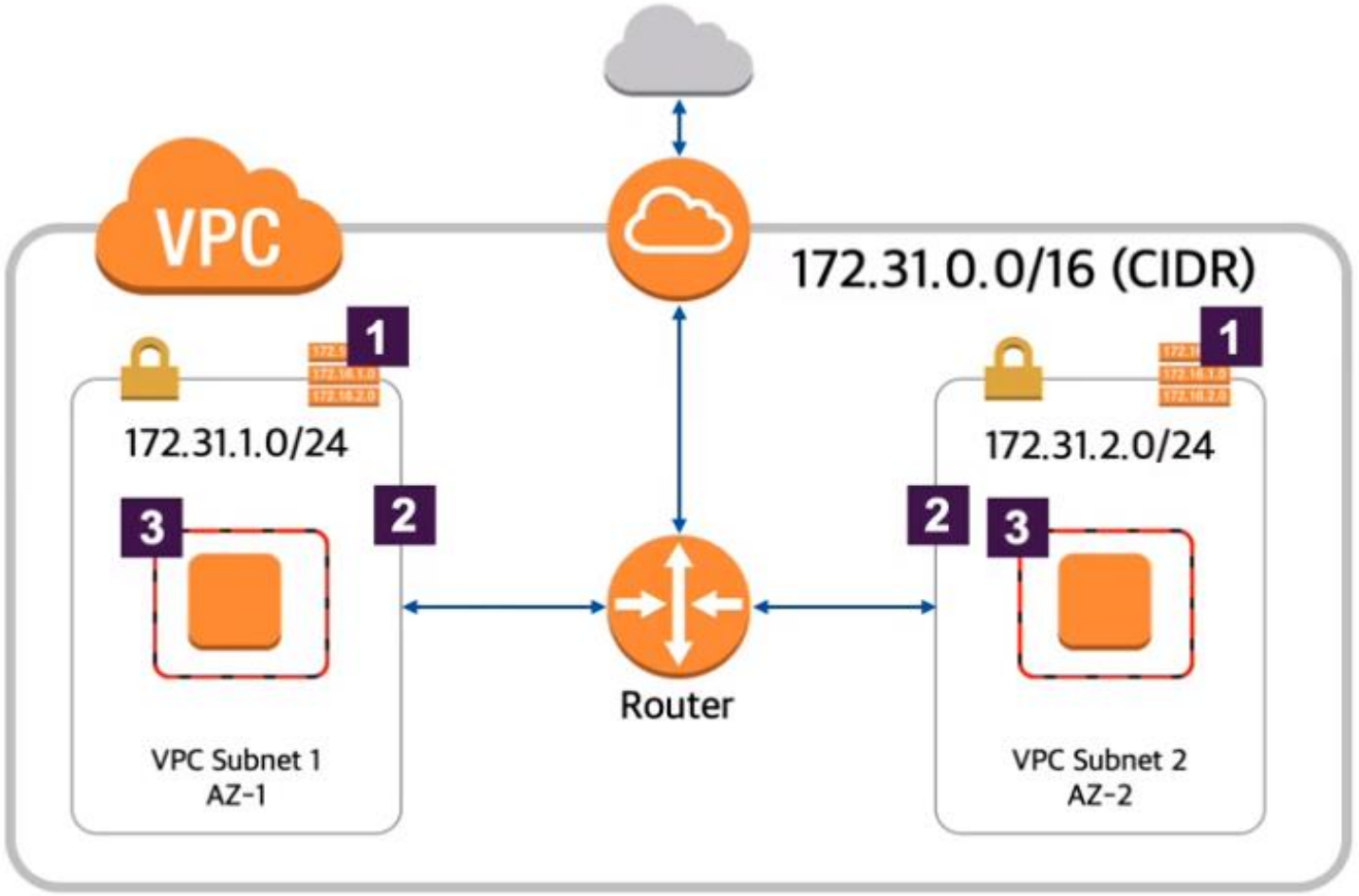
AWS Fundamentals

7.AWS VPC (Virtual Private Cloud)-Part1

학습 목표

AWS의 네트워크서비스인 VPC에 대해 알아봅니다.

