**浙江省委网信办（本级）通用设备及网络安全升级项目**

项目编号：ZZCG2022X-GK-152

**公**

**开**

**招**

**标**

**文**

**件**

采购单位：浙 江 省 政 府 采 购 中 心

地 址：杭州市环城北路305号耀江发展中心

**目录**

**[第一章公开招标采购公告](#_Toc496796635)** [3](#_Toc496796635)

**[第二章投标人须知](#_Toc496796636)** [6](#_Toc496796636)

**[第三章评标办法及评分标准](#_Toc496796637)** [23](#_Toc496796637)

**[第四章招标需求](#_Toc496796638)** [24](#_Toc496796638)

**[第五章浙江省政府采购合同主要条款指引](#_Toc496796639)** [25](#_Toc496796639)

**[第六章投标文件格式附件](#_Toc496796640)** [32](#_Toc496796640)

**第一章 公开招标采购公告**

根据《中华人民共和国政府采购法》《中华人民共和国政府采购法实施条例》《政府采购货物和服务招标投标管理办法》等规定，现就下列项目进行公开招标采购，欢迎提供本国货物、服务的单位或个人前来投标：

一、**项目编号：****ZZCG2022X-GK-152**

**二、公告期限：5个工作日**

**三、采购项目内容、数量及预算**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **标项序号** | **标项名称** | **数量** | **单位** | **预算金额(万元)** | **简要规格描述或标项基本概况介绍** |
| **1** | **浙江省委网信办（本级）通用设备及网络安全升级项目** | **1** | **批** | **517.6** | **详见招标文件** |

**四、合格投标人的资格要求**

符合《中华人民共和国政府采购法》第二十二条规定,且未被“信用中国”（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）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。

**投标人的特定条件：无**

**五、获取采购文件**

1.获取时间：[项目采购-报名开始日期] 至 2022-08-31 09:00:00。

2.获取方式：本项目招标文件实行网上获取。供应商登录浙江政府采购网（<http://zfcg.czt.zj.gov.cn/>）进入政采云系统“项目采购”模块“获取采购文件”菜单，进行网上获取招标文件。

3.招标文件免费获取。

**六、投标截止时间、地点和形式**

**投标截止时间：**2022-08-31 09:00:00**。**

本项目实行电子投标。投标文件应按照本项目招标文件和电子交易平台的要求编制、加密，并应当在投标截止时间前在规定电子交易平台完成传输递交，投标截止时间后送达的投标文件，将被电子交易平台拒收。

如认为需要，投标人可以选择递交备份投标文件，采用数据电文形式，以U盘或DVD光盘形式存储，并在投标截止时间前，通过邮寄方式，送达指定地点，逾期送达或未密封将被拒收。

备份投标文件收件填写人：陶老师，联系方式：0571-88901836，收件地址：浙江省杭州市下城区环城北路305号耀江发展中心三楼浙江省政府采购中心302会议室。（疫情期间仅接收邮寄方式递交的**备份**投标文件,因本大楼疫情管控，推荐使用中国邮政速递和顺丰快递。）

**本项目拒绝接受纸质投标文件。**

**七、开标时间及地点：**

**本次招标将于****2022-08-31 09:00:00时整在****拱墅区杭州市环城北路305号耀江发展中心 3A（四楼）06开标室开标。**

**本项目实行“不见面开评标”，投标人无须派人员到现场出席开标会议。**

|  |  |  |
| --- | --- | --- |
| 开标现场咨询电话 | 201开标室（大）：0571-88907719 | 202评标室（小）：0571-88907720 |
| 3A（四楼）05评标室：0571-88907792 | 3A（四楼）06开标室：0571-88907791 |

**八、电子交易平台的网络地址和登录方法**

**（一）网络地址：**浙江政府采购网 <http://zfcg.czt.zj.gov.cn/>

**（二）登录方法：**投标人须先完成供应商注册并申请CA，再下载客户端编制、加密电子投标文件，最后应在浙江政府采购网政采云用户登录窗口登录，完成电子投标文件传输递交（具体详见第二章 投标人须知前附表）。

**九、其他：**

**（一）本项目采用“电子交易/不见面开评标”，供应商可进入电子卖场服务中心采云学院**

**（https://edu.zcygov.cn/live?utm=a0018.2ef5001f.0.0.1939d340e5db11ea867fb57c149ddb61）自行提前学习**。

**十、业务咨询**

|  |  |
| --- | --- |
| **机 构** | 浙江省政府采购中心 |
| **地 址** | 浙江省杭州市下城区环城北路305号耀江发展中心 |
| **网 站** | 浙江政府采购网http://zfcg.czt.zj.gov.cn/（文件下载、公告查询） |
| **咨询事项** | **联系人** | **联系方式** | **传真** | **备注** |
| 项目联系人（A岗） | 柯泓 | 0571-88901833 | 0571-88907751 | 三楼（采购二部） |
| 项目协办人（B岗） | 高媛沁 | 0571-88907717 |
| 部门负责人 | 高媛沁 | 0571-88907717 |
| 项目监督 | 吴女士 | 0571-88900117 | 三楼（采购监督部） |
| 网站系统问题 | 客 服 | 4008817190 | / | 注册、账号、系统操作等 |

**十一、采购需求咨询**

|  |  |
| --- | --- |
| 采购单位 | 中共浙江省委网络安全和信息化委员会办公室 |
| 地址 | 杭州市西湖区省府路29号 |
| 咨询事项 | 评分标准、采购需求等 |
| 联系人 | 夏威 |
| 联系方式 | 0571-81051281 |
| 传真 |  |
| 备注 |  |

**第二章 投标人须知**

前附表

|  |  |  |
| --- | --- | --- |
| 序号 | 内 容 | 要 求 |
| 1 | 项目名称及数量 | 详见《公开招标采购公告》三 |
| 2 | 信用记录 | 根据财库[2016]125号文件，通过“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn），以开标当日网页查询记录为准。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的供应商，其投标将作无效标处理。 |
| 3 | 中小企业预留份额情况 | **根据《政府采购促进中小企业发展管理办法》财库〔2020〕46号文件的规定，本项目不属于预留份额专门面向中小企业采购的项目。** |
| 4 | 中小企业优惠措施 | 1. **项目属性（货物类）**
2. **中小企业划分标准所属行业（具体根据《中小企业划型标准规定》执行）**

**采购标的：浙江省委网信办（本级）通用设备及网络安全升级项目，所属行业：软件和信息技术服务业****3.根据财库〔2020〕46号的相关规定，在评审时对符合本办法规定的小微企业报价给予 20% 的扣除，取扣除后的价格作为最终投标报价（此最终投标报价仅作为价格分计算）。中小企业参加政府采购活动，应当出具本办法规定的《中小企业声明函》，否则不得享受相关中小企业扶持政策。****接受大中型企业与小微企业组成联合体或者允许大中型企业向一家或者多家小微企业分包的采购项目，对于联合协议或者分包意向协议约定小微企业的合同份额占到合同总金额 30%以上的，对联合体或者大中型企业的报价给予 6% 的扣除，用扣除后的价格参加评审。****组成联合体或者接受分包 的小微企业与联合体内其他企业、分包企业之间存在直接控 股、管理关系的，不享受价格扣除优惠政策。**4.根据财库[2017]141号的相关规定，在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受评审中价格扣除政策。属于享受政府采购支持政策的残疾人福利性单位，应满足财库[2017]141号文件第一条的规定，并在投标文件中提供残疾人福利性单位声明函（见附件）。5.根据财库[2014]68号的相关规定，在政府采购活动中，监狱企业视同小型、微型企业，享受评审中价格扣除政策，并在投标文件中提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件（格式自拟）。”**(注：未提供以上材料的，均不给予价格扣除）。** |
| 5 | 政府采购节能环保产品 | 投标产品若属于节能（环保）产品的，请提供参与实施政府采购节能（环境标志）产品认证机构出具的认证证书或证书发布平台的投标产品认证证书查询截图；参与实施政府采购节能（环境标志）产品认证机构详见《市场监督总局关于发布参与实施政府采购节能产品、环境标志产品认证机构名录的公告》（2019第16号）；证书发布平台详见《财政部 发展改革委 生态环境部 市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）。产品属于政府强制采购节能品目的（详见《关于印发节能产品政府采购品目清单的通知》财库〔2019〕19号），投标人须按上款要求提供节能产品认证证书或规定网站证书查询截图。**产品属于政府强制采购节能产品品目的，投标人未提供节能产品的，其投标将作无效标处理；本文件“第四章招标需求”另有规定的除外。** |
| 6 | 质疑 | 投标人认为采购文件使自己的权益受到损害的，可以自获取采购文件之日或者采购公告期限届满之日（公告期限届满后获取采购文件的，以公告期限届满之日为准）起7个工作日内，对采购文件需求以及评分细则的以书面形式向采购人提出质疑，对其他内容的以书面形式向采购人和招标方提出质疑，格式及内容要求详见总则（五）质疑。 |
| 7 | 是否允许采购进口产品 | 不允许进口产品。 |
| 8 | 是否允许转包与分包 | 转包：否分包：允许分包；非主体、非关键性工作允许分包。当分包份额占到合同总金额100%时，视为转包。此情况根据《中华人民共和国政府采购法实施条例》（国务院令第658号）文件第七十二条规定，将依照政府采购法第七十七条第一款的规定追究相应法律责任。依据政府采购促进中小企业发展管理办法规定享受扶持政策获得政府采购合同的，小微企业不得将合同分包给大中型企业，中型企业不得将合同分包给大型企业。 |
| 9 | 联合体投标 | 标项1:允许联合体投标。 |
| 10 | 是否现场踏勘 | 不组织现场踏勘。 |
| 11 | 是否提供演示 | 不进行演示。 |
| 12 | 是否提供样品 | 不要求提供样品。 |
| 13 | 投标文件组成 | 投标文件均由资质文件、技术商务文件、报价文件组成。投标人提供备份投标文件（正本）的，数量为1份。 |
| 14 | 电子交易平台登录方法 | **第一步：供应商注册****投标人应在投标前注册成为浙江政府采购网的正式供应商（注册网址：<https://middle.zcygov.cn/v-settle-front/registry>）；****第二步：申请CA****投标人应在投标前完成CA数字证书办理（办理流程详见http://zfcg.czt.zj.gov.cn/bidClientTemplate/2019-05-27/12945.html）。完成CA数字证书办理预计一周左右，建议各投标人抓紧时间办理；****第三步：下载客户端****投标人通过政采云电子交易客户端制作投标文件，请自行前往浙江政府采购网下载并安装（下载网址：<http://zfcg.czt.zj.gov.cn/bidClientTemplate/2019-09-24/12975.html>）；****第四步：具体流程****详见浙江省“电子交易/不见面开评标”学习专题（网址<https://edu.zcygov.cn/luban/e-biding>）****提醒：请各投标人合理安排时间，尽快完成第一、二、三步骤，避免影响投标。** |
| 15 | 投标文件的递交与接收 | **投标人应当在投标截止时间前完成电子投标文件的传输递交，并可以补充、修改或者撤回电子投标文件。补充或者修改电子投标文件的，应当先行撤回原文件，补充、修改后重新传输递交。投标截止时间前未完成传输的，视为撤回投标文件。投标截止时间后送达的投标文件，将被电子交易平台拒收。****投标文件的接收以本项目公告要求的时间、地点和“第二章”的“投标文件的编制”等要求为准。****投标人递交备份投标文件，出现下列情况之一的，将被拒收：****1、未按规定密封或标记的；****2、由于包装不妥，在送交途中严重破损或失散的；****3、超过投标截止时间送达的。** |
| 16 | 中标结果公告 | 中标供应商确定之日起2个工作日内，将在浙江省政府采购网([http://www.zjzfcg.gov.cn](http://www.zjzfcg.gov.cn/new))发布中标公告**（中标人为中小企业的，其声明函将随中标结果同时公告）**，公告期限为1个工作日。 |
| 17 | 履约保证金 | 合同签订时，采购人按《中华人民共和国政府采购法实施条例》有关规定自行收取项目履约保证金。采购人要求中标或者成交供应商提交履约保证金的，供应商应当以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式提交。履约保证金的数额不得超过政府采购合同金额的1%。 |
| 18 | 付款方式 | 国库集中支付（采购人自行支付）详见各标项的商务要求表。根据《中华人民共和国中小企业促进法》《保障中小企业款项支付条例》《浙江省财政厅关于坚决打赢疫情防控阻击战进一步做好政府采购资金支持企业发展工作的通知》《浙江省财政厅关于进一步发挥政府采购政策 功能全力推动经济稳进提质的通知》《浙江省财政厅关于进一步发挥政府采购政策功能全力推进经济稳进提质的通知》等规范要求，采购人须在第四部分《招标需求》付款条件中，明确对相关企业在资金支付期限、预付款比例等方面的优惠措施。（备注：采购单位应当在政府采购合同中约定预付款，对中小企业合同预付款比例原则上不低于合同金额的40％，不高于合同金额的70%；项目分年安排预算的，每年预付款比例不低于项目年度计划支付资金额的40％，不高于年度计划支付资金额的70%；采购项目实施以人工投入为主的，可适当降低预付款比例，但不得低于20%。对供应商为大型企业的项目或者以人工投入为主且实行按月定期结算支付款项的项目，预付款可低于上述比例或者不约定预付款。） |
| 19 | 投标文件有效期 | 90天 |
| 20 | 合同签订时间 | 中标通知书发出后30日内。 |
| 21 | 招标方代理费用 | 0元 |
| 22 | 解释权 | 本招标文件的解释权属于浙江省政府采购中心。 |

**一、总 则**

（一）适用范围

仅适用于本次招标文件中采购项目的招标、投标、评标、定标、验收、合同履约、付款等行为（法律、法规另有规定的，从其规定）。

（二）定义

1.招标方：指组织本项目采购的浙江省政府采购中心。

2.投标人：指响应招标、参加投标竞争的法人、其他组织或者自然人。

3.采购人：指委托招标方采购本次货物、服务项目的国家机关、事业单位和团体组织。

4.货物：指招标文件规定投标人须向采购人提供的一切材料、设备、机械、仪器仪表、工具及其它有关技术资料和文字材料。

5.服务：指招标文件规定投标人须承担的劳务以及其他类似的义务。

6.项目：指投标人按招标文件规定向采购人提供的需求总称。

7.电子交易平台:指政府采购项目电子交易平台，即政采云平台。

**8.中小企业：是指在中华人民共和国境内依法设立，依据国务院批准的中小企业划分标准确定的中型企业、小型企业和微型企业，但与大企业的负责人为同一人，或者与大企业存在直接控股、管理关系的除外。**

**符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。**

（三）投标人及委托有关说明

1.如授权代表不是法定代表人，须有法定代表人出具的授权委托书**（格式见附件）。**

2.投标人投标所使用的资格、信誉、荣誉、业绩与企业认证必须为本法人所拥有。投标人投标所使用的采购项目实施人员必须为投标人员工（或投标人控股公司正式员工）。

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

4.投标人应仔细阅读招标文件的所有内容，按照招标文件的要求提交投标文件，并对所提供的全部资料的真实性承担法律责任。

（四）投标费用

不论投标结果如何，投标人均应自行承担所有与投标有关的全部费用（招标文件有其他相反规定除外）。

（五）质疑

1.投标人认为招标过程或中标结果使自己的合法权益受到损害的，可以在中标结果公告期限届满之日起七个工作日内，以书面形式向招标方提出质疑。

 2.质疑应当以书面形式提出，格式见《政府采购质疑和投诉办法》（财政部令第94号）附件范本，下载网址：浙江政府采购网(<http://zfcg.czt.zj.gov.cn/>)，位置：“首页-下载专区-质疑投诉模板”。供应商提出质疑应当提交质疑函和必要的证明材料。供应商应当在法定质疑期内一次性提出针对同一采购程序环节的质疑。

质疑函应当包括下列内容：

a.供应商的姓名或者名称、地址、邮编、联系人及联系电话；

b.质疑项目的名称、编号；

c.具体、明确的质疑事项和与质疑事项相关的请求；

d.事实依据；

e.必要的法律依据；

f.提出质疑的日期。

供应商为自然人的，应当由本人签字；供应商为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。质疑应明确阐述招标过程或中标结果中使自己合法权益受到损害的实质性内容，提供相关事实、依据和证据及其来源或线索，便于有关单位调查、答复和处理,质疑函不符合《政府采购质疑和投诉办法》相关规定的，应在规定期限内补齐的，招标方自收到补齐材料之日起受理；逾期未补齐的，按自动撤回质疑处理。

（六）招标文件的澄清与修改

1.投标人应认真阅读本招标文件，发现其中有误或有不合理要求的，投标人应当于公告发布之日起至公告期限满第7个工作日内以书面形式向招标方提出。招标方将在规定的时间内，在财政部门指定的政府采购信息发布媒体上发布更正公告，并以书面形式通知所有招标文件收受人。**逾期提出招标方将不予受理。**

2.招标方主动进行的澄清、修改：招标方无论出于何种原因，均可主动对招标文件中的相关事项，用补充文件等方式进行澄清和修改。

3.招标文件澄清、答复、修改、补充的内容为招标文件的组成部分。当招标文件与招标文件的答复、澄清、修改、补充通知就同一内容的表述不一致时，以最后发出的书面文件为准。

二、投标文件的编制

（一）投标文件编制工具

**投标文件编制工具为政采云电子交易客户端，下载网址：<http://zfcg.czt.zj.gov.cn/bidClientTemplate/2019-09-24/12975.html>，请自行下载并安装。**

（二）投标文件的组成

**本项目所称投标文件系指电子投标文件或备份投标文件。投标文件需按照本招标文件和电子交易平台的要求制作、加密并递交。**

**“电子投标文件”系指通过政采云电子投标客户端完成投标文件编制后生成并加密的数据电文形式的投标文件（文件扩展名为.jmbs），“备份投标文件”系指与“电子投标文件”同时生成的数据电文形式的电子文件（文件扩展名为.bfbs）。**

**电子投标文件每个标项由资质文件、技术商务文件、投标报价文件三部份组成，具体详见“第六章 投标文件格式附件”。备份投标文件的组成和内容等同电子投标文件。**

**注：法定代表人授权委托书、投标声明书、开标一览表必须按招标文件格式要求正确签署并加盖投标人公章。投标文件中所须加盖公章部分均采用CA签章。**

（三）投标文件的效力

电子投标文件未按时解密，投标人提供了备份投标文件的，以备份投标文件作为依据，否则视为投标文件撤回。电子投标文件已按时解密的，备份投标文件自动失效。

（四）投标文件的语言及计量

1.投标文件以及投标人与招标方就有关投标事宜的所有来往函电，均应以中文简体字书写。除签名、盖章、专用名称等特殊情形外，投标文件中以中文汉语以外的文字表述部分视同未提供。

2.投标计量单位，招标文件已有明确规定的，使用招标文件规定的计量单位；招标文件没有规定的，应采用中华人民共和国法定计量单位（货币单位：人民币元），否则将作无效标处理。

（五）投标文件的有效期

1.自投标截止日起90天内投标文件应保持有效。有效期不足的投标文件将作无效标处理。

2.中标供应商的投标文件自开标之日起至合同履行完毕止均应保持有效。

（六）投标文件的签署和包装

**1.电子投标文件部分：**

**（1） 投标人应根据本招标文件和电子交易平台规定的格式和顺序编制电子投标文件并进行关联定位，投标文件内容不完整、编排混乱、关联错误导致投标文件被误读、漏读或者查找不到相关内容的，是投标人的责任。**

**（2）投标文件须由投标人在规定位置盖章并由法定代表人或法定代表人的授权委托人签署，投标人应写全称。**

**（3）投标文件不得涂改，若有修改错漏处，须加盖投标人公章或者法定代表人或授权委托人签名或盖章。投标文件因字迹潦草或表达不清所引起的后果由投标人负责。**

**2.投标人选择递交备份投标文件的，备份投标文件另须满足以下条件：**

**（1）储存形式：U盘、DVD**

**（2）密封要求：外包装封面上应注明投标人名称、投标人地址、投标人联系方式（授权代表手机）、投标文件名称（备份投标文件）、投标项目名称、项目编号、标项及“开标时启封”字样，并加盖投标人公章。**

（七）投标报价

1.投标文件只允许有一个报价，投标报价应按招标文件中相关附表格式填报，该投标报价应与明细报价汇总相等，且不允许出现报价优惠等字样（明细出现“0”元，视同赠送，按无效标处理）。

2.投标报价应包含项目所需全部产品、服务，不得缺漏，是履行合同的最终价格（含货款、标准附件、备品备件、专用工具、包装、运输、装卸、保险、税金、货到就位以及安装、调试、培训、保修等一切税金和费用）。

3.投标报价金额到元为止，如投标报价总价出现角、分，将被抹除。

4.资质文件、技术商务文件中不得出现投标报价信息，否则按无效标处理。

（八）串通投标认定

有下列情形之一的，视为投标人串通投标，其投标无效：

1.不同投标人的投标文件由同一单位或者个人编制；

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；

（九）投标无效的情形

在评审时，如发现下列情形之一的，投标文件将被视为无效：

1.投标人未能提供合格的资格文件、投标有效期不足的；

2.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；

**3.仅提供备份投标文件的；**

**4.电子投标文件解密失败，且未在规定时间内提交备份投标文件的；**

**5.电子投标文件解密失败，虽然在规定时间内提交了备份投标文件，但是备份投标文件无法导入或者无法读取或者不符合本招标文件和电子交易平台要求的；**

6.投标文件未按招标文件要求签署、盖章的；

7.与招标文件有重大偏离、未满足带“▲”号实质性指标的投标文件；

8.招标需求中要求提供的产品属于节能清单中政府强制采购节能产品品目的，投标人未提供该清单内产品的；

9.投标报价超出招标文件中规定的预算金额或者最高限价的；

10.标项以赠送方式投标的、对一个标项提供两个投标方案或两个报价的；

11.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，且不能证明其报价合理性的；

12.投标人不接受报价文件中修正后的报价的；

13.未按本章“二、投标文件的编制”第七点投标报价要求报价的；

14.投标文件含有采购人不能接受的附加条件的；

15.投标人被视为串通投标的；

16.不符合法律、法规和本招标文件规定的其他实质性要求的。

（十）错误修正

**电子交易平台客户端里开标一览表录入的投标报价信息与扫描上传的报价文件不一致的，以扫描上传的报价文件为准。**

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

**1.投标文件中开标一览表内容与投标文件中相应内容不一致的，以开标一览表为准；**

**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；**

**4.总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。**

**同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价按照经投标人加盖公章后产生约束力，投标人不确认的，其投标无效。**

（十一）采购过程中的异常情况及处理措施

**采购过程中出现以下情形，导致电子交易平台无法正常运行，或者无法保证电子交易的公平、公正和安全时，招标方可中止电子交易活动：**

**1.电子交易平台发生故障而无法登录访问的；**

**2.电子交易平台应用或数据库出现错误，不能进行正常操作的；**

**3.电子交易平台发现严重安全漏洞，有潜在泄密危险的；**

**4.病毒发作导致不能进行正常操作的；**

**5.其他无法保证电子交易的公平、公正和安全的情况。**

**出现前款规定情形，不影响采购公平、公正性的，招标方可以待上述情形消除后继续组织电子交易活动，也可以决定某些环节以纸质形式进行；影响或可能影响采购公平、公正性的，应当重新采购。**

**三、开、评标程序及评标委员会的评审程序**

**（一）组织开标**

招标方将按照招标文件规定的时间、地点和程序组织开标，各投标人授权代表及相关人员**均应当准时在线参加**，无关人员不得进入开标现场。**投标人如未准时在线参加的**，事后不得对采购相关人员、开标过程和开标结果提出异议。

