紫琅科技城网络数据安全服务采购项目

公开招标文件

采购人：南通市中央创新区建设投资有限公司

招标代理：江苏中房工程咨询有限公司

二〇二三年十一月

**目 录**

第一部分 招标公告

第二部分 投标须知

第三部分 项目需求说明

第四部分 开标和评标

第五部分 合同和履约保证

第六部分 质疑提出和处理

第七部分 投标文件组成

**第一部分 招标公告**

紫琅科技城网络数据安全服务采购项目招标公告(资格后审)

江苏中房工程咨询有限公司（以下称代理机构）受南通市中央创新区建设投资有限公司（以下简称“采购人”）委托，就紫琅科技城网络数据安全服务采购项目进行公开招标采购。现公告如下：

一、项目名称：紫琅科技城网络数据安全服务采购项目。

二、采购预算：人民币40万元。

三、交货期：自合同签定之日起30个工作日内完成供货、安装及调试。

四、项目需求：具体详见第三章项目需求说明

五、投标人应具备的资格条件：

(一)符合下列规定的条件，并提供下列材料：

1、具有独立承担民事责任的能力；

2、投标人必须是在中国境内注册并具备独立法人资格；

3、具有良好的商业信誉和健全的财务会计制度；

4、具有履行合同所必需的设备和专业技术能力；

5、有依法缴纳税收和社会保障资金的良好记录；

6、在经营活动中没有重大违法记录；

(二)采购单位其他要求

7、法定代表人为同一个人的两个及两个以上法人，母公司、全资子公司及其控股公司，都不得在同一采购项目相同包中同时投标，一经发现，将视同围标处理；

8、本项目不接受任何形式的联合体投标，中标后不得分包或转包。

**请投标人认真对照资格要求，如不符合要求，无意或故意参与投标的，所产生的一切后果由投标人承担。对提供虚假材料的投标人作无效标处理，投标保证金不予退还，并报财政部门后将其列入政府采购黑名单，视情在南通市公共资源交易网公示。**

六、招标文件的获取

1、获取时间：自本招标公告发布之日起。

2、获取方式：本项目资格审查采用资格后审方式，无报名环节，投标人直接从南通市中央创新区建设投资有限公司网站（http://www.ntscid.cn/）自行下载招标文件、澄清答疑等招标资料。

七、投标文件的递交

1、递交投标文件截止时间及开标时间为**2023年12月7日9时30分**，地点为**南通市崇州大道60号紫琅科技城6号楼811室。**

2、逾期送达或者未送达指定地点的投标文件，采购人不予受理。

八、投标保证金

1、投标保证金金额(人民币)： **捌仟元整。**

2、投标保证金递交方式：**现金（密封）**。

九、评标办法

本项目采用综合评分法，具体详见招标文件。

十、发布公告的媒介

本次招标公告在南通市中央创新区建设投资有限公司网站（http://www.ntscid.cn/）发布。

十一、联系方式

采购人：南通市中央创新区建设投资有限公司

联系人：张先生

联系电话：17312352846

招标代理机构：江苏中房工程咨询有限公司

地 址：南通市崇川区江海大道817号江海财富大厦A座7楼

联 系 人：吴江

电 话：0513-68002662

电 子 邮 箱：[458101863@qq.com](mailto:874786206@qq.com)

**第二部分 投标须知**

**一、招标文件由采购人解释**。

1、投标人下载获取招标文件后，应仔细检查招标文件的所有内容，如有内容或页码残缺、资格要求和技术参数含有倾向性或排他性等表述的，**应在招标文件发布开始之日起**3日内以书面形式提出询问或疑问。未在规定的3日内提出询问或疑问的，视同投标人理解并接受本招标文件所有内容，并由此引起的投标损失自负。投标人不得在招标结束后针对招标文件所有内容提出质疑事项。**非书面形式的不作为日后质疑提出的依据。**

2、投标人应认真审阅招标文件中所有的事项、格式、条款和规范要求等，如果投标人没有按照招标文件要求提交投标文件，或者投标文件没有对招标文件做出实质性响应，其投标将被拒绝，投标人自行承担责任。

**二、招标文件的澄清、修改、答疑**

1、采购人有权对发出的招标文件进行必要的澄清或修改。

2、采购人可视情取消、延长相关时间，不负责解释。

3、采购人对招标文件的澄清、修改将构成招标文件的一部分，对投标人具有约束力。

4、投标人由于对招标文件的任何推论和误解以及采购人对有关问题的口头解释所造成的后果，均由投标人自负。

5、采购人或采购单位视情组织答疑会。

**三、投标报价**

一个包只允许一个报价，不接受任何有选择性的报价。

**四、投标文件的编写、份数和签署**

1、投标人按第七部分“投标文件组成”编写投标文件，投标文件规格幅面A4纸（图纸等除外），正文可使用宋体四号字，按照招标文件所规定的内容顺序，统一编目、编页码装订（投标文件中复印件及彩色宣传资料等均须与投标文件正文一起逐页编排页码）。由于编排混乱导致投标文件被误读或查找不到，其责任应当由投标人承担。不得将内容拆开投标，并牢固装订成册。不允许使用活页夹、拉杆夹、文件夹、塑料方便式书脊（插入式或穿孔式）装订。投标文件不得行间插字、涂改、增删，如修补错漏处，须经投标文件签署人签字并加盖公章。

2、投标文件的**资格审查资料、商务技术标、报价标均为一份正本和四份副本**，并明确标注投标人全称、“正本”、“副本”字样。

3、投标文件正本须打印并由投标人法定代表人或授权人签字并加盖单位印章。副本可复印，但须加盖单位印章。

**五、投标文件的密封及标记**

1、投标人可以将正本、副本及图纸类等（如需提供图纸等其它资料的话）合并密封，统一装在一个密封袋或密封箱内（如有A3大小的图纸类，可单独密封）。正本、副本分别密封的，封袋上应标明“正本”、“副本”字样。

2、报价标须单独密封，不得出现于资格审查资料、商务技术标正本或副本等投标资料中。

3、投标文件的资格审查资料、商务技术标和报价标应分别密封，并在封袋上写明 “**资格审查资料**”、“**商务技术标**”、“**报价标**”，同时还要写明采购人名称、项目名称及投标人名称。封袋上应加盖投标人公章。

**未按上述规定密封的投标文件，采购人不予接收**。

**六、投标文件的递交时间**

投标人必须在规定的投标文件递交截止时间前送达采购人。采购人将拒绝接收在投标截止时间后递交的投标文件。

**七、投标保证金**

1、本项目投标保证金金额：**捌仟元整**

2、投标保证金仅限**现金（密封）** ，不接受其他方式。投标人须在递交投标文件的同时将投标保证金递交给代理机构查验。

3、未按时或未按规定方式提交保证金的，视为放弃投标资格。

4、未中标的投标人保证金银行汇票在项目评审结束后退还。

5、投标单位出现下列情况，取消其投标资格，并没收其投标保证金：

5.1投标截止后投标人撤销投标文件的；

5.2中标人无正当理由不与采购人订立合同；在签订合同时向采购人提出附加条件，或者不按照招标文件要求足额提交履约保证金的。

5.3中标人提供虚假材料谋取中标的，采购人有权取消其中标资格，并有权收取其全额保证金作为违约金。

**八、履约保证金**

1、本项目成交后金额的5%。

2、在中标通知书发出送达后的15个工作日内，中标人凭成交通知书和已经汇至采购人账上的履约保证金凭证，与采购人签订合同，超期或未有协商，则视为自动放弃成交资格。

3、中标人在按要求保质保量的履行完成该项目后，一次性无息退还履约保证金；

4、由于中标人的原因，在签订合同后出现不按合同履行或不适当履行的情况，采购人有权将履约保证金作为违约金，全额不予退还；同时采购人亦有权终止合同，中标人还须依法承担相应的责任。

**九、投标有效期**

投标文件自投标截止时间起45日历内有效。

**十、投标费用**

1、投标人应承担其编制投标文件以及递交投标文件所涉及的一切费用。无论投标结果如何，采购人对上述费用不负任何责任。

2、**招标文件及相关资料费300元，由投标人在递交投标文件时缴纳，售后不退。****本项目招标代理服务费及评委费由中标人支付。招标代理服务费按贰仟元整收取。评委费按实支付。投标人自行考虑相关费用并包含在投标报价内的该项费用及风险并将其综合在单价内，不得单列。**

**第三部分 项目需求说明**

**请投标人在制作投标文件时仔细研究项目需求说明**。投标人不能简单照搬照抄采购单位项目需求说明中的技术、商务要求，必须作实事求是的响应。如照搬照抄项目需求说明中的技术、商务要求的，中标人在同采购单位签订合同和履约环节中不得提出异议，一切后果和损失由中标人承担。如投标人提供的货物和服务同采购单位提出的项目需求说明中的技术、商务要求不同的，必须在《商务部分正负偏离表》和《技术部分正负偏离表》上明示，如不明示的视同完全响应。

**一、招标范围**

安全防护设备（下一代防火墙、日志审计、堡垒机、上网行为管理、入侵防御和杀毒软件授权）、安全运维服务（异地数据备份、安全巡检服务、漏洞扫描服务、安全加固服务、应急响应服务、安全迎检服务）。

