SMP安全策略日志查询不全问题

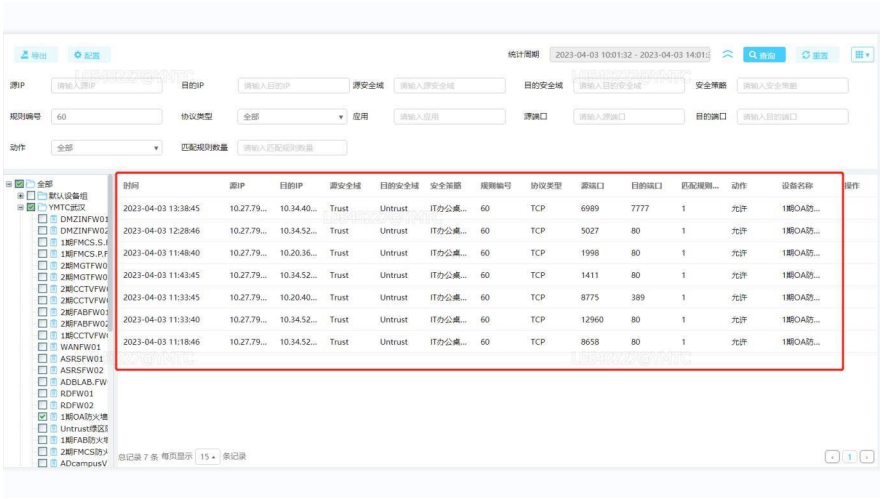
域间策略/安全域 Flow日志 PengfeiShao 2023-04-04 发表

问题描述

问题描述：安全业务管理平台中安全策略日志查询日志不全或者查询不到。
软件版本：E1112P06

防火墙上查询的数据:

SMP查询结果:



过程分析

在SMP平台抓包看显示的后收到的一致，

解决方法

在防火墙开启aspf log sending-realtime enable

aspf log sending-realtime enable命令用来开启日志的实时发送功能。

undo aspf log sending-realtime enable命令用来关闭日志的实时发送功能。

【命令】

aspf log sending-realtime enable

undo aspf log sending-realtime enable

【缺省情况】

日志的实时发送功能处于关闭状态，使用缓存方式发送。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

非缺省vSystem不支持本命令。

日志实时发送功能仅对安全策略、对象策略和包过滤模块的日志发送有效。

日志的发送方式支持如下两种：

· 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。

· 实时发送方式：同一数据流的首报文匹配相关策略生成并发送日志后，设备不缓存此日志，因此这种方式无日志数目的限制。对于一条不间断的流量，若匹配的策略允许报文通过，则设备仅发送一次日志，若匹配的策略拒绝报文通过，则设备将对此条数据流的每个报文均发送一次日志。