멀티클라우드 데이터센터 설계와 운영

(v1.0)

2023년 10월
안종석
james@jslab.kr

1

2

CURRICULUM

주제	세부 내용
개요	• 개요 • 멀티 클라우드 데이터센터 개요 • CSP별 서비스 비교 • 멀티 클라우드 데이터센터 관리 사례
CSP/제조사의 멀티 클라우드 솔루션	• 제조사의 멀티클라우드 솔루션 • 멀티 클라우드 생태계 • 멀티 클라우드 전략 사례 • CSP별 네트워크 구성과 비교
멀티 클라우드의 연동	• 멀티 클라우드 인프라 연동 • 멀티 클라우드 라우팅 • Transit Gateway/Virtual WAN/VCN • 프라이빗 링크(Private Link)
멀티 클라우드 관리	• 멀티 클라우드와 인프라 관리 • 클라우드 보안 • 멀티 클라우드 사례 (데이터플랫폼 / 자동화 / DevSecOps / Telco) • vSwitch / Routing for Transit Gateway (실습)
멀티 클라우드의 Cloud Native 서비스 연동	• 멀티 클라우드 서비스 전략을 위한 인프라 구축 • Managed K8s 서비스의 5G Core/gNB/UE 설계 • 멀티 클라우드의 발전 방향 • 쿠버네티스 서비스의 외부 Load Balancer 연결, 코드기반 인프라 자동화 (실습)

3

❑ 실습 (별도 교재)

- 개요
- vSwitch / 제어기
- vRouter for Transit Gateway
- K8s 설치
- Helm
- K8s의 Load Balancer 연결
- 코드 기반 인프라 자동화

4

I. 개요

Multicloud; Multi-cloud; Multi Cloud

5

멀티 클라우드

❖ **What is cloud?**

- **'기존' IT:** 물리적 프라이빗 데이터센터에서 호스팅되는 기존 시스템
- **프라이빗 클라우드:** 가상화된 환경을 외부 데이터센터에 호스팅 또는 자체의 온프레미스에 호스팅
- **중앙에서 관리되는 플랫폼:** 사용량에 대한 요금이 청구되는 여러 비즈니스 부서를 호스팅
- **퍼블릭 클라우드:** AWS, Microsoft Azure, GCP등과 같이 퍼블릭 클라우드는 공용 인터넷을 사용하여 중앙화된 플랫폼에서 온디맨드 방식으로 IT 서비스를 제공하는 공급자
  - 컴퓨팅, 스토리지, 네트워킹과 같은 IT 서비스를 제공하는 중앙 집중식 플랫폼
  - 전 세계 데이터센터에 분산
  - 데이터센터와 클라우드를 관리
  - 기업은 데이터센터 자체에 투자할 필요 없이 서비스를 '임대'

Source: Mulder, Jeroen. Multi-Cloud Strategy for Cloud Architects: Learn how to adopt and manage public clouds by leveraging BaseOps, FinOps, and DevSecOps, 2nd Edition (pp. 34-35). Packt Publishing. Kindle Edition.

6

멀티 클라우드

❖ Why Multi-Cloud?

- 대부분의 기업은 이미 멀티 클라우드를 사용
- Amazon Web Services(AWS) 또는 Google Cloud Platform(GCP)과 같은 퍼블릭 클라우드에서 호스팅하는 애플리케이션과 함께 Microsoft 및 Salesforce의 Office 365와 같은 SaaS(Software as a Service)를 사용
- 기업이 겪고 있는 디지털 트랜스포메이션, 즉 특정 비즈니스 기능에 적합한 클라우드 서비스를 선택하는 동급 최강의 전략을 개발하는 클라우드 서비스 도입을 통해 비즈니스 민첩성을 확보하는 과정
- 해답을 단일 클라우드 공급업체가 아닌 멀티 클라우드에 기대

Source: Mulder, Jeroen. Multi-Cloud Strategy for Cloud Architects: Learn how to adopt and manage public clouds by leveraging BaseOps, FinOps, and DevSecOps, 2nd Edition (pp. 34-35). Packt Publishing. Kindle Edition.

멀티클라우드 이동 이유

❖ Multi-Cloud 환경 이동 이유

벤더 락인 우려 최고 솔루션 선택

"Most organizations adopt a multicloud strategy out of a desire to avoid vendor lock-in or to take advantage of best-of-breed solutions" - Gartner analyst

유연한 커스터마이징

Flexible Customization
Each Cloud Service Provider has special Features

위험 완화

Risk Mitigation
Deploying critical systems across multiple Cloud services provides additional fault tolerance

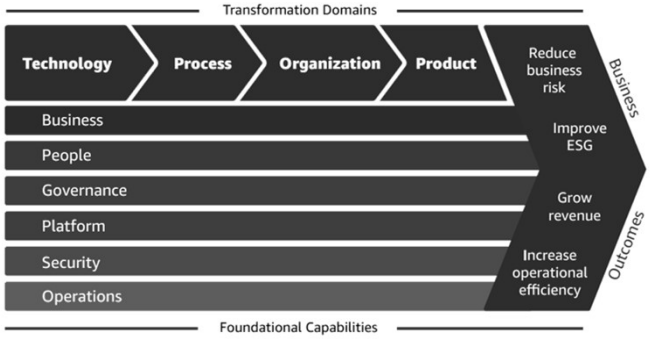
데이터 유실과 다운타임 최소화

Minimize the threat of extensive data loss or downtime due to component failure in cloud.

CLOUD ADOPTION FRAMEWORKS (CAF)

❖ **Accelerating Your Digital Business Transformation**

- 클라우드 혁신은 일련의 기능으로 구현되는 클라우드 기반 조직 변화를 통해 비즈니스 성과가 가속화됨
- 기술 혁신이 프로세스 혁신을 가능하게 하고, 프로세스 혁신이 제품 혁신을 가능하게 하는 조직 혁신
- 주요 비즈니스 성과는 비즈니스 리스크 감소, 환경, 사회, 거버넌스(ESG) 성과 개선, 매출 및 운영 효율성



ESG는 환경(Environmental),사회(Social),지배구조(Governance)의 영문 첫 글자를 조합한 단어로, 기업 경영에서 지속가능성을 달성하기 위한 3가지 핵심 요소

Source: https://d1.awsstatic.com/whitepapers/aws-caf-ebook.pdf , https://services.google.com/fh/files/misc/google_cloud_adoption_framework_whitepaper.pdf

BENEFITS OF MULTI-CLOUD

❖ **More extraordinary perseverance**
(더욱 특별한 인내심)

❖ **Eliminating vendor monopoly**
(공급업체 독점 제거)

❖ **Leveraging the benefits of several providers**
(여러 공급업체의 이점 활용)

❖ **Cost reduction**
(비용 절감)

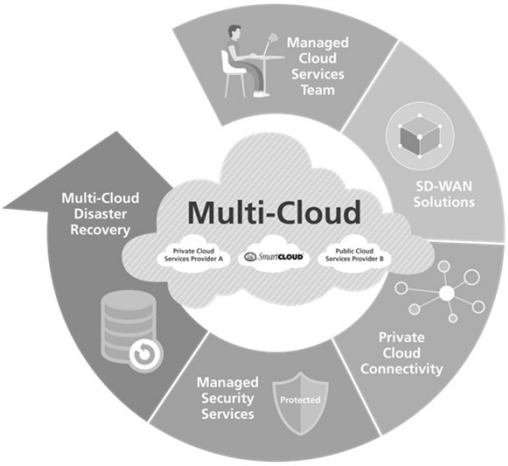
❖ **Compliance with regulations**
(규정 준수)

Source: https://www.infosectrain.com/blog/what-is-multi-cloud-network-architecture/#What-is-multi-cloud-network-architecture

멀티클라우드 모범 사례

❖ 멀티클라우드 모범 사례 (Best Practice of Multi-Cloud)

- 멀티 클라우드를 잘 관리하려면 기업은 유연한 네트워크 인프라, 정보 보안 솔루션, 원스톱 '서비스로서의 IT'를 제공하고 모든 기술 및 전문가 측면을 처리할 수 있는 매니지드 서비스 제공업체가 필요 (To manage Multi-Cloud well, the enterprise require the flexible network infrastructure, information security solutions and a managed services provider who can provide a one-stop "IT-as-a-Service" and take care of all technical and professionals' aspects.)
  - Managed cloud service team
  - SD-WAN solution
  - Private cloud connectivity
  - Managed security services
  - Multi-cloud disaster recovery

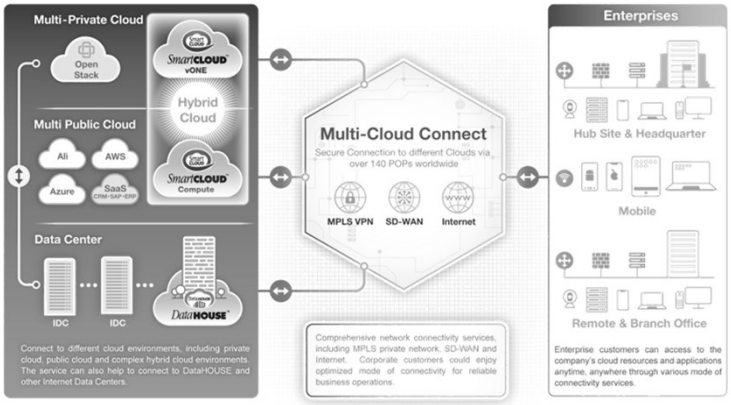


Source: https://www.citictel-cpc.com/en-sg/product-services/multi-cloud-connect

MULTI-CLOUD CONNECT DIAGRAM

❖ Multi-Cloud Connect Diagram

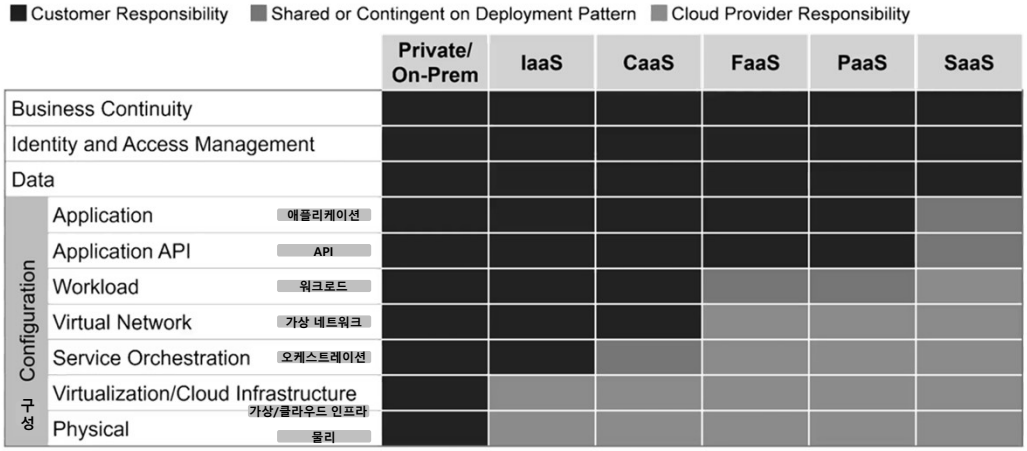
- Highlights
  - Avoiding vendor lock-in 벤더 락인
  - Preventing data loss or downtime due to a localized component failure in the cloud 다운 방지
  - Mitigating risk of disasters with increased redundancy 재난 위험 완화
  - Minimizing costs by combining the best options from multiple service providers 비용
  - Ensuring data security and compliance according to the data sovereignty requirements 보안
  - Low latency – suitable for enterprises who have global presence and need to handle data across different geographical regions while maintain a consistent end-user experience 지연



Source: https://www.citictel-cpc.com/en-sg/product-services/multi-cloud-connect

SPLIT RESPONSIBILITY

❖ **The Nuances of Split Responsibility (클라우드 책임 분담의 차이)와 구성(Configuration)**



Source: Gartner - https://webinar.gartner.com/429960/agenda/session/1033381?login=ML

Source: https://twitter.com/Gartner_inc/status/1534249589435518976

TOP CLOUD CHALLENGES

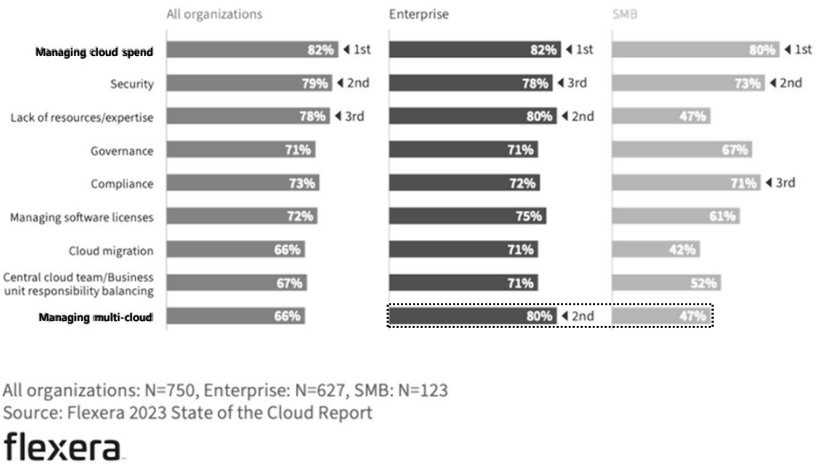
❖ **Managing cloud spend**

❖ **Security**

❖ **Lack of resources/expertise**

❖ **Managing multi-cloud**

❖ **Compliance**



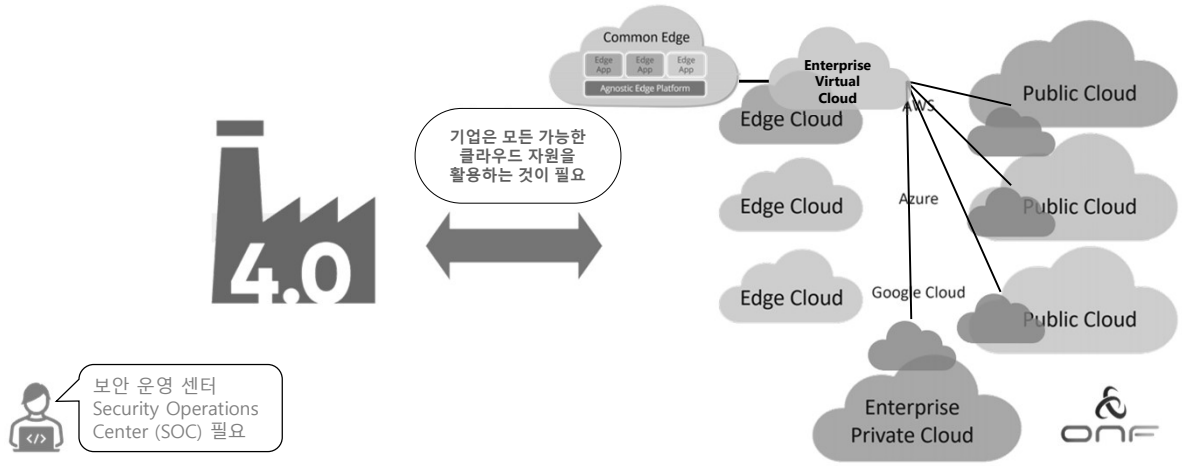
All organizations: N=750, Enterprise: N=627, SMB: N=123
Source: Flexera 2023 State of the Cloud Report

flexera

Source: https://www.flexera.com/blog/cloud/cloud-computing-trends-flexera-2023-state-of-the-cloud-report/

멀티클라우드는 기업의 뉴노멀

❖ 하나의 'Enterprise Virtual Cloud' 필요



15

PLANNING

❖ What You Need to Know When Planning Your Hybrid and Multi-cloud Network

- **Migration and Manageability**
  - ✓ 퍼블릭 클라우드 제공업체에 연결
  - ✓ 클라우드 게이트웨이 설치
  - ✓ IPSec 터널 구축
  - ✓ VPC, VNET 및 CIDR 네트워크 검색
  - ✓ BGP 라우팅 프로세스 구성
  - ✓ 적절한 보안 정책 설치
  - ✓ 인터넷 및 SaaS 서비스에 지역 출구 지점 추가하기
  - ✓ 애플리케이션 수준 정보로 오버레이된 환경 및 네트워크 전반의 모든 트래픽을 시각화
  - ✓ 통합된 보기와 용어로 네트워킹 팀과 보안 팀 간의 협업을 강화
  - ✓ 실행 가능한 인사이트를 통해 이상 징후를 탐지하여 경보 피로를 최소화
  - ✓ 오작동 또는 사고 발생 후 평균 해결 시간(MTTR)을 획기적으로 단축
- **Security**
  - ✓ 사용 중인 여러 클라우드 공급업체에서 일관된 사이버 보안 프로토콜
  - ✓ 각 클라우드 서비스 제공업체의 업그레이드 주기와 새로운 보안 공백이 발생할 가능성
  - ✓ 효과적인 보안 정책의 구현을 초과하는 앱 개발 속도
  - ✓ 직원이 여러 클라우드에서 작업할 수 있는 액세스 자격 증명으로 악의적인 사용자를 차단하고 다양한 사용자에 대한 일관된 권한 정책을 유지
- **Network and Application Observability**
  - ✓ 서버 트래픽 개요(위치, 소스 연결/세그먼트/IP, 대상 IP, 포트 서비스, 프로토콜 등)
  - ✓ 서버 트래픽을 시각화하여 데이터 흐름 및 위치와 관련된 추세를 파악할 수 있습니다.
  - ✓ 상세하고 타임스탬프가 찍힌 네트워크 기록
  - ✓ 애플리케이션에 대한 분석
  - ✓ 사이버 위협 분석 및 의심스러운 행동 식별.
  - ✓ 완벽한 네트워크 및 애플리케이션 가시성을 통해 기업은 잠재적인 사이버 위협을 신속하게 해결하고 네트워크 문제를 사전에 발견

Source: https://www.insidepacket.com/planning-hybrid-and-multi-cloud-network/

16

MULTI-CLOUD MARKET

❖ **Multi-cloud Market Ecosystem** (Market and Market)

- 멀티클라우드 관리
- 클라우드 보안
- 멀티클라우드 네트워킹
- 제로 트러스트 보안

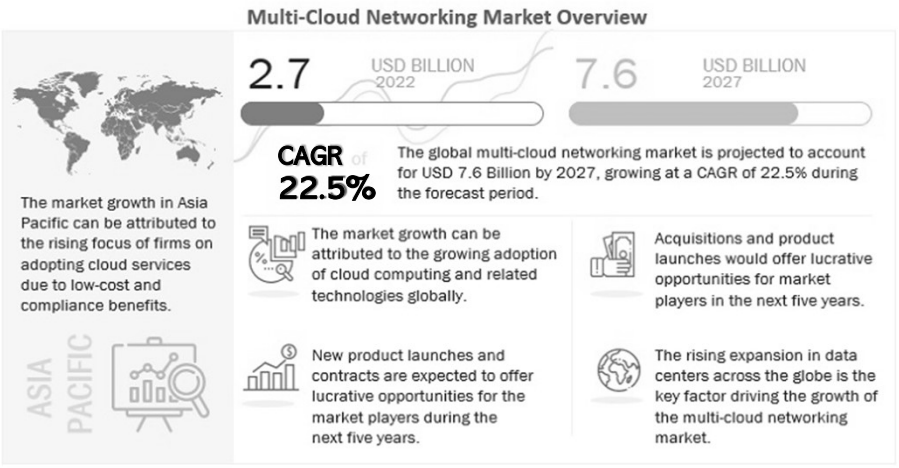
MULTI-CLOUD MANAGEMENT	CLOUD SECURITY	MULTI-CLOUD NETWORKING	ZERO TRUST SECURITY
▪ BMC Software ▪ CenturyLink ▪ Accenture ▪ VMware ▪ DoubleHorn ▪ RightScale ▪ CliQr ▪ Cloudyn ▪ Jamcracker ▪ Dell Technologies ▪ IBM ▪ Citrix ▪ UnityOneCloud ▪ SixSq ▪ Others	▪ Amazon Web Services ▪ Microsoft ▪ Check Point ▪ Google ▪ Palo Alto Networks ▪ McAfee ▪ IBM ▪ Zscaler ▪ Cisco ▪ Fortinet ▪ Sophos ▪ Forseeti ▪ Broadcom ▪ Trend Micro ▪ Tenable ▪ Forcepoint ▪ Netskope ▪ Imperva ▪ Proofpoint ▪ Others	▪ VMware ▪ Oracle ▪ F5 ▪ Cisco ▪ Nutanix ▪ Juniper ▪ Citrix ▪ Illumio ▪ Akamai ▪ Aviatrix ▪ Prosimo ▪ Infoblox ▪ Others	▪ Cisco ▪ Palo Alto Networks ▪ Okta ▪ Check Point ▪ Trend Micro ▪ IBM ▪ FireEye ▪ McAfee ▪ Forcepoint ▪ RSA Security ▪ Illumio ▪ Sophos ▪ Google ▪ Microsoft ▪ VMware ▪ Fortinet ▪ Cloudflare ▪ Others

Source: https://www.marketsandmarkets.com/Market-Reports/multi-cloud-security-market-231733464.html

17

MCN 시장 전망

❖ **Multi-Cloud Networking(MCN) 시장 전망: 연평균 22.5%** (Markets and Markets)



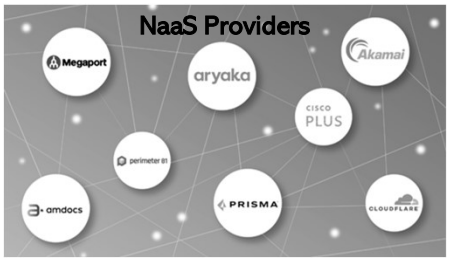
Source: 'https://www.marketsandmarkets.com/Market-Reports/multi-cloud-networking-market-80685691.html

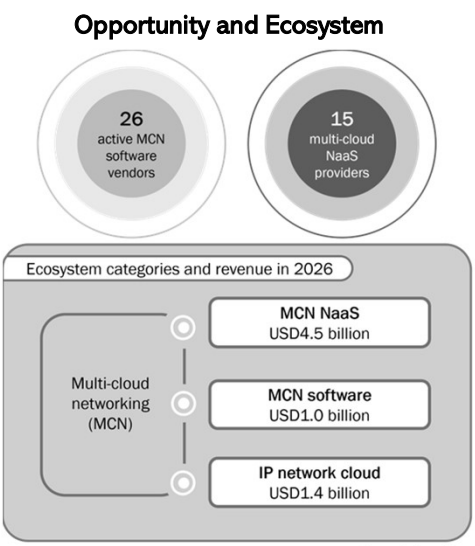
18

멀티클라우드 네트워킹 생태계의 기회

❖ Multi-Cloud Networking: 생태계와 기회

- MCN NaaS (15 multi-cloud NaaS providers)
- MCN Software (26 active MCN software vendors)
- IP network cloud





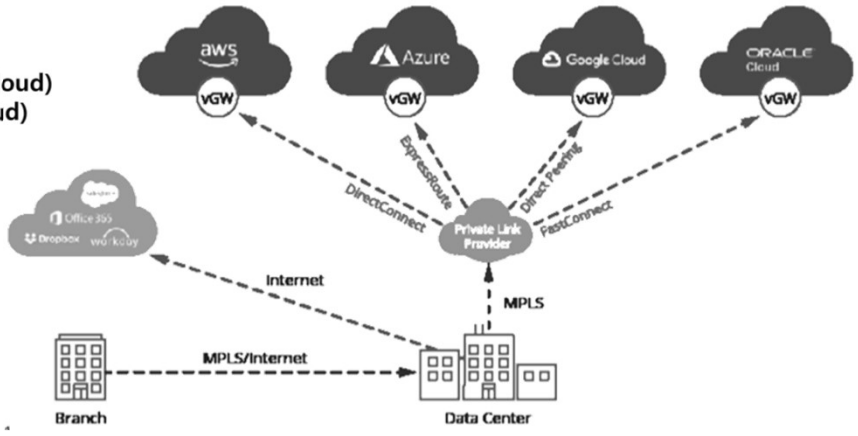
analysys mason

Source: https://www.analysysmason.com/research/content/reports/multi-cloud-networking-rma21/

멀티클라우드 데이터센터 연결

❖ Multi-Cloud Connectivity (예)

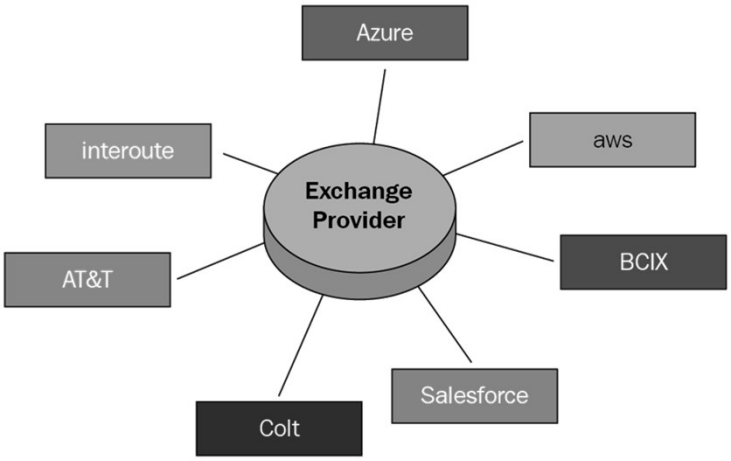
- Private Link Provider
- Direct Connect (AWS)
- Express Route (Azure)
- Direct Peering (Google Cloud)
- Fast Connect (Oracle Cloud)
- Internet
- MPLS



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

EXCHANGE PROVIDER

❖ Exchange providers

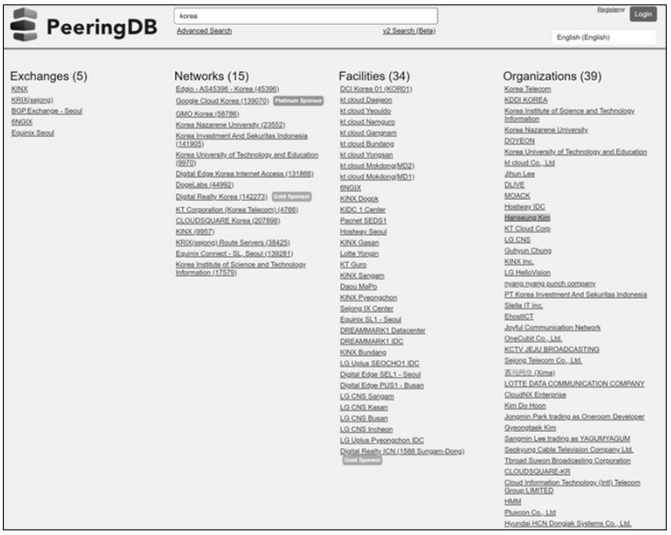


Source: Multi-Cloud for Architects (Published by Packt Publishing Ltd) Florian Klaffenbach, Markus Klein, Suresh Sundaresan

EXCHANGE PROVIDER IN KOREA

❖ Exchange providers in Korea

- KINX
- KRIX
- Equinix Seoul
- 6NGIX
- BGP.Exchange - Seoul

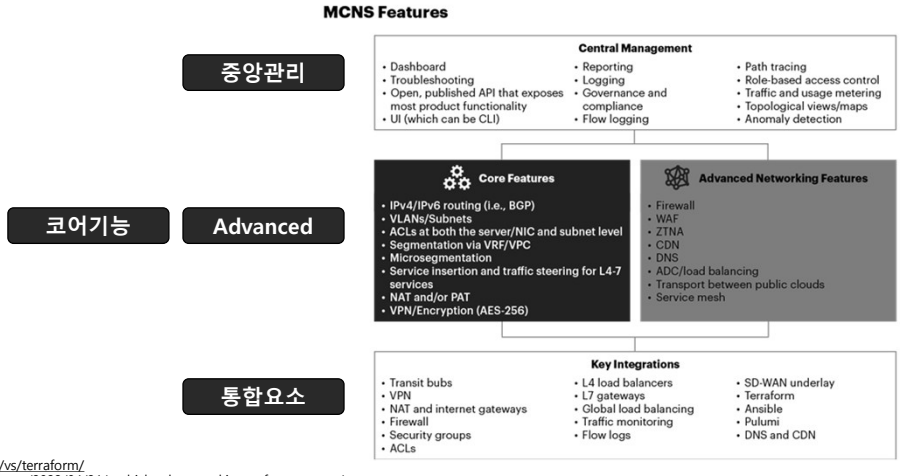


Source: https://www.peeringdb.com/search?q=korea

MCNS

❖ 가트너(예): Multicloud Networking Software (MCNS)

- 중앙관리
- 코어기능
- Advanced 기능



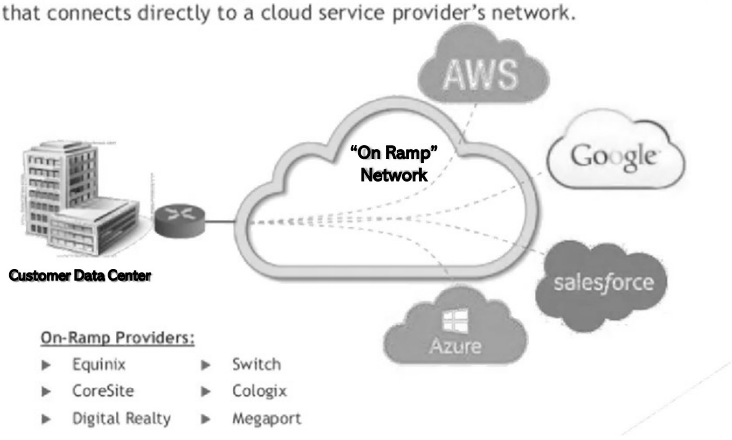
Source: https://www.pulumi.com/docs/intro/vs/terraform/
Source: https://blogs.gartner.com/andrew-lerner/2022/04/21/multicloud-networking-software-mcns/

온램프 서비스

❖ 온램프 서비스 - Cloud "On-Ramp" Service Providers

- Equinix
- CoreSite
- Digital Realty
- Switch
- Cologix
- Megaport

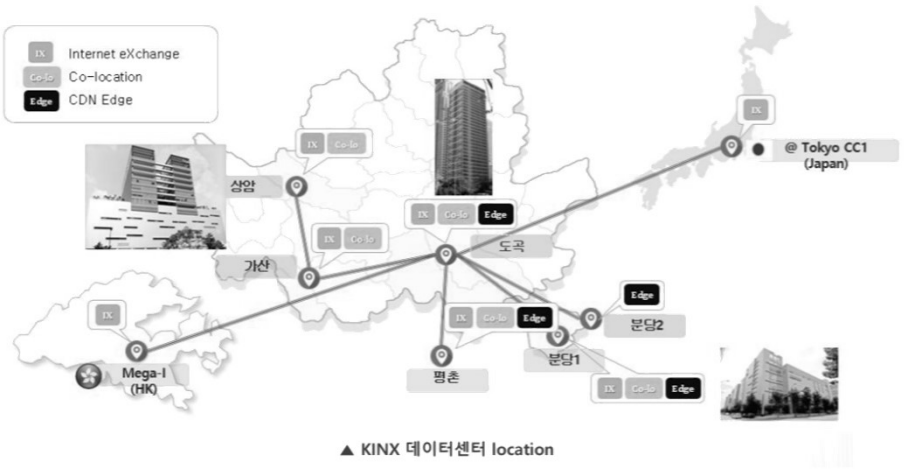
▶ Cloud On Ramp Services provide a connection service within a data center that connects directly to a cloud service provider's network.



Source: Joseph Primicerio

KINX

❖ 온램프 서비스 - KINX



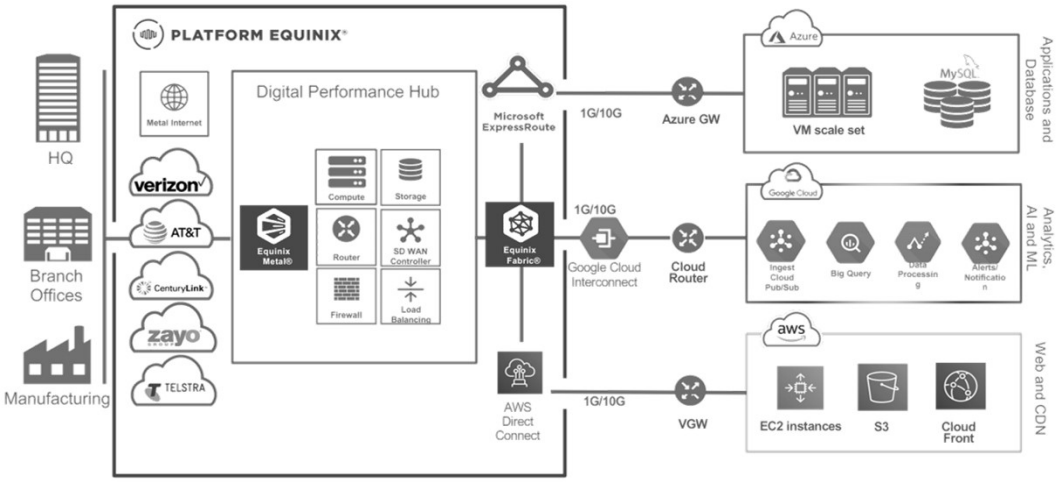
▲ KINX 데이터센터 location

Peering Service: https://www.kinx.net/
Source: [데이터센터 관련주] 케이아이엔엑스(KINX), IDC 사업부문 분석 (tistory.com)

25

온램프 서비스

❖ 온램프 서비스 - Hybrid Multi Cloud Deployment Model (Equinix)



Source: Equinix

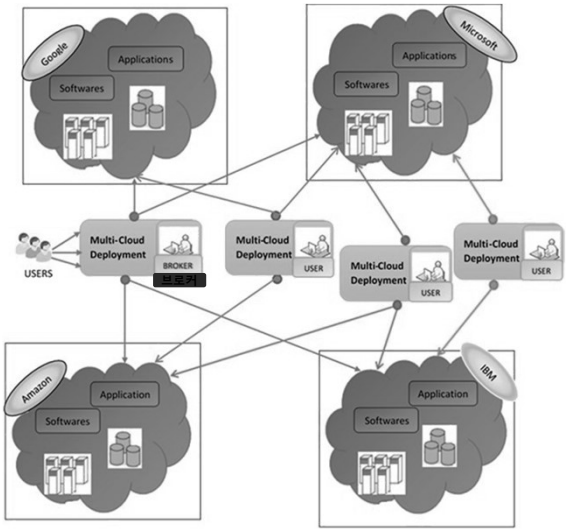
26

멀티클라우드 환경

❖ 멀티클라우드 환경 - Multi-cloud environment

- Cloud Aggregators
- Cloud Integrators
- Cloud Customizers

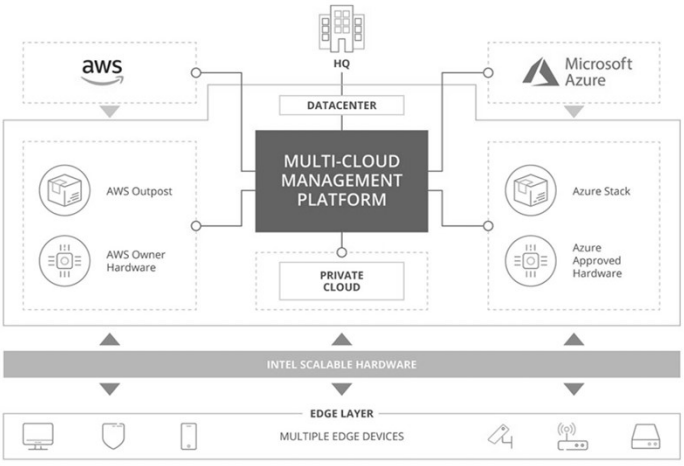
Cloud aggregators are high-level consultants or architects who bring together multiple **cloud** services and offer them as a combined package to customers.
(클라우드 애그리게이터는 여러 클라우드 서비스를 한데 모아 고객에게 결합된 패키지로 제공하는 고급 컨설턴트 또는 아키텍트이다.)



Source: 'Operationalizing Multi-Cloud Environments', Technologies, Tools and Use Cases, B. S. Rajeshwari, Pethuru Raj, Ramkumar Thirunavukarasu (2022)

멀티클라우드 관리 플랫폼

❖ Multi Cloud Management Platform Reference Architecture

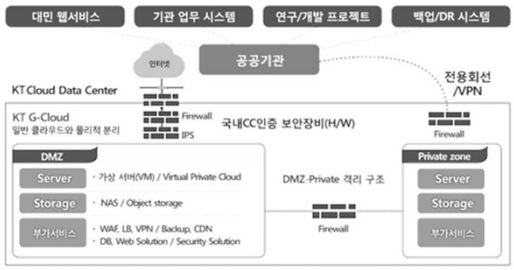


Source: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-designing-hybrid-cloud-architecture-for-the-future.pdf

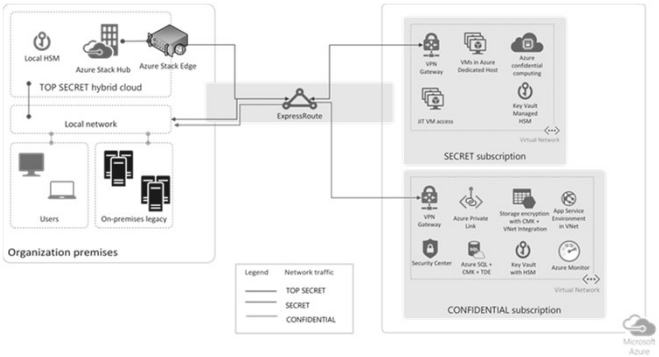
CLOUD FOR GOVERNMENT

❖ 공공 클라우드 (Cloud for Government)

G-Cloud in KT Cloud



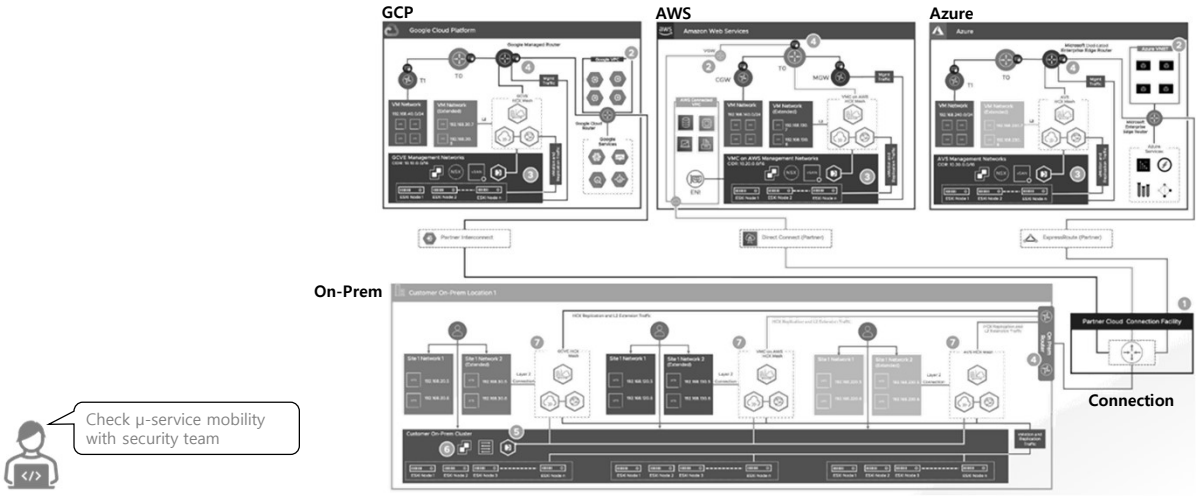
Azure for secure worldwide public sector cloud adoption



Source: https://learn.microsoft.com/en-us/azure/azure-government/documentation-government-overview-wwps

멀티클라우드 아키텍처

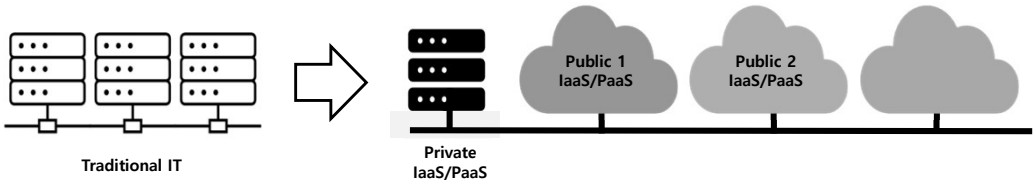
❖ Architecting for app mobility in a multi-cloud environment.



Source: https://blogs.vmware.com/cloud/wp-content/blogs.dir/136/files/2020/12/David1129.png

클라우드 운영 모델의 변화

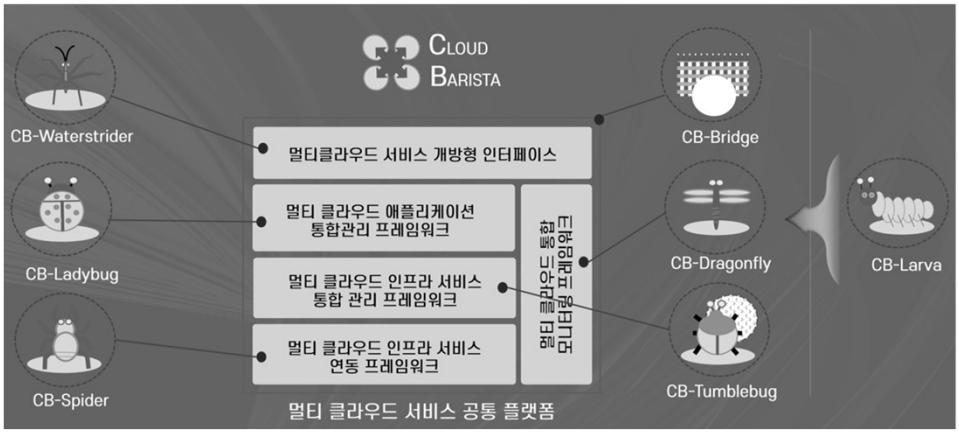
- ❖ Run: 전용 인프라 → 클라우드 상의 스케줄링
- ❖ Connect: 고정 IP 주소 → 서비스 기반 유동 IP
- ❖ Secure: IP 주소 기반 보안 정책 → Identity 기반
- ❖ Provisioning: 전용 서버 → 요청 기반 용량



멀티클라우드 기술 (오픈소스 예)

❖ 클라우드바리스타 (ETRI)

- CB-Waterstrider
- CB-Ladybug
- CB-Spider
- CB-Bridge
- CB-Dragonfly
- CB-Tumblebug
- CB-Larva

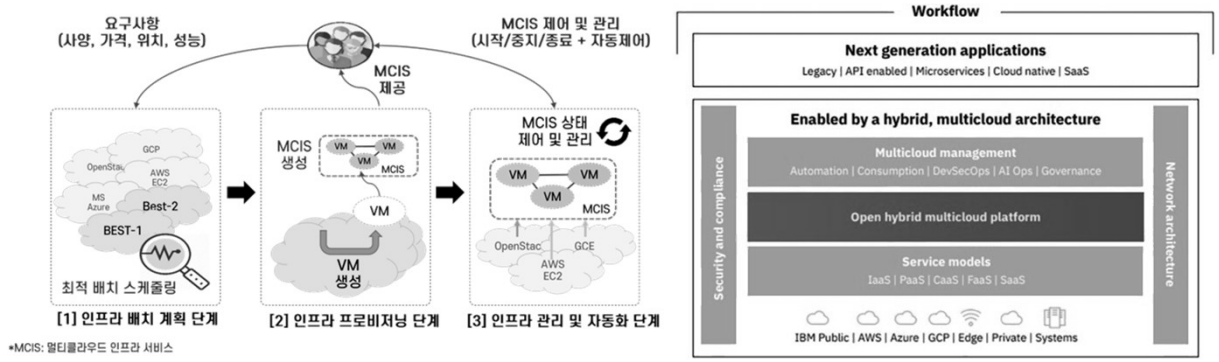


Source: @ ETRI Conference 2022 '멀티클라우드가 만들어가는 세상' (정영우) 참조

MCIS

❖ MCIS: 멀티클라우드 인프라 서비스

❖ Dynamic workflow orchestration in hybrid multi-cloud

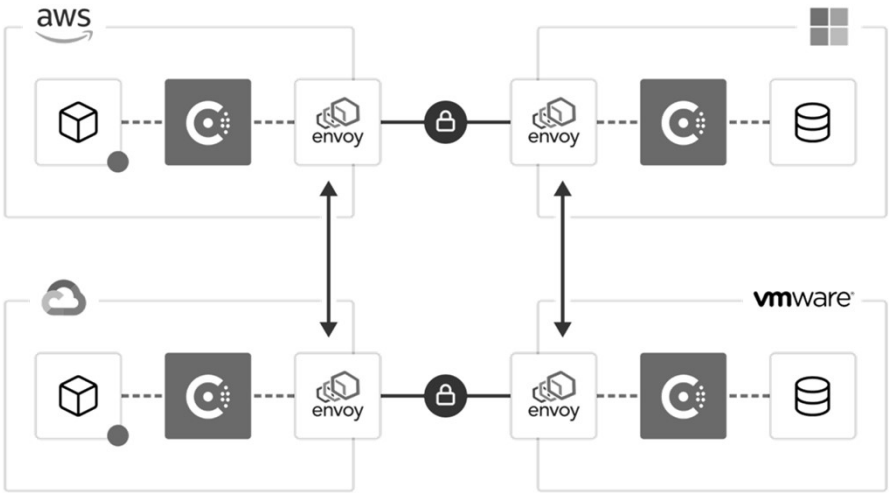


Source: @ ETRI Conference 2022 '멀티클라우드 인프라 통합 관리 기술' (손석호) 참조
Source: 'Operationalizing Multi-Cloud Environments', Technologies, Tools and Use Cases, B. S. Rajeshwari, Pethuru Raj, Ramkumar Thirunavukarasu (2022)

33

MULTI-DATACENTER, MULTI-REGION

❖ Cloud Native Layer



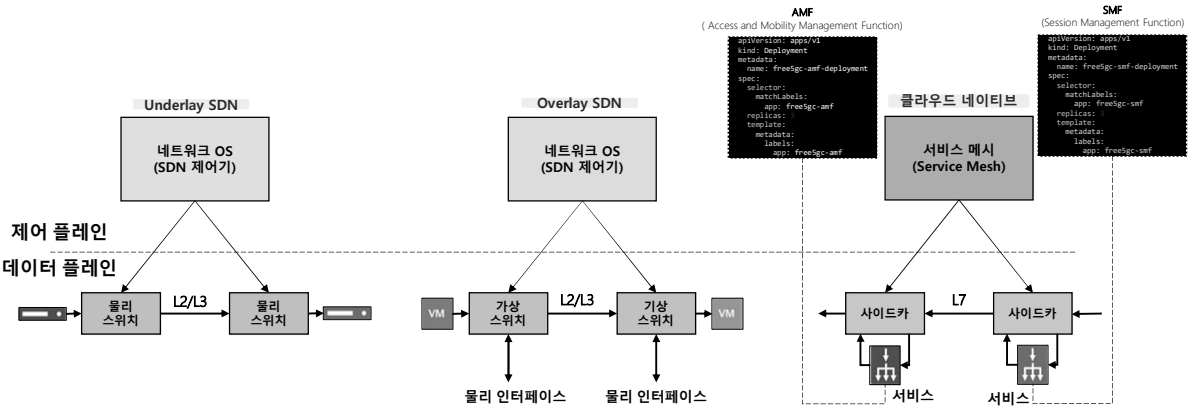
Source: https://www.hashicorp.com/products/consul/multi-platform-service-mesh

34

SDN (가상 네트워크)

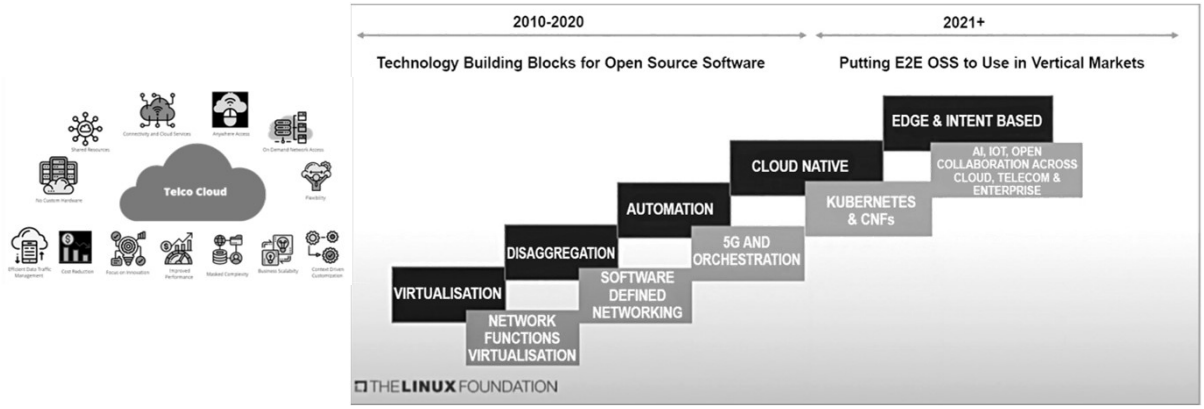
❖ **SDN** (소프트웨어 정의 네트워킹)

- **오버레이 SDN의 분산처리: dSwitch, dRouter, dFW, dLB (VM 이동시 보안 정책 유지)**
- **전용 제어기(SDN Controller) 사용**
- **Overlay/Underlay (물리/가상) 연결: VxLAN 프로토콜 사용 (VLAN, Multicast, VxLAN 헤더)**



LF EDGE PROJECTS

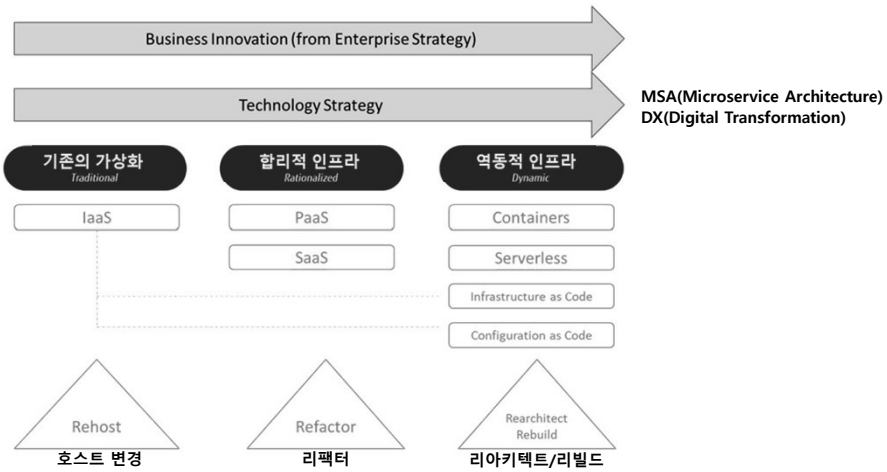
❖ **Focus shifting from building blocks to putting E2E OSS to use (Linux Foundation)**



Source: https://www.electronicsforu.com/technology-trends/open-source-ecosystem-5g-telecom-networks

멀티클라우드 전략

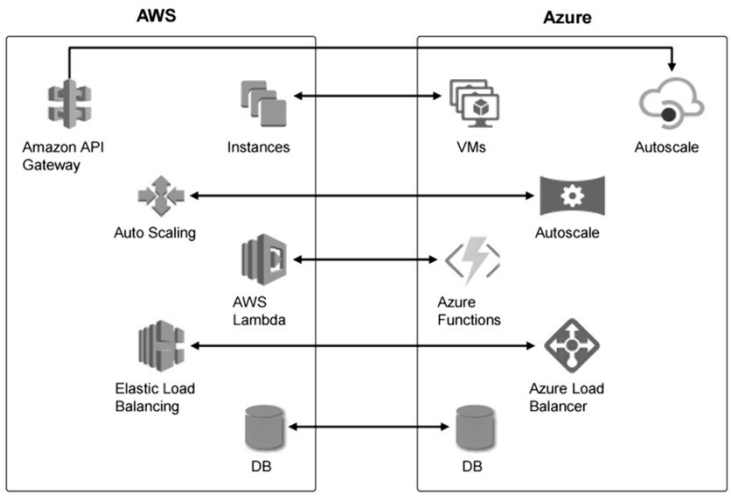
❖ Technology strategy following business innovation



Source: Mulder, Jeroen. Multi-Cloud Architecture and Governance: Leverage Azure, AWS, GCP, and VMware vSphere to build effective multi-cloud solutions (p. 83). Packt Publishing. Kindle Edition.

동일 서비스 고려

❖ 동일 서비스 고려하는 Multi-Cloud Architecture



멀티클라우드 환경의 도전

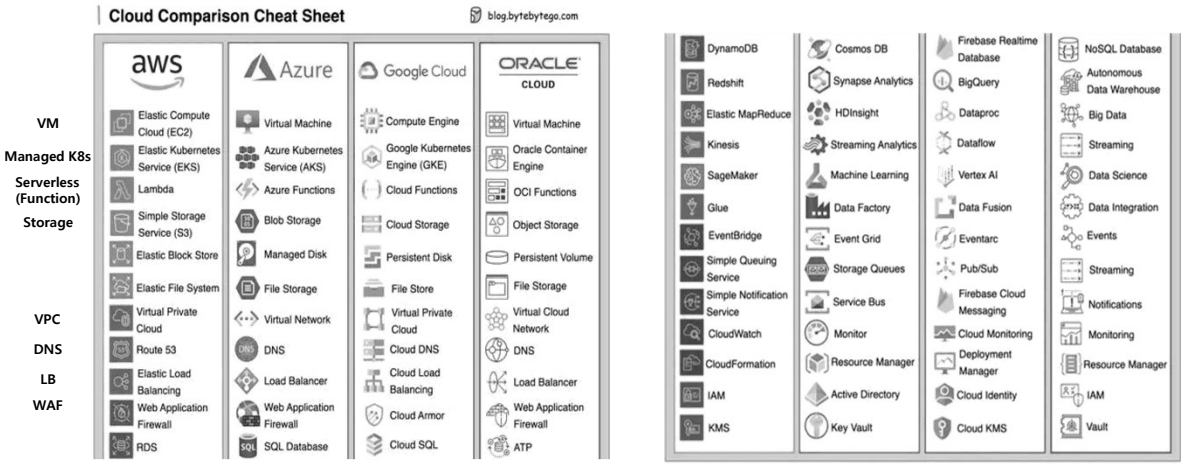
❖ Challenges in multi-cloud environment (도전 과제)

- Managing and monitoring multiple clouds
- Network bandwidth and latency rates
- Platform integration for multi cloud
- Scaling across multiple cloud
- Ensuring governance
- Work portability
- Spiraling
- Availity of skilled staff
- Financial management in multi
- Security

Source: 'Operationalizing Multi-Cloud Environments', Technologies, Tools and Use Cases, B. S. Rajeshwari, Pethuru Raj, Ramkumar Thirunavukarasu (2022)

AWS, GCP, AZURE

❖ Cloud Computing AWS, GCP, Azure

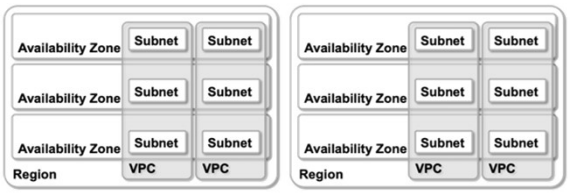


Source: https://www.facebook.com/groups/cloudcomputinglearn/permalink/2293891134128116/?sfnsn=mo&ref=share&mibextid=VhDh1V

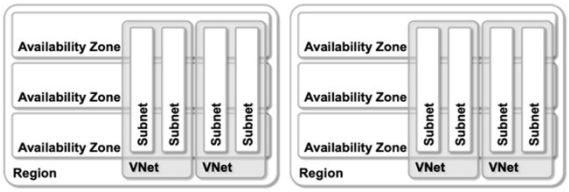
VIRTUAL NETWORKS AND SUBNETS

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

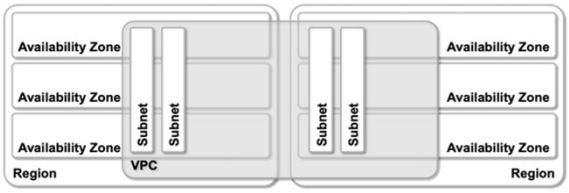
VPCs and subnets in AWS



VNet and subnets in Azure



GCP VPCs and subnets

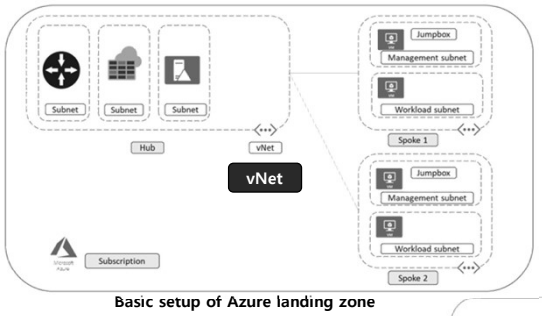


Source: https://blog.ipspace.net/2021/02/vpc-subnets-aws-azure-gcp.html

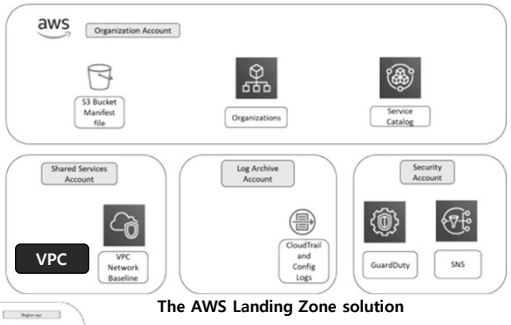
MULTI-CLOUD LANDING ZONE

❖ Creating a multi-cloud landing zone and blueprint

• landing zone: 구현을 위한 클라우드 서비스 세트



Basic setup of Azure landing zone



The AWS Landing Zone solution

Basic setup of a project in GCP, using Compute Engine and Cloud SQL

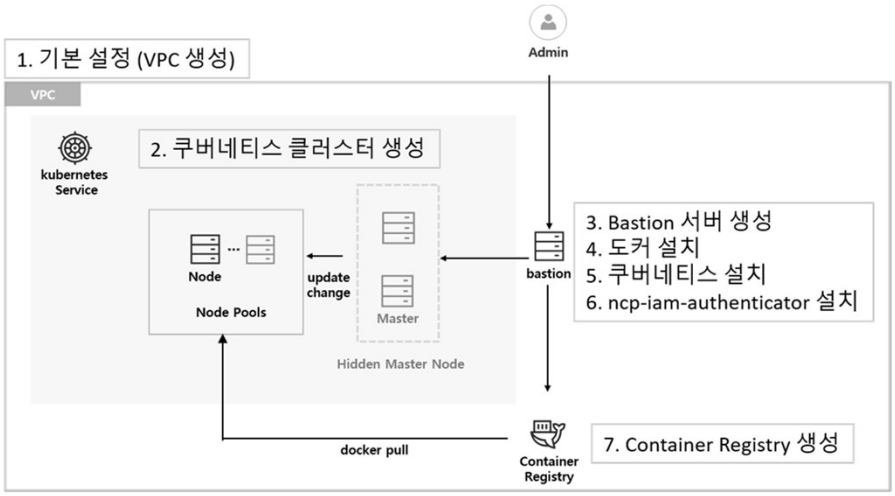
AWS 랜딩존

❖ IaaC (예): Terraform

Source: https://brunch.co.kr/@topasvga/2797

MANAGED K8S

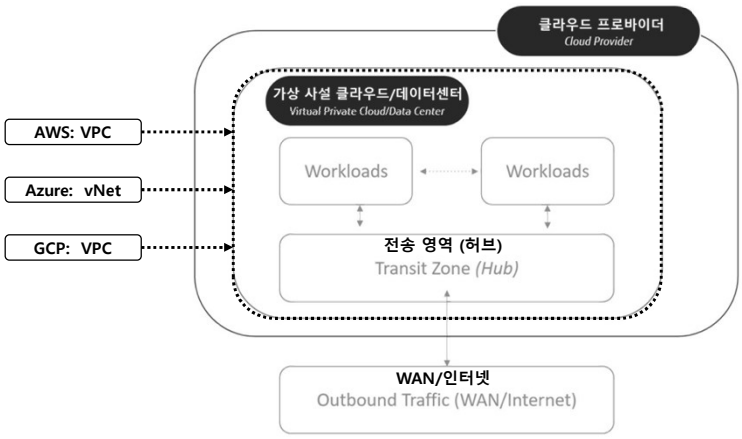
❖ Managed K8s Service (Naver Cloud)



Source: https://hong-jelly.tistory.com/9?fbclid=IwAR3_4a5k1Wl3-UiCiXp68ht6fVH_nSQv9xMvnY7y7VLYYUU9xsvZlpBaKJ8

하이레벨 멀티클라우드 가상데이터센터

❖ High-level diagram of a virtual private cloud/data center



Source: Mulder, Jeroen. Multi-Cloud Architecture and Governance: Leverage Azure, AWS, GCP, and VMware vSphere to build effective multi-cloud solutions (p. 74). Packt Publishing. Kindle Edition.

