

AWS

# VPC Virtual Private Cloud





# CONTENTS

## 01. VPC란?

- VPC 특징
- VPC 구성요소
- IP 주소 지정
- IPv4 CIDR블록

## 02. 서브넷

## 02. 라우팅 테이블

## 04. 외부 연결

- 인터넷 게이트웨이
- NAT 게이트웨이
- Bastion Host
- VCP 피어링

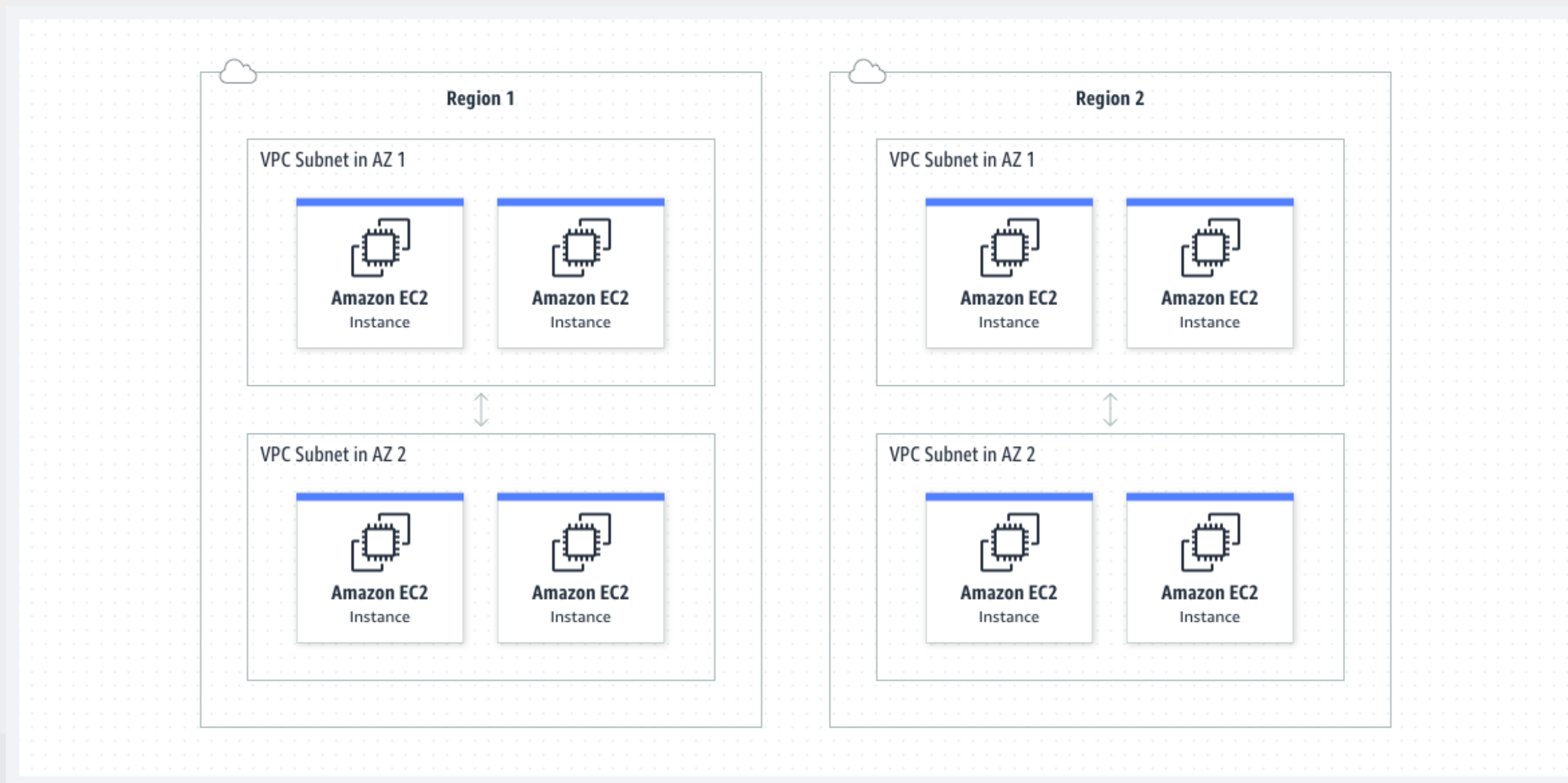
## 05. DHCP 옵션셋

## 06. 보안

- 보안그룹
- ACL

# VPC란?

Amazon Virtual Private Cloud(Amazon VPC)를 사용하면 정의한 논리적으로 격리된 가상 네트워크에서 AWS 리소스를 시작할 수 있습니다. 이 가상 네트워크는 AWS의 확장 가능한 인프라를 사용한다는 이점과 함께 고객의 자체 데이터 센터에서 운영하는 기존 네트워크와 매우 유사합니다.



## VPC의 기본 구성 요소

- 인터넷 게이트웨이
- ACL / 보안 그룹
- 라우트 테이블
- NAT instance / NAT Gateway
- Bastion Host
- VPC EndPoint

## 가용 영역?

AWS 리전에 중복 전원, 네트워킹 및 연결이 있는 하나 이상의 개별 데이터 센터.

