



다양한 클라우드 네트워크 연동

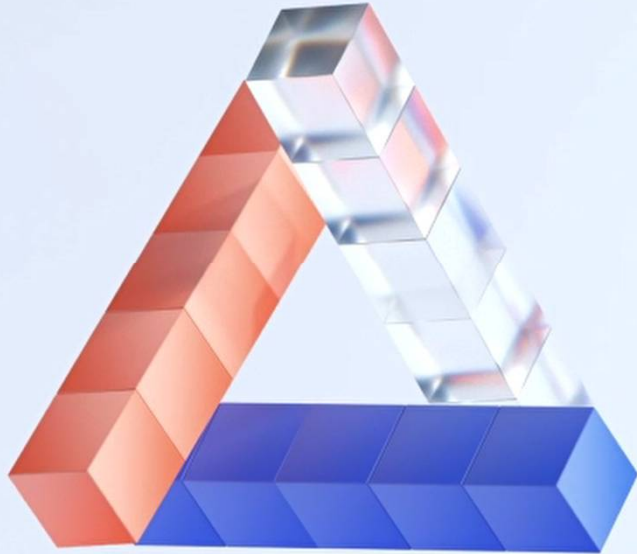
ZIGI(지기)

Blog

ZIGISPACE.NET

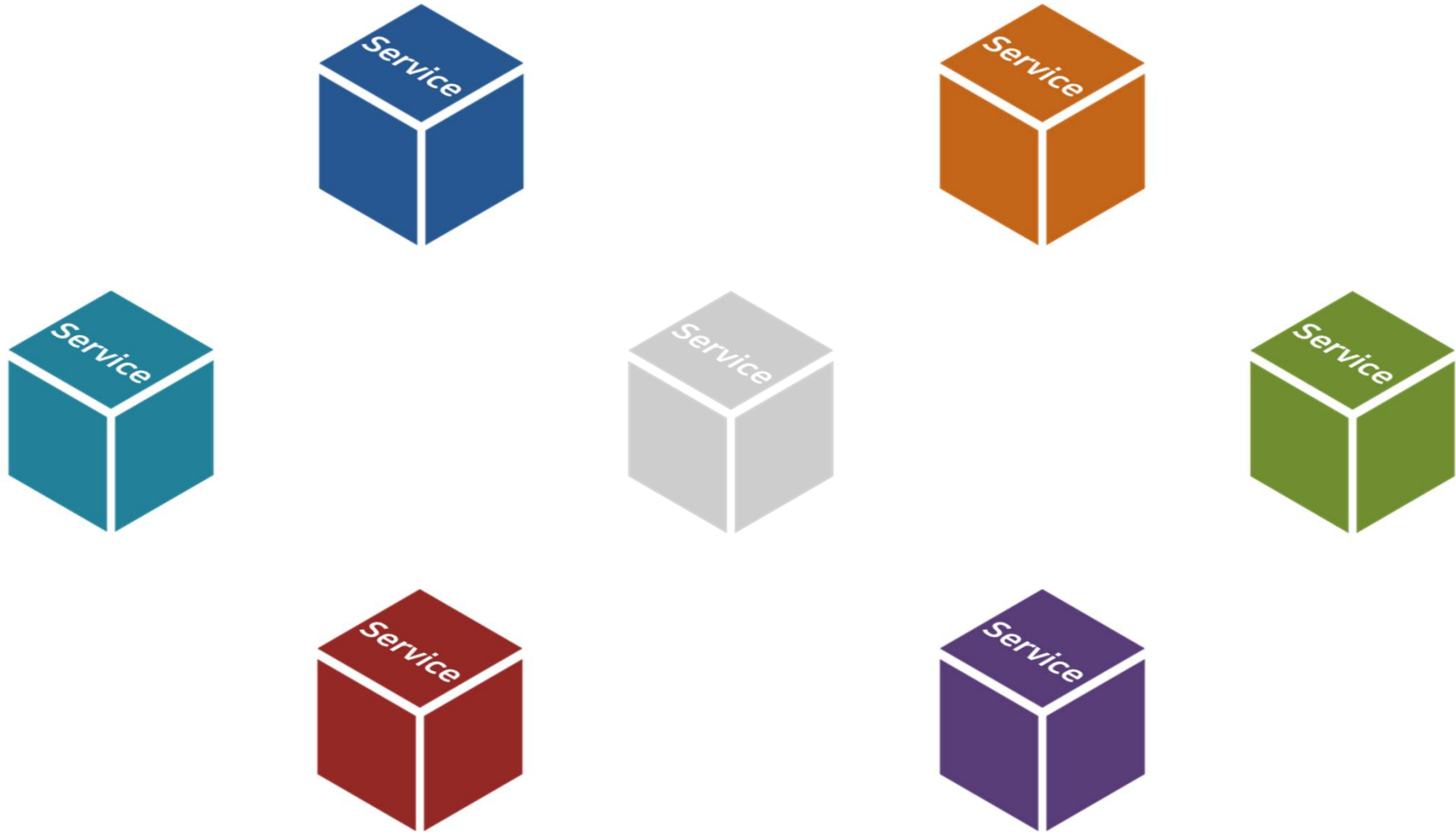


Agenda



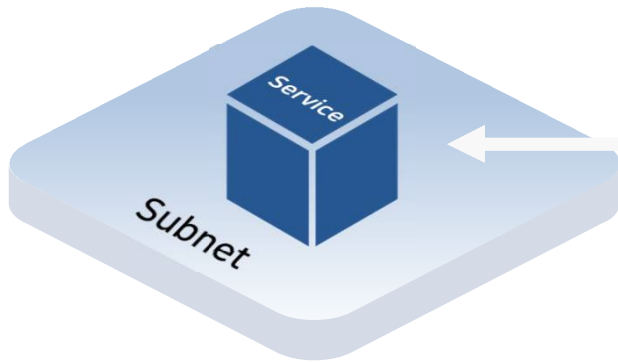
1. 클라우드에서의 라우팅
 - 라우팅 동작
 - 라우팅 테이블
2. 가상 네트워크 간의 연동
 - 1:1 가상 네트워크 연동(Peering)
 - 멀티 가상 네트워크 연동(Transit Gateway/Virtual WAN)
3. 하이브리드와 멀티 클라우드
 - VPN(Virtual Private Network)
 - 전용선(Direct Connect / Express Route)
 - Cloud Hub
4. 프라이빗 링크
 - 서비스 엔드포인트(Endpoint)
 - 프라이빗 링크(Private Link)

서비스를 위해서는..

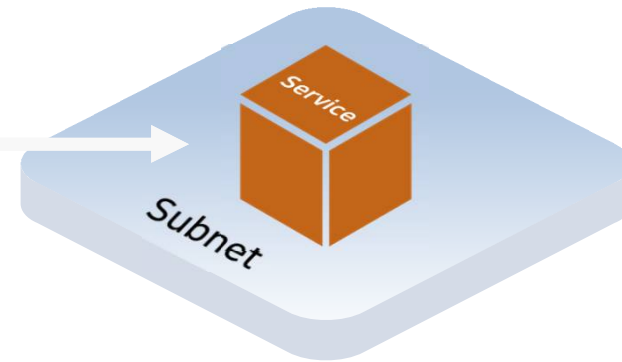


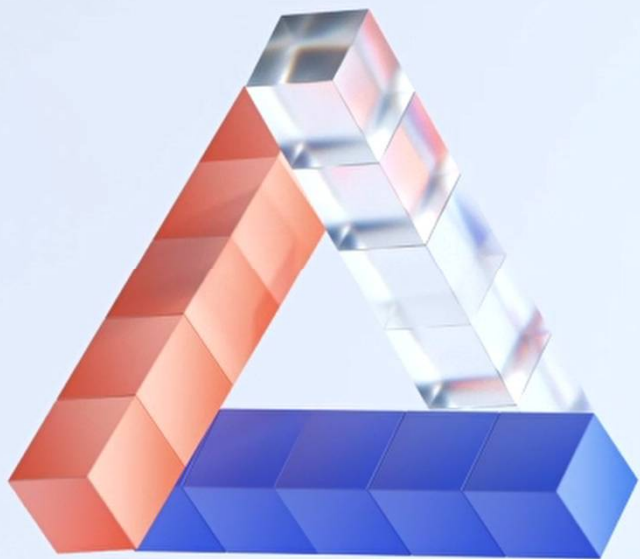


클라우드 가상 네트워크



로컬 통신





클라우드에서의 라우팅



어떤

목적지(네트워크)

로 가려면

여기로(Next Hop)

로 가세요





목적지(네트워크)

여기로(Next Hop)



Destination

Gateway



Destination(대상)

Target(대상)



Address prefix(주소 접두사)

Next Hop(다음 홉)

라우팅 (2)				라우팅 편집
Q 라우팅 필터링		모두	< 1 >	⚙
대상	대상	상태	전파됨	
10.1.0.0/22	local	✓ 활성화	아니요	
0.0.0.0/0	igw-02d8671b65eeb3a51	✓ 활성화	아니요	

【 AWS 라우팅 테이블 】

ZIGI-RT 경로				
경로 테이블				
Q 경로 검색				
이름	주소 접두사	다음 홉 형식	다음 홉 IP 주소	
결과가 없습니다.				

【 Azure 라우팅 테이블 】



Default Type

- Local Route

Custom Route

- Static Route
- Border Gateway Protocol
 - Direct Connect
 - Virtual Private Network

Gateway Association

- Gateway

Destination	Target
가상 네트워크에서 고유한 접두사	Local

【 AWS Local Route 】



System Route

- Azure Default
- Optional Default Route

User Defined Route

- Static Route
- Border Gateway Protocol
 - ExpressRoute
 - Virtual Private Network

Prefix	Next hop
가상 네트워크에서 고유의 접두사	가상 네트워크
0.0.0.0/0	인터넷
10.0.0.0/8	-
172.16.0.0/12	-
192.168.0.0/16	-
100.64.0.0/10	-

【 Azure Default 】

Address Prefixes	Next hop type
가상 네트워크에서 고유의 접두사	가상 네트워크
On-Premise에서 BGP를 통해서 광고 받거나, Local Network Gateway에 설정된 네트워크	Virtual Network Gateway
Multiple	Virtual Network Service Endpoint

