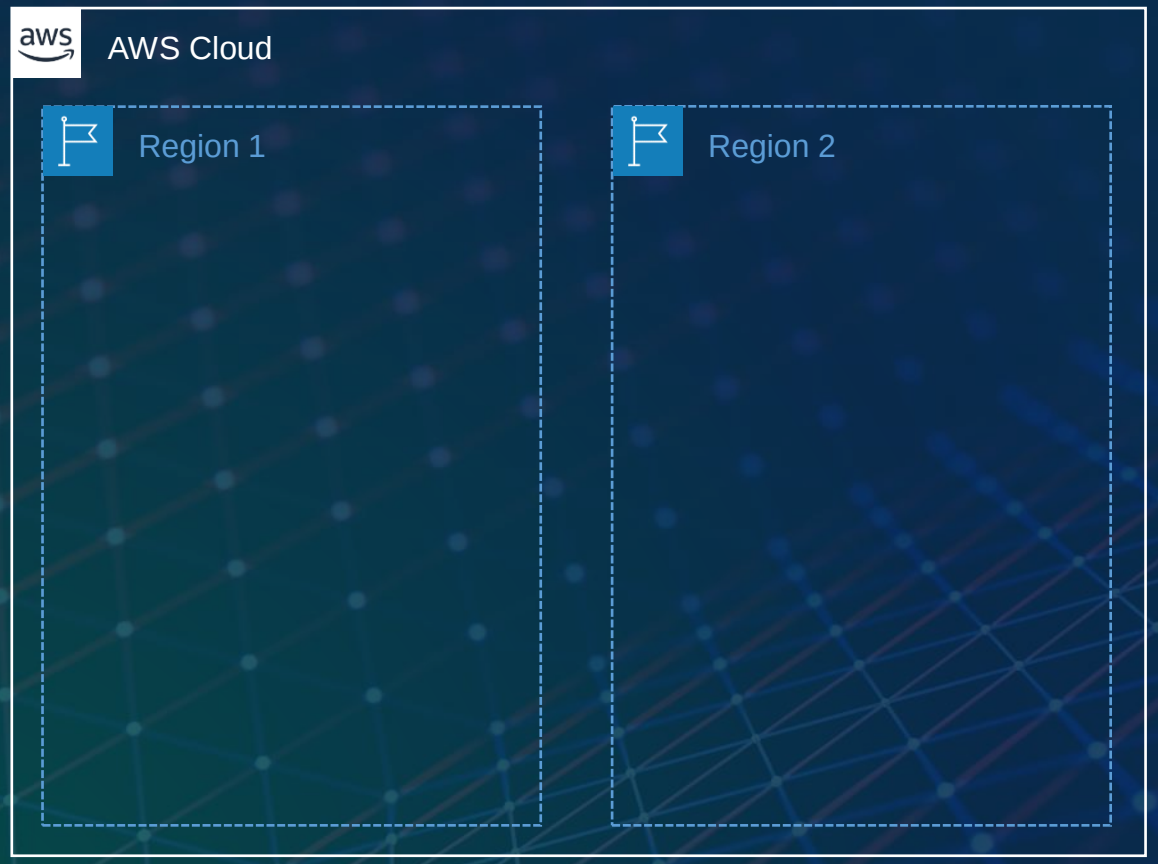

고객과 사회의 행복을 선도하는 TOP TIER 디지털 서비스 기업
CJ OLIVENETWORKS
AWS Network
INFRA TECH LAB
서병환
CJ OLIVENETWORKS

AWS는 전세계 사용자를 대상으로 서비스하고 있으며,

다양한 국가에 REGION 이라는 이름으로 REGIONAL SERVICE를 제공하고 있음

Region



Region의 개념

1. AWS는 미국 4개(OHIO, VIRGINIA, CALIFORNIA, OREGON),
   아시아 10개(SEOUL, HONGKONG, MUMBAI, HYDERABAD, SINGAPORE, SYDNEY, JAKARTA, MELBOURNE, TOKYO, OSAKA),
   유럽 8개(FRANKFURT, ZURICH, IRELAND, LONDON, MILANO, SPAIN, PARIS, STOCKHOLM),
   중동 2개(UAE, BAHRAIN),
   캐나다 1개(CANADA),
   남미 1개(SAO PAULO),
   아프리카 1개(CAPE TOWN)
   2023년 기준 총 27개 GLOBAL REGION을 대상으로 서비스 중

