****

**台州市政府采购招标文件**

**TZCG-2020-GK025D号**

采购项目：台州市公安局智慧\*\*项目

采购人：台州市公安局

台州市政府采购中心

2020年11月5日

**目 录**

1. **公开招标采购公告**
2. **投标人须知**
3. **评标办法及评分标准**
4. **公开招标需求**
5. **政府采购合同主要条款指引**
6. **电子投标文件格式附件**
7. **公开招标采购公告**

#  项目概况

**台州市公安局智慧\*\*项目**的潜在投标人应在“浙江省政府采购网”（http:// www.zjzfcg.gov.cn）和“台州市公共资源交易中心”（ [http://www.tzztb.com](http://www.xjztb.cn)）获取招标文件，并于2020年11月27日 9点00分（北京时间）前递交电子投标文件。

##

## 项目基本情况

## 项目编号：TZCG-2020-GK025D号

项目名称：**台州市公安局智慧\*\*项目**

采购需求：

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **标段号** | **项目****名称** | **简要技术要求服务要求等** | **数量** | **单位** | **预算（万元）** | **最高限价（万元）** | **交货期（合同签订后几天内）** | **交货地点** |
| 1 | 智慧\*\*-安全访问平台 | 详见技术需求 | 1 | 套 | 1043.6万元 | 1021.7096万元 | 60天 | 台州市公安局 |
| 2 | 智慧\*\*-虚拟化平台扩容 | 1 | 批 | 636.2万元 | 606.68万元 | 30天 |

1、本次采购产品为非进口产品。

2、本项目不接受联合体投标。

## 二、申请人的资格要求：

1.满足《中华人民共和国政府采购法》第二十二条规定；

2.本项目的特定资格要求：无

## 三、获取招标文件

时间：2020年11月9日至2020年11月13日

方式：投标人在浙江政府采购云平台（http://www.zcygov.cn）进行网上报名后可免费下载。**提示：采购机构将拒绝非报名供应商的电子投标文件。**

## 四、提交投标文件截止时间、开标时间和地点

 2020年11月27日9点00分（北京时间）

本项目只接受电子投标文件，具体操作要求见前附表。请在开标当日09:00至09:30完成电子投标文件解密。

## 五、公告期限

自本公告发布之日起5个工作日。

## 六、其他补充事宜

1、供应商认为采购文件使自己的权益受到损害的，可以自收到采购文件之日（获取截止日之后收到采购文件的，以获取截止日为准）起7个工作日内且应当在采购投标截止时间之前，以书面形式一次性向采购人和集中采构机构提出同一环节的质疑。否则，被质疑人可不予接受。质疑供应商对采购人、集中采构机构的答复不满意或者采购人、集中采构机构未在规定的时间内作出答复的，可以在答复期满后十五个工作日内向同级政府采购监督管理部门投诉。

2、根据《浙江省政府采购供应商注册及诚信管理暂行办法》浙财采监【2009】28号文件，请各投标供应商及时办理浙江政府采购网“政府采购供应商注册”手续。

3、参与政府采购项目的注册供应商，需登录浙江省政府采购网（[http://www.zjzfcg.gov.cn](http://www.tzztb.com/tzcms/zfcg.jhtml)）进行网上报名；尚未注册的供应商应当先在浙江政府采购网上申请注册，注册后再进行网上报名。

## 七、对本次招标提出询问，请按以下方式联系。

　　**1.采购人（受理采购文件相关质疑及答复）**

名 称：台州市公安局

地址：台州市椒江区康平路2号

联系人：叶老师（第一标段）、赵老师（第二标段）

联系电话：13706550571、13857657666

2.**集中采购机构**

名 称：台州市政府采购中心

地　址：台州市公共资源交易中心

项目联系人：陶先生

联系电话：0576-88685172

窗口联系人：候女士（受理供应商注册、中标结果相关质疑及答复）

联系电话：0576-88685121

 台州市政府采购中心

 2020 年 11月5日

1. **投标人须知**

**前附表**

|  |  |  |
| --- | --- | --- |
| 序号 | 项 目 | 内 容 |
| 1 | 供应商特定资格要求 | 符合招标公告资格要求的供应商 |
| 2 | 答疑会或现场踏勘 | 无 |
| 3 | 电子投标要求 | 投标人须按照采购文件和电子交易平台的要求编制并加密电子投标文件。截止时间：开标当日09:00投标人应当在投标截止时间前完成电子投标文件的传输递交，并可以补充、修改或者撤回电子投标文件。补充或者修改电子投标文件的，应当先行撤回原文件，补充、修改后重新传输递交。投标截止时间前未完成传输的，视为撤回电子投标文件。逾期上传的电子投标文件恕不接受。**温馨提醒：供应商应提前上传，以便在上传时遇到技术问题，有充足的时间请教平台的技术人员。**平台技术人员联系人：徐女士；联系电话：0576-88685161/18806862938 |
| 4 | 电子投标文件解密要求 | 电子投标文件在线解密时间：开标当日09:00至09:30；投标人应当按规定及时解密，若因技术原因导致电子投标文件未能及时解密的，应联系我中心技术人员在**监管人员**监督下远程协助其完成解密，仍无法完成解密的，应按规定及时递交备份电子投标文件，否则，视同放弃投标。 |
| 5 | 备份电子投标文件制作要求 | 备份电子投标文件是通过“政采云”平台电子投标工具制作电子投标文件产生的备份文件，请投标人自行妥善保管。 |
| 6 | 备份电子投标文件使用、递交有关规定 | 1.使用前提：投标人自行在线解密操作失败无法按时寻求技术人员帮助解密，或者投标人寻求技术人员帮助仍无法按时完成解密；2.递交截止时间：开标当日09:50；3.投递邮箱：开标当日钉钉直播群公布的指定邮箱；4.未按上述要求递交备份电子投标文件或所提供的的备份电子投标文件不符合要求的视同放弃投标。 |
| 7 | 样品递交要求 | 无 |
| 8 | 投标有效期 | 投标有效期为开标后90天，投标有效期从提交电子投标文件的截止之日起算。 |
| 9 | 远程在线演示要求 | 无 |
| 10 | 不见面开标直播 |  本项目开评标环节实行全流程电子化，采取不见面钉钉直播开标，投标人可自行下载“钉钉软件”观看。（钉钉直播群号为：31065255，投标人只能于开标当天8：45以后搜索到群号，并申请进群。所有供应商均应当准时在线参加。如未参加，造成无法投标或投标失败等后果由供应商自行承担。） |
| 11 | 投标与开标注意事项 | 1.本项目实行电子采购，采用电子投标文件。若供应商参与投标，自行承担投标一切费用。2.标前准备：各供应商在开标前确保成为浙江省政府采购网正式注册供应商，并完成CA数字证书办理。（办理流程详见本招标公告附件：“政采云CA签章申领操作流程.pdf”）。因未注册入库、未办理CA数字证书等原因造成无法投标或投标失败等后果由供应商自行承担。3.电子投标文件制作：3.1应按照本项目招标文件和政采云平台的要求编制、加密并递交电子投标文件。供应商在使用系统进行投标的过程中遇到涉及平台使用的任何问题，可致电政采云平台技术支持热线咨询，联系方式：400-881-7190。3.2投标人通过“政采云”平台电子投标工具制作电子投标文件，电子投标工具请供应商自行前往浙江省政府采购网下载并安装，（下载网址：http://www.zjzfcg.gov.cn/bidClientTemplate/2019-09-24/12975.html），电子投标文件制作具体流程详见本招标公告附件：“政采云供应商项目采购-电子招投标操作指南.pdf”。 |
| 12 | 投标人信用信息查询渠道及截止时点、信用信息查询记录和证据留存的具体方式、信用信息的使用规则 | 1、查询渠道：信用中国（网址：<http://www.creditchina.gov.cn>）、中国政府采购网(网址：http://www.ccgp.gov.cn）、国家企业信用信息公示系统（http://www.gsxt.gov.cn/index.html）等。2、截止时点：评审结束前。3、信用信息查询记录和证据留存的具体方式：由采购组织机构在规定查询时间内打印信用信息查询记录并归入项目档案。4、使用规则：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及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的供应商，将被拒绝其参与政府采购活动。 |
| 13 | 小微企业查询 | 核查渠道：http://xwqy.gsxt.gov.cn/ |
| 14 | 投标保证金 | 零元 |
| 15 | 履约保证金 | 中标后签订合同前5个工作日内，中标人需支付合同金额的5%作为履约保证金，履约保证金在项目质保期满且无违约扣除情况后30个工作日内无息退还。 |
| 16 | 实质性条款 | 带“▲”的条款是实质性条款，电子投标文件须作出实质性响应，否则作无效投标处理。 |
| 17 | 解释权 | 本招标文件解释权属于采购人和台州市政府采购中心 |

**一 、总 则**

**（一） 适用范围**

本招标文件适用于本次项目的招标、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、“采购组织机构”指采购人委托组织招标的集中采购机构/采购代理机构。

2、采购人：是指委托集中采购机构/采购代理机构采购本次项目的国家机关、事业单位和团体组织。

3、投标人：是指向采购组织机构提交电子投标文件的单位或个人。

4、货物：是指各种形态和种类的物品，包括原材料、燃料、设备、产品等。

5、服务：是指除货物和工程以外的政府采购对象，包括各类专业服务、信息网络开发服务、金融保险服务、运输服务，以及维修与维护服务等。

6、“书面形式”包括信函、传真等。

7、“▲”系指实质性要求条款。

**（三）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（招标文件有相关规定除外）。

**（四）特别说明**

1、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本法人员工（指本法人或控股公司正式员工）。

2、投标供应商所投产品除招标文件中明确规定要求“提供官网截图或相应检测报告的证明材料”以外，所有技术参数描述均以电子投标文件为准。投标供应商对所投产品技术参数的真实性承担法律责任。项目招标结束后、质疑期限内，如有质疑供应商认为中标供应商所投产品、电子投标文件技术参数与招标需求存在重大偏离、错误、甚至造假的情况，应提供具体有效的证明材料。

3、投标人在投标活动中提供任何虚假材料,其投标无效，并报监管部门查处；中标后发现的,根据《中华人民共和国政府采购法》第七十七条第一款第一项之规定，处以采购金额千分之五以上千分之十以下的罚款，列入不良行为记录名单，在一至三年内禁止参加政府采购活动，有违法所得的，并处没收违法所得，情节严重的，由工商行政管理机关吊销营业执照；构成犯罪的，依法追究刑事责任。

### 4、投标人被列入“黑名单”的，采购组织单位将根据《浙江省政府采购供应商注册及诚信管理暂行办法》第四十六条之规定，在处罚有效期内，资格审查时不予通过。

### 5、投标人不得相互串通投标报价，不得妨碍其他投标人的公平竞争，不得损害采购人或其他投标人的合法权益，投标人不得以向采购人、评标委员会成员行贿或者采取其他不正当手段谋取中标。

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

### 7、电子投标文件格式中的表格式样可以根据项目差别做适当调整,但应当保持表格样式基本形态不变。

### 8、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。

### 9、本项目不允许分包。

**二、招标文件**

 （一）招标文件由招标文件总目录所列内容组成。

（二）招标文件的澄清或修改

1、采购组织机构可视采购具体情况对已发出的招标文件进行必要的澄清或者修改。澄清或者修改的内容可能影响电子投标文件编制的，采购人或者采购组织机构应当在投标截止时间至少15日前，在原公告发布媒体上发布澄清公告，澄清或者修改的内容为招标文件的组成部分；不足15日的，采购人或者采购组织机构应当顺延提交电子投标文件的截止时间。

2、投标人在规定的时间内未对招标文件提出疑问、质疑或要求澄清的，将视其为无异议。对招标文件中描述有歧义或前后不一致的地方，评标委员会有权进行评判，但对同一条款的评判应适用于每个投标人。

 **三、电子投标文件**

**（一）电子投标文件的组成**

 投标人接到招标文件后，按照采购组织机构的要求提供：资格证明电子文件、商务与技术电子文件和报价电子文件。【特别提示：如在投标时有要求提供资料原件的，将原件扫描放入电子投标文件。】

**▲1、资格证明电子文件的组成：**

1. 投标声明书；
2. 授权委托书（法定代表人亲自办理投标事宜的，则无需提交)；
3. 法人或者其他组织的营业执照等证明文件，自然人的身份证明；
4. 财务状况报告，依法缴纳税收和社会保障资金的相关材料；
5. 具备履行合同所必需的设备和专业技术能力的证明材料(根据项目性质提供)；
6. 提供采购公告中符合供应商特定条件的有效资质证书扫描件（投标供应商特定条件中有要求的必须提供），以及需要说明的其他资料；

**2、商务与技术电子文件的组成：**

（1）投标人情况介绍（人员与技术力量、企业规模、经营业绩等）。

（2）投标方案描述：

A.项目需求的理解与分析(投标人对项目现状及需求的理解情况，对项目现状和需求描述的全面性、准确性、针对性，项目功能设计完备、对系统各组成部分等功能进行准确的分析，对项目重点、难点的把握，解决方案及合理化建议)。

B.项目组织实施方案（包括项目工期、确保项目供货的措施或方案、项目实施进度安排、项目实施人员及项目负责人的资质、类似经验及社保证明等）。

C.安装、调试及验收方案（包括项目验收标准和验收方法等）和措施；

（3）投标产品描述及相关资料：

A.设备配置（或服务事项）清单（均不含报价）。

B.产品品牌及型号、技术参数指标、性能特点、图片资料以及所遵循的技术规范、产品质保期、出厂标准、产品质量相关检测报告等内容。

注：该项视产品或服务内容设置提供。

C.商务及技术响应表。

D.投标产品中有节能产品的，应列明投标产品中有列入最新一期财政部、发展改革委公布的“节能产品政府采购清单”明细（提供所投产品在清单中所处的页码、截图，并以明显标识标注）；投标产品中有环保产品的，应列明投标产品中有列入最新一期财政部、环境保护部公布的“环境标志产品政府采购清单”明细（提供所投产品在清单中所处的页码、截图，并以明显标识标注）。

【特别提示：节能和环境标志产品最新一期政府采购清单，可在“中国政府采购网”中查看】

（4）投标人通过的质量管理和质量保证体系、环保体系、自主创新相关证书、软件著作权证等等与本项目相关的认证证书或文件；

（5）近三年来类似项目的成功案例（投标人类似项目实施情况一览表、合同复印件及其相应的发票、用户验收报告等；

（6）投标人认为需要提供的其他资料（包括可能影响投标人商务与技术文件评分的各类证明材料）。

（7）售后服务描述及承诺：

A.距采购人最近的服务网点详细介绍（包括地理位置、资质资格、技术力量、工作业绩、服务内容及联系电话等）。

B.针对本项目的售后服务措施及承诺（售后技术服务方案、人员配备、故障响应时间、技术培训方案等）。

**3、报价电子文件的组成**

（1）报价文件由开标一览表、报价明细表、小微企业等声明函、产品适用政府采购政策情况表，以及投标人认为其他需要说明的内容组成。

（2）此报价为投标人一次性报出唯一的最终价格，包含其它一切所要涉及到的费用，有选择的报价将被拒绝。

（3）投标报价是包括货款、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、合同包含的所有风险责任等各项费用及不可预见费等所需的全部费用，全部费用已包含在开标一览表的投标总报价中。

（4）政府采购优惠政策相关资料、产品适用政府采购政策情况表（如有）。

（5）投标报价单填写需清楚明了，并加盖电子印章。因表达不清引起的后果由投标人负责。

（6）投标报价应按招标文件中相关附表格式填写。

1. **电子投标文件的制作、封装及递交要求**

**1、电子投标文件的制作要求**

（1）投标人应按照电子投标文件组成内容及项目招标需求和浙江政府采购云平台要求制作电子投标文件，不按招标文件和浙江政府采购云平台要求制作电子投标文件的将视情处理（拒收、扣分等），由此产生的责任由投标人自行承担。

**电子投标文件部分：投标人应根据“政采云供应商项目采购-电子招投标操作指南”及本招标文件规定的格式和顺序编制电子投标文件并进行关联定位。**

备份电子投标文件：通过“政采云”平台电子投标工具制作电子投标文件所产生的备份文件

（2）投标人应对所提供的全部资料的真实性、有效性承担法律责任，电子投标文件中盖章之处必须加盖公章（采用CA签章）。

（3）电子投标文件以及投标人与采购组织机构就有关投标事宜的所有来往函电，均应以中文汉语书写。除签字、盖章、专用名称等特殊情形外，以中文汉语以外的文字表述的电子投标文件视同未提供。

（4）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）。

（5）若投标人不按招标文件的要求提供资格审查材料，其风险由投标人自行承担。

（6）与本次投标无关的内容请不要制作在内，确保电子投标文件有针对性、简洁明了。

**2、电子投标文件的递交要求**

（1）投标人须按照采购文件和政采云平台的要求编制并加密电子投标文件。在电子投标文件递交截止时间以前完成电子投标文件的传输递交。

（2）如有特殊情况，采购组织机构延长截止时间和开标时间，采购组织机构和投标人的权利和义务将受到新的截止时间和开标时间的约束。

3、电子投标文件的补充、修改和撤回。

（1）补充或者修改电子投标文件的，应当先行撤回原文件，补充、修改后重新传输递交。投标截止时间前未完成传输的，视为撤回电子投标文件。

**（三）电子投标文件的有效期**

1. 自投标截止日起90天电子投标文件应保持有效。有效期不足的电子投标文件将被拒绝。
2. 在特殊情况下，采购人可与投标人协商延长电子投标文件的有效期，这种要求和答复均以书面形式进行。

3.中标人的电子投标文件自开标之日起至合同履行完毕均应保持有效。

**四、开标**

（一）开标事项

采购组织机构在“招标公告”规定的时间和地点公开开标，采购组织机构工作人员接收电子投标文件并登记。评标委员会成员不得参加开标活动。**（本次招标采用先评审商务资格和技术服务方案，后公开并评审商务报价的办法实施。各位供应商投标时必须根据菜单对应上传，切勿误传，否则一切后果自行承担）**。

（二） 开标程序：

1、开标时间到后，招标项目负责人准时组织开标；

2、投标人登录政采云平台，用“项目采购-开标评标”功能对电子投标文件进行在线解密。在线解密电子投标文件时间为开标时间起半个小时内。

3、公布开标结果。

4、特别说明：本项目原则上采用政采云电子招投标开标及评审程序，但有下情形之一的，按以下情况处理：

1. 投标人应当按规定及时解密，若因技术原因导致电子投标文件未能及时解密的，应联系我中心技术人员（陈工：15167606512）在采监处的监督下远程协助其完成解密，仍无法完成解密的，应按规定及时递交备份电子投标文件，否则，视同放弃投标。

（2）开评标细则按政采云电子评标流程进行。**特别说明：政采云公司如对电子化开标及评审程序有调整的，按调整后的程序操作。**

**五、评标**

**（一）组建评标委员会**

本项目评标委员会由政府采购评审专家和采购单位评审代表组成。

**（二）评标程序**

**1、资格审查**

公开招标采购项目开标结束后，采购人或者采购组织机构应当依法对投标人的资格进行审查，对审查发现无效的进行必要的询标，由政采云在线公布无效投标的投标人名单、投标无效的原因。（若系统原因无法公布的，将由录音电话代为公布）

**符合性审查**

评标委员会应当对符合资格的投标人的电子投标文件进行符合性审查，以确定其是否满足招标文件的实质性要求，对审查发现无效的进行必要的询标，对无效投标的投标人名单及投标无效原因的公布方式同上。

**3、综合比较与评价**

（1）对于电子投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评标委员会应当以在线询标形式要求投标人作出必要的澄清、说明或者补正。

（2）评标委员会应当按照招标文件中规定的评标方法和标准，对符合性审查合格的电子投标文件进行商务和技术评估，综合比较与评价。

（3）评标时，评标委员会各成员应当独立对每个投标人的电子投标文件进行评价，并汇总每个投标人的得分。

**4、得分确认及评审报告编写**

（1）评标委员会对报价文件进行复核，对于系统计算出的价格分及总得分进行确认；

（2）评标委员会应当按照招标文件中规定的评标方法和标准，对符合性审查合格的电子投标文件进行商务和技术评估，综合比较与评价。

（3）评标委员会按评标原则及得分情况编写评审报告。

**5、评价**

采购组织机构对评标委员会评审专家进行评价。

**（三）澄清问题的形式**

投标人的澄清、说明或者补正应当采用电子询标形式，并加盖公章（电子印章），并不得超出电子投标文件的范围或者改变电子投标文件的实质性内容。

**（四）错误修正**

电子投标文件报价出现前后不一致的，除招标文件另有规定外，按照下列规定修正：

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

　　2、大写金额和小写金额不一致的，以大写金额为准；

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

　　4、总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

　　同时出现两种以上不一致的，按照前款规定的顺序修正。修正应当采用电子询标的形式，并加盖公章（电子印章）。

**（五）投标人存在下列情况之一的，投标无效**

1、**在资格证明模块或商务与技术模块中出现投标报价的**，或者报价文件中报价的货物跟商务与技术文件中的投标货物出现重大偏差的；

　　2、不具备招标文件中规定的资格要求的。

　 3、电子投标文件含有采购人不能接受的附加条件的。

4、评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在合理的时间内提供进行电子答复，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

5、报价超过招标文件中规定的预算金额/最高限价。

6、主要性能参数指标负偏离 10 项（含）以上的。

7、投标参数未如实填写，完全复制粘贴招标参数的。

8、电子投标文件提供虚假材料的。

9、不符合中华人民共和国财政部令第87号《政府采购货物和服务招标投标管理办法》第三十七条情形之一的，视为投标人串通投标，其投标无效，并移送采购监管部门：

　 （1）不同投标人的电子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）不同投标人的电子投标文件载明的项目管理成员或者联系人员为同一人；

　 （4）不同投标人的电子投标文件异常一致或者投标报价呈规律性差异；

10、不符合法律、法规和招标文件中规定的其他实质性要求的（招标文件

中打“▲”内容及被拒绝的条款）。

11、商务条款不响应。

1. 供应商仅提交备份电子电子投标文件的。

**（六）有下列情况之一的，本次招标作为废标处理**

1、出现影响采购公正的违法、违规行为的；

2、评标委员会发现招标文件存在歧义、重大缺陷导致评标工作无法进行，或者招标文件内容违反国家有关强制性规定的；

3、因重大变故，采购任务取消的；

4、法律、法规和招标文件规定的其他导致评标结果无效的。

**（七）评标原则和评标办法**

1、评标原则。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、评标办法。具体评标内容及评分标准等详见《第三章：评标方法及评分标准》。

**（八）评标过程的监控**

本项目评标过程实行全程录音、录像监控，政府采购监管部门视情进行现场监督，投标人在评标过程中所进行的试图影响评标结果的不公正活动，可能导致其投标被拒绝。

**六、定标**

1、确定中标供应商。评标委员会根据采购单位的《授权意见确认书》，推荐中标候选人或确定中标人。其中推荐中标候选人的，采购组织机构在评审结束后2个工作日内将评标报告送采购人，采购人自收到评审报告之日起5个工作日内在评审报告推荐的中标候选人中按顺序确定中标人。

2、发布中标结果公告。采购组织机构应当自中标人确定之日起2个工作日内，在省级以上财政部门指定的媒体及相关网站上公告中标结果，招标文件应当随中标结果同时公告。

3、通过政采云平台发放电子中标通知书。采购组织机构在发布中标结果公告的同时，向中标人发出中标通知书。

**七、合同签订及公告**

**（一）签订合同**

1、采购人应当自中标通知书发出之日起10个工作日内，按照招标文件和中标人电子投标文件的规定，与中标人签订书面合同或者电子合同。所签订的合同不得对招标文件确定的事项和中标人电子投标文件作实质性修改。

2、采购人不得向中标人提出任何不合理的要求作为签订合同的条件。

3、中标供应商无故拖延、拒签合同的,将取消中标资格。

4、中标供应商拒绝与采购人签订合同的，采购人可以按照评审报告推荐的中标候选人名单排序，确定下一候选人为中标供应商，也可以重新开展政府采购活动。同时，拒绝与采购人签订合同的供应商，由同级财政部门依法作出处理。

5、询问或者质疑事项可能影响中标结果的，采购人应当暂停签订合同，已经签订合同的，应当中止履行合同（中标结果的质疑期为中标结果公告期限届满之日起七个工作日）。

**（二）合同公告及备案**

1、采购人应当自政府采购合同签订之日起2个工作日内，在省级以上财政部门指定的政府采购信息发布媒体及相关网站上公告。

2、采购人应当自政府采购合同签订之日起7个工作日内，将政府采购合同通过政采云网站提交至同级人民政府财政部门备案存档。

1. **评标办法及评分标准**

一、采购组织机构将组织评标委员会，对投标人提供的电子投标文件进行综合评审。

二、本次招标项目的评标方法为综合评分法，总计100分。评标标准按以下6项内容及分值进行评审。

|  |  |  |
| --- | --- | --- |
|  标段类别 | 一 | 二 |
| 技术评分 | 40 | 42 |
| 实力信誉及业绩评分 | 15 | 16 |
| 售后服务评分 | 13 | 10 |
| 投标文件制作评分 | 2 | 2 |
| 价格分 | 30 | 30 |

（一）商务与技术文件中的客观分由评标委员会讨论后统一打分；其余在规定的分值内单独评定打分。

（二）各投标人商务与技术文件得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：

商务与技术文件得分=评标委员会所有成员评分合计数/评标委员会组成人员数。

（三）投标报价得分采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其报价得满分。其他投标人的投标报价得分按下列公式计算：

投标报价得分=(评标基准价／投标报价)× 价格分×100% 。

（四）政府采购政策及优惠：（1）关于小型、微型企业（简称小微企业）投标：小微企业投标是指符合《中小企业划型标准规定》的投标人，通过投标提供本企业制造的货物、承担的工程或者服务，或者提供其他小微企业制造的货物。本项所指货物不包括使用大、中型企业注册商标的货物。小微企业投标应提供《产品适用政府采购政策情况表》（见附件）、《小微企业声明函》，如投标人提供其他小微企业制造的货物，应同时提供制造商的《小微企业声明函（制造商）》，投标人未提供以上资料或者经评标委员会核查不符的，将不能享受相应的小微企业优惠政策。（2）监狱企业参加政府采购活动时，应当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和《产品适用政府采购政策情况表》（见附件），视同小型、微型企业，享受小微企业政府采购优惠政策。（3）残疾人福利性单位在参加政府采购活动时，应提供《残疾人福利性单位声明函》（见附件）和《产品适用政府采购政策情况表》（见附件），视同小型、微型企业，享受小微企业政府采购优惠政策。

具体优惠：对于小型微型企业产品的价格给予 6 %的扣除，用扣除后的价格计算评标基准价和投标报价。同一投标人（包括联合体），小微企业、监狱企业、残疾人福利性单位价格扣除优惠只享受一次，不得重复享受。

注：得分以系统计算为准，保留2位小数。

三、在最大限度地满足招标文件实质性要求前提下，评标委员会按照招标文件中规定的各项因素进行综合评审后，以评标总得分最高的投标人为中标候选人。

四、如综合得分相同，投标报价低者为先；如综合得分且投标报价相同的，货物类采购项目以技术性能得分较高者为先，服务类采购项目以实力信誉及业绩得分较高者为先。

五、提供相同品牌产品的不同投标人参加同一合同项下投标的，按一家供应商认定：（1）采用最低评标价法的采购项目，以其中通过资格审查、符合性审查且报价最低的参加评标；报价相同的，由评标委员会集体确定一个投标人参加评标，其他投标无效。（2）使用综合评分法的采购项目，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，由评标委员会集体推荐一个投标人作为中标候选人，其他同品牌投标人不作为中标候选人。

