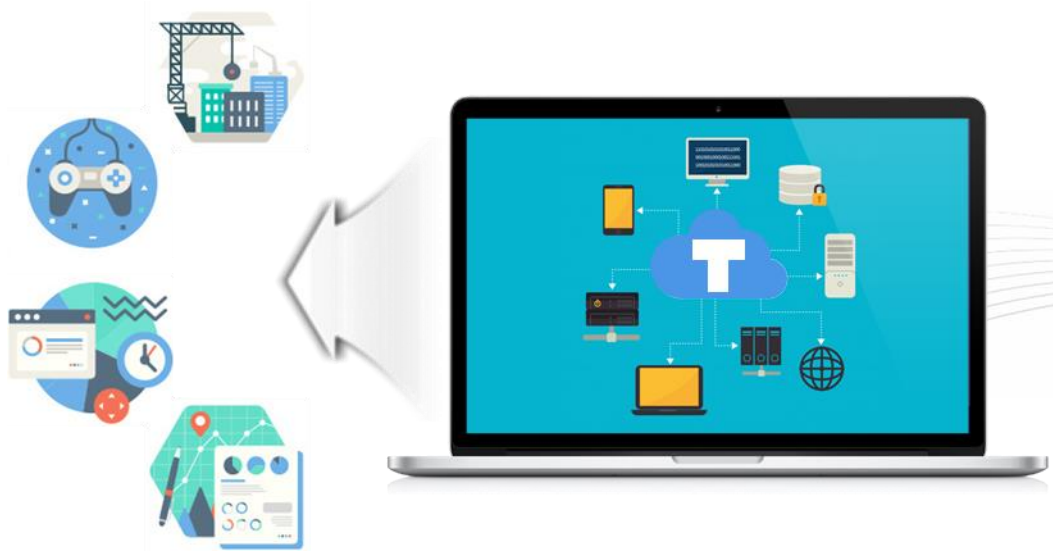


(이론) GCP-4차수

Ⅰ 멀티 클라우드 개념

Ⅱ GCP 하이브리드 네트워킹

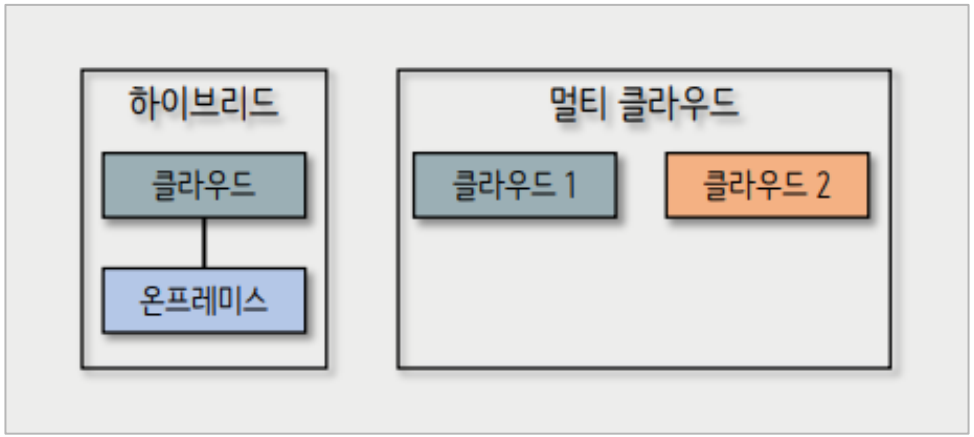
Ⅲ GCP 코어 네트워킹

하이브리드 클라우드

- 하나 이상의 프라이빗 클라우드와 하나 이상의 퍼블릭 클라우드의 조합을 사용하여 애플리케이션을 실행하는 클라우드 컴퓨팅 환경
- 퍼블릭 클라우드(AWS, GCP 등)와 프라이빗 클라우드(온프레미스 데이터 센터 or '에지') 의 컴퓨팅, 스토리지, 네트워킹, 서비스의 조합을 사용

멀티 클라우드

- 2개 이상의 프라이빗 클라우드 또는 2개 이상의 퍼블릭 클라우드 또는 퍼블릭과 프라이빗 클라우드의 조합 등의 여러 클라우드의 조합을 활용하는 클라우드 컴퓨팅 모델



