



개발자가 알아야 할 NAT, DNS

인프라 엔지니어 고재민



목차

01 DNS

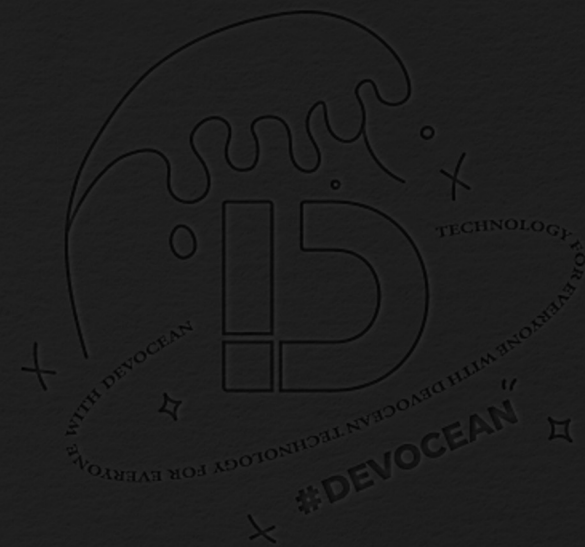
02 DNS 동작방식

03 DNS 도메인 위임

04 NAT

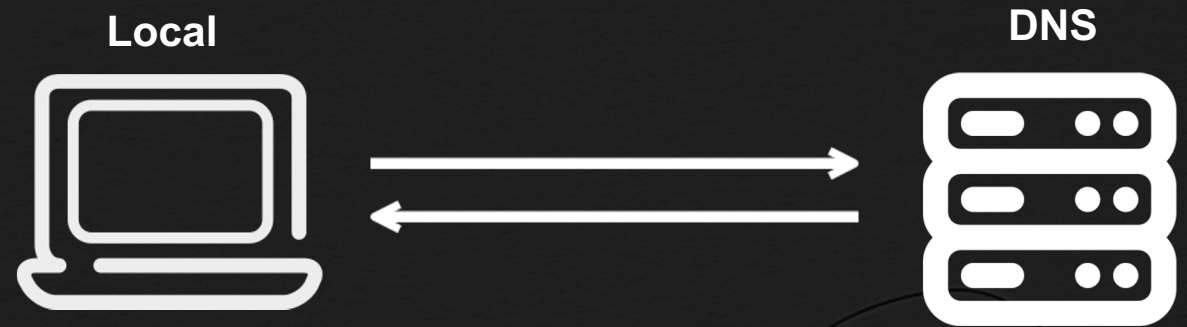
05 NAT 동작방식

06 NAT와 방화벽



01 DNS - DNS(Domain Name Service)란?

- 사람이 읽을 수 있는 도메인 이름을 컴퓨터가 읽을 수 있는 IP주소로 변환하는 것
- 클라우드 기반의 인프라 구성이 많아지며 인프라가 빈번히 변경되어 DNS를 이용한 시스템 설계가 중요해지고 있음
- MSA기반의 서비스에서 다수의 API를 이용할 때 서비스간 API호출이나 인터페이스가 많아져 DNS의 역할이 더욱 중요해짐



01 DNS - DNS 구조

- 루트도메인 – DNS 계층 구조의 최상위 영역으로 전세계에 13개의 루트 네임서버가 존재하며 TLD 도메인으로 DNS요청을 전달
- TOP-LEVEL DOMAIN – 도메인의 용도에 따라 도메인을 분류하는 TLD는 IANA에서 분류한 6가지 유형으로 구분할 수 있음
 - *IANA: 인터넷 할당 관리기관
- gTLD(com, edu, gov, net, ...)
- ccTLD(kr, us, tv, ai, uk, ...)
- sTLD(aero, asia, edu, museum)

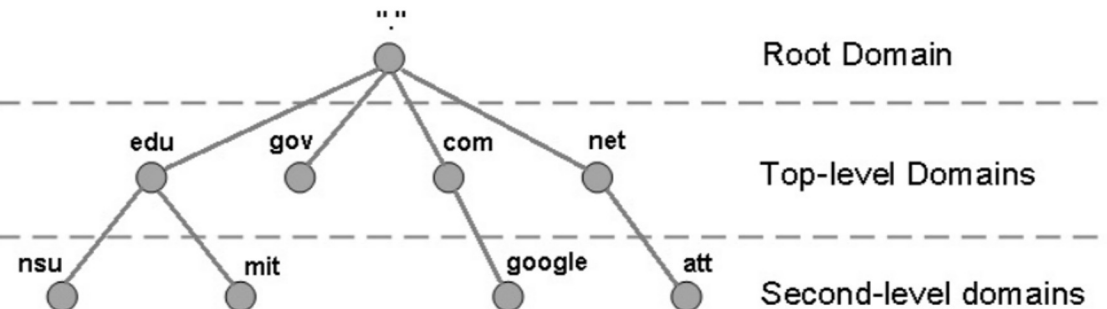
blog.example.com.

sub

Second-level

Top-level

Root



01 DNS - DNS 확인방법

- 일반 pc에서 DNS정보 확인 방법
(ipconfig /displaydns)
- ipconfig /flushdns
로컬 DNS캐시를 비워서 도메인 조회 시 새로운 DNS정보를 가져옴

```
C:\Users\wo005>ipconfig /displaydns

Windows IP 구성

static-ecst.lidn.com
-----
데이터 이름 . . . . . : static-ecst.lidn.com
데이터 유형 . . . . . : 5
TTL(Time To Live) . . : 1744
데이터 길이 . . . . . : 8
섹션 . . . . . : 응답
CNAME 레코드 . . . . . : cs1404.wpc.epsiloncdn.net

데이터 이름 . . . . . : cs1404.wpc.epsiloncdn.net
데이터 유형 . . . . . : 1
TTL(Time To Live) . . : 1744
데이터 길이 . . . . . : 4
섹션 . . . . . : 응답
(호스트) 레코드 . . . . : 152.199.43.62

www.microsoft.com
-----
데이터 이름 . . . . . : www.microsoft.com
데이터 유형 . . . . . : 5
TTL(Time To Live) . . : 5
데이터 길이 . . . . . : 8
섹션 . . . . . : 응답
CNAME 레코드 . . . . . : www.microsoft.com-c-3.edgekey.net

데이터 이름 . . . . . : www.microsoft.com-c-3.edgekey.net
데이터 유형 . . . . . : 5
TTL(Time To Live) . . : 5
데이터 길이 . . . . . : 8
섹션 . . . . . : 응답
CNAME 레코드 . . . . . : www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net

데이터 이름 . . . . . : www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net
데이터 유형 . . . . . : 5
TTL(Time To Live) . . : 5
데이터 길이 . . . . . : 8
섹션 . . . . . : 응답
CNAME 레코드 . . . . . : e13678.dscb.akamaiedge.net

데이터 이름 . . . . . : e13678.dscb.akamaiedge.net
데이터 유형 . . . . . : 1
TTL(Time To Live) . . : 5
데이터 길이 . . . . . : 4
섹션 . . . . . : 응답
(호스트) 레코드 . . . . : 104.94.217.134
```