六、本次评分具体分值细化条款如下表：

第一标段：

|  |  |  |
| --- | --- | --- |
| **评分项目** | **评分细则** | **分值** |
| **技术性能****40分** | **技术方案** | 根据投标人对采购项目现状和招标方案需求的理解、提供的项目实现思路、体系构架、功能模块、关键技术和实施计划进行评分：第一档8-6.5分，第二档6.4-4.9分，第三档4.8-3.3分，第四档3.2-1.7分，第五档1.6-0分。 | 8 |
| **性能指标** | 对投标产品的性能指标及技术参数满足程度进行评分：满足要求的得满分，满分18分。“★”每负偏离一项扣2分，普通项每负偏离一项扣1分，扣完为止。 | 18 |
| 根据投标产品综合性能的优良及先进程度进行评分：第一档9-7.3分，第二档7.2-5.5分，第三档5.4-3.7分，第四档3.6-1.9分，第五档1.8-0分。 | 9 |
| **产品品牌** | 根据核心产品的品牌知名度、市场占有率（IDC报告等证明材料）及信誉度、厂商服务能力等情况进行评分。第一档5-4.1分，第二档4-3.1分，第三档3-2.1分，第四档2-1.1分，第五档1-0分。 | 5 |
| **实力信誉及业绩15分** | **资质** | 根据投标人企业认证、资质、质量管理等情况评分：第一档3-2分；第二档，2-1分；第三档1-0分。（提供相关证明材料。） | 3 |
| **经营状况** | 根据投标人财务经营状况、履约能力和信誉评价等综合评价。 | 2 |
| **项目组情况** | 根据为本项目配备的专业人员的数量、资质、技术能力、工作经验、分工等的合理性，以及拟担任本项目经理和技术负责人的专业资质、技术能力等进行综合评分，第一档5-4.1分，第二档4-3.1分，第三档3-2.1分，第四档2-1.1分，第五档1-0分。注：提供项目组人员的证书扫描件及对应人员近6个月的社保证明。 | 5 |
| **项目案例** | 投标人自2017年11月以来类似项目的成功案例，提供合同扫描件和验收报告（以签订时间为准），根据类似程度每个得1-0分，最高5分。 | 5 |
| **售后服务13分** | 根据售后服务方案（包括定期巡检，保修范围，服务标准，服务力量，人员配备，7\*24小时服务热线，故障响应修复时间方式及保障措施等）进行评分：第一档5-4.1分，第二档4-3.1分，第三档3-2.1分，第四档2-1.1分，第五档1-0分。 | 5 |
| 根据驻点运维人员的数量、经验、资质等情况进行综合评分：第一档3-2分；第二档，2-1分；第三档1-0分。（提供相关证明材料。） | 3 |
| 提供完备的培训方案。 | 1 |
| 备品备件，明确存放方式。 | 1 |
| 根据本地化服务能力及可行性进行打分：第一档3-2分；第二档，2-1分；第三档1-0分。 | 3 |
| **对招标文件响应程度2分** | 根据电子投标文件的内容、结构等情况与招标文件的要求比对，酌情打分。 | 2 |
| **价格30分** | 以投标合格供应商有效投标总报价中的最低价为基准价，基准价为30分。投标报价得分＝（评标基准价/最终投标报价）×30%×100（小数点后保留2位小数）。（注：对于小型和微型企业产品的价格给予6%的扣除，用扣除后的价格参与评审。) | 30 |

第二标段：

|  |  |  |
| --- | --- | --- |
| **评分项目** | **评分细则** | **分值** |
| **技术性能****42分** | **实施方案** | 根据投标人对采购项目现状及需求的理解、提供的项目实施计划进行评分：第一档6-4.9分，第二档4.8-3.7分，第三档3.6-2.5分，第四档2.4-1.3分，第五档1.2-0分。 | 6 |
| 根据投标人提供的数据库系统改造和数据迁移实施方案等进行评分：第一档8-6.5分，第二档6.4-4.9分，第三档4.8-3.3分，第四档3.2-1.7分，第五档1.6-0分。 | 8 |
| **性能指标** | 对投标产品的性能指标及技术参数满足程度进行评分：满足要求的得18分，每项负偏离扣2分，扣完为止。 | 18 |
| 通过硬件设备实现数据压缩功能得1分。 | 1 |
| 根据核心产品的存储控制器CPU数量、总物理核心数、缓存、硬盘裸容量等性能的优良先进程度进行评分：第一档4分，第二档3分，第三档2分，第四档1分。 | 4 |
| **产品品牌** | 根据核心产品的品牌知名度、市场占有率（IDC报告等证明材料）及信誉度、厂商服务能力等情况进行评分：第一档5-4.1分，第二档4-3.1分，第三档3-2.1分，第四档2-1.1分，第五档1-0分。 | 5 |
| **实力信誉及业绩16分** | **投标人资质** | 投标人具备ISO20000IT服务管理体系证书得1分。投标人具备ISO27001信息安全管理体系证书得1分。投标人具备ITSS信息技术服务运行维护标准符合性证书得1分（提供证书原件扫描件）。 | 3 |
| **项目组情况** | 项目经理具备项目管理师（高级）和DEVOPS MASTER专家认证证书，每个得1分，最高2分（证书官网可核查）。项目组人员具有所投品牌存储认证证书、VMware VCP证书、Oracle OCP证书、Oracle OCM证书的，每个得0.5分，最高3分。同一人员以上得分不得累加。要求提供证书原件扫描件及对应人员近6个月的社保证明，否则不得分。数据库证书官网可核查。 | 5 |
| **项目案例** | 投标人自2017年11月以来类似软硬件集成项目的成功案例，提供合同扫描件和验收报告（以签订时间为准），根据类似程度每个得1-0分，最高4分。投标人自2017年11月以来类似数据库迁移项目的成功案例，提供合同扫描件和验收报告（以签订时间为准），根据类似程度每个得1-0分，最高4分。 | 8 |
| **售后服务10分** | 根据售后服务方案（包括定期巡检，保修范围，服务标准，服务力量，人员配备，7\*24小时服务热线，故障响应修复时间方式及保障措施等），进行评分：第一档5-4.1分，第二档4-3.1分，第三档3-2.1分，第四档2-1.1分，第五档1-0分。 | 5 |
| 提供完备的培训方案。 | 1 |
| 备品备件，明确存放方式。 | 1 |
| 根据本地化服务能力及可行性进行评分：第一档3-2分；第二档，2-1分；第三档1-0分。 | 3 |
| **对招标文件响应程度2分** | 根据电子投标文件的内容、结构等情况与招标文件的要求比对，酌情打分。 | 2 |
| **价格30分** | 以投标合格供应商有效投标总报价中的最低价为基准价，基准价为30分。投标报价得分＝（评标基准价/最终投标报价）×30%×100（小数点后保留2位小数）。（注：对于小型和微型企业产品的价格给予6%的扣除，用扣除后的价格参与评审。) | 30 |

**注：1、合同、证书、报告及其他相关证明材料，将原件扫描上传至电子投标文件，并加盖电子印章。**

**2、得分为第一档的指的是各细项指标全部满足甚至优于采购需求的；第二档指的是与采购人目标需求相比，稍有瑕疵的；第三、四、五档依次类推。**

1. **公开招标需求**
2. **招标项目一览表**

本次招标共 2 个标段，具体内容如下表：

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **标段号** | **项目****名称** | **简要技术要求服务要求等** | **数量** | **单位** | **预算（万元）** | **最高限价（万元）** | **交货期（合同签订后几天内）** | **交货地点** |
| 1 | 智慧\*\*-安全访问平台 | 详见技术需求 | 1 | 套 | 1043.6万元 | 1021.7096万元 | 60天 | 台州市公安局 |
| 2 | 智慧\*\*-虚拟化平台扩容 | 1 | 批 | 636.2万元 | 606.68万元 | 30天 |

1. **技术需求**

**第一标段：智慧\*\*-安全访问平台**

1. **项目概况**
2. 建设目标

根据公安大数据智能化总体规划及大数据安全总体技术框架要求，以安全、可信、合规为目标，建设统一的安全访问平台，实现访问用户的身份可信，确保业务仅对合法用户可见；结合业务场景和使用环境进行精细化的动态授权；保护数据安全访问，具备抵御网络攻击的能力；实现访问过程中用户行为及网络风险的全面发现与审计。

通过态势感知、威胁预警、安全审计，把各类网络攻击活动和违规行为消灭在萌芽状态，变静态防护为动态防御，变多个单点防护为综合防控和整体防范，逐步形成事前预警、事中取证、事后查处的新型安全运行管理工作模式。

1. 建设内容

通过项目建设，初步建设成符合公安部规范要求的市本级“安全访问平台”、数据汇聚节点和用户汇聚节点，实现接入网计算机终端安全、可信地访问数据中心的应用和数据。

通过各类安全设备和系统整合，加强主机安全防护，采集、分析网络流量、各类日志中的威胁信息，捕捉虚拟机间横向流量，实时监测、阻断网络边界，扫描主机、应用等漏洞，及时发现、汇总各类威胁信息，并进行可视化展示。

1. 建设依据

\*《公安大数据安全总体技术框架》

\*《公安大数据平台安全访问平台技术设计要求》

\*《浙江省公安厅大数据智能化建设安全规划技术方案（2019-2021）》

1. **采购清单**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | **部署** | **货物名称** | **单位** | **数量** | **备注** |
| 1 | 安全访问平台 | 用户汇聚节点路由器 | 台 | 2 |  |
| 2 | 数据汇聚节点路由器 | 台 | 2 |  |
| 3 | 安全访问平台核心交换机 | 台 | 2 |  |
| 4 | 数据中心核心交换机 | 台 | 2 |  |
| 5 | 前端边界防火墙（含防病毒、IPS、DPI） | 台 | 2 | 前后端异构 |
| 6 | 后端边界防火墙（含防病毒、IPS、DPI） | 台 | 2 | 同上 |
| 7 | 云桌面超融合一体机及软件授权 | 套 | 1 |  |
| 8 | 桌面云管控系统及桌面并发用户授权 | 套 | 1 |  |
| 9 | 云桌面瘦终端（含显示屏） | 套 | 100 |  |
| 10 | 超融合交换机 | 台 | 2 |  |
| 11 | 可信环境感知代理 | 套 | 1 |  |
| 12 | 可信接入代理 | 套 | 2 |  |
| 13 | 负载均衡 | 台 | 2 |  |
| 14 | Web应用防火墙 | 台 | 2 |  |
| 15 | 超融合虚拟化平台 | 台 | 5 |  |
| 16 | 虚拟化集群交换机 | 台 | 2 |  |
| 17 | 可信代理控制服务 | 套 | 1 |  |
| 18 | 可信API代理（含软硬件） | 套 | 2 |  |
| 19 | 日志审计 | 台 | 1 |  |
| 20 | 堡垒机 | 台 | 1 |  |
| 21 | 安全管理中心 | 防火墙 | 台 | 3 |  |
| 22 | APT检测探针 | 台 | 1 |  |
| 23 | 云网安全分析系统 | 套 | 1 |  |
| 24 | 堡垒机 | 台 | 1 |  |
| 25 | 日志审计 | 台 | 1 |  |
| 26 | 数据库审计 | 台 | 1 |  |
| 27 | 漏洞扫描 | 台 | 1 |  |
| 28 | 态势感知 | 套 | 1 |  |
| 29 | 网络管理平台 | 套 | 1 |  |
| 30 | 终端安全管理平台 | 套 | 1 |  |
| 31 | 杀毒软件 | 套 | 1 |  |
| 32 | PKI/PMI系统 | 套 | 1 |  |
| 33 | 显示器 | 台 | 2 |  |
| 34 |  | 集成服务 |  |  |  |
| 35 |  | 三级等保测评服务1次（2.0标准） | 次 | 1 |  |
| 36 |  | 售后驻点运维（2人驻点服务3年） | 年 | 3 |  |

1. **技术参数需求**

**1、用户汇聚节点路由器**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| ★ 性能 | 交换容量≥100Tbps，包转发率≥14000Mpps； |
| 可靠性设计 | 支持主控板、业务板完全物理分离，主控板、业务板分布在不同的物理槽位，需提供设备面板图并指出对应的主控板和业务板槽位； |
| 业务槽扩展性 | 有足够的后向扩展性，业务插槽数≥8； |
| 支持交流电源 | 支持内置交流电源，不能配置外置交流电源（单点故障风险高），也不额外占用业务槽位，提供第三方测试报告； |
| 电源冗余 | 电源个数≥4个，电源系统支持N+M冗余，支持一体化供电方式，任意拔掉两个电源，设备能够正常运行，并提供第三方测试报告； |
| 堆叠特性 | 支持将≥两台物理设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理，跨物理设备的链路聚合； |
| 产品成熟度 | 所投产品是成熟稳定的产品，要求设备入网时间≥半年，提供工信部入网许可证复印件；  |
| 产品实配 | 实配双主控，不少于1200W交流电源模块≥4个，单台实配≥40G口不少于4个，分别位于2块业务处理单元卡；单台实配10个万兆光口，分别位于2块业务处理单元卡；实配主机软件。单台实配8个多模40G光模块，8个万兆单模光模块（10KM）。 |
| 质保 | 原厂五年质保，中标后签订合同前提供原厂商质保承诺函。 |

**2、数据汇聚节点路由器**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| ★性能 | 交换容量≥100Tbps，包转发率≥14000Mpps； |
| 可靠性设计 | 支持主控板、业务板完全物理分离，主控板、业务板分布在不同的物理槽位，需提供设备面板图并指出对应的主控板和业务板槽位； |
| 业务槽扩展性 | 有足够的后向扩展性，业务插槽数≥8； |
| 支持交流电源 | 支持内置交流电源，不能配置外置交流电源（单点故障风险高），也不额外占用业务槽位，提供第三方测试报告； |
| 电源冗余 | 电源个数≥4个，电源系统支持N+M冗余，支持一体化供电方式，任意拔掉两个电源，设备能够正常运行，并提供第三方测试报告； |
| 堆叠特性 | 支持将≥两台物理设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理，跨物理设备的链路聚合； |
| 产品成熟度 | 所投产品是成熟稳定的产品，要求设备入网时间≥半年，提供工信部入网许可证复印件； |
| 产品实配 | 实配双主控，不少于1200W交流电源模块≥4个，单台实配≥40G口不少于6个，分别位于2块业务处理单元卡；单台实配10个万兆光口，分别位于2块业务处理单元卡；实配主机软件。单台实配8个多模40G光模块，2个单模40G光模块（10KM），10个万兆多模光模块。 |
| 质保 | 原厂五年质保，中标后签订合同前提供原厂商质保承诺函。 |

**3、安全访问平台核心交换机**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| ★交换性能 | 交换容量≥400T，包转发率≥85000Mpps； |
| 产品架构 | 支持多级交换架构，能够配置独立的交换网板与独立的主控板 |
| 设备槽位 | 主控引擎≥2；独立交换网板≥4；主控槽位与交换网板槽位宽度相同的全宽槽位；整机业务板槽位数≥6；提供产品截图证明,并标注业务槽位和交换网槽位，确保数量满足要求； |
| 堆叠特性 | 支持虚拟化堆叠技术，热备冗余提升可靠性；支持横向虚拟化技术，提供工信部权威第三方测试报告； |
| IP路由 | 支持静态路由、RIP、RIPng、OSPF、BGP、BGP4+、ISIS |
| 风扇冗余 | 为保证设备散热效果和可靠性，要求设备支持模块化风扇框，可热插拔，当单个风扇框发生故障时，有其他风扇正常运行，保证设备散热，独立风扇框数≥2  |
| 产品成熟度 | 本次提供产品为市场成熟产品，具有半年以上的入网时间，要求提供工信部入网证截图证明； |
| 产品实配 | 实配双主控，四交换网板，业务板槽位≥6，实配万兆光口≥36个，千兆光口≥20个，千兆电口≥24个，40G接口≥4个，实配2根40G堆叠电缆，交流电源模块≥4。 |
| 质保 | 原厂五年质保，中标后签订合同前提供原厂商质保承诺函。 |

1. **数据中心核心交换机**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| ★产品架构 | 能够配置独立的交换网板，控制引擎和交换网板硬件相互独立，主控板故障或者更换不影响整机转发性能。 |
| ▲交换性能 | 交换容量≥360T，包转发率≥230000Mpps； |
| 产品槽位 | 设备支持双主控、六交换网板（交换网板5+1冗余）、业务槽位≥8,风扇框≥2，电源模块≥8； |
| 设备散热 | 设备采用严格的前后风道设计，气流在机框内部始终处于由前向后的流向，业务线卡和网板均使用前面板打孔/前后风道设计，大大提升散热性能； |
| 虚拟化特性 | 虚拟化支持将≥2台设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理，跨物理设备的链路聚合；提供三方权威机构检测报告； |
| 电源冗余 | 最多支持8块电源模块，支持4+4冗余； |
| 风扇冗余 | 机箱支持双风扇框互为冗余，在拔出一个风扇框的情况下，设备可正常运行72小时，无丢包；提供权威第三方检测报告； |
| 业务板卡扩展 | 单板最大支持36口40G板卡，最大支持36口100G业务单板；提供官网链接及截图证明； |
| 产品成熟度 | 本次提供产品为市场成熟产品，具有半年以上的入网时间，要求提供工信部入网证截图证明； |
| 产品实配 | 实配主控≥2，交换网板≥3，实配光口≥120个（万兆光口不少于72个），40G光口≥10个，不少于6块交流电源模块功率≥2000W。单台实配7米40G堆叠电缆2根,QSFP+模块3个。 |
| 质保 | 原厂五年质保，中标后签订合同前提供原厂商质保承诺函。 |

1. **前端边界防火墙（含防病毒、DPI）**

|  |  |
| --- | --- |
| 技术指标 | 设备技术要求 |
| **品牌型号** | ▲要求与后端边界防火墙设备为不同架构和品牌 |
| ★架构及性能要求 | 系统采用多核AMP+架构架构，硬件设计采用高性能一体化智能安全处理引擎，要求提供计算机软件著作权登记证书。 |
| 网络处理能力为80G，并发连接≥900万，每秒新建连接100万/秒，冗余电源。配置≥8个10/100/1000M自适应电口，≥8个万兆SFP+光口插槽，≥2个40G QSFP插槽。支持2个扩展槽，1个Console口，支持液晶屏。需配置入侵防御及网络防病毒模块，提供五年硬件维保及规则库升级服务。 |
| 部署模式 | 支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求。支持旁路模式； |
| 路由协议 | 支持支持静态路由、策略路由及动态路由。策略路由支持用户自定义其优先级，动态路由应至少支持RIP v1/v2/ng， OSPFv2/v3，BGP4/4+协议；必须支持静态和动态多播路由，动态多播路由必须支持PIM-SM（稀疏模式） |
| 地址转换 | 支持全面的NAT转换配置，包括一对一，一对多，多对一的源、目的地址转换，并至少支持FULL\_CONE模式和SYMMETRIC模式 |
| IPV6支持 | 支持IPv6下静态路由及策略路由、动态路由，动态路由应包括RIPng、OSPFv3、BGP4+ |
| 高可靠性 | 支持路由模式、透明模式的HA高可靠性部署，可工作于主备、主主模式，会话、用户、配置可实时同步；设备支持一种多防火墙的负载均衡方法及装置的技术，必须提供自主知识产权证明复印件。HA高可靠性部署支持接口联动，某个端口失效（DOWN），属于同一接口组中其他端口都会进入失效状态（DOWN）；HA高可靠性部署支持配置接口权重；  |
| 访问控制 | 支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查（投标时需要提供上述功能截图） |
| 入侵防御 | 支持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL注入、WEB攻击等六种分类；漏洞防护支持日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于FTP、HTTP、IMAP、OTHER\_APP、POP3、SMB、SMTP等应用协议的漏洞防护。 |
| 支持在设备漏洞防护特征库直接查阅攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息；  |
| 漏洞防护特征库包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云3”、“Struts”、“Struts2”、“Xshell后门代码”以及对应的攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息； |
| 病毒防护 | 能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀 |
| 本地病毒库规模大于3000万，必须支持对最多6级的压缩文件进行解压查杀 |
| 支持基于MD5的自定义病毒签名；支持设置例外特征，对特定的病毒特征不进行查杀 |
| VPN功能 | 支持支持IPSec VPN功能，支持基于主模式（Main Mode）、积极模式（Aggressive Mode）、国密三种协商模式建立的网关-网关加密隧道；支持本地CA并可为参与IPSec VPN隧道建立的设备颁发用于身份认证的证书 |
| 网络异常感知 | 支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机IP、用户名、资产等信息；并对威胁情报发现的恶意主机执行自动阻断 |
| 支持统计网络内威胁事件的数量及对应的风险等级；支持一键跳转查看详情并自动显示关联日志；可基于网络连接、应用名称、威胁事件处置威胁事件；  |
| 安全事件分析 | 提供关联分析面板，可将Top应用、Top威胁、Top URL分类、Top源地址、Top目的地址等信息关联，并支持以任意元素于为过滤条件且不少于35个维度进行数据钻取 |
| 支持基于网络活动，威胁活动、阻止活动等多维关联统计及分析，发现异常行为 |
| 策略与处置 | 可在单条策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能选项。 |
| 支持接收针对突发重大安全事件的“应急响应消息”，并至少在界面显示安全事件名称、类型、当前防护状态、处置状态以及相应的操作等信息；并可根据设备安全配置的变化动态显示应急响应的处理结果 |
| 支持针对“应急响应消息”的手动或自动处置，处置方法至少包括基于漏洞的处置和基于威胁情报的处置（投标时需要提供上述功能截图） |
| 运维管理 | 支持双系统备份，且在系统切换中可实现配置的自动迁移；可记录不同时间点的历史配置文件。 |
| 支持将告警信息以SNMP Trap、邮件、声音、短信等形式通知管理员，告警信息的范围至少包括配置变更、病毒事件、攻击事件、异常事件、CPU利用率、内存利用率、硬盘利用率、接口带宽利用率、NAT利用率等；  |
| 支持三权分立管理，具有独立审计用户，支持标准Syslog日志审计方式，支持Syslog端口自定义（支持内外端机主机名更改，强化日志审计及集中管理功能，能够对功能访问模块拒绝访问进行日志记录，支持对日志的高性能处理和存储，提供高性能Syslog日志处理和存储证书。 |
| ★协同联动 | 支持与云端联动，至少实现病毒云查杀、URL云识别、应用云识别、云沙箱、威胁情报云检测等功能（投标文件需提供能够体现上述功能及配置选项截图） |
| 资质要求（需提供相关扫描件） | 设备需具备计算机信息系统安全专用产品销售许可证(增强级) |
| 设备需具备中国国家信息安全认证产品型号证书 |
| 设备需具备国家信息安全测评信息技术产品安全测评证书（EAL4+级） |
| 服务 | 原厂五年质保，中标后签订合同前提供原厂商质保承诺函。 |

**6、后端边界防火墙（含防病毒、DPI）**

|  |  |
| --- | --- |
| **指标项** |  **要求** |
| 品牌要求 | ▲与前端边界防火墙设备为不同架构和品牌 |
| 配置要求 | ★配置双主控，双电源；配置应用层协议识别及流量控制功能，5年应用协议特征库升级；配置负载均衡功能，配置IPS、防病毒、URL过滤功能，及5年IPS特征库、网络病毒特征库、URL特征库升级；  |
| 硬件架构 | 采用多核路由器架构，双主控，双电源；除两个主控板外，整机扩展插槽≥6 |
| 接口板和业务板分离，电源、主控板、接口板、业务板支持热插拔 |
| 接口要求 | ★单台配置≥40个光口（万兆光口不少于24个），≥4个40G口，≥2个2500W电源，实配≥4个40G多模模块。 |
| 支持40GE，100GE接口，便于平滑扩展需要（提供产品厂商官网上相关规格描述截图与网址链接） |
| 性能要求 | ★IPSec VPN隧道≥95K；吞吐量≥100Gbps，最大并发连接≥3900万，整机可平滑扩展到≥600Gbps。 |
| 开启IPS，防病毒策略后吞吐量≥40Gbps |
| 路由功能 | 支持静态路由、策略路由、RIP、OSPF、BGP、ISIS等路由协议 |
| IPV6 | 支持IPv6协议栈、IPV6穿越技术、IPV6路由协议（提供“IPV6 Ready Phase-2”认证证书复印件） |
| 策略管理 | 支持策略的模糊查询，策略组，策略规则标签，方便策略的管理及运维。 |
| 入侵防御及病毒防护 | 基于特征检测，支持超过12000种特征的攻击检测和防御 |
| 支持基于场景进行策略入侵防御的模板定制。 |
| 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能。（提供功能截图） |
| 可以支持HTTP、FTP、SMTP、POP3、IMAP、NFS等协议的病毒防护 |
| 加密流量安全防护 | 支持对HTTPS，POP3S，SMTPS,IMAPS加密流量代理解密后，并进行内容过滤，审计，安全防护。（提供功能截图） |
| 支持基于URL分类的精细化解密，提高解密性能。（提供功能截图） |
| 负载均衡 | 支持并配置负载均衡功能，包括链路智能选路负载均衡、服务器负载均衡等功能，负载均衡算法包括但不限于简单轮询、加权轮询、最小连接、加权最小连接等 |
| 可靠性 | 支持跨数据中心集群，实现双机快速切换，满足数据中心双活，多活场景； |
| 系统日志 | 支持URL日志，同时包含NAT信息和URL信息（提供功能截图）， |
| 产品资质 | 具有公安部颁发的《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 |

1. **云桌面超融合一体机设备（1套）**包括：资源服务器5台及服务器虚拟化软件

|  |  |
| --- | --- |
| 技术指标 | 具体参数 |
| 数量要求 | ▲本项目总计采购5台云桌面资源服务器及桌面资源服务器的虚拟化授权。提供相关服务器虚拟化与存储虚拟化标准版授权，本项目要求所提供的存储虚拟化授权无容量限制，满足桌面云数据存储空间的扩容需求。要求兼容桌面云控制系统。 |
| 单台硬件规格 | CPU： Gold 6132以上性能\*2颗、内存≥256G、千兆网口≥4个、万兆光口≥2个（配置光模块），冗余双电源；本项目要求至少配备1块≥128G SSD硬盘、2块≥800G SSD硬盘和≥48T的SATA硬盘裸容量。 |
| 部署模式 | 兼容市场上主流x86服务器和存储设备，支持品牌不局限于联想、浪潮，深信服等。无需部署集中管理平台，通过Web方式接入集群主服务器，实现对服务器、虚拟机、网络、存储等进行统一管理。 |
| 部署存储虚拟化之后，可以将服务器直连硬盘组成分布式共享数据存储，构建桌面云提供低成本、高性能的存储方案。要求存储虚拟化和服务器虚拟化采用统一的Web界面进行管理，简化运维。 |
| 功能支持 | 支持服务器端口汇聚技术（管理口、业务口、存储口），将多个网络端口聚合起来，提高网络带宽和容错能力。 |
| 支持集群冗余技术，集群中各主机互为监控，一旦发现某个主机故障，HA机制就会自动触发虚机迁移动作，在另一正常服务器快速拉起、确保VM继续可用。 |
| 支持SSD缓存加速，采用SSD+HDD混合模式，SSD用于缓存热点数据，HDD用于存储个人数据，SSD缓存命中率不低于60%，确保最优用户体验。支持虚拟机集中备份与恢复，可按需选择多个虚拟机或全部虚拟机备份至外置服务器，并可设置备份策略，实现自动化备份。 |
| 支持内存页合并技术，能够有效消除多个虚拟机运行过程中重复只读内存数据，以节省内存使用，提升服务器部署密度。 |
| 支持数据冗余副本技术，每份数据同时写入多台服务器，每次数据变化时自动实时同步，确保磁盘或服务器故障，数据不丢失。 |
| 当磁盘或服务器故障后，桌面业务不中断， IT人员只需要更换新设备，整个数据重建/恢复过程，无需关停机。 |