여러 AZ를 사용해서 단일 데이터 센터에서 가능한 것보다 더 높은 가용성, 내결함성 및 확장성을 갖춘

프로덕션 애플리케이션 및 데이터베이스를 운용할 수 있다.

## IPv4 VPC CIDR 블록

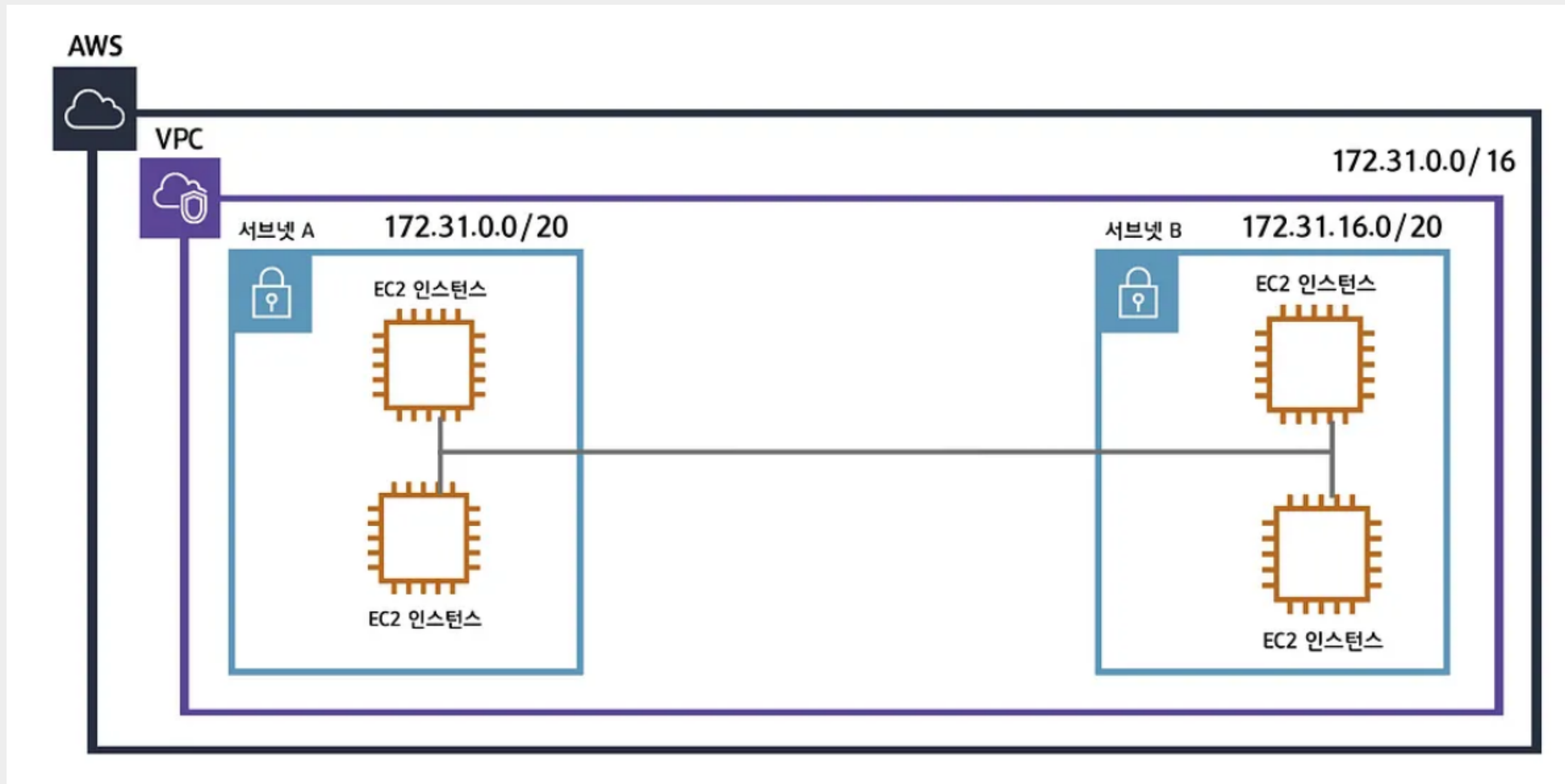
CIDR(Classless Inter-Domain Routing, 사이더)는 클래스 없는 도메인 간 라우팅 기법으로 1993년 도입되기 시작한, 최신의 IP 주소 할당 방법이다. CIDR는 기존의 IP 주소 할당 방식이었던 네트워크 클래스를 대체하였다. CIDR는 IP 주소의 영역을 여러 네트워크 영역으로 나눌 때 기존방식에 비해 유연성을 더해준다.

