安全策略日志发送日志主机后有延时或日志丢失

域间策略/安全域 Syslog日志 聂骋 2021-06-03 发表

组网及说明

不涉及

问题描述

安全策略日志，配置日志主机后发现部分流量触发安全策略日志，但是没有发送，或者是延时一段时间后才能发送。

过程分析

该问题是由于防火墙安全策略日志，域间策略日志或包过滤日志量一般较大，因此防火墙上为了防止日志主机性能不足，提供缓存功能，当上述模块产生日志后，先进入缓存区，若五分钟内还有流量触发该日志，则认为日志有效，五分钟后发送，若五分钟内无第二次流量触发，则直接丢弃该日志，不会发送到日志主机。该功能缺省开启。

解决方法

若日志主机性能足够，可以开启实时发送方式，命令为aspf log sending-realtime enable。则取消缓存方式，任何日志都会发送日志主机，发送前一定要确认日志主机性能情况。