SecCenter CSAP-SA-V 虚拟日志审计平台 nat日志不全

日志采集器　贾珊珊　2024-09-23 发表

组网及说明

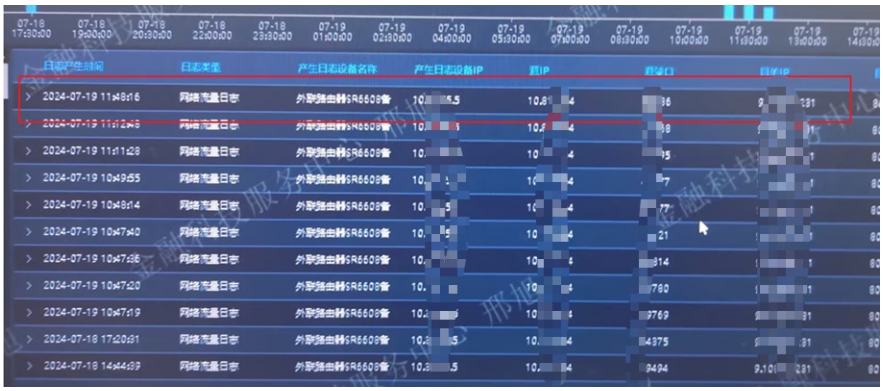
设备型号和版本：SecCenter CSAP-SA-V E1804P04

问题描述

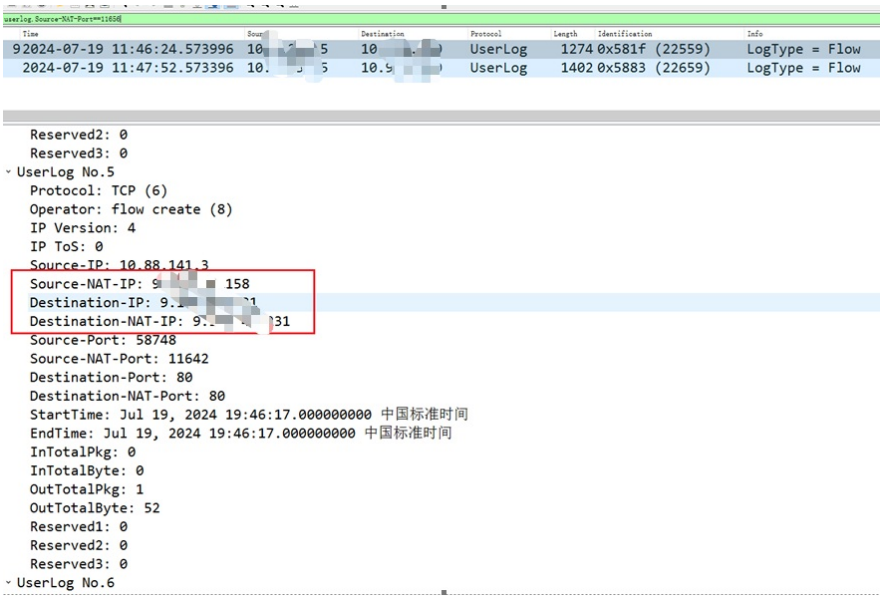
客户需要将msr56(V5)的日志发给日志审计，客户昨天想查某一条日志，没有在日审上找到，才发现部分nat日志没有回显

过程分析

1、 从日志审计上看是有日志产生的



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



```
   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[illegible] 158
   Destination-IP: 9.1[illegible]
   Destination-NAT-IP: 9[illegible]31
   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[illegible]5
 userlog flow export slot 3 host 10[illegible]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。