AWS 네트워크 구조

에 대해 알아보자

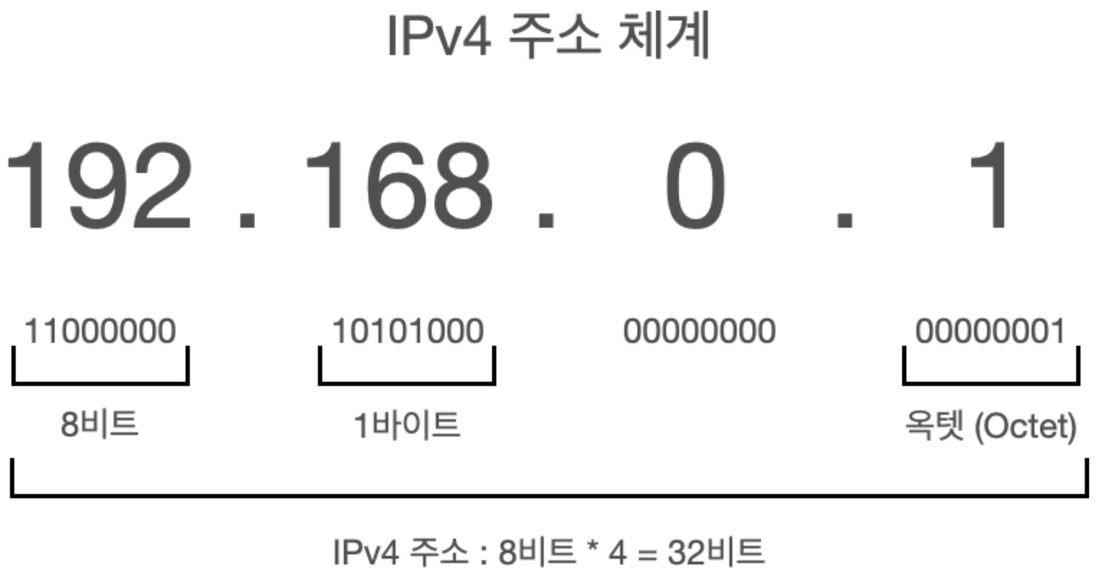
김은빈 2023.10.07

목차

CONTENT

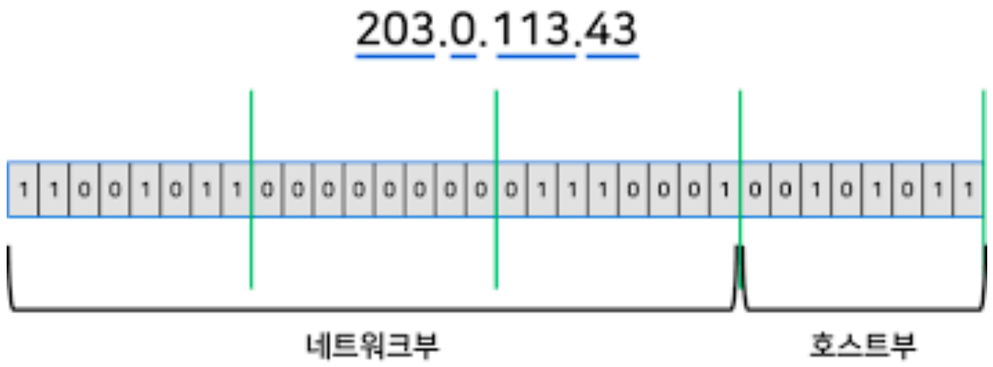
1. IP와 서브넷
2. Private IP와 NAT
3. VPC
4. AWS network 아키텍처 예시

