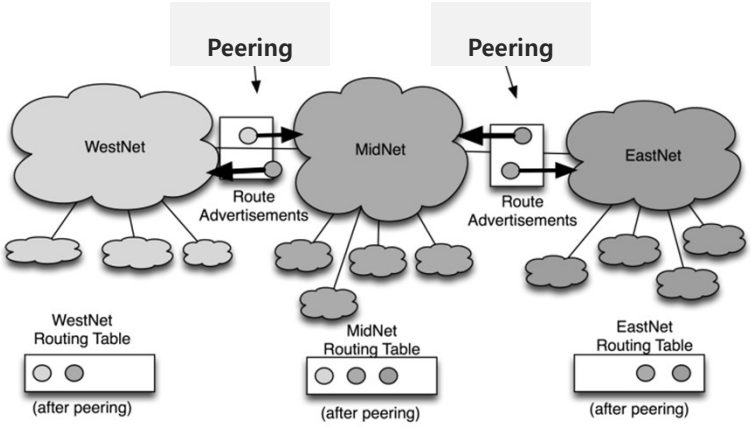
Day 2. 가상 네트워크 간의 연동

구분	주제	세부 내용
이론	Day 1 MCN 개요와 라우팅	• 멀티클라우드 개요 • 멀티클라우드를 위한 라우팅 (CSP, 오픈소스) • 라우팅 동작 • 라우팅 테이블
	Day 2 **가상 네트워크 간의 연동**	**• CSP의 가상네트워크 구성** **• Peering (가상 네트워크 연동)** **• Transit Gateway/Virtual WAN/VCN** **• 멀티 클라우드상의 가상 네트워크 연동**
	Day 3 하이브리드와 멀티 클라우드	• CSP/제조사 하이브리드 클라우드 솔루션 • VPN(Virtual Private Network) • 전용선(Direct Connect / Express Route) • Cloud Hub
이론/실습	Day 4 프라이빗 링크	• CSP의 프라이빗 링크 구성 • 서비스 엔드포인트(Endpoint) • 프라이빗 링크(Private Link) • 멀티클라우드 라우팅 구성 (실습)
	Day 5 멀티 클라우드 네트워킹	• 멀티클라우드 아키텍쳐 (CSP, 제조사) • 멀티클라우드 인프라 연동 • 멀티클라우드 인프라 관리 • 멀티클라우드 관리 플랫폼 (실습)

DAY 2. 가상 네트워크 간의 연동

❖ 피어링 peering (1:1 연결)

• 피어링 내망을 경유해서 다른 망과 연결시켜주는 역할은 제외되기 때문에 WestNet과 EastNet은 MidNet을 경유해서 서로 통신할 수 없음 (즉, 피어링 관계에서는 피어링한 관계 내에서만 통신)

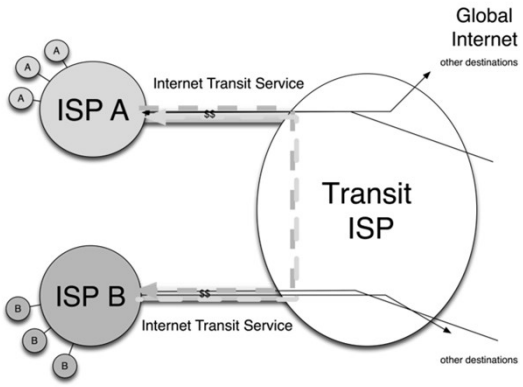


Source: https://m.clien.net/service/board/lecture/17610900

DAY 2. 가상 네트워크 간의 연동

❖ 트랜짓 transit (1:1:N 연결)

- 모든 망 운영자가 서로 피어링을 맺기에는 너무 비효율적 (n개의 망이 있다면, n*(n-1)/2개의 접속이 필요
- 트랜짓 서비스는 경유시켜주는 쪽이 서비스를 제공하는 것으로 트랜짓 서비스는 요금 발생



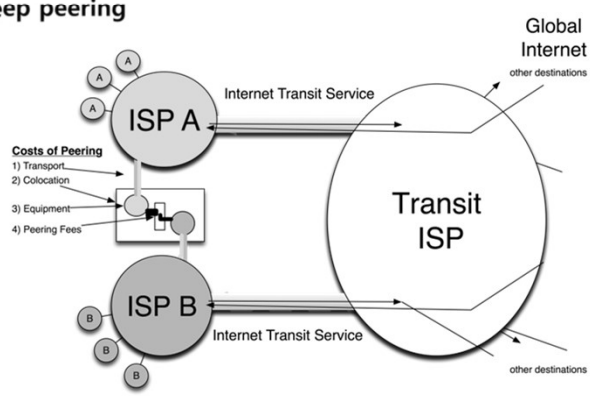
Source: https://m.clien.net/service/board/lecture/17610900

126

DAY 2. 가상 네트워크 간의 연동

❖ 피어링 vs 트랜짓

- 피어링은 상대방하고만 1:1로 통신하기 위한 접속이고, 트랜짓은 상대방뿐만 아니라 상대방을 통해 다른 망과 통신하기 위한 접속
- 피어링은 무료일 수도 있고 유료일 수도 있지만, 유료라 하더라도 트랜짓보다는 저렴
- 무정산 피어링 settlement-free peering, bill-and-keep peering
- 유상 피어링 paid peering
- 트랜짓은 대역폭을 늘리기 어려움



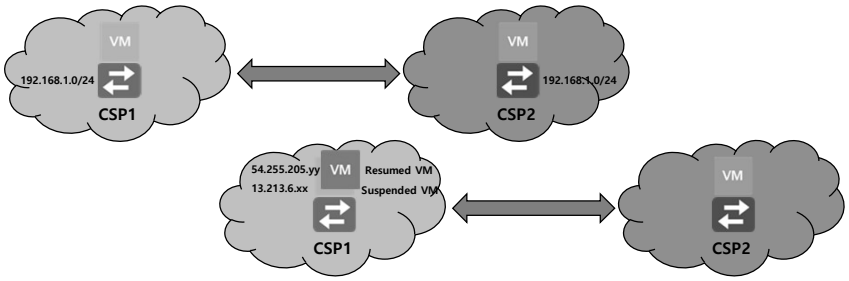
Source: https://m.clien.net/service/board/lecture/17610900

127

DAY 2. 가상 네트워크 간의 연동

❖ Check point

- 인프라 생성전에는 정확한 네트워크 정보를 얻기 어려움
- VPN Gateway를 활용해도 통신이 어려울 수 있고, Supernetting이 쉽지 않음
- Suspended → Resume 시 IP 주소 변경되어 통신 문제 발생 할 수 있음
- 원하는 규모의 IPv4 사설 주소 공간 확보가 어려 울 수 있음



Source: @ ETRI Conference 2022 '멀티클라우드 가상네트워크 기술' (김윤곤) 참조

128

DAY 2. 가상 네트워크 간의 연동

❖ Check point 해결 방법

- 네트워크 정보 동적 업데이트
- 가상/공통 네트워크 제공
  - ✓서로 다른 클라우드의 서로 다른 서브넷상에서 인프라 및 응용 (VM/Container)들이 동일 서브넷에 존재하는 것처럼 사설 IP 기반으로 운용 관리 할 수 있도록 하는 기술
  - ✓멀티클라우드의 다양한 네트워크에 적용 가능한 오버레이 네트워크로 VM 그룹에 동일 네트워크를 제공
- 네트워크 터널링
  - ✓서로 다른 오버레이(Overlay) 네트워크 기술이 적용된 CSP의 제어영역을 통과하여 통신 가능
  - ✓선택적으로 종단간(End-to-End) 암호화(Encryption) 적용 가능

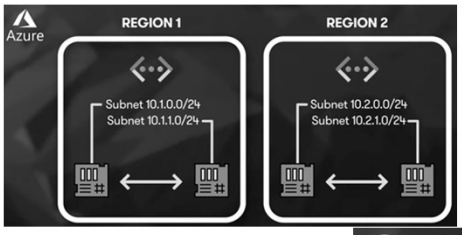
Source: @ ETRI Conference 2022 '멀티클라우드 가상네트워크 기술' (김윤곤) 참조

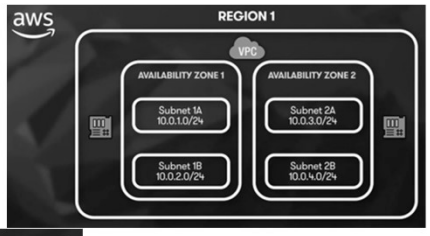
129

DAY 2. 가상 네트워크 간의 연동

❖ Networking services compared: AWS vs Azure vs Google Cloud

• Networking basics





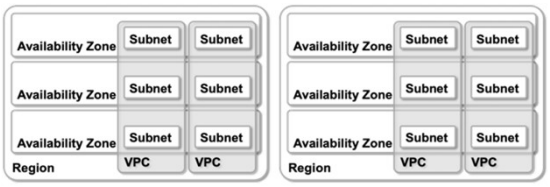
Source: https://acloudguru.com/blog/engineering/networking-services-compared-aws-vs-azure-vs-google-cloud

130

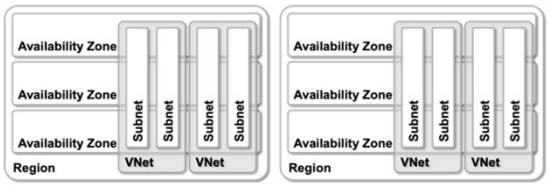
DAY 2. 가상 네트워크 간의 연동

❖ Virtual Networks and Subnets in AWS, Azure, and GCP

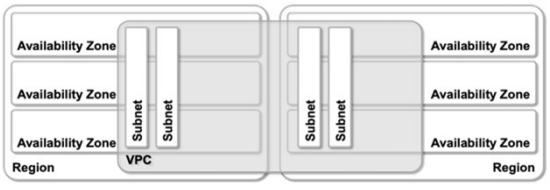
VPCs and subnets in AWS



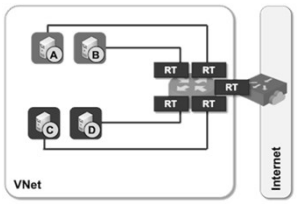
VNet and subnets in Azure



GCP VPCs and subnets



Azure packet forwarding behind the scenes



Source: https://blog.ipspace.net/2021/02/vpc-subnets-aws-azure-gcp.html

131

DAY 2. 가상 네트워크 간의 연동

❖ 가상 네트워크 환경을 위한 VCN 만들기 (Oracle Cloud Infrastructure)

• Virtual Cloud Network(VCN)은 가상 네트워크 환경을 제공합니다.

