Hillstone
山 石 网 科

山石网科安全管理平台（虚拟化版）

Virtual Hillstone Security Management

随着网络规模、业务应用的不断增长，用户面临的安全威胁也日益增多。在网络安全建设方面，用户往往通过部署多种、多台安全设备，实现对信息网络的分域分级保护。然而，部署的多台安全设备总是“孤立”地进行安全检测和控制，却缺乏有效集中的安全管理手段，这使得系统管理员无法从全局角度对信息网络的安全状态做到有效监控，更无法实施整网安全策略。

为此，山石网科推出了可部署在虚拟化环境的 vHSM（Virtual Hillstone Security Management）软件化安全管理平台，为中小企业网络、分支互联网络和数据中心网络等部署多台安全设备的场景，提供有效的集中安全管理，大大降低用户的运维 管理成本。vHSM 综合运用全局性日志管理、统一策略管理、设备状态集中监控、监控数据汇总和报表统计等手段，解决网络安全状况不直观、安全策略管理乱、安全事件响应慢、安全故障定位难等问题，为用户网络提供全面的集中管理解决方案。

产品亮点

策略管理

- 策略集中管理：利用HSM 平台对全网连通性策（NAT&Route）和安全策略、IPS、AV、SLB进行集中收 集、分析、编辑、下发等工作，同时还支持策略快照与回滚 操作，可实现灵活、便捷的策略管理，提高全网策略的部署 效率和安全防护效果。
- 策略继承：支持对一条或一组共性策略，批量的下发到 NGFW上，简化设备配置维护工作;在Hub-Spoken的场景中，中心管理员可以根据管理上的诉求，把共享策略强制继承给分支设备，提高日常策略运维管理的效率。
- 策略清理：策略智能分析引擎实时分析全网安全策略及对象信息，可快速检测出冗余策略、无用对象和策略命中数，从而优化策略配置，提高设备运行效率，提供策略“瘦身”方案。

设备管理

- 设备灵活注册：提供易用灵活的用户设备注册机制，支持设备通过IP、域名和模板的方式在HSM上进行注册。
- 配置备份恢复：手动和自动收集设备配置，集中存储全网设备配 置文件，并提供配置文件备份和恢复功能。
- 配置变更管理：基于4W（Who、When、Where、What）的审计 方法，实时记录文件配置变更的内容，为安全审计提供。

设备巡检

- 可对防火墙的运行状况、资源消耗、特征库及许可证等状态进行检查并自动生成报告通知客户，帮助用户提前发现设备问题，及时修复潜在故障。设备巡检分为以下三种：手动巡检、自动巡检、智能巡检。

安全监控

- 设备可用性监控：对全网部署的山石网科安全设备的可用性 进行监控，监控的指标包括CPU、内存、并发连接数、流量等，实时掌握设备的健康状态。
- VPN 拓扑状态监控：对于已经注册的设备，自动绘制VPN拓扑图，图形化监控VPN链路情况，支持设备隐藏和过滤功能，可

产品亮点

快速定位关注的设备。

- 安全事件集中监控：可集中实时展现全网部署的安全设备的监控信息，包括IP、应用、URL、威胁等，使系统管理人员随时掌握全网安全状态。

权限管理

- 基于角色的用户管理：可根据管理员角色设定HSM管理权限，如管理员、操作员、审计员等，从而防范由于权限集中造成的 审计困难。
- 基于设备的权限管理：HSM主管理员可为其他管理员创建可管 理的设备分组。每个管理员可管理所属域内的设备，避免权限扩散带来的安全隐患。
- 细粒度权限划分：基于“只读”和“读写”对系统的功能模块提供精 细的权限划分，可以对组织内的管理人员进行科学的分级管 理。

工单管理

- 工单系统：支持通过工单系统实现安全策略的自动下发，帮助客户业务快速上线。工单系统支持：工单申请、工单处理、工单审核、工单下发。
- 感兴趣网络：工单处理时根据工单策略的源目地址，自动选择下发的安全设备。
- 冗余检测：工单下发时，对工单安全策略和防火墙上已有的安全策略进行策略冗余检测，确定下发动作。

SD-WAN

- 快速组网：通过在HSM上进行简易的VPN配置，完成分支到总部的自动化VPN组网
- 分支开局：在HSM端添加分支设备导出ztp配置包，通过U盘完成分支设备的一键开局
- 链路优化：基于应用的QoS策略和优先级控制、基于应用的负载均衡和质量保障

产品功能规格

设备配置管理
- NGFW设备集中管理
- NIPS设备集中管理
- WAF设备集中管理
- BDS设备集中管理
- vFW集中管理
- 设备 IP、域名、模板注册
- 设备软件批量升级
- 设备特征库批量升级
- 设备批量重启

设备批量改密
- 设备配置文件备份恢复
- 设备配置文件对比
- 设备配置文件自动同步
- 设备HA状态管理

VPN网络监控
- VPN中国地图监控呈现
- VPN拓扑监控
- 网络状态监控
- 链路中断告警

安全策略管理
- 支持Route、NAT及安全策略
- IPS 策略集中管理
- AV 策略集中管理
- SLB 策略集中管理
- URL 策略集中管理
- iQoS策略集中管理
- AAA 服务器集中管理
- 策略集中编辑与修改
- 用户集中管理
- 角色集中管理
- 策略关联
- 策略集中下发
- 策略对象管理
- 策略冗余检验
- 策略操作审计

设备监控
- 设备运行状态实时监控
- 设备端口流量趋势
- 用户流量趋势
- 设备许可证状态
- 设备应用流量趋势
- TOP10威胁趋势排名
- TOP10 URL访问排名

日志审计
- 设备系统日志审计
- 设备流量日志审计
- 设备安全日志审计
- 数据安全日志审计
- 网络应用日志审计
- HSM系统日志审计
- 支持日志的手动/自动备份和导入
- 支持基于日志查询结果导出可读日志
- 支持将日志转发到第三发syslog服务器

告警
- 支持基于阈值规则告警
- 实时告警
- 支持多种告警方式

报表
- 内置30多种报表模板
- 支持自定义报表
- 支持HTML和PDF格式报表文件
- 支持自定义报表创建人
- 支持自定义报表邮件内容
- 支持VPN断线统计报表

系统管理
- 支持管理员的角色管理
- 支持管理员的设备权限管理
- 支持高可靠性部署
- 支持分布式部署

IPv6
- 支持IPv6的配置管理
- 支持IPv6的日志采集和查询
- 支持IPv6的设备监控

工单管理
- 工单申请
- 工单处理
- 工单审核
- 工单批量导入
- 下发设备自动识别
- 工单策略冗余检测
- 配置脚本导出
- API对接工单系统

SD-WAN管理

VPN星型组网

VPN业务发放和管理

支持分支设备u盘加载配置文件

分支设备上线自动升级版本

分支设备上线自动获取授权

设备及链路状态监测

产品规格

参　数	vHSM			
设备管理数量	25	100	500	1000
vCPU要求	4	8	18	24
内存要求	8GB	16GB	32GB	64GB
存储要求	100GB	2TB	4TB	8TB
网络接口要求	2	2	2	2
虚拟化环境要求	VMware Workstation/EXSI 或 KVM			