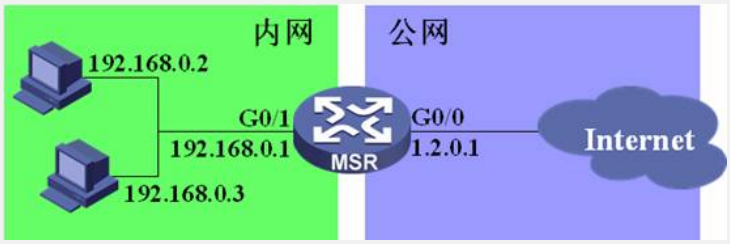
MSR系列路由器NAT连接数限制功能的配置

丘子隽 2008-01-04 发表

MSR系列路由器
NAT连接数限制功能的配置

关键字：MSR; NAT; Connection-limit; 连接数限制

一、**组网需求**：
MSR作为出口NAT路由器，对内部主机192.168.0.3作最多2个NAT会话限制，对192.168.0.2作缺省最多1个NAT会话限制，其余主机不作限制。
设备清单：MSR系列路由器1台
二、组网图：



三、配置步骤：

MSR配置

```
#
 //使能连接限制，必须配置
 connection-limit enable
 //对缺省连接数量上限配置为1，下限为0，达到上限后开始限制，只有达到下限后才允许新建会话
 connection-limit default amount upper-limit 1 lower-limit 0
#
//定义连接限制策略，索引0
connection-limit policy 0
 //对匹配ACL2000的数据流采用缺省连接限制，即上限1，下限0
 limit 0 acl 2000
 //对匹配ACL2001的数据流采用上限2，下限1的会话数量限制
 limit 1 acl 2001 per-source amount 2 1
#
//定义各ACL，其中ACL2002用于NAT转换，2000和2001用于连接限制
acl number 2000
 rule 0 permit source 192.168.0.2 0
acl number 2001
 rule 0 permit source 192.168.0.3 0
acl number 2002
 rule 0 permit source 192.168.0.0 0.0.0.255
#
//连接公网接口配置
interface GigabitEthernet0/0
 port link-mode route
 ip address 1.2.0.1 255.255.255.0
 nat outbound 2002
#
//连接内网接口配置
interface GigabitEthernet0/1
 port link-mode route
 ip address 192.168.0.1 255.255.255.0
#
 //路由配置
 ip route-static 0.0.0.0 0.0.0.0 1.2.0.254
#
 //使能NAT的连接限制，即指定一个策略索引
 nat connection-limit-policy 0
#
```

四、**配置关键点**：
1) 必须要使能connection-limit；
2) 如果不配置connection-limit default amout，那么该例中对策略0的ACL 2000不作限制；
3) 必须要定义connection-limit policy，因为NAT连接限制必须指定策略；
4) 如果连接限制策略中如果只指定ACL，不对per-source、per-destination、per-service进行指定则采取connection-limit default进行限制，如果connection-limit没有配置，则不作限制；
5) 如果连接限制策略中对ACL进行了进一步per-source、per-destination、per-service

的限制，则以此配置为准而不采取connection-limit default限制；
6) 如果不符合连接限制策略的ACL匹配，则不做限制；
7) NAT中必须指定连接限制策略，否则任何限制不生效。