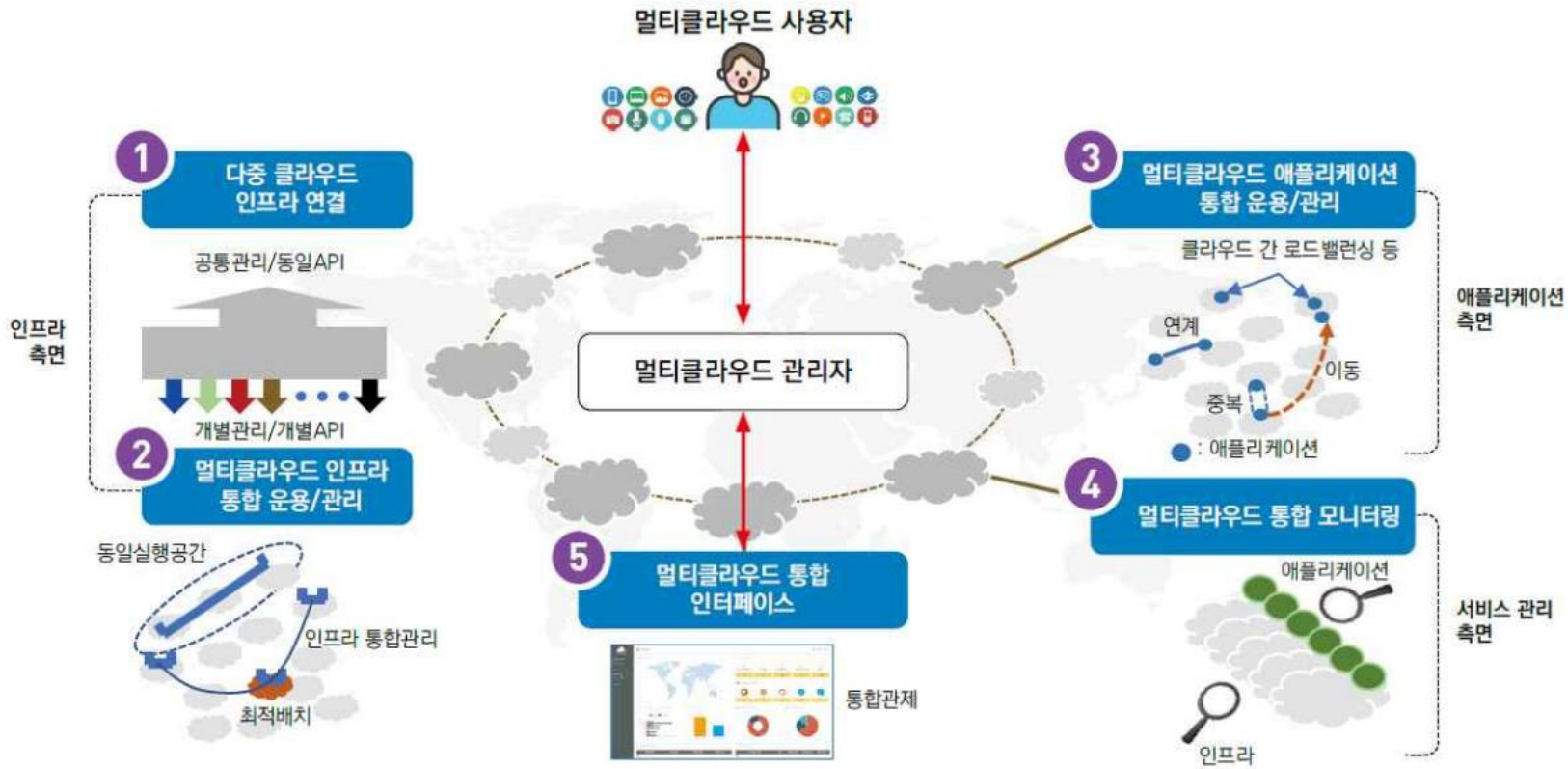
[그림 1] 하이브리드 클라우드와 멀티 클라우드

멀티 클라우드 장단점

장점	단점
유연성	복잡성
근접성 및 네트워크 성능	네트워크 트래픽 비용
공급업체 종속성 완화	여러 클라우드의 이식성 보장
	X
	기술 격차

멀티 클라우드 관리 주요 기술

- 멀티클라우드 관리 기술을 사용자가 직접 구현하여 이용하는 것이 어렵기 때문에, 사용자는 제3의 사업자 지원을 통해 제공받는 경우가 일반적이며, 시장에서는 이를 위한 다양한 기술이 제공됨



