https://www.netmanias.com/ko/?m=view&id=blog&no=5826

NAT 문서 모두 보기

현재 국내 통신사업자는 유선 액세스(FTTH, Ethernet, DSL 등)를 제외한 (거의) 모든 액세스 망에 NAT 장비를 적용하고 있습니다.

- 3G/LTE 망: 3G/LTE Core 망(GGSN/P-GW) 상단에 LSN(Large Scale NAT) 도입 (CGN: Carrier Grade NAT 라고도 부름)
- Wi-Fi Hotspot 망: Wi-Fi Hotspot 용 AP 에서 NAT 수행
- 댁내 망: 통신 사업자가 가입자 댁내에 공급(임대)한 유무선 공유기 혹은 Open Market 의 유무선 공유기(예. EFM 의 ipTIME)에서 NAT 수행

즉, 3G/LTE 사용자, Wi-Fi Hotspot 사용자, 댁내 유무선 공유기를 설치한 사용자 모두 사설 IP 주소(Private IP Address)를 할당 받고 NAT 장비를 통해 공인 IP 주소(Public IP Address)로 변환되어 인터넷과 연결됩니다.

통신 사업자는 NAT 장비 도입을 통해

(1) 사설 IP 주소를 가진 여러대의 단말들이 하나의 공인 IP 주소를 통해 인터넷과 연결됨으로써 공인 IP 주소를 절약할 수 있으며

(2) 3G/LTE 망에 LSN을 도입하여 외부에서 이동통신 단말 혹은 이동 통신망으로 향하는 공격을 차단할 수 있습니다.

기업 역시 사내망을 사설 IP 주소화 하여 외부로 부터의 침입/공격을 차단할 수 있습니다. (방화벽의 개념).

오늘은 RFC 3022(Traditional NAT)와 RFC 2663(IP NAT Terminology and Considerations)에서 기술하고 있는 NAT 용어에 대해 알아보도록 하겠습니다.

용어의 정의 (Terminology)

1. TU Ports

TCP 와 UDP 헤더에는 각각 TCP Source & Destination Port #와 UDP Source & Destination Port #가 존재하는데 이를 총칭하여 TU Ports 라고 부릅니다. 혹은 Transport Identifier 라고도 부릅니다. 보통 단말(Client)이 서버(Server)와 TCP 혹은 UDP 통신 시 TU Destination Port 는 0 ~ 1023 (Well Known Ports, which is defined by IANA) 혹은 1024 ~ 49191 (Registered Ports, which is not defined by IANA) 중에 하나의 값[RFC 1700 에 정의]을 사용하며(대표적인 예. HTTP 는 TCP Destination Port = 80 사용), TU Source Port 는 OS 마다 서로 다른 범위(대략 30,000~60,000)의 값 중에 하나를 random 하게 사용하는데 이를 Ephemeral Port 라고 부릅니다(http://en.wikipedia.org/wiki/Ephemeral_port 참조).

2. Public/Global/External Network

IANA(Internet Assigned Numbers Authority) 기관에서 할당 받은 Globally Unique 한 IP 주소를 가진 네트워크를 말하며 따라서 이 네트워크는 전세계 통신 사업자 망을 통해 라우팅(통신)이 가능합니다. 흔히 "공인 IP 네트워크"라고 부릅니다.

3. Private/Local Network

IANA 에서 할당 받지 않은 IP 주소를 가진 네트워크를 말하며 인터넷에서 라우팅 될 수 없습니다. 흔히 "사설 IP 네트워크"라고 부릅니다.
IANA 에서는 아래 3 개의 IP 블럭을 이 용도로 정의하고 있습니다.

- 10/8, 172.16/12, 192.168/16

4. Session

NAT 에 의해 변환(translation)되는 트래픽의 단위를 Session 으로 정의하고 있는데(A session is defined as the set of traffic that is managed as a unit for translation), 쉽게 말해 TCP/UDP Session 은 {source IP address, source TU port, destination IP address, destination TU port}로 구분되는 것을 말합니다.

5. Application Level Gateway (ALG)

응용에 따라 Payload(TCP/UDP 헤더 이후에 나오는 Application specific 한 데이터)에 IP address or/and TU port 정보가 실리는 경우가 있습니다. ALG 란 응용 별로 Payload 내의 IP address or/and TU port 정보를 변환(translation) 해 줄 수 있는 기능(agent)이 NAT 장비에 올라가 있는 경우이며(Application awareness inside the NAT), 보통 이 NAT 장비는 어떤 어떤 응용(예. FTP, SIP, RTSP, etc)을 지원한다라는 식의 응용 프로그램 리스트를 함께 얘기하곤 합니다. 세상에 쏟아져 나오는 각종 응용 프로그램에 대한 ALG 를 NAT 장비가 모두 지원한다는 건 비현실적이기 때문에 ALG 를 지원하는 NAT 장비는 그리 많지 않은 듯 합니다.

NAT 란? (What is NAT?)

NAT(Network Address Translation)란 한마디로 Private Network 에 위치하는 단말이 Public Network(인터넷)과 통신이 가능하도록 상호 간에 연결 시켜 주는 기능입니다.

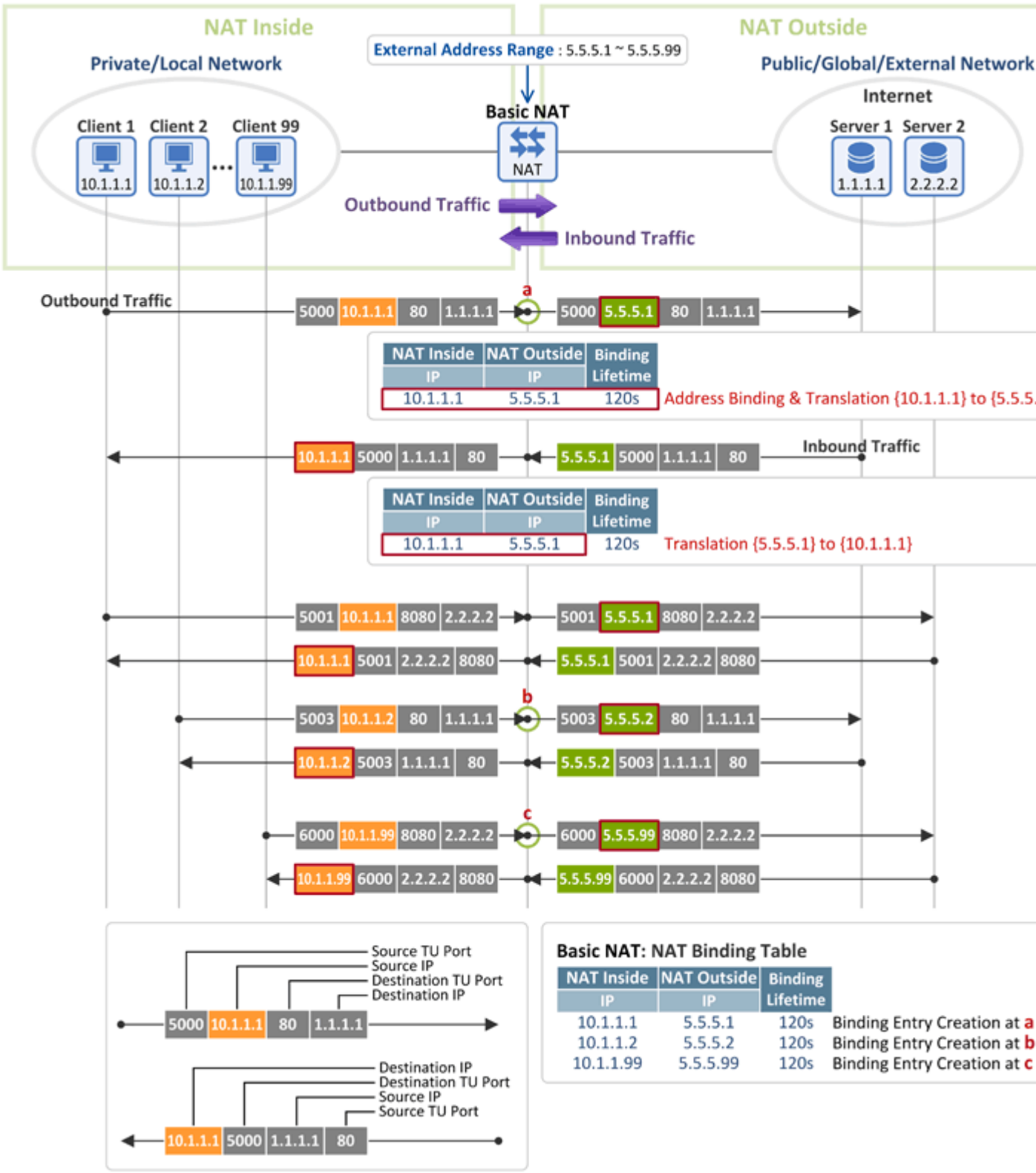
> **Traditional NAT** would allow hosts within a private network to transparently access hosts in the external network, in most cases. In a traditional NAT, sessions are uni-directional, outbound from the private network. Sessions in the opposite direction may be allowed on an exceptional basis using static address for pre-selected hosts. (RFC 3022)
>
> Traditionally, **NAT devices** are used to connect an isolated address realm with private unregistered addresses to an external realm with globally unique registered addresses. (RFC 2663)

NAT 의 종류

RFC 3022/2663 에서는 NAT 를 Basic NAT 와 NAPT(Network Address Port Translation)로 구분하여 설명하고 있으며, 이 2 개를 총칭하여 Traditional NAT 라고 부르고 있습니다. "IPv4 주소의 절약"이라는 목적을 위해 사용되는 NAPT 가 현재 일반적인 NAT 장비의 방식이며, 따라서 그냥 NAT 라고 하는 경우에 NAPT 를 의미하는 경우가 많으며 현재 모든 유무선 공유기는 NAPT 방식을 지원하고 있습니다.

> Basic Network Address Translation or **Basic NAT** is a method by which IP addresses are mapped from one group to another, transparent to end users. Network Address Port Translation, or **NAPT** is a method by which many network addresses and their TCP/UDP (Transmission Control Protocol/User Datagram Proto ports are translated into a single network address and its TCP/UDP ports.
> Together, **these two operations**, referred to as **traditional NAT**, provide a mechanism to connect a realm private addresses to an external realm with globally unique registered addresses. (RFC 3022)

Basic NAT



■ **Definition** : 목적 및 정의

기업망(Enterprise Network)에서 보안의 목적(방화벽)으로 사용하며, Private IP 주소를 가지는 단말 개수 만큼 Pubilc IP 주소를 가지고 인터넷과 연결됨

Nodes on private network could be enabled to communicate with external network by dynamically mapping the set of private addresses to a set of globally valid network addresses. (RFC 3022)

■ **Translation** : Translation 규칙

1:1 translation (1 = Public IP, 1 = Private IP)

■ **Mapping** : Translation 되는 패킷 정보

- Outbound Traffic: Translation {Private Source IP Address} to {Pubilc source IP Address}
- Inbound Traffic: Translation {Public Destination IP Address} to {Private Destination IP Address}

■ Packet Modification : Translation 수행 시 변경되는 패킷 정보

- Outbound Traffic: Source IP Address, IP Header Checksum
- Inbound Traffic: Destination IP Address, IP Header Checksum

■ **Translation Phases of a Session** : Translation 3 단계

1. Address Binding

Private IP Address 를 가진 단말이 보낸 Outbound Traffic 에 대해 Basic NAT 장비가 {Private IP Address}에 대한 {Public IP Address}를 결정하고(1:1 mapping) NAT Binding Table 에 세션 엔트리 생성

2. Address Lookup and Translation

- 이후 Outbound 방향으로(단말에서 NAT 장비로) 패킷이 수신되면 NAT Binding Table을 참조하여 {Private Source IP Address}를 {Public Source IP Address}로 변환하여 인터넷으로 전송

- Inbound 방향으로(인터넷에서 NAT 장비로) 패킷 수신 시 NAT Binding Table을 참조하여 {Public Destination IP Address}를 단말의 IP 즉, {Private Destination IP Address}로 변환하여 단말로 전송

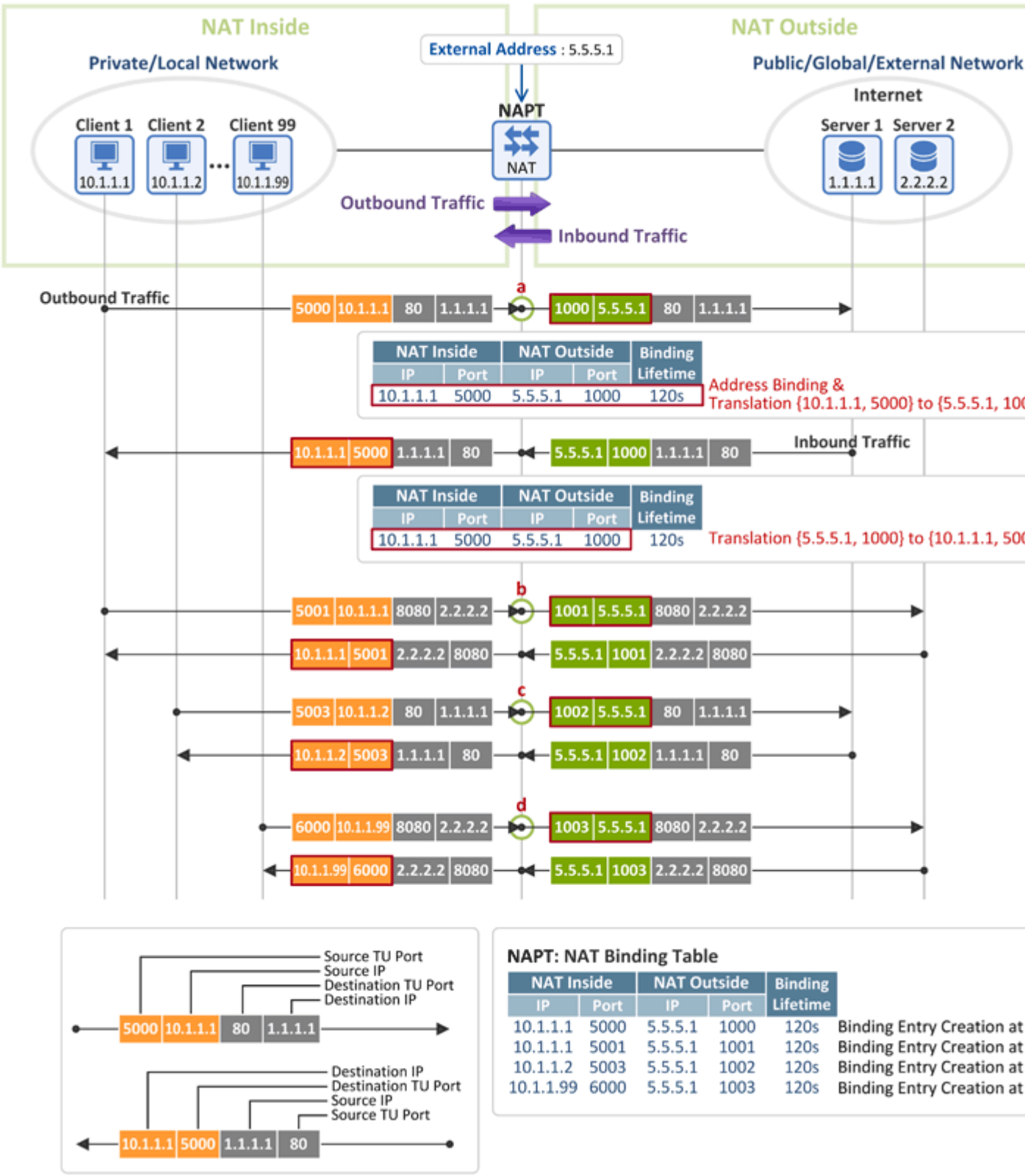
3. Address Unbinding

NAT Binding Table의 해당 엔트리에 대해 일정 시간(NAT 장비마다 다름)동안 패킷이 흐르지 않으면 세션 엔트리를 삭제

■ **Deployment Example** : 적용 예

기업망(Enterprise Network)

NAPT (Network Address Port Translation)



■ **Definition** : 목적 및 정의

Public IP 주소 절약을 목적으로, Private IP 주소를 가지는 여러대의 단말이 하나의 Public IP 주소를 통해 인터넷과 연결되는 방식

Nodes on the private network could be allowed simultaneous access to the external network, using thesingle registered IP address with the aid of NAPT. (RFC 3022)

■ **Translation** : Translation 규칙

1:N translation (1 = Public IP, N = Private IP)

■ **Mapping** : Translation 되는 패킷 정보

- Outbound Traffic: Translation {Private Source IP Address, Local TU Source Port} tuple to {Pubilc Source IP Address, Registered TU Source Port} tuple
- Inbound Traffic: Translation {Public Destination IP Address, Registered TU Destination Port} tuple to {Private Destination IP Address, Local TU Destination Port}

■ Packet Modification : Translation 수행 시 변경되는 패킷 정보

- Outbound Traffic: Source IP Address, IP Header Checksum, TU Source Port, TCP/UDP Header Checksum
- Inbound Traffic: Destination IP Address, IP Header Checksum, TU Destination Port, TCP/UDP Header Checksum

■ **Translation Phases of a Session** : Translation 3 단계

1. Address Binding

Private IP Address 를 가진 단말이 보낸 Outbound Traffic 에 대해 NAPT 장비가 Private IP Address 와 TU Source Port 에 대한 Public IP Address 및 TU Source Port 를 결정하고(1:N mapping) NAT Binding Table 에 세션 엔트리 생성

2. Address Lookup and Translation

- 이후 Outbound 방향으로(단말에서 NAT 장비로) 패킷이 수신되면 NAT Binding Table을 참조하여 {Private Source IP Address, Local TU Source Port}를 {Public Source IP Address, Registered TU Source Port}로 변환하여 인터넷으로 전송 (Registered란 NAT 장비가 할당한 Port 값을 의미함. Local TU Source Port를 Internal Port, Registered TU Source Port를 External Port라고도 부름)

- Inbound 방향으로(인터넷에서 NAT 장비로) 패킷 수신 시 NAT Binding Table을 참조하여 {Public Destination IP Address, Registered TU Destination Port}를 단말의 IP 및 Port 정보 즉, {Private Destination IP Address, Local TU Destination Port}로 변환하여 단말로 전송

3. Address Unbinding

NAT Binding Table의 해당 엔트리에 대해 일정 시간(NAT 장비마다 다름)동안 패킷이 흐르지 않으면 세션 엔트리를 삭제

■ **Deployment Example** : 적용 예

Wi-Fi Hotspot, SOHO, Home, 3G/LTE LSN

NAT 장비는 이렇게 만들어야 하는데... (RFC 4787) - 1편: Mapping Behavior

https://www.netmanias.com/ko/?m=view&id=blog&no=5833

Skype, 카톡 보이스, 온라인 게임 등은 모두 UDP 기반의 P2P(Peer-to-Peer) 응용으로써, 서버를 거치지 않고 두 단말간에 바로 통신을 합니다. 지난 시간에 국내 통신 사업자의 경우 유선을 제외한 모든 액세스망(Wi-Fi, 3G, LTE)에 NAT 장비가 도입되어 있다고 설명을 드렸는데요.

이 P2P 응용 프로그램과 NAT는 서로 상극입니다. (NAT가 가해자, P2P가 피해자~ ^^*)
서로 다른 지역에 위치한 사설 IP 단말 2대가 NAT를 통해 서로 직접 통신은 불가능합니다. 왜냐면 외부에서 NAT 내부로 먼저 연결하는 것, 즉 패킷을 먼저 전송하는 것이 기본적으로 불가능하기 때문입니다. (단말1에서 단말2로 패킷을 보내면 단말2 앞에 있는 NAT가 버리고, 단말2에서 단말1로 패킷을 보내면 이번에는 단말1 앞에 있는 NAT가 버림)

이를 해결하고자 STUN(Session Traversal Utilities for NAT, RFC 5389/RFC5780), TURN(Traversal Using Relays around NAT, RFC 5766), ICE(Interactive Connectivity Establishment, RFC 5245)등의 NAT Traversal(NAT 통과 기법)이 표준화되었으며 이를 간단히 요약하면 다음과 같습니다.

- STUN: 단말(STUN 클라이언트)이 STUN 서버(공인 IP 주소를 가진 서버)와 통신을 통해 (1) 현재 내가 사설망에 있는지(NAT 가 있는지), (2) NAT 의 동작 특성(NAT Behavior)은 어떻게 되는지, (3) NAT에 의해 변경되는 공인 IP 주소와 Source Port는 어떤 값인지 등을 알아내는 방법을 기술함
- TURN: 공인 IP 주소를 가진 Relay 서버(TURN 서버)를 통해 두 단말 간에 통신하는 방법을 기술함 (Relay 서버를 거치므로 응답 속도가 느리겠죠)

- ICE: STUN 이나 TURN 을 이용하여 단말간 세션을 설정할 때 최적의 방법을 찾아주는 방법을 기술함

이와 같은 NAT Traversal 기법은 NAT 장비의 동작 특성에 의존하게 되는데, 그래서 2007 년도에 RFC 4787 을 통해 "효과적인 NAT Traversal 을 위한 NAT Behavior Requirement"가 표준화 되었습니다.
앞으로 총 3 회에 걸쳐 RFC 4787 에서 얘기하는 "P2P 응용을 위해 NAT 는 이렇게 동작하면 좋겠다!"에 대해 설명 드리도록 하겠습니다.