CSP 네트워크 용어

❖ CSP 네트워크 용어 (terminology alignment)

	aws	Azure	Google Cloud
Compute:	EC2 Instance	Virtual Machine (VM)	Compute Engine VMs
Object Storage:	S3	Blob Storage	Cloud Storage
가상 데이터센터 Logical Data Centre:	VPC VPC	vNet VNet	VPC VPC
전용선 Private Connectivity (L2):	Direct Connect Direct Connect	ExpressRoute ExpressRoute	Interconnect Interconnect
Route Gateways:	TGW, VGW, DGW	VNet Gateway	Cloud Router

- Virtual Private Gateway (VGW)
- Direct Connect Gateway (DGW)
- Transit Gateway (TGW)

Source: https://www.megaport.com/blog/comparing-cloud-providers-private-connectivity/

CSP의 주요 네트워크 서비스

❖ CSP의 주요 네트워크 서비스 (예): Key network services for AWS, Azure, and GCP

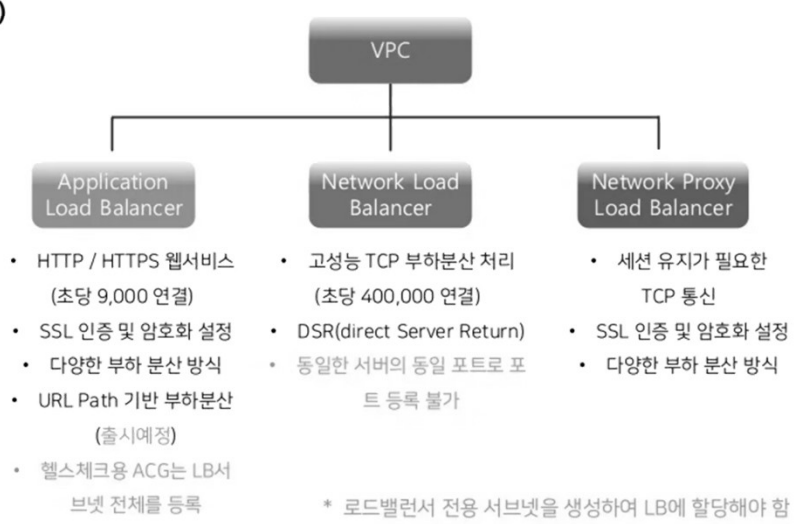
Cloud Platform	Amazon Web Services (AWS)	Microsoft Azure	Google Cloud Platform (GCP)
Virtual Network	Amazon Virtual Private Cloud (VPC)	Virtual Networks (VNets)	Virtual Private Cloud
Data Center integration	Direct Connect	ExpressRoute	Google Cloud Interconnect
Load Balancer	Elastic Load Balancer	Load Balancer	Google Cloud Load Balancing
DNS	Amazon Route 53	Azure DNS	Google Cloud DNS
Firewall	AWS Firewall / Web Application Firewall	Azure Firewall	Google Cloud firewalls

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

로드밸런서

❖ 네이버클라우드플랫폼 (2020)

• 로드밸런서



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

CSP 의 네트워킹 서비스

❖ Networking services compared: AWS vs Azure vs Google Cloud

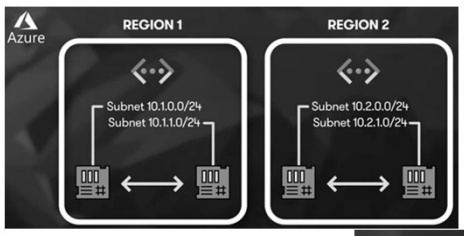
• 가상 사설 데이터센터, BGP, VPN, 전용선, 방화벽

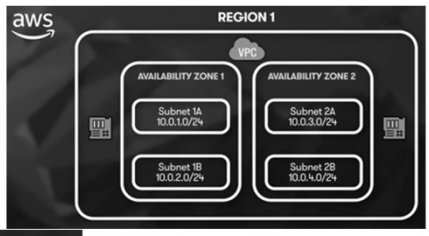
Source: https://acloudguru.com/blog/engineering/networking-services-compared-aws-vs-azure-vs-google-cloud

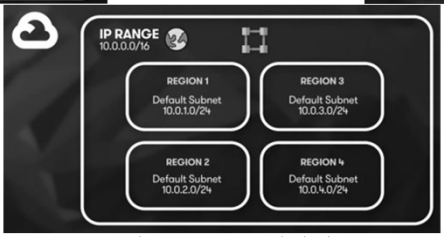
NETWORKING SERVICES

❖ Networking services compared: AWS vs Azure vs Google Cloud

• Networking basics







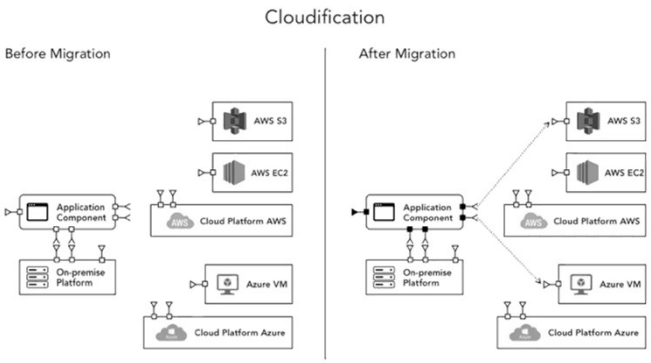
Source: https://acloudguru.com/blog/engineering/networking-services-compared-aws-vs-azure-vs-google-cloud

멀티클라우드 아키텍처 설계 (1 OF 7)

- **Workload Placement:** 지연 시간, 데이터 민감도, 비용과 같은 요소를 기반으로 어떤 워크로드를 어떤 클라우드에서 실행해야 하는지 지연 시간, 데이터 민감도, 비용과 같은 요소를 기반으로 어떤 워크로드를 어떤 클라우드에서 실행해야 하는지 결정지연 시간, 데이터 민감도, 비용과 같은 요소를 기반으로 어떤 워크로드를 어떤 클라우드에서 실행해야 하는지 결정결정
- **Data Management:** 클라우드 전반에서 데이터 스토리지, 복제 및 백업 전략을 계획, 데이터 주권 및 규제 요건을 고려
- **Network Design:** 온프레미스 인프라와 여러 클라우드 간의 안정적이고 안전한 연결을 보장하며, 효율적인 데이터 전송을 위한 전략 구현
- **Security:** 모든 클라우드를 아우르는 암호화, ID 관리, 액세스 제어를 통해 강력한 보안 프레임워크를 설계
- **Scaling and Performance:** 확장성 및 성능 최적화를 위한 설계. 자동 확장, 로드 밸런싱, 콘텐츠 전송 네트워크를 활용

멀티클라우드 아키텍처 설계 (2 OF 7)

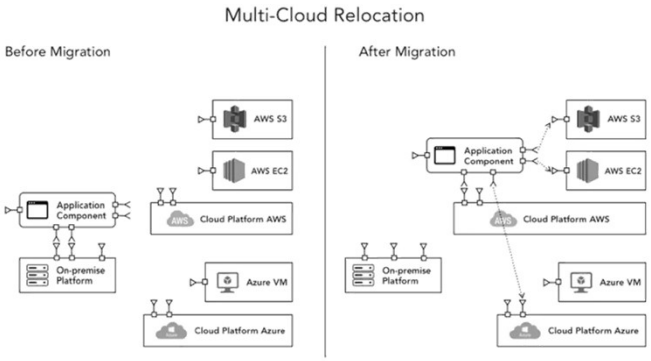
- **Cloudification**
- **Multi-Cloud Relocation**
- **Multi-Cloud Refactor**
- **Multi-Cloud Rebinding**
- **Multi-Cloud Rebinding w/Cloud Brokerage**
- **Multi-application Modernization**



Source: https://www.simform.com/blog/multi-cloud-architecture/

멀티클라우드 아키텍처 설계 (3 OF 7)

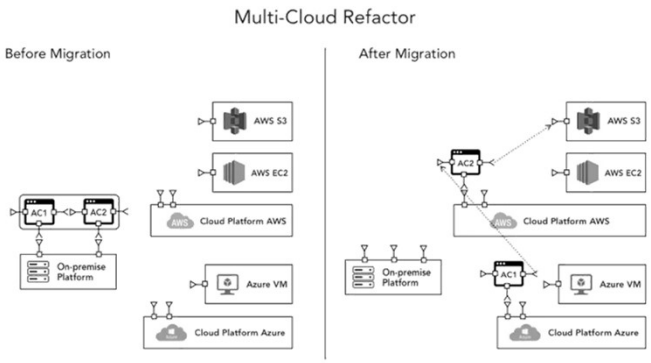
- Cloudification
- Multi-Cloud Relocation
- Multi-Cloud Refactor
- Multi-Cloud Rebinding
- Multi-Cloud Rebinding w/Cloud Brokerage
- Multi-application Modernization



Source: https://www.simform.com/blog/multi-cloud-architecture/

멀티클라우드 아키텍처 설계 (4 OF 7)

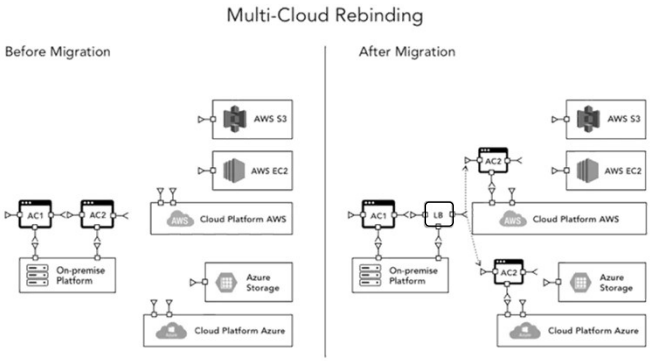
- Cloudification
- Multi-Cloud Relocation
- Multi-Cloud Refactor
- Multi-Cloud Rebinding
- Multi-Cloud Rebinding w/Cloud Brokerage
- Multi-application Modernization



Source: https://www.simform.com/blog/multi-cloud-architecture/

멀티클라우드 아키텍처 설계 (5 OF 7)

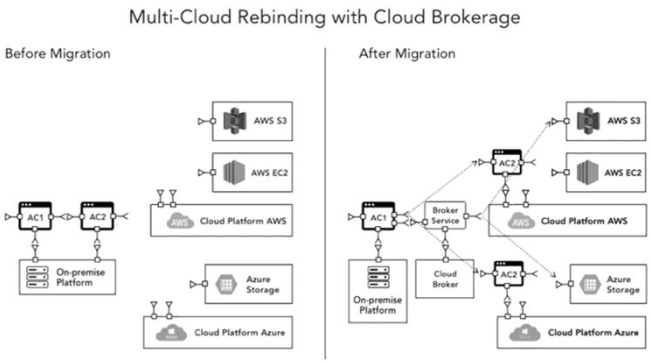
- Cloudification
- Multi-Cloud Relocation
- Multi-Cloud Refactor
- Multi-Cloud Rebinding
- Multi-Cloud Rebinding w/Cloud Brokerage
- Multi-application Modernization



Source: https://www.simform.com/blog/multi-cloud-architecture/

멀티클라우드 아키텍처 설계 (6 OF 7)

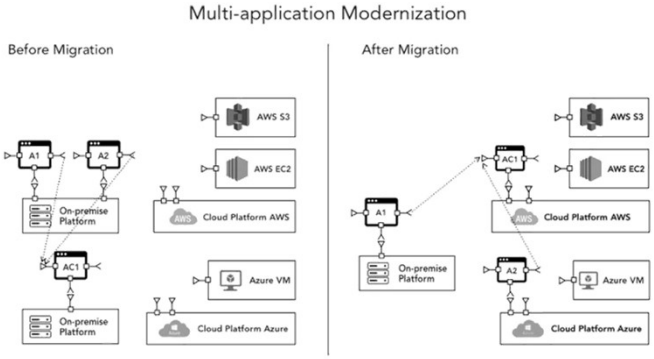
- Cloudification
- Multi-Cloud Relocation
- Multi-Cloud Refactor
- Multi-Cloud Rebinding
- Multi-Cloud Rebinding w/Cloud Brokerage
- Multi-application Modernization



Source: https://www.simform.com/blog/multi-cloud-architecture/

멀티클라우드 아키텍처 설계 (7 OF 7)

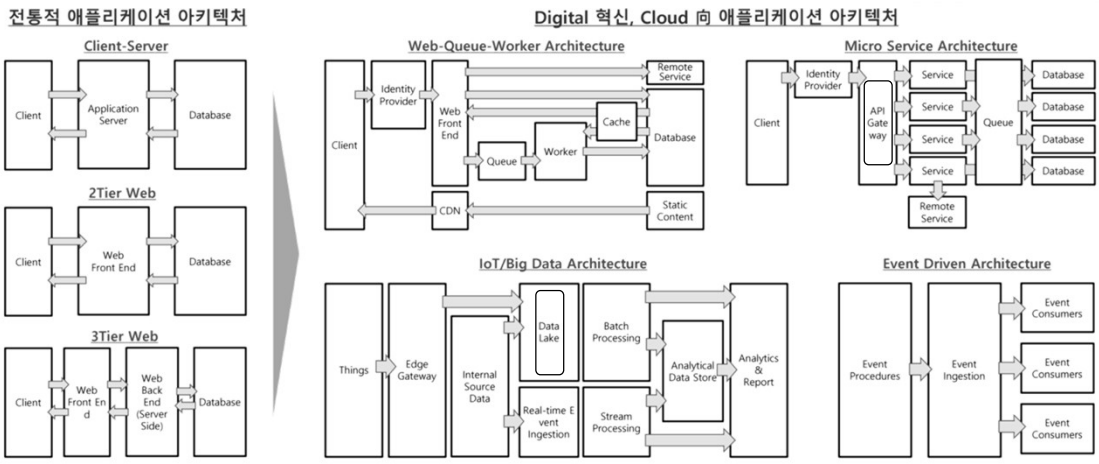
- ❖ Cloudification
- ❖ Multi-Cloud Relocation
- ❖ Multi-Cloud Refactor
- ❖ Multi-Cloud Rebinding
- ❖ Multi-Cloud Rebinding w/Cloud Brokerage
- ❖ Multi-application Modernization



Source: https://www.simform.com/blog/multi-cloud-architecture/

아키텍처 변화

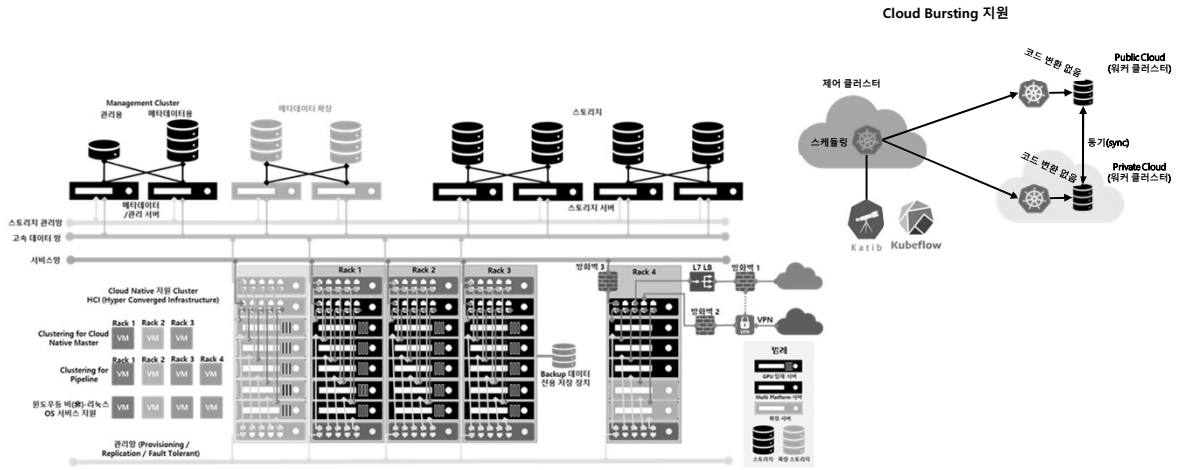
- ❖ VMware, 굿모닝아이텍㈜ (예)



Source: VMware, 굿모닝아이텍㈜

CLOUD BURSTING

❖ Cloud Bursting



LUSTRE의 확장성과 성능

❖ Lustre scalability and performance numbers

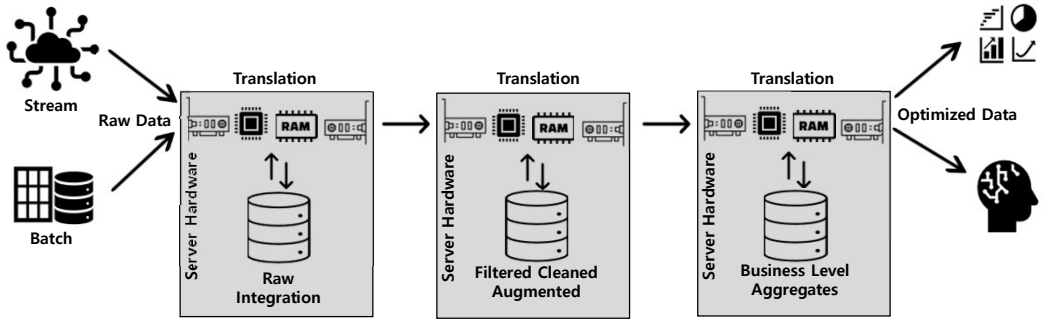
Feature	Current Practical Range	Known Production Usage
Client Scalability	100 - 100,000	50,000+ clients, many in the 10,000 to 20,000 range
Client Performance	*Single client*: 90% of network bandwidth *Aggregate*: 10 TB/s	*Single client*: 4.5 GB/s (FDR IB, OPA1), 1000 metadata ops/sec *Aggregate*: 2.5 TB/s
OSS Scalability	*Single OSS*: 1-32 OSTs per OSS *Single OST (ldiskfs)*: 300M objects, 256TiB per OST *Single OST (ZFS)*: 500M objects, 256TiB per OST *OSS count*: 1000 OSSs w/ up to 4000 OSTs	*Single OSS (ldiskfs)*: 32x8TiB OSTs per OSS, 8x32TiB OSTs per OSS *Single OSS (ZFS)*: 1x72TiB OST per OSS *OSS count*: 450 OSSs w/ 1000 4TiB OSTs, 192 OSSs w/ 1344 8TiB OSTs, 768 OSSs w/ 768 72TiB OSTs
OSS Performance	*Single OSS*: 15 GB/s *Aggregate*: 10 TB/s	*Single OSS*: 10 GB/s *Aggregate*: 2.5 TB/s
MDS Scalability	*Single MDS*: 1-4 MDTs per MDS *Single MDT (ldiskfs)*: 4 billion files, 8 TiB per MDT *Single MDT (ZFS)*: 64 billion files, 64 TiB per MDT *MDS count*: 256 MDSs w/ up to 265 MDTs	*Single MDS*: 3 billion files *MDS count*: 7 MDSs w/ 7x 2 TiB MDTs in production (256 MDSs w/ 256 64 GiB MDTs in testing)
MDS Performance	50,000 create ops/sec, 200,000 metadata stat ops/sec	15,000 create ops/sec, 50,000 metadata stat ops/sec
File system Scalability	*Single File (max size)*: 32 PiB (ldiskfs) or 2^{63} bytes (ZFS) *Aggregate*: 512 PiB total capacity, 1 trillion files	*Single File (max size)*: multi-TiB *Aggregate*: 55 PiB capacity, 8 billion files

Source: https://wiki.lustre.org/Understanding_Lustre_Internals

▪ Pipeline 과 데이터 인프라

❖ Data Pipeline 과 데이터 인프라 (물리 계층/가상화 계층)

- 오픈소스 Spark의 경우 배치(Batch) 데이터는 물론 스트림(Stream) 데이터 프로세싱이 가능하다.
- 데이터 전처리를 위한 파이프라인 속도는 네트워크와 스토리지의 성능이 영향을 준다

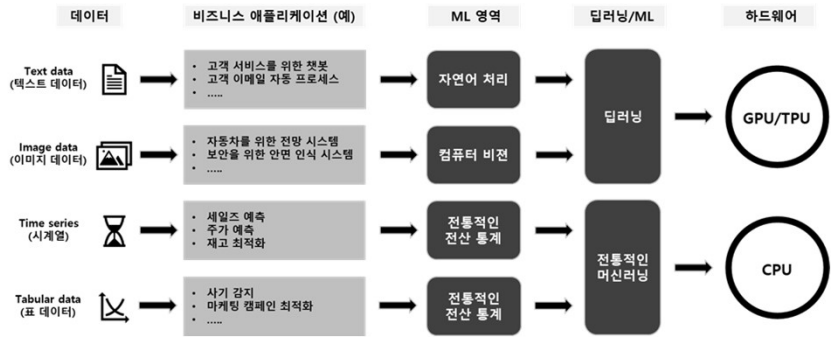


네트워크 가속 기술: 물리적 네트워크 하드웨어 속도와 함께 가상화 네트워크를 위한 오픈소스 기반의 SDN, DPDK, DVR, eBPF 기술 등이 사용 될 수 있다.
Source: 스토리지 가속 기술: 오프로드 기술이나 NVMe등의 물리적인 장치와 함께 소프트웨어 적인 분산처리 등이 사용 될 수 있다.

▪ From Data to Machine

❖ From Data to Machine

- 소재 데이터는 장기적으로 이미지 테이터 처리와 AI/ML 등의 분석이 증가하여 GPU나 TPU 기반의 처리가 증가하는 것에 대응 할 수 있다.

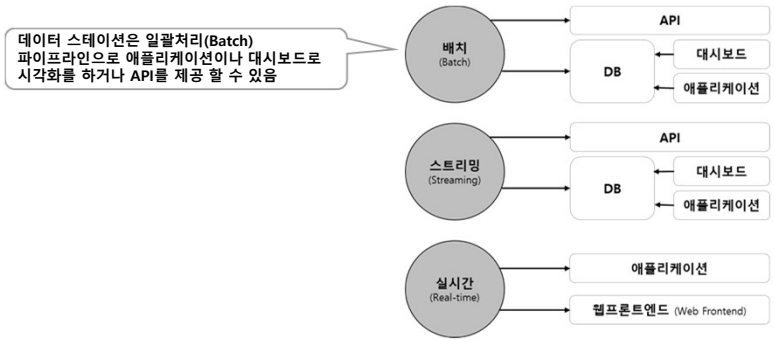


Source: Data를 저장하는 스토리지의 GPU Direct 기술을 사용하면 Data를 CPU를 오프로드하여 GPU로 직접 전달 할 수 있다.

▪ 데이터 분석 및 시각화

❖ 데이터 분석 및 시각화

- 데이터 분석은 데이터를 수집하고 정리하여 의미 있는 정보를 추출하는 과정
- 데이터 분석을 통해 데이터의 특징이나 패턴을 파악하고, 이를 바탕으로 의사결정

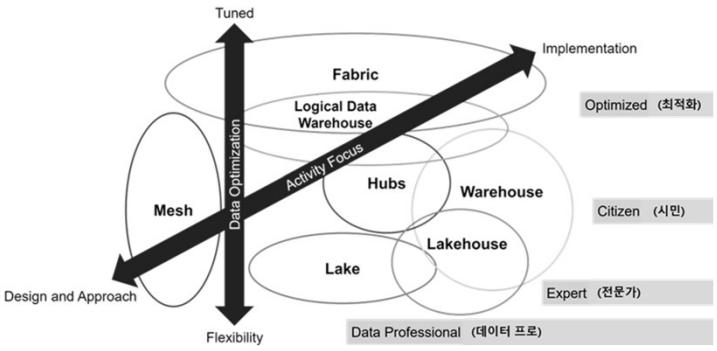


파이썬에서는 matplotlib ,Seaborn, Plotly, Bokeh 등 다양한 라이브러리를 활용하여 데이터 시각화를 할 수 있다.
Source: Tuulos, Ville. Effective Data Science Infrastructure: How to make data scientists productive

▪ 시장 (Gartner 2022)

❖ Data & Analytics Governance Platforms (Gartner 2022)

- 데이터 패브릭 기술은 최적화를 위해 튜닝/구현(Tuned/Implementation) 강화
- 비교 데이터/분석 기술
  - Lake
  - Lakehouse
  - Hubs
  - Warehouse
  - Logical Warehouse
  - Mesh
  - Fabric



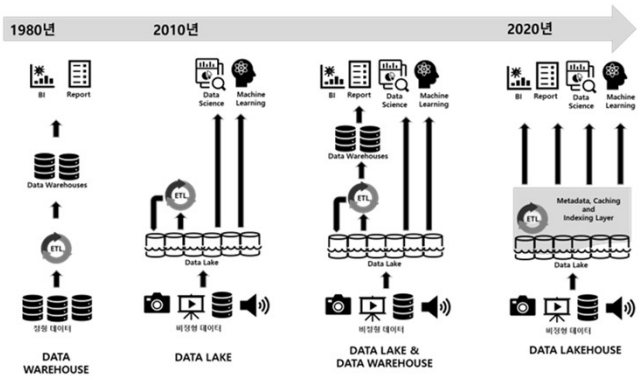
데이터 메시(Data Mesh): 분산된 아키텍처 프레임워크를 사용하는 데이터 관리에 대한 접근 방식
Source: Data & Analytics Governance Platforms (Gartner 2022)

▪ 데이터 아키텍처의 발전

❖ **Data architecture (데이터 아키텍처) or Data Storage Frameworks**

❖ **데이터 패브릭 기술은 아래 기술들을 사용**

- **Data Warehouse**
- **Data Lake**
- **Data Lakehouse**

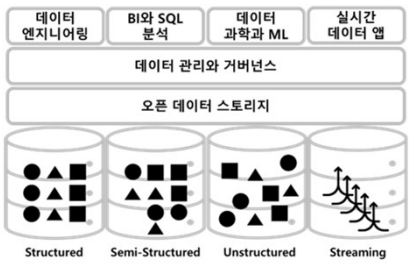


ETL: 추출(Extract), 변환(Transform), 로드(Load)
데이터 레이크하우스(lakehouse): 데이터 웨어하우스의 데이터 구조 및 관리 기능과 데이터 레이크에 사용되는 저비용 스토리지를 결합하는 접근 방식

▪ 레이크 하우스(Lake House)

❖ **레이크 하우스(Lake House)**

- **모든 데이터 유형을 지원하며, 원시 데이터를 보관하는 등록 서비스**
- **원시데이터의 메타정보와 태그 관리로 원하는 데이터의 빠른 검색 서비스**
- **데이터 제공에 적합한 알고리즘과 프레임워크 기반 분석**
- **데이터 자동화 처리의 병목 구간 없이 데이터 통합을 지원하는 무한 확장**



비즈니스 인텔리전스(BI): 데이터를 분석하고 실행 가능한 정보를 제시하여 경영진, 관리자 및 기타 사용자가 정보에 입각한 비즈니스 의사 결정을 내릴 수 있도록 지원하는 기술 중심 프로세스. 데이터에 대한 쿼리를 개발/실행, 보고서, 대시보드 및 데이터 시각화로 기업의 의사 결정자와 운영자가 분석 결과를 사용할 수 있는 도구, 애플리케이션 및 방법론을 포괄

▪ 시스템 구성

❖ 소재 데이터 분석을 위한 시스템 구성

- 서비스 기능 영향
- Data Volume 영향

- 영향 영역 표시 -

서비스 기능 영향

Data Volume 영향

정형 데이터 분석은 시스템 인프라의
- 서비스 기능과
- Data Volume에 영향이 있다.

가상화 계층의 가상 머신의 성능 개선을 위한 구성 튜닝 요소
- vCPU
- vRAM
- vNIC
- vGPU
- vSAN (or Ceph): VM에서 Ceph 접속 성능 이슈

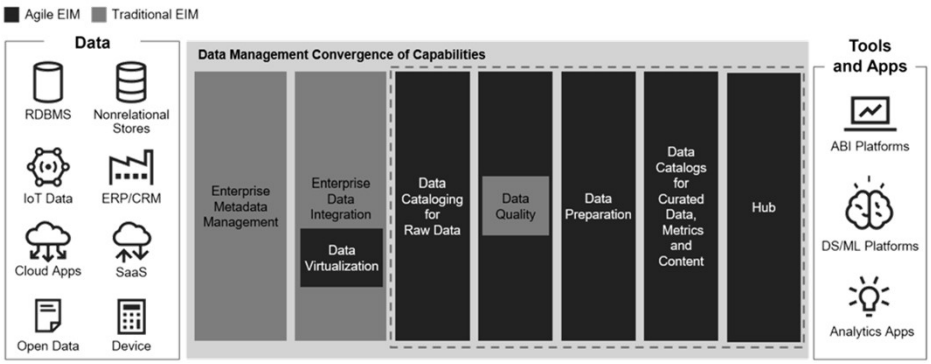
구분	Use Case (예측 관리)	정형 데이터 분석
사용자 인터페이스와 서비스	Security Overlay	Security Overlay
	Workload governance	Workload governance
	Workload management	Workload management
	Workload Provisioning	Workload Provisioning
워크로드	Use cases	Use cases
	머신러닝	머신러닝
	데이터 라이프 사이클	데이터 라이프 사이클
컴퓨팅	CPU	CPU
	GPU	GPU
	Memory	Memory
스토리지	레거시 (HDD 등)	레거시 (HDD 등)
	소프트웨어정의 (HCI)	소프트웨어정의 (HCI)
	NAS	NAS
네트워킹	IP-VPN	IP-VPN
	이더넷/소프트웨어정의(SDN)	이더넷/소프트웨어정의(SDN)
	LTE/5G	LTE/5G
환경	온프레미스	온프레미스
	코로케이션	코로케이션
	하이브리드 클라우드	하이브리드 클라우드
	퍼블릭 클라우드	퍼블릭 클라우드

API: Application Programming Interface, AI/ML/DL: 인공지능(AI), 머신러닝(ML)과 딥러닝(DL)

▪ 기능의 융합

❖ 시장은 데이터 관리의 '기능의 융합(a Convergence of Capabilities)'을 요구 (Gartner 2022)

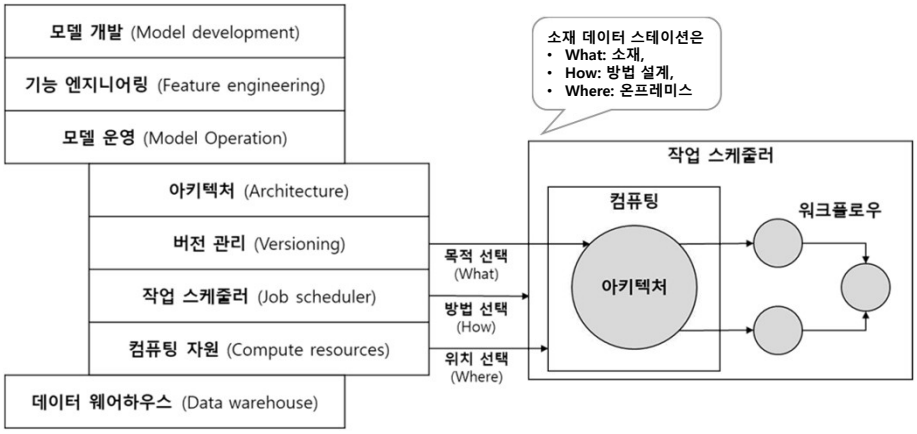
- Data Catalog
- Data Quality
- Data Preparation
- Hub



데이터 카탈로그(Data Catalog): 기업의 데이터 자산 목록으로 사용자가 필요한 정보를 빠르게 찾을 수 있도록 한다.
Source: Data & Analytics Governance Platforms (Gartner 2022)

▪ What, How, Where

❖ 워크플로우 실행의 세가지 고려 사항: What(데이터), How(방법 설계), Where(온프레미스)

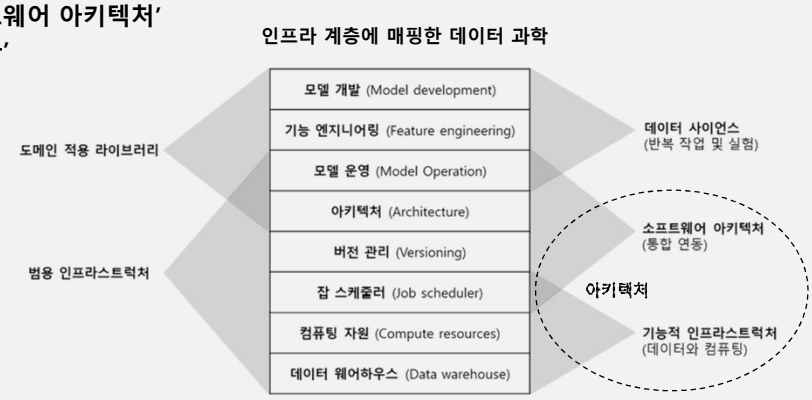


온프레미스 컴퓨팅 자원(Where)과 설계에 사용하는 소프트웨어(How) 등을 고려하여 소재 데이터(What)에 필요한 구성

▪ 인프라 계층에 매핑

❖ 인프라 계층에 매핑한 데이터 과학 프로젝트의 구성 요소

- 반복 작업 및 실험을 하는 '데이터 사이언스'
- 하드웨어를 통합 연동하는 '소프트웨어 아키텍처'
- 데이터와 컴퓨팅의 '기능적 인프라'

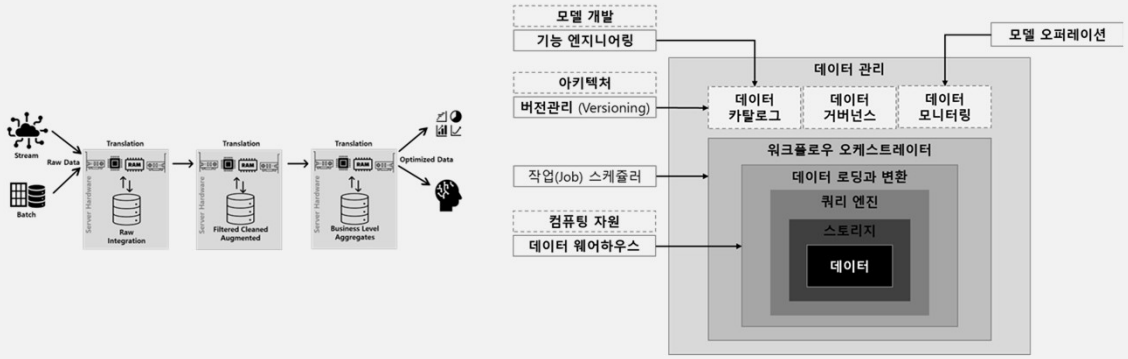


범용 인프라스트럭처: 모델 운영, 아키텍처, 버전관리, 잡 스케줄러, 컴퓨팅 자원, 데이터 웨어하우스
도메인 적용 라이브러리: 모델 개발, 기능 엔지니어링, 모델 운영, 아키텍처

▪ 데이터 과학과 인프라

❖ 데이터 과학 스택과 데이터 인프라의 관계

- 데이터 웨어하우스와 컴퓨팅 자원은 데이터 플랫폼 상의 데이터와 스토리지와 관련
- 소프트웨어 아키텍처는 데이터의 전처리를 위한 작업과 버전 관리(Versioning)에 영향



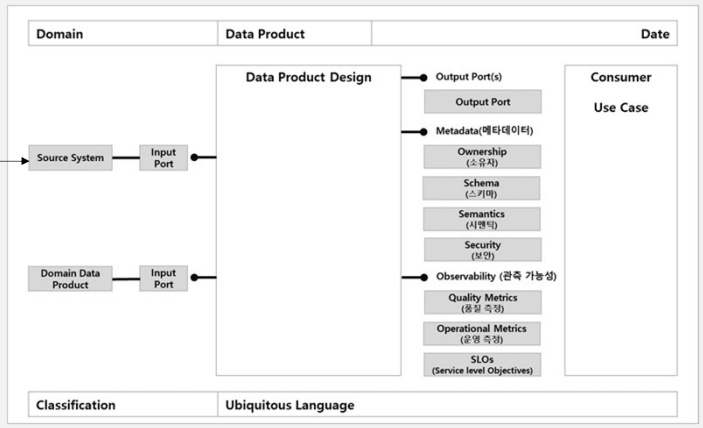
데이터 카탈로그는 모델을 개발하는 기능 엔지니어링과 버전 관리를 위한 아키텍처 등이 연계된다.
워크플로우의 오케스트레이션은 작업들을 스케듈링 한다.

▪ Data Product Canvas

❖ Data Product Canvas에서 고려하는 데이터 플랫폼은 일반적으로 아래의 Canvas 기능을 제공

- 검색 바
- 데이터 개요.
- 데이터 시각화
- 머신 러닝 모델
- 데이터 필터
- 데이터 내보내기

Data Product Canvas



Data Product Canvas: 사용자 관점의 데이터 제품 플랫폼 서비스는 편리한 서비스와 데이터의 활용을 위한 체계가 중요하여 사용자 요구를 설계에 반영하기 위한 도구
Source: https://www.datamesh-architecture.com/data-product-canvas

▪ 데이터 카탈로그

❖ 데이터 카탈로그

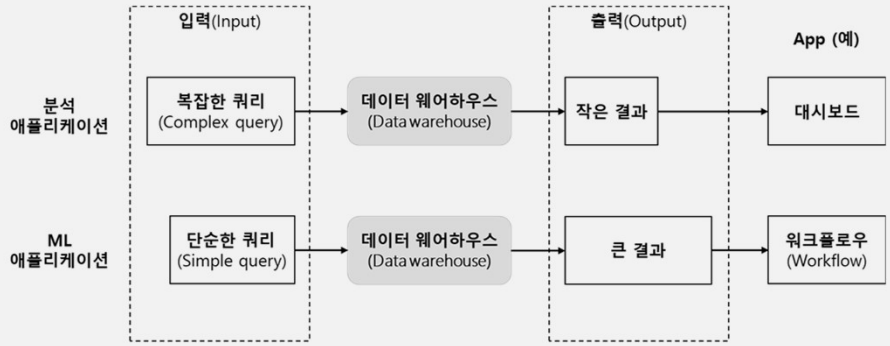
- 사용자가 필요한 정보를 빠르게 찾을 수 있도록 하는 데이터 자산 목록
- 카탈로그는 대부분 다른 데이터에 대한 기본 정보를 제공하고 그것이 무엇인지 설명하는 '메타데이터'
- 사용자는 데이터 관리 및 검색 도구와 결합한 데이터 카탈로그를 가진다

Source: https://www.tibco.com/ko/reference-center/what-is-a-data-catalog

▪ 분석 과 ML의 데이터 흐름

❖ 분석과 ML 애플리케이션의 데이터 흐름 비교

- 분석 애플리케이션은 대시보드로 표시
- ML 애플리케이션은 워크플로우를 사용

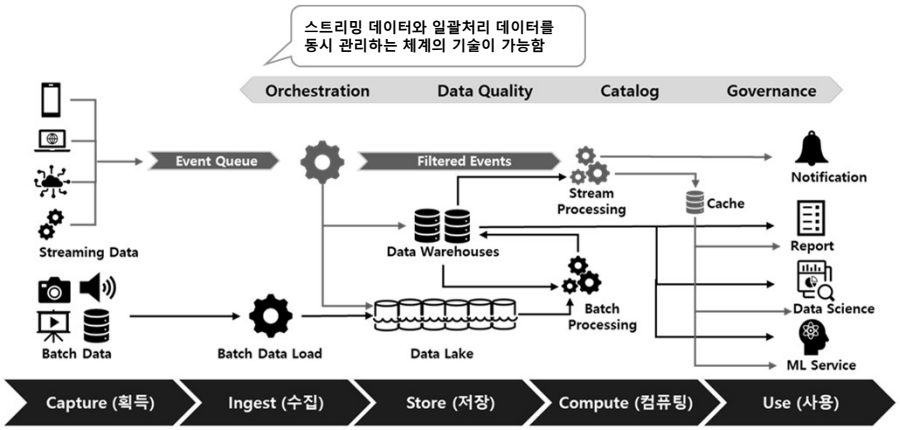


Source: 목적에 따라 데이터의 흐름에서 처리하는 방법이 다를 수 있고, 소재 데이터의 일반적인 특성을 대시보드에 표시하여 워크플로우 설계를 위한 서비스를 개선하는데 사용하여 병행

▪ 데이터 파이프라인

❖ 오픈소스로 구축 가능한 데이터 파이프라인 아키텍처

- Capture (획득)
- Ingest (수집)
- Store (저장)
- Compute (컴퓨팅)
- Use (사용)



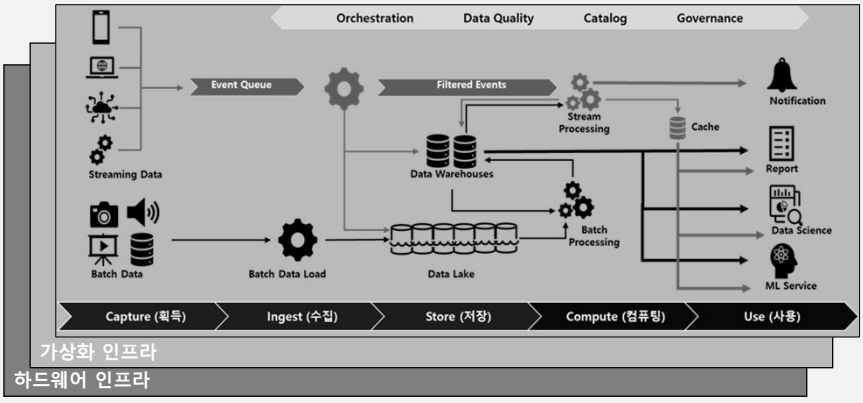
ETL: 추출(Extract), 변환(Transform), 로드(Load)

데이터 레이크하우스(lakehouse): 데이터 웨어하우스의 데이터 구조 및 관리 기능과 데이터 레이크에 사용되는 저비용 스토리지를 결합하는 접근 방식

▪ 인프라 계층화

❖ 인프라 계층화: 계층별 독립적 설계 구축

- 데이터 플랫폼 계층
- 가상화 인프라 계층
- 하드웨어 인프라 계층



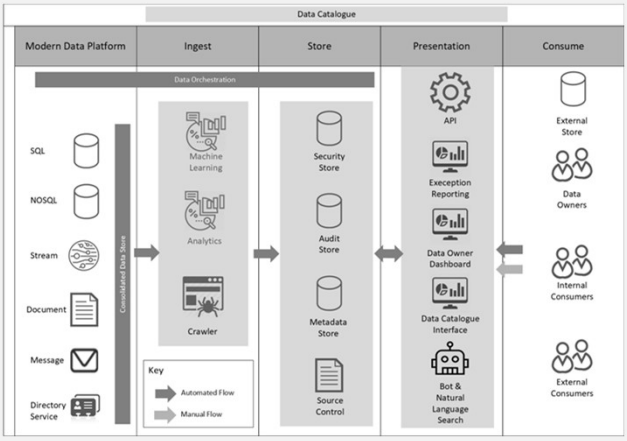
데이터 플랫폼 파이프라인의 최적의 성능을 위해 가상화 인프라와 하드웨어 인프라의 관련 기술을 고려한다.

▪ Architecture for Analytics

❖ Architecture for Analytics end-to-end with Azure Synapse

- **Data Catalogue Interface**
- **Bot & Natural Language Search**
- **Exception Reporting**
- **Data Owner Dashboard**
- **RESTful APIs**

The metadata store combines with the security store, audit store and source control to deliver all metadata known about any type of data asset. This is surfaced to the user using several different technologies, depending on the audience;

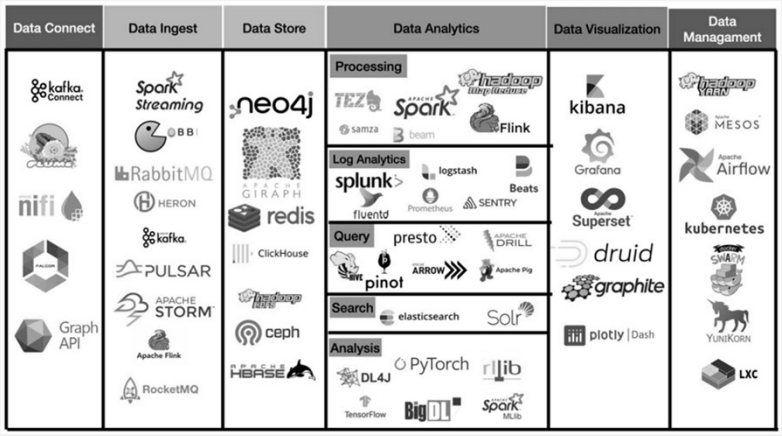


Source: https://www.risual.com/2019/03/modern-data-platform-data-catalogue/

77

▪ 데이터 오픈소스 (2 of 3)

❖ 데이터 엔지니어링을 위한 오픈소스 프레임워크

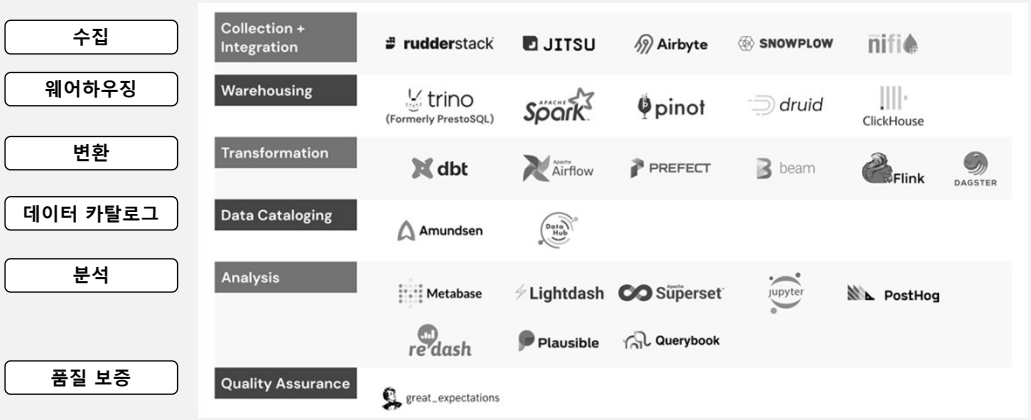


Source: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9743922&fbclid=IwAR08OlkAzEqezXobSwczEKsTIl--MLOrvgZfLZlG8jJYFaq5zHgj4BHu4Ns

78

▪ 데이터 오픈소스 (3 of 3)

❖ **The Modern Data Stack: Open-source Edition**

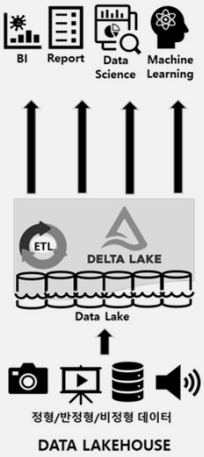


- 출처: https://www.datafold.com/blog/the-modern-data-stack-open-source-edition

▪ 오픈소스 'DELTA LAKE'

❖ **Data Lakehouse 플랫폼을 위한 오픈소스 'DELTA LAKE'**

- **데이터 레이크 위에 Lakehouse 아키텍처를 구축할 수 있는 오픈 소스 프로젝트**
- **Delta Lake는 ACID 트랜잭션, 확장 가능한 메타데이터 처리를 제공하고 S3, A인(Azure Data Lake Storage), GCS 및 HDFS와 같은 기존 데이터 레이크 위에 스트리밍 및 일괄 데이터 처리를 통합**
- **기존 데이터 레이크에 데이터 안정성을 제공하는 오픈 소스 스토리지 계층**
  - 원자성, 일관성, 격리, 내구성(ACID: Atomicity, consistency, isolation, durability) 트랜잭션 ACID 트랜잭션은 여러 데이터 파이프라인이 동일한 테이블에서 데이터를 안정적으로 동시에 읽고 쓸 수 있게 함
  - 확장 가능한 메타데이터 처리
  - 통합 스트리밍 및 일괄 데이터 처리



데이터 파이프라인에 대한 레이크하우스 접근 방식은 신뢰할 수 있는 실시간 분석을 가능하게 하는 스트리밍 데이터를 포함하여 향상된 생산성, 시스템 안정성 및 데이터 신뢰성을 위한 사례 제공

▪ 데이터 가상화 (1 of 2)

❖ **데이터 가상화란?**

- **데이터 가상화는 응용 프로그램이 마치 단일 위치에 모두 저장된 것처럼 서로 다른 여러 데이터 소스의 데이터에 액세스하고 결합할 수 있도록 하는 기술입니다. 데이터가 다른 위치, 형식 또는 구조로 저장될 수 있더라도 한 위치에 있는 것처럼 보이도록 기본 물리적 스토리지 및 스키마를 추상화하여 여러 소스에서 데이터의 가상 뷰를 생성합니다.**
- **데이터 가상화를 통해 조직은 데이터를 이동하거나 복제하지 않고도 데이터베이스, 파일 시스템 및 클라우드 서비스를 비롯한 다양한 소스의 데이터에 액세스하고 사용할 수 있습니다. 이는 물리적 데이터 소스 위에 위치하며 응용 프로그램이 데이터의 물리적 위치나 형식을 몰라도 데이터에 액세스할 수 있도록 하는 가상 데이터 계층을 사용하여 수행할 수 있습니다. 이를 통해 조직은 다음을 수행할 수 있습니다.:**
  - 다양한 소스에서 통합된 데이터 보기를 제공하여 데이터 액세스 및 관리를 개선합니다.
  - 데이터 이동 또는 복제 필요성을 제거하여 데이터 통합 및 데이터 품질 향상
  - 여러 데이터 복사본을 만들고 유지 관리할 필요가 없으므로 비용 절감 및 확장성 향상
  - 데이터 액세스 제어 및 관리를 중앙 집중화하여 보안 향상

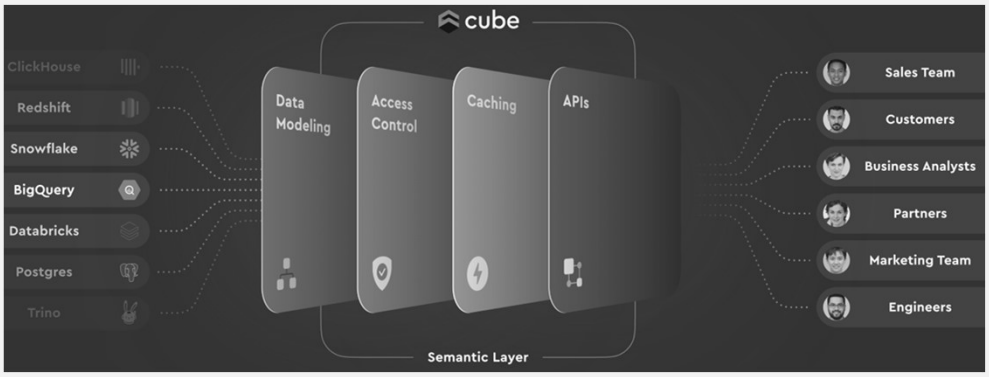
데이터 가상화는 데이터 웨어하우징, 비즈니스 인텔리전스, 빅 데이터 분석 및 데이터 통합 프로젝트에서 조직이 데이터를 더 잘 활용하고 더 빠르고 쉽게 통찰력을 얻을 수 있도록 하는 데 자주 사용된다.

81

▪ 데이터 가상화 (2 of 2)

❖ **데이터 가상화를 위한 Cube 구성 (예): 가상화를 위한 Sematic Layer 제안**

- **응답 시간이 빠르고 운영 애플리케이션을 많이 실행하지 않는 경우에 도움**



Dremio 경우 오픈소스 Apache Arrow 기술을 사용하여 많은 인메모리를 캐시하고 최적화할 뿐만 아니라 빠른 응답 시간을 단축
Source: https://cube.dev/use-cases/semantic-layer

82

▪ Databricks

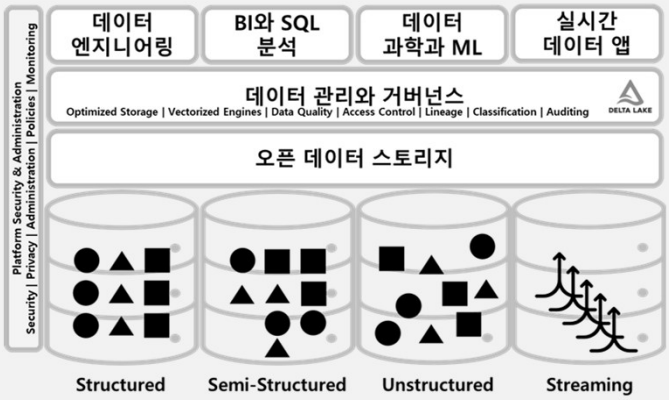
❖ **Databricks: Open-Source Data Lakehouse for AI+Data**

Source: https://www.toptechtopic.com/2022/01/databricks-open-source-data-lakehouse.html

83

▪ Lakehouse Platform (예)

❖ **DELTA LAKE를 사용하는 Databricks 사의 Lakehouse Platform (예)**



- 결합된 단일 클라우드 데이터 플랫폼 지원
- 데이터 웨어하우징과 기계 학습(ML) 통합
- 데이터 팀 효율성 증가
- 비용 절감
- 데이터 거버넌스 단순화
- 데이터 버전 관리 지원
- ETL 작업 단순화
- 데이터 중복 제거
- 직접 데이터 액세스 가능
- BI 도구에 직접 연결
- 보안 처리

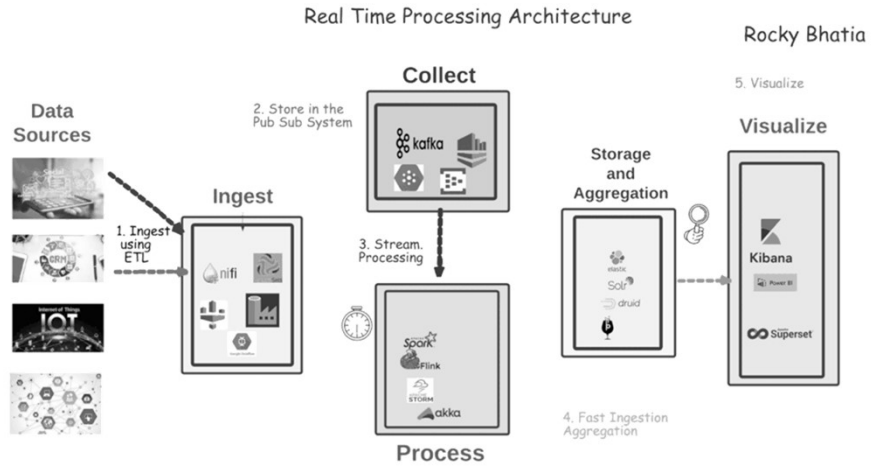
Databrick은 오픈소스 DELTA LAKE 기반으로 사업화
Source: https://www.databricks.com/wp-content/uploads/2021/11/The-Data-Lakehouse-Platform-For-Dummies-1.pdf

84

REAL TIME DATA PROCESSING

❖ Real Time Data Processing

ETL은 다양한 소스에서 데이터를 추출, 변환하고 이를 데이터 웨어하우스 또는 기타 통합 데이터 저장소에 로드하는 프로세스

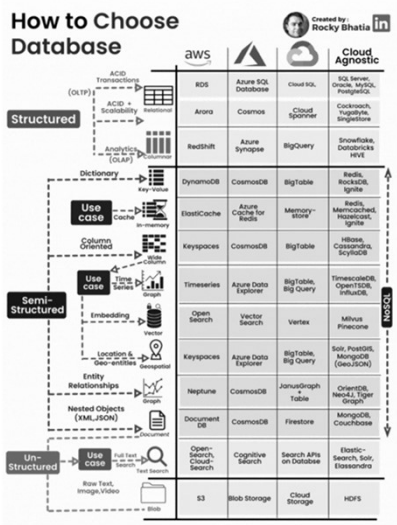


Source: https://www.linkedin.com/pulse/real-time-processing-architecture-rocky-bhatia

DATABASE LANDSCAPE

❖ Navigating the Database Landscape

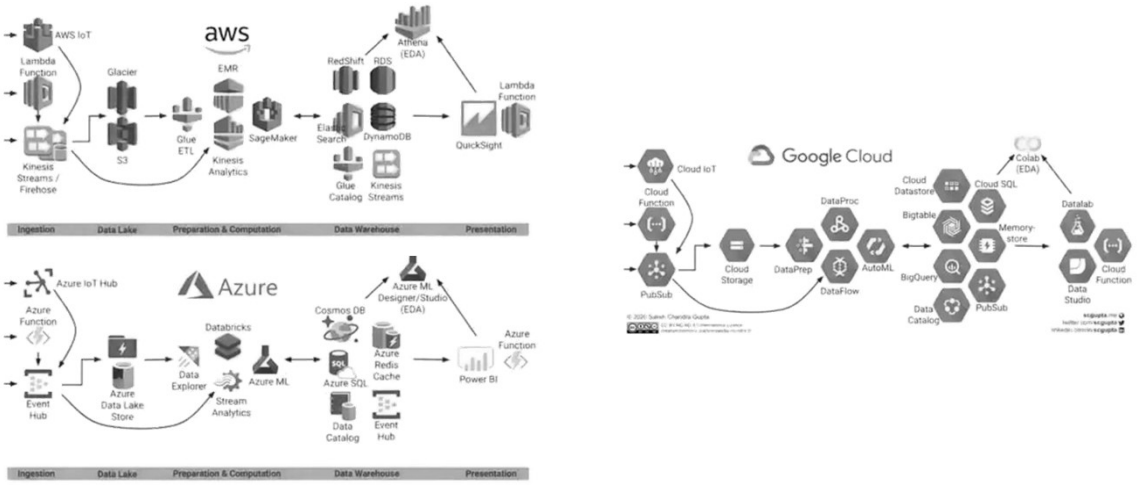
- Understand Your Data Requirements
- Identify Your Use Cases
- Scalability Requirements
- Data Consistency
- Query Complexity
- Data Model
- Compatibility with Technology Stack
- Future Growth



Source: https://www.linkedin.com/posts/rocky-bhatia-a4801010_navigating-the-database-landscape-choosing-activity-7114428781020246016-bvfu?utm_source=share&utm_medium=member_android&fbclid=IwAR39ol-t0LTPo8U7MhOBnztotwANMwwxa9omCnjTNuDeNIQOGk5VZHEWEo8

DATABASE LANDSCAPE

❖ Big Data Pipeline on AWS, MS Azure, and GCP

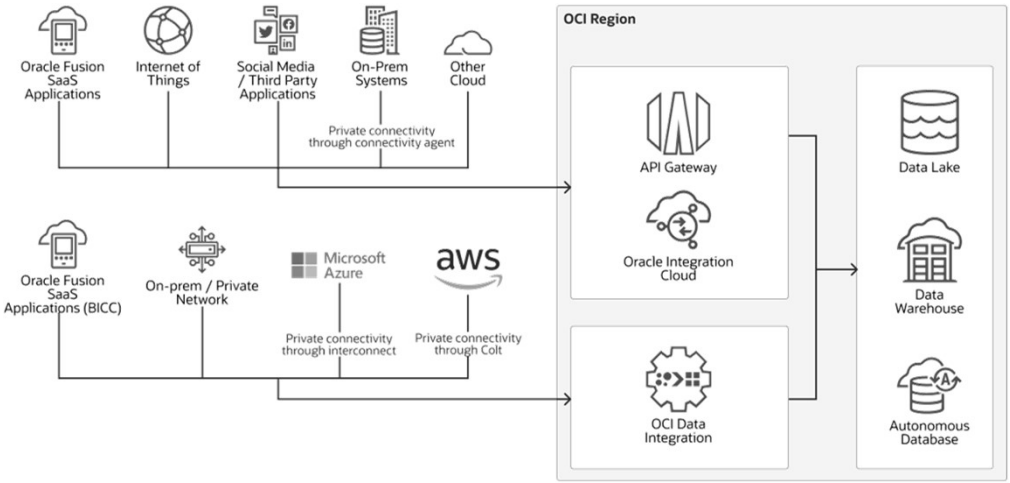


Source: scgupta.link/big-data-pipeline

87

데이터 레이크 통합

❖ 멀티 클라우드 데이터 레이크 통합 아키텍처의 데이터 플로우 (Oracle)

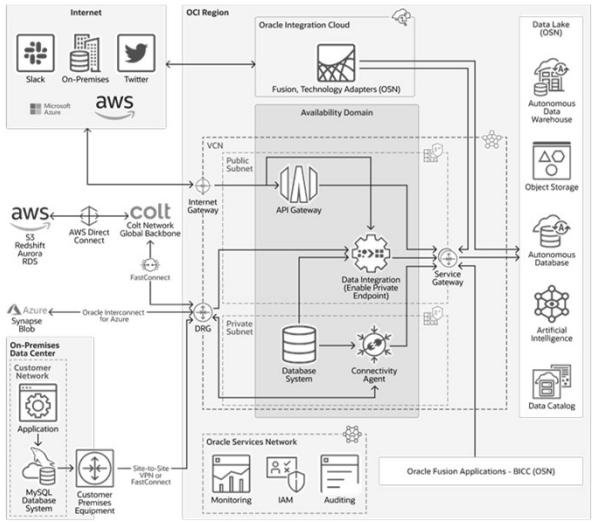


Source: https://docs.oracle.com/ko/solutions/oci-multicloud-datalake/index.html#GUID-845D05DE-3DD1-499B-85F6-3F132346A60D

88

데이터 레이크 통합 아키텍처

❖ 데이터 레이크 통합 아키텍처 (Oracle)



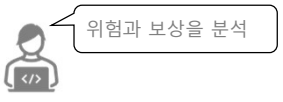
Source: https://docs.oracle.com/ko/solutions/oci-multicloud-datalake/index.html#GUID-845D05DE-3DD1-499B-85F6-3F132346A60D

89

MULTI-CLOUD 통합 비용 고려

❖ 3 rules to avoid high multi-cloud integration costs

- Rule 1. Don't spread components across clouds
- Rule 2. Don't use data centers or VPNs to funnel traffic between clouds
- Rule 3. Interact with data where it's stored
- Other integration cost issues
  - Provider pricing
  - VPN connectivity
  - Consider application design and tradeoffs



Source: https://www.techtarget.com/searchcloudcomputing/tip/Rules-to-avoid-high-multi-cloud-integration-costs?fbclid=IwAR3bYUk8PcA3nTHO3i8uxrdfgZjpAh29-gPyfArfins-lidoRK3Xs8pA4pY

90

COMPARISON FOR CLOUD BURSTING

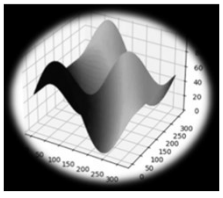
❖ Comparison shopping of vision API providers (2021)

	Algorithmia	Amazon Rekognition	Clarifai	Microsoft Cognitive Services	Google Cloud Vision	IBM Watson Visual Recognition
Image classification	✓	✓	✓	✓	✓	✓
Image detection	✓	✓		✓	✓	
OCR	✓	✓		✓	✓	
Face recognition	✓	✓		✓		
Emotion	✓		✓	✓	✓	
Logo recognition			✓	✓	✓	
Landmark recognition			✓	✓	✓	✓
Celebrity	✓	✓	✓	✓	✓	✓
Multilingual tagging			✓			
Image description				✓		
Handwriting				✓	✓	
Thumbnail generation	✓			✓	✓	
Content moderation	✓	✓	✓	✓	✓	
Custom classification training			✓	✓	✓	✓
Custom detector training				✓	✓	
Mobile custom models			✓	✓	✓	
Free tier	5,000 requests per month	5,000 requests per month	5,000 requests per month	5,000 requests per month	1,000 requests per month	7,500

ATTACK SURFACE의 진화 공식

❖ **Attack Surface의 진화 공식**

- **Complex & Rapidly Evolving**
  - Changes in Infrastructure
  - Changes in User Behaviors
  - New Threats and Vulnerabilities
  - Speed of Business



$$as = [(i + u) * t]^s$$

Speed of Business 비즈니스의 속도

Changes in Infrastructure 인프라 변경

Changes in User Behaviors 사용자 행동 변경

New Threats and Vulnerabilities 새로운 위협과 취약점

Source: https://www.trendmicro.com/

MULTI-CLOUD SECURITY MARKET

❖ **Multi-cloud Security Market** (Global Market Insight)

Source: https://www.gminsights.com/industry-analysis/multi-cloud-security-market

IAAS NETWORKING SERVICES

❖ 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

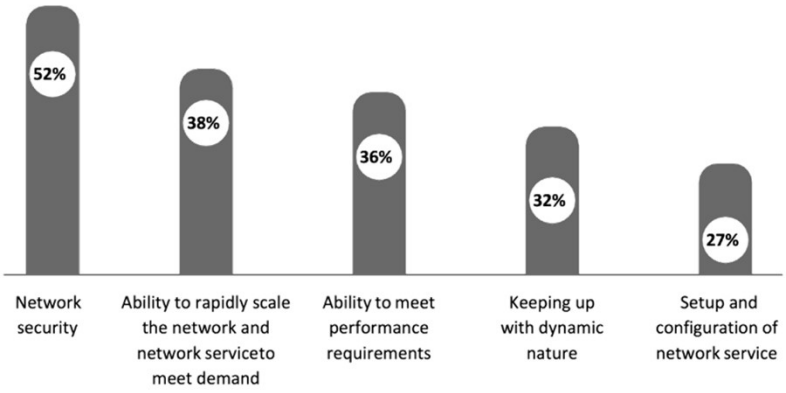
Source: https://aviatrix.com/learn-center/answered-multi-cloud/how-to-do-multicloud-networking-abstraction-and-orchestration-across-aws-azure-and-google/

멀티클라우드 네트워킹의 도전

❖ 멀티클라우드 네트워킹의 도전 - Challenges of Multi-cloud networking

• Top five network challenges in modern multi-cloud environments

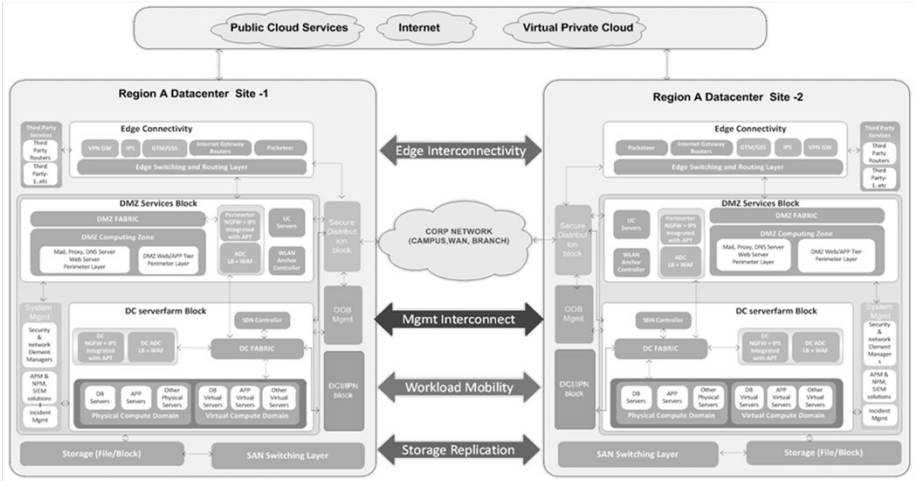
✓네트워크 보안
✓네트워크의 신속한 스케일 요구
✓성능 요구
✓클라우드 특징 다이나믹 지원
✓네트워크 서비스 구성



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

ACTIVE-ACTIVE 데이터센터 설계

❖ Active-Active Data Center design – High Level Architectural Building Blocks

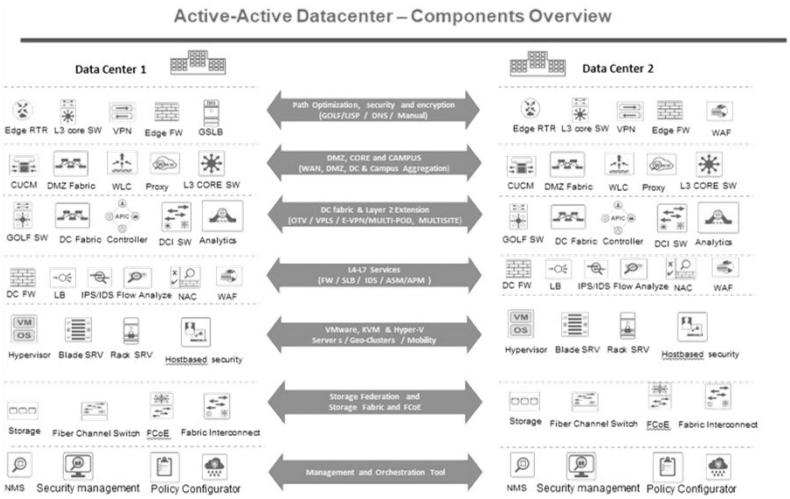


Source: https://www.networkbachelor.com/activedc/

ACTIVE-ACTIVE 데이터센터 설계

❖ Active-Active Data Center design full stack network components

- **Building blocks in networks**
  - Switch
  - Router
  - Firewall
  - Load balancing
  - Virtual Network Function (VNF)
  - Network Function Virtualization (NFV)
  - 블록간 연결



Source: https://www.networkbachelor.com/activedc/

ACTIVE-ACTIVE DATA-CENTER

❖ Active-Active Data Center Technical Requirement

Both DC's servicing application at any time	• Hosting Applications Across the Datacenter • Optimized traffic path when entering and exiting the DC
Recovery Time and Recovery point Objective	• Automatic failover with Minimum service loss in case of devices failure
Quick Service roll out and Consistent policy management	• Consistent security and network policies • Centralized provisioning
IO optimization across the DC, with High performance	• Optimized resource utilization

Source: https://www.networkbachelor.com/activedc/

MONITORING AND MANAGEMENT

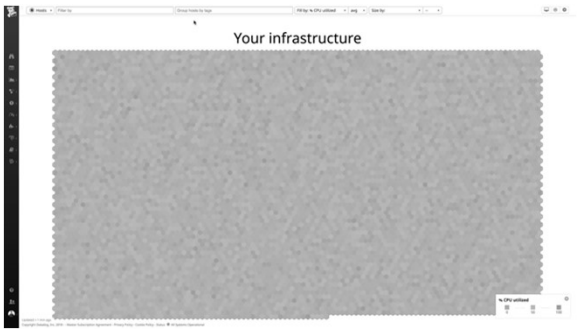
❖ **Monitoring and Management:**

- **Centralized Monitoring:** Implement monitoring tools to gain insights into performance, availability, and security across all clouds.
- **Management Console:** Use a unified management console or dashboard to simplify the administration of multi-cloud resources.

