省消防救援总队国家电子政务外网接入及消防信息系统迁移项目

项目编号：ZZCG2020H-GK-112

**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)** [22](#_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)** [30](#_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：****ZZCG2020H-GK-112**

**二、公告期限：5个工作日**

**三、采购项目内容、数量及预算**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **标项** | **标项名称** | **数量** | **单位** | **预算金额(万元)** |
| **1** | **省消防救援总队国家电子政务外网接入及消防信息系统迁移项目** | **1** | **项** | **1707.1** |

**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》第二十二条和浙财采监【2013】24号《关于规范政府采购供应商资格设定及资格审查的通知》第六条规定,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：**具备工信部颁发的基础电信运营许可证，不允许联合体投标。

**五、获取采购文件：**

1 2020-08-22至 2020-09-17 09:00:00。

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

3.招标文件免费获取。

**六、投标保证金：**

投标保证金（人民币）： （空或0元为无需交纳）;

**七、投标截止时间和地点：**

投标人应于2020-09-17 09:00:00时前通过邮寄方式将投标文件密封送交到指定地点，逾期送达或未密封将予以拒收。（授权代表应当是投标人的在职正式职工）。

投标文件收件人：杨连娣，联系方式：88900116，收件地址：杭州市环城北路305号耀江发展中心三楼302会议室。（疫情期间仅接收邮寄方式递交的投标文件,因本大楼疫情管控，推荐使用中国邮政速递和顺丰快递）

**八、开标时间及地点：**

本次招标将于2020-09-17 09:00:00时整在杭州市环城北路305号耀江发展中心3A（四楼）05评标室开标。

九、本项目采用非现场投递投标文件方式进行投标，供应商询标相关事宜做如下规定：

1. 评标委员会认为需要供应商作出必要澄清或说明，将联系供应商投标文件中的授权代表询标，若无法联系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。

2.供应商应提供电子邮件或传真，评标委员会将通过电子邮件或传真方式将包含询标内容的询标记录表发送至供应商提供的电子邮件或传真。

3. 供应商须将必要澄清或说明填写在询标记录表中，填写完成按招标文件要求签字或盖章后以传真、拍照或扫描后以电子邮件方式递交。

4.本项目开评标过程中询标记录传真号码：0571-88907792；电子邮件地址：441249201@qq.com。本传真、电子邮件仅接受评标委员会要求供应商作出的必要澄清或说明，不接受其他事项。

**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） | 杨连娣 | 0571-88900116 | 0571-88907751 | 三楼通用业务采购部]） |
| 项目协办人  （B岗） | 金子超 | 0571-88907796 | 0571-88907751 |
| 部门负责人 | 程则彬 | 0571-88907721 | 0571-88907751 |
| 项目保证金 | 邵 幸 | 0571-88907705 | 0571-88907704 | 一楼（服务大厅） |
| 项目监督 | 胡晓霞 | 0571-88907768 | 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**

|  |  |
| --- | --- |
| 采购单位 | 浙江省消防救援总队 |
| 地址 | 杭州市下城区文晖路319号 |
| 咨询事项 | 采购需求等 |
| 联系人 | 方先生 |
| 联系方式 | 13857168119 |

**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 | 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。** |
| 4 | 小微企业有关政策 | 1.根据财库〔2011〕181号的相关规定，在评审时对小型和微型企业的投标报价给予6.0 %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）。属于小型和微型企业的，投标文件中投标人必须提供《小微企业声明函》，并在报价明细表中说明制造商情况。  联合体投标时，联合体各方均为小型、微型企业的，联合体视同为小型、微型企业享受政策;联合体其中一方为小型、微型企业的，联合协议中约定小型、微型企业的协议合同金额占到联合体协议合同总额30%以上的，给予联合体 (2-3%)的价格扣除，须同时提供联合体协议约定（包含小型、微型企业的协议合同份额）。  2.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）。  3.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 | 答疑与澄清 | 投标人如对招标文件有异议，应当于公告发布之日起至公告期限满第7个工作日内，以书面形式向招标采购单位一次性提出，逾期不予受理。 |
| 6 | 是否允许采购进口产品： | 不允许进口产品具体要求详见第四章招标需求各标项的对应内容。 |
| 7 | 是否允许转包与分包 | 转包：否  分包：不允许分包 |
| 8 | 是否接受联合体投标 | 标项1:不允许联合体投标  接受联合体投标的请提供联合体协议书。 |
| 9 | 是否现场踏勘 | 不组织现场踏勘  具体要求详见第四章招标需求各标项的对应内容。 |
| 10 | 是否提供演示 | 不进行演示  系统演示具体要求详见第四章招标需求各标项的对应内容。 |
| 11 | 是否提供样品 | 不要求提供样品  具体要求详见第四章招标需求各标项的对应内容。 |
| 12 | 投标文件组成 | 投标文件由资质文件、技术及商务文件、报价文件正本**各 1 份**；副本**各4份**。 |
| 13 | 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://zfcg.czt.zj.gov.cn/)发布中标公告，公告期限为1个工作日，服务台根据预留地址寄送中标通知书。 |
| 14 | 投标保证金 | 交纳：投标保证金应按《招标采购公告》六规定交纳。若一次投多个标项，只需交纳一个标项的投标保证金（按所需保证金最大额的标准交纳为准）。  退还：中标通知书发出之日起5个工作日内，未中标的投标人提供交入投标保证金时取得的第二联“供应商退款凭据”到招标方服务台办理，招标方以电汇或转账等方式退还投标保证金。 |
| 15 | 合同签订时间 | 中标通知书发出后30日内。 |
| 16 | 履约保证金 | 合同签订时，采购人按《中华人民共和国政府采购法实施条例》有关规定自行收取项目履约保证金。采购人要求中标或者成交供应商提交履约保证金的，供应商应当以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式提交。履约保证金的数额不得超过政府采购合同金额的10%。 |
| 17 | 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 |
| 18 | 投标文件有效期 | 90天 |
| 19 | 投标文件的接收 | 招标方于投标截止时间前五个工作日内接收投标文件，政府采购活动现场确认声明书（格式详见附件）应单独提供。  投标人递交投标文件时，如出现下列情况之一的，投标文件将被拒收：  1、未按规定密封或标记的投标文件；  2、由于包装不妥，在送交途中严重破损或失散的投标文件；  3、仅以非纸制文本形式的投标文件；  4、未成功办理投标人招标文件获取手续的；  5、超过投标截止时间送达的投标文件。  投标人在投标截止时间前，可以书面通知（加盖公章）招标方，对所递交的投标文件进行补充、修改或者撤回，补充、修改或者撤回的材料也均通过邮寄方式。补充、修改的内容应当按照招标文件要求签署、盖章、密封后，作为投标文件的组成部分。 |
| 20 | 招标方代理费用 | 0元 |
| 21 | 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。

**（三）投标人及委托有关说明**

1.授权代表须携带有效身份证件。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（投标文件正本用原件，副本用复印件，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.以联合体形式参加政府采购活动的，联合体各方不得再单独参加或者与其他供应商另外组成联合体参加同一合同项下的政府采购活动。

4.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。

5.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.投标人认为采购文件、招标过程或中标结果使自己的合法权益受到损害的，可以在中标结果公告期限届满之日起7个工作日内，以书面形式一次性向招标方提出质疑。

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。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一次性向招标方提出。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）投标文件的组成**

投标文件由资质文件、技术及商务文件、投标报价文件三部分组成。

**1.**资质文件

（1）投标声明书 (格式见附件，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）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）提供有效的依法缴纳税收证明（完税凭证或税务部门出具的证明）；

（5）提供有效的依法缴纳社会保障资金证明（缴纳凭证或人社部门出具的证明）；

（6）联合投标协议书（若需要）;

（7）联合投标授权委托书（若需要）;

（8）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。

**2.技术及商务文件**

（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）投标方认为需要的其他文件资料。

**3.报价文件：**

（1）投标报价明细表（格式见附件）；

（2）投标人针对报价需要说明的其他文件和说明（格式自拟）；

（3）小微企业声明函、网页证明资料（若有，格式见附件）；

（4）残疾人福利企业声明函（若有，格式见附件）。

**注：法定代表人授权委托书、投标声明书、投标报价明细表必须按招标文件格式要求正确签署并加盖投标人公章。资质文件、技术及商务文件中不得出现项目报价信息，否则将作无效标处理。**

**（二）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**。

**（三）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.中标人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。

**（四）投标文件的签署和份数、包装**

1.投标人应按本招标文件规定的格式和顺序编制、装订投标文件并标注页码，投标文件内容不完整、编排混乱或装订易脱落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.投标人应按资质文件、技术及商务文件、报价文件正本、副本规定的份数分别编制并按A4纸规格分别竖面单独装订成册，投标文件的封面应注明“正本”“副本”字样。

3.投标文件的正本需打印或用不褪色的墨水填写，投标文件正本除《投标人须知》中规定的可提供复印件外均须提供原件。副本为正本的复印件。招标方提倡双面打印或书写。

4.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。

5.投标文件不得涂改，若有修改错漏处，须加盖供应商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。

6.投标人应按资质文件、技术及商务文件、投标报价文件分类分别单独密封封装。投标文件封装后，外包装封面上应注明投标人名称、投标人地址、投标文件名称（资质文件、技术及商务文件、报价文件）、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。

**（五）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）**。

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

3.投标报价总价金额到元为止，如投标报价总价出现角、分，将被抹除。

**（六）投标保证金**

1.投标人须按规定提交投标保证金。

2.保证金形式：网银、汇票、电汇、转帐支票。

3.招标方不接受以现金支票、现金及个人转账方式交纳的保证金。

投标保证金若以网银、电汇方式交纳的,请将网银电脑打印凭证、电汇底单复印件写上所投项目名称、编号、投标联系人、联系电话，请在开标前一个工作日前到招标方服务台开收据。

4.招标方在中标通知书发出后五个工作日内退还投标保证金，供应商办理投标保证金退还时需提供收据的第二联“供应商退款凭据”。**详见浙江省政府采购网**http://zfcg.czt.zj.gov.cn/ ，位置：“首页-网上办事指南-其他-省政府采购中心财务程序-财务程序（一）”

保证金不计息。

**5.投标人有下列情形之一的，投标保证金将不予退还：**

（1）投标人在投标截止时间后撤回投标文件的；

（2）投标人在投标过程中弄虚作假，提供虚假材料的；

（3）中标人无正当理由不与采购人签订合同的；

（4）将中标项目转让给他人或者在投标文件中未说明且未经招标采购单位同意，将中标项目分包给他人的；

（5）其他严重扰乱招投标程序的。

**（七）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；

6.不同投标人的投标保证金从同一单位或者个人的账户转出。

**（八）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.未按规定交纳投标保证金的；

2.投标方未能提供合格的资格文件、投标有效期不足的；

3.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；

4.投标文件未按招标文件要求签署、盖章的；

5.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；

6.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；

7.资质文件、技术及商务文件中出现投标价格信息的、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；

8.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；

9.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；

10.投标人不接受报价文件中修正后的报价的；

11.未按本章“二、投标文件的编制”第五点投标报价要求报价的；

12.投标文件含有采购人不能接受的附加条件的；

13.投标人被视为串通投标的；

14.不符合法律、法规和本招标文件规定的其他实质性要求的。

**（九）错误修正**

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：

（一）投标文件中报价明细表内容与投标文件中相应内容不一致的，以报价明细表为准；

（二）大写金额和小写金额不一致的，以大写金额为准；

（三）单价金额小数点或者百分比有明显错位的，以报价明细表的总价为准，并修改单价；

（四）总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价按照经投标人加盖公章，或者由法定代表人或其授权的代表签字确认后产生约束力，投标人不确认的，其投标无效。

**三、开、评标程序及评标委员会的评审程序**

**（一）开标程序**

**招标方将按照招标文件规定的时间、地点和程序组织开标，无关人员不得进入开标现场。**

**1.开标会由招标方主持，主持人介绍开标现场的人员情况，宣读接收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。**

**2.对投标人的投标文件进行查验、核实，由采购人监督人员查验投标文件密封情况并签名确认。**

**3.当众拆封、清点投标文件（包括正本、副本）数量，将其中密封的报价文件现场集中封存保管等候拆封，将拆封后的商务和技术文件由现场工作人员护送至指定的评审地点。**

**4.商务和技术评审结束后，主持人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，由工作人员在评标结束后寄回无效投标人的报价文件。**

**5.拆封投标人报价文件，宣读《报价明细表》有关内容，同时当场制作并打印开标记录表，由采购人监督人员、唱标人、记录人和中心现场监督员在开标记录表上签字确认，不予确认的应说明理由。唱标结束后，由评审小组对报价的合理性、准确性等进行审查核实。**

**6.评审结束后，主持人公布中标候选供应商名单，及采购人最终确定中标或成交供应商名单的时间和公告方式等。**

**（二）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.按规定统一收缴、保存评标现场相关人员通讯工具。**

**2.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。**

**3.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《政府采购评审人员廉洁自律承诺书》及各疫情防控类承诺书。**

**4.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。**

**5.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。**

**6.采购人代表或由采购人委托的评标委员会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。**

**7.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通过电话方式进行陈述、澄清或申辩，并以传真或电子邮件方式确认记录；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。**

**8.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。**

**9.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。**

**（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.评审人员对各供应商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供应商作出必要澄清或说明的，以电话方式通知该投标人以书面形式作出澄清或说明。授权代表无法联系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。**

**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，并向中标方签发书面《中标通知书》，服务台根据预留地址寄送中标通知书。

**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，招标方作为合同签订的鉴证方。

2.中标人拖延、拒签合同的,将被扣罚投标保证金并取消中标资格。

**（二）履约保证金**

1.合同签订时，采购人按《中华人民共和国政府采购法实施条例》有关规定自行收取项目履约保证金。采购人要求中标或者成交供应商提交履约保证金的，供应商应当以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式提交。履约保证金的数额不得超过政府采购合同金额的10%。

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。

**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)

**三、评标内容及标准**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 评分类型 | 评分标准 | | 分值 |
| 1 | 报价（15分） | 项目成本构成合理、满足招标文件要求且报价最低的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算：投标报价得分=（评标基准价/投标报价）×15。 | | 0~15 |
| 2 | 技术（67分） | 投标方案的科学性、完整性、先进性 | 对本项目总体建设目标、建设需求的了解程度。 | 0~5 |
| 现有消防信息网接入政务外网传输网络改造，对现有传输网络情况的了解、传输网络改造设计技术方案的优劣性及于需求的契合程度酌情打分。 | 0~6 |
| 针对现有消防信息网接入政务外网后，实现全省网络统一管控。提供详细的网络安全设计方案。根据方案的优越性酌情打分。 | 0~6 |
| 项目的集成及实施服务方案：包括各级消防信息网接入政务外网政府侧对接集成、方案、IP地址规划、网络割接以及原A类、B类、C类系统迁移割接上线。按方案的详实、科学、合理程度酌情打分。 | 0~8 |
| 投标设备与需求的吻合程度 | 符合明确指标参数得10分。对非关键的性能指标及技术参数属负偏离或缺漏项的每项扣2分（若负偏或缺漏项5个以上的按重大偏离处理）。对性能指标、技术参数属正偏或高配的、有先进程度的正偏离每项加1分（最高分为6分），无实质性意义的正偏离不加分。 | 0~16 |
| 带宽速率提速要求 | 全省长途链路基础带宽，每提升100M带宽加2分，最高加6分；全省本地链路基础带宽，每提升100M带宽加2分，最高加8分。 | 0~14 |
| 节能环保要求 | 提供市场监管总局关于发布参与实施政府采购节能产品、环境标志产品认证机构名录的公告（2019第16号）通过《参与实施政府采购节能产品认证机构名录》认证机构认证的环境标志产品认证证书或者证书的查询网址及截图的，得1分, 节能产品认证证书或者证书的查询网址及截图的，得1分。 | 0~2 |
| 项目进度计划 | 投标人根据本项目的需求提供完整详细的项目实施计划。 | 0~2 |
| 项目组人员个人、团队能力情况（资历及业绩） | 是否具有完备的管理组织、项目实施规范和管理制度，是否有完善的质量管理体系，并能有效实施；拟投入本项目管理与实施人员的综合水平情况。 | 0~2 |
| 项目实施人员能力。担任本项目项目经理和项目组实施人员素质、技术能力、专业分布等情况，数量是否充足，配置是否合理等。 | 0~6 |
| 3 | 商务资信（18分） | 项目维护计划（驻点人员安排，定期巡检等情况）的有效性等 | | 0~3 |
| 售后服务的响应情况（对用户故障响应、处理等） | | 0~3 |
| 培训方案、计划的可行性及合理性 | | 0~2 |
| 公司技术力量情况等 | | 0~5 |
| 经验及业绩(类似项目开发成功案例) | | 0~3 |
| 投标书编制质量。 | | 0~2 |

**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:浙江省公安消防总队全省消防救援队伍国家电子政务外网接入及消防信息系统迁移项目

# 一、项目背景

根据《应急管理部科技和信息化工作领导小组办公室、国家电子政务外网管理中心关于开展国家电子政务外网接入工作的通知》（应急科信办〔2019〕8号）和《部消防救援局关于消防救援队伍国家电子政务外网接入以及消防信息系统迁移相关工作的通知》（应急消〔2019〕135号）的通知要求，结合我省现有消防信息网在网设备实际情况，在前期调研基础上，决定开展全省消防救援队伍国家电子政务外网接入及信息系统迁移工作。

## 二、建设目标

根据应急管理部通知要求，为实现部、省、市、县四级互联互通和主要业务网上办公，省消防救援总队需尽快完成政务外网接入和非涉密政务业务系统迁移工作。

基于全省消防网络和安全设备现状,经研究, 省消防救援总队信通处确立了“安全风险集中管控,敏感信息实时监测,后期网络整体升级”的建设目标，对省、市消防电子政务网进行建设、改造。

## 三、建设内容

本项目需在项目计划时间内通过全省电子政务外网建立覆盖省、市两级消防救援队伍的新消防信息网网络，并迁移相关非涉密业务应用至政务外网，实现全省消防信息网的互联互通及网上办公。铺设本地消防接入政务外网链路，并提升现有消防信息网网络带宽，完成省、市两级消防救援队伍数通设备及安全设备的采购、安装、配置、测试、验收和维保等工作。建设内容主要有：