1. **桌面云管控系统与云桌面并发用户授权**

|  |  |
| --- | --- |
| 数量要求 | ▲**提供2台云桌面管理设备及300并发用户接入授权。** |
| 配置要求 | 为提升桌面云接入性能及稳定性，本项目每组要求配备2一体化专用硬件控制器实现云桌面系统管理。桌面云控制器设备要求:标准2U设备，配置6个千兆电口，2个千兆光口，吞吐量不低于500Mbps，支持并发用户数大于2000个。为了满足不同场景的应用需求，要求每用户授权支持发布个性化桌面、共享式桌面、虚拟应用3种资源类型。**本项目提供云桌面功能软件授权，与云桌面管控系统、云桌面服务器虚拟化软件为同一品牌。** |
| 部署模式 | 桌面云控制器支持集群部署（非双机热备方式），在不借助第三方工具/软件的情况下，实现多台控制器并发使用及故障切换，且切换过程中桌面会话不中断，满足对性能和稳定性的要求。 |
| 用户体验 | 支持Windows7、Windows10、Windows Server等多种云桌面操作系统,并且支持两种以上的Linux虚拟桌面操作系统，其中要包含国产Linux操作系统，如中标麒麟，银河麒麟； |
| 云桌面系统要求兼容后续建设的可信代理控制服务系统，配合实现与可信代理控制服务系统联动。 |
| 支持Windows 10优化工具，关闭和禁用不需要的服务、启动项和视觉特效，让桌面运行更流畅。 |
| 支持接入虚拟机时显示开机画面，同时支持在虚拟机上更改分辨率（在桌面右键点击“个性化分辨率”进行设置），保持与普通PC一样的使用方式。 |
| PC（或笔记本）接入虚拟桌面支持通过导航条或快捷键切换为窗口化模式，用户可随意改变窗口大小且分辨率会自动适应。 |
| 支持远程协助功能，管理员在云桌面控制台中可以直接向需要协助的用户发起远程协助，用户桌面无需安装任何辅助软件。 |
| 支持联动关机技术，可以跟使用PC一样，打开操作系统“开始”菜单、点击“关机”按钮，桌面云终端和操作系统将会一体化关闭，没有多余的操作步骤。 |
| 支持视频重定向，支持本地本地播放器，以及优酷、土豆、腾讯等多种在线视频网站，要求播放1080P高清视频时，桌面CPU利用率不高于15%。支持USB外设映射，兼容高拍仪、扫描枪、扫描仪、摄像头、密码小键盘、指纹收集器、身份证读卡器、手写板、打印机、USB-key等不同外设。 |
| 支持云桌面导航条显示网络状态，支持导航条显示当前终端（瘦终端、PC客户端）与云桌面控制台之间的网络状态，网络状态会以不同的信号格数显示，用户可以实时查看网络状态和时延，当网络状态不佳时在后台进行日志记录，方便管理员进行网络状态查询和维护。 |
| 支持自助快照恢复，当用户自己误操作导致云桌面卡慢、蓝屏、死机或者中病毒的时候，用户通过导航条按钮，可以自助进行系统盘快照还原操作，支持安卓瘦终端、PC客户端。 |
| 客户端连接虚拟桌面无需依赖虚拟机IP，在虚拟机网卡被禁用或被更改IP的情况下，云桌面业务不会中断，这样可以防止因误操作而导致连接中断。 |
| 运维功能 | 支持虚拟机自由分组、支持修改计算机名称、支持根据虚拟机名称、关联用户、用户描述、IP、MAC、所属资源、所属平台等信息搜索虚拟机。 |
| 支持为运行中的云桌面虚拟机进行分组管理和批量设置IP，提升IT人员桌面维护效率。 |
| 支持模板克隆技术，克隆时可指定虚拟机数量、运行位置、存储位置、网口信息、磁盘大小，本项目要求100个虚拟机派时间不超过5分钟。  |
| 支持设置虚拟机开关机计划，一方面可避免并发开机IO风暴问题，另一方面可释放服务器资源。 |
| 支持软件分发，通过创建软件库并关联给虚拟机，实现应用软件、驱动程序的增量式更新，不需要在每个虚拟机执行安装过程，整个分发过程秒级完成。 |
| 支持为云桌面设置还原模式，在操作系统重启后，除个人数据之外其他内容均还原为初始状态，始终为用户呈现干净可用的桌面环境，降低系统故障率。 |
| 支持AD域离线认证，在AD域服务器故障离线后，用户依然可以用AD账号认证登录桌面云。 |
| 支持集中分配个人磁盘，并可以指定磁盘空间大小，在空间不足时还可以为用户新增个人磁盘，以满足用户文档存储需求。 |
| 支持控制器、服务器等组件故障后，通过邮件等方式告警。支持管理员给在线用户推送消息和通知，管理员可以根据需求发给指定用户或者发给所有用户。 |
| 要求支持快照技术，当系统故障时可实现故障回滚；同时支持增量保存快照数据，以节省存储空间。 |
| 安全管理 | 支持多种身份认证方式随需组合，至少应包括账号密码、usb-key认证、短信认证、硬件特征绑定等4种方式，支持设置首次登录强制修改密码、定时修改密码、图形校验码和软键盘等密码安全策略，以保障认证密码安全性，避免越权访问行为。 |
| 支持在管理组件中内置应用管控技术，实现全方位云桌面管控，在禁止名单中可以通过配置规则禁止指定应用或进程在云桌面中运行；在允许名单中通过配置规则只允许规则中的应用或进程在云桌面中运行。 |
| 支持客户端安全检测，可根据用户接入的终端类型、操作系统版本、接入IP和时间、软件安装情况等指定访问策略，如客户端不满足安全检测要求则不允许接入，有效保障接入安全性。 |
| 支持文件导出内容审计，开启文件安全导出后，虚拟机通过剪切板、PC设备和USB设备外发文件的操作将被禁止，用户可以使用虚拟机内部的文件导出工具实现文件外发，所有外发的文件内容都可以加密备份到数据中心，以备后续审计使用，可疑的导出行为会产生告警。 |
| 支持USB黑白名单技术，能够精准识别每一款不同类型的外设（包括高拍仪、摄像头、USB光驱、认证key等），并设置放通或者限制策略，提高管控粒度和安全性。 |
| 支持临时权限，管理员为部分用户临时在某个时间段内放通usb和pc剪切板等权限，并在到期后自动回收该权限，保证数据安全。支持用户终端与云桌面平台之间采用VPN隧道传输，实现数据加密，保障外网接入安全。 |
| 要求支持个人盘加密技术，对云桌面个人数据进行加密保存，保障个人隐私安全。 |
| 桌面云控制器内置防火墙，包括设置过滤规则、NAT设置、访问监控、防DOS攻击、QOS上传下载规则等。 |

**9、云桌面瘦终端（100台）**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 处理器 | ★采用四核处理器，主频1.8Ghz及以上，支持Linux操作系统； |
| 内存 | 使用DDR3内存≥2G，存储≥8G； |
| 网口 | 至少提供1个千兆自适应电口网卡； |
| IO | 支持≥6个USB标准接口，1个耳机口，1个麦克风口，自带壁挂架； |
| VGA | 提供≥1个VGA显示接口，以及提供≥1个HDMI显示接口，最大分辨率支持1920x1200@60Hz； |
| 报告 | 提供3C和CQC节能认证证书及认证报告； |
| 管理 | 支持通过云桌面管理平台集中统一运维管理，包括系统更新、桌面客户端更新、批量开关机等操作。 |
| 实配 | 实配终端1台，19.5寸及以上宽屏显示屏1块。 |
| 质保 | 原厂三年质保，中标后签订合同前提供原厂商质保承诺函。 |

**10、超融合交换机（2台）**

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 交换性能 | 交换容量≥2Tbps，包转发率≥700Mpps，（若官网存在双指标，以较小为准）；双风扇，双电源； |
| 堆叠特性 | 最大支持≥2台设备的堆叠，支持纵向虚拟化（提供第三方检测报告）； |
| 固定接口 | 24个万兆光端口，2个40G接口； |
| 产品实配 | 单台实配：双电源，双风扇，10GE光接口≥24，40GE QSFP+接口≥2，万兆多模光模块≥14； |
| 质保 | 原厂五年质保，中标后签订合同前提供原厂商质保承诺函。 |

1. **可信环境感知代理（1台）**

|  |  |
| --- | --- |
| 技术指标 | 设备技术要求 |
| 硬件性能 | ★Cpu≥28核 2.4GHz ; 内存≥256G ; 硬盘≥1TB；≥2个千兆业务电接口； |
| 客户端请求响应小于200ms |
| 支持≥5000终端在线，本次配置3000点终端授权。 |
| 要求可信环境感知系统与现有网络内终端安全系统联动。 |
| 功能要求 | 环境感知采集端支持windows、linux、中标麒麟国产化等操作系统； |
| 支持对终端进行标识，标识应具备唯一、永久、防篡改、不可伪造等特性，支持感知公安安全U盘、公安PKI\_UKey插拔； |
| 支持终端环境数据采集汇总、分析后统一上报环境感知服务，实现对终端可信环境的状态和变化的实时感知； |
| 可以通过定制开发和用户人像库对接，直接从人像库获取授权人照片进行对比。 |
| 支持漏洞风险感知：能够发现主机系统是否存在高危漏洞。 |
| 支持网络风险感知：具备对当前终端是否连接互联网、是否有无线网卡、是否开放共享服务、是否监听指定端口等网络变化进行风险性感知，对可疑行为实现日志审计并上报、告警和评估。 |
| 支持外设风险感知：具备对终端上外接新的设备的识别采集能力，并对新接入的外部设备进行风险感知分析，支持实时上报、告警和评估；具备对移动存储设备插拔、网络打印机输出、打开摄像头等外部设备变化进行风险感知分析，对可疑行为实现日志审计并上报、告警和评估。 |
| 支持安全配置感知：具备对windows主机的系统配置风险性感知，比如弱口令、权限变化、登陆注销事件、配置变更审计日志等进行风险感知，并对存在的风险项进行审计、上报、告警和评估；其中主要安全基线包括身份鉴别类、安全审计类、访问控制核心配置类、资源控制配置类、入侵防范类等。 |
| 支持恶意代码风险感知：具备对终端是否安装了防病毒软件以及从防病毒软件获得当前系统上存在的恶意代码风险；具备感知防病毒软件的病毒库的更新状态。 |
| 支持终端环境数据采集汇总、分析后统一上报环境感知服务，实现对终端可信环境的状态和变化的实时感知，对终端评分处理平均时间不超过60秒； |
| 支持应用环境风险感知：能够检测到终端运行了指定的非法应用程序，同时能够感知到是否没有运行指定的必备应用程序；能够检测到是否存在指定的非法服务，同时能够感知到是否不存在指定的合法服务；能够检测到是否存在指定的非法注册表项，同时能够感知到是否不存在指定的必备注册表项。 |
| 支持系统应用类风险感知：包括但不限于IE主页相关项目、IE菜单项、IE核心配置、IE外观配置、IE常规设置、IE浏览器图标配置、Internet选项、用户样式表、重置web设置、About协议、域名解析文件Hosts、常用文件关联项、磁盘及文件夹配置、系统常用组件、系统启动配置、系统图标配置、任务栏及开始菜单、系统重要服务组件、组策略、显示属性、Web桌面、网络驱动器、打印机设置、收藏夹快捷方式、桌面图标快捷方式、开始菜单快捷方式、桌面及资源管理器、快速启动栏快捷方式等项目；具备感知浏览器的安全级别和配置，具备感知浏览器的插件配置以及变化情况。 |
| 支持可信环境感知报告:具备感知要素和策略的定制化，比如感知要素选项、感知策略内容、感知风险等级、感知要素权重、综合评分规则、业务考核规则、执行频率等；支持可同时配置并执行多个感知策略。具备可信环境感知报告上报接口，能够根据根据接收到的终端实时环境数据、异步环境数据、历史环境数据，按照业务的安全要求对终端是否可信进行评估和分析，支持不同业务场景下生成不同的可信环境感知报告模板 |
| 支持级联部署、支持集群部署、支持国产化服务器部署，windows和国产化终端以及安可终端统一管理、支持国产数据库部署；支持主流windows系统部署、主流国产操作系统部署、支持安可操作系统部署、支持终端增量升级、支持与PKI证书联动 |
| ★支持主流windows系统部署、主流国产操作系统部署、支持安可操作系统部署、支持终端增量升级、支持与PKI证书联动 |
| 支持通过对终端运行的应用进行识别，可感知到应用程序的启动状态，启动目录等，并可将识别到的信息上报至控制中心； |
| 支持通过“可信加权”原则，对风险权值进行相加，根据不同权值或安全等级指定安全策略并下发控制服务； |
| 使用云桌面访问业务场景下，云桌面中环境感知客户端可以穿透云桌面获取物理机上环境感知客户端信息，包括是否安装环境感知客户端、物理机设备可信标识、物理机基本信息、物理机上感知结果。云桌面穿透适配华为、VMWare、深信服、H3C、升腾、锐捷。提供云桌面穿透适配的标准API，其他云桌面可根据API定制开发完成穿透适配。 |
| 支持具备自我保护功能和加密功能的，而且所有文件均是经过数据签名认证的，可有效保证客户端程序目录下的相关文件均是不可以被篡改、注入、拦截、恶意终止，保证客户端程序本身的可信； |
| 其他 | 原厂五年质保，中标后签订合同前提供原厂商质保承诺函。 |

**12、可信接入代理（2台）**

|  |  |
| --- | --- |
| **指标项** | **技术指标及参数** |
| 基本参数 | 冗余电源; ≥1T硬盘;标配≥6个10/100/1000电口，≥4个万兆SFP+光口插槽。 |
| 每台TAP支持最大并发用户数≥1000人，支持多台负载； |
| 单向加密吞吐≥5Gbps，HTTPS卸载吞吐量≥2.5G（100K页面），HTTPS并发连接数≥2.0万，每秒新建连接≥7000，请求时延小于500us； |
| 支持SM1、SM2、SM3、SM4国密算法 |
| 功能规格 | 设备联动：能够与可信环境感知系统形成联动，具备应用级动态访问控制。 |
| 请求代理转发：支持接收用户发送的访问请求，识别请求中的主体、客体，获取主客体标识， 并向可信代理控制服务发起动态授权判定请求，对授权通过的请求进行流量转发，实现令牌或 权限信息传递; |
| 单点登录：支持为后端应用传递身份和会话令牌实现单点登录，支持为遗留应用通过密码代填 方式实现单点登录； |
| 单点登出：支持与可信代理控制服务联动，当用户会话失效时，对用户实现单点登出； |
| 流量管控：支持对应用请求信息进行流量控制，支持基于请求内容大小、请求速度、请求连接数、访问时段、服务类型等参数进行流量控制； |
| 访问控制：支持接收应用访问请求并和可信代理控制服务联动进行访问控制策略判定，根据判 定结果进行控制，能够在主体环境安全状态变更时，强制撤销当前会话； |
| 二次认证：支持根据可信代理控制服务下发的指令，协同认证服务完成二次认证； |
| 数据转发时延≤100ms |
| 日志审计：记录策略执行日志、网络流量统计等信息，包括用户身份、终端信息、时间、目标 应用、流量等信息，并进行日志上报，便于实现对应用访问进行审计及安全风险分析； |
| 支持3台以上集群部署的负载均衡，以实现热备份，确保服务的高可用性。 |
| 支持IPv6协议栈、IPV6穿越技术、IPV6路由协议，支持IPv6 over IPv4 GRE隧道，6RD隧道，支持NAT66，NAT64 |
| 支持无法改造的应用零改造对接，支持无法改造的应用用户名密码自动代填； |
| 支持代理内置流探针，对网络中的流量进行采集，上送安全管理中心进行威胁分析；（提供页面截图） |
| 提供web防护，基于防护规则（数字签名）对WEB流量进行监控及过滤，防止SQL注入、XSS、溢出攻击，针对CC攻击提供独创session验证模式，高效验证正常访问/机器攻击)，提供相关截图。 |
| 服务要求 | 提供原厂商5年免费质保和软件升级服务 |

**13.负载均衡（2台）**

|  |  |
| --- | --- |
| 技术指标 | 设备技术要求 |
| 硬件及性能要求 | 采用Intel四核或以上CPU的硬件体系架构，必须支持超线程技术，独立的控制CPU。系统内存≥16GB |
| 单台设备配置2个冗余电源。电源模块为220V交流电源，电源需通过80plus认证 |
| 投标设备需配置，以确保系统镜像和日志等信息得到稳定和可靠的存储（需提供网站相关链接及截图，证明投标设备配置硬盘） |
| 支持热插拔智能风扇。能够对风扇工作状态进行监控，对异常状态通过管理界面进行自动告警。 |
| 必须是专业负载设备，非插卡式负载均衡设备。 |
| 最大的并发会话数≥2800万 |
| 四层每秒新建连接数（CPS）≥250,000 |
| 七层每秒新建连接数（1:1 CPS）≥280,000 |
| 四层最大吞吐量≥20Gbps |
| SSL CPS(ECDHE+ECDSA) ≥6500 |
| SSL CPS(RSA 2K) ≥10,000 |
| 需提供投标型号对应的官方网站相关参数链接及截图 |
| 品牌成熟度 | 要求投标产品为现有平台销售产品，并在官方网站上能找到对应的投标产品型号和详细技术参数（需提供网站相关链接及截图） |
| 功能要求 | 同一台设备提供四至七层的应用负载均衡功能，支持TCP/ UDP/ HTTP/ HTTPS/ SIP/ SMTP/ FTP等应用协议的负载均衡功能 |
| 支持一台物理设备虚拟不少于64个负载均衡模块功能授权，为不同应用系统部门提供独立管理负载均衡权限（需提供网站相关链接及截图） |
| 每个虚拟分区可单独定义ARP、路由、负载均衡等配置，每个实例的配置信息和管理互相独立。每个虚拟分区可限制资源使用，至少可以限制并发会话、L4新建连接数、吞吐量等。支持相同IP地址的服务器在不同虚拟分区的复用（需提供设备相关配置界面截图证明以上功能的实现情况） |
| 服务器负载均衡、链路负载均衡、全局负载均衡、Web应用防火墙、DNS防火墙的功能、抗DDoS、虚拟分区（Application Delivery Partition）功能需在同一物理设备内实现或开启。以上功能需同时处于激活可使用状态，无需额外购买相应授权。 |
| 支持以下负载均衡算法：轮询、最小连接、最小响应时间、加权轮询、加权最小连接、URL-Hashing等 |
| 管理界面提供基于某种编程语言（如TCL语言）自定义的流量控制方法，可通过自编程方式实现灵活的流量处理手段。支持负载均衡、DNS处理、用户认证、NAT、路由转发、会话保持等功能的可编程控制。（如支持，请详细描述提供的可编程语言、操作界面，需提供官方网站链接可查询详细说明） |
| 需提供TCP协议优化和应用加速功能，包括：TCP连接复用、HTTP压缩、URL Switching、HTTP Header Rewrite/Insert/Delete等，减轻服务器压力，提高客户端响应速度 |
| 需支持基于策略的负载均衡功能，提供基于ACL的静态/动态更新的黑白名单，限制恶意攻击源；同时，提供连接速率或应用请求速率限制，防止类似CC攻击行为 |
| 支持IPv4/IPv6双协议栈；支持IPv4/IPv6，IPv6/IPv4协议转换；支持IPv6动态路由；支持IPv6业务的高可用性及连接同步 |
| 标准配置需提供对RIPv1/v2、OSPF、ISIS、BGP路由协议的支持（需提供配置界面截图） |
| 支持以下服务器健康检查方法：ICMP、TCP、UDP、HTTP、HTTPS、FTP、SNMP等多种主动式服务器健康检查方法；支持基于脚本的健康检查方法。即：用户可自定义灵活的健康检查方式和检查内容，根据不同需求自行编制脚本。支持基于布尔表达式的健康检查方法 |
| 支持标准的DNS记录类型包括：A记录，MX记录，NS记录，PRT记录，SVR记录，CNAME记录，SOA记录，AAAA记录 |
| 设备同时提供Telnet/SSH/HTTP/HTTPS等多种协议方式进行管理 |
| 支持中文WEB管理界面（需提供系统操作界面截图） |
| 提供全面的API接口，无软件开发语言限制。（需提供网站相关介绍链接及截图） |
| 设备自身提供实时的抓包工具，可远程登录设备，运行其自身提供的实时抓包工具，可以对通过自身设备的数据包进行过滤并抓包分析。能够实时显示抓包信息。抓包结果可以导出为标准的文件格式，并可以用通用的分析工具，如Sniffer, WireShark等工具打开。（需提供实时显示抓包信息及抓包文件可保存导出两项功能的截图） |
| 系统需支持与Openstack联动，支持NVGRE和VxLAN技术 |
| 支持多虚一虚拟机框功能，最少支持八台同型号硬件虚拟为一台负载均衡系统功能 |

**14.web应用防火墙（2台）**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 资质 | 通过公安部检测并获得公安部计算机信息系统安全专用产品销售许可证产品具备国家信息安全测评信息技术产品安全测评证书（EAL3+）产品具备WEB应用防火墙认证证书 |
| 规格 | 标准2U专用千兆硬件平台 |
| 网口数量 | 2千兆电口管理口，千兆业务电口\*4（含2组硬件BYPASS模块），千兆业务光口\*4，万兆业务光口\*2 |
| 性能参数 | 应用吞吐量不小于8GbpsHTTP并发连接不小于400000HTTP新建连接(CPS)不小于40000 |
| 部署方式 | 透明桥部署：防护口不占用IP地址，实现完全透明部署，无需以先终结用户的TCP会话后再发起新的TCP会话到服务器方式处理，并支持路由不对称场景 |
| 透明代理部署：防护口不占用IP地址，实现应用层透明部署，支持TCP连接复用，并优化服务器会话处理改善服务器处理性能 |
| 端口镜像部署：镜像服务器流量即可实现安全审计和告警 |
| 反向代理部署：可支持代理和路由牵引两种模式，客户端源IP可采用透明和非透明两种转发机制，非透明可指定字段进行识别，支持前后端口分离，支持多台WAF设备冗余和集群部署 |
| 支持虚拟化部署，支持KVM、Xen、VMWare等虚拟机环境，并支持WAF镜像导入 |
| 支持链路聚合，提升网络带宽、增加容错性和链路负载均衡 |
| 支持VLAN子接口，业务口可承载多个VLAN通道 |
| 高可用性 | 支持全透明集群模式、主-主模式、主备模式、硬件BYPASS、软件BYPASS |
| 保护对象 | 支持多条链路数据的防护，防护网段数量不限 |
| 支持以域名和IP多种方式进行防护 |
| 支持ipv4/ipv6双协议栈 |
| WEB服务自发现 | 支持WEB站点服务自动侦测功能，支持自动识别VLAN信息，提供界面截图 |
| 防御功能 | 能够识别恶意请求含：跨站脚本(XSS)、注入式攻击（包括SQL注入、命令注入 、Cookie 注入、代码注入、LDAP注入、SSI注入文件注入等）、跨站请求伪造等应用攻击行为 |
| 支持对HTTP请求分割攻击和HTTP响应报文截断攻击的防护 |
| 能够识别服务端响应内容导致的缺陷：敏感信息泄露、已有的网页后门、错误配置、目录浏览等缺陷 |
| 能基于访问行为特征进行分析，能识别盗链、爬虫攻击的能力 |
| 能识别网站中的网页木马程序，通过策略可防止木马网页被用户访问 |
| 内置主流Webshell特征库，对上传内容进行检查，防止恶意Weshell上传 |
| WAF能自动识别扫描器的扫描行为，并智能阻断如Nikto、Paros proxy、WebScarab、WebInspect、Whisker、libwhisker、Burpsuite、Wikto、Pangolin、Watchfire AppScan 、N-Stealth、Acunetix Web Vulnerability Scanner 等多种扫描器的扫描行为 |
| 内置开源CMS漏洞和WEB服务器插件漏洞防护规则 |
| 支持阻断提交政冶敏感、违反法规相关的言论信息 |
| 支持丰富的自定义规则，可以针对多个条件组合，形成深度的WEB防护规则 |
| 支持服务器隐藏，可配置删除服务器响应头信息 |
| 内置身份证、银行卡等服务器敏感信息库，对服务器响应敏感内容进行隐藏，并支持自定义，提供界面截图并加盖公司公章 |
| 支持Cookie安全机制，支持Cookie自学习，防止Cookie被篡改和劫持，并支持Cookie Httponly |
| 智能自学习功能 | 支持网站自学习建模功能，能通过自学习形成网站URL树；通过自学习能生成安全防护策略；通过自学习能发现参数的名称、类型、匹配频率；可配置匹配到自学习特征后放行；可配置匹配不到自学习特征直接阻断请求；提供界面截图 |
| 智能攻击者锁定 | 支持智能识别攻击者，对网站连接发起攻击的IP地址进行自动锁定禁止访问被攻击的网站可配置攻击者识别策略和算法可配置攻击者锁定时间可配置将攻击者直接加入网络黑名单可展示攻击者发生的时间和攻击者所在的地理位置提供界面截图 |
| 基于时间的访问控制 | 可基于时间对客户端IP进行黑白名单控制提供界面截图并加盖公司公章 |
| 防御动作 | 针对触发安全规则的行为进行阻断并发出告警页面 |
| 告警页面支持重定向至其它URL |
| 能将攻击者列入网络黑名单进行网络阻断该IP的访问 |
| 对攻击报文丢弃 |
| WEB访问行为合规 | 可实现访问流程的校验，向网站提交表单前必须先访问指定的网页，并等待可配置的时间长度后才能正常提交表单， |
| CC防护功能 | 可根据URL、请求头字段、目标IP、请求方法等多种组合条件对CC攻击进行检测，检测指标为URL访问速率和URL访问集中度；可根据IP、IP+URL和IP+User\_Agent等算法对客户端进行检测，并支持应用层字段解析和自定义检测字段功能，支持挑战模式，支持基于地址位置的识别，支持对特定的IP地址进行CC规则白名单放行，支持CC慢攻击防护，通过学习业务流量模型，在业务流量异常时开启CC防护，并支持启动配置阈值， |
| 篡改监控 | 系统提供防篡改功能，能够防止被篡改内容被浏览者访问到,一旦检测到被篡改，实时发送告警信息给管理员。 |
| 安全审计 | 能详细记录攻击事件的HTTP请求头信息，含请求的URL、UserAgent、POST内容，cookie等所有的请求头内容 |
| 能详细记录服务器响应头信息，服务器响应内容 |
| 日志分析 | 根据产生的安全日志进行智能分析，提高人工分析效率，减小规则误判概率 |
| 报表 | 根据PCI-DSS要求，对用户的应用进行合规性评估，生成合规报表 |
| 支持自定义报表、定时报表、支持各类导出格式（WORD,PDF等） |
| 报表可自动发至管理员邮箱 |
| 告警方式 | 支持Syslog、手机短信、邮件等多种告警方式 |
| 访问审计 | 具备审计网站正常访问流量的能力，提供按小时，日期、月份生成报表 |
| 能记录、查询所有用户对网站的访问情况 |
| 能分析出访问量最大的URL，IP地址 |
| 能分析出访问流量最大的文件类型 |
| SSL透明代理 | 支持HTTPS服务器的防护，可支持第三方认证机构颁发的证书链，WEB应用防火墙前端与后端均为HTTPS加密链路，实现HTTPS应用系统的防御 |
| 支持对HTTPS站点上传的公钥、私钥、证书链的内容格式进行检查，同时自动检测公钥和私钥是否配对、公钥和证书链是否配对，避免无效证书引起的业务不通的问题 |
| 一个保护站点支持上传多个域名证书 |
| 可以选择需要支持的SSL/TLS协议版本 |
| 部署在SSL网关后面，能够解析到真实的访问者IP，并能对真实的IP进行防护和阻断 |
| 设备管理 | 配置变更时不影响在线业务 |
| 规则库支持手工、在线升级两种方式，在线升级可支持规则定时检查新版本和在线更新，确保WAF能够针对新型的、突发型的Web攻击进行防护 |
| 支持HTTPS方式进行设备管理 |
| 设备管理采用管理员与审计员分离 |
| 操作界面支持全中文界面 |
| 支持LDAP认证 |
| 支持标准网管 SNMPv3，并且兼容SNMP v1和v2c |
| 支持NTP时间同步 |

