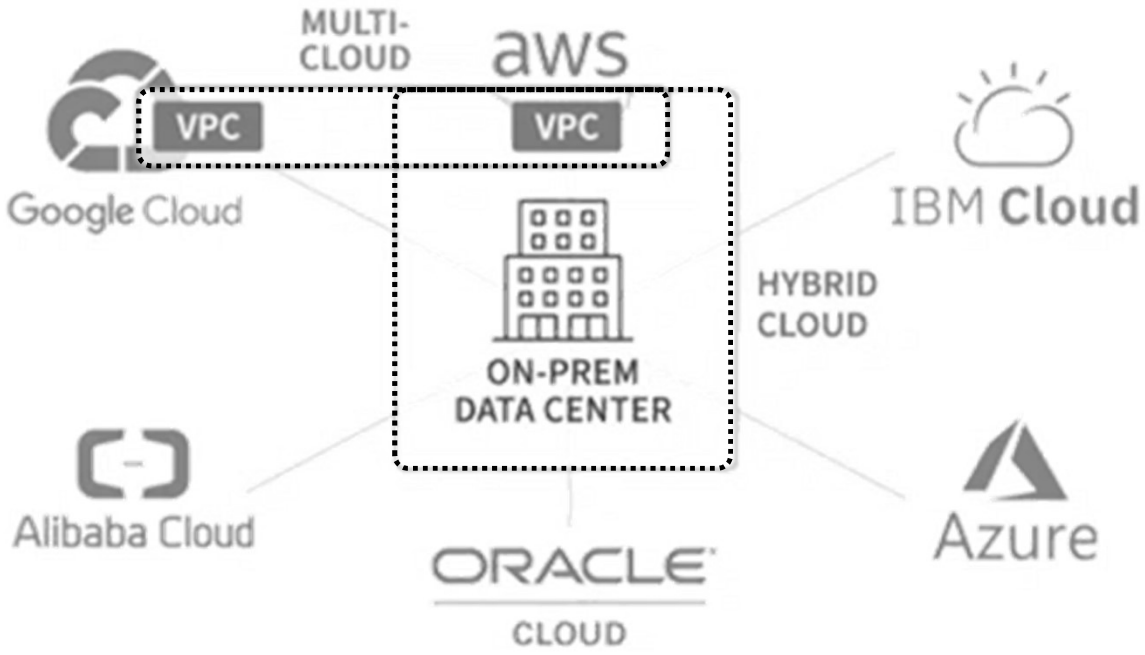
Day 3. 하이브리드와 멀티 클라우드

구분	주제	세부 내용
이론	Day 1 MCN 개요와 라우팅	• 멀티클라우드 개요 • 멀티클라우드를 위한 라우팅 (CSP, 오픈소스) • 라우팅 동작 • 라우팅 테이블
	Day 2 가상 네트워크 간의 연동	• CSP의 가상네트워크 구성 • Peering (가상 네트워크 연동) • Transit Gateway/Virtual WAN/VCN • 멀티 클라우드상의 가상 네트워크 연동
	Day 3 **하이브리드와 멀티 클라우드**	**• CSP/제조사 하이브리드 클라우드 솔루션** **• VPN(Virtual Private Network)** **• 전용선(Direct Connect / Express Route)** **• Cloud Hub**
이론/실습	Day 4 프라이빗 링크	• CSP의 프라이빗 링크 구성 • 서비스 엔드포인트(Endpoint) • 프라이빗 링크(Private Link) • 멀티클라우드 라우팅 구성 (실습)
	Day 5 멀티 클라우드 네트워킹	• 멀티클라우드 아키텍처 (CSP, 제조사) • 멀티클라우드 인프라 연동 • 멀티클라우드 인프라 관리 • 멀티클라우드 관리 플랫폼 (실습)

DAY 3. 하이브리드와 멀티 클라우드

❖ **Hybrid vs. Multi-cloud**



kentik

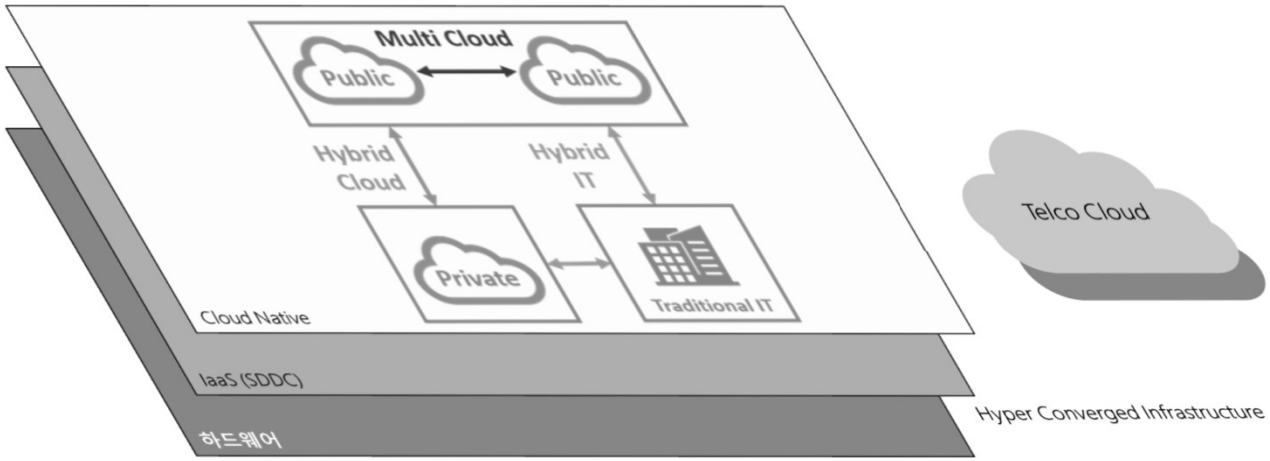
Source: https://www.kentik.com/blog/hybrid-vs-multi-cloud-the-good-the-bad-and-the-network-observability-needed/

DAY 3. 하이브리드와 멀티 클라우드

❖ 계층화 인프라

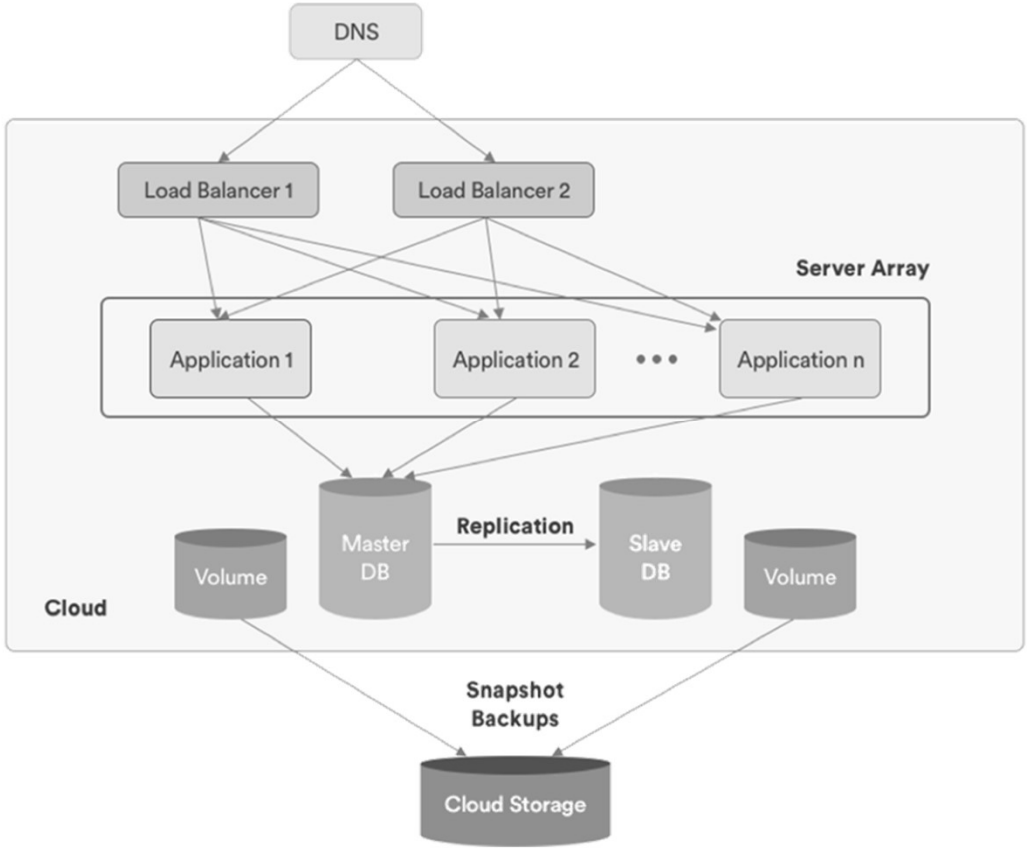
- 인프라의 계층별 추상화 (서비스에 집중)
- 계층간 격리와 정책 기반 서비스 노출
- 성능 개선 (계층 Offload 필요)
- 계층간 연결 호환성

- 제품화를 위한 영역과 계층 고려
- (Managed) Service 제품화 vs. Product 제품화



DAY 3. 하이브리드와 멀티 클라우드

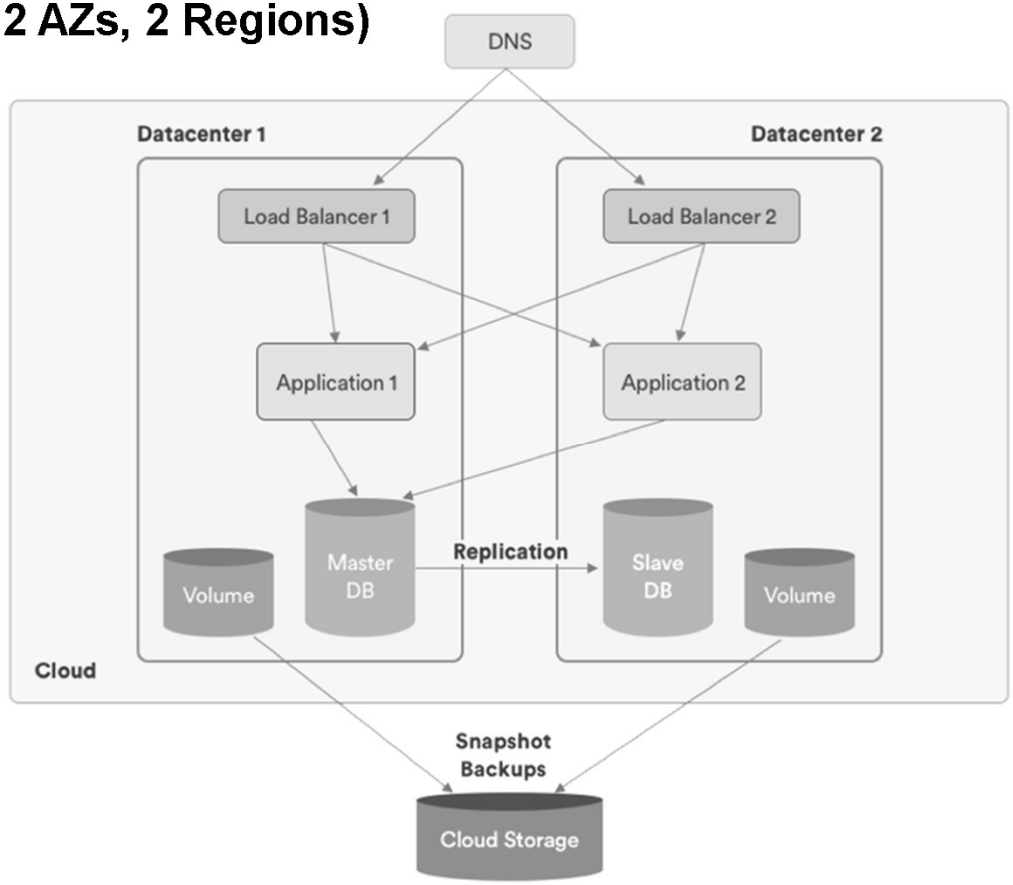
❖ Basic Cloud Architecture



Source: Rightscale

DAY 3. 하이브리드와 멀티 클라우드

❖ **Basic Cloud Architecture (2 Datacenters, 2 AZs, 2 Regions)**

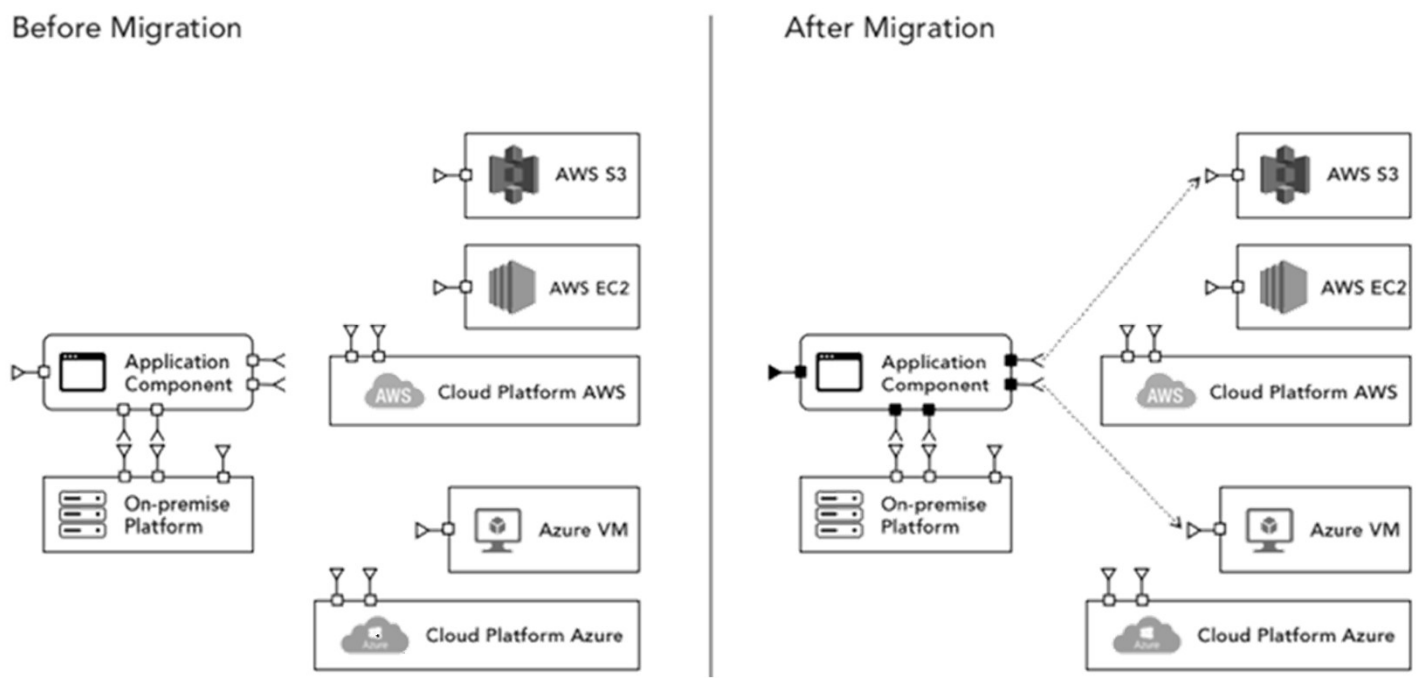


Source: Rightscale

DAY 3. 하이브리드와 멀티 클라우드

❖ 애플리케이션을 위한 Multi-Cloud Architecture

- 애플리케이션의 클라우드화 (Cloudification)

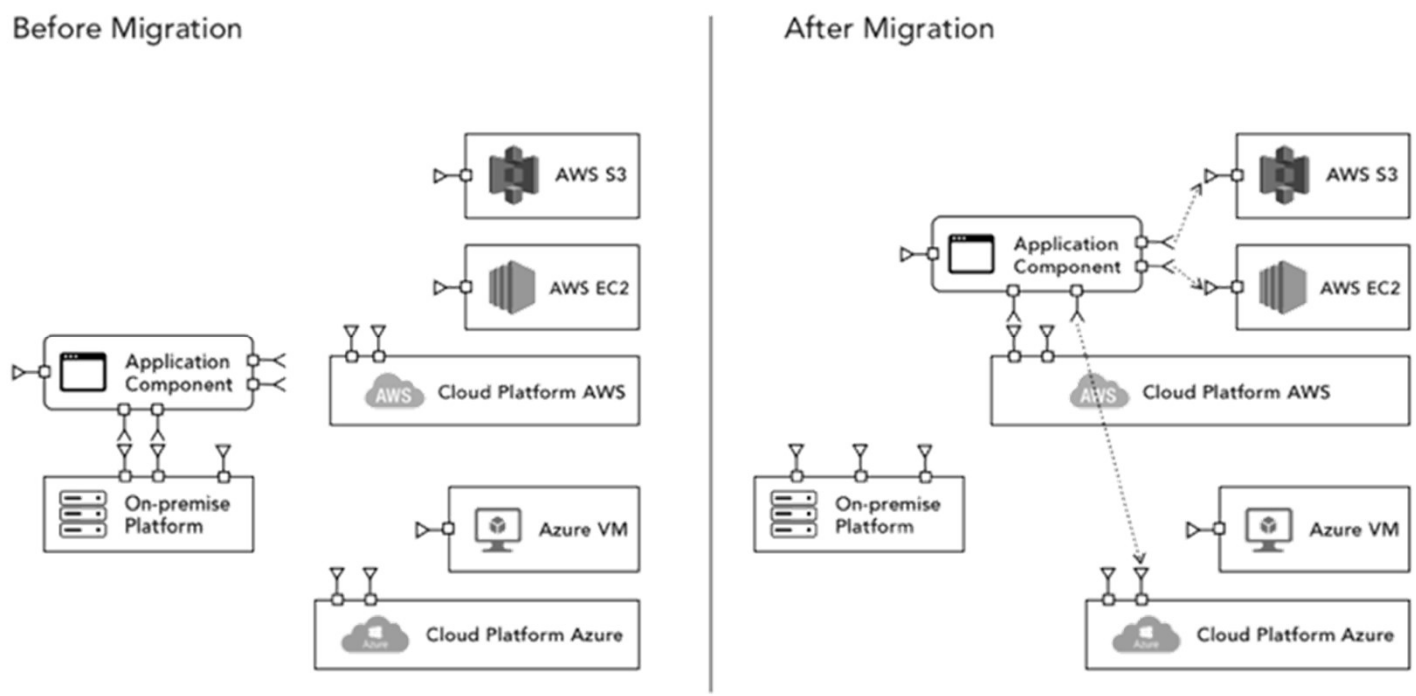


Source: Jignesh Solanki, leads Simform's Product Engineering team

DAY 3. 하이브리드와 멀티 클라우드

❖ 애플리케이션을 위한 Multi-Cloud Architecture

- 클라우드 이전 (Multi-Cloud Relocation)

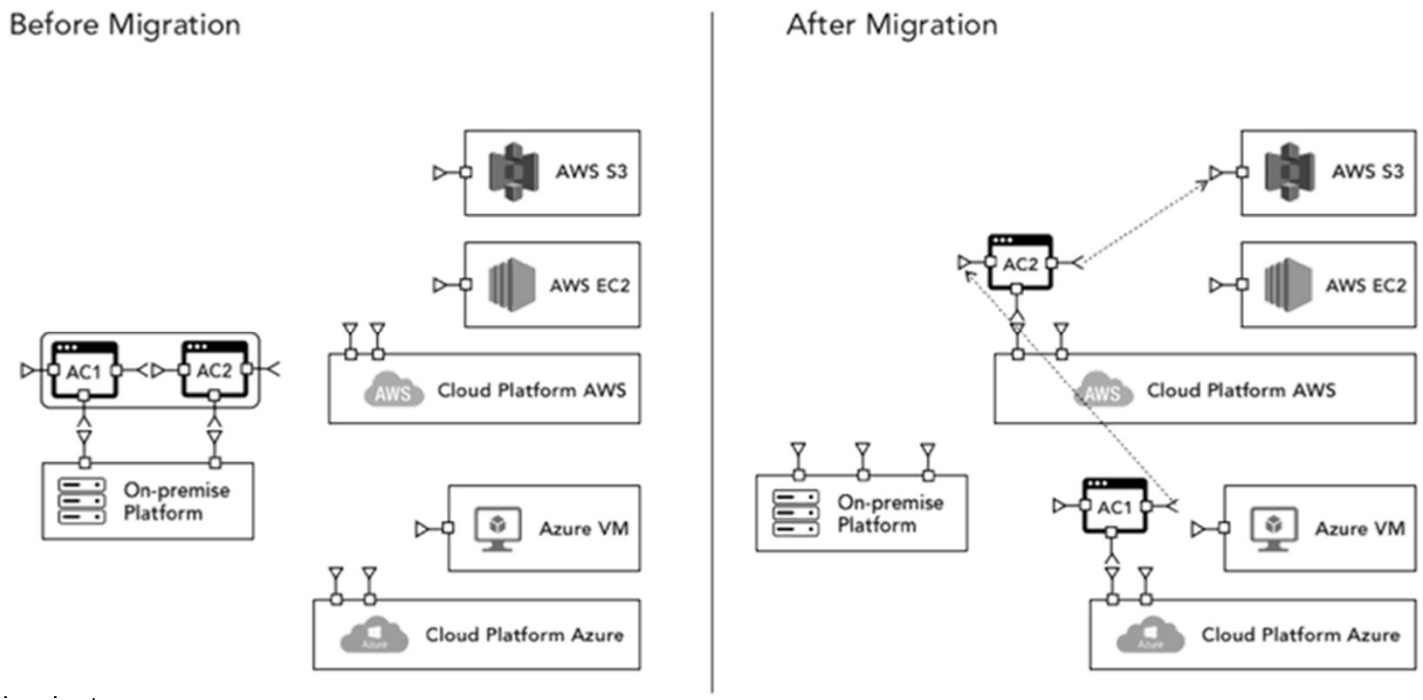


Source: Jignesh Solanki, leads Simform's Product Engineering team

DAY 3. 하이브리드와 멀티 클라우드

❖ 애플리케이션을 위한 Multi-Cloud Architecture

- 클라우드 이전 변환 (Multi-Cloud Refactor)

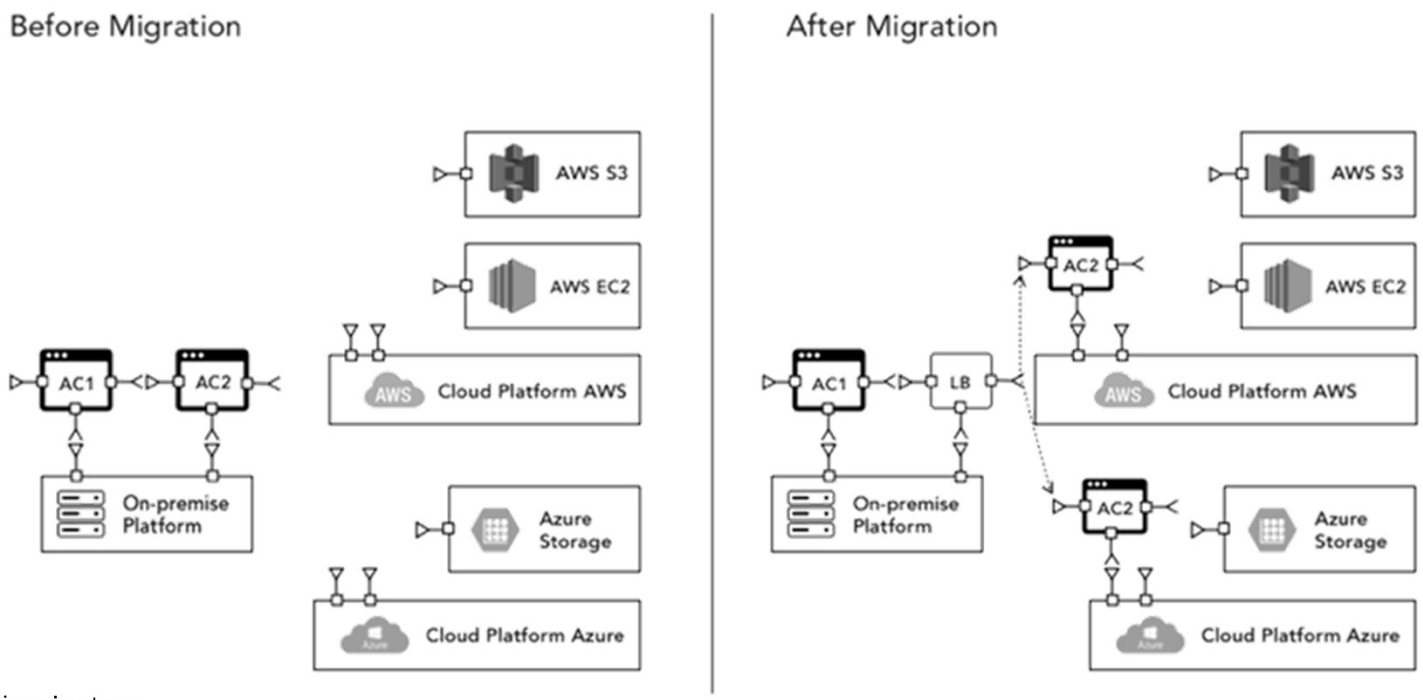


Source: Jignesh Solanki, leads Simform's Product Engineering team

DAY 3. 하이브리드와 멀티 클라우드

❖ 애플리케이션을 위한 Multi-Cloud Architecture

- 결합 (Multi-Cloud Rebinding)

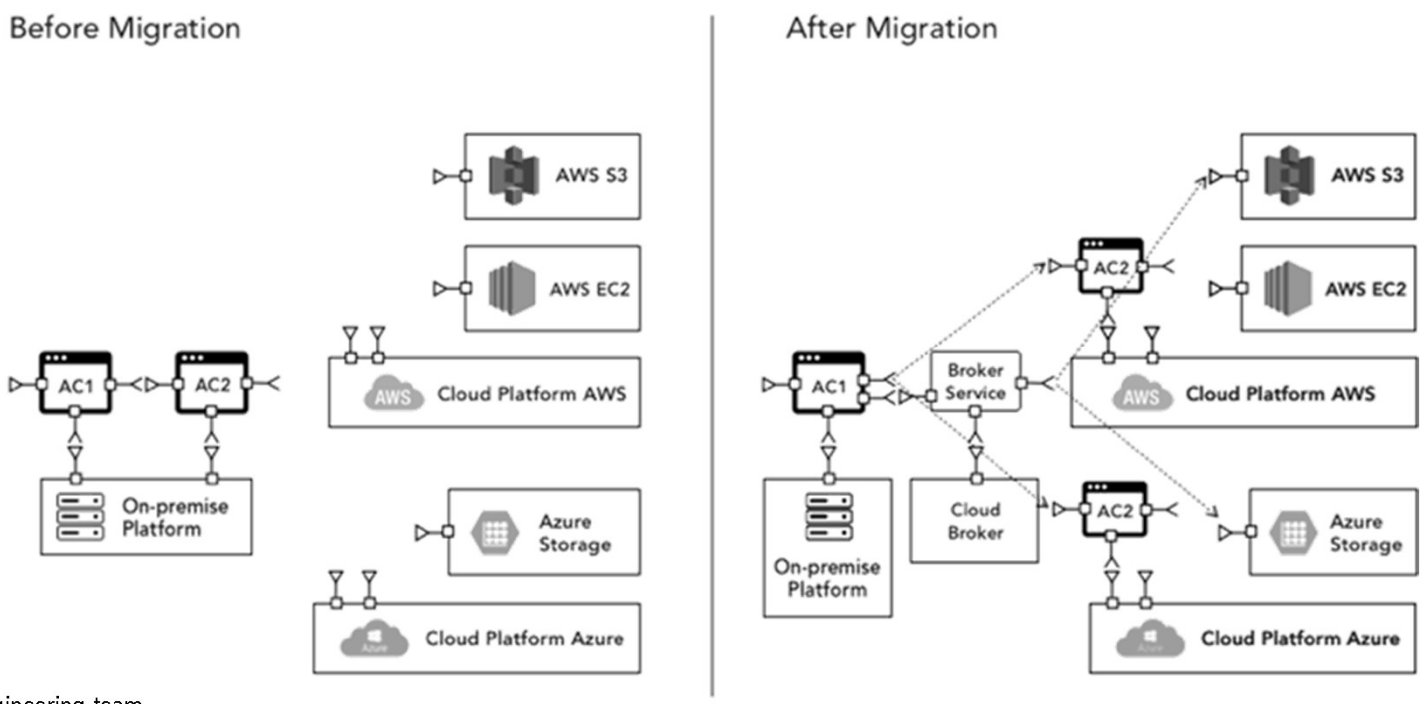


Source: Jignesh Solanki, leads Simform's Product Engineering team

DAY 3. 하이브리드와 멀티 클라우드

❖ 애플리케이션을 위한 Multi-Cloud Architecture

- **Multi-Cloud Rebinding with Cloud Brokerage**

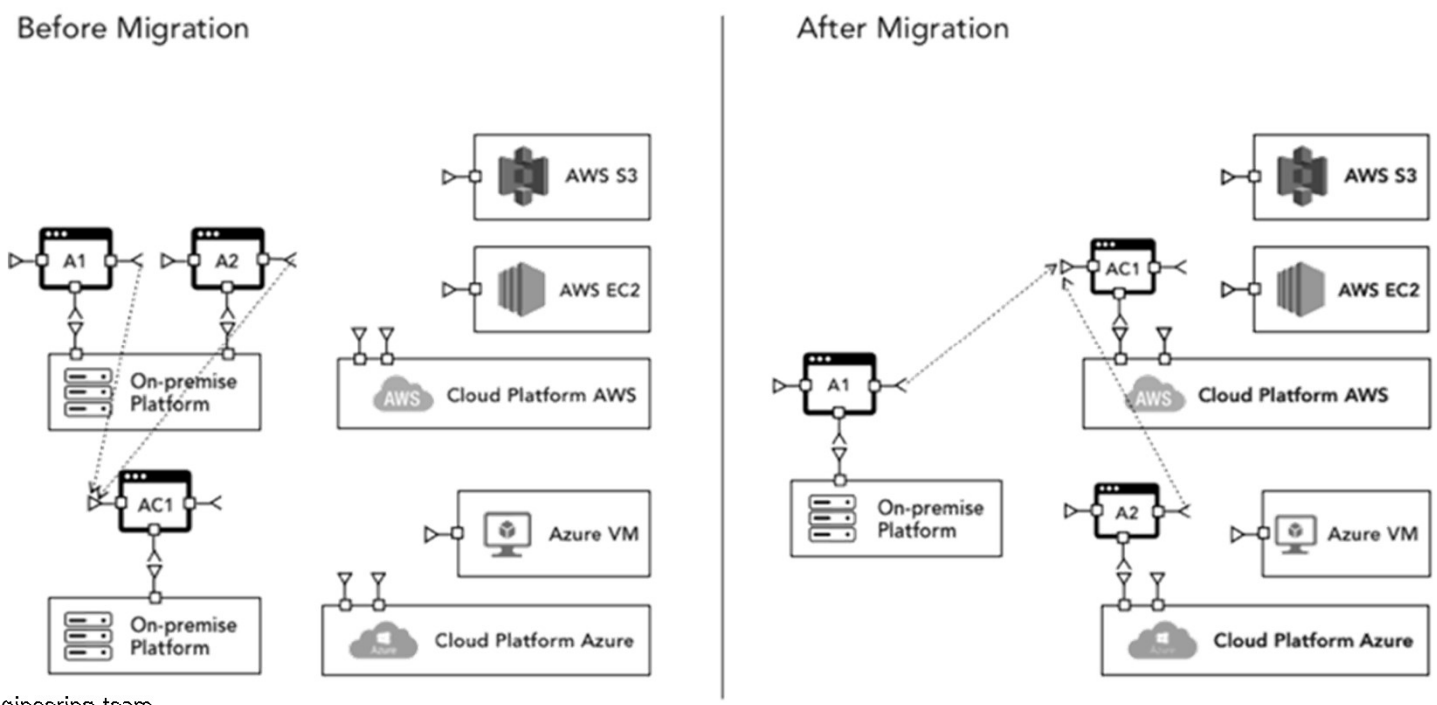


Source: Jignesh Solanki, leads Simform's Product Engineering team

DAY 3. 하이브리드와 멀티 클라우드

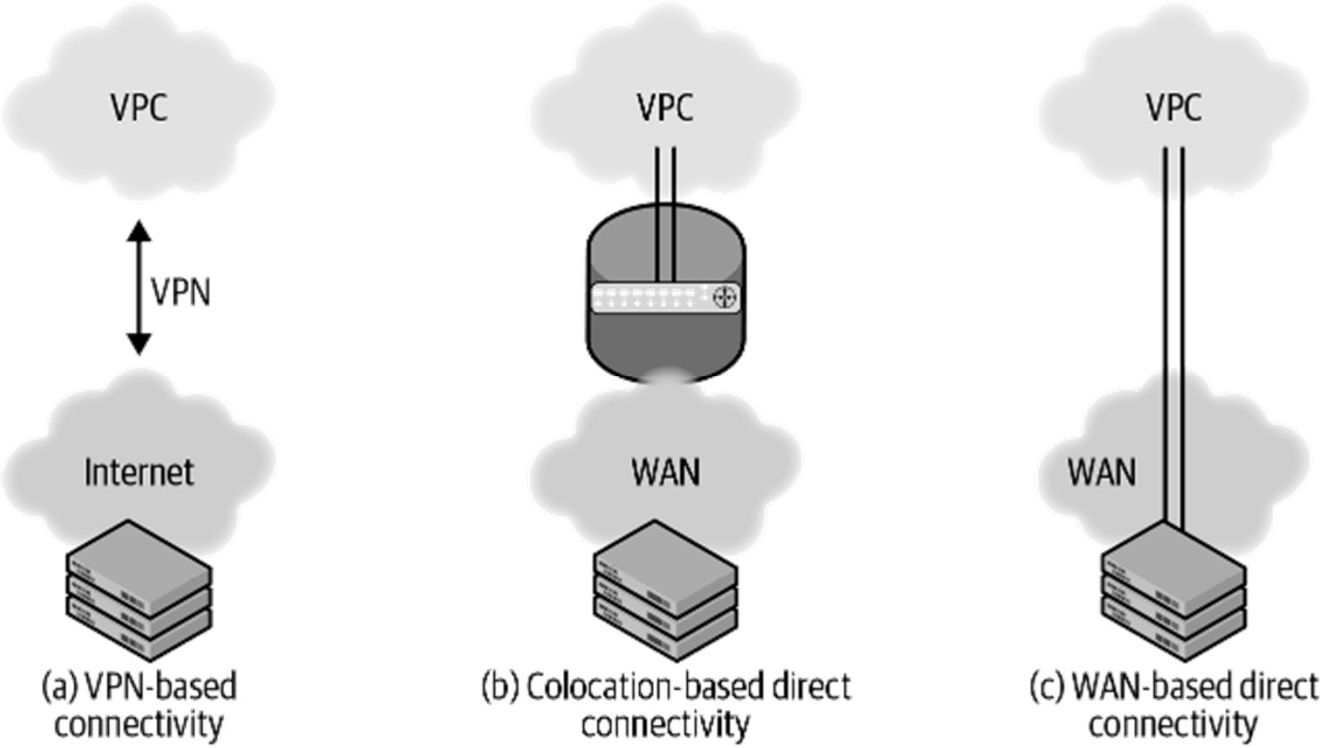
❖ 애플리케이션을 위한 Multi-Cloud Architecture

- 현대화 (Multi-Application Modernization)



