



# 성공적인 하이브리드 클라우드를 위한 Azure 네트워크와 서비스

GLOBAL AZURE VIRTUAL 2020



고재성

Microsoft MVP

Mail

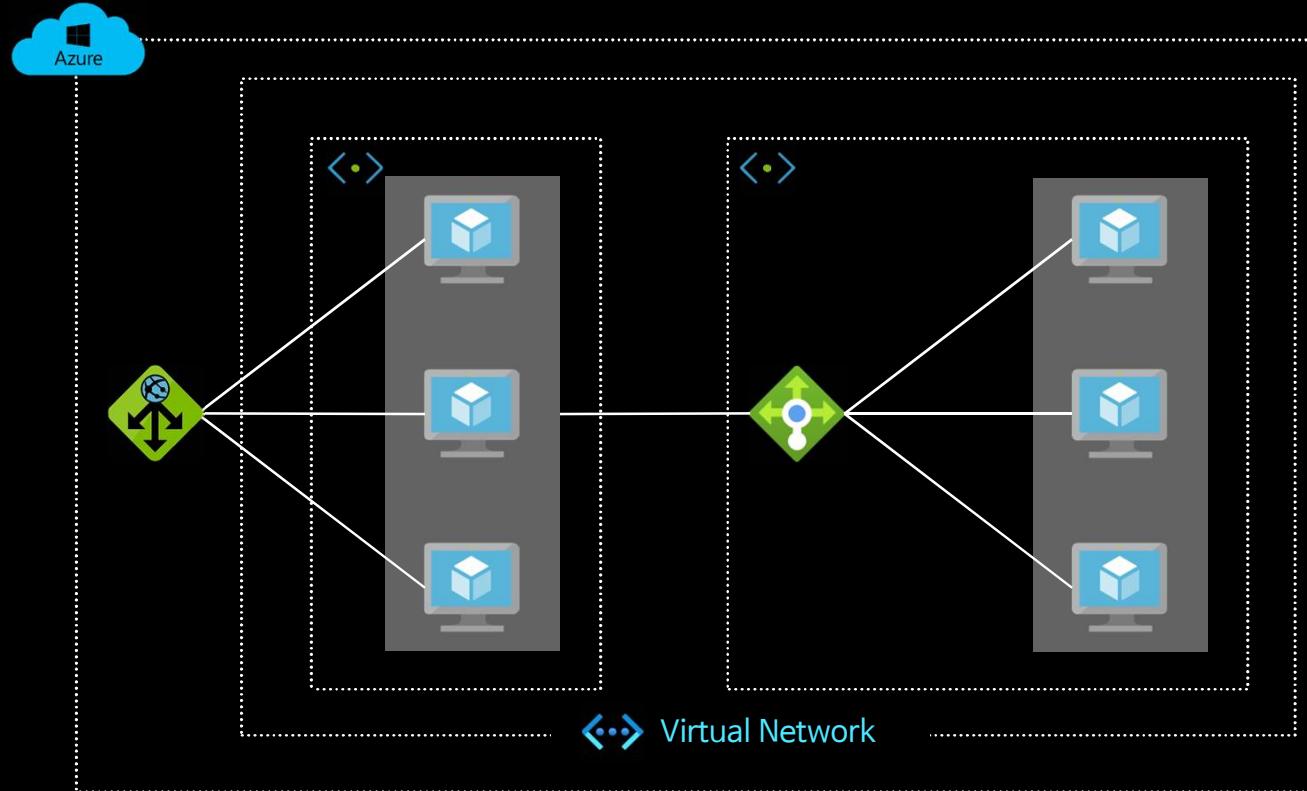
ZIGI@kakao.com

Blog

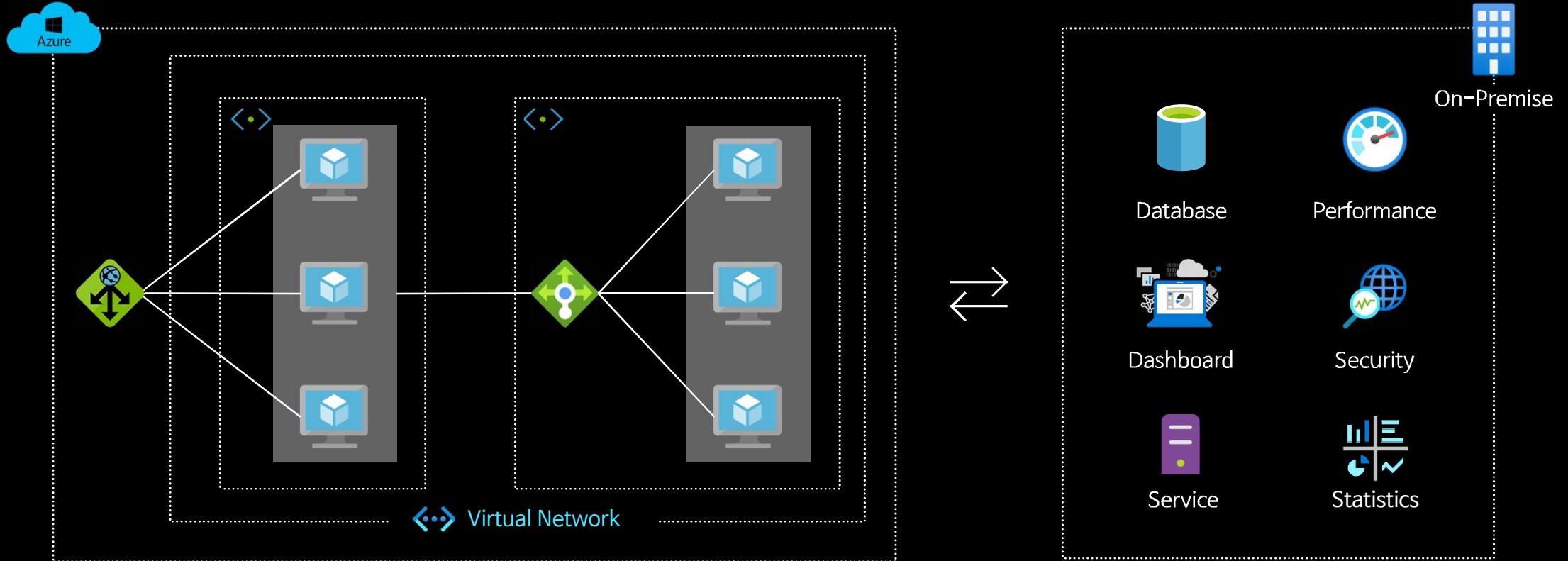
ZIGISPACE.NET

네트워크 전문가 따라잡기 커뮤니티

# Public Cloud를 이용한 서비스 구축



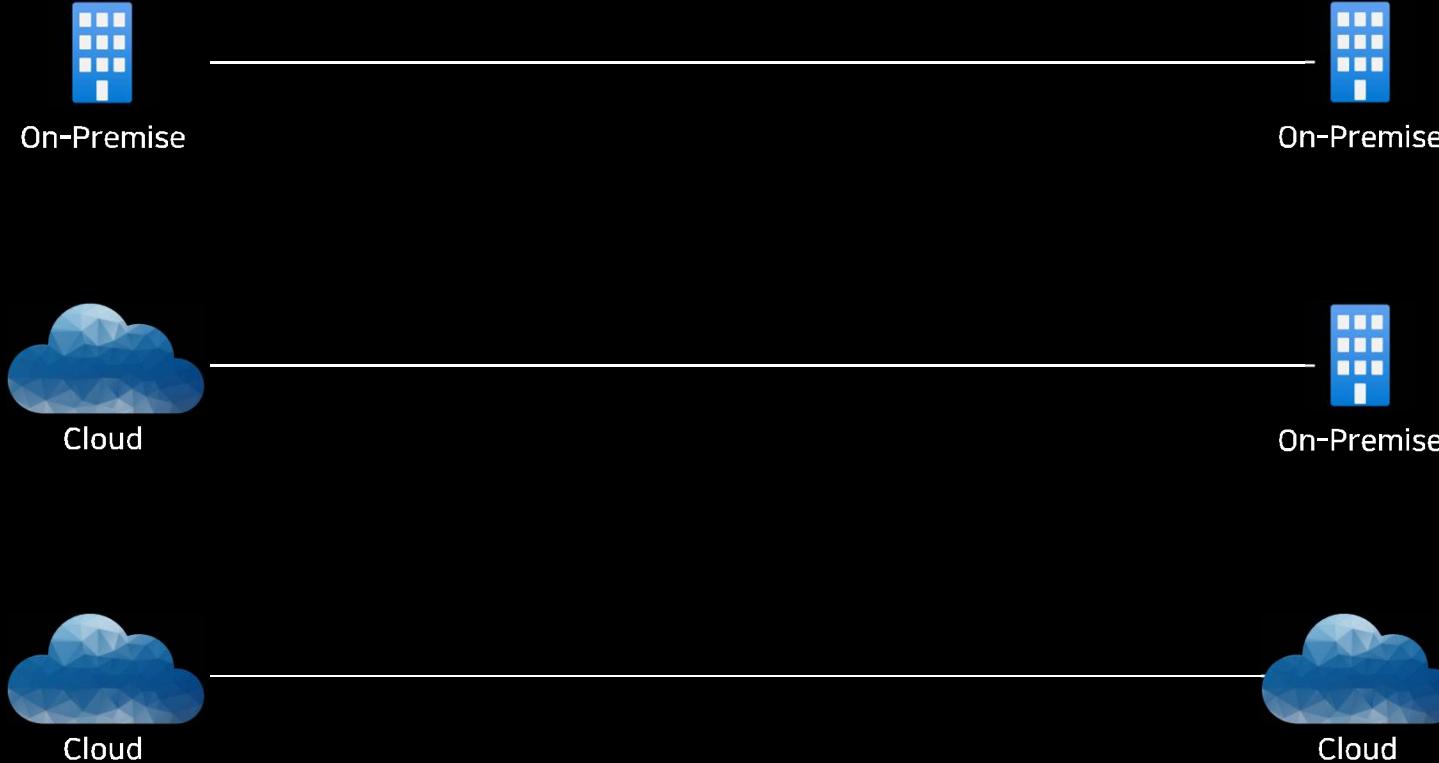
# Hybrid Cloud를 위한 요건



# 쉽게 생각해서 Hybrid Cloud는?



사실...



# Hybrid Cloud도 결국..



# Azure Virtual Network

# <...>Virtual Network

Azure 가상 네트워크 (VNet)



Address Space



Subnet (Address range)

Create virtual network

**Subnet**

Name **\***  
default

Address range **\*** ⓘ  
10.1.0.0/24  
10.1.0.0 - 10.1.0.255 (256 addresses)

DDoS protection ⓘ  
 Basic  Standard

Service endpoints ⓘ  
 Disabled  Enabled

Firewall ⓘ  
 Disabled  Enabled

Add an IPv6 address space ⓘ

Subscription **\***  
Microsoft Azure 스폰서쉽 (c73578f0-3...)