99

CLOUD MANAGEMENT: DATADOG

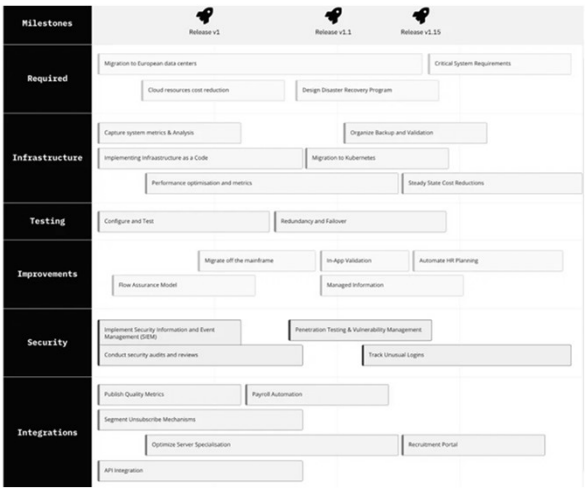
❖ **Cloud Management: Datadog (Video)**



100

TECHNOLOGY ROADMAP

❖ Example of a Miro board showing a technology roadmap



Source: https://miro.com/templates/technology-roadmap/

101

멀티클라우드 사이버보안

❖ 사이버보안 도전 - Cyber security challenges in multi-cloud

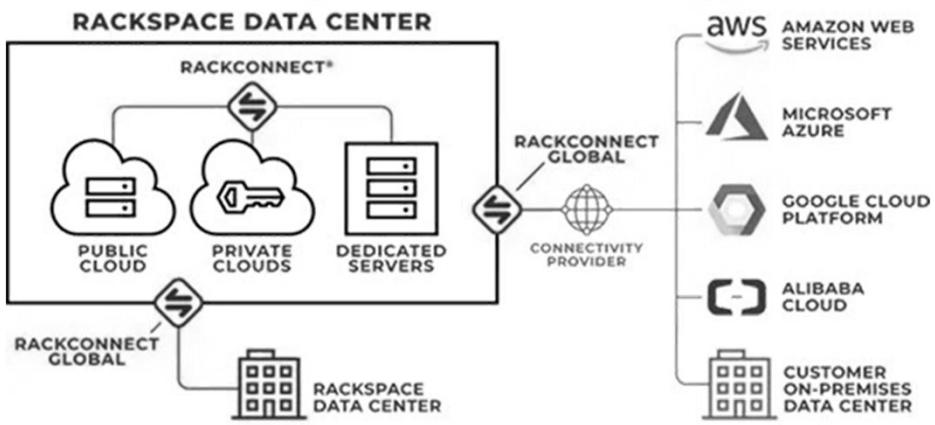
- 준수.. (Compliance..)
- 정책.. (Policy..)
- 가시화.. (Visibility..)
- 음영 (Shadow)
- 탈중앙 제어.. (Decentralized..)
- 클라우드간 ID.. (Identity..)

Source: 'Operationalizing Multi-Cloud Environments', Technologies, Tools and Use Cases, B. S. Rajeshwari, Pethuru Raj, Ramkumar Thirunavukarasu (2022)

102

MULTI-CLOUD SECURITY 전략(예)

❖ Rackspace Multi-Cloud Security Strategy



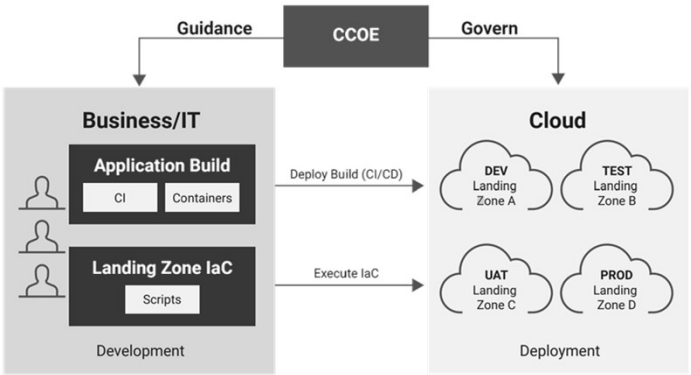
Source: https://www.sdxcentral.com/cloud/definitions/what-is-multi-cloud/rackspace-cloud-strategy/

103

CLOUD DEPLOYMENTS

❖ 클라우드 적용을 위한 애자일 접근 - Agile approach for cloud deployments

- **A CCOE** (Centralized cloud center of excellence) **is a centralized governance function for the organization and acts in a consultative role for central IT, business-unit IT and cloud service consumers in the business. A CCOE is key to driving cloud-enabled IT transformation.**



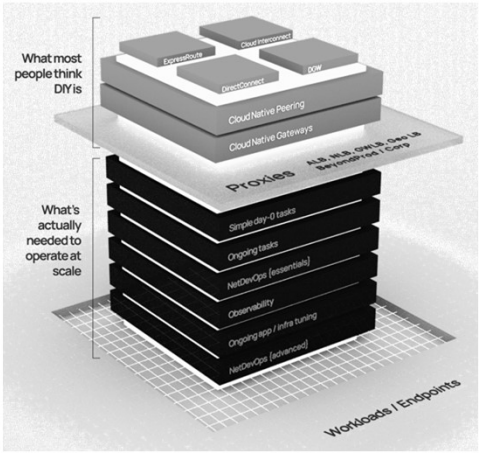
Source: Infrastructure Architecture Essentials for Data Center and Cloud, Shankar Kambhampaty

104

MCN FOR CLOUD NATIVE

❖ MCN for Cloud Native

- DIY complexities for enterprises to solve cloud networking challenge
- Proxies
  - ALB(Application Load Balancer)
  - NLB(Network Load Balancer)
  - GWLB(Gateway Load Balancer)

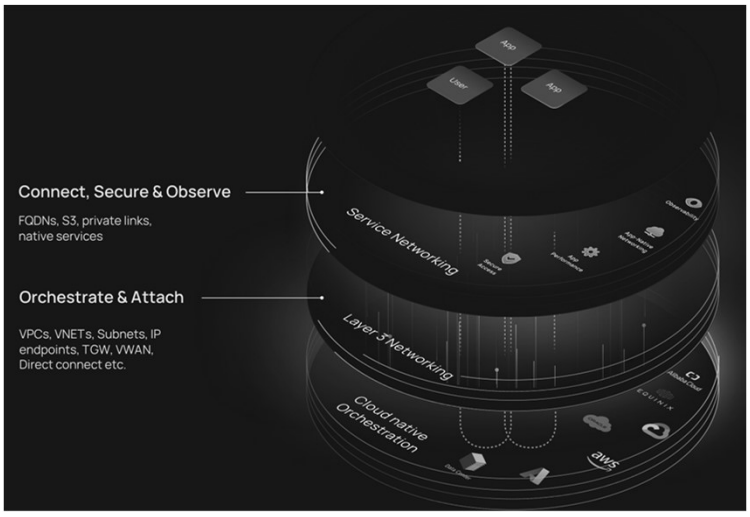


Source: https://prosimo.io/prosimo-mcn-foundation-why-what-how/

ONE PLATFORM

❖ One Platform

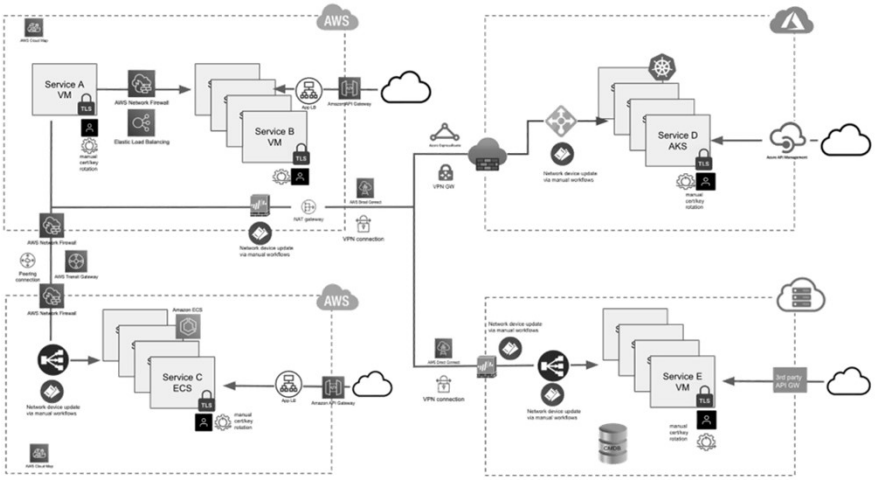
- Service Networking
- Layer 3 Networking
- Cloud Native Orchestration



Source: https://prosimo.io/platform/

CLOUD-VENDOR-SPECIFIC

❖ A multi-cloud architecture using cloud-vendor-specific networking solutions

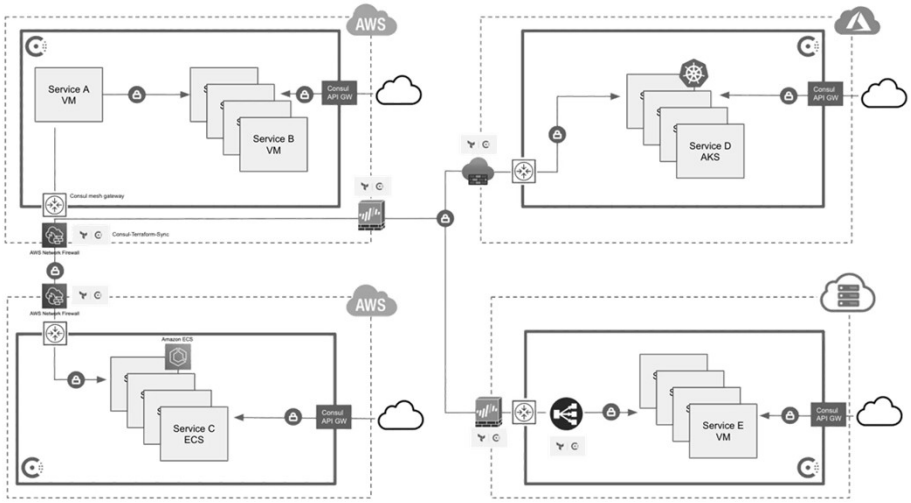


Source: https://www.hashicorp.com/blog/what-can-a-service-mesh-do

107

CLOUD-AGNOSTIC

❖ Using a cloud-agnostic service mesh.



Source: https://www.hashicorp.com/products/consul/multi-platform-service-mesh

108

SINGLE PANE OF GLASS

❖ CloudHealth(예): CloudHealth is more robust than AWS Cost Explorer in that it can ingest data from AWS, GCP, Azure, and Oracle Cloud

Source: https://www.cloudzero.com/blog/single-pane-of-glass

LOAD BALANCING

❖ Networking services compared: AWS vs Azure vs Google Cloud

• Load Balancing

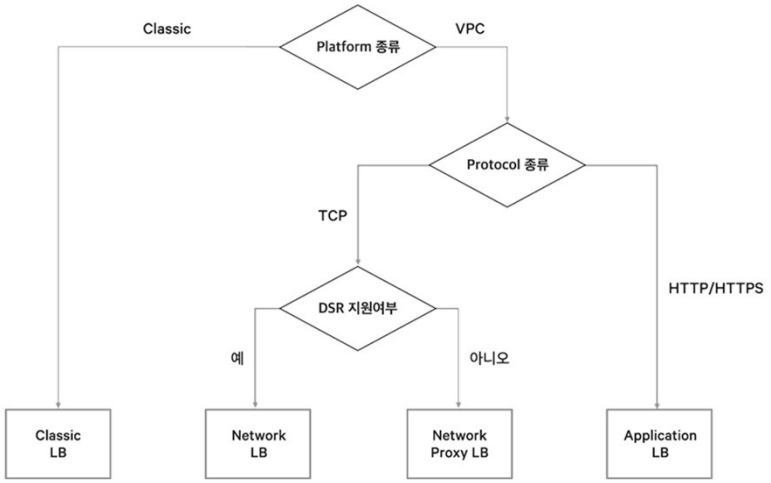
aws		Azure			
NETWORK LOAD BALANCER	LAYER 4 TCP/SSL	AZURE LOAD BALANCER	LAYER 4 TCP/UDP	INTERNAL	REGIONAL PASS-THROUGH TCP or UDP PROXY HTTP(S)
APPLICATION LOAD BALANCER	APPLICATION LAYER	AZURE APPLICATION GATEWAY	APPLICATION LAYER		
ROUTE 53	DNS	TRAFFIC MANAGER	DNS	EXTERNAL	REGIONAL OR GLOBAL PASS-THROUGH TCP or UDP PROXY TCP, SSL or HTTP(S)
		FRONT DOOR	GLOBAL LOAD BALANCING		

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

네이버클라우드플랫폼 (로드밸런서)

❖ 네이버클라우드플랫폼 (2023)

• 로드밸런서



Source: https://www.ncloud.com/product/networking/loadBalancer

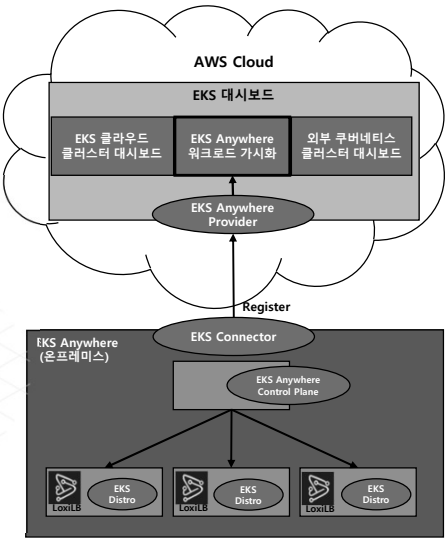
AWS EKS ANYWHERE

❖ eBPF 사용 (예): AWS EKS Anywhere

• Cilium (eBPF)

• MetalLB or LoxiLB (eBPF)

LoxiLB 정책 자동 구성



Source: https://cilium.io/ , https://www.loxilb.io/

기업의 거버넌스 모델

❖ Simplified enterprise governance model

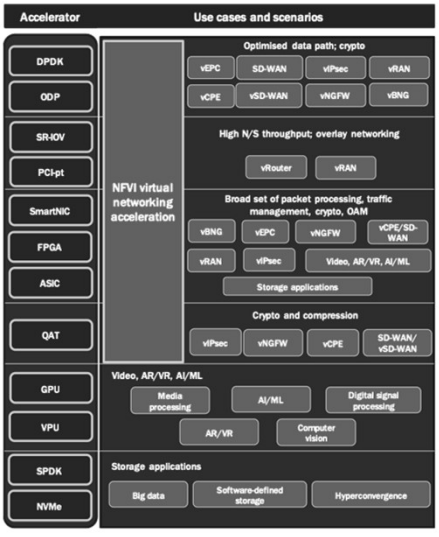
- Strategic: Ambition and Goal
- Tactical: Contract, Service Level Agreement
- Operational: Build, Test, Deploy, Operate, Monitor

Source: Mulder, Jeroen. Multi-Cloud Strategy for Cloud Architects: Learn how to adopt and manage public clouds by leveraging BaseOps, FinOps, and DevSecOps, Packt Publishing.

ACCELERATION TECHNOLOGIES

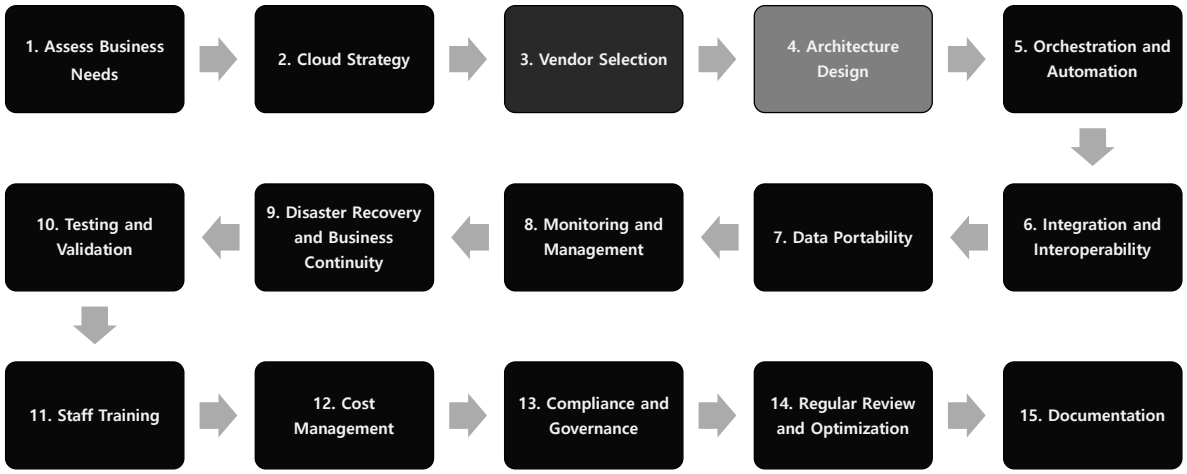
❖ Acceleration technologies and use cases

- 가상화를 위한 가속 기술
  - DPDK
  - SR-IOV
  - SmartNIC
  - FPGA
  - ASIC
  - QAT
- GPU
- DPU
- IPU
- NVMe
- 소프트웨어 가속 eBPF → DPU 배포가능



Source: 5GPPP Architecture Working Group, 5G Architecture White Paper

멀티클라우드 데이터센터 설계하기



115

기업의 멀티클라우드 데이터센터 가이드

❖ Guide on how an enterprise can successfully operate its multi-cloud datacenter

- Centralized Management
- Automation and Orchestration
- Resource Allocation and Optimization
- Cost Management:
- Security and Compliance
- Data Management
- Performance Monitoring
- Disaster Recovery Planning
- Vendor Relationships
- Staff Training
- Incident Response
- Governance and Policies
- Change Management
- Documentation
- Continuous Improvement

116

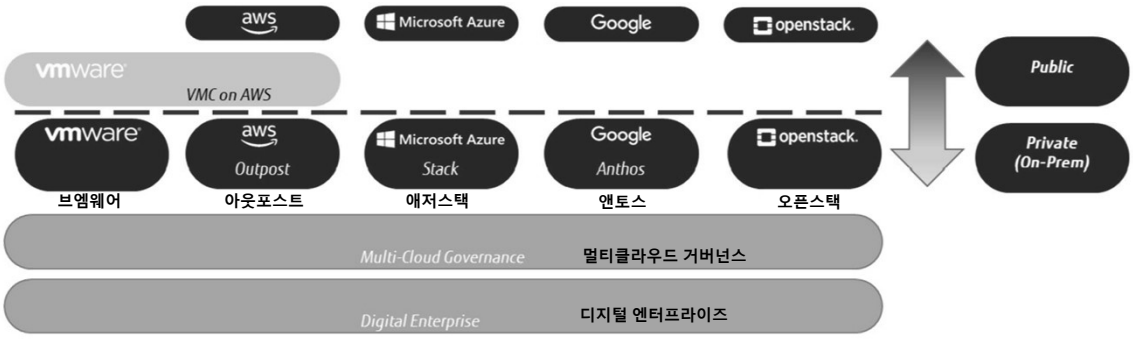
II. CSP/제조사의 멀티 클라우드 솔루션

117

멀티클라우드 플레이어

❖ 주요 멀티클라우드 플레이어 (Main players in the field)

- Public: AWS, Azure, Google, OpenStack, (VMware)
- Private(On-Prem): VMware, Outpost(AWS), Azure Stack, Anthos(Google), OpenStack



Source: Mulder, Jeroen. Multi-Cloud Architecture and Governance: Leverage Azure, AWS, GCP, and VMware vSphere to build effective multi-cloud solutions (p. 48). Packt Publishing. Kindle Edition.

118

MCNS 제조사

❖ MCNS (Multicloud Networking Software) 제조사

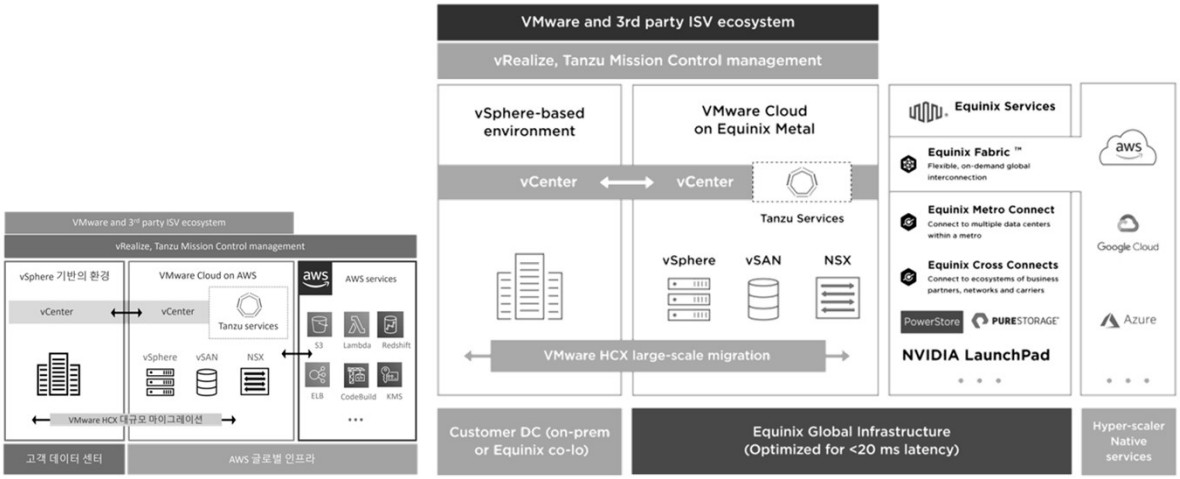
제조사	제품/서비스 또는 플랫폼
Alkira	Cloud Networking
Arrcus	Arrcus Multi-Cloud Networking (MCN)
Arista Networks	Any Cloud Platform
Aviatrix	Aviatrix Cloud Network Platform
Cohesive Networks	VNS3
Cisco	Cisco Cloud Services Router 1000V (CSR1kv), Cisco Catalyst 8000V Edge Software, Cisco Cloud APIC
F5	F5 Distributed Cloud Platform
Prosimo	AXI Platform
VMware	NSX Cloud

Source: https://www.gartner.com/doc/reprints?id=1-29S4R0C1&ct=220419&st=sb

119

VMWARE CLOUD ON EQUINIX METAL

❖ Intercloud (예): VMware Cloud on Equinix Metal



Source: https://www.cloud13.ch/2023/04/05/vmware-cloud-on-equinix-metal-the-new-intercloud/

120

DELL APEX 클라우드 플랫폼

❖ Dell APEX 클라우드 플랫폼 (예):

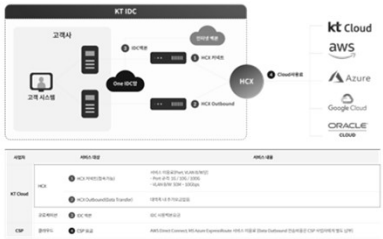
- 퍼블릭클라우드에서 사용하는 에코시스템을 온프레미스로 확장, 최적화
- 공통 플랫폼 및 자동화로 운영 효율화
- 익숙한 운영/개발자 환경으로 생산성 가속
- 멀티클라우드 데이터 및 앱 유연한 확장
- 클라우드 거버넌스/규정 일관된 준수 시행

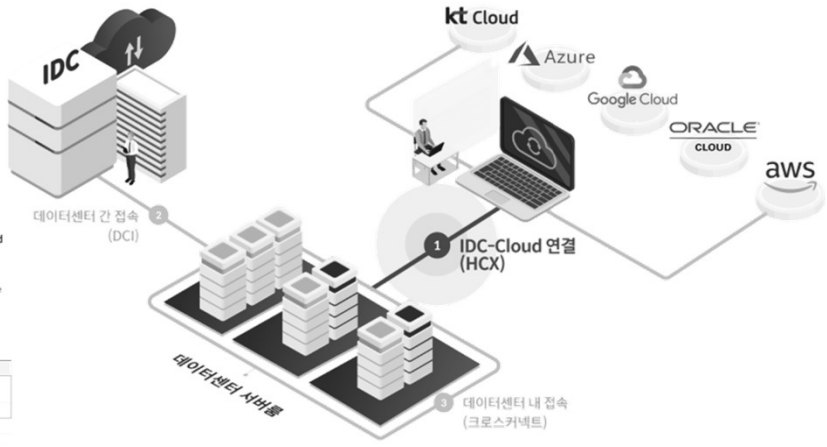
Source: Dell

121

KT CLOUD의 HYBRID/MULTI CLOUD

❖ kt cloud의 Hybrid/Multi Cloud





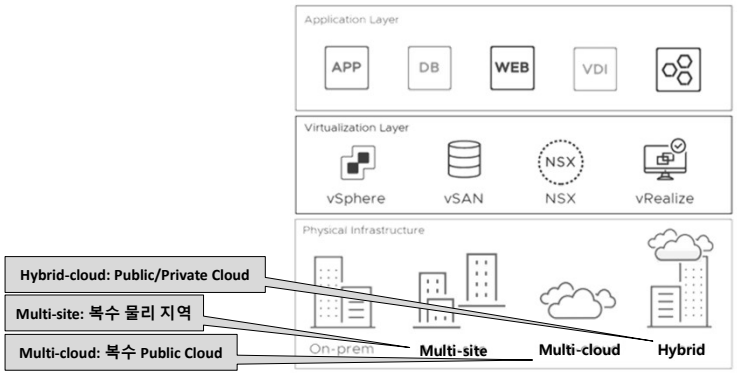
Source: https://www.kt-idc.com/colocation/viewcolocation_1Page

122

NSX OVER ANY FABRIC

❖ 제조사의 멀티클라우드 (예): VMware

- VMware의 Multi-cloud
- NSX over Any Fabric Underlay, Site, Cloud



NSX Features and Values

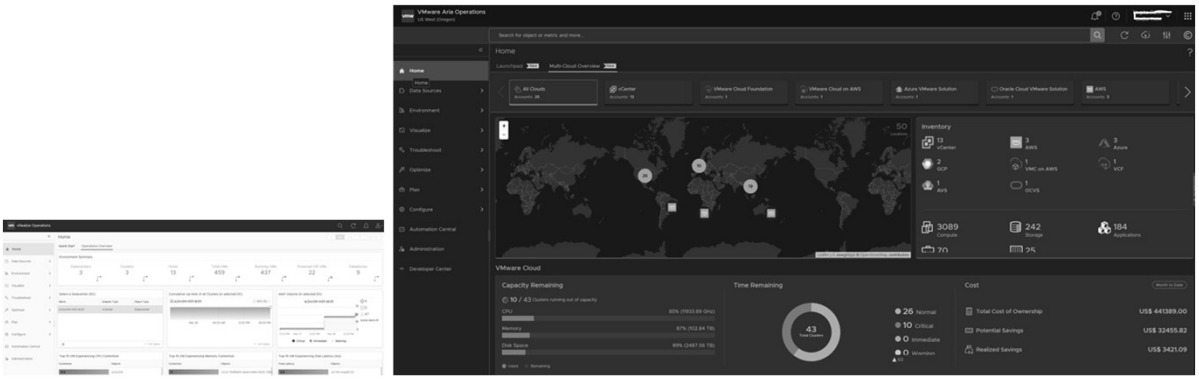
- Hybrid Cloud Automation
- Service-defined Firewall
- Purpose built software
- Inherent extensible services: LB, DDI, NAT, VPN
- 3rd party service chaining
- Physical switching fabric choice
- Improves simplicity, resilience, stability
- Cloud ready, hardware independent SDN
- Easier to troubleshoot, problem scope minimized

Source: DEPLOYING VMWARE NSX WITH CISCO ACI UNDERLAY DESIGN GUIDE (VERSION: 2021)

VMWARE의 MULTI-CLOUD

❖ Multi-Cloud Overview in VMware Aria Operations

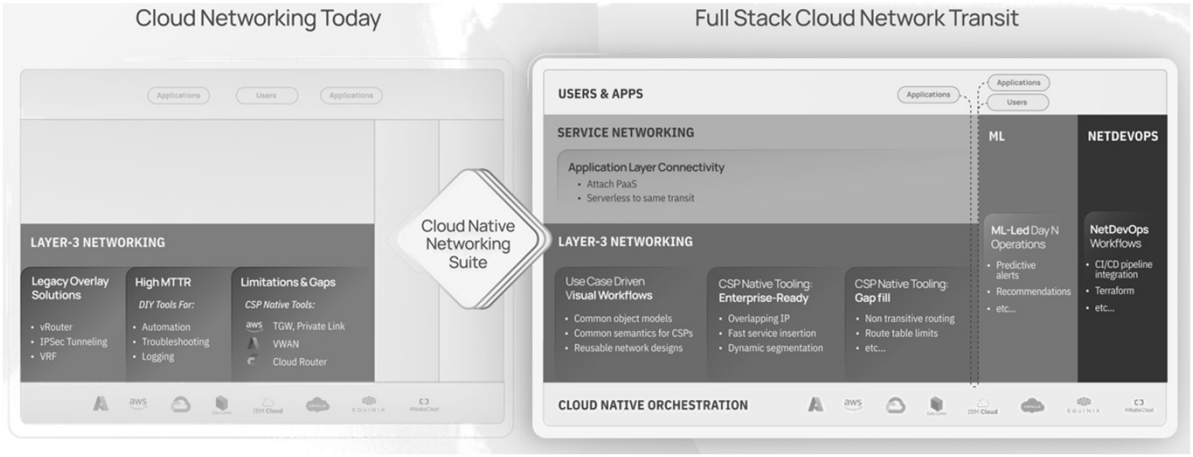
- **Private clouds:** vCenter, VMware Cloud Foundation
- **VMware Clouds:** VMC, VMC-D, Azure VMware Solution, Oracle Cloud VMware Solution, Google Cloud VMware Engine
- **Public Clouds:** AWS, Azure, GCP



Source: https://blogs.vmware.com/management/2023/04/multi-cloud-overview-in-vmware-aria-operations.html

PROSIMO

❖ MCN for Cloud Native

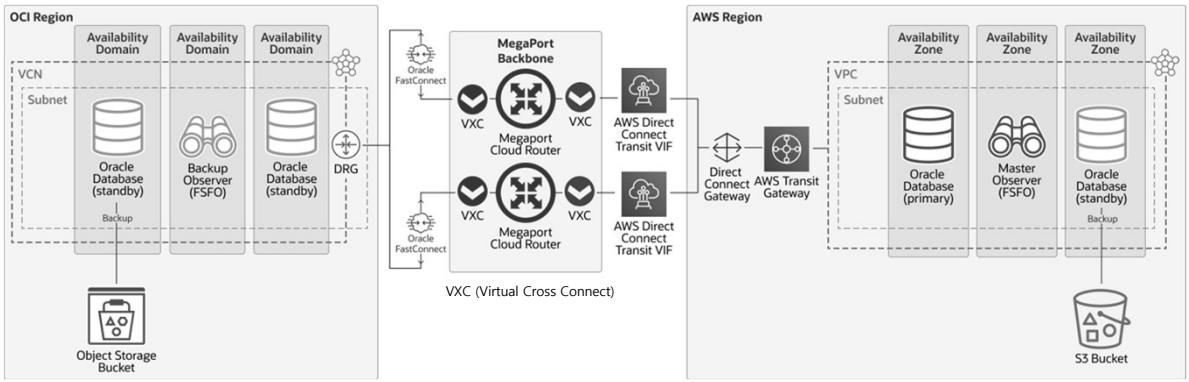


Source: https://prosimo.io/prosimo-mcn-foundation-why-what-how/

125

OCI AND AWS WITH MEGAPORT

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

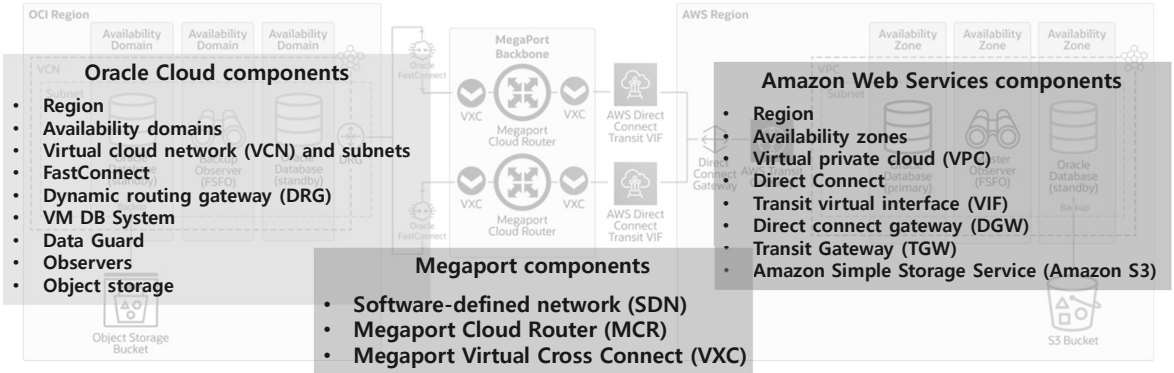


Source: https://docs.oracle.com/en/solutions/multicloud-failover-oci-aws/index.html#GUID-A7E1BFB0-4489-4DD5-8D6F-B4DE38F88BE2

126

OCI AND AWS WITH MEGAPORT

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



Oracle Cloud components

- Region
- Availability domains
- Virtual cloud network (VCN) and subnets
- FastConnect
- Dynamic routing gateway (DRG)
- VM DB System
- Data Guard
- Observers
- Object storage

Megaport components

- Software-defined network (SDN)
- Megaport Cloud Router (MCR)
- Megaport Virtual Cross Connect (VXC)

Amazon Web Services components

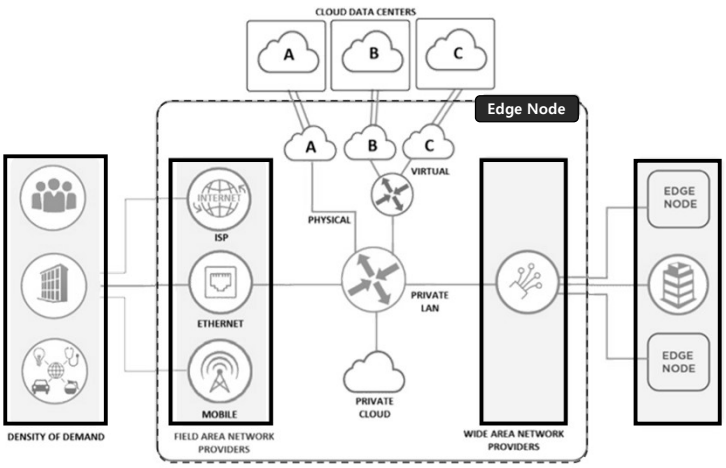
- Region
- Availability zones
- Virtual private cloud (VPC)
- Direct Connect
- Transit virtual interface (VIF)
- Direct connect gateway (DGW)
- Transit Gateway (TGW)
- Amazon Simple Storage Service (Amazon S3)

Source: https://docs.oracle.com/en/solutions/multicloud-failover-oci-aws/index.html#GUID-A7E1BFB0-4489-4DD5-8D6F-B4DE38F88BE2

127

MULTIPLE CLOUDS AT THE DIGITAL EDGE

❖ Connect to Multiple Clouds at the Digital Edge



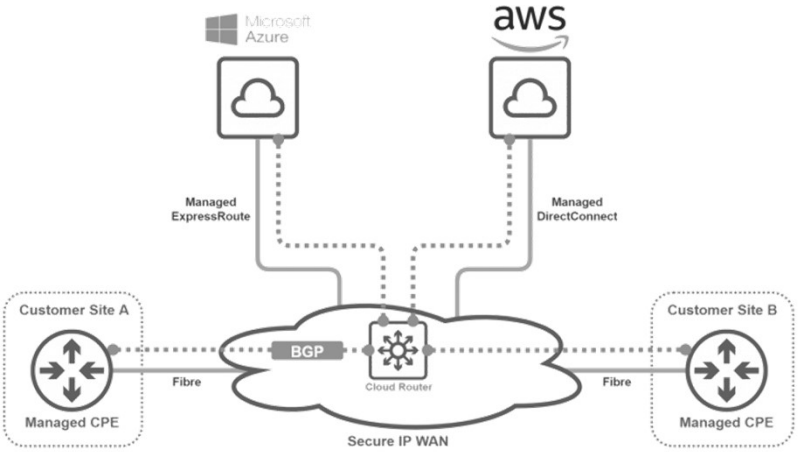
Source: https://blog.equinix.com/blog/2017/05/24/optimizing-multicloud-interconnection-at-the-digital-edge/

128

CLOUD AND DC INTERCONNECT

❖ Cloud and DC Interconnect (Network Solution Group)

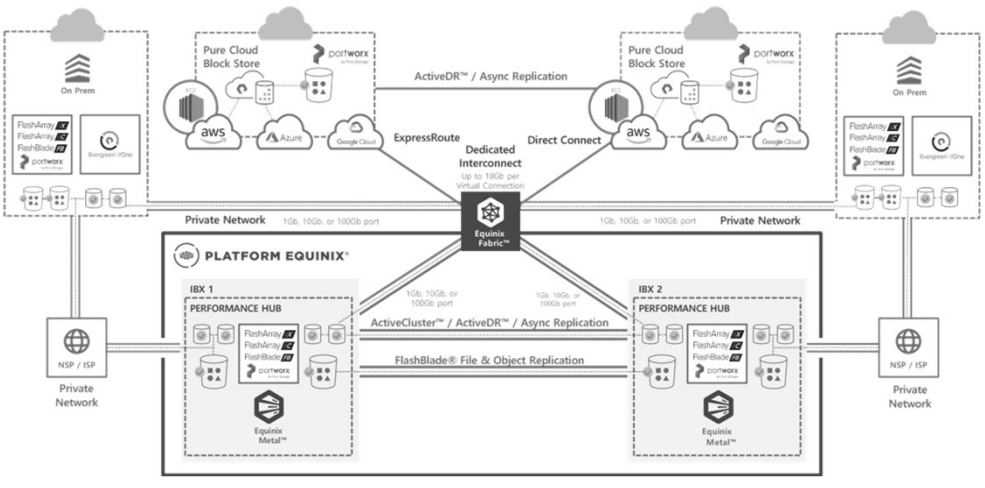
- Services
- Datacenter & Cloud
- Network Design & Engineering
- Network Management



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

PURE STORAGE ON EQUINIX METAL

❖ Pure Storage on Equinix Metal

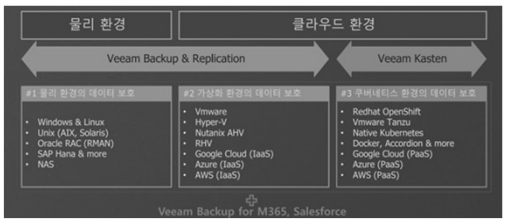


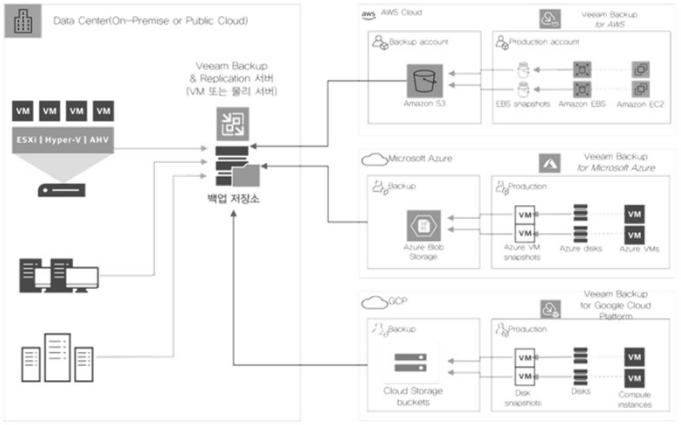
Source: Equinix

멀티/하이브리드 클라우드 백업

❖ 멀티/하이브리드 클라우드 백업 alc 재해복구(예): VEEAM

• 단일 플랫폼으로 다양한 환경의 보호



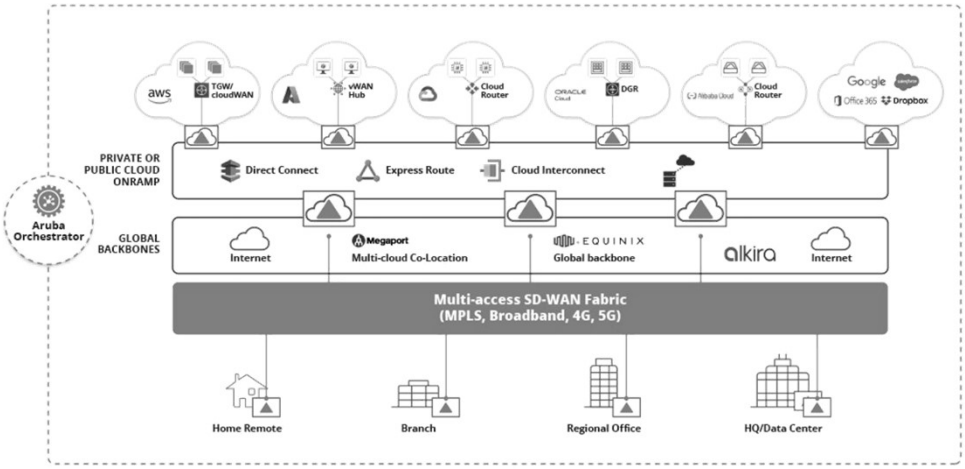


Source: Veeam

131

SD-WAN CLOUD CONNECTIVITY

❖ MCN with Aruba EdgeConnect for flexible, secure, SD-WAN cloud connectivity



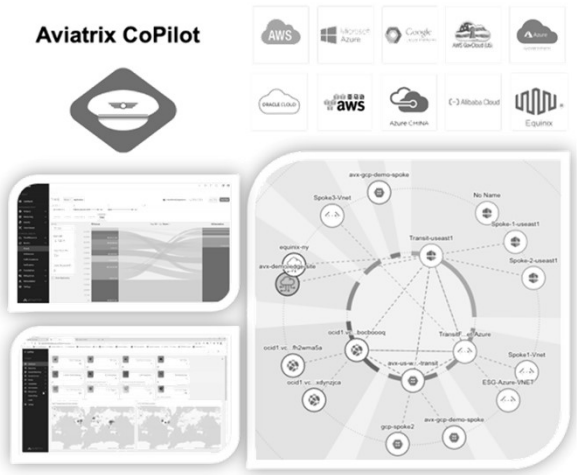
Source: https://www.arubanetworks.com/faq/what-is-multi-cloud-networking/

132

AVIATRIX SECURE CLOUD NETWORK

❖ 제조사의 Multi-cloud networking (Aviatrix)

- Aviatrix Secure Cloud Network:
  - Secure and Predictable
  - Self-Service Automation
  - CostIQ Reduces Spending



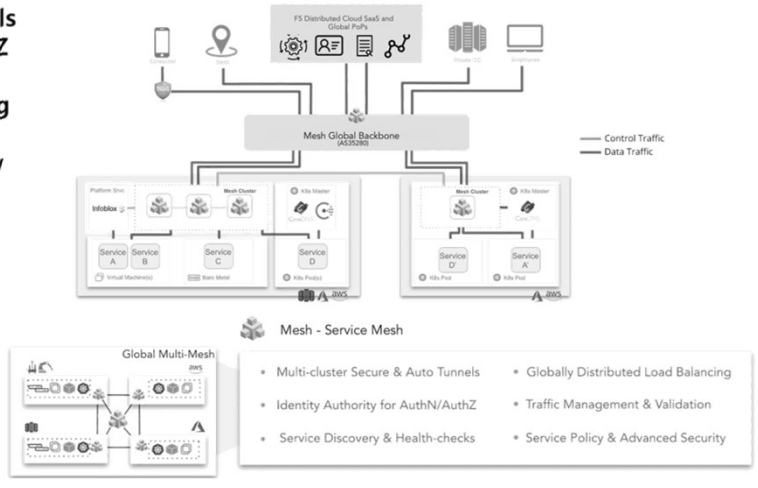
Source: https://www.cisco.com/c/en/us/td/docs/dcn/whitepapers/cisco-hybrid-multicloud-networking-design-guide.html

133

F5의 DISTRIBUTED CLOUD MESH

❖ 제조사의 멀티클라우드 (예): F5 Distributed Cloud Mesh Service Mesh

- Multi-cluster Secure & Auto Tunnels
- Identity Authority for AuthN/AuthZ
- Service Discovery & Health-checks
- Globally Distributed Load Balancing
- Traffic Management & Testing
- Service Policy & Advanced Security



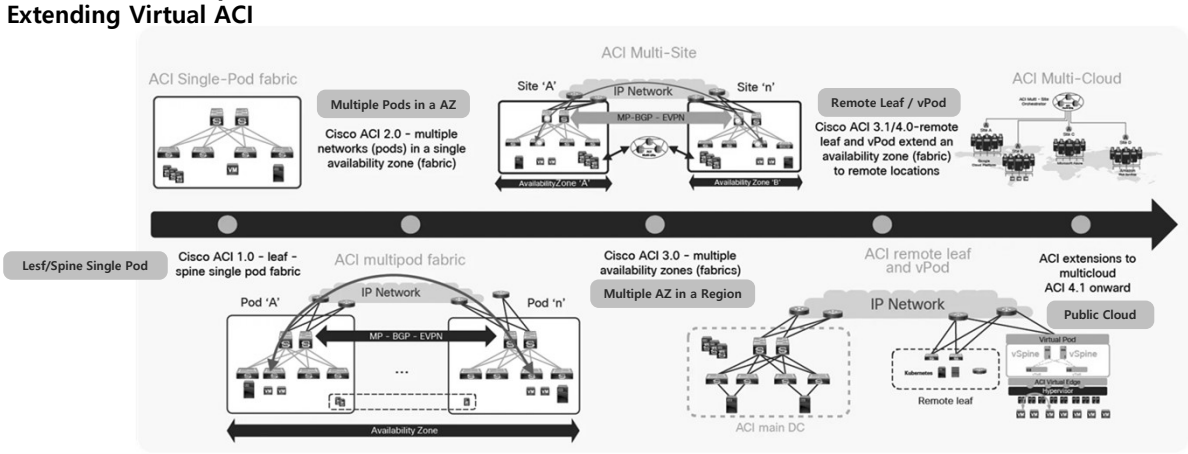
Source: https://docs.cloud.f5.com/docs/services/mesh/service-mesh

134

CISCO ACI

❖ 언더레이 SDN 제조사(예): Cisco ACI

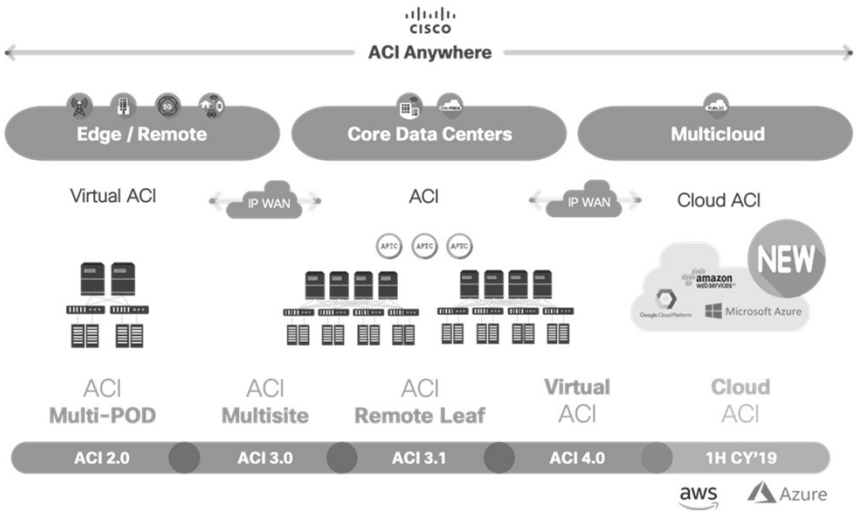
- ACI extensions to public clouds
- Extending Virtual ACI



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

제조사의 멀티클라우드

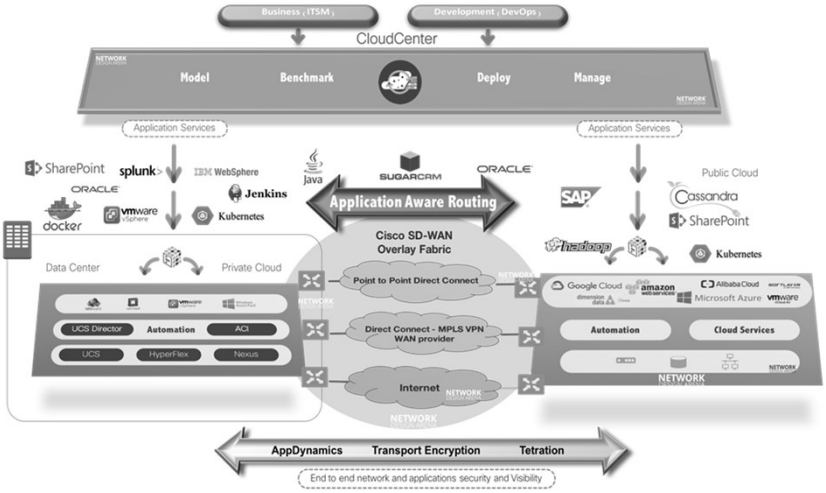
❖ Cisco ACI Anywhere



Source: https://blogs.cisco.com/datacenter/cisco-fulfills-vision-for-aci-anywhere

시스코 CLOUD ARCHITECT

❖ **Multi-Cloud (예) – 시스코 Cloud Architect Perspective**



Source: Cisco, https://www.netdesignarena.com/index.php/2018/05/30/why-cisco-multi-cloud-a-cloud-architect-perspective/

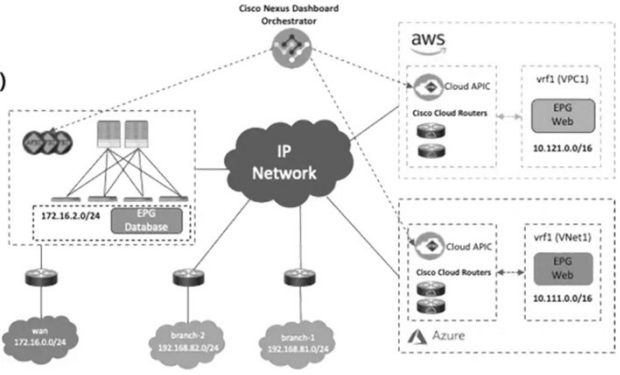
137

CISCO ACI

❖ **Cisco ACI and Cisco Multi-Cloud Networking:**

- Cisco Cloud Network Controller (formerly called Cisco Cloud Application Policy Infrastructure Controller: Cisco Cloud APIC)
- Nexus Dashboard Orchestrator (NDO)
- Virtual Routing and Forwarding (VRF)
- Bridge Domain (BD)
- Endpoint Group (EPG)
- Layer 3 Out or external routed network (L3Out)
- Subnet-based EPG in Layer 3 Out (L3Out External EPG)
- Service Graph

End-Point Group(EPG):
ACI 정책 모델에 엔드포인트 그룹(EPG) 개념 도입 EPG는 다른 네트워크 구성과 무관하게 애플리케이션 또는 애플리케이션 구성 요소를 나타내는 엔드포인트의 그룹

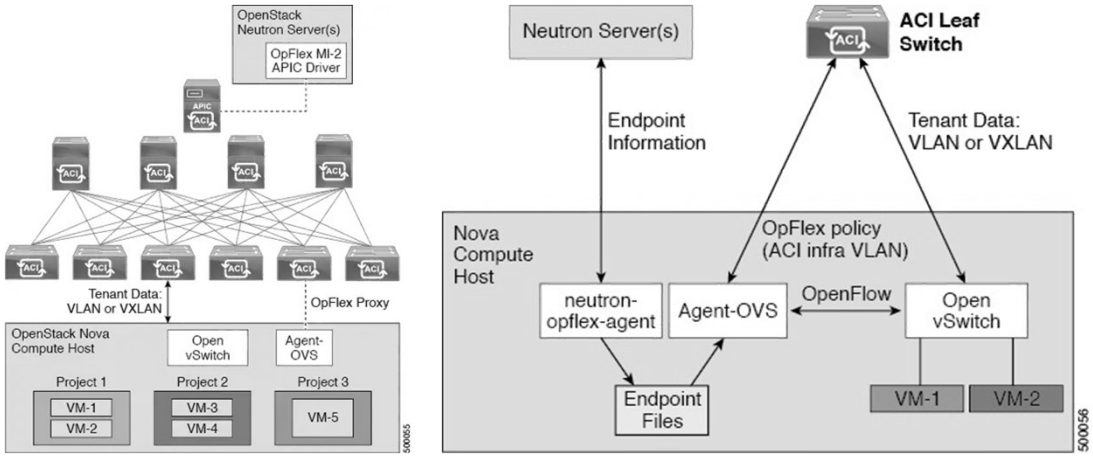


Source: https://www.cisco.com/c/en/us/td/docs/dcn/whitepapers/cisco-hybrid-multicloud-networking-design-guide.html

