MSR、SR设备 如何用QOS和包过滤做过滤

ACL QoS packet-filter 刘安娜 2023-02-20 发表

问题描述

现场允许1.1.1.0/24访问2.2.2.0/24，不允许1.1.1.0/24访问其他网段

解决方法

1、QOS方式：

```
acl advanced 3000
rule 0 permit ip source 1.1.1.0 0.0.0.255 destination 2.2.2.0 0.0.0.255 ///与traffic behavior 1联动，匹配允许访问的地址
#
acl advanced 3001
rule permit ip     ///与traffic behavior 2联动，匹配不允许访问的地址
#
traffic classifier 1 operator and
if-match acl 3000
#
traffic classifier 2 operator and
if-match acl 3001
#
traffic behavior 1
filter permit
#
traffic behavior 2
filter deny
#
qos policy 1
classifier 1 behavior 1  ///匹配acl 3000中的地址，允许访问
classifier 2 behavior 2  ///匹配acl 3001中的地址，不允许访问
#
interface GigabitEthernet0/2
qos apply policy 1 inbound  //在接口入方向调用qos policy
#
```

2、包过滤：

```
acl advanced 3000
rule 0 permit ip source 1.1.1.0 0.0.0.255 destination 2.2.2.0 0.0.0.255
rule 5 deny ip source 1.1.1.0 0.0.0.255
#
interface GigabitEthernet0/2
packet-filter 3000 inbound
```

3、qos和包过滤对于acl的定义不同

（1）qos中，当if-match中引用的ACL规则的动作为deny时，将不执行任何动作，及流量不匹配qos，正常转发。acl deny在qos中应用较少，对于多种过滤规则的报文，建议如上，acl规则都写permit，匹配多个CB对，采取不同的动作。

（2）packet-filter 对于acl允许permit的流量，放通；acl中deny的动作deny掉。