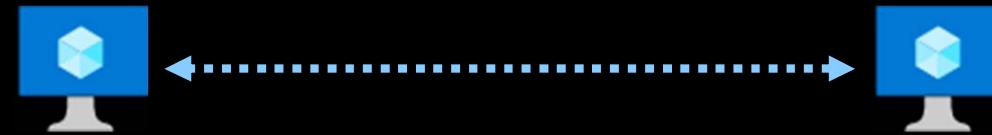
Resource group **\***  
Select existing...   
Create new

Location **\***  
(Asia Pacific) Korea Central

**Create** Automation options

# Azure Network 설계 고려사항

IP Address & Subnet



✓ Private IP Address

✓ Non-overlapping IP Address Design

✗ Can't modify Address Space in using

✓ Various subnet types

• 서비스에 요건에 따른 최적화 된 IP Address와 Subnet 설계

# IP Address

Public & Private

Private IP Address



Public IP Address

# IP Address

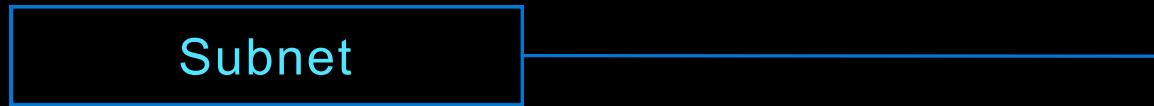
Private IP Address

	Private Network	Subnet Mask	Bit	Address Range
RFC 1918	10.0.0.0	255.0.0.0	8	10.0.0.0 - 10.255.255.255
	172.16.0.0	255.240.0.0	12	172.16.0.0 - 172.31.255.255
	192.168.0.0	255.255.0.0	16	192.168.0.0 - 192.168.255.255
RFC 6598	100.64.0.0	255.255.192.0	10	100.64.0.0 - 100.127.255.255

