AWS VPC 구축이론 및 VPC 중심 네트워크 구성하기

김재현

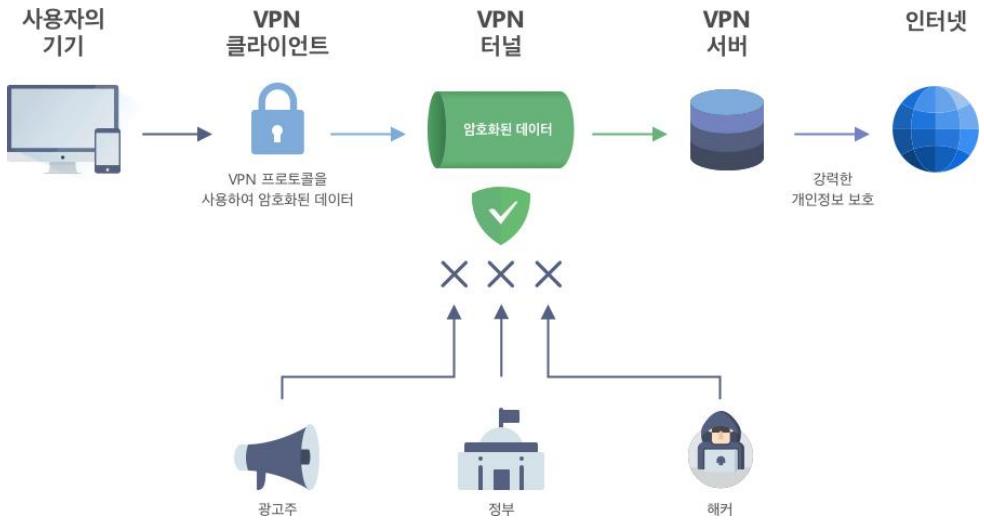
목차

- AWS VPC
- VPC 중심 네트워크 구성
- Hybrid Networking

AWS VPC

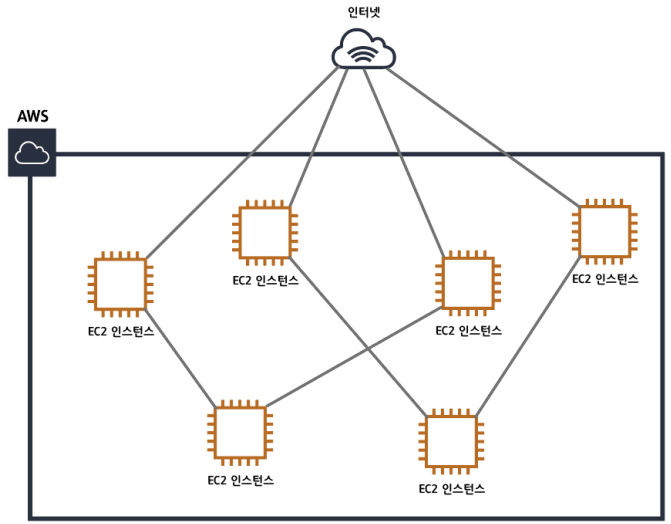
Virtual Private Network(VPN)

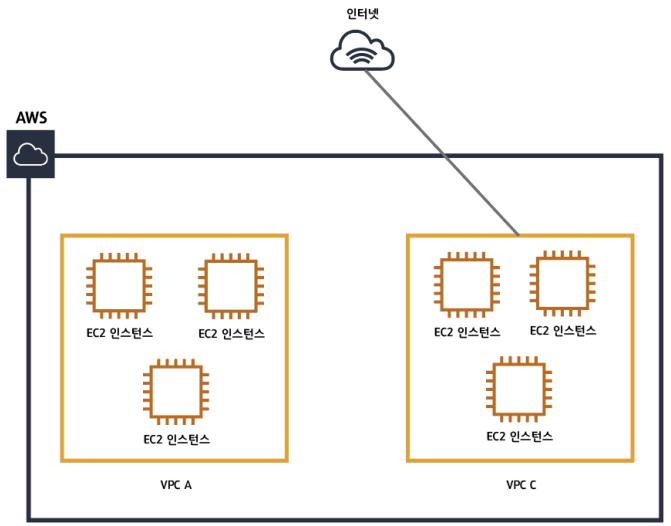
- VPN은 인터넷을 통해 디바이스 간에 네트워크 연결을 생성한다.
- VPN은 퍼블릭 네트워크를 통해 데이터를 안전하게 익명으로 전송하는 데 사용된다.
- 또한 사용자 IP주소를 마스킹하고 데이터를 암호화하여 수신 권한이 없는 사람이 읽을 수 없도록 한다.



AWS VPC

- Amazon Virtual Private Cloud(Amazon VPC)는 사용자가 정의한 가상 네트워크이다.
- 사용자가 구성요소들을 이용하여 원하는 형태로 네트워크망을 구축할 수 있다.