Source: Jignesh Solanki, leads Simform's Product Engineering team

❖ Ways of connecting to a VPC

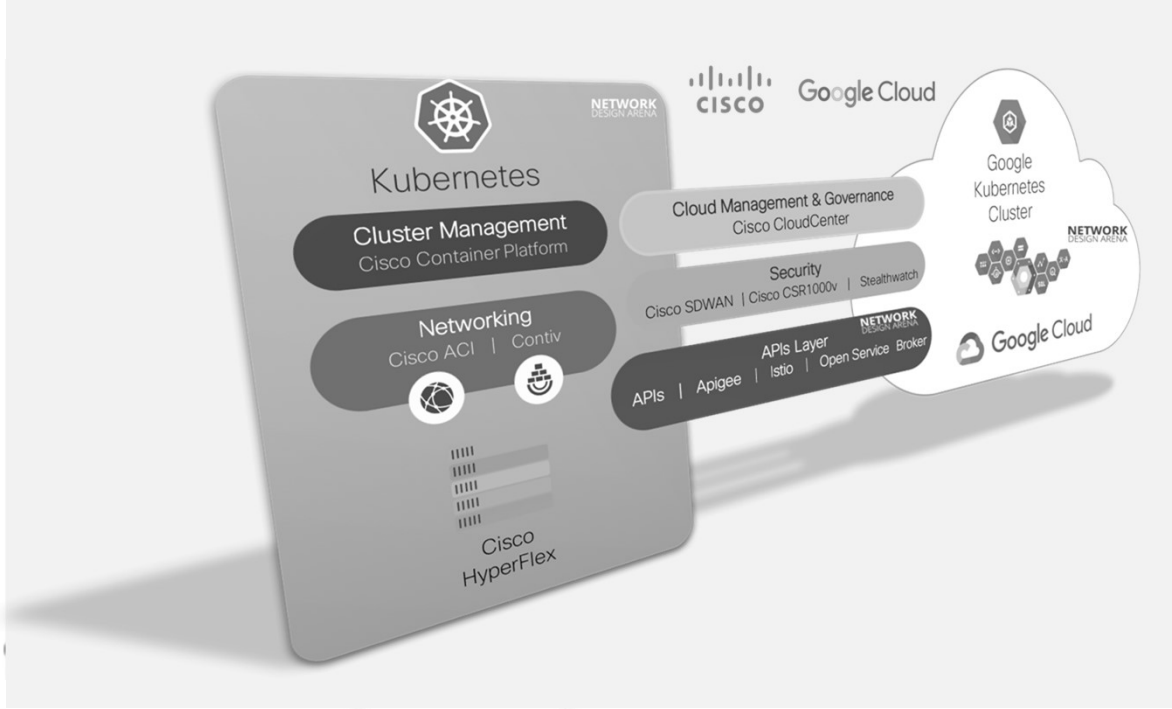


Source: Cloud Native Data Center Networking (Architecture, Protocols, and Tools), Dinesh G. Dutt, O'REILLY

DAY 3. 하이브리드와 멀티 클라우드

❖ 클라우드 서비스 / 제조사 협력 솔루션

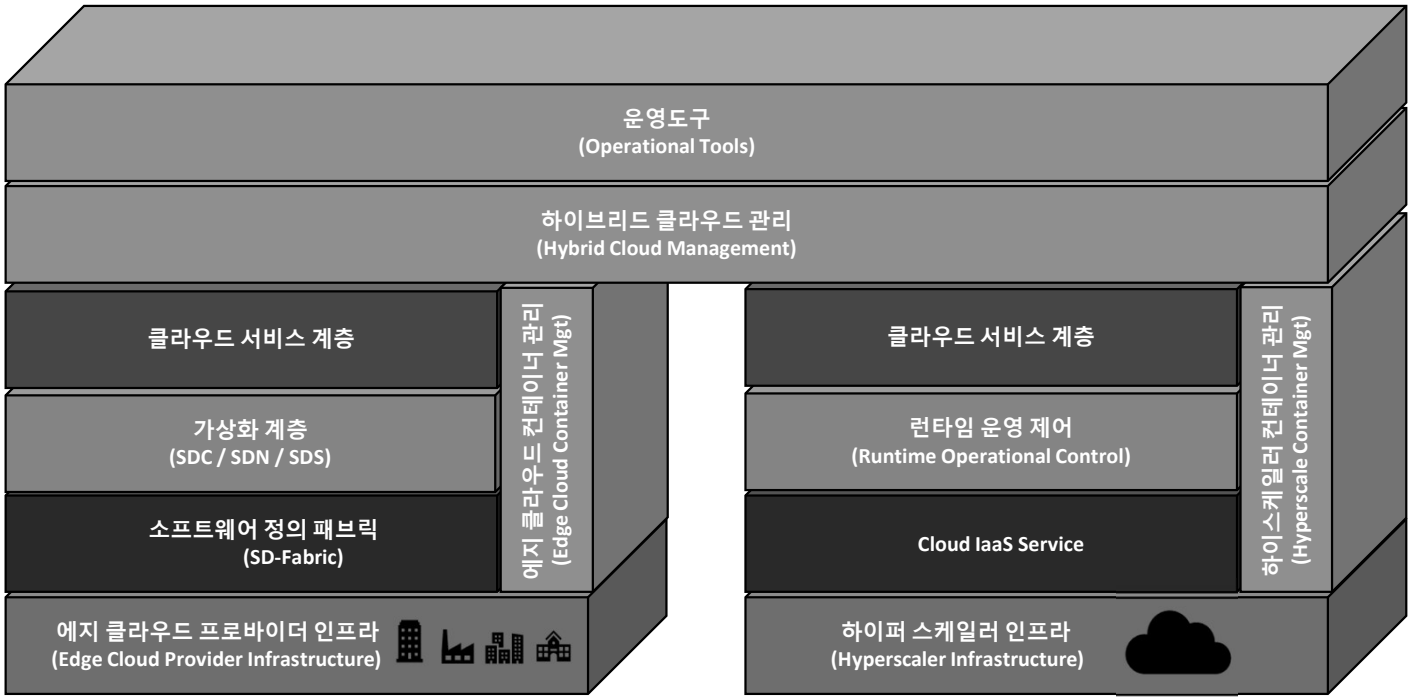
- 서비스/제조사간 협력 또는 인수를 통한 솔루션 확대
- 네트워킹 오픈소스 활용



Source: https://www.cisco.com/c/en/us/td/docs/dcn/whitepapers/cisco-cloud-aci-hybrid-multicloud-design-guide.html
Source: http://www.netdesignarena.com/index.php/2018/05/30/why-cisco-multi-cloud-a-cloud-architect-perspective/

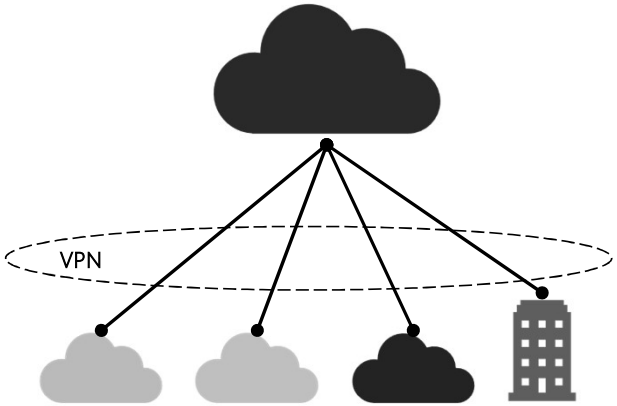
DAY 3. 하이브리드와 멀티 클라우드

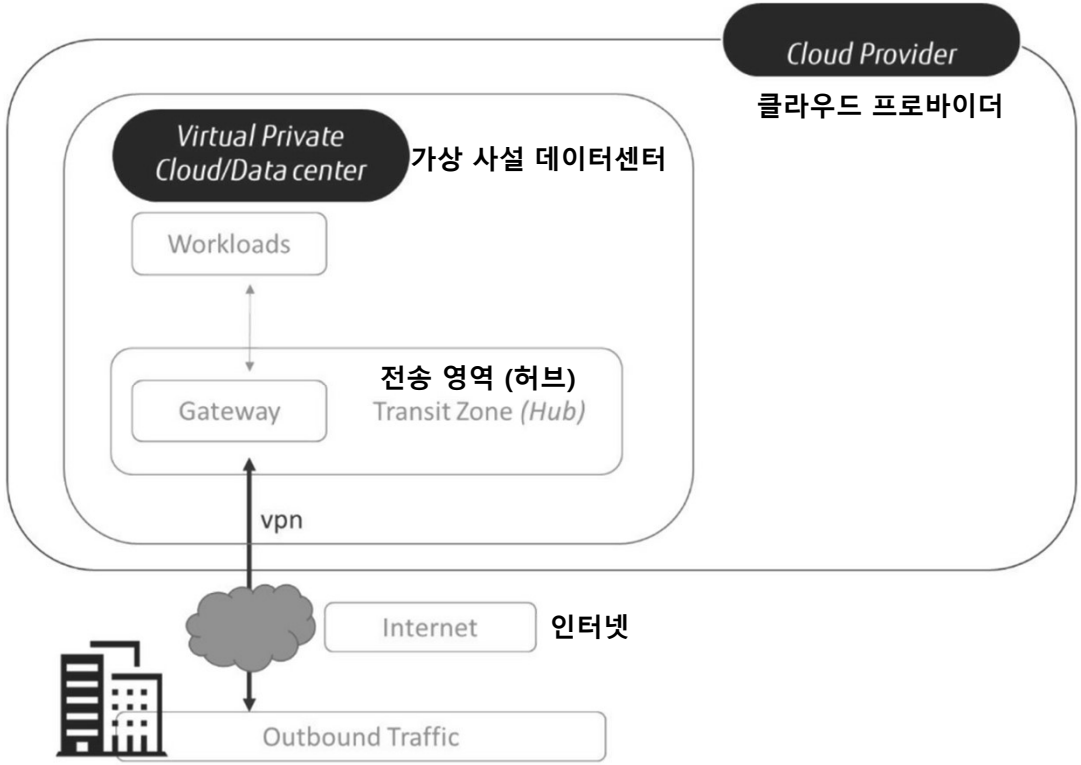
❖ 하이브리드 클라우드 아키텍처와 가상화 계층



DAY 3. 하이브리드와 멀티 클라우드

❖ The basic architecture of VPN connectivity



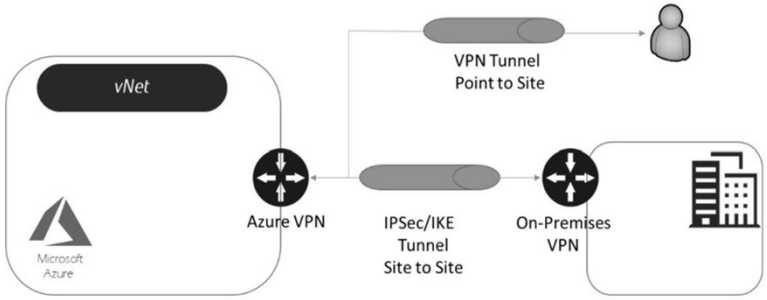


Source: Mulder, Jeroen. Multi-Cloud Architecture and Governance: Leverage Azure, AWS, GCP, and VMware vSphere to build effective multi-cloud solutions (p. 90). Packt Publishing. Kindle Edition.

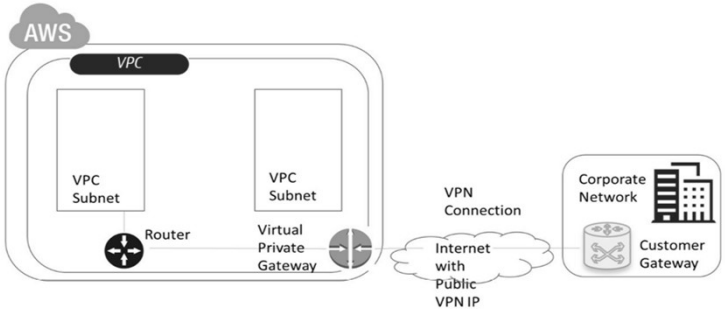
DAY 3. 하이브리드와 멀티 클라우드

❖ VPN의 멀티클라우드 접속 개념

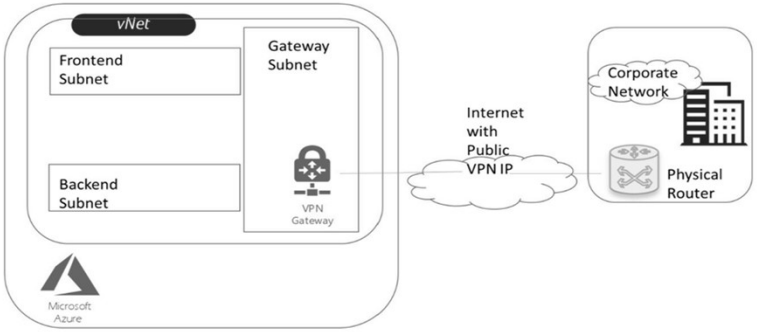
Point-to-site and site-to-site VPN setup in Azure



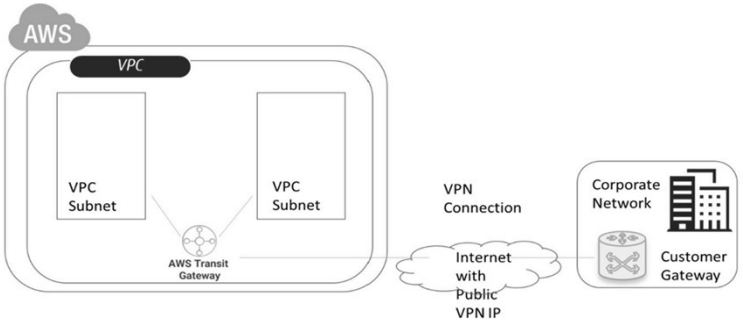
Design of a single site-to-site in AWS



Design of the VPN gateway in Azure



Design of a single site-to-site with AWS Transit Gateway



Source: Mulder, Jeroen. Multi-Cloud Architecture and Governance: Leverage Azure, AWS, GCP, and VMware vSphere to build effective multi-cloud solutions (p. 90). Packt Publishing. Kindle Edition.

❖ Site-to-site VPN (예): VyOS - IKEv1

- WAN interface on eth1
- left subnet: 192.168.0.0/24 site1, server side (i.e. locality, actually there is no client or server roles)
- left local_ip: 198.51.100.3 # server side WAN IP
- right subnet: 10.0.0.0/24 site2,remote office side
- right local_ip: 203.0.113.2 # remote office side WAN IP

left subnet: 192.168.0.0/24 site1, server side
left local_ip: 198.51.100.3 # server side WAN IP

```
# server config
set vpn ipsec esp-group office-srv-esp compression 'disable'
set vpn ipsec esp-group office-srv-esp lifetime '1800'
set vpn ipsec esp-group office-srv-esp mode 'tunnel'
set vpn ipsec esp-group office-srv-esp pfs 'enable'
set vpn ipsec esp-group office-srv-esp proposal 1 encryption 'aes256'
set vpn ipsec esp-group office-srv-esp proposal 1 hash 'sha1'
set vpn ipsec ike-group office-srv-ike ikev2-reauth 'no'
set vpn ipsec ike-group office-srv-ike key-exchange 'ikev1'
set vpn ipsec ike-group office-srv-ike lifetime '3600'
set vpn ipsec ike-group office-srv-ike proposal 1 encryption 'aes256'
set vpn ipsec ike-group office-srv-ike proposal 1 hash 'sha1'
set vpn ipsec ipsec-interfaces interface 'eth1'
set vpn ipsec site-to-site peer 203.0.113.2 authentication mode 'pre-shared-secret'
set vpn ipsec site-to-site peer 203.0.113.2 authentication pre-shared-secret 'SomePreSharedKey'
set vpn ipsec site-to-site peer 203.0.113.2 ike-group 'office-srv-ike'
set vpn ipsec site-to-site peer 203.0.113.2 local-address '198.51.100.3'
set vpn ipsec site-to-site peer 203.0.113.2 tunnel 0 allow-nat-networks 'disable'
set vpn ipsec site-to-site peer 203.0.113.2 tunnel 0 allow-public-networks 'disable'
set vpn ipsec site-to-site peer 203.0.113.2 tunnel 0 esp-group 'office-srv-esp'
set vpn ipsec site-to-site peer 203.0.113.2 tunnel 0 local prefix '192.168.0.0/24'
set vpn ipsec site-to-site peer 203.0.113.2 tunnel 0 remote prefix '10.0.0.0/21'
```

right subnet: 10.0.0.0/24 site2,remote office side
right local_ip: 203.0.113.2 # remote office side WAN IP

```
# remote office config
set vpn ipsec esp-group office-srv-esp compression 'disable'
set vpn ipsec esp-group office-srv-esp lifetime '1800'
set vpn ipsec esp-group office-srv-esp mode 'tunnel'
set vpn ipsec esp-group office-srv-esp pfs 'enable'
set vpn ipsec esp-group office-srv-esp proposal 1 encryption 'aes256'
set vpn ipsec esp-group office-srv-esp proposal 1 hash 'sha1'
set vpn ipsec ike-group office-srv-ike ikev2-reauth 'no'
set vpn ipsec ike-group office-srv-ike key-exchange 'ikev1'
set vpn ipsec ike-group office-srv-ike lifetime '3600'
set vpn ipsec ike-group office-srv-ike proposal 1 encryption 'aes256'
set vpn ipsec ike-group office-srv-ike proposal 1 hash 'sha1'
set vpn ipsec ipsec-interfaces interface 'eth1'
set vpn ipsec site-to-site peer 198.51.100.3 authentication mode 'pre-shared-secret'
set vpn ipsec site-to-site peer 198.51.100.3 authentication pre-shared-secret 'SomePreSharedKey'
set vpn ipsec site-to-site peer 198.51.100.3 ike-group 'office-srv-ike'
set vpn ipsec site-to-site peer 198.51.100.3 local-address '203.0.113.2'
set vpn ipsec site-to-site peer 198.51.100.3 tunnel 0 allow-nat-networks 'disable'
set vpn ipsec site-to-site peer 198.51.100.3 tunnel 0 allow-public-networks 'disable'
set vpn ipsec site-to-site peer 198.51.100.3 tunnel 0 esp-group 'office-srv-esp'
set vpn ipsec site-to-site peer 198.51.100.3 tunnel 0 local prefix '10.0.0.0/21'
set vpn ipsec site-to-site peer 198.51.100.3 tunnel 0 remote prefix '192.168.0.0/24'
```

Source: https://docs.vyos.io/en/equuleus/configuration/vpn/site2site_ipsec.html

DAY 3. 하이브리드와 멀티 클라우드

❖ Site-to-site VPN (예): VyOS - IKEv1

- WAN interface on eth1
- left subnet: 192.168.0.0/24 site1, server side (i.e. locality, actually there is no client or server roles)
- left local_ip: 198.51.100.3 # server side WAN IP
- right subnet: 10.0.0.0/24 site2,remote office side
- right local_ip: 203.0.113.2 # remote office side WAN IP
- Show status of new setup:
- If there is SNAT rules on eth1, need to add exclude rule

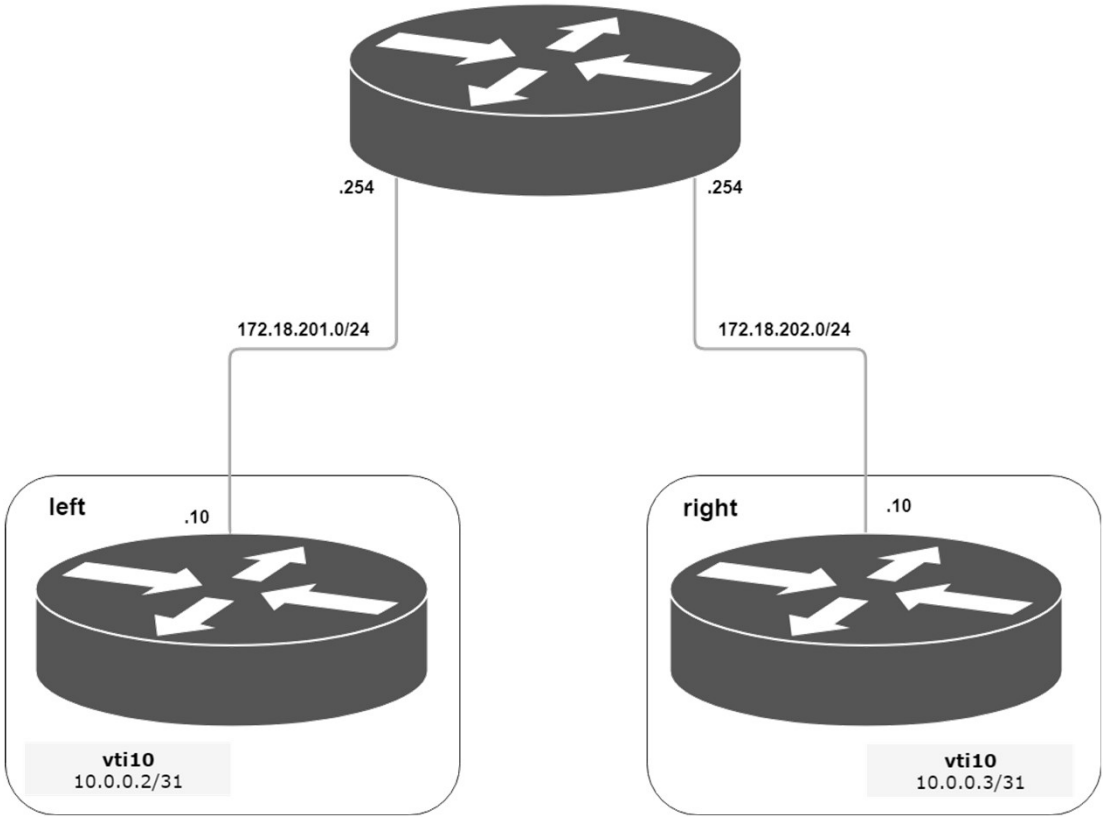
```
vyos@srv-gw0:~$ show vpn ike sa
Peer ID / IP                            Local ID / IP
------------                            -------------
203.0.113.2                                 198.51.100.3
   State  Encrypt  Hash    D-H Grp  NAT-T  A-Time  L-Time
   -----  -------  ----    -------  -----  ------  ------
   up     aes256   sha1    5        no     734     3600

vyos@srv-gw0:~$ show vpn ipsec sa
Peer ID / IP                            Local ID / IP
------------                            -------------
203.0.113.2                                 198.51.100.3
   Tunnel  State  Bytes Out/In   Encrypt  Hash    NAT-T  A-Time  L-Time  Proto
   ------  -----  -------------  -------  ----    -----  ------  ------  -----
   0       up     7.5M/230.6K    aes256   sha1    no     567     1800    all
```

```
# server side
set nat source rule 10 destination address '10.0.0.0/24'
set nat source rule 10 'exclude'
set nat source rule 10 outbound-interface 'eth1'
set nat source rule 10 source address '192.168.0.0/24'

# remote office side
set nat source rule 10 destination address '192.168.0.0/24'
set nat source rule 10 'exclude'
set nat source rule 10 outbound-interface 'eth1'
set nat source rule 10 source address '10.0.0.0/24'
```

Source: https://docs.vyos.io/en/equuleus/configuration/vpn/site2site_ipsec.html

DAY 3. 하이브리드와 멀티 클라우드

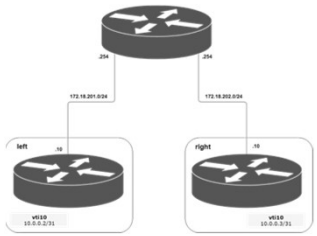
❖ Site-to-site VPN (예): VyOS - IKEv2



Source: https://docs.vyos.io/en/equuleus/configuration/vpn/site2site_ipsec.html

DAY 3. 하이브리드와 멀티 클라우드

❖ Site-to-site VPN (예): VyOS - IKEv2




```
set interfaces vti vti10 address '10.0.0.2/31'

set vpn ipsec esp-group ESP_DEFAULT compression 'disable'
set vpn ipsec esp-group ESP_DEFAULT lifetime '3600'
set vpn ipsec esp-group ESP_DEFAULT mode 'tunnel'
set vpn ipsec esp-group ESP_DEFAULT pfs 'dh-group19'
set vpn ipsec esp-group ESP_DEFAULT proposal 10 encryption 'aes256gcm128'
set vpn ipsec esp-group ESP_DEFAULT proposal 10 hash 'sha256'
set vpn ipsec ike-group IKEv2_DEFAULT dead-peer-detection action 'hold'
set vpn ipsec ike-group IKEv2_DEFAULT dead-peer-detection interval '30'
set vpn ipsec ike-group IKEv2_DEFAULT dead-peer-detection timeout '120'
set vpn ipsec ike-group IKEv2_DEFAULT ikev2-reauth 'no'
set vpn ipsec ike-group IKEv2_DEFAULT key-exchange 'ikev2'
set vpn ipsec ike-group IKEv2_DEFAULT lifetime '10800'
set vpn ipsec ike-group IKEv2_DEFAULT mobike 'disable'
set vpn ipsec ike-group IKEv2_DEFAULT proposal 10 dh-group '19'
set vpn ipsec ike-group IKEv2_DEFAULT proposal 10 encryption 'aes256gcm128'
set vpn ipsec ike-group IKEv2_DEFAULT proposal 10 hash 'sha256'
set vpn ipsec ipsec-interfaces interface 'eth0.201'
set vpn ipsec site-to-site peer 172.18.202.10 authentication id '172.18.201.10'
set vpn ipsec site-to-site peer 172.18.202.10 authentication mode 'pre-shared-secret'
set vpn ipsec site-to-site peer 172.18.202.10 authentication pre-shared-secret 'secretkey'
set vpn ipsec site-to-site peer 172.18.202.10 authentication remote-id '172.18.202.10'
set vpn ipsec site-to-site peer 172.18.202.10 connection-type 'initiate'
set vpn ipsec site-to-site peer 172.18.202.10 ike-group 'IKEv2_DEFAULT'
set vpn ipsec site-to-site peer 172.18.202.10 ikev2-reauth 'inherit'
set vpn ipsec site-to-site peer 172.18.202.10 local-address '172.18.201.10'
set vpn ipsec site-to-site peer 172.18.202.10 vti bind 'vti10'
set vpn ipsec site-to-site peer 172.18.202.10 vti esp-group 'ESP_DEFAULT'
```

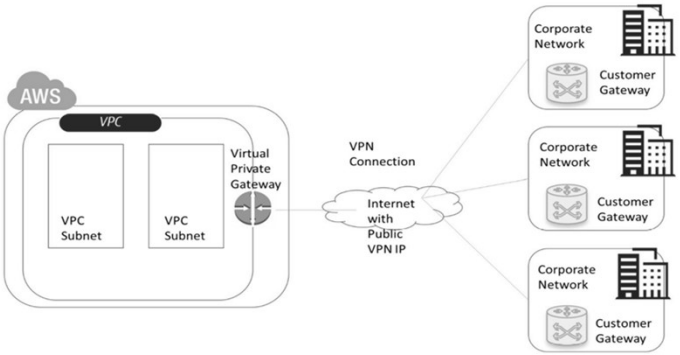
```
set interfaces vti vti10 address '10.0.0.3/31'

set vpn ipsec esp-group ESP_DEFAULT compression 'disable'
set vpn ipsec esp-group ESP_DEFAULT lifetime '3600'
set vpn ipsec esp-group ESP_DEFAULT mode 'tunnel'
set vpn ipsec esp-group ESP_DEFAULT pfs 'dh-group19'
set vpn ipsec esp-group ESP_DEFAULT proposal 10 encryption 'aes256gcm128'
set vpn ipsec esp-group ESP_DEFAULT proposal 10 hash 'sha256'
set vpn ipsec ike-group IKEv2_DEFAULT dead-peer-detection action 'hold'
set vpn ipsec ike-group IKEv2_DEFAULT dead-peer-detection interval '30'
set vpn ipsec ike-group IKEv2_DEFAULT dead-peer-detection timeout '120'
set vpn ipsec ike-group IKEv2_DEFAULT ikev2-reauth 'no'
set vpn ipsec ike-group IKEv2_DEFAULT key-exchange 'ikev2'
set vpn ipsec ike-group IKEv2_DEFAULT lifetime '10800'
set vpn ipsec ike-group IKEv2_DEFAULT mobike 'disable'
set vpn ipsec ike-group IKEv2_DEFAULT proposal 10 dh-group '19'
set vpn ipsec ike-group IKEv2_DEFAULT proposal 10 encryption 'aes256gcm128'
set vpn ipsec ike-group IKEv2_DEFAULT proposal 10 hash 'sha256'
set vpn ipsec ipsec-interfaces interface 'eth0.202'
set vpn ipsec site-to-site peer 172.18.201.10 authentication id '172.18.202.10'
set vpn ipsec site-to-site peer 172.18.201.10 authentication mode 'pre-shared-secret'
set vpn ipsec site-to-site peer 172.18.201.10 authentication pre-shared-secret 'secretkey'
set vpn ipsec site-to-site peer 172.18.201.10 authentication remote-id '172.18.201.10'
set vpn ipsec site-to-site peer 172.18.201.10 connection-type 'initiate'
set vpn ipsec site-to-site peer 172.18.201.10 ike-group 'IKEv2_DEFAULT'
set vpn ipsec site-to-site peer 172.18.201.10 ikev2-reauth 'inherit'
set vpn ipsec site-to-site peer 172.18.201.10 local-address '172.18.202.10'
set vpn ipsec site-to-site peer 172.18.201.10 vti bind 'vti10'
set vpn ipsec site-to-site peer 172.18.201.10 vti esp-group 'ESP_DEFAULT'
```

Source: https://docs.vyos.io/en/equuleus/configuration/vpn/site2site_ipsec.html

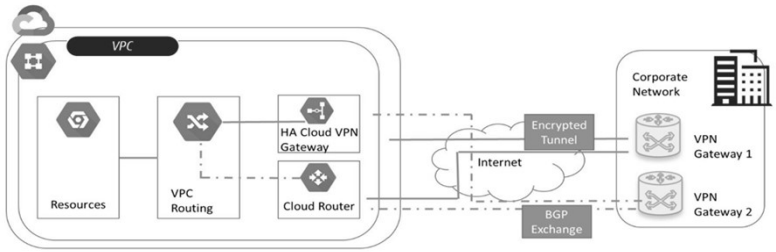
DAY 3. 하이브리드와 멀티 클라우드

❖ VPN의 멀티클라우드 접속 개념

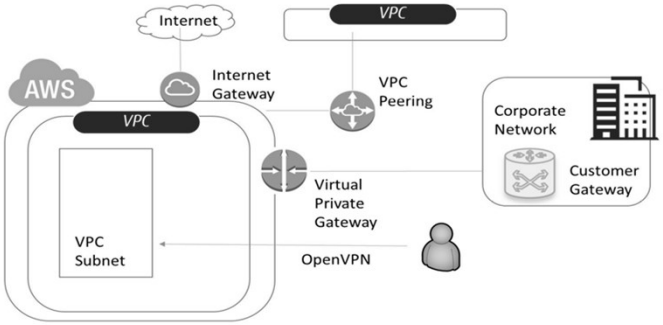
design of AWS CloudHub



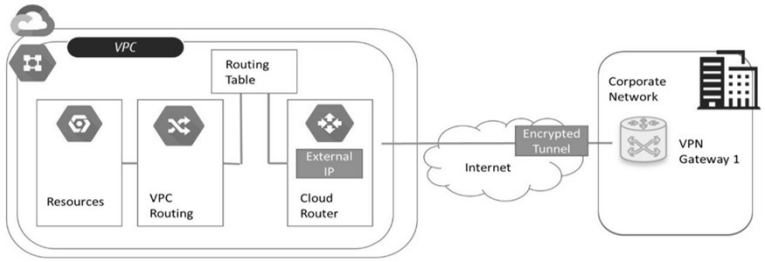
design of HA VPN in Google Cloud



design of AWS Client VPN



design of the Classic VPN gateway in Google Cloud

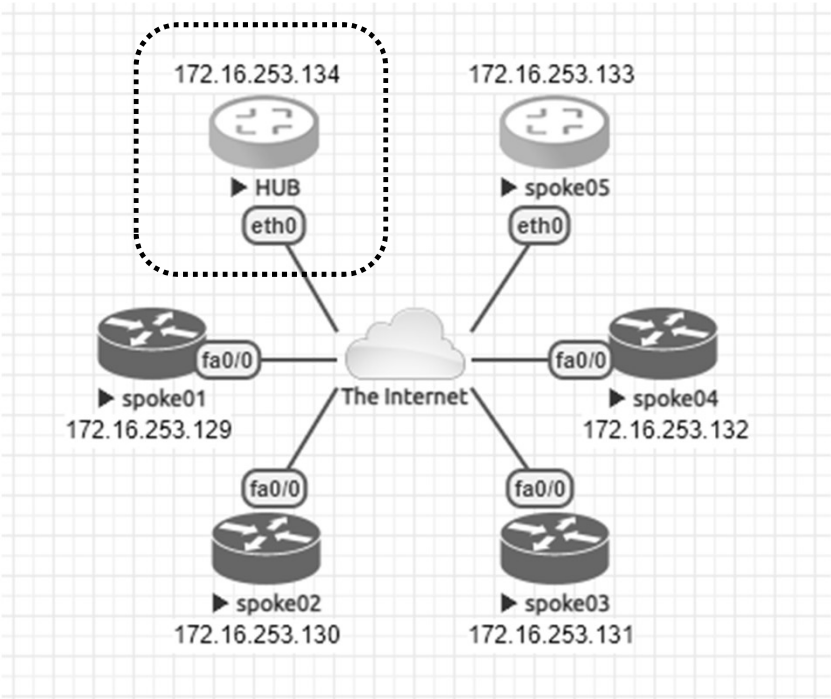


Source: Mulder, Jeroen. Multi-Cloud Architecture and Governance: Leverage Azure, AWS, GCP, and VMware vSphere to build effective multi-cloud solutions (p. 90). Packt Publishing. Kindle Edition.