01 DNS - DNS 확인방법

- Windows server 루트도메인 확인방법

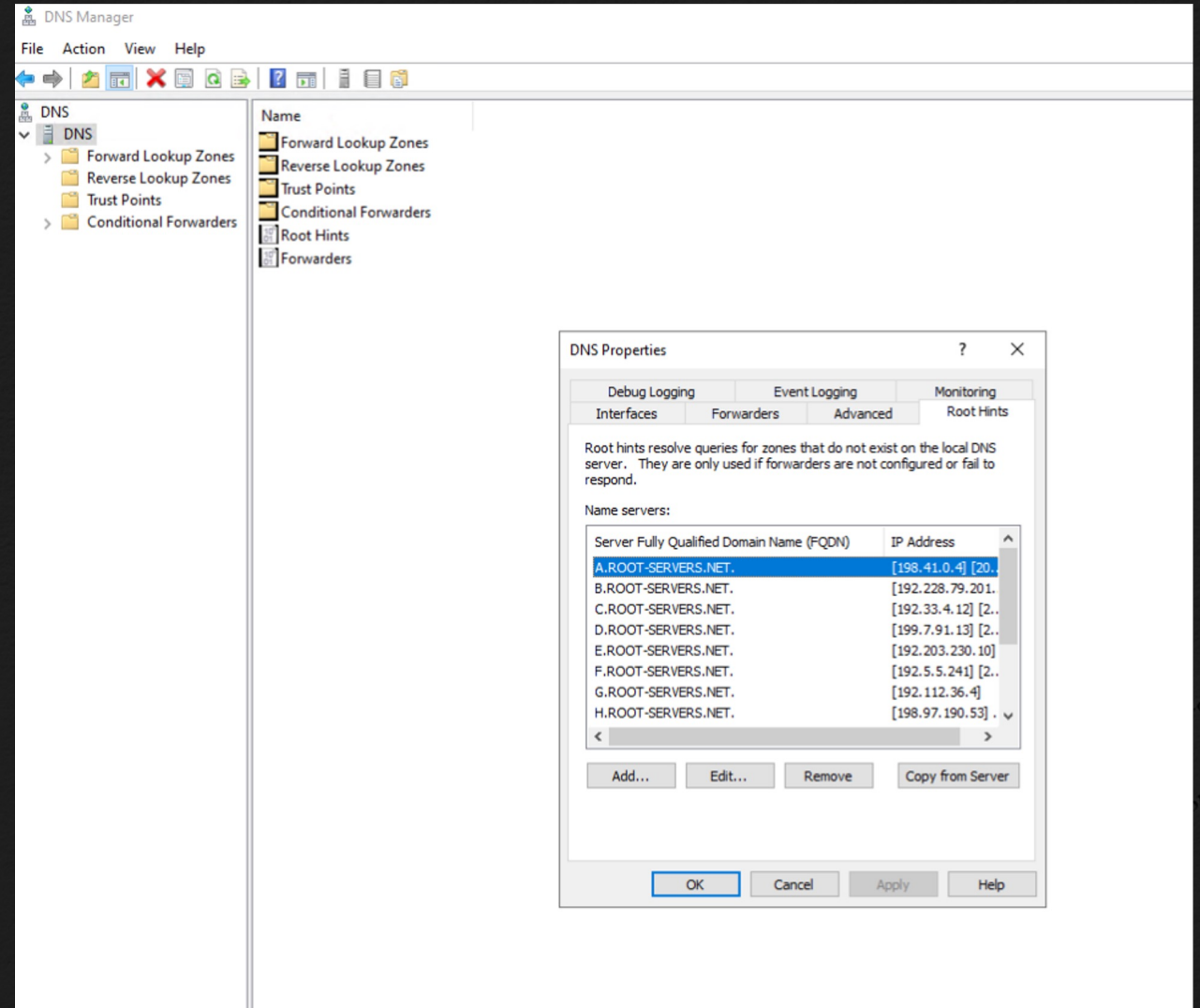
- DNS 서비스 속성 – Root Hints

DNS서버가 도메인 이름을 확인할 때 참조하는 루트 NS의 목록

인터넷의 DNS 구조 최상위에 위치하여 DNS 쿼리의 시작점이 됨

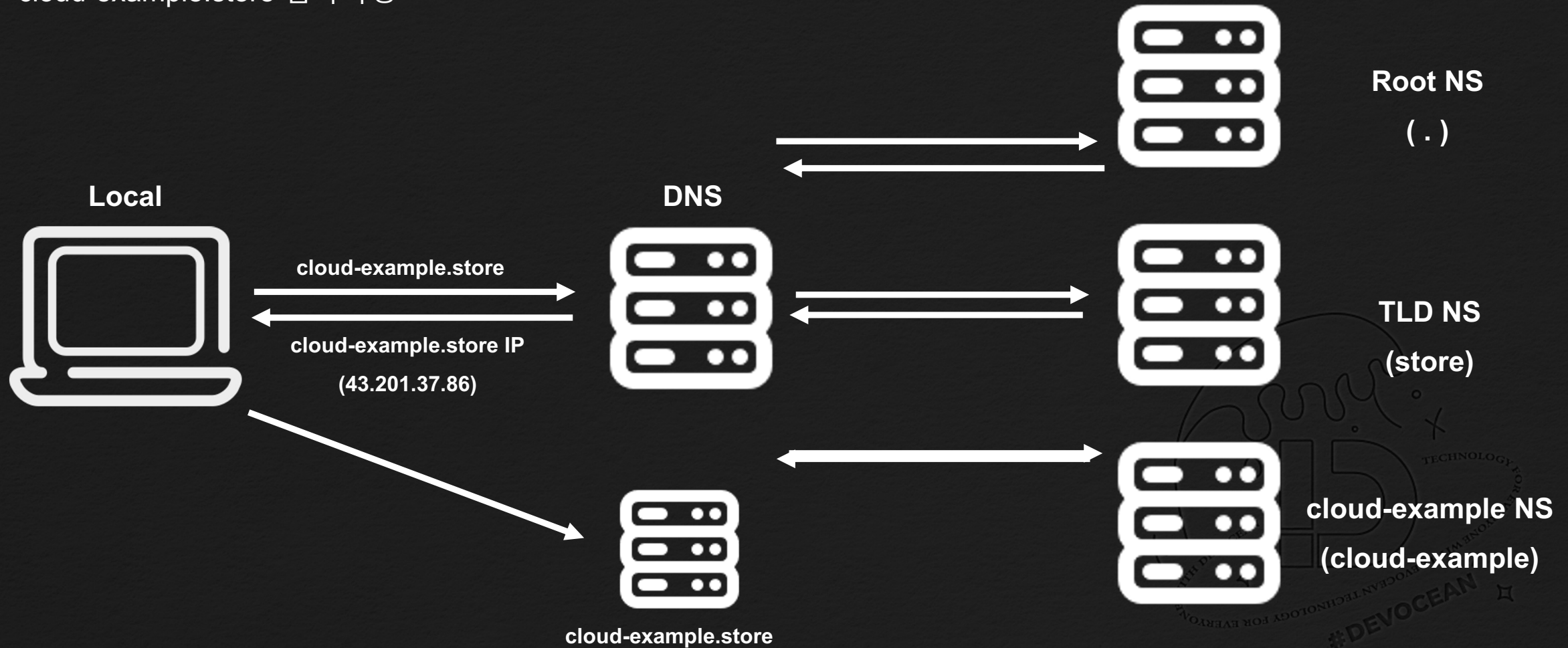
- 루트 힌트파일은 IANA에서 관리

* 인터넷 할당 관리기관



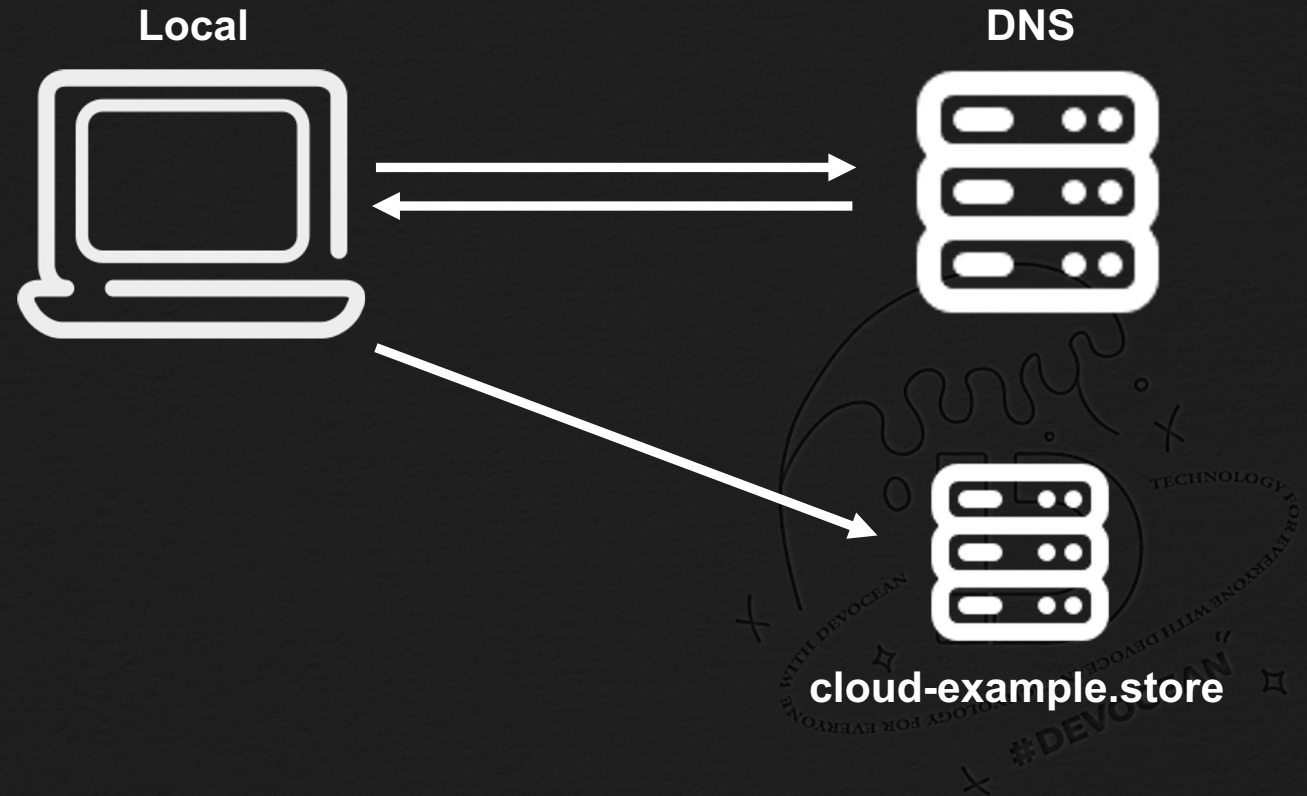
02 DNS 동작방식