【 Optional Default Route 】



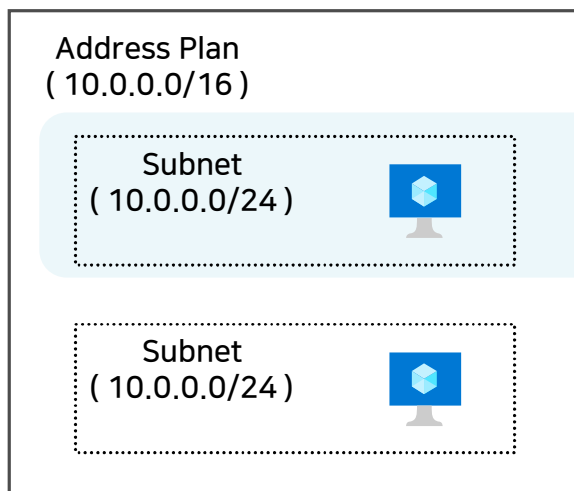
On-Premise



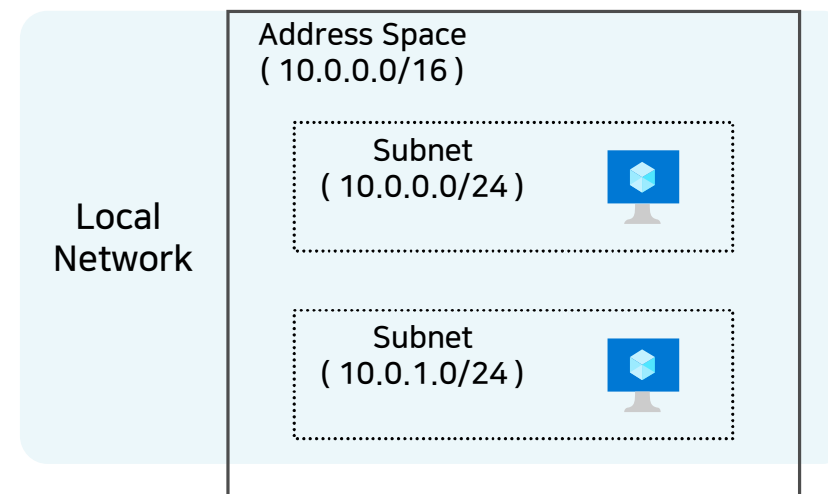
PUBLIC



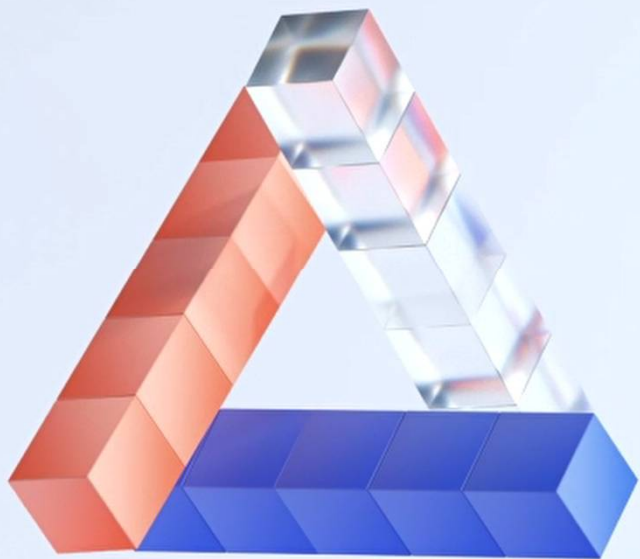
Local Network



Local
Network



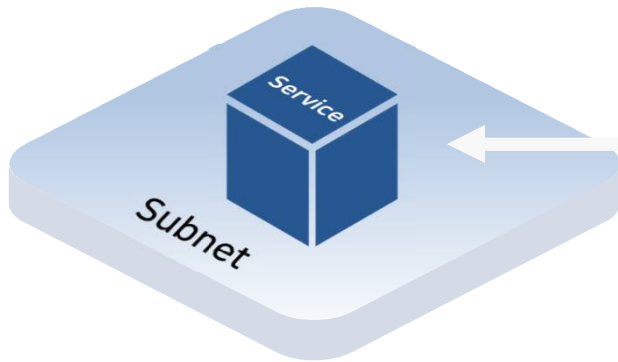
가상 네트워크



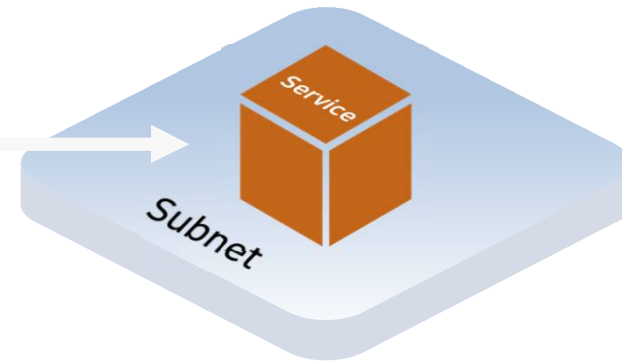
가상 네트워크 간의 연동

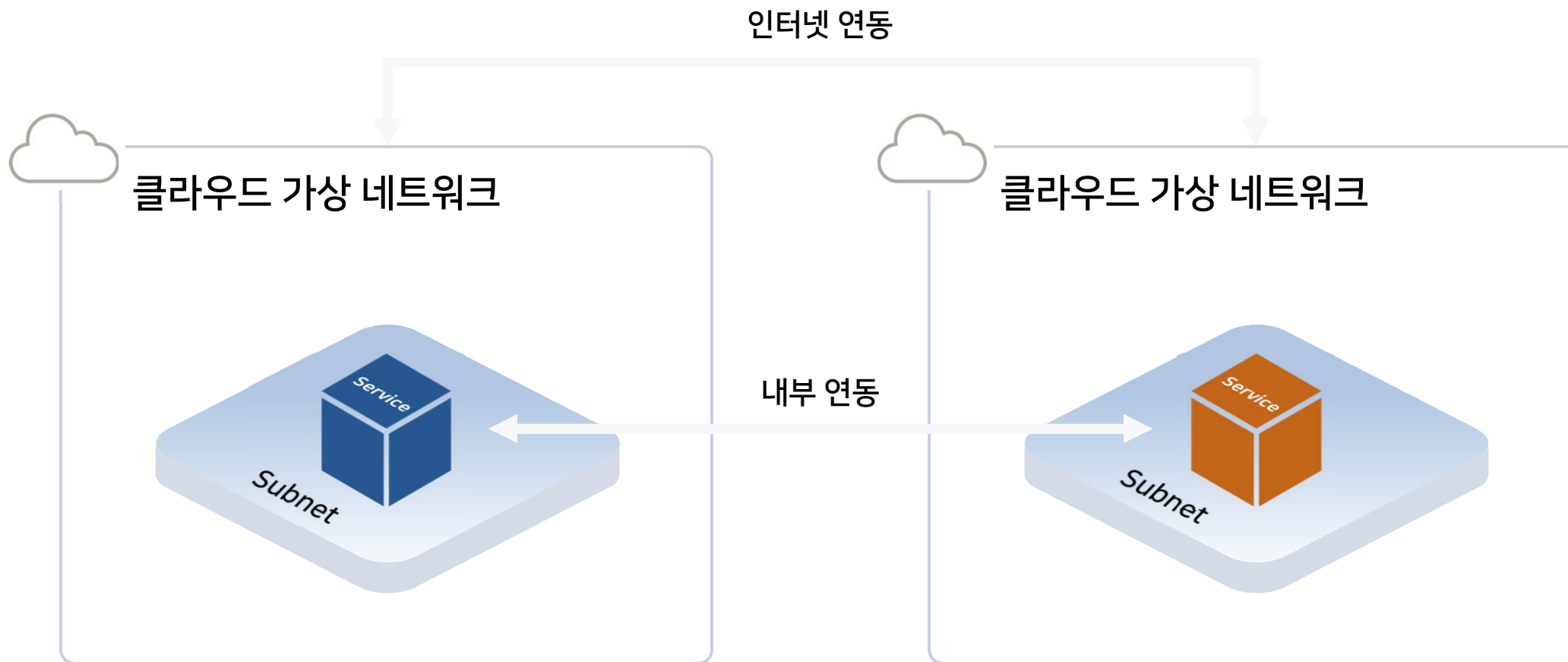


클라우드 가상 네트워크



로컬 통신

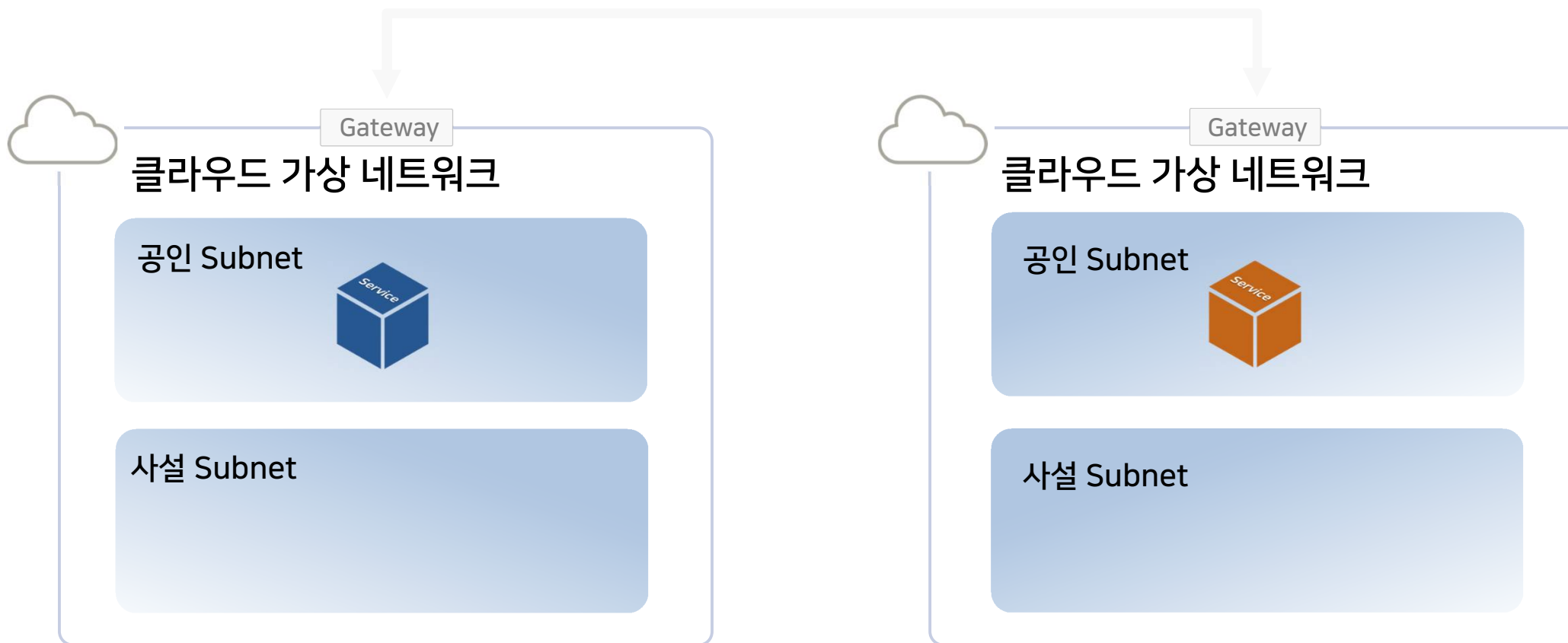




가상 네트워크 간의 연동 : 인터넷 연동



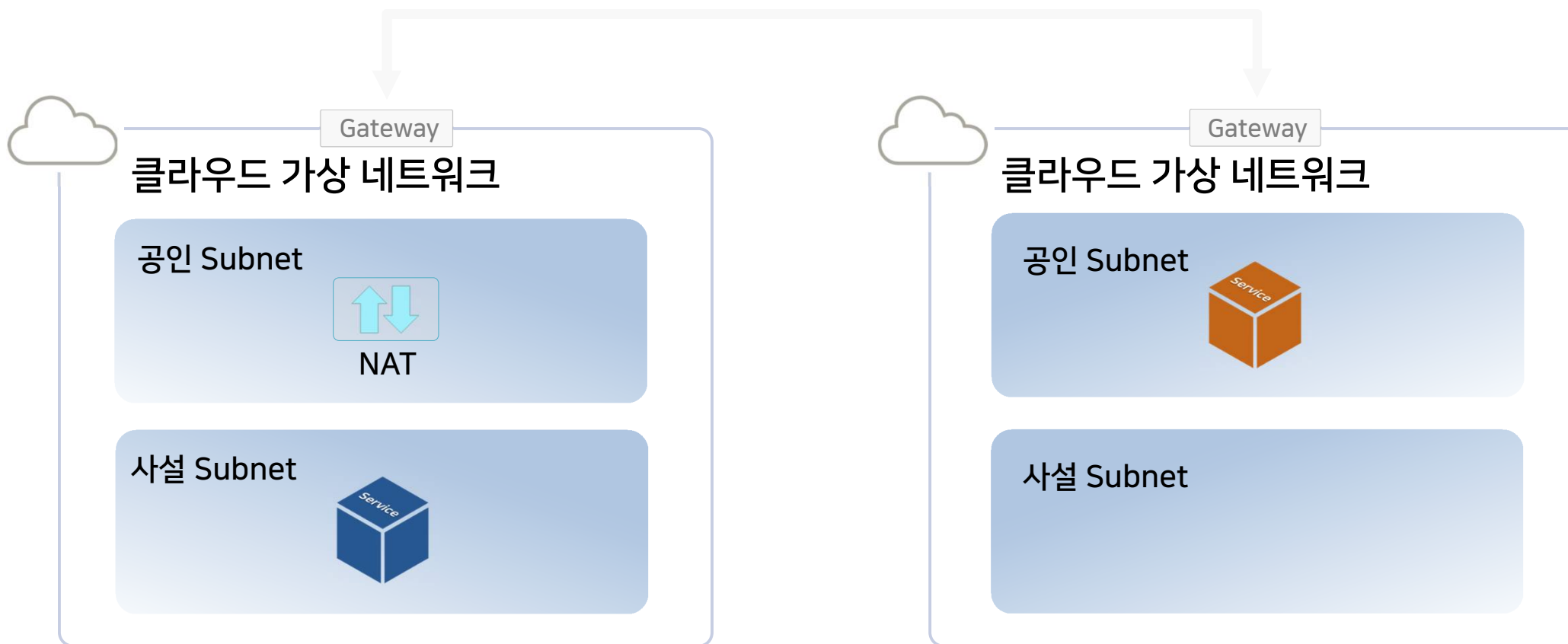
인터넷 연동



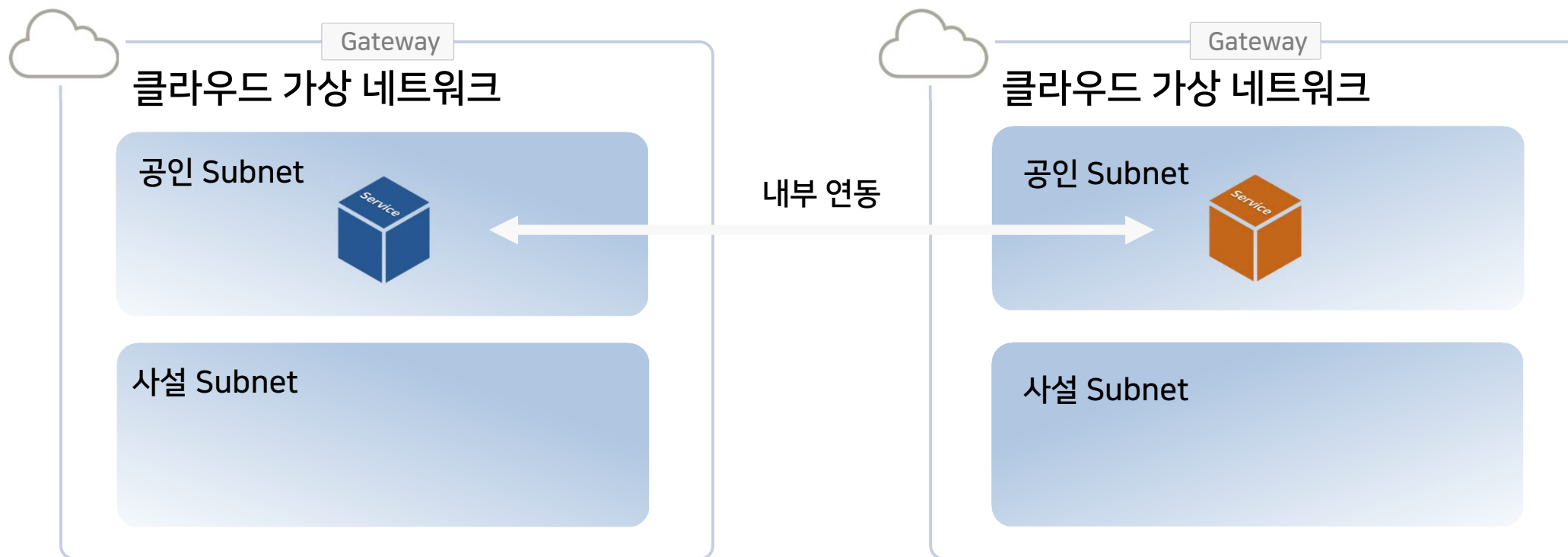
가상 네트워크 간의 연동 : 인터넷 연동



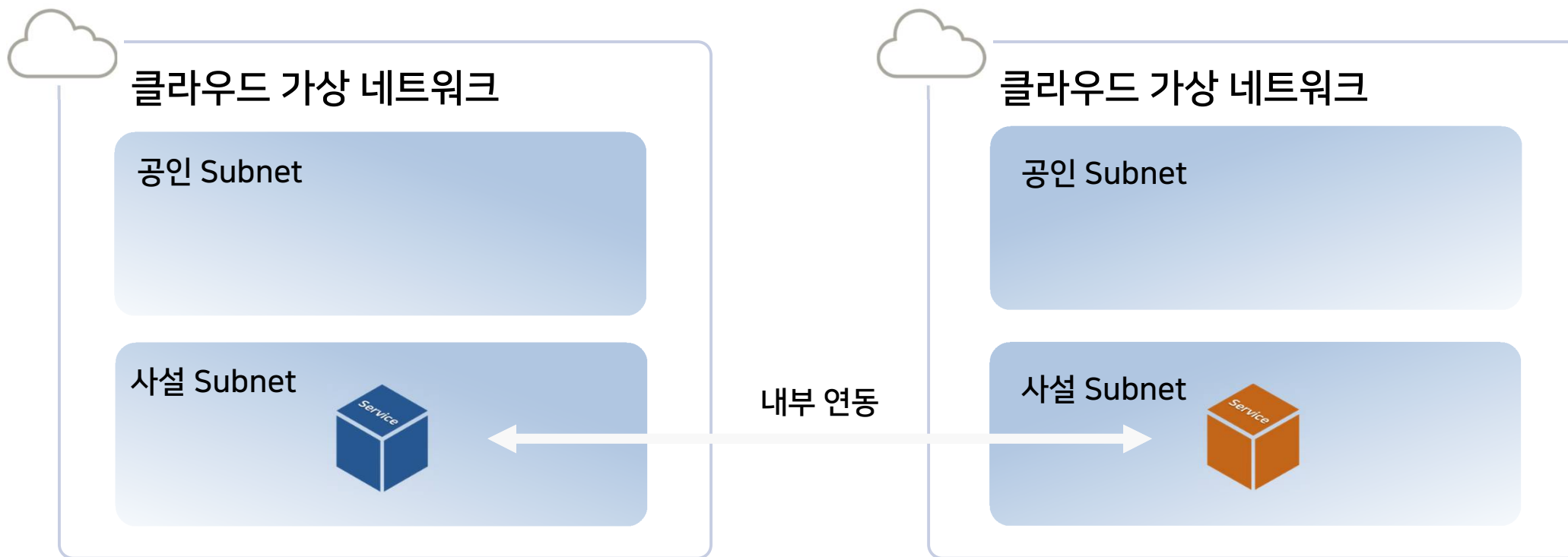
인터넷 연동



가상 네트워크 간의 연동 : 내부 연동



가상 네트워크 간의 연동 : 내부 연동



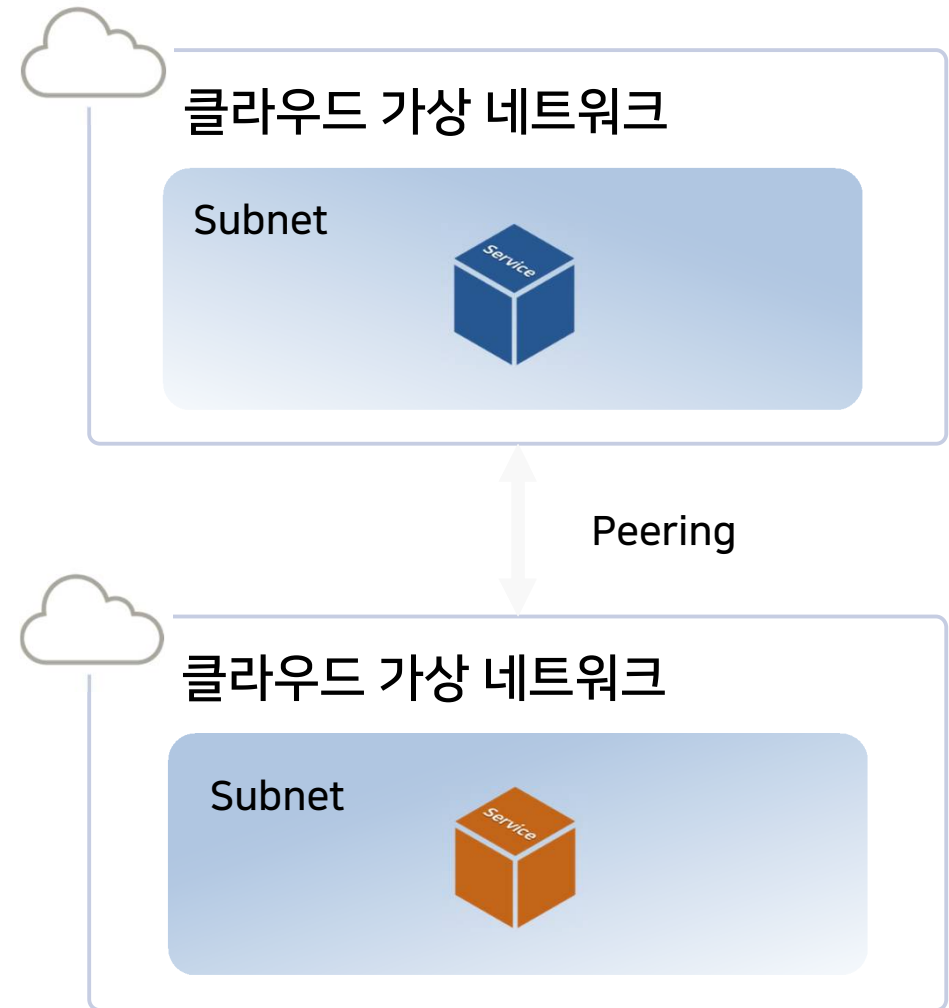
