* AWS Hybrid Cloud Computing
- Disaster Recovery : 일반적인 경우 물리적인 Main Site 와 물리적인 DR Site 를 나누어 장애에 대비함
- AWS 를 이용하여 DR Site 를 구성하거나 일시적인 Bursting 이 필요할 경우 AWS Resource 를 추가하여 안정적인 서비스 제공 가능

* AWS Managed Hardware VPN(Site to Site VPN)
- VPC 내 Virtual Private Gateway(VGW)를 생성하고 각 Subnet 에서 Route table 에 VGW 로 Routing 을 전파해야 함
- On-premise 의 Endpint 인 CGW(Customer Gateway, 아래에 설명)에 연결해야 함
- 가용성을 위해 CGW 를 두 개 생성하여 연결하는 것도 가능, 하나의 VGW 에 두 개의 CGW 를 연결하는 것
- 사설 인증서를 사용하여 터널 엔드포인트를 인증할 수 있음
- Hardware VPN 의 장점
    - 설정하기 쉬움
    - 지속적으로 관리해야 할 필요가 없음
    - 다수의 AZ 에서 Dual tunnel 지원
    - Backup 용도로 Direct Connect 설정 가능
    - Idle period 이후에는 터널이 Time out 되기 때문에 Keep alive 설정이 반드시 필요함
    - Direct Connect 처럼 안정적이지 않음
- Pricing
    - Site to Site VPN 연결요금 : 시간당 0.05 USD
    - 데이터 송신 요금 : 처음 1GB 는 무료이며 그 이후로는 GB 당 요금이 부과됨
- 동일한 VGW 에 대해 두 개의 연결을 생성하여 이중화를 구현할 수 있음
    - 동일한 VGW 를 사용하고 새 CGW 를 생성하여 두번째 Site to Site VPN 연결을 설정
    - 두 번째 CGW 는 첫 번쨔 CGW 와 동일한 IP 대역을 사용해야 함

* Software VPN Introduction
- VPC 내 EC2 에 Software VPN 을 설치하여 On-premise 의 Software VPN 와 연결할 수 있음
- Private subnet 의 Routing table 은 EC2 를 향하도록 해야함
- IPSEC 이 아닌 다른 모든 종류의 VPN 중 하나를 생성하면 사용 가능
- Software VPN 을 설치할 EC2 를 관리해야 함
- Traffic Flow 가 Public Internet 을 통해 이동함
- 가용성 요구시 두 개의 Public subnet 에서 두 개의 EC2 를 통해 VPN 터널 생성 필요

* Hybrid Cloud Architecture(https://docs.aws.amazon.com/ko_kr/whitepapers/latest/aws-vpc-connectivity-options/introduction.html)
- VPN
    - 인터넷을 통해 VPC 의 VGW 와 On-premise 의 CGW 를 연결하여 IPSEC Tunnel 을 구성하는 방식
    - On-premise 의 CGW 를 2 개 구성하여 IPSEC VPN 을 중복으로 구성할 수 있음
- Direct Connect
    - Private VIF 를 사용하여 VPC 의 VGW 와 On-premise 의 CGW 를 연결하여 전용선을 구성하는 방식
    - 두 개의 Direct Connect Location 을 사용하여 중복으로 구성할 수 있음
    - Direct Connect Gateway 를 사용하면 다수의 Region 내 VPC 를 연결할 수 있음
- Direct Connect & VPN
    - VPC 를 Private VIF 가 아닌 Public VIF 를 사용하여 연결을 생성하면 VPN 설정이 가능해짐(공인 IP 를 입력하므로)
    - 전용선 서비스에 더해 트래픽 암호화가 가능해짐
- Software VPN
    - AWS VPC 의 Site-to-Site VPN 이 아닌 VPC 내 EC2 에 Software VPN 을 설치한 후 이를 CGW 와 연결하는 방식
- Transit VPC
    - On-premise 와 다수의 VPC 사이에서 중앙 통로 역할을 하는 'Transit VPC'를 생성
    - Transit VPC 에 VPN 솔루션이 설치된 EC2, Cisco 등의 VPN 연결을 생성하여 다수의 VPC 와 On-premise 를 연결함
    - AWS 의 Site-to-Site VPN 연결 최대 갯수는 50 개이므로 50 개 이상의 연결이 필요할 때 대안이 될 수 있음

* AWS Managed Static Hardware VPN Configuration(Site to Site VPN)
- Customer Gateway(CGW) : 고객측(On-premise) VPN Gateway 로 IP 와 라우팅 등을 정의해야 함
- Virtual Private Gateway(VGW) : VPC 측 VPN Gateway, VPC 와 연결해야 함
- 필요한 설정
    - CGW, VGW, Site-to-Site VPN Name
    - Subnet 내 Route Propagation 'Yes' 설정(라우팅 전파)
    - Routing Option 'BGP' 혹은 'Static' 설정(Site-to-Site VPN)
    - IKE Pre-shared Key 공유(Site-to-Site VPN)
    - 터널 IP 설정(AWS 에서 지정한 IP 를 사용해야 함)(Site-to-Site VPN)

* AWS Managed Hadrware Dynamic BGP VPN 설정
- On Premise(192.168.1.0/24, CGW 1(IP 1.2.3.4), CGW 2(IP 5.6.7.8))과 AWS(AZ1(10.1.1.0/24), AZ2(10.1.2.0/24))를 연결하는 경우
- AWS 측에 Customer Gateway, Virtual Private Gateway, Routing 설정
- AWS 에서 지정한 Public ASN(Autonomous System Number) 7224 를 사용하여 Private VIF / VPN 와 CGW 를 연결
    - 7224 를 이미 사용중이라면 Private ASN 64512 를 지정함

* Using Transit VPC to Connect many VPCs
- VPN 과 VPC Peering, Direct connect 는 일대일 연결이므로 다수의 VPC 를 연결하려면 수많은 연결이 필요함
- 다수의 VPC 와 On-premise 를 연결하기 위한 Gateway 로 다수의 VPC 를 하나의 Gateway 로 On-premise 와 연결할 수 있도록 지원
- Transit Gateway 에 다수의 VPC 를 연결하고 이 Transit Gateway 를 VPN, Direct connect, Peering(다른 Region 의 VPC)에 연결할 수 있음
- Transit Gateway 를 통하여 다른 VPC 와 통신 가능(라우팅 필요)

* Clustered Database in Multiple Region
- VPC Peering이 활성화된 상태에서 다른 리전에 있는 Peer VPC의 보안그룹을 참조할 수 없으므로 Peer VPC의 CIDR Block을 사용해야 함