**15.超融合虚拟化平台（3台）**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 数量要求 | ▲本项目要求≥3台超融合虚拟化服务器 |
| 单台配置 | CPU：INTEL Gold 5220性能以上\*2、内存≥512G、千兆网口≥4个、万兆光口≥2个，配置4个万兆光模块，冗余双电源；本项目要求至少配备1块≥128G SSD硬盘、2块≥800G SSD硬盘和≥80T的SATA硬盘裸容量，支持raid。 |
| 云管理平台技术要求 | ▲本次项目提供1套虚拟化云平台管理授权 |
| 支持多集群管理，支持不低于2000台云主机的管理规模 |
| 提供用户自助服务界面，用户能够通过自助服务门户完成虚拟机的查看、申请、使用、修改、销毁等操作。 |
| 支持工单功能，用户通过工单可以向云管理员反馈云资源使用所遇到的问题；支持多租户划分，平台管理员能够为不同的租户分配CPU、内存、存储等资源配额； |
| 提供统一的镜像管理功能，实现各个可用区上镜像的统一创建和管理，可实现一键快速生成云主机，要求可提供网络设备镜像，方便快速的部署虚拟化安全的组件；  |
| 云资源的申请需要通过管理员审批方可使用，云操作系统支持多级审批流程，可以根据用户实际组织进行自定义； |
| 云平台具备对资源池中CPU、网络、磁盘使用率等指标进行实时的数据统计功能，并提供报表功能； |
| 支持业务整体可靠性指标的集中展示，包括业务可靠性、平台可靠性和硬件可靠性，方便管理员能直观地掌握整个数据中心的可靠性状态。 |
| 提供符合Openstack的API，满足集成或者二次开发的需求。 |
| 服务器虚拟化及管理 | ▲本次项目提供6个物理CPU服务器虚拟化管理授权 |
| 支持配置动态资源扩展功能，系统支持自动评估虚拟机的性能，当虚拟机性能不足时自动为虚拟机添加CPU和内存资源，确保业务持续高效运行 |
| 虚拟化内核基于开源软件KVM底层开发或兼容VMware、KVM等主流虚拟化软件，提供证明。 |
| 支持在本地管理平台实现对VMware vCenter中的虚拟机备份，并能够在超融合的平台实现VMware虚拟机的启动恢复； |
| 支持双向迁移，可将VMware虚拟机在运行状态下迁移到超融合平台上，也可将超融合平台上的虚拟机在运行状态下迁移到VMware vCenter的集群中，迁移最后阶段业务会中断,可选择自动或手动拉起； |
| 支持虚拟机的HA功能。当物理服务器发生故障时，该物理服务器上的所有虚拟机，可以在集群之内的其它物理服务器上重新启动，保障业务连续性。 |
| 支持在线的带存储的虚拟机迁移功能，可以在不停机状态下和非共享存储的环境中，实现虚拟机在集群内的不同物理机上迁移，保障业务连续性。 |
| 支持IO重试，当存储出现故障，导致虚拟机无法读取存储数据时，自动挂起虚拟机，避免业务故障。 |
| 支持虚拟机的无代理备份，能提供至少100个虚拟机的高性能备份功能，支持至少10T的备份数据容量的许可，可将直接将虚拟机备份到磁盘，并支持生成全新虚拟机的方式进行恢复 |
| 管理平台不依赖于某一个虚拟机或物理机部署，采用分布式架构保障平台更可靠 |
| 支持对平台虚拟机的精细化权限管理，可根据单个虚拟机开关机、打开控制台、删除等操作设定不同的权限，管理员也可以根据用户需求合理分配权限。 |
| 支持平台中的集群资源环境一键检测，对硬件健康、平台底层的虚拟化的运行状态和配置，进行多个维度进行检查，提供快速定位问题功能； |
| 虚拟机平台须支持主流的X86架构的操作系统，包括Windows， Redhat、SUSE、CentOS、麒麟等OS； |
| 存储虚拟化 | ★本次项目提供6个物理CPU存储虚拟化管理授权，要求存储虚拟化授权无容量限制。 |
| 支持存储虚拟化功能，无需安装额外的软件，在一个统一的管理平台上使用License激活的方式即可开通使用，存储虚拟化与计算虚拟化为紧耦合架构，减少底层开销，提升性能。 |
| 采用分布式架构设计，由多台物理服务器组成分布式存储集群，通过新增物理服务器可以实现存储容量和性能的横向扩展，扩容过程保证业务零中断。 |
| 支持标准的iSCSI协议，允许外部物理主机或应用通过标准的iSCSI接口访问虚拟存储，实现Server SAN和IP SAN的融合，能够使存储资源的利用率发挥到最大价值。在iSCSI接入场景下支持内部负载均衡和高可用。 |
| 支持磁盘坏道检测功能，虚拟存储集群可以对数据盘进行坏道检测，发现坏道后可自动从另外一个副本读取数据，并对坏道数据进行修复。 |
| 当磁盘或者存储节点故障时系统能自动进行数据重构，在无人工干预的条件下，数据重构速度每TB<30分钟，提供证明材料； |
| 支持多副本冗余功能，支持2个或以上副本，副本互斥地保存在集群的不同节点，当1个或多个主机或者磁盘故障，确保数据依旧正常访问。 |
| 网络虚拟化 | 本次项目提供6个物理CPU服务器虚拟化管理授权 |
| 支持对oracle、sqlserver、Weblogic数据库及中间件监控，实现对数据库的语句的故障定位排错，执行时延分析。 |
| 分布式防火墙能够基于虚拟机进行3-4层安全防护，以虚拟机为单位的安全策略部署，即使改变虚拟机的IP地址信息，安全策略依然生效；分布式防火墙提供实时拦截日志显示，以及支持“数据直通ByPass”功能，方便出现问题快速定位问题。 |
| 通过License激活的方式，实现网络虚拟化功能（支持分布式虚拟交换机、虚拟路由器、虚拟应用防火墙、虚拟化运维堡垒机等功能），支持Vxlan网络和现有的Vlan网络对接，实现虚拟化平台与原有网络的兼容性。 |
| 虚拟路由器支持HA功能，当虚拟路由器运行的主机出现故障时，可以实现故障自动恢复，保障业务的高可靠性 |
| 在管理平台上可以通过拖拽虚拟设备图标和连线就能完成网络拓扑的构建，快速的实现整个业务逻辑，提供虚拟路由器、虚拟交换机等设备的连通性探测功能，方便在虚拟化环境中，进行相应的故障排除和恢复，能够定位到出现故障的虚拟网络设备，并且能够排查到acl策略配置错误等层面。 |
| 产品资质 | 厂商提供的软件或者系统都是厂商自研，非OEM或者采用第三方的产品，要求服务器虚拟化、存储虚拟化、网络虚拟化为同一品牌，并且分别提供相应组件软件著作权。 |
| 其他要求 | 1、提供5年7\*24小时原厂售后服务。2、所投产品要求提供五年原厂免费质保和软件升级服务； |

**16.虚拟化集群交换机（2台）**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 交换性能 | 交换容量≥2Tbps，包转发率≥700Mpps，（若官网存在双指标，以较小为准）；双风扇，双电源； |
| 堆叠特性 | 最大支持≥2台设备的堆叠，支持纵向虚拟化（提供第三方检测报告）； |
| 固定接口 | 24个万兆光端口，2个40G接口； |
| 产品实配 | 单台实配：双电源，双风扇，10GE光接口≥24，40GE QSFP+接口≥2，万兆多模光模块≥14； |
| 质保 | 原厂五年质保，中标后签订合同前提供原厂商质保承诺函。 |

**17.可信代理控制服务（1台）**

|  |  |
| --- | --- |
| **指标项** | **技术指标及参数** |
| 基本参数 | 标配冗余电源（550W）；内存≥128G，≥1T硬盘；≥4\*千兆电口; ≥2个万兆光口。 |
| 最大并发用户数≥1000，每秒新建连接数≥7000 |
| 每秒权限判定数QPS≥3000；支持集群部署，QPS线性可扩展； |
| 支持SM1、SM2、SM3、SM4国密算法； |
| 备用设备要求 | ▲为确保系统高可用性和稳定，在5年服务期内，本次项目要求在用户现场提供相同型号的可信代理控制服务备用设备一台，设备产权归原厂商所有。 |
| 功能规格 | 支持短信验证码、邮箱验证码方式认证；额外支持指纹、人脸等； |
| 支持LDAP、RADIUS、POP3、SMTP、IMAP、HTTP、HTTPS第三方协议认证方式；支额外持kerberos协议； |
| 支持MYSQL、SYBASE、SQL-SERVER、ORACLE、DB2数据库认证方式； |
| 支持可信接入（应用）代理集群的统一管理，统一配置管理维护。 |
| 支持可信（应用）API代理集群的统一管理，统一配置管理维护。 |
| 支持提供应用、API等集中管理和鉴权，提供截图证明； |
| 支持运用缓存技术，提高鉴权性能，以支撑大用户量高并发访问，提供截图证明； |
| 支持通过Web界面对用户、应用的角色进行管理，支持对角色的分配； |
| 权限管理联动：支持与权限管理联动，获取应用、API、运维的权限列表; |
| 权限变更订阅：支持订阅授权服务的权限变更服务，实时获取最新权限; |
| 权限判定：支持为可信接入代理、可信API代理、可信运维代理提供实时的访问权限判定; |
| 会话管理：支持为可信接入代理、可信API代理、可信运维代理提供集中的代理连接会话管理; |
| 风险感知和分析：支持和终端环境感知、行为分析等风险分析平台联动，实时接收风险通报， 并结合代理会话状态、权限列表、访问日志等信息进行综合分析，实时变更权限，实时撤销风 险会话; |
| 风险联动通报：支持将风险和异常信息通报给认证服务。 |
| 集中配置管理：支持对可信接入代理、可信API代理、可信运维代理进行集中配置及配置更改等; |
| 日志审计：提供用户登陆日志、用户操作日志、系统运行日志等信息采集、管理及审计，并支持日志服务器上报。 |
| 高可用性：支持通过负载均衡、集群部署等形式，确保认证服务的持续可用; |
| 公安PKI CA证书双向认证 | 支持可信CA导入/导出管理，支持PEM/DER/PCKS7证书格式导入；支持双向证书认证机制；提供证书过滤、用户/组织关系、用户名+证书多重认证开启功能 |
| 云桌面适配 | 要求支持本次项目云桌面系统联动。 |
| 服务要求 | 提供原厂商5年免费质保和软件升级服务 |

**18.可信API代理（2台）**

|  |  |
| --- | --- |
| **指标项** | **技术指标及参数** |
| 基本参数 | 冗余电源，CPU性能≥ Intel（R）Core（TM）i5-2400CPU@3.10GHz，内存≥8G，硬盘≥1T，≥6个千兆电口。支持软件化部署。 |
| 支持集群扩展；支持HTTP/HTTPSAPI数量≥100; |
| 加密吞吐≥5Gbps，最大并发连接数≥50000，RPS≥40000；支持SM1、SM2、SM3、SM4国密算法，SM2签名（次/秒）≥12600,SM2验证（次/秒）≥4500,SM2密钥对生成（tps）≥10000，SM1加密/解密≥1Gbps，SM4加密/解密≥4Gbps |
|  | 请求代理转发：支持接收应用发起的API访问请求，识别请求中的主体、客体和操作并向可信代理控制服务发起授权请求；支持对授权通过的请求进行流量转发，并实现令牌或权限信息传递； |
| 流量管控：支持对应用请求信息进行流量控制，支持基于请求内容大小、请求速度、请求连接数和访问时段等参数进行流量控制，支持监控被保护应用的流量状态，分析流量异常，支持实时流量监控、历史流量监控。 |
| 熔断机制：支持对API调用启用超时熔断机制，提供主动熔断和被动熔断；支持多维度检查项，检查项可配置，包括：错误率、失败次数、超时时间、并发数；对于以熔断的服务进行自动检测，满足上线要求，自动上线； |
| 访问控制：代理平台具备动态的访问控制执行能力。当API调用者的主体环境发生变化时，代理平台可接收可信访问控制服务提供者的策略更新通知并执：当前API调用者被服务提供者判定为存在安全威胁时，代理平台将终止当前的API访问会话；当API调用者被判定为安全认证强度不足时，代理平台将通知认证服务提供者对当前API调用者进行强制的二次认证。当API在一定时间内未使用后，代理平台将终止当前的API访问会话，若再次使用，再次对行API使用者进行身份认证。 |
| 日志审计：支持记录API授权日志、网络访问流量统计等信息，包括用户身份、终端信息、时间、目标应用及接口、流量等信息，并进行日志上报，便于实现对API访问进行审计及安全风险分析； |
| 通道安全：支持通过国密SSL协议对业务流量进行加密，对应对保存国密SSL证书进行保护； |
| 高可用性：支持通过负载均衡或集群扩展的形式，确保服务的持续可用。支持3台以上集群部署，提供3台以上实际部署证明材料。 |
| 感知联动：系统与可信环境感知系统形成联动，根据可信环境系统评估可信分进行业务授权，支持屏蔽业务系统内部的功能，避免系统内部的重要业务暴露到外部网络。 |
| 支持适应不同的业务系统，提供多种策略方式，保护不同架构、不同开发方法的系统，包括：内容重写、重定向重写、自定义脚本文件等。 |
| 高可用性：支持通过负载均衡或集群扩展的形式，确保服务的持续可用。 |
| 支持API的“零”改造，实现SSL卸载和认证授权； |
| 支持API治理、注册、流量控制、负载均衡、健康检查； |
| 提供基于HTTP/HTTPS协议的API的认证和保护，可以满足用户对基于密码学的高强度身份认证安全需求； |
| 支持BASIC认证方式、CA数字证书的双向认证，一次一密OIDC令牌等认证方式； |
| 支持证书和IP的黑白名单； |
| 可以设置单IP最大连接数，保护API不会被DDOS攻击。支持采用⾮对称加密技术，对API的数据进⾏签名，来防⽌数据篡改以及重放攻击，需提供截图证明； |
| 支持对当前API服务端提供安全防护能力，可对API使用中常见的网络安全攻击进行感知和识别，包括SQL注入，XSS攻击，目录遍历，CC攻击，PHP注入，网站扫描，敏感信息访问，以及异常的访问请求等，提供产品相关证明材料 |
| 提供业务系统前置API访问日志、API访问流量统计等信息，并进行日志上报、日志外发，便于实现业务数据的审计、安全风险的分析。提供的存储空间支持审计日志本地留存6个月以上。 |

**19.日志审计设备（1台）**

|  |  |
| --- | --- |
| 技术指标 | 设备技术要求 |
| 硬件指标 | 事件采集≥10000EPS，事件处理最高≥3000EPS。硬件规格：标准机箱，≥4个千兆电口，2个扩展插槽（可选2万兆光、4千兆电、4千兆光），1个Console接口，单电源。包含100授权节点，包含5年标准维保。 |
| 内置存储总容量≥4TB，支持外接存储设备。产品要求支持SOC产品的硬盘减震技术，第三方检测报告。 |
| 部署模式 | 支持单一部署，也支持分布式部署。 |
| 使用模式 | 采用B/S模式，无需安装客户端，使用WEB浏览器访问管理中心，浏览器端无需安装Java运行环境。支持chrome浏览。 |
| 管理范围 | 能够对企业和组织的IT资源中构成业务信息系统的各种网络设备、安全设备、安全系统、主机操作系统、虚拟化、云计算、数据库、中间件以及各种应用系统的日志、事件、告警等安全信息进行全面的审计。 |
| 审计对象 | 支持审计各种网络设备（路由器、交换机等）配置日志、运行日志、告警日志等；支持审计各种安全设备（防火墙、IDS、IPS、VPN、防病毒网关，网闸，防DDOS攻击，Web应用防火墙、等）配置日志、运行日志、告警日志等；支持审计各种主机操作系统（包括Windows,Solaris, Linux, AIX, HP-UX,UNIX,AS400）配置日志、运行日志、告警日志等；支持审计各种数据库（Oracle、Sqlserver、Mysql、DB2、Sybase、Informix）配置日志、运行日志、告警日志等；支持审计各种中间件（tomcat、apache、webshpere、 weblogic等）配置日志、运行日志、告警日志等；支持各种应用各种应用系统（邮件，Web，FTP，Telnet、等）配置日志、运行日志、告警日志等；以及用户自己的业务系统的日志、事件、告警等安全信息进行全面的审计。 |
| 采集方式 | 支持通过syslog、SNMP Trap、JDBC、Agent代理、WMI、(S)FTP、NetBIOS、文件\文件夹读取、Kafka等多种方式完成各种日志的收集功能； |
| 资产管理 | 能够将资产按照多种维度进行分组、分域管理，如地理位置、组织结构、业务系统等，提供便捷的添加、修改、删除、查询与统计功能；支持资产信息的批量导入和导出，便于安全管理和系统管理人员能方便地查找所需设备资产的信息，并对资产进行CIA赋值，自动计算资产价值，设置等保等级；在资产管理界面可查看每个资产的属性信息，情境信息，本身产生的事件信息、关联告警信息；支持对资产IP地址的地理信息进行管理，支持单个IP、IP段设置行政区及经纬度，支持地图显示（截图证明）。 |
| 日志统计分析 | 1） 可自定义统计场景，统计的字段条件和时间段以及过滤器等可自由设定；2） 支持柱状图、饼图、折线图、面积图、堆积图、环状图、数值图、地图等形式的统计信息可视化展示，并可将统计结果保存为仪表板和报表等。图表数据支持数据下钻。3） 支持将统计结果保存为仪表板、报表和策略（提供截图）。 |
| 告警管理 | 1） 告警规则可以自定义，告警可查询，支持列表和统计展示；2） 告警支持提供告警统计策略，选中某条策略，就能展示某个统计图表，支持柱图、饼图、曲线图等统计展示形式；3） 支持告警归并，有效抑制重复告警，归并规则可自定义；4） 系统自带4中告警分类场景：外部威胁、外连威胁、横向攻击、自身告警 |
| 系统认证 | 产品内部的各个组件之间通信都支持加密传输，浏览器访问管理中心支持HTTPS； |
| 服务 | 原厂五年质保，中标后签订合同前提供原厂商质保承诺函。 |

**20.堡垒机（1台）**

|  |  |
| --- | --- |
| 技术指标 | 设备技术要求 |
| ▲硬件规格 | 采用专用千兆多核硬件平台和安全操作系统，标准机架式，≥2个千兆电口,16G内存，内置≥4TB硬盘，单电源，最大支持150路图形会话或500路字符会话并发，配置300个授权许可。含五年标准售后服务。 |
| 物理旁路，逻辑串联模式，不影响原有网络架构 |
| 功能要求 | 具备用户集中管理功能，能够依据系统功能模块灵活的创建用户角色，实现系统分权管理； |
| 支持多种身份认证方式（动态令牌、手机令牌、域认证）、密码防暴力破解、用户登陆来源（IP、MAC限制）控制，提升用户帐号安全性； |
| 能够统一管理IPv4、IPv6环境下的各类资源，包括主机、网络设备、安全设备、数据库等，并能够自动同步华为云、阿里云、腾讯云等公有云资产；须提供功能界面截图证明； |
| 支持通过应用发布的方式集中管控BS、CS资源，多台应用发布服务器间支持负载均衡功能（无需第三方负载均衡设备），以此满足高并发场景下的接入需求； |
| 支持依据用户、资源及系统账号属性进行访问授权，其中属性可由管理员自定义，实现访问权限的灵活管理；须提供功能界面截图证明； |
| 支持H5方式访问目标资产（字符、图形协议均支持），无需在操作终端安装任何插件即可使用堡垒机。 |
| 支持字符、图形、数据库、文件传输操作审计，方便事后追踪溯源、满足合规建设要求，针对审计记录支持多关键字检索、多条件组合查询、查询结果合并审计功能，便于管理员快速定位相关操作；须提供功能界面截图证明； |
| 支持主机、网络设备系统账号密码自动修改功能，针对修改后的密码支持分段保管功能，同时具备密码工单用于普通用户临时申请密码，过期后自动修改实现一事一密的应用效果；须提供功能界面截图证明； |
| 支持对剪切板、磁盘映射、sftp文件传输进行集中控制审计，其中针对windows剪切板支持文件、文字单独控制（如禁止传输文件允许传输文字），以满足运维、安全管控需求；须提供功能界面截图证明； |
| 支持内置动态令牌认证和手机令牌认证，其中动态令牌支持国密算法加密，需提供认证厂商相应令牌《商用密码产品型号证书》及相应授权函； |
| 具备先进的审计技术，实现数据库及字符操作的精准记录，提供国家权威机构出具的证明文件； |
| 其它 | 原厂五年质保，中标后签订合同前提供原厂商质保承诺函。 |

## 21.防火墙

|  |  |
| --- | --- |
| 技术指标 | 设备技术要求 |
| ▲架构及性能要求 | 系统要求为下一代防火墙产品 |
| 网络处理能力≥20G，并发连接≥600万，每秒新建连接≥20万/秒，冗余电源。 |
| 配置≥4个10/100/1000M自适应电口，≥4个千兆SFP光口插槽，≥4个万兆SFP+光口插槽。需配置入侵防护及网络防病毒模块，提供五年硬件维保及规则库升级服务。 |
| 部署模式 | 支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求。支持旁路模式； |
| 路由协议 | 所投产品必须支持静态路由、策略路由及动态路由。策略路由支持用户自定义其优先级，动态路由应至少支持RIP、OSPF、BGP、等路由协议；  |
| 地址转换 | 所投产品必须支持全面的NAT转换配置，包括一对一，一对多，多对一的源、目的地址转换，并至少支持FULL\_CONE模式和SYMMETRIC模式 |
| IPV6支持 | 所投产品必须支持IPv6协议栈、IPV6路由协议；支持IPv6下静态路由及策略路由、动态路由，动态路由应包括RIPng、OSPFv3、BGP4+ |
| 高可靠性 | 所投产品必须支持路由模式、透明模式的HA高可靠性部署，可工作于主备、主主模式，会话、用户、配置可实时同步；  |
| 访问控制 | 所投产品必须支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN等多种方式进行访问控制。 |
| 入侵防御 | 所投产品必须支持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL注入、WEB攻击等六种分类；漏洞防护支持日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于FTP、HTTP、IMAP、POP3、SMB、SMTP等应用协议的漏洞防护，系统必须具备一种基于网络的入侵检测方法。 |
| 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能；（提供功能截图） |
| 病毒防护 | 所投产品必须能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀 |
| 病毒库数量≥500w |
| 所投产品必须支持基于MD5的自定义病毒签名；支持设置例外特征，对特定的病毒特征不进行查杀 |
| VPN功能 | 支持IPSec、L2TP、GRE VPN，能够对相应VPN隧道报文进行监控统计 |
| 网络异常感知 | 所投产品必须支持统计网络内威胁事件的数量及对应的风险等级；支持查看详情并自动显示关联日志；可基于网络连接、应用名称、威胁事件处置威胁事件；  |
| 安全事件分析 | 所投设备必须支持基于网络活动，威胁活动、阻止活动等多维关联统计及分析，发现异常行为 |
| 运维管理 | 产品支持三权分立管理，具有独立审计用户，支持标准Syslog日志审计方式，支持Syslog端口自定义；开放RESTCONF，NETCONF等北向接口，对接第三方的管理平台； |
| 服务 | 原厂五年质保，中标后签订合同前提供原厂商质保承诺函。包含五年IPS/病毒防护特征库升级 |

**22.APT检测探针**

|  |  |
| --- | --- |
| 技术指标 | 设备技术要求 |
| 架构及性能要求 | 吞吐量≥3Gbps; 冗余电源，标准配置1个10/100/1000M专用管理接口，1个Console口，≥4个千兆电口、≥2个千兆SFP光口、≥2个万兆SFP+光口； |
| HTTP最大并发数≥10万/秒；邮件处理数≥200万封/24小时；文件检测≥10万个/24小时 |
| 提供五年全功能特征库升级服务及硬件维修服务。 |
| 支持通过流量镜像的方式旁路部署在数据链路中，实现网络流量数据采集、威胁检测和日志外发，支持通过重置会话的方式阻断TCP威胁会话连接，支持通过流量被动识别资产。 |
| 审计协议 | 支持解析HTTP、FTP、SMTP、POP3、SMB、IMAP、DNS、Mysql、MSSQL、DB2、Oracle等协议报文，并提供审计协议类型的端口号配置，可根据需要变更端口号，并支持LDAP登录行为识别、VXLAN镜像流量解析检测及HTTPS流量解析能力 |
| 检测风险类别 | 支持检测WEB攻击、异常访问、恶意文件攻击、C&C IP/URL、WEB后门访问、发件人欺骗、邮件头欺骗、邮件钓鱼欺骗、邮件恶意链接、DGA域名请求、SMB远程溢出攻击、WEB行为分析等风险（提供截图证明） |
| 告警黑白名单过滤 | 支持对文件白名单、发件人邮箱白名单、发件人域名白名单、黑域名白名单、黑IP白名单、域名白名单、客户端IP白名单、服务端IP白名单、WEB风险特征白名单进行设置 |
| 弱口令风险检测 | 支持对Telnet、FTP、POP3、SMTP、IMAP等协议进行弱口令检测 |
| 主机威胁分析 | 可自动对内网主机进行威胁指数分析，详细展示具体的威胁指数、威胁活动、历史威胁指数、遭受的攻击类型、攻击次数、攻击状态等 |
| 可根据不同威胁指数的主机实现攻击溯源和攻击过程的可视化分析 |
| 木马回连分析 | 快速识别网络中存在的恶意回连行为，包含回连主机IP、服务器IP、时间、行为等，对基于木马回连的非法数据传输等行为进行取证分析 |
| HTTP解析 | 支持 HTTP协议解析，检测WEB攻击 |
| 双向审计 | 支持双向审计，对请求和响应都进行审计 |
| 攻击检测 | 支持SQL注入、命令注入、跨站脚本、代码注入、协议错误攻击检测 |
| WEBSHELL检测 | 支持WEBSHELL检测，可检测访问webshell的行为，包含具体对应的URL、返回码、返回数据包内容等 |
| 动态分析 | 自动关联行为分析的详细展现，包含SQL注入取数据、表单破解、XSS测试、目录穿越读取文件、多人访问Webshell、APT攻击等 |
| 场景化分析 | 支持场景化的分析能力，对发现的告警进行二次关联，支持对勒索病毒、网站后门、邮件APT攻击等事件进行预警。 |
| 解析协议 | 支持解析webmail、SMTP、POP3类型报文 |
| Webmail攻击检测 | 支持基于webmail攻击类型检测，包括sql注入、跨站、命令注入等攻击检测 |
| 社工类攻击检测 | 对社工类攻击进行检测，检测内容包括：邮件头欺骗、邮件发件人欺骗、邮件钓鱼欺骗、邮件恶意链接 |
| 恶意附件检测 | 支持邮件恶意附件行为检测 |
| 解析协议 | 支持 HTTP、FTP、SMB、SMTP、POP3等协议传输文件检测 |
| 文件类型 | 支持doc, xls, ppt, swf, pdf, java, rar, zip, rar, exe, vbs, scr, html，js等多种文件解析,支持自定义文件类型 |
| 特征检测 | 对文件进行特征匹配，利用已知的特征库发现恶意可以执行代码对文件进行特征匹配，利用已知的特征库发现恶意的非可执行文件 |
| Shellcode检测 | 通过分析文件中的二进制代码，找到文件溢出攻击的代码，并能找到APT攻击中的0day攻击 |
| 兼容性要求 | 要求APT与项目内态势感知系统可以进行数据分析联动 |
| 质保 | 原厂五年质保，中标后签订合同前提供原厂商质保承诺函。 |