138

ACI WITH OPENSTACK

❖ Cisco ACI with OpenStack OpFlex

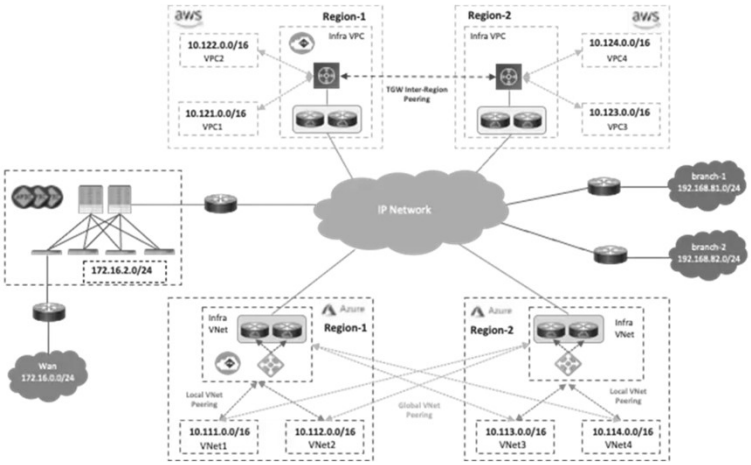


Source: https://www.cisco.com/c/ja_jp/td/docs/switches/datacenter/aci/apic/sw/1-x/openstack/b_ACI_with_OpenStack_OpFlex_Architectural_Overview/b_ACI_with_OpenStack_OpFlex_Architectural_Overview_chapter_010.html

139

네트워킹 설계 가이드 (예)

❖ Cisco Multi-Cloud Networking with Multiple Regions



Source: https://www.cisco.com/c/en/us/td/docs/dcn/whitepapers/cisco-hybrid-multicloud-networking-design-guide.html

140

CISCO CLOUD NETWORK CONTROLLER

❖ 제조사의 멀티클라우드 (예): Multi-Cloud Network (Cisco Cloud Network Controller)

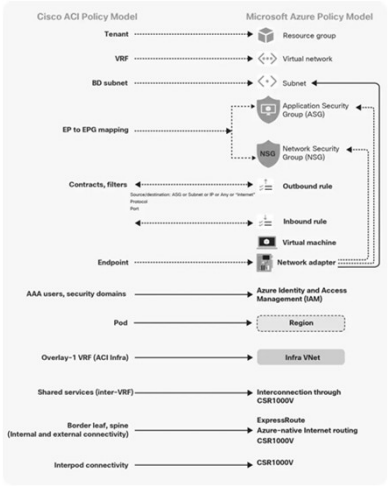
- **Intra-cloud connectivity:** Extend segments across regions, Automate route propagation across virtual networks, Automate L4-L7 service insertion
- **Inter-cloud connectivity:** Automate route propagation across clouds, Extend routing domains and segments across Clouds, Automate L4-L7 service insertion
- **Hybrid cloud connectivity:** Automate Overlay connectivity for different types of Underlays, Extend routing domains and segments between On Premises and Cloud sites, Enable consistent networking and visibility between On Premises and Cloud
- **External network connectivity:** Standards-based IP connectivity to any network, Secure connectivity to external network spanning datacenters and branches.
- **L4-L7 service insertion:** Automate firewall and load balancer insertion, Automatically update routing and security policy to insert L4-L7 services, Integrate with third-party L4-L7 services and cloud native L4-L7 services
- **Brownfield VPC onboarding:** Safe and fast migration and rollback, Ability to use Cloud Network Controller with brownfield environments

Source: https://blogs.cisco.com/datacenter/modernize-your-multi-cloud-network-with-cisco-cloud-network-controller

141

CISCO MODEL TO AZURE

❖ Cisco ACI Policy Model to Microsoft Azure Policy Model Mapping (NSG Per Subnet)

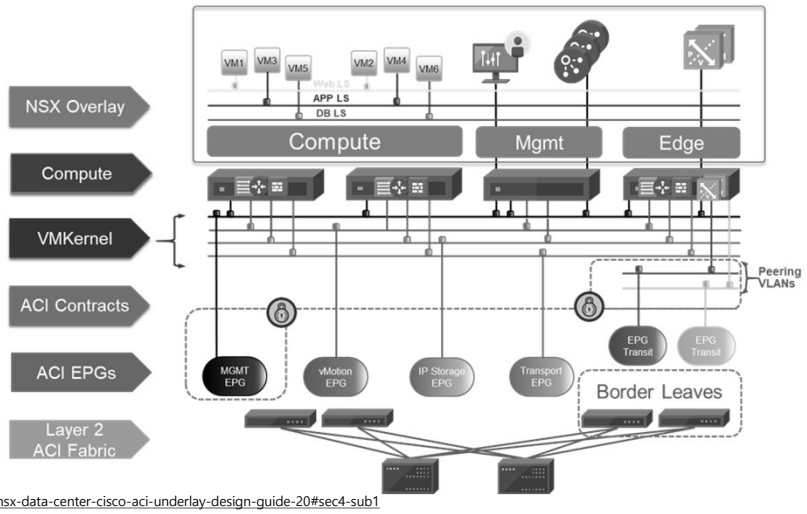


Source: https://www.cisco.com/c/en/us/td/docs/dcn/whitepapers/cisco-hybrid-multicloud-networking-design-guide.html

142

NSX DATA CENTER ON ACI UNDERLAY

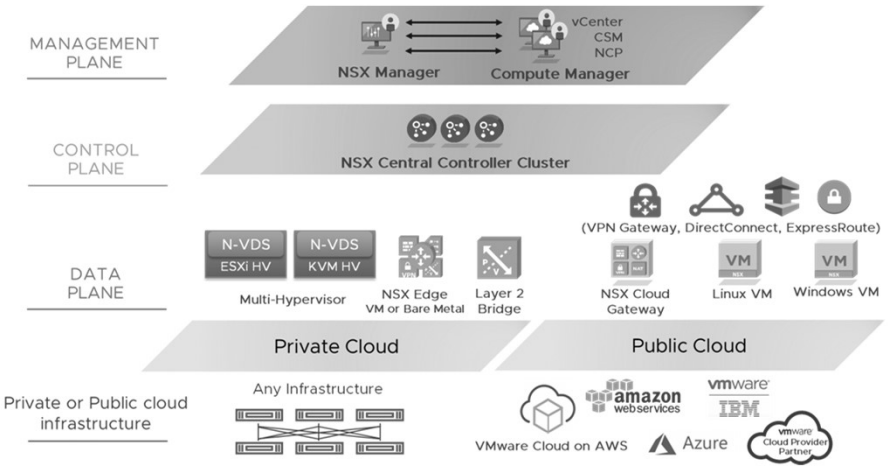
❖ **NSX Data Center Deployed on an ACI Underlay**



Endpoint Security Groups (ESGs)
Source: https://nsx.techzone.vmware.com/resource/deploying-nsx-data-center-cisco-aci-underlay-design-guide-20#sec4-sub1

NSX DATA CENTER ARCHITECTURE

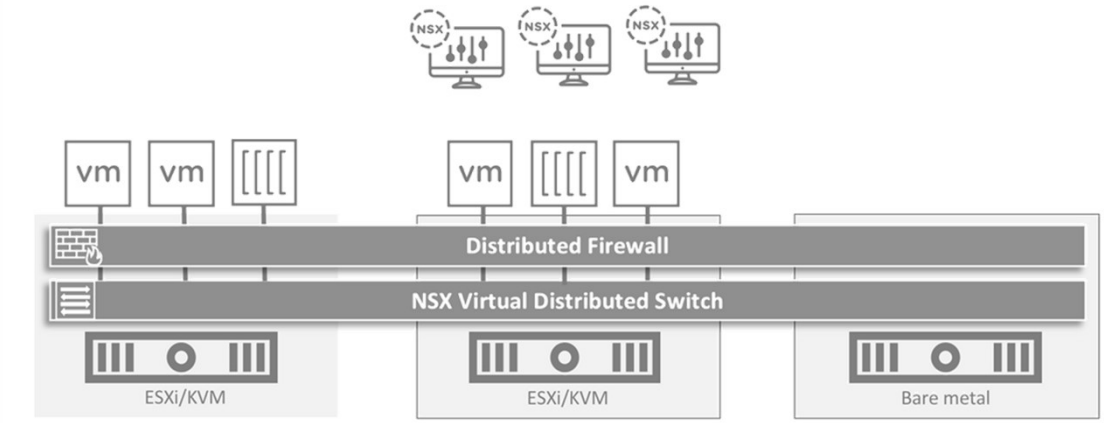
❖ **NSX Data Center Architecture for Private Cloud, Public Cloud**



Source: https://nsx.techzone.vmware.com/resource/deploying-nsx-data-center-cisco-aci-underlay-design-guide-20#section3

VMWARE NSX 분산 방화벽(DFW)

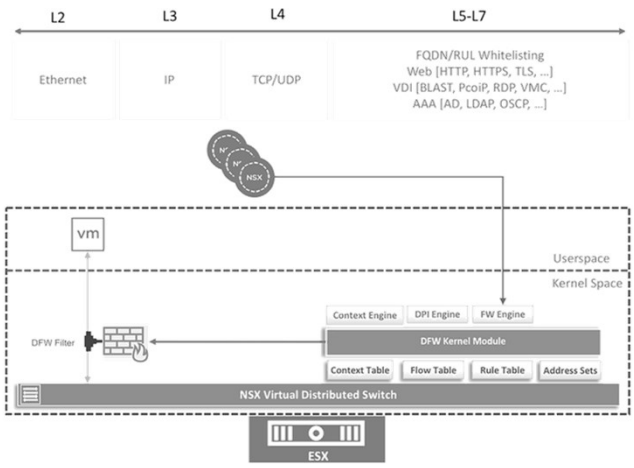
❖ VMware NSX: DFW Enforcement at the Hypervisor Level



Source: https://www.ramyafifi.com/post/micro-segmentation-with-nsx-data-center

VMWARE NSX-T DFW

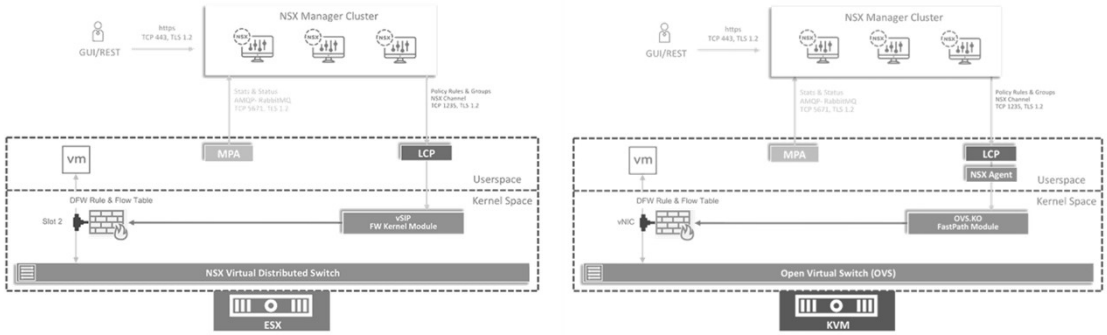
❖ VMware NSX: NSX-T DFW with Layer 7 Context Profiles



Source: https://www.ramyafifi.com/post/micro-segmentation-with-nsx-data-center

ESXI HOST / KVM HOST

❖ ESXi Host / KVM Host - Data Plane Implementation



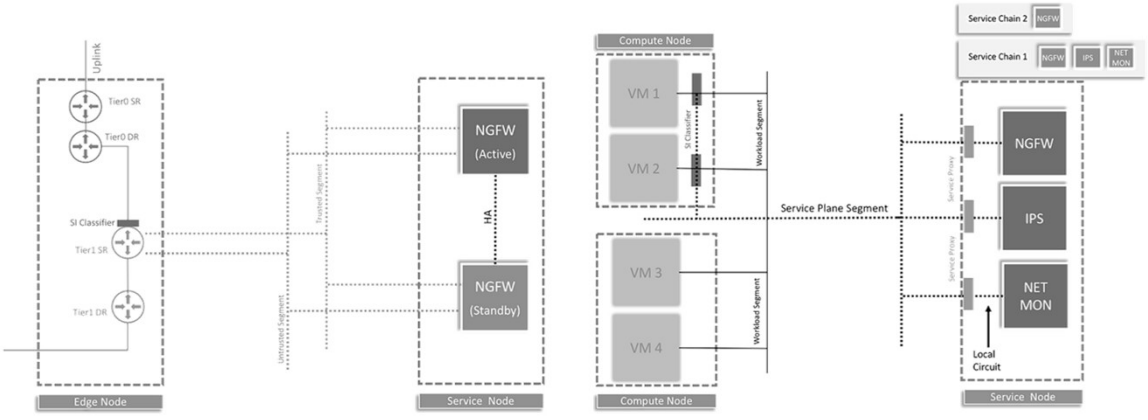
Source: https://www.ramyafifi.com/post/micro-segmentation-with-nsx-data-center

147

NETWORK INTROSPECTION

❖ NSX-T North-South Network Introspection

❖ NSX-T East-West Network Introspection



NSX-T North-South Network Introspection

NSX-T East-West Network Introspection

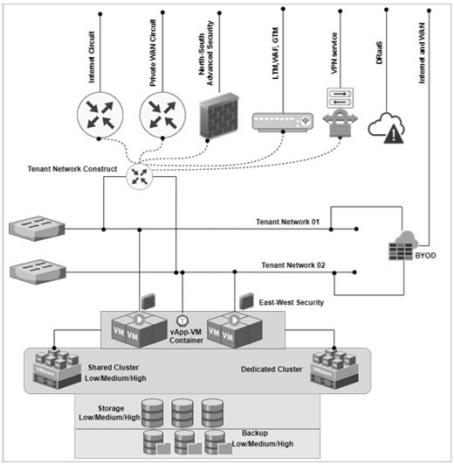
Source: https://www.ramyafifi.com/post/micro-segmentation-with-nsx-data-center

148

NSX-T DESIGN OPTIONS (VMWARE)

❖ NSX-T design options (VMware)

1. No. of VM's/Containers in a network (That could define the no. of Network)
2. VM Microsegmentation (East-West Traffic protection)
3. NAT Service
4. IPsec Service
5. Internet Gateway
6. Private WAN Circuit(MPLS)
7. North-South Security
8. Remote Connection
9. Load Balancer (LTM, WAF, Global Load Balancer)
10. DRaaS (Active-Active or Active-Standby Service hosting)
11. Monitoring and Logging Service and etc



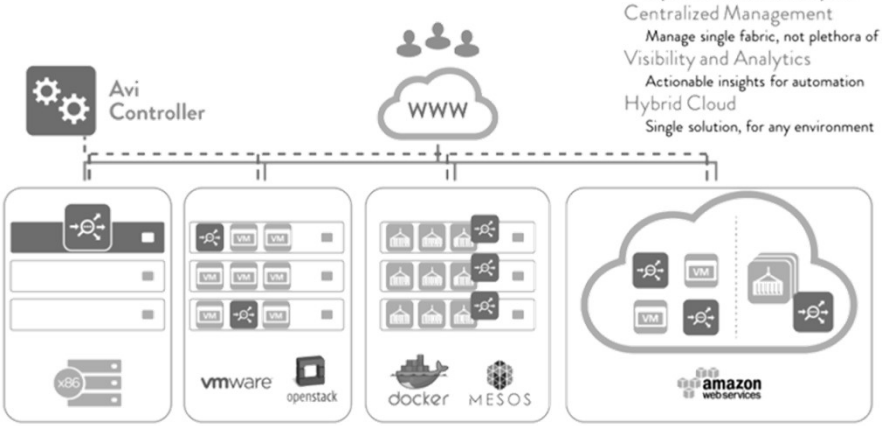
Source: https://www.networkbachelor.com/vcloud-director-nsx-v-to-nsx-t-migration-part-2/

149

ALB (VMWARE)

❖ NSX advanced Load Balancer (Formerly called AVI Vantage)

Scalable Network Services
Separated control and data plane
Centralized Management
Manage single fabric, not plethora of devices
Visibility and Analytics
Actionable insights for automation
Hybrid Cloud
Single solution, for any environment

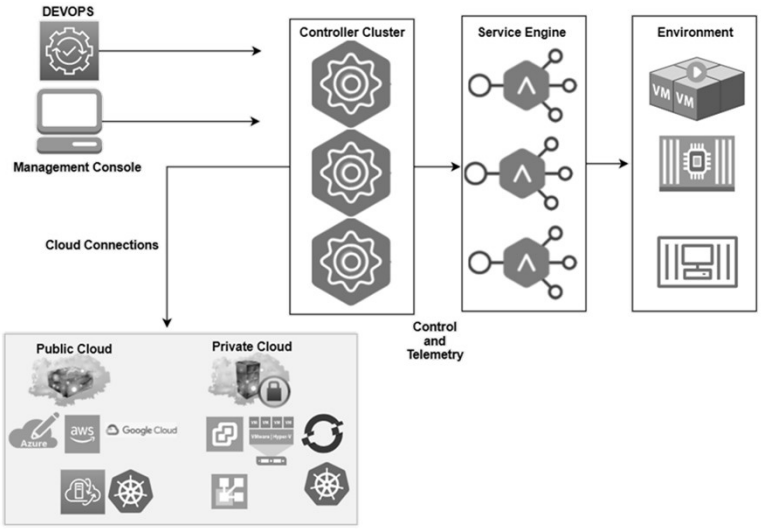


Source: https://www.networkbachelor.com/nsx-t-alb-avi-series-part01/

150

AVI ARCHITECTURE

❖ AVI Architecture



Source: https://www.networkbachelor.com/nsx-t-alb-avi-series-part01/

151

VERSA NETWORKS

❖ **Security Capability Software Stack**

❖ **제조사(예): SD-Branch, SD-WAN, SD-Security** (VERSA Networks)

Market Leading Security Functions					
Stateful Firewall	CGNAT	URL Feeds and Filtering	Lateral Movement Protection	Malware Protection	File Filtering
DOS Protection	NG-Firewall (NGFW)	IP Feeds and Filtering	Captive Portal	Network DLP (*)	NG-IPS
IPSec	User & Group Authentication	Device Fingerprinting	HTTP / SSL Proxy	DNS Feeds and Security (*)	Anti-Virus

- **Visibility & access control**
  - Application, domain & URL
  - User, device & location
- **Layer 7 & content security**
  - SSL decryption
  - App / URL / IP Feeds and filtering
  - File filtering
  - Anti-virus
  - IPS
  - DNS Security (*)

- **Layer 4**
  - Reconnaissance
  - DoS protection (ICMP, UDP, TCP flood)
    - Rate limiting
- **Layer 3**
  - ARP, IP ICMP protocol defence
  - IP spoofing
  - Strict source routing checks
  - Fragment overlaps

VERSA NETWORKS

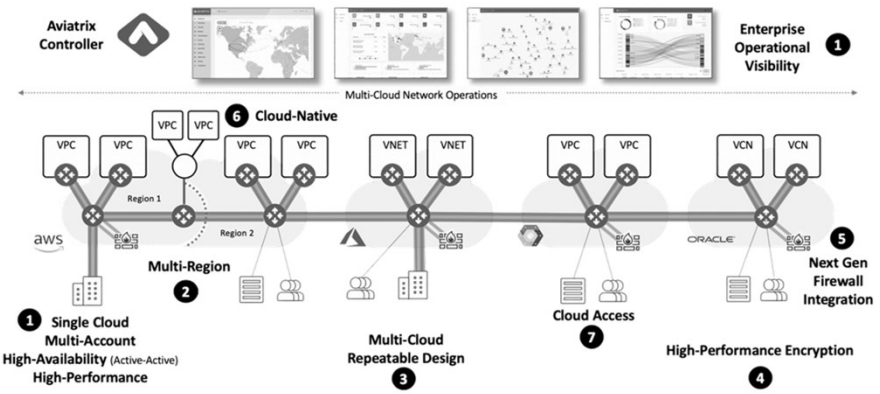
Source: Versa Networks, SDxCentral

152

DATA PLANE

❖ Cloud Network Platform – Data Plane

- HA
- Multi-Region
- Multi-Cloud
- Encryption
- Firewall
- Cloud-Native
- Cloud Access

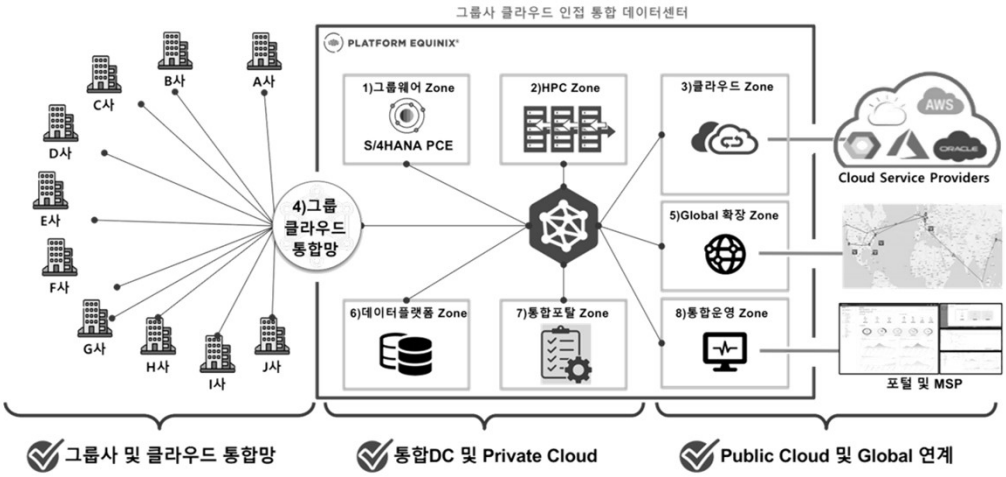


Source: https://aviatrix.com/wp-content/uploads/2020/07/Multi-Cloud-Networking-by-Futuriom-July2020.pdf

153

데이터센터 통합

❖ 데이터센터 통합



Source: Equinix

154

포트폴리오

❖ 포트폴리오

- Digital Service
- Interconnect Service
- Datacenter Service

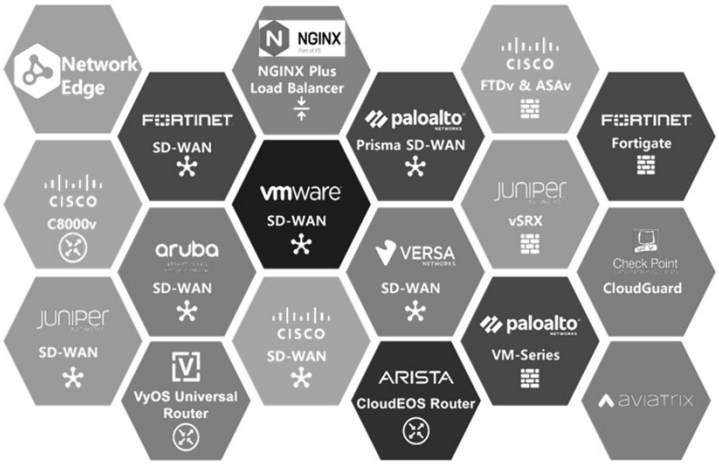
Storage	BCDR	Virtualization	Containers / Kubernetes	DevOps Integrations	HCI	AI
고객 요구 사항을 충족하는 고성능의 유연한 스토리지 솔루션 프로비저닝	고성능 소프트웨어 정의 백업 및 복구	대부분의 가상화 플랫폼을 지원	Kubernetes 클러스터 배포 및 관리 도구	IaC (Infrastructure as Code, 코드형 인프라) 툴을 사용하여 Equinix Metal 프로비저닝을 자동화 및 CI/CD 파이프라인 속도 향상	상호연결을 통해 원하는 위치에 자동 배포되는 HCI 어플라이언스 및 SDDC (SW Defined Data Center)	Equinix Metal은 AI 모델링 및 추론을 지원하기 위해 GPU 인프라를 제공합니다.
PURESTORAGE, NetApp, DELL Power Store, wasabi, LYVE Cloud, Backblaze, CLOUDIAN, MINIO	COHESITY, veeam	vmware vSphere, AHV, KVM, PROXMOX	Anthos, Red Hat OpenShift, aws EKS ECS, CANONICAL, MIRANTIS K3S, RANCHER, PLATFORM9, RAFAY, KUBERMATIC	Terraform, ANSIBLE, Pulumi, Crossplane, Apache Libcloud	NUTANIX, DELL Technologies, VXRAIL	LaunchPad NVIDIA. * LaunchPad는 Equinix 의 프라이빗 가속 컴퓨팅 인프라에서 NVIDIA의 AI 기능을 AI 개발자들이 단기간에 추시 이용할 수 있도록 설계된 NVIDIA와 Equinix 간의 협업 솔루션입니다.

Source: Equinix

155

NFV AT NETWORK EDGE

❖ NFV at Network Edge



Virtual Router Devices
- Cisco Catalyst 8000V Edge Router
- Arista CloudEOS Router
- VyOS Universal Router

Virtual Firewall Devices
- Check Point CloudGuard Network Security
- Cisco Adaptive Security Appliance (ASAv)
- Cisco Firepower Threat Defense (FTDv)
- Fortinet Fortigate VM Firewall
- Juniper vSRX Virtual Firewall
- Palo Alto VM-Series NGFW Firewall

SD-WAN Devices
- Aruba Unity Edge Connect SDWAN (formerly Silver Peak)
- Cisco CSR SD-WAN (formerly Viptela/cEdge)
- Fortinet Fortigate Secure SDWAN
- Juniper VSRX SD-WAN
- Palo Alto Networks Prisma SD-WAN (formerly CloudGenix)
- Versa FlexVNF
- VMware SD-WAN Edge (formerly Velocloud)

Load Balancer
- F5 Networks NGINX Plus Load Balancer

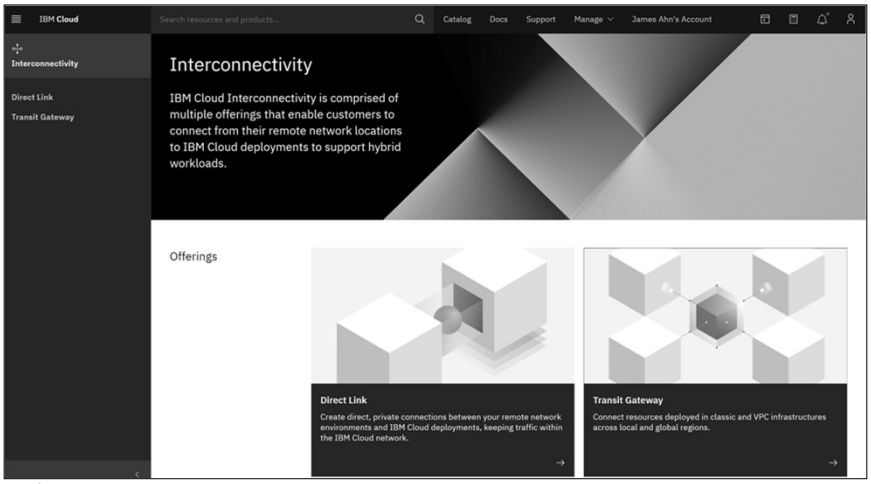
Source: Equinix

156

IBM CLOUD – INTERCONNECTIVITY

❖ CSP 포털 (예): IBM Cloud – Interconnectivity

- Direct Link
- Transit Gateway



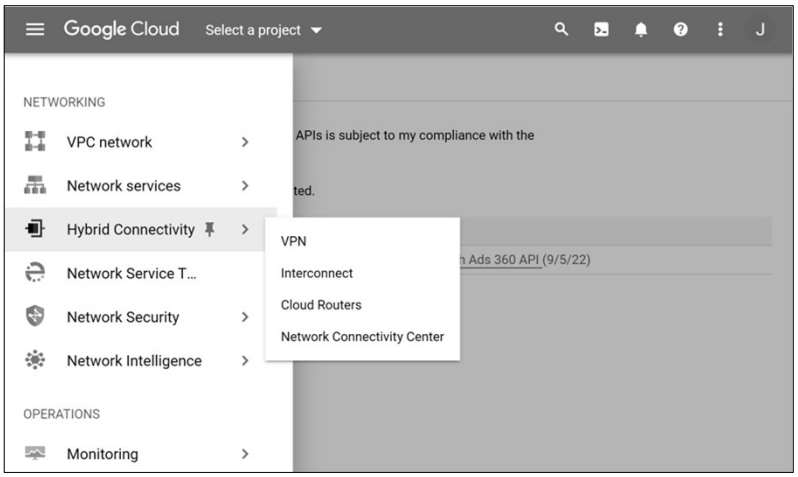
Source: https://cloud.ibm.com/catalog?category=network

157

GOOGLE CLOUD NETWORKING

❖ CSP 포털 (예): Google Cloud Networking – Hybrid Connectivity

- VPN
- Interconnect
- Cloud Routers
- Network Connectivity Center

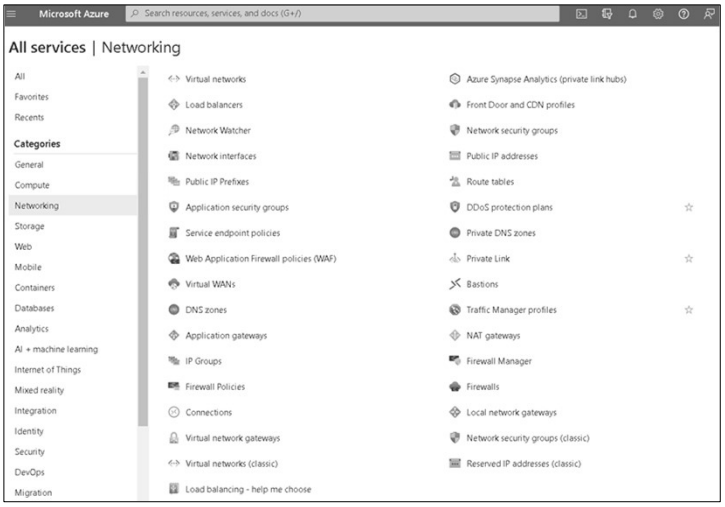


Source: https://console.cloud.google.com/products#networking

158

AZURE NETWORKING

❖ CSP 포털 (예): Azure Networking

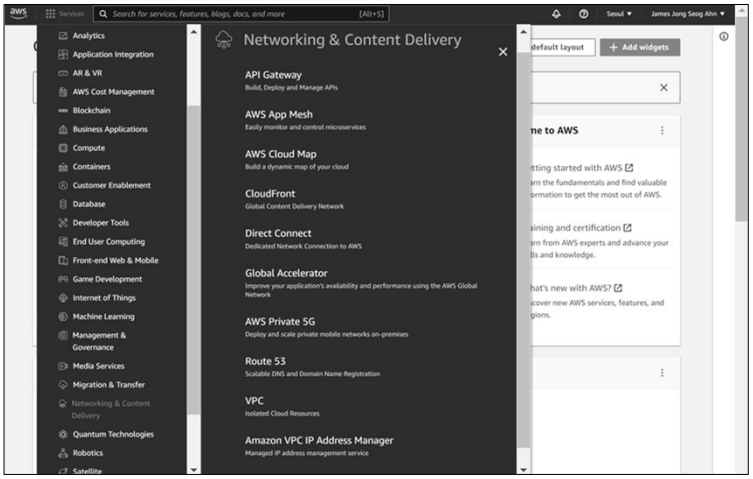


Source: https://portal.azure.com/#allservices/category/Networking

AMAZON AWS – NETWORKING

❖ CSP 포털 (예): Amazon AWS – Networking & Contents Delivery

- API Gateway
- AWS App Mesh
- AWS Cloud Map
- CloudFront
- Direct Connect
- Global Accelerator
- AWS Private 5G
- Route 53
- VPC
- Amazon VPC IP Address Manager

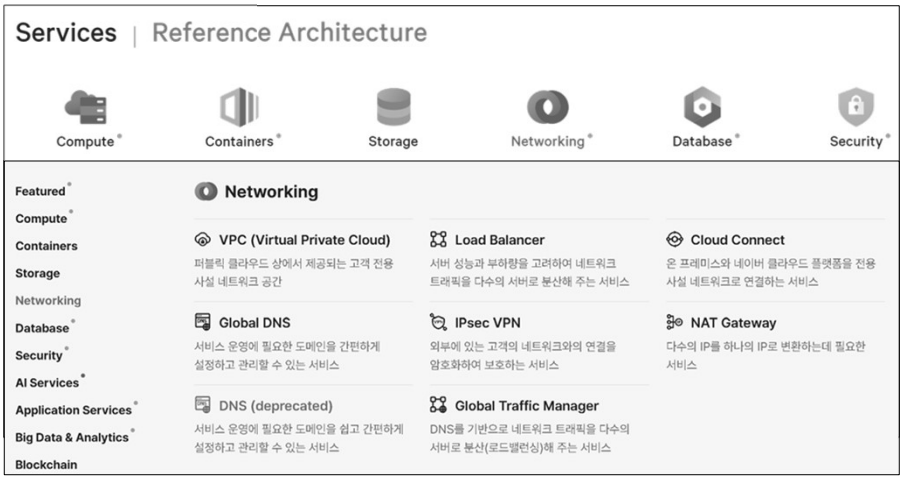


Source: https://ap-northeast-2.console.aws.amazon.com/console/home?region=ap-northeast-2#

NAVER CLOUD – NETWORKING

❖ CSP 포털 (예): Naver Cloud – Networking

- VPC
- Global DNS
- SSL VPN
- Load Balancer
- IPsec VPN
- Global Route Manager
- Cloud Connect
- NAT Gateway
- DNS

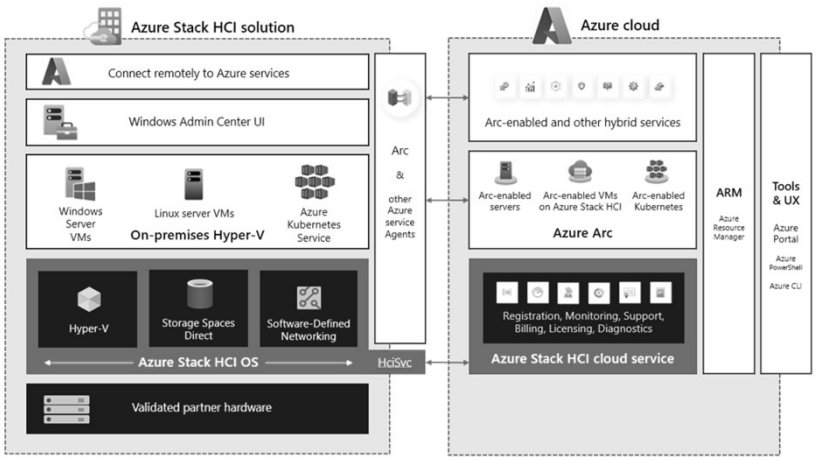


Source: https://www.ncloud.com/

161

AZURE STACK HCI

❖Azure Stack HCI hybrid capabilities with Azure services



Source: https://learn.microsoft.com/en-us/azure-stack/hci/hybrid-capabilities-with-azure-services

162

AZURE STACK EDGE

❖Azure Stack Edge pricing

Pro 2

Pro

Pro R

Azure Stack Edge Pro 2 | Azure Stack Edge Pro | Azure Stack Edge Pro R | Azure Stack Edge Mini R

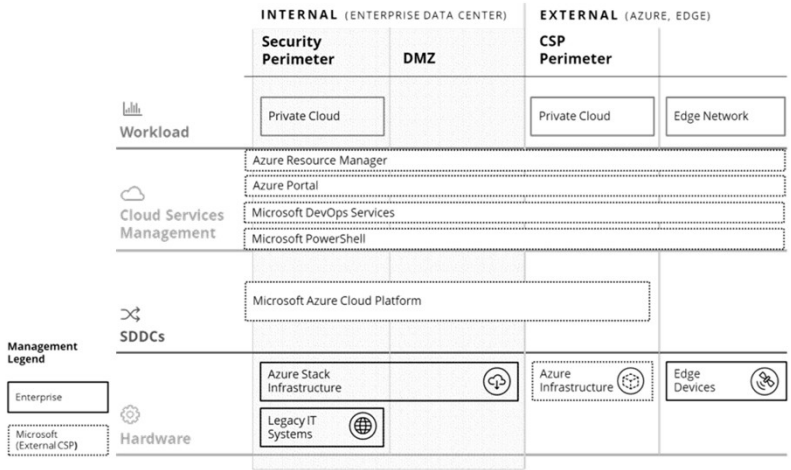
Service	Unit	Price
Monthly subscription fee	Model: 64G2T 32 vCPUs, 51 GB RAM, 720 GB	₩573,936
Monthly subscription fee	Model: 128G4T1GPU 32 vCPUs, 102 GB RAM, 1.6 TB, 1 x NVIDIA A2 GPU	₩748,429
Monthly subscription fee	Model: 256G6T2GPU 32 vCPUs, 204 GB RAM, 2.5 TB, 2 x NVIDIA A2 GPUs	₩885,080
Shipping	1 unit	₩503,983

Source: https://azure.microsoft.com/en-us/pricing/details/azure-stack/edge/#pricing

163

AZURE REFERENCE

❖MICROSOFT HYBRID CLOUD REFERENCE ARCHITECTURE



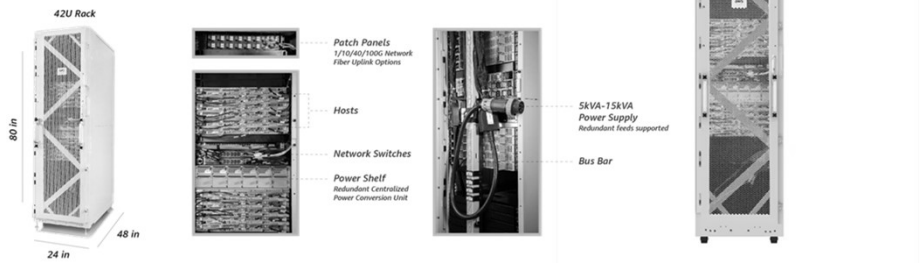
Source: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-designing-hybrid-cloud-architecture-for-the-future.pdf

164

AWS OUTPOSTS

❖**Outposts 실행 가능 AWS 서비스** (AWS Native 또는 VMware 모드 제공)

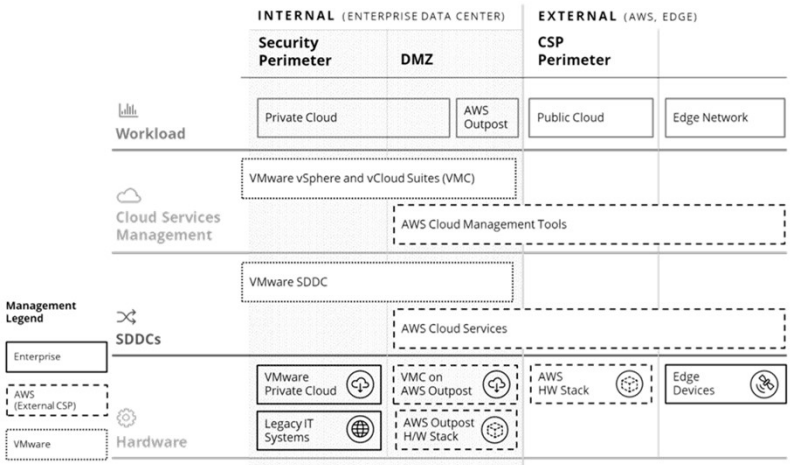
- **컴퓨트: Amazon EC2, Amazon ECS, Amazon EKS**
- **스토리지: Amazon EBS**
- **데이터베이스: Amazon RDS (Preview)**
- **분석: Amazon EMR**



Source: https://aws.amazon.com/ko/outposts/specs/

AWS REFERENCE

❖**AWS Outposts rack AWS OUTPOSTS REFERENCE ARCHITECTURE**

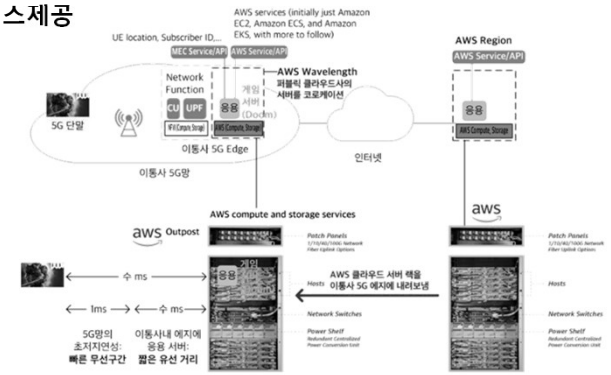


Source: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-designing-hybrid-cloud-architecture-for-the-future.pdf

AMAZON AWS WAVELENGTH

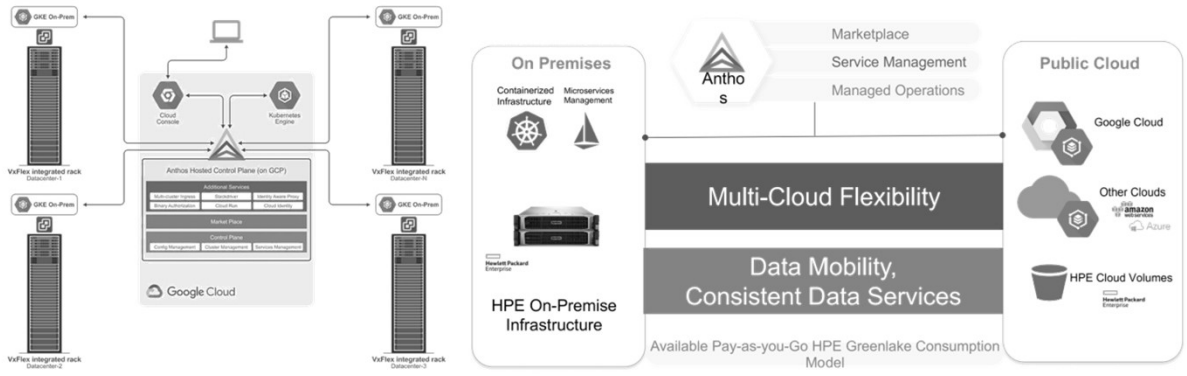
❖**Use Case: Amazon AWS Wavelength**

- **5G 네트워크 에지에서 AWS 커퓨팅 및 스토리지를 사용하여, 5G 기반 모바일 기기 및 사용자에게 초저지연 서비스를 제공하는 애플리케이션 제공 가능 (AWS Ourposts 기반)**
- **AWS 리전과 통신사 5G 망을 직접연결**
- **로컬 컴퓨팅, 스토리지, 데이터베이스 및 기타 서비스제공**
- **5G 기반 새로운 모바일 앱 제공**



ANTHOS

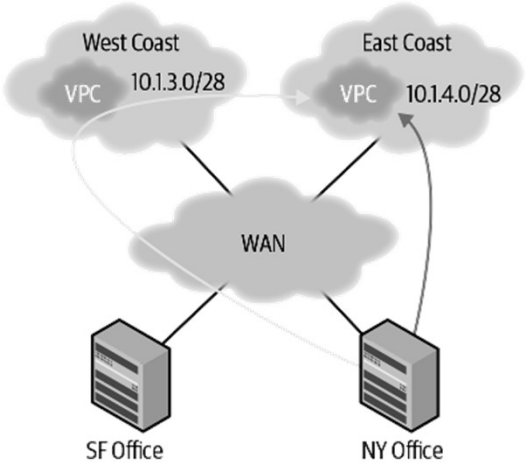
❖**소프트웨어 기반 Anthos 는 구글에서 Dell EMC나 HPE등의 하드웨어 파트너와 협력 멀티클라우드 솔루션으로 확대 중**



Source: https://cloud.google.com/anthos/docs/concepts/overview

DIRECT-CONNECT MODEL

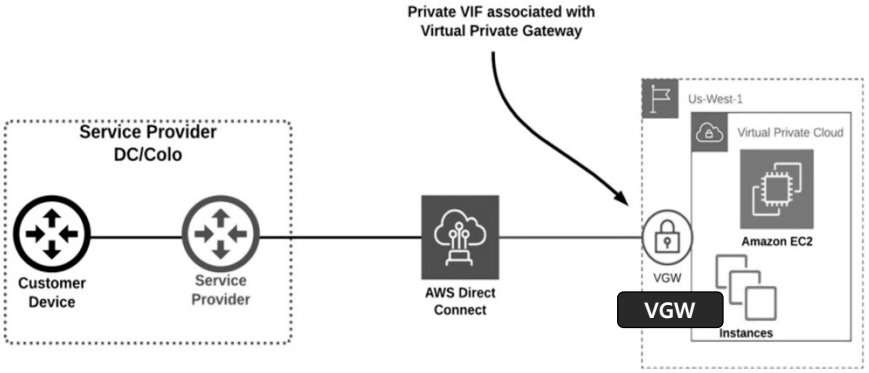
❖ Nonoptimal routing scenario with direct-connect model



Source: Cloud Native Data Center Networking (Architecture, Protocols, and Tools), Dinesh G. Dutt, O'REILLY

VIRTUAL PRIVATE GATEWAY (VGW)

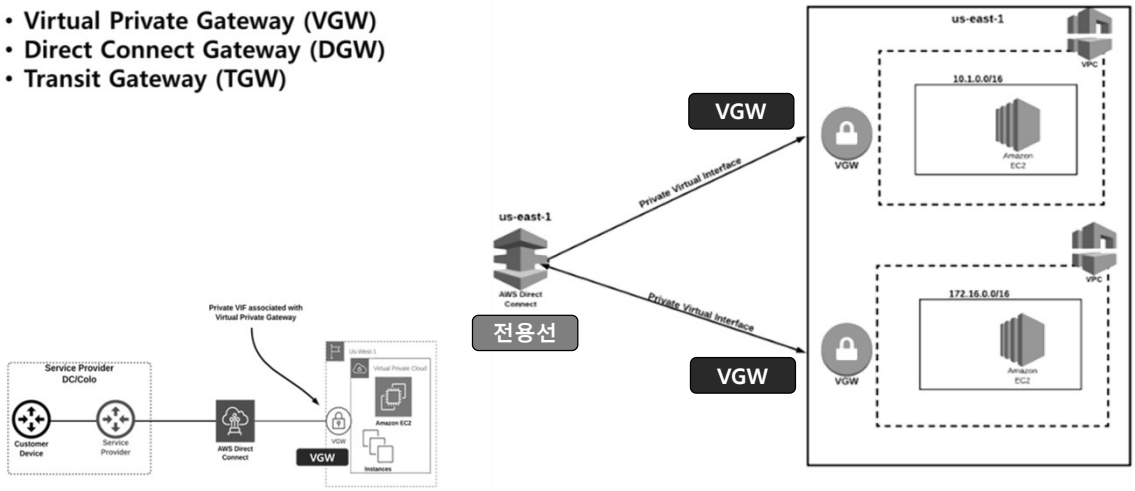
❖ AWS
- Virtual Private Gateway (VGW)
- Direct Connect Gateway (DGW)
- Transit Gateway (TGW)



Source: https://www.megaport.com/blog/aws-vgw-vs-dgw-vs-tgw/

VIRTUAL PRIVATE GATEWAY (VGW)

❖ AWS
- Virtual Private Gateway (VGW)
- Direct Connect Gateway (DGW)
- Transit Gateway (TGW)

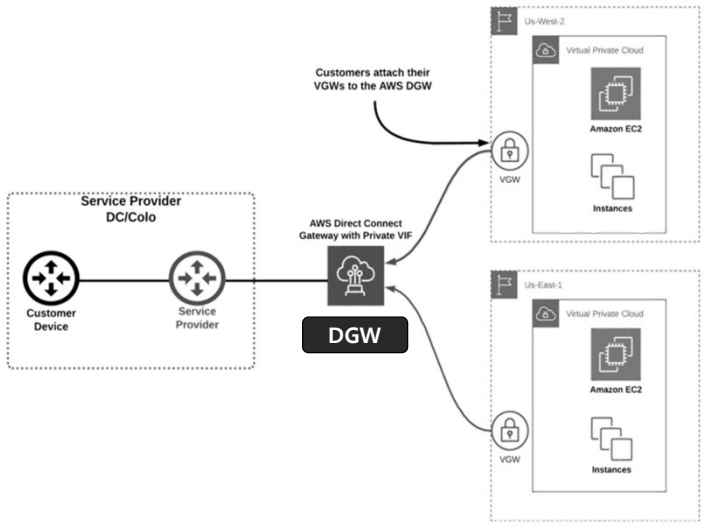


Source: https://www.megaport.com/blog/aws-vgw-vs-dgw-vs-tgw/

171

DIRECT CONNECT GATEWAY (DGW)

❖ AWS
- Virtual Private Gateway (VGW)
- Direct Connect Gateway (DGW)
- Transit Gateway (TGW)

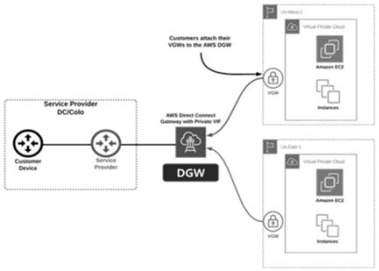


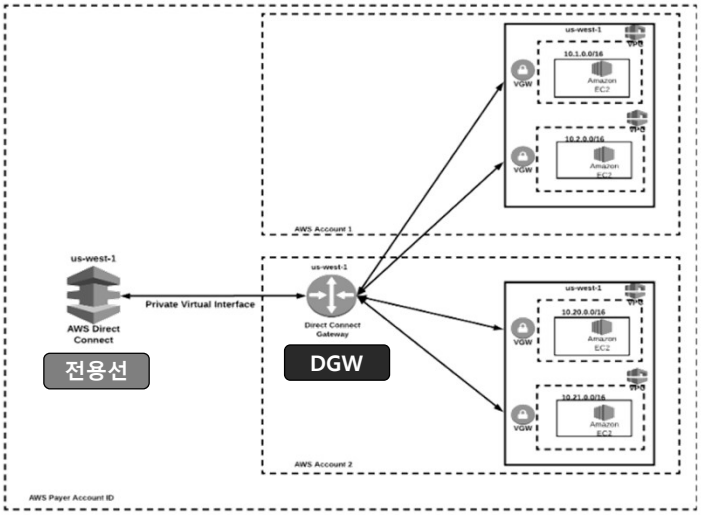
Source: https://www.megaport.com/blog/aws-vgw-vs-dgw-vs-tgw/

172

DIRECT CONNECT GATEWAY (DGW)

❖ AWS
- Virtual Private Gateway (VGW)
- Direct Connect Gateway (DGW)
- Transit Gateway (TGW)



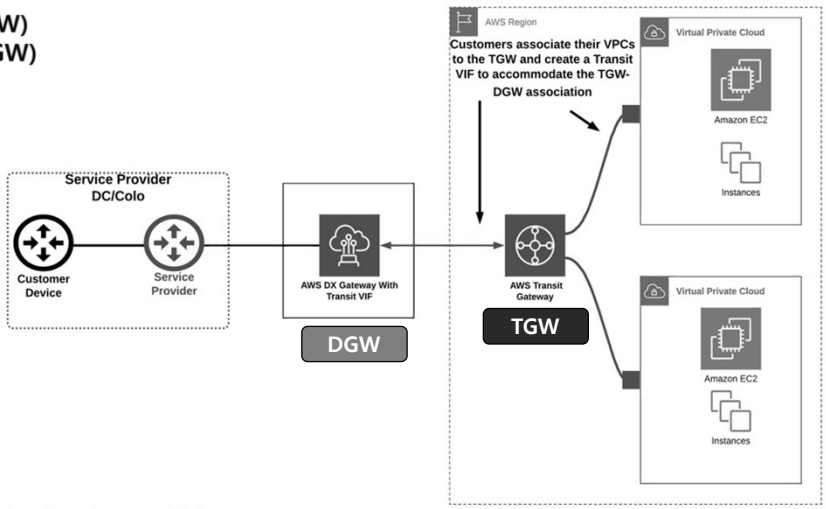


Source: https://www.megaport.com/blog/aws-vgw-vs-dgw-vs-tgw/

173

TRANSIT GATEWAY (TGW)

❖ AWS
- Virtual Private Gateway (VGW)
- Direct Connect Gateway (DGW)
- Transit Gateway (TGW)



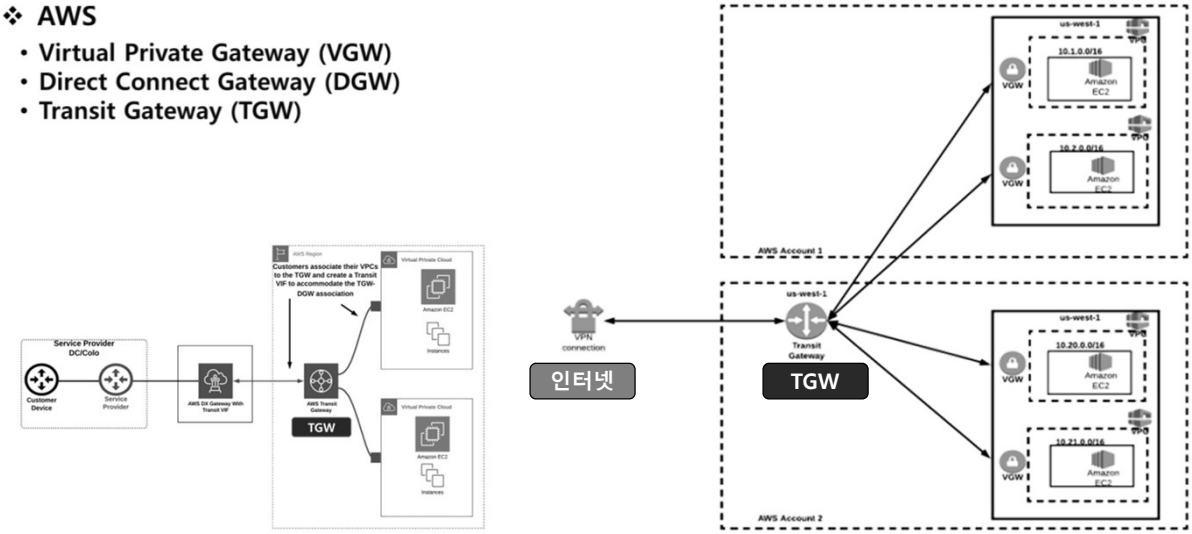
Source: https://www.megaport.com/blog/comparing-cloud-providers-private-connectivity/

174

TRANSIT GATEWAY (TGW)

❖ AWS

- Virtual Private Gateway (VGW)
- Direct Connect Gateway (DGW)
- Transit Gateway (TGW)



Source: https://www.megaport.com/blog/comparing-cloud-providers-private-connectivity/

175

VPN: SITE-TO-SITE VPN

❖ 데이터센터 연결

- VPN: Site-to-Site VPN
- Direct Connect

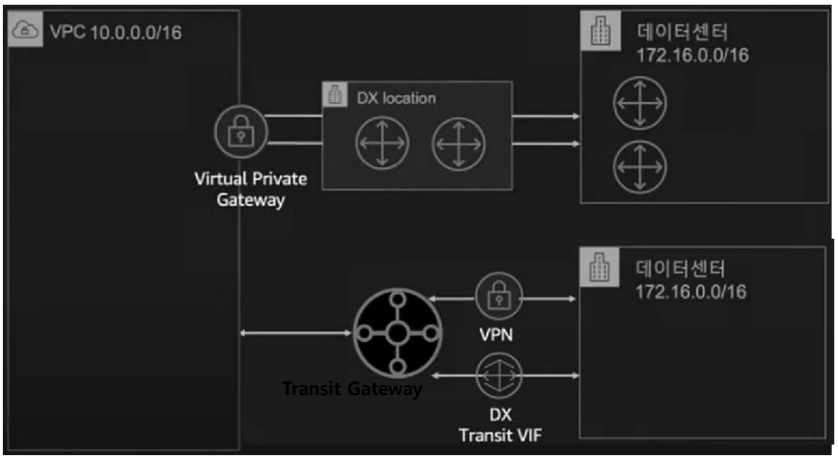
Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

176

DIRECT CONNECT: DX

❖ 데이터센터 연결

- VPN: Site-to-Site VPN
- Direct Connect: DX



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

177

AWS VGW VS DGW VS TGW

❖ AWS VGW vs DGW vs TGW

	Multiple Region	Multiple Account	S2S VPN	Direct Connect	Transitive Routing	Globally Available	Route Segmentation
VGW	✗	✗	☑	☑	✗	☑	✗
DGW	☑	☑	✗	☑	✗	☑	✗
TGW	☑	☑	☑	☑	☑	✗	☑

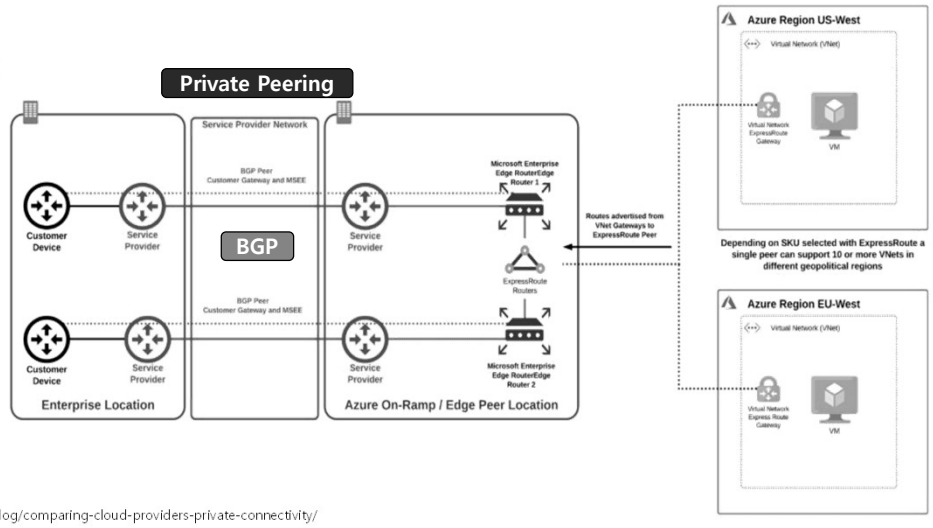
Source: https://www.megaport.com/blog/aws-vgw-vs-dgw-vs-tgw/

178

PRIVATE PEERING

❖ Azure

- Private Peering
- Microsoft Peering



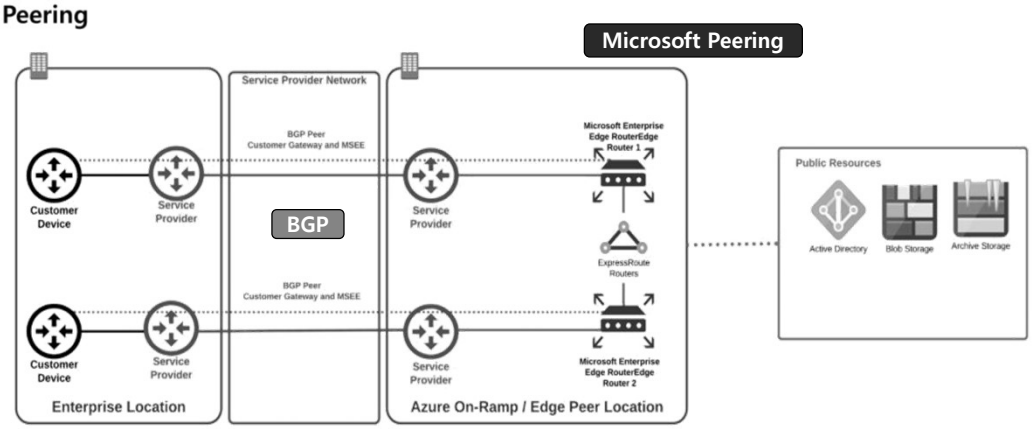
Source: https://www.megaport.com/blog/comparing-cloud-providers-private-connectivity/

179

MICROSOFT PEERING

❖ Azure

- Private Peering
- Microsoft Peering

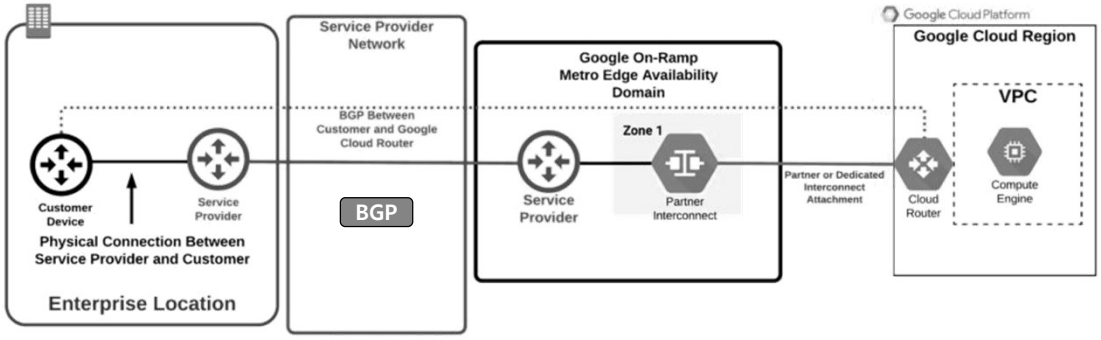


Source: https://www.megaport.com/blog/comparing-cloud-providers-private-connectivity/

180

GOOGLE CLOUD INTERCONNECT

❖ Google Cloud Interconnect

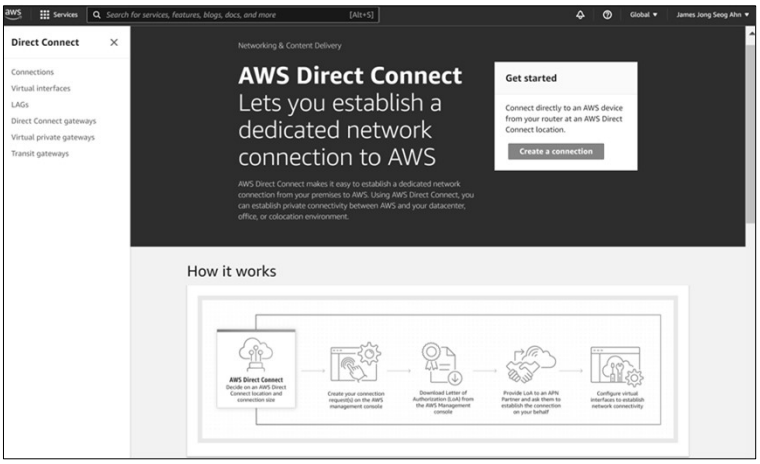


Source: https://www.megaport.com/blog/comparing-cloud-providers-private-connectivity/

AMAZON AWS – DIRECT CONNECT

❖ Amazon AWS – Direct Connect

- Connections
- Virtual interfaces
- LAGs
- Direct Connect gateways
- Virtual private gateways
- Transit gateways

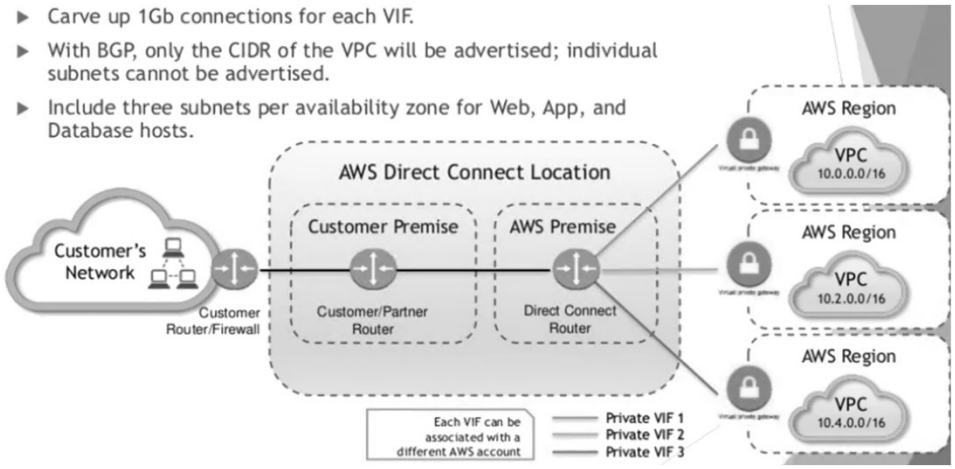


Link aggregation (LAG)
Source: https://us-east-1.console.aws.amazon.com/directconnect/v2/home?region=ap-northeast-2#/

DIRECT CONNECT ARCHITECTURE (AWS)

❖ **Direct Connect Architecture (AWS)**

- Carve up 1Gb connections for each VIF.
- With BGP, only the CIDR of the VPC will be advertised; individual subnets cannot be advertised.
- Include three subnets per availability zone for Web, App, and Database hosts.