**二、项目需执行的国家相关标准规范**

产品必须是全新、未使用过的原装合格正品，完全符合采购文件规定的质量、规格和性能的要求，达到国家或行业规定的标准，实行生产许可证制度的，应提供生产许可证；属于国家强制认证的产品，必须通过认证。

**三、技术参数要求**

1、下一代防火墙

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 配置要求 | 标准1U机箱；▲网络处理能力≥20Gbps，并发连接≥200万，每秒新建连接13万/秒；标准配置≥16个10/100/1000M自适应电，4个SFP插槽，4个SFP+插槽，1个Console口， 2个扩展插槽；含应用控制、URL过滤、病毒防护、入侵防御、威胁情报检测、IPSec VPN（含700授权）、提供300个点的SSL VPN的服务；含三年规则库升级授权，三年标准维保服务。 |
| 部署模式 | 产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求。支持旁路模式； |
| 网络协议 | 所投产品必须支持VTEP（VxLan Tunnel EndPoint）模式接入VxLAN网络，并可作为VXLAN二层、三层网关实现VxLan网络与传统以太网的相同子网内、跨子网间互联互通；支持通过绑定VLAN、VNI（VXLAN Network Identifier）、远程VTEP，手动管理VxLan网络；支持MAC、VNI、VTEP静态绑定**（投标文件需要提供能够体现上述功能的截图）**； |
| 所投产品必须支持MPLS流量透传；支持针对MPLS流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL过滤、基于终端状态访问控制等安全防护功能；**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 所投产品必须支持支持通过802.3ad协议、轮询、热备等方式将多个物理口绑定为一个逻辑接口，实现接口级的冗余，并可根据：源目的MAC组合、MAC和IP组合或TCP/UDP端口组合等方式实现负载和备份**（投标文件需提供能够体现上述组合方式的配置选项截图）** |
| 所投产品必须支持MTU≥9000byte的巨型帧Jumbo Frame **（投标文件需提供能够体现上述组合方式的配置选项截图）** |
| 路由协议 | 所投产品必须支持支持静态路由、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）**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 所投产品必须支持基于策略的路由负载，支持根据应用和服务进行智能选路，支持源地址目的地址哈希、源地址哈希、轮询、时延负载、备份、随机、流量均衡、源地址轮询、目的地址哈希、最优链路带宽负载、最优链路带宽备份、跳数负载等不少于12种路由负载均衡方式，支持基于IPv4或IPv6的TCP、HTTP、DNS、ICMP等方式的链路探测，同时TCP与HTTP可使用自定义目标端口进行测试**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 所投产品必须支持ISP路由负载均衡，最大可支持8条链路负载，支持自定义负载权重，支持基于优先级的ISP路由链路备份；支持基于IPv4或IPv6的TCP、HTTP、DNS、ICMP等方式的链路探测，同时TCP与HTTP可使用自定义目标端口进行测试**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 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**（投标文件需要提供能够体现上述功能及配置选项的截图以及测试方案）** |
| 所投产品必须支持在会话的源、目的地址同为IPv4地址时，可将目的地址转换至指定服务器地址**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 所投产品必须支持在源地址转换过程中，对SNAT（源地址转换）使用的地址池利用率进行监控，并在地址池利用率超过阈值时，通过SNMP Trap、邮件等方式告警。**（投标文件需提供能够体现上述功能配置选项截图)** |
| DNS代理 | 支持IPv4的DNS代理功能，即从指定的入接口或源ISP接收到的DNS解析请求，设备可根据自定义的IP、域名对应关系，代理DNS服务器返回查询结果**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 支持出站的DNS代理功能，支持在不更改内网终端设备DNS服务器地址设置的情况下，将DNS解析请求发送至指定的DNS服务器，并代理原DNS服务器返回解析结果**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 支持DDNS功能，支持Oray向日葵、Pubyun公云、Noip、Changeip提供的DDNS服务，将动态获取的IP地址映射为固定的域名（投标文件需提供能够体现上述功能配置选项及支持)**（投标文件需要提供能够体现上述功能及配置选项、DDNS服务商的截图）** |
| 支持DNS代理策略功能，支持设置入接口、源地址、目的地址、域名等信息配置代理策略，同时支持手动选择代理或不代理功能，方便灵活根据业务需求调整代理策略（投标文件需提供能够体现上述功能配置选项及支持)**（投标文件需要提供能够体现上述功能及配置选项、DDNS服务商的截图）** |
| IPv6支持 | 所投产品必须设备接口支持配置IPv6地址，并可使用IPv6地址管理设备；支持IPv6手动及自动的IP/MAC探测及绑定； |
| 所投产品必须支持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+ |
| 所投产品必须支持NAT64，NAT66、NAT-PT等种IPv4/v6过渡技术，支持针对ICMPv6以及IPv6扩展头防护功能。 |
| 所投产品必须支持DNS64功能；支持IPv6入站的DNS代理功能，即从指定的入接口或源ISP接收到的DNS解析请求，设备可根据自定义的IP、域名对应关系，代理DNS服务器返回查询结果**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 所投产品必须支持配置基于IPv6地址的安全策略，并在一条策略中可同时启用入侵防御、反病毒、URL过滤、应用识别、反间谍软件等安全功能； |
| 所投产品必须支持针对IPv6流量通过HTTP、HTTPS实现Web认证，用户身份信息可存储在本地或Active Directory\Radius\TACACS+\POP3等第三方服务器；通过HTTPS实现Web认证必须支持使用本地CA颁发的证书同时使用证书验证客户端身份**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 所投产品必须支持DS-Lite CPE B4功能，支持成为b4或aftr角色，支持从DHCPv6服务器或手动方式获取AFTR参数**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 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；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；支持链路探测**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 虚拟防火墙功能 | 所投产品必须支持将物理防火墙资源，如会话数、安全策略数、源NAT数、目的NAT数，日志存储数量以保留值及最大值的形式自动分配。**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 所投产品必须支持虚拟防火墙逻辑接口，可以不占用物理网口的情况下实现虚拟系统之间的相互连接、访问**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 所投产品必须支持对虚系统进行系统配置，包括管理设定、管理主机、证书管理、配置文件导入导出、日志配置；虚系统管理员可分权管理**（投标文件需要提供能够体现上述功能及配置选项的截图**） |
| 所投产品必须支持在虚系统内独立配置病毒防护、漏洞利用防护、间谍软件防护、URL过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能。并可支持对本虚系统内产生的日志进行独立审计；**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 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，并支持地理区域对象的导入以及重复策略的检查**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 所投产品比如支持基于IPv4/v6地址、应用的会话限制，限制动作包每IP新建、每IP并发、所有IP新建、所有IP并发，且可以基于安全域指定限制方向**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 所投产品必须支持命中时间分析和安全策略推荐。命中时间分析展示被命中的安全策略的名称、状态、命中数、策略创建时间、首次命中时间和最近命中时间；安全策略推荐定可以指定策略流量，分析后自动生成源地址精度更高的安全策略。 |
| 应用识别与控制 | 所投产品必须支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于6000种，可深度识别每种应用的属性，为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输、风险等级等特征分类**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 所投产品可直观展示不同风险等级的应用在1天（24小时）或一周（7天）内传输流量的绝对数值及占全网流量的百分比。**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 用户识别与认证 | 所投产品必须支持基于用户的访问控制，可与LDAP/Radius/证书/Active Directory/TACACS+/POP3等用户认证系统联动**（投标文件需提供能够体现上述功能截图)** |
| 所投产品必须支持802.1x认证，要求支持基于端口和MAC两种接入控制方式 |
| 支持二层MAC地址IP地址绑定；支持跨三层MAC地址IP地址绑定**（投标文件需提供能够体现上述功能截图)** |
| 邮件过滤 | 所投产品必须支持基于关键字的接收、发送或双向Email发件人、收件人过滤，并支持自定义RLB服务器地址配置，并可结合IP黑名单或白名单 |
| 文件过滤 | 所投产品必须支持对应用的文件传输行为进行上传、下载、双向的文件类型过滤，应用至少包含即时通讯、常用协议、文件共享、论坛、博客、网页邮件五种分类；**（投标文件需提供支持的应用分类和对应的设备配置截图）** |
| 所投产品必须支持上传、下载、双向的文件内容过滤；内容过滤支持手工及文件批量导入两种方式进行敏感信息定义；内容过滤至少支持html、doc、docx、xls、xlsx、ppt、pptx、chm、7z等30种常见文件类型；文件类型识别基于文件特征而非扩展名，更改文件扩展名后仍可有效识别**（投标文件需提供支持的文件类型，敏感信息定义方式及对应的设备配置截图）** |
| 流量管理 | 所投产品必须支持多调度类相互嵌套最大5级的带宽管理设置。支持设置每IP最大或最小带宽，支持对每IP进行带宽配额管理，可通过优先级实现多应用的差分服务，并支持对剩余带宽进行基于优先级的动态分配。**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 支持配置基于IP、用户、应用的流量管理规则，且至少支持对3000种应用定制流量管理规则 |
| 共享上网检测 | 所投产品必须支持共享上网检测功能，支持共享接入检测和共享接入管控功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 服务链管理 | 所投产品支持灵活的服务链编排功能，支持串接链和旁路链，支持网元组的方向和位置设置。（投标文件需要提供能够体现上述功能及配置选项的截图） |
| 所投产品支持添加、编辑、删除串接链，旁路链。 |
| 引流策略 | 所投产品支持引流策略的添加、删除、调序、清除命中数、刷新功能；支持引流策略的启用和禁用功能。 |
| 所投产品支持灵活的细粒度引流策略，可基于源安全域、目的安全域、源用户、源地址、目的地址、服务、VLAN、服务链、流量方向（内网到外网/外网到内网）的引流策略，并详细记录日志。（投标文件需要提供能够体现上述功能及配置选项的截图） |
| 编排流量监控 | 所投产品支持对编排的流量进行监控，至少能从网元组、引流策略两个维度对编排流量监控统计（投标文件需要提供能够体现上述功能及配置选项的截图） |
| 网络攻击防护 | 所投产品必须支持基于不同安全区域防御SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood、NTP Query Flood 、NTP Reply Flood 和SIP Flood 攻击，并支持警告、丢弃、普通防护（首包丢弃）、增强防护（TC反弹技术）、授权服务器防护（NS重定向）、普通防护（自动重定向）、增强防护（手工确认）等多种防护措施**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 所投产品必须支持可配置阈值的基于安全域或基于二层接口局域网广播防护，防止局域网内广播和多播数据包泛滥**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 所投产品必须支持DHCP协议防护；支持手动定义可信DHCP服务器IPv4和基于阈值限制DHCP请求传输速率**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 所投产品必须支持基于安全区域的异常包攻击防御，异常包攻击类型至少包括Ping of Death、Teardrop、IP选项、TCP异常、Smurf、Fraggle、Land、Winnuke、DNS异常、IP分片等；并可在设备页面显示每种攻击类型的丢包统计结果**（投标文件需要提供能够体现上述攻击防护类型及丢包统计结果的截图**） |