- cloud-example.store 접속과정



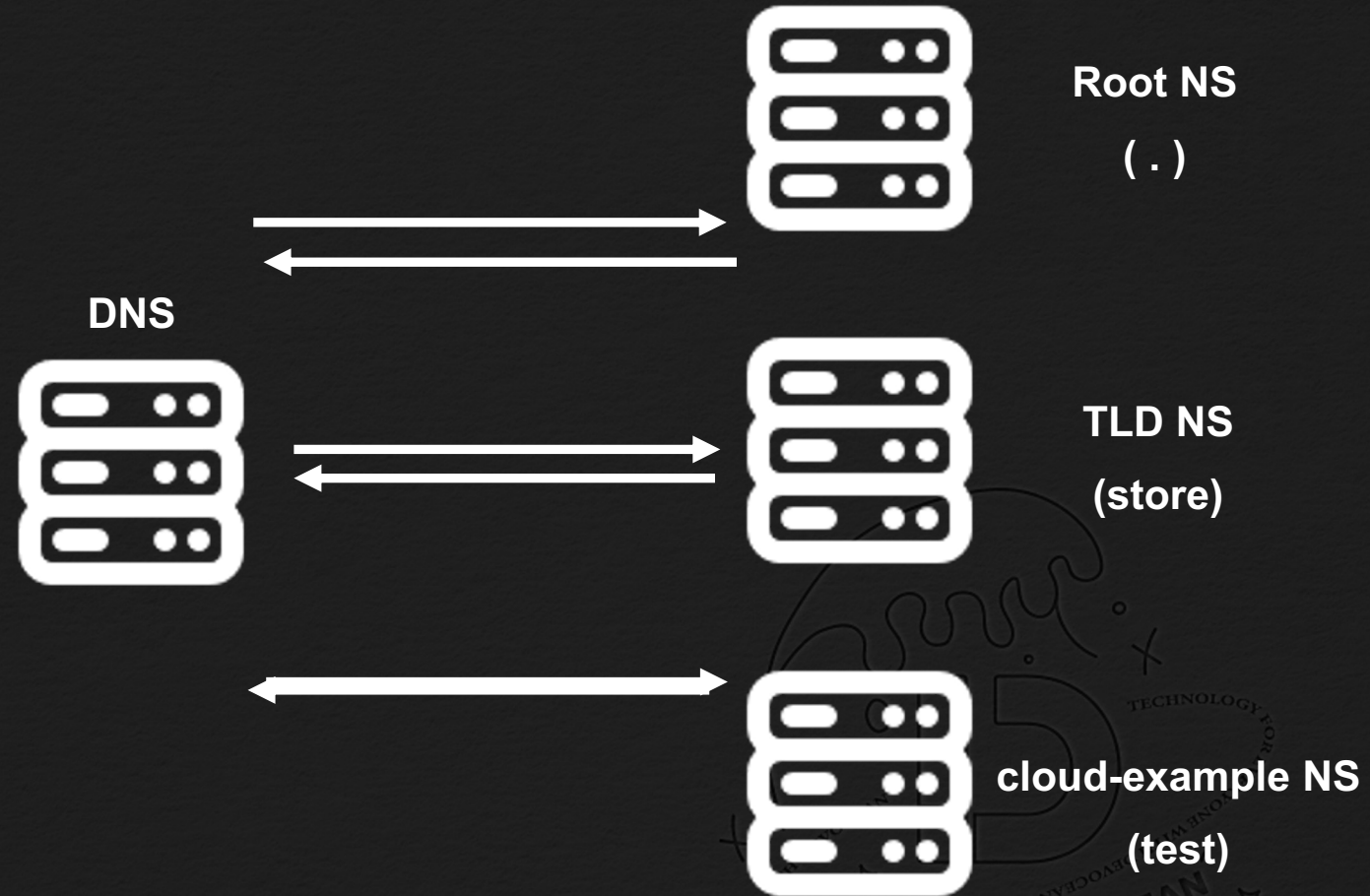
02 DNS 동작방식 - DNS 동작방식(Local + DNS)

- cloud-example.store 도메인 주소의 IP주소가 로컬 캐시에 저장되어 있는지 확인
- 로컬 캐시에 저장되어 있지 않으면 사용자 호스트에 설정된 DNS에 cloud-example.store에 대해 쿼리
- DNS서버는 cloud-example.store이 로컬 캐시와 자체에 설정되어 있는지 확인하고 없다면 루트 NS에 .store에 대한 TLD정보를 가진 도메인 주소를 쿼리함