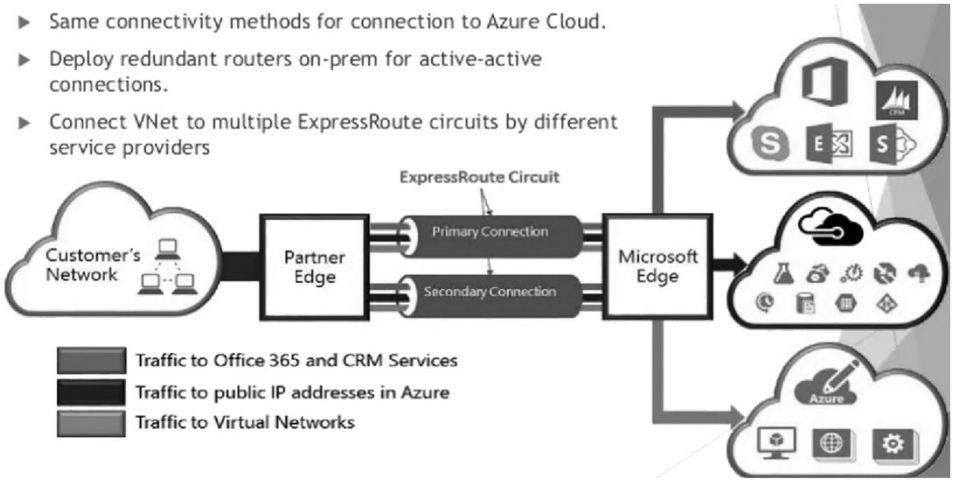
Virtual Network Interface (VIF)
Source: Joseph Primicerio

183

EXPRESSROUTE (AZURE)

❖ **ExpressRoute (Azure)**

- Same connectivity methods for connection to Azure Cloud.
- Deploy redundant routers on-prem for active-active connections.
- Connect VNet to multiple ExpressRoute circuits by different service providers



Source: Joseph Primicerio

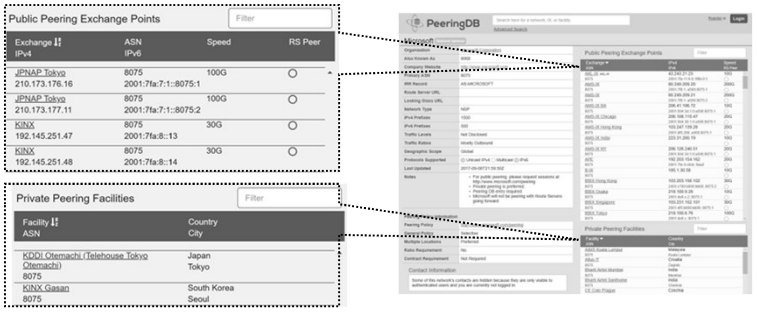
184

PUBLIC INTERCONNECT AND POP

❖ Public interconnect and points of presence(PoP)

- Microsoft is the second-largest network provider on the globe, and this is also reflected in their PoPs.
- For public peering, Microsoft currently offers over 160 locations, and for private peering, they are available in more than 50 locations. Public and private peering is all handled via ASN 8075.

https://www.peeringdb.com/net/694

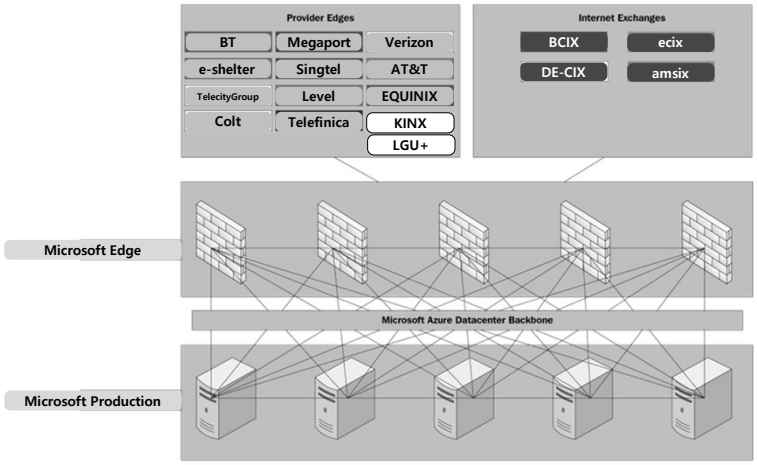


Source: Multi-Cloud for Architects (Published by Packt Publishing Ltd) Florian Klaffenbach, Markus Klein, Suresh Sundaresan

185

MICROSOFT POP OR EDGE SITE

❖ Schematic view of the structure behind a Microsoft PoP or Edge site



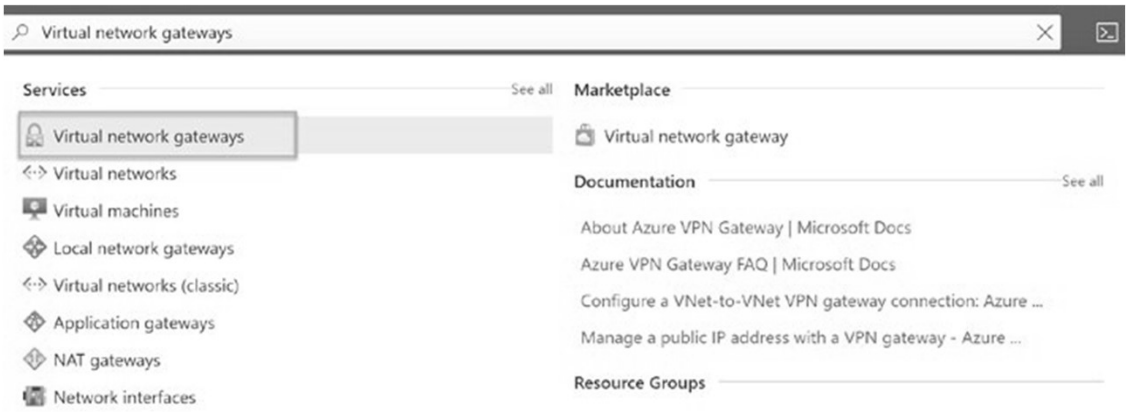
Source: Multi-Cloud for Architects (Published by Packt Publishing Ltd) Florian Klaffenbach, Markus Klein, Suresh Sundaresan

186

AZURE VPN GATEWAYS

❖ Azure VPN Gateways

• Virtual network gateways

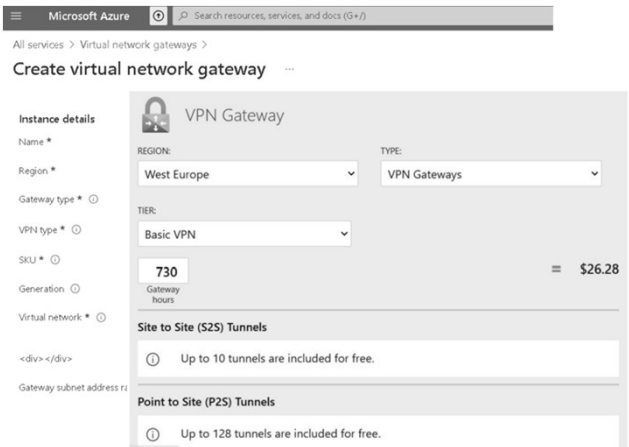


Source: https://portal.azure.com/

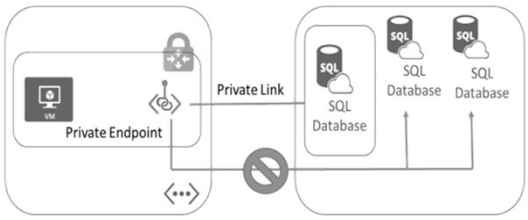
AZURE VPN GATEWAYS

❖ Technology strategy following business innovation

❖ Ordering the VPN Gateway functionality in the Azure cost model



Private Link uses a private endpoint so that gateways with NAT translating from public to private addresses—are no longer required:

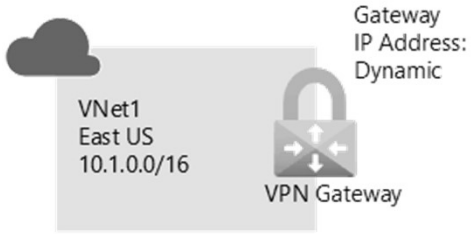


Source: Mulder, Jeroen. Multi-Cloud Architecture and Governance: Leverage Azure, AWS, GCP, and VMware vSphere to build effective multi-cloud solutions (p. 112). Packt Publishing. Kindle Edition.

AZURE VPN GATEWAYS

❖ Create and manage a VPN gateway using the Azure portal

- Create a virtual network
- Create a VPN gateway
- View the gateway public IP address
- Resize a VPN gateway (resize SKU)
- Reset a VPN gateway



Source: https://learn.microsoft.com/en-gb/azure/vpn-gateway/tutorial-create-gateway-portal?WT.mc_id=APC-Virtualnetworkgateways

189

AZURE VPN GATEWAYS

❖ Azure VPN Gateways

- Create a virtual network

✓Resource group: TestRG1
✓Name: VNet1
✓Region: (US) East US
✓IPv4 address space: 10.1.0.0/16
✓Subnet name: FrontEnd
✓Subnet address space: 10.1.0.0/24

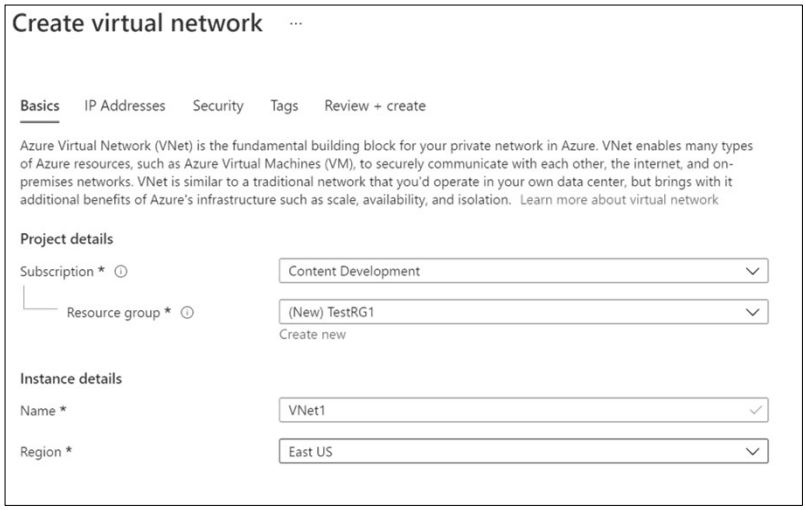
Source: https://learn.microsoft.com/en-gb/azure/vpn-gateway/tutorial-create-gateway-portal?WT.mc_id=APC-Virtualnetworkgateways

190

AZURE VPN GATEWAYS

❖ Azure VPN Gateways

• Create a virtual network



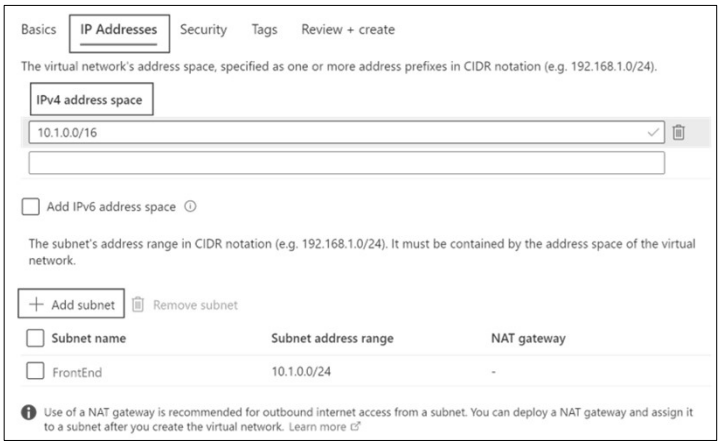
Source: https://learn.microsoft.com/en-gb/azure/vpn-gateway/tutorial-create-gateway-portal?WT.mc_id=APC-Virtualnetworkgateways

191

AZURE VPN GATEWAYS

❖ Azure VPN Gateways

• Select IP Addresses to advance to the IP Addresses tab



Source: https://learn.microsoft.com/en-gb/azure/vpn-gateway/tutorial-create-gateway-portal?WT.mc_id=APC-Virtualnetworkgateways

192

AZURE VPN GATEWAYS

❖ **Azure VPN Gateways**

- **Creating virtual network gateway**
  - ✓Name: VNet1GW
  - ✓Region: East US
  - ✓Gateway type: VPN
  - ✓VPN type: Route-based
  - ✓SKU: VpnGw2
  - ✓Generation: Generation 2
  - ✓Virtual network: VNet1
  - ✓Gateway subnet address range: 10.1.255.0/27
  - ✓Public IP address: Create new
  - ✓Public IP address name: VNet1GWpip

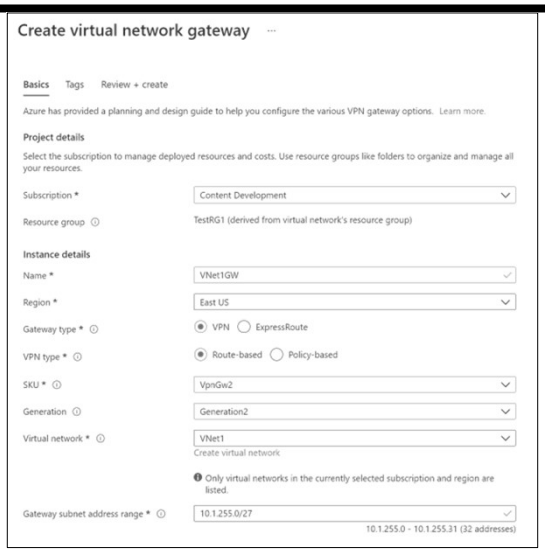
Source: https://learn.microsoft.com/en-gb/azure/vpn-gateway/tutorial-create-gateway-portal?WT.mc_id=APC-Virtualnetworkgateways

193

CREATING AZURE VPN GATEWAYS

❖ **Azure VPN Gateways**

- **Creating virtual network gateway**
  - ✓Name: VNet1GW
  - ✓Region: East US
  - ✓Gateway type: VPN
  - ✓VPN type: Route-based
  - ✓SKU: VpnGw2
  - ✓Generation: Generation 2
  - ✓Virtual network: VNet1
  - ✓Gateway subnet address range: 10.1.255.0/27
  - ✓Public IP address: Create new
  - ✓Public IP address name: VNet1GWpip
- **Creating virtual network gateway**
  - ✓On the Basics tab, fill in the values for Project details and Instance details.



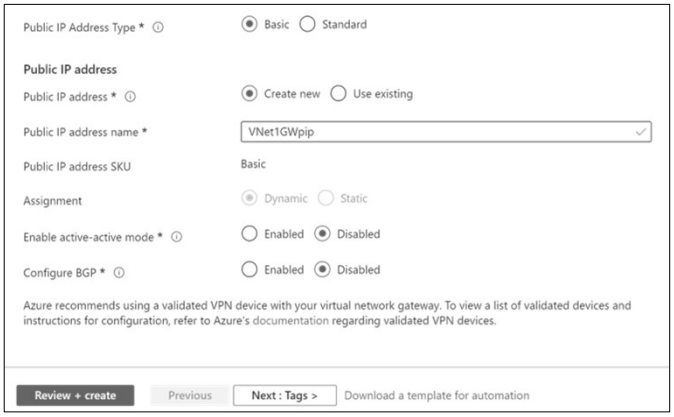
Source: https://learn.microsoft.com/en-gb/azure/vpn-gateway/tutorial-create-gateway-portal?WT.mc_id=APC-Virtualnetworkgateways

194

CREATING AZURE VPN GATEWAYS

❖ Azure VPN Gateways

- Creating virtual network gateway
- Specify in the values for Public IP address



Source: https://learn.microsoft.com/en-gb/azure/vpn-gateway/tutorial-create-gateway-portal?WT.mc_id=APC-Virtualnetworkgateways

195

AZURE VPN GATEWAYS – PUBLIC IP

❖ Azure VPN Gateways

- Creating virtual network gateway

✓View the public IP address

Source: https://learn.microsoft.com/en-gb/azure/vpn-gateway/tutorial-create-gateway-portal?WT.mc_id=APC-Virtualnetworkgateways

196

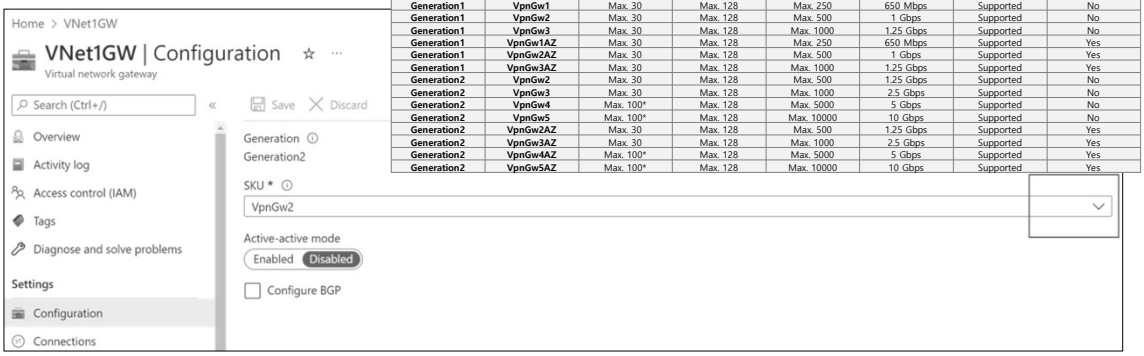
AZURE VPN GATEWAYS - SKU

❖ Azure VPN Gateways

• Creating virtual network gateway

✓Resize a gateway SKU

VPN Gateway Generation	SKU	S2S/VNet-to-VNet Tunnels	P2S SSTP Connections	P2S IKEv2/OpenVPN Connections	Aggregate Throughput Benchmark	BGP	Zone-redundant
Generation1	Basic	Max. 10	Max. 128	Not Supported	100 Mbps	Not Supported	No
Generation1	VpnGw1	Max. 30	Max. 128	Max. 250	650 Mbps	Supported	No
Generation1	VpnGw2	Max. 30	Max. 128	Max. 500	1 Gbps	Supported	No
Generation1	VpnGw3	Max. 30	Max. 128	Max. 1000	1.25 Gbps	Supported	No
Generation1	VpnGw1AZ	Max. 30	Max. 128	Max. 250	650 Mbps	Supported	Yes
Generation1	VpnGw2AZ	Max. 30	Max. 128	Max. 500	1 Gbps	Supported	Yes
Generation1	VpnGw3AZ	Max. 30	Max. 128	Max. 1000	1.25 Gbps	Supported	Yes
Generation2	VpnGw2	Max. 30	Max. 128	Max. 500	1.25 Gbps	Supported	No
Generation2	VpnGw3	Max. 30	Max. 128	Max. 1000	2.5 Gbps	Supported	No
Generation2	VpnGw4	Max. 100*	Max. 128	Max. 5000	5 Gbps	Supported	No
Generation2	VpnGw5	Max. 100*	Max. 128	Max. 10000	10 Gbps	Supported	No
Generation2	VpnGw2AZ	Max. 30	Max. 128	Max. 500	1.25 Gbps	Supported	Yes
Generation2	VpnGw3AZ	Max. 30	Max. 128	Max. 1000	2.5 Gbps	Supported	Yes
Generation2	VpnGw4AZ	Max. 100*	Max. 128	Max. 5000	5 Gbps	Supported	Yes
Generation2	VpnGw5AZ	Max. 100*	Max. 128	Max. 10000	10 Gbps	Supported	Yes



Source: https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways
Source: https://learn.microsoft.com/en-gb/azure/vpn-gateway/tutorial-create-gateway-portal?WT.mc_id=APC-Virtualnetworkgateways

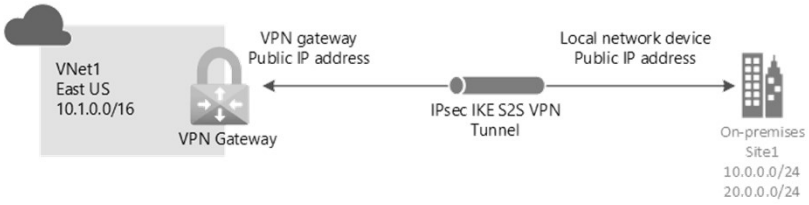
197

SITE-TO-SITE VPN IN THE AZURE PORTAL

❖ Create a site-to-site VPN connection in the Azure portal

• Create a site-to-site VPN connection in the Azure portal

✓Create a virtual network
✓Create a VPN gateway
✓Create a local network gateway
✓Create a VPN connection
✓Verify the connection
✓Connect to a virtual machine



Source: https://learn.microsoft.com/en-gb/azure/vpn-gateway/tutorial-site-to-site-portal

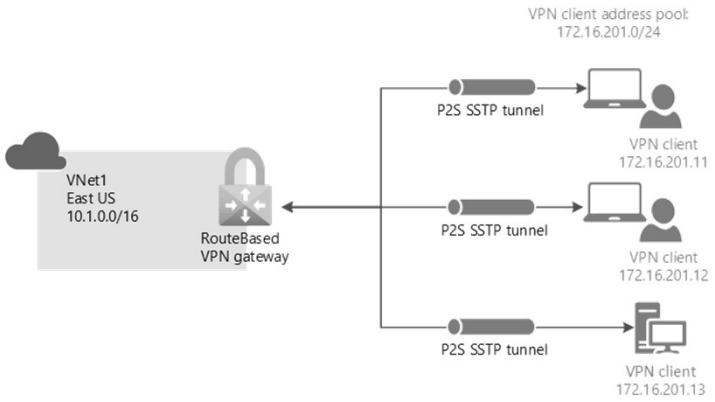
198

POINT-TO-SITE VPN CONNECTION

❖ Configure a point-to-site VPN connection using Azure certificate authentication

• Creating virtual network gateway

✓View the public IP address

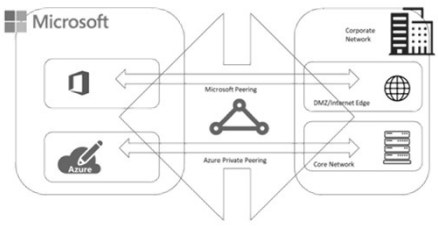


Source: https://learn.microsoft.com/en-gb/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal

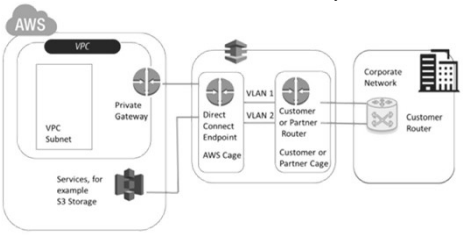
전용선 서비스 연계

❖ 전용선 서비스 연계

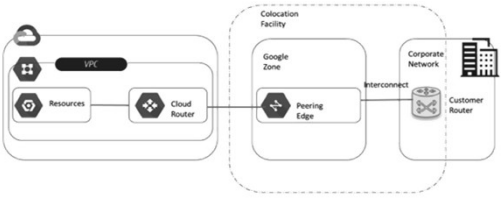
Microsoft's ExpressRoute concept



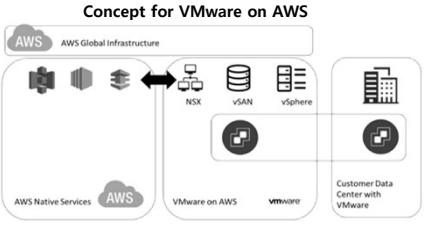
AWS' Direct Connect concept



Google's concept for Dedicated Interconnect



Concept for VMware on AWS



AZURE EXPRESSROUTE

❖ Unlimited Data plan(Azure ExpressRoute 예)

Circuit bandwidth	Local Circuit Price per Month	Standard circuit price per month	Premium circuit price per month	Inbound data transfer included	Outbound data transfer included
50 Mbps	N/A	**$300**	**$375**	Unlimited	Unlimited
100 Mbps	N/A	**$575**	**$675**	Unlimited	Unlimited
200 Mbps	N/A	**$1,150**	**$1,300**	Unlimited	Unlimited
500 Mbps	N/A	**$2,750**	**$3,150**	Unlimited	Unlimited
1 Gbps	**$1,200**	**$5,700**	**$6,450**	Unlimited	Unlimited
2 Gbps	**$2,200**	**$11,400**	**$12,900**	Unlimited	Unlimited
5 Gbps	**$3,600**	**$25,650**	**$28,650**	Unlimited	Unlimited
10 Gbps	**$5,500**	**$51,300**	**$54,300**	Unlimited	Unlimited

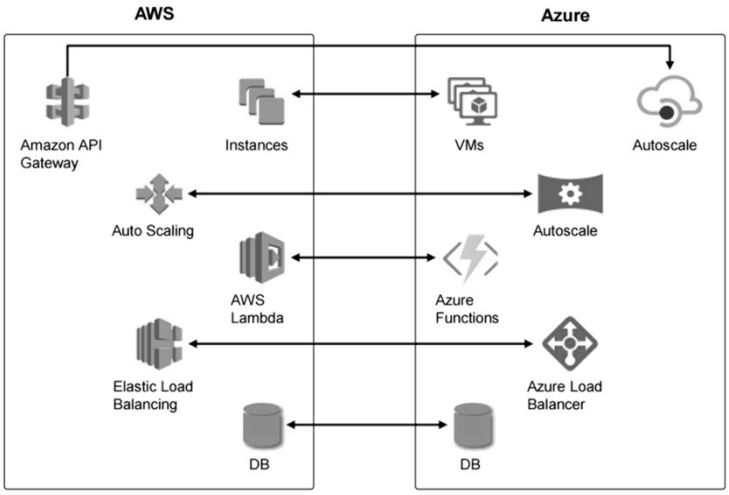
201

III. 멀티 클라우드의 연동

202

동일 서비스 고려

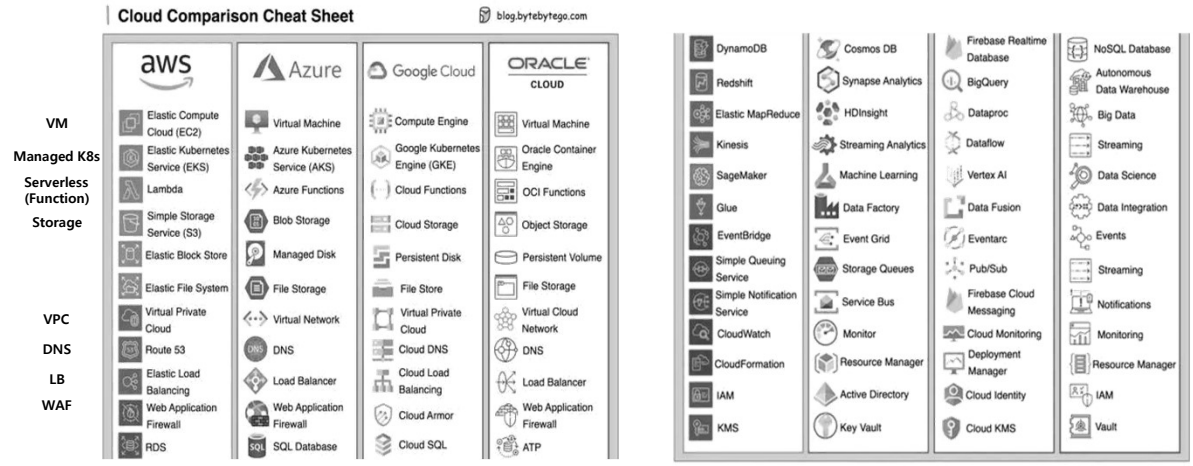
❖ 동일 서비스 고려하는 Multi-Cloud Architecture



203

AWS, GCP, AZURE

❖ Cloud Computing AWS, GCP, Azure



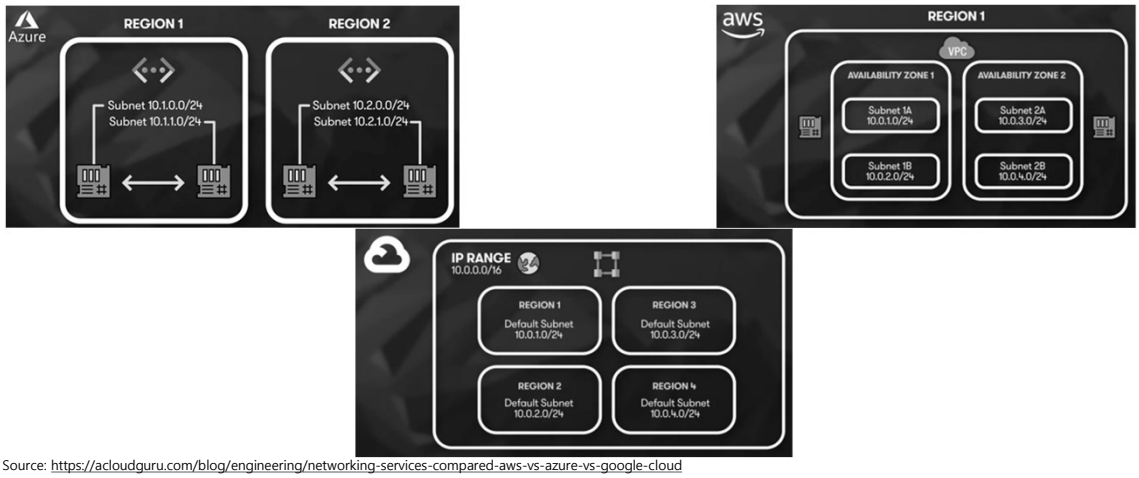
Source: https://www.facebook.com/groups/cloudcomputinglearn/permalink/2293891134128116/?sfnsn=mo&ref=share&mibextid=VhDh1V

204

NETWORKING SERVICES

❖ Networking services compared: AWS vs Azure vs Google Cloud

• Networking basics

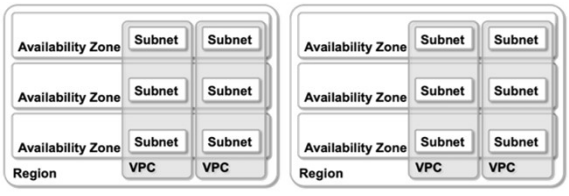


Source: https://acloudguru.com/blog/engineering/networking-services-compared-aws-vs-azure-vs-google-cloud

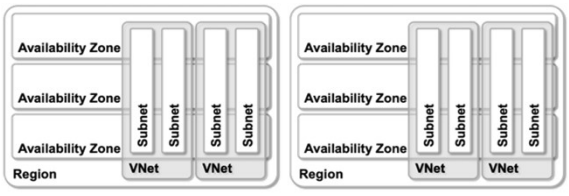
VIRTUAL NETWORKS AND SUBNETS

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

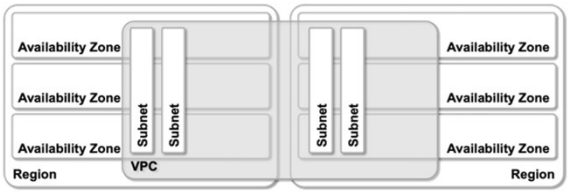
VPCs and subnets in AWS



VNet and subnets in Azure



GCP VPCs and subnets



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

CSP의 주요 네트워크 서비스

❖ CSP의 주요 네트워크 서비스 (예): Key network services for AWS, Azure, and GCP

Cloud Platform	Amazon Web Services (AWS)	Microsoft Azure	Google Cloud Platform (GCP)
Virtual Network	Amazon Virtual Private Cloud (VPC)	Virtual Networks (VNets)	Virtual Private Cloud
Data Center integration	Direct Connect	ExpressRoute	Google Cloud Interconnect
Load Balancer	Elastic Load Balancer	Load Balancer	Google Cloud Load Balancing
DNS	Amazon Route 53	Azure DNS	Google Cloud DNS
Firewall	AWS Firewall / Web Application Firewall	Azure Firewall	Google Cloud firewalls

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

207

IAAS NETWORKING SERVICES

❖ 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/

208

CSP 네트워크 용어

❖ CSP 네트워크 용어 (terminology alignment)

	aws	Azure	Google Cloud
Compute:	EC2 Instance	Virtual Machine (VM)	Compute Engine VMs
Object Storage:	S3	Blob Storage	Cloud Storage
가상 데이터센터 Logical Data Centre:	VPC VPC	vNet VNet	VPC VPC
전용선 Private Connectivity (L2):	Direct Connect Direct Connect	ExpressRoute ExpressRoute	Interconnect Interconnect
Route Gateways:	TGW, VGW, DGW	VNet Gateway	Cloud Router

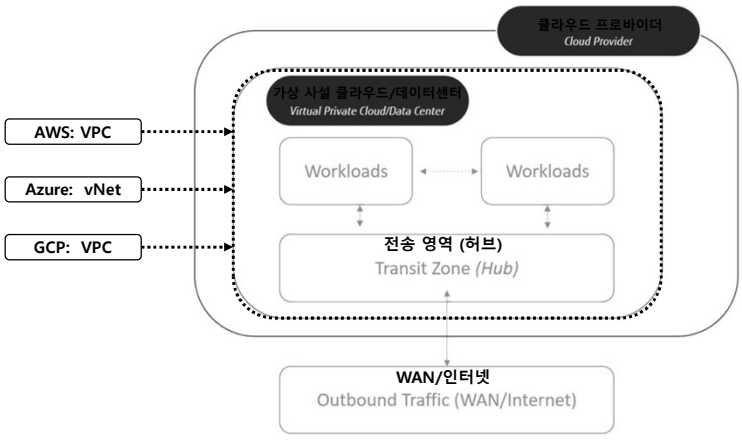
- Virtual Private Gateway (VGW)
- Direct Connect Gateway (DGW)
- Transit Gateway (TGW)

Source: https://www.megaport.com/blog/comparing-cloud-providers-private-connectivity/

209

하이레벨 멀티클라우드 가상데이터센터

❖ High-level diagram of a virtual private cloud/data center



Source: Mulder, Jeroen. Multi-Cloud Architecture and Governance: Leverage Azure, AWS, GCP, and VMware vSphere to build effective multi-cloud solutions (p. 74). Packt Publishing. Kindle Edition.

210

CSP 의 네트워킹 서비스

❖ Networking services compared: AWS vs Azure vs Google Cloud

• 가상 사설 데이터센터, BGP, VPN, 전용선, 방화벽

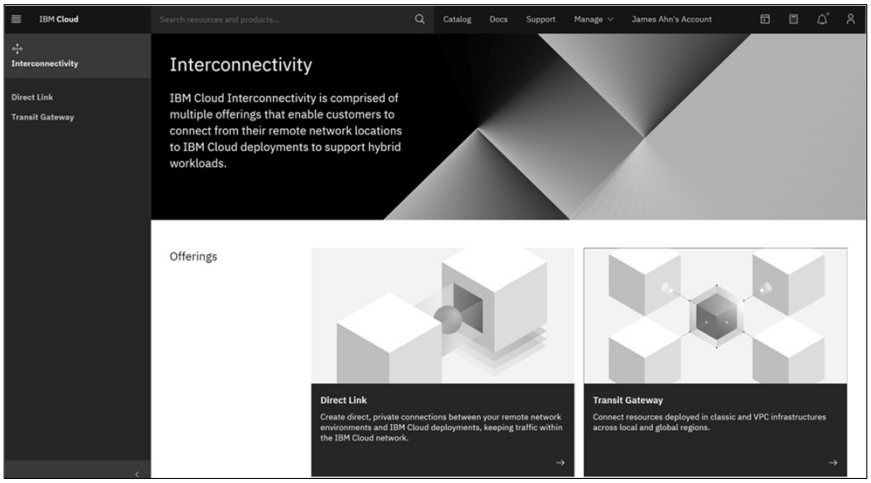
SERVICE NAME	aws	Azure	
	Virtual Private Cloud (VPC)	VNet	Virtual Private Cloud (VPC)
	Border Gateway Protocol BGP (BGP)	Border Gateway Protocol BGP (BGP)	Border Gateway Protocol BGP (BGP)
	AWS Transit Gateway AWS Direct Connect AWS Site-to-Site VPN	VPN Gateway ExpressRoute Gateway Azure Firewall	Shared VPC Cloud VPN Cloud Interconnect

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

IBM CLOUD – INTERCONNECTIVITY

❖ CSP 포털 (예): IBM Cloud – Interconnectivity

• Direct Link
• Transit Gateway

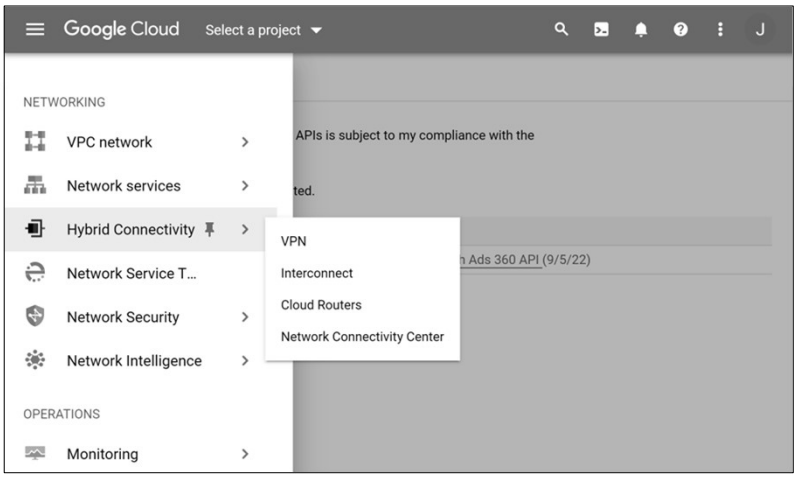


Source: https://cloud.ibm.com/catalog?category=network

GOOGLE CLOUD NETWORKING

❖ CSP 포털 (예): Google Cloud Networking – Hybrid Connectivity

- VPN
- Interconnect
- Cloud Routers
- Network Connectivity Center

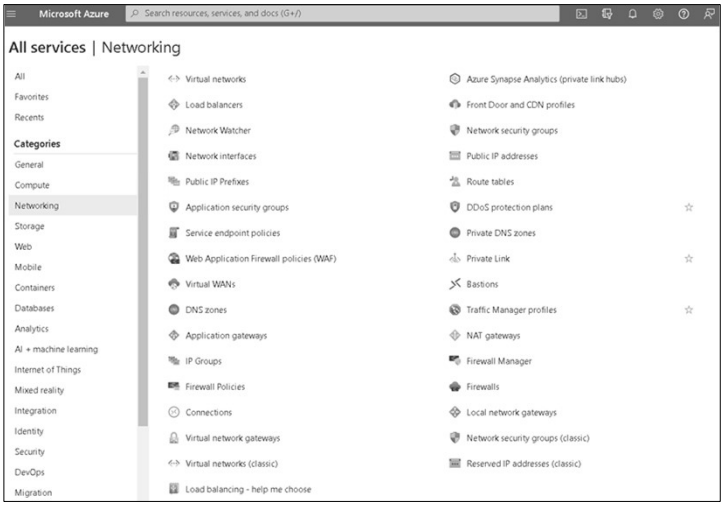


Source: https://console.cloud.google.com/products#networking

213

AZURE NETWORKING

❖ CSP 포털 (예): Azure Networking



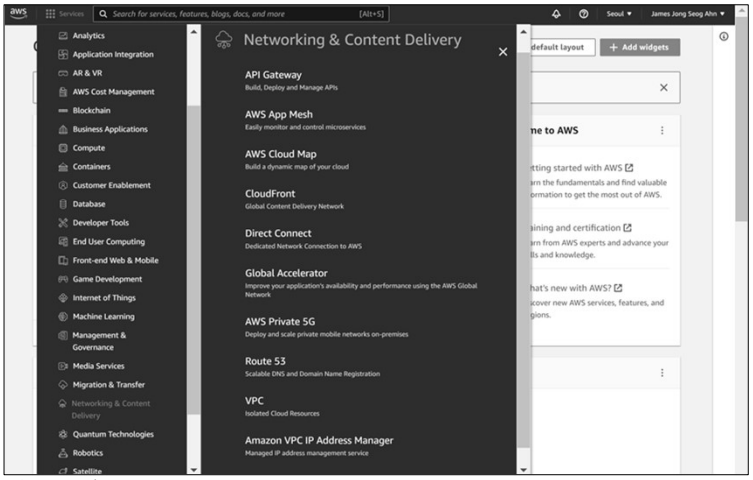
Source: https://portal.azure.com/#allservices/category/Networking

214

AMAZON AWS – NETWORKING

❖ CSP 포털 (예): Amazon AWS – Networking & Contents Delivery

- API Gateway
- AWS App Mesh
- AWS Cloud Map
- CloudFront
- Direct Connect
- Global Accelerator
- AWS Private 5G
- Route 53
- VPC
- Amazon VPC IP Address Manager

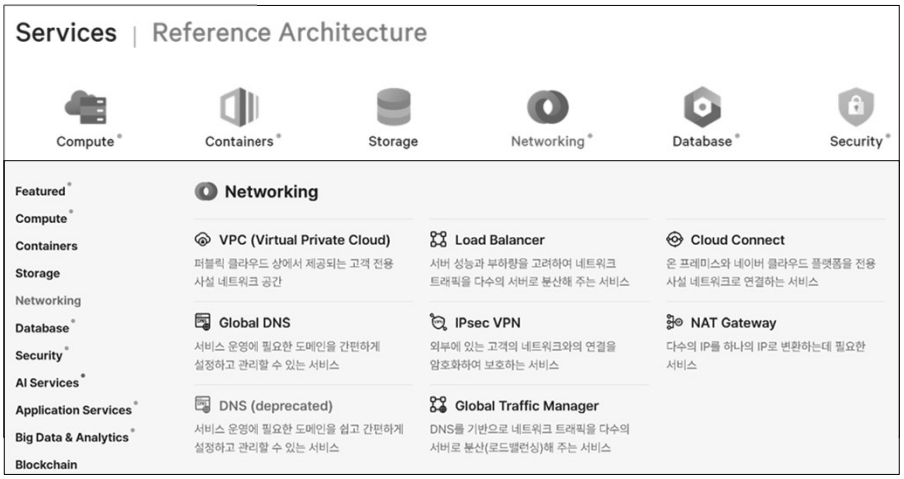


Source: https://ap-northeast-2.console.aws.amazon.com/console/home?region=ap-northeast-2#

NAVER CLOUD – NETWORKING

❖ CSP 포털 (예): Naver Cloud – Networking

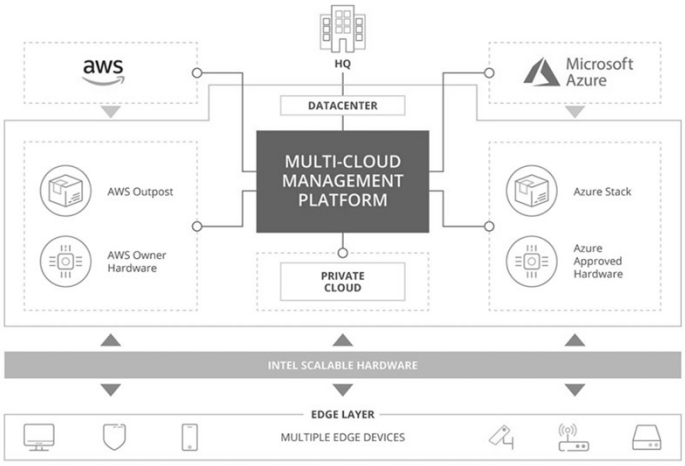
- VPC
- Global DNS
- SSL VPN
- Load Balancer
- IPsec VPN
- Global Route Manager
- Cloud Connect
- NAT Gateway
- DNS



Source: https://www.ncloud.com/

멀티클라우드 관리 플랫폼

❖ Multi Cloud Management Platform Reference Architecture

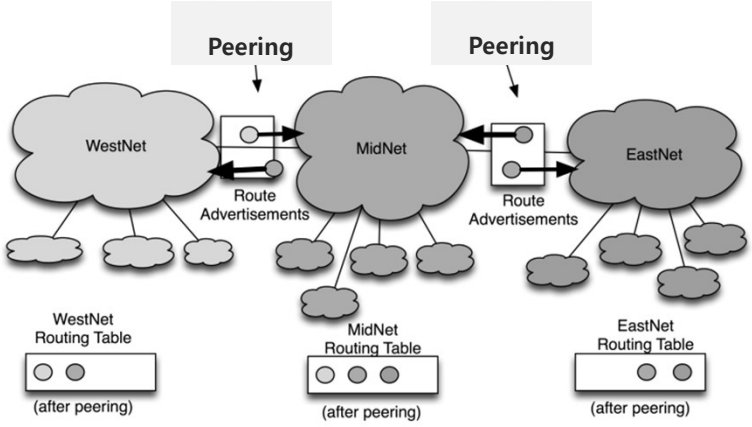


Source: https://www.infosectrain.com/blog/what-is-multi-cloud-network-architecture/#What-is-multi-cloud-network-architecture

피어링 PEERING

❖ 피어링 peering (1:1 연결)

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

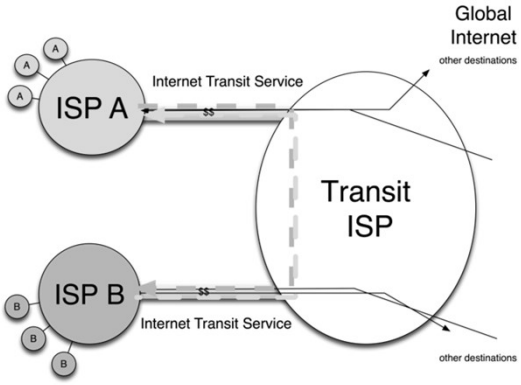


Source: https://m.clien.net/service/board/lecture/17610900

트랜짓 TRANSIT

❖ 트랜짓 transit (1:1:N 연결)

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

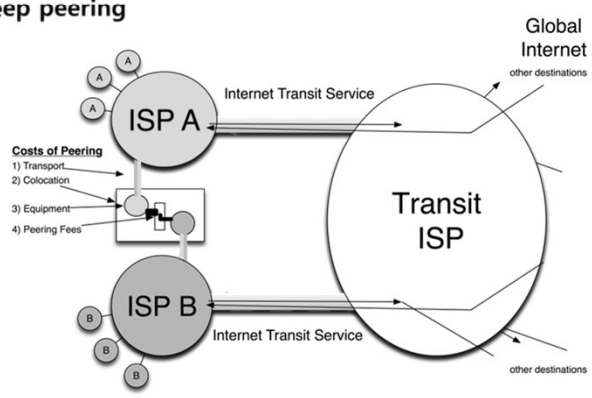


Source: https://m.clien.net/service/board/lecture/17610900

피어링 VS 트랜짓

❖ 피어링 vs 트랜짓

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

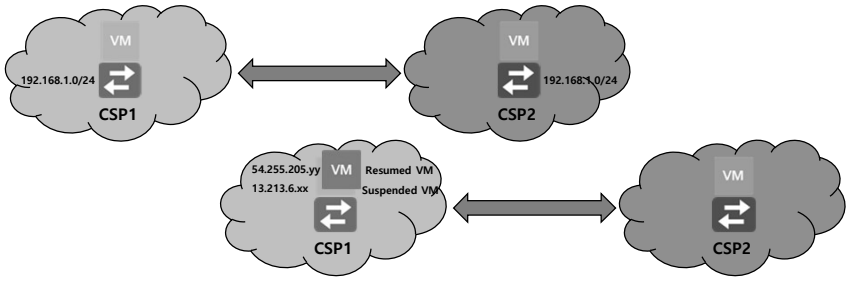


Source: https://m.clien.net/service/board/lecture/17610900

CHECK POINT

❖ Check point

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



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

221

CHECK POINT 해결 방법

❖ Check point 해결 방법

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

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

222

ORACLE CLOUD INFRASTRUCTURE

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

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

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

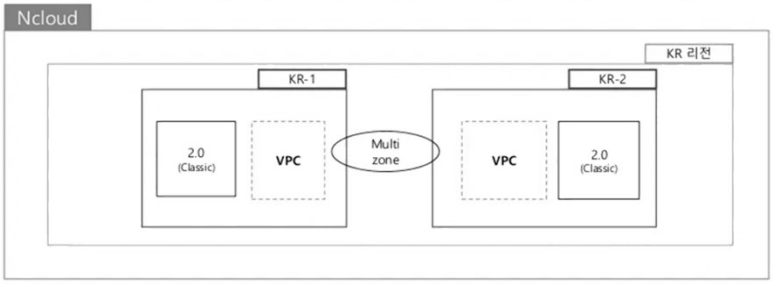
223

네이버클라우드플랫폼

❖ 네이버클라우드플랫폼 (NCP)

• Classic/VPC

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



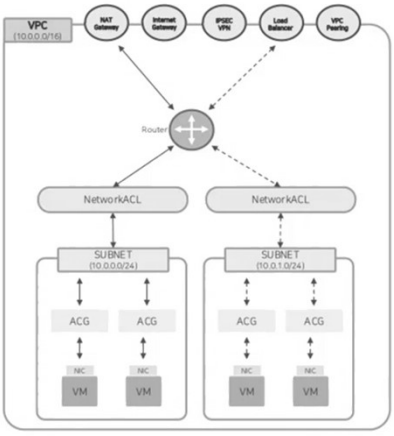
Source: https://www.slideshare.net/n_cloudplatform/ss-239153998

224

네이버클라우드플랫폼 VPC

❖ 네이버클라우드플랫폼 (NCP)

• VPC 기본 제어 기능



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

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

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

225

NCP의 VPC – 네트워크 구성 요소

❖ 네이버클라우드플랫폼 (NCP)

• VPC – 네트워크 구성 요소

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

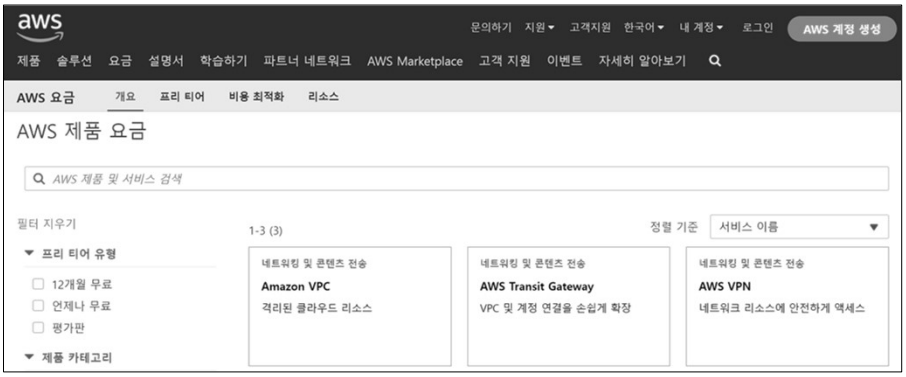
Source: https://www.slideshare.net/n_cloudplatform/ss-239153998

226

AWS 네트워크 제품

❖ AWS 제품 요금: 네트워킹 및 컨텐츠 전송 제품 카테고리

- Amazon VPC
- AWS Transit Gateway
- AWS VPN



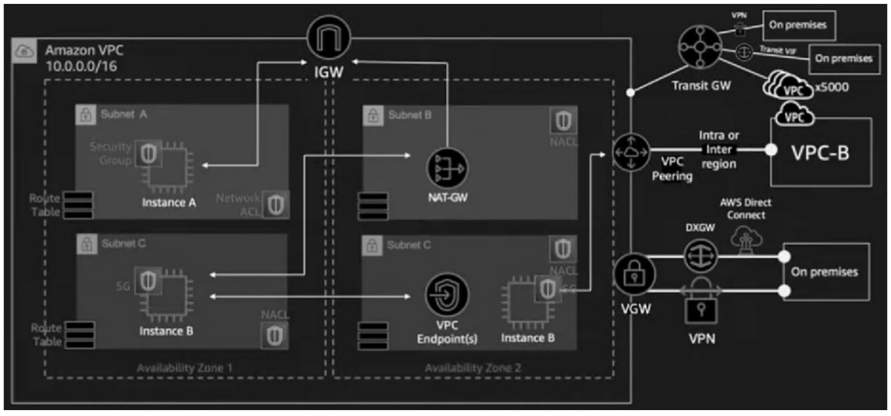
Source: https://aws.amazon.com/vpn/pricing/?did=ap_card&trk=ap_card
Source: https://aws.amazon.com/vpc/pricing/?did=ap_card&trk=ap_card , https://aws.amazon.com/transit-gateway/pricing/?did=ap_card&trk=ap_card

227

AWS VPC 구성 개요

❖ AWS VPC 구성 개요

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



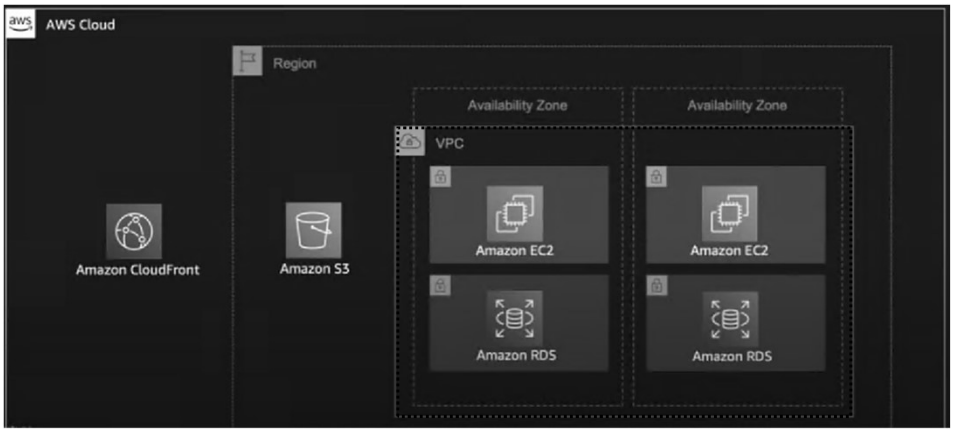
Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

228

AWS DEFAULT VPC

❖ AWS default VPC(버추얼 프라이빗 클라우드) 자원 레벨

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

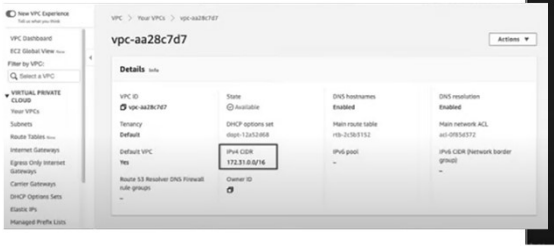


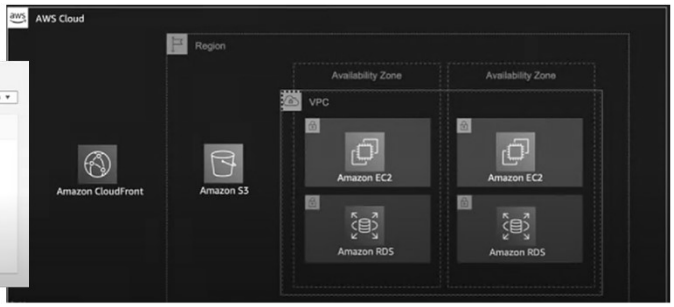
Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

AWS: 기본 VPC의 구성 요소

❖ AWS: 기본 VPC의 구성 요소

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



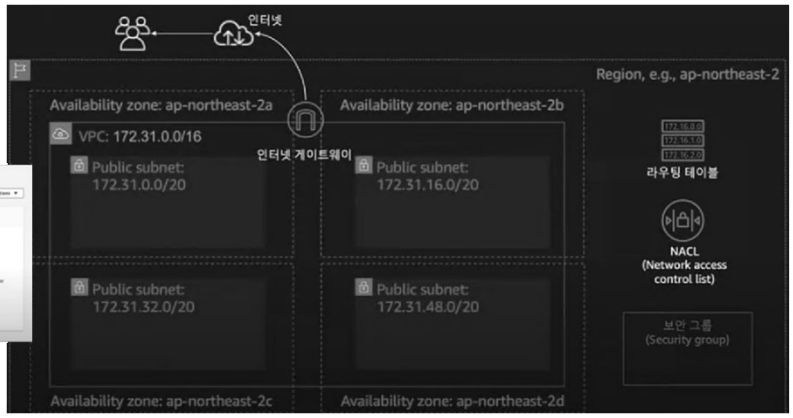


Source: https://www.44bits.io/ko/post/understanding_aws_vpc

DEFAULT VPC IP 주소 범위

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

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



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

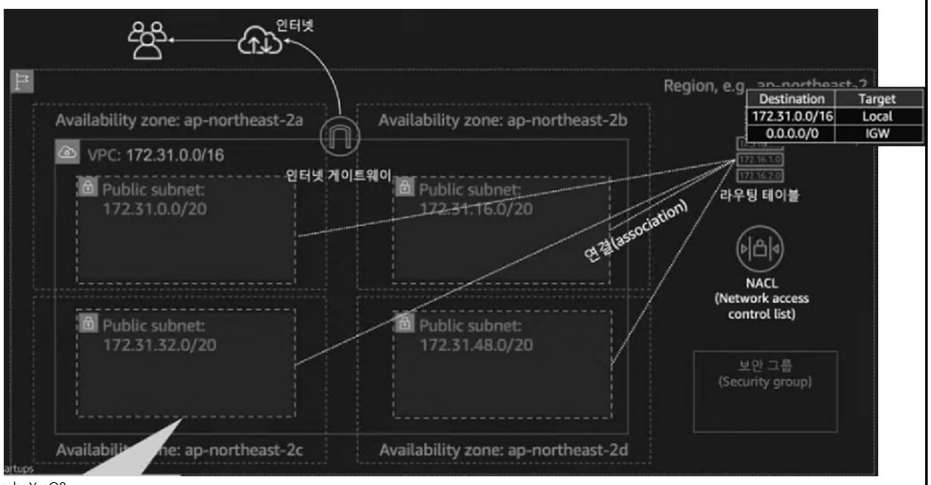
231

DEFAULT VPC 구성 - 라우팅 테이블

❖ AWS: Default VPC 구성 - 라우팅 테이블

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

Internet Gateway (IGW)



