柯桥区电子政务外网网络及安全设备升级项目

（采购编号：[绍柯采[2020]2574号](https://pay.zcy.gov.cn/purchaseplan_front/" \l "/plan/list/detail?id=1000000000000828721&encrypt=3a132e45f110bb9b4f65153b8c83e858" \t "_blank)）

采

购

文

件

采购人：绍兴市柯桥区大数据发展管理中心(盖章)

采购代理机构：绍兴市柯桥区公共资源交易中心(盖章)

绍兴市鼎正建设工程咨询有限公司(盖章)

2020年07月

**目 录**

[关于柯桥区电子政务外网网络及安全设备升级项目的采购公告 3](#_Toc20173710)

[一、前附表 6](#_Toc20173711)

[二、供应商须知 8](#_Toc20173712)

[三、供应商应当提交的资格（资信）证明文件 11](#_Toc20173713)

[四、投标报价要求、投标文件编制要求和投标保证金交纳方式 12](#_Toc20173714)

[五、采购项目的技术规格、要求和数量，包括附件、图纸等 12](#_Toc20173715)

[六、合同主要条款及合同签订方式 36](#_Toc20173716)

[七、交货和提供服务的时间 40](#_Toc20173717)

[八、评标方法、评标标准和废标条款 40](#_Toc20173718)

[九、投标截止时间、开标时间及地点 43](#_Toc20173719)

[十、其他事项 43](#_Toc20173720)

[附件一：投标函 44](#_Toc20173721)

[附件二：法定代表人授权书 44](#_Toc20173722)

[附件三：开标一览表（报价表） 46](#_Toc20173723)

[附件四：投标报价明细表 47](#_Toc20173724)

[附件五：投标技术方案和人力资源安排 48](#_Toc20173725)

[附件六：投标设备材料详细清单 49](#_Toc20173726)

[附件七：投标设备主要技术参数说明 50](#_Toc20173727)

[附件八：技术偏离表 51](#_Toc20173728)

[附件九：投标承诺书 52](#_Toc20173729)

[附件十：投标提问书 53](#_Toc20173730)

[附件十一：答疑纪要 54](#_Toc20173731)

[附件十二：评标办法 55](#_Toc20173732)

# 关于柯桥区电子政务外网网络及安全设备升级项目的采购公告

公告时间：2020年7月21日

根据《中华人民共和国政府采购法》等有关规定，绍兴市柯桥区大数据发展管理中心委托绍兴市柯桥区公共资源交易中心、绍兴市鼎正建设工程咨询有限公司，就柯桥区电子政务外网网络及安全设备升级项目进行公开招标，欢迎国内合格的供应商前来投标。

**一、采购项目编号**: **绍柯采[2020]2574号**

**二、采购项目名称：柯桥区电子政务外网网络及安全设备升级项目**

**三、采购项目组织类型：政府集中采购**

**四、采购项目概况**（包括内容、用途、数量、简要技术要求等）：

本次采购内容为柯桥区电子政务外网网络及安全设备升级项目，包括负载均衡、核心防火墙、核心交换机、上网行为管理、态势感知平台等设备和系统集成服务，采购预算价约592万元，采购上限价为592万元。具体详见采购文件。

**五、投标供应商资格要求：**

①符合政府采购法第二十二条之规定；

②未被列入失信被执行人、重大税收违法案件当事人名单和政府采购严重违法失信行为记录名单的供应商；

③具有本采购项目供货、实施能力，能提供良好的技术支持和售后服务的独立法人。

④本次采购 不接受 联合体投标。

**六、采购文件的获取的时间和方式：**

自公告之日起至 2020年7月29日16:00时截止，由供应商自行在网上下载，登陆政采云平台http://www.zcygov.cn/，在线申请获取采购文件（进入“项目采购”应用，在获取招标文件菜单中选择项目，申请获取采购文件）。

采购文件获取截止时间后至投标截止时间前，潜在投标供应商提出要求获取采购文件的，可允许其获取，但该供应商如对采购文件有疑问的，应在采购文件载明的投标提问截止时间前以传真、电子邮件等形式提出，逾期提出的，采购人有权不予受理、答复。

**七、报名的时间和方式：**

本项目实行网上报名，不接受现场报名。参加本项目投标的供应商应在投标截至时间之前完成网上在线报名，网上报名网站为浙江政府采购云平台，网址http://www.zcy.gov.cn/。未报名投标人的投标文件（如以联合体形式参加政府采购活动的，需联合体牵头人报名）将被拒绝。《供应商网上报名操作指南》网址：浙江政府采购网，位置：“首页-办事指南-省采中心-网上报名”（<http://zfcg.czt.zj.gov.cn/quote/2017-05-25/6708.html?_=2020-02-17%2003:02:20>）。

**八、投标与开标注意事项：**

8.1.本项目实行网上投标，采用电子投标文件。

8.2.标前准备：各供应商应在开标前应确保成为浙江省政府采购网正式注册入库供应商，并完成CA数字证书办理。办理流程详见http://www.zjzfcg.gov.cn/bidClientTemplate/2019-05-27/12945.html）。完成CA数字证书办理预计半个月左右，建议各投标人抓紧时间办理。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。

8.3.投标文件制作：

8.3.1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。

8.3.2投标人通过“政采云”平台电子投标工具制作投标文件，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/2019-05-27/12946.html），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”。

**九、投标截止时间及要求：** 2020 年8月13日 上 午9时30分整之前将电子投标文件上传到“政采云”平台。

**十、开标时间及地点：** 2020 年8月13日 上 午9时30分整在绍兴市柯桥区华齐路1066号绍兴市柯桥区公共资源交易中心三楼3号交易室开标。

开标时间后1小时内**（2020年8月13日10:30前）**供应商可以登录“政采云”平台，用“项目采购-开标评标”功能进行解密投标文件。若供应商在规定时间内**（2020年8月13日10:30前）**无法解密或解密失败，视为投标人放弃投标。

**十一、投标保证金：无**

**十二、招标公告发布：**<http://www.zjzfcg.gov.cn>。

**十三、本项目公告期限：**本公告发布之日起五个工作日。

**十四、质疑和投诉：**供应商认为招标文件、采购过程和中标、成交结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起七个工作日内，以电子邮件的形式向采购人提出质疑，采购人以电子邮件的形式对供应商进行质疑回复。供应商对采购人的质疑答复不满意或者采购人未在规定时间内作出答复的，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。

**十五、其他事项：**

1.供应商注册：参与绍兴市柯桥区政府采购活动的投标人，必须注册并登记加入浙江省政府采购供应商库。供应商可通过浙江政府采购网（http://www.zjzfcg.gov.cn）或浙江政采云平台（http://www.zcy.gov.cn/）进行注册申请，按规定审核后，登记加入“浙江省政府采购供应商库”。

2.本采购文件所涉及的法定代表人或其委托代理人的签字或盖章的内容，投标供应商须盖法定代表人电子签章，如果投标供应商没有法定代表人电子签章，涉及到法定代表人或其委托代理人的签字或盖章的内容，投标供应商可以线下签字或盖章后扫描上传。

**联系方式**

采购人名称：绍兴市柯桥区大数据发展管理中心

详细地点：绍兴市柯桥区群贤路1661号

联 系 人： 沈宏峰

联系电话： 0575- 84119019

采购代理机构名称：绍兴市柯桥区公共资源交易中心、绍兴市鼎正建设工程咨询有限公司

详细地点: 绍兴市柯桥区华齐路1066号；绍兴市二环北路135号金德隆北区B座四楼；

联系人： 张峰

联系电话：0575-85176866

传 真：0575-85155500

# 一、前附表

|  |  |  |
| --- | --- | --- |
| 序号 | 内 容 | |
| 1 | 综合说明 | 1.采购项目名称：柯桥区电子政务外网网络及安全设备升级项目  2.采购项目内容：本次采购内容为柯桥区电子政务外网网络及安全设备升级项目，包括负载均衡、核心防火墙、核心交换机、上网行为管理、态势感知平台等设备和系统集成服务。  3.采购预算价：592万元  4.采购项目交货地点：绍兴市柯桥区大数据发展管理中心 |
| 2 | 资金来源：财政拨款 | |
| 3 | 投标资格：①符合政府采购法第二十二条之规定；②未被列入失信被执行人、重大税收违法案件当事人名单和政府采购严重违法失信行为记录名单的供应商；③具有本采购项目供货、实施能力，能提供良好的技术支持和售后服务的独立法人。④本次招标不接受联合体投标。 | |
| 4 | 投标有效期：90天（日历天数）（从投标截止之日算起） | |
| 5 | 投标保证金：无。 | |
| 6 | 合同履约保证金金额为：合同价的5% | |
| 7 | 质量要求：合格 | |
| 8 | 现场勘察：投标供应商自行组织现场踏勘。现场踏勘所发生的费用由投标供应商自行承担，踏勘过程中的安全责任由投标供应商自负。 | |
| 9 | 供货安装时间：合同签订后 60日历天内完成供货及安装。 | |
| 10 | 采购文件的获取：自公告之日起至2020年7月29日16;00时截止，由供应商自行在网上下载。 | |
| 11 | 投标供应商提出问题的截止时间：2020年7月30日 16：00 时前按《采购公告》中的地址以传真、电子邮件等形式通知采购代理机构。注明：投标提问书中需写明投标供应商名称（盖公章）、联系人、联系电话。 | |
| 12 | 采购人澄清（答疑）和修改的时间：2020 年7月31日16:00时前在浙江省政府采购网网上回复。 | |
| 13 | 投标文件份数：本项目实行网上投标，供应商应准备电子投标文件，按政采云平台项目采购-电子招投标操作指南及本招标文件要求递交。  **注明：供应商需自行准备电脑和制作标书的CA锁。** | |
| 14 | **投标截止时间及要求：** 2020 年8月13日 上 午9时30分整之前将电子投标文件上传到“政采云”平台。 | |
| 15 | **开标时间及地点：** 2020 年 8月13日 上 午9时30分整在绍兴市柯桥区华齐路1066号绍兴市柯桥区公共资源交易中心三楼3号交易室开标。 | |
| 16 | 其他需说明的内容：  1.开标时间后1小时内**（2020年8月13日10:30前）**供应商可以登录“政采云”平台，用“项目采购-开标评标”功能进行解密投标文件。若供应商在规定时间内**（2020年8月13日10:30前）**无法解密或解密失败，视为投标人放弃投标。  **2.本招标文件所涉及的法定代表人或其委托代理人的签字或盖章的内容，投标单位须盖法定代表人电子签章，如果投标单位没有法定代表人电子签章，涉及到法定代表人或其委托代理人的签字或盖章的内容，投标单位可以线下签字或盖章后扫描上传。** | |
| 17 | 样品要求（包括样品内容、数量，样品提供时间、地址等要求）： / | |
| 18 | 现场演示：有 | |
| 19 | 解释：凡涉及本次采购文件的解释权属于采购人。 | |
| 20 | 监管机构：绍兴市柯桥区公共资源交易管理委员会办公室，联系电话：0575-84130780 | |
| 21 | **本项目设上限价，本次采购的上限价为592万元。超过上限价的，作无效标处理。** | |

# 二、供应商须知

**2.1采购方式：公开招标。**

**2.2合格的供应商**

　　凡符合前附表第3项要求，有生产（或供应）、服务能力的国内企业，在国内注册的外国独资或中外合资、合作企业，符合并承认和履行采购文件中的各项规定者，均可参加投标。

**2.3联合投标**

2.3.1不接受联合体投标。

**2.4采购文件的澄清（答疑）和修改**

2.4.1供应商在获得采购文件后，如有疑问，须按前附表的时间要求，以书面形式通知采购人，除非采购人认为确有必要澄清、答复，否则，采购人有权拒绝回复投标人在规定的时间后的任何澄清要求。

2.4.2对在前附表规定时间前收到的疑问，采购人应在答疑回复截止时间之前，对供应商提出的问题予以澄清、答复；或者在投标截止前的任何时候，采购人需要对采购文件进行补充或修改的，采购人将会通过“浙江省政府采购网”以澄清或修改公告形式发布。为使供应商在编制投标文件时把修改或补充通知内容考虑进去，采购人可以酌情延长递交投标文件的截止时间，通知中没有注明更改投标截止时间的视为截止时间不变。

2.4.3澄清或修改公告的内容为采购文件的组成部分。当招标文件与澄清或修改公告就同一内容的表述不一致时，以最后发出的文件内容为准。

2.5现场勘察

2.5.1为使投标供应商对本采购项目情况有所了解，投标供应商自行组织对项目所在场地及周围环境进行现场勘察，以便获取由投标供应商自行负责编制投标文件和签订合同所需的一切资料。现场勘察所发生的费用由投标供应商自行承担。

2.5.2现场勘察完毕，将认为供应商已了解现场情况，并充分理解了为之所承担的风险、义务和责任。

2.5.3在现场勘察过程中，投标供应商应承担在此期间所造成的人身伤害、财产损失或损坏的责任，无论何种原因所造成，采购人均不负责，如由此导致采购人承担责任的，采购人有权向该供应商行使追偿权。

2.6采购文件作为报价、评标、定标、签订服务合同的依据。如有异议，应在招标答疑时提出。否则，将视作认同。

2.7供应商应认真阅读采购文件中所有的事项、格式、条款和规范等要求。如果没有按照采购文件要求提交全部资料或者投标文件，没有对采购文件作出实质性响应，该投标有可能被拒绝，其风险应由供应商自行承担。

