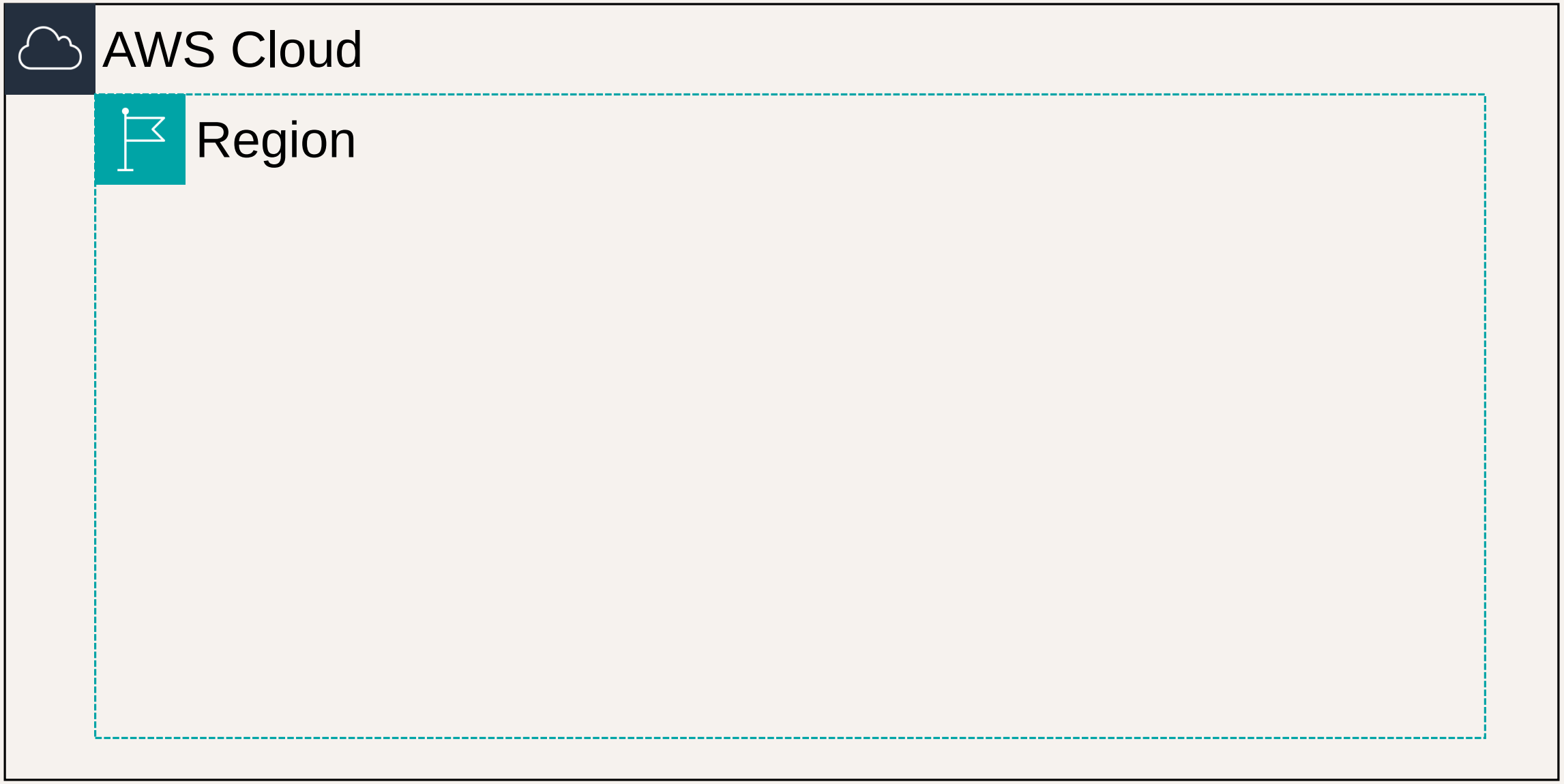
VPC

- **AWS 계정 전용 가상 네트워크**
- **사용자가 정의한 가상의 프라이빗 네트워크환경**
- **EC2 서버, RDS 서버, Lambda 등 구축 가능**