가상 네트워크 간의 연동 : Peering



가상 네트워크 간의 Private 연결

라우팅을 통한 통신

중복되지 않은 IP 주소 설계 필요





VPC Peering

가상 네트워크(VPC)간의 연결만 구성

Peering을 위한 Target 생성

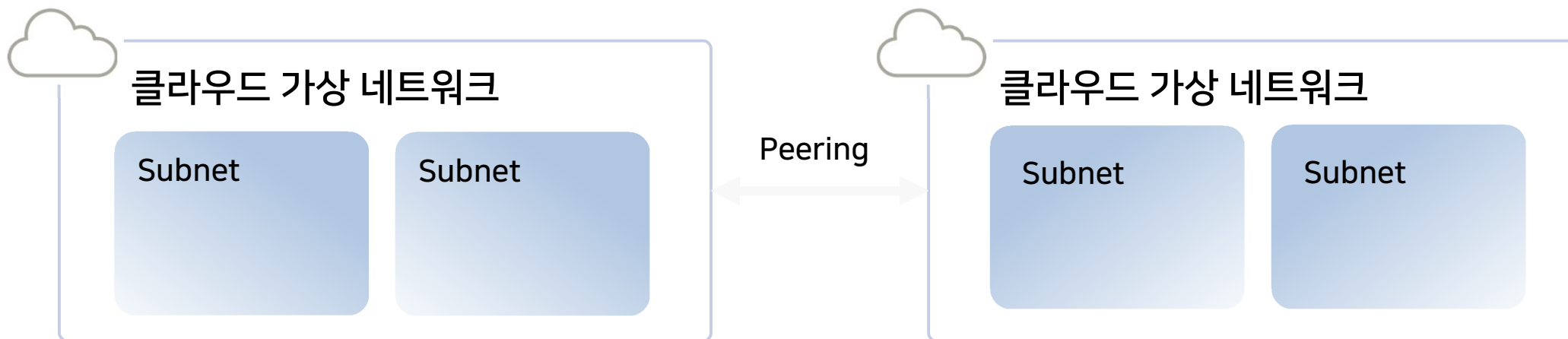
라우팅 설정 필요

VNet Peering

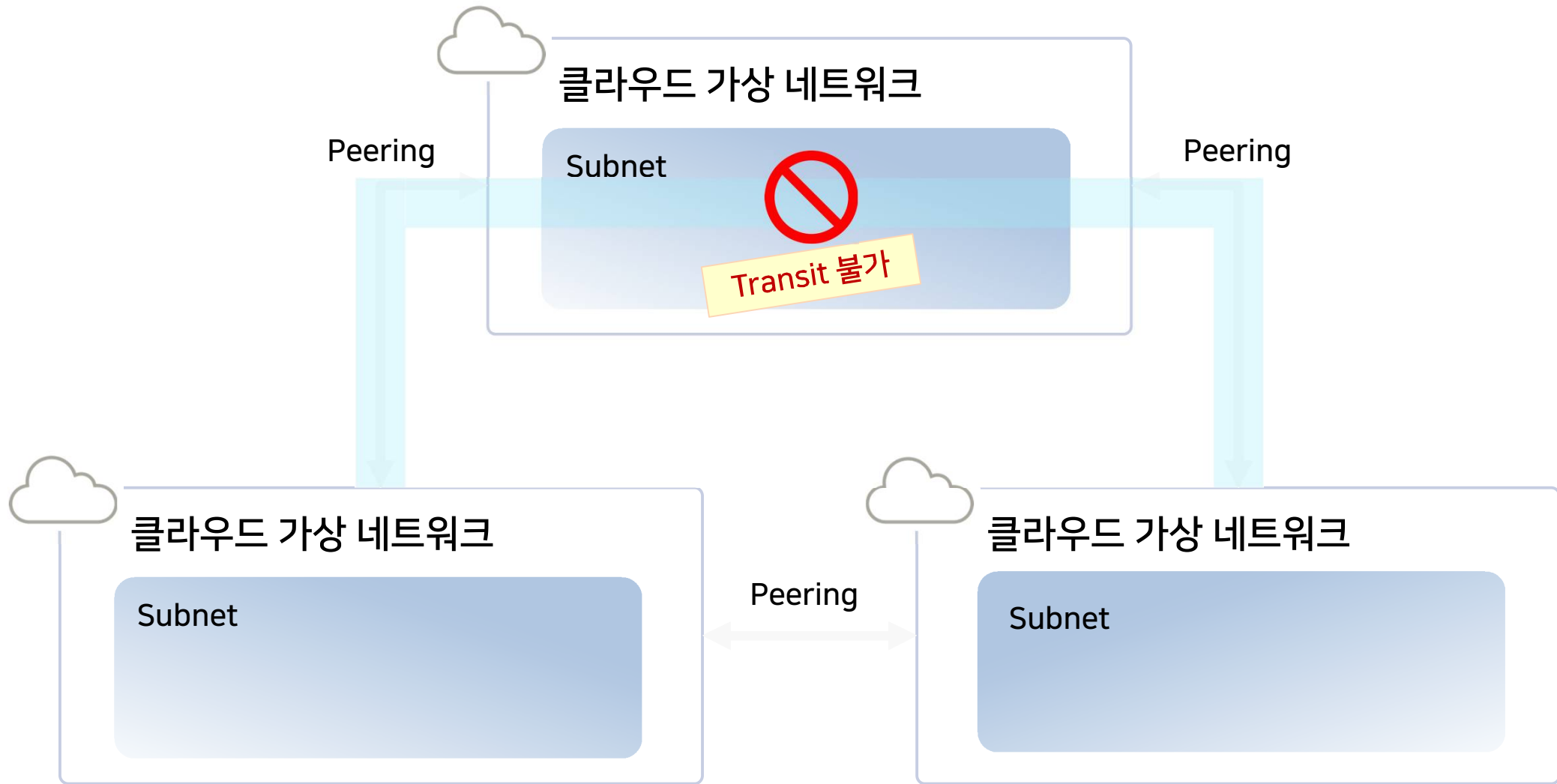
가상 네트워크(VNet)간의 연결 및 라우팅 구성

VNet의 Address Space 모두 적용

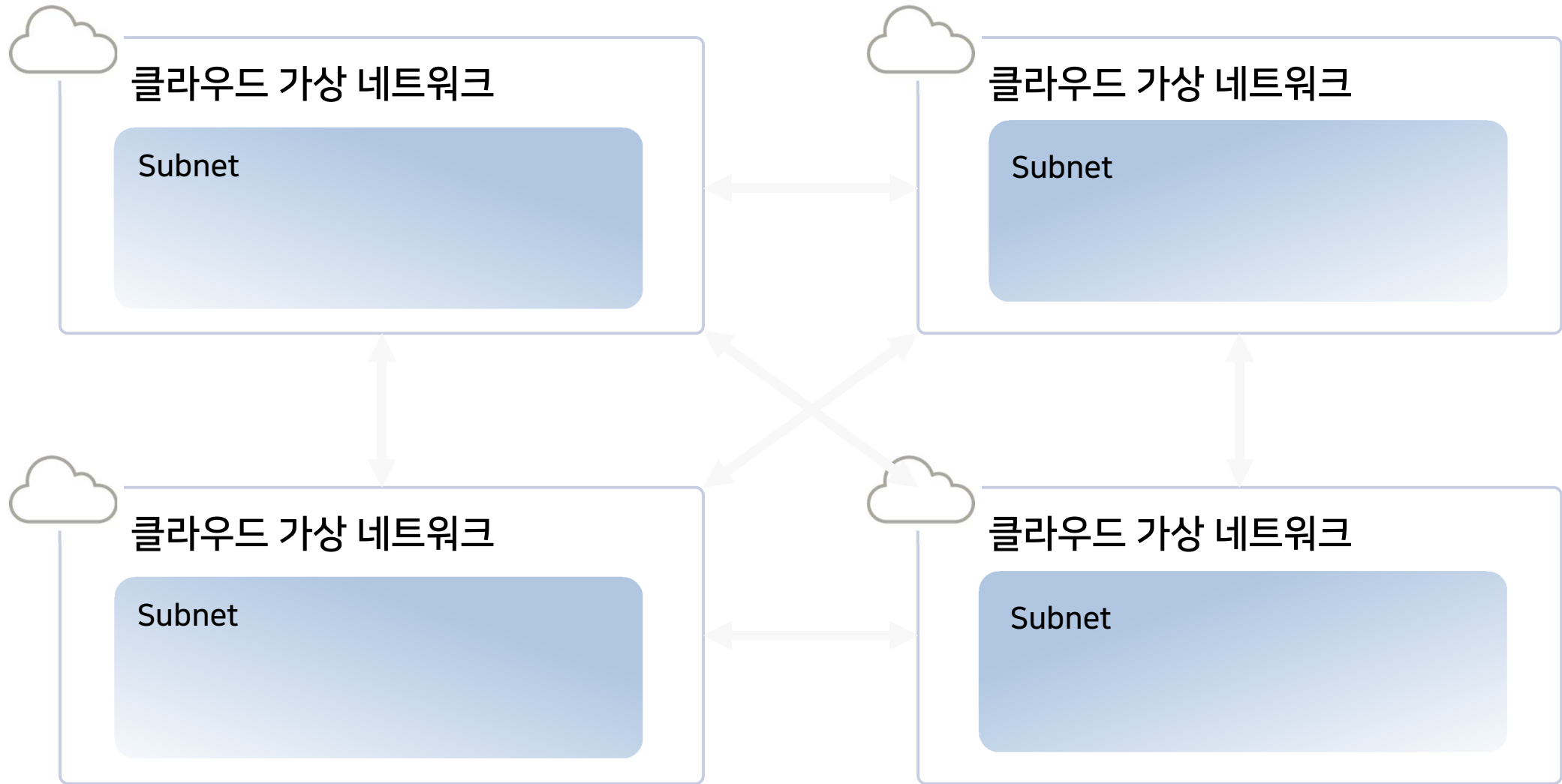
필요 시, NSG를 이용한 연동 대역 제한



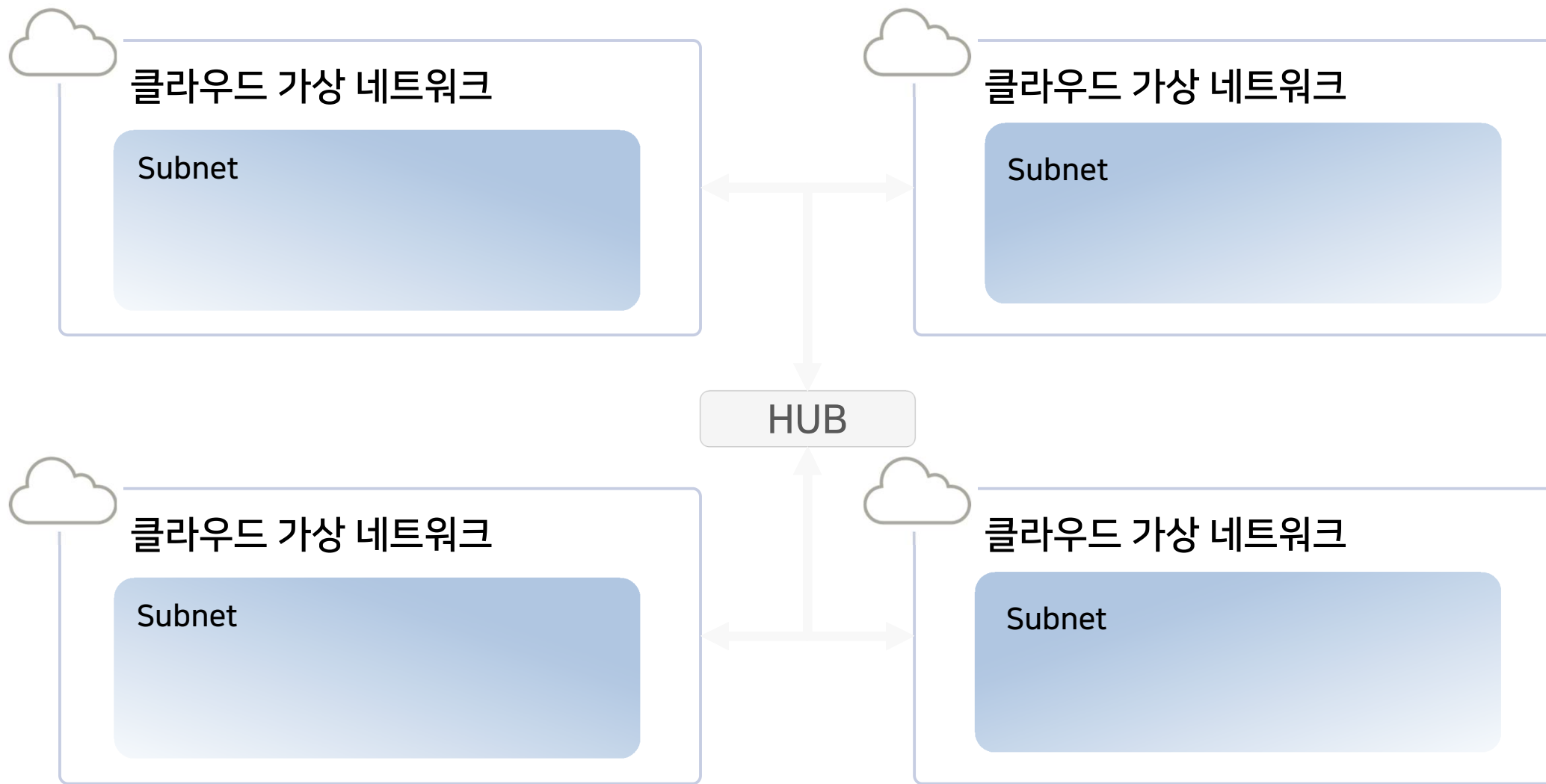
다수의 가상 네트워크 연동 : Peering



다수의 가상 네트워크 연동 : Peering



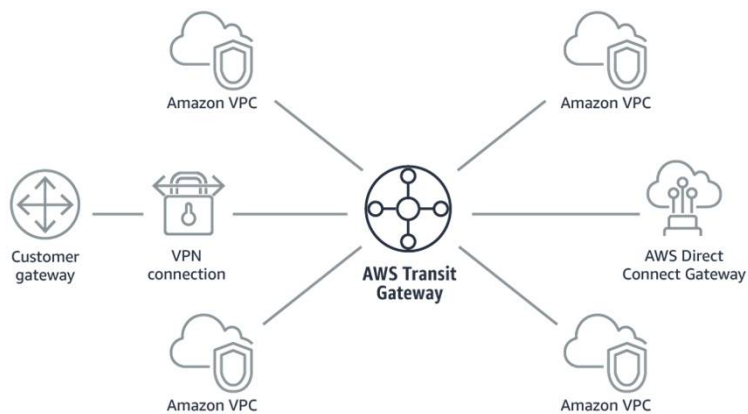
다수의 가상 네트워크 연동 : Peering





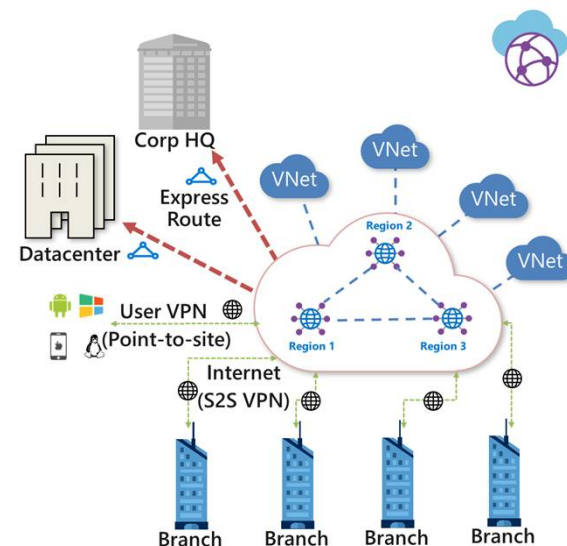
Transit Gateway

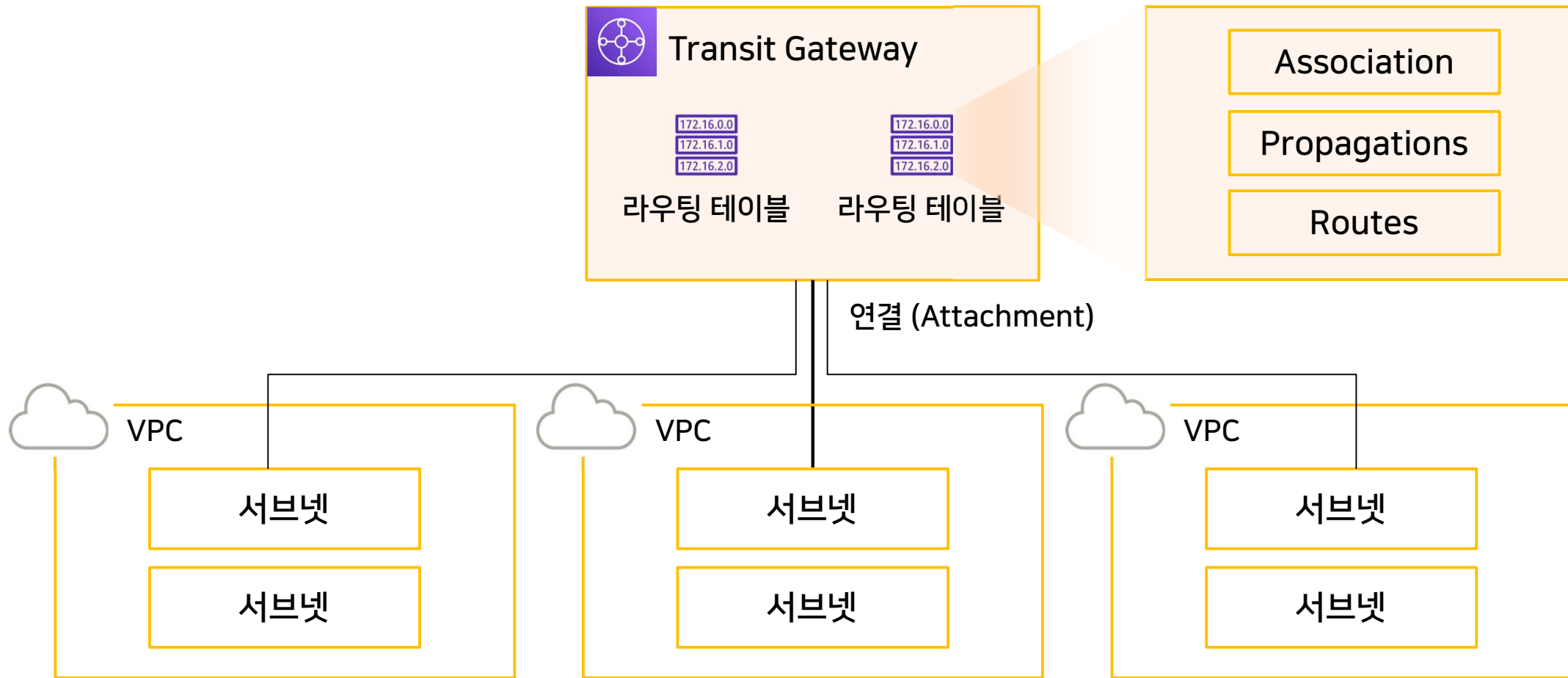
Amazon Virtual Private Cloud(VPC)와
온프레미스 네트워크를 단일 게이트웨이에
연결할 수 있도록 지원해 주는 서비스