1. **网络**：采取总队、支队两级横向接入省、市电子政务外网，由于大、中队现有条件不满足政务外网接入要求，仍通过现有竖向链路，通过市级支队接入政务外网。各级消防救援队伍向各级政府单位申请政务外网59地址段，总队及支队在边界接入防火墙上采用NAT（网络地址转换）方式将消防内网的IP地址转换成政务外网地址，完成对政务外网的访问需求。
2. **系统迁移**：本次迁移涉及总队消防救援一体化业务核心系统21个（A类），常用非核心8个（B类）；总队自建系统80个（C类）；支队核心系统每个支队5个，按总队规划要求逐步完成迁移。
3. **切割工作**：总队、支队两级采取“双网并行、逐步切割”的方式，整体卸载现有公安网电脑“一机两用”管控软件，接入政务外网。大、中队利用窗口期，通过直接切割方式，在窗口期内，由支队完成基层单位电脑终端公安网“一机两用”卸载，服务器脱网，修改系统和服务器配置参数后接入政务外网。
4. **网络设备**：统一更换总队、支队现有核心数通设备及边界防火墙。
5. **安全设备**：为实现全省网络统一管控，总队统一配备防毒墙、主机监控与审计系统、移动存储介质注册管理系统、敏感信息安全检查系统、网络接入控制系统态势感知平台和流量探针等安全设备，各支队配备防毒墙。切割后，总队将委托第三方机构对全省网络开展安全评估。

## 四、项目采购内容

省消防救援总队采购内容

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **类型** | **项目** | **数量** | **说明** |
| 1 | 服务部分 | 全省消防信息网链路费用**（核心产品）** | 五年 | 提供相应带宽链路 |
| 2 | 设备安全调试服务 | 1项 | 省消防救援总队及12消防救援支队设备安装调试及网络割接 |
| 3 | 全省消防信息网应急管理系统迁移服务 | 1项 | 省、市两级消防信息网应急管理系统（A、B、C三类）迁移至政务外网 |
| 4 | 移动办公应用系统定制开发服务 | 1项 | 针对移动办公系统在政务外网应用做对接开发及优化调整 |
| 5 | 其他服务 | 1项 | 5年巡检服务及技术故障处理服务 |
| 1 | 设备部分 | 省消防救援总队及一级消防救援支队边界防火墙 | 5台 | 总队及杭宁温金支队 |
| 2 | 二级消防救援支队边界防火墙 | 8台 | 其他支队（含义乌） |
| 3 | 省消防救援总队边界防毒墙 | 1台 |  |
| 4 | 一级消防救援支队边界防毒墙 | 4台 | 杭宁温金支队 |
| 5 | 二级消防救援支队边界防毒墙 | 8台 | 其他支队（含义乌） |
| 6 | 省消防救援总队及一级消防救援支队核心路由器 | 5台 | 总队及杭宁温金支队 |
| 7 | 二级消防救援支队核心路由器 | 8台 | 其他支队（含义乌） |
| 8 | 省消防救援总队及一级消防救援支队核心交换机 | 5台 | 总队及杭宁温金支队 |
| 9 | 二级消防救援支队核心交换机 | 8台 | 其他支队（含义乌） |
| 10 | 主机监控与审计系统 | 1套 | 省总队 |
| 11 | 移动存储介质注册管理系统 | 1套 | 省总队 |
| 12 | 敏感信息安全检查系统 | 1套 | 省总队 |
| 13 | 网络接入控制系统 | 1台 | 省总队 |
| 14 | 态势感知平台 | 1套 | 省总队 |
| 15 | 普通网闸 | 2台 | 省总队老旧设备替换 |
| 16 | 视频网闸 | 1台 | 省总队老旧设备替换 |
| 17 | 楼层交换机 | 20台 | 省总队老旧设备替换 |
| 18 | 病毒预警机 | 1台 | 省总队安全系统加固 |
| 19 | 防火墙 | 1台 | 省总队老旧设备替换 |
| 20 |  | 核心交换机 | 1台 | 大队测试设备 |
| 21 |  | 防火墙 | 1台 | 大队测试设备 |

## 五、项目进度要求

中标人在中标公示结束后1个月内完成签订合同。从中标通知书发出之日起1个月内完成全部链路铺设、设备供货及安装、配置、调试工作，6个月内完成系统迁移及网络割接工作，项目初验后进行1个月试运行，并完成项目终验工作。

## 六、本次采购内容主要技术参数和要求

## 1．省消防救援总队服务采购内容

## （1）全省消防信息网链路租用

|  |  |  |  |
| --- | --- | --- | --- |
| **电路类型** | **线路带宽** | **数量** | **用途** |
| 长途链路(基于二层技术的高带宽传输电路,如:OTN/MSTP/STN等) | 200M | 12 | 总队至各支队（除杭州）的长途链路 |
| 本地链路(基于二层技术的高带宽传输电路,（如:OTN/MSTP/STN等) | 100M | 210 | 总队至各直属单位；支队至各大中队、直属单位；绍兴基地、质检站、陆搜至绍兴支队 |
| 裸光纤 | / | 1 | 总队至杭州支队 |

## （2）设备安装调试服务

|  |  |  |
| --- | --- | --- |
| **服务名称** | **服务项** | **服务内容** |
| **设备安装调试服务** | 总队设备安装调试 | 总队设备安装、上架、调试 |
| 12支队设备安装调试 | 12支队设备安装、上架、调试 |
| 网络调试割接 | 安排网络割接实施计划，提供详细的割接实施步骤，应急预案及割接测试方法等 |

## （3）全省消防信息网应急管理系统迁移服务

|  |  |  |
| --- | --- | --- |
| **服务名称** | **服务项** | **服务内容** |
| **业务系统迁移** | 前期统计工作 | 具体内容见下 |
| 数据库进行备份、拷贝及还原等工作 |
| 系统调整方面 |
| 机构调整改名数据同步工作 |
| 应用平台搭建方面 |
| 驻场安排专人职守迁移 |

**数据量及应用系统部署方面：**前期统计工作（1个总队，12个支队），初步统计迁移一体化数据约50TB，CPU资源为656核，内存为2031G，各支队一体化数据5696GB。基础平台系统需要如下工作内容：

应用平台

操作系统Windows Server 2008 R2 SP1，做好安全策略、密码策略、服务器命名、开启远程安全维护设置、IIS角色、.NET Framework 3.5.1框架安装等。

SQL Server 2008 R2数据库安装，实例安装、用户密码设置。

JRockitJDK服务的安装和支持，环境变量的设置和验证。

weblogic安装并验证。

数据库平台

统一数据库备份计划时间。新建完整备份计划和差异备份计划并验证其可正常执行，达到统一数据库备份计划时间的和验证备份计划可用性的目的；

数据库备份

1）、完整备份：每周日0点执行；

2）、差异备份：每天0点执行。

安装上述基础平台后进行系统的部署

以综合业务系统为例正常部署系统流程：

消防信息通信传输客户端安装

基础数据平台（jcsj）安装

服务管理平台安装部署

拷贝最新应用文件：文件位置在原公安网应用服务器上，文件路径为”D:\NCISoft”文件夹

数据库全量文件：从原公安网数据库服务器导出最新备份的全量数据库文件，文件扩展名为” .bak”

添加网站

网站配置

安装”ZHYW\_XXJHService”服务

停止网站

授予”NCISoft”文件夹Users权限

修改web.config等多处配置文件

ZHYWPT01数据导入

删除数据库用户XFDB

新建数据库登陆名XFDB

1）启动网站2）系统登录3）发送邮件4）数据同步

与部局互发邮件测试

部署工作需安排一人专职，数据库拷贝和迁移恢复工作需一人专职，测试工作安排一人测试。

为以下重要的和相对较大的数据库进行备份、拷贝及还原等工作使业务系统恢复到正常状态。

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 系统类别 | 系统名称 | 数据库名称 |
| 1 | 平台类 | 基础数据平台 | jcsj |
| 2 | 服务管理系统 | fwgl |
| 3 | 信息交换系统 | xxjh |
| 4 | 工作单位与人员管理模块（OSM） | osm |
| 5 | 身份与授权管理子系统（IAM） | iam |
| 6 | 综合业务平台 | ZHYWPT01 |
| 7 | 消防监督管理系统 | XFJDGL01 |
| 8 | 消防产品质量监督管理系统 | CPJDGL01 |
| 9 | 地理信息服务平台 | bzdz/gisdb |
| 10 | 地理信息代理服务SDE服务 | sde |
| 11 | 社会公众 | 公众信件及公安网管理系统 | gzxj |
| 12 | 灭火救援 | 灭火救援业务管理系统 | mhjy |
| 13 | 指挥中心信息直报系统 | / |
| 14 | 部队管理 | \*\*管理系统 | jwgl |
| 15 | 卫生管理系统 | wsgl |
| 16 | 机关管理系统 | jggl |
| 17 | 被装管理系统 | / |
| 18 | 宣传业务系统 | xcyw |
| 19 | 装备管理系统 | zbgl |
| 20 | 政治工作系统 | zzgz |
| 21 | 营房管理系统 | yfgl |
| 22 | 财务管理系统 | cwgl |
| 23 | 审计管理系统 | ZPmaindb\_V9 |

数据库进行备份、拷贝及还原等工作：需要投入不少于高级工程师2名，中级工程师3名，迁移时间在30天内。前期需要部署测试环境，后续正式切割系统，并提供后续半年的数据同步迁移和联调工作。

系统调整方面：搭建办公内网主页、政治工作网站、后勤网站、防火网站、干部处考核网站、总队消防产品检测管理系统等迁移和调试工作；需要60天内完成。

机构调整改名数据同步工作：总队机构：15个处室1个大队，12个支队：15个处室1个车辆勤务站，机构调整339个（包括总队16个，人员2000多名，需要1周内完成。

应用平台搭建方面：重建虚拟化平台生成虚拟机和灾备系统重迁重建。后续招标完毕新设备进场，重做对网络设备和路由表的配置工作，需要45天内完成。

驻场安排专人职守迁移，负责总队所有网络分配部署工作，需要根据采购方需要对不同应用系统进行网络重组，需安排3人分工各自承担一项重要工作，保证各系统可稳定运行，故障及时解决。其中系统版块可划分为：一体化系统问题、自建系统迁移问题、数据网络及突发事件处理，工作时间约7个月。

## （4）其他服务

|  |  |  |
| --- | --- | --- |
| **服务名称** | **服务项** | **服务内容** |
| **其他服务** | 巡检服务 | 定期对总队、12个支队及210个大、中队涉及的所有设备及线路进行全面的健康性检查，对网络运行情况进行汇总，评估网络健康状况，分析网络中存在的安全隐患和薄弱环节，以便对电路故障进行预先防范，形成巡检报告提交用户。 |
| 技术支持及故障处理等服务 | 对全省总队、12个支队及210个大、中队提供专家技术支持服务（包括全面的技术咨询服务、系统性能调优服务、系统升级支持服务、资源信息管理服务、特殊事件支持服务、辅助故障支持服务、重大节假日服务），并处理全省网络故障。 |

## 2.移动办公应用系统定制开发服务要求

|  |  |  |
| --- | --- | --- |
| **服务名称** | **服务项** | **服务内容** |
| **业务系统迁移** | 软件开发 | 具体内容见下 |
| 软件运维 |
| 全省11个支队推广部署，及后期技术支持 |

### 项目背景

在2016年浙江总队已建设基于安卓平台的移动办公软件，利用消防移动接入平台将现有公安网内的桌面型应用系统延伸到手机终端上，让消防办公人员摆脱时间和空间的束缚，使信息垂手可得，实现工作效率和管理水平的全面提升。但随着消防部队的改制、系统网络的切换以及浙江省政府出台关于移动端应用接入《浙政钉》的管理规定，因此启动钉钉版移动办公软件的开发。

### 质量要求

功能：应满足浙江省消防救援总队业务需求，与消防综合业务平台实现数据对接，钉钉小程序应符合《“浙政钉”应用设计规范》中整体规范的相关规定。

性能：钉钉小程序首页完全加载小于等于3秒，首屏页面小于200K；非极端弱网环境下，应用内容加载、页面的切换时间不应超过 5 秒；

可靠：钉钉小程序访问后台服务链路应采用HTTPS协议进行加密传输；小程序白屏出现率小于0.1%；API调用成功率大于99.99%;

部署：小程序后台服务采用与消防综合业务平台一致的总队、支队两级部署模式，各采用2台服务器进行负载均衡，避免单点风险。

### 软件功能需求

钉钉版移动办公软件由消防移动办公服务系统、钉钉对接中转服务和钉钉小程序三部分组成。

消防移动办公服务系统实现与消防综合业务平台进行对接，获取相应的基础数据、业务数据向钉钉小程序提供服务。

钉钉小程序软件主要实现与消防综合业务平台的日常办公功能集成，包括首页待办提醒、公文阅办、人员和车辆的出入管理和在线邮件等功能。

钉钉对接中转服务解决政务外网的移动办公服务访问互联网的钉钉服务接口问题。

#### 消防移动办公服务系统功能

消防移动办公服务系统包括服务接口和系统维护两部分。

##### 服务接口

提供给钉钉小程序访问的WebService接口。

* 用户登录验证服务；

包括钉钉用户与办公系统用户帐号的登录绑定，每次用户的登录验证等

* 待办事项服务；

根据使用人员编号获取本人未处理的待办事项任务。

* 公文信息服务；

包括收文阅办、发文阅办、文件审批，以及收发文检索、公文接收、批办跟踪等各类公文相关的服务接口。

* 出入信息服务；

包括人员外出、车辆外出和饮酒报备等各项出入信息。

* 在线邮件；

包括邮件查阅、发送和邮件组等管理功能。

* 其他信息服务；

包括批语管理等其他信息服务。

##### 系统维护

**移动办公配置**

包括访问用户的管理、访问服务地址管理等功能。

**待办事项管理**

提供系统管理员查看全部使用人员的移动办公待办事项，提供管理员进行手工维护管理的功能。

**系统日志查询**

可查看全部使用人员在移动办公平台中的登录日志和各功能模块的操作日志等信息。

#### 钉钉小程序软件功能

钉钉小程序主要实现综合业务平台中的日常办公管理功能为主，包括首页待办提醒、公文处理、出入管理和在线邮件等功能。

##### 首页

首次使用时，办公人员打开钉钉小程序后，使用消防一体化的帐号和密码进行登录，登录验证通过后进入首页。后续使用都无需再次输入帐号和密码，直接免登录进入。

在首页中会显示当前用户尚未处理的待办件，并提供收文阅办、发文阅办、文件审批、出车审批、请销假审批、饮酒报备审批和邮件查阅的待办处理功能。

在首页还会根据当前用户所在单位显示相应的通知通告和今日值班等信息。

##### 收文阅办

对本人未处理的收文阅办进行处理，提供公文标题、公文文号、发文单位、发文日期、收文日期等信息和公文正文查阅，并显示公文流转信息和送达信息，提供个人常用批语和个人常用名单进行选择，方便快速阅办处理。

##### 发文阅办

对本人未处理的发文阅办进行处理，提供公文标题、公文文号、承办部门、承办人、签发人、发文日期、主送单位等信息和公文正文查阅，并显示公文流转信息和送达信息，提供个人常用批语和个人常用名单进行选择，方便快速阅办处理。

##### 文件审批

对本人未处理的文件审批事项进行处理，提供公文标题、起草人、起草说明、主送单位等信息和公文正文查阅，并显示公文流转信息和送达信息，提供个人常用批语和根据流程提供下一流转人员和操作方式进行选择，方便快速阅办处理。

**请销假审批**

对本人未处理的请销假审批事项进行处理，提供申请人、外出原因、外出地点、申请外出时间、申请归队时间等信息查阅，并显示流转信息和送达信息。可直接选择同意或不同意，若选择同意则根据流程发送给下一流转人员或审批通过，若选择不同意则反馈申请人。

**出车审批**

对本人未处理的出车审批事项进行处理，提供申请人、外出原因、外出地点、车牌、申请外出时间、申请归队时间等信息查阅，并显示流转信息和送达信息。流转审批人员可对申请人所申请使用的车辆和驾驶员根据实际情况进行调配调整，直接选择同意后根据流程发送给下一流转人员或审批通过，也可选择不同意，反馈申请人。

**饮酒报备审批**

对本人未处理的饮酒报备事项进行审批，提供申请人、饮酒地址、饮酒时间、陪同人员等信息查阅，并显示流转信息和送达信息。流转审批人员可根据实际情况审批，直接选择同意后根据流程发送给下一流转人员或审批通过，也可选择不同意，反馈申请人。

##### 公文处理

公文处理模块提供用户查询本人已阅收文、已阅发文、本人承办文件和批阅文件，并按当前用户的公文查阅权限级别提供本单位收文和发文的检索功能，还提供设置本人公文流转常用名单功能。

**公文接收**

有公文接收权限的人员，可接收上级来文。

**收文登记**

有公文接收权限的人员，可以进行收文登记，将公文流转给第一送达。

**已阅收文**

可查看本人已阅办处理过的收文信息，默认显示公文标题、公文文号和阅办事项等信息，并提供按公文标题、发文日期和发文单位信息项进行检索的功能。

**已阅发文**

可查看本人已阅办处理过的发文信息，并提供按公文标题、发文日期信息项进行检索的功能。

**文件审批**

可查看本人承办的或阅办处理过的文件审批信息，并提供按公文标题、起草日期和审批状态信息项进行检索的功能。

**公文检索**

可根据当前用户的公文查阅权限级别，查看本单位的收文和发文信息，并提供公文标题、收（发）文日期、发文单位等信息项的检索功能。

**常用名单**

可设置和管理本人的公文常用流转人员名单，可在收文传阅、发文传阅等模块使用

##### 外出管理

外出模块提供人员外出、车辆外出和饮酒报备相关管理功能。

**车辆外出**

车辆外出功能包括出车申请、本人申请查询和本人批阅查询。

车辆外出申请功能时需填写外出地点、用车原因、申请外出时间、申请归队时间等信息，并选择相应的审批流程发送给审批领导进行审批。

本人申请查询可查看本人历史的出车申请信息，并可根据申请的审批流转情况。系统提供了出车地点、用车人、申请日期和出车车辆等检索条件。

本人批阅查询可查看本人历史批阅的出车申请信息。

**人员外出**

人员外出包括外出申请、本人申请查询和本人批阅查询。

人员外出申请功能时需填写外出地点、外出原因、申请外出时间、申请归队时间等信息，并选择相应的审批流程发送给审批领导进行审批。

本人申请查询可查看本人历史的外出申请信息，并可根据申请的审批流转情况。系统提供了外出地点、申请人、申请日期和外出类别等检索条件，点击列表标题列可进入外出申请详细信息查看页。

本人批阅查询可查看本人历史批阅的外出申请信息。

**饮酒报备**

饮酒报备包括饮酒报备申请、本人报备查询和本人批阅查询。

饮酒报备申请功能时需填写饮酒地点、饮酒原因、申请饮酒时间等信息，并选择相应的审批流程发送给审批领导进行审批。

本人申请查询可查看本人历史的饮酒报备申请信息，并可根据申请的审批流转情况。系统提供了饮酒地点、申请人、申请日期等检索条件，点击列表标题列可进入饮酒报备申请详细信息查看页，可查看当时的申请的饮酒地点、要求饮酒时间以及相应的流转审批情况。

