**CẤU HÌNH NAT OVERLOAD (PAT)**

***I.* Giới thiệu *:***

NAT (*Network Address Translation*) dùng để chuyển đổi các private address thành địa chỉ public address. Các gói tin từ mạng nội bộ của user gửi ra ngoài, khi đến router biên địa chỉ IP source sẽ được chuyển đổi thành địa chỉ public mà user đã đăng ký v ới ISP. Điều này cho phép các gói tin từ mạng nội bộ có thể được gửi ra mạng ngoài (Internet).

NAT có các loại : NAT static, NAT pool, NAT overload.

NAT static cho phép chuyển đổi *một* địa chỉ nội bộ thành *một* địa chỉ public.

NAT pool cho phép chuyển đổi *các địa chỉ nội bộ* thành một trong *dãy địa chỉ public*. NAT overload cho phép chuyển đổi *các địa chỉ nội bộ* thành *một địa chỉ public*

Trong kỹ thuật NAT overload, router sẽ sử dụng thêm các port cho các địa chỉ khi chuyển

đổi.

**II. Các câu lệnh sử dụng trong bài lab :**

 **ip nat** {inside | outside}

Cấu hình interface là inside hay outside

 **ip nat inside source** {*list* {*access−list−number* | *name*} *pool name* [overload] | static

*local−ip global−i*p}

Cho phép chuyển địa chỉ nội bộ thành địa chỉ public

 **ip nat pool name *start−ip end−ip*** {*netmask* | *prefix−length prefix−length*} [type rotary] Tạo NAT pool

 **show ip nat translations**

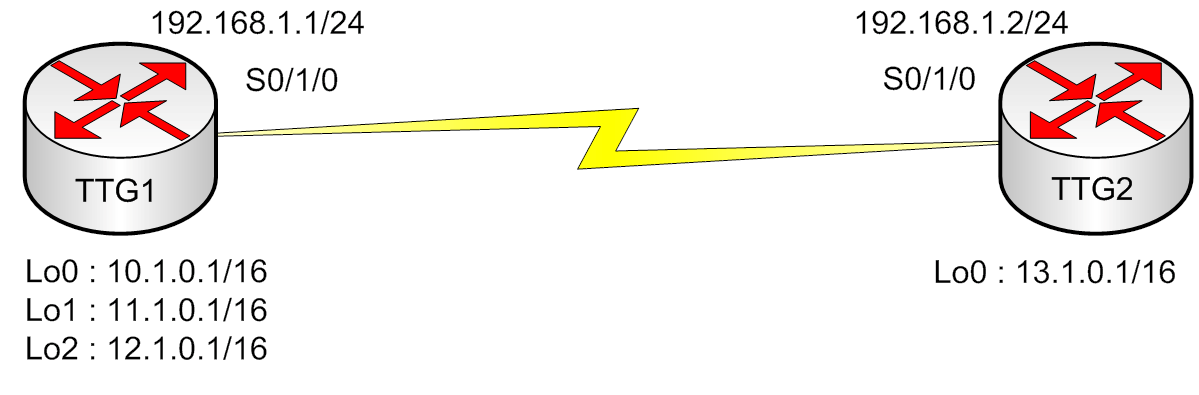
Xem các thông tin về NAT

 **debug ip nat**

Xem hoạt động của NAT

**III. Mô tả bài lab và đồ hình :**

- Đồ hình bài lab như hình trên. Router TTG1 được cấu hình inteface loopback 0, loopback 1, loopback 2. Router TTG2 được cấu hình interface loopback 0. Hai router được nối với nhau bằng cáp Serial. Ta giả lập 3 lớp mạng lo0, lo1, lo2 là những mạng bên trong, khi các traffic ở bên trong mạng này đi ra ngoài ( ra khỏi S0/1/0) tất cả sẽ được chuyển đổi địa chỉ thành 192.168.1.1



**IV. Cấu hình router :**

Hai router được cấu hình các interface như sau :

