ubiQuoss

VP5200 Series Switch

Common User Guide

Chapter #7

ubiQuoss

목 차

7
NAT

본 장에서는 VP 5200 스위치에서의 NAT 설정에 대해 설명한다.

7.1. NAT 개요

Network Address Translation (NAT)는 인터넷의 폭발적인 성장으로 인한 IP 주소 부족 문제에 대한 해결책의 하나로 생겨나게 되었다. 사설 IP 주소를 사용하는 특정 조직은 이 사설 주소를 공인 IP 주소로 변환하여 인터넷에 접속이 가능하게 된다. 이러한 NAT 과정을 거치게 될 경우 어떤 조직의 실제로 사용하는 IP network 주소 공간이 아닌 다른 IP Network 주소 공간으로 외부에 보이게 된다. NAT 는 RFC 1631 에 기술 되어 있다.

7.2. NAT 설정

NAT 를 설정을 시작하기 전에 private 네트워크에서 사용할 inside IP address 와 public 네트워크에서 사용할 outside IP address 를 미리 알고 있어야만 한다.

VP 5200 스위치에서는 다음과 같은 세 가지 NAT 변환 방식을 제공 하고 있다.

1. Static translation

특정 inside IP address 를 특정 outside IP address 로 1 대 1 변환한다.

2. Dynamic translation

여러 inside IP address 들에 대해 하나 이상의 outside IP address 로 IP 주소로 변환한다. VP5200 스위치는 사용할 inside IP address 의 선택 방법에 따라 세 가지의 dynamic translation 을 제공한다.

- MASQUERADE : outside IP address 를 특별히 지정하지 않고, outside interface 에 해당하는 address 를 사용한다.
- PAT : 하나의 outside IP address 만을 사용한다.
- NAT : 두 개 이상의 outside IP address 를 사용한다.

3. Local translation

VP5200 스위치로부터 발생되는 트래픽의 source IP 를 변경하는 방식으로 각 프로토콜 별, 포트 별, 목적지 별로 설정 가능하다.

7.2.1. Static NAT 설정

특정 하나의 inside IP address 를 다른 하나의 outside IP address 로 변경하여 전송하는 방식으로 Global mode 에서 다음의 명령어를 수행한다.

명령어	설명
ip nat static inside *IFNAME address* **outside** *IFNAME address*	■ static NAT 를 위한 inside IP address 와 outside IP address 설정

설정 예제는 다음과 같다.

```
Switch# configure terminal
Switch(config)# ip nat static vlan1 192.168.0.1 outside vlan2
200.1.1.1
```

7.2.2. Dynamic NAT 설정

주소 변환 방식 중 하나인 dynamic translation 을 적용하기 위해서 다음의 명령어를 이용하여 설정한다.

7.2.2.1. Masquerade mode 설정

Dynamic NAT 를 Masquerade 로 설정 할 경우 inside 네트워크에 속하는 패킷의 source IP 는 outside IFNAME 에 해당하는 주소로 변경하여 전송된다.

명령어	설명
ip nat dynamic inside *IFNAME netnum/prefix-len* **outside** *IFNAME*	■ inside 네트워크를 위한 pool 구성 ■ outside 인터페이스 설정

Masquerade mode 를 설정하는 예제는 다음과 같다. private 으로 vlan1 과 192.168.1.0/24 네트워크를 정의하며, outgoing 인터페이스로 vlan2 를 정한다.

```
Switch# configure terminal
Switch(config)# ip nat dynamic inside vlan1 192.168.1.0/24 outside
vlan2
```

7.2.2.2. PAT mode 설정

Global mode 에서 다음의 명령어를 이용하여 PAT(Port Address Translation) mode 로 NAT 를 설정한다. Dynamic NAT 를 PAT mode 로 설정 할 경우 inside 네트워크에 속하는 패킷의 source IP 는 outside IP address 로 설정된 하나의 IP 로 변경하여 전송된다.

명령어	설명
ip nat dynamic inside *IFNAME netnum/prefix-len* **outside** *IFNAME address*	■ inside 네트워크를 위한 pool 구성 ■ outside 인터페이스 설정 및 변환될 IP 설정

다음은 Dynamic NAT 를 PAT mode 로 설정하도록 하며, vlan1 에서 발생하는 트래픽 중에 source IP 가 192.168.1.0/24 에 해당하는 패킷의 source IP 를 200.1.1.1 로 변환하여 전송한다.

```
Switch# configure terminal
Switch(config)# ip nat dynamic inside vlan1 192.168.1.0/24 outside
vlan2 200.1.1.1
```

7.2.2.3. Dynamic NAT 를 NAT mode 로 설정

Global mode 에서 다음의 명령어를 이용하여 NAT mode 로 Dynamic NAT 를 설정한다. Dynamic NAT 를 NAT mode 로 설정 할 경우 inside 네트워크에 속하는 패킷의 source IP 는 outside pool 로 설정된 여러 IP 중에 하나로 변경하여 전송된다.