本人批阅查询可查看本人历史批阅的饮酒报备申请信息。

##### 在线邮件

在线邮件模块可以查看本人未阅邮件、已收邮件和已发邮件，并提供新增邮件发送功能。

**写邮件**

需填写邮件主题和正文，并可从手机中浏览选择相应的附件，也可直接进行拍照上传照片，然后从本人联系人中选择相应的收件人后进行发送。

**收件箱**

显示本人接收的邮件信息，可对已接收的邮件进行检索，提供了主题（或内容）、发件人、送达时间等检索条件，点击邮件标题可进入邮件查阅页。

**发件箱**

显示本人发送的邮件信息，并可对已发送的邮件进行检索、转发等操作。

**文件夹**

显示草稿箱、已删收件、已删发文和本人在综合业务平台中自定义的邮件文件夹。

**邮件组**

显示本人在综合业务平台中所定义的邮件组及组员，可对邮件组进行发送邮件操作。

**联系人**

显示本人在综合业务平台中所定义的内部联系人信息，可对联系人进行发送邮件操作。

##### 其他功能

还提供本人常用批语管理、跟踪领导设置等功能。

**批语管理**

可以管理本人的常用批语，方便流转审批过程无需再录入可直接点选。

**跟踪领导设置**

公文机要人员可以设置本人所服务的领导，在领导对公文阅办处理完成后，自动转发给公文机要人员，公文机要人员可以根据领导批示再进行流转和办理。

#### 钉钉中转服务软件功能

实现与互联网的钉钉服务接口的中转处理功能，包括获取钉钉用户信息、发送钉消息、钉日程管理等功能。

### 技术服务需求

#### 数据清理维护

配合全省进行网络切换（系统从消防网切换至政务外网）和系统中机构调整（取消司、政、后、防等部门），在软件正常运行后，需要对异常数据进行清理和修复18天，每天2人；同时向全省11个支队推广部署，每支队3天，每天2人。支撑总队及各支队软件操作中的问题咨询。全省11个支队推广部署，每支队3天，每天2人。

#### 两年技术支持

软件试运行结束后，根据试运行情况进行软件更新，并在全省各支队进行推广部署，并提供两年的技术支持服务，包括：7\*24小时响应，运行期间发生故障后2小时内响应，4小时内抵达用户现场，对系统进行故障诊断，经双方协商后予以实施和修复；定期访问用户，了解使用情况并对系统进行维护，提供新的技术建议；免费解答用户在系统使用过程中碰到的技术问题。

### 软件功能点清单

| **序号** | **模块** | **功能描述** | **功能点** |
| --- | --- | --- | --- |
| 1 | 服务接口 | 用户登录验证服务 | 用户登录验证 |
| 待办事项服务 | 待办事项信息 |
| 获取未处理待办事项任务 |
| 公文信息服务 | 收文阅办接口 |
| 发文阅办接口 |
| 文件审批接口 |
| 发文检索接口 |
| 公文接收接口 |
| 批办跟踪接口 |
| 出入信息服务 | 人员外出接口 |
| 车辆外出接口 |
| 饮酒报备接口 |
| 在线邮件 | 邮件查阅 |
| 发送 |
| 邮件组 |
| 其他信息服务 | 批语信息 |
| 2 | 系统维护 | 移动办公配置 | 访问用户信息 |
| 访问服务地址信息 |
| 3 | 待办事项管理 |  | 待办事项信息 |
| 查看移动办公待办事项 |
| 4 | 系统日志查询 |  | 查看登录日志 |
| 查看操作日志 |
| 系统日志信息 |
| 5 | 首页 | 收文阅办 | 收文阅办信息 |
| 显示收文流转信息 |
| 显示收文阅办送达信息 |
| 收文正文查阅 |
| 个人常用批语选择 |
| 个人常用名单选择 |
| 发文阅办 | 发文阅办信息 |
| 发文正文查阅 |
| 显示发文流转信息 |
| 显示发文阅办送达信息 |
| 文件审批 | 文件审批事项 |
| 请销假审批 | 请销假审批流程 |
| 请销假信息查阅 |
| 显示请销假流转信息 |
| 显示请销假送达信息 |
| 意见反馈 |
| 出车审批 | 出车审批流程 |
| 出车审批信息查阅 |
| 显示出车审批流转信息 |
| 显示出车审批送达信息 |
| 车辆调整 |
| 驾驶员调整 |
| 饮酒报备审批 | 饮酒报备审批流程 |
| 饮酒报备信息查阅 |
| 显示饮酒报备流转信息 |
| 显示饮酒报备送达信息 |
| 6 | 公文处理 | 公文接收 | 接收上级来文 |
| 公文接收权限 |
| 收文登记 | 收文登记 |
| 已阅收文 | 显示收文信息 |
| 收文信息 |
| 按公文标题检索 |
| 按日期检索 |
| 按发文单位信息项检索 |
| 已阅发文 | 查看发文信息 |
| 按公文标题检索 |
| 按发文日期信息项检索 |
| 已阅发文信息 |
| 公文检索 | 公文查阅权限级别 |
| 查看本单位收文信息 |
| 查看本单位发文信息 |
| 公文信息项检索 |
| 公文信息项 |
| 常用名单 | 设置公文常用流转人员名单 |
| 常用名单信息 |
| 收文传阅 |
| 发文传阅 |
| 7 | 外出管理 | 车辆外出 | 车辆外出申请 |
| 本人申请查询 |
| 检索条件信息 |
| 本人批阅查询 |
| 车辆外出信息 |
| 人员外出 | 人员外出信息 |
| 人员外出申请 |
| 查看本人历史外出申请信息 |
| 人员外出检索条件 |
| 查看本人历史批阅外出申请信息 |
| 饮酒报备 | 饮酒报备申请 |
| 查看本人历史饮酒报备申请信息 |
| 饮酒报备检索条件信息 |
| 饮酒报备申请详细信息查看页 |
| 本人历史批阅饮酒报备申请信息 |
| 8 | 在线邮件 | 写邮件 | 邮件信息录入 |
| 浏览附件 |
| 附件上传 |
| 邮件发送 |
| 收件箱 | 显示本人接收邮件信息 |
| 已接收邮件检索 |
| 收件箱信息 |
| 邮件查阅页 |
| 收件箱检索条件信息 |
| 发件箱 | 显示本人发送邮件信息 |
| 邮件检索 |
| 邮件转发 |
| 文件夹 | 显示草稿箱 |
| 显示已删收件 |
| 显示已删发文 |
| 显示邮件文件夹 |
| 文件夹信息 |
| 邮件组 | 邮件组信息 |
| 显示邮件组及组员 |
| 联系人 | 显示内部联系人信息 |
| 联系人信息 |
| 9 | 其他功能 | 批语管理 | 常用批语信息 |
| 跟踪领导设置 | 设置服务领导 |
| 公文转发 |
| 10 | 钉钉中转服务软件功能 |  | 钉钉服务接口 |
| 获取钉钉用户信息 |
| 获取发送钉消息 |
| 获取钉日程 |

## 3.相关设备采购

## （1）省消防救援总队及一级消防救援支队（杭宁温金）边界防火墙

|  |  |
| --- | --- |
| **功能类别** | **技术要求及指标** |
| 硬件架构 | 采用多核架构；设备高度≤2U |
| ▲配置需求 | 实际配置千兆电口≥8；万兆光口≥2；USB口≥2； |
| 配置SSL VPN≥100个；IPS-AV-URL功能集≥36个月； |
| 模块配置 | 实配千兆单模光模块4个，万兆多模光模块2个 |
| ▲规格性能 | 吞吐量≥8Gbps； |
| 最大并发连接数≥300万； |
| 每秒新建连接数≥8万 |
| 接口镜像 | 支持将任意接口数据完全镜像到设备自身的其他接口,用于抓包分析 |
| 状态检测包过滤 | 能够基于五元组、方向、时间、用户、用户组、应用层协议等多个元素进行访问控制 |
| 路由能力 | 支持静态路由、路由策略、策略路由、RIP、OSPF、BGP、MPLS、ISIS等路由协议； |
| 智能DNS | 支持智能DNS功能。 |
| 智能应用引流 | 支持基于P2P、web视频等应用的智能引流。 |
| 网络地址转换（NAT） | 支持全面NAT功能，对多种应用层协议支持ALG功能，包括ILS、DNS、PPTP、SIP、FTP、ICQ、RTSP等。 |
| 用户管理 | 支持用户、用户组信息的管理，可手动录入或从LDAP\AD导入，优选可以以树型结构清晰的显示用户、用户组信息。 |
| 可自定义用户认证界面风格，包括登录主页面、登录成功界面、登录失败界面等。 |
| 支持在线用户管理功能，可注销、冻结在线用户，并可查看上线用户IP\所属用户组\登录时间\在线时长\使用流量等信息。 |
| 入侵防御 | 基于特征检测，支持基于协议检测，协议自识别，支持协议异常检测，支持自定义IPS签名 |
| 病毒检测 | 支持文件型杀毒（深度扫描）引擎病毒扫描功能；可直接过滤超大文件、密码保护文件、受损文件、超解压层数文件； |
| 支持对需要扫描的文件指定扩展名、指定文件大小、指定响应方式、指定解压层数达到20层； |
| 支持基于HTTP/HTTPS/FTP的内容及病毒检测 |
| 数据安全 | 基于内容感知数据防泄露，对传输的文件和内容进行识别过滤；  20+文件还原和内容过滤，如Word、Excel、PPT、PDF等），60+文件类型过滤。 |
| 攻击防范 | 支持基于应用层协议的攻击防范包括：HTTP、HTTPS、DNS、SIP 等Flood攻击 |
| 支持流量自学习功能，可设置流量自学习时间，并自动生成DDOS攻击防范策略。 |
| 流量控制 | 支持可识别应用层协议数量≥5000种， |
| 可支持基于应用层协议设置流控策略，包括设置最大带宽、保证带宽、协议流量优先级等。 |
| 支持基于地理位置的流量分析，支持基于地理位置的流量控制,支持基于地理位置的流量统计 |
| 多出口智能选路 | 支持内嵌移动、电信、联通、教育网的IP地址表，可根据目的地址智能优选运营商链路 |
| 支持主备接口配置以及按比例分配的负载分担方式 |
| 可靠性 | 支持双机热备，可配置主主、主备方式，双机会话同步。 |
| 支持BFD链路检测，并与VRRP进行联动实现双机快速切换。 |
| 日志审计 | 支持静态环比报表功能，可以基于日、月进行流量/攻击防护/URL访问/应用阻断等的环比统计分析，对一个周期的管理策略提供依据 |
| 产品资质 | 具有公安部颁发的防火墙《计算机信息系统安全专用产品销售许可证》，提供证书复印件 |
| 具有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》，提供证书复印件 |
| 保修服务 | 原厂5年免费保修，中标后提供原厂5年质保。 |

## （2）二级消防救援支队边界防火墙（含义乌）

|  |  |
| --- | --- |
| **功能类别** | **技术要求及指标** |
| 硬件架构 | 采用多核架构；设备高度≤2U |
| ▲配置需求 | 实际配置千兆电口≥8；万兆光口≥2；USB口≥2， |
| 配置SSL VPN≥100个；IPS-AV-URL功能集≥36个月， |
| 模块配置 | 实配千兆单模光模块4个，万兆多模光模块2个 |
| ▲规格性能 | 吞吐量≥6Gbps； |
| 最大并发连接数≥300万； |
| 每秒新建连接数≥8万 |
| 接口镜像 | 支持将任意接口数据完全镜像到设备自身的其他接口,用于抓包分析 |
| 状态检测包过滤 | 能够基于五元组、方向、时间、用户、用户组、应用层协议等多个元素进行访问控制 |
| 路由能力 | 支持静态路由、路由策略、策略路由、RIP、OSPF、BGP、MPLS、ISIS等路由协议； |
| 智能DNS | 支持智能DNS功能。 |
| 智能应用引流 | 支持基于P2P、web视频等应用的智能引流。 |
| 网络地址转换（NAT） | 支持全面NAT功能，对多种应用层协议支持ALG功能，包括ILS、DNS、PPTP、SIP、FTP、ICQ、RTSP等。 |
| 用户管理 | 支持用户、用户组信息的管理，可手动录入或从LDAP\AD导入，优选可以以树型结构清晰的显示用户、用户组信息。 |
| 可自定义用户认证界面风格，包括登录主页面、登录成功界面、登录失败界面等。 |
| 支持在线用户管理功能，可注销、冻结在线用户，并可查看上线用户IP\所属用户组\登录时间\在线时长\使用流量等信息。 |
| 入侵防御 | 基于特征检测，支持基于协议检测，协议自识别，支持协议异常检测，支持自定义IPS签名 |
| 病毒检测 | 支持文件型杀毒（深度扫描）引擎病毒扫描功能；可直接过滤超大文件、密码保护文件、受损文件、超解压层数文件； |
| 支持对需要扫描的文件指定扩展名、指定文件大小、指定响应方式、指定解压层数达到20层； |
| 支持基于HTTP/HTTPS/FTP的内容及病毒检测 |
| 数据安全 | 基于内容感知数据防泄露，对传输的文件和内容进行识别过滤；  20+文件还原和内容过滤，如Word、Excel、PPT、PDF等），60+文件类型过滤。 |
| 攻击防范 | 支持基于应用层协议的攻击防范包括：HTTP、HTTPS、DNS、SIP 等Flood攻击 |
| 支持流量自学习功能，可设置流量自学习时间，并自动生成DDOS攻击防范策略。 |
| 流量控制 | 支持可识别应用层协议数量≥5000种 |
| 可支持基于应用层协议设置流控策略，包括设置最大带宽、保证带宽、协议流量优先级等。 |
| 支持基于地理位置的流量分析，支持基于地理位置的流量控制,支持基于地理位置的流量统计 |
| 多出口智能选路 | 支持内嵌移动、电信、联通、教育网的IP地址表，可根据目的地址智能优选运营商链路 |
| 支持主备接口配置以及按比例分配的负载分担方式 |
| 可靠性 | 支持双机热备，可配置主主、主备方式，双机会话同步。 |
| 支持BFD链路检测，并与VRRP进行联动实现双机快速切换。 |
| 日志审计 | 支持静态环比报表功能，可以基于日、月进行流量/攻击防护/URL访问/应用阻断等的环比统计分析，对一个周期的管理策略提供依据 |
| 产品资质 | 具有公安部颁发的防火墙《计算机信息系统安全专用产品销售许可证》，提供证书复印件 |
| 具有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》，提供证书复印件 |
| 保修服务 | 原厂5年免费保修，中标后提供原厂5年质保。 |

## （3）省消防救援总队边界防毒墙

|  |  |  |
| --- | --- | --- |
| **功能类别** | **技术指标** | **技术指标要求** |
| 硬件参数 | 产品类型 | 硬件, 产品须为国有品牌，须专业反病毒厂商产品，拥有自主知识产权 |
| 产品构架 | 产品为软硬件一体化的专业安全网关，采用X86平台的高性能应用架构设计，具有多重病毒过滤技术。 |
| 多出口 | 要求支持多路链路出口 |
| 工作环境 | 温度0-40摄氏度 湿度20-90%非凝结 |
| 平均无故障间隔时间 | ≥50，000小时 |
| 产品规格 | 2U标准机箱 |
| 硬件平台 | 要求双路多核专业网安硬件平台，保障设备处理性能 |
| 网络接口 | 6个10/100/1000BASE-T接口（支持2对Bypass接口）;支持Bypass光口，要求支持万兆和千兆光口、电口灵活扩展，最多可扩展12个光口 |
| 电源要求 | 要求冗余电源 |
| 性能参数 | 最大吞吐 | 8Gbps |
| HTTP杀毒吞吐 | ≥3Gbps |
| FTP杀毒吞吐 | ≥3Gbps |
| SMTP杀毒吞吐 | ≥3Gbps |
| POP3杀毒吞吐 | ≥3Gbps |
| 最大并发数 | 5,000,000 |
| 新增并发数 | 70,000 |
| 系统功能 | 产品成熟度 | 要求产品采用国内领先的检测过滤技术，并具有专门的安全操作系统 |
| 部署模式（提供防毒墙界面功能截图） | 要求支持旁路监听模式、透明模式等灵活的部署方式，产品即插即用；旁路监听模式支持多端口监听；透明模式支持多路透明网桥； |
| 管理方式 | 要求支持HTTPS、SSH、console方式，支持防毒墙集中管理功能。  可通过上级单位的升级中心进行每周自动升级，以保证每周最新病毒库 |
| 帐户管理 | 要求支持指定管理员管理设备（绑定IP）；支持管理员账户超时、锁定等安全保护 |
| 备份与恢复 | 要求对系统配置进行备份，恢复备份配置、恢复系统默认值 |
| 病毒过滤技术 | 病毒监测能力 | 要求具有针对国内及全球病毒监测网络，具备新病毒及时发现、处置能力及专业技术资源，保障对新病毒的有效拦截及具备先进的病毒分析技术实力 |
| 杀毒引擎 | 要求具有国内独立自主产权杀毒引擎，专业的网关病毒过滤引擎，保障防毒墙在网关过滤病毒的效率及性能 |
| 数据并行处理技术 | 要求具有并行数据处理分析技术，可以完成多链路、高流量环境的病毒过滤 |
| 病毒库特征码 | 要求具有针对国内用户的病毒库，病毒库特征码≥200万 |
| 支持协议及多端口过滤技术（提供防毒墙界面功能截图） | 要求支持SMTP、POP3、FTP和HTTP协议的双向传输病毒过滤, 并可对SMTP、POP3、FTP、HTTP等协议通过不同端口传输的数据同时具有病毒过滤功能 |
| 扩展病毒分析技术 | 要求支持对可执行、库、邮件、脚本、DOS可执行、图片格式病毒查杀 |
| 加壳病毒分析 | 要求必须支持虚拟化病毒分析等脱壳技术，对加壳病毒具备识别及阻断能力 |
| 病毒过滤策略 （提供防毒墙界面功能截图） | 要求支持多层压缩文件中的病毒过滤，可定制压缩层数和不查杀文件类型;支持对病毒文件进行隔离和拥有对未知病毒识别及阻断能力 |
| 恶意网站拦截 | 要求恶意网站URL数量≥2000万 |
| 病毒库升级 | 要求支持在线自动、手动方式升级，局域网升级 |
| 要求在国内有自主的分布式病毒库升级服务器，保障防毒墙设备病毒库升级的可持续性 |
| 入侵防御 | 支持对各种蠕虫病毒攻击的防御。 |
| 双归属链路 | 要求支持对双归属链路环境的支持，可以满足非对称路由网络环境的需求。 |
| 非代理应用层杀毒技术 | 要求保证不改变经过防毒墙数据的任何特征，做到“透明代理”更加透明。 |
| 半连接杀毒技术 | 要求具备对网络中半连接的数据进行病毒查杀的功能。 |
| 白名单配置管理 | 要求支持自定义URL白名单，对访问网址不进行病毒过滤 |
| 要求支持自定义IP地址(范围)白名单，对特定的IP地址不进行病毒过滤 |
| 日志管理 | 日志管理 | 要求提供系统日志、病毒日志、隔离日志、管理日志等 |
| 日志报表 | 要求对详细病毒日志查询及日志统计，并支持日、周、月、季、年、自定义等日志报表功能，可发送日志信息给管理员 |
| 远程日志 | 要求支持SYSLOG、MYSQL远程日志服务 |
| 防毒墙资质 | 产品  资质 | 具有公安部安全产品销售许可证书；  具有计算机软件著作权登记证书；  具有中国信息安全测评信息技术产品安全评估技术报告，级别不低于EAL1级(含EAL1) |
| 其他 | 保修服务 | 原厂5年免费保修，中标后提供原厂5年质保。 |

