前上传至“内蒙古自治区政府采购网--政府采购云平台”） 份。
10	中标人确定	采购人按照评审报告中推荐的成交候选人确定中标（成交）人。
11	备选方案	不允许
12	联合体投标	包1： 不接受 包2： 不接受 包3： 不接受
13	采购机构代理费用	收取
14	代理费用收取方式	向中标/成交供应商收取

15	投标保证金	本招标项目支持“电子保函”和“虚拟子账户”俩种方式收取投标保证金，请投标人按照本招标文件的相关要求进行缴纳投标保证金或者开具电子保函。 同时，本项目允许投标人按照相关法律法规自主选择以支票、汇票、本票、保函等非现金形式缴纳保证金。选择非“虚拟子账户”进行保证金缴纳的，投标人应当在投标文件中附相关证明材料，同时在开标现场提供证明材料原件。 备注：**若本项目采用远程不见面开标，请将相关证明材料原件扫描添加至响应文件中。** 网络安全设备：保证金人民币：52,000.00元整。 安全及密码设备：保证金人民币：59,800.00元整。 网络设备：保证金人民币：21,600.00元整。 开户单位：系统自动生成的缴交账户名称。 开户银行：投标人在内蒙古自治区政府采购网--政府采购云平台获取招标文件后，根据其提示自行选择要缴纳的投标保证金银行。 银行账号： 内蒙古自治区政府采购网根据投标人选择的投标保证金银行，以合同包为单位，自动生成投标人所投合同包的缴纳银行账号（即多个合同包将对应生成多个缴纳账号）。投标人应按照所投合同包的投标保证金要求，缴纳相应的投标保证金。 特别提示： 1、投标人应认真核对账户信息，将投标保证金足额汇入以上账户，并自行承担因汇错投标保证金而产生的一切后果。 2、投标人在转账或电汇的凭证上应按照以下格式注明，以便核对：“（招标编号：***、合同包：***）的投标保证金”。

16	电子招投标	各投标人应当在投标截止时间前上传加密的电子投标文件至“内蒙古自治区政府采购网”未在投标截止时间前上传电子投标文件的，视为自动放弃投标。投标人因系统或网络问题无法上传电子投标文件时，请在工作时间及时拨打联系电话400-0471-010。 不见面开标（远程开标）： 1．项目采用不见面开标（网上开标），如在开标过程中出现意外情况导致无法继续进行电子开标时，将会由开标负责人视情况来决定是否允许投标人导入非加密电子投标文件继续开标。本项目采用电子评标（网上评标），只对通过开标环节验证的电子投标文件进行评审。 2．电子投标文件是指通过投标客户端编制，在电子投标文件中，涉及“加盖公章”的内容应使用单位电子公章完成。加密后，成功上传至内蒙古自治区政府采购网的最终版指定格式电子投标文件。 3．使用投标客户端，经过编制、签章，在生成加密投标文件时，会同时生成非加密投标文件，投标人请自行留存。 4．投标人的法定代表人或其授权代表应当按照本招标公告载明的时间和模式等要求参加开标，在开标时间前30分钟，应当提前登录开标系统进行签到，填写联系人姓名与联系号码。 5．开标时，投标人应当使用 CA 证书在开始解密后30分钟内完成投标文件在线解密，若出现系统异常情况，工作人员可适当延长解密时长。（请各投标人在参加开标以前自行对使用电脑的网络环境、驱动安装、客户端安装以及CA证书的有效性等进行检测，保证可以正常使用。具体环境要求详见操作手册（内蒙古自治区政府采购网--政采业务指南）） 6．开标时出现下列情况的，将视为逾期送达或者未按照招标文件要求密封的投标文件，采购人、采购代理机构应当视为投标无效处理。 （1） 投标人未按招标文件要求参加远程开标会的； （2） 投标人未在规定时间内完成电子投标文件在线解密； （3） 经检查数字证书无效的投标文件； （4） 投标人自身原因造成电子投标文件未能解密的。 7．投标人必须保证在规定时间内完成项目已投标标段的电子投标文件解密。
17	电子投标文件签字、盖章要求	应按照第七章“投标文件格式”要求，使用单位电子签章（CA）进行签字、加盖公章。 说明：若涉及到授权代表签字的可将文件签字页先进行签字、扫描后导入加密电子投标文件。
18	投标客户端	投标客户端需要自行登录“内蒙古自治区政府采购网--政府采购云平台”下载。
19	是否专门面向中小企业采购	采购包1：非专门面向中小企业 采购包2：非专门面向中小企业 采购包3：非专门面向中小企业

20	有效供应商家数	包1：3 此数约定了开标与评标过程中的最低有效供应商家数，当家数不足时项目将不得开标、评标或直接废标；文件中其他描述若与此规定矛盾以此为准。 包2：3 此数约定了开标与评标过程中的最低有效供应商家数，当家数不足时项目将不得开标、评标或直接废标；文件中其他描述若与此规定矛盾以此为准。 包3：3 此数约定了开标与评标过程中的最低有效供应商家数，当家数不足时项目将不得开标、评标或直接废标；文件中其他描述若与此规定矛盾以此为准。
21	报价形式	合同包1（网络安全设备）:总价 合同包2（安全及密码设备）:总价 合同包3（网络设备）:总价
22	项目兼投兼中规则	兼投兼中：本项目兼投兼中。
23	现场踏勘	否
24	其他	

二.投标须知

1.投标方式

1.1投标方式采用网上投标，流程如下：

投标人须在内蒙古自治区政府采购网（http://www.ccgp-neimenggu.gov.cn）投标人库填写相关信息后才可进行网上投标操作。所需资料及办理流程请登录“内蒙古自治区政府采购网”进行查询。

登录内蒙古自治区政府采购网门户网站（ http://www.ccgp-neimenggu.gov.cn ）页面，点击“政府采购云平台”，输入登录“账号”、“密码”、“验证码”；登录完成点击右边“执行交易”进入网上投标页面，点击“应标”二级菜单“项目投标”从待投标列表中选择投标项目，进入投标页面选择右侧对应的，要投标的包号填写“联系人”、“联系人联系号码”等信息点击“确认投标”按钮。

通过内蒙古自治区政府采购网（http://www.ccgp-neimenggu.gov.cn）获取所投项目招标文件，并按照本招标文件的要求制作、上传电子投标文件。

同时，满足本招标文件关于投标的其他要求后，方可完成投标。

1.2缴纳投标保证金（如有）。本采购项目支持“电子保函”和“虚拟子账户”俩种方式收取投标保证金。涉及“虚拟子账户”方式收取保证金的，每一个投标人在所投的每一项目下合同包会对应每一家银行自动生成一个账号，称为“虚拟子账号”。在进行投标信息确认后，应通过应标管理-已投标的项目，选择缴纳银行并获取对应不同包的缴纳金额以及虚拟子账号信息，并在开标时间前，通过转账至上述账号中，付款人名称必须为投标单位全称且与投标信息一致。
若出现账号缴纳不一致、缴纳金额与投标人须知前附表规定的金额不一致或缴纳时间超过开标时间，将导致保证金缴纳失败。涉及“电子保函”方式收取保证金的，每一个投标人在所投的每一项目下合同包选择电子保函模式，跳转到内蒙古自治区金融服务平台开具电子保函，投标人需要确保在开标之前完成电子保函的开具。

1.3查看投标状况。通过应标管理-已投标的项目可查看已投标项目信息。

2.特别提示：

2.1缴纳保证金时间以保证金到账时间为准，由于投标保证金到账需要一定时间，请投标人在投标截止前及早缴纳。

三.说明

1.总则

本招标文件依据《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《政府采购货物和服务招标投标管理办法》（财政部令第87号）及国家和自治区有关法律、法规、规章制度编制。

投标人应仔细阅读本项目信息公告及招标文件的所有内容（包括变更、补充、澄清以及修改等，且均为招标文件的组成部分），按照招标文件要求以及格式编制投标文件，并保证其真实性，否则一切后果自负。

本次公开招标项目，是以招标公告的方式邀请非特定的投标人参加投标。

2.适用范围

本招标文件仅适用于本次招标公告中所涉及的项目和内容。

3.投标费用

投标人应承担所有与准备和参加投标有关的费用。不论投标结果如何，采购代理机构和采购人均无义务和责任承担相关费用。

4.当事人

4.1“采购人”是指依法进行政府采购的国家机关、事业单位、团体组织。本招标文件的采购人特指本项目采购单位。

4.2“采购代理机构”是指本次招标采购项目活动组织方。本招标文件的采购代理机构特指内蒙古中涛工程项目管理有限公司。

4.3“投标人”是指向采购人提供货物、工程或者服务的法人、其他组织或者自然人。

4.4“评标委员会”是指根据《中华人民共和国政府采购法》等法律法规规定，由采购人代表和有关专家组成以确定中标人或者推荐中标候选人的临时组织。

4.5“中标人”是指经评标委员会评审确定的对招标文件做出实质性响应，取得与采购人签订合同资格的投标人。

5.合格的投标人

5.1 符合本招标文件规定的资格要求，并按照要求提供相关证明材料。

5.2单位负责人为同一人或者存在直接控股、管理关系的不同投标人，不得参加同一合同项下的政府采购活动。

5.3为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的投标人，不得再参加该采购项目的其他采购活动。

6.以联合体形式投标的，应符合以下规定：

6.1联合体各方应签订联合体协议书，明确联合体牵头人和各方权利义务，并作为投标文件组成分部分。

6.2联合体各方均应当具备政府采购法第二十二条规定的条件，并在投标文件中提供联合体各方的相关证明材料。

6.3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。

6.4联合体各方中至少应当有一方符合采购人规定的资格要求。由同一资质条件的投标人组成的联合体，应当按照资质等级较低的投标人确定联合体资质等级。

6.5联合体各方不得再以自己名义单独在同一项目中投标，也不得组成新的联合体参加同一项目投标。

6.6联合体各方应当共同与采购人签订采购合同，就合同约定的事项对采购人承担连带责任。

6.7 投标时，应以联合体协议中确定的主体方名义投标，以主体方名义缴纳投标保证金，对联合体各方均具有约束力。

7.语言文字以及度量衡单位

7.1所有文件使用的语言文字为简体中文。专用术语使用外文的，应附有简体中文注释，否则视为无效。

7.2所有计量均采用中国法定的计量单位。

7.3所有报价一律使用人民币，货币单位：元。

8. 现场踏勘

8.1招标文件规定组织踏勘现场的，采购人按招标文件规定的时间、地点组织投标人踏勘项目现场。

8.2投标人自行承担踏勘现场发生的责任、风险和自身费用。

8.3采购人在踏勘现场中介绍的资料和数据等，不构成对招标文件的修改或不作为投标人编制投标文件的依据。

9.其他条款

无论中标与否投标人递交的投标文件均不予退还。

四.招标文件的澄清或者修改

采购人或采购代理机构对已发出的招标文件进行必要的澄清或修改的，澄清或者修改的内容可能影响投标文件编制的，采购人或者采购代理机构应当在投标截止时间15日前，不足15日的，顺延投标截止之日，在“内蒙古自治区政府采购网”上发布澄清或者变更公告进行通知。澄清或者变更公告的内容为招标文件的组成部分，投标人应自行上网查询，采购人或采购代理机构不承担投标人未及时关注相关信息的责任。

五.投标文件

1.投标文件的构成

投标文件应按照招标文件第七章“投标文件格式”进行编写（可以增加附页），作为投标文件的组成部分。

2.投标报价

2.1 投标人应按照“第四章招标内容与要求”的需求内容、责任范围以及合同条款进行报价。并按“开标一览表”和“分项报价明细表”规定的格式报出总价和分项价格。投标总价中不得包含招标文件要求以外的内容，否则，在评审时不予核减。

2.2 投标报价包括本项目采购需求和投入使用的所有费用，如主件、标准附件、备品备件、施工、服务、专用工具、安装、调试、检验、培训、运输、保险、税款等。

2.3 投标报价不得有选择性报价和附有条件的报价。

2.4 对报价的计算错误按以下原则修正：

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

（2）大写金额和小写金额不一致的，以大写金额为准；

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

注：修正后的报价投标人应当采用书面形式，并加盖公章，或者由法定代表人或其授权的代表签字确认后产生约束力，但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，投标人不确认的，其投标无效。

5.投标有效期

5.1投标有效期从提交投标文件的截止之日起算。投标文件中承诺的投标有效期应当不少于招标文件中载明的投标有效期。投标有效期内投标人撤销投标文件的，采购人或者采购代理机构可以不退还投标保证金。

5.2出现特殊情况需要延长投标有效期的，采购人以书面形式通知所有投标人延长投标有效期。投标人同意延长的，应相应

延长其投标保证金的有效期，但不得要求或被允许修改或撤销其投标文件；投标人拒绝延长的，其投标失效，但投标人有权收回其投标保证金。

6.投标保证金

6.1投标保证金的缴纳

投标人在提交投标文件的同时，应按投标人须知前附表规定的金额、开户银行、行号、开户单位、账号和招标文件本章“投标须知”规定的投标保证金缴纳要求递交投标保证金，并作为其投标文件的组成部分。

6.2投标保证金的退还：

（1）投标人在投标截止时间前放弃投标的，自所投合同包结果公告发出后5个工作日内退还，但因投标人自身原因导致无法及时退还的除外；

（2）未中标人投标保证金，自中标通知书发出之日起5个工作日内退还；

（3）中标人投标保证金，自政府采购合同签订之日起5个工作日内退还。

6.3有下列情形之一的，投标保证金将不予退还：

（1）中标后，无正当理由放弃中标资格；

（2）中标后，无正当理由不与采购人签订合同；

（3）在签订合同时，向采购人提出附加条件；

（4）不按照招标文件要求提交履约保证金；

（5）要求修改、补充和撤销投标文件的实质性内容；

（6）要求更改招标文件和中标结果公告的实质性内容；

（7）法律法规和招标文件规定的其他情形。

7.投标文件的修改和撤回

投标人在提交投标截止时间前，可以对所递交的投标文件进行补充、修改或者撤回。补充、修改的内容旁签署（法人或授权委托人签署）、盖章、密封和上传至系统后生效，并作为投标文件的组成部分。

在提交投标文件截止时间后到招标文件规定的投标有效期终止之前，投标人不得补充、修改、替代或者撤回其投标文件。

8.投标文件的递交

在招标文件要求提交投标文件的截止时间之后送达或上传的投标文件，为无效投标文件，采购单位或采购代理机构拒收。采购人、采购代理机构对误投或未按规定时间、地点进行投标的概不负责。

9.样品（演示）

9.1招标文件规定投标人提交样品的，样品属于投标文件的组成部分。样品的生产、运输、安装、保全等一切费用由投标人自理。

9.2开标前，投标人应将样品送达至指定地点，并按要求摆放并做好展示。若需要现场演示的，投标人应提前做好演示准备（包括演示设备）。

9.3评标结束后，中标人与采购人共同清点、检查和密封样品，由中标人送至采购人指定地点封存。未中标投标人将样品自行带回。

六.开标、评审、结果公告、中标通知书发放

1.网上开标程序

1.1主持人按下列程序进行开标：

（1）宣布开标纪律；

（2）宣布开标会议相关人员姓名；

（3）投标人对已提交的加密文件进行解密，由采购人或者采购代理机构工作人员当众宣布投标人名称、投标价格和招标文件规定的需要宣布的其他内容（以开标一览表要求为准）；

（4）参加开标会议人员对开标情况确认；

（5）开标结束，投标文件移交评标委员会。

1.2开标异议

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，应当当场提出询问或者回避申请，开标会议结束后不再接受相关询问、质疑或者回避申请。

1.3 投标人不足三家的，不得开标。

1.4备注说明：

1.4.1若本项目采用不见面开标，开标时投标人使用 CA证书参与远程投标文件解密。投标人用于解密的 CA证书应为该投标文件生成加密、上传的同一把 CA 证书。

1.4.2若本项目采用不见面开标，投标人在开标时间前30分钟，应当提前登录开标系统进行投标人信息确认，未进行确认的以报名投标人信息为准；在系统约定时间内使用 CA 证书解密，未成功解密的视为其无效投标。

1.4.3投标人对不见面开标过程和开标记录有疑义，应在开标系统规定时间内在不见面开标室提出异议，采购代理机构在网上开标系统中进行查看及回复。开标会议结束后不再接受相关询问、质疑或者回避申请。

2.评审（详见第六章）

3.结果公告

中标人确定后，采购代理机构将在内蒙古自治区政府采购网上发布中标结果公告，同时将中标结果以公告形式通知未中标的投标人，中标结果公告期为 1 个工作日。

项目废标后，采购代理机构将在内蒙古自治区政府采购网上发布废标公告，废标结果公告期为 1 个工作日。

4.中标通知书发放

发布中标结果的同时，中标人可自行登录“内蒙古自治区政府采购网--政府采购云平台”打印中标通知书，中标通知书是合

同的组成部分，中标通知书对采购人和中标投标人具有同等法律效力。

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

七.询问、质疑与投诉

1.询问

投标人对政府采购活动事项有疑问的，可以向采购人或采购代理机构提出询问，采购人或采购代理机构应当在3个工作日内做出答复，但答复的内容不得涉及商业秘密。投标人提出的询问超出采购人对采购代理机构委托授权范围的，采购代理机构应当告知其向采购人提出。

2.质疑

2.1投标人认为招标文件、采购过程和中标、成交结果使自己的权益受到损害的，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，以书面形式向采购人提出质疑。

投标人在法定质疑期内应当一次性提出针对同一采购程序环节的质疑。

提出质疑的投标人应当是参与所质疑项目采购活动的投标人。

潜在投标人已依法获取其可质疑的招标文件的，可以对该文件提出质疑。对招标文件提出质疑的，应当在获取招标文件或者招标文件公告期限届满之日起7个工作日内提出。

2.2采购人应当在收到投标人的书面质疑后七个工作日内作出答复，并以书面形式通知质疑投标人和其他有关投标人，但答复的内容不得涉及商业秘密。

2.3询问或者质疑事项可能影响中标结果的，采购人应当暂停签订合同，已经签订合同的，应当中止履行合同。

2.4 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：

（一）投标人的姓名或者名称、地址、邮编、联系人及联系电话；

（二）质疑项目的名称、编号；

（三）具体、明确的质疑事项和与质疑事项相关的请求；

（四）事实依据；

（五）必要的法律依据；

（六）提出质疑的日期。

注：对招标文件质疑的，还需提供已依法获取其可质疑的招标文件的证明材料（在投标人系统中自行截图）。

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。

投标人可以授权代表进行质疑，且应当提交投标人签署的授权委托书。其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。

2.5 投标人在提出质疑时，请严格按照相关法律法规及质疑函范本要求提出和制作，否则，自行承担相关不利后果。

对捏造事实，提供虚假材料或者以非法手段取得证明材料进行恶意质疑的，一经查实，将上报监督部门，并给以相应处罚。

2.6 接收质疑函的方式：为了使提出的质疑事项在规定时间内得到有效答复、处理，质疑可以由法定代表人或授权代表亲自将质疑函递交至采购人或采购代理机构，也可以通过邮寄、快递等方式提交。质疑函以邮寄、快递方式递交的，质疑提起日期以邮寄件上的戳记日期、邮政快递件上的戳记日期和非邮政快递件上的签注之日起计算。

联系部门：采购人、采购代理机构（详见第一章 投标邀请）。

联系电话：采购人、采购代理机构（详见第一章 投标邀请）。

通讯地址：采购人、采购代理机构（详见第一章 投标邀请）。

3.投诉

质疑人对采购人、采购代理机构的答复不满意或者采购人、采购代理机构未在规定的时间内做出书面答复的，可以在答复期满后十五个工作日内向监督部门进行投诉。投诉程序按《政府采购法》及相关规定执行。

投标人投诉的事项不得超出已质疑事项的范围。

第三章 合同与验收

一.合同要求

1.一般要求

1.1采购人应当自中标通知书发出之日起30日内，按照招标文件和中标人投标文件的规定，与中标人签订书面合同。所签订的合同不得对招标文件确定的事项和中标人投标文件作实质性修改。

合同签订双方不得提出任何不合理的要求作为签订合同的条件。

1.2政府采购合同应当包括采购人与中标人的名称和住所、标的、数量、质量、价款或者报酬、履行期限及地点和方式、验收要求、违约责任、解决争议的方法等内容。

1.3采购人与中标人应当根据合同的约定依法履行合同义务。

政府采购合同的履行、违约责任和解决争议的方法等适用《中华人民共和国民法典》。

政府采购合同的双方当事人不得擅自变更、中止或者终止合同。

1.4拒绝签订采购合同的按照相关规定处理，并承担相应法律责任。

1.5采购人应当自政府采购合同签订之日起2个工作日内，将政府采购合同在指定的媒体上公告，但政府采购合同中涉及国家秘密、商业秘密的内容除外。

采购人应当自政府采购合同签订之日起2个工作日内，将政府采购合同在省级以上人民政府财政部门指定的媒体上公告，但政府采购合同中涉及国家秘密、商业秘密的内容除外。

2. 合同格式及内容

2.1具体格式见本招标文件后附拟签订的《合同文本》（部分合同条款），投标文件中可以不提供《合同文本》。

2.2《合同文本》的内容可以根据《民法典》和合同签订双方的实际要求进行修改，但不得改变范本中的实质性内容。

二.验收

中标人在供货、工程竣工或服务结束后，采购人应及时组织验收，并按照招标文件、投标文件及合同约定填写验收单。

政府采购合同（合同文本）

甲方：*（填写采购单位）**

地址（详细地址）：

乙方：*（填写中标投标人）**

地址（详细地址）：

合同号：

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等相关法律法规，甲、乙双方就　　（填写项目名称）　　（政府采购项目编号、备案编号：　　），经平等自愿协商一致达成合同如下：

一、合同文件

本合同所附下列文件是构成本合同不可分割的部分：

1、合同格式以及合同条款

2、中标结果公告及中标通知书

3、招标文件

4、投标文件

5、变更合同

二、本合同所提供的标的物、数量及规格等详见中标结果公告及后附清单。

三、合同金额

合同金额为人民币　　万元，大写：

四、付款方式及时间

***（见招标文件第四章）

五、交货安装

交货时间：

交货地点：

六、质量

乙方提供的标的物应符合国家相关质量验收标准，且能够提供相关权威部门出具的产品质量检测报告；提供的相关服务符合国家（或行业）规定标准。

七、包装

标的物的包装应按照国家或者行业主管部门的技术规定执行，国家或业务主管部门无技术规定的，应当按双方约定采取足以保护标的物安全、完好的包装方式。

八、运输要求

（一）运输方式及线路：

（二）运输及相关费用由乙方承担。

九、知识产权

乙方应保证甲方在中国境内使用标的物或标的物的任何一部分时，免受第三方提出的侵犯其知识产权的诉讼。

十、验收

（一）乙方将标的物送达至甲方指定的地点后，由甲乙双方及第三方（如有）一同验收并签字确认。

（二）对标的物的质量问题，甲方应在发现后向乙方提出书面异议，乙方在接到书面异议后，应当在　　日内负责处理。甲方逾期提出的，对所交标的物视为符合合同的规定。如果乙方在投标文件及谈判过程中做出的书面说明及承诺中，有明确质量保证期的，适用质量保证期。

（三）经双方共同验收，标的物达不到质量或规格要求的，甲方可以拒收，并可解除合同且不承担任何法律责任，

十一、售后服务

（一）乙方应按招标文件、投标文件及乙方在谈判过程中做出的书面说明或承诺提供及时、快速、优质的售后服务。

（二）其他售后服务内容：　　（投标文件售后承诺等）

十二、违约条款

（一）乙方逾期交付标的物、甲方逾期付款，按日承担违约部分合同金额的违约金。

（二）其他违约责任以相关法律法规规定为准，无相关规定的，双方协商解决。

十三、不可抗力条款

因不可抗力致使一方不能及时或完全履行合同的，应及时通知另一方，双方互不承担责任，并在　　天内提供有关不可抗力的相关证明。合同未履行部分是否继续履行、如何履行等问题，双方协商解决。

十四、争议的解决方式

合同发生纠纷时，双方应协商解决，协商不成可以采用下列方式解决：

（一）提交　　仲裁委员会仲裁。

（二）向　　人民法院起诉。

十五、合同保存

合同文本一式五份，采购单位、投标人、政府采购监管部门、采购代理机构、国库支付执行机构各一份，自双方签订之日起生效。

十六、合同未尽事宜，双方另行签订补充协议，补充协议是合同的组成部分。

甲方：　　（章）　　乙 方：（章）

采购方法人代表：　　（签字）　　投标人法人代表：（签字）

开户银行：　　开户银行：

帐 号：　　帐 号：

联系电话：　　联系电话：

签订时间　　年　　月　　日

附表：标的物清单（主要技术指标需与投标文件相一致）（工程类的附工程量清单等）

名称	品牌、规格、标准/主要服务内容	产地	数量	单位	单价（元）	金额（元）
**	**	**	**	**	**	**
合计：人民币大写：**元整						￥：**