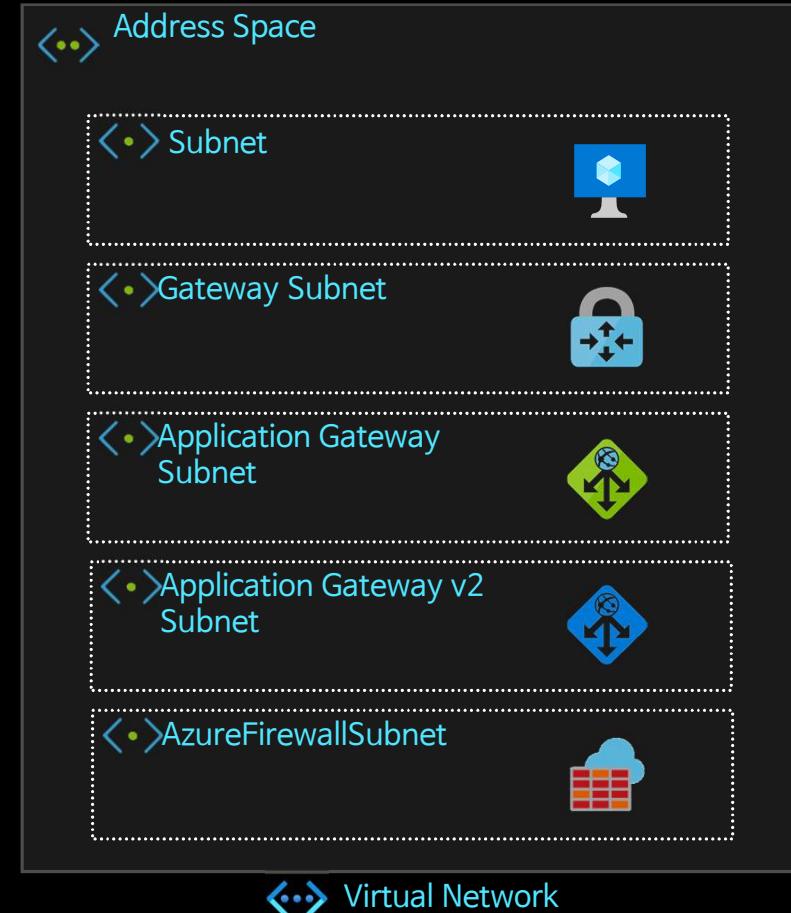
※ IANA - Reserved IPv4 Prefix for Shared Address Space

# Azure Subnet

다양한 서브넷



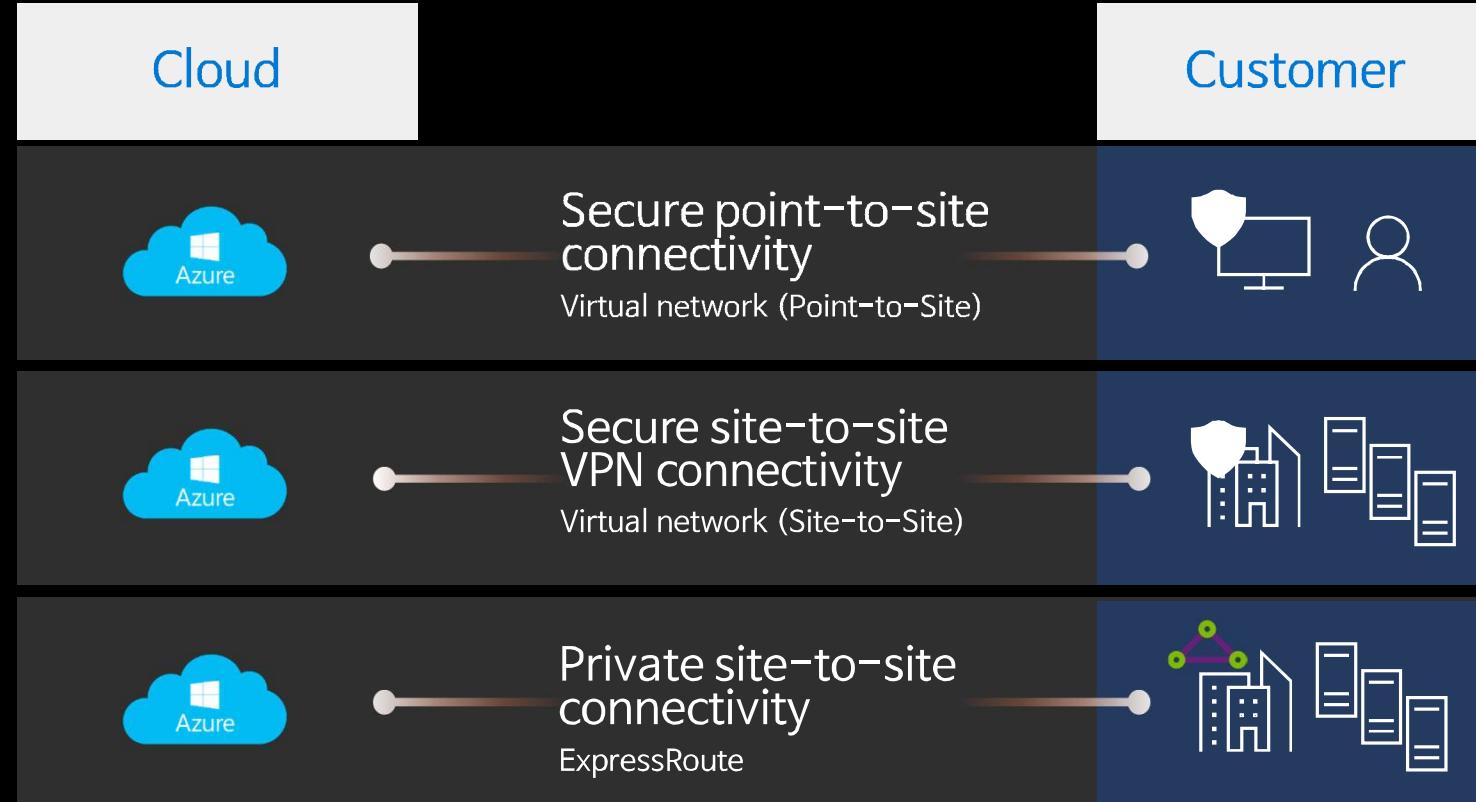
- (일반) 서브넷
- Gateway 서브넷
- Application Gateway 용 서브넷
  - ※ Application Gateway v1/v2 혼용 불가
- Azure Firewall 서브넷



# Hybrid Cloud

# Hybrid Cloud

하이브리드 클라우드 구성

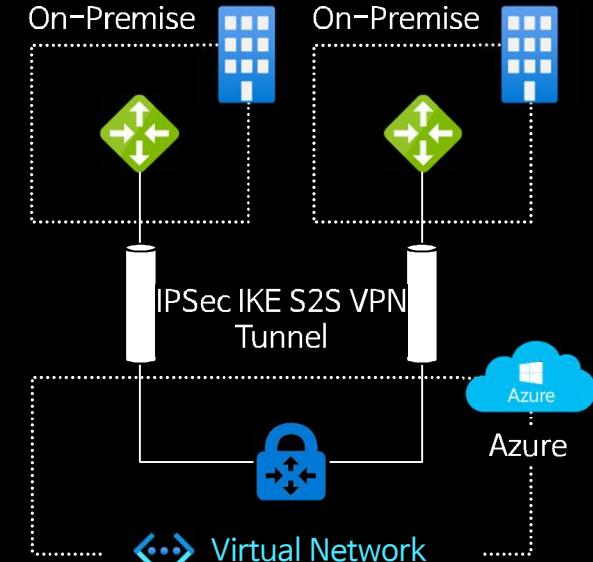


# Virtual Private Network (VPN)

## Site to Site VPN

### S2S VPN

- 일반 인터넷 망을 VPN Gateway를 통해 On-Premise와 VNet간을 연동 및 전송되는 트래픽 암호화를 수행
- IPSec Protocol 사용
- RouteBased 방식의 Routing 권고
- Basic, VpnGw1~5까지의 SKU 제공<sup>1)</sup>
- VpnGw에 대한 영역(AZ) 중복을 위한 별도 SKU 제공<sup>2)</sup>
- 다양한 암호화를 제공하며, 암호화에 따른 용량 상이



1) SKU별 지원되는 VPN 터널 수량 및 처리 가능한 Traffic, Packet 수량이 상이함.