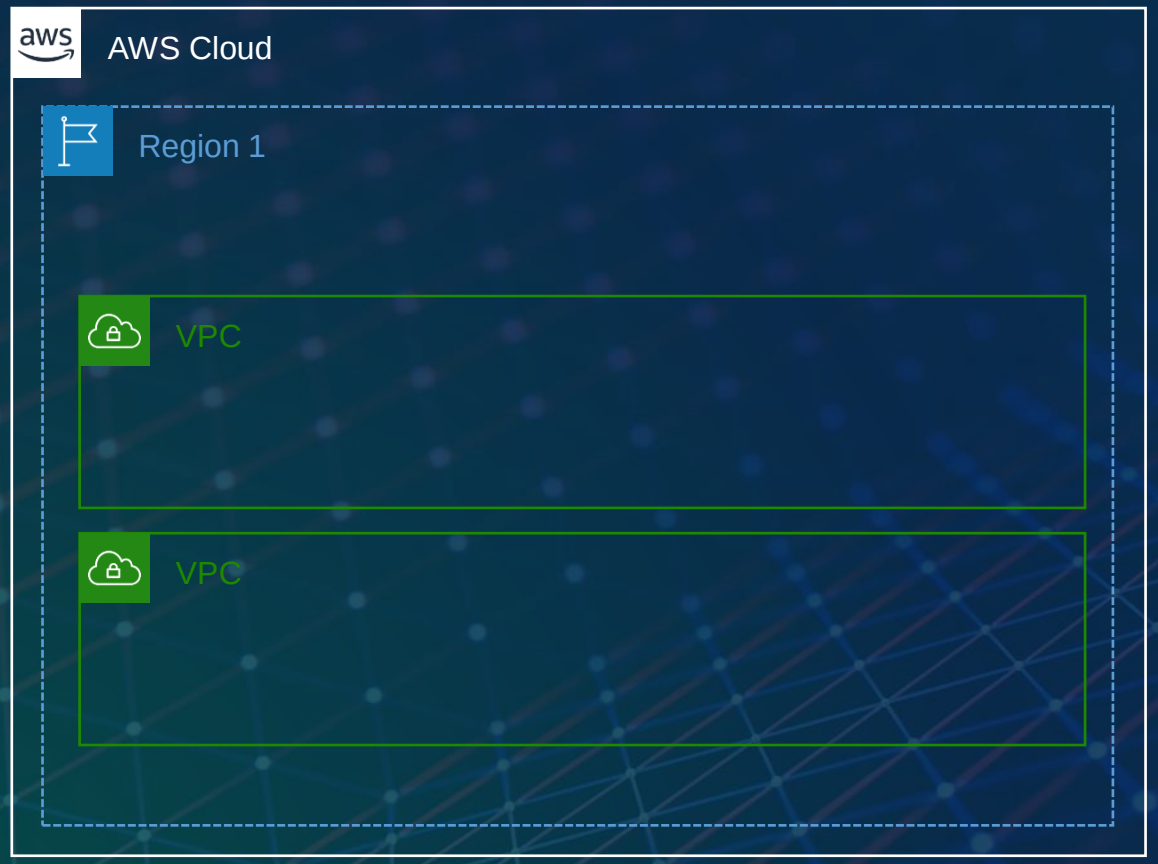
2. 하나의 AWS 계정은 여러 개의 REGION을 사용할 수 있으며, REGION별 RESOURCE는 별도 관리된다.

3. REGION별 RESOURCE간 NETWORK 통신을 위해서는 별도의 서비스를 통해 NETWORK 연결이 필요하다.

VPC는 아주 쉽게 얘기하면 ON-PREMISE와 비교했을 때 하나의 작은 DATACENTER라고 표현할 수 있으며,

AWS RESOURCE 단위에서 가장 핵심이 되는 개념

VPC (Virtual Private Cloud)



VPC의 개념

1. 하나의 AWS 계정에는 여러 개의 VPC가 존재할 수 있다.

2. VPC는 REGION 단위 안에서 존재하고 관리되며,
   동일 REGION 이라 할지라도 여러 개의 VPC가 존재할 수 있다.

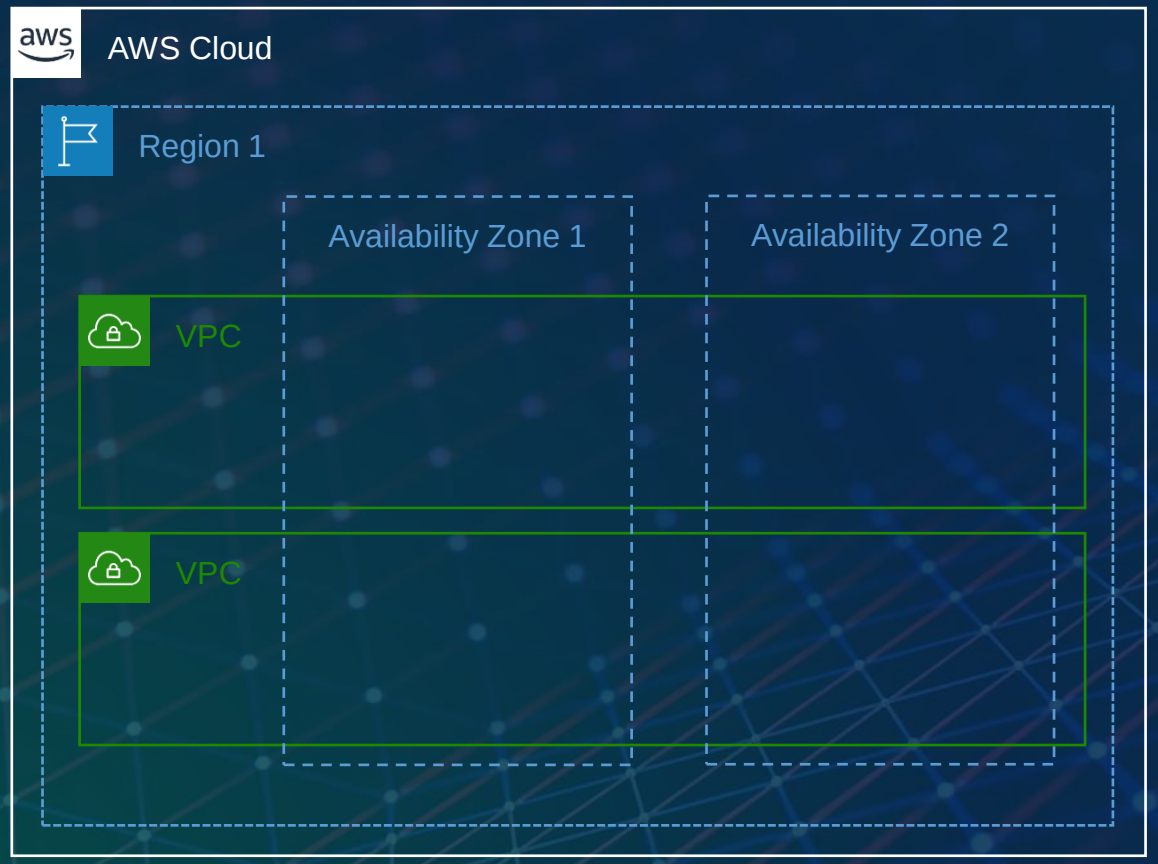
3. VPC 안에서 나머지 AWS RESOURCE들이 생성되기 때문에,
   VPC 삭제 시 VPC 내부 전체 리소스가 삭제된다.
   따라서 생성 전 충분한 계획하에 설계가 필요하다.