第四章 招标内容与技术要求

一. 项目概况 ：

网络安全设备、网络设备、安全与密码设备

合同包1（网络安全设备）

1.主要商务要求

标的提供的时间	合同签订后20个日历日内交货
标的提供的地点	采购人确定交付地点
投标有效期	从提交投标（响应）文件的截止之日起90日历天
付款方式	1期：支付比例50%，支付比例50%，结合预算资金下达情况，合同签订后，收到中标供应商支付的履约保证金及合法凭证后支付合同金额的50%. 2期：支付比例50%，产品到货验收后支付合同金额的50%
验收要求	1期：项目具备初步验收条件后，由采购单位负责组织验收工作小组进行初步验收 2期：项目具备竣工验收条件后，按照相关规定进行竣工验收
履约保证金	收取比例：10%,说明：为保证中标供应商更好地履行合同，中标供应商须向采购人交纳履约保证金，金额为中标金额的10%。履约保证金的交付时间为合同签订后3日内。验收合格正常运行后计算质保期，履约保证金在质保期满1年后的1个月内，原额退还。若中标供应商未能履行其合同规定的任何义务，采购人有权扣罚履约保证金。

其他	**质保期：**本项目质保期为3年。本项目质保期要求为投标方需承诺硬件免费提供三年的原厂质保和软件服务，特殊标注的以标注为准,质保期从项目终验后起算。在质保期内，投标人对所投产品在使用过程中出现的故障和零配件损坏问题，免费提供维修和更换服务；质保期过后，投标人将继续提供免费维修服务，在此期间不收取维护费，如需更换零配件，只收取零配件的成本费，不再收取任何其他费用。在货物的设计使用寿命期内，投标人必须保证零部件的正常供应，对所有部件终身维修服务，对货物定期维护保养，确保货物正常使用。免费安装调试、人员培训、技术支持；定期进行用户回访，及时处理用户意见；所有软件质保期内免费升级。 **售后服务及培训：**1.投标方应提供完善的售后保障服务，在质保期内如有问题投标方应提供7*24小时的应急响应，质保期过后卖方在收到用户第一个报修电话后，应立即有技术人员响应，并通过电话或邮件方式等远程技术支持进行解决，无法解决的，如需现场支持，应在3小时内抵达现场，24小时内解决，维修更换有缺陷的货物或部件，若现场不能解决，应最多不超过7日内将货物修好。在维修过程中由卖方提供一台同种工作效果的货物作为备用机，保证买方不耽误工作。如果卖方在收到通知后7日内没有弥补缺陷，买方可采取必要的补救措施，但风险和费用将由卖方承担。2.对于本次招标项目，投标方需要组织对内蒙古教育考试中心就内蒙古执行指挥互联网应急调度系统的日常使用、简单维护等方面进行专业培训。具体要求如下：（1）投标方应在投标文件中给出详细的培训方案；（2）培训人应拥有从业相关经验，提供培训人的详细背景资料；（3）投标方应提供中文培训资料；（4）如培训未达到预期效果，培训时间进行延长；（5）培训地点为招标方指定地点；（6）培训所需费用由投标方承担；（7）培训时间由内蒙古自治区考试中心按照项目进展情况指定，原则不超过20天。

2.技术标准与要求

序号	核心产品（“△”）	品目名称	标的名称	单位	数量	分项预算单价（元）	分项预算总价（元）	面向对象情况	所属行业	招标技术要求
1		防火墙	防火墙	台	4.00	200,000.00	800,000.00	否	其他未列明行业	详见附表一
2		防火墙	防火墙	台	2.00	400,000.00	800,000.00	否	其他未列明行业	详见附表二
3		入侵检测设备	入侵检测	台	3.00	200,000.00	600,000.00	否	其他未列明行业	详见附表三
4		入侵防御设备	入侵防御	台	2.00	200,000.00	400,000.00	否	其他未列明行业	详见附表四

附表一：防火墙　是否允许进口：否

<table>
<tr><td>参数性质</td><td>序号</td><td>具体技术(参数)要求</td></tr>
<tr><td></td><td></td><td>防火墙-20G
<table>
<tr><th>序号</th><th>参数性质</th><th>技术指标</th><th>技术规格要求</th></tr>
<tr><td>1</td><td>√</td><td rowspan="2">硬件规格</td><td>标准2U设备，双电源；</td></tr>
<tr><td>2</td><td>√</td><td>≥6个10/100/1000MBase-TX，≥4个SPF接口，4个SPF+接口，≥1个接口扩展槽。</td></tr>
<tr><td></td><td></td><td></td><td>实际网络层处理能力≥20Gbps 防病毒处理能力≥8G</td></tr>
</table></td></tr>
</table>

		3	√	性能要求	实际网络层处理能力≥20Gbps,防病毒处理能力≥8Gbps，吞吐量不低于80Gbps；并发连接数至少800万；新建连接数至少20万/s
		4	√	工作模式	支持路由、透明、旁路、混合工作模式
		5	0	网络特性	支持静态路由、RIP、RIPng、OSPFv2、OSPFv3、BGP、ISP路由；
		6	0		内置移动、联通、电信、教育网、网通、长城宽带等ISP服务商地址列表；
		7	0		内置世界各国ISP地址库；需提供功能截图并加盖公章。
		8	0		支持802.1q，支持stp；
		9	0		支持根据入接口、源/目的IP地址、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； 支持不少于8种的选路算法；需提供功能截图并加盖公章。
		10	0		支持手动和LACP链路聚合，可根据源/目的mac、目的IP、等条件提供不少于2种链路负载算法；需提供功能截图并加盖公章。
		11	0		支持IPv4/v6双栈；需提供功能截图并加盖公章。；
		12	0		IP/MAC静态和动态探测绑定；
		13	0		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StickyNAT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；需提供功能截图并加盖公章。
		14	0		支持NAT64,NAT46支持静态转换和前缀转换方式；需提供功能截图并加盖公章。
		15	0		支持NAT66地址转换，支持源地址转换，目的地址转换，静态地址转换；
		16	0		支持NAT源端口复用，单个公网IP支持的并发会话数量无限制；
		17	0		支持SNAT源端口保持功能；
		18	0		支持NAT策略冲突检测；
		19	0		支持NAT地址池利用率告警；
		20	0		支持DNSDoctoring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DNSDoctoring，实现内网资源服务器的负载均衡；需提供功能截图并加盖公章。
		21	0		支持各种应用协议的NAT穿越：FTP、TFTP、H.323、SQL*NET；
		22	0		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；

			23	0		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；需提供功能截图并加盖公章。
			24	0		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；需提供功能截图并加盖公章。
			25	0	无线接入	支持802.11n无线接入，可支持2.4G频段或5G频段；
			26	0		支持LTE-FDD/WCDMA/TD-SCDMA/GSM/EMBB等移动网络制式；
			27	0	访问控制	支持Web认证，在策略中可设置用户Web认证的门户地址；需提供功能截图并加盖公章。
			28	0		支持基于策略的流量统计和会话统计；
			29	0		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；需提供功能截图并加盖公章。
			30	0		支持策略加速技术，减少策略对设备性能的消耗；需提供功能截图并加盖公章。
			31	0		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；需提供功能截图并加盖公章。
			32	0		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、策略命中数等条件进行细粒度查询；需提供功能截图并加盖公章。
			33	0		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；需提供功能截图并加盖公章。
			34	0	IPv6安全防护	支持基于IPv6的入侵防御、病毒防御、DDOS、WEB防护、防御等一系列安全防护功能；需提供功能截图并加盖公章。
			35	0		支持基于IPv6的流量控制、连接限制；需提供功能截图并加盖公章。
			36	0	入侵防御	支持独立的入侵防护规则特征库，特征总数在7000条以上，能对常见漏洞进行安全防护；需提供功能截图并加盖公章。
			37	0		规则库支持根据攻击类型、风险等级、流行程度等进行分类，防护动作包括告警、阻断；需提供功能截图并加盖公章。
			38	0		支持针对地址设置入侵防御白名单，支持攻击规则搜

			38	0		索以及自定义；需提供功能截图并加盖公章。
			39	0	DDOS防御	支持针对ICMP、TCP、UDP、等协议进行DDOS防护；支持预定义和自定义策略模板；
			40	0	病毒过滤	支持对HTTP/SMTP/POP3/FTP/IMAP等协议进行病毒防御；需提供功能截图并加盖公章。
			41	0		病毒特征库规模超过1200万；需提供功能截图并加盖公章。
			42	0	Web防护	支持对100个站点制订web应用防护策略，支持http请求回应的头、体检查；
			43	0		支持自定义web安全防护事件，可以对请求参数、各个头域、内容关键字、文件类型等进行灵活组合生成策略；需提供功能截图并加盖公章。
			44	0		支持对http的合规性检查，包括版本、方法、url、头域字段、传输文件等的合规性检查；需提供功能截图并加盖公章。
			45	0		内置web应用防护特征库，提供定期升级
			46	0	弱口令检查	支持对HTTP、telnet、FTP、SMTP、POP3等各种协议进行弱口令检查，并上报安全事件；需提供功能截图并加盖公章。
			47	0		支持高、中、低三种密码检查强度；
			48	0		支持对源目的ip地址进行过滤检查；
			49	0	黑名单	可设置基于IP过滤条件，实现对特定报文进行快速过滤，支持100万以上黑名单数量；需提供功能截图并加盖公章。
			50	0		内置动态黑名单功能，可与URL过滤、病毒过滤功能实现联动封锁；支持静态和动态黑名单命中统计和监控；支持黑名单添加事件和生效时间展示；需提供功能截图并加盖公章。
			51	0		支持黑名单多种类型导入，如通过文件上传增量添加黑名单、支持页面复制粘贴方式添加黑名单、支持API接口下发黑名单；需提供功能截图并加盖公章。
			52	0		支持按照ip/ip网段模糊检索；
			53	0		黑名单列表支持展示添加时间、添加方式（手工或来自其他安全事件）、命中次数。并支持按照命中次数排序；
			54	0	应用控制/	支持IPv6的应用控制策略；
			55	0		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2000种；
			56	0		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；
			57	0		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

					URL过滤	；需提供功能截图并加盖公章。
			58	0		URL分类库规模不少于2000万条；需提供功能截图并加盖公章。
			59	0		内置P2P应用、网页应用、数据库应用等应用特征库；需提供功能截图并加盖公章。
			60	0		支持超过100类、2000万的URL地址分类库，用户可根据网站类别对自身网络的WEB应用实施全面化管控，杜绝非法、违规网站的访问行为；
	1		61	0	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；需提供功能截图并加盖公章。
			62	0		支持带宽限制、带宽保障和弹性带宽；
			63	0		支持高、中、低优先级通道设置；
			64	0	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；需提供功能截图并加盖公章。
			65	0	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；
			66	0		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；
			67	0		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；
			68	0		支持双路HA物理心跳线，确保HA运行稳定可靠；
			69	0		支持IPv6下的HA环境；
			70	0	用户管控	内置用户身份管理系统，支持本地认证、外部认证及等方式，支持RADIUS、LDAP等第三方外部认证；
			71	0		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、首次登陆修改密码、密码定期修改、密码有效时间等设置；
			72	0		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；需提供功能截图并加盖公章。
			73	0		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；需提供功能截图并加盖公章。
			74	0	IPSECVPN	支持IPSecVPN功能，支持IKEV1、IKEV2、国密的加密类型，支持AES、DES、3DES、MD5、SHA-1、SM3等VPN加密、认证算法，支持对隧道内网络流量进行监控展示；需提供功能截图并加盖公章。
			75	0		无需额外授权，IPSecVPN用户数无限制；

76	0		支持硬件国密加速卡
77	0	SSLVPN	支持SSLVPN功能，满足远程用户安全接入内网；
78	0		无需额外授权，SSLVPN用户数无限制；
79	0		SSLVPN支持代理模式，能够直接代理内网页面到VPN用户登录页面；
80	0		SSLVPN支持隧道模式，可添加多条路由，满足多网段内网的访问需求；
81	0		SSLvpn支持BBR加速，在高延时、丢包等不良网络条件下，可以提升传输效率3-5倍以上
82	0		SSLVPN登录支持双因子认证；
83	0	系统管理	支持Web管理界面，HTTP和HTTPS方式；
84	0		支持中文及英文WEB界面，并可一键切换； 支持多种语言（不少于2种，至少包含英语、俄语）web页面
85	0		支持命令行方式管理，所有功能均可通过命令行实现，支持TELNET、SSH及串口方式进行命令行管理；
86	0		命令行支持中文输入；需提供功能截图并加盖公章。
87	0		支持设定接口为管理接口，管理接口路由与业务路由隔离；需提供功能截图并加盖公章。
88	0		支持SNMPV1/V2/V3；
89	0	升级维护	支持自动创建和手动创建两种方式创建快照，数量不少于16个；自动创建可根据招标方的预设置时间，每周或每月自动创建系统快照；需提供功能截图并加盖公章。
90	0		可以从设备启动页面，选择任何一个快照进行系统恢复；实现整机完全回退；
91	0		可以通过快照列表、状态，展现当前系统的所处状态；
92	0	系统诊断	支持在WEB界面进行网络诊断，支持PING、TRACEROUTE、TCP的诊断方式；需提供功能截图并加盖公章。
93	0		支持在WEB界面进行网络抓包，支持设置接口、IP、协议、端口等过滤条件，抓包文件支持导出；需提供功能截图并加盖公章。
94	0		支持模拟一个数据包，查看数据包匹配详情功能；需提供功能截图并加盖公章。
95	0		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、网站类型流量、VPN流量、在线用户等对象进行监控展示；需提供功能截图并加盖公章。
96	0		支持对设备CPU、内存、整机流量、新建、并发进行统计，展示设备CPU、内存实时利用率及其历史走势

			96	0	统计，展示设备CPU、内存实时利用率及其历史走势图；
			97	0	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；需提供功能截图并加盖公章。
			98	0	支持主机威胁统计和展示，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；需提供功能截图并加盖公章。
			99	0	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、流速；
			100	0	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；需提供功能截图并加盖公章。
			101	0	系统统计详情。针对总流量、CPU、内存利用率，并发连接，新建连接，做72小时精细化曲线统计，曲线支持局部放大。
			102		支持标准syslog协议
			103	0	支持日志合并功能，相同类型的日志支持合并操作，降低日志流量开销；需提供功能截图并加盖公章。
			104	0	支持日志外发至多个SYSLOG服务器；
			105	0	支持流日志功能，将每一条数据流生命周期的各个业务模块的操作，整合为一条完整的日志进行展示；需提供功能截图并加盖公章。
			106	0	支持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；
			107	0	威胁情报具备云端汇集实时热点高威胁情报数据，提供边界防御研判恶意可疑行为，区分高频随机性攻击与高危定向攻击，预判并阻断攻击威胁对业务的影响；
			108	0	威胁情报类型包括可疑行为（垃圾邮件、网络爬虫、挖矿、主机扫描）、攻击威胁（网银大盗、爆破攻击、DDoS攻击、漏洞利用、Web漏洞攻击）、恶意站点（欺诈、赌博、钓鱼）、恶意软件（黑客工具、宏病毒、勒索软件、远控木马、网络蠕虫）、攻击组织（APT组织、僵尸网络C2、IoT攻击C2）、失陷主机（僵尸主机、IoT失陷主机）等；
			109	0	支持扩展集中策略分析模块；需提供功能截图并加盖公章。

110	0	策略梳理	支持集中对所有防火墙安全策略进行冗余分析，可分析出安全策略是否为不必要的冗余配置；需提供功能截图并加盖公章。
111	0		支持集中对所有防火墙安全策略进行收敛分析，也称宽松策略分析。能够支持查看任何一条宽松策略的流量详细信息；需提供功能截图并加盖公章。
112	0		支持集中对所有防火墙安全策略进行命中频率分析，辅助用户快速完成策略次序的调整，从而达到优化防火墙处理性能的目的；需提供功能截图并加盖公章。
113	0		支持集中对所有防火墙安全策略进行潜在冲突分析，辅助用户快速完成策略的调整，从而达到防火墙访问控制的目的；需提供功能截图并加盖公章。
114	0	产品要求	销售许可证：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》，且认证等级为增强级；提供证明材料并加盖公章。
115	0		版权证书：产品具有国家版权局颁发的《计算机软件著作权登记证书》；提供证明材料并加盖公章。

注：

1.“参数性质”栏中划“0”表示此参数为一般性技术参数，划“√”表示此参数为重要技术参数；

2.一般参数、重要技术参数有负偏离的，按照响应程度做不同额度扣分处理；

3.招标人有权要求中标人在合同签署前提供产品进行所有招标要求功能及投标响应的逐一验证，符合招标方要求后才能执行合同流程，验证中发现虚假应标的行为将予以追究相关责任。

1.风险评估服务（本条内容对此包号采购内容进行整体要求）

序号	参数性质	服务指标	技术服务要求
1	0	服务要求	依据国家关键信息基础设施有关网络安全风险分级标准、通过漏洞扫描、配置核查、网络架构分析以及渗透测试等技术服务手段和方法，对系统的脆弱性进行检查分析包括物理环境安全脆弱性检查、网络安全脆弱性核查、主机系统安全脆弱性核查、应用系统安全脆弱性核查、数据安全脆弱性核查等，并形成脆弱性分析报告，含改进建议，按照行内的业务风险分类，对资产、威胁、脆弱性评估结果进行综合分析，并根据风险计算方法确定最终风险排序和等级划分，形成风险评估报告。

2.应急响应服务（本条内容对此包号采购内容进行整体要求）

序号	参数性质	服务指标	技术服务要求
1	0	服务要求	采用高效的信息安全事件响应处置机制对业务系统网络或业务系统遭到的安全事件快速作出响应，根据安全事件等级，可在第一时间采用现场或远程的方式对安全事件进行应急处置，最大限度地降低安全事故带来的危害，抑制事件影响扩散，帮助业务系统负责单位将损失降至最低程度。

2

3.等级保护咨询服务（本条内容对此包号采购内容进行整体要求）

序号	参数性质	服务指标	技术服务要求
1	0	服务要求	基于对信息安全的深刻理解，以信息系统构建“等级化的安全体系”为等级保护工作的服务理念，旨在根据等级保护不同等级、不同阶段的业务特性、安全需求及安全应用重点，在等级保护的框架下构建一个安全、可靠、灵活、可持续改进的信息安全体系。

4.安全技术策略制定服务（本条内容对此包号采购内容进行整体要求）

序号	参数性质	服务指标	技术服务要求
1	0	服务要求	保护对象核心是业务数据，安全技术策是动态全周期。并用业务数据把其他层面策略动态的串起来，形成以业务数据为核心的动态全周期安全技术架构。同时结合最佳实践和行业标准规范，形成可落地、前瞻性、全方位，可支撑业务信息系统安全稳定运行的整体安全技术策略。

5.年度HW技术服务（本条内容对此包号采购内容进行整体要求）

序号	参数性质	服务指标	技术服务要求
1	0	服务要求	提供HW服务，年度HW活动如我方被抽取为防守方，需提供专业人员24小时进行监守防护，HW期间必须满足及时发现、及时处置以及还原攻击链。并且承诺甲方被抽取的标靶（目标）系统不被攻破。

说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。

附表二：防火墙　是否允许进口：否

参数性质	序号	具体技术(参数)要求

防火墙-35G

序号	参数性质	技术指标	技术规格要求
1	√	硬件规格	标准2U设备，双电源；
2	√		≥6个10/100/1000M Base-TX，≥4个SPF接口，4个SPF+接口，≥5个接口扩展槽。
3	√	性能要求	实际网络层处理能力≥35Gbps,防病毒处理能力≥12Gbps，每秒新建连接数不少于40万，并发连接数不少1500万

			4	√	工作模式	支持路由、透明、旁路、混合工作模式
			5	0	网络特性	支持静态路由、RIP、RIPng、OSPFv2、OSPFv3、BGP、ISP路由；
			6	0		内置移动、联通、电信、教育网、网通、长城宽带等ISP服务商地址列表；
			7	0		内置世界各国ISP地址库；需提供功能截图并加盖公章。
			8	0		支持802.1q，支持stp；
			9	0		支持根据入接口、源/目的IP地址、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； 支持不少于8种的选路算法；需提供功能截图并加盖公章。
			10	0		支持手动和LACP链路聚合，可根据源/目的mac、目的IP、等条件提供不少于2种链路负载算法；需提供功能截图并加盖公章。
			11	0		支持IPv4/v6双栈；需提供功能截图并加盖公章。；
			12	0		IP/MAC静态和动态探测绑定；
			13	0		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；需提供功能截图并加盖公章。
			14	0		支持NAT64, NAT46支持静态转换和前缀转换方式；需提供功能截图并加盖公章。
			15	0		支持 NAT66地址转换，支持源地址转换，目的地址转换，静态地址转换；
			16	0		支持NAT源端口复用，单个公网IP支持的并发会话数量无限制；
			17	0		支持SNAT源端口保持功能；
			18	0		支持NAT策略冲突检测；
			19	0		支持NAT地址池利用率告警；
			20	0		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；需提供功能截图并加盖公章。
			21	0		支持各种应用协议的NAT穿越：FTP、TFTP、H.323、SQL*NET；
			22	0		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；
			23	0		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；需提供功能截图并加盖公章

				。
	24	0		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；需提供功能截图并加盖公章。
	25	0	无线接入	支持802.11n无线接入，可支持2.4G频段或5G频段；（部分型号支持）
	26	0		支持LTE-FDD/WCDMA/TD-SCDMA/GSM/EMBB等移动网络制式；（部分型号支持，5G需定制）
	27	0	访问控制	支持Web认证，在策略中可设置用户 Web 认证的门户地址；需提供功能截图并加盖公章。
	28	0		支持基于策略的流量统计和会话统计；
	29	0		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；需提供功能截图并加盖公章。
	30	0		支持策略加速技术，减少策略对设备性能的消耗；需提供功能截图并加盖公章。
	31	0		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；需提供功能截图并加盖公章。
	32	0		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、策略命中数等条件进行细粒度查询；需提供功能截图并加盖公章。
	33	0		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；需提供功能截图并加盖公章。
	34	0	IPv6安全防护	支持基于IPv6的入侵防御、病毒防御、DDOS、WEB防护、防御等一系列安全防护功能；需提供功能截图并加盖公章。
	35	0		支持基于IPv6的流量控制、连接限制；需提供功能截图并加盖公章。
	36	0	入侵防御	支持独立的入侵防护规则特征库，特征总数在7000条以上，能对常见漏洞进行安全防护；需提供功能截图并加盖公章。
	37	0		规则库支持根据攻击类型、风险等级、流行程度等进行分类，防护动作包括告警、阻断；需提供功能截图并加盖公章。
	38	0		支持针对地址设置入侵防御白名单，支持攻击规则搜索以及自定义；需提供功能截图并加盖公章。
	39	0	DDOS防御	支持针对ICMP、TCP、UDP、等协议进行DDOS防护，支持预定义和自定义策略模板；

			御	护；支持预定义和自定义策略模板；
		40	0	病毒过滤	支持对HTTP/SMTP/POP3/FTP/IMAP等协议进行病毒防御；需提供功能截图并加盖公章。
		41	0		病毒特征库规模超过1200万；需提供功能截图并加盖公章。
		42	0	Web防护	支持对100个站点制订web应用防护策略，支持http请求回应的头、体检查；
		43	0		支持自定义web安全防护事件，可以对请求参数、各个头域、内容关键字、文件类型等进行灵活组合生成策略；需提供功能截图并加盖公章。
		44	0		支持对http的合规性检查，包括版本、方法、url、头域字段、传输文件等的合规性检查；需提供功能截图并加盖公章。
		45	0		内置web应用防护特征库，提供定期升级
		46	0	弱口令检查	支持对HTTP、telnet、FTP、SMTP、POP3等各种协议进行弱口令检查，并上报安全事件；需提供功能截图并加盖公章。
		47	0		支持高、中、低三种密码检查强度；
		48	0		支持对源目的ip地址进行过滤检查；
		49	0	黑名单	可设置基于IP过滤条件，实现对特定报文进行快速过滤，支持100万以上黑名单数量；需提供功能截图并加盖公章。
		50	0		内置动态黑名单功能，可与URL过滤、病毒过滤功能实现联动封锁；支持静态和动态黑名单命中统计和监控；支持黑名单添加事件和生效时间展示；需提供功能截图并加盖公章。
		51	0		支持黑名单多种类型导入，如通过文件上传增量添加黑名单、支持页面复制粘贴方式添加黑名单、支持API接口下发黑名单；需提供功能截图并加盖公章。
		52	0		支持按照ip/ip网段模糊检索；
		53	0		黑名单列表支持展示添加时间、添加方式（手工或来自其他安全事件）、命中次数。并支持按照命中次数排序；
		54	0	应用控制/URL过滤	支持IPv6的应用控制策略；
		55	0		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2000种；
		56	0		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；
		57	0		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；需提供功能截图并加盖公章。
		58	0		URL分类库规模不少于2000万条；需提供功能截图并加盖公章。