DAY 3. 하이브리드와 멀티 클라우드

❖ Site-to-site VPN (예): VyOS – DMVPN (VyOS as multiple spoke sites)

- DMVPN Hub and Cisco (7206VXR) and VyOS



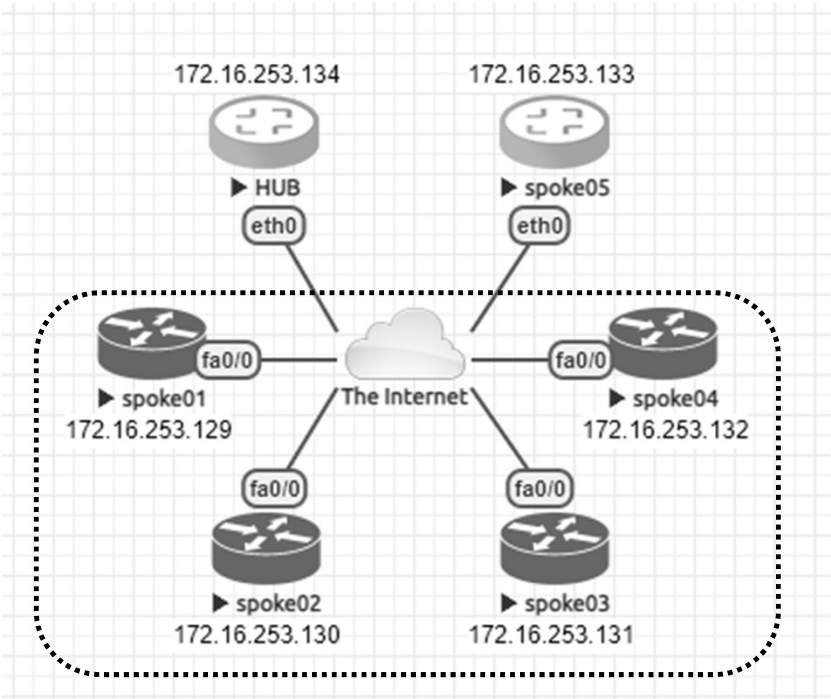

```
set interfaces ethernet eth0 address 192.0.2.1/24

set interfaces tunnel tun100 address '172.16.253.134/29'
set interfaces tunnel tun100 encapsulation 'gre'
set interfaces tunnel tun100 source-address '192.0.2.1'
set interfaces tunnel tun100 multicast 'enable'
set interfaces tunnel tun100 parameters ip key '1'

set protocols nhrp tunnel tun100 cisco-authentication 'secret'
set protocols nhrp tunnel tun100 holding-time '300'
set protocols nhrp tunnel tun100 multicast 'dynamic'
set protocols nhrp tunnel tun100 redirect
set protocols nhrp tunnel tun100 shortcut

set vpn ipsec esp-group ESP-HUB compression 'disable'
set vpn ipsec esp-group ESP-HUB lifetime '1800'
set vpn ipsec esp-group ESP-HUB mode 'transport'
set vpn ipsec esp-group ESP-HUB pfs 'dh-group2'
set vpn ipsec esp-group ESP-HUB proposal 1 encryption 'aes256'
set vpn ipsec esp-group ESP-HUB proposal 1 hash 'sha1'
set vpn ipsec esp-group ESP-HUB proposal 2 encryption '3des'
set vpn ipsec esp-group ESP-HUB proposal 2 hash 'md5'
set vpn ipsec ike-group IKE-HUB ikev2-reauth 'no'
set vpn ipsec ike-group IKE-HUB key-exchange 'ikev1'
set vpn ipsec ike-group IKE-HUB lifetime '3600'
set vpn ipsec ike-group IKE-HUB proposal 1 dh-group '2'
set vpn ipsec ike-group IKE-HUB proposal 1 encryption 'aes256'
set vpn ipsec ike-group IKE-HUB proposal 1 hash 'sha1'
set vpn ipsec ike-group IKE-HUB proposal 2 dh-group '2'
set vpn ipsec ike-group IKE-HUB proposal 2 encryption 'aes128'
set vpn ipsec ike-group IKE-HUB proposal 2 hash 'sha1'

set vpn ipsec ipsec-interfaces interface 'eth0'

set vpn ipsec profile NHRPVPN authentication mode 'pre-shared-secret'
set vpn ipsec profile NHRPVPN authentication pre-shared-secret 'secret'
set vpn ipsec profile NHRPVPN bind tunnel 'tun100'
set vpn ipsec profile NHRPVPN esp-group 'ESP-HUB'
set vpn ipsec profile NHRPVPN ike-group 'IKE-HUB'
```

Source: https://docs.vyos.io/en/equuleus/configuration/vpn/dmvpn.html

DAY 3. 하이브리드와 멀티 클라우드

❖ Site-to-site VPN (예): VyOS – DMVPN (VyOS as multiple spoke sites)

- DMVPN Hub and Cisco (7206VXR) and VyOS



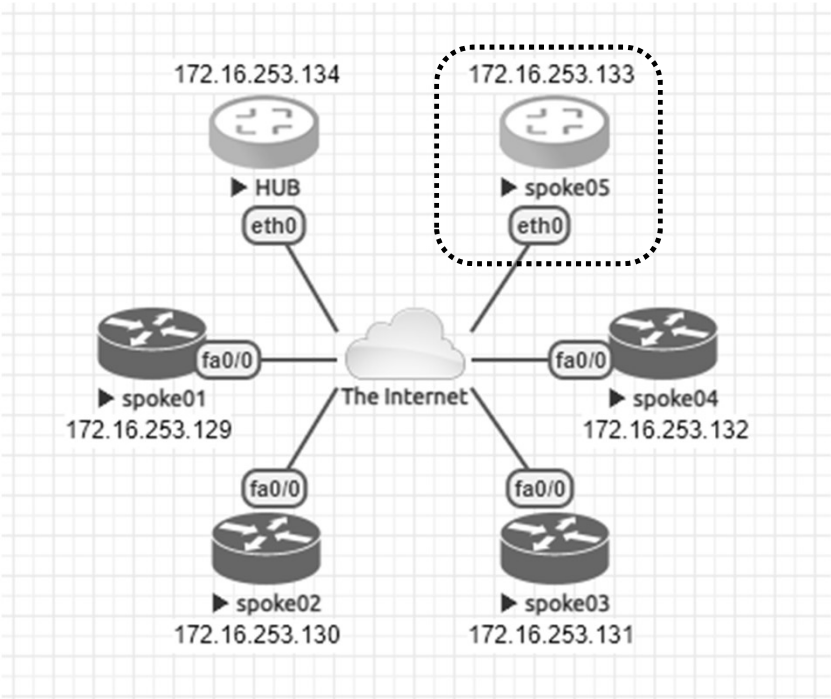

```
crypto keyring DMVPN
  pre-shared-key address 192.0.2.1 key secret
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp invalid-spi-recovery
crypto isakmp keepalive 30 30 periodic
crypto isakmp profile DMVPN
   keyring DMVPN
   match identity address 192.0.2.1 255.255.255.255
!
crypto ipsec transform-set DMVPN-AES256 esp-aes 256 esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN
 set security-association idle-time 720
 set transform-set DMVPN-AES256
 set isakmp-profile DMVPN
!
interface Tunnel10
 ! individual spoke tunnel IP must change
 ip address 172.16.253.129 255.255.255.248
 no ip redirects
 ip nhrp authentication secret
 ip nhrp map 172.16.253.134 192.0.2.1
 ip nhrp map multicast 192.0.2.1
 ip nhrp network-id 1
 ip nhrp holdtime 600
 ip nhrp nhs 172.16.253.134
 ip nhrp registration timeout 75
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN
 tunnel key 1
!
interface FastEthernet0/0
 ip address dhcp
 duplex half
```

Source: https://docs.vyos.io/en/equuleus/configuration/vpn/dmvpn.html

DAY 3. 하이브리드와 멀티 클라우드

❖ Site-to-site VPN (예): VyOS – DMVPN (VyOS as multiple spoke sites)

- DMVPN Hub and Cisco (7206VXR) and VyOS

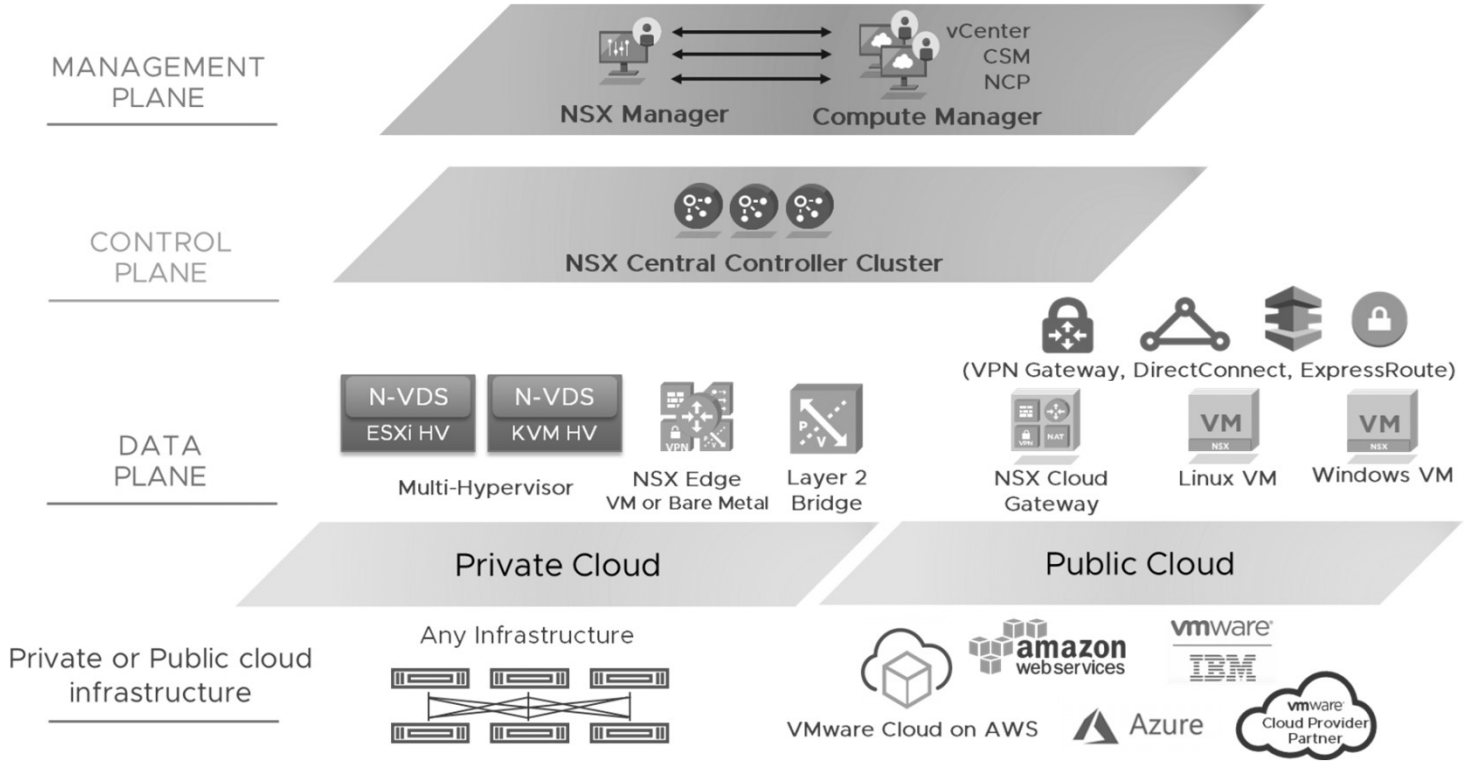



```
set interfaces ethernet eth0 address 'dhcp'

set interfaces tunnel tun100 address '172.16.253.133/29'
set interfaces tunnel tun100 source-address 0.0.0.0
set interfaces tunnel tun100 encapsulation 'gre'
set interfaces tunnel tun100 multicast 'enable'
set interfaces tunnel tun100 parameters ip key '1'

set protocols nhrp tunnel tun100 cisco-authentication 'secret'
set protocols nhrp tunnel tun100 holding-time '300'
set protocols nhrp tunnel tun100 map 172.16.253.134/29 nbma-address '192.0.2.1'
set protocols nhrp tunnel tun100 map 172.16.253.134/29 register
set protocols nhrp tunnel tun100 multicast 'nhs'
set protocols nhrp tunnel tun100 redirect
set protocols nhrp tunnel tun100 shortcut

set vpn ipsec esp-group ESP-HUB compression 'disable'
set vpn ipsec esp-group ESP-HUB lifetime '1800'
set vpn ipsec esp-group ESP-HUB mode 'transport'
set vpn ipsec esp-group ESP-HUB pfs 'dh-group2'
set vpn ipsec esp-group ESP-HUB proposal 1 encryption 'aes256'
set vpn ipsec esp-group ESP-HUB proposal 1 hash 'sha1'
set vpn ipsec esp-group ESP-HUB proposal 2 encryption '3des'
set vpn ipsec esp-group ESP-HUB proposal 2 hash 'md5'
set vpn ipsec ike-group IKE-HUB close-action 'none'
set vpn ipsec ike-group IKE-HUB ikev2-reauth 'no'
set vpn ipsec ike-group IKE-HUB key-exchange 'ikev1'
set vpn ipsec ike-group IKE-HUB lifetime '3600'
set vpn ipsec ike-group IKE-HUB proposal 1 dh-group '2'
set vpn ipsec ike-group IKE-HUB proposal 1 encryption 'aes256'
set vpn ipsec ike-group IKE-HUB proposal 1 hash 'sha1'
set vpn ipsec ike-group IKE-HUB proposal 2 dh-group '2'
set vpn ipsec ike-group IKE-HUB proposal 2 encryption 'aes128'
set vpn ipsec ike-group IKE-HUB proposal 2 hash 'sha1'

set vpn ipsec ipsec-interfaces interface 'eth0'

set vpn ipsec profile NHRPVPN authentication mode 'pre-shared-secret'
set vpn ipsec profile NHRPVPN authentication pre-shared-secret 'secret'
set vpn ipsec profile NHRPVPN bind tunnel 'tun100'
set vpn ipsec profile NHRPVPN esp-group 'ESP-HUB'
set vpn ipsec profile NHRPVPN ike-group 'IKE-HUB'
```

Source: https://docs.vyos.io/en/equuleus/configuration/vpn/dmvpn.html

DAY 3. 하이브리드와 멀티 클라우드

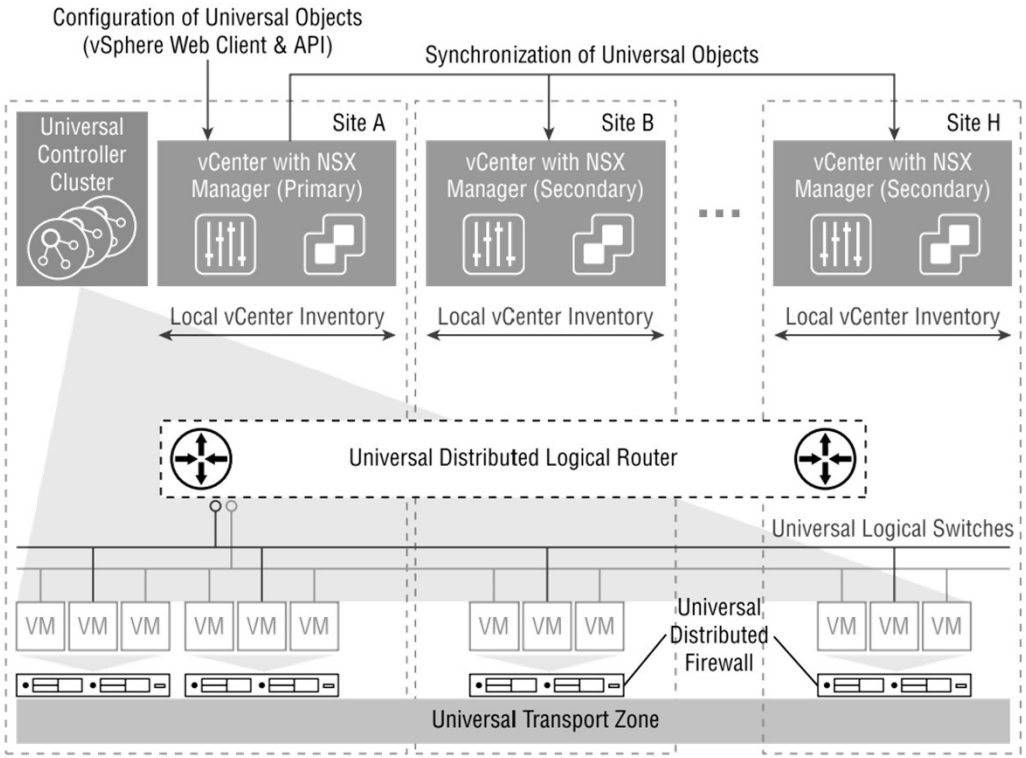
❖ NSX Data Center Architecture for Private Cloud, Public Cloud



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

DAY 3. 하이브리드와 멀티 클라우드

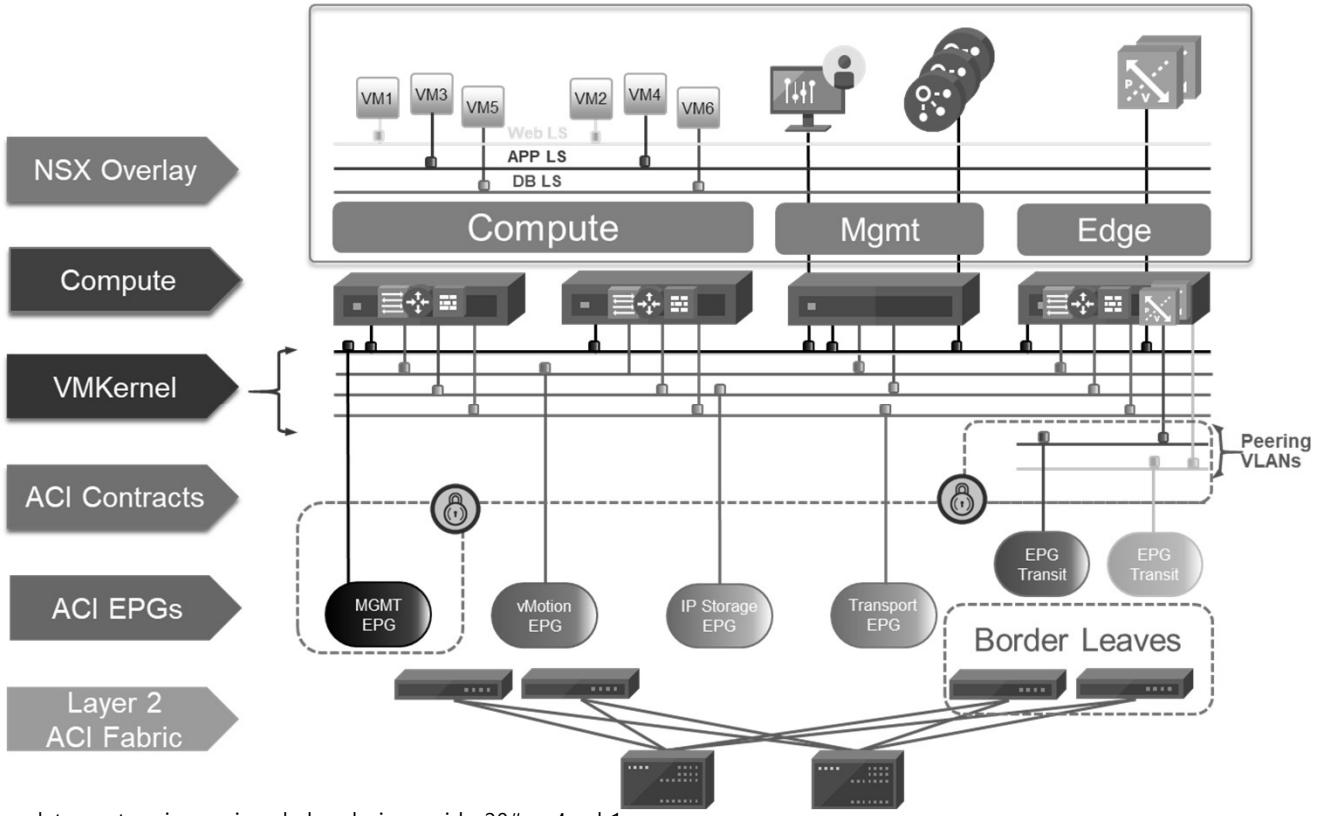
❖ 제조사(예): Cross-vCenter design spanning multiple sites



Source: Mastering VMware NSX® for vSphere®, Elver Sena Sosa, John Wiley & Sons, Inc., Indianapolis, Indiana (2020)

DAY 3. 하이브리드와 멀티 클라우드

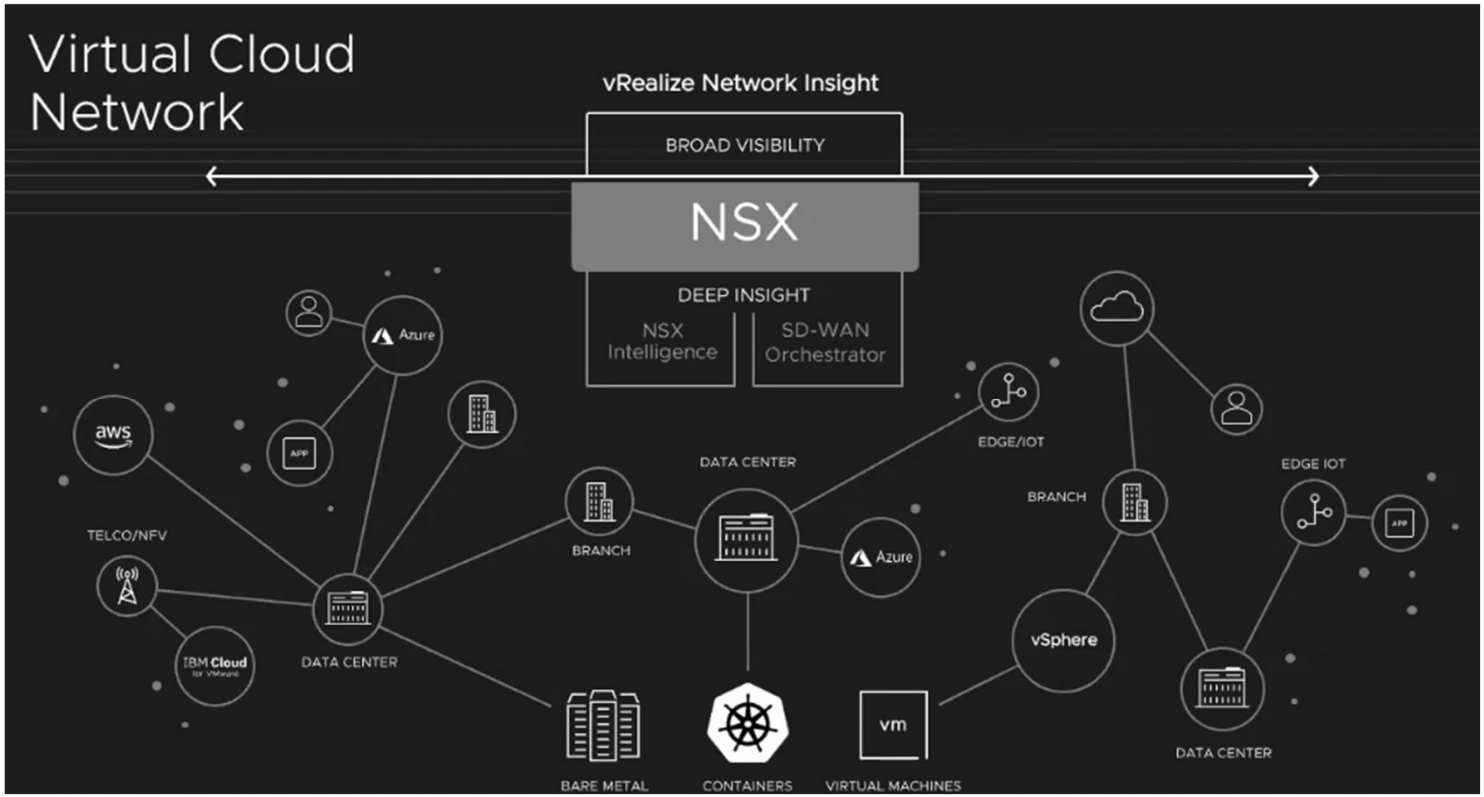
❖ NSX Data Center Deployed on an ACI Underlay



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

DAY 3. 하이브리드와 멀티 클라우드

❖ VMware Virtual Cloud Network (VCN)

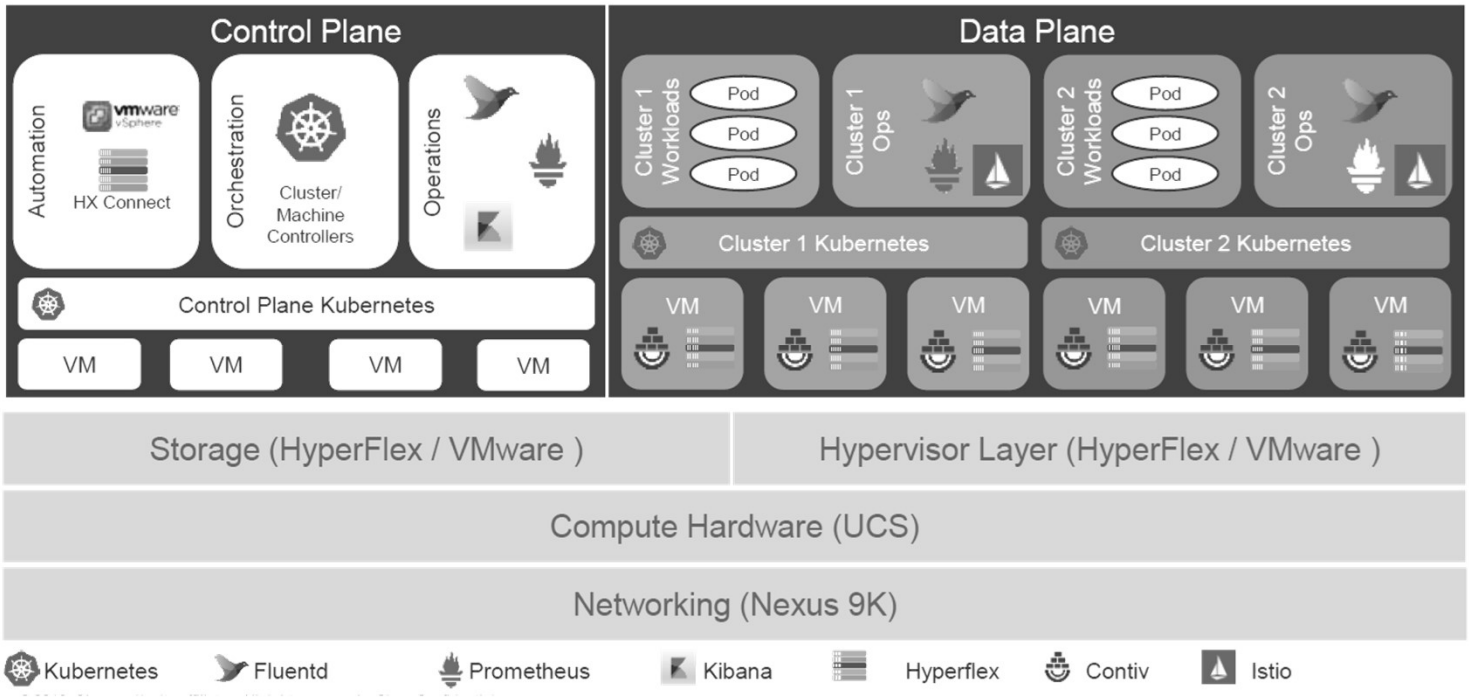


Source: https://www.nextplatform.com/2020/04/08/following-the-network-to-the-cloud-and-edge/

DAY 3. 하이브리드와 멀티 클라우드

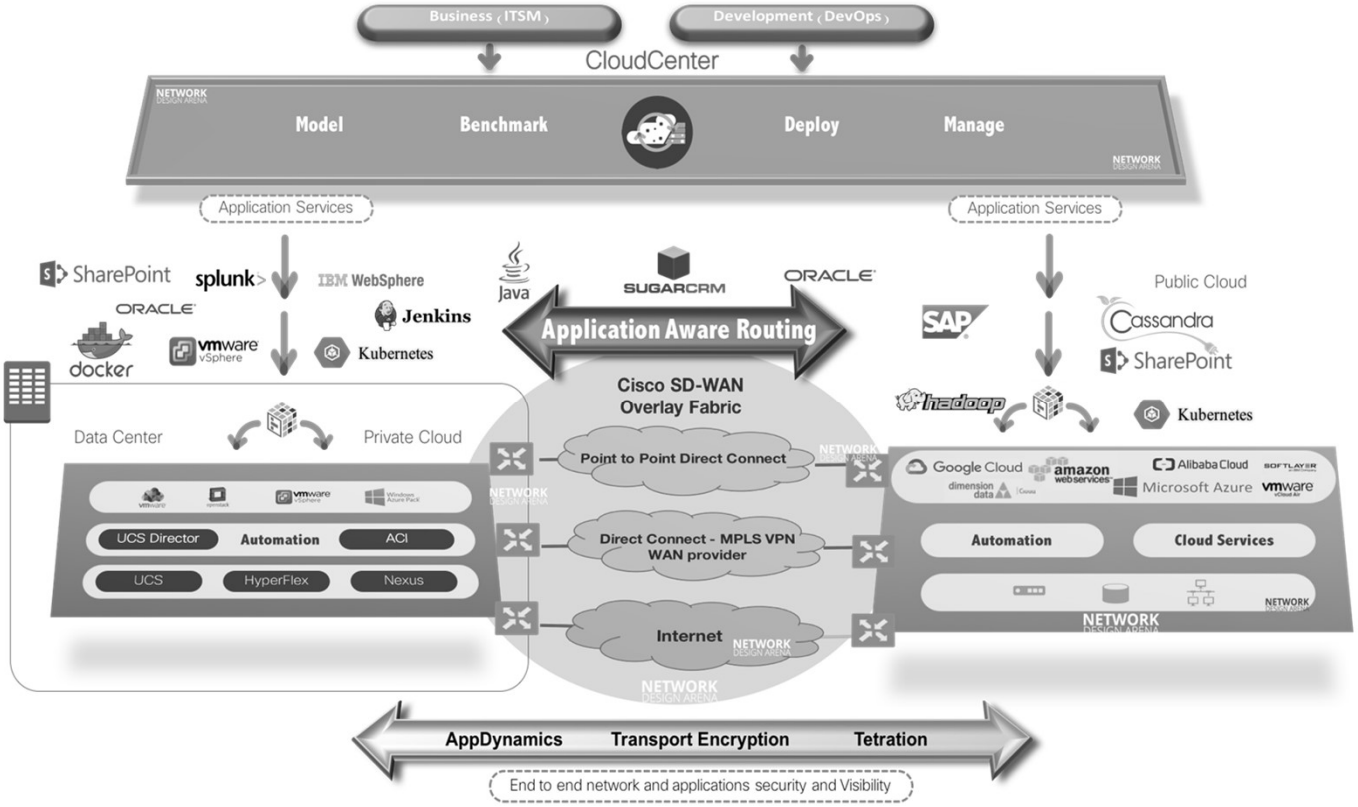
❖ Cisco Container Platform Architecture

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



DAY 3. 하이브리드와 멀티 클라우드

❖ 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/

DAY 3. 하이브리드와 멀티 클라우드

- **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 (*)