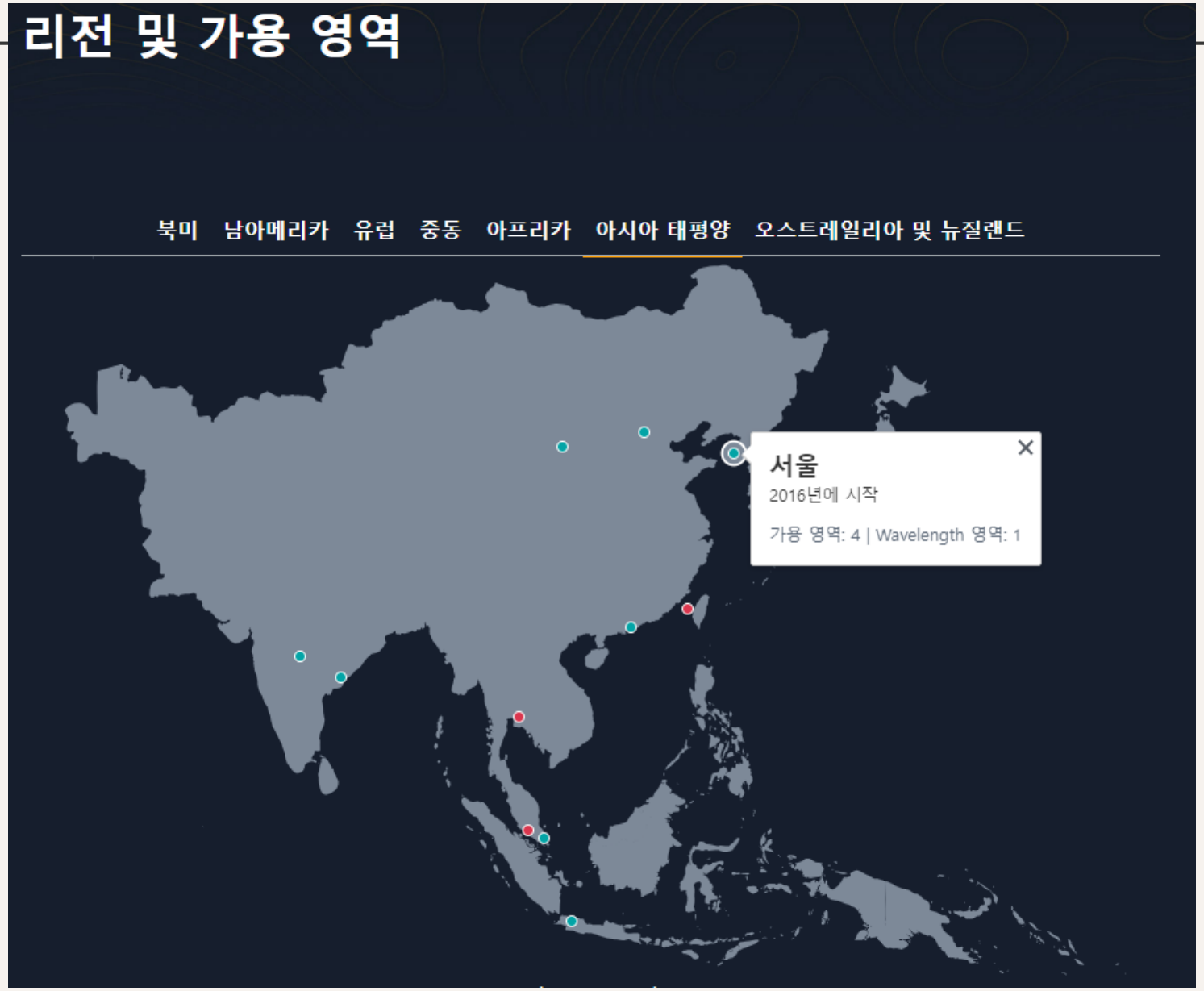
VPC

- 가상 네트워크 제어 가능
  - IP 주소 범위
  - 서브넷팅
  - 라우팅
  - 보안 그룹
- CIDR 블록으로 VPC 크기 지정

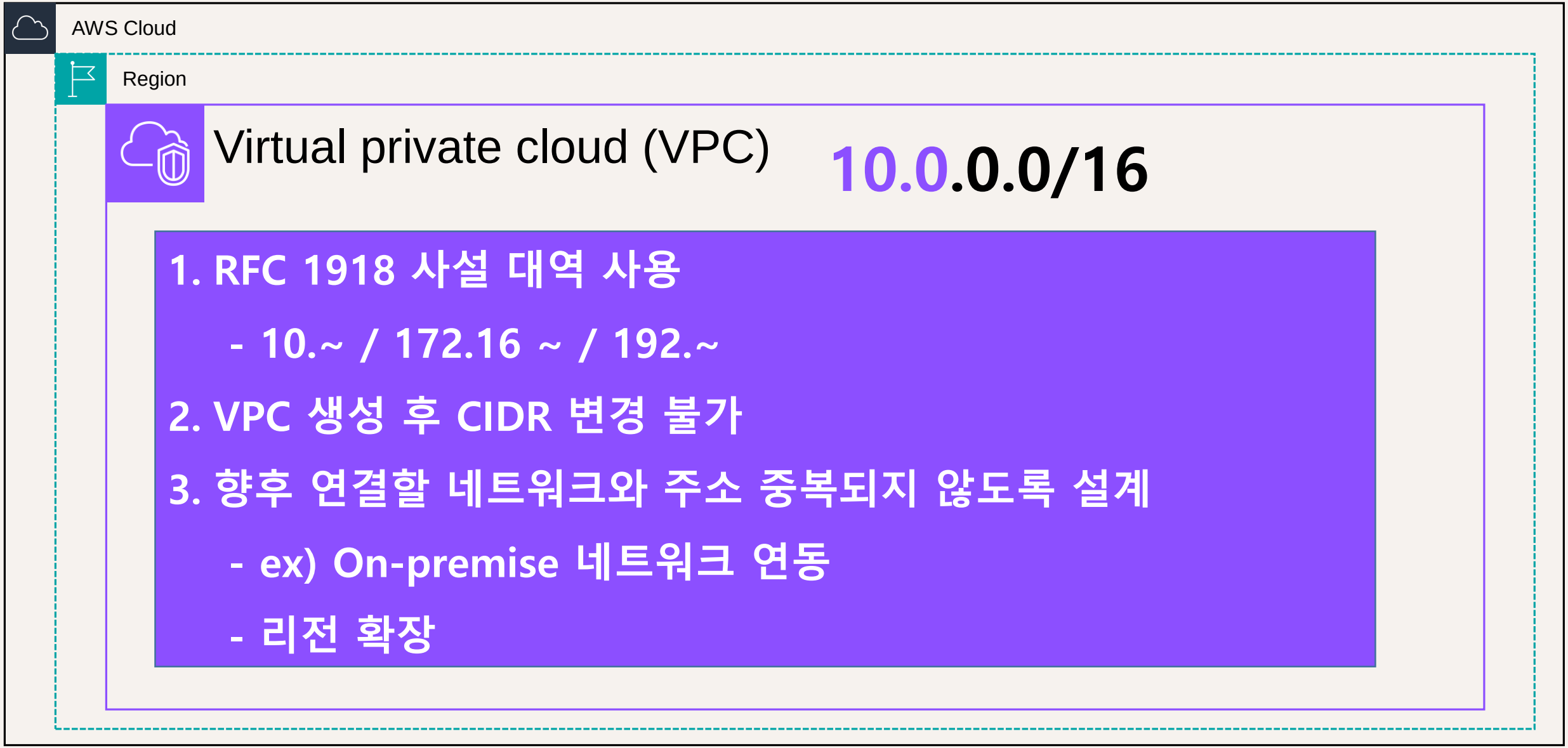
