MSR路由器下发二层ACL的经验案例

马文斌 2013-10-22 发表

MSR路由器下发二层ACL的经验案例

一、 组网：

公司只允许源MAC地址为000f-e2e5-0b70的PC机上公网，携带其他源MAC地址的报文一律不允许通过。

PC连接RTA的Interface Vlan 1接口，RTA的G0/1接口连接公网。

使用版本：R2508-SI

二、 问题描述：

在interface vlan-interface接口上配置firewall packet-filter *INTEGER<4000-4999>* {inbound|outbound}命令，发现PC其他PC依然能够通过RTA上公网，需求没有实现。

然后还可以使用CBQ的方法来配置，在流分类中调用二层ACL，然后通过在接口上下发qos策略，但是下发后却发现策略不生效，其他PC依然能够通过RTA上公网，需求没有实现。

三、 过程分析：

防火墙包过滤方法：

在三层接口上使用防火墙包过滤下发二层ACL时，必须要使用firewall ethernet-frame-filter *INTEGER<4000-4999>* {inbound|outbound}，直接使用firewall packet-filter *INTEGER<4000-4999>* {inbound|outbound}虽然命令可以下发成功，但是此命令只能调用标准的ACL（2000-3999），无法调用二层ACL(4000-4999)，所以二层包过滤会出现不生效的情况。

在以上组网中，内网口采用的是interface vlan接口，在interface vlan-interface接口上无法下发firewall ethernet-frame-filter命令，导致二层ACL无法通过防火墙包过滤的方法下发到interface vlan-interface接口上；

CBQ方法：

在流分类（traffic classifier）中调用二层ACL，然后在动作中设置相应的permit/deny动作，但是CBQ方式虽然可以在接口下发，但是却无法生效，原因为CBQ方法无法直接调用二层ACL，导致流量无法匹配到相应的ACL，所以配置不生效。

四、 解决方法：

遇到如上组网方式，需要在路由器的interface vlan-interface接口上做MAC地址过滤，只能使用CBQ的方法，而且必须使用如下配置：

[H3C]traffic classifier 1

[H3C-classifier-1]if-match source-mac 0001-0001-0001

因为CBQ方式无法直接调用二层ACL，所以匹配流中不能匹配二层ACL，只能够使用如上方式，在匹配流中直接调用MAC地址，这样就可以起到限制MAC地址的效果了。

附：完整配置：

[H3C]traffic classifier 1

[H3C-classifier-1]if-match source-mac 0001-0001-0001

[H3C-classifier-1]quit

[H3C]traffic behavior 1

[H3C-behavior-1]filter deny

[H3C-behavior-1]quit

[H3C]qos policy 1

[H3C-qospolicy-1]classifier 1 behavior 1

[H3C-qospolicy-1]qu

[H3C]interface vlan-interface 1

[H3C-Vlan-interface1]qos apply policy 1 inbound