**2.8投标文件的组成与编制**

投标文件由资格（资信）证明文件、商务技术标、价格标共三部分组成。资格（资信）证明文件按第三章节顺序编制，其他应包括下列内容并按以下顺序编制：

**2.8.1商务技术标：**

2.8.1.1投标函（附件一）；

2.8.1.2投标技术方案和人力资源安排（附件五）；

2.8.1.3投标设备材料详细清单（附件六）；

2.8.1.4投标设备主要技术参数说明（附件七）；

2.8.1.5技术偏离表（附件八）；

2.8.1.6投标承诺书（附件九）；

2.8.1.7产品的技术服务和售后服务的内容和措施及距采购人最近的服务网点的详细介绍；

2.8.1.8商务技术标评审内容；

2.8.1.9优惠条件（如有）；

2.8.1.9.1供应商承诺给予采购人的各种优惠条件，包括货物价格、运输、装卸、安装调试、保险、付款条件、售后服务、技术服务等方面的优惠。

2.8.1.9.2当优惠条件涉及“开标一览表（报价表）”中的各项费用时，必须与投标价格相统一。商务技术标中不得出现投标报价。

**2.8.2价格标**

2.8.2.1开标一览表（报价表）（附件三）；

2.8.2.2投标报价明细表（附件四）；

2.8.3投标文件的形式：投标文件分为电子投标文件。

**电子投标文件投标人应根据“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。电子投标文件中所须加盖公章部分均采用CA签章。**

**本采购文件所涉及的法定代表人或其委托代理人签字或盖章的内容，投标供应商须盖法定代表人电子签章，如果投标供应商没有法定代表人电子签章，涉及到法定代表人或其委托代理人的签字或盖章的内容，投标供应商可以线下签字或盖章后扫描上传。**

**2.9**供应商必须使用采购文件提供的表格格式，但表格可以按同样格式扩展（见附件及附表）。采购文件中未提供的表格格式，供应商可以自拟。

**2.10投标有效期**

2.10.1投标有效期详见前附表第4项。

2.10.2在原定投标有效期满之前，如果出现特殊情况，经采购管理机构核准，采购人可以用在浙江省政府采购网上发布形式向供应商提出延长有效期的要求。供应商需以书面形式予以答复，供应商可以拒绝这种要求而不失去他的投标保证金。同意延长投标有效期的供应商，不需要也不允许修改他的标书，但需要相应地延长投标保证金的有效期，在延长期内，本标书关于投标保证金的退还与没收的规定仍然适用。

**2.11投标文件的修改与撤回**

2.11.1供应商递交投标文件以后，可以在投标文件递交截止时间前，修改或撤回其投标文件。

2.11.2 在投标文件递交截止时间后，不能更改投标文件。 2.11.3在投标文件递交截止时间起至标书中规定的投标文件有效日期终止日之间的这段时间内，供应商不能撤回投标文件。

**2.12投标文件的澄清**

2.12.1为了有助于投标文件的审查、评价和比较，评标委员会可以个别地要求供应商澄清其投标文件，包括单价分析表，但不接受供应商任何主动的澄清、说明或辩解。有关澄清的答复，应在（1小时内）发送至邮箱（303736433@qq.com）并应有法定代表人或其委托代理人的签字或盖章，但不允许更改投标文件中的价格或实质性内容。

2.12.2供应商的澄清文件是投标文件的组成部分，并替代供应商投标文件中被澄清的部分。

**2.13投标文件符合性的确定**

2.13.1实质上符合要求的投标文件，应该与采购文件的全部条款、条件和规范相符，无重大差异或保留。所谓重大差异或保留是指对采购项目的范围、质量、项目的实施与运用产生重大的影响，并对其他按合理价格提交了实质上符合要求的投标文件的供应商的竞争地位，产生不公正的影响。

2.13.2如果投标文件实质上不符合采购文件的要求，其投标文件将被予以拒绝，并且不允许供应商通过修正或撤消其重大差异或保留使之符合要求。

**2.14错误的修正**

2.14.1确定中标候选人前（评标过程中）的修正方法：

评标委员会应对确定为实质上符合要求的投标文件进行校核，看其是否有计算上或累计上的算术错误，修正此类错误的原则如下：

2.14.1.1同一项目出现两种以上不同价格时，取其低的报价核算；

2.14.1.2如果用数字表示的数额与用文字表示的数额不一致时，以文字数额为准。

2.14.1.3当单价与数量的乘积之总和同总额之间不一致时，应以标出的单价为准，除非评标委员会认为单价有明显的小数点错误，此时应以标出的总额为准，并修改单价。

2.14.2确定中标候选人后的修正方法：

2.14.2.1同一项目出现两种以上不同价格时，取其低的报价核算；

2.14.2.2如果用数字表示的数额与用文字表示的数额不一致时，以文字数额为准。

2.14.2.3合价之和与总报价不一致时，以总报价为准，按总报价占调整前的合价之和的比例调整合价，并修改单价；

2.14.2.4 当单项与数量的乘积与合价不一致时，以合价为准，并修改单项。

2.14.3 评标期间，评标委员会不接受任何投标供应商主动提出的对投标报价及单价、合价的调整。

2.14.4投标文件报价，开标时，开标一览表（报价表）的总价与投标报价明细表的总价不一致时，以开标一览表（报价表）的总价为准；大写与小写不一致的以大写为准。

2.14.5按以上原则进行错误修正，调整投标文件的投标报价，经供应商确认后，调整后的报价对供应商起约束作用。若投标供应商不接受修正后的投标报价则其投标将被拒绝且其投标保证金不予以退还。

**2.15投标费用**

供应商应自行承担所有与编写和提交投标文件有关的费用，不论投标的结果如何，采购人在任何情况下均无义务和责任承担这些费用。

# 三、供应商应当提交的资格（资信）证明文件

开标时，由采购人或采购代理机构依法对各投标供应商的资格进行审查。

**3.1资格、资信证明文件单独封装，仅需提供正本一份**。包括下列内容：

3.1.1营业执照复印件(需盖投标供应商公章)；

3.1.2法定代表人的身份证(需盖投标供应商公章)；

3.1.3法定代表人授权书（附件二）；

3.1.4全权代表身份证(需盖投标供应商公章)；

# 四、投标报价要求、投标文件编制要求和投标保证金交纳方式

4.1投标报价及相关要求：

4.1.1本次采购以人民币报价，**供应商的报价（合价）应包括因承包本次采购项目所需的货物价款、劳务、质检（自检）、运输、装卸、安装、调试、缺陷修复、验收、管理、风险、保险、税费、质保、培训及不可预见费用等一切费用。**

4.1.2供应商的报价必须是本标书所要求的全部项目投标价的总和，并以供应商在投标报价清单中提供的单价及总额价为依据。

4.1.3各细目单价应报综合单价，包括一切与供货、安装相关的费用。

4.1.4供应商必须填报各项目单项的价款，今后采购量如有增减，其总价款则按实以单项价款调整。

4.1.5开标一览表（报价表）中标明的价格在合同执行过程中是固定不变的，不得以任何理由予以变更。每个投标供应商只允许有一个报价，任何有选择的报价将不予接受。

4.1.6 开标一览表（报价表）中不得漏填项目，否则当实施合同时供应商没有填入单价与金额的项目，将不予支付，并认为此项目费用已包括在价格表的其他项目的单价和金额之中。

4.1.7 开标一览表（报价表）需加盖投标供应商公章并由法定代表人或其委托代理人签字或盖章。

4.2开标一览表（报价表）按采购人提供的格式要求填写（格式附后，格式不得随意变动，变动者为无效）。

4.3 投标文件的编写

供应商应仔细阅读采购文件，了解采购文件的要求。在完全了解采购货物的技术规范和要求以及商务条件后，编制投标文件。

4.4投标保证金：无。

4.5履约保证金：

4.5.1履约保证金金额详见前附表第6项。

4.5.2履约保证金待履行合同完毕后7个工作日内予以退还（不计息）。

# 五、采购项目的技术规格、要求和数量，包括附件、图纸等

5.1采购原则：

5.1.1本着“实用、可靠、先进、经济”的原则，充分利用现有资源，结合采购人的具体情况和实际工作需求进行配置。

**5.2采购物品名称、数量、技术要求：**

5.2.1主要设备清单(投标供应商可以在采购人的推荐品牌中选择其中一个品牌进行报价，也可根据采购文件的要求选用同档次或高于推荐品牌的优质品牌产品进行报价。参数允许正偏离。)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名称** | **参数** | **数量** | **单位** |
| 1 | 负载均衡 | 4核CPU;配置≥4个万兆光口，≥8个千兆光口；内存：≥32GB；硬盘：≥500GB； 吞吐量：≥20Gbps；配置2个250W AC Power热插拔冗余电源;需配置链路及应用均衡功能；原厂三年质保。 | 2 | 台 |
| 2 | 万兆防火墙 | 2U机箱；最大配置为≥34个接口， 默认包括4个可插拨的扩展槽和2个10/100/1000BASE-T接口，配置≥4个万兆接口和SPF模块；标配模块化双冗余电源；默认包含应用识别功能，含至少1年应用特征库升级许可  性能：防火墙吞吐率：≥32Gbps；并发连接数：≥800万；原厂三年质保。 | 2 | 台 |
| 3 | 核心交换机 | 核心交换机交换容量≥367T bps；包转发率≥230400Mpps；业务槽位≥8个；交换网槽位≥6个；本次配置双主控板卡、双电源、至少5块交换网板卡、1块48端口十兆/百兆/千兆以太网电接口板（RJ45)、1块48端口万兆以太网光接口板(SFP+)；原厂三年质保。 | 2 | 套 |
| 4 | 上网行为管理 | 性能指标：网络吞吐量≥30Gb、推荐带宽≥15Gb、支持用户数≥150000人、最大并发数≥15800000；  硬件指标：2U，双电源，≥4个千兆电口，≥4个千兆光口，≥4个万兆光口， 1个串口(RJ45) ，2个USB2.0，48G内存，硬盘配置1TB+64G SSD;带上网行为管理软件；软件升级三年；原厂三年质保。 | 2 | 套 |
| 5 | 日志服务器 | CPU: 2颗\*4210 /内存:64GB/硬盘：8TB \*6/支持Raid0、1、5/双口千兆/2\*550w/导轨/原厂三年质保。 | 1 | 台 |
| 6 | 态势感知平台（核心产品） | 要求基于实时流数据为用户提供安全分析能力和风险告警及多维度可视化展示。具有实时流数据分析系统、交互式在线分析系统、超大规模存储查询控制系统、用户行为分析（UEBA）系统、深度感知智能引擎、大数据可视化引擎，提供大规模数据存储、高压缩比及快速检索能力、追溯取证能力以满足企业合规要求。智能分析与防护设备形成安全联动能力。提供深度机器学习技术提高数据挖掘能力，为企业安全提供决策依据、提高企业信息安全的纵深防御能力。态势感知展示模块、安全监测模块、通报预警管理、应急处置管理、重大漏洞在线检测模块、移动终端APP等功能模块 1、云端威胁情报订阅模块：需提供威胁情报离线库并支持更新。 2、需提供攻击主机、僵尸网络、病毒木马、恶意软件、APT情报、恶意邮件等情报的活跃时间、可信度、家族分类，可应用于本产品的实时分析； 3、设备需支持在线查询与溯源：云端提供对IoC威胁类型、多源情报、WHOIS、开放端口、SSL证书等多维度的溯源分析； 4、云端服务：需支持订阅高级威胁分析情报，云端提供最新APT入侵、0day漏洞预警、病毒变种情况等分析报告订阅。 平台硬件：1台（2U机架式；内存≥256GB；硬盘≥4TB\*12\H730\1GbE\*2）  原厂三年质保。 | 1 | 套 |
| **网络流量综合探针**  硬件外形：软硬一体化2U标准机架式设备；  电源：1+1冗余电源  CPU：6核12线程\*2  内存：≥128G  硬盘容量：≥2T\*2，带RAID1； 接口数量：标配≥10个； 接口类型：标配千兆管理口≥2 千兆业务口RJ45网口≥4，千兆业务SFP光口≥4 ，万兆光口≥2 吞吐率：≥10Gbps  原厂三年质保。 | 1 | 台 |
| **日志审计探针**  ≥4个电口，1个console口 内存：≥64GB，磁盘：4T\*4 raid5 EPS：≥10000/秒 （峰值：≥14000/秒） 双电源、非CF卡启动 可扩展项：内存可扩展至≥128GB 单个磁盘可扩展至≥4T(8个盘位)，支持HBA卡扩展 网口可扩展至≥12个（本次配置4电、2万兆光） ≥500个日志源  峰值EPS :14000  原厂三年质保。 | 1 | 台 |
| **监控终端设备**  主机 CUP:i9-10900 RTX2060 /内存：32G /硬盘：2T+512G SSD/无线键盘鼠标  液晶显示屏：27英寸 IPS技术屏 4K超高清  (液晶显示屏：每台主机配2只，DP线2根) | 2 | 台 |
| **实时监控展示平台**  要求≥65英寸/超高清4K HDR/人工智能WIFI/四核处理器/运行内存2GB及以上/系统内存8GB及以上/包含安装调试 | 1 | 台 |
| 7 | 数据库审计 | 硬件尺寸：标准2U CPU规格：4核 内存容量：≥8GB\*2 硬盘容量：≥2TB\*2（Raid 1） 网口类型：1000M电口≥6，1000M光口≥4,  10G光口≥2, 电源配置；双电源 硬件最大吞吐量2000Mbps 最大纯数据库流量200Mbps 日志数量存储：≥20亿条  审计日志检索能力≥1500万条/秒  原厂三年质保。 | 1 | 台 |
| 8 | 主机安全及管理系统 | 配置2个系统控制中心，200个服务器端许可 | 1 | 套 |