VPC 구성요소

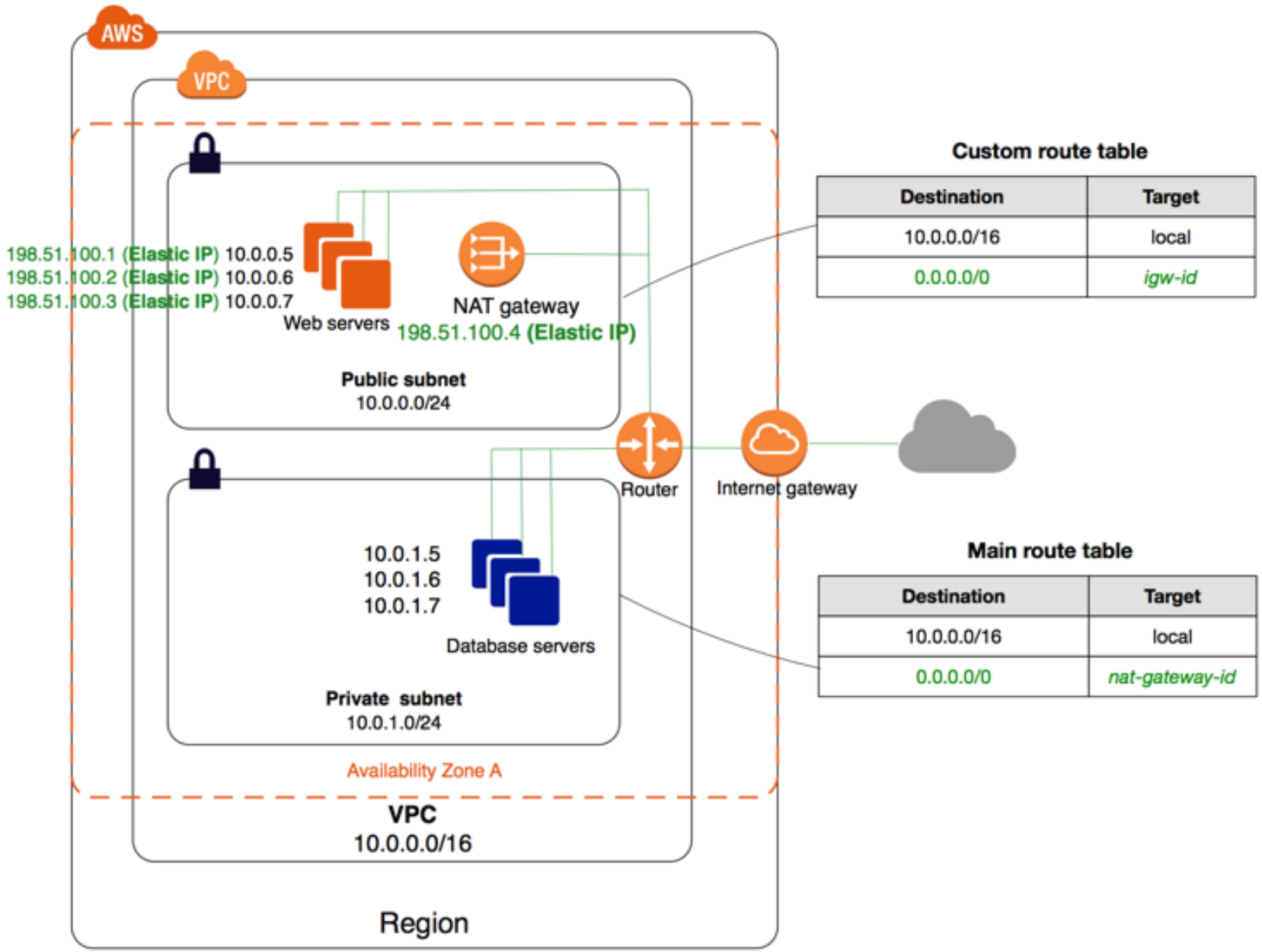
Subnet – VPC를 특정 범위로 나눈 범위

RouteTable – 네트워크 트래픽을 전달한 위치가 명시된 규칙 집합 테이블

Internet GW – VPC의 리소스에서의 인터넷 통신을 활성화하기 위한 게이트 웨이

NAT GW – 네트워크 주소 변환을 통해 private subnet에서 인터넷 통신을 연결하는 게이트웨이

VPC endpoint – NAT, IGW 등을 통하지 않고 AWS의 서비스를 비공개로 연결 가능하게 하는 서비스



Custom route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*igw-id*

Main route table

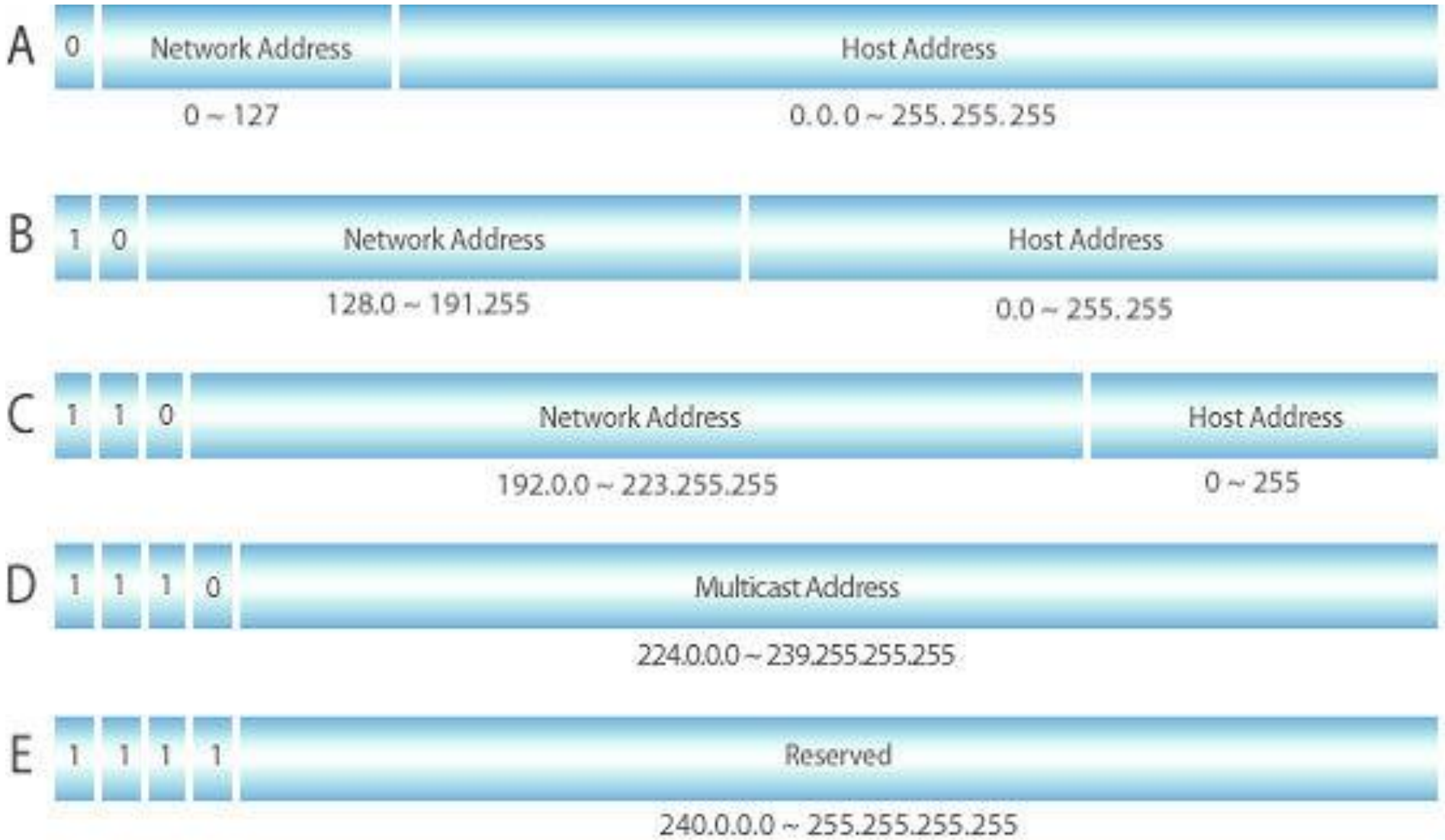
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*nat-gateway-id*

CIDR(Classless Inter-Domain Routing)

- 클래스 없이 유연하게 네트워크 영역을 나누어 IP주소를 할당하는 방식

255.255.255.255

00000000.00000000.00000000.00000000


A
0
Network Address
Host Address
0 ~ 127
0.0.0 ~ 255.255.255
B
1
0
Network Address
Host Address
128.0 ~ 191.255
0.0 ~ 255.255
C
1
1
0
Network Address
Host Address
192.0.0 ~ 223.255.255
0 ~ 255
D
1
1
1
0
Multicast Address
224.0.0.0 ~ 239.255.255.255
E
1
1
1
1
Reserved
240.0.0.0 ~ 255.255.255.255

클래스 구분 체계

CIDR는 /16, /24, /32 로 사용한다

/16 **00000000.00000000**.00000000.00000000

/24 **00000000.00000000.00000000**.00000000

/32 **00000000.00000000.00000000.00000000**

Ex) IP주소가 10.0.1.0/16 일 때

00001010.00000000.00000001.00000000

즉 10.0.1.0/16의 CIDR 그룹에는 10.0.1.0 부터 10.0.255.255가 된다

Ex) IP주소가 10.0.1.0/24 일 때

00001010.00000000.**00000001**.00000000

즉 10.0.1.0/16의 CIDR 그룹에는 10.0.0.0 부터 10.0.1.255가 된다

Default VPC components

When we create a default VPC, we do the following to set it up for you:

- Create a VPC with a size `/16` IPv4 CIDR block (`172.31.0.0/16`). This provides up to 65,536 private IPv4 addresses.
- Create a size `/20` default subnet in each Availability Zone. This provides up to 4,096 addresses per subnet, a few of which are reserved for our use.
- Create an internet gateway and connect it to your default VPC.
- Add a route to the main route table that points all traffic (`0.0.0.0/0`) to the internet gateway.
- Create a default security group and associate it with your default VPC.
- Create a default network access control list (ACL) and associate it with your default VPC.
- Associate the default DHCP options set for your AWS account with your default VPC.

> **Note**
>
> Amazon creates the above resources on your behalf. IAM policies do not apply to these actions because you do not perform these actions. For example, if you have an IAM policy that denies the ability to call CreateInternetGateway, and then you call CreateDefaultVpc, the internet gateway in the default VPC is still created.