Source: https://thekoguryo.github.io/oci/chapter03/2/

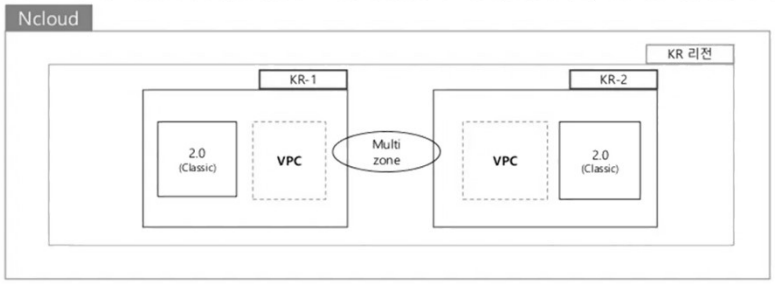
132

DAY 2. 가상 네트워크 간의 연동

❖ 네이버클라우드플랫폼

• VPC

1. on-demand configurable pool of shared computing resources
   논리적으로 완벽하게 격리된 네트워크를 사용자가 직접 설계하여 구성할 수 있도록 제공
2. Ncloud 2.0은 Classic과 VPC가 공존
   KR 리전에 KR-1 , KR-2 멀티존(Multi-AZ) 출시
3. Classic과 VPC는 다른 플랫폼입니다. 그러므로 상품간 연동이 되지 않을 수 있습니다.
   기본적으로 네트워크가 분리되어 있기 때문에 IP 기반의 상품은 상호간 통신 불가하며, 이에 따른 개별 상품의 버전이 상이



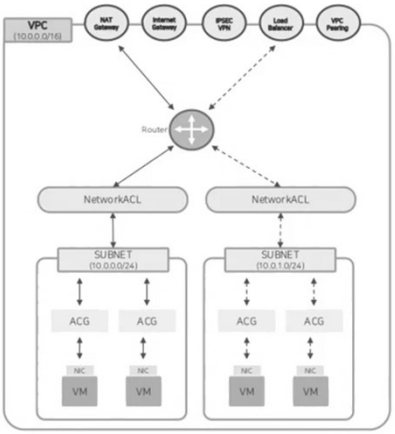
Source: https://www.slideshare.net/n_cloudplatform/ss-239153998

133

DAY 2. 가상 네트워크 간의 연동

❖ 네이버클라우드플랫폼

• VPC 기본 제어 기능



VPC는 클라우드 상에 논리적으로 분리된 고객별 전용 네트워크를 제공
네트워크 접근 제어를 거친 후 서버 접근 제어로 진행되어 보안이 강화됨
다른 사용자와 간섭 발생 영역이 줄어 높은 안정성과 보안성을 제공

구분	내용
VPC 제어	VPC 생성/삭제는 사용자 독립적인 N/W 생성/삭제를 의미
Subnet 제어	VPC 내에서 사용할 Subnet 지정 가능
Routing 제어	라우팅 설정 기능 제공
N/W ACL 제어	Stateless 형태의 트래픽 제어
ACG 제어	Stateful 형태의 트래픽 제어
Endpoint	Internet G/W (공인IP), NAT G/W (SNAT), IPSEC VPN, Loadbalancer, VPC Peering 등

Source: https://www.slideshare.net/n_cloudplatform/ss-239153998

134

DAY 2. 가상 네트워크 간의 연동

❖ 네이버클라우드플랫폼

• VPC – 네트워크 구성 요소

구성 요소	아이콘	세부 설명
VPC	CIDR VPC Name	VPC는 퍼블릭 클라우드 상에 논리적으로 완전하게 분리된 고객 전용 네트워크를 제공하는 서비스. 최대 /16 의 IP 네트워크 공간을 제공. (IP 대역 : RFC 1918)
Subnet (Internet GW)	CIDR Subnet Name Zone	할당된 VPC를 용도에 맞게 네트워크 공간을 세분화하여 사용. /16 ~ /28 의 네트워크 주소 할당이 가능. Public Subnet 생성 시, Internet Gateway가 연결됨
NAT GW		폐쇄된 네트워크에서 외부와의 인터넷 통신 시 사용하는 게이트웨이.
Route Table		네트워크 경로를 설정할 수 있는 기능을 제공. VPC 내부 통신을 위한 Local은 기본적으로 설정.
ACG		서버에서 인바운드/아웃바운드의 네트워크 접근 제어를 지원하며 Stateful 기반으로 동작
NACL		Subnet에서 인바운드/아웃바운드의 네트워크 접근 제어를 지원하며 Stateless 기반으로 동작
Virtual Private Gateway		Cloud Connect와 IPsec VPN에 연결되는 네이버 클라우드 플랫폼의 VPC 측 연결 접점으로서 Cloud Connect과 IPsec VPN 연결을 지원
VPC Peering		VPC 간 사설 연결을 보장하는 기능. 단방향 통신 제공으로 양방향 통신을 원하면 뒤바뀐 두개 정책 필요

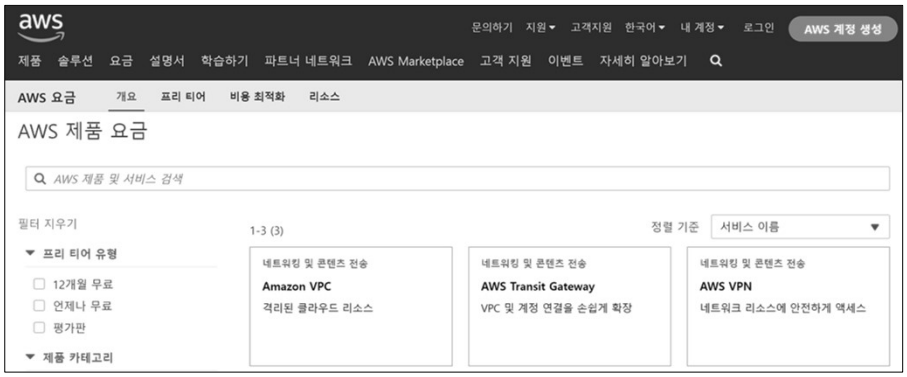
Source: https://www.slideshare.net/n_cloudplatform/ss-239153998

135

DAY 2. 가상 네트워크 간의 연동

❖ AWS 제품 요금: 네트워킹 및 컨텐츠 전송 제품 카테고리

- Amazon VPC
- AWS Transit Gateway
- AWS VPN



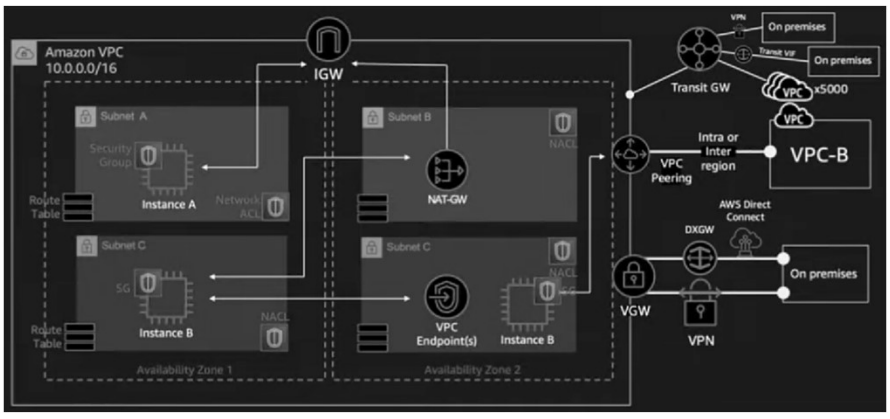
Source: https://aws.amazon.com/vpn/pricing/?did=ap_card&trk=ap_card
Source: https://aws.amazon.com/vpc/pricing/?did=ap_card&trk=ap_card , https://aws.amazon.com/transit-gateway/pricing/?did=ap_card&trk=ap_card

136

DAY 2. 가상 네트워크 간의 연동

❖ AWS VPC 구성 개요

- Subnet
- Routing
- IGW
- NAT-GW
- Security Group
- Network ACL (NACL)
- Transit GW
- VPN/VGW
- Peering
- DXGW/DX



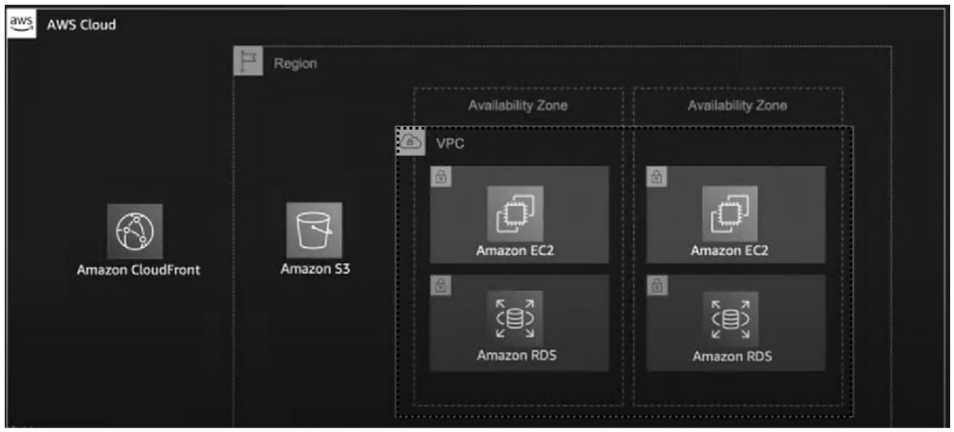
Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

137

DAY 2. 가상 네트워크 간의 연동

❖ AWS default VPC(버추얼 프라이빗 클라우드) 자원 레벨

- 글로벌 (Global)
- 리전 (Region)
- 가용영역 (AZ)



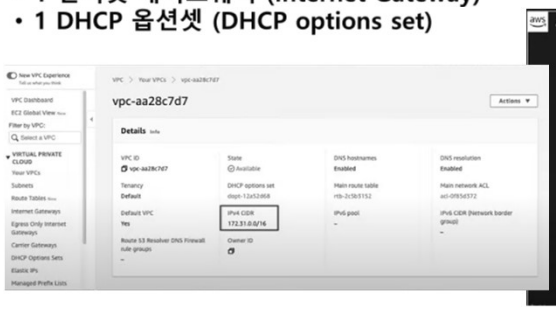
Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

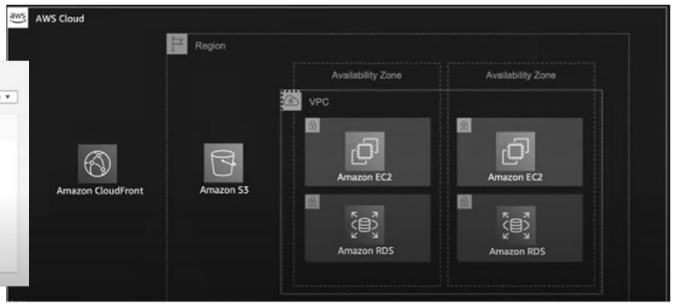
138

DAY 2. 가상 네트워크 간의 연동

❖ AWS: 기본 VPC의 구성 요소

- 1 VPC
- n 서브넷 Subnet(n은 사용할 수 있는 가용존의 개수)
- 1 라우트 테이블 (Route Table)
- 1 네트워크 ACL (Network ACL)
- 1 시큐리티 그룹 (Security Group)
- 1 인터넷 게이트웨이 (Internet Gateway)
- 1 DHCP 옵션셋 (DHCP options set)





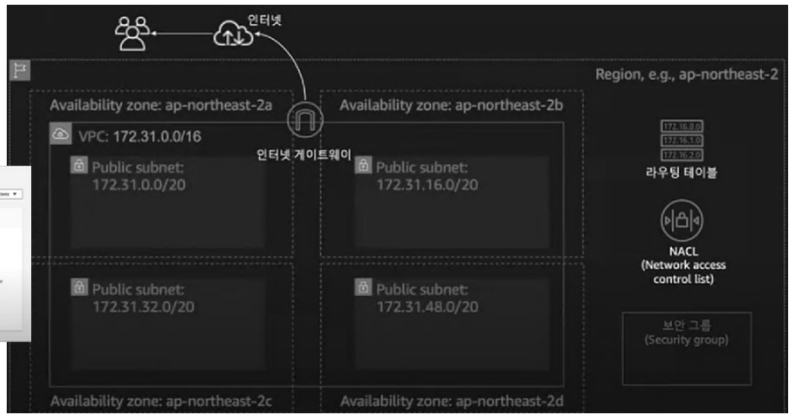
Source: https://www.44bits.io/ko/post/understanding_aws_vpc

139

DAY 2. 가상 네트워크 간의 연동

❖ AWS: Default VPC IP 주소 범위: 172.31.0.0/16 (서울의 경우 4개의 AZ 제공)

- AZ 2a: 172.31.0.0/20
- AZ 2b: 172.31.16.0/20
- AZ 2c: 172.31.32.0/20
- AZ 2d: 172.31.48.0/20



Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

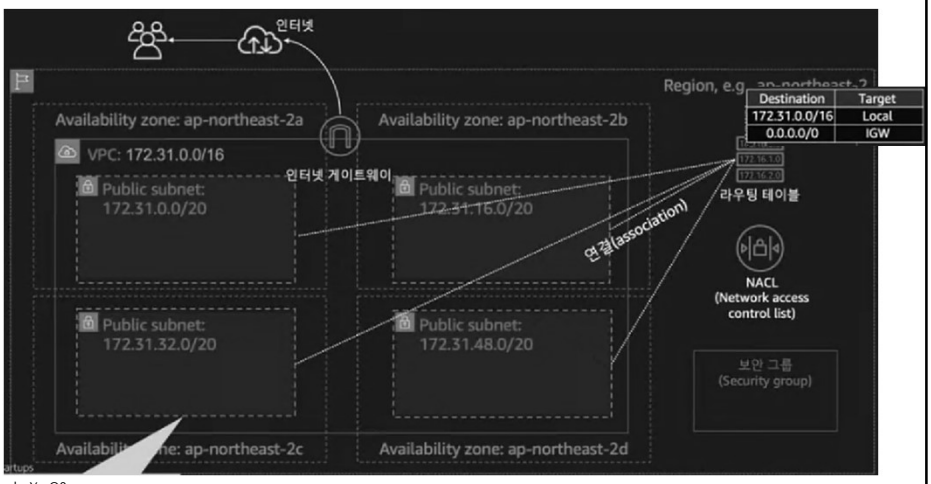
140

DAY 2. 가상 네트워크 간의 연동

❖ AWS: Default VPC 구성 - 라우팅 테이블

- 172.31.0.0/16 (Local)
- 0.0.0.0/0 (IGW)

Internet Gateway (IGW)



Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

141

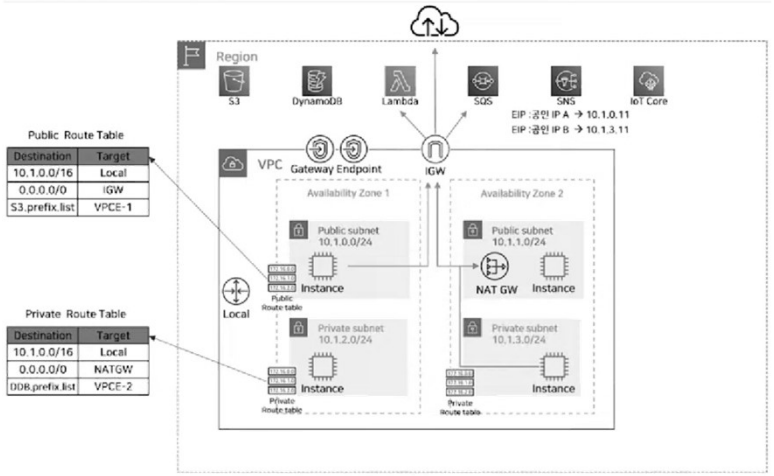
DAY 2. 가상 네트워크 간의 연동

❖ AWS: Default VPC 구성 - 라우팅 테이블

• IGW 연결 VPC 외부 AWS 서비스

- ✓ S3
- ✓ DynamoDB
- ✓ Lambda
- ✓ SQS
- ✓ SNS
- ✓ IoT Core
- ✓ 기타

Internet Gateway (IGW)



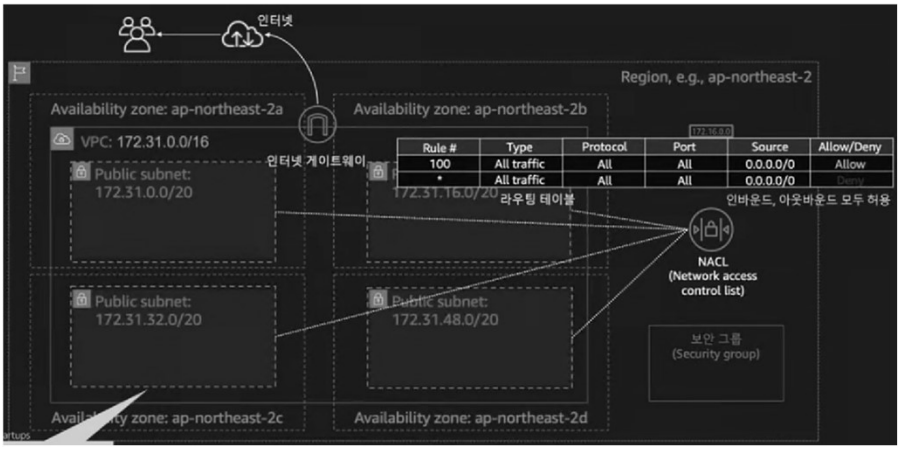
Source: https://www.youtube.com/watch?v=5kUZaGtXXt4

142

DAY 2. 가상 네트워크 간의 연동

❖ AWS: Default VPC 구성 - NACL (Stateless Firewall)

• Rule 번호가 작을수록 우선 처리

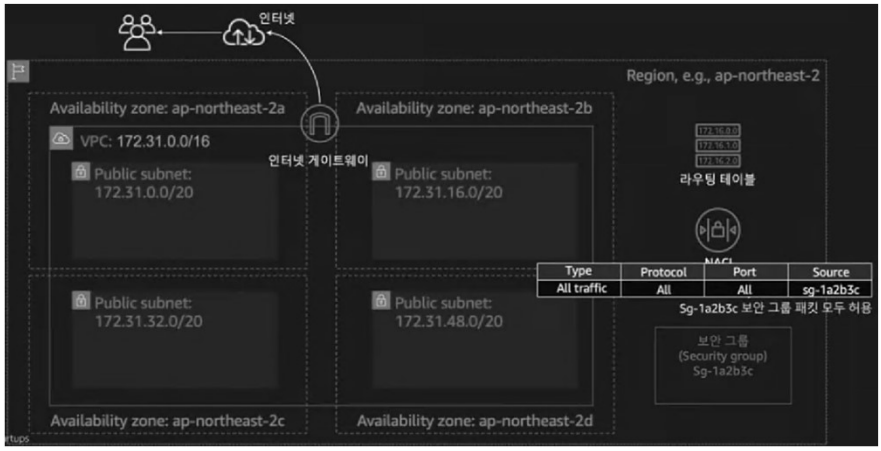


Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

143

DAY 2. 가상 네트워크 간의 연동

❖ AWS: Default VPC 구성 - Security Group



Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

144

DAY 2. 가상 네트워크 간의 연동

❖ AWS: 새로운 VPC 구성 - CIDR 사용 대역 정하기

- Classless Inter-Domain Routing
- RFC 1918: 사설 IP 대역 권장
  - ✓10.0.0.0/8: 10.0.0.0 – 10.255.255.255
  - ✓172.16.0.0/12: 172.16.0.0 – 172.31.255.255
  - ✓192.168.0.0/16: 192.168.0.0 – 192.168.255.255
- VPC CIDR 변경 불가, 대역 추가 가능
- IPv6 선택 시 VPC 대역은 /56, 각 서브넷은 /64 고정
- 서브넷 별로 예약된 IP 고려
  - ✓10.1.0.0: 네트워크 주소
  - ✓10.1.0.1: AWS에서 VPC 라우팅으로 예약
  - ✓10.1.0.2: AWS 예약
  - ✓10.1.0.3: AWS에서 향후 사용을 위해 예약
  - ✓10.1.0.255: 네트워크 브로드캐스트 주소

Class	Subnet Mask	Format	Bits to specify hosts	Number of Hosts	Bits to specify networks	Number of Networks
Class A	8-bit	255.0.0.0	24	$2^{24} - 2$ (=16777214)	1	2^{8-1} (=128)
Class B	16-bit	255.255.0.0	16	$2^{16} - 2$ (=65534)	2	2^{16-2} (=16384)
Class C	24-bit	255.255.255.0	8	$2^{8} - 2$ (=254)	3	2^{24-3} (=2097152)

CIDR Notation	Available Hosts	Subnet Mask
/8	$2^{32-8} - 2$ (=16777214)	255.0.0.0
/9	$2^{32-9} - 2$ (=8388606)	255.128.0.0
/10	$2^{32-10} - 2$ (=4194302)	255.192.0.0
/11	$2^{32-11} - 2$ (=2097150)	255.224.0.0
/12	$2^{32-12} - 2$ (=1048574)	255.240.0.0
/13	$2^{32-13} - 2$ (=524286)	255.248.0.0
/14	$2^{32-14} - 2$ (=262142)	255.252.0.0
/15	$2^{32-15} - 2$ (=131070)	255.254.0.0
/16	$2^{32-16} - 2$ (=65534)	255.255.0.0
/17	$2^{32-17} - 2$ (=32766)	255.255.128.0
/18	$2^{32-18} - 2$ (=16382)	255.255.192.0
/19	$2^{32-19} - 2$ (=8190)	255.255.224.0
/20	$2^{32-20} - 2$ (=4094)	255.255.240.0
/21	$2^{32-21} - 2$ (=2046)	255.255.248.0
/22	$2^{32-22} - 2$ (=1022)	255.255.252.0
/23	$2^{32-23} - 2$ (=510)	255.255.254.0
/24	$2^{32-24} - 2$ (=254)	255.255.255.0
/25	$2^{32-25} - 2$ (=126)	255.255.255.128
/26	$2^{32-26} - 2$ (=62)	255.255.255.192
/27	$2^{32-27} - 2$ (=30)	255.255.255.224
/28	$2^{32-28} - 2$ (=14)	255.255.255.240
/29	$2^{32-29} - 2$ (=6)	255.255.255.248
/30	$2^{32-30} - 2$ (=2)	255.255.255.252

Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

145

DAY 2. 가상 네트워크 간의 연동

❖ AWS: 새로운 VPC 구성 - 서브네팅

• Classless Inter-Domain Routing 사용 (예)

Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

146

DAY 2. 가상 네트워크 간의 연동

❖ AWS: 새로운 VPC 구성 - 서브네팅

• Classless Inter-Domain Routing 권장 구성 (예)

Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

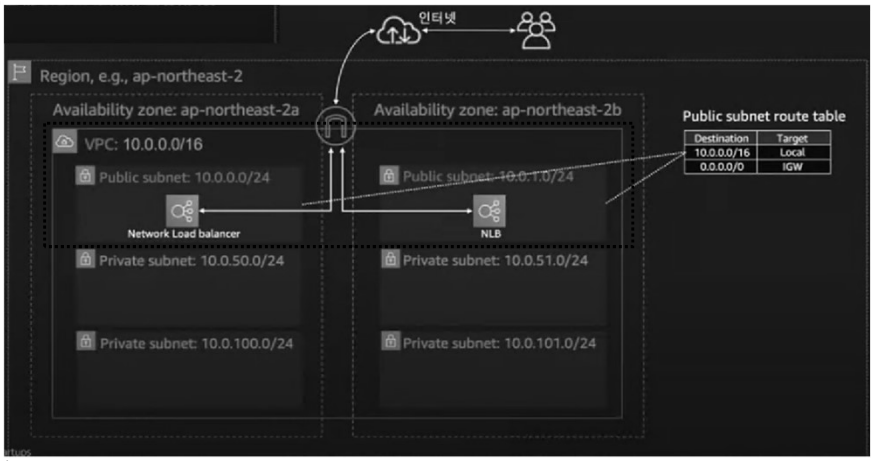
147

DAY 2. 가상 네트워크 간의 연동

❖ AWS: 새로운 VPC 구성 - 라우팅

• 인터넷과 양방향 통신 (예)

Internet Gateway (IGW)



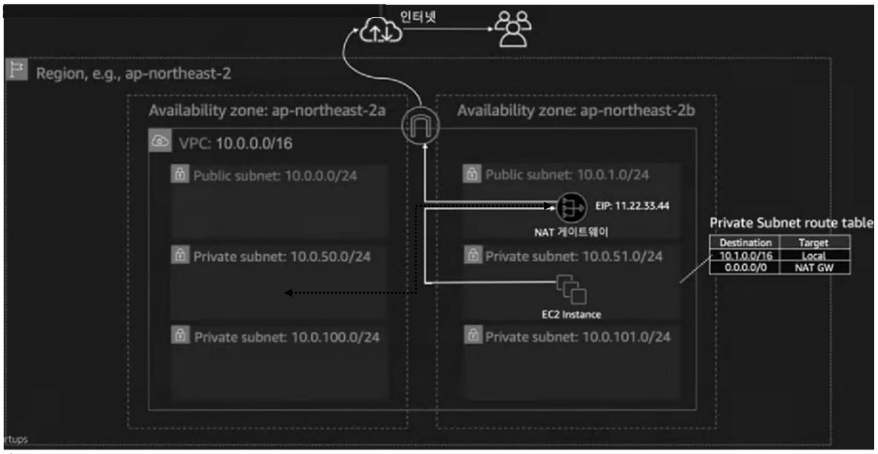
Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