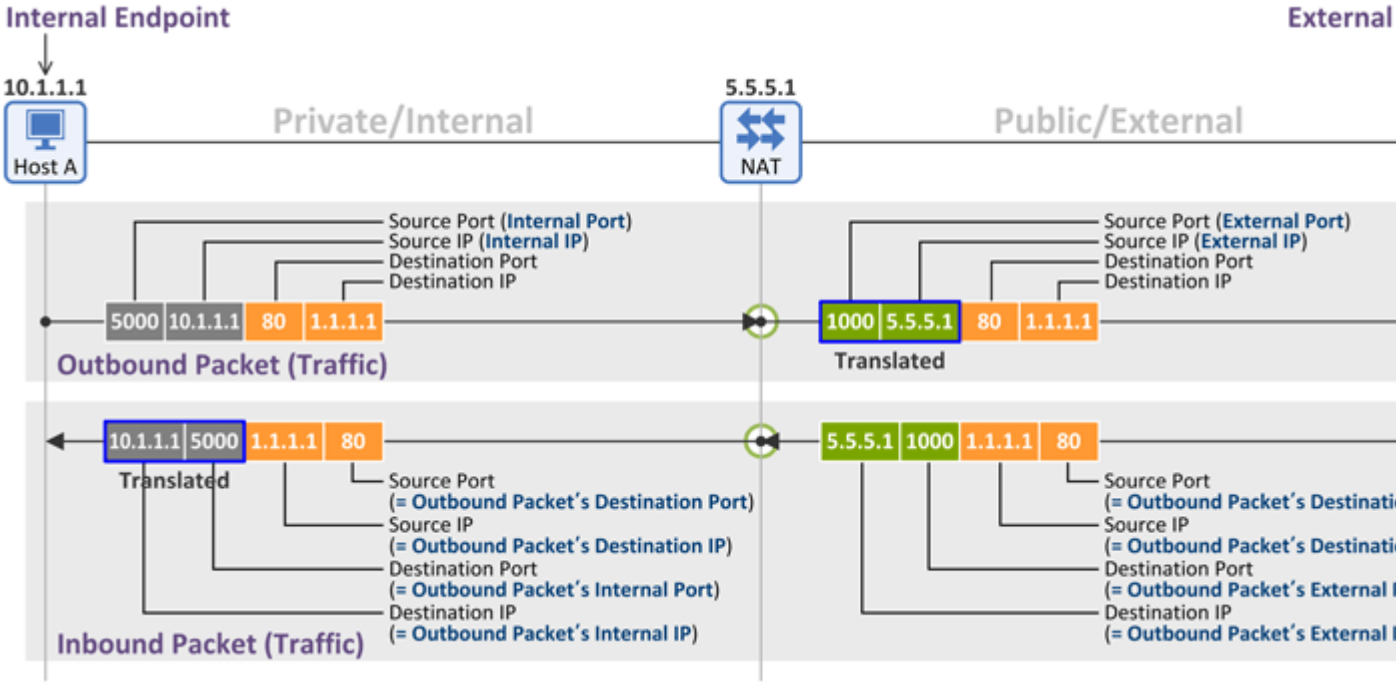
설명을 시작하기에 앞서 용어 정의부터 하겠습니다. (아래 그림 참조)

- **Internal Endpoint**: NAT 내부에 있는 사설 IP 주소를 가지는 단말 (Host A)
- **External Endpoint**: NAT 외부에 있는 공인 IP 주소를 가지는 단말 (Host B)

- **Outbound Packet (Traffic)**: Internal Endpoint 에서 NAT 를 거쳐 External Endpoint 로 전송되는 패킷(트래픽)
- **Inbound Packet (Traffic)**: External Endpoint 에서 NAT 를 거쳐 Internal Endpoint 로 전송되는 패킷(트래픽)

- **Internal Address 와 Internal Port**: Internal Endpoint(Host A)가 보내는 패킷의 Source IP(10.1.1.1)와 Source Port(5000)
- **External Address 와 External Port**: NAT 에 의해 변환되어 External Endpoint(Host B)로 전송되는 패킷의 Source IP(5.5.5.1)와 Source Port(1000)

- 일반적으로 Internal Endpoint(Host A)가 보내는 패킷의 목적지 정보 즉, Destination IP(1.1.1.1), Destination Port(80)는 NAT 에 의해 변환되지 않고 transparent 하게 External Endpoint(Host B)로 전달됨
- 패킷을 수신한 External Endpoint(Host B)는 그 응답으로 다음과 같이 패킷을 구성하여 Internal Endpoint 로 패킷 전송
    - Destination IP = 수신된 패킷의 Source IP 즉, External Address(5.5.5.1)
    - Destination Port = 수신된 패킷의 Source Port 즉, External Port(1000)
    - Source IP = 수신된 패킷의 Destination IP(1.1.1.1) 즉, External Endpoint(Host B)의 IP 주소
    - Source Port = 수신된 패킷의 Destination Port(80)



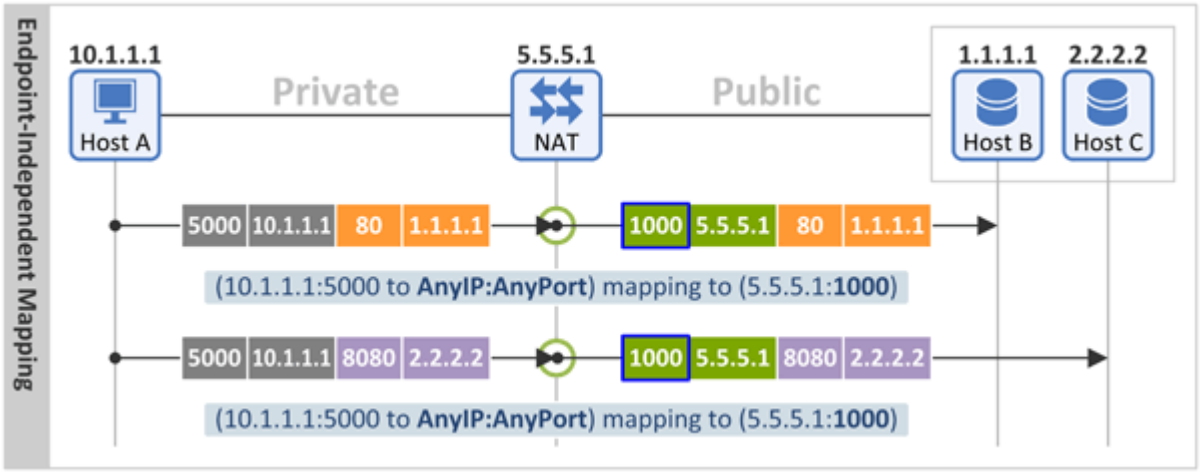
1. Network Address and Port Translation Behavior

1.1 Address and Port Mapping

Endpoint-Independent Mapping

여기서 Endpoint 란 External Endpoint 를 의미합니다.

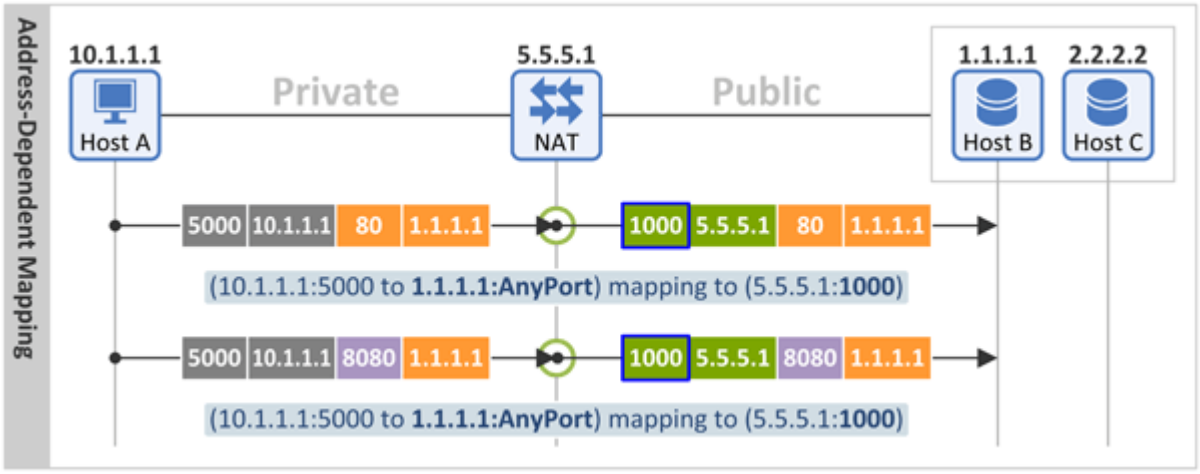
"목적지 독립적 매핑(Endpoint-Independent Mapping)"은 Internal Endpoint(Host A)가 송신하는 패킷의 (1) **Source IP Address**(10.1.1.1)와 (2) **Source Port**(5000)만 동일 하다면 Destination IP Address(1.1.1.1 or 2.2.2.2) 및 Destination Port(80 or 8080) 값에 상관없이 동일한 External Port Mapping 값(Translated Port = 1000)을 사용합니다.



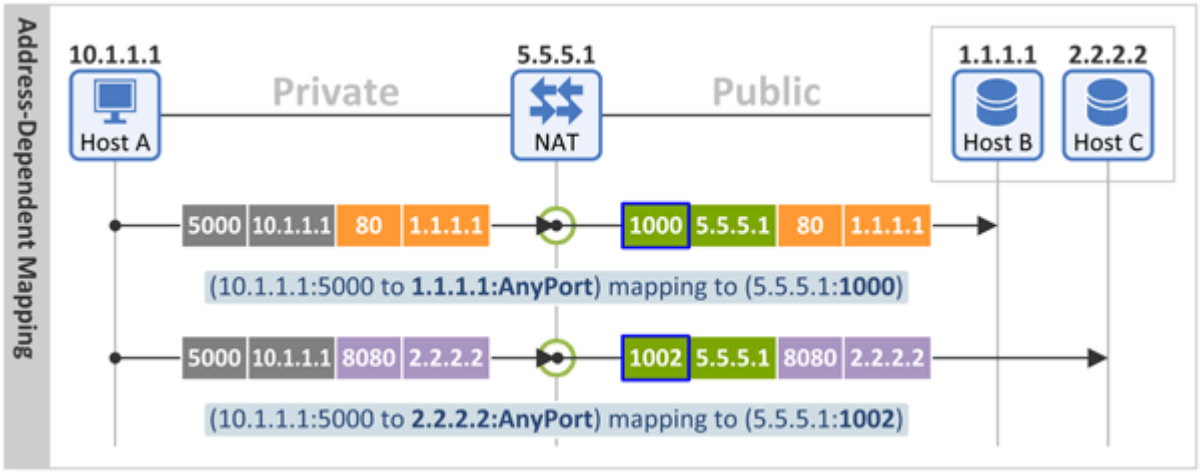
Address-Dependent Mapping

여기서 Address 란 Internal Endpoint 가 송신하는 패킷의 목적지 주소(Destination IP Address)를 의미합니다.

"목적지 주소 의존적 매핑(Address-Dependent Mapping)"은 Internal Endpoint(Host A)가 송신하는 패킷의 (1) **Source IP Address**(10.1.1.1)와 (2) **Source Port**(5000) 그리고 (3) **Destination IP Address**(1.1.1.1)가 동일하면 Destination Port(80 or 8080) 값에 상관없이 동일한 External Port Mapping 값(Translated Port = 1000)을 사용합니다.



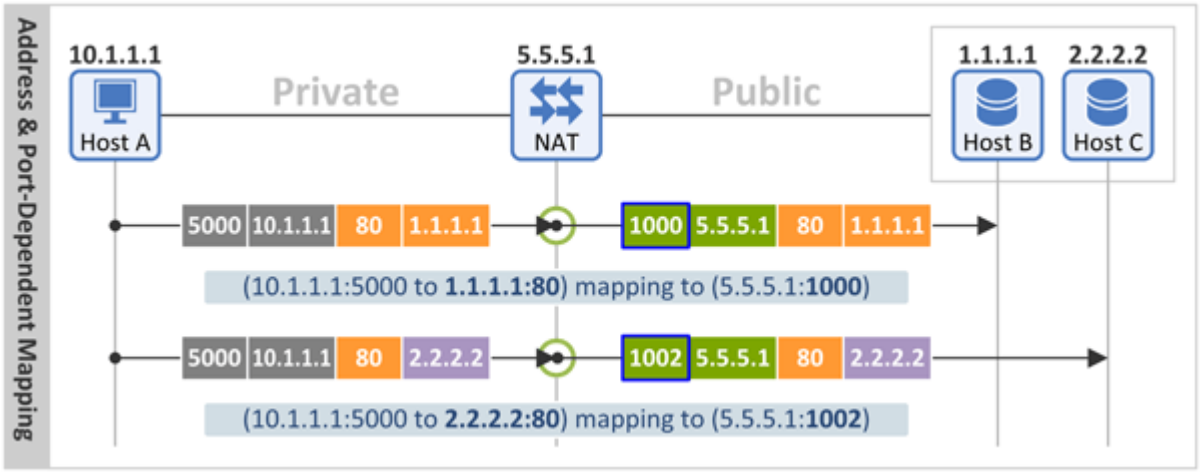
만약 Source IP Address(10.1.1.1)와 Source Port(5000)는 동일하지만 Destination IP Address 가 다르면(1.1.1.1 and 2.2.2.2) 서로 다른 External Port Mapping 값(Translated Port = 1000 and 1002)을 사용합니다.



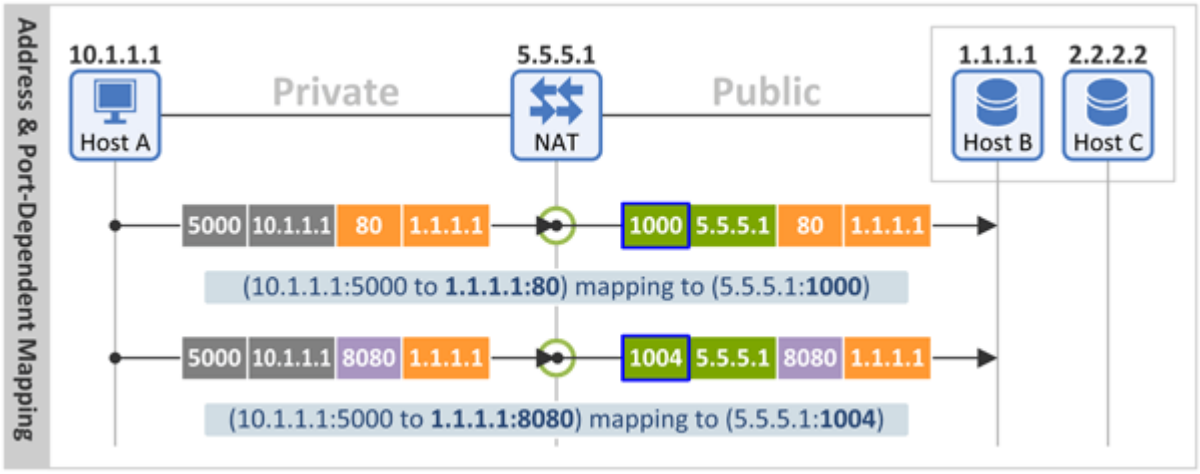
Address and Port-Dependent Mapping

여기서 Address 와 Port 란 Internal Endpoint 가 송신하는 패킷의 목적지 주소(Destination IP Address)와 목적지 포트(Destination Port)를 의미합니다.

"목적지 주소 및 포트 의존적 매핑(Address and Port-Dependent Mapping)"은 Internal Endpoint(Host A)가 송신하는 패킷의 (1) **Source IP Address**, (2) **Source Port** 그리고 (3) **Destination IP Address**, (4) **Destination Port** 가 모두 동일해야 동일 External Port Mapping 값을 사용합니다.
아래 그림에서는 Destination IP Address(1.1.1.1 and 2.2.2.2)가 달라서 다른 External Port Mapping 값(Translated Port = 1000 and 1002)을 사용하였고,



이 그림에서는 Destination Port(80 and 8080)가 달라서 다른 External Port Mapping 값(Translated Port = 1000 and 1004)을 사용하였습니다.



RFC 4787 권고 (REQ-1): A NAT MUST have an "Endpoint-Independent Mapping" behavior
RFC 4787 에 따르면 "본 권고를 지키지 않는 경우 P2P 통신은 Relay 서버(TURN 서버)를 거칠 수 밖에 없게 되어 매우 비효율적이다"라고 얘기하고 있습니다.

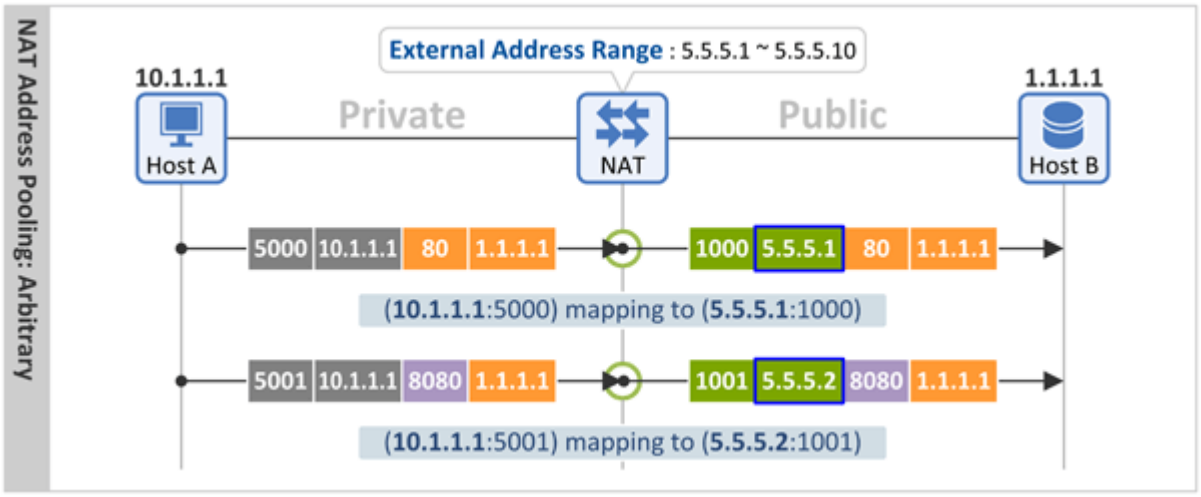
1.2 IP Address Pooling

유무선 공유기나 Wi-Fi Hotspot AP 의 경우 하나의 Public IP 주소를 이용하여 NAPT(Network Address Port Translation)를 수행하는 반면, 3G/LTE 망에 적용된 LSN(Large Scale NAT, 혹은 CGN: Carrier Glade NAT 라 부름)의 경우 여러개의 Public IP 주소(Pool of IP addresses on the external side of the NAT)를 가지게 됩니다.

Arbitrary

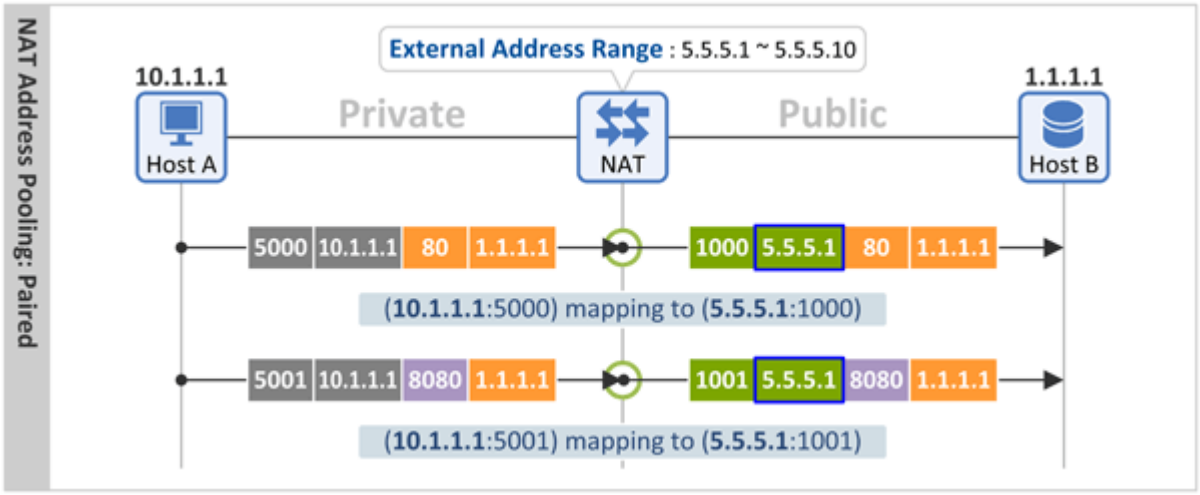
하나의 Internal Endpoint 가 보내는 패킷이지만(동일 Source IP Address 를 가진 패킷), Session(tuple of {Source IP, Source Port, Destination IP, Destination Port})이 다르면 다른 External IP 주소를 사용합니다.
아래 그림과 같이 Internal Endpoint 10.1.1.1(Host A)이 External Endpoint 1.1.1.1(Host B)로 2 개의 Session 을 생성하면 NAT 는 각 Session 에 대해 서로 다른 External IP 주소(5.5.5.1 and 5.5.5.2)를 할당합니다.

- Session 1: {10.1.1.1:5000 to 1.1.1.1:80} -> {5.5.5.1:1000 to 1.1.1.1:80}
- Session 2: {10.1.1.1:5001 to 1.1.1.1:8080} -> {5.5.5.2:1001 to 1.1.1.1:8080}



Paired

하나의 Internal Endpoint 가 보내는 패킷(동일 Source IP Address)에 대해서는 Session(tuple of {Source IP, Source Port, Destination IP, Destination Port})이 달라도 동일 External IP 주소를 사용합니다.
아래 그림과 같이 Internal Endpoint 10.1.1.1(Host A)이 External Endpoint 1.1.1.1(Host B)로 2 개의 서로 다른 Session 을 생성하였지만 NAT 는 각 Session 에 대해 동일 External IP 주소(5.5.5.1)를 할당합니다.