4. VPC는 큰 단위의 IP SUBNET을 속성으로 가지고 있다.
   향후 IP SUBNET을 일정 부분 추가할 수 있다.

VPC의 예)
VPC 1 – 10.0.0.0/8
VPC 2 – 172.16.0.0/12
VPC 3 – 192.168.0.0/16

VPC가 가상의 작은 DATACENTER라면, AZ는 AWS의 거대한 물리적인 DATACENTER로
물리적인 DATACENTER 장애로 인해 서비스 영향을 최소화하기 위해 AZ별 RESOURCE를 배치해야 함

AZ (Availability Zone)



AZ의 특징

1. 하나의 REGION 에는 여러 개의 AZ를 가지고 있다.
2. 각 REGION 별 AZ의 수는 다를 수 있으며, SEOUL REGION인 AP-NORTHEAST-2 REGION에는 4개의 AZ가 존재한다.
3. AZ 별로 장애가 발생할 수 있는 가능성이 있기 때문에 AZ별로 RESOURCE를 배치하여 동시 장애 상황을 최소화 해야 함.
4. 실제 AWS는 AZ별로 물리적인 DATACENTER를 구분 해두었고, 수도권에 총 4개의 물리적인 DATACENTER가 존재한다.

CJ OLIVENETWORKS

AWS의 RESOURCE들을 외부 공격으로부터 보호하기 위하여
SUBNET 설계 시 크게 3가지 형태의 SUBNET 설계를 할 필요가 있음

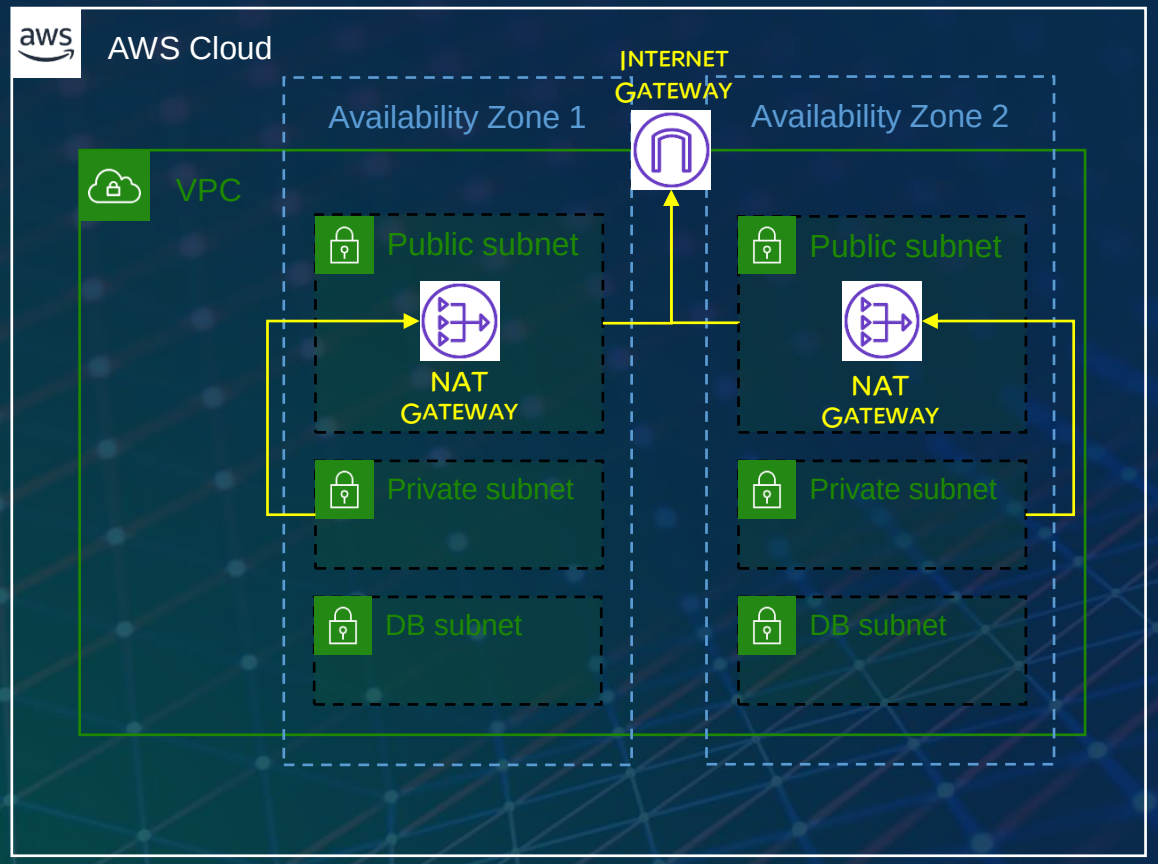
Subnet

Subnet의 특징

1. PUBLIC SUBNET – RESOURCE 자체가 직접 PUBLIC IP를 가지고 외부와 통신해야 하는 RESOURCE를 위한 SUBNET
2. PRIVATE SUBNET – RESOURCE 자체가 직접 PUBLIC IP를 가지고 있지는 않지만, 외부와 통신이 필요한 RESOURCE를 위한 SUBNET
3. DB SUBNET – 말 그대로 DATABASE를 위한 SUBNET으로 외부와의 연결을 단절하고 내부 RESOURCE들만 접근하도록 보호하는 SUBNET