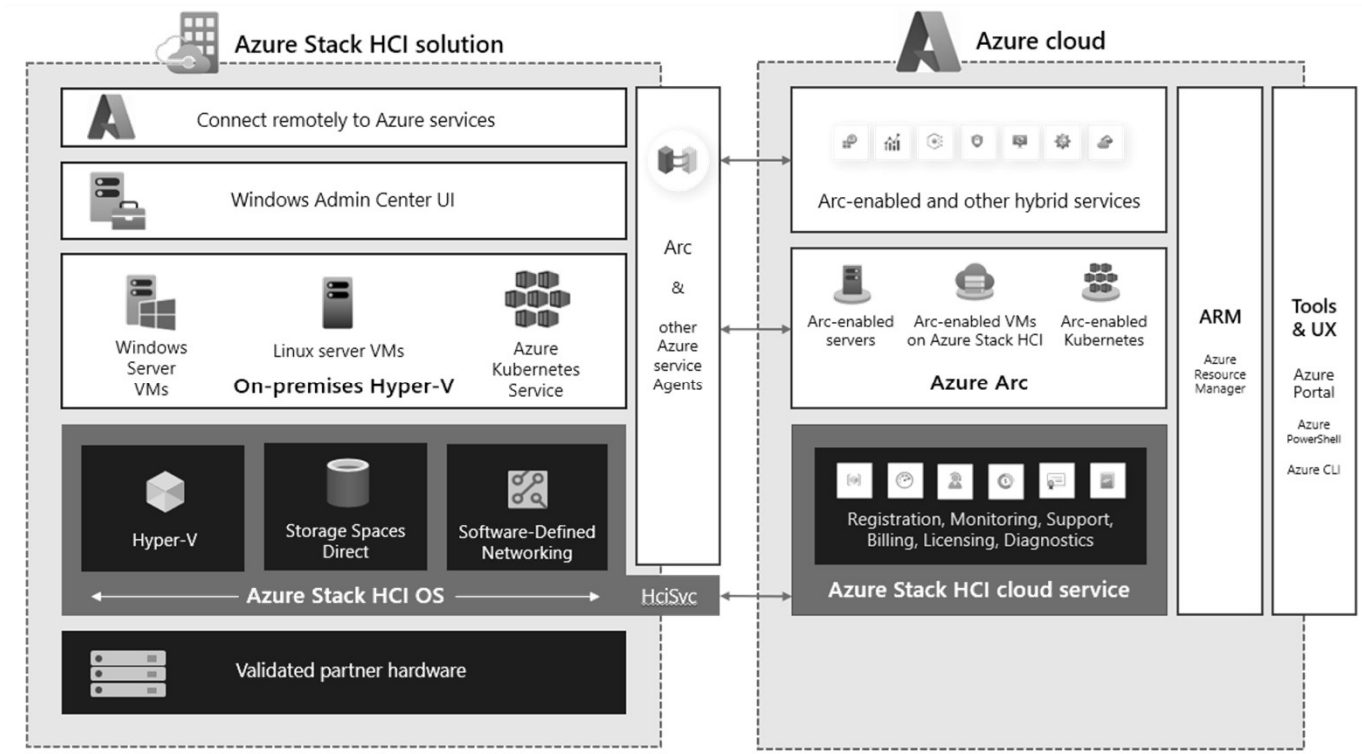
- **Layer 4**
  - Reconnaissance
  - DoS protection (ICMP, UDP, TCP flood)
    - Rate limiting
- **Layer 3**
  - ARP, IP ICMP protocol defence
  - IP spoofing
  - Strict source routing checks
  - Fragment overlaps

VERSA NETWORKS

Source: Versa Networks, SDxCentral

DAY 3. 하이브리드와 멀티 클라우드

❖Azure Stack HCI hybrid capabilities with Azure services



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

❖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

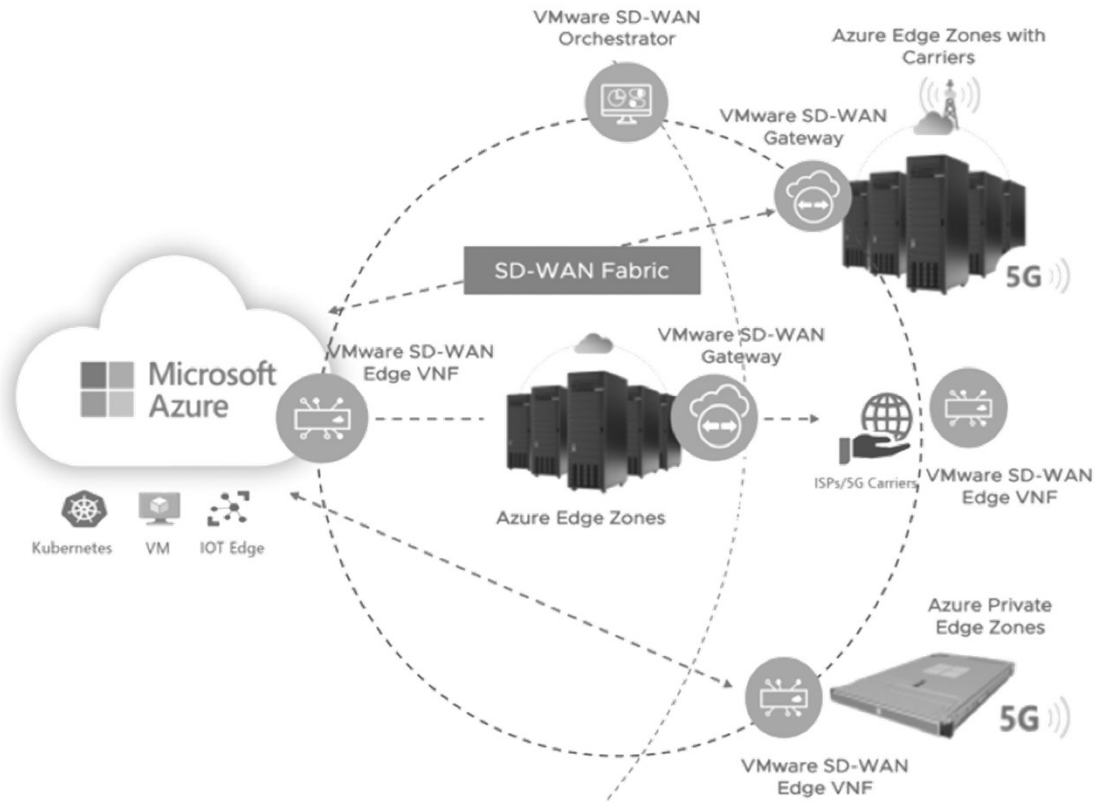
Source: https://azure.microsoft.com/en-us/pricing/details/azure-stack/edge/#pricing

DAY 3. 하이브리드와 멀티 클라우드

❖Use Case: Azure Edge Zone

❖VMware / Microsoft 협력

- VMware SD-WAN VNF
- Azure Edge Zones
- Zero Touch Provisioning (ZTP)
- single SD-WAN Orchestrator.

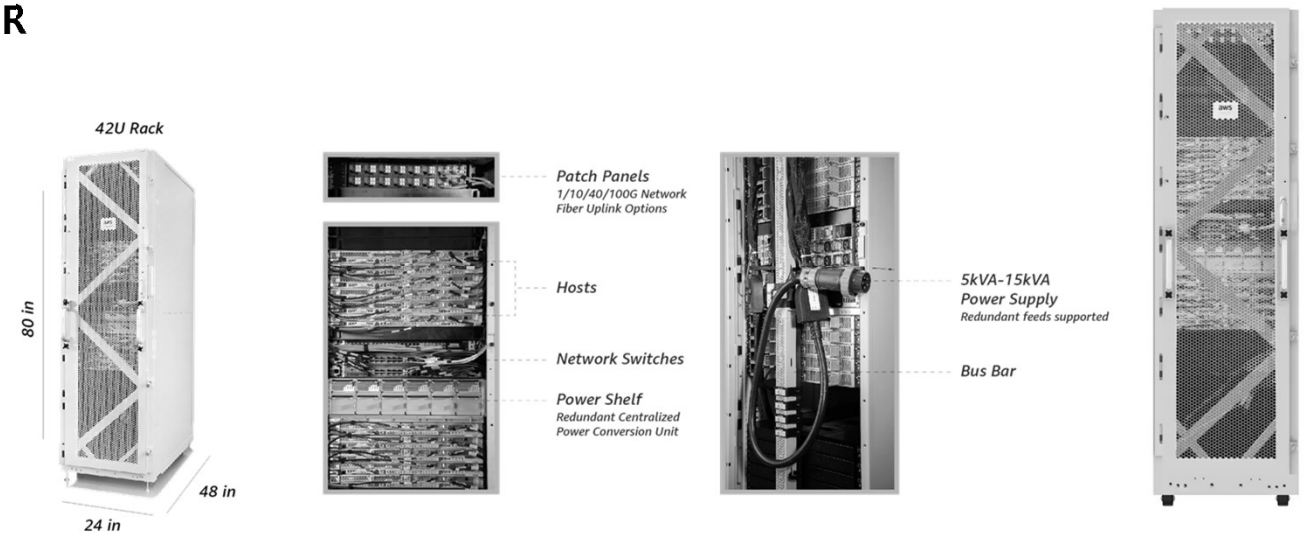


Source: https://blogs.vmware.com/velocloud/2020/03/31/vmware-to-deliver-networking-solutions-with-azure-edge-zones/

DAY 3. 하이브리드와 멀티 클라우드

❖**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/

DAY 3. 하이브리드와 멀티 클라우드

❖AWS Outposts rack pricing

Development & testing units

Resource ID	Description	Configuration	No Upfront	Partial Upfront	All Upfront
OR-L8IF4WF	General purpose unit for development and testing with the smallest capacity footprint	4 m5.12xlarge	$5,407.78 monthly	$90,129.72 upfront, $2,503.60 monthly	$169,443.88
OR-I0OGL02	General purpose unit for development and testing with the smallest capacity footprint and 1G network uplink	4 m5.12xlarge	$5,407.78 monthly	$90,129.72 upfront, $2,503.60 monthly	$169,443.88
OR-LMF5LJ1	Graphics small unit for development and testing of ML inference, virtual desktops and artist workstations	2 g4dn.12xlarge	$5,134.92 monthly	$85,581.95 upfront, $2,377.28 monthly	$160,894.07

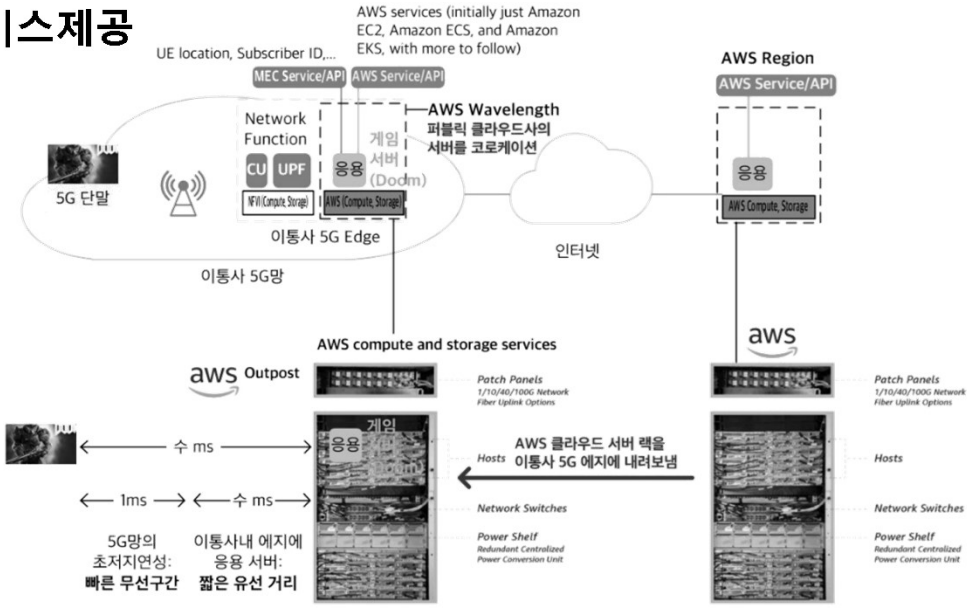
Upfront (선불)

Source: https://aws.amazon.com/outposts/rack/pricing/

DAY 3. 하이브리드와 멀티 클라우드

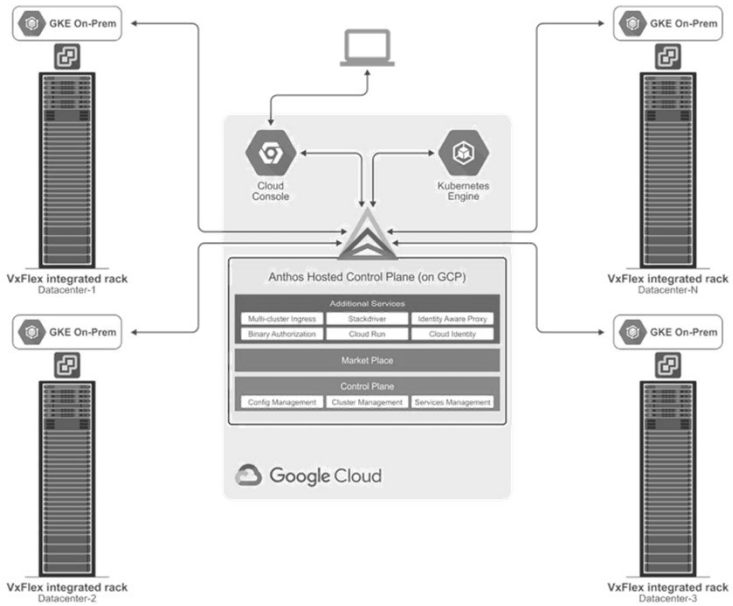
❖Use Case: Amazon AWS Wavelength

- 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



DAY 3. 하이브리드와 멀티 클라우드

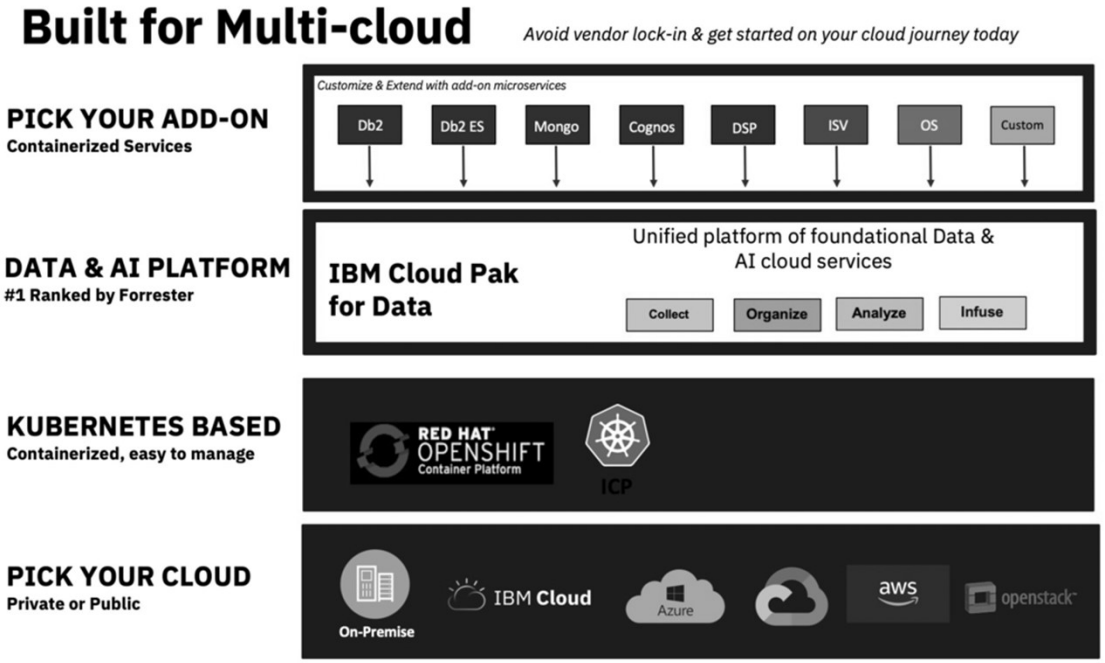
❖소프트웨어 기반 Anthos 는 구글에서 Dell EMC나 HPE등의 하드웨어 파트너와 협력 멀티클라우드 솔루션으로 확대 중



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

DAY 3. 하이브리드와 멀티 클라우드

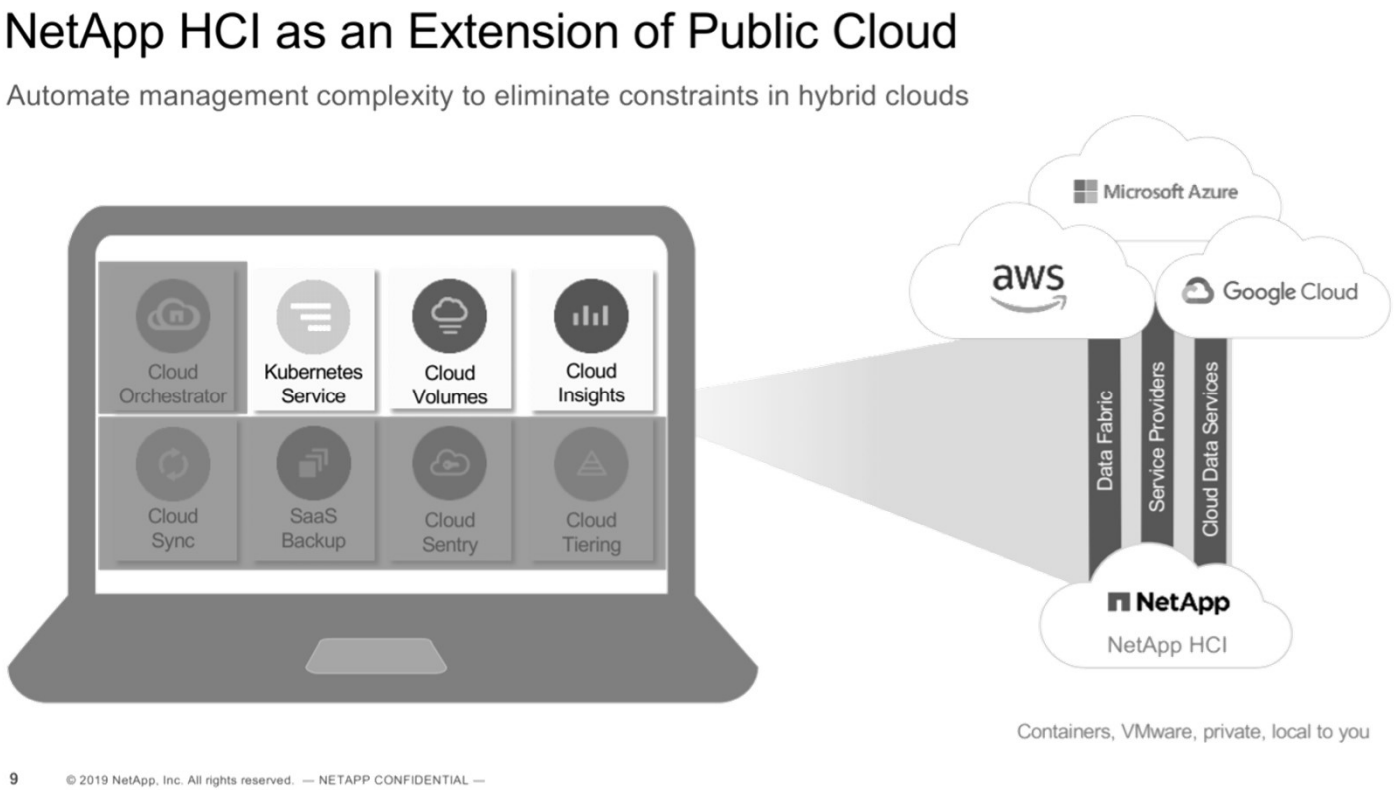
❖IBM Cloud Pak은 멀티 클라우드 솔루션으로 확대



Source: https://www.ibmbigdatahub.com/blog/ibm-cloud-pak-data-v2dot1

DAY 3. 하이브리드와 멀티 클라우드

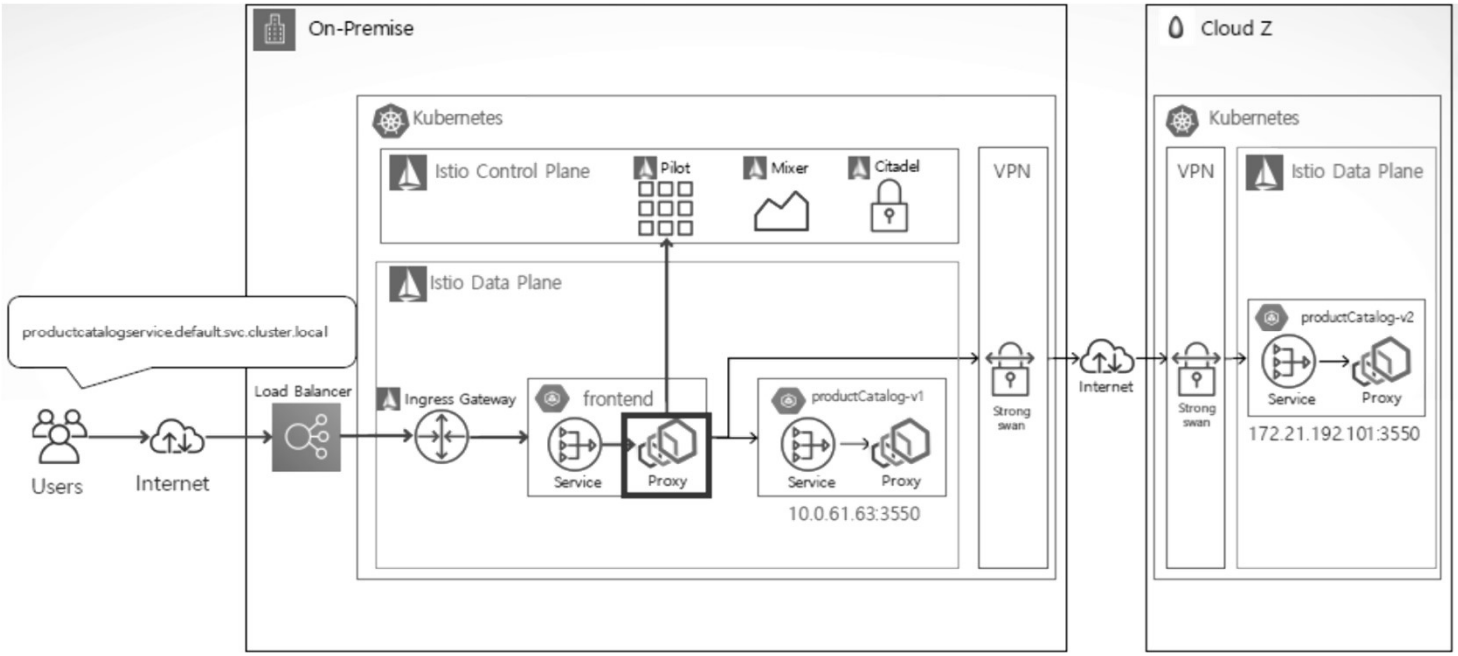
❖NetApp은 HCI 기반의 하이브리드 클라우드 서비스로 확장



DAY 3. 하이브리드와 멀티 클라우드

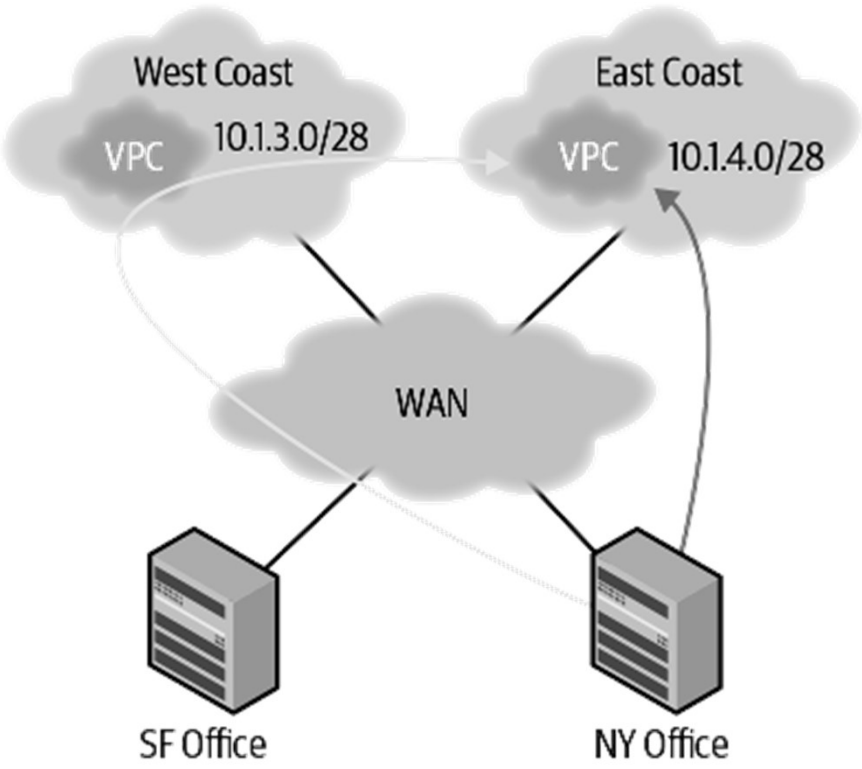
❖ Multi-Cloud Service Mesh Architecture (예)

- **Multi-Cloud(Cross Cluster)간 Service Mesh 연결/확장**



DAY 3. 하이브리드와 멀티 클라우드

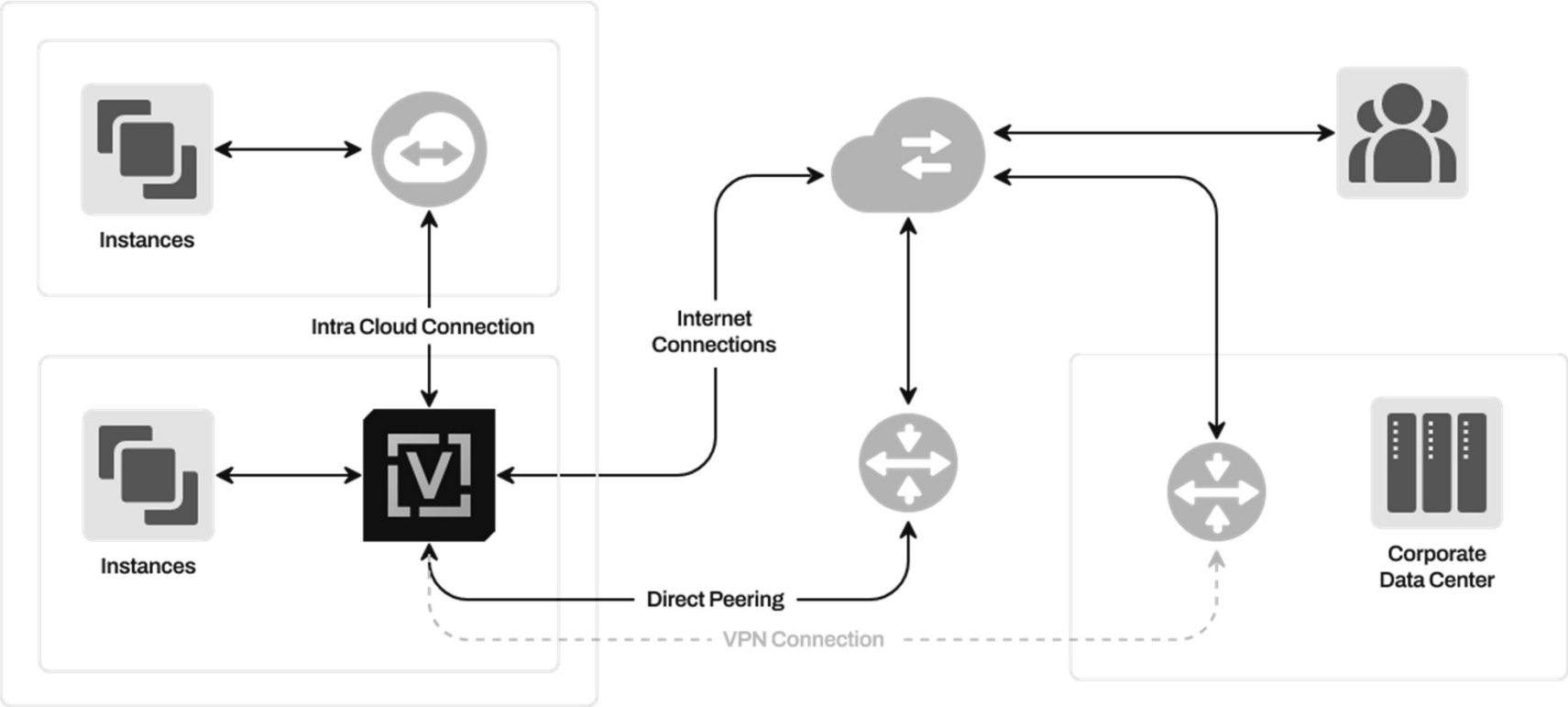
❖ **Nonoptimal routing scenario with direct-connect model**



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

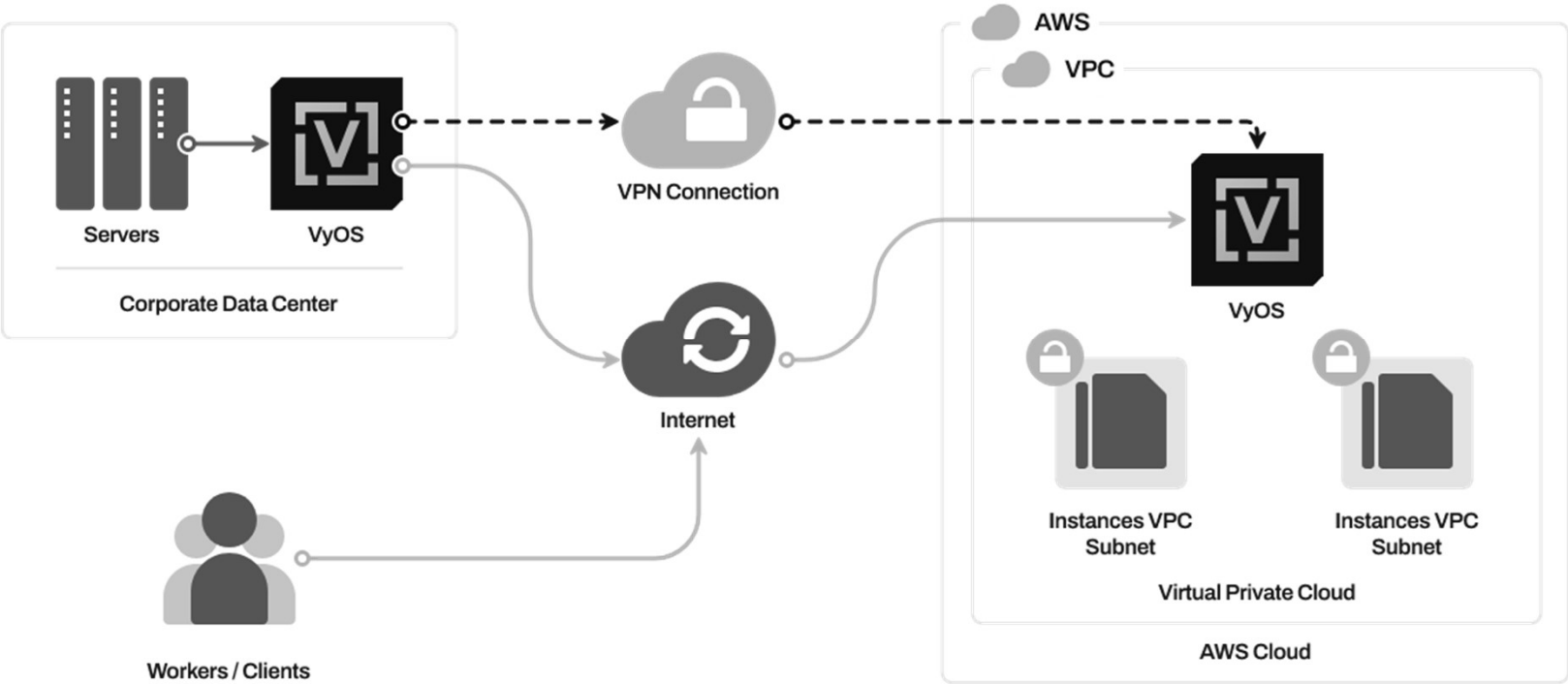
DAY 3. 하이브리드와 멀티 클라우드

❖ Cloud Gateway Environment



Source: https://vyos.io/use-cases/cloud-gateway

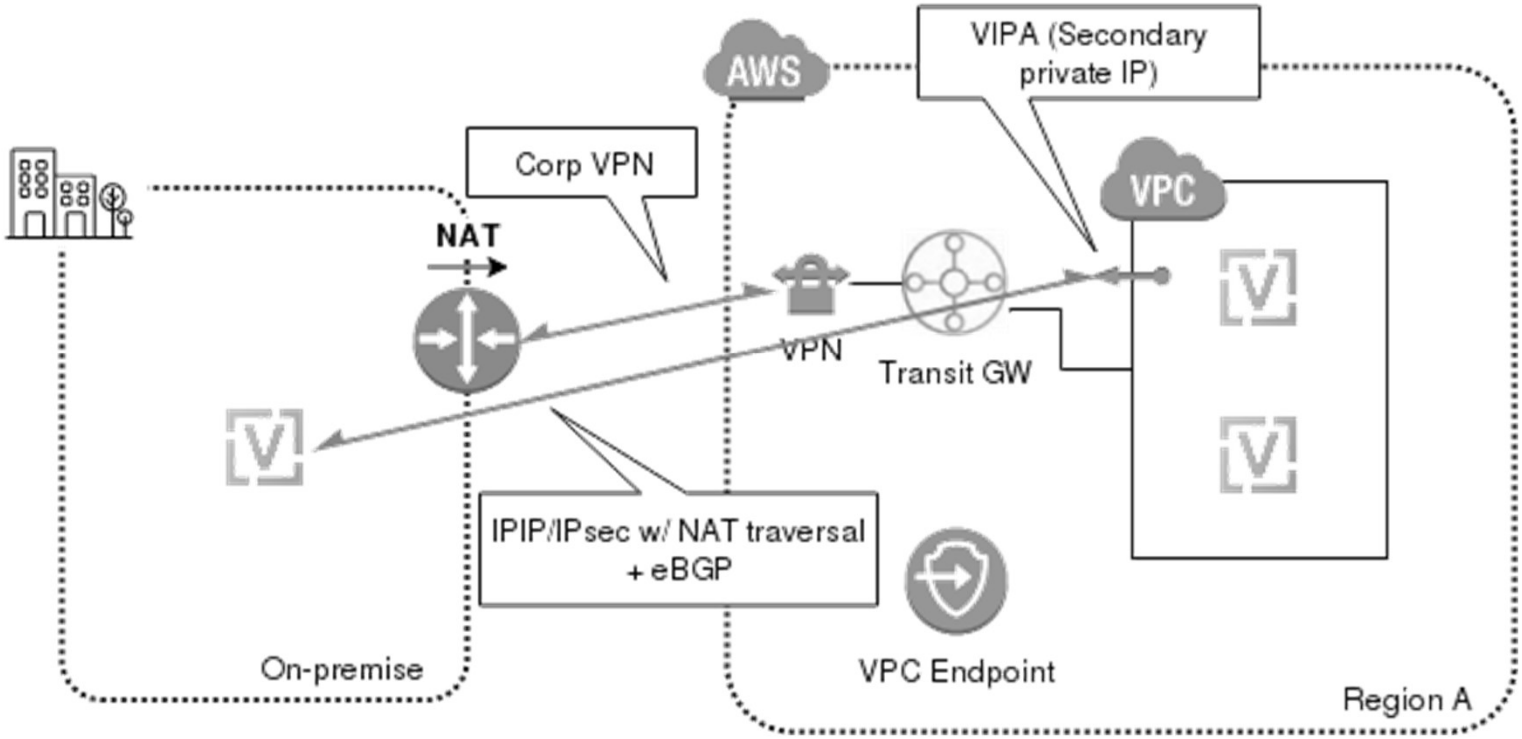
❖ VyOS AWS Solution: Improve your AWS infrastructure with VyOS