**1. 落实工作场地、设施，检查录音录像采集设备运行情况，验证电子交易平台是否能正常登录。**

**2. 开标由招标方主持，主持人介绍开标现场的人员情况，宣读递交投标文件的投标人名单、开标纪律、应当回避的情形等注意事项。**

**3.投标截止时，电子交易平台自动提取所有电子投标文件。招标方点击[开始解密]按钮后，投标人可以在线解密，解密时限为30分钟。**

**4.投标人应当在解密时限内完成解密，如所有投标人的电子投标文件都已经解密完成的，则电子交易平台自动结束解密。如有任一投标人未解密，电子交易平台会在解密时限截止时自动结束解密。**

**解密时限内未完成解密且按规定提供了备份投标文件的，招标方将拆封其备份投标文件，并导入电子交易平台。**

**5.评标委员会在商务和技术评审结束后，主持人通过电子交易平台宣告商务和技术评审无效投标人名称及理由，有效投标人的商务和技术得分情况。**

**6.招标方在电子交易平台开启投标人的报价文件信息，投标人对报价信息进行确认。投标人对报价信息不予确认的不影响后续评标过程。**

**7.评标委员会经商议认为需要投标人作出必要澄清或说明的，应当通过电子交易平台交换数据电文。评标委员会给予投标人提交澄清或说明的时间为半小时，投标人已经明确表示澄清或说明完毕的除外。**

**8.在电子交易平台上公布评审结果。**

**特别说明：政采云公司如对电子化开标及评审程序有调整的，按调整后的程序操作。**

**（二）组织评标程序**

招标方将按照招标文件规定的时间、地点和程序组织评标，各评审专家及相关人员应参加评审活动并接受核验、签到，无关人员不得进入评审现场。

1、开启开标场地录音录像采集设备，并确保正常运行。

2、按规定统一收缴、保存评标现场相关人员通讯工具。

3、介绍评审现场的人员情况，宣布评审工作纪律，告知评审人员应当回避情形；组织推选评标委员会组长。

4、宣读提交投标文件的供应商名单，组织评标委员会各位成员签订纸质形式的《政府采购评审人员廉洁自律承诺书》。

5、采购人可以在评标前说明项目背景和采购需求，说明内容不得含有歧视性、倾向性意见，不得超出招标文件所述范围。说明应当提交书面材料，并随采购文件一并存档。

6、根据需要简要介绍招标文件（含补充文件）制定及质疑答复情况、按书面陈述项目基本情况及评审工作需注意事项等，让评审专家尽快知悉和了解所评审项目的采购需求、评审依据、评审标准、工作程序等；提醒评标委员会对客观评审项目应统一评审依据和评审标准，对主观评审项目应确定大致的评审要求和评审尺度；对评审人员提出的有关招标文件、投标文件的问题进行必要的说明、解释或讨论。

7、采购人代表对投标人资格文件进行审查并以开标当日为准对投标人“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）信用记录情况进行核实，资格不符合的，应组织相关投标人代表进行陈述、澄清或申辩。

8、评标委员会组长组织评审人员独立评审。评标委员会对拟认定为投标文件无效，应组织相关投标人代表进行陈述、澄清或申辩；招标方可协助评标委员会组长对打分结果进行校对、核对并汇总统计；对明显畸高、畸低的评分（其总评分偏离平均分30%以上的），评标委员会组长应提醒相关评审人员进行复核或书面说明理由，评审人员拒绝说明的，由现场监督员据实记录；评审人员的评审、修改记录应保留原件，随项目其他资料一并存档。

9、做好评审现场相关记录，协助评标委员会组长做好评审报告起草、有关内容电脑文字录入等工作，并要求评标委员会各成员签字确认。

10、评审结束后，招标方应对评标委员会各成员的专业水平、职业道德、遵纪守法等情况进行评价；同时按规定向评审专家发放评审费，并交还评审人员及其他现场相关人员的通讯工具。

**11、招标方将在《中标公告》中，公开评标委员会对每个投标人的《评分明细》以及《得分汇总表》情况。**

**（三）评审程序**

1、在评审专家中推选评标委员会组长。

2、评标委员会组长召集成员认真阅读招标文件以及相关补充、质疑、答复文件、项目书面说明等材料，熟悉采购项目的基本概况，采购项目的质量要求、数量、主要技术标准或服务需求，采购合同主要条款，投标文件无效情形，评审方法、评审依据、评审标准等。

3、评审人员对各投标人投标文件的有效性、符合性、完整性和响应程度进行审查，确定是否对招标文件作出实质性响应。

4、评审人员按招标文件规定的评审方法和评审标准，依法独立对投标人投标文件进行评估、比较，并给予评价或打分，不受任何单位和个人的干预。

5、评审人员对各投标人投标文件非实质性内容有疑议或异议，或者审查发现明显的文字或计算错误等，及时向评标委员会组长提出。经评标委员会商议认为需要投标人作出必要澄清或说明的，应通知该投标人以书面形式作出澄清或说明。授权代表未按时确认或拒绝澄清说明或澄清说明的内容改变了投标文件的实质性内容的，评标委员会有权对该投标文件作出不利于投标人的评判。书面通知及澄清说明文件应作为政府采购项目档案归档留存。

6、评审人员需对招标方工作人员唱票或统计的评审结果进行确认，现场监督员应对评审结果签署监督意见。如发现分值汇总计算错误、分项评分超出评分标准范围、客观评分不一致以及存在评分畸高、畸低情形的，应由相关人员当场改正或作出说明；拒不改正又不作说明的，由现场监督员如实记载后存入项目档案资料。

7、评标委员会根据评审汇总情况和招标文件规定确定中标候选供应商排序名单。

8、起草评审报告，所有评审人员须在评审报告上签字确认。

**四、评审原则**

**1.评标委员会必须公平、公正、客观，不带任何倾向性和启发性；不得向外界透露任何与评标有关的内容；任何单位和个人不得干扰、影响评标的正常进行；评标委员会及有关工作人员不得私下与投标人接触。**

**2.评审专家因回避、临时缺席或健康原因等特殊情况不能继续参加评审工作的，应按规定更换评审专家,被更换的评审人员之前所作出的评审意见不再予以采纳，由更换后的评审人员重新进行评审。无法及时更换专家的，要立即停止评审工作、封存评审资料，并告知投标人择期重新评审的时间和地点。**

**3.评审人员对有关招标文件、投标文件、样品或现场演示（如有）的说明、解释、要求、标准存在不同意见的，持不同意见的评审人员及其意见或理由应予以完整记录，并在评审过程中按照少数服从多数的原则表决执行。对招标文件本身不明确或存在歧义、矛盾的内容，应作对投标人而非采购人有利的解释；对因招标文件中有关产品技术参数需求表述不清导致投标人实质性响应不一致时，应终止评审，重新组织采购。评审人员拒绝在评审报告中签字又不说明其不同意见或理由的，由现场监督员记录在案后，可视为同意评审结果。**

**4.财政部令第87号《政府采购货物和服务招标投标管理办法》第三十一条规定：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。**

**非单一产品采购项目，采购人应当根据采购项目技术构成、产品价格比重等合理确定核心产品，并在招标文件中载明。多家投标人提供的核心产品品牌相同的，按前款规定处理。**

**5.财政部令第87号《政府采购货物和服务招标投标管理办法》第六十条规定：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。**

**五、确定中标供应商的原则**

 1.项目由评标委员会根据第三章《评标办法与评分标准》规定提出中标候选人排序。

 2.采购人应当自收到评标报告之日起５个工作日内，在评标报告确定的中标候选人名单中按顺序确定中标人，或者采购人委托评标委员会在评标报告确定的中标候选人名单中按顺序确定中标人。采购人在收到评标报告5个工作日内未按评标报告推荐的中标候选人顺序确定中标人，又不能说明合法理由的，视同按评标报告推荐的顺序确定排名第一的中标候选人为中标人。

 3.采购结果经采购人确认后，招标方将于2个工作日内在浙江省政府采购网上发布中标公告，通过电子交易平台统一签发《中标通知书》。

**六、合同授予**

**（一）签订合同**

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

2.中标人拖延、拒签合同的,将被取消中标资格。

**3.对于通过预留采购项目、预留专门采购包、要求以联合体形式参加或者合同分包等措施签订的采购合同，应当明确标注本合同为中小企业预留合同。其中，要求以联合体形式参加采购活动或者合同分包的，应当将联合协议或者分包意向协议作为采购合同的组成部分。**

**（二）履约保证金**

1.合同签订时，采购人按《中华人民共和国政府采购法实施条例》有关规定自行收取项目履约保证金。采购人要求中标或者成交供应商提交履约保证金的，供应商应当以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式提交。履约保证金的数额不得超过政府采购合同金额的1%。

2.按合同约定办理履约保证金退还手续。

**七、货款的结算**

货款由采购人按采购文件规定的付款方式自行支付。纳入国库集中支付的，按照国库集中支付有关规定付款。

资金支付进度：采购人对于满足合同约定支付条件的，自收到发票后7个工作日内将资金支付到合同约定的供应商账户。迟延支付中小企业款项的，供应商可要求采购人支付逾期利息。

预付款：根据《中华人民共和国中小企业促进法》《保障中小企业款项支付条例》《浙江省财政厅关于坚决打赢疫情防控阻击战进一步做好政府采购资金支持企业发展工作的通知》《浙江省财政厅关于进一步发挥政府采购政策 功能全力推动经济稳进提质的通知》《浙江省财政厅关于进一步发挥政府采购政策功能全力推进经济稳进提质的通知》等相关规范，对预付款支付要求如下：

1.对中小企业合同预付款比例原则上不低于合同金额的40％，不高于合同金额的70%；

2.项目分年安排预算的，每年预付款比例不低于项目年度计划支付资金额的40％，不高于年度计划支付资金额的70%；

3.采购项目实施以人工投入为主的，可适当降低预付款比例，但不得低于20%。

4.对供应商为大型企业的项目或者以人工投入为主且实行按月定期结算支付款项的项目，预付款可低于上述比例或者不约定预付款。

备注：在签订合同时，供应商明确表示无需预付款或者主动要求降低预付款比例的，采购单位可不适用前述预付款比例的规定。

**第三章 评标办法及评分标准**

根据《中华人民共和国政府采购法》等有关法律法规，结合本项目的实际需求，制定本办法。

**一、总则**

本次评标采用综合评分法，总分为100分。合格投标人的评标得分为各项目汇总得分，中标候选资格按评标得分由高到低顺序排列，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，按技术得分由高到低顺序排列。评分过程中采用四舍五入法，并保留小数2位。

**二、分值的计算**

技术、资信、商务及其他分按照评标委员会成员的独立评分结果汇总后的算术平均分计算，计算公式为：

技术、资信商务及其他分=评标委员会所有成员评分合计数/评标委员会组成人员数

投标人评标综合得分=价格分+(技术分+资信商务及其他分)

**特别提醒：**评标委员会对每个投标人的评分明细以及得分汇总表情况在中标公告中公布。

**三、评标内容及标准**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **评分类型** | **评分标准** | **分值** |
| **1** | **报价** | **(最低报价/投标报价)\*最大分值** | **0~30** |
| **1** | **技术** | **符合明确指标参数得24分。标有“★”的，属负偏离或缺漏项的每项扣3分；未标“★”的，属负偏离或缺漏项的每项扣2分；标有“★”的和未标“★”的，负偏离共达到5个及以上的按重大偏离处理。** | **0~24** |
| **2** | **技术** | **对性能指标、技术参数属正偏或高配的、有先进程度的正偏离每项加1分（最高分为5分），无实质性意义的正偏离不加分。** | **0~5** |
| **3** | **技术** | **提供市场监管总局关于发布参与实施政府采购节能产品、环境标志产品认证机构名录的公告（2019第16号）通过《参与实施政府采购节能产品认证机构名录》认证机构认证的环境标志产品认证证书或者证书的查询网址及截图的，得1分, 节能产品认证证书或者证书的查询网址及截图的，得1分。** | **0~2** |
| **4** | **技术** | **所投产品的技术先进性。** | **0~4** |
| **5** | **技术** | **系统集成的具体技术解决方案。** | **0~5** |
| **6** | **技术** | **项目系统集成具体实施计划。** | **0~5** |
| **7** | **技术** | **系统集成项目组实施人员能力情况（详见招标需求）。** | **0~5** |
| **8** | **商务资信** | **项目维护计划（驻点人员安排，定期巡检，备品备件等情况）的有效性等。** | **0~5** |
| **9** | **商务资信** | **售后服务的响应情况（对用户故障响应、处理等）。** | **0~5** |
| **10** | **商务资信** | **培训方案、计划的可行性及合理性。** | **0~2** |
| **11** | **商务资信** | **公司技术力量情况（详见商务要求表）。** | **0~5** |
| **12** | **商务资信** | **经验及业绩（详见商务要求表）。** | **0~3** |

**第四章 招标需求**

**特别说明：**

**1.除采购文件明确的品牌外，欢迎其他能满足本项目技术需求且性能与所明确品牌相当的产品参加。**

**2.需求中不允许偏离的实质性要求和条件，以“▲”号标明，如投标人未响应的，将被视为无效。**

**3.核心产品在各标项内容中明确，如出现同品牌情况的，评标委员会根据评审原则第4条规定执行。**

**4.采购人拟采购的产品属于政府强制采购节能品目的，（详见《关于印发节能产品政府采购品目清单的通知》财库〔2019〕19号），需按《财政部 发展改革委 生态环境部 市场监管总局 关于调整优化节能产品、环境标志产品政府采购执行机制的通知》财库〔2019〕9号要求执行，但无对应细化分类或节能清单中的产品无法满足工作需要的，采购人应当在详细需求中标明并说明理由，否则按照前附表第三点要求执行。**

##

## **标项1:****浙江省委网信办（本级）通用设备及网络安全升级项目**

随着平台业务的扩展，本平台业务在互联网区、网信专网区、政务外网区、网信数据中心四个网络区域进行开展，发现当前在日志审计、终端安全、上网行为管理、应用防护、网络准入、认证访问、运维管理、加密通信以及数据安全等方面的存在安全弱点，基础资源承载能力以及在流量日志汇聚能力上存在不足，现需针对能力短板进行有针对性的提升建设。

### 1、网信专网区

* + **提升日志数据汇聚能力**

由于需要对接移动、联通、电信的日志数据，需对现有日志数据汇聚能力进行扩容，从而满足多维度分析能力，提高安全态势感知预警能力与安全监测水平。

* + **建设终端安全及管理能力**

在重要PC与服务器上安装主机安全及管理系统，通过对终端上用户行为事件、系统安全事件、病毒查杀、防暴力破解、抗CC攻击、网络通信数据等进行归一化处理和关联分析，提供针对性的技术手段对服务器进行防护，对终端资产和安全情况进行全面掌握、清晰、准确判断存在的安全风险，对终端发生的安全事件及时响应处理。

* + **建设上网行为管理能力**

建设上网行为管理能力，让上网行为有据可查、合法合规。对网络中的访问、即时交互系统进行精细化识别和控制。并利用智能流控、智能阻断、智能路由等技术，配合创新的上网行为审计功能、清晰易用的管理日志功能等，提供全面、完善的上网行为审计。

* + **建设应用防护能力**

为了增强网络安全协调指挥平台的应用防护能力，提高与国家、地市等地进行信息交互时的应用防护水平，通过在部署专业WEB应用防火墙，强化应用层防护措施，实现对目标WEB应用系统网站的深度应用攻击防护，抵御各类应用层攻击，如SQL注入、命令注入 、Cookie 注入、Cookie假冒、跨站脚本(XSS) 、敏感信息泄露、恶意代码、错误配置、隐藏字段、参数篡改、应用层拒绝服务等。

* + **建设统一的运维管理能力**

基于目前网信专网区的网络安全现状，急需提高统一的运维管控能力。随着后期专网区服务器及各种网络设备的增加，并考虑到专网区的安全特殊性，对设备的管理必须经过各种认证过程，通过部署堡垒机，建立统一的运维管控平台，运用运维审计系统自身的双因子认证引擎来弥补各系统的单一登陆方式，并在核心交换机上做访问控制，封杀其他一切运维管理通道，实现统一实名帐户管理与单点登录，对各种字符终端协议（SSH、TELNET等）、文件传输协议（FTP、SFTP等）、图形终端协议（RDP等）与web协议（http、https）等进行实时监控与历史查询溯源，满足单位运维内控的同时也减轻了运维工程师的日常运维的工作量。

* + **建设加密通信能力**

为加强网信办大楼和联通机房的通信安全，需新建该链路上的加密通信能力。对两者间的信息进行基于策略的访问控制和完成对通信数据的加密/解密。确保了网络的安全，能有效防止非法分子的攻击。

实现对数据的机密性进行保护，利用加密算法加密用户数据，即使非授权的用户得到数据也不能知道其中的内容；实现对数据的完整性进行保护，数据在传输过程中不被非法用户修改，或者，如果网络中传输数据包被非法用户修改，数据的接收方能发现这是个被非法修改的数据包。

* + **建设网络接入控制冗余能力**

为加强网信专网的网络接入控制能力，保障24小时不间断的进行强控制，需再建一套网络接入控制系统，用以解决设备接入问题，规避非法设备接入引起的病毒传播、数据泄露、恶意攻击、木马植入、静默监听等安全隐患。

* + **建设网络安全运营保障平台（零信任体系）国产化能力**

目前省网信面临着网络环境快速发展下的自主创新网络安全新挑战，随着省委网信办内外网业务系统的建设，国产化环境下业务访问和数据交互的业务场景日趋普遍，如何提供国产化环境下的安全、高效的业务访问和数据安全访问成为国产化业务建设过程中难以绕过的技术难题。

本期针对网信专网国产化网络访问环境，搭建零信任网络安全运营保障平台，构建以身份为中心的动态访问控制，是在不可信的现代网络环境下，以身份为中心，通过动态访问控制技术，以细粒度的应用、接口、数据为核心保护对象，遵循最小权限原则，构筑端到端的逻辑身份边界。本次针对专网和互联网分别建设零信任网络安全运营保障平台，主要进行如下建设：

1、终端环境感知与基础安全

通过PC客户端实现终端安全与环境感知。环境感知能力提供物理环境感知、基础安全感知、应用合规感知、系统安全感知、健康状态感知五大感知能力；终端基础能力包括杀软、漏洞补丁、安全基线等能力，为后续的访问控制提供数据支撑。

2、业务隐藏与保护

通过业务代理对应用资源和服务进行业务隐藏，应用服务为隐身状态，不再直接暴露在网络上。恶意用户无法进行端口扫描和嗅探攻击。同时对业务访问流量进行引流和隧道加密。采用SPA单包授权机制实现端口隐藏，未授权终端无法连接服务端口。只有通过认证的合法用户和终端的业务流量才能到达数据区，业务代理可以根据风险实时阻断访问。

3、动态访问控制

自适应认证：将访问主体（人员、设备和应用）进行数字化身份管理，实现主体组合认证和自适应动态认证。先完成设备认证，再进行用户认证，都成功后才能连接应用，实现层层管控。

动态授权：在RBAC的基础上，叠加IP、时间、设备、地理位置和设备安全要求等属性，实现基于ABAC的属性授权；基于历史行为和访问基线等上下文信息，在RBAC岗位角色授权的基础上，进行权限动态过滤。

风险响应：针对访问主体在访问中存在的风险信息、信任度变化和其他异常，触发相应的指令，如二次认证、退出登录、账号锁定、冻结权限等，实现动态的访问控制能力。

* + **建设数据安全分级与风险评估能力**

通过网络嗅探、协议扫描技术对指定范围内的数据源进行扫描，动态发现数据资产，防止出现对数据的管理盲区。通过抽取样例数据结合内置识别模型和规则分析，完成敏感数据识别和数据分类分级，同时，提供数据安全评估能力。

数据资产风险梳理：对数据资产所在环境的风险状况进行梳理，包括对数据资产存储环境的漏洞状况、安全配置基线及使用隐患等方面进行有效评估，并提供相关安全改进策略及建议。

敏感数据梳理：内置多种发现规则，基于数据内容的识别，不依赖于用户的元数据管理系统、字段名或字段注释等信息。支持用户基于自身需求自定义敏感对象，实现对敏感数据的自动发现和标识。

数据分类分级：结合数据资产梳理、敏感数据发现及梳理、敏感数据分类分级、用户及敏感资产权限梳理，对数据进行全面摸底。内置政府、金融、运营商等行业模板，通过数据资产发现、对业务数据识别和分类，根据业务属性及数据属性，进行分级管理，识别客体数据类别、级别，结合身份进行有限的权限控制。

* + **建设数据脱敏与水印能力**

随着数据共享和开放的推进，加大了数据泄露和被非法利用的风险，传统的基于边界隔离的围栏式安全保护方法将彻底不能满足数据流动下的安全防护需求，亟需构建敏感数据使用安全控制系统。通过对数据的脱敏确保数据流动安全，数据防泄露保障传输、使用中的数据安全，数据水印保障数据的追溯。

数据静态脱敏：通过脱敏技术进行数据变形，实现敏感隐私数据的可靠保护，从而起到信息安全保护的作用。敏感数据从生产环境脱敏完毕之后再下发到非生产环境中使用，解决测试、开发库需要生产库的数据量与数据间的关联，以排查问题或进行数据分析等，但又不能将敏感数据存储于非生产环境的问题。

数据水印：用隐秘的手段将版权说明、用户身份等水印信息嵌入到数据中以有效保护数据版权。在数据库中寻找有效的冗余空间，在不影响数据使用的前提下嵌入水印信息，并在数据泄露以后可以高效溯源，数据溯源算法应不易绕开，通过可回溯算法，便于追溯泄漏源。

### 2、互联网区

* + **建设终端安全及管理能力**

在重要PC与服务器上安装主机安全及管理系统，通过对终端上用户行为事件、系统安全事件、病毒查杀、防暴力破解、抗CC攻击、网络通信数据等进行归一化处理和关联分析，提供针对性的技术手段对服务器进行防护，对终端资产和安全情况进行全面掌握、清晰、准确判断存在的安全风险，对终端发生的安全事件及时响应处理。