**23.云网安全分析系统**

|  |  |
| --- | --- |
| 技术指标 | 设备技术要求 |
| 流量采集与外发 | 支持纯软件化部署，提供自动化部署、远程推送部署、图形化部署等快速安装形式，并提供部署向导，以减少人工部署成本 |
| 支持从云平台底层计算节点处采集流量，无需在虚拟机中植入客户端，无需在核心交换机旁路镜像，无需通过SDN引流的方式实现 |
| 支持云平台自定义流量采集规则策略，可针对不同计算节点、租户、项目、子网、虚拟机进行自定义流量采集（提供相关功能截图） |
| 支持对已采集到的云网流量通过GRE/VXLAN等隧道封装协议进行外发，可针对不同的物理计算节点、租户、项目施加不同的外发规则策略（提供相关功能截图） |
| ★集成对接 | 兼容VMware vSphere、标准Openstack、华为FusionSphere等主流云计算平台，并支持多云平台统一管理 |
| 提供150颗物理CPU授权，包含五年维保服务。 |
| 支持与项目内态势感知平台对接，通过态势感知系统分析数据中心东西向流量的安全风险。 |
| 多租户 | 支持多租户，能够同步多租户云计算平台租户账号、租户项目、租户网络等多租户信息，并通过同步的租户账号登录及多租户同台并发管理维护 |
| 支持多租户账号管理，能够多租户账号展示、扩展信息补充，支持多租户本地启停 |
| 支持单租户、多租户模式切换，并支持单租户云平台、多租户云平台的混合管理 |
| 流量分析与威胁检测 | 提供分布式流量分析及安全检测能力，流量无需统一发送至物理计算节点之外，在计算节点内部即可实现流分析与威胁检测，显著降低网络传输开销 |
| 支持常见的HTTP、DNS、FTP、SSH、SMTP等协议还原和网络流量识别，能够显示区分云内东西向、南北向两个维度的流量 |
| 支持对云网流量进行安全分析，可针对病毒木马、漏洞攻击、DDos、Web攻击等恶意攻击类型进行检测，内置检测规则数不低于8500条 |
| 支持对云网流量进行实时失陷主机检测、文件信誉检测等威胁情报检测 |
| 支持对云网流量中提取的互联网地址进行地理位置GEO、IP情报的查询和展示（提供相关功能截图） |
| 支持自定义情报，能够对IP、文件、Domain、URL/URI等进行自定义检出 |
| 流与业务可视化 | 支持对云内东西向、南北向流量进流量、流速、新建、并发、应用流量等多维度指标分析统计（提供相关功能截图） |
| 支持按照数据中心、集群、计算节点、租户/项目、虚拟机、域等多种维度可视化展示其地理位置关系 |
| 支持按照数据中心、集群、计算节点、租户/项目、虚拟机、域等多种维度可视化展示其访问关系 |
| 支持根据业务节点流量情况可视化展示整体业务的访问关系及流量、访问数等访问情况 |
| 安全分析可视化 | 支持对同类安全日志的组合呈现和时序化分析，以减少同类攻击带来的大量重复无序日志 |
| 支持对攻击者、受害者、威胁规则进行攻击次数、关联受害次数等维度的统计排行 |
| 支持对云内威胁态势进行分值评估 |
| 资产与标签 | 支持展示云计算平台现有资产结构，包括虚拟机ip、mac、cpu、内存、磁盘、操作系统等信息 |
| 服务 | 支持自定义增加、编辑、删除资产信息，支持从云网流量中获取资产信息条目 |
| 支持自定义标签功能，能够从资产、安全事件、业务等多维度进行标签指定 |
| 系统维护 | 支持多用户、多角色，支持对账号的有效期、云平台、启停状态进行管理和配置 |
| 支持Syslog外发，可自定义配置安全日志、系统日志外发 |
| 质保 | 原厂五年质保，中标后签订合同前提供原厂商质保承诺函。 |

**24.堡垒机**

|  |  |
| --- | --- |
| 技术指标 | 设备技术要求 |
| ▲硬件规格 | 采用专用千兆多核硬件平台和安全操作系统，标准2U机架式，≥2个千兆电口,16G内存，内置≥8TB硬盘，单电源，最大支持500路图形会话或2000路字符会话并发，配置1000个授权许可。含五年原厂标准售后服务。 |
| 物理旁路，逻辑串联模式，不影响原有网络架构 |
| 功能要求 | 具备用户集中管理功能，能够依据系统功能模块灵活的创建用户角色，实现系统分权管理； |
| 支持多种身份认证方式（动态令牌、手机令牌、域认证）、密码防暴力破解、用户登陆来源（IP、MAC限制）控制，提升用户帐号安全性； |
| 能够统一管理IPv4、IPv6环境下的各类资源，包括主机、网络设备、安全设备、数据库等。  |
| 支持通过应用发布的方式集中管控BS、CS资源，多台应用发布服务器间支持负载均衡功能（无需第三方负载均衡设备），以此满足高并发场景下的接入需求； |
| 支持依据用户、资源及系统账号属性进行访问授权，其中属性可由管理员自定义，实现访问权限的灵活管理；须提供功能界面截图证明； |
| 支持H5方式访问目标资产（字符、图形协议均支持），无需在操作终端安装任何插件即可使用堡垒机。 |
| 支持字符、图形、数据库、文件传输操作审计，方便事后追踪溯源、满足合规建设要求，针对审计记录支持多关键字检索、多条件组合查询、查询结果合并审计功能，便于管理员快速定位相关操作；须提供功能界面截图证明； |
| 支持主机、网络设备系统账号密码自动修改功能，针对修改后的密码支持分段保管功能，同时具备密码工单用于普通用户临时申请密码，过期后自动修改实现一事一密的应用效果；须提供功能界面截图证明； |
| 支持对剪切板、磁盘映射、sftp文件传输进行集中控制审计，其中针对windows剪切板支持文件、文字单独控制（如禁止传输文件允许传输文字），以满足运维、安全管控需求；须提供功能界面截图证明； |
| 支持内置动态令牌认证和手机令牌认证，其中动态令牌支持国密算法加密； |
| 具备先进的审计技术，实现数据库及字符操作的精准记录 |
| **其它** | 原厂五年质保，中标后签订合同前提供原厂商质保承诺函。 |

**25.日志审计**

|  |  |
| --- | --- |
| 技术指标 | 设备技术要求 |
| 硬件指标 | 采用标准机架式硬件，系统独立运行不依赖于硬盘；冗余电源。 |
| ▲事件处理最高≥10000EPS，事件处理平均≥6000EPS。 |
| ≥4个千兆电口，≥4千兆光，≥1个Console接口；包含1000授权节点，包含5年标准维保。 |
| 内置存储总容量≥4TB，硬盘支持热插拔 |
| 部署模式 | 支持单一部署，也支持分布式部署。提供旁路接入模式，设备部署不影响原有网络结构；审计工作不影响被审计对象的性能、稳定性或日常管理流程 |
| 使用模式 | 采用B/S模式，无需安装客户端，使用WEB浏览器访问管理中心，浏览器端无需安装Java运行环境。支持chrome浏览。 |
| 日志采集 | 支持目前各种主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等配置日志、运行日志、告警日志的采集；支持审计各种中间件（tomcat、apache、webshpere、 weblogic等）配置日志、运行日志、告警日志等；支持常见的虚拟机环境日志收集，包括Xen、VMWare、Hyper-V等。 |
| 采集方式 | 支持通过syslog、SNMP Trap、JDBC、Agent代理、WMI、(S)FTP、NetBIOS、文件\文件夹读取、Kafka等多种方式完成各种日志的收集功能； |
| 资产管理 | 能够将资产按照多种维度进行分组、分域管理，如地理位置、组织结构、业务系统等，提供便捷的添加、修改、删除、查询与统计功能；支持资产信息的批量导入和导出，便于安全管理和系统管理人员能方便地查找所需设备资产的信息注册用户资产时，提供自动发现识别能力； |
| 日志统计分析 | 1） 可自定义统计场景，统计的字段条件和时间段以及过滤器等可自由设定；2） 支持柱状图、饼图、折线图、面积图、堆积图、环状图、数值图、地图等形式的统计信息可视化展示。3） 系统内置多种类报表模板，支持自定义审计报告； 4） 支持动态\静态（日报、周报、月报）两种系统生成方式；支持导出html、Excel、PDF； |
| 日志查询  | 支持B/S模式管理，支持SSL加密模式访问；支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作对象等参数进行过滤查询；支持用任意关键字对所有事件进行高性能全文检索；支持可指定多个查询条件进行组合查询；支持将查询的条件存储为查询模版，方便再次使用；极高的日志高查询性能，支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果。 |
| 日志备份 | 可设置日志存储备份策略；支持日志备份自动传送到远程服务器。 |
| 用户管理 | 根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，审计员只负责查看相关的审计结果及告警内容；日志员只负责完成对系统本身的用户操作日志管理；系统自带自身管理日志； |
| 系统许可方式 | ▲永久许可方式，再增加审计用户的情况下不用增加授权许可； |
| 资质要求（提供相关资质证明） | 提供《计算机软件著作权登记证书》 |
| 公安部《计算机信息系统专用产品销售许可证》 |
| 服务 | 原厂五年质保，中标后签订合同前提供原厂商质保承诺函。 |

**26.数据库审计**

|  |  |
| --- | --- |
| 技术指标 | 设备技术要求 |
| **▲**硬件规格 | CPU规格≥4核，内存≥16GB； |
| 要求≥4个10/100/1000千兆电口，≥2个千兆光口，支持监听接口扩展； |
| 系统内置≥4TB硬盘，支持外部网络存储或硬盘扩展；  |
| 性能要求 | 事件处理数≥20000条/秒  |
| ★不限制审计数据库实例数量 |
| 1GB事件量查询平均响应时间不超过10秒 |
| 部署管理 | 采用旁路部署方式对原有网络不造成影响，网络审计产品的故障不影响被审计系统的正常运行 |
| 采用B/S管理方式 |
| 无需在被审计系统上安装任何代理 |
| 数据库审计支持 | 支持包括MS SQL Server、Oracle、DB2、Sybase、MySQL、Informix、六种主流数据库审计 |
| 支持PostgreSQL、HANA、Teradata、Cache、人大金仓、达梦、南大通用数据库审计； |
| 支持MongoDB、Hbase非关系型数据库审计； |
| ★支持在目标数据库安装agent解决云环境、虚拟化环境内部流量无法镜像场景下数据库的审计，并提供证明 |
| 可审计数据库的DDL(创建、修改、删除)，DML(新增、更新、删除、查询)，DCL(授权、取消权限、拒绝)和其它(事物控制、执行、set、show、use、desc、备份恢复、导入导出、应答、dbcc、声明、其它操作),用户登录注销等行为 |
| 支持审计HTTP/HTTPS协议的URL、访问模式、cookie、页面内容、Post内容 |
| 可审计内容细化到库、表、记录、用户、存储过程、函数等，审计内容包含sql参数 |
| 支持与堡垒主机自动关联审计通过ssh、rdp等加密协议操作数据库行为 |
| 审计能力 | 支持数据库绑定变量审计 |
| 支持访问数据库的源主机名、源主机用户的审计 |
| 支持SQL操作响应时间的审计  |
| 支持Select操作返回行数的审计 |
| 支持数据库操作类、表、视图、索引、触发器、存储过程、域、Schema、游标、事物等各种对象的SQL操作审计 |
| 事件查询 | 查询条件易于使用，审计查询条件均为非正则表达式形式进行支持采用部分匹配模糊查询方式检索审计日志支持基于数据库访问日期、时间、源/目的IP、来源、数据库名、数据库表名、字段值、数据库登陆账号、SQL关键词、数据库返回码、SQL响应时间、数据库操作类型、影响行数等条件的审计查询； |
| 系统自身监控 | 用户对本软件系统的操作都记录日志并进行持久化存储，便于追踪、审核和告警 |
| 用户模式 | 采用B/S架构管理，支持中文界面，使用安全https访问管理中心，支持系统安全配置（会话锁定、超时退出、IP地址访问控制、密码复杂性管理、验证码登陆等措施） |
| 采集方式 | 采用旁路侦听方式接入获取数据，在不改变网络结构的情况下精确监控，不会对网络内部的流量与数据信息造成任何瓶颈，设备本身运转与否都不影响网络的正常工作 |
| 资质要求 | 要求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》 |
| 质保 | 中标后，签订合同前提供设备五年原厂商质保服务承诺函及授权书。 |

**27.漏洞扫描**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 硬件规格 | 标准2U硬件平台，RJ45串口≥1，GE网口≥2，USB口≥2，双电源，硬盘≥1T |
| 部署方式 | 支持旁路部署，无需改变原有的网络架构 |
| 扫描对象 | 主机、软件漏洞扫描 |
| 功能要求 | 产品要求界面友好，并有详尽的技术支持文档，所有图形界面要求中文。 |
| 系统为B/S架构，并采用SSL加密通信方式，用户可以通过浏览器远程方便对产品访问操作，支持多用户同时登陆操作。 |
| 提供分布式部署，上级管理设备能够方便查看下级设备状态。 |
| 提供三权分立的账户体系，支持上下级部门管理，非上下级的不同部门任务、资产隔离。 |
| 提供审计功能，能够对登陆日志、操作日常进行记录和查询，并可以将日志导入导出操作。 |
| 提供日志自动审计功能，根据指定的审计标准自动、定时审计；并将审计结果发送到指定邮箱当中。 |
| 漏洞策略库大于20000条；  |
| 系统内置不同的策略模板如针对Linux、Windows操作系统等模板，同时允许用户定制扫描策略；用户可定义扫描范围、定义扫描端口、扫描使用的参数集等具体扫描选项。 |
| 支持Windows系列操作系统，支持Linux主流操作系统（Centos、Redhat、Debian、Fedora、Ubuntu、Suse等），支持Unix主流操作系统（AIX、HPUX、Solaris等）； |
| 支持对Web、FTP、电子邮件等应用系统、Apache等web中间件服务器以及Office等常用软件进行漏洞扫描； |
| 可以自定义扫描端口范围、端口扫描策略 |
| 提供采用SMB、SSH等协议对Windows、Linux系统进行登录授权扫描。  |
| 具备弱口令扫描功能，提供多种弱口令扫描协议，包括SMB、RDP、SSH、TELNET、FTP、SMTP、IMAP、POP3、MySQL、MSSQL、REDIS、RTSP等协议进行弱口令扫描，允许用户自定义用户、密码字典。 |
| 支持发现非默认端口启动的服务，支持服务的协议识别、版本 |
| 可根据端口识别出的软件版本提供可能存在的相关漏洞列表 |
| 支持HTML、WORD、PDF、XLS报告格式 |
| 数据库弱点扫描模块 | 支持Oracle、Mysql、SQLServer、DB2、informix、达梦、人大金仓的授权数据库漏洞扫描，提供产品截图； |
| WEB应用弱点扫描模块 | 支持识别国内外主流Web应用防火墙品牌； |
| 支持各种WEB应用系统以及各种典型的应用漏洞进行检测（如SQL注入、Cookie注入、XPath注入、LDAP注入、跨站脚本、代码注入、表单绕过、弱口令、敏感文件和目录、管理后台、敏感数据、第三方软件等）； |
| 质保 | 原厂五年软硬件上门质保服务；中标后签订合同前提供原厂商质保承诺函。 |

**28.态势感知**

|  |  |
| --- | --- |
| 技术指标 | 设备技术要求 |
| ▲硬件配置要求 | CPU： 2颗≥10核CPU主频2.20GHz以上；内存：≥256G。系统盘：600GB及以上固态硬盘2块，并提供Raid 进行备份。存储盘：48TB企业级SATA盘；网卡：≥2个千兆电口及2个万兆光口电源：冗余电源 |
| 支持集群部署，基于大数据架构可水平扩展至多台设备集群。 |
| 性能规格 | 升级后达到能够实时深度解析≥6Gbps的网络流量吞吐量；数据采集和处理性能≥10000EPS，每条数据大小>1KB； |
| 数据接入 | 支持接入并管理日志采集器、流量采集器，可支持第三方采集器接入；  |
| 支持对日志采集器进行采集配置并下发；提供Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、agent等采集方式；支持对网络设备、主机系统等安全日志、网络流量以及业务信息等多种数据源的采集； |
| 支持通过多种类型的安全、泛安全类数据接入采集，应包括但不限于设备日志数据、流量数据、弱点漏洞数据、系统性能数据、威胁情报数据、资产人员数据； |
| 支持通过流量采集设备采集接入全流量数据，包含流量中的请求包和返回包等信息，并可在数据检索中体现包信息； |
| 支持接入文本格式、CVS等格式的文件数据，可通过模板文件的填写导入实现资产数据的导入和管理； |
| 日志类型 | 支持自定义日志类型功能，可在线对其字段信息、存储类型、存储时间、分区方式、位置等基础属性信息进行配置，从而达到分类存储日志的目的；  |
| 支持本地威胁情报的检索，检索类型支持域名、IP地址、文件MD5值；能够自定义威胁情报，支持类型包含IP、MD5、域名、URL、IP地址:Port、IP地址：URI、IP:Port/URI、域名:Port、域名:Port/URI。 |
| 资产管理 | 支持管理资产主机设备、网络设备、安全设备、应用系统等资产类型管理；支持资产详情信息的展示，能够展现资产基础信息（资产名称、IP地址、分组、厂家、型号、操作系统类型、物理地址、资产使用状态等）；支持资产服务信息管理，支持对服务的IP地址、端口号、服务名、服务版本、协议、Banner等服务属性进行管理，支持对IPV6资产的管理 |
| 威胁预警 | 支持对重大网络安全事件（如永恒之蓝，Struts 2漏洞利用等新生大面积爆发的严重事件）进行威胁预警。通过厂商对重大网络安全事件的追踪生成预警包，并赋能分发给用户。支持通过预警包导入完成网络安全事件的影响面评估，并持续的跟进事态的发展，快速完成重大网络安全事件的预警及处置。 |
| 支持隐蔽信道检测，包括dns信道、端口反弹等对外通讯方式。 |
| WEBSHELL检测模型>10种，能够分别检测WEBSHELL上传、植入、控制阶段；SQL注入、命令注入、跨站脚本、代码注入、协议错误攻击检测模型>1000种；支持对HTTP、Telnet、FTP、POP3、SMTP、IMAP等协议进行弱口令检测。 |
| 支持钓鱼邮件检测，对社工类攻击进行检测，检测内容包括：邮件头欺骗、邮件发件人欺骗、邮件钓鱼欺骗、邮件恶意链接；支持垃圾邮件检测。 |
| 拓扑管理 | 支持逻辑拓扑的绘制，提供在线拓扑绘制工具,可手动进行逻辑拓扑的绘制； |
| 支持导入背景图，支持（PNG、BMP、JPG、JPEG）四种文件格式； |
| 支持拓扑图的整体拖拽和缩放操作，支持对单个节点施放操作，支持关联拓扑下钻； |
| 支持拓扑图节点属性信息的显示与隐藏，支持查看节点的详细信息； |
| 资产风险评估 | 支持按照单一资产进行资产风险评估列表展示，内容至少包含“资产名称、资产风险值、资产告警数、资产脆弱性数、资产失陷状态标识”等信息；支持按照单一资产图形化展示资产告警及脆弱性数量，可按照趋势、等级、处置状态等信息系进行展示。 |
| 支持按照资产分组进行资产组风险评估列表展示，内容至少包含“资产组名称、资产组风险值、资产组告警数、资产组脆弱性数、资产组失陷主机”等信息；支持按照资产分组图形化展示告警及脆弱性数量，可按照趋势、等级、处置状态等信息系进行展示。 |
| 联动处置 | 支持与现有网络内现有防火墙、终端安全管理产品进行联动处置能力，当发现失陷主机、恶意域名等威胁事件后，可以及时给联动设备下发阻断或告警的安全防护策略动作且防护策略支持对生效时长的配置，支持的联动处置消息类型包括IPv4地址；  |
| 威胁展示 | 支持展示预警事件中攻击者、受害者、既是攻击者也是受害者的IP之间关系。支持统计预警事件中影响资产的统计，包括风险资产、受攻击资产、失陷资产的统计。支持展示当前威胁预警事件对资产造成的影响趋势，包括风险资产、受攻击资产、失陷资产的影响趋势 |
| 登录管理 | 提供三权分立的用户管理能力：配置员、用户管理员、审计员相互独立，支持根据对象属性自定义划分系统管理角色和一般用户角色，按照数据和功能分级灵活设置用户权限。 |
| 支持用户角色管理，可以为不同角色赋予不同系统功能模块及数据的读写权限，未赋予此模块读写权限的用户，将无此功能模块的显示或配置的权限。 |
| 支持双因子认证方式登录系统，认证方式支持短信和邮箱。支持对登录的并发会话数的设置，限制同时登陆系统的用户数量。 |
| 资质要求 | 产品具备公安部销售许可证。 |
| **其它** | 原厂五年质保，中标后签订合同前提供原厂商质保承诺函。 |

**29.网络管理**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 硬件要求 | CPU ≥2.2GHz 10核心 20线程\*2，内存≥64G，GRAID卡≥2，可用存储空间不低于1T，千兆电口≥4个 |
| 功能要求 | 分布式部署：要求资源拓扑、告警、性能等功能模块支持多服务器分布式虚拟化部署，可实现负载分担，满足大规模网络环境的统一管理。 |
| 用户分权管理：可以为不同的管理员设置不同的用户名、密码，并限制管理员的管理权限和管理范围，实现用户分权管理。 |
| 多平台支持：支持Windows、Linux平台、麒麟等国产操作系统，及MS SQL、Oracle、达梦等数据库，支持B/S架构。 |
| 自动发现拓扑：自动发现网络中的所有网络设备，并在拓扑中显示出来，支持拓扑图自定义修改，包括设备、链路等。 |
| 支持IP拓扑、二层拓扑、自定义拓扑视图（支持网络区域的任意划分、命名、拖拽、折叠和展开）、全景拓扑、Vxlan拓扑、邻居拓扑、LLDP-MED拓扑、流量拓扑、数据中心拓扑、数据中心机架拓扑、IRF拓扑、MDC虚拟网络拓扑、MDC和IRF组合拓扑等多种拓扑类型；二层拓扑支持多协议，包括Bridge、NDP、CDP、MSTP、STP、LLDP、DISMAN-PING等二层协议，支持聚合链路，支持第三方的设备；拓扑可融合链路状态、设备告警等多种信息。并支持以GIS地图为拓扑背景图。 |
| 故障管理：支持对全网设备告警的实时监控和统一浏览；支持多种提醒方式，如告警实时提醒（告警板）、告警音响提示；支持多种转发方式，比如转E-mail，转短信，转上级网管或其它网管等。支持告警分析，可以屏蔽重复告警、闪断告警，支持告警自动确认功能； |
| 告警智能分析，包括告警分类关联分析、告警多源关联分析、告警拓扑根源分析、告警网络影响度分析。 |
| 提供直观的设备的面板视图：支持设备面板的显示、定时刷新、面板缩放功能，通过面板管理，网络管理人员可以直观地看到设备、板卡、端口的工作状态；并提供基于设备面板的设备、单板、端口配置功能。 |
| 支持虚拟网络资源管理、虚拟网络拓扑展示、虚拟网络告警管理、虚拟网络性能监控、虚拟交换机配置管理、虚拟网络配置迁移管理。 |
| 多厂商设备配置及软件管理：支持H3C/HUAWEI/3COM/CISCO/HP设备的批量配置和软件管理，包括的软件版本和软件库中最新可用的软件，更新设备的软件。支持220+设备厂商，8000+设备款型。 |
| 支持管理第三方设备：新设备注册，告警注册，新性能指标注册，新Syslog解析注册，Mib编译，第三方设备配置管理-CLI下发，配置管理-配置备份、软件升级（使用TCL/ Expect /Perl模板自定制），第三方设备管理系统集成。 |
| 二次开发接口：提供基于REST、SOAP的接口开放能力。并提供北向SNMP接口。 |
| 本次实配可管理网络及安全设备≥200 |
| 质保 | 原厂五年软硬件上门质保服务；中标后签订合同前提供原厂商质保承诺函。 |