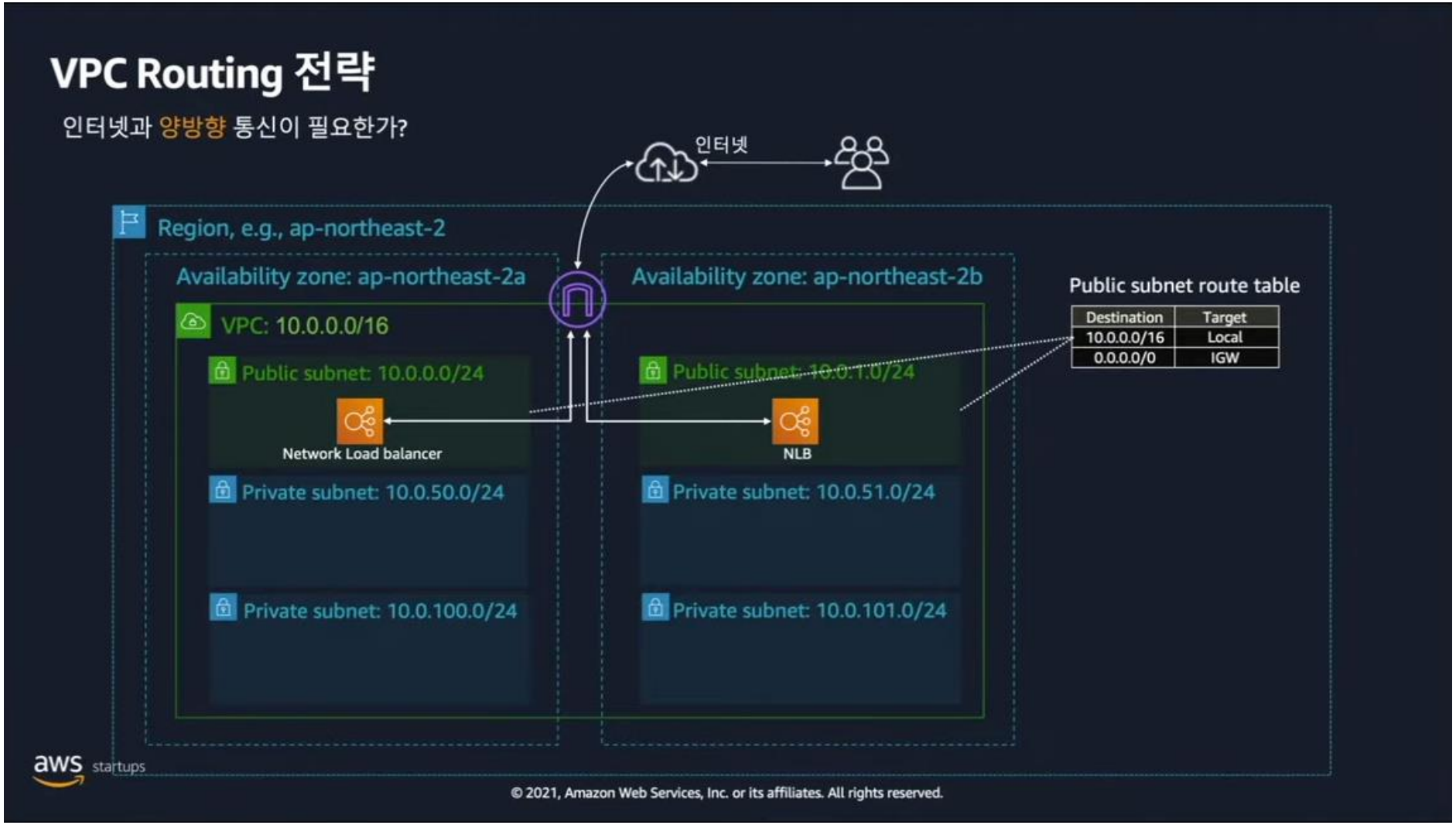
VPC 중심 네트워크 구성

VPC 대역 정하기

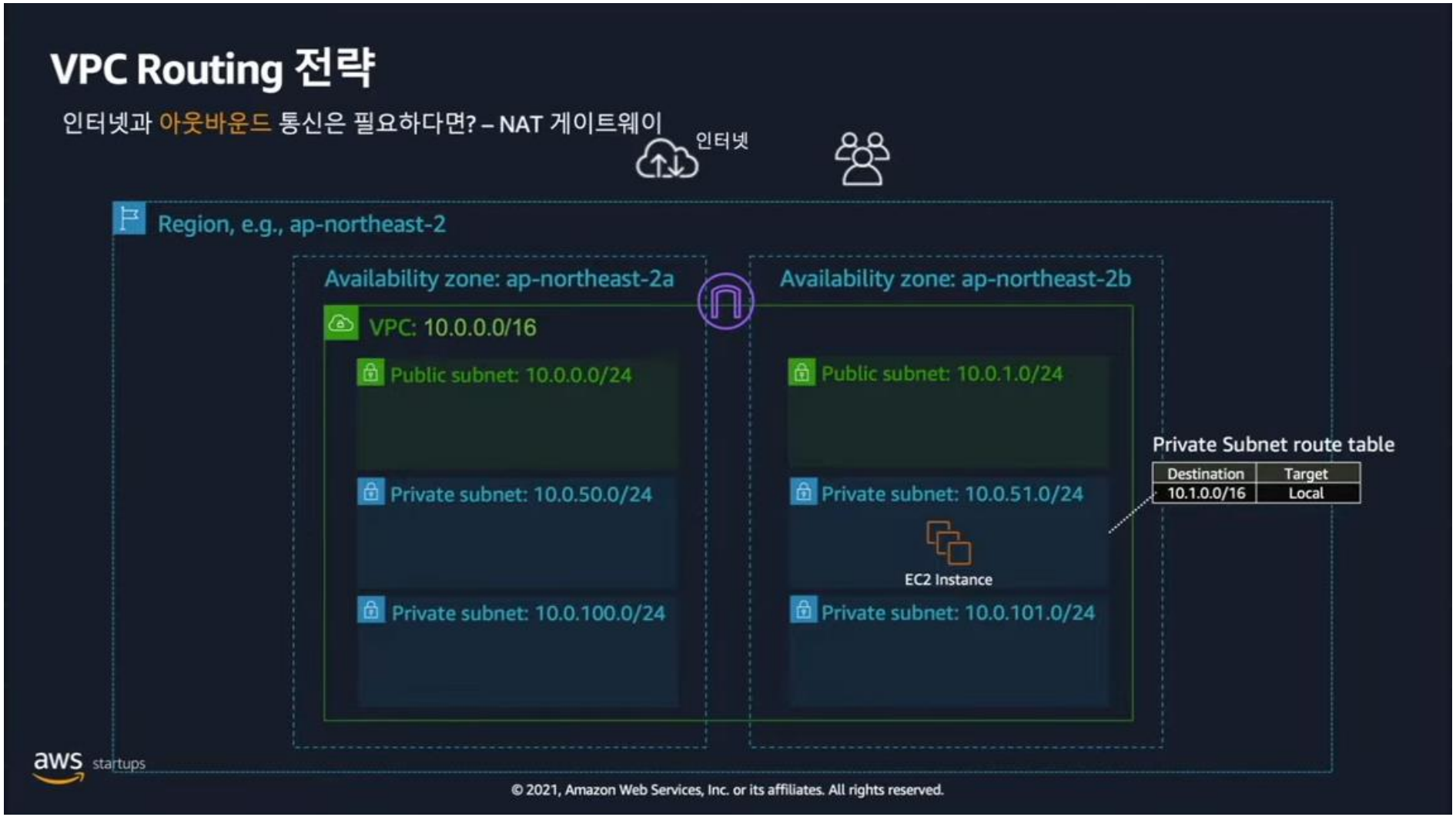
- IPv4의 경우 /16(65,536) ~ /28(16개) 넷마스크 허용
- RFC 1918에 정의된 사설 IP대역 사용 권장
  - **10.0.0.0/8:** 10.0.0.0 ~ 10.255.255.255
  - **172.16.0.0/12:** 172.16.0.0 ~ 172.31.255.255
  - **192.168.0.0/16:** 192.168.0.0 ~ 192.168.255.255
- VPC CIDR 변경 불가, 대역 추가는 가능
  - (선택사항) IPv6sms VPC 대역은 /56, 각 서브넷은 /64 고정
- 서브넷마다 예약된 IP 고려 필요 (예: 10.1.0.0/24)
  - **10.1.0.0:** 네트워크 주소
  - **10.1.0.1:** AWS에서 VPC 라우터용으로 예약
  - **10.1.0.2:** AWS에서 예약
  - **10.1.0.3:** AWS에서 나중에 사용하려고 예약
  - **10.1.0.255:** 네트워크 브로드캐스트 주소

