# 采购清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **基本参数** | **数量** | **单位** |
| 1 | 防火墙1 | 详见“产品技术要求” | 1 | 套 |
| 2 | 防火墙2 | 详见“产品技术要求” | 2 | 套 |
| 特别说明：（1）投标产品的质量性能指标及服务内容不得低于参考品牌型号的质量性能指标和服务内容。带★号的指标为重要指标，不接受负偏离；（2）所投设备（包括所有元部件）均为原厂生产，设备最终用户名为：宁波市海曙区南门街道社区卫生服务中心（原厂800电话可查），投标时提供原厂质保函；（3）投标企业必须是在中华人民共和国境内注册的独立企业法人，投标商必须在宁波市内有常设的售后服务机构（投标时附营业执照）；（4）本项目为交钥匙工程，为实现项目设备及软件正常运行所需配套的辅助材料及设备或软件，须由投标人自行考虑并计入报价。项目实施涉及的设备、软件及其他辅助材料的供货安装、系统集成、验收及3年质保期售后服务。（5）投标人必须配有较强的专业技术队伍，能确保现场实施和售后现场服务响应，投标人必须能保证在接到用户故障服务请求后2小时内到达现场服务（或远程响应）。（6）投标时提供公司信息、工商营业执照复印件、产品报价单、法人授权书、产品彩页、产品功能证明、售后服务承诺书。**注：投标单位须根据上述要求在竞价文件中提供相应的文档，若没有按照相关要求提供的，则视为无效标处理。** |

# 二、产品技术要求

**1、防火墙1**

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| ★性能要求 | 产品必须采用通过中国信息安全测评中心安全可靠测评的国产CPU和国产操作系统。设备最大吞吐量≥6Gbps，最大并发连接数≥300万，每秒新建连接数≥5万，提供三年IPS、防病毒、WEB防护模块及升级服务。 |
| 硬件要求 | 双电源，内存≥8GB，硬盘≥2TB HDD。≥8个千兆电口(含≥2组电口Bypass），≥4个千兆光口，≥2个接口扩展槽 |
| ★部署模式 | 支持路由模式、交换模式、旁路模式、虚拟网线工作模式；部署模式切换无需重启设备，需与现有APT设备进行联动，当发现威胁进行自动阻断。 |
| NAT | 支持IPv4/IPv6双栈协议的源地址转换、目的地址转换、双向NAT、NAT64等地址转换 |
| DNS | 支持DNS代理功能。支持DNS解析动态缓存，缓存信息包括但不限于域名、CName、IP和TTL |
| 路由支持 | 支持静态路由、动态路由、ISP路由；支持基于入接口、源地址、目的地址、服务的策略路由 |
| 访问控制 | 支持一体化安全策略：可基于安全域、MAC地址、IP地址、服务、时间、用户、应用等属性，配置防病毒、入侵防御、内容过滤、URL过滤、文件过滤、Web防护、SSL解密、弱密码防护、防暴力破解、会话老化时间等高级访问控制功能；支持图形化整体策略展示效果。 |
| ★入侵防御 | 系统预定义超过11000条主流攻击规则，包含对应IPS规则的级别、防护对象、操作系统、CVE编号等详细信息。（提供截图与第三方检测报告证明） |
| 病毒防护 | 系统定义最大超过800万条主流病毒检测规则。 |
| Web防护 | 支持独立的Web防护模块，系统定义超过4500条WAF规则防护功能，支持常规HTTP漏洞、SQL注入、组件、CMS、WebShell和XSS等类型的Web防护；支持HTTP协议的URL、Method、Referer、User-Agent、Cookie、URL-args等字段的等于、不等于、包含、不包含、正则等多种匹配方式的访问控制。 |
| 资产指纹库 | 系统定义超过20万条资产指纹库，可识别的主机资产类型包括但不限于通用主机、移动电话、防火墙、网络摄像机、温湿度变送器、呼叫中心、云安全等；可识别的主机资产操作系统包括但不限于Windows，Linux，MAC OS，Android，IOS等；可识别的软件资产类型包括但不限于WEB组件、WEB中间件等WEB应用，Oracle、Hive等数据库，电脑游戏、图像设计等桌面软件以及各类网络协议等；可识别的软件包括但不限于CrushFTP httpd，Android VNC Server等。 |
| 漏洞扫描 | 支持产品内置的默认模板以及自定义模板进行漏洞扫描，可扫描出漏洞名称、漏洞级别、漏洞描述、CVE-ID、CNNVD-ID等信息；支持查看资产关联的漏洞信息，并跳转到详情。 |
| ★威胁情报 | 威胁情报检测能力：支持检测C&C、勒索软件、僵尸网络、挖矿软件、矿池地址等安全攻击类型。（提供第三方构检测报告证明） |
| 其他防护 | 安全模式支持智能模式和普通模式。在普通模式下，安全引擎处理网络报文遇到资源不足时会将报文直接丢弃，会影响网络转发；在智能模式下，安全引擎将尽可能的处理网络报文，但不影响网络转发。 |
| 提供对控制策略、上网认证策略、带宽策略、策略路由、源NAT等策略的策略分析，可分析并展示问题策略数量以及所占百分比、问题策略详情、策略宽松度分布情况，简化运维工作。 |
| ★售后服务支持 | 提供不少于三年质保服务，包含但不限于硬件保修、系统升级等服务内容，投标时提供原厂出具的承诺函。设备最终用户为海曙区南门街道社区卫生服务中心。 |

