**数据中心防火墙采购项目的**

**反向竞价说明**

根据《中华人民共和国政府采购法》《浙江省政府采购电子卖场暂行管理办法》等相关规定，现就数据中心防火墙采购项目进行反向竞价，欢迎国内合格的供应商参与反向竞价。

1. **反向竞价项目编号****：**
2. **采购组织类型：反向竞价**

**三、反向竞价项目概况**：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **采购内容** | **数量** | **备注** |
| 1 | 数据中心防火墙采购 | 1 | 本项目最高限价：￥：110000.002.详细需求见附件 |

**四、反向竞价供应商资格要求：**

1、符合政府采购法第二十二条规定的投标人资格条件。

2、未被信用中国（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）列入行政处罚、黑名单、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。

**五、反向竞价响应开始时间：**以“政采云”设定时间为准

**六、反向竞价响应开始时间：**以“政采云”设定时间为准

**七、反向竞价响应截止时间：**以“政采云”设定时间为准

**八、其他事项：**

1、网上自动成交后，需双方确认达成一致结果才为正式成交。

2、如供货商响应中有漏项或者核心技术参数负偏离，采购方有权取消供应商中标资格并重新组织在线招投标。

**九、联系方式：**

采购人名称：温州城市大学

联系人：胡老师，联系方式：88282373

**附件一：采购清单**

**附件二：商务要求**

**附件二：技术要求**

 温州城市大学

 2024年3月28日

**附件一：采购清单**

**编号：**

采购单位名称：**温州城市大学**

1. 项目清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 名称 | 数量（台） | 最高单价（元） | 最高总价（元） |
| 1 | 数据中心防火墙设备 | 1 | 110000 | 110000 |
|  | 合计 |  |  | 110000 |

**附件二：商务要求**

一、供货商必须响应全部技术参数，如有漏项或者技术参数负偏离，采购方有权取消供应商中标资格并重新组织竞价。供应商按照参考品牌进行响应，按照技术要求在预中标3日内提供相关功能证明材料以及向我校信息技术服务中心演示相关设备功能。

二、售后服务及质保。设备验收合格后免费提供3年质保，**中标后3日内提供原厂商保修服务函**。质保期内，供应商应当提供 7×24 小时电话支持服务。供应商接到采购单位保修通知后2个小时内响应，4个小时内需上门服务并排除故障。对于质保期内不能修复的产品/部件，供应商应在24 个小时内免费更换备品备件。

三、供货验收。中标单位应提供运输服务并承担运费，在采购合同签订后10个工作日内派人到采购方指定地点现场交货、安装、调试并完成验收。

报价是指供应商在正确地完全履行合同义务后采购方应支付给供应商所有的货物价款，即货物的供货、包装、运输、装卸、安装调试、验收（含第三方验收）、质保期内软件升级、售后服务、材料税费、辅材费、搬运费、税费（含税货物）以及完成合同所需的一切本身和不可或缺的所有工作开支、政策性文件规定，合同包含的所有风险、责任等相关各项其他可能产生的全部费用。实行固定费用总包干，供应商应根据上述因素自行考虑含入总报价。

四、付款方式。完成验收后，由供货商提供合同金额100%发票，采购方进行一次性付款。

五、其他要求。供应商在响应报价前需仔细评估自身履约能力，谢绝恶意低价、不按要求报价、中标后无故放弃、不按合同履行等违约行为。对出现此类行为的预成交供应商，将依法依规提请政采云平台进行处罚，处罚内容包括停止推送报价信息、禁止报价、协议暂停、罚款、诚信体系中记录不良行为或黑名单等，记入政府采购诚信档案。

