浙江省公安厅（本级）浙江省人员流动JMZK系统-信息安全防护体系-零信任安全访问能力项目

项目编号：ZZCG2022D-GK-134

**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：****ZZCG2022D-GK-134**

**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)** |
| **1** | **浙江省公安厅（本级）浙江省人员流动JMZK系统-信息安全防护体系-零信任安全访问能力项目** | **批** | **1** | **1176.77** |

**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：** **标项1:允许联合体投标**

**五、获取采购文件**

1.获取时间：2022年7月13日至2022年8月4日 。

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年8月4日上午09:00**。**

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。

投标文件收件人：杜鹃鸣 ，联系方式：0571-88901837，实际投标文件收件人：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会议室上午08:30-12:00 下午14:00-17:30。（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年8月4日上午09:00时整在杭州市环城北路305号耀江发展中心二楼评标室开标。**

**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） | 杜女士 | 0571-88901837 | 0571-88907783 | 三楼专业项目采购部]） |
| 项目协办人（B岗） | 高女士 | 0571-88907717 | 0571-88907783 |
| 部门负责人 | 高女士 | 0571-88907717 | 0571-88907783 |
| 项目监督 | 吴女士 | 0571-88900117 | 0571-88907751 | 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**

标项1：

|  |  |
| --- | --- |
| **采购单位** | 浙江省公安厅（本级） |
| **地 址** | 杭州市上城区民生路66号 |
| **咨询事项** | **联系人** | **联系方式** | **传真** | **备注** |
| 采购需求等 | 黄先生 | 0571-87287131 |  |  |
| 项目监督 | 黄先生 | 0571-87287131 |  |  |

**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，本项目否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（服务类）**
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：浙江省公安厅（本级）浙江省人员流动JMZK系统-信息安全防护体系-零信任安全访问能力项目，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，对评分标准及采购文件需求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。 |
| 9 | 是否接受联合体投标 | 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》、《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》、《浙江省人民政府关于印发浙江省贯彻落实国务院扎实稳住经济一揽子政策措施实施方案的通知》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。）**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。** |
| 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、货到就位以及安装、调试、培训、保修等和费用，本项目不含车辆购置税）。

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。

（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》、《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》、《浙江省人民政府关于印发浙江省贯彻落实国务院扎实稳住经济一揽子政策措施实施方案的通知》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**

货款由采购人按招标文件规定的付款方式自行支付。若资金在采购人处的，由采购人直接支付；若资金在核算中心的，由采购人向核算中心发起支付令，由核算中心把货款打入中标商帐户。

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**

**标项1的评分方法**

|  |  |  |  |
| --- | --- | --- | --- |
| **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** | **20** |
| **1** | **技术** | **功能需求：对业主所属行业、系统部署环境、网络层级架构、数据分部结构的现状和理解。** | **5** |
| **2** | **技术** | **本项目目标、难点、特点的理解** | **2** |
| **3** | **技术** | **软件平台的部署和实施方案的先进性** | **5** |
| **4** | **技术** | **功能点及架构：软件整体架构与功能点的可行性、合理性、规范性** | **5** |
| **5** | **技术** | **硬件设备符合各项指标要求。对非关键的性能指标及技术参数负偏离或缺漏项的每项扣2分，（若负偏或缺漏项10个及以上的按重大偏离处理）。** | **28** |
| **6** | **技术** | **测试方案、进度控制计划** | **5** |
| **7** | **技术** | **项目系统集成综合解决方案** | **5** |
| **8** | **技术** | **软件开发工程量计算(技术文件中提供不含价格的工程量计算清单，要求到人\*天，格式自定)** | **2** |
| **9** | **技术** | **项目组人员个人、团队开发能力情况（资历及业绩）（详见商务要求表）** | **5** |
| **10** | **商务资信** | **项目维护计划（驻点人员安排，定期巡检等情况）的有效性等** | **5** |
| **11** | **商务资信** | **售后服务的响应情况（对用户故障响应、处理等）** | **4** |
| **12** | **商务资信** | **培训方案、计划的可行性及合理性** | **2** |
| **13** | **商务资信** | **公司技术力量情况等（详见商务要求表）** | **5** |
| **14** | **商务资信** | **经验及业绩(类似项目开发成功案例) （详见商务要求表）** | **2** |

**第四章招标需求**

**特别说明：**

**1.根据浙财采监字[2007]2号文件规定：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:** **浙江省公安厅（本级）浙江省人员流动JMZK系统-信息安全防护体系-零信任安全访问能力项目**

# 一、项目背景与建设目标

# 项目背景：按照公安部相关标准规范要求，结合省公安厅云平台、警综平台等建设实际及信息安全现状，为提升JMZK信息安全防护能力，规范建设安全管理能力，为新一代公安信息网智能化建设提供立体化纵深防御体系，形成严密安全保障。

# 目标内容：基于我省新一代公安信息网及安全基础设施，升级扩容省厅现有安全访问通道；建设数据交换通道，加强可信检控管理，部署数据中心配套安全防护能力；建设零信任体系一期，包括统一认证服务、权限管理服务、业务审计服务、环境感知服务、业务安全策略控制服务等；加强各服务联动和能力集成，实现各安全子系统的整体对接协同，初步构建零信任体系。

# 二、项目采购清单

详细采购清单如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **建设任务** | **建设分项** | **分项说明** | **采购类型** | **单位** | **数量** |
| 安全访问通道（升级扩容） | 可信检控管理（政法链路） | 为可信接入检控、可信应用检控提供集中配置、集群管理、连接会话管理、访问授权判定、风险响应等能力。根据设备环境、用户行为等属性及可信环境感知状态，动态控制用户的应用访问，保证业务应用访问的安全策略控制及强制实施。2U机箱;冗余电源（550W）、4T硬盘;2\*USB;1\*VGA;1\*BMC;标配4\*千兆电口;产品3年质保；为TAP、TIP提供集中配置、管理、会话、授权等能力。可和外部身份与访问管理平台实现认证、权限策略管理等能力。 | 硬件 | 台 | 2 |
| 可信检控管理 | 为可信接入检控、可信应用检控提供集中配置、集群管理、连接会话管理、访问授权判定、风险响应等能力。根据设备环境、用户行为等属性及可信环境感知状态，动态控制用户的应用访问，保证业务应用访问的安全策略控制及强制实施。2U机箱;冗余电源（550W）、4T硬盘;2\*USB;1\*VGA;1\*BMC;标配4\*千兆电口;产品3年质保；为TAP、TIP提供集中配置、管理、会话、授权等能力。可和外部身份与访问管理平台实现认证、权限策略管理等能力。 | 硬件 | 台 | 2 |
| 数据泄露检测 | 网络数据防泄漏系统，机架式设备，网络流量监控能力2G。支持常见的网络数据保护，包括：HTTP、HTTPS、FTP、SMTP、IMAP协议解析、对通过网络上传的附件和外发的内容进行扫描和监控、支持实现网络风险事件审计功能；支持多种策略配置，包括支持根据不同的组织机构下发不同的策略、支持针对不同的用户、用户组下发不同的策略、支持针对不同类别/级别的数据下发不同的策略、支持根据指定邮件域、收发邮件地址进行策略配置；支持基于机器学习和自然语言处理识别技术；支持持续样本学习及机器学习智能规则管理；支持通过机器学习实现数据内容识别规则在线调优，可持续提高识别准确性。 | 硬件 | 台 | 1 |
| 日志审计 | 性能：事件处理最高3000EPS。硬件规格：标准1U机箱，6个千兆电口，2个扩展插槽（可选2万兆光、4千兆电、4千兆光），1个Console接口，单电源，4T硬盘。包含50个日志源授权，三年硬件维保服务和三年软件升级维护服务。 | 硬件 | 台 | 1 |
| 负载均衡 | 性能参数：最高4层吞吐量：40Gbps，并发连接数：12000000，4层新建连接数 CPS：500000，7层新建连接数 RPS：500000。硬件参数：规格：2U，硬盘容量：240G SSD，电源：冗余电源，接口：6千兆电口+2万兆光口SFP+。要求同时支持链路负载均衡，服务器负载均衡，全局负载均衡，支持主动与被动故障检测等功能。产品质保(\*5年)；软件升级(\*5年)； | 硬件 | 台 | 2 |
| 蜜罐 | 主机（2U标准上架设备；含滑轨）一台。4\*GE电口；2\*10GE光口；4\*USB接口；1\*DB9 Console接口；冗余电源；4TB SATA存储硬盘。含系统软件一套。含三年产品标准维保服务；三年软件升级维护服务。 | 硬件 | 台 | 1 |
| 驻场人员服务 | 日常运维安全访问通道，配置相关策略，针对各业务系统对接提供相关指导协助。熟练掌握本项目安全系统的规划部署、测试、实施及优化等；熟练掌握公安大数据智能化应用安全体系要求；具备良好的逻辑分析能力及较强的学习能力，有团队合作精神和敬业精神；语言表达能力较强，思路清晰，能顺畅的与管理部门和业务对象进行沟通。 | 服务 | 年 | 3 |
| 原信息中心安全设备升级 | **防火墙系统（一级网）（核心产品）** | 多核AMP+架构，网络层吞吐量60G，并发连接≥1000万，每秒新建连接数60万，标准2U机箱，冗余电源， 标准配置1个Console口 、1个HA接口，1个MGT接口，4口万兆多模SFP板卡，支持2对硬件bypass；4口千兆多模SFP板卡；支持2对硬件bypass；8千兆电口板卡；另有1个接口板卡扩展插槽，支持液晶屏，含三年硬件维保服务。三年IPS和三年AV特征库升级。 | 硬件 | 台 | 2 |
| 日志审计系统（原信息中心） | 事件处理性能最高10000EPS。硬件规格：标准2U机箱，4个千兆电口，1块RAID卡，2个扩展插槽（可选2万兆光、4千兆电、4千兆光），冗余电源，8TB\*3块硬盘，使用RIAD5数据保护。包含500授权节点，包含三年硬件标准维保，三年软件升级服务。 | 硬件 | 台 | 1 |
| 负载均衡（PKI系统） | 标准2U设备，千兆电口≥6个，万兆电口≥2个，双电源，四层吞吐≥30G，最大并发连接数≥1200万，4层每秒新建连接数（CPS）≥50万/秒，7层每秒新建连接数(RPS)≥60万/秒。硬盘256G SSD.，质保5年，软件升级5年。 | 硬件 | 台 | 2 |
| 数据传输通道 | 下一代防火墙1 | 采用多核架构，1U机架式设备，千兆电口14个，千兆光口8个，万兆光口8个（配置2个万兆单模光模块）。 | 硬件 | 台 | 4 |
| 下一代防火墙2 | 采用多核架构，CPU物理核心数：8，内存16G，硬盘配置：64G SSD，2U机架式设备，8个千兆电口，4个千兆光口，4个万兆光口，2个扩展槽位，双交流电源。 | 硬件 | 台 | 2 |
| 集控探针 | Linux操作系统，网络接口≥6个10/100M/1000M电口 | 硬件 | 台 | 1 |
| 设备准入控制器 | 6个1000MBASE-T接口，2个万兆光口。每秒事务数（TPS)：≥22000（次/秒），最大吞吐量：≥4Gbps | 硬件 | 台 | 2 |
| 数据交换节点 | 交换能力：≥4Gbps；最大支持服务个数：≥60；最大传输延时：＜10ms。 | 硬件 | 台 | 8 |
| 数据交换接口机 | 4个10/100/1000Mbase-TX；4个万兆口（含万兆光模块），支持扩展插槽； | 硬件 | 台 | 4 |
| 数据传输节点 | 内外网接口各标配6个100/1000M Base-TX网络接口，2个10000M 光口。具有两个独立主机，独立主机之间，仅使用单个无源分光器进行单纤连接，不存在反方向的物理通道。 | 硬件 | 台 | 6 |
| 数据交换管控节点 | 配置4个100/1000M Base-TX网口 | 硬件 | 台 | 1 |
| 可信应用数据检控节点 | 4个10/100/1000MBase-T电口，2个万兆光口。 | 硬件 | 台 | 1 |
| 集中监控管理系统 | 4个10/100M/1000M电口；数据库容量：≥1TB；最大支持业务数量：≥1000；最大监控并发用户数量：≥5000； | 硬件 | 台 | 1 |
| 交换机1 | 交换容量≥2.56Tbps，包转发率≥720Mpps，以上指标以官网最小值为准；万兆光口≥24个（满配万兆多模光模块），40G QSFP+端口≥2个，业务插槽≥2个，冗余250W交流电源，冗余风扇； | 硬件 | 台 | 2 |
| 交换机2 | 交换容量≥2.56Tbps，包转发率≥720Mpps，以上指标以官网最小值为准；万兆光口≥24个（配置12个万兆多模光模块），5G/2.5G/1G自适应电口≥8个，40G QSFP+端口≥2个，业务插槽≥2个，冗余250W交流电源，冗余风扇； | 硬件 | 台 | 4 |
| 零信任体系一期 | 警综平台.零信任模块-认证服务 | 升级警综平台认证功能，建设零信任模块认证服务。在数据域单独部署，提供可信检控点的接口服务，增加认证因子，提供认证代理服务。 | 定制化软件 | 人/月 | 56 |
| 警综平台.零信任模块-权限服务 | 升级警综平台权限功能，建设零信任模块权限服务，包含个人管理权限，异常鉴权的预警等功能。 | 定制化软件 | 人/月 | 32 |
| 警综平台.零信任模块-基础要素管理 | 升级警综平台应用管理、建设服务目录，建设零信任模块，部署到数据域。包含服务目录管理、应用目录、对接API网关、对接云服务总线等功能。 | 定制化软件 | 人/月 | 8 |
|  | 警综平台.零信任模块-地市级级联 | 升级警综平台认证服务、基础要素管理服务，支持针对地市级开放统一标准化接口。 | 定制化软件 | 人/月 | 4 |
|  | 环境感知服务中心 | 提供2000节点环境感知客户端软件，三年服务期内提供免费升级服务。 | 商品化软件 | 点 | 2000 |
| 环境感知代理提供环境感知客户端的接入代理功能，将客户端到环境感知服务之间的请求以及环境感知风险信息发送到环境感知服务。环境感知服务负责对终端身份进行可信标识，对终端环境进行感知和度量，并传递给策略控制服务，协助策略控制服务完成终端的可信环境核查，从而实现动态访问控制的目的。环境感知服务应具备生成终端身份标识管理、感知策略管理、环境感知内容管理、终端环境感知报告、云桌面联动感知等功能。环境感知内容应具备系统环境感知与度量、物理环境感知与度量、安全配置风险感知与度量等方面。环境感知服务与策略控制服务、终端、应用之间联动。与策略控制服务联动实现可信环境感知结果的查询和通知；与终端联动实现终端环境数据的上报及感知策略下发；与应用联动是实现应用环境数据的上报及感知策略下发。 | 商品化软件 | 套 | 48 |
| 业务安全策略控制中心 | (1) 实时数据：业务策略控制中心的首页从系统概览，提高获取信息效率的角度，提供了展示当前天实时的数据接入、信任查询推送、登录设备数、登录用户数、各信任模型的计算情况以及资源使用情况。(2) 风险汇聚：业务策略控制提供了风险汇聚的能力，可将环境感知中心、审计中心、权限中心、认证中心和安全访问平台及安全防护策略控制服务传递的风险信息进行收集、汇聚，用于后续关联分析和信任评估。(3) 风险识别：业务策略控制中心内置了事件的详细分类信息，只有被系统识别，并且能归类到系统事件分类中的事件，才会被响应。(4) 信任评估：业务策略控制中心的信任基线计算根据多方输入的事件、日志等信息的持续性分析，根据基线配置，对用户、终端设备、移动端设备、服务器设备、API用户5个大类主体进行信任等级的计算，界面上展示各类主体的基线配置项数据。(5) 联动通报指令：业务策略控制提供下发安全控制指令的能力，策略执行点下发相关执行指令。(6) 统计中心：在业务策略控制中心数据统计中心部分，管理员可以对其它模块请求提交日志进行搜索查看，对大数据应用访问情况有总体统计展示，并且能够自己定义并生成相关的日志访问报表。支持厅机关新一代公安网业务系统100个以内的访问汇聚风险，提供风险识别和大数据分析。 | 商品化软件 | 套 | 65 |
| 省厅零信任体系集成开发 | 集成开发整体零信任体系，梳理业务需求，统一协调各功能模块进行对接，规范管理接口文档，组织相关测试方案。按照部标的要求进行功能点核对. | 服务 | 套 | 1 |
| 驻场人员1名 | 日常运维零信任体系，配置零信任体系相关策略，针对各业务系统对接提供相关指导协助。一名驻场人员（综合运营）三年驻场服务 | 服务 | 年 | 3 |
|  | 整体项目集成费用 | 根据项目总体费用，项目集成费用3.3%。 | 服务 | 项 | 1 |

## 定制化软件工作量测算

|  |  |  |  |
| --- | --- | --- | --- |
| **建设中心** | **功能模块** | **指标参数** | 人/月 |
| 警综平台.零信任模块-认证服务 | 与环境感知客户端对接 | 与环境感知客户端进行对接获取客户端评分，用以判断用户是否可以进行登录及后续操作。需对接各地市部署的环境感知评分获取接口，解析接口响应信息；向警综平台输出环境感知结果，包含评分信息、优化建议、安全软件下载链接、环境感知软件下载链接等信息；风险分析，根据评分执行阻断、提醒等操作，并记录分析日志 |  |
| 令牌管理 | 令牌分为用户令牌、应用令牌；用户令牌中需包含用户标识、机构标识、创建时间、过期时间等信息；应用令牌需包含用户标识、机构标识、应用标识、创建时间、过期时间等信息；令牌生成需基于JWT+国密算法进行令牌生成。 |  |
| 支持国密算法,保证令牌信息的机密性,系统除支持 RSA 算法的证书外，同时支持国产的 SM算法证书,支持基于国产密码算法的 SSL 功能，保证客户端到服务器之间的数据传输安全 |
| 提供用户令牌和应用令牌在各使用节点的全生命周期集中管理，包括：签发、撤销、验证、更新、加密等。管理功能：支持通过用户名、用户身份证号、用户IP、令牌类型、在线时间、部门信息进行令牌的筛选；支持对指定令牌的手动注销功能 |
| 支持根据接收到的风险指令或自有策略判断结果，调整相应令牌状态； |
|  支持将令牌及其状态通知给需要核验令牌的相关方。 |
| 令牌黑名单管理 | 1、包含增加、删除、查询功能；2、可以设置指定用户、IP、时间段，令牌受限，不允许登录零信任体系内的所有功能。 |  |
| 系统注册升级 | 支持认证因子、认证等级、AK、SK、固定SK配置管理 |  |
| 应用管理升级 | 1、认证管理部分添加零信任令牌属性选择2、细化应用管理，分为基本配置、高级配置、扩展信息、附加信息； |  |
| 认证管理升级 | 1. 在认证参数列表中添加令牌信息2、对接认证服务中心，获取用户令牌和应用令牌3、添加零信任令牌发放功能，包含用户令牌和应用令牌，对应用统一认证、第三方组件代理认证等相关模块进行功能集成
 |  |
| 认证功能 |  根据配置确定应用的认证方式； |  |
| 根据认证方式调用对应的认证因子进行认证； |
| 根据各认证因子反馈的认证结果进行综合判定，根据结果签发令牌； |
| 支持持续认证； |
| 支持认证过程中的风险检测输出及处理。人像认证组件： B/S端自动调起摄像头； 自动识别画面内是否存在人像； 自动拍照并上传服务器进行校验； 支持活体检测功能与人像1:1比对接口对接； 与认证中心对接，完成认证后可以进入警综平台； |
| 二次认证 | 支持用户二次认证，例如：用户通过短信验证码登录门户（当前安全等级较低为一级），需要登录安全等级较高的应用，例如执法办案系统，此时则会弹出二次认证界面，要求进行PKI认证。支持权限提升需要时的二次认证；支持登录状态失效是的二次认证；提供独立组件，供第三方系统需要时进行二次认证；二次认证支持单因子认证也支持多因子认证； |  |
| 认证因子管理 | 支持的认证因子包含但不限于口令、数字证书、生物特征，其中生物特征包括但不限于人脸、声纹等生物特征以及复合生物特征； |  |
|  认证因子信息包括但不限于认证因子名称、安全等级、启用状态、认证因子管理平台地址； |
| 支持认证因子信息的管理，包括但不限于增、删、改、查； |
|  支持认证因子的标准化接入和管理； |
| 支持活体检测等措施与多因子认证的组合； |
| 支持组合不同的认证因子满足不同的安全级别需求：支持申请材料的上传、删除、下载等功能；支持认证因子的启用、停用功能。 |
| 认证因子第三方对接 | 支持格尔网关认证 |  |
| 支持辅警证书认证 |
| 认证服务代理 | 支持代理跨网跨域访问认证服务；部署在安全访问通道或用户域。实现认证信息和返回令牌的跨域传递，最终通过令牌实现用户在用户域内能够访问数据域内的资源。 |  |
| 支持与认证服务间加密通信；支持标准协议，认证服务接口支持国密SSL；支持通过负载均衡和集群部署等形式，确保认证服务的持续可用，同时允许对认证能力进行扩容。 |
| 日志管理 | 支持多维度日志记录，包括但不限于注册、配置、认证、维护等操作日志； |  |
| 支持相关认证因子认证日志的接收； |
| 支持日志的标准化输出。定时对早期日志进行归档； |
| 认证服务接口 | 用户基本信息接口服务 |  |
| 用户详细信息接口服务 |
| 用户令牌生成服务 |
| 应用令牌生成服务 |
| 用户令牌校验服务 |
| 应用令牌校验服务 |
| 用户令牌更新服务 |
| 应用令牌更新服务 |
| 用户令牌撤销服务 |
| 应用令牌撤销服务 |
| 添加应用信息同步接口，支持第三方需要使用本接口的系统可以通过本接口获取全部应用信息，并保持增量更新。所有接口服务都需注册到服务总线；提供统一的第三方调用辅助JAR；支持全省应用对接并提供技术支持 |
| 与第三方对接 | 与业务安全策略控制、审计中心等服务对接推送风险、日志等信息，包含风险传递服务对接、认证令牌接收服务对接、认证日志接收服务对接、用户下线推送服务对接、应用下线推送服务对接、审计日志中的登录、应用操作等日志推送服务对接等安全管理中心对接用户、组织机构、应用目录、服务目录数据 |  |
| 警综平台.零信任模块-权限服务 | 规则权限配置 | 1. 包含规则权限的增、删、改、查等功能2、支持根据部门、人员类别、警种之中的单个或多个构建规则组合，并与应用进行关联配置