**29.终端安全管理平台**

|  |  |
| --- | --- |
| **指标项** | **技术要求** |
| 内网安全管理（基本功能） | 支持与数字证书捆绑注册，能获取数字证书的信息；支持带界面注册、静默注册、不带界面有进度有提醒注册；  |
| 实配1500个前端终端准入管理 |
| 策略管理：系统支持根据用户和根据设备两种模式的策略下发，还可根据用户所在组、IP地址、操作系、统、自定义检索等多种方式进行策略分发 |
| 策略采用下载到本地执行的方式，断网重连后终端再次获取最新策略，同时上报离线期间审计记录。终端安全程序可自动侦测网络连接情况，根据连接内网/未连接内网可执行不同的安全策略 |
| 具备独立审计账户、管理账户，权限各自独立。提供系统运行审计和操作审计机制，系统管理员登录要求支持IP地址访问限定，只有获得授权的计算机才能进入系统控制台 |
| 硬件变化管理：系统要求支持设备硬件变化行为报警；支持对未注册设备、注册程序卸载行为的报警 |
| 系统兼容Intel vPro主动管理技术。（需提供功能截图） |
| 终端支持代理软件和IE代理禁用功能 |
| 要求支持网管统一管理的主机防火墙功能 |
| 支持进程管理功能：支持对（包括软件厂商名、源文件产品名、源文件名、进程名等）的进程进行黑白名单的控制，黑名单内进程自动被禁止，白名单内进程自动启动。（需提供功能截图） |
| 具备对客户端流量的控制和采样，能够设定终端流量阈值 |
| 可定期自动将客户端指定文件备份到服务器、支持增量备份。（需提供功能截图） |
| 资产管理 | 支持每日统计设备注册状态，并支持按区域、按部门进行统计查询，包含：IP设备总数、应注册数、已注册数、保护数、非应注册数、应注册未注册数、应注册未注册已保护数、注册率；支持定时对设备类型进行统计，并支持按区域、按部门进行统计查询；支持每日统计杀毒软件安装情况，包括：未安装杀毒软件设备数、杀毒软件覆盖率，并支持按区域、按部门进行统计查询。 |
| 支持注册IP审核,需展示信息包含：IP地址、MAC地址、责任人、联系电话、所属部门、设备所在地、审核状态、申请时间，其中待审核数据支持操作审核通过、审核不通过。支持注册审核开关配置，开启注册审核后，新安装终端代理程序的设备需管理员审核通过后允许入网。支持与数字证书捆绑注册，能获取数字证书的信息； |
| 支持按设备类型、按区域/部门、按自定义组、按硬件配置对管辖区域内设备信息进行查询，设备信息包括基础信息（如：IP地址、MAC地址、责任人、联系电话、所属部门、设备类型、注册状态、在线状态、保护状态、阻断状态、锁定状态）、扩展信息（如：生产厂商）、开放端口情况、在线/离线审计；支持设备操作：保护/取消保护、阻断/取消阻断、编辑、删除、导出、添加自定义组、设备部门重置、指定天数的未上线设备删除；支持IP使用整理：取消IP配置与部门划分不一致的设备保护状态； |
| 对已注册设备支持实时点对点控制，包含：离线临时解绑、在线临时解绑、编辑IP、消息推送、屏幕控制、卸载终端、查看软件、查看硬件、查看服务、查看端口、查看进程、查看策略、查看计算机账户、查看服务端防护日志。 |
| 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。 |
| 发现所有已注册设备的软件安装情况，包含：类型、名称、版本、发布者；支持软件分布设备查询。 |
| 发现管控范围内的网络服务，并将服务分类为：WEB服务、数据库服务、网络基础服务、资源共享服务、操作系统服务、其他服务；网络服务信息包含：服务类型、服务名称、描述、端口号、协议类别、协议名称； |
| 主机监控审计 | 支持对设定目录文件的操作审计，包括文件创建、打印、读写、复制、改名、删除、移动等的记录，同时将信息上报管理信息库供查询；具备对终端的系统、软件和共享等目录中的文件具有保护功能，设定访问、删除、修改权限；支持全盘文件禁止删除，审计自定义文件扩展名。（需提供功能截图） |
| 具备对用户的网页访问行为进行控制并对用户访问的网页进行本地审计和记录上报。能够设置访问域名或IP的黑白名单 |
| 具备对主机刻录行为进行管理和审计的功能，能够审计终端刻录行为，客户端集成专用刻录软件，自动屏蔽其他刻录软件和系统自带刻录功能，只能通过专用软件刻录；具备普通刻录和封口刻录的功能；刻录前需要输入操作人的账号密码以验证身份。（需提供功能截图） |
| 具体审计用户/组权限更改，操作系统内用户/组的增、删操作 |
| 补丁管理 | 具备补丁自动分发安装，同时支持默认和用户自定义补丁分发策略，并自主配置分发 |
| 具备终端代理转发技术，未下载补丁的终端可从已下载补丁的终端获取补丁，从而缓解服务器压力，提高补丁分发效率。（需提供功能截图） |
| 具备补丁内网自动测试功能，即用户可自主选定内网部分设备为补丁安装测试设备，系统将新获得的补丁自动发送给这些设备，在测试设备安装指定时间间隔后再自动分发给其他设备。（需提供功能截图） |
| 具备文件分发功能，能自动向终端分发各类文件和可执行程序，支持后台静默安装和运行分发的程序 |
| 能够通过文件、进程等信息判断分发的程序是否下载并安装成功，能够统计文件分发结果。（需提供功能截图） |
| 移动存储介质管理 | 支持U盘、移动硬盘、存储卡等存储设备注册管理 |
| 注册登记与加密处理。对于处于敏感信息的移动存储介质，在使用之前需进行登记注册和加密处理。登记信息包括：使用人、使用部门、联系电话等等 |
| 支持多标签管理，相互隔离网络的U盘可写入不同的标签，杜绝不同网络之间U盘交叉使用。（需提供功能截图） |
| 支持标签U盘双分区。（需提供功能截图） |
| 系统支持多标签管理，同一网络不同部门的U盘可写入不同的标签，从而实现同一网络不同部门之间U盘交叉使用的权限控制 |
| 非法外联监控 | 能快速发现和控制网络中的非法外联行为，阻断终端通过多网卡、WIFI、3G/4G网卡、手机等多种方式网络非法外联访问，杜绝网络非法外联行为发生 |
| 系统支持违规联网监测和取证功能，可发现内网设备违规联入互联网的行为，并进行报警和阻断，审计终端违规外联的路由情况。（需提供功能截图） |
| 支持扩展部署模式，在互联网扩展部署外网报警服务器，终端违规接入互联网自动与服务器通信，上报终端信息，实现违规外联强审计和抗抵赖。（需提供功能截图） |

**30.杀毒软件管控平台（含非法外联管控）**

|  |  |
| --- | --- |
| 技术指标 | 指标要求 |
| 客户端安装要求 | 操作系统支持： Windows 7/ 8/10/2008/2012/linux |
| 提供1000个Windows客户端授权,100个linux授权。 |
| 系统管理 | 控制中心：采用B/S架构管理端，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、统一漏洞修复、统一管控、统一终端准入合规、终端软件管理、硬件资产管理以及各种报表和查询等功能； |
| 客户端提供控制中心管理所需的相关数据信息，通讯可选择非明文方式；客户端执行最终的木马病毒查杀、漏洞修复等安全操作； |
| 支持自定义默认分组的终端默认功能模块,包括产品功能模块及实用工具等； |
| 支持控制中心防暴力破解 |
| 支持加密的控制中心远程访问，支持管理账户并发、密码有效期、鉴别失败锁定等设置； |
| 支持根据分组、计算机名称、IP地址、操作系统、在线状态等条件的组合筛选出符合条件的终端进行管理； |
| 终端安全管控 | 支持tcp、ping、域名解析三种外联探测方式，支持自定义探测地址，探测频率，支持外联告警断网，支持终端互联网出口IP探测 |
| 可监控指定终端网络、应用程序的上传，下载速度与流量； |
| 支持冗余有线网卡、无线网卡、3G网卡、MODEM、ADSL、ISDN等设备的外联控制；违规外联发生时可针对内外网连接状态分别设置违规处理措施 |
| 支持对终端各种外设（USB存储、硬盘、存储卡、光驱、打印机、扫描仪、摄像头、手机、平板等）、接口（USB口、串口、并口、1394、PCMIA）设置使用权限 |
| 支持自定义外设黑白名单，且支持分组执行、支持以设备名称或者PID/VID例外 |
| 支持对终端桌面系统的账号密码、本地安全策略、控制面板、屏保与壁纸、浏览器安全、杀毒软件检查 |
| 病毒库与补丁库支持与上级集联，及时更新 |
| 服务 | 原厂五年质保，中标后签订合同前提供原厂商质保承诺函。 |

**31.PKI/PMI系统**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| ★基本要求 | 为了安全认证网关能够与身份认证服务器系统兼容联动用户属性信息和策略发布，须同一品牌。 |
| 集中认证网关 | 设备规格性能：标准2U安全专用设备，4个千兆网口，冗余电源；最大新建连接数（RSA）：5000次/秒;最大新建连接数（SM2）：5000次秒;每秒完成交易数(TPS)：25000次/秒;最大并发连接数：10000;最大吞吐流量：≥850Mbps。 |
| 系统同时支持国密SM2算法和RSA算法。 |
| 支持RSA/SM2证书自适应，系统配置RSA和SM2两张证书，并同时启用，根据客户端的算法能力进行自动适应 |
| ★支持多种认证策略方式、使用的协议、加密强度、以及是否传递相关信息等进行控制满足不同需要。（提供相关功能截图） |
| 支持多应用类型支持，可以对B/S应用进行安全防护外，对于FTP、Telnet、SSH、远程桌面、SMTP、POP3等多种非B/S应用也可以进行安全防护。 |
| 支持认证服务连接模式正反代理、协议类型、数据流向，定义多个服务，根据业务实际需求可灵活多变支持。（提供相关功能截图） |
| 支持多服务功能，支持创建多个SSL服务，保护不同的应用服务，也支持同一个SSL服务保护多个应用服务。 |
| 支持与数字证书认证系统无缝兼容同步获取证书CRL吊销列表及黑名单，对用户证书有效性验证。提供黑名单服务配置、LDAP服务配置、黑名单上传下载配置、黑名单自动更新、黑名单管理（提供相关功能截图）。 |
| 支持认证一致性，通过特有的HTTP注入技术将根据不同的公安行业用户的证书信息传送给后台应用，使应用无需证书接口开发就可以方便的获取用户证书信息 |
| ★支持证书信息绑定，将信息绑定到cookie、URL和HTTP的位置，也可绑定文件类型，支持自定义，显示对绑定内容和站点列表的查看。（提供相关功能截图） |
| 支持访问控制功能，实现URL级别的访问控制，对于不同用户、不同角色实现不同的控制。 |
| 支持单点登录，采用用户映射技术，将证书映射为原有系统中的账户并进行自动登录，应用无需修改的情况下实现单点登录。 |
| 支持策略统一下发，系统实现客户端策略的统一下发，用户无需对客户端进行任何配置。 |
| 支持与数字证书认证系统无缝兼容同步用户注册信息、机构角色，结合证书状态动态策略发布，实现对用户使用证书的权限监管。 |
| 支持信息统计，系统能够对用户连接数、应用访问情况，系统资源占用等信息进行详细统计。 |
| 支持性能检测功能，系统支持对CPU、内存、磁盘容量、连接数、进程等资源情况的收集，便于系统的维护和问题定位。 |
| 具备自主研发知识产权的软件著作权证书。具备符合通过公安部测试的集中认证网关产品目录中的产品。 |
| 身份认证服务器 | 性能指标：平均响应时间（申请单张证书 ms）：<500ms；单位时间最大处理能力：>6000张/小时； |
| 自主知识产权，符合国密算法标准规范，同和符合国际通用标准规范， |
| 支持RSA算法和国密SM2算法的数字证书发放； |
| 完全自有的一体化管理和证书的命周期管理，内含用户注册、证书签发、证书发布、密钥管理等核心功能； |
| 基于B/S结构的管理界面，采用https安全远程管理机制进行安全登录； |
| 支持遵循 X.509 V3 的证书格式标准，并且支持 SSL 协议和 S/MIME 协议； |
| 支持证书签发：签发各种实体证书 |
| 支持证书延期：根据要求延期证书，包括由注册发起的证书延期功能；由用户发起的在线证书延期申请功能 |
| 支持证书更新：能够根据要求，实现证书的更新。包括证书用户信息更新，用户的密钥的更新等。 |
| 支持证书的冻结和解冻：由管理方发起，对证书进行冻结，使证书列入黑名单，暂时因为失效而无法使用；同时，也可对被冻结的证书进行解冻操作，使该证书恢复正常的使用功能。 |
| 支持证书废除：吊销实体证书，分为CA中心强制废除和用户申请废除。 |
| 支持证书恢复：CA中心根据系统策略，由注册管理员将废除原因为“暂时不使用”的已废除的用户证书进行恢复操作。 |
| 支持系统内置LDAP服务，基于LDAP证书发布，基于LDAP和HTTP的CRL发布 |
| 支持配合根CA部署为二级CA的模式 |
| 支持签发多应用用户证书，SSL 客户端证书，设备证书，VPN 证书； |
| 支持签发电子邮件证书和对应的证书发布模式，可以使用OutLook，Foxmail、安全电子邮件等进行电子邮件的加密和签名。 |
| 具有灵活的策略配置机制，可新增证书策略； |
| 支持使用CSP和SKF接口签发双证书，无缝接入新的证书介质； |
| 跨平台支持多种RSA、SM2算的的多种密码机和密码卡； |
| 支持系统管理：包含系统备份/恢复、系统在线升级、系统日志查询、License在线升级、管理员管理、网络配置等； |
| 支持10000license并支持继续扩容； |
| 具备自主研发知识产权的软件著作权证书。具备商用密码产品认证证书和计算机信息系统安全专用产品销售许可证。 |
| 质保 | 原厂五年软硬件上门质保服务；中标后签订合同前提供原厂商质保承诺函。 |

**32.显示器**

|  |  |
| --- | --- |
| 显示器 | 工业显示器，》75寸，》1080P，支持VGA\HDMI\DVI等多种接口，提供支架及底座。 |

**33.集成服务**

|  |  |
| --- | --- |
| 集成服务 | 本项目所有硬件产品要求提供原厂商工程师安装、配置服务，以及定期巡检服务 |
| 相关可信组件必须实现与上级公安机关安全访问平台对接，按公安部规定实现访问相互认证。（免费对接） |
| 可信代理控制服务、可信接入代理、可信API代理和可信环境感知代理等设备之间对接、联调、优化。 |
| 公安机关以外单位VPN接入电路访问公安业务对接；与网安、技侦数据中心的网络融合。 |
| 项目实施期间（设备到货后起，项目验收止），投标人提供一名固定的有经验驻场技术人员，全程联系并会同厂商工程师进行软硬件安装实施、系统部署和调试配置等工作，同时由该工程师联系和协助处理后续项目相关的细节技术问题 |
| 实现可信代理控制系统和pki/pmi系统人员信息的联动，实现访问动态授权 |
| 安全设备系统可以将各类威胁日志送到态势感知平台实现对接 |
| 防火墙设备机房上架实施，提供线缆连接、安全策略配置、调试、优化等。 |
| 虚拟云桌面资源服务器和万兆汇聚交换机上架实施，服务器虚拟化软件、云桌面管控系统及虚拟云桌面软件安装部署及网络配置。 |
| 超融合虚拟化服务器设备上架实施，虚拟化软件、系统安装、调试、优化等。 |
| 审计设备架实施、完成市局现有安全设备、数据库、应用系统、网络设备等各类设备日志接入配置、联调测试和优化。 |
| 投标产品由于软件等其他无法适配的，硬件接口不够的，由中标人免费更换产品 |
| 提供6个以上(椒江)移动IDC机房的机柜 |
| 本项目硬件正常运行使用集成及部署实施所需的所有网络、光纤、电源PDU、线缆及电源插座、标签耗材等由中标方提供。 |

**34.三级等保测评服务1次（2.0标准）**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 等保测评 | 安全访问平台（含安全管理中心）按三级等保（2.0）标准开展测评一次。 |

**35.运维服务**

|  |  |
| --- | --- |
| **指标项** | **服务要求** |
| 运维要求 | 二名工程师驻点3年，分别运维安全访问平台及安全管理中心的软硬件，对网络设备和安全设备有三年以上的实际操作经验有网络和安全中级以上认证的资质证书，有参加此项目现场实施的经验。 |

1. **实施要求**

4.1 项目进度要求（根据实际情况调整）

投标人需承诺在合同签订后60个工作日内需完成设备到货，本项目要求中标后6个月内完成实施及部署，通过初验，进入为期3个月的试运行。中标后12个月内完成项目竣工验收。

投标人应按照上述时间安排，制定相应的项目实施详细进度计划，确定每个实施阶段的时间表及工作目标。

如项目无法按进度要求开展，采购方有权利终止合同并扣没项目履约保证金。

4.2 安装、调试和验收要求

1、中标方有责任检查安装现场是否符合产品安装条件。

2、货物到达买方指定的现场后，将由中标方与采购方、监理方共同开箱清点，并进行签字确认。若有差异，应由中标方承担责任。

3、产品实施过程中，如果牵涉到与第三方系统集成工作，中标方应与其他供应商无推诿合作，并提供必要的技术支持。

4、中标方应保证其提供的货物在正确安装、正常使用和保养条件下，在使用寿命期内应具有满意的性能，中标方应对由于设计、工艺或材料的缺陷而产生的故障负完全责任。

5、系统验收合格的条件必须至少满足以下三个要求：已提供了合同的全部货物和资料、完成了系统集成工作，通过了系统联合测试；试运行期间，系统运行稳定、正常，性能满足合同及招标文件、中标方投标文件要求。

4.3 人员培训要求

中标方应安排技术人员对用户进行免费培训或技术指导。培训人数不少于3人，次数不少于5次，培训时间不少于20小时。培训内容主要为本项目采购的各软硬件产品，培训目标要求使用户能够独立进行日常管理和维护。人员培训费用计入投标总价。

4.4 技术支持及售后服务要求

1、采购需求文件中无特别说明的，所有软硬件产品要求提供原厂五年免费质保，并需在合同签订后提供原厂免费质保服务承诺函（加盖原厂公章）。承诺函需承诺质保期内软硬件免费质保，且免费提供最新的软件版本及特征库等升级服务。硬件设备和商品化软件维保期、定制化软件维保期从项目验收合格之日算起。

2、在保修期内由于设备本身质量原因造成的任何损伤或损坏，中标方须免费负责修理或更换。

3、对于出现紧急故障情况，中标方应承诺商务时间30分钟内响应，一般故障2小时内响应，6小时内到达现场，重大故障1小时内响应，2小时内到现场服务，4个小时内解决问题；不能修复的，12小时内提供备品、备件或备机等措施，以保证用户的正常使用。

4、在保修期结束前，须由中标方工程师和采购方代表进行一次全面检查，任何缺陷必须由中标方负责修理，在修理之后，中标方应将缺陷原因、修理内容、完成修理及恢复正常的时间和日期等报告给采购方。

5、中标方须作出无推诿承诺。即中标方应提供特殊措施，无论由于哪一方产生的问题而使系统发生不正常情况时，并在得到采购方通知后，须立即派工程师到场，使系统尽快恢复正常。

6、要求服务工作人员对工作中涉及到的用户的数据、文件等任何资料进行保密。因工作人员的行为造成泄密等问题由中标单位承担相应的责任；

4.5 项目验收要求

项目的验收包括初步验收、试运行和竣工验收。

1）项目初验

项目初验前，中标方应首先对系统进行自测，并将系统自测报告提交采购方和监理方审查。中标方依本合同约定向采购方提交成果及相关文档，并向采购方提出初验申请。采购方接到中标方初验申请后，组织相关单位进行初验，初验合格后联合签署初验报告。

2）试运行

初验合格后，系统进入试运行，试运行时间为3个月。

3）终验

系统通过试运行后，中标方向采购方提出终验申请，采购方组织相关单位进行系统的终验。系统终验通过，进入正式运行阶段。系统终验收合格的条件必须至少满足以下三个要求：已提供了合同要求的全部设备、软件和资料；试运行时性能满足合同及招标文件、中标方投标文件要求；性能测试和试运行验收时出现的问题已被解决。

4）验收相关功能及性能指标

可信接入代理：应用通过可信接入代理发布，实现访问控制和加密传输。

可信API代理：实现应用前置区与后置区网络间高效的API方式数据交互。

虚拟桌面：使用虚拟桌面、水印等防止敏感应用和数据泄露。

软硬件设备功能需满足采购需求标明的参数和指标。

云桌面并发用户：支持300个并发用户。

公安接入网用户应用访问时延≦200ms。

**第二标段：智慧\*\*-虚拟化平台扩容**

**1、项目建设背景**

近年来，台州市公安局信息化应用多部署在虚拟化平台上，随着科技业务迅猛增长，虚拟化平台的计算资源和存储资源已趋饱和；另外我局小型机上也运行十多年，设备逐步老化，故障风险逐步增加。因此，拟对现有虚拟化平台进行扩容，满足未来业务需求；并对原部署在小型机的应用、数据库进行迁移，确保公安核心业务高速稳定运行。

**2、采购清单**

|  |  |  |
| --- | --- | --- |
| **序号** | **产品名称** | **数量及单位** |
| 1 | 核心数据库存储（核心产品） | 2台 |
| 2 | 虚拟化平台存储 | 2台 |
| 3 | 数据库服务器 | 4台 |
| 4 | 虚拟机服务器 | 12台 |
| 5 | GPU服务器 | 1台 |
| 6 | 光纤交换机 | 2台 |
| 7 | 备份一体机扩容 | 1台 |
| 8 | 网卡扩容 | 6块 |
| 9 | 核心交换机 | 1台 |
| 10 | 核心交换机扩容 | 1块 |
| 11 | 下一代防火墙 | 2台 |
| 12 | 堡垒机 | 1台 |
| 13 | 综合日志审计系统 | 1台 |
| 14 | 数据库审计系统 | 1台 |
| 15 | 准入控制系统 | 1台 |
| 16 | 终端安全管理平台 | 1套 |

**3、技术规格参数**

**3.1核心数据库存储（2台）**

|  |  |
| --- | --- |
| **指标项** | **配置及参数要求** |
| 品牌 | 国产知名品牌 |
| 控制器 | 配置双活控制器（非AP模式），支持控制器扩展，最大支持≥4控，提供相关功能证明截图或第三方测试报告。每个控制器物理CPU核心数不少于10核 |
| 存储缓存容量 | 缓存容量配置≥256GB（不含性能加速卡或SSD缓存等） |
| 前端主机通道接口 | 支持8/16/32Gbps FC作为前端通道端口类型；配置≥8\*16Gb FC接口（FC接口满配多模光模块） |
| 配置硬盘 | 配置企业级 SSD硬盘（SAS接口，非SATA接口），配置≥24块SSD硬盘，单盘容量≥1.92TB；SAS 10K RPM硬盘配置裸容量≥194T，单盘容量≥1.8TB。最大支持磁盘插槽个数≥480 |
| 支持RAID | 支持RAID 1、RAID 10、RAID50、RAID 5、RAID6等可选配置。 |
| SAN功能特性 | 配置精简配置功能；配置数据迁移功能，支持存储系统内和存储系统间的业务数据在线迁移，兼容异构存储间数据迁移，配置相应许可。配置数据分层功能，提供图形化的自动分层策略调整工具，能够对数据分层的时间窗口和分层方式进行调整。提供SSD、SAS、NL-SAS三级分级配置界面截图。可支持QoS功能，提供图像化管理界面, 能够按照IOPS、吞吐量、响应时间等维度进行策略调整。 |
| 双活功能 | 配置存储双活功能1）提供双活架构，实现两套核心存储数据双活，任何一套设备宕机均不影响上层业务系统运行（业务不中断）。提供权威第三方检测报告。2）双活架构需要配置独立的仲裁设备。仲裁设备故障时，不影响业务运行，同时双活卷仍能保持数据实时一致；3）配置无限容量的双活许可。 |
| 数据压缩功能 | 具备数据压缩功能（响应时需要明确实现方式） |
| 可靠性 | 磁盘、电源可不停机热插拔 |
| 多路径软件 | 支持多路径软件 |
| 服务 | 提供五年原厂维保服务；提供原厂存储双活实施服务； |

**3.2虚拟化平台存储（2台）**

|  |  |
| --- | --- |
| **指标项** | **配置及参数要求** |
| 品牌 | 国产知名品牌 |
| 控制器 | 配置双活控制器（非AP模式），支持控制器扩展，最大支持≥4控，提供相关功能证明截图或第三方测试报告。每个控制器物理CPU核心数不少于10核 |
| 存储缓存容量 | 缓存容量配置≥256GB（不含性能加速卡或SSD缓存等） |
| 前端主机通道接口 | 支持8/16/32Gbps FC作为前端通道端口类型；配置≥8\*16Gb FC接口（FC接口满配多模光模块） |
| 配置硬盘 | 配置企业级 SSD硬盘（SAS接口，非SATA接口），配置≥18块SSD硬盘，单盘容量≥1.92TB；SAS 10K RPM硬盘配置裸容量≥162T，单盘容量≥1.8TB最大支持磁盘插槽个数≥480 |
| 支持RAID | 支持RAID 1、RAID 10、RAID50、RAID 5、RAID6等可选配置。 |
| SAN功能特性 | 配置精简配置功能；配置数据迁移功能，支持存储系统内和存储系统间的业务数据在线迁移，兼容异构存储间数据迁移，配置相应许可。配置数据分层功能，提供图形化的自动分层策略调整工具，能够对数据分层的时间窗口和分层方式进行调整。提供SSD、SAS、NL-SAS三级分级配置界面截图。可支持QoS功能，提供图像化管理界面, 能够按照IOPS、吞吐量、响应时间等维度进行策略调整。 |
| 双活功能 | 配置存储双活功能1）提供双活架构，实现两套核心存储数据双活，任何一套设备宕机均不影响上层业务系统运行（业务不中断）。提供权威第三方检测报告。2）双活架构需要配置独立的仲裁设备。仲裁设备故障时，不影响业务运行，同时双活卷仍能保持数据实时一致；3） 配置无限容量的双活许可。 |
| 数据压缩功能 | 具备数据压缩功能（响应时需要明确实现方式） |
| 可靠性 | 磁盘、电源可不停机热插拔 |
| 多路径软件 | 支持多路径软件 |
| 服务 | 提供五年原厂维保服务；提供原厂存储双活实施服务； |

**3.3数据库服务器（4台）**

|  |  |
| --- | --- |
| **指标项** | **配置及参数要求** |
| 品牌 | 国产知名品牌 |
| 形态 | 2U 4路机架服务器 |
| CPU | INTEL 6248\*4（不低于） |
| 内存实配规格 | 16\*32G ECC DDR4内存 |
| 实配硬盘 | 6\*1.8TB SAS 10k 硬盘 |
| 阵列控制器 | SAS RAID阵列卡；2GB缓存 |
| PCI I/O插槽 | 提供≥6个标准PCIE3.0插槽 |
| 网卡 | 配置4个万兆光口（含光模块） |
| HBA卡 | 2块双口16Gb HBA卡（含光模块） |
| NVME固态盘 | PCI-E接口，不少于7TB，读带宽不少于5GB/S |
| 电源 | 满配热插拔冗余电源 |
| 风扇 | 满配热插拔冗余风扇 |
| 产品资质 | 中国环境标志产品认证证书（中国） |
| 服务 | 五年原厂商质保服务 |

**3.4虚拟机服务器（12台）**

|  |  |
| --- | --- |
| **指标项** | **配置及参数要求** |
| 品牌 | 国产知名品牌 |
| 形态 | 2U 2路机架服务器 |
| CPU | INTEL 5218\*2（不低于） |
| 内存实配规格 | 16\*32G ECC DDR4内存 |
| 实配硬盘 | 3\*600GB SAS 10k 硬盘 |
| 阵列控制器 | SAS RAID阵列卡；2GB缓存 |
| PCI I/O插槽 | 提供≥6个标准PCIE3.0插槽 |
| 网卡 | 配置4个万兆光口（含光模块） |
| HBA卡 | 2块双口16Gb HBA卡（含光模块） |
| 电源 | 满配热插拔冗余电源 |
| 风扇 | 满配热插拔冗余风扇 |
| 产品资质 | 中国环境标志产品认证证书（中国） |
| 服务 | 五年原厂商质保服务 |

