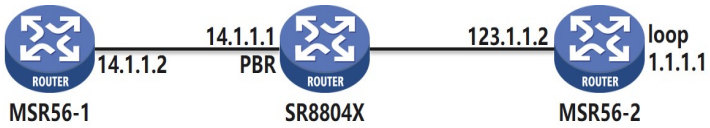
SR8808X策略路由acl匹配规则经验案例

ACL 郭昊 2019-10-31 发表

组网及说明



SR8804X做PBR，其本身没有到1.1.1.1的路由，对MSR56-1 ping 1.1.1.1的流量，SR8804X按照PBR转发至MSR56-2。

问题描述

SR8804X等硬件设备，PBR的acl匹配处理规则与MSR等软件设备有区别，对于acl rule deny的处理容易存在歧义。此案例列举几个典型配置场景及对应测试情况，分别对应R7655P12、R7951P04版本，下发PBR的接口所在板卡为CSPEX-1404S。

过程分析

1. **SR88X使用R7655P12版本**

A.

```
#
acl advanced 3000
 rule 5 deny ip
#
policy-based-route 1 permit node 10
 if-match acl 3000
 apply next-hop 123.1.1.2
#
[MSR5660-1]ping 1.1.1.1
Ping 1.1.1.1 (1.1.1.1): 56 data bytes, press CTRL_C to break
Request time out
======>说明流量不会被deny ip匹配到，不会因为被deny执行permit node动作
```

B.

```
#
acl advanced 3000
 rule 5 deny ip
 rule 10 permit ip
#
policy-based-route 1 permit node 10
 if-match acl 3000
 apply next-hop 123.1.1.2
#
<MSR5660-1>ping 1.1.1.1
Ping 1.1.1.1 (1.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.1.1: icmp_seq=0 ttl=254 time=0.710 ms
========>对同一个acl，流量会从上向下检查，即使先匹配到deny，还是会被后面permit ip匹配到，并执行对应的permit node动作
```

C.

```
#
acl advanced 3000
 rule 5 deny ip
#
acl advanced 3001
 rule 5 permit ip
#
policy-based-route 1 permit node 10
 if-match acl 3000
 apply next-hop 123.1.1.3
```

#
policy-based-route 1 permit node 20
 if-match acl 3001
 apply next-hop 123.1.1.2
#
<MSR5660-1>ping 1.1.1.1
Ping 1.1.1.1 (1.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.1.1: icmp_seq=0 ttl=254 time=0.668 ms
=======>流量不会因为node 10的acl deny而跳出pbr，也不认为匹配到node 10而执行node 10。会继续向下检查是否匹配到其他node。

D.
#
acl advanced 3000
 rule 5 deny ip
#
acl advanced 3001
 rule 5 permit ip
#
policy-based-route 1 deny node 10
 if-match acl 3000
#
policy-based-route 1 permit node 20
 if-match acl 3001
 apply next-hop 123.1.1.2
#
<MSR5660-1>ping 1.1.1.1
Ping 1.1.1.1 (1.1.1.1): 56 data bytes, press CTRL_C to break
Request time out

#
acl advanced 3000
 rule 0 permit ip
#
acl advanced 3001
 rule 5 permit ip
#
policy-based-route 1 deny node 10
 if-match acl 3000
#
policy-based-route 1 permit node 20
 if-match acl 3001
 apply next-hop 123.1.1.2
#
<MSR5660-1>ping 1.1.1.1
Ping 1.1.1.1 (1.1.1.1): 56 data bytes, press CTRL_C to break
Request time out
======>对于deny node，无论acl是permit ip还是deny ip，都认为匹配到了deny node，跳出pbr。

1. **SR88X使用R7951P04版本**
   上述ABC三种配置下，R7951P04与R7655P12结果一致，不赘述。
   R7951P04对应上面D配置情况如下，
   #
   acl advanced 3000
    rule 5 deny ip
   #
   acl advanced 3001
    rule 5 permit ip
   #
   policy-based-route 1 deny node 10
    if-match acl 3000
   #
   policy-based-route 1 permit node 20

```
 if-match acl 3001
 apply next-hop 123.1.1.2
#
<MSR5660-1>ping -c 1 1.1.1.1
Ping 1.1.1.1 (1.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.1.1: icmp_seq=0 ttl=254 time=0.581 ms


#
acl advanced 3000
 rule 0 permit ip
#
acl advanced 3001
 rule 5 permit ip
#
policy-based-route 1 deny node 10
 if-match acl 3000
#
policy-based-route 1 permit node 20
 if-match acl 3001
 apply next-hop 123.1.1.2
#
<MSR5660-1>ping 1.1.1.1
Ping 1.1.1.1 (1.1.1.1): 56 data bytes, press CTRL_C to break
Request time out
```

==========>对于deny node，需要acl permit到这个流量，才会认为匹配到deny node，并跳出pbr。

解决方法

综上，如果需求为“特定流量不走PBR，其他流量走PBR”，建议配置pbr deny node + acl rule permit，逻辑上不容易出错。