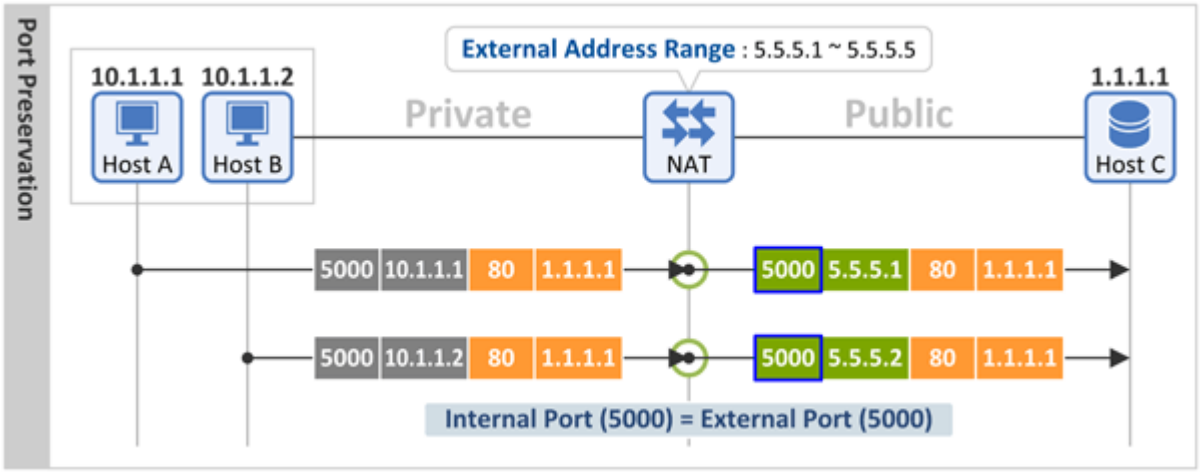


RFC 4787 권고 (REQ-2): It is RECOMMENDED that a NAT have an "IP address pooling" behavior of "Paired"

1.3 Port Assignment

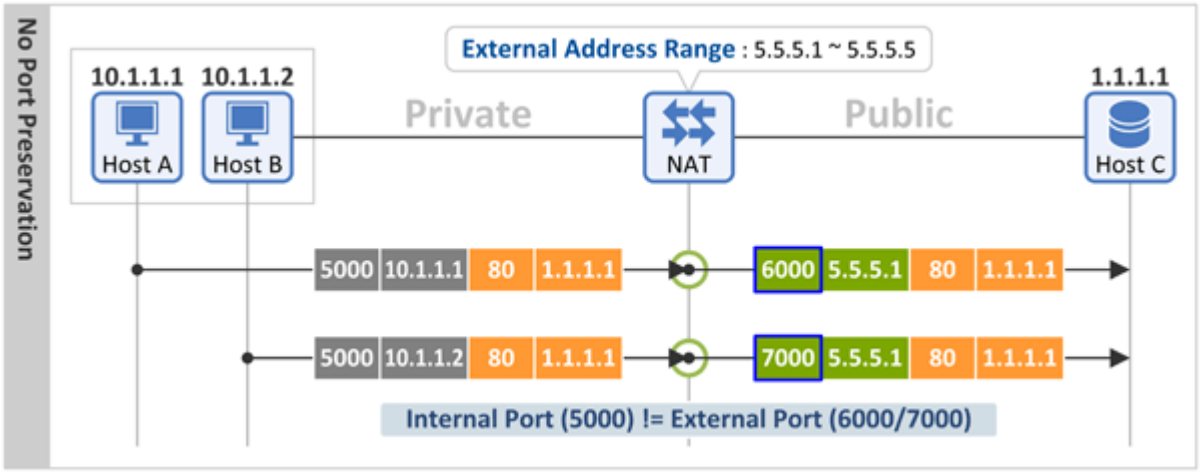
Port Preservation

Internal Endpoint 가 보낸 Source Port(Internal/Local Port) 값이 NAT 변환 후에도 그 값을 유지(Preservation)합니다(External Port = Internal Port).



No Port Preservation

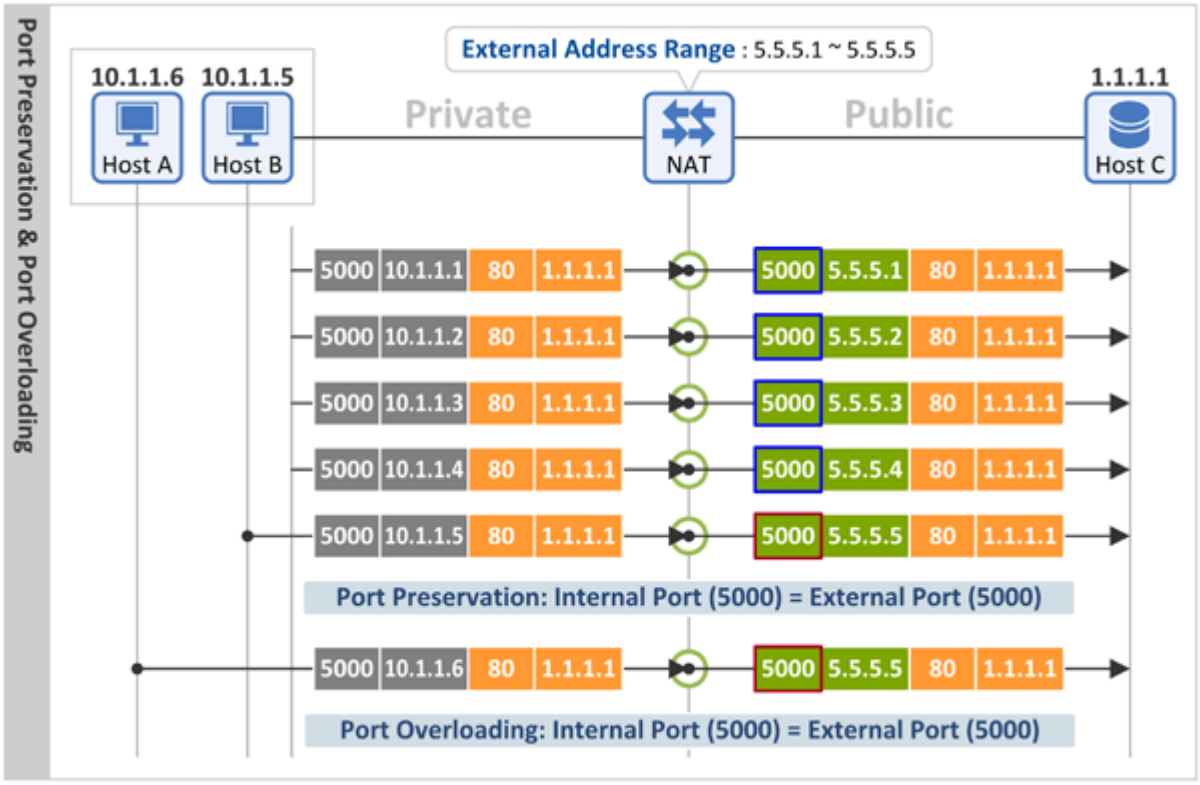
Internal Endpoint 가 보낸 Source Port(Internal Port) 값을 유지하지 않고 따라서 NAT 장비가 임의의 Source Port(External Port) 값으로 변경합니다(External Port != Internal Port).



Port Overloading (in Port Preservation)

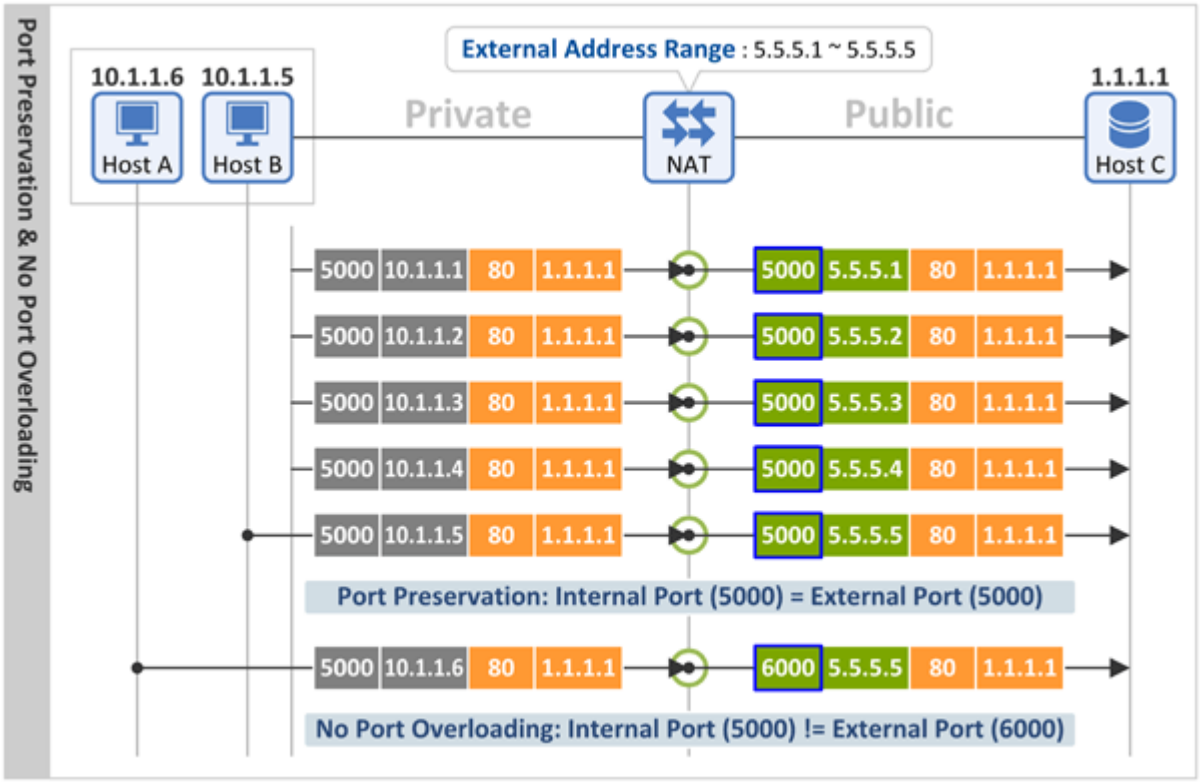
Port Preservation 을 지원하는 NAT 장비가 더 이상 사용 가능한 External IP Address(Public IP Address)가 없는 상황에서 동일 Source Port 를 가진 Outbound 패킷이 들어오면 어떻게 해야 할까요?

Port Overloading 은 아주 무식한 방식입니다. Port Collision 이 발생하면 기존 Binding Entry 를 새것으로 덮어 써 버립니다. 즉, Port Preservation 룰을 계속 유지하겠다는 건데, 이렇게 되면 아래 그림과 같이 Host B 를 위해 생성된 Binding Entry 가 Host A 에 의해 덮어 써 지게 됩니다.
Host A 와 Host B 가 NAT 를 통해 Host C 로 송신한 패킷이 동일한 External Address(5.5.5.5) 및 External Port(5000)를 가지게 되고, Host C 가 송신하는 Inbound 패킷에 대해 NAT 는 Host A 로 패킷을 전달하게 되어 결국 Host B 는 Host C 와 통신이 불가능한 상태가 되어 버립니다. 요즘 이렇게 만든 장비는 없겠죠?



No Port Overloading (in Port Preservation)

Port Collision 발생 시 더 이상 Port Preservation 룰을 유지 하지 않고, Internal Port 와 다른 값의 External Port 를 할당합니다.



RFC 4787 권고 (REQ-3): A NAT MUST NOT have a "Port assignment" behavior of "Port overloading"

1.4 Port Assignment Rule

본 RFC 에서는 No Port Preservation 을 지원하는 NAT 에 대해서 "Internal Port 에 대한 External Port 할당 규칙"에 대해서도 언급을 하고 있습니다. IANA(Internet Assigned Numbers Authority)에서는 다음과 같이 Port Range 를 정의하고 있으며,

- Well-Known: 0 ~ 1023 (IANA 에서 표준화한 값, 예. HTTP = 80)
- Registered: 1024 ~ 49151 (IANA 에서 표준화하지 않았으나 널리 사용되고 있는 값)
- Dynamic/Private: 49192 ~ 65535

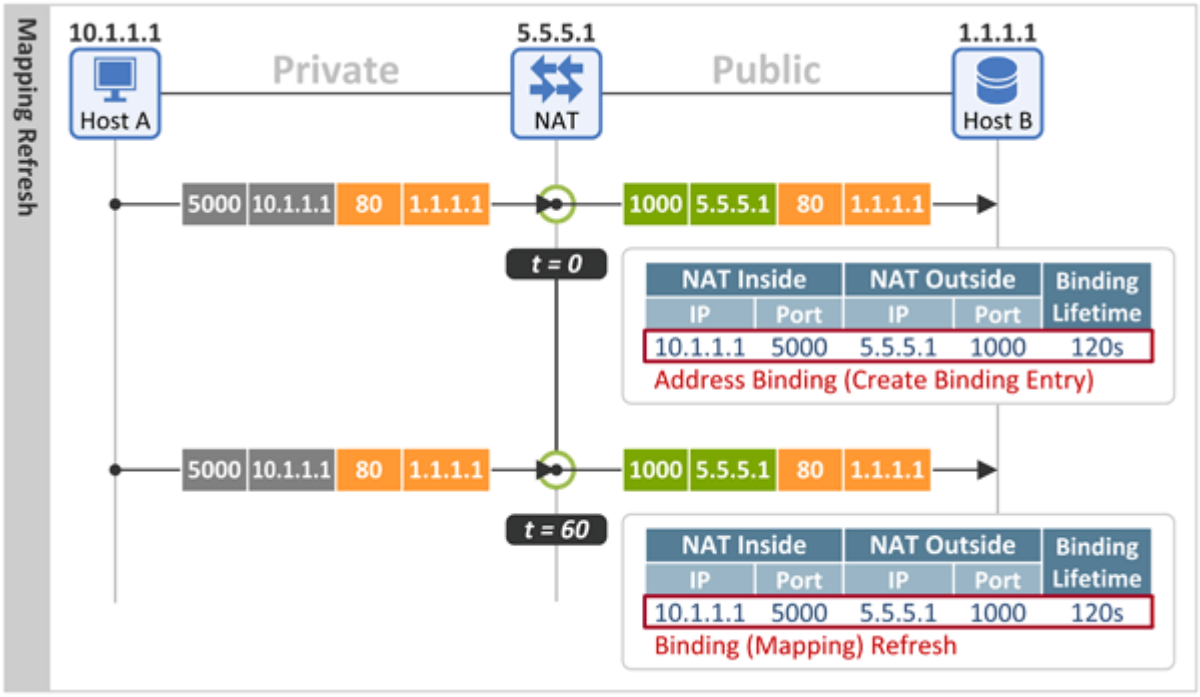
NAT 의 구현에 따라 다음과 같이 External Port 할당 규칙을 적용할 수 있다고 합니다.

- Dynamic/Private 범위(49192 ~ 65535)의 값을 External Port 로 사용하는 경우 (이 경우 하나의 공인 IP 주소로 지원할 수 있는 NAT 세션 수는 16K 개로 제한)
- Well-Known 을 제외한 범위(1024 ~ 65535)의 값을 External Port 로 사용하는 경우 (먼저 Dynamic/Port 의 값을 사용 후 부족하면 Registered 의 값 사용)

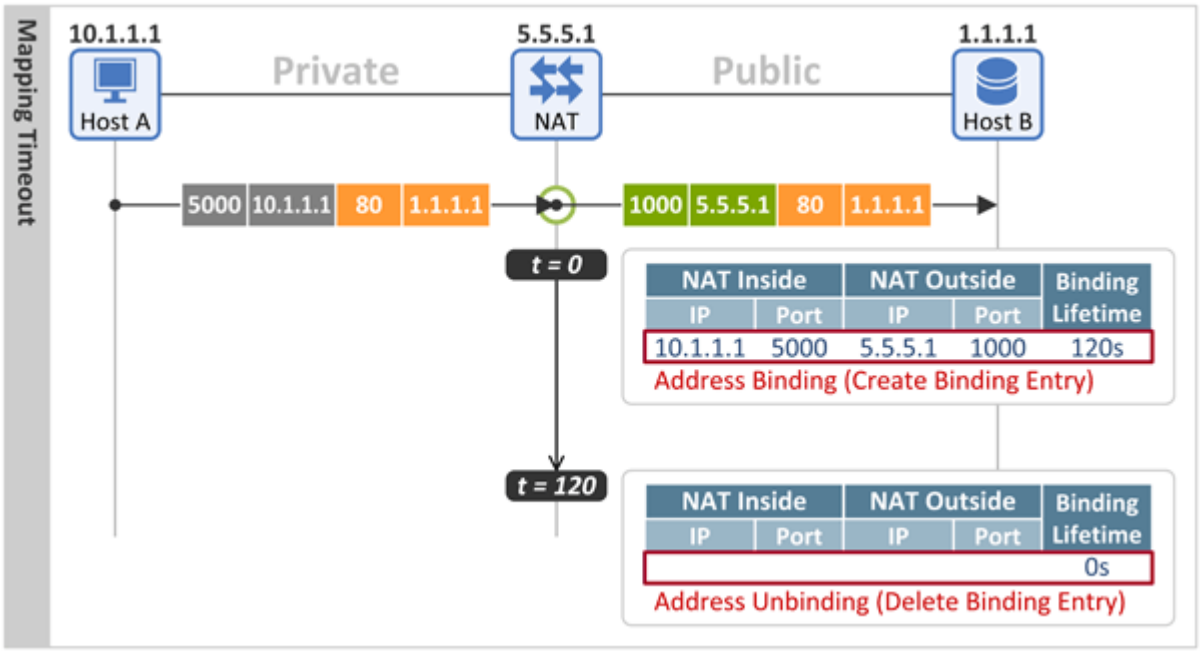
1.5 Mapping Timer (Binding Refresh Timer)

Outbound 트래픽에 의해서 생성된 NAT 의 Binding Entry 는 해당 엔트리를 거치는 트래픽이 있는 경우 계속 유지되지만, 만약 트래픽이 없다면 Mapping Timer(혹은 Binding Refresh Timer, Binding Lifetime 이라 부름) 시간 후에 해당 엔트리는 삭제됩니다.
이 시간이 짧으면 단말(NAT friendly application)에서 NAT session 유지를 위해 Keep Alive 패킷을 자주 보내야 하고 유선, Wi-Fi 망의 경우 별 문제가 없겠으나 3G/LTE 망의 종량제 사용자 입장에서는 별로 바람직하지 않겠죠.

아래 그림은 NAT Mapping Timer 가 2 분으로 설정된 상황에서, t=0 에 단말이 첫 패킷을 보내 Binding Entry 생성 후 1 분 후에 다시 패킷을 보내어 Binding Entry 가 2 분으로 다시 refresh(reset) 됨을 보이고 있고,



이 그림은 2 분이 지나도록 트래픽이 없어 NAT 에 Binding Entry 가 삭제됨을 보이고 있습니다.



RFC 4787 권고 (REQ-5): A NAT UDP mapping timer MUST NOT expire in less than two minutes, unless REQ-5a applies

a) For specific destination ports in the well-known port range (ports 0-1023), a NAT MAY have shorter UDP mapping timers that are specific to the IANA-registered application running over that specific destination port

b) The value of the NAT UDP mapping timer MAY be configurable

c) A default value of five minutes or more for the NAT UDP mapping timer is RECOMMENDED

1.6 Mapping Refresh Behavior

■ **NAT Outbound refresh behavior of "True"**

Outbound Traffic(Internal Endpoint 에서 External Endpoint 로의 패킷)에 의해 Mapping Timer 가 refresh 되는 경우

■ **NAT Inbound refresh behavior of "True"**

Inbound Traffic(External Endpoint 에서 Internal Endpoint 로의 패킷)에 의해 Mapping Timer 가 refresh 되는 경우

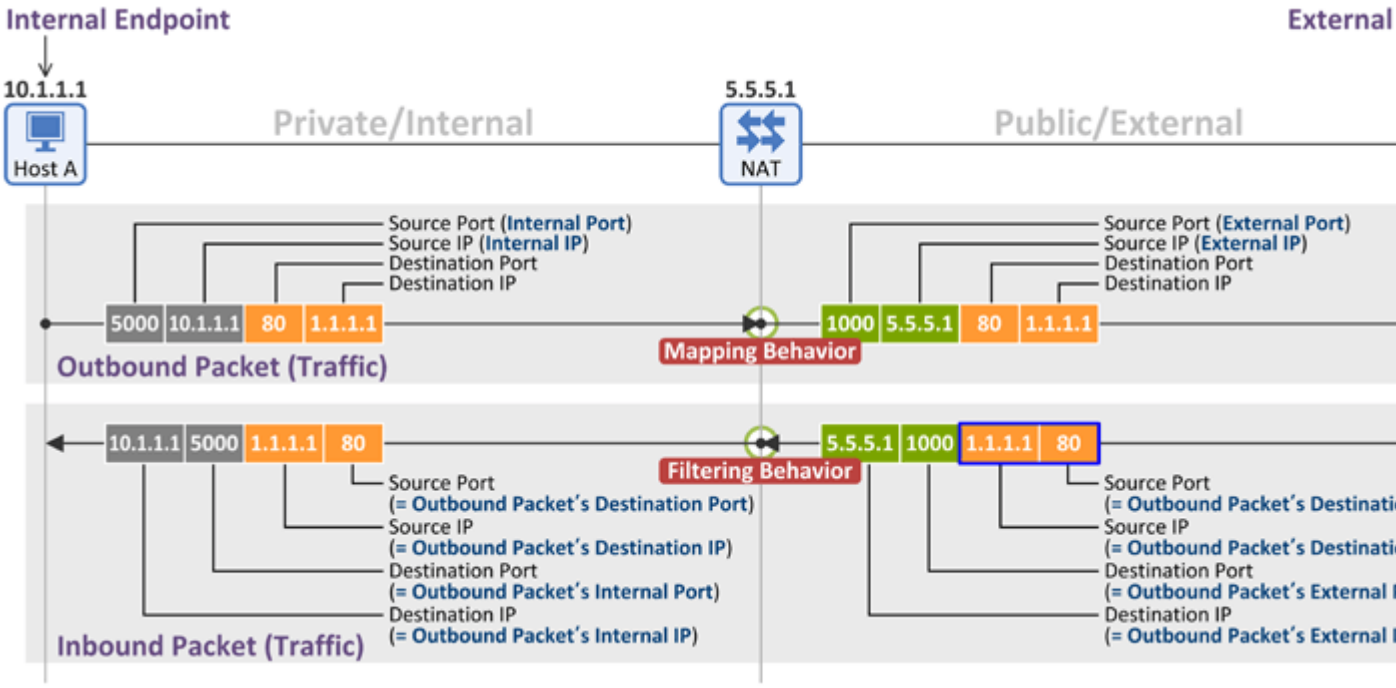
RFC 4787 권고 (REQ-6): The NAT mapping Refresh Direction MUST have a "NAT Outbound refresh behavior" of "True"

NAT 장비는 이렇게 만들어야 하는데... (RFC 4787) - 2편: Filtering Behavior

https://www.netmanias.com/ko/?m=view&id=blog&no=5839

지난 시간에 이어 RFC 4787 의 NAT 동작에 대한 설명을 이어 나가겠습니다.