NAT GATEWAY는 PUBLIC SUBNET 내에 위치하며
PRIVATE SUBNET 내 RESOURCE가 외부와 통신하기 위해서는 NAT GATEWAY를 통해서 통신함

Subnet별 외부 통신



Subnet별 외부 통신 특징

1. PUBLIC SUBNET – PUBLIC SUBNET 내 NAT GATEWAY를 포함한 RESOURCE들은 PUBLIC IP를 가지고 INTERNET GATEWAY를 통해 외부와 통신함.

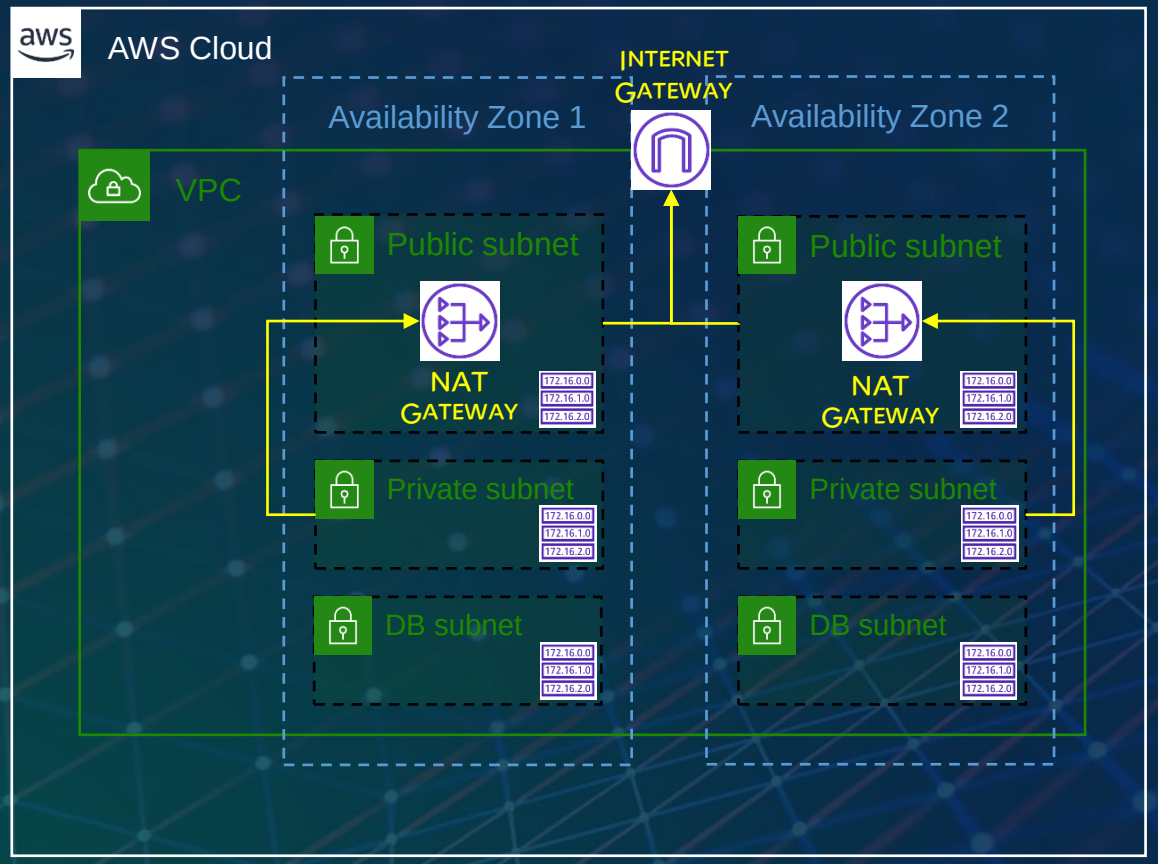
2. PRIVATE SUBNET – PUBLIC IP를 가지고 있지 않은 PRIVATE SUBNET RESOURCE들은 NAT GATEWAY의 PUBLIC IP를 기반으로 외부와 통신함.

3. DB SUBNET – 외부와 단절은 위해 INTERNET GATEWAY, NAT GATEWAY 어느 것과도 연결되어 있지 않아 내부 통신만 가능함.

CJ OLIVENETWORKS

각 SUBNET 별로 ROUTING 경로를 구분하기 위하여 별도 ROUTING TABLE을 만들고
각 ROUTING TABLE 별로 경로를 구분하여 보안에 최적화 함

