**项目采购需求**

**一、项目基本情况**

1、项目名称：中山市中医院防火墙采购项目

2、项目内容：医院拟采购两台协作区域边界防火墙，以满足信息网络安全需要。

3、项目上限价：￥260000元，超过采购上限价的属于无效响应。

4、供货期：合同签订后30天

5、报价：总价包干，报价应包括硬件采购、安装调试、验收、培训、售后服务、各种税费及合同实施过程中的不可预见费用等。

**二、技术参数要求**

|  |  |  |
| --- | --- | --- |
| 序号 | 项目名称 | 技术要求 |
| 1 | 硬件要求 | 规格≥1U、内存≥16G、硬盘容量≥480GB SSD、冗余电源、接口≥16千兆电口+6万兆光口SF |
| 2 | 性能要求 | 网络层吞吐量≥35G、应用层吞吐量≥20G、防病毒吞吐量≥3.5 G、IPS吞吐量≥3G、全威胁吞吐量≥2G、并发连接数≥800万、HTTP新建连接数≥18万、IPSec最大隧道数≥4000、IPSec VPN吞吐量≥1.2G |
| 3 | NAT功能 | 支持源地址转换SNAT、目的地址转换DNAT和双向NAT等功能， 支持一对一、一对多、多对一等形式的NAT |
| 4 | 访问控制 | 支持多维度安全策略设置，可基于时间、用户、应用、IP、域名等内容进行安全策略设置 |
| 5 | 应用控制 | 产品内置应用特征识别库，支持不少于5000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。 |
| 6 | 流量控制 | 基于线路、IP地址、上下行通道进行流量控制，保障核心业务带宽正常使用 |
| 7 | 防病毒 | 产品支持对压缩病毒文件进行检测和拦截，压缩层数支持15层及以上。支持多种专业反病毒厂商的病毒特征库。病毒特征库规模不少于160万种+云端百亿级威胁情报，突破传统防火墙本地规则限制。 |
| 8 | 入侵防御 | 产品预定义漏洞特征数量不低于16000种，支持在产品漏洞特征库中以漏洞名称、漏洞ID、漏洞CVE标识、危险等级和漏洞描述等条件快速查询特定漏洞特征信息，支持用户自定义IPS规则；支持僵尸主机检测功能，产品预定义特征库不低于128万种，可识别主机的异常外联行为 |
| 9 | Web安全防护 | 支持对常见Web应用攻击防御，攻击类型至少包括跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等类型，产品预定义Web应用漏洞特征库不低于4580种；支持对请求报文头的X-Forward-For字段检测，并对非法源IP进行日志记录和联动封锁；支持针对地址、应用设置WAF白名单，支持攻击规则搜索以及自定义 |
| 10 | 会话控制 | 支持基于IP对象的会话控制策略，实现并发连接数的合理限制 |
| 11 | 访问控制策略 | 支持多维度安全策略设置，可基于时间、用户、应用、IP、域名等内容进行安全策略设置 |
| 12 | 地域访问控制 | 支持与国家位置信息结合设置安全策略，识别流量发起的国家或地区的位置信息，根据流量发起的国家或地区的访问位置信息实现对不同区域访问的差异化控制 |
| 13 | URL分类过滤 | 支持全面的URL分类库，针对网站类别实现细粒度管控，杜绝非法、违规网站的访问行为 |
| 14 | 文件过滤 | 支持对文件传输行为进行安全过滤，支持基于上传、下载、双向的文件内容过滤，内容过滤类型至少支持网页、脚本、压缩文件、图片、可执行文件、适配、文本等常见文件类型 |
| 15 | 受保护业务  账号安全 | 支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生；支持文件目录防护功能，通过对用户账号进行认证，对网站内容的修改行为进行合法性控制 |
| 16 | 管理员账号权限管控 | 支持三权分立功能，根据管理员权限分为安全管理员、审计员、系统管理员三种角色 |
| 17 | 认证 | 支持管理员双因素认证功能，用户通过用户名/密码和Key等不同方式登陆产品管理界面 |
| 18 | 网管协议 | 支持标准网管协议SNMP V1、SNMP V2、SNMP V3、SNMP Trap |
| 19 | 入侵攻击防御 | 产品支持僵尸主机检测功能，产品内置僵尸网络特征库不低于128万种，可识别主机的异常外联行为。 |
| 20 | 业务资产管理 | 支持被动监测和主动扫描两种资产识别方式，可梳理离线资产、高危端口开放、冗余端口等安全风险；同时通过可视化的拓扑关系图，直观地展示资产和资产之间的访问关系、访问细节协议端口等信息 |
| 21 | 其他 | 所投产品符合CESI-WA-20240101《网络安全技术 网络型防火墙互联互通接口内容和格式》相关要求 |

**三、质量要求**

1、供应商提供的货物质量必须符合国家相关标准、行业标准及项目要求。

2、供应商提供的货物为厂家原装正品、全新产品，无侵权行为、表面无划损、无任何缺陷隐患，在中国境内可安全合法使用。

3、供应商保证对其出售的设备享有所有权或处分权，并且没有法律、法规禁止或限制出售的情形。同时，供应商出售的设备也没有侵犯第三人的知识产权和商业秘密等权利。如采购人使用该设备构成上述侵权，供应商承担全部相关责任。

4、供应商对由于设计工艺或材料的缺陷所发生的任何故障负责，所需费用由供应商承担。

**四、服务要求**

1、供应商须有专人负责货品供应事宜，包括配送、安装调试、售后服务等。

2、供应的货物如在拆封使用时发现有质量问题，成交供应商应给予退货或更换。

3、产品质保期、运维支持、软件升级须不少于三年，若国家或生产厂家对该设备质量保证期的规定高于本项目要求，则按国家或生产厂家的规定执行。

4、质保期内供应商提供“包退、包换、包修”的质量“三包”服务，一切维修费用、备品备件费用均由供应商免费提供。

5、投保期内，供应商提供技术支持和指导，故障情况下的现场问题解决，包括但不限于兼容性问题的微码升级、固件升级等。

6、售后服务响应时间：供应商应提供7\*8小时的技术咨询和故障受理服务，在质保期内，供应商响应时间为30分钟内，若确需到达现场处理的，到达现场时间为24小时内。

7、安装调试期间，不能影响医院网络系统的正常使用，否则造成的一切责任事故由供应商负责。

**五、验收与结算**

1、供应商将货物送到采购人指定地点，安装调试后按国家相关标准、行业标准及项目要求进行验收。

2、供应商需将所有设备的用户手册、保修手册、有关单证资料及配备件、随机工具等交付给采购人。

3、供应商须提供免费的培训服务，直接采购人熟悉设备操作及日常保养为止。

4、项目验收合格，凭供应商开具的全额发票和验收资料，采购人于60个自然日内支付合同款项；如中标人为中小企业，按中小企业相关法律法规或政策执行。