VPC Subnetting

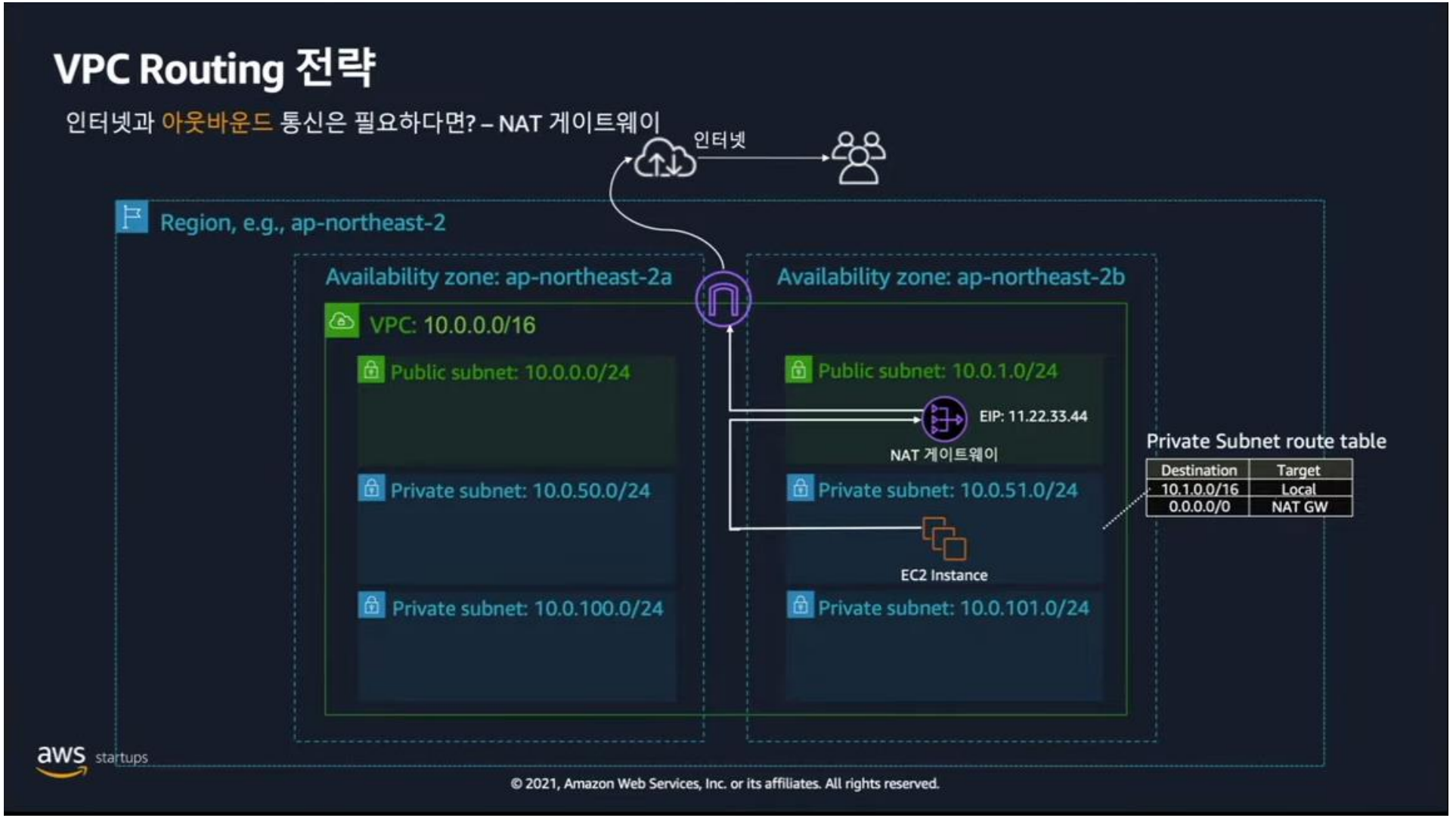
VPC Routing 전략



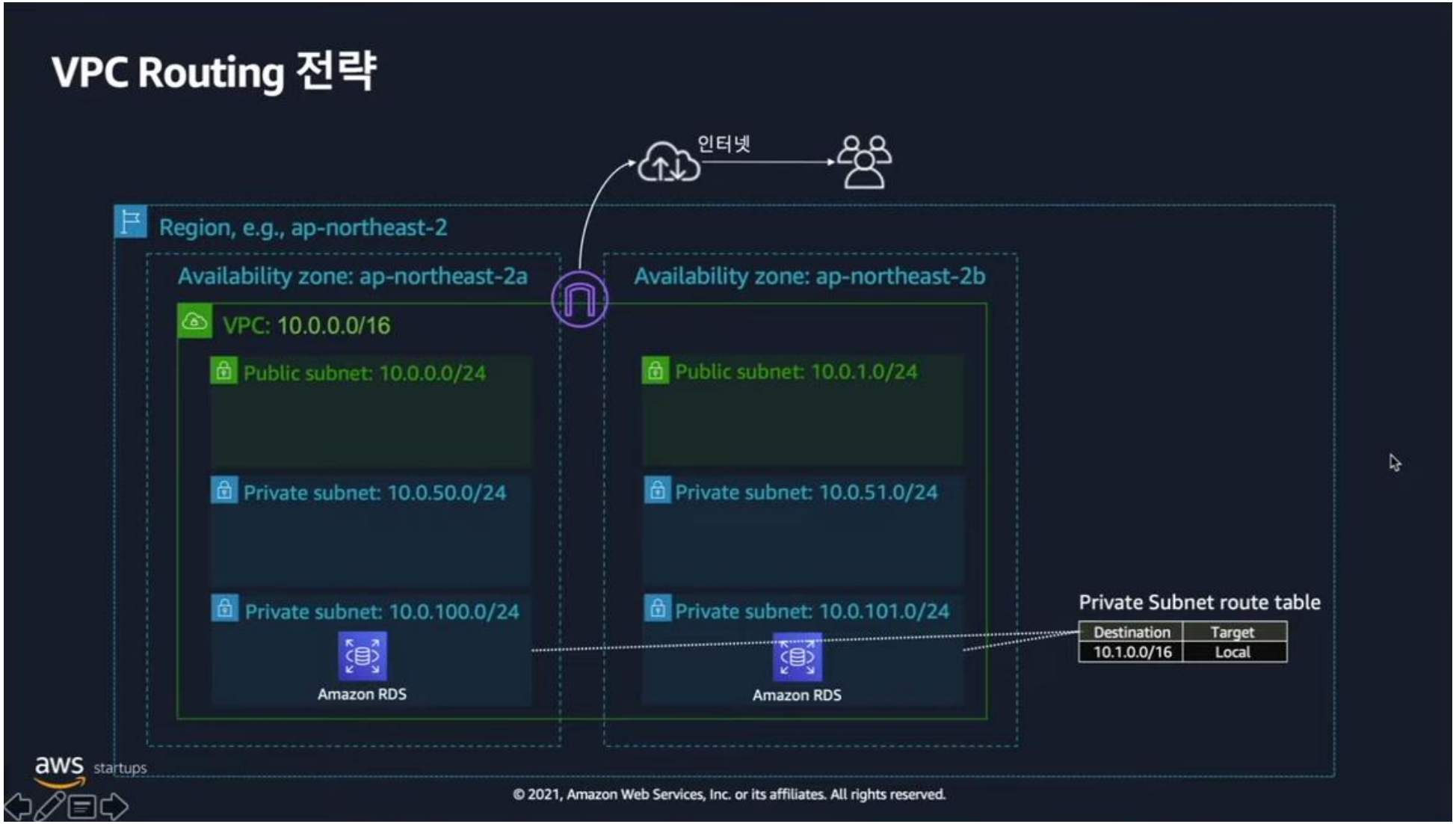
VPC Routing 전략



VPC Routing 전략

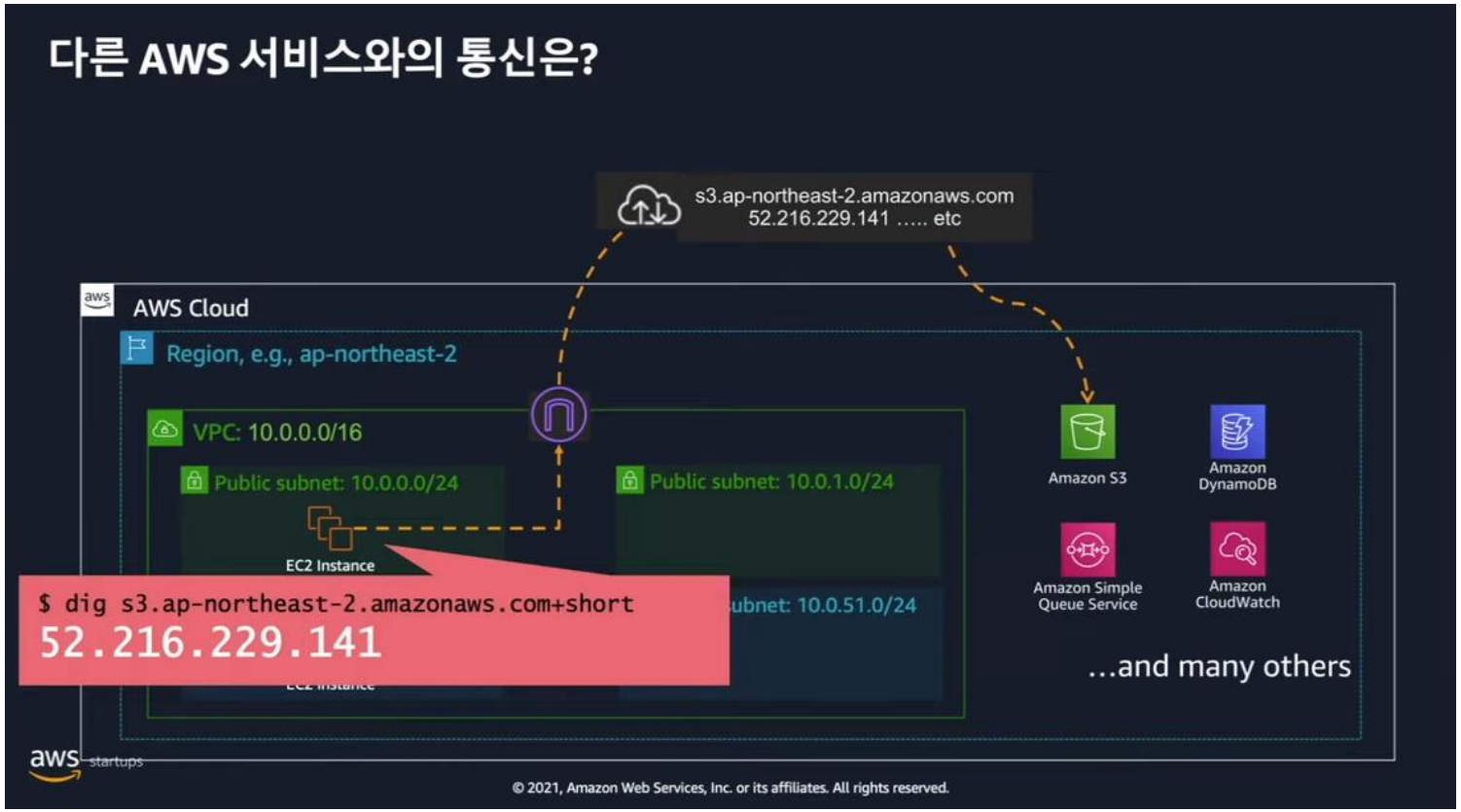


VPC Routing 전략



Hybrid Networking