**Router TTG1 :** Router>enable Router#configure terminal

Router(configure)# hostname TTG1

TTG1(configure)# interface Loopback0

TTG1(configure-if)# ip address 10.1.0.1 255.255.0.0

TTG1(configure-if)#exit

TTG1(configure)# interface Loopback1

TTG1(configure-if)# ip address 11.1.0.1 255.255.0.0

TTG1(configure-if)#exit

TTG1(configure)# interface Loopback2

TTG1(configure-if)# ip address 12.1.0.1 255.255.0.0

TTG1(configure-if)#exit

TTG1(configure)#interface Serial0/1/0

TTG1(configure-if)# ip address 192.168.1.1 255.255.255.0

TTG1(configure-if)#clockrate 64000

TTG1(configure-if)#exit **Router TTG2 :** Router>enable Router#configure terminal

Router(configure)# hostname TTG1

TTG1(configure)# interface Loopback0

TTG1(configure-if)# ip address 13.1.0.1 255.255.0.0

TTG1(configure-if)#exit

TTG1(configure)#interface Serial0/1/0

TTG1(configure-if)# ip address 192.168.1.2 255.255.255.0

TTG1(configure-if)#clockrate 64000

TTG1(configure-if)#exit

- Chúng ta cấu hình NAT trên router TTG1 theo các bước sau :

 **Bước 1** : *Cấu hình các interface inside và outside*

Trong bài lab này, chúng ta cấu hình cho các interface loopback của TTG1 là inside còn interface serial 0 là out side.

TTG1(config)#interface loopback 0

TTG1(config-if)#ip nat inside

TTG1(config)#in loopback 1

TTG1(config-if)#ip nat inside

TTG1(config-if)#interface loopback 2

TTG1(config-if)#ip nat inside

TTG1(config-if)#interface s0/0/0

TTG1(config-if)#ip nat outside

TTG1(config-if)#exit

 **Bước 2** : *Tạo access list cho phép mạng nào được NAT.*

Chúng ta cấu hình cho phép mạng 10.1.0.0/16 và mạng 11.1.0.0/16 được cho phép, cấm mạng 12.1.0.0/16

TTG1(config)# access-list 1 deny 12.1.0.0 0.0.255.255

TTG1(config)#access-list 1 permit any

 **Bước 3 :** *Tạo NAT pool cho router TTG1*

Cấu hình NAT pool tên TTG1 có địa chỉ từ 172.1.1.1/24 đến 172.1.1.5/24

TTG1(config)#ip nat pool TTG1 172.1.1.1 172.1.1.5 netmask 255.255.255.0

 **Bước 4** : *Cấu hình NAT cho router*

TTG1(config)#ip nat inside source list 1 pool TTG1 **overload**

Câu lệnh trên cấu hình overload cho NAT pool

 **Bước 5** : *Định tuyến cho router*

TTG1(config)#ip route 13.1.0.0 255.255.0.0 192.168.1.2

TTG2(config)#ip route 172.1.1.0 255.255.255.0 192.168.1.1

*Lưu ý : đối với router TTG2, nếu ta định tuyến theo dạng : TTG2(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1*

*thì chúng ta có thể ping thấy được các mạng ở trong router TTG1 (10.1.0.0/16, 11.1.0.0/16). Nhưng thực tế, ISP chỉ định tuyến xuống cho user bằng địa chỉ mà user đã đăng ký (Inside global address).*

 **Bước 6** : *Kiểm tra hoạt động của NAT*

Chúng ta sẽ kiểm tra NAT bằng câu lệnh *debug ip nat*

TTG1#debug ip nat

IP NAT debugging is on

- Sau khi bật debug NAT, chúng ta sẽ ping đến loopback0 của TTG2 từ loopback0 của TTG1. Ta giả lập traffic từ host 10.1.0.1 đến mạng 13.1.0.1. Lúc này khi traffic của 10.1.0.1 qua S0 sẽ chuyển đổi địa chỉ.