| 所投产品必须支持防御基于安全域的IP地址欺骗攻击，指定IP或网段必须从特定安全域流入 |
| ★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；本地病毒库规模大于3000万 |
| 所投产品必须支持对最多16级的压缩文件进行解压查杀 |
| 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**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
|
| ★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、OTHER\_APP、POP3、SMB、SMTP等应用协议的漏洞防护**（投标文件需要提供能够体现漏洞防护特征库分类信息、支持的执行动作以及支持的应用协议的截图）** |
| 所投产品必须支持在设备漏洞防护特征库直接查阅攻击的名称、CVEID、CNNVDID、CWEID、严重性、影响的平台、类型、描述、解决方案建议等详细信息；**（投标文件需要提供能够在设备上显示以上内容详细信息的截图）** |
| 所投产品的漏洞防护特征库及间谍软件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、CWEID、严重性、影响的平台、类型、描述、解决方案建议等（CVEID、CNNDID、CWEID等信息在漏洞攻击特征中体现）详细信息；**（投标文件需要提供设备包含上述所有高危漏洞攻击的特征及对应详细信息的截图）** |
| 所投产品必须支持间谍软件防护功能，同时将间谍软件特征库分类，至少包括木马后门、病毒蠕虫、僵尸网络等三种分类;支持在防火墙间谍软件签名库直接查阅攻击的名称、严重性、描述等信息；间谍软件防护支持日志、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等应用协议的间谍软件防护**（投标文件需提供能够体现上述功能及配置选项截图）** |
| 所投产品必须支持自定义TCP、UDP、HTTP协议的漏洞特征，漏洞特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配，并可自定义漏洞的源、目的端口范围；同时可标识自定义漏洞的CVE编号或CNNVD编号。**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 所投产品必须支持自定义基于TCP、UDP、HTTP协议的间谍软件特征。间谍软件特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配；并可自定义间谍软件的源、目的端口范围**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| ★WEB服务防护 | 所投产品支持web服务防护（包含缓冲区溢出，跨站脚本，恶意扫描，web注入，SQL注入等），支持数据库服务防护，FTP服务防护，邮件服务防护等。**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| IPSec VPN | 所投产品必须支持支持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**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 所投产品必须支持支持GRE隧道，支持GRE over IPSec VPN |
| 所投产品的IPSec VPN功能必须支持无损数据压缩算法 |
| 其他VPN | 所投产品必须支持L2TP、支持L2TP over IPSec、支持PPTP ，并支持本地认证以及LDAP/Radius/证书/Active Directory/TACACS+/POP3等第三方用户认证系统。支持客户端地址分配**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 所投产品必须支持SSL VPN，支持使用SSL VPN客户端与防火墙建立SSL VPN加密隧道，支持对远程用户进行口令认证或证书认证，或证书认证+口令认证双因素；口令认证支持本地认证以及LDAP/Radius/证书/Active Directory/TACACS+/POP3等第三方用户认证系统；支持USB-key证书；支持本地CA并可为SSL VPN客户端颁发用于身份认证的证书；支持Windows客户端、安卓客户端、IOS客户端和MAC OS客户端。**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 网络异常感知 | 所投产品必须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**（投标文件需提供能够体现被入侵、攻破的主机状态的截图）** |
| 所投产品必须支持基于主机或威胁情报视图，统计网络中存在安全风险的主机数量以及对应的风险等级，至少可查看遭遇风险的时间、威胁类别、情报来源、威胁简介、失陷主机IP、用户名、资产等信息**（投标文件需提供能够体现存在安全风险的主机数量以及对应风险等级的截图）** |
| 所投产品必须支持本方案中配置的威胁感知设备协同，实现主机状态检测及告警；**（投标文件需提供包含云端或本方案中配置的威胁感知设备的截图）** |
| 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；**（投标文件需提供能够体现以上功能的截图）** |
| 所投产品必须支持用户自定义重点URL分类和应用，并可基于定义的重点关注对象进行用户维度关联，并结合分析中心进行基于关联的用户/地址、URL分类、应用进行二次递进式深度分析，挖掘异常用户及异常网络行为。**（投标文件需提供能够体现以上功能的设备截图）** |
| 安全事件分析 | 所投设备必须提供关联分析面板，可将Top应用、Top威胁、Top URL分类、Top源地址、Top目的地址等信息关联，并支持以任意元素于为过滤条件且不少于35个维度进行数据钻取，**(投标文件需提供包含上述信息的关联分析面板截图)** |
| 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，**(投标文件需提供包含上述信息的多维关联分析面板截图)** |
| 所投设备必须提供关联的威胁事件日志，系统可自动将产生威胁事件的连接经过防病毒、防漏洞、防间谍软件、URL过滤、文件过滤等安全模块检查的日志集中显示，**(投标文件需提供关联的威胁事件日志的截图)** |
| 所投设备必须支持自定义一个或多个过滤条件，防火墙上的全部日志进行模糊检索或指定条件的精确检索，快速定位特定目标当前行为是否存在异常，网络中是否存在异常等问题，并可记录一个或者多个自定义过滤条件历史。**(投标文件需要提供能够体现上述功能及配置选项的截图)** |
| 策略与处置 | 所投设备可在单条策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能选项。**(投标文件需提供在单条策略中启用安全功能选项的截图)。** |
| 所投设备必须支持安全策略的快速检索及基于名称、地址、端口、协议多维度的高级策略检索，支持策略的复制、调序、查询 |
| 所投产品必须支持基于受害主机的一键式阻断链接、记录日志等处置动作，处置周期至少包括1天、7天、30天、90天、永久等；**(投标文件需提供能够体现上述功能及配置选项的截图)。** |
| 所投产品必须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**（投标文件需提供能够体现上述功能及配置选项截图）** |
| 所投产品必须支持针对“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**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 运维管理 | 所投产品必须支持双系统备份，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**（投标文件需提供历史配置文件＞2个设备截图）** |
| 所投产品必须支持三权分立管理 ，权限设置至少包括全部权限，仅具有策略变更权限和仅具有日志审计权限、仅具有账户配置权限、虚系统配置管理权限以及虚系统审计权限；并支持以读写、只读、无权限的方式自定义权限管理，权限管理的范围至少包括策略配置、对象配置、网络配置、系统配置、统计分析、威胁处置等**（投标文件需提供能够体现上述功能及配置选项截图）** |
| 所投产品必须支持加密的WebUI和CLI管理，且支持网页命令行管理（WebUI中内嵌CLI管理界面），**投标文件需提供WebUI内嵌CLI管理界面的设备截图** |
| 所投产品必须支持将告警信息以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、失陷主机告警、并发数告警、CPU利用率、内存利用率、硬盘利用率、接口带宽利用率、NAT端口池利用率等；**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 所投产品必须支持将不同设备模块产生的不同重要性的日志发送至不同的日志服务器，设备模块至少包括流量、URL过滤、内容过滤、邮件过滤、行为、威胁等，重要性等级至少包括紧急、警报、严重、错误、告警、通知、信息、调试八种**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 所投产品必须支持日志模板功能，可以设置置各种日志发送的哪些字段以及字段的顺序，满足日志字段定制化需求 |
| 所投产品必须支持IPS特征库、威胁情报库、应用识别库等数据库的实时更新或手动更新。**（投标文件需要提供能够体现上述功能及配置选项的截图）** |
| 所投产品必须提供可明文或加密方式调用的Restful API，并可指定Restful API使用的本地端口；为确保设备管理的安全性，所投产品必须支持限制特定主机调用Restful API**（投标文件需要提供能够体现上述功能及配置选项的截图）**支持定义第三方设备、平台通过调用Restful API 至少可配置所投设备的访问控制策略、源NAT策略、目的NAT策略、静态路由、高可用以及区域、地址、服务、时间、用户对象等功能**（投标文件必须提供所投产品的Restful API使用说明并加盖公司公章）。** |
| 所投产品必须web页面必须内置抓包工具，并可通过表达式方便灵活的指定抓包过滤条件。**（投标文件需提供能够体现上述功能及配置选项截图）** |
| 所投产品必须提供中英文双语管理界面，并在登录页面可选择Web页面使用的语言**（投标文件需提供能够体现上述功能及配置选项截图）** |
| 所投产品必须支持业务接口下Netflow功能，能够通过Netflow实现对网络进行监控，对接口流量进行抓包，并在可将Netflow抓包文件数据外发**（投标文件需提供能够体现上述功能及配置选项截图）** |
| 所投产品必须支持资产管理，能够通过设置资产监控、VPN、源安全域来控制资产识别范围，支持scanner或onvif类型的扫描方式和网段，实现自动或手动资产扫描；支持通过设置IP地址、MAC地址、资产类型、生效市场、厂商、位置等信息来制定黑/白名单，方便日常资产管理，支持通过设置IP地址、MAC地址、资产类型、操作系统、应用、开放的端口和访问的端口等信息来制定资产指纹库**（投标文件需提供能够体现上述功能及配置选项截图）** |
| 具备LLDP功能，可以向网络中其它节点公告自身的存在，并保存各个邻近设备的发现信息，如设备配置和设备识别等详细信息。 |
| 云端协同 | 所投产品必须支持与云端联动，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）** |
| ▲终端安全软件联动 | 所投产品必须支持与本方案中配置的桌面杀毒或终端管理软件联动，实现基于终端健康状态的访问控制；并支持阻断“高风险”终端网络活动的同时，提示被阻断原因及重定向自定义网址。**（投标文件需要提供能够体现上述功能及配置选项的截图）；** |
| ★产品资质 | 所投产品具备《计算机软件著作权登记证书》，**投标文件提需供证书复印件并加盖厂商公章；** |
| 所投产品具备国家信息安全测评中心颁发的《信息技术产品安全测评证书》（EAL4+），**投标文件需提供证书复印件并加盖厂商公章；** |
| 所投产品具备公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》（增强级），投标文件需提供证书复印件并加盖厂商公章，在计算机信息系统安全专用产品销售许可证服务平台可查（https://ispl.mps.gov.cn/ispl/） |
| 具备《中国国家信息安全产品认证证书》（增强级），**投标文件提需供证书复印件并加盖厂商公章；** |
| 具备中华人民共和国工业和信息化部颁发的《电信设备进网许可证》 |
| 具备中国信息安全测评中心颁发的《国家信息安全漏洞库兼容性资质证书》，**投标文件提需供证书复印件并加盖厂商公章。** |
| 具备IPv6 Enabled Logo认证 |
| 产品生产厂商具备CIC信息化建设及数字化能力评价（一级）证书(**需提供证书复印件**)。 |