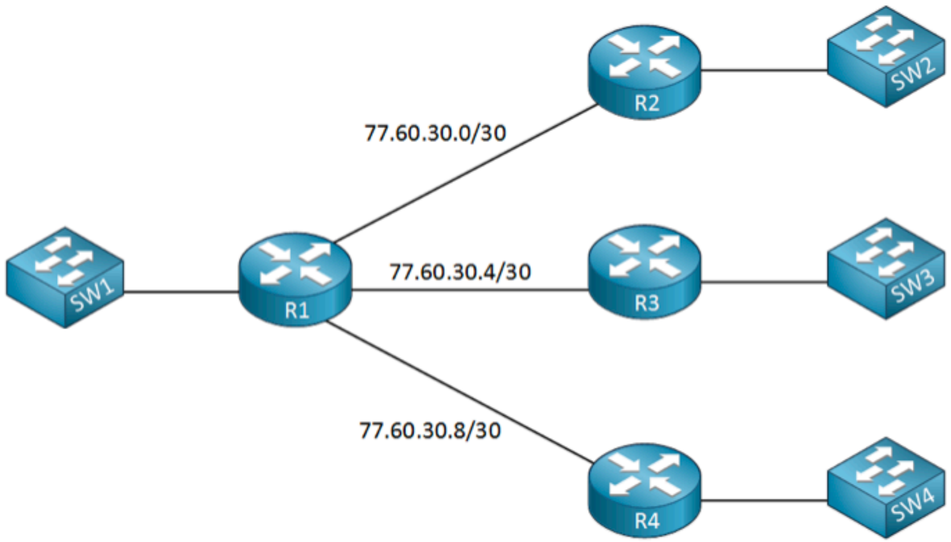
IP 주소



* IP 통신에서 기기들이 서로 식별하기 위해 필요한 고유 번호이다.
* 총 32비트, 8비트씩 끊어서 표기한다.

서브넷





* IP는 네트워크부와 호스트부로 나뉜다.

* IP 범위를 할당할 때 네트워크부의 길이를 조절해서 네트워크의 크기를 정한다.
  '/' 뒤의 숫자가 네트워크부의 길이를 뜻함

* Ex) 77.60.30.0/28을 4개로 나누려면?

77.60.30.0000/0000
네트워크부 호스트부

00XX 77.60.30.0/30
01XX 77.60.30.4/30
10XX 77.60.30.8/30
11XX 77.60.30.12/30

이처럼 네트워크부 길이를 자유롭게 바꿔서
IP 범위를 할당하는 기법을 *CIDR*라고 부르고, 서브넷팅이라고도 함

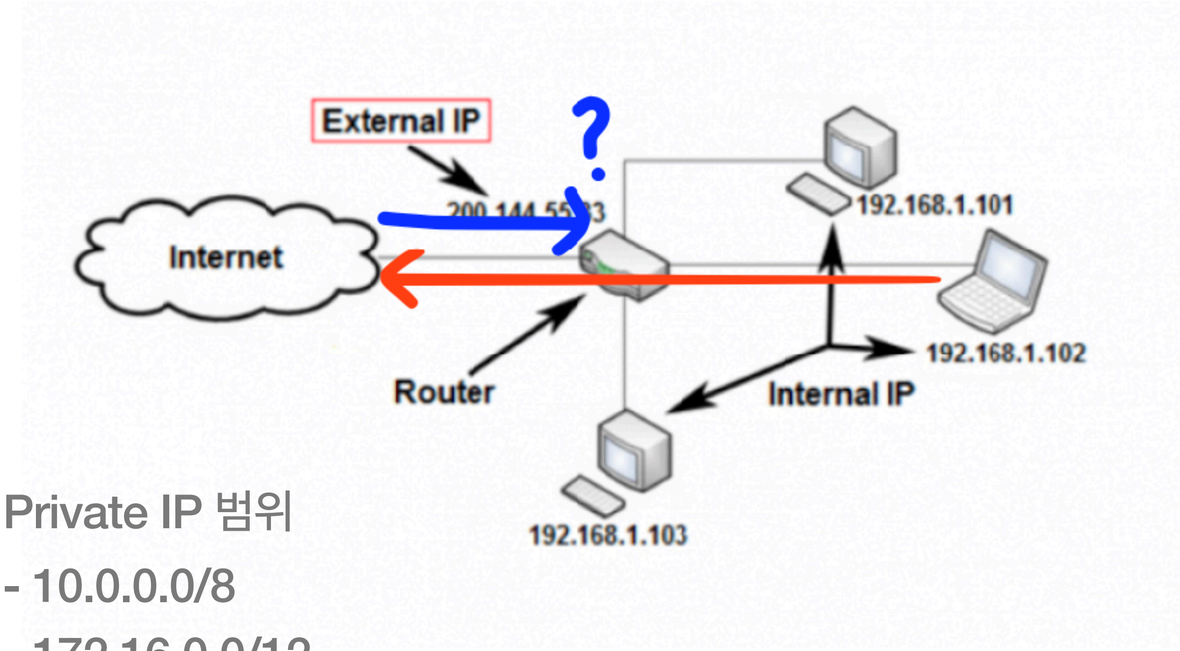
2. Private IP와 서브넷

Private IP

라우터(200.144.55.33)