Routing Table



Subnet별 Routing Table 특징

1. PUBLIC SUBNET

DESTINATION	TARGET
192.168.0.0/24	LOCAL
0.0.0.0/0	IGW-ID

2. PRIVATE SUBNET

DESTINATION	TARGET
192.168.0.0/24	LOCAL
0.0.0.0/0	NGW-ID

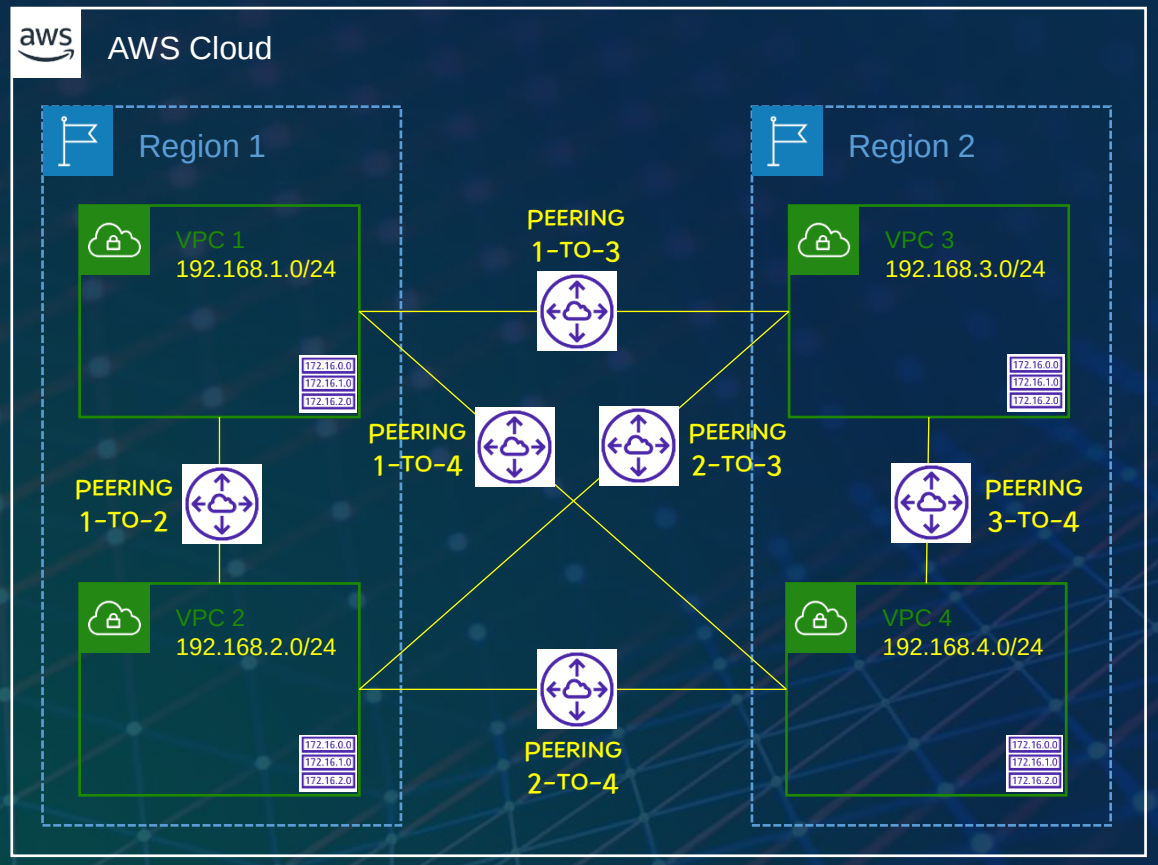
3. DB SUBNET

DESTINATION	TARGET
192.168.0.0/24	LOCAL

CJ OLIVENETWORKS

VPC간 연결이 필요한 경우,
AWS VPC PEERING 서비스를 통해서 VPC간 네트워크 연결을 할 수 있음

VPC Peering



VPC Peering의 개념

1. VPC PEERING은 서로 다른 VPC간 통신이 필요할 때 연결하는 서비스임.

2. 총 4개의 VPC가 있다고 했을 때, 총 필요한 PEERING 개수는
   3 + 2 + 1 = 6개의 PEERING 구성이 필요함.