**5.2.2 设备详细技术参数**

**5.2.2.1负载均衡**

|  |  |
| --- | --- |
| 指标 | 技术参数 |
| 性能参数要求 | |
| 节能设计 | 采用绿色高效电源 |
| CPU | 4核CPU;支持多核CPU并行处理技术 |
| 端口和吞吐量 | ≥4个万兆光口；≥8个千兆光口；4层吞吐能力≥20Gbps；7层吞吐能力≥20Gbps |
| 内存 | ≥32GB |
| 存储介质 | ≥500GB |
| 最大并发连接数 | ≥28M |
| 四层处理能力（每秒新建连接数） | ≥250K CPS，可在不更换硬件的情况下扩展至450K及以上 |
| 七层处理能力（每秒处理请求数） | ≥650K RPS，可在不更换硬件的情况下扩展至1.1M及以上 |
| RSA SSL TPS 2K Key | ≥10000 TPS，可在不更换硬件的情况下扩展至20000及以上 |
| ECC SSL TPS ECDSA P-256 | ≥6500 TPS，可在不更换硬件的情况下扩展至10000及以上 |
| SSL 吞吐量 | ≥10Gbps，可在不更换硬件的情况下扩展至15Gbps及以上 |
| 压缩吞吐量 | ≥6Gbps，可在不更换硬件的情况下扩展至10Gbps及以上 |
| DNS处理能力 | ≥480K QPS，可在不更换硬件的情况下扩展至880K及以上 |
| 应用交付功能要求 | |
| 服务器负载均衡 | 完善的第四/七层交换功能，支持可定制的基于应用层的健康检查方式，支持基于IP地址、Cookie等信息的会话保持，并可根据特定信息定制会话保持方式。 |
| 链路负载均衡 | 支持Inbound、Outbound链路负载均衡，提供多种动态和静态的负载均衡算法：  1.静态算法(轮询 比例 优先权)  2.动态算法(最少连接数 最快响应等) |
| 物联网MQTT协议负载均衡 | 支持MQTT协议的协议解析，日志审计和负载分发。 |
| 可支持对SSL/TLS 算法分组 | 支持处理SSL/TLS加密流量时，用户可以通过web管理界面自定义可支持的SSL/TLS算法组合，细化SSL/TLS算法的管理，可以更好的匹配用户实际场景中的加密场景和需求。 |
| 可定制的基于应用层的健康检查方式 | 可根据应用系统提供的检查入口参数对应用进行应用级的监控以避免服务器地址端口监听正常而实际应用挂起的情况；可根据App服务进程信息定制应用服务级的健康检查方式。 |
| ▲IPv6支持 | 标配IPV6功能，在IPv4和IPv6网络之间提供完整的IP转换和负载均衡能力可以支持用户迁移以及建立IPv4和IPv6混合主机资源。 |
| 优化功能 | 标配压缩，缓存，多连接复用，SSL卸载等优化加速功能。 |
| 可编程流量管理 | 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。并提供专用的编辑工具。 |
| 支持Multi-path TCP技术 | 支持在多重网络环境下可以通过多种网络环境（WIFI、3G、4G）同时发起请求的Multipath TCP连接方式 |
| HTTP/2和SPDY协议网关 | 支持HTTP/2和SPDY网关部署。 |
| HTTPDNS网关 | 支持HTTPDNS解析功能，将HTTPDNS查询转换为传统的DNS查询，配合智能DNS服务器实现全局负载均衡。 |
| 四/七层带宽管理和流量整形(Qos) | 标配支持通过优先级、队列、以及基于七层协议和内容的带宽限制和带宽容许，确保关键应用能够优先交付。 |
| 基本会话保持 | 提供基于源IP、URL、HASH、插入cookie等多种方式多种场景下的会话保持功能。 |
| 高级会话保持 | 提供SSL ID、手机串号IMEI及自定义字段等高级会话保持功能，实现在一段时间内将同一个用户的请求发送给同一台应用服务器。 |
| 灰度发布 | 提供业务按需发布，便于应用平滑上线，版本迭代。 |
| ▲支持混合云部署模式 | 支持在中国的AWS、 Azure及阿里云等公有云部署，流量自动调度并和本地数据中心设备联动，实现混合云部署。（提供在阿里云云市场上的应用展示截图并加盖投标人公章） |
| 支持云管理平台 | 支持Openstack，Cisco ACI，VMware NSX，华为等主流云管理平台对设备进行管理。 |
| 安全功能要求 | |
| SSLVPN并发用户许可 | 免费提供不低于10个并发用户许可证。 |
| IPSEC VPN | 支持与CISCO等第三方主流IPSEC VPN设备建立加密通道，保障多站点之间业务及数据传输安全。 |
| 系统功能要求 | |
| 多重引导 | 支持同一台设备同时并存四个及以上不同的系统版本，便于系统升级或回退，并且支持不中断业务通过web页面进行软件版本更迭，系统切换后配置自动导入，无需手工配置。 |
| ▲集群 | 支持Active-Active及Active-Standby冗余方式；提供连接会话的镜像功能, 实现无缝故障切换, 支持不同型号，不同License的32台设备的N+M集群方式。可以与在线使用的负载均衡设备做集群。（投标文件中提供相关配置截图或官方网站证明文档并加盖投标人公章） |
| ▲系统保护 | 提供设备root密码，并允许用户修改该密码；严禁设备存在任何密码不向最终用户公开的超级权限用户。可针对用户级别进行权限微调，支持当密码错误输入次数多过时，对用户进行自动锁定。只允许授权的IP地址访问设备管理页面，以防止来自内网、外网的非受信访问（投标文件中提供相关配置截图并加盖投标人公章） |
| 系统管理 | 支持HTTPS/SSH的管理模式，WEB管理同时支持IE浏览器和非IE浏览器(FireFox、Chrome等)。主、备双机可同时被管理、可同时在主备设备上修改配置，并实现同步。 |
| 自助巡检 | 可以进行自动系统诊断，通过在线网站自动生成诊断和分析报告。 |
| 自动化执行脚本 | 根据特定的统计事件或周期性执行自定义脚本，比如在设备出现问题的情况下，自动收集故障信息并发送给指定的服务器。 |
| 应用性能监控 | 管理界面可通过图形化界面直接提供应用访问的网络延时和服务器延时、TOP URL、以及各虚拟服务器的CPU、内存等资源的占用比。 |
| 应用配置和管理模板 | 内置对主流应用如SAP、Oracle Application Server、SharePoint、VMware View的配置模板，支持一键部署应用。） |
| LCD液晶管理面板 | 提供可触摸液晶面板实现直观管理，显示设备工作状态和报警，便于机房管理人员巡检及日常运维管理。 |
| 服务 | 厂商需在中国境内自建完善的售后服务团队，并提供国内技术支持中心的400免费技术支持热线电话。要求提供三年原厂软件升级，故障修复，NBD备件、备机先行服务。 |

**5.2.2.2 万兆防火墙**

|  |  |  |
| --- | --- | --- |
| **指标** | **技术参数** | |
| ▲基本要求 | 系统结构 | 产品由专用的硬件平台、安全操作系统及功能软件构成。设备采用自主知识产权的专用安全操作系统，采用多核多平台并行处理特性（提供相应资质证明复印件并加盖投标人公章）； |
| 操作系统 | 安全操作系统采用冗余设计，出于安全性考虑，多系统需在设备启动过程中进行选择不得在WEB维护界面中设置系统切换选项。  必须是国产安全产品，提供信息安全测评中心颁发的《信息安全产品自主原创证明》复印件并加盖投标人公章；  为保证系统软件设计全面性、保密性、完整性，要求招标产品系统遵从行业标准和政府法规，符合GB/T 18336信息技术安全性评估标准，提供信息技术产品安全测评EAL4+证书复印件并加盖投标人公章； |
| 接口配置 | 2U机箱 最大配置≥34个接口， 默认包括4个可插拔的扩展槽和2个10/100/1000BASE-T接口，配置≥4个万兆SFP+接口，并配置4个万兆光模块，标配模块化双冗余电源，默认包含应用识别功能 |
| ▲系统要求 | 产品设计 | 信息安全设备、系统软件的开发、生产符合TL9000-HSV 标准，提供相关证明复印件并加盖投标人公章； |
| ★系统性能 | 防火墙吞吐 | ≥32Gbps |
| 最大并发 | ≥800万 |
| 网络  接入 | 工作模式 | 支持路由、交换、混合、虚拟线工作模式； |
| 主备部署 | 考虑到整体网络可靠性与可用性，提高整体网络的冗余能力，防火墙支持主备冗余模式部署，避免出现单点故障；正常情况下，两台设备只有主墙在运行，从墙处于待机状态。网络数据只由主墙交互。  当主墙的链路断开时，主墙通过心跳线告知从墙，监控接口出现故障，由从墙接替主墙继续运行。此时主墙处于待机状态，从墙处于工作状态。 |
| 路由交换 | 支持静态路由、ISP路由及动态路由协议，支持802.1q、QinQ模式； |
| 支持基于源/目的地址、源/目的端口、用户、应用的策略路由，保证关键业务流量通过优质链路转发； |
| 接入功能 | 支持GRE与IPSEC VPN接入； |
| 链路聚合 | ▲为提高链路可靠性，需支持手工链路聚合及LACP链路聚合，提供不少于11种的负载分担算法，灵活实现对聚合组内业务流量的负载分担（提供相关截图并加盖投标人公章；） |
| IP/MAC绑定 | 支持手动添加绑定，基于IP、接口的动态探测绑定，支持跨三层IP/MAC绑定，IP/MAC绑定表可导入导出； |
| 地址转换 | 支持一对一SNAT、多对一SNAT、一对一DNAT、双向NAT、NoNAT等多种转换方式；支持Sticky NAT开关，使相同源IP的数据包经过地址转换后为其转换的源 IP 地址相同；（提供相关截图并加盖投标人公章） |
| ▲支持MAP66功能，将从内部发往Internet的数据包的源IPv6地址修改为全球单播源IPv6地址，实现IPv6网络间的地址转换；（提供相关截图并加盖投标人公章） |
| 智能DNS | 支持智能DNS及DNS Doctoring功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡 |
| IPv6 | 双栈模式 | 支持IPv4/IPv6双栈工作模式； |
| 访问控制 | 支持IPv6安全控制策略设置，能针对IPv6的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置； |
| 安全防护 | 支持基于IPv6的应用层检测（FTP\TFTP）、病毒过滤、URL过滤、ADS、IPS检测； |
| 为适应IPv6发展，要求产品支持IPv6环境接入、支持IPv6&IPv4双栈运行，支持RFC246X、RFC4861、RFC4862等IPv6一致性测试要求 ； | |
| 用户管控 | 认证方式 | 内置强大的用户身份管理系统，支持本地认证、证书认证及免认证等方式，同时支持RADIUS、LDAP、TACACS等多种第三方外部认证设置； |
| 用户管控 | 综合运用身份认证与访问控制技术，通过内置智能过滤引擎实现基于用户身份的安全防护策略部署与可视化监控；支持手动创建用户、批量导入导出用户，同时支持设备扫描方式创建用户； |
| 支持设置密码有效性，如首次登陆修改密码、密码定期修改、密码有效时间等设置，用户忘记密码时，支持密码找回； |
| ▲支持本地CA和第三方CA，支持作为CA认证中心为其他人签发证书，也可采用第三方CA为其他人签发证书（提供相关截图并加盖投标人公章）；支持标准CRL列表，支持CRL手工更新，同时支持CRL自动下载，通过HTTP或者LDAP方式定时自动下载更新CRL文件； |
| 应用管控 | 应用识别 | 内置强大应用识别引擎，综合运用端口识别、行为识别、特征识别、关联识别等技术手段，准确识别传统应用如P2P、web应用、移动应用、云应用、加密应用等；内置独立应用识别特征库，总数2100种以上，支持应用特征库在线或本地更新，支持应用特征自定义； |
| 带宽管理 | 支持基于IP/IP组、用户/用户组、服务/服务组、应用/应用组和时间等配置带宽策略，支持带宽策略优先级，可配置包含链路、父通道、子通道的5层多级带宽策略，对流量进行细分管理，保证带宽的利用率； |
| 连接控制 | 支持对单条访问控制策略进行最大并发连接数限制； |
| 为保护内部网络资源以及合理分配设备系统资源，需支持对指定的源/目的IP地址、MAC地址、应用制定相应的连接限制策略，策略包含三种限制类型：单个IP每秒新建连接限制、单个IP连接数限制及连接总数限制； |
| 支持监控功能，显示最近被拦截的IP、地址对象及应用的节点信息；同时支持对连接数限制策略匹配信息进行分类统计，方便管理员根据统计分析结果进行相应的防护控制； |
| 访问控制 | 一体化访问控制 | 内置高度集成的一体化智能过滤引擎技术，实现在同一条访问控制策略中配置传统的五元组信息、用户、域名、应用、服务、时间、安全引擎（入侵防御、URL过滤、病毒过滤、数据过滤、文件过滤、审计）的识别与控制； |
| 访问控制策略执行动作支持允许、禁止及认证，对符合条件的流量进行Web认证，在策略中可设置用户 Web 认证的门户地址； |
| 提供智能策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查，并且可在WEB界面显示检测结果：红色为冗余策略，绿色为冲突策略； |
| 支持黑名单功能，可设置多个对象条件，如：五元组信息、地址范围、应用、用户等，实现对特定报文进行快速过滤； |
| 安全防护 | DDOS防御 | 内置流量检测清洗引擎，支持基于IP、ICMP、TCP、UDP、DNS、HTTP、NTP等众多协议类型的防护策略；提供丰富的策略模板，且支持策略模板自定义； |
| 支持根据DOS/DDOS攻击行为自动添加动态黑/白名单功能，可自定义动态黑/白名单超时时间； |
| 入侵防御 | 内置攻击检测引擎，采用协议分析、模式识别、统计阀值和流量异常监视等综合技术手段来判断入侵行为；支持web攻击识别和防护，如跨站脚本攻击、SQL注入攻击；支持超过4100+攻击特征库（提供截图），同时支持自定义特征库,且厂商具备强大的漏洞和功放研究能力，为CNNVD一级支撑单位，能够确保每周至少更新1次攻击特征库。 |
| 病毒过滤 | 内置病毒检测引擎，支持HTTP/SMTP/POP3/FTP/IM等协议的病毒防御，对每种协议数据流的检测方向可选双向、上传、下载； |
| ▲内置至少2种专业反病毒厂商或研究机构的病毒特征库，符合等级保护相关标准对网关防病毒特征库和主机防病毒特征库异构的要求。（提供至少2家专业防病毒厂商或研究机构的合作文件复印件或承诺合作证明文件并加盖投标人公章）病毒特征库规模超过400万（提供截图） |
| 支持病毒白名单，用户可以根据实际业务需求将特定威胁进行排除；（提供截图并加盖投标人公章） |
| 文件过滤 | 内置文件过滤引擎，支持对即时通讯、社交网络、网络硬盘、网页邮箱、IM文件传输等应用类型以及HTTP/FTP/SMTP/POP3等标准协议进行检测，识别可执行文件、office文件、视频文件、图片文件、帮助文件、压缩文件、数据文件等超过50种文档类型的文件过滤； |
| 内容过滤 | 支持基于http、ftp、telnet、smtp、pop3等协议的内容过滤策略，可对微博、贴吧上传的内容及附件进行过滤，可对FTP上传/下载的文件名进行过滤，同时支持过滤FTP信令：上传文件、下载文件、删除文件、重命名文件、创建目录、删除目录、列出目录等，邮件过滤支持对发件人、收件人、主题、内容、附件等进行过滤； |