2) 한국 리전에서는 영역 중복 게이트웨이가 현재 지원되지 않음('20.4 현재)

# Virtual Private Network (VPN)

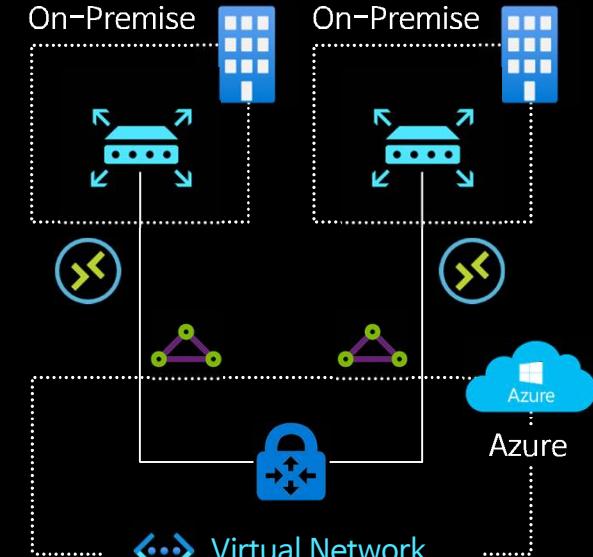
## VPN Gateway

Generation	SKU	Tunnel	Aggregate Throughput Benchmark
Gen 1	Basic	최대 10 개	100 Mbps
	VpnGw1		650 Mbps
	VpnGw2	최대 30 개	1 Gbps
	VpnGw3		1.25 Gbps
Gen 2	VpnGw2		1.25 Gbps
	VpnGw3		2.5 Gbps
	VpnGw4	최대 30개	5 Gbps
	VpnGw5		10 Gbps

# ExpressRoute

## ExpressRoute

- Azure와 On-Premise 간의 연결을 위한 전용선 서비스
- 빠른 속도, 서비스 품질보장, 강화된 보안 제공
- BGP 사용 필수
- 다양한 대역폭 옵션 제공 및 동적 조정 가능<sup>1)</sup>
- Standard, High/Ultra Performance SKU 제공<sup>2)</sup>
- 서비스 안정성을 위해 모든 피어링 위치는 이중화
- Azure 서비스 및 Office 365 서비스 액세스 가능<sup>3)</sup>



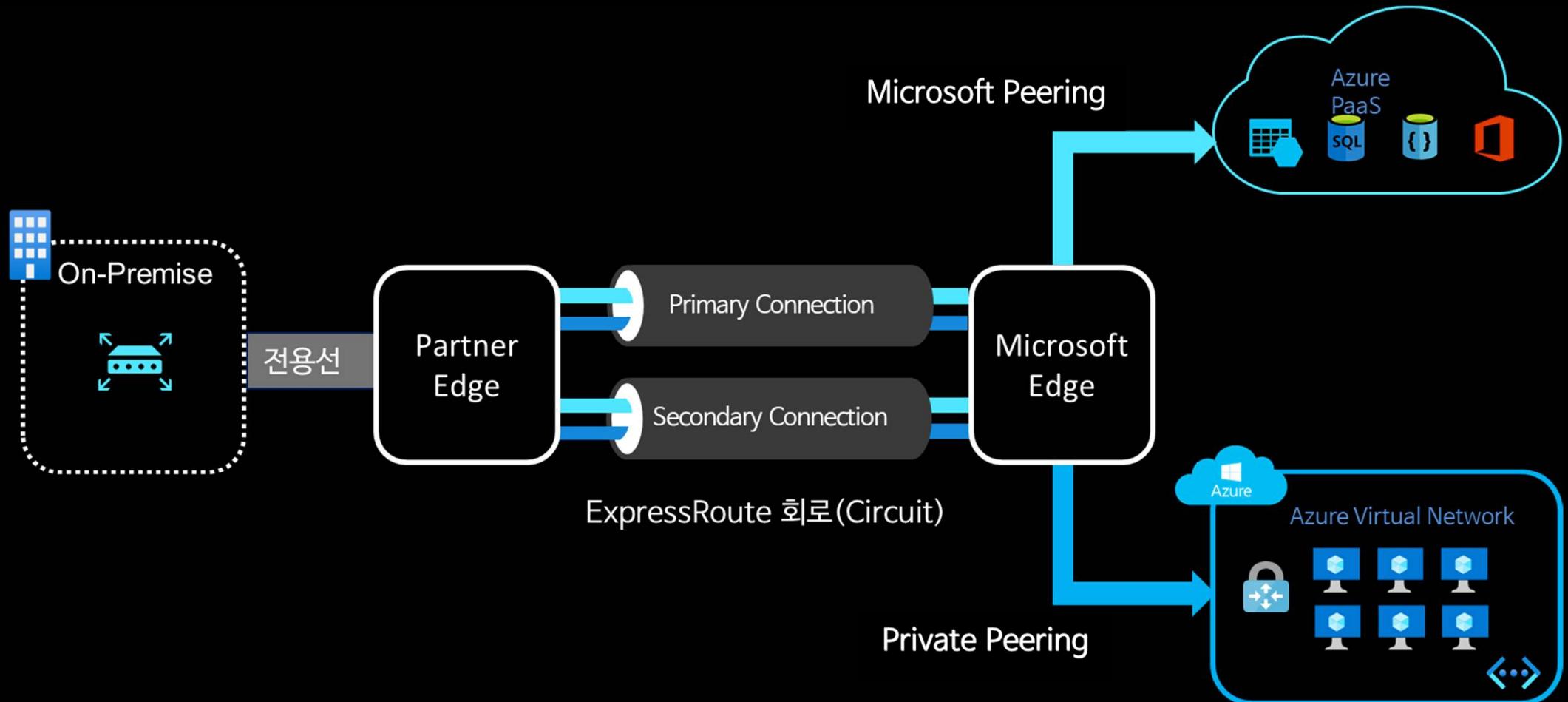
1) 제공되는 대역폭 : 50M, 100M, 200M, 500M, 1G, 2G, 5G, 10G

2) SKU별 지원되는 Bandwidth, PPS, CPS가 상이함.