아래 설명에서 사용되는 용어(Internal Endpoint, External Endpoint, Outbound Traffic, Inbound Traffic 등등)는 지난 시간 블로그의 용어 정의를 참조하시기 바랍니다.



2. Filtering Behavior

지난 시간에 설명드린 Address and Port Mapping Behavior 는 Outbound Packet 을 수신한 NAT 가 패킷의 Destination IP 와 Destination Port 값에 따라 어떻게 External Port 를 변환/매핑하는지에 대한 룰이었다면, 오늘 말씀 드릴 Filtering Behavior 는 Inbound Packet 을 수신한 NAT 가 패킷의 Source IP 와 Source Port 의 값(위 그림의 파란색 박스)에 따라 그 패킷을 허용(Pass, Internal Endpoint 로 패킷 전달) 혹은 폐기(Drop)하는지를 결정하는 룰입니다.

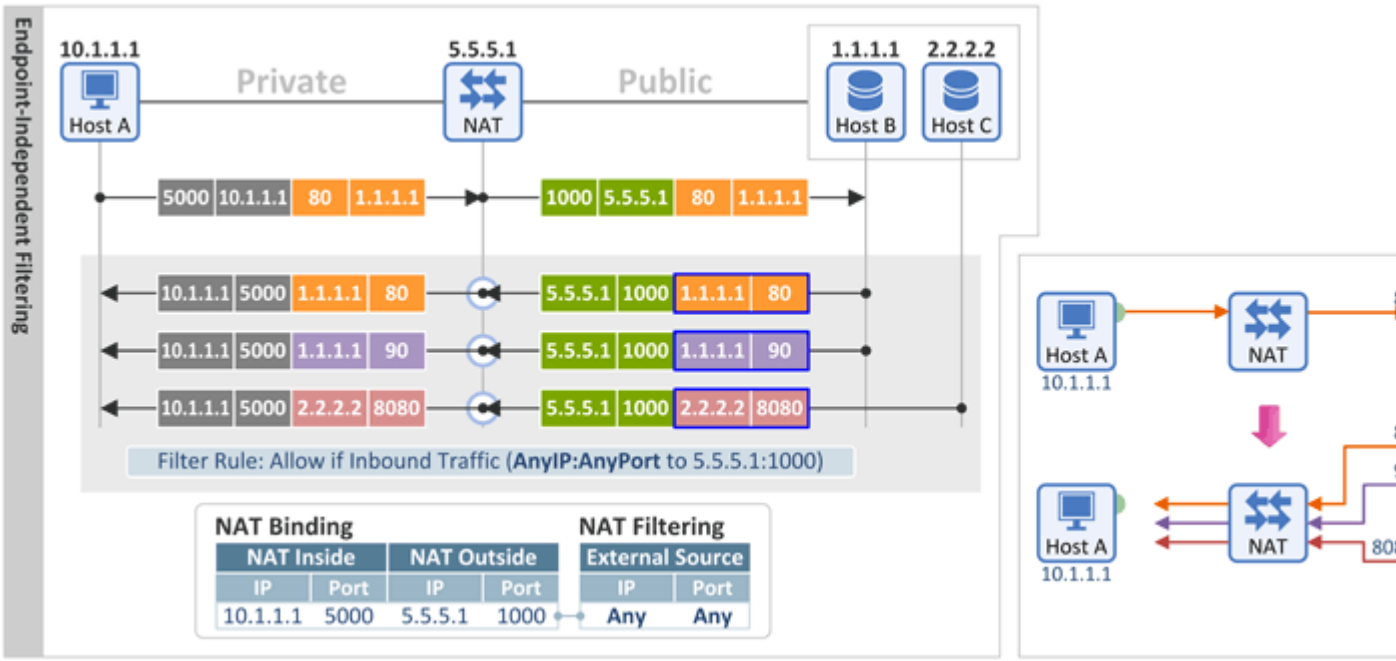
Endpoint-Independent Filtering

여기서 Endpoint 는 External Endpoint 를 의미합니다.
"목적지 독립적 필터링(Endpoint-Independent Filtering)"은 External Endpoint 가 보내는 Inbound Packet 에 대해 (1)**Destination IP** 와 (2) **Destination Port** 만 검사하여 패킷의 허용 여부를 판단하고, External Endpoint 의 소스 정보 즉, Source IP 와 Source Port 는 어떤 값(Any IP & Any Port)이라도 상관하지 않습니다. 즉, Inbound Packet 의 External Endpoint 정보(Source IP & Source Port)는 신경쓰지 않겠다는 것이죠.

[아래 그림] Host A 에서 Host B 로의 패킷 전송에 의해 다음과 같이 Binding Entry 와 Filtering Entry 가 생성 되며

- Binding Entry: {Internal IP : Internal Port} <-> {External IP : External Port} = {10.1.1.1:5000} <-> {5.5.5.1 : 1000}
- Filtering Entry: Allow if Inbound Packet **{Any IP : Any Port}** to {5.5.5.1 : 1000}

Host B나 Host C에서 Host A로 보내는 패킷(Inbound Packet)의 Destination IP/Destination Port = 5.5.5.1/1000이면 NAT는 Source IP(1.1.1.1 or 2.2.2.2)와 Source Port(80 or 8080) 값에 상관없이 이 패킷을 허용합니다.



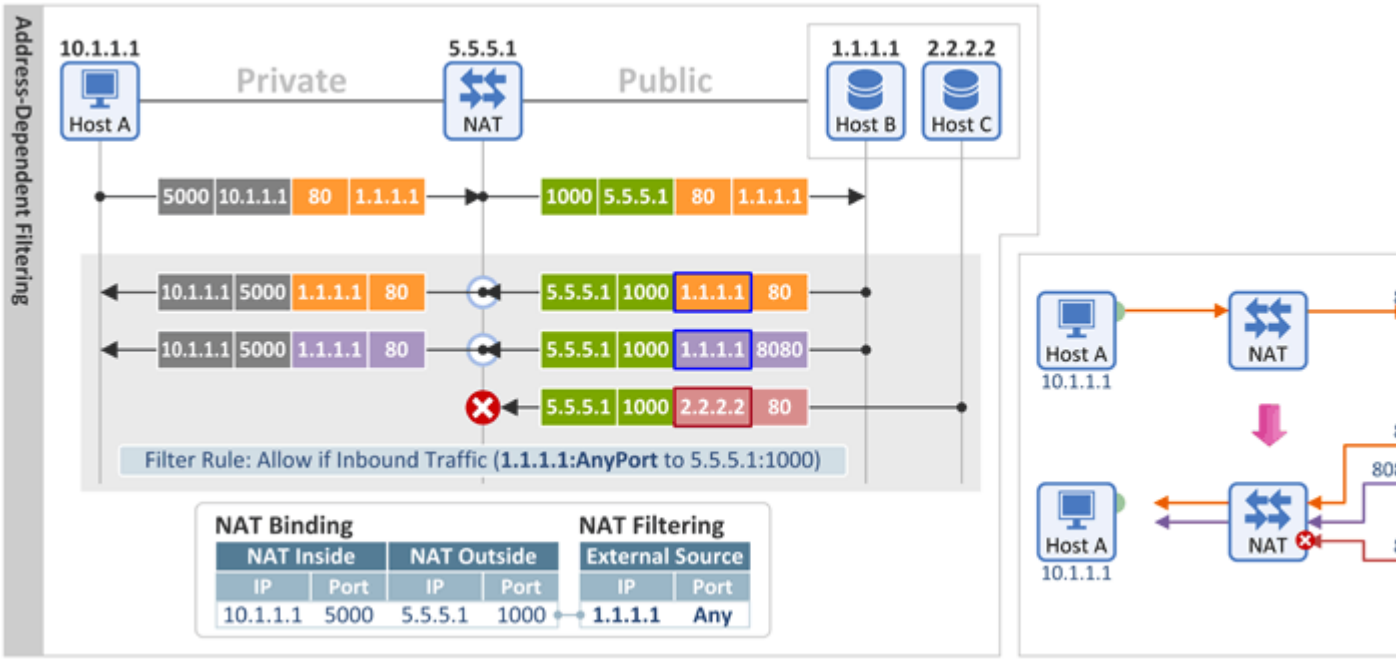
Address-Dependent Filtering

여기서 Address 는 External Endpoint 의 주소(Source IP)를 의미합니다.
"주소 의존적 필터링(Address-Dependent Filtering)"은 External Endpoint 가 보내는 Inbound Packet 에 대해 (1)**Destination IP** 와 (2) **Destination Port** 그리고 (3) **Source IP** 를 검사하여 패킷의 허용 여부를 판단하고, Source Port 는 어떤 값(Any Port)이라도 상관하지 않습니다. 즉, Internal Endpoint 가 보낸 패킷의 목적지(Source IP)로부터의 패킷만 허용하겠다는 것이죠.

[아래 그림] Host A 에서 Host B 로의 패킷 전송에 의해 다음과 같이 Binding Entry 와 Filtering Entry 가 생성 되며

- Binding Entry: {Internal IP : Internal Port} <-> {External IP : External Port} = {10.1.1.1:5000} <-> {5.5.5.1 : 1000}
- Filtering Entry: Allow if Inbound Packet **{1.1.1.1 : Any Port}** to {5.5.5.1 : 1000}

Source IP = 1.1.1.1를 가진 Host B가 보내는 Destination IP/Destination Port = 5.5.5.1/1000 패킷은 허용하고(Source Port 값에 상관 없이), Source IP = 2.2.2.2를 가진 Host C가 보내는 패킷은 폐기합니다.



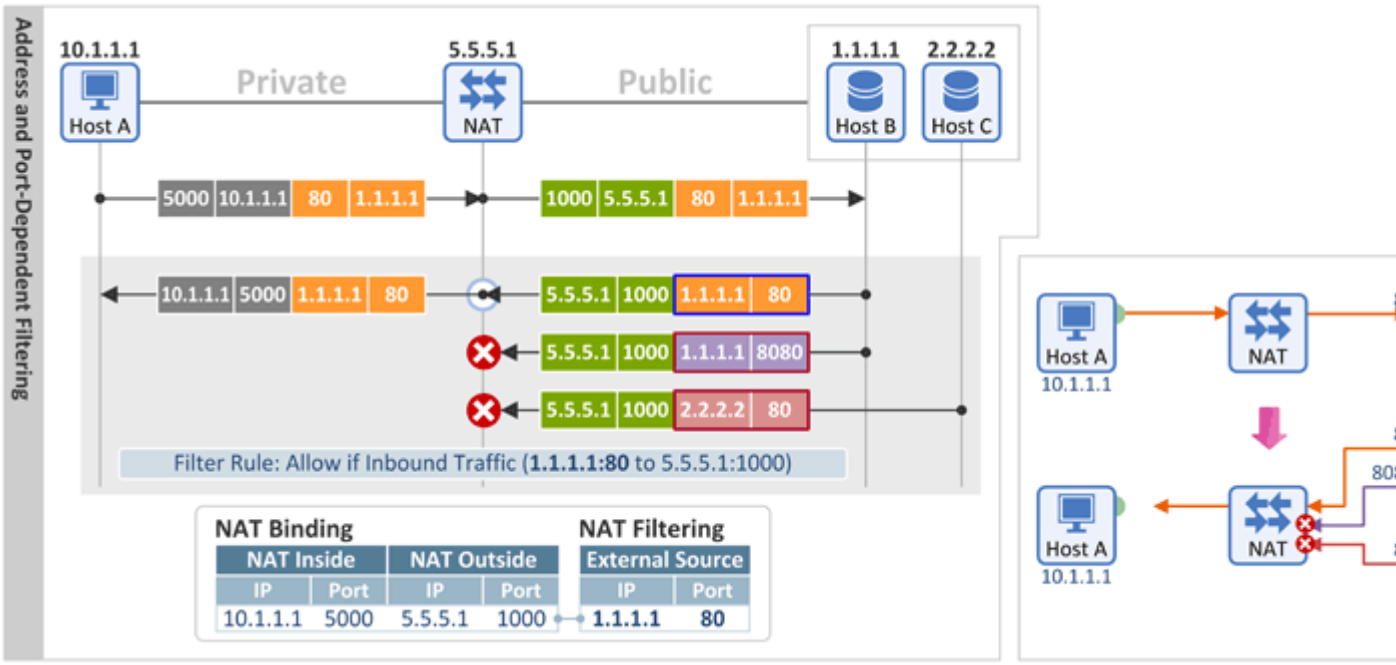
Address and Port-Dependent Filtering

여기서 Address 와 Port 는 External Endpoint 의 주소와 포트(Source IP & Source Port)를 의미합니다.
"주소 및 포트 의존적 필터링(Address and Port-Dependent Filtering)"은 External Endpoint 가 보내는 Inbound Packet 에 대해 (1) **Destination IP** 와 (2) **Destination Port** 그리고 (3) **Source IP** 와 (4) **Source Port** 를 검사하여 패킷의 허용 여부를 판단합니다.
즉, Internal Endpoint 가 보낸 패킷에 대한 응답 패킷(Source IP & Source Port)만 허용하겠다는 것이죠.

[아래 그림] Host A 에서 Host B 로의 패킷 전송에 의해 다음과 같이 Binding Entry 와 Filtering Entry 가 생성 되며

- Binding Entry: {Internal IP : Internal Port} <-> {External IP : External Port} = {10.1.1.1:5000} <-> {5.5.5.1 : 1000}
- Filtering Entry: Allow if Inbound Packet **{1.1.1.1 : 80}** to {5.5.5.1 : 1000}

Host A가 Host B로 보낸 패킷 {5.5.5.1:1000 to 1.1.1.1:80}에 대한 응답 패킷 {1.1.1.1:80 to 5.5.5.1:1000}만 허용하고, 나머지 경우는 모두 폐기합니다.



RFC 4787 권고 (REQ-8): If application transparency is most important, it is RECOMMENDED that a NAT have "Endpoint-Independent Filtering" behavior. If a more stringent filtering behavior is most important, it is RECOMMENDED that a NAT have an "Address-Dependent Filtering" behavior

RFC4798 에 따르면 Endpoint-Independent Filtering 이나 Address-Dependent Filtering 방식의 NAT 에 대해서는 ICE (Interactive Connectivity Establishment, RFC 5245)를 통해 Peer-to-Peer 통신이 가능하지만, Address and Port Dependent Mapping + Address and Port-Dependent Filtering 방식의 NAT 에 대해서는 Peer-to-Peer 통신이 불가능하여 모든 트래픽이 Relay 서버(TURN 서버)를 거칠 수 밖에 없다고 합니다.

3. Hairpinning Behavior

동일 NAT 에 속한 2 대의 Internal Endpoint 가 NAT 를 통해 서로 통신을 하는 기능을 Hairpinning 이라 합니다. 3G/LTE 망에 적용된 LSN(Large Scale NAT, 혹은 CGN(Carrier Grade NAT)라고도 함)을 통해 2 대의 무선 단말이 통신(Skeyp, 카톡 보이스 등)을 하는 경우가 대표적인 예일텐데요.
Hairpinning Behavior 는 2 가지로 나눌 수 있습니다.

External Source IP Address and Port

Host A 가 Host B 로 보내는 패킷(NAT 가 수신하는 패킷)은 아래와 같습니다.

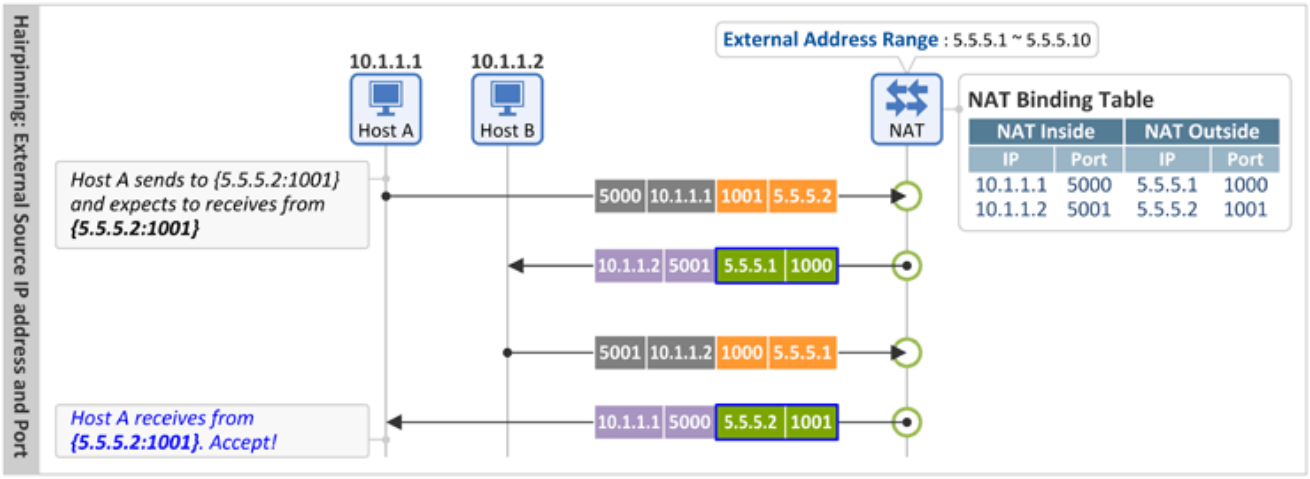
- Destination IP = Host B 의 External Address (5.5.5.2)
- Destination Port = Host B 의 External Port (1001)
- Source IP = Host A 의 Internal Address (10.1.1.1)
- Source Port = Host A 의 Internal Port (5000)

그리고 이를 수신한 NAT는 Binding Table을 참조하여 Host B로 아래와 같이 패킷 정보를 변경하여 전송합니다. 여기서 중요한 건 Source IP/Source Port가 External Address/Port라는 점입니다.

- Destination IP = Host B 의 Internal Address (10.1.1.2)
- Destination Port = Host B 의 Internal Port (5001)
- Source IP = Host A 의 External Address (5.5.5.1)
- Source Port = Host A 의 External Port (1000)

이 경우는 아주 바람직한 NAT Behavior 입니다. Host A(sender)가 보낸 패킷의 Destination IP/Port(5.5.5.2/1001)로 응답 패킷이 수신되므로(Source IP/Port=5.5.5.2/1001) 두 단말간 통신에 아무 문제가 없습니다.

아래 그림 상에 Host A의 External Address(5.5.5.1)와 Host B의 External Address(5.5.5.2)가 서로 다른 값으로 표현 되었지만 NAT의 Behavior에 따라 이 두개의 값은 같을 수도 있습니다.