**3.5 GPU服务器（1台）**

|  |  |
| --- | --- |
| **指标项** | **配置及参数要求** |
| 品牌 | 国产知名品牌 |
| 形态 | 2U 2路机架服务器 |
| CPU | INTEL 4210R\*2（不低于） |
| 内存实配规格 | 2\*32G ECC DDR4内存 |
| 实配硬盘 | 4\*2.4TB SAS 10K 硬盘 |
| 阵列控制器 | 独立阵列卡 |
| PCI I/O插槽 | 提供≥6个标准PCIE3.0插槽 |
| GPU | 配置Tesla GPU板卡，显存≥32G |
| HBA卡 | 1块双口16Gb HBA卡（含光模块） |
| 电源 | 满配热插拔冗余电源 |
| 风扇 | 满配热插拔冗余风扇 |
| 产品资质 | 中国环境标志产品认证证书（中国） |
| 服务 | 五年原厂商质保服务 |

**3.6光纤交换机（2台）**

|  |  |
| --- | --- |
| **指标项** | **配置及参数要求** |
| 类型 | 原厂生产，非OEM |
| 指标 | 单台光纤交换机最大支持≥48个端口，冗余电源。 |
| 激活48端口，配置48个16Gb/s短波SFP模块 |
| 光纤交换机架构为无阻塞，全线速最大16Gbps |
| 所有的端口上均可进行全光纤网络操作和通用端口操作 |
| 光纤交换机最大交换能力为≥768 Gbit/sec  |
| 支持基于帧的干线合并，每条ISL干线最多8个16 Gbit/sec端口；每条ISL干线最高速率达128 Gbit/sec (8端口×16 Gbit/sec [线速]) |
| 支持光纤通道(FC)集成路由功能 |
| 支持高级分区、Web 工具的智能管理和监控、Fabric Watch 和性能监控功能。 |
| 支持Acess Gateway工作模式 |
| 支持WINDOWS、LINUX、AIX、HP-UNIX等操作系统，支持IBM、HP、富士通、HDS等主流厂商的存储阵列。 |
| 支持Telnet、HTTP、SNMP管理 |
| 五年原厂保修 |

**3.7备份一体机扩容（1台）**

爱数VX820备份一体机增扩8块8TB NL-SAS 7200转硬盘及相应的软件许可。

**3.8服务器网卡扩容（6块）**

适用于联想及HPE服务器，双端口万兆网卡（含2个万兆光纤模块）及相应配件。

**3.9核心交换机（1台）**

|  |  |
| --- | --- |
| **指标** | **规格要求** |
| 设备性能 | 交换容量≥38.4Tbps、包转发率≥7200Mpps（以官网低指标为准，官网参数若标注为交换容量“A/B”，以A/B中更小值为准）；配置主控引擎模块≥2，满足1+1冗余、冗余电源，业务槽位数≥3，万兆光口≥32，千兆电口≥48，32个万兆多模模块； |
| 接口要求 | 单槽位能够同时提供千兆光口、千兆电口、万兆光口，且实际可用端口总数≥48，提高槽位利用率和业务可靠性 |
| 多业务融合化 | 支持扩展硬件防火墙业务板、IPS入侵防御系统业务板、负载均衡业务板、应用控制网关业务板、SSL VPN业务板、EPON业务板 |
| 带宽控制 | 支持带宽控制，控制粒度<=64Kbps |
| 无线功能 | 支持无线控制器功能，包括精细的用户控制管理、完善的RF管理及安全机制、快速漫游、超强的QoS和对IPv6的支持等，为客户组建有线无线一体化网络的提供更丰富的选择。 |
| 虚拟化技术要求 | 1、多虚一技术(N:1)，支持4框虚拟化技术：可将4台物理设备虚拟化，实现流量负载分担功能，提供工信部权威第三方测试报告；2、支持有线无线统一管理功能，提供工信部权威第三方测试报告； |
| 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； |
| 认证协议特性 | 支持802.1X和802.1X Sever |
| 跨三层互联技术 | 支持主流的MAC in IP技术，如EVI，实现跨三层网络的二层互联， |
| 组播协议 | 支持GMRP、IGMP v1/v2/v3、IGMP v1/v2/v3 Snooping、PIM-DM、PIM-SM、PIM-SSM等协议支持MSDP，MLDv2/MLDv2 Snooping，PIM-SMv6、PIM-DMv6、PIM-SSMv6 |
| 路由协议 | 支持静态路由、RIP V1/V2、OSPF、BGP |
| IPv6 | 支持RIPng、OSPFv3、BGP4+、IS-ISv6协议支持IPv6策略路由；支持DHCPv6功能、IPv6 portal功能、IPv6管理功能；支持基于IPv6的VXLAN二三层互通；支持基于IPv6的VRRP功能 |
| 网管功能一体化 | 内置智能管理功能，支持通过图形化界面设备配置及命令一键下发和版本智能升级 |
| 生成树协议 | 支持IEEE 802.1d（STP）/802.1w（RSTP）/802.1s（MSTP）标准，支持BPDU guard， Root guard |
| 硬件加密技术 | 支持硬件级加密技术Macsec技术（802.1ae） |
| 可靠性 | 支持主控板冗余，倒换时间为0ms；支持BFD，BFD for VRRP/BGP/IS-IS/OSPF/RSVP/LDP/RIP/静态路由，BFD收敛时间<50ms；支持IP FRR，满足网络收敛<50ms |
| 设备管理 | 支持SNMP V1/V2/V3  |
| 运维管理软件 | 提供一站式智能运维界面，通过智能运维门户可以提供向导式的网络运维，设备管理、故障排查、维护大全、开局助手、控制台、云图、工具宝箱等功能，提供软件功能截图；提供故障排查及脚本管理功能，可通过选择故障设备、选择故障类型、确定前置条件，然后通过信息收集，信息分析，提供向导式解决方法； |
| 资质证书 | 提供工信部入网证书和检测报告； |

**3.10核心交换机扩容（一块）**

H3C S10500 核心交换机增扩一块48端口万兆以太网光接口板卡(SFP+,LC)(SG) ，含48个光模块。

**3.11下一代防火墙（2台）**

|  |  |
| --- | --- |
| **指标** | **规格要求** |
| 硬件架构 | 采用多核网络专用架构，使用64位MIPS多核处理器，非X86多核架构或ASIC架构 |
| 产品规格 | 标准1U专用千兆硬件平台，内置交流单电源，4G内存 |
| 网口数量 | 标准配置6个10/100/1000M自适应电口，4个千兆光口，1个Console口 |
| 性能 | 网络层吞吐量6G，并发连接≥200万，每秒新建连接数6万， |
| 双机热备 | 支持路由模式、透明模式的HA高可靠性部署，可工作于主备、主主模式，会话、用户、配置可实时同步；HA高可靠性部署支持接口联动，链路探测 |
| 访问控制 | 支持一体化安全策略：可基于设备接口/安全域、地址、服务、应用、用户、时间等属性，配置入侵防御、病毒防护、URL过滤、应用过滤、会话老化时间、终端过滤等高级访问控制功能。 |
| 用户认证 | 支持本地认证、Radius认证、LDAP认证 和LDAP用户同步 |
| SSL解密 | 支持对SSL协议进行解密，解密类型支持https和邮箱 |
| 流量管理 | 支持基于线路和多层通道嵌套的带宽管理和流量控制功能，提供至少四层管道嵌套；支持基于地址、用户、服务、应用、时间等匹配条件进行流量控制；并支持配置保障带宽、最大带宽、每IP带宽、每用户带宽、带宽优先级等QoS动作 |
| 支持带宽动态调整技术，带宽繁忙通道支持动态借用空闲通道的带宽，避免带宽浪费 |
| 入侵防御 | 系统定义主流攻击规则，包含用户提权、任意代码执行、木马、后门、挖矿、Web序列化、Webshell等主流防护类型。 |
| 所投产品的漏洞防护特征库包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云3”、“Struts”、“Struts2”、“Xshell后门代码”以及对应的攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息； |
| 病毒防护 | 支持HTTP，FTP，POP3，SMTP，IMAP协议的病毒查杀，支持查杀邮件正文/附件、网页及下载文件中包含的病毒，支持3000万余种病毒的查杀，并支持在线升级和手动升级病毒库 |
| 产品资质 | 具备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（增强级）》 |
| 具备中国信息安全认证中心颁发的《中国国家信息安全产品认证证书（增强级）》 |

**3.12堡垒机（1台）**

|  |  |
| --- | --- |
| **指标项** | **要求** |
| 硬件配置 | 软硬件一体化产品，1U、磁盘空间不少于1T、单电源、至少配备6个100/1000M自适应电口，至少配备4个千兆光口 |
| 可管理设备数量 | 可管理设备数量至少200个，运维用户无限制 |
| 并发性能 | 单台堡垒机字符类并发会话≥200个、图形类并发会话≥50个 |
| 设备部署 | 设备采用旁路部署，不得影响业务环境；须支持HA主备模式，管理口和心跳口须支持多链路端口绑定功能，防止单网卡或单线故障。 |
| 用户管理要求 | 支持用户多角色划分功能，如系统管理员、部门管理员、运维员、审计管理员、密码管理员等，对各类角色需要进行细粒度的权限管理。 |
| 支持用户的批量导入/导出，按用户类型等分组方式；支持用户安全策略功能，如密码锁定次数、密码有效期、密码复杂度、用户有效期、用户登录时间限制、用户登录IP范围等。 |
| 支持按部门组织架构（至少5个层级的部门）管理用户数据、资产数据、授权数据、审计数据。 |
| 每个部门可以管理本部门及下级部门的用户角色：部门管理员、运维管理员、审计管理员、运维员。 |
| 每个部门的部门管理员可以管理本部门及下级部门的主机、授权关系、策略。 |
| 每个部门的审计管理员可以管理本部门及下级部门的运维会话日志。 |
| 身份认证要求 | 支持本地、RADIUS和AD域等认证方式 |
| 支持与get、post、soap发送方式的http短信网关平台进行联动，实现短信动态口令双因素认证机制  |
| 支持手机APP动态口令认证方式登录堡垒机，且新用户首次登录后需强制绑定APP动态口令。 |
| 堡垒机须内嵌动态令牌和usbkey认证引擎，可同时使用动态令牌和USBkey |
| 基于不同的用户设置不同的双因子认证模式，如user1用动态令牌、user2用USBkey、user3手机APP动态口令认证 |
| 支持域认证与双因子认证结合使用，如同时使用AD/LDAP用户名+AD/LDAP密码+手机APP动态口令登录堡垒机、同时使用AD/LDAP用户名+AD/LDAP密码+短信口令登录堡垒机 |
| 支持认证窗口的全局设置：可以选择启用哪种或者哪几种认证登录窗口 |
| 设备管理要求 | 支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP、rlogin；可通过应用发布的方式进行协议扩展，如数据库Oracle、MSSQL、MySQL、VMware vSphere Client、浏览器等客户端工具 |
| 支持DB2、oracle、mysql、sqlserver主流数据库协议代理运维，可直接调用本地windows系统的数据库客户端工具，支持自动登录、无需应用发布前置机 |
| 支持以云盘形式在堡垒机上存储常用文件，实现操作端、堡垒机、目标服务器三者之间文件共享，提供相关截图 |
| 自动改密 | 支持定期自动修改windows服务器、网络设备、linux/unix等目标设备密码功能 |
| 运维审计日志 | 支持对运维操作会话的在线监控、实时阻断、日志回放、起止时间、来源用户、来源IP、目标设备、协议/应用类型、命令记录、操作内容（如对文件的上传、下载、删除、修改等操作等）的详细行为日志。 |
| 安全策略 | 支持通过基于时间、IP/IP段、用户/用户组、设备/设备组、设备账号、命令关键字、控制动作、黑白名单等组合访问控制策略，授权用户可访问的目标设备。 |
| 日志报表 | 内置丰富的报表统计模板，显示柱状图、曲线图，且支持多格式导出 |

**3.13综合日志审计系统（1台）**

|  |  |
| --- | --- |
| **指标项** | **要求** |
| 硬件规格 | 标准2U硬件、6个工作管理口（千兆电口），1个Console口；内存：8GB，磁盘：4T\*1（不支持raid）双电源；网口可扩展至10个（可扩展模块：4电、4光）； |
| 处理性能 | 支持审计100个日志源； 平均处理能力（每秒日志解析能力EPS）：4000 EPS；峰值处理能力（每秒日志解析能力EPS）：5000 EPS。 |
| 日志收集 | 支持Syslog、SNMP Trap、OPSec、FTP协议日志收集；支持使用代理(Agent)方式提取日志并收集；支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等； |
| 日志分析 | 可以以日志等级进行过滤；应该可以通过自定义配置将用户不关心的日志过滤掉；支持对收集到的重复的日志进行自动的聚合归并，减少日志量；支持可由用户定义和修改的日志的聚合归并逻辑规则；支持将收集到的日志转发，当原始日志设备无法设置多个日志服务器时，可以通过本系统的日志转发功能将日志转发到其他日志存储设备；支持对收集到的日志进行解析（标准化、归一化），解析规则可以根据客户要求定制扩展；可对日志进行细粒度解析，解析后的日志根据具体日志包含但不限于：日期、发生时间、接收时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作主体、操作对象、行为方式、技术动作、技术效果、攻击类型、特征类型、协议、地理信息（公网情况）；支持基于内存的实时关联分析，跨设备的多事件关联分析；支持自定义条件的事件进行聚合； |
| 日志备份 | 可设置日志存储备份策略。包括系统日志保存期（天）、磁盘使用率百分比；支持日志备份自动传送到远程服务器。 |
| 日志查询 | 支持B/S模式管理支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作对象、技术方式、技术动作、技术效果、攻击类型、地理城市等参数进行过滤查询；支持用任意关键字对所有事件进行高性能全文检索；支持可指定多个查询条件进行组合查询；支持将查询的条件存储为查询模版，方便再次使用；极高的日志高查询性能，支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果。 |
| 告警功能 | 可预设置安全告警策略；支持数据阀值设置，超过阀值将产生告警；可以通过邮件、短信和屏幕显示进行告警； |
| 日志实时分析和统计 | 可对收集的日志进行分类实时分析和统计，从而快速识别安全事故。分析统计结果支持柱图、饼图、曲线图等形式并自动实时刷新，图表数据支持数据下钻。日志实时分析在内存中完成，不需借助数据库和文件系统。 |
| 报表管理 | 提供丰富的报表管理功能。报表可以保存为excel，文本，pdf等多种格式。提供自定义报表。报表可根据设置自动运行,调度生成日报、周报和月报。 |

**3.14数据库审计系统（1台）**

|  |  |
| --- | --- |
| **指标项** | **要求** |
| 硬件指标 | 系统：产品采用专用工控机硬件架构，标准2U硬件，非普通PC服务器， MTBF(平均故障间隔时间)≥65000小时； 处理器：Intel高性能CPU；单电源内存≥16GB DDR3 1600Mhz，硬盘≥8T（4T\*2），支持RAID1，网络端口：支持监听接口扩展，配备至少2个千兆电口管理口；支持千兆网络环境下的监听能力，标配至少4个千兆电口和4个千兆光口； |
| 处理能力 | 审计性能：审计数据库数量无限制峰值SQL处理能力≥20,000条/秒;硬件最大吞吐量2000Mbps，最大纯数据库流量200Mbps，标配日志存储数20亿条；审计日志检索能力≥1500万条/秒。 |
| 部署方式 | 旁路部署模式下无须在被审计数据库系统上安装任何代理即可实现审计支持在目标数据库安装agent解决云环境、虚拟化环境内部流量无法镜像场景下数据库的审计. |
| 协议支持 | 支持Oracle、SQL-Server、DB2、Informix、Sybase、MySQL六种主流数据库审计；支持PostgreSQL、HANA、Teradata、Cache、人大金仓、达梦、南大通用数据库审计； 支持主流业务协议 HTTP、Telnet、FTP、SMTP、POP3、DCOM； |
| 审计功能 | 支持数据库操作类、表、视图、索引、存储过程等[各种对象的所有SQL操作审计](#_支持各种对象的SQL审计_1)旁路阻断功能（非串联方式）。阻断两种模式，宽松模式：对单一会话危险操作阻断；严格模式：源IP操作的所有请求直接阻断，提供截图 |
| 智能发现 | 自动识别流量中存在的数据库，也可通过扫描发现网络中的数据库支持定期自动扫描数据库漏洞和不安全配置，提供漏洞扫描报告； |
| 应用关联 (三层关联) | 支持B/S业务系统三层关联审计；支持通过部署agent实现java web环境100%准确关联；支持旁路自动学习三层审计关联功能 |
| 安全审计 | 支持审计记录中敏感数据的模糊化处理，内置常见敏感数据掩码规则，支持自定义内置安全特征库不少于300条，如SQL注入、缓冲区溢出等；可自定义审计规则，审计规则至少支持18个条件；规则各条件之间支持[与或非逻辑](#_支持与或非逻辑关联)关系； 告警数量需[支持最大告警数量限制](#_最大告警数限制)，超过告警阈值之后便不告警；告警查询应支持根据登陆用户、客户端工具名、客户端IP、规则进行归并分析，能详细展示每类告警占总告警数量百分比，便于告警分析处理 |
| 审计查询 | 具有高效的查询性能，支持全数据库检索，检索效率高达亿条数据秒级响应。支持采用部分匹配模糊查询方式检索审计日志支持基于数据库访问日期、时间、源/目的IP、来源、数据库名、数据库表名、字段值、数据库登陆账号、SQL关键词、数据库返回码、SQL响应时间、数据库操作类型、影响行数等条件的审计查询； |
| 统计报表 | 系统提供内置多种报表模板库报表支持严格按照塞班斯（SOX）法案、等级保护标准要求生成多维度综合报告；支持按照数据库访问行为生成报表，智能识别帐号的增删、权限变更、密码修改、特权操作等行为；支持按照时间曲线统计流量、在线用户数、并发会话、DDL操作数、DML操作数、执行量最多的SQL语句等报表； 支持[性能分析](#_按性能分析)，准确提炼出SQL语句执行频率和执行时间异常的报表；支持[Word、PDF](#_导出格式)等格式的报表导出；支持[报表自定义](#_报表自定义)。  |
| 系统管理 | 支持用户界面告警、Syslog、SNMP、邮件、短信、ftp六种方式告警；采用B/S架构管理，[支持中英文两种管理界面](#_中英文切换)支持[系统安全配置](#_系统安全配置)（会话锁定、超时退出、IP地址访问控制、密码复杂性管理、验证码登陆等措施）支持[NTP时间同步、SNMP](#_NTP、SNMP)(v1、V2、V3)网络管理协议 |

**3.15准入控制系统（1台）**

|  |  |
| --- | --- |
| **指标项** | **要求** |
| 规格要求 | 1U硬件设备，网络接口：至少具备6\*1000Mbps RJ45；可控上限：500 User；接口：2个USB2.0接口、1个RJ45串口 |
| 系统架构 | 标准采用B/S架构，便利易操作管理设计；提供断电保护机制，如心跳、Bypass等，确保异常时网络不受影响。 |
| 部署要求 | 设备支持旁路部署方式，避免串行设备部署导致单点故障设备部署过程中不改变原有网络结构及网络、安全等设备的配置； |
| 准入技术 | 针对复杂的网络接入环境，准入技术支持单独或组合使用的方式同时使用；可对网络划分不同的网络访问范围，至少能够划分合法用户访问范围、安全隔离用户访问范围、来宾用户访问范围，各范围可以根据实际需要进行修改；支持拓扑发现及展现功能，并可进行拓扑图的自定义绘制；支持重定向引导页面并能够详细描述被准入的原因。 |
| 违规外联管理 | 能够及时发现终端发生违规外联或具备外联的能力；违规外联后能够对违规终端进行报警提示操作 |
| 联动能力 | 支持与终端管理联动能力，支持大面积自动化部署终端管理，保证终端管理的安装覆盖率，防止卸载，规范终端入网流程，保障终端入网的安全可信 |
| 支持与防火墙产品联动，达到网关边界联动防御效果，提供截图 |
| 实时监测终端是否安装终端管理，快速引导安装，安装成功后执行合规检查，保障入网终端始终处于合规、可控范围内，实时上报安全动态及入网数据进行风险分析 |
| 安全测评 | 能够自动对入网终端进行安全项目检查，不符合安全规范的终端不允许接入网络，检查项目包括：网络监听端口、IP/MAC 绑定、ARP欺骗、恶意代码防范、操作系统补丁、来宾账户、口令安全、黑名单口令、Windows防火墙、超时锁屏登录、系统服务、远程桌面、系统时间、AD域环境、共享资源、telnet、红名单程序、黑名单程序等终端入网安全检测项； |
| 支持设置检测项目的关键项设置，关键项目必须检查通过的才能够接入网络； |
| 支持自动检测、循环评测、一键修复及后台自动修复功能。 |
| 报警项目 | 支持硬件变化报警、违规外联报警、未安装恶意代码防范程序报警、存在操作系统漏洞报警、ARP攻击报警、终端流量超出阈值报警等违规行为报警。 |
| 报警策略 | 能够对违规终端进行报警提示操作； |
| USB禁止使用 | 支持对存储类USB设备进行禁用，不影响非存储类USB外设使用；支持对USB接口使用进行只读或读写权限设置，禁止通过USB接口向外拷贝数据。 |
| 终端安全规范 | 支持禁用终端所有USB存储设备、便携式设备、光驱介质、无线网卡、3G无线上网卡、手机代理上网、调制解调器、蓝牙设备、其它网卡（除与服务器连接应用的网卡）、打印机等外接设备；支持IP/MAC绑定； |
| 补丁管理 | 支持对终端的补丁漏洞自动检测功能，能够汇总单独或全网终端的补丁漏洞信息；支持对补丁未安装的报警功能。 |

**3.16终端安全管理平台（1套）**

|  |  |
| --- | --- |
| **指标项** | **要求** |
| 基础架构及远程控制管理 | 控制中心：采用B/S架构管理端，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、统一漏洞修复、统一管控、统一终端准入合规、终端软件管理、硬件资产管理以及各种报表和查询等功能；支持多种主流浏览器：Microsoft Internet Explorer 7.0及以上、Google Chrome 谷歌浏览器（推荐）、Apple Safari 苹果浏览器、Mozilla Firefox 火狐浏览器等 |
| 升级管理功能 | 1、可以独立部署一个或多个升级服务器，多个服务器间支持自动平衡网络压力，支持树形级联升级，实现下一级服务从上级服务器升级，支持手动更新升级服务器内容，并以升级服务自身的内容为基础，制作定制安装包。2、可以同时配置多个升级源。允许自动匹配可用的多个升级地址升级。3、升级方式支持上传离线升级包、手动升级、自动升级、客户端游离到外网升级，并且可配置升级网络代理; 病毒库支持智能增量升级模式; 支持大型网络环境升级减压、错峰的随机延迟升级。 |
| 平台管理功能 | 客户端组件支持自我保护，包括相关进程防杀、相关服务防止卸载、修改，以及防止安装目录的文件被删除以及创建新的未知文件。客户端组件卸载或者停止工作有密码保护，防止任意卸载。且支持管理员自定义客户端显示的主、副产品标题。 |
| 防病毒功能 | 1)支持杀毒引擎支持多核cpu的并行计算，可手动配置选择引擎，也可根据客户端环境智能选择引擎，适当的环境选用适当的方案。加快查杀效率提高文件扫描速度,支持公有云、私有云查杀，病毒检测及清除能力达到公安部一级品认证标准。 |
| 2)通过P2P扫描技术，初次对虚拟机模板扫描后，后续对虚拟主机扫描采用增量扫描，降低资源消耗，优化系统使用。 |
| 3)支持智能主动防御技术，提供基于保护系统安全的系统加固功能和保护应用程序的应用加固功能。支持文件监控、邮件监控，可远程集中式查看监控状态及开关监控。支持U盘监控，可在U盘刚接入时就进行一次安全扫描，确保接入环境的U盘安全。 |
| 4)支持可查杀OFFICE宏病毒，支持网络下载文件的病毒实时查杀、支持族群式变种病毒的查杀。 |
| 5) 支持扫描模式包括快速扫描、全盘扫描、自定义扫描；并且管理员可以在控制台上远程查看客户端扫描状态信息、并控制快速扫描或者全盘扫描的扫描过程；支持单独给全盘扫描、快速扫描设置定时查杀任务；支持用户拖拽扫描，方便用户及时手动扫描可疑文件，对已染毒文件，管理员可以在中心控制台远程恢复可能误杀的文件，自定义白名单、排除列表，提交企业内部防护效率。 |
| 6)支持根据监控状态、未执行扫描状态以及根据计算机名称、IP地址等信息快速查找计算机，方便更有针对性的进行全网管理，可远程锁定客户端用户不能关闭监控功能，提高全网安全，支持引导扇区和主引导记录区备份和恢复 |
| 补丁分发与漏洞修复 | 产品具备漏洞集中修复，强制修复，自动修复；具备蓝屏修复功能，提供截图 |
| 终端支持智能屏蔽过期补丁、与操作系统不兼容的补丁，可以查看或搜索系统已安装的全部补丁；  |
| 文档操作和审计功能 | 支持文档操作和审计功能，可以审计记录客户端对U盘、网络盘或指定磁盘位置的文件的复制、删除、打印等文件操作，并统一汇总在控制台上；支持跟踪操作到用户（非计算机），提供按用户名统计查看。可以记录共享的文件夹被其他终端的访问情况，记录内容包括资源名称、IP、访问动作（读、写）；可强制关闭终端的系统默认共享或者远程管理 |
| XP防护 | 支持针对Windows XP系统可带来安全隐患的设计机制进行加固性修复，支持远程漏洞攻击防护、本地钓鱼攻击防护和浏览器漏洞攻击防护；提供截图。 |
| U盘审计与统一管理 | 支持U盘的使用审计与统一管理：可以禁止使用未登记的U盘、允许使用已经登记的U盘、禁止使用已经登记的U盘；  |
| 网络安全审计 | 网络安全审计：可对不符合以下检测规则的终端进行网络隔离，防止其访问其他网络资源；IP地址管理和ARP防护客户端IP防篡改，防止终端用户自己随意更改本机IP地址；防止本机发ARP欺骗包，并检测内网的恶意ARP欺骗包；本机IP保护功能，可以防止IP地址冲突时，本机网络断开； |
| 产品资质 | 具有公安部安全产品销售许可证书且标注为一级品； |

**4、集成实施服务要求**

**4.1总体要求**

1）本项目属于“交钥匙”工程，即所提供的软、硬件产品按招标方的要求采购、安装、调试。本次项目中要求中标人针对采购人提供数据库改造迁移服务、存储数据迁移等服务，协助采购方完成于本次项目相关的系统调整和优化等工作，中标方须提供项目集成实施服务，并提供五年售后免费现场技术支持服务，中标方须对系统集成的完整性负责，如相关配件在招标清单中未列出但安装所采购设备时须用到，中标人须提供，产生的一切费用，均由中标方负责。

2）项目实施期间发生的所有劳务支出、安全保险、住宿、运输、税金、验收等一切费用都已包含在~~竞~~投标报价中，由中标方自行负责。

3）投标人须具有数据库迁移项目实施经验（提供相应的合同复印件等证明材料），投标人具有Oracle OCP或以上认证的数据库工程师。

**4.2具体实施要求**

1）完成设备安装、上电、测试、初始化配置等工作，需满足客户环境的实际需求。

2）中标方需确保新购部件许可，能与甲方现有环境兼容，并满足项目功能需求，不得影响甲方现有业务系统的稳定运行。

3）至少完成5套Oracle数据库改造及迁移工作、7套数据库的在线迁移工作，最终数据库改造迁移数量以采购人实际需求为准。

4）新购服务器加入原有虚拟机环境，完成应用迁移工作。

5）完成系统测试等相关工作。

**4.3售后服务要求**

1）对所提交的设备提供自“终验合格”签署之日起5年的免费质保期（扩容设备除外）。

2）在质保期内均提供7\*24小时上门维护、升级服务，对故障即时响应，6小时以内到现场，到达现场后2小时以内提出问题解决方案并实施,在故障发生后12小时内解决问题。逾期未作出响应，投标人应承担由于故障所造成的全部损失。质保期内产生的维护费用均由投标人承担。