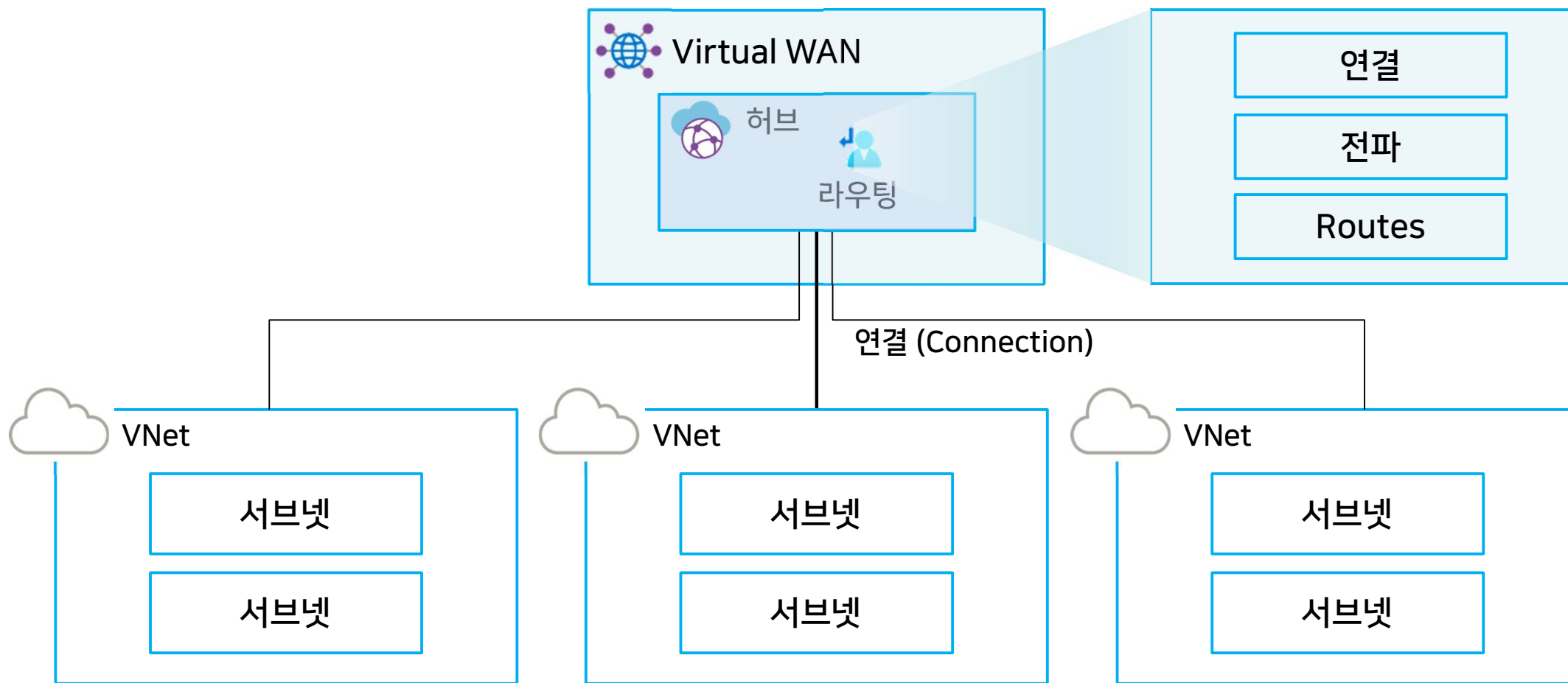


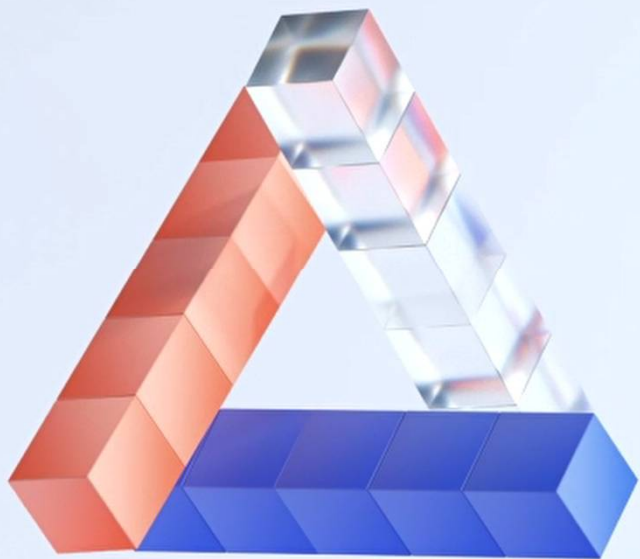
Virtual WAN

S2S VPN, User VPN 및 ExpressRoute와
같은 다양한 Azure 클라우드 연결 서비스를
단일 운영 인터페이스로 통합



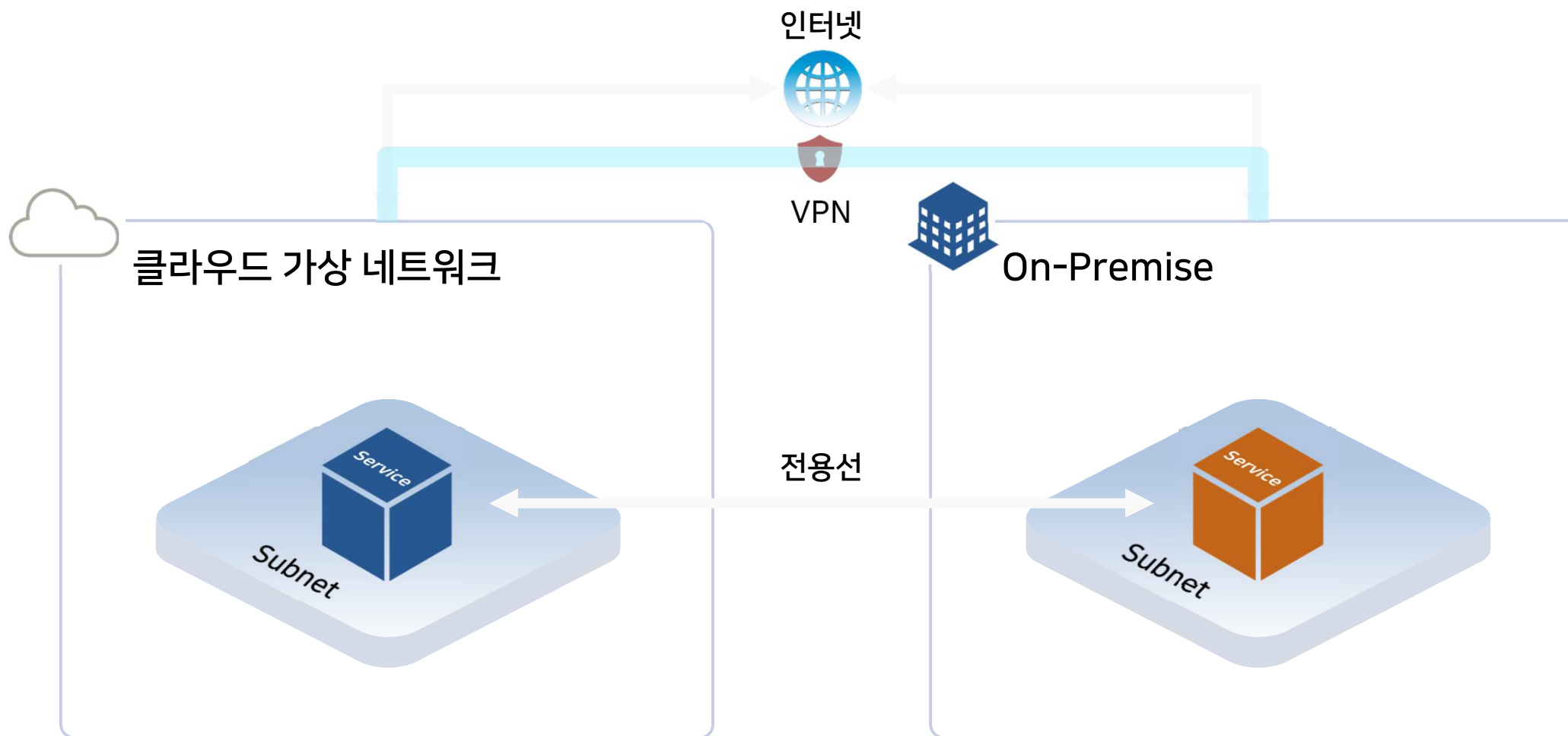


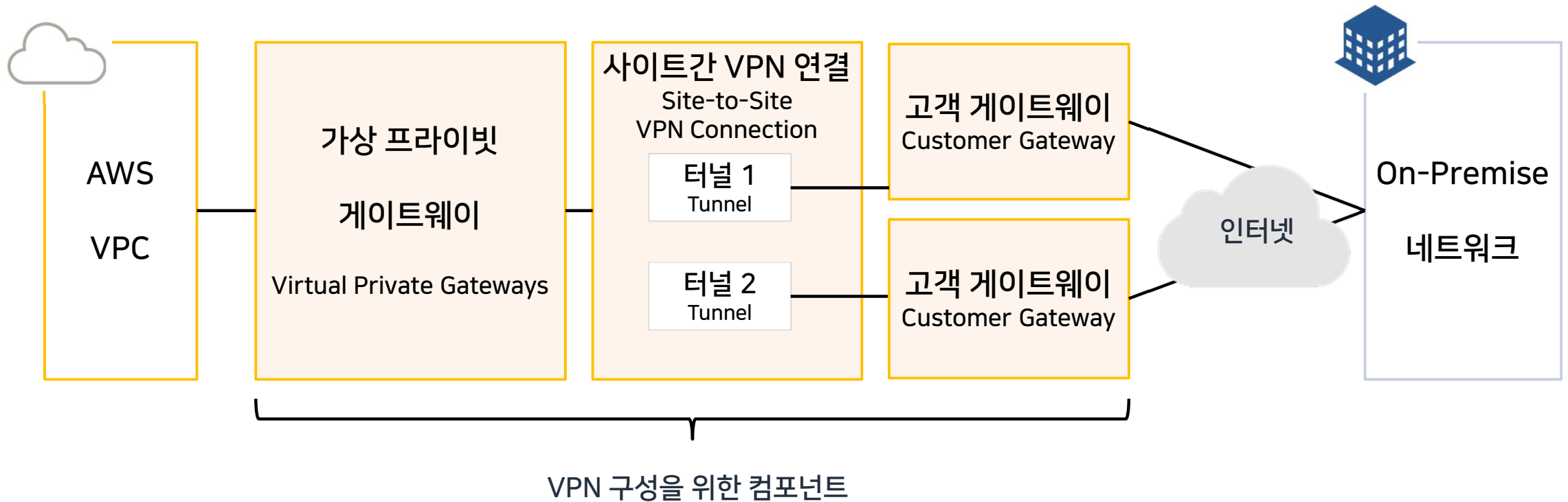


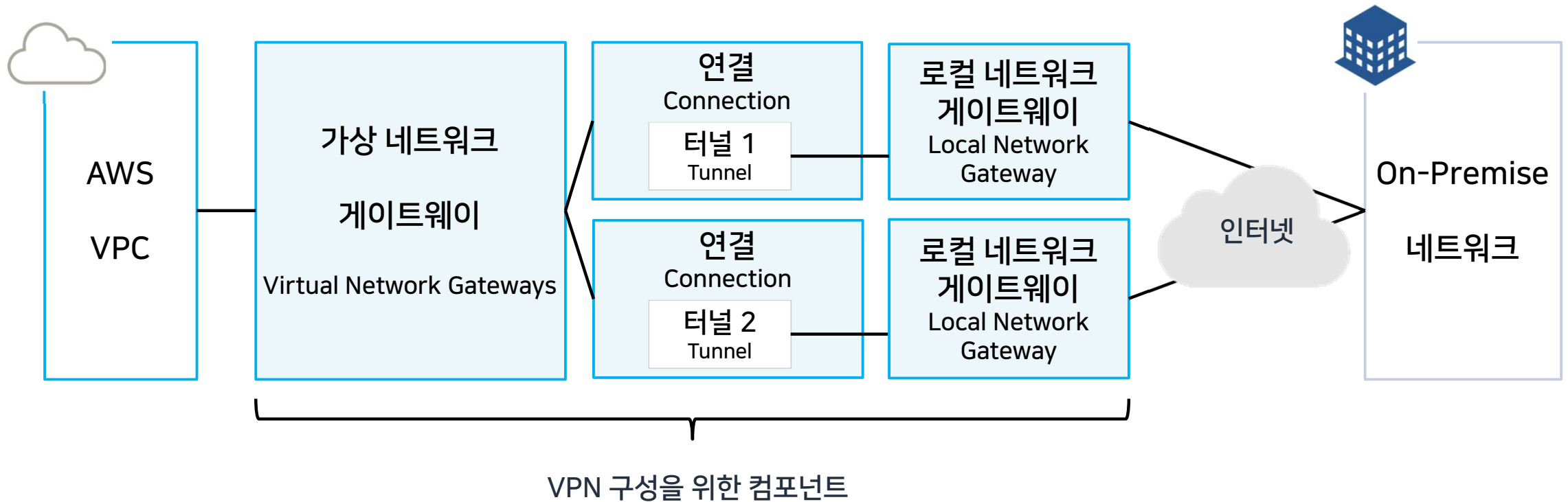


하이브리드와 멀티 클라우드

하이브리드 클라우드 구성 방안



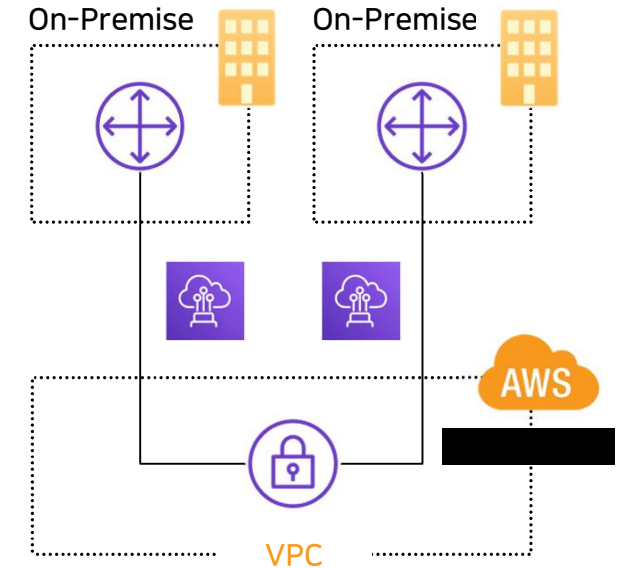






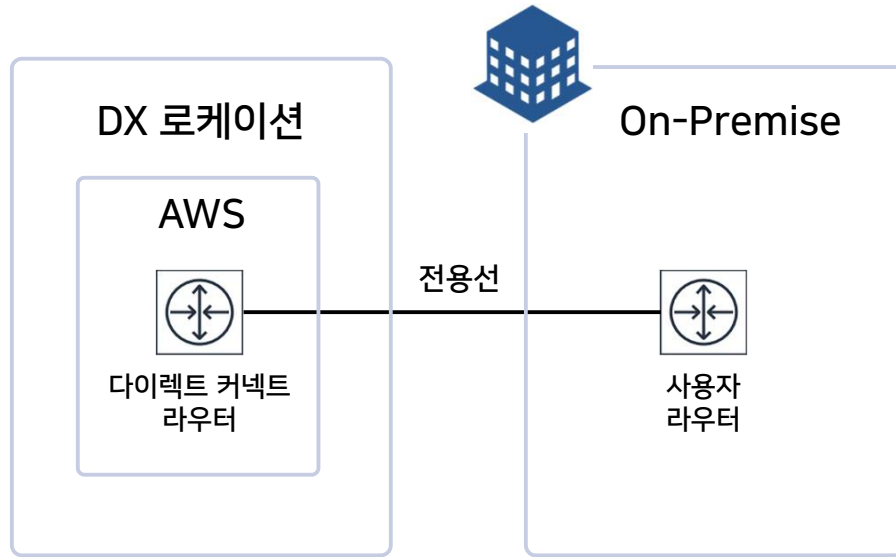
Direct Connect

- AWS와 On-Premise 간의 연결을 위한 전용선 서비스
- 빠른 속도, 서비스 품질보장, 강화된 보안 제공
- BGP 사용 필수
- 다양한 대역폭 옵션 제공¹⁾
- 서비스 안정성을 위해 이중화 구성 필요
- AWS 서비스 액세스 가능²⁾