## （4）一级消防救援支队边界防毒墙（杭宁温金）

|  |  |  |
| --- | --- | --- |
| 功能类别 | 技术指标 | 技术指标要求 |
| 硬件参数 | 产品类型 | 硬件, 产品必须为国有品牌，必须专业反病毒厂商产品，拥有自主知识产权， |
| 产品构架 | 产品为软硬件一体化的专业安全网关，采用X86平台的高性能应用架构设计，具有多重病毒过滤技术。 |
| 多出口 | 要求支持多路链路出口 |
| 工作环境 | 温度0-40摄氏度 湿度20-90%非凝结 |
| 平均无故障间隔时间 | ≥50，000小时 |
| 产品规格 | 2U标准机箱 |
| 硬件平台 | 要求双路多核专业网安硬件平台，保障设备处理性能 |
| 网络接口 | 6个10/100/1000BASE-T接口（支持2对Bypass接口）;支持Bypass光口，要求支持万兆和千兆光口、电口灵活扩展，最多可扩展12个光口 |
| 电源要求 | 要求冗余电源 |
| 性能参数 | 最大吞吐 | 7Gbps |
| 最大并发数 | 2,000,000 |
| 新增并发数 | 42,000 |
| 系统功能 | 产品成熟度 | 要求产品采用国内领先的检测过滤技术，并具有专门的安全操作系统 |
| ▲部署模式（提供防毒墙界面功能截图） | 要求支持旁路监听模式、透明模式等灵活的部署方式，产品即插即用；旁路监听模式支持多端口监听；透明模式支持多路透明网桥； |
| 管理方式 | 要求支持HTTPS、SSH、console方式，支持防毒墙集中管理功能。  ▲可通过上级单位的升级中心进行每周自动升级，以保证每周最新病毒库 |
| 帐户管理 | 要求支持指定管理员管理设备（绑定IP）；支持管理员账户超时、锁定等安全保护 |
| 备份与恢复 | 要求对系统配置进行备份，恢复备份配置、恢复系统默认值 |
| 病毒过滤技术 | 病毒监测能力 | 要求具有针对国内及全球病毒监测网络，具备新病毒及时发现、处置能力及专业技术资源，保障对新病毒的有效拦截及具备先进的病毒分析技术实力 |
| 杀毒引擎 | 要求具有国内独立自主产权杀毒引擎，专业的网关病毒过滤引擎，保障防毒墙在网关过滤病毒的效率及性能 |
| 数据并行处理技术 | 要求具有并行数据处理分析技术，可以完成多链路、高流量环境的病毒过滤 |
| 病毒库特征码 | 要求具有针对国内用户的病毒库，病毒库特征码≥200万 |
| 支持协议及多端口过滤技术（提供防毒墙界面功能截图） | 要求支持SMTP、POP3、FTP和HTTP协议的双向传输病毒过滤, 并可对SMTP、POP3、FTP、HTTP等协议通过不同端口传输的数据同时具有病毒过滤功能 |
| 扩展病毒分析技术 | 要求支持对可执行、库、邮件、脚本、DOS可执行、图片格式病毒查杀 |
| 加壳病毒分析 | 要求必须支持虚拟化病毒分析等脱壳技术，对加壳病毒具备识别及阻断能力 |
| 病毒过滤策略 （提供防毒墙界面功能截图） | 要求支持多层压缩文件中的病毒过滤，可定制压缩层数和不查杀文件类型;支持对病毒文件进行隔离和拥有对未知病毒识别及阻断能力 |
| 恶意网站拦截 | 要求恶意网站URL数量≥2000万 |
| 病毒库升级 | 要求支持在线自动、手动方式升级，局域网升级 |
| 要求在国内有自主的分布式病毒库升级服务器，保障防毒墙设备病毒库升级的可持续性 |
| 入侵防御 | 支持对各种蠕虫病毒攻击的防御。 |
| 双归属链路 | 要求支持对双归属链路环境的支持，可以满足非对称路由网络环境的需求。 |
| 非代理应用层杀毒技术 | 要求保证不改变经过防毒墙数据的任何特征，做到“透明代理”更加透明。 |
| 白名单配置管理 | 要求支持自定义URL白名单，对访问网址不进行病毒过滤 |
| 要求支持自定义IP地址(范围)白名单，对特定的IP地址不进行病毒过滤 |
| 日志管理 | 日志管理 | 要求提供系统日志、病毒日志、隔离日志、管理日志等 |
| 日志报表 | 要求对详细病毒日志查询及日志统计，并支持日、周、月自定义等日志报表功能，可发送日志信息给管理员 |
| 远程日志 | 要求支持SYSLOG远程日志服务 |
| 防毒墙资质 | 产品资质 | 具有公安部安全产品销售许可证书；  具有计算机软件著作权登记证书；  具有中国信息安全测评信息技术产品安全评估技术报告，级别不低于EAL1级(含EAL1) |
| 其他 | 保修服务 | 原厂5年免费保修，中标后提供原厂5年质保。 |

## （5）二级消防救援支队边界防毒墙（含义乌）

|  |  |  |
| --- | --- | --- |
| 功能类别 | 技术指标 | 技术指标要求 |
| 硬件参数 | 产品类型 | 硬件, 产品必须为国有品牌，必须专业反病毒厂商产品，拥有自主知识产权， |
| 产品构架 | 产品为软硬件一体化的专业安全网关，采用X86平台的高性能应用架构设计，具有多重病毒过滤技术。 |
| 多出口 | 要求支持多路链路出口 |
| 工作环境 | 温度0-40摄氏度 湿度20-90%非凝结 |
| 平均无故障间隔时间 | ≥50，000小时 |
| 产品规格 | 1U标准机箱 |
| 硬件平台 | 要求双路多核专业网安硬件平台，保障设备处理性能 |
| 网络接口 | 1.10/100/1000BASE-T接口：6个（支持2对Bypass接口） |
| 电源要求 | 要求ATX电源(250W) |
| 性能参数 | 最大吞吐 | ≥6Gbps |
| 最大并发数 | 1800,000 |
| 新增并发数 | 38,000 |
| 系统功能 | 产品成熟度 | 要求产品采用国内领先的检测过滤技术，并具有专门的安全操作系统 |
| ▲部署模式（提供防毒墙界面功能截图） | 要求支持旁路监听模式、透明模式等灵活的部署方式，产品即插即用；旁路监听模式支持多端口监听；透明模式支持多路透明网桥。 |
| 管理方式 | 要求支持HTTPS、SSH、console方式，支持防毒墙集中管理功能。  ▲可通过上级单位的升级中心进行每周自动升级，以保证每周最新病毒库 |
| 帐户管理 | 要求支持指定管理员管理设备（绑定IP）；支持管理员账户超时、锁定等安全保护 |
| 备份与恢复 | 要求对系统配置进行备份，恢复备份配置、恢复系统默认值 |
| 病毒过滤技术 | 病毒监测能力 | 要求具有针对国内及全球病毒监测网络，具备新病毒及时发现、处置能力及专业技术资源，保障对新病毒的有效拦截及具备先进的病毒分析技术实力 |
| 杀毒引擎 | 要求具有国内独立自主产权杀毒引擎，专业的网关病毒过滤引擎，保障防毒墙在网关过滤病毒的效率及性能 |
| 数据并行处理技术 | 要求具有并行数据处理分析技术，可以完成多链路、高流量环境的病毒过滤 |
| 病毒库特征码 | 要求具有针对国内用户的病毒库，病毒库特征码≥200万 |
| 支持协议及多端口过滤技术（提供防毒墙界面功能截图） | 要求支持SMTP、POP3、FTP和HTTP协议的双向传输病毒过滤, 并可对SMTP、POP3、FTP、HTTP等协议通过不同端口传输的数据同时具有病毒过滤功能 |
| 扩展病毒分析技术 | 要求支持对可执行、库、邮件、脚本、DOS可执行、图片格式病毒查杀 |
| 加壳病毒分析 | 要求必须支持虚拟化病毒分析等脱壳技术，对加壳病毒具备识别及阻断能力 |
| 病毒过滤策略（提供防毒墙界面功能截图） | 要求支持多层压缩文件中的病毒过滤，可定制压缩层数和不查杀文件类型;支持对病毒文件进行隔离和拥有对未知病毒识别及阻断能力 |
| 恶意网站拦截 | 要求恶意网站URL数量≥2000万 |
| 病毒库升级 | 要求支持在线自动、手动方式升级，局域网升级 |
| 要求在国内有自主的分布式病毒库升级服务器，保障防毒墙设备病毒库升级的可持续性 |
| 入侵防御 | 支持对各种蠕虫病毒攻击的防御。 |
| 双归属链路 | 要求支持对双归属链路环境的支持，可以满足非对称路由网络环境的需求。 |
| 非代理应用层杀毒技术 | 要求保证不改变经过防毒墙数据的任何特征，做到“透明代理”更加透明。 |
| 白名单配置管理 | 要求支持自定义URL白名单，对访问网址不进行病毒过滤 |
| 要求支持自定义IP地址(范围)白名单，对特定的IP地址不进行病毒过滤 |
| 日志管理 | 日志管理 | 要求提供系统日志、病毒日志、隔离日志、管理日志等 |
| 日志报表 | 要求对详细病毒日志查询及日志统计，并支持日、周、月自定义等日志报表功能，可发送日志信息给管理员 |
| 远程日志 | 要求支持SYSLOG远程日志服务 |
| 防毒墙资质 | 产品  资质 | 具有公安部安全产品销售许可证书；  具有计算机软件著作权登记证书；  具有国家信息安全测评信息技术产品安全评估技术报告，级别不低于EAL1级(含EAL1) |
| 其他 | 保修服务 | 原厂5年免费保修，中标后提供原厂5年质保。 |

## （6）省消防救援总队及一级消防救援支队（杭宁温金）核心路由器

|  |  |
| --- | --- |
| **功能类别** | **技术要求及指标** |
| 体系架构 | 支持多核CPU |
| 非堆叠架构 |
| 主控冗余 | 支持主控冗余 |
| 电源冗余 | 支持电源冗余，电源≥2个 |
| 热插拔 | 电源，风扇，板卡高可靠支持热插拔，不需要配置命令 |
| 整机高度 | 整机高度≤4U |
| ▲性能参数 | 包转发能力≥60Mpps； |
| ▲固定接口 | 10个GE口+2个10GE口（以上所有端口均为三层路由口)提供官网截图和产品彩页证明 |
| 模块配置 | 实配千兆单模光模块4个 |
| 内存 | 内存≥2GB |
| 基础功能 | DHCP server/client/relay，PPPoE server/client，NAT，子接口管理 |
| 局域网 | IEEE 802.1P，IEEE 802.1Q，IEEE 802.3 ，VLAN管理，VLAN聚合，MAC管理，STP/RSTP/MSTP等 |
| IPV4单播路由 | 路由策略，静态路由，RIP，OSPF，IS-IS，BGP |
| IPV6单播路由 | 静态路由，路由策略， RIPng，OSPFv3，IS-ISv6，BGP4+ |
| IPV6基本功能 | IPv6 ND，IPv6 PMTU，IPv6 FIB，IPv6 ACL，ICMPv6，DNSv6，DHCPv6 |
| IPV6隧道技术 | 手工隧道，自动隧道，GRE隧道，6over4隧道，6to4，ISATAP |
| 组播 | IGMP V1/V2/V3，PIM SM，PIM DM，MSDP，MBGP，IPv6 PIM，MLD |
| MPLS | LDP，MPLS L3 VPN，VLL，PWE3，静态LSP，动态LSP，IP FRR，LDP FRR，TE FRR |
| VPN | IPsec VPN，GRE VPN，L2TP |
| QoS | Diffserv模式，MPLS QoS，优先级映射，流量监管（CAR），流量整形，拥塞避免，拥塞管理，HQoS，MQC（流分类，流行为，流策略），端口三级调度和三级整形（Hierarchical QoS） |
| 安全 | ACLv4/v6，基于域的状态防火墙，802.1x认证，MAC认证，Portal认证，AAA，RADIUS，HWTACACS，PKI，广播风暴抑制，ARP安全，ICMP防攻击，攻击源追踪，国密算法， |
| 管理维护 | 升级管理，设备管理，Web网管，GTL，SNMP（v1/v2c/v3），RMON，NTP，CLI， |
| 保修服务 | 原厂5年免费保修，中标后提供原厂5年质保。 |

## （7）二级消防救援支队核心路由器（含义乌）

| **功能类别** | **技术要求及指标** |
| --- | --- |
| 体系架构 | 支持多核CPU |
| 非堆叠架构 |
| 电源冗余 | 支持电源冗余，电源≥2个 |
| 热插拔 | 电源，风扇，板卡高可靠支持热插拔，不需要配置命令 |
| 整机高度 | 整机高度≤2U |
| ▲性能参数 | 包转发能力≥25Mpps； |
| ▲固定接口 | 6\*GE口（以上所有端口均为三层路由口)  提供官网截图和产品彩页证明 |
| 模块配置 | 实配千兆单模光模块4个 |
| 内存 | 内存≥2GB |
| 基础功能 | DHCP server/client/relay，PPPoE server/client，NAT，子接口管理 |
| 局域网 | IEEE 802.1P，IEEE 802.1Q，IEEE 802.3 ，VLAN管理，VLAN聚合，MAC管理，STP/RSTP/MSTP，SEP等 |
| IPV4单播路由 | 路由策略，静态路由，RIP，OSPF，IS-IS，BGP |
| IPV6单播路由 | 静态路由，路由策略， RIPng，OSPFv3，IS-ISv6，BGP4+ |
| IPV6基本功能 | IPv6 ND，IPv6 PMTU，IPv6 FIB，IPv6 ACL，ICMPv6，DNSv6，DHCPv6 |
| IPV6隧道技术 | 手工隧道，自动隧道，GRE隧道，6over4隧道，6to4，ISATAP |
| 组播 | IGMP V1/V2/V3，PIM SM，PIM DM，MSDP，MBGP，IPv6 PIM，MLD |
| MPLS | LDP，MPLS L3 VPN，VLL，PWE3，静态LSP，动态LSP，IP FRR，LDP FRR，TE FRR |
| VPN | IPsec VPN，GRE VPN，L2TP |
| QoS | Diffserv模式，MPLS QoS，优先级映射，流量监管（CAR），流量整形，拥塞避免，拥塞管理，HQoS，MQC（流分类，流行为，流策略），端口三级调度和三级整形（Hierarchical QoS） |
| 安全 | ACLv4/v6，基于域的状态防火墙，802.1x认证，MAC认证，Portal认证，AAA，RADIUS，HWTACACS，PKI，广播风暴抑制，ARP安全，ICMP防攻击，攻击源追踪，国密算法， |
| 管理维护 | 升级管理，设备管理，Web网管，GTL，SNMP（v1/v2c/v3），RMON，NTP，CLI， |
| 保修服务 | 原厂5年免费保修，中标后提供原厂5年质保。 |

## （8）省消防救援总队及一级消防救援支队（杭宁温金）核心交换机

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| ▲性能 | 交换容量≥52Tbps，包转发率≥7000Mpps（若以上规格官网有两个值，则以最小值为准，提供官网截图证明）； |
| ▲配置要求 | 实配冗余主控，支持独立交换网板，业务板卡≥8，电源数量≥2个； |
| 实配千兆光口≥28个，万兆光接口≥4个； |
| 实配千兆多模模块8个，万兆多模模块4个； |
| 实配IPv6功能授权； |
| 支持无线控制器功能； |
| 二层功能 | 支持IEEE 802.1d(STP)、 802.w(RSTP)、 802.1s(MSTP)；  支持VLAN内端口隔离；  支持DHCP Client, DHCP Server，DHCP Relay； |
| IP路由 | 支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6；  支持GR for OSPF/IS-IS/BGP； |
| 可靠性 | 要求支持真实业务流的实时检测技术，秒级快速故障定位，非常规模拟业务流检测方式； |
| 支持G.8032标准以太环网协议，倒换时间≤50ms， |
| 支持硬件BFD/OAM，3.3ms稳定均匀发包检测，提高设备的可靠性 |
| 虚拟化技术 | 支持纵向虚拟化技术 |
| QoS | 交换机每端口200ms大缓存； |
| 支持5级H-QoS； |
| 用户管理 | 支持802.1X、MAC、Portal等认证方式； |
| 绿色节能 | 通过国际绿色产品认证，在环保、回收、节能、碳足迹等方面严格符合国际标准 |
| 资质 | 提供工信部入网证书 |
| 投标产品须是国内外主流厂商产品 |
| 保修服务 | 原厂5年免费保修，中标后提供原厂5年质保。 |

## （9）二级消防救援支队核心交换机（含义乌）

|  |  |
| --- | --- |
| **功能类别** | **技术要求及指标** |
| ▲性能 | 交换容量≥19Tbps，包转发率≥2800Mpps（若以上规格官网有两个值，则以最小值为准）； |
| ▲配置要求 | 实配冗余主控，业务板卡≥6，电源数量≥2个； |
| 实配万兆光接口≥4个，千兆光接口≥28个； |
| 每台设备实配千兆单模模块8个，万兆多模模块4个； |
| 实配IPv6功能授权； |
| 二层功能 | 支持IEEE 802.1d(STP)、 802.w(RSTP)、 802.1s(MSTP)  支持VLAN内端口隔离  支持DHCP Client, DHCP Server，DHCP Relay；  支持整机MAC地址≥1M；MAC学习速率>8000/s |
| IP路由 | 支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6；  支持GR for OSPF/IS-IS/BGP；  支持整机ARP表项≥256K；ARP学习速率≥1000/s |
| 可靠性 | 要求支持真实业务流的实时检测技术，秒级快速故障定位，非常规模拟业务流检测方式 |
| 支持G.8032开放环或SEP、REP半环协议,可与其他厂商设备混合组网，要求倒换时间≤50ms。 |
| 支持BFD/OAM，遵循协议标准，3.3ms稳定均匀发包检测，50ms内完成故障倒换,保证设备高可靠性 |
| 虚拟化技术 | 支持纵向虚拟化技术 |
| QoS | 支持GE/10GE端口200ms大缓存，提供官网截图证明 |
| 支持5级H-QoS |
| 增值业务 | 要求本次采购设备支持硬件级别无线控制器； |
| 支持防火墙插卡； |
| 支持IPSEC板卡； |
| 用户管理 | 支持802.1X、MAC、Portal等认证方式 |
| 支持基于流量、DAA目的地址和时长计费方式 |
| 资质要求 | 提供工信部入网证书 |
| 投标产品须是国内外主流厂商产品 |
| 保修服务 | 原厂5年免费保修，中标后提供原厂5年质保。 |

