**商品名称:** 下一代防火墙

**商品分类**：网络安全产品

**品牌：深信服**

**规格型号：**AF-2000-B2132-AK

**数量：**一套

**基本描述：**性能参数：网络层吞吐量：20G，应用层吞吐量：8G，IPS吞吐量：1.3G，防病毒吞吐量：1.5G，全威胁吞吐量：1G，并发连接数：220万，HTTP新建连接数：15万，SSL VPN推荐用户数（单独购买）：30，SSL VPN最大用户数（单独购买）：150，SSL VPN最大理论加密流量（单独购买）：350M，IPSec最大隧道数：1000，IPSec VPN吞吐量：400M。

硬件参数：规格：1U，内存大小：8G，硬盘容量：128G minisata SSD，电源：冗余电源，接口：6千兆电口+2万兆光口SFP+。

功能描述：深信服下一代防火墙以保障用户核心资产为目标，提供L2-L7层各类威胁的检测和防护，是一款能够有效应对传统网络攻击和未知威胁攻击的网络安全产品。

**服务要求：**1.成交后10日内供货并负责整体安装调试，设备质保三年，提供设备三年质保承诺书。

2.项目实施地点：江苏省南通中学。

3.须缴纳成交价的5%作为质量保证金，质保一年后无息返还。

下一代防火墙参数

|  |  |
| --- | --- |
| 指标项 | 详细功能项 |
| 性能及接口 | 三层吞吐量≥20G，应用层吞吐量≥8G，并发连接数≥220万，每秒新建连接≥15万/秒，千兆电口≥6个，万兆光口≥2个，1U标准架构，冗余电源 |
| 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 |
| ★支持多链路出站负载，支持基于源/目的IP、源/目的端口、协议、应用类型以及国家地域来进行选路的策略路由选路功能（需提供相关功能截图证明） |
| 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） |
| ★支持根据国家/地区来进行地域访问控制（需提供相关功能截图证明） |
| ★支持基于应用类型，网站类型，文件类型进行流量控制，支持基于IP段、时间、国家/地区、认证用户、子接口和VLAN进行流量控制；（需提供相关功能截图证明） |
| 支持IPSec VPN，SSL VPN，GRE，GRE over OSPF，GRE over IPSec等VPN接入方式； |
| ★IPSec VPN支持智能选路功能，保障业务的高可靠性。（需提供相关功能截图证明） |
| DoS/DDoS攻击防护 | 支持SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood等泛洪类攻击防护，支持IP地址扫描和端口扫描攻击防护。 |
| 支持TearDrop 攻击、IP数据块分片传输、Land攻击、Smurf攻击、WinNuke攻击、超大ICMP数据攻击等异常报文攻击防护，支持IP协议异常报文和TCP协议异常报文攻击防护。 |
| 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） |
| 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 |
| 具备僵尸网络检测功能，可基于僵尸网络检测引擎发现主机的异常外联行为，并提供威胁等级和非法外联次数作为举证。 |
| 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 |
| 安全策略管理 | 支持针对业务攻击事件汇总，展示攻击事件类型TOP5及当前业务命中的全网实时热点事件，支持通过地图区域颜色深浅展示攻击者的分布与数量。 |
| ★支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便策略的管理和运维。（需提供相关功能截图证明） |
| 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） |
| ★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） |
| 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 |