VPC



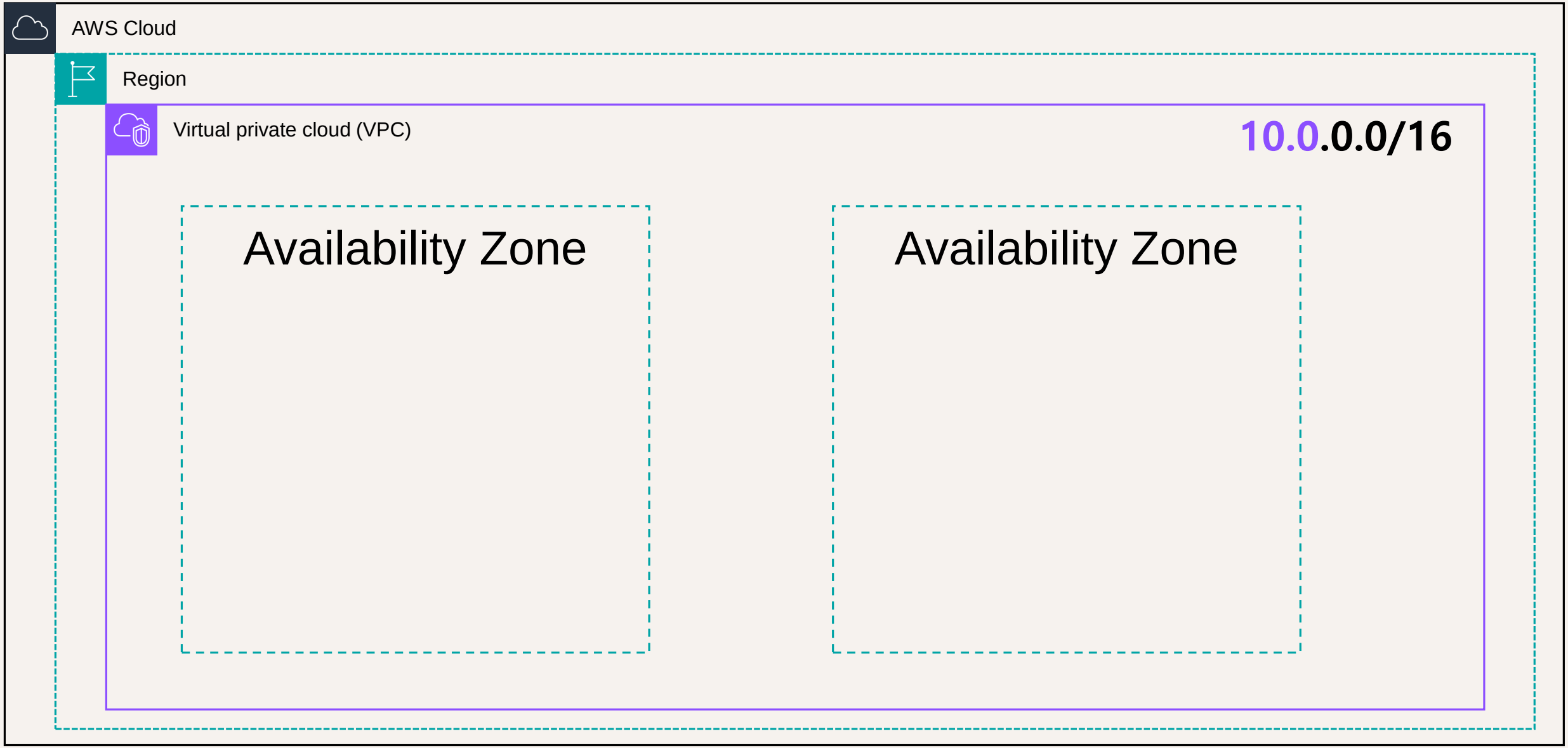
Region


리전 및 가용 영역
북미
남아메리카
유럽
중동
아프리카
아시아 태평양
오스트레일리아 및 뉴질랜드
서울
2016년에 시작
가용 영역: 4 | Wavelength 영역: 1