## （10）主机监控与审计系统

|  |  |  |
| --- | --- | --- |
| **指标项** | | **产品性能参数和要求** |
| 总体要求 | 产品资质 | 1）产品须获得中华人民共和国公安部的《计算机信息系统安全专用产品销售许可证》；  2）产品须具有《计算机软件著作权登记证书》；  3）投标产品具有公安部信息安全产品检测中心出具的检验报告 |
| 运行环境 | 1）系统必须采用B/S架构，管理员只需浏览器即可连接到系统进行各种操作。  2）系统必须运行在经安全加固的专用Linux操作系统之上。  3）产品要求集成数据库，无须再独立安装数据库系统，亦无须对数据库进行专门的维护。 |
| 使用界面 | 1）系统必须采用基于浏览器的用户界面，至少支持IE、Chrome。  2）为了适应不同用途，用户可以对标题、LOGO、背景进行调整。 |
| 性能指标 | 设备总量：支持10000台注册终端的管控。 |
| 部署 | 部署方式 | 支持单级部署和级联部署。 |
| 功能要求 | 客户端 | 1）支持与数字证书捆绑注册，能获取数字证书的信息；  2）支持带界面注册、不带界面注册静默注册、不带界面有进度有提醒注册；  3）支持托盘可见或隐藏；  4）终端代理软件提供最小化安装包，原则上安装包小于5Mb。 |
| 工作台 | 1）支持安全指标展示，并可通过模块权限分配及技术支持中心个性化配置需要展示的指标项，包括：注册率、杀毒软件覆盖率、补丁打全率、口令异常设备；  2）支持查看安全指标的波动因素；  3）支持查看注册率、杀毒软件覆盖率、补丁打全率的区域排名情况；  4）提供管理员日常工作的统一展示及快捷入口，包含：设备异常、注册审核、应用行为；  4）支持书签栏管理并通过书签快捷进入对应菜单；  5）支持系统异常检测，包含服务器CPU使用率、服务器内存使用率、系6统所在磁盘空间、上级通信状态；  6）支持级联区域监测，包含下级区域的WEB及管控中心状态； |

## （11）移动存储介质注册管理系统

|  |  |  |
| --- | --- | --- |
| **指标项** | | **产品性能参数和要求** |
| 总体要求 | 产品资质 | 1）产品须获得中华人民共和国公安部的《计算机信息系统安全专用产品销售许可证》；  2）产品须具有《计算机软件著作权登记证书》；  3）投标产品具有公安部信息安全产品检测中心出具的检验报告 |
| 运行环境 | 1）系统必须采用B/S架构，管理员只需浏览器即可连接到系统进行各种操作。  2）系统必须运行在经安全加固的专用Linux操作系统之上。  3）产品要求集成数据库，无须再独立安装数据库系统，亦无须对数据库进行专门的维护。 |
| 使用界面 | 1）系统必须采用基于浏览器的用户界面，至少支持IE、Chrome。  2）为了适应不同用途，用户可以对标题、LOGO、背景进行调整。  3）系统必须与主机监控与审计系统整合至一个统一风格的用户界面，只需一次登录，即可执行各种操作。 |
| 管理范围 | 涵盖移动硬盘、U盘、SD卡类介质。 |
| 性能指标 | 设备总量：支持10000台注册终端的管控。 |
| 部署 | 部署方式 | 支持单级部署和级联部署。 |
| 功能要求 | 客户端 | 1）支持与数字证书捆绑注册，能获取数字证书的信息；  2）支持带界面注册、不带界面注册静默注册、不带界面有进度有提醒注册；  3）支持托盘可见或隐藏； |
| 移动存储管控 | 普通介质 | 1）注册介质统计：根据介质类型统计已注册已审核的普通介质数；  2）待审核介质：查询需要审核的介质和有“介质管理”权限的用户可以对介质进行审核操作，支持按注册人、介质类型、注册时间查询，展示内容包含：介质注册人、所属部门、联系电话、介质类型、区域编号、产品名称、产品容量、注册时间；  3）注册介质查询：查询注册介质以及介质的使用日志，支持按照介质类型、介质状态（已注册已审核/已注销/吊销）、介质编号查询注册介质，展示内容包含：介质注册人、所属部门、联系电话、介质类型、区域编号、介质编号、介质状态、产品名称、产品容量、注册时间，点击查看使用介质使用日志，有“介质管理”权限的用户可以对介质进行吊销和取消吊销的操作；  4）终端设备介质使用日志：查询使用介质的终端设备以及终端设备上介质的使用日志。 |
| 安全U盘 | 1）注册介质统计：根据介质类型分别统计已注册已审核的安全U盘数；  2）注册介质查询：查询注册介质以及介质的使用日志，支持按注册人、介质类型、注册时间查询，展示内容包含：介质注册人、所属部门、介质类型、厂商名称、介质编号、注册时间、U盘状态，点击查看具体使用日志；  3）注册介质统计（专用版）：统计类型和方法同注册介质统计，专用版的区别为针对特殊行业或有特殊需求而做的安全U盘，故区别于普通U盘；  4）注册介质查询（专用版）：同注册介质查询，专用版的区别为针对特殊行业或有特殊需求而做的安全U盘，故区别于普通U盘。 |
| 未注册介质使用控制 | 根据配置规则控制普通未注册介质在内网中的使用权限，在内网使用时审计介质与介质内文件操作等。 |
| 自主注册介质控制 | 控制介质自主注册的方式、数字证数的个数、介质的类型以及介质是否需要审核和需要审核的介质的类型。 |
| 光驱和安全U盘控制 | 控制光驱和安全U盘的使用权限，使用时审计介质与介质内文件操作。 |
| 介质编号控制 | 根据介质编号控制普通已注册介质在内网中的使用权限，包括拒绝使用、读写使用、只读使用、只写使用、只读能删除，审计介质内的文件操作，包括读取、写入、新建、删除、改名，及介质接入、移除动作。 |
| 分组名称控制 | 根据分组名称控制普通已注册介质在内网中的使用权限，包括拒绝使用、读写使用、只读使用、只写使用、只读能删除，审计介质内的文件操作，包括读取、写入、新建、删除、改名，及介质接入、移除动作。 |
| 区域编号控制 | 根据区域编号控制普通已注册介质在内网中的使用权限，包括拒绝使用、读写使用、只读使用、只写使用、只读能删除，审计介质内的文件操作，包括读取、写入、新建、删除、改名，及介质接入、移除动作。 |
| 硬件ID控制 | 根据硬件ID控制普通已注册介质在内网中的使用权限，包括拒绝使用、读写使用、只读使用、只写使用、只读能删除，审计介质内的文件操作，包括读取、写入、新建、删除、改名，及介质接入、移除动作。 |
| 移动介质分组配置 | 配合分组名称控制策略使用，对各种介质类型按需进行分组。 |
| 移动介质外网报警 | 配置内部介质在外网使用时报警日志上传的服务器地址。 |
| 数字证书组织结构配置 | 配合注册模式中的数字证书捆绑注册使用，由于数字证书的组织机构更新不及时，固此处可配置最新的组织机构，注册时使用该组织机构进行注册。 |

## （12）敏感信息安全检查系统

|  |  |  |
| --- | --- | --- |
| **指标项** | | **产品性能参数和要求** |
| 总体要求 | 产品资质 | 1）产品须获得中华人民共和国公安部的《计算机信息系统安全专用产品销售许可证》；  2）产品须具有《计算机软件著作权登记证书》；  3）产品具有公安部信息安全产品检测中心出具的检验报告； |
| 运行环境 | 1）系统必须采用B/S架构，管理员只需浏览器即可连接到系统进行各种操作。  2）系统必须运行在经安全加固的专用Linux操作系统之上。  3）产品要求集成数据库，无须再独立安装数据库系统，亦无须对数据库进行专门的维护。 |
| 使用界面 | 1）系统必须采用基于浏览器的用户界面，至少支持IE、Chrome。  2）为了适应不同用途，用户可以对标题、LOGO、背景进行调整。  3）系统必须与主机监控与审计系统整合至一个统一风格的用户界面，只需一次登录，即可执行各种操作。 |
| 管理范围 | 涵盖磁盘、移动存储介质上的文件。 |
| 性能指标 | 设备总量：支持10000台注册终端的管控。 |
| 部署 | 部署方式 | 支持单级部署和级联部署。 |
| 功能要求 | 客户端 | 1）支持与数字证书捆绑注册，能获取数字证书的信息；  2）支持带界面注册、不带界面注册静默注册、不带界面有进度有提醒注册；  3）支持托盘可见或隐藏； |
| 敏感信息检查 | 敏感信息监管 | 1）通过智能检查（文档结构检查）及知识库检查（内容特征）发现敏感信息日志，并支持按关键字过滤；  2）对发现的敏感信息进行学习，智能完善文件识别库，发现相似文件，同时支持手动提取知识库；  3）支持按照文件名、IP地址、登录账户、处理状态、密级标识、最小相似度等查询监管日志；展示内容包含：文件名、文件路径、文件大小、设备基本属性信息、登录账户、相似度、密级标识、审查标记、处理状态、最早发现时间、最后发现时间；  4）支持按设备查询监管日志，展示内容包含：设备基本属性信息、文档数，点击文档数展示详情；  5）监管日志的操作包含：相似文件查询、文件片段查看、提取文件、审查文件、审查相似文件、终端提醒、提取知识。 |
| 知识库管理 | 1）支持将已发现的敏感信息，相似度≥89且符合知识提取的文件自动提取知识库；  2）支持将已发现的敏感信息并符合知识提取的文件手动提取知识库；  3）支持手动导入知识库，导入的内容来源于：  下载并运行知识库提取工具；  指定待学习的敏感文件路径；  学习完成后导出知识库； |
| 敏感信息检查 | 1）通过关键字检查方式依据配置的任务检查敏感信息文件；  支持根据任务查看敏感信息详情，展示内容包含：文件名、文件路径、文件大小、关键字、审查标记、设备基本属性信息、登录账户等；  2）支持根据区域或部门统计近5次的检查任务，包含：检查设备数、敏感文件数、敏感设备数、设备违规率。 |
| 介质接入检查 | 对接入计算机的移动存储介质（U盘、移动硬盘）执行关键字检查；支持按文件名、关键字、发现时间、IP地址等查询敏感信息日志；展示内容包含：设备基本属性信息、关键字、文件名称、文件路径、发现时间。 |
| 普通介质拷贝检查 | 对普通介质拷贝的文件进行敏感信息关键字检查；支持按审计结果（不处理/拒绝）、所属部门、更新时间查询；展示内容包含：IP地址、责任人、所属部门、审计结果、文件名称、文件内容等。 |
| 安全U盘拷贝检查 | 对安全U盘拷贝的文件进行敏感信息关键字检查；支持按审计结果（不处理/拒绝）、所属部门、更新时间查询；展示内容包含：IP地址、责任人、所属部门、审计结果、文件名称、文件内容等。 |

## （13）网络接入控制系统

|  |  |  |
| --- | --- | --- |
| **指标项** | | **规格要求** |
| 设备参数 | 硬件规格 | 采用标准机架式的1U硬件设备，全内置封闭式结构，专用安全加固Linux操作系统 |
| 硬件参数 | CPU：i7及以上处理器；内存容量≥8G DDR3；硬盘容量≥128G |
| 网络接口 | 6个千兆电口，2个万兆光口 |
| 性能指标 | QPS（TPS）： ≥2000个（IP数量）  并发处理数： ≥100万个数据包/秒  最大镜像流量：≥4Gbps |
| 整体要求 | 产品资质 | 投标产品具有计算机软件著作权证书 |
| 投标产品具有公安部计算机信息系统安全专用产品销售许可证 |
| 投标产品具有公安部信息安全产品检测中心出具的检验报告。 |
| 部署要求 | 以旁路控制技术为主，秉承不改变现有网络结构的特性，为用户解决终端入网的合规性要求。 |
| 支持单点部署和集群部署模式，用于满足通过部署多套产品对多个网络汇聚节点进行监测并集中管理的需求。 |
| 使用界面 | 1）系统必须采用基于浏览器的用户界面，至少支持IE、Chrome。  2）为了适应不同用途，用户可以对标题、LOGO、背景进行调整。  3）系统必须与主机监控与审计系统整合至一个统一风格的用户界面，只需一次登录，即可执行各种操作。 |
| 入网管理 | 入网申请和审核 | 申请者通过引导页发起设备入网申请，管理员在后台审核，通过审核的设备会置成保护状态，申请者可在引导界面查询审核状态。 |
| 批量入网申请和审核 | 申请者通过引导页发起设备批量入网申请，管理员在后台审核，审核后可在引导界面查询状态。支持通过短信网关短信通知管理员入网申请及申请者申请状态。 |
| 维保/施工人员管理 | 登记维保/施工人员的信息，包括姓名、联系电话、所属单位、人员属性、设备MAC等信息。 |
| 接入控制日志 | 能查询接入控制日志，包括源IP、目的IP、执行动作、上报时间等信息。日志分析，能按时间段查询阻断或跳转次数。 |
| 接入控制 | 数据流管控（即旁路镜像）准入 | 基于源IP和目的IP设置准入控制策略，通过TCP阻断和HTTP跳转的技术手段对数据流在网络层进行管控，阻断非法设备的访问并强制跳转进行引导注册，支持对NAT下设备的管控。 |
| 双向认证准入 | 基于客户端防火墙实现，在安装客户端的主机上鉴别访问者的合法性，阻断未授权的网络访问。 |
| 虚拟网关 | 支持与核心交换机联动的方式对未符合要求的设备进行跳转或阻断。 |
| 802.1x准入 | 提供已安装客户端的终端设完成交换机802.1x协议认证，支持EAP-MD5认证方式。 |
| ARP准入 | 提供ARP阻断功能，支持生效范围及例外设备的配置；可查看阻断日志，内容包含IP地址、MAC地址、最后一次阻断时间。 |
| 安检管理 | 入网安检 | 提供已安装客户端的终端设备在接入网络前进行安全检查，检查项包括：杀毒软件、补丁检查、不可信进程、不可信软件、账户弱口令、来宾账户、必要服务、必要软件，其中对于杀毒软件和必要软件可配置软件推送安装。对不符合安全要求的终端设备进行断网隔离，修复完成后才能入网。 |
| 安检日志 | 提供入网安检设备的安检日志查询功能，包括设备IP地址、MAC地址、责任人、部门、规范名称、安检时间、安检状态、安检描述等信息。 |

## （14）态势感知平台

|  |  |
| --- | --- |
| **指标项** | **主要技术参数** |
| 性能配置 | 2U，96G内存，SSD 128G系统盘、SATA 32T存储、双电源，RAID50、标配4个千兆电口 |
| 资产识别与管理 | 支持自动识别资产，在不影响内部网络的前提下，通过主动发送微量包的扫描方式探测潜在的服务器以及学习服务器的基础信息，如：操作系统、开放的端口号等； |
| 支持自动识别已知服务器，通过被动检测机制，对经过探针的流量进行分析，识别已知服务器对外提供的所有服务、已开放端口及端口传输的协议/应用等； |
| 支持安全域维度感知资产，可定义安全域名称、安全域属性、责任人、责任人邮箱、IP范围、备注等信息，并支持导入导出csv配置文件； |
| 支持分支维度感知资产，可定义分支名称、责任人、责任人邮箱、设备、地理位置地图，地图可选择在线地图、离线地址或本地导入地图（需提供截图证明）。 |
| 脆弱性感知 | 支持从威胁情报、应用安全、系统安全和设备安全的业务场景维度对告警进行二次分析； |
| 支持主机爆破、弱口令、未授权行为、挖矿行为检测。 |
| 高级威胁检测 | 具备僵尸网络识别能力，行为规则近40万条，并能够与CNCERT、VIRUSTOTAL等国内外权威机构共享威胁情报； |
| 支持DNSFlow分析引擎，利用机器学习算法结合威胁情报，能够从大量的样本中进行学习，总结其伪装的规律，从而发现伪装的恶意DNS协议 |
| 支持SMBFlow分析引擎，利用机器学习技术,发现主机传输可疑文件、恶意软件行为、文件或关键目录的可疑操作行为以及SMB暴力破解等； |
| 支持自定义关键词发现恶意邮件还支持邮件白名单，检测内容包含：发件人、收件人、关键词、邮件主题、抄送、附件文件名、邮件正文； |
| 支持对业务资产主动外连行为检测，包含：外连IP、外连IP归属、服务商、外连流量大小。 |
| 处置与分析 | 支持与云端安全运营中心联动。设备能连接互联网时，安全专家在云端分析并撰写威胁分析报告下发到设备上共用户查阅；设备离线时，可将关键数据离线导出上传到云端安全运营中心，安全专家进行分析撰写威胁分析报告。 |
| 支持邮件告警功能，可以定时向指定邮箱发送APT事件、攻击利用、恶意软件、拒绝服务等类型的告警信息。 |
| 支持检测隧道、Tor暗网通信、端口反弹等对外通信方式，支持区分国内外区域； |
| 日志类型至少包含漏洞利用攻击、网站攻击、僵尸网络、业务弱点、DOS攻击、邮件安全、文件安全、网络流量、DNS日志、HTTP日志、用户日志、数据库日志、文件审计日志、POP3日志、SMTP等各类日志，并可按照以上类型日志的各个关键字段搜索日志； |
| 提供告警展示场景，支持展示场景的切换。每个告警展示场景中支持自定义页面数据展示的范围，方便管理人员的日常运维工作。 |
| 安全管理服务 | ▲支持AES256、SM4数据传输加密，确保数据传输的安全性 |
| 大屏可视 | 支持大屏展示综合安全态势，包括资产态势、脆弱性态势、网络攻击态势、安全事件态势、外连态势、横向威胁态势，支持页面跳转到对应态势大屏； |
| 支持大屏展示业务脆弱性态势，包括漏洞风险态势、漏洞类型TOP5、高危漏洞TOP5、业务总览、脆弱性业务TOP5、实时脆弱性监测；（需提供截图证明）。 |
| 支持大屏展示业务外连态势，包括外连风险总览、外连威胁TOP10、外连态势、外连地区TOP5、实时威胁监控，并支持国际、国内地图自主切换； |
| 支持大屏展示资产态势，包括服务器操作系统分布、业务开发服务TOP5、最新资产动态、最近变动资产。 |
| 支持大屏展示网络攻击态势，包括攻击者、攻击总数、残余攻击、被攻击服务器、被攻击服务器TOP5、攻击态势，并支持攻击全景地图展示。 |
| 支持大屏展示正常横向访问和正常外连监控，正常横向访问监控包括被访问最多的业务TOP5、最活跃终端TOP5、应用TOP5、实时访问监控等，正常外连监控包括外连最多的业务TOP5、外连最多终端TOP5、外连态势、外连国家TOP5,并支持国际、国内地图切换； |
| 支持图形化大屏展示横向威胁态势，包括业务与终端访问、发起威胁终端TOP5、遭受威胁业务TOP5、访问趋势图，并支持不同颜色标注横向攻击、违规访问、可疑行为、风险访问； |
| 支持不同视角展示全网态势，包括综合安全态势、分支安全态势、安全事件态势、网络攻击态势、外连风险态势、横向威胁态势、脆弱性态势、资产态势等8个独立的大屏展示功能，并支持大屏轮播。 |
| 产品管理 | 支持 TB级数据秒级查询;  支持检索接入设备传输过来的所有安全日志，可基于时间、攻击类型、严重等级等选择项进行组合查询，可基于具体设备、来源/目的所属、IP地址、特征ID、URL进行具体条件搜索；支持通过syslog等接收、存储第三方设备的日志，并提供详细的字段搜索能力； |
| 支持管控接入探针的统一升级，可展示当前所有接入探针的规则库日期、是否过期等，并支持禁用指定探针的升级；  对接入的非探针设备，具备监控能力，包括展示是否在线、日志传输模式、今日传输日志量、当前传输总量等； |
| 支持接入防火墙、上网行为管理、终端杀毒、无线控制器、数据库审计和潜伏威胁探针等设备,并支持在页面中显示安全组件接入的数量和状态。 |
| 支持与同品牌终端EDR组件联动响应，发现威胁事件后支持在终端上进行追踪溯源发现相应的恶意进程并对其进行查杀 |
| 产品资质 | 要求具备公安颁发的销售许可证；（提供资质证明）  提供原厂五年质保服务。 |