192.168.1.102에서 ~~ 서버에 요청을 보내고 싶구나!

나한테 n번 포트로 응답을 주면, 192.168.1.102의 m번 포트로 돌려줘야겠다



Private IP 범위

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

* 모든 인터넷 기기가 하나의 IP를 가진다면 IP가 고갈될 것이다. (총 42억개)

→ **Private IP 사용**

* 고유한 **Public IP**는 라우터(공유기)만 가진다.

* 라우터에 연결된 기기는 네트워크 안에서만 사용할 수 있는 **Priavte IP**를 할당받는다.

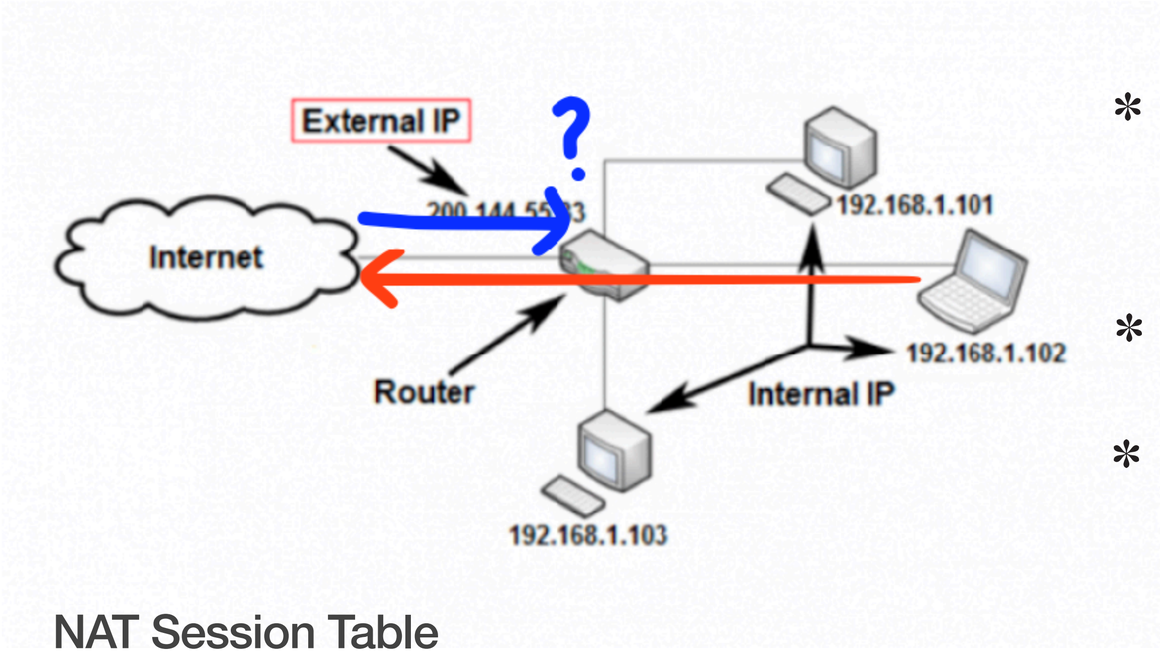
2. Private IP와 서브넷

NAT

라우터(200.144.55.33)

192.168.1.102에서 ~~ 서버에 요청을 보내고 싶구나!

