H3C iMC SSM 安全业务管理组件

产品概述

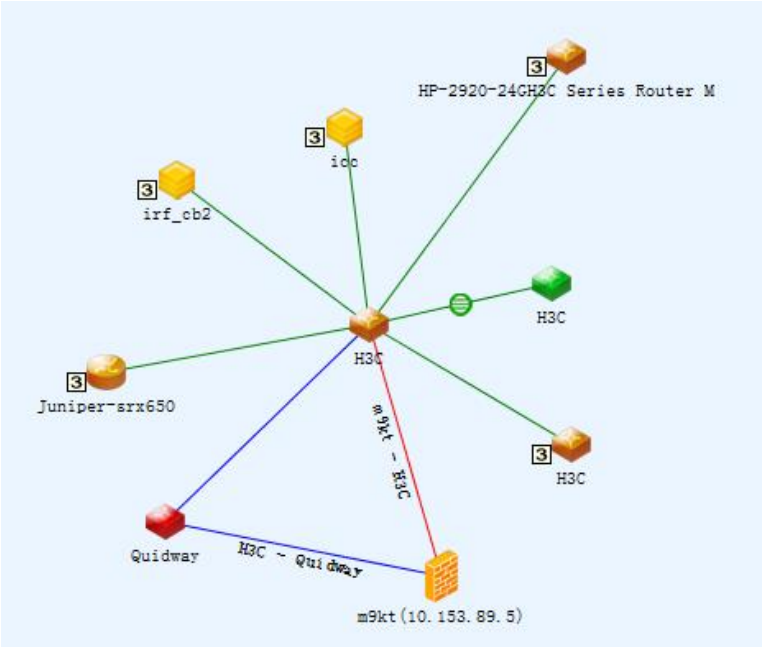
SSM（Security Service Manager，安全业务管理）是 iMC 平台下的一个负责网络安全业务的组件，主要用于根据实时监控的网络数据转发动态或网络入侵行为来规范和管理网络。SSM 中能够对网络中的安全设备进行统一管理。它能够适应各种网络规模需求，为部署于各关键位置的安全设备提供集中的安全策略管理与控制，并能直观的为实时事件监控和综合分析攻击等各种安全事件提供丰富的统计报告，方便用户随时了解网络安全状况。作为一个强大、高效的安全业务管理系统，SSM 可以对网络中多个安全设备集中管理，对全网安全策略规则统一部署，对攻击事件信息集中收集并分析，提供实时监控、事件快照、综合分析、策略下发以及日志审计等功能。并且能对全网范围内的安全事件进行集中的统计分析。

SSM 主要包括安全拓扑管理、安全事件管理、全局资源管理和防火墙业务配置功能。其中安全拓扑管理主要用于显示系统所管理的拓扑结构，安全事件管理主要用于根据实时监控到的网络数据来规范和管理网络，全局资源管理是对物理设备、虚拟设备、用户、全局 IP、服务的管理和对全局参数的配置，防火墙业务配置用于对安全域、域间规则、规则优化和作业部署进行管理。

产品特点

智能安全拓扑管理及终端联动

安全拓扑管理包含安全拓扑以及攻击路径拓扑，用来展示安全业务管理的网络结构以及对安全业务进行管理，通过攻击日志定位攻击源，攻击目的，通过与 AAA 服务器联动定位攻击用户，计算攻击路径并对其下发限制策略。



