SMP综合日志审计平台看不到防火墙的审计日志

Syslog日志　王听宇　2024-01-04 发表

组网及说明

不涉及

告警信息

不涉及

问题描述

Fw 侧抓包，看抓包飞书的审计日志已经发给 smp 了

Syslog 633 LOCAL7.INFO: Jan 04 12:32:44 2024 FW2 %%10 VsysId:1 AUDIT/6/AUDIT_RULE_M

smp侧tcpdunm抓包，能收到飞书审计日志

过程分析

SMP不显示防火墙发送的配置日志 - 知了社区 (h3c.com)

某局点SecPath F1000-AK165(V7) 在SMP平台上显示不全日志 - 知了社区 (h3c.com)

某局点 SecCenter SMP 安全业务管理平台（原SSM-G2） 无法显示ips日志 - 知了社区 (h3c.com)

解决方法

现场配置了vrrp，fw发出日志报文时，使用了接口下实际地址，

smp上 业务ip 修改为fw发出的源地址后正常显示审计日志