			59	0		内置P2P应用、网页应用、数据库应用等应用特征库；需提供功能截图并加盖公章。
			60	0		支持超过100类、2000万的URL地址分类库，用户可根据网站类别对自身网络的WEB应用实施全面化管控，杜绝非法、违规网站的访问行为；
	1		61	0	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；需提供功能截图并加盖公章。
			62	0		支持带宽限制、带宽保障和弹性带宽；
			63	0		支持高、中、低优先级通道设置；
			64	0	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；需提供功能截图并加盖公章。
			65	0	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；
			66	0		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；
			67	0		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；
			68	0		支持双路HA物理心跳线，确保HA运行稳定可靠；
			69	0		支持IPv6下的HA环境；
			70	0	用户管控	内置用户身份管理系统，支持本地认证、外部认证及等方式，支持RADIUS、LDAP等第三方外部认证；
			71	0		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、首次登陆修改密码、密码定期修改、密码有效时间等设置；
			72	0		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；需提供功能截图并加盖公章。
			73	0		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；需提供功能截图并加盖公章。
			74	0	IPSEC VPN	支持IPSec VPN功能，支持IKEV1、IKEV2、国密的加密类型，支持AES、DES、3DES、MD5、SHA-1、SM3等VPN加密、认证算法，支持对隧道内网络流量进行监控展示；需提供功能截图并加盖公章。
			75	0		无需额外授权，IPSec VPN用户数无限制；
			76	0		支持硬件国密加速卡(部分型号支持)；
			77	0		支持SSL VPN功能，满足远程用户安全接入内网；

			78	0	无需额外授权，SSL VPN用户数无限制；
			79	0	SSL VPN支持代理模式，能够直接代理内网页面到VPN用户登录页面；
			80	0	SSL VPN支持隧道模式，可添加多条路由，满足多网段内网的访问需求；
			81	0	SSL vpn支持BBR加速，在高延时、丢包等不良网络条件下，可以提升传输效率3-5倍以上
			82	0	SSL VPN登录支持双因子认证；
			83	0	支持Web管理界面，HTTP和HTTPS方式；
			84	0	支持中文及英文WEB界面，并可一键切换； 支持多种语言（不少于2种）web页面
			85	0	支持命令行方式管理，所有功能均可通过命令行实现，支持TELNET、SSH及串口方式进行命令行管理；
			86	0	命令行支持中文输入；需提供功能截图并加盖公章。
			87	0	支持设定接口为管理接口，管理接口路由与业务路由隔离；需提供功能截图并加盖公章。
			88	0	支持 SNMP V1/V2/V3；
			89	0	支持自动创建和手动创建两种方式创建快照，数量不少于16个；自动创建可根据招标方的预设置时间，每周或每月自动创建系统快照；需提供功能截图并加盖公章。
			90	0	可以从设备启动页面，选择任何一个快照进行系统恢复；实现整机完全回退；
			91	0	可以通过快照列表、状态，展现当前系统的所处状态；
			92	0	支持在WEB界面进行网络诊断，支持PING、TRACEROUTE、TCP的诊断方式；需提供功能截图并加盖公章。
			93	0	支持在WEB界面进行网络抓包，支持设置接口、IP、协议、端口等过滤条件，抓包文件支持导出；需提供功能截图并加盖公章。
			94	0	支持模拟一个数据包，查看数据包匹配详情功能；需提供功能截图并加盖公章。
			95	0	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、网站类型流量、VPN流量、在线用户等对象进行监控展示；需提供功能截图并加盖公章。
			96	0	支持对设备CPU、内存、整机流量、新建、并发进行统计，展示设备CPU、内存实时利用率及其历史走势图；
			97	0	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；需提供功能截图并加盖公章。

SSL VPN	
系统管理	
升级维护	
系统诊断	

			98	0	监控类型	支持主机威胁统计和展示，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；需提供功能截图并加盖公章。
			99	0		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、流速；
			100	0		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；需提供功能截图并加盖公章。
			101	0		系统统计详情。针对总流量、CPU、内存利用率，并发连接，新建连接，做72小时精细化曲线统计，曲线支持局部放大。
			102		日志	支持标准syslog协议
			103	0		支持日志合并功能，相同类型的日志支持合并操作，降低日志流量开销；需提供功能截图并加盖公章。
			104	0		支持日志外发至多个SYSLOG服务器；
			105	0		支持流日志功能，将每一条数据流生命周期的各个业务模块的操作，整合为一条完整的日志进行展示；需提供功能截图并加盖公章。
			106	0	威胁情报防护	支持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；
			107	0		威胁情报具备云端汇集实时热点高威胁情报数据，提供边界防御研判恶意可疑行为，区分高频随机性攻击与高危定向攻击，预判并阻断攻击威胁对业务的影响；
			108	0		威胁情报类型包括可疑行为（垃圾邮件、网络爬虫、挖矿、主机扫描）、攻击威胁（网银大盗、爆破攻击、DDoS攻击、漏洞利用、Web漏洞攻击）、恶意站点（欺诈、赌博、钓鱼）、恶意软件（黑客工具、宏病毒、勒索软件、远控木马、网络蠕虫）、攻击组织（APT组织、僵尸网络C2、IoT攻击C2）、失陷主机（僵尸主机、IoT失陷主机）等；
			109	0		支持扩展集中策略分析模块；需提供功能截图并加盖公章。
			110	0		支持集中对所有防火墙安全策略进行冗余分析，可分析出安全策略是否为不必要的冗余配置；需提供功能截图并加盖公章。
						支持集中对所有防火墙安全策略进行收敛分析，也称

			111	0	策略梳理	宽松策略分析。能够支持查看任何一条宽松策略的流量详细信息；需提供功能截图并加盖公章。
			112	0		支持集中对所有防火墙安全策略进行命中频率分析，辅助用户快速完成策略次序的调整，从而达到优化防火墙处理性能的目的；需提供功能截图并加盖公章。
			113	0		支持集中对所有防火墙安全策略进行潜在冲突分析，辅助用户快速完成策略的调整，从而达到防火墙访问控制的目的；需提供功能截图并加盖公章。
			114	0	产品要求	销售许可证：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》，且认证等级为增强级；提供证明材料并加盖公章。
			115	0		版权证书：产品具有国家版权局颁发的《计算机软件著作权登记证书》；提供证明材料并加盖公章。
			注： 1.“参数性质” 栏中划“0”表示此参数为一般性技术参数，划“√”表示此参数为重要技术参数； 2.一般参数、重要技术参数有负偏离的，按照响应程度做不同额度扣分处理； 3.招标人有权要求中标人在合同签署前提供产品进行所有招标要求功能及投标响应的逐一验证，符合要求后才能执行合同流程，验证中发现虚假应标的行为将予以追究相关责任。			
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。					

附表三：入侵检测　是否允许进口：否

参数性质	序号	具体技术(参数)要求			
		序号	参数性质	技术指标	技术规格要求
		1	√	硬件规格	工作接口≥2个SPF+接口，≥1个Console口，≥1个带外管理口，≥1个HA口，≥3个扩展插槽，≥2个USB接口。
		2	√	性能要求	三层检测≥10Gbps，应用层检测≥6Gbps，最大并发连接数≥350万，每秒新建HTTP连接数≥20万。
		3	0		攻击检测基础能力，系统应支持IP碎片重组、TCP流重组、TCP流状态跟踪、2至7层的协议分析、系统应支持工作在非默认端口下的周知服务（如运行在8000端口下的Web Server）的协议识别与协议分析能力；
		4	0		系统需要支持如下常见协议的解析：ETHER、ARP、RARP、IP、ICMP、IGMP、PPPoE、Vlan Tag、MPLS、TCP、UDP、NetBIOS、CIFS、SMB、FTP、TELNET、POP3、SMTP、IMAP、SNMP、MSRPC、SUNRPC、TNS、TDS、HTTP、QQ、MSN、BT、Thunder、CHARGEN、ECHO、AUTH、

						DNS、FINGER、IRC、MSPROXY、NFS、NNTP、NTALK、PCT、WHOIS等，协议覆盖面广，与之对应的事件库完备，需提供截图证明；
			5	0		设备具有抗逃避检测机制，可以针对分片逃逸攻击、重叠逃逸攻击、加入多余或者无用字节逃逸攻击进行有效防范，并且能具体说明，提供技术报告或者截图；
			6	0		支持全面的攻击检测能力，可检测常见的Web攻击、缓冲溢出攻击、安全漏洞攻击、安全扫描攻击、拒绝服务攻击、木马后门攻击、蠕虫病毒攻击、穷举探测攻击、CGI攻击等，需提供截图；
			7	0		系统需具备全面的Web应用类攻击检测能力，能够检测各种SQL注入攻击、XSS跨站攻击、Webshell上传、命令注入、目录遍历、命令执行等攻击行为，需提供截图；
			8	0		系统首页提供最近24小时内网络发生的展示界面，包括对拒绝服务事件、扫描事件、蠕虫事件、木马病事件、网络整体状况等展示，需提供界面截图；
			9	0	攻击检测	系统提供有效最新攻击特征，并且根据协议类型、安全类型、流行程度、影响设备等方式做有效分类，需提供截图；
			10	0		系统需具备攻击检测能力的扩展功能，可提供检测规则自定义的高级接口，接口具备丰富的协议变量，可以自定义配置特协议变量特征值，需提供截图；
			11	0		系统需支持TCP协议攻击特征自定义，提供tcp_ack、tcp_fin、tcp_flag、tcp_payload、tcp_syn、tcp_urg、tcp_seq、tcp_rst等协议变量特征的自定义，支持设置协议变量的操作符，操作符包括等于、不等于、包含、不包含；
			12	0		系统需提供对事件的二次检测能力，即对已生成的事件进行二次分析与统计，并根据统计结果进行报警，同时，系统需支持对统计阈值进行设定的图形化用户接口，通过该图形化接口，用户可以选择需要统计的基础事件并对阈值进行设置与调整；
			13	0		系统需具备针对如下几种拒绝服务攻击的检测能力：针对特定主机的TCP（SYN）FLOOD、针对特定主机的TCP （STREAM）FLOOD、针对特定主机的UDP FLOOD、针对特定主机的ICMP FLOOD；对上述所有攻击检测都可通过控制界面配置统计时间、报警阈值（投标时需提供加盖原厂商公章的产品界面截图）；
			14	0		提供网关IP-MAC地址绑定的功能识别arp地址欺骗

			14	0		攻击，需提供界面截图；
	1		15	0		系统提供自定义弱口令规则的能力，使用户可以灵活定义网络内的弱口令条件，需提供界面截图；
			16	0		统可配置过滤条件，可根据MAC过滤和IP过滤关系进行“与”“或”策略配置，需提供界面截图；
			17	0		系统提供威胁的实时展示能力，可以将引擎检测到的威胁在威胁展示界面进行实时显示，现实内容需全面丰富，包括：事件名称、源IP、目的IP、攻击发生时间、事件级别、流行程度、攻击类型、事件返回参数、事件说明和事件解决方案等
			18	0	威胁分析能力	系统首页需提供如下关键报警及汇总数据：24小时重点威胁事件汇总，并支持下钻查看具体攻击事件内容、24小时发生事件的Top5排名、今日流量曲线
			19	0		系统需具备提取攻击原始报文的能力，针对产生的告警事件，可以对攻击行为的特征数据包进行提取，方便事件分析人员对攻击行为进行分析，需提供截图
			20	0		系统需具备全面的流量统计能力，可以支持实时统计当前网络中的总流量、Web应用流量、数据库应用流量、邮件应用流量、P2P应用流量，并按照流量趋势图的形式进行可视化展现，需提供截图；
			21	0	流量统计能力	系统需具备流量分析能力，支持根据历史流量数据，计算出当前时刻历史均值流量大小，并形成历史均值流量曲线，可以与实时流量曲线进行同时呈现并形成对比，方便分析人员掌握网络流量态势，需提供截图；
			22	0		系统需具备完善的流量告警能力，支持按照历史流量同期对比和设置流量阈值两种方式配置告警参数，告警级别包含偏低、偏高等多种类型，需提供截图；
			23	0		系统需提供完善的报表系统所提供的报表模板不应少于50个，能辅助用户分析一段时间内的威胁；
			24	0		系统需提供事件名称+目的地址+源地址；事件名称+源地址+目的地址的三维交叉报表，能辅助用户快速定位问题；
			25	0	报表功能	系统需提供完善的报表系统，支持面向安全结论的分析报表；报表需支持如下格式：HTML、PDF、EXCEL、WORD，所生成的报表可以自动发送到多个邮箱，能辅助用户查阅；
			26	0		报表需支持手动立即执行、周期性自动执行两种执行方式；
						系统需具备完善的特征库升级能力，特征库升级支

			27	0	持在线和离线升级方式，通过官网下载离线升级特征库，支持web界面一键导入方式进行升级；
			28	0	系统需支持多级部署、集中管理能力，可以添加组件（包括控制中心、引擎），至少支持五级以上部署环境；
			29	0	级联环境中，系统需具备支持上级对下级转发事件库升级包、系统升级补丁包，上级控制中心可以对下级统一下发策略集，方便统一管理；
			30	0	系统管理	系统需具备Web界面服务配置能力，可配置启用/停用http和https服务，支持配置http和https访问设备WEB界面端口，需提供截图；
			31	0	系统需具备用户管理能力，支持三权分立原则，系统具有用户管理员、审计管理员、配置管理员，支持创建不同的配置管理员，并赋予不同的授权角色，控制管理员的配置权限，需提供截图；
			32	0	系统需具备绑定管理员用户IP地址的能力，支持对管理员用户的IP地址进行绑定，防止非法IP的使用账号访问设备，需提供截图；
			33	0	产品资质	国家版权局-计算机软件著作权登记证书。提供证明材料并加盖厂家公章。
			34	0	公安部-计算机信息系统安全专用产品销售许可证（万兆）。提供证明材料并加盖厂家公章。
			注： 1.“参数性质” 栏中划“0”表示此参数为一般性技术参数，划“√”表示此参数为重要技术参数； 2.一般参数、重要技术参数有负偏离的，按照响应程度做不同额度扣分处理； 3.招标人有权要求中标人在合同签署前提供产品进行所有招标要求功能及投标响应的逐一验证，符合要求后才能执行合同流程，验证中发现虚假应标的行为将予以追究相关责任。		
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。				

附表四：入侵防御　是否允许进口：否

参数性质	序号	具体技术(参数)要求			
		序号	参数性质	技术指标	技术规格要求
		1	√	硬件规格	工作接口≥4个千兆电口，≥4个SPF接口，≥4个SPF+接口，≥1个Console口，≥1个带外管理口，≥1个HA口，≥1个扩展插槽，≥2个USB接口，工作电口均应支持内置硬件bypass，光口支持外接bypass设备。
		2	√	性能要求	三层吞吐≥35Gbps，应用层吞吐≥16Gbps，最大并发连接数≥1500万，每秒新建HTTP连接数≥70万。
		3	0		系统入侵防御事件库事件数量不少于5000条。

			4	0	系统应支持自定义事件升级内容。升级界面中至少包含高中低三种级别事件的升级启用选项。并支持可自动修改动作为通过，满足业务高连续要求下的事件监测要求。需提供功能截图并加盖厂商公章。
			5	0	系统应支持无线攻击检测和防护功能扩展，可手工或自动识别和区分内部AP和外部AP，也可以手工或自动识别合法终端，并基于此设定无线准入策略，通过射频信号阻止非法AP、终端的接入。支持无线扫描、欺骗、DoS、破解等常见无线网络攻击行为的检测、告警、阻断功能，同时支持多种类型流氓AP的检测与阻断。需提供功能截图并加盖厂商公章。
			6	0	系统应内置未知恶意代码检测引擎，能检测流经的http、ftp、邮件协议中包含的office文档、图片文档及压缩文档中的未知恶意文件,报警信息应包括源目的IP、协议类型、文件基本信息、检测方法、危险等级及文件的应用的详细信息（如邮件的发件人、收件人、标题等），方便跟踪恶意文件，需说明此引擎和防病毒引擎的区别、实现原理和效果。需提供功能截图并加盖厂商公章。
			7	0	系统应支持单独的恶意样本检测规则升级功能，方便对恶意样本检测功能进行扩充。需提供功能截图并加盖厂商公章。
			8	0	系统应支持恶意样本自学习功能，除通过网络文件捕获外，还支持通过系统直接上传文件，自动识别黑白文件并提供简要信息。
			9	0	系统应支持与恶意代码动态检测系统联动。系统将流经的http、ftp、邮件协议中包含的office文档、图片文档及压缩文档提交给APT检测系统，并可查询APT的检测结果。需提供功能截图并加盖厂商公章。
			10	0	系统应支持未知C&C通道（隐蔽通道）检测功能，能够提供C&C通道的危险级别、连接建立时间、连接持续时间、控制端IP地址和端口、受控端IP地址和端口等C&C通道信息。提供各种响应动作：阻断会话、临时阻断和抓包分析等。需提供功能截图并加盖厂商公章。
			11	0	可基于IP地址、网段、时间、VLAN、协议类型等条件设定IPS检测及响应方式。
			12	0	支持虚拟IPS功能，不同的用户可以方便定制满足自身要求的检测模版，至少支持400个用户。
			13	0	系统应具备网络准入控制能力，通过和终端管理系统联动，拒绝不安全主机连入网络，说明网络准入控制原理和实现效果。
			14	0	系统应支持威胁情报，具备软件著作权。需提供功能截图并加盖厂商公章。
					威胁情报类型不少于50类，至少覆盖安卓恶意程序、APT

			15	0	入侵防御功能	攻击、远控木马、僵尸网络、僵尸主机、挖矿、DDOS攻击、欺诈、赌博、物联网/IOT攻击网络、物联网/IOT失陷主机、恶意网站、钓鱼、勒索软件、web攻击主机、网络蠕虫等。需提供功能截图并加盖厂商公章。
			16	0		系统应支持威胁情报，通过通用接口获得第三方的威胁情报，提升防御能力。需提供功能截图并加盖厂商公章。
			17	0		系统应支持特殊环境下的攻击源真实地址还原能力。
			18	0		系统应具备终端和服务器环境感知能力，通过主动扫描和扫描结果导入获得终端环境情况。
			19	0		系统应支持事件响应模版，能够批量修改事件响应动作，包括：事件级别、事件启用开关、动作、日志合并方式、日志开关、抓包取证。
			20	0		系统应支持多种事件响应方式，满足招标方的安全要求，需包括：重置、临时阻断、丢弃报文、丢弃会话等动作。需提供功能截图并加盖厂商公章。
			21	0		采用先进的模式匹配及协议分析技术实现对网络报文的分析；
			22	0		具备协议自动识别功能；
			23	0		支持检测规则自定义功能；自定义参数不低于100种。
			24	0		系统应支持常见默认事件集，便于用户使用，默认事件集至少包括：全集、中高级事件、僵尸木马蠕虫事件集、WEB事件。需提供功能截图并加盖厂商公章。
			25	0		事件库应支持CVE和CNNVD兼容能力。
			26	0		系统应支持QQ和MSN应用识别功能，支持黑白名单功能，阻止或允许部分帐号登录。需提供功能截图并加盖厂商公章。
			27	0		系统应支持密码穷举探测功能，提供至少20种密码穷举行为特征探测和阻断。需提供功能截图并加盖厂商公章。
			28	0		系统应支持弱口令检测功能，需支持至少8种网络协议并支持至少7种弱口令检测元素，文字说明支持的网络协议和定义弱口令的检测元素。需提供功能截图并加盖厂商公章。
			29	0		系统入侵防御事件库事件数量不少于5000条，
			30	0		系统应支持自定义事件升级内容。升级界面中至少包含高中低三种级别事件的升级启用选项。并支持可自动修改动作为通过，满足业务高连续要求下的事件监测要求。需提供功能截图并加盖厂商公章。
			31	0		系统应支持无线攻击检测和防护功能扩展，可手工或自动识别和区分内部AP和外部AP，也可以手工或自动识别合法终端，并基于此设定无线准入策略，通过射频信号阻止非法AP、终端的接入。支持无线扫描、欺骗、DoS、破解等常见无线网络攻击行为的检测、告警、阻断功能，同时支

						持多种类型流氓AP的检测与阻断。需提供功能截图并加盖厂商公章。
	1		32	0		系统应内置未知恶意代码检测引擎，能检测流经的http、ftp、邮件协议中包含的office文档、图片文档及压缩文档中的未知恶意文件,报警信息应包括源目的IP、协议类型、文件基本信息、检测方法、危险等级及文件的应用的详细信息（如邮件的发件人、收件人、标题等），方便跟踪恶意文件，需说明此引擎和防病毒引擎的区别、实现原理和效果。需提供功能截图并加盖厂商公章。
			33	0	部署方式	系统应提供旁路部署及在线、旁路混合部署等部署方式。
			34	0		系统应支持IP地址转换（NAT）功能，包括：源地址转换、目的地址转换、静态地址转换。
			35	0		系统应支持桥组部署方式，并支持STP协议。
			36	0		系统应支持路由模式，至少包括：静态路由、策略路由、ISP和OSPF路由协议。
			37	0		支持DHCP功能，包括DHCP服务器和DHCP中继功能。并可以获得IP地址，满足招标方自动化管理的需要。需提供功能截图并加盖厂商公章。
			38	0		系统应支持端口聚合/链路捆绑协议，并提供手工方式和LACP两种配置方式。
			39	0		系统应支持完善的会话管理功能，可实时查看当前会话状态，支持根据源地址、目的地址、端口号或协议类型查询会话。
			40	0	防病毒功能	系统应支持通过授权扩展支持对HTTP、FTP、SMTP、POP3、IMAP协议的病毒检测和过滤功能；
			41	0		系统应支持通过授权扩展支持对HTTP、FTP、SMTP、POP3、IMAP协议的文件屏蔽功能，防止文件的下载和传输。
			42	0		系统应支持VLAN、VoIP数据流病毒过滤；
			43	0		系统应支持双病毒引擎，需提供包括国产厂商在内的防病毒引擎厂商合作证明并加盖厂商公章。
			44	0		系统应支持对文件感染型病毒、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30万。
			45	0		系统应支持HTTP协议和邮件协议防病毒，通过信息替换功能，用以通知用户病毒被阻断，管理员可以自行设置替换信息。
			46	0	内容防护	系统应支持Web过滤功能，至少支持黑白名单、关键字过滤、禁止HTTP代理外，还支持Script、 Java Applet等过滤，并能通过统一模版设置，
			47	0		系统应支持邮件内容过滤功能，有效防止恶意邮件及信息外泄。可根据邮件SMTP命令、发件人、主题、附件、IP及邮件大小进行过滤，
						系统应支持敏感信息防护功能，识别信息和文件中的关键

			48	0		字、身份证、手机号码、固定电话号码、银行卡、IP地址等敏感信息，并支持文件指纹识别和白名单功能。 并说明支持的应用情况和处理方式。需提供功能截图并加盖厂商公章。
			49	0	高可用性	系统应支持双机热备和双机主备功能，并且主备热备时需支持连接状态和配置同步。
			50	0		系统应支持硬件BYPASS。在设备故障、重启及断电的情况下可保障网络畅通，能够手动配置BYPASS的启停。
			51	0		系统应支持软件Bypass功能，通过CPU和内存阈值实现软件Bypass的开启，提供不同的阈值计算方式（最高值/平均值、时间区间等），
			52	0		系统应支持重点资产和应用监控功能，当资产和应用出现异常时，通过syslog和邮件进行告警，并可以记录日志。需提供功能截图并加盖厂商公章。
			53	0		系统应支持多种设备管理方式，包括HTTPS、CONSOLE、SSH、TELNET等；
			54	0	管理功能	系统应支持WEB登录图像验证码功能，防止暴力破解。需提供功能截图并加盖厂商公章。
			55	0		系统应支持在线管理员数目限制和管理员唯一性检查功能，提高系统管理的安全性。
			56	0		需支持动态口令卡或Ukey方式的双因子认证，增强配置管理的安全性。需提供功能截图并加盖厂商公章。
			57	0		系统应支持定期修改密码功能。
			58	0		系统应支持较强的密码安全性，提供首次登录密码修改功能，首次登录时提供强制修改和提醒修改两种方式。需提供功能截图并加盖厂商公章。
			59	0		系统应提供系统监控和趋势曲线图展示，至少支持内存占用率、CPU占用率、总流量、每秒新建连接数、并发会话数的趋势图，可按照1小时、6小时、12小时、1-7等时间段展示趋势曲线。需提供功能截图并加盖厂商公章。
			60	0		系统应支持历史入侵事件处理功能，直接对历史事件进行分析和处理，并用于未来事件检测。并可以查询处理情况。
			61	0		支持场景分析功能，提供进行更深入的分析能力，至少包括僵尸木马蠕虫的分布式攻击场景分析。
			62	0		系统应支持本地日志及SYSLOG日志发送，支持向至少3个syslog服务器发送日志。需提供功能截图并加盖厂商公章。
			63	0		系统应支持syslog格式修改功能，通过对日志内容裁剪、修改次序，满足用户安全管理平台日志格式要求。
			64	0		系统应提供netflow日志发送功能，满足第三方管理平台对netflow日志的审计需求。

			65	0		系统应支持声音报警，通过设置事件级别、入侵事件级别和病毒事件进行声音报警。
			66	0		系统应支持报表个性化设置，通过自定义报表生成单位、报表生成人、单位logo和安全摘要信息等信息，快速生成符合单位特点的报告，减少工作量。需提供功能截图并加盖厂商公章。
			67	0		系统应提供定期自定发送报表功能，通过邮件将html、doc、xls、CSV和pdf格式报表发送给管理员。
			68	0	产品要求	具备公安部颁发的《计算机信息系统安全专用产品销售许可证》(国标三级)。需提供证明材料并加盖厂商公章。
			69	0		具有国家版权局颁发的多核并行操作系统的《计算机软件著作权登记证书》
			注： 1.“参数性质”栏中划“0”表示此参数为一般性技术参数，划“√”表示此参数为重要技术参数； 2.一般参数、重要技术参数有负偏离的，按照响应程度做不同额度扣分处理； 3.招标人有权要求中标人在合同签署前提供产品进行所有招标要求功能及投标响应的逐一验证，符合招标方要求后才能执行合同流程，验证中发现虚假应标的行为将予以追究相关责任。			
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。					

