

组网及说明

设备型号和版本: SecCenter CSAP-SA-V E1804P04

问题描述

客户需要将msr56(V5)的日志发给日志审计, 客户昨天想查某一条日志, 没有在日审上找到, 才发现部分nat日志没有回显

过程分析

1、从日志审计上看是有日志产生的

日志产生时间	日志来源	产生日志设备名称	产生日志设备IP	源IP	目的IP	端口	端口
2024-07-19 11:46:16	网络流量日志	外联路由器R6600	10.0.0.5	10.88.141.3	80	31	
2024-07-19 11:46:46	网络流量日志	外联路由器R6600	10.0.0.5	10.0.0.1	80	31	
2024-07-19 11:47:28	网络流量日志	外联路由器R6600	10.0.0.5	10.0.0.1	80	31	
2024-07-19 10:48:55	网络流量日志	外联路由器R6600	10.0.0.5	10.0.0.1	80	31	
2024-07-19 10:48:14	网络流量日志	外联路由器R6600	10.0.0.5	10.0.0.1	80	31	
2024-07-19 10:47:40	网络流量日志	外联路由器R6600	10.0.0.5	10.0.0.1	80	31	
2024-07-19 10:47:26	网络流量日志	外联路由器R6600	10.0.0.5	10.0.0.1	80	31	
2024-07-19 10:47:20	网络流量日志	外联路由器R6600	10.0.0.5	10.0.0.1	80	31	
2024-07-19 10:47:19	网络流量日志	外联路由器R6600	10.0.0.5	10.0.0.1	80	31	
2024-07-19 17:20:01	网络流量日志	外联路由器R6600	10.0.0.5	10.0.0.1	80	31	
2024-07-19 14:44:29	网络流量日志	外联路由器R6600	10.0.0.5	10.0.0.1	80	31	

2、但是在11点46左右后台抓的包, 到现在都没有在日志审计上显示出来

```
userlog.Source=NAT-Port=1668
Time          2024-07-19 11:46:24.573396  Source      10.0.0.5      Destination 10.0.0.1      Protocol     UserLog       Length       1274          Identification 0x581f (22559)  Info         LogType = Flow
2024-07-19 11:47:52.573396  10.0.0.5     10.0.0.1     UserLog      1402          0x5883 (22659)  LogType = Flow

Reserved2: 0
Reserved3: 0
- UserLog No.5
  Protocol: TCP (6)
  Operator: flow create (8)
  IP Version: 4
  IP ToS: 0
  Source-IP: 10.88.141.3
  Source-NAT-IP: 9.1.1.158
  Destination-IP: 9.1.1.1
  Destination-NAT-IP: 9.1.1.131
  Source-Port: 58748
  Source-NAT-Port: 11642
  Destination-Port: 80
  Destination-NAT-Port: 80
  StartTime: Jul 19, 2024 19:46:17.000000000 中国标准时间
  EndTime: Jul 19, 2024 19:46:17.000000000 中国标准时间
  InTotalPkg: 0
  InTotalByte: 0
  OutTotalPkg: 1
  OutTotalByte: 52
  Reserved1: 0
  Reserved2: 0
  Reserved3: 0
- UserLog No.6
```

3、日志审计配置如下:



4、路由器配置如下:

```
#
userlog flow export version 3
userlog flow export timestamps localtime
userlog flow export source-ip 10.10.10.5
userlog flow export slot 3 host 10.10.10.10 30514
#
```

解决方法

经产品线分析：CSAP-SA-V不推荐使用流日志，推荐使用快速日志，流日志只解析日志里的第一条，由于流日志一条里能带一二十条日志，性能没法控制，日志审计-V的版本性能扛不住，比如这条，一条里就带16条日志。

190	170.068702	10.10.10.5	10.10.10.10	UserLog	634 LogType = Flow
199	177.068755	10.10.10.5	10.10.10.10	UserLog	698 LogType = Flow
200	177.346086	10.10.10.5	10.10.10.10	UserLog	1466 LogType = Flow
201	178.068744	10.10.10.5	10.10.10.10	UserLog	442 LogType = Flow
202	179.068776	10.10.10.5	10.10.10.110	UserLog	1274 LogType = Flow
203	180.068729	10.10.10.5	10.10.10.110	UserLog	314 LogType = Flow


```
Frame 78: 1082 bytes on wire (8656 bits), 1082 bytes captured (8656 bits)
Ethernet II, Src: Hangzhou_88:ea:fa (60:0b:03:88:ea:fa), Dst: HuaweiTe_8d:7d:a2 (ac:b3:b5:8d:7d:a2)
Internet Protocol Version 4, Src: 10.10.10.5, Dst: 10.10.10.10
User Datagram Protocol, Src Port: 40000, Dst Port: 30514
UserLog Protocol, Log Count = 16
  > UserLog Header
  > UserLog No.1
  > UserLog No.2
  > UserLog No.3
  > UserLog No.4
  > UserLog No.5
  > UserLog No.6
030  52 4a 00 66 65 c6 00 00 03 00 06 08 04 00 0a 90  RJ-fe...
040  08 32 09 6c 2e 9e 09 6c 2f e7 09 6c 2f e7 9a 56  -2-1...1 /-1/-V
050  2f 45 00 50 00 50 66 9a 52 43 66 9a 52 43 00 00  /E-P-Pf RCF-RC..
060  00 00 00 00 00 00 00 00 00 01 00 00 00 38 00 00  .....8..
```