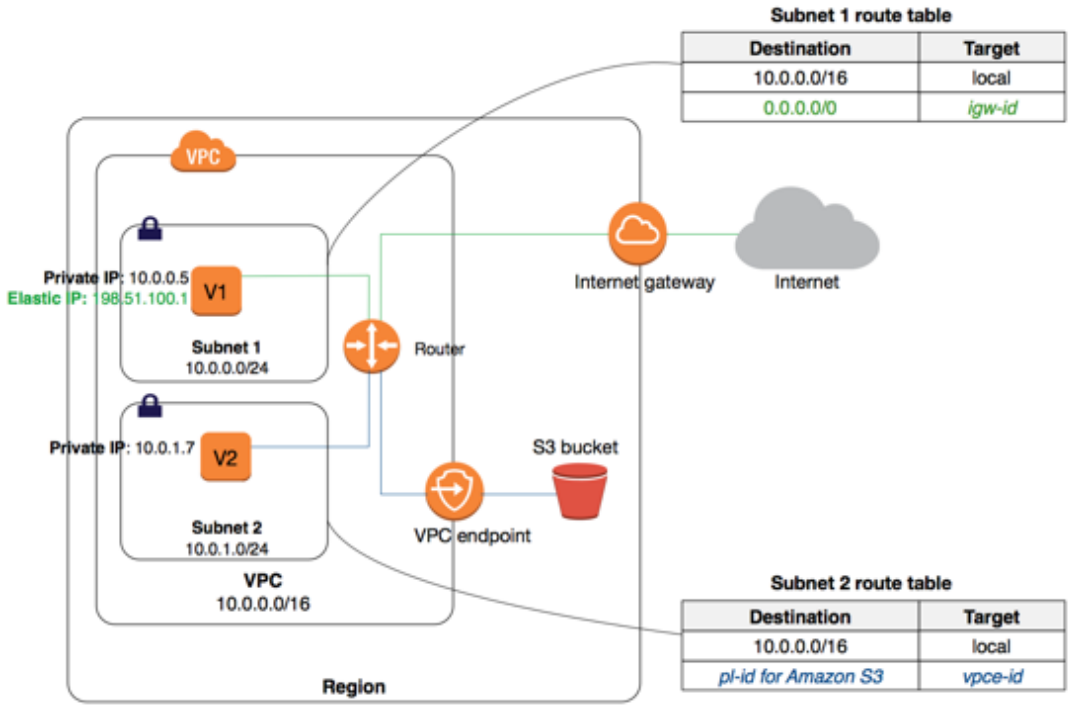
Hybrid Networking



1. 게이트웨이 엔드포인트
2. 인터페이스 엔드포인트(PrivateLink)

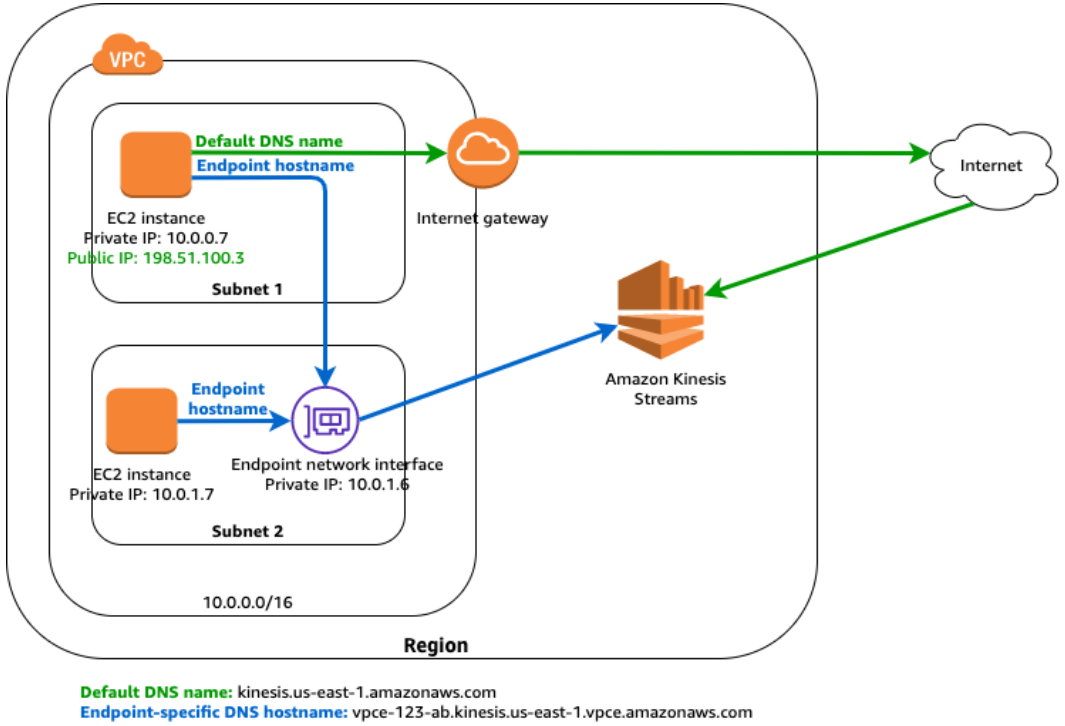
Gateway Endpoint

- 게이트웨이 엔드포인트는 VPC용 인터넷 게이트웨이 또는 NAT 디바이스가 없어도 Amazon S3 및 DynamoDB에 대한 안정적인 연결을 제공한다.