VPC 만들기 :네트워크 트래픽 통제



1 Route Table

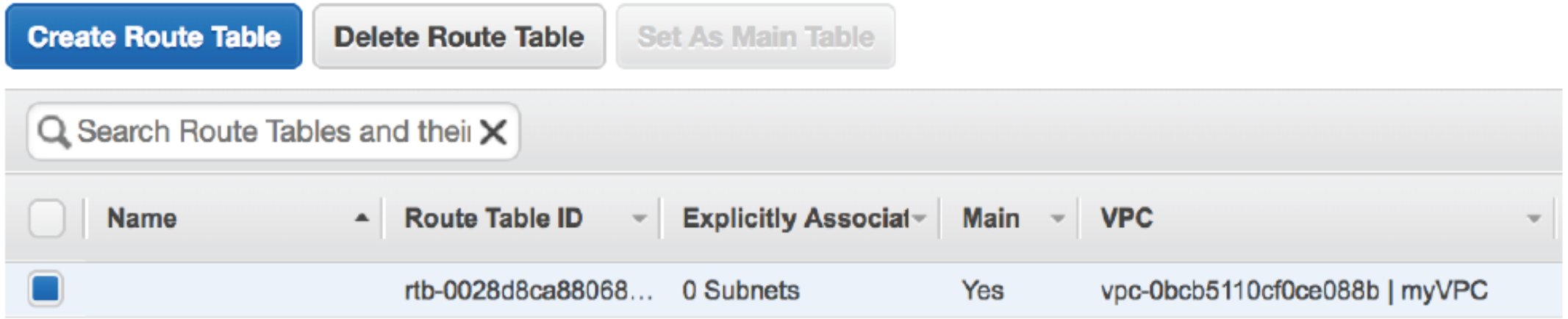
- Subnet 단위 라우팅 통제

2 Network ACL

- Subnet 단위
- Stateless 방화벽
- Allow/Deny
- Rule # ordering

3 Security Group

- 인스턴스 단위
- Stateful 방화벽
- Allow only



rtb-0028d8ca88068723d

Summary | **Routes** | Subnet A | Tags

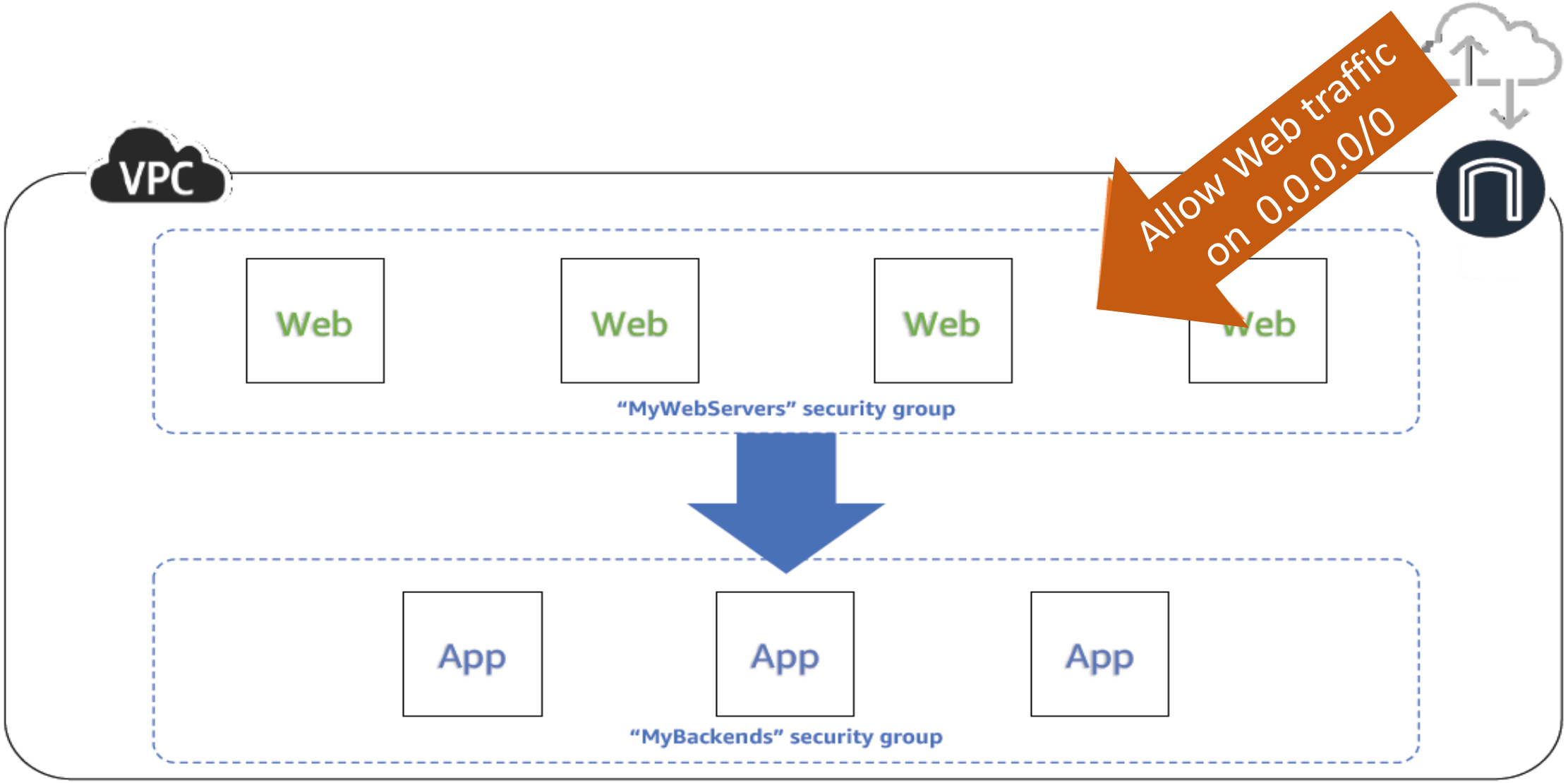