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

232

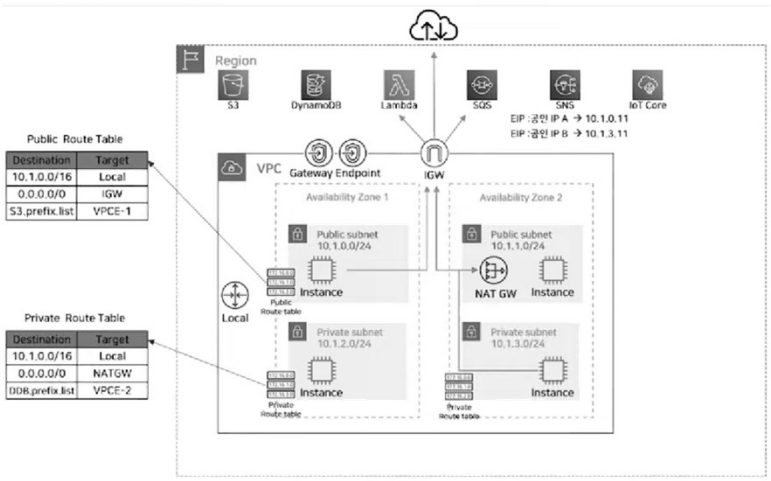
IGW 연결 VPC 외부 AWS 서비스

❖ AWS: Default VPC 구성 - 라우팅 테이블

• IGW 연결 VPC 외부 AWS 서비스

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

Internet Gateway (IGW)



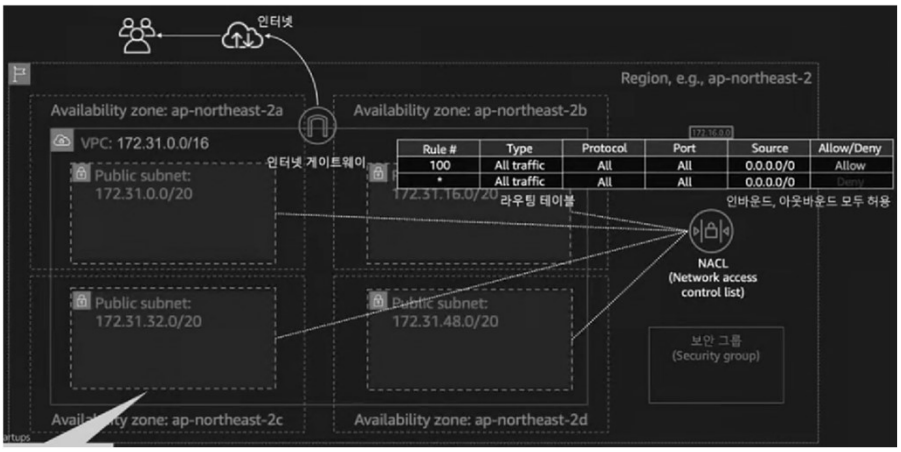
Source: https://www.youtube.com/watch?v=5kUZaGtXXt4

233

NACL (STATELESS FIREWALL)

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

• Rule 번호가 작을수록 우선 처리

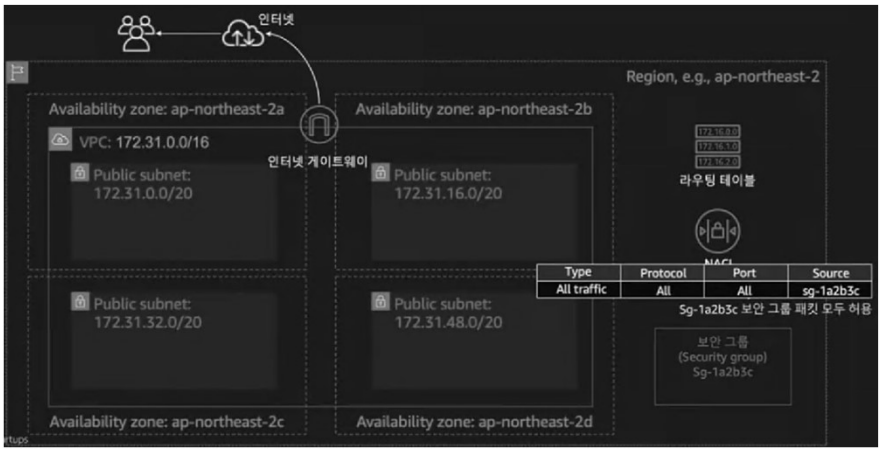


Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

234

SECURITY GROUP

❖ AWS: Default VPC 구성 - Security Group

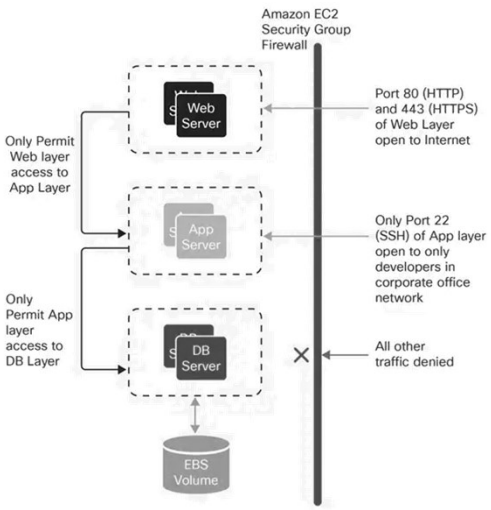


Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

235

SG-BASED NETWORK MODEL

❖ AWS SG-Based Network Model

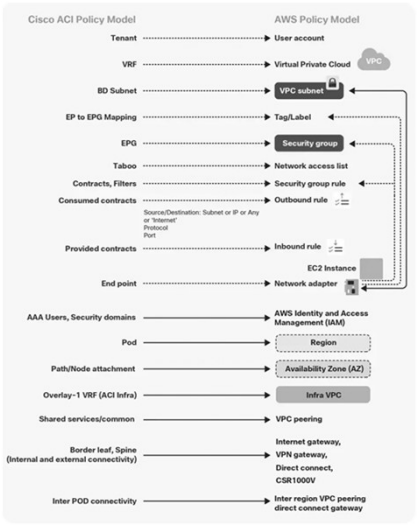


Source: https://www.cisco.com/c/en/us/td/docs/dcn/whitepapers/cisco-hybrid-multicloud-networking-design-guide.html

236

CISCO ACI POLICY MODEL

❖ Cisco ACI Policy Model to AWS Mapping

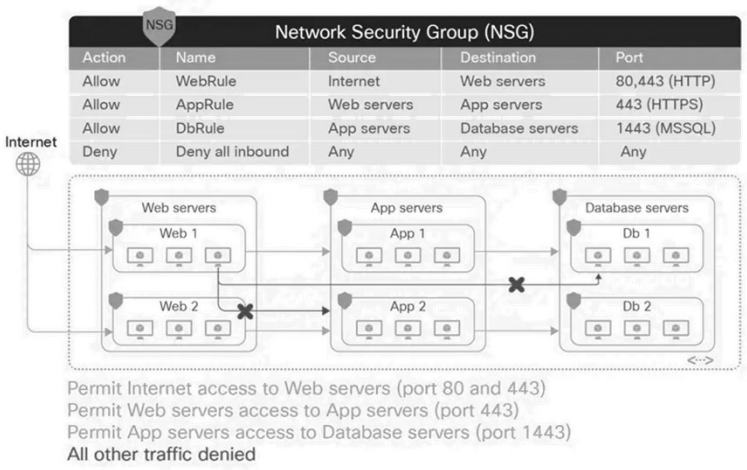


Source: https://www.cisco.com/c/en/us/td/docs/dcn/whitepapers/cisco-hybrid-multicloud-networking-design-guide.html

237

MICROSOFT AZURE SECURITY GROUP

❖ Microsoft Azure Security Group-Based Network Model



Source: https://www.cisco.com/c/en/us/td/docs/dcn/whitepapers/cisco-hybrid-multicloud-networking-design-guide.html

238

VPC 구성 - CIDR 사용

❖ AWS: 새로운 VPC 구성 - CIDR 사용 대역 정하기

- Classless Inter-Domain Routing
- RFC 1918: 사설 IP 대역 권장
  - ✓10.0.0.0.0/8: 10.0.0.0 – 10.255.255.255
  - ✓172.16.0.0/12: 172.16.0.0 – 172.31.255.255
  - ✓192.168.0.0/16: 192.168.0.0 – 192.168.255.255
- VPC CIDR 변경 불가, 대역 추가 가능
- IPv6 선택 시 VPC 대역은 /56, 각 서브넷은 /64 고정
- 서브넷 별로 예약된 IP 고려
  - ✓10.1.0.0: 네트워크 주소
  - ✓10.1.0.1: AWS에서 VPC 라우팅으로 예약
  - ✓10.1.0.2: AWS 예약
  - ✓10.1.0.3: AWS에서 향후 사용을 위해 예약
  - ✓10.1.0.255: 네트워크 브로드캐스트 주소

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

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

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

239

VPC 구성 - 서브네팅

❖ AWS: 새로운 VPC 구성 - 서브네팅

- Classless Inter-Domain Routing 사용 (예)

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

240

CLASSLESS INTER-DOMAIN ROUTING

❖ AWS: 새로운 VPC 구성 - 서브네팅

• Classless Inter-Domain Routing 권장 구성 (예)

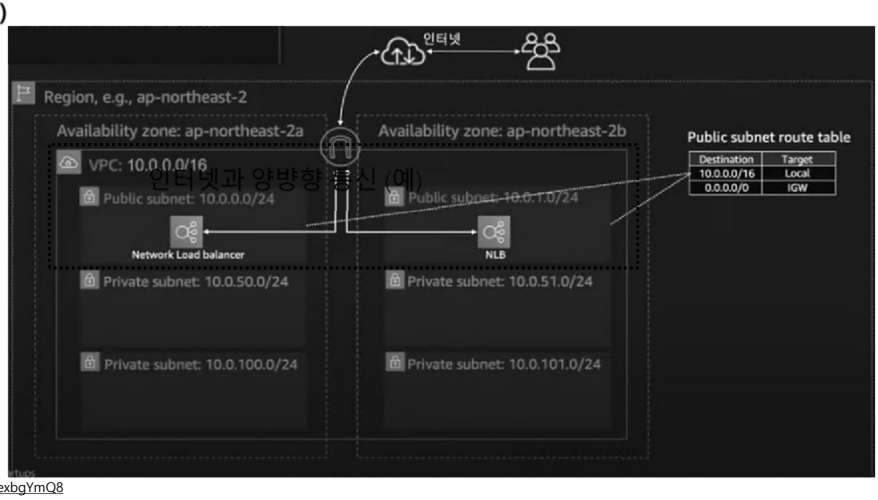
Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

인터넷과 양방향 통신

❖ AWS: 새로운 VPC 구성 - 라우팅

• 인터넷과 양방향 통신 (예)

Internet Gateway (IGW)

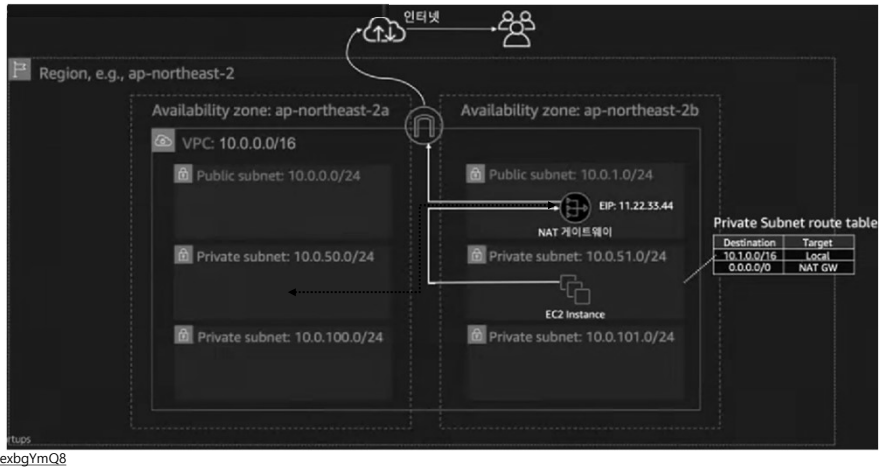


Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

NAT 게이트웨이

❖ AWS: 새로운 VPC 구성 - NAT 게이트웨이

• 인터넷과 아웃바운드 통신 (예)

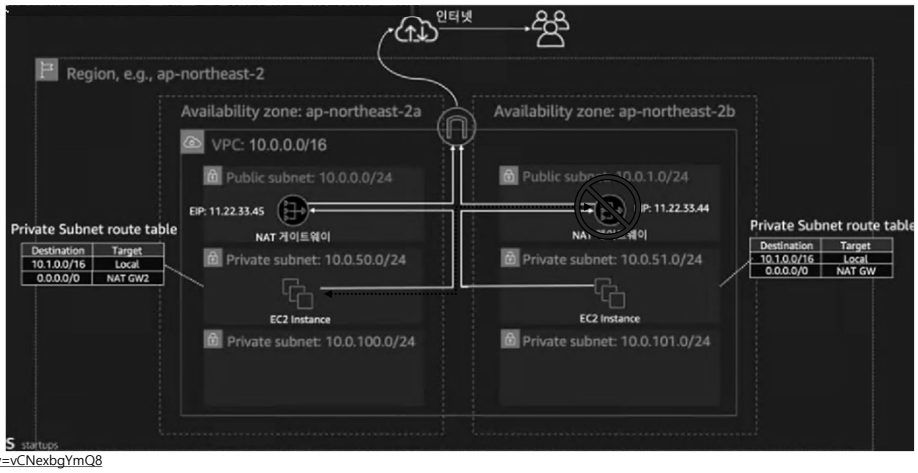


Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

NAT 게이트웨이 이중화

❖ AWS: 새로운 VPC 구성 - NAT 게이트웨이 이중화

• 인터넷과 아웃바운드 통신 (예)

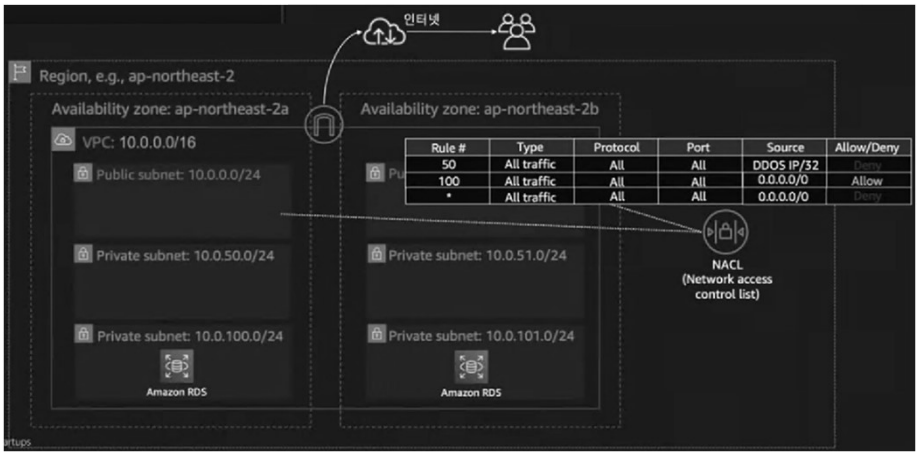


Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

DDOS 공격 차단

❖ AWS: 새로운 VPC 구성 - DDoS 공격 차단

• VPC NACL 사용 (예)



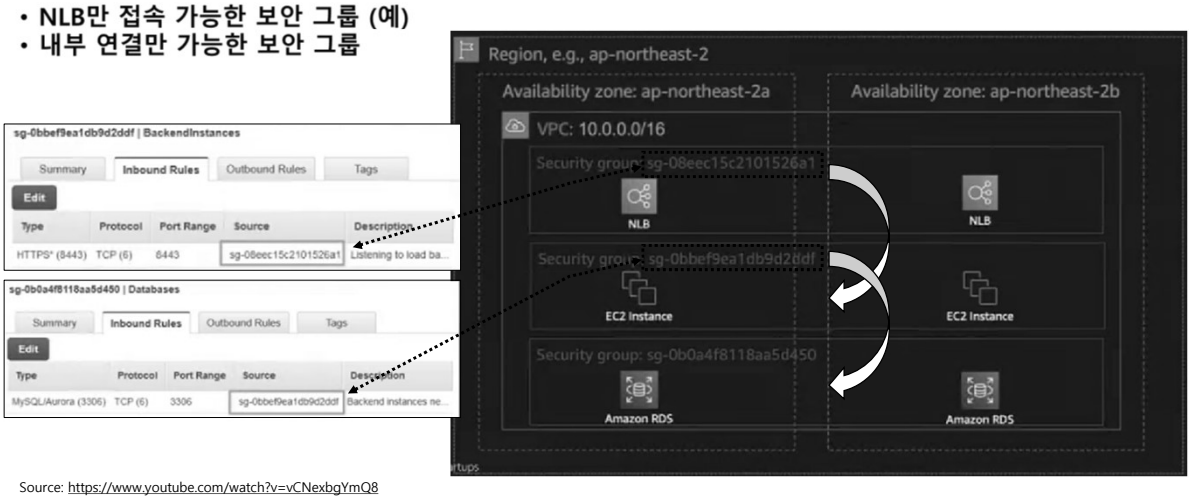
Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

245

SECURITY GROUP

❖ AWS: 새로운 VPC 구성 - Security Group

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



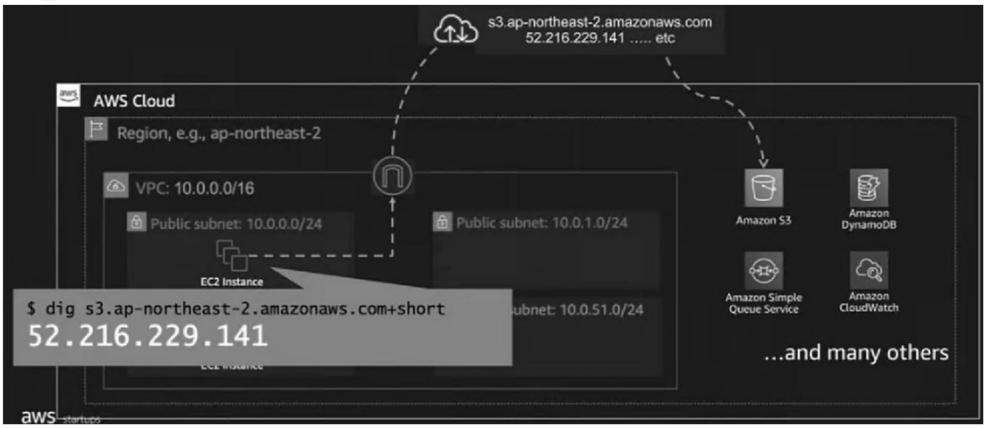
Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

246

PRIVATE LINK

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

- 게이트웨이 엔드포인트
- 인터페이스 엔드포인트



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

게이트웨이 엔드포인트

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

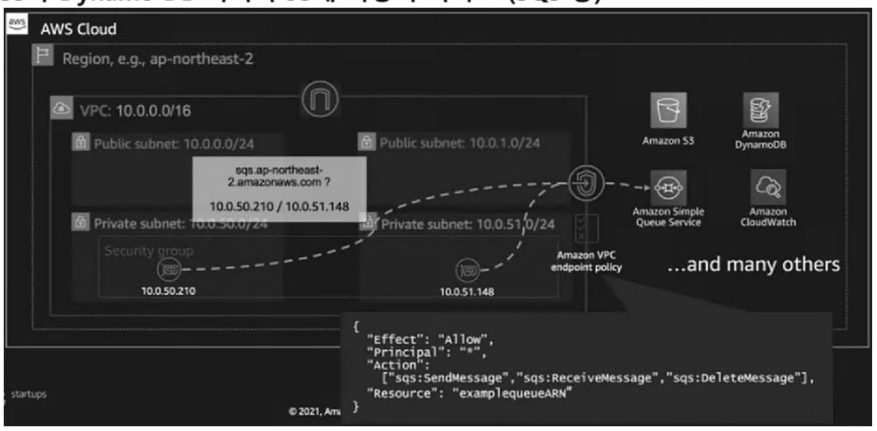
- 게이트웨이 엔드포인트: S3나 DynamoDB등을 지원
- 인터페이스 엔드포인트

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

인터페이스 엔드포인트

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

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

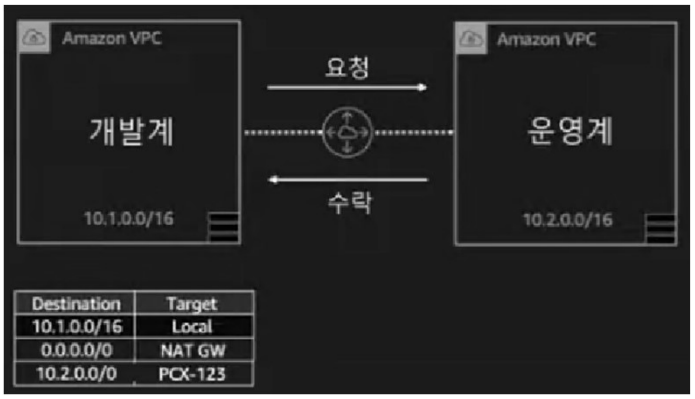


Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

하나 이상의 VPC 이용

❖ AWS: VPC 구성 - 하나 이상의 VPC 이용

- VPC Peering
- Transit Gateway

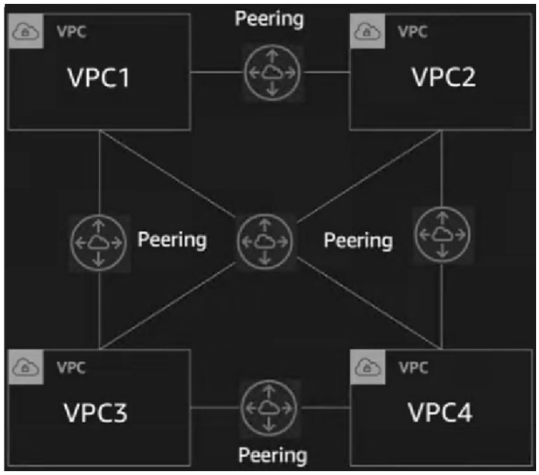


Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

VPC PEERING

❖ AWS: VPC 구성 - 하나 이상의 VPC 이용

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

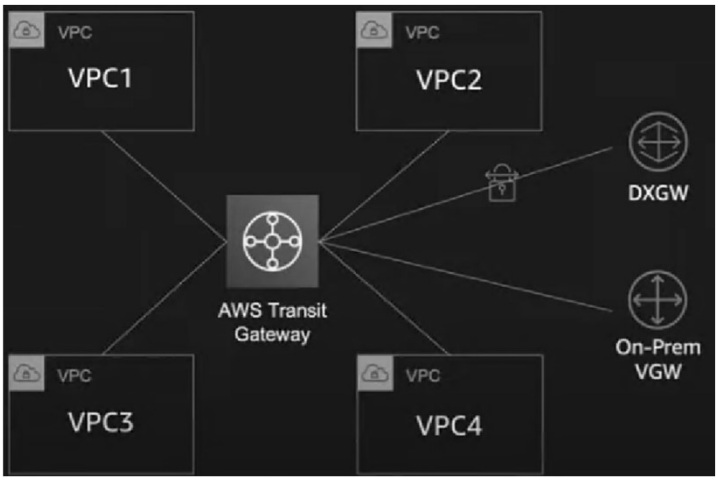


Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

TRANSIT GATEWAY

❖ AWS: VPC 구성 - 하나 이상의 VPC 이용

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

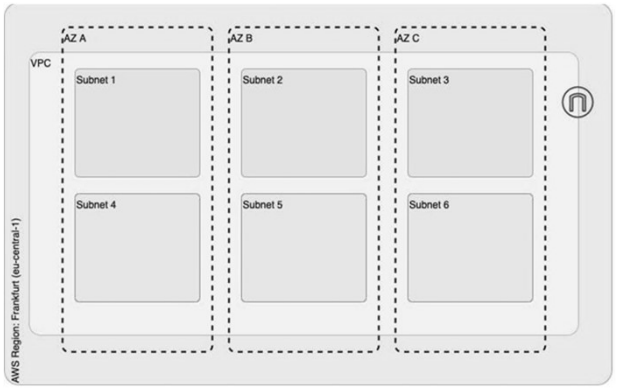


Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

BUILD AWS VPC USING TERRAFORM

❖ Build AWS VPC using Terraform

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



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

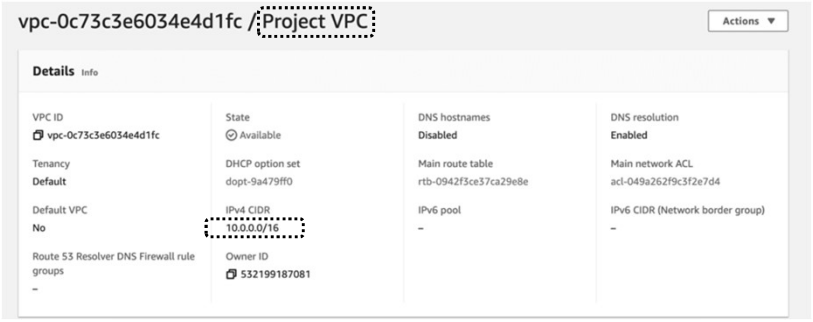
CREATE A VPC

❖ Build AWS VPC using Terraform

- AWS VPC
  - ✓ Create a VPC

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

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



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

CREATE SUBNETS

❖ Build AWS VPC using Terraform

- AWS VPC
  - ✓ Create Subnets

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

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

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

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

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

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

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

255

CHECK CREATED SUBNETS

❖ Build AWS VPC using Terraform

- AWS VPC
  - ✓ Create Subnets

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

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

Subnets (6) Info

Actions ▼ | Create subnet

Filter subnets

VPC: vpc-0c73c3e6034e4d1fc ✕ | Clear filters

Name	Subnet ID	VPC	Availability Zone	Network border group
Public Subnet 1	subnet-0ac0ea7022c8be0bc	vpc-0c73c3e6034e4d1fc | Proj...	eu-central-1c	eu-central-1
Public Subnet 3	subnet-0ea385bdde2fcb942	vpc-0c73c3e6034e4d1fc | Proj...	eu-central-1c	eu-central-1
Public Subnet 2	subnet-0cb6909b61e9b06b0	vpc-0c73c3e6034e4d1fc | Proj...	eu-central-1c	eu-central-1
Private Subnet 1	subnet-02276f5631f36f72e	vpc-0c73c3e6034e4d1fc | Proj...	eu-central-1c	eu-central-1
Private Subnet 3	subnet-062ec4dfa174dbb90	vpc-0c73c3e6034e4d1fc | Proj...	eu-central-1c	eu-central-1
Private Subnet 2	subnet-0809198f93e491c77	vpc-0c73c3e6034e4d1fc | Proj...	eu-central-1c	eu-central-1

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

256

CREATE SUBNETS WITH AZ

❖ Build AWS VPC using Terraform

- AWS VPC
  - ✓ Create Subnets with AZ

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

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

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

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

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

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

CHECK CREATED SUBNETS WITH AZ

❖ Build AWS VPC using Terraform

- AWS VPC
  - ✓ Create Subnets

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

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

Subnets (6) Info

Actions ▼ Create subnet

Filter subnets

VPC: vpc-0c98ad127b906c06d ✕ Clear filters

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

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

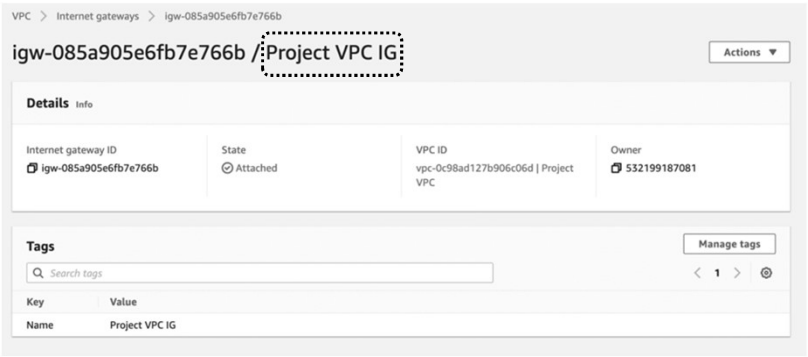
CREATE INTERNET GATEWAY

❖ Build AWS VPC using Terraform

- AWS VPC
  - ✓ Internet Gateway

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

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



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

CREATE A 2ND ROUTE TABLE

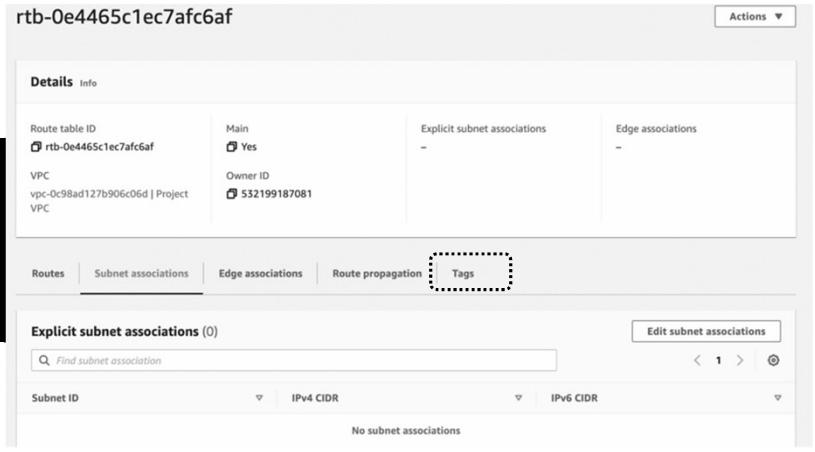
❖ Build AWS VPC using Terraform

- AWS VPC
  - ✓ Create a 2nd Route Table

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

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

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



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

CHECK CREATED A 2ND ROUTE TABLE

❖ Build AWS VPC using Terraform

• AWS VPC

✓ Create a 2nd Route Table

Subnets without explicit associations (6)

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Edit subnet associations

Find subnet association

1

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-05267deb229b1b2dc / Public Subnet 1	10.0.1.0/24	–
subnet-0822129878ed14178 / Private Subnet 1	10.0.4.0/24	–
subnet-0a0bba97e6dfba49e / Private Subnet 3	10.0.6.0/24	–
subnet-0c1274a75a9b46aa1 / Public Subnet 2	10.0.2.0/24	–
subnet-09fb51a9d2433d961 / Public Subnet 3	10.0.3.0/24	–
subnet-07422f3a4b2af8808 / Private Subnet 2	10.0.5.0/24	–

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

CHECK CREATED A 2ND ROUTE TABLE

❖ Build AWS VPC using Terraform

• AWS VPC

✓ Create a 2nd Route Table

Details Info

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-0e15111955d1ab14f	No	–	–

VPC	Owner ID
vpc-0c98ad127b906c06d | Project VPC	532199187081

Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (2)

Edit routes

Filter routes

Both

1

Destination	Target	Status	Propagated
0.0.0.0/0	igw-085a905e6fb7e766b	Active	No
10.0.0.0/16	local	Active	No

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

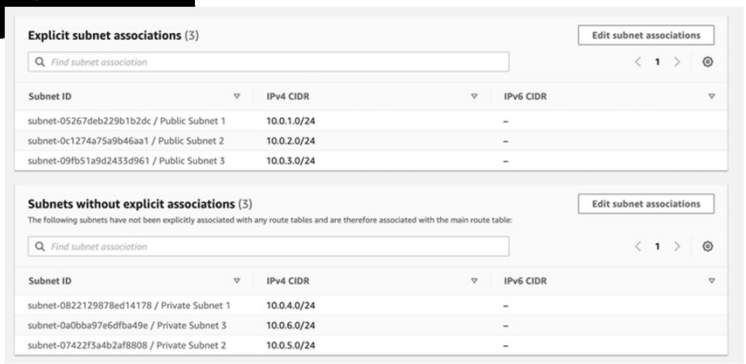
ASSOCIATING PUBLIC SUBNETS

❖ Build AWS VPC using Terraform

• AWS VPC

✓ Associating Public Subnets to the Second Route Table

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



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

263

AWS: DIRECT CONNECT

❖ AWS: Direct Connect 비용 고려사항

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

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

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

264

PRIVATE PEERING

❖ Private peering or private network interconnect

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

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

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

265

INTERNET DIRECT PEERING

❖ Internet direct peering or public peering and remote peering

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

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

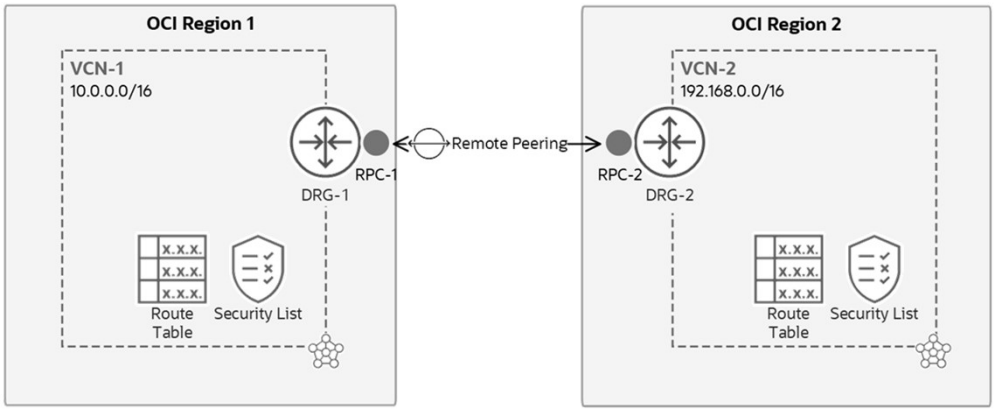
Source: Multi-Cloud for Architects (Published by Packt Publishing Ltd) Florian Klaffenbach, Markus Klein, Suresh Sundaresan

266

REMOTE PEERING

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

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



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

267

AMAZON VPC, VPC 피어링 요금

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

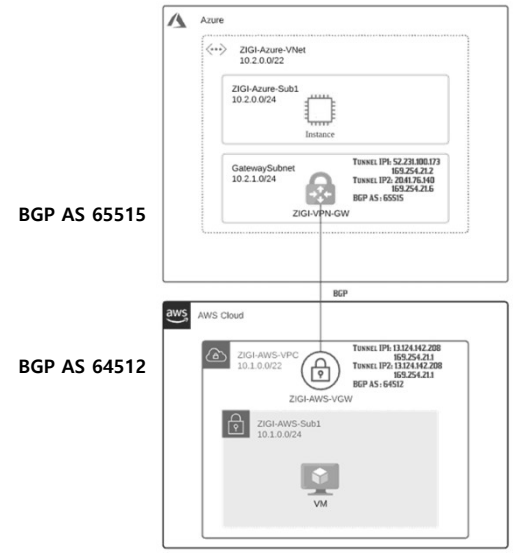
- 가용 영역(AZ) 내에 유지되는 VPC 피어링 연결을 통한 모든 데이터 전송은 무료
- 가용 영역을 가로지르는 VPC 피어링 연결을 통한 모든 데이터 전송은 계속 리전 내 표준 데이터 전송 요금이 청구
- 가용 영역 ID를 사용하면 서로 다른 AWS 계정 간에서 가용 영역을 고유하고 일관되게 식별
- 고객은 한 리전 내에서 VPC를 상호 연결하기 위해 VPC 피어링을 사용
- VPC 피어링은 한 리전에서 적은 수의 VPC를 상호 연결하여 전체 메시 연결성을 달성하려고 할 때 일반적으로 사용
- 대규모로 수백 또는 수천 개의 VPC를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

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

268

'AZURE – AWS' 간의 VPN 연동

❖ 'Azure – AWS' 간의 VPN 연동 및 BGP 연결



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

269

EBGP CONFIGURATION

❖ eBGP configuration 연결 (예): VyOS

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

Node 1:

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

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

Node 2:

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

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

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

270

BGP CONFIGURATION VIA IPV6

❖ eBGP configuration 연결 (예): VyOS

• BGP configuration via IPv6

Node 1:

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

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

Node 2:

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

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

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

ROUTE FILTER

❖ eBGP configuration 연결 (예): VyOS

• Route Filter

Node 1:

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

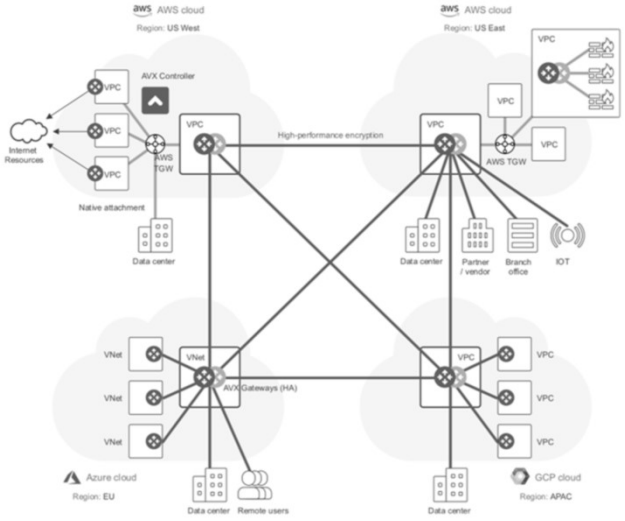
Node 2:

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

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

MULTI-CLOUD BACKBONE

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

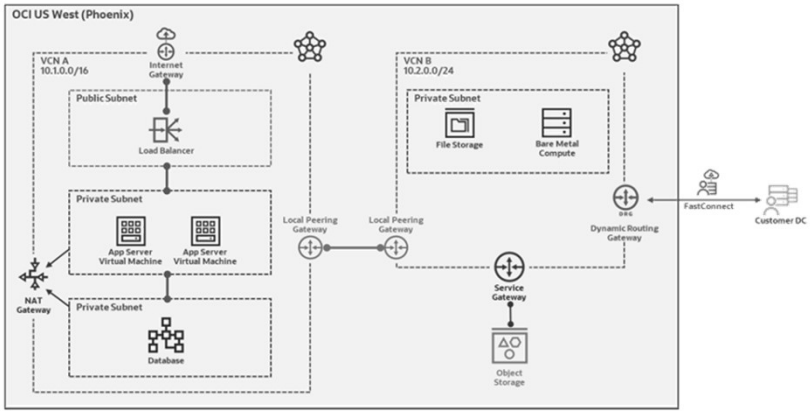


Source: https://www.simform.com/compute-pricing-comparison-aws-azure-googlecloud/

ORACLE CLOUD INFRASTRUCTURE

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

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

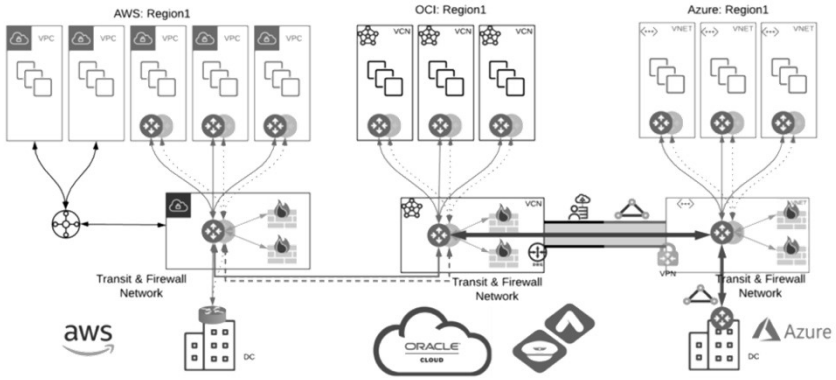


Source: https://aviatrix.com/oracle-oci-multi-region-transit-connectivity/

MULTI-CLOUD W/ORACLE OCI

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

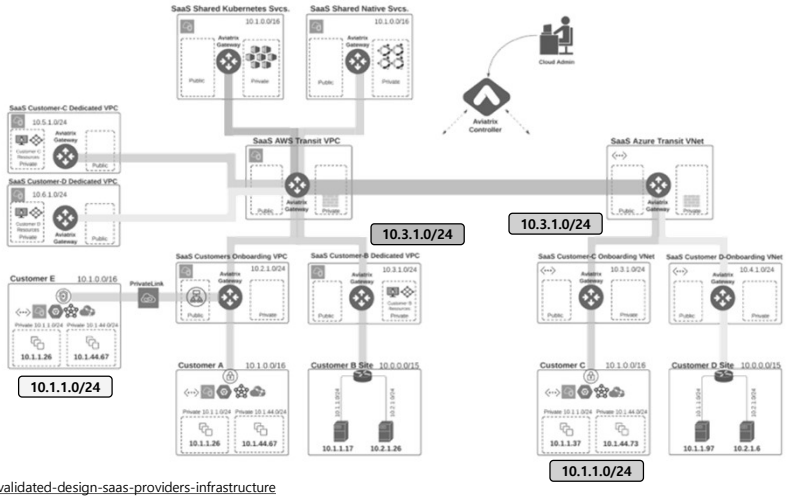
• Oracle OCI — Multi-cloud, multi-region transit connectivity with Aviatrix MCNA



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

AVIATRIX의 SAAS 서비스 (1 OF 2)

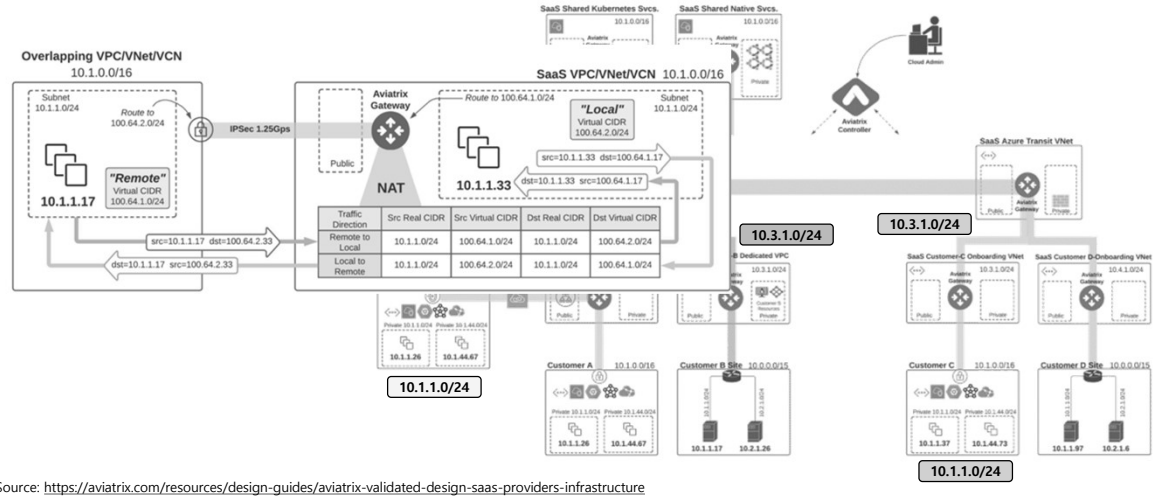
❖ 제조사 (예): Aviatrix의 SaaS 서비스



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

AVIATRIX의 SAAS 서비스 (2 OF 2)

❖ 제조사 (예): Aviatrix의 SaaS 서비스



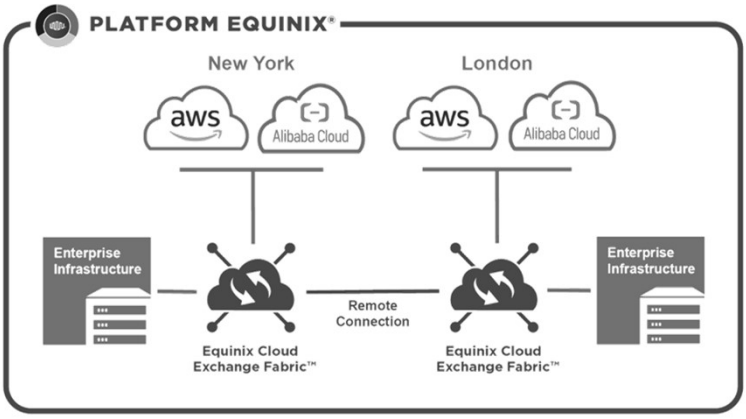
Source: https://aviatrix.com/resources/design-guides/aviatrix-validated-design-saas-providers-infrastructure

277

CLOUD "ON-RAMP" SERVICE

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

- Hybrid Multicloud - business continuity/disaster recovery



EQUINIX | INTERCONNECTIONS

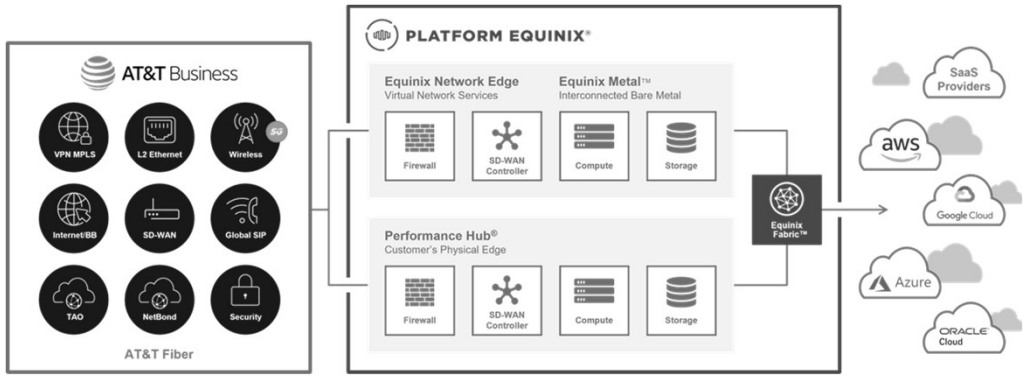
Source: https://blog.equinix.com/blog/2020/07/31/equinix-and-alibaba-are-extending-the-reach-of-hybrid-multicloud/

278

CLOUD "ON-RAMP" SERVICE

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

• Equinix Fabric Use Cases for Network Service Providers



EQUINIX | INTERCONNECTIONS

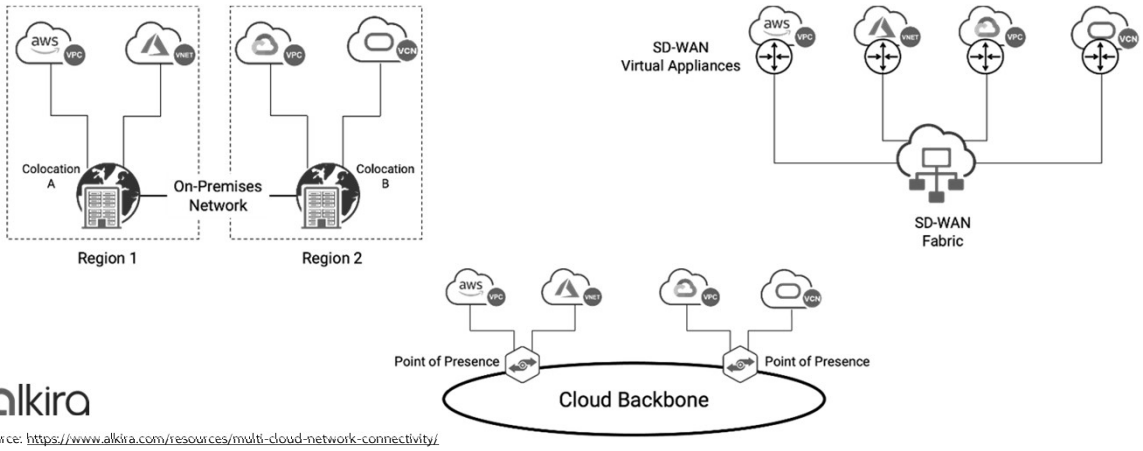
Source: https://blog.equinix.com/blog/2022/07/11/5-equinix-fabric-use-cases-for-network-service-providers/

279

CLOUD NETWORK CONNECTIVITY

❖ 제조사 (예): Alkira

• Multi-Cloud Network Connectivity



alkira

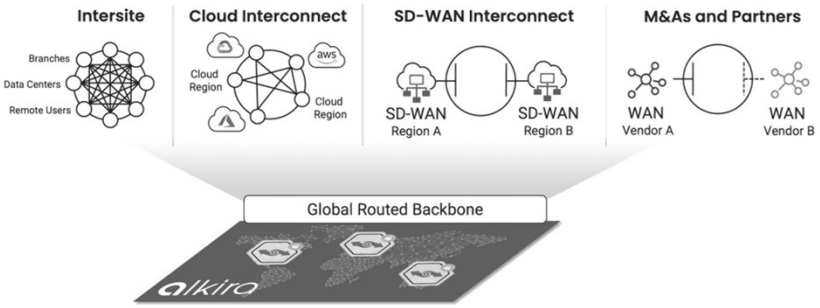
Source: https://www.alkira.com/resources/multi-cloud-network-connectivity/

280

CLOUD BACKBONE

❖ 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.

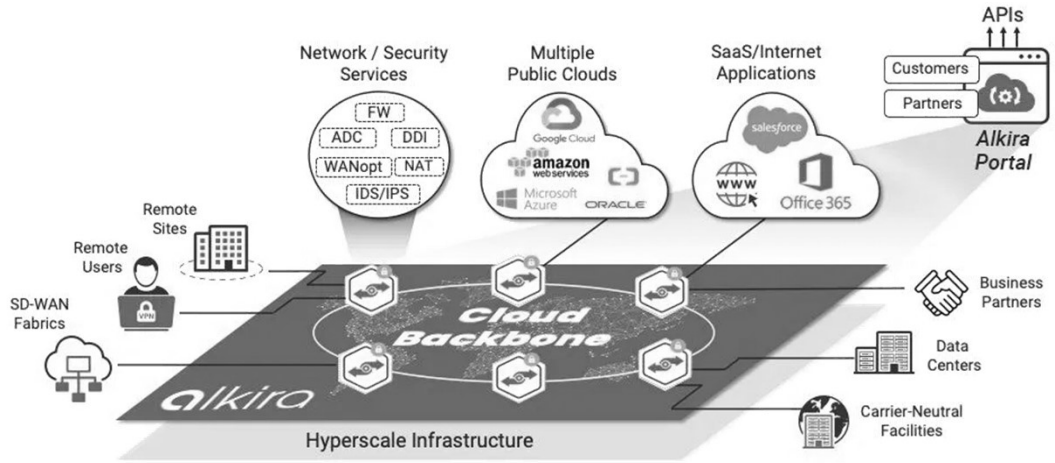


Source: https://www.alkira.com/multi-cloud-networking-reinvented-cto-whitepaper/

281

ALKIRA CLOUD AREA NETWORKING

❖ Alkira Cloud Area Networking



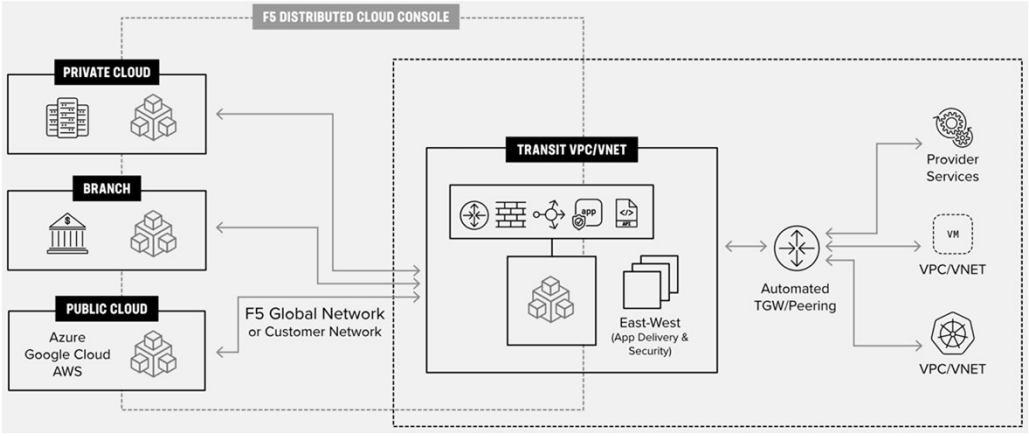
Source: https://www.alkira.com/multi-cloud-networking-reinvented-cto-whitepaper/

282

DISTRIBUTED CLOUD TRANSIT

❖ 제조사 (예): F5

• Distributed Cloud Multi-Cloud Transit



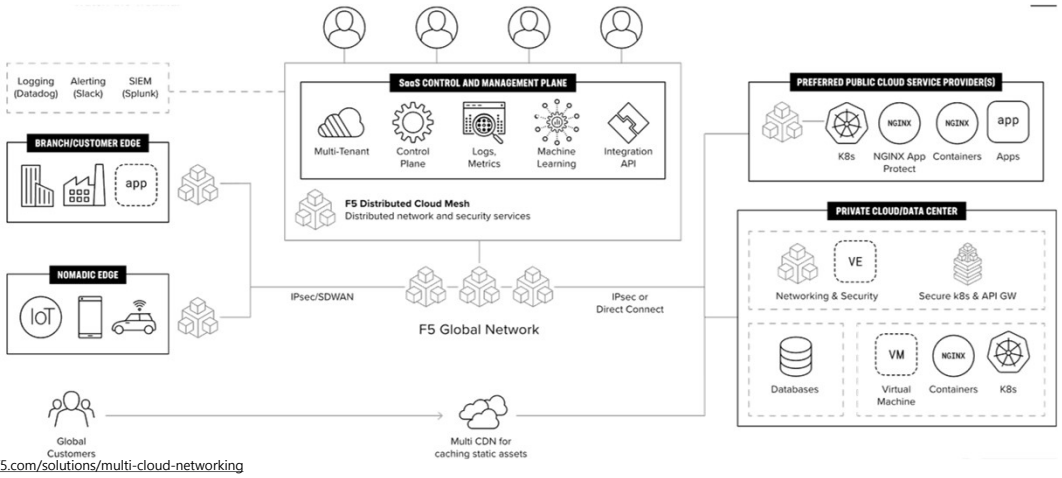
Source: https://www.f5.com/solutions/multi-cloud-networking

283

SAAS FOR MULTI-CLOUD NETWORK

❖ 제조사 (예): F5

• SaaS for Multi-Cloud Network



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

284

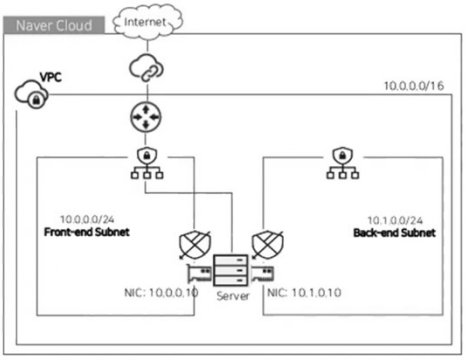
네이버클라우드 네트워크 보안

❖ 네이버클라우드플랫폼 (2020)

• 네트워크 보안

• VPC VPC

VPC를 사용하여 격리된 사설 네트워크 구성



Virtual Private Cloud

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

Network Security

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

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

285

네이버클라우드 네트워크 보안

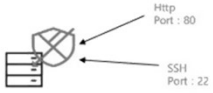
❖ 네이버클라우드플랫폼 (2020)

• 네트워크 보안

• ACG (Access Control Group)

VM 단위 Stateful 방화벽

인바운드/아웃바운드 트래픽 , IP/Port 에 대한 허용/차단



• NACL (Network ACL)

서브넷 단위 Stateless 적용

DENY 규칙 적용 가능

[ACG / NACL 비교]

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

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

286

대외 기관 시스템 연계

❖ 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

PRIVATELINK

❖ 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

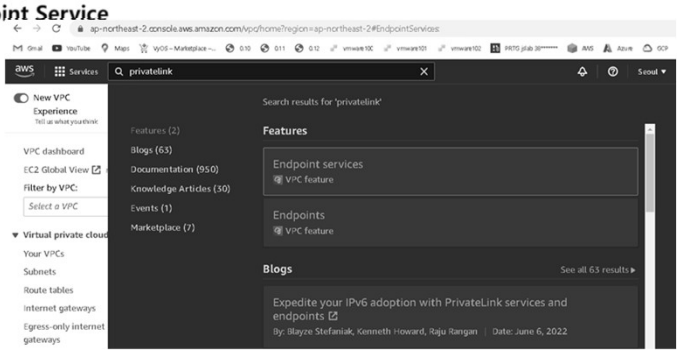
Amazon Elastic Container Registry (ECR)
AWS Key Management Service (KMS)

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.

