

네트워크 개론 Part 9

: Policy NAT & Twice NAT

(NAT : Network Address Translation)

글. 조인준 KBS 미디어기술연구소 차장

지난 연재를 통해 로컬 네트워크의 호스트 디바이스를 인터넷의 외부 호스트 디바이스와 연결하기 위해 필요한 Static NAT, Static PAT, Dynamic NAT, Dynamic PAT에 관해 다루었습니다.

위 4가지 방식 모두 로컬 호스트의 사실 IP 주소를 인터넷에서 사용 가능한 공인 IP 주소로 맵핑하기 위한 것들이며, 패킷이 어디로 가느냐에 상관없이 로컬 호스트의 사실 IP 주소에는 하나의 공인 IP 주소가 맵핑됩니다.

하지만 패킷이 어디로 가느냐에 따라 로컬 네트워크에 속한 같은 호스트 디바이스의 사실 IP 주소라도 다른 공인 IP 주소로 맵핑하는 것이 필요할 때도 있고, 목적지의 IP 주소도 다른 IP 주소로 맵핑해야 하는 경우도 있습니다. 이렇듯 패킷의 목적지에 따라 송신 IP 주소 또는 수신 IP 주소를 맵핑하기 위해 Policy NAT과 Twice NAT이라는 방식이 있으며, 이번 연재에서는 이에 관한 설명을 드리겠습니다.

• Policy NAT

Policy NAT은 로컬 호스트가 패킷을 보내는 외부의 호스트에 따라 라우터에서 로컬 호스트의 사실 IP 주소에 다른 공인 IP 주소를 맵핑시키는 방식입니다. 앞선 연재를 통해 소개된 Static NAT, Static PAT, Dynamic NAT, Dynamic PAT 네 가지 방식 중 어느 방식을 기반으로 하던 패킷이 보내지는 목적지 IP 주소에 따라 사실 IP의 공인 IP 주소 맵핑을 달리하면 Policy NAT이라고 부를 수 있습니다.

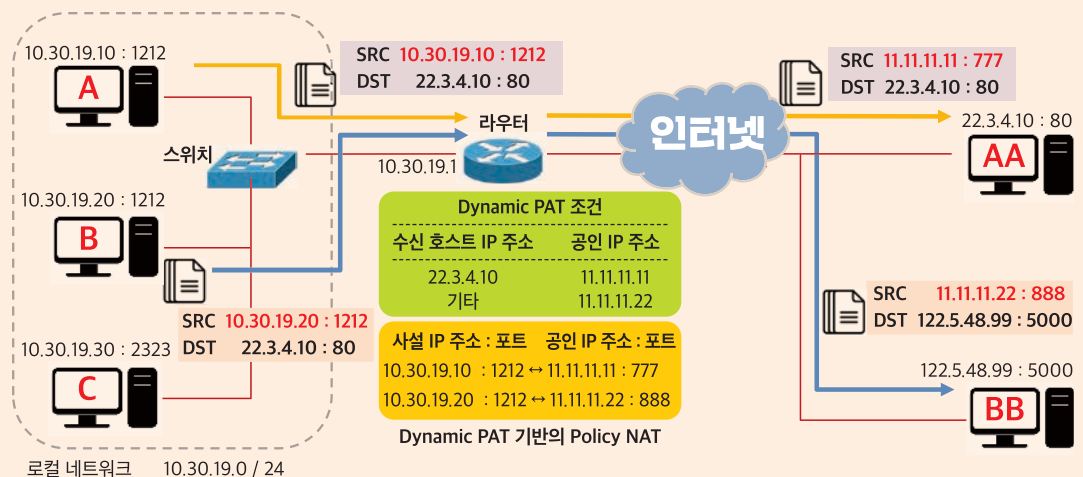


그림 1. Policy NAT

Static NAT, Static PAT, Dynamic NAT, Dynamic PAT 중 어느 것을 사용하더라도 Policy NAT을 구현할 수 있

지만, 네 가지 경우 모두에 대해 비슷한 내용을 반복하는 것은 비효율적이므로 Dynamic PAT을 기반으로 한 Policy NAT만을 예로 들겠습니다. 나머지 경우에 대해서도 같은 방식이 적용되므로 이해가 간단할 것입니다. 설명을 위해 [그림 1]을 보겠습니다.