合同包2（安全及密码设备）

1.主要商务要求

标的提供的时间	合同签订后20个日历日内交货
标的提供的地点	采购人确定交付地点
投标有效期	从提交投标（响应）文件的截止之日起90日历天
付款方式	1期：支付比例50%，支付比例50%，结合预算资金下达情况，合同签订后，收到中标供应商支付的履约保证金及合法凭证后支付合同金额的50%. 2期：支付比例50%，产品到货验收后支付合同金额的50%
验收要求	1期：项目具备初步验收条件后，由采购单位负责组织验收工作小组进行初步验收 2期：项目具备竣工验收条件后，按照相关规定进行竣工验收
履约保证金	收取比例：10%,说明：为保证中标供应商更好地履行合同，中标供应商须向采购人交纳履约保证金，金额为中标金额的10%。履约保证金的交付时间为合同签订后3日内。验收合格正常运行后计算质保期，履约保证金在质保期满1年后的1个月内，无息原额退还。若中标供应商未能履行其合同规定的任何义务，采购人有权扣罚履约保证金。
其他	

2.技术标准与要求

序号	核心产品（“△”）	品目名称	标的名称	单位	数量	分项预算单价（元）	分项预算总价（元）	面向对象情况	所属行业	招标技术要求
1		防火墙	WEB应用防火墙	台	3.00	300,000.00	900,000.00	否	其他未列明行业	详见附表一
2		其他安全设备	抗APT攻击设备	台	1.00	250,000.00	250,000.00	否	其他未列明行业	详见附表二
3		其他安全设备	安全管理中心设备	台	1.00	200,000.00	200,000.00	否	其他未列明行业	详见附表三
4		密码产品	服务器密码机	台	4.00	150,000.00	600,000.00	否	其他未列明行业	详见附表四
5		网上行为管理设备	上网行为	台	2.00	80,000.00	160,000.00	否	其他未列明行业	详见附表五
6		虚拟专用网（VPN）设备	VPN设备	台	2.00	250,000.00	500,000.00	否	其他未列明行业	详见附表六
7		密码产品	签名验签服务器	台	1.00	130,000.00	130,000.00	否	其他未列明行业	详见附表七
8		其他安全设备	堡垒机	台	2.00	125,000.00	250,000.00	否	其他未列明行业	详见附表八

附表一：WEB应用防火墙　是否允许进口：否

参数性质	序号	具体技术(参数)要求

序号	参数性质	技术指标	标准参数值
1	√	接口要求	2U机箱，提供≥1个10/100M管理接口、≥1个10/100/1000M HA口，≥4个千兆电口，≥4个SPF接口，≥4个SPF+接口，支持≥2个扩展插槽。
2	√	性能要求	设备网络层吞吐率不少于20G
3	√		设备应用层吞吐率不少于8G
4	√		设备最大HTTP并发连接数不小于100万
5	√		设备每秒新建HTTP连接数不少于10万
6	0	接入模式	应支持透明、代理模式、旁路部署、单臂部署、策略路由部署。
7	0		应支持智能部署，上线WAF设备能够自动感知Web网站IP和端口，提供功能截图并加盖公章。
8	0		应具备恶意重定向防护功能，提供功能截图并加盖公章。
9	0		应支持安装向导式部署，按照该部署方式可直接部署完成，提供功能截图并加盖公章。
10	0		应支持NAT环境下的用户识别能力，提供功能截图并加盖公章。
11	0		应支持链路绑定功能。支持IP地址组为维度指定相关安全策略。

			12	0	应支持对Web相关应用协议进行自定义，并提供详细协议分析变量。
			13	0	应具备Web恶意扫描防护的检测与防御能力，专利级别防护能力，提供功能截图并加盖公章。
			14	0	应具备人机识别功能，提供功能截图并加盖公章。
			15	0	应具备威胁情报功能，提供功能截图并加盖公章。
			16	0	应具备检测到攻击日志可高亮显示，有利于用户比较直观看到攻击脚本，提供功能截图并加盖公章。
			17	0	上报日志中有日志解码工具，通过解码工具可准确查看攻击语句，有利于用户查看和分析攻击日志，提供功能截图并加盖公章。
			18	0	设备具有对外提供API接口能力，可通过API接口给设备下发策略，提供功能截图并加盖公章。
			19	0	应具备双引擎防护功能，提供功能截图并加盖公章。
			20	0	应具蜜罐检测功能，诱使攻击方对它实施攻击，从而可以对攻击行为进行捕获和阻断，提供功能截图并加盖公章。
			21	0	应具备业务合规功能，可对业务进行恶意试探、恶意撞库、恶意登录等行为进行检测及拦截，提供功能截图并加盖公章。
			22	0	应具备网站锁功能，对网站进行锁定，可按日期、周期进行锁定时间设置，提供功能截图并加盖公章。
			23	0	应具备API防护功能，提供功能截图并加盖公章。
	1		24	0	应具备网站一键关停功能，提供功能截图并加盖公章。
			25	0	应具备源访问区域控制功能，可按照国家、省进行地址访问限制，防止区域性攻击对Web网站造成影响，提供功能截图并加盖公章。
			26	0	应具备访问控制功能，预防恶意进行访问频率的多层次恶意访问，提供功能截图并加盖公章。
			27	0	应支持获取Web安全事件的原始攻击信息，提供功能截图并加盖公章。
			28	0	Web安全事件日志存储，应支持主流的服务器操作系统及主流的数据库类型。
			29	0	应具备Web安全事件的报表功能，支持一般的单一

Web攻击防护

Web安全事件统计分析与报

				分析与报表	条件报表输出、专业的多维度统计报表输出。
			30	0	应具备自定义报表功能，并支持导出为WORD\EXCEL\PDF \HTML 等常用公文处理格式。
			31	0	系统管理	应支持B/S管理方式Web管理界面。
			32	0		应具备设备集中管理功能，可实现设备分布式部署、集中式监控管理，适合大规模部署环境。
			33	0		应具备多设备拓扑显示功能，可以在界面上以图形化的方式显示当前的部署拓扑，提供功能截图并加盖公章。
			34	0		应支持SNMP、 SYSLOG。
			35	0		应支持主主模式且主主模式配置、运行状态进行同步，提供功能截图并加盖公章。
			36		升级管理	应支持手动执行产品升级。
			37	0		应支持自动执行产品升级，不需要用户每次手动升级特征库，提供功能截图并加盖公章。
			38	0		公司网站应提供产品离线升级包下载。
			39	0		应对登陆用户提供防暴力猜解功能。
			40	0	蜜罐	支持轻量级蜜罐防御功能，提供伪造的后台管理系统页面防御功能
			41	0	移动管理	支持移动终端管理功能，不需要安装APP和第三方插件，通过手机浏览器即可管理设备，并可查看设备CPU、内存使用情况。
			42	0	产品要求	应标产品具备国家版权局软件著作权登记证书，需提供证明材料并加盖公章。
			43	0		产品具有《计算机信息系统安全专用产品销售许可证》，销售许可证中必须标注"万兆"字样，且销售许可证为WAF国标-增强级，提供证书复印件及盖公章
			注： 1.“参数性质”栏中划“0”表示此参数为一般性技术参数，划“√”表示此参数为重要技术参数； 2.一般参数、重要技术参数有负偏离的，按照响应程度做不同额度扣分处理； 3.招标人有权要求中标人在合同签署前提供产品进行所有招标要求功能及投标响应的逐一验证，符合招标方要求后才能执行合同流程，验证中发现虚假应标的行为将予以追究相关责任。			
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。				

附表二：抗APT攻击设备　是否允许进口：否

参数性质	序号	具体技术(参数)要求

序号	参数性质	技术指标	标准参数值
1	√	硬件指标	应标设备为标准2U服务器式机架，必须配置冗余电源，支持热插拔
2	0		应标设备具备RAID能力（即必须集成RAID控制器）,具备高可靠性与高效磁盘结构，必须使用Raid10
3	√		应标设备硬盘容量必须大于等于8TB容量，内存必须大于等于128GB
4	√		标准2U机架式安全设备，配置冗余电源，提供1个1000M管理接口、1个1000M私有云口，业务口配置不少于4个10/100/1000M自适应电口，2个SPF+接口，额外配置≥6个接口扩展槽位。扩展接口理论满配支持≥14个万兆光口或28个千兆电口（或光口）
5	√		设备网络层吞吐率不少于12G，设备应用层吞吐率不少于6G，最大HTTP并发连接数不小于80万，每秒新建HTTP连接数不少于5万。文件处理性能不低于20万个/天
6	0	部署模式	支持旁路部署、集群部署
7	0		应标产品具备100种以上格式的文件检测能力，涵盖Windows、Linux、Android多种操作系统, 支持自定义文件类型。需提供截图证明
8	0		应标产品需具备不少于3种检测机制（静态检测、漏洞检测、行为检测），每种检测机制检测流程可自定义配置。需提供截图证明
9	0		应标产品支持不少于10种样本检测工作流配置，每种工作流可自定义选取相应的样本格式。需提供截图证明
10	0		应标产品具备邮件检测、HTTP检测、FTP检测、SMB检测，支持可疑样本手动上传检测
11	0		应标产品具备全过程工作的检测流程配置模板。需提供截图证明
12	0		应标产品具备多种虚拟沙箱检测环境的能力
13	0		应标产品具备恶意样本库、隐蔽信道库、威胁情报库的能力
14	0		应标产品必须具备与防火墙、终端防病毒、网闸、网络审计、入侵检测、入侵防御、WAF等7种以上专业安全设备协同联动，需提供联动设备的联动界面截图证明
15	0		应标产品可对协同联动设备提交的可疑样本文件展示其检测结果、检测时间、来源、类型、状态等信息

			16	0		应标产品应支持反沙箱检测不少于20种行为。需提供截图证明
			17			应标产品可提供恶意文件MD5,并展示相同MD5值对应的文件匹配次数
			18	0		应标产品支持对文件运行产生的C&C地址的威胁情报检测机制。通过威胁情报标注样本的家族类型。需要提供截图证明。
			19	0	未知威胁检测	应标产品应支持邮件正文内容提取并展示，可提取邮件正文中的URL。 需提供截图证明
			20	0		应标产品应支持加密压缩文件解密，支持压缩文件子文件单独检测。需提供截图证明
			21	0		应标产品支持中文标签展示恶意代码类型，并支持按照中文标签检索。需提供截图证明
			22	0		应标产品支持自定义YARA规则进行检测的能力。需提供截图证明
			23	0		具备以下格式样本(office)文件类型的精确识别能力 "doc","dot","xls","xlt","xla","ppt","rtf","pub","docm","dotx","dotm","docx","xltm","xlam","xlsm","xlsb","xltx","xlsx","pptx","ppsx","potx","ppam","ppsm","pptm","potm","thmx","slk","hwp","jtd","odt","ods","odp"。需提供截图证明
			24	0		支持对文件样本的网络行为检测，记录文件运行时的网络通信会话，并支持在线查看目的IP、目的端口、16进制和ASCII格式数据包内容等通信会话详情。需要提供截图证明。
			25	0		支持检测：释放PE文件、删除文件夹、修改文件、拷贝自身、感染文件等敏感行为下载文件；支持详细记录对文件系统的监控操作，包括写入文件（夹）、删除文件（夹）、读取文件（夹）等。需要提供截图证明。
	1		26	0		支持检测：创建、删除自启动项，创建启动服务、创建异常注册表键值等敏感行为；支持记录详细注册表操作，如：写入、读取、删除注册表。需要提供截图证明。
			27	0		支持检测：打开系统进程中的线程、启动可疑进程、启动子进程、向系统进程内写入数据、注入其他进程、在系统进程中创建远程线程、遍历进程、向其他进程写入可疑内容、试图将该进程作为傀儡进程启动等敏感行为；支持记录：进程启动等详细行为信息。需要提供截图证明。
						应标产品具备事件特征库不少于4500条以上，并且

			28	0	可以按照协议类型、攻击类型、安全类型、流行程度、事件级别等分类编排事件特征。需提供截图证明
			29	0	应标产品系统策略集至少包括失陷主机、行为分析、攻击路径策略集。需提供截图证明
			30	0	应标产品支持下载匹配上特征检测策略的原始报文信息，需提供截图证明
			31	0	应标产品支持手动导入pcap包检测，检测内容必须包括特征检测、样本检测、隐蔽信道检测，能够展示pcap包与事件对应关系，能够展示检测时间和发生时间。需提供截图证明
			32	0	应标产品具备35种以上协议分析能力、拒绝服务扫描类事件，需提供截图证明
			33	0	应标产品具备弱口令检测，口令配置项不少于7种。需提供截图证明
			34	0	应标产品具备事件合并能力，并且可根据“周期”“次数”自定义配置。需提供截图证明
			35	0	应标产品应具备WEB攻击事件研判能力，能够明文展示攻击点请求响应报文内容。需提供截图证明
			36	0	应标产品具备Syslog和SNMP trap响应能力
			37	0	应标产品具备FTP加密方式外发样本，以及支持样本检测报告等自定义信息的外放，需提供截图证明
			38	0	应标产品具备邮件报警能力，将报警信息通过邮件发送给管理员
			39	0	应标产品支持通过Kafka接口将样本检测日志、特征检测日志、隐蔽信道日志、恶意URL日志发送给第三方平台。需提供截图证明
			40	0	应标产品支持可视化展示恶意样本攻击地图
			41	0	应标产品应支持展示恶意样本等级占比图、安全类型TOP5、样本标签TOP5
			42	0	应标产品应提供恶意代码行为的详细报告，能够显示进程/线程状态、注册表项操作、文件操作、互斥量操作、网络操作、服务相关、关键API调用等行为等信息供分析。需提供截图证明
			43	0	应标产品提供日志分析报表，报表类型至少包括分析报表、基础统计报表、高级统计报表、详细事件报表，报表需支持如下格式：HTML、PDF、EXCEL、WORD。需提供截图证明
			44	0	应标产品具备批量下载检测样本和样本报告信息
			45	0	应标产品具备中文管理界面，并且可配置管理员、用户管理员、审计管理员等
			46	0	应标产品具备私有云扩展能力，需提供截图证明
					应标产品需全面支持ipv6，支持ipv6管理、检测ipv

			47	0		6流量
			48	0	自身安全	应标产品核心构件通信采用SSL加密传输、支持访问控制列表
			49	0	行为分析	支持告警的深度行为分析，行为包括DNS解析行为、TCP/UDP交互行为、WEB访问行为、传输文件行为。
			50	0	挖矿检测	支持门罗币、莱特币、以太坊、比特币等币种的检测
			51	0	产品资质	应标产品具备独立的高级可持续威胁（APT）安全监测产品的销售许可证（增强级），需提供证明材料并加盖公章。
			52	0		应标产品具备国家版权局软件著作权登记证书，需提供证明材料并加盖公章。
			注： 1.“参数性质”栏中划“0”表示此参数为一般性技术参数，划“0”表示此参数为重要技术参数； 2.一般参数、重要技术参数有负偏离的，按照响应程度做不同额度扣分处理； 3.招标人有权要求中标人在合同签署前提供产品进行所有招标要求功能及投标响应的逐一验证，符合招标方要求后才能执行合同流程，验证中发现虚假应标的行为将予以追究相关责任。			
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。					

附表三：安全管理中心设备　是否允许进口：否

参数性质	序号	具体技术(参数)要求			
		序号	**参数性质**	**技术指标**	**技术规格要求**
		1	√	硬件指标	2U标准机架式，冗余电源，专用千兆硬件平台和安全操作系统，≥6个千兆电口，≥2个SPF+接口，≥1个管理口，≥2个USB接口，≥1个接口可扩展插槽，CF卡启动，存储容量≥4TB。
		2	√	性能	综合处理性能不低于≥3000EPS，管理中心的并发监控任务个数可以达到≥200个。
		3	√	管理对象	支持≥50个管理对象授权。
		4	0	运行环境	系统必须采用B/S架构，管理员只需浏览器即可连接到系统进行各种操作。
		5	0		产品要求集成数据库，无须再独立安装数据库系统，亦无须对数据库进行专门的维护。
		6	0	使用界面	系统必须采用基于浏览器的用户界面，至少支持IE、Firefox、谷歌。
		7	0	管理范围	涵盖网络设备、安全设备、主机、数据库、中间件以及各种应用系统

8	0	部署方式	支持单级部署和级联部署，支持分布式部署。
9	0		单级部署：无需安装任何其他软件和组件，用户只需要安装管理中心即可实现对全网资源的安全管理；
10	0		级联部署：两个管理中心之间可以进行级联，形成大规模统一管理；
11	0		分布式部署：一个管理中心可以连接多个分布式事件及性能采集器或者日志代理，实现对全网分散IT资源的统一管理
12	0	综合展示	用户登录即可进入综合展示界面。通过该界面，能够快速的导航到各个功能；
13	0		用户可以自定义一级功能菜单，可以根据自身需要调整一级功能菜单的顺序；
14	0		在综合展示界面中能够显示系统的环境状态信息（至少包含CPU、内存、磁盘信息）、基本管理信息，包括最近24小时资产告警排行、最近10条告警、最近1小时事件类型TOP、最近24小时告警分布。
15	0		可展示最近1小时和1天的事件趋势曲线和告警趋势图，事件总数和采集事件数同比前1个小时的变化量及百分比，可展示最新1小时内各等级事件数量【提供截图】
16	0		可展示最近24小时活跃日志源TOP、最近24小时活跃设备类型TOP【提供截图】
17	0	工作台	工作台为用户提供了一个从用户自身业务需要出发使用本系统的快速入口。用户可以在工作台中自定义仪表板，按需设计仪表板显示的内容和布局，可以为不同角色的用户建立不同维度的仪表板；
18	0		仪表板中的每个显示区域都能够放大、缩小、拖动【提供截图】；
19	0		1、系统具有资产管理的功能，能够将被管理IT资产进行分组、分域的统一维护，支持对资产增删改查以及批量导入导出。支持IP地址组为维度指定相关安全策略。
20	0		2、系统提供基于资产的拓扑视图，可以显示资产之间的逻辑连接关系。系统可以按列表和拓扑两种模式显示资产拓扑节点，且支持一键切换【提供截图】；
21	0		3、用户可以手工编辑资产拓扑，包括添加节点，添加/编辑连线，任意拖动节点，可以对拓扑图进行缩放，可以更换拓扑图背景；

			22	0	资产管理	4、在资产拓扑上和列表上选择每个资产节点，可查看该资产的相关属性、事件信息、核查信息、告警信息、性能信息、漏洞信息和风险信息等，并且支持向下钻取，直接进入事件列表、关联告警列表【提供截图】；
			23	0		5、支持资产多个数据维度的图形化展示能力，包括基于资产的漏洞趋势、事件趋势、告警趋势、性能趋势图【提供截图证明】
			24	0		6、可展示资产的CPU、内存、磁盘使用率信息，安全属性信息（包括机密性、完整性、可用性性、资产价值、等保级别等），可对资产进行安全评分。
			25	0		7、支持根据日志信息和漏扫信息进行自动识别新的资产，并支持自动添加到资产清单中去；
			26	0		8、用户可以对资产定义标签，实现对资产属性的动态扩展。
			27	0	日志采集	1、无需另外安装软件组件，管理中心即可通过SNMPTrap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、SFTP、NetBIOS、OPSEC等多种方式完成日志收集功能；可灵活定制不支持的数据源采集，而无须改动代码。
			28	0		2、支持对es、kafka、http/https、国产化数据库、内存数据库、VMWare应用日志的采集。支持转存kafka日志【提供截图】。
			29		日志范式化	系统必须具备日志范式化功能，实现对异构日志格式的统一化；范式化字段至少应包括事件接收时间、事件产生时间、事件持续时间、用户名称、源地址、源MAC地址、源端口、操作、目的地址、目的MAC地址、目的端口、事件名称、事件摘要、等级、原始等级、原始类型、网络协议、网络应用协议、设备地址、设备名称、设备类型等；
			30	0		产品界面支持范式化文件的导入导出功能。【提供截图】
			31	0		支持智能范式化，可自动对日志字段进行解析识别、图形化编辑配置【提供截图】
			32	0		可对配置文件进行管理，界面展示每个解析文件中的所有解析规则，并可编辑调整【提供截图】
			33	0	日志转发	支持加密压缩方式转发，定时转发【提供截图】。
			34	0		支持对无用日志的进行自动过滤和合并，减少

					垃圾数据数量；
			35	0	过滤条件可以按照所有范式化后的字段属性来定义。
			36	0	支持建立日志合并规则，支持自定义合并的时间范围【提供截图】。
			37	0	系统可以统计不同采集器和不同安全域下的设备个数并以饼图展示，统计采集器或安全域中事件量Top10以柱图展示，配以统计列表；【提供截图】
			38	0	系统可以统计不同采集器和不同安全域下周期【小时\天\周\月】范围内的事件趋势、设备接入比、事件范式化比、事件量设备TOP、接收事件速率趋势、接收事件和范化事件量、范式化成功率等信息，并均可图表化展示【提供截图】
			39	0	可以根据日志源断点时间进行配置，并生成告警【提供截图】
			40	0	支持实时监视策略的形式查看安全事件；可查看事件范式化信息和原始信息。
			41	0	可以显示一段时间的动态事件移动图，能够在图上显示每个时间切片的事件数量、等级，并能够在图上显示每秒事件数【提供截图】。用户点击每个时间切片，可以查看该切片内的事件；
			42	0	可以对事件依据其源目的IP和端口信息进行深入的事件追踪调查，支持无限次数的追踪调查；
			43	0	支持选择某条日志进行事件响应，响应动作包括生成告警、加入观察列表、加入威胁情报和生成解析规则、关联解析规则等；【提供截图】；
			44	0	可以对选中的事件源/目的IP地址进行全球地图定位，包括在线定位和离线定位【提供截图】；
			45	0	可以对选中的事件进行事件拓扑分析，并可视化的展示一幅描述事件之间相互关系的的事件拓扑图【提供截图】；
			46	0	可以以图形化的方式展示日志属性之间的聚合关系，显示多维事件分析图【提供截图】；
			47	0	可以对选中日志进行视网膜视图分析，以可视化方式展示日志的源IP与目的IP分布走向。【提供截图】；
					支持对安全事件进行实时和历史统计分析，根

			48	0	事件统计分析	据统计结果可直接钻取符合条件的事件，统计策略支持导入导出，统计结果支持导出。
			49	0		内置大量统计策略并支持策略搜索，具体分类上包括综合分类、设备分类、事件分类、系统事件、性能事件、宏观监测、漏洞事件和风险事件等八类，【提供截图】；
			50	0	事件查询	可对安全事件进行模糊搜索查询；
			51	0		自定义事件查询策略，基于事件分类的查询条件不少于10大项50小项【提供截图】；
			52	0		自定义事件查询策略，基于操作方式的查询条件不少于6大类50小项【提供截图】；
	1		53	0	基于规则的事件实时关联分析	安全事件实时关联分析能力，支持基于图形化方式的规则编辑器；规则支持新增、删除、移动、复制、导入、导出、启用和禁用等动作；【提供截图】
			54	0		编写具体关联分析规则时，可以引用相关知识和案例；【提供截图】
			55	0		在编辑规则条件的时候，可以针对事件属性引用规则、应用资产分类、引用漏洞、引用观察列表和引用威胁情报等【提供截图】；
			56	0		具备测试功能，分析师能够更方便地对新设计的关联规则进行模拟测试，以便调校规则的作用效果【提供截图】
			57	0		具有多级关联的能力，即一次关联后的事件可以跟其他事件再次关联，并不断的延展下去，二次关联，三次关联等等，深度不限，即支持多事件关联，对不同来源的安全事件进行复杂的相关性分析【提供截图】；
			58	0		提供图形化化展示自定义规则数统计、规则启用数统计、规则命中数TOP的统计
			59	0	弱点管理	系统具有弱点管理功能，能够导入资产的弱点信息，并计算资产/安全域/业务系统的脆弱性值。
			60	0		支持主流漏扫导入漏扫结果。
			61	0		系统能够通过多种方式展示资产/安全域/业务系统的弱点信息，可以查看单个资产的弱点，可以查看某个安全域的弱点值；
			62	0		系统具备漏洞库，所有导入的漏洞信息都可以检索，用户可以编辑漏洞信息。
			63	0		系统通过内置的风险计算模型，综合考虑资产的价值、脆弱性和威胁，计算风险的可能性和风险的影响性；