3、规则权限服务缓存服务在系统启动时自动将规则权限加载到内存中；自动从数据库中将新的规则更新到规则中；4规则解析服务根据部门、人员类别、警种自动遍历组装，通过特定算法重新生成新的规则列表；提升用户登录平台后获取规则权限无需等待，大幅度降低等待时间；5规则权限与警综平台权限体系融合 |  |
| 个人权限管理 | 1. 包含个人权限申请、个人权限申请审批、个人权限收回等功能2、个人权限申请：

用户可以在应用商店中对无权限的应用发起权限申请；支持按警综角色、应用信息（菜单级）申请；支持自动查找管理员，若管理员不存在则无法申请；3、个人权限申请审批：包含审批通过、审批退回等功能包含待审批列表、历史列表支持通过用户名、虚拟号、所属部门、查询范围、人员类别等信息进行筛选支持申请内容查看4、个人权限收回：包含收回、全部收回、组合收回等功能；支持同步应用树查看人员数量支持应用树查询；支持按用户姓名、身份证号、所属部门等信息进行筛选支持查看个人信息支持多应用进行人员筛选并进行权限回收 |  |
| 权限审批-辅助管理员 | 1. 根据应用管理中的辅助管理员配置分配本功能模块权限2、包含审批通过、审批退回、待审批列表、历史记录等功能3、管理员审批时可以查看审批内容、申请理由、申请时间、申请人等信息4、管理员审批时可以填写理由，并通过消息中心反馈给申请人

5、申请单失效自动回收，提供定时任务，自动检测预期的申请单，自动设置为失效 |  |
| 辅助管理员授权 | 1. 根据应用管理中的辅助管理员配置分配本功能模块权限2、提供管理人员列表的查询、详情查看、授权等功能3、辅助管理员授权仅允许单行数据操作

4、权限授权列表 展现辅助管理员拥有的权限列表 支持一级权限的授权、回收； 支持子级应用的授权、回收； 支持应用简称、全称的筛选功能。 |  |
| 应用级鉴权服务接口 | 1. 支持第三方系统、网关、安全通道等第三方应用或服务通过本接口获取应用权限信息；2、传入用户令牌，服务接口返回对应有权限的应用列表

3、支持单应用、多应用鉴权4、支持按人员获取权限列表5、支持资源权限等级获取 |  |
| 异常鉴权预警 | 支持对鉴权过程中的非正常鉴权产生预警； |  |
| 预警种类包括：用户异常时间鉴权预警、用户异常IP鉴权预警等；接收风险指令结果，对鉴权过程进行阻断；标准化输出预警结果； |
| 日志管理 | 支持多维度日志记录，包括但不限于注册、配置、认证、维护等操作日志； |  |
| 支持相关认证因子认证日志的接收； |
| 支持日志的标准化输出。定时对早期历史日志进行归档； |
| 警综平台.零信任模块-基础要素管理 | 服务目录 | 1、包含服务目录的增、删、改、查、启用、停用、导入、导出等功能；2、服务包含但不限于服务名称、服务IP、服务端口、服务目录、注册人、责任民警、运维人员、所属应用、登记时间、更新时间、数据来源等信息；3、对接云资源管理平台服务目录，支持定时同步数据到本服务目录；4、提供服务全量、增量同步接口服务，为零信任可信API网关提供数据支持；5、记录操作日志，方便管理员回溯历史记录； |  |
|  | 应用目录升级 | 1. 添加警种、运维工程师、责任民警、所属部门、责任领导、辅助管理员、相关人员、简要说明等信息的维护管理2、针对应用添加业务、地区、层次、警种等分类方式

3、支持应用手册的上传、下载、删除等功能4、支持AK、SK、固定SK信息的获取及查看5、应用上架服务及应用同步服务升级 |  |
| 警综平台.零信任模块-地市级级联 | 地市级级联 | 认证服务支持开发通用接口，允许地市级通过标准化接口进行级联。2、服务目录支持地市服务目录级联，支持定时同步数据到本服务目录。3、基础要素库人员目录开放标准通用接口，支持传输加密认证，支持地市级级联。4、基础要素库应用管理目录开放标准通用接口，支持传输加密认证，支持地市级级联。 |  |

# 项目详细采购需求

## 硬件采购详细需求

### 安全访问通道扩容

#### 可信检控管理（政法链路）（2台）

|  |  |
| --- | --- |
| **指标项** | **技术指标及参数** |
| 集群化部署 | ▲要求与公安厅原有安全访问通道政法链路的可信检控控制服务器进行集群化部署 |
| 基本参数 | 2U机箱;冗余电源（550W）、≥4T硬盘; ≥1 Console口；标配≥4\*千兆电口; ≥4个万兆光口。 |
| 最大并发用户数≥1000，每秒新建连接数≥7000，每秒权限判定数≥3000 |
| 标配国密卡，支持SM1、SM2、SM3、SM4国密算法，SM2签名（次/秒）≥12600,SM2验证（次/秒）≥4500,SM2密钥对生成（tps）≥10000，SM1加密/解密≥1Gbps，SM4加密/解密≥4Gbps |
| 可信应用检控集群管理 | 可信接入检控集群的统一管理，统一配置管理维护 |
| 配置管理可信接入检控集群，支持IP、端口、类型，启用/停用配置 |
| 配置管理消息支持自动、手动两种类型分发 |
| 集群消息支持消息签名验证，保障消息传递安全 |
| 消息推送传递失败后，记录状态，支持手动强制同步 |
| 可信应用检控集群管理 | 可信应用检控集群的统一管理，统一配置管理维护 |
| 配置管理可信应用检控集群，支持IP、端口、类型，启用/停用配置 |
| 配置管理消息支持自动、手动两种类型分发 |
| 集群消息支持消息签名验证，保障消息传递安全 |
| 消息推送传递失败后，记录状态，支持手动强制同步 |
| OAuth2标准支持 | 支持标准OAuth2，须提供Authorization Code模式 |
| 支持标准OAuth2，提供RestAPI接口服务 |
| 支持标准OAuth2，提供JAVA、PHP、Python、C/C++客户端SDK及Demo |
| OIDC标准支持 | 支持标准OIDC开放身份协议，提供ID\_Token身份令牌服务 |
| 支持标准OIDC开放身份协议，提供RestAPI接口服务 |
| 支持标准OIDC开放身份协议，提供JAVA、PHP、Python、C/C++客户端SDK及Demo |
| XACML标准支持 | 可配置过滤RBAC角色，删减RBAC中不满足属性的权限 |
| 基于属性的扩展授权协议，提供主体、客体授权策略配置 |
| 环境属性配置支持：来源IP、设备系统、系统帐号配置 |
| 可信环境感知：设备可信风险分等级设置 |
| 用户管理 | 提供用户、分组统一管理功能，包括用户信息增删改查用户信息备份导出、状态管理 |
| 单个、批量添加，导入/导出用户及用户组，支持导入导出密码加解密 |
| 支持按组、按用户选择认证服务器 |
| 提供名字、密码、邮箱、电话等属性设置，允许自定义用户属性、扩展字段 |
| 支持强密码校验，首次登录强制修改密码功能 |
| 用户/组可形成1比N归属，支持父组/子组之间继承 |
| 支持用户按认证服务器、组织关系自动分组 |
| 用户状态可设置：允许，锁定、禁止状态控制，支持认证失败次数、属性设定自动锁定用户状态 |
| 资源管理 | 支持API服务/API服务组两级分类资源配置，API组包含API服务列表 |
| 支持API用户、API用户组两级分类资源配置，API用户组支持父组/子组模式 |
| 支持HTTP、HTTPS类WEB应用配置 |
| 配置管理支持密码代填、Token传递、透传模式、代理模式四类WEB应用代理，提供产品功能相关证明材料 |
| 支持GET、POST方法设置，支持URLEncoding、JSON、Format格式设置登录格式，支持用户标识URI、用户标识属性提取自定义设置。 |
| 支持SSH、RDP、TELNET、VNC四类运维资源配置管理 |
| 统一提供AppID、访问密钥管理配置，为各类资源提供认证、验签服务接口，提供产品功能相关证明材料。 |
| 设备管理 | 提供设备状态、可信风险属性的查询、管理。 |
| 提供终端管理、状态查询功能，可按区域、状态过滤查询 |
| 考虑兼容、对接、运维等因素，建议可信检控控制服务能与可信接入检控 、可信应用检控等产品和组件为同一品牌。 |
| 授权策略管理 | 支持基于角色的授权策略配置，配置主体、客体角色授权 |
| 支持基于属性的授权策略配置，可为角色授权提供属性条件过滤规则与控制 |
| 提供可信环境风险、用户行为分析、用户环境属性多维度的授权策略统一管理功能 |
| 支持和授权服务联动 | 通过授权服务的应用授权接口、API授权接口、运维授权接口等获取应用、API、运维业务权限列表 |
| 支持权限变更订阅 | 支持订阅授权服务的权限变更服务，以便实时获取最新权限 |
| 授权判定与执行 | 支持为可信接入检控、可信应用检控、可信运维代理提供实时的访问权限判定 |
| 代理连接会话管理 | 支持为可信接入检控、可信应用检控、可信运维代理提供集中的代理连接会话管理 |
| 用户会话服务 | 提供用户会话自动创建、维护、销毁全生命周期管理 |
| 用户会话状态查询、状态控制功能 |
| 用户会话支持分布式、持久化机制，全局生效，宕机自恢复 |
| 访问令牌服务 | 提供用户令牌、应用令牌、API令牌的申请、颁发、撤销、同步等安全访问控制机制 |
| 支持三级令牌管理：用户、应用、API三级令牌的全生命周期管理 |
| 令牌转换服务：提供OIDC、SAML、OAuch2令牌转换服务 |
| 动态访问控制引擎 | 提供动态策略评估引擎，动态计算用户、行为、风险、环境等安全因子，持续完成用户、设备、应用的可信状态评估，具备一种基于用户的安全访问控制的方法，提供相关证明。 |
| 引擎提供对外RestAPI标准接口，可完成内部、外部授权访问的动态评估 |
| 支持数据库、NoSQL库、策略、设备、用户信息外部资源信息查询 |
| 支持XACML标准、JSON格式，自定义属性、类型引擎决策 |
| 系统具备多核多平台并行安全操作系统。支持硬件或微服务扩展。 |
| 设备属性跨级汇聚 | 支持部、省、市三级的设备属性自动汇聚、上报 |
| 设备可信状态属性自动汇聚 |
| 部级管理可设置、过滤感知部分省、市级风险 |
| 省级管理可设置、过滤感知省级、市级风险 |
| 各级设备可信状态属性可在统一管理平台查询 |
| 可信风险通报 | 风险通报实现将异常信息通报给统一身份与权限管理。异常信息包括：终端异常、违规操作等。支持统一多级式风险感知与通报。 |
| 公安PKI CA证书双向认证 | 支持可信CA导入/导出管理，支持PEM/DER/PCKS7证书格式导入 |
| 支持双向证书认证机制 |
| 提供证书CRL撤销列表、OPCS撤销同步机制 |
| 提供证书过滤、用户/组织关系、用户名+证书多重认证开启功能 |
| RADIUS认证 | 支持监听地址、端口、超时、PAP/CHAP/MS-CHAPv1/MS-CHAPv2协议 |
| 支持NAS配置管理，支持每个NAS配置不同密钥 |
| 支持RADIUS验证多种模式：密码+动态口令、前缀模式、后缀模式、Challenge模式认证 |
| AD认证&LDAP认证 | 支持LDAP认证，支持Client BaseDN设置及认证 |
| 支持LDAP协议的查询、认证指令 |
| 支持Windows IWA统一认证，支持用户通过IWA机制自动认证、免密登录 |
| 其它第三方认证协议 | 支持数据库用户名、密码认证：配置数据库、登录名、表、行列 |
| 支持POP3、SMTP、IMAP三种邮件协议、服务器设置，支持邮件帐号密码认证 |
| 支持HTTP认证：IP、端口、URL、用户、密码及HTTP Response检测认证 |
| 支持短信认证：短信网关设置、单次短信有效时间、发送超时、短信提示模板、验证失败次数配置 |
| 单点登录SSO | 提供单点登录令牌认证服务 |
| 提供SSO共享、不共享配置及策略控制 |
| 支持密码代填、Token验证两类SSO机制 |
| 支持单点登出、登出过程自定义流程控制功能 |
| 可靠性 | 支持3台以上分布式集群。 |
| 统一管理门户，支持用户会话、应用、API多级令牌持久化 |
| 支持统一存储、分布式缓存及状态监控 |
| 支持一键集群自动安装，分布式安装、升级、启停业务 |
| 日志审计 | 要求拥有高性能的syslog日志处理和存储方法技术，要求提供相关技术文件复印件。提供用户登陆日志、用户操作日志、系统运行日志等信息采集、管理及审计，并支持日志服务器上报。本地存储空间支持审计日志本地留存6个月以上。 |

#### 可信检控管理（2台）

|  |  |
| --- | --- |
| **指标项** | **技术指标及参数** |
| 集群化部署 | ▲要求与原有安全访问通道数据域链路的可信检控管理系统进行集群化部署 |
| 基本参数 | 2U机箱;冗余电源（550W）、≥4T硬盘; ≥1 Console口；标配≥4\*千兆电口; ≥4个万兆光口。 |
| 最大并发用户数≥1000，每秒新建连接数≥7000，每秒权限判定数≥3000 |
| 标配国密卡，支持SM1、SM2、SM3、SM4国密算法，SM2签名（次/秒）≥12600,SM2验证（次/秒）≥4500,SM2密钥对生成（tps）≥10000，SM1加密/解密≥1Gbps，SM4加密/解密≥4Gbps |
| 可信接入检控集群管理 | 可信接入检控集群的统一管理，统一配置管理维护 |
| 配置管理可信接入检控集群，支持IP、端口、类型，启用/停用配置 |
| 配置管理消息支持自动、手动两种类型分发 |
| 集群消息支持消息签名验证，保障消息传递安全 |
| 消息推送传递失败后，记录状态，支持手动强制同步 |
| 可信应用检控集群管理 | 可信应用检控集群的统一管理，统一配置管理维护 |
| 配置管理可信应用检控集群，支持IP、端口、类型，启用/停用配置 |
| 配置管理消息支持自动、手动两种类型分发 |
| 集群消息支持消息签名验证，保障消息传递安全 |
| 消息推送传递失败后，记录状态，支持手动强制同步 |
| OAuth2标准支持 | 支持标准OAuth2，须提供Authorization Code模式 |
| 支持标准OAuth2，提供RestAPI接口服务 |
| 支持标准OAuth2，提供JAVA、PHP、Python、C/C++客户端SDK及Demo |
| OIDC标准支持 | 支持标准OIDC开放身份协议，提供ID\_Token身份令牌服务 |
| 支持标准OIDC开放身份协议，提供RestAPI接口服务 |
| 支持标准OIDC开放身份协议，提供JAVA、PHP、Python、C/C++客户端SDK及Demo |
| XACML标准支持 | 可配置过滤RBAC角色，删减RBAC中不满足属性的权限 |
| 基于属性的扩展授权协议，提供主体、客体授权策略配置 |
| 环境属性配置支持：来源IP、设备系统、系统帐号配置 |
| 可信环境感知：设备可信风险分等级设置 |
| 用户管理 | 提供用户、分组统一管理功能，包括用户信息增删改查用户信息备份导出、状态管理 |
| 单个、批量添加，导入/导出用户及用户组，支持导入导出密码加解密 |
| 支持按组、按用户选择认证服务器 |
| 提供名字、密码、邮箱、电话等属性设置，允许自定义用户属性、扩展字段 |
| 支持强密码校验，首次登录强制修改密码功能 |
| 用户/组可形成1比N归属，支持父组/子组之间继承 |
| 支持用户按认证服务器、组织关系自动分组 |
| 用户状态可设置：允许，锁定、禁止状态控制，支持认证失败次数、属性设定自动锁定用户状态 |
| 资源管理 | 支持API服务/API服务组两级分类资源配置，API组包含API服务列表 |
| 支持API用户、API用户组两级分类资源配置，API用户组支持父组/子组模式 |
| 支持HTTP、HTTPS类WEB应用配置 |
| 配置管理支持密码代填、Token传递、透传模式、代理模式四类WEB应用代理，提供产品功能相关证明材料 |
| 支持GET、POST方法设置，支持URLEncoding、JSON、Format格式设置登录格式，支持用户标识URI、用户标识属性提取自定义设置。 |
| 支持SSH、RDP、TELNET、VNC四类运维资源配置管理 |
| 统一提供AppID、访问密钥管理配置，为各类资源提供认证、验签服务接口，提供产品功能相关证明材料。 |
| 设备管理 | 提供设备状态、可信风险属性的查询、管理。 |
| 提供终端管理、状态查询功能，可按区域、状态过滤查询 |
| 考虑兼容、对接、运维等因素，建议可信检控控制服务能与可信应用接入代理 、可信应用检控等产品和组件为同一品牌。 |
| 授权策略管理 | 支持基于角色的授权策略配置，配置主体、客体角色授权 |
| 支持基于属性的授权策略配置，可为角色授权提供属性条件过滤规则与控制 |
| 提供可信环境风险、用户行为分析、用户环境属性多维度的授权策略统一管理功能 |
| 支持和授权服务联动 | 通过授权服务的应用授权接口、API授权接口、运维授权接口等获取应用、API、运维业务权限列表 |
| 支持权限变更订阅 | 支持订阅授权服务的权限变更服务，以便实时获取最新权限 |
| 授权判定与执行 | 支持为可信接入检控、可信应用检控、可信运维代理提供实时的访问权限判定 |
| 代理连接会话管理 | 支持为可信接入检控、可信应用检控、可信运维代理提供集中的代理连接会话管理 |
| 用户会话服务 | 提供用户会话自动创建、维护、销毁全生命周期管理 |
| 用户会话状态查询、状态控制功能 |
| 用户会话支持分布式、持久化机制，全局生效，宕机自恢复 |
| 访问令牌服务 | 提供用户令牌、应用令牌、API令牌的申请、颁发、撤销、同步等安全访问控制机制 |
| 支持三级令牌管理：用户、应用、API三级令牌的全生命周期管理 |
| 令牌转换服务：提供OIDC、SAML、OAuch2令牌转换服务 |
| 动态访问控制引擎 | 提供动态策略评估引擎，动态计算用户、行为、风险、环境等安全因子，持续完成用户、设备、应用的可信状态评估，具备一种基于用户的安全访问控制的方法，提供相关证明。 |
| 引擎提供对外RestAPI标准接口，可完成内部、外部授权访问的动态评估 |
| 支持数据库、NoSQL库、策略、设备、用户信息外部资源信息查询 |
| 支持XACML标准、JSON格式，自定义属性、类型引擎决策 |
| 系统具备多核多平台并行安全操作系统。支持硬件或微服务扩展。 |
| 设备属性跨级汇聚 | 支持部、省、市三级的设备属性自动汇聚、上报 |
| 设备可信状态属性自动汇聚 |
| 部级管理可设置、过滤感知部分省、市级风险 |
| 省级管理可设置、过滤感知省级、市级风险 |
| 各级设备可信状态属性可在统一管理平台查询 |
| 可信风险通报 | 风险通报实现将异常信息通报给统一身份与权限管理。异常信息包括：终端异常、违规操作等。支持统一多级式风险感知与通报。 |
| 公安PKI CA证书双向认证 | 支持可信CA导入/导出管理，支持PEM/DER/PCKS7证书格式导入 |
| 支持双向证书认证机制 |
| 提供证书CRL撤销列表、OPCS撤销同步机制 |
| 提供证书过滤、用户/组织关系、用户名+证书多重认证开启功能 |
| RADIUS认证 | 支持监听地址、端口、超时、PAP/CHAP/MS-CHAPv1/MS-CHAPv2协议 |
| 支持NAS配置管理，支持每个NAS配置不同密钥 |
| 支持RADIUS验证多种模式：密码+动态口令、前缀模式、后缀模式、Challenge模式认证 |
| AD认证&LDAP认证 | 支持LDAP认证，支持Client BaseDN设置及认证 |
| 支持LDAP协议的查询、认证指令 |
| 支持Windows IWA统一认证，支持用户通过IWA机制自动认证、免密登录 |
| 其它第三方认证协议 | 支持数据库用户名、密码认证：配置数据库、登录名、表、行列 |
| 支持POP3、SMTP、IMAP三种邮件协议、服务器设置，支持邮件帐号密码认证 |
| 支持HTTP认证：IP、端口、URL、用户、密码及HTTP Response检测认证 |
| 支持短信认证：短信网关设置、单次短信有效时间、发送超时、短信提示模板、验证失败次数配置 |
| 单点登录SSO | 提供单点登录令牌认证服务 |
| 提供SSO共享、不共享配置及策略控制 |
| 支持密码代填、Token验证两类SSO机制 |
| 支持单点登出、登出过程自定义流程控制功能 |
| 可靠性 | 支持3台以上分布式集群。 |
| 统一管理门户，支持用户会话、应用、API多级令牌持久化 |
| 支持统一存储、分布式缓存及状态监控 |
| 支持一键集群自动安装，分布式安装、升级、启停业务 |
| 日志审计 | 要求拥有高性能的syslog日志处理和存储方法技术，要求提供相关技术文件复印件。提供用户登陆日志、用户操作日志、系统运行日志等信息采集、管理及审计，并支持日志服务器上报。本地存储空间支持审计日志本地留存6个月以上。 |
| 云桌面适配 | 要求支持公安厅已建设的云桌面系统联动。提供相关证明文件 |

