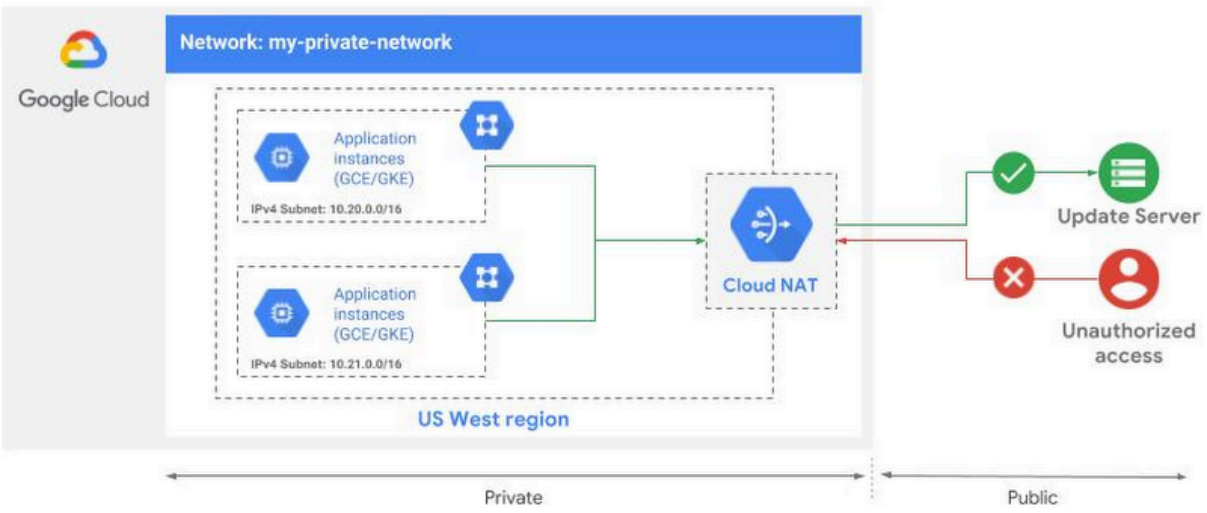
# 네트워크 설계

## Cloud NAT

- 가급적이면, VM 인스턴스에 내부 IP 주소만 할당하는 것이 좋다.
- Cloud NAT은 구글의 관리형 네트워크 주소변환서비스다. Cloud NAT을 사용하면 공개 IP 주소 없이 애플리케이션 인스턴스를 프로비저닝할 수 있을 뿐만 아니라 제어 가능하고 효율적인 방식으로 인스턴스의 인터넷 액세스를 허용할 수 있다. 즉, 비공개 인스턴스가 업데이트, 패치, 구성 관리 등을 위해 인터넷에 액세스할 수 있다.




## GCP vs AWS

- GCP는 AWS처럼 Public Subnet 및 Private Subnet 개념이 존재하지 않는다.
- 모든 VPC의 서브넷에는 Internet Gateway로 설정이 되어 있으며, Public IP를 가지지 않은 VM의 경우는 Cloud NAT가 설정되어 있어야만, 외부 통신이 가능하다. 즉 서브넷에서 Public IP를 가진 VM은 외부 IP로 직접 통신이 가능하고 Public IP를 가지지 않은 VM은 Cloud NAT을 통해서 외부 통신이 가능하다.
- Cloud BAT는 리전 베이스로 동작하기 때문에, VPC 내에서 Cloud NAT가 설정된 리전에 속한 모든 서브넷이 대상이 되며 필요 시 커스텀 모드로 특정 서브넷만 포함할 수 있다.

| 구분 | GCP | AWS |
| --- | --- | --- |

| | | |
|---|---|---|
| Public 통신<br>(inbound, Outbound 모두 가능) | VM에 외부 IP 할당(기본) | Public Sutnet<br>Internet Gateway와 연동 |
| Outbound 통신만 가능 | Subnet에 Cloud NAT 연동 | Private Subnet<br>NAT Gateway와 연결 |
| VPC 외부와 완전 격리 | VM에 외부 IP 없고 해당 서브넷에 Cloud NAT 연동 없음 | Private Subnet<br>NAT Gateway 연결 없음 |

# 비공개 Google Access