**5.2.2.3 核心交换机**

|  |  |
| --- | --- |
| 指标 | 技术参数 |
| 实配 | 双主控板，交换网板≥5，3000W电源≥4，10GE以太网光口≥48，GE以太网电口≥48 |
| ★设备性能 | 交换容量≥367Tbps，包转发率≥230400 Mpps（提供产品官网截图并加盖投标人公章及链接） |
| 硬件规格 | 业务槽位数≥8 |
| ▲交换网板插槽数量≥6, 且支持网板N+M 冗余，并提供官网截图并加盖投标人公章; |
| ▲CPU、LSW均为国产自研芯片，提供第三方测试报告并加盖投标人公章； |
| ▲风扇框冗余设计，要求风扇框个数>=3,任意风扇框故障或者不在位不能造成业务中断，并提供设备硬件截图并加盖投标人公章 |
| 基于正交CLOS架构设计，主控引擎与交换网板硬件分离,主控板故障或者更换不影响整机转发性能； |
| 支持信元交换：要求单条流可以负载分担到多块交换网，提高交换网利用效率，提供官网截图并加盖投标人公章 |
| 严格前后风道 |
| 二层功能 | 支持端口聚合，802.3ad |
| 支持M-LAG或vPC等类似技术（跨框链路聚合，要求配对设备有独立的控制平面，不能用堆叠等多虚一技术实现）。 |
| 支持N:1镜像、流镜像、远程端口镜像 |
| 三层功能 | 支持RIP、OSPF、ISIS、BGP等IPv4动态路由协议 |
| 支持RIPng、OSPFv3、ISISv6、BGP4+等IPv6动态路由协议 |
| ▲支持IP分片和重组，提供官网截图并加盖投标人公章 |
| QoS | 支持PQ、WFQ、PQ+WFQ等队列调度方式 |
| 支持ACL、CAR、Remark等动作 |
| 支持WRED、尾丢弃等拥塞避免机制 |
| 支持流量整形 |
| 支持出方向ACL，CAR，统计 |
| 可靠性 | 支持硬件BFD（Bidirectional Forwarding Detection）3.3ms检测间隔。 |
| 支持堆叠、群集、双机功能，当其中一台交换机发生故障时，另一台毫秒级协商完成主备切换，接替原有业务，保证业务连续性。 |
| DC特性 | 支持1虚多技术，最多能虚拟成16台逻辑交换机 |
| 支持Vxlan协议，且支持BGP EVPN协议 |
| ▲支持缓存的微突发状态统计，提供官网截图并加盖投标人公章 |
| 支持MAC Flapping |
| 支持VXLAN over IPv6 |
| 支持IPv6 VXLAN over IPv4 |
| 安全性 | 支持二层到四层的ACL |
| 支持微分段，提供官网截图并加盖投标人公章 |
| 支持单播、组播和广播风暴控制 |
| 支持DHCPv4 Server、Relay和snooping |
| 支持IP/ARP/ICMP 安全 |
| 配置和维护 | 支持Telemetry |
| 支持VxLAN OAM: VxLAN ping, VxLAN tracert |
| ▲支持iPCA，提供官网截图并加盖投标人公章 |
| 支持配置回滚 |
| 支持BootROM升级和远程在线升级 |
| 支持Ansible自动化配置，Module开源发布。 |
| 流量分析 | 支持Netstream |

**5.2.2.4 上网行为管理**

|  |  |
| --- | --- |
| 指标项 | 技术参数 |
| ★性能配置 | 产品为标准2U机架式设备，需满足多核X86架构，48G内存。双电源，4个千兆电口，4个千兆光口，4个万兆光口， 1个串口(RJ45) ，2个USB2.0。性能配置：  网络吞吐量≥30Gb  推荐带宽性能≥15Gb  用户规模≥150000人  并发会话数≥15800000  硬盘≥1TB+64G SSD  支持BYPASS |
| 部署方式 | 要求设备支持网关模式，支持NAT、路由转发、DHCP等功能；支持网桥模式，以透明方式串接在网络中；支持旁路模式，无需更改网络配置，实现上网行为审计；必须支持两台及两台以上设备同时做主机的部署模式。 |
| 登陆设置 | 设备可以设置登录密码不等于用户名，可设置密码最小长度以及密码组成中包括数字或字母或特殊字符，密码更改时新旧密码不能相同 |
| IPv6支持 | 支持部署在IPv6环境中，其所有功能（认证、应用控制、内容审计、报表等）都支持IPv6 |
| 高可用性 | 支持设备双机部署，支持主主模式、主备模式两种双机模式部署。 一旦发生单点故障可以实现热备切换，不影响业务访问。支持和原有机房行为管理设备联动，方便管理和操作。 |
| 链路负载 | 为了提高出口多链路利用率，要求支持按剩余带宽、带宽比例、平均分配、前面优先的方式进行多链路负载。支持使用VPN做专线备份，支持链路故障检测； |
| 多终端自动绑定 | 同一个账号，支持与指定数量的多个终端进行自动绑定； |
| 域属性和用户属性 | 新增域属性和用户属性，用户上网策略和流控策略可以直接引用，给策略提供更多维度的权限划分。 |
| 公共账号个数限制 | 公共账号可以提供给多个人同时上网，可以指定公共账号的同时上线人数。避免公共账号被滥用。 |
| 业务需要 | ▲支持二维码认证，管理员扫描访客的二维码后对其网络访问授权（提供产品界面截图并加盖投标人公章） |
| ★对私接无线上网的行为管理，要求设备能自动发现网络中通过无线上网的热点和移动终端的IP和终端类型，匹配管理员配置的热点信任列表，对信任列表外非法接入的热点和终端能够进行阻止上网，支持冻结用户IP，并通过邮件形式告警通知管理员，支持显示以IP或用户名的维度统计一段时间内的趋势图。（提供产品界面截图并加盖投标人公章） |
| 针对内网用户的web访问质量进行检测，对整体网络提供清晰的整体网络质量评级，支持以列表形式展示访问质量差的用户名单，支持对单用户进行定向web访问质量检测 |
| 应用识别规则库 | 目前互联网应用种类较多，为降低管理员配置管理策略的难度，要求设备能够按照管控需求对应用进行标签化，应用标签至少默认包含安全风险、高带宽消耗、发送电子邮件、降低工作效率、外发文件泄密风险、主流论坛和微博发帖6大类，此外可根据我单位需求自定义标签，根据标签做应用控制。 |
| 应用控制 | 设备内置应用识别规则库，支持超过5500条应用规则数，支持超过2800种以上的应用，1000种以上移动应用，并保持每两个星期更新一次，保证应用识别的准确率； |
| 移动应用的细分控制 | 支持对移动应用的细分权限控制，微信：微信网页版、微信传文件、微信朋友圈、微信游戏。移动QQ：QQ传文件、QQ视频语音等。 |
| URL访问及关键字控制 | 要求设备内置海量的URL地址库，可根据访问URL的网页关键字进行过滤控制，特别对于SSL加密的网页、论坛、BBS上的发帖行为也需要支持关键字过滤控制 |
| 流控黑名单 | 基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中（需提供配置界面截图并加盖投标人公章） |
| 认证黑名单 | 每条认证策略提供黑名单功能，在黑名单中的用户不能通过认证上线。 |
| 终端管理 | 支持终端调用管理员指定脚本/程序以满足个性化检查要求，比如检测系统更新是否开启、开放端口、已安装程序列表、终端发通知等； |
| 动态流控 | 要求设备可以针对整体线路或者某流量通道内流量情况进行实时监控，根据设定的流量空闲值自动的调整流控控制策略，提升我单位带宽使用率 |
| P2P智能流控 | 支持通过抑制P2P的上行流量，来减缓P2P的下行流量，从而解决网络出口在做流控后仍然压力较大的问题； |
| 移动APP审计 | 支持常见论坛（天涯社区、猫扑社区、百度贴吧、新浪论坛、搜狐社区等）、微博（新浪）、新闻评论类（腾讯新闻、网易新闻、搜狐新闻、新浪新闻）的移动APP内容审计 |
| IM审计 | 支持对QQ（客户端版本）、阿里旺旺、万德（Wind）、路透等应用的聊天，群聊天等内容的审计 |
| 邮件审计 | 支持对加密HTTPS、SMTP-SSL、SMTP-TLS、SMTP、Gmail、闪电邮客户端的邮件进行关键字过滤 |
| SSL加密网页 | ▲为确保我单位不会通过SSL加密内容发生通过互联网出口泄密事件，要求设备必须能够识别并过滤SSL加密的钓鱼网站、金融购物网站、非法网站等（提供自主知识产权证明并加盖投标人公章）；审计SSL网页时，支持加密证书自动分发功能，用户点击网页上的工具即可一次性安装完成。解决管理员给每台PC单独安装证书的问题（要求提供产品界面截图并加盖投标人公章） |
| 网络整体状况报表 | 设备能根据管理者自定义的风险行为特征自动挖掘并输出离职风险、泄密风险、安全风险、工作效率风险、法律风险智能报表 |
| 单用户行为分析 | 针对单用户的行为分析（包括：应用流速趋势、应用流量排行、域名流量排行、应用时长排行、域名时长排行、行为汇总排行等） |
| 趋势报表 | ▲支持基于时间段/用户/用户组/终端类型/位置等多种维度的流速趋势报表、流控通道趋势报表、应用行为趋势报表、网站分类行为趋势报表等（提供产品界面截图并加盖投标人公章） |

**5.2.2.5 日志服务器**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 规格 | 2U，支持导轨及理线架 |
| 处理器 | Intel Xeon SP系列处理器 |
| 本次处理器配置数量：2个英特尔至强银牌4210 |
| 内存 | 内存类型：ECC DDR4 2400MHz或以上 RDIMM |
| 内存插槽 支持≥16个 |
| 本次配置内存容量：64GB |
| 存储 | 内置硬盘类型：热插拔SAS/SATA/SSD硬盘 |
| 本次配置内置硬盘容量数目：6\*8TB SATA |
| 网口 | 配置2\*GE电口 |
| 阵列卡 | Raid8222 |
| 扩展 | 最多 2 个 x16 插槽 ；VGA、4个USB、串口 |
| 管理 | idrac9 with Lifecycle Controller (Express、Enterprise)，专用 IDRAC 微型 USB和网口 |
| 电源 | 本次配置2\*550 W |

