**浙江省公路与运输管理中心高速公路联网运行省中心系统网络**

**安全等保三级建设项目**

项目编号：ZZCG2019R-GK-117

**公**

**开**

**招**

**标**

**文**

**件**

浙江省政府采购中心

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** 3](#_Toc496796635)

[**第二章 投标人须知** 5](#_Toc496796636)

[**第三章 评标办法及评分标准** 21](#_Toc496796637)

[**第四章 招标需求** 24](#_Toc496796638)

[**第五章 浙江省政府采购合同主要条款指引** 76](#_Toc496796639)

[**第六章 投标文件格式附件** 81](#_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：ZZCG2019R-GK-117**

**二、公告期限：5个工作日**

**三、采购项目内容、数量及预算**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 标项 | 采购内容 | 单位 | 数量 | 预算（万元） | 最高限价（万元） | 使用单位 |
| 1 | 高速公路联网运行省中心系统网络安全等保三级建设项目 | 项 | 1 | 900 | 860 | 省公路与运输管理中心 |

**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：**

**标项1：不允许联合体投标。**

**五、投标报名：**

1、报名时间：2019年8月8日至2019年8月27日上午08:30-11:30；下午14:30-17:00（节假日除外）。

2、报名方式：本项目实行网上报名，不接受现场报名。供应商登录浙江政府采购网（http://www.zjzfcg.gov.cn）进行报名。

《供应商网上报名操作指南》网址：浙江政府采购网，位置：“首页-办事指南-省采中心-网上报名”（ [http://www.zjzfcg.gov.cn/bs\_other/2018-03-30/12002.html?\_=2018-03-30 11:40:47](http://www.zjzfcg.gov.cn/bs_other/2018-03-30/12002.html?_=2018-03-30%2011:40:47)）。

3、招标文件售价：0元，招标文件请至公告附件处下载。

**六、投标保证金：0元（空或0元为无需交纳）。**

**七、投标截止时间和地点：**

投标人应于2019年8月28日9:00时前半小时内派授权代表将投标文件密封送交到杭州市环城北路305号耀江发展中心二楼大会议室，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，并携带身份证及法定代表人授权书有效证明出席）**投标人在递交投标文件时另行提供投标文件送达回执、政府采购活动现场确认声明书（格式详见附件，不密封进投标文件）。**

**八、开标时间及地点：**

本次招标将于2019年8月28日9:00时整在杭州市环城北路305号耀江发展中心二楼大会议室开标，投标人可以派授权代表出席开标会议。

**九、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://www.zjzfcg.gov.cn/new> （文件下载、公告查询） |
| **咨询事项** | **联系方式** | **传真** | **备注** |
| 项目联系人 | 张女士0571-88907711 | 0571-88907783 | 三楼 |
| 项目投标报名 | 陈女士0571-88907723 | 0571-88907704 | 一楼（服务大厅） |
| 项目监督 | 高先生0571-88907706 | 0571-88907751 | 三楼（采购监督部） |
| 网站系统问题 | 40088171904008371020 | / | 注册、账号等 |
| / | 其他问题 |

**十、采购需求咨询**

|  |  |
| --- | --- |
| **采购单位** | 浙江省公路与运输管理中心 |
| **咨询事项** | **联系人** | **联系方式** | **传真** | **备注** |
| 采购需求等 | 赵先生 | 0571-87813837 |  |  |

**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》二 |
| 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，请提供财政部、环境保护保部发布有效期内环境标志产品政府采购清单以及财政部、发改委联合发布有效期内节能产品政府采购清单。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，投标人须提供该清单内产品，**否则其投标将作为无效标处理。** |
| 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 %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的《中小企业声明函》以及本单位、制造商（如有）“国家企业信用信息公示系统——小微企业名录”页面查询结果（查询时间为投标前一周内，并加盖本单位公章），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%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提出，逾期不予受理。 |
| 6 | 是否允许采购进口产品： | 否。 |
| 7 | 是否允许转包与分包 | 转包：否**分包：安全厂商原厂安全服务、安全厂商运维人员驻场服务、三级等保测评允许分包。** |
| 8 | 是否接受联合体投标 | 否。 |
| 9 | 是否现场踏勘 | 否。 |
| 10 | 是否提供演示 | **否。** |
| 11 | 是否提供样品 | 否。 |
| 12 | 投标文件组成 | **每个标项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6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://www.zjzfcg.gov.cn](http://www.zjzfcg.gov.cn/new))发布中标公告，公告期限为1个工作日，服务台根据报名时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半小时内接收投标文件，投标文件送达回执、政府采购活动现场确认声明书（格式详见附件）应单独提供，如投标人递交投标文件时未提供回执，视同不需要回执。**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、未成功办理投标人报名手续的；****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”系指组织本项目采购的浙江省政府采购中心。

2、“投标人”系指向招标方提交投标文件的单位或个人。

3、“采购人” 系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”系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”系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”系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(www.zjzfcg.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、投标报价文件三部份组成。**具体详见“第六章 投标文件格式附件”。**

**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。**活页装订（是指用卡条、抽杆夹、订书机等形式装订，使标书可以拆卸或者在翻动过程中易脱落的一种装订方式）的投标文件将作无效标处理。**

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://www.zjzfcg.gov.cn/new/ ，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、组织开、评标程序及评标委员会的评审程序**

**（一）组织开标程序**

招标方将按照招标文件规定的时间、地点和程序组织开标，各投标人授权代表及相关人员应参加开标会并接受核验、签到，无关人员不得进入开标现场。投标人如不派授权代表参加开标会的，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、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，组织投标人签署不存在影响公平竞争的《政府采购活动现场确认声明书》。

2、对投标人保证金缴纳情况进行查验、核实，提请投标人代表或公证人员查验投标文件密封情况并签名确认，如投标人代表对密封情况有不同意见的，按照少数服从多数的原则，以多数投标人意见为准。

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，同时告知投标人代表拆封报价文件的预计时间。对不符合装订要求的投标文件，由现场工作人员退还供应商代表。

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，无效投标人代表可收回未拆封的报价文件并签字确认。

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，由投标人代表、唱标人、记录人和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。投标人授权代表未到现场的，或开标记录不予确认且不说明理由的，视为无异议。唱标结束后，现场工作人员将报价文件及开标记录表护送至指定评审地点，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）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、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》。

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。

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，应通知该投标人以书面形式作出澄清或说明。授权代表未到场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》，服务台根据报名时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**

## 标项1：

|  |  |  |
| --- | --- | --- |
| **评分项目** | **分值** | **评标要点及说明** |
| 价格（30） | 30 | 满足招标文件要求且投标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）\*30 |
| 技术（50） | 20 | 指标参数：1.符合招标文件中明确指标参数的得16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3分（扣完为止）。2.符合以下明确需求的得4分。据投标人选择的态势感知平台系统处理性能满足详细技术要求中的描述；支持和现网安全产品联动，策略下发；基于流量对资产进行识别；支持对资产漏洞进行监控，并能对高危漏洞进行自动化验证；支持边界完整性检测，对非法内外联行为进行识别等。 |
| 2 | 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2分），无实质性意义的正偏离不加分。 |
| 2 | 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。**（如属于非单一产品采购项目的，以采购人确定的核心产品为准）** |
| 8 | 项目技术解决方案：1.项目总体解决方案：投标人对用户联网运行省中心系统现状（包括设备型号、配置、运行环境、功能情况）以及问题和需求的了解是否全面、详尽、准确；详细阐述系统的建设目标、架构规划、实现思路和关键技术，提出具体可行的实施解决方案（4分）。2.项目关键性技术解决方案：投标人对项目重点、难点的理解，以及与现网网络安全设备联动上，与等保三级建设标准匹配上，与部路网中心并网要求中关于国密加密等建设内容上是否具有完整、先进、合理、切实可行的关键性技术解决方案（4分）。 |
| 10 | 项目实施计划方案及兼容性方案：1. 项目实施计划方案：包括到货时间安排、人员配置、施工进度安排、安装调试及试运行安排、等保三级测评通过等详细计划安排（3分）；2. 项目可行性实施计划方案：包括投标人对用户骨干通信路由环网现状（包括设备型号、配置、运行环境、功能情况）以及问题和需求的了解是否全面、详尽、准确；详细阐述针对骨干通信环网的调优规划、安全防护建设思路，详细阐述各骨干通信路由节点与路段单位连接调优规划（4分）；3. 项目具体兼容性方案：根据投标人选择的安全类产品和现网安全产品、安全管理平台，提供无缝兼容方案，包括统一管理、产品方案对用户前期安全投资的保护性、产品扩展性、部署时考虑采购人现有的系统架构等（3分）。 |
| 8 | 项目组人员能力**(具体对应招标需求)** |
| 商务（20） | 售后服务（10） | 3 | 项目维护计划（驻点人员安排，定期巡检，备品备件等情况）的有效性等**(具体对应商务要求表)** |
| 3 | 售后服务的响应情况（对用户故障响应、处理等）**(具体对应商务要求表)** |
| 2 | 本地化服务**(具体对应商务要求表)** |
| 2 | 培训方案、计划的可行性及合理性**(具体对应商务要求表)** |
| 履约能力（10） | 5 | 公司技术力量情况**(具体对应商务要求表)** |
| 3 | 经验及业绩**(具体对应商务要求表)** |
| 2 | 投标文件编制有序、装订整齐、书面整洁、内容详实 |

**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产品范围（详见财政部国家发展改革委关于\*\*\*节能产品政府采购清单的通知），但最新一期节能清单中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：高速公路联网运行省中心系统网络安全等保三级建设项目**

## 概况

2001年底，浙江省全面实施全省高速公路联网收费，目前，全省高速公路联网里程4200多公里，经营业主54家， 11个市级ETC服务处，7000多个ETC一站式服务网点，423个收费站，ETC用户数700万，2018年全年高速公路通行费收入359亿元。

高速公路联网运行省中心系统是一个7×24实时运行的业务生产系统，是全省高速公路联网运营的基础应用平台，是高速公路联网收费管理、运行监控管理、ETC发行与服务的核心业务系统，是保障各高速公路业主利益，保障收费站正常收费，保障全省各ETC网点业务办理实现“最多跑一次”的关键系统。

我省高速公路收费、监控、通信系统实行联网运行，全省高速公路通信网系统由两个层次组成：

1.路段通信系统 : 指各路段通信中心连接其所辖分中心、收费站的通信系统，主要完成路段内部的传输任务。

2.骨干通信系统 : 指连接省中心和各路段通信中心的骨干网络系统，负责省中心与各路段通信中心之间的传输任务。

目前，全省高速公路骨干通信网已建成骨干通信站13个，包括省中心站、彭埠站、半山站、萧山站、丽水站、金华站、台州站、温州站、傅村站、湖州站、杭州南站、嘉兴站、宁波西站等。

全省高速公路联网运行骨干通信系统采用DPT/IP技术构建，带宽2.5G，通过动态包传输技术实现高效故障恢复，路由协议使用成熟的OSPF动态路由协议，为全路网的收费、监控（数据、图像）、通信业务等提供骨干级传输平台，保障全省高速公路联网运行业务不间断实时运行。

省中心系统通过一台cisco N9k核心交换机与各服务器相连，并通过cisco12410路由器与骨干通信网相连。省中心局域网中已经部署了部分网络安全产品，所有网络连接出口都部署了防火墙，此外还采用了网站防护、漏洞扫描及其他日志审计、双因素认证、准入控制等安全系统，采用一套安全管理中心对防火墙、漏扫等安全设备进行统一管理。省中心网络已经具备了一定的安全防护能力，但离等保三级标准还有一定的差距。

## 工程目标和要求

根据《国务院办公厅关于印发深化收费公路制度改革取消高速公路省界收费站实施方案的通知》（国办发[2019]23号）、《交通运输部关于印发联网收费系统省域并网接入网络安全基本技术要求的通知》（交科技函[2019]338号）的相关规定，联网收费系统整体网络安全按照等级保护第三级进行定级、备案、建设、测评、保护。

为使省中心系统需满足等保三级要求，从结构安全角度出发，针对骨干网络链路、骨干网络设备和关键的安全设备，需要提供冗余性设计，且性能冗余50%以上，因此综合考虑现网网络安全架构，针对核心交换机、核心路由器、核心防火墙等关键节点进行冗余部署。

另外根据第三方测评单位出具的差距分析结果，当前省中心系统在入侵防范、安全审计等方面的符合程度上还不够完善，欠缺专业的入侵防范措施及运维安全管理(堡垒机)系统、数据库审计系统，且现网的日志审计系统存储记录也无法达到6个月以上要求。

同时基于等保2.0标准和交通部并网安全接入要求，系统应具备针对威胁的主动感知和主动防御的能力，需要并行建设针对全网风险监测的安全预警平台及态势感知平台，态势感知平台能与交通部态势感知平台进行对接，上报安全日志报告。

根据交通部要求，使用国密算法完成部-省通信线路的数据加密传输及数据完整性保证，以及国密RA中心的建设。

此外由于信息安全的动态性，随着时间的变化会不断暴露出新的安全漏洞、恶意软件、攻击手段，新业务的上线也会给原有安全体系带来新的变化和挑战，打破原有信息安全的平衡。为此仅仅依靠静态的安全设备还无法匹配动态的安全形势，为此需要以专业的安全服务手段来弥补设备无法解决的问题，并针对性解决现网问题和潜在风险，为现网业务的安全可靠运行提供保障。

结合以上内容，本次工程主要目标及要求如下：

1. 增补1台高性能核心交换机，与现有核心交换机形成设备级冗余，满足等保三级建设要求。
2. 现有cisco3850接入交换机增加4端口万兆光口模块。
3. 增补万兆核心防火墙，并与现网核心防火墙形成双机热备，毫米级切换
4. 增补万兆防火墙，与现网边界部署的万兆防火墙做冷备，防止因边界防火墙单点故障而造成业务影响
5. 增补万兆IPS入侵防御系统，对省中心与骨干通信网、外联边界进行安全防护加固。
6. 规划建设独立的针对外联单位进行数据和视频等的数据交换区，采用专业安全隔离与信息交换系统对数据、视频交换进行安全防护。
7. 规划建设数据业务区，对数据业务区内服务器集群进行应用负载建设。
8. 规划建设独立的维护接入区并进行安全加固。
9. 在联网运行省中心系统部署运维安全管理（堡垒机）系统、数据库审计系统及对现网日志审计系统设备进行扩容升级，满足等保三级要求。
10. 规划建设态势感知系统，采用主动监测和防御的方式来提前发现并解决未知或未发现的威胁，并可针对网络资产的漏洞、违规外联行为进行检测和定位。
11. 针对骨干通信环网进行网络调优，同时针对与路段中心对接的边界进行安全加固建设。
12. 针对钱江新城ETC中心边界进行安全防护加固建设。
13. 对现网安全管理平台进行定制开发，满足对新增设备的安全管理和配置。
14. 针对联网运行省中心系统向安全厂商购买为期1年的原厂商安全服务。
15. 针对联网运行省中心系统向安全厂商购买为期1年的2人原厂商驻场人员服务。
16. 针对现网PC、windows server服务器、Lunix服务器采购部署网络版杀毒软件，完成病毒防护及漏洞补丁升级更新。
17. 针对省中心应用软件系统按照等保三级相关的软件安全要求进行升级改造。
18. 按照交通运输部要求，在联网运行省中心系统部署国密RA中心，建设国密应用支撑平台。
19. 根据三级等保的要求，协助甲方完善修订相关网络安全管理制度。
20. **通过三级等保的测评及相关整改，最终在年内取得备案证书。**

## 项目范围

投标人应提供本项目相关设备设施的提供、运输、交货、安装、调试、试运行、培训、文件、交付使用、保修、技术服务等工作项目，主要内容有（但不限于此）：

1台核心交换机、若干台防火墙、若干台万兆IPS、1套安全隔离与信息交换系统、1台数据库审计、1台堡垒机、1套态势感知平台、1年安全厂商原厂安全服务、2人1年原厂商安全运维人员驻场服务、杀毒软件、应用软件安全改造、国密RA中心及国密应用支撑平台建设（应用安全网关和签名服务器）等设备设施的供货、安装、调试及安全服务等（详见项目清单）；