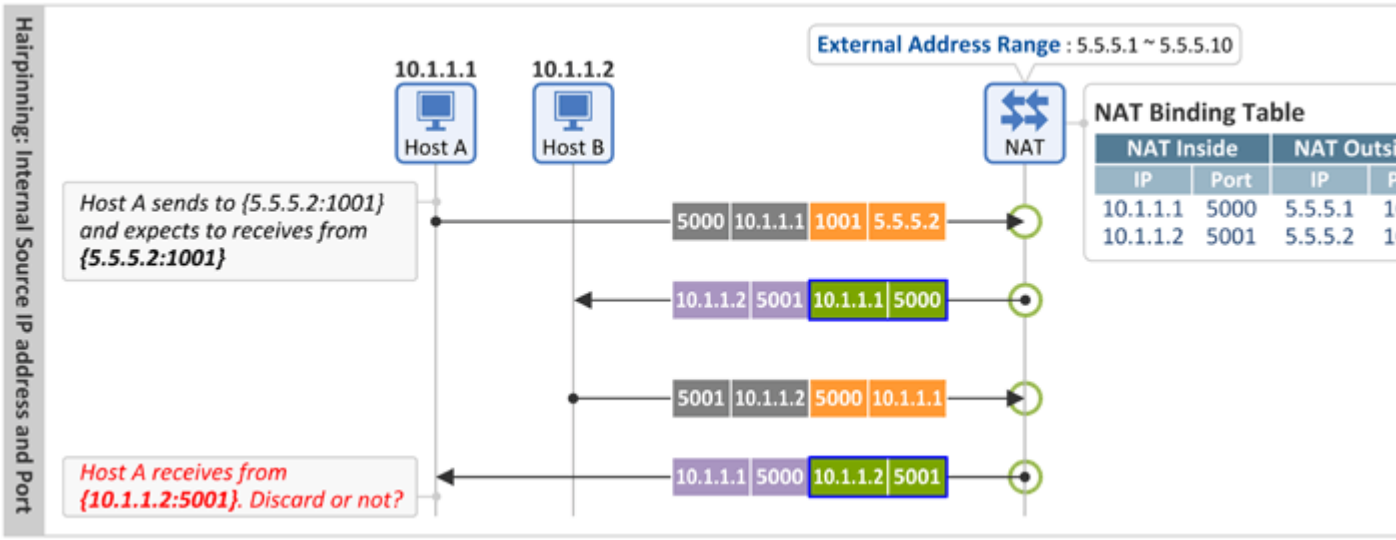
Internal Source IP Address and Port

Host A 가 Host B 로 보내는 패킷(NAT 가 수신하는 패킷)은 위와 동일하구요.
그리고 이를 수신한 NAT는 Binding Table을 참조하여 Host B로 아래와 같이 패킷 정보를 변경하여 전송합니다. 위와의 차이점은 Source IP/Source Port가 Internal Address/Port라는 점입

니다.

- Destination IP = Host B 의 Internal Address (10.1.1.2)
- Destination Port = Host B 의 Internal Port (5001)
- Source IP = Host A 의 Internal Address (10.1.1.1)
- Source Port = Host A 의 Internal Port (5000)

이 경우 Host A(sender)가 보낸 패킷의 Destination IP/Port(5.5.5.2/1001)로 응답 패킷이 수신되지 않아(Source IP/Port=10.1.1.2/5001) 커널의 TCP/IP 스택에서 본 패킷은 폐기 될 것입니다.



RFC 4787 권고 (REQ-9): A NAT MUST support "Hairpinning"

a) A NAT Hairpinning behavior MUST be "External source IP address and port"

STUN(RFC 3489)과 STUN(RFC 5389/5780)의 차이

https://www.netmanias.com/ko/?m=view&id=blog&no=5847

오늘은 RFC 3489 와 RFC 5780 에서 정의하고 있는 NAT 타입에 대해서 설명을 드리도록 하겠습니다.

지난 시간을 통해 NAT 의 Mapping Behavior 와 Filtering Behavior 에 대해 설명을 드렸는데, 그 내용을 숙지하셔야만 오늘 내용을 이해하실 수 있을 것입니다.

STUN 이란?

STUN 은 P2P 통신을 위해 두 단말 사이에 NAT 의 존재 유무 및 NAT 타입을 식별(discover)하고 또한 NAT 에 의해 변경되는 External IP 주소 및 External Port 값을 P2P 단말이 알 수 있도록 해 주는 프로토콜입니다.

본 프로토콜은 2003 년도 RFC 3489(Standards)를 통해 먼저 표준화 되었고, 이후 2008 년도 RFC 5389(Standard)와 2010 년도 RFC 5780(Experimental)을 통해 개정되었습니다.
RFC 5389 의 설명에 따르면, "Classic STUN 즉, RFC 3489 에 기술된 NAT 타입 식별 알고리즘에는 오류가 있으며, 현재 시중에 나와 있는 NAT 장비를 RFC 3489 에 정의된 4 가지 타입으로 분류하는데 한계가 있다."라고 되어 있습니다.
이에 RFC 5389 를 통해 기존 STUN 프로토콜이 수정(Binding Message 의 Attribute 추가) 되었고, 또한 RFC 5780 을 통해 NAT 타입 분류 재정의 및 NAT 타입 식별 알고리즘(방식)을 수정하게 되었습니다.

RFC 3489 와 RFC 5389 표준에서는 STUN 이란 동일 제목을 사용하고 있지만 아래와 같이 그 풀이를 다르게 하고 있습니다.

- RFC 3489: STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
- RFC 5389: Session Traversal Utilities for NAT (STUN)

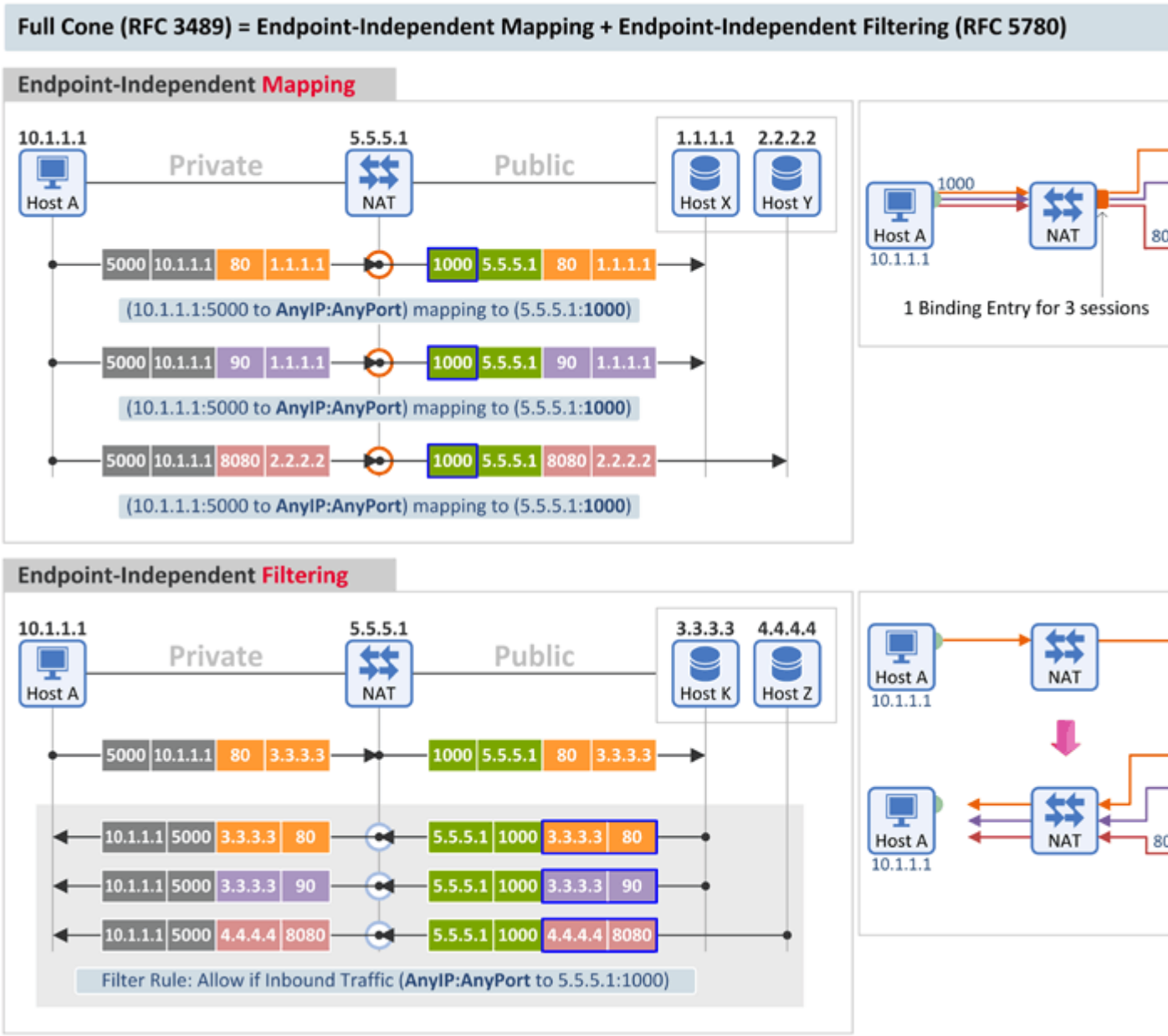
RFC 3489 의 NAT 타입 및 RFC 5780 과의 관계

■ Full Cone

[Mapping Behavior] A full cone NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. **[Filtering Behavior]** Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address. (RFC 3489)

Full Cone 타입은 RFC 5780 에 Endpoint-Independent Mapping(이하 EIM)과 Endpoint-Independent Filtering(이하 EIF)으로 동작하는 방식을 말합니다.

- Mapping Behavior: Outbound 패킷의 (1) Source IP, (2) Source Port 만 동일하다면 Destination IP, Destination Port 에 상관없이 같은 Port Mapping 값(Translated Port = 1000)을 사용
- Filtering Behavior: Inbound 패킷에 대해 (1) Destination IP, (2) Destination Port 만 검사하여 패킷의 허용 여부를 판단하고, External Endpoint 의 소스 정보 즉, Source IP 와 Source Port 값은 상관하지 않음



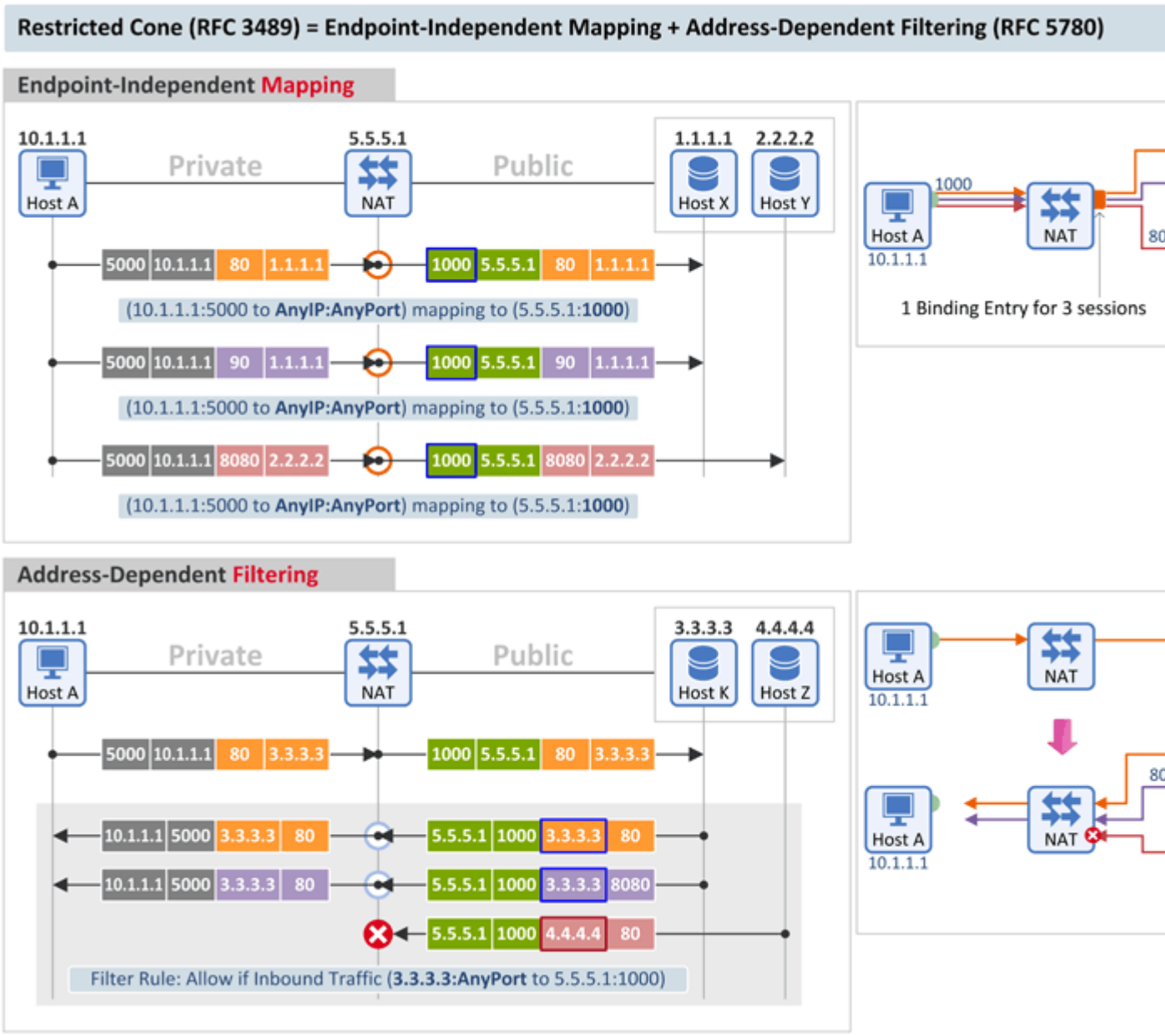
■ Restricted Cone

[Mapping Behavior] A restricted cone NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. **[Filtering**

Behavior] Unlike a full cone NAT, an external host (with IP address X) can send a packet to the internal host only if the internal host had previously sent a packet to IP address X. (RFC 3489)

Restricted Cone 타입은 RFC 5780 에 EIM 과 Address-Dependent Filtering(이하 ADF)으로 동작하는 방식을 말합니다.

- Mapping Behavior: Full Con 과 동일
- Filtering Behavior: Inbound 패킷에 대해 (1) Destination IP, (2) Destination Port 그리고 (3) Source IP 를 검사하여 패킷의 허용 여부를 판단하고, External Endpoint 의 Source Port 값은 상관하지 않음



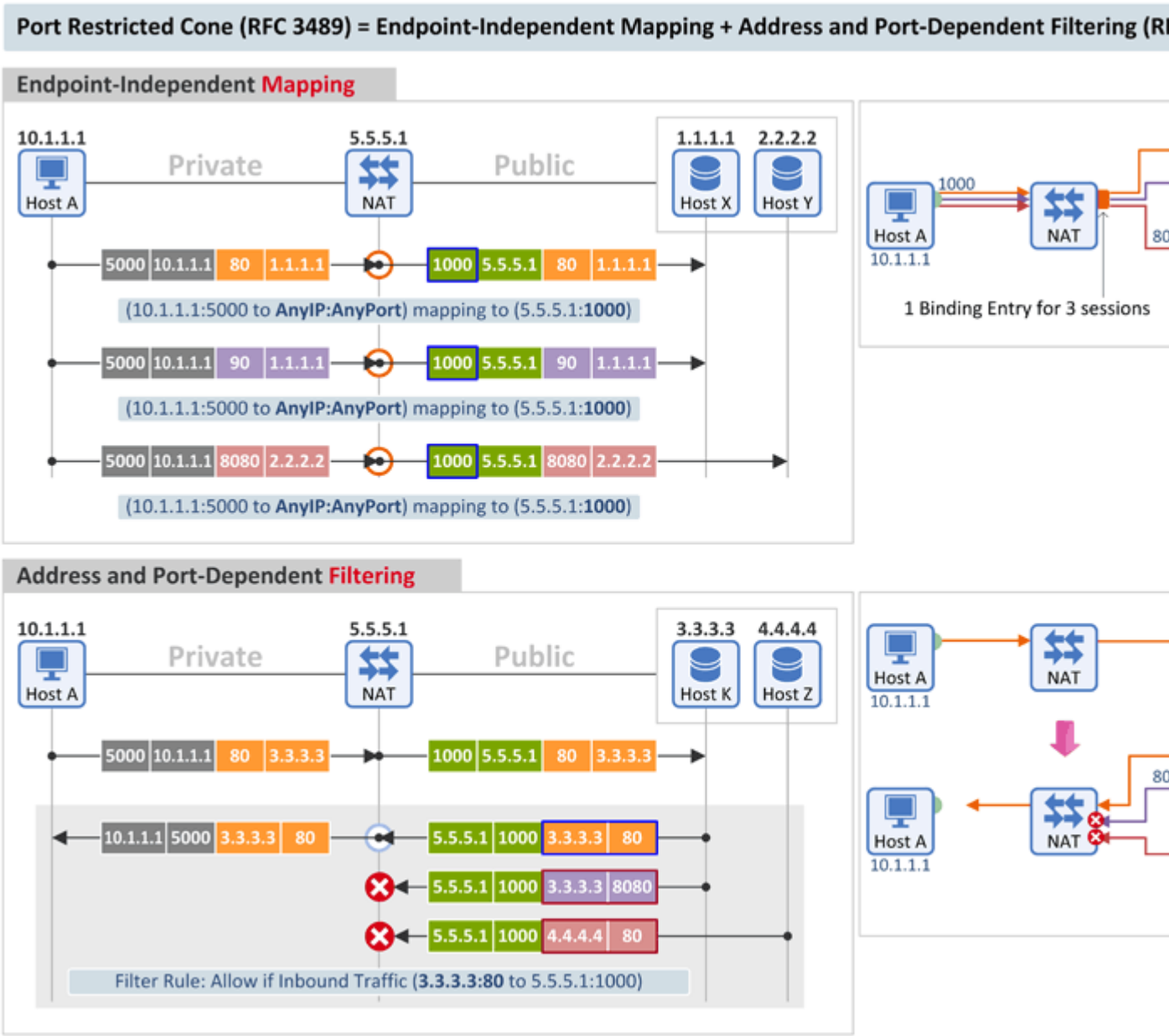
■ Port Restricted Cone

[Mapping Behavior] A port restricted cone NAT is like a restricted cone NAT, **[Filtering Behavior]** but the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P. (RFC 3489)

Port Restricted Cone 타입은 RFC 5780 에 EIM 과 Address and Port-Dependent Filtering(이하 APDF)으로 동작하는 방식을 말합니다.

- Mapping Behavior: Full Con 과 동일

- Filtering Behavior: Inbound 패킷에 대해 (1) Destination IP, (2) Destination Port 그리고 (3) Source IP, (4) Source Port 를 검사하여 패킷의 허용 여부를 판단함

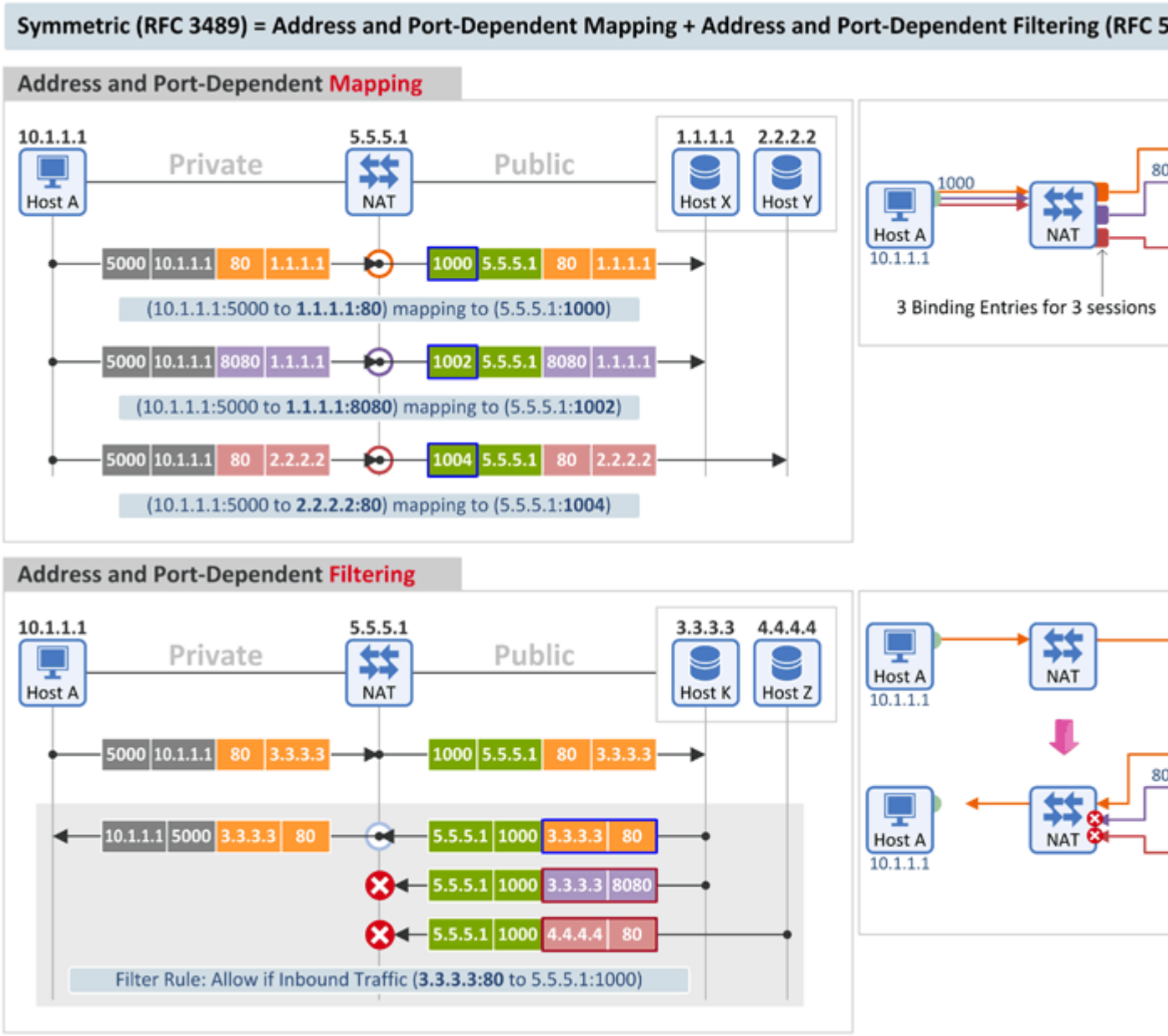


■ Symmetric

[Mapping Behavior] A symmetric NAT is one where all requests from the same internal IP address and port, to a specific destination IP address and port, are mapped to the same external IP address and port. If the same host sends a packet with the same source address and port, but to a different destination, a different mapping is used. **[Filtering Behavior]** Furthermore, only the external host that receives a packet can send a UDP packet back to the internal host. (RFC 3489)