148

DAY 2. 가상 네트워크 간의 연동

❖ AWS: 새로운 VPC 구성 - NAT 게이트웨이

• 인터넷과 아웃바운드 통신 (예)



Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

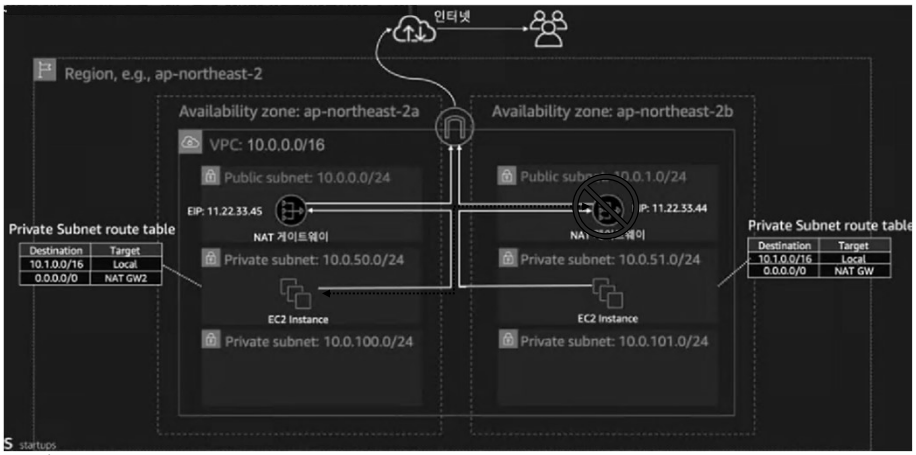
149

DAY 2. 가상 네트워크 간의 연동

150

❖ AWS: 새로운 VPC 구성 - NAT 게이트웨이 이중화

• 인터넷과 아웃바운드 통신 (예)



Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

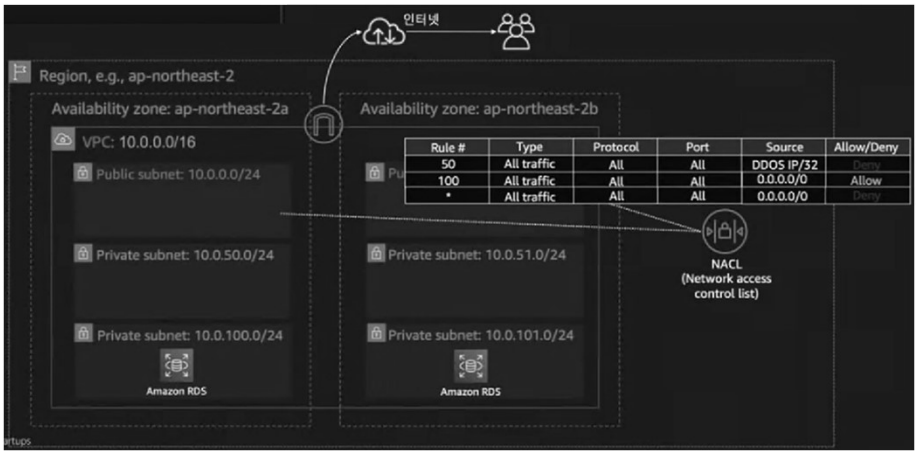
150

DAY 2. 가상 네트워크 간의 연동

151

❖ AWS: 새로운 VPC 구성 - DDoS 공격 차단

• VPC NACL 사용 (예)



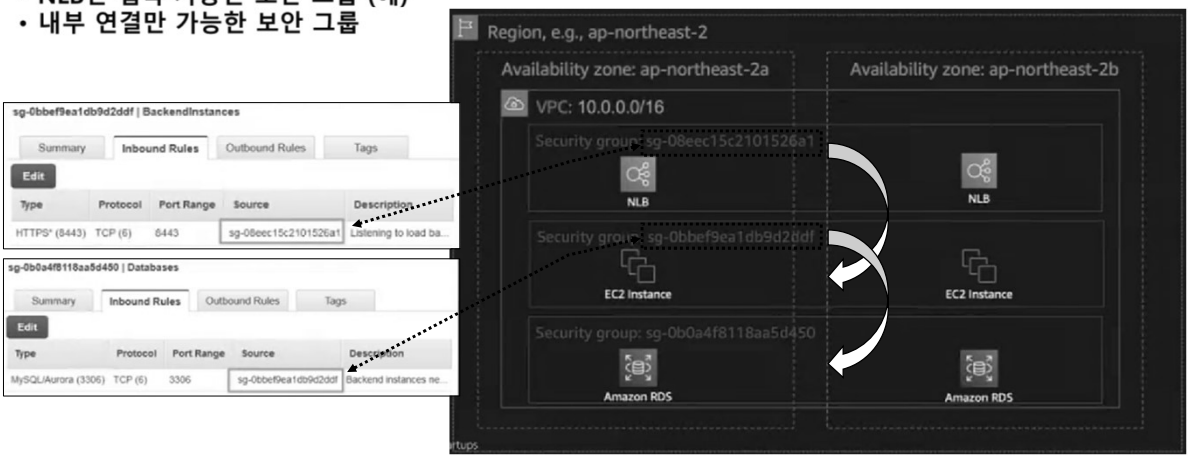
Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

151

DAY 2. 가상 네트워크 간의 연동

❖ AWS: 새로운 VPC 구성 - Security Group

- NLB만 접속 가능한 보안 그룹 (예)
- 내부 연결만 가능한 보안 그룹



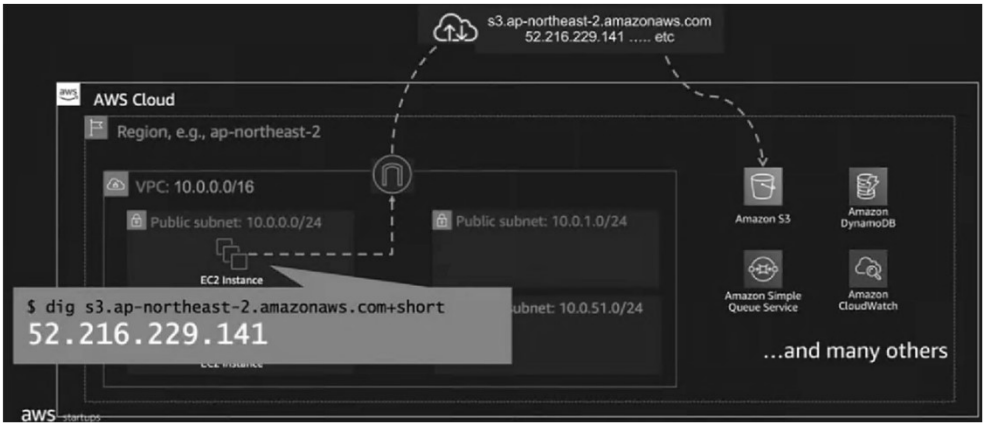
Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

152

DAY 2. 가상 네트워크 간의 연동

❖ AWS: VPC 구성 - 다른 AWS 서비스와 통신 (Private Link)

- 게이트웨이 엔드포인트
- 인터페이스 엔드포인트



Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

153

DAY 2. 가상 네트워크 간의 연동

❖ AWS: VPC 구성 - 다른 AWS 서비스와 통신 (Private Link)

- 게이트웨이 엔드포인트: S3나 DynamoDB등을 지원
- 인터페이스 엔드포인트

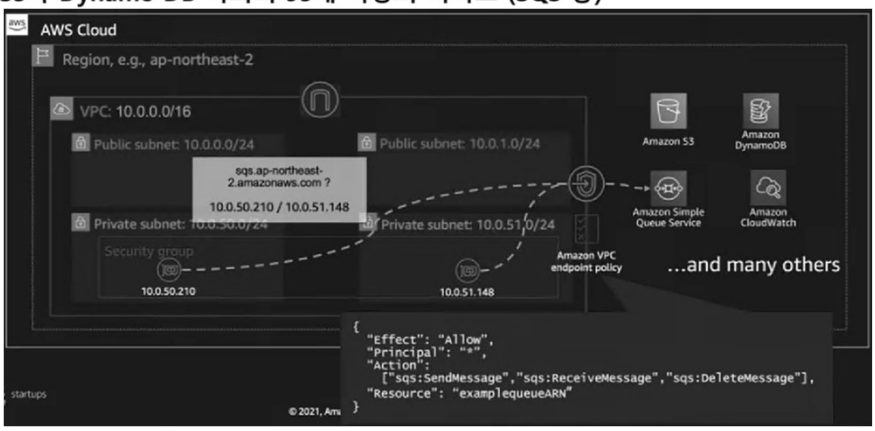
Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

154

DAY 2. 가상 네트워크 간의 연동

❖ AWS: VPC 구성 - 다른 AWS 서비스와 통신 (Private Link)

- 게이트웨이 엔드포인트
- 인터페이스 엔드포인트 : S3나 Dynamo DB 이외의 95개 이상의 서비스 (SQS 등)



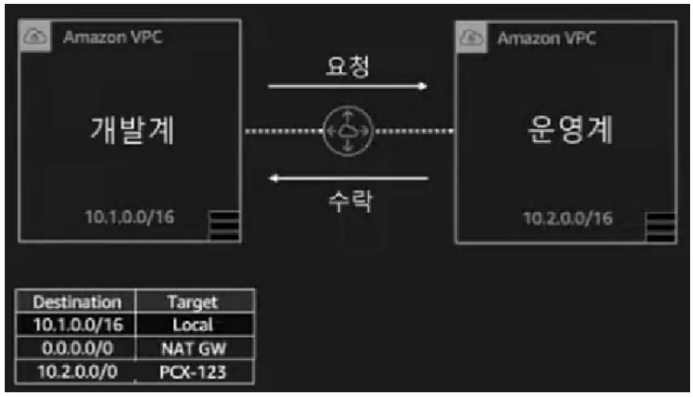
Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

155

DAY 2. 가상 네트워크 간의 연동

❖ AWS: VPC 구성 - 하나 이상의 VPC 이용

- VPC Peering
- Transit Gateway



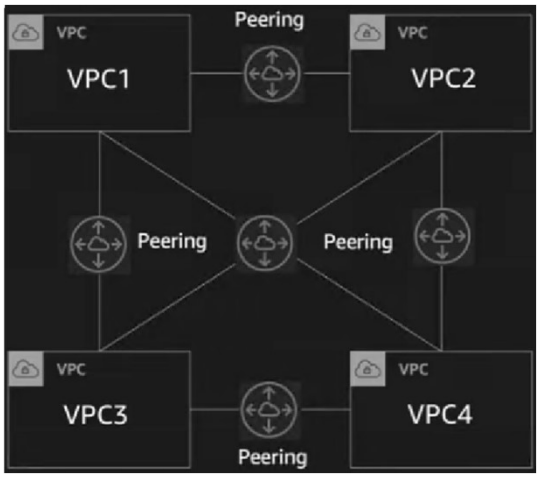
Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