[그림 1] 중앙에 녹색으로 표시된 블록에는 라우터에 정의된 Dynamic PAT 설정이 요약되어 있습니다. 이 설정에 따르면 10.30.19.0/24 로컬 네트워크의 호스트 디바이스들이 공인 IP 주소가 22.3.4.10인 외부 호스트에 데이터 패킷을 보낼 때는 로컬 호스트들의 사설 IP 주소에 11.11.11.11을 공인 IP 주소로 맵핑하고, 그 외의 외부 호스트에 데이터 패킷을 보낼 때는 로컬 호스트들의 사설 IP 주소에 11.11.11.22를 공인 IP 주소로 맵핑하도록 되어 있습니다. 이 룰을 적용하여 [그림 1]의 사설 IP 주소 10.30.19.10을 갖는 로컬 호스트 디바이스 'A'가 1212번 포트를 사용하여 공인 IP 주소 22.3.4.10을 갖는 외부 호스트 디바이스 'AA'의 80번 포트로 데이터 패킷을 보내고 사설 IP 주소 10.30.19.20을 갖는 로컬 호스트 디바이스 'B'가 1212번 포트를 사용하여 공인 IP 주소 122.5.48.99를 갖는 외부의 호스트 디바이스 'BB'의 5000번 포트로 데이터 패킷을 보내는 과정을 통해 Policy NAT의 중요한 특징을 살펴보겠습니다.

'A'가 외부로 패킷을 보내기 위해서는 우선 해당 패킷을 라우터로 보내야 합니다. 'A'가 보내는 패킷을 받은 라우터는 자신에게 정의된 Dynamic PAT 설정에 따라 'A'가 보낸 패킷의 목적지의 공인 IP 주소를 체크합니다. 목적지의 공인 IP 주소가 22.3.4.10임을 확인하면 정해진 설정에 따라 공인 IP 주소 11.11.11.11에 포트 번호 777을 동적으로 할당하여 'A'의 사설 IP 주소 및 포트 번호 10.30.19.10:1212에 배정합니다. 이로써 [그림 1] 중앙에 옐렌지색으로 표시된 블록과 같이 라우터 내부에 10.30.19.10:1212 ↔ 11.11.11.11:777의 맵핑이 생성됩니다. 곧이어 'B'가 1212번 포트로 'BB'의 5000번 포트에 패킷을 보내면 라우터는 목적지의 공인 IP 주소를 확인 후 설정에 따라 공인 IP 주소 11.11.11.22에 888번 포트를 동적으로 할당하여 10.30.19.20:1212 ↔ 11.11.11.22:888의 맵핑을 추가합니다.

이러한 방법으로 22.3.4.10으로 보내지는 모든 패킷은 송신 IP 주소로 공인 IP 주소 11.11.11.11을 갖게 되며, 그 외의 패킷들은 송신 IP 주소로 공인 IP 주소 11.11.11.22를 갖습니다. [그림 1]은 Dynamic PAT을 기반으로 한 Policy NAT의 예이며, Static NAT 등 기타 다른 방식을 기반으로 하더라도 목적지 IP 주소에 따라 라우터에서 사설 IP 주소 ↔ 공인 IP 주소 맵핑을 달리하면 Policy NAT이 될 수 있습니다.