所有设备、设施安装调试、售后服务所需的备件、专用仪器、工具及交通车辆等的提供；

在合同中未提到的但为工程完工所需的基本材料和附属材料的提供。

## 详细技术要求

1. **物理机房改造**
2. 按照等保三级2.0标准要求，针对现有物理机房环境进行改造，增加防盗报警等内容。
3. 针对现有物理机房中的48个服务器机柜间光缆、线缆进行综合布线，需考虑本次新增设备的走线等。
4. **核心交换机（核心产品）**

|  |  |
| --- | --- |
| **功能类别** | **技术要求及指标** |
| 机型 | 国内主流品牌 |
| ▲交换容量 | ≥184Tbps |
| 包转发率 | ≥11500Mbps |
| ▲产品架构 | 采用正交CLOS架构，支持独立的交换网板，配置独立交换网模块≥5 |
| 主控引擎 | 实配主控引擎≥2，满足1+1冗余，主控槽位与交换网板槽位（或业务卡槽位）宽度相同的全宽槽位，提供更好的扩展性和可靠性 |
| 业务槽位 | ≥8 |
| 电源模块 | 实配电源模块≥2，满足1+1冗余 |
| 端口配置 | 至少96个SFP+ 1/10G光口，24个万兆以太网电口，96个千兆以太网电口，配置万兆光模块45块，前兆光模块15块。 |
| 多业务板卡 | 支持防火墙业务板、无线控制业务板、流量分析业务板、应用控制网关业务板； |
| VLAN特性 | 支持基于端口的VLAN，支持基于协议的VLAN； |
| 支持基于MAC的VLAN； |
| 最大VLAN数(不是VLAN ID)>=4094 |
| 镜像功能 | 支持本地端口镜像和远程端口镜像RSPAN； |
| 支持流镜像 |
| 同时支持N：M的端口镜像（M大于1） |
| 路由协议 | 支持IPv4静态路由、RIP V1/V2、OSPF |
| 支持IPv6静态路由、RIPng |
| 管理和维护 | 支持SNMP V1/V2/V3、RMON、SSHV2 |
| 支持OAM(802.1AG， 802.3AH)以太网运行、维护和管理标准 |
| 为方便维护，交换机与网络管理平台采用同一品牌 |
| 链路聚合 | 聚合组数≥128组，每组成员≥8个 |
| 支持跨设备链路聚合 |
| 支持对广播、组播、单播报文的均匀分担 |
| 支持链路聚合+ECMP情况也可以对报文均匀分担，即等价路由的链路是由聚合链路组成情况下的报文分担 |
| ACL | 支持双向ACL，ACL≥4K |
| 支持端口ACL |
| 支持VLAN ACL |
| QOS | 每端口支持8个优先级队列，3个丢弃优先级，支持SP、WRR、SP+WRR三种队列调度算法 |
| 支持精细化的流量监管，粒度可达8K |
| 支持流量整形Shapping |
| 支持WRED拥塞避免 |
| 支持802.1p、TOS、DSCP、EXP优先级映射 |
| 可靠性 | 双引擎快速倒换，主备切换时候板内转发无丢包  |
| 支持NSF/GR for OSFP/BGP/IS-IS |
| 支持热补丁功能，可在线进行补丁升级 |
| 支持BFD，BFD for VRRP/BGP/IS-IS/OSPF/RSVP/LDP/RIP/静态路由。 |
| 支持N：1虚拟化，N≥4 |
| MPLS | 支持L3 VPN |
| 支持VLL |
| 支持VLPS |
| 支持MCE |
| 跨三层互联技术 | 支持主流的MAC in IP技术，如EVI/EVN/OTV等，实现跨三层网络的二层互联 |
| 安全特性 | 支持IPv4 uRPF |
| 支持DHCP Snooping |
| 支持ARP防攻击 |
| 支持IP Source Guard |
| 支持CoPP |
| 支持广播风暴抑制 |
| 支持EAD |
| 支持IEEE 802.1ae介质访问控制安全技术 |
| 支持端口隔离 |
| 支持IP+MAC+VLAN+PORT的绑定 |
| 支持报文过滤功能，黑洞路由、黑洞MAC |
| 管理特性 | 支持Console/AUX/Telnet/SSH2.0 |
| 支持风扇管理 |
| 支持电源管理 |
| 支持在线诊断 |
| 支持SNMPv1/v2 |
| 支持 SNMPv3 |
| 支持RMON(RFC2819) |
| 支持端口镜像 |
| 支持VLAN镜像 |
| 支持RSPAN |
| 支持流镜像 |
| 认证 | 支持802.1x |
| 支持mac认证 |
| 支持Portal |
| 支持本地认证 |
| 支持Radius认证 |
| 支持Tacacs+认证 |
| **产品要求（提供证书复印件或证明材料）** | **为实现降低能源消耗、提高能源利用率、促进国家节能减排的目标。投标产品在设计、研发、生产、过程中符合国家节能标准。产品生产厂商需通过能源管理体系认证(认证覆盖的业务范围包括本次投标产品)；** |
| **产品制造厂商应具有健全的环保体系，建立有害物质的检测手段，严格管理产品采购和生产环节，禁止或控制有毒有害物质的使用。通过QC 080000有害物质过程管理体系认证(认证覆盖的业务范围包括本次投标产品)；** |
| **为响应国家低碳的要求，产品厂商在产品设计、研发、生产、过程需采取有效减少温室气体排放措施，符合国家温室气体排放和清除的量化和报告的规范。产品生产厂商需通过ISO 14064温室气体核查(认证覆盖的业务范围包括本次投标产品)** |
| **其他** | **原厂三年质保，合同签订后3个工作日内提供原厂商三年质保服务承诺函** |

1. **3850交换机4端口万兆光口模块**

现有cisco 3850接入交换机万兆光口不足，需增加4端口万兆上联光口板卡。

1. **万兆防火墙**

|  |  |  |
| --- | --- | --- |
| **技术指标** | **指标项** | **参数要求** |
|  | 机型 | 国产品牌 |
| 系统硬件要求 | 架构平台 | 2U高度标准19寸设备，多核处理器架构，电源、风扇等部件冗余设计 |
| ▲接口要求 | 接口配置：≥4个万兆光接口, ≥2个千兆电口和≥4个千兆光电复用接口，≥4个扩展插槽，并含2个高速USB2.0接口，1个RJ45串口，配置4个万兆多模光模块；扩展1块4端口千兆电接口卡 |
| 安全系统 | **要求具备自主研发的安全操作系统，并提供该安全操作系统的软件著作权证书复印件** |
| 型号说明 | 投标产品必须为现有平台销售产品； |
| 配置文件 | 要求支持多配置文件引导，支持一键回滚及定时保存配置文件 |
| 配置概览 | 支持配置概览功能， 在该功能下可浏览设备所有安全策略的配置，简化运维 |
| 功能特性 | 全面具备下一代防火墙功能，支持IPS应用层防护、异常侵入行为管控、DDOS防护 |
| ▲性能要求 | 吞吐量 | ≥30Gbps |
| 并发连接数 | ≥600万 |
| 每秒新建连接数 | ≥30万 |
| VPN隧道数 | 支持IPsec VPN、SSL VPN；IPSec VPN性能≥10Gbps，内置硬件加密芯片，本次实际配置≥300个SSLvpn授权 |
| 访问控制 | IPv4基本策略 | 支持能够基于源/目的安全域、源/目的地址（网络地址对象、网络地址组、域名）、源/目的MAC（MAC地址对象、MAC地址对象组）、服务（预定义服务对象、自定义服务对象、服务组）、生效时间、策略动作、策略启用或禁用； |
| IPv6基本策略 | 支持能够基于源/目的安全域、源/目的地址（网络地址对象）、源/目的MAC（MAC地址对象、MAC地址对象组）、服务（预定义服务对象、自定义服务对象、服务组）、扩展头（知名头部：逐条选项、目的选项、路由首部、分片首部、认证首部、安全净荷封装）、动作、生效时间、状态（启用、禁用）、匹配计数；  |
| 高级策略 | 支持多种访问控制的策略动作：允许通过、拒绝通过及应用层的高级安全业务控制；支持对一条访问控制条目同时进行QoS流量标记、应用级访问控制、URL分类过滤、行为审计、防病毒、入侵防御等策略；  |
| 策略组管理 | 支持策略组管理、策略筛选（可根据策略组名称、策略名称、源安全域、目的安全域、源地址、目的地址、服务、状态等条件进行筛选查看）、显示/隐藏列等功能；  |
| URL过滤 | 支持对域名的IP解析，并可作为地址资源被访问控制策略引用，实现对域名地址的访问控制； |
| 支持使用自定义URL分类和预定义URL分类配置URL黑/白名单，并支持自定义推送消息； |
| 地址转换 | 地址转换类型 | 支持源IP地址转换、目的IP地址转换、一对一IP地址转换、多对多地址转换； |
| ALG功能 | 支持FTP、GTP、H.323、IRC、MMS、PPTP、RPC、DNS、TFTP、SIP等预定义协议的ALG功能，且支持自定义ALG协议； |
| 端口块NAT | 支持端口块NAT，能够提供NAT溯源特性； |
| 组播NAT | 支持组播源NAT、组播目的NAT功能； |
| IPv6 NAT | 支持NAT64、NAT66、DS-Lite等IPv6环境下的地址转换技术； |
| 入侵防御能力 | 提供基于对恶意攻击行为、病毒传播行为的检测防护并提供可视化告警和溯源；可提供最新的威胁情报信息，官方网站每周会进行安全通告，能够对新爆发的流行高危漏洞进行预警和自动检测； |
| 病毒防护能力 | 具备对HTTP，FTP，SMTP，POP3协议进行病毒文件检测；具备杀毒白名单功能，可以根据URL或者IP进行排除不检测病毒；检测到病毒后的操作支持阻断，记录杀毒日志； |
| 安全可视化 | 支持对被保护对象的流量进行分析，发现被保护对象的不同业务流量情况，支持生成和导出相关报告；支持对被保护对象的流量进行分析，通过对流量日志的统计整理，智能生成包过滤策略，提高运维人员工作效率；支持自定义统计指定IP/用户组/用户/应用在指定时间段内的攻击事件及审计日志等内容，并形成报表；支持每天/每周/每月自动生成报表，并将报表自动发送到指定邮箱，可以自定义报表内容；支持报表以HTML、Excel、PDF等格式导出；支持通过命令行的方式对数据流进行分析，帮助迅速定位网络故障 |
| 安全监测 | 支持安全设备的集中管理，包括配置统一下发，规则库统一更新，安全日志，流量日志实时上报等功能。支持接入统一的安全监测平台，通过安全监测平台可以实时看到每台安全设备的详细安全状态信息，包括安全评分级别、最近有效事件、有效事件趋势、用户安全统计、服务器安全统计和攻击来源统计。支持所有安全设备的安全日志汇总，并能够通过时间、严重等级、动作、ip、用户、特征/漏洞ID等多个条件查询过滤日志。 |
| 支持通过命令行的方式对数据流进行分析，帮助迅速定位网络故障 |
| **产品要求****（提供证书复印件）** | **具备中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证（增强级）》；** |
| **具有中国国家保密局测评中心颁发的《涉密信息系统产品检测证书》；** |
| **具有中国国家信息安全测评认证中心颁发的《信息技术产品安全测评证书－EAL3+》；** |
| **设备厂商要求（提供证书复印件）** | **提供QC080000电气与电子元件和产品有害物质过程控制管理体系认证；** |
| **提供CMMI5级软件成熟度认证证书；** |
| **提供《TL9000质量管理体系认证证书》；** |
| 其他要求 | 能够与现网万兆核心防火墙联动，实现冗余双机，并可实现设备配置状态及会话状态实时同步，故障切换时间毫秒级。 |
| 能够接受现网安全管理平台的统一管理，实现拓扑生成，配置下发，日志呈现等。 |
| **保修服务** | **原厂三年质保，合同签订后3个工作日内提供原厂商三年质保服务承诺函** |

1. **防火墙一**

|  |  |  |
| --- | --- | --- |
| **技术指标** | **指标项** | **参数要求** |
| 设备选型 | 机型 | 国产品牌 |
| 系统硬件要求 | 架构平台 | 多核处理器架构，电源、风扇等部件冗余设计 |
| ▲配置要求 | 配置≥8个千兆电口和≥16个千兆非复用光口，≥2个万兆光口，支持≥2个扩展插槽，1个RJ45串口。配置2个万兆多模光模块 |
| 安全系统 | **要求具备自主研发的安全操作系统，并提供该安全操作系统的软件著作权证明** |
| 型号说明 | 投标产品必须为现有平台销售产品 |
| 配置文件 | 要求支持多配置文件引导，支持一键回滚及定时保存配置文件 |
| 配置概览 | 支持配置概览功能， 在该功能下可浏览设备所有安全策略的配置，简化运维 |
| 功能特性 | 全面具备下一代防火墙功能，支持IPS应用层防护、异常侵入行为管控、DDOS防护 |
| ▲性能要求 | 吞吐量 | ≥20Gbps |
| 并发连接数 | ≥400万 |
| 每秒新建连接数 | ≥15万 |
| VPN隧道数 | 支持IPsec VPN、SSL VPN；IPSec VPN性能≥6Gbps，内置硬件加密芯片，本次实际配置≥300个SSLvpn授权 |
| 访问控制 | IPv4基本策略 | 支持能够基于源/目的安全域、源/目的地址（网络地址对象、网络地址组、域名）、源/目的MAC（MAC地址对象、MAC地址对象组）、服务（预定义服务对象、自定义服务对象、服务组）、生效时间、策略动作、策略启用或禁用； |
| IPv6基本策略 | 支持能够基于源/目的安全域、源/目的地址（网络地址对象）、源/目的MAC（MAC地址对象、MAC地址对象组）、服务（预定义服务对象、自定义服务对象、服务组）、扩展头（知名头部：逐条选项、目的选项、路由首部、分片首部、认证首部、安全净荷封装）、动作、生效时间、状态（启用、禁用）、匹配计数；  |
| 高级策略 | 支持多种访问控制的策略动作：允许通过、拒绝通过及应用层的高级安全业务控制；支持对一条访问控制条目同时进行QoS流量标记、应用级访问控制、URL分类过滤、行为审计、防病毒、入侵防御等策略；  |
| 策略组管理 | 支持策略组管理、策略筛选（可根据策略组名称、策略名称、源安全域、目的安全域、源地址、目的地址、服务、状态等条件进行筛选查看）、显示/隐藏列等功能；  |
| URL过滤 | 支持对域名的IP解析，并可作为地址资源被访问控制策略引用，实现对域名地址的访问控制； |
| 支持使用自定义URL分类和预定义URL分类配置URL黑/白名单，并支持自定义推送消息； |
| 地址转换 | 地址转换类型 | 支持源IP地址转换、目的IP地址转换、一对一IP地址转换、多对多地址转换； |
| ALG功能 | 支持FTP、GTP、H.323、IRC、MMS、PPTP、RPC、DNS、TFTP、SIP等预定义协议的ALG功能，且支持自定义ALG协议； |
| 端口块NAT | 支持端口块NAT，能够提供NAT溯源特性； |
| 组播NAT | 支持组播源NAT、组播目的NAT功能； |
| IPv6 NAT | 支持NAT64、NAT66、DS-Lite等IPv6环境下的地址转换技术； |
| 安全可视化 | 支持对被保护对象的流量进行分析，发现被保护对象的不同业务流量情况，支持生成和导出相关报告；支持对被保护对象的流量进行分析，通过对流量日志的统计整理，智能生成包过滤策略，提高运维人员工作效率；支持自定义统计指定IP/用户组/用户/应用在指定时间段内的攻击事件及审计日志等内容，并形成报表；支持每天/每周/每月自动生成报表，并将报表自动发送到指定邮箱，可以自定义报表内容；支持报表以HTML、Excel、PDF等格式导出；支持通过命令行的方式对数据流进行分析，帮助迅速定位网络故障 |
| 安全监测 | 支持安全设备的集中管理，包括配置统一下发，规则库统一更新，安全日志，流量日志实时上报等功能。支持接入统一的安全监测平台，通过安全监测平台可以实时看到每台安全设备的详细安全状态信息，包括安全评分级别、最近有效事件、有效事件趋势、用户安全统计、服务器安全统计和攻击来源统计。支持所有安全设备的安全日志汇总，并能够通过时间、严重等级、动作、ip、用户、特征/漏洞ID等多个条件查询过滤日志。 |
| 支持通过命令行的方式对数据流进行分析，帮助迅速定位网络故障 |
| 入侵防御能力 | 提供基于对恶意攻击行为、病毒传播行为的检测防护并提供可视化告警和溯源；可提供最新的威胁情报信息，官方网站每周会进行安全通告，能够对新爆发的流行高危漏洞进行预警和自动检测； |
| 病毒防护能力 | 具备对HTTP，FTP，SMTP，POP3协议进行病毒文件检测；具备杀毒白名单功能，可以根据URL或者IP进行排除不检测病毒；检测到病毒后的操作支持阻断，记录杀毒日志； |
| **产品要求（提供证书复印件）** | **具备中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证（增强级）》；** |
| **具有中国国家保密局测评中心颁发的《涉密信息系统产品检测证书》；** |
| **具有中国国家信息安全测评认证中心颁发的《信息技术产品安全测评证书－EAL3+》；** |
| **设备厂商要求（提供证书复印件）** | **提供QC080000电气与电子元件和产品有害物质过程控制管理体系认证；** |
| **提供CMMI5级软件成熟度认证证书；** |
| **提供《TL9000质量管理体系认证证书》；** |
| 其他要求 | 能够接受现网安全管理平台的统一管理，实现拓扑生成，配置下发，日志呈现等。 |
| **保修服务** | **原厂三年质保，合同签订后3个工作日内提供原厂商三年质保服务承诺函。** |

