预算金额：19.8万元

期望收货时间：默认

送货地址：江苏南通市崇川区江苏南通市崇川区工农路1号崇川法院

产品品牌：深信服。

商品分类：防火墙

规格型号：详见采购清单

服务要求：软件平台须提供三年软件免费升级，三年硬件免费质保（由供应商承诺）、送货时随附深信服营业执照复印件加盖鲜红印章、保修卡、合格证。提供具备生产厂家认证的工程师上门服务。提供安装、调试、培训等服务，成交后在规定时间内交付使用。

附件：

**一、清单**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **配置参数** | **数量** | **单位** | **品牌** | **型号** |
| 1 | 防火墙 | 性能参数：网络层吞吐量：20G，应用层吞吐量：2.8G，并发连接数：2200000，新建连接数：150000；  硬件参数：规格：1U，内存大小：8G，硬盘容量：128G minisata SSD，电源：单电源，接口：6千兆电口+2万兆光口SFP+。  开通IPS入侵防御、URL&应用识别功能；开通AV防病毒功能；  本次配置3年IPS攻击规则库、URL&应用识别升级许可；3年病毒库升级许可；软硬件三年保。 | 1 | 台 | 深信服 | AF-2000-B2100-AK |
| 2 | 功能模块 | 开通IPS入倾侵防御模块，特征库三年；  开通AV防病毒模块，特征库三年。 | 1 | 套 | 与原有设备兼容 |  |

**二、参数要求**

4.1 防火墙参数要求

|  |  |
| --- | --- |
| 指标项 | 详细功能项 |
| 性能要求 | 多核架构，三层吞吐量≥20G，并发连接数≥220万，每秒新建连接≥15万/秒，SSL最大加密流量≥350Mbps，IPSec VPN最大接入数≥1000，IPSec VPN加密速度≥600Mbps； |
| 设备接口 | 千兆电口≥6个，万兆光口≥2个，1U标准架构，单电源 |
| 部署方式 | 支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式 |
| 网络特性 | 支持802.1Q VLAN Trunk、access接口，VLAN三层接口，子接口 |
| 支持链路聚合功能 |
| 支持端口联动功能，当上行/下行端口链路出现故障时，对应的另一端下行/上行端口自动切断链路 |
| 支持IPV6环境部署，包括接口/区域配置、路由配置等网络适应性功能，支持核心常用安全功能，包括僵尸网络，IPS漏洞防御，WEB应用防护等，支持协议一致性（包括但不限于Core、NDP、Autoconfig、PMTU、ICMPV6）和协议健壮性检测（IPv6畸形报文、ICMPv6畸形报文、其他协议畸形报文），支持IPV6的地址转换、双栈的过渡技术 |
| 路由支持 | 支持静态路由，ECMP等价路由以及RIPv1/v2，OSPFv2/v3，BGP等动态路由协议 |
| 基础功能 | 支持连接会话展示，可针对具体的IP地址进行会话详情查询，支持封锁异常会话信息，并支持设置监听具体IP的会话记录 |
| ★访问控制规则支持基于源／目的IP，源端口，源／目的区域，用户（组），应用/服务类型，时间组的细化控制方式，支持长连接功能并可以配置连接时长；（需提供相关功能截图证明并加盖原厂公章） |
| ★访问控制规则支持数据模拟匹配，输入源目的IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试（需提供相关功能截图证明并加盖原厂公章） |
| 能够识别管控的应用类型超过1200种，应用识别规则总数超过3000条 |
| 支持IPSec VPN，SSL VPN，GRE，GRE over OSPF，GRE over IPSec等VPN接入方式； |
| 内容安全 | 内置病毒样本数量超过1000万 |
| ★支持采用无特征AI检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测，给出基于AI技术的病毒检测报告； （需提供相关功能截图证明并加盖原厂公章） |
| 支持针对SMTP、POP3、IMAP邮件协议的内容检测，如邮件附件病毒检测、邮件内容恶意链接检测，邮件账号撞库攻击检测等，支持根据邮件附件类型进行文件过滤（需提供相关功能截图证明并加盖原厂公章） |
| DoS/DDoS攻击防护 | 支持Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing攻击防护，支持SYN Flood、IPv4和IPv6 ICMP Flood、UDP Flood、DNS Flood、ARP Flood攻击防护，支持IP地址扫描，端口扫描防护，支持ARP欺骗防护功能、支持IP协议异常报文检测和TCP协议异常报文检测 |
| 支持内网访问控制，配置内网区域只允许指定的IP地址或IP范围对外进行访问，防止内部伪造源IP对外DoS攻击的情况 |
| 支持对信任区域主机外发的异常流量进行检测，如ICMP，UPD，SYN，DNS Flood等DDoS攻击行为 |
| 入侵防护功能 | ★设备具备独立的入侵防护漏洞规则特征库，特征总数在7400条以上（需提供相关功能截图证明并加盖原厂公章） |
| 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telne、Weblogic、VNC）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能 |
| 支持同防火墙访问控制规则进行联动，可以针对检测到的攻击源IP进行联动封锁，支持自定义封锁时间； |
| 具备防护常见网络协议（SSH、FTP、RDP、VNC、Netbios）和数据库（MySQL、Oracle、MSSQL）的弱密码扫描功能 |
| ★可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则（需提供相关功能截图证明并加盖原厂公章） |
| 僵尸主机检测 | ★设备具备独立的热门威胁库，防护类型包括木马远控、恶意脚本、勒索病毒、僵尸网络、挖矿病毒等，特征总数在60万条以上；（需提供相关功能截图证明并加盖原厂公章） |
| ★对于未知威胁具备同云端安全分析引擎进行联动的能力，上报可疑行为并在云端进行沙盒检测，并下发威胁行为分析报告 |
| 安全可视化 | ★支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别（需提供相关功能截图证明并加盖原厂公章） |
| ★支持安全运营中心功能，可以对全网所有的服务器和主机的威胁进行全面评估，管理员通过一键便可完成对服务器和主机的资产更新识别、脆弱性评估、策略动作的合理化监测、当前服务器和用户的保护状态、当前的服务器和主机的风险状态及需要管理员待办的紧急事项等，可以自动化直观的展示最终的风险；（需提供相关功能截图证明并加盖原厂公章） |
| 支持自动生成安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，具备有效攻击行为次数统计和攻击举证 |
| 相关资质 | ★厂商软件研发实力需通过CMMI L5及以上认证（需提供相关功能截图证明并加盖原厂公章） |
| 国家信息安全漏洞共享平台(CNVD)技术组成员 |
| 产品应具备计算机信息系统安全专用产品销售许可证 |
| ★所投产品的生产厂商应是第八届国家互联网应急响应中心网络安全应急服务国家级支撑单位 |