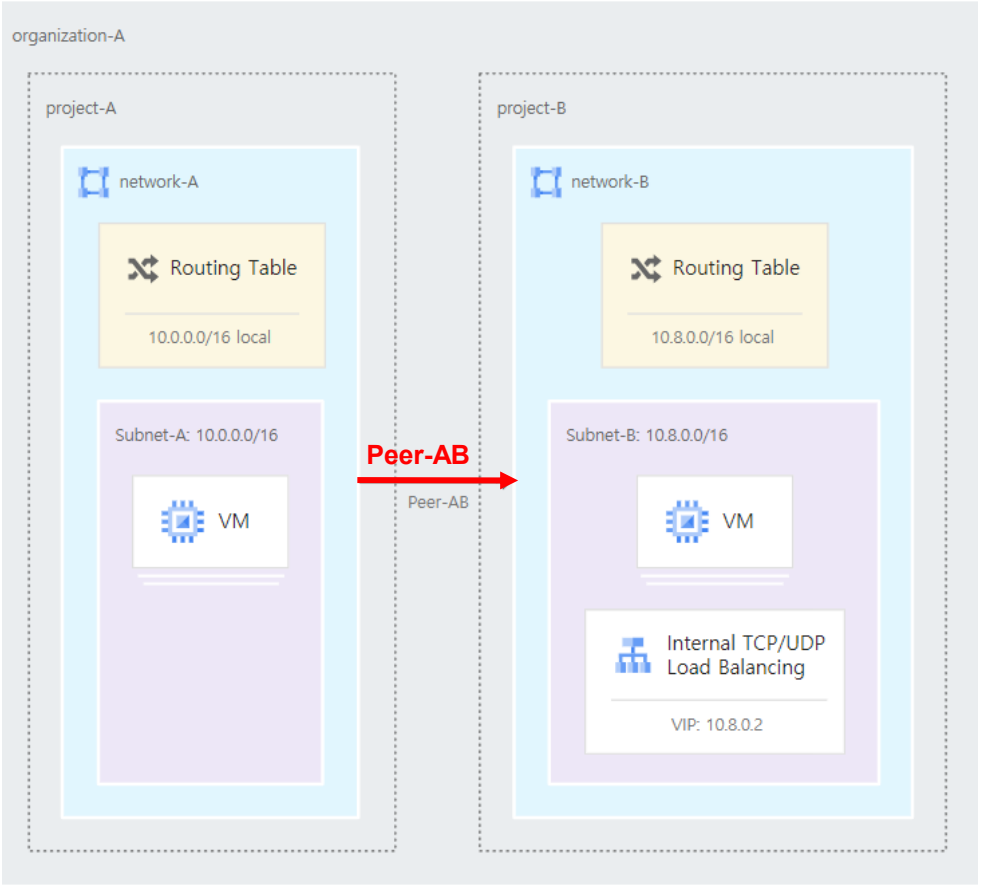
[그림 2] 멀티클라우드 관리 주요 기술

VPC 네트워크 피어링

- GCP 내 두 VPC(동일·다른 프로젝트·조직 포함)를 내부 IP로 직접 연결
- 두 개의 단절된 Network 환경 간에 전송되는 Traffic을 Public으로 보내지 않고 곧바로 상대의 Network 환경으로 보내는 연결 방식
- Network 간에 통상적인 Transit 전송을 이용하지 않고 IXP(Internet exchange point)를 이용한 전송을 사용함으로써 Provider의 간섭 없이 Traffic 교환을 하는 방식

특징

- Google 백본만 이용
- 암호화 없이도 VPC 내 통신과 동일한 지연·가용성
- 각 VPC가 자체 서브넷 경로만 교환. Transitive Peering 불가
  (A↔B, B↔C여도 A↔C 불가)
- 피어링 VPC 간 서브넷 CIDR이 겹치면 안 됨