**4.4技术培训**

根据实际项目实施，提供用户的现场技术培训，包括产品的功能、部署条件、部署步骤和注意事项、产品升级、日常维护事项等方面，使用户达到能独立进行管理、维护测试和故障处理等工作，以使所提供的软硬件产品能够正常、安全的运行。

所有培训所涉及的所有费用应由中标人出资，不得另行向采购人收取。

**4.5验收要求**

中标人应负责在项目工程实施完成时将系统的全部有关技术文件、图表资料及测试、验收报告等文档汇集成册交付采购人，包括但不限于以下文档：

项目投标文件

项目实施方案

产品安装实施报告

系统测试报告

项目完工总结报告

系统安装维护手册

其他所有项目实施过程中产生的文档。

**三、商务需求**

**1、质保期：**

**第一标段：**原厂质保五年。

**第二标段：**原厂质保五年。

**2、交货时间及地点：**同前面“招标项目一览表”内所填的相关内容。

**3、付款条件**：

第一标段：合同签订完成后10个工作日内，支付合同总价的60%；项目初验后10个工作日内支付合同总价的20%；项目终验后10个工作日内支付合同总价的20%。

第二标段：合同签订完成后10个工作日内，甲方支付合同总价的60%；设备到货清点初验合格后支付合同总价的30%，项目通过竣工验收后，30个工作日内支付合同总价的10%。

**四、相关说明**

**1、现场勘察：**无

**2、项目对接费用：无**

1. **政府采购合同主要条款指引**

**货物类**

以下为成交后签定本项目合同的通用条款，成交供应商不得提出实质性的修改，关于专用条款将由采购人与成交供应商结合本项目具体情况协商后签订。

项目名称： 项目编号：

甲方：（采购单位） 所在地：

乙方：（中标供应商） 所在地：

甲、乙双方根据××(采购组织机构名称）关于××单位××项目公开招标的结果，签署本合同。

一、合同文件：

1.合同条款。

2.中标通知书。

3.更正补充文件。

4.招标文件。

5.中标供应商投标文件。

6.其他。

上述所指合同文件应认为是互相补充和解释的，但是有模棱两可或互相矛盾之处，以其所列内容顺序为准。

**二、货物内容**

1. 货物名称：

2. 型号规格：

3. 技术参数：

4. 数量（单位）：

**三、合同金额**

 本合同金额为（大写）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_元（￥\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_元）人民币。

**四、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货物的有关技术资料。

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。

**五、知识产权**

1.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。

2.若侵犯,由乙方赔偿甲方因此遭受的损失（包括但不限于应对及追偿过程中所支付的律师费、差旅费、诉讼费、保全费、鉴定费、评估费等）。

**六、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。

**七、履约保证金**

本项目履约保证金为合同金额的\_5\_%。[履约保证金交至采购人处，在项目质保期满且无违约扣除情况后30个工作日内无息退还]

**八、转包或分包**

1.本合同范围的货物，应由乙方直接供应，不得转让他人供应；

2.除非得到甲方的书面同意，乙方不得将本合同范围的货物全部或部分分包给他人供应；

3.如有转让和未经甲方同意的分包行为，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。

**九、质保期**

1. 质保期\_\_\_年。（自交货验收合格之日起计）

**十、交货期、交货方式及交货地点**

1. 交货期：

2. 交货方式：

3. 交货地点：

**十一、货款支付**

1. 付款方式：

2.当采购数量与实际使用数量不一致时，由采购单位向同级财政部门申请并经批准后，可以由乙方根据实际使用量供货，合同的最终结算金额按实际使用量乘以成交单价进行计算。

**十二、税费**

本合同执行中相关的一切税费均由乙方负担。

**十三、质量保证及售后服务**

1. 乙方应按招标文件规定的货物性能、技术要求、质量标准向甲方提供未经使用的全新产品。

2. 乙方提供的货物在质保期内因货物本身的质量问题发生故障，乙方应负责免费更换。对达不到技术要求者，根据实际情况，经双方协商，可按以下办法处理：

⑴更换：由乙方承担所发生的全部费用。

⑵贬值处理：由甲乙双方合议定价。

⑶退货处理：乙方应退还甲方支付的合同款，同时应承担该货物的直接费用（运输、保险、检验、货款利息及银行手续费等）。

3. 如在使用过程中发生质量问题，乙方在接到甲方通知后在 小时内到达甲方

现场。

4. 在质保期内，乙方应对货物出现的质量及安全问题负责处理解决并承担一切

费用。

5.上述的货物免费保修期为年，因人为因素出现的故障不在免费保修范围

内。超过保修期的机器设备，终生维修，维修时只收部件成本费。

**十四、调试和验收**

1. 甲方对乙方提交的货物依据招标文件上的技术规格要求和国家有关质量标准

进行现场初步验收，外观、说明书符合招标文件技术要求的，给予签收，初

步验收不合格的不予签收。货到后，甲方需在五个工作日内验收。

2. 乙方交货前应对产品作出全面检查和对验收文件进行整理，并列出清单，作

为甲方收货验收和使用的技术条件依据，检验的结果应随货物交甲方。

3. 甲方对乙方提供的货物在使用前进行调试时，乙方需负责安装并培训甲方的

使用操作人员，并协助甲方一起调试，直到符合技术要求，甲方才做最终验

收。

4.对技术复杂的货物，甲方应请国家认可的专业检测机构参与初步验收及最终

验收，并由其出具质量检测报告。

5.验收时乙方必须在现场，验收完毕后作出验收结果报告；验收费用由甲方负

责。

**十五、货物包装、发运及运输**

1. 乙方应在货物发运前对其进行满足运输距离、防潮、防震、防锈和防破损装卸等要求包装，以保证货物安全运达甲方指定地点。

2. 使用说明书、质量检验证明书、随配附件和工具以及清单一并附于货物内。

3. 乙方在货物发运手续办理完毕后24小时内或货到甲方48小时前通知甲方，以准备接货。

4. 货物在交付甲方前发生的风险均由乙方负责。

5. 货物在规定的交付期限内由乙方送达甲方指定的地点视为交付，乙方同时需

通知甲方货物已送达。

6.乙方运送的货物涉及商品包装和快递包装的，参考《商品包装政府采购需求标准（试行）》、《快递包装政府采购需求标准（试行）》(财办库〔2020〕123号)

**十六、违约责任**

1. 甲方无正当理由拒收货物的，甲方向乙方偿付拒收货款总值的百分之五违约金。

2. 甲方无故逾期验收和办理货款支付手续的,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. 乙方逾期交付货物的，乙方应按逾期交货总额每日千分之六向甲方支付违约金，由甲方从待付货款中扣除。逾期超过约定日期10个工作日不能交货的，甲方可解除本合同。乙方因逾期交货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.若发生纠纷，由违约方赔偿守约方因纠纷所支付的费用（包括但不限于律师费、差旅费、诉讼费、保全费、鉴定费、评估费等）

**十七、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。

**十八、解决争议的方法**

1. 如双方在履行合同时发生纠纷，应协商解决；协商不成时，可提请政府采购管理部门调解；调解不成的通过以下方式解决（两种解决方式只能择其一）：
（1） 提交台州仲裁委员会仲裁。
（2） 依法向人民法院提起诉讼。

**十九、合同生效及其它**

1. 合同经双方法定代表人或授权代表签字并加盖单位公章后生效。

2. 本合同未尽事宜，遵照《合同法》有关条文执行。

3. 本合同一式四份。甲、乙双方各执一份，采购组织机构及同级人民政府财政部门各执一份。本项目未尽事宜以招标文件、投标文件及澄清文件等为准。

甲方（公章） 乙方（公章）

法定代表人： 法定代表人：

委托代理人： 委托代理人：

联系电话： 联系电话：

开户银行： 开户银行：

帐号： 帐号：

地址及邮编： 地址及邮编：

签订时间： 年 月 日

**服务类**

以下为成交后签定本项目合同的通用条款，成交供应商不得提出实质性的修改，关于专用条款将由采购人与成交供应商结合本项目具体情况协商后签订。

项目名称： 项目编号：

甲方：（采购单位） 所在地：

乙方：（中标供应商） 所在地：

甲、乙双方根据××(采购组织机构名称）关于××单位××项目公开招标的结果，签署本合同。

一、合同文件：

1.合同条款。

2.中标通知书。

3.更正补充文件。

4.招标文件。

5.中标供应商投标文件。

6.其他。

上述所指合同文件应认为是互相补充和解释的，但是有模棱两可或互相矛盾之处，以其所列内容顺序为准。

**二、货物内容**

1. 货物名称：

2. 型号规格：

3. 技术参数：

4. 数量（单位）：

**三、合同金额**

 本合同金额为（大写）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_元（￥\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_元）人民币。

**四、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货物的有关技术资料。

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。

**五、知识产权**

1.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。

2.若侵犯,由乙方赔偿甲方因此遭受的损失（包括但不限于应对及追偿过程中所支付的律师费、差旅费、诉讼费、保全费、鉴定费、评估费等）。

**六、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。

**七、履约保证金**

中标后签订合同前5个工作日内，乙方需支付甲方合同金额的5%作为履约保证金，甲方在质保期满后5个工作日内退还乙方。

**八、转包或分包**

1.本合同范围的货物，应由乙方直接供应，不得转让他人供应；

2.除非得到甲方的书面同意，乙方不得将本合同范围的货物全部或部分分包给他人供应；

3.如有转让和未经甲方同意的分包行为，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。

**九、质保期**

1. 质保期\_\_\_年。（自交货验收合格之日起计）

**十、交货期、交货方式及交货地点**

1. 交货期：

2. 交货方式：

3. 交货地点：

**十一、货款支付**

1. 付款方式：

2.当采购数量与实际使用数量不一致时，由采购单位向同级财政部门申请并经批准后，可以由乙方根据实际使用量供货，合同的最终结算金额按实际使用量乘以成交单价进行计算。

**十二、税费**

本合同执行中相关的一切税费均由乙方负担。

**十三、质量保证及售后服务**

1. 乙方应按招标文件规定的货物性能、技术要求、质量标准向甲方提供未经使用的全新产品。

2. 乙方提供的货物在质保期内因货物本身的质量问题发生故障，乙方应负责免费更换。对达不到技术要求者，根据实际情况，经双方协商，可按以下办法处理：

⑴更换：由乙方承担所发生的全部费用。

⑵贬值处理：由甲乙双方合议定价。

⑶退货处理：乙方应退还甲方支付的合同款，同时应承担该货物的直接费用（运输、保险、检验、货款利息及银行手续费等）。

3. 如在使用过程中发生质量问题，乙方在接到甲方通知后在 小时内到达甲方

现场。

4. 在质保期内，乙方应对货物出现的质量及安全问题负责处理解决并承担一切

费用。

5.上述的货物免费保修期为年，因人为因素出现的故障不在免费保修范围

内。超过保修期的机器设备，终生维修，维修时只收部件成本费。

**十四、调试和验收**

1. 甲方对乙方提交的货物依据招标文件上的技术规格要求和国家有关质量标准

进行现场初步验收，外观、说明书符合招标文件技术要求的，给予签收，初

步验收不合格的不予签收。货到后，甲方需在五个工作日内验收。

2. 乙方交货前应对产品作出全面检查和对验收文件进行整理，并列出清单，作

为甲方收货验收和使用的技术条件依据，检验的结果应随货物交甲方。

3. 甲方对乙方提供的货物在使用前进行调试时，乙方需负责安装并培训甲方的

使用操作人员，并协助甲方一起调试，直到符合技术要求，甲方才做最终验

收。

4.对技术复杂的货物，甲方应请国家认可的专业检测机构参与初步验收及最终

验收，并由其出具质量检测报告。

5.验收时乙方必须在现场，验收完毕后作出验收结果报告；验收费用由甲方负

责。

**十五、货物包装、发运及运输**

1. 乙方应在货物发运前对其进行满足运输距离、防潮、防震、防锈和防破损装卸等要求包装，以保证货物安全运达甲方指定地点。

2. 使用说明书、质量检验证明书、随配附件和工具以及清单一并附于货物内。

3. 乙方在货物发运手续办理完毕后24小时内或货到甲方48小时前通知甲方，以准备接货。

4. 货物在交付甲方前发生的风险均由乙方负责。

5. 货物在规定的交付期限内由乙方送达甲方指定的地点视为交付，乙方同时需

通知甲方货物已送达。

**十六、违约责任**

1. 甲方无正当理由拒收货物的，甲方向乙方偿付拒收货款总值的百分之五违约金。

2. 甲方无故逾期验收和办理货款支付手续的,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. 乙方逾期交付货物的，乙方应按逾期交货总额每日千分之六向甲方支付违约金，由甲方从待付货款中扣除。逾期超过约定日期10个工作日不能交货的，甲方可解除本合同。乙方因逾期交货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.若发生纠纷，由违约方赔偿守约方因纠纷所支付的费用（包括但不限于律师费、差旅费、诉讼费、保全费、鉴定费、评估费等）

**十七、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。

**十八、解决争议的方法**

1. 如双方在履行合同时发生纠纷，应协商解决；协商不成时，可提请政府采购管理部门调解；调解不成的通过以下方式解决（两种解决方式只能择其一）：
（1） 提交台州仲裁委员会仲裁。
（2） 依法向人民法院提起诉讼。

**十九、合同生效及其它**

1. 合同经双方法定代表人或授权代表签字并加盖单位公章后生效。

2. 本合同未尽事宜，遵照《合同法》有关条文执行。

3. 本合同一式四份。甲、乙双方各执一份，采购组织机构及同级人民政府财政部门各执一份。本项目未尽事宜以招标文件、投标文件及澄清文件等为准。

甲方（公章） 乙方（公章）

法定代表人： 法定代表人：

委托代理人： 委托代理人：

联系电话： 联系电话：

开户银行： 开户银行：

帐号： 帐号：

地址及邮编： 地址及邮编：

签订时间： 年 月 日

1. **投标文件格式附件**

**附件1**  　　　本

项目名称

项目编号：（标段）

投

标

文

件

（**资格证明文件）**

投标人全称（电子印章）：

地 址：

时 间：

**资格证明文件目录**

1. 声明书（附件2）
2. 授权委托书（附件3）
3. 法人或者其他组织的营业执照等证明文件，自然人的身份证明

4、财务状况报告，依法缴纳税收和社会保障资金的相关材料

5、具备履行合同所必需的设备和专业技术能力的证明材料

6、本项目要求的特定资质证书

**附件2**

**投标声明书**

××（集中采构机构/采购代理机构名称）：

（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，我公司自愿参加贵方组织的（招标项目名称）（编号为）的投标，为此，我公司就本次投标有关事项郑重声明如下：

1. 我公司声明截止投标时间近三年以来：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及其他不符合《中华人民共和国政府采购法》第二十二条规定的条件。【说明：供应商在截止投标时间近三年以来，如有上述所列情形，但限制期届满的，可按实陈述，并提供相应证明文件。】

2、我公司在参与投标前已详细审查了招标文件和所有相关资料，我方完全明白并认为此招标文件没有倾向性，也没有存在排斥潜在投标人的内容，我方同意招标文件的相关条款，放弃对招标文件提出误解和质疑的一切权利。

3、我公司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。

4、我公司保证，采购人在中华人民共和国境内使用我公司投标货物、资料、技术、服务或其任何一部分时，享有不受限制的无偿使用权，如有第三方向采购人提出侵犯其专利权、商标权或其它知识产权的主张，该责任由我方承担。我方的投标报价已包含所有应向所有权人支付的专利权、商标权或其它知识产权的一切相关费用。

5、我公司严格履行政府采购合同，不降低合同约定的产品质量和服务，不擅自变更、中止、终止合同，或拒绝履行合同义务；

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

 投标人名称(电子印章)：

 法定代表人或授权委托人(签字)：

 日期：××年 ×× 月 ×× 日

**附件3**

**授权委托书**

××（集中采构机构/采购代理机构名称）：

 （投标人全称） 法定代表人（或营业执照中单位负责人） （法定代表人或营业执照中单位负责人姓名） 授权 （全权代表姓名） 为全权代表，参加贵单位组织的 项目的采购活动，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。我方对全权代表的签字事项负全部责任。

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

全权代表无转委托权，特此委托。

法定代表人签字或盖章：

投标人全称（电子印章）： 日期：

**附：**

|  |
| --- |
| **法定代表身份证复印件粘帖处** |

法定代表人姓名：

传真：

电话：

详细通讯地址：

邮政编码：

|  |
| --- |
| **全权代表身份证复印件粘帖处** |

全权代表姓名：

职务：

传真：

电话：

详细通讯地址：

邮政编码：

**附件4：**

项目名称

项目编号：（标段）

投

标

文

件

（商务与技术文件**）**

投标人全称（电子印章）：

地 址：

时 间：

**商务与技术文件目录**

**第一部分 技术方案描述部分**

1、投标人情况介绍（附件5）；

2、项目需求的理解与分析；

3、项目组织实施方案(可视情选用附件6、附件7)；

4、安装、调试及验收方案；

**第二部分 投标产品描述部分**

1、投标产品描述及相关资料（可视情选用附件8、附件9）；

2、投标人需要说明的其他内容；（包括可能影响投标人技术性能评分项的各类证明材料）

**第三部分 商务响应部分**

1、证书一览表（附件10）；

2、近三年来类似项目的成功案例（附件11）；

3、售后服务描述及承诺（可视情选用附件12，附件13）；

4、投标人需要说明的其他内容。（包括可能影响投标人企业实力及信誉评分项以及售后服务评分项的各类证明材料）

**第四部分 其他参考表格（此部分视情况选用）**

1、主要货物用材响应表(类似家具类货物采用，附件14)

（以上内容具体描述详见“第三部分投标人须知”中“三、投标文件”的组成说明）

**附件5**

 **投标人基本情况表**

|  |  |  |  |
| --- | --- | --- | --- |
| 企业名称 |  | 法人代表 |  |
| 地址 |  | 企业性质 |  |
| 股东姓名 |  | 股权结构（%） |  | 股东关系 |  |
| 联系人姓名 |  | 固定电话 |  | 传真 |  |
| 手机 |  |
| 1.企业概况 | 职工人数 |  | 具备大专以上学历人数 |  | 国家授予技术职称人数 |  |
| 占地面积 |  | 建筑面积 | 平方米 □自有□租賃 | 生产经营场所及场所的设施与设备 |  |
| 注册资金 |  | 注册发证机关 |  | 公司成立时间 |  |
| 核准经营范围 |  |
| 发展历程及主要荣誉： |
| 2．企业有关资质获证情况 | 产品生产许可证情况（对需获得生产许可证的产品要填写此栏） | 产品名称 | 发证机关 | 编号 | 发证时间 | 期限 |
|  |  |  |  |
| 企业通过质量体系、环保体系、计量等认证情况 |  |
| 企业获得专利情况 |  |

**要求：**

1.姓名栏必须将所有股东都统计在内，若非股份公司此行（第三行）无需填写；

投标人名称（电子印章）：

投标人代表签字或盖章：

职 务：

日 期：：

**附件6**

**项目实施人员一览表（第 标）**

（主要从业人员及其技术资格）

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **姓名** | **职务** | **职责** | **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** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**要求：**

**1.**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。

2.附人员证书复印件；

　　3.出具上述人员在本单位服务的外部证明，如：投标截止日之前六个月以内的代缴个税税单、参加社会保险的《投保单》或《社会保险参保人员证明》等。

投标人名称（电子印章）：

投标人代表签字或盖章：

职 务：

日 期：

**附件7**

**项目负责人资格情况表**

采购项目： 采购编号：

|  |  |  |
| --- | --- | --- |
| **姓名** |  | **近年来主要工作业绩** |
| **性别** |  | 注：业绩证明应提供旁证材料（供货合同或中标通知书）。 |
| **年龄** |  |
| **职称** |  |
| **毕业时间** |  |
| **学校专业** |  |
| **联系电话** |  |
| **最近一年工作状况** |  |
| **拟在本项目中担任主要工作** |  |

投标人名称（电子印章）：

投标人代表签字或盖章：

职 务：

日 期：

**附件8**

**供货清单 (第 标)**

 项目编号：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **品牌** | **规格型号** | **产地** | **数量** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**要求：**

**1.**本表中的名称、数量应与报价明细表中相对应的报价名称、数量一致

投标人名称（电子印章）：

投标人代表签字或盖章：

职 务：

日 期：

**附件9**

技术需求响应表**(第 标)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **规格型号** | **招标参数** | **投标参数** | **偏离说明** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**要求：**

1. 本表的名称须与《报价明细表》一致。

2.本表参照本招标文件第二部分“招标需求”内第二条“具体技术需求”填制，投标人应根据投标设备的性能指标、服务指标，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”。

3.对于投标产品的技术偏离情况需严格按照招标文件的技术要求一一比对给出，未达到技术要求中规定的数值应以负偏离标注。若因技术实现方式等其他问题而导致的理解不同未标注负偏离的，需在备注中具体说明；若未按要求标注负偏离又未予以说明的，评审小组将视偏离程度给予扣分或认定为虚假应标。

投标人名称（电子印章）：

投标人代表签字或盖章：

职 务：

日 期：

**附件10**

**证书一览表**

|  |  |  |  |
| --- | --- | --- | --- |
| **证书名称** | **发证单位** | **证书等级** | **证书有效期** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**要求：**

1.填写投标人获得资质、认证或企业信誉证书；

2.附所列证书复印件或其他证明材料。

投标人名称（电子印章）：

投标人代表签字或盖章：

职 务：

日 期：：

**附件11**

**投标人类似项目实施情况一览表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **项目名称** | **项目地址** | **合同总价** | **实施时间** | **项目质量** | **项目单位名称及其联系人电话** |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| … |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**要求：**

1.业绩证明应提供证明材料（合同复印件可只提供首页、含金额页、盖章页并加盖投标人电子印章）；

2.报价供应商可按此表格式复制。

投标人名称（电子印章）：

投标人代表签字或盖章：

职 务：

日 期：

**附件12**

**资信及商务需求响应表(第 标)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** |  **内容** | **招标需求** | **是否响应** | **投标人的承诺或说明** |
|  | 售后服务保障要求 |  |  |  |
|  | 备品备件及耗材等要求 |  |  |  |
|  | 质保期 |  |  |  |
|  | 交货和服务时间及地点 |  |  |  |
|  | 付款条件 |  |  |  |
|  | …… |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

投标人名称（电子印章）：

投标人代表签字或盖章：

职 务：

日 期：

**附件13**

**售后服务情况表**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **项目** | **投标人情况** | **备注** |
| 1 | 保修期内售后服务情况(服务方式、服务网点、售后服务的内容和措施等等，可用附页和宣传材料) | 生产厂商售后服务情况： |  |
| 投标人售后服务情况： |  |
| 2 | 保修期后售后服务 |  |  |
|  3 | 培训方案（可用附页） |  |  |
| …… | …… |  |  |

投标人名称（电子印章）：

投标人代表签字或盖章：

职 务：

日 期：

**附件14**

**主要货物用材响应表(类似家具类货物采用)**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 货物名称 | 产品配置 | 产品主要用材 |
| 材料规格及参数 | 品牌商标 | 生产厂家 | 符合标准 | 性能说明 | 备注 |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**要求：**

1.请列出以上产品的各项主要用材、辅料、油漆、五金件等。

2.本表所列产品主要用材均为采购人抽样送检的范围。

投标人名称（电子印章）：

投标人代表签字或盖章：

职 务：

日 期：

**附件15**

项目名称

项目编号：（标段）

**报**

**价**

**文**

**件**

供应商全称（电子印章）：

地 址：

时 间：

**报价文件目录**

1、开标一览表（附件16）；

2、报价明细表（附件17）；

3、针对报价投标人认为其他需要说明的；

4、小微企业等声明函（附件18）；

5、产品适用政府采购政策情况表（附件19）。

**附件16**

**开标一览表 (第 标)**

**项目编号：**

**项目名称：** [货币单位：人民币元]

|  |  |  |
| --- | --- | --- |
| 投标总报价(元) | 大写 |  |
| 小写 |  |

**填报要求：**

1.投标总报价是包括货款、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、合同包含的所有风险责任等各项费用及不可预见费等所需的全部费用。

2.报价一经涂改，应在涂改处加盖单位电子印章，或者由法定代表人或全权代表签字或盖章，否则其投标作无效标处理。

投标人名称（电子印章）：

投标人代表签字或盖章：

职 务：

日 期：

**附件17**

**报价明细表 (第 标)**

 项目编号： [货币单位：人民币元]

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **报价项目** | **品牌、产地** | **型号规格** | **数量** | **单价** | **小计** | **备注** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **合计人民币：大写 小写** |

**要求：**

1. 本表为《开标一览表》的报价明细表，如有缺项、漏项，视为投标报价中已包含相关费用，采购人无需另外支付任何费用。

2.“报价明细表”中的报价合计应与“开标一览表”中的投标总报价相一致，不一致时，以开标一览表为准。

3.投标报价明细表所填内容按招标文件采购设备清单要求为准。如有漏报的，视同已包含在投标总价内或已作优惠处理。有重大缺项的将作无效标处理。

▲4. 本表中的型号规格必须明确，软件服务及招标文件中明确要求定制的除外。

投标人名称（电子印章）：

投标人代表签字或盖章：

职 务：

日 期：

**附件18**

**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：第四条第\_\_\_\_\_\_项\_\_\_\_\_\_行业，本公司*（此处填写从业人员和营业收入的具体数据）*，为\_\_\_\_\_\_（请填写：小型、微型）企业。

2.本公司参加×××政府采购中心组织的采购项目（项目编号： ）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。

~~3.本公司小微信息查询网址：~~

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。

投 标 人（单位电子印章）：

日期： ××年××月××日

**小微企业声明函（制造商）**

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）的规定和《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：第四条第\_\_\_\_\_\_项\_\_\_\_\_\_行业，本公司（此处填写营业收入和从业人员的具体数据），为\_\_\_\_\_\_（请填写：小型、微型）企业，信息查询网址为：

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（单位电子印章）：

日期： ××年××月××日

**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（电子印章）：

 日 期：

**附件19**

**产品适用政府采购政策情况表**

|  |  |  |
| --- | --- | --- |
| 小微企业扶持政策 |

|  |
| --- |
| **小型、微型企业投标且所投产品（指货物、工程、服务）由本企业制造，或者所投产品（仅指货物）含有其他小型、微型企业制造的，应按要求列出具体产品与金额。** |

 |
| 产品名称（品牌、型号） | 制造企业名称 | 金额 |
|  |  |  |
|  |  |  |
|  |  |  |
| 小型、微型企业产品金额合计（元） |  |

填报要求：

1. 本表的产品名称、规格型号和注册商标、金额要与《报价明细表》一致。
2. 制造商为小型或微型企业时才需要填“制造商企业类型”栏，填写内容为“小型”或“微型”。
3. 请投标人正确填写本表，所填内容将作为评分依据（以“小型、微型企业产品金额合计”为准进行价格折扣，表中所填内容必须与政府采购优惠政策需提供的相关资料相符，如出现不相符或提供资料不全的，该小型、微型企业不符产品核计金额将不予以享受小微企业扶持政策优惠）。