附件

**报价函**

致中共淮安市纪律检查委员会:

我单位已认真阅读本项目的询价文件，经仔细研究后，现决定参加本项目的询价采购活动。

按照询价文件中规定各项要求，我方愿以（大写） 元（RMB￥ 元）的总报价提供所需货物和服务。本项目的明细报价如下:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 项目名称 | 数量 | 技术参数要求 | 所报品牌及型号 | 是否响应 | 总价 |
| 防火墙 | 1台 | 产品要求：信创目录产品  1.配置要求：标准2U机箱，冗余电源，网络层吞吐量≥15G，并发连接≥550万，每秒新建连接数≥16万，管理接口≥1个，≥8个10/100/1000M自适应电口，≥8个千兆光口，≥1个Console口，**配置三年AV防病毒升级许可**  2.系统结构：国产化硬件平台、国产化安全操作系统及功能软件构成；  3.路由交换：支持RIP、OSPF、BGP4、策略路由，支持根据入接口、源/目的IP地址、协议、用户、应用、选路算法、探测等多种条件设置策略路由；  4.DNS Doctoring：支持DNS Doctoring功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡；  5.支持访问控制、域名控制，支持行为分析。  6.DDOS防御：支持针对IP、ICMP、TCP、UDP、DNS、HTTP、NTP等协议进行DDOS防护；支持DNS FLOOD防护，能对DNS QUERY FLOOD、DNS REPLY FLOOD、DNS投毒、DNS格式等攻击提供DNS REPLY源认证、源限速、目的限速、域名限速等综合防护手段；  7.支持HTTP DDOS防护，8.支持NTP流量检测清洗，能对NTP REQUEST FLOOD、NTP REPLY FLOOD等攻击进行检测并提供基于NTP请求限速、NTP响应限速、源认证、会话认证的防御策略；  9.支持根据DOS/DDOS攻击行为自动添加动态黑名单功能；包括流量统计、威胁统计、三权分立、病毒过滤：支持对HTTP/SMTP/POP3/FTP/IM等协议进行病毒防御，病毒特征库规模超过200万；  10.内置邮件安全防护功能，支持邮件过滤、邮箱防暴力破解、邮件泛洪攻击防护、邮件黑、白名单检测；   * 所投安全产品具备公安部颁发的《计算机信息系统安全专用产品销售许可证》，生产厂商具有“国家信息安全服务（安全开发类）资质” 具备CNNVD（中国国家信息安全漏洞库）一级支撑单位   提供原厂商三年免费软件更新服务、产品保修服务，3年7x24技术支持服务，原厂安装服务。 |  |  |  |
| 专用型安全审计产品（上网行为管理） | 1台 | 信创目录产品，内存: ≥16GB，硬盘: ≥2TB，网络接口 ≥1个，管理口≥1个，HA口≥8个，千兆电口≥4个，千兆光口≥4个和2个万兆光口  整机规格:2U机箱，默认带36个月硬件维保。产品能够对网络环境中的通讯协议(HTTP、FTF、TELNET、SMTP/POP3等)进行审计和分析:提供按条件查询审计记录、统计分析、潜在危害分析、事件分级和告警响应等功能。  1.设备部署：设备可直路串联在一条或多条原有网络线路上，进行行为分析、审计和控制。不改变网络拓扑，路由表项。支持设备模式选择，可以设置为Portal模式实现Portal服务器功能。  2.安全管理：持配置病毒查杀策略，检查网络中传输的文件是否是病毒。支持记录日志、病毒过滤；支持恶意URL访问日志查询，日志应包含时间/用户/终端类型/内外网IP地址和端口号/MAC/网址/网站类型/访问控制类型。支持失陷主机检测日志查询，日志应包含时间/用户/终端类型/内外网IP地址和端口号/MAC/类别/威胁情报/失陷威胁简介/访问控制类型。  3.应用管理：应用协议库包含的应用数量不低于6000种，应用规则总数不低于10000种。当用户的网页访问被网页浏览策略封堵时，用户如果发现分类错误能够在页面中向管理员进行反馈；管理员可查看用户反馈的分类错误，并可以选择向服务器反馈；设备内置常用应用标签，分类至少包含内容外发风险、期货行业合规、证券行业合规、高安全风险、影响工作效率、消耗带宽6大类；能够基于发件人、收件人、主题、内容、附件名维度进行过滤、记录、告警；能够支持SSL加密的SMTP邮件审计。  4.文件管理：支持FTP文件上传管理，可根据文件大小、文件名、扩展名、传输方向、内容关键字进行审计过滤；支持对帐号、命令的审计与过滤。  支持对流行应用客户端外发文件进行关键字过滤和封堵  5.流量管理：多级虚拟通道，可以将物理带宽分成至少7级虚拟通道，合理分配物理带宽资源。支持在设置流量策略后，可根据整体线路空闲情况，允许流量通道内的流量突破策略上限，以提升带宽的高使用率；空闲值可自定义  6.支持基于连接数进行流量管理，可以每个人的并发/新建连接数量进行控制。  共享接入：可基于源IP、用户、位置、终端台数、PC台数、移动台数、阻塞时间和动作，配置多条共享接入策略。  7.支持配置禁用PC热点开启功能。禁用时PC仍可以使用网络，但是无法通过随身wifi或笔记本自带功能创建热点。  8.用户管理：支持本地、LDAP、Radius、邮件认证方式的WEB认证。支持在界面上通过配置，将一台设备作为独立的认证服务器配合审计设备使用，提升认证性能。可以建立认证页面与多个认证跳转成功页面，供不同的Web认证策略引用，并支持用户完全自定义。  9.日志统计与报表：支持上网行为分析报表、网络带宽分析报表、合规分析报表、效率分析报表、安全分析报表。支持通过FTP和SFTP方式将日志导出到指定服务器，日志支持SSL加密和ZIP压缩，支持自定义导出数据的时间段和数据定时上传的频率。支持定义导出日志数据的范围、用户、位置和工具。  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。具备国家计算机网络应急技术处理协调中心颁发《CNCERT应急服务支撑单位 》。  提供原厂商三年免费软件更新服务、产品保修服务，3年7x24技术支持服务，原厂安装服务。 |  |  |  |

供应商名称（加盖公章）:

供应商联系人:

联系电话:

报价时间: 年 月 日