VPC 1 ROUTING TABLE

DESTINATION	TARGET
192.168.1.0	LOCAL
192.168.2.0	PEERING 1-TO-2
192.168.3.0	PEERING 1-TO-3
192.168.4.0	PEERING 1-TO-4

VPC 2 ROUTING TABLE

DESTINATION	TARGET
192.168.1.0	PEERING 1-TO-2
192.168.2.0	LOCAL
192.168.3.0	PEERING 2-TO-3
192.168.4.0	PEERING 2-TO-4

VPC 3 ROUTING TABLE

DESTINATION	TARGET
192.168.1.0	PEERING 1-TO-3
192.168.2.0	PEERING 2-TO-3
192.168.3.0	LOCAL
192.168.4.0	PEERING 3-TO-4

VPC 4 ROUTING TABLE

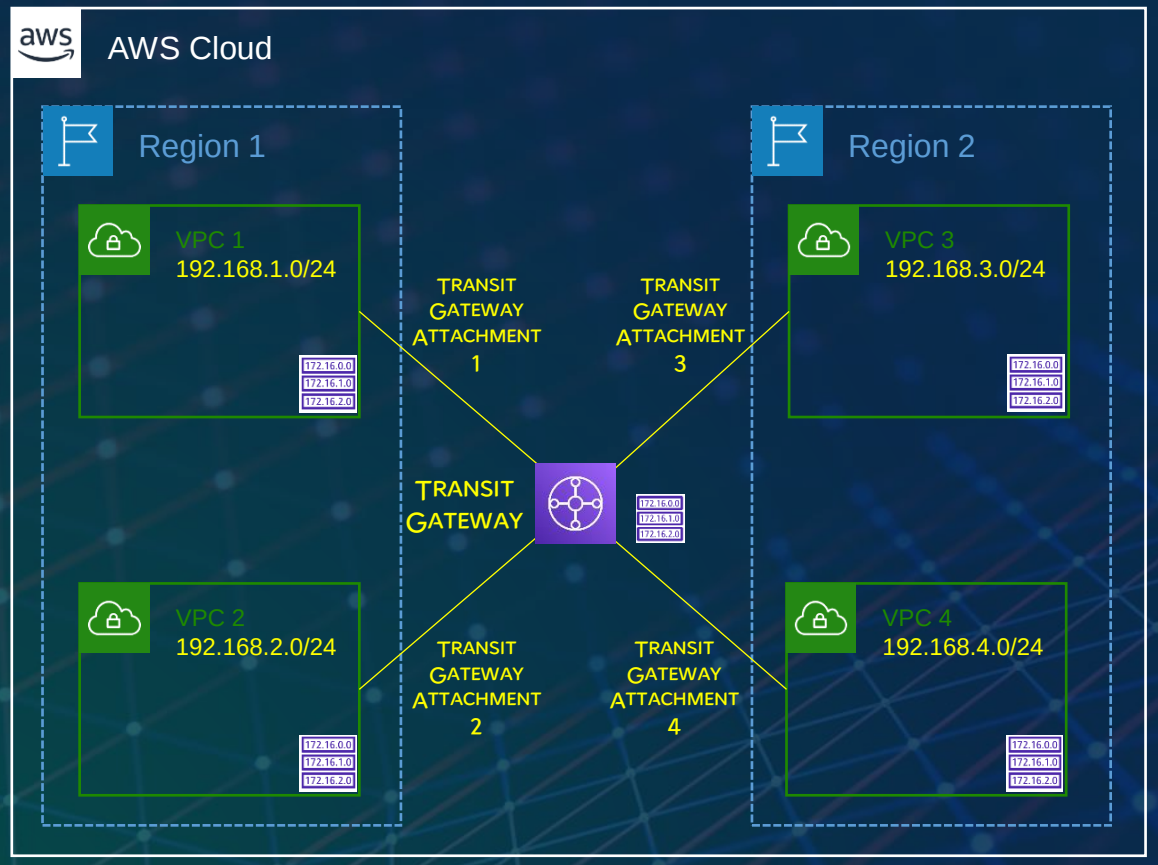
DESTINATION	TARGET
192.168.1.0	PEERING 1-TO-4
192.168.2.0	PEERING 2-TO-4
192.168.3.0	PEERING 3-TO-4
192.168.4.0	LOCAL

CJ OLIVENETWORKS

VPC간 연결이 복잡하고 관리가 어려운 네트워크 환경의 경우

AWS TRANSIT GATEWAY 서비스를 통해서 복잡한 네트워크를 간소화할 수 있음

Transit Gateway



Transit Gateway의 개념

1. TRANSIT GATEWAY는 네트워크 간소화를 제공하는 클라우드 라우터 서비스임.

2. TRANSIT GATEWAY는 크게 TRANSIT GATEWAY ATTACHMENT와 TRANSIT GATEWAY ROUTING 으로 구성되어 있음.

VPC 1 ROUTING TABLE

DESTINATION	TARGET
192.168.1.0	LOCAL
192.168.2.0	TGW-ID
192.168.3.0	TGW-ID
192.168.4.0	TGW-ID

VPC 2 ROUTING TABLE

DESTINATION	TARGET
192.168.1.0	TGW-ID
192.168.2.0	LOCAL
192.168.3.0	TGW-ID
192.168.4.0	TGW-ID

TRANSIT GATEWAY ROUTING TABLE

DESTINATION	TARGET
192.168.1.0	TGWA1-ID
192.168.2.0	TGWA2-ID
192.168.3.0	TGWA3-ID
192.168.4.0	TGWA4-ID

VPC 3 ROUTING TABLE

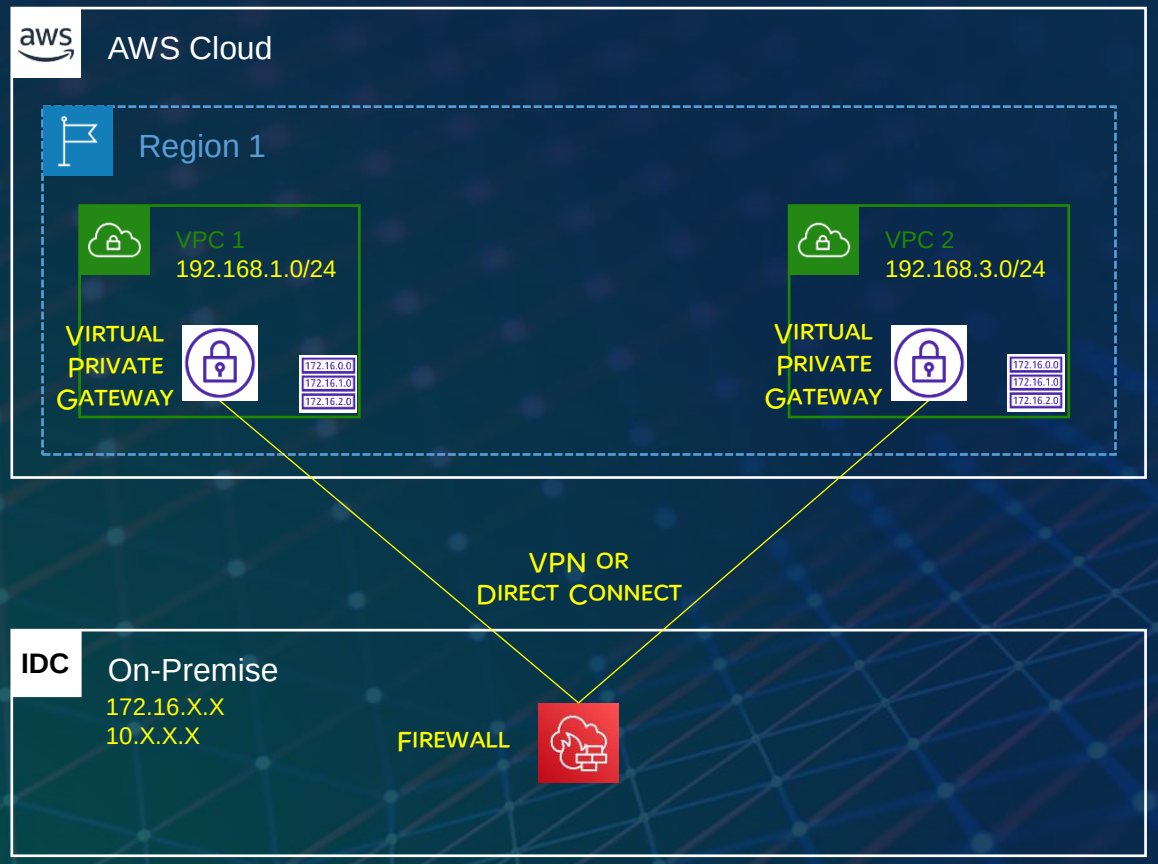
DESTINATION	TARGET
192.168.1.0	TGW-ID
192.168.2.0	TGW-ID
192.168.3.0	LOCAL
192.168.4.0	TGW-ID