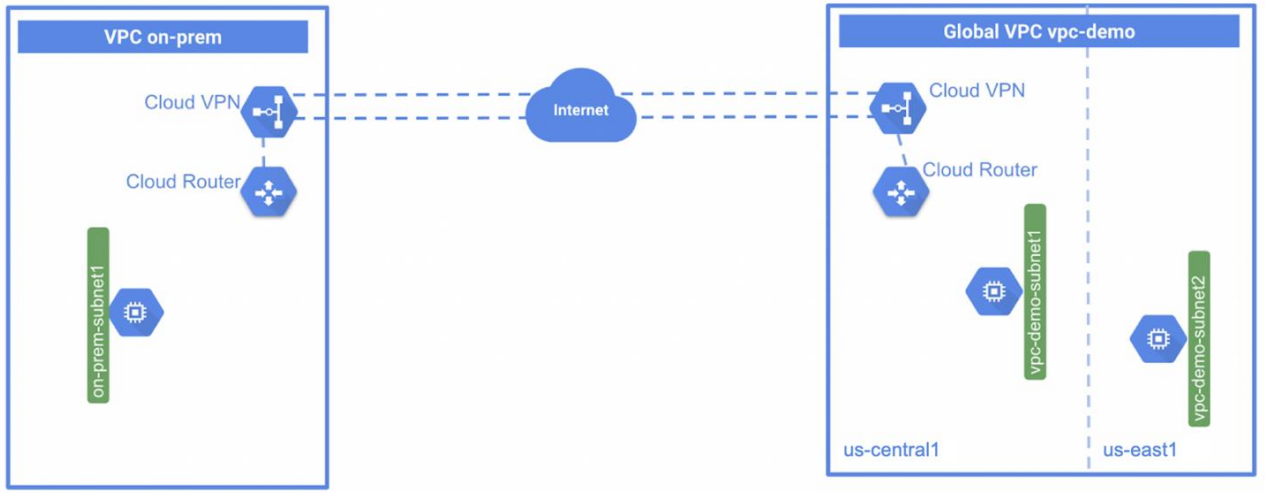
[그림 3] VPC 네트워크 피어링 예시

VPC 네트워크 피어링

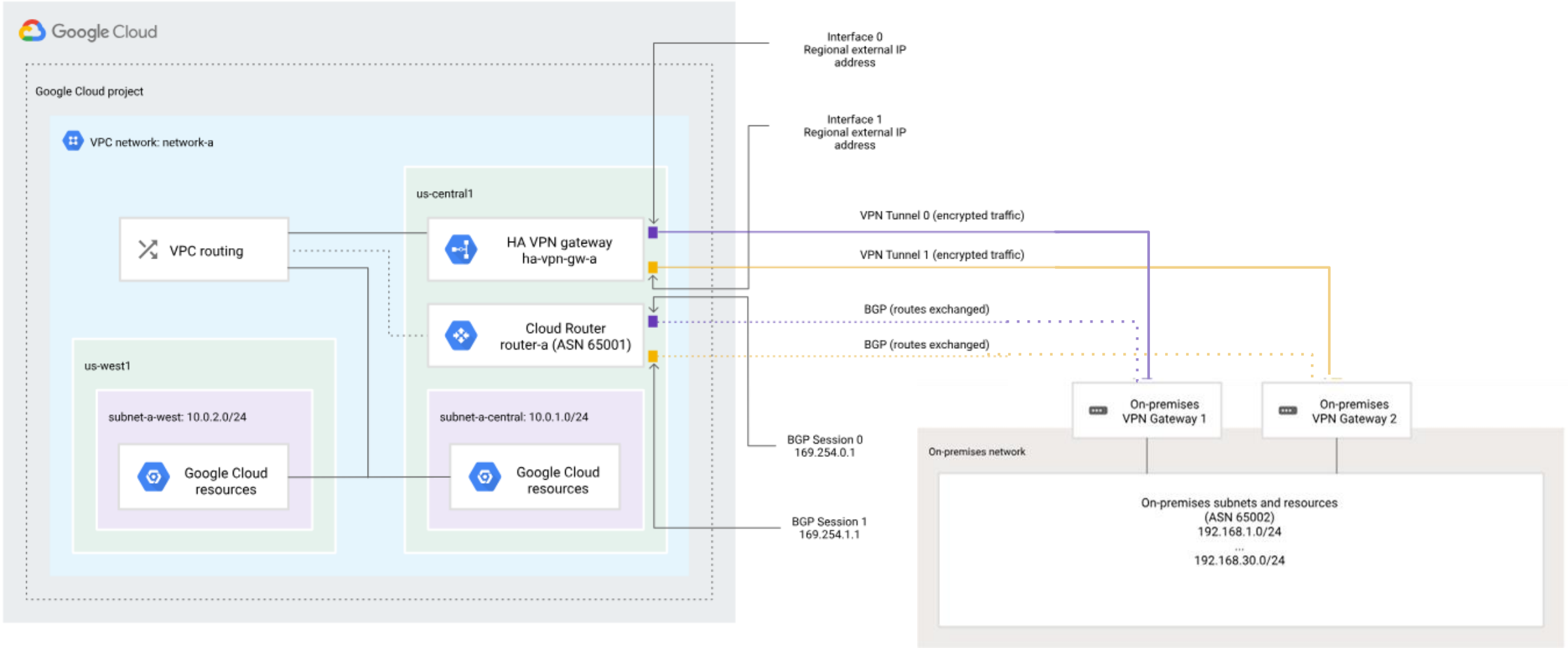
- VPC ↔ 온프레미스, 다른 클라우드, 또는 GCP 내 다른 VPC(드물게) 와 연결할 때, 전송 중인 데이터를 IPsec으로 암호화하여 연결하는 방식
- VPN 연결은 암호화를 처리하는 VPN 게이트웨이 하나와 복호화를 처리하는 다른 VPN 게이트웨이로 네트워크 간에 이동하는 트래픽을 암호화

특징

- 전송 단계에서 IPsec 적용 → 외부망 경유에도 기밀성 확보
- 라우팅은 퍼블릭 경로이므로 대역폭·지연이 회선 및 ISP 품질에 영향받음
- 장비 투자 없이 빠르게 연결을 시험할 때 유리