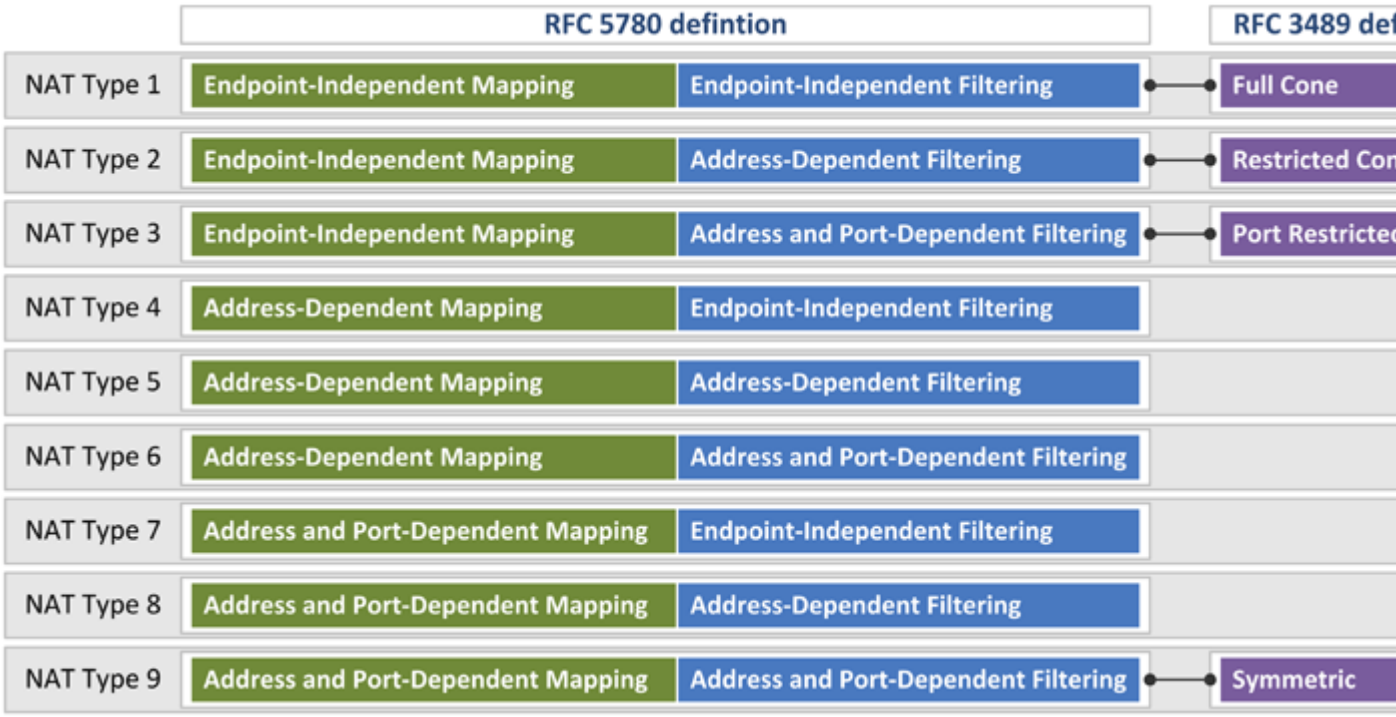
Symmetric 타입은 RFC 5780 에 Address and Port-Dependent Mapping(이하 APDM)과 APDF 로 동작하는 방식을 말합니다.

- Mapping Behavior: Outbound 패킷의 (1) Source IP, (2) Source Port 그리고 (3) Destination IP, (4) Destination Port 가 모두 동일해야 같은 Port Mapping 값을 사용
- Filtering Behavior: Port Restricted Con 과 동일



요약

아래 그림은 RFC 5780 에서 정의하고 있는 9 개의 NAT 타입과 RFC 3489 에서 정의하고 있는 4 개의 NAT 타입 간의 관계를 보이고 있습니다.



STUN(RFC 5780)을 이용한 NAT Behavior Discovery

https://www.netmanias.com/ko/?m=view&id=blog&no=5856

지난 시간을 통해 RFC 3489 에서 정의하고 있는 NAT 타입 조사(NAT Behavior Discovery) 알고리즘에 대해 설명을 드렸는데요. 오늘은 RFC 5780 의 NAT 타입 조사 알고리즘에 대해서 알아 보도록 하겠습니다.

지난 시간과 마찬가지로 본 내용을 이해하기 위해서는 아래 블로그글을 반드시 먼저 읽어 보시기 바랍니다.

1. NAT 장비는 이렇게 만들어야 하는데... (RFC 4787) - 1편: Mapping Behavior
2. NAT 장비는 이렇게 만들어야 하는데... (RFC 4787) - 2편: Filtering Behavior

3. STUN(RFC 3489)과 STUN(RFC 5389/5780)의 차이

STUN Protocol

STUN 프로토콜은 참 간단하게 설계 되어 있습니다. 단말(STUN Client)은 서버(STUN Server)로 Binding Request 메시지를 보내고, 서버는 그 응답으로 Binding Response 메시지를 단말로 보냅니다. 이게 전부입니다.
NAT 타입(Mapping & Filtering Behavior)을 검출하기 위해 서버는 2 개의 Public IP 주소와 2 개의 소스 포트(보통 3478, 3479)를 가지고 있어야 하며, 하나를 Primary IP/Port(예: 1.1.1.1:3478), 다른 하나를 Alternate IP/Port(예: 2.2.2.2:3479)라 부릅니다.
그리고 이 두 메시지에는 아래와 같은 Attribute 들이 실리게 됩니다.

[Client -> Server] Binding Request message's Attribute

- **CHANGE-REQUEST**: Filtering Behavior 를 조사하기 위해 사용되는 attribute 로, "Change IP" flag 와 "Change Port" flag 로 구성됩니다. 단말에서 이 flag 를 0 으로 하여 보내면, 서버는 단말이 전송한 Binding Request 메시지의 Destination IP/Port 를 그대로 Binding Response 메시지의 Source IP/Port(예: 1.1.1.1:3478)로 사용하고, 만약 flag 가 1 로 되어 있으면 서버가 가지고 있는 다른 IP/Port(예: 2.2.2.2:3479)를 사용하여 응답하게 됩니다.

[Client <- Server] Binding Response message's Attribute

- **MAPPED-ADDRESS**: 서버가 수신한 Binding Request 메시지의 Source IP/Port 값이 본 attribute 에 실립니다. 만약 NAT 가 존재하지 않는다면 이 필드의 값은 단말의 Source IP/Port 가 될 것이고, NAT 가 존재한다면 NAT 에 의해 변경된 값이 들어갈 것입니다.
- **RESPONSE-ORIGIN**: 서버가 전송하는 Binding Response 메시지의 Source IP/Port 정보가 이 attribute 에 실립니다.
- **OTHER-ADDRESS**: 서버는 2 개의 IP/Port 를 가진다고 말씀드렸는데요. 이 attribute 에는 서버가 수신한 Binding Request 메시지의 Destination IP/Port(서버의 IP/Port)와 다른 값의 (서버가 소유한) IP/Port 가 실리게 됩니다.
- **XOR-MAPPED-ADDRESS**: MAPPED-ADDRESS 와 동일한 값이 XOR 연산으로 변형되어 실리게 됩니다. 이를 수신한 단말은 역시 XOR 연산을 통해 MAPPED-ADDRESS 의 값을 알아 냅니다. 어떤 NAT 의 경우 잘못된 ALG 구현으로 인해 Payload(Binding

Request/Response 필드) 내에 IP 헤더와 동일한 IP 주소 값이 존재하면 이를 변경하는 경우가 있어 MAPPED-ADDRESS 의 값이 훼손될 수 있습니다. 이와 같이 잘못된 ALG 구현으로 인한 NAT 타입 검출 오류를 방지하고자 XOR-MAPPED-ADDRESS 를 정의하였습니다. 그래서 RFC 5780 에서는 MAPPED-ADDRESS 의 값을 사용하지는 않습니다. 다만 RFC 3489 와의 하위 호환성을 위해 유지하고 있습니다.

NAT Mapping Behavior

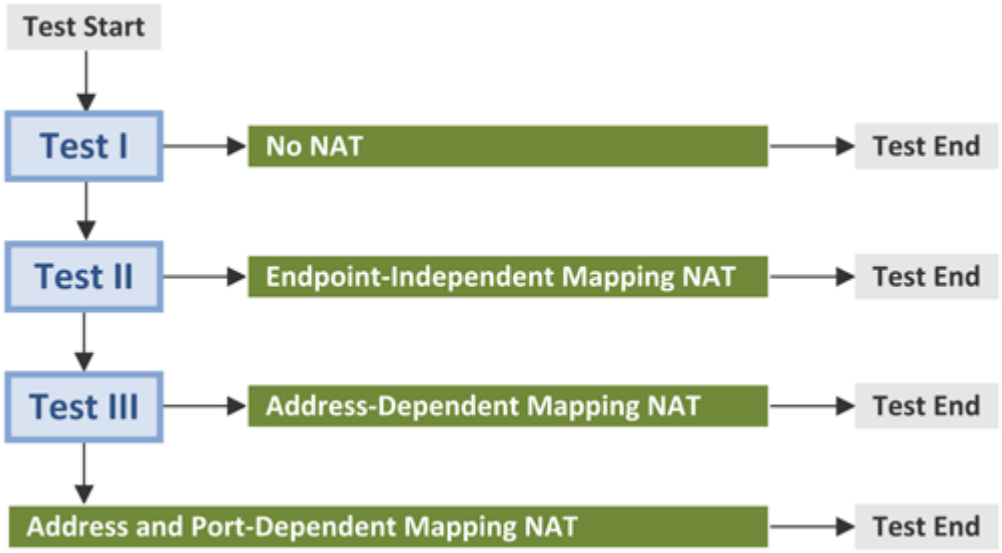
아래는 RFC 5780 에서 설명하고 있는 NAT Mapping Behavior Discovery 알고리즘입니다. 본 내용을 바탕으로 NAT 의 Mapping Behavior 타입 별로 시험 과정을 나누어 설명 드리도록 하겠습니다.

4.3 Determining NAT Mapping Behavior

This will require at most three tests. In **test I**, the client performs the UDP connectivity test. The server will return its alternate address and port in OTHER-ADDRESS in the binding response. If OTHER-ADDRESS is not returned, the server does not support this usage and this test cannot be run. The client examines the XOR-MAPPED-ADDRESS attribute. If this address and port are the same as the local IP address and port of the socket used to send the request, the client knows that it is not NATed and the effective mapping will be Endpoint-Independent.

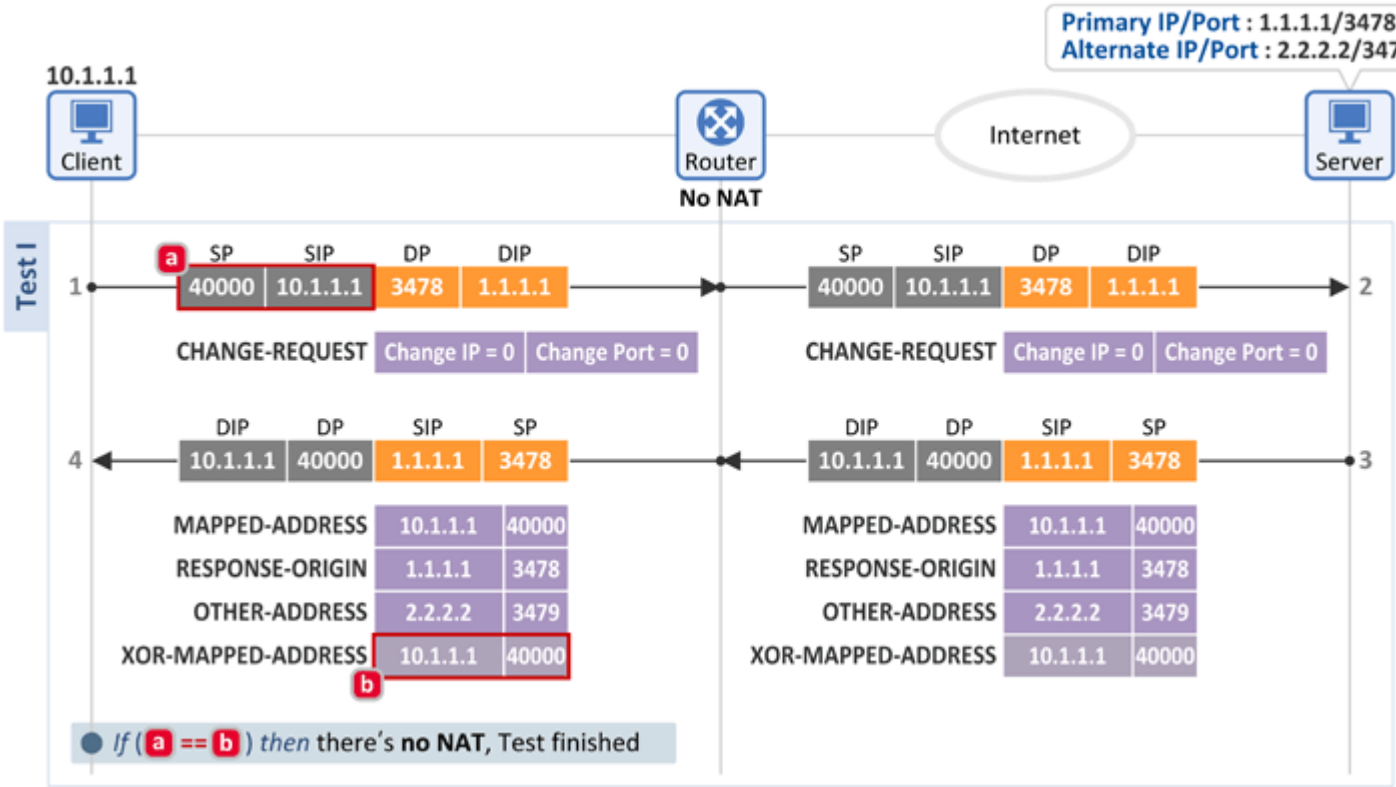
In **test II**, the client sends a Binding Request to the alternate address, but primary port. If the XOR-MAPPED-ADDRESS in the Binding Response is the same as test I the NAT currently has Endpoint-Independent Mapping. If not, **test III** is performed: the client sends a Binding Request to the alternate address and port. If the XOR-MAPPED-ADDRESS matches test II, the NAT currently has Address-Dependent Mapping; if it doesn't match it currently has Address and Port-Dependent Mapping.

■ Test (Discovery) Procedure



- Test I 을 통해 NAT 의 존재 유무 확인
- Test II 를 통해 Endpoint-Independent Mapping NAT 식별
- Test III 를 통해 Address-Dependent Mapping NAT 혹은 Address and Port-Dependent Mapping NAT 식별

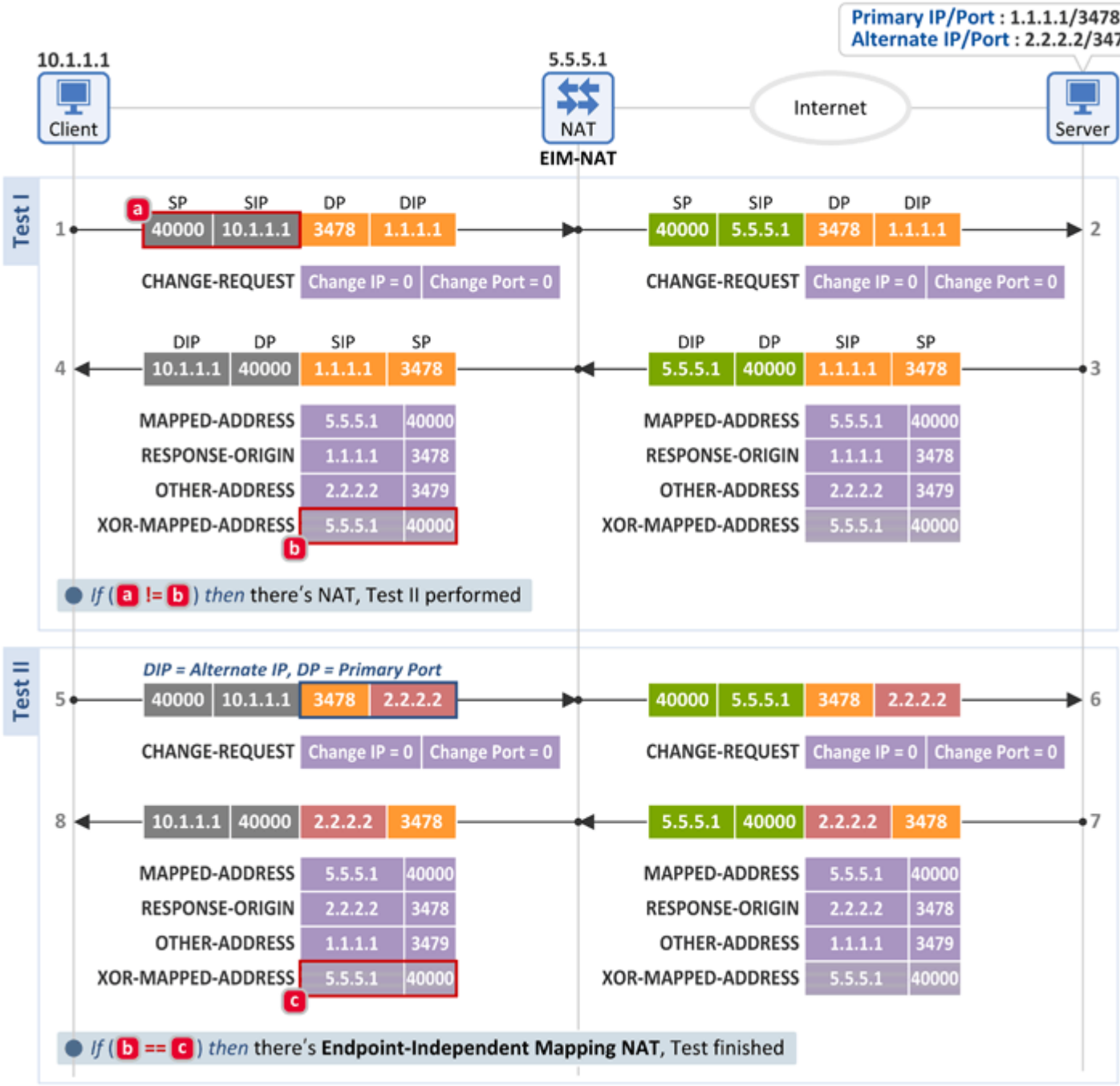
■ NAT가 없는 경우



■ **Test I**

- 단말은 서버의 Primary IP:Primary Port(1.1.1.1:3478)로 Binding Request 메시지를 전송하고 그 응답으로 Binding Response 메시지를 수신합니다.
- 그리고 단말은 아래 2 개의 필드를 비교하여 그 값이 동일하면 단말과 인터넷 사이에 NAT 가 없다고 판단합니다.
    - **[a]** Binding Request 메시지: IP 헤더 소스 정보 = 10.1.1.1.:40000
    - **[b]** Binding Response 메시지: XOR-MAPPED-ADDRESS attribute = 10.1.1.1:40000
- 서버는 Binding Request 메시지의 소스 정보[a]를 Binding Response 메시지의 XOR-MAPPED-ADDRESS[b]에 실어 단말로 전송하므로 이 2 개의 값이 같다는 것은 NAT 가 존재하지 않아 주소/포트 변환이 일어나지 않았다는 의미입니다.