1. **防火墙二**

|  |  |  |
| --- | --- | --- |
| **技术指标** | **指标项** | **参数要求** |
| 设备选型 | 机型 | 国产品牌 |
| 系统硬件要求 | 架构平台 | 多核处理器架构，电源、风扇等部件冗余设计 |
| ▲接口要求 | 配置≥8个千兆电口和≥16个千兆非复用光口，≥2个万兆光口，支持≥2个扩展插槽，1个RJ45串口。配置万兆多模光模块1个，千兆多模光模块1个；配置三年IPS特征库、病毒库升级许可。 |
| 安全系统 | **要求具备自主研发的安全操作系统，并提供该安全操作系统的软件著作权证书复印件** |
| 型号说明 | 投标产品必须为现有平台销售产品 |
| 配置文件 | 要求支持多配置文件引导，支持一键回滚及定时保存配置文件； |
| 配置概览 | 支持配置概览功能，在该功能下可浏览设备所有安全策略的配置，简化运维； |
| 功能特性 | 全面具备下一代防火墙功能，具备IPS应用层防护、异常侵入行为管控、DDOS防护。 |
| ▲性能要求 | 吞吐量 | ≥20Gbps |
| 并发连接数 | ≥400万 |
| 每秒新建连接数 | ≥15万 |
| VPN隧道数 | 支持IPsec VPN、SSL VPN；IPSec VPN性能≥6Gbps，内置硬件加密芯片，本次实际配置≥300个SSLvpn授权 |
| 访问控制 | IPv4基本策略 | 支持能够基于源/目的安全域、源/目的地址（网络地址对象、网络地址组、域名）、源/目的MAC（MAC地址对象、MAC地址对象组）、服务（预定义服务对象、自定义服务对象、服务组）、生效时间、策略动作、策略启用或禁用； |
| IPv6基本策略 | 支持能够基于源/目的安全域、源/目的地址（网络地址对象）、源/目的MAC（MAC地址对象、MAC地址对象组）、服务（预定义服务对象、自定义服务对象、服务组）、扩展头（知名头部：逐条选项、目的选项、路由首部、分片首部、认证首部、安全净荷封装）、动作、生效时间、状态（启用、禁用）、匹配计数；  |
| 高级策略 | 支持多种访问控制的策略动作：允许通过、拒绝通过及应用层的高级安全业务控制；支持对一条访问控制条目同时进行QoS流量标记、应用级访问控制、URL分类过滤、行为审计、防病毒、入侵防御等策略；  |
| 策略组管理 | 支持策略组管理、策略筛选（可根据策略组名称、策略名称、源安全域、目的安全域、源地址、目的地址、服务、状态等条件进行筛选查看）、显示/隐藏列等功能；  |
| URL过滤 | 支持对域名的IP解析，并可作为地址资源被访问控制策略引用，实现对域名地址的访问控制； |
| 支持使用自定义URL分类和预定义URL分类配置URL黑/白名单，并支持自定义推送消息； |
| 地址转换 | 地址转换类型 | 支持源IP地址转换、目的IP地址转换、一对一IP地址转换、多对多地址转换； |
| ALG功能 | 支持FTP、GTP、H.323、IRC、MMS、PPTP、RPC、DNS、TFTP、SIP等预定义协议的ALG功能，且支持自定义ALG协议； |
| 端口块NAT | 支持端口块NAT，能够提供NAT溯源特性； |
| 组播NAT | 支持组播源NAT、组播目的NAT功能； |
| IPv6 NAT | 支持NAT64、NAT66、DS-Lite等IPv6环境下的地址转换技术； |
| 安全可视化 | 支持对被保护对象的流量进行分析，发现被保护对象的不同业务流量情况，支持生成和导出相关报告；支持对被保护对象的流量进行分析，通过对流量日志的统计整理，智能生成包过滤策略，提高运维人员工作效率；支持自定义统计指定IP/用户组/用户/应用在指定时间段内的攻击事件及审计日志等内容，并形成报表；支持每天/每周/每月自动生成报表，并将报表自动发送到指定邮箱，可以自定义报表内容；支持报表以HTML、Excel、PDF等格式导出；支持通过命令行的方式对数据流进行分析，帮助迅速定位网络故障 |
| 安全监测 | 支持安全设备的集中管理，包括配置统一下发，规则库统一更新，安全日志，流量日志实时上报等功能。支持接入统一的安全监测平台，通过安全监测平台可以实时看到每台安全设备的详细安全状态信息，包括安全评分级别、最近有效事件、有效事件趋势、用户安全统计、服务器安全统计和攻击来源统计。支持所有安全设备的安全日志汇总，并能够通过时间、严重等级、动作、ip、用户、特征/漏洞ID等多个条件查询过滤日志。 |
| 支持通过命令行的方式对数据流进行分析，帮助迅速定位网络故障 |
| 入侵防御能力 | 提供基于对恶意攻击行为、病毒传播行为的检测防护并提供可视化告警和溯源；可提供最新的威胁情报信息，官方网站每周会进行安全通告，能够对新爆发的流行高危漏洞进行预警和自动检测； |
| 病毒防护能力 | 具备对HTTP，FTP，SMTP，POP3协议进行病毒文件检测；具备杀毒白名单功能，可以根据URL或者IP进行排除不检测病毒；检测到病毒后的操作支持阻断，记录杀毒日志； |
| **产品要求（提供证书复印件）** | **具备中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证（增强级）》；** |
| **具有中国国家保密局测评中心颁发的《涉密信息系统产品检测证书》；** |
| **具有中国国家信息安全测评认证中心颁发的《信息技术产品安全测评证书－EAL3+》；** |
| **厂商要求（提供证书复印件）** | **提供QC080000电气与电子元件和产品有害物质过程控制管理体系认证；** |
| **提供CMMI5级软件成熟度认证证书；** |
| **提供《TL9000质量管理体系认证证书》。** |
| 其他要求 | 能够无缝兼容现网安全管理平台，进行统一管理，实现拓扑生成，配置下发，日志呈现等。 |
| **保修服务** | **三年原厂维保，中标后签订合同时提供所投产品原厂商三年质保函、原厂授权书。** |

1. **万兆IPS一**

|  |  |
| --- | --- |
| **指标项** | **规格要求** |
| 设备选型 | 国产品牌  |
| ▲配置要求 | 要求具备自主研发的安全操作系统，无已知安全漏洞, 且非OEM产品**，提供软件著作权证书复印件** |
| 本次投标产品必须为标准机架的专业IPS设备，不能提供防火墙或UTM的IPS功能。 |
| 配置≥8个千兆光口，≥8个千兆电口，≥4个万兆光口，满足以上接口配置后冗余不少于2个扩展槽位；配置双电源； 配套2对光口PFP掉电保护，并配置8个万兆多模光模块； |
| 配置不少于3年病毒库和攻击特征库升级； |
| ▲性能要求 | 安全处理能力≥10Gbps |
| 并发连接数≥800W |
| 每秒新建连接数≥15W |
| 设备生命周期 | 投标产品必须为现有平台销售产品 |
| 部署方式 | 支持透明、透明桥接、旁路等部署模式，支持带内、带外管理 |
| 基本攻击防护 | 内置IPS特征库，特征规则数量不少于6100条，并可根据CVE编号查询具体的攻击特征；具备系统一键修改特征级别的功能，用户可根据自身安全需求将特征内容根据流行度规则高低进行检索，并可一键修改流行度规则级别（警告、一般、严重、致命、废除） |
| 入侵防御事件库应符合国家信息安全CNNVD漏洞库标准，事件描述为中文；事件特征库在线升级频率不少于一周一次 |
| 支持畸形包攻击防范，支持针对协议漏洞的畸形包攻击防范，对LAND、死亡之Ping、IP分片重叠、UDP Fraggle、WinNuke、ICMP Smurf、Tear Drop等常见攻击的检测防御，并可根据用户自身安全需求设置相应防护策略 |
| 病毒防护 | 集成第三方专业防病毒厂商的专业病毒库，特征规则数量不少于10000条； |
| 具备对病毒感染主机或黑客主机的网络隔离功能，用户可以根据自身的安全需求设置高、中、低三种流行度规则，可以设置告警、阻断、邮件病毒替换、TCP Reset等方式进行防御，并且用户可以自定义配置告警推送内容； |
| 未知威胁防护 | 具备虚拟环境检测引擎，通过在虚拟环境中运行文件，跟踪并记录其行为，基于大数据的统计分类及动态行为分析等技术，有效识别未知威胁；支持HTTP、FTP、SMB、POP3、IMAP、SMTP等协议，满足复杂网络需求下的未知威胁防护； |
| 可识别多种文件类型，如压缩文件（rar、zip、tar、gz、tgz、z、cab、7z等）、文档文件（ppt、pot、pptx、doc、dot、docx、xls、xlsx、wps、pdf、rtf等）、其他文件（dll、exe、html、js、py、swf、swc等）； |
| DDoS攻击防护 | 支持IPv4、IPv6环境下对每个IP的新建速率设置阈值并进行监控，支持对TCP、ICMP、UDP等协议下报文速率的阈值设置，并可根据用户自身需求设置防护级别；支持对SYN Flood、UDP Flood、ICMP Flood等攻击设置防护策略 |
| 支持对会话维持时间参数进行调整，如TCP会话、UDP会话、GRE会话、PPTP GRE会话、ESP会话等，以优化系统资源利用率，避免设备本身被拒绝服务攻击 |
| 具备DDOS自定义指纹防护，可根据报文长度、TTL值、源目的端口和IP、序列号、flag标记等信息构成的正常流量模型进行指纹防护，并可根据用户需求设置相应的检测、防护阈值及多种防护动作； |
| 应用控制 | 支持基于IP地址、域名、HTTPS主机名、正则表达式的URL过滤功能，可扩展URL特征库，特征规则数量不少于350万条，实现高风险、不良网站过滤，用户可自定义配置告警推送内容； |
| 支持应用管控功能，可识别超过5000种应用协议，包括文件共享、电子邮件应用、网络游戏、即时通讯、网络电视、数据库应用、Web应用、P2P下载、金融证券、移动音乐等，且支持基于类型、协议、参数等维度自定义应用。支持通过源IP、目的IP、应用类型、时间等维度进行应用管控； |
| 支持敏感信息防护，通过识别系统内部敏感数据、文件类型，对敏感数据使用情况进行监控从而保障用户敏感信息不被泄露，可基于文件传输、电子邮件、即时通讯等应用对敏感信息如银行卡号、身份证号、手机号等进行有效防护，且支持在不同的时间生效不同的防护策略。 |
| 网络特性 | 可以在IPv4/IPv6双栈、MPLS等复杂网络环境下良好的工作，可以识别并检测QinQ、PPPoE、MPLS、GRE、Vlan等特殊封装的网络报文，具备面向下一代网络的各种特性； |
| 攻击取证 | 支持攻击取证功能：支持查看攻击事件明细，分析攻击源目的IP及端口，并可针对攻击事件分析攻击报文内容，便于分析提取关键攻击特征； |
| 威胁可视化 | 支持攻击监控平台，可对用户整网安全情况进行大致评估，统计攻击总数、高危事件、被拦截数。可图形化展示出攻击事件的地理位置分布情况，实时展示攻击日志及攻击趋势，具有攻击源排行及攻击目的排行。针对某些关键攻击事件可展现出当前攻击所在阶段，直观展现用户网络安全状况。 |
| 支持未知威胁监控平台，可实时展示未知威胁日志，支持恶意域名、恶意IP、恶意邮箱、恶意FTP的排名统计与展示。 |
| 系统功能 | 系统具备健康状态异常告警机制，发现异常状态时可通过邮件、短信等各种方式及时通知管理员，告警触发条件可设置； |
| 支持基于物理接口或vlan配置虚拟引擎，每个虚拟引擎能够支持资源分配，如：吞吐量、CPU使用率、内存使用率等，每个虚拟引擎可由超级管理员分配独立的用户名和密码，并且各个虚拟引擎可独立配置防护策略； |
| 支持IPv4、IPv6环境下部署，NTP时钟同步可提供Server、Client两种模式，支持认证加密； |
| 支持实现配置的自动同步和手动同步，保证会话同步； |
| 支持页面登录、指纹登录方式，支持Web图形界面配置，支持SSH、、TELNET、CONSOLE命令行模式配置和集中管理模式； |
| 报表展示 | 系统应提供丰富的报表功能，支持TopN事件、TopN源地址、TopN目的地址、TopN服务、事件类型分布与趋势、危险程度分类统计与趋势等多种报表模板； |
| 为便于分析，还应支持用户自定义报表模版，能够按照用户需求生成各种风格的统计报表； |
| 支持攻击取证，可以基于攻击事件、攻击时间等维度查询具体的攻击事件明细，如攻击的源目的MAC、源目的IP、源目的端口，并可获取到相应攻击的报文内容，便于分析攻击特点； |
| 系统应具备地址簿功能，在报表中可直观显示所有攻击事件的攻击源IP所处省份或某个运营商等信息； |
| 日志管理 | 支持网管软件统一网管，支持SNMPv1，SNMPv2c和SNMPv3；支持通过SNMP用户进行认证，支持认证加密和数据传输加密功能； |
| 提供Syslog日志，操作日志，业务日志的查询功能并提供对日志的多种查询方式；可以根据日志监控到接口状态信息、设备状态信息变更；可以基于时间维度、IP地址范围、关键字查询操作日志，监控到访问者的IP地址以及访问的功能模块； |
| 支持设备性能监控，可监控cpu、内存利用率、磁盘剩余空间和在线状态监控； |
| 系统支持以中文图表形式输出流量报表、安全报表、综合报表；支持doc、excel、pdf等格式的报表生成，并支持通过邮件等多种方式输出。报表支持日报、周报、月报和年报，并且支持对设备、IP群组、单台主机形式输出以上报表； |
| 支持告警和日志管理功能：支持攻击事件触发告警、支持告警通知（短信，邮件、声音）、支持告警过滤、支持自定义日志存储时间、支持告警日志和操作日志支持转储功能； |
| **产品要求（提供证书复印件）** | **具备中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》；** |
| **具备国家保密科技检测中心《涉密信息系统产品检测证书》** |
| **具备中国信息安全测评中心《国家信息安全测评信息技术产品安全测评证书EAL3+级》** |
| **具备IPv6 Forum《IPv6 Ready Logo Phase-2证书》** |
| **厂家要求（提供证书或相关证明复印件）** | **具备中国信息安全测评中心颁发的《信息安全服务资质-安全工程类二级》资质；** |
| **具备中国信息安全认证中心颁发的《信息安全应急处理一级》资质；** |
| **具备中国信息安全认证中心颁发的《信息安全风险评估服务一级》资质；** |
| **信息安全设备、系统软件的开发、生产符合TL9000-HS R6.0/R5.5标准；** |
| **具备中国信息安全测评中心颁发的《国家信息安全漏洞库（CNNVD）技术支撑单位等级证书（一级）》；** |
| **具备能力成熟度模型集成认证CMMI5。** |
| **其他要求** | **IPS能够接受现网安全管理平台的统一管理，实现拓扑生成，配置下发，日志呈现等，需详细描述实现方式或提供实现证明。** |
| **保修服务** | **原厂三年质保，合同签订后3个工作日内提供原厂商三年质保服务承诺函** |