나한테 n번 포트로 응답을 주면, 192.168.1.102의 m번 포트로 돌려줘야겠다



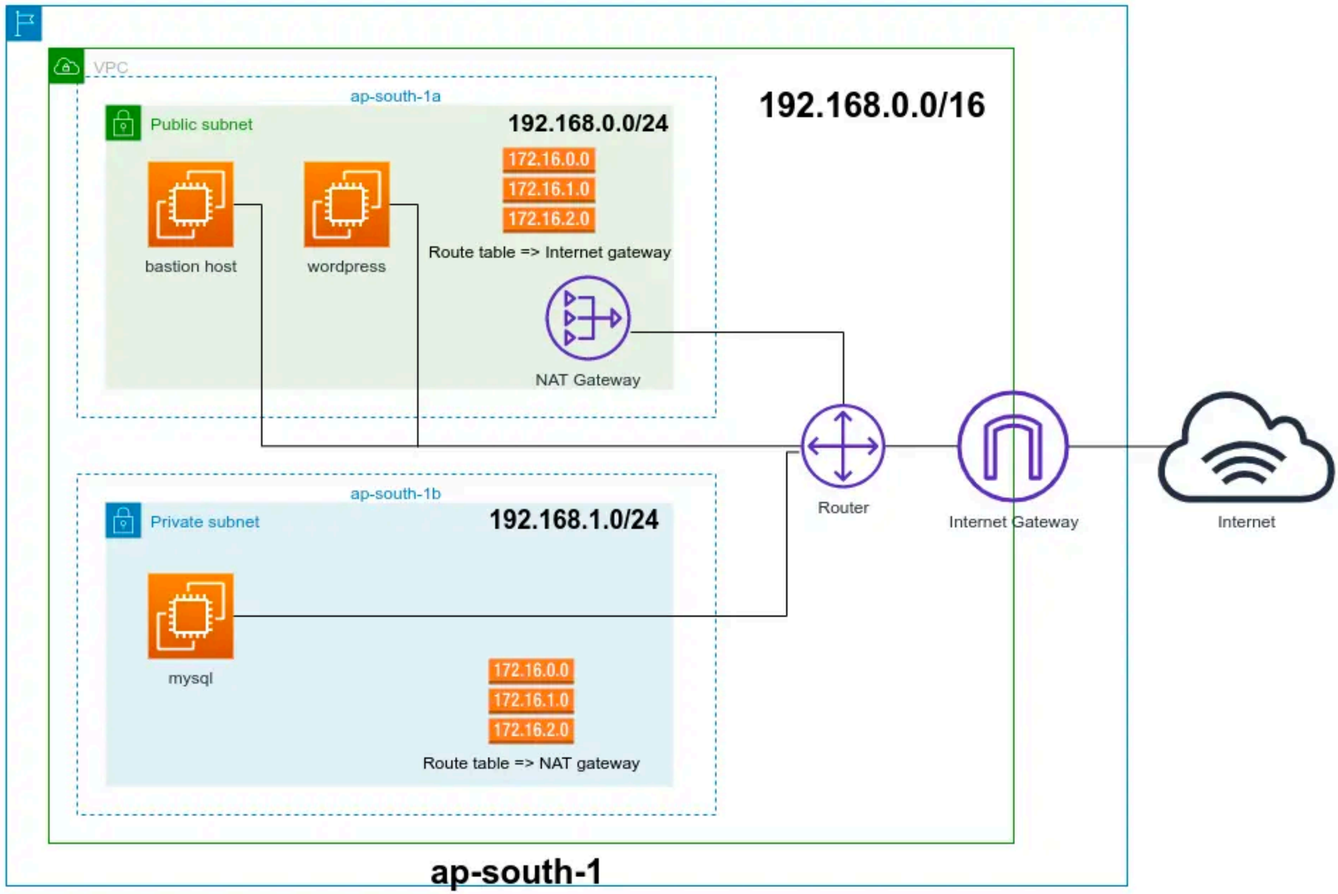
NAT Session Table

Origin IP	Origin Port	NAT IP	NAT Port
192.168.1.102	m	200.144.55.33	n

* Private 네트워크가 인터넷과 통신할 수 있도록 출발지, 목적지를 저장하고 패킷 정보를 바꿔주는 것
* 해당 정보는 세션 테이블에 저장된다.
* NAT를 수행하는 기기는 다양하다.
  보통 집 네트워크에서는 공유기가 이 역할을 한다.