[그림 4] Google Cloud HA-VPN



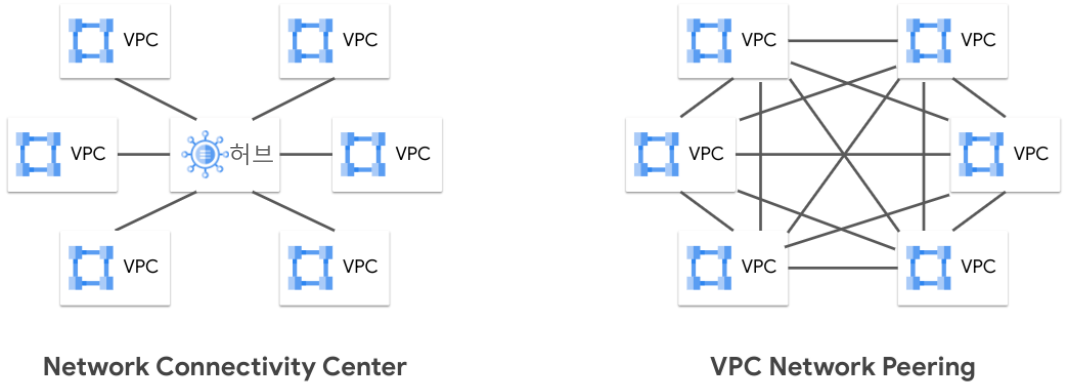
[그림 5] GCP와 온프레미스 VPN 연결 예시

Network Connectivity Center

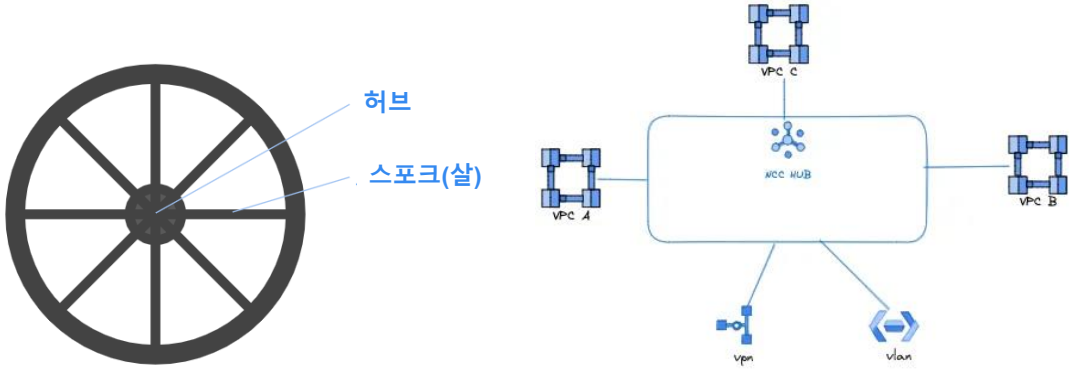
- Hub라는 중앙 관리 리소스에 연결된 Spoke 리소스 간의 네트워크 연결을 간소화하는 오케스트레이션 프레임워크
- 개별 쌍별 VPC 네트워크 피어링 연결을 관리하는 데 따른 운영 복잡성을 줄임

특징

- Hub and Spoke 구조 (Hub는 VPC Spoke 또는 하이브리드 Spoke만 가질 수 있음)
- Hub는 transitive connectivity를 제공하지 않음
  (A↔B, B↔C여도 A↔C 불가) ?



[그림 6] VPC 네트워크 피어링과의 차이



[그림 7] Hub and Spoke 네트워크

허브

- Network Connectivity Center 허브는 스포크를 연결하는 전역 리소스
- 단일 허브에 여러 리전의 스포크가 포함될 수 있음

스포크

- 스포크는 허브에 연결된 하나 이상의 Google Cloud 네트워크 리소스
- 스포크를 만들 때는 지원되는 하나 이상의 리소스와 연결해야 함(지원 리소스)

유형	설명
VPC 스포크	• 허브에 VPC 네트워크를 연결 • 연결된 다른 스포크 VPC의 모든 서브넷 경로를 가져오는 방식
프로듀서 VPC 스포크	• 허브에 GCP 에서 제공하는 서비스의 서비스 제작자 네트워크와 연결 • 예) Cloud SQL, Filestore, Looker, Vertex AI 등
하이브리드 스포크	**라우터 어플라이언스 스포크** • 라우터 어플라이언스 VM 인스턴스와 연결된 스포크
	HA VPN 터널 스포크 • Cloud VPN 터널과 연결된 스포크
	Cloud Interconnect VLAN 연결 스포크 • Cloud Interconnect VLAN 연결과 연결된 스포크

[표 1] 스포크 유형

Cloud Interconnect

- Google Cloud Platform (GCP)와 다른 네트워크 (온프레미스 또는 다른 클라우드) 간의 고대역폭, 저지연 연결을 제공하는 서비스
- 온프레미스 네트워크와 Google Cloud 간의 물리적 또는 파트너를 통한 전용 회선을 통해 고속 연결을 제공

특징

- GCP 리소스에 내부 IP 주소를 사용하여 통신할 수 있음
- 고속연결·저지연·안정적 연결
- HA VPN을 활용하여 트래픽에 IPsec 암호화 적용 가능

종류	설명
Dedicated Interconnect	• Google 데이터센터와 고객 온프레미스 데이터센터 간의 물리적 연결을 제공
Partner Interconnect	• Google과 협력하는 서비스 제공업체를 통해 연결을 제공

[표 2] Cloud Interconnect 종류

위치	서비스 제공업체	유형
서울	콘솔 Connect by PCCW Global	Layer 2, Layer 3
	Dreamline	Layer 2
	Equinix	Layer 2, Layer 3
	KINX	Layer 2, Layer 3
	KT Cloud	Layer 2, Layer 3
	LG CNS	Layer 2, Layer 3
	LG Uplus	Layer 2, Layer 3
	Sejong Telecom	Layer 2
	SK텔레콤	Layer 2

[그림 8] Cloud Interconnect 지원 서비스 제공 업체

Cloud Router

- 경계 게이트웨이 프로토콜(BGP : Border Gateway Protocol)를 사용하여 VPC 네트워크와 원격 네트워크 간의 최적 경로를 자동으로 선택하고 유지하는 서비스
- Cloud Router는 Cloud Interconnect, Cloud VPN, 라우터 언플라이언스에 BGP 서비스를 제공과 Cloud NAT의 제어 영역 역할을 함

주요 기능	설명
BGP 세션 관리	**양방향 전달감지 (BFD : Bidirectional Forwarding Detection)** • 대부분의 상용 라우터에서 지원하는 전달 경로 중단 감지 프로토콜 • BGP 기반 장애 감지는 60초가 걸리는 것과 달리 기본 설정으로 구성된 BFD에서는 5초 내에 장애를 감지 **MD5 인증** • BGP 피어 간의 세션에서 메시지 무결성을 보장하기 위해 사용되는 보안 • 기본적으로 Cloud Router BGP 세션은 MD5 인증을 사용하지 않지만, HA VPN, Cloud Interconnect 제품과 함께 사용하면 MD5 인증을 사용할 수 있음
공지된 경로 (Advertised Routes)	• 온프레미스나 타 클라우드 라우터에게 연결된 VPC의 IP 주소 범위 공지 • 기본값은 VPC 전체 서브넷 공개지만, 필요한 서브넷만 선택하여 공지 가능
학습된 경로 (Learned Routes)	• BGP 피어가 보내오는 목적지 프리픽스를 받아서 VPC 내부에 동적 경로로 등록 • 받은 경로가 여러 개거나 지정된 할당량을 초과하면 BGP 세[션을 재설정
BGP 경로 정책 (BGP Route Policy)	• 들어오거나 나가는 BGP 경로를 조건-행동 쌍으로 필터/수정하는 규칙 집합