* + **建设日志数据汇聚能力**

由于需对接部分无法接入网信专网的流量探针日志，需在互联网区建立日志数据汇聚能力，从而满足多维度分析能力，提高安全态势感知预警能力与安全监测水平。

* + **建设网络安全运营保障平台（零信任体系）国产化能力**

本期针对互联网国产化网络访问环境，搭建零信任网络安全运营保障平台，构建以身份为中心的动态访问控制，是在不可信的现代网络环境下，以身份为中心，通过动态访问控制技术，以细粒度的应用、接口、数据为核心保护对象，遵循最小权限原则，构筑端到端的逻辑身份边界。本次针对专网和互联网分别建设零信任网络安全运营保障平台，主要进行如下建设：

1、终端环境感知与基础安全

通过PC客户端实现终端安全与环境感知。环境感知能力提供物理环境感知、基础安全感知、应用合规感知、系统安全感知、健康状态感知五大感知能力；终端基础能力包括杀软、漏洞补丁、安全基线等能力，为后续的访问控制提供数据支撑。

2、业务隐藏与保护

通过业务代理对应用资源和服务进行业务隐藏，应用服务为隐身状态，不再直接暴露在网络上。恶意用户无法进行端口扫描和嗅探攻击。同时对业务访问流量进行引流和隧道加密。采用SPA单包授权机制实现端口隐藏，未授权终端无法连接服务端口。只有通过认证的合法用户和终端的业务流量才能到达数据区，业务代理可以根据风险实时阻断访问。

3、动态访问控制

自适应认证：将访问主体（人员、设备和应用）进行数字化身份管理，实现主体组合认证和自适应动态认证。先完成设备认证，再进行用户认证，都成功后才能连接应用，实现层层管控。

动态授权：在RBAC的基础上，叠加IP、时间、设备、地理位置和设备安全要求等属性，实现基于ABAC的属性授权；基于历史行为和访问基线等上下文信息，在RBAC岗位角色授权的基础上，进行权限动态过滤。

风险响应：针对访问主体在访问中存在的风险信息、信任度变化和其他异常，触发相应的指令，如二次认证、退出登录、账号锁定、冻结权限等，实现动态的访问控制能力。

### 3、政务外网区

* + **建设政务外网与网信专网的物理隔离**

建设政务外网与网信专网的物理隔离能力，实现政务外网与网信专网的信息摆渡，保证两个网络之前没有直接的物理通路。通过分时地进行两个网络中的数据交换，从而达到隔离与交换的目的。

* + **建设日志审计能力**

建设日志审计能力。通过全面收集网络设备、安全设备、主机、应用及数据库的Syslog、SNMP等日志协议信息，帮助建立信息资产的综合性管理平台，通过对网络设备、安全设备、主机和应用系统日志进行全面的标准化处理，及时发现各种安全威胁、异常行为事件，并通过周期性合规型和事件型报表为管理人员提供全局的视角，确保单位业务的不间断运营安全。并增加了对安全事件的追溯的能力及手段，方便管理员进行事件跟踪和定位，并为事件的还原提供有力证据。从而满足等保2.0的合规要求。

* + **建设上网行为管理能力**

建设上网行为管理能力，让上网行为有据可查、合法合规。对网络中的访问、即时交互系统进行精细化识别和控制。并利用智能流控、智能阻断、智能路由等技术，配合创新的上网行为审计功能、清晰易用的管理日志功能等，提供全面、完善的上网行为审计。

### 4、网信数据中心

* + **云平台建设**

本次云平台目定位为面向网信专网基础设施资源自主可控云平台的建设，采用云建设方式并提供IaaS服务，通过改造构建出独立的网信自主可控云资源模块，部署所需的网络资源、计算资源、存储资源、备份资源及云管理服务平台等设备，对外提供基础设施资源（IaaS层）,同时试点建设部分PaaS服务，重点支持网信办未来专网业务系统统一入云部署需求。

为保证本项目中系统能够长期、安全、稳定、可靠、高效的运行，需满足以下通用技术需求：

* 系统平均年故障时间＜48小时；
* 系统可用性99%；
* 系统操作平均响应时间：简单处理响应时间≤2秒，复杂处理响应时间≤4秒，超过时间需准确的进度提示；
* 页面响应时间不考虑网络延迟、拥堵、文件大小等因素的影响前提下，Web查询的响应时间＜2秒；
* 应用系统具备高易用性、高可靠性、高兼容性、高健壮性，能够提供7×24小时的连续运行能力，具有较强的系统安全性和灾难恢复能力；
* 系统访问控制应覆盖到功能模块、数据、角色级。

本次云平台需要兼容原有商用X86架构112CPU超融合，同时为了满足未来信创资源池的扩容要求。做到多个资源池统一调度，统一管理。

云平台通过基于自主可控基础设施服务层的建设，构建自控可控资源池，为后续各市直单位业务应用系统迁移提供安全可靠的资源环境。

目前安全可靠CPU主要有鲲鹏、海光、龙芯、飞腾、兆芯、申威等，其中涵盖了ARM、MIPS以及自主可控X86等底层技术路线。本云平台解决方案，支持不同异构芯片的管理，并且兼容不同软件厂家，满足不同的业务场景需求。

本项目建设云平台基础设施服务层总体架构如下图所示：

* + **金华灾备中心存储扩容**

目前在前期建设中，网信办已形成杭州电信机房、移动机房和金华灾备机房的两地三中心架构。



目前金华机房内仅仅包含5节点超融合集群，无法做到杭州机房全量业务数据备份（除探针日志数据外）。

本次将在异地数据备份中心（距离浙江省网信办200km外的金华机房），部署一套高性能、高并发的备份软件，后挂集中式存储作为备份数据存储介质。

首先将备份软件安装到现有利旧的服务器上，整体作为备份策略主机，在杭州电信、移动网信办机房对重要的50T数据进行全量备份，备份介质为集中式存储。在全量备份后，将备份策略主机及备份介质运输至金华数据机房，后续进行关键业务的增量备份。

* + **网络扩容**

目前网信办超融合集群的管理网络采用复用管理网与业务网融合的方式。随着网络建设的高速发展，网络覆盖要求在不断增加，并随着业务的发展，机房中不同种类的通信设备也在不断增加。此外随着市场竞争的不断增强，对网络故障响应时间的要求也不断严格。因此对于网络维护工作而言，不但工作量增加，而且压力不断在增加。当网络上设备出现问题，处理速度有限。另外，由于设备数量较多，设备品牌也较多，通过单一的第三方集中网管进行配置管理能实现的功能有限，且存在部署上的地址规划问题。因此需要找到一种更稳定、更安全、更方便、更快捷的综合网络设备的管理方式。

根据政策导向，未来将会扩容信创资源池，将业务网与管理网融合的方式，目前的交换机带宽无法满足将业务流和管理流同时纳管，容易导致业务中断。

除此以外，目前专网的出口路由带宽已无法满足大业务的转发，且为配合流量的管理，需要提供具备大转发性能且能够将业务流量实时分析的高性能路由器。

由于此前管理网和业务网并非分开部署，容易导致上述问题，此次建设选择采用带外网管系统作为管理方法。带外网管能够实现设备紧急访问通道、集中访问控制、分级授权管理、操作日志记录、故障告警等功能。能够减少运营成本、提高运营效率、减少宕机时间、提高服务质量，在提高机房设备管理水平、加强设备运行维护功能、降低运营维护成本方面起着很重要的作用，也是符合网络建设依据的主流管理方式。



此次建设主要包括管理网的建设、出口路由的替换以及镜像流量的增加。

## 二、招标设备清单及技术要求

### 1、招标清单一览表

|  |  |  |
| --- | --- | --- |
| **序号** | **内容** | **数量** |
| 1 | 网信专网区 | 日志汇聚系统 | 1套 |
| 2 | 终端安全与管理系统 | 1套 |
| 3 | 上网行为管理系统 | 1台 |
| 4 | 应用防火墙**（核心产品）** | 2台  |
| 5 | 运维审计与风险控制系统 | 2台 |
| 6 | IPSec VPN | 2台 |
| 7 | 网络准入管理系统 | 1台 |
| 8 | 网络安全运营保障平台（零信任体系）（信创版） | 1套 |
| 9 | 数据安全分级与风险评估系统 | 1套 |
| 10 | 数据脱敏系统 | 1套 |
| 11 | 互联网区 | 终端安全与管理系统 | 1套 |
| 12 | 日志汇聚系统 | 1套 |
| 13 | 网络安全运营保障平台（零信任体系）（信创版） | 1套 |
| 14 | 政务外网区 | 安全隔离网闸 | 2台 |
| 15 | 日志审计分析平台 | 1套 |
| 16 | 上网行为管理系统 | 1台 |
| 17 | 网信数据中心 | 云管理平台 | 1套 |
| 18 | 备份软件 | 1套 |
| 19 | 备份存储 | 1套 |
| 20 | 千兆汇聚交换机 | 7台 |
| 21 | 千兆接入交换机 | 6台 |
| 22 | 千兆路由器 | 2台 |
| 23 | TAP交换机 | 2台 |
| 24 | 光模块 | 1套 |

### 2、设备技术规格要求

#### 1）网信专网区

##### 1、日志汇聚系统（1套）

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 产品资质要求 | 产品获得公安部计算机信息系统安全产品销售许可证，提供证书复印件 |
| 产品取得软件著作权登记证书，提供给证书复印件 |
| 产品获得全球IPv6论坛IPv6 Ready Logo 委员会颁发的《IPv6 Ready Logo认证》证书，提供证书复印件 |
| 产品获得中国网络安全审查技术与认证中心颁发的《中国国家信息安全产品认证证书》，提供证书复印件  |
| 性能要求 | 支持审计≥100个日志源 |
| 部署方式 | 支持分布式部署，支持页面一键添加子节点，自动进行绑定添加，采集器可以选择同步日志范围，按需转发数据 |
| 功能扩展 | 采用解决方案包上传对产品进行功能扩展，无需要代码开发 |
| 支持kafka日志接收转发、大数据安全域同步、APT沙箱报告转发等大数据联调功能，Kafka收发支持SSL加密。 |
| 日志收集 | 支持Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP协议日志收集；支持阿里云SLS日志的采集。 |
| 可通过接收协议限制日志接收速率，包括Http接收、syslog接收、SNMPtrap接收、TCP接收、WMI接收、aliyun接收。 |
| 支持使用代理(Agent)方式提取日志并收集，安装包支持界面下载，且安装支持可视化向导。 |
| 日志分析 | 内置5000+解析规则，支持对收集的5000+设备类型日志进行解析（标准化、归一化），解析维度多达200+，解析规则可以根据客户要求定制扩展； |
| 三维关联分析；支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件。 |
| 日志备份 | 可设置日志存储备份策略。包括系统日志保存期（天）、磁盘使用率百分比等策略； |
| 支持日志本地备份及恢复； |
| 支持日志备份自动传送到远程服务器； |
| 支持从远程仓库恢复数据； |
| 支持FTP、SAMBA、NFS和FILE，4种方式的远程服务器 |
| 应用性能监控（APM） | 通过在目标主机上安装Agent程序，支持监测目标主机的CPU利用率、内存使用率、磁盘使用率、磁盘使用情况、流量等信息。 |
| 告警功能 | 支持磁盘空间阈值告警，当磁盘使用率达到设定的阈值时可产生并外发告警；资产性能监控异常告警，对于监控的资产系统资源进行监测当指定指标使用率达到设定的阈值时可产生并外发告警；资产状态监控，当资产处于不活跃状态时可产生并外发告警；远程仓库状态监测可告警，当远程仓库可用性检测失败或备份包自动上传失败时可产生并外发告警 |
| 用户管理 | 用户支持双因子认证登录，双因子认证令牌支持绑定至具体用户； |
| 提供一键式故障排除功能； |
| 提供自助式的升级接口，支持对产品升级、规则升级。 |
| 资产管理 | 注册用户资产时，提供自动发现识别能力； |
| 资产拓扑支持按照实际的用户环境进行编辑发布并可以和资产进行绑定，拓扑可以显示资产采集的事件数量被采集资产的状态等信息。（须提供权威机构第三方检测报告） |
| 售后服务 | 提供7\*24小时原厂商400支持热线；提供不少于三年质保服务，包含但不限于系统升级等服务内容，本地需要至少5个（含）CISP-BDSA资质证书设备厂商人员提供支持。（须提供近三个月投标所在地社保证明） |
| 厂家资质 | 国家信息安全测评信息安全服务资质证书（安全工程类三级），提供证书复印件； |
| 国家信息安全测评信息安全服务资质证书（风险评估二级），提供证书复印件； |

##### 2、终端安全与管理系统（1套）

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 产品资质要求 | 产品通过IPv6论坛IPv6 Ready Logo委员会认证并获得认证证书，提供证书复印件。 |
| 通过公安部检测获得网络版防病毒产品（一级品）销售许可证书，提供证书复印件。 |
| 规格要求 | 支持200套服务器防护，50套终端防护。 |
| 基本功能 | 全网风险可视 | 支持当前待处理高危风险展示，包括弱口令、待处理病毒、待处理漏洞数据，并支持一键跳转到对应处理页面 |
| 一体化安全策略 | 只支持自定义安全策略、安全策略可继承，内置多个初始策略模板，包括防护模板、审计模板 |
| 系统性能监控 | 支持对CPU、内存、磁盘读写、网络上下行流量达到配置阈值时告警。支持对CPU、内存达到一定阈值时客户端进行熔断。 |
| 资产指纹 | 支持自动收集终端资产信息，包括：计算机名称、内核版本、操作系统、处理器、主板、内存、硬盘、显卡、终端版本、病毒库版本、最近更新时间 |
| 高级威胁防护模块 | 支持对本机的扩展行为（信息收集、权限提升）进行监测，防止提权行为和信息泄露。 |
| 识别渗透过程中的隧道代理（端口映射、端口转发、内网代理），可阻断隧道代理搭建行为。 |
| 系统安全性模块 | 违规外联支持黑、白名单双模式，白名单模式可配置是否允许访问特定的网站和地址；黑名单模式可自定义恶意IP，支持黑名单告警和阻断。 |
| 移动存储介质管理：1.支持管理员对入网的移动存储介质进行注册，可以对已注册的移动介质进行管理，包括授权、启用、停用、删除、导出注册列表、行为监控及审计等。2.支持客户端自主申请移动存储介质注册，管理员统一对申请进行审批。3.支持管理员设置自动审批客户端注册请求。4.支持从资产维度、设备维度对存储介质的权限进行精细化设置，同一设备可针对不同的资产设置不同的读写权限，有效控制不明来历的移动存储可能带来的病毒传播等隐患。 |
| 防病毒模块 | 针对Windows系统，提供内核级的数据防护能力，保护文件不被恶意修改、加密等，可自定义配置保护的文件及目录，支持设置例外进程 |
| 告警功能 | 告警类型包括：护网高级威胁、系统防护、网络防护、Web应用防护。 |
| 告警内容至少包括：资产名称、IP地址、日志类型、风险概况、风险评级、事件发生时间等详细内容。告警方式包括：邮件告警、Syslog、短信告警及SNMP trap。 |
| 管理功能 | 集中管控 | 管理平台支持一键设置客户端卸载密码、一键卸载监控端、一键解除绑定、一键停止/恢复所有防护、一键关闭/重启主机、一键重启客户端、一键迁移资产。 |
| 用户管理 | 支持多级用户管理：租户管理员、租户。 |
| 可视化功能 | 能展示各个服务器或主机节点的信息，包括运行状态、活动规律、行为变化趋势和详细资料，以及历史行为数据查询、全局安全态势等。 |
| 安全服务 | 安全事件 | 支持监控用户和应用实时流速，包括用户名、应用名、用户组、上行速率、下行速率、总速率、会话数等信息，帮助管理员快速甄别网络异常行为；支持提供重大事件应急响应预案。 |
| 软件升级 | 提供3年的病毒库、程序升级服务。 |
| 应急响应 | 对于新发现的病毒、零日漏洞，厂商能够于24小时内作出响应，及时通知用户，并提供专门应急预案、处置工具或专杀工具。 |
| 技术支持 | 支持7\*24小时威胁溯源服务。 |
| 售后服务 | 提供7\*24小时原厂商400支持热线；提供不少于三年质保服务，包含但不限于系统升级等服务内容；本地需要至少5个（含）CISP-BDSA资质证书设备厂商人员提供支持。（须提供近三个月投标所在地社保证明） |
| 厂家资质 | 国家信息安全测评信息安全服务资质证书（安全工程类三级），提供证书复印件； |
| 知识产权管理体系认证证书，提供证书复印件。 |

##### 3、上网行为管理系统（1台）

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 规格要求 | 标准1U机柜型硬件平台，硬盘容量≥1TB SSD支持千兆接口总数≥6个支持万兆接口总数≥2个 |
| 性能要求 | 支持带宽≥750 Mbps最大并发连接数≥1,000,000每秒新建连接数≥20,000 |
| 部署模式 | 支持路由模式、透明（网桥）模式、混合模式、旁路模式；旁路部署支持直接加入2个以上物理接口，无需使用聚合接口；部署模式切换无需重启设备。 |
| 端口镜像 | 支持端口镜像功能，支持入流量、出流量和双向流量等维度镜像，支持将接口的流量镜像到另一个接口，方便网络问题定位。 |
| 接口 | 接口支持配置从属IP地址，每个接口支持至少200个从属IP。内外接口无固化，支持修改接口属性，修改接口IP类型、地址模式无需重启设备。 |
| 路由支持 | 支持基于入接口、源地址、目的地址、用户、服务、应用、时间、域名的策略路由。 |
| IPv6 | 支持IPv6/v4双栈，支持IPv6安全策略、包括审计策略、NAT策略、流量控制策略、会话控制策略、黑名单、白名单、认证策略等 |
| 接入认证 | 支持与浙政钉2.0平台同步组织架构，并能在用户管理界面呈现组织架构、登录用户、登录时间、在线时长等信息（提供功能截图证明） |
| 应用识别 | 应用特征不少于7000个，移动应用不少于2200个。支持自定义应用，包括但不限于数据包方向、协议、端口、IP地址、目标域名、关键字识别维度，数据包方向包括任意、请求数据、响应数据，关键字匹配模式支持文本或正则表达式；支持DNS域名学习模式，可引用数据包特征中的目标域名或指定域名。支持智能识别模式和快速识别模式。在智能识别模式下应用引擎尽可能地用各种方式识别网络流量；在快速识别模式下应用引擎将关闭部分智能分析功能以提高性能。 |
| 应用控制 | 可识别多种文件类型，包括电影、音频、文本、图片、压缩文件（zip、rar、gz、bz2、Z、tgz、tbz、7z、cab、bz等）、应用程序、Office系列等；并支持对应用的文件传输行为进行上传、下载、双向的文件类型过滤。支持基于协议、端口、策略的会话维持功能，老化时间不少于2000小时。 |
| URL识别与控制 | 支持基于DNS前置技术，实现在DNS解析阶段针对HTTP和HTTPS域名进行过滤，防止HTTPS域名过滤逃逸情况。 |
| 旁路阻断 | 支持在设备旁路部署时针对违规上网行为进行阻断过滤。 |
| SSL加密内容审计与控制 | 支持配置解密策略，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HTTPS域名库，预定义域名以及自定义域名；支持针对SSL解密证书进行自动推送。 |
| 流量管理 | 基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中（需提供配置界面截图证明） |
| 终端管理 | 支持对网络接入的终端进行可视化管理，展示终端详细信息、异常状态等，支持查看终端类型，以及终端详细信息（厂商，系统，端口等），支持查看终端类型分布（提供功能截图证明） |
| 防私接路由 | 针对私接网络行为，惩罚方式包括但不限于无操作、阻断和限速，阻断和限速支持自定义惩罚时长。 |
| 用户认证 | 支持IP准入、MAC准入、IP+MAC准入、本地认证、混合认证和免认证；支持用户MAC感知，当用户MAC地址变更后，要求重新认证，避免冒名认证现象；支持伪Portal抑制技术，支持通过HTTP302重定向或HTML-refresh方式抑制非正常的HTTP或HTTPS的页面请求，从而保障系统稳定高效运行；支持基于HTTPS协议推送认证页面。 |
| 非法外联管控 | 支持6种以上外联方式的检查，包含拨号行为、双网卡行为、有4G网卡、有无线网卡行为、连接非法wifi行为、连接外网行为等（提供功能截图证明） |
| 数据分析 | 支持监控用户和应用实时流速，包括用户名、应用名、用户组、上行速率、下行速率、总速率、会话数等信息，帮助管理员快速甄别网络异常行为；支持数据下钻跳转至详细列表，针对用户支持通过趋势图形式，按照时间顺序展示该用户网络会话和流量趋势，支持下钻跳转至详细列表访问的应用组成和流速情况。针对应用支持通过趋势图形式，按照时间顺序展示该应用会话和流量趋势，支持下钻跳转至详细列表使用该应用的用户、速率和会话数等情况。支持会话的统计与分析，支持统计会话源Top20、会话目的Top20，以趋势图方式展示并发会话、新建、TCP、UDP、其他协议等趋势信息；针对会话支持正向排名，支持数据下钻跳转至详细列表，深入钻取会话中用户、用户组、源目IP、源目端口、协议、连接类型、应用、流量、时间等信息；支持多条件组合形成筛选条件。 |
| 审计类法规 | 支持上网行为记录本地留存，方便事后行为回溯；支持将日志记录发送至第三方平台进行数据分析和呈现，发送数据支持蝶式交换加密算法 |
| 安全防护 | 支持本地安全防护，包括但不限于入侵防御、病毒防护、Web防护、威胁情报等，入侵防御规则不少于8600条，病毒防护规则不少于400万。 |
| 业务需要 | 针对内网用户的web访问质量进行检测，对整体网络提供清晰的整体网络质量评级，支持以列表形式展示访问质量差的用户名单，支持对单用户进行定向web访问质量检测（提供配置界面截图证明） |
| 管理员认证 | 支持管理员三权模式，默认包括权限管理员、账号管理员、审核员和管理员，各管理员权限制约；支持针对管理员分别设置精细化的读写权限和读写内容。 |
| 系统维护 | 支持SNMPv1、v2、v3版本，支持跨三层自学习MAC地址Web管理界面支持Ping、Traceroute、TCP Syn诊断工具，可支持基于接口、协议、IP地址、端口、应用进行网络抓包，并可下载导出分析 |