2.上网行为管理

|  |  |
| --- | --- |
| **指标项** | **详细参数要求** |
| 产品规格 | ★产品不少于4个千兆电口，单电源，硬盘≥128Gminisata SSD，1U； |
| ★网络层吞吐量≥2Gbps，应用层吞吐量≥15Mbps，支持用户数≥500，每秒新建连接数≥1000,最大并发连接数≥50000，内存≥4G； |
| 部署方式 | 支持路由模式（NAT、路由转发、DHCP、GRE、OSPF）、网桥模式（多路桥接模式）、旁路模式； |
| 管理员账号 | 支持细致的管理员权限划分，包括对不同用户组的管理权限、对各种主要功能界面的配置和查看权限； |
| 实时监控 | ★支持首页分析显示接入用户人数、终端类型；带宽质量分析、实时流量排名；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行；（需提供产品功能截图证明） |
| 排障工具 | 支持PPS异常、丢包异常、ARP异常、内网DOS攻击等异常情况实时监测，显示每日异常事件个数及情况； |
| ★支持针对用户认证的故障进行分析，给出错误详情以及排查建议；（需提供产品功能截图证明） |
| 用户管理 | 支持从本地导入和扫描导入，支持以CSV格式文件导入帐户/分组/IP/MAC/描述/密码等信息；用户分组支持树形结构，支持父组、子组、组内套组等； |
| 认证管理 | 基于IP网段、VlanID、MAC、SSID、地址等实现新用户差异化自动分组、认证规则； |
| 支持认证页面分权分域管理；启用后，普通管理员只能看到自己有权限的页面，其他管理员页面不可见； 系统管理员可以将某个页面授权给指定的普通管理员管理； |
| 认证方式 | 支持radius、AD、POP3、Proxy、PPPOE、 H3C IMC/CAMS、锐捷 SAM、城市热点等系统进行认证单点登录，简化用户操作，可强制指定用户、指定IP段的用户必须使用单点登录； |
| 支持触发式WEB认证、用户名密码认证、IP/MAC认证、短信认证、自注册认证； |
| ★支持终端用户账号绑定手机号码和微信号，绑定后可以通过手机验证码和微信扫码实现上网快捷登录认证；（需提供产品功能截图证明） |
| 支持二维码认证，担保人扫描访客的二维码后对其网络访问授权；支持访客填写信息、担保人填写信息、担保人扫码审核三种模式； |
| 应用管理 | ★设备内置应用识别规则库，支持超过9000条应用规则数、支持超过6000种以上的应用；支持根据标签选择应用，并支持给每个应用自定义标签；支持根据标签选择一类应用做控制；（需提供产品功能截图证明） |
| ★支持超过900种主流Saas应用，对Saas应用有默认分类标签，帮助客户统一配置策略；（需提供产品功能截图证明） |
| 邮件管理 | ★支持允许用户登录Webmail收邮件，而禁止发送Webmail邮件的功能；（需提供产品功能截图证明） |
| 流量管理 | ★支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率；空闲值可自定义；（需提供产品功能截图证明） |
| ★支持通过抑制P2P的下行丢包，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；（需提供产品功能截图证明） |
| 用户配额管理 | ★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；用户指定应用上网流速超过预设阈值后，网关自动提醒该用户；（需提供产品功能截图证明） |
| 日志管理 | 支持内置日志中心和独立日志中心；支持分级配置管理员日志查看权限，管理员登录日志中心只能查看指定用户组的上网行为日志； |
| 资质要求 | ★所投产品的生产厂商的软件研发实力具备CMMI L5认证，提供有效证书的复印件。 |
| ★为保障产品成熟度，要求所投产品的生产厂商具备中国网络安全审查技术与认证中心的信息安全软件开发服务一级资质，提供有效证书复印件。 |

3.日志审计

|  |  |
| --- | --- |
| **指标项** | **详细参数要求** |
| 硬件和性能规格 | 标准1U机箱，单电源；★综合日志处理性能2600EPS；默认配置≥4个千兆电口，1个Console接口，≥2TB硬盘；▲包含≥50个日志源授权，含三年软件升级服务和三年硬件维保服务。 |
| 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；  支持审计主机各种操作系统（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. |
| 日志采集与转发 | 支持通过Syslog、Syslog-NG、SNMP Trap、Netflow V5、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，支持多行日志采集合并为一行； |
| 支持按照Syslog-NG标准及自有格式进行转发，转发时包含原始日志源IP地址； |
| 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，支持资产组可以在页面不同的分组中移动。  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；  支持对资产日志进行过滤，设置允许接收和拒绝接收日志，并可以对资产设置一定时间范围内未收到事件后进行主动告警。 |
| 支持对资产IP地址（含内网IP）的地理信息进行管理，设置单IP及IP段行政区及经纬度，支持地图显示 |
| 支持自定义资产类型及资产属性；支持对资产自定义标签，支持对标签内容进行查询和管理 |
| 日志归一化 | 支持对日志进行归一化处理并保留原始日志，方便用户对关键日志快速定位和事后取证； |
| 系统提供页面可视化编辑归一化策略，对页面查看的日志编辑归一化策略，所见即所得，也支持通过归一化文件的导入来支持归一化,不需修改系统程序。 |
| 系统可自动识别收集的日志并自动选择范化策略，也可由人工设置设备的范化策略。 |
| 解析时间格式字段时能够自动匹配推荐格式。范化绑定支持添加多IP；范化策略可以进行复制操作，下面的二级策略也可以一同复制。新建策略时进行自动编号。字段查询，支持使用汉语拼音首字母查询。 |
| 支持对日志中的源和目的IP地址进行自动补全，补全IP地址的资产、国家、区域和城市等信息 |
| 日志交互式分析 | 系统具备全文检索的大数据处理能力，能够对事件进行非格式化的文本式处理，可将原始信息进行自动索引，快速搜索分析各类安全事件。系统提供即席查询功能，支持归一化字段及关键字搜索，从海量事件原始信息中获取与关键字匹配或部分匹配的所有事件。系统支持基于正则表达式的检索功能，用户可在搜索栏内输入正则表达式，系统可搜索出原始信息中与正则表达式相匹配的所有事件； |
| 用户可自定义事件搜索查询条件，并可保存为策略，以树形结构进行组织，形成一个搜索分析策略树；每个查询场景都可以查询策略的形式进行存储。 |
| 可以显示一段时间的动态事件移动图，能够在图上显示每个时间切片的事件数量，点击该时间切片，可以查看该切片内的所有事件；动态事件移动图可设置动态刷新频率，根据刷新时间显示实时事件； |
| 系统支持即席在线查询，支持嵌套查询，可针对查询结果任意回退，收敛事件范围；用户可根据需要配置事件显示的字段内容等。查询结果可支持加密导出； |
| 用户点击单条事件，可对该事件进行展开，显示事件详细信息和原始信息； |
| 用户点击事件的某一字段，可以该字段及内容为条件在当前事件集中进行事件搜索，显示相应结果； |
| 可以以图形化的方式展示日志属性之间的聚合关系，并支持手动选择日志属性，显示多维事件分析图；属性可增加或减少，且支持图片大小调整。 |
| 日志统计分析 | 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； |
| 支持柱状图、饼图、折线图、面积图、堆积图、环状图、数值图、地图、3D地球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。 |
| 支持将统计结果保存为仪表板、报表和策略。 |
| 日志综合展现 | 系统提供可编辑的灵活强大的自定义仪表板； |
| 资质 | 《计算机软件著作权登记证书》（复印件加盖投标人公章，未提供的作负偏离处理） |
| ★产品具备公安部网络安全保卫局颁发《计算机信息系统专用产品销售许可证》网络通信安全审计类（增强级）**(需提供证书复印件)** |