1. **万兆IPS二**

|  |  |
| --- | --- |
| **指标项** | **规格要求** |
| 设备选型 | 国产品牌 |
| ▲配置要求 | 要求具备自主研发的安全操作系统，无已知安全漏洞, 且非OEM产品,**提供软件著作权证书复印件** |
| 本次投标产品必须为标准机架的专业IPS设备，不能提供防火墙或UTM的IPS功能。 |
| 配置≥8个千兆光口，≥8个千兆电口，≥4个万兆光口，满足以上接口配置后冗余不少于2个扩展槽位；配置双电源； 配套3对光口PFP掉电保护，并配置6个万兆多模，12个千兆多模光模块； |
| 配置不少于3年病毒库和攻击特征库升级； |
| 性能要求 | 安全处理能力≥10Gbps |
| 并发连接数 | 并发连接数≥800W |
| 每秒新建连接数 | 每秒新建连接数≥15W |
| 设备生命周期 | 投标产品必须为现有平台销售产品 |
| 部署方式 | 支持透明、透明桥接、旁路等部署模式，支持带内、带外管理 |
| 基本攻击防护 | 内置IPS特征库，特征规则数量不少于6100条，并可根据CVE编号查询具体的攻击特征；具备系统一键修改特征级别的功能，用户可根据自身安全需求将特征内容根据流行度规则高低进行检索，并可一键修改流行度规则级别（警告、一般、严重、致命、废除）； |
| 入侵防御事件库应符合国家信息安全CNNVD漏洞库标准，事件描述为中文；事件特征库在线升级频率不少于一周一次 |
| 支持畸形包攻击防范，支持针对协议漏洞的畸形包攻击防范，对LAND、死亡之Ping、IP分片重叠、UDP Fraggle、WinNuke、ICMP Smurf、Tear Drop等常见攻击的检测防御，并可根据用户自身安全需求设置相应防护策略； |
| 病毒防护 | 集成第三方专业防病毒厂商的专业病毒库，特征规则数量不少于10000条； |
| 具备对病毒感染主机或黑客主机的网络隔离功能，用户可以根据自身的安全需求设置高、中、低三种流行度规则，可以设置告警、阻断、邮件病毒替换、TCP Reset等方式进行防御，并且用户可以自定义配置告警推送内容； |
| 未知威胁防护 | 具备虚拟环境检测引擎，通过在虚拟环境中运行文件，跟踪并记录其行为，基于大数据的统计分类及动态行为分析等技术，有效识别未知威胁；支持HTTP、FTP、SMB、POP3、IMAP、SMTP等协议，满足复杂网络需求下的未知威胁防护； |
| 可识别多种文件类型，如压缩文件（rar、zip、tar、gz、tgz、z、cab、7z等）、文档文件（ppt、pot、pptx、doc、dot、docx、xls、xlsx、wps、pdf、rtf等）、其他文件（dll、exe、html、js、py、swf、swc等）； |
| DDoS攻击防护 | 支持IPv4、IPv6环境下对每个IP的新建速率设置阈值并进行监控，支持对TCP、ICMP、UDP等协议下报文速率的阈值设置，并可根据用户自身需求设置防护级别；支持对SYN Flood、UDP Flood、ICMP Flood等攻击设置防护策略 |
| 支持对会话维持时间参数进行调整，如TCP会话、UDP会话、GRE会话、PPTP GRE会话、ESP会话等，以优化系统资源利用率，避免设备本身被拒绝服务攻击； |
| 具备DDOS自定义指纹防护，可根据报文长度、TTL值、源目的端口和IP、序列号、flag标记等信息构成的正常流量模型进行指纹防护，并可根据用户需求设置相应的检测、防护阈值及多种防护动作； |
| 应用控制 | 支持基于IP地址、域名、HTTPS主机名、正则表达式的URL过滤功能，可扩展URL特征库，特征规则数量不少于350万条，实现高风险、不良网站过滤，用户可自定义配置告警推送内容； |
| 支持应用管控功能，可识别超过5000种应用协议，包括文件共享、电子邮件应用、网络游戏、即时通讯、网络电视、数据库应用、Web应用、P2P下载、金融证券、移动音乐等，且支持基于类型、协议、参数等维度自定义应用。支持通过源IP、目的IP、应用类型、时间等维度进行应用管控； |
| 支持敏感信息防护，通过识别系统内部敏感数据、文件类型，对敏感数据使用情况进行监控从而保障用户敏感信息不被泄露，可基于文件传输、电子邮件、即时通讯等应用对敏感信息如银行卡号、身份证号、手机号等进行有效防护，且支持在不同的时间生效不同的防护策略； |
| 网络特性 | 可以在IPv4/IPv6双栈、MPLS等复杂网络环境下良好的工作，可以识别并检测QinQ、PPPoE、MPLS、GRE、Vlan等特殊封装的网络报文，具备面向下一代网络的各种特性； |
| 攻击取证 | 支持攻击取证功能：支持查看攻击事件明细，分析攻击源目的IP及端口，并可针对攻击事件分析攻击报文内容，便于分析提取关键攻击特征； |
| 威胁可视化 | 支持攻击监控平台，可对用户整网安全情况进行大致评估，统计攻击总数、高危事件、被拦截数。可图形化展示出攻击事件的地理位置分布情况，实时展示攻击日志及攻击趋势，具有攻击源排行及攻击目的排行。针对某些关键攻击事件可展现出当前攻击所在阶段，直观展现用户网络安全状况。 |
| 支持未知威胁监控平台，可实时展示未知威胁日志，支持恶意域名、恶意IP、恶意邮箱、恶意FTP的排名统计与展示。 |
| 系统功能 | 系统具备健康状态异常告警机制，发现异常状态时可通过邮件、短信等各种方式及时通知管理员，告警触发条件可设置； |
| 支持基于物理接口或vlan配置虚拟引擎，每个虚拟引擎能够支持资源分配，如：吞吐量、CPU使用率、内存使用率等，每个虚拟引擎可由超级管理员分配独立的用户名和密码，并且各个虚拟引擎可独立配置防护策略； |
| 支持IPv4、IPv6环境下部署，NTP时钟同步可提供Server、Client两种模式，支持认证加密； |
| 支持实现配置的自动同步和手动同步，保证会话同步； |
| 支持页面登录、指纹登录方式，支持Web图形界面配置，支持SSH、、TELNET、CONSOLE命令行模式配置和集中管理模式； |
| 报表展示 | 系统应提供丰富的报表功能，支持TopN事件、TopN源地址、TopN目的地址、TopN服务、事件类型分布与趋势、危险程度分类统计与趋势等多种报表模板； |
| 为便于分析，还应支持用户自定义报表模版，能够按照用户需求生成各种风格的统计报表； |
| 支持攻击取证，可以基于攻击事件、攻击时间等维度查询具体的攻击事件明细，如攻击的源目的MAC、源目的IP、源目的端口，并可获取到相应攻击的报文内容，便于分析攻击特点； |
| 系统应具备地址簿功能，在报表中可直观显示所有攻击事件的攻击源IP所处省份或某个运营商等信息； |
| 日志管理 | 支持网管软件统一网管，支持SNMPv1，SNMPv2c和SNMPv3；支持通过SNMP用户进行认证，支持认证加密和数据传输加密功能； |
| 提供Syslog日志，操作日志，业务日志的查询功能并提供对日志的多种查询方式；可以根据日志监控到接口状态信息、设备状态信息变更；可以基于时间维度、IP地址范围、关键字查询操作日志，监控到访问者的IP地址以及访问的功能模块； |
| 支持设备性能监控，可监控cpu、内存利用率、磁盘剩余空间和在线状态监控； |
| 系统支持以中文图表形式输出流量报表、安全报表、综合报表；支持doc、excel、pdf等格式的报表生成，并支持通过邮件等多种方式输出。报表支持日报、周报、月报和年报，并且支持对设备、IP群组、单台主机形式输出以上报表； |
| 支持告警和日志管理功能：支持攻击事件触发告警、支持告警通知（短信，邮件、声音）、支持告警过滤、支持自定义日志存储时间、支持告警日志和操作日志支持转储功能； |
| **产品要求（提供证书复印件）** | **具备中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》；** |
| **具备国家保密科技检测中心《涉密信息系统产品检测证书》；** |
| **具备中国信息安全测评中心《国家信息安全测评信息技术产品安全测评证书EAL3+级》；** |
| **具备IPv6 Forum《IPv6 Ready Logo Phase-2证书》；** |
| **厂家要求（提供证书或相关证明复印件）** | **具备中国信息安全测评中心颁发的《信息安全服务资质-安全工程类二级》资质；** |
| **具备中国信息安全认证中心颁发的《信息安全应急处理一级》资质；** |
| **具备中国信息安全认证中心颁发的《信息安全风险评估服务一级》资质；** |
| **信息安全设备、系统软件的开发、生产符合TL9000-HS R6.0/R5.5标准；** |
| **具备中国信息安全测评中心颁发的《国家信息安全漏洞库（CNNVD）技术支撑单位等级证书（一级）》；** |
| **具备能力成熟度模型集成认证CMMI5** |
| **其他要求** | **IPS能够接受现网安全管理平台的统一管理，实现拓扑生成，配置下发，日志呈现等。** |
| **保修服务** | **原厂三年质保，合同签订后3个工作日内提供原厂商三年质保服务承诺函。** |

1. **IPS三**

|  |  |
| --- | --- |
| **指标项** | **规格要求** |
| 设备选型 | 国产品牌 |
| ▲硬件配置要求 | 要求具备自主研发的安全操作系统，无已知安全漏洞, 且非OEM产品,提供软件著作权证书 |
| 配置≥16个千兆光口，≥8个非复用千兆电口，满足以上接口配置后冗余不少于2个扩展槽位，最大可扩展至24个千兆接口+2个万兆接口；配置双电源； 配置不少于6个千兆多模光模块 |
| 配置不少于3年病毒库和攻击特征库升级； |
| 性能要求 | 安全处理能力≥2Gbps |
| 并发连接数 | 并发连接数≥300W |
| 每秒新建连接数 | 每秒新建连接数≥5W |
| 设备生命周期 | 投标产品必须为现有平台销售产品 |
| 部署方式 | 支持透明、透明桥接、旁路等部署模式，支持带内、带外管理 |
| 基本攻击防护 | 内置IPS特征库，特征规则数量不少于6100条，并可根据CVE编号查询具体的攻击特征；具备系统一键修改特征级别的功能，用户可根据自身安全需求将特征内容根据流行度规则高低进行检索，并可一键修改流行度规则级别（警告、一般、严重、致命、废除）； |
| 入侵防御事件库应符合国家信息安全CNNVD漏洞库标准，事件描述为中文；事件特征库在线升级频率不少于一周一次 |
| 支持畸形包攻击防范，支持针对协议漏洞的畸形包攻击防范，对LAND、死亡之Ping、IP分片重叠、UDP Fraggle、WinNuke、ICMP Smurf、Tear Drop等常见攻击的检测防御，并可根据用户自身安全需求设置相应防护策略； |
| 病毒防护 | 集成第三方专业防病毒厂商的专业病毒库，特征规则数量不少于10000条； |
| 具备对病毒感染主机或黑客主机的网络隔离功能，用户可以根据自身的安全需求设置高、中、低三种流行度规则，可以设置告警、阻断、邮件病毒替换、TCP Reset等方式进行防御，并且用户可以自定义配置告警推送内容； |
| 未知威胁防护 | 具备虚拟环境检测引擎，通过在虚拟环境中运行文件，跟踪并记录其行为，基于大数据的统计分类及动态行为分析等技术，有效识别未知威胁；支持HTTP、FTP、SMB、POP3、IMAP、SMTP等协议，满足复杂网络需求下的未知威胁防护； |
| 可识别多种文件类型，如压缩文件（rar、zip、tar、gz、tgz、z、cab、7z等）、文档文件（ppt、pot、pptx、doc、dot、docx、xls、xlsx、wps、pdf、rtf等）、其他文件（dll、exe、html、js、py、swf、swc等）； |
| DDoS攻击防护 | 支持IPv4、IPv6环境下对每个IP的新建速率设置阈值并进行监控，支持对TCP、ICMP、UDP等协议下报文速率的阈值设置，并可根据用户自身需求设置防护级别；支持对SYN Flood、UDP Flood、ICMP Flood等攻击设置防护策略 |
| 支持对会话维持时间参数进行调整，如TCP会话、UDP会话、GRE会话、PPTP GRE会话、ESP会话等，以优化系统资源利用率，避免设备本身被拒绝服务攻击； |
| 具备DDOS自定义指纹防护，可根据报文长度、TTL值、源目的端口和IP、序列号、flag标记等信息构成的正常流量模型进行指纹防护，并可根据用户需求设置相应的检测、防护阈值及多种防护动作； |
| 应用控制 | 支持基于IP地址、域名、HTTPS主机名、正则表达式的URL过滤功能，可扩展URL特征库，特征规则数量不少于350万条，实现高风险、不良网站过滤，用户可自定义配置告警推送内容； |
| 支持应用管控功能，可识别超过5000种应用协议，包括文件共享、电子邮件应用、网络游戏、即时通讯、网络电视、数据库应用、Web应用、P2P下载、金融证券、移动音乐等，且支持基于类型、协议、参数等维度自定义应用。支持通过源IP、目的IP、应用类型、时间等维度进行应用管控； |
| 支持敏感信息防护，通过识别系统内部敏感数据、文件类型，对敏感数据使用情况进行监控从而保障用户敏感信息不被泄露，可基于文件传输、电子邮件、即时通讯等应用对敏感信息如银行卡号、身份证号、手机号等进行有效防护，且支持在不同的时间生效不同的防护策略。 |
| 网络特性 | 可以在IPv4/IPv6双栈、MPLS等复杂网络环境下良好的工作，可以识别并检测QinQ、PPPoE、MPLS、GRE、Vlan等特殊封装的网络报文，具备面向下一代网络的各种特性； |
| 攻击取证 | 支持攻击取证功能：支持查看攻击事件明细，分析攻击源目的IP及端口，并可针对攻击事件分析攻击报文内容，便于分析提取关键攻击特征； |
| 威胁可视化 | 支持攻击监控平台，可对用户整网安全情况进行大致评估，统计攻击总数、高危事件、被拦截数。可图形化展示出攻击事件的地理位置分布情况，实时展示攻击日志及攻击趋势，具有攻击源排行及攻击目的排行。针对某些关键攻击事件可展现出当前攻击所在阶段，直观展现用户网络安全状况。 |
| 支持未知威胁监控平台，可实时展示未知威胁日志，支持恶意域名、恶意IP、恶意邮箱、恶意FTP的排名统计与展示。 |
| 系统功能 | 系统具备健康状态异常告警机制，发现异常状态时可通过邮件、短信等各种方式及时通知管理员，告警触发条件可设置； |
| 支持基于物理接口或vlan配置虚拟引擎，每个虚拟引擎能够支持资源分配，如：吞吐量、CPU使用率、内存使用率等，每个虚拟引擎可由超级管理员分配独立的用户名和密码，并且各个虚拟引擎可独立配置防护策略； |
| 支持IPv4、IPv6环境下部署，NTP时钟同步可提供Server、Client两种模式，支持认证加密； |
| 支持实现配置的自动同步和手动同步，保证会话同步； |
| 支持页面登录、指纹登录方式，支持Web图形界面配置，支持SSH、、TELNET、CONSOLE命令行模式配置和集中管理模式； |
| 报表展示 | 系统应提供丰富的报表功能，支持TopN事件、TopN源地址、TopN目的地址、TopN服务、事件类型分布与趋势、危险程度分类统计与趋势等多种报表模板； |
| 为便于分析，还应支持用户自定义报表模版，能够按照用户需求生成各种风格的统计报表； |
| 支持攻击取证，可以基于攻击事件、攻击时间等维度查询具体的攻击事件明细，如攻击的源目的MAC、源目的IP、源目的端口，并可获取到相应攻击的报文内容，便于分析攻击特点； |
| 系统应具备地址簿功能，在报表中可直观显示所有攻击事件的攻击源IP所处省份或某个运营商等信息； |
| 日志管理 | 支持网管软件统一网管，支持SNMPv1，SNMPv2c和SNMPv3；支持通过SNMP用户进行认证，支持认证加密和数据传输加密功能； |
| 提供Syslog日志，操作日志，业务日志的查询功能并提供对日志的多种查询方式；可以根据日志监控到接口状态信息、设备状态信息变更；可以基于时间维度、IP地址范围、关键字查询操作日志，监控到访问者的IP地址以及访问的功能模块； |
| 支持设备性能监控，可监控cpu、内存利用率、磁盘剩余空间和在线状态监控； |
| 系统支持以中文图表形式输出流量报表、安全报表、综合报表；支持doc、excel、pdf等格式的报表生成，并支持通过邮件等多种方式输出。报表支持日报、周报、月报和年报，并且支持对设备、IP群组、单台主机形式输出以上报表； |
| 支持告警和日志管理功能：支持攻击事件触发告警、支持告警通知（短信，邮件、声音）、支持告警过滤、支持自定义日志存储时间、支持告警日志和操作日志支持转储功能； |
| **产品要求（提供证书复印件）** | **具备中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》；** |
| **具备国家保密科技检测中心《涉密信息系统产品检测证书》** |
| **具备中国信息安全测评中心《国家信息安全测评信息技术产品安全测评证书EAL3+级》** |
| **具备IPv6 Forum《IPv6 Ready Logo Phase-2证书》** |
| **厂家要求（提供证书或相关证明复印件）** | **具备中国国家认证认可监督管理委员会颁发的《ISO14001：GB/T24001-2016）环境管理体系认证》资质；** |
| **信息安全设备、系统软件的开发、生产符合TL9000-HS R6.0/R5.5标准；** |
| **具备中国信息安全测评中心颁发的《国家信息安全漏洞库（CNNVD）技术支撑单位等级证书（一级）》；** |
| **具备能力成熟度模型集成认证CMMI5** |
| **其他要求** | **IPS能够接受现网安全管理平台的统一管理，实现拓扑生成，配置下发，日志呈现等。** |
| **保修服务** | **原厂三年质保，合同签订后3个工作日内提供原厂商三年质保服务承诺函** |

1. **安全隔离与信息交换系统**

|  |  |  |
| --- | --- | --- |
| **分类** | **特性/功能** | **详细描述** |
| 产品架构 | ▲系统基本架构 | 三机三系统架构非2+1架构，仲裁机对流经信息进行过滤审计，内外端机为TCP/IP网络协议的终点，阻断TCP/IP协议的直接贯通仲裁机与内外端机采用专用硬件和专用协议进行连接，不可编程三机以软硬件结合的方式，有效地隔断内外网络间直接的连接，防止信息无限制交换 |
| ▲安全体系结构 | 仲裁审计系统部署在独立于内外端机的仲裁机上，具备主动仲裁功能，通用协议无法通过内外端机直接连接到仲裁机；只能通过仲裁机上的仲裁口对网闸进行配置，避免内外端机由于被黑客入侵，导致隔离网闸被黑客完全控制的现象； |
| 操作系统 | 系统基于可信安全操作平台，提供内核级主动防御，具有可信操作系统免疫平台著作权证书；能够对两个主机系统提供多层次、高强度的安全防护，保护其重要进程、文件、数据不受黑客侵袭；采用对象互斥和线程守护技术，保护主要进程的安全性和稳定性；不采用通用的指令库和函数库，只提供有限的内部调试用指令函数。 |
| 功能要求 | 系统管理 | 三权分立：安全管理流程主要由安全管理员、系统管理员和安全审计员通过安全管理中心执行，分别实施系统维护、安全策略制定和部署、审计记录分析和结果响应等。可支持指纹认证登录支持管理端IP地址限制支持负载均衡支持所有配置导入导出自带数据分析和网络诊断工具支持日志详细查询、备份和回滚机制支持邮件告警 |
| 支持协议 | 标准TCP、UDP协议 |
| 支持网络 | 支持IPV4与IPV6 |
| 安全上网功能 | 提供安全的上网访问，支持HTTP协议及代理等；访问控制对象：源地址、目标地址、源端口、目的端目、域名、URL、访问方式等；内容过滤：关键字过滤；脚本过滤：javascript、Applet、ActiveX等；支持对基于HTTP的SOAP协议进行过滤，确保访问的安全；其他过滤策略：文件类型、页面提交方式等。 |
| 安全邮件功能 | 提供安全的邮件访问，支持POP3、SMTP协议；支持发件地址、收件地址、邮件主题、邮件内容、邮件附件过滤。 |
| 文件传输功能 | 提供安全的文件传输功能，支持FTP、NFS、SAMBA等文件传输协议；支持FTP对传输文件的类型过滤；支持FTP指令控制；支持FTP文件名黑白名单控制；支持FTP传输文件大小控制； |
| 文件同步功能 | 可通过专用客户端和网闸主动获取两种方式提供安全的文件同步功能；支持windows平台和linux平台；支持不同任务设置不同的扫描间隔和扫描的时间段；支持任务优先级控制；支持实时扫描、多对一传输、增量传输；支持目录内子目录同步，至多支持32级目录；支持中文文件名或目录同步；支持传输后删除源文件；提供详细的日志审计；支持对格式类型进行特征过滤，并允许用户通过样本文件自定义格式类型；支持文件在线编辑、在线预览等操作；支持文件分享功能，可设置到期时间和提取密码。 |
| 数据库访问功能 | 提供对多种主流数据库（SQL、ORACLE、DB2、MYSQL等）数据库系统的安全访问；支持同步表双向检索功能；支持用户查询、修改、添加、删除等操作；支持全表复制、增量更新、全表更新等；支持各种实例访问。 |
| 数据库同步功能 | 提供多种主流数据库（SQL、ORACLE、DB2、MYSQL等）的单、双向数据交换；无需修改数据库表结构，不涉及到代码修改及二次开发；同步粒度可以达到表内具体字段；支持多种增量同步方式，可分别定义增加、删除、修改的传输方式；支持数据一对一、一对多、多对多的单向或双向交换和同步。支持实时交换或定时同步的策略定义； |
| 视频传输功能 | 实现视频网络与信息通信网的网络隔离，切断所有基于网络协议的连接；支持多种视频硬件平台，如摄像头、DVR（数字硬盘机）、流媒体服务器、视频服务器等设备；支持服务端口控制，对访问视频管理服务器的端口进行控制，其它视频端口默认关闭；支持标准SIP协议，RTSP协议▲支持符合GB/ T28181标准的视频业务，提供公安部检测报告 |
| 自定义功能 | 支持用户基于标准TCP、UDP开发的自定义协议软件，无需对自定义协议软件进行二次修改开发，可以根据需求开发新的专用协议处理过滤功能支持MAC强制访问控制通道，针对被访问端文件进行类别和等级标记，通过标记匹配才能正常访问文件。 |
| 可靠性要求 | 多机热备 | 可实现多台设备互相冗余的应用模式 |
| 网口冗余 | 使一端机多网口冗余，可实现链路备份冗余的工作模式，支持lacp、负载均衡、主备模式； |
| 负载均衡 | 以浮动IP的形式对外提供服务；结合轮询、比重、流量比、服务类别等算法，保证业务实时的连续性。 |
| 审计要求 | SNMP支持 | 支持SNMP协议，可与标准网管平台无缝兼容，能够针对读团体字、系统位置、系统联系人等参数进行自定义； |
| SYSLOG支持 | 支持SYSLOG协议，可与标准日志服务器平台无缝兼容，可实时发送网闸运行状态 |
| 其他要求 | 管理配置功能 | 管理端采用B/S结构；管理端：用于通道建立、策略制定、日志查询、分析、导出等；安全终端管理：可通过串口终端管理方式对网闸进行维护；管理口拥有独立路由，可避免和通讯网口发生路由冲突或干扰 |
| **产品要求（提供证书复印件）** | **具有公安部计算机信息系统安全专用产品销售许可证（增强级）****具有国家保密局科学技术成果鉴定证书****具有中国国家信息安全产品认证证书****具有计算机软件著作权登记证书** |
| 硬件配置及性能指标 | 硬件配置要求 | 内端机2个万兆SFP+光模块槽，4个10/100/1000M RJ45接口，1个扩展槽（至多可扩展4个口），1个串口，2个USB口，1个液晶面板，1个VGA口外端机2个万兆SFP+光模块槽，4个10/100/1000M RJ45接口，1个扩展槽（至多可扩展4个口），1个串口，2个USB口，1个液晶面板，1个VGA口 |
| ▲性能指标 | 网络吞吐量：≥6Gbps至少支持标清（2M）3000路，支持高清（4M）1500路系统整体时延：<0.1ns |
| 保修服务 | 原厂三年质保，合同签订后3个工作日内提供原厂商三年质保服务承诺函 |