##### 4、应用防火墙（2台）

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 产品资质要求 | 产品获得公安部计算机信息系统安全产品销售许可证，提供证书复印件 |
| 产品取得软件著作权登记证书，提供证书复印件 |
| [产品需获得国家信息安全漏洞库兼容性资质证书](#_7.1.6_国家信息安全漏洞库兼容性资质证书_1)，提供证书复印件 |
| 规格要求 | 标准2U硬件平台，含2\*GE电管理口，4\*GE电业务口，4\*GE光业务口，硬盘≥2T，串口：1\*RJ45，标准可热插拔电源模块\*2  |
| 性能要求 | 网络吞吐量≥4GbpsHTTP应用吞吐量≥2GbpsHTTP最大并发数≥20万HTTP新建连接(CPS) ≥20000 |
| 基本 功能 | 部署模式 | 支持透明串接、反向代理、旁路镜像等多种部署模式部署，支持链路聚合  |
| 高可用 | 支持集群模式、主-主模式、主备模式、硬件BYPASS、软件BYPASS |
| HTTPS防护 | 支持HTTPS协议的选择可以选择SSL/TLS协议版本，可选SSLv3、TLS1.0、TLS1.1、TLS1.2 |
| 支持HTTPS站点SSL算法自动探测功能。探测时可以设置指定站点及端口，可以显示探测结果 |
| 支持透明串接和旁路反向代理下的HTTPS业务的安全防护 |
| 攻击检测 | 支持对跨站脚本(XSS)和注入式攻击（包括SQL注入、命令注入 、代码注入、文件注入、LDAP注入、SSI注入等）的检测防护 |
| 支持对HTTP请求关键字段进行合规性的检测（包括Host字段、User-Agent、Content-type字段等） |
| 支持对HTTP头部各字段内容长度进行限制并可以自定义调整限制大小，包括参数名长度、参数值长度、HTTP请求头部长度、URI长度、cookie长度、User-Agent长度、Content-type长度、Host长度等 |
| 支持识别HTTP报文常见的编码和编码攻击：URL解码、Base64解码、HTML解码、16进制转换、JSON解析、XML解析、PHP反序列解析、UTF-7解码等 |
| 应用层安全防护 | 支持对服务器响应安全设置，可通过选择不同的操作策略对响应头内容进行增删改。在修改响应头时，要保证触发条件的准确性，不得随意修改。 |
| 支持客户端安全防护，插入特殊的HTTP报头以保护客户端免受某些攻击包括但不限于增加以下安全报头：X-Frame-Options（用于防护客户端免受Clickjacking攻击）、X-Content-Type-Options（以防止浏览器将文件解释为内容类型声明以外的其他内容）、X-XSS-Protect（用于当检测到XSS攻击时，指示浏览器停止加载页面）、Content-Security-Policy（用于降低浏览器上的XSS风险和数据注入攻击） |
| 爬虫、扫描器等自动化工具的安全检测  | 内置安全规则可有效识别Acunetix、nessus 、WebScan、Webdump、AppScan 、等扫描器的扫描行为 |
| 内置安全规则可有效识别baidu、google、yahoo等常见网络爬虫的访问行为 |
| 高级功能 | 智能语义分析 | 内置对SQL注入、XSS攻击检测的语义分析规则  |
| 机器学习 | 1、具有机器学习安全引擎，可以对用户web业务系统建立安全的访问模型 ，学习的内容包括URL地址、URL请求参数等信息2、支持设定学习的周期，域名信息，可信任的客户端IP，不可信的客户端IP以及不学习的URL信息3、模型数据可以显示学习中的URL数量，学习完成的URL数量、检测中URL数量、学习失败的URL数量，同时可以显示各个阶段的占比情况4、具有通用的机器学习模型，数据模型可实现在线更新（须提供权威机构第三方检测报告）  |
| CC防护功能 | 支持根据细粒度条件对CC攻击进行检测和防护；匹配条件由URL参数、请求头部字段、目的IP、请求方法、地理位置组成；测量指标由请求速率、请求集中度、请求离散度组成；客户端检测对象由IP、IP+URL、IP+User\_Agent等参数组成；支持从请求头字段获取真实源IP地址（须提供权威机构第三方检测报告） |
| 区域态势分析和阻断 | 按地理区域对攻击次数等进行统计，并通过地图展示；支持在地图上对某一地理区域设置阻断此区域IP的访问（须提供权威机构第三方检测报告） |
| 威胁情报 | 支持威胁情报库在线同步，可主动发现恶意IP发起的访问行为，并进行告警和拦截，威胁情报库支持离线更新（须提供权威机构第三方检测报告） |
| 安全审计 | 能详细记录攻击事件的HTTP请求头信息，含请求的URL、UserAgent、POST内容，cookie等所有的请求头内容 |
| 能详细记录服务器响应头信息，服务器响应内容 |
| 日志报表管理 | 日志分析 | 根据产生的安全日志进行智能分析，提高人工分析效率，减小规则误判概率。 |
| 日志记录 | 支持记录应用防护日志、网络防护日志、CC防护日志、访问审计日志、防篡改日志、操作日志、系统日志、升级日志 |
| 访问审计  | 具备审计网站正常访问流量的能力，提供按小时，天、月份生成生成报表 |
| 能记录、查询所有用户对网站的访问情况，包括访问的URL、客户端IP、服务器返回的状态码（须提供权威机构第三方检测报告） |
| 售后服务 | 提供7\*24小时原厂商400支持热线；提供不少于三年质保服务，包含但不限于硬件保修、系统升级等服务内容；本地需要至少5个（含）CISP-BDSA资质证书设备厂商人员提供支持。（须提供近三个月投标所在地社保证明） |
| 厂家资质 | 国家信息安全测评信息安全服务资质证书（安全工程类三级），提供证书复印件 |
| 知识产权管理体系认证证书，提供证书复印件 |

##### 5、运维审计与风险控制系统（2台）

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 产品资质要求 | 通过公安部检测并获得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），提供证书复印件 |
| 产品获得由国家信息安全漏洞库颁发的《国家信息安全漏洞库兼容性资质证书》，提供证书复印件 |
| 产品需符合GB/T 18336-2015《信息技术 安全技术 信息技术安全评估准则》（idt ISP/IEC 15408:2008）,并获得由中国信息安全测评中心信息安全实验室颁发的《国家信息安全 信息技术产品安全测评证书》，级别应为EAL3+，提供证书复印件 |
| 拥有自主知识产权并获得计算机软件著作权登记证书，提供证书复印件 |
| 规格要求 | 机箱高度：2U含2千兆电口管理口，千兆业务电口\*4，千兆业务光口\*4硬盘容量：2T\*2，RAID 1内存≥16GUSB口：USB2.0口\*2串口：RJ45口\*1电源：1+1热插拔冗余电源USBkey\*1硬件加密卡\*1 |
| 性能要求 | 授权资产≥1000个并发字符连接数≥1000个并发图形连接数≥300个 |
| 设备部署 | 设备采用旁路部署,管理口和业务口须支持多链路端口绑定功能，防止单网卡或单线故障。 |
| 身份鉴别能力要求 | 应支持身份鉴别功能，功能应使用SM2/3/4等商用密码算法对登录的用户进行身份鉴别，保证用户身份的真实性。 |
| 数据传输机密性与完整性要求 | 数据传输机密性 | 应支持数据传输机密性功能，功能应使用SM2/3/4等商用密码算法保证重要数据在传输过程中的机密性。 |
| 数据传输完整性 | 应支持数据传输完整性功能，功能应使用SM2/3/4等商用密码算法保证重要数据在传输过程中的完整性。 |
| 数据存储机密性与完整性要求 | 数据存储机密性 | 本设备应使用SM2/3/4等商用密码算法对核心数据进行加密存储，保证数据存储的机密性。 |
| 数据存储完整性 | 本设备应使用SM2/3/4等商用密码算法对核心数据进行完整性校验，保证数据存储的完整性。 |
| 数据原发抗抵赖和数据接收抗抵赖 | 应使用SM2/3/4等商用密码算法对操作日志进行签名操作，保证数据的不可否认性。（需提供使用商用密码证明材料，如使用到第三方密码产品的，需提供第三方密码产品的《商用密码产品认证证书》及第三方密码产品厂家授权函） |
| 用户管理要求 | 用户角色 | 支持用户多角色划分功能，如系统管理员、部门管理员、运维员、审计管理员、密码管理员等，对各类角色需要进行细粒度的权限管理 |
| 用户管理和用户策略 | 支持用户的批量导入/导出；支持用户安全策略功能，如用户有效期、用户登录时间限制、用户登录IP范围等 |
| 单点登录认证 | 支持标准化对接CAS、JWT单点登录认证，且支持配置是否自动创建堡垒机中不存在用户 |
| 多用户双因子认证 | 基于不同的用户设置不同的双因子认证模式 |
| 设备管理要求 | 支持的协议和应用 | 支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP、rlogin；可通过应用发布的方式进行协议扩展，如数据库Oracle、MSSQL、MySQL、VMware vSphere Client、浏览器等客户端工具 |
| 登录模式 | 支持设备帐户和密码的自动登录、手工登录、二次自动登录模式 |
| 共享账户 | 支持设置共享账户，用于不同主机拥有相同账户名及密码的场景 |
| 数据库管理 | 数据库兼容性 | 标准支持DB2、oracle、mysql、sqlserver、PG、人大金仓、达梦数据库的协议运维代理，可实现自动登录，自动登录可直接调用本地windows系统的数据库客户端工具（包括ssms、sqlwb、workbench、mysql、DbVisualizer、plsql、sqlplus、toad、dbcmd、Quest Central、pgadmin3、psql、ksql、Isql、DIsql、DMmanger等），无需应用发布前置机 |
| 数据库双重审计 | 支持同时对数据库会话记录图形审计及命令提取 |
| 数据库双向审计 | 支持对数据库运维会话的上行和下行命令进行审计 |
| 工单流程要求 | 运维工单 | 运维人员可以向管理员申请需要访问的设备，申请时可以选择：设备IP、设备账户、运维有效期、备注事由等，并且运维工单以邮件方式通知管理员。 |
| 自动改密要求 | 主机自动改密 | 支持定期自动修改windows服务器、网络设备、linux/unix等目标设备密码功能，且自动改密不借助于Agent，无需开放445、135、139等高危端口；未借助于agent及相关端口 |
| 数据库/web自动改密 | 支持对数据库及Web应用的自动改密功能 |
| 账号切换改密 | 支持Unix/Linux系统账号自动改密功能。并支持账号切换改密功能，当root不能直接远程登录时，依旧可以修改root密码。 |
| 运维方式要求 | 专用客户端运维 | 支持Windows/Mac操作系统下C/S架构的堡垒机专用客户端，可通过此专用客户端登录堡垒机，对堡垒机进行简单的管理及运维资产操作。 |
| 运维客户端自带运维工具，可不依赖 xshell/Securecrt/mstsc等工具进行运维操作 |
| 客户端还至少需支持资产分组、资产连通性检测，批量运维、资产运维审批、命令审批、二次运维审批等能力。其中资产分组操作支持个性化设置，即每个运维人员可单独设置分组，相互之间独立。 |
| 客户端支持VPN登录功能 |
| H5运维 | H5运维方式：支持ssh、telnet、rlogin、rdp、vnc协议的H5运维，无需本地运维客户端工具 |
| 会话协同功能支持在运维界面实时查看协同人员，可由会话发起人在线进行操控权分配，可实时踢出会话协同人员；会话协同人员可主动申请当前会话操控权，待会话发起者同意后可拥有会话操作权 |
| H5运维方式下，可支持RDP/SSH在线文件传输，无需借助第三方客户端工具，通过web页面即可 |
| 连通性检测 | 支持对主机连通性、账号有效性进行周期性检测。并可设置是否开启检测连通性、有效性功能 |
| 客户端工具登录 | 客户端访问方式：支持使用本地的mstsc/Xshell/SecureCRT/Putty/winscp/Xftp等客户端工具登录堡垒机访问图形、字符或SFTP、FTP设备 |
| SSH网关代理直连 | 支持使用本地的SecurCRT/Xshell/OpenSSH工具通过SSH网关代理方式直接登录字符设备 |
| SSH-agent-forwarding | 可以使用SSH-agent-forwarding登录到ssh服务器，用于登录堡垒机和登录ssh主机使用相同私钥的场景 |
| SSH登录方式 | 可以使用密码或公钥的方式登录到SSH资产，并且可以发送运维用户信息、运维来源IP等环境变量到资产上。 |
| 批量自动登录字符主机 | 支持批量登录字符设备功能：能自动生成SecurCRT/Xshell工具的批量登录文件，实现在工具中批量自动登录多台设备 |
| 批量登录 | 可一键批量登录不同协议的主机资产，并且可选择不同资产的登录方式，如所有资产均采用H5运维，或A资产采用H5运维，B资产采用调用本地工具运维 |
| 审计日志要求 | 运维审计日志 | 支持对运维操作会话的在线监控、实时阻断；支持录像回放、支持记录起止时间、来源用户、来源IP、目标设备、协议/应用类型、命令记录、操作内容（如对文件的上传、下载、删除、修改等操作等）的详细行为日志 |
| 禁审功能 | 支持提供禁止审计功能，可对部分设定策略的会话不审计录像，防止机密信息二次泄漏 |
| SQL记录 | 支持审计主流数据库（如DB2、oracle、mysql、sql server、PG、人大金仓、达梦）运维中的SQL语句，可进行关键信息定位查询，并可过滤数据库客户端自动发起的语句，方便查询真实人为的数据库操作 |
| 安全策略要求 | 运维规则策略 | 支持通过基于时间、IP/IP段、用户/用户组、主机组、主机账号、命令控制策略等组合访问控制策略，授权用户可访问的目标设备。 |
| 系统管理要求 | 系统自审 | 支持自身审计，包括但不限于：系统状态检测、登录日志、用户日志、资产日志、策略操作日志、审计日志、配置日志、维护日志、运维日志等 |
| 存储管理 | 支持NAS存储 |
| 安全接入 | 支持内置VPN模块，无需与其他VPN设备联动，实现运维入口安全接入 |
| 售后服务 | 提供7\*24小时原厂商400支持热线；提供不少于三年质保服务，包含但不限于硬件保修、系统升级等服务内容；本地需要至少5个（含）CISP-BDSA资质证书设备厂商人员提供支持。（须提供近三个月投标所在地社保证明） |
| 厂家资质 | 国家信息安全测评信息安全服务资质证书（安全工程类三级），提供证书复印件； |
| 知识产权管理体系认证证书，提供证书复印件。 |

##### 6、IPSec VPN（2台）

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| ★产品资质要求 | 具有商用密码产品认证证书  |
| 规格要求 | 标准1U设备，10个千兆电口，4个千兆光口，支持双机热备，冗余电源 |
| 性能要求 | 支持国密2/3/4算法，加密速率1.8Gbps，隧道数20000条/规则数20000条 |
| 功能要求 | 支持IPV4；支持路由模式、透明模式；采用国家密码管理局鉴定的硬件随机数发生器；内置ca，内置ca支持SM2，同时支持生成SM2证书请求；确保受到浙江省委网信办设备集中管理中心的集中管控；确保与中央网信办实现互联互通，密文传输； |

##### 7、网络准入管理系统（1台）

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 总体要求 | 国产品牌，产品必须为自主研发（非OEM），操作系统平台不能基于标准发行版本（Windows/Linux）。 |
| 须提供《涉密信息系统产品检测证书》、《计算机信息系统安全专用产品销售许可证》、《计算机软件著作权登记证书》、《质量管理体系认证证书》，并提供证书复印件。 |
| 所投产品须具有中国国家信息安全产品认证证书，并提供证书复印件。 |
| 规格要求 | 标准1U机架式设备CPU不低于双核1.8GHz、内存不低于2G、硬盘不低于500G、至少2个千兆电口；授权许可数≥500点； |
| 部署要求 | 支持纯旁路部署，不能以任意串联方式（包括策略路由等逻辑串联）部署。 |
| 支持分级部署，可以通过部署探针的方式纵向扩展链路层准入技术，集中在上级管理，配置自动下发到探针，无需登录探针维护。 |
| 支持分布式部署，可以通过横向和纵向部署多台服务器来扩展管理范围和增加管理能力，纵向支持无限分级，支持集中大屏查看部署图，支持全局根据IP/MAC/责任人等定位终端设备。 |
| 支持高可用性双机部署，主机故障后备机无降级容灾接管，防止准入系统故障终端不能正常入网，主备切换时间不能大于10秒。 |
| 支持为关键服务提供容灾工具，DHCP容灾工具可在服务器宕机后自动接管IP地址分配工作，容灾工具分配IP时仍要保持IP/MAC绑定关系。 |
| 准入技术 | 支持多种准入控制技术（包括802.1X、MAC认证、DHCP、ARP、SNMP、数据镜像等），一套系统需支持多种准入技术并行启用。 |
| 支持自定义不同安全级别的接入事件选用不同的阻断技术进行隔离，例如未授权接入设备，应达到边界级阻断，授权未符合安全要求的，基于应用级阻断控制，可灵活定义。 |
| 支持基于终端的部门/终端类型/操作系统/标签和接入VLAN配置不同的准入策略，管理员可查看符合每条准入策略的终端。 |
| 支持对非法和违规终端的多层阻断，可同时支持应用级、交换机端口级、网络边界级（同HUB之间互访阻断）的阻断效果。（须提供相关截图证明及准入技术原理说明） |
| 支持在达到边界级阻断效果情况下，对终端的Web Portal引导入网功能，即终端通过浏览器访问同HUB其它终端也能弹出引导页面。 |
| 终端发现 | 支持管理员自定义终端类型和终端类型组，可自定义终端类型显示的图标。 |
| 支持自动发现在网终端的MAC地址、IP地址、网卡厂商、TCP服务端口、接入VLAN、接入交换机端口等信息。 |
| 支持自动识别终端类型，如办公机、交换机、路由器、打印机等，生成终端类型统计报表。 |
| 支持管理员自定义类型识别库规则，可基于网卡厂商、主机名、IP地址、TCP服务、操作系统等多维度组合定义识别规则，支持查看每条规则识别的终端信息。 |
| 支持当终端信息发生变化、类型识别库规则发生变化后，自动秒级重新识别终端类型。 |
| 终端注册 | 支持新终端入网注册策略，此策略可基于子网配置是否开启。支持采用浏览器Portal页面方式进行终端注册。 |
| 支持管理员自定义注册内容，包括注册项、前后顺序、标题、提示语句、是否必填等，对于关键注册项，如用户名、部门等支持选择模式和输入模式切换，以上配置需支持基于子网区分配置。 |
| 支持注册码管理，可自定义注册码有效期、使用次数、限制注册的终端和IP等，并可定义注册码关联的注册部门，采用注册码注册可自动划分部门。 |
| 注册申请支持人工审核、无验证自动审核、账号密码认证自动审核、手机验证码自动审核、审核码自动审核等多种审核方式，管理员可基于子网定义不同审核方式。 |
| 支持注册申请的多级审核功能，管理员可自定义审核流程，中间审核人员可同意和拒绝申请。 |
| 支持基于注册账号自动划分终端隶属部门，支持自动绑定终端和注册人。 |
| 支持限制每个用户注册的终端数目，并可基于标签区分不同用户可注册终端的数目。 |
| 支持开启用户注销功能，可定义是否允许用户自行注销终端注册信息。 |
| 支持自定义重装操作系统、重装客户端是否重新进行终端注册。 |
| 支持基于部门配置不同注册有效期，当注册过期后需重新注册。 |
| 支持离线重新注册功能，可基于部门、设备类型定义不同离线重新注册的时间策略。 |
| 用户认证 | 支持用户账号认证入网策略，并可配置终端与用户账号的双向绑定关系，禁止不符合绑定关系终端入网。 |
| 支持与外部用户认证平台如AD/LDAP联动进行认证，须采用LDAPS认证方式，可手动/自动同步AD上的部门架构和用户账号到本地。 |
| 支持访客管理，访客入网支持验证码和二维码扫描方式，支持全局二维码和员工授权二维码的方式入网，并可追溯访客与被访问员工记录。 |
| 支持对外提供标准的RADIUS认证接口，可为其它业务系统提供统一认证平台功能。 |
| 网络策略 | 支持动态VLAN下发，并支持与系统内置的DHCP服务相结合，构建终端漫游，实现动态VLAN下发、动态IP地址下发静态化管理、漫游接入管控等效果。 |
| 支持多网卡终端管理，管理员可人工合并/拆分多网卡终端，系统也可自动合并多网卡终端。 |
| 支持定义IP/MAC绑定策略，支持在不同VLAN绑定不同IP地址，并可限定终端能够接入的VLAN，支持基于终端分组限制终端入网是否必须绑定IP/MAC地址。 |
| 支持IP冲突发现功能，能够定位冲突IP的MAC地址，能够对绑定的IP/MAC进行保护，对违规使用绑定IP的终端进行阻断。 |
| 支持定义MAC/PORT绑定策略，支持限定终端可接入的交换机和交换机端口，也可限定交换机端口只允许绑定终端接入。 |
| 支持在不安装客户端或插件的情况下，进行MAC地址仿冒（MAC克隆）检查，支持IP地址、MAC地址、TCP监听端口、交换机接入端口同时仿冒情况下违规行为的发现和阻断。（须提供相关截图证明及仿冒鉴别技术原理说明） |
| 支持在不安装客户端或插件的情况下，利用TCP监听端口检测应用软件合规性功能，可灵活的基于部门、操作系统、标签、设备类型定义不同的TCP合规策略，对不合规的终端进行阻断并能够通过Portal页面引导软件下载。 |
| 支持入网时间策略，管理员可基于不同终端分组定义不同的入网时间限制，至少可基于星期和小时两个维度定义策略。 |
| 支持入网后授权访问策略控制，可基于部门、设备类型、操作系统、标签等多维度组合定义设备入网后权限，并可记录越权访问日志。 |
| 支持在准入服务器和探针上虚拟蜜罐服务进行可疑行为监测，记录异常访问日志，管理员可自定义整体访问频率、单个服务访问频率、服务数访问频率等阈值进行告警和阻断。 |
| 主机策略 | 客户端应兼容WindowsXP、Windows7、Windows8、Windows10等32/64位操作系统，且支持基于Linux的国产化操作系统。 |
| 客户端界面支持管理员自定义功能，包括托盘是否隐藏、客户端界面菜单、界面Logo、显示内容等。 |
| 支持管理员基于终端分组自定义允许卸载的策略，支持在线审批卸载请求，离线请求码/卸载码卸载、离线超级卸载码等不同方式卸载，管理员可自定义超级卸载码。 |
| 支持管理员自定义安全域功能，客户端和服务器双向认证，管理员可自定义那些安全域内的客户端可接入本服务器，也可限制安装了本服务器客户端的机器接入其它服务器安全域列表。 |
| 支持客户端版本分区分域管理，不同区域采用不同客户端版本，管理员可自定义版本和区域的对应关系，可强制某区域内客户端升级到制定版本。 |
| 支持对主机进行CPU/内存/硬盘变动检查、网卡类型检查、操作系统版本检查、软件/进程/服务/文件/注册表/监听端口检查、杀毒软件、系统安全策略检查。 |
| 支持对U盘管理，能够对私接U盘告警及断网处置，或能够禁止U盘使用。 |
| 支持检查终端是否登录域，检查登录域名合法性，可检测登录同样域名的仿冒域功能，支持禁止启用本地系统用户功能。 |
| 支持入网合规性检测，并支持入网后对主机合规性进行在线实时检查，管理员能够自定义在线检查的周期。 |
| 支持对检查项进行自动修复功能，管理员可将修复软件上传到服务器，客户端自动修复入网。 |
| 支持离线断网功能，当终端离开网络的时候自动屏蔽网络通信，防止其接入互联网等，并支持离线断网的IP地址白名单。 |
| 支持管理员自定义是否禁止重新安装客户端，是否禁止重装操作系统的策略。 |
| 支持自动搜集终端硬件和软件资产，并生成统计报表，可记录每台终端软硬件资产变动日志。 |
| 网络边界 | 能够发现内网私接的HUB、不可网管交换机等，能够及时产生告警并阻断接入设备入网。 |
| 支持自动发现网中网行为，如小路由、随身WiFi、免费WIFI、代理上网等行为。 |
| 支持自动发现违规外联行为，定位设备的IP/MAC/责任人/部门等，在内网和互联网都支持对违规行为的取证。 |
| 支持对两个物理上（或者逻辑上）隔离的两个网络互联（误联）行为进行智能发现并告警，支持自动定位互联位置并自动断开 |
| 支持关闭长时间未接入终端的交换机端口，管理员可自定义时间限制，并支持定义交换机口只允许绑定的终端才能接入。 |
| 终端维护 | 支持终端的增删改查功能，支持终端属性的自定义无限添加，并可定义属性是否下拉框选择模式。 |
| 支持管理员自定义功能，可自定义显示内容、前后顺序、分页格式，支持排序、模糊/精确搜索功能，支持跨页批处理功能，下拉框项目过多支持输入动态过滤功能。 |
| 支持自动清理长时间不在线终端功能，管理员可基于部门、终端类型、注册状态等定义不同的离线时长。 |
| 支持自动绑定功能，可自动绑定IP/MAC、MAC/PORT、责任人/使用人、自动划分隶属部门等。 |
| 支持终端资产状态管理功能，管理员自定义终端不在线时长，系统基于条件自动切换终端资产状态，管理员可自定义资产状态的入网策略。 |
| 支持用户登录自服务系统维护责任终端，管理员可定义自服务页面的内容和格式，可限定能够修改的终端属性。 |
| 网络设备管理 | 支持自动生成网络拓扑，支持区分编辑模式和查看模式，可手动修改连接关系。支持分组框选拖动，以及上下左右/水平/垂直对齐功能，支持保存和恢复拓扑图快照功能。 |
| 支持在拓扑图上显示非法终端告警，支持在拓扑图上搜索、定位终端功能。 |
| 支持自动生成交换机面板图，可基于端口开关状态/连接状态/接入终端数目/告警终端等区分展示，可直接在面板图上对端口进行开关操作。 |
| 支持将IP/MAC绑定和MAC/PORT绑定策略同步到交换机配置上。 |
| 支持批量修改交换机密码功能，支持批量下发自定义命令到交换机。 |
| 支持自动备份交换机配置，图形化高亮提示配置变动，管理员可选中某一个备份配置进行自动恢复到交换机。 |
| IP地址管理 | 支持DHCP集中管理IP地址，支持IP地址的固定下发、在线监控、定期回收、历史审计等全生命周期的IP地址管理。 |
| 支持Trunk管理多VLAN的IP分配功能，无需配置交换机DHCP RELAY即可实现为所有VLAN分配固定IP地址。 |
| 支持自定义DHCP option功能，以兼容未来不同网络环境。能够基于部门、标签、终端类型、操作系统下发固定的IP地址段。 |
| 支持IP地址网格视图管理，能够通过图示直观的查看各网段中在线、离线、从未使用的状态，能够通过颜色区分保留IP地址、可用IP地址、绑定IP、告警IP等。 |
| 入网报告 | 支持记录终端每次上线/下线时间，记录总在线时长等，并提供在线率统计报告，为提高统计精确度，管理员可定义在线统计的有效时间段、是否排除周末、节假日等。 |
| 支持记录终端所有网络接入日志，包括上线、下线、IP变更、IP冲突、接入端口变更、主机检查结果、用户认证、新终端入网、违反入网策略、被阻断、解除阻断等。 |
| 支持管理员自定义每个入网事件的处理动作，如是否记录、是否告警、是否需要管理员人工确认、是否需要发送SYSLOG/邮件/短信等，并可基于终端部门、类型、操作系统、标签等条件设置。 |
| 告警事件支持自定义告警级别，并可基于不同级别自定义不同颜色、字体大小、粗体等。 |
| 入网报告支持模糊和精确搜索功能，在200万日志情况下精确搜索速度不能超过1秒。对于大量日志支持分表存储，可以对历史日志表进行查询、导出、统计等操作。 |
| 系统管理 | 支持管理员分权，至少可划分系统管理员、安全管理员和安全审计员三类，每一类管理员都可创建多个，可限定管理员管理的部门，其只能看到和管理制定部门的终端。 |
| 支持管理员角色管理，通过角色细粒度控制管理员的管理权限，包括定义终端、用户账号、策略等管理对象的读取和修改权限。 |
| 支持代办事件的页面提醒功能，包括新终端注册、客户端卸载、待处理的入网事件、待处理的终端告警等。 |
| 支持管理菜单的自定义功能，首页Dashboard支持显示内容和顺序的自定义，用户侧所有Portal页面中的文字、图片、按钮、背景等需支持自定义。 |
| 支持强制入网终端收看培训视频的功能，支持页面、代理客户端播放视频，可基于部门和时间来设置播放策略，不同部门不同时间来播放不同的培训视频。 |
| 支持备份恢复功能，支持自动备份配置到外部存储的功能，并支持管理员自定义自动备份周期。 |
| 支持审计报告记录管理员操作日志，可细粒度追溯管理员对系统的配置、对终端设备属性的修改等。并支持将审计报告通过SYSLOG形式发送给其它系统。 |
| 支持提供SNMP接口给其它系统获取自身运行状态，如CPU占用率/内存占用率/磁盘占用率等。 |
| 支持提供RESTful接口给其它系统获取终端设备信息以及统计信息，包括终端IP地址、MAC地址、责任人、在线状态、告警状态、隶属部门等信息。 |
| 支持提供数据库视图接口给其它系统获取终端设备信息，包括终端IP地址、MAC地址、责任人、在线状态、告警状态、隶属部门等信息。 |