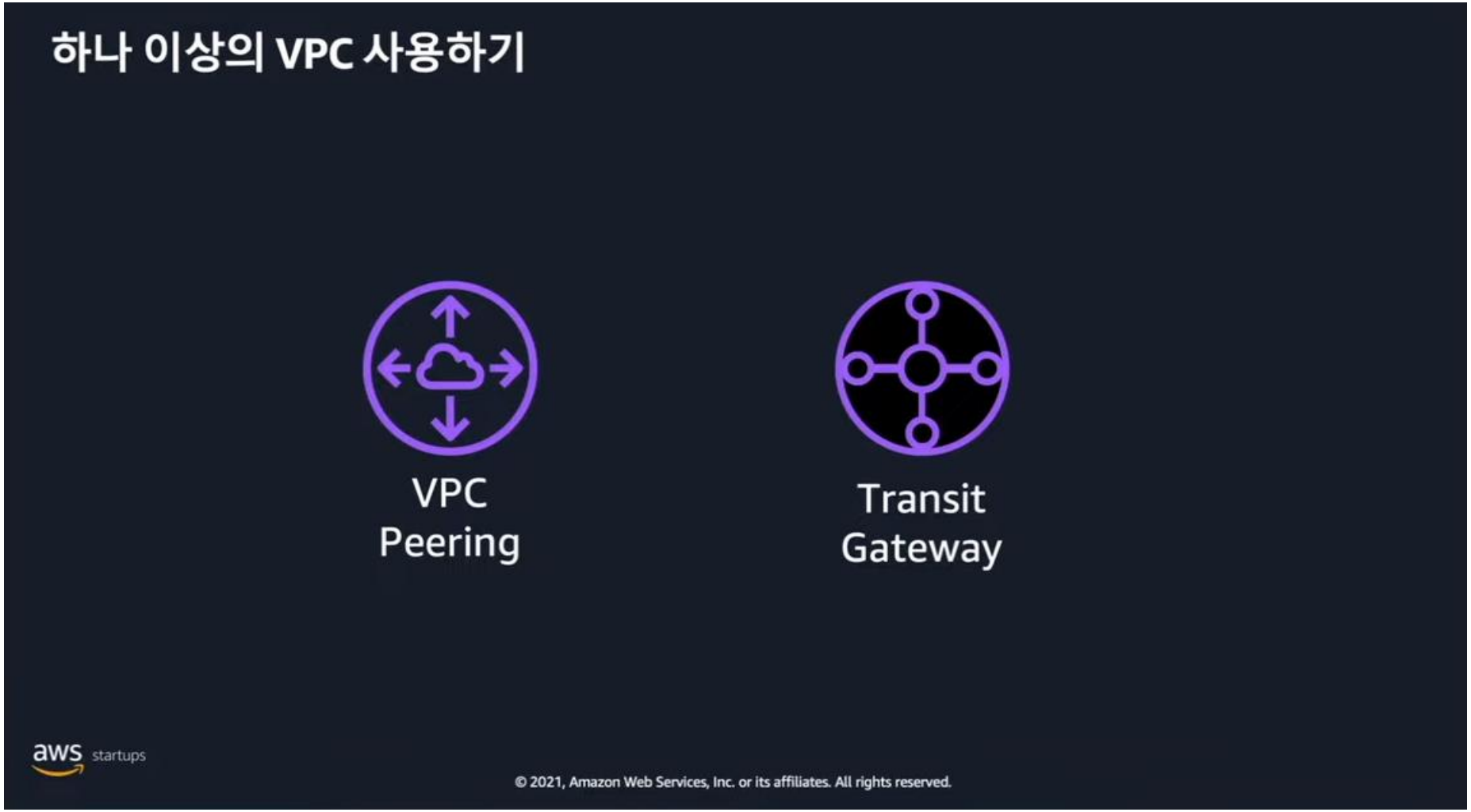


Interface VPC Endpoint(AWS PrivateLink)

- 인터페이스 VPC 엔드포인트(인터페이스 엔드포인트)를 통해 AWS PrivateLink로 지원하는 서비스에 연결할 수 있다.

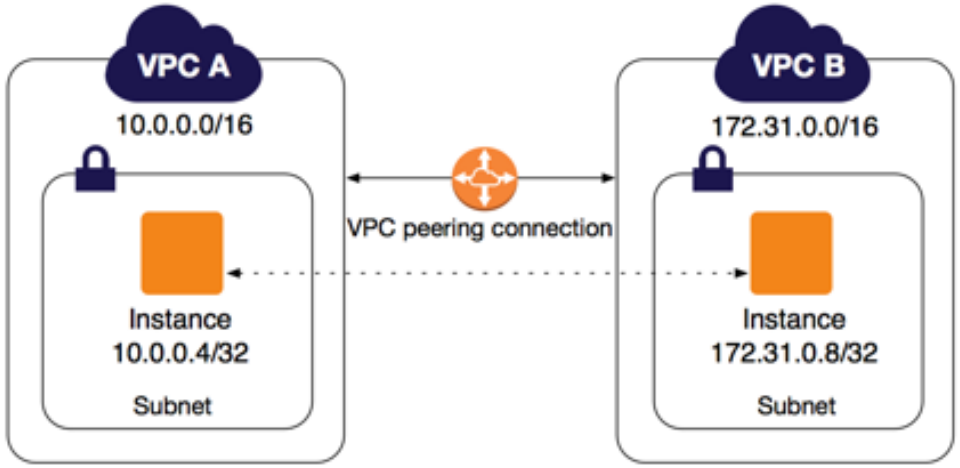


하나 이상의 VPC 사용하기



VPC Peering

- VPC 피어링 연결은 프라이빗 IPv4 주소 또는 IPv6 주소를 사용하여 두 VPC 간에 트래픽을 라우팅 할 수 있도록 하기 위한 두 VPC 사이의 네트워킹 연결이다.
- 동일한 네트워크에 속하는 경우와 같이 VPC의 인스턴스가 서로 통신할 수 있다.
- 사용자의 자체 VPC 또는 다른 AWS 계정의 VPC와 VPC 피어링 연결을 만들 수 있다. 또한 VPC는 다른 리전에 있을 수 있다(리전 간 VPC 피어링 연결이라고도 함).