VPC내에서 송/수신되는
트래픽은 VPC내에서 라우팅

Edit

View: All rules

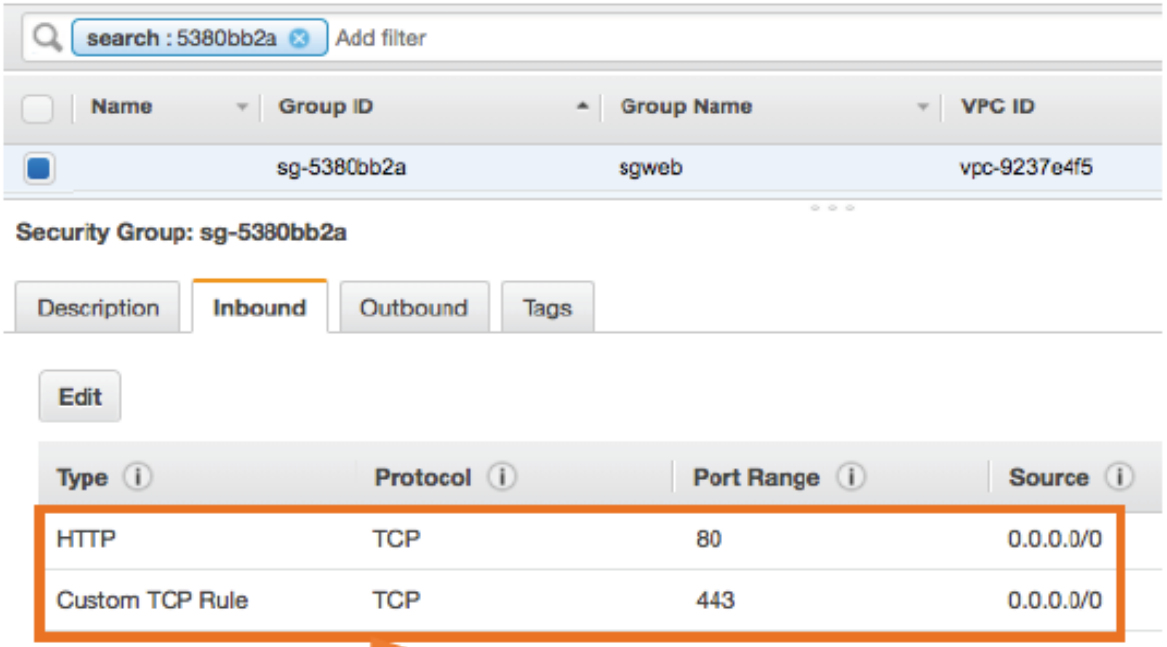
Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
2600:1f16:14d:6300::/56	local	Active	No

VPC 만들기 : 네트워크 트래픽 통제 (Security Group)



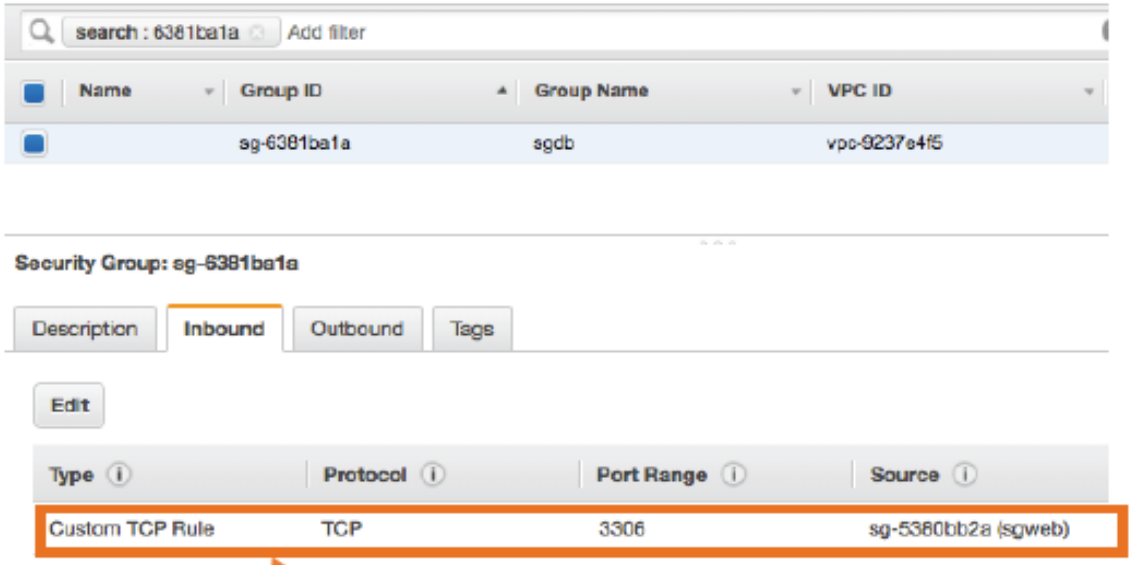
VPC 만들기 : 네트워크 트래픽 통제 (Security Group)