4.堡垒机

|  |  |
| --- | --- |
| **指标项** | **详细参数要求** |
| ▲配置 | 标配接口≥6个千兆电口,支持2个接口扩展槽位，内置≥2TB硬盘，最大支持150路图形会话或400路字符会话并发。授权50个被管资源数； |
| 身份认证 | 支持多因子认证，包括手机令牌、手机短信、动态令牌、国密USBKey、指纹识别等方式**（需提供相关截图证明）** |
| 支持微信小程序动态口令认证方式登录堡垒机，且当用户需要使用手机令牌登录时，需要强制绑定手机令牌 |
| 用户管理 | 系统内置部门管理员、策略管理员、审计管理员、运维员等角色，并支持按模块和功能自定义角色权限，便于管理，用于复杂的业务场景需求；支持角色权限细粒度划分，包括新建部门、安全配置、网络配置、HA配置、端口配置、外发配置、认证配置、工单配置、告警配置、系统风格等权限划分**（需提供相关截图证明）** |
| 资源管理 | 支持的运维协议包含SSH、RDP、VNC、Telnet、FTP、SCP、SFTP、DB2、MySQL、Oracle、SQL Server、Rlogin、DM、Redis等 |
| 支持云主机资源批量导入，包括阿里云、百度云、华为云、腾讯云、Ucloud、AWS、Azure云平台的资源，支持设置优先导入公网和内网IP设置，支持导入同时批量新建标签 |
| 针对核心设备可配置双人授权，需要管理员现场审批才能访问资源 |
| 支持对MySQL、Oracle和达梦数据库的访问操作进行控制，可基于库、表、命令实现对数据库操作的细粒度访问控制，执行动作包括但不限于断开连接、拒绝执行、动态授权、允许执行**（需提供相关截图证明）** |
| 资源运维 | 不限操作系统类型，无需安装任何客户端插件，使用浏览器通过H5方式即可直接运维SSH、RDP、Telnet、VNC、Rlogin和SFTP资源**（需提供相关截图证明）** |
| 支持SSH、RDP、TELNET、VNC协议资源的批量登录功能，并且支持混合协议的批量登录，支持同时在一个页面运维不同协议的资源 |
| 支持以云盘形式在堡垒机上存储常用文件，实现操作端、堡垒机和目标资源三者之间文件共享（支持多文件和文件夹下载，文件展示最近修改时间和权限） |
| 工单管理 | 申请工单支持文件管理、RDP剪切板、磁盘映射、键盘审计、剪切板审计（上行、下行）、显示水印、上传、下载权限、OCR识别申请 |
| 支持管理员对工单的修改，管理员可以对自己审批节点的工单内容进行修改，增加或者取消非必要权限 |
| 审计日志 | 支持对实时会话进行无延时的实时监控和切断 |
| 支持采用OCR识别技术，可以识别图形操作中的操作系统文字、应用软件文字、浏览器文字等文本信息，支持设置识别精细度和识别间隔时间，以平衡性能开销和识别精度 |
| 支持水印功能，用户在运维或者是监控、查看会话时，H5页面会将用户的登录名作为水印展示，避免数据泄露无法追责，支持在H5运维SSH、RDP、TELNET、VNC、应用发布等资源时显示水印**（需提供相关截图证明）** |
| 系统管理 | 支持自定义系统事件的告警等级及方式，例如系统消息、邮件、手机短信，支持告警等级细粒度配置，例如CPU使用率超过50%为中风险告警，CPU使用率超过90%为高风险告警 |
| 产品需支持专属手机app远程管理（非浏览器方式），可在app端实现用户管理、主机管理、工单审批、告警消息、会话管理等功能**（需提供app功能截图证明并）** |
| ★资质 | 具备中国电子工业标准化技术协会信息技术服务分会颁发《ITSS运行维护符合性证书》二级**(需提供证书复印件)** |
| 产品生产厂商具备中国网络安全审查技术与认证中心颁发《信息安全服务资质-软件安全开发》（一级）**(需提供证书复印件)** |
| 产品生产厂商具备中国信息安全测评中心颁发的信息安全服务资质证书（安全工程类不低于三级）**(需提供证书复印件)** |
| 产品生产厂商参与信息安全等级保护关键技术国家工程实验室共建协议**(需提供证书复印件)。** |

5.杀毒软件

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| ★平台环境要求 | 管理中心操作系统支持Windows Server 2012 R2/2016/2019/2022的64位版本（简体中文版）；客户端支持windows pc、Windows Server、linux、mac、国产化等系统 |
| 产品形态 | 软件版本。 |
| ▲授权要求 | 本项目要求提供windows 终端200台；服务器 windows server 11台，Liunx 2台 |
| 国产化支持 | 支持中标麒麟/银河麒麟/普华/深度/红旗桌面操作系统。 |
| 基础功能 | 支持根据分组、计算机名称、IP地址、MAC地址、通信IP地址、接入点、客户端类型、操作系统类型、操作系统版本等条件的组合筛选出符合条件的终端进行管理，自由对终端进行转移分组、删除终端、重启系统和终端跃迁。 |
| 支持自动分组，按IP地址、CPU数量、MEM容量、主机名、计算机工作组等参数进行自动动态调整分组 |
| 客户端主程序、病毒库版本支持按分组和多批次进行灰度更新，保持在低风险中完成终端能力更新。支持设置不同终端类型设置和每批次观察时长。当检测到新版本将从第一批次重新观察。**（提供产品功能截图）** |
| 安全小助手 | 支持手动扫描和清理软件安装残留文件以及系统历史记录文件 |
| 支持检测系统启动项、服务项、计划任务，并支持启动项的优化 |
| 病毒防护 | 病毒防护概况：终端基础信息、病毒库版本、发现病毒数、未处理病毒数、最后查杀时间、文件防护状态、引擎使用状态、扩展病毒库版本 |
| 支持通过文件数字签名添加黑白名单管理 |
| 支持对终端当扫描到感染型病毒、顽固木马时，自动进入深度查模式，可设置禁止终端用户管理路径或文件白名单、禁止终端用户管理扩展名白名单、扫描时不允许终端用户暂停或停止扫描任务。 |
| 支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少大约10层模式下的扫描。 |
| 支持对进程防护、注册表防护、驱动防护、U盘安全防护、邮件防护、下载防护、IM防护、局域网文件防护、网页安全防护、勒索软件防护。**（提供产品功能截图）** |
| 支持无文件攻击防护、文档攻击防护、横移渗透攻击防护、内存攻击防护。**（提供产品功能截图）** |
| 补丁管理 | 支持对Windows操作系统、IE、.NET Framework、Office、Adobe Flash Player、Adobe Acrobat和Adobe Acrobat Reader DC、硬件驱动更新等软件进行补丁修复 |
| 支持管理员预先设置好灰度发布批次和漏洞修复策略（分时间段、按级别、排除有兼容性问题的补丁等），每当控制台更新补丁库，自动化编排完成漏洞修复——将全网终端划分为由小到大的多个批次，根据企业环境，自动先推送给第一个小批次分组，如无问题自动推送给下一个批次，直到推送给全网。如有问题，只需将有问题的补丁添加到排除列表和卸载已安装的终端即可。整个推送安装过程自动化编排，无需管理员过多参与，只需在有问题时添加排除列表和下发卸载补丁任务。**（提供产品功能截图）** |
| 支持按照补丁的维度统计补丁安装情况，包括补丁号、系统类型、补丁类型、补丁级别、补丁名称、补丁描述、发布日期、漏洞CVE编号、漏洞CNNVD编号、未安装、已安装、已安装未生效、已排除、未更新补丁库。并支持导出统计报表。**（提供产品功能截图）** |
| 主机防火墙 | 支持主机防火墙功能，通过添加IP、域名规则、支持允许/拒绝规则、支持任意流向拦截和允许，支持TCP、UDP、TCP+UDP、ICMP、多播和组播，支持自定义端口范围、支持自定义目标IP，支持输入IP范围。 |
| 弹窗防护 | 支持全屏/非全屏模式拦截已知第三方软件弹窗，拦截所有第三方软件弹窗以及不拦截弹窗。 |
| 支持对不同类型主流软件的弹窗进行拦截，终端可定期更新云端弹窗规则库 |
| 终端管控 | 支持对单点维护功能，可远程查看终端实时运行的进程，需要包含进程名称，进程用户、命令行（执行路径+执行参数）、内存占用、支持远程结束进程。支持远程查看计算机各个网卡配置信息。 |
| 支持对外设进行多维度的放行，包括设备名称、PID/VID、实例路径，通过添加实现例外或加黑。 |
| 支持对终端节能管理，支持对长时间运行、定时关机、空闲节能、工作时间外开机等节能类型设定策略，支持仅提示、关机、注销、锁定、关闭显示器、锁定+关闭显示器、休眠和睡眠处理。并支持提示倒计时弹窗，可设置在终端取消后下一次提醒时间。**（提供产品功能截图）** |
| ▲联动 | 本次所投终端安全管理系统支持和防火墙设备联动 |
| ★资质要求 | 产品生产厂商具备国测信息安全服务资质-云计算安全类一级**（提供相关证明文件）** |
| 产品生产厂商获得CNNVD漏洞预警报送专项奖**(需提供证书复印件)** |
| 产品生产厂商具备中国网络安全审查技术与认证中心颁发《信息安全服务资质-软件安全开发》（一级）**(需提供证书复印件)** |
| 产品生产厂商具备中国信息安全测评中心颁发的信息安全服务资质证书（安全工程类不低于三级）**(需提供证书复印件)** |
| 产品生产厂商参与信息安全等级保护关键技术国家工程实验室共建协议**(需提供证书复印件)**。 |

