

Day 4. 프라이빗 링크

구분	주제	세부 내용
이론	Day 1 MCN 개요와 라우팅	<ul style="list-style-type: none"> 멀티클라우드 개요 멀티클라우드를 위한 라우팅 (CSP, 오픈소스) 라우팅 동작 라우팅 테이블
	Day 2 가상 네트워크 간의 연동	<ul style="list-style-type: none"> CSP의 가상네트워크 구성 Peering (가상 네트워크 연동) Transit Gateway/Virtual WAN/VCN 멀티 클라우드상의 가상 네트워크 연동
	Day 3 하이브리드와 멀티 클라우드	<ul style="list-style-type: none"> CSP/제조사 하이브리드 클라우드 솔루션 VPN(Virtual Private Network) 전용선(Direct Connect / Express Route) Cloud Hub
이론/ 실습	Day 4 프라이빗 링크	<ul style="list-style-type: none"> CSP의 프라이빗 링크 구성 서비스 엔드포인트(Endpoint) 프라이빗 링크(Private Link) 멀티클라우드 라우팅 구성 (실습)
	Day 5 멀티 클라우드 네트워킹	<ul style="list-style-type: none"> 멀티클라우드 아키텍처 (CSP, 제조사) 멀티클라우드 인프라 연동 멀티클라우드 인프라 관리 멀티클라우드 관리 플랫폼 (실습)

실습교재 별도

DAY 4. 프라이빗 링크

❖ 대외 기관 시스템 연계 (예): AWS

• AWS VPC ↔ 온프레미스

- ✓ AWS Direct Connect
- ✓ AWS site-to-site VPN
- ✓ AWS Transit Gateway
- ✓ Software VPN

• AWS VPC ↔ AWS VPC

- ✓ AWS VPC Peering
- ✓ AWS PrivateLink
- ✓ AWS site-to-site VPN
- ✓ AWS Transit Gateway
- ✓ Software VPN

- AWS VPC에서 인터넷을 통하지 않고 S3, ECR, KMS 등의 서비스를 호출 하기
- 회사 네트워크와 AWS VPC를 (안전한) 연결
- 대외 기관과 (안전한) 시스템 연계
- 분리된 VPC 들의 (안전한) 연결

Source: <https://www.youtube.com/watch?v=tBZBYozvTO8>



DAY 4. 프라이빗 링크

- ❖ 퍼블릭 IP를 쓰지 않고 트래픽이 인터넷을 통과하지 않고도 Amazon Virtual Private Cloud(VPC)에서 전용으로 AWS 서비스를 이용.
- ❖ AWS PrivateLink는 모든 네트워크를 AWS 네트워크 내부로 유지하면서 고객이 높은 가용성과 확장성 방식으로 AWS 서비스를 이용하는 기술
- ❖ AWS PrivateLink가 제공하는 AWS 서비스에 엔드포인트를 새로 만들면, 이러한 서비스 엔드포인트가 VPC의 프라이빗 IP가 있는 ENI(탄력적 네트워크 인터페이스)로 나타남
- ❖ PrivateLink는 퍼블릭 IP의 허용 목록 등록 필요성이나 AWS 서비스에 연결하기 위해 인터넷 게이트웨이, NAT(Network Address Translation) 장치, 방화벽 프록시 등을 이용해 인터넷 연결을 관리할 필요성을 없애줌
- ❖ PrivateLink에서 이용할 수 있는 AWS 서비스는 AWS Direct Connect 상에서 프라이빗 연결도 지원하므로, 서비스 엔드포인트를 이용해 Amazon 프라이빗 네트워크를 통해 AWS 서비스로 고객의 데이터 센터의 애플리케이션을 연결할 수 있음

Amazon Elastic Container Registry (ECR)
AWS Key Management Service (KMS)

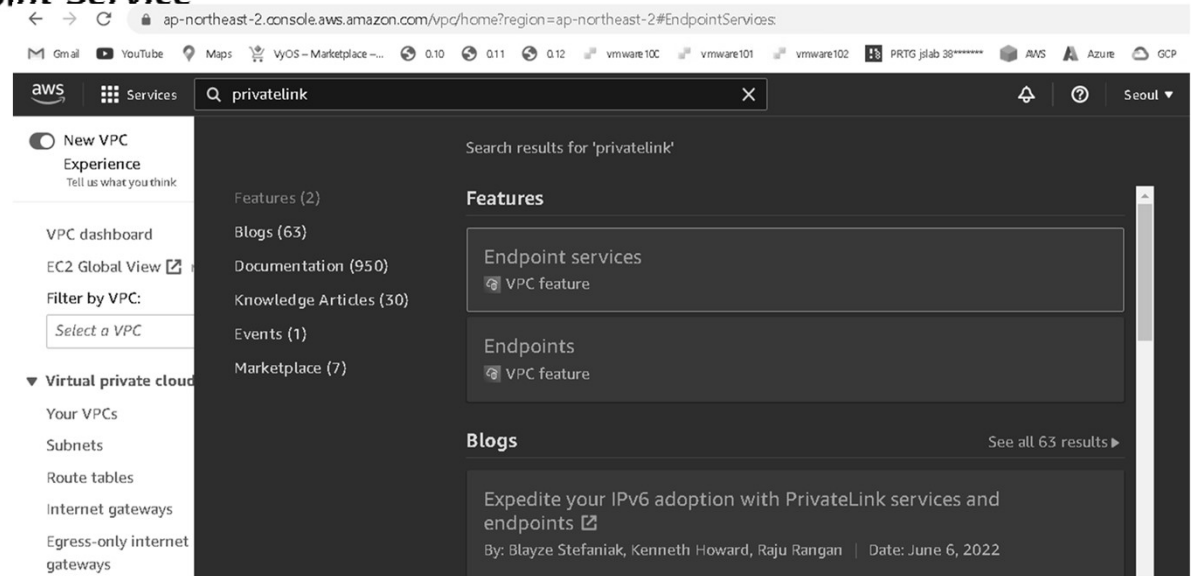
Source: <https://aws.amazon.com/ko/about-aws/whats-new/2017/11/introducing-aws-privatelink-for-aws-services/#:~:text=PrivateLink%EB%8A%94%20%ED%8D%BC%EB%B8%94%EB%A6%AD%20IP%EC%9D%98,%ED%95%A0%20%ED%95%84%EC%9A%94%EC%84%B1%EC%9D%84%20%EC%97%86%EC%95%A0%EC%A4%8D%EB%8B%88%EB%8B%A4.>



DAY 4. 프라이빗 링크

❖ AWS PrivateLink

- AWS VPC와 대상 서비스간 안전한 연결을 위한 기술
- 고가용성 및 확장성 제공
- 지원 서비스
 - ✓ 다른 AWS 계성 상에서 제공하는 서비스 - VPC Endpoint
 - ✓ AWS 마켓플레이스 상의 파트너 서비스
 - ✓ AWS 서비스 (S3, ECR, KMS 등) – VPC Endpoint Service



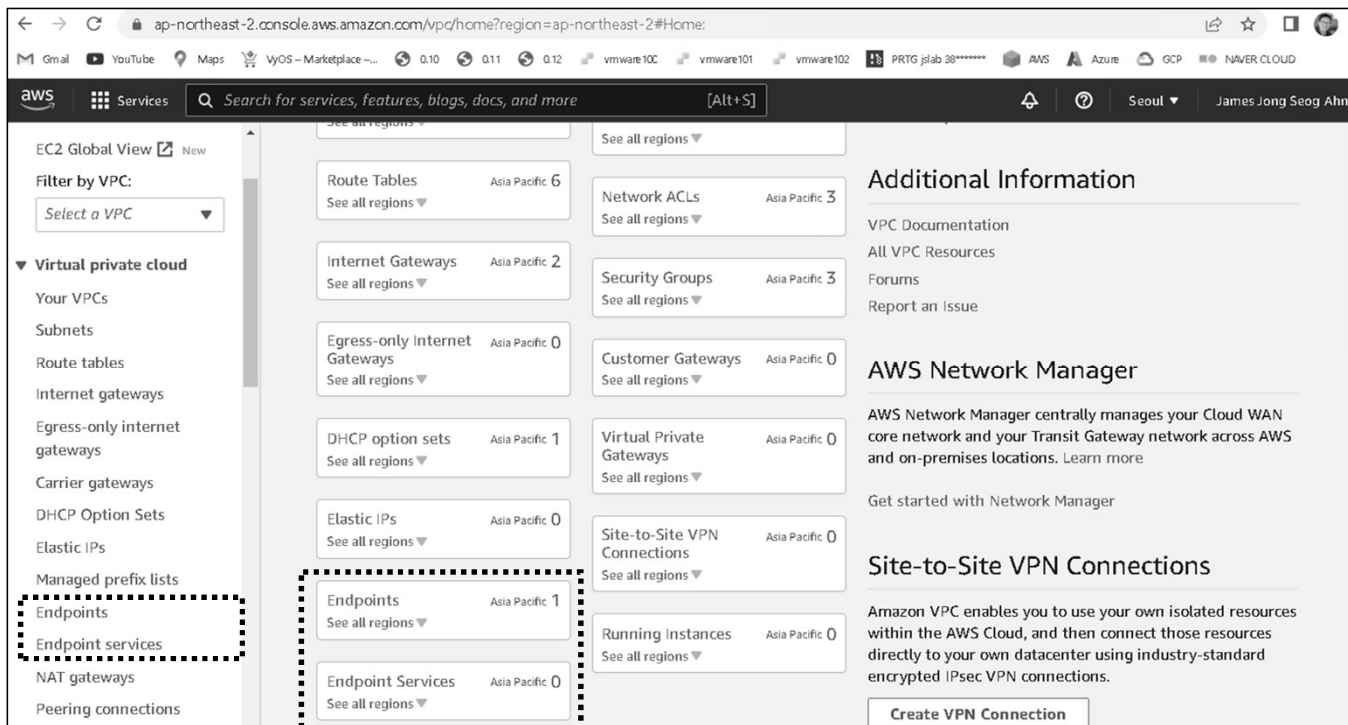
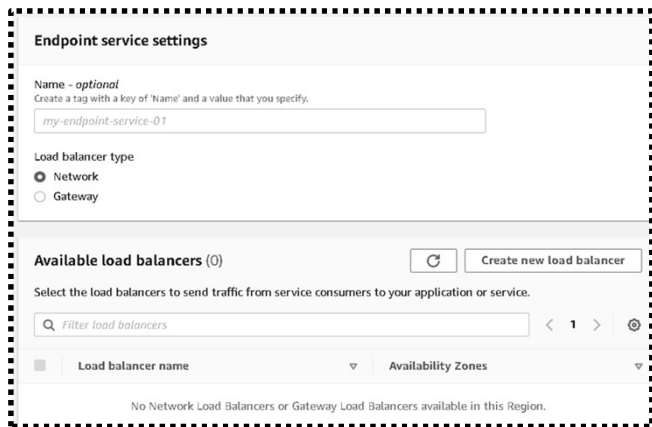
Source: <https://www.youtube.com/watch?v=tBZBYozvTO8>



DAY 4. 프라이빗 링크

❖ AWS PrivateLink 구성 요소

- Endpoint (서비스 제공자)
- Endpoint Service
 - ✓ Gateway Load Balancer Endpoint
 - ✓ Gateway Endpoint
 - ✓ Interface Endpoint

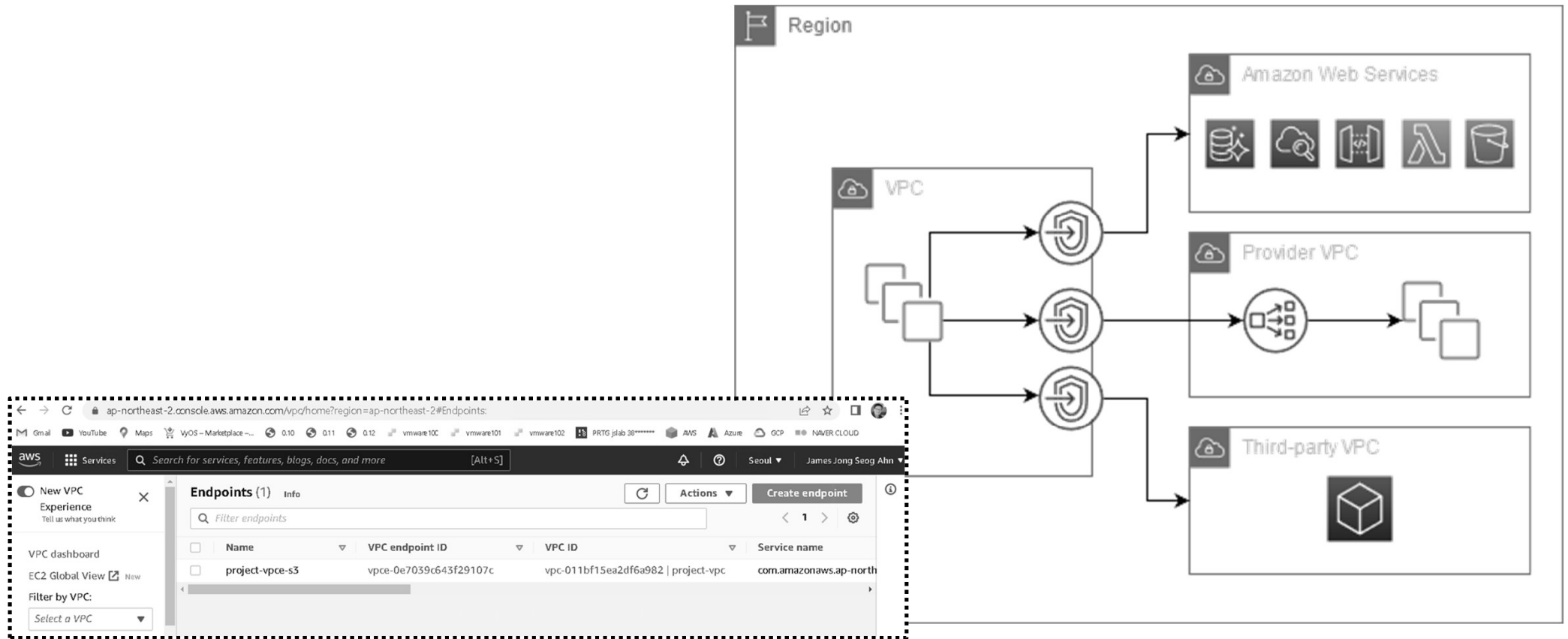


Source: <https://www.youtube.com/watch?v=tBZBYozvTO8>



DAY 4. 프라이빗 링크

❖ AWS PrivateLink를 사용하여 서비스에 VPC 연결

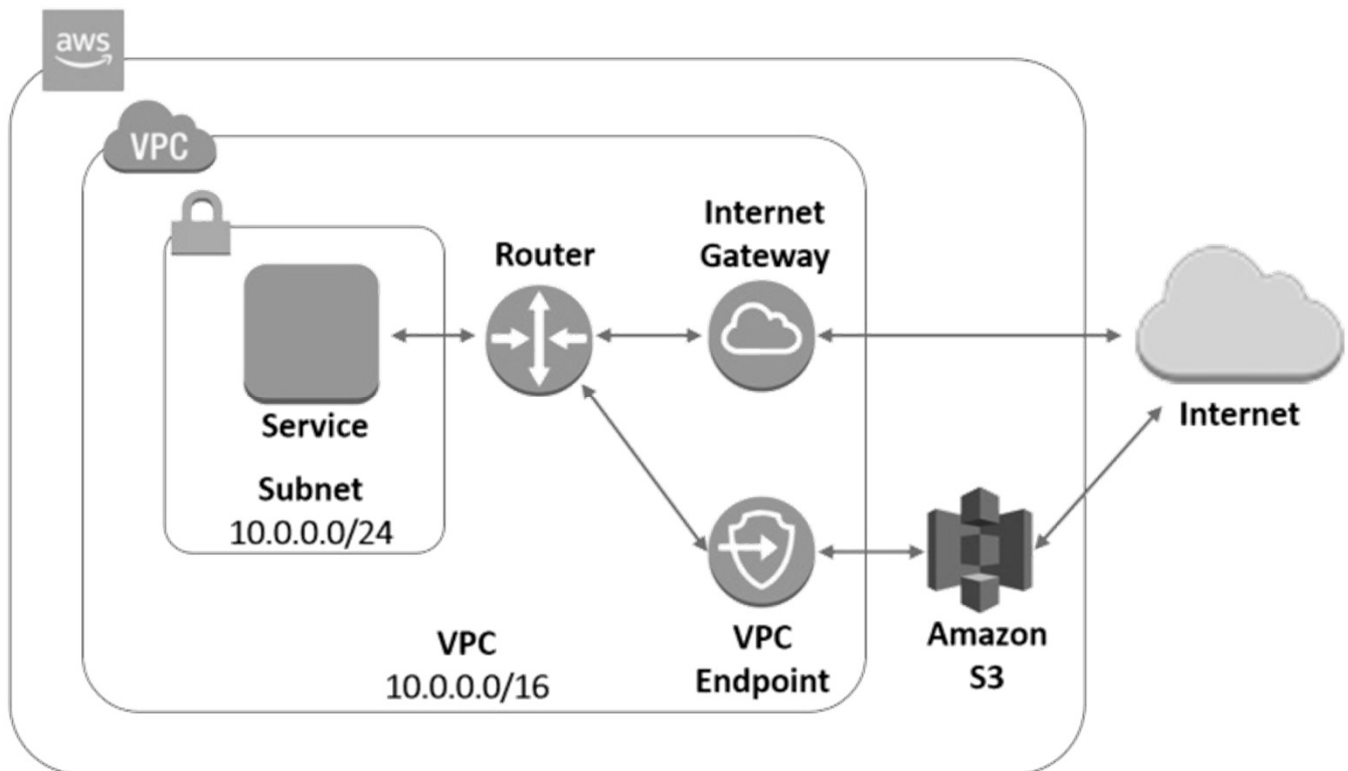


Source: https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/endpoint-services-overview.html



DAY 4. 프라이빗 링크

- ❖ AWS PrivateLink를 통한 새로운 SaaS
 - 인터넷 게이트웨이 또는 VPC 엔드 포인트로 AWS 서비스에 액세스

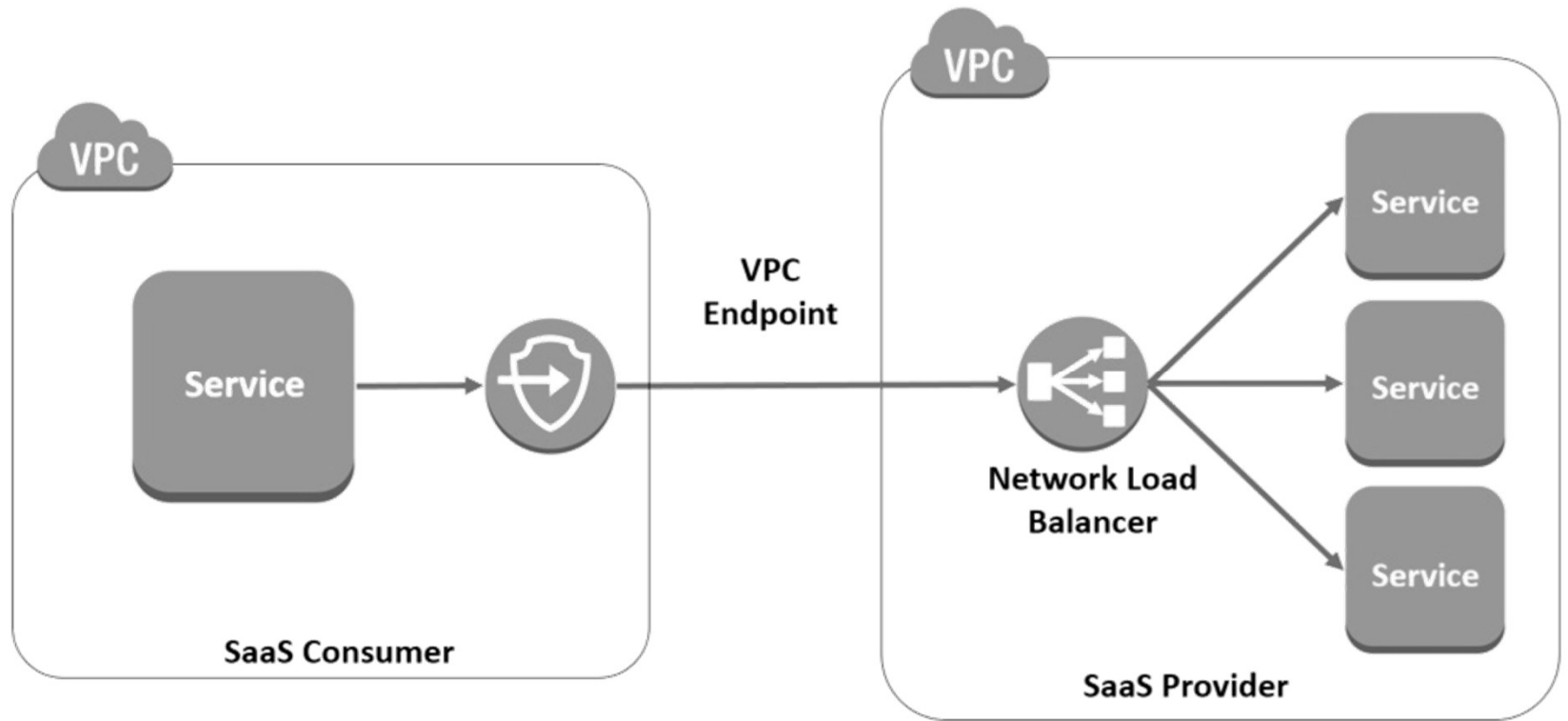


Source: https://www.megazone.com/techblog_191113_aws-privatelink/



DAY 4. 프라이빗 링크

- ❖ AWS PrivateLink를 통한 새로운 SaaS
 - VPC 엔드 포인트를 통한 기본 서비스 노출

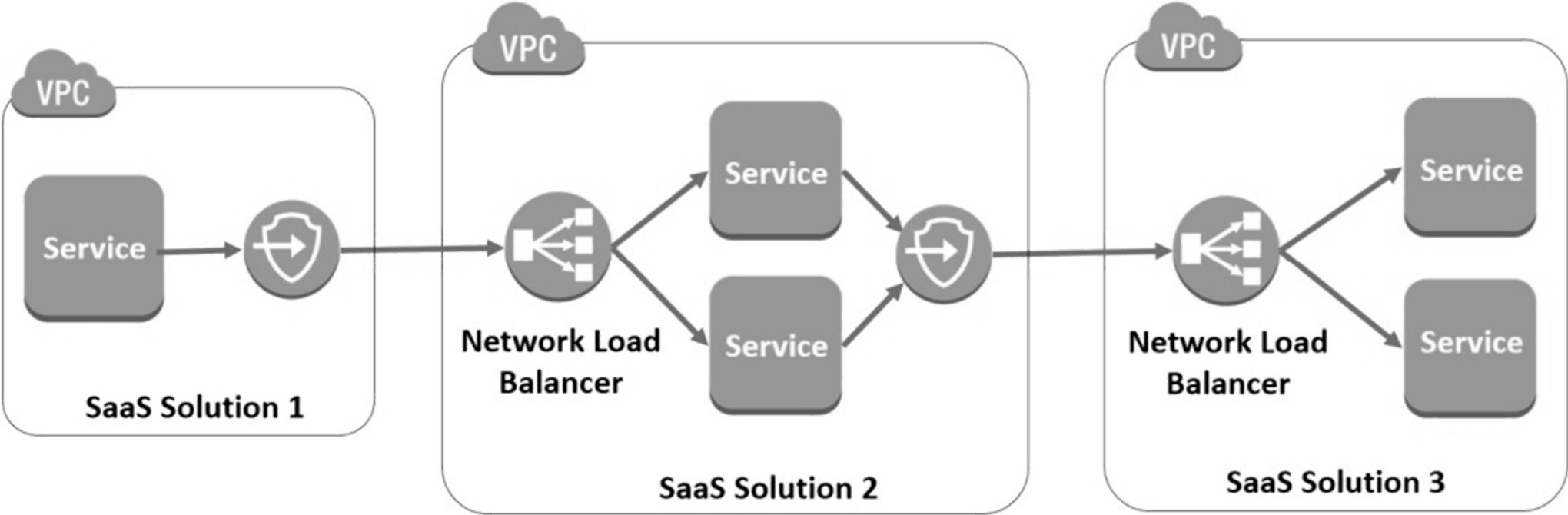


Source: https://www.megazone.com/techblog_191113_aws-privatelink/



DAY 4. 프라이빗 링크

- ❖ AWS PrivateLink를 통한 새로운 SaaS
 - AWS PrivateLink를 사용하여 SaaS 통합 촉진

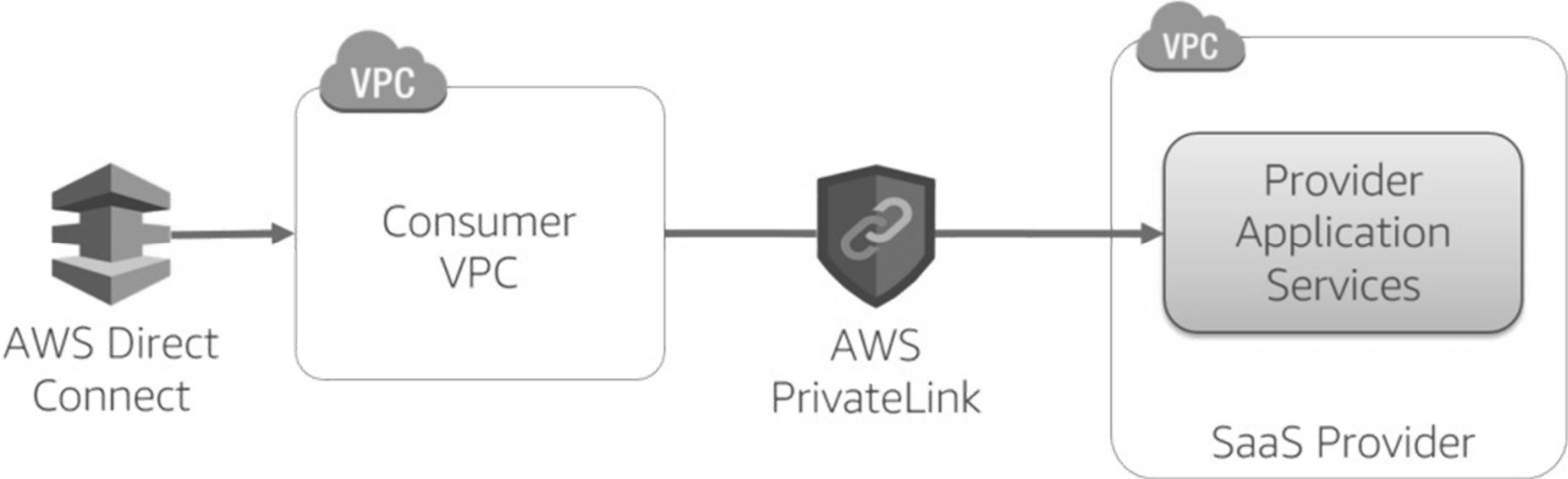


Source: https://www.megazone.com/techblog_191113_aws-privatelink/



DAY 4. 프라이빗 링크

- ❖ AWS PrivateLink를 통한 새로운 SaaS
 - AWS PrivateLink를 사용하여 온 프레미스 환경에서 서비스에 액세스

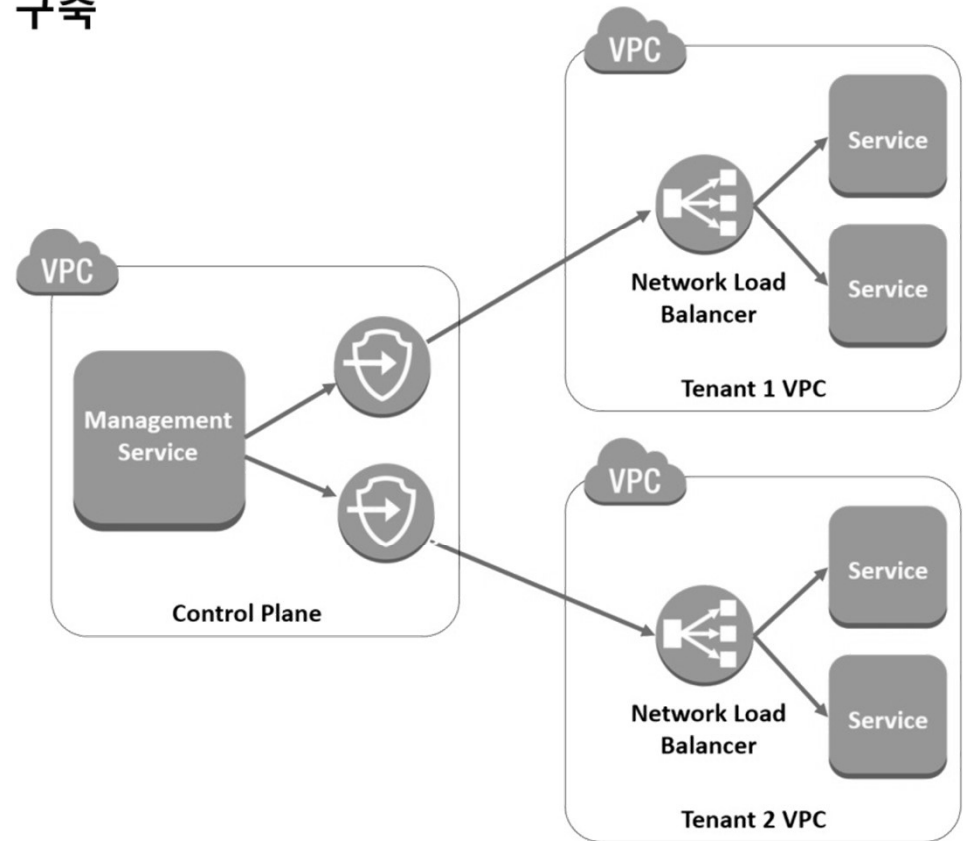


Source: https://www.megazone.com/techblog_191113_aws-privatelink/



DAY 4. 프라이빗 링크

- ❖ AWS PrivateLink를 통한 새로운 SaaS
 - AWS PrivateLink를 사용하여 다중 VPC 컨트롤 플레인 구축

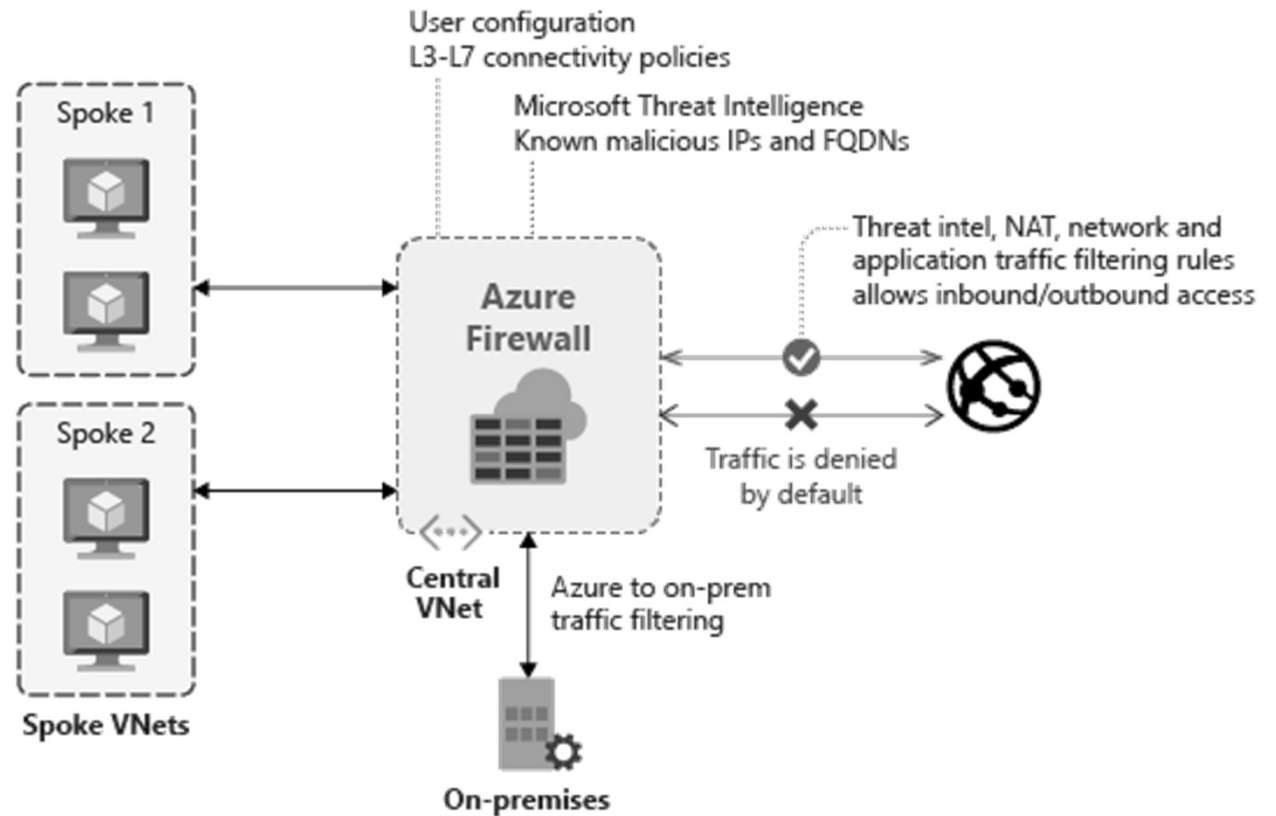


Source: https://www.megazone.com/techblog_191113_aws-privatelink/



DAY 4. 프라이빗 링크

❖ Obtaining A Static Outbound IP from an Azure Virtual Network

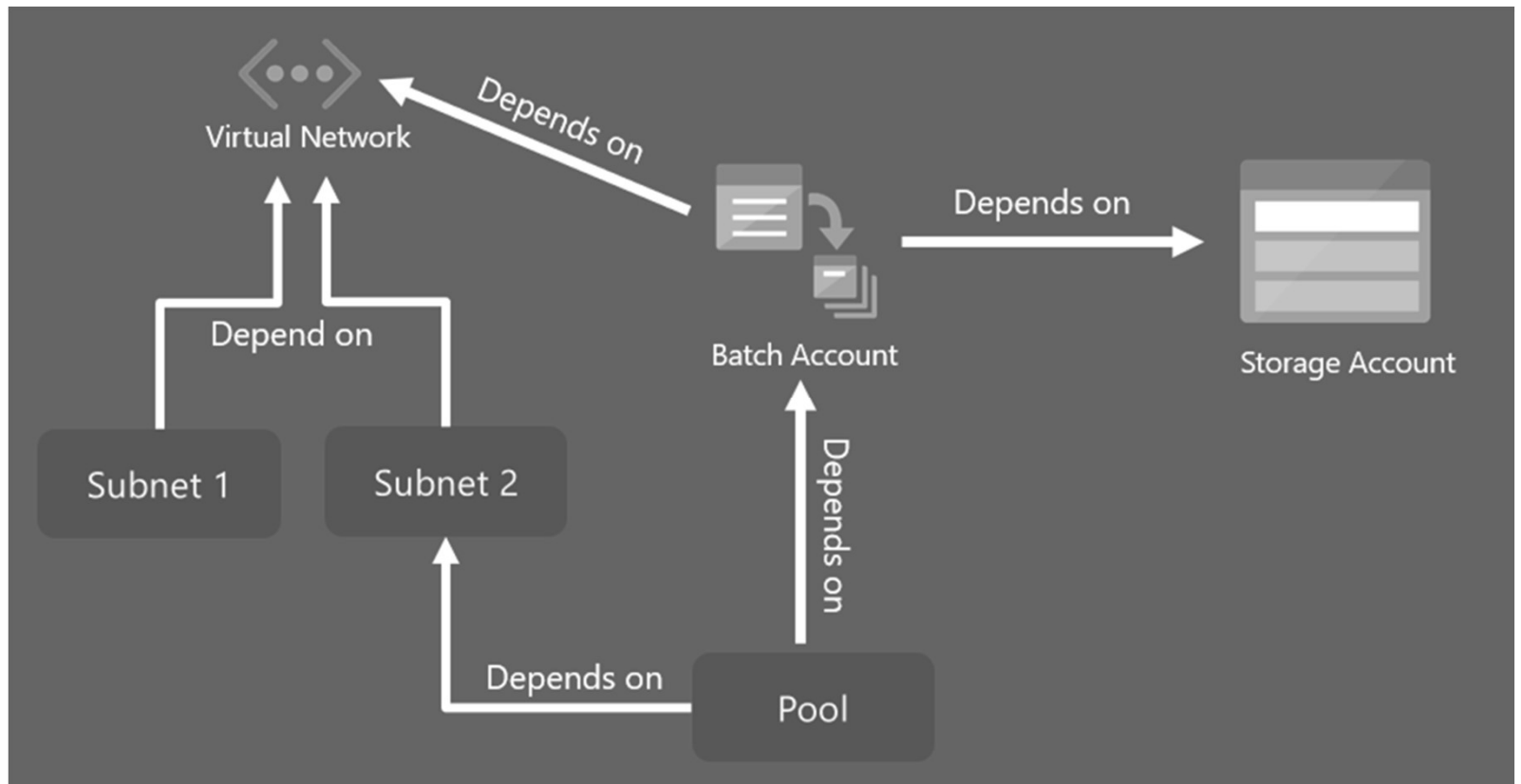


Source: <https://samcogan.com/obtaining-a-static-outbound-ip-from-an-azure-virtual-network/>



DAY 4. 프라이빗 링크

❖ Azure Batch without Public IP

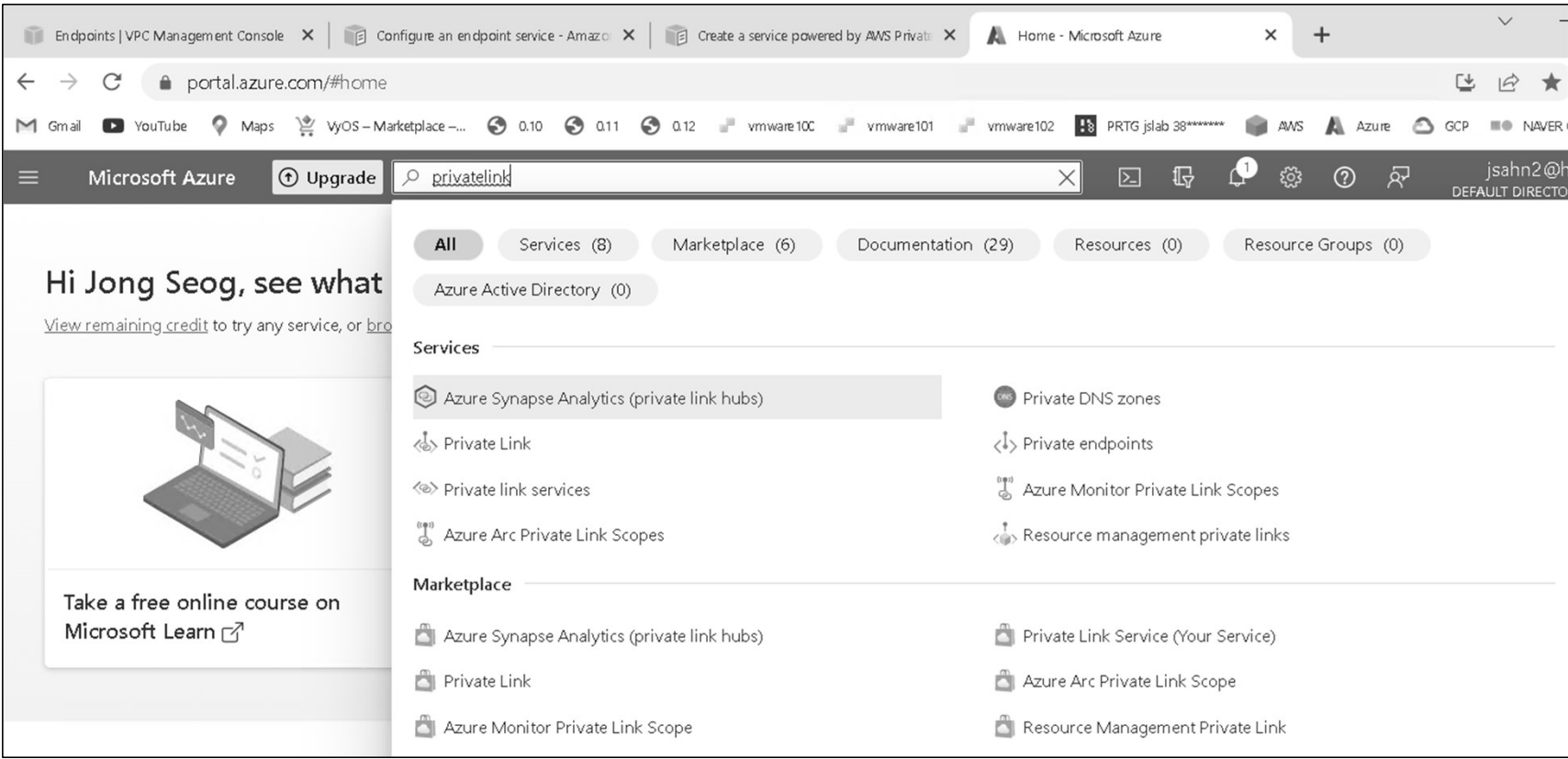


Source: <https://charotamine.medium.com/azure-batch-security-azure-private-link-a04dc21d87ed>



DAY 4. 프라이빗 링크

❖ Azure Private Link 서비스



Source: <https://docs.microsoft.com/ko-kr/azure/private-link/private-link-service-overview>



DAY 4. 프라이빗 링크

❖ Azure Private Link

Private Link Center - Microsoft

https://portal.azure.com/#create/Microsoft.PrivateLink-ARM

Microsoft Azure

Search resources, services, and docs (G+)

user@contoso.com

Home > New > Private Link >

Private Link Center

Search (Cmd+/)

- Overview
- Pending connections
- Private endpoints
- Private link services

Resources

- Active connections
- Supported resources

Build and allow private connections between resources with Private Link

Azure Private Link is a secure and scalable way to create, share, and connect to Azure. All data that flows from a provider to a consumer is isolated from the internet and stays on the Microsoft back end. Learn more about private links

- Consumers: To privately connect to a service, create a private endpoint.
- Providers: To privately render a service, create a private link service or private resource.