3) Microsoft Peering을 통한 연동

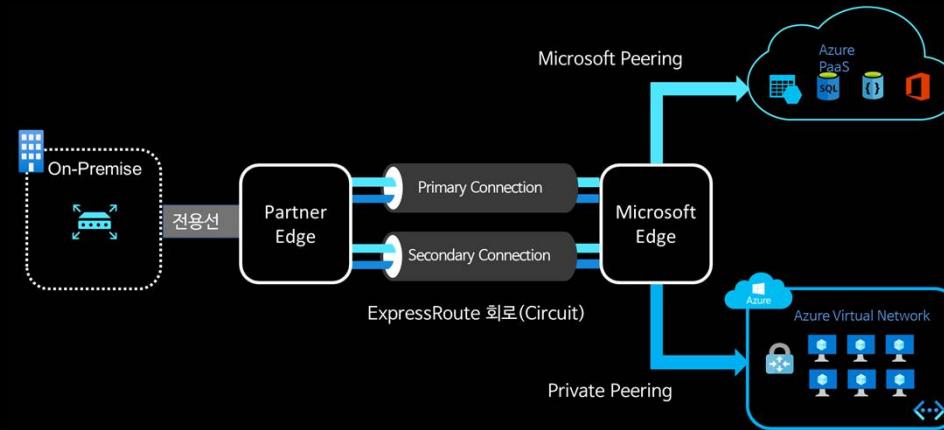
# ExpressRoute

ER 연동 방식



# ExpressRoute

ER 연동 방식



Microsoft Peering

Azure PaaS, MS SaaS 연동

공인 AS / IP로만 연동 가능

Private Peering

Virtual Network 연동

사설 AS / IP로 연동 가능

# ExpressRoute

## ER Gateway

SKU	Mbps (Megabits per Second)	PPS (Packets per Second)	CPS (Connection per Second)
Basic (deprecated)	500	-	-
Standard (표준)	1,000	100,000	7,000
High Performance (고성능)	2,000	250,000	14,000
Ultra Performance (울트라 퍼포먼스)	10,000	1,000,000	28,000

# ExpressRoute

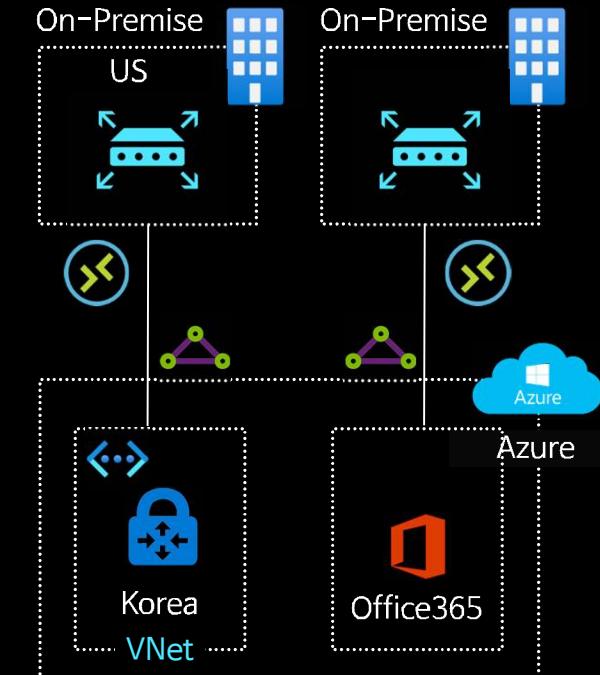
Circuit SKU

## Standard

- ExpressRoute의 표준 사양

## Premium

- Private Peering용 Routing Table 경로 ( $4K \rightarrow 10K$ )
- Circuit에 연결 가능한 가상 네트워크 수( $10 \rightarrow 100$ )<sup>1)</sup>
- Office 365 연결
- Global connectivity 제공



1) Premium의 경우 Circuit 대역폭에 따라 연결 가능한 가상 네트워크 수가 달라짐(최소 20 ~ 최대 100)

# ExpressRoute

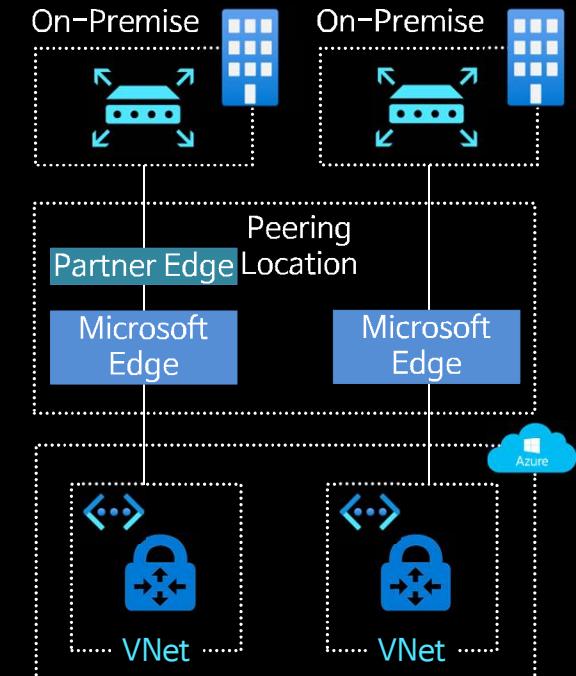
## ExpressRoute Direct

### ER-Direct

- Azure Peering Location에서 Microsoft Edge에 직접 연동
- 10G/100G 인터페이스 제공<sup>1)</sup>
- Storage/Cosmos DB와 같은 대규모 데이터 수집 시 사용
- Standard / Premium 이외에 Local Type 추가 지원

### ER-Local

- Peering Location 인근의 Azure regions만 연결 가능
- 데이터 전송 비용 무 과금



1) 실제 사용하기 위한 Circuit는 하위 속도 선택 가능

# ExpressRoute

무제한 데이터 요금제

대역폭	Local	Standard	Premium
50 Mbps	N/A	686,037	798,502
100 Mbps	N/A	1,383,320	1,580,134
200 Mbps	N/A	2,586,695	2,924,090
500 Mbps	N/A	5,848,180	6747,900
1 Gbps	1,799,440	9,784,455	11,415,198
2 Gbps	2,811,625	19,568,910	22,099,373
5 Gbps	4,386,135	46,110,650	49,484,600
10 Gbps	6,747,900	92,221,300	95,595,250