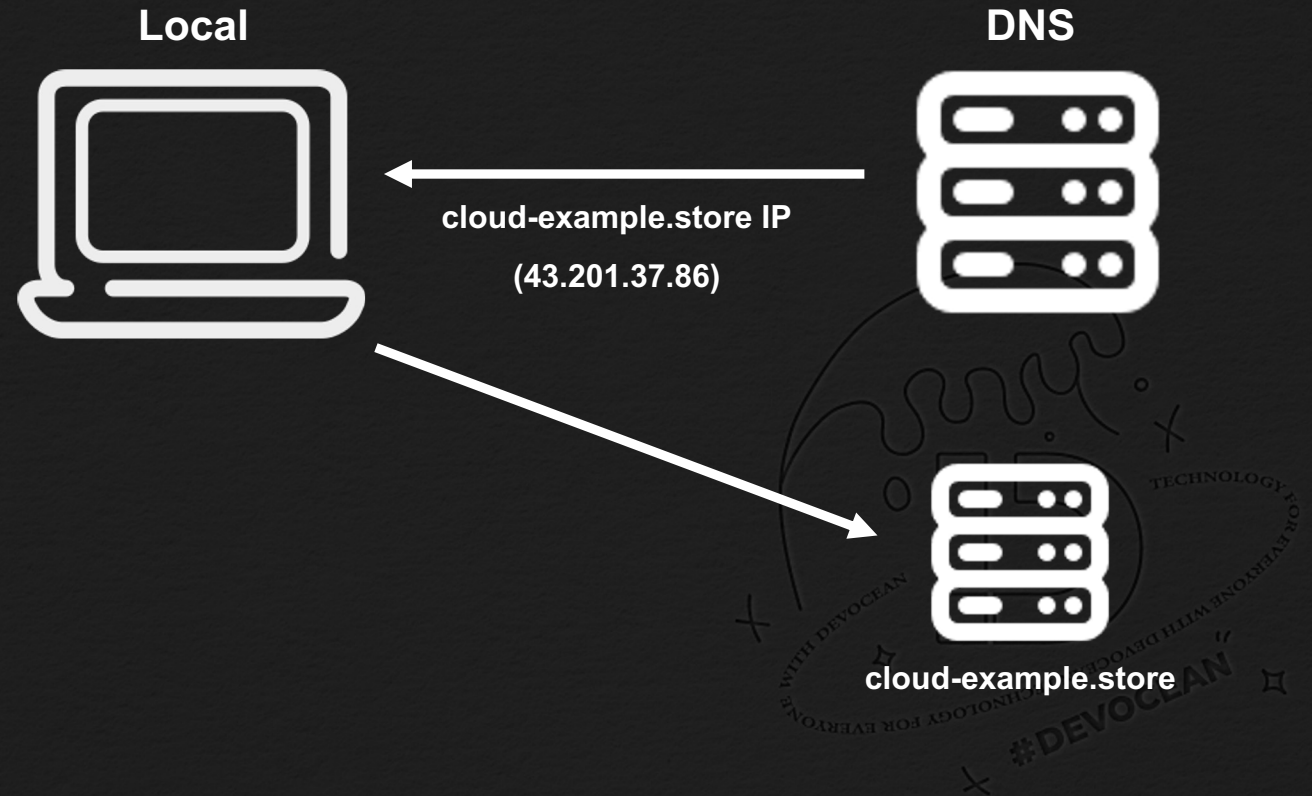
02 DNS 동작방식 - DNS 동작방식(DNS + NS)

- 루트 DNS는 cloud-example.store의 TLD인 .store을 관리하는 TLD네임 서버 정보를 DNS 서버에 응답
- DNS는 TLD네임 서버에 cloud-example.store에 대한 정보를 다시 쿼리
- TLD 네임 서버는 cloud-example.store에 대한 정보를 가진 cloud-example NS에 대한 정보를 DNS서버로 응답



02 DNS 동작방식 - DNS 동작방식(DNS + Local)

- DNS는 cloud-example.store에 대한 정보를 로컬 캐시에 저장
- 처음 쿼리를 받은 DNS서버는 루트, TLD, cloud-example 네임서버가 반복적으로 쿼리한 결과(cloud-example.store)를 호스트에 응답



02 DNS 동작방식 - TTL

TTL과 DNS

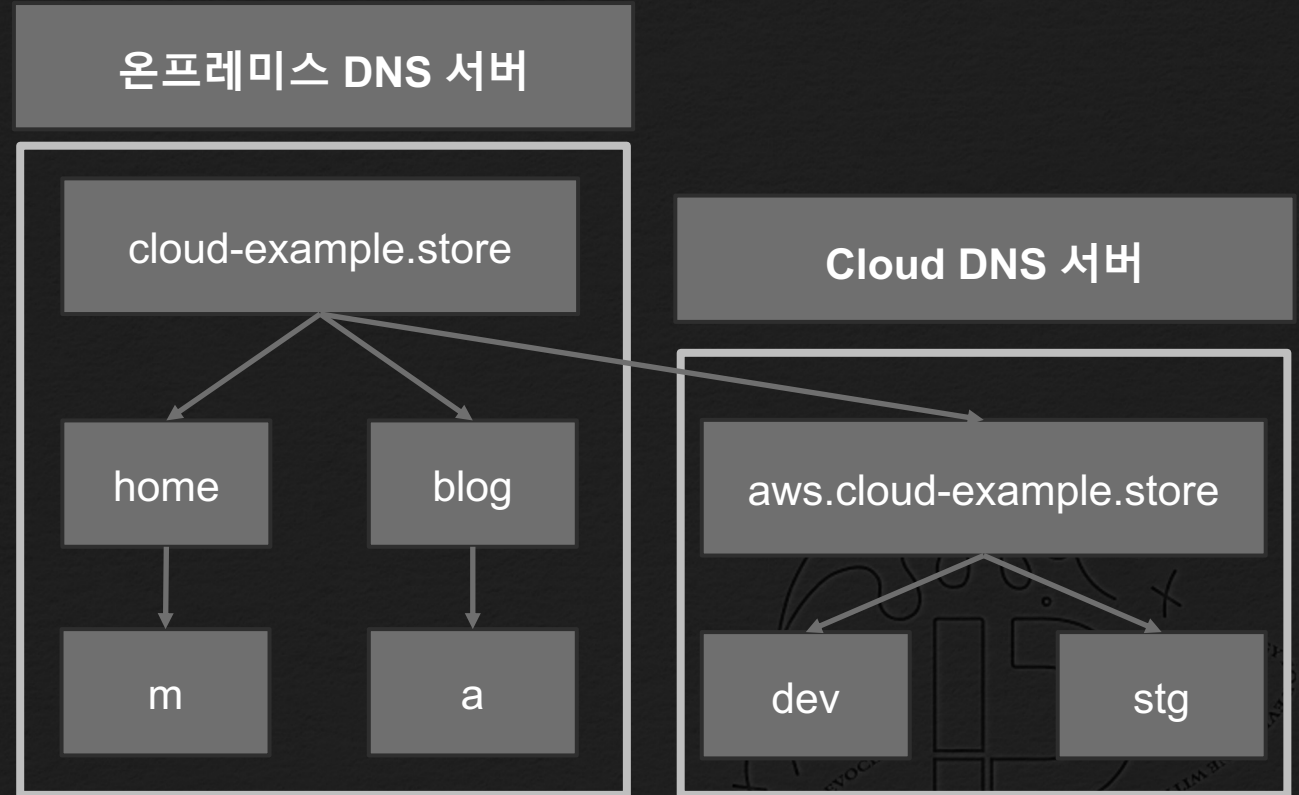
- TTL이 짧을수록 도메인이 바뀌었을 때 이를 PC가 알아차리는 속도가 빠르다.
- 하지만, 쿼리를 자주 해야 하기 때문에 DNS서버에 부하가 증가한다.
- TTL이 길면 쿼리를 자주 안해도 되는 장점이 있지만 도메인 정보가 바뀌었을 때 이를 알아차리지 못한다.