##### 8、网络安全运营保障平台（零信任体系）（信创版）（1套）

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 可信环境感知模块 | 基础安全感知：感知发现终端是否存在病毒、感知终端病毒库是否及时更新；系统安全感知：对终端登录失败的限制，终端账户密码维护，远程登录的安全性感知应用合规感知：感知终端是否安装违规的软件，运行违规的进程、启动违规服务、开启高危端口。 |
| 可信API代理模块 | API发布管理：根据API业务的重要程度形成可信分并进行授权；API服务安全防护：使用黑白名单机制来控制API调用者的访问权限。 |
| 可信访问控制台模块 | 动态认证及管理：当终端设备信任分不能达到设定的要求时，不能进行登录访问；动态授权：基于一定时间内，根据同一用户登录设备次数进行动态授权，动作为可拒绝访问、可二次认证、可放行；风险动态控制：基于用户终端环境感知内容进行分析，形成终端配置风险策略实现动态控制阻断，并能对终端配置风险事件次数进行设置。 |
| 可信应用代理模块 | 应用安全加固：对用户发起的应用请求的字段的合法性检测；应用级动态访问控制：在接收到主体可信环境安全状态变更通报时，根据可信访问控制台策略进行策略执行；能够执行基于访问的IP提供应用系统的访问控制策略；能够执行设备认证异常情况下二次认证访问控制策略 |

##### 9、数据安全分级与风险评估系统（1套）

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 产品资质要求 | 产品取得软件著作权登记证书，提供证书复印件 |
| 产品获得公安部计算机信息系统安全产品销售许可证，提供证书复印件 |
| 规格要求 | 纯软件形态部署模式 |
| 数据源资源管理 | 支持数据库类型包括但不限于MySQL、Oracle、PostgreSQL、Hive、SQLServer、IPMALA、MongoDB、ElasticSearch、ClickHouse、Greenplum、INFORMIX、SYBASE、DM7、ODPS、DB2、GBASE8A（南大通用）、KINGBASE8(人大金仓)、POLARDB、Teradata、VERTICA、CacheDB等数据库。支持通过FTP/SFTP/LOCAL文件协议对csv、txt等文件进行分类分级。 |
| 支持创建数据源时，将数据源绑定对应的部门、责任人。每个数据源都可以使用不同的行业模板，达到不同行业模板的多数据源并行执行分类分级任务。 |
| 支持手动添加数据源，编辑数据源名称、数据源类型、主机及端口、库名/实例名、版本号、账号、密码等信息，也可以批量导入数据库，进行数据资产管理。支持通过指定的IP段、端口段，定时扫描发现当前环境下的数据库资产。 |
| 支持数据源展示功能，至少包括但不限于数据源名称、数据源类型、主机及端口、创建用户、创建时间等数据源基本信息，也支持展示具体每个数据源的库、表、字段信息。 |
| 分类分级管理 | 应支持分类分级任务管理，包括对任务的启动、终止，并展示任务的执行进度情况。支持任务的定时启动，自动发现敏感数据的动态变化。 |
| 内置不少于70种常见敏感字段识别规则，且支持自定义创建识别规则。自定义规则包括但不限于正则、字典等。具备结合算法识别能力以保障敏感数据识别精准度，至少包括但不限于正则+luhn、NER算法等 |
| 支持分类模板的管理，支持自定义模板导入。且内置不少于15种行业法规标准模板，包括但不限于网络安全法、金融、证券、电信、GDPR、CCPA、等保、电信-专项、网约车、工业互联网、公安、通用、疫情数据安全法和个人信息安全规范等，同时应支持对内置模板进行下载或克隆  |
| 支持通过对发现字段的敏感级别进行逻辑计算，通过多种策略实现对表的分类分级。表分类策略支持分类合集（使用去重后所有已识别数据字段的类别集合，作为表分类）和就多原则（使用数据字段所属最多的分类，作为表分类）两种维度定义表类别。（提供软件界面截图）表分级策略可以在就高原则(使用表中所有字段的最高数据级别，作为表级别)和加权平均(根据表中各数据级别出现的比例进行加权计算)两种模式切换。 |
| 应具备自动推荐引擎，当同一列中识别出多种字段信息时，需提供该列数据的规则命中列表，并给出精确的较高的推荐结果，便于用户根手工修改确认梳理，实现迅速、高效的手动确认。 |
| 支持通过对字段内容、字段名称和字段注释进行模糊匹配，并可通过调整权重配比，提高数据自动分类分级准确性。 |
| 支持对相似表、相似字段进行聚合并在页面中统一展示，以便于人工二次确认或修改分类分级结果 |
| 数据库安全评估 | 提供数据库脆弱性检查功能，脆弱性检查至少包括数据库漏洞检查、配置项检查、弱口令检查等手段实现安全评估，并提供图表分析结果和数据源安全排名，实现对数据库状况的安全监控和评估。 |
| 支持账号权限发现功能，至少包括但不限于数据库账号、数据源名称、拥有权限、禁止权限、状态和密码有效期等信息，同时支持检测账号动态变化和权限变更。 |
| 内置不少于2600种数据库漏洞库，提供风险检测的数据库漏洞检测，至少包括但不限于漏洞名称、CVE编号、漏洞等级、漏洞描述、解决建议、数据库类型、数据库版本、操作等信息。（须提供相关截图证明） |
| 售后服务 | 提供7\*24小时原厂商400支持热线；提供不少于三年质保服务，包含但不限于系统升级等服务内容；  |
| 厂家资质 | 国家信息安全测评信息安全服务资质证书（安全工程类三级），提供证书复印件； |
| 知识产权管理体系认证证书，提供证书复印件； |

##### 10、数据脱敏系统（1套）

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 产品资质要求 | 产品取得软件著作权登记证书，提供证书复印件 |
| 产品获得公安部计算机信息系统安全产品销售许可证，提供证书复印件 |
| 规格要求 | 纯软件形态部署模式 |
| 性能要求 | 单表单任务执行脱敏性能20MB/s |
| 敏感数据发现 | 支持数据源管理功能，主流数据源类型包括但不限于MySQL、Oracle、Db2、MSSQL、PostgreSQL、Greenplum、SybaseASE、Informix、Hive、ODPS、MariaDB、Clickhouse、Elasticsearch、MongoDB、MariaDB、达梦、GBase8A、Kingbase，同时支持新增本地文件【xls、xlsx、csv、txt】、SFTP\FTP数据源的添加。 |
| 应支持自动数据识别发现敏感项，包括敏感表和敏感列以及敏感项的动态变化 |
| 需提供数据目录，可以查看数据的分布情况，包含表级别分布和列级别分布；同时提供包括数据库梳理、敏感表数量、识别字段数、敏感列数和已经梳理占比情况等信息 |
| 支持数据分级分类任务任务的管理功能，包括但不限于务名称、数据源名称、主机、发现结果、状态、次数、周期、创建时间、最新发现时间、操作。提供查看任务详情，可以查看以图表形式展示当前数据源分类分级的概况。 |
| 敏感数据脱敏 | 支持自定义脱敏算法模板库，用户可将若干脱算法略组合成为适用于该场景的脱敏算法模板库，脱敏模板库定后，可被重复利用。 |
| 应支持脱敏任务的配置功能，提供数据库到数据库、数据库到文件、文件到数据库、文件到文件流程的脱敏任务新增功能，支持数据处理配置和脱敏算法的配置。 |
| 应支持脱敏任务的展示功能，包括但不限于任务名称、脱敏流程、任务状态、执行次数、执行周期、新增时间、最近执行时间、执行耗时和操作等信息，同时支持任务的编辑、查询功能。 |
| 开启脱敏任务审批后，用户提交脱敏任务审批后，权限管理员可以进入该界面进行脱敏任务的审批，审批通过后方可执行脱敏任务。 |
| 应支持水印配置功能，水印配置界面可直观展现水印的使用状态，支持在水印中自动附加时间信息，提供方便便于维护管理水印。 |
| 脱敏算法 | 静态脱敏支持不低于20类，240种及以上的脱敏算法（须提供相关截图证明） |
| 数据溯源 | 可通过数据上传和数据输入两种方式溯源，定位水印处理后数据的单位信息（即对应的水印名称）（须提供相关截图证明） |
| API接口开放 | 支持任务创建、数据脱敏、数据水印等脱敏能力以API方式提供，方便与第三方应用或平台进行整合对接，提升产品适用场景。 |
| 脱敏报表 | 支持指定时间段内的脱敏任务统计报表，包括并不限于脱敏任务名称、脱敏执行时间、数据库类型、任务概况、脱敏算法分布情况、脱敏数据量占比情况，同时可配置对比时间周期，从而获取脱敏的变化情况 |
| 产品联动 | 支持与分类分级平台对接，用户可对统一类不同级别的数据灵活配置脱敏算法 |
| 系统管理 | 支持用户管理功能。 |
| 提供管理用户登录相关的安全配置。 |
| 支持配置外部日志的存储以及脱敏任务是否需要审批的开关。（须提供相关截图证明） |
| 提供所有用户的相关操作日志的展示。 |
| 售后服务 | 提供7\*24小时原厂商400支持热线；提供不少于三年质保服务，包含但不限于系统升级等服务内容； 本地需要至少5个（含）CISP-BDSA资质证书设备厂商人员提供支持。（须提供近三个月投标所在地社保证明） |
| 厂家资质 | 国家信息安全测评信息安全服务资质证书（安全工程类三级），提供证书复印件； |
| 知识产权管理体系认证证书，提供证书复印件； |

#### 2）互联网区

##### 1、终端安全与管理系统（1套）

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 产品资质要求 | 产品通过IPv6论坛IPv6 Ready Logo委员会认证并获得认证证书，提供证书复印件。 |
| 通过公安部检测获得网络版防病毒产品（一级品）销售许可证书，提供证书复印件。 |
| 规格要求 | 支持100套服务器防护，50套终端防护。 |
| 基本功能 | 全网风险可视 | 支持当前待处理高危风险展示，包括弱口令、待处理病毒、待处理漏洞数据，并支持一键跳转到对应处理页面 |
| 一体化安全策略 | 只支持自定义安全策略、安全策略可继承，内置多个初始策略模板，包括防护模板、审计模板 |
| 系统性能监控 | 支持对CPU、内存、磁盘读写、网络上下行流量达到配置阈值时告警。支持对CPU、内存达到一定阈值时客户端进行熔断。 |
| 资产指纹 | 支持自动收集终端资产信息，包括：计算机名称、内核版本、操作系统、处理器、主板、内存、硬盘、显卡、终端版本、病毒库版本、最近更新时间 |
| 高级威胁防护模块 | 支持对本机的扩展行为（信息收集、权限提升）进行监测，防止提权行为和信息泄露。 |
| 识别渗透过程中的隧道代理（端口映射、端口转发、内网代理），可阻断隧道代理搭建行为。 |
| 系统安全性模块 | 违规外联支持黑、白名单双模式，白名单模式可配置是否允许访问特定的网站和地址；黑名单模式可自定义恶意IP，支持黑名单告警和阻断。 |
| 移动存储介质管理：1.支持管理员对入网的移动存储介质进行注册，可以对已注册的移动介质进行管理，包括授权、启用、停用、删除、导出注册列表、行为监控及审计等。2.支持客户端自主申请移动存储介质注册，管理员统一对申请进行审批。3.支持管理员设置自动审批客户端注册请求。4.支持从资产维度、设备维度对存储介质的权限进行精细化设置，同一设备可针对不同的资产设置不同的读写权限，有效控制不明来历的移动存储可能带来的病毒传播等隐患。 |
| 防病毒模块 | 针对Windows系统，提供内核级的数据防护能力，保护文件不被恶意修改、加密等，可自定义配置保护的文件及目录，支持设置例外进程 |
| 告警功能 | 告警类型包括：护网高级威胁、系统防护、网络防护、Web应用防护。 |
| 告警内容至少包括：资产名称、IP地址、日志类型、风险概况、风险评级、事件发生时间等详细内容。告警方式包括：邮件告警、Syslog、短信告警及SNMP trap。 |
| 管理功能 | 集中管控 | 管理平台支持一键设置客户端卸载密码、一键卸载监控端、一键解除绑定、一键停止/恢复所有防护、一键关闭/重启主机、一键重启客户端、一键迁移资产。 |
| 用户管理 | 支持多级用户管理：租户管理员、租户。 |
| 可视化功能 | 能展示各个服务器或主机节点的信息，包括运行状态、活动规律、行为变化趋势和详细资料，以及历史行为数据查询、全局安全态势等。 |
| 安全服务 | 安全事件 | 支持监控用户和应用实时流速，包括用户名、应用名、用户组、上行速率、下行速率、总速率、会话数等信息，帮助管理员快速甄别网络异常行为；支持提供重大事件应急响应预案。 |
| 软件升级 | 提供3年的病毒库、程序升级服务。 |
| 应急响应 | 对于新发现的病毒、零日漏洞，厂商能够于24小时内作出响应，及时通知用户，并提供专门应急预案、处置工具或专杀工具。 |
| 技术支持 | 支持7\*24小时威胁溯源服务。 |
| 售后服务 | 提供7\*24小时原厂商400支持热线；提供不少于三年质保服务，包含但不限于系统升级等服务内容；本地需要至少5个（含）CISP-BDSA资质证书设备厂商人员提供支持。（须提供近三个月投标所在地社保证明） |
| 厂家资质 | 国家信息安全测评信息安全服务资质证书（安全工程类三级），提供证书复印件； |
| 知识产权管理体系认证证书，提供证书复印件； |

##### 2、日志汇聚系统（1套）

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 产品资质要求 | 产品获得公安部计算机信息系统安全产品销售许可证，提供证书复印件 |
| 产品取得软件著作权登记证书，提供给证书复印件 |
| 产品获得全球IPv6论坛IPv6 Ready Logo 委员会颁发的《IPv6 Ready Logo认证》证书，提供证书复印件 |
| 产品获得中国网络安全审查技术与认证中心颁发的《中国国家信息安全产品认证证书》，提供证书复印件  |
| 性能要求 | 支持审计≥100个日志源 |
| 部署方式 | 支持分布式部署，支持页面一键添加子节点，自动进行绑定添加，采集器可以选择同步日志范围，按需转发数据 |
| 功能扩展 | 采用解决方案包上传对产品进行功能扩展，无需要代码开发 |
| 支持kafka日志接收转发、大数据安全域同步、APT沙箱报告转发等大数据联调功能，Kafka收发支持SSL加密。 |
| 日志收集 | 支持Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP协议日志收集；支持阿里云SLS日志的采集。 |
| 可通过接收协议限制日志接收速率，包括Http接收、syslog接收、SNMPtrap接收、TCP接收、WMI接收、aliyun接收。 |
| 支持使用代理(Agent)方式提取日志并收集，安装包支持界面下载，且安装支持可视化向导。 |
| 日志分析 | 内置5000+解析规则，支持对收集的5000+设备类型日志进行解析（标准化、归一化），解析维度多达200+，解析规则可以根据客户要求定制扩展； |
| 三维关联分析；支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件。 |
| 日志备份 | 可设置日志存储备份策略。包括系统日志保存期（天）、磁盘使用率百分比等策略； |
| 支持日志本地备份及恢复； |
| 支持日志备份自动传送到远程服务器； |
| 支持从远程仓库恢复数据； |
| 支持FTP、SAMBA、NFS和FILE，4种方式的远程服务器 |
| 应用性能监控（APM） | 通过在目标主机上安装Agent程序，支持监测目标主机的CPU利用率、内存使用率、磁盘使用率、磁盘使用情况、流量等信息。 |
| 告警功能 | 支持磁盘空间阈值告警，当磁盘使用率达到设定的阈值时可产生并外发告警；资产性能监控异常告警，对于监控的资产系统资源进行监测当指定指标使用率达到设定的阈值时可产生并外发告警；资产状态监控，当资产处于不活跃状态时可产生并外发告警；远程仓库状态监测可告警，当远程仓库可用性检测失败或备份包自动上传失败时可产生并外发告警 |
| 用户管理 | 用户支持双因子认证登录，双因子认证令牌支持绑定至具体用户； |
| 提供一键式故障排除功能； |
| 提供自助式的升级接口，支持对产品升级、规则升级。 |
| 资产管理 | 注册用户资产时，提供自动发现识别能力； |
| 资产拓扑支持按照实际的用户环境进行编辑发布并可以和资产进行绑定，拓扑可以显示资产采集的事件数量被采集资产的状态等信息。（须提供权威机构第三方检测报告） |
| 售后服务 | 提供7\*24小时原厂商400支持热线；提供不少于三年质保服务，包含但不限于系统升级等服务内容，本地需要至少5个（含）CISP-BDSA资质证书设备厂商人员提供支持。（须提供近三个月投标所在地社保证明） |
| 厂家资质 | 国家信息安全测评信息安全服务资质证书（安全工程类三级），提供证书复印件； |
| 国家信息安全测评信息安全服务资质证书（风险评估二级），提供证书复印件； |