**附件三：技术要求**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **标的名称** | **技术指标** | **备注** |
| 1 | 下一代防火墙(AF-FH全行业型号（新）) | **性能要求：**★性能参数：网络层吞吐量≥35G，应用层吞吐量≥20G，并发连接数≥410万，HTTP新建连接数≥18万。硬件参数：规格≥1U，内存大小≥16G，硬盘容量≥256G SSD，电源：冗余电源，接口：支持不低于16千兆电口+6万兆光口SFP+。**产品架构要求**：★产品采用自主知识产权的专用操作系统，应用多核并行处理技术保障产品处理性能，需提供公安部计算机信息系统安全产品质量监督检验中心、中国信息安全测评中心、中华人民共和国国家版权局、公安部信息安全产品检测中心之中任意一家检测机构出具关于“多核并行安全操作系统”的证书或检测报告。**部署方式**：支持路由、透明、虚拟网线、旁路镜像、混合等多种部署方式，适应复杂使用环境的接入要求。**链路聚合**：具备链路聚合功能，将2个或者更多物理链路组合成一个更高带宽的逻辑链路接口，提高链路带宽和链路可靠性。**网络服务**：具备ARP代理功能，对指定地址的ARP请求使用指定接口的MAC地址应答，实现保护内网主机。**地址转换**：支持IPv4／IPv6下NAT地址转换，包括支持源地址转换SNAT，目的地址转换DNAT和双向地址转换双向NAT， 支持一对一、一对多、多对一等多种转换方式。**地域访问控制**：支持基于对象、区域和地域维度设置安全访问控制策略，允许或拒绝特定国家或者地区的对象访问内部网络，保障业务重大时期安全可靠性。 | 1 |
|  |  | **应用识别**：★产品内置应用特征识别库，支持不少于9000种应用规则，支持对游戏、P2P下载工具、聊天工具、网上银行、视频软件、股票软件、木马控制软件等类型应用进行检测与控制。（需提供产品功能截图证明）**流量控制**:★具备基于国家/地区的流量管理功能，提供具有CNAS、CMA等同级别任一官方认证的第三方测试机构关于“国家/地区的流量管理”产品功能检测报告，或提供现场演示环境以证明此项功能满足业务需求。**安全策略管理：**产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。（需提供产品功能截图证明）**DDoS防御**：支持产品支持对ICMP、UDP、DNS、SYN等协议进行DDOS防护，支持IP地址扫描和端口扫描攻击防护。 支持异常包攻击防御，异常包攻击类型至少包括Ping of Death、Teardrop、Smurf、Land、WinNuke等攻击类型。**勒索病毒防御**：★支持勒索病毒检测与防御功能，为保障勒索病毒的防御效果，所投产品需提供具备CMA（中国国家认证认可监督管理委员会）、CNAS（中国合格评定国家认可委员会）认证的第三方权威机构关于“勒索软件通信防护”功能项的产品检测报告；或提供现场演示环境以证明此项功能满足业务需求。**入侵防御**：★产品内置IPS检测引擎，支持口令暴力破解、僵尸网络、恶意软件、服务器与终端漏洞攻击等检测和防护，支持超过10000种特征规则。（需提供产品功能截图证明） 具备僵尸网络检测功能，可基于僵尸网络检测引擎发现主机的异常外联行为，并提供威胁等级和非法外联次数作为举证。**网端云联动**：★具备网端云协同联动功能，提供具有CNAS、CMA等同级别任一官方认证的第三方测试机构关于“网端云协同联动”产品功能检测报告，或提供现场演示环境以证明此项功能满足业务需求。 |  |
|  |  | **策略生命周期管理**：支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便策略的管理和运维。**资产识别**：支持Web服务器自动侦测功能，根据Web服务器在线状态、端口使用状态、Web服务器之间的互访关系生成业务资产列表，同时展示内网资产访问的风险等级。（需提供产品功能截图证明）**用户管理权限**：支持三权分立功能，根据用户权限分为安全管理员、审计员、系统管理员三种角色；**双因素认证**：支持管理员双因素认证，包含用户名/密码和Key等不同方式。**设备联动**：★要求支持学校的安全态势感知平台和终端检测响应平台(EDR)联动处置网络安全事件。 |  |