#### 数据防泄漏检测

|  |  |
| --- | --- |
| **指标项** | **指标参数** |
| 产品硬件和性能规格 | 2U机架式设备，4个千兆电口，硬盘容量≥4TB，最大网络流量≥1.5Gbps；提供三年维保服务。 |
| 产品功能 | 产品支持分布式部署架构，可以同一业务平台管理多个网络DLP节点和多个邮件DLP节点，用户可以分别给不同的节点下发策略、设置不同的节点数据访问权限。 |
| 产品应具备灵活部署的能力，支持旁路、串路部署，AGENT部署。 |
| 支持集中管理、分布式部署，以保证可存储海量事件和证据文件。系统通过统一管理平台对所有组件包括网络监控、邮件保护）进行管理和监控。 |
| 支持office，wps及常用文件类型，如：ceb、doc、docx、xls、xlsx、ppt、pptx、rtf、pdf、txt、html、xml、C/C++、perl、shell、rar、zip、tar、gzip、7z、iso 等常见的文档类型解析和内容提取。 |
| 产品支持内置行业字典库，可选择各个字典库中的内容为依据设置策略。 |
| 支持事件日志统一查询，支持按照邮件、Web 邮件、HTTPS、HTTP、FTP、论坛、微博、网盘等网络应用类型进行查询，支持按网关IP、事件时间、发送IP、事件等级等条件进行快速查询。 |
| 产品支持策略数据审计统计、策略阻断统计、全量数据设计统计，分不同维度查看数据态势，如协议分布、文件类型分布、时间分布、策略分布等。 |
| 具备邮件防护能力，支持对审批的流程进行自定义设置，包括审批层级、范围、形式等内容。 |
| 支持邮件DLP，在邮件边界下的邮件统一信息展现与统计，统计维度包含：策略数据、最新策略数据、海量数据统计、海量附件统计等，展板支持：策略数据分析、海量数据分析等。 |
| 支持解析访问数据库返回的结果集，并依策略对敏感数据识别匹配；支持关系数据库/NoSQL数据库结果集的审计。 |
| 产品资质要求 | 产品具备数据泄露防护产品《计算机信息系统安全专用产品销售许可证》，提供证书证明。 |
| 产品具备计算机软件著作权登记证书，提供证书证明。 |

#### 蜜罐

|  |  |
| --- | --- |
| 指标项 | 指标参数 |
| 性能指标 | 主机（2U标准上架设备；含滑轨）一台。4\*GE电口；2\*10GE光口；4\*USB接口；1\*DB9 Console接口；冗余电源；4TB SATA存储硬盘。含系统软件一套。含三年产品标准维保服务；三年软件升级维护服务。 |
| 支持同时运行的实例数量 | 支持同时运行20个高交互蜜罐数量或40个中交互蜜罐或者80个低交互蜜罐 |
| 响应能力 | 95%的蜜罐实例页面10S内响应 |
| 告警处理能力 | 告警处理能力不小于2000/s |
| 监测中心 | 告警统计分析，支持统计某段时间范围内蜜罐告警数量，并且通过环比的方式展示告警趋势的变化 |
| 告警威胁等级分析，支持统计某段时间内告警等级的总数和分布 |
| 攻击IP TOP5，统计某段时间内攻击次数排名的前5的攻击IP极其归属地信息 |
| 蜜罐实例告警统计，统计展示某段时间范围内不同蜜罐告警实例产生告警的数量和比例 |
| 展示某段时间内范围内产生告警数量排名前10的告警类型的统计 |
| 展示系统的运行状态，包括CPU利用率、内存利用率、存储空间使用率、网络流量，日志外发情况的展示 |
| 攻击流量牵引 | 持通过SDN的方式进行攻击力量的牵引，支持对SDN交换机的链路和接口进行管理、支持引流策略的管理。 |
| 支持通过代理模式进行流量牵引，无需外置硬件探针 |
| SDN模式下支持引流的白名单，包括对源IP、目的IP、域名的过滤。 |
| SDN模式支持自动策略和手动策略，自动策略模式下支持和流量检测分析设备进行联动，将指定告警类型告警流量引入到蜜罐系统中。手动策略可以配置需要引流的源IP和目的IP |
| 攻击流量智能分析及处置 | 支持按照协议类型将不同的攻击流量引入不同的蜜罐实例 |
| 支持HTTP攻击流量进行诱骗，涵盖的Web攻击类型包括：文件读取、目录遍历、命令执行、代码执行、SQL注入、XSS等 |
| 支持对漏洞使用的攻击诱捕，包括对已知漏洞、未知漏洞利用的完整攻击行为事件，支持一种网络入侵行为检测系统及检测方法，提供相关证明文件 |
| 支持常见网络行为的捕获，包括网络连接、网络断开连接、网络访问 |
| 支持对会话、登录行为的捕获，包括账户本地登录、密码修改、远程登录、会话创建及注销等 |
| 支持对特定攻击流量应答，降低对高交互蜜罐的依赖 |
| 蜜罐 | 支持内置常见漏洞的靶场，包含weblogic、Struts2、tomcat、thinkphp、springboot等 |
| 内置爬虫模块，对目的IP进行主动爬取，并对爬取后的页面进行了自动化的容错处理，包括对资源的引用问题等，并自动化构建新服务。 |
| 支持蜜罐代理功能，在将攻击者引入高交互蜜罐之前，蜜罐代理根据协议类型、服务类型、攻击类型进行预处理。 |
| 支持对蜜网网段的管理，支持IP的添加和删除 |
| 支持内置蜜罐模版，数量不少于30个 |
| 支持通过模版的方式导入蜜罐模版，可以配置蜜罐模版名称、服务名称、端口、硬件规格，类型包括高交互蜜罐、中交互蜜罐和低交互蜜罐 |
| 低交互蜜罐：支持对常见网络设备或服务仿真：apple,unbound, bind,proftpd, stupid-ftpd,apache, nginx, iis,dovecot, novell,samba, printer, ibm, windows,default, novell,rustock, exim,ubuntu, cisco, centos, comware, debian, freebsd, huawei等。 |
| 低交互蜜罐: 支持仿真常见的协议服务 如ftp、ssh、telnet、tftp、http、ntp、snmp、mysql、rdp、vnc、redis、httpproxy、git、mssql、imap、ldap、ibm-db2、imap、dns等近30种，部分协议可以设置仿真设备种类近百种 |
| 中交互蜜罐：支持SSH服务的仿真 |
| 高交互蜜罐: 支持仿真 linux、windows操作系统环境 |
| 支持登录反制蜜罐，用于定制真实网站的登录界面仿真，与真实网站的登录界面一致，并含有反制与钓鱼功能 |
| 支持qcow2类型的蜜罐模版文件 |
| 支持对蜜罐实例的管理，支持蜜罐实例的开启、关闭、编辑和删除操作。 |
| 支持蜜罐诱饵的配置，包括Xshell连接诱饵、SSH历史命令诱饵、账号信息诱饵、远程桌面诱饵、hostname映射诱饵 |
| 支持通过分发程序在指定目标上发布诱饵，通过诱饵将攻击目标转移到蜜罐系统 |
| 支持实时监控蜜罐运行状态 |
| 反制功能 | 支持在指定的实例上配置反制功能，通过反制功能获取攻击者的浏览器隐私数据、主机账号、主机IP及端口开放情况、个人应用账号、身份ID等信息 |
| 支持通过JSONP进行反制 |
| 支持通过文件下载欺骗的方式进行反制，可以通过系统构造具备下载功能的页面，诱骗攻击者点击运行 |
| 支持MYSQL反制 |
| 支持RDP反制 |
| 完全机制 | 自定义蜜网与业务网络隔离 |
| 蜜罐KVM支持内核级安全加固，防止虚拟机逃逸 |
| 告警日志查询 | 支持按时间、受害IP、攻击IP、实例名称、威胁名称、告警类型、威胁等级、攻击结果查询系统的告警日志 |
| 支持按照告警类型和告警数量进行统计，展示告警态势 |
| 支持告警类型日志的展示,告警详情的展示 |
| 支持和该告警关联告警的展示 |
| 报表管理 | 支持快速报表并提供报表模版 |
| 快速报表：可自定义选择报表生成的时间范围、报表格式、报表模版 |
| 报表模版：默认提供多种报表模版，模版包括告警总数、告警等级，攻击IP，攻击类型 |
| 系统设置 | 支持证书管理：导入/导出 |
| 支持网络配置：可进行IP配置及DNS配置 |
| 支持系统离线升级 |
| 支持运营配置：支持导航LOGO、系统LOGO、企业LOGO、系统名称、浏览器页签、版权信息的配置 |
| 支持配置反制外网IP地址信息 |
| 支持用户账号的安全性管理，支持密码强度设定、支持密码锁定、支持密码更换周期的设定 |
| 支持的平台重要操作的日志审计，并支持审计日志的导出 |
| 支持通过SNMP向第三方平台发送设备状态日志 |
| 支持通过SYSLOG向第三方平台发送告警日志和设备状态日志，支持高性能的Syslog日志处理和存储方法，提供相关证明文件。 |
| 支持通过页面对设备进行关机、重启、服务重启等操作，支持重点调试日志的导出 |

#### 日志审计设备（安全访问通道）

|  |  |
| --- | --- |
| **指标项** | **指标参数** |
| 产品硬件和性能规格 | 1U机架式设备, 10/100/1000M电口≥6，接口扩展槽位≥2, 硬盘容量≥4TB, 缺省授权至少支持接入50个日志源；提供三年原厂维保服务。 |
| 产品功能 | 系统应采用大数据平台架构，具备海量数据收集与快速检索能力。 |
| 系统应支持单机部署，集群部署，分布式部署。 |
| 系统应支持范式化日志多级提取，支持字段提取、字段转换、字段修正等。 |
| 系统应支持正则表达式、分隔符、KV、JSON字符串等多种灵活的提取方式,支持自动生成正则以高效的辅助提取，提供产品功能相关证明材料。 |
| 系统应支持通过分析上报的日志信息来自动发现资产，无需手动录入资产，从而减少了用户的工作量，提供产品功能相关证明材料。 |
| 系统应能够对WEB服务器日志展开深度分析，分析内容包括但不限于发起请求的地址及浏览器情况、响应结果、访问趋势及注册表审核监控等。 |
| 系统应能支持自定义报表目录、LOGO等，支持统计项引用到报表。 |
| 系统应支持资产以拓扑图形式展示，鼠标移动至资产图标可展示对应的资产信息。 |
| 系统应能够实现范式化日志的枚举值管理，实现对范式化日志字段的灵活翻译。 |
| 系统应支持IPv4、IPv6日志数据的采集、范式化、分析、展示。 |
| 为满足日志数据扩展需求，系统应支持日志存储扩展，如NFS网络共享存储扩展，提供产品功能相关证明材料。 |
| 系统应提供日志转发功能，应支持日志转发多个目标地址，可实现原始日志、范式化日志的转发，且不丢失原始日志源IP信息。 |
| 系统应支持主备切换，在主机工作时，部署备机实时心跳监控主机状态，发生意外时主备替换，避免因意外导致的数据丢失。 |
| 系统应支持外置采集器，外置采集器数据应提供加密压缩传输，以确保数据安全以及传输效率。 |
| 系统应支持规则自适应日志接入，应支持将新接收的日志信息与系统内置规则、自定义规则进行匹配，将匹配度最高的规则与接收到的日志进行关联，完成自动接入。 |
| 产品资质要求 | 产品具备中国信息安全认证中心颁发的《中国国家信息安全产品认证证书》，提供证书证明。 |
| 产品具备中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书》EAL3+等级证书，提供证书证明。 |

#### 负载均衡

| **指标项** | **规格要求** |
| --- | --- |
| 硬件规格 | 标准2U设备，千兆电口≥6个，万兆光口≥2个，双电源；硬盘≥240G SSD. |
| 性能要求 | 四层吞吐≥42G，最大并发连接数≥1200万，4层每秒新建连接数（CPS）≥50万/秒，7层每秒新建连接数(RPS)≥60万/秒。 |
| 部署模式 | 支持路由、旁路部署，以及三角传输 |
| 高可用性 | 支持主主（AA）、主备（AS）工作模式，IP地址可在设备间漂移，根据设备状态将流量牵引到主设备。支持包括半连接，全连接会话信息全状态同步；支持会话保持信息同步；以保障业务不间断切换。 |
| 支持浮动MAC，HA切换过程MAC地址不变。 |
| 支持基于心跳信号丢失、链路断开、远端服务不可达等多种方式的HA切换条件及逻辑。 |
| 支持标准VRRP协议。需要提供界面相关证明材料， |
| 集群部署：可以实现两台以上设备集群部署，多台设备同时负载一台设备在线备份。 |
| 应用系统加速 | 支持一个虚拟服务，可选择多个SSL证书，适用于多个域名共用一个虚拟服务发布，同时域名均要求做SSL卸载的应用场景。需要提供界面相关证明材料。 |
| 负载均衡算法 | 支持轮询、加权轮询、最小连接数、加权最小连接数、源ip哈希、源ip+端口哈希、动态就近性、动态反馈、最快响应、最小带宽、最小流量、最小延时、最小抖动、最小丢包率等算法。需要提供界面相关证明材料 |
|  | 通过TCP丢包预测，快速重传和恢复机制，提高TCP协议的数据传输速度，当广域网链路出现延时和丢包的情况时，可明显改变TCP传输效率，提升传输速率不用在用户终端上安装任何插件和软件，即可提升链路访问速度，节省带宽资源。 |
| 支持智能DNS功能，实现链路智能Inbound访问，避免跨运营商访问。 |
| 根据用户实时访问情况，动态探测每条链路到用户访问服务的的目标可达性，及延迟信息；并计算出最佳访问链路。并且随着链路质量的变化，可自动调整重新选择最佳发送链路。 |
| 支持基于链路负荷情况的拥塞控制功能，能够根据链路的上行/下行带宽占用率情况执行对出站/入站流量的高级调度策略。 |
| 支持基于URL的流量调度功能，可设定访问特定的URL选择指定的线路转发，且内置国外URL地址库。 |
| 服务器负载均衡 | 支持基于ICMP、TCP、UDP、FTP、HTTP、HTTPS、LDAP、POP3、Radius、SMTP、SNMP，ORACLE，MSSQL，MYSQL等协议的服务器健康检查。 |
| 支持配置每台服务器最大连接限制和新建连接限制，以及单个特定用户或者一个用户组中所有用户访问指定应用服务的最大连接限制、新建速率限制，以及所发布应用的上下行带宽限制、单个用户访问应用的上下行带宽限制，避免应用系统的服务器过载。需要提供界面相关证明材料 |
| 支持用户自定义方式的健康检查，用户可根据节点运行的实际业务流程来编写代码，检查业务处理逻辑是否正常。 |
| 全局负载 | 支持地域优先、静态就近性、动态就近性、最小连接数、最小流量、最小带宽等全局负载均衡算法。 |
| IPV6改造 | 支持IPV6/V4双栈同时工作。 |
| 支持NAT66、NAT64、NAT46翻译技术。 |
| 支持DNS64。 |
| 支持基于IPV6地址的 HTTP内容负载，可基于HOST、 URL、Cookie、User-Agent的负载分担。 |
| 网络特性 | 支持RIP，OSPFv2/v3、BGP动态路由协议。 |
| 支持且提供设备虚拟化功能：一台物理设备可以虚拟出多台设备使用；各虚拟设备间完全隔离，分别具有独立的管理员及配置，可运行相同或不同的业务。 支持虚拟设备CPU，内存，网络I/O等计算资源按需分配，支持VLan Tag 及接口的虚拟网络隔离。 |
| 界面及运维管理 | 支持全中文的管理界面和HTTPS方式登录。 |
| 支持角色管理、多级授权管理。 |
| 支持管理员ACS认证，支持主备ACS认证服务器。提供页面截图 |
| 支持SNMP V1/V2/V3协议。 |
| 支持标准SYSLOG格式日志信息，可以根据预置条件自动把日志信息发送给远端服务器。 |
| 支持统计虚拟服务和真实服务器的流量、访问次数、并发连接数。 |
| 支持自动或手动生成HTML和PDF两种格式报表。 |
| 产品资质 | 必须提供产品通过IPv6 Ready Logo Certified证书（提供证明文件）必须提供国家版权局颁发的软件著作权登记证（提供证明文件）必须提供计算机信息系统安全专用产品销售许可证（提供证明文件） |

