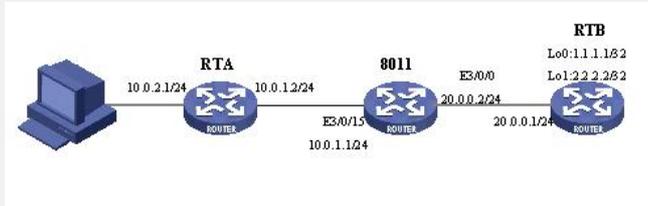


NE80/NE40/S8016产品VRP5.3版本访问控制功能的配置

一、组网需求:

在8011的E3/0/15接口入方向做访问控制,使RTA能ping通RTB的Loopback0接口地址1.1.1.1,但不能ping通RTB的Loopback1接口地址2.2.2.2

二、组网图:



RTA和RTB可以为任意路由器或三层交换机,8011为需要实现访问控制功能的NE80/NE40/S8016设备。8011上VRP软件版本为5.3

配置步骤:

1. 组网并完成各路由器上的OSPF配置,在OSPF中发布所有接口,包括物理接口和Loopback接口的路由。
2. 在8011上配置EACL,在E3/0/15接口入方向做访问控制,使RTA能ping通RTB的Loopback0接口地址1.1.1.1,但不能ping通RTB的Loopback1接口地址2.2.2.2。配置命令如下:

- 1) 创建流分类permit,定义允许通过的流
[8011]acl number 10000
[8011-acl-simple-10000]rule ip source any destination 1.1.1.1 0.0.0.0
[8011]traffic classifier permit
[8011-classifier-permit]if-match acl 10000
 - 2) 创建流分类deny,定义不允许通过的流
[8011]acl number 10001
[8011-acl-simple-10001]rule ip source any destination 2.2.2.2 0.0.0.0
[8011]traffic classifier deny
[8011-classifier-deny]if-match acl 10001
 - 3) 创建流行为permit,并指定行为为允许流通过
[8011]traffic behavior permit
[8011-behavior-permit]permit
 - 4) 创建流行为deny,并指定行为为禁止流通过
[8011]traffic behavior deny
[8011-behavior-deny]deny
 - 5) 创建流策略filter,将流分类与流行为绑定,允许流permit通过,禁止流deny通过
[8011]traffic policy filter
[8011-trafficpolicy-filter]classifier permit behavior permit
[8011-trafficpolicy-filter]classifier deny behavior deny
 - 6) 进入相应端口视图并在该端口应用流策略
[8011]interface Ethernet 3/0/15
[8011-Ethernet3/0/15]traffic-policy filter inbound vlan all
 - 7) 在全局激活流策略
[8011]commit traffic policy
3. 从RTA上ping路由器RTB的Loopback接口地址1.1.1.1和2.2.2.2,结果可以ping通1.1.1.1,而不能ping通2.2.2.2

三、配置关键点:

配置过程有5步:先创建acl定义各条需要进行过滤的流,并把acl和traffic classifier绑定定义需要过滤的流分类;再创建traffic behavior定义需要进行的操作;然后创建traffic policy将流分类和相应的流行为绑定起来,形成完整的针对不同流的流处理策略;接着将定义好的traffic policy在相应端口应用;最后,不要忘了在全局提交激活流策略。