1. **应用负载系统**

|  |  |
| --- | --- |
| **指标项** | **规格要求** |
| 系统内核 | 采用封闭式的专有操作系统，无已知安全漏洞, 且非OEM产品,**提供软件著作权证书复印件** |
| ▲硬件配置要、性能要求 | 千兆电口≥8个，千兆光口≥16个,万兆光口≥2个，≥2个扩展槽配置双电源配置6个万兆多模光模块 |
| 吞吐量≥15Gbps， |
| 每秒新建连接数≥200K， |
| 设备生命周期 | 产品为现有平台销售产品 |
| 部署方式 | 支持串接、旁路和三角传输部署模式 |
| 二三层转发 | 支持RIPv1/v2、OSPF、BGP、ISIS等路由协议 |
| 支持IPV4/IPV6双协议栈。 |
| L4-L7负载均衡 | 基于Web网页内容的健康检查，当检测到返回的网页内容不是指定的检查内容时，告警并将用户访问连接转移到其他正常的服务器， |
| 支持源IP、http cookie(多种cookie模式)、http header、Radius、DHCP等会话保持 |
| 支持轮询、加权轮询、最小连接、加权最小连接、源地址散列、源地址源端口散列、目的地址散列、最小流量、最小响应时间、加权最佳性能、每源地址轮训等负载均衡调度算法 |
| 支持x-fordward-for功能，用来识别通过HTTP代理或负载均衡方式连接到Web服务器的客户端最原始的IP地址的HTTP请求头字段，实现对访问源的溯源 |
| 支持在同一界面上配置虚服务、真实服务、健康检查，对多个虚服务批量删除、修改，简化逻辑配置，提升配置效率 |
| 链路负载均衡 | 支持多种链路检测方法，能够通过PING、TCP、DNS等方式监控链路的连通性 |
| 配置≥6条链路负载能力； |
| 支持基于域名的流量调度，针对特定网站选择指定的链路转发 |
| 基于链路流量阈值的调度，当链路的实际流量超过所配置的带宽和阈值（百分比）的乘积后，不会再将新建的请求（命中应用会话保持的除外）调度至此链路，使得链路的流量会平稳缓慢下降，当降低到阈值内后，才会继续允许流量调度至此链路 |
| 基于链路质量/状态的调度，当链路配置健康检查以后，会依据健康检查的结果，在设定检测次数范围内，计算这条链路的延时和丢包率平均值，当这两项检测结果中任意一项超过所配置的阈值后，设备会判断此链路出现故障，并将流量调度至其他正常链路。 |
| 支持智能DNS解析功能，引导访问用户从最优路径的线路接入应用系统。 |
| 支持DNS透明代理功能，可基于负载均衡算法代理内网用户进行DNS请求转发，避免单运营商DNS解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率 |
| 支持基于应用协议的智能选路，能对P2P、视频等流量进行调度 |
| 服务器性能优化 | 内置SSL加速芯片，无需配置独立的SSL加速卡,提供服务器SSL卸载功能 |
| 虚拟化 | 负载均衡设备提供一台物理设备虚拟多个负载均衡功能，为不同应用系统部门提供独立管理负载均衡权限，可对虚拟管理系统进行会话、新建速率、吞吐量、CPU使用率、内存使用率进行设置 |
| 全局负载均衡 | 支持多链路均衡和多数据中心全局负载均衡能力，能够对数据流量在容灾数据中心、业务服务器之间提供流量切换的能力 |
| 多合一功能集成 | 单一设备可同时支持包括链路负载均衡、全局负载均衡和服务器负载均衡的功能，三种功能同时处于激活可使用状态  |
| 可靠性要求 | 支持双机热备、VRRP多主、静默双机等多种模式，满足不同级别的可靠性需求 |
| 可编程脚本语言 | 提供灵活的编程语言，可自定义应用业务的控制方法 |
| 地址转换 | 支持动态端口NAT、动态地址NAT、静态端口NAT ,NAT64、NAT66等，适合各种复杂的网络环境 |
| 智能告警 | 支持智能告警系统, 支持E-mail、短信、SNMP Trap三种告警方式，管理员可基于业务安全所关注方面来选择告警触发事件与对应的告警方式，当业务网络环境中发生问题时（如服务器宕机、网络攻击、链路中断、链路拥塞、出口流量突增突降等故障场景），即会自动向管理员发送告警信息 |
| 设备管理及运维 | 支持下列管理方式：CLI，WEB（HTTP/HTTPS），SSH管理，支持SNMP协议的管理，支持API接口和标准XML接口 |
| 支持通过命令行的方式对数据流在设备内部的处理过程进行分析，帮助迅速定位网络故障 |
| **产品要求（提供证书复印件）** | **所投产品具备《计算机信息系统安全专用产品销售许可证》** |
| **设备生产商具备能力成熟度模型集成CMMI5证书** |
| **其他要求** | **能够接受现网安全管理平台的统一管理，实现拓扑生成，配置下发，日志呈现等。** |
| **售后服务** | **原厂三年质保，合同签订后3个工作日内提供原厂商三年质保服务承诺函** |

1. **运维安全管理（堡垒机）系统**

|  |  |  |
| --- | --- | --- |
| **指标名称** | **指标项** | **详细描述** |
| **要求** | **产品要求（提供证书复印件）** | **产品的《计算机软件著作权登记证书》；****国家公安部计算机信息系统安全专用产品销售许可证；****国家涉密信息系统产品检测证书；****产品必须是自主研发而不是OEM产品；** |
| **厂家要求（提供证书复印件）** | **拥有省级以上高新技术企业资质；****通过ISO9001:2008质量管理体系认证；** |
| 系统架构 | 产品架构 | 软硬件一体化产品，采用标准2U机架式硬件结构； |
| 部署方式 | 旁路代理模式，不影响正常业务流量；支持HA双机部署； |
| 管理结构 | B/S架构，采用HTTPS方式远程安全管理，无需安装管理客户端； |
| 网络接口 | ≥100/1000M RJ45\*4个自适应以太网口；可扩展8个千兆电口或光口； |
| 数据存储 | 设备内置存储系统，存储空间不低于4TB，采用RAID磁盘阵列； |
| 可管理对象数 | 内置500个主机/设备操作监控许可证书； |
| 性能要求 | 并发会话数 | 图形并发会话数≥1200字符型并发会话数≥800 |
| 功能要求 | 支持协议 | 字符型远程操作协议：SSH(V1、V2)、TELNET、RLOGIN、AS400；图形化远程操作协议：RDP、VNC、X11；文件传输协议：FTP、SFTP； 数据库远程操作协议：支持ORACLE、MSSQL、Sybase、Mysql、DB2数据库远程访问协议审计；支持通过应用发布的代理进行协议扩展，支持Radmin、Pcanywhere、 HTTP/HTTPS，可定制开发其它访问协议及客户端支持；应用发布代理支持RemoteAPP穿透方式；支持协议端口自定义；  |
| 服务器访问方式 | Web访问方式:通过系统的Web页面控件直接访问服务器或通过WEB页面调用本地工具（含数据库官方客户端）直接访问服务器；（多种类浏览器支持：IE（6-9）、firefox、chrome、safari；web方式访问支持所有远程协议；web访问方式支持历史访问配置参数自动记忆功能；web访问方式支持直接输入目标IP快速连接功能；通过web方式使用SSH协议支持clone session功能；支持直接调用SFTP功能；支持设定窗口颜色、保存屏幕内容、打印屏幕内容、复制粘贴等功能；通过web方式使用图形化远程操作协议，支持自适应浏览器窗口大小；通过web方式使用RDP协议支持剪切板、磁盘映射功能； |
| 客户端访问方式：支持通过管理员常用的客户端(如SecureCRT、PUTTY、Mstsc、PLsql、SQLplus等)直接连接堡垒机再访问到服务器；支持客户端(SecureCRT、putty)clone session功能；支持secure shell client软件中直接调用sftp功能； |
| 登录资源菜单访问：客户端访问审计系统即可显示用户能访问的主机资源菜单，用户通过字符菜单或图形菜单选择列表方式直接访问服务器；菜单方式访问支持所有协议；  |
| 身份认证及访问授权 | 支持多种认证方式：本地密码认证、UsbKey认证、第三方CA证书认证、RSA动态口令认证、安盟动态口令认证、RADIUS认证、LDAP认证、AD域认证以及短信认证；支持系统自带的Usbkey和Token令牌强身份认证模式；内置配置管理员、密码管理员、审计管理员、系统管理员、系统审计员、普通运维用户等管理角色；支持SSO功能，运维人员不必输入服务器帐号及密码，无需进行二次登录认证；支持基于用户（用户组）、目标设备（设备组）、系统帐号、协议类型、生效时间范围、源IP地址等条件组合设置访问控制策略；支持粗放式访问授权模式，授权条件仅基于运维用户（用户组）和目标主机IP地址段，不限制使用的系统账号及协议等其它条件；支持审批模式：运维用户访问特定的服务器设备必须经过管理员的临时审批授权才能进行，否则无法进行任何操作；支持备注模式：运维用户访问服务器前必须先填写该次访问的维护目的等内容，否则不能进行访问操作；支持工单授权功能：通过运维人员申请或管理员下发工单的方式来赋予运维人员访问目标服务器的权限，且有工单生效时间限制；支持登录预处理命令设置；支持设定会话连接单位时间内空闲无操作，连接自动断开；支持运维用户多次登录失败自动锁定账号功能及解锁机制设定； |
| 访问控制及异常告警 | 支持按用户（用户组）、目标设备（设备组）、系统帐号、命令集和生效时间等内容或按访问授权策略设定安全事件规则；支持指令黑白名单； 支持对违规操作的指令（黑名单）进行告警、忽略处理、自动阻断或指令审批；支持以屏幕、邮件、SYSLOG、Snmp Trap、短信方式实时发送告警信息； |
| 用户管理功能 | 支持添加、删除、修改以及启用、停用运维用户；支持用户账号批量导入导出功能；支持运维账号使用有效期管理；支持运维用户密码强度管理；支持用户组管理，可方便添加、删除、修改组信息及组成员； |
| 主机管理功能 | 支持添加、删除、修改主机内容；支持主机组管理功能，可方便添加、删除、修改组信息及组成员；支持系统类型管理：内置常见系统类型，可自定义添加目标设备的系统类型及内容，包括显示图标、该系统拥有的协议及默认端口等内容；支持在线ping主机功能，即时获取该主机存活信息；支持主机账号及协议通道验证功能，即时获知该账号及访问通道是否有效；支持主机登录限制，同一台服务器可以只允许一个用户登录，防止已登录用户被登出；支持IP地址集、时间集、指令集管理功能； |
| 操作行为记录 | 针对SSH、Telnet、Rlogin、FTP/SFTP、数据库操作进行记录及审计；记录发生时间、发生地址、服务端IP、客户端IP、操作指令、返回信息、操作备注、客户端端口、服务器端口、运维用户帐号、运维用户姓名、审批用户帐号、审批用户姓名、服务器用户名等信息；针对RDP、VNC、X11等图形终端操作的连接情况进行记录及审计；记录发生时间、发生地址、服务端IP、客户端IP、操作指令、返回信息、操作备注、客户端端口、服务器端口、运维用户帐号、运维用户姓名、审批用户帐号、审批用户姓名、服务器用户名等信息；能够记录RDP协议中的活动窗口名称、删除文件等动作，并能记录RDP会话中的键盘输入信息； |
| 会话过程回放 | 支持以WEB在线视频回放方式重现维护人员对服务器的所有操作过程，无须在客户端安装播放客户端软件；支持倍速/低速播放、拖动、暂停、停止、重新播放等播放控制操作；支持从特定操作指令开始进行定位回放；支持回放界面中显示键盘输入、功能键、鼠标动作；支持下载回放文件到本地保存，并通过厂家专用播放器查看，防止会话视频记录泄密； |
| 密码管理 | 支持按设备（设备组）、系统帐号、计划执行时间、改密周期、密码策略、改密结果发送等生成详细的改密计划，到期自动执行；支持随机生成不同密码、随机生成相同密码以及手工指定相同密码的密码策略，并能严格遵守密码强度设置；支持手工改密功能；支持改密结果自动发送至密码管理员或FTP上传；支持手工下载全部或部分主机密码功能；支持自动改密结果报表； |
| 实时监控 | 支持实时监控近期发生的所有会话信息，显示会话状态（连接中、退出、阻断）；支持对会话进行同步监控，执行会话回放、监控和阻断操作；支持Vi、Smit、rhel下setup等图形或菜单操作进行全程同步监控；支持实时监控审计系统CPU、内存、磁盘的使用情况；支持记录审计系统自身的管理操作，保障审计系统自身安全； |
| 历史查询及审计报表 | 支持单一条件快速查询、查询结果二次过滤以及多重条件组合高级查询功能；支持同一次会话中的指令关联查询，显示会话中所有操作指令；支持根据查询结果直接定位视频文件，回放历史会话；系统内置多种运行维护报表模板；支持以html、CSV或PDF方式生成并导出报表；支持管理员自定义审计报表模板；支持以日报、周报、月报的方式自动生成周期性报表，并自动发送至指定邮箱； |
| 数据安全管理 | 提供专用数据存储系统的著作权证书；提供高性能日志及行为审计系统证书；支持自动归档和手动备份、支持以FTP/SFTP等方式自动上传归档数据；支持备份数据恢复导入；支持空间自管理功能，存储空间不足时能够自动清理老的数据；支持系统配置的导入、导出功能； |
| 协同操作 | 支持双人协同操作功能； |
| 批量执行 | 支持批量执行功能；支持会话批量连接登录功能；支持对批量执行结果进行成功或失败判断；  |
| 消息中心功能 | 支持工作任务流程及消息中心管理功能：支持用户间互相发送消息，通过消息下发工作任务等功能；支持关键事件自动生成消息如：二次审批、备注审批、协同操作邀请；支持专用消息接收客户端； |
| 系统管理功能 | 支持页面证书下载；支持页面下载系统相关软件；支持时间同步功能支持从WEB界面修改网卡IP设置、静态路由设置等内容；支持修改不同访问模式（客户端直连、菜单方式）的默认访问端口支持从WEB管理界面重启、关闭设备；支持页面超时设置；支持通过web界面进行系统升级；支持系统告警日志发送； |
| 其他要求 | 联动能力 | 支持与现网日志管理综合审计系统实施联动部署，全面实现数据库业务访问、后台维护操作、网络运行日志及应用系统日志的综合审计，**需详细描述实现方式或提供实现证明。** |
| **保修服务** | **原厂三年质保，合同签订后3个工作日内提供原厂商三年质保服务承诺函** |

