|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 硬件架构 | 采用非X86多核架构，自带单交流电源 |
|
| 接口要求 | ≥8个千兆电口，≥2个Bypass接口，≥2个Combo光电复用口 |
| 存储要求 | 支持硬盘扩展≥1,可支持扩展1T 的HDD硬盘，480G SSD硬盘； |
| 性能要求 | 应用层吞吐量≥1Gbps，网络层吞吐量≥4G，最大并发连接数≥400万，每秒新建连接数≥1.8万。 |
| SSL VPN并发用户≥650； |
| IPSec VPN隧道数≥750； |
| AI智能策略 | 支持一体化安全策略，能够基于时间、用户/用户组、应用层协议、五元组、内容安全统一界面进行安全策略配置 |
| 支持智能的对配置的策略进行冗余分析， 冲突策略分析以及命中率统计。 |
| 支持通过应用层检测引擎智能地分析安全策略允许通过的流量中存在的潜在风险，为设备中所有安全策略的安全系数进行总体评估并给出调优建议和防护措施。 |
| 支持AI智能指纹识别，支持文件指纹识别，终端指纹识别，实现多样化的接入方式和认证策略，差异化的用户权限控制。 |
| 支持对全网流量进行深度分析，形成安全基线模型，可根据不同安全级别对五元组、时间、用户、协议种类、协议字段类型及典型值等与基线模型进行对比，同时结合威胁情报，有效发现异常流量并给出策略推荐。 |
| URL过滤 | 设备提供海量预分类的URL地址库，支持根据URL类别实现URL过滤； |
| 设备支持管理者自定义新的URL地址和URL分类； |
| ▲支持联动云端URL地址库进行全面实施核查。（提供功能截图） |
| AI智能分析 | 支持对C&C通信中的恶意软件、DNS隐藏通道、ICMP隐藏通道、加密隐藏通道及DGA域名等进行感知、发现并及时进行阻断。 |
| 支持聚类分析算法，将防火墙获取的不同数据源中的数据进行提取、过滤和关联分析，最终形成用户维度的数据关联分析日志，大大降低管理人员分析工作量 |
| ▲提供基于用户名（或用户IP地址）实现对用户行为统一分析界面，采用饼状图对访问应用流量、网站访问集中分析展示，包含基于时间轴的访问行为轨迹(应用账号、行为内容等)，关联账号（微信、QQ）等相关用户行为审计内容。（提供功能截图） |
| 数据安全 | 支持数据防泄露，对传输的文件和内容进行识别过滤，对内容与身份证、信用卡、银行卡、社会安全卡号等类型进行匹配。 |
| ▲加密流量检测 | 支持HTTPS加密流量的安全检测。（提供功能截图） |
| 负载均衡 | 支持多出口智能选路，可根据目的地址智能优选运营商链路，支持主备接口配置以及按比例分配的负载分担方式。 |
| 支持PPPOE拨号功能，支持PPPOE链路与专线链路的智能负载 |
| 支持基于用户、应用以及域名等的链路负载 |
| 支持智能DNS解析功能，引导访问用户从最优路径的线路接入应用系统。 |
| ▲支持DNS透明代理功能，可基于负载均衡算法代理内网用户进行DNS请求转发，避免单运营商DNS解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率。（需提供设备功能界面截图证明） |
|
| 支持包括轮询、加权轮询、最小连接、加权最小连接、随机、加权随机、源地址Hash、源地址端口Hash、目的地址Hash、优先级等负载均衡调度算法。 |
| 支持基于Http Accept-Encoding、HTTP Accept-Language、Http Host、Http Request-Method、Http URL-File、Http User-Agent、DHCP、RADIUS、RTSP、SIP等协议 |
| 支持温暖上线，支持满宕和立即停止功能的灵活配置 |
| ▲AI智能诊断 | 支持当内网用户访问某网页出现故障时，对网络进行基本的诊断，给出诊断信息。能快速协助内网用户进行访问WEB问题排查。 |
| 支持报文示踪功能，可对原始报文进行回放。（提供功能截图） |
| 支持丢包统计，提供详细分析丢包原因。（提供功能截图） |
| 国密算法 | 支持国密SM1/2/3/4算法。 |
| ▲厂商资质 | 设备制造厂商具备CNNVD（中国国家信息安全漏洞库）一级支撑单位资质 |
| 设备制造厂商具备CNVD（中国国家信息安全漏洞共享平台）技术组成员资质 |
| 设备制造厂商软件能力通过CMMI 5级认证 |
| 上述资质，须提供相关证书证明，提供证书复印件 |
| ▲产品资质 | 所投产品须具备公安部颁发的防火墙《计算机信息系统安全专用产品销售许可证》（增强级） |
| 所投产品须具备公安部颁发的第二代防火墙《计算机信息系统安全专用产品销售许可证（增强级） |
| 上述资质，须提供相关证书证明，提供证书复印件 |