### 原信息中心安全设备升级

#### 日志审计设备(信息中心)

|  |  |
| --- | --- |
| 指标项 | 指标性能 |
| 性能 | 事件处理性能最高10000EPS。硬件规格：标准2U机箱，4个千兆电口，1块RAID卡，2个扩展插槽（可选2万兆光、4千兆电、4千兆光），冗余电源，8TB\*3块硬盘，使用RIAD5数据保护。包含500授权节点，包含三年硬件标准维保，三年软件升级服务。 |
| 用户使用模式 | 界面100%都是B/S模式，无需安装客户端，使用IE浏览器访问管理中心，浏览器端无需安装Java运行环境。 |
| 管理范围 | 能够对企业和组织的IT资源中构成业务信息系统的各种网络设备、安全设备、安全系统、主机操作系统、数据库以及各种应用系统的日志、事件、告警等安全信息进行全面的审计。 |
| 日志审计对象 | 支持对各类网络设备（路由器，交换机）、安全设备（包括防火墙，VPN，IDS，IPS，防病毒网关，网闸，防DDOS攻击，Web应用防火墙）、安全系统（Symantec、瑞星、江民、微软ISA、Windows防火墙）、主机操作系统（包括Windows,Solaris, Linux, AIX, HP-UX,UNIX,AS400）、各种数据库（Oracle、Sqlserver、Mysql、DB2、Sybase、Informix）、各种应用系统（邮件，Web，FTP，Telnet），网管系统告警日志、终端管理系统（或是内网管理系统、桌面管理系统）告警日志，网络综合审计系统告警日志，上网行为审计系统日志，以及用户自己的业务系统的日志、事件、告警等安全信息进行全面的审计。 |
| 日志采集方式 | 可通过syslog、snmp trap、netflow、netscreem、jdbc、odbc、opensec lea、agent代理、wmi等多种方式完成各种日志的收集功能。对windows服务器（系统、应用和安全）日志和文件类型日志，可免日志代理或插件；支持用户环境中EVT格式的业务系统日志采集。对于保存在日志文件和数据库中的日志使用agent采集方便，无需定制开发采集。 |
| 资产管理 | 按照设备资产重要程度和管理域的方式组织设备资产，提供便捷的添加、修改、删除、查询与统计功能，支持资产信息的批量导入和导出，便于安全管理和系统管理人员能方便地查找所需设备资产的信息，并对资产进行关键度赋值。针对资产可以设置允许接收和拒绝接收日志，在资产日志中显示最近一条日志的接收时间，并可以对资产设置一定时间范围内未收到事件后进行主动告警；可以限定资产的管理员（可以设置为多个），该资产日志只允许所添加管理员查看和审计。 |
| 日志归一化处理 | 日志收集后进行字段和安全等级的归一化处理，系统归一化字段至少应有50个,并至少有5个可自定义字段,收集并归一化后的日志需保留原始日志，方便用户对关键日志快速定位。系统应提供灵活简单的归一化方式,对系统默认不支持的日志只需修改配置文件即可支持,不需修改系统程序。系统具备一种大规模事件处理的规则群组系统及处理方法技术，为避免虚假应标，投标时要求提供国家知识产权局出具的相关证明文件复印件或检测报告。 |
| 日志审计查询 | 所有日志采用统一的日志查询界面，用户可以自定义各种查询场景，并以树形结构组织。查询场景可保存，并可支持在查询结果中继续查询。系统内置针对windows服务器的各类应用、系统、安全事件的查询场景，查询结果与windows事件查看器显示字段一致。支持原始消息中的关键字查询，可进行全文检索，可显示查询记录总数，当前查询耗时，可对查询结果进行分组排序，可对查询结果跳转到指定页数。查询结果可导出。在查询过程中用户转入其他页面时，可以提示用户继续等待或结束当前查询。在查询结果中可以选择跳转到指定页数、可以对查询结果任意字段进行排序。 |
| 日志实时监视 | 系统提供实时的日志滚动显示和查询，可自定义实时监视的日志内容，可查看实时日志详细信息，可通过雷达图等直观显示目前日志量，可以控制日志对管理员账号的可见性管理。 |
| 日志实时分析和统计 | 可对收集的日志进行分类实时分析和统计，从而快速识别安全事故。分析统计结果支持柱图、饼图、曲线图等形式并自动实时刷新，图表数据支持数据下钻。日志实时分析在内存中完成，不需借助数据库和文件系统。 |
| 日志处理 | 为了满足在大数据环境下对日志进行高速地采集和处理，要求拥有高性能的syslog日志处理和存储方法技术，以便于设备达到最佳日志处理性能，为避免虚假应标，投标时要求提供国家知识产权局出具的相关证明文件复印件。 |
| 事件可视化展现 | 支持通过世界地图定位IP地址，通过事件攻击图展示网络安全态势，通过行为分析图展示一段时间内的用户访问行为。（要求提供配置界面相关证明材料） |
| 日志在线挖掘 | 系统具备事件挖掘能力可通过事件调查工具可以对某条感兴趣的日志中的源IP地址、目的IP地址、或者目的端口进行相关性日志检索。 |
| 事件分配 | 用户在实时监视的过程中如果发现某条事件的相关属性需要持续予以关注，可以将该事件分配到黑白名单中。 |
| 趋势分析 | 可对收集的日志根据过滤条件，针对设备地址、源地址、目标地址等进行事件数量、流量等的趋势分析。 |
| 事件追溯 | 对于关联告警事件，用户可以进行追溯，查看导致该关联事件的所有原始事件。 |
| 事件定位 | 能够在世界地图上实时定位事件源/目的IP地址的地理位 |
| 日志关联分析告警 | 系统应至少默认有50条告警规则，系统提供可视化规则编辑器，对告警规则进行增删改查。系统内置针对服务器和其他安全设备的访问ip地址、访问账户和访问时间的访问控制规则；告警规则可按照树型结构组织，并可在该树型结构上直接查看该规则的告警信息，对告警日志可按各告警字段进行分组排序。可对不同类型设备的日志之间进行关联分析，支持递归关联，统计关联，时序关联，这几种关联方式能同时应用于一个关联分析规则。 |
| 告警和响应管理 | 通过关联分析，对于发现的严重事件可以进行自动告警。告警方式包括邮件、短信、SNMP Trap、Syslog、MSN、飞鸽传书等。响应方式包括：自动执行预定义脚本，自动将事件属性作为参数传递给特定命令行程序。此外，还支持设备联动，即可以在告警后对防火墙/NIDS/网络设备下发联动策略，及时阻断威胁。 |
| 告警查询 | 支持显示所有和按规则树结果分别显示告警事件信息，对告警查询结果字段可以分别二次排序显示。 |
| 报表管理 | 提供丰富的报表管理功能，预定义了针对各类服务器、网络设备、防火墙、入侵检测系统、防病毒系统、终端安全管理系统、数据库、策略变更、流量，设备事件趋势以及总体报表，满足等保等其他合规性要求；根据时间、数据类型等生成报表，提供打印、导出以及邮件送达等服务；直观地为管理员提供决策和分析的数据基础，帮助管理员掌握网络及业务系统的状况。报表可以保存为html，excel，文本，pdf等多种格式。提供自定义报表，用户可根据自身需要进行定制。报表可根据设置自动运行,调度生成日报、周报和月报。 |
| 备份归档 | 支持按日志属性（原始日志、重要日志、告警日志）、日志类型、存储周期的方式选择备份，支持原始日志与分析后日志分离。支持数据库备份；支持历史日志恢复导入；支持各种配置项的备份和导入。支持各种配置项的一键备份和恢复；当磁盘空间日志存储量达到一定百分比时可设定为删除磁盘中的历史日志或接收的日志不再入库，并进行告警；手动备份和恢复时，可以显示恢复和备份的进度。 |
| 权限管理 | 采用基于角色的权限管理机制，通过角色定义支持多用户访问。角色能够从设备和功能两个维度进行定义，从而达到控制谁可以对什么设备进行什么操作的控制粒度；支持禁止与允许用户访问日志审计系统的IP地址限制。支持限定管理员只允许查看自己所负责设备的日志； |
| 系统自身监控 | 系统自身的健康状况监控。包括CPU、内存、磁盘的利用率。可以对所有注册了的通用日志采集器的工作状态进行实时监控，包括采集器的启动、停止，以及配置采集器发送什么类型的日志到管理中心。 |
| 系统自身日志审计 | 用户对本软件系统的操作都记录日志并进行持久化存储，便于追踪、审核和告警。系统日志格式的属性包括：时间、源IP、用户名、操作类型、操作说明、操作结果（成功/失败）。 |
| 系统认证 | 支持用户名密码认证方式，认证时需要提供验证码；支持USB key双因子身份认证方式。支持动态口令认证。 |
| 系统自身安全 | 产品内部的各个组件之间通信都支持加密传输，浏览器访问管理中心支持HTTPS，多级管理中心之间采用加密协议进行传输。 |
| 数据安全 | 对采集到的日志都进行了加密存储，保证数据的完整性 |
| IPv6网络支持 | 系统支持IPv6网络环境。 |

#### 防火墙（一级网）

|  |  |
| --- | --- |
| **指标项** | **指标参数** |
| 系统架构 | 为了确保网络数据能够极速稳定转发，系统采用多核架构，硬件设计采用高性能一体化智能安全处理引擎，要求提供计算机软件著作登记证书。 |
| 流量镜像功能 | 提供网络端口的流量镜像功能，实现将防火墙经过的全流量数据镜像提供给第三方设备使用。 |
| 性能规格 | 多核AMP+架构，网络层吞吐量60G，并发连接≥1000万，每秒新建连接数60万，标准2U机箱，冗余电源， 标准配置1个Console口 、1个HA接口，1个MGT接口，4口万兆多模SFP板卡，支持2对硬件bypass；4口千兆多模SFP板卡，支持2对硬件bypass；8千兆电口板卡；另有1个接口板卡扩展插槽，支持液晶屏，含三年硬件维保服务。三年IPS和三年AV特征库升级。 |
| 基础组网和网络适应能力 | 产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求。支持旁路模式； |
| 支持支持通过802.3ad协议、轮询、热备等方式将多个物理口绑定为一个逻辑接口，实现接口级的冗余。 |
| 所投产品必须支持全面的NAT转换配置，包括包括一对一，一对多，多对一的源、目的地址转换 |
| 支持DNS透明代理 |
| 支持双机热备和双机负载均衡功能。支持标准VRRP协议，支持路由、透明模式下“主-备”、“主-主”方式部署，设备支持一种多防火墙的负载均衡方法及装置的技术，提供相关证明文件。 |
| 支持基于权重的路由负载均衡，算法支持：源地址目的地址哈希、轮询、源地址哈希、目的地址哈希、源地址轮询、备份、随机、流量均衡、最优链路带宽负载、最优链路带宽备份、时延负载、跳数负载 |
| 支持静态路由，支持策略路由，支持对称路由；支持ISP路由，并支持手动导入；支持动态路由协议RIPv1/v2、OSPF、BGP |
| 要求防火墙支持IPSEC VPN、SSL VPN、PPTP功能。IPSec VPN隧道≥500 |
| 所投产品可直观展示不同风险等级的应用在1天（24小时）或一周（7天）内传输流量的绝对数值及占全网流量的百分比。 |
| 支持IPv6地址配置，支持IPV6手动及自动的IP/MAC探测及绑定，支持IPV6的本地认证；支持IPV6下静态路由及策略路由 |
| 访问控制功能 | 支持基于源目的IP地址、源目的安全域、VLAN ID、MAC地址、时间、用户、地理区域、服务协议及应用等多种方式进行访问控制； |
| 支持一条访问控制策略同时对端口和协议进行管控。 |
| 支持通过一条安全策略配置应用控制、入侵防护、URL过滤、病毒检测、内容过滤、网络行为管理等高级访问控制功能，且无需编辑即可直观审计策略配置。支持一种基于用户的安全访问控制的方法，提供相关文件。 |
| 能实现对rdp、ssh、telnet、vnc、pcanywhere等各类远程访问控制协议的识别和阻断，要求支持的远程访问控制协议种类在35种以上，。并支持对特定IP的开启例外功能。能实现对主要种类数据库协议的识别和阻断，要求支持的协议种类超过9种，。并支持对特定IP的开启例外功能。 |
| 标准SNMP协议支持 | 要求提供标准SNMP协议支持，允许第三方网管软件对防火墙的CPU、内存、网络流量等性能、可用性等进行监测。 |
| 病毒防护 | 提供病毒查杀和防护功能模块，能够HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀；支持对压缩文件进行解压查杀； |
| 支持基于MD5的自定义病毒签名；支持设置例外特征，对特定的病毒特征不进行查杀 |
| 病毒库不少于600万种病毒特征，支持病毒库扩充，支持添加特定病毒种类特征。支持病毒云查杀功能。要求提供病毒库来源和名称病毒库，建议以目前国内流行病毒为主。 |
| 应用识别和行为管理 | 所投产品必须支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于2800种，可深度识别每种应用的属性，为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输方式等特征分类。 |
| 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。 |
| 入侵防御 | IPS特征库不少于3000条特征值。 |
| 所投产品的漏洞防护特征库包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云3”、“Struts”、“Xshell后门代码”以及对应的攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息； |
| 支持对拒绝服务、缓冲区溢出、恶意扫描、木马后门、病毒蠕虫、僵尸网络、跨站脚本、SQL注入、WEB攻击等的防御，具备针对DNS、FTP、ICMP、IMAP、SQL、NNTP、POP、SMTP、SNMP等协议类型的入侵检测与防御。 |
| 支持对应用层 Flood攻击进行五种处理动作：警告、阻断、普通防护、增强防护及授权服务器防护；支持局域网广播防护，支持全局配置的局域网广播防护及基于二层接口的局域网广播防护，可以防止局域网内广播和多播数据包泛滥，保障网络正常通信。 |
| 支持基于防护类型及防护级别的预定义IPS模板；基于行业类型特点的预定义URL模板。 |
| 内容过滤 | 实现HTTP、FTP、POP3、SMTP、IMAP五种应用协议的双向内容过滤，支持预定义敏感信息库及自定义敏感信息库两种方式进行敏感信息定义，支持阻断及日志两种处理动作； |
| 安全事件分析和异常感知 | 支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破、存在安全风险的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机IP、用户名、资产等信息 |
| 所投设备必须提供关联分析面板，可将Top应用、Top威胁、Top URL分类、Top源地址、Top目的地址等信息关联，并支持以任意元素为过滤条件进行数据钻取  |
| 支持基于网络活动，威胁活动、阻止活动等多维关联统计及分析，发现异常行为  |
| 所投设备提供关联的威胁事件日志，系统可自动将产生威胁事件的连接经过防病毒、防漏洞、防间谍软件、URL过滤、文件过滤等安全模块检查的日志集中显示 |
| 策略与处置 | 所投设备可在单条策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能选项，支持一种安全网关中进行安全策略统一处理的方法，提供相关证明文件。 |
| 所投产品支持基于受害主机的一键式阻断链接、记录日志等处置动作，处置周期至少包括1天、7天、30天、90天、永久等； |
| 所投产品支持接收针对突发重大安全事件的“应急响应消息”，并至少在界面显示安全事件名称、类型、当前防护状态、处置状态以及相应的操作等信息；并可根据设备安全配置的变化动态显示应急响应的处理结果 |
| 运维管理 | 所投产品支持双系统备份，且在系统切换中可实现配置的自动迁移；可记录不同时间点的历史配置文件 |
| 所投产品必须支持加密的WebUI和CLI管理，且支持网页命令行管理（WebUI中内嵌CLI管理界面） |
| 所投产品支持将告警信息以SNMP Trap、邮件、声音、短信等形式通知管理员，告警信息的范围至少包括配置变更、病毒事件、攻击事件、异常事件、CPU利用率、内存利用率、硬盘利用率、接口带宽利用率等； |
| 终端安全软件联动 | 所投产品支持与桌面杀毒或终端管理软件联动，实现基于终端健康状态的访问控制；增强防火墙对木马特征的识别能力 |
| 用户登陆认证 | 支持基于web的无客户端方式用户登陆认证；管理页面登陆支持客户端IP地址限定。 |
| 产品要求 | 所投产品具备公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》（万兆三级），或防火墙（万兆增强级）销售许可证。 |
| 要求防火墙产品支持IPv6 |

#### 负载均衡（PKI系统）

| **指标项** | **规格要求** |
| --- | --- |
| 硬件规格 | 标准2U设备，千兆电口≥6个，万兆光口≥2个，双电源；硬盘≥240G SSD. |
| 性能要求 | 四层吞吐≥30G，最大并发连接数≥1200万，4层每秒新建连接数（CPS）≥50万/秒，7层每秒新建连接数(RPS)≥60万/秒。 |
| 部署模式 | 支持路由、旁路部署，以及三角传输 |
| 高可用性 | 支持主主（AA）、主备（AS）工作模式，IP地址可在设备间漂移，根据设备状态将流量牵引到主设备。支持包括半连接，全连接会话信息全状态同步；支持会话保持信息同步；以保障业务不间断切换。 |
| 支持浮动MAC，HA切换过程MAC地址不变。 |
| 支持基于心跳信号丢失、链路断开、远端服务不可达等多种方式的HA切换条件及逻辑。 |
| 支持标准VRRP协议。需要提供界面相关证明材料， |
| 集群部署：可以实现两台以上设备集群部署，多台设备同时负载一台设备在线备份。 |
| 应用系统加速 | 支持一个虚拟服务，可选择多个SSL证书，适用于多个域名共用一个虚拟服务发布，同时域名均要求做SSL卸载的应用场景。需要提供界面证明材料。 |
| 负载均衡算法 | 支持轮询、加权轮询、最小连接数、加权最小连接数、源ip哈希、源ip+端口哈希、动态就近性、动态反馈、最快响应、最小带宽、最小流量、最小延时、最小抖动、最小丢包率等算法。需要提供界面证明材料 |
|  | 通过TCP丢包预测，快速重传和恢复机制，提高TCP协议的数据传输速度，当广域网链路出现延时和丢包的情况时，可明显改变TCP传输效率，提升传输速率不用在用户终端上安装任何插件和软件，即可提升链路访问速度，节省带宽资源。 |
| 支持智能DNS功能，实现链路智能Inbound访问，避免跨运营商访问。 |
| 根据用户实时访问情况，动态探测每条链路到用户访问服务的的目标可达性，及延迟信息；并计算出最佳访问链路。并且随着链路质量的变化，可自动调整重新选择最佳发送链路。 |
| 支持基于链路负荷情况的拥塞控制功能，能够根据链路的上行/下行带宽占用率情况执行对出站/入站流量的高级调度策略。 |
| 支持基于URL的流量调度功能，可设定访问特定的URL选择指定的线路转发，且内置国外URL地址库。 |
| 服务器负载均衡 | 支持基于ICMP、TCP、UDP、FTP、HTTP、HTTPS、LDAP、POP3、Radius、SMTP、SNMP，ORACLE，MSSQL，MYSQL等协议的服务器健康检查。 |
| 支持配置每台服务器最大连接限制和新建连接限制，以及单个特定用户或者一个用户组中所有用户访问指定应用服务的最大连接限制、新建速率限制，以及所发布应用的上下行带宽限制、单个用户访问应用的上下行带宽限制，避免应用系统的服务器过载。需要提供界面相关证明材料 |
| 支持用户自定义方式的健康检查，用户可根据节点运行的实际业务流程来编写代码，检查业务处理逻辑是否正常。 |
| 全局负载 | 支持地域优先、静态就近性、动态就近性、最小连接数、最小流量、最小带宽等全局负载均衡算法。 |
| IPV6改造 | 支持IPV6/V4双栈同时工作。 |
| 支持NAT66、NAT64、NAT46翻译技术。 |
| 支持DNS64。 |
| 支持基于IPV6地址的 HTTP内容负载，可基于HOST、 URL、Cookie、User-Agent的负载分担。 |
| 网络特性 | 支持RIP，OSPFv2/v3、BGP动态路由协议。 |
| 支持且提供设备虚拟化功能：一台物理设备可以虚拟出多台设备使用；各虚拟设备间完全隔离，分别具有独立的管理员及配置，可运行相同或不同的业务。 支持虚拟设备CPU，内存，网络I/O等计算资源按需分配，支持VLan Tag 及接口的虚拟网络隔离。 |
| 界面及运维管理 | 支持全中文的管理界面和HTTPS方式登录。 |
| 支持角色管理、多级授权管理。 |
| 支持管理员ACS认证，支持主备ACS认证服务器。提供页面截图 |
| 支持SNMP V1/V2/V3协议。 |
| 支持标准SYSLOG格式日志信息，可以根据预置条件自动把日志信息发送给远端服务器。 |
| 支持统计虚拟服务和真实服务器的流量、访问次数、并发连接数。 |
| 支持自动或手动生成HTML和PDF两种格式报表。 |
| 产品资质 | 必须提供产品通过IPv6 Ready Logo Certified证书（提供证明文件）必须提供国家版权局颁发的软件著作权登记证（提供证明文件）必须提供计算机信息系统安全专用产品销售许可证（提供证明文件） |

