M9000流镜像剔除部分镜像流失败

包过滤 **徐箫宇** 2022-03-17 发表

组网及说明

M9000做流镜像

问题描述

现场M9000上存在内访外和内访内的流量，现场想对于内访外的流量进行镜像，不想对内访内的流量进行镜像。

由于采用qos策略进行配置流镜像时，ACL里面仅用于匹配流量，ACL中的deny无法剔除流量，所以建议现场采用如下方式进行镜像：

```
traffic classifier neifangnei operator and
if-match acl 3000   //匹配内访内流量
#
traffic classifier neifangwai operator and
if-match acl 3001   //匹配其他所有流量
#
traffic behavior neifangnei
filter permit     //转发
#
traffic behavior neifangwai
mirror-to interface Ten-GigabitEthernet1/1/1/3    //镜像到接口
#
qos policy 1
classifier neifangnei behavior neifangnei
classifier neifangwai behavior neifangwai
 #
interface FortyGigE1/1/1/2
qos apply policy 1 inbound enhancement
qos apply policy 1 outbound enhancement
```

配置完成后，还是能抓取到内网访问内网的流量

过程分析

配置QOS策略，实现内访内的流量匹配QOS的第一个cb对转发，其余流量匹配第二个cb对进行镜像。应该是没有问题。

后续确认，qos中的动作filter permit ,与ACL结合调用outbound方向时，ACL无法下发，实际动作不生效，导致内访内流量仍能匹配第二个cb对进行镜像

解决方法

方法1：将qos策略中的第一个cb对的动作也配置为mirror-to,镜像到一个不使用的接口，down接口也可以。

方法2：不采用outbound方向,在设备流量两端都采用inbound方向下发镜像