- 업데이트시에는 TTL설정을 짧게 하고(업데이트 된 도메인이 빠르게 전파되도록)
- 자주 바뀌지 않는 도메인이라면 TTL을 길게 변경할 수 있다.



03 DNS 도메인위임

- 상위도메인에서 하위 도메인의 네임서버(NS)를 지정하여 관리 권한을 넘겨주는 것을 의미한다.
- 상위도메인의 일부 권한을 하위도메인에 위임하여 세부 레코드를 관리하도록 구성할 수 있다.
- Ex) cloud-example.store 도메인은 NCP에서 관리 / aws.cloud-example.store는 AWS에서 관리



03 DNS 도메인위임 – NCP 도메인관리

- 실습(NCP – cloud-example.store 도메인 관리)

Global DNS 1

+ 도메인 추가 상품 더 알아보기 X 다운로드 전체 다운로드 새로 고침 업로드 기존 V1 도메인 가져오기

도메인 cloud-example.store

레코드 추가 레코드 수정 레코드 삭제 등록기관 설정 정보 설정 적용 (0)

도메인	TTL	Master NS	Refresh	Retry
cloud-example.store	300	ns1-1.ns-ncloud.com, ns1-2.ns-ncloud.com	21600	1800

☐ 호스트	도메인	레코드 타입	레코드 값	TTL
☐ @	cloud-example.store	SOA	ns1-1.ns-ncloud.com, ns1-2.ns-ncloud.com, 10 21600 1800 1209600 300	300
☐ @	cloud-example.store	NS	ns1-1.ns-ncloud.com, ns1-2.ns-ncloud.com	600
☒ aws	cloud-example.store	NS	ns-1199.awsdns-21.org, ns-439.awsdns-54.com	300
☐ *	cloud-example.store	CNAME	cloud-example.store.s3-website.ap-northeast-2.amazonaws.com	300

주의 요함 cloud-example.store

[Home](#) | [Test](#)

홈 페이지



03 DNS 도메인위임 – AWS 하위 도메인 관리

- 실습(AWS – aws.cloud-example.store 하위 도메인 관리)

Route 53 > 호스팅 영역 > aws.cloud-example.store

aws.cloud-example.store 정보

▶ 호스팅 영역 세부 정보

레코드(3) | DNSSEC 서명 | 호스팅 영역 태그(0)

레코드 (3) 정보

Automatic 모드는 최상의 필터 결과에 최적화된 현재 검색 동작입니다. 모드를 변경하려면 설정(settings)으로 이동합니다.

Q 속성 또는 값을 기준으로 레코드 필터링

레코드 이름	유형	라우팅 ...	차별...	별칭	값/트래픽 라우팅 대상
☐ aws.cloud-example.store	NS	단순	-	아니오	ns-1199.awsdns-21.org. ns-439.awsdns-54.com. ns-1789.awsdns-31.co.uk. ns-706.awsdns-24.net.
☐ aws.cloud-example.store	SOA	단순	-	아니오	ns-1199.awsdns-21.org. aws...
☐ test.aws.cloud-example.store	A	단순	-	아니오	43.201.37.86

AWS SubDomain x +

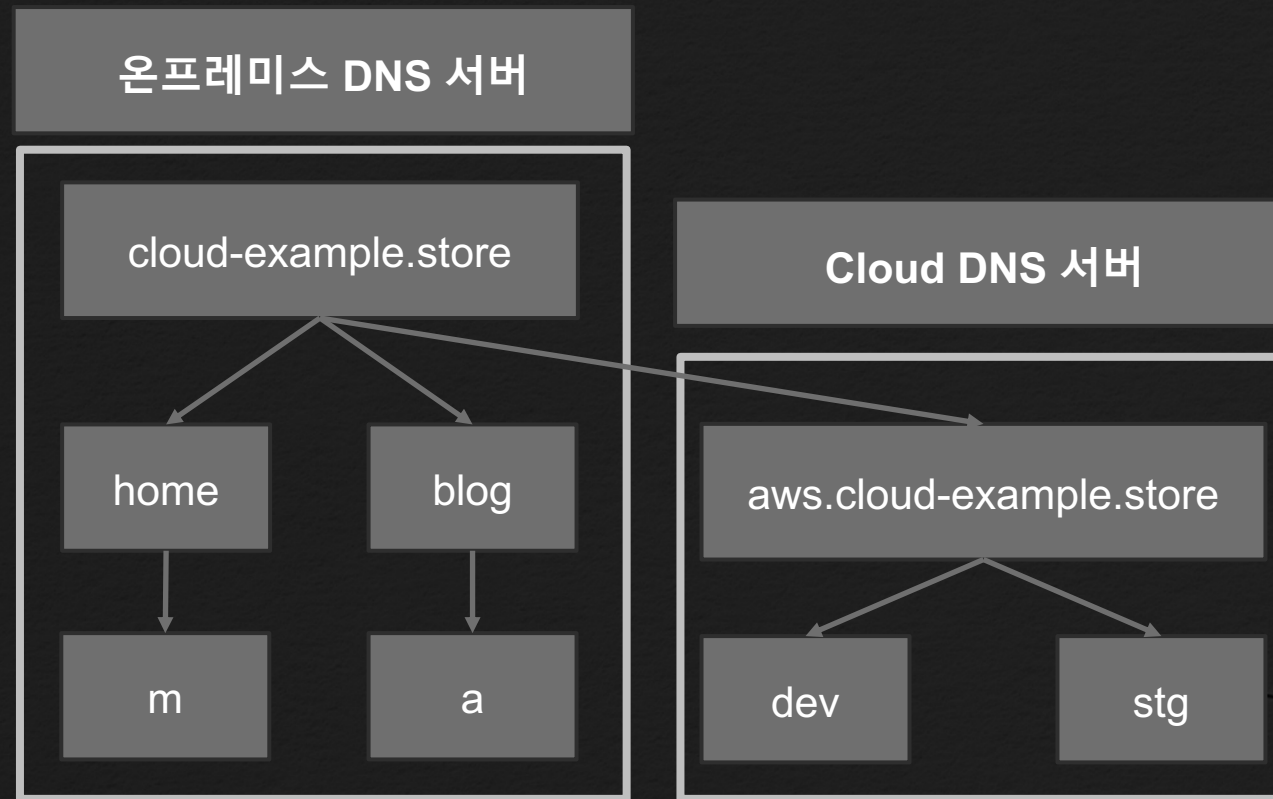
← → ↺ 주의 요함 test.aws.cloud-example.store ☆

DNS위임: aws.cloud-exam.store 도메인입니다.