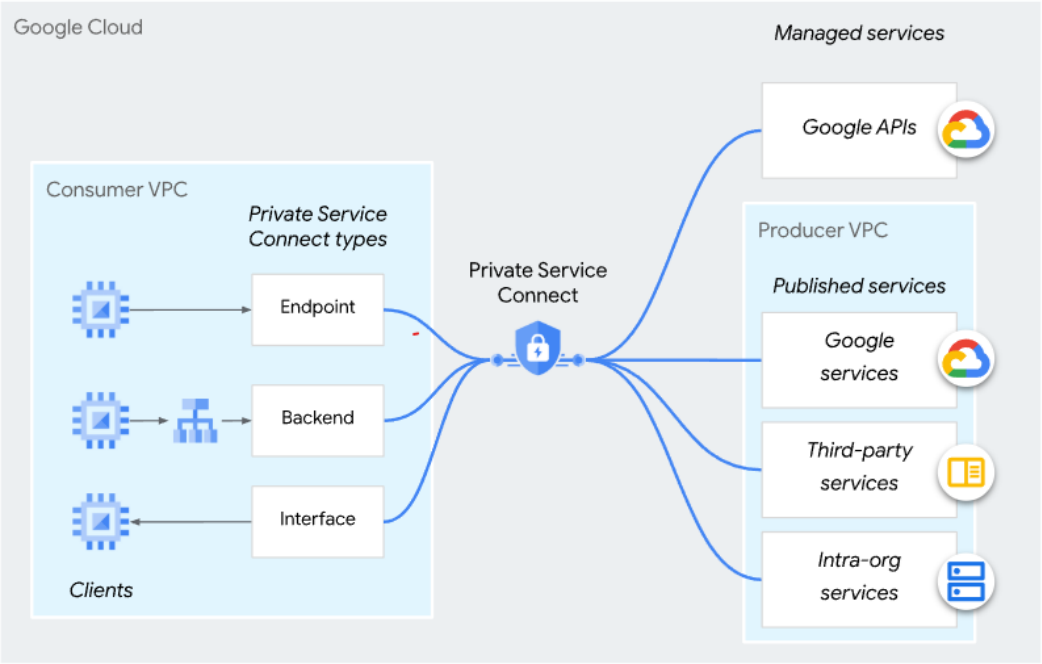
[표 3] Cloud Router 주요 기능

Private Service Connect

- 소비자가 VPC 네트워크 내부에서 비공개로 관리형 서비스에 액세스할 수 있도록 허용하는 Google Cloud 네트워킹 기능
- 엔드포인트(전달 규칙 기준) 또는 백엔드(부하 분산기 기준)를 사용하여 Cloud Storage 또는 BigQuery와 같은 Google API에 액세스 가능

특징

- 내부 IP 주소를 사용하여 서비스에 액세스
- 트래픽이 중간 홉 또는 프록시 없이 소비자에서 프로듀서 백엔드로 직접 이동
- Andromeda라는 Google Cloud의 SDN을 사용하여 구현됨