인터넷 연결이 필요한 경우 반드시 사설망 대역을 사용해야 한다

- 10.0.0.0 ~ 10.255.255.255(10/8 prefix)
- 172.16.0.0 ~ 172.31.255.255(182.16/12 prefix)
- 192.168.0.0 ~ 192.168.255.255(192.168/16 prefix)

# 서브넷

서브넷은 VPC의 IP 주소 범위



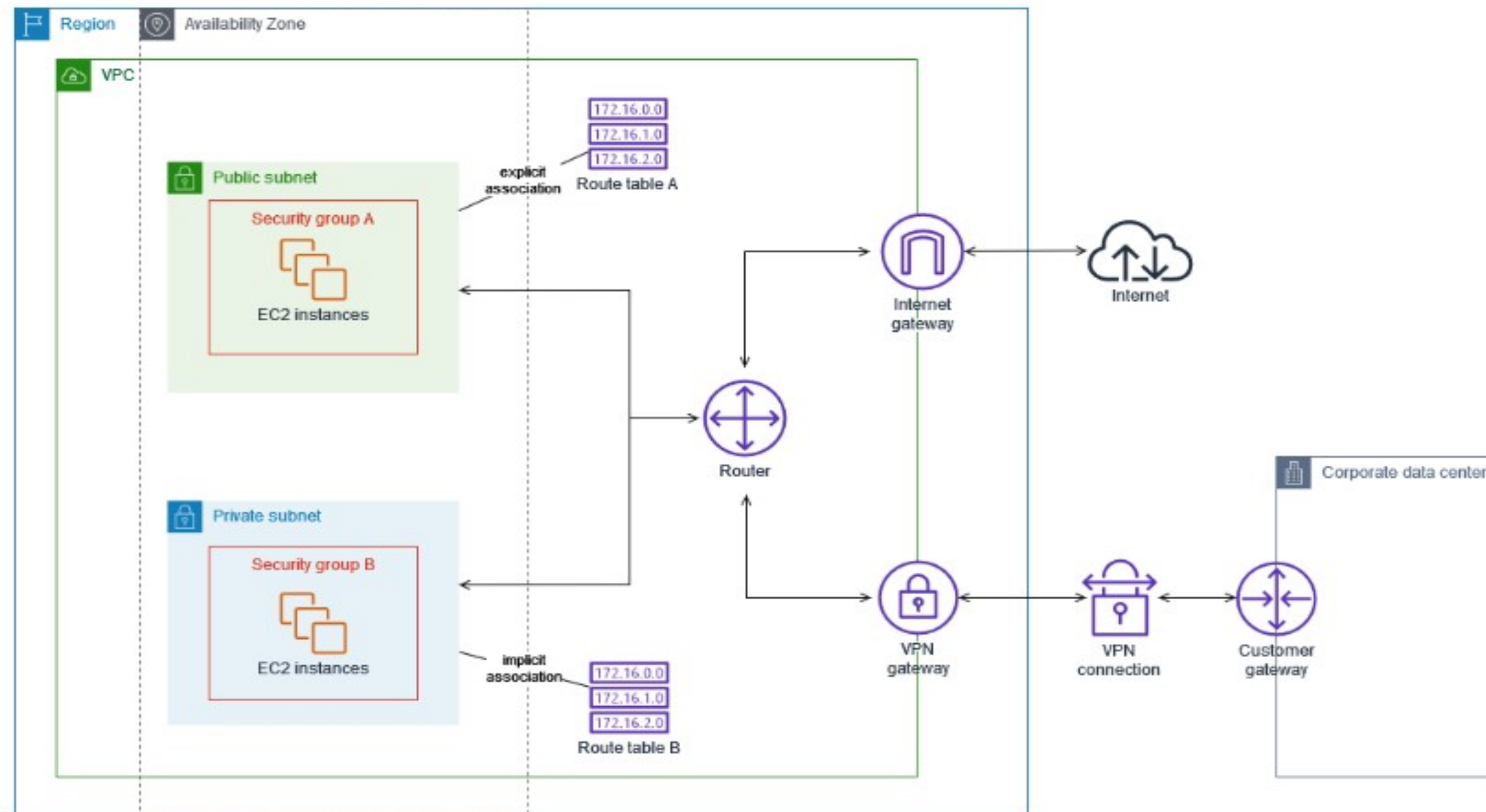
## 서브넷의 종류

- 퍼블릭 서브넷
- 프라이빗 서브넷
- VPN 서브넷
- 격리된 서브넷



## 라우팅 테이블

VPC에는 암시적 라우터가 있으며 라우팅 테이블을 사용하여 네트워크 트래픽이 전달되는 위치를 제어합니다. 테이블의 각 라우팅은 목적지 및 대상을 지정합니다.



# 라우팅 테이블

대상 주소	대상	
10.0.0.0/16	Local	IPv4 트래픽 Local 경로
172.31.0.0/16	pcx-11223344556677889	피어링 연결
0.0.0.0/0	igw-12345678901234567	인터넷 게이트웨이