하나 이상의 VPC 사용하기

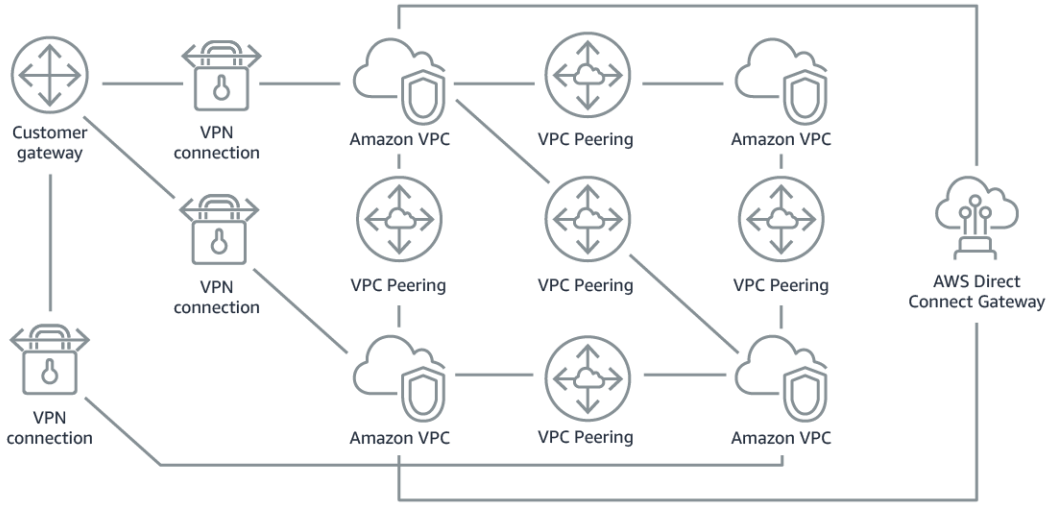
다수의 VPC를 연결하기 위해서는

- VPC Full Mesh 연결 기반의 관리

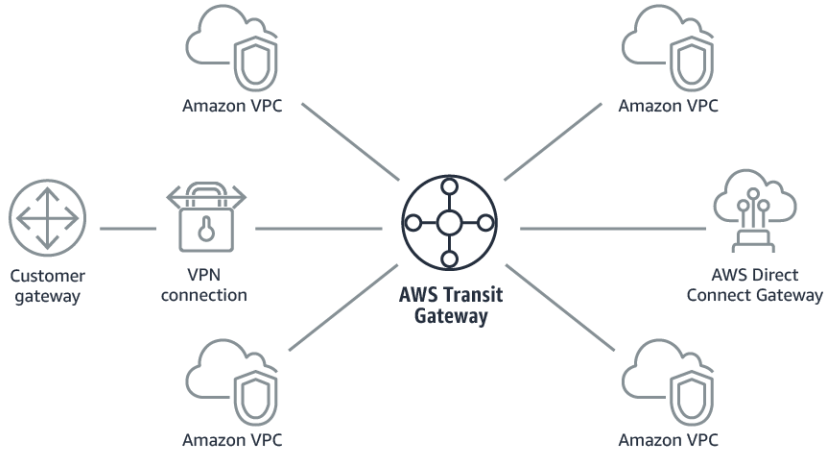
aws startups

Transit Gateway

- Transit Gateway는 가상 사설 클라우드(VPC)와 온프레미스 네트워크를 상호 연결하는데 사용할 수 있는 네트워크 전송 허브.

