* VPC란?
- Virtual Private Cloud
- AWS의 계정 전용 가상 네트워크 서비스
- VPC 내에서 각종 리소스(EC2, RDS, ELB 등)을 시작할 수 있으며 다른 가상 네트워크와 논리적으로 분리되어 있음
- S3, Cloudfront 등은 비VPC 서비스(글로벌 서비스)로 VPC 내에서 생성되지 않음
- 각 Region별로 VPC가 다수 존재할 수 있음
- VPC는 하나의 사설 IP 대역을 보유하고, 서브넷을 생성하며 사설 IP 대역 일부를 서브넷에 할당할 수 있음
- 허용된 IP 블록 크기는 /16(IP 65536개) ~ /28(IP 16개)
- 권고하는 VPC CIDR 블록(사설 IP 대역과 동일함)
    - 10.0.0.0 ~ 10.255.255.255(10.0.0.0/8)
    - 172.16.0.0 ~ 172.31.255.255(172.16.0.0/12)
    - 192.168.0.0 ~ 192.168.255.255.(192.168.0.0/16)

* Subnet
- VPC 내 생성된 분리된 네트워크로 하나의 서브넷은 하나의 AZ(Availability Zone)에 연결됨
- VPC가 가지고 있는 사설 IP 범위 내에서 '서브넷'을 쪼개어 사용가능
- 실질적으로 리소스들은 이 서브넷에서 생성이 되며 사설 IP를 기본적으로 할당받고 필요에 따라 공인 IP를 할당받음
- 하나의 서브넷은 하나의 라우팅 테이블과 하나의 NACL(Network ACL)을 가짐
- 서브넷에서 생성되는 리소스에 공인 IP 자동할당 여부를 설정할 수 있음
- Public Subnet과 Private Subnet 등을 만들어 커스터마이징 가능
- 서브넷 트래픽이 인터넷 게이트웨이(차후 설명)로 라우팅 되는 경우 해당 서브넷을 Public Subnet, 그렇지 않은 서브넷의 경우 Private Subnet이라 함
- 각 서브넷의 CIDR 블록에서 4개의 IP 주소와 마지막 IP 주소는 예약 주소로 사용자가 사용할 수 없음, 예를 들어 서브넷 주소가 172.16.1.0/24일 경우
    - 172.16.1.0 : 네트워크 주소(Network ID)
    - 172.16.1.1 : VPC Router용 예약 주소(Gateway)
    - 172.16.1.2 : DNS 서버의 IP 주소
    - 172.16.1.3 : 향후 사용할 예약 주소
    - 172.16.1.255 : 네트워크 브로드캐스트 주소(VPC는 브로드캐스트를 지원하지 않음)

* ENI(Elastic Network Interface)
- 가상 네트워크 인터페이스
- VPC 내 리소스들은 ENI와 사설 IP를 기본적으로 할당받음
- 선택적으로 공인 IP도 할당 가능
- Public Subnet의 경우, 리소스 생성시 자동으로 공인 IP를 할당함
- 사설 IP 주소는 추가로 할당 가능하며 공인 IP 역시 나중에 할당 가능

* Routing Table
- 서브넷 내의 트래픽이 전송되는 위치를 결정하는 라우팅의 규칙 집합
- 라우팅 테이블은 기본적으로 VPC의 범위에 해당하는 범위를 기본 라우팅으로 가지며(ex. 172.16.1.0/24) 이를 'Local'로 표시함
- Internet Gateway, NAT Gateway, VPC Endpoint, Peering 등을 설정하고 그 서비스로 트래픽을 보내도록 라우팅 설정할 수 있음
- '0.0.0.0/0'은 Default Routing을 뜻함, 트래픽이 가고자 하는 목적지가 라우팅 테이블에 존재하지 않을때 사용하는 라우팅으로 보통 Internet Gateway나 NAT Gateway로 외부 인터넷을 지정할 때 씀
- 하나의 서브넷은 하나의 라우팅 테이블만 가지지만, 하나의 라우팅 테이블은 다수의 서브넷을 가질 수 있음
- Public Subnet의 라우팅 테이블에는 인터넷 게이트웨이로의 라우팅이 있으며, Private Subnet에서 외부 인터넷 통신이 필요할 경우 NAT Gateway로의 라우팅을 설정해야 함

* Internet Gateway
- VPC 내 리소스가 외부 인터넷을 사용하고자 할 때 사용하는 게이트웨이
- 인터넷 게이트웨이가 없으면 외부 인터넷을 사용할 수 없음
- 인터넷 게이트웨이를 생성한 후, '0.0.0.0/0'에 대하여 라우팅 테이블을 인터넷 게이트웨이로 잡아주면 사용 가능
- 인터넷 게이트웨이가 있다 하더라도, VPC 내 리소스가 공인 IP를 가지고 있지 않다면 인터넷 사용 불가능
- 위의 설정을 모두 했음에도 인터넷이 제대로 되지 않는다면, 보안그룹과 Network ACL을 확인해야 함

* Egress-only Internet Gateway
- IPv6를 보유한 VPC 내 인스턴스가 외부 인터넷으로 "아웃바운드" 통신을 가능케 하는 기능
- 아웃바운드 통신만 가능함
- Network ACL을 통해 제어할 수 있음

* NAT Gateway
- 외부에서의 접촉이 원천적으로 차단되어 있는 Private Subnet에서 인터넷 접속을 통해야 할 경우 사용하는 게이트웨이
- VPC 내부 리소스가 NAT Gateway를 통해 인터넷을 접속할 수 있지만, 외부에서 NAT Gateway를 통해 VPC 내부로 들어올 수 없음
- 인터넷이 연결된 Public sunbet에 NAT Gateway를 생성한 후, Private Subnet의 라우팅 테이블에 '0.0.0.0/0'에 대하여 라우팅을 NAT Gateway로 잡아주면 사용 가능
- CloudWatch를 이용하여 모니터링 가능

* NAT Instance(추천하지 않음)
- Public Subnet에 생성된 NAT Gateway 대신 EC2 인스턴스를 사용하는 방법
- Public Subnet에 공인 IP를 가진 특수한 인스턴스를 게이트웨이로 삼고, Private Subnet의 라우팅 테이블에 '0.0.0.0/0'에 대하여 NAT Instance로 설정한 후, SrcDestCheck 속성을 비활성화해야 함
- 커뮤니티 AMI에 있는 'ami-vpc-nat'로 시작하는 인스턴스로 사용 가능
- 인스턴스이기 때문에 후술할 보안그룹의 설정을 적용 받으므로 트래픽을 제어할 수 있음

* NAT Instance vs NAT Gateway
- NAT Gateway는 AWS에서 관리하기 때문에 유지보수할 필요가 없으나 NAT Instance는 사용자가 직접 관리해야 함
- NAT Instance는 인스턴스이기 때문에 장애가 발생할 가능성이 있어 스크립트로 인스턴스간 Failover를 신경써야 함
- NAT Gateway는 대역폭을 최대 45Gbps까지 확장할 수 있지만, NAT Instance는 인스턴스 유형에 따라 다름
- NAT Gateway는 보안그룹을 사용할 수 없지만, NAT Instance는 보안그룹을 사용할 수 있음
- NAT Gateway와 NAT Instance 모두 NACL을 통해 트래픽 제어 가능