구체적인 IP : local > 피어링 > 인터넷 게이트웨이

# 기본 생성 라우팅 테이블

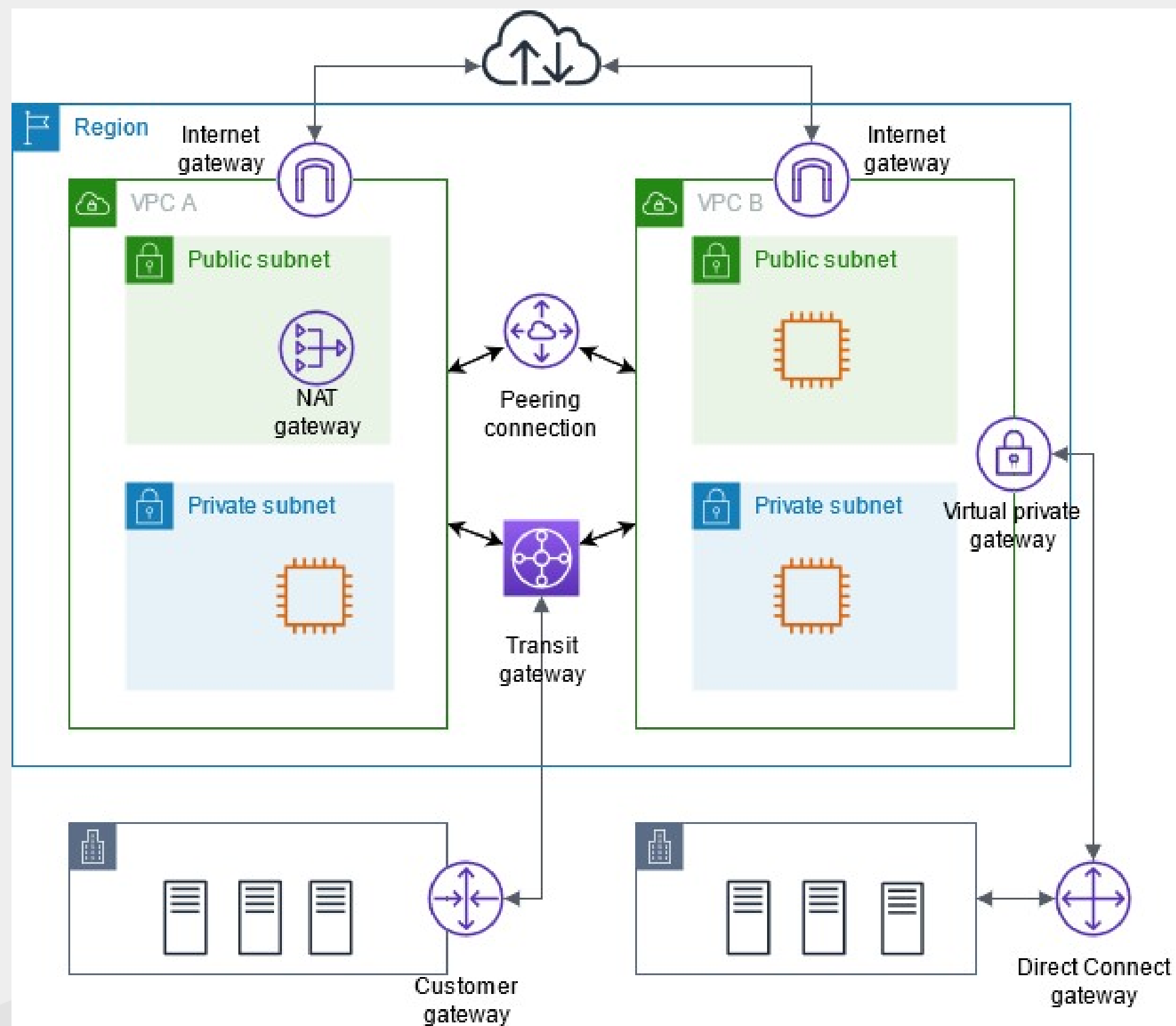
VPC를 만들면 기본 라우팅 테이블이 자동으로 생성된다. 서브넷이 라우팅 테이블과 명시적으로 연결되지 않은 경우 서브넷은 기본 라우팅 테이블이 기본적으로 사용된다.