Security Group **for Web Servers**



인터넷 구간으로부터 HTTP, HTTPS Connection 허용

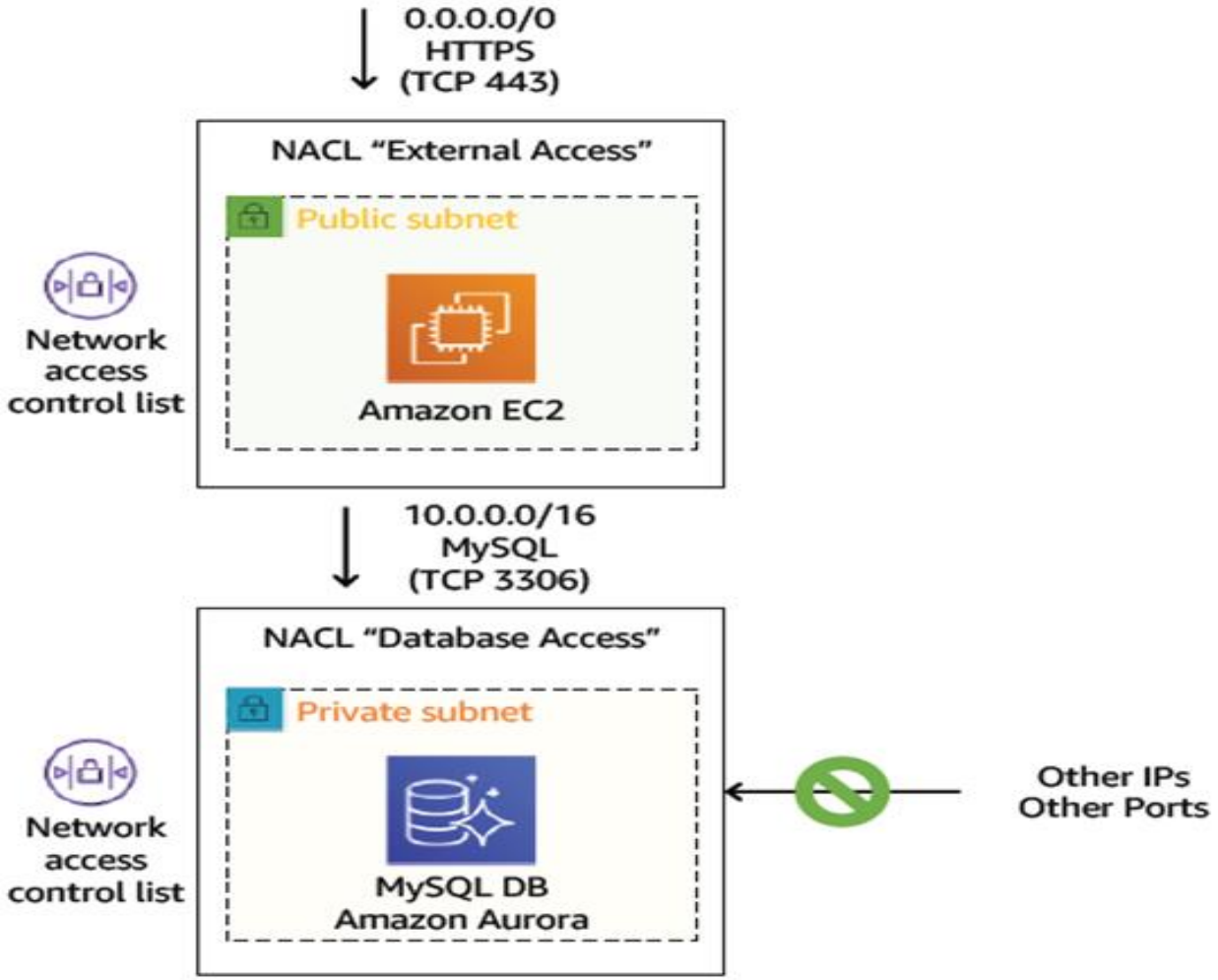
Security Group **for DB Servers**



웹서버 Security Group으로부터 3306 Port Connection 허용

VPC 만들기 : 네트워크 트래픽 통제 (Network ACL)