##### 3、网络安全运营保障平台（零信任体系）（信创版）（1套）

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 可信环境感知模块 | 基础安全感知：感知发现终端是否存在病毒、感知终端病毒库是否及时更新；系统安全感知：对终端登录失败的限制，终端账户密码维护，远程登录的安全性感知应用合规感知：感知终端是否安装违规的软件，运行违规的进程、启动违规服务、开启高危端口。 |
| 可信API代理模块 | API发布管理：根据API业务的重要程度形成可信分并进行授权；API服务安全防护：使用黑白名单机制来控制API调用者的访问权限。 |
| 可信访问控制台模块 | 动态认证及管理：当终端设备信任分不能达到设定的要求时，不能进行登录访问；动态授权：基于一定时间内，根据同一用户登录设备次数进行动态授权，动作为可拒绝访问、可二次认证、可放行；风险动态控制：基于用户终端环境感知内容进行分析，形成终端配置风险策略实现动态控制阻断，并能对终端配置风险事件次数进行设置。 |
| 可信应用代理模块 | 应用安全加固：对用户发起的应用请求的字段的合法性检测；应用级动态访问控制：在接收到主体可信环境安全状态变更通报时，根据可信访问控制台策略进行策略执行；能够执行基于访问的IP提供应用系统的访问控制策略；能够执行设备认证异常情况下二次认证访问控制策略 |

#### 3）政务外网区

##### 1、安全隔离网闸（2台）

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 产品资质要求 | 公安部计算机信息系统安全专用产品销售许可证（三级），提供证书复印件 |
| 国家保密局涉密信息系统产品检测证书，提供证书复印件 |
| 规格要求 | 支持千兆接口总数≥8个，支持USB口总数≥8个，支持串口总数≥2个， |
| 性能要求 | 网络带宽≥800Mbps并发用户数≥20000纳秒级开关延时 |
| 功能要求 | 提供统一接口，包括C或JAVA，为业务应用系统提供统一的安全跨域数据安全交换平台。提供和业务系统测试联调。由内网机、外网机两个主机系统和一个隔离交换网关组成。系统可以完成协议终止和内容检查。支持数据库、文件、流数据交换，支持内容过滤和数据格式检查。 |

##### 2、日志审计分析平台（1套）

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 产品资质要求 | 产品获得公安部计算机信息系统安全产品销售许可证，提供证书复印件 |
| 产品取得软件著作权登记证书，提供给证书复印件 |
| 产品获得全球IPv6论坛IPv6 Ready Logo 委员会颁发的《IPv6 Ready Logo认证》证书，提供证书复印件 |
| 产品获得中国网络安全审查技术与认证中心颁发的《中国国家信息安全产品认证证书》，提供证书复印件  |
| 性能要求 | 支持审计≥100个日志源 |
| 部署方式 | 支持分布式部署，支持页面一键添加子节点，自动进行绑定添加，采集器可以选择同步日志范围，按需转发数据 |
| 功能扩展 | 采用解决方案包上传对产品进行功能扩展，无需要代码开发 |
| 支持kafka日志接收转发、大数据安全域同步、APT沙箱报告转发等大数据联调功能，Kafka收发支持SSL加密。 |
| 日志收集 | 支持Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP协议日志收集；支持阿里云SLS日志的采集。 |
| 可通过接收协议限制日志接收速率，包括Http接收、syslog接收、SNMPtrap接收、TCP接收、WMI接收、aliyun接收。 |
| 支持使用代理(Agent)方式提取日志并收集，安装包支持界面下载，且安装支持可视化向导。 |
| 日志分析 | 内置5000+解析规则，支持对收集的5000+设备类型日志进行解析（标准化、归一化），解析维度多达200+，解析规则可以根据客户要求定制扩展； |
| 三维关联分析；支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件。 |
| 日志备份 | 可设置日志存储备份策略。包括系统日志保存期（天）、磁盘使用率百分比等策略； |
| 支持日志本地备份及恢复； |
| 支持日志备份自动传送到远程服务器； |
| 支持从远程仓库恢复数据； |
| 支持FTP、SAMBA、NFS和FILE，4种方式的远程服务器 |
| 应用性能监控（APM） | 通过在目标主机上安装Agent程序，支持监测目标主机的CPU利用率、内存使用率、磁盘使用率、磁盘使用情况、流量等信息。 |
| 告警功能 | 支持磁盘空间阈值告警，当磁盘使用率达到设定的阈值时可产生并外发告警；资产性能监控异常告警，对于监控的资产系统资源进行监测当指定指标使用率达到设定的阈值时可产生并外发告警；资产状态监控，当资产处于不活跃状态时可产生并外发告警；远程仓库状态监测可告警，当远程仓库可用性检测失败或备份包自动上传失败时可产生并外发告警 |
| 用户管理 | 用户支持双因子认证登录，双因子认证令牌支持绑定至具体用户； |
| 提供一键式故障排除功能； |
| 提供自助式的升级接口，支持对产品升级、规则升级。 |
| 资产管理 | 注册用户资产时，提供自动发现识别能力； |
| 资产拓扑支持按照实际的用户环境进行编辑发布并可以和资产进行绑定，拓扑可以显示资产采集的事件数量被采集资产的状态等信息。（须提供权威机构第三方检测报告） |
| 售后服务 | 提供7\*24小时原厂商400支持热线；提供不少于三年质保服务，包含但不限于系统升级等服务内容，本地需要至少5个（含）CISP-BDSA资质证书设备厂商人员提供支持。（须提供近三个月投标所在地社保证明） |
| 厂家资质 | 国家信息安全测评信息安全服务资质证书（安全工程类三级），提供证书复印件； |
| 国家信息安全测评信息安全服务资质证书（风险评估二级），提供证书复印件； |

##### 3、上网行为管理系统（1台）

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 规格要求 | 标准1U机柜型硬件平台，硬盘容量≥1TB SSD支持千兆接口总数≥6个支持万兆接口总数≥2个 |
| 性能要求 | 支持带宽≥750 Mbps最大并发连接数≥1,000,000每秒新建连接数≥20,000 |
| 部署模式 | 支持路由模式、透明（网桥）模式、混合模式、旁路模式；旁路部署支持直接加入2个以上物理接口，无需使用聚合接口；部署模式切换无需重启设备。 |
| 端口镜像 | 支持端口镜像功能，支持入流量、出流量和双向流量等维度镜像，支持将接口的流量镜像到另一个接口，方便网络问题定位。 |
| 接口 | 接口支持配置从属IP地址，每个接口支持至少200个从属IP。内外接口无固化，支持修改接口属性，修改接口IP类型、地址模式无需重启设备。 |
| 路由支持 | 支持基于入接口、源地址、目的地址、用户、服务、应用、时间、域名的策略路由。 |
| IPv6 | 支持IPv6/v4双栈，支持IPv6安全策略、包括审计策略、NAT策略、流量控制策略、会话控制策略、黑名单、白名单、认证策略等 |
| 接入认证 | 支持与浙政钉2.0平台同步组织架构，并能在用户管理界面呈现组织架构、登录用户、登录时间、在线时长等信息（提供功能截图证明） |
| 应用识别 | 应用特征不少于7000个，移动应用不少于2200个。支持自定义应用，包括但不限于数据包方向、协议、端口、IP地址、目标域名、关键字识别维度，数据包方向包括任意、请求数据、响应数据，关键字匹配模式支持文本或正则表达式；支持DNS域名学习模式，可引用数据包特征中的目标域名或指定域名。支持智能识别模式和快速识别模式。在智能识别模式下应用引擎尽可能地用各种方式识别网络流量；在快速识别模式下应用引擎将关闭部分智能分析功能以提高性能。 |
| 应用控制 | 可识别多种文件类型，包括电影、音频、文本、图片、压缩文件（zip、rar、gz、bz2、Z、tgz、tbz、7z、cab、bz等）、应用程序、Office系列等；并支持对应用的文件传输行为进行上传、下载、双向的文件类型过滤。支持基于协议、端口、策略的会话维持功能，老化时间不少于2000小时。 |
| URL识别与控制 | 支持基于DNS前置技术，实现在DNS解析阶段针对HTTP和HTTPS域名进行过滤，防止HTTPS域名过滤逃逸情况。 |
| 旁路阻断 | 支持在设备旁路部署时针对违规上网行为进行阻断过滤。 |
| SSL加密内容审计与控制 | 支持配置解密策略，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HTTPS域名库，预定义域名以及自定义域名；支持针对SSL解密证书进行自动推送。 |
| 流量管理 | 基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中（需提供配置界面截图证明） |
| 终端管理 | 支持对网络接入的终端进行可视化管理，展示终端详细信息、异常状态等，支持查看终端类型，以及终端详细信息（厂商，系统，端口等），支持查看终端类型分布（提供功能截图证明） |
| 防私接路由 | 针对私接网络行为，惩罚方式包括但不限于无操作、阻断和限速，阻断和限速支持自定义惩罚时长。 |
| 用户认证 | 支持IP准入、MAC准入、IP+MAC准入、本地认证、混合认证和免认证；支持用户MAC感知，当用户MAC地址变更后，要求重新认证，避免冒名认证现象；支持伪Portal抑制技术，支持通过HTTP302重定向或HTML-refresh方式抑制非正常的HTTP或HTTPS的页面请求，从而保障系统稳定高效运行；支持基于HTTPS协议推送认证页面。 |
| 非法外联管控 | 支持6种以上外联方式的检查，包含拨号行为、双网卡行为、有4G网卡、有无线网卡行为、连接非法wifi行为、连接外网行为等（提供功能截图证明） |
| 数据分析 | 支持监控用户和应用实时流速，包括用户名、应用名、用户组、上行速率、下行速率、总速率、会话数等信息，帮助管理员快速甄别网络异常行为；支持数据下钻跳转至详细列表，针对用户支持通过趋势图形式，按照时间顺序展示该用户网络会话和流量趋势，支持下钻跳转至详细列表访问的应用组成和流速情况。针对应用支持通过趋势图形式，按照时间顺序展示该应用会话和流量趋势，支持下钻跳转至详细列表使用该应用的用户、速率和会话数等情况。支持会话的统计与分析，支持统计会话源Top20、会话目的Top20，以趋势图方式展示并发会话、新建、TCP、UDP、其他协议等趋势信息；针对会话支持正向排名，支持数据下钻跳转至详细列表，深入钻取会话中用户、用户组、源目IP、源目端口、协议、连接类型、应用、流量、时间等信息；支持多条件组合形成筛选条件。 |
| 审计类法规 | 支持上网行为记录本地留存，方便事后行为回溯；支持将日志记录发送至第三方平台进行数据分析和呈现，发送数据支持蝶式交换加密算法 |
| 安全防护 | 支持本地安全防护，包括但不限于入侵防御、病毒防护、Web防护、威胁情报等，入侵防御规则不少于8600条，病毒防护规则不少于400万。 |
| 业务需要 | 针对内网用户的web访问质量进行检测，对整体网络提供清晰的整体网络质量评级，支持以列表形式展示访问质量差的用户名单，支持对单用户进行定向web访问质量检测（提供配置界面截图证明） |
| 管理员认证 | 支持管理员三权模式，默认包括权限管理员、账号管理员、审核员和管理员，各管理员权限制约；支持针对管理员分别设置精细化的读写权限和读写内容。 |
| 系统维护 | 支持SNMPv1、v2、v3版本，支持跨三层自学习MAC地址Web管理界面支持Ping、Traceroute、TCP Syn诊断工具，可支持基于接口、协议、IP地址、端口、应用进行网络抓包，并可下载导出分析 |

#### 4）网信数据中心

##### 1、云管理平台（112C）

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 资质要求 | 投标厂商的IaaS私有云服务通过由工信部中国电子技术标准化研究院发起的《信息技术 云计算参考架构》标准符合性评估，并提供相关证书复印件 |
| ★投标云管理平台需承建过符合国家网信办安全审查（评估）的案例，网信办官网可查 |
| ★兼容性 | 云管理平台可以兼容主流国产化X86、ARM服务器，提供海光、鲲鹏或同等主流名录厂商三个兼容性证书 |
| 云管理平台可以兼容主流国产化数据库，提供达梦、南大通用、人大金仓或同等主流名录厂商三个数据库兼容性证书 |
| 云管理平台可以兼容主流国产化中间件，提供金蝶、中创或同等主流名录厂商两个中间件兼容性证书 |
| 基本要求 | 云管理平台基于业界主流OpenStack Pike及以上版本开发 |
| 平台提供自动化安装部署能力，提供独立的安装部署界面，满足云管理平台的快速部署上线的要求。 |
| 云管理平台管理节点须支持Docker集群部署，并支持部署在虚拟机上，提供平滑升级扩展、高可靠容错机制，各云服务组件之间松耦合，支持不同的服务组件如IaaS、PaaS、大数据、数据库、安全等独立部署，支持不同的服务组件单独启用或停用，单云服务组件升级对其他云服务和云管理平台无影响。 |
| 云管理平台兼容主流x86虚拟化平台，支持KVM、VMware、Hyper-V、Xenserver等。 |
| 云管理平台兼容主流小型机虚拟化平台，支持PowerVM、HPVM等。 |
| 云管理平台支持业界主流的容器技术 Docker 及容器编排引擎 Kubernetes，支持Spring Cloud和Istio等主流微服务治理框架。云管理平台提供DevOps服务，实现代码托管、CI/CD、项目管理等功能，帮助用户完成软件研发流程的全生命周期管理。 |
| 云管理平台支持至少三家厂商的SDN控制器对接，能通过SDN控制器实现对物理网络设备的自动化配置，实现虚拟路由器、虚拟私有网络、弹性IP、虚拟防火墙、虚拟负载均衡等网络服务的增加、删除、修改和查询，以确保开放性。 |
| 云管理平台支持至少三家厂商的集中式存储设备为虚拟机提供块存储服务。 |
| 云管理平台提供用户自助服务界面，用户能够通过自助服务门户完成云资源申请、使用、修改、销毁等操作。服务门户能够为用户提供云主机、云硬盘、云防火墙、云负载均衡、容器、K8S集群、云数据库、大数据、微服务、DevOps等服务。为保证系统数据的安全性，云管理平台须与虚拟化平台、容器平台、数据平台统一品牌，软件本体均要求在本地机房部署。 |
| 平台功能 | 云管理平台支持多租户划分，为不同的租户分配资源配额，配额包括CPU、内存、云主机、路由器、VPN、网卡、防火墙、负载均衡、安全组、公网IP个数等，租户管理员可以根据租户内部架构，划分子租户 |
| 云管理平台可同时为租户分配多个不同品牌，不同性能的计算资源池和存储资源池 |
| 云管理平台支持角色功能和权限的自定义，云管理员能够根据需求定制角色分组，向特定用户开放相应功能界面 |
| 云管理平台支持自定义服务目录，可以控制云服务下各服务目录的启动和停止，停止服务目录后将不展示该服务；可以扩展目录，在系统中自定义添加新目录或更改当前目录的链接内容。 |
| 云资源的申请需要通过管理员审批方可使用，云管理平台最大支持九级审批流程，可以充分根据用户实际组织进行自定义，不同组织支持设置不同的审批流程，审批环节支持邮件通知相应责任人， |
| 支持云服务计费，云管理员可以对云资源和云服务进行计费策略设定，计费策略可以基于CPU、内存、硬盘、存储、网络带宽、主机、Power主机、云桌面、裸金属、防火墙等资源制定费率，支持按小时、天、月为周期进行计费，支持同时设置单项规格和组合规格的计费方式。 |
| 支持工单功能，用户通过工单可以向云管理员反馈云资源使用所遇到的问题，支持自定义工单的问题分类、问题处理责任人等配置。 |
| 支持资源租期功能，为云管理员提供统一管理租期选项的能力，用户在申请资源时只能选择指定的资源租期，管理员可以及时调整租期选项以满足云服务的运营需求。云管理平台可以指定资源到期策略（如自动关闭、自动销毁、邮件通知等），并在资源到期前提前给资源使用人发送到期提醒通知，使用人可以根据需要进行资源续期处理。 |
| 云管理平台支持多种用户认证方式。除支持本地密码认证外，还支持对接LDAP、Oauth 2.0等方式认证、支持设置CAS和OPENID两种协议的SSO单点登录；支持邮件验证码、短信验证码和图片验证码等双重认证，提高账户登录的安全性。 |
| 云管理平台支持设定用户账号的安全策略。管理员可进行账号锁定/解锁，设定账号密码策略，如密码长度、密码复杂度、密码有效期、连续登录失败锁定，同一账号的接入点限制与ACL等策略。 |
| 为了提高云平台数据库的安全性，云管理平台可以自定义允许访问系统数据库的白名单IP，只有添加进白名单的IP才能访问云管理平台的数据库。 |
| 云管理平台可以收集系统日志、操作日志、诊断日志并进行日志统计以及全文检索，记录平台的运行状态以及故障记录。当监控到异常数据时，系统会将日志自动同步到syslog日志服务器。 |
| 云管理平台支持为系统设置备份策略，支持手动或自动备份到本地或远端，并设置备份频率、备份时间和最大副本数。 |
| 支持用户使用图形化界面通过拖拽的方式编排自己的VDC，用户可以通过拖拽的方式指定云主机、云网络、云路由器、云负载均衡等云资源的逻辑连接关系，当部署成功后，生成的云主机、云网络、云路由器、云防火墙、云负载均衡等云设备之间的连接关系应与编排时保持一致。 |
| 云管理平台支持运营统计，提供资源统计、费用报表、资源报表等功能，支持将报表导出为execl或cvs格式到本地进行查看；支持首页直观展示CPU、内存、存储、裸金属、弹性IP等基础资源的资源总量、已分配和已使用情况，资源使用率TOP10的租户情况；报表类型应包含资源费用报表、组织费用报表、费用趋势报表、资源租期报表、计算/存储/网络等资源报表、VLAN报表、组织配额报表、IP报表、云主机报表等 |
| 系统支持一键巡检功能，可以检测当前系统节点状态、资源利用情况及告警信息等。 |
| 云管理平台支持大屏展示功能，展示云管平台IaaS层计算、网络、存储、组织用户等资源统计信息和资源分配情况、告警信息及PaaS层应用状态统计信息等内容，支持自定义大屏，可以根据需求调整大屏分辨率。 |
| IaaS-计算 | 用户可以通过自助服务门户批量申请云主机。申请云主机时可以定义所需操作系统、CPU核数、内存、硬盘、IP及安全组，可以为云主机选择自定义密码、随机生成密码或密钥对登录，并直接选择虚拟机所在资源区域、物理主机及设置虚拟机亲和性和反亲和性。 |
| 用户能够通过自助服务门户完成云主机的启动、关闭、重启、恢复、挂起、修改、快照、迁移、修改所有者、配置QoS策略等全生命周期操作，支持监控虚拟机的CPU、内存、磁盘IO和网络IO的使用情况。 |
| 支持用户重建云主机，用户可以通过公有镜像或私有镜像重新创建云主机。 |
| 云主机支持定时整机快照策略，支持带内存快照，云主机快照是某一时刻云主机状态的副本，可以保存云主机的设置和磁盘数据，支持内部快照和外部快照两种快照方式，内部快照存储在其磁盘文件中，外部快照通过创建增量磁盘存储增量数据。 |
| 支持用户采用密钥对方式登录云主机，保证用户登陆安全。 |
| 云主机支持标签管理，可以为云主机添加一个或多个标签，并通过标签筛选虚拟机，支持系统管理员、组织管理员、用户等不同的角色分别管理云主机标签。 |
| 支持云主机回收站，为了防止误删云主机，用户通过该功能可以将云主机移入回收站，而非直接销毁。在云主机回收保存期内用户可以从回收站中还原云主机，超过保存期后云主机将被自动销毁。 |
| 云管理平台支持对资源扩展和收缩策略的灵活配置，能够根据虚拟机CPU、内存、连接数等参数动态的增加虚拟机或删除虚拟机以满足“业务量大时使用多个虚拟机提供服务、业务量少时使用少量虚拟机提供服务”的业务需求，整个过程不需要人工干预。 |
| 云管理平台支持裸金属服务，用户可以申请裸金属服务器并安装操作系统，或纳管正在运行的裸金属服务器。支持对裸金属服务器进行启动、停止、销毁等生命周期操作。 |
| 云管理平台支持云桌面服务，支持桌面资源规格（CPU/GPU/内存）和桌面镜像（操作系统/应用软件）定义，提供虚拟桌面的申请、启动、关闭、重启、删除、配置管理等生命周期操作。 |
| 云桌面服务支持桌面池管理、终端管理、桌面资源概览等基础功能，并能够提供文件分发、软件分发、消息推送、盲水印解析、桌面云盘等能力，系统支持创建VDI、IDV、VOI三种不同类型的云桌面。 |
| 云管理平台支持备份服务，可以对云主机、云硬盘创建备份任务制定备份策略，进行定时定期备份，并可以根据备份数据恢复云主机或云硬盘，确保数据可靠性。 |
| 云管理平台支持灾备管理，系统管理员可以在主可用域和备可用域进行容灾配置，当主可用域主机池或生产机因意外（灾害、人为破坏等）停止工作时，由备可用域接替业务，保证业务不中断。主可用域云主机配置变化自动同步到备可用域，实现业务同步。支持计划恢复、故障恢复、反向恢复；计划恢复与故障恢复可将云主机复制到备可用域运行保持业务继续；主可用域恢复后，一键反向恢复，将业务恢复到主可用域。 |
| IaaS-存储 | 云管理平台支持根据计算或存储资源的硬件配置、虚拟化类型乃至地理位置等信息将计算或存储资源划分到不同的可用域中，从而保证不同的组织能以最优的方式使用计算或存储资源。 |
| 云管理平台管理虚拟化平台的存储资源时可以根据SSD/SAS/SATA、IOPS等参数配置不同的存储资源池（如高速、中速、低速等类型），用户申请存储资源时可根据需要选择对应的资源池，达到云存储规格分级管理与使用的需要，不同资源池提供独立的资源规格和计费策略。 |
| 云管理平台可支持云硬盘服务，支持新建、销毁、修改所有者、在线扩展硬盘容量、快照、备份、克隆等操作，支持云硬盘自动快照策略，同时支持云硬盘加密功能。 |
| 支持共享云硬盘，可以将同一个云硬盘同时挂载给多台虚拟机或裸金属服务器。 |
| 云管理平台支持为虚拟机（包括Vmware虚拟机）挂载厚置备与精简置备两种类型的云硬盘。 |
| 用户可以通过自助服务门户批量申请云硬盘。申请云硬盘时可以定义资源所属区域，类型，是否共享，硬盘容量，是否挂载到云主机等。 |
| 云管理平台支持对象存储服务，支持新建、修改、删除对象存储容器；支持已创建的容器中创建、删除文件夹；支持已创建容器中文件的上传、下载、复制、编辑和删除。 |
| 云管理平台支持文件存储服务，支持NFS协议和CIFS协议；支持共享文件的创建、修改、删除、权限设置以及自动挂载给虚拟机。 |
| 云管理平台可提供云网盘服务，租户管理员可以直接创建云网盘，普通用户可自助申请私有网盘空间。网盘所有者可对网盘的文件夹或者文件设置共享权限，从而共享给组织内的其他用户。云网盘可以通过手机APP进行远程访问。 |
| 技术支撑 | 配置专人（1人一年）提供云管理平台运营服务 |