VPC


AWS Cloud
Region
Virtual private cloud (VPC)
10.0.0.0/16
1. RFC 1918 사설 대역 사용
- 10.~ / 172.16 ~ / 192.~
2. VPC 생성 후 CIDR 변경 불가
3. 향후 연결할 네트워크와 주소 중복되지 않도록 설계
- ex) On-premise 네트워크 연동
- 리전 확장

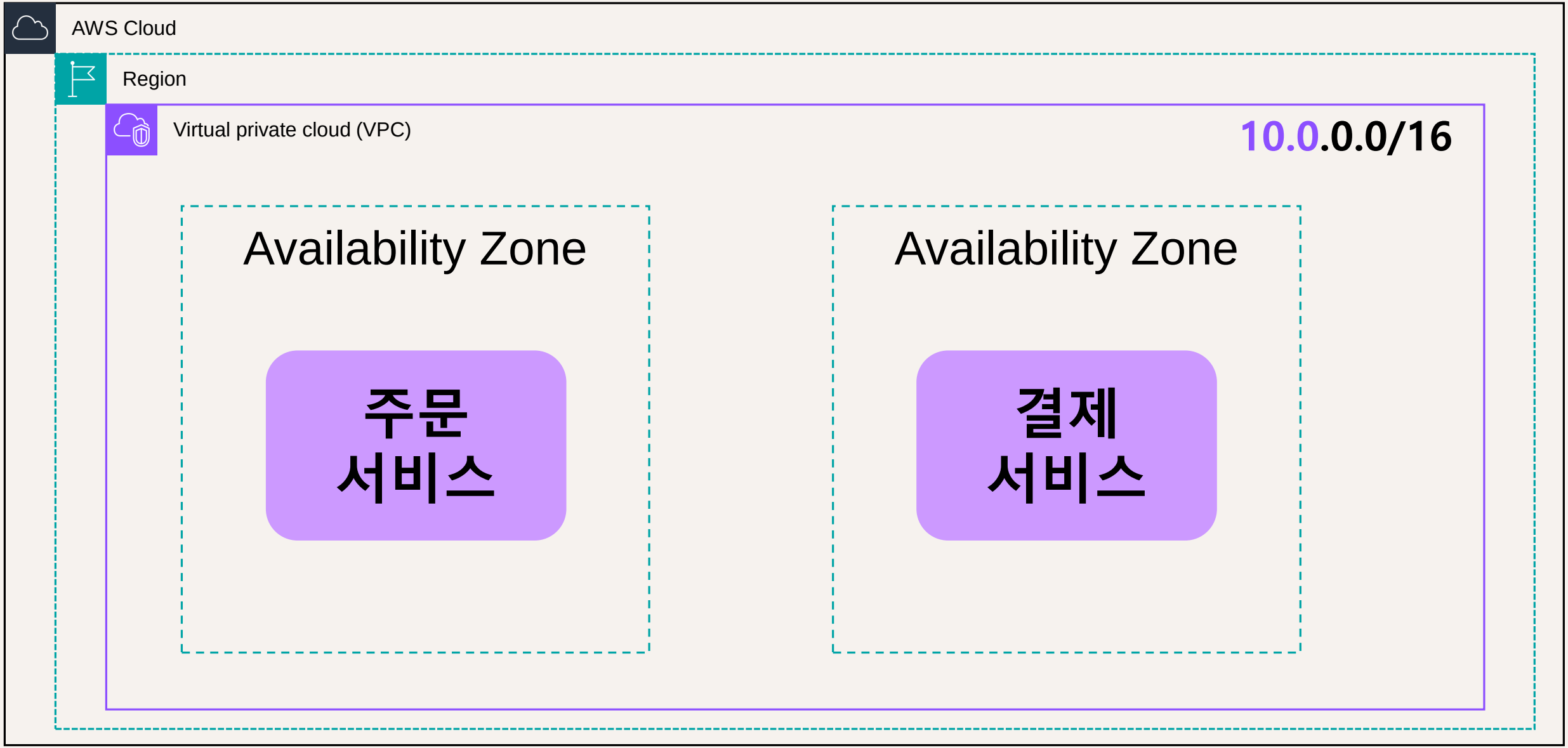
AZ (가용 영역)


AWS Cloud
Region
Virtual private cloud (VPC)
10.0.0.0/16
Availability Zone
Availability Zone