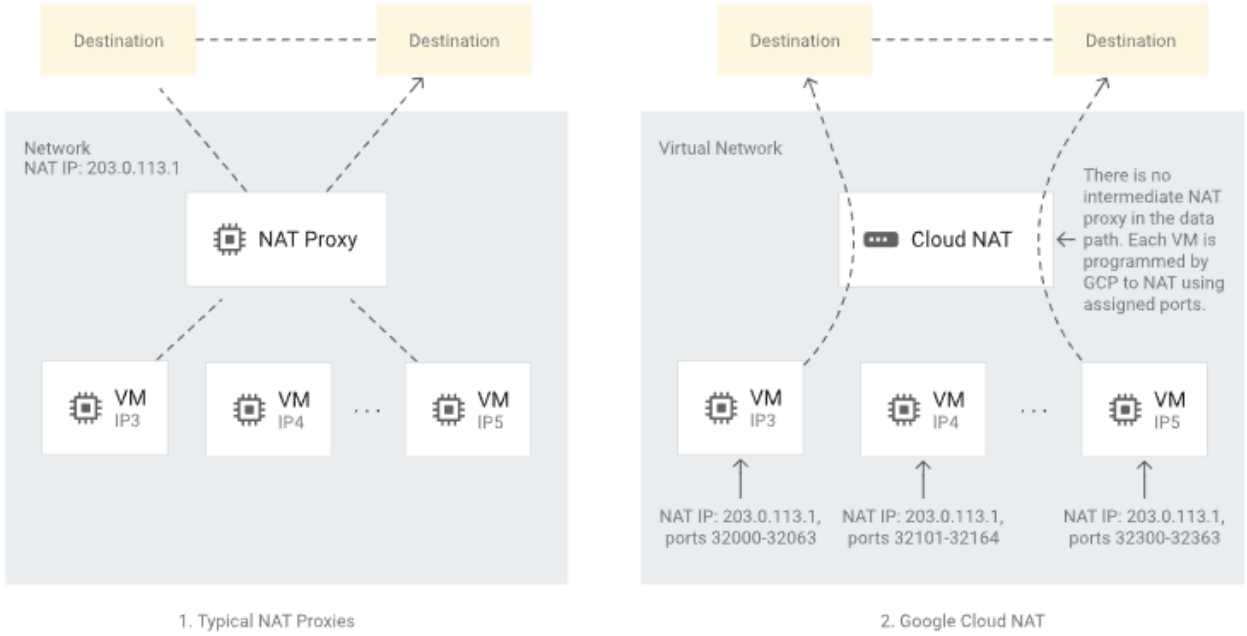
[그림 9] Private Service Connect 예시

Cloud NAT

- Cloud NAT는 Google Cloud 리소스의 아웃바운드 트래픽에 네트워크 주소 변환(NAT)을 제공
- 지원 리소스
  - Compute Engine VM 인스턴스
  - GKE 클러스터
  - Cloud Run, Cloud Run functions, App Engine 표준 환경
  - 리전별 인터넷 네트워크 엔드포인트 그룹(NEG)

Cloud NAT 사용의 이점

- 보안성 :개별 VM이 각각 외부 IP 주소를 가져야 할 필요성을 줄임
- 가용성 : 프로젝트의 VM 또는 단일 물리적 게이트웨이 기기에 의존하지 않
- 확장성 : 사용되는 NAT IP 주소 수를 자동으로 확장하도록 구성됨
- 성능 : VM 별 네트워크 대역폭 저하 X



[그림 10] 기존 NAT와 Cloud NAT 비교

Public NAT

- Google Cloud 리소스(예: VM 인스턴스)가 Public NAT를 사용하여 아웃바운드 연결에 공유 외부 IPv4 주소 및 소스 포트 세트를 할당받고 인터넷과 통신

실행 흐름

1. NAT-GW-US-EAST 에 NAT IP 두 개(192.0.2.50, 192.0.2.60)와 VM 인스턴스 당 최소 64 포트 지정

   예) 예시 VM에는 192.0.2.50:34000 ~ 34063이 할당됨

1. 아웃바운드(Ingress) 통신 흐름

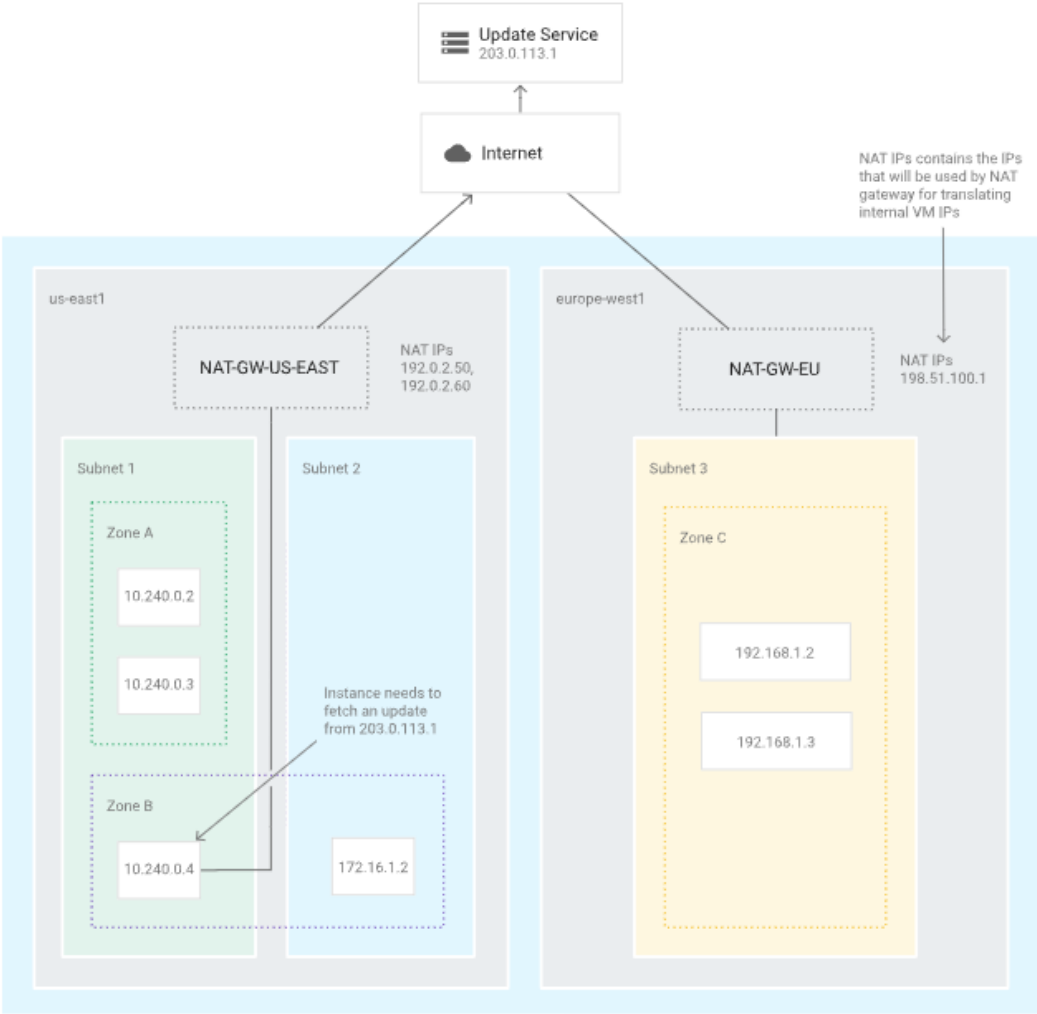
   VM → NAT | 요청패킷 { 10.240.0.4:24000 → 203.0.113.1:80 }