**探针**

|  |  |
| --- | --- |
| **指标项** | **主要技术参数（具体功能要求）** |
| 性能配置 | 1Gbps，硬件指标：1U，单电源，标配4个千兆电口+2个千兆光口； |
| 基础检测功能 | 具备报文检测引擎,可实现IP碎片重组、TCP流重组、应用层协议识别与解析等, 具备多种的入侵攻击模式或恶意URL监测模式,可完成模式匹配并生成事件,可提取URL记录和域名记录,在特征事件触发时可以基于五元组和二元组(IP对)进行原始报文的录制。 |
| 监测识别规则库 | 能够识别应用类型超过1100种，应用识别规则总数超过3000条，具备亿万级别URL识别能力。漏洞利用规则特征库数量在4000条以上，漏洞利用特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，影响系统，对应CVE编号 |
| 异常会话检测 | 可实现对外联行为分析、间歇会话连接分析、加密通道分析、异常域名分析、上下行流量分析等在内 的多场景网络异常通信行为分析能力。 |
| 深度监测能力 | 可提供网络流量的会话级视图,根据网络流量的正常行为轮廓特征建立正常流量模型,判别流量是否出现异常,对原始流记录进行异常检测,可发现网络蠕虫、网络水平扫描、网络垂直扫描、IP地址扫描，端口扫描，ARP欺骗，IP协议异常报文检测和TCP协议异常报文等常见网络异常流量事件类型;  支持对节点检测节点内部主机外发的异常流量进行检测 支持对信任区域主机外发的异常流量进行检测，如ICMP，UPD，SYN，DNS Flood等DDoS攻击行为；  支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解检测功能； |
| 高级检测 | 支持同步DNS审计日志，主要用于平台dns flow分析引擎进行安全分析；同步HTTP审计日志，主要用于平台http flow分析引擎进行安全分析；同步SMB审计日志，主要用于平台smb flow分析引擎进行安全分析；同步SMTP审计日志主要用于平台smtp flow分析引擎进行安全分析 |
| 支持5种类型日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求 |
| Web应用安全检测能力 | 支持HTTP 1.0/1.1，HTTPS协议的安全威胁检测；  支持针对B/S架构应用抵御SQL注入、XSS、系统命令等注入型攻击；支持跨站请求伪造CSRF攻击检测；支持对ASP,PHP,JSP等主流脚本语言编写的webshell后门脚本上传的检测；支持其他类型的Web攻击，如文件包含，目录遍历，信息泄露攻击等的检测；  产品应具备独立的Web应用检测规则库，Web应用检测规则总数在3000条以上；  支持敏感数据泄密功能检测能力，支持敏感信息自定义，支持根据文件类型和敏感关键字进行信息过滤；  支持对被Web网站是否被挂黑链进行检测 |
| 僵尸主机检测 | 支持对终端种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为；  具备独立的僵尸主机识别特征库，恶意软件识别特征总数在40万条以上；  对于未知威胁具备同云端安全分析引擎进行联动的能力，上报可疑行为并在云端进行沙盒检测，并下发威胁行为分析报告； |
| 违规访问检测 | 能够针对IP，IP组，服务，端口，访问时间等策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单（哪些访问逻辑是正常的）和黑名单（哪些访问逻辑肯定是异常的）两种方式，并对检测到的违规访问进行实时告警 |
| 流量记录 | 能对网络通信行为进行还原和记录，以供进行取证分析，还原内容包括：TCP会话记录、Web访问记录、SQL访问记录、DNS解析记录、文件传输行为、LDAP登录行为。 |
| 沙盒对接 | 支持将流量还原文件发送至沙盒进行静态检测和动态模拟执行。 |
| 抓包分析 | 支持通过设备对流量进行抓包分析，可定义抓包数量、接口、IP地址、端口或自定义过滤表达式 |
| 管理功能 | 可支持在线升级和离线升级，并依托安全感知平台进行统一管控  可实时监控设备的CPU、内存、存储空间使用情况。  能够监控监听接口的实时流量情况 |
| 集中管控 | 支持安全感知平台对接入探针的统一升级，可展示当前所有接入探针的规则库日期、是否过期等，并支持禁用指定探针的升级 |
| 部署 | 支持旁路部署，对镜像流量进行监听  可以多台采集器同时部署于客户网络不同位置并将数据传输到同一套分析平台 |

## （15）普通网闸

|  |  |
| --- | --- |
| **指标项** | **主要技术参数** |
| 系统架构 | 产品采用“2+1”（即双主机系统+物理隔离数据通道控制系统）体系结构；具备数据通道控制系统证书；通过嵌入式数据通道控制系统隔离外部网络，而不是采用DMA、SCSI、网卡等方式实现；采用特有控制逻辑和专用通讯协议完全控制数据的实时交换，确保可信网络（域）和非可信网络（域）之间任何连接的断开，彻底阻断TCP/IP协议及其他网络协议。 |
| 系统要求 | ▲采用具有自主知识产权的基于linux内核的多核多线程并行安全操作系统TPSecOS，提供安全操作系统软件著作权登记证书； |
| 物理参数 | 2U机架式EIA RS-310C标准机箱，高强度钢结构机箱； |
| 接口配置 | 内网机：2个SFP插槽，6个10/100/1000BASE-T接口，1个console接口；2个USB接口，最大可扩展至6个SFP插槽或10个10/100/1000BASE-T接口； |
| 外网机：2个SFP插槽，6个10/100/1000BASE-T接口，1个console接口；2个USB接口，最大可扩展至6个SFP插槽或10个10/100/1000BASE-T接口； |
| 性能 | 吞吐量≥600 Mbps；  最大并发连接数≥100,000；  MTBF≥50,000小时；  系统延时＜1μs；  最大并发视频路数≥240路D1视频；  最大数据库同步速率≥2,000条/秒； |
| 系统监控 | ▲带液晶屏，液晶菜单可显示内外网机IP地址、CPU使用率和内存使用率等整机信息，面板可操控整机复位、关机，具有设备异常（如网络IP冲突、通讯异常等）监测报警功能；（投标时必须提供物理结构图和功能图） |
| 文件同步 | 文件同步支持SMBFS、SAMBA、NFS等文件传输协议，可以实现内网到外网、外网到内网、双向的文件传输；  支持文件传输方向可控，实现单向或双向传输； |
| 支持病毒检测；（投标时提供功能截图并加盖公章） |
| 支持文件断点续传功能； |
| 支持对传输文件的文件名检测机制；  支持对文件类型的黑白名单控制，根据文件格式特征进行过滤，并且不依赖于文件扩展名；支持文件扩展名自定义功能；  ▲支持对文件内容智能语义分析，对包含指定内容的文件进行过滤；提供语义分析系统软件著作权登记证书； |
| 支持时间策略，实时或定时文件摆渡； |
| 支持按任务进行策略过滤；支持一源多目及多源一目文件同步； |
| 支持增量传输、传输后删除、改名传输、删除同步等传输策略；  支持目录内子目录同步，子目录级别不受限制；  支持对重名文件的控制策略，提供“覆盖”、“丢弃”、“重命名”等重名策略； |
| 支持文件同步容错策略和告警策略，同步出错能够自动重传,出现异常同步状况能够终止同步弹出告警提示并记录日志。 |
| 文件交换 | 提供专用文件交换客户端提供安全的文件交换功能。 |
| 支持文件自动收发功能，文件交换服务能够控制单个用户和分组用户的文件收发权限；文件交换可提供客户端和无客户端的操作； |
| 支持文件传输时的身份认证及加密传输功能； |
| 文件交换客户端支持自动接收文件功能； |
| 文件交换客户端支持自动启动、支持下载目录自定义和管理功能； |
| 支持客户端登录，用户列表支持十级以上在组织结构； |
| 支持发送文件功能支持一对一用户、一对多用户和多对一用户； |
| ▲文件交换客户端支持扩展windows右键菜单发送文件、支持拖拽方式发送文件、客户端界面按钮选择文件三种方式发送文件；（投标时提供功能截图并加盖公章） |
| ▲文件交换客户端支持windwos AD域帐号登录身份鉴别；（投标时提供功能截图并加盖公章） |
| 数据库同步 | 支持ORACLE、SYBASE、MySQL、SQL Server、DB2等主流数据库同步和支持国产达梦、人大金仓、南大通用等数据库的同步；  数据库同步应用可通过灵活的同步机制保证安全等级不同的网络中的数据库系统实现数据同步更新；  提供灵活的接口，方便后期对其他数据库类型进行扩展，具备可配置性，松耦合，模块化； |
| 同步由网闸主动发起并完成，不需要第三方软件支持（无需在数据库安装任何第三方软件），支持Windows、Linux、Unix 等多种操作系统，且网闸无需开放端口以杜绝安全隐患；  支持有客户端、无客户端多种部署方式实现数据库同步； |
| 支持多种同步方式（如先镜像后增量、增量），同步模式支持单向和双向同步； （投标时提供功能截图并加盖公章）  支持表级、字段级同步；  支持同构数据库之间、异构数据库之间的数据同步，无需修改数据库表结构；  支持对指定字段允许同步或不允许同步；  支持对指定字段的指定内容允许同步或不允许同步；  支持自定义间隔时间执行同步任务，支持指定时间执行同步任务，支持同步数据的数量可选及自定义；（投标时提供功能截图并加盖公章）  ▲支持 Oracle 数据库 RAC 集群同步；（投标时提供功能截图并加盖公章）  ▲支持SuperMap、ArcGIS软件自定义生成的数据库表增加、修改及数据库表字段增加、修改操作进行同步；（投标时提供功能截图并加盖公章）  ▲支持GIS数据发布同步模块，支持GIS数据中点、线、面数据实现同步；（投标时提供功能截图并加盖公章）  可以同时发送和接收一个关系数据库中的多个表；  可分别定义增加、修改的数据传输；  根据指定字段值进行条件传输；  支持大字段数据同步交换包括BLOB、CLOB、Long等；  支持不同类型数据库之间的异构数据安全传输； |
| 支持不同数据库类型相同表结构同步；  支持相同数据库相似表结构相同字段类型同步；  支持不同数据库类型相似表结构相同字段类型同步； |
| 数据库同步支持大字段、1G以上字段；  数据库同步支持空间数据库、空间字段；  支持上亿级别数据的数据库同步； |
| 支持灵活的数据库冲突处理策略，当关键字数据发生冲突时可选择：覆盖/丢弃； |
| 支持数据库同步实时日志记录，提供日志审计、查询； |
| 数据库访问 | 提供对Oracle 、DB2、SyBase、SQL Server、MySql等主流数据库和支持国产达梦、人大金仓、南大通用等数据库的安全访问，实现内外网之间数据库及表内容安全传输； |
| 支持客户端安全访问网络另一侧的数据库服务器的功能； |
| 支持任务单独启停管理，不影响数据库同步的其他任务运行； |
| 支持对访问源地址、目的地址、本机地址和端口的自定义访问控制； |
| 支持对数据库库名和数据库表访问控制，根据用户与数据库表对应关系，进行相应数据库操作过滤； |
| 支持访问时段控制；提供数据库访问用户名过滤和控制；提供数据库访问日志。 |
| 视频交换 | 支持D4、D1、VGA、2/3D1、1/2D1、1/1.8D1、SIF、3/4D1、CIF、4CIF、QCIF 、SQCIF等视频分辨率；  特别针对流媒体文件进行优化，满足avi,wav,vob,mpg,wma,mp3等格式音视频高速传输与交换；  支持完全深度检测：MPEG-2编码文件（\*.MP2 \*.bwf \*.s48等光电常用协议）；  支持常规深度检测：\*.mp4 \*.avi \*.wav \*.mpg \*.rmvb \*.wmv \*.mov \*.flv \*.psd \*.swf \*.vob等各种常见音视频格式；  支持H.263、H.264、M-JEPG、MPEG4编码格式；  支持SCTP、国标GB28181、H.323、H.248等主流视频协议； |
| 支持视音频同时传输；支持基于动态端口传输的流媒体视频应用；  支持GB28181、RTSP代理，支持GB28181、RTSP指令控制，支持RTSP、RTCP、RTP系列协议；  支持视频管理服务器数据转发，视频管理服务器通道建立，支持视频SIP服务器数据转发，SIP管理服务器通道建立； |
| 支持海康、大华、H3C、天视、星望、科达、天久、互信互通、先进视讯视频等主流视频厂商控制协议；支持通过视频模块、公安三所视频模块、公安一所视频模块、蛙视视频模块等视频服务；支持视频会议；支持DB33标准；支持能对各视频平台进行二次开发； |
| 能够严格区分视频数据流和控制信令流，根据策略配置可以控制视频数据的单向传输； |
| 支持视频文件传输白名单功能，对文件进行细微检测；  支持自定义扩展名检测； |
| 对接入点身份进行审查，对未通过审查的对象一律丢弃，保证视频数据交换的安全可靠； |
| 工业控制 | 支持OPC、MODBUS、S7、WINCC、DNP3、IEC等工业协议；  支持DCS/SCADA两网之间的OPC应用数据传输；  支持OPC UA标准； |
| 支持DCS/SCADA生产网络与办公网络之间的OPC应用数据的传输，支持同步、异步监测数据的传输；  ▲只需绑定固定的一个起始端口即可满足动态端口的数据传输。（提供功能截图并加盖公章） |
| ▲持DCS/SCADA网络与办公网络之间的ModBus应用数据的传输；支持ModBus控制协议解析及设备ID控制，支持基于TCP及UDP协议功能码控制，例如读写线圈、读写寄存器的控制（提供功能截图并加盖公章）；  可自定义读写地址，读写地址范围0-65535可选；支持根据源IP、源端口、目的IP、目的端口自定义MODBUS规则（提供功能截图并加盖公章）； |
| ▲支持DCS/SCADA网络与办公网络之间西门子S7应用数据的传输；支持西门子控制协议解析控制，支持协议功能组及功能码控制（提供功能截图并加盖公章）；  支持根据源IP、源端口、目的IP、目的端口自定义S7规则； |
| ▲支持DCS/SCADA生产网络与办公网络之间的DNP 3.0应用数据的传输；支持基于TCP及UDP协议功能码控制，可指定发送者地址及接收者地址；（提供功能截图并加盖公章）  支持根据源IP、源端口、目的IP、目的端口自定义DNP规则； |
| ▲支持DCS/SCADA生产网络与办公网络之间的IEC应用数据的传输；支持协议、ASDU地址域、信息对象地址、传输原因及控制命令；（提供功能截图并加盖公章）  支持根据源IP、源端口、目的IP、目的端口自定义IEC规则； |
| FTP访问 | 支持动态数据通道建立，并可对访问端口号自定义；可提供对本机FTP虚拟服务地址和端口的自由定义设置； |
| 支持对FTP主动、被动传输模式的转换，并可灵活设置允许或禁止传输； |
| 支持病毒检测功能； |
| 支持对FTP命令的黑白名单控制策略；  支持文件大小、文件名传输控制策略；  支持传输文件扩展名过滤；  支持对用户、命令、文件类型等细粒度访问控制；  强化文件安全传输，内容过滤； |
| 支持基于会话级的内容过滤策略，允许不同会话采用不同的内容访问控制策略； |
| 支持时间访问控制策略； |
| 支持对访问源地址、目的地址和端口进行访问控制； |
| 支持用户分组控制策略，对不同用户组进行不同访问控制；支持访问用户的黑白名单过滤；  支持文件传输时的身份认证及加密传输功能； |
| 安全浏览 | 支持HTTP五种请求类型（GET/POST/PUT/HEAD/CONNECT）的黑白名单控制；支持HTTPS网络传输； |
| 支持基于会话级的内容过滤策略，允许不同会话采用不同的内容访问控制策略； |
| 支持对访问源地址、目的地址、源端口、目的端目、域名进行访问控制； |
| 支持代理模式； 支持URL地址过滤；（投标时提供功能截图并加盖公章）  支持关键字网页过滤；  支持对下载文件的大小、类型过滤； |
| 支持用户名+密码+IP+MAC等多种认证方式，对多次认证失败的用户可锁定其IP或用户名； |
| 支持安全浏览日志及认证失败用户记录，可导出列表；  支持用户上网时段控制策略； |
| 支持上网用户列表及操作日志查询，可即时阻断单个用户或IP上网； |
| 邮件传输 | 支持病毒扫描功能；  支持基于SMTP协议的邮件发送和POP3协议的邮件接收，内外网隔离环境下可实现邮件收、发； |
| 支持邮件传输过滤控制；  支持对邮件地址、主题、正文内容、附件、关键字等过滤；  支持附件大小控制、支持字符/字符串过滤、支持邮件地址过滤；（投标时提供功能截图并加盖公章） |
| 支持对邮件源地址、目的地址和端口、本机地址和端口的自定义访问过滤控制； |
| 支持邮件收发时段控制策略； |
| 支持邮件收发日志记录，方便日志审计和管理； |
| 定制访问 | 实现特定TCP、UDP协议的数据隔离交换，可合作定制开发针对特定协议的安全检测，实现如黑白名单控制、关键字过滤等；  支持TCP/UDP的透明访问和普通访问；  支持对访问源地址、目的地址、源端口、目的端目进行访问控制；  支持路由映射功能；  支持时段控制策略，时间策略可以是一次性或者周循环模式； |
| 防病毒 | 支持病毒检测：对文件交换进行病毒检测和过滤；支持病毒库在线升级和手动升级；（投标时提供功能截图并加盖公章） |
| 入侵检测 | ▲具有实时入侵检测机制；支持对BasicAttack、 SMTP、FTP、DNS、DOS/DDOS 攻击、PortScan 的检测；（投标时提供功能截图并加盖公章） |
| 身份认证 | 支持socks4/socks5代理；  采用用户名和密码、IP地址、MAC地址、Radius多种组合方式实现客户端访问控制；（投标时提供功能截图并加盖公章） |
| 安全管理 | 支持CPU、内存、硬盘状态实时监控；支持HTTPS的Web方式管理，实现了远程管理信息加密传输；支持命令行方式管理，可以通过命令方式进行资源分配、排错、查看日志、深层次管理；支持远程SSH管理，远程管理的信息以密文形式传输；（投标时提供功能截图并加盖公章） |
| 必须通过内网主机系统来管理和配置网闸，而不是采用低安全的管理方式，如采用内外网口分别管理和配置网闸；必须采用硬件USB钥匙加密管理；（投标时提供功能截图并加盖公章） |
| 系统采用系统管理员、保密管理员、日志审计管理员三权分立的管理模式； |
| 防爆力  破解限制 | 支持时间控制管理，可设置多个时间点来控制网闸网络服务的启动、终止；支持系统防爆处理，对管理员登陆有密码次数限制，密码输入错误，超过限定次数，自动锁定设备，阻止非法管理员再次登录。根据限定期限，可自动解除锁定；（投标时提供功能截图并加盖公章） |
| 多网隔离能力 | 支持多网隔离，每个网络接口可以接不同安全级别的网络； |
| 接入方式 | 支持IPV4/IPV6双栈接入；（投标时提供功能截图并加盖公章）  可根据来源、目的地、用户特权和时间来控制对特定的 HTTP、文件交换或 FTP 等资源的访问；支持相同网络地址段之间部署；支持透明接入方式，支持普通接入方式，不同接入方式单独控制； |
| 路由配置 | 支持IPV4静态路由，IPV6静态路由；（投标时提供功能截图并加盖公章） |
| 集中管理 | 支持标准的SNMP协议；  支持集中管理，支持对多台设备进行统一管理和策略下发（投标时提供功能截图并加盖公章）； |
| 设备冗余 | 支持配置同步；通过独立的热备端口及普通业务端口实现双机热备；（投标时提供功能截图并加盖公章）； |
| 日志审计 | 专用日志服务程序处理系统日志：包括日志分类统计、日志浏览、查询、导出、手工删除；支持日志自动删除功能； |
| 记录内网预警信息日志、内网FTP同步日志、FTP代理日志、邮件发送日志、邮件接收日志、用户登录日志、内网链路日志、内网双机热备日志、文件共享同步日志、数据库同步日志、管理员日志；（投标时提供功能截图并加盖公章）  记录外网预警信息日志、外网FTP同步日志、FTP代理日志、文件发送日志、文件接收日志、用户登录日志、外网链路日志、入侵检测日志、文件共享同步日志等；（投标时提供功能截图并加盖公章） |
| 支持SysLog，Mysql标准； |
| 日志管理 | 支持本地日志导出，支持本地日志存储空间不足报警；  ▲日志导出支持可选择任意时间段，日志导出类型支持XLSX加密及非加密等；日志下载可选日志导出类别；（投标时提供功能截图并加盖公章）  支持日志上传，可按日志类别选择上传日志；  支持删除过期日志，可自定义日志删除时间，可按日志类别选择删除的日志； |
| 日志空间管理 | 支持自定义日志空间大小，告警百分比，日志留存天数；（投标时提供功能截图并加盖公章） |
| 告警管理 | ▲支持对管理员的操作、FTP同步、文件共享同步、数据库同步等进行实时的告警，告警信息可显示告警级别、详细告警事件、备注信息、创建时间等，可以删除及批量删除历史过期的告警信息； |
| 系统调试 | 支持针对指定网卡进行故障测试，测试工具包含traceroute、telnet、ping、arp、tcpdump等；（投标时提供功能截图并加盖公章） |
| **系统检测** | ▲系统支持自动检测、周期性检测，可下载自动产测报告、周期性检测结果、messages；**（投标时提供功能截图并加盖公章）** |
| **产品资质** | 公安部计算机信息系统安全专用产品销售许可证（增强级）及公安部计算机信息系统安全产品质量监督检验中心检验报告； |
| 国家保密局涉密信息系统产品检测证书； |
| 国家密码管理局商用密码检测证书 |
| 中国国家信息安全产品认证证书； |
| 数据通道控制系统软件著作权登记证书； |
| 语义分析系统软件著作权登记证书； |
| 基于PKI的身份认证与管理系统证书； |
| 安全隔离与信息交换系统软件著作权登记证书； |
| 制造商通过最新的GB/T19001-2016/ISO9001-2015质量体系认证； |