# 라우팅 테이블

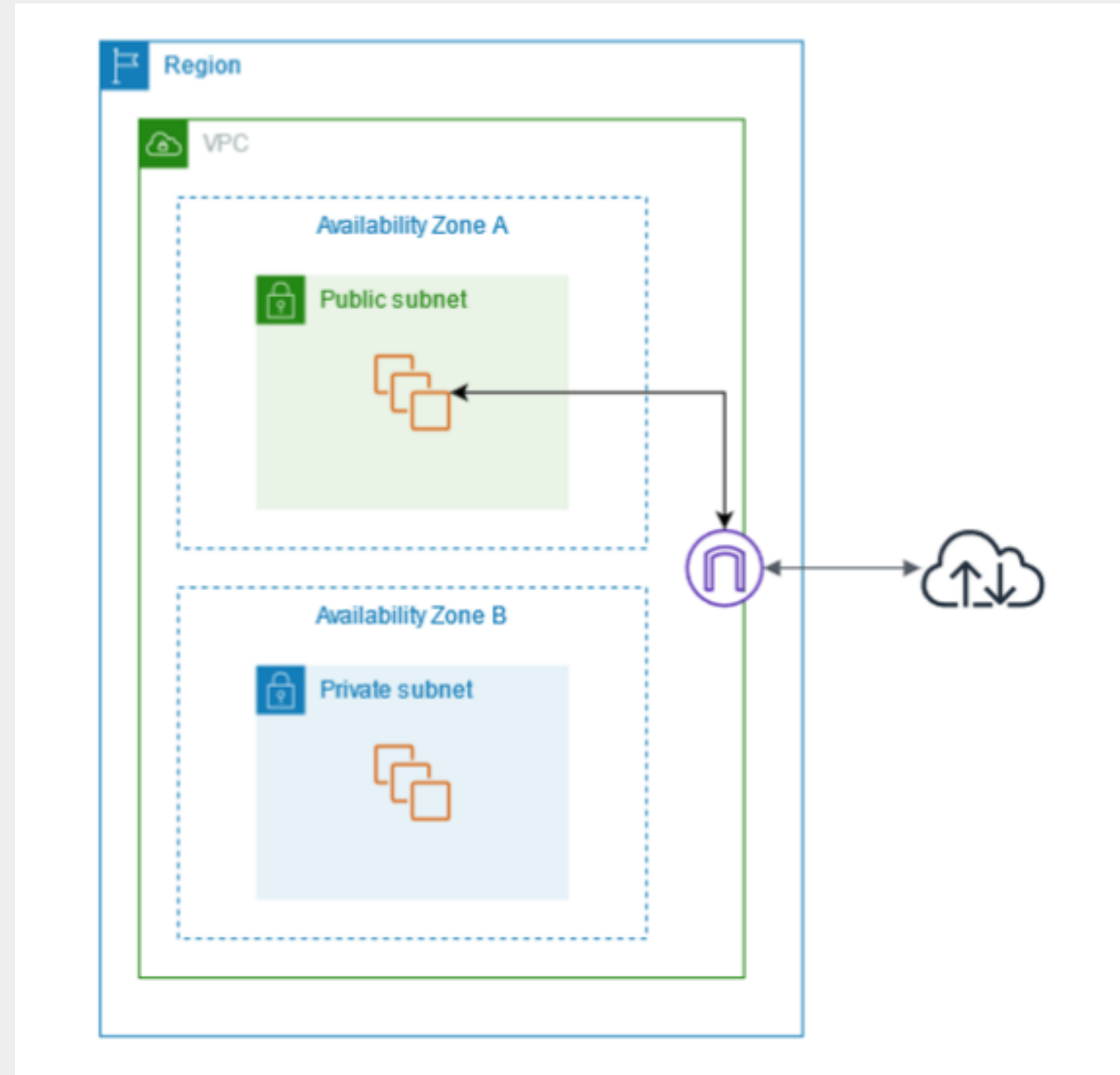
대상 주소	대상	
10.0.0.0/16	Local	IPv4 트래픽 Local 경로
172.31.0.0/16	pcx-11223344556677889	피어링 연결
0.0.0.0/0	igw-12345678901234567	인터넷 게이트웨이