03 DNS 도메인위임

- 온프레미스 도메인에 대한 정보는 기존 DNS를 사용하고 하위도메인의 경우 다른 DNS서버로 위임을 할 수 있다



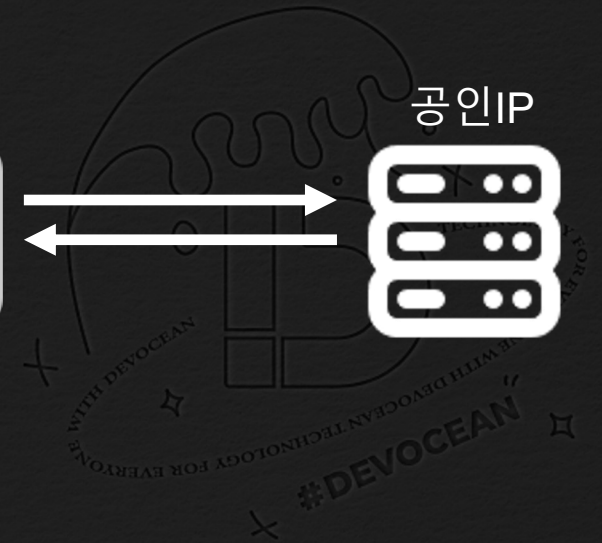
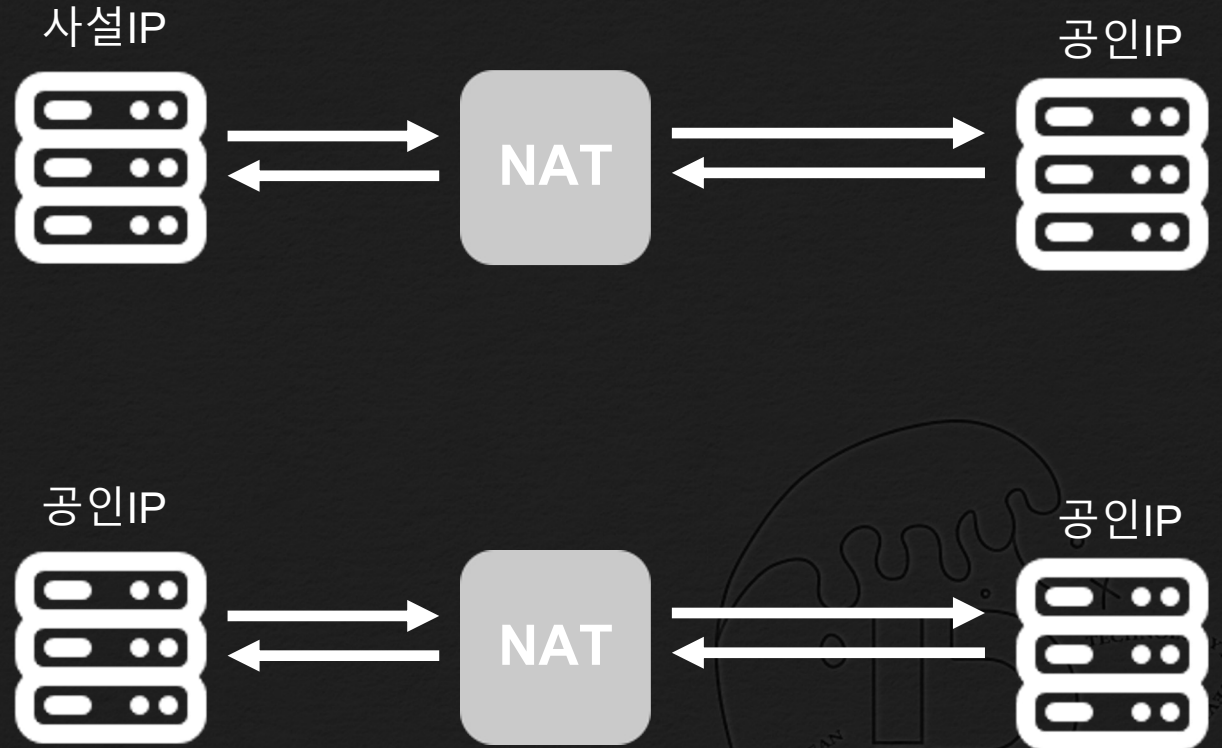