156

DAY 2. 가상 네트워크 간의 연동

❖ AWS: VPC 구성 - 하나 이상의 VPC 이용

- VPC Peering: VPC간 1:1 통신
- Transit Gateway



Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

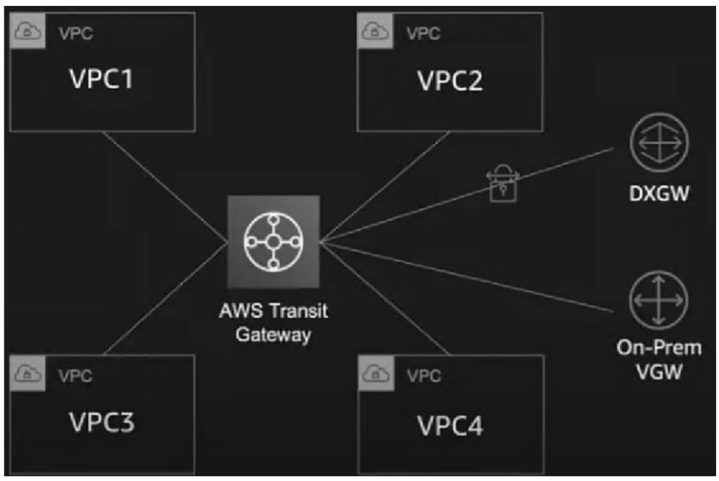
157

DAY 2. 가상 네트워크 간의 연동

158

❖ AWS: VPC 구성 - 하나 이상의 VPC 이용

- VPC Peering
- Transit Gateway:
  - ✓다수 VPC 연결 간소화
  - ✓VPN, DX를 TGW로만 연결
  - ✓ECMP, Multicast 기능 제공



Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

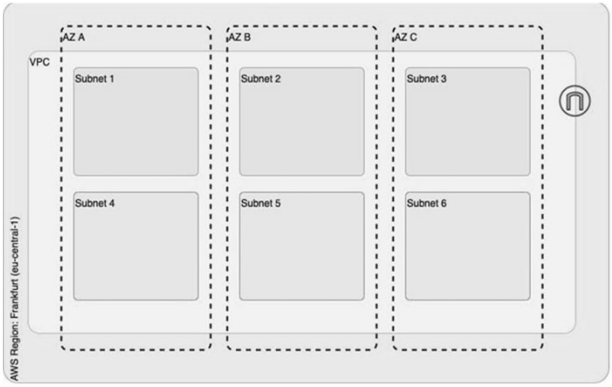
158

DAY 2. 가상 네트워크 간의 연동

159

❖ Build AWS VPC using Terraform

- AWS VPC
  - ✓ VPC in eu-central-1 zone
  - ✓ 1 Internet Gateway (IGW)
  - ✓ 3 Public Subnets, one in each AZ
  - ✓ 3 Private Subnets, one in each AZ
  - ✓ Route Table configurations (main and 2nd)



Source: https://spacelift.io/blog/terraform-aws-vpc

159

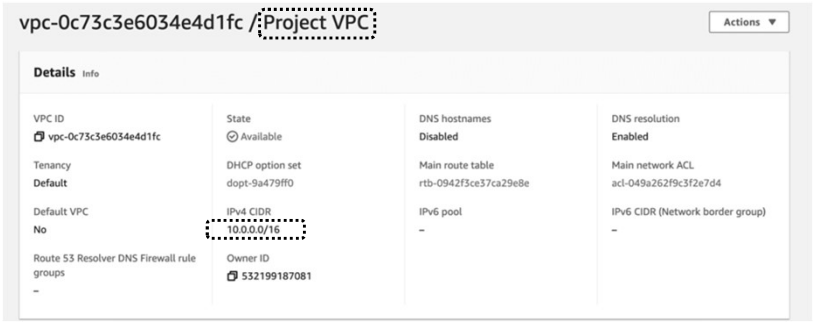
DAY 2. 가상 네트워크 간의 연동

❖ Build AWS VPC using Terraform

- AWS VPC
  - ✓ Create a VPC

```
resource "aws_vpc" "main" {
 cidr_block = "10.0.0.0/16"

 tags = {
   Name = "Project VPC"
 }
}
```



Source: https://spacelift.io/blog/terraform-aws-vpc

160

DAY 2. 가상 네트워크 간의 연동

❖ Build AWS VPC using Terraform

- AWS VPC
  - ✓ Create Subnets

```
variable "public_subnet_cidrs" {
 type        = list(string)
 description = "Public Subnet CIDR values"
 default     = ["10.0.1.0/24", "10.0.2.0/24", "10.0.3.0/24"]
}

variable "private_subnet_cidrs" {
 type        = list(string)
 description = "Private Subnet CIDR values"
 default     = ["10.0.4.0/24", "10.0.5.0/24", "10.0.6.0/24"]
}
```

```
resource "aws_subnet" "public_subnets" {
 count      = length(var.public_subnet_cidrs)
 vpc_id     = aws_vpc.main.id
 cidr_block = element(var.public_subnet_cidrs, count.index)

 tags = {
   Name = "Public Subnet ${count.index + 1}"
 }
}

resource "aws_subnet" "private_subnets" {
 count      = length(var.private_subnet_cidrs)
 vpc_id     = aws_vpc.main.id
 cidr_block = element(var.private_subnet_cidrs, count.index)

 tags = {
   Name = "Private Subnet ${count.index + 1}"
 }
}
```

Source: https://spacelift.io/blog/terraform-aws-vpc

161

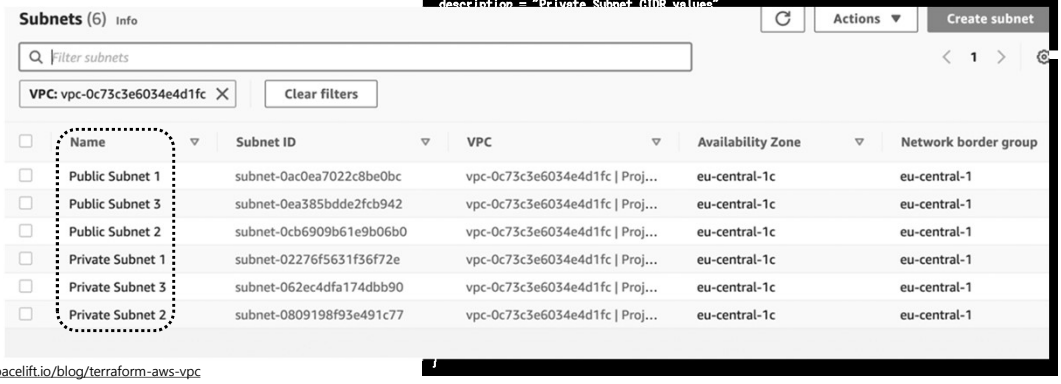
DAY 2. 가상 네트워크 간의 연동

❖ Build AWS VPC using Terraform

- AWS VPC
  - ✓ Create Subnets

```
variable "public_subnet_cidrs" {
 type        = list(string)
 description = "Public Subnet CIDR values"
 default     = ["10.0.1.0/24", "10.0.2.0/24", "10.0.3.0/24"]
}

variable "private_subnet_cidrs" {
 type        = list(string)
 description = "Private Subnet CIDR values"
```



Source: https://spacelift.io/blog/terraform-aws-vpc

162

DAY 2. 가상 네트워크 간의 연동

❖ Build AWS VPC using Terraform

- AWS VPC
  - ✓ Create Subnets

```
variable "azs" {
 type        = list(string)
 description = "Availability Zones"
 default     = ["eu-central-1a", "eu-central-1b", "eu-central-1c"]
}
```

```
resource "aws_subnet" "public_subnets" {
 count             = length(var.public_subnet_cidrs)
 vpc_id            = aws_vpc.main.id
 cidr_block        = element(var.public_subnet_cidrs, count.index)
 availability_zone = element(var.azs, count.index)

 tags = {
   Name = "Public Subnet ${count.index + 1}"
 }
}

resource "aws_subnet" "private_subnets" {
 count             = length(var.private_subnet_cidrs)
 vpc_id            = aws_vpc.main.id
 cidr_block        = element(var.private_subnet_cidrs, count.index)
 availability_zone = element(var.azs, count.index)

 tags = {
   Name = "Private Subnet ${count.index + 1}"
 }
}
```

Source: https://spacelift.io/blog/terraform-aws-vpc

163

DAY 2. 가상 네트워크 간의 연동

❖ Build AWS VPC using Terraform

- AWS VPC
  - ✓ Create Subnets

```
variable "azs" {
  type        = list(string)
  description = "Availability Zones"
  default     = ["eu-central-1a", "eu-central-1b", "eu-central-1c"]
}
```

```
resource "aws_subnet" "public_subnets" {
  count             = length(var.public_subnet_cidrs)
```

Subnets (6) Info

Actions ▼ | Create subnet

Filter subnets

VPC: vpc-0c98ad127b906c06d ✕ | Clear filters

Name	Subnet ID	VPC	Availability Zone	Network border group
Private Subnet 1	subnet-0822129878ed14178	vpc-0c98ad127b906c06d | Pro...	eu-central-1a	eu-central-1
Private Subnet 2	subnet-07422f3a4b2af8808	vpc-0c98ad127b906c06d | Pro...	eu-central-1b	eu-central-1
Private Subnet 3	subnet-0a0bba97e6dfba49e	vpc-0c98ad127b906c06d | Pro...	eu-central-1c	eu-central-1
Public Subnet 1	subnet-05267deb229b1b2dc	vpc-0c98ad127b906c06d | Pro...	eu-central-1a	eu-central-1
Public Subnet 2	subnet-0c1274a75a9b46aa1	vpc-0c98ad127b906c06d | Pro...	eu-central-1b	eu-central-1
Public Subnet 3	subnet-09fb51a9d2433d961	vpc-0c98ad127b906c06d | Pro...	eu-central-1c	eu-central-1

Source: https://spacelift.io/blog/terraform-aws-vpc

164

DAY 2. 가상 네트워크 간의 연동

❖ Build AWS VPC using Terraform

- AWS VPC
  - ✓ Internet Gateway

```
resource "aws_internet_gateway" "gw" {
  vpc_id = aws_vpc.main.id

  tags = {
    Name = "Project VPC IG"
  }
}
```

VPC > Internet gateways > igw-085a905e6fb7e766b

igw-085a905e6fb7e766b / Project VPC IG | Actions ▼

Details Info

Internet gateway ID	State	VPC ID	Owner
igw-085a905e6fb7e766b	Attached	vpc-0c98ad127b906c06d | Project VPC	532199187081

Tags | Manage tags

Search tags

Key	Value
Name	Project VPC IG

Source: https://spacelift.io/blog/terraform-aws-vpc

165

DAY 2. 가상 네트워크 간의 연동

❖ Build AWS VPC using Terraform

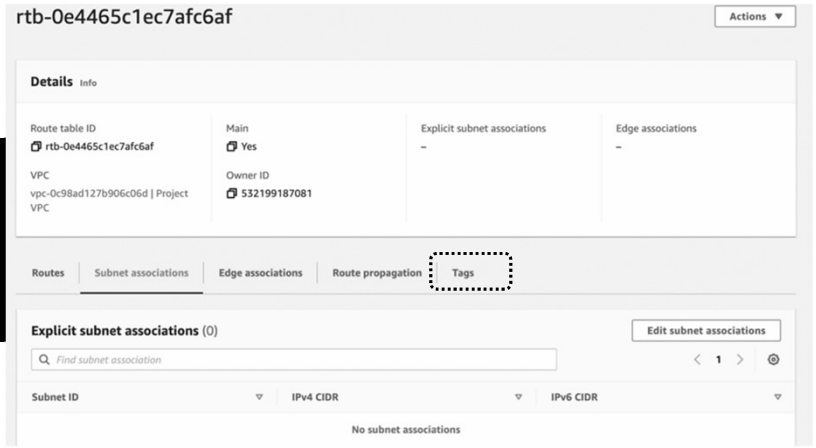
• AWS VPC

✓ Create a 2nd Route Table

```
resource "aws_route_table" "second_rt" {
 vpc_id = aws_vpc.main.id

 route {
   cidr_block = "0.0.0.0/0"
   gateway_id = aws_internet_gateway.gw.id
 }

 tags = {
   Name = "2nd Route Table"
 }
}
```