## 视频网闸

|  |  |
| --- | --- |
| **指标项** | **主要技术参数** |
| **系统架构** | 产品采用“2+1”（即双主机系统+物理隔离数据通道控制系统）体系结构；具备数据通道控制系统证书；通过嵌入式数据通道控制系统隔离外部网络，而不是采用DMA、SCSI、网卡等方式实现；采用特有控制逻辑和专用通讯协议完全控制数据的实时交换，确保可信网络（域）和非可信网络（域）之间任何连接的断开，彻底阻断TCP/IP协议及其他网络协议。 |
| **系统要求** | ▲采用具有自主知识产权的基于linux内核的多核多线程并行安全操作系统TPSecOS，提供安全操作系统软件著作权登记证书； |
| **物理参数** | 2U机架式EIA RS-310C标准机箱，高强度钢结构机箱； |
| **接口配置** | 内网机：5个10/100/1000BASE-T接口，1个HA接口（10/100/1000BASE-T），  一个console口；最大可扩展至8个SFP插槽或14个10/100/1000BASE-T接口； |
| 外网机：5个10/100/1000BASE-T接口，1个HA接口（10/100/1000BASE-T），  一个console口；最大可扩展至8个SFP插槽或14个10/100/1000BASE-T接口； |
| **性能** | 吞吐量≥1 Gbps；  最大并发连接数≥200,000；  MTBF≥50,000小时；  系统延时＜1μs；  最大并发视频路数≥400路D1视频；  最大数据库同步速率≥3,000条/秒； |
| **系统监控** | ▲带液晶屏，液晶菜单可显示内外网机IP地址、CPU使用率和内存使用率等整机信息，面板可操控整机复位、关机，具有设备异常（如网络IP冲突、通讯异常等）监测报警功能；**（投标时提供功能截图并加盖公章）** |
| **视频交换** | 支持D4、D1、VGA、2/3D1、1/2D1、1/1.8D1、SIF、3/4D1、CIF、4CIF、QCIF 、SQCIF等视频分辨率；  特别针对流媒体文件进行优化，满足avi,wav,vob,mpg,wma,mp3等格式音视频高速传输与交换；  支持完全深度检测：MPEG-2编码文件（\*.MP2 \*.bwf \*.s48等光电常用协议）；  支持常规深度检测：\*.mp4 \*.avi \*.wav \*.mpg \*.rmvb \*.wmv \*.mov \*.flv \*.psd \*.swf \*.vob等各种常见音视频格式；  支持H.263、H.264、M-JEPG、MPEG4编码格式；  支持SCTP、国标GB28181、H.323、H.248等主流视频协议； |
| 支持视音频同时传输；支持基于动态端口传输的流媒体视频应用；  支持GB28181、RTSP代理，支持GB28181、RTSP指令控制，支持RTSP、RTCP、RTP系列协议；  支持视频管理服务器数据转发，视频管理服务器通道建立，支持视频SIP服务器数据转发，SIP管理服务器通道建立； |
| 支持海康、大华、H3C、天视、星望、科达、天久、互信互通、先进视讯视频等主流视频厂商控制协议；支持通过视频模块、公安三所视频模块、公安一所视频模块、蛙视视频模块等视频服务；支持视频会议；支持DB33标准；支持能对各视频平台进行二次开发； |
| 能够严格区分视频数据流和控制信令流，根据策略配置可以控制视频数据的单向传输； |
| 支持视频文件传输白名单功能，对文件进行细微检测；  支持自定义扩展名检测； |
| 对接入点身份进行审查，对未通过审查的对象一律丢弃，保证视频数据交换的安全可靠； |
| **文件同步** | 文件同步支持SMBFS、SAMBA、NFS等文件传输协议，可以实现内网到外网、外网到内网、双向的文件传输；  支持文件传输方向可控，实现单向或双向传输； |
| 支持病毒检测；**（投标时提供功能截图并加盖公章）** |
| 支持文件断点续传功能； |
| 支持对传输文件的文件名检测机制；  支持对文件类型的黑白名单控制，根据文件格式特征进行过滤，并且不依赖于文件扩展名；支持文件扩展名自定义功能；  ▲支持对文件内容智能语义分析，对包含指定内容的文件进行过滤；提供语义分析系统软件著作权登记证书； |
| 支持时间策略，实时或定时文件摆渡； |
| 支持按任务进行策略过滤；支持一源多目及多源一目文件同步； |
| 支持增量传输、传输后删除、改名传输、删除同步等传输策略；  支持目录内子目录同步，子目录级别不受限制；  支持对重名文件的控制策略，提供“覆盖”、“丢弃”、“重命名”等重名策略； |
| 支持文件同步容错策略和告警策略，同步出错能够自动重传,出现异常同步状况能够终止同步弹出告警提示并记录日志。 |
| **文件交换** | 提供专用文件交换客户端提供安全的文件交换功能。 |
| 支持文件自动收发功能，文件交换服务能够控制单个用户和分组用户的文件收发权限；文件交换可提供客户端和无客户端的操作； |
| 支持文件传输时的身份认证及加密传输功能； |
| 文件交换客户端支持自动接收文件功能； |
| 文件交换客户端支持自动启动、支持下载目录自定义和管理功能； |
| 支持客户端登录，用户列表支持十级以上在组织结构； |
| 支持发送文件功能支持一对一用户、一对多用户和多对一用户； |
| 文件交换客户端支持扩展windows右键菜单发送文件、支持拖拽方式发送文件、客户端界面按钮选择文件三种方式发送文件；**（投标时提供功能截图并加盖公章）** |
| 文件交换客户端支持windwos AD域帐号登录身份鉴别；**（投标时提供功能截图并加盖公章）** |
| **数据库同步** | 支持ORACLE、SYBASE、MySQL、SQL Server、DB2等主流数据库同步和支持国产达梦、人大金仓、南大通用等数据库的同步；  数据库同步应用可通过灵活的同步机制保证安全等级不同的网络中的数据库系统实现数据同步更新；  提供灵活的接口，方便后期对其他数据库类型进行扩展，具备可配置性，松耦合，模块化；  ▲支持 Oracle 数据库 RAC 集群同步；**（投标时提供功能截图并加盖公章）** |
| 同步由网闸主动发起并完成，不需要第三方软件支持（无需在数据库安装任何第三方软件），支持Windows、Linux、Unix 等多种操作系统，且网闸无需开放端口以杜绝安全隐患；  支持有客户端、无客户端多种部署方式实现数据库同步； |
| **数据库访问** | 提供对Oracle 、DB2、SyBase、SQL Server、MySql等主流数据库和支持国产达梦、人大金仓、南大通用等数据库的安全访问，实现内外网之间数据库及表内容安全传输； |
| **FTP访问** | 支持动态数据通道建立，并可对访问端口号自定义；可提供对本机FTP虚拟服务地址和端口的自由定义设置； |
| 支持对FTP主动、被动传输模式的转换，并可灵活设置允许或禁止传输； |
| 支持病毒检测功能； |
| 支持对FTP命令的黑白名单控制策略；  支持文件大小、文件名传输控制策略；  支持传输文件扩展名过滤；  支持对用户、命令、文件类型等细粒度访问控制；  强化文件安全传输，内容过滤； |
| 支持基于会话级的内容过滤策略，允许不同会话采用不同的内容访问控制策略； |
| 支持时间访问控制策略； |
| 支持对访问源地址、目的地址和端口进行访问控制； |
| 支持用户分组控制策略，对不同用户组进行不同访问控制；支持访问用户的黑白名单过滤；  支持文件传输时的身份认证及加密传输功能； |
| **安全浏览** | 支持HTTP五种请求类型（GET/POST/PUT/HEAD/CONNECT）的黑白名单控制；支持HTTPS网络传输； |
| 支持基于会话级的内容过滤策略，允许不同会话采用不同的内容访问控制策略； |
| 支持对访问源地址、目的地址、源端口、目的端目、域名进行访问控制； |
| 支持代理模式； 支持URL地址过滤；  支持关键字网页过滤；  支持对下载文件的大小、类型过滤； |
| 支持用户名+密码+IP+MAC等多种认证方式，对多次认证失败的用户可锁定其IP或用户名； |
| 支持安全浏览日志及认证失败用户记录，可导出列表；  支持用户上网时段控制策略； |
| 支持上网用户列表及操作日志查询，可即时阻断单个用户或IP上网； |
| **邮件传输** | 支持病毒扫描功能；  支持基于SMTP协议的邮件发送和POP3协议的邮件接收，内外网隔离环境下可实现邮件收、发； |
| 支持邮件传输过滤控制； |
| 支持对邮件源地址、目的地址和端口、本机地址和端口的自定义访问过滤控制； |
| 支持邮件收发时段控制策略； |
| 支持邮件收发日志记录，方便日志审计和管理； |
| **定制访问** | 实现特定TCP、UDP协议的数据隔离交换，可合作定制开发针对特定协议的安全检测，实现如黑白名单控制、关键字过滤等；  支持TCP/UDP的透明访问和普通访问；  支持对访问源地址、目的地址、源端口、目的端目进行访问控制；  支持路由映射功能；  支持时段控制策略，时间策略可以是一次性或者周循环模式； |
| **防病毒** | 支持病毒检测：对文件交换进行病毒检测和过滤；支持病毒库在线升级和手动升级； |
| **入侵检测** | 具有实时入侵检测机制；支持对BasicAttack、 SMTP、FTP、DNS、DOS/DDOS 攻击、PortScan 的检测；**（投标时提供功能截图并加盖公章）** |
| **身份认证** | 支持socks4/socks5代理；  采用用户名和密码、IP地址、MAC地址、Radius多种组合方式实现客户端访问控制； |
| **安全管理** | 支持CPU、内存、硬盘状态实时监控；支持HTTPS的Web方式管理，实现了远程管理信息加密传输；支持命令行方式管理，可以通过命令方式进行资源分配、排错、查看日志、深层次管理；支持远程SSH管理，远程管理的信息以密文形式传输； |
| 必须通过内网主机系统来管理和配置网闸，而不是采用低安全的管理方式，如采用内外网口分别管理和配置网闸；必须采用硬件USB钥匙加密管理； |
| 系统采用系统管理员、保密管理员、日志审计管理员三权分立的管理模式； |
| **防爆力**  **破解限制** | 支持时间控制管理，可设置多个时间点来控制网闸网络服务的启动、终止；支持系统防爆处理，对管理员登陆有密码次数限制，密码输入错误，超过限定次数，自动锁定设备，阻止非法管理员再次登录。根据限定期限，可自动解除锁定； |
| **多网隔离能力** | 支持多网隔离，每个网络接口可以接不同安全级别的网络； |
| **接入方式** | 支持IPV4/IPV6双栈接入；  可根据来源、目的地、用户特权和时间来控制对特定的 HTTP、文件交换或 FTP 等资源的访问；支持相同网络地址段之间部署；支持透明接入方式，支持普通接入方式，不同接入方式单独控制； |
| **路由配置** | 支持IPV4静态路由，IPV6静态路由； |
| **集中管理** | 支持标准的SNMP协议；  支持集中管理，支持对多台设备进行统一管理和策略下发 |
| **设备冗余** | 支持配置同步；通过独立的热备端口及普通业务端口实现双机热备； |
| **日志审计** | 专用日志服务程序处理系统日志：包括日志分类统计、日志浏览、查询、导出、手工删除；支持日志自动删除功能； |
| **日志管理** | 支持本地日志导出，支持本地日志存储空间不足报警；  日志导出支持可选择任意时间段，日志导出类型支持XLSX加密及非加密等；日志下载可选日志导出类别；  支持日志上传，可按日志类别选择上传日志；  支持删除过期日志，可自定义日志删除时间，可按日志类别选择删除的日志； |
| **日志空间管理** | 支持自定义日志空间大小，告警百分比，日志留存天数； |
| **告警管理** | 支持对管理员的操作、FTP同步、文件共享同步、数据库同步等进行实时的告警，告警信息可显示告警级别、详细告警事件、备注信息、创建时间等，可以删除及批量删除历史过期的告警信息； |
| **系统调试** | 支持针对指定网卡进行故障测试，测试工具包含traceroute、telnet、ping、arp、tcpdump等； |
| **系统检测** | 系统支持自动检测、周期性检测，可下载自动产测报告、周期性检测结果、messages； |
| **产品资质** | 公安部计算机信息系统安全专用产品销售许可证（增强级）及公安部计算机信息系统安全产品质量监督检验中心检验报告； |

## 楼层交换机

|  |  |
| --- | --- |
| **指标项** | **主要技术参数** |
| 基本配置 | 交换容量：≥336Gbps/3.36Tbps  包转发率：≥108/126Mpps，24个10/100/1000Base-T以太网端口，4个万兆，电源冗余：支持1+1，MAC特性：支持32K。 |