### 数据交换通道

#### 防火墙1

|  |  |
| --- | --- |
| 指标项 | 指标参数 |
| 性能 | 采用多核架构，1U机架式设备，千兆电口14个，千兆光口8个，万兆光口8个（配置2个万兆单模光模块）。 |
| 吞吐量20Gbps；并发连接数1000万，每秒新建连接数（HTTP）15万 |
| 功能 | 支持路由、透明、混合模式部署，支持U盘零配置上线； |
| 支持基于AI的策略冗余分析、策略命中分析以及应用风险调优等能力； |
| 支持WEB安全防护、资产扫描、加密流量检测与控制、应用审计、数据安全、网页过滤、带宽管理、IPS、AV等应用层安全功能； |
| 支持链路负载； |
| 支持SSL VPN \IPSEC VPN等多种VPN功能； |
| 支持国密算法，支持IPV6协议； |

#### 防火墙2

|  |  |
| --- | --- |
| 指标项 | 指标参数 |
| 性能 | 采用多核架构，CPU物理核心数：8，内存16G，硬盘配置：64G SSD，2U机架式设备，8个千兆电口，4个千兆光口，4个万兆光口，2个扩展槽位，双交流电源。 |
| 吞吐量40Gbps；并发连接数1000万，每秒新建连接数（HTTP）18万。 |
| 功能 | 支持路由、透明、混合模式部署，支持U盘零配置上线； |
| 支持基于AI的策略冗余分析、策略命中分析以及应用风险调优等能力； |
| 支持WEB安全防护、资产扫描、加密流量检测与控制、应用审计、数据安全、网页过滤、带宽管理、IPS、AV等应用层安全功能； |
| 支持链路负载； |
| 支持SSL VPN \IPSEC VPN等多种VPN功能； |
| 支持国密算法，支持IPV6协议； |

#### 集控探针

|  |  |
| --- | --- |
| 指标项 | 指标参数 |
| 性能 | 安全专用操作系统，网络接口≥6个10/100M/1000M电口 |
| 功能 | 支持采集多种设备的运行状态信息； |
| 支持对多种设备的流量信息采集； |
| 支持SYSLOG协议； |
| 支持SNMP v2/SNMP v3协议。 |

#### 设备准入控制系统

|  |  |
| --- | --- |
| 指标项 | 指标参数 |
| 性能 | 6个1000MBASE-T接口，2个万兆光口。每秒事务数（TPS)：22000（次/秒），最大吞吐量：4Gbps |
| 功能 | 准入设备应提供客户端的准入模式和无客户端准入模式，可供自定义部署和管理； |
| 支持基于802.1x的网络准入方式，包括有线环境802.1x与无线环境802.1x，准入设备支持VLAN隔离技术，实现无客户端下端口级准入控制；（提供功能证明材料） |
| 能够通过SNMP、SSH、TELNET等方式自动、批量添加网络设备； |
| 准入设备支持交换机到终端计算机的网络拓扑管理功能，能够自动绘制出网络拓扑图； |
| 支持NAT设备发现、告警、阻断，并可以针对NAT设备下接终端进行准入控制； |
| 支持数字证书认证方式，必须支持证书的本地管理和发放，实现证书签发、管理和操作。 |

#### 数据交换节点

|  |  |
| --- | --- |
| 指标项 | 指标参数 |
| 性能 | 交换能力：4Gbps；最大支持服务个数：60；最大传输延时：＜10ms。 |
| 功能 | 支持内外网多个数据交换节点组件形成集群部署，可实现组件热插拔式动态扩容和删减，以及实现接入业务的负载均衡及冗余热备。 |
| 支持与管控中心组件无缝对接，接受管控中心的统一管控，实现交换节点设备的注册、修改、删除等功能。支持与管控中心组件之间的身份认证机制。通过IP/MAC、数字证书等方式，实现与管控中心之间的双向身份认证； |
| 支持与Ka\*\*a集群直接对接部署，实现Ka\*\*a消息队列数据跨网交换，满足海量小文件跨网高性能交换需求； |
| 支持共享、客户端、FTP、NFS等多种模式的文件交换服务。 |
| 支持通过解析数据库日志文件的技术原理，在不同类型的数据库之间进行数据同步。无需在数据库中创建触发器、存储过程、临时表等对象，实现低干扰的数据采集； |
| 数据库同步过程中，支持把交互数据落地为私有格式文件进行落地交换，保障数据库交互的安全性； |
| 支持各种数据之间的异构交换，如：Oracle-ODPS；MySQL-ODPS等数据库种类异构、Ka\*\*a-DATAHUB同步。（提供公安厅出具的相关功能测试报告） |
| 支持平面文件与数据库之间的互相转换； |
| 具备多种抗恶意数据攻击能力，如：exe文件过滤、exe文件后缀伪装、图片文件夹带恶意代码、jpg文件捆绑可执行程序、恶意代码穿透等；（要求提供国家权威机构证明材料） |
| 支持IPv4/IPv6双协议栈网络环境； |
| 支持云环境下的数据安全交换，适用于云环境内部不同VPC之间的数据安全交换及不同云环境之间的数据安全交换； |
| 支持数据交换全流程审计，如：数据来源、交换开始时间、交换结束时间、数据大小、数据类型、交换方向、交换结果等。保证数据交换行为可追溯； |
| 支持一键检测功能，可以对系统硬件资源、操作系统、核心进程、业务运行状态等进行分项快速检测，协助管理员快速定位故障； |
| 支持多隔离设备容错，当一台隔离设备出现故障，系统会自动选择无故障的隔离设备继续运行，不影响数据的正常交换；  |
| 支持多套系统集群部署，当多套系统都运行正常时，多套系统之间可以实现负载均衡；当某套系统故障时，业务会自动切换到其他正常系统中继续运行；系统内置负载均衡模块，不需要第三方软硬件设备即可实现多套系统间的负载均衡； |
| 支持服务水平分析，对文件服务器、数据库服务器的服务水平进行详细分析； |
| 产品不存在漏洞库中已知的中、高风险漏洞。（要求提供国家权威机构证明材料） |

#### 数据交换接口机

|  |  |
| --- | --- |
| 指标项 | 指标参数 |
| 性能 | 4个10/100/1000Mbase-TX；4个万兆口（含万兆光模块），支持扩展插槽； |
| 数据摄取速度不小于10000条/秒； |
| 最快服务响应延时：1ms； |
| 单个节点最大并发请求不小于500； |
| 单个节点无错率≥99%；（500个并发请求下） |
| 稳定性运行时间(MTBF)>50000小时 |
| 功能 | 多数据容器支持：支持各关系型数（Oracle、MySQL、Postgres、DB2、SQL Server等）、MPP数据库（Gbase、Greenplum、infomix、达梦等）、Hadoop、Mangodb、Hbase、全文库等。 |
| 分布式集群架构，基于主题的发布订阅、广播、组播、点到点方式均支持；支持同步、异步方式； |
| 访问控制：黑白名单，支持对特定IP地址的黑、白名单的设置 |
| 访问控制：访问频率，支持对每个服务的访问频率，按每小时、每天、每周、每月设置 |
| 策略控制：提供熔断机制，支持超出最大请求次数时，自动触发熔断机制；限流机制，支持基于请求限流和基于资源限流机制；排队机制，支持超出最大请求次数时，自动触发排队机制； |
| 安全机制：红名单管理，支持用户级红名单；证书管理，支持系统自生成的SSL证书和其他厂商上传的证书的管理 |
| 敏感数据机制；基于机器学习,更加智能的数据脱敏，支持包括身份证和电话号码的敏感数据的脱敏 |
| 提供服务资源目录、服务注册、服务路由、日志审计、接入适配、访问控制等传统ESB总线功能。 |

#### 数据传输节点

|  |  |
| --- | --- |
| 指标项 | 指标参数 |
| 性能 | 内外网接口各标配6个100/1000M Base-TX网络接口，2个10000M 光口。具有两个独立主机，独立主机之间，仅使用单个无源分光器进行单纤连接，不存在反方向的物理通道。（提供相关证明材料） |
| 功能 | 系统要求：内、外网主机系统分别采用冗余双系统启动模式，当A系统运行失败后，能从B系统启动，且A、B系统可互为备份；（提供产品功能界面） |
| 能够事先定义任务的过滤规则，并根据过滤规则对数据进行严格的格式检查和过滤； |
| 根据系统管理员配置任务规则进行单向传输，对数据内容进行深层次细粒度的过滤检查，可对内容过滤，可对大字段内容检查。内建杀毒引擎查杀病毒。 |
| 支持包过滤功能：含IP、内容范围、包内容、包大小等； |
| 支持两端KA\*\*A的业务环境对接。 |
| 支持共享、客户端、FTP、NFS等多种模式的文件交换服务。 |
| 具有灵活的文件交换冲突选项，支持重名策略：覆盖、放弃、重命名； |
| 支持数据库的单向导入：要求支持ORACLE、SQLSERVER、SYBASE、DB2、Mysql、神州通用(oscar)、达梦、南大通用等多种数据库类型数据库的单向导入；（提供功能相关证明材料） |
| 支持文件名、关键字、文件格式白名单过滤，深度识别PE可执行文件。 |
| 支持不同类型数据库之间及异构数据库的数据类型转换（表名、表字段、表字段类型、表主键、表外部键不同）；支持BLOB、CLOB、LONG、TEXT、IMAGE等大字段的异构，支持不同字符集的异构。 |
| 支持传输流量分析和流量控制功能，（提供功能相关证明材料）流量分析提供分析结果值，支持下一代网络协议IPV6网络环境。（提供IPv6认证证书） |
| 支持断点重传功能，在出现断电或传输中断等情况下，能够保证系统恢复时，交换的数据能重传或续传且不出数据丢失现象。 |
| 支持全文审计功能，能够追溯历史传输数据。 |
| 采用具有人性化的B/S管理界面，非信任端与信任端分开管理，管理口与业务口分离，增加配置信息的抗干扰能力。 |
| 能与集中监控与管理系统无缝对接，支持将审计信息或报警信息发送到集中监控系统统一管理。 |
| 数据传输过程采用数据完整性校验机制，保证数据的有效性、正确性、完整性。 |

#### 数据交换管控节点

|  |  |
| --- | --- |
| 指标项 | 指标参数 |
| 性能 | 配置4个100/1000M Base-TX网口 |
| 功能 | 通过管控中心对所有节点设备进行统一管理，具备节点增、删、改、查；软件升级等功能。 |
| 对节点设备的运行状态信息进行自动感知，统一监控各节点业务运行状态。 |
| 对所有业务进行统一配置管理，通过负载算法来掌握不同节点的负载情况，把配置的业务自动分配到不同的节点，对所有节点进行统一调度，智能负载；可以实现交换节点非对称部署，单一节点故障及时切换保障业务的稳定性。 |
| 数据交换安全管控中心业务配置区域可以通过模糊查询检索某服务，以服务端口、IP、服务名称等进行检索。 |
| 为了保障业务配置的稳定性，数据交换安全管控中心两套可以热备部署。 |
| 各个节点设备及业务发生异常时，及时报警；对交换记录进行详细审计；对所有审计日志进行统一查询和展示。 |

#### 可信应用数据检控节点

|  |  |
| --- | --- |
| 指标项 | 指标参数 |
| 性能 | 4个10/100/1000MBase-T电口，2个万兆光口。 |
| 功能 | 可信应用/数据检控提供零信任的业务应用与数据交互的检控能力，需依据用户访问、数据交换模式选择对应的支撑能力， |
| 加密流量解密 | 在安全访问模式，应提供SSL/TLS加密流量解密能力，实现安全检测； |
| 检查与控制 | 令牌检查与控制：提供用户令牌、应用令牌检查能力，支持令牌格式、签名、内容、有效期的安全检查，根据检查结果阻断或放行； |
| 协议格式检查与控制：在安全访问模式，提供请求和响应报文头、报文体的格式检查能力，支持HTTP、WebSocket等应用层协议检查能力；在数据交换模式，提供数据库协议、文件传输协议的检查能力，根据检查结果阻断或放行； |
| 业务应用访问权限检查与控制：在安全访问模式，提供业务应用对应用服务/数据服务访问检查能力，可提供应用API访问指定信息的检查能力，根据检查结果阻断或放行； |
| 数据交换内容检查与控制：在数据交换模式，可提供文件、数据等检控能力，支持对指定信息的检查能力，依据检查结果进行阻断或放行； |
| 验证签名 | 数据交换模式支持数据验证签名能力，对数据标签、事件标签中签名的有效值进行检查，依据检查结果进行阻断或放行； |
| 日志记录和报送 | 提供业务应用访问/数据交换的日志、检控告警记录及上报能力。 |
| 资质 | 设备厂商具有销售许可证 |

#### 集中监控管理系统

|  |  |
| --- | --- |
| 指标项 | 指标参数 |
| 性能 | 4个10/100M/1000M电口；数据库容量：1TB；最大支持业务数量：1000；最大监控并发用户数量：5000； |
| 功能 | 支持对多种设备的监测、审计与集中管理。 |
| 能够以拓扑图的形式直观实时展示单向导入、安全数据交换接入链路设备当前的运行状况。 |
| 支持根据不同接入对象的信息注册，管理接入设备及业务。 |
| 能够实时收集各种设备发送给集控系统的异常事件（如病毒、木马、未授权访问、流量超过阀值等），并提供短信报警接口，能将设备、业务报警信息以短信的方式通知给运维人员，并可自定义短信报警内容。 |
| 支持自制网络拓扑图，支持监控设备图形化拖拽，直观显示网络情况。 |
| 支持报表、图形等多种展示方式，为决策分析提供支撑。 |
| 产品不存在漏洞库中已知的中、高风险漏洞。（要求提供国家权威机构证明材料） |

#### 交换机1

|  |  |
| --- | --- |
| 指标项 | 指标参数 |
| 性能 | 交换容量2.56Tbps，包转发率720Mpps，以上指标以官网最小值为准；万兆光口24个（满配万兆多模光模块），40G QSFP+端口2个，业务插槽2个，冗余250W交流电源，冗余风扇； |
| 功能 | 支持横向虚拟化，纵向虚拟化； |
| 支持VxLAN，支持IPv4/IPv6； |
| 支持Macsec硬件级加密技术； |
| 支持Netstream可视化技术 |
| 支持多虚一技术，支持BFD/BGP/IS-IS/OSPF/RIP/静态路由； |
| 为保障接入层安全，支持安全业务插卡，支持FW、IPS、ACG、LB、SSL VPN等功能，以满足后续控制、管理的要求 |

#### 交换机2

|  |  |
| --- | --- |
| 指标项 | 指标参数 |
| 性能 | 交换容量2.56Tbps，包转发率720Mpps，以上指标以官网最小值为准；万兆光口24个（配置12个万兆多模光模块），5G/2.5G/1G自适应电口8个，40G QSFP+端口2个，业务插槽2个，冗余250W交流电源，冗余风扇； |
| 功能 | 支持横向虚拟化，纵向虚拟化； |
| 支持VxLAN，支持IPv4/IPv6； |
| 支持Macsec硬件级加密技术； |
| 支持Netstream可视化技术 |
| 支持多虚一技术，支持BFD/BGP/IS-IS/OSPF/RIP/静态路由； |
| 为保障接入层安全，支持安全业务插卡，支持FW、IPS、ACG、LB、SSL VPN等功能，以满足后续控制、管理的要求 |

## 商品化软件详细采购需求

### 环境感知客户端及服务中心系统功能要求

环境感知中心应支持对终端身份进行不可仿冒标识，对终端环境进行感知和度量，并传递给业务策略控制，协助业务策略控制完成终端的安全环境核查，从而实现动态访问控制的目的。 环境感知服务应具备生成终端身份标识、系统环境感知与度量、物理环境感知与度量、安全配置风险感知与度量、安全环境感知报告及报告传递等功能。环境感知中心的能力要求应遵从《GA/DSJ 351-2019》的相关要求。

#### 环境感知客户端基本要求

环境感知客户端终端授权许可>=2000点。

客户端支持和访问控制联动，提供终端设备可信标识、终端基本信息以及感知结果信息。

客户端请求响应小于200ms。

#### 可信标识管理

**标识管理**

可信标识管理子系统应支持终端设备身份标识的统一管理。

**设备可信标识**

支持为终端机器生成唯一设备可信标识。具备唯一性、不变性。

**双向认证**

客户端生成私有公私钥，终端敏感数据上报通过私钥加密，服务端解密，实现客户端可服务端的双向认证。

**白盒加密**

客户端私钥应支持存储在白盒中，确保私钥文件不被窃取、不被篡改。

**通信加密**

客户端和服务端通信应支持https加密。管理端访问使用https通信加密。

**自我保护**

客户端具备自我保护功能，实现恶意软件或服务无法终止客户端相关进程，无法修改客户端的配置文件，无法绕过客户端的感知监控引擎的运行。

#### 授权管理

应支持利用授权机制对一些知识产权进行保护，授权管理子系统应支持整个环境感知中心授权管理。支持采用序列号与授权文件的方式，并结合密码学技术，对授权进行保护。授权管理的子系统应具备授权识别和授权管理等核心功能。

#### 基础安全感知

基础安全感知应支持防病毒软件安装感知，能够发现终端上是否安装防病毒软件；支持病毒APT环境感知，能够发现终端中病毒感染情况；支持病毒库更新情况感知，能够发现病毒库的更新及时情况；支持系统高危漏洞感知，能够发现系统中是否存在高危漏洞。支持漏洞库更新情况感知。能够漏洞库的更新及时情况。

#### 环境感知管理

环境感知中心应具备环境感知策略的管理能力。感知管理子系统就是终端环境感知策略编排的子系统，能够支持环境感知的模板创建功能，感知模板目前支持基础安全感知、系统安全感知、应用合规感知、健康状况感知等四大感知分类的百余项配置项，能够对所有感知风险进行风险的自定义和扣分规则的自定义，并能够创建多个不同模板。同时通过模板分发功能将不同的模板分发到不同的分组的终端中。感知管理子系统目前包括分发管理、模板分发、感知模板配置、终端策略配置、环境感知报告等核心功能。