1. **数据库审计系统**

|  |  |  |
| --- | --- | --- |
| **指标名称** | **指标项** | **详细描述** |
| **要求** | **产品要求（提供证书复印件）** | **提供产品的《计算机软件著作权登记证书》；****国家公安部计算机信息系统安全专用产品销售许可证；****通过国家保密局涉密信息系统产品认证；** |
| 系统架构 | 产品结构 | 要求为一个完整的软硬件一体化产品；无需用户另行提供服务器、操作系统、数据库、防火墙软件、及用户手动升级系统补丁； |
| 产品架构 | 采用标准2U机架式硬件，且审计主机与探测器必须相互独立且为同一品牌； |
| 操作系统 | 深度定制优化的Linux系统； |
| 管理方式 | B/S方式，采用HTTPS方式远程安全管理，无需安装管理客户端； |
| 设备部署 | 提供旁路接入模式，设备部署不影响原有网络结构； |
| 数据存储 | 所供系统设备必须自带本地存储功能；**提供基于海量日志专用存储的文件系统著作权证书复印件，**禁止采用通用关系型数据库来存储日志；物理磁盘空间>=8TB；日志存储量至少十亿条；（指标以原厂公开资料为准）；RAID架构以保证数据可靠性,（指标以原厂公开资料为准）；支持后期扩展外部网络存储(IP SAN、NAS、DAS、磁盘阵列等)； |
| 网络接口 | 审计主机至少提供千兆RJ45\*4（一路数据传输口；一路系统管理口）；探测器至少提供千兆RJ45\*6，支持多路网络镜像监听；网络接口支持电口，可升级为光口； |
| 日志生命周期管理 | 包括日志采集、实时分析、存储备份、审计报告功能； |
| 处理性能 | 日志采集能力：7000条/秒以上 |
| 审计要求 | 审计对象范围 | 全面支持DB2、Oracle、MSSQL，MYSQL、Informix、SyBase数据库各版本的访问行为审计；全面支持各类Windows系统、Unix系统、Linux系统、网络设备（交换机、路由器、负载均衡器等）、安全设备（防火墙、VPN、IDS/IPS、防毒墙等）的系统日志集中审计； |
| ▲必备功能 | 审计系统支持以syslog、snmp trap、opsec lea、WMI等标准协议接口采集各类日志数据；审计系统自动将采集的操作语句解析为查询、增改、删除、过程等类型呈现；审计记录包括行为发生时间、员工工号、操作终端主机名及IP地址、终端工具名称、服务器端主机名及IP地址、数据库名、表名、SQL语句、返回结果等关键信息。提供工号信息接口，将数据库操作语句与操作者工号建立关联关系，实现操作者实名认证；审计系统能够对未经许可的客户端工具直接访问数据库的行为实施阻断；支持配置操作行为解析模型（黑白名单），灵活区别正常操作和异常操作事件；支持依据语句解析模型，以操作频率为条件实施行为阻断；支持将可疑的数据库查询语句以在线的方式反显执行，并即时在线查看返回结果；支持将异常操作的完整会话信息进行前后操作语句关联查看分析；支持分中心部署方式，能够配置分支数据集中上传至中心机；扩展性强，能够与运维安全审计、日志综合审计、应用系统审计整合成统一安全审计平台； |
| 基本功能 | 实时分析功能 | 实时窗口以多种图形方式展示流量分析、事件分析、告警分析及综合分析结果；流量分析：以业务系统工号为基线，统计分析当天某段时间（自定义）内的操作流量；事件分析：依据安全策略，以时间为基线，统计异常事件的发生数量和趋势；告警分析：依据安全策略，以时间为基线，统计严重告警事件的发生数量和趋势；综合分析：以数据库操作类型为基线统计各类操作状况，并统计审计系统资源以及系统操作的状况；实时操作数据以不同等级（丢弃、过滤、安全、重要、事件、告警）进行分类显示；实时操作语句直接以查询、增改、删除、过程等操作类型分类显示； |
| 审计分析报告 | 系统默认报告数量不少于百种；以图(柱、曲线、饼等)，统计、明细数据的方式表现；支持动态\静态（日报、周报、月报）两种系统生成方式；支持报告模版创建、修改、删除功能；支持报告的邮件转发、生成提醒功能；支持多人邮件接收；支持自定义审计报告；支持多层嵌套报告；支持报告自定义归类；支持导出html、Excel、PDF；报告名称以树型菜单统一高效管理； |
| 查询检索 | 日志数据全字段检索至少满足500万条<5秒；支持多条件组合查询方式；支持逻辑运算符(或、与、非)；支持正则表达式；支持IP、字符、数字、日期、时间等日志字段；支持查询模版创建、修改、删除功能；支持历史查询任务列表的查看；支持查询结果导出；支持日志字段自定义选择显示； |
| 分析策略 | 全局策略：支持以服务器IP、数据库类型、数据库表、操作类型（查询、增改、删除等）设定策略，采集（过滤）核心关注（无关紧要）的数据，将操作数据进行分类（安全、重要、事件、告警等）入库；模型分析策略：支持以入库的操作语句为原型，根据获取的语句内容片段、数据库表名、条件字段、操作频率以及结果影响行数设定分析策略（黑白名单），区分正常操作和异常告警操作；三层业务策略：支持通过该策略配置，识别数据库三层架构中用户信息实时规则策略：支持根据日志字段为条件预设置分析策略；系统内置策略模板，可以直接加载生效；支持以告警页面、短信、邮件、SYSLOG、SNMP等各种方式呈现告警信息； |
| 备份归档 | 支持以日志属性、日志类型、存储周期的方式选择备份；支持归档日志恢复导入；支持自动与手动两种归档策略；支持本地、FTP上传等归档方式；  |
| 系统管理 | 支持审计系统帐号、组管理（添加、修改、删除）；支持资产管理，即所有采集日志源管理维护；支持页面升级；支持页面重启、关机；支持时间同步设置；支持系统配置导入、导出； |
| 系统安全 | 系统自身安全 | 系统内置安全防火墙；支持控制访问审计主机范围；必需提供内部通讯检查机制，传输128加密；管理接口支持串口或电口的方式管理；管理界面与其他功能模块分离； |
| 日志数据安全 | 审计日志数据以文件方式存储；审计日志加密导出审计系统；支持所有审计管理员操作审计系统的动作进行审计；支持记录审计系统之间的物理、逻辑状态变化； |
| 日志权限 | 审计员只限于操作权限设置范围内的日志数据，无权限日志数据透明；支持日志类型权限设置；支持IP地址权限设置；支持页面功能模块权限设置； |
| 其他要求 | 审计平台联动能力 | 支持与现网的日志综合审计系统实施联动部署，全面实现数据库业务访问及后台维护操作、网络运行日志、应用系统日志综合审计；支持审计主机及探测器分布式部署升级； |
| **保修服务** | **原厂三年质保，合同签订后3个工作日内提供原厂商三年质保服务承诺函** |

1. **日志审计系统**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| ▲兼容性 | 针对现网日志审计系统LogBase-A3600存储容量进行升级，升级后要求能满足核心交换机镜像流量日志存储达到6个月以上，同时针对原有日志进行原盘备份服务。 |
| 硬盘 | 硬盘8T\*2，支持RAID0，1，5等。 |
| 其它 | 所供硬盘提供原厂三年质保；质保内若出现硬件故障，须更换原件，原件不予返还，并无条件提供原件数据恢复、同步等操作。 |

1. **态势感知大数据分析平台**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| ▲处理性能要求 | 采用分布式处理框架，处理性能≥100Gbps，并支持平滑扩展 |
| 部署方式 | 支持分布式部署，支持集中式管理，需包含如下引擎：全流量威胁检测系统、安全风险检测系统； |
| 支持与高速公路联网运行收费系统省中心现网网络安全设备进行联动处置、下发策略 |
| 支持硬件采集探针数量 | 不少于65个 |
| 大数据功能模块 | 具备高容错、高吞吐量的数据处理能力，采用Hadoop、Storm、Spark、ElasticSearch大数据功能组件 |
| ▲安全事件管理功能模块 | 支持安全事件的统计分析，安全事件类型包括但不限于：1.高危攻击事件：分析高危攻击事件趋势、高危攻击类型占比、威胁等级占比及攻击列表展示，攻击列表包含发起方及受害方信息，统计维度包括但不限于：资产类型、资产状态、发起方及受害方数量、最近攻击时间、事件类型、攻击次数等，并支持点击查看进行攻击溯源、还原攻击链，以及各展示维度的关键字检索。2.恶意文件：分析恶意文件类型分布、时间和数量维度的恶意文件发现趋势及恶意文件列表展示，恶意文件列表统计维度包括但不限于：时间、探针ID、唯一标示、文件名称、文件类型、检测来源等，并支持各展示维度的关键字检索。3.恶意域名：分析恶意域名、恶意网站，支持列表展示，展示维度包括但不限于：域名、来源、地理位置、最近访问时间、访问主机数等，并支持各展示维度的关键字检索。4.C&C攻击事件：分析统计C&C攻击事件的攻击源TOP、攻击目的TOP、攻击次数及时间维度的受害资产分布、C&C攻击列表展示，展示内容包括但不限于：时间、源IP、源端口、目的IP、目的端口、攻击类型、攻击名称等，支持查看攻击报文明细，并支持各展示维度的关键字检索。5.威胁情报事件：分析统计威胁源IP TOP、受害IP TOP、威胁类型TOP、威胁事件列表展示，展示内容包括但不限于威胁源IP、受威胁次数、最新发现时间、威胁事件类型，并支持各展示维度的关键字检索。6.黑恶档案：分析统计黑客地理位置分布、常用手段分布、黑客列表展示，展示内容包括但不限于：黑客IP、地理位置、威胁的资产数量，并支持各展示维度的关键字检索，支持点击查看黑客详情，详情内容包括但不限于攻击频率分布图表展示、资产攻击关系图形化展示、攻击详情列表展示。 |
| 安全威胁分析功能模块 | 支持多维度的安全威胁分析，能从外到内、内到内、内到外三个方向展开，攻击列表可显示出攻击发起方、地理位置、威胁范围、事件类型及次数等，并可以转化为攻击链分析，攻击链阶段包括：侦查追踪、武器构建、载荷投递、漏洞利用、安装植入、命令和控制、目标达成; |
| 威胁情报关联功能模块 | 支持独立的威胁情报模块，集成威胁情报信息，支持威胁情报的查询、关键字检索，威胁情报详情包括但不限于：某IP作为攻击源的攻击目的TOP、攻击类型TOP、攻击趋势，作为攻击目的的攻击源TOP、攻击协议TOP、攻击趋势，攻击关联日志，作为访问源的访问目的TOP、访问协议TOP、访问趋势，作为访问目的的访问源TOP、访问协议TOP、访问趋势，会话关联日志，威胁情报日志； |
| 异常流量分析功能模块 | 支持内外部的流量分析，包括但不限于访问量与被访问量分析、会话详情、访问趋势、会话量、端口协议分布的图表展示，访问关系的图形化展示，并支持各展示维度的关键字检索； |
| ▲漏洞监控功能模块 | 1）支持资产漏洞监控，监控内容包括但不限于资产类型、资产风险、实时漏洞情况、高危端口、弱口令、模拟人工渗透测试结果等，**提供产品功能截图或具有此项功能的证明材料；**2）支持漏洞检测任务管理，展示列表包括但不限于任务名称、检测方式、检测对象、关联探针、执行方式等。支持检测任务的新增、删除，支持检测任务手动执行及按日、周、月执行，支持查看扫描历史，**提供产品功能截图或具有此项功能的证明材料。** |
| 资产管理功能模块 | 支持资产管理，通过流量自动化进行资产识别并生成资产列表，可针对单一资产进行网络维度和安全维度的分析，支持资产监控范围、资产地域配置。支持资产类型、资产状态、资产范围、资产标签的资产列表展示，支持从资产列表中跳转但一资产查看资产详情； |
| 安全报告功能模块 | 支持报表管理，系统中可进行报表的个性化设置，包括报表类型、生成周期、报表格式、邮件接收人等； |
| 日志检索功能模块 | 1.支持日志检索，通过关键字进行快速查询，可查看会话日志、流量日志、攻击日志，支持日志快速检索功能，提供快速检索模版，包括但不限于：HTTP、FTP、DNS、DHCP、SMTP、SSL、SSH；2.支持第三方安全设备日志采集，采集维度包括但不限于：时间、设备IP、源IP、源端口、目的IP、目的端口、攻击类型，并支持各展示维度的关键字检索。支持与现网安全设备进行联动处置、下发策略。 |
| 可视化能力 | 支持7个维度的动态实时展示大屏，包括安全综合监控大屏、会话监控大屏、全网威胁监控大屏、内部威胁大屏、外联威胁大屏、外部威胁大屏、漏洞监控大屏等; |
| **厂家要求（提供证书复印件）** | **为保障软件平台成熟度，所投产品厂商需具备能力成熟度模型集成认证CMMI5；****为保障平台安全运营与应急支撑，所投产品厂商需具备中国信息安全测评中心颁发的《信息安全服务资质-安全工程类二级》证书；****具备中国信息安全认证中心颁发的《信息安全风险评估服务一级》证书；****《信息安全应急处理一级》证书。** |
| **产品要求（提供证书复印件）** | **所投产品需具备计算机软件著作权登记证书、公安部销售许可证。** |
| **保修服务** | **原厂三年质保，合同签订后3个工作日内提供原厂商三年质保服务承诺函** |

1. **态势感知全流量分析探针**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| ▲硬件、处理性能要求 | 标准2U架构，CPU≥10核，内存≥128G，万兆光口≥2；冗余电源；配置2个万兆多模光模块。 |
| 威胁检测探针吞吐量≥10G； |
| 恶意文件检测 | 支持显示探针接口状态、设备状态、流量趋势，支持参数配置，包括设置采集接口的服务配置、恶意文件检测配置，配置恶意文件类型包括但不限于：恶意脚本文件、Office文件、可执行文件、文本文件、压缩文件、Java文件、PDF文件、图片文件、音频和视频文件； |
| 病毒防护能力 | 集成第三方防病毒厂商专业病毒库，具备反病毒引擎； |
| 入侵检测能力 | 具备多种入侵类型的检测能力，包括但不限于：目录遍历漏洞检测, 跨站脚本攻击漏洞检测, 文件上传漏洞检测, 远程文件引用漏洞检测, 其他漏洞检测, 命令注入漏洞检测, SQL注入漏洞检测 |
| 网络通信行为检测 | 具备全流量检测引擎,可实现IP碎片重组、TCP流重组、应用层协议识别与解析，能够对网络通信行为进行识别，包括但不限于：FTP行为、SMTP行为、DHCP行为、HTTP行为、DNS行为、SSL通信等；  |
| Web安全检测 | 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，支持对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； |
| 僵木蠕检测 | 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分析； |
| **▲兼容性要求** | **与安全态势感知大数据分析平台同一品牌，并能够与大数据分析平台进行数据对接；** |
| **厂家要求（提供证书复印件）** | **为保障安全威胁情报的全维度，产品厂商需具备国家漏洞库（CNNVD）一级支撑单位资质；为保证所投产品质量，产品厂商需通过TL9000认证、ISO27001质量管理体系认证。** |
| **保修服务** | **原厂三年质保，合同签订后3个工作日内提供原厂商三年质保服务承诺函** |

1. **态势感知主动风险监测探针**

|  |  |
| --- | --- |
| **项目** | **技术要求** |
| ▲硬件、性能指标要求 | 2U 机架式服务器产品，提供产品设备图片。CPU ≥8核，内存≥64GB，存储≥1T，网口≥4 |
| 实配无限地址扫描授权 |
| 资产盘点功能模块 | 产品具备丰富资产指纹库及自主研发的识别引擎，对目标资产进行多维度信息探测，支持场景下全资产盘点包括：操作系统识别、中间件识别、数据库识别、开启端口与服务识别、网络设备识别、安全设备识别，支持各类前端设备的识别能力。产品可生成导出专业盘点报告（支持HTML、EXCL等格式），报告内容包括但不限于：资产汇总（设备分类、往期盘点资产对比）、资产分析（区域资产分析、厂商分析、离线资产分析、应用服务分析）、资产详情（地址、厂商信息、设备型号、序列号、开放端口及服务、资产上下线详情）。减轻运维工作量，可基于A 段、B 段创建下发资产盘点任务，检测任务可发现目标范围内在线的资产，可检测到在线资产的 IP 地址、 MAC 地址、操作系统、设备类型、设备厂商、设备型号、软件版本，并在报告中展示设备开放的高危端口。 |
| 安全检测功能模块 | 产品具备物联网资产检测能力，具备对物联网资产漏洞及弱口令的识别能力；产品具备高危漏洞的专项检测能力，适用于服务器、业务系统等设备极多的网络环境下快速安全检测；▲**产品对高危漏洞提供自动化验证功能。自动化验证不需要任何人进行参与，平台自动对漏洞进行验证、判断，并可在安全检测报表中体现，并提供第三方机构产品测试报告；**产品可生成专业安全检测报告（支持HTML等格式），报告内容包括但不限于：检测汇总（总体安全评级及安全风险分布、区域资产总体风险分析）、检测结果详情分析（主机资产风险、前端监控设备风险等、漏洞分类分析）、资产漏洞统计（IP、资产类型、漏洞分布、风险评级）、模拟人工渗透详细风险描述等。 |
| **边界完整性检测功能模块** | **▲产品具备边界完整性检测能力，可检测出目标设备连接智能手机热点、通过智能手机 USB 共享网络等违规双网卡共享外联行为，可检测出违规内联行为。** |
| 安全可视化 | 平台具备安全可视化监测大屏，7×24h监控资产状态及安全风险态势。可展示当前安全评分，前端监控设备统计，最新安全风险包括：时间、资产、风险以及风险级别。 |
| 行业化安全知识库 | 产品需集成安全漏洞验证知识库（提供行业迎检知识库、等级保护知识库、安全攻防知识库、安全应急知识库、安全设计方案知识库）。 |
| **厂家要求（提供证书复印件）** | **具备国家信息安全漏洞库（CNNVD） 技术支撑一级单位** |
| **具备能力成熟度模型集成认证CMMI5；** |
| **具备TL9000电信业质量体系认证证书；** |
| **其他** | **生产厂商在本地有售后服务人员及机构，原厂三年质保，合同签订后3个工作日内提供原厂商三年质保服务承诺函** |

