* Network Address Translation Instance(NAT Instance)
- NAT 기능을 수행하는 EC2 로 Public subnet 에 소속되어 Public IP 를 보유함
- Private subnet 의 Route table Default gateway(0.0.0.0/0)를 NAT Instance 로 설정해야 함
- Source / Destination check 를 해제해야 함
- Traffic Flow
    1. Private subnet 의 EC2 가 외부 인터넷 통신을 시도하면 Default gateway 로 가기 위해 VPC Router 로 향함
    2. Public subnet 내 NAT Instance 로 이동함
    3. NAT Instance 에서 Source IP NAT 가 발생하여 Private subnet 의 EC2 Source IP 는 NAT Instance 의 Public IP 가 됨
    4. NAT Instance 의 Public IP 를 달고 외부 인터넷으로 나아감
- Internet Gateway 와 NAT Instance 가 있는 Public subnet 이 장애가 발생할 경우 외부 인터넷 접속이 어려워짐
    - 고가용성이 필요함
- 사용량에 따라 EC2 유형을 바꾸어야 함

* Network Address Translation Gatweay
- NAT 를 사용하기 위한 EC2 가 아닌 별도의 서비스인 NAT Gateway 사용
- EC2 를 만든다는 점을 제외하면 사용방법은 NAT Instance 와 동일

* NAT Instance 대비 NAT Gateway 의 장점
- NAT Gateway 는 EC2 가 필요하지 않음
- NAT Gateway 는 AZ 내 중복적으로 구현되기 때문에 가용성이 높음(사용자 입장에서는 하나이지만 AZ 내부에는 다수가 구현됨)
- NAT Gateway 는 별도의 Scaling 없이 최대 45 Gbps 까지 대역폭을 자동확장함
- NAT Gateway 는 관리, 패치, 크기 재조정을 AWS 가 맡아서 처리함

* NAT Gateway 의 단점
- NAT Instance 를 Bastion host 로 사용할 수 있는 것과 달리 NAT Gateway 는 불가능
- Port Forwarding 과 같은 임의 설정 불가능(필요시 NAT Instance 를 써야 함)
- Security group 적용 불가능
- NAT Gateway 는 시간당 요금이 존재하며, 1GB data 전송시 요금을 별도로 부과함. 또한 NAT Gateway 와 EC2 가 다른 AZ 에 있을 경우 데이터 전송요금이 부과됨
    - Private subnet 에 존재하는 EC2 가 외부 인터넷 사용을 위해 Public subnet 의 NAT Gateway 에 접속하여 사용하므로 결국 Data 전송 요금을 별도로 부담해야 함

* NAT Gateway 의 Limit(매우 중요!!!! 문서 확인할 것, https://aws.amazon.com/ko/premiumsupport/knowledge-center/vpc-resolve-port-allocation-errors/)

- 최대 1 개의 Elastic IP 적용 가능
- Security group 을 적용할 수 없는 것과 달리, Network ACL 의 영향은 받음
- Port 는 1024-65535 을 사용함
- 특정 목적지 IP 에 대해 최대 55,000 개의 동시 Connection 을 지원함, 즉 IP 가 달라지면 추가적인 55,000 개의 Connection 을 지원한다는 의미
    - 이로 인해 이 임계값을 초과할 경우 'ErrorPortAllocation' 에러 발생
- NAT Gateway 의 'ErrorPortAllocation' 오류 해결
    - Cloudwatch 에서 'IdleTimeoutCount' 지표 값이 증가하는 것이 보이면 App 또는 Instance 의 유효 연결을 종료하여 새 연결에 포트를 할당함
    - 서브넷을 나누고 다수의 NAT Gateway 를 생성하여 Routing 을 분산시켜 포트 사용량을 줄임
    - 클라이언트가 단일 대상에 설정할 수 있는 연결 수를 제한
    - NAT Gateway 대신 VPC Endpoint 사용