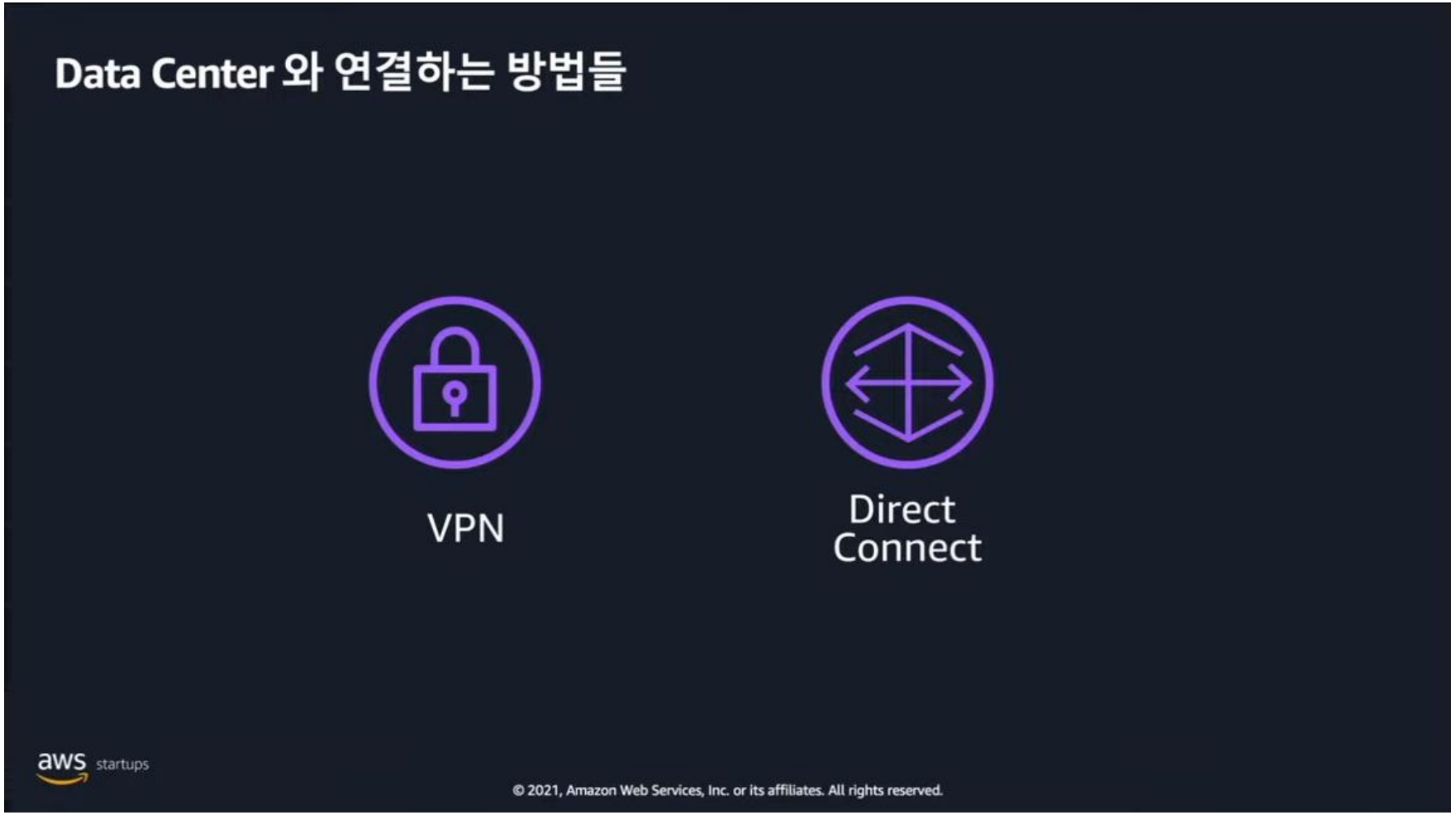


Transit Gateway 미사용 시



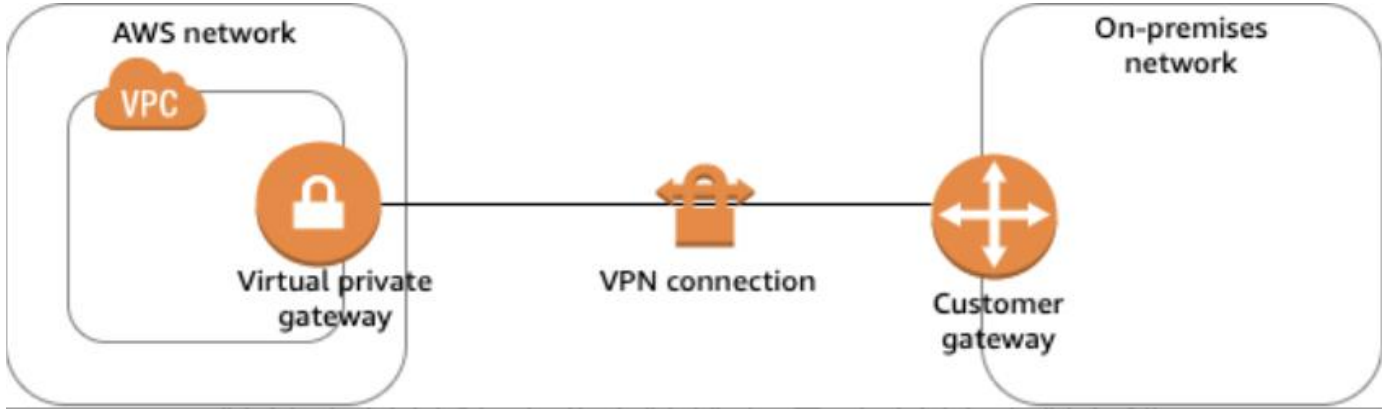
Transit Gateway 사용 시

Data Center와 연결하는 방법들



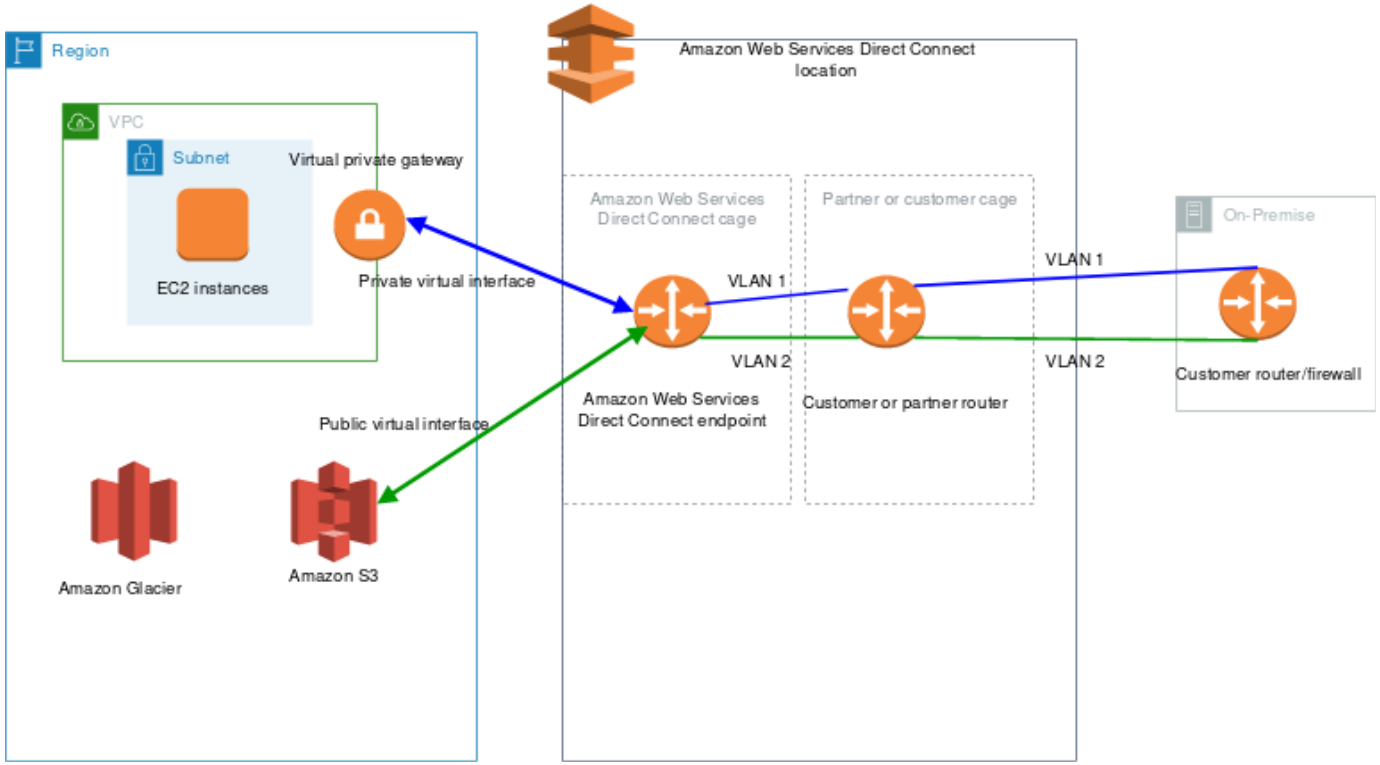
AWS Site-to-Site VPN

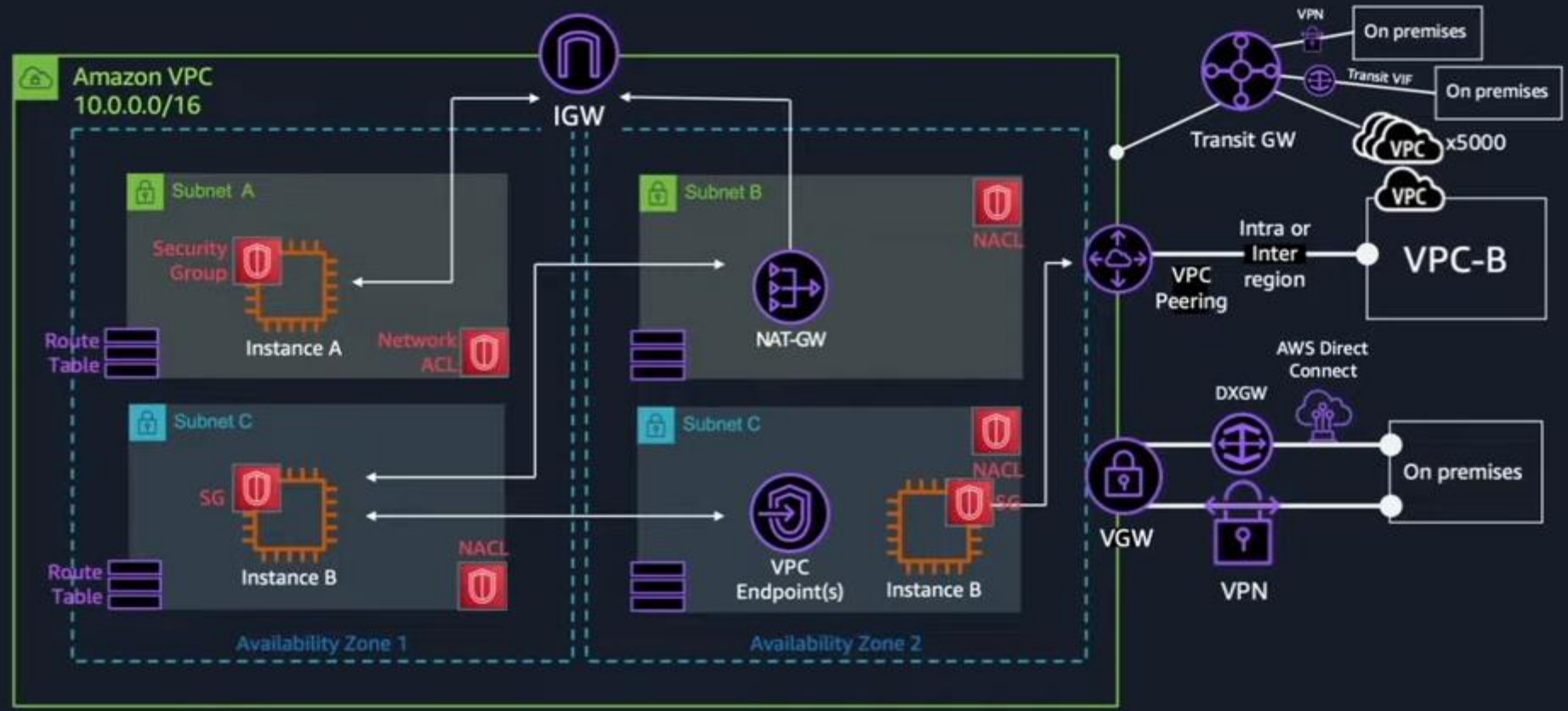
- 기본적으로 Amazon VPC로 시작하는 인스턴스는 원격 네트워크와 통신할 수 없다.
- AWS Site-to-Site VPN 연결을 통해 트래픽을 전달하도록 라우팅을 구성하여 VPC에서 원격 네트워크에 대한 액세스를 활성화할 수 있다.



AWS Direct Connect

- AWS Direct Connect를 사용하면 표준 이더넷 광섬유 케이블을 통해 내부 네트워크를 AWS Direct Connect 위치에 연결할 수 있다.





aws startups