명령어	설명
ip nat dynamic inside *IFNAME netnum/prefix-len* **outside** *IFNAME lowest-address highest-address*	■ inside 네트워크를 위한 pool 구성 ■ outside 인터페이스 설정 및 변환될 IP pool 설정

다음은 Dynamic NAT 를 NAT mode 로 설정하도록 하며 vlan1 에서 발생하는 트래픽 중에 source IP 가 192.168.1.0/24 에 해당하는 패킷의 source IP 를 200.1.1.1~ 200.1.1.4 중의 하나로 변환하여 전송한다.

```
Switch# configure terminal
Switch(config)# ip nat dynamic inside vlan1 192.168.1.0/24 outside
vlan2 200.1.1.1 200.1.1.4
```

7.2.3. local NAT 설정

local NAT 는 VP5200 스위치에서 발생되는 트래픽의 source IP address 를 변환하는 방식으로 다음의 명령어를 이용하여 설정한다.

명령어	설명
ip nat local inside *source-netnum/prefix-len protocol portnum destination-netnum/prefix-len* **outside** *address*	■ protocol : tcp, udp, icmp 특정 설정이 없는 경우는 any ■ portnum : 적용할 포트 번호 또는 특정 포트를 구분하지 않을 경우는 any ■ destination-netnum/prefix : 특정 목적지로 향하는 트래픽의 변환, 특별히 구분하지 않을 경우는 any ■ address : 변경 할 IP

다음 예제는 VP 5200 스위치에서 발생하는 소스 IP 가 10.1.1.0/24 인 트래픽 중 ftp 서버 20.1.1.1 로 향하는 트래픽의 소스 IP 변환 예이다.

```
Switch# configure terminal
Switch(config)# ip nat local inside 10.1.1.0/24 tcp 21 20.1.1.1/32
outside 200.1.1.1
```

Notice 포트 번호는 프로토콜로서 TCP 또는 UDP 가 설정된 경우에만 설정 가능하다. 특정하게 정하기를 원치 않는 필드는 any 로 설정하면 된다.

7.2.4. NAT 활성화

먼저, NAT 가 동작하기 위해서는 Global mode 에서 다음의 명령어를 이용하여 NAT 엔진을 활성화시킨다.

명령어	설명
service nat	NAT 엔진을 활성화시키다.

```
Switch# configure terminal
Switch(config)# service nat
Switch(config)# exit
```

Notice NAT 설정 후 flow-rule(본 매뉴얼 chapter7.4 를 참조)을 설정하여야 한다.

7.3. NAT 설정 보기

7.3.1. Static NAT 설정 정보 조회

명령어	설명
show ip nat static	Static NAT 의 현재 설정 정보를 출력

다음은 vlan3 인터페이스를 10.2.3.0/24 로 설정한 후에, static NAT 를 설정했을 때의 설정 정보이다.

```
Switch# show ip nat static
MODE    Private IP      Public IP                 Direction
STATIC 10.2.3.10        200.1.1.101               vlan3->vlan2
total 1 pools found
```

7.3.2. Dynamic NAT 설정 정보 조회

명령어	설명
show ip nat dynamic	Dynamic NAT 의 현재 설정 정보를 출력

다음은 vlan1 인터페이스를 10.1.1.0/16 으로 설정한 후에, dynamic NAT 를 각각 다른 대역에 대해 Masquerade, PAT 그리고 NAT 모드로 설정했을 때의 설정 정보이다.

```
Switch# show ip nat dynamic
MODE    Private IP      Public IP                   Direction
MASQ    10.1.1.0/24         -                      vlan1->vlan2
PAT     10.1.2.0/24     200.1.1.100                vlan1->vlan2
NAT     10.1.3.0/24     200.1.1.200-200.1.1.204    vlan1->vlan2
total 3 pools found
```

7.3.3. Local NAT 설정 정보 조회

명령어	설명
show ip nat local	Local NAT 의 현재 설정 정보를 출력

```
Switch# show ip nat local
MODE      SRC-IP          PROTO  PORT DEST-IP            PUB-IP
LOCAL     10.1.1.0/24     tcp    23   210.108.10.0/24    200.1.1.99
LOCAL     10.1.1.0/24     tcp    21   20.1.1.1/32        200.1.1.1
total 2 pools found
```

7.3.4. Translation 정보 조회

명령어	설명
show ip nat translations	NAT 를 거친 패킷의 정보를 출력

```
Switch# show ip nat translations
PROTO STATE     SRC-IP   TRANSLATED-IP SRC-PORT    DST-IP      DST-PORT   REPLY
tcp   CLOSE      10.1.1.1  200.1.1.9      1089   222.122.195.6    80   UNREPLIED
udp   TIME_WAIT  10.1.2.1   200.1.1.1     1088   222.231.8.162    80
total 2 pools found
```

7.4. NAT 를 위한 Flow-Rule 설정

NAT 설정 후 flow-rule 을 설정 하여야 한다. 그 방법은 아래와 같다.

```
Switch# configure terminal
Switch(config)# ip nat dynamic inside vlan1 192.168.1.0/24 outside
vlan4092 200.1.1.1
Switch(config)# service nat
Switch(config)# flow-rule nat classify ip 200.1.1.1/32 any
Switch(config)# flow-rule nat match dynamic-nat
Switch(config)# policy-map nat flow-rule nat
Switch(config)# service-policy gi1 ingress nat
Switch(config)# exit
```

	**Notice**	기존 gi1 에 policy-map 이 이미 적용된 경우에는 해당 policy-map 에 NAT flow-rule 를 추가하여야 한다.
	**Notice**	flow-rule 에 의해 classify 되어야 할 IP address 는 NAT rule 로 인해 변경된 source IP address 이어야 한다.