TTG1#ping

Protocol [ip]:

Target IP address: **13.1.0.1**

Repeat count [5]: Datagram size [100]: Timeout in seconds [2]: Extended commands [n]: y

Source address or interface: **10.1.0.1**

Type of service [0]:

Set DF bit in IP header? [no]: Validate reply data? [no]: Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 13.1.0.1, timeout is 2 seconds:

!!!!!

**Success rate is 100 percen**t **(5/5)**, round-trip min/avg/max = 40/40/44 ms

TTG1#

00:31:12: NAT: s=10.1.0.1->172.1.1.1, d=13.1.0.1 [190]

00:31:12: NAT\*: s=13.1.0.1, d=172.1.1.1->10.1.0.1 [190]

00:31:12: NAT: s=10.1.0.1->172.1.1.1, d=13.1.0.1 [191]

00:31:12: NAT\*: s=13.1.0.1, d=172.1.1.1->10.1.0.1 [191]

00:31:12: NAT: s=10.1.0.1->172.1.1.1, d=13.1.0.1 [192]

00:31:12: NAT\*: s=13.1.0.1, d=172.1.1.1->10.1.0.1 [192]

00:31:12: NAT: s=10.1.0.1->172.1.1.1, d=13.1.0.1 [193]

00:31:12: NAT\*: s=13.1.0.1, d=172.1.1.1->10.1.0.1 [193]

00:31:12: NAT: s=10.1.0.1->172.1.1.1, d=13.1.0.1 [194]

00:31:12: NAT\*: s=13.1.0.1, d=172.1.1.1->10.1.0.1 [194]

- Từ kết quả trên ta thấy được, các gói tin từ mạng 10.1.0.1 đã đư ợc đổi source IP thành

171.1.1.1.

- Sử dụng câu lệnh ***show ip nat translations*** để xem các thông về NAT TTG1#show ip nat translations

Pro Inside global Inside local Outside local Outside global icmp 172.1.1.1:**2459** 10.1.0.1:**2459** 13.1.0.1:**2459** 13.1.0.1:**2459** icmp 172.1.1.1:**2460** 10.1.0.1:**2460** 13.1.0.1:**2460** 13.1.0.1:**2460** icmp 172.1.1.1:**2461** 10.1.0.1:**2461** 13.1.0.1:**2461** 13.1.0.1:**2461** icmp 172.1.1.1:**2462** 10.1.0.1:**2462** 13.1.0.1:**2462** 13.1.0.1:**2462** icmp 172.1.1.1:**2463** 10.1.0.1:**2463** 13.1.0.1:**2463** 13.1.0.1:**2463**

- Các số được in đậm là port NAT sử dụng cho địa chỉ 10.1.0.1.

- Lập lại các bước trên để kiểm tra NAT cho loopback 1, loopback 2 của router TTG1

TTG1#ping

Protocol [ip]:

Target IP address: **13.1.0.1**

Repeat count [5]: Datagram size [100]: Timeout in seconds [2]: Extended commands [n]: y

Source address or interface: **11.1.0.1**

Type of service [0]:

Set DF bit in IP header? [no]: Validate reply data? [no]: Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 13.1.0.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 40/40/44 ms

TTG1#

00:33:16: NAT: s=11.1.0.1->172.1.1.1, d=13.1.0.1 [210]

00:33:16: NAT\*: s=13.1.0.1, d=172.1.1.1->11.1.0.1 [210]

00:33:16: NAT: s=11.1.0.1->172.1.1.1, d=13.1.0.1 [211]

00:33:16: NAT\*: s=13.1.0.1, d=172.1.1.1->11.1.0.1 [211]

00:33:16: NAT: s=11.1.0.1->172.1.1.1, d=13.1.0.1 [212]

00:33:16: NAT\*: s=13.1.0.1, d=172.1.1.1->11.1.0.1 [212]

00:33:17: NAT: s=11.1.0.1->172.1.1.1, d=13.1.0.1 [213]