完善的事件分析和统计报表

防火墙管理系统提供完善的安全事件综合分析与统计报表，采用“上图下表”的方式，提供基于月、周、天及特定时间段内的安全事

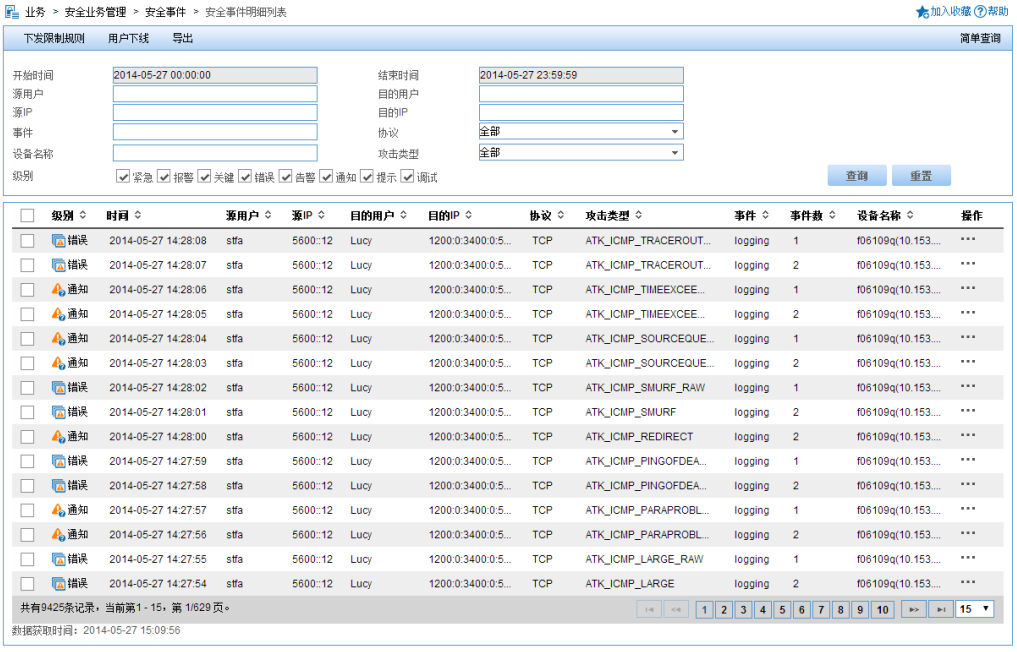
件分析，支持按严重级别划分的事件趋势图分析、饼图分析，支持对综合分析报表的人工手动与定时自动集中导出。

通过对安全事件的深入分析和总结，利于管理员直接了解网络中的攻击行为与活动，为未来网络非法攻击、非法访问进行严格界定

细致的整网安全事件审计

SSM 可从异常流量日志、黑名单日志、NTA 日志、域间访问控制日志、MPLS 日志、SSL VPN 日志、系统操作日志等多方面来对网络安全事件进行跟踪与分析，直观了解安全事件的来源、目的地等的行为状况，详细记录攻击事件、异常流量、非法访问、非法系统操作等，帮助管理员了解到网络攻击、异常流量状况，并对用户操作进行跟踪，便于事后审计和追踪。

同时，SSM 提供强有力的搜索查询能力，能够从海量的历史数据中，基于设备、时间、事件类型、协议、攻击级别、源/目的 IP、端口号等多维度定义进行快速查询。如通过对攻击类型的查询，可得到以时间顺序排列的攻击者源 IP、目的 IP、端口号、协议号、详细事件信息等的事件记录



智能资源管理和策略调优

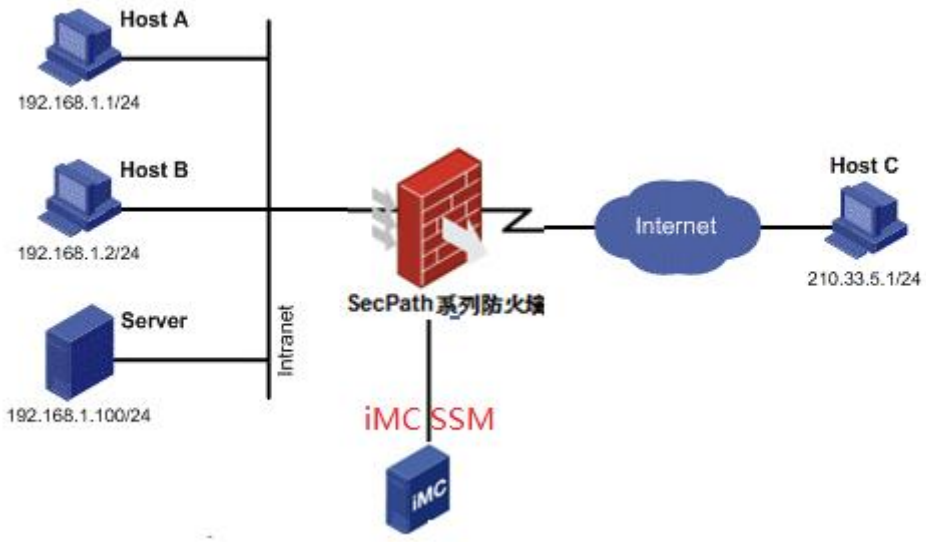
SSM 可智能化管理网络中的安全设备。管理员可以对安全设备进行导入配置、同步、业务配置等操作。利于实现网络资源的集中化管理，保障网络整体运行安全，及时发现网络和系统主机的故障和性能瓶颈。同时可根据安全设备策略运行状态对安全策略智能调优，确保安全设备始终最优状态运转。