**5.2.2.6 态势感知平台1套（包含态势感知、网络流量综合探针、日志审计探针1台）**

|  |  |
| --- | --- |
| ★产品形态 | 1.为灵活适应现场环境，必须满足软硬一体化形态和纯软件形态部署模式，软件形态支持部署在物理机/虚拟机/云环境；  2. 支持横向平滑扩展，可以通过增加硬件服务器数量的方式增加平台集群的计算处理性能。 |
| ★物理机硬件配置 | CPU≥24核，内存≥256GB，配置企业级存储磁盘总容量≥48TB（或磁盘可用容量≥40TB）；  接口要求：千兆电口\*2 |
| 性能规格 | 能够实时深度解析≥10Gbps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；  10亿数据关键字查询结果响应时间<2秒。 |
| 数据接入 | 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；  支持通过云端对接、本地导入或手动编辑的方式，接入威胁情报数据。 |
| 数据共享 | 大数据平台中的安全数据，包括告警数据、资产数据、工单等至少20种可共享给第三方系统，实现数据共享和交换；  同时支持原始日志、标准化数据、告警数据≥3种数据的共享和交换。 |
| 性能检测 | 设备在线状态检测；  Web应用访问成功率检测；  服务器性能检测。 |
| 安全分析和自动化编排 | 1.平台应内置包括规则模型、关联模型、统计模型、情报模型、离线模型等在内的≥5大类安全分析模型；  2.安全分析模型支持自定义创建，可通过字段映射、静态值、模板、表达式等多种方式自由定义分析模型的告警名称、威胁等级、告警类型、攻击链、可选字段、告警描述、处置建议等内容；  3.支持对安全日志里200个以上字段进行任意形式的逻辑与或非形式组合建模，并能根据组合方式自动生成运算表达式；  4.支持与不同品牌的网关类安全产品进行联动防护，防护策略支持设置每次阻断不同时长生效时间，时间设置包括10分钟，30分钟，6小时，24小时，72小时，永久阻断；  5.支持与EDR集成联动，一键查杀木马病毒； |
| AI高级分析 | 平台内置不少于8种机器学习分析场景模型，可检测发现勒索挖矿告警数异常、安全设备日志数异常、网络会话数异常、域名请求数异常等特定场景条件下的安全态势异常；  支持自定义部署AI机器学习模型，允许用户选用的高级机器学习算法不少于4种，通过输入任意指标类数据进行模型训练，发现异常行为并生成安全事件与告警，辅助用户发现潜在的安全风险。  ▲支持时间序列、UEBA、Bayes、随机森林等长周期高级机器学习算法；（提供相关功能相关专利受理证明材料复印件并加盖投标人公章） |
| 网络实体分析画像 | 实现实体间网络互访关系的多级钻取，支持≥5跳的流量自动关联关系分析，支持通过端口、协议、异常访问类型过滤关联关系；  支持与终端检测类产品对接，查看主机进程、软件版本、漏洞病毒情况。 |
| 场景化分析 | 1.支持暴力破解、Web攻击、恶意程序、端口扫描等内置安全分析场景，基于场景特性进行默认条件的数据聚合分析，支持至少3个任意字段的快速聚合分析，聚合后的所有数据均支持快速统计分析，展示统计排序信息，支持分析结果导出。  2.支持自定义场景安全分析，可对安全告警的任意字段进行聚合分析，支持的聚合的字段不少于300个，支持分析结果导出；  3.支持智能检索语句分析，支持检索语句的中英文、拼音智能联想，支持逻辑运算符与字段值的自动提示补全；检索语句支持快速保存，历史检索语句快速导入；检索语句可直接发布成实时分析模型，对实时数据进行分析与告警。 |
| 取证分析 | ▲支持调查场景的四维自定义攻击流向图取证，攻击趋势取证、攻击链分布取证、和实体信息取证，展示攻击者和受害者的威胁情报与资产信息，可联动会话详情，点击查看不同溯源维度的会话详情，通过请求头，payload等详情字段定位攻击（要求提供截图并加盖投标人公章）  支持对原始日志的数据挖掘分析，可选择柱状图、折线图、面积图、表格、数值图、饼状图等多种报表样式自由对历史数据的任意字段进行可视化统计分析，辅助研判安全事件风险。 |
| 安全态势可视化 | 1.支持安全态势的可视化呈现，以大屏的方式从攻击事件、资产安全、追踪溯源、运行监测、重保方案等多个维度进行可视化展示，提供不少于10块大屏展示界面；  2.支持外部对内部攻击、内部跨安全域横向攻击、内部外连攻击3种威胁方向监测。 |
| 仪表盘 | 支持可视化图表类型≥15种，包括但不限于时序图、饼图、柱状图等；  统计类图表支持展示升序或降序的TOP5到TOP100，可针对数据中任意字段的计数、平均值、求和、最大值、最小值、唯一值等≥5种算子的统计结果配置可视化图表；  可视化图表可通过拖拽配置组装成仪表盘，仪表盘不少于7种布局类型，仪表盘展示时支持时间范围自定义选择。 |
| 安全运营门户 | 1.平台应具有统一的安全运营门户，作为多个安全态势分析与感知功能的统一入口，集成态势感知、威胁狩猎、通报预警、异常监测、运行监测等多个功能模块，实现平台内部业务、数据、服务、资源的无缝整合与集成；  2.支持每个用户配置个人专属的统一门户，可配置项包括门户名称、应用名称、应用图标等  3.统一门户应支持与第三方产品集成，一键跳转至产品功能界面。 |
| 智能检索 | 支持对原始日志数据、安全告警数据进行分类检索，从检索结果可关联威胁情报和资产信息并一键跳转；  支持不少于10000条检索结果导出，导出内容字段可自定义选择，支持excel或CSV格式。 |
| 数据字典管理 | 支持管理系统中原始日志、安全事件、安全告警的所有字段和取值，每个字段均有清晰的说明；  支持数据标准管理，用户可以根据实际需求，对字典进行编辑，支持手动修改、增加或删除相应的字段； |
| 威胁情报 | 支持通过离线导入或手动编辑添加的方式，形成本地威胁情报，允许用户自建行业情报库，并实现情报库的增删改查、导入、导出功能  情报查询支持通过IOC同时跨越多个情报源查询，结果汇总展示；  ▲碰撞情报IOC支持通过情报源、IOC类型、标签、置信度等多维度进行碰撞分析，内置威胁情报条数不少于400万条。（要求提供截图并加盖投标人公章） |
| 资产管理 | 支持通过流量无侵入式自动发现资产，支持发现终端、Web服务器、DNS服务器、邮件服务器、FTP文件服务器等类型≥5种，其中web服务器支持自动识别服务域名和服务站点名称；  支持资产信息的全量导入导出；  支持一键访问安全设备的管理界面、监控大屏、设备日志、处置联动记录；  支持以单个IP地址、IP区间、子网掩码等3种模式录入安全域信息。 |
| 业务拓扑监控 | 支持拓扑图的增加、修改、删除、导入、导出，支持创建>50个业务或网络拓扑，支持建立平面拓扑和3D拓扑；  支持监控安全域、Web业务系统、服务器、终端、安全设备等至少5种网络实体类型；  支持在拓扑图上一键点击跳转查询相应网络实体的安全日志。 |
| 安全运营 | 支持统一的安全运营工作台，在工作台可以集中查看当前用户的待办工单、最新通报预警状态  工单详情与备注支持多种内容格式，包括但不限于文字、图片、超链接、表格、代码片段、附件等类型；  支持工单举证信息一键溯源，工单处置人员可以直接定位到工单关联的原始信息进行查看；  支持通过安全告警自动派发工单到对应的安全管理员，支持自定义编辑预警信息内容；  支持将预警信息直接转为内部通报，支持将通报内容作为工单定向指派。 |
| 安管协作 | 组织架构中各级单位支持设定独立的安全管理员、业务系统、安全域；  支持多级管理员间资产风险信息的隔离和共享，总部用户管理员可以分配下属组织架构的功能权限。分部安全管理员只可以使用所属组织架构具备的功能；  支持按月和按周考核各组织架构的安管工作成果。 |
| 分析报告 | ▲支持用户自定义编辑报告模板，根据实际的业务需求自定义统计分析的指标对象，生成有针对性的分析报告，安全分析中的所有字段内容，都可以作为报告的统计对象，并自定义时间范围实现报告导出；（要求提供截图并加盖投标人公章）  内置深度威胁分析、攻击者取证等2个以上报告模板，报告订阅支持通过邮件方式在设定时间点发送日报、周报、月报到不同邮箱，可配置订阅规则数量≥10条。 |
| 重大活动保障 | ▲支持重大活动保障任务前期、中期、后期分阶段的任务管理，保障预案管理；（要求提供截图并加盖投标人公章）  支持任意保障区域和系统，支持设置保障监控拓扑，支持重大保障态势大屏实时监测；  保障监测视角覆盖云管端、边界、应用、安全设备等监测维度≥6种。 |
| 黑白名单 | 支持通过黑白名单功能对分析对象进行过滤筛选；  支持通过任意字段进行组合，配置筛选条件并生成黑白名单过滤规则。 |
| 运维监控 | 1.支持大数据平台本身的计算、存储资源利用率监控；  2.支持数据集与数据索引健康度监控；  3.支持对平台各组件运行健康状态的集中监控  4.支持平台运行状态告警，运行监测引擎可独立于安全分析引擎工作，展示运维告警趋势、分布等  5.支持态势感知平台一键巡检，一键检查项包含但不限于数据健康、探针健康检查、大数据集群健康、Elasticsearch健康、实时流计算引擎健康、管理服务健康、服务器节点健康等多种维度检查，并能提供处置建议，一键导出各类服务的故障日志，包括但不限于Elasticsearch、Logstash、Ka\*\*a、实时计算引擎、操作系统等。 |
| 用户管理 | 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。 |
| 系统恢复 | 支持安全模型的启用状态恢复出厂设置；  支持通过权限认证实现数据恢复出厂设置。 |
| 级联管理 | 适配部、省、市、区、县的多级部署架构；  总部支持查询全网安全态势和告警，分部只支持查询单位内部相关的安全态势和告警。 |
| 监控终端 | 提供监控终端设备2台、27寸显示器4台及≥65英寸实时监控展示平台一台，作为态势感知平台数据实时展示。 |
| **网络流量综合探针1台** | |
| 硬件参数 | 软硬一体化2U标准机架式设备；  1+1冗余电源；  内存≥128G；  可用硬盘容量≥2T，支持RAID1；  接口数量不少于 10个，其中千兆RJ45网口不少于4个，千兆SFP光口不少于4个，万兆光口不少于2个；  吞吐率≥10Gbps； |
| 高可用性 | 部署方式：旁路镜像模式部署，不影响服务器处理性能和网络架构；  运行监控： 可监控系统CPU、内存、磁盘使用情况、网口状态、网口流量、网口丢包情况及数据外送量大小情况。 |
| 数据同步 | 支持通过KA\*\*A接口向态势感知平台报送流量审计数据与风险告警信息  自定义配置：可在前端页面自定义配置探针与大数据平台之间的数据传输类型、各类型数据均支持任意字段的发送配置。 |
| 行为审计与  可疑通信检测 | 支持违规操作、违规访问、违规应用、违规外发等300种以上行为审计检测规则，可针对任意单条规则进行启用和禁用；  支持隧道通信、可疑内容、恶意IP、恶意域名、恶意证书、远程控制等3000种以上可疑通信检测规则，可针对任意单条规则进行启用和禁用； |
| 扫描探查检测 | ▲支持端口扫描、服务扫描、Web扫描、扫描器指纹检测等300种以上的扫描探查检测规则，可针对任意单条规则进行启用和禁用；（要求提供截图并加盖投标人公章） |
| 漏洞利用检测 | ▲支持SMB漏洞、RDP漏洞、软件漏洞、设备漏洞、系统漏洞、拒绝服务漏洞、shellcode等7000种以上漏洞利用检测规则，可针对任意单条规则进行启用和禁用；（要求提供截图并加盖投标人公章） |
| 恶意文件检测 | ▲支持挖矿活动、流氓软件、可疑文件、勒索软件、僵木蠕、Webshell等25000种以上恶意程序检测规则，可针对任意单条规则进行启用和禁用；（要求提供截图并加盖投标人公章） |
| 配置风险检测 | 支持弱口令风险、明文传输风险、HTTP配置风险、中间件配置风向、数据库配置风险、服务配置风险等100种以上配置风险检测规则 |
| 主机和账号异常检测 | 支持端口异常、主机对外扫描、主机对外攻击等主机异常检测能力，对任意单条检测规则支持启用和禁用。  支持登录异常、暴力破解、行为异常等账号异常检测能力，对任意单条检测规则支持启用和禁用 |
| Web攻击检测 | 支持Webshell请求、XSS攻击、SQL注入、远程代码执行、命令注入、远程文件包含、本地文件包含、文件上传、路径遍历、信息泄露、越权访问、XXE注入、网页篡改等13类、6000种以上web攻击检测规则，对任意单条检测规则支持启用和禁用 |
| 规则库管理 | 威胁检测规则数量≥43000种，针对任意单条规则支持页面启用、禁用；  威胁检测规则支持页面查看，具备中文相关介绍，包括但不限于漏洞名称，危险等级，影响系统，对应CVE编号；  支持基于规则ID、规则名称、CVE编号、规则等级、规则类型、规则状态、应用协议等不同条件进行规则快速检索； |
| 策略管理 | 支持IP地理信息重映射，用户可新增指定IP或IP段的地理信息，支持IP或IP段地理信息导入导出，确保输出数据地理信息准确；  支持IP NAT配置管理、flow数据清洗管理。 |
| 系统管理 | 支持与态势感知平台进行数据同步，同步信息包括安全域、内IP等；  支持前端可视化配置管理接口、监听接口，包括修改IP地址、启用禁用监听接口等  ▲支持前端可视化进行设备运维操作，包括重启设备、关机重启服务、开关SSH服务等，可一键下载探针运行日志，方便运维人员日常运维工作（要求提供截图并加盖投标人公章）。 |
| **日志审计探针1台** | |
| 工作模式 | 独立完成审计日志采集，不依赖于设备或系统自身的日志系统；  审计结果存储于独立存储空间；  提供全中文WEB管理界面，无需安装任意客户端软件或插件。 |
| 硬件规格 | 4个电口；  内存：64GB，磁盘：4T\*4 RAID5；  双电源、非CF卡启动；  可扩展项：内存可扩展至128GB，单个磁盘可扩展至4T（8个盘位），支持HBA卡扩展，网口可扩展至12个（本次配置4电、2万兆光）。 |
| 处理性能 | 支持审计500个日志源；  平均处理能力（每秒日志解析能力EPS）：10000 EPS；  峰值处理能力（每秒日志解析能力EPS）：14000 EPS。 |
| 功能扩展 | 采用解决方案包上传对产品进行功能扩展，无需要代码开发；  支持ka\*\*a日志接收转发、大数据安全域同步、APT沙箱报告转发等大数据联调功能；  支持手动或按周期自动备份系统配置，可随时对系统资产等配置进行还原操作，且自动备份周期与备份包个数可配；支持系统配置备份自动备份至远程服务器。 |
| 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；  支持常见的虚拟机环境日志收集，包括Xen、VMWare、Hyper-V等。 |
| 日志分析 | 可以基于日志等级进行过滤；  支持对收集到的重复日志进行自动聚合归并，减少日志量；  支持可由用户定义和修改的日志聚合归并逻辑规则;  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；  内置非法访问、可疑入侵、病毒爆发、设备异常、弱点针对等5大类50子类的安全分析场景；  进行关联分析的规则可定制；  ▲三维关联分析；支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件（提供第三方检测报告复印件并加盖投标人公章）。 |
| 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、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；  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。 |
| 应用性能监控  （APM） | 支持监控设备自身CPU、内存、磁盘等工作运行状况；  ▲通过在目标主机上安装Agent程序，支持监测目标主机的CPU利用率、内存使用率、磁盘使用率、磁盘使用情况、流量等信息（提供第三方检测报告复印件并加盖投标人公章）；  支持以下对象的性能监控：  操作系统 - Windows、Linux、Aix、FeeBSD、HP-UX/Tru64、Max OS、Sun Solaris、数据库 - MySQL、Oracle、应用服务器 - Weblogic、Tomcat、Web服务器 - Apache  支持应用性能历史详情回溯查看； |
| 脆弱性管理 | 支持从IBM Rational AppScan、安恒明鉴Web应用监测工具、安恒明鉴数据库弱点扫描器、NetSparker Web应用扫描器、Nessus网络扫描器、OpenVAS扫描器导入资产弱点漏洞信息；  内置73000+条CVE漏洞数据知识库；  内置数十项符合OWASP的Web漏洞数据知识库。 |
| 地理安全系统 | 内置GeoSec地理安全子系统，内置世界以及中国安全GIS地图；  支持在地理地图上标注威胁事件的发生分布；  内置IP地址到经纬度的转换库；  支持切换Google地图（需要连通互联网）。 |
| 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；  ▲支持磁盘空间阈值告警，当磁盘使用率达到设定的阈值时可产生并外发告警；资产性能监控异常告警，对于监控的资产系统资源进行监测当指定指标使用率达到设定的阈值时可产生并外发告警；资产状态监控，当资产处于不活跃状态时可产生并外发告警；远程仓库状态监测可告警，当远程仓库可用性检测失败或备份包自动上传失败时可产生并外发告警（提供该功能截图并加盖投标人公章）。 |
| 综合查询及报表管理 | 内置合规性报表1000+种；  内置SOX、ISO27001、WEB安全等解决方案包；  内置完善的等级保护合规报表；  支持用户自定义报表；  支持报表导出为PDF和Word格式文件。 |
| 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；  用户支持双因子认证登录，双因子认证令牌支持绑定至具体用户；  提供一键式故障排除功能； |
| 资产管理 | 注册用户资产时，提供自动发现识别能力；  ▲资产拓扑支持按照实际的用户环境进行编辑发布并可以和资产进行绑定，拓扑可以显示资产采集的事件数量被采集资产的状态等信息（提供第三方检测报告复印件并加盖投标人公章）。 |
| 部署方式 | 支持分布式部署，支持页面一键添加子节点资产，自动进行绑定添加；  支持分级管理模式； |