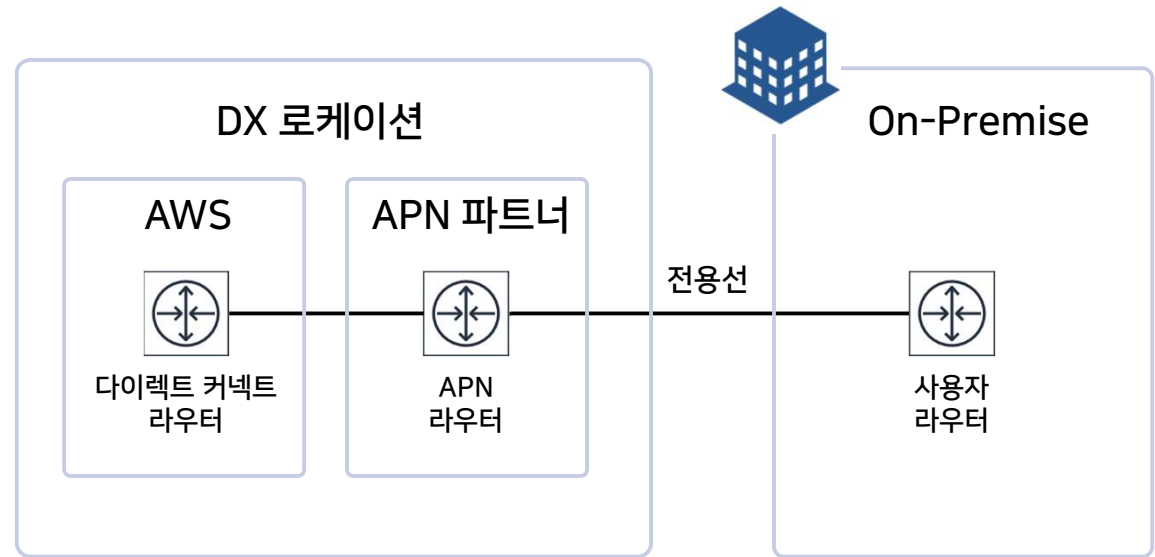


1) 제공되는 대역폭 : 50M, 100M, 200M, 300M, 400M, 500M, 1G, 2G, 5G, 10G, 100G

2) Public VIF를 통한 연동



Dedicated 방식

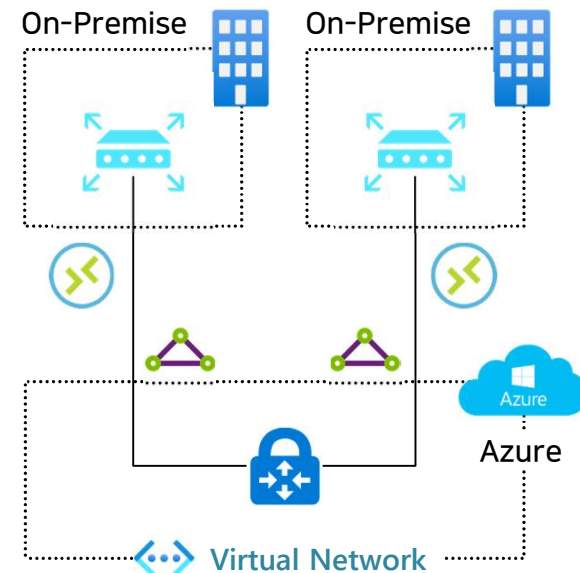


Hosted 방식



Express Route

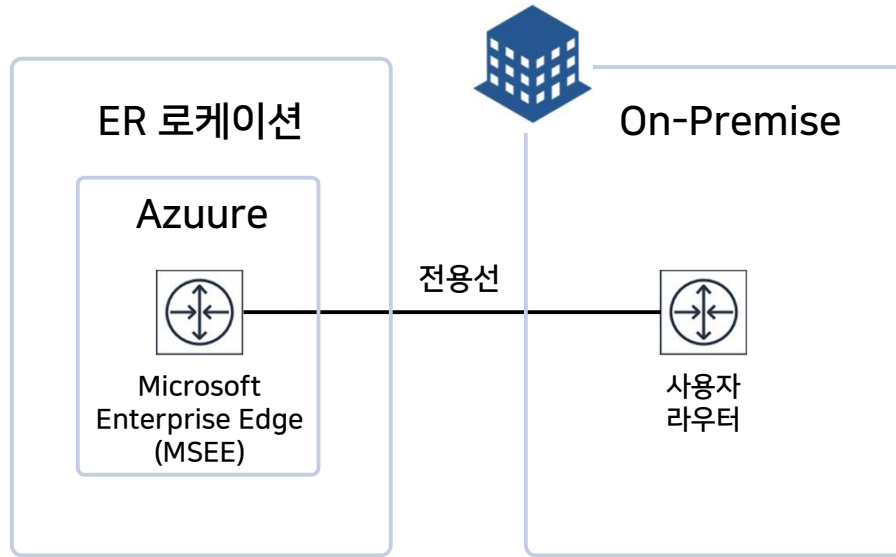
- Azure와 On-Premise 간의 연결을 위한 전용선 서비스
- 빠른 속도, 서비스 품질보장, 강화된 보안 제공
- BGP 사용 필수
- 다양한 대역폭 옵션 제공¹⁾
- Standard, High/Ultra Performance SKU 제공²⁾
- 서비스 안정성을 위해 모든 피어링 위치는 이중화
- Azure 서비스 및 Office 365 서비스 액세스 가능³⁾



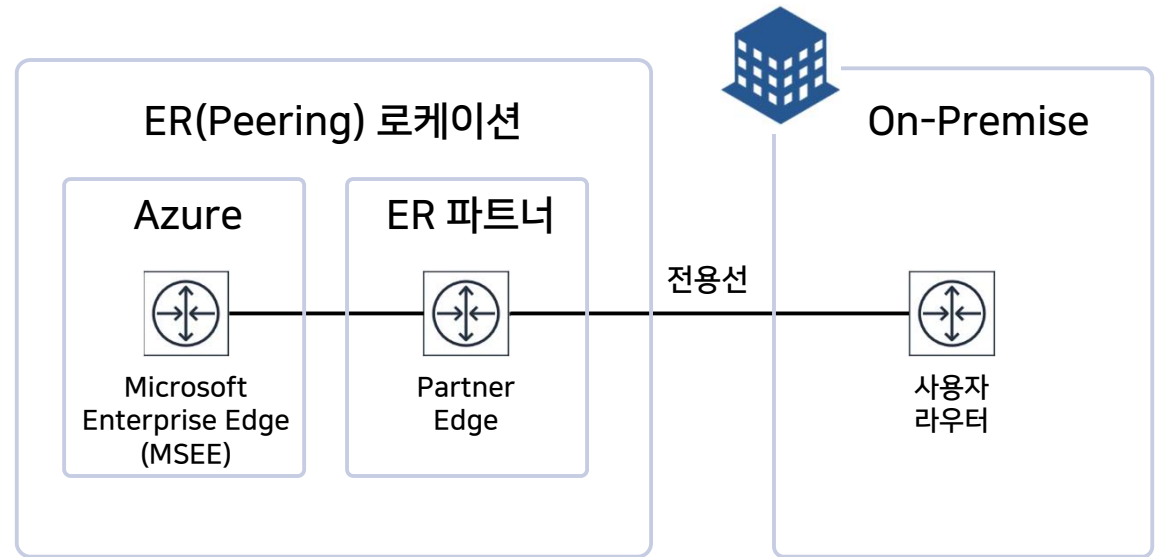
1) 제공되는 대역폭 : 50M, 100M, 200M, 500M, 1G, 2G, 5G, 10G, 100G

2) SKU별 지원되는 Bandwidth, PPS, CPS가 상이함.

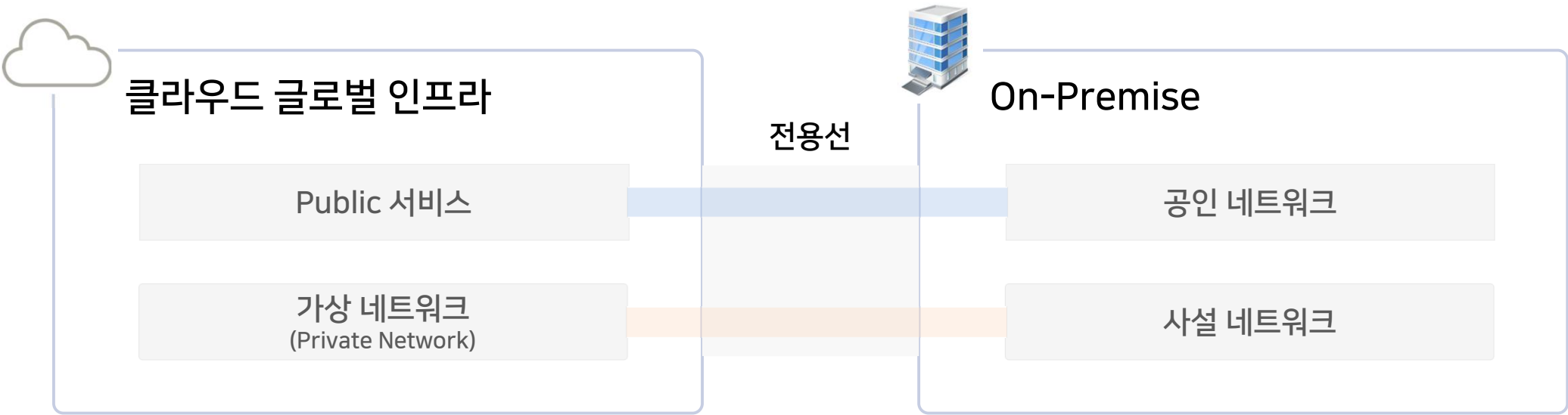
3) Microsoft Peering을 통한 연동



Express Route Direct

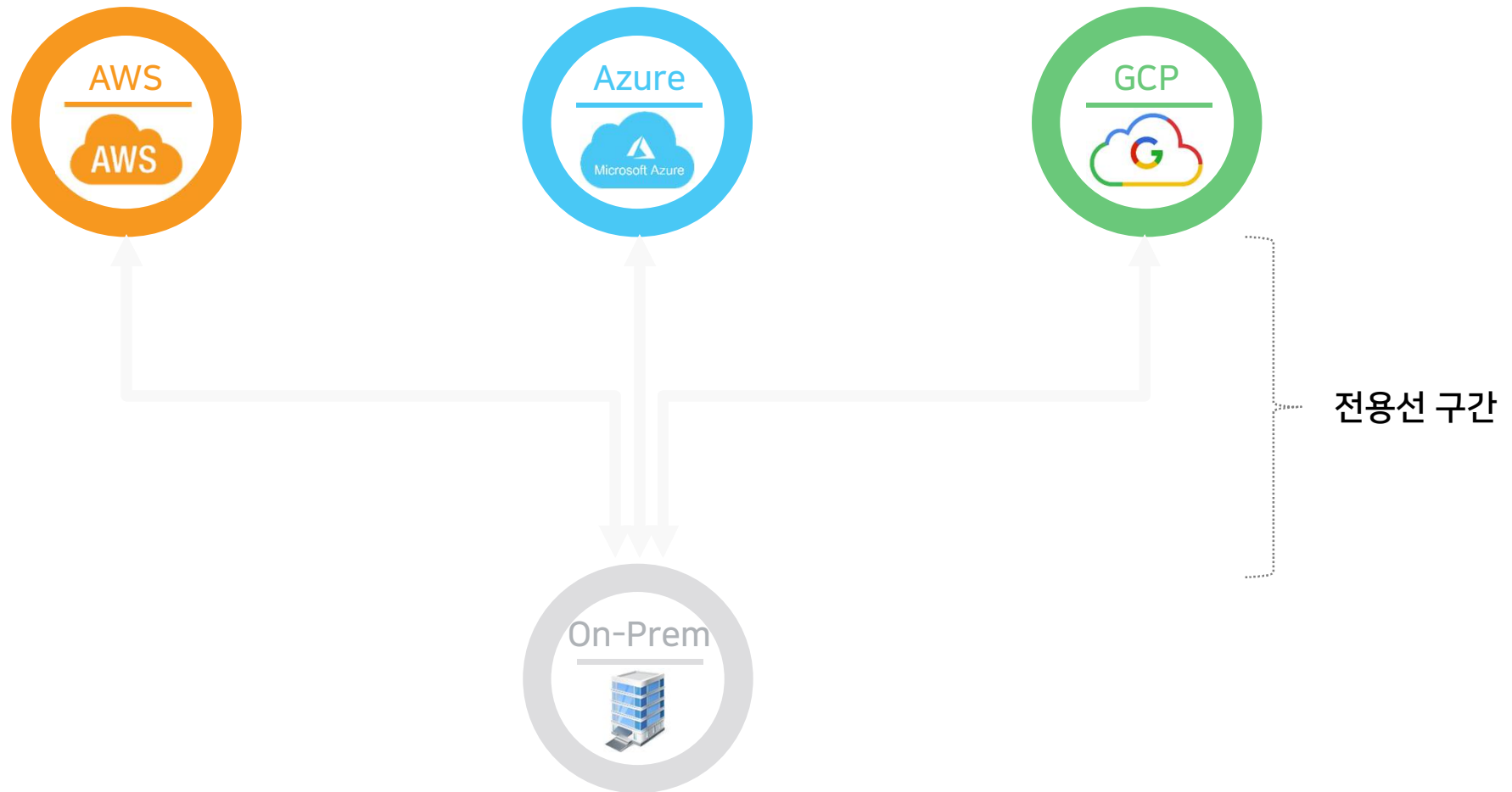


Express Route



Public Service 연동	Private Network 연동
AWS / Azure Public 서비스 연동	VPC / Virtual Network 연동
공인 AS / IP로만 연동 가능	사설 AS / IP로 연동 가능
Public VIF / Microsoft Peering	Private VIF / Private Peering