- 인바운드 및 아웃 바운드
- 서브넷 레벨 검사
- 선택적 보안 수준
- 기본적으로 모든 트래픽을 허용
- stateless
- IP 및 TCP / UDP 포트 기반
- 허용 및 거부 규칙 지원
- 마지막에 모두 거부



VPC 만들기 : 네트워크 트래픽 통제

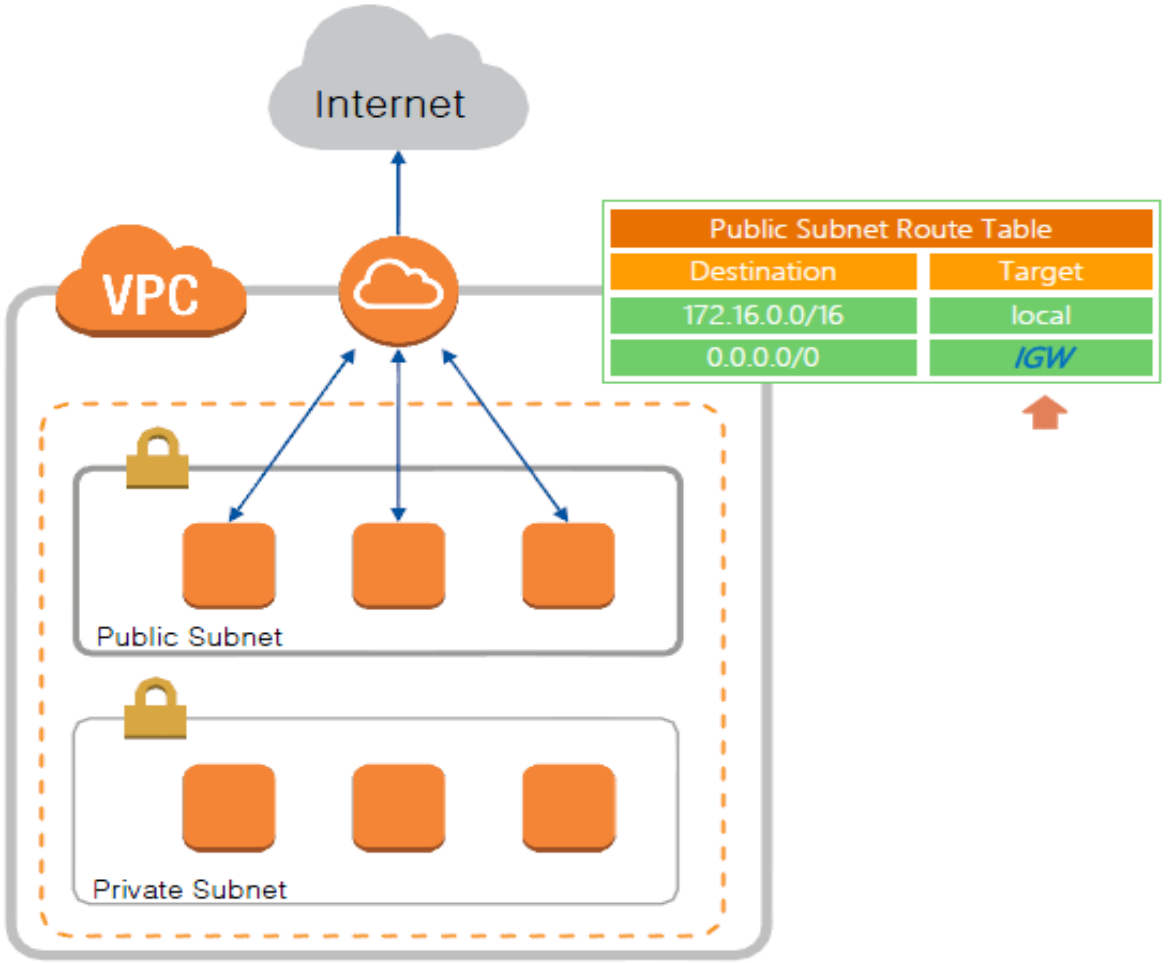
- Security Group vs Network ACL

Security Group	Network ACL
인스턴스 단위 인스턴스에 개별 적용	서브넷 단위 서브넷 내 인스턴스에 자동 적용
allow 규칙 만	allow / deny 규칙
stateful : return 트래픽 자동 허용	stateless : return 트래픽에 대해 allow 규칙 설정 필요
모든 규칙을 확인 후 판단	순서대로 규칙을 확인 allow/deny 규칙 만족 시 중단