1. **80Km千兆单模光模块**

|  |  |
| --- | --- |
| **指标项** | **规格要求** |
| 千兆80km光模块 | SFP千兆光模块,单模,(1550nm,80km,LC) |

1. **现网安全管理平台定制开发**

|  |  |
| --- | --- |
| **指标项** | **规格要求** |
| **开发要求** | **针对联网运行省中心系统现网使用的安全管理平台进行进行定制开发，以确保本次新增所有安全设备的管理模块并配置相应授权数量，开发后能够统一管理在网相关安全设备并进行配置下发，能够进行日志集中管控和拓扑生成展示。** |

1. **安全厂商原厂安全服务**

#### 服务商要求

1. **安全服务厂商资格要求**
2. **服务商未被列入失信被执行人名单、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单，信用信息以投标截止日信用中国网站（www.creditchina.gov.cn）公布为准；**
3. **服务商必须具备以下信息安全资质，并提供资质证明材料；**

**具有中国信息安全测评中心颁发的信息安全服务安全工程类二级以上资质；**

**具有中国信息安全认证中心颁发的风险评估二级以上资质；**

**具有中国信息安全认证中心颁发的应急处理二级以上资质；**

**具有公安部颁发的信息安全等级保护建设资质；**

**具有ISO 27001信息安全管理体系认证；**

**具有CMMI3以上认证；**

**作为国家信息安全漏洞共享平台CNVD技术组或国家漏洞库CNNVD支撑；**

**具有国家级网络安全应急服务支撑单位证书或具有国家计算机网络应急技术处理协调中心浙江分中心ZJCERT合作支撑单位；**

1. **需提供服务商安全研究能力证明材料，提供自2015年1月1日起不少于5个中国信息安全测评中心颁发的安全漏洞提交证明；**
2. **需提供服务商安全服务案例证明材料，提供近2016年1月1日起不少于5个安全服务，并提供合同证明材料；**
3. **服务商自2017年1月1日起不存在因网络安全服务管理、服务实施与质量被中国通信企业协会等主管部门通报要求限期整改的情况；**
4. **服务商应在浙江省境内设立办事处或分公司或子公司（需提供相关部门证明）。**
5. **实施团队要求（具体详见“第六点第8款项目组实施人员要求”对应要求）**

服务商须保持实施人员相对稳定性及持续的人力投入，服务商人员如有离职或调整，须承诺人员增减一周至两周内完成，具备完整的人员交接方案，交接方案需详实合理，并定期反馈调整进度，不可影响正常工作。

1. **服务商服务要求**
2. 采购人有权在合同期内不定期对服务商的服务人员进行考查，若发现与投标不符，采购人有权取消服务合同，并追究服务商责任。如在安全服务实施过程中，采购人认为服务商服务人员能力有限，可要求服务商更换服务人员，服务商需按采购人要求执行。
3. 服务商在投标时须提供与本项目服务项输出物样例以及此次的安全服务方案作为技术评分的参考。
4. 安全检测服务过程中所需要的安全检测工具，由服务商自行准备，并承担相关费用。
5. 服务商须保证在任何时候，不论是合同有效期内还是合同终止以后，对采购人提供的技术文件以及事务、业务或操作方法实行严格保密。服务商应就一切有意、无意泄露采购人秘密信息的行为向采购人承担赔偿责任。赔偿金包括一切直接、间接损失及由此而支出的费用。
6. 服务商在安全服务实施前，须要先提供相应的技术方案与采购人充分沟通，在获得授权许可后，方可进行相应操作，以确保系统的安全运行。
7. 服务商在安全服务实施过程中不能对采购人应用系统的正常运行产生影响，包括系统性能明显下降、网络拥塞、服务中断等，同时做好备份和应急措施。
8. 在安全服务实施过程中产生的所有过程文档、原始数据、扫描报告、正式报告、整改意见等必须进行电子和纸制双重归档，在项目结束后全部移交给采购人。

#### 项目服务内容

1. **项目服务期限**

 本项目服务期限为一年，自合同签订之日起开始计算。

1. **项目进度要求**

 中标人自签订合同之日起开始提供服务。

1. **项目工具要求**
2. 为了服务期间实时流量检测，并避免网络改动和降低配合难度，服务商必须提供“分流工具”一台，实现流量一对一分流和多对一分流，配合驻场人员进行流量安全监控。要求可通过五元组（源IP、目的IP、源端口、目的端口、传输层协议）进行流量筛选，工具具备病毒流量模型发现功能和异常会话发现和限制功能，具备DDOS流量过滤。工具具备独立18个千兆电口，独立4个千光口，高度小于等于1U；或可选择同类型、功能、性能的相关设备执行，需经过用户方评估确认。
3. **服务过程中提供专业安全检测工具，工具需具有国家CNNVD兼容性认证或国际CVE认证，**以实现网络资产脆弱性检测、破坏边界完整性的违规行为检测，能够针对现网资产实现盘点识别、漏洞检测、终端违规外联检测、违规内联检测，同时可针对检查出来的漏洞进行自动化验证。或可选择同类型、功能、性能的相关设备执行，需经过用户方评估确认。
4. **项目服务内容**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务项目** | **服务描述** | **服务方式** | **服务说明** | **服务输出物** |
| 1 | 安全风险评估与规划 | 依据信息安全标准和国家法律法规要求，梳理网络与信息系统资产，对网络架构和网络资产进行评估，包括网络拓扑分析还原、安全域分析、VLAN分析、核心网络设备、核心设备漏洞风险、核心设备配置风险等，分析面临的威胁和脆弱性，评估存在的安全风险及严重程度，并对安全风险提出针对性的防护建议和规划方案。 | 现场 | 1个物理机房，200信息资产（其中网络设备100台以内，安全设备50台以内）； | 输出物包括但不限于《XXX单位网络安全风险评估报告》、《XXX单位网络安全建设规划报告》 |
| 2 | 渗透测试服务 | 在采购人授权和监督下，模拟黑客攻击方法，对采购人指定的网站和其他业务系统进行非破坏性质的攻击测试，查找存在的漏洞并给出详细的修复建议，业务系统漏洞修复完成后，需对漏洞进行复测。 | 现场 | 每次2个业务系统（含C/S和B/S系统）每季度1次 | 输出物包括但不限于《XXX系统渗透测试报告》 |
| 3 | APP安全检测 | 在采购人授权和监督下，通过专家人工+检测工具的方式，运用专业的检测技术，对APP应用（客户端、服务端）进行安全评估，查找存在的安全漏洞和安全风险，并提供针对性的修复建议，确保APP应用的安全 | 现场 | 每季度1次 | 输出物包括但不限于《XXX APP应用安全风险评估报告》 |
| 4 | 代码审计服务 | 在采购人授权和监督下，检查指定业务系统源代码中的安全漏洞、安全隐患、安全缺点、错误信息，分析并验证这些问题可能导致的安全风险，并提供对应的代码修复建议，从而确保系统代码层面的安全 | 现场 | 按300万行代码预估，包含回归测试 | 输出物包括但不限于《XXX系统代码审计分析报告》 |
| 5 | 安全巡检服务 | 定期对指定目标进行安全漏洞检测、基线配置核查、安全日志审计，完成后提供全面的安全巡检服务报告，给出存在的安全风险并提供对应的修复建议。 | 现场 | 每季度1次，资产数量200台；核心网络安全设备日志分析 | 输出物包括但不限于《XXX单位网络安全巡检报告》 |
| 6 | 安全加固指导 | 对目标系统的安全漏洞进行修复、配置隐患进行指导优化的过程。加固指导内容包括但不限于系统补丁、防火墙、防病毒、危险服务、共享、自动播放、密码安全。 | 现场 | 100以内服务器，100台以内终端 | 输出物包括但不限于《XXX系统安全加固建议》 |
| 7 | 安全应急响应 | 在业务系统遭受黑客入侵攻击时，第一时间对入侵事件进行分析、抑制、还原、处理，查找入侵来源并恢复系统正常运行，完成后给出对应的应急响应报告。 | 现场 | 要求30分钟内响应，2小时到达现场 | 输出物包括但不限于《XXX系统安全事件分析报告》 |
| 8 | 重大活动安全保障 | 重大会议、节假日等特殊时期内，按采购人要求对目标系统进行现场安全值守和保障，对业务系统的安全状况进行实时监控和日志分析；在现场安全保障期间，当目标遭受黑客入侵攻击时，启动应急响应预案，事后给出对应的解决建议； | 现场 | 提供全年重大活动安全保障 | 输出物包括但不限于《XXX单位重保总结报告》 |
| 9 | 安全攻防培训 | 为用户提供一个理论结合实际、可上机操作实践、场景真实逼真的安全攻击和防护培训。在培训中，我们会通过虚拟机的方式，搭建仿真攻防实验环境，针对理论教学的内容，进行操作演练。 | 现场 | 每年提供1次攻防技术培训 | 输出物包括但不限于《XXX单位攻防技能培训计划》 |
| 10 | 安全应急演练 | 根据应急预案和演练方案，协助用户完成各类安全事件的应急处置演练工作，确保安全应急工作的标准化和流程化，以及安全应急的效率和质量。 | 现场 | 每年1次攻防应急演练 | 输出物包括但不限于《XXX单位应急演练实施方案》 |
| 11 | 服务汇报 | 对服务期间服务情况进行汇总分析，进行汇报讲解 | 现场 | 每年1次 | 现场汇报输出物包括但不限于《XXX单位安全服务年度报告》 |
| 12 | 管理制度修订完善 | 根据等保三级要求，协助甲方对现有规则管理制度进行修订完善。 | 现场 | 一次性 | 输出相关制度汇编 |

1. **安全厂商运维人员驻场服务**

#### 驻场服务要求（具体详见“第六点第8款项目组实施人员要求”对应要求）；

1. 驻场人员上班时间与采购人工作时间同步，严格服从采购人工作安排，遇节假日加班所产生费用由服务商承担。
2. 服务商须保持实施人员相对稳定性及持续的人力投入，服务商人员如有离职或调整，须承诺人员增减一周至两周内完成，具备完整的人员交接方案，交接方案需详实合理，并定期反馈调整进度，不可影响正常工作。

#### 驻场服务内容

1. **项目服务期限**

**本项目服务期限为一年，驻场人员自项目验收完成之日起开始计算。**

1. **项目服务内容**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **服务项目** | **服务描述** | **服务说明** | **服务输出物** |
| 1 | 网络资产整理 | 按采购人要求定期梳理当前网络构架内的网络资产，包括但不限于网络设备、应用系统、APP应用、数据库应用、中间件、终端、服务器等。 |  | 输出物包括但不限于《XXX单位业务资产调研表》 |
| 日常安全运维 | 针对采购人信息系统设备进行网络安全设备日常配置维护、安全日志分析、安全设备策略调优，包括不限于针对网络、安全、服务器、存储等设备的配置管理。 |  | 输出物包括但不限于《XXX单位安全服务月度报告》 |
| 日常巡检 | 针对现网设备运行状况、配置参数等进行巡检，保障设备工作保持良好状态 | 每2周1次 | 输出物包括但不限于《XXX单位设备巡检双周报告》 |
| 安全意识培训 | 驻场期间为业主单位提供安全意识培训，内容包括信息安全普及知识、法律法规、安全趋势、大数据安全、移动安全、办公安全以及安全管理等 | 2次培训 | 输出物包括但不限于《XXX单位安全意识培训方案》 |
| 每月安全通告 | 每月提供一期安全态势报告，内容包括安全漏洞、安全预警、安全建议。同时，在出现重大安全漏洞和突发事件时，提供对应的安全分析报告。 | 每月1次 | 输出物包括但不限于《第XX期网络安全研究报告》 |

1. **网络版杀毒软件**

网络版杀毒软件，针对现网50台PC、50台windows server服务器、40台Lunix服务器全部部署杀毒软件，并支持漏洞补丁升级更新。

1. **应用软件改造**

**应用软件改造范围：**

联网收费系统应用软件具体包括：数据传输系统、在线费率服务平台、后台ETC路径识别系统、路网图片管理系统、车辆识别流水管理系统、联网稽查与车辆信用系统、客户服务系统、运营质量评价系统、主线断面流量分析系统、费率系统和清分结算系统、通讯管理查询系统、ETC门架、ETC/MTC混合车道、ETC车道等

**应用软件改造内容：**

（1）实现身份鉴别功能

a)实现身份认证或登录模块，对上下级机构请求的系统节点或用户进行身份标识和鉴别。

b)实现对同一来源的请求采用两种鉴别技术，实现用户身份鉴别功能；

c)实现身份认证信息复杂度检查功能，复杂度检查内容包括长度，字母、数字及特殊符号、定期更换周期等，但采用口令进行鉴别时，实现强制密码策略，由数字、大小写字母、符号混排，无规律的方式，用户口令的长度至少为8位，口令每季度更换一次，更新的口令至少5次内不能重复；

c)实现对上下级机构请求的系统或用户身份标识唯一性和复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；

d)实现认证失败处理功能，失败后结束会话、限制非法请求认证次数。

（2）实现访问控制功能

a)制定传输系统访问控制策略，并根据访问控制策略实现访问控制；

b)实现能够根据访问控制策略对资源（如文件和数据库等）进行权限内访问的功能，禁止越权访问；

c)实现对重要信息资源能够设置敏感标记的功能；

d)实现系统能够根据安全策略对有敏感标记重要信息资源的访问的功能。

（3）实现安全审计功能

a)实现覆盖到每个节点或者每次传输请求的安全审计功能，对应用系统重要安全事件进行审计；

b)实现未授权不能中断审计或修改审计策略功能，不能单独中断审计进程，不能通过应用系统无法删除、修改或覆盖审计记录；

c)实现审计记录日志模块，日志包括事件发生的日期和时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源、事件的结果等；

d)实现审计记录进行统计、查询分析等功能，实现审计报表统计功能，能定期对记录数据进行分析。

（4）实现剩余信息保护功能

a)实现能够清除身份认证信息的功能，禁止身份认证信息存在本地磁盘；

b)实现系统正常退出和非强制关闭后，应用系统和操作系统临时文件无残留的身份鉴别信息。

（5）实现通信完整性功能

a)在设计文档中，明确对通信数据完整性校验的功能；

b)采用MD5、SHA-1等密码算法进行完整性保护和采用SSL等加密通信方式，即实现对数据进行加密和签名后传输的功能。

1. **国密RA中心**

|  |  |  |
| --- | --- | --- |
| **技术指标** | **指标项** | **参数要求** |
| 功能要求 | ▲RA管理 | 支持作为二级RA对接交通部RA网关并完成证书申请、更新、作废等操作。具备多级权限管理功能。 |
| 算法支持 | 支持国密及国际算法。 |
| 用户管理 | 用户管理功能。包括用户注册，用户批量注册，用户审核，用户查询。 |
| 证书管理 | 提供证书申请、作废、更新、查询和下载等功能；提供证书批量申请、批量更新功能。证书发放数量和情况可根据要求分层次分别统计； |
| ▲API支持 | 提供证书申请、作废、更新、查询、下载、批量申请、批量更新接口；其中批量申请、批量更新接口符合《交通部RA系统批量制证接口规范》。 |
| 日志及审计 | 日志记录操作员详细的日常操作，包括操作员、操作时间、操作类型和操作结果等内容。对记录的日志，RA Server提供查询和审计的服务。审计员通过设置查询条件查询日志；并可以在查看日志时进行审计操作。 |
| **保修服务** | **原厂三年质保，合同签订后3个工作日内提供原厂商三年质保服务承诺函** |

1. **应用安全网关**

|  |  |  |
| --- | --- | --- |
| **技术指标** | **指标项** | **参数要求** |
| 硬件要求 | 硬件配置 | 标准2U设备，1T硬盘，16G内存，10个千兆电口，双电源 750W-850W，8核16线程CPU X1 |
| 功能要求 | 安全传输功能 | 国密双向SSL安全传输，通过数字证书实现SSL/TLS协议的加密传输。支持业务接收的同时支持业务的发起，实现双向SSL传输功能。作为SSL的客户端时，可以独立地配置多个服务通道，对接交通部级联网中心国密SSL服务。每个服务通道均可独立地配置表明其身份的数字证书，以及证书信任链。安全传输的加密强度控制，提供进行加密强度的管理服务，系统可以通过设置完成加密强度的控制。  |
| Download CRL服务 | 证书有效性验证数字证书作为连接双方的电子身份证，保证传输的可识别性。确保非可信的证书认证中心（CA）颁发的证书、没有在有效使用期内的证书、已经作废或者注销的证书无法进行含身份确认的操作。 |
| SSL对接要求 | 支持对接部级在线密钥管理和服务平台。 |
| 签名验签功能 | 提供基于HTTP方式的数字签名服务 |
| 性能要求 | SSL性能要求 | 国密SSL TPS 300SSL 并发连接 2000 |
| **产品要求（提供证书复印件）** | **国家密码管理局SM2产品型号证书；****公安部计算机信息系统安全专用产品销售许可证；****计算机软件著作权登记证书。** |
| 保修服务 | 三年原厂维保，中标后签订合同时提供所投产品原厂商三年质保函，原厂授权书； |