Source: https://spacelift.io/blog/terraform-aws-vpc

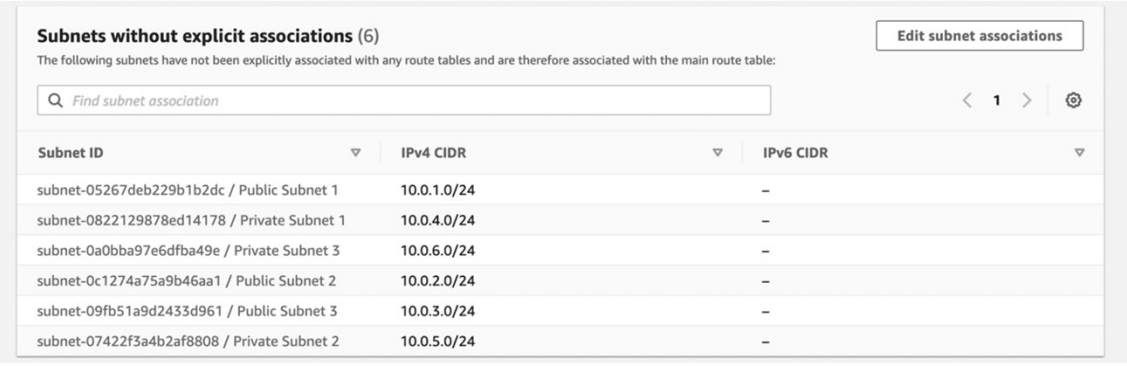
166

DAY 2. 가상 네트워크 간의 연동

❖ Build AWS VPC using Terraform

• AWS VPC

✓ Create a 2nd Route Table



Source: https://spacelift.io/blog/terraform-aws-vpc

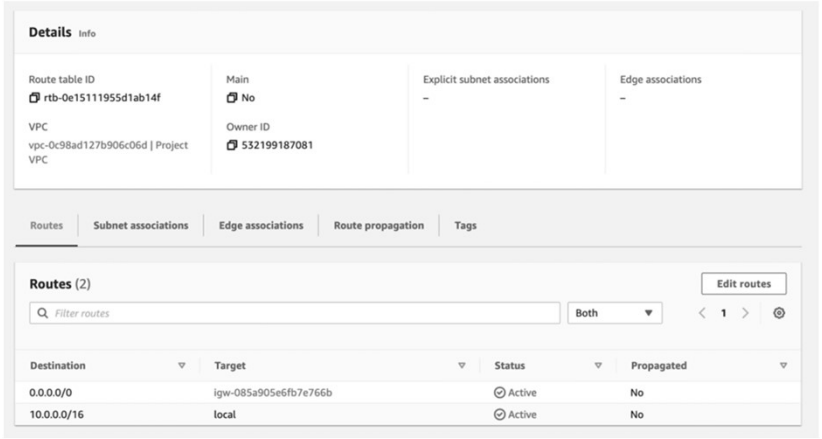
167

DAY 2. 가상 네트워크 간의 연동

❖ Build AWS VPC using Terraform

• AWS VPC

✓ Create a 2nd Route Table



Source: https://spacelift.io/blog/terraform-aws-vpc

168

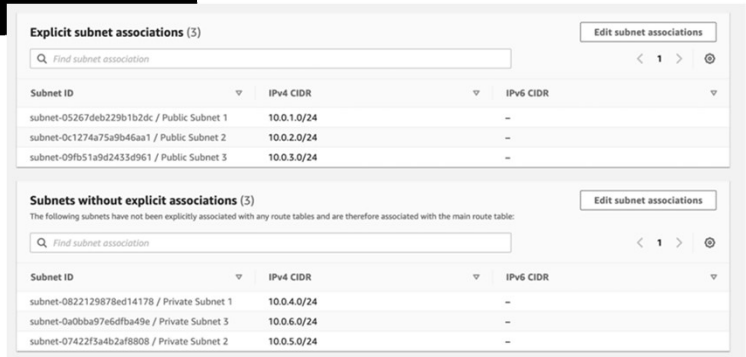
DAY 2. 가상 네트워크 간의 연동

❖ Build AWS VPC using Terraform

• AWS VPC

✓ Associating Public Subnets to the Second Route Table

```
resource "aws_route_table_association" "public_subnet_asso" {
 count = length(var.public_subnet_cidrs)
 subnet_id      = element(aws_subnet.public_subnets[*].id, count.index)
 route_table_id = aws_route_table.second_rt.id
}
```



Source: https://spacelift.io/blog/terraform-aws-vpc

169

DAY 2. 가상 네트워크 간의 연동

❖ AWS: Direct Connect 비용 고려사항

- Port 사용비용/시간 + 데이터 전송료
- 데이터 IN, 데이터 OUT (리전별 상이)
- 전용 회선 비용 (온프레미스-DX로케이션, 크로스,커넥션)
- 데이터센터의 인터넷 회선 비용(VPN)

요금 적용 방식: AWS Direct Connect 요금에는 모든 AWS Direct Connect 위치에 대한 포트-시간당 요금과 AWS Direct Connect 위치에서의 데이터 전송 요금이라는 두 가지 주요 비용 구성 요소가 있다. 각 비용 구성 요소에 대한 세부 정보는 AWS Direct Connect 요금을 참조.
예상 비용: 미 동부 리전인 버지니아에 대해 1GB의 연결을 주문하고 매달 1TB를 전송할 것으로 예상한다고 가정시 포트-시간당 요금 0.30 USD, GB당 데이터 전송 요금 0.02 USD를 적용. 따라서 1TB의 데이터 전송 요금은 포트 요금 216 USD에 데이터 전송 요금 20 USD를 합쳐 한 달에 총 236 USD가 소요.

Source: https://aws.amazon.com/ko/getting-started/hands-on/connect-data-center-to-aws/services-costs/
Source: https://www.youtube.com/watch?v=jdnrgVxRXJ0

DAY 2. 가상 네트워크 간의 연동

❖ Private peering or private network interconnect

- Private peering is the direct interconnection between two networks. This connection leverages a medium OSI, layer 1 or 2, with dedicated bandwidth. Private peering is not shared by any other network or third party.
- Nowadays, most private interconnections are established at carrier hotels or carrier-neutral collocation facilities called meet-me rooms. These are facilities in which a direct cross-connection can be provided between participants that are located in the same building or at the same data center campus.
- These network-to-network interconnects usually have much lower costs than telecommunication circuits.

A telco circuit is any line or provider that information or data is transmitted through.

Source: Multi-Cloud for Architects (Published by Packt Publishing Ltd) Florian Klaffenbach, Markus Klein, Suresh Sundaresan

DAY 2. 가상 네트워크 간의 연동

❖ **Internet direct peering or public peering and remote peering**

- **Public peering is accomplished across an exchange point, internet exchange, or a layer 2 access technology called a network access point. At these locations, multiple providers interconnect with one or more other carriers across a single physical port.**
- **Public peering allows networks to interconnect, or "peer", with many other networks. Public peering, is often seen as offering a lower capacity than private peering because there are third-party costs for the internet exchange, but it allows for the connection to a larger number of networks. It also allows new network or content providers to send traffic to other networks without private peering.**

Most of the internet exchange points are commercially organized and offer carrier-neutral peering. The two most important conferences for those peers are the Global Peering Forum and the European Peering Forum.

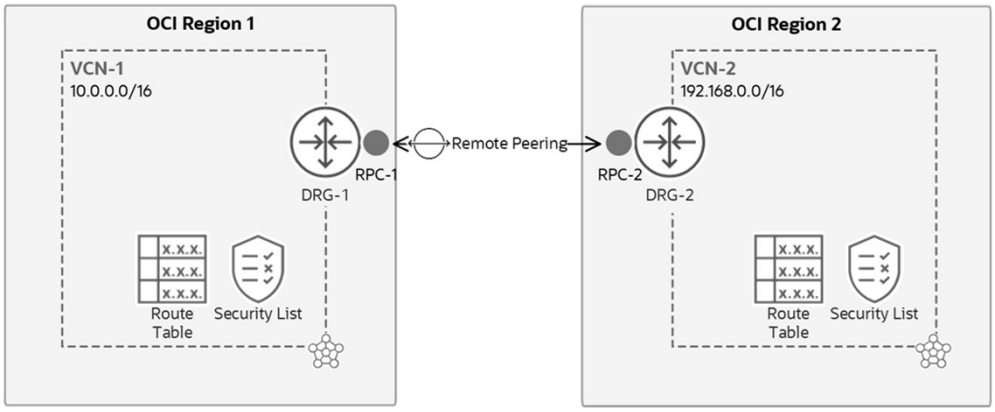
Source: Multi-Cloud for Architects (Published by Packt Publishing Ltd) Florian Klaffenbach, Markus Klein, Suresh Sundaresan

172

DAY 2. 가상 네트워크 간의 연동

❖ **리전(Region)간 Remote Peering (OCI VPN)**

- **Oracle Cloud Infrastructure (OCI) - Virtual Cloud Network (VCN)**



Source: https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/remoteVCNpeering.htm

173

DAY 2. 가상 네트워크 간의 연동

❖ **Amazon VPC, VPC 피어링 요금** (게시된 날짜: May 5, 2021)

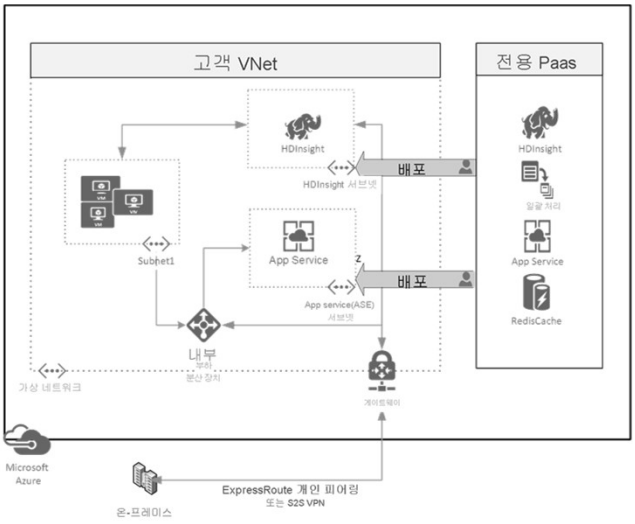
- 가용 영역(AZ) 내에 유지되는 VPC 피어링 연결을 통한 모든 데이터 전송은 무료
- 가용 영역을 가로지르는 VPC 피어링 연결을 통한 모든 데이터 전송은 계속 리전 내 표준 데이터 전송 요금이 청구
- 가용 영역 ID를 사용하면 서로 다른 AWS 계정 간에서 가용 영역을 고유하고 일관되게 식별
- 고객은 한 리전 내에서 VPC를 상호 연결하기 위해 VPC 피어링을 사용
- VPC 피어링은 한 리전에서 적은 수의 VPC를 상호 연결하여 전체 메시 연결성을 달성하려고 할 때 일반적으로 사용
- 대규모로 수백 또는 수천 개의 VPC를 상호 연결하려면 AWS Transit Gateway 및 AWS PrivateLink가 권장 메커니즘
- 이 변경 사항은 AWS Gov Cloud(US) 리전을 포함한 모든 AWS 리전에 적용

Source: https://aws.amazon.com/ko/about-aws/whats-new/2021/05/amazon-vpc-announces-pricing-change-for-vpc-peering/

174

DAY 2. 가상 네트워크 간의 연동

❖ **가상 네트워크에 전용 Azure 서비스 배포**



Source: https://docs.microsoft.com/ko-kr/azure/virtual-network/virtual-network-for-azure-services