			64	0	风险评估	能够定期自动地计算出资产、安全域和业务系统的风险值，并刻画出资产、安全域和业务系统随时间变化的风险变化曲线，支持风险钻取与分析；
			65	0		系统能够形象地展示出安全域的风险矩阵【必须提供风险矩阵截图】，从可能性和影响性两个角度标注安全域中资产风险的分布情况，通过风险矩阵法，指导管理员进行风险分析，采取相应的风险处置对策；
			66	0		能够显示任意安全域的威胁Top10资产，风险Top10资产；
			67	0	宏观监测	通过对单位时间内的海量事件进行熵值计算，得出安全事件报送IP聚合度的变化幅度，以此来刻画这段时间内这些安全事件所属网络的安全状态，并预测下一步的整体安全走势
			68	0	告警管理	告警动作支持告警重定义、弹出提示框、播放警示音、发送邮件、发送SNMPTrap、发送短信、执行命令脚本、设备联动、发送飞鸽传书、光告警、发送Syslog、设置观察列表等方式；支持设备联动，执行命令行脚本。
			69	0		告警内容可以自定义，可以根据日志的实际情况将参数（即预定义变量）传递给命令行脚本；
			70	0		用户可以对告警进行查询，导出查询结果；支持根据关联规则进行告警信息查询【提供截图】；
			71	0		具备告警抑制功能，可以把同一时间内相同的告警合并成一条事件进行展示；告警抑制规则中的时间范围与合并数目可以手动进行配置，告警抑制规则可实时启用和停用。
			72	0		可对告警进行分级统计展示，并支持分类查询。具备告警的批处理能力，追溯能力。
			73	0		支持告警的生命周期管理，可对每条告警事件从告警来源、中间处理过程到最终响应进行图形化流程展示【提供截图】
			74	0		支持告警处置建议的配置
			75	0		支持通过文本采集、目录采集的方式进行告警采集【提供截图】
			76	0		支持以派发工单的形式进行告警响应。
			77	0		系统允许管理员以告警统计策略的形式从各个维度进行告警信息进行统计分析；
			78	0		用户可自定义告警统计策略，并以树形结构进行组织，形成一棵告警统计策略树【提供截图

				】；
		79	0	告警统计策略的条件和时间段可自由设定；
		80	0	系统内置了资产、事件、监控、风险等报表报告，且内置报表编辑器，可以自定义报表。
		81	0	提供内置报表模板；
		82	0	支持按照天、月度、季度、年度等时间周期生成报表，并支持邮件自动投递；
		83	0	支持在报表中以柱状图、曲线图、饼状图方式统计安全报警情况；
		84	0	报表管理 支持报表报告的导出，导出的格式支持PDF、HTML、PNG、DOCX、XLSX、RTF、XLS等格式；
		85	0	系统内置报表编辑器，可以自定义报表。
		86	0	提供内置报告模板，支持自定义模板，可自动生成周报、月报报告。
		87	0	支持新增、删除、启动、停用报告模板，点击可查看模板详情，以及该模板生成的所有报告
		88	0	系统提供开放的知识管理功能，内置了大量的安全知识，包括：案例库、漏洞库、事件分类库、字典库等；同时也允许用户在系统使用过程中不断丰富和完善。
		89	0	用户可以对所有的知识点进行基于关键字的全文检索。
		90	0	系统内置日志字典库，方便用户查询不同原始日志信息的错误ID号和详细描述信息
		91	0	知识管理 内置交换机的事件编码知识库【提供截图】；
		92	0	内置Windows、Linux、Solaris、AIX操作系统的事件ID知识库【提供截图】；
		93	0	内置Oracle、SQLServer、MySQL、Informix、DB2数据库的事件编码知识库【提供截图】；
		94	0	支持查看系统内置的事件库中事件类型名称及其描述信息【提供截图】。
		95	0	系统允许上级管理中心对下级管理中心的节点进行集中管理和展示，上级管理中心可以访问下级管理中心；
		96	0	级联管理 在上级管理中心，可以对下级管理中心的节点进行配置和监控；
		97	0	上级节点可以统一对下级节点下发日志的解析策略【提供截图】。
		98	0	支持对系统自身的CPU、内存、数据库空间大小等进行监控，并支持设置使用率告警阈值【

				提供截图】；
99	0	系统管理	支持系统时间同步，能够指定时钟服务器，确保安管平台系统与用户网络环境的时间保持同步【提供截图】。
100	0		可分析长期和短期事件的实时关联分析，可将关注的事件或符合条件的事件保存至观察列表中供后续规则读取并关联；
101	0		可记录系统自身日志，可查询；
102	0		系统内置实时抓包工具。【提供截图】
103	0		系统内置多种解码工具，包括Unicode\UTF-8\URL\HEX\BASE64\时间戳转换等【提供截图】
104	0		系统支持在页面进行网口配置、路由配置【提供截图】
105	0		系统支持本地备份和远程备份，包括FTP\SFTP\SMB等【提供截图】
106	0	权限管理	实现基于角色的权限管理，所有的用户的权限都通过角色来赋予；
107	0		要求系统管理员、用户权限管理员和审计管理员三权分立；系统内置上述三类管理员。
108	0	资产对象	支持资产管理IP类型资产，包括主机、网络设备、数据库、中间件、安全设备、应用系统、机房设备等
109	0	日志富化	支持对采集到的日志进行归一化处理并保留原始日志。具备数据归一化功能，且能够补全源和目的IP地址等信息
101	0	产品要求	产品须获得中华人民共和国公安部的《计算机信息系统安全专用产品销售许可证》，并出具产品检验报告，并且该产品检验报告必须符合公安部《信息安全技术安全管理平台产品检验规范》，需提供证明材料并加盖公章。
102	0		应标产品具备国家版权局软件著作权登记证书，需提供证明材料并加盖公章。

注：

1.“参数性质”栏中划“0”表示此参数为一般性技术参数，划“0”表示此参数为重要技术参数；

2.一般参数、重要技术参数有负偏离的，按照响应程度做不同额度扣分处理；

3.招标人有权要求中标人在合同签署前提供产品进行所有招标要求功能及投标响应的逐一验证，符合招标方要求后才能执行合同流程，验证中发现虚假应标的行为将予以追究相关责任。

说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。

附表四：服务器密码机　是否允许进口：否

参数性质	序号	具体技术(参数)要求

序号	参数性质	技术指标	技术规格要求
1	√	硬件规格	2U机架式设备，要求配备不少于4个10/100/1000 Base-T千兆电口、1个RJ-45管理口、1个RS232 串口、1个HA口、6个USB 接口、2个万兆SFP+插槽，具备冗余电源；具备液晶显示屏。
2	√		要求配备服务器密码机管理员KEY、审计员KEY、操作员KEY，用于服务器密码机的安全管理。
3	0		支持液晶屏显示信息。
4	√	系统性能	对称密钥存储容量：≥2000个
5	√		非对称密钥存储容量：≥4000对
6	√		SM2密钥对产生速率：≥6800对/秒
7	√		SM2签名速率：≥10000次/秒
8	√		SM2验签速率：≥4000次/秒
9	√		SM3计算Hash速率：≥850Mbps
10	√		SM1加解密速率：≥850Mbps
11	√		SM4加解密速率：≥850Mbps
12	√		最大并发数：≥5000
13	0	支持算法	对称算法支持：SM1、SM4、SM7、SSF33、ZUC、DES/3DES、AES等； 非对称算法：SM2、SM9、RSA、DSA、ECDSA、EdDSA等； 杂凑算法：SM3、SHA-1、SHA-2等。 需提供证明材料并加盖厂商公章。
14	0	支持接口	服务器密码机支持GM/T 0018-2012《密码设备应用接口规范》定义的接口规范，同时支持PKCS#11、JCE、CSP等国际标准接口。
15	0		要求业务通道和管理通道均支持国密SSL协议；
16	0		要求系统采用三层密钥结构保障密钥及系统安全性，保证关键密钥在任何时候不以明文形式出现在设备外，同时要求密钥备份文件受备份密钥的加密保护；需提供证明材料并加盖厂商公章。
17	0		要求支持主-备模式、主-主模式、多机集群模式，保证系统运行和密钥存储的可靠性；
18	0		要求支持物理防撬密钥保护机制，一旦非法撬动机箱会自动触发密钥自毁功能，能够有效保护服务器密码机内部密钥安全；
19	0		要求支持随机数服务功能，须采用国家密码管理局认可的双 WNG8物理噪声源芯片生成真随机数。

		20	0	系统功能	要求支持密钥存储功能，能够为第三方应用系统提供安全的密钥存储与管理。
		21	0		要求能够以接口服务的方式提供数据加解密、数据完整性保护等密码运算功能。
		22	0		要求服务器密码机支持对用户进行管理，采用基于角色的访问控制方式，能够针对不同管理员给予不同的操作权限；
		23	0		具备系统监测功能，可对用户连接数、应用访问情况、系统资源占用情况进行实施监测和统计分析。具备认证一致性、自动登录策略统一下发、错误重定向、访问控制等功能
		24	0		具备证书管理、证书有效性验签、动态黑名单、多证书链、获取证书信息、RSA和国密算法双证、国密算法双证功能。
		25	0		要求具备国家密码管理局颁发的《商用密码产品认证证书》，提供证书复印件；需提供证明材料并加盖厂商公章。
		26	0	产品资质	具备国家版权局颁发的《计算机软件著作权登记证书》，提供证书复印件；需提供证明材料并加盖厂商公章。
		注： 1.“参数性质” 栏中划“0”表示此参数为一般性技术参数，划“0”表示此参数为重要技术参数； 2.一般参数、重要技术参数有负偏离的，按照响应程度做不同额度扣分处理； 3.招标人有权要求中标人在合同签署前提供产品进行所有招标要求功能及投标响应的逐一验证，符合招标方要求后才能执行合同流程，验证中发现虚假应标的行为将予以追究相关责任。			
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。				

附表五：上网行为　是否允许进口：否

参数性质	序号	具体技术(参数)要求			
		序号	参数性质	技术指标	技术规格要求
		1	0	硬件规格	标准1U设备
		2	√		≥12GE(电)+12SPF(光)，2个SPF+接口，存储容量≥500G。
		3	√	性能要求	网络层吞吐量≥8G，应用层吞吐量≥4G，带宽性能≥800Mbps，支持用户数≥4000，每秒新建连接数不少于20万，并发连接数不少于300万。
		4	0		支持路由模式、透明（网桥）模式、混合模式，支持镜像接口，部署模式切换无需重启设备
		5	0		支持静态路由、策略路由、动态路由、ISP路由；策略路由支持七元组策略；动态路由支持RIP、OSPF等；ISP路由支持运营商地址自定义。
		6	0		支持IPV6网络，可对IPV6网络进行审计、流量控制。
		7	0		支持4G网络，在主线路出现问题时，自动切换到4G网络，保障网络正常运

		7	0	部署适应性	行（提供功能截图并加盖厂商公章）
		8	0		网络部署支持虚拟网线部署，且支持vlan标签的过滤（提供功能截图并加盖厂商公章）
		9	0		支持针对链路质量的实时监控（提供功能截图并加盖厂商公章）
		10	0		支持服务器负载均衡，支持一个公网IP映射到内网多台服务器，服务器间支持连接和源地址hash,支持服务器健康检查（提供功能截图并加盖厂商公章）
		11	0	行为管控	系统内置多个常见场景的应用标签，且标签支持管理员自定义。（提供web截图）
		12	0		用户管理、应用管理支持树型结构。（提供功能截图并加盖厂商公章）
		13	0		支持HTTPS解密功能，支持页面及命令行配置解密策略，包括入接口、源地址对象、目的地址对象、https对象、域名排除等。支持针对HTTPS网站、HTTPS搜索记录、HTTPS邮箱等内容进行审计；HTTPS邮箱支持审计主题、内容、附件等；支持HTTPS域名库，预定义域名以及自定义域名；
		14	0		基于P2P行为和迅雷行为的应用智能识别技术。（提供功能截图并加盖厂商公章）
		15	0		支持广告推送功能，支持PC端推送4个方位（针对电脑屏幕上下左右）的广告，手机端支持推送全屏广告提供（提供功能截图并加盖厂商公章）
		16	0		支持支持基于邮件收件人、发件人的黑白名单自定义控制方式（提供功能截图并加盖厂商公章）
		17	0		应用特征数支持6800+（提供功能截图并加盖厂商公章）
		18	0		支持终端类型检测和控制，以及显示终端趋势（提供功能截图并加盖厂商公章）
		19	0		针对系统运行过程中的应用统计，支持应用的热度图（提供功能截图并加盖厂商公章）
		20	0		基于全局白名单功能，可针对IP和MAC地址（提供功能截图并加盖厂商公章）
		21	0		终端提示页面基于代码层面的用户自定义（提供功能截图并加盖厂商公章）
	1	22	0	上网认证	支持WEB Portal认证功能，支持本地认证、Radius认证、LDAP认证 和LDAP用户同步，支持对接IMC、SAM等常见AAA服务器，支持配置强制重新认证间隔，支持配置认证通过后重定向URL，要求本机自身支持短信认证功能。
		23	0		支持二维码认证，终端可以通过管理员扫描二维码授权方式上网（提供功能截图并加盖厂商公章）
		24	0		支持旁路部署WEB认证（提供功能截图并加盖厂商公章）
		25	0	策略配置	提供智能策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查，并可在WEB界面显示检测结果；支持实时和周期性对所有安全策略进行分析。 (提供功能截图并加盖厂商公章)
		26	0		独立的控制策略和审计策略，精准匹配（提供功能截图并加盖厂商公章）
		27	0		支持杀毒功能，可对HTTP、FTP、POP3、SNMP、IMAP协议的病毒进行查杀；支持ZIP、RAR等压缩文件的病毒查杀。压缩默认支持5层，最大20层（提供功能截图并加盖厂商公章）

		28	0	安全防护	提供WEB防护功能，可对防盗链、CSRF攻击、CC等攻击行为进行防护。（提供功能截图并加盖厂商公章）
		29	0		支持端口扫描功能，用于直观的了解网内主机所存在的安全问题。（提供功能截图并加盖厂商公章）
		30	0		支持弱密码扫描功能，即时了解网内主机是否存在弱口令，内置弱口令库，并可自定义字典库。（提供功能截图并加盖厂商公章）
		31	0		提供威胁情报功能，支持全网威胁情报的搜索查询，可供攻击溯源，预知风险；支持威胁情报订阅，及时对突发威胁进行防护建议；支持威胁分类，包括C&C、僵木蠕、勒索、钓鱼、垃圾邮件等（提供功能截图并加盖厂商公章）
		32	0		支持IPS功能，支持基于源、目的、规则集的入侵检测；支持针对WEB服务器防护，包括网页防爬虫、网页防篡改、DDOS攻击防护、WEB攻击过滤等。（提供功能截图并加盖厂商公章）
		33	0	其它	系统支持软件补丁升级，以及热补丁技术（提供功能截图并加盖厂商公章）
		34	0		支持ssl VPN，至少提供300个授权（提供功能截图并加盖厂商公章）
		35	0		系统管理员外部方式认证方式，外部认证服务器故障可以切换为本地认证（提供功能截图并加盖厂商公章）
		36	0		针对设备系统健康检测功能，可以在某一时间段内逐级深入，并篡取任一时间内的详细信息，并可路转系统日志。（提供功能截图并加盖厂商公章）
		37	0		支持应用、用户流量统计，应用流量支持趋势图、饼状图呈现，可查看某一应用的流量趋势图和其Top流量用户。
		38	0		内网资产监控，可对终端风险级别、操作系统、浏览器类型、应用、杀毒软件等方面进行监控（提供功能截图并加盖厂商公章）
		39	0	产品资质	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》
		40	0		产品具有国家版权局颁发的《计算机软件著作权登记证书》
		注： 1.“参数性质” 栏中划“0”表示此参数为一般性技术参数，划“0”表示此参数为重要技术参数； 2.一般参数、重要技术参数有负偏离的，按照响应程度做不同额度扣分处理； 3.招标人有权要求中标人在合同签署前提供产品进行所有招标要求功能及投标响应的逐一验证，符合招标方要求后才能执行合同流程，验证中发现虚假应标的行为将予以追究相关责任。			
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。				

附表六：VPN设备　是否允许进口：否

参数性质	序号	具体技术(参数)要求			
		序号	参数性质	技术指标	技术规格要求
		1	√	网络接口	≥6电4光，2个扩展槽
		2	√	硬件参数	2U冗电，内置加密卡
		3	√		整机吞吐率：≥20Gbps
		4	√		最大并发连接数：≥400万
		5	√		每秒新建连接数：≥5.2万
		6	√		IPSec加密吞吐率：≥800M

		性能参数	
7	√		IPSec VPN隧道数：≥10000条
8	√		SSL VPN并发用户数：≥7000
9	√		SSL VPN每秒新建用户：≥4000
10	√		SSL VPN加密吞吐：≥800M
11	0	部署方式	产品支持网关模式、单臂模式、双机模式、集群模式的部署方式。
12	0		支持虚拟化软件部署方式
13	0	系统管理	支持多系统引导，可在管理员界面直接配置启动顺序，至少支持两个操作系统，管理员可自由选择当前启动系统，每个系统拥有独立的配置文件，且分别支持加密导入导出，需提供证明材料并加盖厂商公章。
14	0		支持管理员分权管理，支持三权分立，包括系统管理员，安全管理员，审计管理员；支持自定义权限模板，为管理员分配管理权限，需提供证明材料并加盖厂商公章。
15	0		支持分级管理，将用户组、资源、角色按照组织架构进行分级管理，可以为各级别管理员分别创建管理员，并可逐级授权。，需提供证明材料并加盖厂商公章。
16	0		支持配置管理主机IP，仅开放白名单地址访问权限，支持管理员口令复杂度设置，自定义管理员证书，提高管理员身份认证强度，需提供证明材料并加盖厂商公章。
17	0		支持全局配置安全检查，支持一键加固风险配置项，需提供证明材料并加盖厂商公章。
18	0		支持远程SSH和串口命令行配置,支持基于WEB界面的CLI命令行功能，需提供证明材料并加盖厂商公章。
19	0	基本功能	专业 IPSec VPN和 SSL VPN二合一设备，采用符合国际标准SSL、TLS 协议，同时支持IPSec VPN和SSL VPN功能，为非插卡或防火墙带VPN模块设备。
20	0		内置硬件商密加密卡，采用国家商用密码算法实现隧道加密，支持国家商用密码算法包括:SM1/SM2/SM3/SM4
21	0		支持PC终端使用包括Windows、Mac OS、Linux 等主流操作系统来登录SSL VPN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；支持IOS或Android等操作系统的智能手机、PDA、平板电脑（PAD）等移动终端的SSL VPN接入，或通过PPTP、L2TP VPN方式接入；
22	0		支持终端使用包括IE6、7、8、9、10、11或其他IE内核的浏览器，以及最新版本的非IE内核浏览器，如Windows Edge，Google Chrome， Firefox，Safari，Opera等浏览器登录SSL VPN网关，登录后可完整支持各种IP层以上的B/S和C/S应用。
23	0		支持龙芯、兆芯、飞腾、鲲鹏等国产化平台，支持中标麒麟，银河麒麟，普华、深度（deepin）、优麒麟、UOS统信操作系统、中科方德等国产化操作系统；（提供至少两种国产化操作系统的证明）
24	0		支持国际密码算法包括：AES、DES、3DES、DH、RSA、RC4、MD5、SHA1 SHA2；

		25	0		支持自定义虚拟门户，可在一台设备上为不同用户群配置多种登录门户，支持域名或者IP地址访问。
		26	0	虚拟门户	登录门户支持自定义主题模板，包括基本信息、登录页面logo、欢迎页面等，支持中英文切换，
		27	0		支持登录门户加密协议选择，TLS1.2/1.1/1.0 SSL3.0/2.0； 支持加密算法套件选择RSA_DES_CBC_SHA，RSA_RC4_MD5， RSA_RC4_SHA，RSA_WITH_AES_SHA；支持安全密钥更新周期设置；需提供证明材料并加盖厂商公章。
		28	0	SSL VPN	支持配置多种资源类型，包括WEB应用、TCP/UDP应用，NC应用；同时支持资源负载均衡，可控制终端接入类型，如PC端（浏览器）、移动端（Android/iOS）、SDK，需提供证明材料并加盖厂商公章。
		29	0		支持WebVPN跨平台免插件访问，支持基于泛域名发布Web资源，自动进行URL改写，无需手动修正Web参数，无需启动虚拟网卡建立三层VPN，解决动态页面和外链资源无法正常显示问题，简化资源发布流程和提升访问体验
		30	0		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。支持CS单点登录工具助手，支持自动识别登录窗口自动形成配置文件。，需提供证明材料并加盖厂商公章。
		31	0		支持设置SSL代理模式，可选择用户以VPN 接口IP、源地址、或为用户分配独立虚拟IP 模式，来访问应用便于对用户访问行为进行审计溯源，需提供证明材料并加盖厂商公章。
		32	0		支持QuickLink资源映射，支持单向认证、双向认证，支持自定义登录门户加密协议选择，TLS1.2/1.1/1.0 SSL3.0/2.0； 支持加密算法套件选择RSA_DES_CBC_SHA，RSA_RC4_MD5， RSA_RC4_SHA，RSA_WITH_AES_SHA
		33	0		支持IPSec、SSL 、PPTP、L2TP VPN的统一用户管理和认证体系，实现用户名口令一次配置，即可适用于全部VPN类型接入，无需分别购买不同类型VPN接入授权，需提供证明材料并加盖厂商公章。
		34	0		支持用户组及用户分级管理，支持上下级认证策略、关联角色、认证方式的继承关系配置，需提供证明材料并加盖厂商公章。
		35	0		支持基于用户组的并发用户数限制，需提供证明材料并加盖厂商公章。
		36	0		支持口令认证、Radius、LDAP、CAS、AD、本地动态令牌，第三方动态令牌、CA证书、短信等认证方式，支持多因素认证方式自由组合，支持调整认证顺序
		37	0		支持CAS认证服务联动，通过简单配置即可实现基于身份票据的单点登录，需提供证明材料并加盖厂商公章。
		38	0		支持丰富的短信认证类型，支持短信猫、CMPP2.0/3.0、SGIP1.2、SMGP3.0等短信认证模板，支持基于http、webservice接口的自定义短信网关模板，无需二次开发支持主流的互联网短信网关厂家，需

					提供证明材料并加盖厂商公章。
		39	0	用户认证	支持自定义口令强度策略，支持软键盘、动态附加码，支持强制首次登录修改口令、定期更改口令，支持口令、动态令牌、短信防爆破，支持短信防恶意发送，需提供证明材料并加盖厂商公章。
		40	0		支持通过WEB界面对第三方认证服务器进行连通性测试
		41	0		支持LDAP用户信息直接导入本地，导入过程可以支持用户组选择，支持与本地用户列表的重复性判断配置，需提供证明材料并加盖厂商公章。
		42	0		支持配置Radius、LDAP组映射属性，支持根据Radius的CLASS、NAS-ID、User-Name ,LDAP的DN等或者自定义属性将远程用户信息映射到本地用户组，需提供证明材料并加盖厂商公章。
		43	0		支持角色映射,支持将LDAP角色属性映射到VPN本地角色，支持一个LDAP用户映射多个角色。，需提供证明材料并加盖厂商公章。
		44	0		支持内置PKI，内置CA可根据请求文件离线签发证书，同时支持在线申请证书，支持导入第三方CA，支持基于SCEP协议在线获取数字证书
		45	0		支持符合SAML框架规范的单点登录功能，需提供证明材料并加盖厂商公章。支持对象属性认证和资源权限调用，无需传递应用系统用户名口令，即可实现单点登录
		46	0	可信接入	支持硬件特征码绑定，支持硬盘序列号、MAC地址绑定，特征码信息无需用户手动设置输入可自动生成，支持自定义用户绑定终端数量。支持硬件特征码批量导入导出。，需提供证明材料并加盖厂商公章。
		47	0		支持自定义终端信息注册模板,可以有管理员自定义终端审核时填写的信息，可以自定义输入框，下拉菜单 单选和多选按钮，设定必填和可编辑等属性。，需提供证明材料并加盖厂商公章。
	1	48	0		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
		49	0		可基于用户和角色设定准入策略，针对操作系统、操作系统补丁、浏览器、进程、服务、端口、文件、注册表、登录IP、时间、凭证、终端指纹进行登录前和使用时定期检查
		50	0		支持接入策略配置，可以设定用户退出时清除Internet缓存文件、Cookie、浏览器历史记录、保存的表单等。提供证明材料并加盖厂商公章。
		51	0		支持会话策略配置，可设定使用VPN时仅能访问内网资源，禁止对互联网的访问，支持登录超时限制时间功能。，需提供证明材料并加盖厂商公章。
		52	0		支持终端环境诊断排查，提供终端诊断工具，支持Windows、MAC系统，支持对当前终端的基本环境进行扫描和一键修复。
		53	0		IPSec VPN支持网关、单臂部署模式，IPSec VPN支持透明、路由、冗余等网络接入方式，需提供证明材料并加盖厂商公章。
		54	0		支持IPSec隧道组和隧道热备份，多条链路IPSec隧道接入时，确保传输稳定可靠，需提供证明材料并加盖厂商公章