Source: https://vyos.io/solutions/vyos-on-aws

DAY 3. 하이브리드와 멀티 클라우드

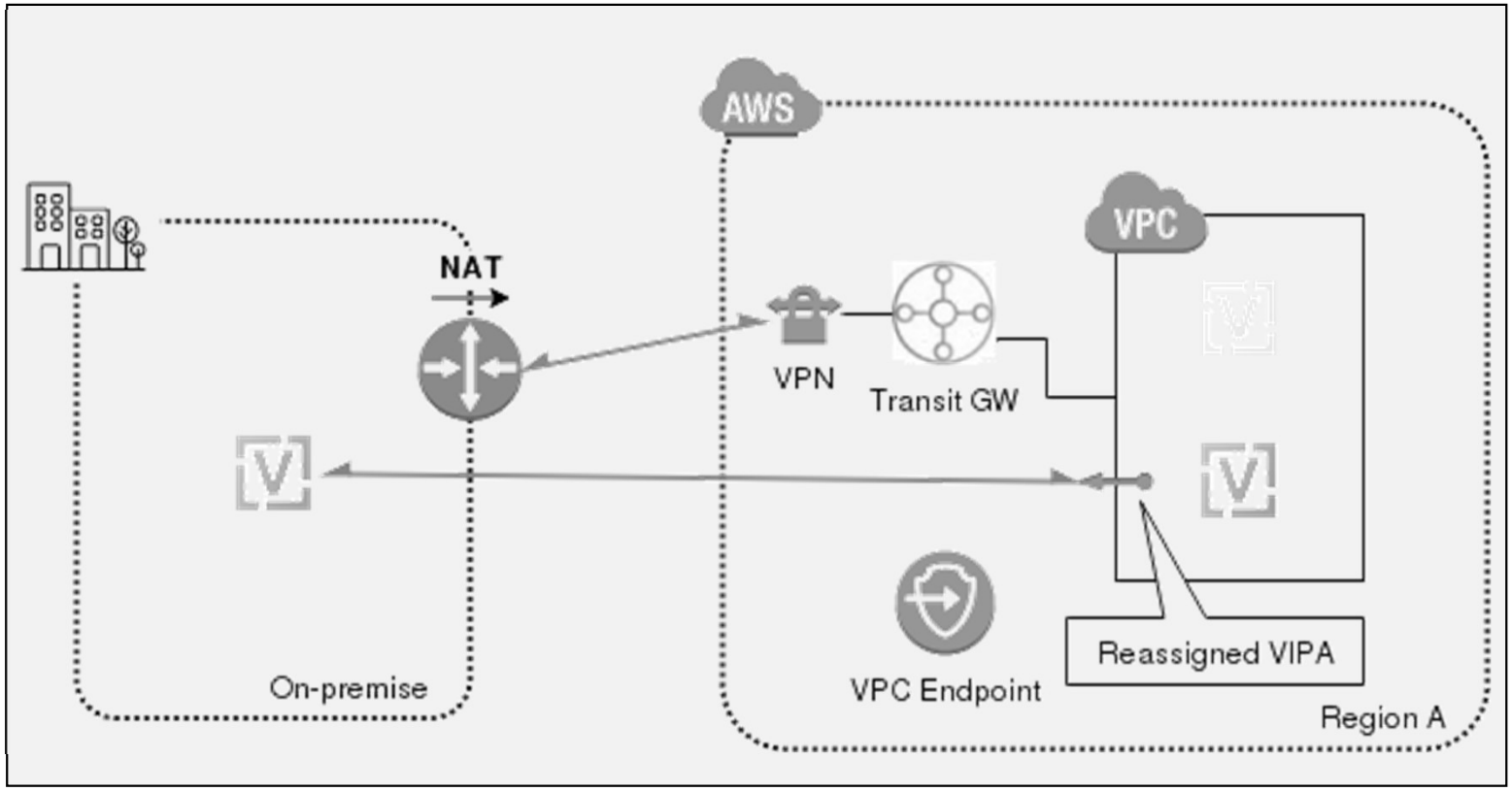
❖ VyOS HA in AWS (1 of 2)



Source: https://blog.stratio.com/vyos-ha-in-aws/

DAY 3. 하이브리드와 멀티 클라우드

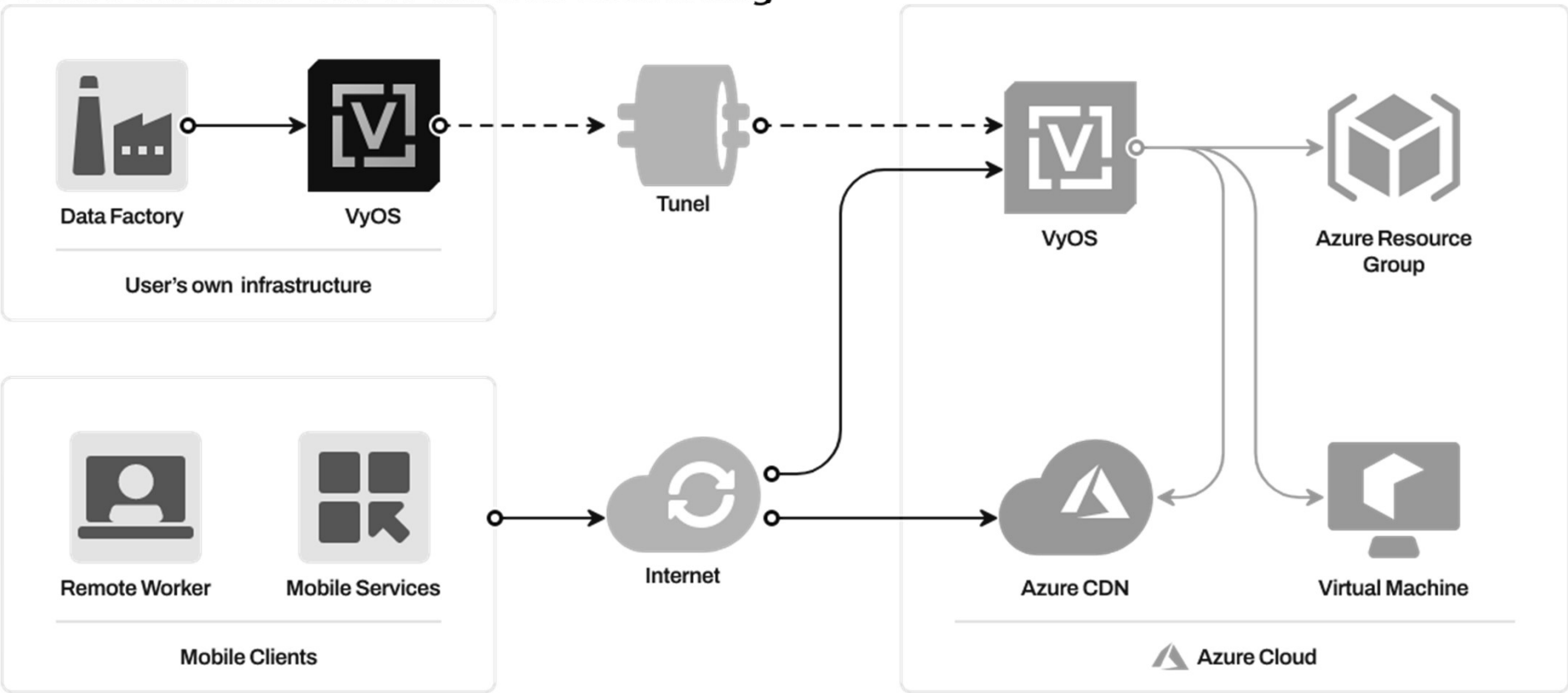
❖ VyOS HA in AWS (2 of 2)



Source: https://blog.stratio.com/vyos-ha-in-aws/

DAY 3. 하이브리드와 멀티 클라우드

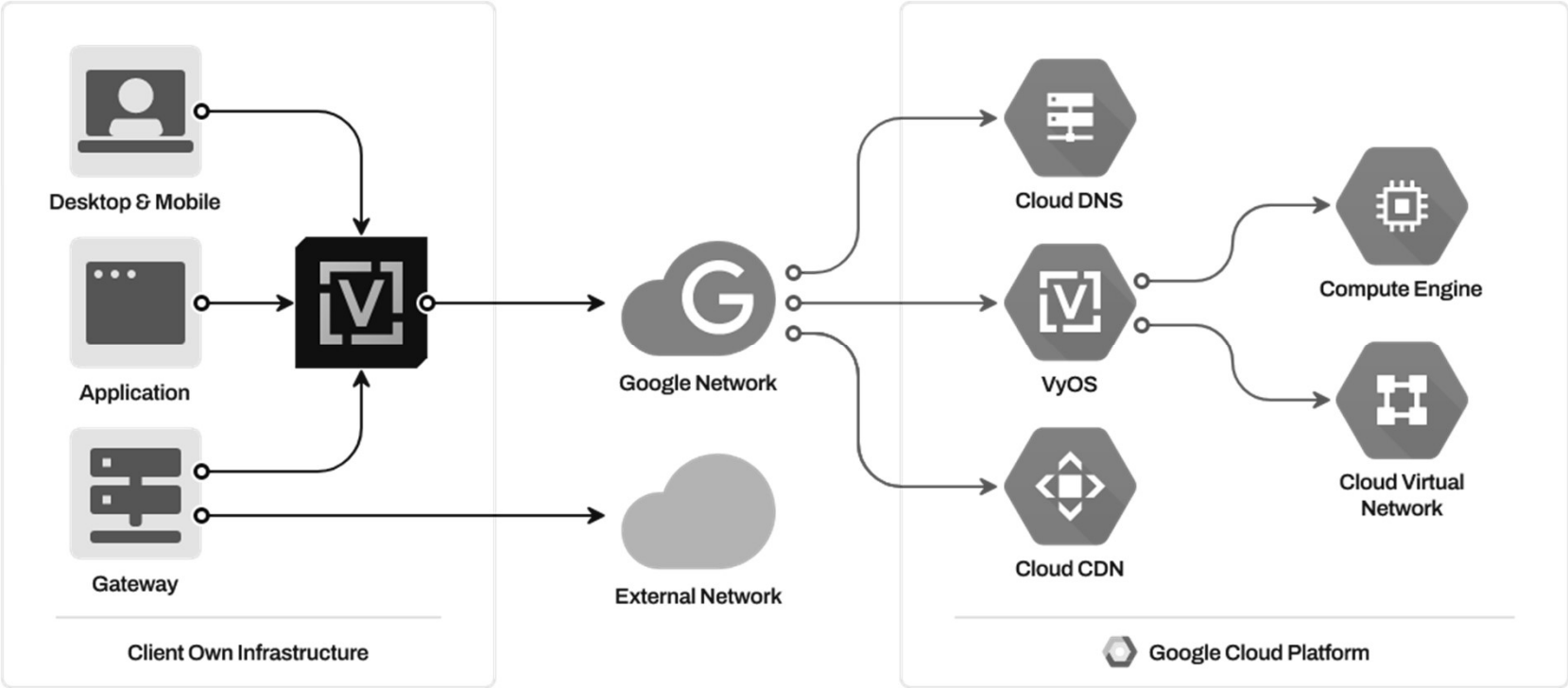
❖ VyOS Azure Solution: Out of the box networking



Source: https://vyos.io/solutions/vyos-on-azure

DAY 3. 하이브리드와 멀티 클라우드

❖ VyOS Google Cloud Solution: Improve your GCP infrastructure with VyOS

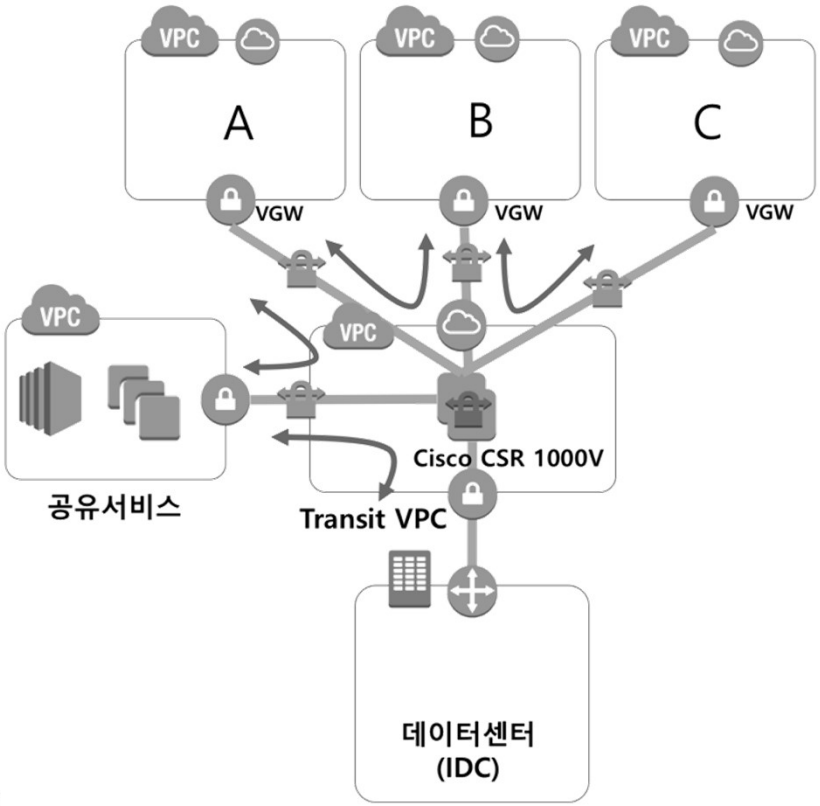


Source: https://vyos.io/solutions/vyos-on-gcp

DAY 3. 하이브리드와 멀티 클라우드

❖ Transit VPC를 통한 Cloud HUB 디자인하기 – AWS 서드 파티 도구 기반

- Cisco CSR1000V를 이용한 Transitive Routing 구성 방식

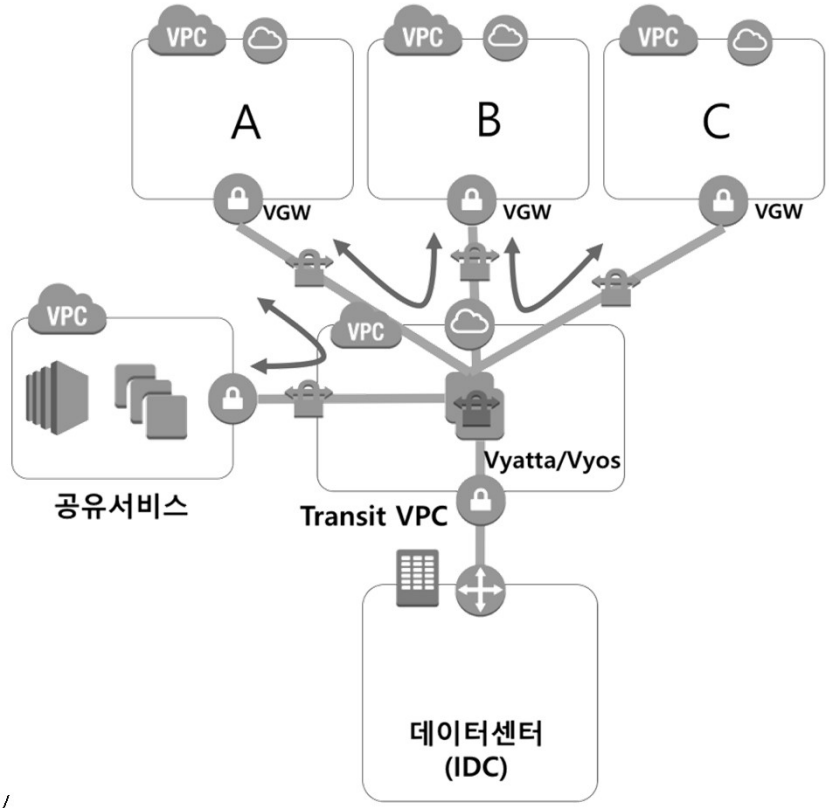


Source: https://aws.amazon.com/ko/blogs/korea/transit-vpc-cloud-hub-design-using-aws-marketplace-tools/

DAY 3. 하이브리드와 멀티 클라우드

❖ Transit VPC를 통한 Cloud HUB 디자인하기 – AWS 서드 파티 도구 기반

- Vyatta 및 VyOS를 통한 Cloud HUB 디자인
- Vyatta 혹은 VyOS를 이용한 Transitive Routing 구성 방식

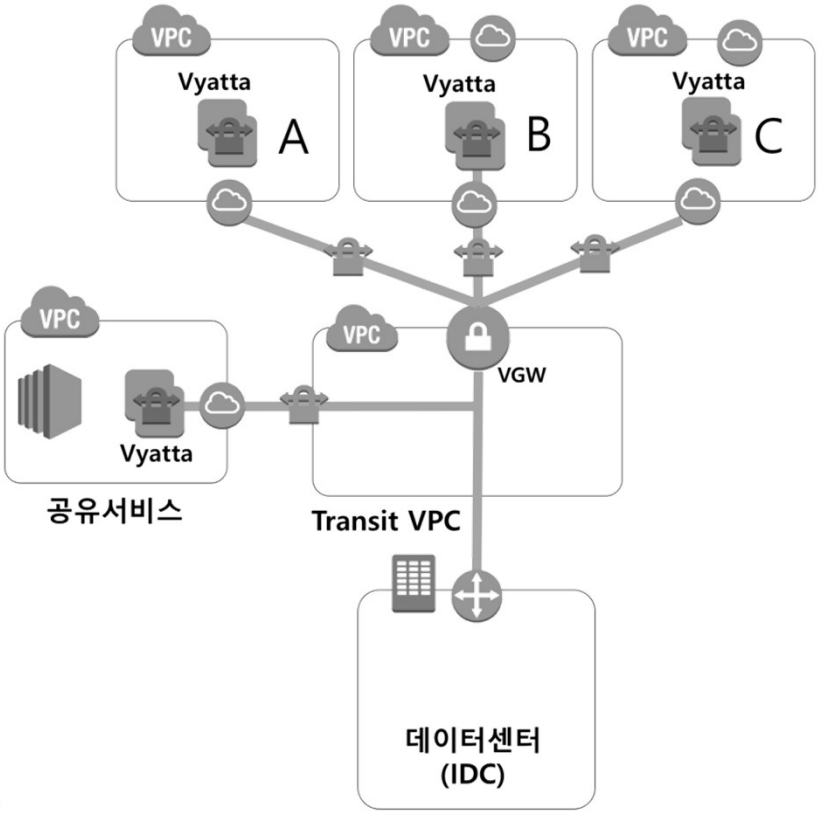


Source: https://aws.amazon.com/ko/blogs/korea/transit-vpc-cloud-hub-design-using-aws-marketplace-tools/

DAY 3. 하이브리드와 멀티 클라우드

❖ Transit VPC를 통한 Cloud HUB 디자인하기 – AWS 서드 파티 도구 기반

- 단일 VPC(VGW)를 통한 Cloud HUB 디자인 아키텍처

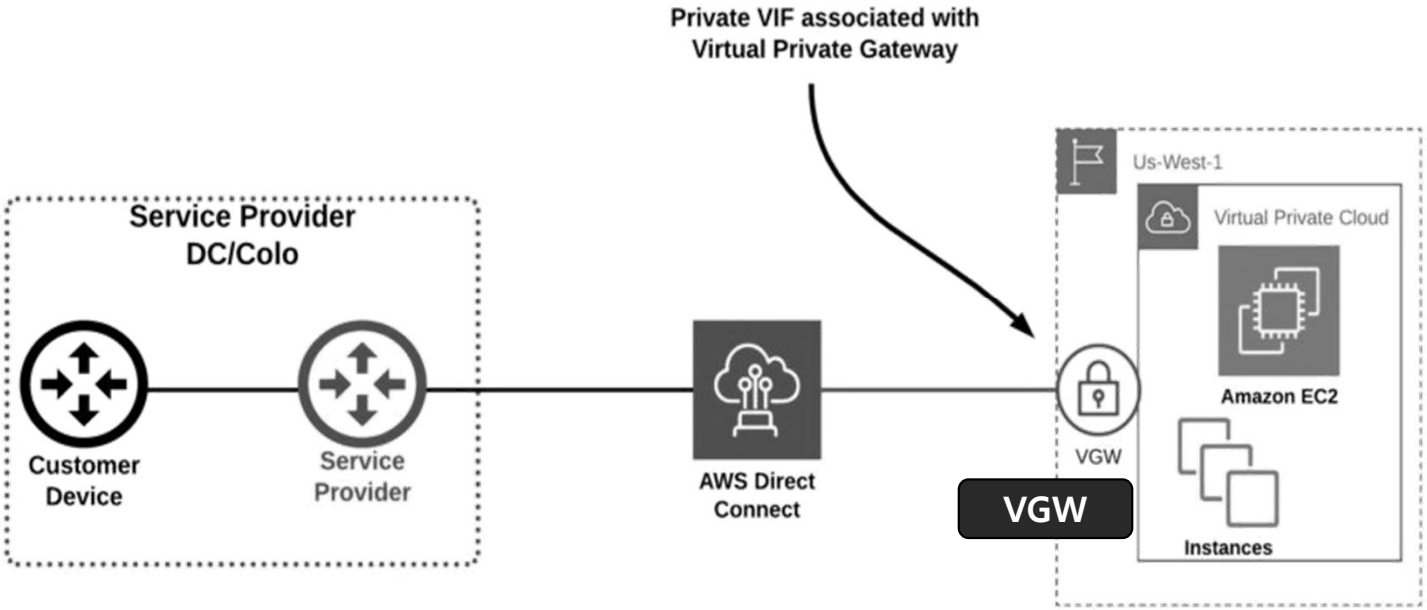


Source: https://aws.amazon.com/ko/blogs/korea/transit-vpc-cloud-hub-design-using-aws-marketplace-tools/

DAY 3. 하이브리드와 멀티 클라우드

❖ AWS

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

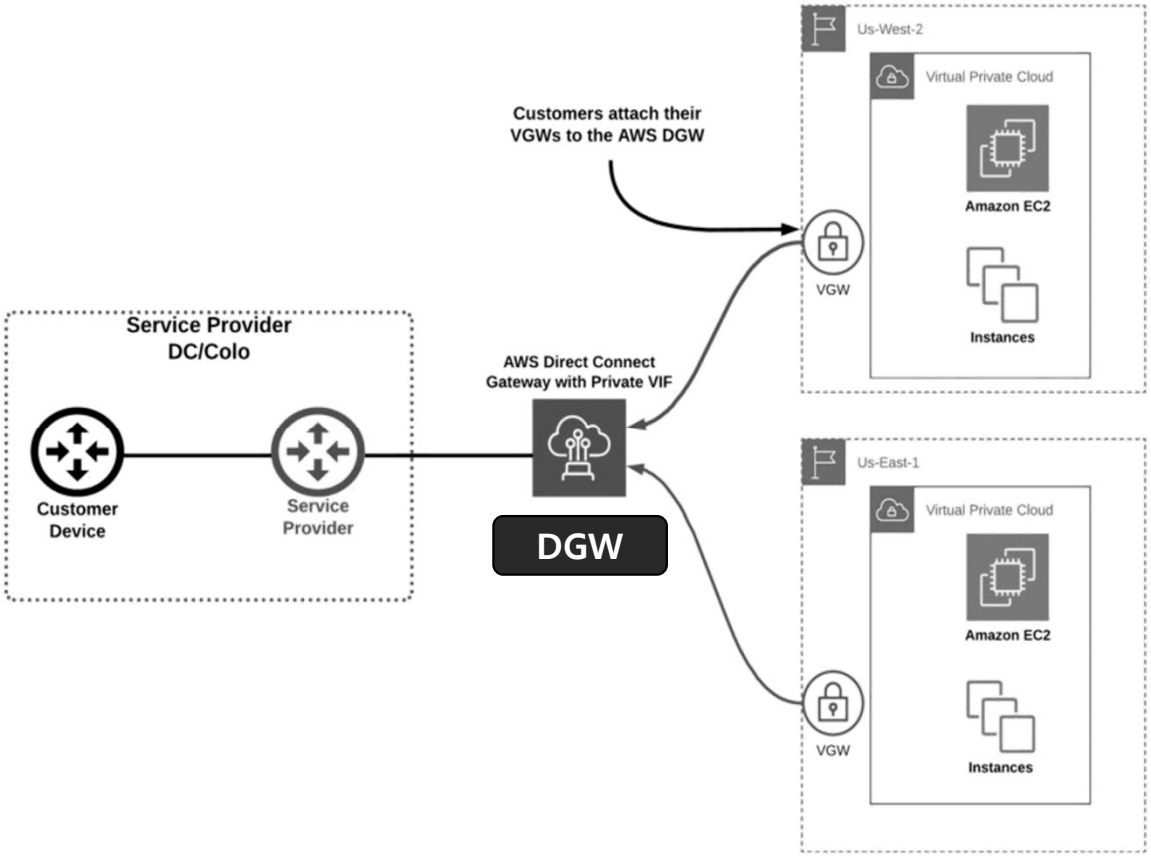


Source: https://www.megaport.com/blog/aws-vgw-vs-dgw-vs-tgw/

DAY 3. 하이브리드와 멀티 클라우드

❖ AWS

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

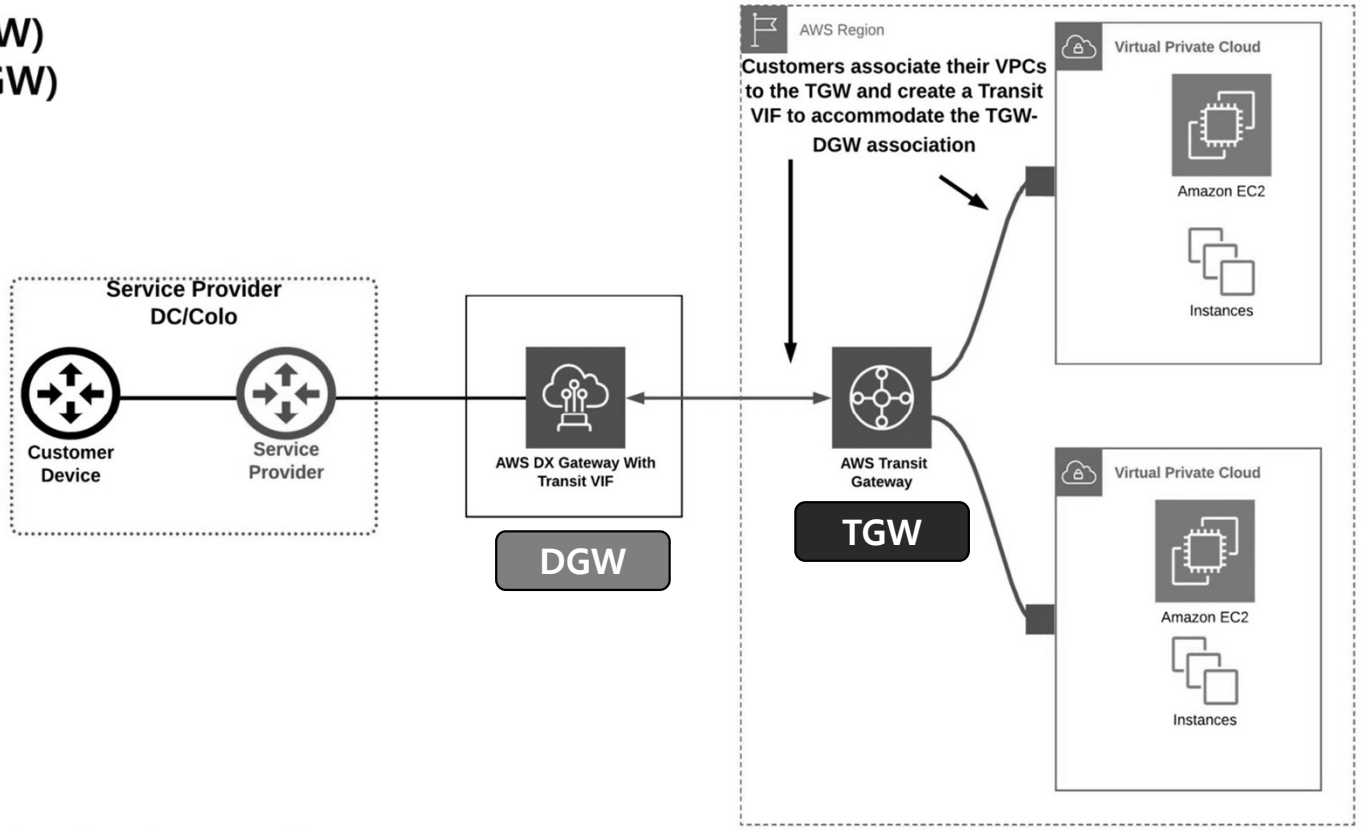


Source: https://www.megaport.com/blog/aws-vgw-vs-dgw-vs-tgw/

DAY 3. 하이브리드와 멀티 클라우드

❖ AWS

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



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

DAY 3. 하이브리드와 멀티 클라우드

❖ 데이터센터 연결

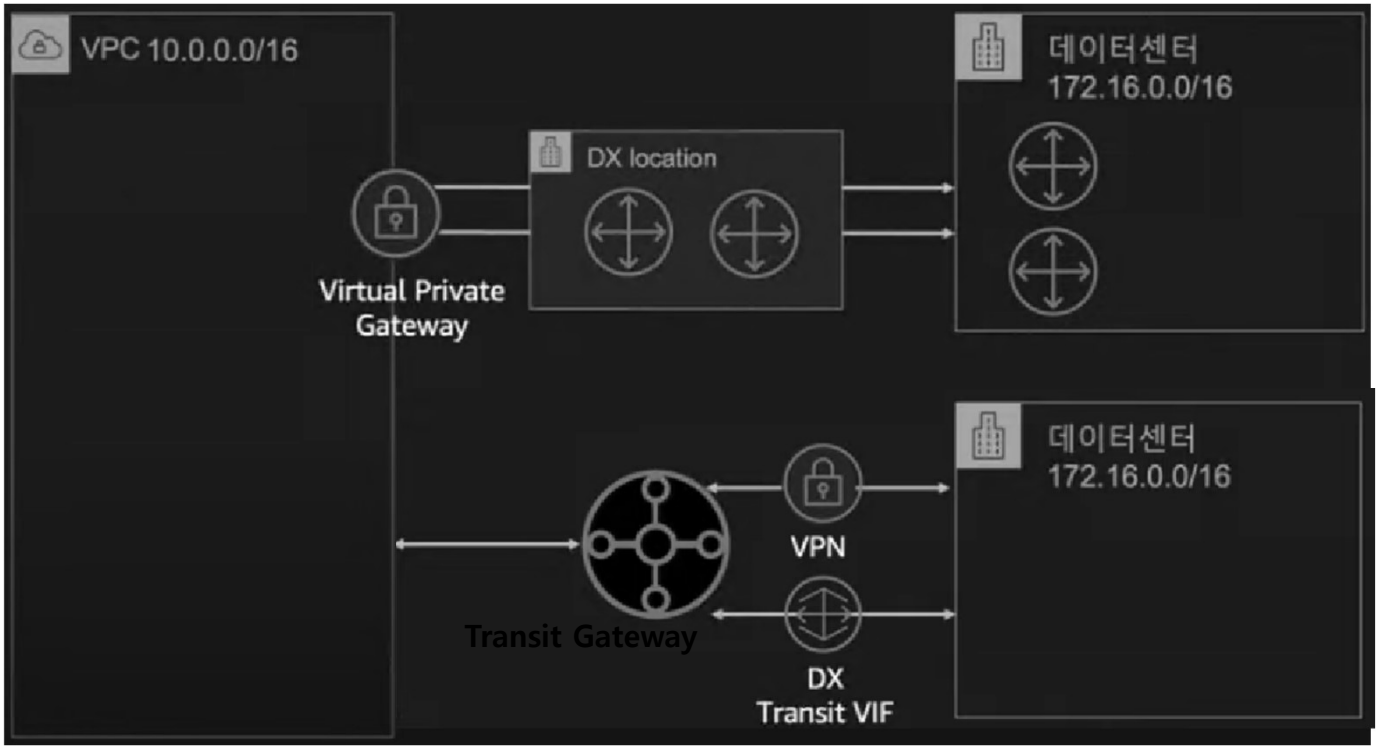
- VPN: Site-to-Site VPN
- Direct Connect