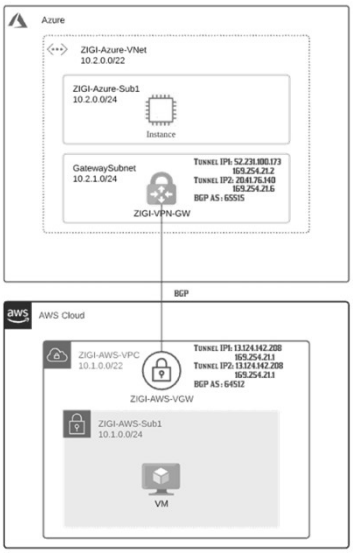
175

DAY 2. 가상 네트워크 간의 연동

❖ 'Azure – AWS' 간의 VPN 연동 및 BGP 연결

BGP AS 65515

BGP AS 64512



Source: https://devocean.sk.com/blog/techBoardDetail.do?ID=163211

176

DAY 2. 가상 네트워크 간의 연동

❖ eBGP configuration 연결 (예): VyOS

- the CIDR declared in the network statement MUST exist in your routing table (dynamic or static), the best way to make sure that is true is creating a static route

Node 1:

```
set protocols bgp 65534 neighbor 192.168.0.2 ebgp-multihop '2'
set protocols bgp 65534 neighbor 192.168.0.2 remote-as '65535'
set protocols bgp 65534 neighbor 192.168.0.2 update-source '192.168.0.1'
set protocols bgp 65534 address-family ipv4-unicast network '172.16.0.0/16'
set protocols bgp 65534 parameters router-id '192.168.0.1'
```

```
set protocols static route 172.16.0.0/16 blackhole distance '254'
```

Node 2:

```
set protocols bgp 65535 neighbor 192.168.0.1 ebgp-multihop '2'
set protocols bgp 65535 neighbor 192.168.0.1 remote-as '65534'
set protocols bgp 65535 neighbor 192.168.0.1 update-source '192.168.0.2'
set protocols bgp 65535 address-family ipv4-unicast network '172.17.0.0/16'
set protocols bgp 65535 parameters router-id '192.168.0.2'
```

```
set protocols static route 172.17.0.0/16 blackhole distance '254'
```

Source: https://docs.vyos.io/en/crux/configuration/protocols/bgp.html

177

DAY 2. 가상 네트워크 간의 연동

❖ eBGP configuration 연결 (예): VyOS

• BGP configuration via IPv6

Node 1:

```
set protocols bgp 65534 neighbor 2001:db8::2 ebgp-multihop '2'
set protocols bgp 65534 neighbor 2001:db8::2 remote-as '65535'
set protocols bgp 65534 neighbor 2001:db8::2 update-source '2001:db8::1'
set protocols bgp 65534 neighbor 2001:db8::2 address-family ipv6-unicast
set protocols bgp 65534 address-family ipv6-unicast network '2001:db8:1::/48'
set protocols bgp 65534 parameters router-id '10.1.1.1'
```

```
set protocols static route6 2001:db8:1::/48 blackhole distance '254'
```

Node 2:

```
set protocols bgp 65535 neighbor 2001:db8::1 ebgp-multihop '2'
set protocols bgp 65535 neighbor 2001:db8::1 remote-as '65534'
set protocols bgp 65535 neighbor 2001:db8::1 update-source '2001:db8::2'
set protocols bgp 65535 neighbor 2001:db8::1 address-family ipv6-unicast
set protocols bgp 65535 address-family ipv6-unicast network '2001:db8:2::/48'
set protocols bgp 65535 parameters router-id '10.1.1.2'
```

```
set protocols static route6 2001:db8:2::/48 blackhole distance '254'
```

Source: https://docs.vyos.io/en/crux/configuration/protocols/bgp.html

178

DAY 2. 가상 네트워크 간의 연동

❖ eBGP configuration 연결 (예): VyOS

• Route Filter

Node 1:

```
set policy prefix-list AS65535-IN rule 10 action 'permit'
set policy prefix-list AS65535-IN rule 10 prefix '172.16.0.0/16'
set policy prefix-list AS65535-OUT rule 10 action 'deny'
set policy prefix-list AS65535-OUT rule 10 prefix '172.16.0.0/16'
set policy prefix-list6 AS65535-IN rule 10 action 'permit'
set policy prefix-list6 AS65535-IN rule 10 prefix '2001:db8:2::/48'
set policy prefix-list6 AS65535-OUT rule 10 action 'deny'
set policy prefix-list6 AS65535-OUT rule 10 prefix '2001:db8:2::/48'
set policy route-map AS65535-IN rule 10 action 'permit'
set policy route-map AS65535-IN rule 10 match ip address prefix-list 'AS65535-IN'
set policy route-map AS65535-IN rule 10 match ipv6 address prefix-list 'AS65535-IN'
set policy route-map AS65535-IN rule 20 action 'deny'
set policy route-map AS65535-OUT rule 10 action 'deny'
set policy route-map AS65535-OUT rule 10 match ip address prefix-list 'AS65535-OUT'
set policy route-map AS65535-OUT rule 10 match ipv6 address prefix-list 'AS65535-OUT'
set policy route-map AS65535-OUT rule 20 action 'permit'
set protocols bgp 65534 neighbor 2001:db8::2 address-family ipv6-unicast route-map export 'AS65535-OUT'
set protocols bgp 65534 neighbor 2001:db8::2 address-family ipv6-unicast route-map import 'AS65535-IN'
set protocols bgp 65534 neighbor 192.168.0.2 address-family ipv4-unicast route-map export 'AS65535-OUT'
set protocols bgp 65534 neighbor 192.168.0.2 address-family ipv4-unicast route-map import 'AS65535-IN'
```

Node 2:

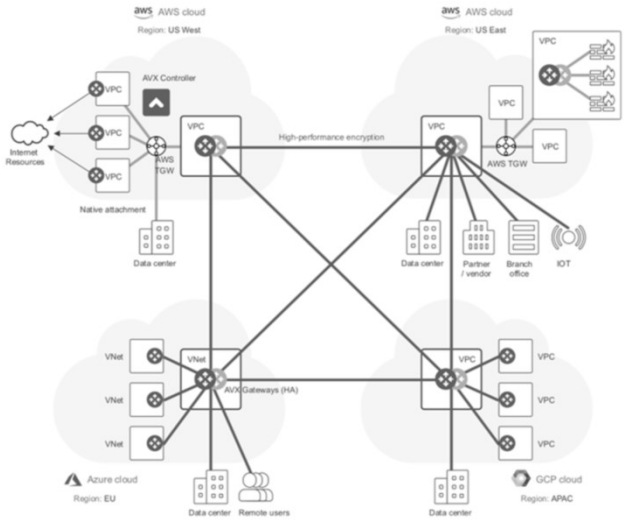
```
set policy prefix-list AS65534-IN rule 10 action 'permit'
set policy prefix-list AS65534-IN rule 10 prefix '172.17.0.0/16'
set policy prefix-list AS65534-OUT rule 10 action 'deny'
set policy prefix-list AS65534-OUT rule 10 prefix '172.17.0.0/16'
set policy prefix-list6 AS65534-IN rule 10 action 'permit'
set policy prefix-list6 AS65534-IN rule 10 prefix '2001:db8:1::/48'
set policy prefix-list6 AS65534-OUT rule 10 action 'deny'
set policy prefix-list6 AS65534-OUT rule 10 prefix '2001:db8:1::/48'
set policy route-map AS65534-IN rule 10 action 'permit'
set policy route-map AS65534-IN rule 10 match ip address prefix-list 'AS65534-IN'
set policy route-map AS65534-IN rule 10 match ipv6 address prefix-list 'AS65534-IN'
set policy route-map AS65534-IN rule 20 action 'deny'
set policy route-map AS65534-OUT rule 10 action 'deny'
set policy route-map AS65534-OUT rule 10 match ip address prefix-list 'AS65534-OUT'
set policy route-map AS65534-OUT rule 10 match ipv6 address prefix-list 'AS65534-OUT'
set policy route-map AS65534-OUT rule 20 action 'permit'
set protocols bgp 65535 neighbor 2001:db8::1 address-family ipv6-unicast route-map export 'AS65534-OUT'
set protocols bgp 65535 neighbor 2001:db8::1 address-family ipv6-unicast route-map import 'AS65534-IN'
set protocols bgp 65535 neighbor 192.168.0.1 address-family ipv4-unicast route-map export 'AS65534-OUT'
set protocols bgp 65535 neighbor 192.168.0.1 address-family ipv4-unicast route-map import 'AS65534-IN'
```

Source: https://docs.vyos.io/en/crux/configuration/protocols/bgp.html

179

DAY 2. 가상 네트워크 간의 연동

❖ **기업용 Multi-Cloud Backbone** (Aviatrix 예)



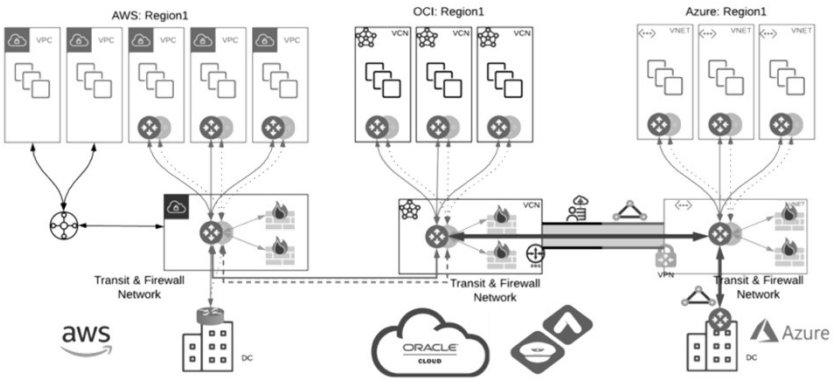
Source: https://www.simform.com/compute-pricing-comparison-aws-azure-googlecloud/

180

DAY 2. 가상 네트워크 간의 연동

❖ **가상 네트워크 환경을 위한 VCN 만들기 - Oracle Cloud Infrastructure** (Aviatrix 예)

- **Oracle OCI — multi-region transit connectivity with Aviatrix MCNA**



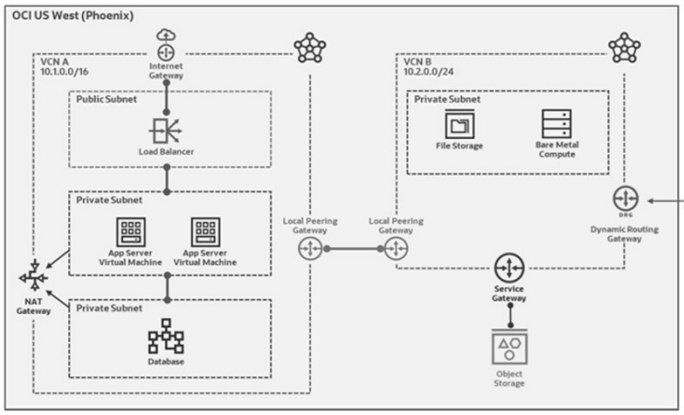
Source: https://aviatrix.com/oracle-oci-multi-region-transit-connectivity/

181

DAY 2. 가상 네트워크 간의 연동

❖ 가상 네트워크 환경을 위한 VCN 만들기 - Oracle Cloud Infrastructure (Aviatrix 예)

• Oracle OCI — multi-region transit connectivity with Aviatrix MCNA



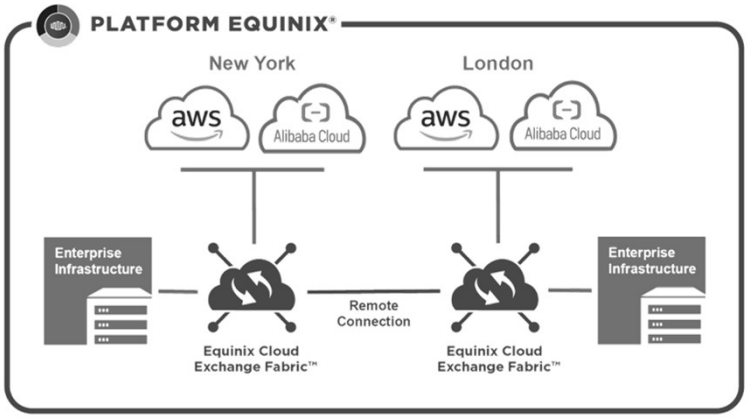
Source: https://aviatrix.com/oracle-oci-multi-region-transit-connectivity/