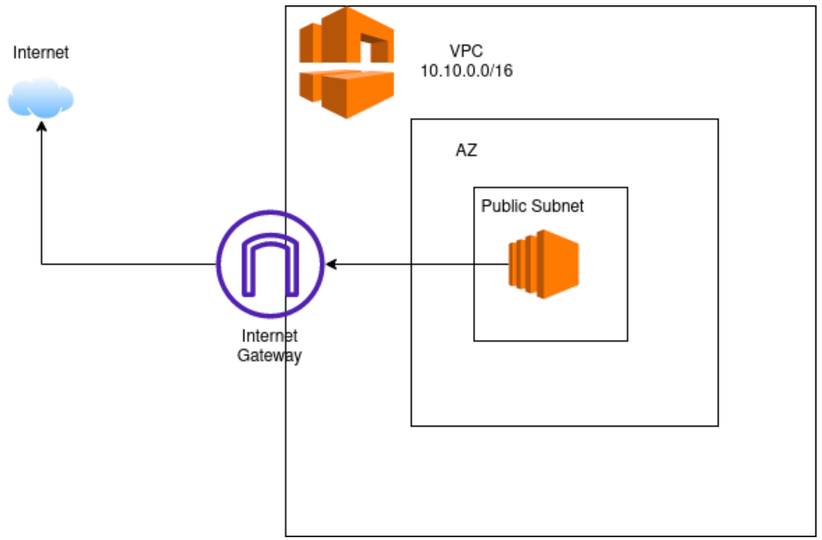
VPC

- AWS 안에 있는 나만의 네트워크
- EC2, RDS 등 리소스들은
  모두 VPC 내에 속함
- /16 ~ /24 사이로 IP 대역을 정할 수 있음
- VPC에서 10.0.1.0/24와 10.0.2.0/24
  두 서브넷을 쪼개서 사용함.
- 특정 리소스를 서브넷에 연결시킬 수 있음

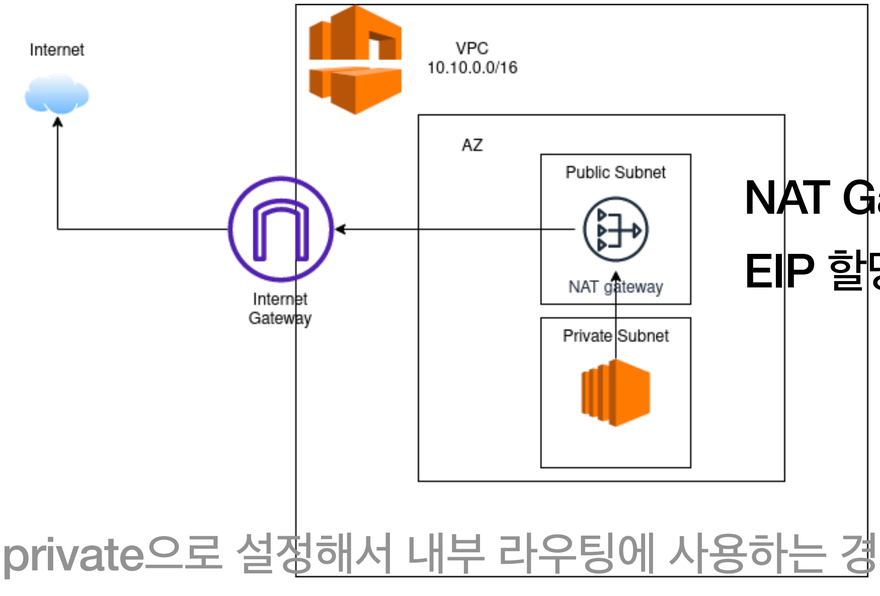


Public, Private subnet

- Public subnet
  - Internet gateway(IGW)과 연결된 서브넷
  - IGW가 NAT를 수행해준다
  - IGW는 요금 부과 없음
  - Inbound, Outbound 통신 모두 가능



- Private subnet
  - Internet gateway와 연결되지 않은 서브넷
  - NAT Gateway와 연결하면 Outbound 통신만 가능
  - NAT Gateway는 요금 부과됨
  - 외부 접근이 불가능하므로 보안적으로 안전