VPC 4 ROUTING TABLE

DESTINATION	TARGET
192.168.1.0	TGW-ID
192.168.2.0	TGW-ID
192.168.3.0	TGW-ID
192.168.4.0	LOCAL

VPC와 ON-PREMISE 환경 간의 NETWORK 연결 시 VPC 단위로 연결을 구성해야 하기 때문에
VPC가 많을 경우 상당히 복잡한 NETWORK 구성이 될 수 있음

On-Premise 연동(w/ VPC)



On-Premise 연동(w/ VPC)의 개념

1. ON-PREMISE 환경(IDC OR OFFICE)와의 NETWORK 연동 시 AWS의 RESOURCE 단위인 VPC 단위로 연결을 해야 함.
   (VPC 별로 ROUTING TABLE을 별도 관리하기 때문)

2. 따라서 VPC를 1개만 사용할 경우에는 상관없지만, 복수 VPC를 사용하는 환경에서는 VPC PEERING 처럼 복수 연결이 필요할 수 밖에 없음.

3. AWS와 ON-PREMISE 연동은 가상의 네트웍을 만드는 VPN 방식과 전용회선을 이용한 AWS DIRECT CONNECT 를 사용하는 방식이 있음.

4. VPN은 일반적인 인터넷 회선으로 연동이 가능하기 때문에 상대적으로 비용이 저렴하다는 장점이 있지만 전용회선 대비 품질이 떨어질 수 있음.

VPC 1 ROUTING TABLE

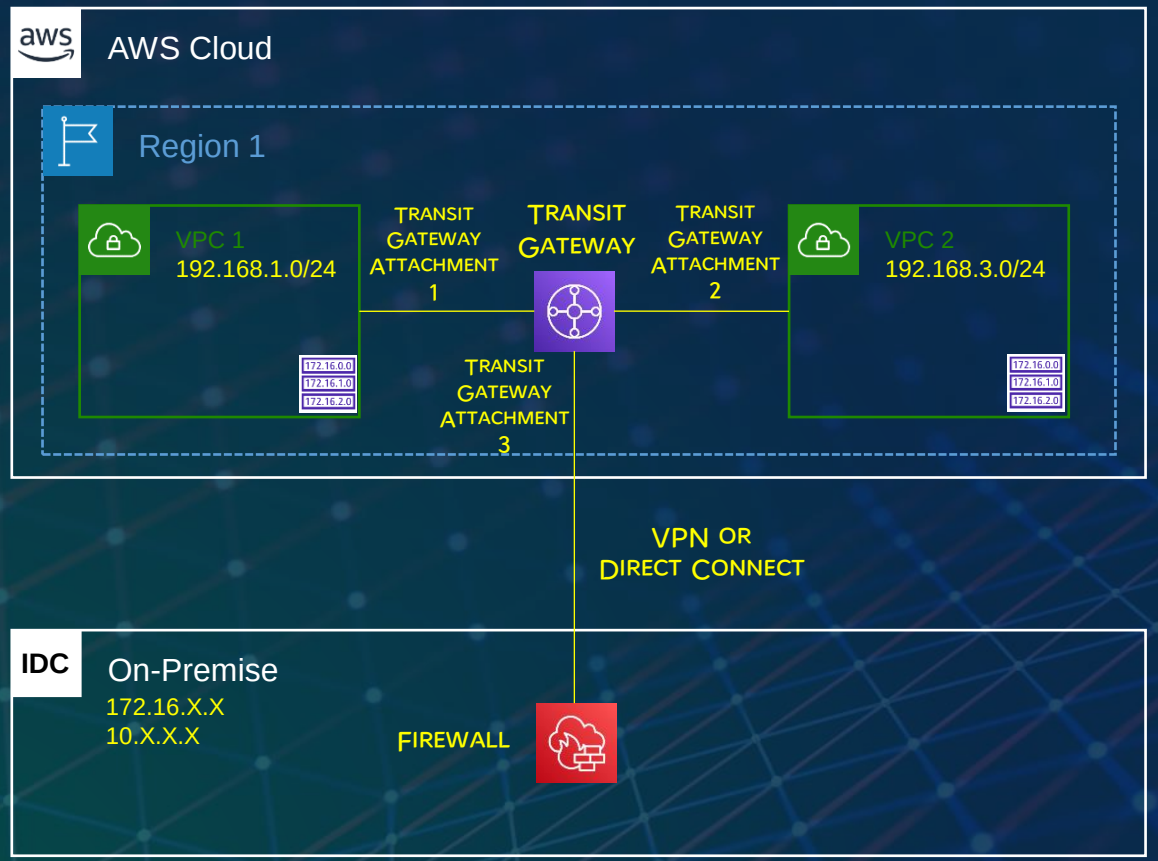
DESTINATION	TARGET
192.168.1.0	LOCAL
172.16.X.X	VGW1-ID
10.X.X.X	VGW1-ID

VPC 2 ROUTING TABLE

DESTINATION	TARGET
192.168.3.0	LOCAL
172.16.X.X	VGW2-ID
10.X.X.X	VGW2-ID

VPC와 ON-PREMISE 환경 간의 NETWORK 연결 시 VPC 단위로 연결을 구성해야 하기 때문에
VPC가 많을 경우 상당히 복잡한 NETWORK 구성이 될 수 있음