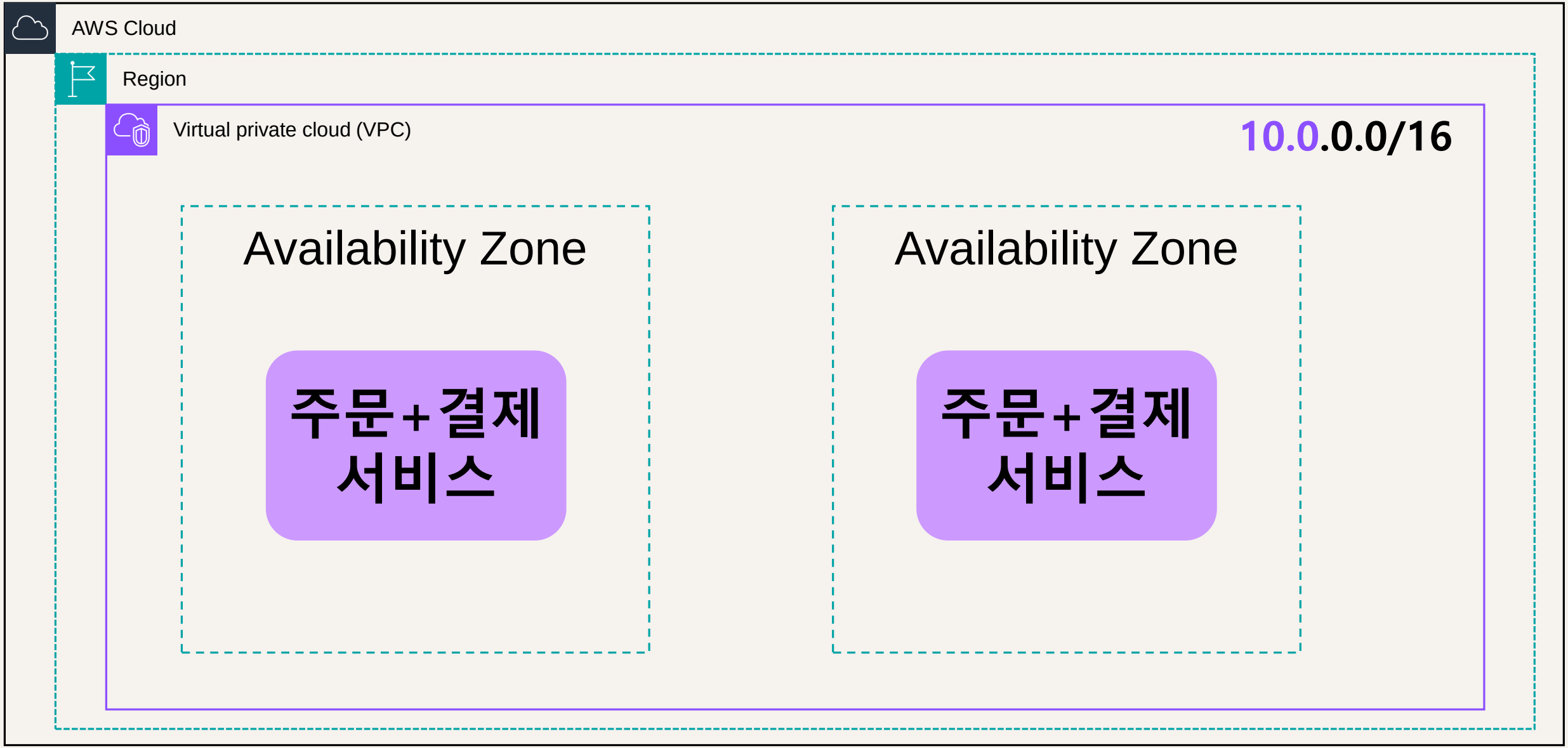
AZ (가용 영역)

- **지역별 물리적으로 존재하는 데이터 센터**
- **단일 데이터 센터를 사용하는 것보다 가용성, 확장성 등에서 유용함.**

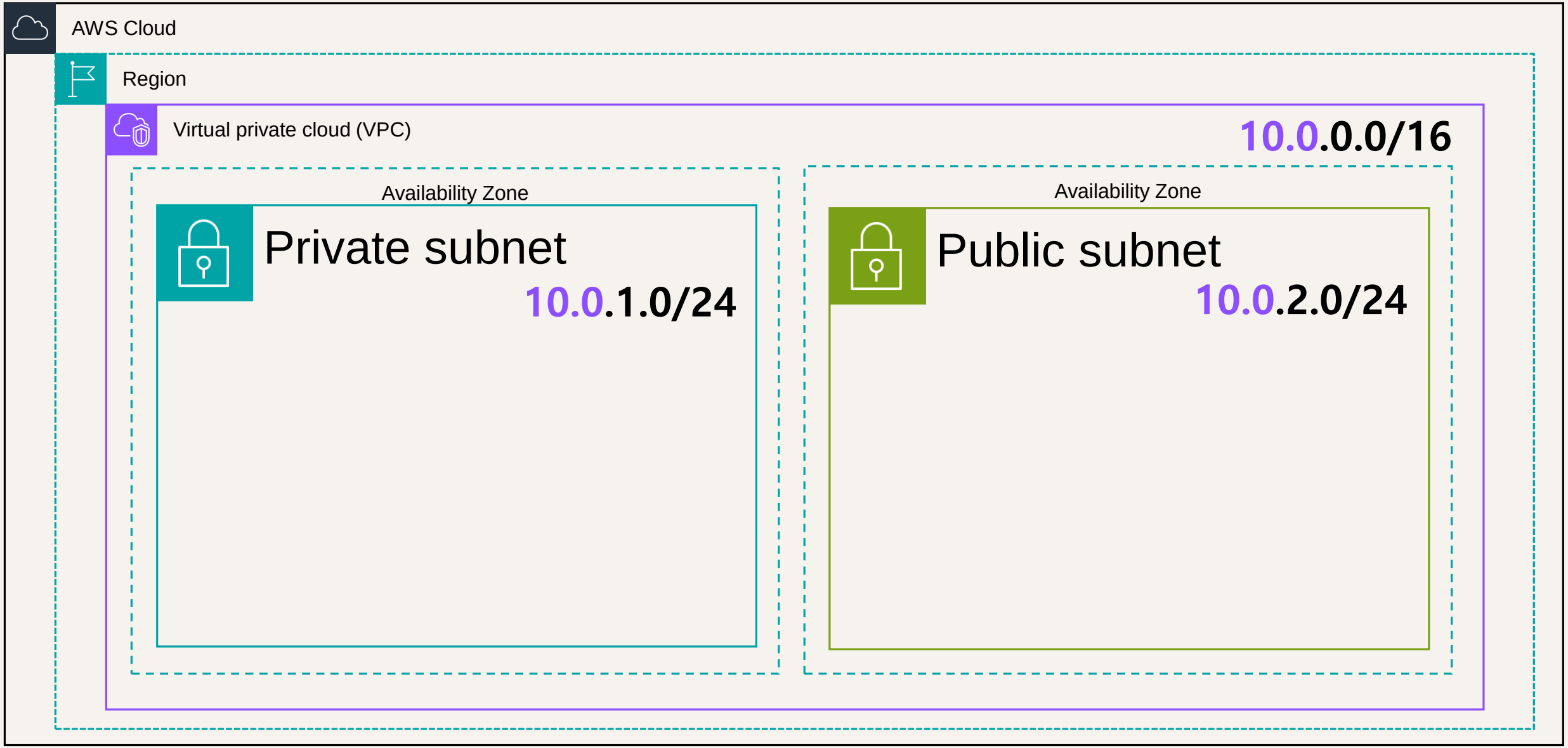
AZ (가용 영역)