NAT

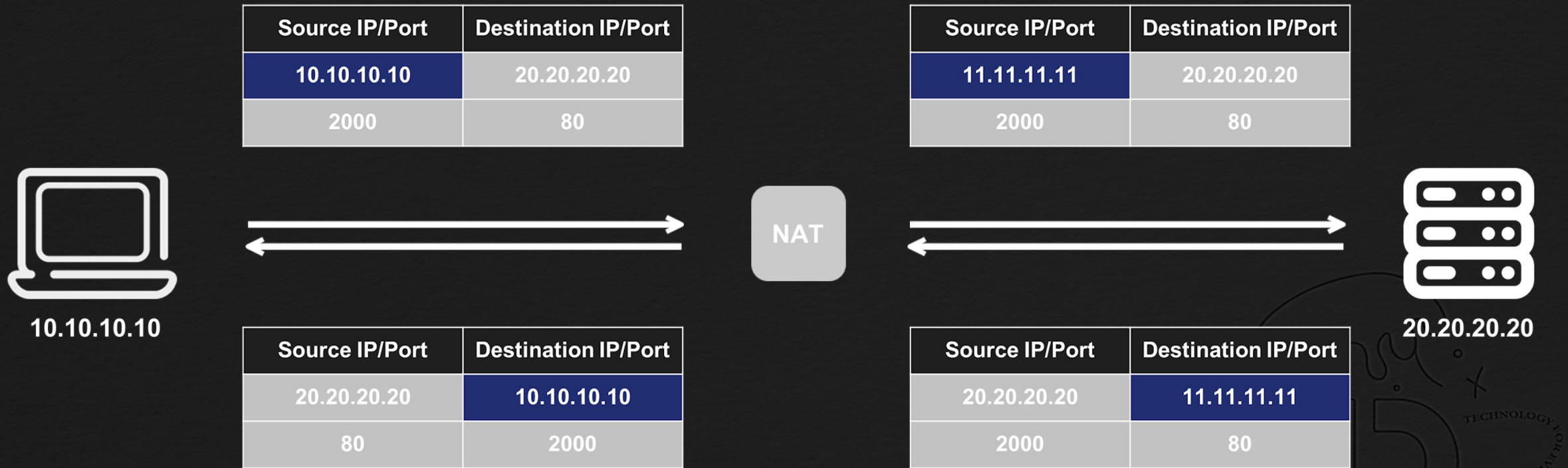


04 NAT - NAT(Network Address Translation)란?

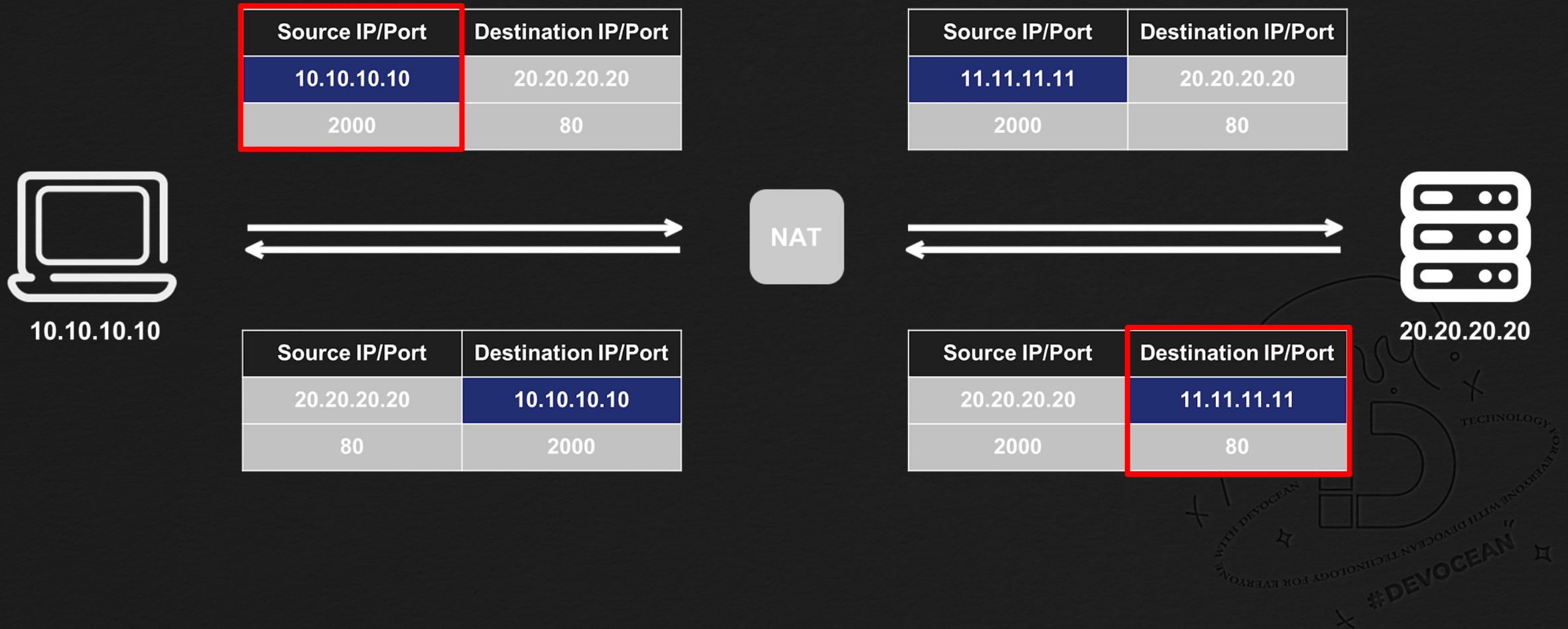
- NAT는 IP주소를 다른 IP주소로 변환해 라우팅을 원활히 해주는 기술
(ex. 사설 IP에서 공인 IP로의 변환, 공인 IP에서 또 다른 공인 IP로 전환, IPv4주소를 IPv6로 변환 등...)
- NAT는 기본적으로 하나의 네트워크 주소를 다른 네트워크 주소로 변환하는 1:1 변환이 기본이지만 다수의 IP를 변환하기도 함
- 여러개의 IP를 하나의 IP로 변환하는 것도 NAT지만 공식용어는 NAPT(Network Address Port Translation)로 실무에서는 PAT로 불림