##### 2、备份软件（1套）

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 品牌 | 与备份存储同品牌 |
| 软件授权 | 配置60TB后端存储容量授权，软件全功能开放 |
| ★平台兼容性 | 备份客户端支持部署在Windows、Linux、AIX、Solaris、HP-UX等操作系统，以及基于龙芯、飞腾、海光、兆芯、申威、华为鲲鹏处理器架构下的银河麒麟和统信UOS操作系统等国产操作系统。 |
| 支持磁盘块存储、蓝光光盘塔、磁带机、物理磁带库、虚拟磁带库、对象存储等作为备份数据的存储介质。 |
| 管理与运维 | 支持通过图形化向导管理界面按设定好的步骤完成备份管理服务端的账号生成、存储池创建、系统自备份的配置，客户端注册和客户端权限划分等功能的开通，减少服务端部署的初始化复杂度。 |
| WEB管理界面支持多种语言设置，包含简体中文、繁体中文、英文和西班牙文。 |
| 支持报表统计和报表导出功能：报表数据来源涵盖作业、作业数量、作业历史、备份成功率、警报、存储资源等。支持生成指定时间段的报表，报表中的字段支持重命名、删减和排序。报表导出格式必须包括XML、CSV、UOF，并且UOF能够打开并以表格（非XML格式）形式展现。（要求提供软件截图证明） |
| 支持使用Access Key的用户登录模式，有效解决用户应用系统密码定期自动变更和无密码场景下备份作业的按期执行。（要求提供软件截图证明） |
| 支持管理员自定义哪些类型的业务需要启用审批，业务类型包括：修改存储池、创建备份作业、创建恢复作业等。（要求提供软件截图证明） |
| 文件与操作系统保护服务 | 支持在线文件备份，包含：全量备份、增量备份与合成备份。支持对Windows、Linux、UNIX平台单文件/目录进行细颗粒度的合成备份和恢复。备份支持通过名称或通配符进行文件过滤，排除操作系统文件和一些指定扩展名的文件类型。支持全量备份、增量备份、合成备份生成的备份数据集通过挂载方式进行快速恢复。 |
| 支持多通道技术，且备份通道数设置范围为1～255，可根据客户端资源情况调整备份通道数量。（要求提供软件截图证明） |
| 支持文件、对象存储、Hadoop HDFS的在线备份和彼此之间的交互恢复，支持对象存储和Hadoop HDFS的备份数据恢复到异构的Linux文件系统。（要求提供软件截图证明） |
| 无需安装备份客户端软件，即可实现挂载快速恢复文件数据。（要求提供软件截图证明） |
| 支持在线备份Windows、Linux平台的操作系统及卷数据。支持Windows、Linux操作系统卷级和文件级的细粒度恢复。支持Windows操作系统在裸机恢复过程中提供驱动程序更换界面，允许客户针对不同的硬件驱动程序做恢复现场的替换。支持Linux操作系统备份和裸机恢复，支持原机恢复和异机恢复。 |
| 大数据平台保护服务 | 支持Hadoop分布式文件系统HDFS的文件备份，包含：完全备份、增量备份、合成备份。备份数据支持恢复到Linux、Unix文件系统和对象存储中，实现HDFS数据在异构文件系统中自动转换和有效恢复。支持Hadoop分布式文件系统HDFS的完全备份、增量备份、合成备份的备份数据，无需通过还原数据过程，直接通过挂载方式，实现数据的快速恢复。支持多通道技术，且备份通道数设置范围支持1～255，可根据客户端资源情况在线调整备份通道数量。（要求提供软件截图证明） |
| 支持MongoDB分布式文件存储数据库的逻辑备份、完全备份和日志备份，并支持恢复到任意时间点。支持MongoDB分布式文件存储数据库备份到本地存储，磁带库和对象存储，支持通过LAN-Free的方式备份到磁带库。 |
| 支持对Oracle、SQL Server、MySQL、DB2、PostgreSQL、Informix、Sybase、达梦、人大金仓、神舟通用等主流数据库的备份数据进行定时容灾演练，符合等级保护的要求以检验备份集的可用性。（要求提供软件截图证明） |
| 支持通过挂载方式实现Oracle、SQL Server、MySQL数据库的挂载恢复，挂载方式必须支持iSCSI、FC协议进行挂载。 |
| 支持Oracle日志解析，可以界面化展现Oracle事务中的SCN和具体事务操作，并选择准确的SCN号来确定数据恢复点。通过日志解析获取事务具体操作的SQL语句，实现在线创建事务日志撤销作业。（要求提供软件截图证明） |
| 支持SQL Server AlwaysOn Availability Groups的备份和恢复，自动化实现恢复时可用性组移出移入操作，简化操作流程，避免人为误操作。支持SQL Server的合成备份和挂载恢复，支持恢复到指定的LSN事务日志序列号。（要求提供软件截图证明） |
| 支持MySQL的物理合成备份、日志备份和挂载恢复，且备份过程不锁表，支持恢复到指定的GTID（Global Transaction Identifier）。支持MySQL采用持续日志备份方式，连续监控并复制变化的Binlog文件，实现对数据库变化数据达到秒级以内的备份保护。兼容MySQL复杂部署环境，包括MySQL的高可用架构MHA。（要求提供软件截图证明） |
| 虚拟化与云平台保护服务 | 支持VMware、Hyper-V、XenServer、Xen、KVM、FusionCompute、FusionCloud（Huawei Cloud Stack）、H3C CAS、OpenStack、CNware、RHV、易捷行云EasyStack、腾讯云Tstack、网安凌云、浪潮云等虚拟化平台或云平台的备份恢复 |
| 支持虚拟化平台的无代理备份，平台类型包括但不限于VMware、FusionCompute、FusionCloud、H3C CAS、CNware。以上虚拟化应用均无需在虚拟机内部安装任何代理软件或插件。 |
| 支持VMware的合成备份，通过挂载方式实现虚拟机的快速恢复。 |
| 支持以VMware vAPP分组来展现虚拟机，并以vAPP分组为对象创建备份作业，包括完全备份、差异备份、增量备份，从而达到对vAPP分组内所有虚拟机的备份要求。 |
| 结合vSphere Web Client Plugin，在VMware vCenter的管理界面上可以直接查看备份产品中虚拟机备份任务的状态，为用户提供更好的VMware虚拟化备份管理体验。（要求提供软件截图证明） |
| 支持虚拟化与云平台从整机备份数据中进行细粒度的文件级恢复，平台类型包括但不限于VMware、OpenStack等。支持虚拟化和云平台的虚拟机恢复后自动开、恢复网络标签（包含MAC地址），平台包括但不限于VMware、FusionCloud、FusionCompute。 |
| 同时支持华为FusionSphere基于Xen的版本和KVM的版本。 |
| 支持FusionCloud（或Huawei Cloud Stack）基于LAN-Base传输模式和LAN-Free的SAN传输模式。支持快照保留和清理的功能。支持FusionCloud部署在X86平台和华为鲲鹏ARM平台上的虚拟机备份与恢复。支持后端存储为Ocenstor或FusionStorage类型的FusionCloud备份和恢复，支持FusionCloud 6.1/6.3/6.5等版本。 |
| NAS备份保护服务 | 支持通过NDMP协议备份NAS设备，备份方式支持完全备份和增量备份。支持NDMP V3和V4协议，备份数据支持重复数据删除功能和NAS的备份数据存储到磁带设备中。 |
| LAN-Free功能要求 | 支持采用LAN-Free方式对文件、数据库、操作系统和虚拟化平台进行数据备份，节省网络流量开销。LAN-Free的网络协议必须能支持iSCSI和FC。 |
| 支持D2T和D2D2T两种模式。 |
| 支持通过LAN-Free的方式将数据备份到物理磁带，网络协议要求支持FC和iSCSI。 |
| 重复数据删除保护 | 支持固定块、变长块的数据重删技术，在创建重删存储空间时，需要提供变长和固定长度的块大小选择。（要求提供软件截图证明） |
| 支持源端重删和目标端重删技术。 |
| 支持将虚拟化应用的备份数据经重删后存入到对象存储。 |
| 远程复制保护 | 支持备份数据的远程复制，通过使用灾备端的备份数据恢复应用系统，以及本机或异机上的恢复。支持对远程复制设置带宽上限设定、数据传输加密、断线重连等规则。 |
| 支持对远程复制进行流量控制，合理控制带宽资源。支持对数据传输和存储进行加密，提升传输过程以及存储的安全性。具备断点续传特性，当远程复制过程中出现中断时，恢复正常后可基于上一次断点处进行续传。 |
| 支持本地数据远程复制到磁带库和云端对象存储进行保存。 |
| 支持将重复数据删除后的备份数据直接复制到容灾端存储。 |
| 系统安全保护 | 支持AES、Blowfish、SM4等加密算法。加密算法可选择CBC、CFB、ECB、OFB等加密模式，对于AES的密钥长度支持设置128、192、256等。（要求提供软件截图证明） |
| 针对系统的高危操作（如：恢复作业、清理备份集等）前要求输入四位或以上的随机数字验证码，待验证通过后才能执行操作，防止人为误操作危害数据。（要求提供软件截图证明） |
| 支持配置IP地址和MAC地址白名单、密码复杂度、密码加密传输、密码使用期限、历史密码重复限制、登录失败尝试次数、登录失败的锁定时间等功能。用户登录后提示上次登录的时间、IP地址、认证失败记录等信息。 |
| 用户登录系统除使用用户名和密码之外，还可以支持由系统触发生成六位或以上的字母加数字的随机认证码发送到对应用户账户的邮箱，从对应的邮件中获取随机认证码，正确输入到备份登录系统后进行二次身份验证，防止恶意破解密码。 |

##### 3、备份存储（1套）

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 品牌 | 国产知名品牌，非OEM产品，具备自主研发能力，提供分布式存储的软件著作权登记证书； |
| 节能认证 | 产品具有中国节能产品认证证书，提供证书复印件； |
| 抗震检测 | 产品通过第三方权威机构的抗震性能检测，满足9级烈度抗震要求，提供证书复印件作为证明； |
| 产品组成 | 提供软硬件一体机产品（或服务器与分布式软件统一品牌），不接受纯软件+第三方服务器投标；  |
| 部署方式 | Scale-out横向扩展的分布式架构，节点间完全对称，无独立的元数据物理服务器或索引服务器； |
| 数据服务 | 在一个集群内同时提供块存储、文件存储、对象以及HDFS存储服务，提供具备CNAS和CMA资质的第三方评测机构签字盖章的测试报告复印件，本次配置不限容量的块、文件、对象存储服务授权许可； |
| 节点数量 | 本次配置≥3个节点，支持节点在线平滑扩展，系统能够自动识别所加入的节点； |
| CPU | 每节点配置≥2个20核Intel Cascade lake处理器，主频≥2.1GHz； |
| 内存 | 每节点配置≥256GB缓存，每节点支持可扩展至≥1.5TB缓存（该内存须系统自带，不能以插PCI卡和闪存盘方式扩充，提供厂商官网截图和产品彩页作为证明）；支持配置英特尔®傲腾™数据中心级持久内存 |
| 硬盘 | 每节点配置≥2块480GB企业级SSD硬盘，每节点配置≥2块1TB企业级NVMe SSD硬盘，配置≥8块7200转8TB企业级SATA硬盘； |
| 接口 | 单节点配置≥4个10GE以太网接口和≥1个管理网口，前端业务网络与管理网络物理隔离； |
| 支持1Gb/10Gbps/25Gbps/40Gbps 以太网，支持100Gb InfiniBand网络； |
| 块访问方式 | 支持iSCSI连接，支持Windows、Linux、UNIX、Mac OS、Vmware ESXi等操作系统，支持KVM、vSphere、Xen、Hyper-V等虚拟化平台，提供厂商官网截图作为证明； |
| 兼容性 | 通过VMware兼容性认证，提供VMware的链接以及官网截图 |
| 卷配置 | 集群最大支持卷数量≥80000个，单卷最大支持容量≥64TB； |
| 精简配置 | 支持精简配置技术，应用实际写数据时才分配相应的物理存储空间； |
| 厚配置 | 支持厚配置，根据业务需求分配固定的物理存储空间，提供厂商官网截图和产品彩页作为证明； |
| NAS协议 | 兼容POSIX标准接口，支持NFS、CIFS、FTP共享，提供厂商官网截图和产品彩页作为证明； |
| 跨协议访问 | 兼容SMB1.0、SMB2.0、SMB2.1、SMB3.0、NFS3.0 、NFS4.0、NFS4.1、NFS4.2协议，支持CIFS/NFS跨协议访问； |
| 集群规模 | 单个文件规模支持≥64TB，系统最大支持文件数≥100亿个，单个目录最大支持文件数≥100万个，系统最大支持创建≥5000万个目录； |
| 配额管理 | 提供配额管理功能，包括目录配额、用户配额、容量配额、文件数配额、计算配额、强制配额等； |
| WORM技术 | 配置WORM技术，一次写入后禁止删除，有效保障数据安全性，支持手动或自动提交文件为保护状态，提供具备CNAS和CMA资质的第三方评测机构签字盖章的测试报告复印件； |
| 回收站 | 支持文件回收站功能，支持文件删除后自动保存一段时间，可以从回收站恢复文件，支持文件过期后自动删除，提供具备CNAS和CMA资质的第三方评测机构签字盖章的测试报告复印件； |
| 对象协议 | 兼容S3、Swift接口，支持通过http或CLI进行管理，提供厂商官网截图和产品彩页作为证明； |
| 对象管理 | 支持查询、创建、修改、删除、复制对象，支持分片上传和下载； |
| 权限配额 | 支持ACL权限控制和访问控制，支持精细化的Policy策略管理，支持用户和桶的配额管理； |
| WORM技术 | 配置WORM技术，一次写入后禁止删除，有效保障数据安全性，支持手动或自动提交文件为保护状态，提供具备CNAS和CMA资质的第三方评测机构签字盖章的测试报告复印件； |
| 对象加密 | 支持对象的加密，数据保护指在数据传输和处于静态期间保护数据，提供具备CNAS和CMA资质的第三方评测机构签字盖章的测试报告复印件； |
| 对象压缩 | 可对写入到对象存储中的数据进行压缩，可以达到减少对象存储空间的使用，提高对象存储空间利用率,提供具备CNAS和CMA资质的第三方评测机构签字盖章的测试报告复印件； |
| 对象追加修改 | 支持对已上传的对象进行追加修改，提供具备CNAS和CMA资质的第三方评测机构签字盖章的测试报告复印件； |
| 多租户 | 支持多租户功能，使用同一套系统为不同用户和应用提供存储服务，并确保这些数据之间相互隔离，提供具备CNAS和CMA资质的第三方评测机构签字盖章的测试报告复印件； |
| 生命周期管理 | 存储需要存储固定时间或固定容量的数据，超过指定时间或容量后，后面写入的数据会自动覆盖最老的数据,提供具备CNAS和CMA资质的第三方评测机构签字盖章的测试报告复印件； |
| 智能负载均衡 | 支持节点间智能负载均衡功能，支持轮询方式，支持按照CPU使用率、剩余内存容量、客户端连接数、网络吞吐量、综合负载等多种方式，实时选择最优的节点用于业务分担； |
| 多副本 | 支持多副本保护，支持2到6个副本，提供厂商官网截图和产品彩页作为证明； |
| 数据重构 | 每TB数据重构恢复时间≤15分钟，提供具备CNAS和CMA资质的第三方评测机构签字盖章的测试报告复印件； |
| 支持数据重构Qos，可设置不同档位的重构速率，调整故障重构的优先级； |
| 快照保护 | 支持快照数据保护，支持创建只读快照、可写快照、定时快照、一致性组快照，提供产品彩页和软件界面截图作为证明； |
| 支持手动或自动创建快照，支持快照过期后自动删除，单个卷最大支持≥2048个快照，支持快照回滚恢复，支持快照映射到业务主机进行读写； |
| 故障隔离 | 支持基于机架或节点的故障域设置，同一分条数据不能存储到同一个故障域中，支持创建节点级别的物理隔离保护域（节点池），单个数据只能存在于一个节点池内； |
| 节点扩展 | 单一系统支持≥2000个节点的横向扩展，提供厂商官网截图和产品彩页作为证明； |
| 容量扩展 | 单一命名空间存储容量可扩展至EB级，提供厂商官网截图和产品彩页作为证明； |
| 管理界面 | 提供功能全面的中文图形化管理软件，支持Web或其它图形化方式进行远程管理； |
| 管理HA | 支持管理节点HA高可用，管理平台部署于主备两个节点，主节点故障时，自动完成主备切换； |
| 系统监测 | 提供对存储系统各个参数的实时监测，管理界面内可查看各个存储池的信息，包括冗余策略、所属硬盘池、数据健康度和状态等，支持对硬盘容量、硬盘负载、内存占用、CPU占用的监控； |
| 智能预测 | 支持对硬盘故障检测，提前感知硬盘故障风险并预警；支持对存储容量增长趋势进行预测；支持对系统性能增长进行预测；上述功能提供具备CNAS和CMA资质的第三方评测机构签字盖章的测试报告复印件； |
| 性能监控 | 支持存储卷性能监控，包括IOPS、带宽、时延、平均I/O大小等，管理界面可查看每个集群、存储池的IOPS/带宽，支持保存≥7天的性能监控数据； |

##### 4、千兆汇聚交换机（7台）

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 能指标 | 交换容量≥750Gbps，包转发率≥220Mpps  |
| 接口要求 | 以太网支持千兆电口、千兆光口、万兆光口、万兆电口、25G、40G端口 |
| 扩展性 | 为满足未来扩展需求，扩展插槽≥1 |
| 可靠性 | 支持多虚一技术 |
| 支持BGP/IS-IS/OSPF/LDP/RIP/静态路由 |
| VXLAN | 支持VXLAN 二层交换，支持VXLAN 路由交换，支持VXLAN 网关 |
| IPv6 | 支持BGP4+、IS-ISv6协议支持IPv6策略路由支持DHCPv6功能、IPv6 portal功能、IPv6管理功能 |
| 配置要求 | 配置冗余电源，冗余风扇≥4个10G光端口，≥24个千兆光口（8combo端口） |

##### 5、千兆接入交换机（6台）

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 性能指标 | 交换容量≥430Gbps，包转发率≥80Mpps，提以较小值为准 |
| 可靠性 | 支持多虚一技术，最大堆叠台数≥9台  |
| 支持OSPF/RIP/静态路由 |
| 支持PVST功能：收敛时间≤50ms  |
| IPv6 | 支持IPv6静态路由、RIPng，支持IPv6 ACL； |
| 绿色节能 | 符合IEEE 802.3az（EEE）节能标准 |
| 成熟度 | 提供工信部入网证，且入网时间大于5年 |
| 配置要求 | ≥4个千兆光端口，≥48个千兆电口 |

##### 6、千兆路由器（2台）

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 包转发率 | ≥10Mpps  |
| 硬件要求 | 端口≥3GE Combo |
| 槽位≥8 |
| 冗余交流电源，可插拔模块化电源设计 |
| 虚拟化 | 支持虚拟化特性，将物理上两台设备虚拟化成一台逻辑设备  |
| 上网行为审计 | 支持记录终端用户访问互联网的日志，包括：用户名、源/目的IP地址、时间、访问的域名、URL等，权威第三方机构的测试报告 |
| 应用识别控制 | 支持对PC、移动终端常见互联网应用识别，并能够针对应用下发过滤和限速控制策略，权威第三方机构的测试报告 |
| URL过滤黑名单功能 | 支持对终端用户域名访问控制功能，权威第三方机构的测试报告 |
| 基于域的防火墙 | 支持划分安全域，用于管理防火墙设备上安全需求相同的多个接口，权威第三方机构的测试报告 |
| IPS入侵防御功能 | 支持对已知网络攻击进行安全防御，提高网络安全性，权威第三方机构的测试报告 |
| SSL VPN | 支持ssl vpn，并提供设备满足此功能的权威第三方机构的测试报告 |
| Segment Routing | Segment Routing，控制流量按照预先设置的网络节点逐跳转发，权威第三方机构的测试报告 |
| 广域网优化 | 支持对HTTP/FTP等TCP业务流量进行优化传输技术，提高广域网带宽利用率 |
| 资质证书 | 提供工信部入网许可证复印件  |
| 设备支持IPv6，提供IPv6 Ready Phase II证书 |
| 配置要求 | 配置冗余交流电源，≥3个GE combo接口，  |

##### 7、TAP交换机（2台）

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 国产化 | 采用国产化核心芯片 |
| 性能指标 | 交换容量≥4.8Tbps，包转发率≥2000Mpps，以较小值为准 |
| 关键部件热插拔 | 电源、风扇等关键部件可热插拔 |
| 路由协议 | 支持BFD/BGP/IS-IS/OSPF/RIP/静态路由 |
| IPv6 | 支持RIPng、BGP4+、IS-ISv6协议支持IPv6策略路支持DHCPv6功能、IPv6 portal功能、IPv6管理功能支持基于IPv6的VRRP功能 |
| TAP分流功能 | 流量的负载均衡 |
| N:M的流量镜像 |
| 识别报文头及更改报文信息 |
| 流量识别及处理，匹配ACL策略 |
| 剥离VLAN标记，解封装GRE/NVGRE/VXLAN隧道 |
| 资质证书 | 提供工信部入网证 |
| 配置要求 | 配置冗余电源，冗余风扇≥2个QSPF+光端口，≥4个QSPF28光端口，≥48个万兆光端口 |

##### 8、光模块

|  |  |  |
| --- | --- | --- |
| **功能及技术指标** | **详细技术参数** | **数量** |
| 40G多模光模块 | QSFP+ 40G光模块(850nm,300m,CSR4,支持1分4) | 6 |
| 万兆多模光模块 | SFP+ 万兆模块(850nm,300m,LC) | 16 |
| 万兆单模光模块 | SFP+ 万兆模块(1310nm,10km,LC) | 7 |
| 40G单模长距光模块 | QSFP+ 40G 光模块(1310nm,40km,ER4,LC) | 2 |
| 千兆单模光模块 | SFP-GE-单模模块-(1310nm,10km,LC) | 22 |
| 千兆多模光模块 | SFP-GE-多模模块-(850nm,0.55km,LC) | 2 |

### 技术要求

1.项目工期要求

本次项目要求在合同签订后30个自然日内完成设备到货，到后货30个自然日内完成安装部署。要求投标人提供合理的项目计划和建议，保证项目按时保质保量完成。

2. 项目组人员技术能力要求

投标人应在充分理解本项目需求的基础上，根据本技术方案的要求，建立专门项目团队并提供人员名单，确认项目经理1名、网安高级工程师1名、云数高级工程师1名以及相关技术人员、提供相应设备证明。

项目组人员能力情况要求：

（1）拟派项目经理取得信息系统项目管理师资格（人力资源和社会保障部、工业和信息化部批准颁发），取得信息安全工程师资格（人力资源和社会保障部、工业和信息化部批准颁发），每个证书1分，共2分；

