

知 SR8800-X NAT典型配置

NAT 陈丹威 2015-08-13 发表

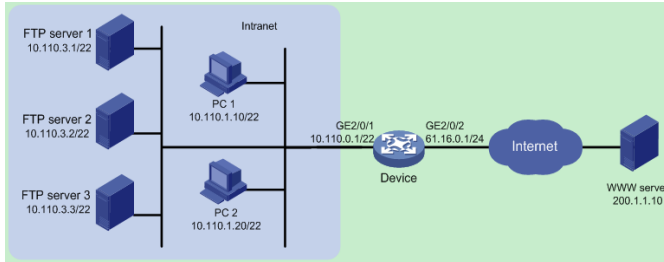
某公司内网地址是10.110.0.0/22，向运营商申请的公网地址是61.16.0.1~61.16.0.3。公司内网用户使用10.110.0.0~10.110.2.255地址段内IP地址；公司内网目前共有3台FTP服务器可以同时提供服务，服务器使用10.110.3.1~10.110.3.3的IP地址。

要求实现如下功能：

内网用户经过地址转换后使用61.16.0.2~61.16.0.3公网地址访问Internet；

外网主机和内网主机都可以通过61.16.0.1访问内网中的FTP服务器；

3台FTP服务器提供服务时进行负载分担，但不允许主动访问外网。



为了实现10.110.0.0~10.110.2.255可以转换成61.16.0.2~61.16.0.3公网地址访问Internet，需要定义ACL规则，实现只对内网匹配指定的ACL规则的报文在Device的GigabitEthernet2/0/2出方向上进行动态地址转换。

为了保证3台FTP服务器同时提供服务，需要配置NAT内部服务器组，并采用负载分担方式。

为了实现内网用户也可以使用61.16.0.1地址访问FTP服务器，需要在Device的GigabitEthernet2/0/1上使能NAT hairpin功能。

1.1 配置步骤

1. 配置接口IP地址

配置接口GigabitEthernet 2/0/1和GigabitEthernet 2/0/2的IP地址。

system-view

[Device] interface gigabitethernet 2/0/1

[Device-GigabitEthernet2/0/1] ip address 10.110.0.1 255.255.252.0

[Device-GigabitEthernet2/0/1] quit

[Device] interface gigabitethernet 2/0/2

[Device-GigabitEthernet2/0/2] ip address 61.16.0.1 255.255.255.0

[Device-GigabitEthernet2/0/2] quit

2. 配置内网用户访问外网

配置地址组0，包含两个外网地址61.16.0.2和61.16.0.3。

[Device] nat address-group 0

[Device-nat-address-group-0] address 61.16.0.2 61.16.0.3

[Device-nat-address-group-0] quit

配置ACL 2000，仅允许对内部网络中10.110.0.0~10.110.2.255网段的用户报文进行地址转换。

[Device] acl number 2000

[Device-acl-basic-2000] rule permit source 10.110.0.0 0.0.1.255

[Device-acl-basic-2000] rule permit source 10.110.2.0 0.0.0.255

[Device-acl-basic-2000] quit

在接口GigabitEthernet2/0/2上配置出方向动态地址转换，允许使用地址组0中的地址对匹配ACL 2000的报文进行源地址转换，并在转换过程中使用端口信息。

[Device] interface gigabitethernet 2/0/2

[Device-GigabitEthernet2/0/2] nat outbound 2000 address-group 0

[Device-GigabitEthernet2/0/2] quit

3. 配置FTP服务器同时提供服务

配置内部服务器组0及其成员10.110.3.1、10.110.3.2和10.110.3.3。

[Device] nat server-group 0

[Device-nat-server-group-0] inside ip 10.110.3.1 port 21

[Device-nat-server-group-0] inside ip 10.110.3.2 port 21

[Device-nat-server-group-0] inside ip 10.110.3.3 port 21

```
[Device-nat-server-group-0] quit
```

在接口GigabitEthernet2/0/2上配置负载均衡分担内部服务器，引用内部服务器组0，该组内的主机共同提供FTP服务。

```
[Device] interface gigabitethernet 2/0/2
```

```
[Device-GigabitEthernet2/0/2] nat server protocol tcp global 61.16.0.1 ftp inside server-group 0
```

在接口GigabitEthernet2/0/1上使能NAT hairpin功能。

```
[Device] interface gigabitethernet 2/0/1
```

```
[Device-GigabitEthernet2/0/1] nat hairpin enable
```

4. 指定提供NAT服务的业务板

在接口GigabitEthernet2/0/1上指定4号单板为提供NAT服务的业务板。

```
[Device-GigabitEthernet2/0/1] nat service slot 4
```

```
[Device-GigabitEthernet2/0/1] quit
```

在接口GigabitEthernet2/0/2上指定4号单板为提供NAT服务的业务板。

```
[Device] interface gigabitethernet 2/0/2
```

```
[Device-GigabitEthernet2/0/2] nat service slot 4
```

```
[Device-GigabitEthernet2/0/2] quit
```

