报价单及有关承诺、说明

**采购人：**

我单位愿意按照本询价文件（ 盐城市亭湖高级中学校园网络升级维护）的要求和下面的报价提供所需商品和服务，并保证所供商品为原厂原配产品。

一、产品报价单 货币单位：人民币元

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 采购号 | 采购商品 | 品牌 | 型号 | 配置参数相关说明（可附页） | 数量 | 投标单价 | 投标金额 | 不同于项目需求的说明（技术参数、商务条款偏离情况）（可附页） |
| 1 | 第二代防火墙 | 网神 | NSG-1260-Y1 |

|  |
| --- |
| 多核AMP+架构，网络处理能力4G，并发连接≥140万，每秒新建连接5万/秒，1U机箱，单电源，标准配置6个10/100/1000M自适应电口及2个SFP插槽，1个Console口，下一代防火墙系统软件，支持200条VPN隧道，支持控制、URL过滤、病毒防护、入侵防御功能 |
| **性能要求：** |
| 1.支持路由、透明、交换、旁路以及混合模式接入，满足复杂应用环境的接入需求； |
| 2.支持物理子接口技术，可以虚拟多个逻辑接口（不依靠vlan区分）；聚合模式（Channel模式）支持三种：轮询、热备、802.3ad；802.3ad方式支持3种负载算法：根据源目的mac组合、根据mac和ip组合、根据ip和TCP/UDP端口组合 |
| 3.支持DHCP地址绑定（根据MAC地址静态分配IP地址）；支持DHCP Server、DHCP Client和DHCP中继功能； |
| ★4.支持DNS透明代理，防火墙收到客户端DNS请求报文时，防火墙会将请求报文中的DNS地址替换为防火墙指定的代理DNS地址，帮助其实现DNS解析 |
| 5.支持使用命令对策略路由默认优先级进行调整 |
| 6.支持基于权重的路由负载均衡，算法支持：源地址目的地址哈希、轮询、源地址哈希、目的地址哈希、源地址轮询、备份、随机、流量均衡、最优链路带宽负载、最优链路带宽备份、时延负载、跳数负载 |
| 7.支持静态路由，支持策略路由，支持对称路由；支持ISP路由，并支持手动导入；支持动态路由协议RIPv1/v2、OSPF、BGP； |
| 8.支持IPv6地址配置，支持IPV6手动及自动的IP/MAC探测及绑定，支持IPV6的本地认证；支持IPV6下静态路由及策略路由； |
| 9.支持基于源目的IP地址、源目的安全域、VLAN ID、MAC地址、时间、用户、地理区域、服务协议及应用等多种方式进行访问控制；支持通过一条安全策略配置应用控制、入侵防护、URL过滤、病毒检测、内容过滤、网络行为管理等高级访问控制功能，且无需编辑即可直观审计策略配置 |
| 10.支持八种会话长连接自定义设置，每种长连接可以被任意安全策略引用，实现不同的业务、不同的会话保持时长最长可达50天 |
| 11.支持按源目的IP、源目的接口、用户、地理区域及应用进行流量排名，并显示流量统计 |
| 12.支持全面的NAT转换能力，支持对源目的地址、端口的转换；包括一对一，一对多，多对一，多对多地址转换方式 |
| ★13.支持FULL\_CONE和SYMMETRIC两种类型的转换方法，默认为SYMMETRIC |
| 14.支持基于优先级的链路备份，具有备援网关功能 |
| 15.支持基于web的无客户端方式用户认证；在使用web认证客户端时支持NAT探测； |
| 16.实现HTTP、FTP、POP3、SMTP、IMAP五种应用协议的双向内容过滤，支持预定义敏感信息库及自定义敏感信息库两种方式进行敏感信息定义，支持阻断及日志两种处理动作； |
| 17.支持自定义添加关键字，并设置每一个关键字的权重值。当命中的关键字权重相加超过警戒值之后，将会触发内容过滤策略，数据会依据内容过滤策略的动作判断是允许还是拒绝 |
| 18.支持根据IP地址、用户、服务、应用、时间等信息划分虚拟QoS通道进行带宽管理；支持QoS配置向导，支持多层级调度类嵌套，支持优先级设置实现差分服务； |
| 19.支持对应用层 Flood攻击进行五种处理动作：警告、阻断、普通防护、增强防护及授权服务器防护；支持局域网广播防护，支持全局配置的局域网广播防护及基于二层接口的局域网广播防护，可以防止局域网内广播和多播数据包泛滥，保障网络正常通信 |
| 20.支持对拒绝服务、缓冲区溢出、恶意扫描、木马后门、病毒蠕虫、僵尸网络、跨站脚本、SQL注入、WEB攻击等的防御； |
| 21.支持病毒云查杀（要求提供截图） ；支持通过与终端安全管理系统联动及木马云查杀功能生成日志或者动态策略。生成的木马专项查杀动态策略可以在数据被监测携带木马时，根据动态策略配置阻断数据或者记录日志，IPS特征库不少于3000条特征值 |
| 22.支持对拒绝服务、缓冲区溢出、恶意扫描、木马后门、病毒蠕虫、僵尸网络、跨站脚本、SQL注入、WEB攻击等的防御，具备针对DNS、FTP、ICMP、IMAP、SQL、NNTP、POP、SMTP、SNMP等协议类型的入侵检测与防御 |
| 23.支持基于防护类型及防护级别的预定义IPS模板；基于行业类型特点的预定义URL模板 |
| ★24.防火墙动态策略功能，可以通过与入侵防护策略、防弱口令扫描、威胁情报中心、终端安全管理系统的联动，生成动态策略信息，根据用户在基本配置中配置的动态策略动作，命中动态策略的数据将会被阻断或者记录日志 |
| 25.支持针对FTP、SMTP、POP3、IMAP、MYSQL协议防弱口令扫描功能，可以帮助用户记录或者拦截网络中猜测FTP用户名密码，邮件用户名密码的行为。并支持生成动态策略，下发给防火墙，再次受到相同攻击时，用户可以选择禁止还是允许口令猜测的行为 |