AWS Cloud
Region
Virtual private cloud (VPC)
10.0.0.0/16
Availability Zone
주문
서비스
Availability Zone
결제
서비스

AZ (가용 영역)


AWS Cloud
Region
Virtual private cloud (VPC)
10.0.0.0/16
Availability Zone
주문+결제 서비스
Availability Zone
주문+결제 서비스

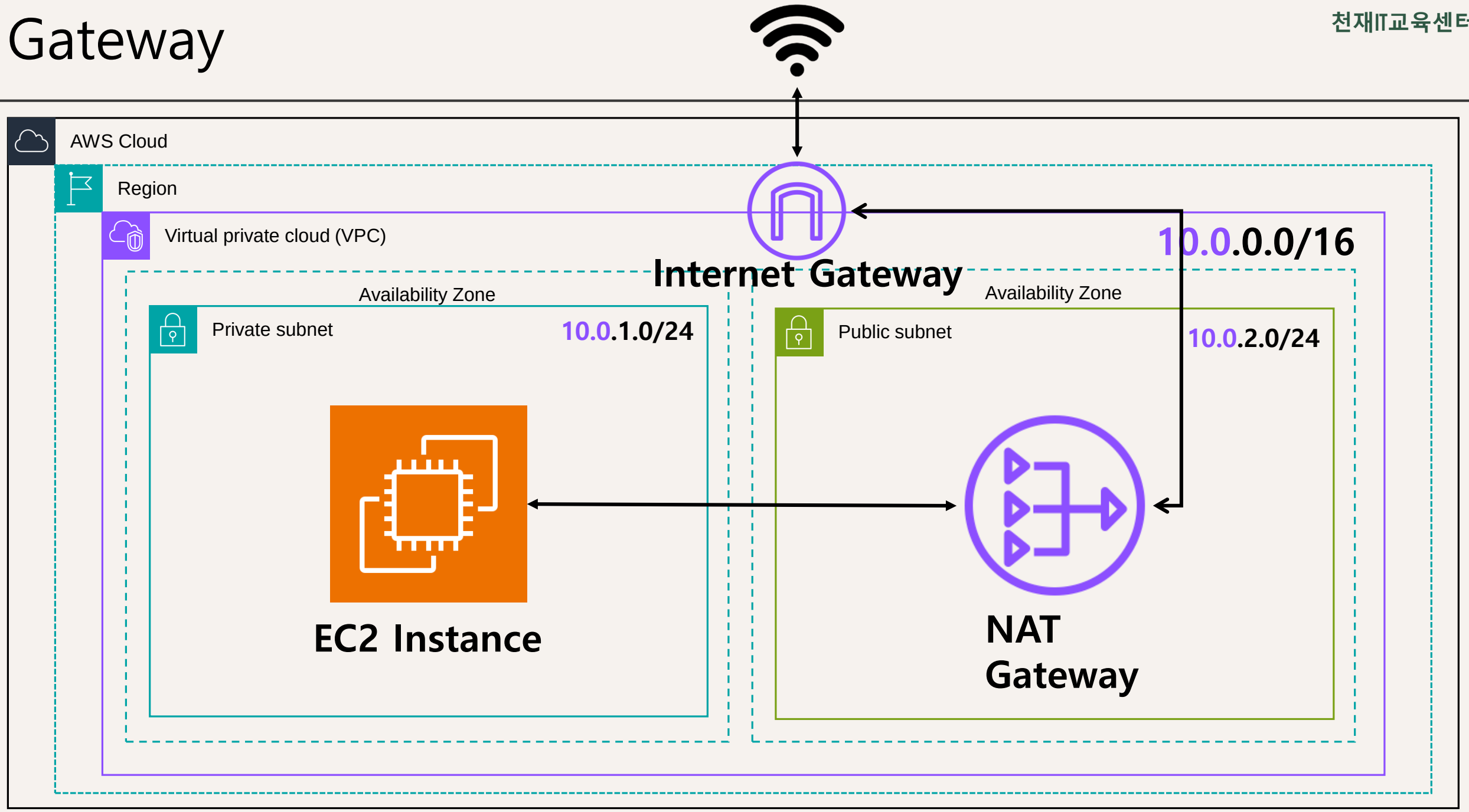
Subnet


AWS Cloud
Region
Virtual private cloud (VPC)
10.0.0.0/16
Availability Zone
Private subnet
10.0.1.0/24
Availability Zone
Public subnet
10.0.2.0/24