## 病毒预警机

|  |  |
| --- | --- |
| **指标项** | **主要技术参数** |
| **硬件要求** | 机架式2U |
| 6个10/100/1000M-BaseT 电口, 4个光口，以应对多网段现状 |
| 病毒数据处理能力900M |
| 病毒库总量800万以上 |
| http背景压力2万/秒 |
| MTBF大于等于50000小时 |
| **功能要求** | 采用旁路部署，安全可靠；每个病毒监测探针可同时支持至少2路以上的网络病毒监测； |
| 可通过上级单位的升级中心进行每周自动升级，以保证每周最新病毒库  能有效减少上级单位安全通告平台的传毒传毒受毒通告；  实现对全省消防单位作全网病毒状态分析报告；  定期上门升级病毒库，同时制作月度报表 |
| 具备对已知病毒的检测能力，要求支持SMTP、POP3、FTP、HTTP、SAMBA和IPMSG协议的病毒检测; 且可对SMTP、POP3、FTP、HTTP协议通过不同端口传输的数据同时具有病毒检测功能。 |
| 支持监控各种病毒、蠕虫、木马、广告软件、灰色软件、流行的入侵软件等； |
| 具有智能脚本分析引擎技术，可以识别网页中的恶意脚本、Java applet、ActiveX控件和Cookies； |
| 要求支持多层压缩文件中的病毒扫描，可定制压缩层数; 要求可定制不扫描文件类型; 要求支持对病毒文件进行隔离; 要求拥有对未知病毒识别及检测能力 |
| 升级功能：病毒监测探针具有多种升级方式，可以实现自动升级和手动升级。 |
| **产品**  **资质** | 具有公安部安全产品销售许可证书；  具有计算机软件著作权登记证书； |
| **保修服务** | 提供原厂五年质保服务。 |

## 大队测试核心交换机

|  |  |
| --- | --- |
| **功能类别** | **技术要求及指标** |
| ▲性能 | 交换容量≥15Tbps，包转发率≥1400Mpps（若以上规格官网有两个值，则以最小值为准）； |
| ▲配置要求 | 实配冗余主控，业务板卡≥3，电源数量≥2个； |
| 实配万兆光接口≥4个，千兆光接口≥44个； |
| 每台设备实配千兆单模模块8个，万兆多模模块4个； |
| 实配IPv6功能授权； |
| 二层功能 | 支持IEEE 802.1d(STP)、 802.w(RSTP)、 802.1s(MSTP)  支持VLAN内端口隔离  支持DHCP Client, DHCP Server，DHCP Relay；  支持整机MAC地址≥1M；MAC学习速率>8000/s |
| IP路由 | 支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6；  支持GR for OSPF/IS-IS/BGP；  支持整机ARP表项≥256K；ARP学习速率≥1000/s |
| 可靠性 | 要求支持真实业务流的实时检测技术，秒级快速故障定位，非常规模拟业务流检测方式 |
| 支持G.8032开放环或SEP、REP半环协议,可与其他厂商设备混合组网，要求倒换时间≤50ms。 |
| 支持BFD/OAM，遵循协议标准，3.3ms稳定均匀发包检测，50ms内完成故障倒换,保证设备高可靠性 |
| 虚拟化技术 | 支持纵向虚拟化技术，提供权威第三方测试报告 |
| QoS | 支持GE/10GE端口200ms大缓存，提供官网截图证明 |
| 支持5级H-QoS |
| 增值业务 | 要求本次采购设备支持硬件级别无线控制器； |
| 支持防火墙插卡； |
| 支持IPSEC板卡； |
| 用户管理 | 支持802.1X、MAC、Portal等认证方式 |
| 支持基于流量、DAA目的地址和时长计费方式 |
| 资质要求 | 提供工信部入网证书 |
| 投标产品须是国内外主流厂商产品 |
| 保修服务 | 原厂5年免费保修，中标后提供原厂5年质保。 |

## 大队测试防火墙

|  |  |
| --- | --- |
| **功能类别** | **技术要求及指标** |
| 硬件架构 | 采用多核架构；设备高度≤2U |
| ▲配置需求 | 实际配置千兆电口≥8；万兆光口≥2；USB口≥2， |
| 配置SSL VPN≥100个；IPS-AV-URL功能集≥36个月， |
| 模块配置 | 实配千兆单模光模块4个，万兆多模光模块2个 |
| ▲规格性能 | 吞吐量≥6Gbps； |
| 最大并发连接数≥300万； |
| 每秒新建连接数≥8万 |
| 接口镜像 | 支持将任意接口数据完全镜像到设备自身的其他接口,用于抓包分析 |
| 状态检测包过滤 | 能够基于五元组、方向、时间、用户、用户组、应用层协议等多个元素进行访问控制 |
| 路由能力 | 支持静态路由、路由策略、策略路由、RIP、OSPF、BGP、MPLS、ISIS等路由协议； |
| 智能DNS | 支持智能DNS功能。 |
| 智能应用引流 | 支持基于P2P、web视频等应用的智能引流。 |
| 网络地址转换（NAT） | 支持全面NAT功能，对多种应用层协议支持ALG功能，包括ILS、DNS、PPTP、SIP、FTP、ICQ、RTSP等。 |
| 用户管理 | 支持用户、用户组信息的管理，可手动录入或从LDAP\AD导入，优选可以以树型结构清晰的显示用户、用户组信息。 |
| 可自定义用户认证界面风格，包括登录主页面、登录成功界面、登录失败界面等。 |
| 支持在线用户管理功能，可注销、冻结在线用户，并可查看上线用户IP\所属用户组\登录时间\在线时长\使用流量等信息。 |
| 入侵防御 | 基于特征检测，支持基于协议检测，协议自识别，支持协议异常检测，支持自定义IPS签名 |
| 病毒检测 | 支持文件型杀毒（深度扫描）引擎病毒扫描功能；可直接过滤超大文件、密码保护文件、受损文件、超解压层数文件； |
| 支持对需要扫描的文件指定扩展名、指定文件大小、指定响应方式、指定解压层数达到20层； |
| 支持基于HTTP/HTTPS/FTP的内容及病毒检测 |
| 数据安全 | 基于内容感知数据防泄露，对传输的文件和内容进行识别过滤；  20+文件还原和内容过滤，如Word、Excel、PPT、PDF等），60+文件类型过滤。 |
| 攻击防范 | 支持基于应用层协议的攻击防范包括：HTTP、HTTPS、DNS、SIP 等Flood攻击 |
| 支持流量自学习功能，可设置流量自学习时间，并自动生成DDOS攻击防范策略。 |
| 流量控制 | 支持可识别应用层协议数量≥5000种 |
| 可支持基于应用层协议设置流控策略，包括设置最大带宽、保证带宽、协议流量优先级等。 |
| 支持基于地理位置的流量分析，支持基于地理位置的流量控制,支持基于地理位置的流量统计 |
| 多出口智能选路 | 支持内嵌移动、电信、联通、教育网的IP地址表，可根据目的地址智能优选运营商链路 |
| 支持主备接口配置以及按比例分配的负载分担方式 |
| 可靠性 | 支持双机热备，可配置主主、主备方式，双机会话同步。 |
| 支持BFD链路检测，并与VRRP进行联动实现双机快速切换。 |
| 日志审计 | 支持静态环比报表功能，可以基于日、月进行流量/攻击防护/URL访问/应用阻断等的环比统计分析，对一个周期的管理策略提供依据 |
| 产品资质 | 具有公安部颁发的防火墙《计算机信息系统安全专用产品销售许可证》，提供证书复印件 |
| 具有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》，提供证书复印件 |
| 保修服务 | 原厂5年免费保修，中标后提供原厂5年质保。 |

## 七、设备材料总体要求

1、投标人所投设备材料必须是厂商全新的，型号、性能及指标符合国家及招标文件提出的有关技术、质量、安全标准。

2.所有设备材料在开箱检验时必须完好，无破损，配置与装箱单相符。数量、质量及性能不低于招标文件的要求。对投标产品的关键性指标，若发现中标产品不符合要求的, 用户有权要求通过第三方测试机构对中标产品进行验收，以确保产品实际质量及性能满足需求。对不满足招标文件指标要求的产品，采购人有权不对其进行验收,并上报相关监管部门,费用由中标方承担。投标产品的具体指标中要求提供第三方测试报告、产品手册截图等证明材料均为复印件，投标方必须如实提供，为防止虚假应标，用户有权进行事后查证，如发现提供虚假证明的，采购人将上报相关监管部门处置，由此造成的后果由中标方承担。

3、设备材料外观清洁，标记编号等字体清晰，明确。铭牌、使用指示、警告指示应以中文或英文及易懂的通用符号来表示；应准确无误地表明型号、规格、制造厂及生产或出厂日期。

4、对于影响设备材料正常工作的必要组成部分，无论在技术规范中指出与否，投标人都应提供并在投标文件中明确列出。

5、所有设备材料提供出厂合格证等质量证明文件。

6、随带资料齐全，并在工程验收后统一移交给采购人。

## 八、运输、保管、保险

1、投标人应承诺负责设备材料到现场或采购人指定的地点过程中的全部运输，包括装卸车、设备材料现场的搬运。

2、投标人应承诺承担设备材料在移交前的保管责任。

3、投标人应承诺承担设备材料在移交前的保险负责，并承诺承担其派出的现场服务人员人身意外保险。

## 九、项目集成及实施服务要求（与评分标准对应）

**1、系统集成具体技术方案要求**

投标技术具体方案内容必须遵照招标文件要求，提供完整、清晰、结构合理，无遗漏、无歧义的技术设计方案，且必须体现以下内容（共14分）：

（1）全省消防信息网接入政务外网网络规划设计技术方案要求。

（2）全省消防信息网接入政务外网政府侧实施方案要求。

（3）全省消防信息网应急管理系统A类、B类、C类迁移割接上线方案。

**2项目进度计划要求**

投标方应提供详细的项目实施计划，应满足项目进度要求，且包括针对本项目的：工程组织计划、测试计划、运行维护服务计划、实施过程及流程与质量控制措施、应急保障措施、实施完成后交付的成果文档以及其它认为需要的说明的内容；安全设备需提供原厂人员硬件设备实施计划。

**3、项目实施人员能力要求**

投标人应针对本项目建立项目管理及技术支持团队，项目组成员具备集成维护经验和能力、具有相应技术资质，负责专网整合现场实施工作，并在期间应充分了解安装进度要求，保证施工质量，解决施工中出现的技术问题，具体要求如下（共8分）：

（1）项目负责人1名，具备PMP及CCIE等证书（2分）、具备5年以上省电子政务外网集成维护经验和能力（出具相关证明，否则不得分）（2分）；

（2）要求至少具有4名网络工程师，每个网络工程师具备CCIE或H3CTE或HCIE等同等水平资质（2分）；

（3）要求至少具有3名安全工程师，每个安全工程师具备CISP或CISA或CISSP等资质（2分）；

（4）要求至少具有5名数据库工程师，其中高级数据库工程师不少于2人，要求具备高级证书。中级数据库工程师不少于3人，要求具备中级证书。(2分)

备注：提供以上相关人员证书复印件以及相关简介证明材料。

**4、现场安装与调试**

投标方指定的工程师提前联系各节点项目负责人，确认链路的放置是否到位，并协商确定节点工程实施时间。

投标方需派指定的工程师到达现场，确认节点施工环境，并确认本地的网络拓扑结构、IP地址、路由配置使用情况、现有主要设备、端口、模块使用情况等，备份相关网络设备配置文件，并与节点技术人员商定工程实施细则及安排工程实施进度。

**5、项目验收要求**

各节点工程实施完成，投标方提交详细的节点工程项目文档（包括节点网络连接图、设备配置说明、日常维护手册、故障申报流程及联系方式等）后，由投标方工程师与节点技术人员共同进行节点初验，并填写节点工程测试验收单。

全省所有节点工程完成，中标方向采购方提交详细的整体工程项目文档，全省网络系统正常试运行一个月后，由采购方组织整体工程验收。

**6、其它要求**

（1）中标人应确保其技术建议以及所提供的设备的完整性、实用性，保证全部系统及时投入正常运行。否则若出现因中标方提供的设备不满足要求、不合理，或者其所提供的技术支持和服务不全面，而导致系统无法实现或不能完全实现的状况，中标供应商负全部责任。

（2）项目实施过程中因缺少设备、配件或服务导致采购人网络系统无法正常运行，中标方须承诺免费提供。中标方在项目实施、线路迁移割接、设备安装调试和业务应用网络迁移过程中，若需要第三方单位配合，由此产生的费用由中标方承担。项目实施过程中，若因技术问题需要讨论、论证、咨询，以及项目验收等产生的费用，由中标方承担。

（3）为有序推进项目实施，中标人应在项目实施前，与用户协商组织一次全省项目启动会议，负责安排联络人员、会议地点、项目总体安排等事宜并承担相关费用。

**7、验收标准**

市级消防信息网接入改造由各消防救援支队自行组织项目验收；省级消防信息网接入改造，在中标方提交全省项目实施总结报告、各级市消防救援支队接入改造验收单后，由省消防救援总队统一组织全省项目终验。

**资信商务需求:**

|  |  |
| --- | --- |
| 供货时间（项目工期） | 5年 |
| 供货地点（项目地点） | 浙江省各地市 |
| 违约责任及争议解决方式 | 按相关违约责任及争议解决方式处置。 |
| 售后服务-项目维护计划 | 质保期：整体软硬件五年原厂服务和售后维护服务，包括系统软件版本、特征规则库等升级。合同签订时提供所有设备购买原厂服务的证明材料。在运行维护期内发现质量缺陷的，中标人应当负责返工或者采取补救措施。质保期内所有的服务均为免费上门服务。投标人应具备交钥匙工程的能力。投标人的服务应包括产品提供、配套设备提供、设备安装、调试、保修及保修期外的有偿维护,投标人需提供五年“7×24”的专门电话技术服务，提供一站服务电话，并必须在1小时内对所提出的维修及服务要求做出实质性响应，必要时必须提供现场服务。 |
| 售后服务-响应情况 | 系统故障处理：中标人提供7\*24小时电话支持，网络运行过程中如果出现技术故障，投标方应保证线路故障4小时内完成故障修复；针对网络设备故障及系统配置故障投标方应保证6小时内完成故障修复，恢复网络正常运行。若需要更换故障件，则提供相同档次的备机供使用。 |
| 售后服务-本地化服务要求 | 须有完善的长期本地化的售后服务机构和服务体系，能提供及时、周到的本地化技术支持。 |
| 售后服务-技术培训 | 为相关人员提供业务培训，培训内容为本项目相关的数据通信产品、数据配置以及网络和系统运维工作等内容。 培训费用：本项目培训所产生的费用，包括应包含在总报价中费用，无需在报价明细表中单独列报。所有培训费用（食宿费用、场地费用、教材费用等）应包含在本次项目中，不可另外向采购人收费如有最新规定，按财政最新规定列支。 |
| 履约能力-公司技术力量情况 | 在全省范围内具备网元出租能力，具备工信部颁发的基础电信运营许可证等。 |
| 履约能力-经验或业绩要求 | 提供2017年1月1日以来类似项目案例合同复印件。 |
| 付款条件-付款方式 | 项目初验合格后，支付合同款的20%；第二年3月1日前，支付至合同款的40%；第三年3月1日前，支付至合同款的60%；第四年3月1日前，支付至合同款的80%；合同期满后1一个月内，支付至合同款的100%。； |

**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）：

**鉴证方:** 浙江省政府采购中心

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

**一、项目内容及合同价格**

金额单位：元

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

注：1.项目具体技术需求及采购人地址等详见招标文件、投标文件以及询标记录。

　2.以上合同总价包含项目达到预期使用效果所需的一切费用。

**二、技术资料**

1.乙方应按招标文件规定的时间向甲方提供使用项目的有关技术资料。

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

**三、知识产权**

乙方应保证所提供的货物或其任何一部分均不会侵犯任何第三方的知识产权。

**四、产权担保**

乙方保证所交付的货物的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。

**五、转包或分包**

不允许转包。

允许分包部分 。

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

**六、质保期和履约保证金**

1.质保期 年。（自项目验收合格交付使用之日起计）

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

**七、项目工期及实施地点**

1.交货期：

2.实施地点：

**八、货款支付**

付款方式：

**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。

**十二、货物包装**

详见招标文件。

**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《浙江省合同管理办法》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、鉴证方三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，须经采购中心、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.本合同未尽事宜，遵照《合同法》有关条文执行。

5.本合同一式六份，具有同等法律效力，甲、乙、鉴证三方各执二份。

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

合同鉴证方（盖章）:

法定代表人或主要负责人:

鉴证日期: 年 月 日

**第六章 投标文件格式附件**

附件1**：** 正本或副本

项目名称

项目编号：ZZCG2020H-GK-112（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，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）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）提供有效的依法缴纳税收证明（完税凭证或税务部门出具的证明）；

（5）提供有效的依法缴纳社会保障资金证明（缴纳凭证或人社部门出具的证明）；

（6）联合投标协议书（若需要）;

（7）联合投标授权委托书（若需要）;

（8）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ZZCG2020H-GK-112）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.我方参与本项目前3年内的经营活动中没有重大违法记录；**

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：

授权代表身份证号码：

授权代表联系手机：

授权代表邮箱：

法定代表人签名（或签名章）： 职务：

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**：**  正本或副本

项目名称

项目编号：ZZCG2020H-GK-112（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）投标方认为需要的其他文件资料。

附件7：

**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8：

**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9：

**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10：

**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11：

**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12：

**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13**：**  正本或副本

项目名称

项目编号：（标项 ）

**报**

**价**

**文**

**件**

投标人全称：

地 址：

时 间：

3、**报价文件目录**

（1）投标报价明细表（见附件14）；

（2）投标人针对报价需要说明的其他文件和说明（格式自拟）；

（3）小微企业声明函（见附件15）；

（4）残疾人福利企业声明函（见附件16）。

附件14：

**投 标 报 价 明 细 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** | |
| **是否小微企业** | **企业全称** |
| **…** | |  |  | |  |  |  |  |  |  |
| **服务类** | | | | | | | | | | |
| **服务内容** | | | | **服务人员数量** | | **工作量** | **单价**  **（元）** | **总价（元）** | **制造商情况** | |
| **是否小微企业** | **企业全称** |
| **…** | | | |  | |  |  |  |  |  |
| **小微企业价格合计金额大写： 小写： ￥** | | | | | | | | | | |
| **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.小微企业价格合计金额应与“制造商为小微企业”的明细报价汇总相等（如有错误修正，以修正后的明细报价为准），评标委员会按前附表“小微企业有关政策”要求对小微企业价格进行确认，并对符合要求的小微企业价格部分给予价格扣除。**  5**.**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15：

**小微企业声明函**

本公司郑重声明，根据《政府采购促进中小企业发展暂行办法》（财库〔2011〕181号）的规定，本公司为 （请填写：小型、微型）企业。即，本公司同时满足以下条件：

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

2.本公司参加 单位的 项目采购活动提供本企业制造的货物，由本企业承担工程、提供服务，或者提供其他 （请填写：小型、微型）企业制造的货物。本条所称货物不包括使用大型企业注册商标的货物。

本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日 期：

**备注说明：**

1.《小微企业声明函》中，须同时满足以上两个条件。若投标人提供非本企业制造的货物，其制造商也须为小型、微型企业；

2.若联合体投标时，联合体各方均为小型、微型企业的，联合体各方均须提供《小微企业声明函》；联合体其中一方为小型、微型企业的，联合协议中须约定小型、微型企业的协议合同金额占到联合体协议合同总额30%以上。

附件16：

**残疾人福利性单位声明函**

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

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

单位名称（盖章）：

日 期：