**5.2.2.7 数据库审计设备1台**

|  |  |
| --- | --- |
| 硬件规格 | 产品采用专用工控机硬件架构，非普通PC服务器，MTBF(平均故障间隔时间)≥65000小时；  处理器采用Intel高性能CPU，内存≥16GB DDR3 1600Mhz，硬盘≥4TB（2T\*2），支持RAID1，最大支持扩展到4T\*2硬盘；  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, 2个万兆光口；  支持最大扩展至8电8光或16电或16光共16个千兆以太网口。 |
| 处理能力 | 审计性能：同时支持12个数据库数审计能力，不会产生漏审；  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 | 为适应各种复杂的部署环境，产品部署模式应满足以下要求：  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，（提供第三方检测机构检测报告复印件并加盖投标人公章；）  支持分布式部署，管理中心可实现统一配置、统一报表生成、统一查询；  管理中心和探测器都可存储审计数据，实现大数据环境下磁盘空间的有效利用和扩展；  支持IPV4/IPV6双栈审计；  支持和ES平台对接，将审计日志和告警日志存储在ES系统中，并支持通过页面查询日志；  支持在审计页面配置审计代理的CPU亲和性、最大CPU使用率、最大内存使用率、CPU使用率阈值、内存使用率阈值、流量接收端口、抓包过滤串；  支持在审计页面批量安装、卸载、重新安装审计代理。 |
| 协议支持 | 为审计和防护不同类型、不同版本的数据库，产品协议支持应满足以下要求：  支持Oracle、SQL Server、DB2、Informix、Sybase、MySQL、MariaDB等主流数据库审计；  支持PostgreSQL、GuassDB、HANA、Teradata、人大金仓（Kingbase）、达梦（DM）、南大通用数据库（Gbase）、Oscar、Redis审计；  支持MongoDB、Hbase、Hive、impala、Elastic Search、HDFS、Canssandra非关系型数据库审计；  支持主流业务协议HTTP、HTTPS、Telnet、FTP的审计；  可以通过导入证书的方式实现审计和防护，支持对SQL Server（2005及以上版本）数据库；  ▲可以通过导入证书的方式实现MySQL 5.7及以上版本采用了加密协议通讯的审计（提供功能截图并加盖投标人公章）；  支持对各种协议自动识别编码及在web界面手工配置特定编码。 |
| 审计功能 | 为满足对数据库操作行为审计，满足业务、安全等方面的需求，产品需要满足以下要求：  支持数据库操作表、视图、索引、存储过程等[各种对象的所有SQL操作审计](" \l "_支持各种对象的SQL审计_1)；  ▲支持数据库请求和返回的双向审计，特别是返回字段和结果集、执行状态、返回行数、执行时长、客户端工具、主机名等内容，支持通过返回行数控制返回结果集大小, （提供第三方检测机构检测报告复印件并加盖投标人公章；）  支持跨语句、跨多包的绑定变量名及绑定变量值审计；  支持超长SQL语句（最长4M）审计。 |
| 智能发现 | 支持自动发现流量中的数据库信息，简化配置。 |
| 安全审计 | 为发现数据库中不安全访问行为及审计数据二次泄露等问题，数据库审计需支持以下功能：  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； |
| 审计查询 | 为满足审计追踪溯源、分析安全问题等需求，数据库审计应满足以下查询需求：  支持基于数据库[访问日期、时间、源/目的IP、来源](" \l "_多维度查询)、数据库名、数据库表名、字段值、数据库登录账号、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 | 为满足事后分析需求，数据库审计应满足以下需求：  系统内置[多种报表模板库](" \l "_内置多种报表模板)，报表不少于20种；  报表支持严格按照[塞班斯（SOX）法案、等级保护标准](" \l "_SOX、等级保护合规多维度)要求生成多维度综合报告；  支持按照[时间曲线统计流量](" \l "_时间曲线等报表)、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[HTML、PDF、P](" \l "_导出格式)NG、Word等格式的报表导出。 |
| 模型分析 | 为了更加智能发现数据库安全问题，产品需要具备以下功能：  ▲支持对数据库[自动建模及智能对异常行为告警功能](" \l "_自动建模告警)，（提供第三方检测机构检测报告复印件并加盖投标人公章；）  可通过行为[轨迹图方式](" \l "_轨迹图方式展示)展示数据库访问行为；  对学习的安全基线以外的行为自动智能进行告警。 |
| 数据管理 | 为满足数据备份保留的需求，产品需要具备以下功能：  支持将审计日志通过FTP的方式外送，支持自定义在线数据备份时间周期；  提供审计策略和[系统配置信息的单独导入、导出](" \l "_系统配置单独导入导出)功能。 |
| 系统管理 | 为增加系统管理的安全性、适应性、可维护性，产品需要具备以下的功能：  支持用户界面告警、SNMP、邮件、短信、钉钉五种方式告警；  支持[NTP时间同步，客户端浏览器时间同步、SNMP](" \l "_NTP、SNMP)（v1、V2、V3）网络管理协议。 |
| API化 | 功能全面API化，支持第三方调用（需要提供API功能列表）。 |
| 易用性 | 支持分组管理，分组管理包含IP组、应用用户组、对象组、时间组、数据库账号组；  支持一键取证；  支持配置过滤规则，过滤规则包含IP过滤、SQL模板过滤和自定义过滤，自定义过滤条件不少于28个条件。 |

**5.2.2.8 主机安全及管理系统**

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 许可数量 | 配置2个系统控制中心，200个服务器端许可 |
| 数据耦合性 | 软件可根据具体业务需求进行配置和功能定制化开发。 |
| 分布式架构 | 软件支持分布式部署，用于提升数据处理性能。 |
| 支持的操作系统 | Windows server 2008、win7、win8、win10 、Window2003 、XP等，Redhat、CentOS、SUSE、Ubuntu等。 |
| 支持的Web服务器 | IIS、Apache，Java系列(Weblogic，Websphere，Tomcat，Jboss)等 |
| 支持的数据库 | MSSQL，Oracle、Sybase、Informix、DB2、MySQL等关系型数据库；Mongodb、Cassandra等非关系型数据库。 |
| 系统性能监控 | 支持对CPU使用率监控、内存占用率监控、磁盘读写监控、上下行流量监控，在达到配置阈值时报警。 |
| 支持网络通信全时监控。 |
| 系统安全性模块 | 支持防端口扫描，防违规外联，锁定恶意的端口扫描及外联行为，并记录告警。 |
| ▲违规外联支持黑、白名单双模式，白名单模式可配置是否允许访问特定的网站和地址；黑名单模式可自定义恶意IP，支持黑名单告警和阻断。（提供截图并加盖投标人公章。） |
| 支持网站防护，包括SQL注入、XSS、Web应用及容器漏洞防护、访问控制、屏蔽扫描器等。 |
| 支持智能检测防御CC攻击，并可进行高、中、低三档设置。 |
| 内核级防火墙（业务间流量东西向隔离）功能，包括IP、端口、协议、流向等细粒度权限控制。 |
| 支持流量画像，支持全网流量可视化、应用级流量可视化；支持威胁横向扩散路径可视化与一键阻断；支持违规外联路径可视化与一键阻断。 |
| 支持登录防护，包括以系统账号为粒度的异常登录防护、支持五个任意维度(任意地理位置，任意IP，任意域名，任意计算机名，任意时间)的系统登录访问策略设置、防暴力破解、弱口令检测并告警。触发登录防护后，自动联动添加微隔离规则。 |
| 具有系统漏洞扫描和修复功能，提供真实漏洞补丁。管理中心可作为补丁服务器，支持管理中心可上网和不可上网2种情况。提供离线补丁下载器，按需智能获取内网所需补丁。 |
| 支持对外设的行为监控、权限管理、行为审计。 |
| 支持用户录制定制化的配置模板，应用到所有或者指定的机器上；自带10个以上默认模板。对关键操作，比如病毒查杀等关键安全项检查支持创建自动巡检任务，定时执行。 |
| 支持开启进程白名单，只允许受信任的进程启动。 |
| 防病毒模块 | 支持进程主动式防御，在进程启动、文件创建时自动触发。 |
| 支持域环境下普通账户登录的病毒木马查杀及策略的配置。 |
| 开启进程监控后能完全预防已知病毒的危害。 |
| ▲提供专门的勒索风险评估功能。至少需要包含：弱口令检测、系统漏洞检测、恶意进程检测、高危端口检测等能力。（提供截图并加盖投标人公章。） |
| ▲提供专门的针对已知勒索病毒的防御引擎，并提供功能开关项。对于已知勒索病毒确保进程无法启动。（提供截图并加盖投标人公章。） |
| ▲提供专门的针对未知勒索病毒的防御引擎，并提供功能开关项。对于未知勒索病毒确保无法加密。（提供截图并加盖投标人公章。） |
| 提供专门的挖矿风险评估工具。评估项目至少包括：弱口令、系统漏洞、恶意进程、DNS历史查询、违规外联等。 |
| ▲提供专门的挖矿实时防御工具，并提供功能开关。（提供截图并加盖投标人公章。） |
| 自研免疫引擎通过强制访问控制技术免WannaMine1.0/2.0/3.0等免杀病毒。 |
| 支持强力查杀，对于无法普通隔离的病毒文件强制停止进程并隔离或动态移除到删除队列。 |
| 支持部分病毒感染文件的修复功能，对于二进制文件可剥离感染部分，保证应用正常使用。 |
| 可防范、检测并清除隐藏于电子邮件、公共文件夹及数据库中的计算机病毒、恶性程序、病毒邮件。 |
| 支持查杀映像劫持类型的病毒。 |
| 支持查杀防范网页中的恶意代码。 |
| 支持对压缩文件、打包文件查、杀毒（默认支持9层压缩扫描，可根据用户需求增加扫描层数）。 |
| 支持内存查杀毒。 |
| 支持运行文件查杀毒。 |
| 支持支持图片、视频等多媒体文件的查杀毒。 |
| 支持查杀各类Office文档中的宏病毒，支持查杀各类Office文档格式夹带型木马。 |
| 告警功能 | 告警类型包括：异常文件、网站防护、性能监控、登录防护。 |
| 告警内容至少包括事件发生时间、事件类型、访问的资源、 IP源地址等详细内容。 |
| 告警方式包括：Email，短信，声音，syslog，snmptrap，自定义。 |
| 升级系统 | 支持离线升级及在线自动升级，包括管理中心平台、客户端程序、病毒库、补丁库、Web后门库、违规外联黑名单库。 |
| 客户端程序支持在线热升级，升级之后旧版本驱动等程序无残留。 |
| 集中管控 | 管理平台支持一键卸载客户端、一键设置客户端卸载密码、一键停止/恢复所有防护、一键解除绑定。 |
| 支持导出已安装客户端程序的资产清单。支持导出日志。 |
| 能够通过统一的管理中心对多个服务器或主机进行监控。 |
| 能实时检测工作组件工作状态以及系统关键资源的运行状态。 |
| 能对服务器或主机节点进行分组管理。 |
| 软件升级 | 提供3年的病毒库、程序升级服务。 |
| 产品资质 | 通过公安部信息安全产品检测中心检测并获得销售许可证书  软件要求具备自主知识产权。  注：提供上述相关证书复印件并加盖投标人公章。 |

**5.3其它要求**

5.3.1．**中标供应商须在中标后公示结束后签订合同前提供所投设备原厂三年质保承诺书，未提供或超出规定时间的采购单位有权将取消中标资格。鉴于上述设备均为柯桥区电子政务外网网络骨干线路关键性设备，中标后3个工作日内，根据用户要求提供样机进行上述功能的逐一测试验证(所发生的费用由中标人承担)，以确保产品实际质量及性能满足需求，全部通过后才能执行合同流程，测试中发现虚假应标的行为，采购人有权单方面取消中标供应商的中标资格，并保留对中标方追究相关责任的权利。**

5.3.2．**原有设备利旧**

**中标方须完成原有网络替换下来设备的利旧使用。原有核心交换机华为CE12808、防火墙等设备迁移至鉴湖大院机房使用或用于柯桥区电子政务内网继续使用，中标方需完成相应的设备迁移、系统集成等工作，相关费用包括在总报价内。**

5.3.3． 投标供应商如进行现场勘察，应当充分了解本项目的实施要求，采购人不承担现场勘察时需要发生的相关费用。

5.3.4.设备出现故障时，中标供应商应在接到电话故障报告后30分钟内做出实质性响应，确保原厂认证工程师在2小时内到达故障现场，对故障件免费提供备件支持，并负责故障件更换、维护和故障恢复工作。中标供应商在规定时间（24小时内）解决设备故障，规定时间内故障不能解决而影响设备正常使用时，中标供应商负责提供相当性能的备机，保障系统正常运行。

5.3.5.用户在服务期内为设备添购或更换任何配件时，中标供应商应安排原厂认证工程师进行安装实施。本次招标包含质保过程中产生的所有费用。自合同生效内，质保过程中产生的所有费用皆由中标供应商负责。

5.3.6.本项目报价应包括维护费和材料费。

5.3.7．如果发现有假货/水货/串货等行为，将取消中标资格。

# 六、合同主要条款及合同签订方式

**6.1签订合同：**

中标供应商以浙江省政府采购网中标公示为依据，按《中标通知书》规定的时间、地点与采购人签订合同并交纳履约保证金(不计息)。

**6.2合同组成：**

6.2.1本项目的合同文件包括下列附件：采购文件（包括采购补充文件），投标文件（包括投标补充文件），答疑纪要，询标纪要，中标通知书，合同履行中双方就有关问题协商达成的纪要或补充协议，项目技术文件（包括安装图纸、会议纪要、变更联系单等其他技术资料）等。所有附件与合同正本具有同等法律效力。

**6.3 合同主要条款**

**6.3.1 承包范围：**按采购文件内容。

**6.3.2 承包方式：**

本项目承包方式在约定范围内实行包项目总造价、包货物量、包安装、包供货安装时间、包维修、包质量、包安全、包文明施工管理的承包方式。

**6.3.3 工期要求**

6.3.3.1货物供应及安装完成时间详见前附表第9项。

6.3.3.2 合同供货安装时间如遇下列情况，经甲方书面确认后，供货安装时间可相应顺延。

6.3.3.2.1 合同履行中发生重大变更而确实影响到供货安装进度（属中标人组织生产、安装等失误引起的供货安装进度滞后由中标人负责）。

6.3.3.2.2 不可抗力因素。

6.3.3.2.3 非中标人原因而确实影响到供货安装进度的。

除上述外，中标人不得以任何理由变更供货安装时间。

**6.3.4 技术要求**

6.3.4.1 所有投标的货物、设施必须满足相应标准或使用要求。

6.3.4.2 本项目应遵照国家的有关技术（验收）规程、规范、标准。

**6.3.5 质量要求**

6.3.5.1合格，且必须符合本标文第五部分所有条款要求。

6.3.6 中标供应商必须严格按照项目技术要求进行安装，并接受采购人的监督管理。

6.3.7 所有的货物进场时须同时提供货物出厂合格证书、检测报告。国外生产的必须有合法的进货渠道证明，如海关报关单、原产地证明、商检证明等。

6.3.8 所有货物必须在检验合格经采购人同意后，方可用于本项目。

6.3.9采购人有权监督、检查、检验中标人的货物质量及安装质量进度，整改方案须经采购人认可后方能实施，中标供应商应把货物质量放在首位，加强技术管理和质量保证体系，严格认真地执行技术标准和规范。

6.3.10 中标人在供货安装中如发生质量事故（责任由中标人全部承担），应及时报告采购人。做到及时查清事故原因，分清事故责任，并采取有效的补救措施。一般质量事故的处理方案应送采购人共同研究实施；重大质量事故的处理按国家相关条例执行。

