某局点 S12510-S 策略路由不生效

策略路由 李鹏飞 2022-04-24 发表

组网及说明

PC------bagg1007(vlan 2017)---核心---(vlan 1003)---1.70

告警信息

不涉及

问题描述

PBR不生效

#
interface Vlan-interface2017
description TO_ERQIHULIAN_FW
ip address 10.152.152.113 255.255.255.248
ip policy-based-route 1
#
#
policy-based-route 1 permit node 10
if-match acl 3500
apply next-hop 10.152.1.70
#
acl advanced 3500
rule 0 permit ip source 10.152.190.246 0
rule 5 permit ip source 10.152.190.247 0
rule 10 permit ip source 10.152.190.248 0
#
interface Vlan-interface1003
description conn:dmzsw
ip address 10.152.1.69 255.255.255.252 下一跳的出接口
#

过程分析

1、远程故障环境查看底层PBR ACL下发情况， ACL底层rule和下一跳下发正常

2、将主机发到设备的报文上送cpu打印出来，查看ICMP报文封装正常；

3、查看软件限速softcar发现ROOT项持续有上送cpu的报文，ROOT限速项包括其他没有在softcar中可匹配到规则的报文，都会归属于ROOT 类型，比如找不到下一跳。ROOT项一直有报文上送cpu，怀疑主机发来的报文被当做无法转发的报文被丢弃

4、查看设备上到报文的目的ip，没有对应的arp表项和路由，且全局配置了ip unreachables enable，配置了ip unreachables enable后，找不到路由的报文都会被上送cpu，S12510-S设备ip unreachables enable优先级比PBR高，导致报文优先被上送cpu丢弃，而导致PBR不生效，但是如果设备上有到目的地址的路由（黑洞路由也行），就会绕过ip unreachables enable流程，走PBR转发流程。

解决方法

芯片限制，软件暂时无法修改。删除ip unreachables enable，或者添加一条默认路由规避。