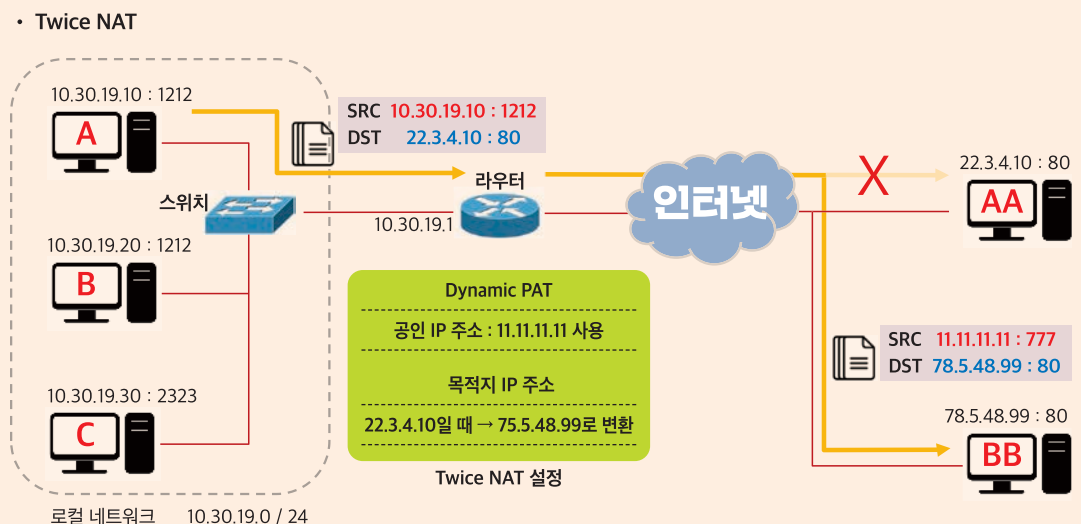


그림 2. Twice NAT

Policy NAT에서는 로컬 호스트가 패킷을 보내는 대상에 따라 라우터에서 다른 공인 IP 주소를 사용하여 로컬 호스트의 사설 IP 주소를 공인 IP 주소로 변환했습니다. 하지만 때에 따라서는 패킷에 수신 IP로 지정된 외부 호스트의 IP 주소를 라우터에서 변환해야 할 때도 있습니다. 즉, 패킷을 보내는 로컬 호스트의 사설 IP 주소를 공인 IP 주소로 변환함과 동시에 패킷에 수신 IP로 지정된 특정 외부 호스트의 공인 IP 주소 또한 다른 공인 IP 주소로 변환하는 것이 필요한 경우가 있고 이를 Twice NAT이라고 합니다.

[그림 2]를 통해 Twice NAT을 설명하겠습니다. [그림 2] 중앙에 녹색으로 표시된 블록에는 라우터에서

- ① 사설 IP 주소를 공인 IP 주소로 변환하기 위해 사용하는 Dynamic PAT의 공인 IP 주소 11.11.11.11과
- ② 목적지 IP 주소의 변환에 대한 특이 사항이 적혀 있으며, 이것이 이 라우터가 수행하는 Twice NAT의 주요 내용입니다.

우선 라우터에 정의된 Dynamic PAT에 의해서 좌측 로컬 네트워크의 호스트에서 외부로 보내는 모든 패킷에 포함된 사설 IP 주소와 사용된 포트 번호는 공인 IP 주소 11.11.11.11과 임의로 할당된 포트번호로 변환됩니다. 또한 패킷에 포함된 목적지 IP 주소 또한 명시된 조건에 따라 다른 IP 주소로 변환되며, 이렇게 하는 여러 이유 중 간단한 하나를 예로 들자면 다음과 같습니다.

인터넷상의 서버 'AA'가 존재한다고 가정합니다. 그런데 어떤 이유로 독자 여러분의 회사에서는 'AA' 대신 'AA'와 같은 기능을 하는 회사가 외부에 설치한 서버 'BB'를 이용하도록 하고 있습니다. 이때 모든 시스템이 'AA' 대신 'BB'에 패킷을 보내도록 설정하거나, 사용자들에게 'AA' 대신 'BB'를 사용하도록 교육하는 것은 많은 시간과 노력을 요구하며, 실수가 발생할 수도 있습니다. 이런 경우 라우터에서 'AA'의 공인 IP 주소인 22.3.4.10을 목적지로 갖는 모든 패킷의 목적지를 'BB'의 공인 IP 주소인 78.5.48.99로 변환하게 설정한다면, 앞의 문제를 간단하게 해결할 수 있습니다.

위의 과정을 [그림 2]를 통해 하나씩 짚어보면 다음과 같습니다. 10.30.19.0/24 로컬 네트워크의 사설 IP 주소 10.30.19.10을 갖는 호스트 'A'가 1212번 포트를 이용하여 인터넷상의 공인 IP 주소 22.3.4.10을 갖는 서버 'AA'의 80번 포트로 패킷을 보냅니다. 이 패킷은 인터넷으로 나가기 위해 라우터로 보내지고, 라우터에는 Dynamic PAT이 설정되어 있어서 사설 IP 주소로 된 패킷의 송신 IP 주소 및 포트번호 10.30.19.10:1212를 공인 IP 주소 및 포트번호인 11.11.11.11:777로 변환합니다. 동시에 수신 IP 주소를 검사하여 22.3.4.10임을 확인하고 수신 IP 주소 및 포트번호를 22.3.4.10:80에서 78.5.48.99:80으로 변환하여 'AA' 대신 'BB'로 보내지게 합니다.

이렇듯 송신 IP 주소와 수신 IP 주소를 동시에 바꾸기 때문에 Twice NAT이라 불리며, [그림 2]에서는 Dynamic PAT을 기반으로 한 Twice NAT을 예로 들었지만 Dynamic PAT 이외의 방식을 기반으로도 Twice NAT을 구성할 수 있습니다.

이로써 다양한 NAT에 대한 설명을 마무리하겠습니다. 네트워크 개론 연재를 종합해보시면 네트워크를 통해 패킷이 어떻게 이동하고, 로컬 네트워크와 인터넷이 어떻게 연결되는지에 관한 이해의 초석이 마련되었을 것 같습니다.

다음 연재부터는 지금까지의 내용을 통해 형성된 IP 네트워크에 대한 이해를 기반으로 일반적으로 사용되는 IP 통신 프로토콜인 TCP와 UDP에 관한 설명을 이어가도록 하겠습니다. 📖