

## \* VPC Router

- Cisco Router 와는 다른 개념의 존재로 접근할 수 없으며, 설정할 수 없음
- Router 는 AZ 에 걸쳐 있기 때문에 Single point of hardware 가 존재하지 않음
- VPC 는 기본적으로 Main route table 을 보유하고 있으며 Table 내 Local route 를 탑재하고 있음
- Local route : VPC 내 Subnet 들에 한해 VPC 내 모든 대역을 목적지로 하는 Local routing 이 있어 별도의 Routing 없이 통신 가능
- 하나의 Subnet 에만 해당하는 Route table 을 만들기 위해서는 Custom route table 을 만들어 해당 Subnet 만 적용하면 됨
  - Custom route table 또한 Local route 를 보유함
- Custom route table 을 갖는 Subnet 이 외부 인터넷과 통신하기 위해서는 Internet Gateway(IGW)를 생성한 이후 Custom route table 에 외부 인터넷에 대한 Route 를 추가해야 함
  - 목적지를 0.0.0.0/0 로 잡고 next hop 을 IGW 로 잡는 Default routing 설정 또한 필요
  - Subnet 내 서비스들도 Public IP 를 보유해야 함
- IGW 뿐만 아니라 NAT Gateway, VPC Peering, Egress Only Internet Gateway, Network Interface, Instance(NAT Instance) 등을 Next hop 으로 지정 가능

## \* Reserved Addresses in AWS VPC

- 각 Subnet 마다 예약되어있는 첫 4 개의 IP
- 가장 높은 주소가 예약되어있음
- 예를 들어 10.0.1.0/24 일 경우
  - 10.0.1.0 : Network ID
  - 10.0.1.1 : VPC Router 용 주소, 즉 Default Gateway IP
  - 10.0.1.2 : DNS Server IP, Subnet 에 있는 Instance 의 DNS 기능을

## 활성화시킴

- 10.0.1.3 : 미래에 사용할 목적인 예약 주소
- 10.0.1.255 : Broadcast 주소, VPC 는 Broadcast 를 지원하지 않으므로

## 예약됨

- 위 IP 는 수정하거나 사용할 수 없음

## \* Dual-Homed Instances in AWS VPC

- 같은 AZ 에 소속된 Subnet 에 한해서 하나의 EC2 가 다수의 Subnet 에 Interface 를 두는 것이 가능
- 2 개의 Subnet 에 Network interface 를 둔 Instance 를 말하며, 2 개의 Subnet 은 AZ 는 같으나 다른 Network 임

- 2 개의 Subnet 은 서로에 대한 Routing table 이 존재하지 않으며, 통신도 불가능
- Public subnet 에 Interface 를 하나 두고, Private subnet 에 Interface 를 하나 둔 뒤 Server 가 Web Service 를 제공하고 Private subnet 에서 VPN 을 통해 On-premise 로 연결하는 것도 가능

\* Internet gateway(IGW)

- 외부 인터넷과 통신하기 위한 Gateway
- EC2 가 Public IP 를 가지고 있더라도 Internet gateway 가 없다면 외부 인터넷 통신이 불가능
- IGW 의 관리는 AWS 가 맡음
- Routing table 에 0.0.0.0/0(Destination)에 대하여 IGW 를 추가해야 함
- 10.0.1.23 IP 를 가진 EC2 가 외부 인터넷 통신을 할 경우, IGW 를 지날 때 자신이 가진 Public IP 로 Source NAT(Network Address Translation)되어 외부로 나아감
  - 이동 과정 : Source 10.0.1.23(Public IP 59.54.23.52) / Destination 8.8.8.8 == > IGW == > Source 59.54.23.52 / Destination 8.8.8.8
- 10.0.1.23 IP 를 가진 Ec2 로 외부 인터넷에서 접속시, IGW 를 지날 때 EC2 가 갖고 있는 Public IP 가 Private IP 로 Destination NAT(Network Address Translation)되어 내부로 들어옴
  - 이동 과정 : Source 8.8.8.8 / Destination 59.54.23.52 == > IGW == > Source 8.8.8.8 / Destination 10.0.1.23

\* VPC 요약

- VPC 에서 이미 생성한 IP 대역 크기를 재조절할 수 없음
- Multiple CIDR 로 이루어진 같은 VPC 를 생성할 수 없음. 10.0.0.0/16 이 이미 있을 때, 10.0.1.0/24 대역을 만들 수 없음
- VPC 에서 추가로 IPv4 대역(Secondary CIDR)를 생성할 수 있음
- IPv6 대역은 1개만 추가로 생성 가능하며 대역은 자동으로 정해짐