防火墙产品功能参数

支持 IPv4\IPv6 双栈流量
支持路由模式、透明模式、旁路模式等多种部署方式。支持基于数据包五元组的基础包过滤功能。
支持源地址转换，目的地址转化，源目的 IP 同时转换，支持 NAT64 和 NAT46 地址转换方式。
支持 3 种以上的用户认证方式,包含单点登录、本地账号密码、外部账号密码认证。
支持 MPLS 技术，对数据包分配使能接口、MPLS 标签，全面提高数据包交换、传输速率。
支持链路聚合功能，可以将多个物理链路组合成一个性能更高的逻辑链路接口，提高链路带宽和链路可靠性。
产品支持对安全策略管理和审计功能，记录安全策略变更时间、变更账号、变更类型等内容
支持基于 URL 的策略路由，可实现为不同的 URL 类型智能选择相应链路。
支持 IP 黑名单批量导入功能，满足重保、演练、护网场景下 IP 黑名单的手动导入；支持外部动态列表更新功能，满足从 HTTP 服务器定期自动获取黑名单，导入模式支持增量导入和覆盖导入，IP 黑名单库最大支持 110 万条。
产品具备抓取数据包的功能，支持 WEB 页面和命令行两种方式，支持配置保存文件数、单文件包数、超时时间等，也提供报文下载功能；
硬件巡检包含设备序列号、设备运行状态、设备名、设备版本信息。
支持攻击防护，包含 SYN Flood、UDP Flood、ICMP Flood、Ping of Death、Smurf、ARP 欺骗攻击，扫描与欺骗等，支持告警、丢弃两种模式，对不同安全域可设定不同阈值和处理模式。
同时支持 WEB 和命令行两种配置方式。
便于管理员识别策略有效性，防火墙支持安全策略冗余冲突检测，策略时间表有效性检测，策略命中分析功能，在页面显示策略创建时间、首次命中时间、最近一次命中时间和最近未命中天数，实现对策略优化检查。
支持 BFD 探测，支持对 IPv4/IPv6 地址进行有效性探测，支持主动、被动、单臂回声三种工作模式；支持设置接收最小 TTL、最小发包间隔、最小收包间隔、探测倍数、源地址、出接口设置；支持多跳探测。
支持 WEB 界面故障分析功能，当某个业务不通时，可根据设备对数据包的处理流程自动分析出故障点，便于管理员排查故障，提升运维效率。
支持 SNAT/DNAT 冗余检测分析，帮助管理员梳理冗余 NAT 规则；支持 SNAT/DNAT 命中数分析，显示创建时间、命中数、首次命中时间、最近一次命中时间、未命中天数等信息，并可针对分析结果，对 NAT 规则进行删除或禁用。
支持基于 IPv4/IPv6 的源地址/源地址组、目的地址/目的地址组的白名单。支持域名白名单。
支持 IPSec VPN 隧道数 11000 条，IKE 阶段的加密算法支持 3DES、DES、AES-128、AES-192、AES-256 等，验证算法支持 MD5、SHA-1、SHA-256、SHA-384、SHA-512 等；支持智能选路，可根据隧道质量选择最优线路隧道。