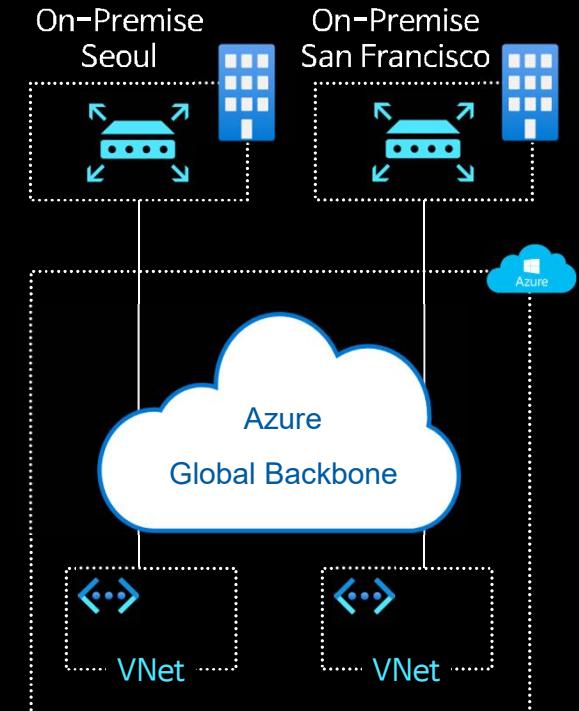
※ 월 730시간 기준 금액

# ExpressRoute

Global Reach

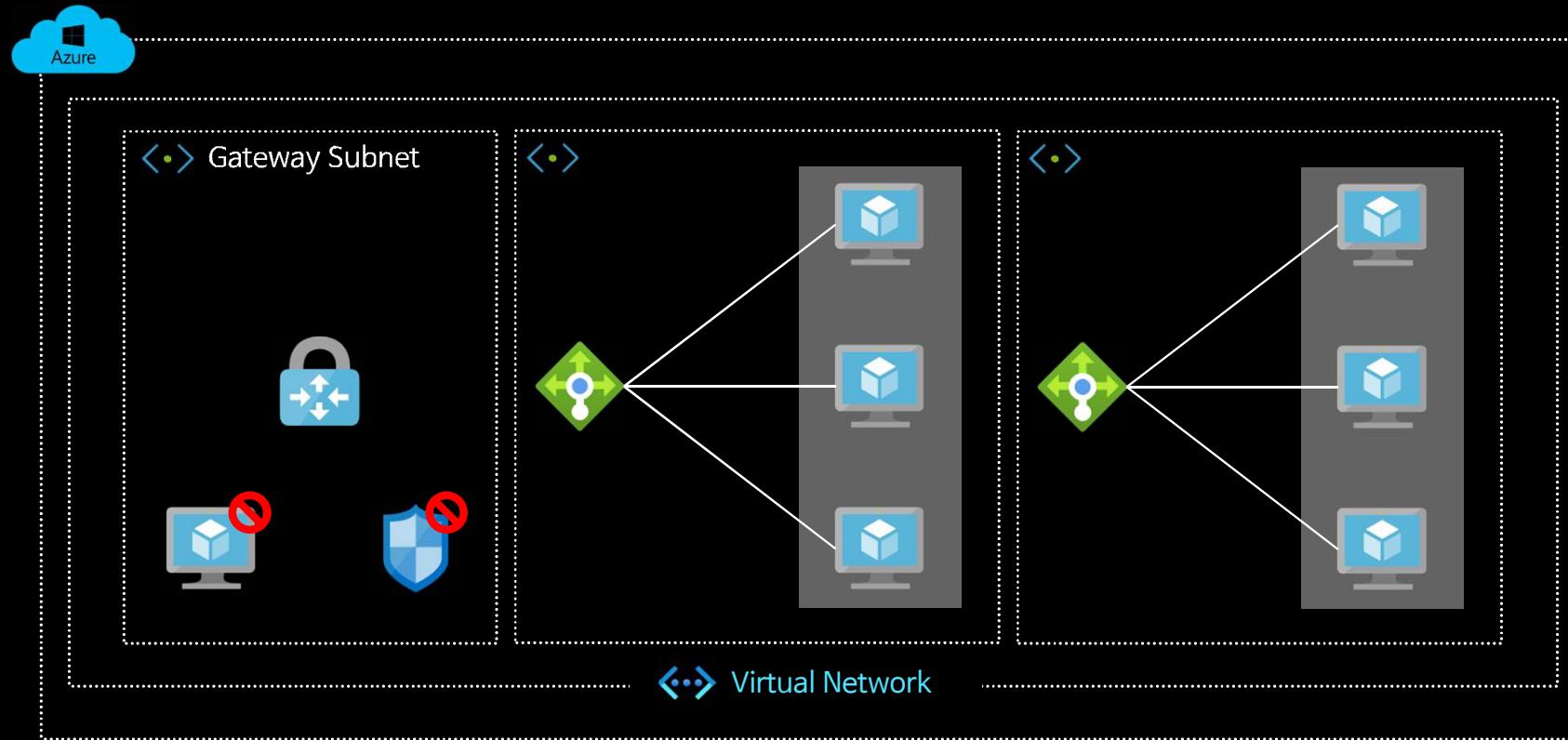
## Global Reach

- Microsoft Global Network를 통해서 Express-Route가 연결된 On-Premise 간의 네트워크를 연결
- ExpressRoute Circuit이 동일한 지리적 리전 인 경우 Standard로 연결 가능하며, 다른 지리적 리전 인 경우 Premium으로 연결해야 함.
- ExpressRoute Local에서는 지원하지 않음



