S3610_S5510系列交换机IPv4 ACL的配置

陈玉龙 2007-05-25 发表

S3610_S5510系列交换机IPv4 ACL的配置

一　组网需求：

在端口Ethernet1/0/2配置IPv4报文过滤，允许源地址为1.0.0.0/8的报文通过，但是禁止源地址为1.1.1.1的报文通过。

二　组网图：

无

三　配置步骤：

1. 配置IPv4 ACL

进入系统视图

<Switch> system-view

配置源地址为1.1.1.1的访问规则

[Switch] acl number 3001

[Switch-acl6-adv-3001] rule deny ip source 1.1.1.1 0

配置其他源地址的访问规则

[Switch] acl number 3002

[Switch-acl6-adv-3002] rule permit ip source 1.0.0.0 0.255.255.255

2. 配置端口Ethernet1/0/1入方向的IPv4报文过滤

配置拒绝接收源地址为1.1.1.1报文的类和流行为

[Switch] traffic classifier 1

[Switch-classifier-1] if-match acl 3001

[Switch-classifier-1] quit

[Switch] traffic behavior 1

[Switch-behavior-1] filter deny

[Switch-behavior-1] quit

配置允许其他源地址的类和流行为

[Switch] traffic classifier 2

[Switch-classifier-2] if-match acl 3002

[Switch-classifier-2] quit

[Switch] traffic behavior 2

[Switch-behavior-2] filter permit

[Switch-behavior-2] quit

配置策略

[Switch] qos policy test

[Switch-qospolicy-test] classifier 1 behavior 1

[Switch-qospolicy-test] classifier 2 behavior 2

[Switch-qospolicy-test] quit

应用策略

[Switch] interface Ethernet 1/0/1

[Switch-Ethernet1/0/2] qos apply policy test inbound

四　配置关键点：

1.　ACL最终的匹配动作是permit还是deny，不由ACL中rule的动作决定，而是由此ACL所对应的behavior的动作决定的。

2.　对于既有permit又有deny要求的访问控制，必须规定两个behavior，一个为permit，一个为deny。