（2）项目小组人员可以提供H3CIE/CCIE/HCIE证书（任一），每个证书0.5分，共1分；（证书颁发机构为华三、思科、华为等主流网络设备生产厂商）

（3）项目小组提供注册信息安全专业人员证书（CISP或CISSP）（中国信息安全测评中心颁发），每个证书0.5分，共1分；

以上三点提供投标人为其缴纳社保的凭证（近三个月）

（4）提供1人年驻场服务，得1分。

5、其他要求

1、本次采购内容为通用设备的采购，包括设备的供货、运输、系统集成、设备上架、安装验收、技术培训、售后服务以及伴随的其他服务等。

**2**、投标人须保证所提供产品符合国家有关规定。投标人须保证所提供产品具有合法的版权或使用权，本项目采购的产品，如在本项目范围内使用过程中出现版权或使用权纠纷，应由中标人负责，采购人不承担责任。

3、投标人应确保所提供产品的完整性、实用性，保证全部系统及时投入正常运行。否则若出现因投标人提供的产品不满足要求、不合理，而导致系统无法实现或不能完全实现的状况，投标人承担全部责任，由此产生风险和费用由投标人承担。

**4、中标人有义务保证采购人系统的完整性，如项目实施过程中因缺少所投标设备的配件或服务导致采购人系统无法正常运行，中标人须无偿提供。**

5、项目的工作内容及成果

（1）按照招标文件要求对全部设备的型号、规格、数量、外型、包装及资料（如保修单、随箱介质）进行验收。测试中出现性能指标或功能上不符合招标文件和合同要求时，采购人有拒收的权利。如果出现不符合招标文件和合同要求的严重质量问题时，采购人保留索赔权利。

（2）技术文档需求

中标人在工程开始和结束时应向用户提供下述技术文档：

（1）产品安装、运行、使用、测试、诊断和维修的技术文件。

（2）系统拓扑图、设备及软件产品配置清单。

（3）所购设备及软件的安装指南、使用手册、许可证、介质。

6、验收要求成交人需积极配合由甲方采购产生的第三方监理公司进行全过程监理。成交人需要按照第三方监理公司要求配合做好项目验收等各阶段资料完善递交的相关工作，并允许用户方工作人员参与配合设备的测试、安装、诊断及解决问题等各项工作。成交人在验收之前应提供本项目的验收方案，该方案由采购人审核并确认。

（1）验收步骤：采购人（包括邀请的专家）、成交人双方共同参与整个项目验收，分为初验、试运行和终验三个阶段。

（2）验收方法：采购人（包括邀请的专家）、成交人双方共同组成初验和终验的验收小组。由成交人提供测试结果，采购人提供使用报告，根据功能、性能要求进行验收。

（3）验收标准：主要性能及技术指标不得地域采购文件中的要求。

**商务要求表**

|  |  |
| --- | --- |
| **▲项目工期（交货期）及地点** | 服务时间：本次项目要求在合同签订后30个自然日内完成设备到货，到后货30个自然日内完成安装部署。地点：用户指定地点。 |
| **▲付款条件（明确是否需要履约保证金）** | 合同签订后总体设计方案得到采购人认可，自收到发票后7个工作日内支付合同总额的50%；硬件到货后，自收到发票后7个工作日内，支付合同总额的30%；项目完成且终验后，自收到发票后7个工作日内支付余款。本项目须缴纳履约保证金，履约保证金的数额为政府采购合同金额的1%（允许以履约保函的形式提交）。**备注：在签订合同时，供应商明确表示无需预付款或者主动要求降低预付款比例的，采购单位可不适用前述预付款比例的规定。** |
| **违约责任及争议解决方式** | 无特别说明，按“第五章 浙江省政府采购合同主要条款指引”相关违约责任及争议解决方式内容。 |
| **售****后****服务** | **项目维护计划** | 本项目整体质保期：3年项目（本项目硬件产品质保期三年）。硬件产品须含三年的上门服务。 |
| **响应情况** | 本项目必须具备较强得售后服务能力，能确保对用户方现场服务的快速相应及优质服务。0.5小时相应，2小时到现场，8小时恢复系统。中标人所提供得技术服务与产品使用功能无法满足招标文件要求，视为产品与服务不合格，采购人有权利拒绝支付剩余款项。 |
| **技术培训** | 培训为现场培训，培训内容包括系统平台使用和维护等，响应方有责任完成对所有软件产品、系统集成及工具等在内的全部培训，培训包括业务人员培训、技术维护培训。老师培训费、教材费等所有费用包含在本次报价中。 |
| **履约能力** | **投标人技术力量情况** | （1）投标人具备ISO9001质量环境体系认证证书；（2）投标人具备ISO27001信息安全管理体系认证证书；（3）投标人具备ISO14001环境管理体系认证证书；（4）投标人具备ISO27017云安全管理体系证书；（5）投标人具备信息系统安全集成服务资质一级；每满足一项得1分，最高得5分。 |
| **经验或业绩要求** | 提供自2019年1月1日以来类似成功案例，提供合同复印件并加盖公章，每提供一个得1分，最高得3分。 |

**第五章 浙江省政府采购合同主要条款指引**

 合同编号：

 确认书号：

**甲方**（采购人）：

**乙方**（供应商）：

甲、乙双方根据浙江省政府采购中心关于项目编号为 的（标项及名称）项目公开招标的结果，签署本合同。

**一、项目内容及合同价格**

金额单位：元

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 项目名称 | 技术需求 | 数量 | 单价 | 总价 |
|  | 详见项目对应招投标文件 |  |  |  |
| 合 计 |  |  |
| 合同总价大写： 小写：￥ |

注：1.项目具体技术需求及采购人地址等详见招标文件、投标文件以及询标记录。

　2.以上合同总价包含项目达到预期使用效果所需的一切费用。

**二、技术资料**

1.乙方应按招标文件规定的时间向甲方提供使用项目的有关技术资料。

2.没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。

**三、知识产权**

乙方应保证所提供的货物或其任何一部分均不会侵犯任何第三方的知识产权。

**四、产权担保**

乙方保证所交付的货物的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。

**五、转包或分包**

不允许转包。

允许分包部分 。

如乙方将项目转包或将不允许分包部分就行了分包，甲方有权解除合同，没收履约保证金并追究乙方的违约责任。

**六、质保期和履约保证金**

1.质保期年。（自项目验收合格交付使用之日起计）

2.履约保证金元。[履约保证金交至采购人处，在合同约定交货验收合格满（ ）个月之日起5个工作日内无息退还]

**七、项目工期及实施地点**

1.交货期：

2.实施地点：

**八、货款支付**

付款方式：

合同签订后总体设计方案得到采购人认可，自收到发票后7个工作日内支付合同总额的50%；硬件到货后，自收到发票后7个工作日内，支付合同总额的30%；项目完成且终验后，自收到发票后7个工作日内支付余款。

**九、税费**

本合同执行中相关的一切税费均由乙方负担。

**十、质量保证及售后服务**

详见招标文件。

**十一、调试和验收**

详见招标文件、投标文件。

**十二、货物包装**

详见招标文件、投标文件。

**十三、违约责任**

1.甲方无正当理由拒收验收项目的，甲方向乙方偿付拒收合同总价的百分之五违约金。

**2. 甲方收到乙方提供的发票，结合验收情况，验收合格的，在15日内将采购资金支付到乙方约定账户。**

甲方无故逾期验收和办理合同款项支付手续的,甲方应按逾期付款总额每日万分之五向乙方支付违约金。

3.乙方逾期交付项目的，乙方应按逾期交付项目总额每日千分之六向甲方支付违约金，由甲方从合同款项中扣除。逾期超过约定日期10个工作日不能交付的，甲方可解除本合同。乙方因逾期交付或因其他违约行为导致甲方解除合同的，乙方应向甲方支付合同总值5%的违约金，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

4.乙方所交的货物品种、型号、规格、技术参数、质量不符合合同规定及招标文件规定标准的，甲方有权拒收该货物，乙方愿意更换货物但逾期交货的，按乙方逾期交货处理。乙方拒绝更换货物的，甲方可单方面解除合同。

5.解除合同应按《浙江省政府采购合同暂行办法》向财政备案。

**十四、不可抗力事件处理**

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

2.不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

3.不可抗力事件延续120天以上，双方应通过友好协商，确定是否继续履行合同。

**十五、诉讼**

双方在执行合同中所发生的一切争议，应通过协商解决。如协商不成，可向甲方所在地法院起诉。

**十六、合同生效及其它**

1.合同经甲、乙两方签名并加盖单位公章后生效。

2.合同执行中涉及采购资金和采购内容修改或补充的，须双方经财政部门审批，并签书面补充协议，经报政府采购监督管理部门备案后，方可作为主合同不可分割的一部分。

3.招标文件、投标文件与本合同具有同等法律效力。

**4.对于通过预留采购项目、预留专门采购包、要求以联合体形式参加或者合同分包等措施签订的采购合同，应当明确标注本合同为中小企业预留合同。其中，要求以联合体形式参加采购活动或者合同分包的，应当将联合协议或者分包意向协议作为采购合同的组成部分。**

5.本合同未尽事宜，遵照《中华人民共和国民法典》有关条文执行。

6.本合同一式四份，具有同等法律效力，甲、乙两方各执二份。

甲方（盖章）：

地址：

法定（授权）代表人：

签名日期： 年 月 日

乙方（盖章）：

地址：

开户行：

开户帐号：

法定（授权）代表人：

签名日期： 年 月 日

**第六章 投标文件格式附件**

附件1**：**

**浙江省委网信办（本级）通用设备及网络安全升级项目**

项目编号：ZZCG2022X-GK-152（标项 ）

**资**

**质**

**文**

**件**

投标人全称：

地 址：

时 间：

**1、资质文件目录**

（1）投标声明书 (格式见附件2，含重大违法记录声明)；

（2）法定代表人授权委托书(格式见附件3)；

（3）提供有效的营业执照复印件并加盖公司公章；事业单位的，则提供有效的《事业单位法人证书》副本复印件并加盖单位公章；自然人的，则提供有效的身份证复印件并签字；

（4）联合投标协议书（若需要，格式见附件4）;

（5）联合投标授权委托书（若需要，格式见附件5）;

（6）分包意向协议（若需要，格式见附件6）

（7）提供采购公告中符合投标人特定条件要求的有效的其他资质复印件并加盖公司公章及需要说明的资料。

附件2：

**声 明 书**

致浙江省政府采购中心：

（投标人名称）系中华人民共和国合法企业，经营地址 。

我（姓名）系（投标人名称）的法定代表人，我方愿意参加贵方组织的（招标项目名称）（编号为ZZCG2022X-GK-152）的投标，为此，我方就本次投标有关事项郑重声明如下：

1.我方已详细审查全部招标文件，同意招标文件的各项要求，包括疫情期间采取的各项应急开标措施。

2.我方向贵方提交的所有投标文件、资料都是准确的和真实的。

3.若中标，我方将按招标文件规定履行合同责任和义务。

4.我方不是采购人的附属机构；在获知本项目采购信息后，与采购人聘请的为此项目提供咨询服务的公司及其附属机构没有任何联系。

5.投标文件自开标日起有效期为90天。

**6.我方承诺已经具备参与政府采购活动的资格条件并且没有税收缴纳、社会保障等方面的失信记录。**

7.我方通过“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）查询，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。

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

法定代表人签名（或签名章）： 日 期：

投标人全称（公章）：

附件3：

**法定代表人授权委托书**

浙江省政府采购中心：

我（姓名）系（投标人名称）的法定代表人，现授权委托本单位在职职工 （姓名）为授权代表，以我方的名义参加项目编号： 项目名称： 项目的投标活动，并代表我方全权办理针对上述项目的投标、开标、评标、签约等具体事务和签署相关文件。我方对授权代表的签名事项负全部责任。

在撤销授权的书面通知以前，本授权书一直有效。授权代表在授权书有效期内签署的所有文件不因授权的撤销而失效。

授权代表无转委托权，特此委托。

授权代表签名： 职务： 联系方式：

邮箱： 传真：

授权代表身份证号码：

法定代表人签名（或签名章）： 职务：

联系方式：

投标人全称（公章）： 日 期：

附件4：

**联合投标协议书**

甲方：

乙方：

（如果有的话，可按甲、乙、丙、丁…序列增加）

各方经协商，就响应 组织实施的编号为号的招标活动联合进行投标之事宜，达成如下协议：

一、各方一致决定，以 为主办人进行投标，并按照招标文件的规定分别提交资格文件。

二、在本次投标过程中，主办人的法定代表人或授权代理人根据招标文件规定及投标内容而对招标方和采购人所作的任何合法承诺，包括书面澄清及响应等均对联合投标各方产生约束力。如果中标并签订合同，则联合投标各方将共同履行对招标方和采购人所负有的全部义务并就采购合同约定的事项对采购人承担连带责任。

三、联合投标其余各方保证对主办人为响应本次招标而提供的产品和服务提供全部质量保证及售后服务支持。

四、本次联合投标中，甲方承担的工作和义务为:

乙方承担的工作和义务为：

（甲方 ）的合同份额占到合同总金额 %，（乙方 ）的合同份额占到合同总金额 %……

五、有关本次联合投标的其他事宜：

六、本协议提交招标方后，联合投标各方不得以任何形式对上述实质内容进行修改或撤销。

七、本协议签约各方各持一份，并作为投标文件的一部分。

|  |  |
| --- | --- |
| 甲方单位： （公章）法定代表人： （签章）日 期： 年 月 日 | 乙方单位： （公章）法定代表人： （签章）日 期： 年 月 日 |

附件5：

**联合投标授权委托书**

 本授权委托书声明：根据 与签订的《联合投标协议书》的内容，主办人的法定代表人现授权 为联合投标代理人，代理人在投标、开标、评标、合同谈判过程中所签署的一切文件和处理与这有关的一切事务， 联合投标各方均予以认可并遵守。

 特此委托。

授权人（签名）：

日期： 年 月 日

授权代表（签名）；

日期： 年 月 日

|  |  |
| --- | --- |
| 联合体甲方单位： （公章）法定代表人： （签章）日 期： 年 月 日 | 联合体乙方单位： （公章）法定代表人： （签章）日 期： 年 月 日 |

附件6：

**分包意向协议**

（投标人名称 ）若成为（项目名称 ）(招标编号： ）的中标供应商，将依法采取分包方式履行合同。（投标人名称 ）与（所有分包供应商名称 ）达成分包意向协议。 （投标人名称 ）负责签署投标文件，（投标人名称 ）的所有承诺均认为代表了（所有分包供应商名称 ）意愿。

一、分包内容在采购文件分包要求的范围内，并符合相关法律规定等

二、分包标的及数量

（投标人名称 ）将 工作内容 分包给（分包供应商名称 ），（分包供应商名称 ），具备承担 工作内容 相应资质条件且不得再次分包；

……

三、分包工作履行期限、地点、方式

四、质量

五、价款或者报酬

六、违约责任

七、争议解决的办法

八、其他

（分包供应商名称 ）的合同份额占到合同总金额 %以上。当分包份额占到合同总金额100%时，视为转包。此情况根据《中华人民共和国政府采购法实施条例》（国务院令第658号）文件第七十二条规定，将依照政府采购法第七十七条第一款的规定追究相关法律责任。

投标人名称(盖公章)：

分包供应商名称（盖公章）：

……

 日期： 年 月 日

附件7**：**

**浙江省委网信办（本级）通用设备及网络安全升级项目**

项目编号：ZZCG2022X-GK-152（标项 ）

**技**

**术**

**及**

**商**

**务**

**文**

**件**

投标人全称：

地 址：

时 间：

2、**技术及商务文件目录**

（1）评分对应表（格式见附件，主要用于评委对应评分内容）

（2）投标项目明细清单（含货物、服务等）；

（3）技术响应表（格式见附件）；

（4）项目总体解决方案（可包含且不限于对项目总体要求的理解、项目总体架构及技术解决方案等）；

（5）项目实施计划（可包含且不限于保证工期的施工组织方案及人力资源安排、项目组人员清单等）；

（6）列入政府采购节能环保清单的证明资料（若有）；

（7）商务响应表（格式见附件）；

（8）售后服务计划（可包含且不限于对用户故障的响应、处理、定期巡检、备品备件、常用耗材提供、驻点人员情况等）；

（9）技术培训计划（若有）；

（10）投标人履约能力（可包含且不限于技术力量情况、投标人各项能力证书）；

（11）案例的业绩证明（投标人业绩情况一览表、合同复印件等）；

（12）投标人认为需要的其他文件资料。

附件8：

**评分对应表**

投标人全称（公章）： 标项：

|  |  |  |
| --- | --- | --- |
| 评分项目 | 投标文件对应资料 | 投标文件页码 |
| 对应第三章评分办法及评分标准（报价除外） |  |  |
| …… |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

授权代表签名： 日期：

附件9：

**投标项目明细清单**

投标人全称（公章）： 标项：

货物类

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 货物名称 | 品牌 | 规格型号 | 单位及数量 | 性能及指标 | 产地 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

服务类

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务内容 | 服务人员数量 | 工作量 |
|  |  |  |  |
|  |  |  |  |

注：在填写时，如上表不适合本项目的实际情况，可在确保投标明细内容完整的情况下，根据上表格式自行划表填写。

授权代表签名： 日期：

附件10：

**技 术 响 应 表**

投标人全称（公章）： 标项：

|  |  |  |
| --- | --- | --- |
| 招标文件要求 | 投标文件响应 | 偏离情况  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

注：投标人应根据投标设备的性能指标、对照招标文件要求在“偏离情况”栏注明“正偏离”、“负偏离”或“无偏离”。

授权代表签名： 日 期：

附件11：

**项目组人员清单**

投标人全称（公章）： 标项：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 姓名 | 职务 | 专业技术资格 | 证书编号 | 参加本单位工作时间 | 劳动合同编号 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

注：在填写时，如本表格不适合投标单位的实际情况，可根据本表格式自行划表填写。

授权代表签名： 日 期：

附件12：

**商务响应表**

投标人全称（公章）： 标项：

|  |  |  |  |
| --- | --- | --- | --- |
| 项目 | 招标文件要求 | 是否响应 | 投标人的承诺或说明 |
| 供货时间（项目工期）及地点 |  |  |  |
| 付款条件 |  |  |  |
| 违约责任及争议解决方式 |  |  |  |
| 项目维护计划 |  |  |  |
| 响应情况 |  |  |  |
| 本地化服务要求 |  |  |  |
| 技术培训 |  |  |  |
| 公司技术力量情况 |  |  |  |
| 经验或业绩要求 |  |  |  |
| …… |  |  |  |

授权代表签名： 日期：

附件13：

**投标人业绩情况一览表**

投标人全称（公章）：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 采购单位名称 | 设备或项目名称 | 采购数量 | 单价 | 合同金额（万元） | 附件页码 | 采购单位联系人及联系电话 |
| 合同 | 验收报告 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 备注 | 提供投标人同类项目合同复印件、用户验收报告（如有）。 |

授权代表签名：　　　　　 时 间：

附件14**：**

**浙江省委网信办（本级）通用设备及网络安全升级项目**

项目编号：**ZZCG2022X-GK-152**（标项 ）

**报**

**价**

**文**

**件**

投标人全称：

地 址：

时 间：

3、**报价文件目录**

（1）开标一览表（见附件15）；

（2）投标人针对报价需要说明的其他文件和说明（格式自拟）；

（3）中小企业声明函（若需要，格式见附件16）；

（4）残疾人福利企业声明函（若需要，格式见附件17）；

附件15：

**开 标 一 览 表**

投标人全称（公章）：

招标编号及标项：

|  |
| --- |
| **货物类** |
| **货物****名称** | **品牌** | **产地** | **规格****型号** | **数量** | **单价****（元）** | **总价（元）** | **制造商情况** |
| **是否中小企业** | **企业全称** | **中小企业商号或注册商标** |
| **…** |  |  |  |  |  |  |  |  |  |
| **投标总价合计金额大写： 小写： ￥** |
| 备注 | 1.此表应按项目的明细情况列项填报,在填写时，如上表不适合本项目的实际情况，可在确保投标明细内容完整的情况下，根据上表格式自行划表填写。2.报价要求：项目费用包括项目实施所需的工程费、工时费、服务费、运输费、安装调试费、税费及其他一切费用。3.报价中不允许出现报价优惠等字样（明细出现“0”元，视同赠送）,投标总价合计金额应与明细报价汇总相等。4**.开标时，招标方在电子交易平台公开投标人的报价信息，投标人对报价信息进行确认。投标人对报价信息不予确认的不影响后续评标过程。** |

授权代表签名： 日期：

**开 标 一 览 表**

投标人全称（公章）：

招标编号及标项：

|  |
| --- |
| **服务类** |
| **服务内容** | **服务人员数量** | **工作量** | **单价****（元/人/天）** | **总价（元）** | **承接服务的企业情况** |
| **是否中小企业承接** | **企业全称** | **服务人员是否依照《中华人民共和国劳动合同法》订立劳动合同** |
| **…** |  |  |  |  |  |  |  |
| **投标总价合计金额大写： 小写： ￥** |
| 备注 | 1.此表应按项目的明细情况列项填报,在填写时，如上表不适合本项目的实际情况，可在确保投标明细内容完整的情况下，根据上表格式自行划表填写。2.报价要求：项目费用包括项目实施所需的工程费、工时费、服务费、运输费、安装调试费、税费及其他一切费用。3.报价中不允许出现报价优惠等字样（明细出现“0”元，视同赠送）,投标总价合计金额应与明细报价汇总相等。**4.开标时，招标方在电子交易平台公开投标人的报价信息，投标人对报价信息进行确认。投标人对报价信息不予确认的不影响后续评标过程。** |

授权代表签名： 日期：

**开 标 一 览 表**

投标人全称（公章）：

招标编号及标项：

|  |
| --- |
| **工程类** |
| 工程项目名称 | **施工范围** | **具体内容** | **施工工期** | **单价（元）** | **总价（元）** | **承建工程的企业情况** |
| **是否中小企业** | **企业全称** |
|  |  |  |  |  |  |  |  |
| **…** |  |  |  |  |  |  |  |
| **投标总价合计金额大写：小写：￥** |
| 备注 | 1.此表应按项目的明细情况列项填报,在填写时，如上表不适合本项目的实际情况，可在确保投标明细内容完整的情况下，根据上表格式自行划表填写。2.报价要求：项目费用包括项目实施所需的工程费、工时费、服务费、运输费、安装调试费、税费及其他一切费用。3.报价中不允许出现报价优惠等字样（明细出现“0”元，视同赠送）,投标总价合计金额应与明细报价汇总相等。**4.**开标时，现场工作人员当众拆封，并宣布投标人名称、投标总价合计金额。 |

授权代表签名： 日期：

附件16：

**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 1，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。

投标人名称（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，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）。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 1，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。

投标人名称（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。

附件17：

**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。

 投标人名称（盖章）：

 日 期：