分发管理：支持对当前系统分发的感知策略进行管理，可以查看每种模板分发的目标范围、应用情况和下发时间，并能对目标重新分发。

模板分发：支持对当前系统配置的感知策略模板进行分发，可以自定义策略的执行方式和风险预警方式，同时能自定义分发目标。

感知模板配置：支持对当前系统创建的模板进行自定义配置，可以根据自身需要开启或关闭四大感知分类的百余项配置，能够自定义部分检查项，满足个性化需要，同时支持对所有感知项进行风险自定义和扣分规则自定义。

终端策略配置：支持对换进感知Agent的密码保护、升级、通讯、外观和模块等进行配置和管理。

环境感知报告：支持对风险等级进行自定义并统计和展示终端风险等级的分布，可以展示全网各风险项的风险情况，以及按照终端和分组进行排名等。

#### 系统安全感知

系统安全感知应支持感知系统安全基线状态，评估终端的使用配置和习惯是否存在安全隐患。

支持登录失败限制的风险感知。至少包括：账户锁定阀值、账户锁定时间、重置账户锁定计数器。

支持本地身份防盗用风险感知。至少包括：唤醒计算机时需要密码（使用电池）、唤醒计算机时需要密码（接通电源）、启用屏幕保护程序、密码保护屏幕保护程序。

支持密码维护要求风险感知。至少包括：密码长度最小值、密码最短使用期限、密码最长使用期限、强制密码历史、密码必须符合复杂性要求、使用可还原的加密来存储密码

支持账户管理审核风险感知。至少包括：审核帐户管理、审核计算机帐户管理、审核用户帐户管理、审核其他帐户管理事件、审核帐户锁定、审核登录事件、审核登录、审核帐户登录事件、审核凭据验证、审核其他帐户登录事件、审核注销、审核其他登录/注销事件、审核特殊登录

支持对象访问审核风险感知、配置变更审核风险、系统事件审核等风险感知。

支持网络安全访问控制风险感知。至少包括：不允许 SAM 帐户的匿名枚举、不允许 SAM 帐户和共享的匿名枚举、可匿名访问的命名管道、可匿名访问的共享、远程过程调用：用于未验证的RPC客户端的限制、远程过程调用：RPC终点映射程序客户端验证、NetMeeting：禁止远程桌面共享、远程桌面配置

支持数据泄密控制风险感知。至少包括：关机时清除虚拟内存页面文件。

支持账户访问控制与账户权限控制风险感知。至少包括：来宾帐户状态、使用空密码的本地帐户只允许进行控制台登录、重命名管理员帐户、重命名来宾帐户；用户权限分配：拒绝从网络访问此计算机、用户权限分配：允许通过远程桌面服务登录

支持功能组件控制风险感知。包括：Internet Information Services、Telnet服务器

支持网络配置入侵防范风险感知。包括：Internet通信设置：关闭手写个性化数据共享

支持应用安全配置入侵防范风险感知。包括：Windows资源管理器：关闭外壳协议保护模式、Windows资源管理器：关闭资源管理器的数据执行保护、附件管理器：打开附件时通知防病毒程序、疑难解答：允许用户从疑难解答访问联机疑难解答内容、自动播放策略：关闭自动播放、自动播放策略：自动运行的默认行为、自动播放策略：关闭非卷设备的自动播放

支持windows防火墙状态感知。

所有感知项应支持风险等级、扣分标准、修复方式的自定义。 支持自动修复。

#### 健康状态感知

健康状态感知应支持感知系统整体健康状态，能够感知不少于十项与系统健康状态相关的能力。

IE健康状态感知：支持对IE主页相关项、菜单项、核心配置、外观配置、常规设置、图标配置以及Internet选项等进行感知。

系统配置健康状态感知：支持对系统常用组件、系统重要服务组件、启动项、系统图标、组策略、任务栏及开始菜单等进行感知。

桌面健康状态感知：支持对桌面、桌面图标快捷方式、收藏夹快捷方式、开始菜单快捷方式、快速启动栏快捷方式、资源管理器、网络驱动及打印机驱动等进行感知。

#### 物理环境感知

物理环境感知子应能够通过终端的可视设备对终端周围环境进行感知。当授权人离开终端时，应支持重新触发环境感知，保证终端访问业务的安全可信；当多人在终端前进行围观时，物理环境发生变化，需要能够感知多人围观场景的数据泄露问题，也需要触发对应的环境感知策略，保证终端接入业务的安全性。物理环境感知子系统应具备授权人离席感知和多人围观感知等核心功能。

#### 终端管理

终端管理应支持对所有环境感知终端进行统一管理，能够解决大规模环境感知终端的统一管理问题。终端管理子系统应支持服务器性能监控、终端分组、终端筛选、感知概况等核心功能。

服务器性能监控：支持动态查看环境感知服务器的CPU、内存、磁盘网络以及数据库连接数等的占用或使用情况。

终端分组：支持对终端进行分组管理，支持自定义分组和设置自动分组规则，支持导入导出。

终端筛选：支持终端自定义展示，并通过计算机名、IP地址、在线状态等进行筛选；

感知概况：支持展示终端的相关信息，至少包括计算机名、IP地址、分组、终端版本、策略名称、最终得分、审批状态等信息，支持删除终端和转移分组。

#### 系统管理

系统管理应支持对整个环境感知服务系统进行管理，至少包含系统管理子系统、系统设置、帐号管理、系统日志管理、日志清理、数据备份与恢复、迁移、准入控制等核心功能。

系统设置：支持对环境感知中心进行相应的设置和管理，至少包括通用设置如IP显示、带宽设置、日志清理设置等，安全设置，升级设置，级联设置和证书管理。

账号管理：支持对管理员进行管理，至少包括新建、权限配置以及安全设置等。

系统日志管理：支持记录系统操作、运行和升级等信息的记录和管理。

日志清理：支持对记录的日志进行清理管理，可自定义要清理的日志数据以及开始清理的时间。

数据备份与恢复：支持手动和自动对环境感知中心的数据进行备份和恢复。

迁移：支持更换环境感知中心或代理后，对终端进行迁移。

终端准入控制：支持设置终端接入的黑名单或白名单，定义允许访问环境感知中心的终端范围。

#### 接口管理

零信任中心终端环境感中心应能够将识别出的风险种类及属性形成风险报告传递给访问控制中心，访问控制中心应支持将具体属性与业务进行绑定，实现更加细粒度的访问控制策略。接口管理子系统应至少具备云桌面接口功能、感知模板查询接口功能、Syslog外发接口功能、命令接口功能等核心功能。

### 业务安全策略控制服务

#### 实时数据

零信任安全中心业务策略控制中心的首页应支持系统概览，支持展示当前天实时的数据接入、信任查询推送、登录设备数、登录用户数、各信任模型的计算情况以及资源使用情况。

**用户和设备统计**

业务策略控制中心应支持统计接入用户、设备的相关信息。在首页中为相关人员提供了用户设备数量的概览。应至少包括：当日设备数、全部设备数，当日用户数、全部用户数。

**系统监控**

业务策略控制中心应支持系统监控功能，为相关人员提供了友好的系统监控信息展示，在界面上即可查看系统的CPU使用率、内存使用率、磁盘使用率、IO读/写速率。

**本日信任查询**

业务策略控制中心应支持为相关联的平台和服务提供了信任查询，本日信任查询支持可视化的查询的用户等级信息。至少包括信任查询等级的分布情况概览，以及详细用户名称、信任等级、查询时间的展示。

**本日信任基线评估**

业务策略控制中心应支持本日信任基线评估，支持各种信任基线的信任情况概览以及详细信息展示。支持概览展示用户、终端、移动端、服务器端、API的五个信任等级的数目。详细信息支持展示IP地址、基线分类、信任等级、时间的具体信息。

#### 风险汇聚

业务策略控制应支持风险汇聚，可将零信任中心环境感知中心、审计中心和安全感知和访问控制系统及安全防护策略控制服务传递的风险信息进行收集、汇聚，用于后续关联分析和信任评估。

业务策略控制中心汇聚的风险，应包括访问风险、防护风险；访问风险主要在用户访问过程中产生，来源于业务访问数据流经的终端、安全感知和访问控制系统和零信任中心。、

**业务审计风险汇聚**

零信任中心审计中心应支持将采集到异常的日志、失败日志等风险信息报送业务策略控制中心，包括但不限于：

（a）异常日志：审计中心采集到的异常日志，如异常认证日志、异常权限日志、异常操作日志等。

（b）失败日志：审计中心采集到的认证失败日志、授权和鉴权失败日志等。

业务策略控制中心应支持为审计中心提供Restful形式的审计风险上报接口，审计服务应支持通过该接口向业务策略控制中心上报审计风险。

上报的审计风险信息应包含且不限于：来源、风险类型、风险事件内容、风险等级、风险时间、风险的主体、风险主体类型、风险的客体、风险客体类型、处理结果等信息。

**环境感知风险汇聚**

零信任中心环境感知中心应支持将感知到的终端环境风险信息上报到业务策略控制中心，包括但不限于：

(a) 终端感染病毒风险：感知到终端被感染到病毒信息。

(b) 黑名单软件风险：感知终端运行了列入黑名单的软件风险。

(c) 多人围观风险：配合业务终端上的摄像头，感知到有人员对业务终端操作进行围观的风险。

(d) 授权人离席风险：配置业务终端上的摄像头，感知到被访问终端操作人员离开工作席位。

业务策略控制中心应支持为环境感知中心提供Restful形式的终端风险上报接口，环境感知服务应支持通过该接口向业务策略控制中心上报终端风险。

#### 风险识别

业务策略控制中心应支持内置事件的详细分类信息，只有被系统识别，并且能归类到系统事件分类中的事件，才会被响应。

在事件的识别方面，系统应支持精确匹配，模糊匹配，正则表达式，自然语义处理等多种技术手段，将其他系统发生的事件做分类汇聚。具体如下：

1、精确匹配：如果事件的信息是固定描述，那么推荐使用，匹配精准；

2、模糊匹配：如果事件的辨识度较高，可以使用基于字符串的模糊匹配，可能存在匹配错误的情况；

3、正则表达式：如果事件的规律性很高，推荐使用正则表达式方式，匹配精准；

4、自然语义处理：如果以上不符合，可以使用系统基于自然语义分析去匹配事件分类，可能存在匹配错误的情况。

#### 信任评估

**信任基线计算**

零信任中心业务策略控制中心的信任基线计算应支持根据多方输入的事件、日志等信息的持续性分析，根据基线配置，对用户、终端设备、移动端设备、服务器设备、API用户5个大类主体进行信任等级的计算，界面上应支持展示各类主体的基线配置项数据。具体情况如下：

1、信任基线分为极高、高、中、低、极低这5个等级；

2、预置用户、终端设备、移动端设备、服务器设备、API用户5个大类多个基线插件项；

3、页面可配置极高、高、中、低、极低这5个等级的基线检测项；

4、支持基线插件的快速开发与热更新；

5、支持对外查询接口；

6、支持信任基线的回溯查看。

**信任模型计算**

零信任中心业务策略控制中心的信任模型计算应支持根据日志信息进行信任计算，至少包含6个信任模型，如“用户访问行为分析模型”，“用户输入行为分析模型”，“API访问行为分析模型”，“机器行为识别分析模型”，“对等组离群行为分析模型”，“设备信任分析模型”等。基本情况如下：

1、支持模型默认定时运行；

2、支持界面触发立即运行或者禁用各个模型；

3、支持提供各模型的运行状态。

**用户访问行为分析模型**

零信任中心业务策略控制中心的用户访问行为分析模型应支持根据多方输入的事件、日志等信息，构建用户模型，基于用户访问行为分析模型做用户信任评估分析，为每个用户提供信任等级。支持图形化显示全局和个体的用户访问信任评估情况。具体要求如下：

1、支持对用户访问行为统计，确定用户访问行为基线；

2、支持根据用户访问行为，确定与基线的异常偏离概率；

3、支持界面可视化调整偏离阈值对应的信任等级；

4、支持确定用户访问行为的信任等级；

5、支持对外查询接口；

6、支持用户访问行为信任评估的回溯查看。

**用户输入行为分析模型**

零信任中心业务策略控制中心的用户访问行为分析模型应支持根据用户登录键盘输入的信息，构建用户输入行为模型，基于用户输入行为分析模型做用户信任评估分析，为每个用户提供信任等级。图形化显示全局和个体的输入行为信任评估情况。具体要求如下：

1、支持对用户输入行为统计，确定用户输入行为基线；

2、支持根据用户输入行为，确定与基线的异常偏离概率；

3、支持界面可视化调整偏离阈值对应的信任等级；

4、支持确定用户输入行为的信任等级；

5、支持对外查询接口；

6、支持用户输入行为信任评估的回溯查看。

**API访问行为分析模型**

零信任中心业务策略控制中心的API访问行为分析模型应支持根据多方输入的事件、日志等信息，构建API访问行为模型，基于API访问行为分析模型做API访问信任评估分析，为每个API提供信任等级。图形化显示全局和个体的API访问信任评估情况。具体要求如下：

1、支持对API访问行为统计，确定API访问行为基线；

2、支持根据API访问行为，确定与基线的异常偏离概率；

3、支持界面可视化调整偏离阈值对应的信任等级；

4、支持确定API访问行为的信任等级；

5、支持对外查询接口；

6、支持API访问行为信任评估的回溯查看。

**机器行为识别分析模型**

零信任中心业务策略控制中心的机器行为分析模型应支持根据多方输入的事件、日志等信息，分析出用户的API调用是否存在循环调用模式或是否符合随机分布调用。具体要求如下：

1、支持统计各个周期用户的API调用行为，确定各周期的相似性，周期内资源的调用概率；

2、支持界面可视化调整相似性阈值对应的信任等级；

3、支持确定是否存在循环调用模式或是否符合随机分布调用；

4、支持对外查询接口；

5、支持机器行为信任评估的回溯查看。

**对等组离群行为分析模型**

零信任中心业务策略控制中心的对等组离群行为分析模型应支持根据多方输入的事件、日志等信息，构建对等组离群行为行为模型，可基于对等组离群行为模型做对等组离群行为分析，为每个用户提供信任等级。图形化显示全局和个体的用户对等组离群行为情况。具体要求如下：

1、支持用户的资源访问、流量、社交、认证等数据源；

2、支持对数据源的不同时间段进行对等组划分；

3、支持界面可视化调整迁移阈值对应的信任等级；

4、支持确定用户的对等组离群行为信任等级；

5、支持对外查询接口；

6、支持对等组离群行为信任评估的回溯查看。

**设备信任分析模型**

零信任中心业务策略控制中心的设备信任分析模型应支持根据多方输入的事件、日志等信息，基于ATT&CK 攻击模型，评估设备信任。支持由策略配置安全和行为风险两部分进行评估。策略配置安全度量控制风险发生的能力，行为风险是当前设备可能存在的异常风险，它们共同组成了当前设备的信任。具体要求如下：

1、支持策略配置安全的信任计算、行为风险评估的计算；

2、支持信任等级的划分及分数计算；

3、支持对外查询接口；

4、支持设备信任评估的回溯查看。

**信任处置策略**

零信任中心业务策略控制中心管理员应能够设置临时的信任处置策略。设置了该策略后，支持匹配到的用户直接返回给来查询等级的系统设定的等级，再根据响应系统的业务逻辑做后续操作，如撤销其访问令牌等，即不通过模型计算、直接返回等级。策略支持设置成单个用户名，也可以设成全体用户，策略还有手动控制的功能，支持对该条处理策略设置禁用、启动、删除、编辑等功能，新增按有效期类型时间、次数分类，当是类型是时间时，到了该时间该条数据自动清除，即策略失效；当是类型是次数时，次数达到后该条数据自动清除，即策略失效，做到细粒度的策略处置。支持每匹配到一次用户查询，“命中数”+1直到有效次数用完或有效时间到期，该策略即失效。

**信任推送策略**

零信任中心业务策略控制中心设置了该策略后，当用户、API、设备等的等级发生变化时，支持向接收方推送变化通知。接收方收到通知后，支持调用业务策略控制服务的等级查询接口，查询最新的主体信任等级。输入框至少包括策略名称、推送的主体、接收方，支持针对不同的主体向不同的接收方推送变化信息，策略支持编辑、删除。

#### 风险决策

**风险处置策略**

零信任中心业务策略控制中心风险处置策略应支持关联单个或多个风险推导规则，当风险事件匹配处置策略中所配置的规则时，立刻发送风险信息给接收方。

支持管理员查看每条策略的事件命中情况，也可通过开关启用或停用相应策略。

**风险推导规则**

风险推导规则配置模块应支持创建风险规则，与风险处置策略配套使用，支持通过运算符与/或等组合不同的事件。

#### 联动通报指令

零信任中心业务策略控制中心应具备提供下发安全控制指令的能力，策略执行点支持下发相关执行指令。如用户登录认证后，收到相关风险信息，并经业务策略控制进行相关综合评估，若确实可能产生安全风险，业务策略控制将对认证服务下发令牌撤销指令；业务策略控制中心支持为认证服务和安全访问平台下发控制指令，指令下发支持校验机制避免指令伪造，并支持下发失败重传机制，避免指令丢失。

安全策略下发，应支持OpenC2规范，支持通用的Restful接口推送服务。用户可自定义接收端、推导结果和信任等级，从而选择不同的指令来定义策略，具有高度的灵活性。相关要求具体如下：

1、指令支持下线，二次认证，通知等动作指令；

2、指令支持基于OpenC2规范通过Restful接口下发。

3、支持向认证服务、权限服务、安全访问平台等下发指令

**认证服务指令下发**

当终端或用户信任状况发生变化时，业务策略控制中心应支持将会用户令牌作为主要依据，向认证服务通报的相应控制指令，而后认证服务根据指令对相应用户令牌实施管控，进而实现对用户的管控。

业务策略控制中心下发给认证服务的指令包括但不限于以下内容：

（1）撤销令牌：支持收到该指令后，认证服务应撤销相应的用户令牌。

（2）二次认证：支持多因子认证指令，认证服务应对该用户进行多因子认证。

（3）锁定用户：支持收到该指令后，认证服务应对该用户进行锁定，锁定后将拒绝登录。解锁操作在认证服务手工解锁。

（4）通知：支持下发信任评估结果，认证服务应根据下发的信任评估结果，对有关用户、设备进行管控。

**权限服务指令下发**

当终端或用户信任状况发生变化时，业务策略控制中心应支持将用户令牌作为主要依据，向权限服务通报的相应控制指令，而后权限服务根据指令对相应用户令牌实施有关权限的管控，进而实现对用户的管控。

业务策略控制中心下发给权限服务的指令包括但不限于以下内容：

（1）撤销权限：支持收到该指令后，权限服务应撤销相应用户的权限。

（2）冻结权限：支持收到该指令后，权限服务应冻结用户的权限。

（3）权限降级：支持收到该指令后，权限服务应对相应用户的权限进行降级处理。

（4）通知：支持下发信任评估结果，权限服务应根据下发的信任评估结果，对有关用户、设备等权限进行管控。

**安全访问系统指令下发**

当终端或用户信任状况发生变化时，业务策略控制中心应支持将会用户令牌作为主要依据，向安全访问系统通报的相应控制指令，而后安全访问系统根据指令对相应用户令牌实施用户访问控制。

业务策略控制中心下发给安全访问系统的指令包括但不限于以下内容：

（1）撤销令牌：支持收到该指令后，安全访问系统应撤销相应的令牌。

（2）评估通知：支持下发信任评估结果，安全访问系统应根据下发的信任评估结果，对有关用户、设备等进行管控。

**安全防护风险通报**

当终端或用户信任状况发生变化时，业务策略控制中心应支持将会用户令牌作为主要依据，向安全防护策略控制通报的相应控制指令，而后安全防护策略控制根据指令对相应用户令牌实施用户访问控制。

业务策略控制中心指令下发给安全防护策略控制的指令包括但不限于以下内容：

通知：支持下发信任评估结果，通用安全防护策略控制应根据下发的信任评估结果，对有关用户、设备等进行管控。

#### 分析模型

**设备信任分析**

设备信任分析应支持对所有登录设备进行基于安全配置及风险事件的信任评估，支持为主体信任评估提供的设备信任参考及异常告警。

1. 设备信任分析支持基于基本安全控制策略（CIScontrol等）的设备安全配置的评估及基于威胁模型的多数据来源的设备当前风险评估，支持给出同时基于设备安全配置评估及设备风险评估的直接及间接组合而成计算的设备信任等级。