Build a private connection to a service
Create a private endpoint to privately connect to a service. Learn more
Create private endpoint

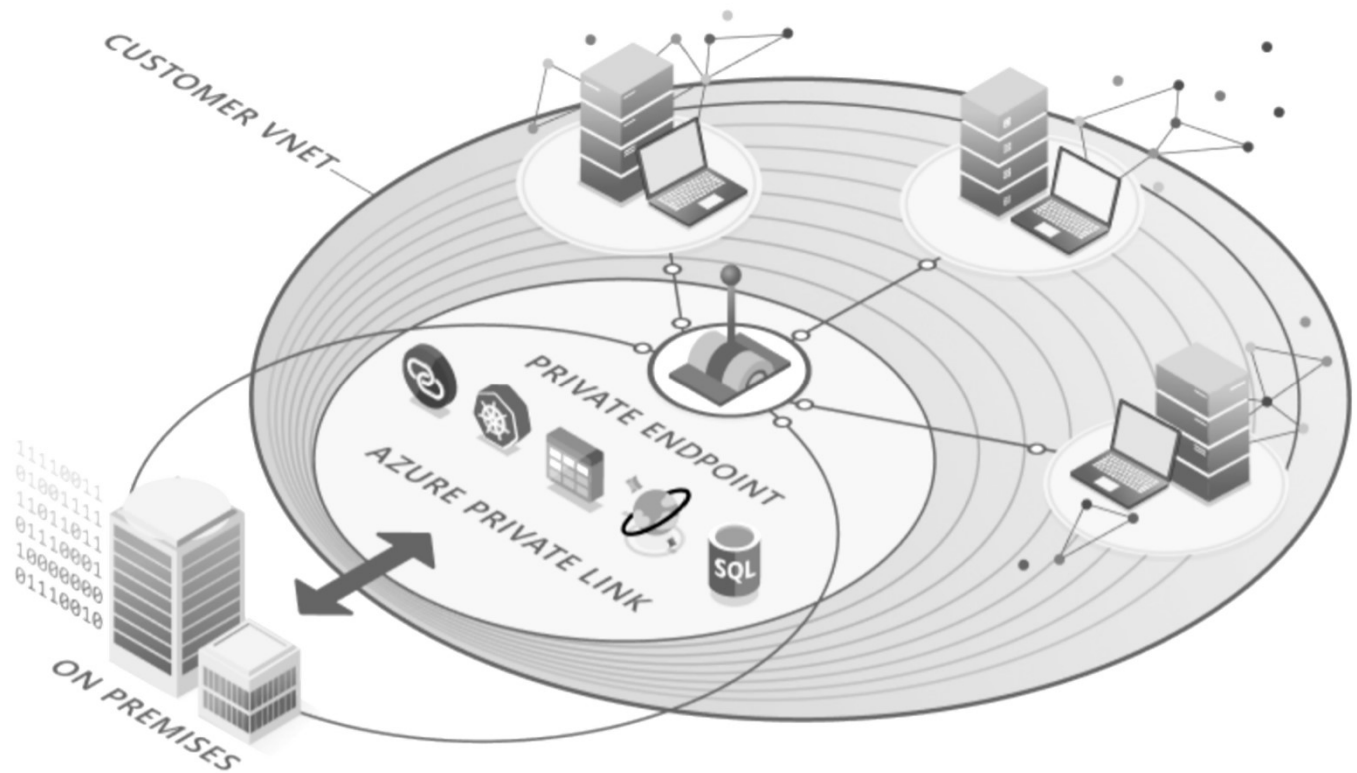
Expose your own service so others can connect
Create a private link service to enable private connections to an existing service. Your existing service must be behind a standard load balancer. Learn more
Create private link service

Source: <https://docs.microsoft.com/ja-jp/azure/private-link/private-link-overview>



DAY 4. 프라이빗 링크

❖ Cloud Security And Azure Private Link

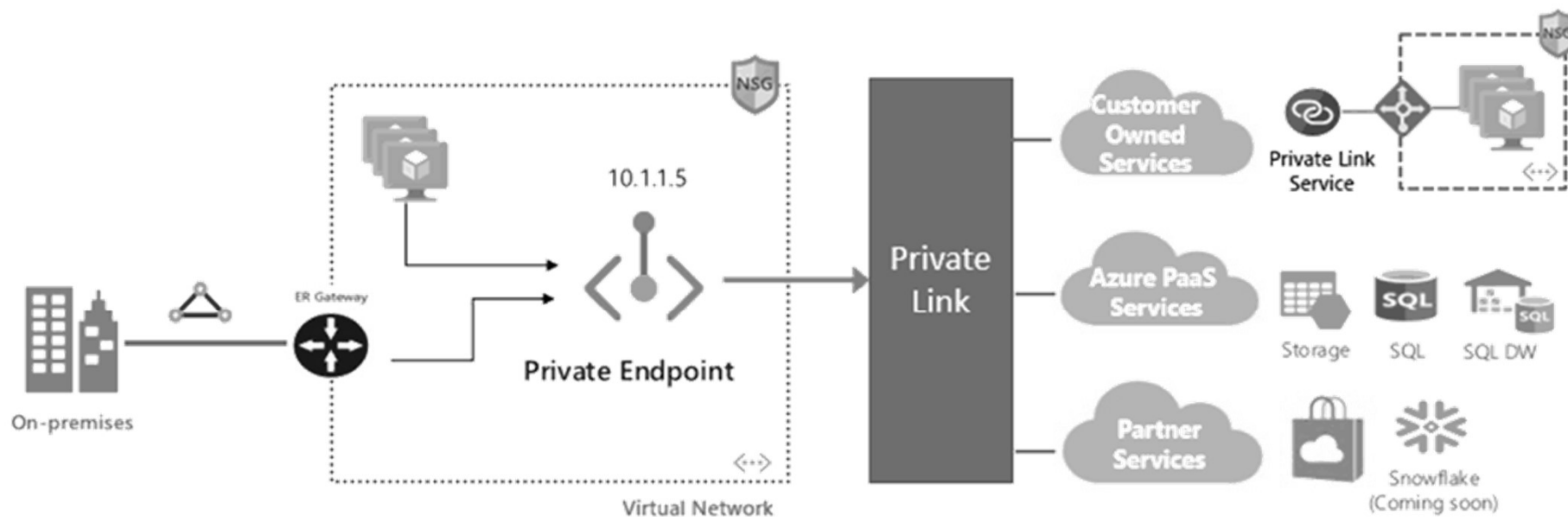


Source: <https://wcollins.io/post/2021/cloud-security-and-azure-private-link/>



DAY 4. 프라이빗 링크

❖ Azure Private EndPoint



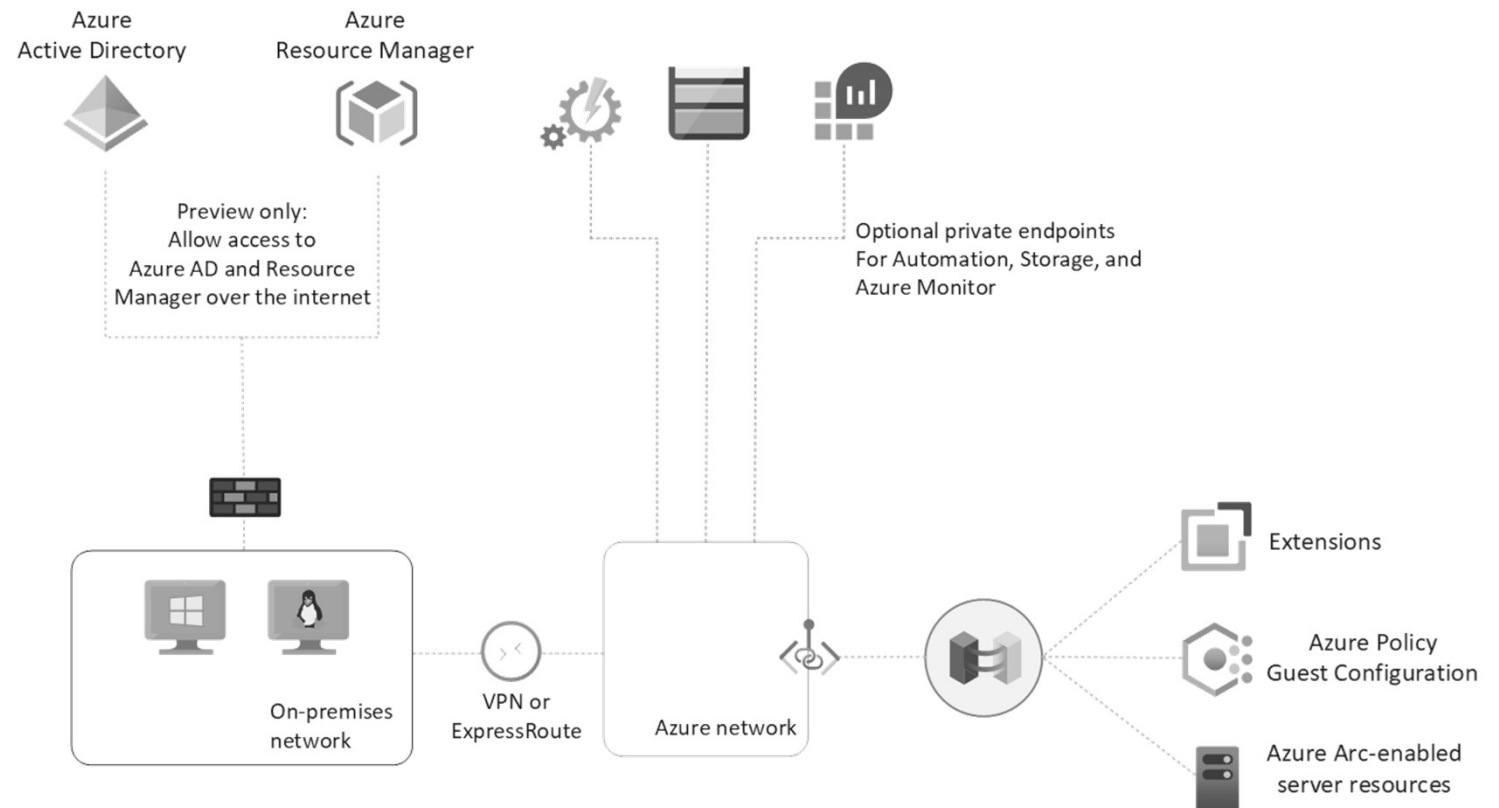
Azure Private Link – Connecting Azure Services privately to your Network

Source: <https://www.azuredocs.com/azure-private-link-nedir/>



DAY 4. 프라이빗 링크

❖ Use Azure Private Link to securely connect servers to Azure Arc

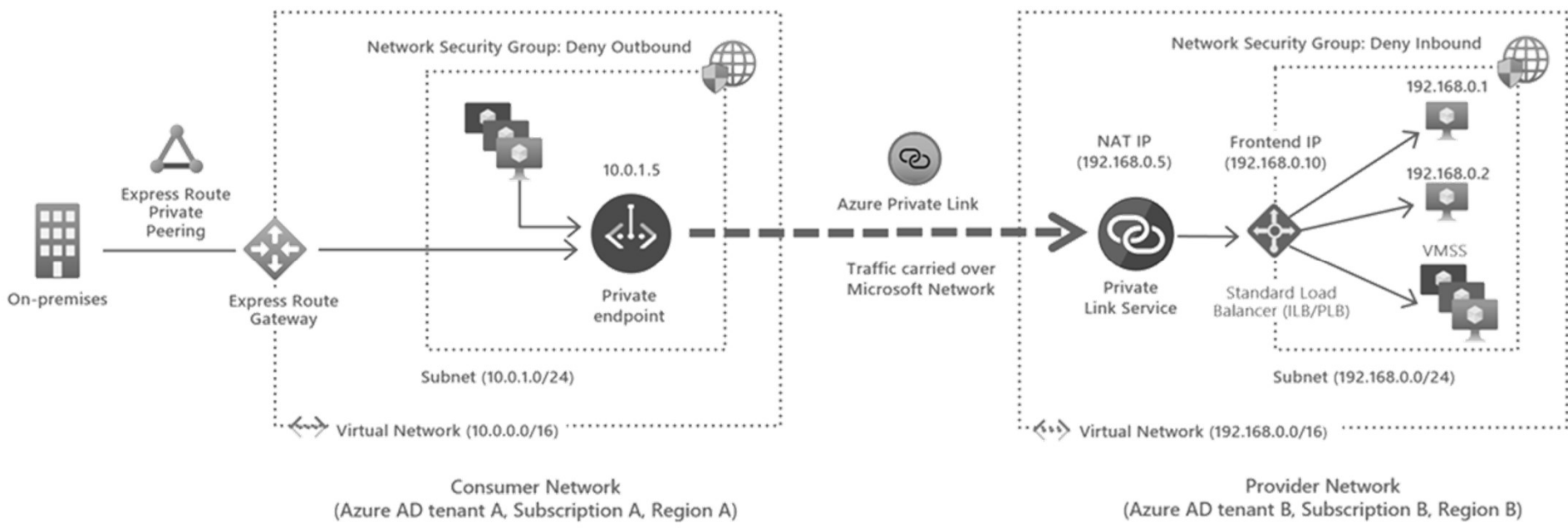


Source: <https://docs.microsoft.com/en-us/azure/azure-arc/servers/private-link-security>



DAY 4. 프라이빗 링크

- ❖ Azure Private Link 서비스는 Azure Standard Load Balancer 뒤에서 실행되는 서비스는 서비스에 대한 소비자가 자신의 VNet에서 비공개로 액세스할 수 있도록 Private Link 액세스를 사용하도록 설정할 수 있다. (Azure Private Link 서비스는 표준 Load Balancer에서만 지원)
- ❖ 고객은 VNet 내에서 프라이빗 엔드포인트를 만들고 이 서비스에 매핑할 수 있음

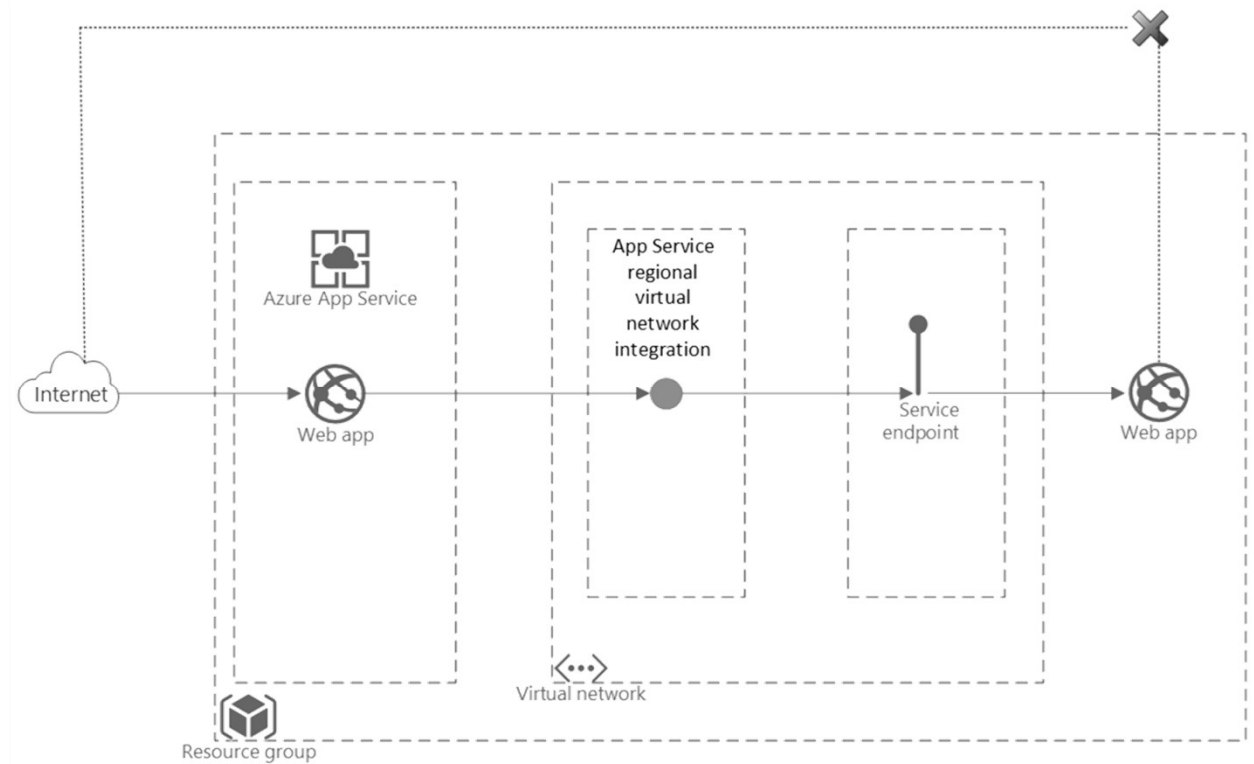


Source: <https://docs.microsoft.com/ko-kr/azure/private-link/private-link-service-overview>



DAY 4. 프라이빗 링크

❖ Multi-tier app service with service endpoint

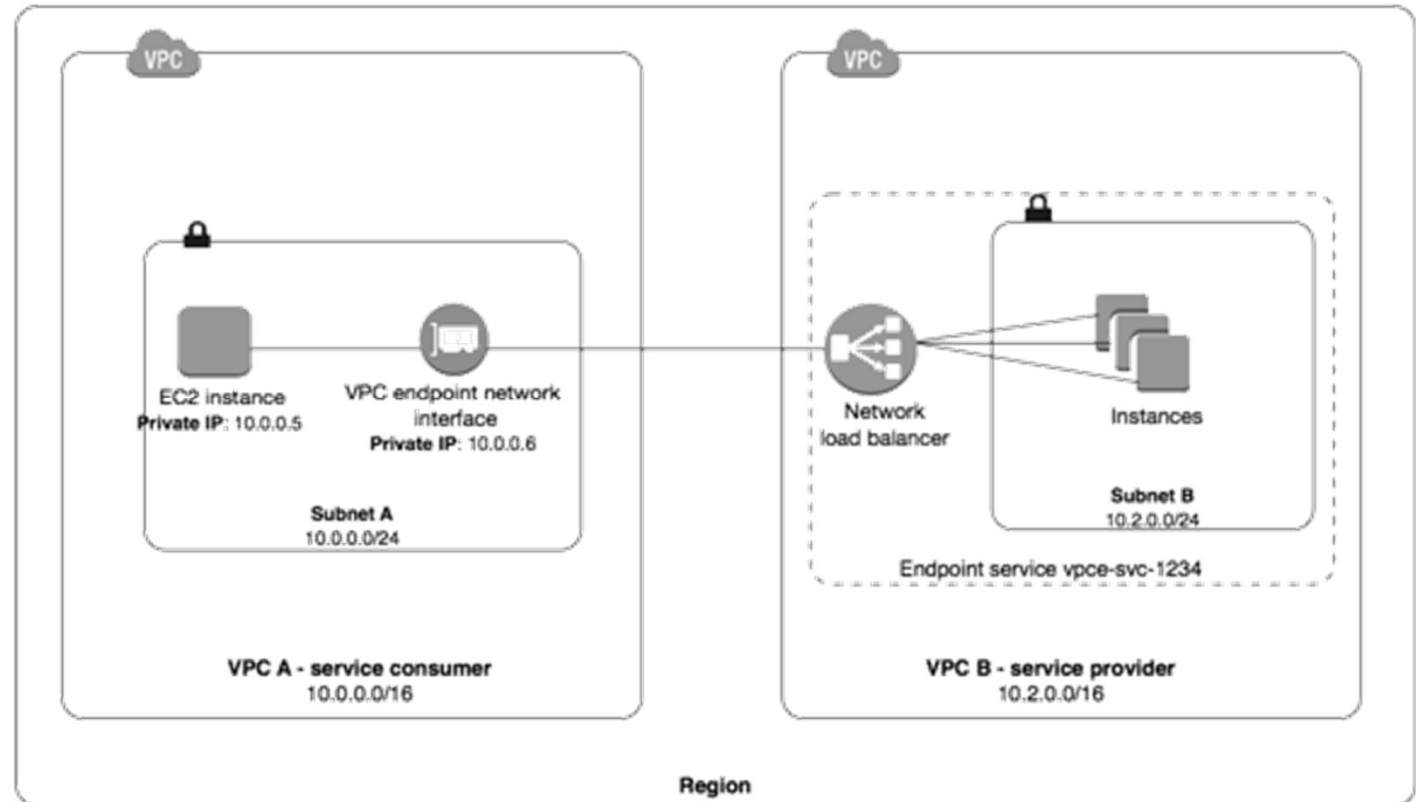


Source: <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/app-service-web-app/multi-tier-app-service-service-endpoint>



DAY 4. 프라이빗 링크

❖ 인터페이스 엔드포인트를 위한 VPC 엔드포인트 서비스



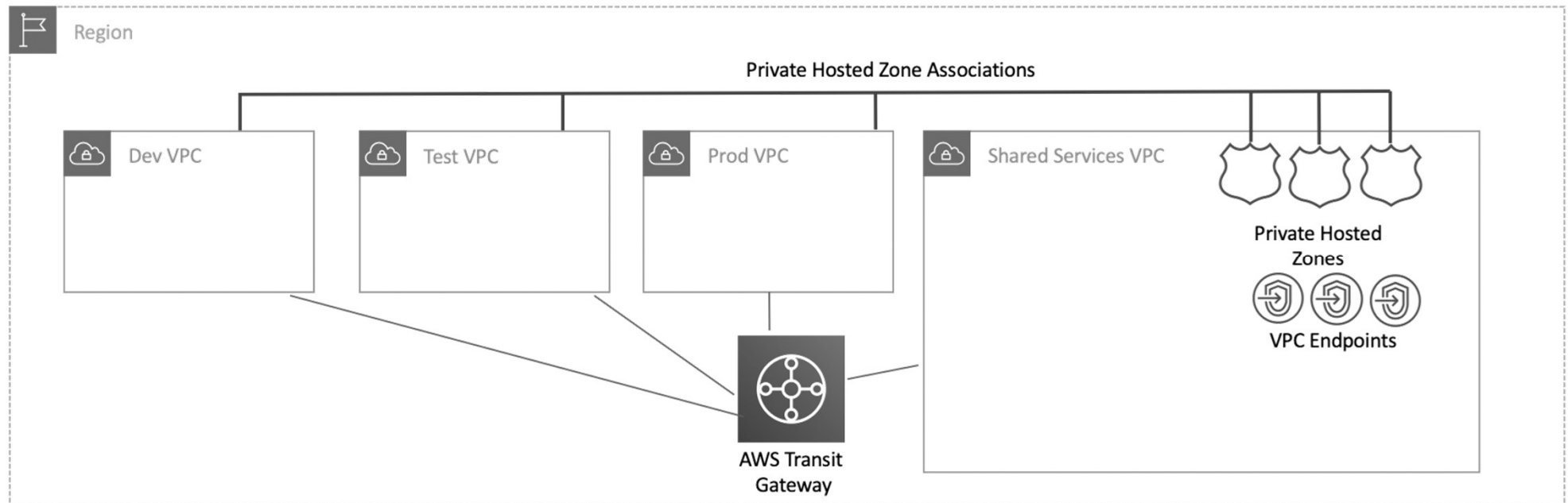
Source: https://docs.aws.amazon.com/ko_kr/vpc/latest/privatelink/endpoint-service-overview.html



DAY 4. 프라이빗 링크

❖ Services using VPC peering and AWS PrivateLink

- VPC to VPC

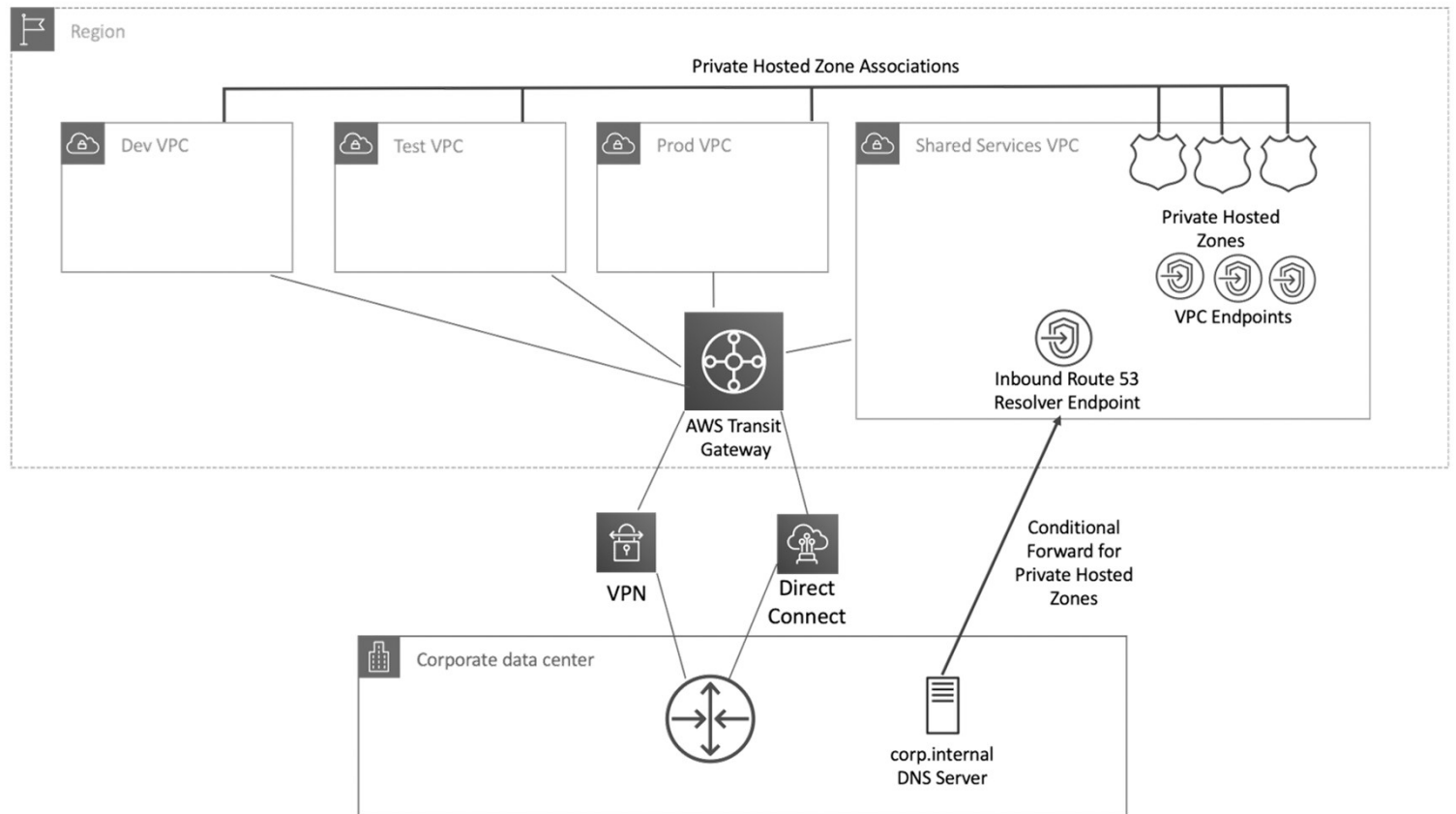


Source: <https://aws.amazon.com/blogs/networking-and-content-delivery/integrating-aws-transit-gateway-with-aws-privatelink-and-amazon-route-53-resolver/>



DAY 4. 프라이빗 링크

❖ On premises

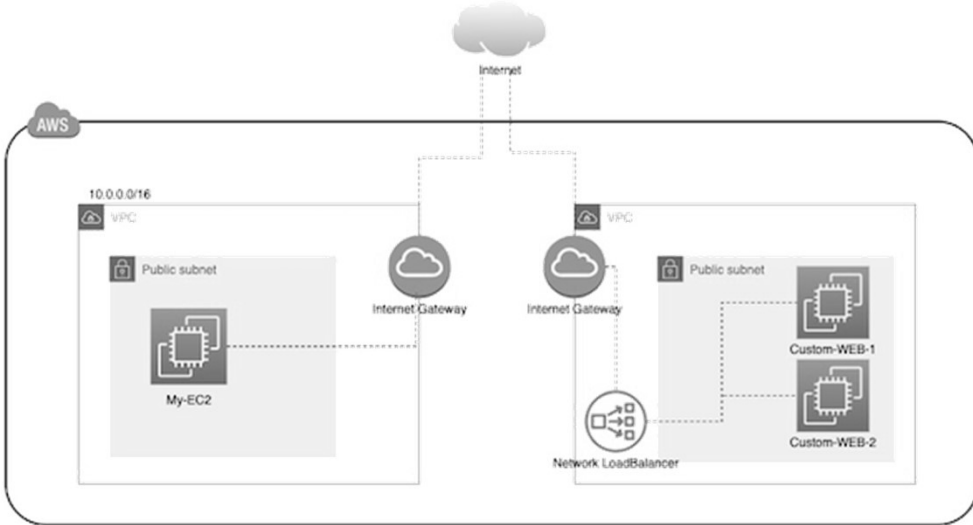


Source: <https://aws.amazon.com/blogs/networking-and-content-delivery/integrating-aws-transit-gateway-with-aws-privatelink-and-amazon-route-53-resolver/>



DAY 4. 프라이빗 링크

❖ EndPoint Service를 이용해서 PrivateLink 구성 해보기



자원	태그 이름	정보
VPC	MyVPC	10/0.0.0/16
	CustomVPC	20.0.0.0/16
퍼블릭 서브넷	My-public-subnet	10.0.0.0/24
	Custom-public-subnet	20.0.0.0/24
퍼블릭 라우팅 테이블	My-public-rt	My-public-subnet
	Custom-public-rt	Custom-public-subnet
인터넷 게이트웨이	My-IGW	MyVPC
	Custom-IGW	CustomVPC
퍼블릭 EC2 인스턴스	My-EC2	퍼블릭 IP 활성화
	Custom-WEB-1	퍼블릭 IP 활성화
	Custom-WEB-2	퍼블릭 IP 활성화
NLB	NLB-test	Custom-WEB-1, Custom-WEB-2

Source: <https://dev.classmethod.jp/articles/organize-private-links-with-endpoints/>



DAY 4. 프라이빗 링크

❖ EndPoint Service를 이용해서 PrivateLink 구성 해보기

- 퍼블릭에서 연결 테스트

```
dig +short NLB-test-c82933481368db30.elb.ap-northeast-1.amazonaws.com
```

```
[ec2-user@ip-10-0-0-107 ~]$ dig +short NLB-test-c82933481368db30.elb.ap-northeast-1.amazonaws.com  
18.180.234.125
```

```
curl NLB-test-c82933481368db30.elb.ap-northeast-1.amazonaws.com
```

```
<!DOCTYPE html>  
<html>  
  <head>  
    <title>Welcome to the AWS IMD</title>  
    <link href="style.css" media="all" rel="stylesheet" type="text/css" />  
  </head>
```

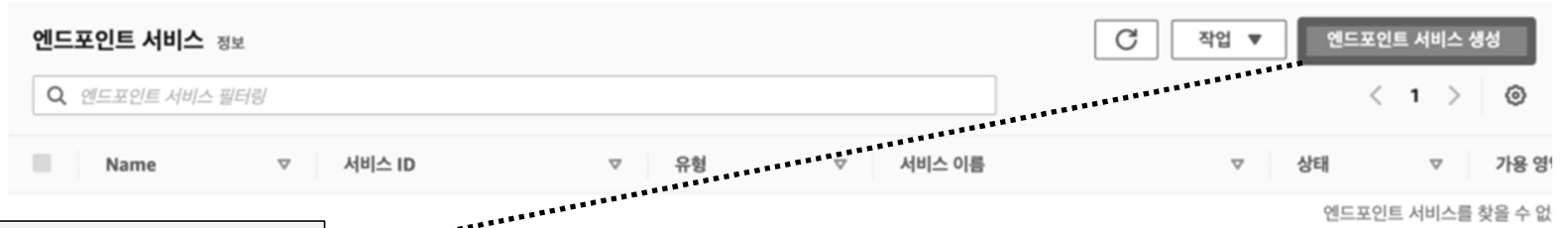
Source: <https://dev.classmethod.jp/articles/organize-private-links-with-endpoints/>



DAY 4. 프라이빗 링크

❖ EndPoint Service를 이용해서 PrivateLink 구성 해보기

- 엔드포인트 생성



Source: <https://dev.classmethod.jp/articles/organize-private-links-with-endpoints/>



DAY 4. 프라이빗 링크

❖ EndPoint Service를 이용해서 PrivateLink 구성 해보기

• 엔드포인트 생성

보안 그룹 선택

그룹 ID 그룹 이름 VPC ID 설명 소유자 ID

sg-0417db72...	My-EC2-Sec...	vpc-0246794...	EC2-VPC	My-EC2-Sec...	
sg-0ee0bb6d...	default	vpc-0246794...	EC2-VPC	default VPC s...	

키 (최대 127자) 값 (최대 255자)

이 리소스에는 현재 태그가 없습니다.

태그 추가 50개 남음 (최대 50개 태그)

취소 엔드포인트 생성

VPC 엔드포인트를 사용하면 VPC를 다른 AWS 서비스에 안전하게 연결할 수 있습니다. 인터페이스 엔드포인트는 PrivateLink를 통해 실행되며, ENI(탄력적 네트워크 인터페이스)를 서비스 트래픽의 진입점으로 사용합니다. 게이트웨이 엔드포인트는 서비스 트래픽에 대한 라우팅 테이블의 라우팅 대상 역할을 합니다.

서비스 범주

- AWS 서비스
- 이름별 서비스 찾기
- AWS Marketplace 서비스

서비스 이름 프라이빗 서비스 이름을 입력하고 확인합니다. ⓘ

com.amazonaws.vpc.ap-northeast-1.vpc-svc-063

서비스 이름을 찾았습니다.

확인

VPC* vpc-024679418f657cd60 ⓘ

Name	엔드포인트 ID	VPC ID	서비스 이름	엔드포인트 유형	상태	생성 시간
	vpce-0014dea8a6f...	vpc-024679418f6...	com.amazonaws.vpc.ap-north...	Interface	수락 대기 중	2021년 10월 3일 오후 5시 16분

인터페이스: vpce-0014dea8a6f821bad

세부 정보

엔드포인트 ID	vpce-0014dea8a6f821bad	VPC ID	vpc-024679418f657cd60 MyVPC
상태	수락 대기 중	Status message	
생성 시간	2021년 10월 3일 오후 5시 16분 6초 UTC+9	서비스 이름	com.amazonaws.vpc.ap-northeast-1.vpc-svc-06378c80cbf0cd69
엔드포인트 유형	Interface	DNS 이름	vpce-0014dea8a6f821bad-eviog1uz.vpc-svc-06378c80cbf0cd69.ap-northeast-1.vpc.amazonaws.com (Z2E726K9Y6RL4W) vpce-0014dea8a6f821bad-eviog1uz.ap-northeast-1a.vpc-svc-06378c80cbf0cd69.ap-northeast-1.vpc.amazonaws.com (Z2E726K9Y6RL4W)

세부 정보 | 로드 밸런서 | 보안 주체 허용 | 엔드포인트 연결 | 알림 | 태그

엔드포인트 연결 (1/1) 정보

엔드포인트 연결을 기준으로 필터링

엔드포인트 연결 요청 수락

엔드포인트 연결 요청 거부

엔드포인트 ID	소유자	상태	생성됨
vpce-0014dea8a6f821bad	196092325216	Pending acceptance	2021년 10월 3일 일요일 17:...