**6.3.11 培训保修**

6.3.11.1 在项目组织验收之前，应完成对采购人不少于2名操作人员的培训（提供完整的技术培训，使采购人今后能自行操作、维护）。

6.3.11.2 中标供应商应分别提供称职的指导人员，为采购人确定的培训人员在现场提供操作和维护培训。

6.3.11.3 中标供应商应对采购人提供全面的技术和维护咨询。

6.3.11.4 本项目的质保期为验收合格之日起3年，货物在3年内损坏的（非人为造成）由中标供应商全权负责，如造成采购人相应的经济损失由中标供应商承担。

**6.3.12 货物的供应**

6.3.12.1 按采购文件内容和要求；

6.3.12.2 中标供应商必须经采购人确认后方可进行货物供应，擅自供应的货物采购人不予以认可**。**

**6.3.13 货物、安装款的支付**

6.3.13.1付款条件：合同签订后7个工作日内支付合同总价的30%，货物全部到位且安装调试完毕，验收合格后7个工作日内支付合同总价的97.5%；

6.3.13.2尾款2.5%待项目验收合格满一年后7天内付清；

6.3.13.3中标供应商未能在约定的供货安装时间内完成的，未达到合同规定的质量要求的，采购人有权暂缓支付货物、安装款；

6.3.13.4 发票应随付款进度同时提供（按照国家有关规定缴纳相应税费）。

**6.3.14 采购人职责**

6.3.14.1 采购人负责对货物质量、货物安装质量进度和合同执行进行监督检查。

6.3.14.2 组织验收和结算。

**6.3.15 中标供应商职责**

6.3.15.1 供货前，中标供应商应熟悉安装现场环境及做好其他各项准备工作，费用由中标供应商自理。

6.3.15.2 在合同实施中，中标供应商应兑现投标书中的所有承诺。

6.3.15.3 中标供应商必须严格按照本项目技术要求进行精心安装、强化现场原始记录和检测，确保货物质量。

6.3.15.4 中标人在货物供应、安装期间如发生安全事故，由中标供应商处理并承担全部责任。

6.3.15.5 在货物安装过程中，中标供应商应接受采购人指令，并严格服从采购人监督。

6.3.15.6 中标供应商必须在约定时间内组织供货、安装，确保如期完成。

6.3.15.7 当具备验收条件时，中标供应商应提前十天将验收报告送至采购人，并由采购人组织验收。

6.3.15.8 中标供应商的计划进度安排、质量监督、协调管理、安装配合、安全文明施工，应完全接受采购人对本项目的统一管理，完成后将归档技术资料交予采购人。

**6.3.16 验收**

6.3.16.1 验收以采购文件和技术文件、投标文件、合同及安装技术要求为依据。

6.3.16.2 供货安装完成后，中标供应商应该向采购人提交申请验收报告。

6.3.16.3 验收必须符合国家、地方有关规范、标准及设计要求。

6.3.16.4 符合验收条件的，由采购人组织有关部门按照国家、地方有关规范、标准及设计要求进行验收。验收后中标供应商应按照验收中提出的意见整改。

6.3.16.5 整改完毕且复验合格后将本项目货物交给采购人使用，完成日期以通过复验日期为准。

6.3.16.6采购人在中标供应商送货、安装、调试后对货物服务进行检查验收，如果发现数量不足或有质量、技术等问题，中标供应商应负责根据合同及采购人的要求采取补足或更换等处理措施，并承担由此发生的一切损失和费用。验收合格后，采购人在验收单上签字并加盖单位公章。

**6.3.17 违约责任及奖罚**

6.3.17.1 安装完成经验收，不能达到采购文件规定的“质量要求”，无偿返工，并承担由此发生的一切损失和费用。

6.3.17.2 不能在规定时间内完成货物供应及安装的，每逾期一天，按本采购文件7.1处理（非中标供应商原因除外）。

6.3.17.3 因中标供应商违约造成终止合同的，则扣除全部履约保证金，同时作违约论处。

6.3.17.4 因采购人违约造成终止合同，采购人应退还中标供应商缴纳的履约保证金，同时支付给中标供应商履约保证金同等金额的违约金，但属执行国家行政指令造成的合同终止，不支付违约金。

**6.3.18争议解决**

6.3.18.1因执行本合同所发生的，或与本合同有关的一切争议，采购人与中标供应商双方应通过友好协商解决。

6.3.18.2如经协商仍不能解决争议时，可要求有关主管部门调解。如其中一方不愿调解或调解不成，可按下一种方式解决争议。

6.3.18.2.1双方达成仲裁协议，向采购人所在地的仲裁机构申请仲裁。

6.3.18.2.2向有管辖权的人民法院起诉。

**6.4其他要求：**

中标供应商必须按规定程序和有关要求进行实施，供货过程中的各种意外，其责任由中标供应商承担，采购人不承担任何责任。

**6.5变更：**

6.5.1采购合同履行中，采购人需追加与合同标的相同的货物、工程或者服务的，在不改变合同其他条款的前提下，可以与供应商协商签订补充合同，但所有补充合同的采购金额不得超过原合同采购金额的百分之十。

6.5.2 当变更只是采购量增减时，按投标所报的单价进行结算。

**6.6专利权**

6.6.1 供应商应承诺保护采购人在使用合同产品或其任何一部分时不受第三方提出侵犯专利权、商标权和工业设计权等的起诉。如果任何第三方提出侵权指控，由供应商负责与第三方交涉并承担可能发生的一切费用和相关法律责任，采购人不承担由此引起的一切经济和法律责任。

**6.7结算原则**

6.7.1采购文件、招标答疑会纪要、中标供应商的中标报价等作为结算依据；

6.7.2中标单价一次性包死，不再调整，经采购人分级审批认可的数量增减，在结算时按中标单价按实调整。

**6.8签订合同时间：**中标通知书签发后30天内。

**6.9售后服务要求：**

6.9.1中标供应商须提供从验收合格之日起，原厂3年的免费质保服务。供应商承诺超过本要求的，以优惠者为准。无论在质保期内还是质保期满后，中标供应商负责对其实施的项目提供现场服务。要求中标供应商在接到采购人的电话后0.5小时内响应，2小时内到达现场，并最迟在24小时内排除故障，24小时内无法修复的，必须采取临时调换等措施，以保证采购人的正常使用。临时调换的设备要求不低于原有的设备要求。

6.9.2供应商若有其他服务承诺，也将一并执行。

6.9.3中标供应商必须将公司的服务热线明确告知采购人。

6.10采购人应当自采购合同签订之日起七个工作日内，按照有关规定将采购合同副本报绍兴市柯桥区公共资源交易管理委员会办公室备案。

**6.11 其他**

合同双方确认，本合同及本合同约定的其它文件组成部分中的各项约定都是通过法定招标过程形成的合法成果，不存在与采购文件和中标人投标文件实质性内容不一致的条款。如果存在任何此类不一致的条款，也不是合同双方真实意思的表示，对合同双方不构成任何合同或法律约束力。合同双方也不存在且也不会签订任何背离本合同实质性内容的其他协议或合同。如果存在或签订背离本合同实质性内容的其他协议或合同，也不是合同双方真实意思的表示，对合同双方不构成任何合同或法律约束力。

# 七、交货和提供服务的时间

7.1交货（含安装调试）和提供服务的时间：**本采购项目的交货（含安装调试）和提供服务的时间详见前附表第9项，延期赔偿金按1000元/天计。**并要求在投标书中予以承诺，否则可作为无效标论处。采购人由于某种原因需延长工期时，违约金可不计，中标供应商也不作任何赔偿。

7.2 供应商应明确说明具体的交货和提供服务的时间。供应商所提供的必须是合法生产的货物和服务，并能确保在中标合同有效期内按照合同中规定的要求及时交付。

# 八、评标方法、评标标准和废标条款

8.1开标：

8.1.1**在投标截止时间前按规定提交投标文件的供应商在三家及以上的**，由采购人组织进行开标。

8.1.2 **电子招投标开标及评审程序**

（1）投标截止时间后，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1个小时内。

（2）评标委员会依照本招标文件规定进行审查、评议；

（3）在系统上公开资格和资信技术评审结果；

（4）在系统上公开报价开标情况；

（5）评标委员会对报价情况进行评审；

（6）在系统上公布评审结果。

**特别说明：政采云公司如对电子化开标及评审程序有调整的，按调整后的程序操作。**8.1.3采购人在招标文件要求提交投标文件的截止时间前收到的投标文件，开标时都应当众予以拆封、宣读。

8.1.4采购人对开标过程进行记录，并存档备查。

8.1.5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：

8.1.6若采购人在规定时间内无法解密或解密失败，视为投标人放弃投标。

8.1.7采购过程中出现以下情形，导致电子交易平台无法正常运行，或者无法保证电子交易的公平、公正和安全时，采购组织机构可中止电子交易活动：

8.1.7.1电子交易平台发生故障而无法登录访问的；

8.1.7.2电子交易平台应用或数据库出现错误，不能进行正常操作的；

8.1.7.3电子交易平台发现严重安全漏洞，有潜在泄密危险的；

8.1.7.4病毒发作导致不能进行正常操作的；

8.1.7.5其他无法保证电子交易的公平、公正和安全的情况。

出现前款规定情形，不影响采购公平、公正性的，采购组织机构可以待上述情形消除后继续组织电子交易活动。

8.1.8 开标时，由采购人或者采购代理机构对供应商资格进行审查，并通过“信用中国”网站(www.creditchina.gov.cn)、中国政府采购网(www.ccgp.gov.cn)查询相关投标人信用记录，对供应商信用记录进行甄别。

**8.1.9 开标顺序为：先查验资信证明文件，其次开商务技术标，最后开价格标。资格（资信）证明文件或商务技术标经过评标委员会评审未获通过的，将不再开启价格标。**

8.2 评标：

8.2.1采购人将组织评标委员会进行评标，依照本采购文件规定进行审查、评议；

8.2.2 将从以下几方面对有效的投标文件进行综合评判：

8.2.2.1 供应商详细的服务技术方案和实施计划；

8.2.2.2 投标价格是否具有优势；

8.2.2.3 对招标文件中的付款方式是否响应，如不响应将被拒绝；

8.2.2.4 供应商的综合实力、业绩及信誉等；

8.2.2.5 售后服务承诺是否完整、真实、可行；

8.2.2.6 投标文件是否完整、真实、整洁。

8.2.3 与采购文件有重大偏离的投标文件将被拒绝。

8.3 定标方式：采用综合评分法

8.3.1 投标供应商根据采购人所需的柯桥区电子政务外网网络及安全设备升级项目的主要性能、技术指标等要求进行标书制作和报价。

8.3.2 经评标委员会综合评定后，以总得分最高者为第一中标候选人，若最高总得分出现并列时，以报价低者为第一中标候选人；若最高总得分与报价均相同时，由采购人当场随机抽签选定第一中标候选人。

8.3.3具体评分方式详见“评标办法”。

8.4 定标：按本采购文件“8.3定标方式”规定确定中标者。

8.5 出现下列情形之一的，采购人将予以废标。

8.5.1在投标截止时间前，按规定提交投标文件的供应商不足三家的；

8.5.2供应商的报价均超过了采购人上限价或采购预算，采购人不能支付的；

8.5.3出现影响采购公正的违法、违规行为的。

8.6 采购人不向供应商解释未中标的原因，不退还投标文件。

8.7投标文件有下列情况之一，经认定属未实质性响应采购文件的，将视为无效：

8.7.1投标文件正本或正本的开标一览表（报价表）未加盖供应商公章的；

8.7.2 未按采购文件规定填写，内容不全或关键字迹模糊、无法辨认的；

8.7.3 供应商递交两份或多份内容不同的投标文件，或在一份投标文件中对同一采购项目报有两个或多个报价，且未声明哪一个有效；

8.7.4 供应商名称或组织机构与资格预审时不一致的；

8.7.5 投标文件未按采购文件要求封装、提交的。

8.7.6不具备采购文件中规定资格要求或未按采购文件要求提供资格、资信证明文件的。

8.7.7不符合法律、法规和采购文件中规定的其他实质性要求的。

8.8 采购代理机构应当在评标结束后两个工作日内将评标报告送采购人。

8.9 采购人应当在收到评标报告后五个工作日内，在评标报告推荐的中标候选人中确定中标供应商。

# 九、投标截止时间、开标时间及地点

9.1投标文件递交截止时间：详见前附表第14项。

9.2开标时间：详见前附表第15项。

9.3开标地点：详见前附表第15项。

# 十、其他事项

10.1采购活动全过程由柯桥区公证处实施公证。

10.2本标文未尽事宜，另行以在浙江省政府采购网上发布形式补充说明，并按照《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》的基本原则和精神执行。

10.3本次招标采购监督管理部门：绍兴市柯桥区公共资源交易管理委员会办公室，监督电话：0575-84130780

10.4凡参加开标会的供应商，均视同对本标文及评标办法的认可，无异议。

采购人：绍兴市柯桥区大数据发展管理中心

采购代理机构：绍兴市柯桥区公共资源交易中心

绍兴市鼎正建设工程咨询有限公司

2020年7月21日

# 附件一：投标函

（采购人）：

我单位认真研究了编号为 的关于 的采购文件，愿意遵守采购文件的所有要求，承担采购文件规定的中标供应商的全部责任和义务。我单位承诺：

1、我单位愿意以开标一览表（报价表）所填报的报价承接本采购项目的供应、安装就位、调试、检测、验收及技术服务等的任务。

2、一旦我单位中标，我们保证按照采购文件的要求完成货物供应安装、售后服务、验收并交付使用。

3、我单位同意提供按照采购人可能要求的与其投标有关的一切数据或资料，完全理解和接受不一定按最低价中标。

4、如果我单位中标，我方将按照要求提交履约保证金，并严格履行合同义务。

5、除非另行达成协议并生效，你方的中标通知书和本投标函将构成约束你我双方的合同。

6、本供货质量承诺为 。

7、我单位一旦发生下述行为，我单位（或公司）同意采购人取消我单位投（中）标资格。

（一）从开标日起到投标有效期满撤回投标；

（二）开标、评标到定标期间发生违反采购文件规定的行为；

（三）在收到中标通知书后未按规定与采购人签订合同。

8、我单位声明：参加政府采购活动前3年内在经营活动中没有重大违法记录。

9、我方在此声明，我单位未被列入失信被执行人、重大税收违法案件当事人名单和政府采购严重违法失信行为记录名单。

供应商：（盖章）

法定代表人或其委托代理人：（签字或盖章）

地址：

日期： 年 月 日

# 附件二：法定代表人授权书

（采购人）

本授权委托书声明：我 （姓名）系 （供应商名称）的法定代表人，现授权委托 （姓名）为我公司唯一代理人，以本公司的名义参加贵中心组织的 采购的招标活动。代理人在投标、开标、评标、合同谈判过程中所签署的一切文件和处理与之有关的一切事务，我均予以承认。