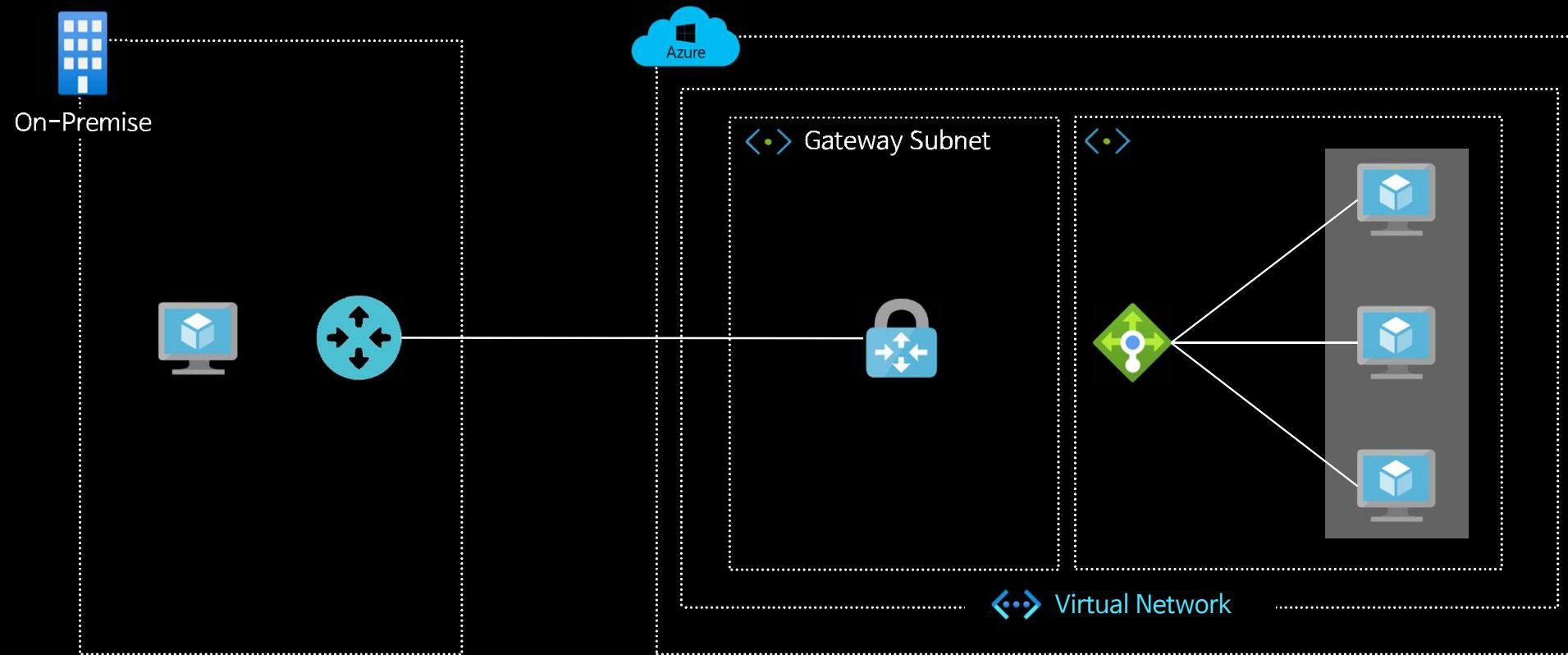
# Gateway Subnet

게이트웨이 서브넷



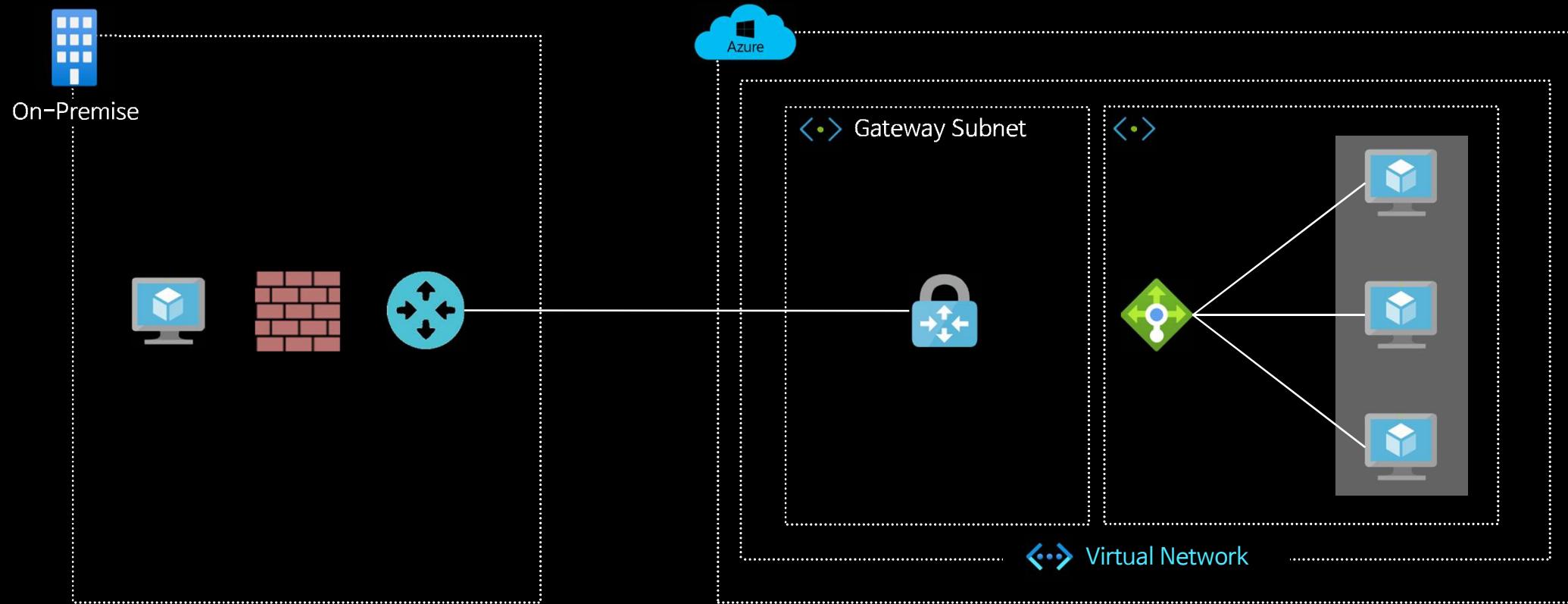
# Security Architecture

# Hybrid Cloud



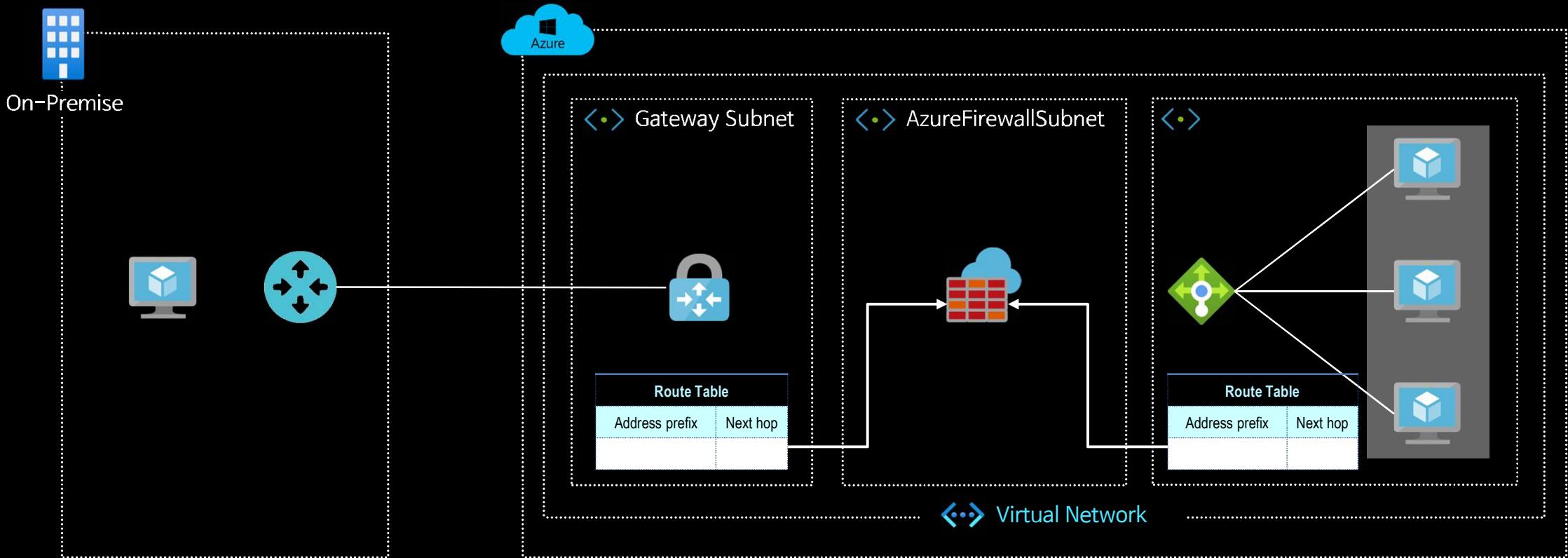
# Hybrid Cloud Security

On-Premise Firewall