2. 支持发现常用设备的安全配置，为设备信任评估提供安全配置依据参考，以及发现大规模设备配置异常。

3. 支持与设备画像，用户画像关联，发现关联的设备及用户。从多源数据发现风险威胁，提高异常事件告警概率。

4. 支持查询及展示单个设备的信任等级详情，其中包括了设备信任计算涉及到基本配置的安全评估及设备风险事件，设备风险事件评估支持基本的信息泄露风险检测、配置异常检测、连接异常检测、钓鱼软件/邮件等风险事件。

5. 支持对设备信任等级、设备安全配置、设备风险的统计及可视化展示。设备信任等级统计应支持一定时间段各类型设备的信任等级展示，以更清晰的方式展示系统内设备信任等级分布情况，为客户提供系统安全可靠性参考。设备安全配置统计，应支持对各类型的配置完整型统计展示，及从最高到最低配置详情的展示，使客户对安全配置有了总体了解。风险事件统计展示，应支持对一定时间段发生过的风险事件统计，使客户发现出现次数较多的风险，依此追溯原因，完善系统。

**用户访问行为分析**

用户访问行为分析应支持展示用户的信任计算详情，可以看到整体情况和每个用户具体的异常行为等。页面提供用户名查询、根据等级过滤等功能。

支持查看单个用户的信任计算详情，具体的异常事件类型及发生的事件数趋势。

**用户输入行为分析**

用户输入行为分析支持从具有键盘输入行为的用户访问操作中，构建用户输入操作模型检测用户输入行为异常，为主体信任评估提供用户信任参考，及异常告警。

1. 支持基于键盘操作的用户访问操作中获取用户输入行为数据建立用户输入行为模型，包括登录认证时账号密码输入（脱敏处理）、访问界面有打印行为的键盘输入、提供特定文字描述的统一键盘输入等。

2. 支持基于用户输入行为模型的异常输入行为检测，当用户发生某次输入行为时与用户输入行为模型库中的模型数据比较发现异常，给出告警。

3. 支持与其他访问异常、设备异常、用户画像等关联，从多源数据发现及展示异常

4. 支持对输入行为统计的可视化展示，包括异常输入及正常输入的趋势展示、以不同访问客体的异常率展示分析、用户的异常输入率展示分析。对访问异常率展示，清楚发现异常率较高的访问客体，关联其他异常事件，可分析原因，提高客体信任等级，降低访问客体被攻击的概率。对访问主体异常率的展示，清楚了解异常率较高的用户，对这些用户做一定的访问及操作限制，降低内部威胁概率。

5. 支持展示每次发生输入异常的事件详情，包括用户、时间、访问客体等，其中详情包括了对此次异常数据与其他正常历史行为数据的脱敏可视化详情展示。将事件发生详情与其他异常事件对比，发现及提高告警率，及时降低用户信任等级，减少内部威胁。

**API访问行为分析**

业务策略控制服务分析模块针对API访问行为分析应支持以下几部分：

1.API用户行为基线计算

支持基于用户API调用日志，当API用户的调用行为次数超过阈值时，统计用户调用时间、常用地理位置、调用行为次数、设备使用的行为基线，对用户调用API行为进行刻画。

* 时间基线: 支持将全天划分成7个时间段，统计每个用户在每个时间段的调用行为次数；
* 地理位置基线: 支持统计每个账户在所有城市的操作次数，城市包括直辖市及地级市；
* 调用行为次数基线: 支持统计用户在某个时间段（时、日、周、月）的平均操作次数；
* 设备使用基线: 支持统计每个用户在每台设备的使用次数。

2.API用户异常事件识别

支持基于API用户调用行为基线，计算用户某次调用行为和基线的偏离程度，基于偏离程度来判断是否异常。支持对以下异常事件进行识别：

* 基于个人异常时间调用
* 账号在非常用地理位置调用
* 账号同时在不同地理位置调用
* 多账号在同一设备调用
* 同账号在多设备调用
* 调用次数超过个人均值

3.API用户信任级别评估

支持基于API用户调用异常事件，每个时间段对所有用户进行信任分计算，综合多个时间段对用户评定总体信任等级。

支持将API用户异常事件分为时间异常、位置异常、设备异常、操作异常四类，基于事件分类进行扣分（每类扣分有限制），得到时间段的用户信任分。支持基于时间衰减法则综合多个时间段对用户进行信任评估。

4.API用户信任级别溯源

对API用户进行信任等级评估后，应能够查询到用户所有相关的异常事件及异常事件相关统计结果，也能够通过时间、事件、事件分类进行检索。

**API机器行为分析**

零信任中心业务策略控制中心分析模块应支持基于API调用日志，采用机器学习、行为分析等技术，对API调用行为进行分析建立行为基线，结合不同检测维度进行API机器行为检测。支持API机器行为分析能够对爬虫、攻击行为等进行识别，提升API安全防护能力。

**API风险分析**

零信任中心业务策略控制中心应支持通过统计、处理、分析用户与API访问等相关数据，可检测至少六大类API安全风险。

1.对象级别授权风险检测

对象级别授权风险：攻击者将API调用中自己的资源的ID替换为属于另一个用户的资源的ID。如果缺少适当的授权检查，攻击者可以访问指定的资源。这种攻击也称为IDOR（不安全的直接对象引用）。

访问未授权对象资源风险：检测用户在通过API访问某个资源时是否存在未授权风险，如果分析判断出可能存在风险，则将该风险信息写入数据库，并在页面展示用户访问的资源相关API信息。

2.身份验证风险检测

身份验证风险：不安全的，缺少保护的身份验证机制有以下风险；

* + 攻击者可以伪造或者绕过身份验证，目的是接管一个或多个账户，并使攻击者获得与被攻击用户相同的特权。
	+ 用户身份验证凭据在存储时未被保护，例如没有对存储的用户名和密码值进行加密和哈希处理。
	+ URL重写，将会话ID公开放在URL
	+ 用户密码较弱，登录凭据可被暴力破解。
	+ 身份认证有效期过长。

URL重写风险：检测用户在通过API认证成功时是否存在URL重写风险，如果分析判断出可能存在风险，则将该风险信息写入数据库，并在页面展示用户认证成功的相关API信息。

URL暴力登录风险：检测用户在通过API认证失败时是否存在暴力登录风险，如果分析判断出可能存在风险，则将该风险信息写入数据库，并在页面展示用户认证失败的相关API信息。

身份认证有效期过长风险：检测用户在通过API认证时是否存在身份认证有效期过长风险，如果分析判断出可能存在风险，则将该风险信息写入数据库，并在页面展示用户认证时使用相关身份认证凭据的API信息。

账户被盗风险：检测用户在通过API认证时是否存在账户被盗风险，如果分析判断出可能存在风险，则将该风险信息写入数据库，并在页面展示可能被盗用户的相关API信息。

攻击者IP风险：检测用户在通过API认证时是否存在攻击者IP风险，如果分析判断出可能存在风险，则将该风险信息写入数据库，并在页面展示攻击者IP的相关API信息。

3.数据泄露过多风险检测

API可能会包含客户端所展示的数据以外更多的数据，这取决于客户端如何进行过滤。而在客户端过滤敏感信息，存在用户敏感信息泄露风险。

敏感信息泄露判断：敏感信息识别主要判断敏感信息是否为电话、邮箱、地址、ip、身份证号等。如果分析判断出可能存在敏感信息泄露风险，则将该风险信息写入数据库，并在页面展示敏感信息可能泄露的相关API信息。

4.API请求速率和资源限制缺失风险检测

支持限制API被请求速率以及负载，防止大量请求或大量的负载调用，可能会使API崩溃，导致DDoS攻击，暴力破解攻击。

速率限制缺失风险：检测用户在通过API访问时是否存在速率限制缺失风险，如果分析判断出可能存在风险，则将该风险信息写入数据库，并在页面展示缺乏速率限制的相关API信息。

资源限制缺失风险：检测用户在通过API访问时是否存在资源限制缺失风险，如果分析判断出可能存在风险，则将该风险信息写入数据库，并在页面展示缺乏资源限制的相关API信息。

5.功能级别授权风险检测

API功能参数可预测，普通用户可执行管理员操作。一些管理功能公开为API，易于被检测和利用。非特权用户可以未经授权访问这些功能。

功能级别授权风险：检测用户在通过API访问时使用的功能参数（method）是否存在未授权风险，如果分析判断出可能存在风险，则将该风险信息写入数据库，并在页面展示用户使用的功能参数相关API信息。

6.批量分配风险检测

在API调用过程中，通常API对调用者非常信任，API不过滤传入的数据，一律视为正确的结构将其存储。攻击者可以通过查看GET请求数据来猜测字段。

批量分配异常识别：检测用户调用API时是否存在批量分配异常，如果分析判断出可能存在异常，则将该异常信息写入数据库，并在页面展示存在异常的相关API信息。

**休眠帐号分析**

零信任中心业务策略控制中心应支持通过认证中心通报的用户令牌，结合安全访问系统报送的用户访问行为日志等数据信息，进行关联分析，建立用户账号的访问时间记录，通过与相应的休眠账号时间阈值进行比较，对于超过阈值时间的账号，则认定为休眠账号。

业务策略控制中心的休眠账号分析具体要求如下：

1、支持时间段检索查询休眠账号；

2、支持休眠账号以列表形式展示，至少包括已休眠天数、最近更新时间、最近计算时间等；

3、支持定义休眠帐号时间阈值。

**特权帐号分析**

零信任中心业务策略控制中心应支持通过认证中心通报的用户令牌，权限服务通报的权限信息，结合安全访问系统报送的用户访问行为日志等数据信息，进行关联分析，建立用户账号的权限基线，支持通过权限基线比较，对等组分析等，挖掘和发现特权账号。

业务策略控制中心的特权账号分析具体要求如下：

1、支持关联账号趋势分析

2、支持特权账号统计

3、支持特权账号分析明细

4、支持时间段的查询和统计分析

**分析参数配置**

分析参数配置应支持身份治理有关的休眠账号分析、特权账号分析相关参数进行配置和维护功能。支持通过设置不同的参数对使得休眠账号、特权账号分析会得到不同的结果。

1.休眠账号阈值

休眠账号阈值设置是指为休眠账号分析指定相应的休眠天数。应支持通过计算分析发现某账号非活跃时间超过设定的此值，并认定此账号为休眠账号。

2.特权帐号配置

特权账号配置应支持添加已知的、明确的特权账号，业务策略控制中心在特权账号分析时，支持对这些设定的特权账号进行分析，追踪这些特权账号行为轨迹。特权账号配置具体要求如下：

支持特权账号的添加、编辑和删除。

支持特征账号名称、详情的列表。

#### 对接接口

业务策略控制中心，支持通过接口管理功能，根据实际对接和交互的系统，进行接口配置，如风险事件接收API、认证指令接收API和环境感知查询API等参数的配置。

**认证服务接口**

在用户进行登录认证时，认证中心应支持向业务策略控制中心查询相应的终端风险信息，并根据风险情况颁发或者拒绝颁发用户令牌。

在颁发用户令牌之后，认证中心应能够向业务策略控制中心同步相应的用户令牌。

上述业务场景涉及认证中心与业务策略控制中心的服务接口应至少包含以下几种：

（1）风险上报接口：零信任中心认证中心将有关的认证风险通过该接口上报到业务策略控制中心，从而实现由业务策略控制中心的风险汇聚。

（2）风险信息查询接口：零信任中心认证中心在用户登录时，可使用该接口查询终端环境风险信息，并根据查询结果颁发或者拒绝颁发用户令牌。

（3）接收用户令牌接口：零信任中心认证中心在完成用户令牌颁发之后，通过该接口向业务策略控制中心发送已颁发的用户令牌。业务策略控制中心将此令牌做为后续指令下发的依据。

（4）信任评估查询接口：零信任中心认证中心根据业务需要，可使用该接口向业务策略控制中心查询信任评估结果，并根据查询结果实现相应的认证策略。

**权限中心接口**

在用户进行鉴权时，零信任中心权限中心应支持向业务策略控制中心查询相应的终端风险信息，并根据风险情况授予或者拒绝授予用户权限。

在用户鉴权过程中，权限中心应支持将相应的权限风险信息上报到业务策略控制中心，从而实现由业务策略控制中心的风险汇聚。

上述业务场景涉及权限服务与业务策略控制中心的服务接口应至少包含以下几种：

（1）风险上报接口：权限中心将有关的权限风险通过该接口上报到业务策略控制中心，从而实现有业务策略控制中心的风险汇聚。

（2）风险信息查询接口：权限中心在用户鉴权时，可使用该接口查询终端环境风险信息，并根据查询结果授予或者拒绝授予用户权限。

（3）信任评估查询接口：权限中心根据业务需要，可使用该接口向业务策略控制中心查询信任评估结果，并根据查询结果实现相应的权限控制策略

**审计中心接口**

零信任中心业务策略控制中心的各类系统日志应支持报送给审计中心，为审计中心的日志审计提供支撑。

零信任中心审计中心在进行审计行为，对发现的相关行为风险，应支持报送给业务策略控制中心，从而实现由业务策略控制中心的风险汇聚。

上述业务场景涉及审计中心与业务策略控制中心的服务接口应至少包含以下几种：

（1）风险上报接口：零信任中心审计中心将有关的审计风险通过该接口上报到业务策略控制中心，从而实现有业务策略控制中心的风险汇聚。

（2）日志上报接口：业务策略控制中心按照审计中心的接口要求，通过该接口向审计中心报送日志信息，为审计中心的日志审计提供支撑。

**环境感知中心相关接口**

零信任中心环境感知中心应支持将采集到的终端环境和风险信息报送给业务策略控制中心，为业务策略控制中心的风险汇聚和信任评估提供基础数据支撑。

当环境感知中心感知到终端风险时，引起终端设备信任状况变化时，应能够及时推送给业务策略控制中心。

上述业务场景涉及环境感知中心与业务策略控制中心的服务接口应至少包含以下几种：

（1）环境信息变更接口：零信任中心环境感知中心感知到终端环境信息和风险变化时，通过该接口上报将相关信息到业务策略控制中心，从而实现有业务策略控制中心的环境信息和风险汇聚。

（2）环境风险信息查询接口：零信任中心业务策略控制中心在需要时，会主动通过该接口向环境感知服务查询终端环境信息和风险。

**安全访问系统相关接口**

安全访问系统在对用户进行访问控制的过程中，应支持向业务策略控制中心报送用户的访问日志，以便为业务策略控制中心进行用户信任评估提供支撑。同时，安全访问平台应支持根据业务需要向业务策略控制中心查询终端环境和风险信息、用户信任评估结果等，并实施相应控制措施。

业务策略控制中心应支持通过分析计算，发现用户信任评估状况发生变化时，也会主动向安全访问平台进行发送信任状况变更通知。

上述业务场景涉及安全访问系统与业务策略控制中心的服务接口应至少包含以下几种：

（1）访问日志接口：安全访问系统将有关的用户访问过程的日志通过该接口上报到业务策略控制中心，为实现业务策略控制中心的信任评估提供支撑。

（2）风险信息查询接口：安全访问系统根据业务需要，可使用该接口向业务策略控制中心查询终端环境信息和信任状况，并根据查询结果实现相应的控制措施。

（3）信任评估变更通知接口：在用户信任状况发生变化时，业务策略控制中心通过该接口向安全访问系统发送变更通知。安全访问系统可根据通知情况，实施相应的控制措施。

（4）信任评估查询接口：安全访问系统根据业务需要，可使用该接口向业务策略控制中心查询信任评估结果，并根据查询结果实现相应的控制措施。

**安全防护策略控制相关接口**

安全防护策略控制应支持对用户进行访问控制的过程中，向业务策略控制中心报送用户的访问日志。同时，安全防护策略控制应支持根据需要向业务策略控制中心查询终端环境和风险信息、用户信任评估结果等，并实施相应控制措施。

业务策略控制中心应支持通过分析计算，发现用户信任评估状况发生变化，并主动向安全防护策略控制进行发送信任状况变更通知。

上述业务场景涉及安全防护策略控制与业务策略控制中心的服务接口应至少包含以下几种：

（1）访问日志接口：安全防护策略控制将的用户访问过程的日志通过该接口上报到业务策略控制中心，为实现业务策略控制中心的信任评估提供支撑。

（2）风险信息查询接口：安全防护策略控制根据业务需要，可使用该接口向业务策略控制中心查询终端环境信息和信任状况，并根据查询结果实现相应的控制措施。

（3）信任评估变更通知接口：在用户信任状况发生变化时，业务策略控制中心通过该接口向安全防护策略控制发送变更通知。安全访问系统可根据通知情况，实施相应的控制措施。

（4）信任评估查询接口：安全防护策略控制根据业务需要，可使用该接口向业务策略控制中心查询信任评估结果，并根据查询结果实现相应的控制措施。

#### 系统管理

业务策略控制中心，应支持系统的日常管理功能，管理员应能够随时了解系统运行状态，系统管理员通过系统完成对系统的配置、系统运行情况的监测和相关策略执行情况的查看等。

**系统部署**

业务策略控制中心应支持系统部署相关的配置功能，支持通过界面直观配置，将数据传送到后台，并经过后台程序进行相关信息的读取和执行，确保业务策略控制中心便捷高效的部署和正常运行的能力：

1、系统网络配置能力：支持IP地址，子网掩码，网关信息；

2、提供服务器的DNS信息配置；

3、支持统一配置多台服务器的系统时间能力，并且可以配置用户的NTP时间服务器。

**账号管理**

支持管理员新建、修改和删除账号等信息的功能。能对新建的用户进行权限配置，定义每个用户的访问权限及相关角色，同时账号管理支持用户及其相关属性的增、删、改和查等功能。

**操作日志**

业务策略控制中心的日志管理功能，除支持本身相关信息的操作记录外，还应支持对外日志信息的输出功能，即可通过日志管理功能，将系统日志进行整理并配置接收方的相关接口参数，实时的将产生的日志和接收的风险等信息，发送给业务审计服务。

**系统信息**

业务策略控制中心应支持系统运行的加固和信息展示：

1、业务策略控制中心支持对自身软件运行的操作系统进行安全和稳定性的优化处理，确保自身运行的高效稳定运行；

2、系统信息及加固应支持业务策略控制中心授权信息，授权有效期管理和显示功能；

3、业务策略控制中心系统信息及加固应支持系统使用的磁盘空间等信息统计和展示。

## 定制化软件详细采购需求

### 警综平台.零信任模块-认证服务

#### 警综平台升级

##### 与环境感知客户端对接

* 与环境感知客户端进行对接获取客户端评分，用以判断用户是否可以进行登录及后续操作。
* 需对接各地市部署的环境感知评分获取接口，解析接口响应信息；
* 向警综平台输出环境感知结果，包含评分信息、优化建议、安全软件下载链接、环境感知软件下载链接等信息；
* 风险分析，根据评分执行阻断、提醒等操作，并记录分析日志

##### 认证管理升级

* 对接认证服务中心，获取用户令牌和应用令牌
* 添加零信任令牌发放功能，包含用户令牌和应用令牌
* 对应用统一认证、第三方组件代理认证等相关模块进行功能集成

##### 认证因子升级

* 支持格尔网关认证
* 支持辅警证书认证
* 支持人脸认证

##### 二次认证

* 支持用户二次认证，例如：用户通过短信验证码登录门户（当前安全等级较低为一级），需要登录安全等级较高的应用，例如执法办案系统，此时则会弹出二次认证界面，要求进行PKI认证；
* 支持权限提升需要时的二次认证；
* 支持登录状态失效是的二次认证；
* 提供独立组件，供第三方系统需要时进行二次认证；
* 二次认证支持单因子认证也支持多因子认证；