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

DAY 3. 하이브리드와 멀티 클라우드

❖ 데이터센터 연결

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

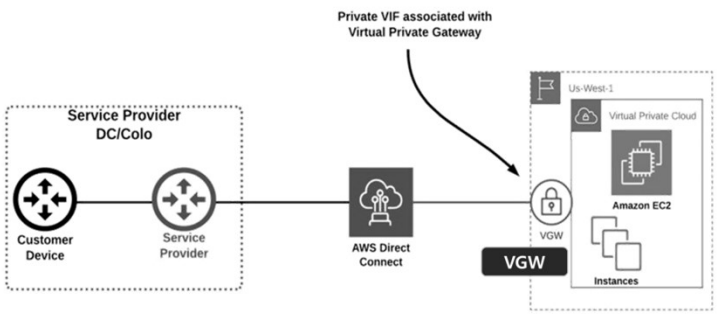


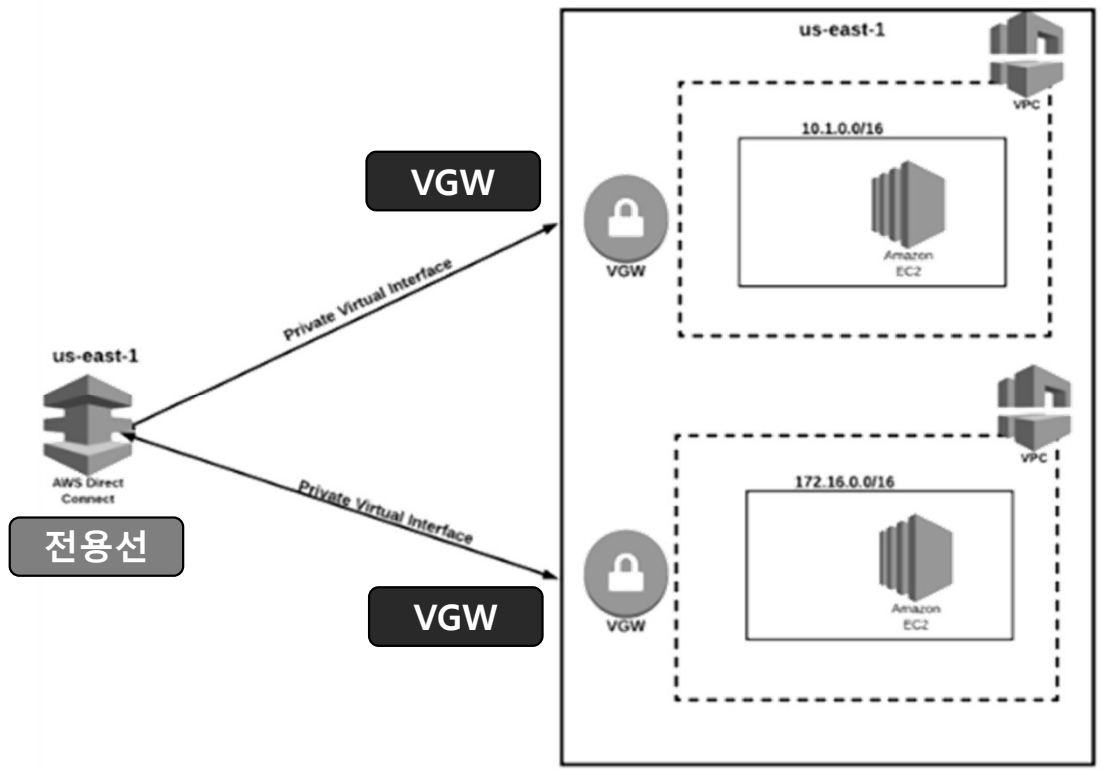
Source: https://www.youtube.com/watch?v=vCNexbgYmQ8

DAY 3. 하이브리드와 멀티 클라우드

❖ AWS

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



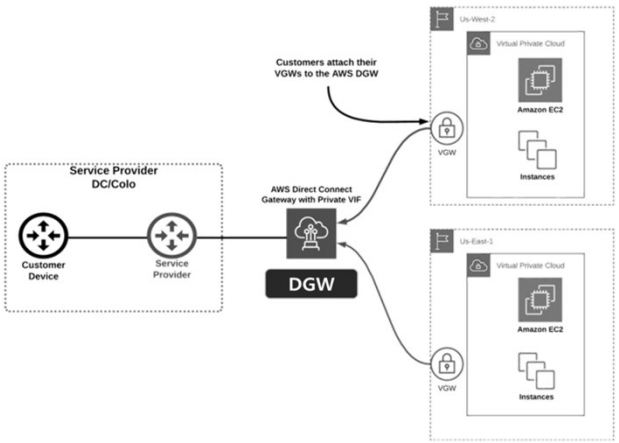


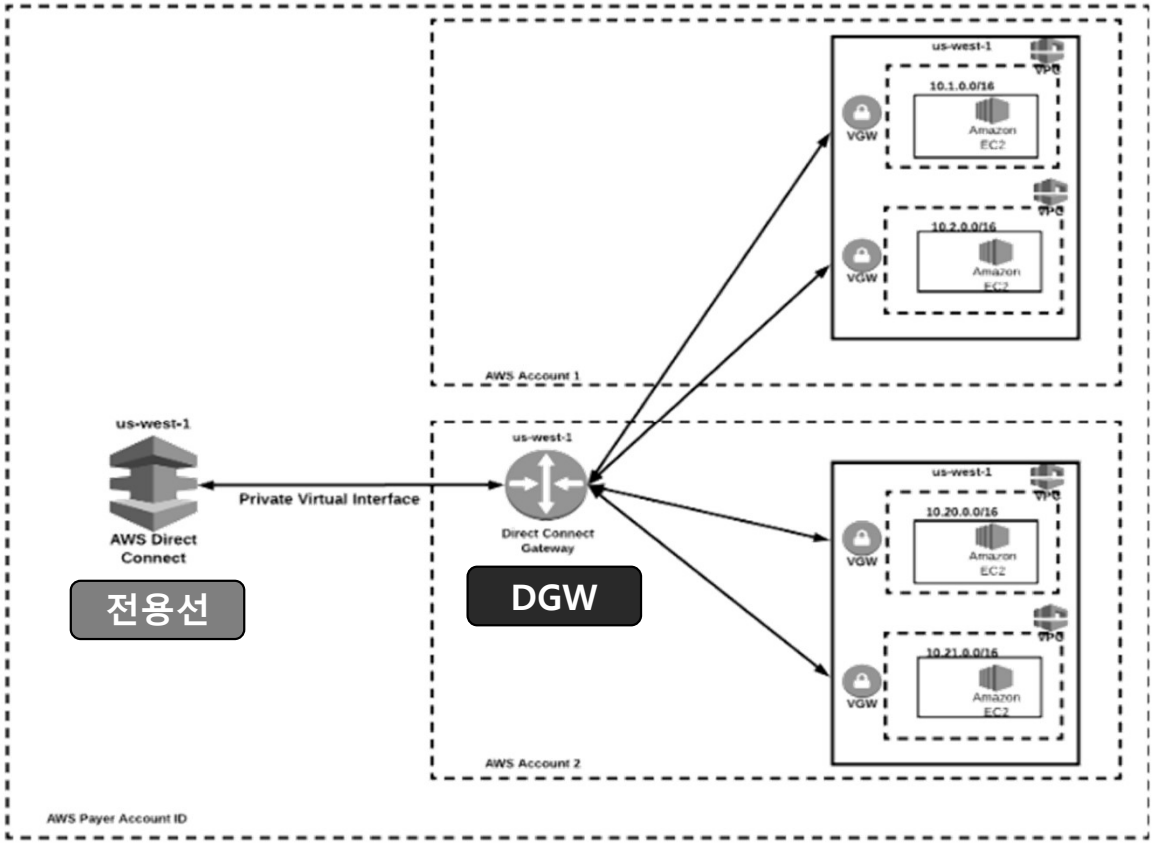
Source: https://www.megaport.com/blog/aws-vgw-vs-dgw-vs-tgw/

DAY 3. 하이브리드와 멀티 클라우드

❖ AWS

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



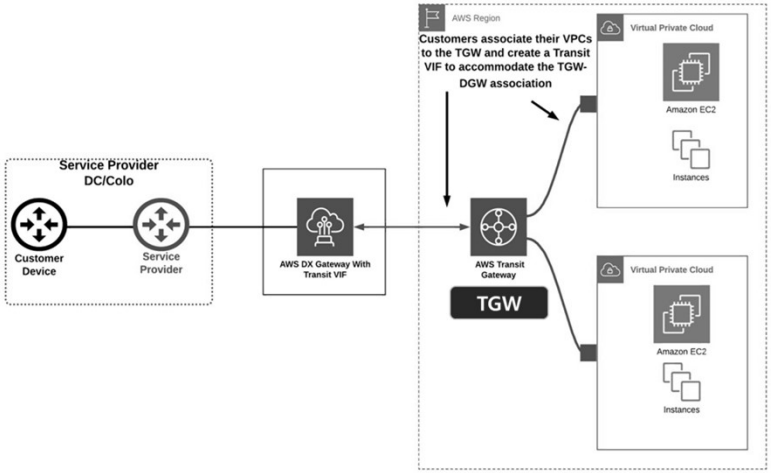


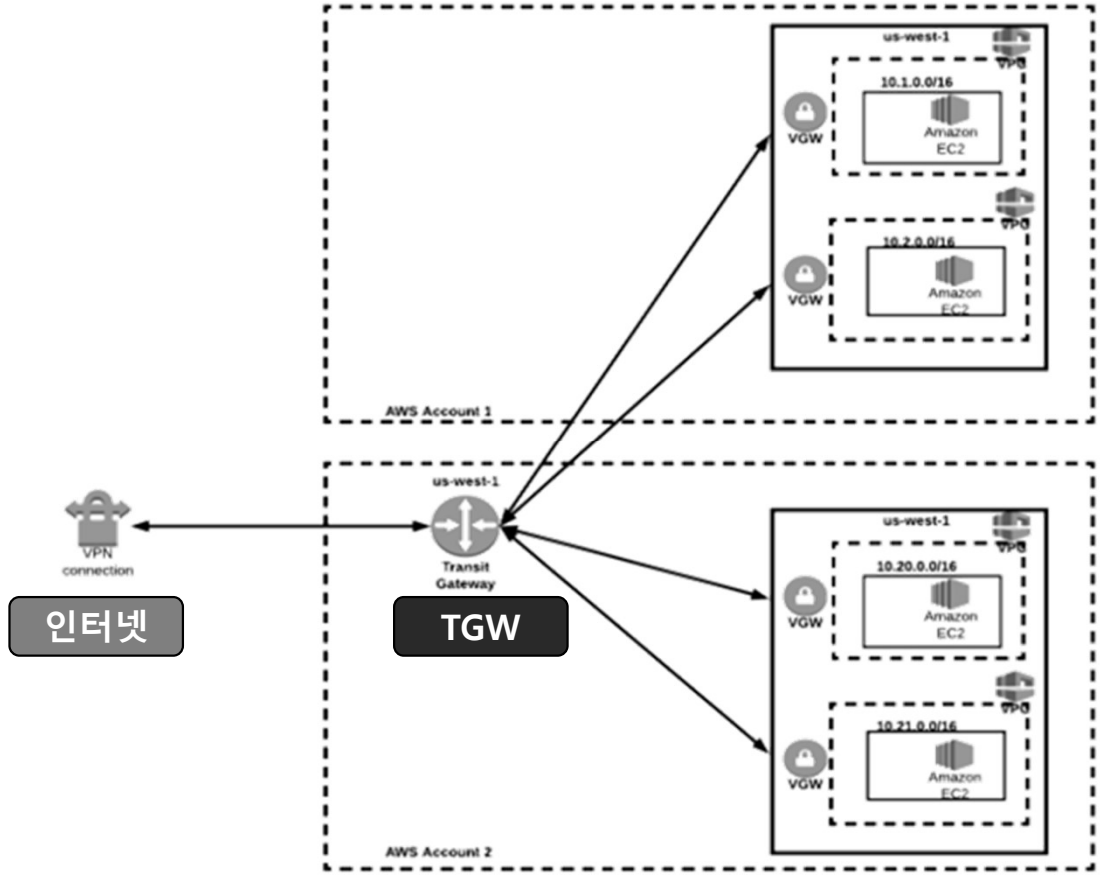
Source: https://www.megaport.com/blog/aws-vgw-vs-dgw-vs-tgw/

DAY 3. 하이브리드와 멀티 클라우드

❖ AWS

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





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

DAY 3. 하이브리드와 멀티 클라우드

❖ AWS VGW vs DGW vs TGW

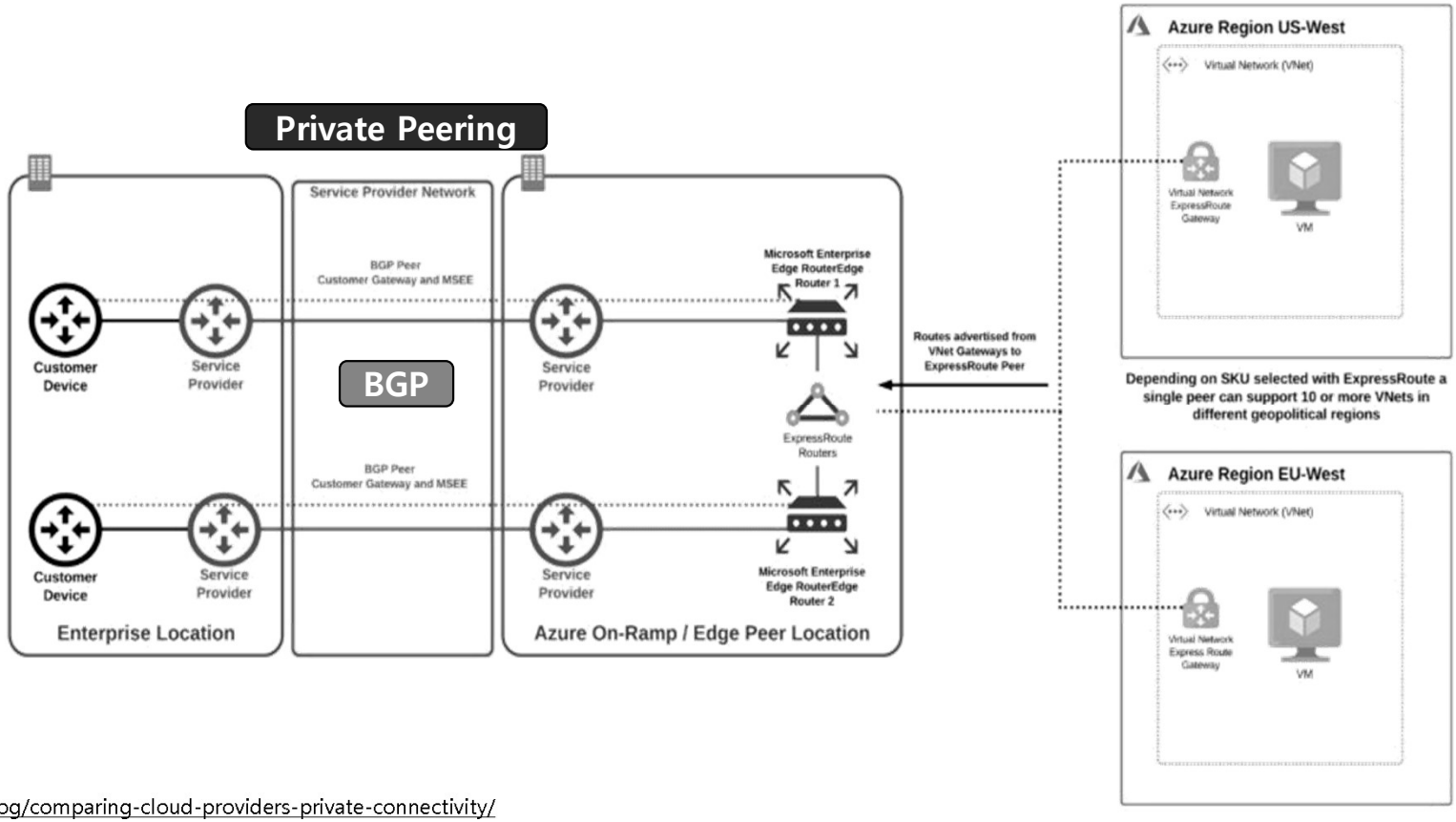
	Multiple Region	Multiple Account	S2S VPN	Direct Connect	Transitive Routing	Globally Available	Route Segmentation
VGW	❌	❌	✅	✅	❌	✅	❌
DGW	✅	✅	❌	✅	❌	✅	❌
TGW	✅	✅	✅	✅	✅	❌	✅

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

DAY 3. 하이브리드와 멀티 클라우드

❖ Azure

- Private Peering
- Microsoft Peering

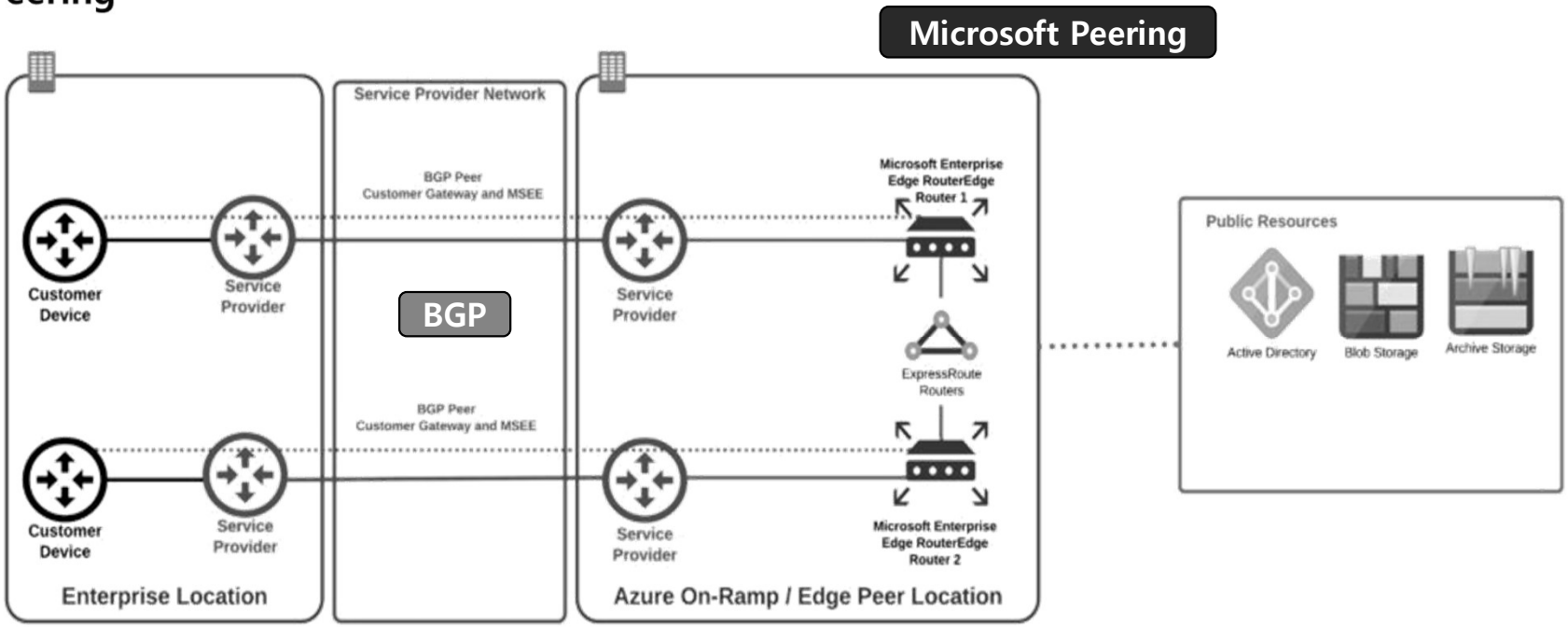


Source: https://www.megaport.com/blog/comparing-cloud-providers-private-connectivity/

DAY 3. 하이브리드와 멀티 클라우드

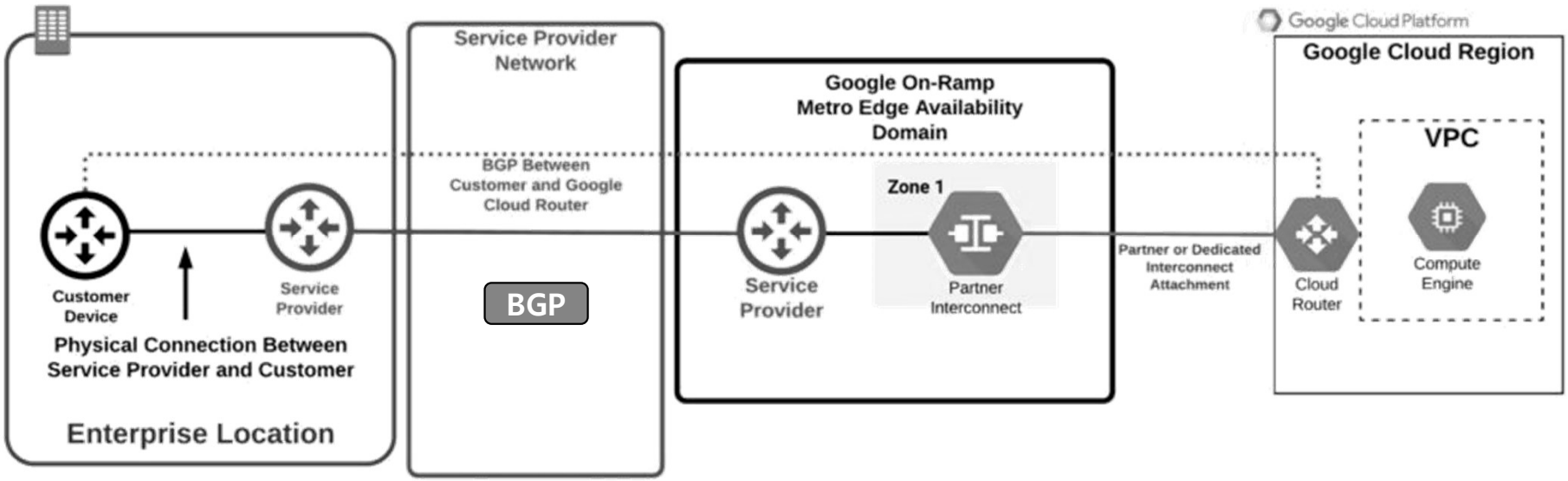
❖ Azure

- Private Peering
- Microsoft Peering



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

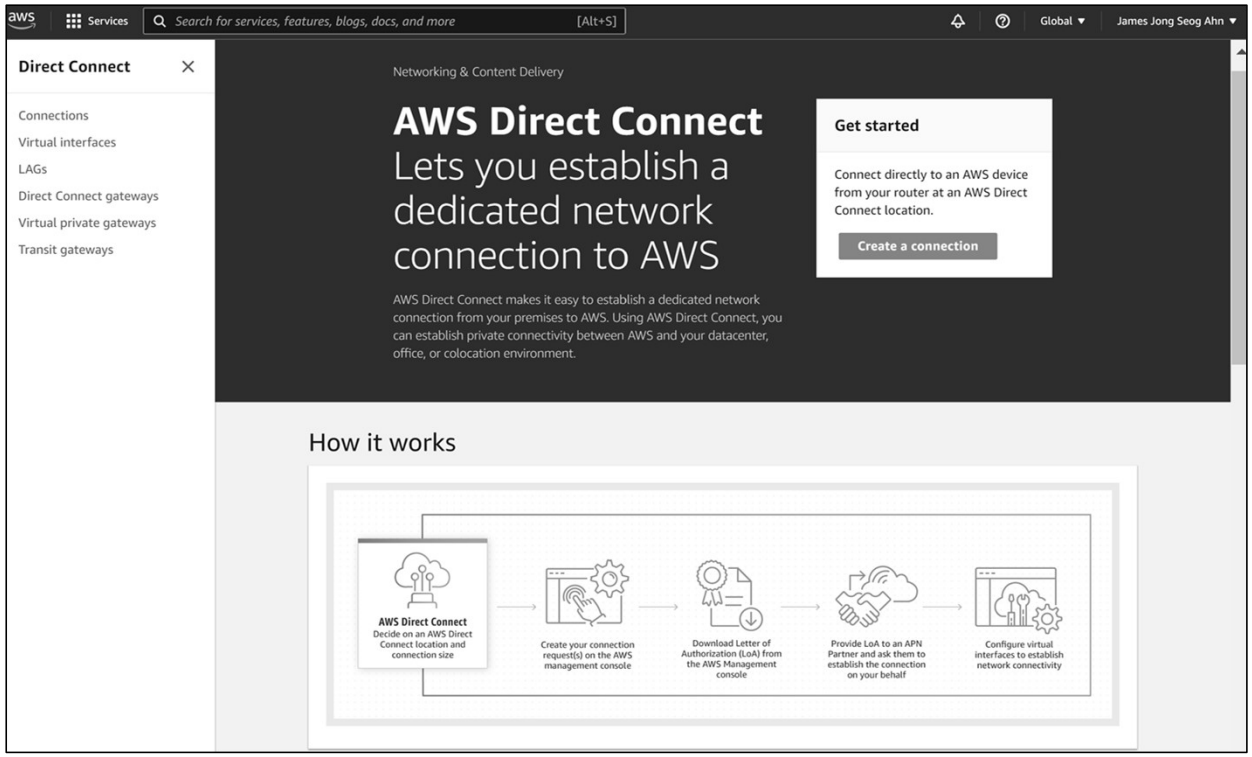
❖ Google Cloud Interconnect



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

❖ Amazon AWS – Direct Connect

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

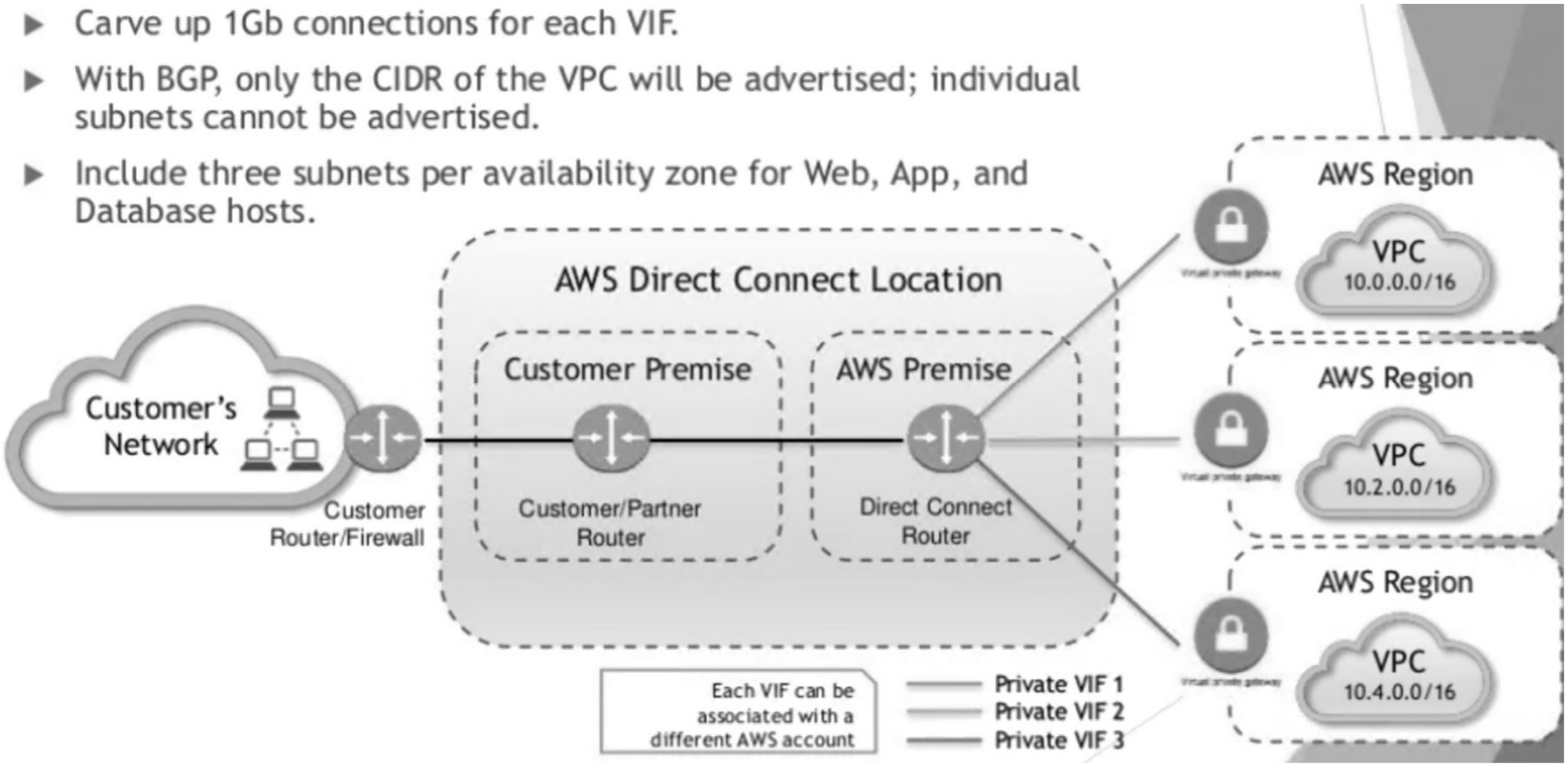


Link aggregation (LAG)

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

❖ Direct Connect Architecture (AWS)

- 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.