Source: <https://dev.classmethod.jp/articles/organize-private-links-with-endpoints/>

DAY 4. 프라이빗 링크

❖ EndPoint Service를 이용해서 PrivateLink 구성 해보기

- 엔드포인트 서비스 테스트

```
dig +short vpce-0014dea8a6f821bad-eviog1uz.vpce-svc-06378c80c0bf0cd69.ap-northeast-1.vpce.amazonaws.com
[ec2-user@ip-10-0-0-107 ~]# dig +short vpce-0014dea8a6f821bad-eviog1uz.vpce-svc-06378c80c0bf0cd69.ap-northeast-1.vpce.amazonaws.com
10.0.0.249

curl vpce-0014dea8a6f821bad-eviog1uz.vpce-svc-06378c80c0bf0cd69.ap-northeast-1.vpce.amazonaws.com
<!DOCTYPE html>
<html>
  <head>
    <title>Welcome to the AWS IMD</title>
    <link href="style.css" media="all" rel="stylesheet" type="text/css" />
  </head>
```

VPC ID	vpce-024679418f657cd60 MyVPC
Status message	
서비스 이름	com.amazonaws.vpce.ap-northeast-1.vpce-svc-06378c80c0bf0cd69
DNS 이름	vpce-0014dea8a6f821bad-eviog1uz.vpce-svc-06378c80c0bf0cd69.ap-northeast-1.vpce.amazonaws.com (Z2E726K9Y6RL4W) 1
	vpce-0014dea8a6f821bad-eviog1uz-ap-northeast-1a.vpce-svc-06378c80c0bf0cd69.ap-northeast-1.vpce.amazonaws.com (Z2E726K9Y6RL4W) 2

Source: <https://dev.classmethod.jp/articles/organize-private-links-with-endpoints/>



DAY 4. 프라이빗 링크

❖ EndPoint Service를 이용해서 PrivateLink 구성 해보기

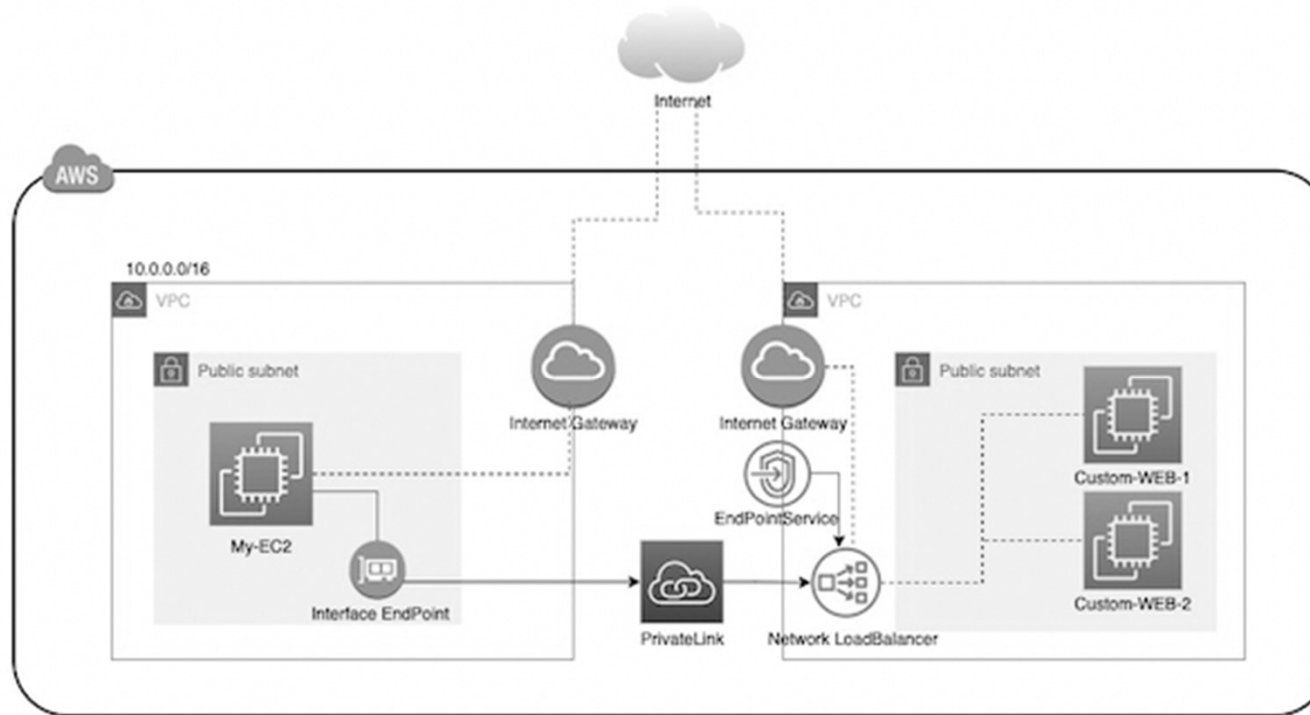
- 엔드포인트 서비스 테스트

```
dig +short vpce-0014dea8a6f821bad-eviog1uz.vpce-svc-06378c80c0bf0cd69.ap-northeast-1.vpce.amazonaws.com
```

```
ap-northeast-1.vpce.amazonaws.com
```

```
vpce.amazonaws.com
```

```
ss" />
```



```
VPC ID    vpc-024
Status message
서비스 이름 com.am
           06378c
DNS 이름   vpce-00
           06378c
           1.vpce.
           vpce-00
           1a.vpce
           1.vpce.
```

Source: <https://dev.classmethod.jp>

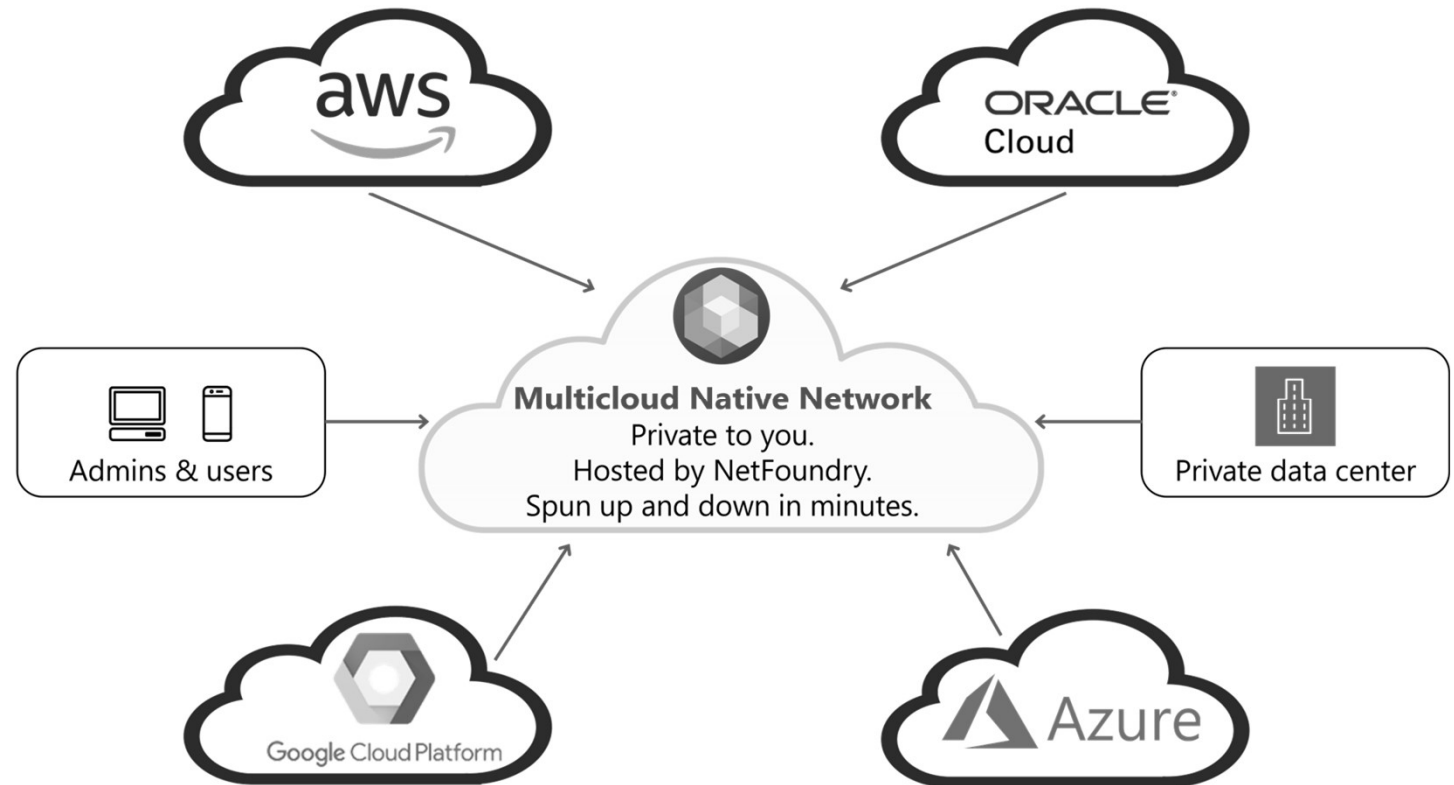
Day 5. 멀티 클라우드 네트워킹

구분	주제	세부 내용
이론	Day 1 MCN 개요와 라우팅	<ul style="list-style-type: none"> 멀티클라우드 개요 멀티클라우드를 위한 라우팅 (CSP, 오픈소스) 라우팅 동작 라우팅 테이블
	Day 2 가상 네트워크 간의 연동	<ul style="list-style-type: none"> CSP의 가상네트워크 구성 Peering (가상 네트워크 연동) Transit Gateway/Virtual WAN/VCN 멀티 클라우드상의 가상 네트워크 연동
	Day 3 하이브리드와 멀티 클라우드	<ul style="list-style-type: none"> CSP/제조사 하이브리드 클라우드 솔루션 VPN(Virtual Private Network) 전용선(Direct Connect / Express Route) Cloud Hub
이론/ 실습	Day 4 프라이빗 링크	<ul style="list-style-type: none"> CSP의 프라이빗 링크 구성 서비스 엔드포인트(Endpoint) 프라이빗 링크(Private Link) 멀티클라우드 라우팅 구성 (실습)
	Day 5 멀티 클라우드 네트워킹	<ul style="list-style-type: none"> 멀티클라우드 아키텍처 (CSP, 제조사) 멀티클라우드 인프라 연동 멀티클라우드 인프라 관리 멀티클라우드 관리 플랫폼 (실습)

실습교재 별도

DAY 5. 멀티 클라우드 네트워킹

❖ Multicloud native networking



Source: <https://netfoundry.io/multicloud-networking/>



DAY 5. 멀티 클라우드 네트워킹

❖ Multi-Cloud 운영 이슈



DAY 5. 멀티 클라우드 네트워킹

❖ 클라우드 네트워킹의 복잡성

- **라우팅:** Routing traffic rapidly and securely between disparate cloud platforms is complex; avoid complex Managed VPN solutions
- **자동화:** Automation needed for disparate CLI's, BGP ASN's, and routing tables
- **관리:** Managing multiple cloud, SaaS, network, and colocation providers is a juggling act!
- **중앙 관리:** Every provider will have their own proprietary method for management, monitoring, storage, and network solutions.
- **표준 보안 정책:** Establishing standard security capabilities and policies
- **보안 강화:** Ability to enforce security for users, data, and applications everywhere is essential



DAY 5. 멀티 클라우드 네트워킹

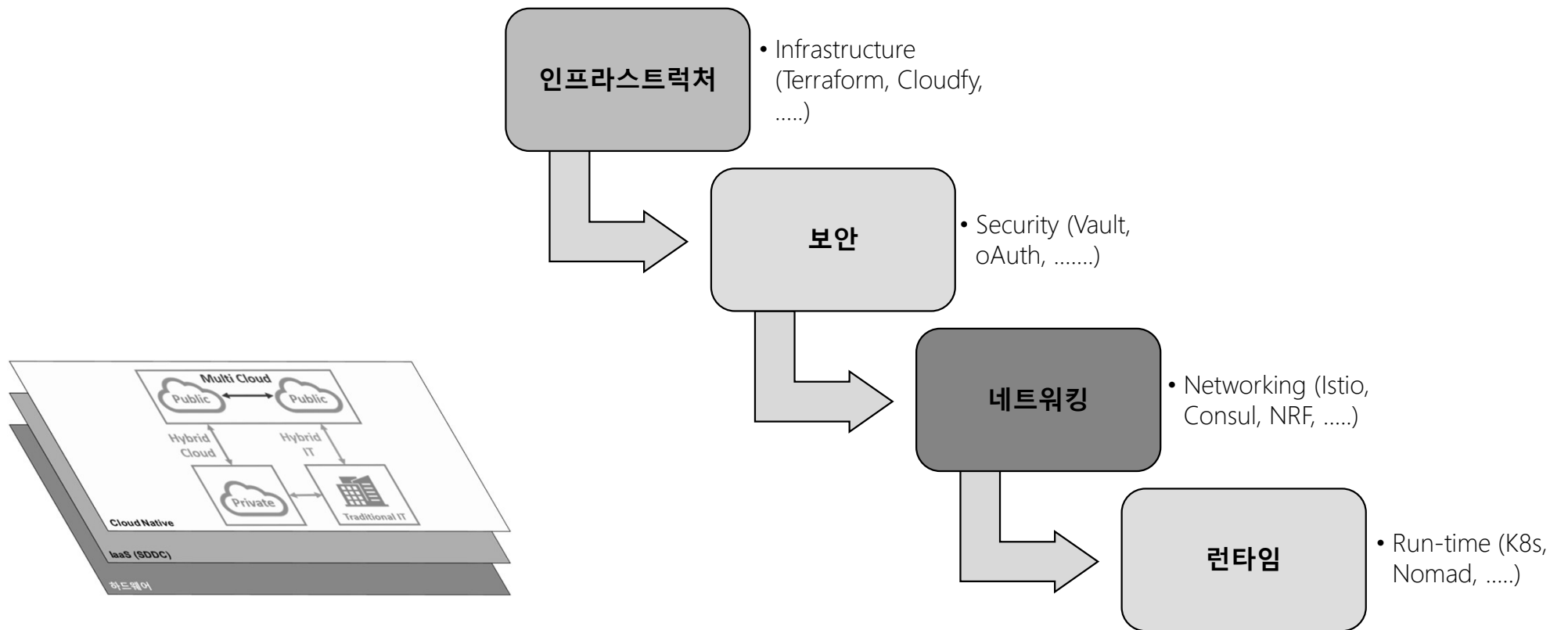
❖ 복잡성 단순화 (Simplifying Complexity)

- **단순화 필요:** While a multi-cloud strategy will help to avoid vendor lock-in, increase reliability and protect mission-critical data, it has inherent complexity. Before leaping into multi-cloud, consider these few potential methods to simplify the complexity.
- **단순화 방안 (Potential Methods)**
 - ✓ **SD-WAN or Software-defined networking**
 - ✓ **Cloud On Ramp Service Providers**
 - ✓ **Carrier-Neutral Colocation Services**
 - ✓ **AWS Direct Connect**
 - ✓ **Azure Express Route**
 - ✓ **Products and Services from Local Vendors**



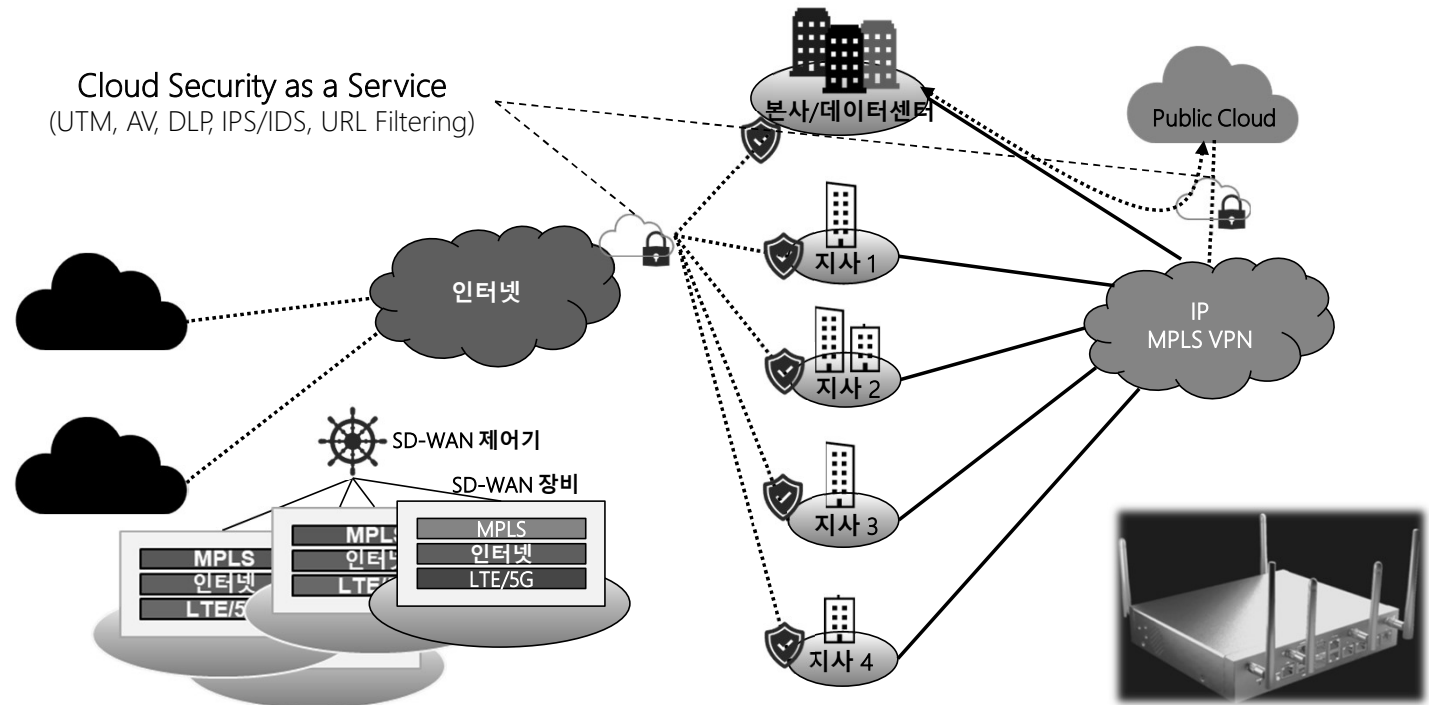
DAY 5. 멀티 클라우드 네트워킹

❖ 클라우드 구성



DAY 5. 멀티 클라우드 네트워킹

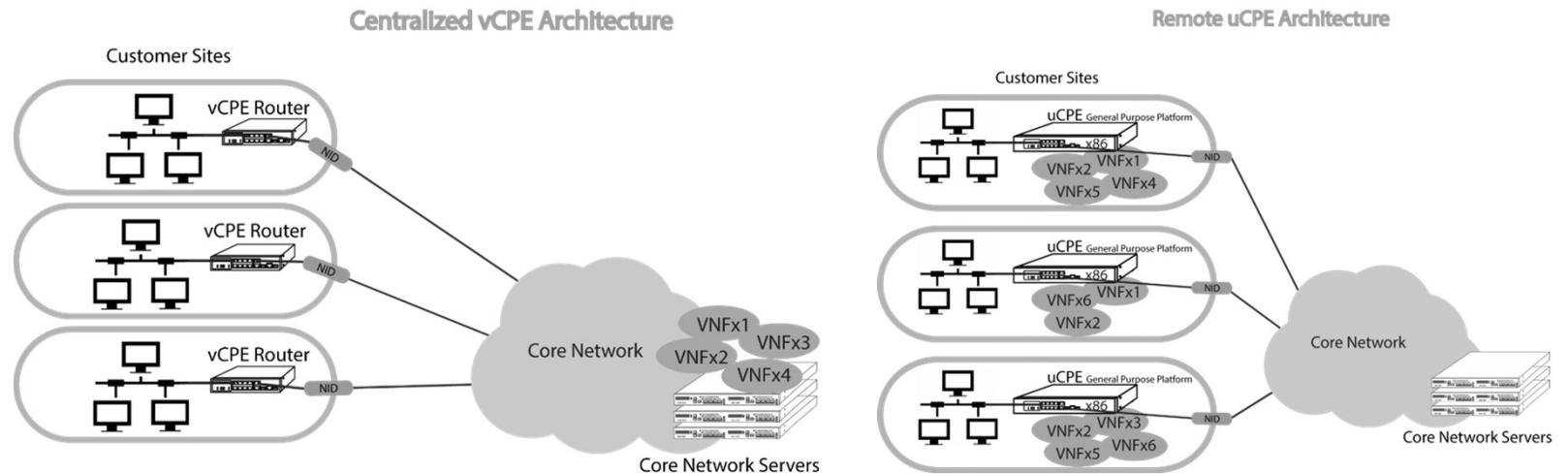
- ❖ SD-WAN의 발전
- ❖ Multi-Cloud 를 위한 엔터프라이즈 인터넷 접속 (하이브리드 클라우드)
- ❖ Cloud Security as-a-Service



DAY 5. 멀티 클라우드 네트워크

❖ 가상화 네트워크 기능 배포 기반 SD-WAN 구성

- 지역 배포 (예): uCPE (universal CPE)
 - ✓ 고사양 SD-WAN 하드웨어
 - ✓ 환경 변화에 따른 설계의 유연성
- 중앙 서비스 (예): vCPE or virtualized CPE
 - ✓ 저사양 SD-WAN 하드웨어
 - ✓ 데이터센터 집중 관리



DAY 5. 멀티 클라우드 네트워킹

❖ 자동화를 위한 소프트웨어 정의 네트워크(SDN) 기술 확장

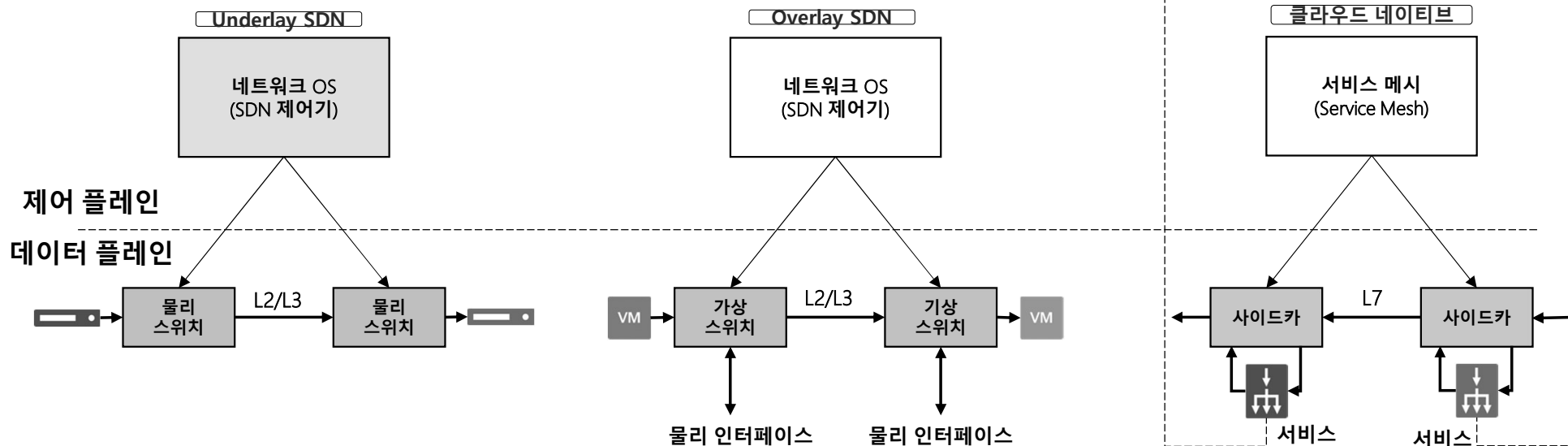
- 언더레이(Underlay) SDN
- 오버레이(Overlay) SDN - 가상화 네트워크
- 서비스 메시(Service Mesh) - 클라우드 네트워크

AMF
(Access and Mobility Management Function)