AWS PRIVATELINK

❖ AWS PrivateLink

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

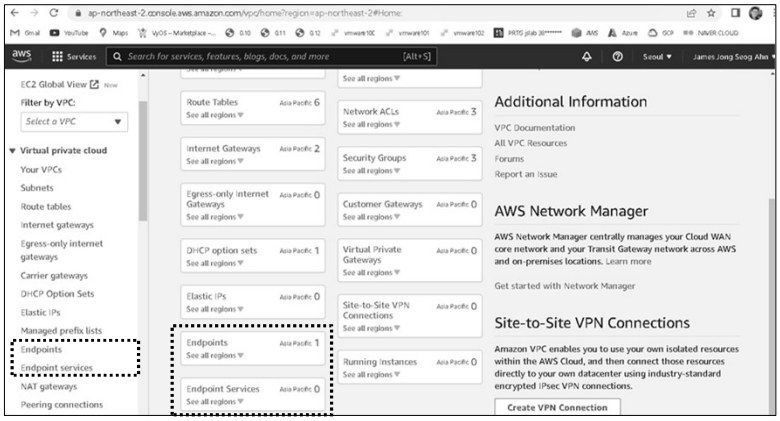


Source: https://www.youtube.com/watch?v=tBZBYozvTO8

AWS PRIVATELINK 구성 요소

❖ AWS PrivateLink 구성 요소

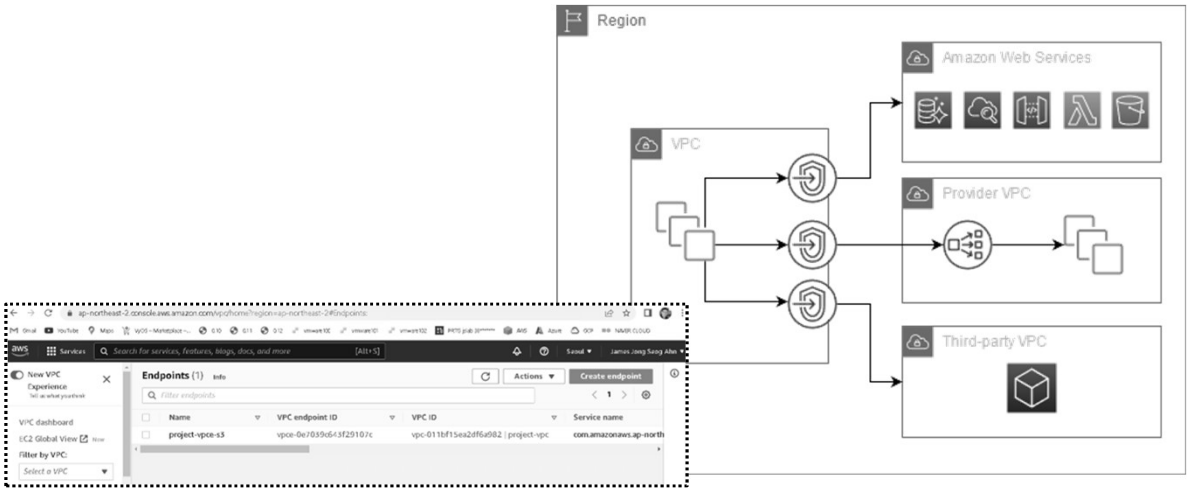
- Endpoint (서비스 제공자)
- Endpoint Service
  - ✓Gateway Load Balancer Endpoint
  - ✓Gateway Endpoint
  - ✓Interface Endpoint



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

AWS PRIVATELINK 사용 VPC 연결

❖ AWS PrivateLink를 사용하여 서비스에 VPC 연결

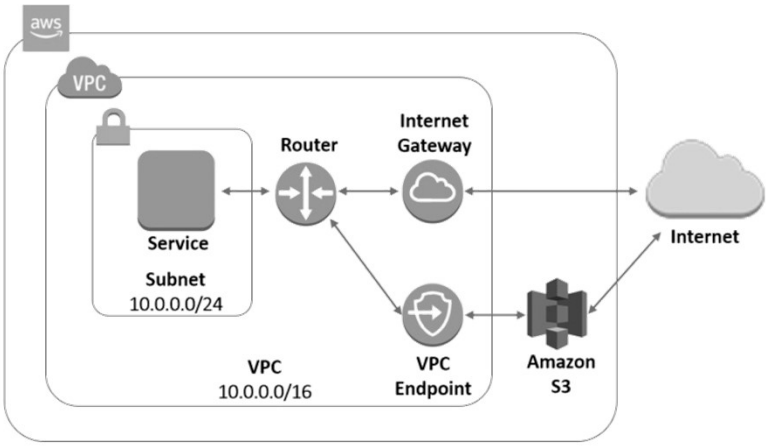


Source: https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/endpoint-services-overview.html

AWS 서비스에 액세스

❖ AWS PrivateLink를 통한 새로운 SaaS

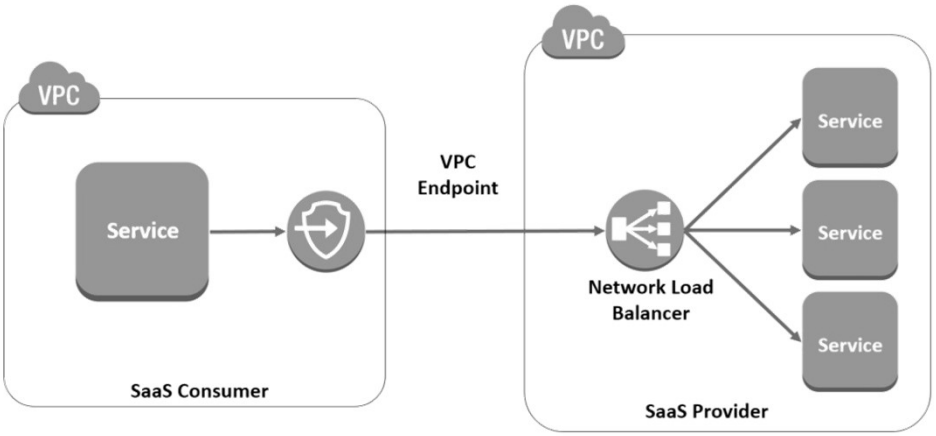
• 인터넷 게이트웨이 또는 VPC 엔드 포인트로 AWS 서비스에 액세스



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

AWS PRIVATELINK - VPC 엔드 포인트

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

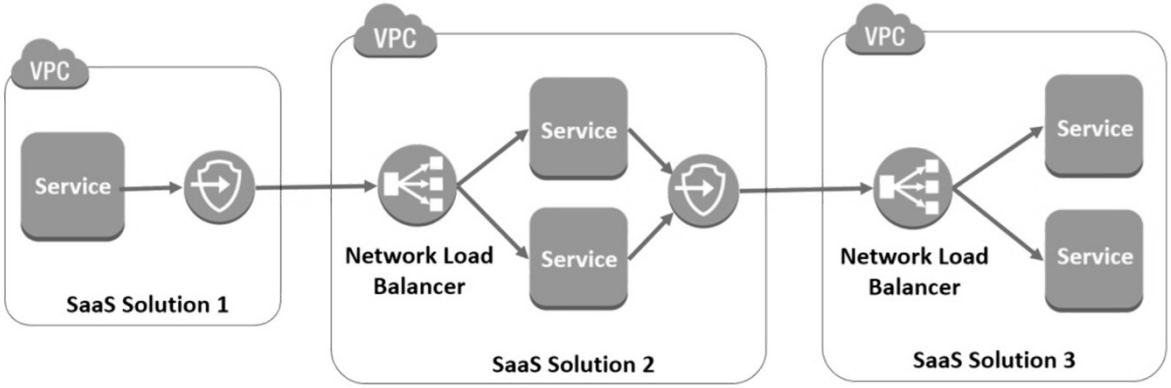


Source: https://www.megazone.com/techblog_191113_aws-privatelink/

293

AWS PRIVATELINK - SAAS

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



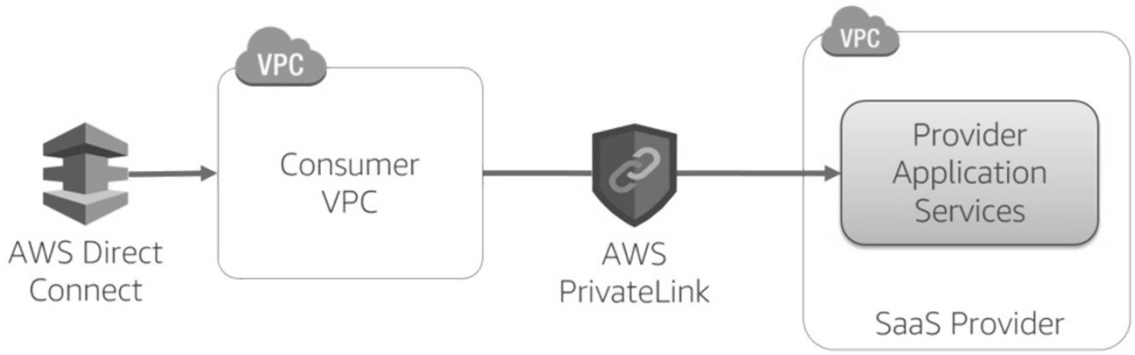
Source: https://www.megazone.com/techblog_191113_aws-privatelink/

294

AWS PRIVATELINK - 온프레미스 환경

❖ AWS PrivateLink를 통한 새로운 SaaS

• AWS PrivateLink를 사용하여 온프레미스 환경에서 서비스에 액세스



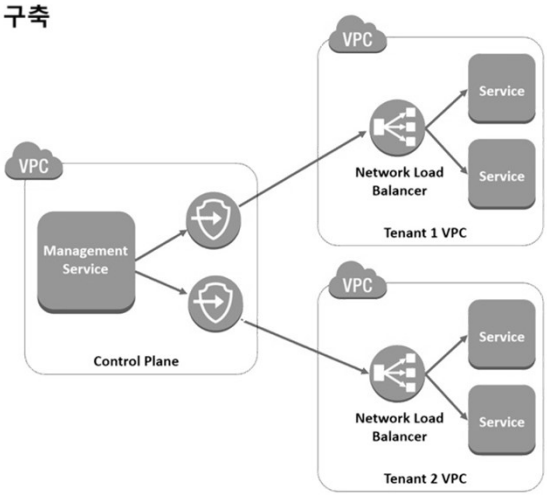
Source: https://www.megazone.com/techblog_191113_aws-privatelink/

295

AWS PRIVATELINK - 다중 VPC 컨트롤

❖ AWS PrivateLink를 통한 새로운 SaaS

• AWS PrivateLink를 사용하여 다중 VPC 컨트롤 플레인 구축

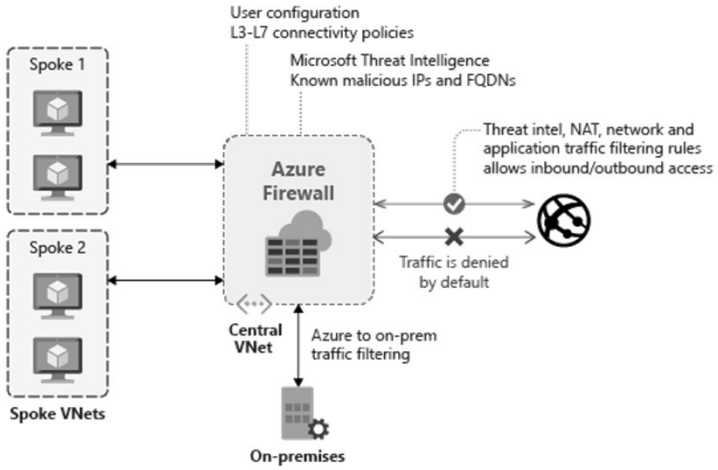


Source: https://www.megazone.com/techblog_191113_aws-privatelink/

296

AZURE VIRTUAL NETWORK

❖ Obtaining A Static Outbound IP from an Azure Virtual Network

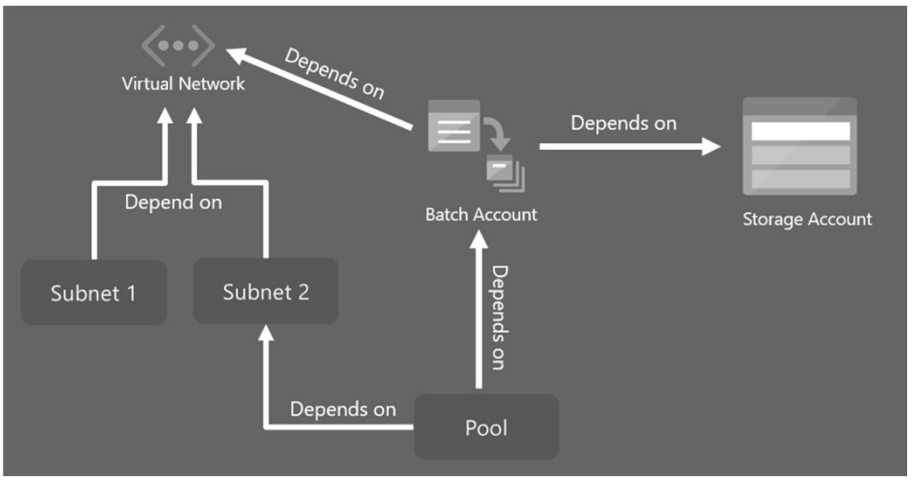


Source: https://samcogan.com/obtaining-a-static-outbound-ip-from-an-azure-virtual-network/

297

AZURE BATCH

❖ Azure Batch without Public IP

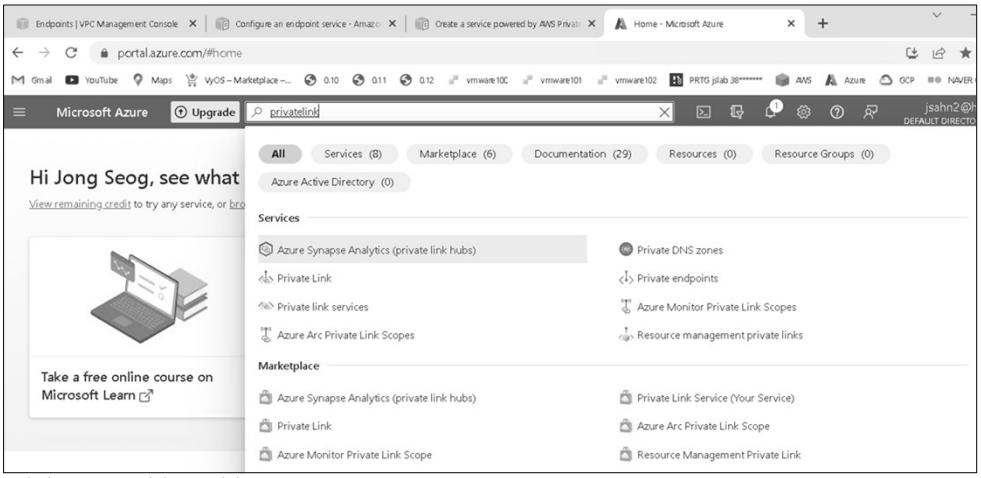


Source: https://charotamine.medium.com/azure-batch-security-azure-private-link-a04dc21d87ed

298

AZURE PRIVATE LINK

❖ Azure Private Link 서비스

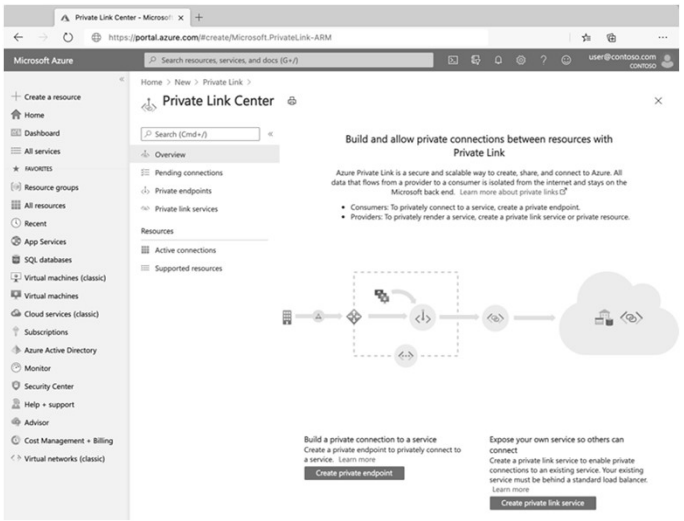


Source: https://docs.microsoft.com/ko-kr/azure/private-link/private-link-service-overview

299

AZURE PRIVATE LINK

❖ Azure Private Link

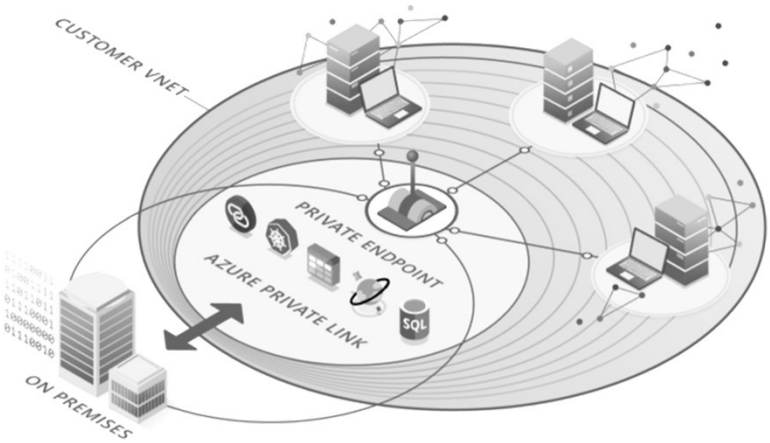


Source: https://docs.microsoft.com/ja-jp/azure/private-link/private-link-overview

300

AZURE PRIVATE LINK

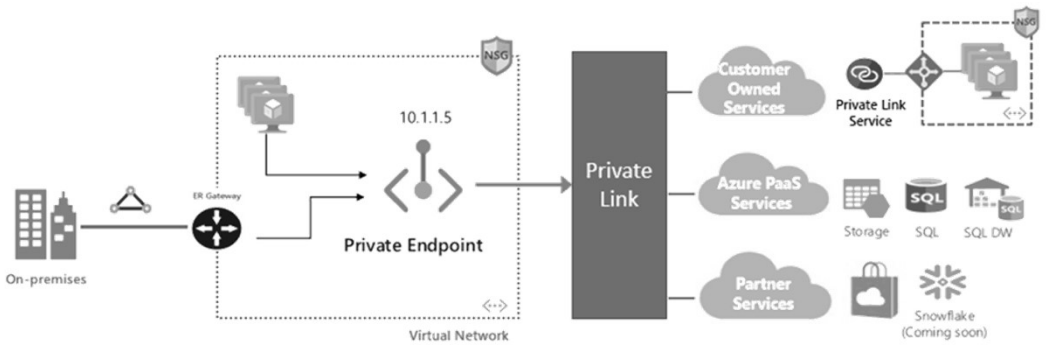
❖ Cloud Security And Azure Private Link



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

AZURE PRIVATE ENDPOINT

❖ Azure Private EndPoint

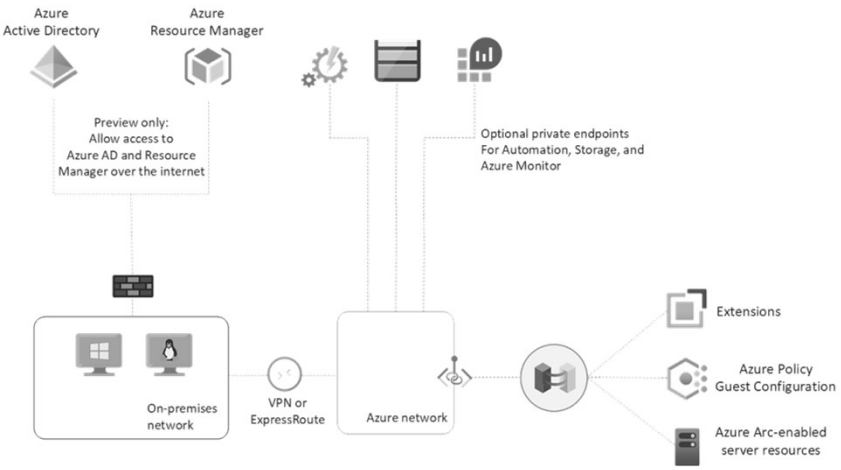


Azure Private Link – Connecting Azure Services privately to your Network

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

AZURE PRIVATE LINK

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



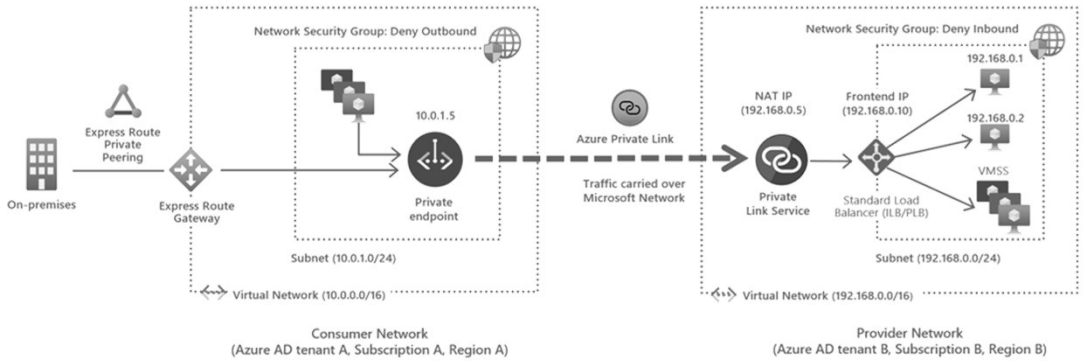
Source: https://docs.microsoft.com/en-us/azure/azure-arc/servers/private-link-security

303

AZURE PRIVATE LINK

❖ 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

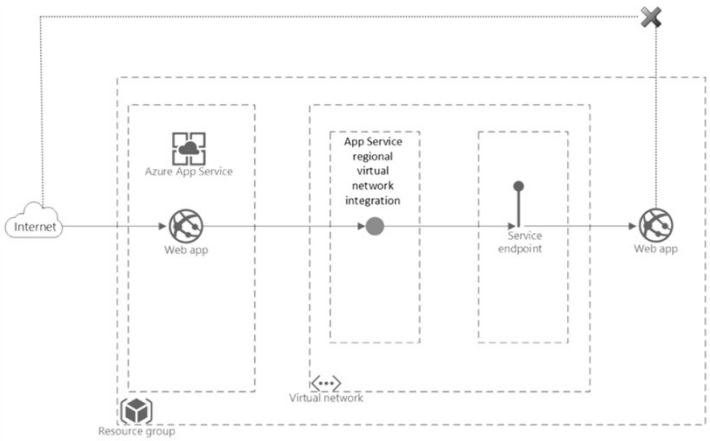


Source: https://docs.microsoft.com/ko-kr/azure/private-link/private-link-service-overview

304

MULTI-TIER APP SERVICE

❖ Multi-tier app service with service endpoint

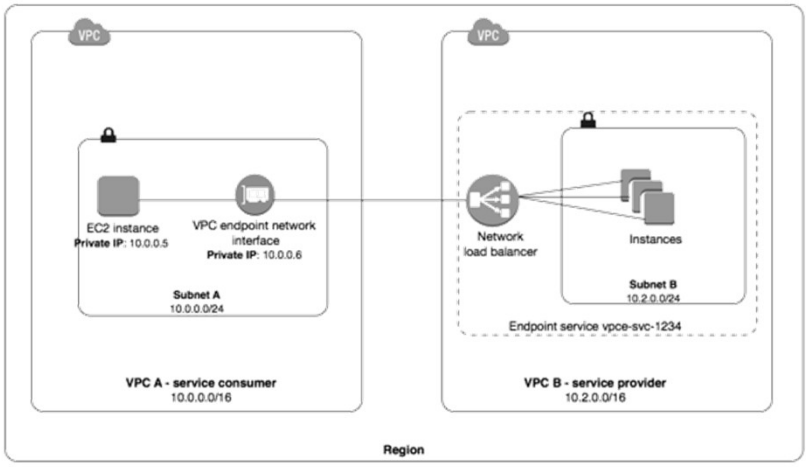


Source: https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/app-service-web-app/multi-tier-app-service-service-endpoint

305

VPC 엔드포인트 서비스

❖ 인터페이스 엔드포인트를 위한 VPC 엔드포인트 서비스



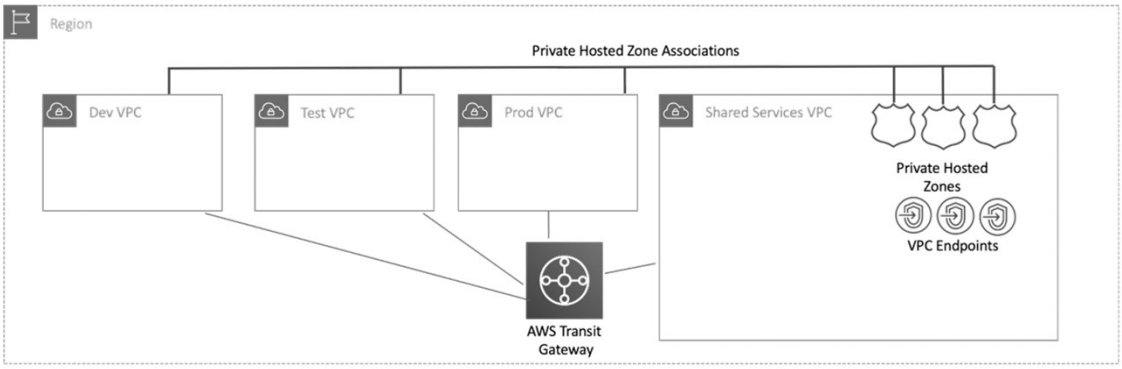
Source: https://docs.aws.amazon.com/ko_kr/vpc/latest/privatelink/endpoint-service-overview.html

306

VPC TO VPC

❖ Services using VPC peering and AWS PrivateLink

• VPC to VPC

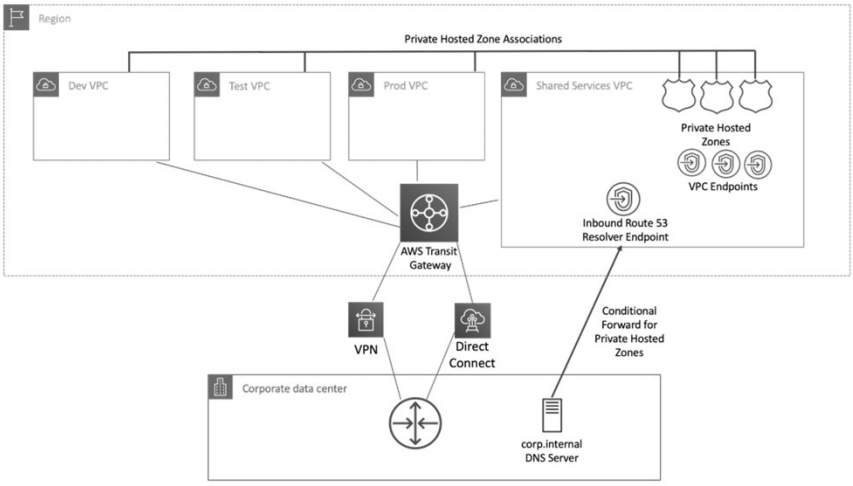


Source: https://aws.amazon.com/blogs/networking-and-content-delivery/integrating-aws-transit-gateway-with-aws-privatelink-and-amazon-route-53-resolver/

307

ON PREMISES

❖ On premises

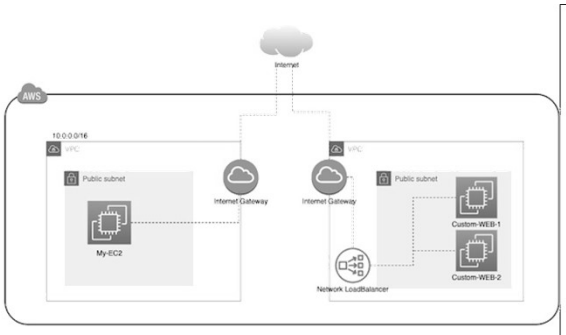


Source: https://aws.amazon.com/blogs/networking-and-content-delivery/integrating-aws-transit-gateway-with-aws-privatelink-and-amazon-route-53-resolver/

308

ENDPOINT SERVICE 이용 PRIVATELINK

❖ 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/

퍼블릭에서 연결 테스트

❖ 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/

PRIVATELINK 구성

❖ EndPoint Service를 이용해서 PrivateLink 구성 해보기

• 엔드포인트 생성

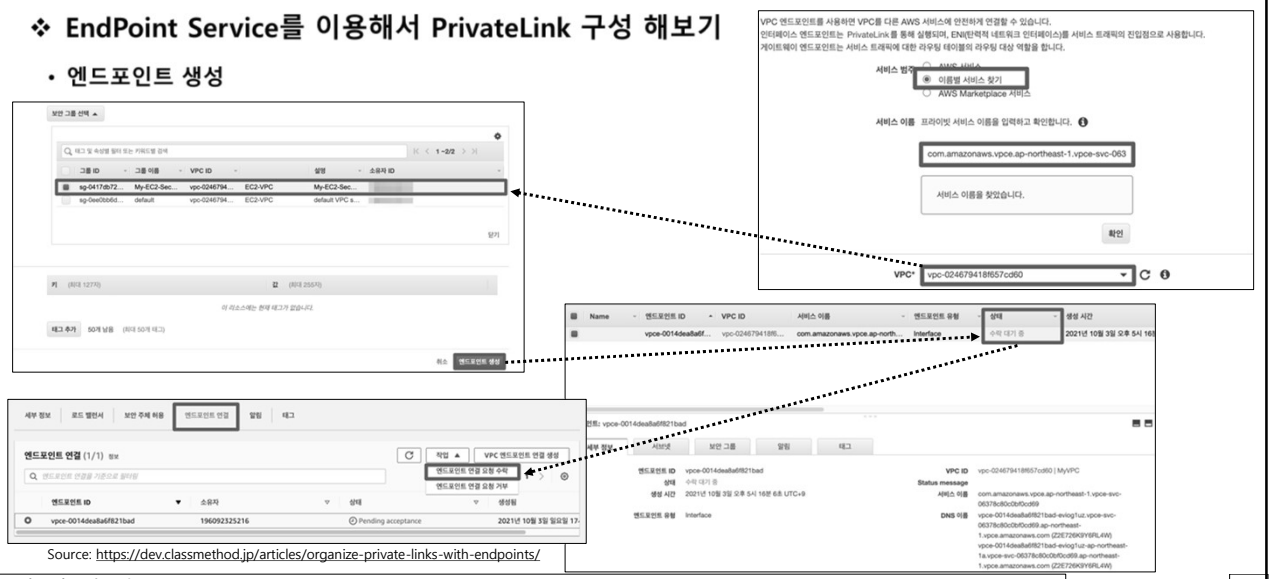
Source: https://dev.classmethod.jp/articles/organize-private-links-with-endpoints/

311

엔드포인트 생성

❖ EndPoint Service를 이용해서 PrivateLink 구성 해보기

• 엔드포인트 생성



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

312

엔드포인트 서비스 테스트

❖ EndPoint Service를 이용해서 PrivateLink 구성 해보기

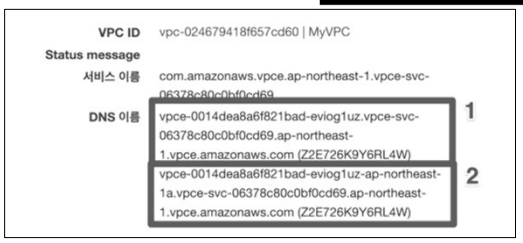
• 엔드포인트 서비스 테스트

```
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>
```



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

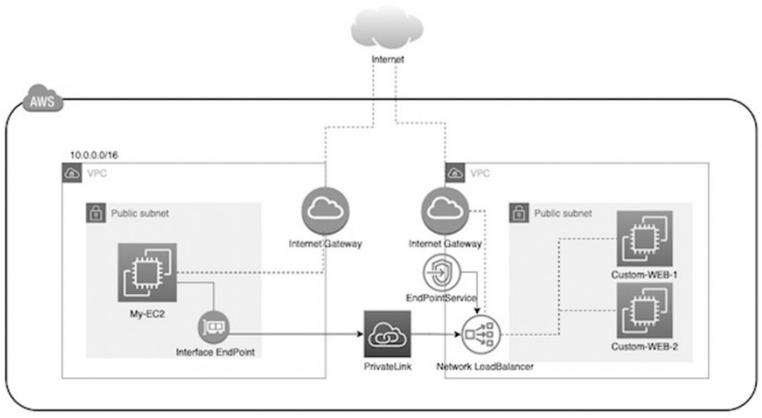
313

엔드포인트 서비스 테스트

❖ EndPoint Service를 이용해서 PrivateLink 구성 해보기

• 엔드포인트 서비스 테스트

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



Source: https://dev.classmethod.jp

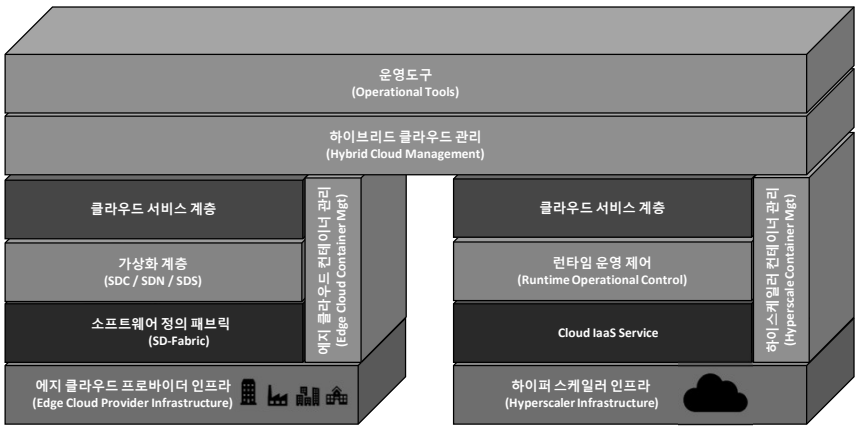
314

IV. 멀티 클라우드 관리

315

하이브리드 클라우드 아키텍처

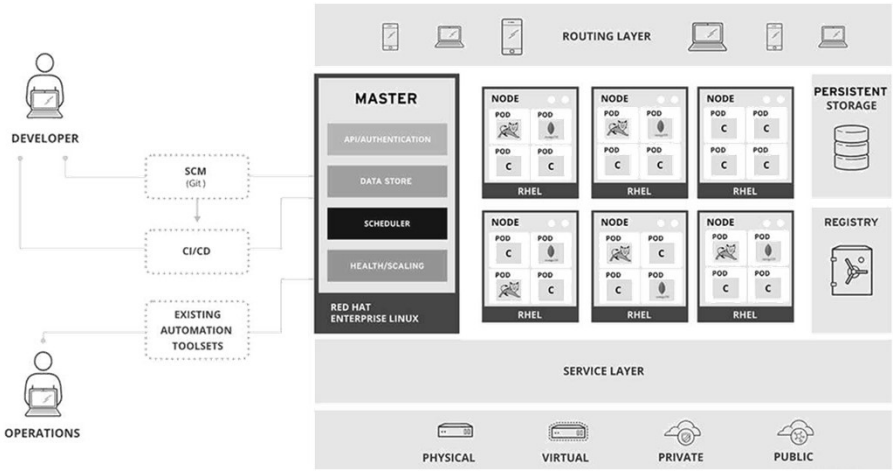
❖ 하이브리드 클라우드 아키텍처와 가상화 계층



316

MULTI-CLOUD MANAGEMENT

❖ Multi-Cloud Management with OpenShift, Cloud Foundry, Mirantis, & OnApp

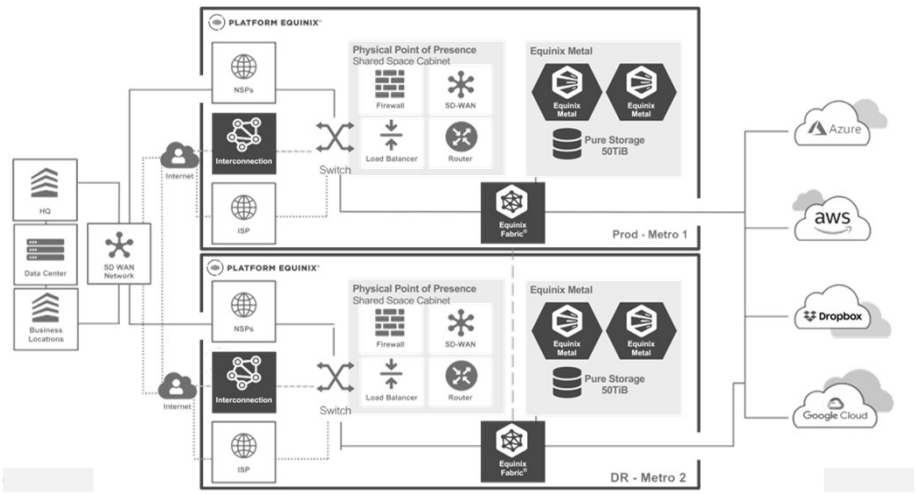


Source: https://hostadvice.com/blog/web-hosting/cloud/multi-cloud-management-with-openshift-cloud-foundry-mirantis-onapp/

317

PROD/DR DEPLOYMENT MODEL

❖ Prod/DR Deployment Model



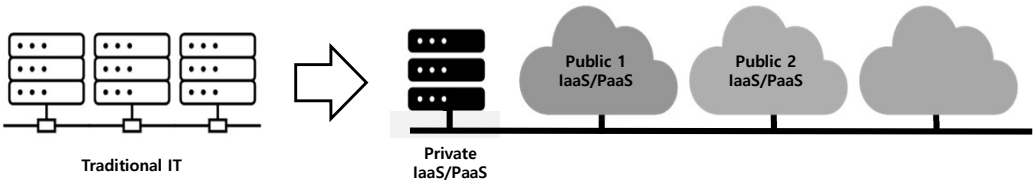
Source: Equinix

318

클라우드 운영 모델의 변화

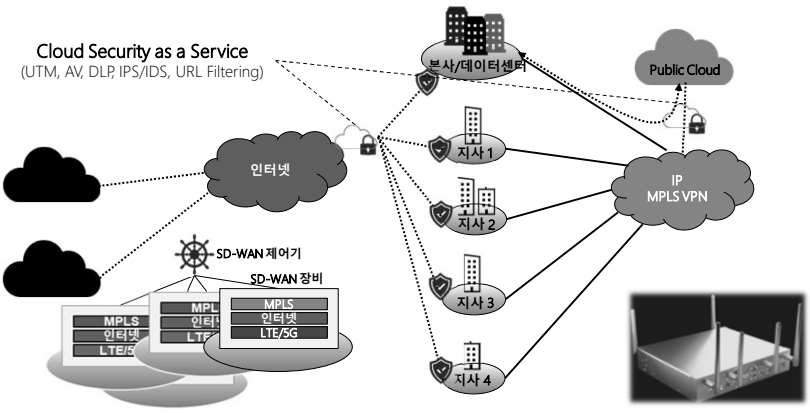
❖ **클라우드 운영 모델의 변화**

- **Run:** 전용 인프라 → 클라우드 상의 스케듈링
- **Connect:** 고정 IP 주소 → 서비스 기반 유동 IP
- **Secure:** IP 주소 기반 보안 정책 → Identity 기반
- **Provisioning:** 전용 서버 → 요청 기반 용량



SD-WAN

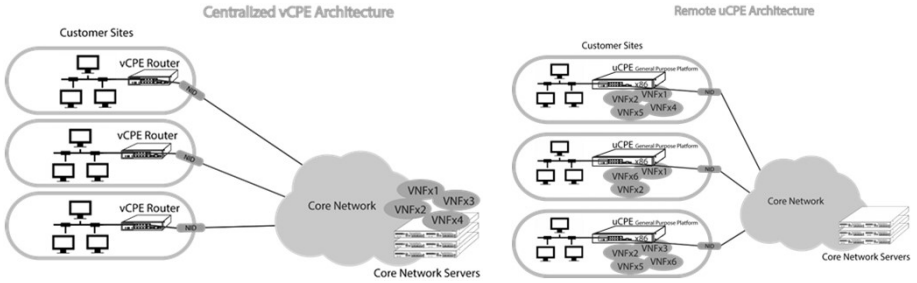
❖ **SD-WAN의 발전**
❖ **Multi-Cloud 를 위한 엔터프라이즈 인터넷 접속 (하이브리드 클라우드)**
❖ **Cloud Security as-a-Service**



UCPE / VCPE

❖ **가상화 네트워크 기능 배포 기반 SD-WAN 구성**

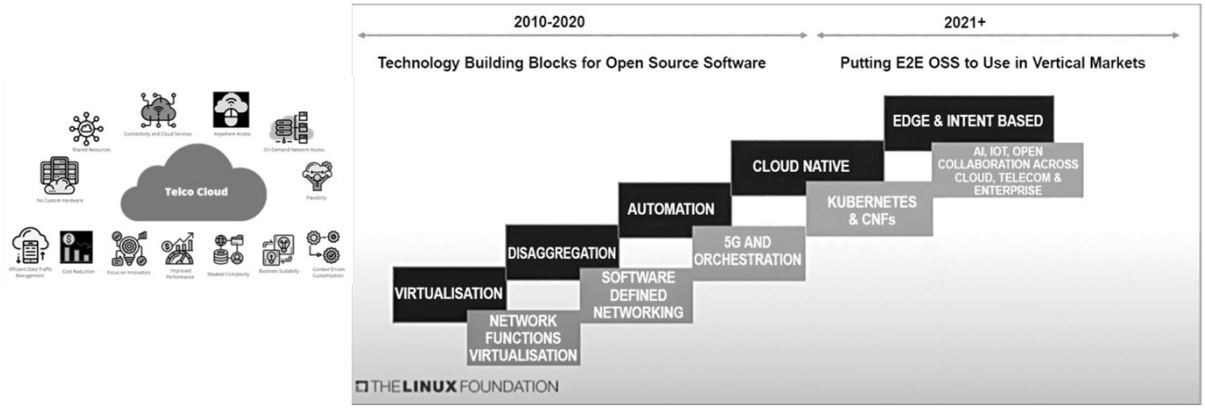
- **지역 배포 (예): uCPE (universal CPE)**
  - ✓ 고사양 SD-WAN 하드웨어
  - ✓ 환경 변화에 따른 설계의 유연성
- **중앙 서비스 (예): vCPE or virtualized CPE**
  - ✓ 저사양 SD-WAN 하드웨어
  - ✓ 데이터센터 집중 관리



321

LF EDGE PROJECTS

❖ **Focus shifting from building blocks to putting E2E OSS to use (Linux Foundation)**



Source: https://www.electronicsforu.com/technology-trends/open-source-ecosystem-5g-telecom-networks

322

MULTI-CLOUD 운영 이슈

❖ **Multi-Cloud 운영 이슈**

클라우드 네트워킹의 복잡성

❖ **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

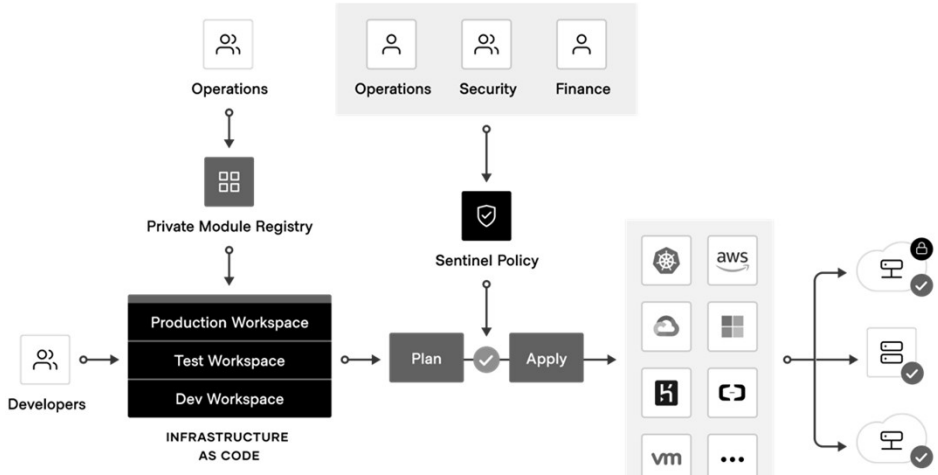
SIMPLIFYING COMPLEXITY

❖ **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**

PROVISIONING WITH TERRAFORM

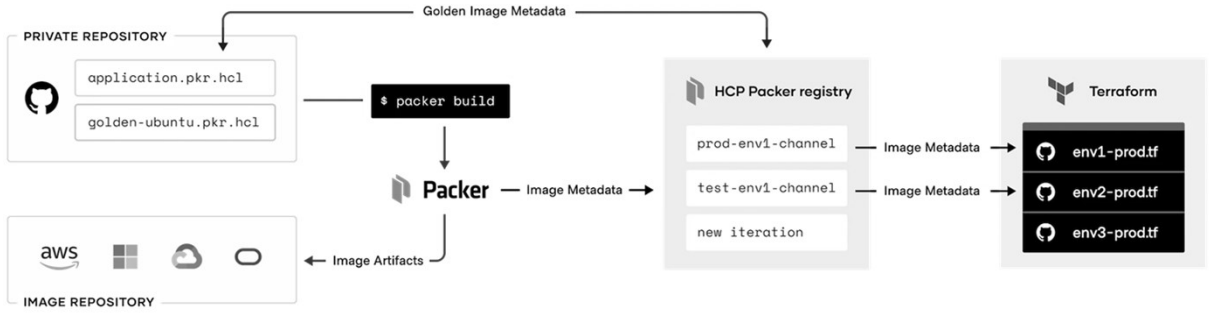
❖ Infrastructure Provisioning with Terraform



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

BUILD AUTOMATED IMAGES

❖ **Build Automated Images with HashiCorp Packer** (HashiCorp)



Source: https://www.hashicorp.com/cloud-operating-model

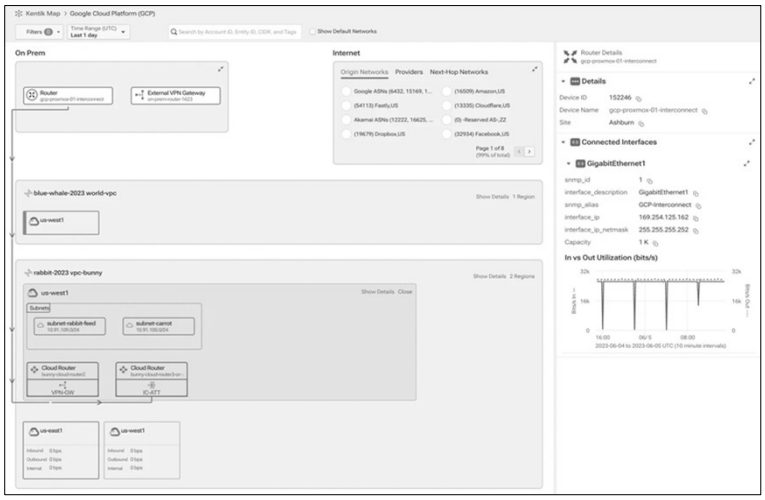
MONITORING WITH AIOPS

❖ Monitoring with AIOps

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

PLANNING

❖ Multicloud Network Observability

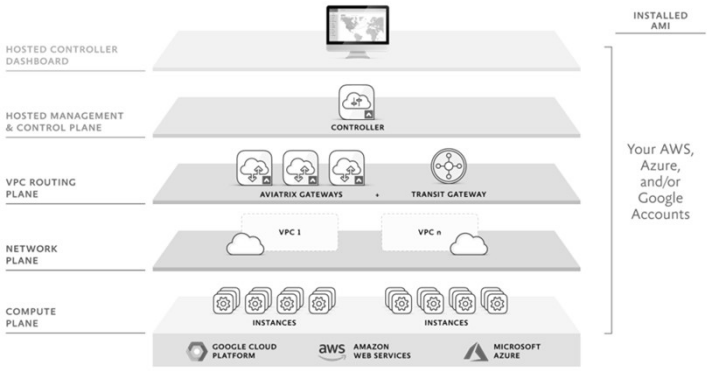


Source: https://www.kentik.com/kentipedia/multicloud-networking/

BUSINESS MODEL (1 OF 5)

❖ 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

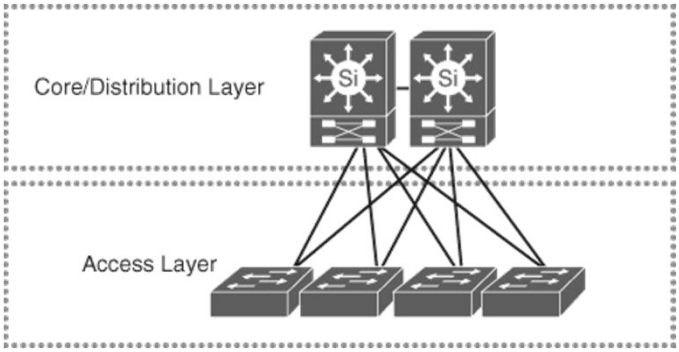


Source: https://hackmd.io/@terrencec51229/outline/%2FKF8s-B9kQwuAqub7ZheBFQ

BUSINESS MODEL (2 OF 5)

❖ 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

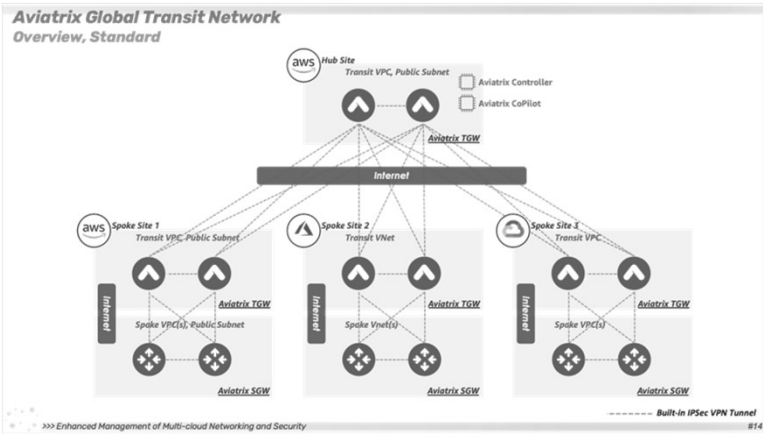


Source: https://hackmd.io/@terrencec51229/outline/%2FKF8s-B9kQwuAqub7ZheBFQ

BUSINESS MODEL (3 OF 5)

❖ 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

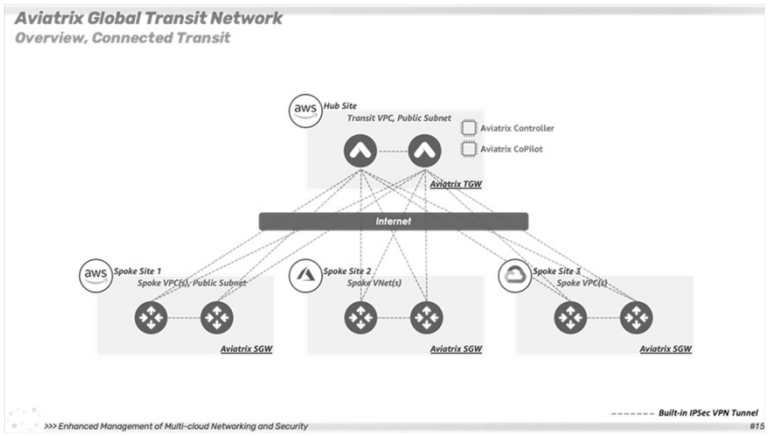


Source: https://hackmd.io/@terrencec51229/outline/%2FKF8s-B9kQwuAqub7ZheBFQ

BUSINESS MODEL (4 OF 5)

❖ 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

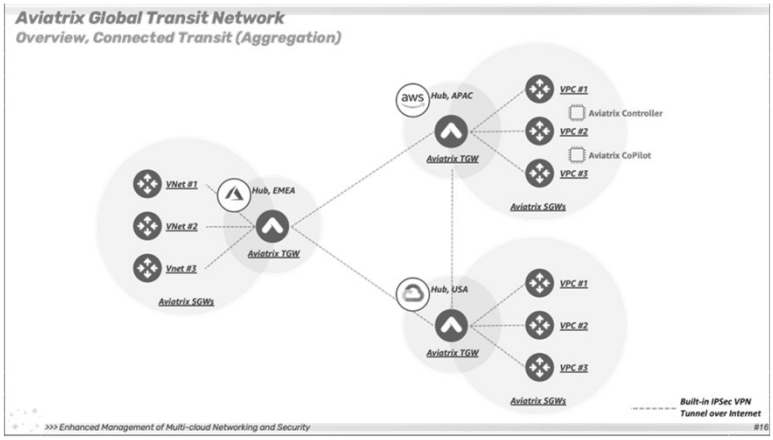


Source: https://hackmd.io/@terrencec51229/outline/%2FKF8s-B9kQwuAqub7ZheBFQ

BUSINESS MODEL (5 OF 5)

❖ 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

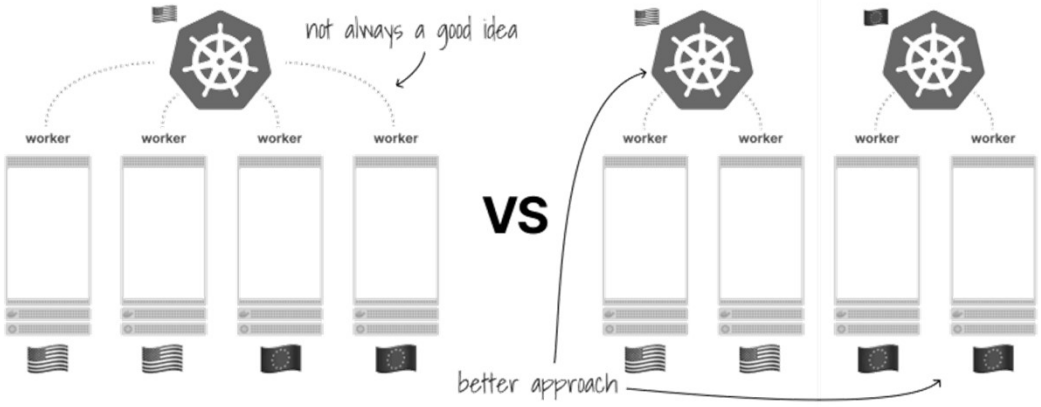


Source: https://hackmd.io/@terrencec51229/outline/%2FKF8s-B9kQwuAqub7ZheBFQ

KUBERNETES

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

• Scaling Kubernetes to multiple clusters and regions



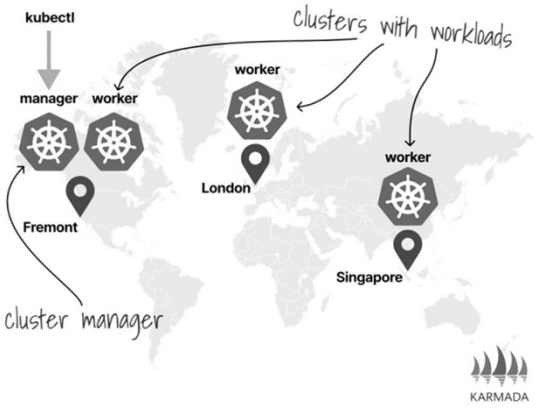
Source: https://dev.to/danielepolencic/scaling-kubernetes-to-multiple-clusters-and-regionss-294b?fbclid=IwAR2X-TIy2ehLRf2hewOoy6VE0ZVdaL2FkTLY_pgH7gT6oDltKZb_ssoukzo

335

KARMADA

❖ 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.

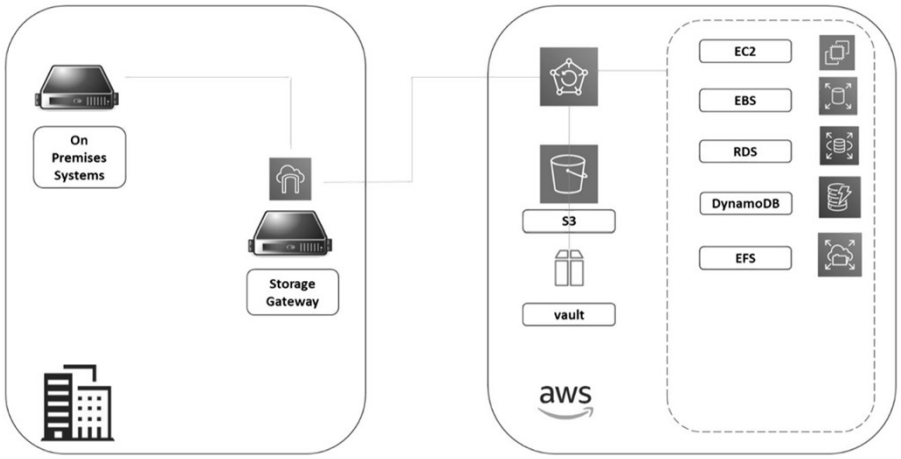


Source: https://karmada.io/docs/userguide/scheduling/resource-propagating

336

HYBRID BACKUP IN AWS

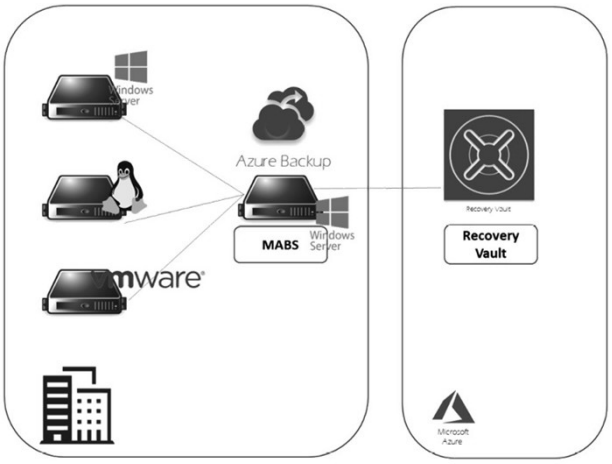
❖ 클라우드 백업 (예): Hybrid backup in AWS



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.

AZURE BACKUP SERVER

❖ 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.

멀티클라우드 데이터센터 관리(예)

❖ Multi-Cloud Management: 설계 스토리보드 (예)

별도 슬라이드 자료 사용

CMP FOR MULTI-CLOUD

❖ 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.bunnyshell.com/blog/multi-cloud-management-platforms

NETWORK MANAGEMENT

❖ 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/

OPEN SOURCE CLOUD MONITORING

❖ 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

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

OPEN SOURCE CMP

❖ Open Source Cloud Management Platforms (CMP)

- 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/

CMP

❖ 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
- Sematext - 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

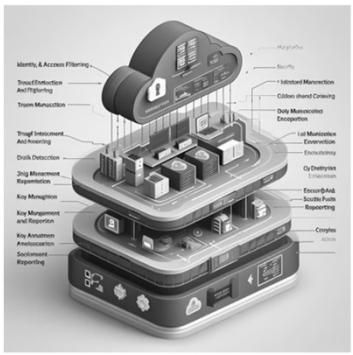
CMP

❖ Comparison Of The BEST Cloud Management Platforms (2023)

- 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/

V. 멀티 클라우드 보안



WHAT IS MULTI-CLOUD SECURITY?

❖ WHAT IS MULTI-CLOUD SECURITY?

• THE SHARED RESPONSIBILITY MODEL

RESPONSIBILITY	On-Premises	IaaS	FaaS	SaaS	PaaS	CIS Controls Cloud 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	●	○	○	○	○		

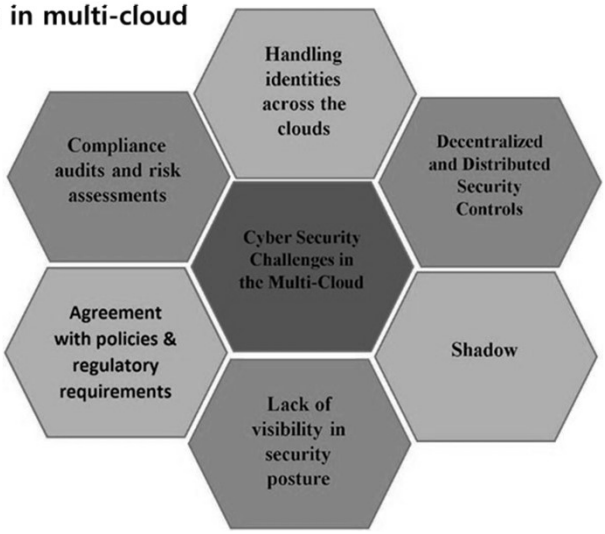
● Cloud Customer ○ Cloud Provider

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

CYBER SECURITY CHALLENGES

❖ 사이버보안 도전 - Cyber security challenges in multi-cloud

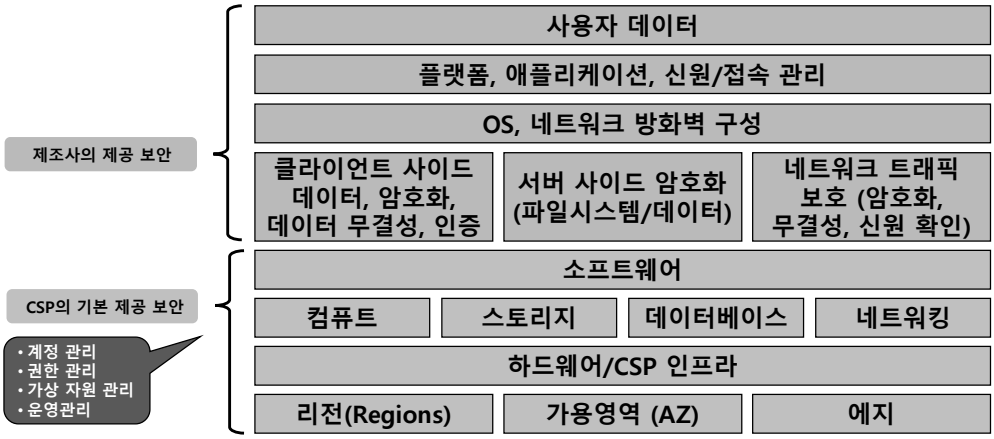
- 준수.. (Compliance..)
- 정책.. (Policy..)
- 가시화.. (Visibility..)
- 음영 (Shadow)
- 탈중앙 제어.. (Decentralized..)
- 클라우드간 ID.. (Identity..)