			稳定可靠，需提供证明材料并加盖厂商公章。
55	0	IPSec VPN	支持IPSec VPN隧道间路由实现隧道接力，减少多级组网时的隧道数量，需提供证明材料并加盖厂商公章。
56	0		支持隧道内关联地址组，只需配置一条隧道，即可关联多个保护子网
57	0		支持IPSec手动隧道，手动输入密钥参数，无需协商，可以满足IPSec VPN跨越单向光闸传输加密要求，需提供证明材料并加盖厂商公章。
58	0		支持DMVPN动态组网功能，网络扩展时仅需配置新增节点，无需配置原中心节点和分支节点，即可扩展VPN网络，需提供证明材料并加盖厂商公章。
59	0		支持IPSec隧道例外规则添加，支持在大网段中设定例外地址流量不进入加密隧道，需提供证明材料并加盖厂商公章。
60	0	IPv6	支持Ipv6地址配置，支持Ipv6路由表，支持Ipv6静态路由、策略路由、支持运营商Ipv6地址池
61	0		支持Ipv6 to Ipv4隧道，支持Ipv6的两端保护子网在Ipv4网络上建立隧道，需提供证明材料并加盖厂商公章。
62	0		SSL VPN IPSec VPN 同时支持本地网络与传输网络网络Ipv6 Ipv4类型不一致的远程隧道传输。
63	0		支持Ipv6防火墙访问控制策略、带宽策略；支持Ipv6 SNAT、端口映射、IP映射
64	0		支持Ipv6会话管理、会话统计
65	0	访问控制	支持访问控制策略配置，可基于源目的地址、端口，服务，时间的访问控制策略，支持带宽管理策略，支持IP/MAC地址自动探测与绑定
66	0		支持全局抗攻击功能（包括抗地址欺骗、抗源路由攻击、抗SMURF攻击、抗LAND攻击、抗WINNUKE攻击、抗QUESO扫描、抗SYN/FIN扫描、抗NULL扫描、抗圣诞树攻击、抗FIN扫描、抗Ping of Death）支持基于包过滤规则的抗SYN FLOOD、抗UDP FLOOD、抗ICMP FLOOD和IP会话数控制，需提供证明材料并加盖厂商公章。
67	0	高可用性	在NAT、路由、透明模式下支持A-A,A-S模式，支持集群部署模式，且切换时间小于3秒，并支持防火墙相关状态同步技术
68	0		支持主备模式下，定时同步在线用户，主备切换时，SSL VPN在线用户不掉线，无需重新认证
69	0		负载均衡支持NAT 和 DR 模式，确保分发器故障时可以自动重新选举分发器。支持多个虚拟组，可以为用户提供多个负载均衡集群，需提供证明材料并加盖厂商公章。
70	0	状态监控	支持系统状态监控，支持首页一览，包括CPU、内存使用率，网口状态、IP地址、接口速率，支持实时查看IPSec隧道数量、SSL在线用户数、整机吞吐以及SSL VPN/IPSec VPN/L2TP/PPTP/HA等服务启用情况
71	0		支持查看在线用户、在线设备和已锁定用户，支持自动刷新，可自定义刷新频率。支持多维度信息展示，包括用户名、用户组、源IP、虚拟IP、认证方式、终端类型、在线时间、流量情况等，支持批量强制在线用户、设备下线，支持批量解锁异常用户
72	0		支持本地存储日志，支持存储位置自定义，存储时长不小于6个月

		73	0	支持对接第三方日志服务器，仅需简单配置，即可实现日志外发
		74	0	支持异常信息告警，支持管理员页面、设备蜂鸣、邮件等告警方式
		75	0	支持查看系统日志、管理日志，支持基于在线时间、访问流量、登录次数等维度生成用户报表，支持基于资源名称、访问次数、访问流量等维度生成服务报表，支持报表导出
		76	0	支持日志导出、导入，支持一键清空日志
		77	0	支持Windows和MAC、Android、iOS操作系统下应用虚拟化功能，应用数据存储在服务器端，退出后本地不保存任何数据，需提供证明材料并加盖厂商公章。
		78	0	应用虚拟化数据传输过程中使用SSLVPN协议加密，保证了数据传输的合法性和安全性；
		79	0	应用虚拟化支持国产化操作系统，支持国产化CPU架构
		80	0	应用虚拟化符合用户使用习惯，比如：支持本地输入法、支持文件导入导出、支持打印等。地磁盘资源映射、本地打印机、本地串行口、本地智能卡，本地输入法；支持剪切板，并能够实现剪贴板数据流控制
		81	0	可以无需二次开发，即把Windows应用发布到移动智能终端中，也可以支持无需开发，将C/S资源Web化。，需提供证明材料并加盖厂商公章。
		82	0	应用虚拟化必须支持集群多主控和负载均衡策略，即当存在多台终端发布服务器时，可以根据预先配置策略将用户分配到不同的终端服务器。，需提供证明材料并加盖厂商公章。
		83	0	支持用户配置一键复制，提高部署效率，可以复制各种插件设置、cookie设置、权限设置等，需提供证明材料并加盖厂商公章。
		84	0	独立的统计报表统计通过应用虚拟化使用者登录情况、应用使用频次情况、服务器性能占用情况，需提供证明材料并加盖厂商公章。
		85	0	支持对数据上传下载的单向控制、双向控制，细粒度控制，支持根据黑白名单规则进行安全过滤
		86	0	支持服务器还原点配置和自动修复机制，可以自动下载所需软件，支持守护进程模块，会对系统核心服务与进行保护与值守，在WEB服务与核心进程服务出现问题时，可以3秒内自动修复并重启问题服务，保障整个平台的持续性
		87	0	支持私人网盘功能，可以在应用服务器创建只能由本人访问的存储区域；支持对数据上传下载的单向控制、双向控制，颗粒化控制；对上传文件能够根据黑白名单规则进行安全过滤
		88	0	VPN产品在用户登录前，进行桌面管理软件进行检查并给出提示，必须安装终端管理系统才能够登录，支持终端进行黑白红名单，支持注册表检查，支持防病毒软件版本检查，和病毒库更新检查。
		89	0	支持终端屏幕水印和点阵式水印，水印内容支持显示终端特征信息、支持自定义文字或图片，防止对录屏、截屏、拍照等行为获取到的页面或数据进行利用。
				可支持终端本地查看包含敏感信息文件信息。采用自有文档解析的技

		90	0		术，识别不需要安装任何Office组件或第三方文档解析组件。支持基于终端的常用泄密途径的监控，支持文件拷贝、粘贴板、打印、刻录、QQ、邮件、web、FTP等行为。能够定义终端自动响应规则。响应规则支持记录、警告、阻止、使用人确认、拷贝加密等。支持全盘或指定位置检查是否存在敏感文件及文件敏感等级等信息，无需周期性扫描检查。
		91	0	产品资质	具备公安部颁发的，《计算机信息系统安全专用产品销售许可证》（要求出具证书复印件和公安部检测报告复印件
		92	0		具备国家版权局颁发的《计算机软件著作权登记证书》，要求出具证书复印件
		93	0		具备国家密码管理局商用密码检测中心颁发的《商用密码产品认证证书》要求出具证书复印件
		注： 1.“参数性质”栏中划“0”表示此参数为一般性技术参数，划“0”表示此参数为重要技术参数； 2.一般参数、重要技术参数有负偏离的，按照响应程度做不同额度扣分处理； 3.招标人有权要求中标人在合同签署前提供产品进行所有招标要求功能及投标响应的逐一验证，符合招标方要求后才能执行合同流程，验证中发现虚假应标的行为将予以追究相关责任。			
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。				

附表七：签名验签服务器　是否允许进口：否

参数性质	序号	具体技术(参数)要求			
		序号	参数性质	技术指标	技术规格要求
		1	√	硬件规格	2U机架式设备，要求配备不少于4个10/100/1000 Base-T千兆电口、1个RJ-45管理口、1个RS232 串口、1个HA口、6个USB 接口、2个万兆SFP+插槽，具备冗余电源；具备液晶显示屏。
		2	0		要求配备签名验签服务器管理员KEY、审计员KEY、操作员KEY，用于签名验签服务器的安全管理。
		3	0		支持液晶屏显示厂商名称信息。须提供产品外观图片。
		4	√	系统性能	SM2、RSA密钥对存储容量≥1024对
		5	√		SM2密钥对产生速率：≥3000对/秒
		6	√		SM2 PKCS1签名/验签速率：≥2900/2000次/秒
		7	√		SM2 PKCS7签名/验签速率：≥2500/1500次/秒
		8	√		SM2数字信封加解密≥400/500次/秒
		9	√		SM2带签名的数字信封封装解封≥240/300次/秒
		10	√		最大并发数≥1000
		11	0	支持算法	非对称算法支持：SM2、SM9、RSA、DSA、ECDSA、EdDSA等； 杂凑算法支持：SM3、SHA-1、SHA-2等。 需提供证明材料并加盖厂商公章

				需提供证明材料并加盖厂商公章。
		12	0	支持接口	要求支持符合GM/T 0018-2012《密码设备应用接口规范》。
1		13	0	系统功能	要求业务通道和管理通道均支持国密SSL协议；
		14	0		要求采用三层密钥结构保障密钥及系统安全性，保证关键密钥不以明文形式出现在设备外，同时要求密钥备份文件受备份密钥的加密保护；需提供证明材料并加盖厂商公章。
		15	0		要求支持主-备模式、主-主模式、多机集群模式，保证系统运行和密钥存储的可靠性；
		16	0		要求支持物理防撬密钥保护机制，一旦非法撬动机箱会自动触发密钥自毁功能，能够有效保护签名验签服务器内部密钥安全；
		17	0		要求支持随机数服务功能，须采用国家密码管理局认可的双 WNG8物理噪声源芯片生成真随机数。
		18	0		要求支持密钥存储功能，能够为第三方应用系统提供安全的密钥存储与管理。
		19	0		多应用支持：所投产品支持不同应用的证书及对应密钥的生成及存储；
		20	0		多信任域支持：支持配置不同的证书信任域，证书验证策略支持配置不验证、根证书、CRL、OCSP等多种验证策略；需提供证明材料并加盖厂商公章。
		21	0		数字签名/验证：所投产品支持基于SM2、RSA等算法的PKCS#1签名/验证、PKCS#7 Attached签名/验证、P7 Detached签名/验证功能；签名格式符合PKCS#7、GM/T0010等标准中定义的数据类型，需提供证明材料并加盖厂商公章。
		22	0		数字信封加密和解密：所投产品支持基于SM2、RSA等算法的数字信封加密、解密功能，数字信封格式符合PKCS#7、GM/T0010等标准中定义的数据类型；
		23	0		要求签名验签服务器支持对用户进行管理，采用基于角色的访问控制方式，能够针对不同管理员给予不同的操作权限；
		24	0	产品资质	要求具备国家密码管理局颁发的《商用密码产品认证证书》，需提供证明材料并加盖厂商公章。
		25	0		具备国家版权局颁发的《计算机软件著作权登记证书》，需提供证明材料并加盖厂商公章。
		注： 1.“参数性质”栏中划“0”表示此参数为一般性技术参数，划“0”表示此参数为重要技术参数；			

		2.一般参数、重要技术参数有负偏离的，按照响应程度做不同额度扣分处理； 3.招标人有权要求中标人在合同签署前提供产品进行所有招标要求功能及投标响应的逐一验证，符合招标方要求后才能执行合同流程，验证中发现虚假应标的行为将予以追究相关责任。
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。	

附表八：堡垒机　是否允许进口：否

参数性质	序号	具体技术(参数)要求

序号	参数性质	技术指标	技术规格要求
1	√	硬件要求	1U标准机架型设备，≥6个千兆电口，≥2个万兆光口，≥2个千兆光口，≥1个Console管理口，存储容量≥4TB，单电源，带液晶面板，≥2个扩展槽。
2	√	性能要求	字符协议≥700个 图形协议≥200个
3	0	IPV4/IPV6	支持在IPV4,IPV6，IPV4与IPV6网络环境下部署，提供功能截图并加盖厂商公章。
4	0	部署方式	物理旁路，逻辑串联模式，无需镜像、无需改造现有网络结构
5	0		单机部署、双机热备（HA)部署
6	0		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，提供功能截图并加盖厂商公章。
7	0		分布式部署： 支持添加一台或多台协议代理服务器，分担堡垒机主服务器性能压力，便于提高整体性能； 并支持限定不同的协议代理服务器节点访问不同的资源； 多协议代理服务器节点可访问相同资源时实现自动负载均衡；提供功能截图并加盖厂商公章。 堡垒机主服务器集中管理配置和收集展现日志信息。提供功能截图并加盖厂商公章。
8	0	分权分域	系统内置系统管理员、审计管理员、安全管理员三种角色，系统管理员可针对不同用户指定不同的管理权限，可设定用户（组）和资源（组）的管理范围
9	0		支持用户管理，包括添加、删除、启用、禁用、移动、修改功能
10	0		支持用户组管理，包括添加、删除、修改功能

			10	0	，支持IP地址组为维度指定相关安全策略；
			11	0	支持用户帐号的批量导入导出功能
			12	0	支持批量修改用户帐号属性
			13	0	用户管理	用户密码策略包括：最小密码长度（强制最小8位）、密码复杂度（小写字母，大写字母，数字，特殊字符）、不允许密码与用户一致设置，不允许密码与用户逆序，密码周期（过期前提醒）、历史密码对比
			14	0	支持用户帐号有效期配置
			15	0	支持IP和MAC限制，支持黑白名单两种工作模式，提供功能截图并加盖厂商公章。
			16	0	AD域用户抽取	支持从AD域抽取组织机构和用户帐号，方便快速建立组织机构和用户帐号
			17	0	资源管理	支持资源管理功能，包括添加、删除、启用、禁用、移动、修改功能
			18	0	支持资源组管理功能，包括添加、删除、修改功能
			19	0	支持资源（包括服务和资源帐号）批量导入导出功能
			20	0	内置常见资源分类和资源系统类型
			21	0	支持限制RDP访问使用剪贴板上、下行控制、磁盘映射功能
			22	0	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，提供功能截图并加盖厂商公章。
			23	0	资源自动发现	支持资源自动发现和添加，便于快速添加资源，提供功能截图并加盖厂商公章。
			24	0	RBAC授权	1、支持基于角色进行授权访问控制RBAC（Role-Based Access Control），包括系统管理员根据不同角色进行管理工作、运维人员根据不同角色进行运维工作，从而满足最小特权原则、责任分离原则和数据抽象原则。提供功能截图并加盖厂商公章。 2、运维角色支持时间、命令和审批策略，支持角色克隆，方便管理员快速对运维权限进行管理。提供功能截图并加盖厂商公章。 3、支持超过角色中时间策略中的时间范围，系统将阻断运维会话，提供功能截图并加盖厂商公章。 4、支持用户、资源与角色关联，形成访问策略。可对访问策略进行增删改查，从而实现对运维权限的细粒度控制。提供功能截图并加盖

					厂商公章。
			25	0	规则管理	1、支持字符、传输、数据库协议的命令规则定义 2、支持时间规则定义 3、支持审批规则定义
			26	0	帐号托管	支持资源制定不同改密分组，执行周期性、手动改密操作
			27	0		改密类型支持： 1、Linux类； 2、国产化操作系统中标麒麟、银河麒麟等； 3、网络设备（华为、华三、思科、中兴等）； 4、Windows类 5、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)，提供功能截图并加盖厂商公章。
			28	0		自动改密密码策略支持随机生成不同密码 、随机生成相同密码 、手工指定相同密码，随机密码支持自定义密码强度
			29	0		支持改密结果自动发送到指定改密计划的管理员邮箱或发送到FTP服务器；密码文件加密保存，需要专用查看工具查看，以保证安全性
			30	0		支持验证登录，可验证当前密码是否可以正常登录。
			31	0		支持通过改密记录进行密码找回，在当前密码丢失的情况下，可找回历史密码，资源再次回到可正常登录的状态。
			32	0		支持对改密计划的执行日志进行完整记录。
			33	0		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，提供功能截图并加盖厂商公章。
			34	0	帐号稽核	支持僵尸、幽灵、孤儿帐号稽核功能，并可以导出异常账号稽核情况报告，方便管理员统计异常账号情况，提供功能截图并加盖厂商公章。 僵尸帐号：周期内登录次数低于3次的用户帐号和资源帐号； 幽灵帐户：堡垒机中未托管但又真实存在的的资源帐号； 孤儿帐户：没有建立授权关系的用户帐号和资源帐号。
						支持通过WEB更新系统许可、升级系统版本

			35	0		支持通过WEB更新系统许可，升级系统版本、重启系统、关机
			36	0	系统管理	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，提供功能截图并加盖厂商公章。
			37	0		支持页面空闲超时退出，支持启用验证码，支持多次登录锁定帐号
			38	0		支持WEB页面配置时区、时间
			39	0		支持NTP时间同步功能
			40	0		支持自定义产品名称、产品logo图片，无需定制开发，提供功能截图并加盖厂商公章。
			41	0	系统检查工具	系统界面可进行Ping、tracetroute等诊断，并可一键导出诊断信息，提供功能截图并加盖厂商公章。
			42	0	数据库审计	实现数据库命令级审计，支持的数据库类型包括：Oracle（支持ORACLE RAC）、SQL Server、IBM DB2、Sybase、IBM Informix Dynamic Server、MySQL、PostgreSQL、Teradata，不需采用数据镜像方式实现，以免增加部署的复杂性和网络负担
			43	0		支持Oracle、Postgresql、Sybase、MySQL、SQL server数据库下行返回行数记录，提供功能截图并加盖厂商公章。 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，提供功能截图并加盖厂商公章。
			44	0		支持通过应用发布实现数据库操作的命令级审计和图形审计的双重审计效果，命令级审计便于重现真实的完整操作命令，图形审计便于直观的查看到真实的操作行为，并支持通过搜索操作语句关键字定位审计回放
			45	0	字符、文件传输协议审计	支持SSH协议服务端启用强加密算法hmac-sha2-256,hmac-sha2-512。
			46	0		支持字符协议SSH、TELNET和文件传输协议FTP、SFTP的协议审计，审计详细的操作语句和操作语句的执行结果
			47	0		支持通过应用发布实现字符协议和文件传输协议的命令级审计和图形审计的双重审计效果，命令级审计便于重现真实的完整操作命令，图形审计便于直观的查看到真实的操作行为，并支持通过搜索操作语句或执行结果中关键字定位审计回放，提供功能截图并加盖厂商公章。

	1		48	0	图形协议审计	支持RDP、VNC图形操作行为的审计，图形回放形式还原真实操作过程
			49	0		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
			50	0		支持RDP窗口标题审计，并支持通过窗口标题内容检索定位回放
			51	0		支持RDP剪切板上、下行控制，提供功能截图并加盖厂商公章。
			52	0		支持对剪贴板拷贝文件记录文件名、拷贝文本进行字符记录，并支持通过搜索字符信息关键字定位审计回放
			53	0	协议扩展	支持通过应用发布进行协议扩展，支持http/https协议、X11协议、VMware vSphere Client、Radmin等工具，并支持模拟帐号密码代填登录；应用发布调用只能推送应用工具窗口，不得推送windows桌面。
			54	0	实时监控	实时监控当前连接发生的所有会话信息，发现高危操作可实时切断会话
			55	0	会话回放	WEB在线视频回放方式重现维护人员对服务器的所有操作过程
			56	0		离线回放重现维护人员对服务器的所有操作过程（回放文件下载到本地播放）
			57	0		倍速播放、拖动、暂停、停止、重新播放等播放控制操作
			58	0		支持通过搜索操作关键字定位回放
			59	0	审计查询和报表	自定义审计查询条件，包括：时间范围、用户与用户IP、资源IP、资源服务、命令关键字条件
			60	0		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，提供功能截图并加盖厂商公章。
			61	0		提供用户统计报表和系统运行报表，支持Word，Excel，PDF，HTML方式导出，提供功能截图并加盖厂商公章。
			62	0		支持以下身份认证方式： 1、基本认证：本地帐号+密码认证，支持内置USB-KEY认证、动态口令认证、国密动态口令认证、手机令牌认证，无须额外增加认证服务器 2、可集成其它外部认证协议： Windows AD

				身份认证	、RADIUS、LDAP、短信、北京CA、吉大正元等第三方认证。 提供功能截图并加盖厂商公章。
			63	0	支持用户以手机号码或邮箱地址作为用户身份登录，提供功能截图并加盖厂商公章。
			64	0	运维用户多次登录失败自动锁定登录帐号或登录IP，到期自动解锁
			65	0	限制用户同一时间只能从一个IP登录
			66	0	密码找回：支持用户忘记登录密码时，可通过邮件方式获取验证码，验证通过后重置登录密码，提供功能截图并加盖厂商公章。
			67	0	本地运维工具单点登录，支持字符、文件传输、图形协议类型如下： 1、字符协议类型：SSH、TELNET 2、文件传输协议类型：FTP、SFTP、SCP 3、图形协议类型：RDP、VNC 4、数据库协议类型：Oracle、PostgreSQL、MySql、DB2、Informix、SYBASE，Mssql(2005,2008,2012)
			68	0	单点登陆SSO	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、PLSQL Dev、Toad for Oracle、Db2cmd（DB2）、Quest Central for DB2、Teradata SQL Assistant、SqlDbx Personal、SqlDbx Professional、pgAdmin3、Mysql Command、SSMS、Dbvisualizer、Navicat，提供功能截图并加盖厂商公章。
			69	0		登录方式支持如下： 1、自动登录：从帐号密码自动代填，运维人员不必知道服务器帐号及密码 2、半自动、手动登录：运维人员也可以选择自行输入资源帐号密码登录，也可选择保存帐号密码，下次不再输入帐号密码
			70	0	运维工具自动发现	支持扫描本地运维工具并进行配置保存，提供功能截图并加盖厂商公章。
			71	0	运维方式	1、WEB运维模式:支持运维人员通过IE（9-11版本）、谷歌浏览器、Firefox浏览器单点登录资源，无需安装Java控件 2、SSH/RDP直连菜单模式：为运维用户提供SSH/RDP CLI工具直连模式，通过认证后进行资源的访问。支持SecureCRT，Mstsc等工具

72	0	C/S模式	支持C/S模式：提供C/S功能，用于运维人员和管理员通过C/S模式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，提供功能截图并加盖厂商公章。
73	0	智能终端运维	支持运维人员在苹果（iMac,iPad,iPhone）和安卓终端以SSH/RDP直连菜单模式登录堡垒机并进行运维操作，提供功能截图并加盖厂商公章。
74	0	H5运维	支持HTML5运维与审计，通过浏览器即可运维常见字符协议和图形协议资源，无须安装任何控件，摆脱对终端环境的限制，国产化桌面版操作系统上也可进行运维操作。提供功能截图并加盖厂商公章。
75	0	二次审批	命令审批：支持根据需求对特殊指令操作进行二次审批功能，运维人员操作过程中触发命令策略，需要得到审批员的审批后才能继续执行后续操作
76	0		登录审批：可设置审批规则与资源角色关联，对运维人员访问资源制定登录审批策略，需要得到审批员的审批后才能继续执行后续操作，提供功能截图并加盖厂商公章。
77	0	网络设备配置备份	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（华为、h3c等）配置的自动备份、供用户查看、下载，提供功能截图并加盖厂商公章。
78	0	命令自动执行	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，提供功能截图并加盖厂商公章。
79	0		支持对命令自动执行任务进行审批，提升命令自动执行安全性，提供功能截图并加盖厂商公章。
80	0	批量登录	支持多种工具批量登录设备
81	0	特权切换	支持以普通管理模式登录网络设备或主机并自动切换到特权模式
82	0	应用发布	1、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，提供功能截图并加盖厂商公章。 2、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，提供功能截图并加盖厂商公章。 3、支持根据屏幕变化或鼠标键盘操作进行闲

				时录像过滤，降低审计回放文件大小，节约磁盘存储空间，提供功能截图并加盖厂商公章。 4、支持将当前应用发布配置批量应用到其他应用发布服务器上，提升应用发布管理效率，提供功能截图并加盖厂商公章。 5、支持消息广播，以对话框形式出现在所有已登录的用户屏幕上，提供功能截图并加盖厂商公章。
			83	0	剪切板控制	应用发布剪贴板控制，防止运维用户拷贝数据到本地，提升运维过程数据安全的管控能力
			84	0	运维屏幕水印	支持通过应用发布开启运维屏幕水印，运维本地无法篡改水印内容，震慑不规范的运维行为，提升运维过程数据安全性，提供功能截图并加盖厂商公章。
			85	0	工单管理	支持管理员下发工单，授权运维人员有权限在指定时间内访问指定的资源
			86	0		支持运维用户主动申请访问权限的工单，管理员审批通过后即可登录运维
			87	0	通讯安全性	管理模式 B/S，采用HTTPS方式远程安全管理
			88	0		系统自身HTTPS 证书签名支持高强度SHA256算法
			89	0		支持网口聚合功能
			90	0		支持国密HTTPS通信，可通过国密浏览器进行访问，提供功能截图并加盖厂商公章。
			91	0	自监控与告警	实时监控系统CPU、内存、磁盘的使用情况，支持CPU、内存、磁盘使用超过阈值邮件告警，支持对系统关机、重启操作进行邮件告警，并可以设置不同事件级别，提供功能截图并加盖厂商公章。
			92	0	空间管理	空间自管理功能，存储空间不足时能够自动清理历史数据，并支持设置触发清理的存储空间阈值
			93	0	数据外发	支持系统配置与审计日志通过FTP或SFTP方式异地备份
			94	0	自动备份	支持系统配置自动备份、审计日志自动、手动备份
			95	0	历史日志导入与查询	支持历史审计日志备份文件导入与历史审计日志查询，提供功能截图并加盖厂商公章。
			96	0	SNMP	支持SNMP Agent方式对外提供设备基础信息（支持SNMP v2c和v3）
			97	0	日志外发	支持以Syslog对外发送运维审计日志
			98	0		支持配置多个日志接收服务器