**2、防火墙2**

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| ★性能要求 | 产品必须采用通过中国信息安全测评中心安全可靠测评的国产CPU和国产操作系统。设备最大吞吐量≥10Gbps，最大并发连接数≥400万，每秒新建连接数≥20万，提供三年IPS、防病毒、WEB防护模块及升级服务。 |
| 硬件要求 | 冗余电源，内存≥16GB，硬盘≥2TB HDD。≥10个千兆电口(≥4组电口Bypass），≥8个千兆光口，≥2个接口扩展槽 |
| ★部署模式 | 支持路由模式、交换模式、旁路模式、虚拟网线工作模式，部署模式切换无需重启设备，需与现有APT设备进行联动，当发现威胁进行自动阻断。 |
| NAT | 支持IPv4/IPv6双栈协议的源地址转换、目的地址转换、双向NAT、NAT64等地址转换 |
| DNS | 支持DNS代理功能。支持DNS解析动态缓存，缓存信息包括但不限于域名、CName、IP和TTL |
| 路由支持 | 支持静态路由、动态路由、ISP路由；支持基于入接口、源地址、目的地址、服务的策略路由 |
| 访问控制 | 支持一体化安全策略：可基于安全域、MAC地址、IP地址、服务、时间、用户、应用等属性，配置防病毒、入侵防御、内容过滤、URL过滤、文件过滤、Web防护、SSL解密、弱密码防护、防暴力破解、会话老化时间等高级访问控制功能；支持图形化整体策略展示效果。 |
| 入侵防御 | 系统预定义超过11000条主流攻击规则，包含对应IPS规则的级别、防护对象、操作系统、CVE编号等详细信息。 |
| 病毒防护 | 系统定义最大超过800万条主流病毒检测规则。 |
| Web防护 | 支持独立的Web防护模块，系统定义超过4500条WAF规则防护功能，支持常规HTTP漏洞、SQL注入、组件、CMS、WebShell和XSS等类型的Web防护；支持HTTP协议的URL、Method、Referer、User-Agent、Cookie、URL-args等字段的等于、不等于、包含、不包含、正则等多种匹配方式的访问控制。 |
| ★资产指纹库 | 系统定义超过20万条资产指纹库，可识别的主机资产类型包括但不限于通用主机、移动电话、防火墙、网络摄像机、温湿度变送器、呼叫中心、云安全等；可识别的主机资产操作系统包括但不限于Windows，Linux，MAC OS，Android，IOS等；可识别的软件资产类型包括但不限于WEB组件、WEB中间件等WEB应用，Oracle、Hive等数据库，电脑游戏、图像设计等桌面软件以及各类网络协议等；可识别的软件包括但不限于CrushFTP httpd，Android VNC Server等（需提供截图证明）。 |
| 漏洞扫描 | 支持产品内置的默认模板以及自定义模板进行漏洞扫描，可扫描出漏洞名称、漏洞级别、漏洞描述、CVE-ID、CNNVD-ID等信息；支持查看资产关联的漏洞信息，并跳转到详情。 |
| 威胁情报 | 威胁情报检测能力：支持检测C&C、勒索软件、僵尸网络、挖矿软件、矿池地址等安全攻击类型。 |
| 其他防护 | ★安全模式支持智能模式和普通模式。在普通模式下，安全引擎处理网络报文遇到资源不足时会将报文直接丢弃，会影响网络转发；在智能模式下，安全引擎将尽可能的处理网络报文，但不影响网络转发。（提供第三方机构检测报告证明） |
| 提供对控制策略、上网认证策略、带宽策略、策略路由、源NAT等策略的策略分析，可分析并展示问题策略数量以及所占百分比、问题策略详情、策略宽松度分布情况，简化运维工作（需提供截图证明）。 |
| ★售后服务支持 | 提供不少于三年质保服务，包含但不限于硬件保修、系统升级等服务内容，投标时提供原厂出具的承诺函。设备最终用户为海曙区南门街道社区卫生服务中心。 |