VPC 확장: Internet

VPC Internet Gateway

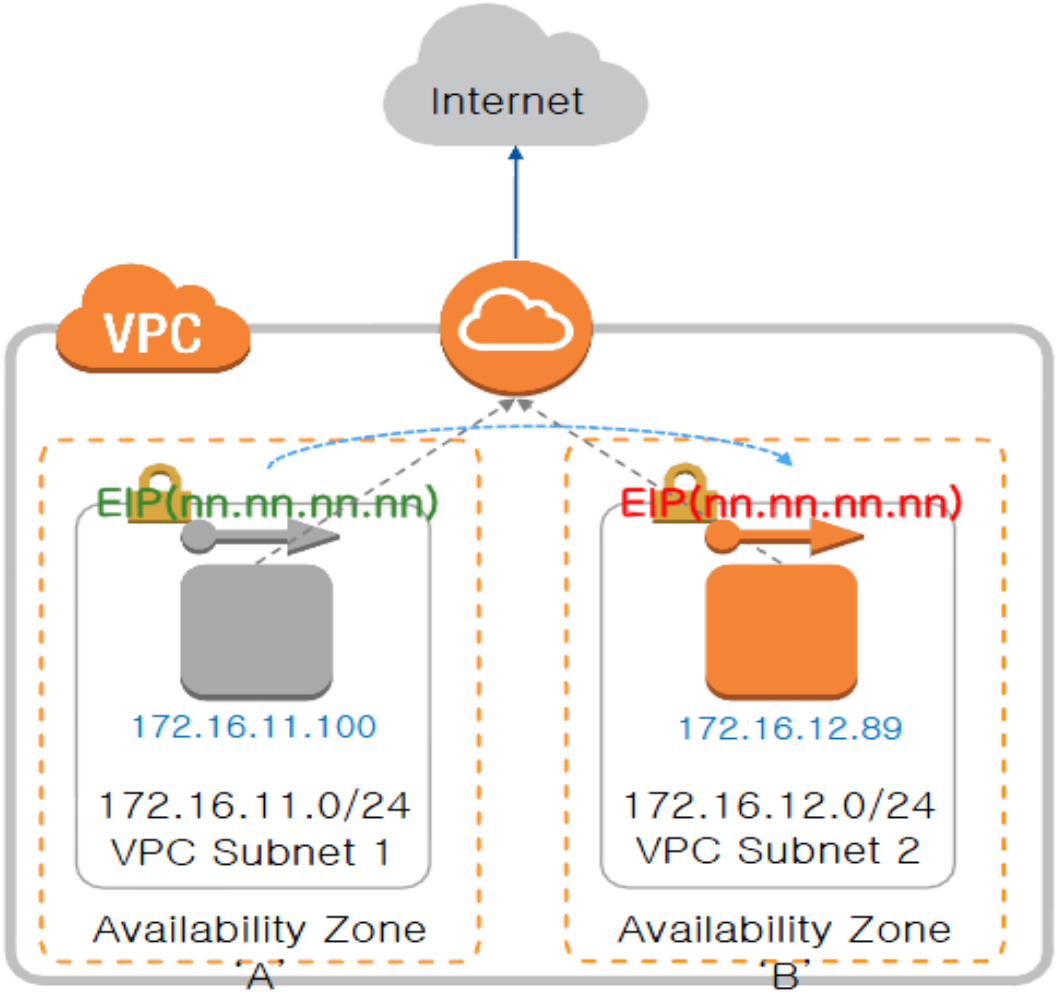
- Managed Service
  - 확장성, 가용성, 중복성 보장 설계
- VPC 당 Attach 가능한 Internet Gateway : 1개
- VPC 인스턴스와 인터넷 간의 통신
- 1:1 NAT
  - 인터넷 구간과 연결하려는 EC2 인스턴스는 Public IP나 EIP(Elastic IP)를 가져야 함
- Public Subnet의 Routing Table 수정
- IPv4, IPv6 지원



VPC 확장: Internet

EIP (Elastic IP)

