

知 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:

| 发起方源IP | 发起... | 发起... | 发起... | 接收接口 | 接收... | 发起... | 发起... | 会话... | 创建时间 |
|--------------|-------|-------|-------|------------------|-------|-------|-------|--------|------------------|
| 10.27.79.129 | 13974 | 40763 | VPN:公 | Route-Aggregatio | Trust | 4 | 765 | TCP_ES | 2023-04-03 14:12 |
| 10.27.79.129 | 13997 | 44417 | VPN:公 | Route-Aggregatio | Trust | 4 | 761 | TCP_ES | 2023-04-03 14:12 |
| 10.27.79.129 | 8726 | 46659 | VPN:公 | Route-Aggregatio | Trust | 203 | 85369 | TCP_ES | 2023-04-03 14:12 |
| 10.27.79.129 | 14033 | 38627 | VPN:公 | Route-Aggregatio | Trust | 4 | 765 | TCP_ES | 2023-04-03 14:12 |
| 10.27.79.129 | 13942 | 43278 | VPN:公 | Route-Aggregatio | Trust | 4 | 765 | TCP_ES | 2023-04-03 14:12 |
| 10.27.79.129 | 13971 | 56730 | VPN:公 | Route-Aggregatio | Trust | 4 | 765 | TCP_ES | 2023-04-03 14:12 |
| 10.27.79.215 | 11575 | 80 | VPN:公 | Route-Aggregatio | Trust | 5 | 1192 | TCP_ES | 2023-04-03 14:54 |
| 10.27.79.129 | 13979 | 35234 | VPN:公 | Route-Aggregatio | Trust | 4 | 765 | TCP_ES | 2023-04-03 14:12 |
| 10.27.79.58 | 4802 | 17610 | VPN:公 | Route-Aggregatio | Trust | 305 | 45351 | TCP_ES | 2023-04-03 09:26 |
| 10.27.79.129 | 13902 | 37051 | VPN:公 | Route-Aggregatio | Trust | 4 | 753 | TCP_ES | 2023-04-03 14:12 |
| 10.27.79.129 | 13964 | 53543 | VPN:公 | Route-Aggregatio | Trust | 4 | 765 | TCP_ES | 2023-04-03 14:12 |
| 10.27.79.129 | 13982 | 58953 | VPN:公 | Route-Aggregatio | Trust | 4 | 765 | TCP_ES | 2023-04-03 14:12 |
| 10.27.79.129 | 14036 | 54368 | VPN:公 | Route-Aggregatio | Trust | 4 | 765 | TCP_ES | 2023-04-03 14:12 |

SMP查询结果:

统计周期: 2023-04-03 10:01:32 - 2023-04-03 14:01:32

源IP: 请输入源IP 目的IP: 请输入目的IP 源安全域: 请输入源安全域 目的安全域: 请输入目的安全域 安全策略: 请输入安全策略

规则编号: 60 协议类型: 全部 应用: 请输入应用 源端口: 请输入源端口 目的端口: 请输入目的端口

动作: 全部 匹配规则数量: 请输入匹配规则数量

| 时间 | 源IP | 目的IP | 源安全域 | 目的安全域 | 安全策略 | 规则编号 | 协议类型 | 源端口 | 目的端口 | 匹配规则... | 动作 | 设备名称 | 操作 |
|---------------------|-------------|-------------|-------|---------|----------|------|------|-------|------|---------|----|----------|----|
| 2023-04-03 13:38:45 | 10.27.79... | 10.34.40... | Trust | Untrust | IT办公域... | 60 | TCP | 6989 | 7777 | 1 | 允许 | 1期OA防... | |
| 2023-04-03 12:28:46 | 10.27.79... | 10.34.52... | Trust | Untrust | IT办公域... | 60 | TCP | 5027 | 80 | 1 | 允许 | 1期OA防... | |
| 2023-04-03 11:48:40 | 10.27.79... | 10.20.36... | Trust | Untrust | IT办公域... | 60 | TCP | 1998 | 80 | 1 | 允许 | 1期OA防... | |
| 2023-04-03 11:43:45 | 10.27.79... | 10.34.52... | Trust | Untrust | IT办公域... | 60 | TCP | 1411 | 80 | 1 | 允许 | 1期OA防... | |
| 2023-04-03 11:33:45 | 10.27.79... | 10.20.40... | Trust | Untrust | IT办公域... | 60 | TCP | 8775 | 389 | 1 | 允许 | 1期OA防... | |
| 2023-04-03 11:33:40 | 10.27.79... | 10.34.52... | Trust | Untrust | IT办公域... | 60 | TCP | 12960 | 80 | 1 | 允许 | 1期OA防... | |
| 2023-04-03 11:18:46 | 10.27.79... | 10.34.52... | Trust | Untrust | IT办公域... | 60 | TCP | 8658 | 80 | 1 | 允许 | 1期OA防... | |

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。