代理人无转委权。特此委托。

供应商：（盖章）

授权人：（签字或盖章）

被授权的代理人：（签字或盖章）

日期： 年 月 日

# 附件三：开标一览表（报价表）

项目名称：

采购编号：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **项目内容** | | **数量** | **综合**  **单价** | **合价** | **备注** |
| 1 |  | |  |  |  | 须附投标报价明细表 |
| 2 |  | |  |  |  | 须附投标报价明细表 |
| 3 |  | |  |  |  | 须附投标报价明细表 |
| 总报价（小写） | | 人民币 元 | | | | |
| 总报价（大写） | | 人民币 元 | | | | |

**说明：1、综合单价为包含所有相关费用的单价。**

**2、必须附投标报价明细表，否则作无效标处理。**

供应商（盖章）： 法定代表人或其委托代理人（签字或盖章）：

2020年 月 日

# 附件四：投标报价明细表

项目名称：

采购编号：

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 货物名称 | 型号、规格 | | 技术参数 | 生产厂家 | 品牌及其产地 | 数量 | 单位 | 金额（元） | |
| 综合单价 | 合价 |
|  |  |  | |  |  |  |  |  |  |  |
|  |  |  | |  |  |  |  |  |  |  |
|  |  |  | |  |  |  |  |  |  |  |
|  |  |  | |  |  |  |  |  |  |  |
|  |  |  | |  |  |  |  |  |  |  |
|  |  |  | |  |  |  |  |  |  |  |
|  |  |  | |  |  |  |  |  |  |  |
|  |  |  | |  |  |  |  |  |  |  |
| 合 计 | | | （小写） | | | | | | | |
| （大写） | | | | | | | |

**注：1、本表格可自行扩展。**

**2、综合单价为包含所有相关费用的单价。**

**3、本表所填内容必须与附件六“投标设备材料详细清单”对应内容相一致。**

供应商（盖章）： 法定代表人或其委托代理人（签字或盖章）：

2020年 月 日

# 附件五：投标技术方案和人力资源安排

（由供应商自行填写）

主要包括：对本项目技术要点阐述、安装技术方案、技术措施和人力资源安排等。

供应商（盖章）： 法定代表人或其委托代理人（签字或盖章）：

2020年 月 日

# 附件六：投标设备材料详细清单

项目名称：

采购编号：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 货物名称 | 型号、规格 | 技术参数 | 生产厂家 | 品牌及其产地 | 数量 | 单位 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

供应商（盖章）： 法定代表人或其委托代理人（签字或盖章）：

年 月 日

**注：1、本表格可自行扩展。**

**2、本表所填内容必须与附件四“投标报价明细表”对应内容相一致。**

# 附件七：投标设备主要技术参数说明

投标设备名称(型号规格)：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 部件名称 | 技术参数、性能、特点 | 生产厂商、产地 |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
| 6 |  |  |  |
| 7 |  |  |  |
| 8 |  |  |  |
| 9 |  |  |  |
|  |  |  |  |
|  |  |  |  |
| … |  |  |  |

**注：如果不同型号规格的部件有不同，应该依据此表分别填写，并注明投标设备(型号规格)。**

供应商（盖章）： 法定代表人或其委托代理人（签字或盖章）：

2020年 月 日

# 附件八：技术偏离表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 编号 | 项目名称 | 招标技术  参数要求 | 投标技术  参数响应 | 备注 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

供应商（盖章）： 法定代表人或其委托代理人（签字或盖章）：

年 月 日

# 附件九：投标承诺书

（采购人）：

我公司自愿参加 项目标段 / 的采购招标活动，完全遵守招标文件的所有要求，并作如下承诺：

我公司提供免费维修保养期后的维修保养办法及费用：

供供应商（盖章）： 法定代表人或其委托代理人（签字或盖章）：

2020年 月 日

# 附件十：投标提问书

：

我们认真阅读了 采购项目的招标文件等技术资料，并对投标的项目现场进行了踏勘，本公司愿意遵守和接受招标文件中所有的内容和条款，恪守信誉、严肃竞标规则，在不改变要求的条件下，对下列容易产生理解上歧义的条款和未明确事项，提请采购人予以澄清解答。

需在投标中澄清、解答的问题：（可添页）

1、

2、

3、

4、

联系电话： 投标供应商：（盖章）

传 真： 经 办 人：（签字或盖章）

年 月 日

# 附件十一：答疑纪要

各投标供应商在研究了 采购项目的招标文件等有关资料后，各投标供应商于 年 月 日16时前提交了投标提问书，现采购人对各投标供应商的提问和招标文件作如下说明：

一、对各投标供应商提问的回复：

1、

**答：**

2、

**答：**

二、对招标文件补充说明如下：

1、

2、

采购人： （盖单位章）

采购代理： （盖单位章）

2020年 月 日

# 附件十二：评标办法

根据《中华人民共和国政府采购法》等有关法律法规，结合本项目的实际，按照公正、公平、科学的原则择优选择中标供应商，特制定本评标办法。

一、总则

评标工作必须遵循公平、公正的竞争原则。最大限度地保护当事人的权益，评标委员会应严格按照采购文件的商务技术标、价格标要求，对投标文件进行综合分析评价。评标人员必须严格遵守保密规定，不得泄露评标有关的情况，不得索贿，不得参加影响评标的任何活动。

二、评标组织

评标委员会：评标委员会按相关规定共由5人及以上单数组成。

三、评标程序

1、开标后，首先验证供应商资格，评标委员会对投标书进行符合性审查。再对供应商资质、资信及方案进行评审；凡投标书设备、技术的实质性内容严重不符合采购文件规定或不响应采购文件要求者，经评标委员会及采购人认定，作为无效投标予以废除。

2、采用综合评分法，评标委员会委员将根据供应商的商务技术标等内容对投标文件进行分析、评议、打分，如有疑问，将对供应商进行询标，供应商要向评标委员会澄清有关问题，并最终以书面形式进行答复。商务技术标评审结束后，依次开价格标，评标委员会委员审核价格标，并计算分值。

3、具体评审步骤和方法：

①第一步，由评标委员会对通过资格审查的供应商的商务技术标进行评审打分。评审打分完成后向供应商公布商务技术标分值。

②第二步，开启价格标，对各供应商的价格标由评标委员会统一评审进行计算评分。

③第三步，计算出各供应商的总得分。

4、编写评标报告。

5、根据中标结果在柯桥区公共资源交易中心指定的媒体上公示。

四、评分项目说明

1、商务技术分+价格分总分为100分，评标委员会成员评分在得分栏中填上分值。

2、商务技术标70%，即满分70分。评标委员会成员按各供应商的商务技术标内容充分审核、讨论、评议后，按评分细则进行独立评判、打分。各供应商商务技术标的最终评分值为评标委员会各成员评分值的算术平均值。

3、价格标30%，即满分30分。评标委员会成员按评分细则对各供应商的报价进行统一计算评分。

4、专家打分分值保留小数点后1位。统计或计算分值时的精度最终精确到小数点后2位。

五、评分细则

1、商务技术分评分70%,即满分70分。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **评分内容** | **评分标准** | | **分值** |
| 1 | 投标人资质 | 1.具有涉密信息系统集成乙级及以上资质的得3分；  2.具有信息技术服务运行维护标准ITSS证书的得3分；  3.具有国家信息安全服务资质证书（安全工程类一级）得2分；  **注：投标文件中提供上述证书复印件并加盖投标人公章。** | | 8分 |
| 2 | 成功案例 | 2017年1月1日以来具有类似信息化项目的案例每个得2分，最高得6分；（该项目须非分包与转包项目）  **注：投标文件中装订案例合同复印件并加盖投标人公章,否则不得分。** | | 6分 |
| 3 | 产品质量 | 1、为保证出口万兆防火墙的稳定性，所投防火墙生产厂商具有信息安全测评中心颁发的信息安全产品自主原创证明文件和芯片级硬件性能加速技术证明文件的，得2分，没有不得分。  2、核心产品态势感知平台厂商对等级保护标准有较深入研究，能够根据等保要求对网络进行安全加固并且是公安部认可的信息安全等级保护检查工具箱研发单位并有相关证明材料，得2分，没有不得分。  3、核心产品态势感知平台厂商具有企业知识产权管理体系认证，能提供证明材料得2分，没有不得分。  **注：提供上述相关证明材料复印件并加盖投标人公章,否则不得分。** | | 6分 |
| 4 | 产品指标参数 | 根据投标的设备基本性能配置是否符合招标文件的要求及符合程度进行评比打分，基本性能满足或高于招标文件要求得满分。性能指标中带“★”项为必须满足项，不满足做无效标处理。性能指标中带“▲”项，每负偏离一项扣3分；其他性能指标项每负偏离一项扣1分；扣完为止。 | | 21分 |
| 5 | 整体方案设计和演示 | 投标方案总体设计，包括方案的科学性、先进性、可行性和扩展性；设计方案是否科学合理、安全严密、具有一定的前瞻性，是否有独到的优势；提供现有网络拓扑和最终的网络拓扑图。好得2分，一般得1分。 | | 2分 |
| **核心产品态势感知平台**  本次演示相关的设备或网络环境由投标单位提供并自建，云安全管理平台的部分功能演示共计8个功能项，投标人按照表格要求进行逐条演示，每条功能满足得1.5分，不满足得0分，共计12分。**演示内容通过录制视频以U盘存储形式提交（提交方式采用顺丰邮寄或现场即交即走），中标单位需在签订合同前向采购人提供设备针对8个功能项逐一现场演示，不能满足的认定为虚假应标，取消中标资格。**  注：投标人应于2020年8月13日上午9时30分之前将演示录制视频存储U盘密封以顺丰邮寄或现场即交即走的方式送达至绍兴市柯桥区华齐路1066号绍兴市柯桥区公共资源交易中心三楼招投标中介机构服务区**，收件人：张峰，联系电话：0575-85176866，邮政编码：312030**，如采用邮寄的，请寄件人在邮件外包装注明投标项目名称，投标供应商名称，被授权人姓名及联系电话，接收邮寄快递包裹的时间为工作日9:00-17:00，邮寄以签收时间为准，逾期送达或未密封将予以拒收（或作无效标处理）。 | | 12分 |
| 安全分析和自动化编排 | 1、安全分析模型支持自定义创建，可通过字段映射、静态值、模板、表达式等多种方式自由定义分析模型的告警名称、威胁等级、告警类型、攻击链、可选字段、告警描述、处置建议等内容； |
| 2、支持对安全日志里200个以上字段进行任意形式的逻辑与或非形式组合建模，并能根据组合方式自动生成运算表达式 |
| 3、支持与不同品牌的网关类安全产品进行联动防护，防护策略支持设置每次阻断不同时长生效时间，时间设置包括10分钟，30分钟，6小时，24小时，72小时，永久阻断； |
| 安全运营门户 | 4、统一门户应支持与第三方产品集成，一键跳转至产品功能界面 |
| 流量探针规则库管理 | 5、支持基于规则ID、规则名称、CVE编号、规则等级、规则类型、规则状态、应用协议等不同条件进行规则快速检索； |
| 场景化分析 | 6、支持暴力破解、Web攻击、恶意程序、端口扫描等内置安全分析场景，基于场景特性进行默认条件的数据聚合分析，支持至少3个任意字段的快速聚合分析，聚合后的所有数据均支持快速统计分析，展示统计排序信息，支持分析结果导出。 |
| 7、支持智能检索语句分析，支持检索语句的中英文、拼音智能联想，支持逻辑运算符与字段值的自动提示补全；检索语句支持快速保存，历史检索语句快速导入；检索语句可直接发布成实时分析模型，对实时数据进行分析与告警 |
| 运维监控 | 8、支持态势感知平台一键巡检，一键检查项包含但不限于数据健康、探针健康检查、大数据集群健康、Elasticsearch健康、实时流计算引擎健康、管理服务健康、服务器节点健康等多种维度检查，并能提供处置建议，一键导出各类服务的故障日志，包括但不限于Elasticsearch、Logstash、Ka\*\*a、实时计算引擎、操作系统等 |
| 6 | 施工组织方案 | 根据施工技术方案、施工质量目标及保证措施、施工组织、人力资源安排、施工进度计划、工期及安全保证措施，施工重点、难点及采取的应对措施方案。方案科学、合理、可行、周全等内容详细真实、完全符合现场实际情况。优秀得2分，一般得1分，差的得0.5分。 | | 2分 |
| 7 | 项目组人员配置情况 | 根据投标供应商拟派本项目组专业人员的技术能力情况评分：  1.投标供应商拟派承担本工程的项目经理：同时具有系统集成高级项目经理证书和高级工程师证的得4分；  2.投标供应商拟派本项目技术支撑团队：  ①具有高级信息系统项目管理师每个得1分，最高得2分；  ②具有国家信息安全测评注册信息安全专业人员证书(CISP)的每一名得1分，最高得4分。  注：以上人员须为投标供应商在职员工，投标文件中须提供相关证书复印件并加盖投标人公章以及提供近3个月（2020年4月至2020年6月）投标人所在地社保机构缴纳的社保证明复印件加盖投标人公章，否则不得分）。 | | 10分 |
| 8 | 售后服务承诺 | 评标专家参考投标单位注册地及售后服务机构地点与柯桥城区的距离远近,进行综合评判打分。  注：需提供营业执照复印件加盖投标人公章，未提供不得分。 | | 3分 |

2、价格分评分标准

价格标30%，即满分30分。

价格标评审应在投标报价范围口径一致的基础上进行（开标一览表（报价表）中不得漏填项目，否则当供应商中标后，采购人对供应商没有填入单价与金额的项目将不予支付，并认为此项目费用已包括在价格表的其他项目的单价和金额之中，如中标，缺报的设备或项目免费提供）。

价格评分采用低价优先法计算，即在有效报价中，满足采购文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分30分。其他供应商的价格分统一按照下列公式计算：投标报价得分=（评标基准价/投标报价）×30%×100。小数点保留2位。

有效报价是指小于或等于采购人上限价的报价。上限价为592万元，超过上限价的报价作无效标处理，直接予以淘汰。当有效报价不足3家时，开标终止，重新组织采购。

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