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: free5gc-amf-deployment
spec:
  selector:
    matchLabels:
      app: free5gc-amf
  replicas: 3
  template:
    metadata:
      labels:
        app: free5gc-amf
```

SMF
(Session Management Function)

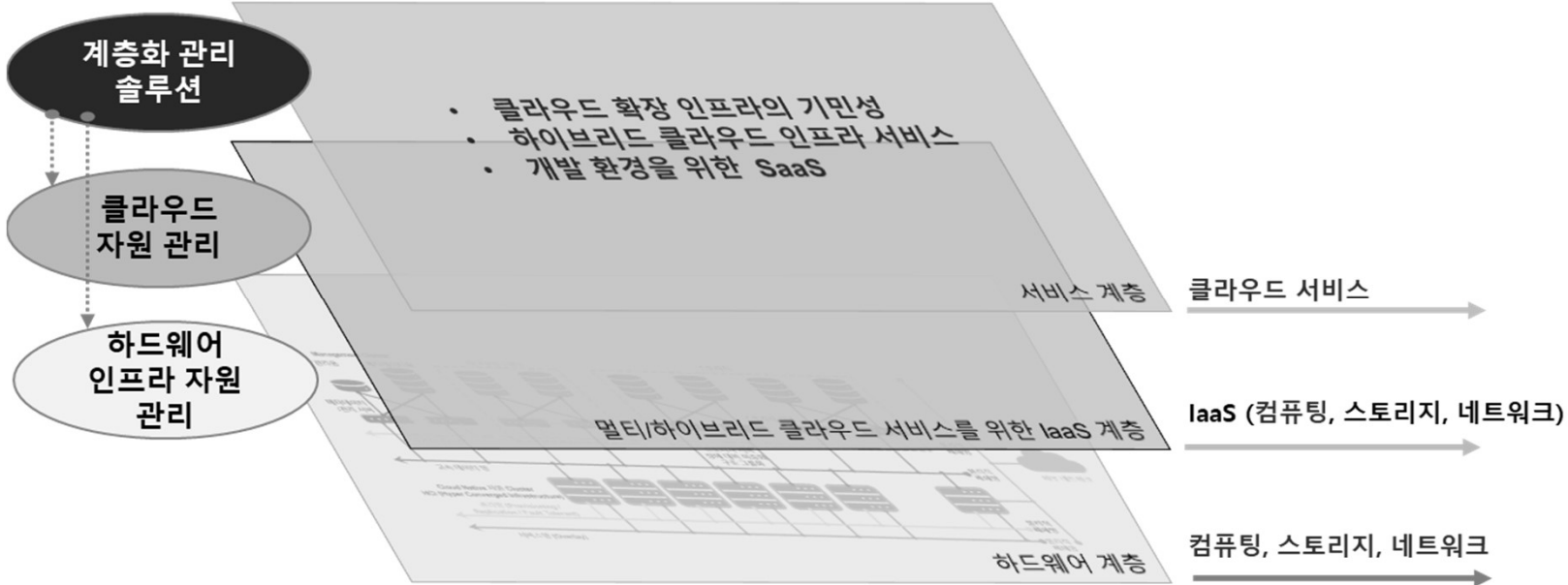
```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: free5gc-smf-deployment
spec:
  selector:
    matchLabels:
      app: free5gc-smf
  replicas: 3
  template:
    metadata:
      labels:
        app: free5gc-smf
```



DAY 5. 멀티 클라우드 네트워킹

❖ 멀티 클라우드 네트워킹의 계층 구조

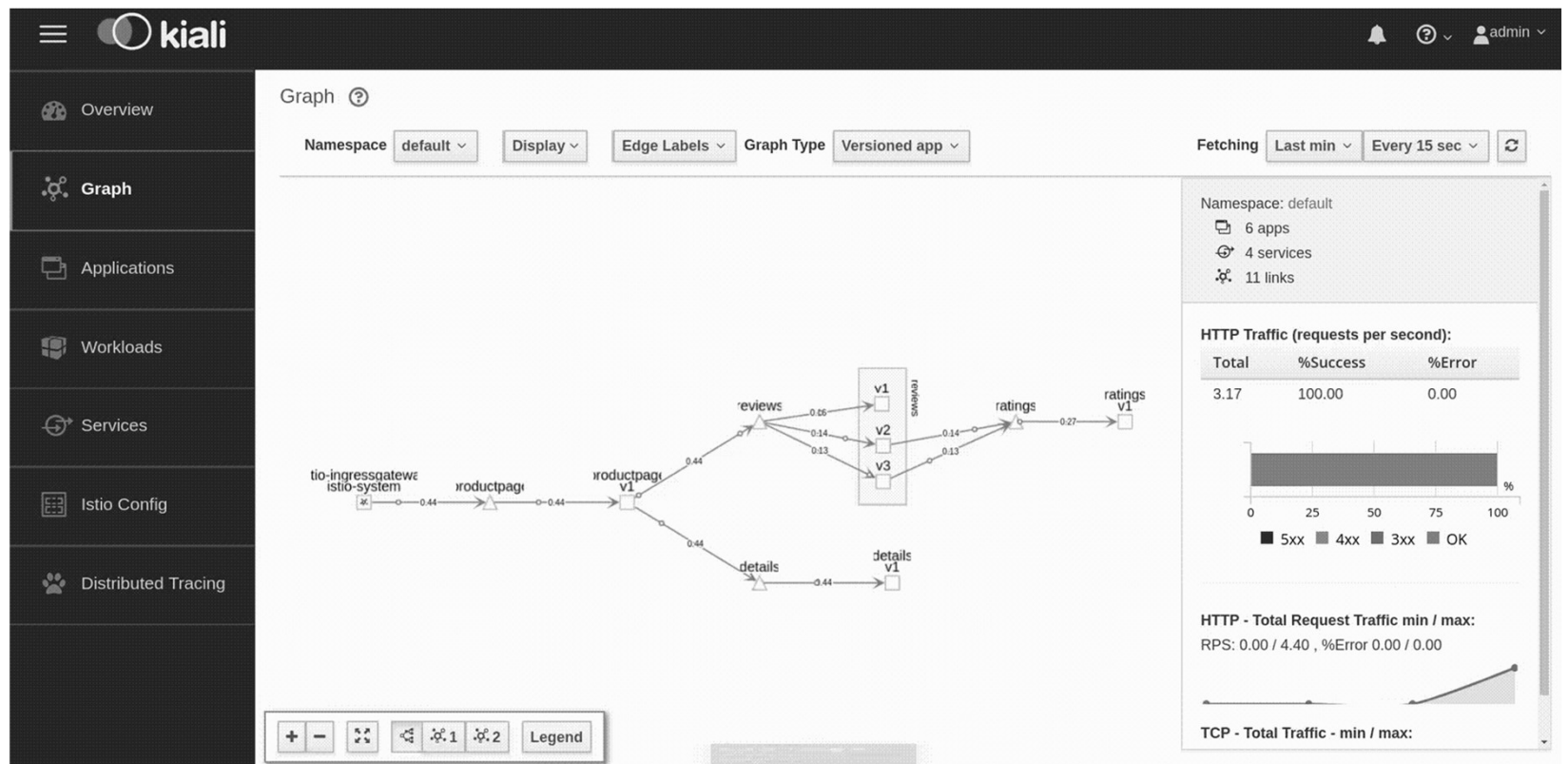
- 클라우드 네트워킹: 가상과 물리 네트워크와 독립적 추상화
- 가상 네트워크 환경 (Overlay SDN): OpenStack Neutron, VMware NSX 등
- 물리 네트워크 환경 (Underlay SDN): OCP Network, Cisco의 ACI 등



DAY 5. 멀티 클라우드 네트워킹

❖ Multi-Cloud Service Networking

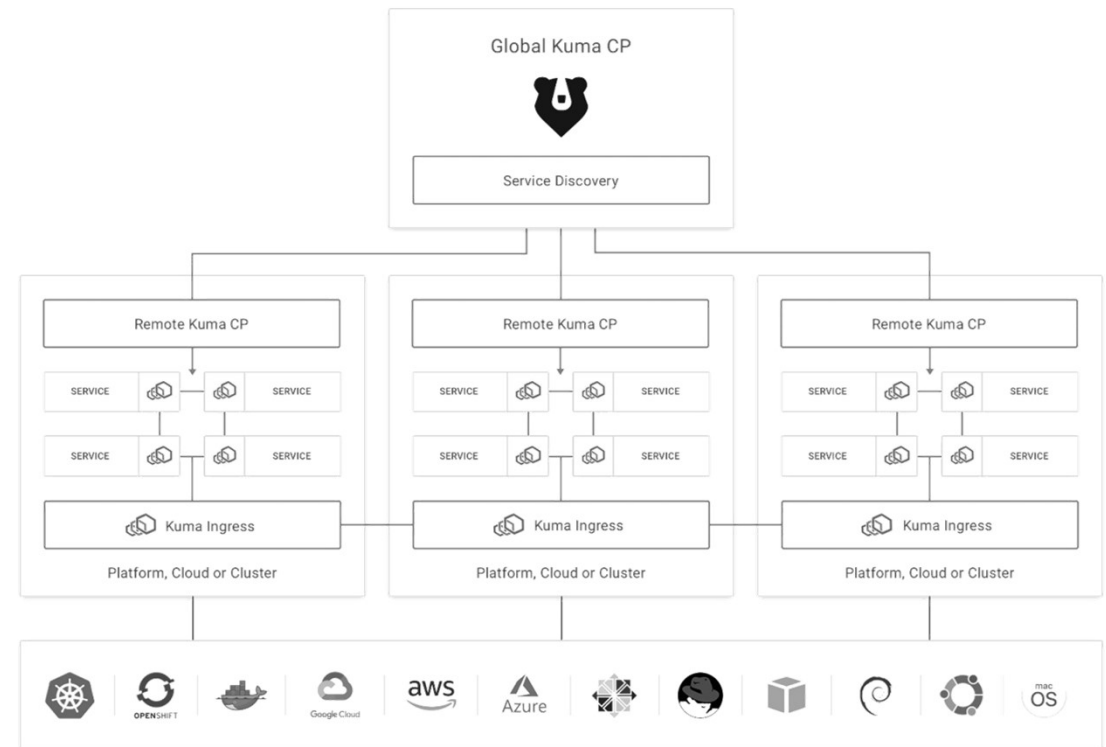
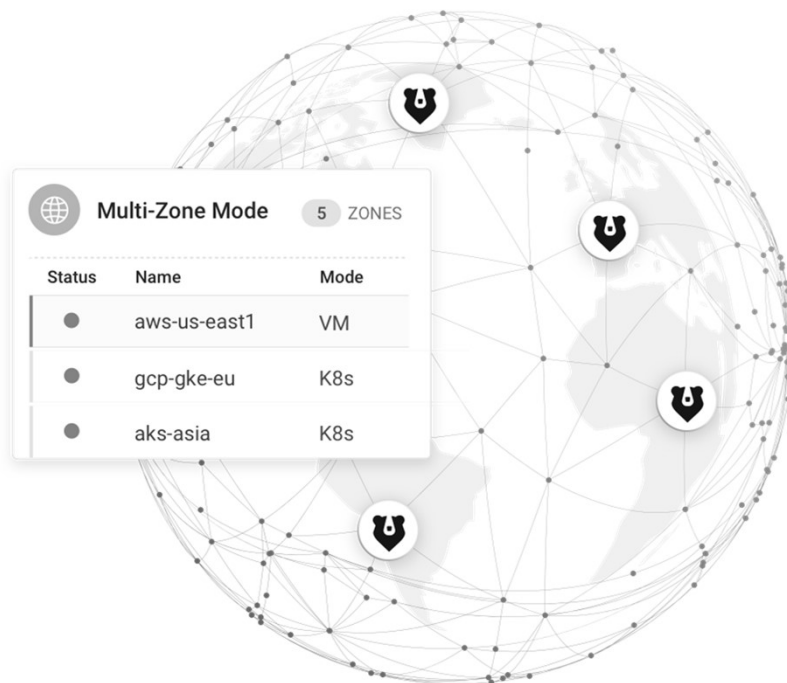
▪ Istio (Service Mesh)



DAY 5. 멀티 클라우드 네트워킹

❖ Multi-Cloud Service Networking

▪ Multi-Cluster & Multi-Cloud Service Mesh with Kuma and Envoy



Source: <https://kuma.io/>



DAY 5. 멀티 클라우드 네트워킹

❖ 클라우드 네트워킹의 복잡성 관리

- **라우팅:** Routing traffic rapidly and securely between disparate cloud platforms is complex; avoid complex Managed VPN solutions
- **자동화:** Automation needed for disparate CLI's, BGP ASN's, and routing tables
- **관리:** Managing multiple cloud, SaaS, network, and colocation providers is a juggling act!
- **중앙 관리:** Every provider will have their own proprietary method for management, monitoring, storage, and network solutions.
- **표준 보안 정책:** Establishing standard security capabilities and policies
- **보안 강화:** Ability to enforce security for users, data, and applications everywhere is essential



DAY 5. 멀티 클라우드 네트워킹

❖ Multi-Cloud Management Platforms Tools

- Dell Multi Cloud Manager
- Nutanix Enterprise Cloud Platform
- Red Hat CloudForms:
- VMware vRealize Suite
- BMC Multi Cloud Management
- Embotics vCommander
- Flexera Multi-Cloud Platform
- Scalr Cloud Management Platform

Source: <https://www.bunnysshell.com/blog/multi-cloud-management-platforms>



DAY 5. 멀티 클라우드 네트워킹

❖ Simulation Tools

- CloudSim
- CloudReports
- Cloud Analyst
- CloudSME
- MDCSim
- DCSim
- SimIC

Source: [file:///C:/Users/jsahn/AppData/Local/Temp/MicrosoftEdgeDownloads/752c126d-c6f5-4e08-887a-f257b259a64f/28878-77420-2-PB%20\(1\).pdf](file:///C:/Users/jsahn/AppData/Local/Temp/MicrosoftEdgeDownloads/752c126d-c6f5-4e08-887a-f257b259a64f/28878-77420-2-PB%20(1).pdf)



DAY 5. 멀티 클라우드 네트워킹

❖ Top 10 Network Management and Monitoring Tools in 2022

1. Auvik
2. Domotz
3. Datadog Network Performance Monitoring
4. Entuity
5. ManageEngine OpManager
6. PRTG Network Monitor
7. Nagios XI
8. SolarWinds Network Performance Monitor
9. Spiceworks Connectivity Dashboard
10. WhatsUp Gold

About the company	USP	Pricing	Pricing
Auvik	It is a Canadian company that builds IT, network, and security monitoring tools.	It has a robust API library that simplifies integration and automation.	Pricing starts at \$150 per month.
Domotz	It is a U.S.-based company with a presence in 90+ countries.	It is a plug-and-play solution, which can be set up in 10 minutes.	It costs approximately \$25 per month per site.
Datadog	It is a U.S.-Based, NASDAQ traded observability tools provider.	It correlates network issues with application issues to speed up root cause analysis.	Pricing starts at \$5 per month for performance monitoring and \$7 per month for device monitoring.
Entuity	It is powered by the U.S.-based software company Park Place, which also provides managed services.	It has 100+ pre-built reports, automation features, default noise rules, etc., which can be used out of the box.	It is custom-priced with a free trial.
ManageEngine	It is part of Zoho, an Indian technology company that targets SMBs.	It has a threshold calculation feature that triggers an alarm.	Pricing starts at \$245.
PRTG Network Monitor	It is a tool built by the German technology company Paessler.	It has a free failover solution, never to lose access to your network management dashboard.	Pricing starts at \$1,750 per server for perpetual licenses.
Nagios XI	It is a commercial tool built on the open-source infrastructure monitoring solution, Nagios, launched in 2002.	Its open-source architecture drives flexibility and extensibility while operating out of a Linux environment.	Pricing starts at \$1,995.
SolarWinds Network Performance Monitor	SolarWinds is a multinational monitoring tools company traded on the NYSE.	It offers proprietary technologies like PerfStack™, NetPath™, and Orion® Maps and simplifies critical path analysis.	Pricing starts at \$1,638.
Spiceworks Connectivity Dashboard	It is a U.S.-based company that develops tools, frameworks, and resources for IT pros.	It is a free network management and monitoring tool that integrates with other Spiceworks offerings.	It is available for free.
WhatsUp Gold	It was initially built by Ipswitch, which was recently acquired by Progress.	It supports add-on modules such as virtualization monitoring, failover management, and more without investing in a separate	

Source: <https://www.spiceworks.com/tech/networking/articles/best-network-monitoring-tools/>



DAY 5. 멀티 클라우드 네트워킹

❖ Open Source Cloud monitoring tools

- Prometheus.
- Zabbix.
- Nagios.
- Riemann.
- Sensu.
- Icinga.
- Cacti.
- LibreNMS.
- Observium Community.
- Pandora FMS.

Zabbix: This open-source software is mostly recommended because of its easy-to-use interface. It stores the data in a relational database for well-organised processing. Zabbix can do the following tasks:

- Network Monitoring.
- Server Monitoring.
- Cloud Monitoring.
- Application Monitoring.
- Service Monitoring

실습 대상이었음

Source: <https://www.e2enetworks.com/blog/open-source-cloud-monitoring-tools>



DAY 5. 멀티 클라우드 네트워킹

❖ Open Source Cloud Management Platforms

- Apache CloudStack: <https://cloudstack.apache.org/>
- OpenStack: <http://www.openstack.org>
- ManageIQ (CMP for hybrid IT environments): <http://manageiq.org>
- Cloudify (cloud and NFV orchestration product): <http://www.cloudify.co>
- Mist.io (platform that simplifies cloud management): <http://www.mist.io>
