跨域VPN-OptionC组网如何实现ip报文过滤

MPLS L3VPN QoS ACL 刘安娜 2023-03-10 发表

问题描述

在跨域VPN-OptionC组网中，SR88设备作为PE设备，如何控制终端间的访问？

示例：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

目前较新的高端路由器版本已支持入方向匹配MPLS内层IP功能，可以直接配置QOS执行对应动作

```
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 mpls-inner   ///匹配MPLS报文的内层报文信息
#
traffic classifier 2 operator and
if-match acl 3001 mpls-inner   ///匹配MPLS报文的内层报文信息
#
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
#
```

mpls-inner：用来指定ACL规则用于匹配MPLS报文的内层报文信息，未配置mpls-inner则表示ACL规则匹配的是未经过封装报文的信息或封装后的MPLS报文的外层报文头信息，此配置仅满足以下条件时生效：

1.匹配IPV4高级ACL规则

2.QOS策略应用在MPLS网络Transit或者Egress节点接口的入方向上

3.配置在CSPEX类单板（CSPEX-1204除外），SPE类单板和CEPC类单板上