# 三、实施进度、测试与验收

1)投标人有责任检查安装现场是否符合产品安装条件。

2)投标人应承担投标软件的安装、测试和有关配置工作，进行实际的测试。

3)投标人应全力与采购人及运维单位配合，根据采购人的详细需求，提交实施方案得到采购人确认后实施，保证系统按时、正常地投入运行。

4)产品实施过程中，如果牵涉到与第三方产品集成工作，投标人应与集成商及其他供应商通力合作，并提供必要的技术支持。

5)系统验收合格的条件必须至少满足以下三个要求：试运行时性能满足合同要求；性能测试和试运行验收时出现的问题已被解决。

# 四、商务要求

1、本项目招标所有参数作为实质性条款必须满足，否则视为无效投标。禁止不符合参数要求供应商恶意低价报价，造成采购单位工期进度的报上级部门反映该情况，责任由供应商承担。本项目涉及安装调试及后期维保，要求提供上门送货等本地化服务，拒绝快递邮寄。

2、采购人若存疑或其他投标人质疑时，中标人在成交确认前需提供相关检测报告原件、产品参数官网截图及厂家质保承诺函等资料（按招标规格参数内要求的提供），进行核查。采购人若有疑问时投标人在成交确认前需提供主要设备样品（设备应由采购人指定）逐项演示产品功能并测试，测试方法包括与询价单参数进行核对、采用专业工具进行测量，对样品存在质量、安全隐患、不符合询价单要求、则取消询价结果。测试造成的费用或损失由供应商自行承担，如果测试结果不符合要求所有测试费用由供应商承担，并上报上级财政部门及政采云处理，追究其相关责任。请供应商在报价前仔细评估自身履约能力，按照文件要求进行报价。如有违规违约行为，将根据在线询价违约处理规则，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、禁止报价等，并记入政府采购诚信档案。

3、采购人若有疑问时可要求中标人提供5%的履约保证金汇至采购人指定的财政账户，直至服务期满后没有任何质量问题无息退还。

4、验收合格后支付全部货款，一旦发现提供产品技术参数不达标，采购人有权不支付货款。

5、项目验收：正式供货阶段验收，按采购人的技术要求、商务要求对所供商品进行全面验收。验收过程发现交付的货物品种、型号、规格、技术参数、质量、安全要求不符合询价单要求或合同规定的，或货物质量低于样品（采购人有疑问是要求提供的测试设备）的，严格要求中标供应商进行替换。为确保业主正常的开展日常工作，在中标供应商未提供符合要求的商品之前，被替换的产品由业主单位免费使用，中标供应商不得撤回。未能提供符合要求的商品，则履约验收不合格，采购人有权拒绝支付货款，并视为中标供应商将前期提供的不合格产品免费赠予本单位。