##### 独立部署

* 升级原警综平台认证功能，独立建设零信任体系认证模块，认证模块服务部署在省厅数据域，与原警综平台松耦合

#### 令牌管理

* 令牌分为用户令牌、应用令牌；
* 用户令牌中需包含用户标识、机构标识、创建时间、过期时间等信息；
* 应用令牌需包含用户标识、机构标识、应用标识、创建时间、过期时间等信息；
* 令牌生成需基于JWT+国密算法进行令牌生成。
* 支持国密算法,保证令牌信息的机密性,系统除支持 RSA 算法的证书外，同时支持国产的 SM算法证书,支持基于国产密码算法的 SSL 功能，保证客户端到服务器之间的数据传输安全
* 提供用户令牌和应用令牌在各使用节点的全生命周期集中管理，包括：签发、撤销、验证、更新、加密等。
* 支持令牌管理功能：

支持通过用户名、用户身份证号、用户IP、令牌类型、在线时间、部门信息进行令牌的筛选；

支持对指定令牌的手动注销功能

* 支持根据接收到的风险指令或自有策略判断结果，调整相应令牌状态；
* 支持将令牌及其状态通知给需要核验令牌的相关方。

#### 令牌黑名单管理

* 包含增加、删除、查询功能；
* 可以设置指定用户、IP、时间段，令牌受限，不允许登录零信任体系内的所有功能。

#### 认证功能

* 根据配置确定应用的认证方式；
* 根据认证方式调用对应的认证因子进行认证；
* 根据各认证因子反馈的认证结果进行综合判定，根据结果签发令牌；
* 支持持续认证；
* 支持认证过程中的风险检测输出及处理；
* 人像认证组件：

 B/S端自动调起摄像头；

 自动识别画面内是否存在人像；

 自动拍照并上传服务器进行校验；

 支持活体检测功能

* 与人像1:1比对接口对接；
* 与认证中心对接，完成认证后可以进入警综平台；

#### 认证因子管理

* 支持的认证因子包含但不限于口令、数字证书、生物特征，其中生物特征包括但不限于人脸、声纹等生物特征以及复合生物特征；
* 认证因子信息包括但不限于认证因子名称、安全等级、启用状态、认证因子管理平台地址；
* 支持认证因子信息的管理，包括但不限于增、删、改、查；
* 支持认证因子的标准化接入和管理；
* 支持活体检测等措施与多因子认证的组合；
* 支持组合不同的认证因子满足不同的安全级别需求；
* 支持申请材料的上传、删除、下载等功能；
* 支持认证因子的启用、停用功能。

#### 认证服务代理

* 支持代理跨网跨域访问认证服务；部署在安全访问通道或用户域。实现认证信息和返回令牌的跨域传递，最终通过令牌实现用户在用户域内能够访问数据域内的资源。
* 支持与认证服务间加密通信；
* 支持标准协议，认证服务接口支持国密SSL；
* 支持通过负载均衡和集群部署等形式，确保认证服务的持续可用，同时允许对认证能力进行扩容。

#### 应用管理升级

* 认证管理部分添加零信任令牌属性选择
* 细化应用管理，分为基本配置、高级配置、扩展信息、附加信息；

#### 系统注册升级

* 支持认证因子、认证等级、AK、SK、固定SK配置管理

#### 日志管理

* 支持多维度日志记录，包括但不限于注册、配置、认证、维护等操作日志；
* 支持相关认证因子认证日志的接收；
* 支持日志的标准化输出；
* 定时对早期日志进行归档；

#### 认证服务接口

* 用户基本信息接口服务
* 用户详细信息接口服务
* 用户令牌生成服务
* 应用令牌生成服务
* 用户令牌校验服务
* 应用令牌校验服务
* 用户令牌更新服务
* 应用令牌更新服务
* 用户令牌撤销服务
* 应用令牌撤销服务
* 添加应用信息同步接口，支持第三方需要使用本接口的系统可以通过本接口获取全部应用信息，并保持增量更新
* 所有接口服务都需注册到服务总线；
* 提供统一的第三方调用辅助JAR；
* 支持全省应用对接并提供技术支持

#### 与第三方对接

* 与业务安全策略控制、审计中心等服务对接推送风险、日志等信息
* 包含风险传递服务对接、认证令牌接收服务对接、认证日志接收服务对接、用户下线推送服务对接、应用下线推送服务对接、审计日志中的登录、应用操作等日志推送服务对接
* 安全管理中心对接用户、组织机构、应用目录、服务目录数据

### 警综平台.零信任模块-权限服务

#### 规则权限配置

* 包含规则权限的增、删、改、查等功能
* 支持根据部门、人员类别、警种之中的单个或多个构建规则组合，并与应用进行关联配置
* 规则权限服务缓存服务

在系统启动时自动将规则权限加载到内存中；

自动从数据库中将新的规则更新到规则中；

* 规则解析服务

根据部门、人员类别、警种自动遍历组装，通过特定算法重新生成新的规则列表；

提升用户登录平台后获取规则权限无需等待，大幅度降低等待时间；

* 规则权限与警综平台权限体系融合

#### 个人权限管理

* 包含个人权限申请、个人权限申请审批、个人权限收回等功能
* 个人权限申请：

用户可以在应用商店中对无权限的应用发起权限申请；

支持按警综角色、应用信息（菜单级）申请；

支持自动查找管理员，若管理员不存在则无法申请；

* 个人权限申请审批：

包含审批通过、审批退回等功能

包含待审批列表、历史列表

支持通过用户名、虚拟号、所属部门、查询范围、人员类别等信息进行筛选

支持申请内容查看

* 个人权限收回：

包含收回、全部收回、组合收回等功能；

支持同步应用树查看人员数量

支持应用树查询；

支持按用户姓名、身份证号、所属部门等信息进行筛选

支持查看个人信息

支持多应用进行人员筛选并进行权限回收

#### 权限审批-辅助管理员

* 根据应用管理中的辅助管理员配置分配本功能模块权限
* 包含审批通过、审批退回、待审批列表、历史记录等功能
* 管理员审批时可以查看审批内容、申请理由、申请时间、申请人等信息
* 管理员审批时可以填写理由，并通过消息中心反馈给申请人
* 申请单失效自动回收，提供定时任务，自动检测预期的申请单，自动设置为失效

#### 辅助管理员授权

* 根据应用管理中的辅助管理员配置分配本功能模块权限
* 提供管理人员列表的查询、详情查看、授权等功能
* 辅助管理员授权仅允许单行数据操作
* 权限授权列表

 展现辅助管理员拥有的权限列表

 支持一级权限的授权、回收；

 支持子级应用的授权、回收；

 支持应用简称、全称的筛选功能。

#### 应用级鉴权服务接口

* 支持第三方系统、网关、安全通道等第三方应用或服务通过本接口获取应用权限信息；
* 传入用户令牌，服务接口返回对应有权限的应用列表
* 支持单应用、多应用鉴权
* 支持按人员获取权限列表
* 支持资源权限等级获取

#### 异常鉴权预警

* 支持对鉴权过程中的非正常鉴权产生预警；
* 预警种类包括：用户异常时间鉴权预警、用户异常IP鉴权预警等；
* 接收风险指令结果，对鉴权过程进行阻断；
* 标准化输出预警结果；

#### 日志管理

* 支持多维度日志记录，包括但不限于注册、配置、认证、维护等操作日志；
* 支持相关认证因子认证日志的接收；
* 支持日志的标准化输出；
* 定时对早期日志进行归档；

### 警综平台.零信任模块-基础要素管理

1. **服务目录**
* 包含服务目录的增、删、改、查、启用、停用、导入、导出等功能；
* 服务目录包含但不限于服务名称、服务IP、服务端口、所属部门、注册人、责任民警、责任领导、运维人员、所属应用、登记时间、更新时间、数据来源等信息；
* 支持对接云服务总线及其他各服务总线服务目录，支持定时同步数据到本服务目录；
* 提供服务全量、增量同步接口服务，为零信任可信API网关提供数据支持；
* 记录操作日志，方便管理员回溯历史记录；
* 对接API网关，同步相关服务接口配置给API网关，由API网关进行开启、关闭控制；
* 独建设服务目录功能，服务目录模块部署在省厅数据域，与原警综平台松耦合。
1. **应用管理目录升级**
* 添加警种、运维工程师、责任民警、所属部门、责任领导、辅助管理员、相关人员、简要说明等信息的维护管理
* 针对应用添加业务、地区、层次、警种等分类方式
* 支持应用手册的上传、下载、删除等功能
* 支持AK、SK、固定SK信息的获取及查看
* 应用上架服务及应用同步服务升级

### 警综平台-零信任模块-地市级级联

* 认证服务支持开发通用接口，允许地市级通过标准化接口进行级联。
* 服务目录支持地市服务目录级联，支持定时同步数据到本服务目录。
* 基础要素库人员目录开放标准通用接口，支持传输加密认证，支持地市级级联。
* 基础要素库应用管理目录开放标准通用接口，支持传输加密认证，支持地市级级联。

## 系统集成及配套服务详细采购需求

总体要求本项目所有硬件产品要求提供原厂商工程师安装、配置服务，以及定期巡检服务

### 驻场人员服务要求

#### 安全访问通道技术驻场人员

要求安全访问通道驻场人员接受建设方面试同意，如不符合建设方要求，投标方需更换驻场人员，驻场人员要求为环境感知原厂厂商指定驻场人员。

熟练掌握本项目安全系统的规划部署、测试、实施及优化等；

熟练掌握公安大数据智能化应用安全体系要求；

具备良好的逻辑分析能力及较强的学习能力，有团队合作精神和敬业精神；

语言表达能力较强，思路清晰，能顺畅的与管理部门和业务对象进行沟通。

#### 零信任体系驻场人员

驻场运维服务三年，驻场人员要求：

1）熟悉SLB云服务总线接口的发布及对接流程，具备撰写接口对接文档的能力；

2）熟练掌握SQL数据库语言，可以基于数据库日志排查慢SQL、优化SQL语句；

3）熟练掌握基于省厅阿里云ECS、SLB、REDIS、DRDS、RDS、OSS等云上组件开发实施零信任项目；

4）熟练掌握java编程语言，熟悉软件项目开发、系统运维的基本流程，能够解决系统运行中发现基础的问题、独立完成功能模块的开发；

工作职责要求：

1）负责数据域认证服务中心日常运维工作，处理、协调和解决项目中出现的技术问题，撰写应用对接需要的技术文档；

2）负责数据域应用对接的技术支持及疑难解答；指导第三方对接厂商可以顺利对接；

3）能够参与系统运维过程中问题诊断发现工作，针对具体问题协同各方提出有效可行性方案。

#### 系统集成要求

安全访问通道和数据交换通道，需要对接省厅零信任体系；数据交换通道集中监控管理系统对接省厅安全管理中心；数据检控支持对接零信任体系。

项目终验前，公安部主管部门如要求对本系统项目开展达标检测的，承建方应承担相应的检测费用，并确保本次采购范围的软硬件产品符合公安部标准要求。

# 投标技术方案及其他要求

## 项目系统集成的具体技术方案要求

1. **项目技术方案必须符合要求，投标公司应当将本项目采购的软硬件设备按照公安部及我省大数据安全体系相关技术规范要求，结合实际进行部署实施初步设计，并提供简要实施部署方案。**
2. 根据采购需求文件要求，建议投标供应商提供各类商品化软硬件产品相关功能、性能、成熟度等方面要求的相关证明材料、证明材料（或承诺文件）。提供详细材料清单文件（盖章）（产品名称、品牌型号、证明材料名称、材料说明、证明材料附件页码）。**提供的证明材料可以为正式的内部测试报告、用户测试证明、第三方证明材料、用户合同（合同中要求明确相关产品品牌、型号和功能）等。**

## 项目投标方案相关要求

1. 投标人须对项目详细采购需求中的技术要求进行实质性相应。为确保提供的技术参数偏离表真实有效，原则上要求所有的软件产品及硬件设备的技术偏离表需加盖投标人公章。
2. 本项目接受第三方监理全程监督。对投标供应商提供的所有软硬件产品，将逐一对照招标文件、投标响应文件进行核对，对品牌型号、配置、性能、功能等进行严格检查。
3. 本项目中各类软硬件及服务不接受零报价，出现零报价的作为无效标处理。不接受免费赠送软硬件产品或服务。投标人根据项目实际实施需要，提出的合理建议及配套增加提供的软硬件设备或服务，必须明确标注价格，对于不合理的、不采纳的建议，用户经研究在实际项目实施中不予执行，并在项目决算时对相关内容予以审减。

## 知识产权等相关要求

1、本项目中如存在定制开发软件产品，相关知识产权归浙江省公安厅享有；2、定制开发软件的源代码（含质保期内的后续升级版本）必须遵循相关标准和规范，并无条件提交给我厅；3、涉及接口必须遵循相关标准和规范，向下部署的，必须无条件开放所有接口且满足国家共享相关规定要求，项目承建单位（施工单位、实施单位）有义务配合信息中心做好有关信息共享工作（不得人为设置技术壁垒）4、本项目在开发、使用和维护过程中接触到的浙江省公安厅的所有资料，未经浙江省公安厅授权代表书面许可，不得留存，私自查阅及向任何第三方泄露；5、本项目的设计开发专利申请权、技术的使用权和转让权归浙江省公安厅所有；6、若未能做到以上要求项目承建单位需承担相应责任。

## 项目建设安全相关要求

定制化软件建设完成后，符合国家信息安全等级保护要求，根据等级保护要求进行定级、备案及测评。

## 项目验收要求

1. 功能指标
2. 提供安全访问通道冗余能力。
3. 提供用户域与数据域之间的数据交换能力。
4. 提供安全访问通道和数据交换通道的安全防护能力。
5. 建设零信任体系的环境感知和业务安全策略控制能力
6. 性能指标
7. 安全访问通道、零信任服务用户访问并发大于等于2000人。
8. 数据交换通道性能，数据交换文件交换吞吐量单向导入和单向导出不少于6Gbps，数据库同步不低于每秒12000条，指令交换默认10个标准接口对接服务，指令请求并发500个。
9. 实施验收要求

第一阶段 合同签订后3个月内，所有商品化软硬件产品到货，并完成硬件设备安装部署工作。并组织初步验收，并投入试运行。

第二阶段 初验后10个月内完成项目终验。

**商务要求表**

|  |  |
| --- | --- |
| **▲项目工期（交货期）及地点** | 合同签订后3个月内完成项目中涉及的所有软硬件设备交货，货物送达省公安厅信息中心机房。软硬件设备完成安装部署和调试工作后，组织初步验收，并投入试运行；初验后10个月内完成项目终验。 |
| **▲付款条件（明确是否需要履约保证金）** | 1、履约保证金缴纳：签订合同后10个工作日内，成交供应商向采购人提交合同金额的1%作为履约保证金（或提供保函等）。成交供应商若以电汇、网上银行方式交纳的,请将电汇底单、网上银行电脑打印凭证写上成交项目名称及编号、成交人及联系人、联系电话传真至0571-87286476）。缴款账户信息为：户 名：浙江省公安厅开户行：工行解放路支行银行帐号：12020207099000112662、履约保证金退还：按合同约定办理履约保证金退还手续。办理履约保证金退还手续时，成交人凭以下材料办理。（1）由采购人开具的交入履约保证金往来款收据原件(如无法提供原件的，提供复印件及采购单位开具的收据)。（2）合同原件或复印件一份；（3）使用单位的验收证明(需两人以上签名并盖章)（4）保证金交入时的银行回单复印件。（5）如原账户发生变更，提供说明和账户变更资料。3、项目合同签订后一周内中标方向采购方提交工作计划，经采购方审核通过且采购方收到中标方缴纳的履约保证金后支付合同总价40%，项目初验合格后支付合同总价30%，项目终验合格后支付合同余款。项目最终支付金额按照本年度财政批复为准，不足部分在下一年度支付。如财政批复原因导致采购方未按合同约定向中标方支付任何款项的，采购方不构成违约，无需向中标方承担任何责任。中标方不得就此向采购方主张任何权利或索赔。 |
| **违约责任及争议解决方式** | 如无特别说明，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** | **项目维护计划及响应情况** | 1. 要求服务工作人员对工作中涉及到的用户的数据、文件等任何资料进行保密。因工作人员的行为造成泄密等问题由中标单位承担相应的责任；
2. 对于出现紧急故障情况，中标方应承诺商务时间30分钟内响应，一般故障2小时内响应，4小时内到达现场，重大故障1小时内响应，2小时内到现场服务，4个小时内解决问题；不能修复的，12小时内提供备品、备件或备机等措施，以保证用户的正常使用。

采购需求文件中无特别说明的，所有软硬件产品要求提供原厂五年免费质保，提供原厂免费质保服务。质保期内软硬件免费质保，且免费提供最新的软件版本及特征库等升级服务。**硬件设备和商品化软件维保期从项目初验合格之日算起、定制化软件维保期从项目终验合格之日算起。** |
| **备品备件及耗材等要求** | 1. 按照采购需求文件要求提供备品备件。
2. 采购需求文件中未明确说明的，备品备件种类和数量由投标商根据所投产品自行确定。
 |
| **技术培训** | 中标方应安排技术人员对用户进行免费培训或技术指导。培训人数不少于3人，次数不少于1次，培训时间不少于4小时。培训内容主要为本项目采购的各软硬件产品，培训目标要求使用户能够独立进行日常管理和维护。对于投标文件中不合理培训内容及费用，用户在项目实际实施中不予执行的，在项目决算时对相关费用予以审减。 |
| **履约能力** | **投标人技术力量情况** | 1、 大型涉密信息系统的集成与软件开发能力，具备国家保密局颁发的涉密信息系统集成资质证书（系统集成/软件开发类），提供乙级资质证书。（2.5分）2、 CNCERT网络安全应急服务支撑单位（国家级）。（2.5分） |
| **经验或业绩要求** | 投标单位提供自2018年1月以来同类项目案例的合同复印件，每提供一个得0.5分，最高得2分。开标时提供原件备查。 |
| **实施团队** | 为保证项目规范且高效开展，投标人为本项目所配备项目经理经理进行服务，项目经理具有中国信息安全产品测评认证中心颁发的CISP证书和计算机技术与软件专业技术资格证书-信息系统管理工程师（中级）。（2分）保证项目有效的实施部署，投标人提供6人以上的实施团队，实施团队人员具有中国信息安全产品测评认证中心颁发的CISP证书。（2分）为保证项目在部署后能快速响应日常运维需求，投标人需在项目所在地提供4人以上的售后技术团队。（1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：签订合同后10个工作日内，成交供应商向采购人提交合同金额的1%作为履约保证金（或提供保函等）。

**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：项目合同签订后一周内中标方向采购方提交工作计划，经采购方审核通过且采购方收到中标方缴纳的履约保证金后支付合同总价40%，项目初验合格后支付合同总价30%，项目终验合格后支付合同余款。项目最终支付金额按照本年度财政批复为准，不足部分在下一年度支付。如财政批复原因导致采购方未按合同约定向中标方支付任何款项的，采购方不构成违约，无需向中标方承担任何责任。中标方不得就此向采购方主张任何权利或索赔。

**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**：**

**浙江省公安厅（本级）浙江省人员流动JMZK系统-信息安全防护体系-零信任安全访问能力项目**

项目编号：ZZCG2022D-GK-134（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ZZCG2022D-GK-134）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：

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： （采购编号 ）】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。

1. 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 XX工作内容 分包给（某分包供应商名称 ），（某分包供应商名称 ），具备承担XX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

1. 质量

五、价款或者报酬

六、违约责任

1. 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你公司法律责任。**

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**：**

**浙江省公安厅（本级）浙江省人员流动JMZK系统-信息安全防护体系-零信任安全访问能力项目**

项目编号：ZZCG2022D-GK-134（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**：**

**浙江省公安厅（本级）浙江省人员流动JMZK系统-信息安全防护体系-零信任安全访问能力项目**

项目编号：**ZZCG2022D-GK-134**（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）中小企业声明函（若需要，格式见附件16）；

（3）残疾人福利企业声明函（若需要，格式见附件17）；

（4）投标人针对报价需要说明的其他文件和说明（格式自拟）；

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）** | **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：