- VirtEngine (CMP can be used to build private or public clouds): <http://www.virtengine.com>
- openQRM (cloud computing management platform): <http://openqrm-enterprise.com>
- OpenNebula (private clouds and manage data centre virtualization): <http://www.opennebula.org>
- Eucalyptus (Infrastructure as a Service (IaaS)): <https://www.eucalyptus.cloud/>

Source: <https://www.opensourceforu.com/2019/11/the-top-nine-open-source-cloud-management-platforms/>



DAY 5. 멀티 클라우드 네트워킹

❖ The 15 Best Cloud Management Software Platforms In 2022

- **CloudZero** - Cloud cost intelligence platform
- **Kubernetes** - Container and microservices management platform
- **Morpheus** - Self-service hybrid cloud management and automation platform
- **Apache CloudStack** - Open-source cloud management platform for small and medium businesses
- **Terraform** - Infrastructure-as-code software for managing multiple cloud services
- **TotalCloud** - Workflow-based cloud management software
- **Cloud Orchestrator by IBM** - Policy-based cloud management software
- **RedHat Cloud Suite** - RedHat's All-in-one cloud management tools
- **AppDynamics** - Cloud monitoring and management for on-premises and hybrid clouds
- **Azure Management Tools** - End-to-end Microsoft Azure cloud infrastructure management
- **CoreStack** - Multicloud governance software
- **Semantext** - On-premise and cloud-native infrastructure monitoring solution
- **SolarWinds** - Hybrid cloud server monitoring software
- **LaceWork** - All-in-one cloud security platform for companies of all sizes
- **Sensu** - Free, open-source, and hybrid cloud monitoring platform

Source: <https://www.cloudzero.com/blog/cloud-management-software>



DAY 5. 멀티 클라우드 네트워킹

❖ Comparison Of The BEST Cloud Management Platforms

- VMware
- IBM Cloud Orchestrator
- Flexera Rightscale
- Apache CloudStack
- BMC Cloud Lifecycle Management
- Scalr
- Embotics
- OpenStack
- RedHat CloudForms
- CloudHealth
- Turbonomic
- Abiquo

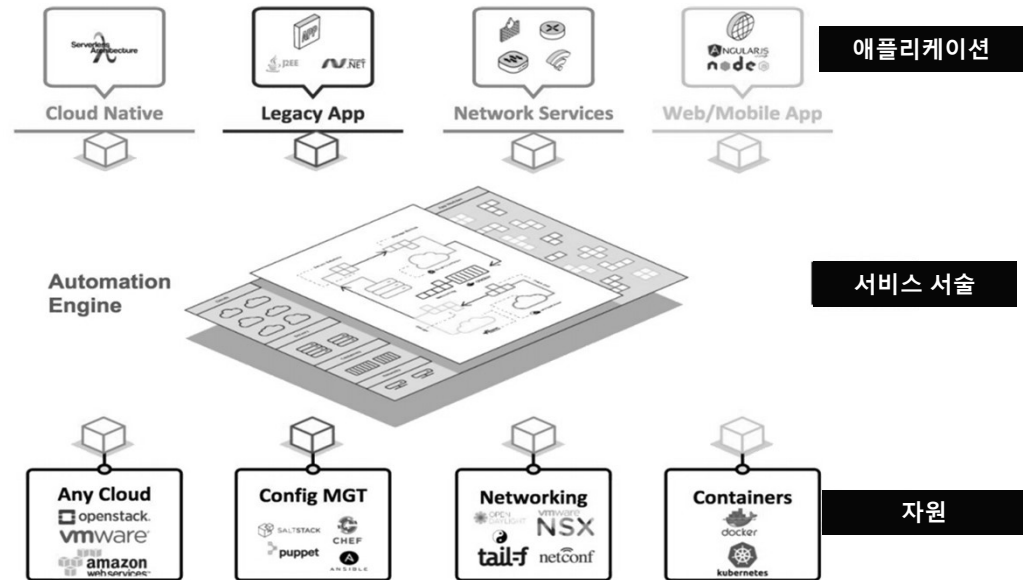
Source: <https://www.softwaretestinghelp.com/cloud-management-platforms/>



DAY 5. 멀티 클라우드 네트워킹

❖ 필요한 멀티클라우드 관리 기능 채택 (예)

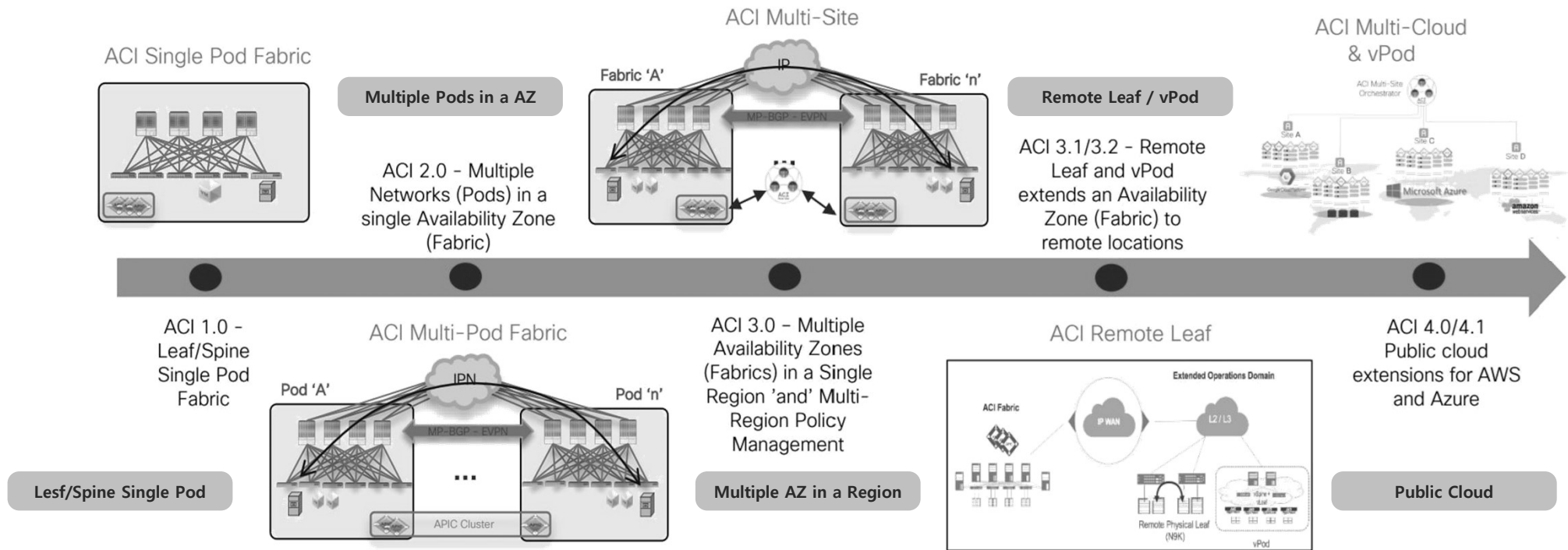
- 컨테이너 사용 가능
- 대부분의 주요 클라우드에서 지원하는 쿠버네티스(K8s) 사용
- 멀티 클라우드와 플랫폼 호환성과 통합이 가능한 자동화 프레임워크
- 애플리케이션의 요청에 따라 추상화한 인프라 자원을 제공



DAY 5. 멀티 클라우드 네트워킹

❖ 언더레이 SDN 제조사(예): Cisco ACI

- ACI extensions to public clouds
- Extending Virtual ACI

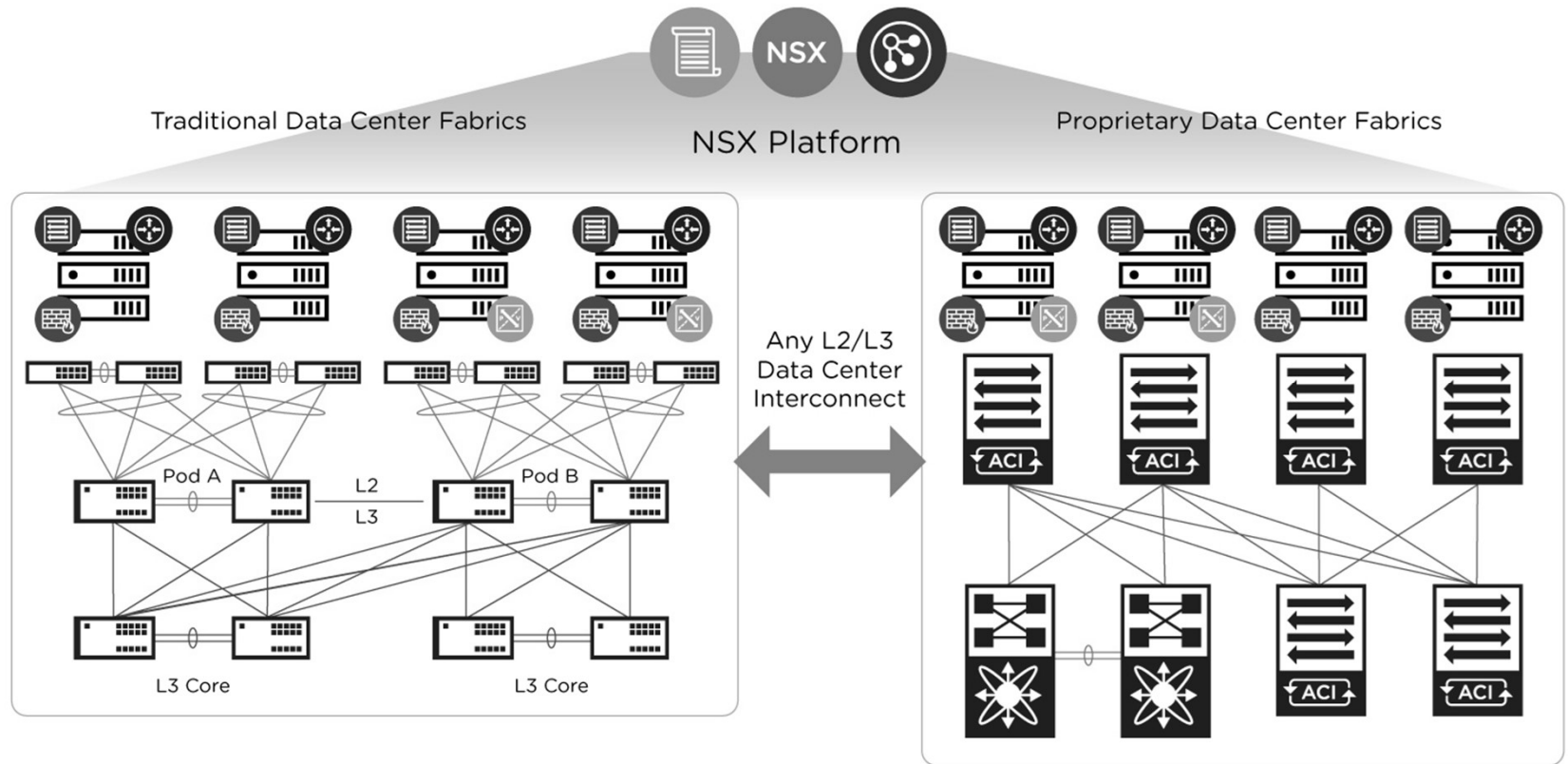


Source: <https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-740861.html>



DAY 5. 멀티 클라우드 네트워킹

❖ Cisco ACI

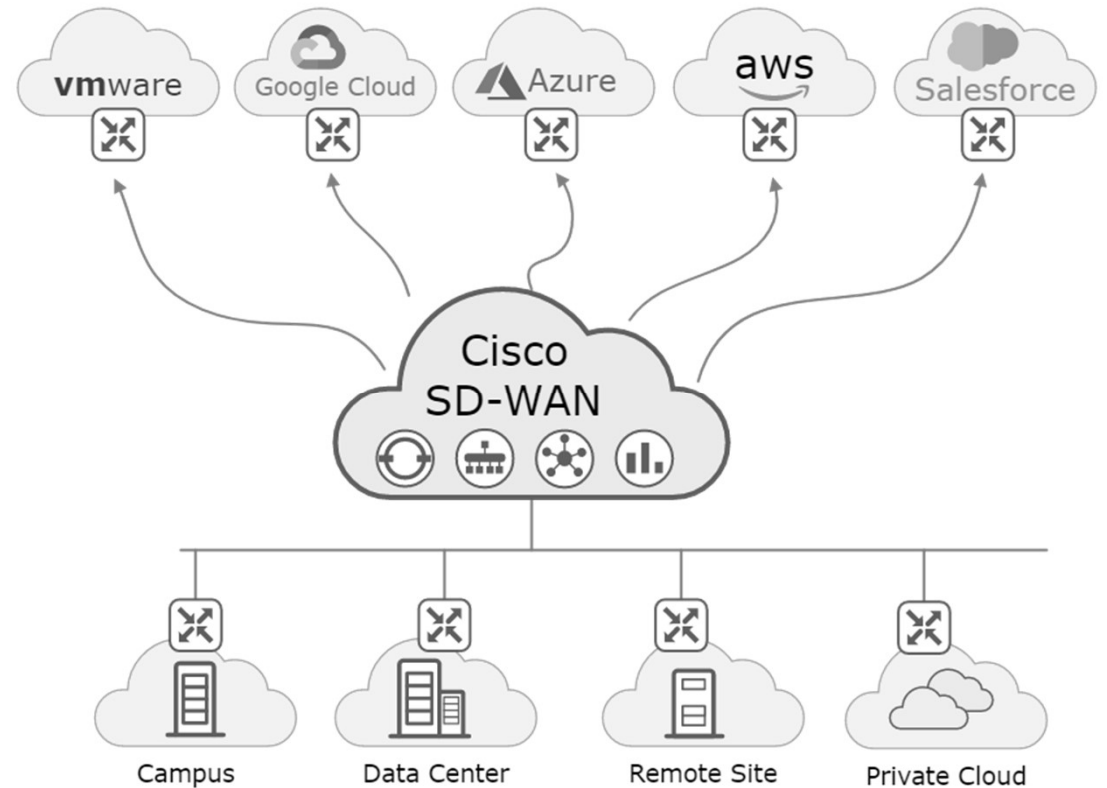


Source: <https://blogs.vmware.com/networkvirtualization/2018/09/reference-guide-update-nsx-on-aci.html/>



DAY 5. 멀티 클라우드 네트워킹

❖ Cisco SD-WAN as Multi-Cloud Interconnect

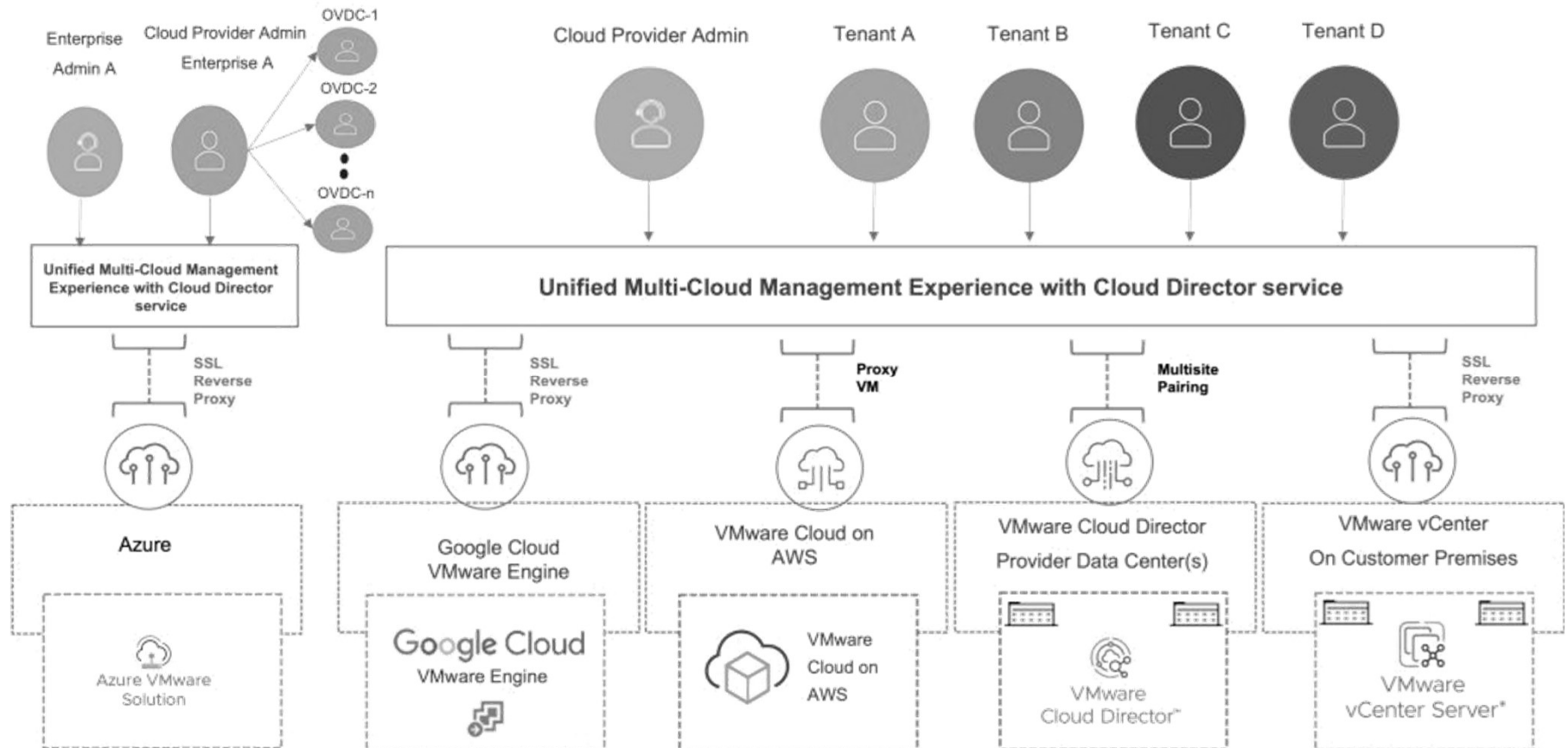


Source: <https://www.networkacademy.io/ccie-enterprise/sdwan/interconnecting-multiple-clouds>



DAY 5. 멀티 클라우드 네트워킹

❖ Cloud Director Service Expanding Multi-Cloud Services on Azure VMware Solution

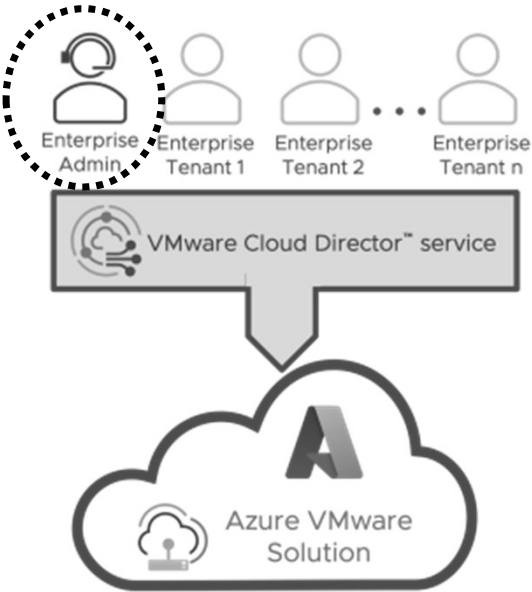


Source: https://blogs.vmware.com/cloudprovider/2022/08/cloud-director-service-expanding-multi-cloud-services-on-azure-vmware-solution.html?utm_source=rss&utm_medium=rss&utm_campaign=cloud-director-service-expanding-multi-cloud-services-on-azure-vmware-solution



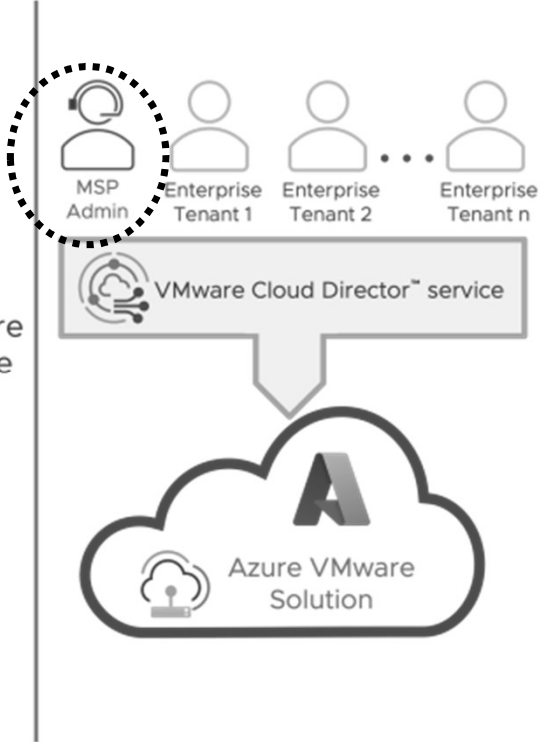
DAY 5. 멀티 클라우드 네트워킹

❖ Cloud Director Service Expanding Multi-Cloud Services on Azure VMware Solution



Self-Managed Enterprise Cloud

- Enterprise wants self-service multi-tenancy
- Tenants have secure isolation & resource allocations
- Enterprise purchases Cloud Director service
- Enterprise purchases AVS



Outsourced Enterprise Cloud Management

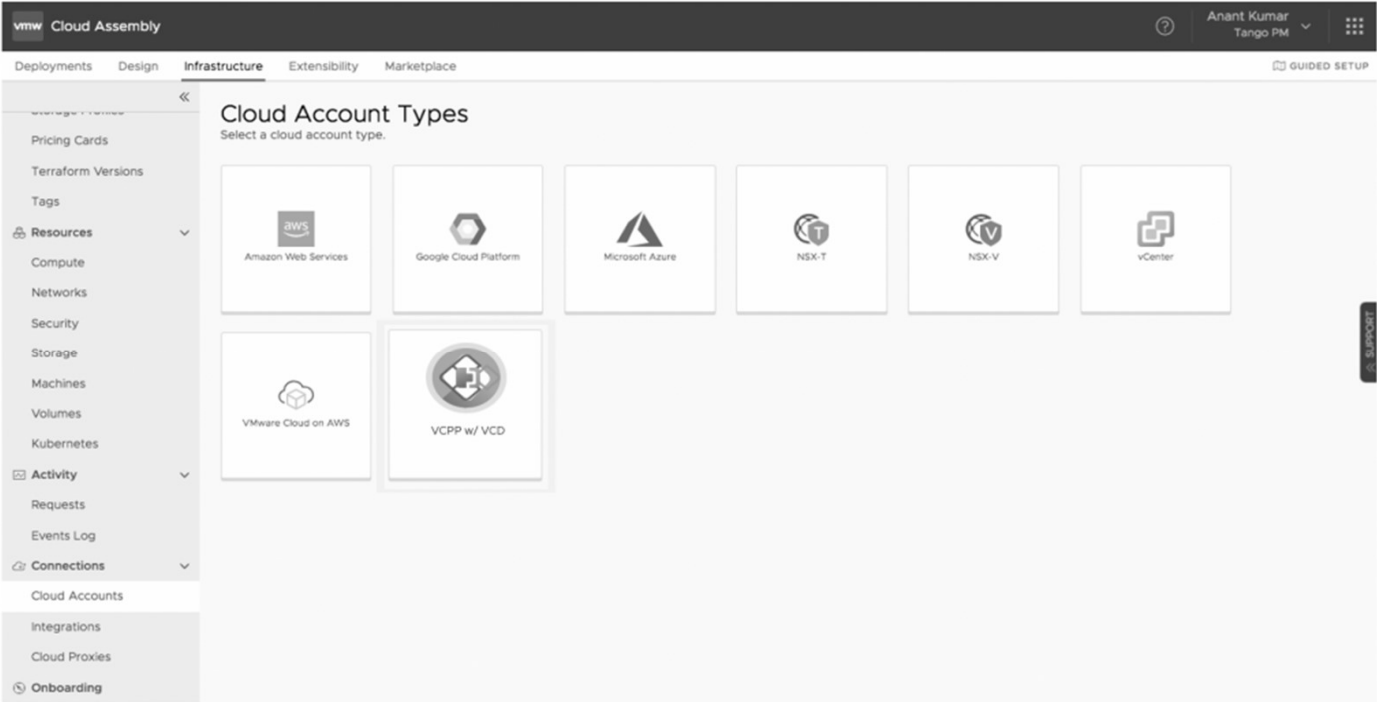
- Managed Service Provider administers enterprise's cloud tenants
- Tenants have secure isolation & resource allocations
- MSP purchases Cloud Director service
- Enterprise purchases AVS

Source: https://blogs.vmware.com/cloudprovider/2022/08/cloud-director-service-expanding-multi-cloud-services-on-azure-vmware-solution.html?utm_source=rss&utm_medium=rss&utm_campaign=cloud-director-service-expanding-multi-cloud-services-on-azure-vmware-solution



DAY 5. 멀티 클라우드 네트워킹

❖ Monetize self-service multi-cloud management with the NEW VCD endpoint for vRA



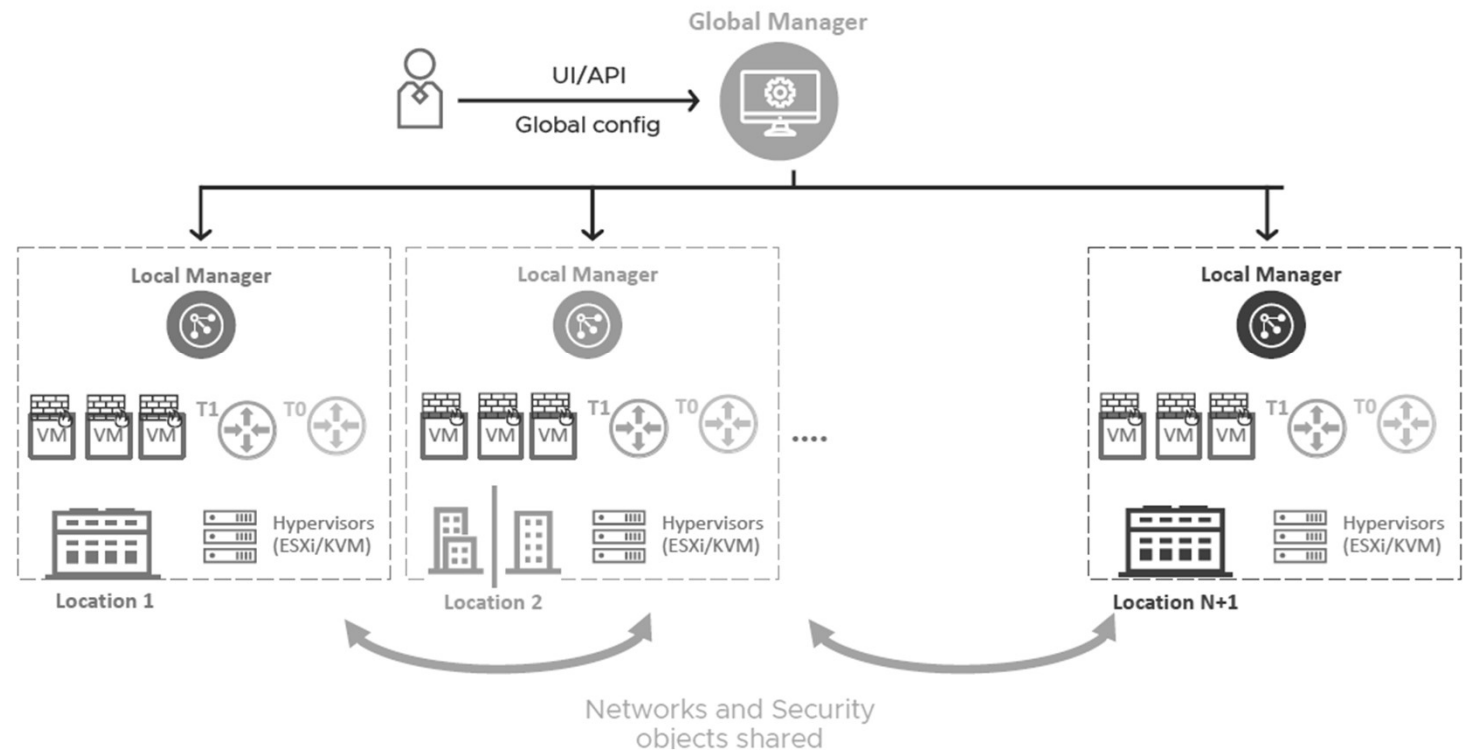
**vRealize Automation (vRA)
VMware Cloud Director (VCD)**

Source: <https://blogs.vmware.com/cloudprovider/2021/11/monetize-self-service-multi-cloud-management-with-the-new-vcd-endpoint-for-vra.html>



DAY 5. 멀티 클라우드 네트워킹

❖ VMware NSX-T 3.0

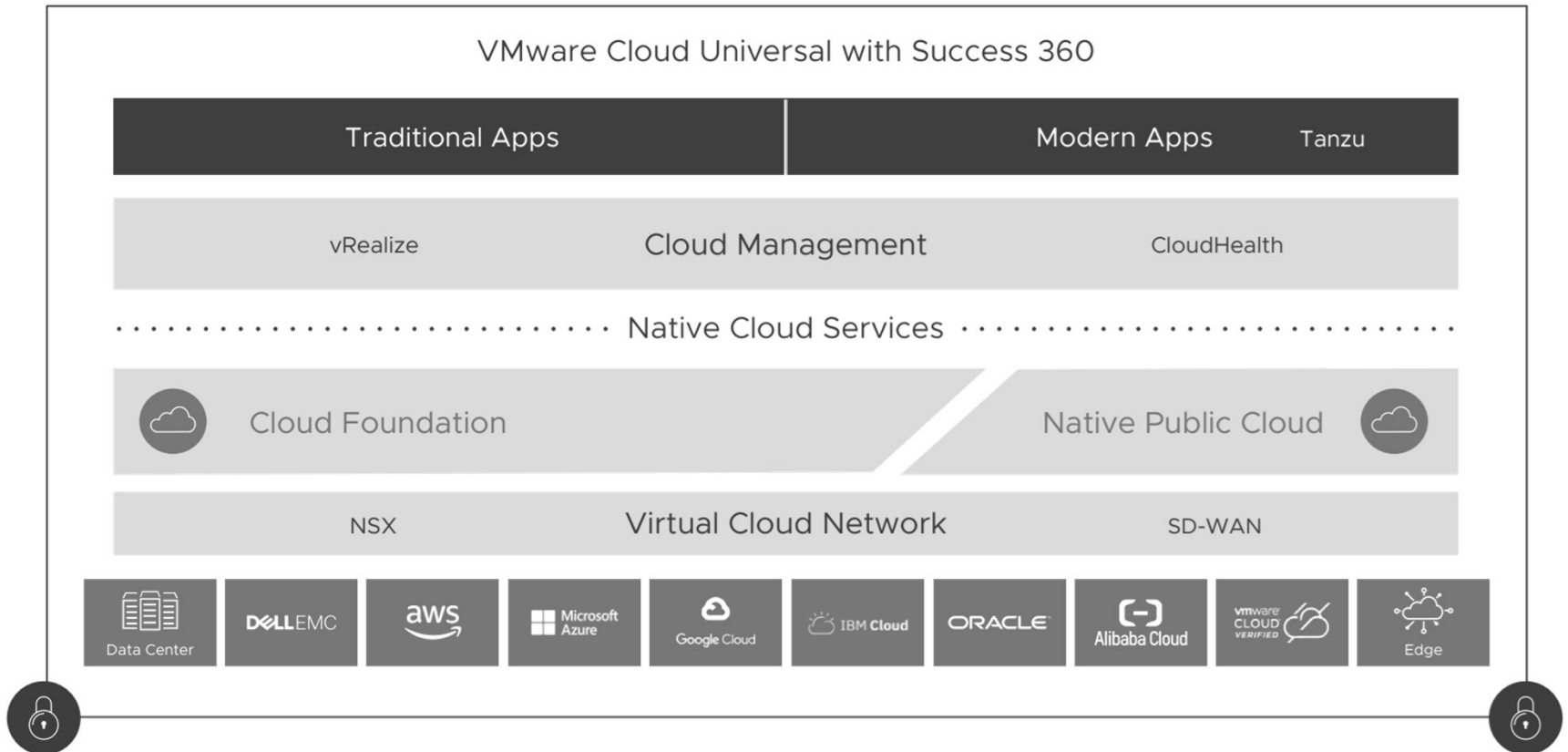


Source: <https://www.definetomorrow.co.uk/blog/2020/4/8/introducing-nsx-t-30-whats-new>



DAY 5. 멀티 클라우드 네트워킹

❖ VMware Cloud

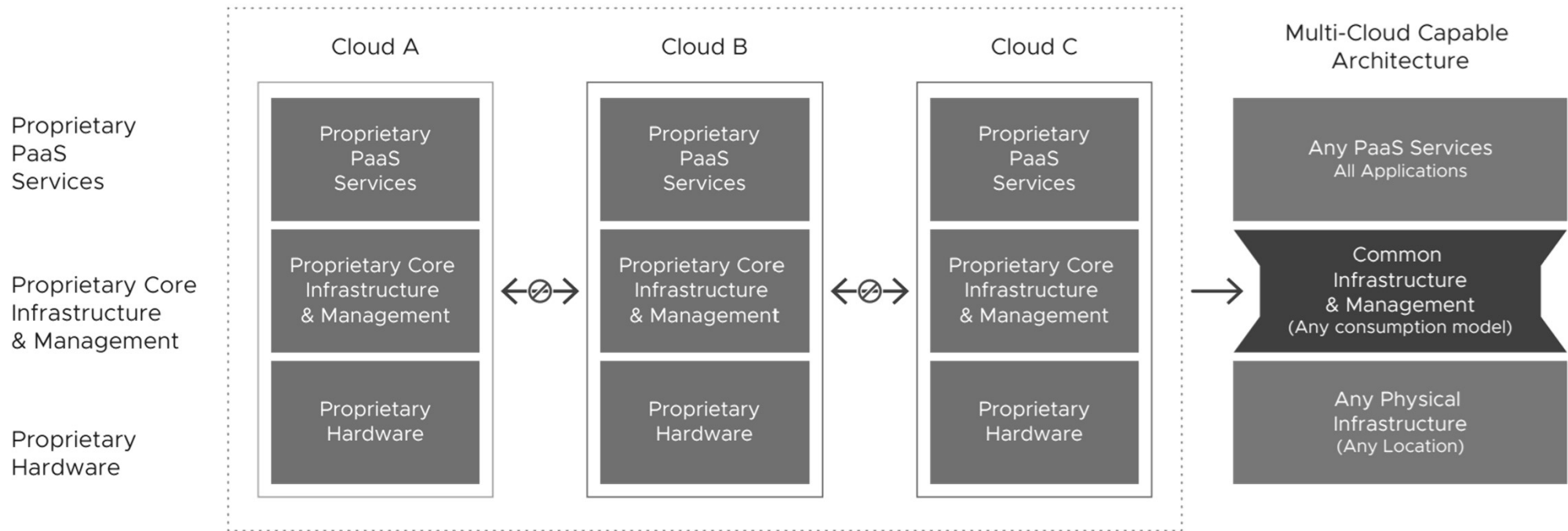


Source: Architecting Your Multi-Cloud Environment, VMware



DAY 5. 멀티 클라우드 네트워킹

❖ The challenge of siloed public clouds

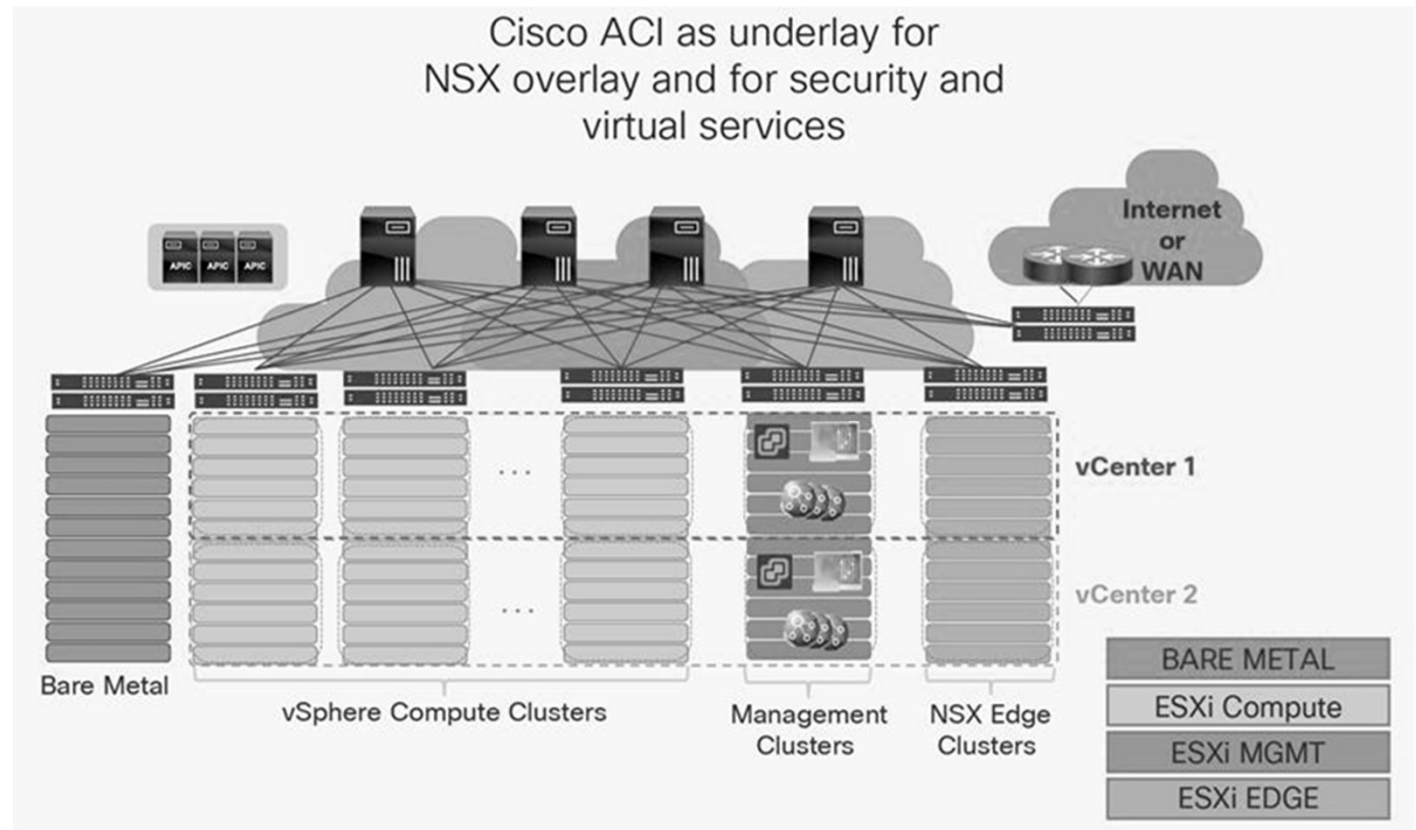


Source: Architecting Your Multi-Cloud Environment, VMware



DAY 5. 멀티 클라우드 네트워킹

❖ Cisco ACI as underlay

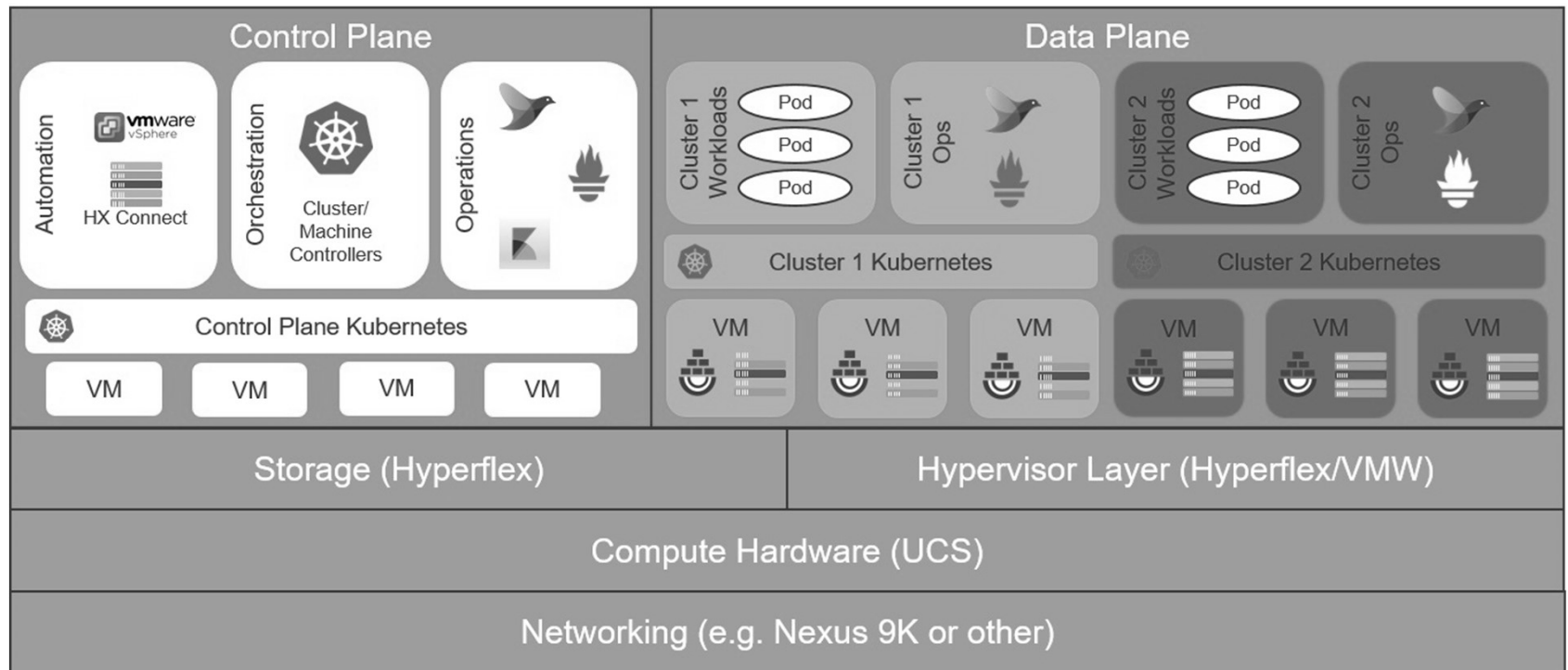


Source: <https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/white-paper-c11-740124.html>



DAY 5. 멀티 클라우드 네트워킹

- ❖ Container Platform
- ❖ Cisco Container Platform Architecture Overview



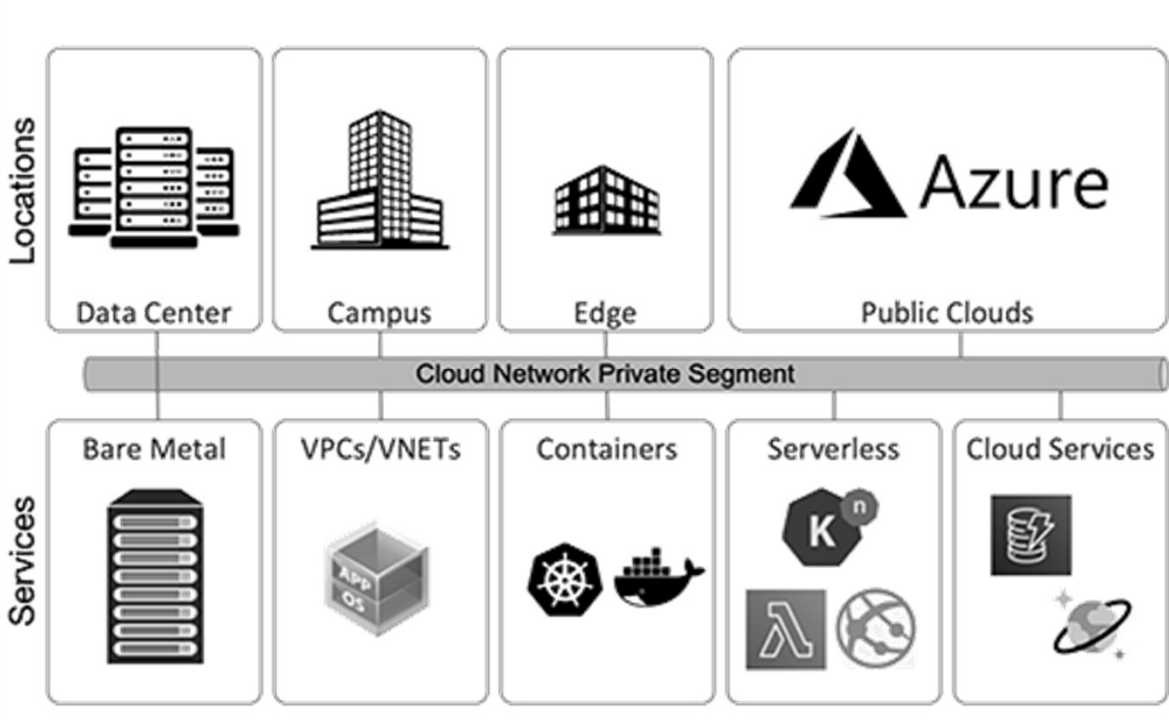
Source: https://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_container_platform/3-1/Installation_Guide/CCP-Installation-Guide-3-1-0/CCP-Installation-Guide-3-1-0_chapter_00.html



DAY 5. 멀티 클라우드 네트워킹

❖ Arista

- CloudEOS Router provides multi-cloud networking and security using proven EOS Software

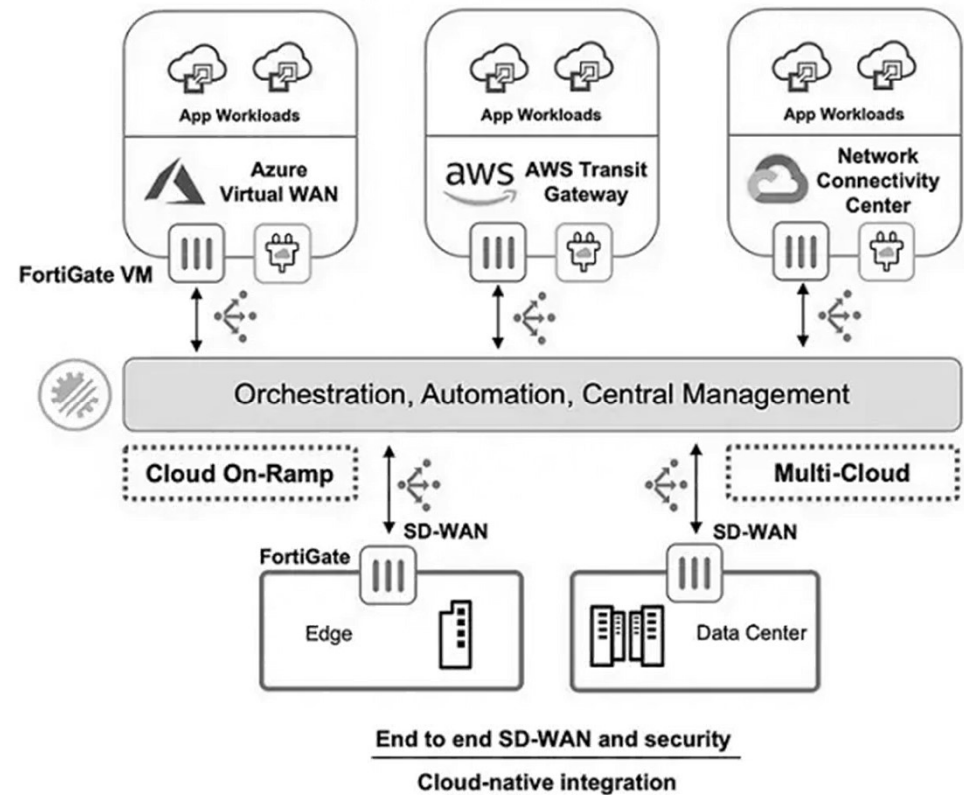


Source: <https://azuremarketplace.microsoft.com/en-us/marketplace/apps/arista-networks.cloudeos-router-payg?tab=Overview>



DAY 5. 멀티 클라우드 네트워킹

❖ Secure SD-WAN for Multi-Cloud Infrastructure (포티넷)



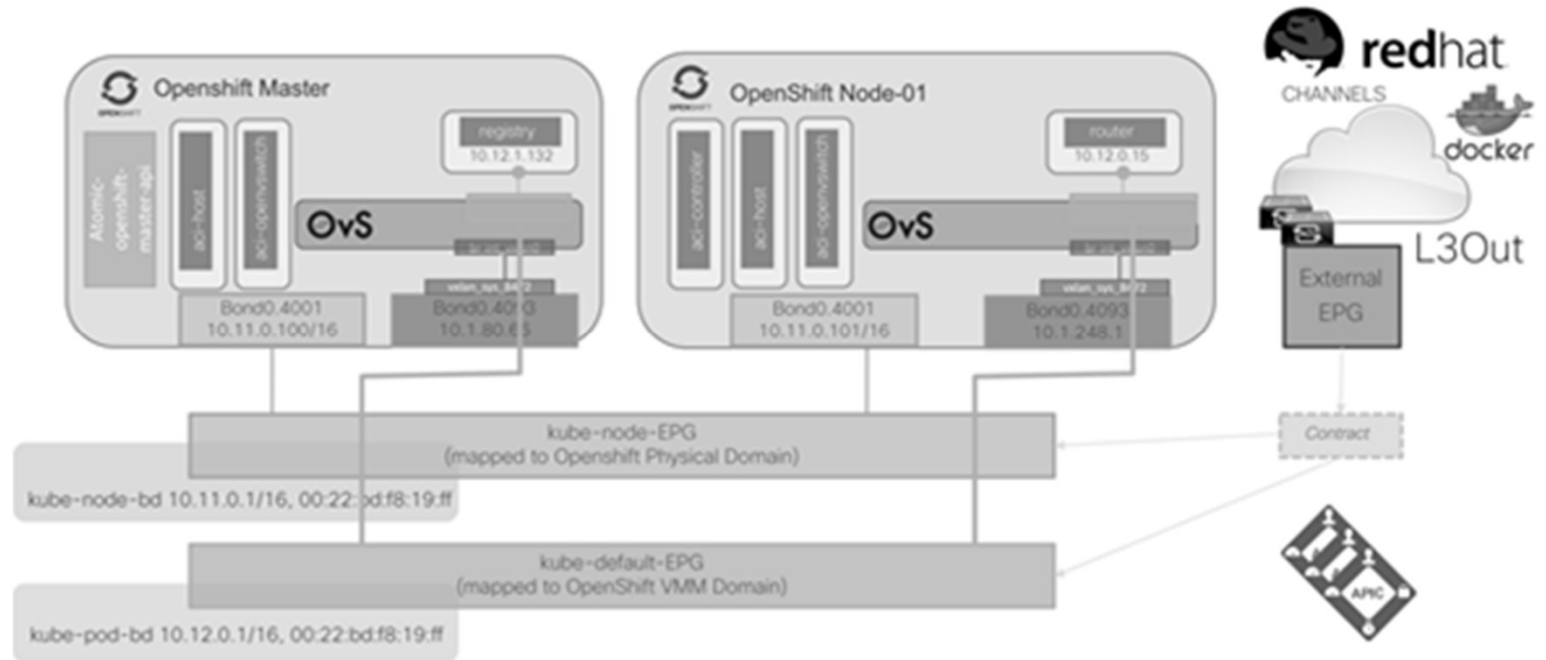
Source: <https://www.fortinet.com/solutions/enterprise-midsize-business/sd-wan-multi-cloud>



DAY 5. 멀티 클라우드 네트워킹

❖ 제조사 솔루션 연동

- 제조사들의 멀티클라우드 기반 아키텍처에 오픈소스 네트워킹 기술 채택
- Red Hat, Cisco, VMware 등



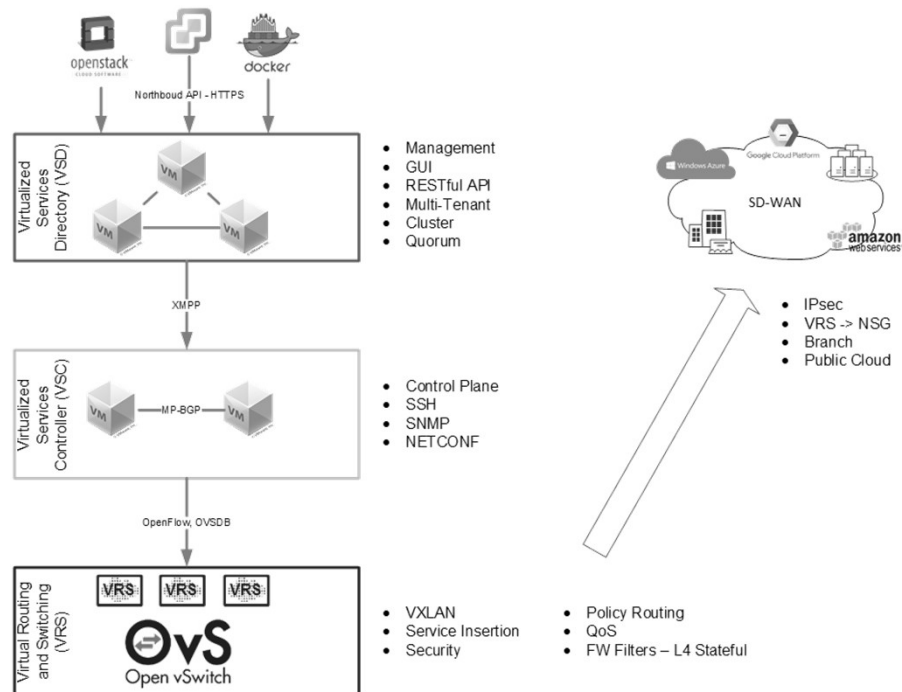