1. **签名服务器**

|  |  |  |
| --- | --- | --- |
| **技术指标** | **指标项** | **参数要求** |
| 硬件要求 | 配置要求 | 1T硬盘，8G内存，4个千兆电口。双电源冗余配置。 |
| 功能要求 | 签名功能要求 | 支持使用国密定义的SM2/SM3/SM4算法：支持在签名验签名中使用SM3 with SM2算法；支持国密算法的PDF签名验签名；支持使用SM4算法制作数字信封。支持通过HTTP和LDAP方式下载CFCA CRL完成用户证书有效性验证。可对下载的CRL文件进行有效性验证。 |
| API要求 | 提供C、C++、Java等多种平台的API接口支持选择使用短连接，长连接，连接池；支持自动重建连接；支持配置多个签名服务器IP端口，由API自动以HA或轮询方式分配交易请求；通过API接口访问签名服务器，可在签名服务器上配置对部署API的服务器进行认证，通过校验访问口令、设备MAC地址等方式，拒绝非法的访问。支持交通部密钥在线平台json签名验签。 |
|  | 冗余要求 | 设备自身支持多机冗余部署模式（包括主备模式和负载模式） |
| 性能要求 | 签名性能要求 | RSA2048：1000TPS，SM2：20KTPS； |
| 验签性能要求 | RSA2048：22000TPS，SM2：15KTPS；。 |
| **产品要求（提供证书复印件）** | **国家密码管理局SM2产品型号证书；****公安部计算机信息系统安全专用产品销售许可证；****计算机软件著作权登记证书。** |
| **保修服务** | **原厂三年质保，合同签订后3个工作日内提供原厂商三年质保服务承诺函** |

1. **4G路由器**

|  |  |
| --- | --- |
| **指标项** | **规格要求** |
| 配置要求 | 支持4个千兆RJ45电口，支持电信、移动、联通的4G网络，向下兼容3G。2个SIM卡槽位，支持双网同时独立运行。支持链路自动主备切换，以有线为主，4G为备。工作温度：-25℃~+70℃。 |

1. **三级等保测评**

针对高速公路联网运行省中心系统进行等级保护第三级的定级、备案、建设、测评，保障本系统能拿到等保三级测评通过证书。**▲中标人必须委托有效期内的国家网络安全等级保护工作协调小组办公室推荐的测评机构。**

## 项目清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备(系统)名称** | **单位** | **数量** |
| 1 | 物理机房改造（含布线） | 套 | 1 |
| 2 | 核心交换机**（核心产品）** | 台 | 1 |
| 3 | 3850交换机4端口万兆光口模块 | 块 | 2 |
| 4 | 万兆防火墙 | 台 | 1 |
| 5 | 防火墙一 | 台 | 4 |
| 6 | 防火墙二 | 台 | 13 |
| 7 | 万兆IPS一 | 台 | 2 |
| 8 | 万兆IPS二 | 台 | 1 |
| 9 | IPS三 | 台 | 2 |
|  10 | 安全隔离与信息交换系统 | 套 | 1 |
| 11 | 应用负载系统 | 台 | 2 |
| 12 | 运维安全管理（堡垒机）系统 | 台 | 1 |
| 13 | 数据库审计系统 | 台 | 1 |
| 14 | 日志审计系统扩容 | 套 | 1 |
| 15 | 态势感知大数据分析平台 | 套 | 1 |
| 16 | 态势感知全流量分析探针 | 套 | 1 |
| 17 | 态势感知风险检测探针 | 套 | 1 |
| 18 | 80KM千兆单模光模块 | 个 | 35 |
| 19 | 现网安全管理平台定制开发 | 项 | 1 |
| 20 | 安全厂商原厂安全服务 | 套 | 1 |
| 21 | 安全厂商运维人员驻场服务（1年） | 人 | 2 |
| 22 | 网络版杀毒软件 | 套 | 1 |
| 23 | 应用软件改造 | 项 | 1 |
| 24 | 国密RA中心 | 套 | 1 |
| 25 | 应用安全网关 | 套 | 1 |
| 26 | 签名服务器 | 套 | 1 |
| 27 | 4G路由器 | 台 | 1 |
| 28 | 三级等保测评 | 项 | 1 |

## 集成服务和其他要求

投标人须负责完成本项目涉及的整体规划、安装调试、服务实施等相关工作，须详细确认和理解采购人原有的系统情况、本次项目的建设目标和服务要求，并严格根据用户项目进度安排完成实施工作，如有偏差由投标人负责。

1.投标时投标人需提供相关设备完整配置清单，同时投标人就所提供的设备给予详细说明。

2.投标时投标人需提供完整的系统集成实施方案、实施计划、项目管理规划等。

3.如集成实施过程中出现不符合招标文件要求的严重质量问题时，采购人保留索赔的权利。投标人根据项目实际需求，对系统集成实施方案进行统一设计、规划。

4.投标人需对整体项目方案的可行性负责，根据用户要求完成本项目的所有实施工作，解决实施过程中的全部技术问题。如在项目实施过程中出现无法实施或者缺少相关设备不能满足用户需求的情况应无条件提供相关设备与配件。凡在本次项目实施时，如需对原有的系统架构进行相应的调整，中标人应根据用户的实际要求，提供相应的技术支持，由此所涉及的相关费用，由中标人负责。

5.投标人需按用户要求完成各类网络资产调查、梳理工作，并配合用户完成漏洞通报、配置变更、系统暂停服务、风险处置、事件处置等网络安全管理流程的梳理、设计工作。

6.验收要求：完成所有设备的安装调试及管理制度的完善整改，并通过等保三级测试，取得等保三级备案证书后（最晚年内12月份需取得备案证书），进行验收。

**7．项目组实施人员要求（对应评分标准）：**

中标人项目组要求：项目组实施人员须提供高级项目经理1名（具备高级项目经理认证）(2分)，具备现网网络厂商、安全厂商认证资质的认证工程师5名以上，项目组成员为中标人在职工程师(1分)。**（提供以上人员证书复印件、经验证明以及近半年在本单位社保缴纳证明）**。

安全厂商原厂安服的人员要求：所有成员为安全厂商正式在编人员，安全厂商须提供包括项目经理、实施组成员和渗透组成员的5人以上实施团队，团队成员须且具有丰富的服务经验。项目经理主要职责为负责组织和协调服务工作，须满足以下条件：5年以上工作经验，具有CISP、CISSP、CCSK、PMP或高级项目管理师、ISO27001LA、等级保护测评师、信息安全工程师、ITIL、COBIT5、软件测评师范围内至少五项证书（2分）；实施组成员须满足以下条件：具备CISP或CISSP认证证书，其中1人要求5年以上工作经验；渗透组成员具有较强漏洞挖掘能力（1分）。**（提供以上人员证书复印件、经验证明以及近半年在本单位社保缴纳证明）**。

安全厂商运维驻场人员要求：安全厂商须为本项目配置原厂驻场运维服务工程师2人，原厂商驻场人员为安全厂商正式在编人员，要求具备CISP或CISSP认证证书，至少1人具备现网主要网络安全设备厂商原厂认证工程师资质（1分），至少1人具备CCNP以上思科认证资质，能熟练操作现网思科网络设备（1分）。**（提供以上人员证书复印件、经验证明以及近半年在本单位社保缴纳证明）**。

**▲8.报价要求**

**本项目为交钥匙工程，项目费用包括项目实施所需的以上项目清单中所有设备（含数量）、软硬件对接费用（如有）、培训费、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。**

**商务要求表（对应评分标准）**

|  |  |
| --- | --- |
| **▲供货时间（项目工期）及地点** | 时间：合同签订后15天内设备到货，安装调试20天。项目缺陷责任期自验收之日起12个月。交货地点：用户指定地址。 |
| **▲付款条件** | 鉴于财政预算等情况，本项目预算于2020年下达。待正式确认书下达后，合同签订且项目验收完成后，一次性支付合同款。 |
| **违约责任及争议解决方式** | 按“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（3分）** | 1.中标人负责本项目软硬件设备的供货、运输、保管、安装、调试、培训及售后服务等。硬件提供3年原厂质保（自到货验收合格之日起算），软件提供3年质保（自到货验收合格，安装后运行稳定之日起算，含原厂版本升级服务）；安全厂商原厂安全服务为期1年；安全厂商运维人员驻场服务2人，为期1年。2.中标人应充分了解项目的实际需要和难度，确保设备正常运行，所有耗材由中标人提供。所有软件、设备要求提供三年质保及全包技术支持服务，响应级别为7\*24\*4。**3.原厂三年质保，中标人须在合同签订后3个工作日内提供所有投标产品原厂商三年质保服务承诺函。** |
| **响应情况（3分）** | 软硬件故障响应时间1小时，故障修复时间2小时，4小时内无法修复，需提供应急替代方案。提供7X24小时电话、邮件、网站、传真等远程技术支持服务。 |
| **本地化服务要求（2分）** | 非本地公司在杭州具有分支机构或办事处**(提供相关部门证明材料)**以确保项目的售后服务。 |
| **技术培训** | （一）中标人需对用户进行相关培训，使用户能够理解并熟练掌握。培训费用包含在本次项目中，无需在报价文件中列项。1、培训主要内容：本项目涉及的各产品相关培训，包括但不限于产品功能、产品使用、配置操作、日常故障排查等；原厂商认证工程师培训。2、培训人员组成：培训人员为主要安全厂商指定培训讲师或第三方培训机构。3、培训方式：现场培训、原厂商认证培训4、培训时间、人数：现场培训天数人数不限；原厂商认证培训不少于2人、不少于3天，最终由用户确定。（二）培训期间符合相关规定要求：1、省委办公厅、省府办公厅关于印发《浙江省省直机关会议活动管理规定（试行）的通知》（浙委办【2013】82号；2、省财政厅关于印发浙江省省级机关会议费管理规定的通知（浙财行【2014】7号）；3、省财政厅关于印发浙江省省级机关培训费管理规定的通知（浙财行【2014】8号）；4、省财政厅关于差旅费等公务活动费用开支管理规定有关问题解答的通知（浙财行【2014】93号）；5、中央党的群众路线教育实践活动领导小组中共中央组织部教育部关于严格规范领导干部参加社会化培训有关事项的通知（中组发【2014】18号）；6、浙江省财政厅关于调整省级机关会议费培训费有关规定的通知浙财行〔2018〕1号；7.按最新文件执行。 |
| **履约能力** | **公司技术力量情况（提供相关证明材料）****（5分）** | 根据采购人需求要求，投标人：1.具备ISO20000信息技术服务管理体系认证证书（0.5分）；2.具备ISO27001信息安全管理体系认证证书（0.5分）；3.具备ISO9000系列质量管理体系认证证书（1分）；4.具有涉密信息系统集成证书（乙级）（1分）；5.达到ITSS信息技术服务运行维护标准（1分）；6.具有CMMI5级证书（1分）**（注：同一事项不重复计算，开标时提供原件备查）。** |
| **经验或业绩要求（3分）** | 1.投标人案例：提供2016年7月1日以来同类项目成功案例合同复印件**（以合同签订日期为准，每提供1个得0.5分，最多得2分）。**2.投标产品案例：提供2016年7月1日以来针对行政事业单位所投产品（防火墙、IPS、安全管理平台等主要安全产品）成功案例合同复印件**（以合同签订日期为准，每提供1个得0.5分，最多得1分）**。**（注：同一事项不重复计算，开标时提供合同原件备查）。** |

**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（标项及标项名称）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**

不允许转包和分包。

如乙方将项目转包或将不允许分包部分自行分包，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。[履约保证金交至甲方处，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。

**（此页无正文）**

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：ZZCG2019R-GK-117（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）提供自招标公告发布之日起至投标截止日内任意时间的“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）投标人信用查询网页截图。（以开标当日采购人或由采购人委托的评标委员会核实的查询结果为准）

（3）法定代表人授权委托书(格式见附件)；

（4）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；

（5）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）；

（6）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）；

（7）联合投标协议书（若需要）；

（8）联合投标授权委托书（若需要）；

（9）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ZZCG2019R-GK-117）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**，对招标文件的合理性、合法性不再有异议。**

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：

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：ZZCG2019R-GK-117（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，按照项目清单顺序同时附招标文件中所要求的截图、证明、证书复印件等证明材料）；

（3）技术响应表（格式见附件）；

（4）项目总体方案（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、项目明确指标方案、项目总体解决方案、项目关键性技术解决方案等）；

（5）项目实施计划及兼容性方案（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、项目实施计划方案、项目可行性实施计划方案、项目具体兼容性方案等）；

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

2. 投标人完全复制招标文件的技术规格相关部分内容作为其投标文件的一部分的，视为未实质性响应招标文件要求，其投标文件将被视为无效。

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）；

（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）；

（4）残疾人福利企业声明函（见附件）。

附件14：

**投 标 报 价 明 细 表**

投标人全称（公章）：

招标编号及标项：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **项目（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** |
| 物理机房改造（含布线） |  |  |  |  |  |  |  |  |
| 核心交换机**（核心产品）** |  |  |  |  |  |  |  |  |
| 3850交换机4端口万兆光口模块 |  |  |  |  |  |  |  |  |
| 万兆防火墙 |  |  |  |  |  |  |  |  |
| 防火墙一 |  |  |  |  |  |  |  |  |
| 防火墙二 |  |  |  |  |  |  |  |  |
| 万兆IPS一 |  |  |  |  |  |  |  |  |
| 万兆IPS二 |  |  |  |  |  |  |  |  |
| IPS三 |  |  |  |  |  |  |  |  |
| 安全隔离与信息交换系统 |  |  |  |  |  |  |  |  |
| 应用负载系统 |  |  |  |  |  |  |  |  |
| 运维安全管理（堡垒机）系统 |  |  |  |  |  |  |  |  |
| 数据库审计系统 |  |  |  |  |  |  |  |  |
| 日志审计系统扩容 |  |  |  |  |  |  |  |  |
| 态势感知大数据分析平台 |  |  |  |  |  |  |  |  |
| 态势感知全流量分析探针 |  |  |  |  |  |  |  |  |
| 态势感知风险检测探针 |  |  |  |  |  |  |  |  |
| 80KM千兆单模光模块 |  |  |  |  |  |  |  |  |
| 现网安全管理平台定制开发 |  |  |  |  |  |  |  |  |
| 安全厂商原厂安全服务 |  |  |  |  |  |  |  |  |
| 安全厂商运维人员驻场服务（1年） |  |  |  |  |  |  |  |  |
| 网络版杀毒软件 |  |  |  |  |  |  |  |  |
| 应用软件改造 |  |  |  |  |  |  |  |  |
| 国密RA中心 |  |  |  |  |  |  |  |  |
| 应用安全网关 |  |  |  |  |  |  |  |  |
| 签名服务器 |  |  |  |  |  |  |  |  |
| 4G路由器 |  |  |  |  |  |  |  |  |
| 三级等保测评 |  |  |  |  |  |  |  |  |
| **…** |  |  |  |  |  |  |  |  |
| **…** |  |  |  |  |  |  |  |  |
| **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： **本项目为交钥匙工程，项目费用包括项目实施所需的项目清单中所有设备（含数量）、软硬件对接费用（如有）、培训费、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，投标总价合计金额应与明细报价汇总相等。**报价中出现报价优惠等字样或报价明细出现“0”元（视同赠送），按无效标处理。****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），是否给予价格扣除按前附表“小微企业有关规定”要求认定。**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、《中小企业声明函》中，须同时满足以上两个条件。如投标人提供非本企业制造的货物，须提供制造商“国家企业信用信息公示系统——小微企业名录”页面查询结果（查询时间为投标前一周内，并加盖投标人公章）；**

**2、如联合体投标时，联合体各方均为小型、微型企业的，联合体各方须提供《中小企业声明函》以及“国家企业信用信息公示系统——小微企业名录”页面查询结果（查询时间为投标前一周内，并加盖本单位公章）；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：

**（以下附件在递交投标文件时单独提供即可，无需密封进投标文件）**

附件17：

**投标文件接收回执**

\_ （投标人全称）

你单位递交的以下项目投标文件，经查验，投标文件的包装、密封情况符合招标文件要求，已于 年 月 日 时 分由我中心工作人员接受。

|  |  |  |  |
| --- | --- | --- | --- |
| 项目编号 |  | 标 项 |  |
| 项目名称 |  |

**请仔细阅读以下内容：**

1、本回执中除接收时间、接收人签名以外均为必填，如因信息填写错误、疏漏等造成投标文件接收出现任何问题，责任由投标单位自负。

2、标项填写方式：如该项目只有一个标项填“1”，多个标项请填写投标的完整标项号。

3、本回执投标单位按要求填写打印后，由授权代表携带至投标现场，与投标文件一并交至省政府采购中心现场工作人员。如投标人递交投标文件时未提供回执，视同不需要回执。

 浙江省政府采购中心

接收人签名或签章：

附件18：

**政府采购活动现场确认声明书**

**浙江省政府采购中心：**

本人经由 （单位）负责人 （姓名）合法授权参加 项目（编号： ）政府采购活动，经与本单位法人代表（负责人）联系确认，现就有关公平竞争事项郑重声明如下：

1. 本单位与采购人之间 □不存在利害关系 □存在下列利害关系 ：

 A.投资关系 B.行政隶属关系 C.业务指导关系

 D.其他可能影响采购公正的利害关系（如有，请如实说明） 。

 二、现已清楚知道参加本项目采购活动的其他所有供应商名称，本单位 □与其他所有供应商之间均不存在利害关系 □与 （供应商名称）之间存在下列利害关系 ：

 A.法定代表人或负责人或实际控制人是同一人

 B.法定代表人或负责人或实际控制人是夫妻关系

 C.法定代表人或负责人或实际控制人是直系血亲关系

 D.法定代表人或负责人或实际控制人存在三代以内旁系血亲关系

 E.法定代表人或负责人或实际控制人存在近姻亲关系

 F.法定代表人或负责人或实际控制人存在股份控制或实际控制关系

 G.存在共同直接或间接投资设立子公司、联营企业和合营企业情况

 H.存在分级代理或代销关系、同一生产制造商关系、管理关系、重要业务（占主营业务收入50%以上）或重要财务往来关系（如融资）等其他实质性控制关系

 I.其他利害关系情况 。

1. 现已清楚知道并严格遵守政府采购法律法规和现场纪律。
2. 我发现 供应商之间存在或可能存在上述第二条第 项利害关系。

 （供应商代表签名）

 年 月 日