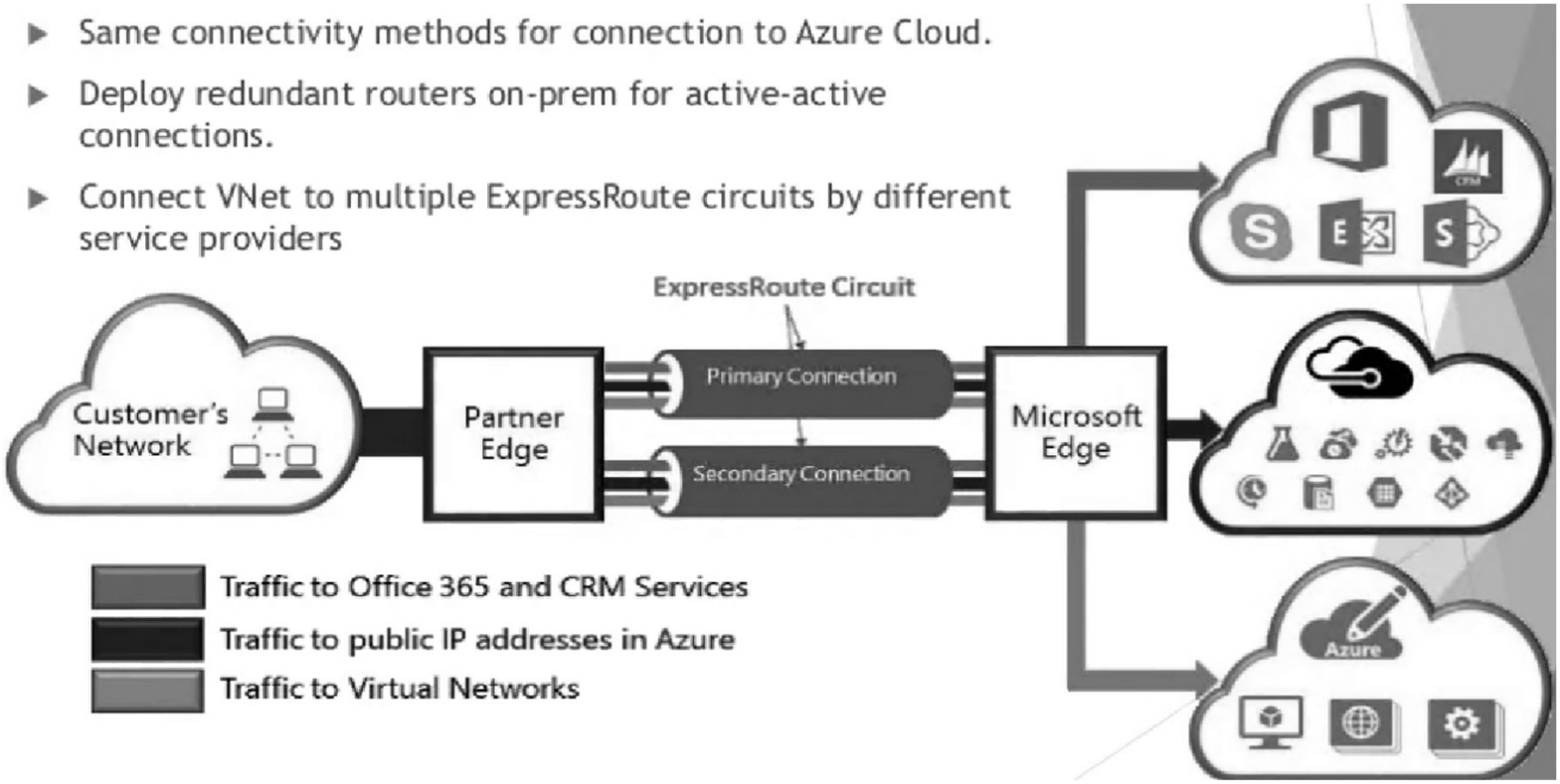


Virtual Network Interface (VIF)
Source: Joseph Primicerio

DAY 3. 하이브리드와 멀티 클라우드

❖ 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



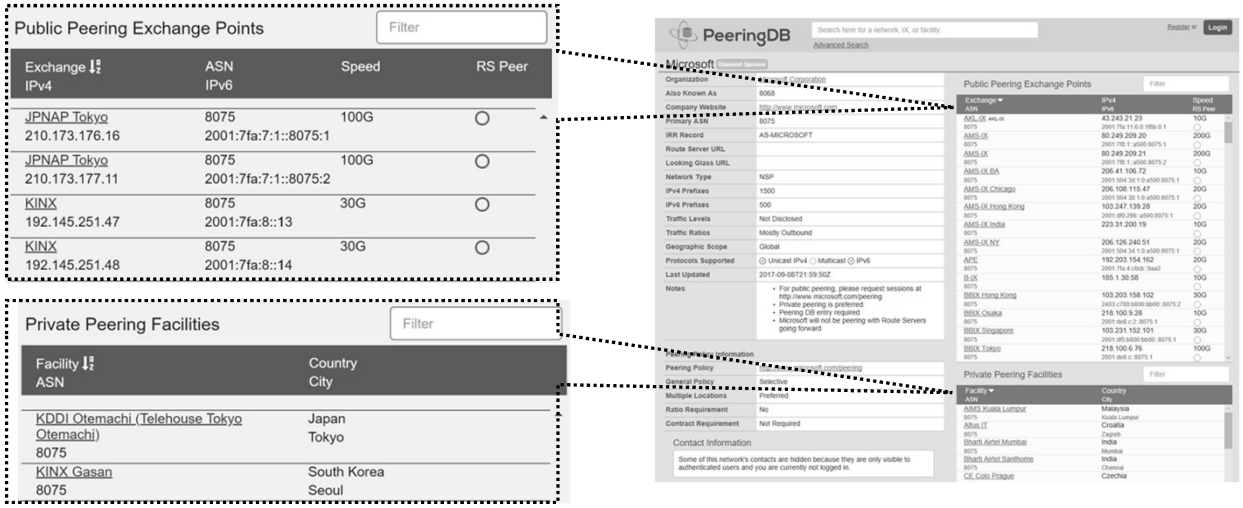
Source: Joseph Primicerio

DAY 3. 하이브리드와 멀티 클라우드

❖ Public interconnect and points of presence

- 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



Public Peering Exchange Points

Filter

Exchange IPv4	ASN IPv6	Speed	RS Peer
JPNAP Tokyo 210.173.176.16	8075 2001:7fa:7:1::8075:1	100G	○
JPNAP Tokyo 210.173.177.11	8075 2001:7fa:7:1::8075:2	100G	○
KINX 192.145.251.47	8075 2001:7fa:8::13	30G	○
KINX 192.145.251.48	8075 2001:7fa:8::14	30G	○

Private Peering Facilities

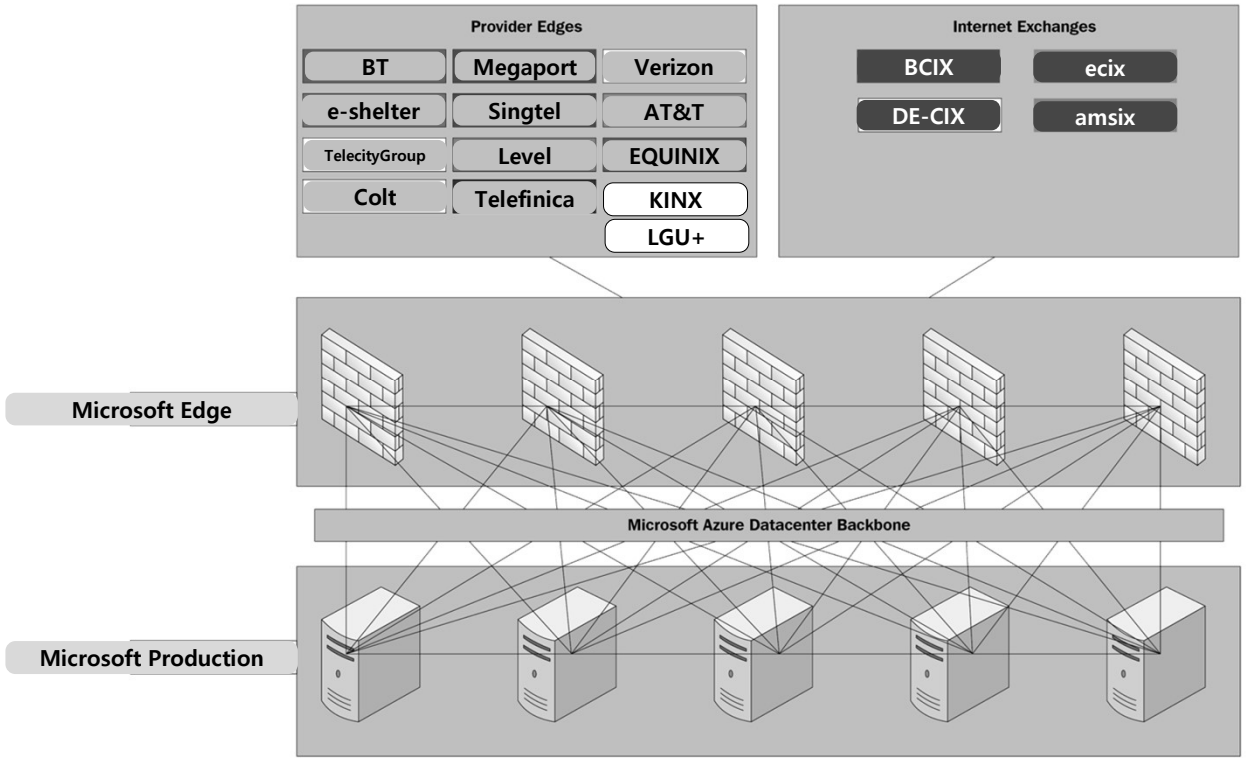
Filter

Facility ASN	Country City
KDDI Otemachi (Telehouse Tokyo Otemachi) 8075	Japan Tokyo
KINX Gasan 8075	South Korea Seoul

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

DAY 3. 하이브리드와 멀티 클라우드

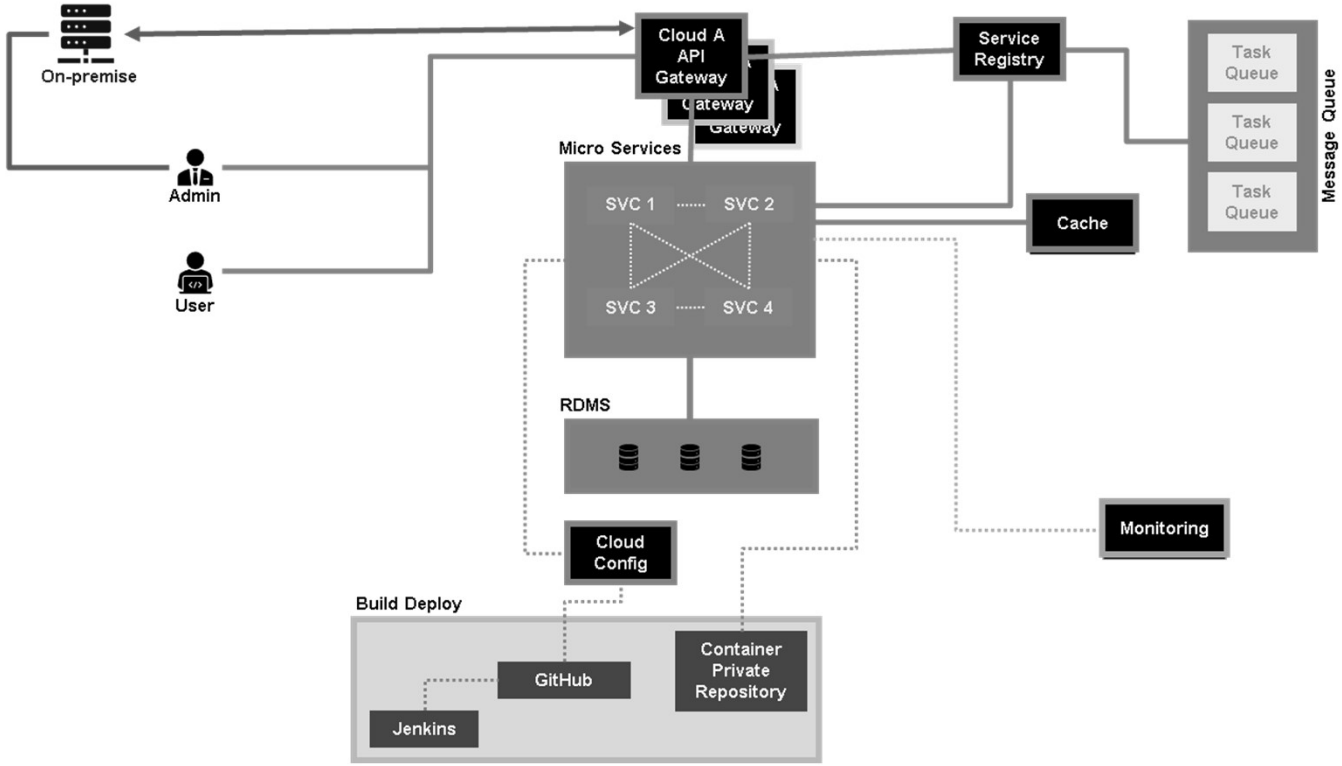
❖ Schematic view of the structure behind a Microsoft PoP or Edge site



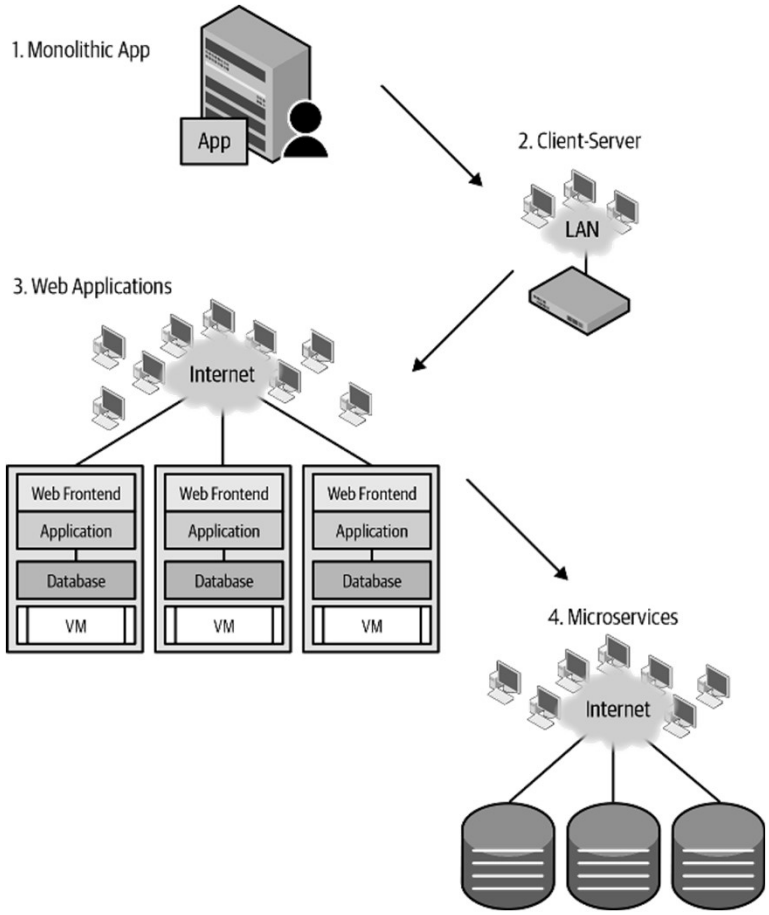
Source: Multi-Cloud for Architects (Published by Packt Publishing Ltd) Florian Klaffenbach, Markus Klein, Suresh Sundaresan

DAY 3. 하이브리드와 멀티 클라우드

❖ 온프레미스 연동 고려 Hybrid/Multi-Cloud Architecture (예)

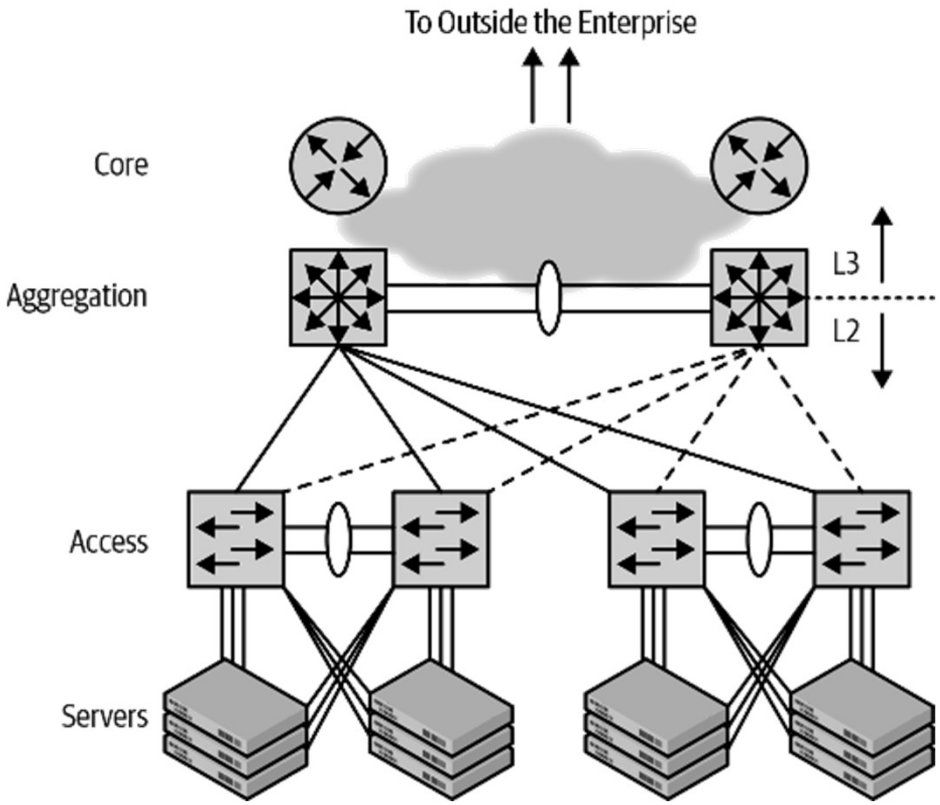


❖ Evolution of application architecture



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

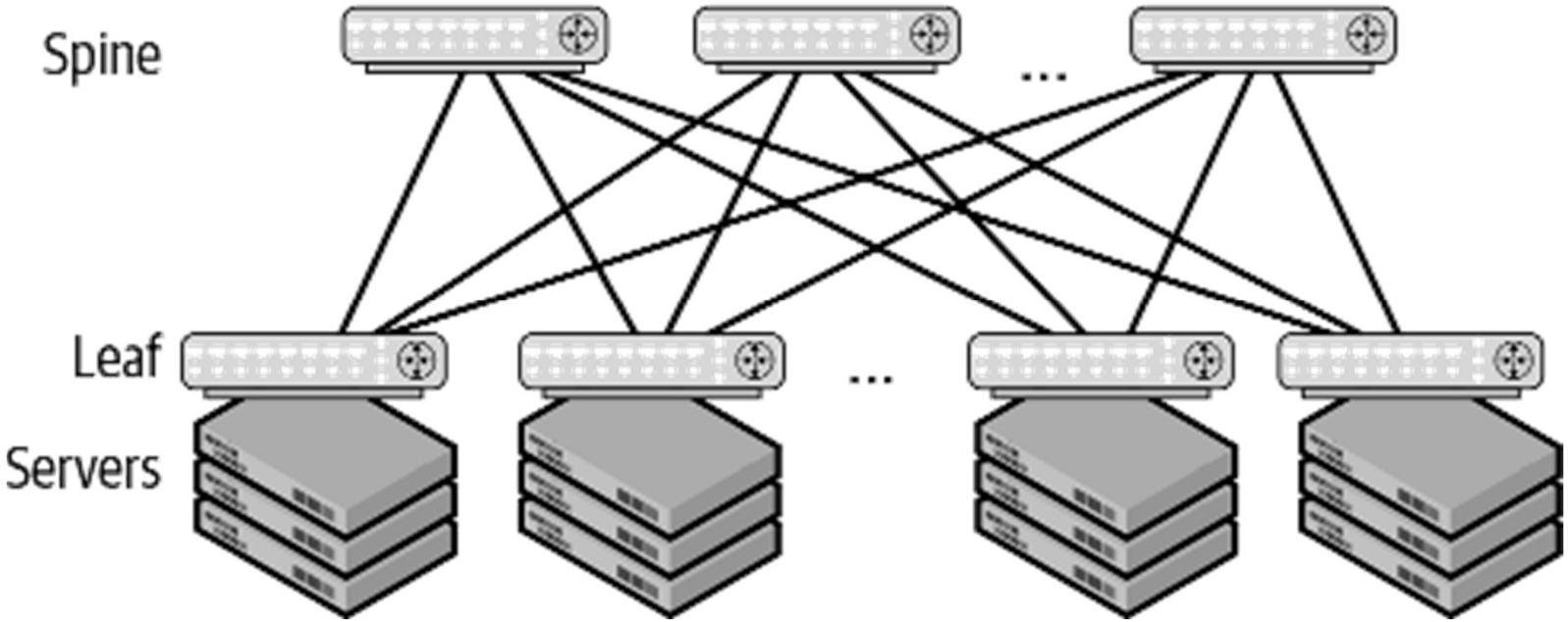
❖ **Access-aggregation-core network architecture**



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

DAY 3. 하이브리드와 멀티 클라우드

❖ **Illustration of a common Clos topology**



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

❖ Common connectivity options for cloud providers

- Most cloud providers basically offer the same solutions to connect to their cloud services. We will take a brief look at those solutions.

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

❖ Encryption via the internet

- The first type of connectivity that we will look at is direct connectivity to a cloud service via the internet. Most cloud service providers use HTTP and SSL, via port 443, to enable access. In those HTTP sessions, they encapsulate different protocols — such as the Remote Desktop Protocol (RDP)—mail traffic, API access, or regular website access.

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

❖ Virtual private network tunnels via the internet

- A Virtual Private Network (VPN) extends a private network across the internet and other public networks and enables companies to send and receive data across those shared networks. Devices connected to a VPN are directly connected to the private network of the organization. When we look at VPN tunnels over the internet, we can see that these tunnels have high limitations to their SLA, routing, performance, or high availability. You will get an SLA for most sites that use a VPN tunnel (as is the case with Azure, for example), for the virtual network gateways, or for internet access from your internet provider, but you will have nothing regarding the SLA in between when using the internet. The internet is still the best option.

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

❖ Private network interconnect via Ethernet, MPLS, or an IPVPN provider

- The primary service that all cloud providers offer is a private WAN connection via a network, possibly also including exchange providers. These private connections offer a direct connection to cloud services and cloud applications. These connections are mostly based on layer-2 Ethernet, layer-3 MPLS, or IPVPN connections to the cloud data center of the provider.

- When working with an enterprise-grade cloud environment, these direct connections are necessary to provide low latency and highly available network connections to cloud resources. Some examples of these services are Microsoft ExpressRoute and AWS Direct Connect.

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

❖ What matters the most

- When working in a hosted environment or with cloud providers, there are some facts or that matter more than others. First, latency and bandwidth—they define how many cloud services you can consume and how fast you can reach your data. The second factor is the data that is stored and the data that is in transit. This information describes where your data is right now.

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

❖ Latency and bandwidth

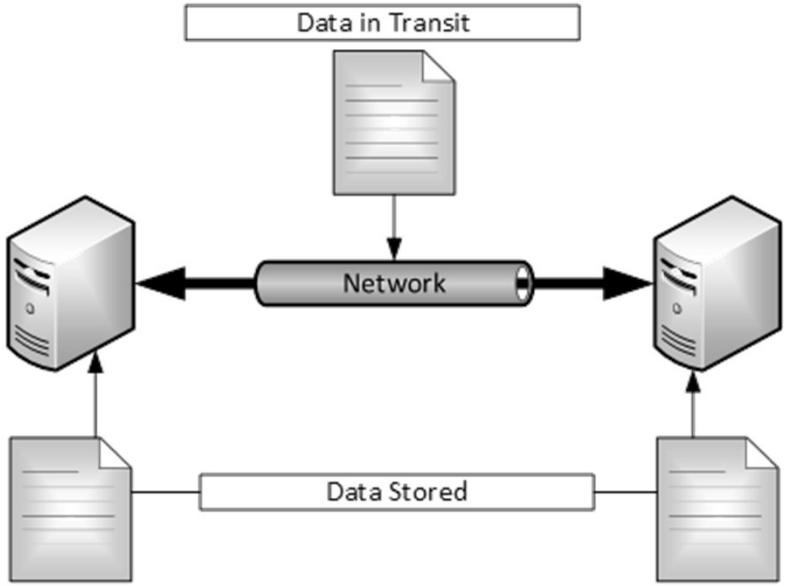
- In general, if you move a service to the cloud, you can say that, without WAN optimization, the service needs the same bandwidth as it needs on premise. There are options available to minimize this traffic, but it depends on the solution and protocols that are used.
- For latency, there is a small, empirical formula. Latency is about 1 millisecond per 200 kilometers, which is nearly the speed of light. In the field, you will mostly see about 1 millisecond per 150 kilometers.

Korea 100Km

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

❖ Data in transit and data that's stored

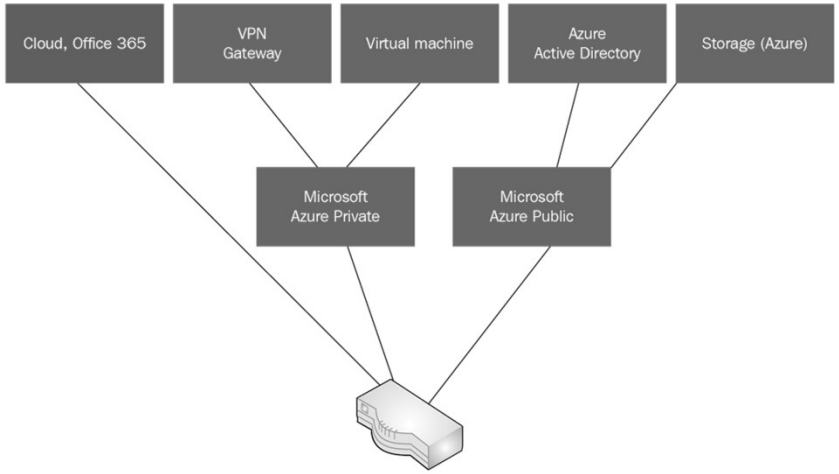
- The data is traveling across carrier and data center networks and always takes the shortest available route.



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

❖ Interconnect via internet (HTTPs)

- Microsoft cloud services communicate with one another on a public IP, even in the Microsoft global backbone.
- Let's look at an example of a big layer-3 routing device, handling all internal and external requests from Microsoft, ensuring that Microsoft service communications stay on the backbone and are reachable for external access.



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

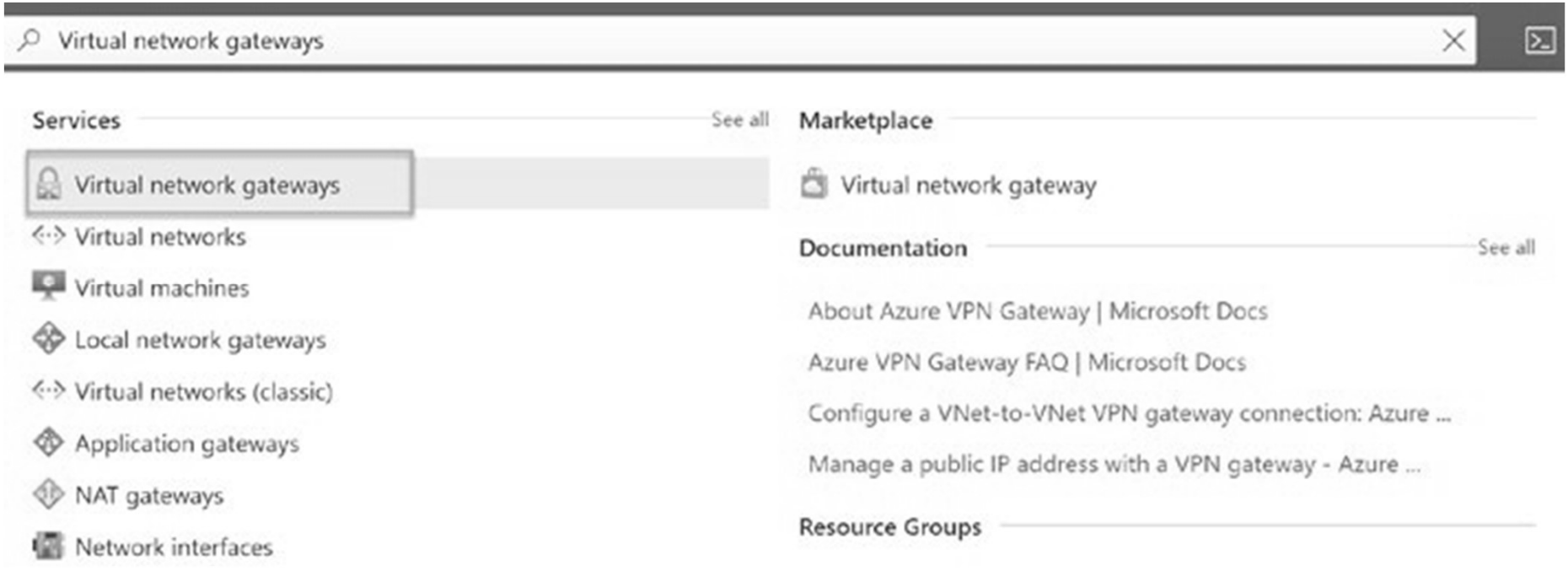
❖ Data in transit and data that's stored

- The data is traveling across carrier and data center networks and always takes the shortest available route.

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

❖ Azure VPN Gateways

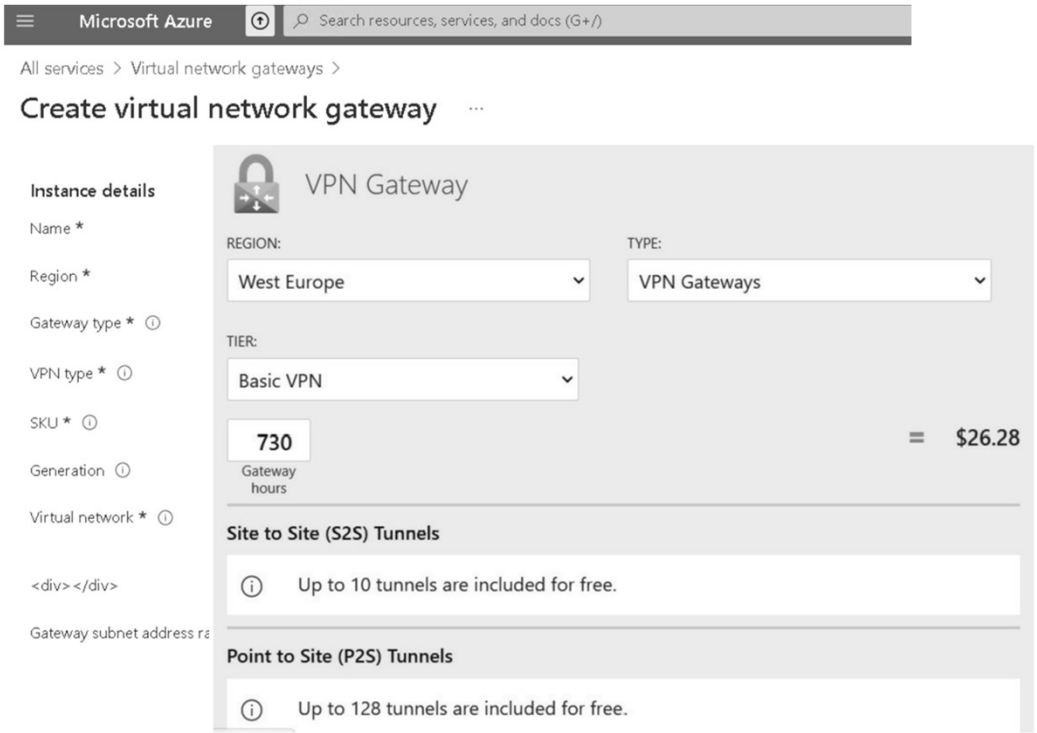
- **Virtual network gateways**



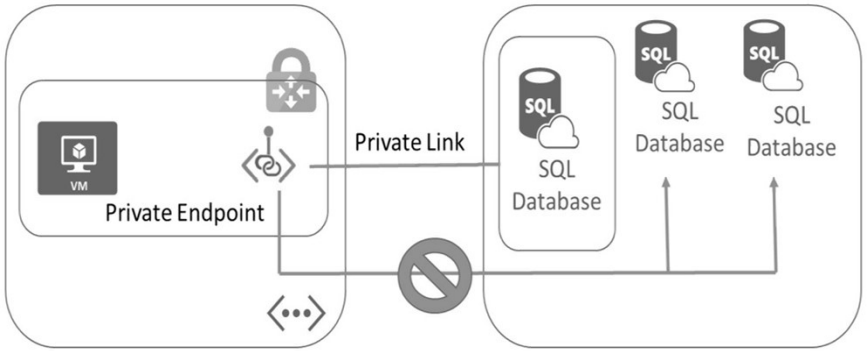
Source: https://portal.azure.com/

DAY 3. 하이브리드와 멀티 클라우드

- Technology strategy following business innovation
- Ordering the VPN Gateway functionality in the Azure cost model



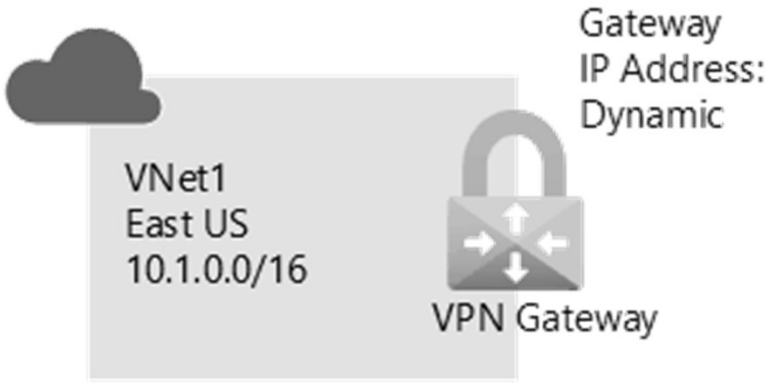
Private Link uses a private endpoint so that gateways with NAT translating from public to private addresses—are no longer required:



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.

