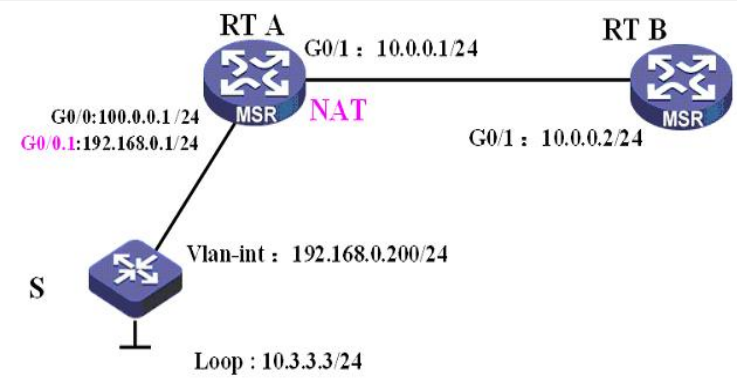
MSR系列路由器子接口启用防火墙的典型配置

姚忆斌　2007-07-17 发表

MSR系列路由器
子接口启用防火墙的典型配置

关键字：MSR; 子接口; 防火墙

一、组网需求：
RT A与交换机通过子接口相连，并在RT A的G0/1接口上使能NAT，要求在路由器内网接口上使能防火墙功能，以保证
交换机下挂设备禁止访问RT B。
设备清单：MSR系列路由器2台；三层交换机1台
二、组网图：



三、配置步骤：
适用设备和版本：MSR系列、Version 5.20, Release 1205P01后所有版本。

交换机S的配置

```
#
 sysname Switch
#
vlan 1
#
vlan 200

//创建Vlan-interface 200,用于与路由器通信

#
interface Vlan-interface200
 ip address 192.168.0.200 255.255.255.0
#
interface Ethernet1/0/1
... ...

//与RT A连接的接口，设置为Trunk

#
interface Ethernet1/0/34
 port link-type trunk
 port trunk permit vlan all
#
interface Ethernet1/0/35
#
... ...
#
//创建LoopBack口，模拟交换机下挂设备

interface LoopBack1
 ip address 10.3.3.3 255.255.255.255
#
 ip route-static 0.0.0.0 0.0.0.0 192.168.0.1 preference 60
#
return
```

RT A的配置

```
#
 sysname H3C
#

//打开MSR的防火墙功能，缺省为关闭

 firewall enable
#
vlan 1
#
acl number 2000
 rule 0 permit
#

//建立过滤ACL，匹配从交换机下挂设备发出的到RT B的报文

acl number 3100
 rule 0 deny ip source 10.3.3.0 0.0.0.255 destination 10.0.0.0 0.0.0.255
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 100.0.0.1 255.255.255.0
#

//在与交换机相连的子接口上使能包过滤防火墙

interface GigabitEthernet0/0.1
 vlan-type dot1q vid 200
 firewall packet-filter 3100 inbound
 ip address 192.168.0.1 255.255.255.0
#
interface GigabitEthernet0/1
 port link-mode route
 nat outbound 2000
 ip address 10.0.0.1 255.0.0.0
#
 ip route-static 10.3.3.0 255.255.255.0 192.168.0.200
#
return
```

RT B的配置仅包含接口地址和缺省路由，此处略去。

四、配置关键点:

1) 系统缺省情况下为禁止防火墙firewall disable，需要使用命令“firewall enable”来使能防火墙功能。

2) 注意在接口上配置流量过滤时方向的配置，Inbound和Outbound不能搞混。