			99	0	产品资质	国家版权局计算机软件著作权登记证书，提供证明材料并加盖厂家公章。
			100	0		公安部：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），提供证明材料并加盖厂家公章。
			注： 1.“参数性质” 栏中划“0”表示此参数为一般性技术参数，划“0”表示此参数为重要技术参数； 2.一般参数、重要技术参数有负偏离的，按照响应程度做不同额度扣分处理； 3.招标人有权要求中标人在合同签署前提供产品进行所有招标要求功能及投标响应的逐一验证，符合招标方要求后才能执行合同流程，验证中发现虚假应标的行为将予以追究相关责任。			
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。					

合同包3（网络设备）

1.主要商务要求

标的提供的时间	合同签订后20个日历日内交货
标的提供的地点	采购人确定交付地点
投标有效期	从提交投标（响应）文件的截止之日起90日历天
付款方式	1期：支付比例50%，支付比例50%，结合预算资金下达情况，合同签订后，收到中标供应商支付的履约保证金及合法凭证后支付合同金额的50%. 2期：支付比例50%，产品到货验收后支付合同金额的50%
验收要求	1期：项目具备初步验收条件后，由采购单位负责组织验收工作小组进行初步验收 2期：项目具备竣工验收条件后，按照相关规定进行竣工验收
履约保证金	收取比例：10%,说明：为保证中标供应商更好地履行合同，中标供应商须向采购人交纳履约保证金，金额为中标金额的10%。履约保证金的交付时间为合同签订后3日内。验收合格正常运行后计算质保期，履约保证金在质保期满1年后的1个月内，无息原额退还。若中标供应商未能履行其合同规定的任何义务，采购人有权扣罚履约保证金。
其他	

2.技术标准与要求

序号	核心产品（“△”）	品目名称	标的名称	单位	数量	分项预算单价（元）	分项预算总价（元）	面向对象情况	所属行业	招标技术要求
1		其他交换设备	应用服务器核心交换机	台	1.00	1,080,000.00	1,080,000.00	否	其他未列明行业	详见附表一

附表一：应用服务器核心交换机　是否允许进口：否

参数性质	序号	具体技术(参数)要求			
		序号	参数性质	技术指标	技术规格要求
		1	√	交换容量	不小于31Tbps
		2	√	IPv4包转发率	不小于5760Mpps

3	√	槽位数量	不少于9个
4	0	冗余设计	主控、电源、风扇支持冗余
5	√	配置	实配双电源、双主控、不少于48个千兆电接口、不少于20个千兆光接口、不少于20个万兆光接口
6	0	二层特性	支持IEEE802.1P(CoS优先级)
7	0		支持IEEE802.1Q（VLAN）
8	0		支持IEEE802.1d（STP）/802.1w（RSTP）/802.1s（MSTP）
9	0		支持IEEE802.1ad（QinQ），灵活QinQ和Vlan mapping
10	0		支持IEEE802.3x（全双工流控）和背压式流控（半双工）
11	0		支持IEEE802.3ad（链路聚合）和跨板链路聚合
12	0		支持IEEE802.3（10Base-T）/802.3u（100Base-T）
13	0		支持IEEE802.3z（1000BASE-X）/802.3ab（1000BaseT）
14	0		支持IEEE802.3ae（10Gbase）
15	0		支持IEEE802.3af（PoE）
16	0		支持IEEE802.3at（PoE+）
17	0		支持RRPP（快速环网保护协议）
18	0		支持跨板端口/流镜像
19	0		支持端口广播/多播/未知单播风暴抑制
20	0		支持JumboFrame
21	0		支持基于端口、协议、子网和MAC的VLAN划分
22	0		支持SuperVLAN
23	0		支持PVLAN
24	0		支持MulticastVLAN+
25	0		支持点到点单VLAN交叉连接、双VLAN交叉连接
26	0		全部依靠VLAN-ID进行转发，不涉及MAC地址学习
27	0		支持最大VLANMAPING/灵活QinQ表项
28	0		全面支持VLANMAPPING能力
29	0		支持GVRP
30	0		支持LLDP
31	0		支持ARPProxy
32	0		支持DHCPRelay
33	0		支持DHCPServer
34	0		支持静态路由
35	0		支持RIPv1/v2

			36	0	IPv4路由特性	支持OSPFv2
			37	0		支持IS-IS
			38	0		支持BGPv4
			39	0		支持OSPF/IS-IS/BGPGR
			40	0		支持等价路由
			41	0		支持策略路由
			42	0		支持路由策略
			43	0	IPv6路由特性	支持ICMPv6
			44	0		支持ICMPv6重定向
			45	0		支持DHCPv6
			46	0		支持ACLv6
			47	0		支持OSPFv3
			48	0		支持RIPng
			49	0		支持BGP4+
			50	0		支持IS-ISv6
			51	0		支持手工隧道
			52	0		支持ISATAP
			53	0		支持6to4隧道
			54	0		支持IPv6和IPv4双栈
			55	0		支持等价路由
			56	0		支持策略路由
			57	0		支持路由策略
			58	0	组播	支持IGMPv1/v2/v3
			59	0		支持IGMPv1/v2/v3Snooping
			60	0		支持IGMPFilter
			61	0		支持IGMPFastleave
			62	0		支持PIM-SM/PIM-DM/PIM-SSM
			63	0		支持MSDP
			64	0		支持AnyCast-RP
			65	0		支持MLDv2/MLDv2Snooping
			66	0		支持PIM-SMv6、PIM-DMv6、PIM-SSMv6
			67	0	ACL/QoS	支持标准和扩展ACL
			68	0		支持基于VLAN的ACL
			69	0		支持Ingress/EgressACL
			70	0		支持Ingress/EgressCAR，粒度可达8Kbps
			71	0		支持两级Meter能力
			72	0		支持VLAN聚合CAR，MAC聚合CAR功能
			73	0		支持流量整形（TrafficShaping）
			74	0		支持802.1P/DSCP优先级Mark/Remark
			75	0		支持层次化QoS（H-QoS）
			76	0		支持8个优先级队列

	1		77	0		支持队列调度机制，包括SP、WRR、SP+WRR、CBWFQ
			78	0		支持拥塞避免机制，包括Tail-Drop、WRED
			79	0		支持Mirroring
			80	0	SDN/OPENFLOW	支持OPENFLOW1.3标准
			81	0		支持多控制器（EQUAL模式、主备模式）
			82	0		支持多表流水线
			83	0		支持Grouptable
			84	0		支持Meter
			85	0	VxLAN	支持VXLAN二层交换
			86	0		支持VXLAN路由交换
			87	0		支持VXLAN网关
			88	0	MPLS/VPLS	支持L3MPLSVPN
			89	0		支持L2VPN:VLL(Martini,Kompella)
			90	0		支持MCE
			91	0		支持MPLSOAM
			92	0		支持VPLS,VLL
			93	0		支持分层VPLS，以及QinQ+VPLS接入
			94	0		支持P/PE功能
			95	0		支持LDP协议
			96	0	安全机制	支持EAD安全解决方案
			97	0		支持Portal认证
			98	0		支持MAC认证
			99	0		支持IEEE802.1x和IEEE802.1xSERVER
			100	0		支持AAA/Radius
			101	0		支持HWTACACS,支持命令行认证
			102	0		支持SSHv1.5/SSHv2
			103	0		支持ACL流过滤机制
			104	0		支持OSPF、RIPv2及BGPv4报文的明文及MD5密文认证
			105	0		支持命令行采用分级保护方式，防止未授权用户的非法侵入，为不同级别的用户有不同的配置权限
			106	0		支持受限的IP地址的Telnet的登录和口令机制
			107	0		支持IP地址、VLANID、MAC地址和端口等多种组合绑定
			108	0		支持uRPF
			109	0		支持主备数据备份机制
			110	0		支持故障后报警和自恢复
			111	0		支持数据日志
			112	0		支持微分段

113	0	系统管理	支持FTP、TFTP、Xmodem
114	0		支持SNMPv1/v2/v3
115	0		支持sFlow流量统计
116	0		支持RMON
117	0		支持NTP时钟
118	0		支持NetStream流量统计功能
119	0		支持电源智能管理，支持802.3az高效节能以太网
120	0		支持设备在线状态监测机制，实现对包括主控引擎，背板，芯片和存储等关键元器件进行检测
121	0		支持Telemetry流量可视化功能
122	√	售后服务	提供原厂售后服务承诺函（加盖原厂公章）。

注：1.“参数性质” 栏中划“0”表示此参数为一般性技术参数，划“√”表示此参数为重要技术参数；

2. 依据参数性质，扣分额度不同；

3.招标人有权要求中标人在合同签署前提供产品进行所有招标要求功能及投标响应的逐一验证，符合招标方要求后才能执行合同流程，验证中发现虚假应标的行为将予以追究相关责任。

1、网络架构优化服务（本条内容对此包号采购内容进行整体要求）

序号	参数性质	服务指标	技术服务要求
1	0	服务要求	对目标网络的网络现状、网络建设规范性、网络可靠性、网络边界安全、网络流量分析、网络通信安全、网络设备安全和网络安全管理这八个方面进行网络架构安全性的全面分析，对整体网络中的脆弱点进行识别评估，评估结果包括定性和定量分析，让招标方对网络中存在的风险和薄弱点了如指掌。

2、安全巡检服务（本条内容对此包号采购内容进行整体要求）

序号	参数性质	服务指标	技术服务要求
1	0	服务要求	对网络体系、网络安全体系等开展安全检查，内容包括端口状况扫描、端口监听检查、用户列表检查、进程检查、病毒检查、系统木马检查等安全检查与分析工作。

3、安全值守服务（本条内容对此包号采购内容进行整体要求）

			序号	参数性质	服务指标	技术服务要求
			1	0	服务要求	在攻防演习及重要时期（法定节假日、重大会议活动等）期间，提供现场网络专家值守服务，实时监测、分析、研判、处置各类网络攻击，保障业务系统安全稳定运行。以“事前准备、事中保障（值守、监控、应急、处置）、事后总结（复盘、提升）”的思路来保障网络系统的安全。
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则可能导致投标无效。					

第五章 投标人应当提交的资格、资信证明文件

投标人应提交证明其有资格参加投标和中标后有能力履行合同的相关文件，并作为其投标文件的一部分，所有文件必须真实可靠、不得伪造，否则将按相关规定予以处罚。

1.法人或者其他组织的营业执照等证明文件，自然人的身份证明：

法人包括企业法人、机关法人、事业单位法人和社会团体法人；其他组织主要包括合伙企业、非企业专业服务机构、个体工商户、农村承包经营户；自然人是指《中华人民共和国民法典》（以下简称《民法典》）规定的具有完全民事行为能力、能够承担民事责任和义务的公民。如投标人是企业（包括合伙企业），要提供在工商部门注册的有效“企业法人营业执照”或“营业执照”；如投标人是事业单位，要提供有效的“事业单位法人证书”；投标人是非企业专业服务机构的，如律师事务所，会计师事务所要提供执业许可证等证明文件；如投标人是个体工商户，要提供有效的“个体工商户营业执照”；如投标人是自然人，要提供有效的自然人身份证明。

这里所指“其他组织”不包括法人的分支机构，由于法人分支机构不能独立承担民事责任，不能以分支机构的身份参加政府采购，只能以法人身份参加。“但由于银行、保险、石油石化、电力、电信等行业具有其特殊性，如果能够提供其法人给予的相应授权证明材料，可以参加政府采购活动”。

2.财务状况报告，依法缴纳税收和社会保障资金的相关材料（详见资格性审查表要求）

3.具有履行合同所必须的设备和专业技术能力的声明。

4.投标人参加政府采购前三年内在经营活动中没有重大违法记录书面声明函。

5.信用记录查询

（1）查询渠道：通过“信用中国”网站(www.creditchina.gov.cn)和“中国政府采购网”（www.ccgp.gov.cn）进行查询；

（2）查询截止时点：本项目资格审查时查询；

（3）查询记录：对列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单、信用报告进行查询；

采购人或采购代理机构应当按照查询渠道、查询时间节点、查询记录内容进行查询，并存档。对信用记录查询结果中显示投标人被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的投标人作无效投标处理。

6. 按照招标文件要求，投标人应当提交的资格、资信证明文件。

第六章 评审

一、评审要求

1.评标方法

网络安全设备：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。（最低报价不是中标的唯一依据。）
安全及密码设备：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。（最低报价不是中标的唯一依据。）
网络设备：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。（最低报价不是中标的唯一依据。）

2.评标原则

2.1评标活动遵循公平、公正、科学和择优的原则，以招标文件和投标文件为评标的基本依据，并按照招标文件规定的评标方法和评标标准进行评标。

2.2具体评标事项由评标委员会负责，并按招标文件的规定办法进行评审。

2.3 合格投标人不足三家的，不得评标。

3.评标委员会

3.1评标委员会由采购人代表和有关技术、经济等方面的专家组成，成员人数为5人及以上单数，其中技术、经济等方面的评审专家不得少于成员总数的三分之二。

3.2 评标委员会成员有下列情形之一的，应当回避：

（1）参加采购活动前三年内,与投标人存在劳动关系,或者担任过投标人的董事、监事,或者是投标人的控股股东或实际控制人；

（2）与投标人的法定代表人或者负责人有夫妻、直系血亲、三代以内旁系血亲或者近姻亲关系；

（3）与投标人有其他可能影响政府采购活动公平、公正进行的关系；

3.3评标委员会负责具体评标事务，并独立履行下列职责：

（1）审查、评价投标文件是否符合招标文件的商务、技术等实质性要求；

（2）要求投标人对投标文件有关事项作出澄清或者说明；

（3）对投标文件进行比较和评价；

（4）确定中标候选人名单，以及根据采购人委托直接确定中标人；

（5）向采购人、采购代理机构或者有关部门报告评标中发现的违法行为；

（6）法律法规规定的其他职责。

4.澄清

对于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、说明或者补正。

投标人的澄清、说明或者补正应当采用书面形式，并加盖公章，或者由法定代表人或其授权的代表签字。投标人的澄清、说明或者补正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。

4.1评标委员会不接受投标人主动提出的澄清、说明或补正。

4.2评标委员会对投标人提交的澄清、说明或补正有疑问的，可以要求投标人进一步澄清、说明或补正。

5.有下列情形之一的，视为投标人串通投标：

（1）不同投标人的投标文件由同一单位或者个人编制；（不同投标人投标文件上传的项目内部识别码一致）；

（2）不同投标人委托同一单位或者个人办理投标事宜；

（3）不同投标人的投标文件载明的项目管理成员或者联系人员为同一人；

（4）不同投标人的投标文件异常一致或者投标报价呈规律性差异；

（5）不同投标人的投标文件相互混装；

（6）不同投标人的投标保证金为从同一单位或个人的账户转出；

说明：在项目评审时被认定为串通投标的投标人不得参加该合同项下的采购活动

6. 有下列情形之一的，属于恶意串通投标：

（1）投标人直接或者间接从采购人或者采购代理机构处获得其他投标人的相关情况并修改其投标文件或者响应文件；

（2）投标人按照采购人或者采购代理机构的授意撤换、修改投标文件或者响应文件；

（3）投标人之间协商报价、技术方案等投标文件或者响应文件的实质性内容；

（4）属于同一集团、协会、商会等组织成员的投标人按照该组织要求协同参加政府采购活动；

（5）投标人之间事先约定由某一特定投标人中标、成交；

（6）投标人之间商定部分投标人放弃参加政府采购活动或者放弃中标、成交；

（7）投标人与采购人或者采购代理机构之间、投标人相互之间，为谋求特定投标人中标、成交或者排斥其他投标人的其他串通行为。

7.投标无效的情形

详见资格性审查、符合性审查和招标文件其他投标无效条款。

8.废标的情形

出现下列情形之一的，应予以废标。

（1）符合专业条件的投标人或者对招标文件作实质响应的投标人不足3家；（或参与竞争的核心产品品牌不足3个）的；

（2）出现影响采购公正的违法、违规行为的；

（3）投标人的报价均超过了采购预算；

（4）因重大变故，采购任务取消；
（5）法律、法规以及招标文件规定其他情形。

9.定标

评标委员会按照招标文件确定的评标方法、步骤、标准，对投标文件进行评审。评标结束后，对投标人的评审名次进行排序，确定中标人或者推荐中标候选人。

二.政府采购政策落实

1.节能、环保要求

采购的产品属于品目清单范围的，将依据国家确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书，对获得证书的产品实施政府优先采购或强制采购，具体按照本招标文件相关要求执行。

2.对小型、微型企业、监狱企业或残疾人福利性单位给予价格扣除

依照《政府采购促进中小企业发展管理办法》、《关于政府采购支持监狱企业发展有关问题的通知》和《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》的规定，凡符合要求的小型、微型企业、监狱企业或残疾人福利性单位，按照以下比例给予相应的价格扣除：（监狱企业、残疾人福利性单位视同为小、微企业）

合同包1（网络安全设备）

序号	情形	适用对象	价格扣除比例	计算公式
1	小型、微型企业，监狱企业，残疾人福利性单位	非联合体	10%	货物由小微企业制造，即货物由小微企业生产且使用该小微企业商号或者注册商标时，给予价格扣除C1，即：评标价=投标报价×（1-C1）;监狱企业与残疾人福利性单位视同小型、微型企业，享受同等价格扣除，当企业属性重复时，不重复价格扣除。
注：（1）上述评标价仅用于计算价格评分，成交金额以实际投标价为准。（2）组成联合体的大中型企业和其他自然人、法人或者其他组织，与小型、微型企业之间不得存在投资关系。				

合同包2（安全及密码设备）

序号	情形	适用对象	价格扣除比例	计算公式
1	小型、微型企业，监狱企业，残疾人福利性单位	非联合体	10%	货物由小微企业制造，即货物由小微企业生产且使用该小微企业商号或者注册商标时，给予价格扣除C1，即：评标价=投标报价×（1-C1）;监狱企业与残疾人福利性单位视同小型、微型企业，享受同等价格扣除，当企业属性重复时，不重复价格扣除。
注：（1）上述评标价仅用于计算价格评分，成交金额以实际投标价为准。（2）组成联合体的大中型企业和其他自然人、法人或者其他组织，与小型、微型企业之间不得存在投资关系。				

合同包3（网络设备）

序号	情形	适用对象	价格扣除比例	计算公式
1	小型、微型企业，监狱企业，残疾人福利性单位	非联合体	10%	货物由小微企业制造，即货物由小微企业生产且使用该小微企业商号或者注册商标时，给予价格扣除C1，即：评标价=投标报价×（1-C1）;监狱企业与残疾人福利性单位视同小型、微型企业，享受同等价格扣除，当企业属性重复时，不重复价格扣除。
注：（1）上述评标价仅用于计算价格评分，成交金额以实际投标价为准。（2）组成联合体的大中型企业和其他自然人、法人或者其他组织，与小型、微型企业之间不得存在投资关系。				

3.价格扣除相关要求。

（1）所称小型和微型企业应当同时符合以下条件：

①符合中小企业划分标准；

②提供本企业制造的货物、承担的工程或者服务，或者提供其他中小企业制造的货物。本项所称货物不包括使用大型企业注册商标的货物。

中小企业划分标准，是指国务院有关部门根据企业从业人员、营业收入、资产总额等指标制定的中小企业划型标准。

小型、微型企业提供中型企业制造的货物的，视同为中型企业。符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。

（2）在政府采购活动中，供应商提供的货物、工程或者服务符合下列情形的，享受《政府采购促进中小企业发展管理办法》规定的中小企业扶持政策：

①在货物采购项目中，货物由中小企业制造，即货物由中小企业生产且使用该中小企业商号或者注册商标；

②在工程采购项目中，工程由中小企业承建，即工程施工单位为中小企业；

③在服务采购项目中，服务由中小企业承接，即提供服务的人员为中小企业依照《中华人民共和国劳动合同法》订立劳动合同的从业人员。

在货物采购项目中，供应商提供的货物既有中小企业制造货物，也有大型企业制造货物的，不享受《政府采购促进中小企业发展管理办法》规定的中小企业扶持政策。

以联合体形式参加政府采购活动，联合体各方均为中小企业的，联合体视同中小企业。其中，联合体各方均为小微企业的，联合体视同小微企业。

（3）投标人属于小微企业的应填写《中小企业声明函》；监狱企业须投标人提供由监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件；残疾人福利性单位应填写《残疾人福利性单位声明函》，否则不认定价格扣除。

说明：投标人应当认真填写声明函，若有虚假将追究其责任。投标人可通过“国家企业信用信息公示系统”（http://www.gsxt.gov.cn/index.html），点击“小微企业名录”（http://xwqy.gsxt.gov.cn/）对投标人和核心设备制造商进行搜索、查询，自行核实是否属于小微企业。

（4）提供投标人的《中小企业声明函》、《残疾人福利性单位声明函》（格式后附，不可修改），未提供、未盖章或填写内容与相关材料不符的不予价格扣除。

三、评审程序

1.资格性审查和符合性审查

资格性审查。依据法律法规和招标文件的规定，对投标文件中的资格证明文件等进行审查，以确定投标投标人是否具备投标资格。（**详见后附表一资格性审查表**）

符合性审查。依据招标文件的规定，从投标文件的有效性、完整性和对招标文件的响应程度进行审查，以确定是否对招标文件的实质性要求作出响应。（**详见后附表二符合性审查表**）

资格性审查和符合性审查中凡有其中任意一项未通过的，评审结果为未通过，未通过资格性审查、符合性审查的投标单位按无效投标处理。

2. 投标报价审查

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。

3.政府采购政策功能落实

对于小型、微型企业、监狱企业或残疾人福利性单位给予价格扣除。

4. 核心产品同品牌审查

采用最低评标价法的采购项目，提供相同品牌产品的不同投标人参加同一合同项下投标的，以其中通过资格审查、符合性审查且报价最低的参加评标；报价相同的，按技术指标或售后服务条款或业绩的优劣顺序排列确定进入评审的投标人，其他投标无效。

使用综合评分法的采购项目，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参加同一合同项下投标的，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规定的方式确定一个投标人获得中标人推荐资格，招标文件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。

5.详细评审

综合评分法：分为投标报价评审、商务部分评审、技术部分评审（得分四舍五入保留两位小数）。（详见后附表三详细评审表）

最低评标价法：无

6.汇总、排序

综合评分法：评标结果按评审后总得分由高到低顺序排列。总得分相同的，按投标报价由低到高顺序排列。得分且投标报价相同的，按技术指标或售后服务条款或业绩的优劣顺序排列确定；上述相同的，按照提供优先采购产品证明材料的数量进行排序；以上均相同的属于保护环境、不发达地区和少数民族地区企业的优先。

最低评标价法：投标文件满足招标文件全部实质性要求，且进行政府采购政策落实的价格扣除后，对投标报价进行由低到高排序，确定价格最低的投标人为中标候选人。价格相同的，按技术指标或售后服务条款或业绩的优劣顺序排列确定。上述相同的，按照提供优先采购产品证明材料的数量进行排序；以上均相同的属于保护环境、不发达地区和少数民族地区企业的优先。

表一资格性审查表：

合同包1（网络安全设备）

具有独立承担民事责任的能力	审查投标人有效的营业执照或事业单位法人证书或执业许可证或自然人的身份证明。
具有良好的商业信誉和健全的财务会计制度	审查投标人2020或2021年度经会计师事务所出具的财务审计报告或其基本开户银行出具的近一年内的银行资信证明。
有依法缴纳税收和社会保障资金的良好记录	1.提供递交投标文件截止之日前一年内（至少一个月）的良好缴纳税收的相关凭据。（以税务机关提供的纳税凭据或银行入账单为准） 2.提供递交投标文件截止之日前一年内（至少一个月）缴纳社会保险的凭证。（以专用收据或社会保险缴纳清单为准） 注：其他组织和自然人也需要提供缴纳税收的凭据金额缴纳社保的凭据。依法免税或不需要缴纳社会保障资金的投标人，应提供相应文件证明其依法免税或不需要缴纳社会保障资金。
具有履行合同所必须的设备和专业技术能力	审查投标人出具的“具有履行合同所必须的设备和专业技术能力”声明。
参加采购活动前3年内，在经营活动中没有重大违法记录	审查投标人出具的“参加政府采购前三年内在经营活动中无重大违法记录”书面声明函。
信用记录	到提交投标文件的截止时间，投标人未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。