❖ 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

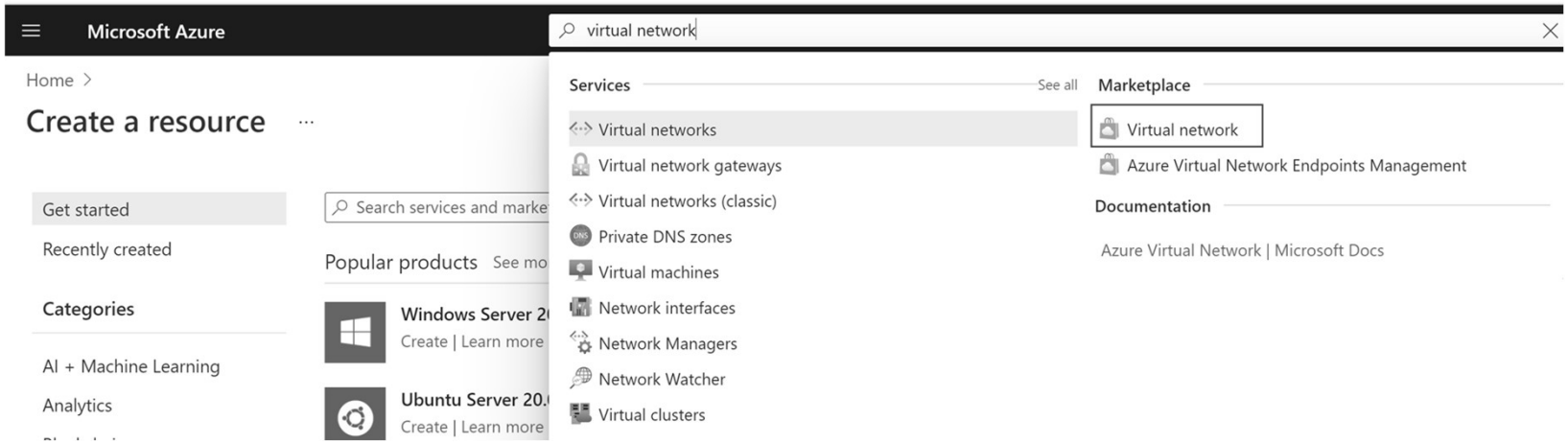


Source: https://learn.microsoft.com/en-gb/azure/vpn-gateway/tutorial-create-gateway-portal?WT.mc_id=APC-Virtualnetworkgateways

❖ Azure VPN Gateways

- **Create a virtual network**

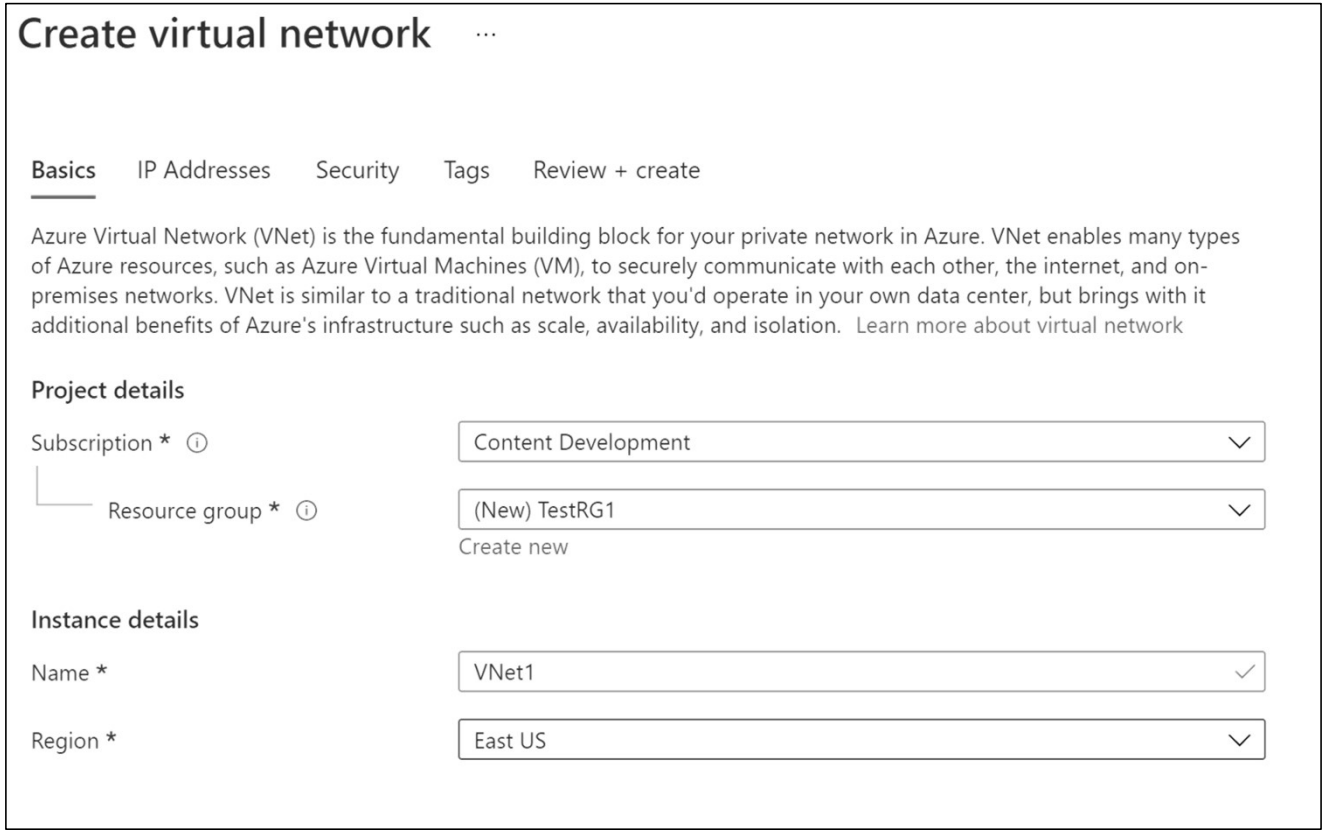
✓Resource group: TestRG1
✓Name: VNet1
✓Region: (US) East US
✓IPv4 address space: 10.1.0.0/16
✓Subnet name: FrontEnd
✓Subnet address space: 10.1.0.0/24



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

❖ Azure VPN Gateways

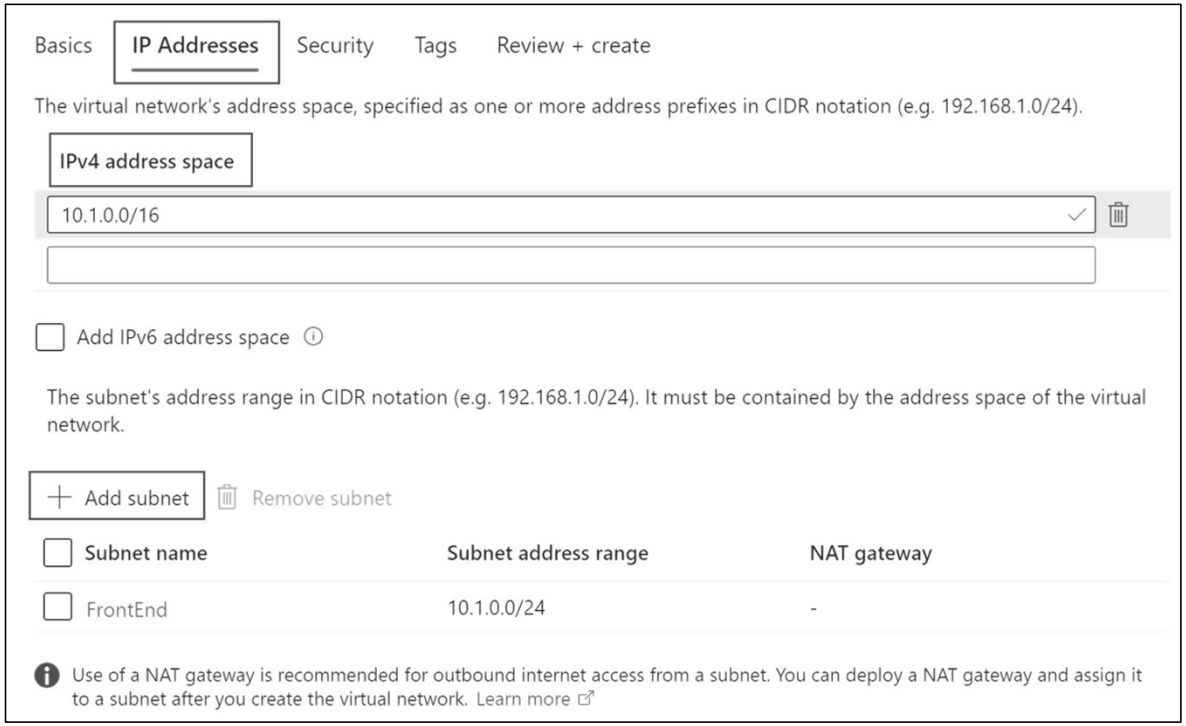
- **Create a virtual network**



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

❖ Azure VPN Gateways

- Select IP Addresses to advance to the IP Addresses tab

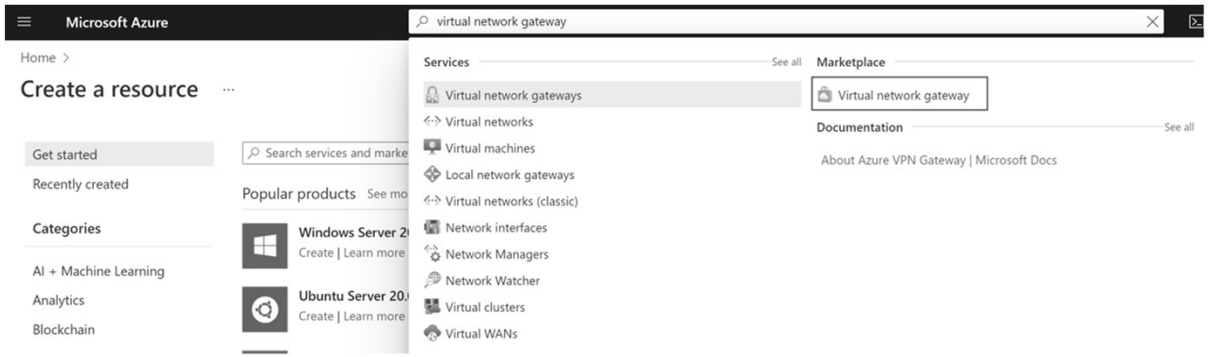


Source: https://learn.microsoft.com/en-gb/azure/vpn-gateway/tutorial-create-gateway-portal?WT.mc_id=APC-Virtualnetworkgateways

❖ Azure VPN Gateways

- **Creating virtual network gateway**

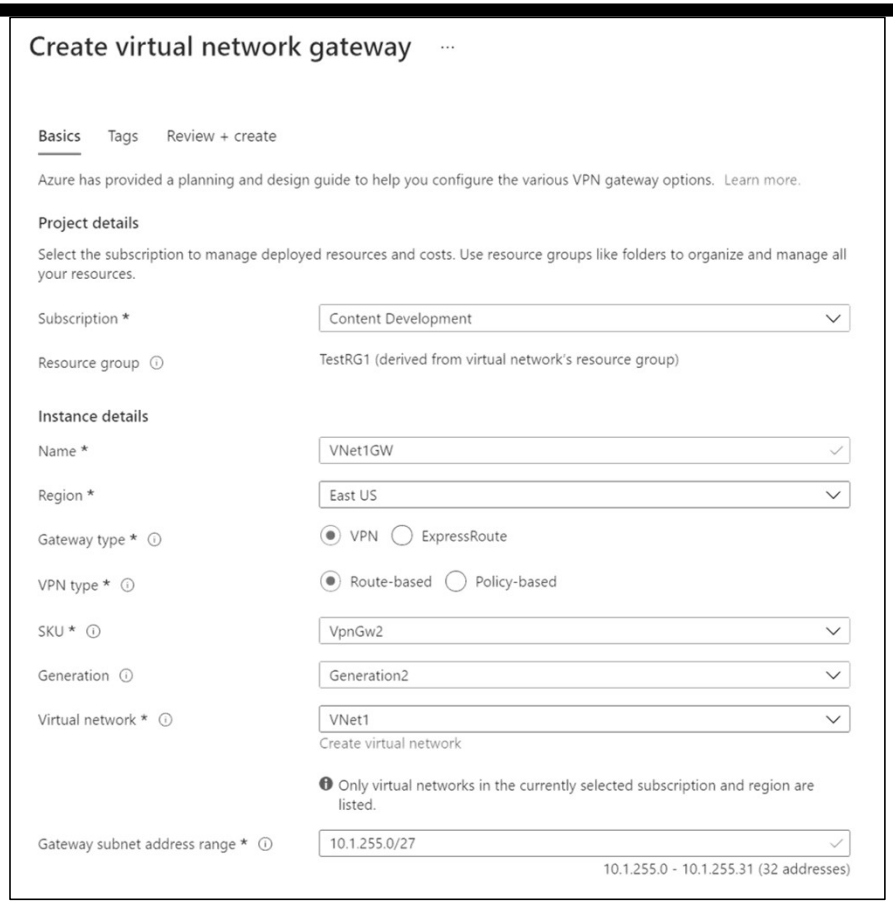
  ✓Name: VNet1GW
  ✓Region: East US
  ✓Gateway type: VPN
  ✓VPN type: Route-based
  ✓SKU: VpnGw2
  ✓Generation: Generation 2
  ✓Virtual network: VNet1
  ✓Gateway subnet address range: 10.1.255.0/27
  ✓Public IP address: Create new
  ✓Public IP address name: VNet1GWpip



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

❖ Azure VPN Gateways

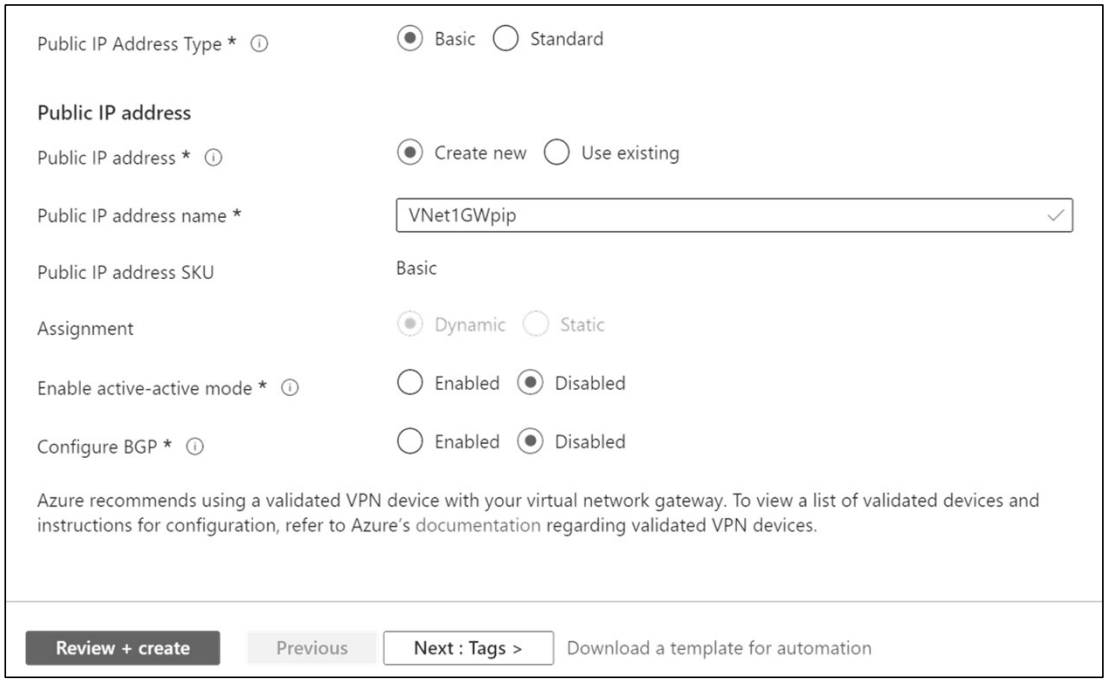
- **Creating virtual network gateway**
  - ✓Name: VNet1GW
  - ✓Region: East US
  - ✓Gateway type: VPN
  - ✓VPN type: Route-based
  - ✓SKU: VpnGw2
  - ✓Generation: Generation 2
  - ✓Virtual network: VNet1
  - ✓Gateway subnet address range: 10.1.255.0/27
  - ✓Public IP address: Create new
  - ✓Public IP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

❖ 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

❖ 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

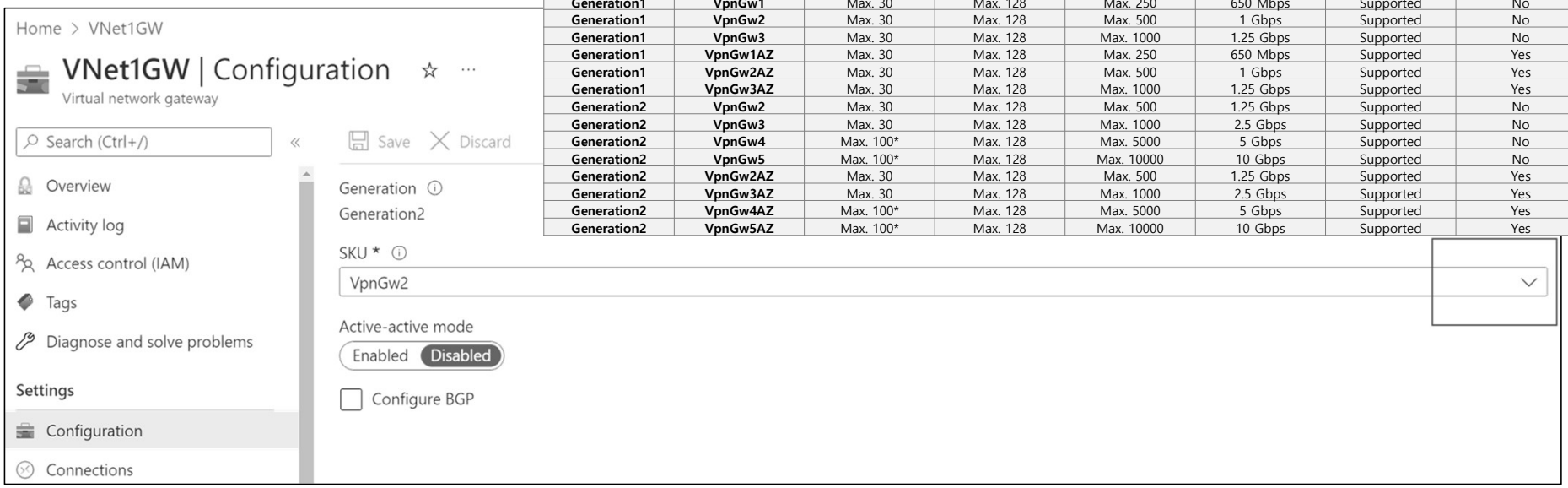
DAY 3. 하이브리드와 멀티 클라우드

❖ Azure VPN Gateways

- **Creating virtual network gateway**

✓Resize a gateway SKU

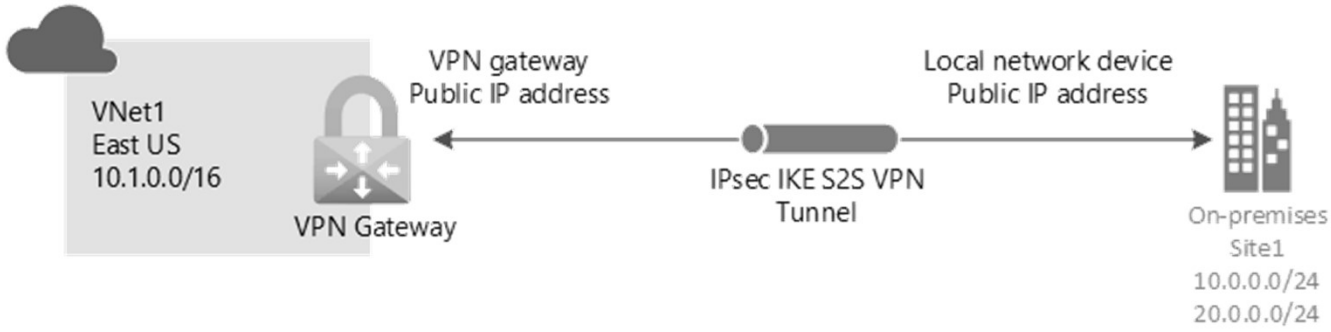
VPN Gateway Generation	SKU	S2S/VNet-to-VNet Tunnels	P2S SSTP Connections	P2S IKEv2/OpenVPN Connections	Aggregate Throughput Benchmark	BGP	Zone-redundant
Generation1	**Basic**	Max. 10	Max. 128	Not Supported	100 Mbps	Not Supported	No
Generation1	**VpnGw1**	Max. 30	Max. 128	Max. 250	650 Mbps	Supported	No
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

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

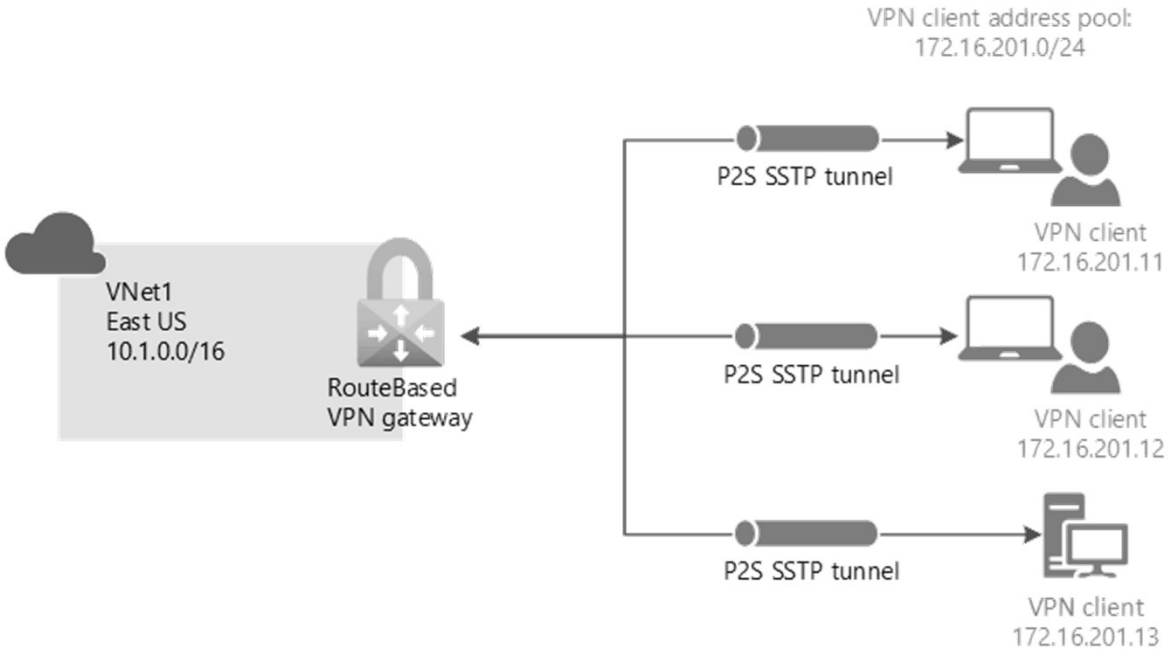
- **Create a site-to-site VPN connection in the Azure portal**
  - ✓Create a virtual network
  - ✓Create a VPN gateway
  - ✓Create a local network gateway
  - ✓Create a VPN connection
  - ✓Verify the connection
  - ✓Connect to a virtual machine



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

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

- **Creating virtual network gateway**
  - ✓View the public IP address

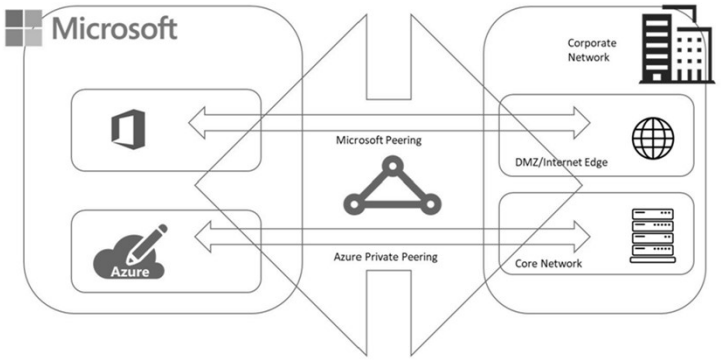


Source: https://learn.microsoft.com/en-gb/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal

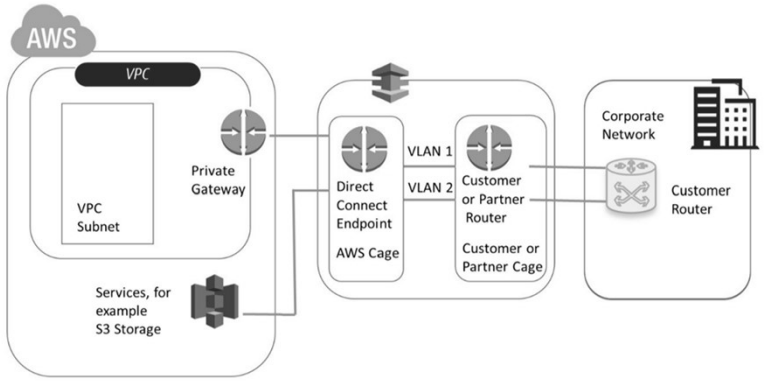
DAY 3. 하이브리드와 멀티 클라우드

❖ 전용선 서비스 연계

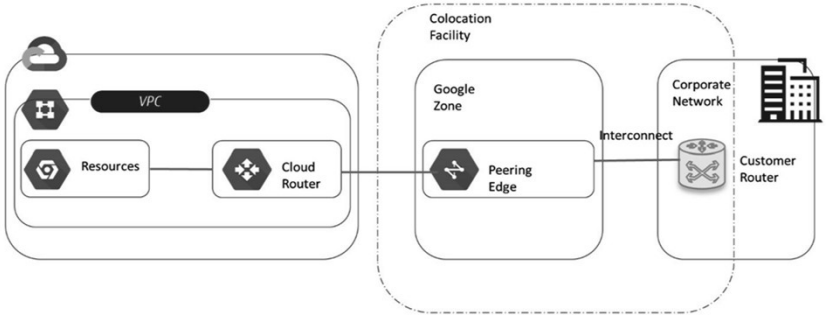
Microsoft's ExpressRoute concept



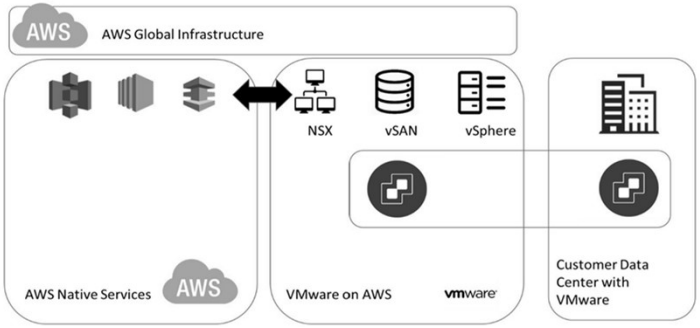
AWS' Direct Connect concept



Google's concept for Dedicated Interconnect



Concept for VMware on AWS



DAY 3. 하이브리드와 멀티 클라우드

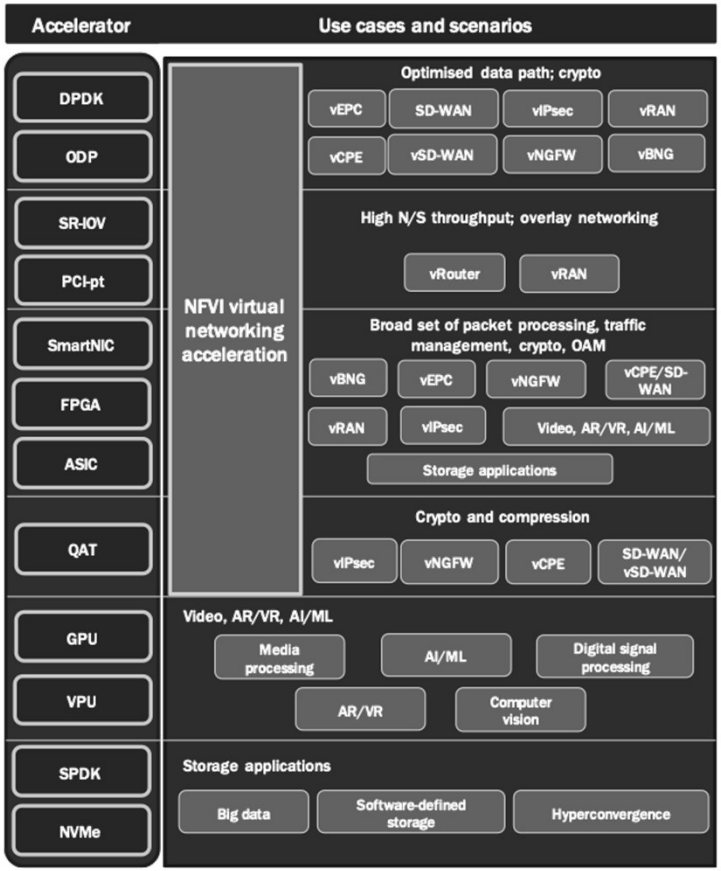
❖ Unlimited Data plan(Azure ExpressRoute 예)

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

DAY 3. 하이브리드와 멀티 클라우드

❖ Acceleration technologies and use cases

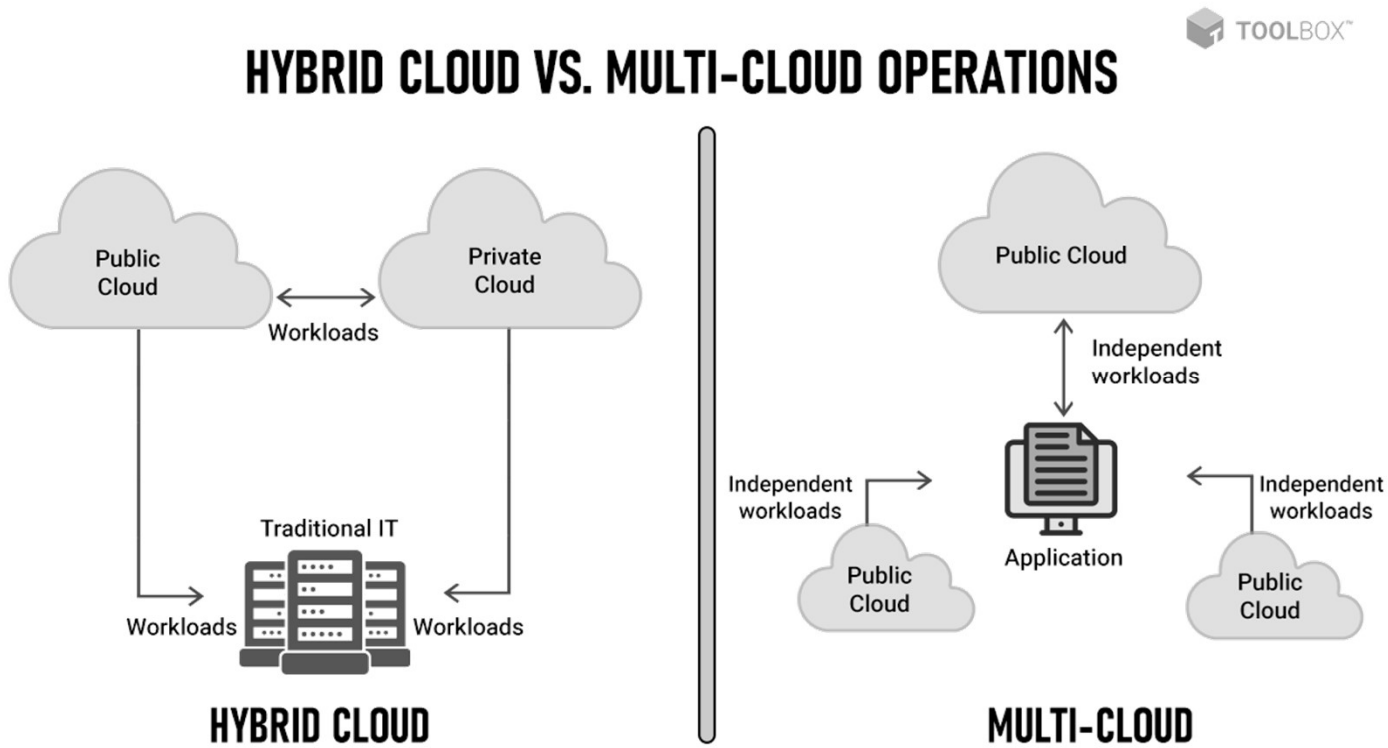
- 가상화를 위한 가속 기술
- DPDK
- SR-IOV
- SmartNIC
- FPGA
- ASIC
- QAT
- GPU
- DPU
- IPU
- NVMe



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

DAY 3. 하이브리드와 멀티 클라우드

❖ Multi-Cloud vs. Hybrid Cloud: 10 Key Comparisons

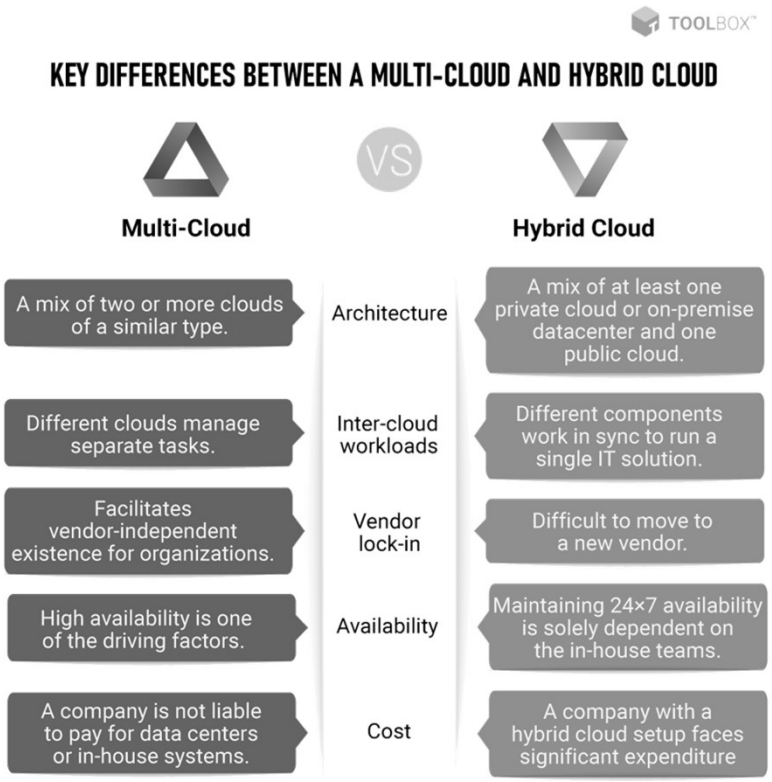


Source: https://www.spiceworks.com/tech/cloud/articles/multi-cloud-vs-hybrid-cloud/

DAY 3. 하이브리드와 멀티 클라우드

❖ Multi-Cloud vs. Hybrid Cloud: 10 Key Comparisons

Point of Comparison	Multi-Cloud	Hybrid Cloud
I. Architecture	Multi-cloud architecture is a mix of two or more clouds of a similar type. There is no inter-cloud communication between the clouds. Also, multi-cloud lacks a single identity management system (IdM), unified logging, cloud monitoring, and alerting (LMA) stacks, or an integrated network. In a multi-cloud environment, all kinds of data can be stored on multiple public clouds.	Hybrid cloud architecture is always a mix of at least one private cloud or on-premise datacenter and one public cloud. The involved infrastructural components share a single identity management system, unified logging, cloud monitoring, and alerting stacks, in addition to integrations between internal networks. Hybrid clouds support high levels of interconnectivity. This allows the public environment to act as an extension of the private cloud system. Additionally, in hybrid cloud environments, on-premise data centers or private clouds are used to store critical data. Here, public clouds do not keep any valuable data records.
II. Inter-cloud workloads	Different clouds in a multi-cloud setup manage separate tasks. As such, data and associated processes operate independently of each other.	Different components in a hybrid cloud setting work in sync to run a single IT solution. As a result, data and processes intersect with one another.
III. Vendor lock-in	Multi-cloud facilitates vendor-independent existence for organizations as they don't have to maintain a locked state with a single cloud provider. Multiple public clouds managing separate workloads allow vendors to be changed easily and quickly. Besides, an enterprise can change cloud providers based on upcoming technological opportunities, service expenses, technical requirements, or geographic location. Multi-cloud avoids vendor lock-in, allowing the business to respond, adjust, and adapt to dynamic market changes with agility.	In a hybrid setting, organizations customize the underlying environments that work in sync to fit the use case under consideration. As such, there is a requirement for high-level integration between an on-premise system and the public cloud. Such an arrangement makes it even more difficult to move to a new vendor. This can also cause significant downtime if at all vendor transition takes place.
IV. Availability	High availability is one of the driving factors of a multi-cloud environment. It gives enterprises a reliable cloud backup system with an additional standby facility. This implies that if one of the vendors has a temporary issue, the entire workload can be shifted to another vendor's cloud. As a result, the end users do not experience any downtime issues. Additionally, a multi-cloud setting enables companies to set up individual public clouds nearby to users' locations. This solves the latency issue significantly for users.	In a hybrid cloud system, maintaining 24×7 availability is solely dependent on the in-house teams as most of the workload operates on-premise or on the private cloud. Consider a scenario where an app experiences a sudden spike in traffic, and there's a public cloud failure. In such cases, cloud bursting isn't feasible due to public cloud problems. In such cases, the hybrid system can be problematic as downtime is inevitable here. Hence, a hybrid cloud setup cannot provide any solution other than evolving into a multi-cloud system.
V. Cost	In a multi-cloud setting, a company is not liable to pay for data centers or in-house systems. However, the concerned teams must be well aware of the cloud computing expenses to avoid unnecessary expenditure.	A hybrid system with a private cloud does not face any issue of over expenditure as the system only has a single public cloud. However, a company planning to set up a private cloud system must also hire qualified staff to seamlessly manage the hybrid environment. The company is also responsible for equipment and maintenance costs, apart from the staff and public cloud expenses



Source: https://www.spiceworks.com/tech/cloud/articles/multi-cloud-vs-hybrid-cloud/


THANK
YOU