Source: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/white_papers/Cisco-ACI-CNI-Plugin-for-OpenShift-Architecture-and-Design-Guide.html



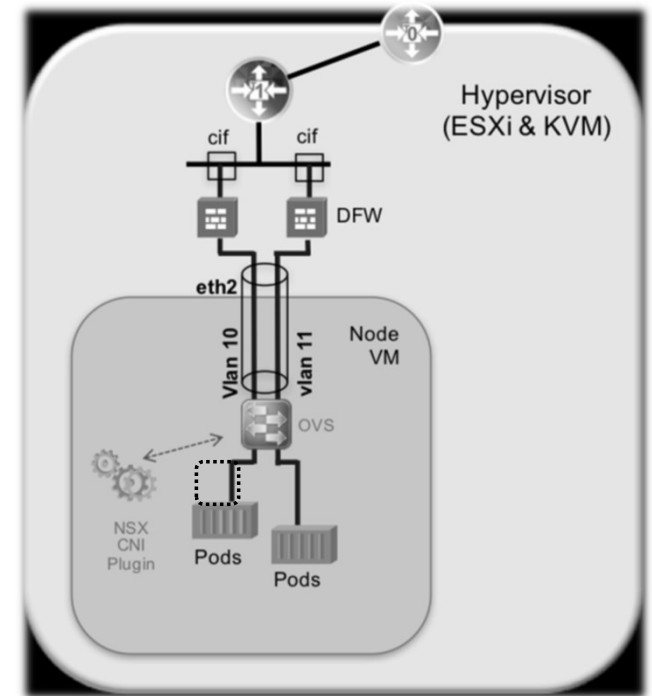
DAY 5. 멀티 클라우드 네트워킹

❖ 제조사 솔루션 연동

- 제조사들의 멀티클라우드 기반 아키텍처에 오픈소스 네트워킹 기술 채택
- Red Hat, Cisco, VMware 등



Source: <https://thedataplumber.net/nsx-t-vs-nsx-v-and-a-little-bit-of-nuage-vsp/>

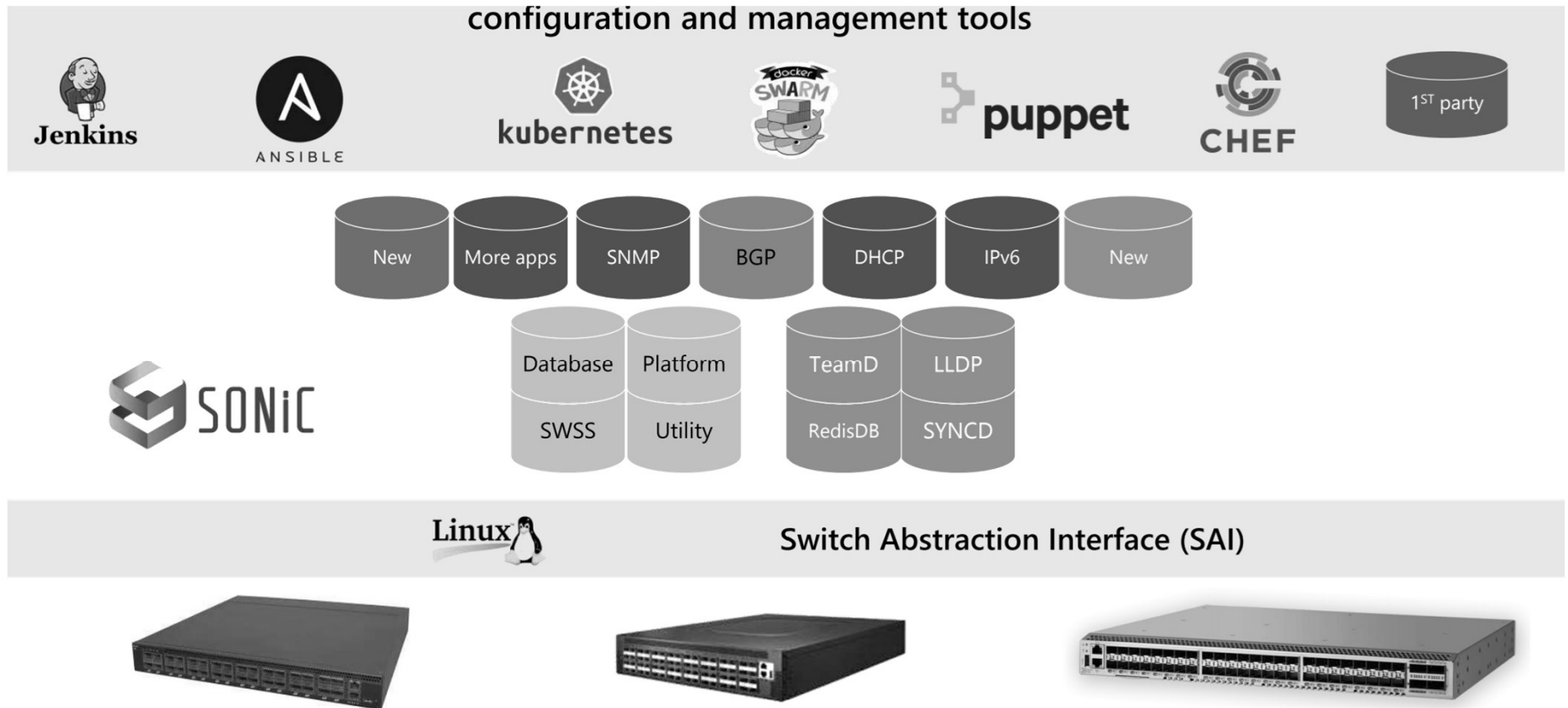


Source: <https://www.routetocloud.com/category/nsx-t/>



DAY 5. 멀티 클라우드 네트워킹

❖ SONiC (Software for Open Networking in the Cloud)

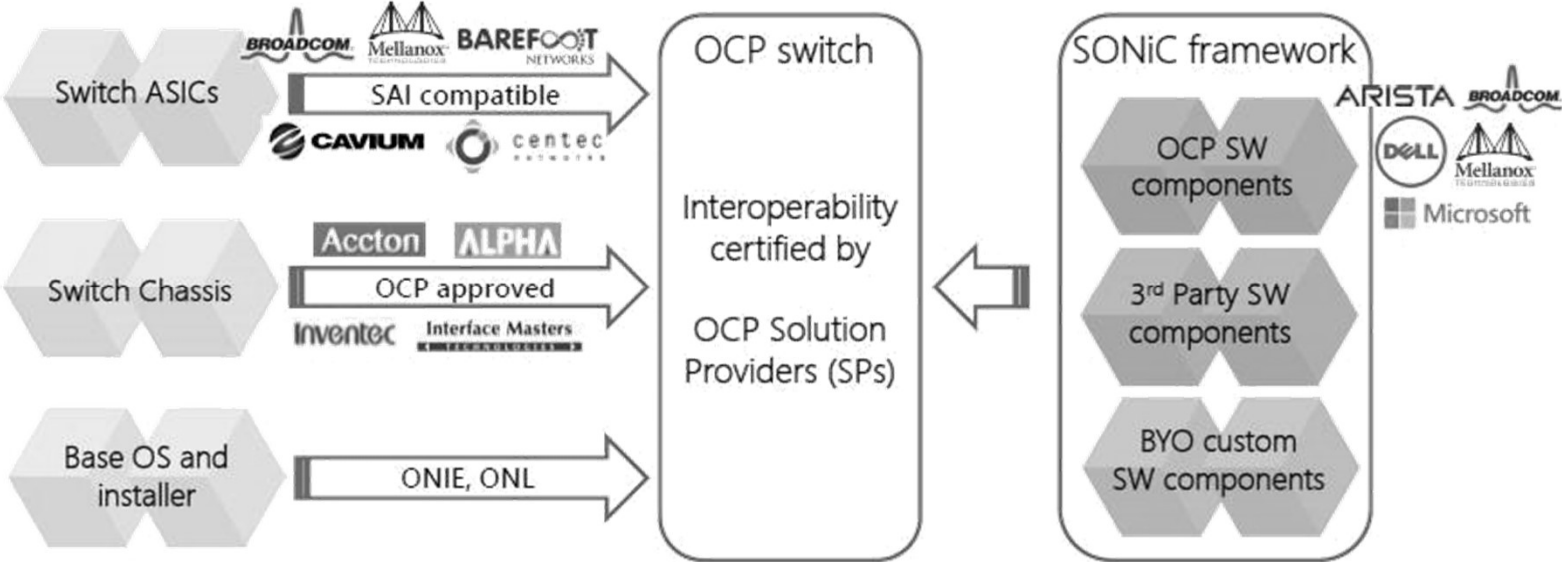


DAY 5. 멀티 클라우드 네트워킹

❖ SONiC ecosystem

- SONiC (Software for Open Networking in the Cloud)

SONiC vision for the OCP switch ecosystem

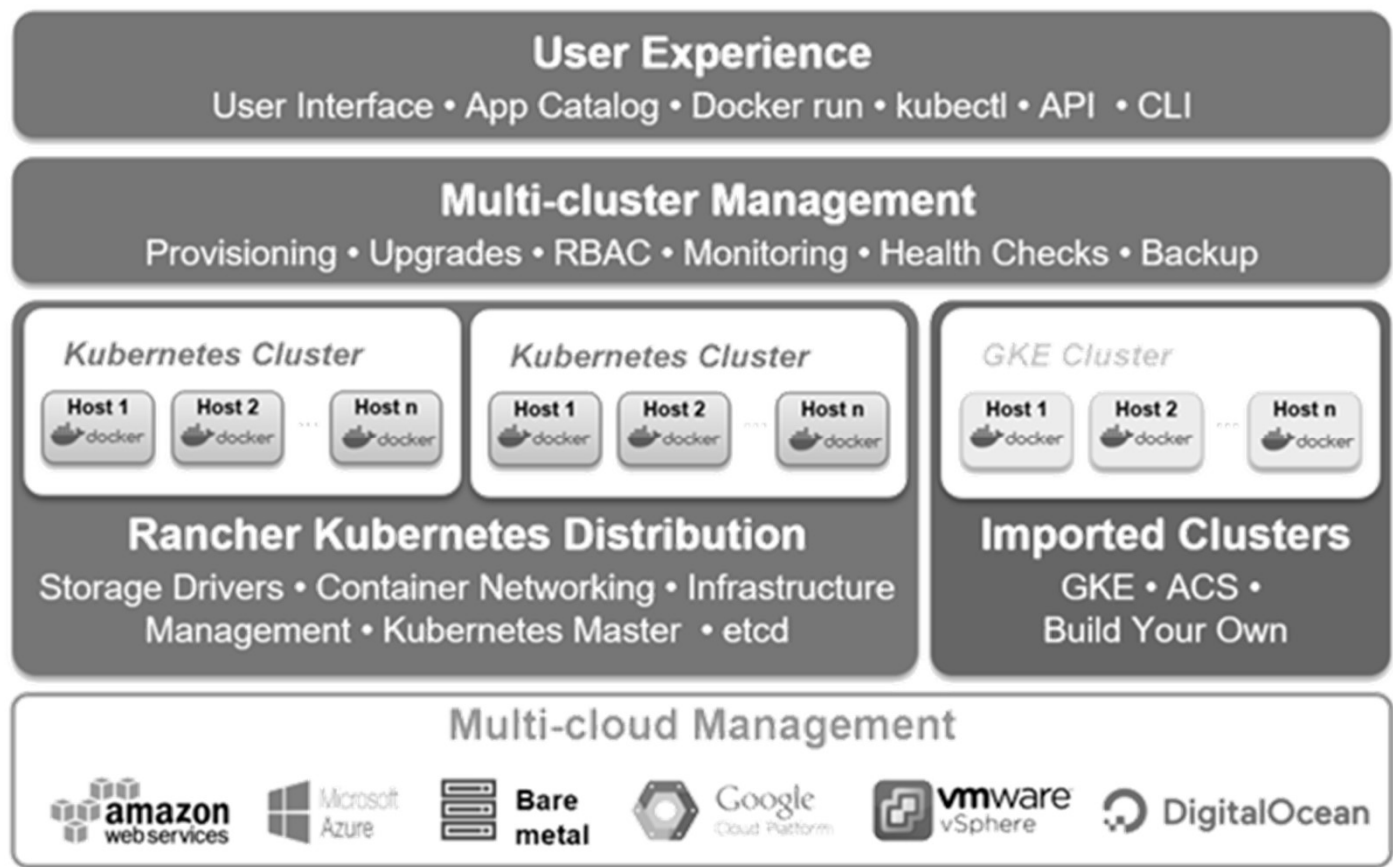


Fully Open Sourced switching platform - Increased choices for OCP end users



DAY 5. 멀티 클라우드 네트워킹

- ❖ Rancher Labs
 - Rancher 2.x



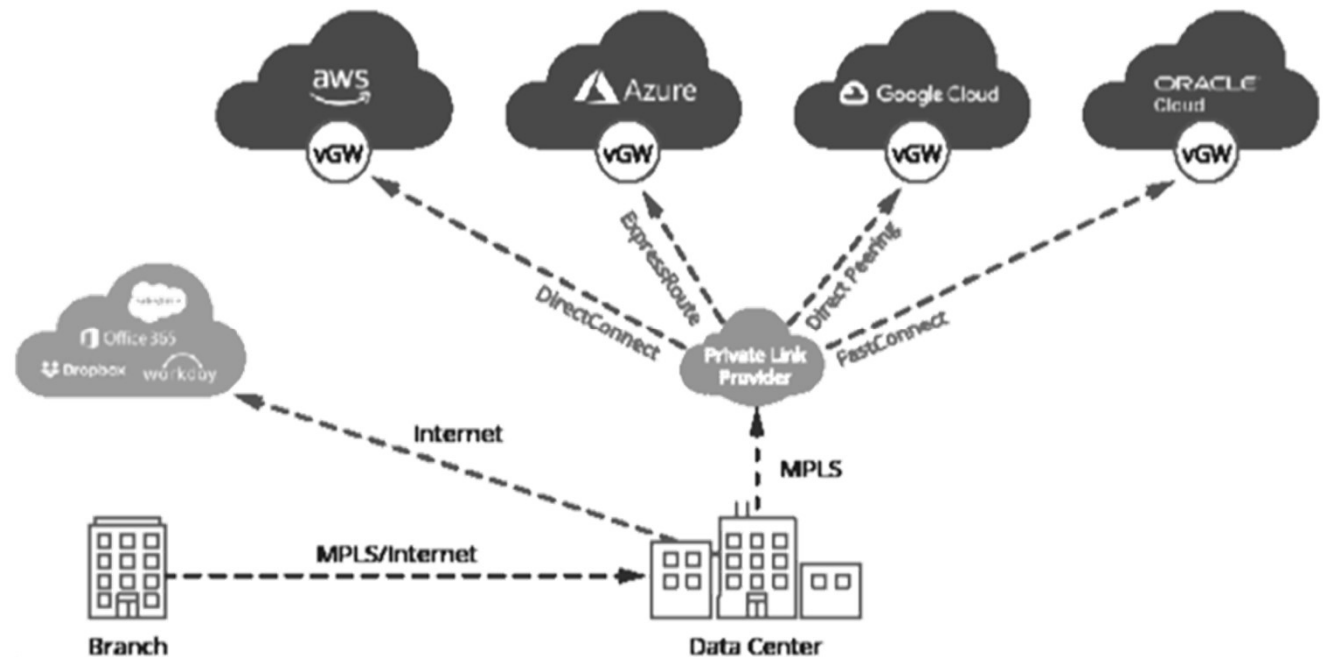
Source: <https://rancher.com/announcing-rancher-2-0/>



DAY 5. 멀티 클라우드 네트워킹

❖ Silver Peak: Direct Branch Multi-Cloud Connectivity

- Directed to cloud IaaS or SaaS providers using a private high-speed link on the backend such as Microsoft Azure ExpressRoute and Amazon AWS Direct Connect for IaaS services and MPLS or business-grade broadband for SaaS



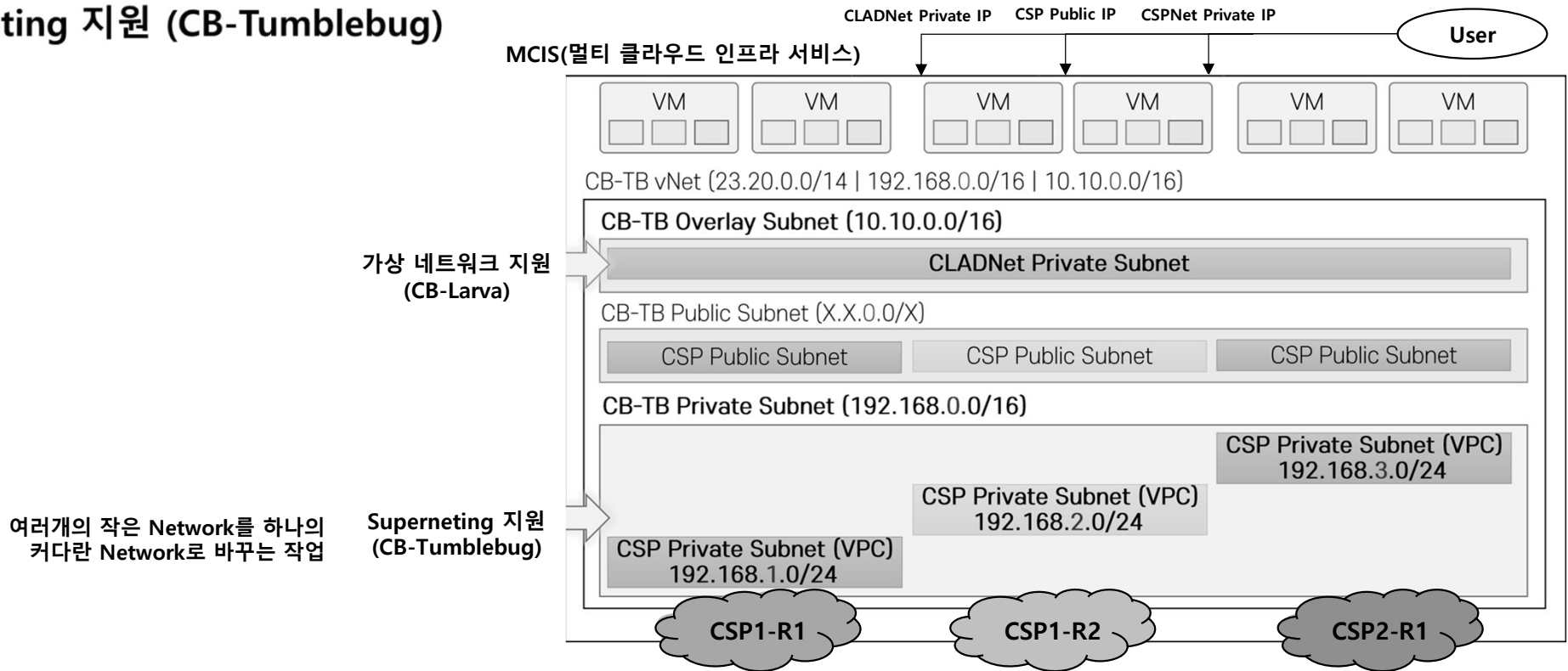
Source: <https://www.silver-peak.com/resource-center/use-cases/how-sd-wan-addresses-multi-cloud-connectivity-challenges>



DAY 5. 멀티 클라우드 네트워킹

❖ 오픈소스(예): MCIS(멀티 클라우드 인프라 서비스)

- 가상 네트워크 지원 (CB-Larva)
- Superneting 지원 (CB-Tumblebug)

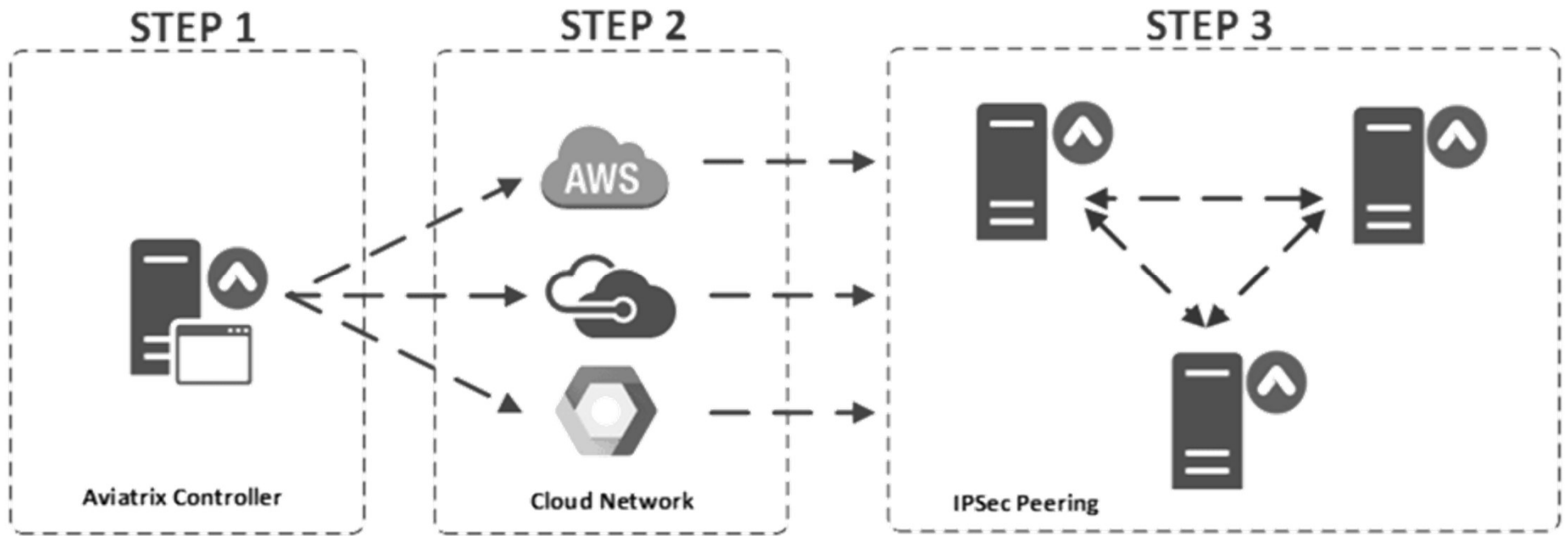


Source: @ ETRI Conference 2022 '멀티클라우드 가상네트워크 기술' (김윤곤) 참조



DAY 5. 멀티 클라우드 네트워킹

❖ Point and Click Networking with Aviatrix



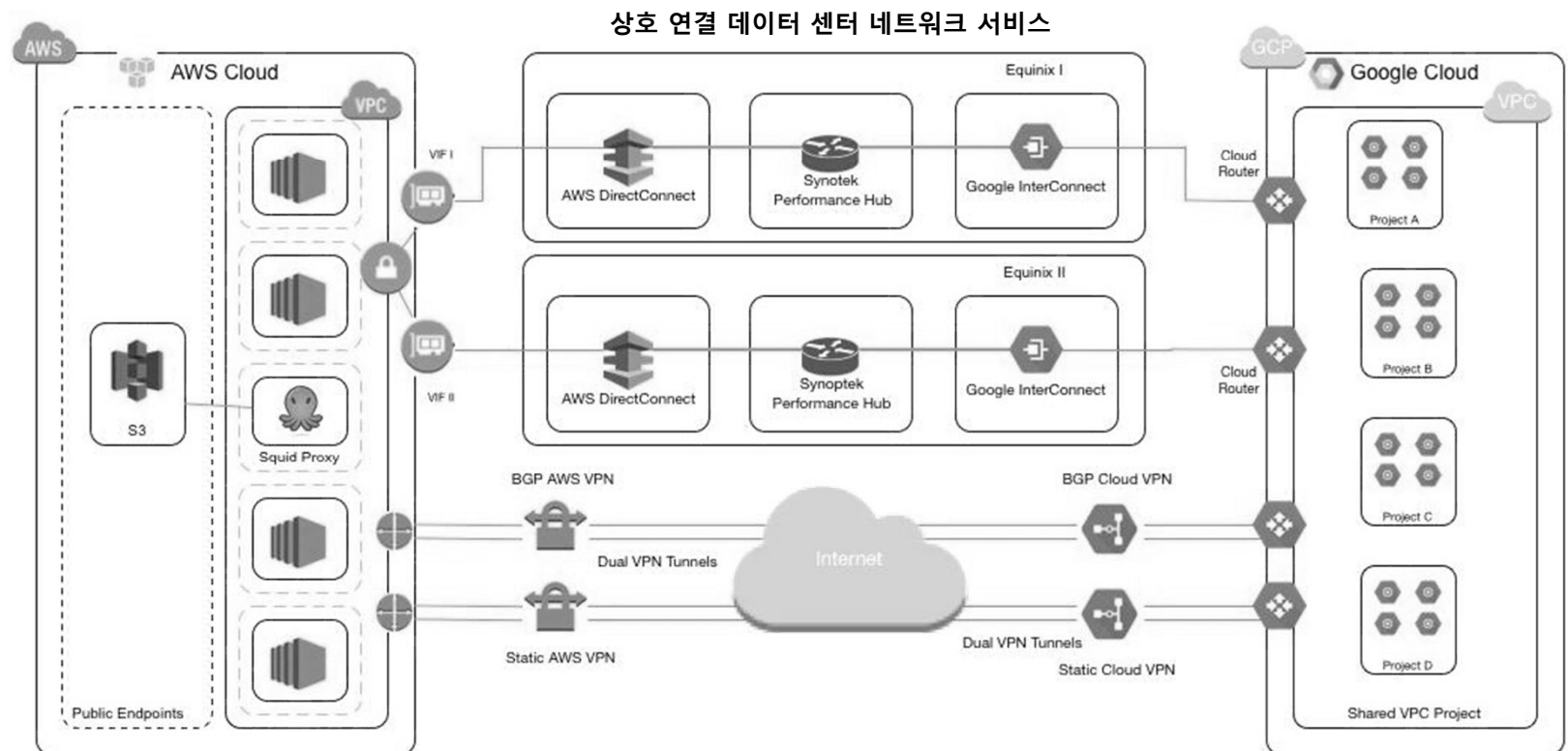
Source: <https://aviatrix.com/learn-center/answered-multi-cloud/how-to-do-multicloud-networking-abstraction-and-orchestration-across-aws-azure-and-google/>



DAY 5. 멀티 클라우드 네트워킹

❖ CSP 서비스

- Transit Gateway (클라우드 라우터)
- 전용선 및 허브
- VPN 터널링

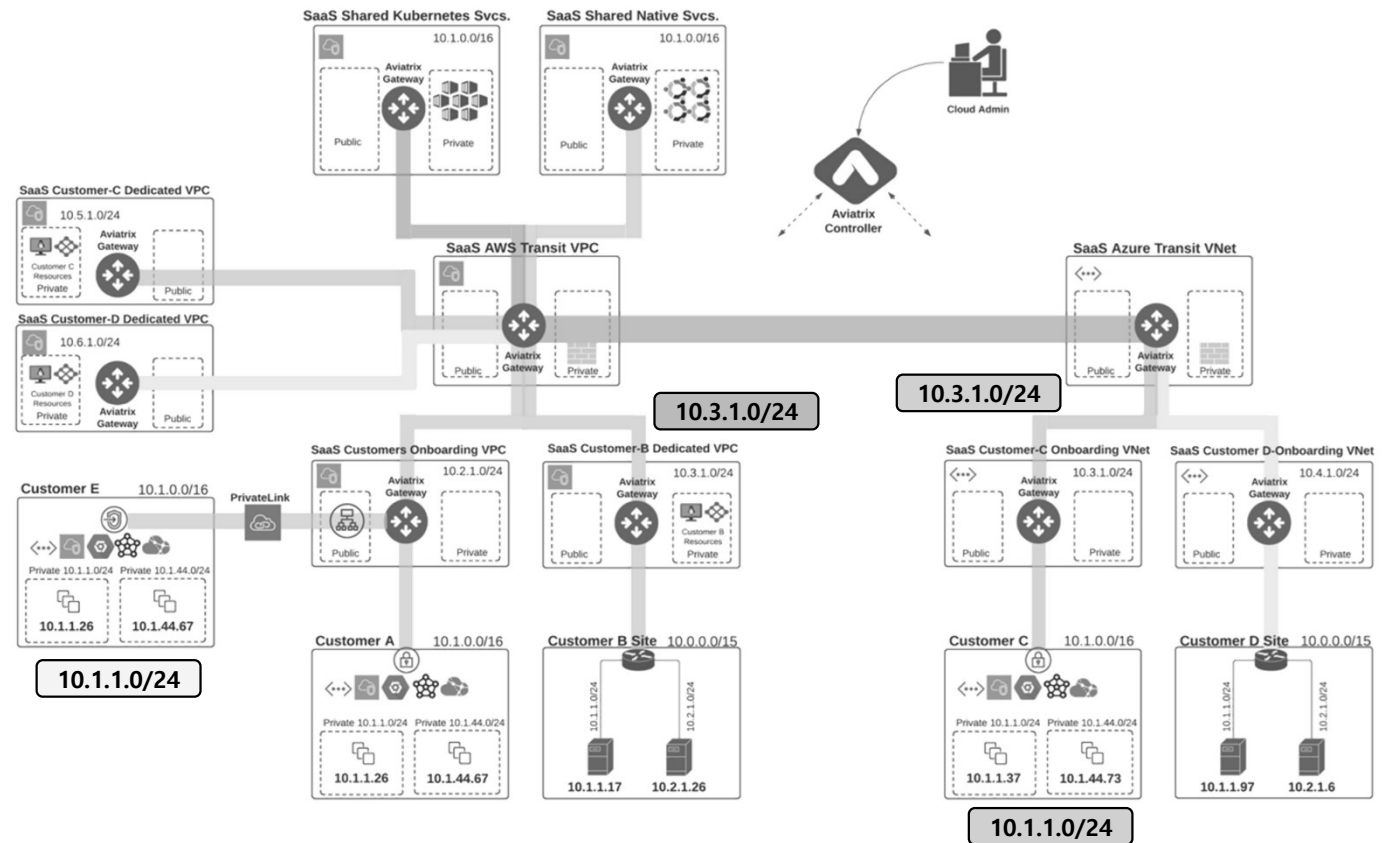


Source: @ ETRI Conference 2022 '멀티클라우드 가상네트워크 기술' (김윤곤) 참조



DAY 5. 멀티 클라우드 네트워킹

❖ 제조사 (예): Aviatrix의 SaaS 서비스

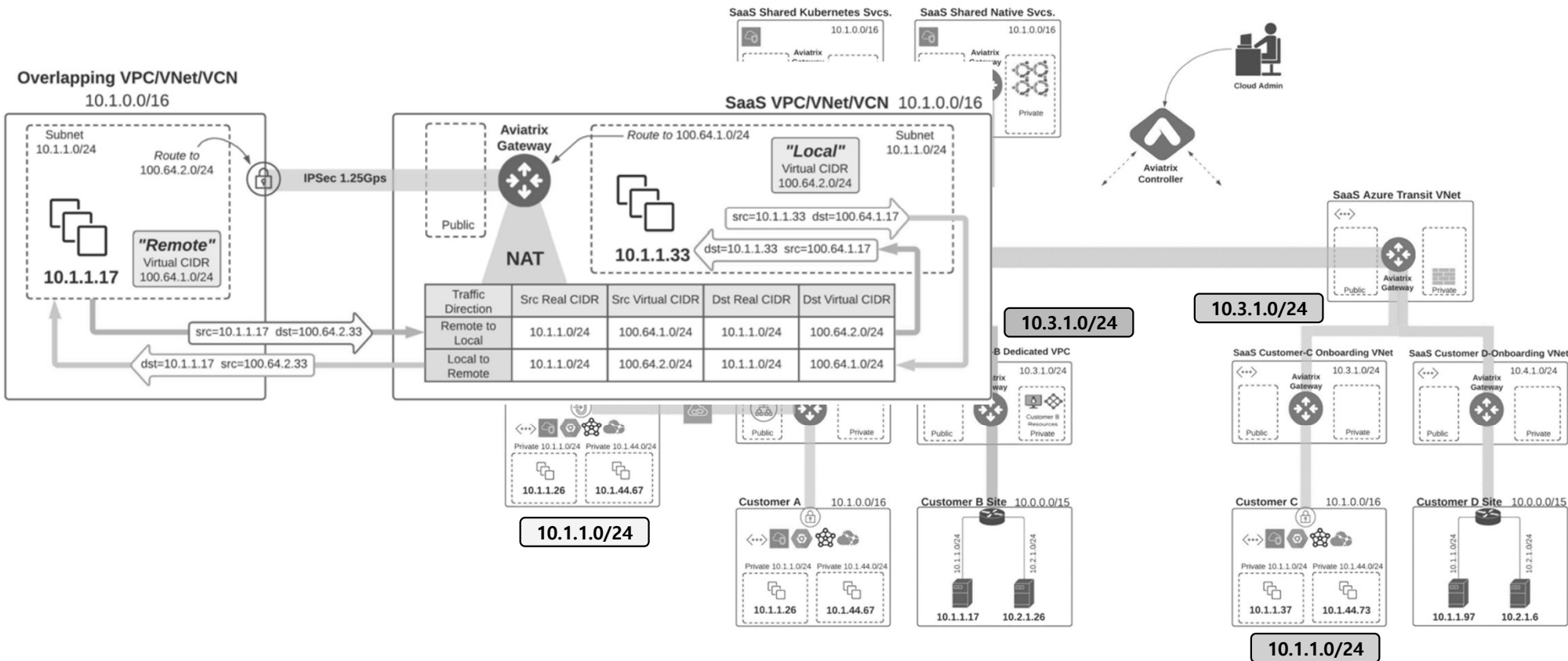


Source: <https://aviatrix.com/resources/design-guides/aviatrix-validated-design-saas-providers-infrastructure>



DAY 5. 멀티 클라우드 네트워킹

❖ 제조사 (예): Aviatrix의 SaaS 서비스

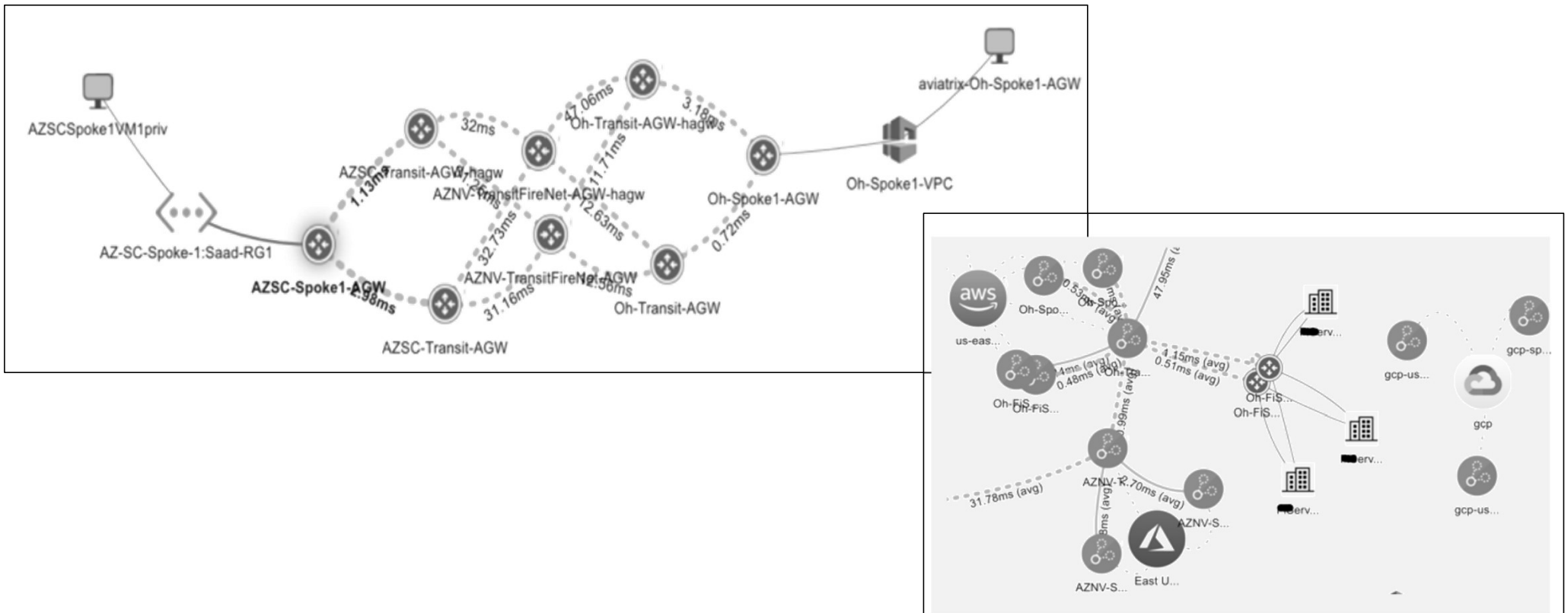


Source: <https://aviatrix.com/resources/design-guides/aviatrix-validated-design-saas-providers-infrastructure>



DAY 5. 멀티 클라우드 네트워크

❖ 제조사 (예): Aviatrix for Visibility and Troubleshooting

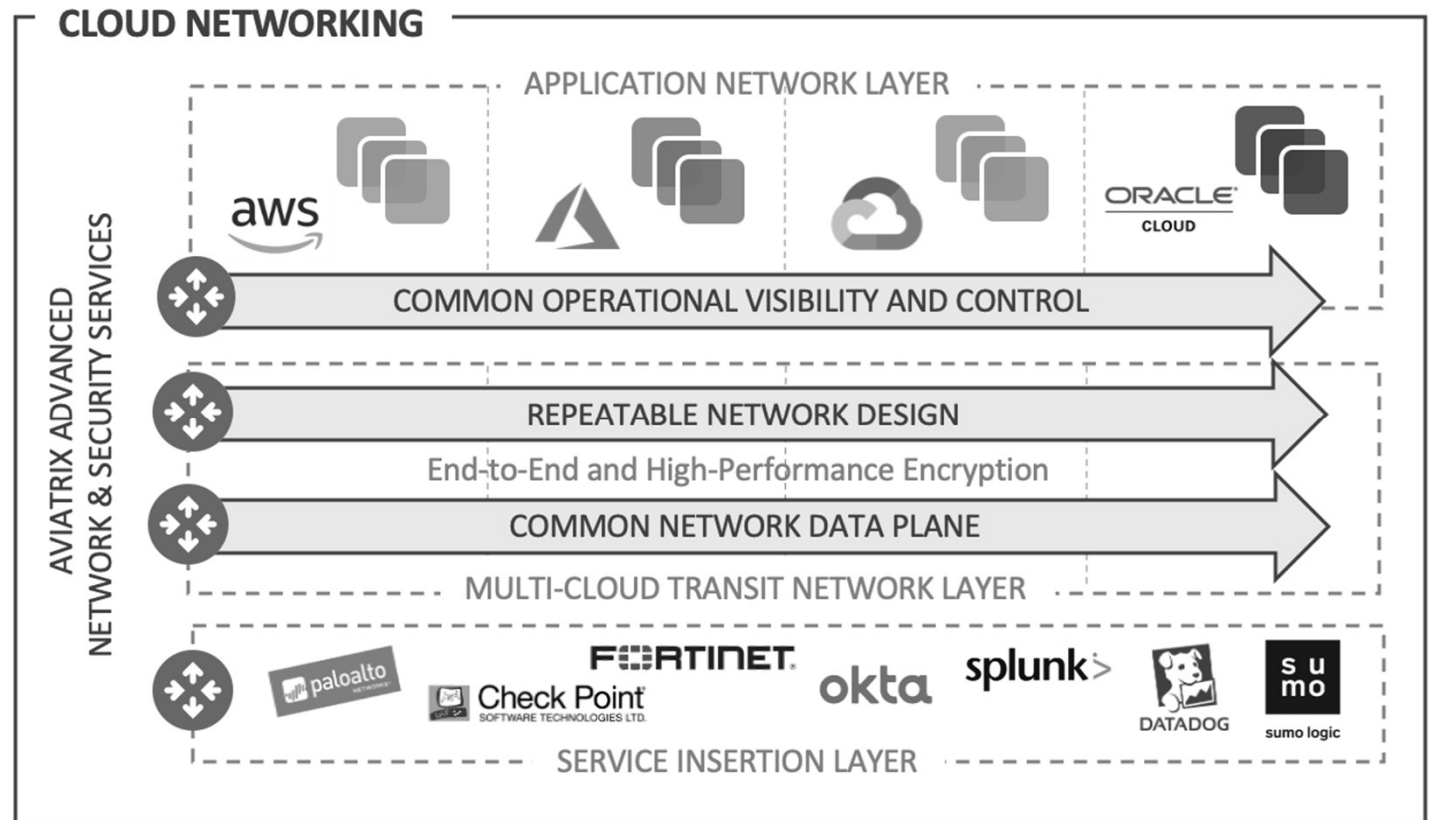


Source: <https://aviatrix.com/resources/design-guides/aviatrix-validated-design-saas-providers-infrastructure>



DAY 5. 멀티 클라우드 네트워킹

❖ from AWS networking to Multicloud Networking Software (MCNS) with Aviatrix



Source: <https://www.linkedin.com/pulse/reincarnation-from-aws-networking-multicloud-software-evgeny-vaganov>



DAY 5. 멀티 클라우드 네트워킹

❖ IAAS Networking Services across AWS, Azure, GCP

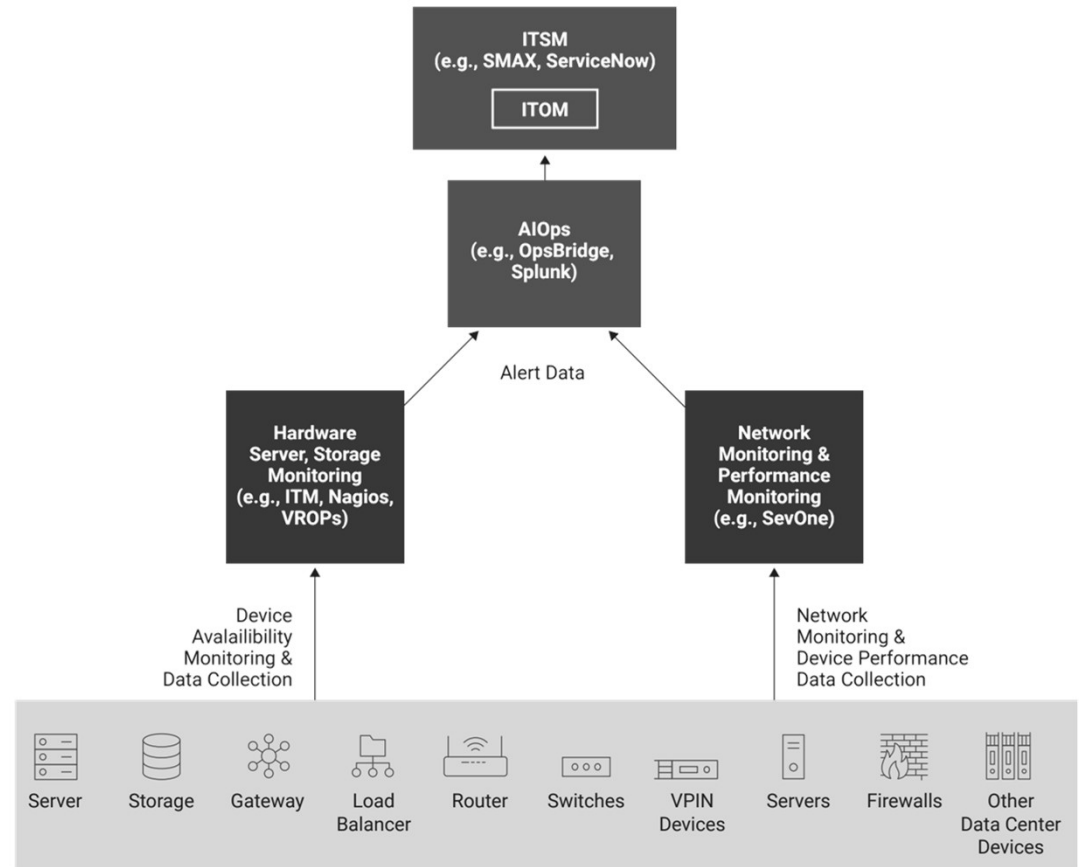
Network Services/Function	AWS	Azure	Google
Network Administration	Account	Subscription	Project
Virtual Network	VPC & Subnets	VNET & Subnet	VPC and Sub-Network
DNS	Route 53	Traffic Manager	Cloud DNS
VPN	VGW	VPN Gateway	VPN Gateway
Peering	AWS Peering or DirectConnect	Azure Peering or ExpressRoute	Google Cloud Interconnect
Load Balancer	ELB	NLB	Cloud Load Balancer
Security	Sec Groups	Network Security Groups	Network ACLs
Storage	S3	Blob Storage	Cloud Storage
Notifications	SNS	Notification hubs	Cloud Messaging
Messaging	SQS	Batch	Pub/Stub
Logging	CloudTrail	Operational Insights	Cloud Logging
Monitoring	CloudWatch	Application Insights	Cloud Monitoring

Source: <https://aviatrix.com/learn-center/answered-multi-cloud/how-to-do-multicloud-networking-abstraction-and-orchestration-across-aws-azure-and-google/>



DAY 5. 멀티 클라우드 네트워킹

❖ Monitoring with AIOps

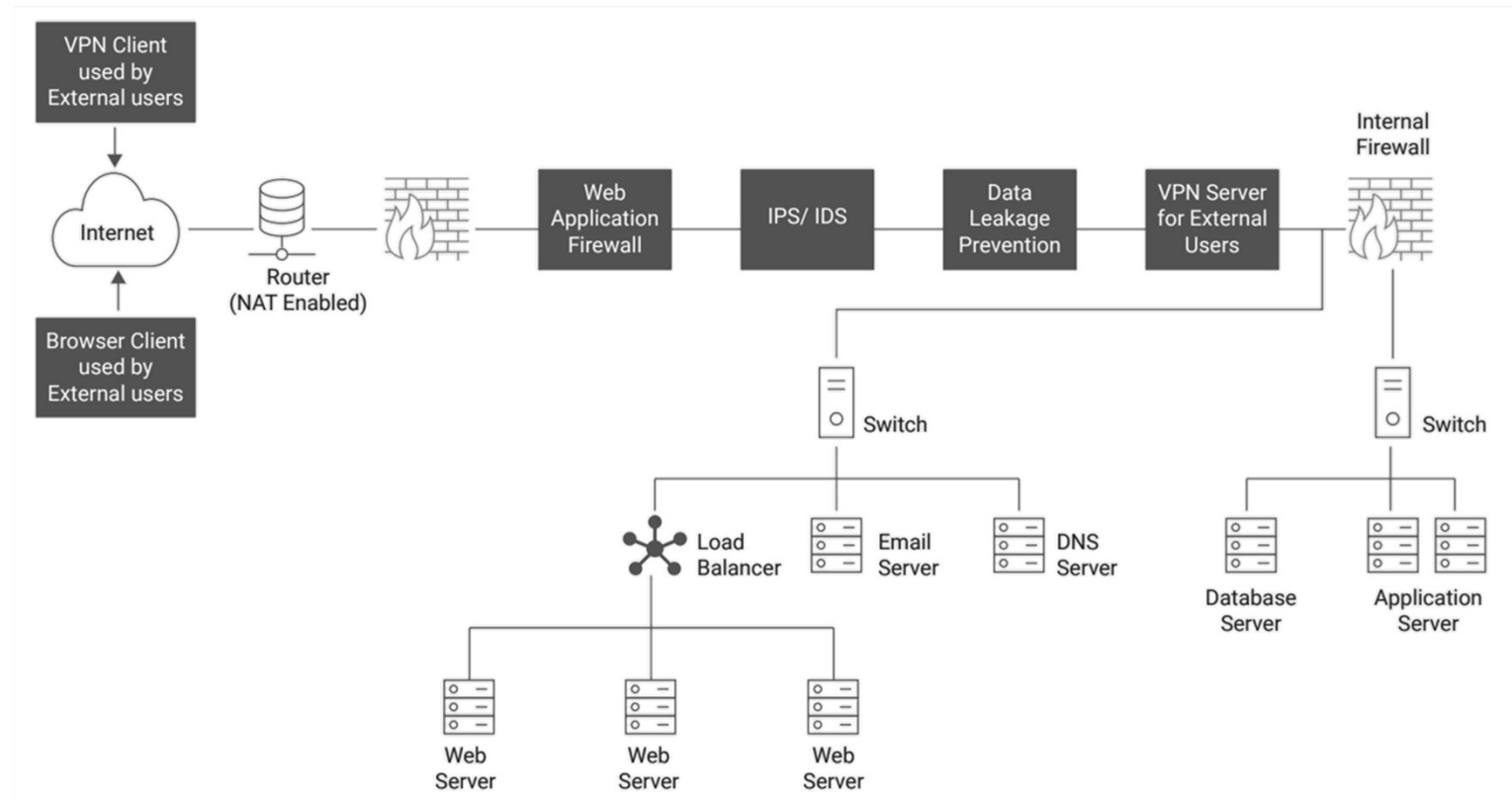


Source: Infrastructure Architecture Essentials for Data Center and Cloud, Shankar Kambhampaty



DAY 5. 멀티 클라우드 네트워킹

❖ Connectivity Security

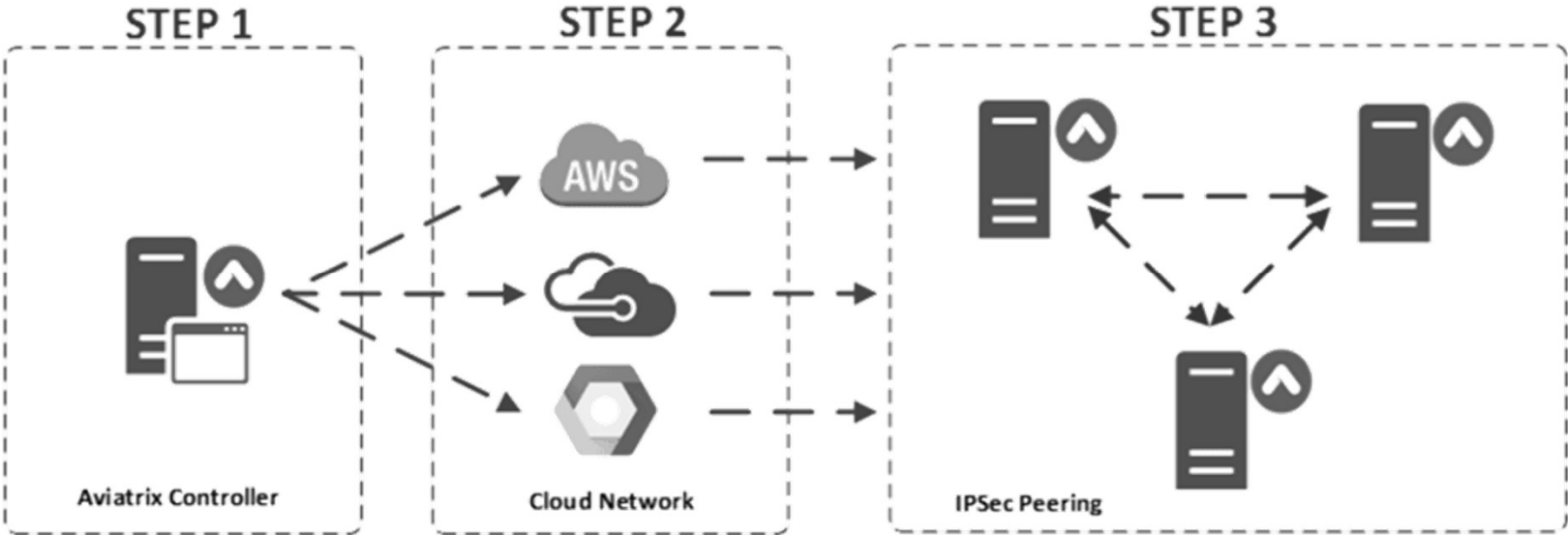


Source: Infrastructure Architecture Essentials for Data Center and Cloud, Shankar Kambhampaty



DAY 5. 멀티 클라우드 네트워킹

- ❖ Point and Click connect VPCs and VNETs across multiple clouds.
 - Point and Click Networking with Aviatrix



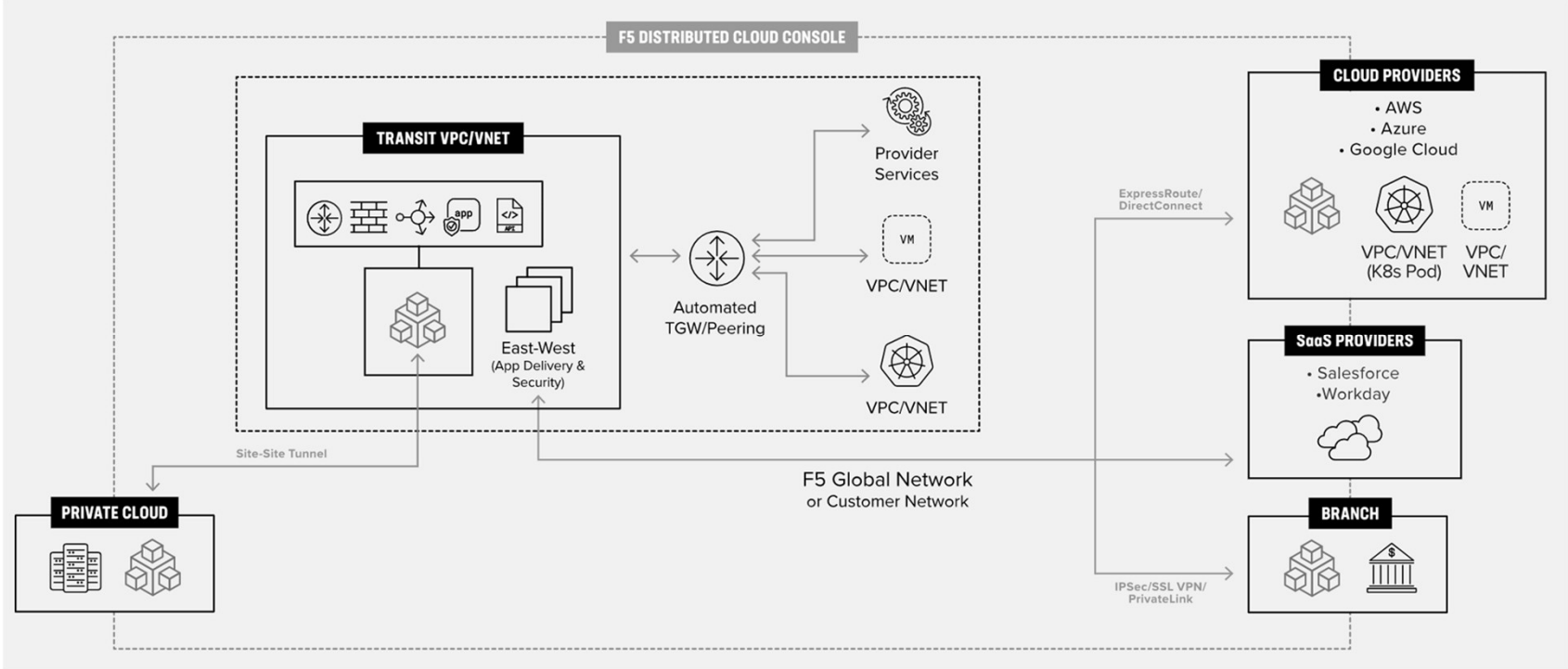
Source: <https://aviatrix.com/learn-center/answered-multi-cloud/how-to-do-multicloud-networking-abstraction-and-orchestration-across-aws-azure-and-google/>



DAY 5. 멀티 클라우드 네트워킹

❖ 자동화를 위한 소프트웨어 정의 네트워크(SDN) 기술 확장

- Deliver seamless secure networking across clouds



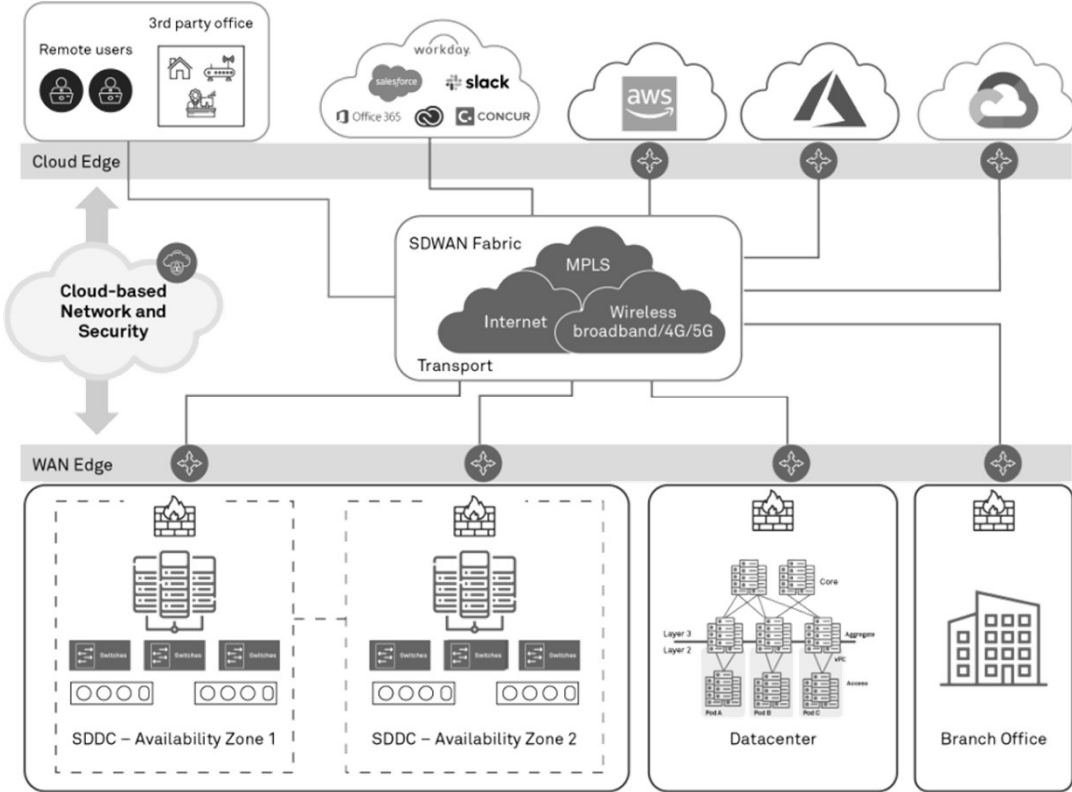
Source: <https://www.f5.com/cloud/use-cases/multi-cloud-networking>



DAY 5. 멀티 클라우드 네트워킹

❖ The Strategy to Build Secure Multi-cloud Networking

- 언더레이(Underlay) SDN



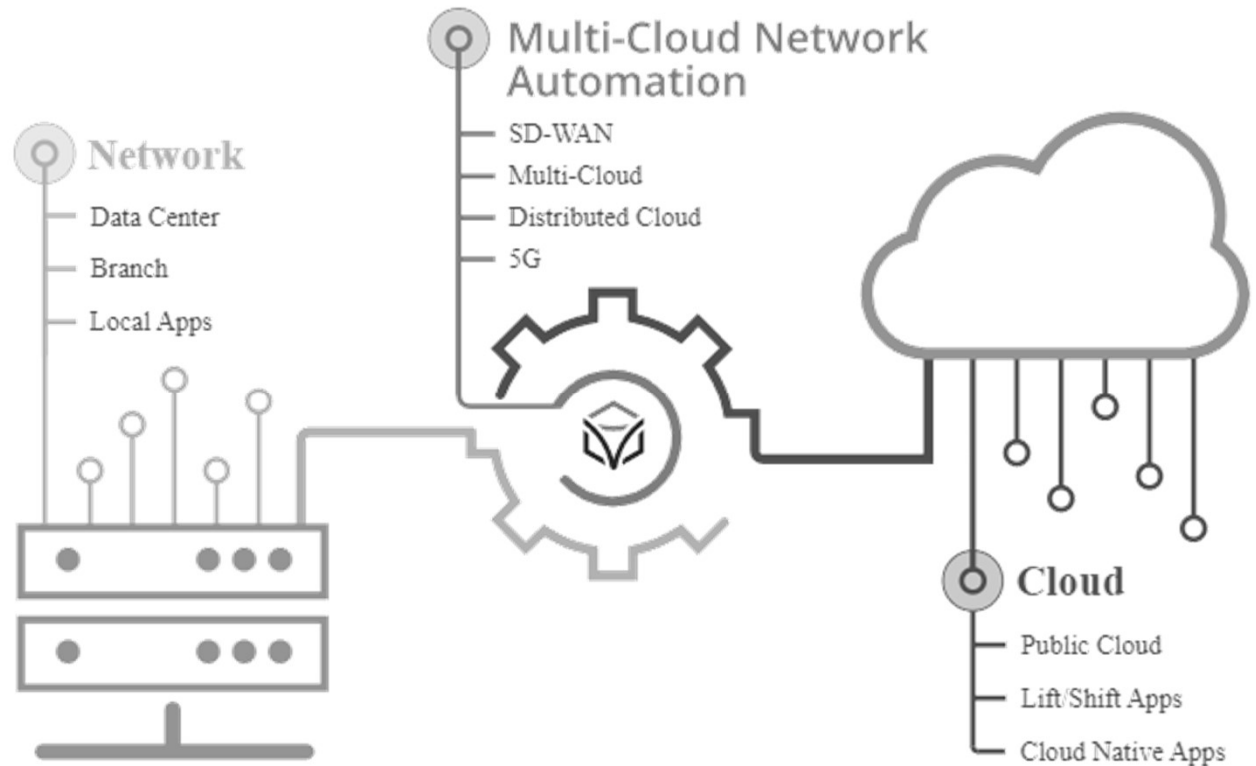
Source: <https://www.wipro.com/infrastructure/the-strategy-to-build-secure-multi-cloud-networking/>



DAY 5. 멀티 클라우드 네트워킹

❖ Automating Multi-Cloud Networking

- 언더레이(Underlay) SDN



Source: <https://www.itential.com/network-automation-use-cases-2/multi-cloud-network-automation/>



DAY 5. 멀티 클라우드 네트워킹

❖ Distributed Cloud / Multi Cloud

• 언더레이(Underlay) SDN

DevOps

- **Consistent Environment**
- Auto Scale Across Env

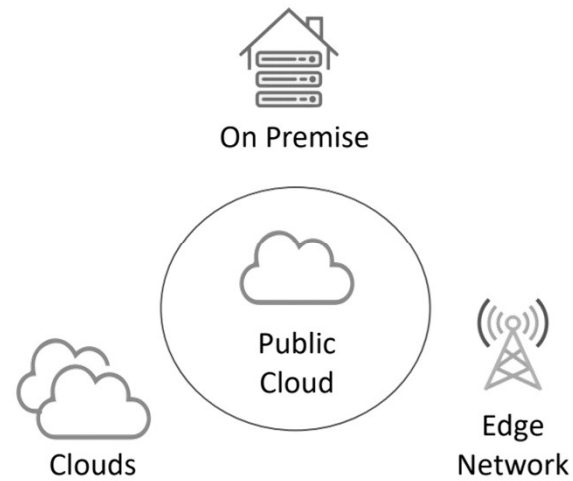


DevOps

- **Innovation**
- AI/ML Across All Environment

DevSecOps

- **Governance**
- Security Policies
- Network Policies



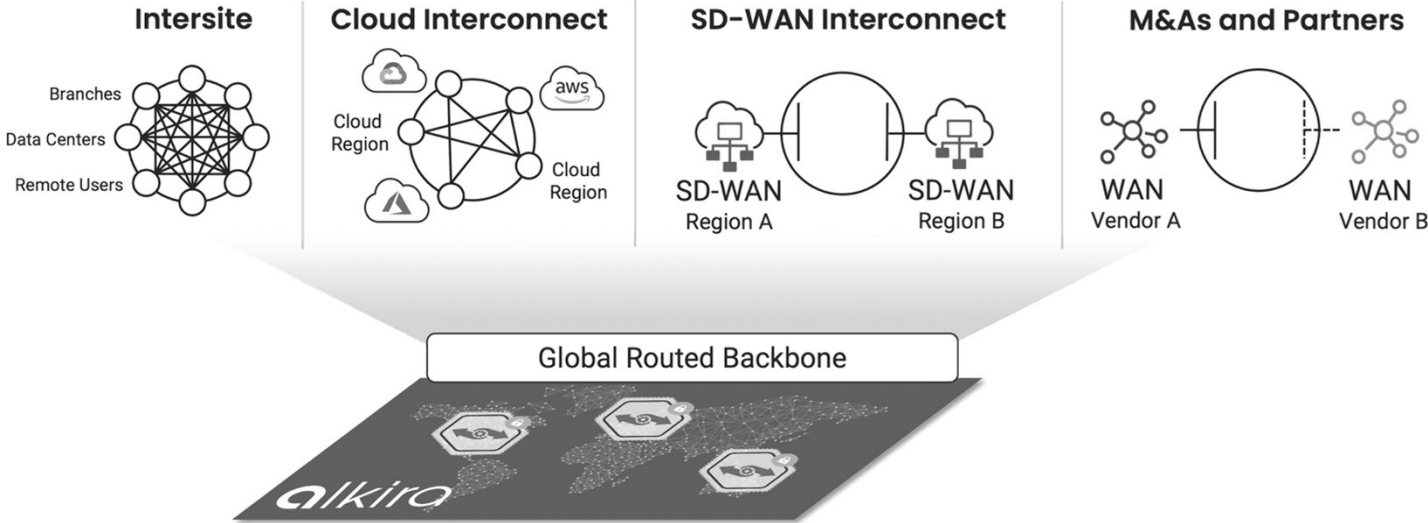
Source: <https://speakerdeck.com/arafkarsh/cloud-architecture-multi-cloud-edge-on-premise?slide=54>



DAY 5. 멀티 클라우드 네트워킹

❖ Alkira Cloud Backbone

- Tying together data centers, branches, campus locations and remote users
- Cloud interconnect
- Interconnect for SD-WAN islands from the same vendor or different vendors
- Network integration to support mergers and acquisitions or to onboard partners.



Source: <https://www.alkira.com/multi-cloud-networking-reinvented-cto-whitepaper/>



DAY 5. 멀티 클라우드 네트워킹

❖ Multy vs Terraform

• Example

Multy