产品规格

项目	H3C iMC SSM 安全业务管理组件
快速入门	展示所有模块依赖关系。
安全拓扑管理	在拓扑中展示防火墙信息，查看攻击信息。
安全事件概览	对整网安全事件的实时监控和集中采集并显示最近一小时的各种攻击事件的 TopN 列表。
实时事件列表	用于对全网攻击事件进行实时监控，实时显示近期安全事件状态，以列表的形式显示攻击时间、攻击源、攻击目的、攻击事件等信息。
安全事件分析	提供完善的安全事件综合分析，采用图形和表格的方式，提供基于天、周、月及自定义时间段的安全事件分析，支持按严重级别划分的事件趋势图分析、饼图分析。
安全事件明细	用于展示整网的攻击事件，以列表的形式显示攻击时间、攻击源、攻击目的、攻击事件等信息。针对某一个攻击，SSM 可以在拓扑中绘制出攻击路径，对攻击源进行限制。
域间访问控制日志审计	用于展示，查询，导出设备管理列表中设备产生的域间访问控制日志。
异常流量日志审计	用于展示，查询，导出设备管理列表中设备产生的异常流量日志。
黑名单日志审计	用于展示，查询，导出设备管理列表中设备产生的黑名单日志。
操作日志审计	用于展示，查询，导出设备管理列表中设备产生的操作日志。
NAT 日志审计	用于展示，查询，导出设备管理列表中设备产生的 NAT 日志。
其他日志审计	用于展示，查询，导出设备管理列表中设备产生的非以上几种类型的日志。
日志综合审计	用于展示，查询，导出设备管理列表中设备产生的各种日志。
设备管理	用于管理防火墙安全设备，主要包括导入设备配置，同步设备，对设备的域间规则、安全域、服

项目	H3C iMC SSM 安全业务管理组件
	务、IP 进行管理。
虚拟设备管理	用于管理虚拟防火墙设备，主要包括增加、修改、删除、查询、启动、停止虚拟设备。
IP 地址管理	用于管理全局的 IP 地址，包括主机地址、范围地址、子网地址和 IP 地址组。
服务管理	用于管理全局的服务，包括系统预定义服务、自定义服务和服务组。
用户管理	将 iMC 平台的用户账号信息同步到防火墙模块中，通过在防火墙中对用户制定一系列过滤规则，从而实现对用户的管理。
全局参数配置	查看、修改全局参数。
数据转储	定期转储数据库与文件中的日志。
安全域管理	用于管理防火墙设备上安全需求相同的多个接口。 管理员将安全需求相同的接口进行分类，并划分到不同的安全域，能够实现安全策略的统一管理。
域间规则管理	用于管理域间规则，主要包括增加、删除、修改、复制、查询域间规则。
规则优化管理	用于查看设备上每条规则的匹配速率和最后一次匹配时间，管理员还可以将长期不匹配的规则删除。
作业部署管理	作业部署提供在多个设备上同时执行增加（或卸载）域间规则的功能。

典型组网



订购信息

项目	描述
H3C iMC-智能管理平台标准版(不含节点)-纯软件(DVD)	必配，iMC 平台。
H3C iMC- SSM 安全业务管理组件-纯软件(DVD)	必配，iMC SSM 平台。
H3C iMC- SSM 安全业务管理组件 5 节点 License 费用	选配，增加 5 SSM 管理授权 License。
H3C iMC- SSM 安全业务管理组件 20 节点 License 费用	选配，增加 20 SSM 管理授权 License。
H3C iMC- SSM 安全业务管理组件 50 节点 License 费用	选配，增加 50 SSM 管理授权 License。
H3C iMC- SSM 安全业务管理组件 200 节点 License 费用	选配，增加 200 SSM 管理授权 License。
H3C iMC- SSM 安全业务管理组件-IPS 管理功能 License 费用	选配，IPS 功能管理授权 License。
H3C iMC- SSM 安全业务管理组件-LB 管理功能 License 费用	选配，LB 功能管理授权 License。

杭州华三通信技术有限公司

http://www.h3c.com.cn

杭州基地
杭州市滨江区长河路 466 号
邮编：310052
电话：0571-86760000
传真：0571-86760001

北京分部
北京市宣武门外大街 10 号庄胜广场中
央办公楼南翼 16 层
邮编：100052
电话：010-63108666
传真：010-63108777

客户服务热线
400-810-0504

版本：20150527-V1.2