■ Endpoint-Independent Mapping NAT(EIM-NAT)인 경우



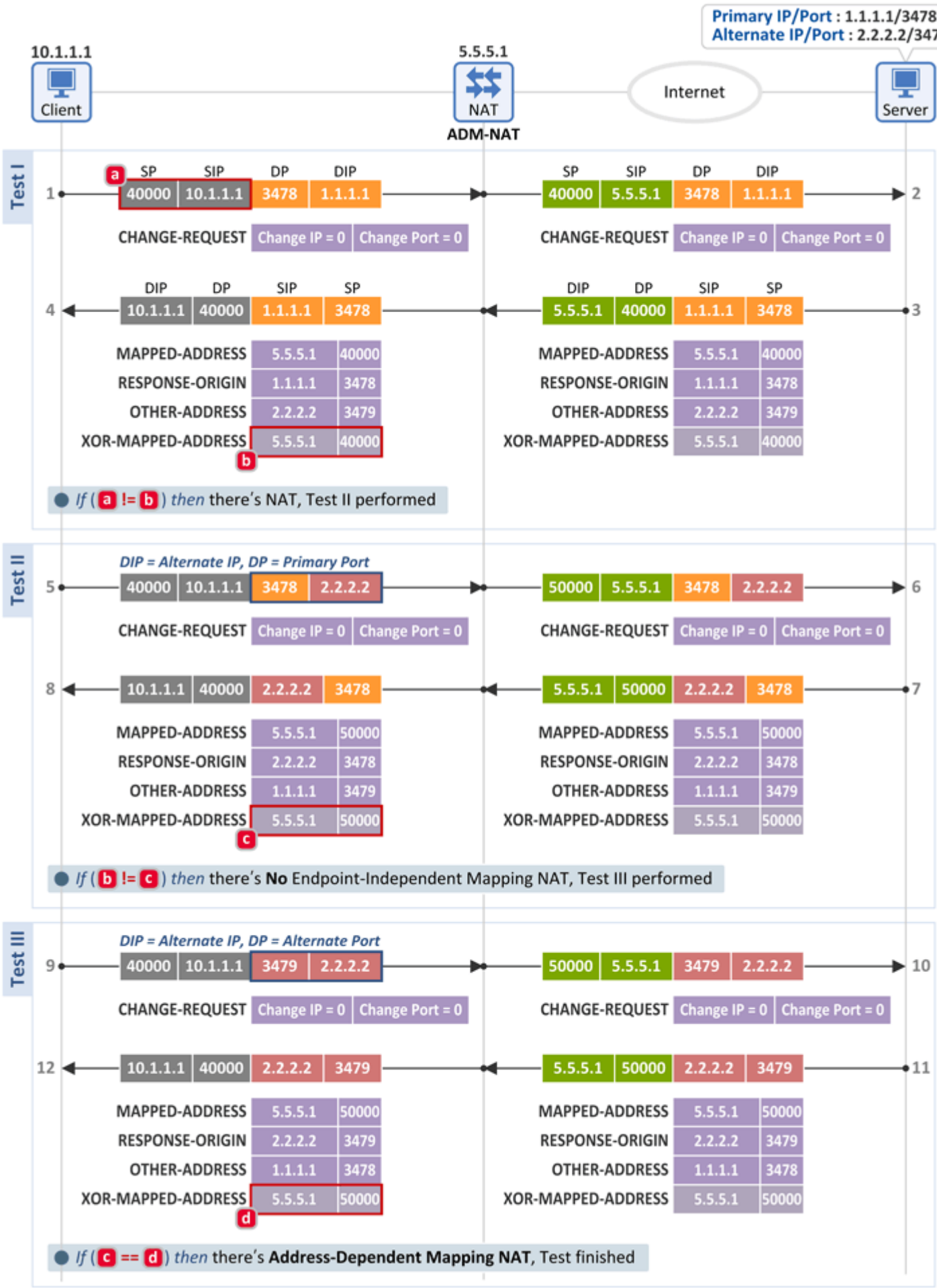
■ Test I

- 단말은 서버의 Primary IP:Primary Port(1.1.1.1:3478)로 Binding Request 메시지를 전송하고 그 응답으로 Binding Response 메시지를 수신합니다.
- 그리고 단말은 아래 2 개의 필드를 비교하여 그 값이 같지 않으면 단말과 인터넷 사이에 NAT 가 존재한다고 판단하고 Test II 를 진행합니다.
    - **[a]** Binding Request 메시지: IP 헤더 소스 정보 = 10.1.1.1.:40000
    - **[b]** Binding Response 메시지: XOR-MAPPED-ADDRESS attribute = 5.5.5.1:40000

■ **Test II**

- 단말은 서버로 Binding Request 메시지를 전송하는데 Test I 과 다른 점은 Destination IP 주소로 Alternate IP 를 사용한다는 것입니다. 즉, Alternate IP:Primary Port(2.2.2.2:3478)로 Binding Request 메시지를 송신하고 그 응답으로 Binding Response 메시지를 수신합니다.
- 그리고 단말은 아래 2 개의 필드를 비교하여 그 값이 동일하면 EIM-NAT(Endpoint-Independent Mapping NAT)가 존재한다고 판단합니다.
    - **[b]** Binding Response 메시지: XOR-MAPPED-ADDRESS attribute = 5.5.5.1:40000
    - **[c]** Binding Response 메시지: XOR-MAPPED-ADDRESS attribute = 5.5.5.1:40000
- 즉, 서로 다른 Destination IP(1.1.1.1 or 2.2.2.2)로 전송한 2 개의 패킷이 동일한 External IP:Port(5.5.5.1:40000)로 매핑되었으므로 EIM-NAT 입니다.

■ Address-Dependent Mapping NAT(ADM-NAT)인 경우


Primary IP/Port : 1.1.1.1/3478
Alternate IP/Port : 2.2.2.2/347
10.1.1.1
Client
5.5.5.1
NAT
ADM-NAT
Internet
Server
Test I
SP SIP DP DIP
a
1
40000 10.1.1.1 3478 1.1.1.1
CHANGE-REQUEST Change IP = 0 Change Port = 0
SP SIP DP DIP
2
40000 5.5.5.1 3478 1.1.1.1
CHANGE-REQUEST Change IP = 0 Change Port = 0
DIP DP SIP SP
4
10.1.1.1 40000 1.1.1.1 3478
MAPPED-ADDRESS 5.5.5.1 40000
RESPONSE-ORIGIN 1.1.1.1 3478
OTHER-ADDRESS 2.2.2.2 3479
XOR-MAPPED-ADDRESS 5.5.5.1 40000
b
DIP DP SIP SP
3
5.5.5.1 40000 1.1.1.1 3478
MAPPED-ADDRESS 5.5.5.1 40000
RESPONSE-ORIGIN 1.1.1.1 3478
OTHER-ADDRESS 2.2.2.2 3479
XOR-MAPPED-ADDRESS 5.5.5.1 40000
If (a != b) then there's NAT, Test II performed
Test II
DIP = Alternate IP, DP = Primary Port
5
40000 10.1.1.1 3478 2.2.2.2
CHANGE-REQUEST Change IP = 0 Change Port = 0
6
50000 5.5.5.1 3478 2.2.2.2
CHANGE-REQUEST Change IP = 0 Change Port = 0
8
10.1.1.1 40000 2.2.2.2 3478
MAPPED-ADDRESS 5.5.5.1 50000
RESPONSE-ORIGIN 2.2.2.2 3478
OTHER-ADDRESS 1.1.1.1 3479
XOR-MAPPED-ADDRESS 5.5.5.1 50000
c
7
5.5.5.1 50000 2.2.2.2 3478
MAPPED-ADDRESS 5.5.5.1 50000
RESPONSE-ORIGIN 2.2.2.2 3478
OTHER-ADDRESS 1.1.1.1 3479
XOR-MAPPED-ADDRESS 5.5.5.1 50000
If (b != c) then there's No Endpoint-Independent Mapping NAT, Test III performed
Test III
DIP = Alternate IP, DP = Alternate Port
9
40000 10.1.1.1 3479 2.2.2.2
CHANGE-REQUEST Change IP = 0 Change Port = 0
10
50000 5.5.5.1 3479 2.2.2.2
CHANGE-REQUEST Change IP = 0 Change Port = 0
12
10.1.1.1 40000 2.2.2.2 3479
MAPPED-ADDRESS 5.5.5.1 50000
RESPONSE-ORIGIN 2.2.2.2 3479
OTHER-ADDRESS 1.1.1.1 3478
XOR-MAPPED-ADDRESS 5.5.5.1 50000
d
11
5.5.5.1 50000 2.2.2.2 3479
MAPPED-ADDRESS 5.5.5.1 50000
RESPONSE-ORIGIN 2.2.2.2 3479
OTHER-ADDRESS 1.1.1.1 3478
XOR-MAPPED-ADDRESS 5.5.5.1 50000
If (c == d) then there's Address-Dependent Mapping NAT, Test finished

■ **Test I**

- EIM-NAT 시험과 동일

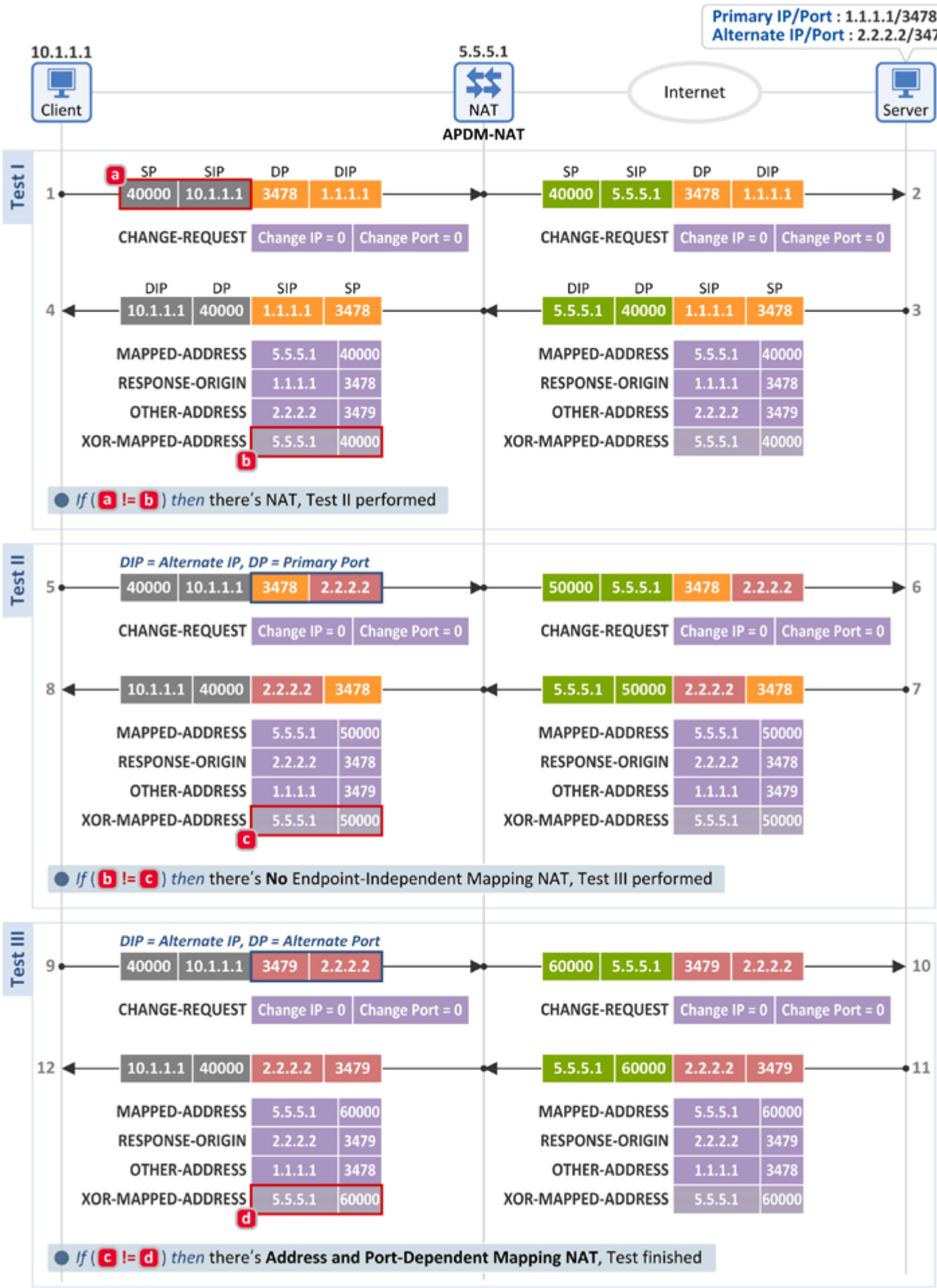
■ **Test II**

- EIM-NAT 시험과 동일한 Binding Request 메시지를 전송하고 그 응답으로 Binding Response 메시지를 수신하여,
- 단말은 아래 2 개의 필드를 비교하여 그 값이 같지 않으면 EIM-NAT 가 아니라고 판단하고 Test III 를 진행합니다.
    - **[b]** Binding Response 메시지: XOR-MAPPED-ADDRESS attribute = 5.5.5.1:40000
    - **[c]** Binding Response 메시지: XOR-MAPPED-ADDRESS attribute = 5.5.5.1:50000

■ **Test III**

- 단말은 서버의 Alternate IP:Alternate Port(2.2.2.2:3479)로 Binding Request 메시지를 전송하고 그 응답으로 Binding Response 메시지를 수신합니다.
- 그리고 단말은 아래 2 개의 필드를 비교하여 그 값이 동일하면 ADM-NAT(Address-Dependent Mapping NAT)가 존재한다고 판단합니다.
    - **[c]** Binding Response 메시지: XOR-MAPPED-ADDRESS attribute = 5.5.5.1:50000
    - **[d]** Binding Response 메시지: XOR-MAPPED-ADDRESS attribute = 5.5.5.1:50000
- 즉, 동일 Destination IP(2.2.2.2)에 서로 다른 Destination Port(3478 or 3479)로 전송한 2 개의 패킷이 동일한 External IP:Port(5.5.5.1:50000)로 매핑되었으므로 ADM-NAT 입니다.

■ Address and Port-Dependent Mapping NAT(APDM-NAT)인 경우


Primary IP/Port : 1.1.1.1/3478
Alternate IP/Port : 2.2.2.2/347
10.1.1.1
Client
5.5.5.1
NAT
APDM-NAT
Internet
Server
Test I
1
SP SIP DP DIP
a
40000 10.1.1.1 3478 1.1.1.1
CHANGE-REQUEST Change IP = 0 Change Port = 0
2
SP SIP DP DIP
40000 5.5.5.1 3478 1.1.1.1
CHANGE-REQUEST Change IP = 0 Change Port = 0
4
DIP DP SIP SP
10.1.1.1 40000 1.1.1.1 3478
MAPPED-ADDRESS 5.5.5.1 40000
RESPONSE-ORIGIN 1.1.1.1 3478
OTHER-ADDRESS 2.2.2.2 3479
XOR-MAPPED-ADDRESS 5.5.5.1 40000
b
3
DIP DP SIP SP
5.5.5.1 40000 1.1.1.1 3478
MAPPED-ADDRESS 5.5.5.1 40000
RESPONSE-ORIGIN 1.1.1.1 3478
OTHER-ADDRESS 2.2.2.2 3479
XOR-MAPPED-ADDRESS 5.5.5.1 40000
If (a != b) then there's NAT, Test II performed
Test II
DIP = Alternate IP, DP = Primary Port
5
40000 10.1.1.1 3478 2.2.2.2
CHANGE-REQUEST Change IP = 0 Change Port = 0
6
50000 5.5.5.1 3478 2.2.2.2
CHANGE-REQUEST Change IP = 0 Change Port = 0
8
10.1.1.1 40000 2.2.2.2 3478
MAPPED-ADDRESS 5.5.5.1 50000
RESPONSE-ORIGIN 2.2.2.2 3478
OTHER-ADDRESS 1.1.1.1 3479
XOR-MAPPED-ADDRESS 5.5.5.1 50000
c
7
5.5.5.1 50000 2.2.2.2 3478
MAPPED-ADDRESS 5.5.5.1 50000
RESPONSE-ORIGIN 2.2.2.2 3478
OTHER-ADDRESS 1.1.1.1 3479
XOR-MAPPED-ADDRESS 5.5.5.1 50000
If (b != c) then there's No Endpoint-Independent Mapping NAT, Test III performed
Test III
DIP = Alternate IP, DP = Alternate Port
9
40000 10.1.1.1 3479 2.2.2.2
CHANGE-REQUEST Change IP = 0 Change Port = 0
10
60000 5.5.5.1 3479 2.2.2.2
CHANGE-REQUEST Change IP = 0 Change Port = 0
12
10.1.1.1 40000 2.2.2.2 3479
MAPPED-ADDRESS 5.5.5.1 60000
RESPONSE-ORIGIN 2.2.2.2 3479
OTHER-ADDRESS 1.1.1.1 3478
XOR-MAPPED-ADDRESS 5.5.5.1 60000
d
11
5.5.5.1 60000 2.2.2.2 3479
MAPPED-ADDRESS 5.5.5.1 60000
RESPONSE-ORIGIN 2.2.2.2 3479
OTHER-ADDRESS 1.1.1.1 3478
XOR-MAPPED-ADDRESS 5.5.5.1 60000
If (c != d) then there's Address and Port-Dependent Mapping NAT, Test finished

■ **Test I**

- ADM-NAT 시험과 동일

■ **Test II**

- ADM-NAT 시험과 동일

■ **Test III**

- ADM-NAT 시험과 동일한 Binding Request 메시지를 전송하고 그 응답으로 Binding Response 메시지를 수신하며,
- 단말은 아래 2 개의 필드를 비교하여 그 값이 같지 않으면 APDM-NAT(Address and Port-Dependent Mapping NAT)가 존재한다고 판단합니다.
    - **[c]** Binding Response 메시지: XOR-MAPPED-ADDRESS attribute = 5.5.5.1:50000
    - **[d]** Binding Response 메시지: XOR-MAPPED-ADDRESS attribute = 5.5.5.1:60000
- 즉, 동일 Destination IP(2.2.2.2)에 서로 다른 Destination Port(3478 or 3479)로 전송한 2 개의 패킷이 서로 다른 External IP:Port(5.5.5.1:50000 and 5.5.5.1:60000)으로 매핑되었으므로 APDM-NAT 입니다.

NAT Filtering Behavior

아래는 RFC 5780 에서 설명하고 있는 NAT Filtering Behavior Discovery 알고리즘입니다.

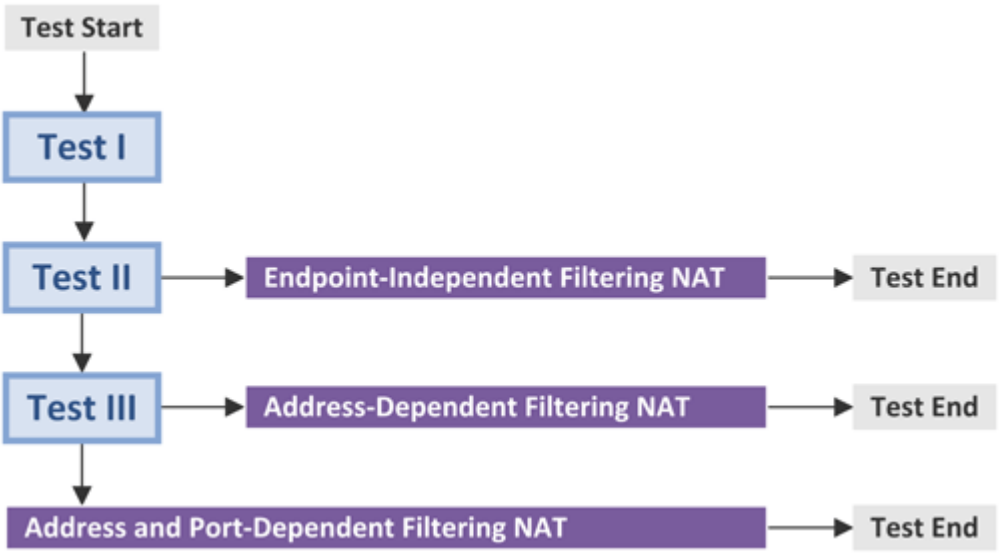
4.4 Determining NAT Filtering Behavior

In **test I**, the client performs the UDP connectivity test. The server will return its alternate address and port in OTHER-ADDRESS in the binding response. If OTHER-ADDRESS is not returned, the server does not support this usage and this test cannot be run.

In **test II**, the client sends a binding request to the primary address of the server with the CHANGE-REQUEST attribute set to change-port and change-IP. This will cause the server to send its response from its alternate IP address and alternate port. If the client receives a response, the current behavior of the NAT is Endpoint-Independent Filtering.

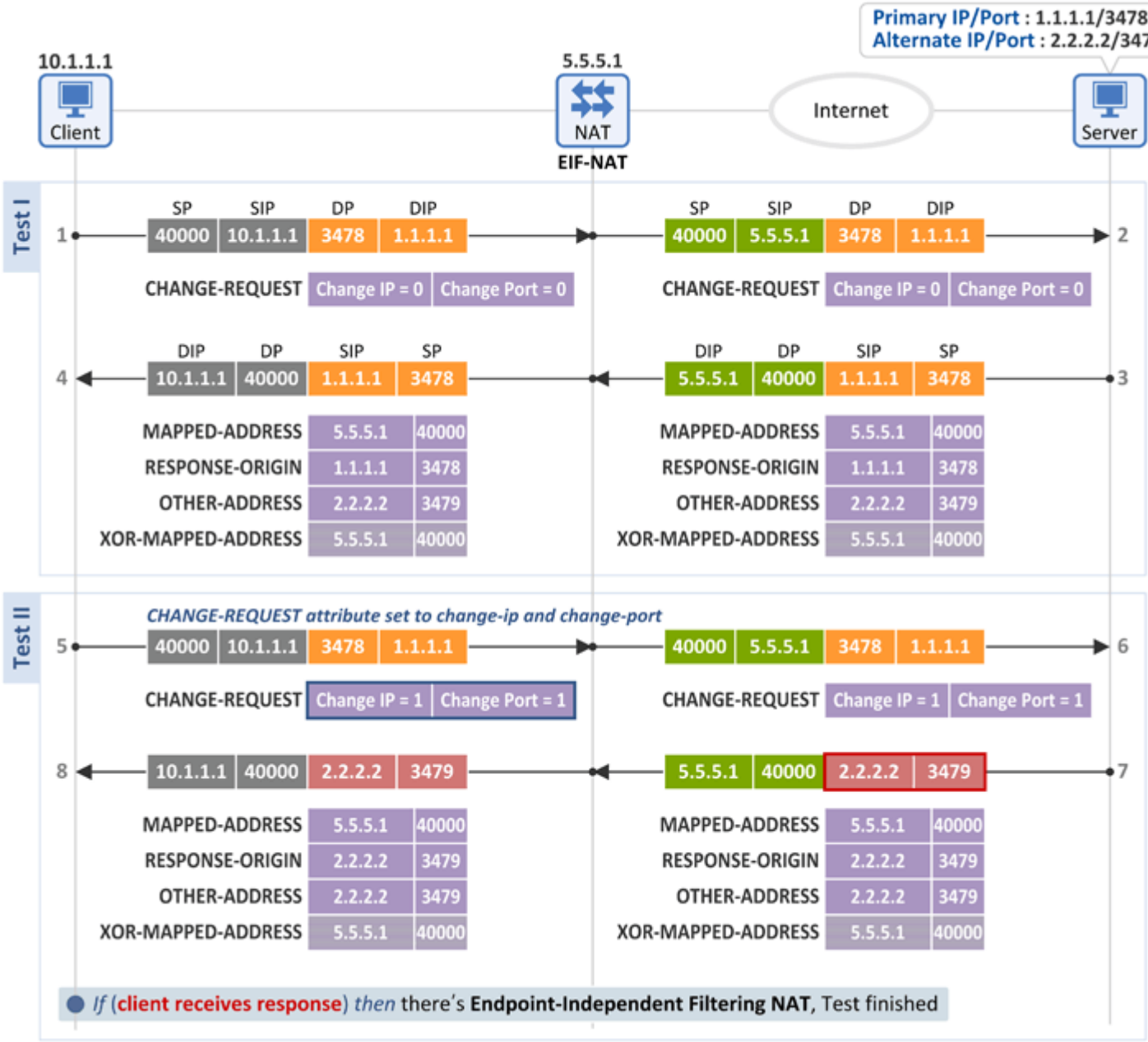
If no response is received, test III must be performed to distinguish between Address-Dependent Filtering and Address and Port-Dependent Filtering. In **test III**, the client sends a binding request to the original server address with CHANGE-REQUEST set to change-port. If the client receives a response, the current behavior isAddress-Dependent Filtering; if no response is received, the current behavior is Address and Port-Dependent Filtering.