On-Premise 연동(w/ TGW)



On-Premise 연동(w/ TGW)의 개념

1. TRANSIT GATEWAY를 통해서 ON-PREMISE 환경과 연동 시에는 VPC 별로 연결할 필요 없이 하나의 연결 만으로 NETWORK 연동이 가능함

2. 따라서 VPC를 1개만 사용할 경우에는 상관없지만, 복수 VPC를 사용하는 환경에서는 VPC PEERING 처럼 복수 연결이 필요할 수 밖에 없음.

VPC 1 ROUTING TABLE

DESTINATION	TARGET
192.168.1.0	LOCAL
172.16.X.X	TGW-ID
10.X.X.X	TGW-ID

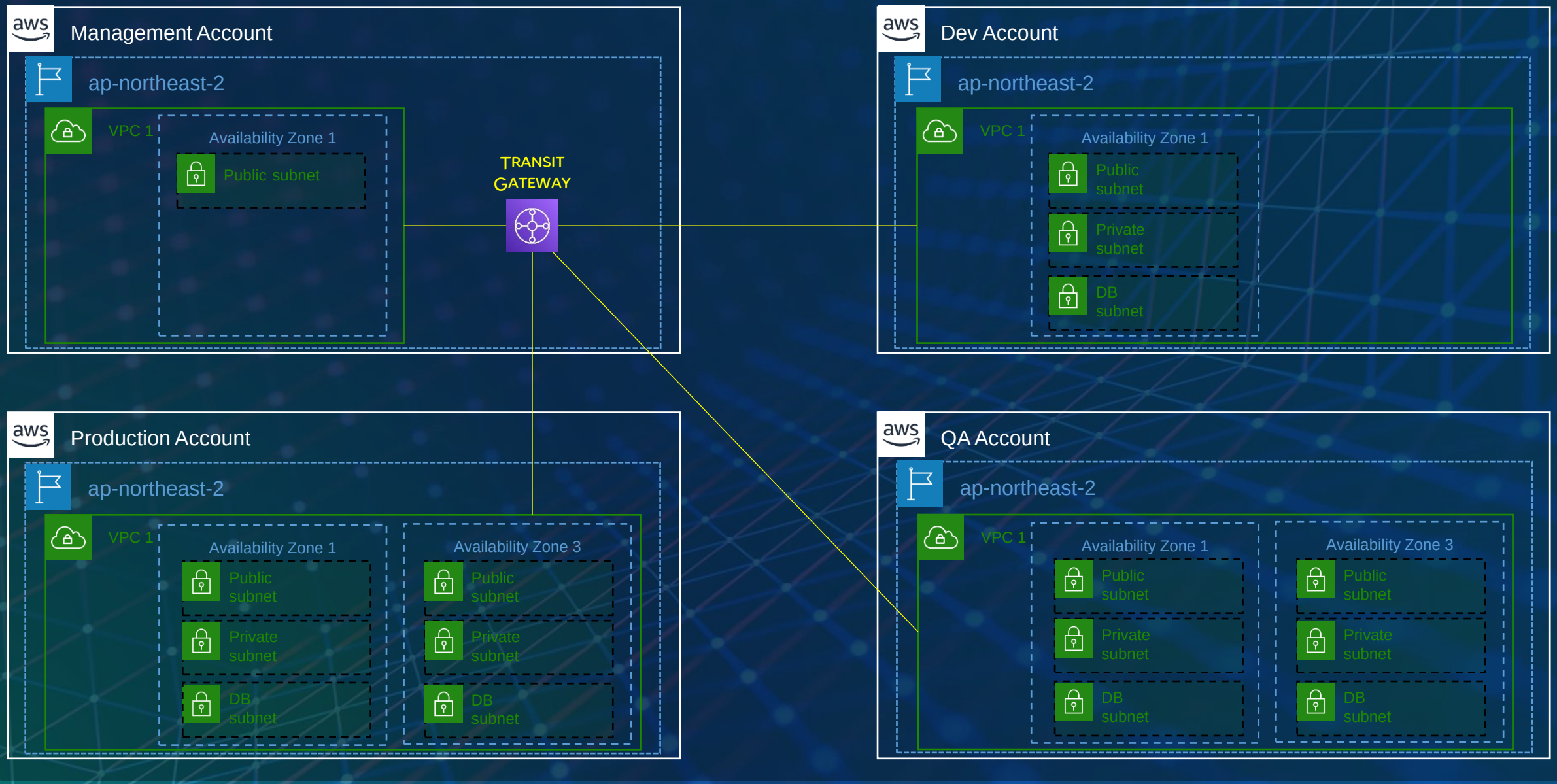
TRANSIT GATEWAY ROUTING TABLE

DESTINATION	TARGET
192.168.1.0	TGWA1-ID
192.168.3.0	TGWA2-ID
172.16.X.X	TGWA3-ID
10,X,X,X	TGWA3-ID

VPC 2 ROUTING TABLE

DESTINATION	TARGET
192.168.3.0	LOCAL
172.16.X.X	TGW-ID
10.X.X.X	TGW-ID

AWS Network | Best Practice




End of Document