6.安全运维服务

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 下一代防火墙入侵防御和防病毒授权维保 | 对原有的华为下一代防火墙USG6585E中的入侵防御和防病毒模块授权三年维保。 | 套 | 3 |
| 2 | 异地数据备份服务 | 按需提供业务，支持完全备份、差异备份、增量备份；支持系统、数据库等整体恢复，也可针对问题数据进行还原，实现业务快速恢复。可分别设置定时任务和备份数据集的保留时间，使备份计划更加合理，含（配套主机），通过点对点数据专线连接，备份地点位置在南通以外区域(需提供承诺函)。 | 年 | 3 |
| 3 | 安全巡检服务 | 对网络设备和服务器等进行巡检服务，并且根据巡检情况，及时调整安全策略，保证安全设备有效、可靠运行。每季度一次。 | 年 | 3 |
| 4 | 漏洞扫描服务 | 对网络设备、服务器操作系统、应用系统进行漏洞扫描，从而可以进行漏洞修复。每季度一次。 | 年 | 3 |
| 5 | 安全加固服务 | 对巡检过程中发现的问题进行安全策略调整；对漏洞扫描过程中发现的各种安全隐患，进行安全加固和安全优化。根据甲方实际情况，按需进行。 | 年 | 3 |
| 6 | 应急响应服务 | 当发生黑客入侵、系统崩溃或其它影响业务正常运行的安全事件时，第一时间对安全事件进行应急响应处理。根据实际情况，按需进行。 | 年 | 3 |
| 7 | 安全迎检服务 | 配合完成公安等上级部门网络安全检查，配合完成检查前准备，文档编制等工作，检查中配合工作，检查后整改工作。根据实际情况，按需进行。 | 年 | 3 |

注：本次采购项目需要投标人对清单中设备提供为期三年的原厂质保和软件升级服务。提供针对本项目的原厂质保服务承诺函复印件，中标后签订合同后提供承诺函原件，不能提供或故意拖延，采购人有权终止合同，并由投标人承担相应的法律责任。

**四、配置清单**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 类别 | | 设备名称 | 数量 | 作用 |
| 安全防护设备 | 硬件设备 | 上网行为管理 | 1台 | 对访问互联网的用户行为进行审计和分析 |
| 下一代防火墙 | 1台 | 对服务器区边界的恶意代码、入侵行为进行阻断 |
| 堡垒机 | 1台 | 对运维人员的操作行为进行记录和审计 |
| 日志审计 | 1台 | 对服务器和其他安全设备的日志进行统一收集管理 |
| Liscense | 下一代防火墙入侵防御和防病毒授权 | 3年 | 对出口边界的恶意代码、入侵行为进行检测和阻断 |
| 杀毒软件 | 3年 | 对服务器和终端电脑进行统一杀毒管理 |
| 安全运维服务 | | 异地数据备份 | 3年 | 对所有业务系统的数据进行备份，提高机房容灾能力 |
| 安全巡检服务 | 3年 | 对网络设备和服务器等进行巡检服务，并且根据巡检情况及时调整安全策略保证安全设备可靠运行。 |
| 漏洞扫描服务 | 3年 | 对网络设备、服务器操作系统、应用系统进行漏洞扫描和漏洞修复。 |
| 安全加固服务 | 3年 | 对巡检过程中发现的问题进行安全策略调整；对漏洞扫描过程中发现的各种安全隐患进行安全加固和优化。 |
| 应急响应服务 | 3年 | 当发生黑客入侵、系统崩溃或其它影响业务正常运行的安全事件时，第一时间对安全事件进行应急响应处理。 |
| 安全迎检服务 | 3年 | 迎接公安等上级部门网络安全检查，完成检查前准备，文档编制等工作，检查中配合工作，检查后整改工作。 |

（1）所有产品均要求全新原厂原包装。

（2）交货期：自合同签定之日起30个工作日内完成供货、安装及调试。

（3）交货（服务）地点：用户指定地点。

**五、项目需满足的服务标准、期限、效率等要求**

本项目中包含的设备和软件，质保期三年及软件免费升级三年，免费送货、安装、培训，在质保期内免费维护维修及技术支持。须承诺发生故障时，接到用户通知2小时内上门，24小时内解决问题。

**六、项目的验收标准**

采购单位按合同约定积极配合投标人履约，按合同约定及时组织相关专业技术人员，必要时邀请相关部门等共同参与验收，并出具验收报告。

**七、项目的其他技术、服务等要求**

（1）投标人应提供详细的售后服务方案；

（2）质保内免费提供产品的维修维护，包括非人为因素发生的产品修理、更换的费用。过质保期后应提供上门维修，维修费用只收取零部件成本费；

**八、项目付款条件**

签订合同后10日内，采购人支付项目总价的50%,设备安装调试完成经验收后10日内支付至项目总价的95%，本项目质保期3年，质保期满后10日内支付至项目总价的100%。

**九、投标报价**

1、本项目不接受任何有选择的报价。

2、投标报价均以人民币为报价的货币单位。

3、报价表必须加盖投标人公章且必须经法定代表人或委托代理人签署。总价和明细价的大小写金额必须一致，若有差异，以大写为准。

4、报价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。

5、投标报价采用综合总价报价：

（1）投标人对投标报价中应包括响应及完成本项目工作所需的一切费用。包含但不限于设备、服务劳务、管理、培训费、材料费、运输费、保险、售后服务、利润、税金、政策性文件规定及合同包含的所有风险、责任等各项应有费用。

（2）投标报价为成交价。一旦成交，除因特殊原因并经与采购人协商取得同意，成交的投标人不得再要求追加任何费用。

（3）除非合同条款中另有规定，否则，投标人所报价格一旦成交，在合同实施期间不因任何市场变化的因素而变动。

6、招标文件未列明，而投标人认为必需的费用可列入报价，但须包含在报价内。项目报价：包括买方项目需求所涉及的所有费用，项目单价按配置及明细报价表中各分项要求填报。

7、投标报价为最终报价，即**本次招标项目仅为一次报价。**

8、除非因特殊原因并经采购人和中标人双方协商同意，中标人不得再要求追加任何费用。同时，除非合同条款中另有规定，否则，中标人的中标价在合同实施期间不因市场变化因素而变动。