구체적인 IP : local > 피어링 > 인터넷 게이트웨이

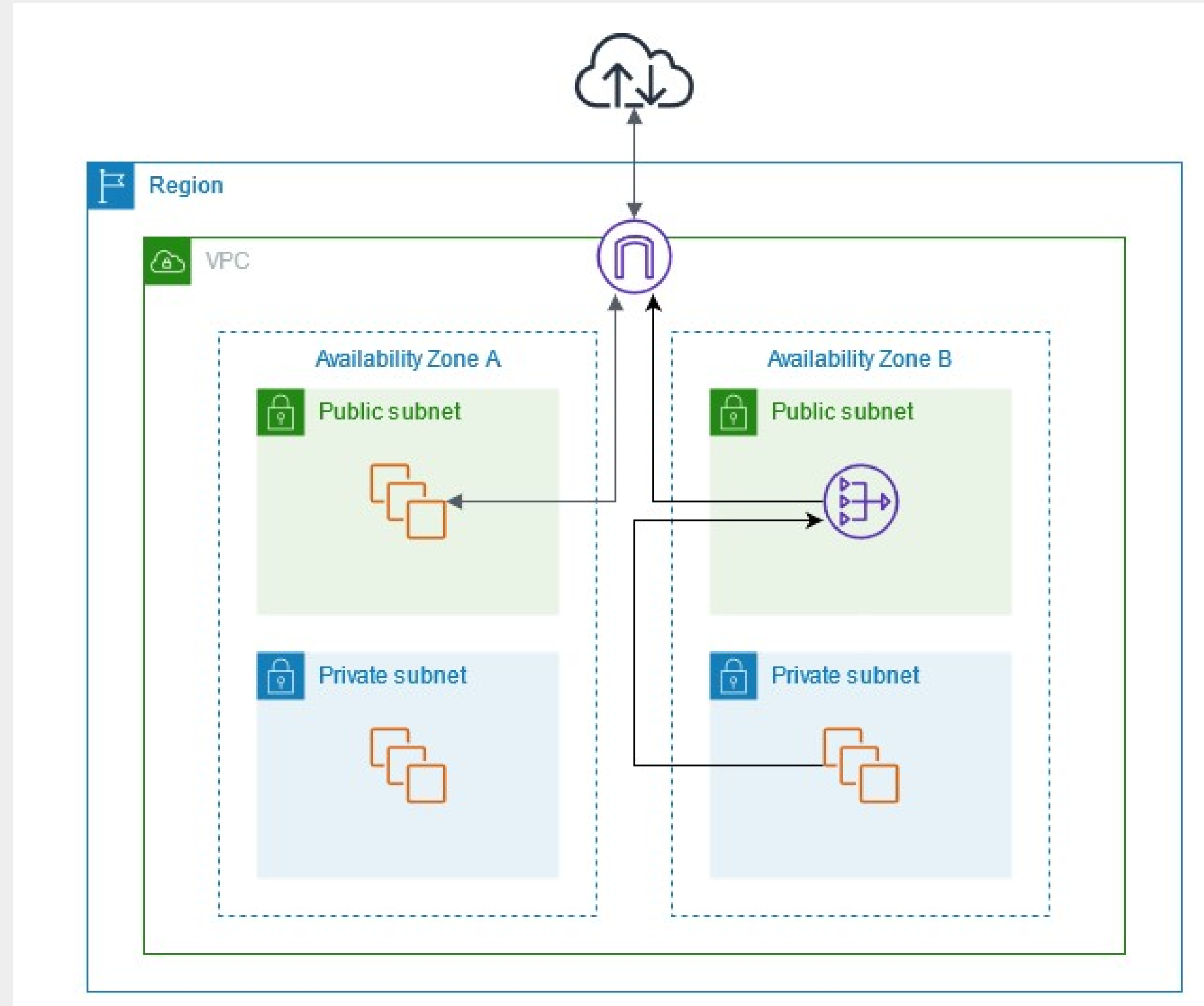
## 외부연결



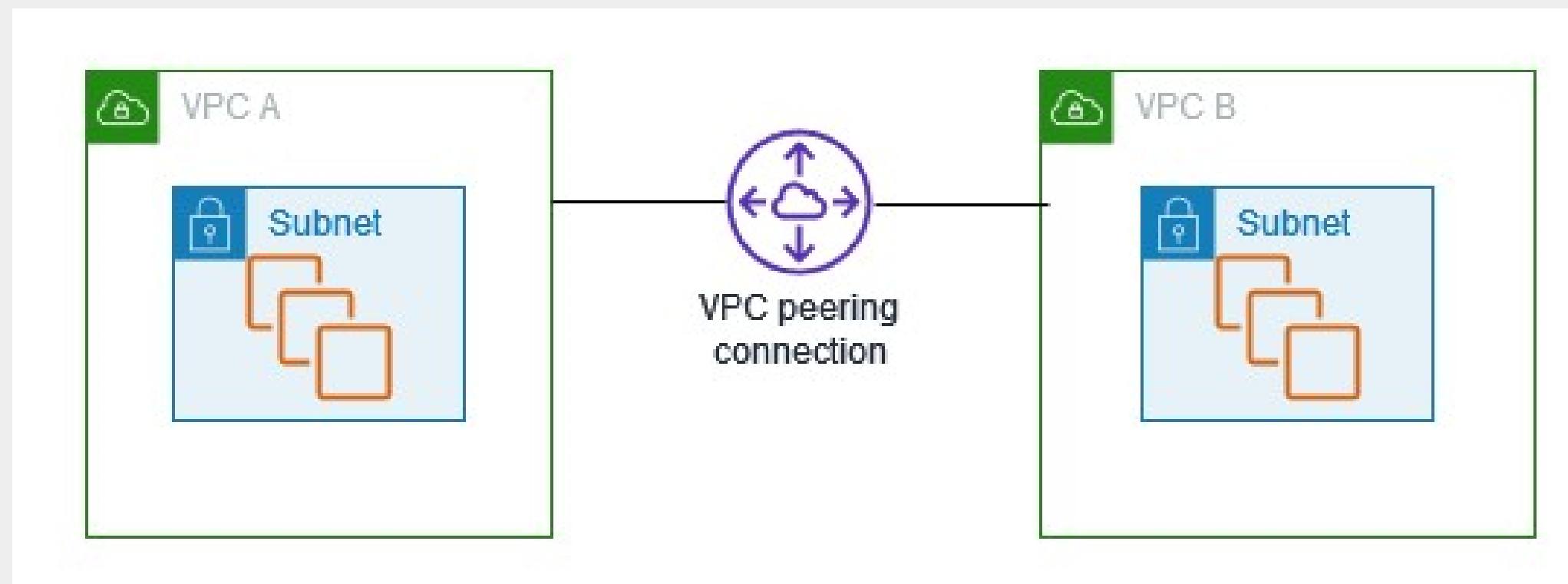