 | 1 | 50000 | 50000 | 无偏离 |
| 2 | Web应用防火墙 | 实茂 | WAF-2610 | 产品采用1U专用机架式硬件设备，系统硬件为全内置封闭式结构,非NGFW、NGAF等下一代防火墙或UTM安全网关产品，自动学习并构建网站的URL模型，禁止违反现有模型的尝试行为，支持更新、修正现有URL模型，IPv6协议通过和防护，支持解析通过代理服务器访问用户的真实IP地址，默认支持X-Real-IP或X-Forwarded-For字段的值作为真实来源IP地址，同时支持用户自定义字段名称。支持用户自定义防护策略集，针对不同的来源/目的IP，目的URL选择不用的策略集。提供高度灵活的自定义规则向导，适用于高级用户，支持超长报文组包（默认30M），支持对恶意扫描行为开启防扫描功能，用户可自定义防护等级，支持木马上传日志，记录上传时间，源地址，目的地址，目的URL，拦截原因。支持将木马文件直接下载至本地进行人工分析。支持**网页篡改防护，支持数据库防篡改，**支持敏感关键字过滤，用户可自定义关键字内容，记录登陆过程中使用的弱密码，检测网站的备案情况，对于通过备案网站放行，未通过备案禁止访问，**防CC攻击防护，抗拒绝服务攻击，**支持端口汇聚（Trunk），显著提高设备间的吞吐能力，支持VLAN解码，在Trunk线路上部署并提供防护，统计每天访问所有站点或某个站点的地域统计，并以地理热点分布图的形式体现。统计每天访问所有站点或某个站点的浏览器类型和比例，并以图表方式体现。统计每天访问所有站点或某个站点的操作系统类型和比例，并以图表方式体现。内置bypass模块，设备故障直接切换到bypass模式。 | 1 | 80000 | 80000 | 无偏离 |
| 3 | 日志审计系统 | 实茂 | 200AH | 标准机架式硬件设备，无需在目标系统上安装任何软件；产品功能的实现无需额外增加服务器等设备。要求系统能够稳定运行，系统应用程序能够提供持续稳定的服务。支持集中和分布式部署、集群部署、热扩容，采用旁路接入模式，设备部署不影响原有网络结构。支持**资产管理，**对日志格式进行标准化操作时，将不破坏原始日志内容。标准化自动识别系统类型至少达到200种，系统从不同设备或系统中所获得的各类日志、事件中抽取相关片段准确和完整地映射至安全事件的标准字段，日志清洗后的标准化字段粒度至少达到90个字段。对安全事件重新定级。能根据统一的安全策略，按照安全设备识别名、事件类别、事件级别等所有可能的条件及各种条件的组合对事件严重级别进行重定义，系统能够将标准格式的事件写入存储设备，系统的标准化策略具备良好的可扩展性，可通过配置文件或界面实现管理功能，支持不同设备相同IP的日志识别。支持**日志处理，**系统需具有归并技术，安全事件收集代理会在一段时间内比较收到的安全事件，如果安全事件相同，则只需发送一条安全事件，该安全事件应包括安全事件详情及该安全事件发生的次数，这样可以减少安全事件通信量，支持**实时监控、日志查询、关联策略，**为了挖掘不同类型、来源于不同设备或系统的日志或安全事件之间可能存在的关联关系，系统提供了GUI方式的关联规则设置功能，关联的类型包括基于规则和基于统计的，支持基于因果式的状态关联分析，支持显示审计事件分类统计列表，根据审计策略名称、审计事件类型、被审计人员、目标设备地址四个维度展现。提供可视化方式进行策略制定。可通过事件的任意字段制定规则创建策略。支持告警响应联动防火墙等安全设备。系统提供全文检索功能。能对系统内的对象提供全文检索功能，对于海量数据的检索可限定检索时间段（主要针对安全事件）。全文检索提供一个输入栏，需要置顶，在任何页面都能够看到。包括报表内置实例管理和报表任务管理。支持根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，审计员只负责查看相关的审计结果及告警内容；日志员只负责完成对系统本身的用户操作日志管理。 | 1 | 80000 | 80000 | 无偏离 |
| 4 | 软件版Web应用防火墙 | 实茂 | 无 | 与防火墙同品牌专业网站防护软件，可深度解析http协议，可防护Sql注入，xss，命令执行等常见应用层攻击。 | 10 | 2000 | 20000 | 无偏离 |
| 5 | 短信 | 移动 | 无 | 免费提供100000条短信服务 | 1 | 0 | 0 | 无偏离 |
| 合计人民币（大写）： 贰拾叁万 小写：230000 |
| 供货期限：合同签定后 20个（工作日或日历）日内交货并安装调试完毕。 |

二、详细方案、承诺及说明：

为甲方提供免费培训服务，并指派专人负责与甲方联系售后服务事宜。主要培训内容为货物的基本结构、性能、主要部件的构造及处理。

所购货物按乙方承诺24小时内解决故障。保修期内，负责对其提供的货物整机进行维修和系统维护，不再收取任何费用，但不可抗力（如火灾、雷击等）造成的故障除外。

若货物故障在检修8工作小时后仍无法排除，我单位在24小时内免费提供不低于故障货物规格型号档次的备用货物供甲方使用，直至故障货物修复。

投标人（单位公章）：

法定代表人或授权代表（签字或盖章）：

年月 日