**第四部分 开标和评标**

**一、采购人组织开标。**

投标人的法定代表人或授权委托人须持本人**有效身份证原件**参加开标会。

**二、评委会**由有关专家组成，对投标文件进行审查、质疑、评估、比较。评委会按照公平、公正、择优的原则进行独立评标。

评委会对投标人的投标资格及有关资质是否符合要求，进行审查后进入评审环节。

**（一）评审内容**

1、要求的保证金是否已提供；

2、投标资格是否符合；

3、投标文件是否完整；

4、投标文件是否恰当签署；

5、是否作出实质性响应（**是否有实质性响应，只根据投标文件本身，而不寻求外部证据）；**

6、是否有计算错误。

**（二）相应的规定**

1、如果单价汇总金额与总价金额有出入，以单价金额计算结果为准；

2、单价金额小数点有明显错位的，应以总价为准；

3、正本与副本有矛盾的，以正本为准；

4、若文件大写表示的数据与数字表示的有差别，以大写表示的数据为准。

**三、陈述、演示、答疑、澄清**

如评委会认为有必要，投标人按评委会的要求作陈述、演示、答疑及澄清其投标内容。时间由评委会掌握。

重要澄清答复应是书面的，但不得对投标内容进行实质性修改。

**四、出现下列情形之一的，作无效投标处理**

1、未提供原件包的；

2、未按照招标文件规定要求装订、密封、签署、盖章的；

3、不具备招标文件中规定的资格要求的；

4、投标报价高于采购预算价或最高限价的；

5、不符合法律、法规和招标文件中规定的其他实质性要求的。

**五、出现下列情形之一的，作废标处理**

1、符合专业条件的投标人或者对招标文件作实质响应的投标人不足3家的；

2、出现影响采购公正的违法违规行为的；

3、投标人的报价均高于采购预算价或最高限价的；

4、因重大变故，采购任务取消的。

上述均保留评委会认定可以确定为无效投标或废标的其他情况。

**六**、**变更为其他方式采购的情形**

投标截止时间出现如下情形的，参加投标的投标人不足3家的，及评标中出现符合专业条件的投标人或对招标文件作实质响应的投标人不足3家的，除采购任务取消外，视情采取其他方式采购。本次招标文件中对投标人资质、技术等要求，将作为其他方式采购的基本要求和依据。原已经参加投标并符合要求的投标人，根据自愿原则，参加其他方式采购。

**七、评标方法**

采用综合评分法。分价格标、商务技术标两部分评审，总分值为100分。

首先评审商务技术标，待商务技术标评审结束后，再开启价格标。

**(一) 商务技术分（70分）**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **评分点名称** | **分值** | **评审标准** |
| 1 | 技术参数响应程度 | 30 | 投标人根据响应文件技术参数要求进行逐条应答，并提供技术偏离表（未提供的，视为负偏离）参数中带▲项不允许负偏离。参数中带★项的为重要技术参数，负偏离有一条扣2分；其他的负偏离有一条扣1分，扣完为止。所投产品应标参数完全满足得30分。 |
| 2 | 综合信誉 | 14 | 1、投标人具有有效的ISO9001质量管理体系认证、ISO20000信息技术服务管理体系认证、ISO27001信息安全管理体系认证证书、ISO27701隐私信息管理体系认证证书、ISO22301业务连续性管理体系认证证书的，每有一个得1分，本项最高得5分。  2、投标人具有信息系统建设和服务能力等级证书的，CS3及以上得2分，CS2及以下得1分，本项最高得2分。  3、投标人具有信息技术服务运行维护能力（ITSS）二级及以上资质得2分，否则不得分。  4、投标人具备CCRC信息安全服务资质认证的信息系统安全运维服务三级及以上资质的得1分，具备CCRC信息安全服务资质认证的信息系统安全集成服务二级及以上资质的得1分，最高得2分。  5、投标人具有机电工程施工总承包资质的得1分，否则不得分。  6、投标人能提供服务响应时间承诺书的得2分。  投标人须提供以上相关证书的扫描件并加盖公章，否则不得分。 |
| 3 | 服务能力 | 5 | 1、拟投入本项目的项目经理(唯一)具有高级信息系统项目管理师、注册信息安全工程师认证证书、网络与信息安全应急人员认证证书、IT服务项目经理证书，每提供一个证书得0.5分，最高得2分。未提供不得分。  2、项目组实施成员具有软件设计师、信息系统安全专业认证（CISSP）、CISAW信息安全保障人员认证证书、高级用户研究工程师、高级程序员证书、系统分析师证书，每提供一个证书得0.5分，本项最高得3分。  注:投标时需提供以上人员相关资质证书扫描件并加盖投标人公章以及上述人员企业为其在社保部门缴纳的社保纳证明2023年5月-2023年10月连续的社保缴纳记录)，以上材料提供不全的不得分。 |
| 4 | 异地灾备产品实力证明 | 5 | 1、投标人或所投产品制造商需具备信息技术服务能力标准 ITSS 一级（云计算服务能力）以上资质证书得2分；提供：资质证书复印件并加盖投标人公章。  2、投标人为本项目提供的解决方案需满足“云灾备容灾解决方案评估”的认证证书的得2分，否则不得分；提供第三方认证机构官网截图以及第三方认证机构认证证书的复印件，并加盖投标人公章。  3、投标人为本项目提供的云资源获得“云安全中心”的认证证书的得1分，否则不得分；提供第三方认证机构官网截图以及第三方认证机构认证证书的复印件，并加盖投标人公章。 |
| 5 | 类似业绩 | 4 | 投标人需提供自2020 年 1月 1 日以来（时间以合同签订时间为准）具有类似业绩案例（提供案例承建单位必须与本投标主体一致），每提供1个得1分，最高得4分。提供相关合同原件扫描件并加盖投标人公章，不提供不得分。 |
| 6 | 项目方案 | 12 | 供应商根据招标需求进行集成服务的方案设计。方案内容需包含项目背景、安全巡检方案、漏洞扫描方案、安全加固方案、实施方案、实施流程、应急响应方案、人员配备、售后服务等。  方案非常详细、完善、合理，可行性非常强，能完全满足或优于项目需求的得9-12分。  方案较详细、完善、合理，可行性较强，能基本满足项目需求的得5-8分。  方案不够详细、完善、合理，可行性差，能满足项目部分需求的得0-4分。  不提供不得分。 |

技术分取各位评委打分的平均值，分值保留小数点后两位。

**(二)价格分（30分）**

1、投标报价低于或等于采购预算价格40万元的，为有效投标报价。超采购预算的投标报价为无效投标报价。

2、价格分统一采用低价优先法计算，即满足招标文件要求且最后报价最低的投标报价为评标基准价，其价格分为满分。其他投标报价得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）×价格权值×100

**本办法未尽事宜，由评标委员会依据相关法规研究确定。**

**八、中标人及中标价的确定**

1、汇总三项分数后，推荐得分最高者为中标单位。

2、如出现二个及以上相同的最高分，按项目维保投标报价分高的推荐为中标单位。

3、如综合得分且投标报价也相同的，现场随机抽签决定。

**九、其他注意事项**

1.在开标、评审期间，投标人不得向评委询问情况，不得进行旨在影响评标结果的活动。

2.评委会不得向投标人解释落标原因。

3.在投标、评标过程中，如果投标人联合故意压低报价或出现其他不正当行为，采购人有权中止投标或评标。

4.凡在投标、开标过程中，采购人已提示是否异议的事项，投标人当时没有提出异议的，事后投标人不得针对上述事项提出质疑。比如：采购人在开标中提示评委是否回避，投标人现场未提出异议的，事后不得针对评委回避事项提出质疑。

**十、中标通知**

中标结果在南通市中央创新区建设投资有限公司网站（http://www.ntscid.cn/）公示，公示期限为1个工作日。《中标通知书》一经发出，如采购单位改变中标结果，或者中标人放弃中标的，各自承担相应的法律责任。《中标通知书》是采购合同的组成部分。

**第五部分 合同及履约保证**

一、中标人和采购单位自中标（成交）通知书发出之日起30日内按时签订合同。合同签订后中标人方可履约，否则引起的一切后果由中标人自行承担。所签合同不得对采购文件作实质性修改。采购单位不得向中标人提出不合理的要求作为签订合同的条件，不得与中标人私下订立背离采购文件实质性内容的协议。

二、采购单位按合同约定积极配合中标人履约，中标人履约到位后，请以书面形式向采购单位提出验收申请，采购单位接到申请后原则上在10个工作日内及时组织相关人员共同参与验收，并出具验收报告，作为支付货款的依据。

三、采购单位故意推迟项目验收时间的，与中标人串通或要求中标人通过减少货物数量或降低服务标准的，在履行合同中采取更改配置、调换物品等手段的，要求中标人出具虚假发票或任意更改销售发票的，谋取不正当利益的，承担相应的法律责任。

四、中标人出现违约情形，应当及时纠正或补偿；造成损失的，按合同约定追究违约责任；发现有假冒、伪劣、走私产品、商业贿赂等违法情形的，应由采购单位移交工商、质监、公安等行政执法部门依法查处。

五、不响应付款方式的，视同无效投标处理。款项由采购单位按相关财务支付规定办理支付手续，不得故意拖延支付时间。

**第六部分 质疑提出和处理**

**一、质疑的提出**

1、质疑人必须是直接参加本次招标活动的当事人。

2、领取招标文件的投标人应根据第二部分“投标须知”中“第一款”的约定提出疑问；质疑提出的有效时限，见《中华人民共和国政府采购法实施条例》第五十三条。

3、提出质疑时，必须坚持“谁主张，谁举证”、“实事求是”的原则，不能臆测。属于须由法定部门调查、侦查或先行作出相关认定的事项，质疑人应当依法申请具有法定职权的部门查清、认定，并将相关结果提供给采购人。采购人不具有法定调查、认定权限。