## 인터넷 게이트웨이



## NAT 게이트웨이

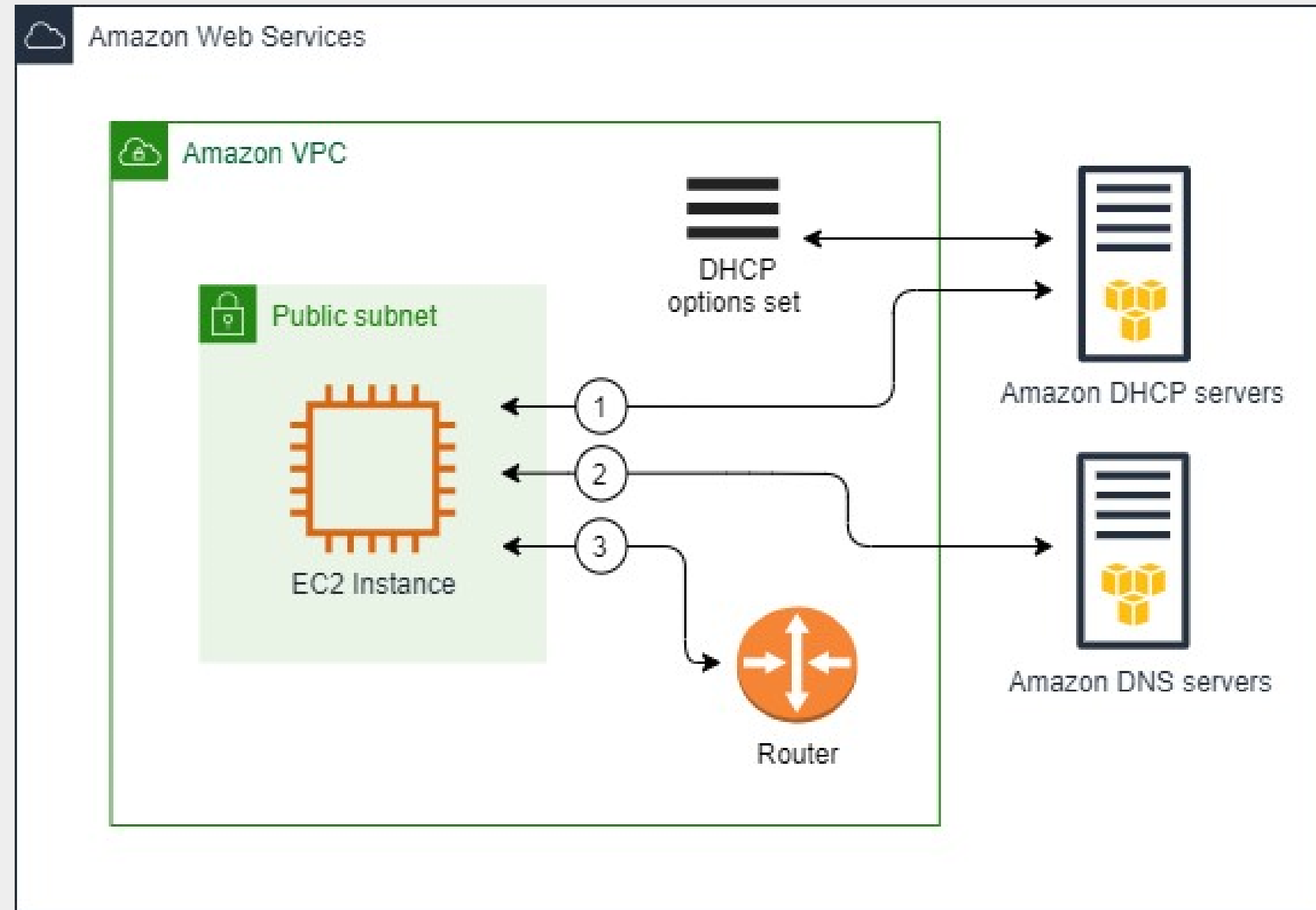


## VPC 피어링

