某局点T1080旁路部署不生效问题处理经验案例

特征库升级 特征库 应用审计 **刘文峰** 2019-09-28 发表

组网及说明

无

问题描述

某局点新增T1080设备想实现对流量进行审计，但是又不想改变现有组网，最后决定旁挂在核心75E交换机上旁路部署，75E上镜像来回的流量上T1080，当前配置完成之后，流量已上到T1080，接口统计有增长，但是看安全策略没命中，也看不到安全日志和应用审计日志，特征库已升级最新，查看配置，跟之前案例配置无差别。参考下面配置：

```
bridge 2 blackhole
 add interface Ten-GigabitEthernet1/0/24
security-zone name inline
 import interface Ten-GigabitEthernet1/0/24 vlan 2
interface Ten-GigabitEthernet1/0/24
 port link-mode bridge
 port access vlan 2
security-policy ip
 rule 0 name 1
  action pass
  logging enable
  counting enable
  profile 0_IPv4
  source-zone inline
  destination-zone inline
```

过程分析

看配置都无任何问题，怀疑还是流量特征问题，远程登入到核心查看镜像的配置，发现75E上是二层转发，镜像上来的报文都是带vlan tag，导致被防火墙的接口（port access vlan 2）给丢弃了，造成旁路部署失败。

解决方法

把防火墙上接收镜像报文的接口改成三层口之后，问题解决。