某局点 S6520X-54XG-EI-G PBR匹配到错误的下一跳

策略路由 刘倩 2021-12-22 发表

组网及说明

不涉及

问题描述

1. 网关vlan241下调用策略路由，node10匹配acl PBR的主机设置下一跳为10.0.0.2，对应公网地址为180.167.254.81；node20匹配acl PBR-2的主机设置下一跳为10.0.0.6，对应公网地址为116.228.89.1。
2. Acl PBR为明细地址，acl PBR-2为大段，两者有重复的部分。

相关配置：

```
#
policy-based-route PBR permit node 10
if-match acl name PBR
apply next-hop 10.0.0.2
#
policy-based-route PBR permit node 20
if-match acl name PBR-2
apply next-hop 10.0.0.6
#

#
interface Vlan-interface241
ip address 10.10.10.1 255.255.0.0
ip address 10.10.9.1 255.255.255.0 sub
packet-filter name DEV-VLAN241 inbound
ip policy-based-route PBR
ipv6 dhcp server apply pool test
ipv6 nd ra prefix 2408:8026:400:C00::/64 no-advertise
ipv6 address 2408:8026:400:C00::2/64
ipv6 address auto
ipv6 nd autoconfig managed-address-flag
ipv6 nd autoconfig other-flag
#

#
ip route-static 0.0.0.0 0 10.0.0.6 preference 250 description TO_ZJ-OA-FW-USG6550_FOR_INTERNET
ip route-static 0.0.0.0 0 10.0.0.2 track 1 description des TO_ZJ-OA-FW-PA3020_FOR_INTERNET
ip route-static 3.3.3.0 24 10.0.0.2
ip route-static 10.111.0.0 16 10.10.10.153
ip route-static 116.228.89.1 32 10.0.0.6
ip route-static 180.167.254.81 32 10.0.0.2
ip route-static 192.168.0.0 22 10.10.10.153
ip route-static 192.168.8.0 24 10.10.10.153
ip route-static 192.168.12.0 24 10.10.10.153
ip route-static 192.168.50.0 24 10.10.10.230
ipv6 route-static :: 0 2408:8026:400:C00::1
#

#
acl advanced name PBR
rule 0 permit ip source 10.10.30.41 0
rule 5 permit ip source 10.10.9.53 0
rule 10 permit ip source 10.10.20.210 0
rule 15 permit ip source 10.10.31.250 0
rule 20 permit ip source 10.10.21.49 0
rule 25 permit ip source 10.10.20.157 0
rule 30 permit ip source 10.10.20.158 0
rule 35 permit ip source 10.10.20.200 0
rule 40 permit ip source 10.10.30.15 0
rule 45 permit ip source 10.10.30.10 0
rule 50 permit ip source 10.10.11.56 0
rule 55 permit ip source 10.10.10.35 0
```

rule 60 permit ip source 10.10.20.242 0
rule 65 permit ip source 10.10.20.243 0
rule 70 permit ip source 10.10.11.120 0
rule 75 permit ip source 10.10.20.19 0
rule 80 permit ip source 10.10.30.30 0
rule 85 permit ip source 10.10.21.40 0
rule 90 permit ip source 10.10.20.242 0
#
rule 95 permit ip source 10.10.30.130 0
rule 100 permit ip source 10.10.21.50 0
rule 105 permit ip source 10.10.20.121 0
rule 110 permit ip source 40.40.32.14 0
#
packet-filter name DEV-VLAN241 inbound
#
ipv6 policy-based-route PBR
#
ipv6 dhcp select server
ipv6 dhcp server apply pool test
#
ipv6 dhcp server allow-hint preference 255 rapid-commit
#
acl advanced name PBR-2
rule 0 permit ip source 10.10.0.0 0.0.255.255
rule 5 permit ip source 10.0.0.0 0.255.255.255
#
ipv6 nd autoconfig other-flag
#
interface Vlan-interface241
ip address 10.10.10.1 255.255.255.0
ip address 10.10.9.1 255.255.255.0 sub
ipv6 address 2408:8226:420:C00::2/64
ipv6 address auto
ipv6 nd autoconfig managed-address-flag
ipv6 nd autoconfig other-flag
#
acl advanced name DEV-VLAN241
rule 0 permit ip destination 10.197.18.3 0
rule 5 permit ip destination 10.197.18.131 0
rule 10 permit ip destination 10.197.18.15 0
rule 15 permit ip source 10.10.21.111 0 destination 10.197.0.0 0.0.255.255
rule 20 permit ip source 10.10.20.103 0 destination 10.197.18.58 0
rule 25 permit ip source 10.10.22.49 0 destination 10.197.0.0 0.0.255.255
rule 30 permit ip source 10.10.22.50 0 destination 10.197.0.0 0.0.255.255
rule 35 permit ip source 10.10.10.250 0 destination 10.197.0.0 0.0.255.255
rule 40 permit ip source 10.10.21.125 0 destination 172.22.24.0 0.0.0.255
rule 45 permit ip source 10.10.21.125 0 destination 10.197.0.0 0.0.255.255
rule 50 permit ip source 10.10.10.250 0 destination 172.22.24.0 0.0.0.255
rule 55 permit ip source 10.10.20.164 0 destination 10.197.0.0 0.0.255.255
rule 60 permit ip source 10.10.20.210 0 destination 172.22.24.0 0.0.0.255
rule 65 permit ip source 10.10.20.164 0 destination 10.197.0.0 0.0.255.255
rule 70 permit ip source 10.10.20.164 0 destination 172.22.24.0 0.0.0.255
rule 75 permit ip source 10.10.30.130 0 destination 10.197.0.0 0.0.255.255
rule 80 permit ip source 192.168.0.25 0 destination 10.197.0.0 0.0.255.255
rule 85 deny ip destination 172.22.0.0 0.0.255.255
rule 90 deny ip destination 10.197.0.0 0.0.255.255
rule 95 permit ip
#

过程分析

与这个包过滤配置有关，包过滤优先级高级PBR，而XC设备当前只支持一次查找匹配，无法像75E、105一样并行查找，这样优先会匹配包过滤，匹配包过滤后就无法再匹配PBR了。

包过滤没有匹配的报文默认就是放行的，rule 95 permit ip可以不用配。

3、用PBR-2大段内测试主机，地址为10.10.30.129，做ping外网操作后，PBR对应node20的匹配数+1，但是trace外网发现路由走的是10.0.0.2

解决方法

包过滤没有匹配的报文默认就是放行的，rule 95 permit ip可以不用配。