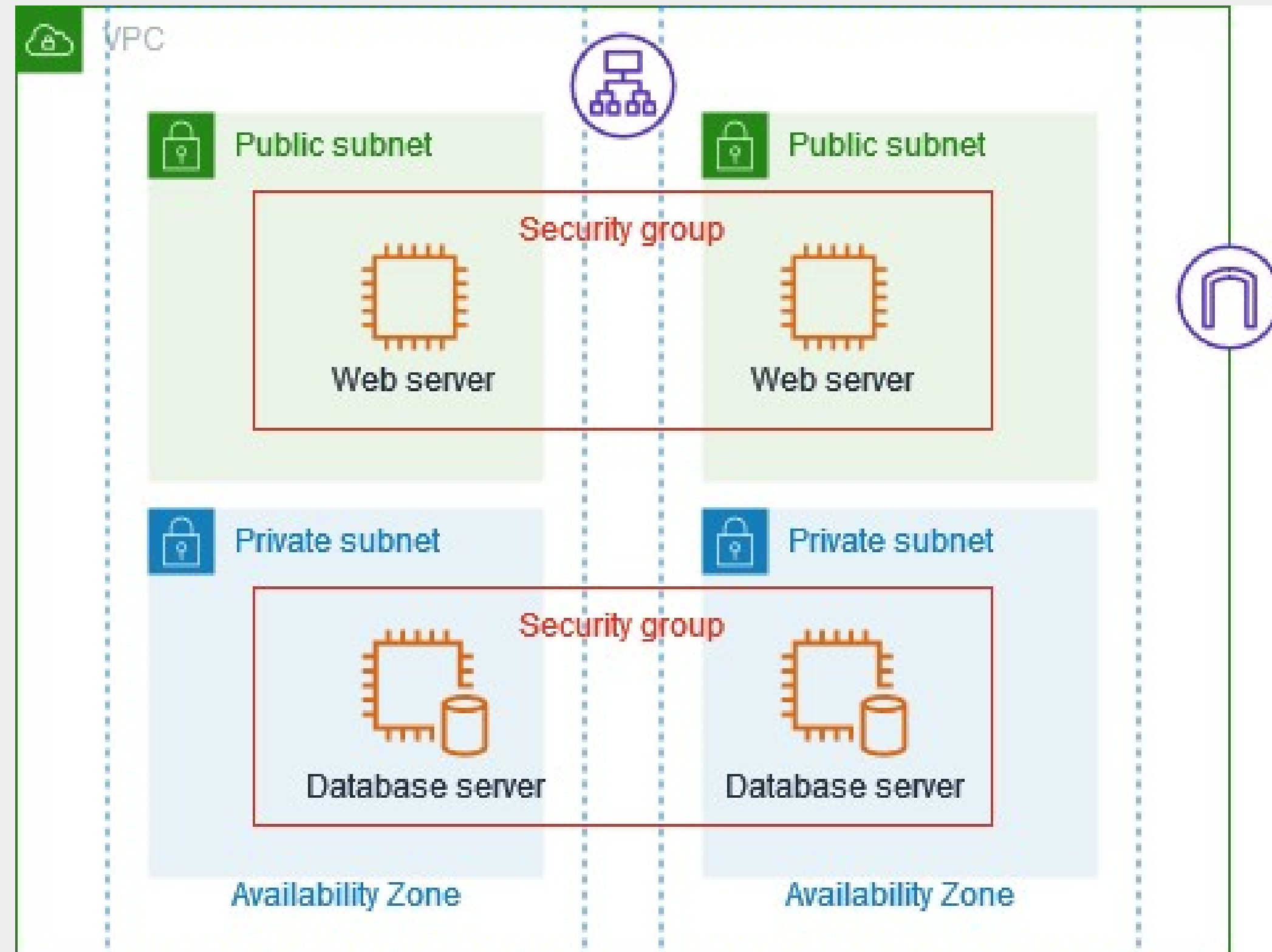




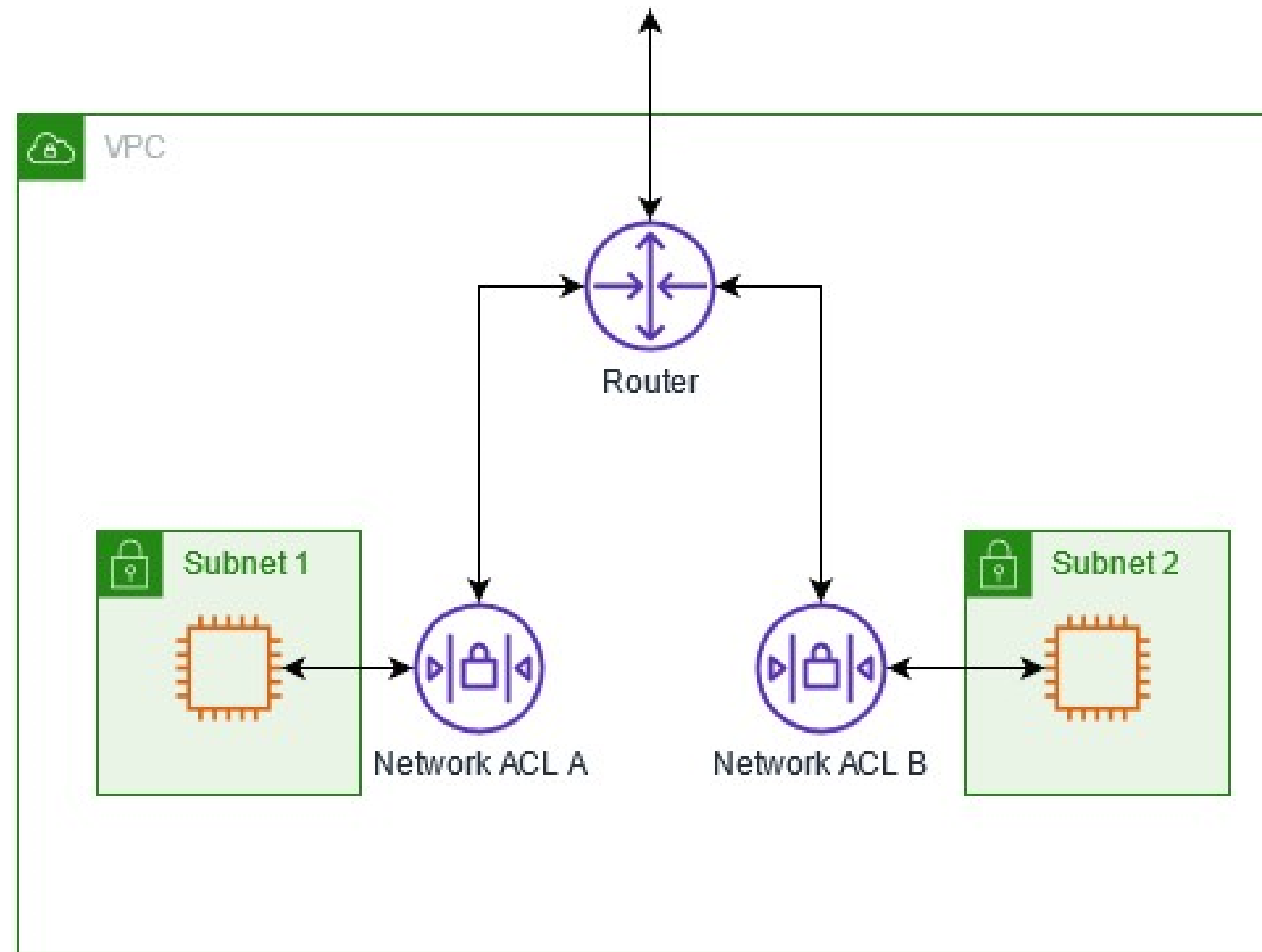
# DHCP 옵션셋



## 보안그룹



## ACL



실습