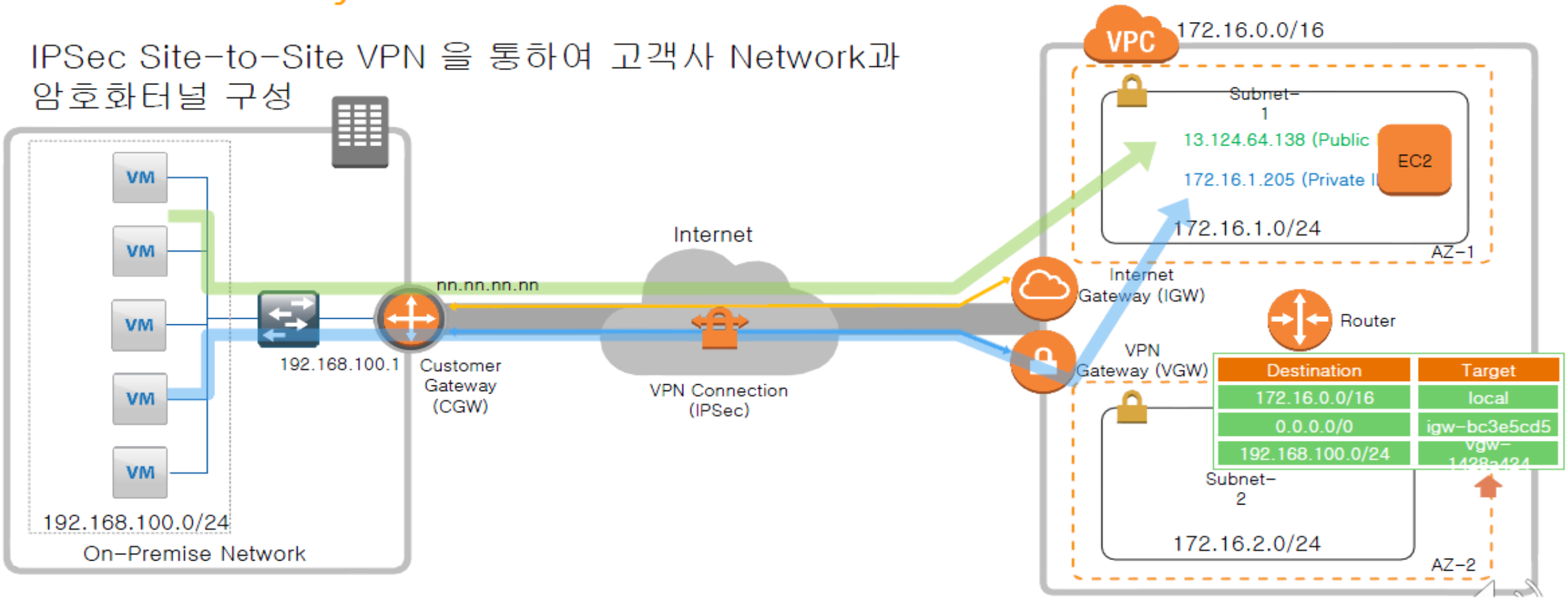
- Account에 할당되어 변경되지 않는 Elastic IP(EIP)를 할당
- EC2 Instance 장애시, 다른 EC2 Instance로 EIP를 Re-Associate
- Region당 기본 5개의 Elastic IP Address 할당 가능(Soft-Limit)
- Allocation / Release
  - Account에 EIP 할당 또는 반납
- Associate / Disassociate
  - EC2/NAT GW Instance에 EIP 연결 또는 분리