```
resource "multy_virtual_network" "multy_vn" {
  name = "multy-vn"
  cidr_block = "10.0.0.0/16"
  location = "eu_west_1"
  cloud = "aws" # or "azure"
}
```

Terraform - AWS

```
resource "aws_vpc" "aws_vn" {
  tags = {
    "Name" = "multy-vn"
  }
  cidr_block = "10.0.0.0/16"
}
```

Terraform - Azure

```
resource "azurerm_resource_group" "vn-rg" {
  name = "vn-rg"
  location = "ukwest"
}

resource "azurerm_virtual_network" "azure_vn" {
  resource_group_name = azurerm_resource_group.vn-rg.name
  name = "multy-vn"
  location = "ukwest"
  address_space = ["10.0.0.0/16"]
}
```

Terraform - GCP

```
resource "google_compute_network" "gcp_vn" {
  name = "multy-vn"
  routing_mode = "REGIONAL"
  auto_create_subnetworks = false
  delete_default_routes_on_create = true
}
```

Source: <https://docs.multy.dev/comparison/terraform>

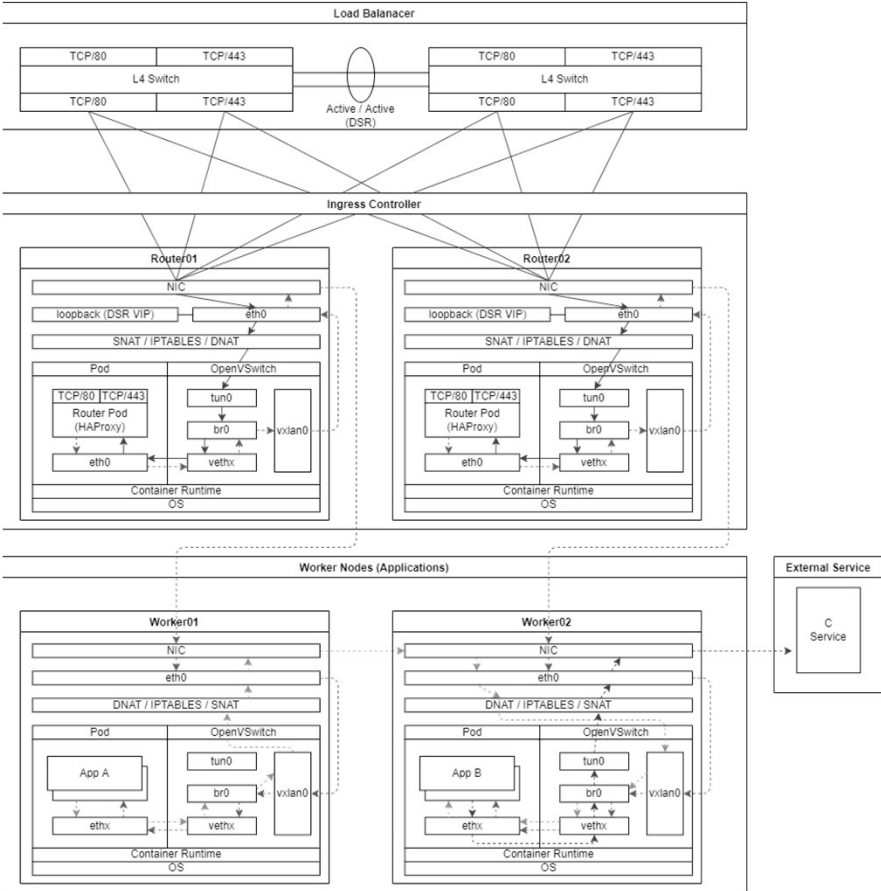


DAY 5. 멀티 클라우드 네트워킹

❖ OpenShift - 네트워크 흐름도 및 이슈 분석

• OpenShift 네트워크 흐름도

➢ 서로 다른 노드간 통신



Source: https://gist.github.com/ruo91/0ebc8f14e8b294794efb4ef2609b6aee?fbclid=IwAR0XrRO_7lpqkP2iKmCyTvtuzsGI3AQMWggPUxiIEQYJiri82iHBF_JDPBE

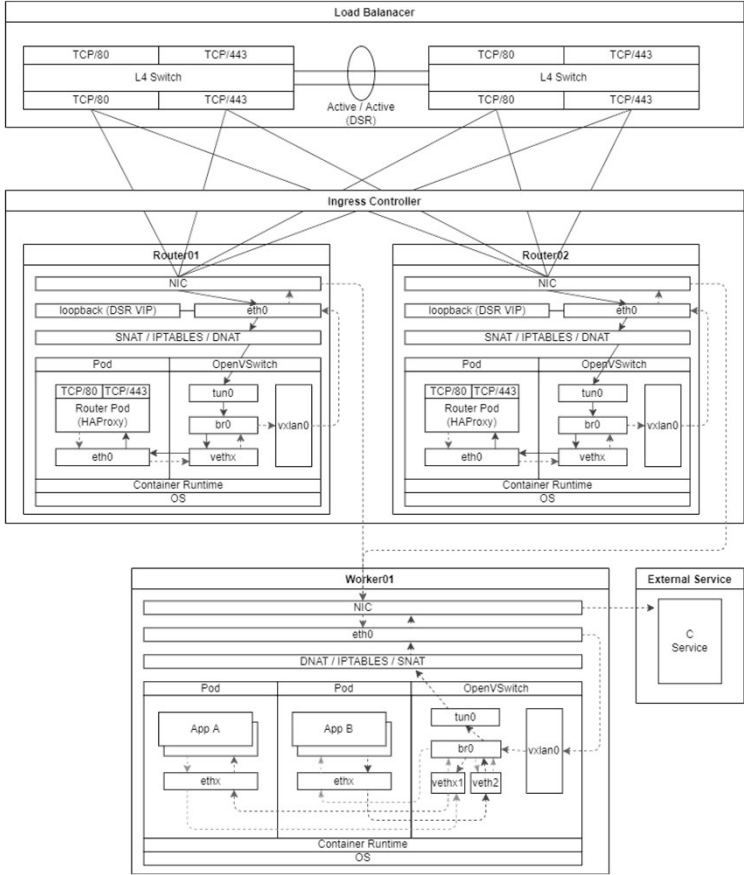


DAY 5. 멀티 클라우드 네트워킹

❖ OpenShift - 네트워크 흐름도 및 이슈 분석

• OpenShift 네트워크 흐름도

➢ 같은 노드간 통신

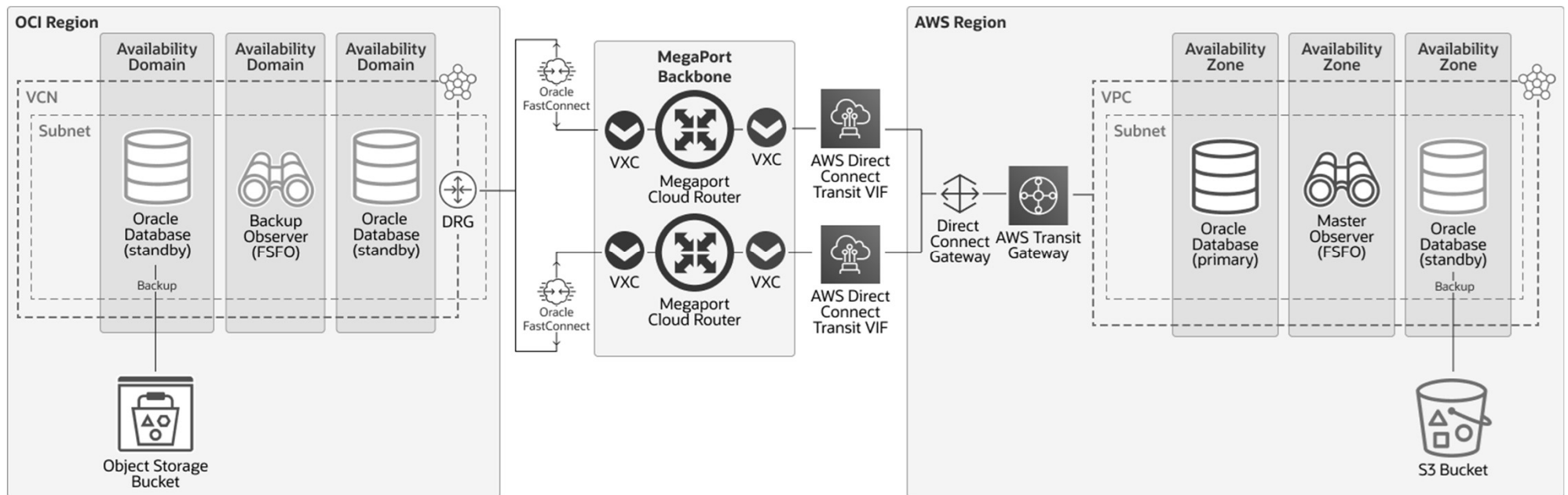


Source: https://gist.github.com/ruo91/0ebc8f14e8b294794efb4ef2609b6aee?fbclid=IwAR0XrRO_7lpqkP2iKmCyTvtuzsGI3AQMWggPUxilEQYJiri82iHBF_JDPBE



DAY 5. 멀티 클라우드 네트워킹

❖ Multi-Cloud high availability and data protection across OCI and AWS with Megaport

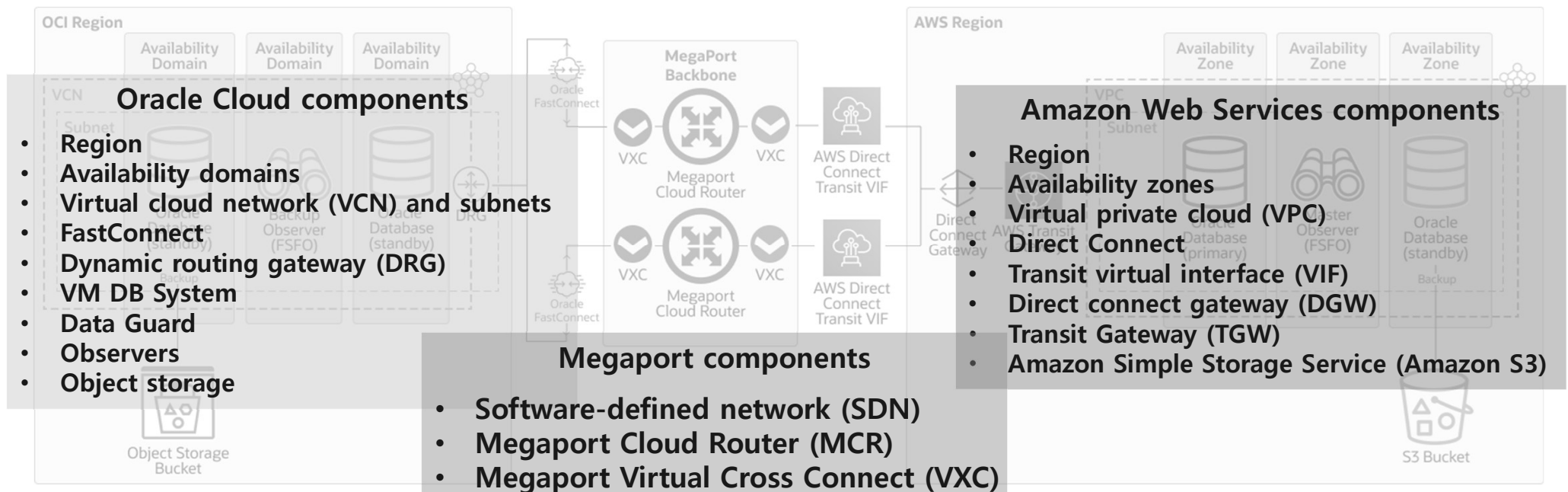


Source: <https://docs.oracle.com/en/solutions/multicloud-failover-oci-aws/index.html#GUID-A7E1BF80-4489-4DD5-8D6F-B4DE38F88BE2>



DAY 5. 멀티 클라우드 네트워킹

❖ Multi-Cloud high availability and data protection across OCI and AWS with Megaport

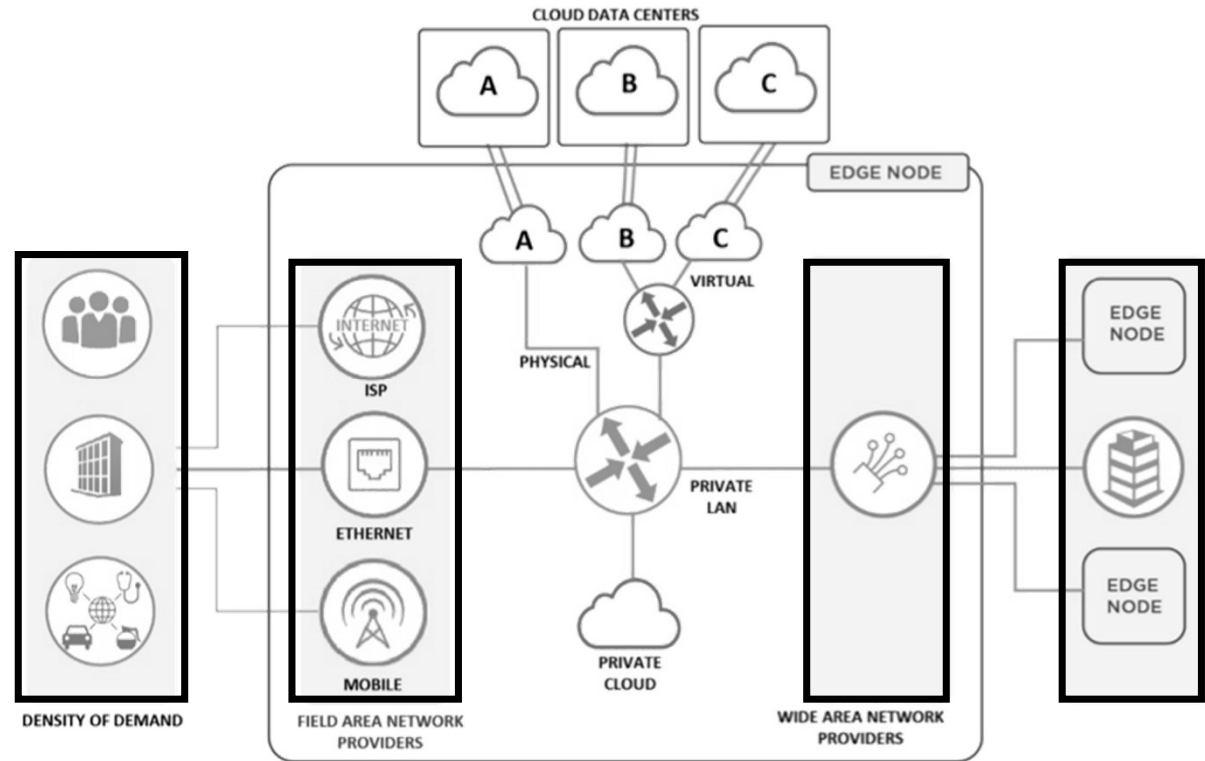


Source: <https://docs.oracle.com/en/solutions/multicloud-failover-oci-aws/index.html#GUID-A7E1BF80-4489-4DD5-8D6F-B4DE38F88BE2>



DAY 5. 멀티 클라우드 네트워킹

❖ Connect to Multiple Clouds at the Digital Edge

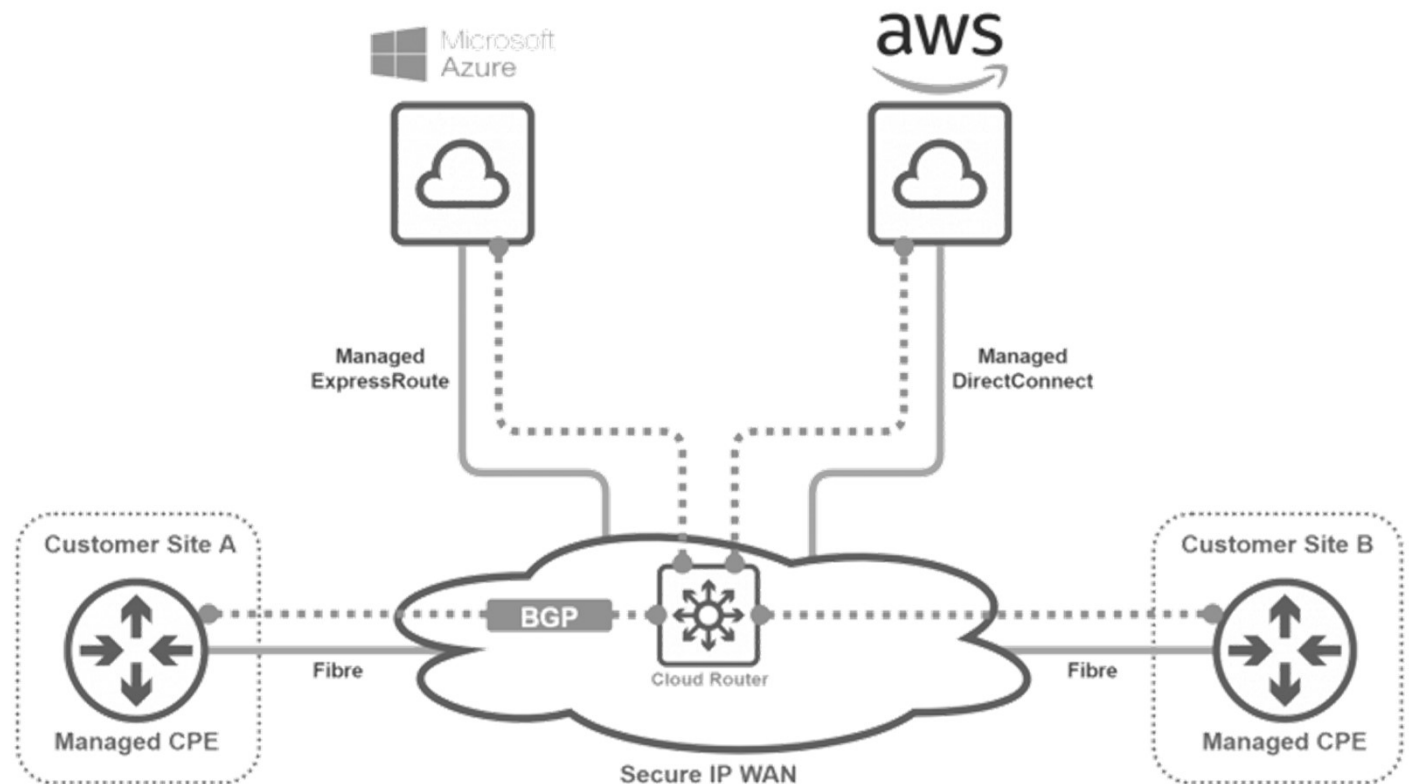


Source: <https://blog.equinix.com/blog/2017/05/24/optimizing-multicloud-interconnection-at-the-digital-edge/>



DAY 5. 멀티 클라우드 네트워킹

- ❖ Multi-Cloud connectivity platform for customers looking to connect to multiple Private Cloud providers.

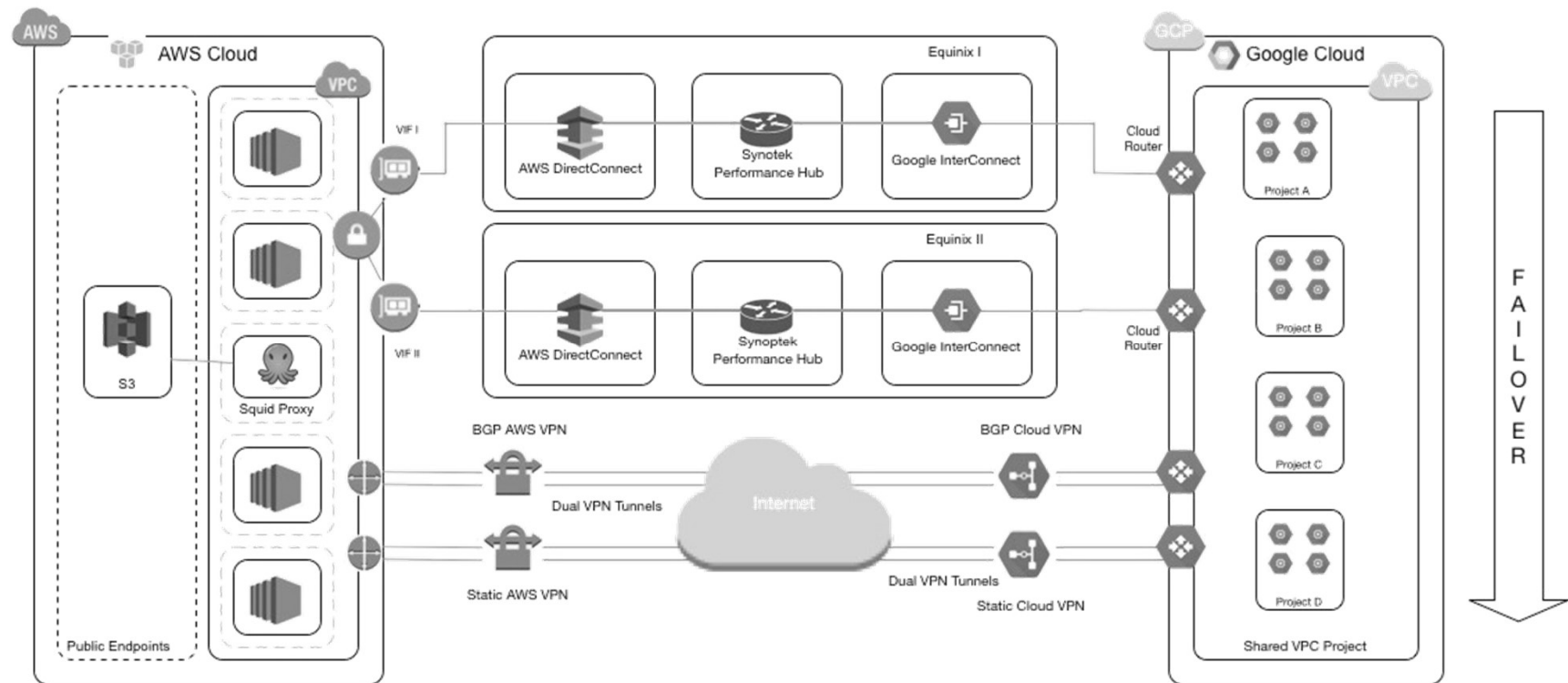


Source: <https://www.netsg.co/dc-cloud/cloud-and-dc-interconnect/>



DAY 5. 멀티 클라우드 네트워킹

❖ Behind the Scenes of our Transition to a Multi-Cloud Environment







Source: <https://metamarkets.com/2017/behind-the-scenes-of-our-transition-to-a-multi-cloud-environment/>



DAY 5. 멀티 클라우드 네트워킹

❖ Multi-Cloud Challenges

- Different Cloud Service Providers Have Different APIs

	Static		Dynamic			
	DEDICATED		PRIVATE CLOUD	AWS	AZURE	GCP
 Run Deployment	vSphere	→	vSphere	EKS / ECS Lambda	AKS / ACS Azure Functions	GKE Cloud Functions
 Connect Networking	Hardware	→	Various Hardware	CloudMap AppMesh	Proprietary	Google Istio
 Secure Security	IP: Hardware	→	Identity: AD/LDAP	Identity: AWS IAM	Identity: Azure AD	Identity: GCP IAM
 Provision Operations	vCenter	→	Terraform	CloudFormation	Resource Manager	Cloud Deployment Manager

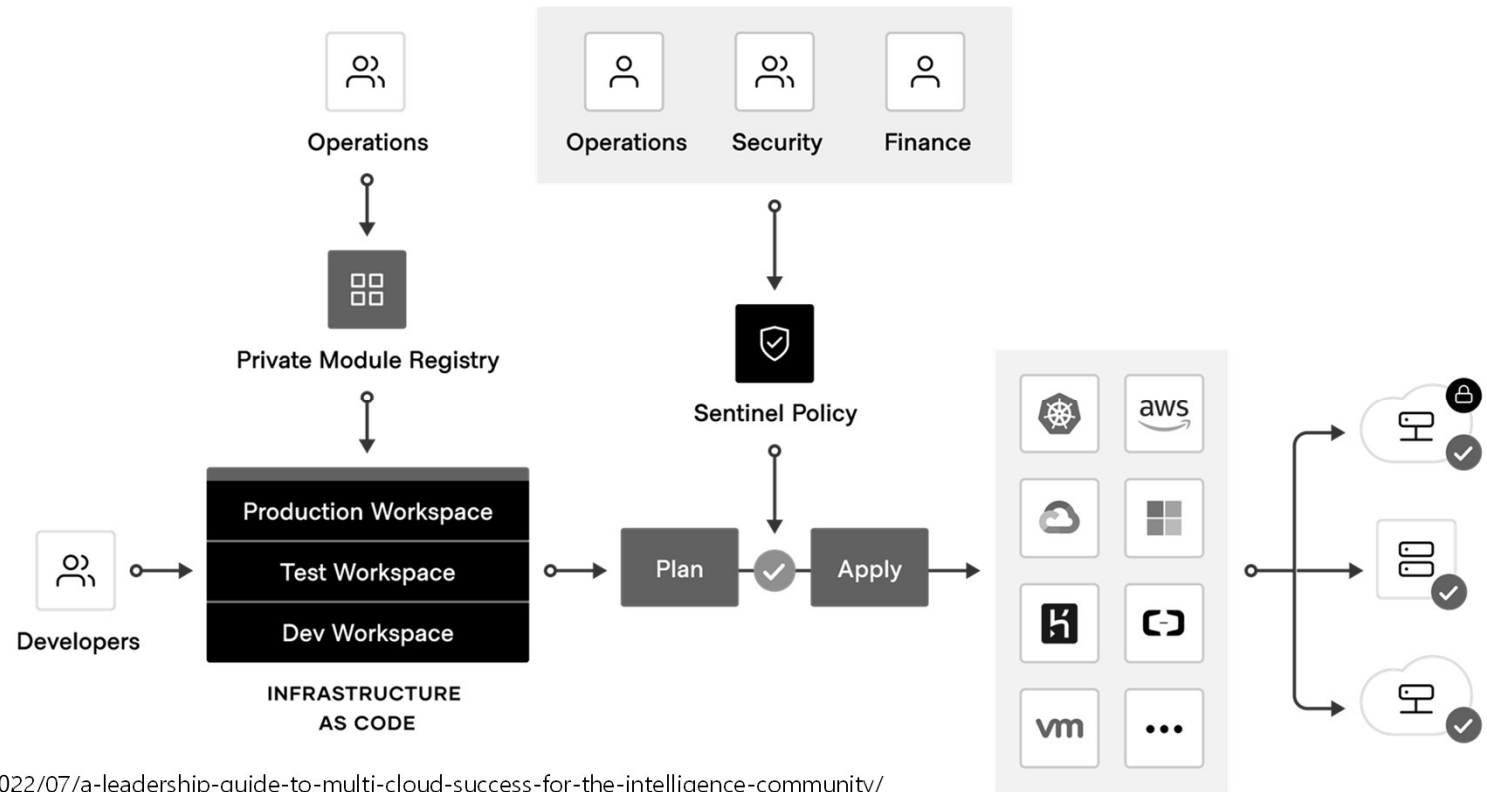
Source: <https://wtop.com/sponsored-content/2022/07/a-leadership-guide-to-multi-cloud-success-for-the-intelligence-community/>



DAY 5. 멀티 클라우드 네트워킹

❖ Multi-Cloud Challenges

- Infrastructure Provisioning with Terraform

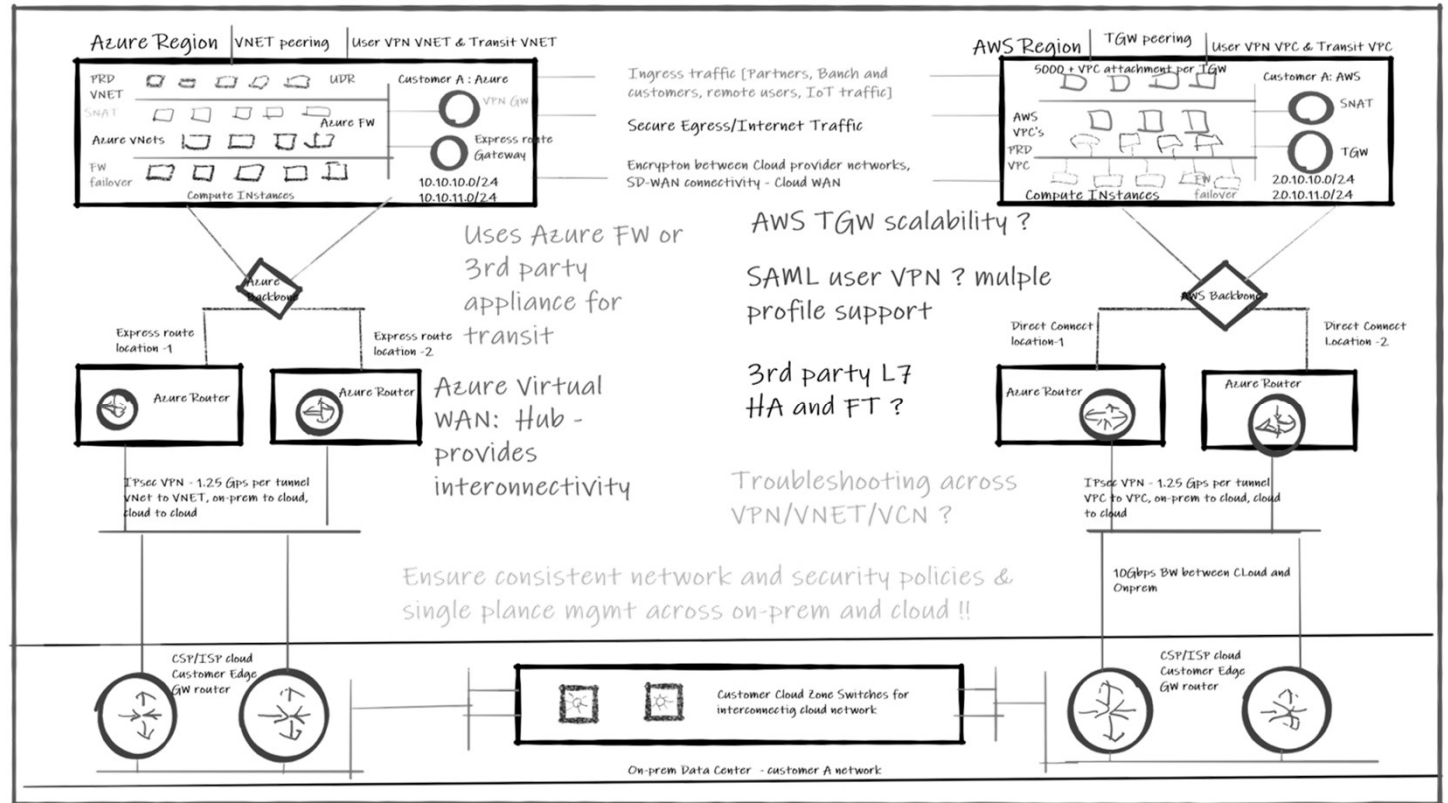


Source: <https://wtop.com/sponsored-content/2022/07/a-leadership-guide-to-multi-cloud-success-for-the-intelligence-community/>



DAY 5. 멀티 클라우드 네트워킹

❖ Multi-cloud Networking and Security Challenges



Source: <https://www.networkbachelor.com/multi-cloud-networking-and-security-challenges/>



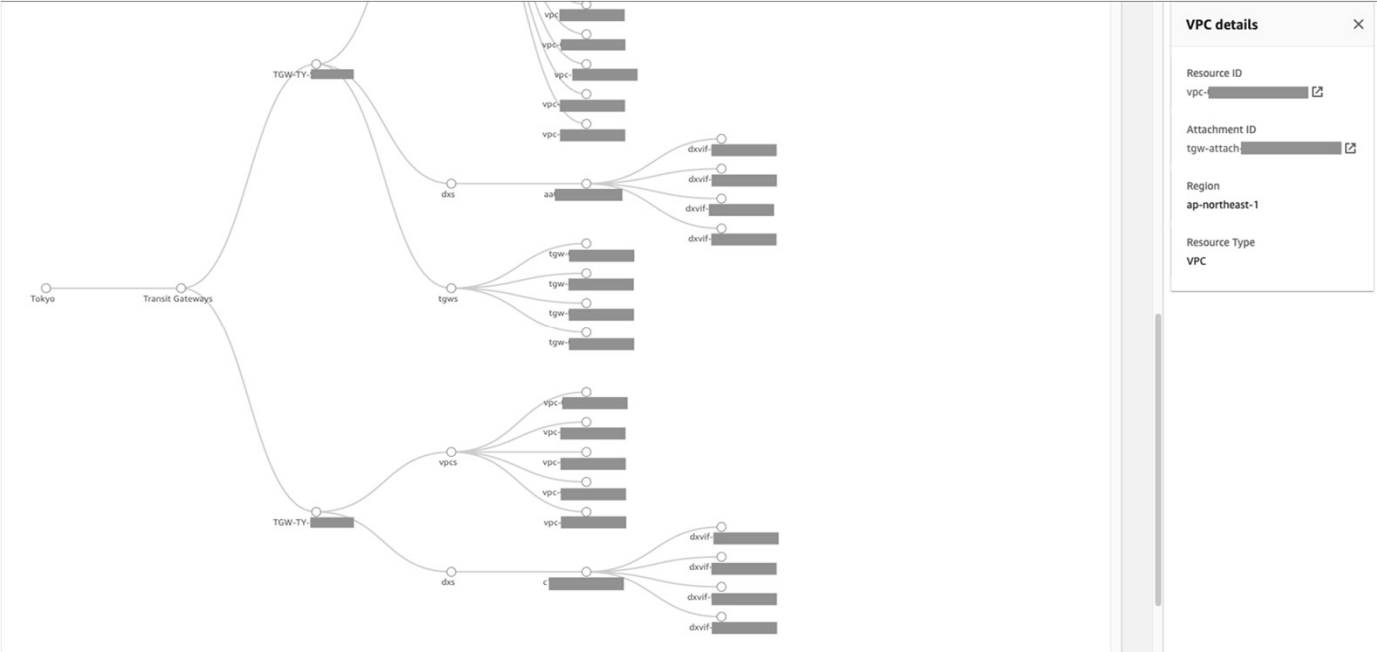
DAY 5. 멀티 클라우드 네트워킹

❖ Enhanced Management of Multi-cloud Networking and Security

- Business Model Nowadays

- What Are The Absences
- How To Efficiently Operate Your Clouds
 - ✓ Global Transit Network
 - ✓ FireNet
 - ✓ Egress FQDN Filtering
 - ✓ Observability

- Conclusion



Source: <https://hackmd.io/@terrencec51229/outline/%2FKF8s-B9kQwuAqub7ZheBFQ>



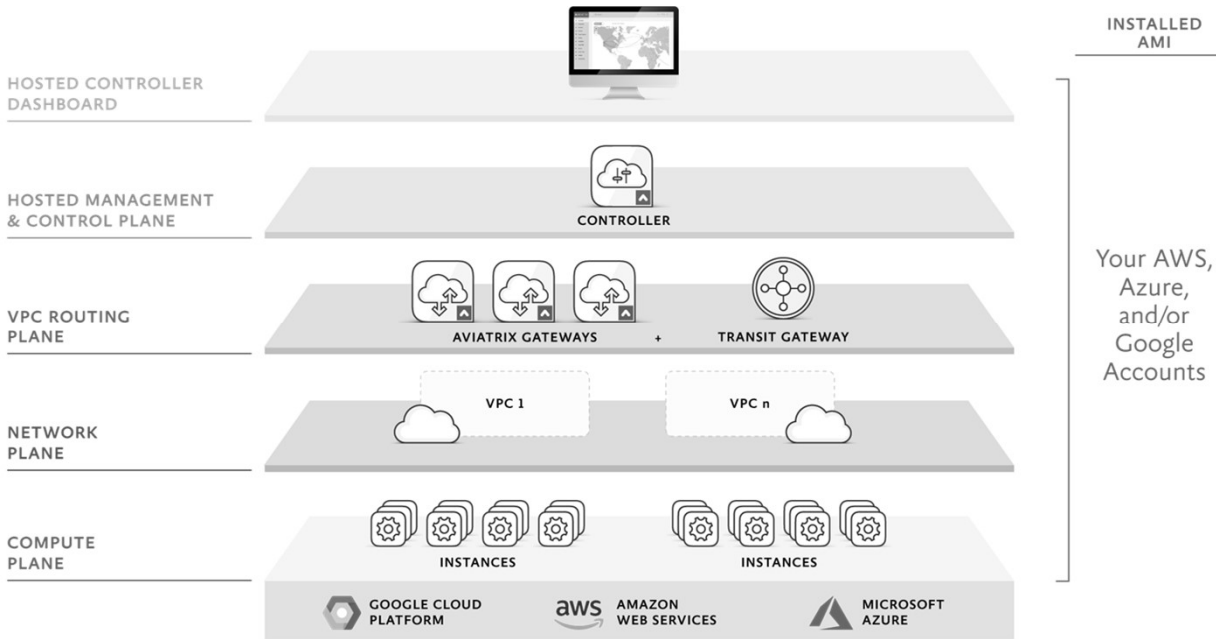
DAY 5. 멀티 클라우드 네트워킹

❖ Enhanced Management of Multi-cloud Networking and Security

• Business Model Nowadays

- What Are The Absences
- How To Efficiently Operate Your Clouds
 - ✓ Global Transit Network
 - ✓ FireNet
 - ✓ Egress FQDN Filtering
 - ✓ Observability

➤ Conclusion



Source: <https://hackmd.io/@terrencec51229/outline/%2FKF8s-B9kQwuAqub7ZheBFQ>



DAY 5. 멀티 클라우드 네트워킹

❖ Enhanced Management of Multi-cloud Networking and Security

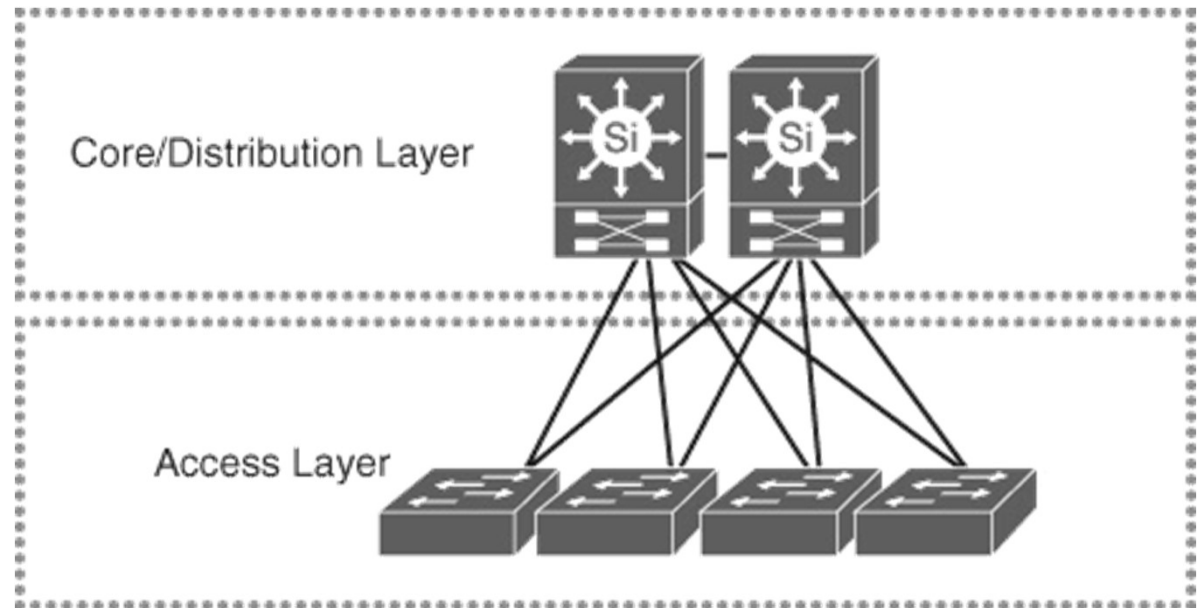
• Business Model Nowadays

➤ What Are The Absences

➤ How To Efficiently Operate Your Clouds

- ✓ Global Transit Network
- ✓ FireNet
- ✓ Egress FQDN Filtering
- ✓ Observability

➤ Conclusion



Source: <https://hackmd.io/@terrencec51229/outline/%2FKF8s-B9kQwuAqub7ZheBFQ>

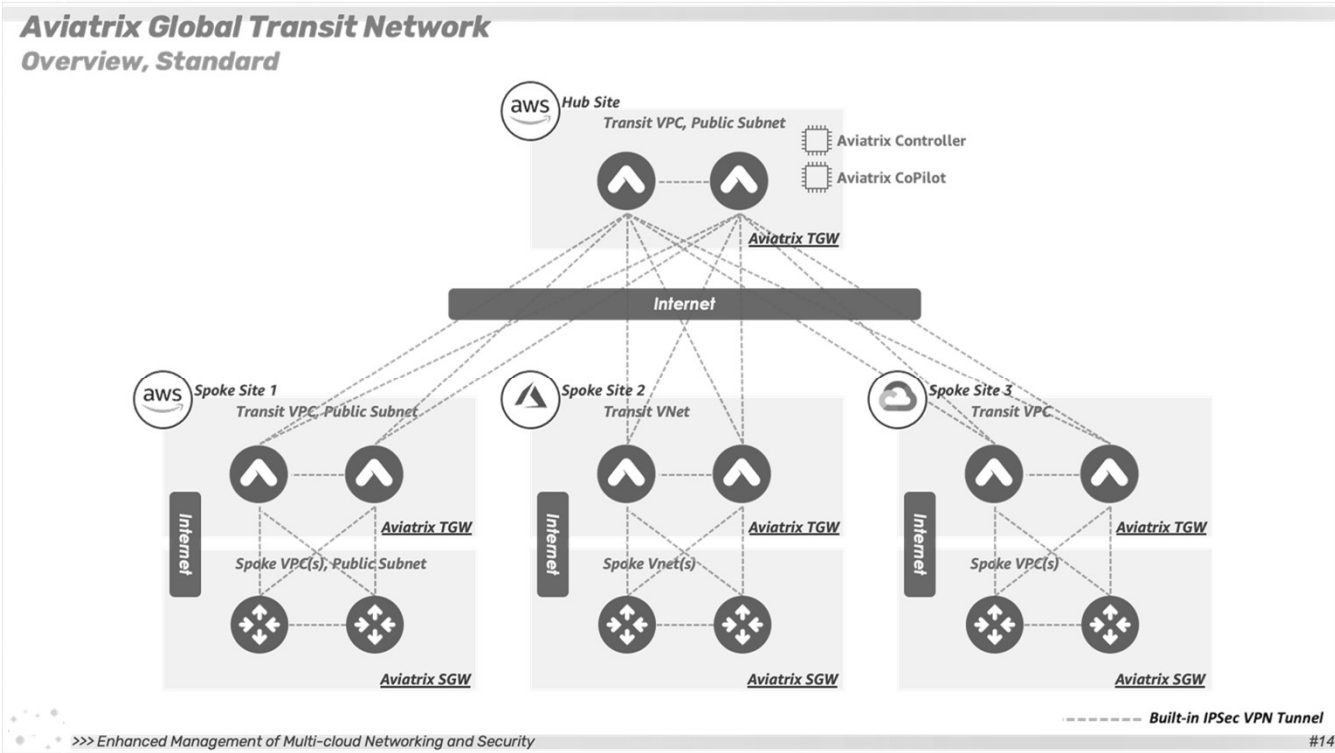


DAY 5. 멀티 클라우드 네트워킹

❖ Enhanced Management of Multi-cloud Networking and Security

• Business Model Nowadays

- What Are The Absences
- How To Efficiently Operate Your Clouds
 - ✓ Global Transit Network
 - ✓ FireNet
 - ✓ Egress FQDN Filtering
 - ✓ Observability
- Conclusion



Source: <https://hackmd.io/@terrencec51229/outline/%2FKF8s-B9kQwuAqub7ZheBFQ>

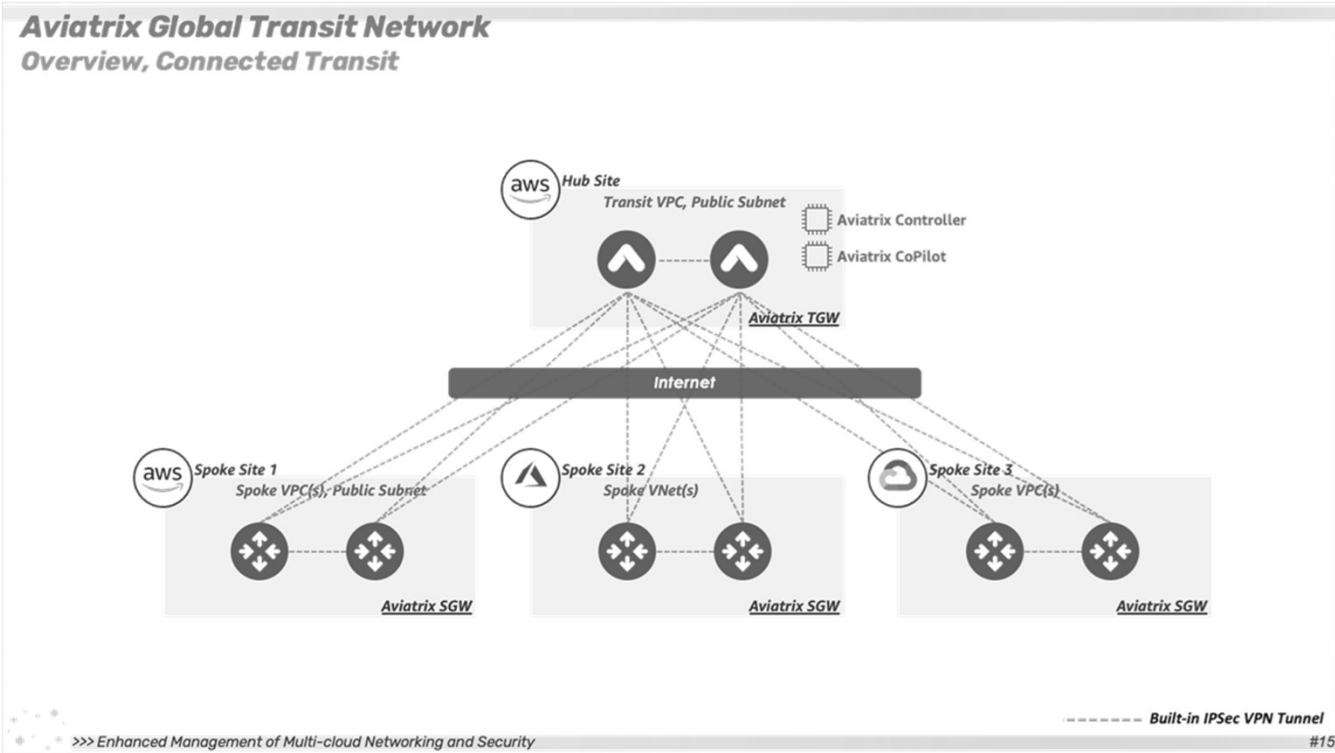


DAY 5. 멀티 클라우드 네트워킹

❖ Enhanced Management of Multi-cloud Networking and Security

• Business Model Nowadays

- What Are The Absences
- How To Efficiently Operate Your Clouds
 - ✓ Global Transit Network
 - ✓ FireNet
 - ✓ Egress FQDN Filtering
 - ✓ Observability
- Conclusion



Source: <https://hackmd.io/@terrencec51229/outline/%2FKF8s-B9kQwuAqub7ZheBFQ>



DAY 5. 멀티 클라우드 네트워킹

❖ Enhanced Management of Multi-cloud Networking and Security

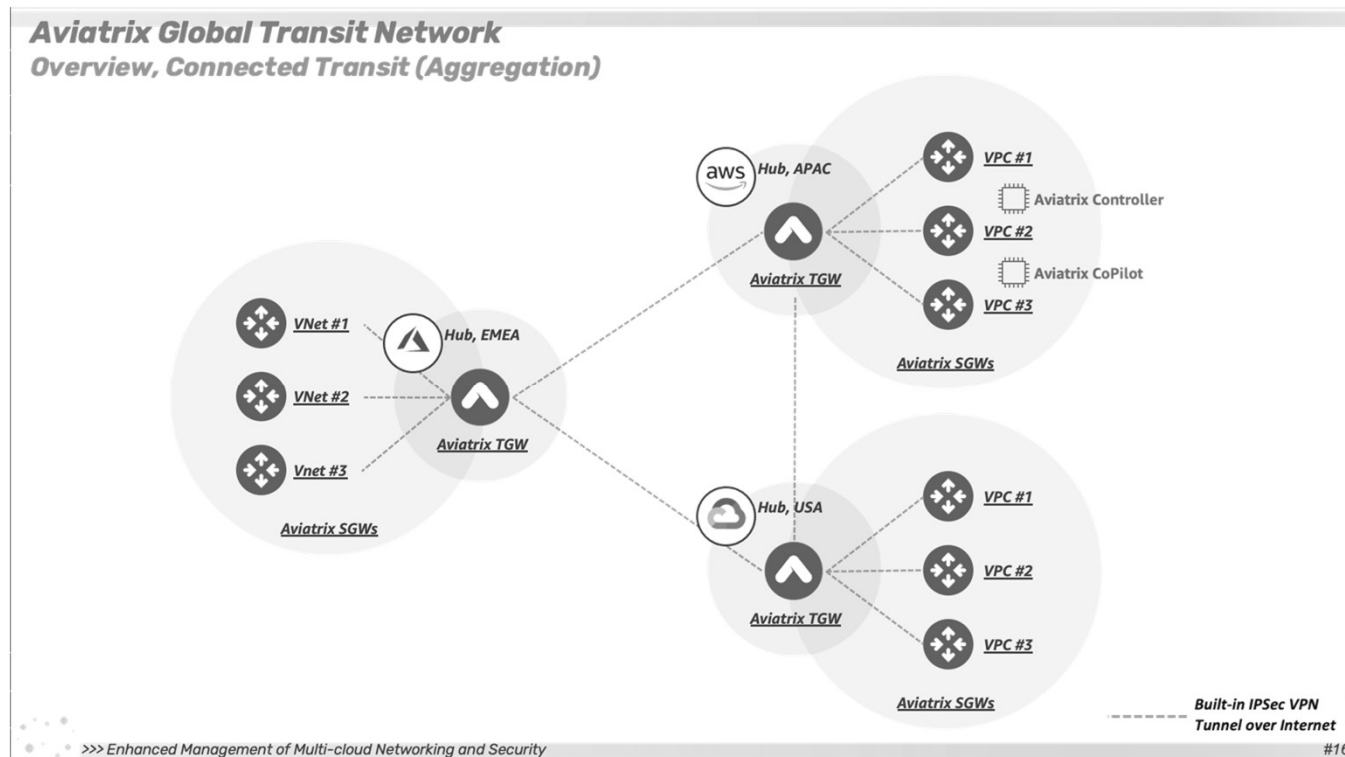
• Business Model Nowadays

➤ What Are The Absences

➤ How To Efficiently Operate Your Clouds

- ✓ Global Transit Network
- ✓ FireNet
- ✓ Egress FQDN Filtering
- ✓ Observability

➤ Conclusion

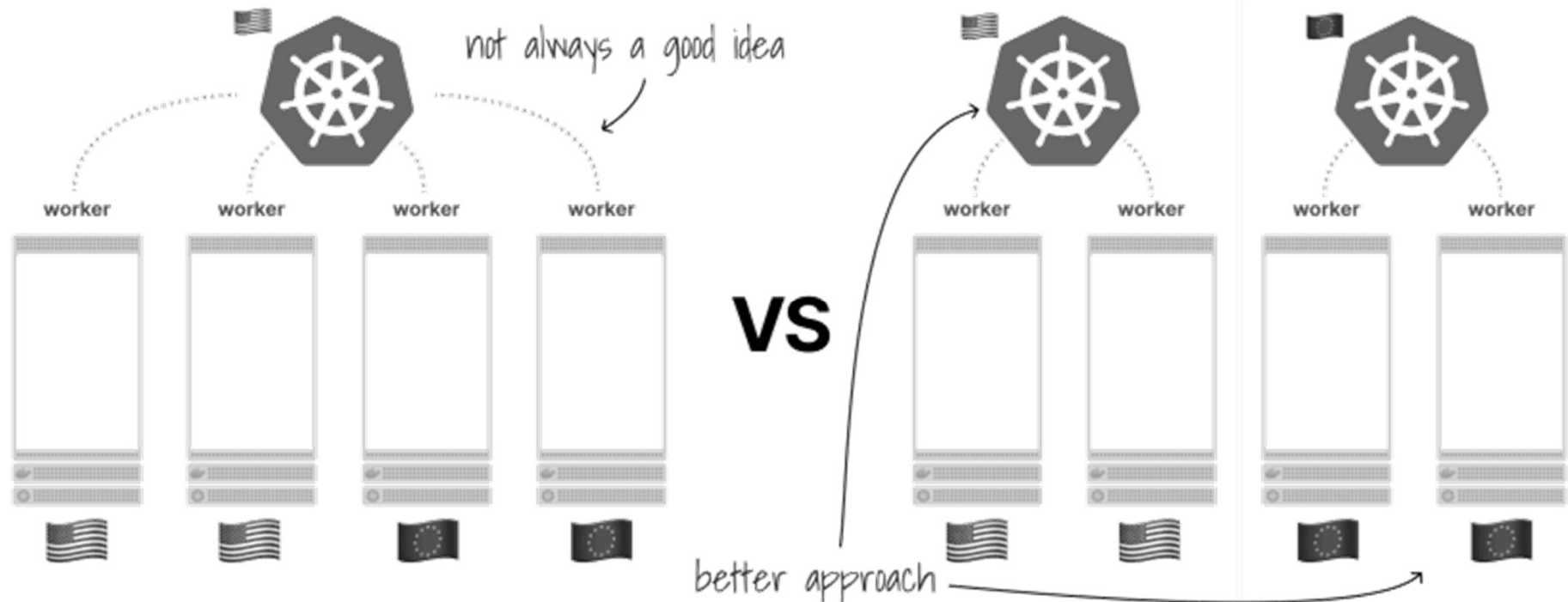


Source: <https://hackmd.io/@terrencec51229/outline/%2FKF8s-B9kQwuAqub7ZheBFQ>



DAY 5. 멀티 클라우드 네트워킹

- ❖ Kubernetes: Multi-Cluster/Multi-Region/Multi-Cloud
 - Scaling Kubernetes to multiple clusters and regions