Source: 'Operationalizing Multi-Cloud Environments', Technologies, Tools and Use Cases, B. S. Rajeshwari, Pethuru Raj, Ramkumar Thirunavukarasu (2022)

CSP와 제조사

❖ 클라우드 보안을 위한 CSP와 제조사 (예)



보안 솔루션 비교

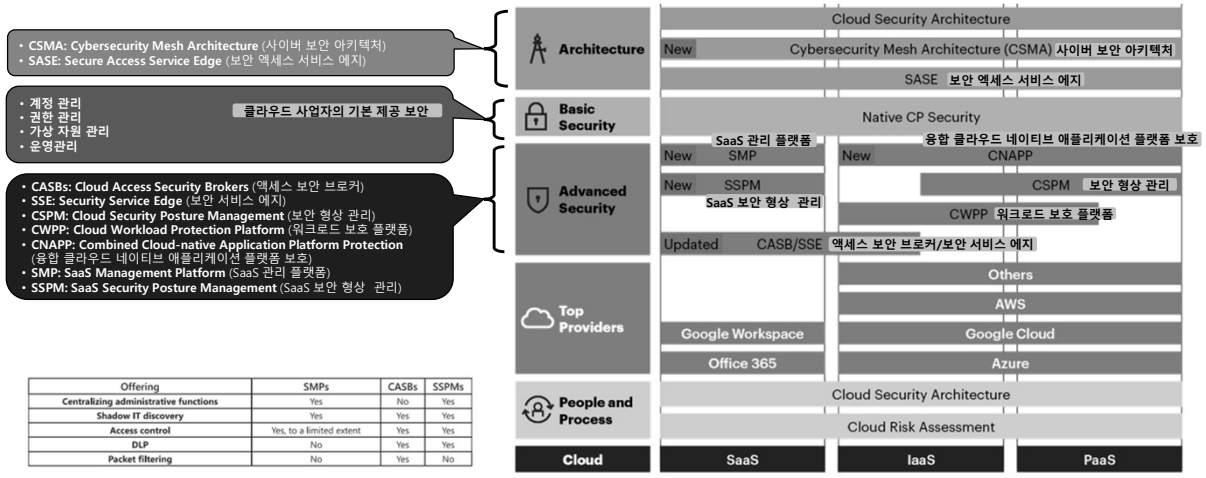
❖ CSP Native vs 3rd Party 보안 솔루션 비교

		비교 우위	
비용 효율성	CSP Native는 초기 투자 비용이 없으며 사용한 만큼 지불 할 수 있음	CSP Native	3rd Party ISV
가용성	CSP Native는 CSP가 SLA를 보장하며, 고객의 운영 부담이 낮음	CSP Native	3rd Party ISV
탄력성	CSP Native는 사용량 증감에 따라 CSP가 자동으로 Resource를 조절함	CSP Native	3rd Party ISV
도입 및 전환 속도	CSP Native 보안 기능은 구매 / 설치 등의 절차가 불필요함	CSP Native	3rd Party ISV
Multi 클라우드	3rd Party ISV는 모든 CSP에 동일 솔루션 적용 및 관리 가능함	CSP Native	3rd Party ISV
Hybrid 클라우드	3rd Party ISV는 On-premise까지 동일 솔루션 적용 및 관리 가능함	CSP Native	3rd Party ISV
난이도 및 기술지원	3rd Party ISV는 각 솔루션 제조사의 기술지원을 받기 용이함	CSP Native	3rd Party ISV

Source: https://www.samsungsds.com/kr/insights/cloud_security.html

적용 영역

❖ 가트너의 클라우드 보안 주요 주제에 대한 다양한 적용 영역



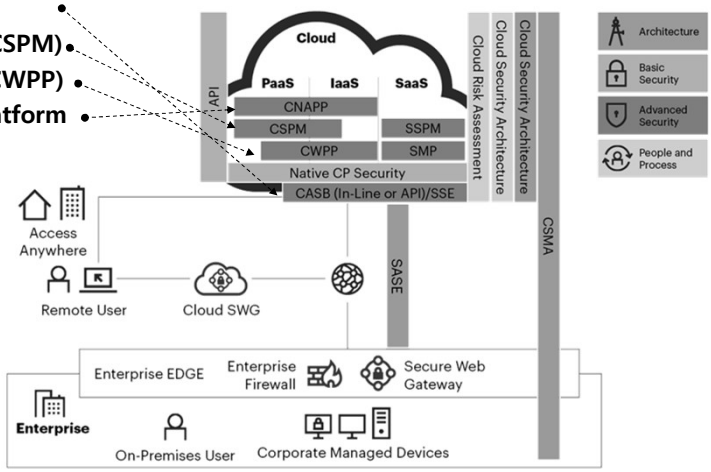
Offering	SMPs	CASBs	SSPMs
Centralizing administrative functions	Yes	No	Yes
Shadow IT discovery	Yes	Yes	Yes
Access control	Yes, to a limited extent	Yes	Yes
DLP	No	Yes	Yes
Packet filtering	No	Yes	No

Source: https://emtemp.gcom.cloud/ngw/eventassets/en/conferences/2023/secme10/documents/gartner_uae_sec_guide_to_cloud_security_concepts.pdf

LOGICAL ARCHITECTURE

❖ Cloud Security Logical Architecture

- Cloud Access Security Brokers (CASBs)
- Cloud Security Posture Management (CSPM)
- Cloud Workload Protection Platform (CWPP)
- Combined Cloud-native Application Platform Protection (CNAPP)



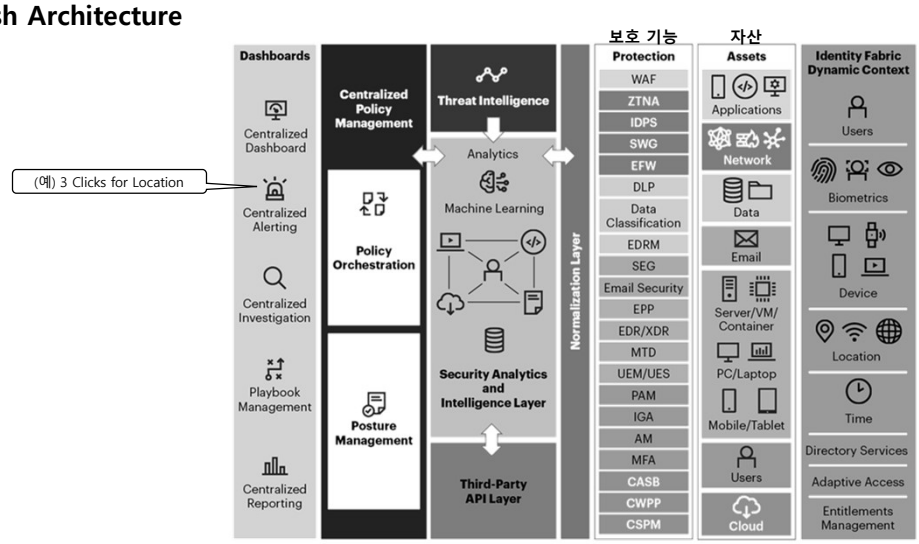
SSE: Security Service Edge (보안 서비스 에지)

CSMA: Cybersecurity Mesh Architecture (사이버 보안 아키텍처)

Source: Gartner

CYBERSECURITY MESH ARCHITECTURE

❖ **Cybersecurity Mesh Architecture**

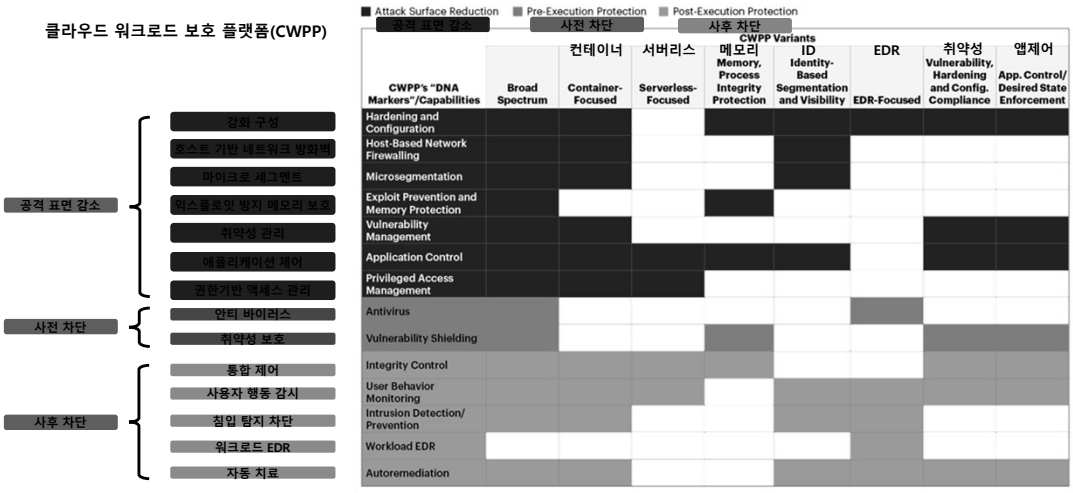


Source: Gartner

353

CWPP

❖ **Types of Cloud Workload Protection Platforms(CWPP) and Their Minimum Capabilities**



■ Attack Surface Reduction ■ Pre-Execution Protection ■ Post-Execution Protection

공격 표면 감소 | 사전 차단 | 사후 차단

CWPP's "DNA Markers"/Capabilities	CWPP Variants: Broad Spectrum	컨테이너 Container-Focused	서버리스 Serverless-Focused	메모리 Memory, Process Integrity Protection	ID Identity-Based Segmentation and Visibility	EDR EDR-Focused	취약성 Vulnerability, Hardening and Config. Compliance	앱제어 App. Control/ Desired State Enforcement
Hardening and Configuration	■	■		■			■	■
Host-Based Network Firewalling	■	■			■			
Microsegmentation	■	■			■			
Exploit Prevention and Memory Protection	■			■				
Vulnerability Management	■	■					■	■
Application Control	■	■	■	■	■		■	■
Privileged Access Management	■	■	■					
Antivirus	■					■		
Vulnerability Shielding	■			■			■	■
Integrity Control	■	■	■	■			■	■
User Behavior Monitoring	■	■	■		■	■	■	■
Intrusion Detection/ Prevention	■	■			■	■		
Workload EDR						■		
Autoremediation	■	■			■	■	■	■

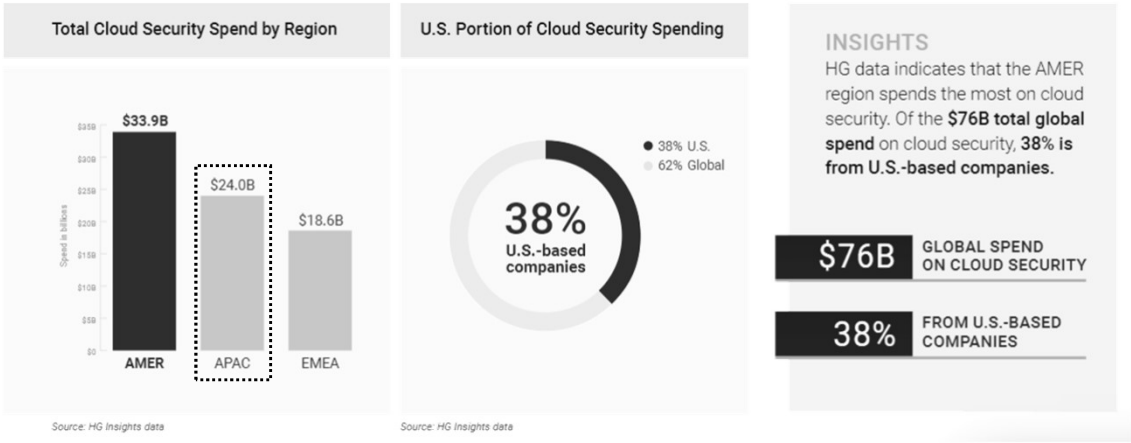
Source: Gartner

Endpoint detection and response (EDR)

354

글로벌 클라우드 보안 시장

❖ **글로벌 클라우드 보안 시장 규모 및 전망** (2023)

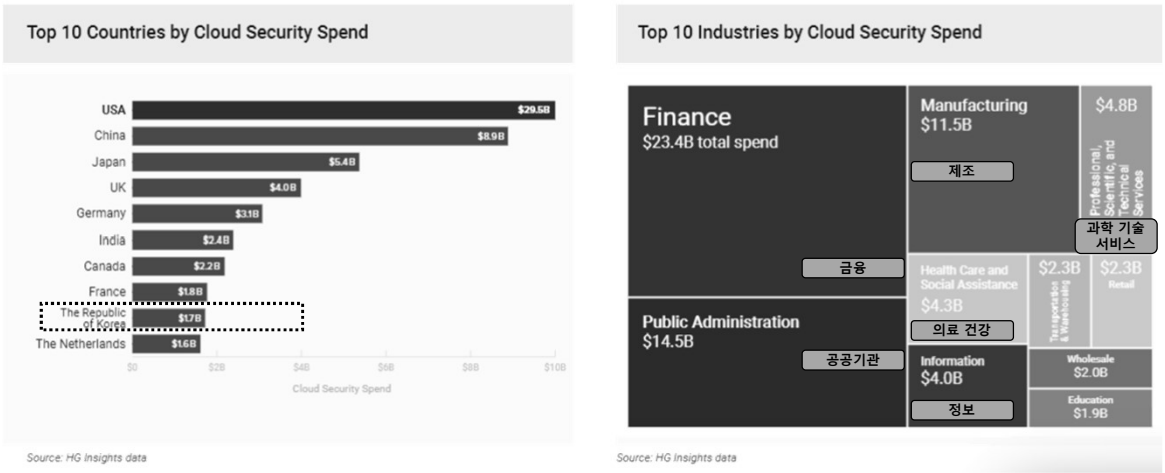


Source: https://hginsights.com/blog/2023-cloud-security-market-size-growth-forecast

355

CLOUD SECURITY SPEND

❖ **Top 10 Countries and Industries by Cloud Security Spend** (2023)



Source: https://hginsights.com/blog/2023-cloud-security-market-size-growth-forecast

356

보안 분야별 사용자 지출

❖ **2021-2023 전세계 보안 분야별 사용자 지출**

표1. 2021-2023년 전 세계 정보 보안 및 리스크 관리 분야별 최종 사용자 지출(단위: 백만 달러)

시장 분야	2021 지출	2021 성장률 (%)	2022 지출	2022 성장률(%)	2023 지출	2023 성장률(%)
애플리케이션 보안	4,963	20.8	6,018	21.3	7,503	24.7
클라우드 보안	4,323	36.3	5,276	22.0	6,688	26.8
데이터 개인 정보	1,140	14.2	1,264	10.8	1,477	16.9
데이터 보안	3,193	6.0	3,500	9.6	3,997	14.2
아이덴티티 액세스 관리(IAM)	15,865	22.3	18,019	13.6	20,746	15.1
인프라 보호	24,109	22.5	27,408	13.7	31,810	16.1
통합 리스크 관리(IRM)	5,647	15.4	6,221	10.1	7,034	13.1
네트워크 보안 장비	17,558	12.3	19,076	8.6	20,936	9.7
기타 정보 보안 소프트웨어	1,767	26.2	2,032	15.0	2,305	13.4
보안 서비스	71,081	9.2	71,684	0.8	76,468	6.7
소비자 보안 소프트웨어	8,103	13.7	8,659	6.9	9,374	8.3
총계	157,749.7	14.3	169,156.2	7.2	188,336.2	11.3

출처: 가트너 (2022년10월)

Source: https://zdnet.co.kr/view/?no=20221014164810

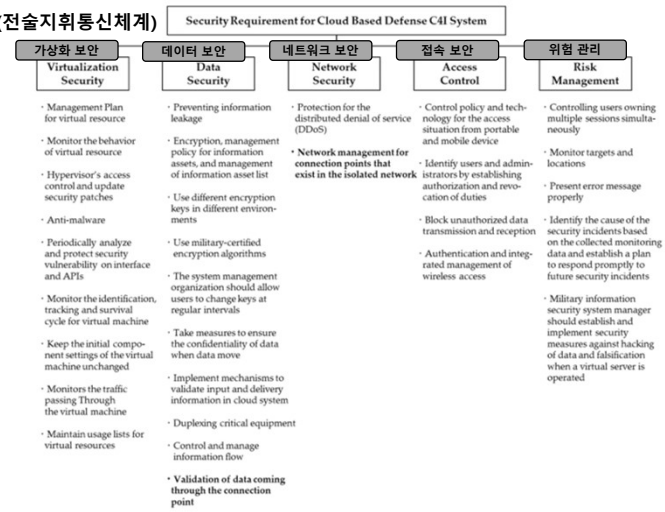
CLOUD-BASED DEFENSE C4I SYSTEM

❖ **Security requirements for cloud-based defense C4I system.**

- **Risk Management**
- **Access Control**
- **Network Security**
- **Data Security**
- **Virtualization Security**
  - 가상자원 관리
  - 가상자원 모니터
  - 하이퍼바이저 보안
  - Anti-malware
  - 주기적 보안 분석
  - VM 모니터
  - VM 세팅 유지
  - VM 트래픽 모니터
  - 가상 자원 사용 관리

클라우드 확장 모니터 오픈소스(예)
https://www.netdata.cloud/

C4I 체계(전술지휘통신체계)

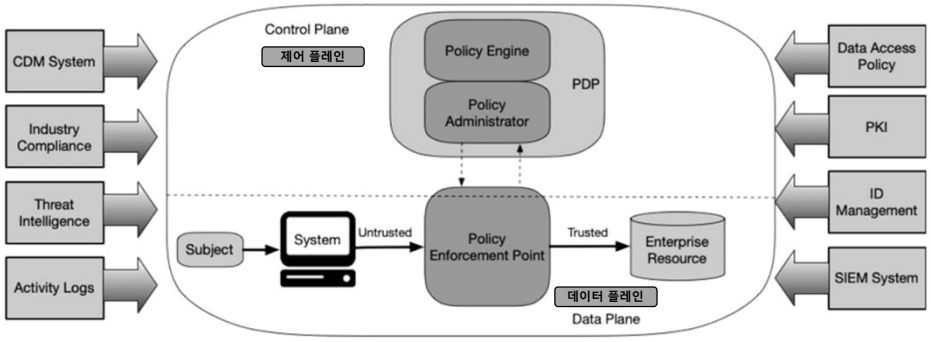


Source: https://www.mdpi.com/2071-1050/13/24/13827/htm

LOGICAL ZERO TRUST COMPONENTS

❖ NIST(National Institute of Standards and Technology), 미국 국립표준기술연구소

• Logical Zero Trust Components: 800-207 Zero Trust Architecture



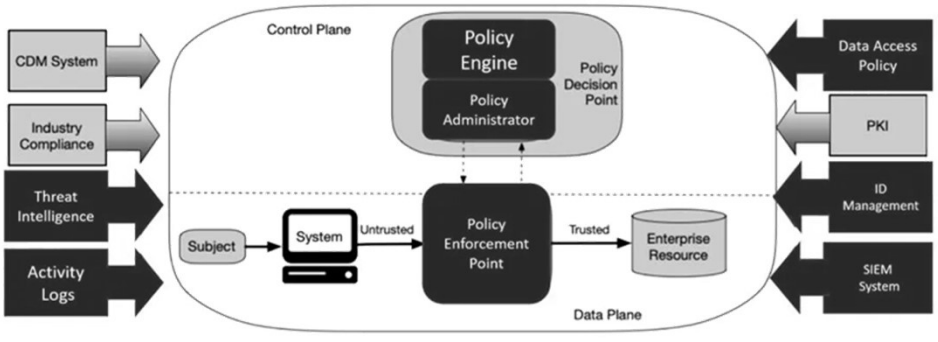
Core Zero Trust Logical Components

PDP (Policy Decision Point), PEP (Policy Enforcement Point), CDM (Clean Development Mechanism), PKI (Public Key Infrastructure)
Source: https://www.techrepublic.com/article/zero-trust-security-a-cheat-sheet/

359

RSA SECURITY BUSINESS

❖ RSA Security Business Unit Applicable Overlay



Core Zero Trust Logical Components (from NIST SP 800-207)

RSA Security Business Unit Applicable Overlay

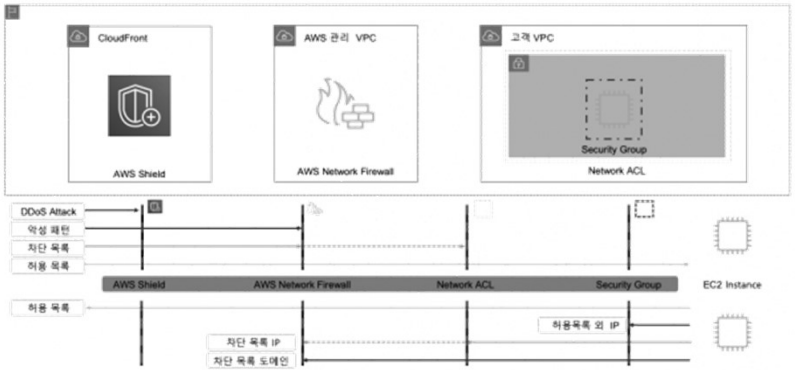
Source: https://www.rsa.com/zero-trust/what-is-zero-trust/

360

AWS 가상네트워크(VPC) 인프라 보안

❖ AWS 가상네트워크(VPC) 인프라 보안: AWS 서비스 보안

- AWS 실드(AWS Shield)
- AWS 네트워크 파이어월(AWS Network Firewall)
- NACL(Network Access Control List)
- 보안 그룹(Security Group)
- 데이터 암호화



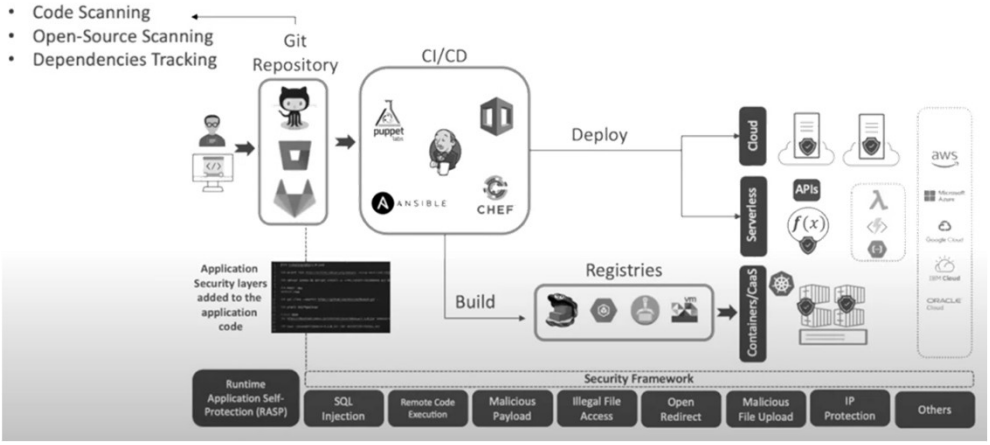
Source: http://www.datanet.co.kr/news/articleView.html?idxno=178057

361

RSA SECURITY BUSINESS

❖ Trend Micro - Embedding Microservices Security

- Code Scanning
- Open-Source Scanning
- Dependencies Tracking

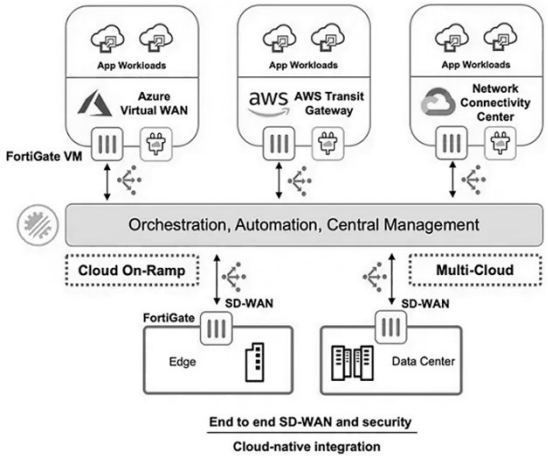


Source: https://www.trendmicro.com/en_dk/devops/22/a/microservice-security-how-to-proactively-protect-apps.html

362

SECURE SD-WAN FOR MULTI-CLOUD

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



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

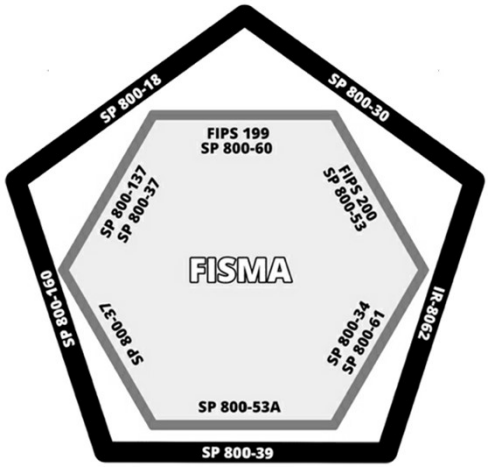
363

FISMA

❖ **Federal Information Security Modernization Act:**

- **FISMA is composed of a number of NIST publications.**

- **FIPS-199: Categorization**
- **SP 800-60 Vol. 1 Rev. 1: Guide for Mapping Types of Information and Information Systems to Security Categories**
- **SP 800-37 Rev. 2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy**
- **SP 800-53A Rev. 5: Assessing Security and Privacy Controls in Information Systems and Organizations**
- **SP 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations**
- **SP 800-61 Rev. 2: Computer Security Incident Handling Guide**
- **SP 800-18 Rev. 1 : Guide for Developing Security Plans for Federal Information Systems**



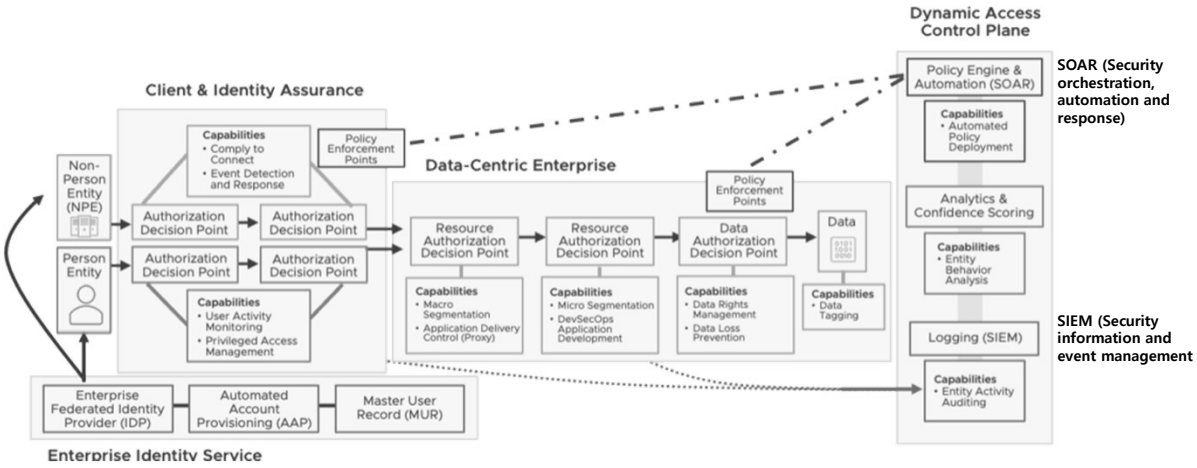
NIST (National Institute of Standards and Technology), 미국 국립표준기술연구소

Source: Coombs, Ted. Cloud Security For Dummies (p. 307). Wiley. Kindle Edition.

364

ZERO–TRUST ARCHITECTURE 엔터프라이즈

❖ Zero – Trust Architecture 엔터프라이즈 (예)

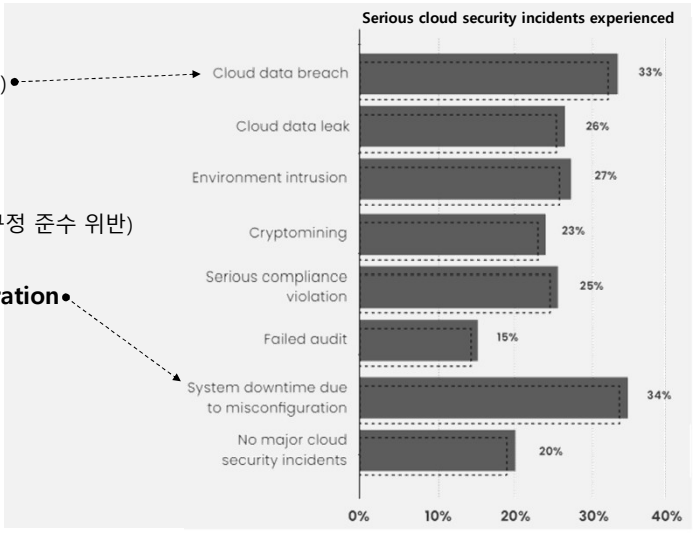


365

클라우드 보안 사고

❖ **심각한 클라우드 보안 사고 경험**

- **Cloud data breach** (클라우드 데이터 침해)
- **Cloud data leak** (클라우드 데이터 유출)
- **Environment intrusion** (환경 침입)
- **Cryptomining** (암호화폐 채굴)
- **Serious compliance violation** (심각한 규정 준수 위반)
- **Failed audit** (감사 실패)
- **System downtime due to misconfiguration** (잘못된 구성으로 인한 시스템 다운타임)
- **No major cloud security incidents** (주요 클라우드 보안 사고 없음)



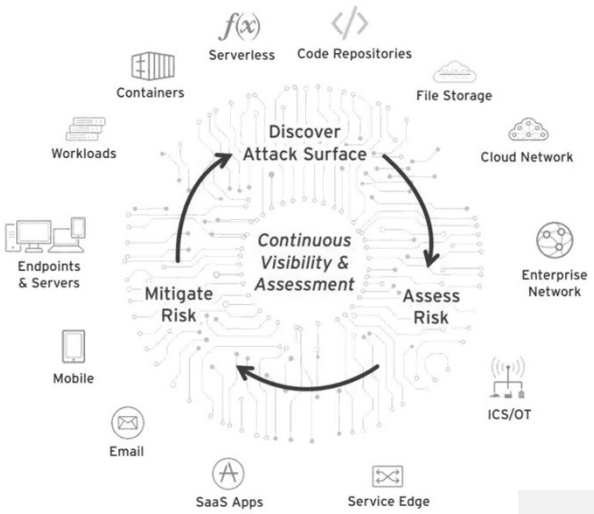
Source: https://resources.snyk.io/state-of-cloud-security , The State of Cloud Security Report 2022, synk

366

ATTACK SURFACE

❖ **다양한 공격 표면**(Attack Surface), 2023

- **Massive growth in SaaS applications**
  (SaaS 애플리케이션의 큰 성장)
- **Software supply chain uncertainty**
  (소프트웨어 공급망의 불확실성}
- **Work-from home**
  (재택 근무)
- **IT / OT convergence & 5G**
  (IT/OT 융합 및 5G)
- **Rapid growth in cloud native services**
  (클라우드 네이티브 서비스의 급속한 성장)
- **Cloud native applications**
  (클라우드 네이티브 애플리케이션)

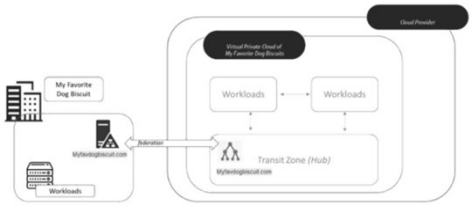


Source: https://www.trendmicro.com/en_gb/ciso/22/d/attack-surface-management.html

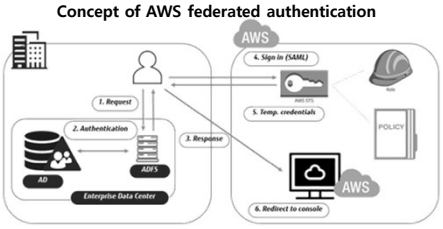
ACCESS MANAGEMENT

❖ Designing access management across multi-cloud

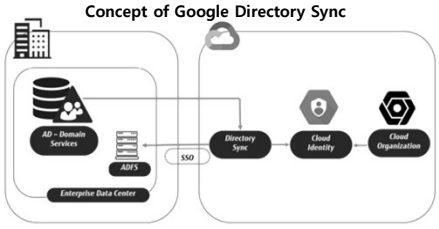
Conceptual overview of AD federation



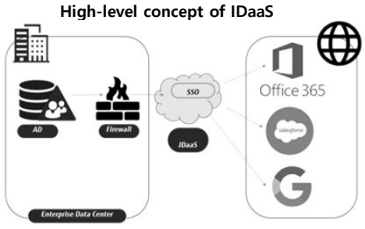
Concept of AWS federated authentication



Concept of Google Directory Sync



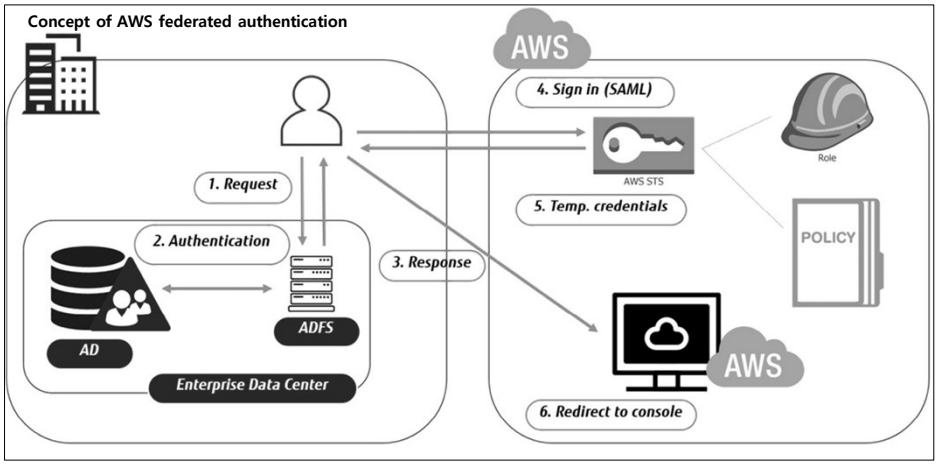
High-level concept of IDaaS



FEDERATED AUTHENTICATION

❖ Designing access management across multi-cloud

• Concept of AWS federated authentication



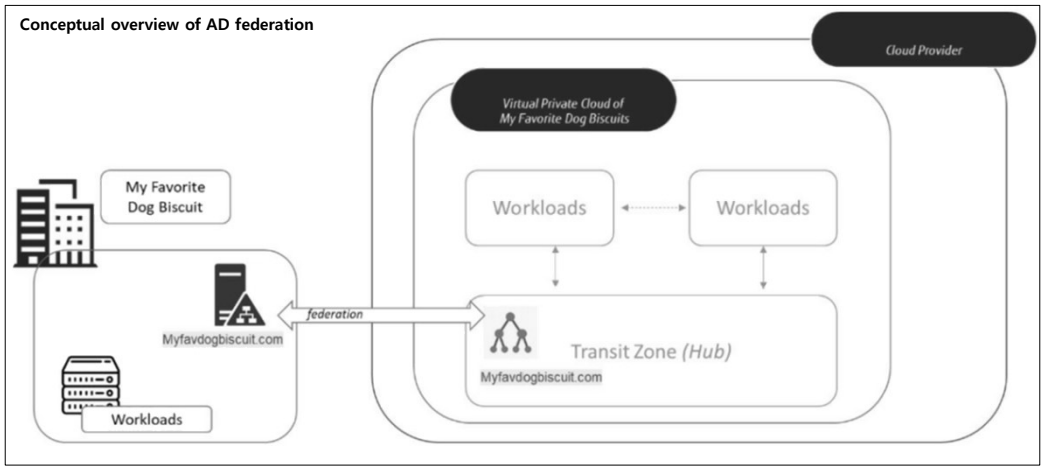
Source: Mulder, Jeroen. Multi-Cloud Architecture and Governance: Leverage Azure, AWS, GCP, and VMware vSphere to build effective multi-cloud solutions (p. 394). Packt Publishing. Kindle Edition.

369

AD FEDERATION

❖ Designing access management across multi-cloud

• Conceptual overview of AD federation



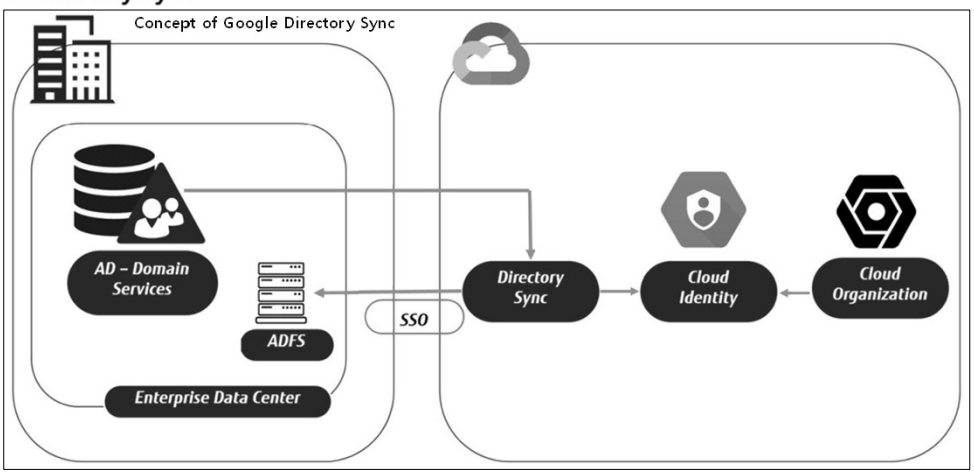
Source: Mulder, Jeroen. Multi-Cloud Architecture and Governance: Leverage Azure, AWS, GCP, and VMware vSphere to build effective multi-cloud solutions (p. 145). Packt Publishing. Kindle Edition.

370

GOOGLE DIRECTORY SYNC

❖ 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.

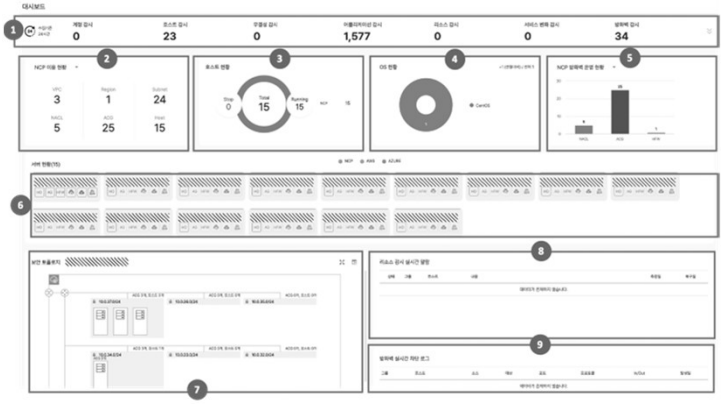
371

클라우드 보안 형상관리 서비스

❖ 네이버클라우드: 클라우드 보안 형상관리 서비스 'Cloud Security Watcher'

• 네이티브 클라우드 보안 형상관리 서비스 (Cloud Security Posture Management, CSPM)
• 자산 가시성 확보, 보안 규정 준수 평가, 위협 교정 지원, 멀티 클라우드 통합 관리

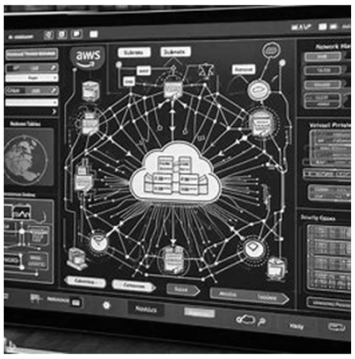
영역	설명
① 24시간 변동 현황 모니터링	대시보드 상단에 배치된 메뉴
② 이용 현황	사용 중인 클라우드 서비스에서 그룹, 클라우드, 리전 정보, VPC/VNet, 서브넷 등 이용 현황
③ 호스트 현황	사용 중인 클라우드 서비스의 전체 호스트 현황
④ OS 현황	사용 중인 클라우드 서비스에 설치된 OS 현황
⑤ 방화벽 운영 현황	사용 중인 클라우드 서비스의 전체 방화벽 운영 현황
⑥ 서버 현황	클라우드 서비스 내 등록된 서버 현황
⑦ 보안 토폴로지	호스트의 네트워크별 정보를 기반으로 생성된 토폴로지
⑧ 리소스 감시 실시간 알람	클라우드 서비스 내 등록된 호스트들에 대한 정책 설정 시 지정한 임계치별 호스트 상태의 위험, 주의가 발생된 내역
⑨ 방화벽 실시간 차단 로그	클라우드 서비스 내 등록된 호스트들의 방화벽 차단에 발생한 최근 알람 리스트



Source: https://guide.ncloud-docs.com/beta/docs/csw-use

372

VI. 멀티 클라우드의 Cloud Native 서비스 연동

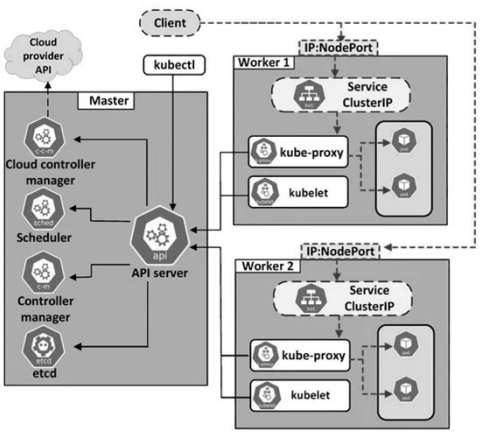


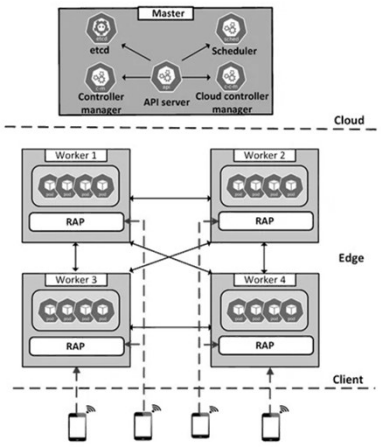
373

KUBERNETES INFRASTRUCTURE

❖ **Load-Balancing of Kubernetes-Based Edge Computing Infrastructure**

- **Using Resource Adaptive Proxy (RAP)**



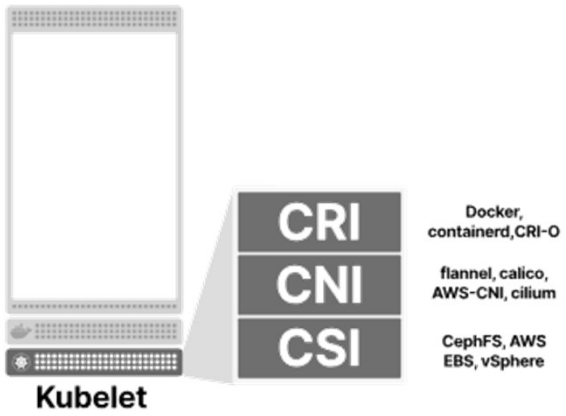


Source: https://www.mdpi.com/1424-8220/22/8/2869/htm

374

CRI/CNI/CSI

- Container Runtime Interface - CRI
- Container Network Interface - CNI
- Container Storage Interface - CSI

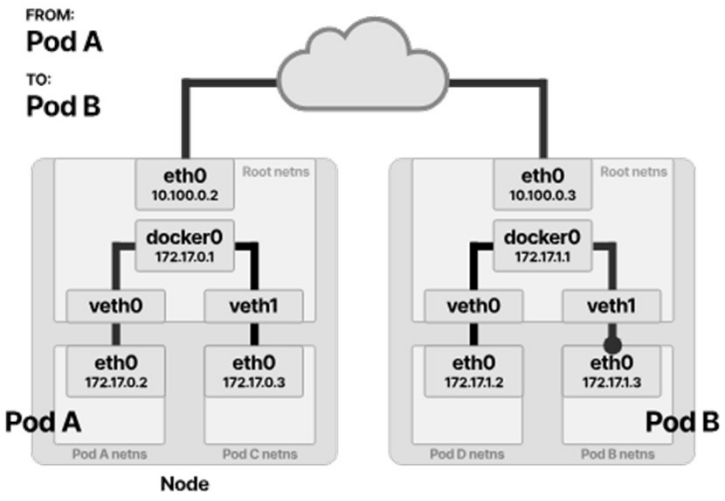


Source: https://learnk8s.io/kubernetes-network-packets

375

TRACING NETWORK TRAFFIC

- Pod-to-Pod.

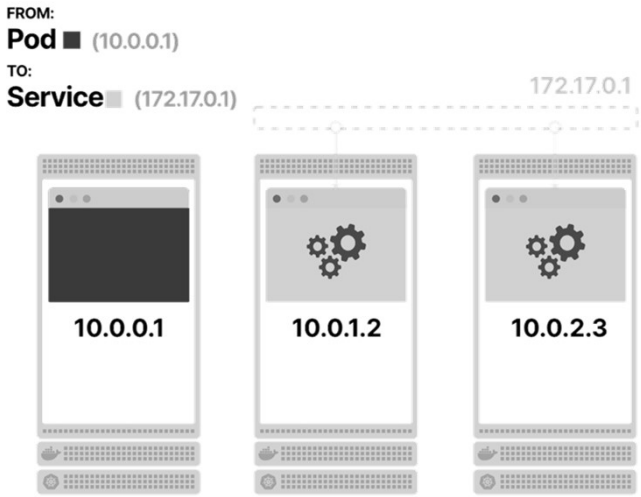


Source: https://learnk8s.io/kubernetes-network-packets

376

POD-TO-POD

❖ **Pod-to-Pod**



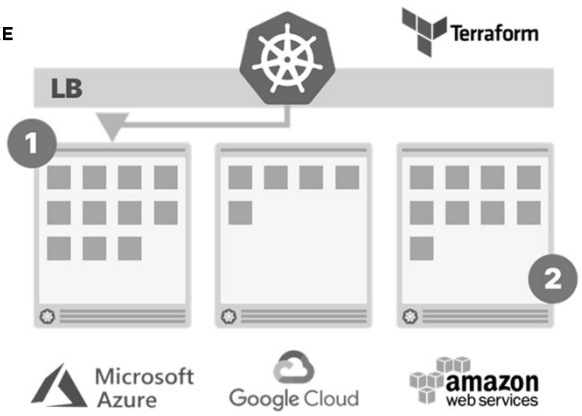
Source: https://learnk8s.io/kubernetes-long-lived-connections

377

CREATING K8S WITH TERRAFORM

❖ **Creating Kubernetes clusters with Terraform**

1. Provisioning K8s clusters on AWS with Terraform and EKS
2. Getting started with Terraform and K8s on Azure AKS
3. Provisioning K8s clusters on GCP with Terraform and GKE
4. Provisioning K8s clusters on Linode with Terraform



Source: https://learnk8s.io/kubernetes-terraform

378

MULTI-CLOUD CHALLENGES

❖ Multi-Cloud Challenges

- Different Cloud Service Providers Have Different APIs

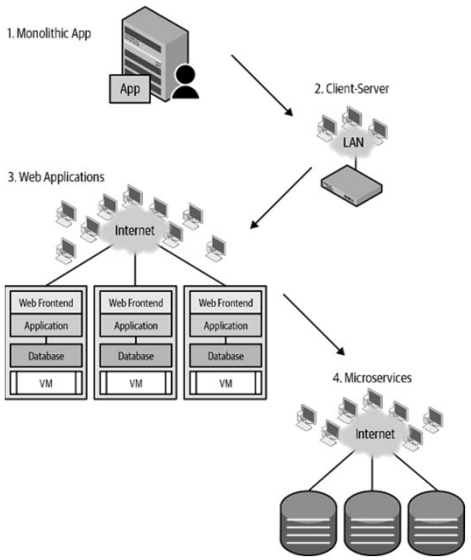
	Static		Dynamic			
	DEDICATED		PRIVATE CLOUD	AWS	AZURE	GCP
Run Deployment	vSphere	→	vSphere	EKS / ECS Lambda	AKS / ACS Azure Functions	GKE Cloud Functions
Connect Networking	Hardware	→	Various Hardware	CloudMap AppMesh	Proprietary	Google Istio
Secure Security	IP: Hardware	→	Identity: AD/LDAP	Identity: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

379

EVOLUTION OF APPLICATION

❖ Evolution of application architecture

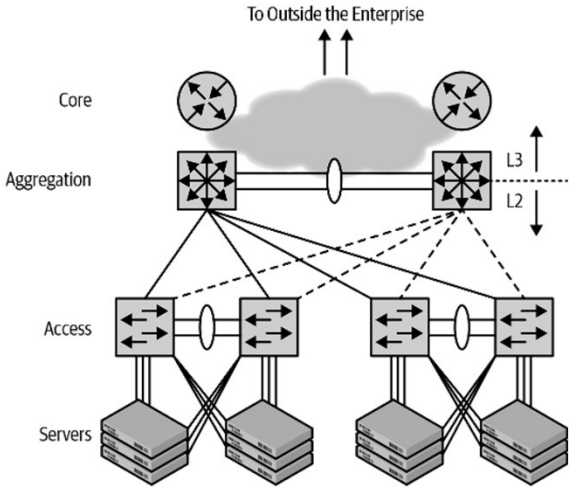


Source: Cloud Native Data Center Networking (Architecture, Protocols, and Tools), Dinesh G. Dutt, O'REILLY

380

ACCESS-AGGREGATION-CORE

❖ Access-aggregation-core network architecture



Source: Cloud Native Data Center Networking (Architecture, Protocols, and Tools), Dinesh G. Dutt, O'REILLY

381

CODE-TO-CLOUD RISK

❖ Code-to-Cloud Risk Visibility, Prioritization and Remediation.

	Code		Build		Deploy		Run in Cloud
Developer	Developer Identities						Runtime Cloud-Native Application Risk
	Secrets Management						
Tools	IDE	Code/Git Repository	Build Servers	Configuration	Staging	Continuous Deployment	
Artifacts	• Custom Code • Custom APIs • Third-Party APIs • Declarative APIs (e.g., OpenAPI) • Third-Party SDKs • Application Platforms • OSS Libraries • OSS Frameworks		• Compiled Code • Container Layers • Containers • Virtual Machines • Serverless Functions		• IaC Scripts • Kubernetes YAML Files • Kubernetes Helm Charts		
Attack Path Analysis	= Cloud Control Plane Risk Scanning		+ Artifact Risk Scanning				

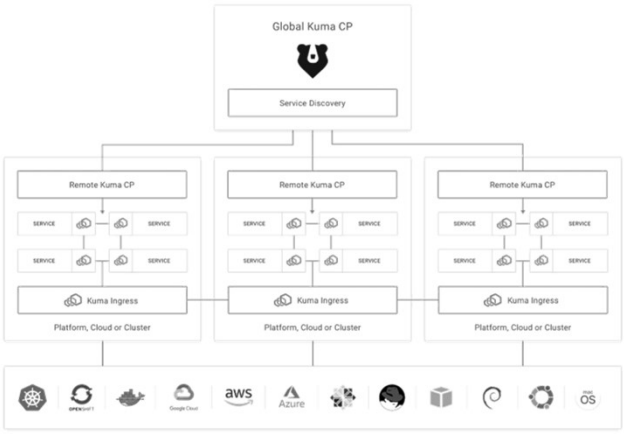
IDE = integrated development environment; OSS = open-source software

Source: https://www.uptycs.com/blog/6-takeaways-cnapp-gartner-market-guide-2023

SERVICE MESH

❖ **Multi-Cloud Service Networking**

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

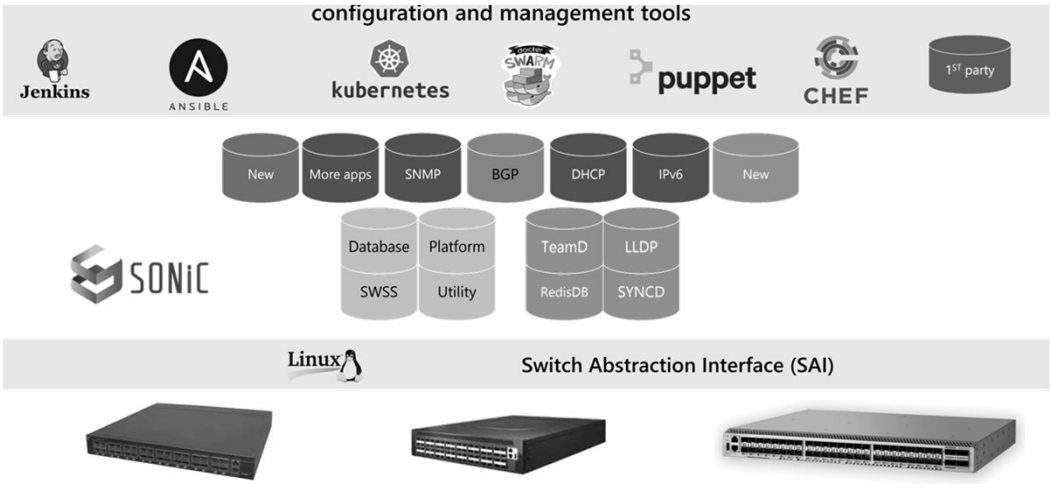


Source: https://kuma.io/

383

SONIC

❖ **SONiC** (Software for Open Networking in the Cloud)

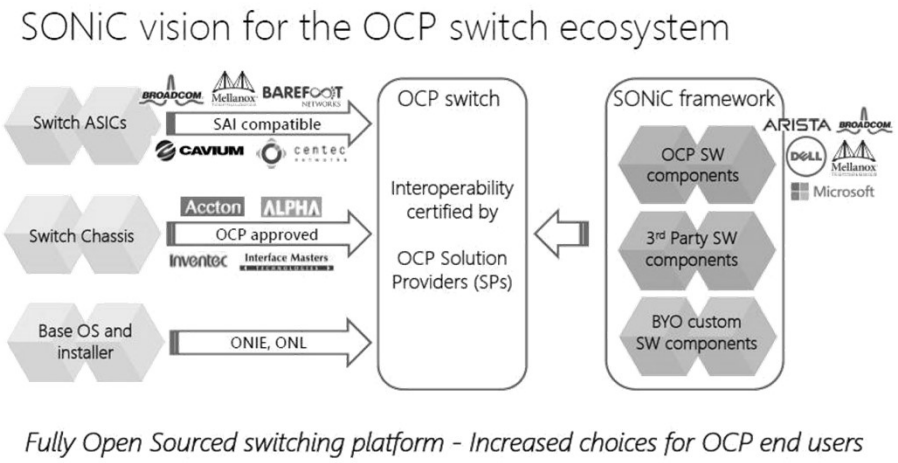


384

SONIC ECOSYSTEM

❖ **SONiC ecosystem**

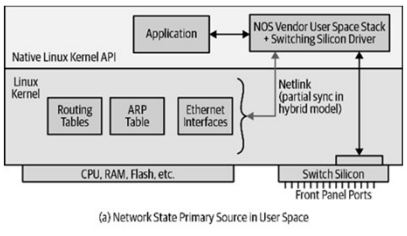
- SONiC (Software for Open Networking in the Cloud)

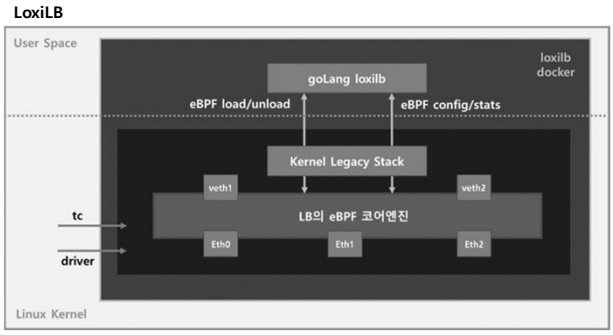


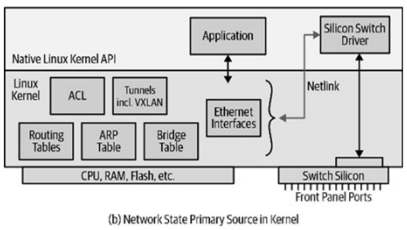
EBPF

❖ **How a user-space switching-silicon driver gets information**

- **Kernel-space 생성 정보 수집 필요**
- **eBPF(Kernel-space sandbox app):** Cilium, LoxiLB, EKS Anywhere



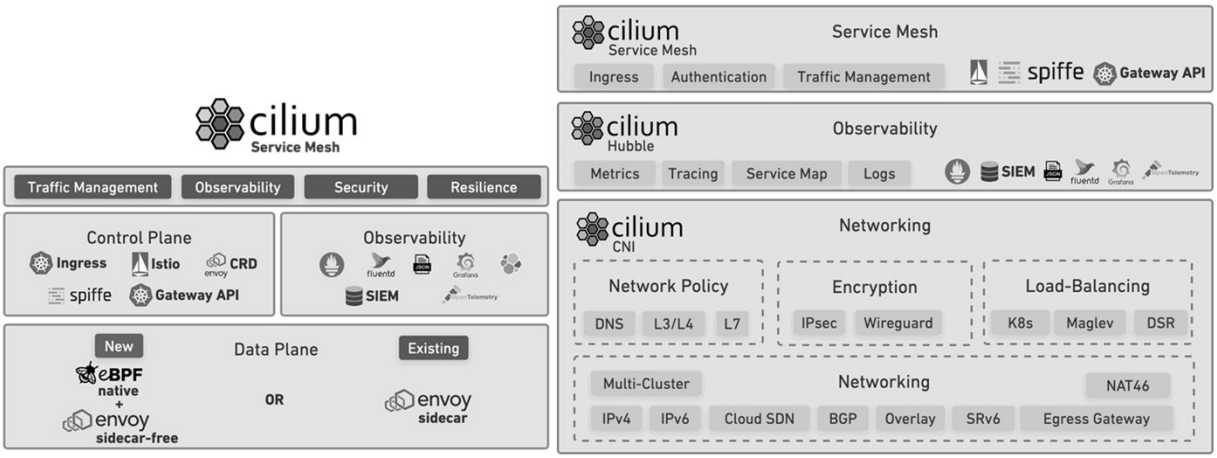




Source: Cloud Native Data Center Networking (Architecture, Protocols, and Tools), Dinesh G. Dutt, O'REILLY

CILIUM

❖ eBPF 사용 (예): Cilium 1.12 Major Features



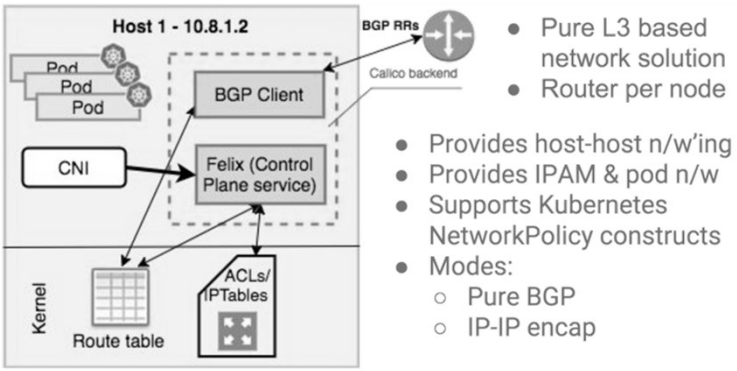
Source: https://www.cncf.io/blog/2022/07/20/cilium-1-12-ga-cilium-service-mesh-and-other-major-new-features-for-enterprise-kubernetes/

387

CALICO PROJECT

❖ Kubernetes CNI의 BGP 사용 (예): Calico Project

- Pure L3 based network solution
- Router per node
- Host-Host Networking
- IPAM/ pod Network
- Network Policy
- Modes
  - ✓ Pure BGP
  - ✓ IP-IP encap



Source: https://platform9.com/blog/kubernetes-networking-achieving-high-performance-with-calico/

388

CALICO'S EBPF DATAPLANE

❖ eBPF 사용 (예): Calico Project

- Calico's eBPF dataplane

Factor	Standard Linux Dataplane	eBPF dataplane
Throughput	Designed for 10GBit+	Designed for 40GBit+
First packet latency	Low (kube-proxy service latency is bigger factor)	Lower
Subsequent packet latency	Low	Lower
Preserves source IP within cluster	Yes	Yes
Preserves external source IP	Only with externalTrafficPolicy: Local	Yes
Direct Server Return	Not supported	Supported (requires compatible underlying network)
Connection tracking	Linux kernel's conntrack table (size can be adjusted)	BPF map (fixed size)
Policy rules	Mapped to iptables rules	Mapped to BPF instructions
Policy selectors	Mapped to IP sets	Mapped to BPF maps
Kubernetes services	kube-proxy iptables or IPVS mode	BPF program and maps
IPIP	Supported	Supported (no performance advantage due to kernel limitations)
VXLAN	Supported	Supported
Wireguard	Supported (IPv4 and IPv6)	Supported (IPv4)
Other routing	Supported	Supported
Supports third party CNI plugins	Yes (compatible plugins only)	Yes (compatible plugins only)
Compatible with other iptables rules	Yes (can write rules above or below other rules)	Partial; iptables bypassed for workload traffic
Host endpoint policy	Supported	Supported
Enterprise version	Available	Available
XDP DoS Protection	Supported	Supported
IPv6	Supported	Not supported (yet)

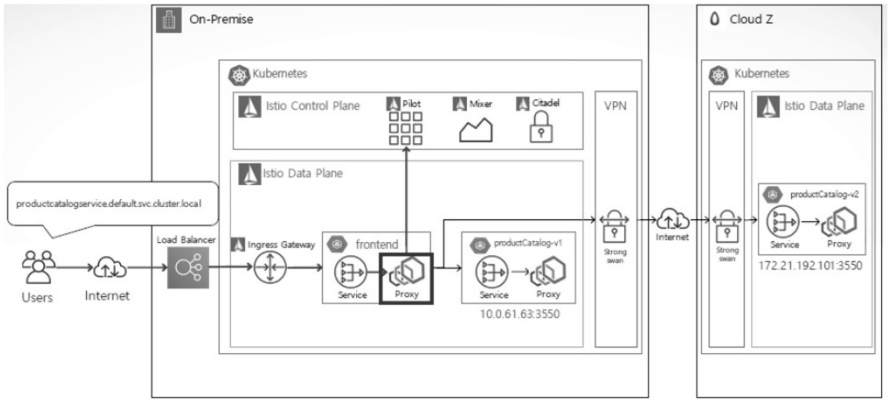
Source: https://projectcalico.docs.tigera.io/maintenance/ebpf/enabling-ebpf

389

HYBRID-CLOUD SERVICE MESH

❖ Hybrid-Cloud Service Mesh Architecture (예)

- Cross Cluster간 Service Mesh 연결/확장

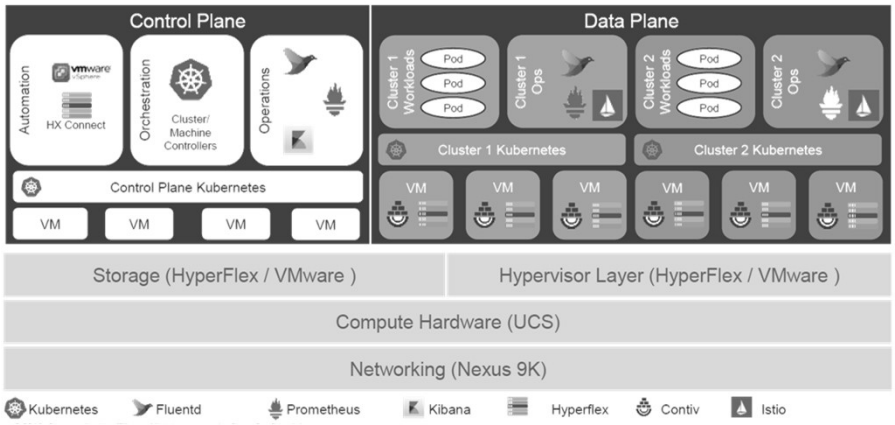


390

CISCO CONTAINER PLATFORM

❖ **Cisco Container Platform Architecture**

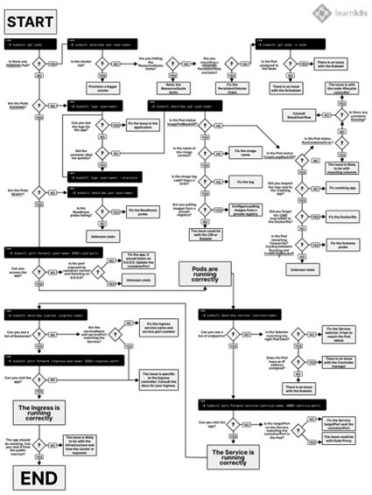
- **구성**: ACI, UCS, HCI
- **가상화 기반 클라우드 네이티브 서비스**



TROUBLESHOOTING

❖ **A visual guide on troubleshooting Kubernetes deployments**

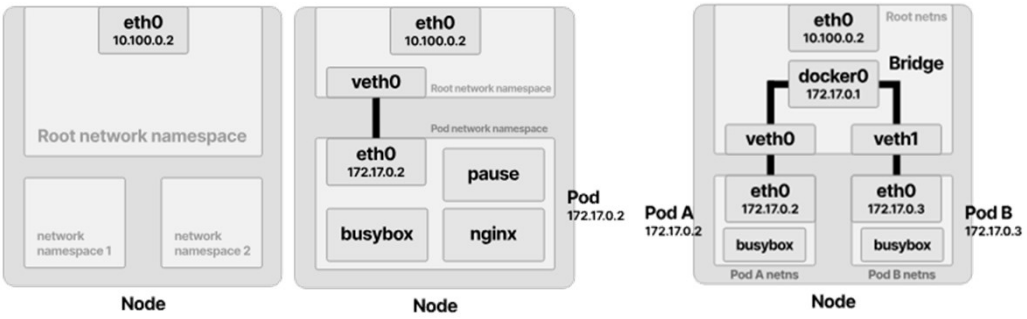
- **kubectl get pods**
- **kubectl describe pod <pod-name>**
- **kubectl log <pod-name>**
- **…**



Source: https://learnk8s.io/troubleshooting-deployments

TRACING NETWORK TRAFFIC

❖ **Tracing the path of network traffic in Kubernetes**



Source: https://learnk8s.io/troubleshooting-deployments

393

실습 교재 (별도)

394

395