|  |  |
| --- | --- |
| **指标项** | **技术参数要求** |
| 产品资质 | 所投产品获得公安部计算机信息系统安全专用产品销售许可证，需提供相应证书复印件 |
| 性能要求 | 并发连接≥800万，新建连接≥17万/秒，网络吞吐量≥15Gbps  |
| 硬件要求 | USB口≥2个，管理口≥2个，千兆电口≥8个，千兆光接口≥8个 |
| 信创要求 | 采用国产化硬件平台，并采用国产操作系统 |
| 部署模式 | ★支持路由、透明接入、虚拟线、混合4种工作模式（提供截图证明材料） |
| IP/MAC绑定 | 支持IP/MAC检查；支持手动添加和自动探测IP／MAC对应关系；具备IPv6协议栈的IP/MAC绑定及检查功能； |
| NAT | 支持一对一SNAT，多对一SNAT，一对一DNAT，双向NAT |
| 协议 | ★支持自定义协议，除五元组外，还可配置自定义协议的优先级、应用技术、应用属性、风险级别、类型、子类、协议、匹配内容、应用层长度，可做到多层次自定义协议防护（提供截图证明材料） |
| ACL | ★支持基于IPv4的ACL访问控制功能，可通过五元组、时间调度、用户、网络服务、流入接口、应用对象、源域、目的域等基本配置条件来匹配数据流，支持源目的地址的取反操作；同时也支持通过源、目的MAC地址、报文头部信息（SYN标志、分片标志、TTL、DSCP、Precedence、TOS）、内网域地址、外网域地址、记录日志、长连接超时时间等高级配置条件来匹配数据流。（提供截图证明材料） |
| ALG | 支持控制FTP、H.323、H.323GK、TNS、PPTP、MMS、RTSP、SIP、XDMCP、SQL\*NAT/TNS等ALG，同时支持V2V协议过滤 |
| 快速向导 | 支持防火墙配置向导功能，配置流程为：基本信息、系统时间、部署方式、网络、防火墙配置、核对信息。 |
| WEB站点安全防护 | 支持对web站点安全防护，可实现HTTPS单双向代理以及证书认证，支持CSRF、盗链防护、URL访问控制，可实现CSRF、盗链配置Target、Referer字段，盗链防护URL重定向、防护算法，支持URL访问控制，提供15类URL请求方法的配置。 |
| 规则类防护和规则类深度防护 | 支持通用规则及深度规则防护，涵盖了移动代码、内容防护、爬虫行为、WEB扫描攻击、目录遍历、自定义策略等6大类100余种WAF通用规则库和SQL注入、跨站攻击、等12类300余种深度规则特征，对WEB站点进行安全防护，可实现对非法访问的放行、拒绝、记录日志以及声音报警等处理动作。 |
| WEB网站信息防护 | 支持访问网站时错误信息、响应码的替换功能，可对Server、X-Powered-By字段的隐藏，实现WEB重定向的过滤，并记录日志及告警；支持对网站上传、下载文件的类型和大小的控制，提供Cookie加密和签名防护，支持HTTP协议1.0和1.1版本包括URL最大长度、Accapt最大长度等字段的验证，可支持16种HTTP请求方法的检测，符合合法策略的放行，。 |
| WAF监控 | 支持WAF事件监控，可按照事件时间、名称、级别、攻击类型、IP地址对WAF事件进行检索。支持生成WAF事件日报/月报/周报/自定义事件报表，以及PDF/TXT/HTML/CSV/DOCX5种报表文件类型，支持WAF报表预览、下载、邮件发送。 |
| 防病毒引擎和病毒库 | ★支持自研防病毒引擎和第三方防病毒引擎双引擎，可提供16大类500余万病毒特征库用于对用户流量的病毒检查，确保用户安全的网络安全。（提供截图证明材料） |
| 防病毒技术 | 支持配置防病毒策略，支持快速模式、深度模式两种扫描模式，最多可支持16层的压缩文件检测。支持基于http、ftp、imap、pop3、smtp协议50多种文件类型的病毒检测功能。支持基于MD5值自定义黑白名单设置，通过检测文件MD5值，判断文件安全性，。 |
| 病毒特征库升级 | 支持病毒特征库的在线、离线升级，支持每天、每周特定时间升级，间隔特定时间升级。 |
| 入侵防护 | 支持IPS检测和抗逃逸技术，可阻挡缓冲区溢出、SQL注入、扫描刺探、间谍软件、拒绝服务、病毒、木马后门、漏洞攻击潜在风险以及自定义的攻击。 |
| 入侵防护特征库 | 内置攻击特征库，特征数量超过10000条，支持病毒特征库的在线、离线升级，支持每天、每周特定时间升级，间隔特定时间升级，支持基于TCP/ICMP/UDP/HTTP协议的入侵特征码、正则表达式的自定义特征的构造。 |
| 口令检测 | 支持口令暴力破解的口令检测，对包含口令字段的常用8种应用层协（SMTP/IMAP/POP3L/TELNET/FTP/RLOGIN/NNTP/TDS-MS-SQL）的口令尝试频率的检测；支持弱口令检测功能，检测包括POP3/FTP/TELNET3种协议、口令长度、口令复杂度等7种检测元素。 |
| 黑白名单 | 支持黑白名单功能，可基于攻击源、攻击目标进行黑白名单的阻断和放行。 |
| 流量学习 | 支持流量的自学习功能，可设置流量学习时间，通过报文、IP排名、域名统计类型建立当前网络模型下设备的流量基线。 |
| 洪水防护 | 支持基于ACL的DDoS洪水防护，支持对ICMP洪水、IGMP洪水、SYN ACK洪水、数据流洪水、ACK洪水、DHCP洪水、最大连接数洪水、每秒新建连接数洪水、UDP洪水、SYN洪水、HTTP报文洪水、CC、端口扫描、ICMP SWEEP攻击、ARP洪水、分片洪水、teardrop的防护。 |
| URL过滤 | 支持URL过滤功能，对用户访问的网址进行检查，支持关键字和正则两种过滤方式，可通过白名单、黑名单控制用户可访问的网站，白名单优先。 |
| 大屏 | 支持全屏展示中国地图、世界地图攻击效果展示。可显示攻击事件的源域、目的域，并形成完整攻击路线，根据攻击事件等级，攻击路线以不同颜色进行区分。支持显示IPS告警数、AV病毒告警数、资源监控、设备运行状态、威胁趋势、风险主机TOP10、用户流量TOP5、业务TOP5 |
| 事件取证 | ★支持对单个攻击事件保存其原始报文以供取证分析，报文文件可通过接口进行传输保存，还可以保存到本地。可对取证文件进行查找、导出和删除。（提供截图证明材料） |
| NTP | 支持NTP同步功能，配置参数包括NTP/SNTP服务的IP/域名、密钥ID、认证密码等。 |
| SNMP | 支持SNMP协议（V1，V2，V3），能够基于SNMP接收网络节点通知消息及告警事件报告获知设备运作状态等信息。 |
| 配置文件导入导出 | 支持配置文件保存、导入、导出等功能，支持查看配置文件的当前、历史及时间等信息，并支持设置指定下次启动的配置文件。 |
| 升级维护 | 支持对本地存储的系统软件版本进行维护管理，管理员可选择不同历史版本的ROM文件在下次启动时使用，支持显示、查看当前软件版本、系统升级历史、系统重启历史、运行时间、重启时间、重启原因等信息，并支持配置备注信息。 |