5. 配置QoS重定向策略将符合条件的报文重定向到4号单板

配置重定向报文的访问控制列表2001。由于本例中重定向到提供NAT服务的业务板的报文为需要地址转换的报文，因此ACL 2001中定义的ACL规则与ACL 2000相同，但也可以根据实际组网需求定义不同的规则。

```
[Device] acl number 2001
```

```
[Device-acl-basic-2001] rule permit source 10.110.0.0 0.0.1.255
```

```
[Device-acl-basic-2001] rule permit source 10.110.2.0 0.0.0.255
```

```
[Device-acl-basic-2001] quit
```

创建流分类1，匹配ACL 2001

```
[Device] traffic classifier 1
```

```
[Device-classifier-1] if-match acl 2001
```

```
[Device-classifier-1] quit
```

创建流行为1，用于将报文重定向到4号单板。

```
[Device] traffic behavior 1
```

```
[Device-behavior-1] redirect slot 4
```

```
[Device-behavior-1] quit
```

创建QoS策略1，将流分类1和流行为1进行关联。

```
[Device] qos policy 1
```

```
[Device-qospolicy-1] classifier 1 behavior 1
```

```
[Device-qospolicy-1] quit
```

将QoS策略1应用到接口GigabitEthernet2/0/1。

```
[Device] interface Gigabitethernet 2/0/1
```

```
[Device-GigabitEthernet2/0/1] qos apply policy 1 inbound
```

```
[Device-GigabitEthernet2/0/1] quit
```

1.2 验证配置

当PC 1访问WWW server时，可以看到生成的NAT会话信息。

```
[Device] display nat session verbose
```

Initiator:

Source IP/port: 10.110.1.10/1024

Destination IP/port: 200.1.1.10/80

DS-Lite tunnel peer: -

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

Protocol: UDP(17)

Responder:

Source IP/port: 200.1.1.10/80

Destination IP/port: 61.16.0.2/1025

DS-Lite tunnel peer: -

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

Protocol: UDP(17)

State: UDP_READY

Application: HTTP

Start time: 2014-07-08 13:30:47 TTL: 60s

Interface(in) : GigabitEthernet2/0/1
Interface(out): GigabitEthernet2/0/2
Initiator->Responder: 21946552 packets 2414120720 bytes
Responder->Initiator: 650389 packets 71542790 bytes

Total sessions found: 1

当有两个外网用户 (61.16.0.10、61.16.0.11) 同时请求FTP服务时, 可以查看到建立了2条NAT会话, 并且FTP server 1和FTP server 2分别为这两个用户提供FTP服务。

[Device] display nat session verbose

Initiator:

Source IP/port: 61.16.0.11/1024
Destination IP/port: 61.16.0.1/21
DS-Lite tunnel peer: -
VPN instance/VLAN ID/VLL ID: -/-/
Protocol: TCP(6)

Responder:

Source IP/port: 10.110.3.1/21
Destination IP/port: 61.16.0.11/1024
DS-Lite tunnel peer: -
VPN instance/VLAN ID/VLL ID: -/-/
Protocol: TCP(6)

State: TCP_ESTABLISHED

Application: FTP

Start time: 2014-07-08 14:11:41 TTL: 3600s

Interface(in) : GigabitEthernet2/0/2

Interface(out): GigabitEthernet2/0/1

Initiator->Responder: 598098 packets 65790780 bytes

Responder->Initiator: 0 packets 0 bytes

Initiator:

Source IP/port: 61.16.0.10/1024
Destination IP/port: 61.16.0.1/21
DS-Lite tunnel peer: -
VPN instance/VLAN ID/VLL ID: -/-/
Protocol: TCP(6)

Responder:

Source IP/port: 10.110.3.2/21
Destination IP/port: 61.16.0.10/1024
DS-Lite tunnel peer: -
VPN instance/VLAN ID/VLL ID: -/-/
Protocol: TCP(6)

State: TCP_ESTABLISHED

Application: FTP

Start time: 2014-07-08 14:12:00 TTL: 3600s

Interface(in) : GigabitEthernet2/0/2

Interface(out): GigabitEthernet2/0/1

Initiator->Responder: 74783 packets 8226130 bytes

Responder->Initiator: 0 packets 0 bytes

Total sessions found: 2

当PC 1通过61.16.0.1地址访问FTP服务器时, 可以查看到建立的NAT会话。

[Device] display nat session verbose

Initiator:

Source IP/port: 10.110.1.10/1024
Destination IP/port: 61.16.0.1/21
DS-Lite tunnel peer: -
VPN instance/VLAN ID/VLL ID: -/-/
Protocol: TCP(6)

Responder:

Source IP/port: 10.110.3.1/21
Destination IP/port: 61.16.0.2/1025
DS-Lite tunnel peer: -
VPN instance/VLAN ID/VLL ID: -/-/
Protocol: TCP(6)
State: TCP_ESTABLISHED
Application: FTP
Start time: 2014-07-08 14:24:15 TTL: 3600s
Interface(in) : GigabitEthernet2/0/1
Interface(out): GigabitEthernet2/0/1
Initiator->Responder: 209716 packets 23068760 bytes
Responder->Initiator: 0 packets 0 bytes

Total sessions found: 1

目前除SPC-CP2LA和SPC-CP2LB单板外，其他业务板都可以提供NAT处理。实现NAT功能时，需要配置QoS策略将流量入接口收到的报文重定向到出接口上指定的提供NAT处理的业务板，这样流量才会进行NAT处理。
NAT功能目前仅在独立运行模式下支持。