멀티/하이브리드 클라우드 구성

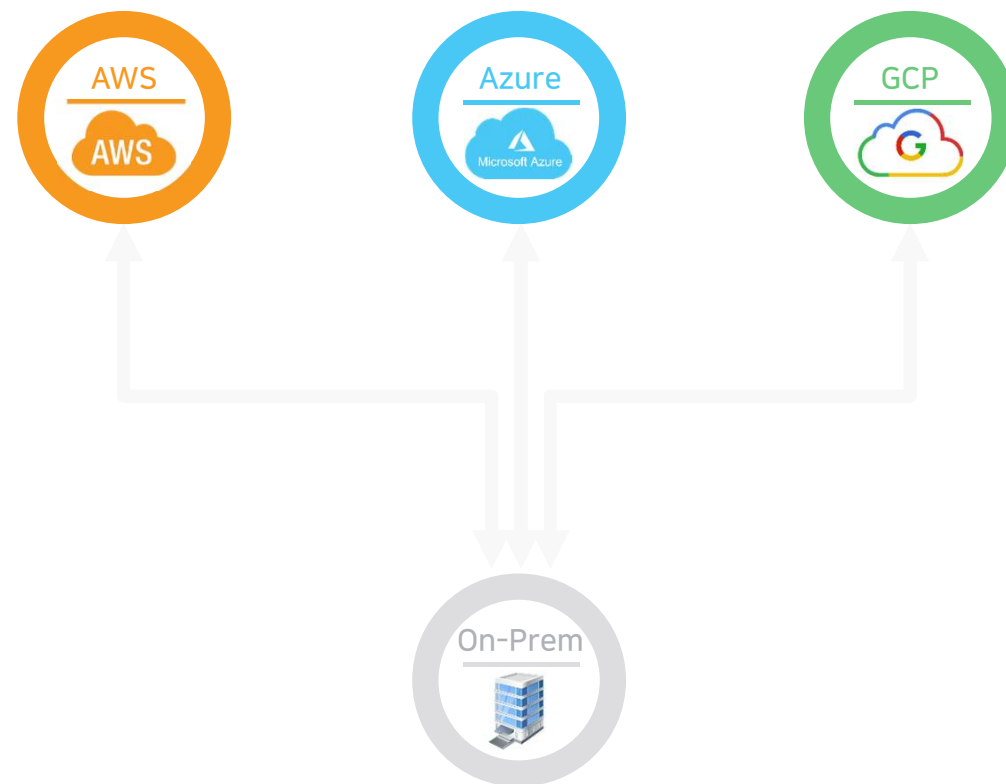




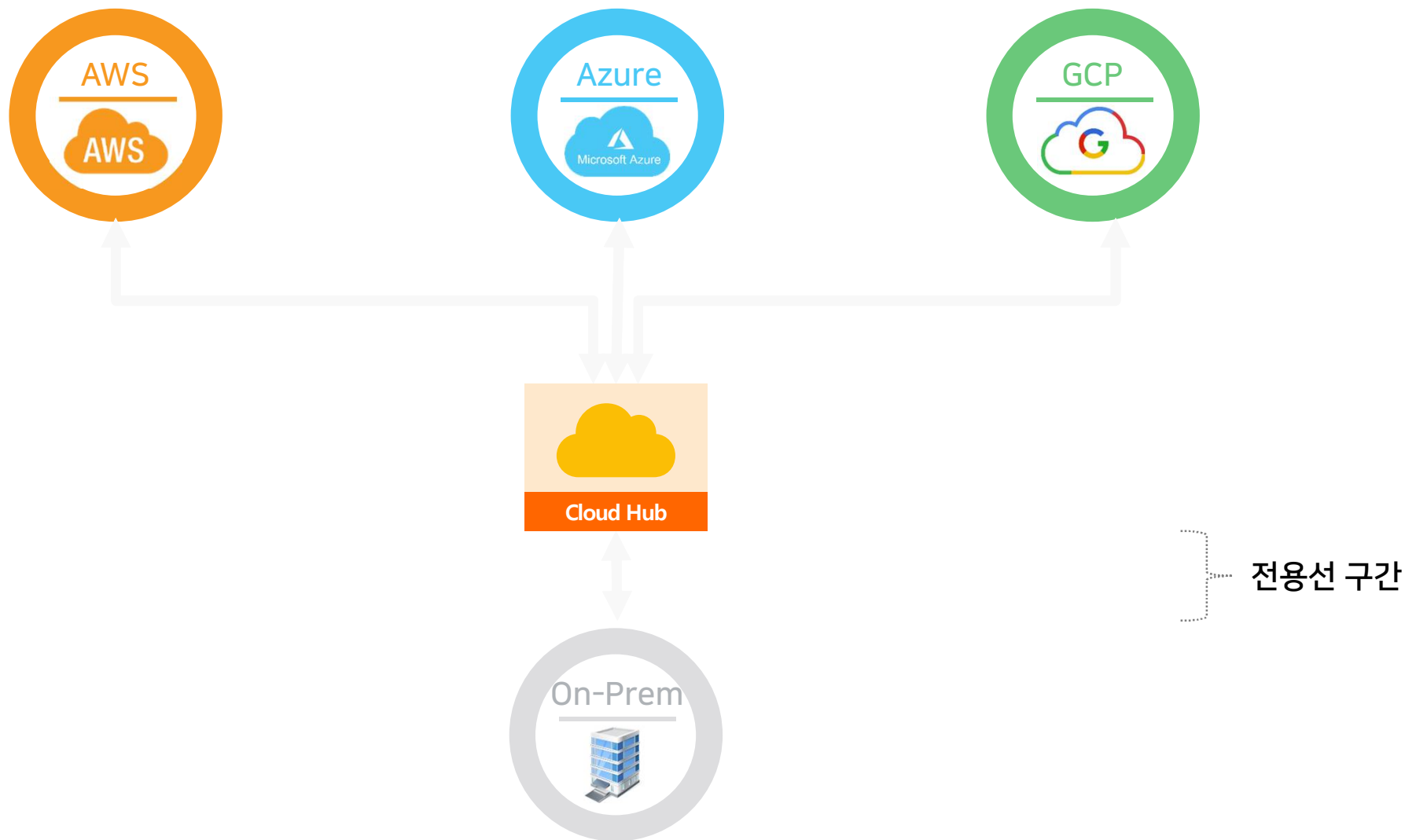
다양한 클라우드 사업자 사용

AI / ML 서비스를 위한 대용량 데이터

고가의 전용선



멀티 클라우드를 위한 전용선 연동 허브 : Cloud Hub

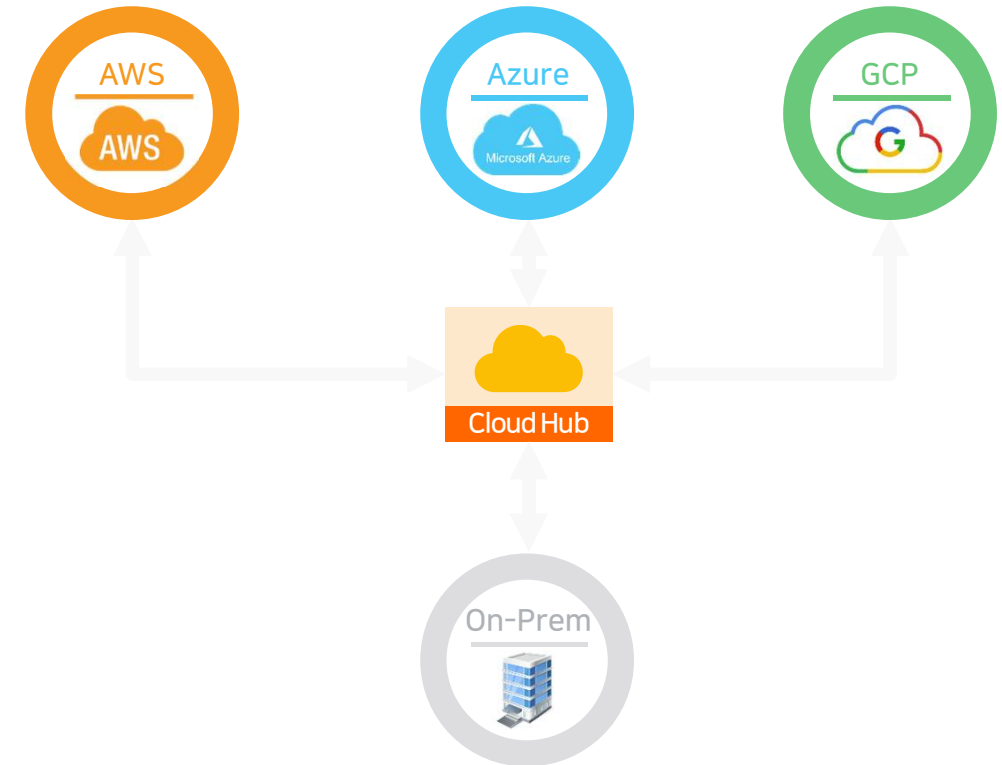
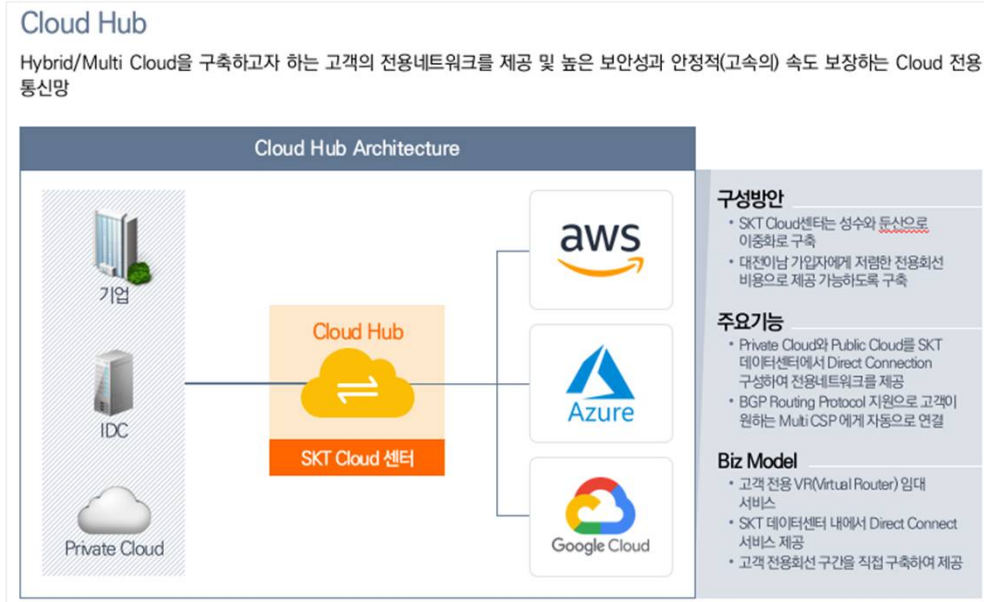


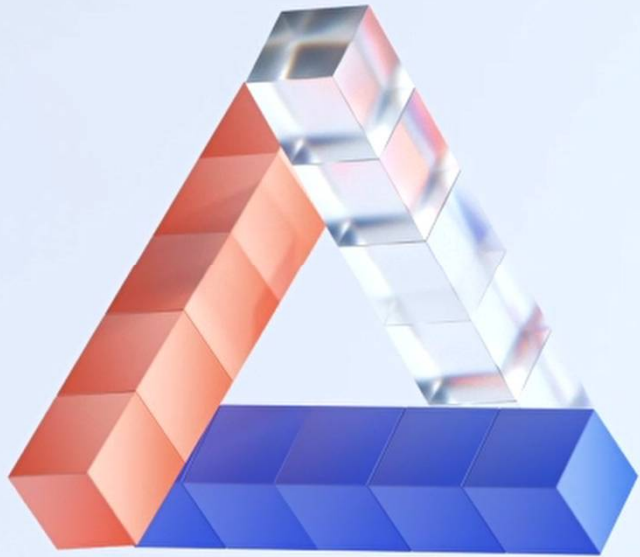
멀티 클라우드를 위한 전용선 연동 허브 : Cloud Hub



Cloud Hub

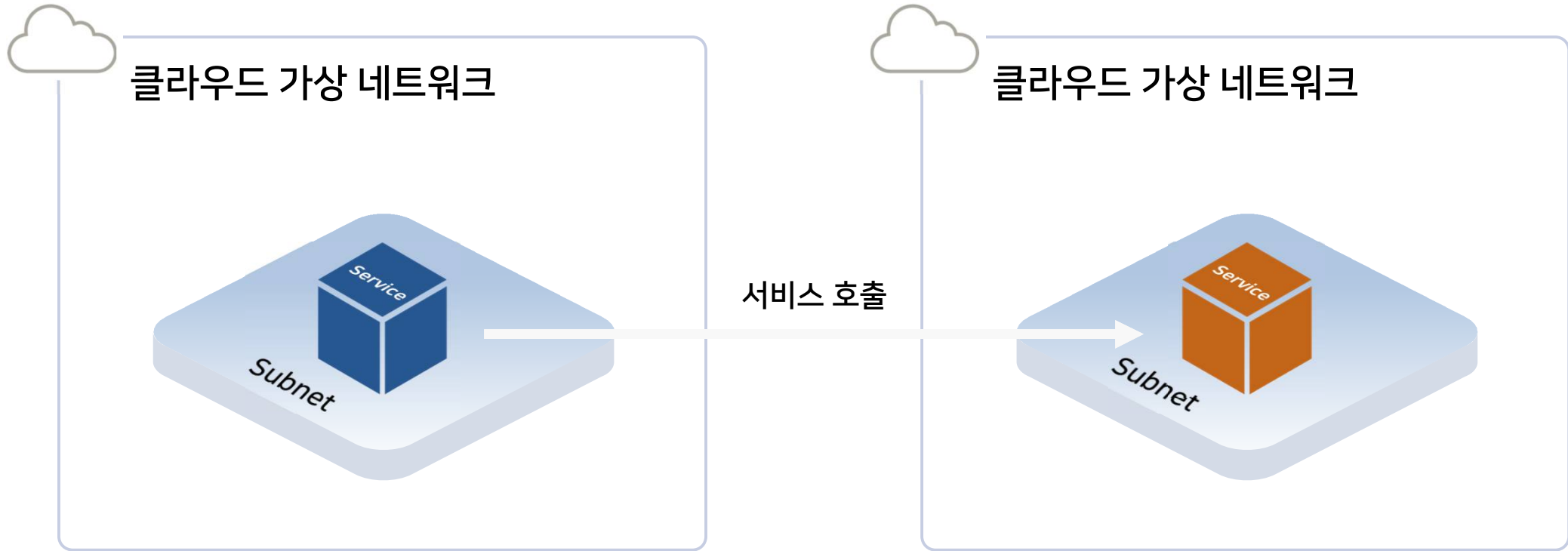
- 멀티 클라우드 구성을 위한 전용선 연동 허브 서비스
- 멀티/하이브리드 클라우드 시의 전용선 비용 최적화
- 멀티 클라우드 간 통신 시의 경로 최적화



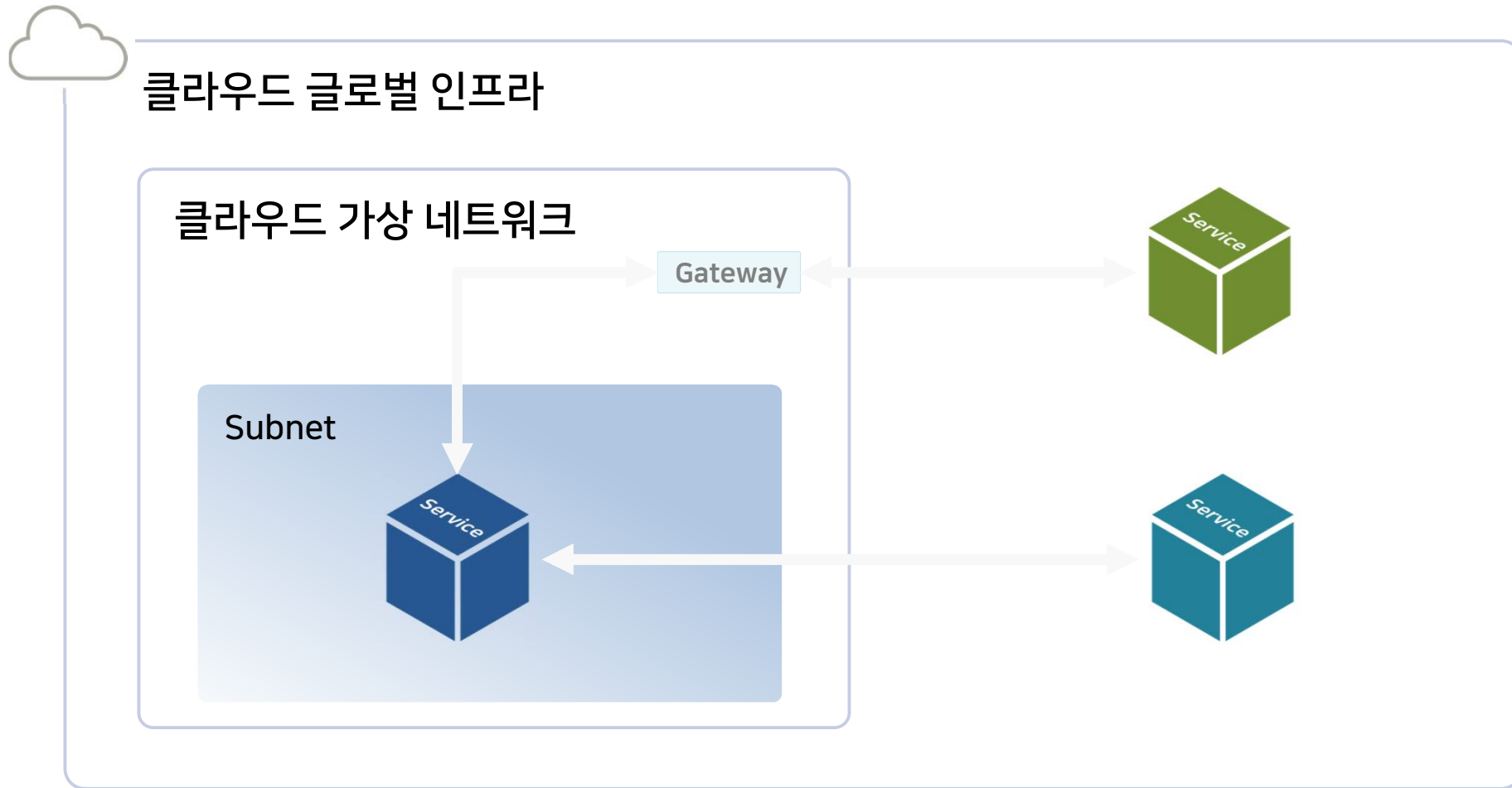


Endpoint와 Private Link

가상 네트워크 간의 Private 통신



Endpoint / Private Link



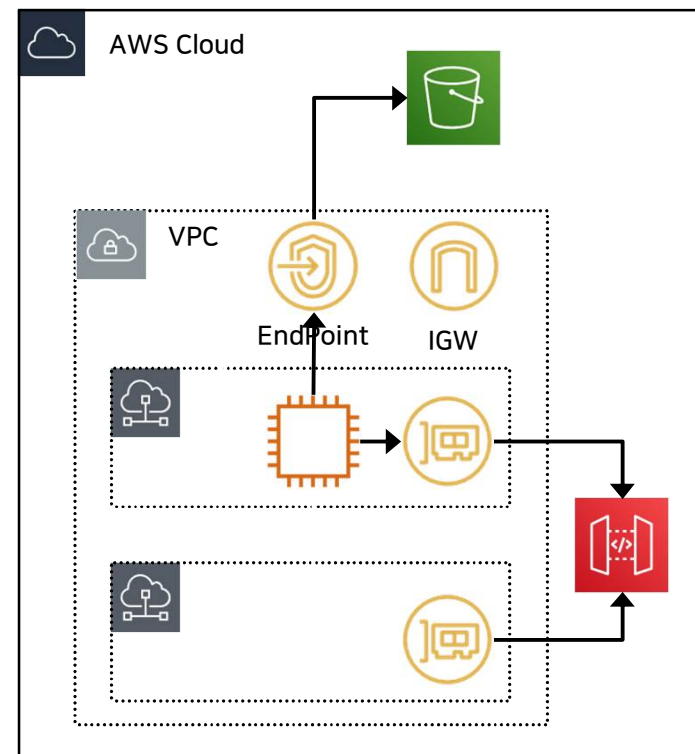


Gateway Type

- Public 서비스 접근을 Gateway 생성
- 라우팅 Target이 Gateway Endpoint가 됨
- S3 , DynamoDB

Interface

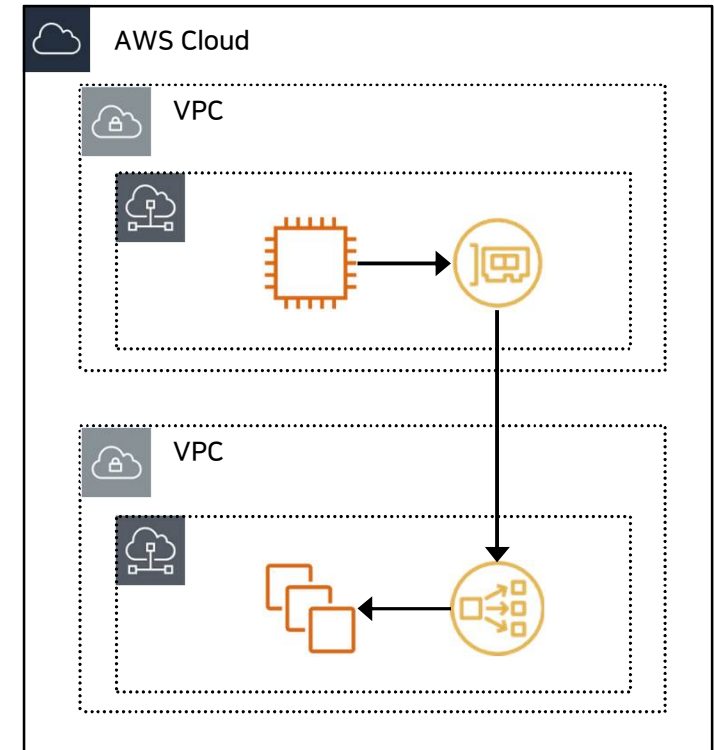
- Endpoint가 VPC 내에 ENI(Elastic Network Interface)로 생성
- Public Service 접근 시, ENI로 접근 가능
- API Gateway, App Mesh, Athena, Kinesis 등 다수