4、对本次招标有质疑的，实行实名制，不得进行虚假、恶意质疑。质疑人应在质疑有效期内以书面形式提出《质疑函》（格式请下载），《质疑函》内容应包括质疑事项、主要内容、事实依据、适应法规条款、佐证材料等。同时，质疑人应保证其提出的质疑内容及相关佐证材料的真实性及来源的合法性，并承担相应的法律责任。

对不能提供相关佐证材料的、涉及商业秘密的、非书面形式的、非送达的、匿名的《质疑函》将不予受理。

相关佐证材料要具备客观性、关联性、合法性，无法查实的（如宣传册、媒体报道、猜测、推理等）不能作为佐证材料。

**采购人、招标代理机构不负责搜集相关佐证材料等工作。**

**二、《质疑函》的受理和回复**

1、《质疑函》须由质疑人的法定代表人或参加本次招标授权人送达招标代理机构和采购人。

2、对符合提出质疑要求的，招标代理机构和采购人签收并出具《质疑受理通知书》。在处理过程中，发现需要质疑人进一步补充相关佐证材料的，请质疑人在规定的时间内提供，质疑回复时间相应顺延。质疑人不能按时提供相关佐证材料的，视同放弃质疑。

3、对不符合提出质疑要求的，出具《质疑退回通知书》并提出相关补充材料要求，质疑人未在规定的时间内提供补充佐证材料的，视同放弃质疑。

4、招标代理机构、采购人负责将质疑人提出的质疑相关材料提供给相关专家或评委审核，并将审核意见回复质疑人。

必要时，可向被质疑人转发《质疑函》及相关佐证材料。被质疑人应当在要求的时间内，以书面形式作出说明，并提交相关证据。被质疑人在规定时间内，无正当理由未提交相关证据的，视同放弃说明权利，认可被质疑事项。

5、因质疑情况复杂，组织论证或审查时间较长的，招标代理机构、采购人以书面形式通知质疑人，可适当延长质疑回复处理时间。

**三、质疑处理**

**1、质疑成立的处理。**采购人终止采购，并建议有关部门给相关当事人予以处理。

**2、质疑不成立的处理。**

1）质疑人书面《申请撤回质疑函》的，不作违约处理。

2）质疑人在规定的时间内不配合进行质疑调查处理的，按自动撤回《质疑函》处理。

3）质疑人不按《质疑函》格式就提出质疑的，作违约处理。采购人有权收取其保证金的10%作为违约金；同时，视情列入不良供应商名单。

4）质疑人虽提供了相关佐证材料，但不能证明其质疑成立的，采购人请质疑人补充相关佐证材料，仍不能证明其质疑成立的，作违约处理。采购人有权收取其保证金的50%作为违约金；同时，列入不良供应商名单。

5）质疑人不能提供相关佐证材料的，采购人已指出，质疑人仍然坚持提出质疑的，作违约处理。采购人有权收取其保证金的100%作为违约金；取消相应会员资格6个月，同时，列入不良供应商名单。

6）对明显有违背事实的、经相关专家或评委认定无依据的、经其他投标人举证无依据的质疑，作违约处理，采购人有权取消其会员资格，收取其保证金的100%作为违约金，列入不良供应商名单；同时，对其中每一项不成立的质疑给予质疑人1年内禁入由采购人组织的政府采购活动的违约处理，依次类推；视情在南通市公共资源交易网、省、国家级相关媒体予以披露。

7）质疑人承担使用虚假材料或恶意方式质疑的法律责任。

**四、无佐证材料的举报作违约处理。**供应商不得进行不提供相关佐证材料（含无法查实的如宣传册、媒体报道、猜测、推理等）向有关部门的举报，否则作违约处理，并在1至3年内禁止其参加由南通市中央创新区建设投资有限公司及下属单位组织的采购活动。

**五、投诉不成立的作违约处理。**供应商进行质疑后，采购人回复质疑不成立，供应商仍进行投诉的，并最终投诉不成立的，作违约处理，并在1至3年内禁止其参加由南通市中央创新区建设投资有限公司及下属单位组织的采购活动。

**六、《质疑函》、《质疑回复函》，质疑、举报、投诉不成立的**等相关情况，视情在南通市公共资源交易网、省、国家级等相关媒体予以披露。并建议相关政府采购机构对该供应商同步实施1至3年内禁入。

**第七部分 投标文件组成**

**投标文件由资格审查证明材料、报价标、商务技术标三部分组成。**

**一、资格审查证明材料(正本一份、副本二份，单独密封)：**

1、关于资格的声明函；

2、法定代表人身份证明书（提供复印件并加盖公章）；

3、法定代表人授权委托书原件，投标代表本人身份证复印件（原件随身备查）；

4、提供招标公告第五条资格要求中的相应的佐证材料（提供复印件并加盖公章）：

4.1营业执照副本（提供复印件并加盖公章）；

4.2企业2022年度财务报告(新成立企业可不提供)；

4.3企业2022年度缴纳税收和社会保障资金的记录；

4.4近3年在经营活动中没有重大违法记录的承诺书；

4.5投标人根据招标公告认为需要提交的其他资料。

**三、报价标(正本一份、副本二份，单独密封。不得出现在原件包、资格审查证明材料、商务技术标)：**

1、报价函(格式见附件)；

2、投标报价明细表(如有、格式自拟)。

**四、商务技术标（正本一份、副本二份，不得出现报价。单独密封）：**

1、投标人情况一览表

2、技术部分正负偏离表

**填制正负偏离表，完全响应的，请以空白表列示。不完全响应的，必须在偏离表中列示；列示不全的，视同故意隐瞒。**

3、技术部分、商务部分评标办法中要求提供的全部资料。

4、投标人认为需要提交的其他资料。

**为方便评委评审，请投标人按评标办法中所涉及的事项顺序进行编制，可以**

**补充相关材料。**附件1

**投标人关于资格的声明函**

南通市中央创新区建设投资有限公司：

我公司认真对照招标公告，符合贵方提出的资格要求，自愿参加投标响应，并保证提供的资料文件是准确的和真实的。提供虚假材料的愿意承担相应的法律责任。

我公司承诺投标前3年内没有受各级管理部门的处分或处罚（含其授权服务的子公司、分公司等）。如被事后发现的，我公司同意被取消报名、投标、中标等资格，同时自愿承担违约处理（保证金的10%作为违约金）。

投标人名称（公章）

法定代表人(签字)：

被委托授权人(签字)：

年 月 日

附件2

**法定代表人身份证明书**

先生／女士，现任我单位　　　　　　　职务，为本单位法定代表人，特此证明。

身份证号码：

**注：提供法定代表人的身份证复印件盖公章**

投标人名称（盖章）

年 月 日

**法定代表人授权委托书**

附件3

南通市中央创新区建设投资有限公司**：**

本授权委托书声明：我　　 　（姓名）系　　 　（投标人名称）的法定代表人，现授权委托　　 （姓名）为我公司代理人，以本公司的名义参加本项目的投标活动。代理人在开标、评标、合同招标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。

被委托授权人无转委权。特此委托。

被委托授权人身份证号：

法定代表人签字：

被委托授权人签字：

投标人名称（盖章）

年 月 日

**注：提供被委托授权人的身份证复印件盖公章**

附件4

**投标人情况一览表**

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 企业名称： | | |
| 2 | 总部地址： | | |
| 3 | 当地代表处地址： | | |
| 4 | 电话： | 联系人： | |
| 5 | 传真： | 电子邮件： | |
| 6 | 注册地： | 注册年份： | |
| 7 | 公司资质等级证书号（请附有关证书的复印件） | | |
| 8 | 公司（是否通过，何种）质量保证体系认证（如通过请附相关证书复印件。） | | |
| 9 | 服务经营范围1.；2.……………………… | | |
| 10 | 投标人从事投标项目的年数 | |  |
| 11 | 其他需要说明的情况，可自行添加 | | |

注：本表不是格式化表格，投标人可根据需要，自行添加删除。

投标人名称(公章)：

法定代表人或授权代表（签字）：

日 期：

附件5

**报价函**

南通市中央创新区建设投资有限公司**：**

（一）我方已认真阅读项目的招标文件，并全部响应招标文件中的所有要求。

（二）根据已收到的项目的招标文件，遵照有关规定并根据招标文件的要求，经慎重考虑后，我单位报价为： 元，按招标文件的要求承担本次招标范围内的全部内容。

(三)贵单位的招标文件、中标通知书和本投标文件将构成约束我们双方的合同。

投标人(盖法人章)：

法定代表人或委托代理人(签字或盖章)：

日期：年 月 日

附件6

**技术部分正负偏离表**

（由投标人据实提交，表格不够自行添加）

附件7

货物或服务名称：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 项目 | 招标文件要求 | 投标文件响应情况 | 偏离说明 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**注：**

1**、**投标人提交的投标文件中与招标文件第三部分“项目需求说明”中的商务、技术部分的要求有不同时，应逐条填列在偏离表中，否则将认为投标人接受招标文件的所有要求。

2、“偏离说明”一栏选择“正偏离”、“负偏离”进行填写。正偏离的确认和负偏离的是否响应招标文件，经三分之二评委认定。

3、投标人如果虚假响应，将承担被没收全额投标保证金的风险。

4、投标人若提供其他增值服务，可以在表中自行据实填写。