■ Test (Discovery) Procedure



- Test II 를 통해 Endpoint-Independent Filtering NAT 식별
- Test III 를 통해 Address-Dependent Filtering NAT 혹은 Address and Port-Dependent Filtering NAT 식별

■ Endpoint-Independent Filtering NAT(EIF-NAT)인 경우



■ Test I

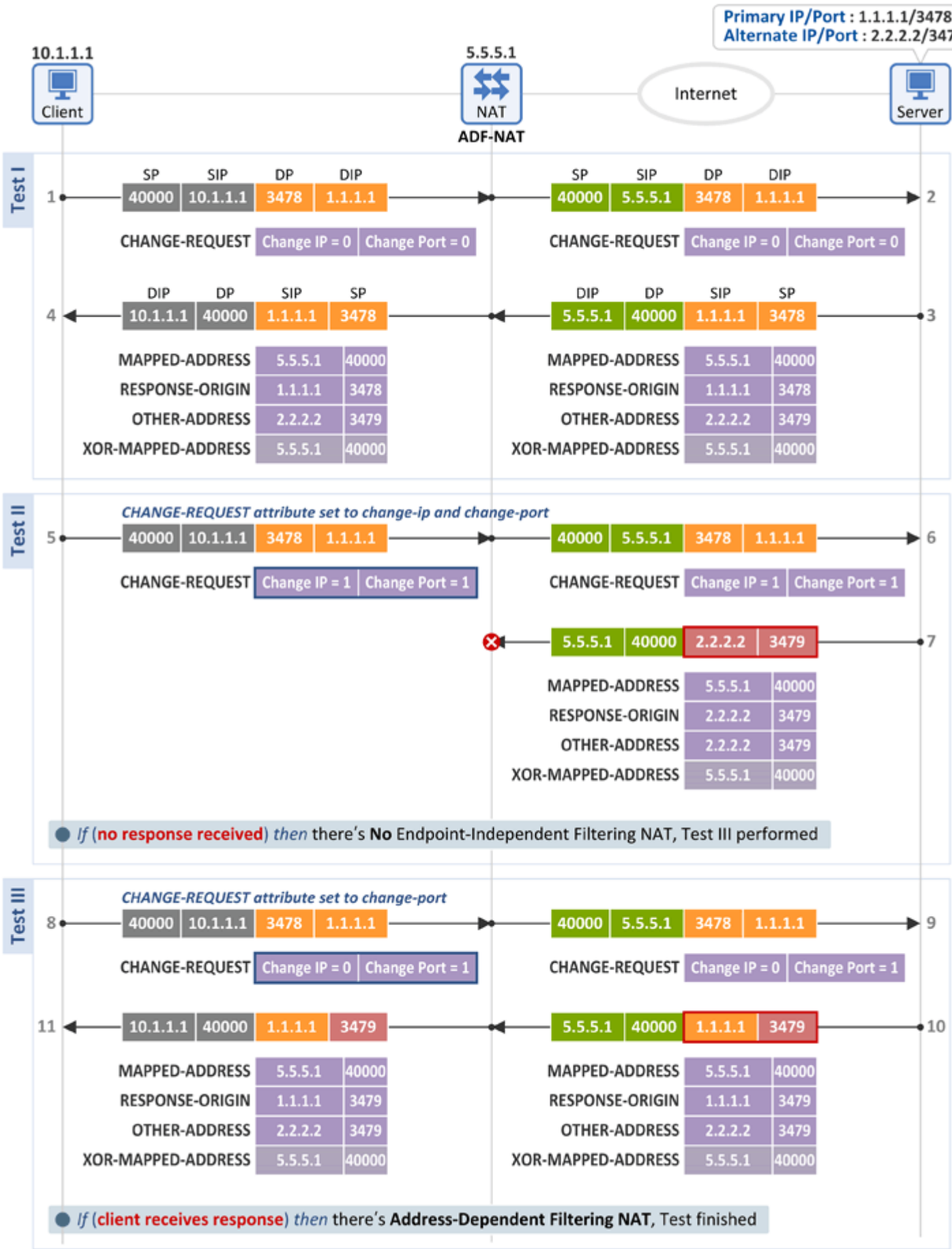
- 단말은 서버의 Primary IP:Primary Port(1.1.1.1:3478)로 Binding Request 메시지를 전송하고 이 때의 CHANGE-REQUEST attribute 의 Change IP 와 Change Port flag 는 모두 0 입니다. 그리고 당연히 응답으로 Binding Response 메시지를 수신합니다.

■ Test II

- 이번에는 단말이 CHANGE-REQUEST attribute 의 Change IP 와 Change Port 의 flag 를 모두 1 로 하여 Binding Request 메시지를 서버로 전송합니다.

- 이를 수신한 서버는 수신된 패킷의 Primary IP:Primary Port(1.1.1.1:3478)와 다른 주소/포트인 Alternate IP:Alternate Port(2.2.2.2:3479)를 소스 정보로 하여 Binding Response 메시지를 단말로 전달합니다.
- 만약 이 메시지가 수신되었다면 단말은 EIF-NAT(Endpoint-Independent Filtering NAT)가 존재한다고 판단합니다.
- 즉, Outbound 패킷의 목적지 정보(1.1.1.1:3478)와 다른 소스 정보(2.2.2.2:3479)를 가진 Inbound 패킷을 허용(Allow)하였으므로 EIF-NAT 입니다.

■ Address-Dependent Filtering NAT(ADF-NAT)인 경우


Primary IP/Port : 1.1.1.1/3478
Alternate IP/Port : 2.2.2.2/347
10.1.1.1
Client
5.5.5.1
NAT
ADF-NAT
Internet
Server
Test I
SP SIP DP DIP
1
40000 10.1.1.1 3478 1.1.1.1
SP SIP DP DIP
40000 5.5.5.1 3478 1.1.1.1
2
CHANGE-REQUEST Change IP = 0 Change Port = 0
CHANGE-REQUEST Change IP = 0 Change Port = 0
DIP DP SIP SP
4
10.1.1.1 40000 1.1.1.1 3478
DIP DP SIP SP
5.5.5.1 40000 1.1.1.1 3478
3
MAPPED-ADDRESS 5.5.5.1 40000
RESPONSE-ORIGIN 1.1.1.1 3478
OTHER-ADDRESS 2.2.2.2 3479
XOR-MAPPED-ADDRESS 5.5.5.1 40000
MAPPED-ADDRESS 5.5.5.1 40000
RESPONSE-ORIGIN 1.1.1.1 3478
OTHER-ADDRESS 2.2.2.2 3479
XOR-MAPPED-ADDRESS 5.5.5.1 40000
Test II
CHANGE-REQUEST attribute set to change-ip and change-port
5
40000 10.1.1.1 3478 1.1.1.1
40000 5.5.5.1 3478 1.1.1.1
6
CHANGE-REQUEST Change IP = 1 Change Port = 1
CHANGE-REQUEST Change IP = 1 Change Port = 1
5.5.5.1 40000 2.2.2.2 3479
7
MAPPED-ADDRESS 5.5.5.1 40000
RESPONSE-ORIGIN 2.2.2.2 3479
OTHER-ADDRESS 2.2.2.2 3479
XOR-MAPPED-ADDRESS 5.5.5.1 40000
If (no response received) then there's No Endpoint-Independent Filtering NAT, Test III performed
Test III
CHANGE-REQUEST attribute set to change-port
8
40000 10.1.1.1 3478 1.1.1.1
40000 5.5.5.1 3478 1.1.1.1
9
CHANGE-REQUEST Change IP = 0 Change Port = 1
CHANGE-REQUEST Change IP = 0 Change Port = 1
11
10.1.1.1 40000 1.1.1.1 3479
5.5.5.1 40000 1.1.1.1 3479
10
MAPPED-ADDRESS 5.5.5.1 40000
RESPONSE-ORIGIN 1.1.1.1 3479
OTHER-ADDRESS 2.2.2.2 3479
XOR-MAPPED-ADDRESS 5.5.5.1 40000
MAPPED-ADDRESS 5.5.5.1 40000
RESPONSE-ORIGIN 1.1.1.1 3479
OTHER-ADDRESS 2.2.2.2 3479
XOR-MAPPED-ADDRESS 5.5.5.1 40000
If (client receives response) then there's Address-Dependent Filtering NAT, Test finished

■ **Test I**

- EIF-NAT 시험과 동일

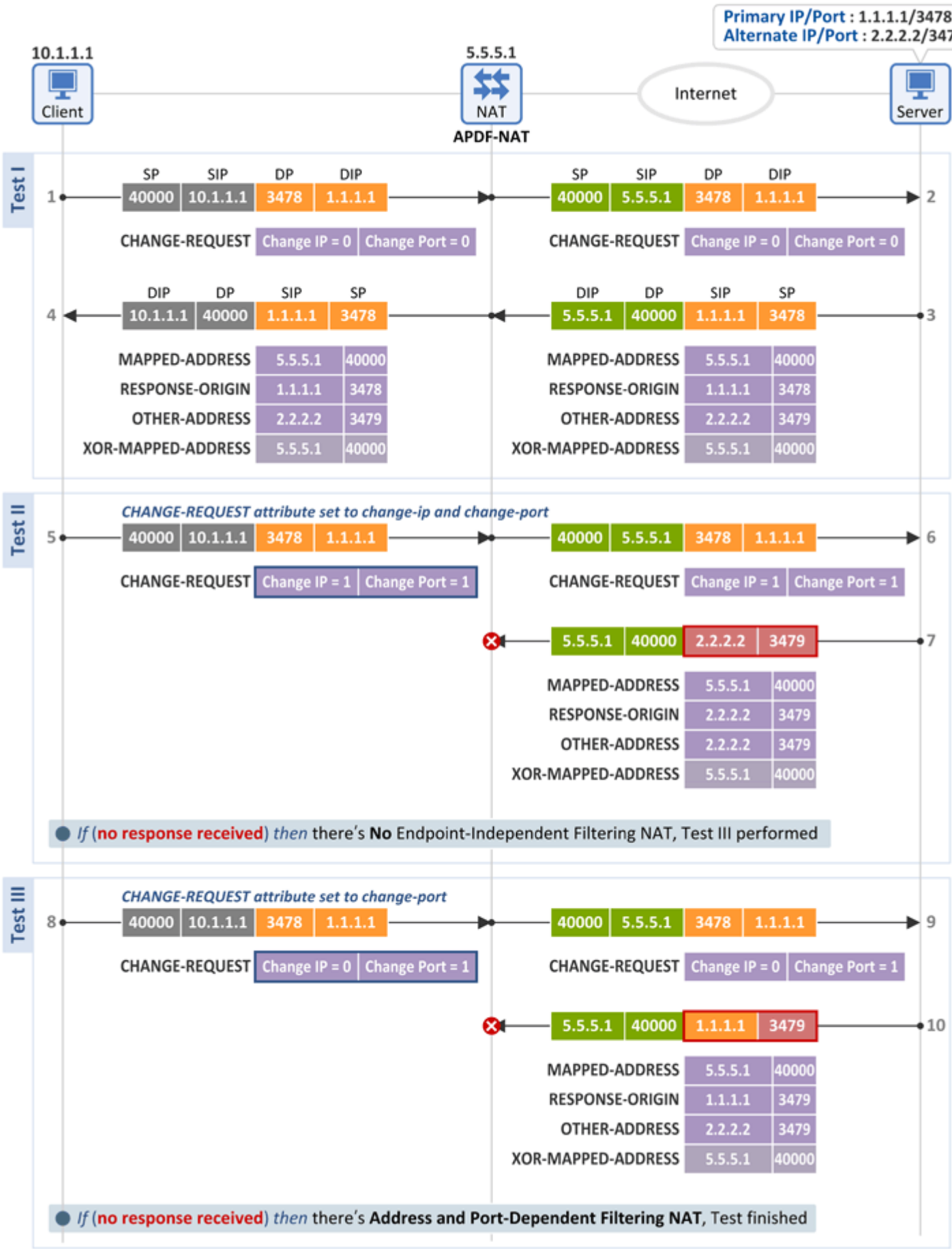
■ **Test II**

- EIF-NAT 시험과 동일한 Binding Request 메시지를 전송하고 그 응답을 수신하지 못하였습니다.
- 따라서 단말은 EIM-NAT 가 아니라고 판단을 하고 Test III 과정을 진행합니다.

■ **Test III**

- 이번에는 단말이 CHANGE-REQUEST attribute 의 Change Port flag 만 1 로 하여 Binding Request 메시지를 서버로 전송합니다.
- 이를 수신한 서버는 수신된 패킷의 Primary IP:Primary Port(1.1.1.1:3478)와 동일 주소/다른 포트인 Primary IP:Alternate Port(1.1.1.1:3479)를 소스 정보로 하여 Binding Response 메시지를 단말로 전달합니다.
- 만약 이 메시지가 수신되었다면 단말은 ADF-NAT(Address-Dependent Filtering NAT)가 존재한다고 판단합니다.
- 즉, Outbound 패킷과 "동일 Destination IP & 다른 Port"를 소스 정보(1.1.1.1:3479)로 한 Inbound 패킷을 허용(Allow)하였으므로 ADF-NAT 입니다.

■ Address and Port-Dependent Filtering NAT(APDF-NAT)인 경우


Primary IP/Port : 1.1.1.1/3478
Alternate IP/Port : 2.2.2.2/347
10.1.1.1
Client
5.5.5.1
NAT
APDF-NAT
Internet
Server
Test I
SP SIP DP DIP
1
40000 10.1.1.1 3478 1.1.1.1
CHANGE-REQUEST Change IP = 0 Change Port = 0
SP SIP DP DIP
40000 5.5.5.1 3478 1.1.1.1
2
CHANGE-REQUEST Change IP = 0 Change Port = 0
DIP DP SIP SP
4
10.1.1.1 40000 1.1.1.1 3478
MAPPED-ADDRESS 5.5.5.1 40000
RESPONSE-ORIGIN 1.1.1.1 3478
OTHER-ADDRESS 2.2.2.2 3479
XOR-MAPPED-ADDRESS 5.5.5.1 40000
DIP DP SIP SP
5.5.5.1 40000 1.1.1.1 3478
3
MAPPED-ADDRESS 5.5.5.1 40000
RESPONSE-ORIGIN 1.1.1.1 3478
OTHER-ADDRESS 2.2.2.2 3479
XOR-MAPPED-ADDRESS 5.5.5.1 40000
Test II
CHANGE-REQUEST attribute set to change-ip and change-port
5
40000 10.1.1.1 3478 1.1.1.1
CHANGE-REQUEST Change IP = 1 Change Port = 1
40000 5.5.5.1 3478 1.1.1.1
6
CHANGE-REQUEST Change IP = 1 Change Port = 1
5.5.5.1 40000 2.2.2.2 3479
7
MAPPED-ADDRESS 5.5.5.1 40000
RESPONSE-ORIGIN 2.2.2.2 3479
OTHER-ADDRESS 2.2.2.2 3479
XOR-MAPPED-ADDRESS 5.5.5.1 40000
If (no response received) then there's No Endpoint-Independent Filtering NAT, Test III performed
Test III
CHANGE-REQUEST attribute set to change-port
8
40000 10.1.1.1 3478 1.1.1.1
CHANGE-REQUEST Change IP = 0 Change Port = 1
40000 5.5.5.1 3478 1.1.1.1
9
CHANGE-REQUEST Change IP = 0 Change Port = 1
5.5.5.1 40000 1.1.1.1 3479
10
MAPPED-ADDRESS 5.5.5.1 40000
RESPONSE-ORIGIN 1.1.1.1 3479
OTHER-ADDRESS 2.2.2.2 3479
XOR-MAPPED-ADDRESS 5.5.5.1 40000
If (no response received) then there's Address and Port-Dependent Filtering NAT, Test finished

■ **Test I**

- ADF-NAT 시험과 동일

■ **Test II**

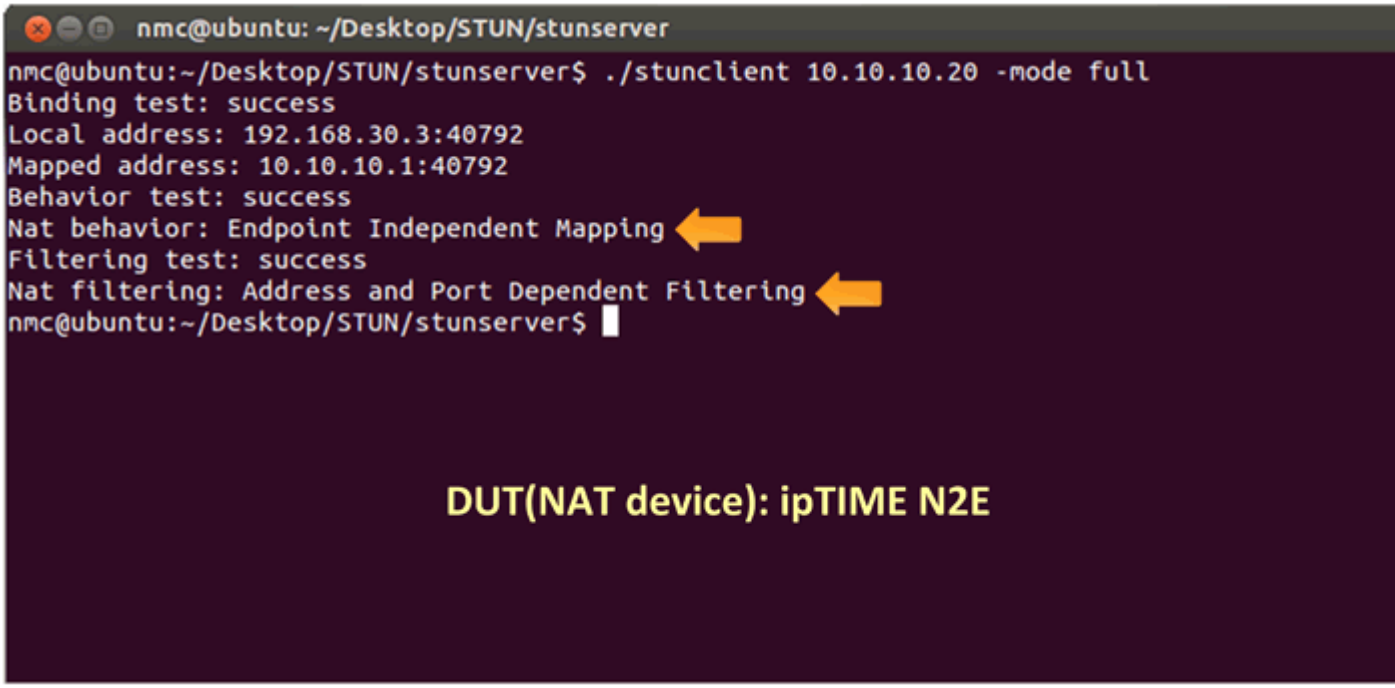
- ADF-NAT 시험과 동일

■ **Test III**

- ADF-NAT 시험과 동일한 Binding Request 메시지를 전송하고 그 응답을 수신하지 못한 경우 단말은 APDF-NAT 가 존재한다고 판단합니다.
- 즉, 아래 두 종류의 Inbound 패킷을 모두 폐기(Deny)하였으므로 APDF-NAT 입니다.
    - Outbound 패킷과 "다른 Destination IP & 다른 Port"를 소스 정보(2.2.2.2:3479)를 가진 Inbound 패킷
    - Outbound 패킷과 "동일 Destination IP & 다른 Port"를 소스 정보(1.1.1.1:3479)를 가진 Inbound 패킷

RFC 5780 NAT Behavior Discovery Tool 소개

☐ **Tool Name:** STUNTMAN (STUN Server & Client)
☐ **URL:** http://www.stunprotocol.org/
☐ **Test:** ipTIME N2E 를 대상으로 STUNTMAN 을 이용하여 NAT Mapping & Filtering Behavior 를 시험
☐ **Test Result:** Endpoint-Independent Mapping & Address and Port-Dependent Filtering



요약

Mapping & Filtering Behavior 검사 방법을 요약하면,

- NAT Mapping Behavior 는 단말이 송신하는 Binding Request 메시지의 Primary/Alternate IP/Port 값을 변경하고, 그 응답으로 수신되는 Binding Response 메시지의 XOR-MAPPED-ADDRESS 값을 검사하여 Mapping Behavior 를 판단하고,
- NAT Filtering Behavior 는 단말이 송신하는 Binding Request 메시지의 CHANGE-REQUEST flag 를 변경하고, 그 응답의 도달 여부를 통해 Filtering Behavior 를 판단합니다.