Private Link Service

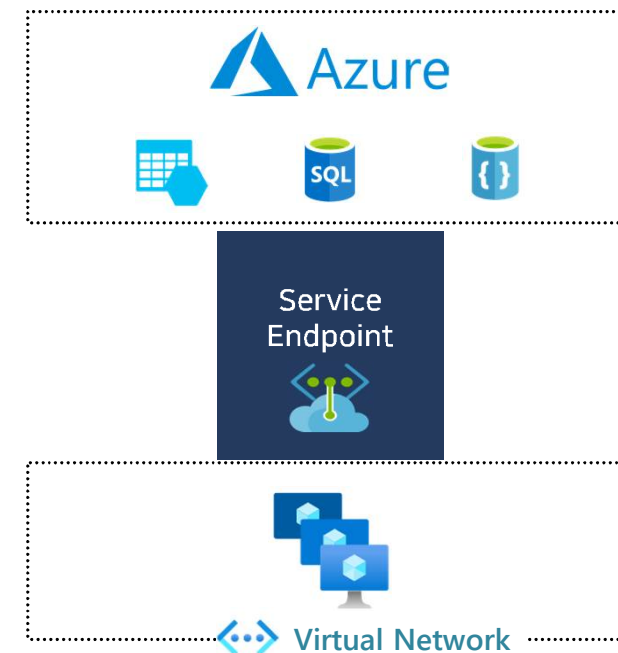
- 사용자가 만든 서비스를 Private Link를 통해서 사용할 수 있도록 제공하는 서비스
- Network Load Balancer를 이용해서 구성





Service Endpoint

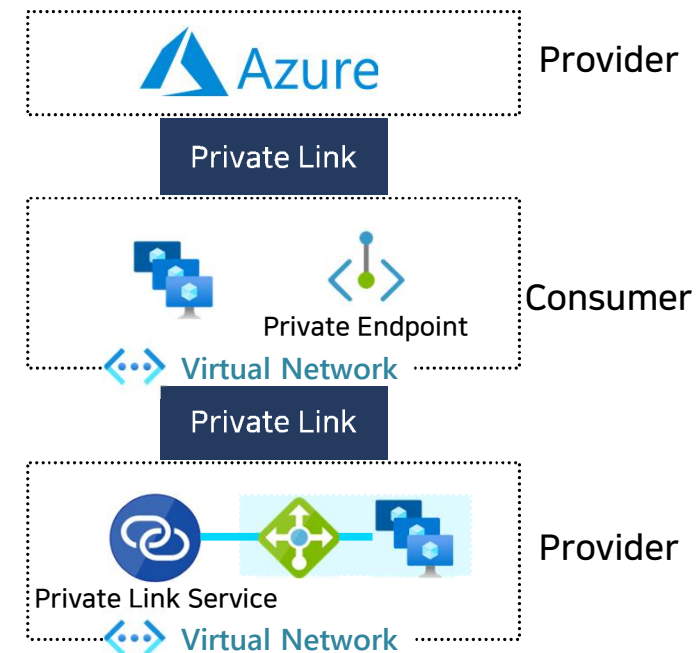
- Azure 가상 네트워크의 Service Endpoint를 이용해서 Azure PaaS Service(Azure Storage, Cosmos DB, SQL Database 등)에 접근할 수 있도록 하는 서비스
- Service Endpoint를 이용하는 경우 Azure 가상 네트워크는 인터넷 경로를 사용하지 않고, Microsoft Backbone 네트워크를 사용





Private Link

- Azure 가상 네트워크의 Private Endpoint를 이용해서 Azure PaaS Service(Azure Storage, Cosmos DB, SQL Database 등)와 Azure에 올린 사용자/파트너 서비스에 접근 할 수 있도록 하는 서비스
- Private Link를 이용하는 경우 Azure 가상 네트워크는 인터넷 경로를 사용하지 않고, Microsoft Backbone 네트워크를 사용



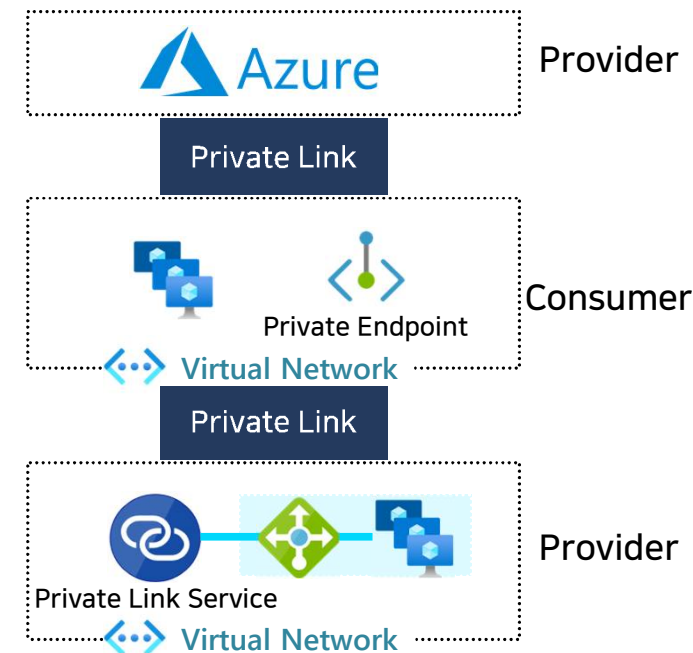


Private Endpoints

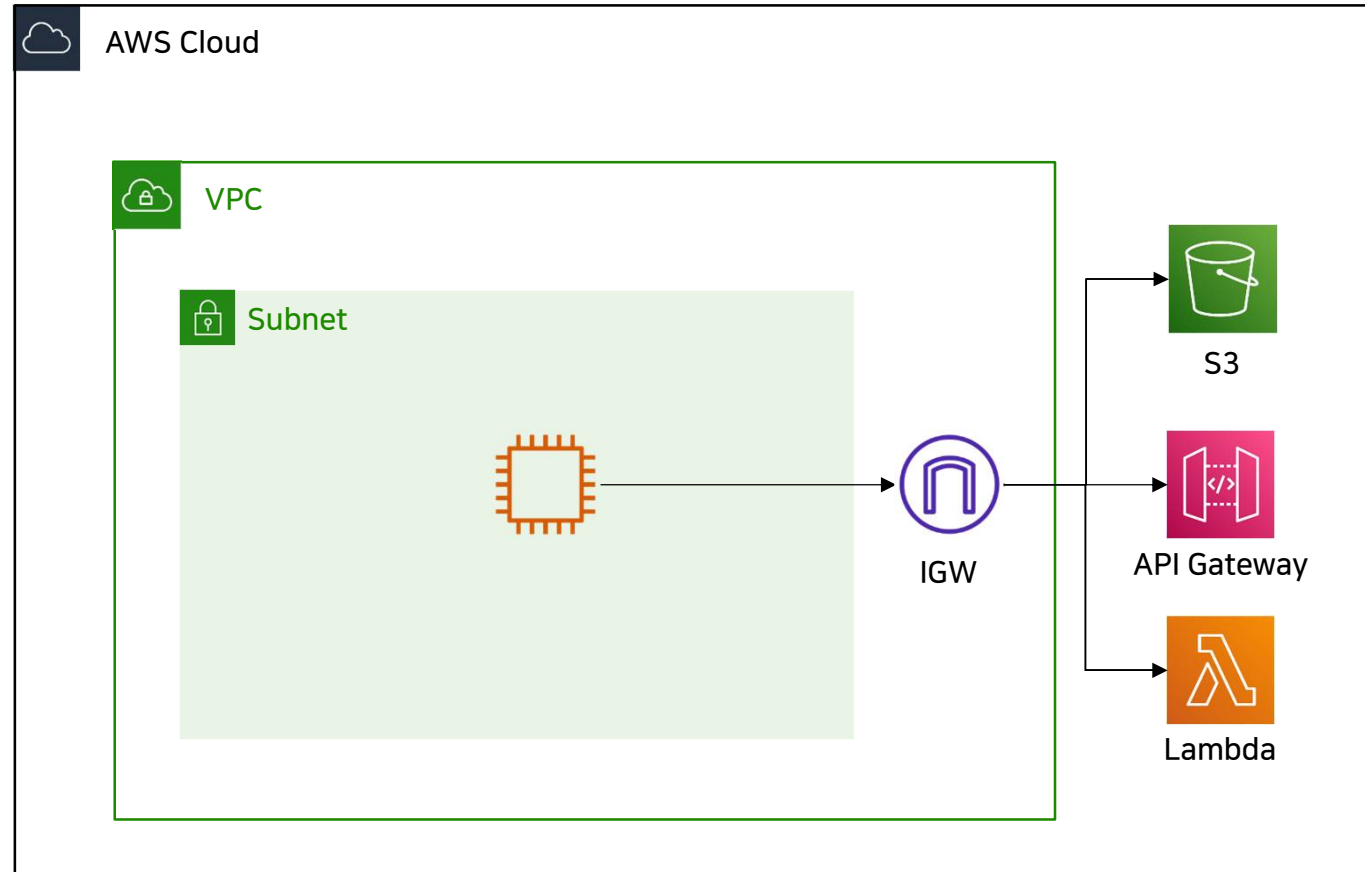
- 가상 네트워크에서 Private Link가 제공하는 서비스로 연결하기 위한 네트워크 인터페이스
- Azure 가상 네트워크의 서브넷에 Private IP를 사용

Private Link Service

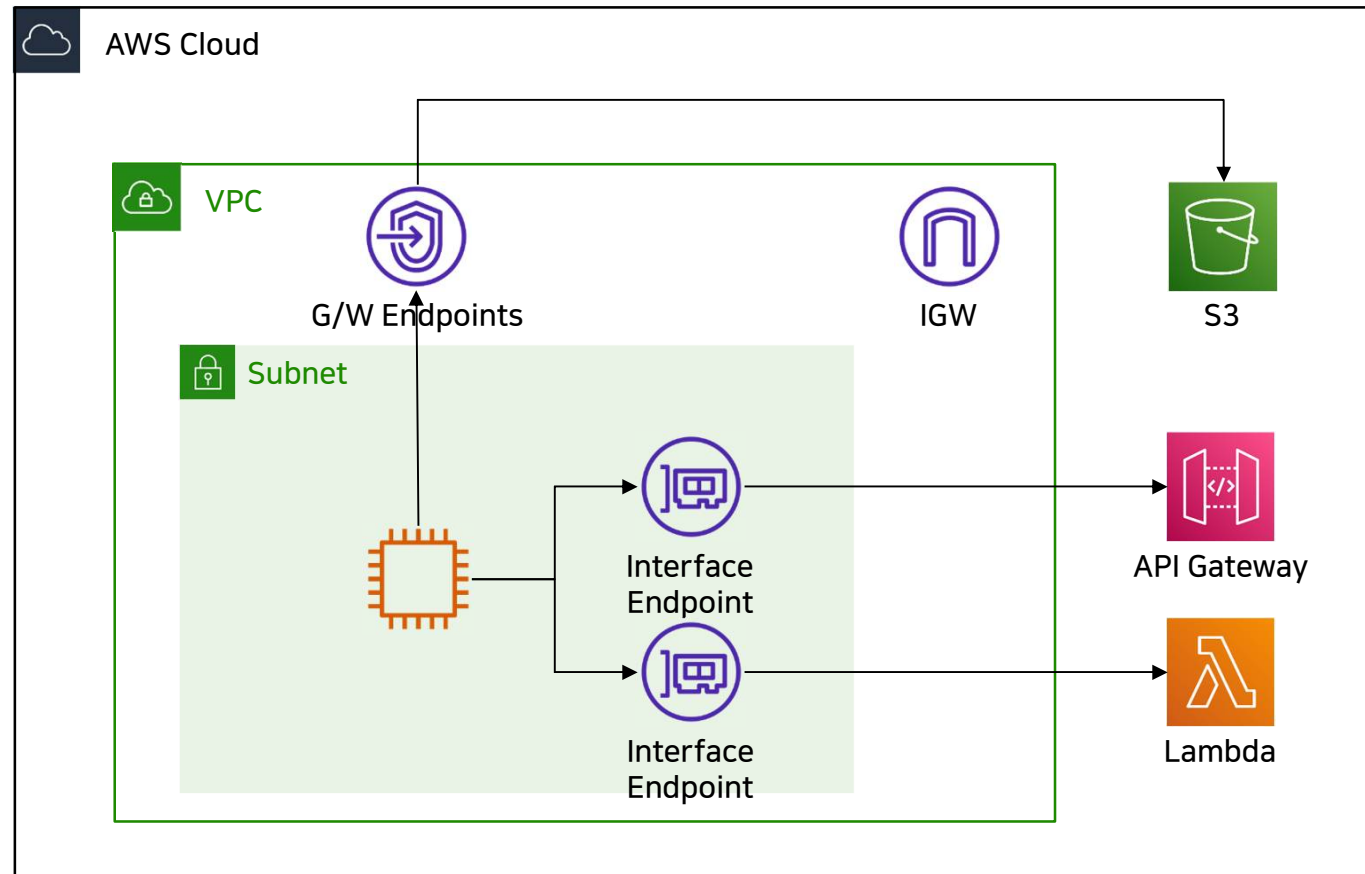
- 사용자가 만든 서비스를 Private endpoint에서 사용할 수 있도록 제공하는 서비스
- Standard Load Balancer를 이용해서 구성