合同包2（安全及密码设备）

具有独立承担民事责任的能力	审查投标人有效的营业执照或事业单位法人证书或执业许可证或自然人的身份证明。
具有良好的商业信誉和健全的财务会计制度	审查投标人2020或2021年度经会计师事务所出具的财务审计报告或其基本开户银行出具的近一年内的银行资信证明。
有依法缴纳税收和社会保障资金的良好记录	1.提供递交投标文件截止之日前一年内（至少一个月）的良好缴纳税收的相关凭据。（以税务机关提供的纳税凭据或银行入账单为准） 2.提供递交投标文件截止之日前一年内（至少一个月）缴纳社会保险的凭证。（以专用收据或社会保险缴纳清单为准） 注：其他组织和自然人也需要提供缴纳税收的凭据金额缴纳社保的凭据。依法免税或不需要缴纳社会保障资金的投标人，应提供相应文件证明其依法免税或不需要缴纳社会保障资金。
具有履行合同所必须的设备和专业技术能力	审查投标人出具的“具有履行合同所必须的设备和专业技术能力”声明。
参加采购活动前3年内，在经营活动中没有重大违法记录	审查投标人出具的“参加政府采购前三年内在经营活动中无重大违法记录”书面声明函。
信用记录	到提交投标文件的截止时间，投标人未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。

合同包3（网络设备）

具有独立承担民事责任的能力	审查投标人有效的营业执照或事业单位法人证书或执业许可证或自然人的身份证明。
具有良好的商业信誉和健全的财务会计制度	审查投标人2020或2021年度经会计师事务所出具的财务审计报告或其基本开户银行出具的近一年内的银行资信证明。
有依法缴纳税收和社会保障资金的良好记录	1.提供递交投标文件截止之日前一年内（至少一个月）的良好缴纳税收的相关凭据。（以税务机关提供的纳税凭据或银行入账单为准） 2.提供递交投标文件截止之日前一年内（至少一个月）缴纳社会保险的凭证。（以专用收据或社会保险缴纳清单为准） 注：其他组织和自然人也需要提供缴纳税收的凭据金额缴纳社保的凭据。依法免税或不需要缴纳社会保障资金的投标人，应提供相应文件证明其依法免税或不需要缴纳社会保障资金。
具有履行合同所必须的设备和专业技术能力	审查投标人出具的“具有履行合同所必须的设备和专业技术能力”声明。
参加采购活动前3年内，在经营活动中没有重大违法记录	审查投标人出具的“参加政府采购前三年内在经营活动中无重大违法记录”书面声明函。
信用记录	到提交投标文件的截止时间，投标人未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。

表二符合性审查表：

合同包1（网络安全设备）

投标及保证金缴纳情况	按要求进行网上投标、进行保证金缴纳。（审查汇款凭证）
投标报价	投标报价（包括分项报价，投标总报价）只能有一个有效报价且不超过采购预算或最高限价，投标报价不得缺项、漏项。
投标文件规范性、符合性	投标文件的签署、盖章、涂改、删除、插字、公章使用等符合招标文件要求；投标文件文件的格式、文字、目录等符合招标文件要求或对投标无实质性影响。
主要商务条款	审查投标人出具的“满足主要商务条款的承诺书”，且进行签署、盖章。
联合体投标	符合关于联合体投标的相关规定（本项目不接收联合体投标）
技术部分实质性内容	1.明确所投标的的产品品牌、规格型号或服务内容或工程量； 2.投标文件应当对招标文件提出的要求和条件作出明确响应并满足招标文件全部实质性要求。
其他要求	招标文件要求的其他无效投标情形；围标、串标和法律法规规定的其它无效投标条款。

合同包2（安全及密码设备）

投标及保证金缴纳情况	按要求进行网上投标、进行保证金缴纳。（审查汇款凭证）
投标报价	投标报价（包括分项报价，投标总报价）只能有一个有效报价且不超过采购预算或最高限价，投标报价不得缺项、漏项。
投标文件规范性、符合性	投标文件的签署、盖章、涂改、删除、插字、公章使用等符合招标文件要求；投标文件文件的格式、文字、目录等符合招标文件要求或对投标无实质性影响。
主要商务条款	审查投标人出具的“满足主要商务条款的承诺书”，且进行签署、盖章。
联合体投标	符合关于联合体投标的相关规定（本项目不接收联合体投标）
技术部分实质性内容	1.明确所投标的的产品品牌、规格型号或服务内容或工程量； 2.投标文件应当对招标文件提出的要求和条件作出明确响应并满足招标文件全部实质性要求。
其他要求	招标文件要求的其他无效投标情形；围标、串标和法律法规规定的其它无效投标条款。

合同包3（网络设备）

投标及保证金缴纳情况	按要求进行网上投标、进行保证金缴纳。（审查汇款凭证）
投标报价	投标报价（包括分项报价，投标总报价）只能有一个有效报价且不超过采购预算或最高限价，投标报价不得缺项、漏项。
投标文件规范性、符合性	投标文件的签署、盖章、涂改、删除、插字、公章使用等符合招标文件要求；投标文件文件的格式、文字、目录等符合招标文件要求或对投标无实质性影响。
主要商务条款	审查投标人出具的“满足主要商务条款的承诺书”，且进行签署、盖章。
联合体投标	符合关于联合体投标的相关规定（本项目不接收联合体投标）
技术部分实质性内容	1.明确所投标的的产品品牌、规格型号或服务内容或工程量； 2.投标文件应当对招标文件提出的要求和条件作出明确响应并满足招标文件全部实质性要求。
其他要求	招标文件要求的其他无效投标情形；围标、串标和法律法规规定的其它无效投标条款。

网络安全设备

评审因素	评审标准
分值构成	技术部分45.0分 商务部分25.0分 报价得分30.0分

技术部分	技术参数满足程度 (15.0分)	投标人提供的服务和参数完全满足招标文件规定的要求得15分，重要参数有一项不满足扣1分，一般参数有一项不满足扣0.5分，扣完为止。
	技术方案 (10.0分)	根据投标人提供的整体技术方案进行综合评分，内容描述清楚、完整，对采购人业务需求理解充分、分析准确，工作计划和进度具有可行性、合理性，内容不偏离，优得8-10分、良得4-7分、一般得0-3。
	项目实施方案 (8.0分)	根据投标人提供的项目管理与实施方案进行综合评分：项目管理与实施方案包括但不限于实施进度、人员安排、质量控制、安全措施、应急处理、组织保障等内容进行综合评价，优得6-8分、良得3-5分、一般得0-2。
	售后服务方案 (7.0分)	1、根据投标人提供的售后服务方案进行综合评分：售后服务方案包括但不限于售后服务承诺、售后服务体系、售后服务内容、方式、专业的技术服务团队及其他资源保障等内容进行综合评价，优得4-5分、良得2-3分、一般得0-1；2、为确保本项目产品间兼容性及后期运维统一性，所投所有产品为同一品牌得2分，非同一品牌不得分。
	项目培训方案 (5.0分)	根据投标人提供的项目培训方案进行综合评分：项目培训方案包括但不限于培训目标、培训计划、培训师资力量、培训课程、培训教材、培训质量保证措施等内容进行综合评价，优得4-5分、良得2-3分、一般的0-1。
商务部分	人员配备情况 (8.0分) ）	投标人拟派服务团队每具备下列一项得1分，最高得8分。 具备国家网络安全应用检测专业测评人员高级证书；具备国家互联网应急中心颁发网络安全能力认证网络安全技术人员证书；具备国家互联网应急中心颁发网络与信息安全应急人员证书；具备网络安全等级保护技术能力证书；具备网络分析师证书；具备国家重要信息系统保护人员证书；具备信息系统审计师证书；具备国家级重大活动网络安保活动优秀个人证书（证书颁发单位需为国家级网络安全主管行政机关）。（一人多证只记一次分，其余证件不予计分。以上人员须提供供应商为其缴纳的自2021年11月至今任意连续6个月的社保证明材料。未提供则不予计分）。
	类似业绩 (3.0分)	供应商自2019年1月1日至投标截止时间承揽过同类项目的每一个得0.5分，本项满分为3分。（须提供合同与中标通知书的复印件，以合同签订时间为准。未提供则不予计分）。
	综合实力 (14.0分)	1、所投所有产品的生产厂商应具备充分的网络安全研究能力，累计的CVE漏洞发现数超过90个，请给出漏洞发现列表（CVE编号，漏洞描述）及证明方法；提供证明材料并加盖公章。 2、所投所有产品的生产厂商应具备售后服务体系认证证书（GB/T27922-2011）；（提供证明材料并加盖公章）。 3、所投所有产品的生产厂商需具备信息安全服务资质（信息安全应急处理服务和信息安全服务资质（CCRC颁发），一级信息安全风险评估服务）；（提供证明材料并加盖公章）。 4、所投所有产品的生产厂商需具备国家计算机网络应急技术处理协调中心颁发的《网络安全应急服务支撑单位证书（国家级）》；提供证明材料并加盖公章）。 5、所投所有产品的生产厂商需具备CMMI5认证证书；（提供证明材料并加盖公章）。 6、所投所有产品的生产厂商需具备ITSS符合性证书(运行维护三级)；（提供证明材料并加盖公章）。 7、所投所有产品的生产厂商需具备中国信息安全测评中心颁发的信息安全服务资质证书-安全工程三级；（提供证明材料并加盖公章）。 以上要求每满足1项得2分，最高14分。

投标报价	投标报价得分 (30.0分)	投标报价得分=（评标基准价/投标报价）×价格分值【注：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。】最低报价不是中标的唯一依据。因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。

安全及密码设备

评审因素	评审标准	
分值构成	技术部分45.0分 商务部分25.0分 报价得分30.0分	
技术部分	技术参数满足程度 (15.0分)	投标人提供的服务和参数完全满足招标文件规定的要求得15分，重要参数有一项不满足扣1分，一般参数有一项不满足扣0.5分，扣完为止。
	技术方案 (9.0分)	根据投标人提供的整体技术方案，内容描述清楚、完整，对采购人业务需求理解充分、分析准确，工作计划和进度具有可行性、合理性，内容不偏离，进行综合评价，优得7-9分、良得3-6分、一般得0-2。
	项目实施方案 (8.0分)	根据投标人提供的项目管理与实施方案进行综合评分：项目管理与实施方案包括但不限于实施进度、人员安排、质量控制、安全措施、应急处理、组织保障等内容进行综合评价，优得6-8分、良得3-5分、一般得0-2。
	售后服务方案 (8.0分)	1、根据投标人提供的售后服务方案进行综合评分：售后服务方案包括但不限于售后服务承诺、售后服务体系、售后服务内容、方式、专业的技术服务团队及其他资源保障等内容进行综合评价，优得4-5分、良得2-3分、一般得0-1； 2、为确保本项目产品间兼容性及后期运维统一性，所投所有产品为同一品牌得3分，非同一品牌不得分。
	项目培训方案 (5.0分)	根据投标人提供的项目培训方案进行综合评分：项目培训方案包括但不限于培训目标、培训计划、培训师资力量、培训课程、培训教材、培训质量保证措施等内容进行综合评价，优得4-5分、良得2-3分、一般的0-1。
商务部分	人员配备情况 (8.0分) ）	投标人拟派服务团队每具备下列一项得1分，最高得8分。 具备国家网络安全应用检测专业测评人员高级人员证书；具备国家互联网应急中心颁发网络安全能力认证网络安全技术人员证书；具备国家互联网应急中心颁发网络与信息安全应急人员证书；具备商用密码应用安全性评估工作技术能力人员认证；具备网络分析师证书；具备国家重要信息系统保护人员证书；具备信息系统审计师证书，具备国家级重大活动网络安保活动优秀个人证书（证书颁发单位需为国家级网络安全主管行政机关）人员1名。（一人多证只记一次分，其余证件不予计分。以上人员须提供供应商为其缴纳的自2021年11月至今任意连续6个月的社保证明材料。未提供则不予计分）。
	类似业绩 (3.0分)	供应商自2019年1月1日至投标截止时间承揽过同类项目的每一个得0.5分，本项满分为3分。（须提供合同与中标通知书的复印件，以合同签订时间为准。未提供则不予计分）。

	综合实力 (14.0分)	1、所投所有产品的生产厂商应具备充分的网络安全研究能力，累计的CVE漏洞发现数超过90个，请给出漏洞发现列表（CVE编号，漏洞描述）及证明方法；提供证明材料并加盖公章。 2、所投所有产品的生产厂商应具备售后服务体系认证证书（GB/T27922-2011）；（提供证明材料并加盖公章）。 3、所投所有产品的生产厂商需具备信息安全服务资质（信息安全应急处理服务和信息安全服务资质（CCRC颁发），一级信息安全风险评估服务）；（提供证明材料并加盖公章）。 4、所投所有产品的生产厂商需具备国家计算机网络应急技术处理协调中心颁发的《网络安全应急服务支撑单位证书（国家级）》；提供证明材料并加盖公章）。 5、所投所有产品的生产厂商需具备CMMI5认证证书；（提供证明材料并加盖公章）。 6、所投所有产品的生产厂商需具备ITSS符合性证书(运行维护三级)；（提供证明材料并加盖公章）。 7、所投所有产品的生产厂商需具备中国信息安全测评中心颁发的信息安全服务资质证书-安全工程三级；（提供证明材料并加盖公章）。 以上要求每满足1项得2分，最高14分。
投标报价	投标报价得分 (30.0分)	投标报价得分＝（评标基准价/投标报价）×价格分值【注：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。】最低报价不是中标的唯一依据。因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。

网络设备

评审因素	评审标准	
分值构成	技术部分45.0分 商务部分25.0分 报价得分30.0分	
技术部分	技术参数满足程度 (15.0分)	投标人提供的服务和参数完全满足招标文件规定的要求得15分，重要参数有一项不满足扣1分，一般参数有一项不满足扣0.5分，扣完为止。
	技术方案 (10.0分)	根据投标人提供的整体技术方案，内容描述清楚、完整，对采购人业务需求理解充分、分析准确，工作计划和进度具有可行性、合理性，内容不偏离，进行综合评价，优得8-10分、良得4-7分、一般得0-3。
	项目实施方案 (8.0分)	根据投标人提供的项目管理与实施方案进行综合评分：项目管理与实施方案包括但不限于实施进度、人员安排、质量控制、安全措施、应急处理、组织保障等内容进行综合评价，优得6-8分、良得3-5分、一般得0-2。
	售后服务方案 (7.0分)	1、根据投标人提供的售后服务方案进行综合评分：售后服务方案包括但不限于售后服务承诺、售后服务体系、售后服务内容、方式、专业的技术服务团队及其他资源保障等内容进行综合评价，优得4-5分、良得2-3分、一般得0-1； 2、为确保本项目产品间兼容性及后期运维统一性，所投所有产品为同一品牌得2分，非同一品牌不得分。
	项目培训方案 (5.0分)	根据投标人提供的项目培训方案进行综合评分：项目培训方案包括但不限于培训目标、培训计划、培训师资力量、培训课程、培训教材、培训质量保证措施等内容进行综合评价，优得4-5分、良得2-3分、一般的0-1。

商务部分	人员配备情况 (8.0分) ）	投标人拟派服务团队每具备下列一项得1分，最高得8分。,具有主流厂商网络交换类高级技术认证证书、具备信息安全等级保护安全建设专业技术人员证书、具备网络分析师证书、具备国家网络安全应用检测专业测评人员高级人员证书；具有国家互联网应急中心颁发网络安全能力认证网络安全技术人员证书、具有国家互联网应急中心颁发网络与信息安全应急人员证书；具备国家级重大活动网络安保活动优秀个人证书（证书颁发单位需为国家级网络安全主管行政机关）、具备信息系统审计师证书人。（一人多证只记一次分，其余证件不予计分。以上人员须提供供应商为其缴纳的自2021年11月至今任意连续6个月的社保证明材料。未提供则不予计分）。
	类似业绩 (5.0分)	供应商自2019年1月1日至投标截止时间承揽过同类项目的每一个得1分，本项满分为5分。（须提供合同与中标通知书的复印件，以合同签订时间为准。未提供则不予计分）。
	综合实力 (12.0分)	投标人需具备数通设备基础实施能力及与网络安全体系联动对接能力，具备高新技术企业证书、信息安全等级保护安全建设服务机构能力评估合格证书、原厂售后服务技术服务单位证明，每项4分，最高得12分，不具备不得分。
投标报价	投标报价得分 (30.0分)	投标报价得分＝（评标基准价/投标报价）×价格分值【注：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。】最低报价不是中标的唯一依据。因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。

第七章 投标文件格式与要求

投标人提供投标文件应按照以下格式及要求进行编制，且不少于以下内容。

格式一：

投标文件封面

（项目名称）
投标文件
（正本/副本）

项目编号：
包　　号：第 包（若项目分包时使用）

（投标人名称）

年 月 日

格式二：

投标文件目录

格式三：

投标承诺书

采购单位、内蒙古中涛工程项目管理有限公司：

1.按照已收到的　　项目（项目编号：　　）招标文件要求，经我方　（投标人名称）　认真研究投标须知、合同条款、技术规范、资质要求和其它有关要求后，我方愿按上述合同条款、技术规范、资质要求进行投标。我方完全接受本次招标文件规定的所有要求，并承诺在中标后执行招标文件、投标文件和合同的全部要求，并履行我方的全部义务。我方的最终报价为总承包价，保证不以任何理由增加报价。

2. 我方同意招标文件关于投标有效期的所有规定。

3. 我方郑重声明：所提供的投标文件内容全部真实有效。如经查实提供的内容、进行承诺的事项存在虚假，我方自愿接受有关处罚，及由此带来的法律后果。

4. 我方将严格遵守《中华人民共和国政府采购法》、《中华人民共和国民法典》等有关法律、法规规定，如有违反，无条件接受相关部门的处罚。

5. 我方同意提供贵方另外要求的与其投标有关的任何数据或资料。

6. 我方将按照招标文件、投标文件及相关要求、规定进行合同签订，并严格执行和承担协议和合同规定的责任和义务。

7. 我单位如果存在下列情形的，愿意承担取消中标资格、投标保证金不予退还、赔偿超过投标保证金金额的损失部分、接受有关监督部门处罚等后果：

（1）中标后，无正当理由放弃中标资格；

（2）中标后，无正当理由不与招标人签订合同；

（3）在签订合同时，向招标人提出附加条件或不按照相关要求签订合同；

（4）不按照招标文件要求提交履约保证金；

（5）要求修改、补充和撤销投标文件的实质性内容；

（6）要求更改招标文件和中标结果公告的实质性内容；

（7）法律法规和招标文件规定的其他情形。

详细地址：　　邮政编码：

电 话：　　电子函件：

投标人开户银行：　　账号/行号：

投标人法人签字：　　（加盖公章）

年　月　日

格式四：

开标一览表

投标人名称：

项目名称、包号：　　项目编号：

投标总报价（元）
大写：
小写：

说明：1．所有价格均系用人民币表示，单位为元。

2．价格应按照“投标人须知”的要求报价。

3．格式、内容和签署、盖章必须完整。

4.《开标一览表》中所填写内容与投标文件中内容不一致的，以开标一览表为准。

注：采用电子招投标的项目无需编制该表格，投标供应商应在投标客户端【报价部分】进行填写，投标客户端软件将自动根据供应商填写信息在线生成。

法定代表人或授权委托人（签字）：

加盖公章：

年　月　日

格式五：

授权委托书

本人_____（姓名）系_____（投标人名称）的法定代表人，现委托_____（姓名）为我方代理人。代理人根据授权，以我方名义签署、澄清确认、递 交、撤回、修改招标项目投标文件、签订合同和处理有关事宜，其法律后果由我方承担。委托期限：_____。

代理人无转委托权。

投 标 人：_____（加盖公章）

法定代表人：_____（签字）

授权委托人：_____（签字）

法定代表人身份证扫描件 正面	法定代表人身份证扫描件 反面
授权委托人身份证扫描件 正面	授权委托人身份证扫描件 反面

____年_____月_____日

格式六：

投标保证金

投标人应在此提供保证金的凭证的复印件。

格式七：

投标人基本情况表

投标人名称		注册资金	
注册地		注册时间	
法定代表人		联系电话	
技术负责人		联系电话	
开户银行			
开户银行账号			
主营范围：			
企业资质：			

格式八：

提供具有独立承担民事责任的能力的证明材料

格式九：

提供具有良好的商业信誉和健全的财务会计制度的证明材料

格式十：

提供依法缴纳税收和社会保障资金的良好记录

格式十一：

具有履行合同所必须的设备和专业技术能力的声明

我公司具备履行本次投标项目合同所必须的设备和专业技术能力。

特此声明。

投标人名称：（加盖公章）

年　　月　　日

格式十二：

参加政府采购前三年内在经营活动中无重大违法记录书面声明

内蒙古中涛工程项目管理有限公司：

我公司自愿参加本次政府采购活动（本次投标项目），严格遵守《中华人民共和国政府采购法》、《政府采购法实施条例》及所有相关法律、法规和规定，同时声明：在参加此次政府采购活动前三年内，本公司在经营活动中无重大违法记录。

特此声明。

投标人名称：（加盖公章）

年　　月　　日

格式十三：（不属于可不填写内容或不提供）

联合体协议书

_____（所有成员单位名称）自愿组成_____（联合体名称）联合体，共同参加_____（项目名称）招标项目投标。现就联合体投标事宜订立如下协议。

1.（某成员单位名称）为（联合体名称）牵头人。

2. 联合体各成员授权牵头人代表联合体参加投标活动，签署文件，提交和接收相关的资料、信息及指示，进行合同谈判活动，负责合同实施阶段的组织和协调工作，以及处理与本招标项目有关的一切事宜。

3. 联合体牵头人在本项目中签署的一切文件和处理的一切事宜，联合体各成员均予以承认。联合体各成员将严格按照招标文件、投标文件和合同的要求全面履行义务，并向招标人承担连带责任。

4. 联合体各成员单位内部的职责分工如下：_____。

5. 本协议书自所有成员单位法定代表人或其授权代表签字或盖单位章之日起生效，合同履行完毕后自动失效。

6. 本协议书一式_____份，联合体成员和招标人各执一份。

协议书由法定代表人签字的，应附法定代表人身份证明；由授权代表签字的，应附授权委托书。

联合体牵头人名称：_____（加盖公章）

法定代表人或其授权代表：_____（签字）

联合体成员名称：_____（加盖公章）

法定代表人或其授权代表：_____（签字）

_____年_____月_____日

格式十四：（不属于可不填写内容或不提供）

中小企业声明函（货物）

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，提供的货物全部由符合政策要求的中小企业制造。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*（采购文件中明确的所属行业）行业*；制造商为*（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*（采购文件中明确的所属行业）行业*；制造商为*（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：

1.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

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*（采购文件中明确的所属行业）*；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*（采购文件中明确的所属行业）*；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）*；

……

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：

1.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

格式十五：（不属于可不填写内容或不提供）

监狱企业

提供由监狱管理局、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。

格式十六：（不属于可不填写内容或不提供）

残疾人福利性单位声明函

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）的规定，本单位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（由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

单位名称（加盖公章）：

日 期：

格式十七：

分项报价明细表

序号	标的名称	品牌、规格型号/主要服务内容	制造商名称	产地	数量	单位	单价（元）	总价（元）
1								
2								
3								
…								

说明：

1.“投标标的”为货物的：上述表格应全部填写。

2.“投标标的”为服务的：如服务内容涉及品牌、规格型号的，上述表格应全部填写；如不涉及品牌、规格型号的，“制造商名称和产地”部分可不填写内容。

3.“投标标的”为工程的：如不涉及品牌、规格型号的，“制造商名称和产地”部分可不填写内容。

注：采用电子招投标的项目无需编制该表格，投标供应商应在投标客户端【报价部分】进行填写，投标客户端软件将自动根据供应商填写信息在线生成。

格式十八：

主要商务要求承诺书

我公司承诺可以完全满足本次采购项目的所有主要商务条款要求（如标的提供的时间、标的提供的地点、投标有效期、采购资金支付、验收要求、履约保证金等）。若有不符合或未按承诺履行的，后果和责任自负。

如有优于招标文件主要商务要求的请在此承诺书中说明。

具体优于内容 （如标的提供的时间、地点，质保期等） 。

特此承诺。

投标人名称：（加盖公章）

年 月 日

格式十九：

技术偏离表

序号	标的名称	招标技术要求		投标人提供响应内容	偏离程度	备注
1		★	1.1			
			1.2			
			……			
2		★	2.1			
			2.2			
			……			
……						

说明：

1.投标人应当如实填写上表“投标人提供响应内容”处内容，对招标文件提出的要求和条件作出明确响应，并列明具体响应数值或内容，只注明符合、满足等无具体内容表述的，将视为未实质性满足招标文件要求。

2.“偏离程度”处可填写满足、响应或正偏离、负偏离。

3.“备注”处可填写偏离情况的具体说明。

4. 上表中“招标技术要求”应详细填写招标要求。

格式二十：

项目组成人员一览表

序号	姓名	本项目拟任职务	学历	职称或执业资格	身份证号	联系电话
1						
2						
3						
……						

按招标文件要求在本表后附相关人员证书。

注：

1.本项目拟任职务处应包括：项目负责人、项目联系人、项目服务人员或技术人员等。

2.如投标人中标，须按本表承诺人员操作，不得随意更换。

格式二十一：

项目实施方案、质量保证及售后服务承诺等内容和格式自拟。

格式二十二：

投标人业绩情况表

序号	使用单位	业绩名称	合同总价	签订时间
1				
2				
3				
4				
…				

投标人根据上述业绩情况后附销售或服务合同复印件。

格式二十三：

各类证明材料

1.招标文件要求提供的其他资料。
2.投标人认为需提供的其他资料。