Subnet : Private / Public

- 네트워크 분할 기술 (네트워크 안의 네트워크)
- AZ과 서브넷은 1:N 관계
- CIDR 기법을 사용하여 네트워크 범위 관리
- 외부 통신 : Public Subnet
- 내부 통신 : Private Subnet

Gateway

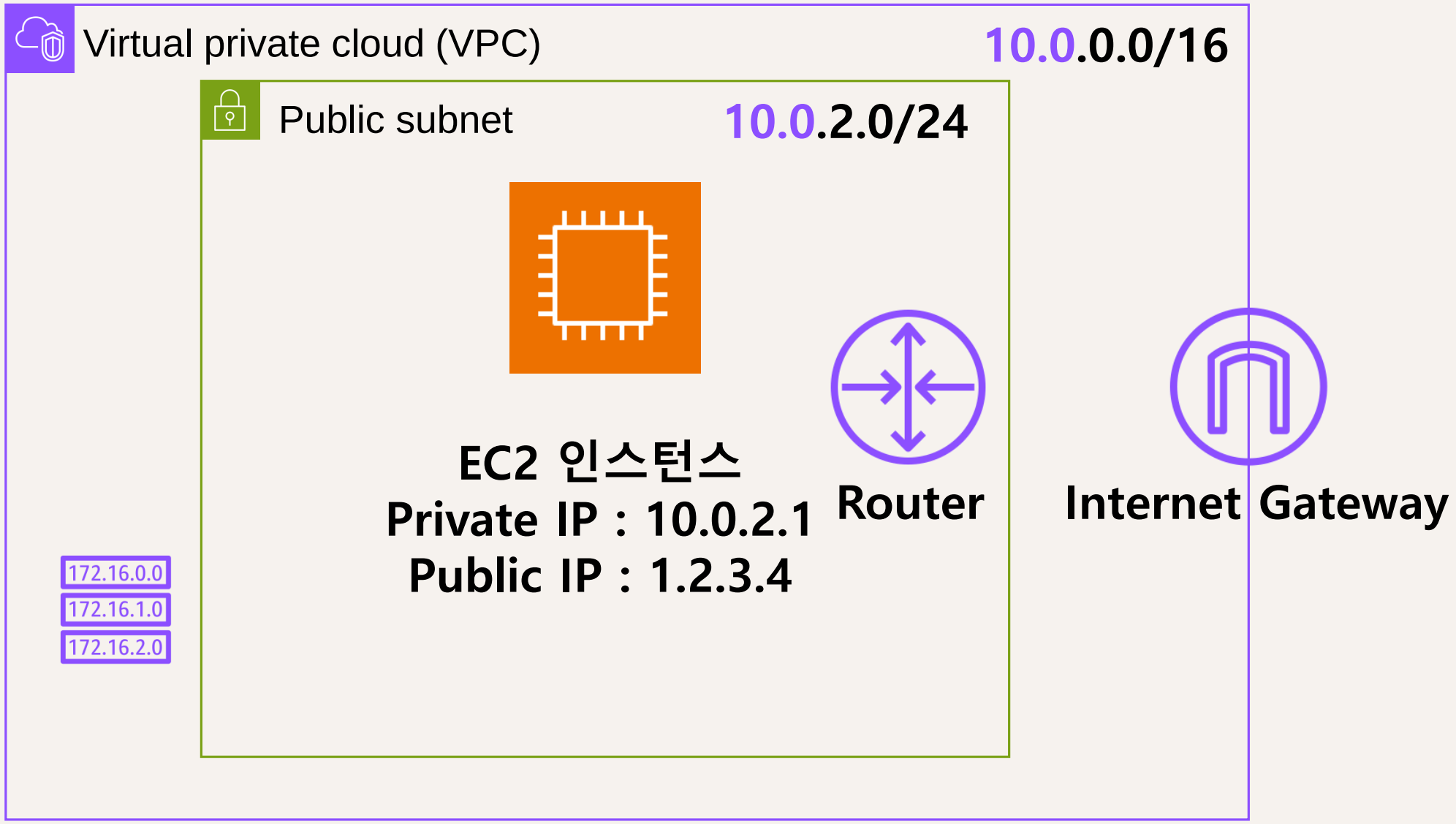

AWS Cloud
Region
Virtual private cloud (VPC)
10.0.0.0/16
Internet Gateway
Availability Zone
Private subnet
10.0.1.0/24
EC2 Instance
Availability Zone
Public subnet
10.0.2.0/24
NAT Gateway