Source: https://dev.to/danielepolencic/scaling-kubernetes-to-multiple-clusters-and-regionss-294b?fbclid=IwAR2X-Tly2ehLRf2hewOoy6VE0ZVdaL2FkTLY_pgH7gT6oDltKZb_ssoukzo



DAY 5. 멀티 클라우드 네트워킹

- ❖ **Kubernetes: Multi-Cluster/Multi-Region/Multi-Cloud**
 - Challenges of Multi-cluster

CHALLENGES OF MULTICLUSTER

- 1 Scheduling**
how should the pod be distributed?
- 2 Networking (north-south)**
how do I route the traffic to the right cluster?
- 3 Networking (east-west)**
should pod in one cluster be able to reach pods in others?
- 4 Data & stateful apps**
if a pod is rescheduled in a different cluster, what should you do with the data?

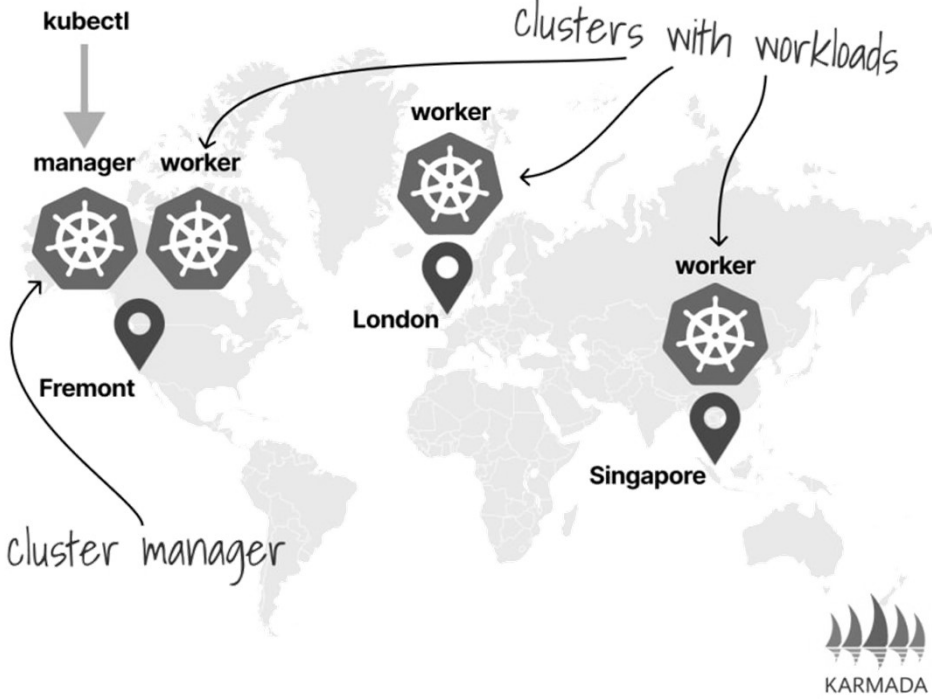
Source: https://dev.to/danielepolencic/scaling-kubernetes-to-multiple-clusters-and-regionss-294b?fbclid=IwAR2X-Tly2ehLRf2hewOoy6VE0ZVdaL2FkTLY_pgH7gT6oDltKZb_ssoukzo



DAY 5. 멀티 클라우드 네트워킹

❖ Kubernetes: Multi-Cluster/Multi-Region/Multi-Cloud

- Karmada uses a Kubernetes cluster as the manager and creates a second control plane that is multicluster aware.

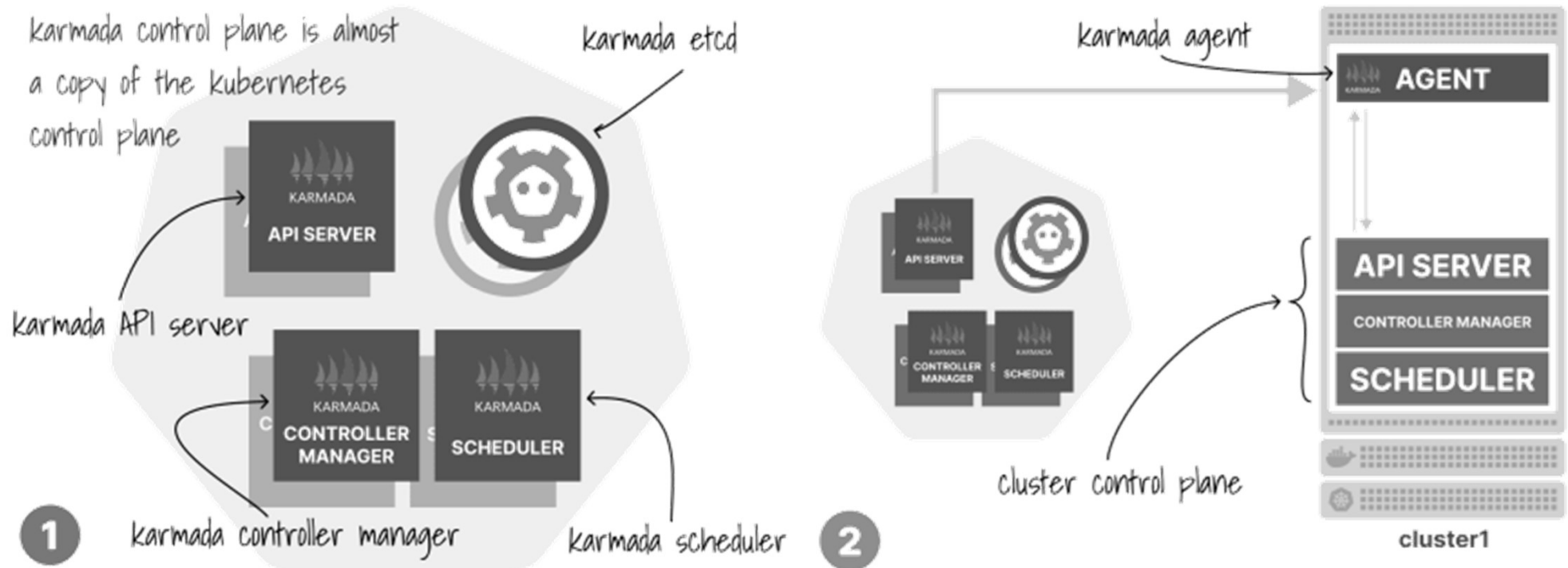


Source: <https://karmada.io/docs/userguide/scheduling/resource-propagating>



DAY 5. 멀티 클라우드 네트워킹

- ❖ The Karmada controller manager uses those agents to sync and dispatch commands.

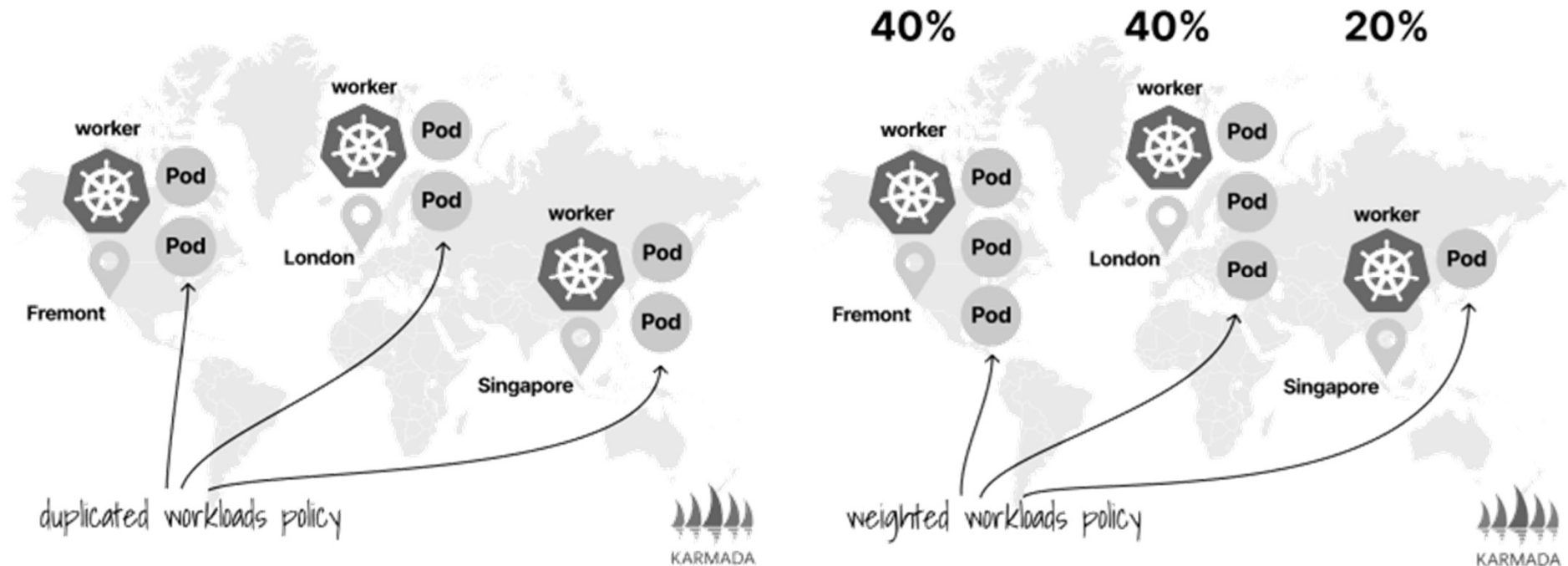


Source: https://dev.to/danielepolencic/scaling-kubernetes-to-multiple-clusters-and-regionss-294b?fbclid=IwAR2X-Tly2ehLRf2hewOoy6VE0ZVdaL2FkTLY_pgH7gT6oDltKZb_ssoukzo



DAY 5. 멀티 클라우드 네트워킹

- ❖ You could have policies to have a deployment equally distributed across regions.
- ❖ Or you could place your pods in a single region.

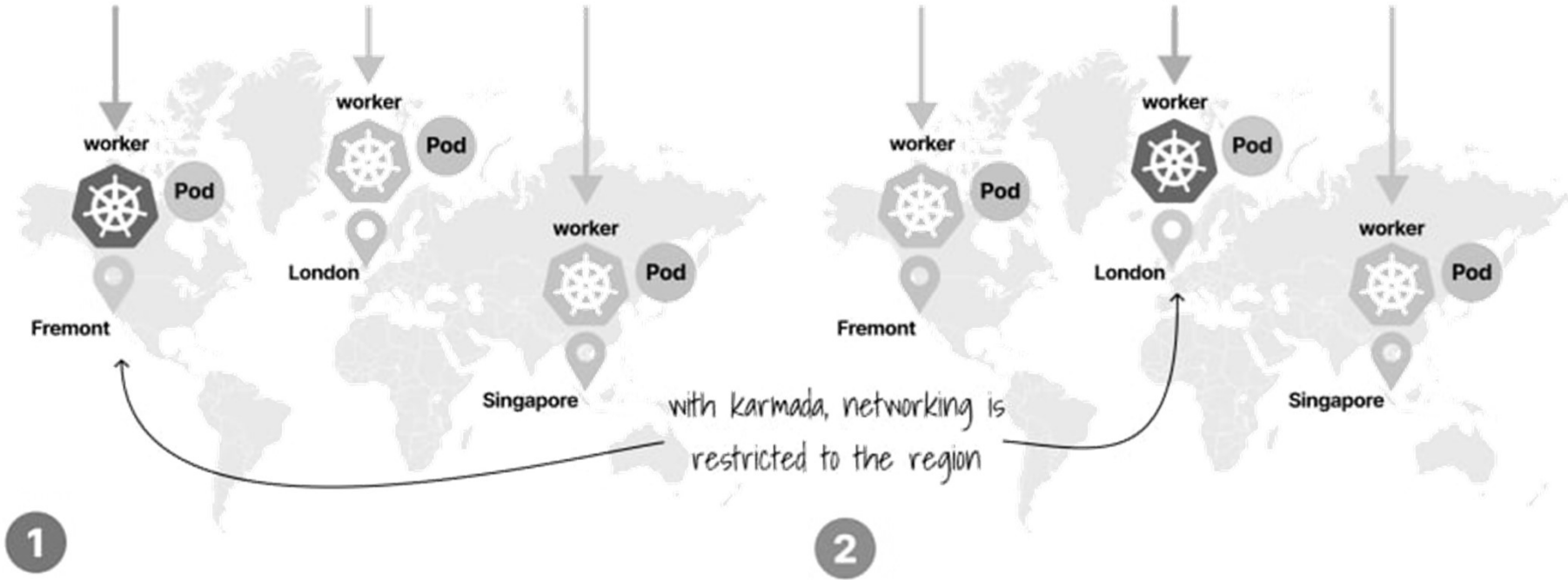


Source: https://dev.to/danielepolencic/scaling-kubernetes-to-multiple-clusters-and-regionss-294b?fbclid=IwAR2X-Tly2ehLRf2hewOoy6VE0ZVdaL2FkTLY_pgH7gT6oDltKZb_ssoukzo



DAY 5. 멀티 클라우드 네트워킹

❖ Karmada is essentially a multicluster orchestrator but doesn't provide any mechanism to connect the clusters' networks.



Source: https://dev.to/danielepolencic/scaling-kubernetes-to-multiple-clusters-and-regionss-294b?fbclid=IwAR2X-Tly2ehLRf2hewOoy6VE0ZVdaL2FkTLY_pgH7gT6oDltKZb_ssoukzo



DAY 5. 멀티 클라우드 네트워킹

- ❖ Istio can discover other instances in other clusters and forward the traffic to other clusters.



Source: https://dev.to/danielepolencic/scaling-kubernetes-to-multiple-clusters-and-regionss-294b?fbclid=IwAR2X-Tly2ehLRf2hewOoy6VE0ZVdaL2FkTLY_pgH7gT6oDltKZb_ssoukzo



DAY 5. 멀티 클라우드 네트워킹

- ❖ Karmada is essentially a multicluster orchestrator but doesn't provide any mechanism to connect the clusters' networks.

Source: https://dev.to/danielepolencic/scaling-kubernetes-to-multiple-clusters-and-regionss-294b?fbclid=IwAR2X-Tly2ehLRf2hewOoy6VE0ZVdaL2FkTLY_pgH7gT6oDltKZb_ssoukzo



DAY 5. 멀티 클라우드 네트워킹

- ❖ Cloud-Agnostic
- ❖ Building Applications – Infrastructure as Code

	Cloud-Native	Cloud-Agnostic
Source Code Repositories	AWS CodeCommit Azure DevOps Repos Google Cloud Source Repositories	GitHub GitLab Bitbucket
CI/CD Pipelines	AWS CodePipeline Azure DevOps Pipelines Google Cloud Build	Jenkins GitHub Actions CircleCI
IaC Templates	AWS CloudFormation Azure Resource Manager (ARM) Templates Google Cloud Deployment Manager	Terraform Pulumi serverless framework

특정 클라우드 서비스와 무관한 CI/CD, IaC

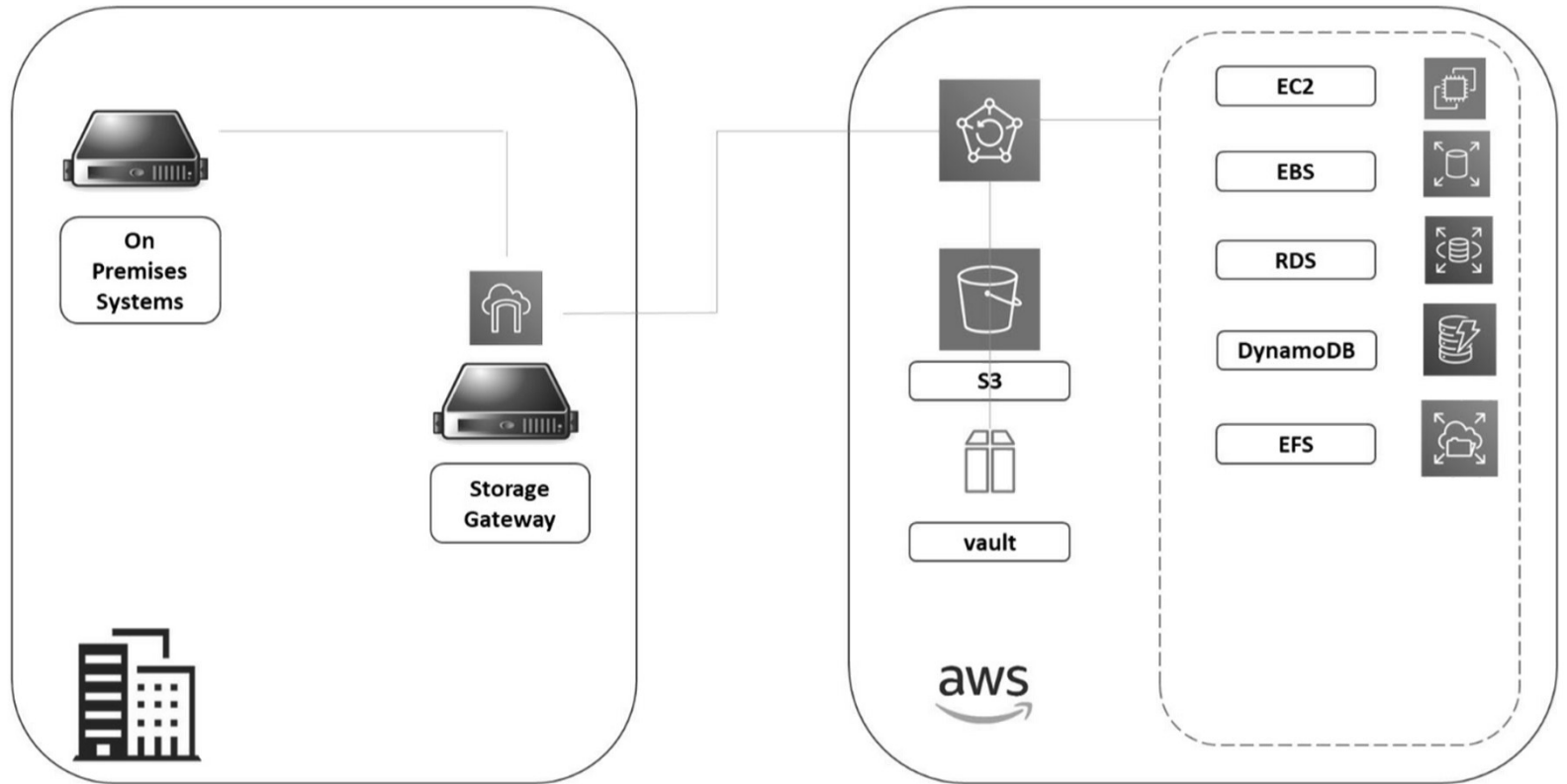


Cloud-agnostic platforms are environments that are capable of operating with any public cloud provider with minimal disruptions to a business.



DAY 5. 멀티 클라우드 네트워킹

❖ 클라우드 백업 (예): Hybrid backup in AWS

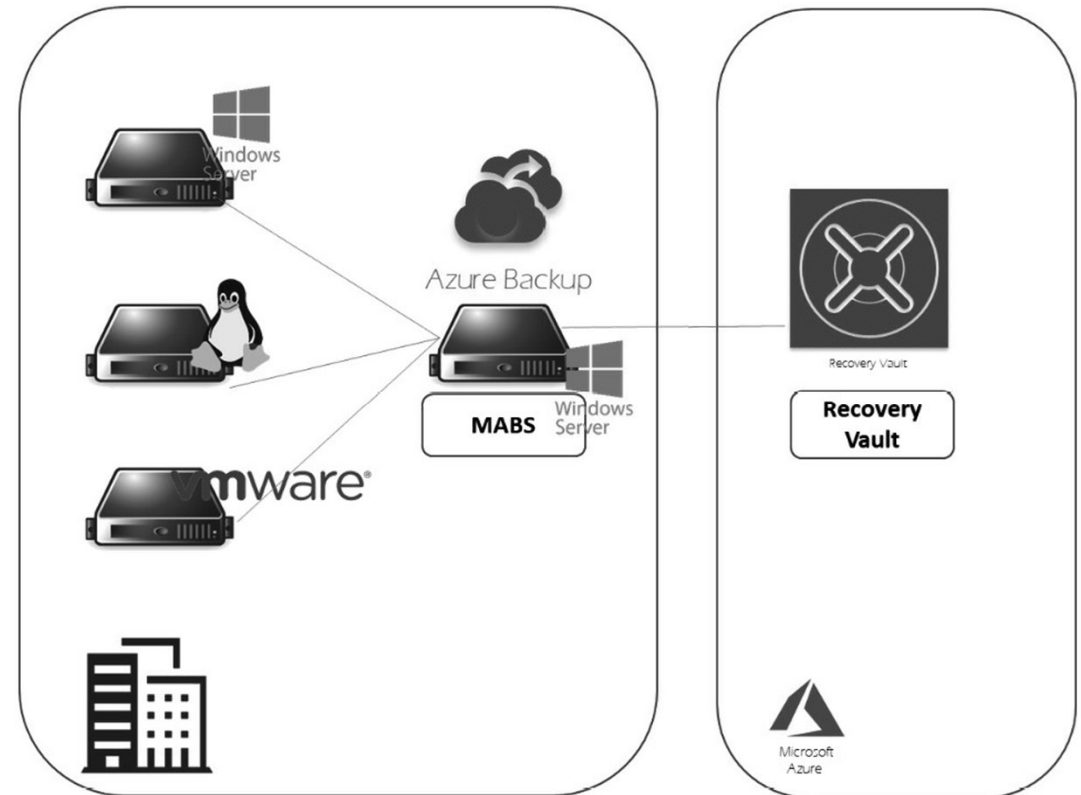


Source: Mulder, Jeroen. Multi-Cloud Architecture and Governance: Leverage Azure, AWS, GCP, and VMware vSphere to build effective multi-cloud solutions (p. 248). Packt Publishing. Kindle Edition.



DAY 5. 멀티 클라우드 네트워킹

❖ High-level overview of the setup for Microsoft Azure Backup Server

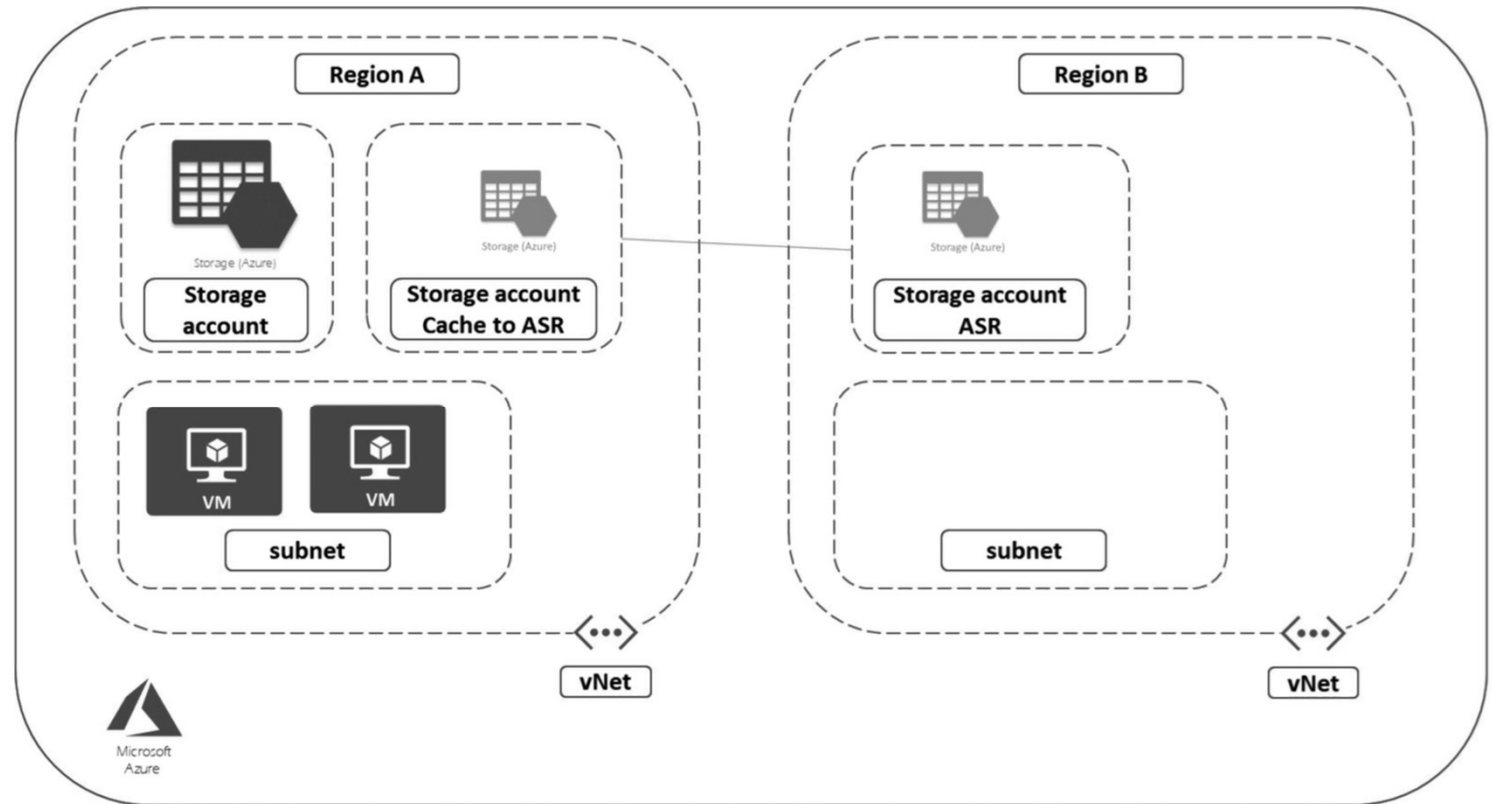


Source: Mulder, Jeroen. Multi-Cloud Architecture and Governance: Leverage Azure, AWS, GCP, and VMware vSphere to build effective multi-cloud solutions (p. 242). Packt Publishing. Kindle Edition.



DAY 5. 멀티 클라우드 네트워크

❖ High-level overview of Azure Site Recovery (ASR)



Source: Mulder, Jeroen. Multi-Cloud Architecture and Governance: Leverage Azure, AWS, GCP, and VMware vSphere to build effective multi-cloud solutions (p. 243). Packt Publishing. Kindle Edition.



DAY 5. 멀티 클라우드 네트워킹

❖ WHAT IS MULTI-CLOUD SECURITY?

• THE SHARED RESPONSIBILITY MODEL

RESPONSIBILITY	On-Premises	IaaS	FaaS	SaaS	PaaS	CIS Controls Companion Guide	CIS Foundations Benchmarks
Data classification and accountability	●	●	●	●	●	✓	✓
Client and endpoint protection	●	●	●	●	●	✓	✓
Identity and access management	●	●	◐	◐	◐	✓	✓
Application-level controls	●	●	◐	◐	◐	✓	✓
Network controls	●	◐	◐	◐	◐	✓	✓
Host infrastructure	●	◐	◐	◐	◐	✓	
Physical security	●	◐	◐	◐	◐		

Cloud Customer
 Cloud Provider

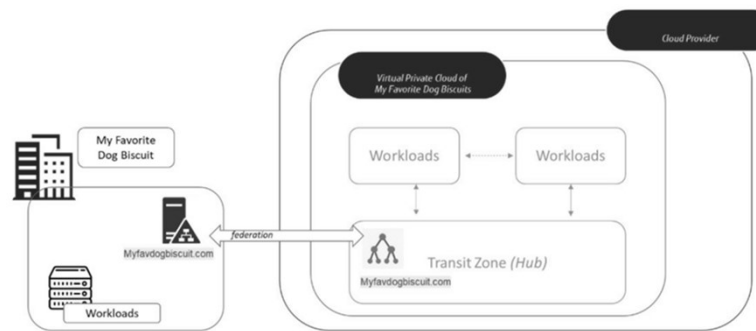
Source: <https://valtix.com/resources/what-is-multi-cloud-security/>



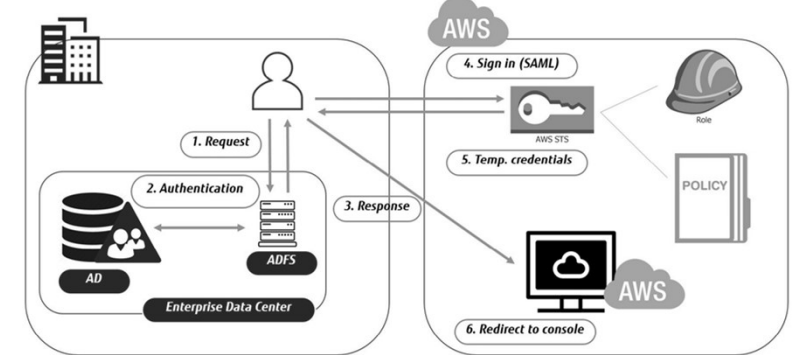
DAY 5. 멀티 클라우드 네트워크

❖ Designing access management across multi-cloud

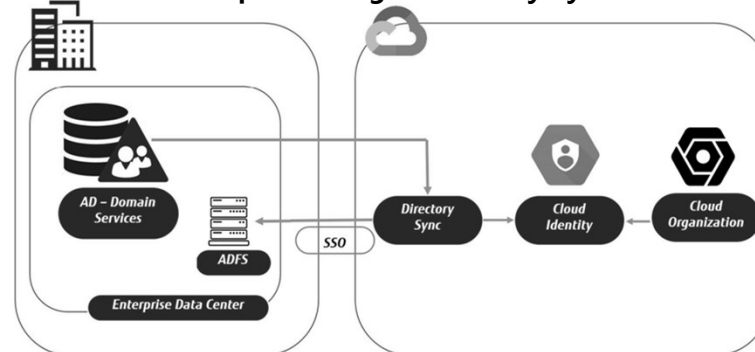
Conceptual overview of AD federation



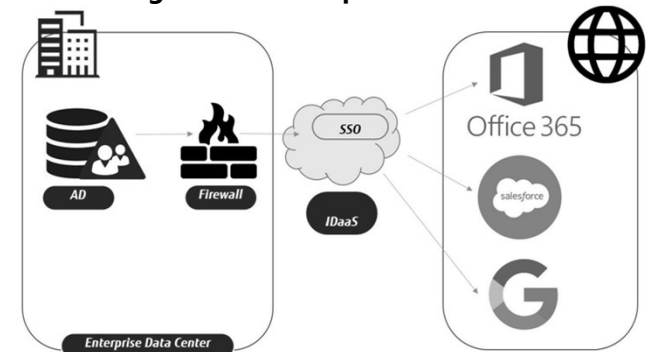
Concept of AWS federated authentication



Concept of Google Directory Sync

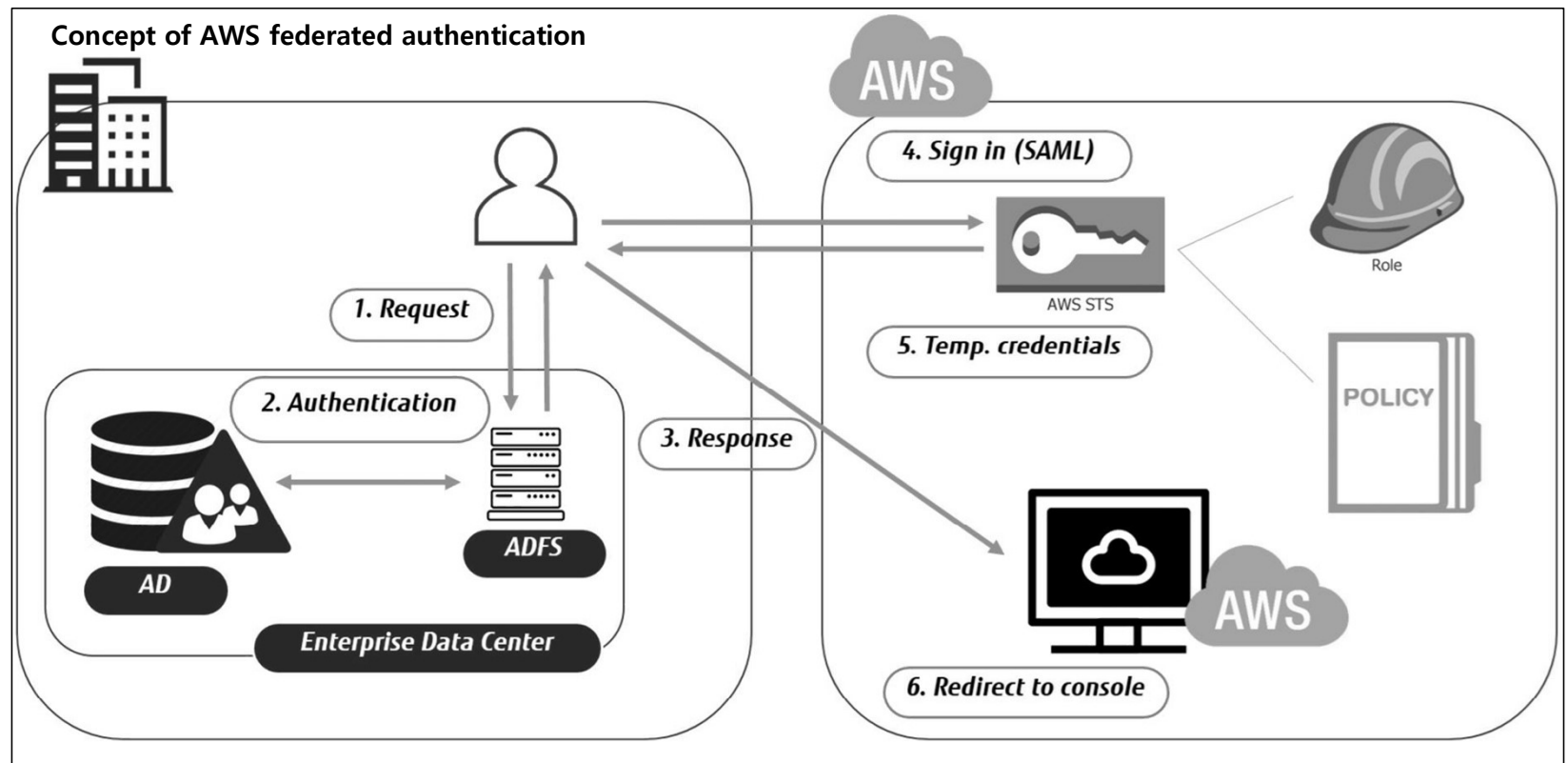


High-level concept of IDaaS



DAY 5. 멀티 클라우드 네트워크

- ❖ Designing access management across multi-cloud
 - Concept of AWS federated authentication



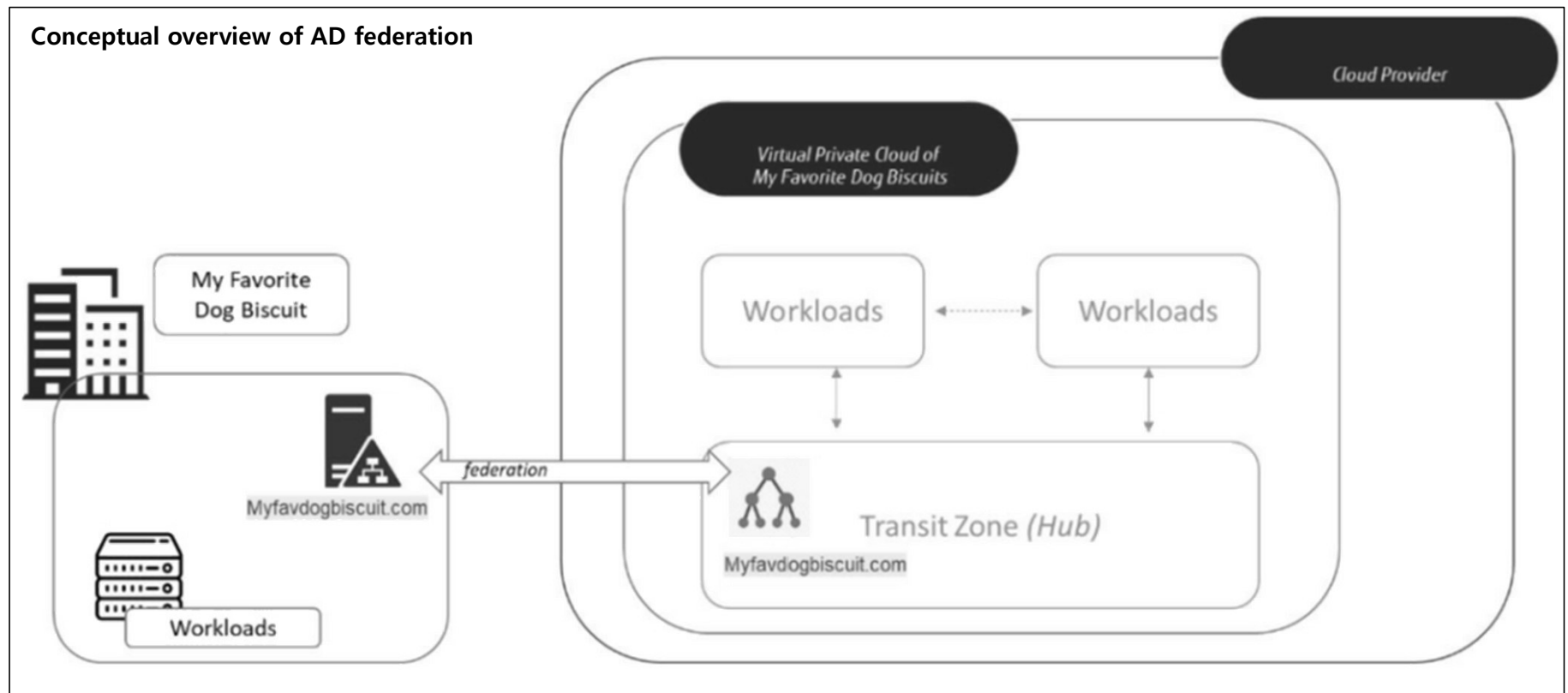
Source: Mulder, Jeroen. Multi-Cloud Architecture and Governance: Leverage Azure, AWS, GCP, and VMware vSphere to build effective multi-cloud solutions (p. 394). Packt Publishing. Kindle Edition.



DAY 5. 멀티 클라우드 네트워킹

❖ Designing access management across multi-cloud

- Conceptual overview of AD federation



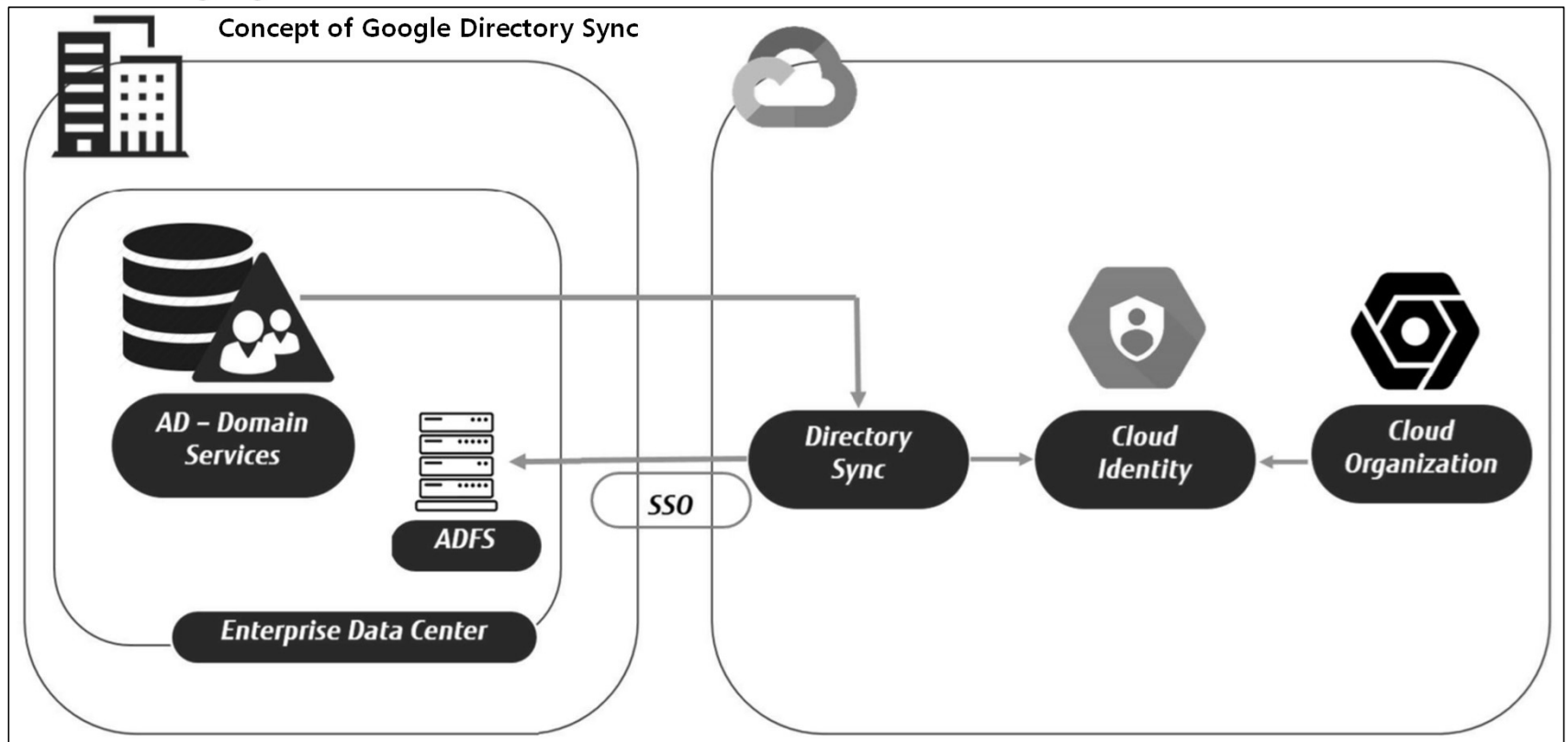
Source: Mulder, Jeroen. Multi-Cloud Architecture and Governance: Leverage Azure, AWS, GCP, and VMware vSphere to build effective multi-cloud solutions (p. 145). Packt Publishing. Kindle Edition.



DAY 5. 멀티 클라우드 네트워크

❖ Designing access management across multi-cloud

• Concept of Google Directory Sync



Source: Mulder, Jeroen. Multi-Cloud Architecture and Governance: Leverage Azure, AWS, GCP, and VMware vSphere to build effective multi-cloud solutions (p. 395). Packt Publishing. Kindle Edition.





**THANK
YOU**