182

DAY 2. 가상 네트워크 간의 연동

❖ Cloud "On-Ramp" Service Provider (예): Equinix

• Hybrid Multicloud - business continuity/disaster recovery



EQUINIX | INTERCONNECTIONS

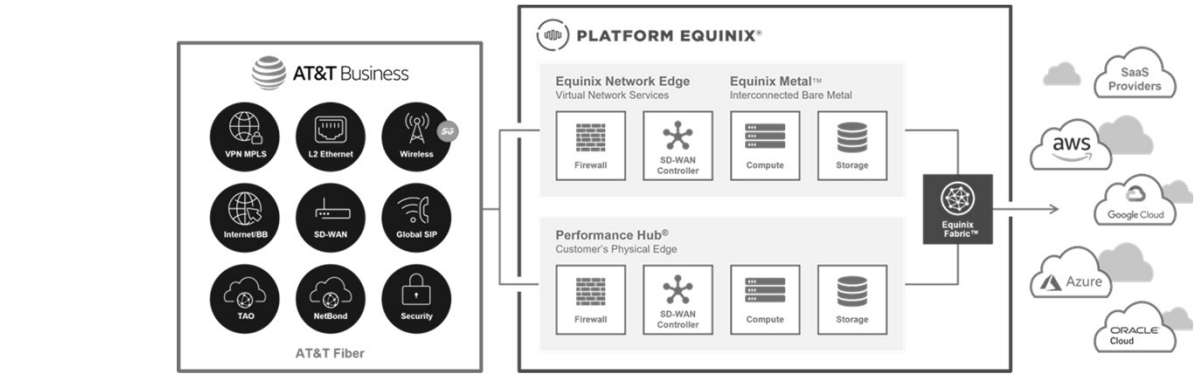
Source: https://blog.equinix.com/blog/2020/07/31/equinix-and-alibaba-are-extending-the-reach-of-hybrid-multicloud/

183

DAY 2. 가상 네트워크 간의 연동

❖ Cloud "On-Ramp" Service Provider (예): Equinix

• Equinix Fabric Use Cases for Network Service Providers



EQUINIX | INTERCONNECTIONS

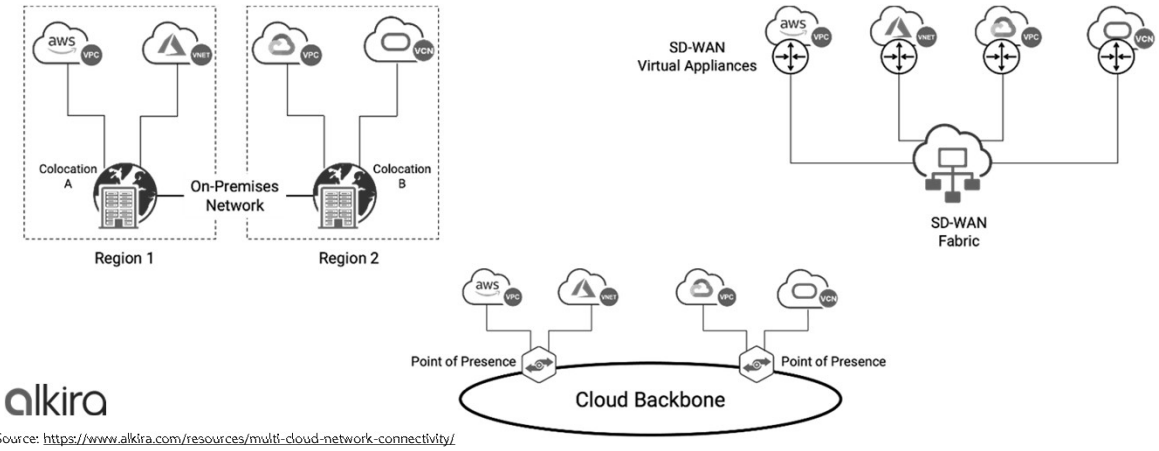
Source: https://blog.equinix.com/blog/2022/07/11/5-equinix-fabric-use-cases-for-network-service-providers/

184

DAY 2. 가상 네트워크 간의 연동

❖ 제조사 (예): Alkira

• Multi-Cloud Network Connectivity



alkira

Source: https://www.alkira.com/resources/multi-cloud-network-connectivity/

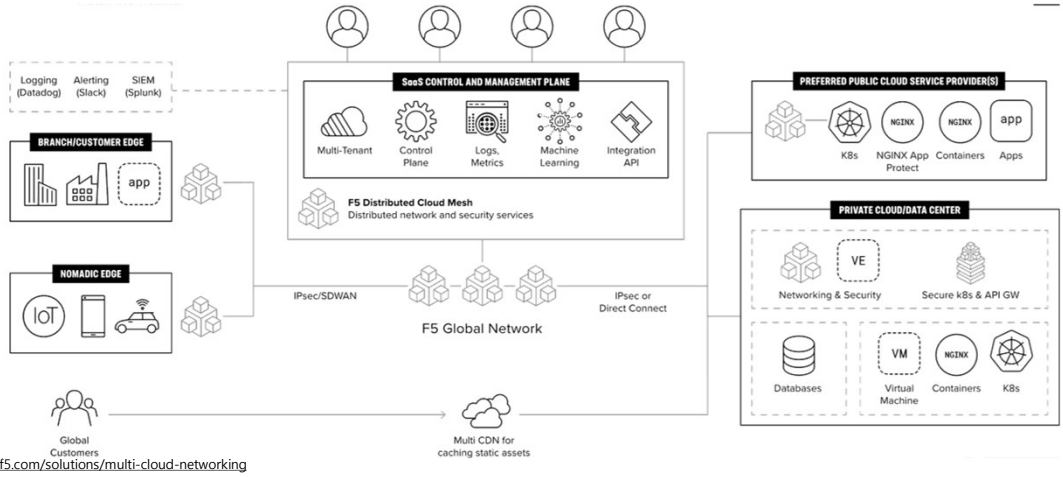
185

DAY 2. 가상 네트워크 간의 연동

186

❖ 제조사 (예): F5

• SaaS for Multi-Cloud Network



Source: https://www.f5.com/solutions/multi-cloud-networking

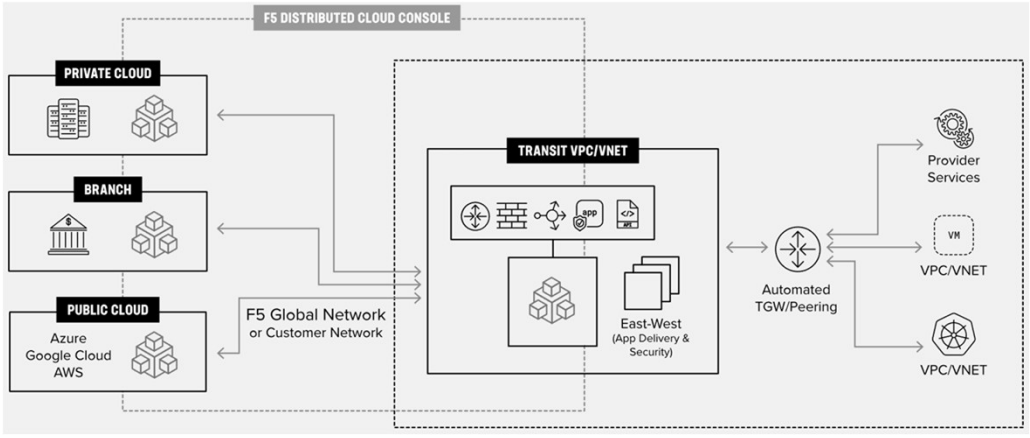
186

DAY 2. 가상 네트워크 간의 연동

187

❖ 제조사 (예): F5

• Distributed Cloud Multi-Cloud Transit



Source: https://www.f5.com/solutions/multi-cloud-networking

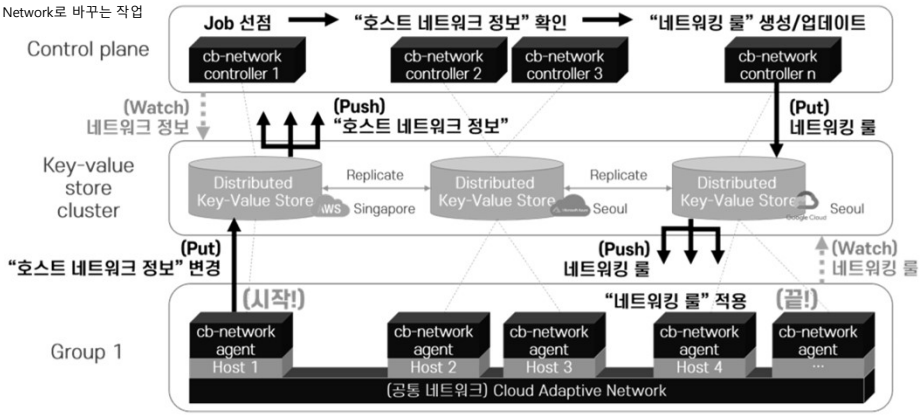
187

DAY 2. 가상 네트워크 간의 연동

❖ 네트워크 정보 동적 업데이트 기술 (ETRI)

- 가상네트워크 지원(CB-Larva)
- Supernetting 지원(CB-Tumblebug)

여러개의 작은 Network를 하나의 커다란 Network로 바꾸는 작업



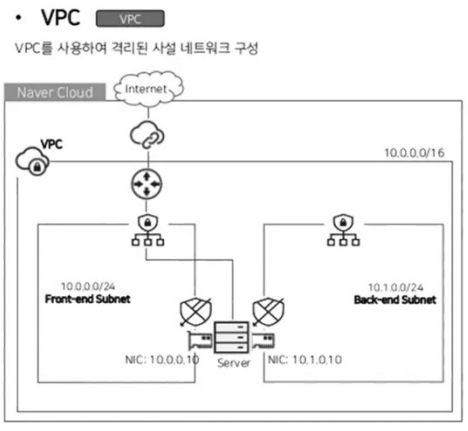
Source: @ ETRI Conference 2022 '멀티클라우드 가상네트워크 기술' (김윤곤) 참조

188

DAY 2. 가상 네트워크 간의 연동

❖ 네이버클라우드플랫폼 (2020)

- 네트워크 보안



Virtual Private Cloud

- 논리적으로 분리된 가상 사설망 제공
- VPC 상에서 사설 IP대역 을 선택
- 서비스별 서브넷팅 후 VM배치

Network Security

- 외부로 부터 트래픽과 라우팅 통제
- 소유하지 않은 VM에 대한 스니핑 불가
- IP Spooping 과 같은 Layer 2 공격차단

Source: https://www.slideshare.net/n_cloudplatform/ss-239153998

189

DAY 2. 가상 네트워크 간의 연동

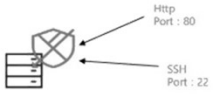
❖ 네이버클라우드플랫폼 (2020)

• 네트워크 보안

• ACG (Access Control Group)

VM 단위 Stateful 방화벽

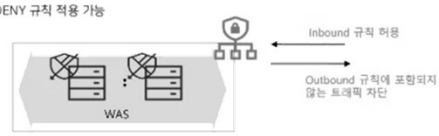
인바운드/아웃바운드 트래픽 , IP/Port 에 대한 허용/차단



• NACL (Network ACL)

서브넷 단위 Stateless 적용

DENY 규칙 적용 가능



[ACG / NACL 비교]

구분	ACG	NACL
적용 대상	서버의 접근 제어	Subnet의 접근 제어
지원 규칙	허용 (Allow)	허용 및 거부 (Allow/Deny)
상태 저장 여부	상태 저장 (규칙에 관계없이 반환 트래픽이 자동으로 허용됨)	상태 비저장 (반환 트래픽이 규칙에 의해 명시적으로 허용되어야 함)
적용 방법	서버의 NIC에 ACG 정책 적용	Subnet 단위로 적용 (Subnet 별 1개만 허용)

Source: https://www.slideshare.net/n_cloudplatform/ss-239153998

190

409