05 NAT 동작방식 - NAT동작방식

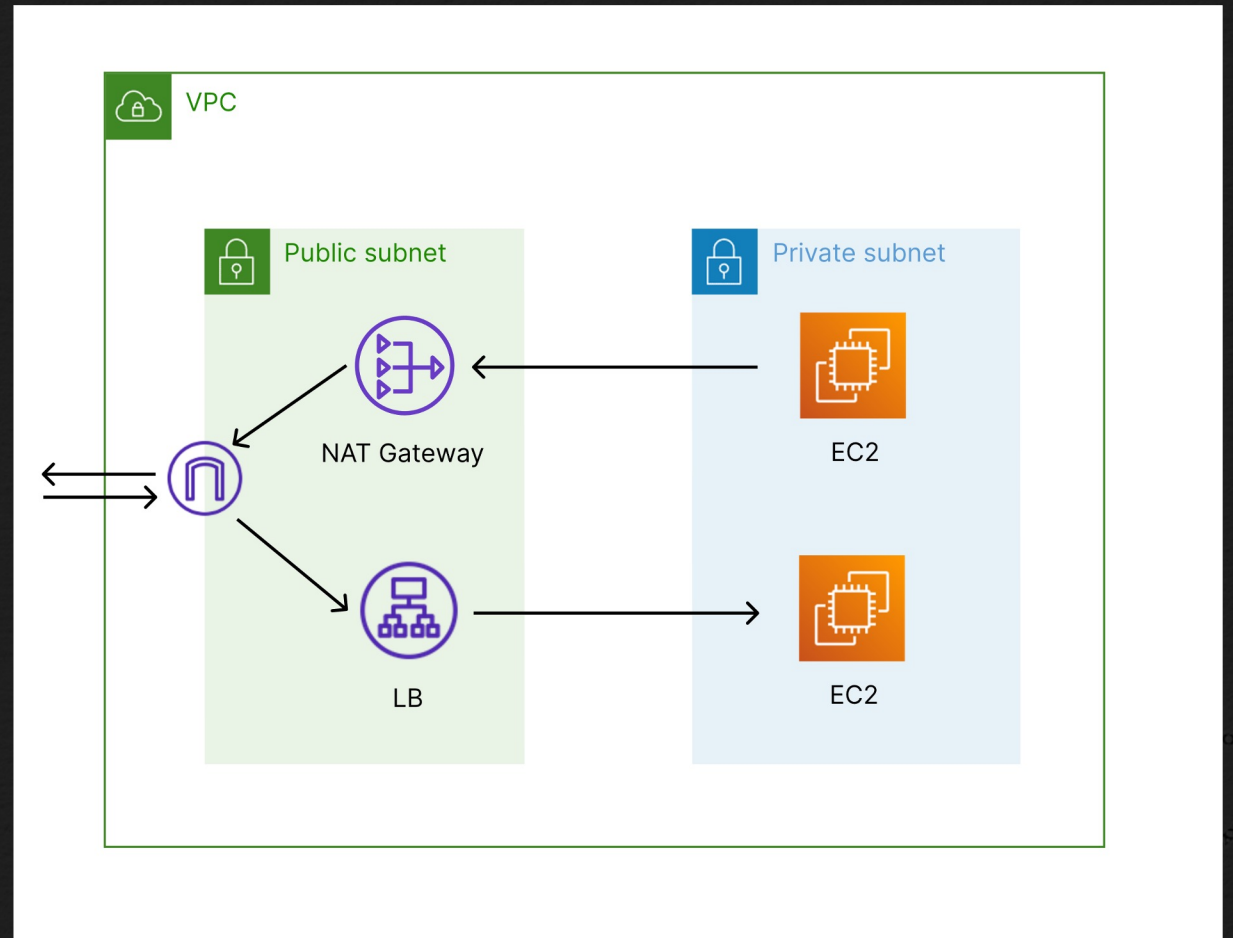


05 NAT 동작방식 - SNAT, DNAT



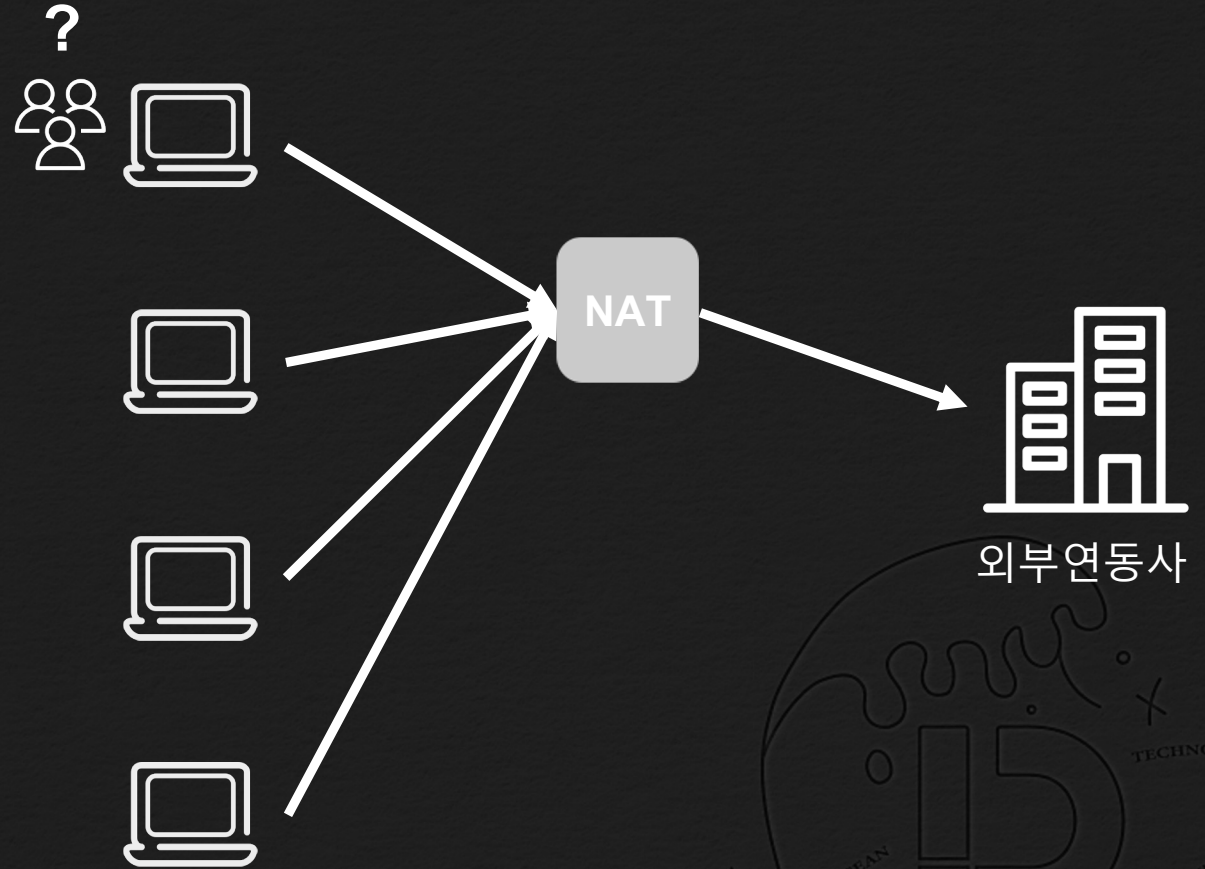
05 NAT 동작방식 – AWS에서의 NAT

- Source NAT: 출발지 IP를 변환하는 NAT 프라이빗 서브넷 EC2 -> NAT GW
- Destination NAT: 목적지 IP를 변환하는 NAT 로드밸런서 -> EC2



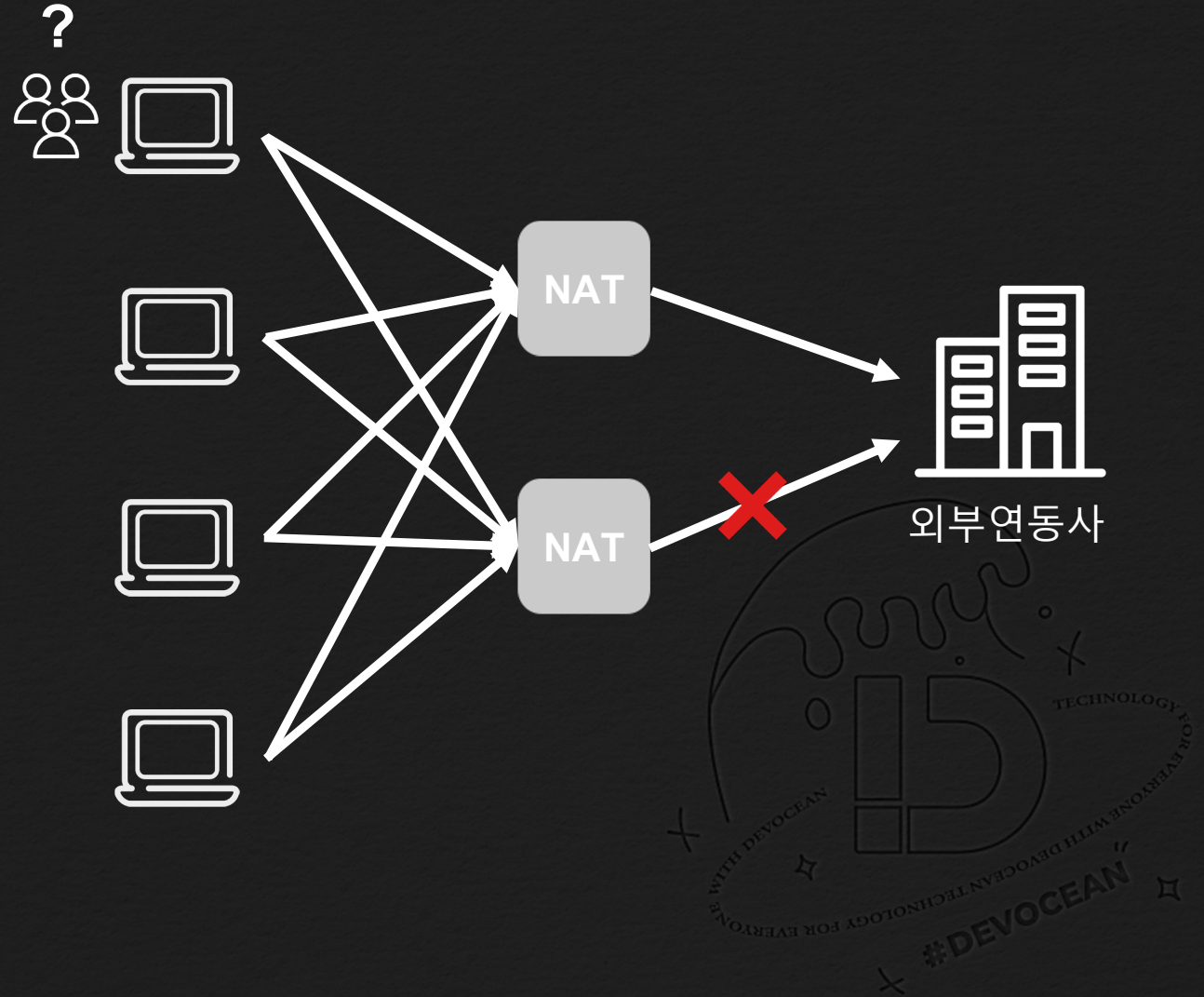
06 NAT와 방화벽

- 개발 업무 중 외부 연동을 위해 NAT IP에 대한 방화벽 요청이 필요할 수 있음
- 이중화 구성이 되어있는 사내 네트워크에서 하나의 NAT IP만 외부 연동을 신청하면 연결이 되었다 안되었다 할 수 있다.
- 사내의 NAT IP를 미리 파악해서 신청을 하면 네트워크 문제를 해결할 수 있다.



06 NAT와 방화벽

- 개발 업무 중 외부 연동을 위해 NAT IP에 대한 방화벽 요청이 필요할 수 있음
- 이중화 구성이 되어있는 사내 네트워크에서 하나의 NAT IP만 외부 연동을 신청하면 연결이 되었다 안되었다 할 수 있다.
- 사내의 NAT IP를 미리 파악해서 신청을 하면 네트워크 문제를 해결할 수 있다.



마치며...

- DNS를 활용한 온프레미스 + 클라우드 운영방법(+GSLB with 재해복구)
- MSA, 쿠버네티스 환경에서의 Service Registry, Service Discovery
- DNS A 레코드, CNAME 레코드
- NAT 이중화 시 방화벽 허용

- 짧지만 긴 시간 동안 네트워크에 대해 학습할 수 있어서 좋았습니다.
- 취업을 준비하며 멘토로만 봐왔던 분과 함께 해서 새로웠습니다.
- 퇴근후에 다른일을 한다는게 얼마나 대단한지 깨닫게 되었습니다.





감사합니다

2024.08.08 고재민