Gateway

- **NAT Gateway**
  - 사설 IP를 공용 IP 주소로 변환
  - Private Subnet 인스턴스가 인터넷 통신하기 위해 제공되는 AWS 관리형 서비스

- **Internet Gateway**
  - VPC와 인터넷 사이에 통신을 가능하게 하는 VPC 요소

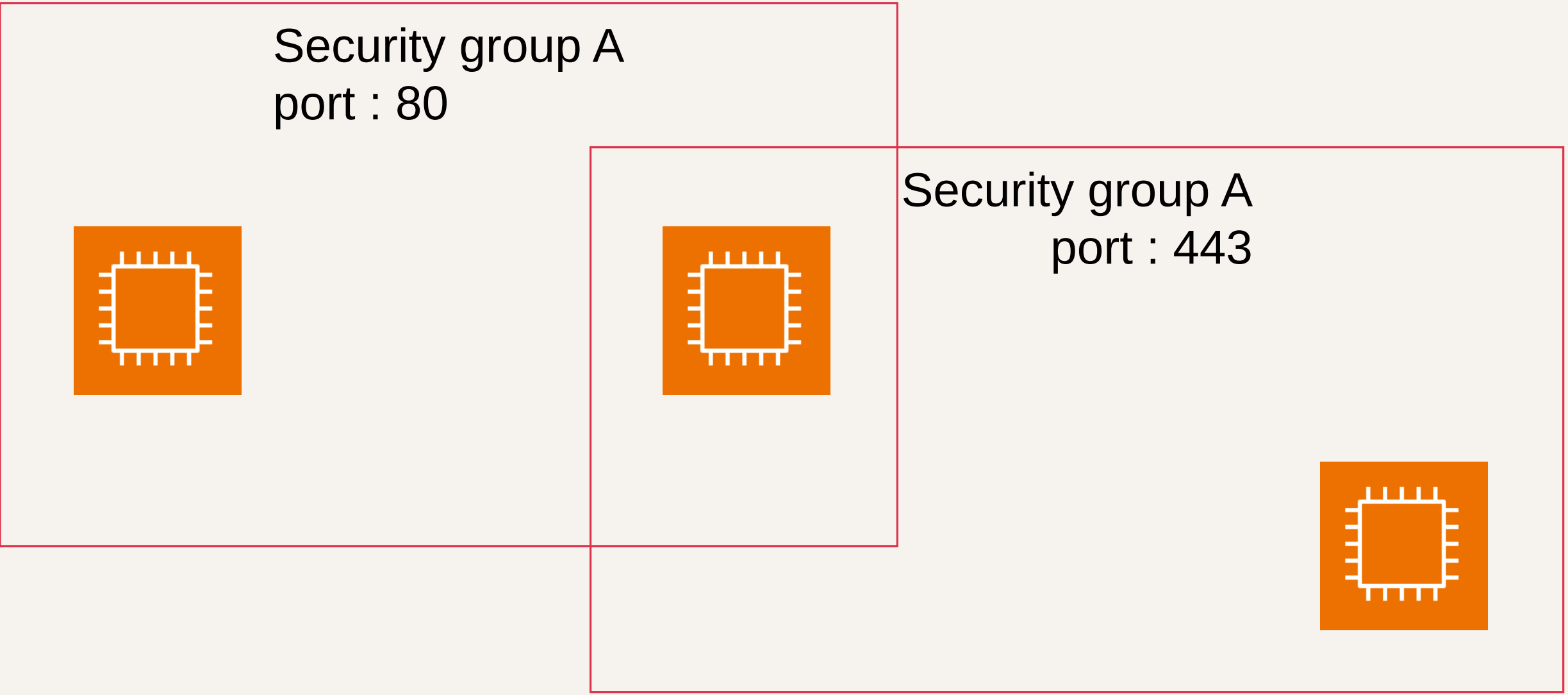
Public IP


Virtual private cloud (VPC)
10.0.0.0/16
Public subnet
10.0.2.0/24
EC2 인스턴스
Private IP : 10.0.2.1
Public IP : 1.2.3.4
Router
Internet Gateway
172.16.0.0
172.16.1.0
172.16.2.0

보안 그룹(Security Group : SG)

- **인스턴스 단위 방화벽**
- **인바운드 / 아웃바운드 접근 제어 (Port)**
- **상태 저장 O**
- **Allow만 설정 가능 (Default : Deny)**

보안 그룹(Security Group : SG)



NACL(Network Access Control List)

- **서브넷 단위 방화벽**
- **상태 저장 X**
- **Allow / Deny 설정 가능**
- **우선 순위 지정 가능**

Summary

VPC	AWS 계정 전용 가상 네트워크
리전	AWS 컴퓨팅 서비스가 호스팅 되는 위치
가용 영역(AZ)	리전 내에 하나 이상의 데이터 센터
서브넷	네트워크 분할 기술 (네트워크 안의 네트워크) 프라이빗 / 퍼블릿

Summary

NAT Gateway	프라이빗 서브넷의 인스턴스가 인터넷과 통신되기 위한 서비스 (사설IP -> 공용IP)
Internet Gateway	VPC와 인터넷 사이에 통신을 가능하게 하는 VPC요소
보안 그룹	인스턴스 단위 방화벽 인/아웃 바운드 접근 제어(Port)
NACL	서브넷 단위 방화벽 잇/아웃 바운드 접근 제어(Port)

감사합니다.

Thank You