VPC 확장:On-Premise

VPN Gateway

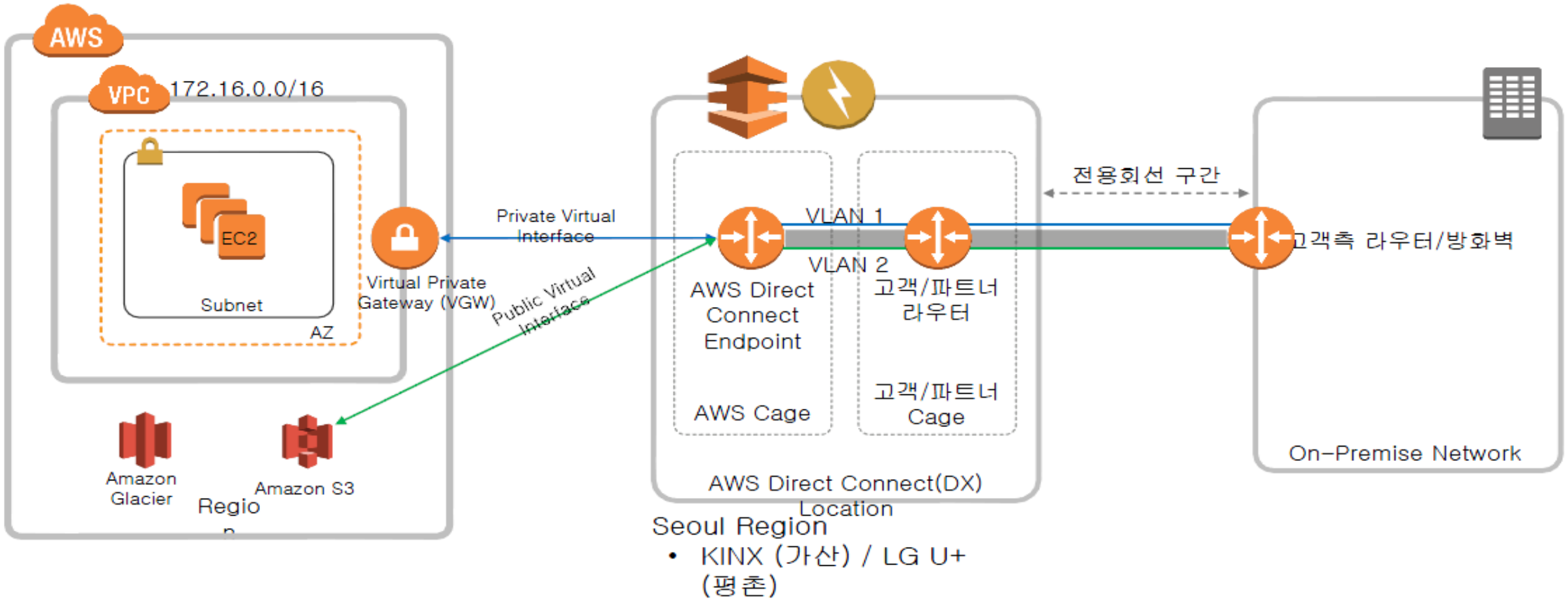
IPSec Site-to-Site VPN 을 통하여 고객사 Network과 암호화터널 구성



VPC 확장:On-Premise

AWS Direct Connect

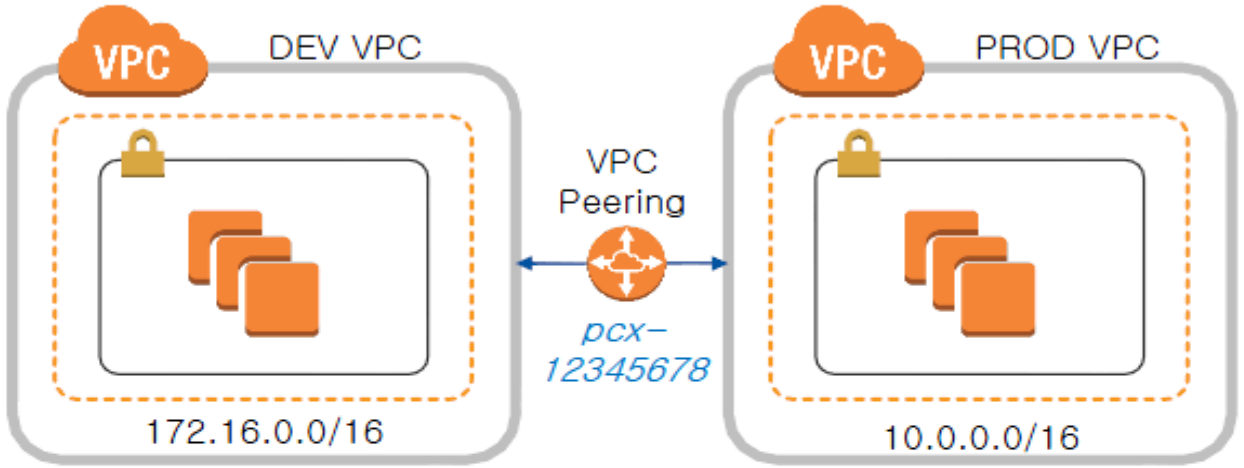
전용회선을 통하여 고객사와 직접 연결



VPC 확장:Other AWS Regions

VPC Peering

- 동일 Region내 VPC간 완전히 격리된 전용의 연결 (동일 Account및 다른 사용자 Account간)
- VPC간 하나의 VPC Peering만 제공되며, VPC간 IP Address가 중복 될 수 없음
- 고가용성 및 Traffic에 대한 수평적 확장 제공
- Routing Table을 통하여 통제가 가능하고, Transit Routing은 제공되지 않음
- 구성 사례 : 인증, 디렉터리 서비스, 모니터링, 로깅, 공통 서비스
- 전송 중 암호화 (Inter Region VPC)



Route Table	
Destination	Target
172.16.0.0/16	local
0.0.0.0/0	IGW
10.0.0.0/16	VPC Peer

Route Table	
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	IGW
172.16.0.0/16	VPC Peer

강의 요약

- 이 강의에서는 지난 시간에 이어 VPC 확장 기술인 내부게이트웨이,Elastic IP,VPC게이트웨이,다이렉트 연결,Peering 에 대해 학습하였습니다.