M9K/T9k外发安全策略日志到日志主机不全

Syslog日志 Flow日志 **李瑞** 2023-05-01 发表

组网及说明

不涉及

告警信息

不涉及

问题描述

现场M9K或T9K开启日志外发的功能，将安全策略日志全量发送到日志主机，日志主机上查看有部分日志丢失，即日志不全，查看大量安全策略日志的deny日志没有收到

过程分析

设备默认开启聚合日志发送功能，即缓存发送方式：同一数据流的首报文匹配相关策略生成并发送日志后，设备缓存此日志，同时启动发送日志的时间间隔定时器，只有时间间隔到达后，才会判断是否继续发送此日志。在此时间间隔内若有流量匹配此日志，则发送日志，若没有则删除缓存的此日志。日志缓存数目达到上限后，新增数据流匹配相关策略时不能生成日志。日志发送时间间隔缺省为5分钟，且不能修改。

由于缓存大小优先，如果现场日志量非常大，就会导致缓存满（每5分钟1W条），导致日志缺失

解决方法

配置aspf log sending-realtime enable，使用实时发送方式，发送全量日志