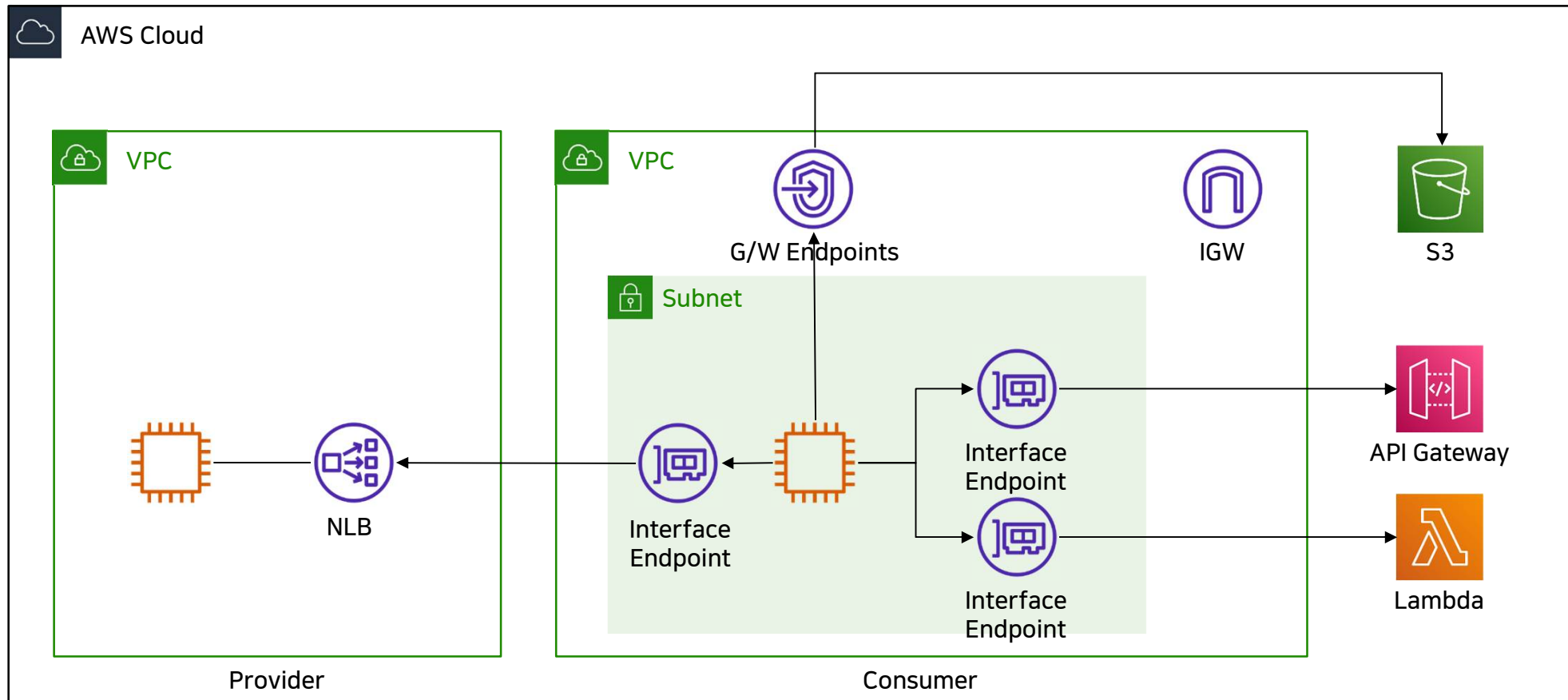
AWS Endpoint

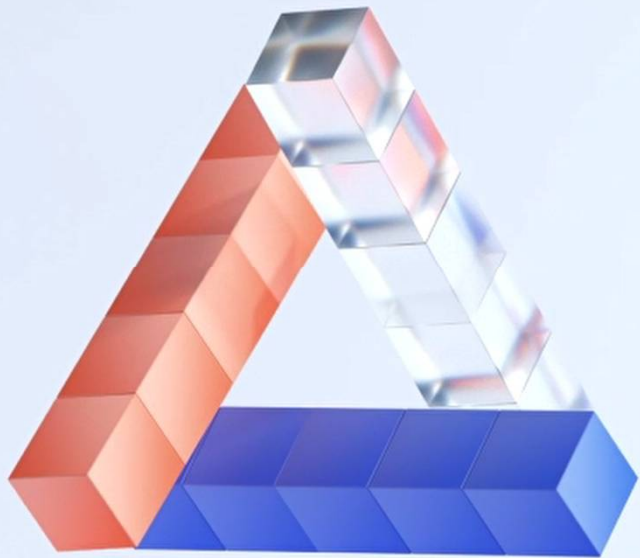


AWS Endpoint/Private Link



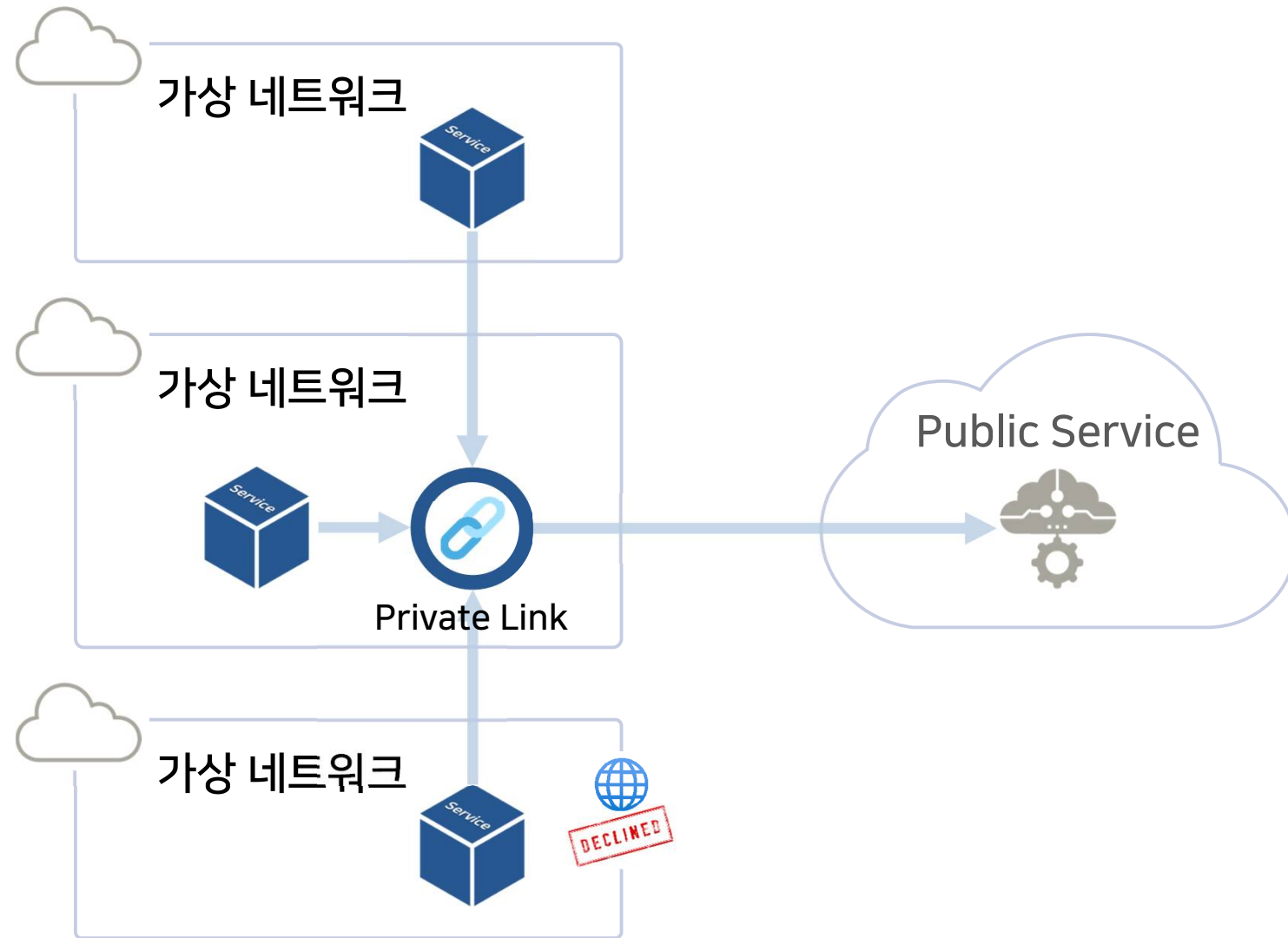
AWS Endpoint/Private Link





클라우드 연동 방안 활용

Private Link 활용하기





중복된 네트워크 대역을 갖는 On-Prem과 Private 연동



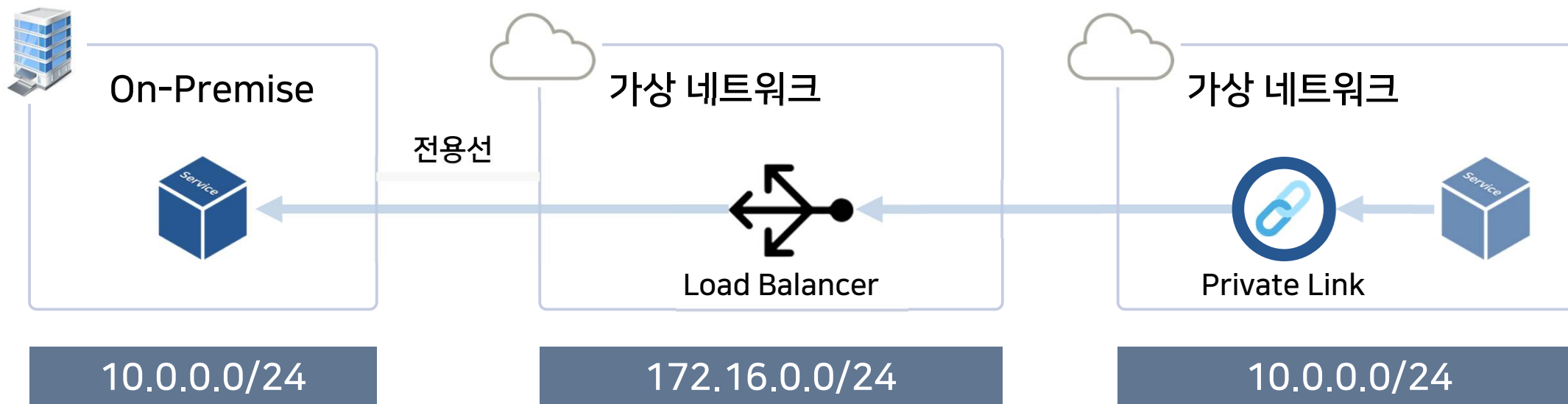
On-Prem → Cloud



중복된 네트워크 대역을 갖는 On-Prem과 Private 연동



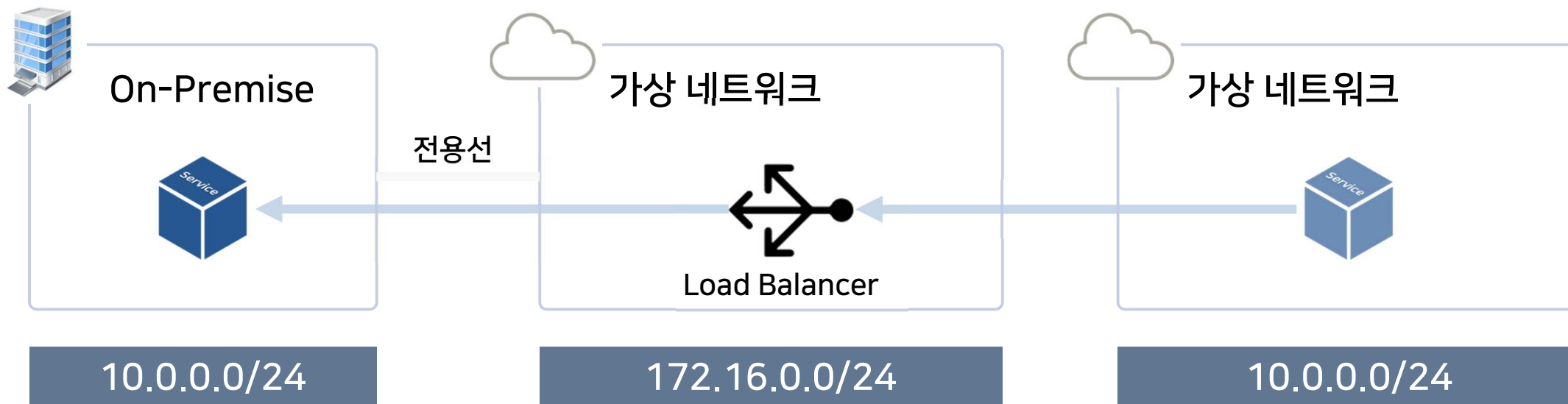
Cloud → On-Prem



중복된 네트워크 대역을 갖는 On-Prem과 Private 연동



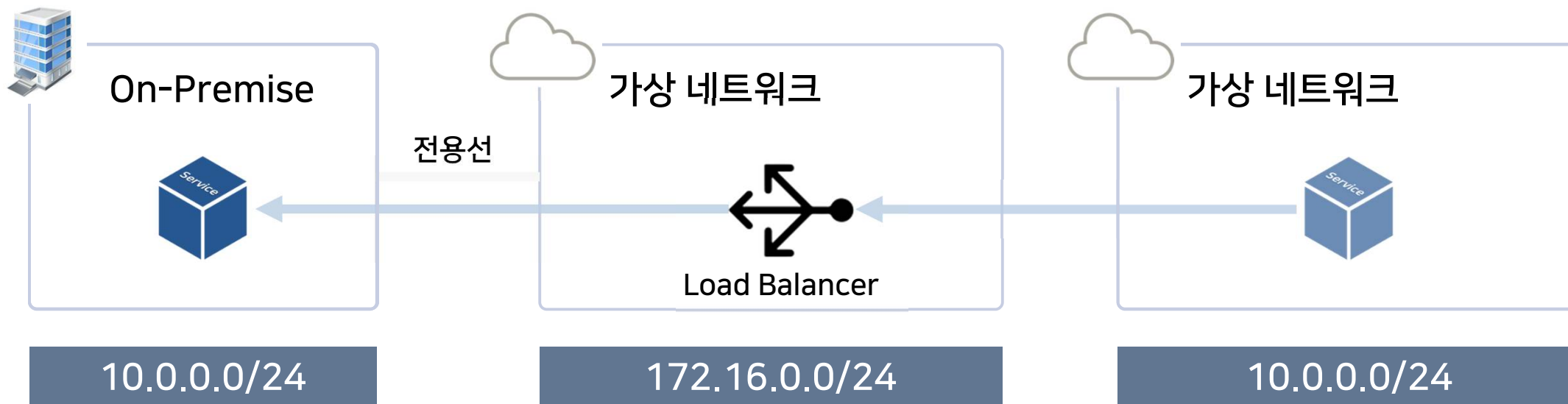
Cloud → On-Prem



중복된 네트워크 대역을 갖는 On-Prem과 Private 연동



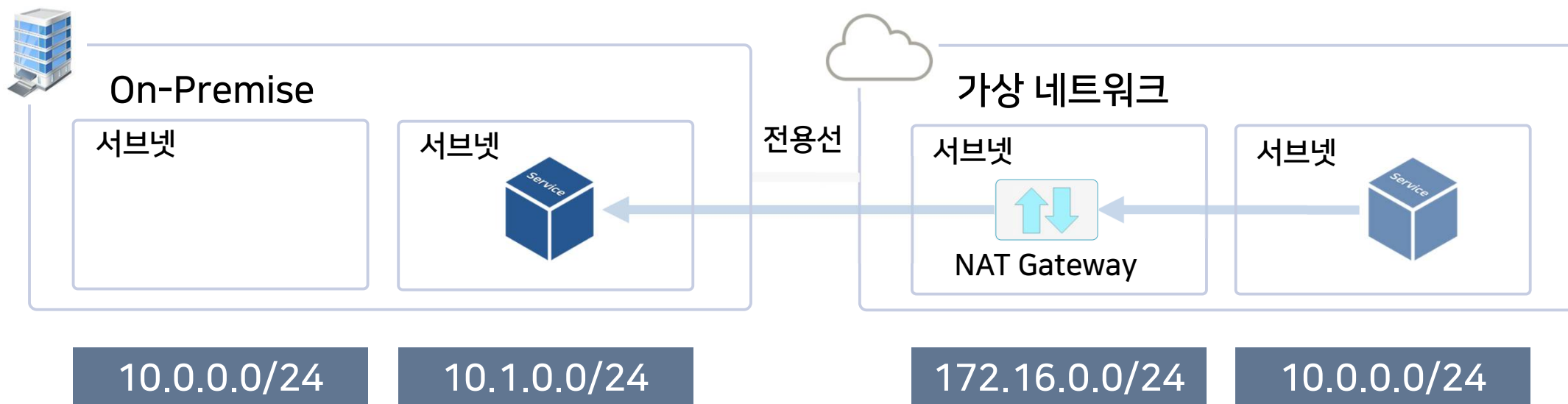
Cloud → On-Prem



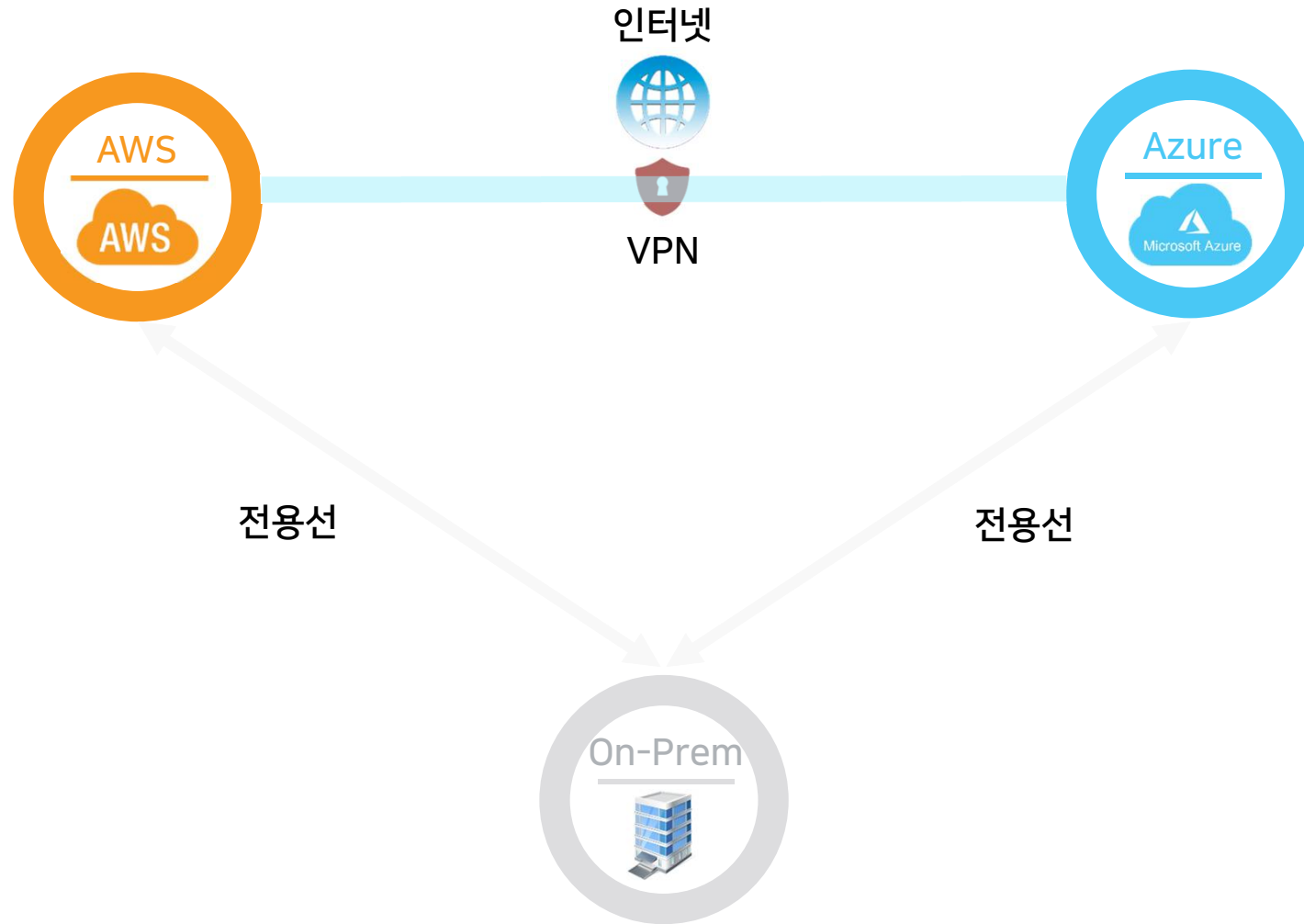
중복된 네트워크 대역을 갖는 On-Prem과 Private 연동



Cloud → On-Prem



CSP 간의 VPN 연동을 통한 이중화





Thank you