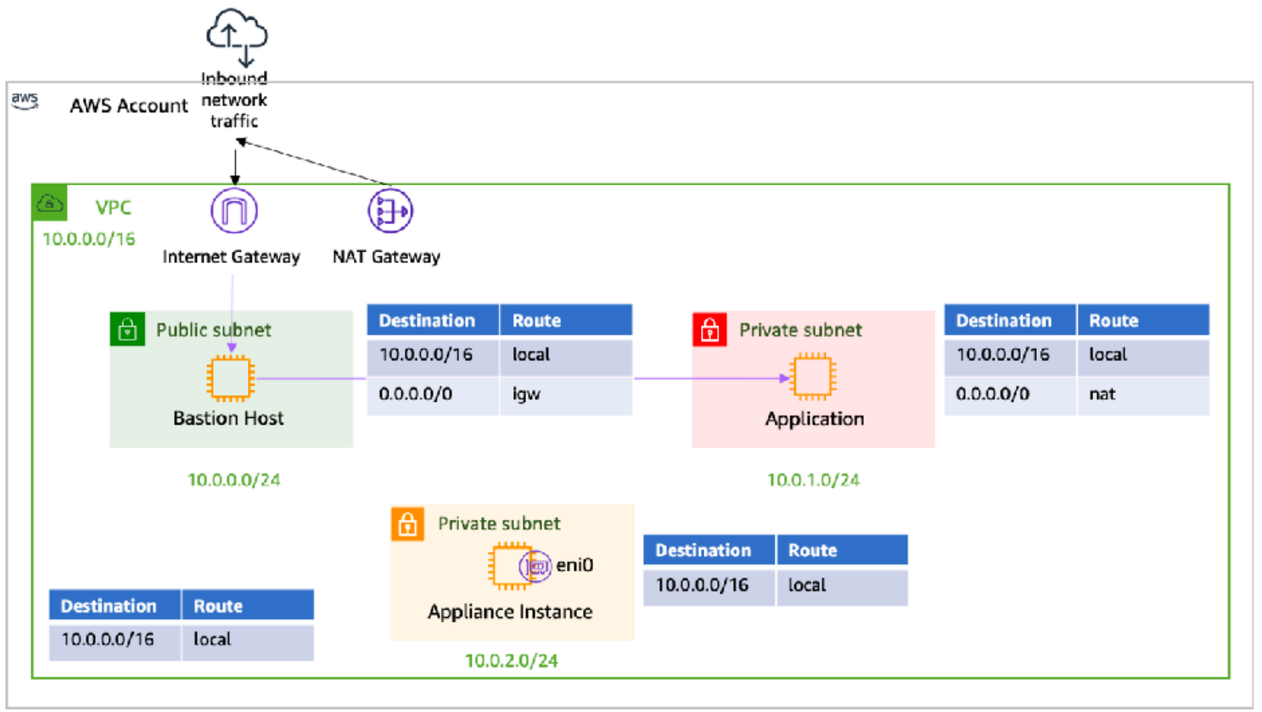
NAT Gateway에
EIP 할당해줘야함

NAT gateway를 private으로 설정해서 내부 라우팅에 사용하는 경우도 있긴 함

3. VPC

Routing table 어디로 라우팅할지 정하는 테이블

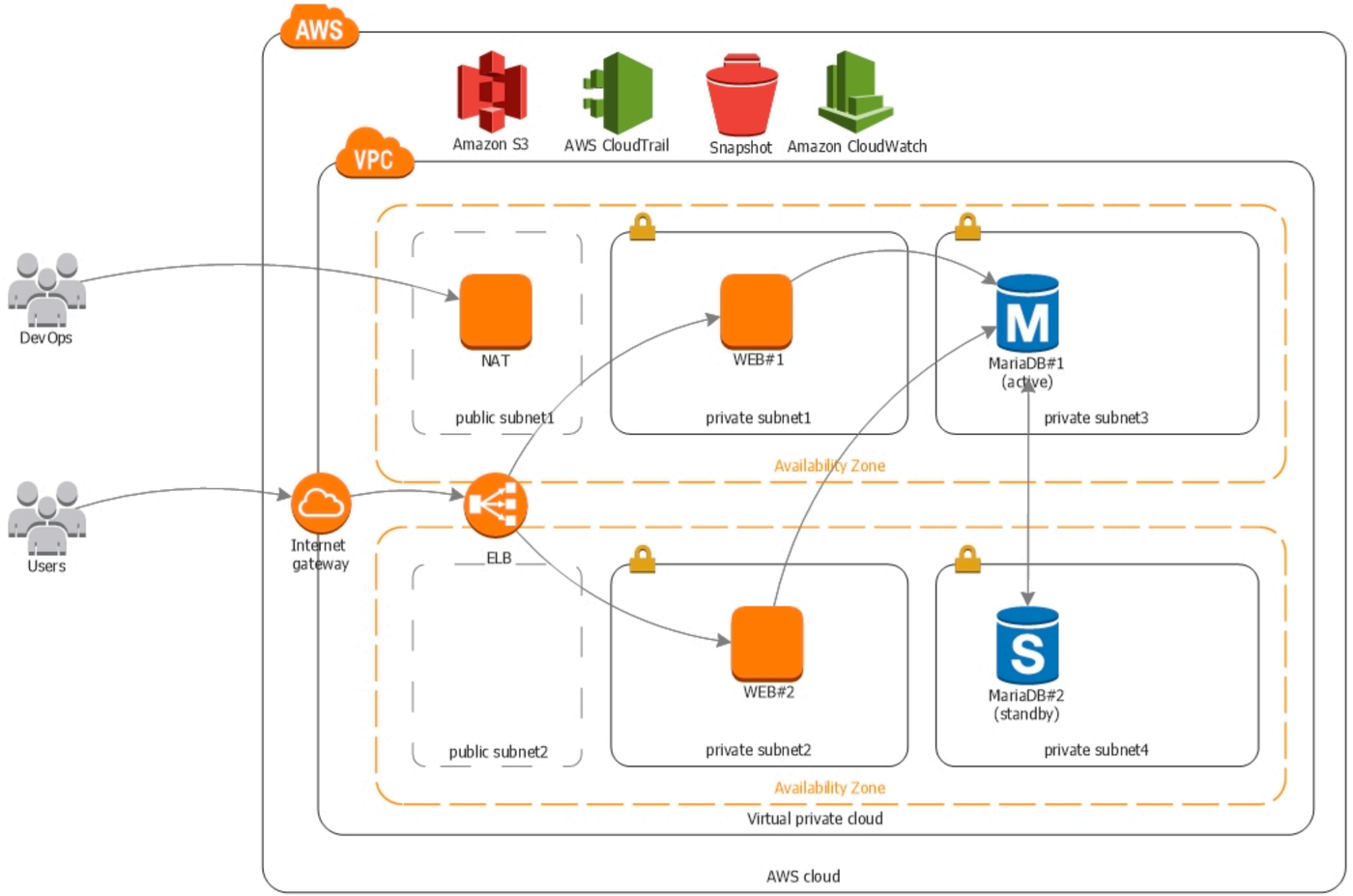
- Public subnet의 Route table
  - VPC 내부 IP 대역은 내부 네트워크로 라우팅
  - 나머지는 igw(외부 인터넷)으로 라우팅
- NAT 있는 Private subnet의 Route table
  - VPC 내부 IP 대역은 내부 네트워크로 라우팅
  - 나머지는 NAT(외부 인터넷)으로 라우팅
- NAT 없는 Private subnet의 Route table
  - VPC 내부 IP 대역은 내부 네트워크로 라우팅



4. AWS network 아키텍처 예시

1번 예시

- 보안을 위해 애플리케이션 서버 및 DB는 Private subnet에 둠
- 사용자가 서버에 접근할 때는 지정된 포트로만 ELB를 통해 가능
- S3, CloudTrail과 같은 서비스는 VPC에 속하지 않음



4. AWS network 아키텍처 예시

2번 예시

- Xquare 인프라
- 이런식으로 서버를 private subnet으로 빼는게 유명한 best practice임
- 현재는 NAT Gateway 비용이 비싸 EC2도 private subnet으로 옮겨놓음