   SNAT 수행 | 요청패킷 { 192.0.2.50:34022 → 203.0.113.1:80 }

1. 인바운드 통신 흐름(응답)

   인터넷 → NAT | 응답패킷 { 203.0.113.1:80 → 192.0.2.50:34022 }

   DNAT 수행 | 응답패킷 { 203.0.113.1:80 → 10.240.0.4:24000 }



[그림 11] Public NAT 변환 예시

Hybrid NAT

- Hybrid NAT를 사용하면 VPC 네트워크가 네트워크의 서브넷 IP 주소 범위가 겹치더라도 온프레미스 네트워크 또는 다른 클라우드 제공업체 네트워크와 통신 가능

실행 흐름

1. 경로 교환(BGO)

   Cloud Router → 외부 라우터에 10.1.2.0/29 공지

   외부 라우터 → Cloud Router에 192.168.2.0/24 공지

   VPC가 목적지 subnet-b 경로 학습

1. pvt-nat-gw 에 NAT IP(10.1.2.0/29, 192.0.2.60)와 VM 인스턴스 당 최소 64 포트 지정

   예) 예시 VM에는 10.1.2.2:34000 ~ 34063이 할당됨

1. 아웃바운드(Ingress) 통신 흐름

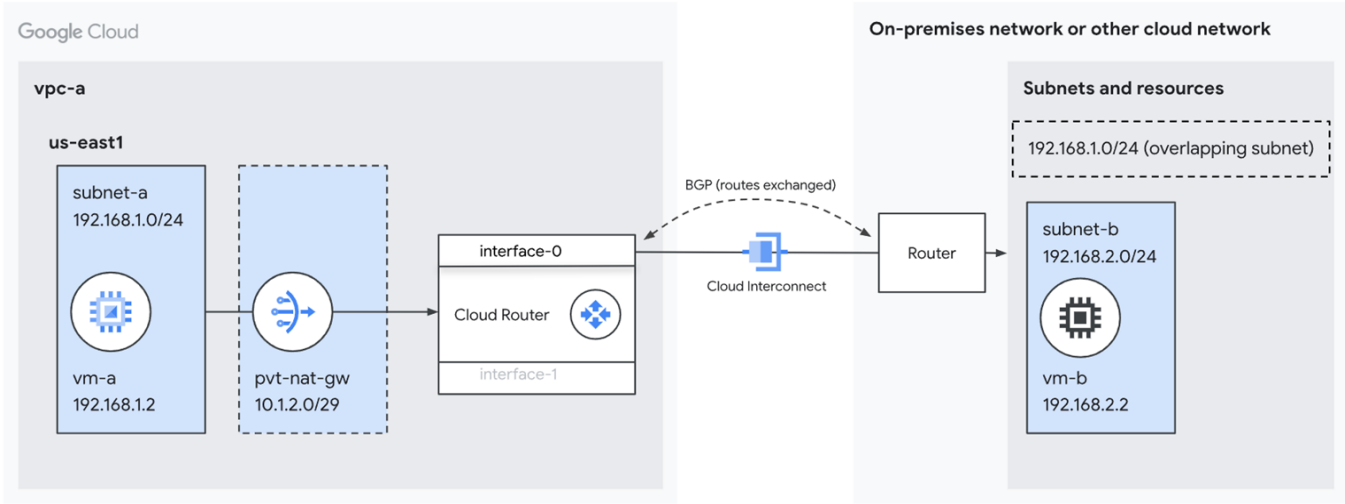
   VM → NAT | 요청패킷 { 192.168.1.2:24000 → 192.168.2.2:80 }

   SNAT 수행 | 요청패킷 { 10.1.2.2:34022 → 192.168.2.2:80 }

1. 인바운드 통신 흐름(응답)

   인터넷 → NAT | 응답패킷 { 192.168.2.2:80 → 10.1.2.2:34022 }

   DNAT 수행 | 응답패킷 { 192.168.2.2:80 → 192.168.1.2:24000 }



[그림 11] Hybrid NAT 변환 예시

추가 설명

vm-a 와 vm-b 를 연결하고 싶어도
vpc-a의 서브넷과 온프레미스의 서브넷의 IP 주소 범위가 겹침이 존재(둘 다 192.168.1.0/24)

이러한 네트워크 간의 연결을 위해 Private NAT의 일종인 Hybrid NAT을 구현하여 가짜 IP 주소로 네트워크 간의 통신 수행