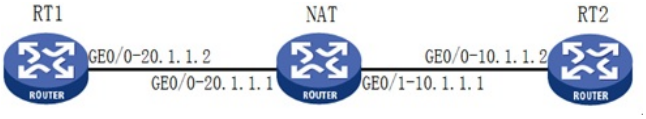
MSR V7双向NAT的典型配置一

NAT 马文斌 2015-10-26 发表

一、 组网需求：

某客户内网有一台RT1设备，需要作为telnet服务器向外网提供telnet服务器，在出口有一台MSR3620设备作为NAT设备，要求外网设备RT2在访问RT1的telnet服务时，MSR3620需要将RT2发过来的报文的源地址和目的地址都要做转换，即RT1不能感知到RT2的公网地址，RT2也不能知道RT1的私网地址。

二、 组网图：



三、 配置步骤：

要实现这种需求，可以使用外网口配置nat server，内网口配置nat outbound的方法。

RT1的配置：

```
#
 sysname RT1
#
 telnet server enable  //开启telnet服务
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 20.1.1.2 255.255.255.0
#
line vty 0 63
 authentication-mode scheme //设置登陆方式为用户名/密码方式
 user-role network-operator
#
 ip route-static 0.0.0.0 0 20.1.1.1
#
#
local-user admin class manage  //创建登陆用户名/密码，这里都是admin
 password hash $h$6$JLVQjDsBXo7KVeFn$0gxWZyKDHIAWTpfvTWdA9J1/78mCUuaO6yB18YE+tV6wMui3SBJsBrZtl/gbqDt8qzgyKL9PZNBYALbe1DP2Aw==
 service-type telnet  //用户服务类型为telnet
 authorization-attribute user-role network-admin  //赋予用户最高权限
```

RT2的配置：

```
sysname RT2
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 10.1.1.2 255.255.255.0
#
```

ip route-static 0.0.0.0 0 10.1.1.1

NAT的配置:

sysname NAT

#

interface GigabitEthernet0/0 //连接RT1的内网口

port link-mode route

combo enable copper

ip address 20.1.1.1 255.255.255.0

nat outbound 3000 address-group 1 //下发nat outbound，关联acl和地址池

#

interface GigabitEthernet0/1 //连接RT2的外网口

port link-mode route

combo enable copper

ip address 10.1.1.1 255.255.255.0

//下发nat server使用的对外地址和端口为2.2.2.2 2323，映射内网的20.1.1.2 23端口

nat server protocol tcp global 2.2.2.2 2323 inside 20.1.1.2 23

#

acl advanced 3000 //配置内网口nat outbound使用的acl

rule 0 permit tcp destination-port eq telnet //匹配目的端口为telnet的端口的报文

#

nat address-group 1 //nat outbound关联的地址池

address 1.1.1.1 1.1.1.10

【验证】

在RT2上telnet 2.2.2.2可以登录到RT1上

telnet 2.2.2.2 2323

Trying 2.2.2.2 ...

Press CTRL+K to abort

Connected to 2.2.2.2 ...

****

* Copyright (c) 2004-2014 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *

* Without the owner's prior written consent, *

* no decompiling or reverse-engineering shall be allowed. *

****

login: admin //输入用户名/密码：admin/admin

Password:

//登录到RT1设备上

NAT上开启deb：

The current terminal is enabled to display logs.

*Oct 15 13:00:42:411 2015 NAT NAT/7/COMMON:

//RT2报文发到MSR3620的G0/1接口匹配nat server转换目的地址和端口

PACKET: (GigabitEthernet0/1-in) Protocol: TCP

10.1.1.2:42308 - 2.2.2.2: 2323(VPN: 0) ------>

10.1.1.2:42308 - 20.1.1.2: 23(VPN: 0)

*Oct 15 13:00:42:412 2015 NAT NAT/7/COMMON:

//G0/0接口匹配nat outbound 3000转换源地址和端口

PACKET: (GigabitEthernet0/0-out) Protocol: TCP

10.1.1.2:42308 - 20.1.1.2: 23(VPN: 0) ------>

1.1.1.5: 1027 - 20.1.1.2: 23(VPN: 0)

*Oct 15 13:00:42:412 2015 NAT NAT/7/COMMON:

//RT1回复报文发到MSR3620的G0/0接口匹配nat会话转换目的地址

PACKET: (GigabitEthernet0/0-in) Protocol: TCP

20.1.1.2: 23 - 1.1.1.5: 1027(VPN: 0) ------>

20.1.1.2: 23 - 10.1.1.2:42308(VPN: 0)

*Oct 15 13:00:42:412 2015 NAT NAT/7/COMMON:

//G0/0收到RT1的回复报文，匹配nat会话，将源地址转换回来

PACKET: (GigabitEthernet0/1-out) Protocol: TCP

20.1.1.2: 23 - 10.1.1.2:42308(VPN: 0) ------>

2.2.2.2: 2323 - 10.1.1.2:42308(VPN: 0)

在NAT设备上查看nat会话表项：

display nat session verbose

Slot 0:

Initiator: //初始地址为10.1.1.2：42309通过G0/1访问2.2.2.2:2323

Source IP/port: 10.1.1.2/42309

Destination IP/port: 2.2.2.2/2323

DS-Lite tunnel peer: -

VPN instance/VLAN ID/VLL ID: -/-/-

Protocol: TCP(6)

Inbound interface: GigabitEthernet0/1

Responder: //回应地址为20.1.1.2:23通过G0/0响应1.1.1.5:1208

Source IP/port: 20.1.1.2/23

Destination IP/port: 1.1.1.5/1028

DS-Lite tunnel peer: -

VPN instance/VLAN ID/VLL ID: -/-/-

Protocol: TCP(6)

Inbound interface: GigabitEthernet0/0

State: TCP_ESTABLISHED

Application: OTHER

Start time: 2015-10-15 13:15:55 TTL: 3590s

Initiator->Responder: 0 packets 0 bytes

Responder->Initiator: 0 packets 0 bytes

Total sessions found: 1 //当前共一条会话

四、 配置关键点：

1、外网口的nat server中的global地址可以写成当前接口地址，也可以写成其他地址。

2、建议内网口的nat outbound要关联acl，精确控制需要转换的报文

3、V7上使用这种配置方法，不需要关闭快转，这点和V5设备不一致