00:33:17: NAT\*: s=13.1.0.1, d=172.1.1.1->11.1.0.1 [213]

00:33:17: NAT: s=11.1.0.1->172.1.1.1, d=13.1.0.1 [214]

00:33:17: NAT\*: s=13.1.0.1, d=172.1.1.1->11.1.0.1 [214]

- TTG1#show ip nat translations

Pro Inside global Inside local Outside local Outside global icmp 172.1.1.1:6407 11.1.0.1:6407 13.1.0.1:6407 13.1.0.1:6407 icmp 172.1.1.1:6408 11.1.0.1:6408 13.1.0.1:6408 13.1.0.1:6408 icmp 172.1.1.1:6409 11.1.0.1:6409 13.1.0.1:6409 13.1.0.1:6409 icmp 172.1.1.1:6410 11.1.0.1:6410 13.1.0.1:6410 13.1.0.1:6410 icmp 172.1.1.1:6411 11.1.0.1:6411 13.1.0.1:6411 13.1.0.1:6411

TTG1#ping

Protocol [ip]:

Target IP address: **13.1.0.1**

Repeat count [5]: Datagram size [100]: Timeout in seconds [2]: Extended commands [n]: y

Source address or interface: **12.1.0.1**

Type of service [0]:

Set DF bit in IP header? [no]: Validate reply data? [no]: Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 13.1.0.1, timeout is 2 seconds:

…..

**Success rate is 0 percent (0/5)**

- Đối với 12.1.0.1, chúng ta không ping ra ngoài được vì mạng 12.1.0.0/16 đã b ị cấm trong access list 1.

- Đứng ở router TTG2, chúng ta ping xuống các loopback của router TTG1

**TTG2#ping 10.1.0.1**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.0.1, timeout is 2 seconds:

.....

**Success rate is 0 percent (0/5) TTG2#ping 11.1.0.1**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 11.1.0.1, timeout is 2 seconds:

.....

**Success rate is 0 percent (0/5) TTG2#ping 12.1.0.1**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 12.1.0.1, timeout is 2 seconds:

.....

**Success rate is 0 percent (0/5)**

**- Nhận xét** : tất cả đều không thành công Nguyên nhân là router TTG2 không có route nào đến các loopback của router TTG1. Trong thực tế, ta cũng có kết quả tương tự do ISP chỉ định tuyến xuống địa chỉ mà user đăng ký, còn các địa chỉ mạng bên trong của user thì không được ISP định tuyến.

**Một số lệnh liên quan đến bài lab :**

**1. Cấu hình các interface inside và outside**

|  |  |
| --- | --- |
| Router (config)#**interface loopback 0** | Cấu hình interface loopback 0 là interface  inside |
| Router (config-if)#**ip nat inside** |
| Router (config-if)#**interface s0/0/0** | Cấu hình interface loopback 0 là interface outside |
| Router (config-if)#**ip nat outside** |

**2. Tạo access list cho phép mạng nào được NAT**

|  |  |
| --- | --- |
| Router (config)# **access-list 1 deny 12.1.0.0**  **0.0.255.255** | Tạo một ACL để cho phép mạng  12.1.0.0/16 có thể được NAT. |
| Router (config)#**access-list 1 permit any** | Cấu hình Access-list để cho phép tất cả các mạng còn lại |

**3. Tạo NAT pool cho router**

Router (config)#**ip nat pool TTG1 172.1.1.1** Cấu hình NAT pool tên TTG1 có địa chỉ từ

|  |  |
| --- | --- |
| **172.1.1.5 netmask 255.255.255.0** | 172.1.1.1/24 đến 172.1.1.5/24 |
| Router (config)#**ip nat inside source list 1**  **pool TTG1 overload** | Tạo NAT bằng cách gán list 1 với pool tên là  TTG1. Phương pháp Overloading sẽ được thực thi. |
| Router (config)#**ip nat inside source list 1 interface s0/0/0 overload** | Tạo NAT bằng cách gán list 1 dùng chung ip của interface s0/0/0 |