**关于南京医科大学附属口腔医院 防火墙项目征集潜在供应商的调研公告**

南京医科大学附属口腔医院拟对以下项目进行摸底、调研，公开征集潜在供应商。欢迎符合要求的供应商前来报名。

**一、项目概况**

**项目名称： 防火墙**

**二、资质要求：**

1、响应供应商应具有独立法人资格，营业执照。

2、与本项目相关的特殊资质证照。

**提供有效的证书复印件加盖公章。**

**三、项目基本技术要求（见附件）：**

1、软件部分见附件；

2、请同时提供满足本项目实施要求所需硬件配置清单及技术要求。

**四、请仔细阅读本项目技术参数要求，并提供以下书面材料一式四份。**

1. 本公司满足本项目全部技术参数要求，无疑问。

或

本公司对本项目技术参数有正/负偏离，并附下表表述。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 指标 | 原技术指标 | 正/负偏离 | 原因 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

2、本公司对本项目技术参数有疑问，并附下表表述，标明原技术参数，建议修改内容并阐明原因。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 指标 | 原技术指标 | 建议修改 | 原因 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

1. 该项目人员配置（项目建设及服务团队）

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 姓名 | 所属工种 | 证书 |
| 1 |  |  |  |
| 2 |  |  |  |

1. 与本项目类似的成功案例（合同或中标通知书复印件）
2. 与本项目相关的公司资质证书专利等证明材料。
3. 描述质保期内及质保期后的服务方案。
4. 硬件产品须为合同签订时间一年内出厂，全新、未使用过的原装合格正品，不得使用已停产或拟停产产品，提供承诺书并加盖公章。

**五、 价款的支付方式、时间及条件：**签订合同后，支付合同总价款的30%；乙方完成全部产品安装、调试，正常使用30日后，经甲方验收合格，签署《南京医科大学附属口腔医院验收报告》，凭发票支付合同总价的60%；留合同总价的10%作为本项目的尾款，自甲方支付至90%合同款12个月后，产品运行正常，售后服务良好，无质量、安全和服务问题，经甲方确认，支付合同尾款10%。

**六、报价一览表**

按照硬件、软件进行分项报价，硬件部分应按照设备组成分项报价，软件部分应按照功能模块分项报价。所有价格信息在报价一览表中详细列明，可另行加行。

|  |  |
| --- | --- |
| **项目名称** | **南京医科大学附属口腔医院 项目**  |
| **软 件** |
| **序号** | **产品名称** | **品牌规格型号** | **单位** | **数量** | **单价（元）** | **总价（元）** |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| **硬 件** |
| **序号** | **产品名称** | **品牌规格型号** | **单位** | **数量** | **单价（元）** | **总价（元）** |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| **合计金额** | **人民币（大写） 元****（¥ 元）** | **软件：¥ 元** |
| **硬件：¥ 元** |
| **质保期** | **硬件：** |
| **软件：** |
| **质保期后****维保费用** | **硬件：** |
| **软件：** |
| **项目实施期** |  |

**单位名称（公章）：**

**法定代表人（授权代表）签名：**

 **联系电话（手机）：**

 **年 月 日**

**七、项目调研会议安排：**

时间：2023年11月2日(星期四)下午15:30

**（请各供应商委派商务及技术人员参会，PPT产品介绍时间不超过10分钟）**

地 点：江苏省口腔医院新综合楼十三楼1301会议室

联系方式： 李老师 69593126 69593206

**注： 1. 提供虚假文件一经查实将终止其参与资格。**

 **2. 资料一式四份，加盖单位公章并装订成册，概不退还。**

**附件：南京医科大学附属口腔医院 防火墙 项目要求**

1. 产品不少于16个10/100/1000M以太网电口， 6个SFP+口，支持2个USB口和1个RJ45串口，支持交流冗余电源，2U机箱，网络层吞吐量≥40Gbps，应用层吞吐量≥25Gbps，并发连接数≥420万，每秒新建连接数≥19万，提供不少于三年质保和软件升级，提供不少于2台设备满足双机冗余要求。
2. 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；
3. 产品内置不低于13800种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则。（需提供截图证明并加盖原厂商公章）
4. 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。（需提供截图证明并加盖原厂商公章）
5. 产品支持基于IMAP、FTP、RDP、VNC、SSH、TELNET、ORACLE、MYSQL、MSSQL等应用协议进行深度检测与防护。
6. 产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过128万种，可识别主机的异常外联行为。（需提供截图证明并加盖原厂商公章）
7. 产品支持云情报网关技术，通过全球超过30+pop节点，实现对威胁流量进行实时检测&拦截，所有流量在转发前均经过威胁情报的检测并已明确结果，实现恶意流量在转发前被阻断，保护资产安全。（需提供截图证明并加盖原厂商公章）
8. 产品支持X-Forworded-For字段检测，并对非法源IP进行日志记录和联动封锁。
9. 产品内置超过4580种WEB应用攻击特征，支持对跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护。（需提供截图证明并加盖原厂商公章）
10. 产品支持勒索病毒检测与防御功能，需提供产品功能截图证明，并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“勒索病毒”的证书或检测报告证明功能有效性。。
11. 产品支持Cookie攻击防护功能，并通过日志记录Cookie被篡改。所投产品必须提供具备CMA认证的第三方权威机构关于“Cookie攻击防护”功能项的产品检测报告。（需提供截图证明并加盖原厂商公章）
12. 产品支持与现网中态势感知平台产品联动，将本地防火墙产品产生的安全日志等数据上报至态势感知平台，并在态势感知平台进行威胁展示。
13. 产品支持安全策略有效性分析功能，分析内容至少包括策略冗余分析、策略匹配分析、风险端口风险等内容，提供安全策略优化建议。
14. 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资质。（需提供截图证明并加盖原厂商公章）
15. 要求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，安全工程类不低于一级。（需提供截图证明并加盖原厂商公章）