# Security Hybrid Cloud

Azure Firewall

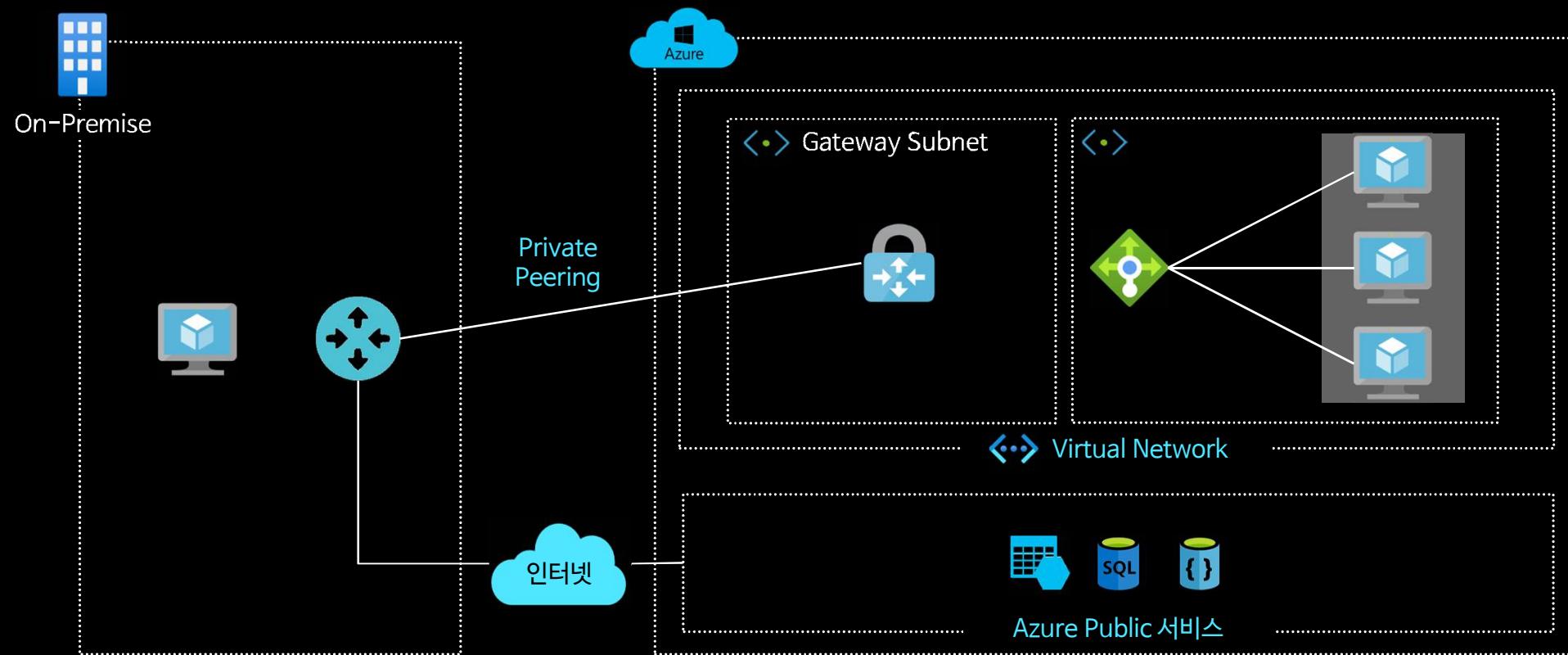


# Azure Public Service

사용하기

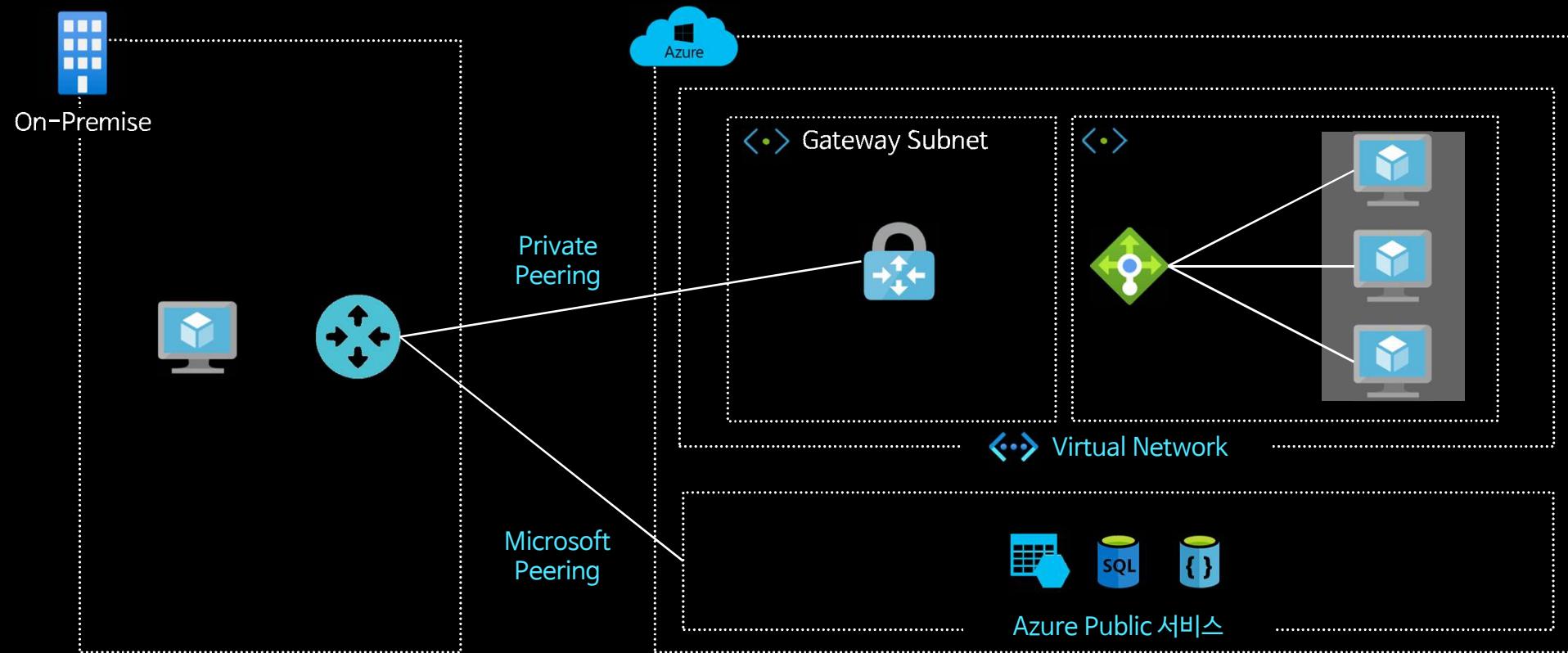
# On-Premise에서 Azure Public 서비스 사용

인터넷



# On-Premise에서 Azure Public 서비스 사용

Microsoft Peering



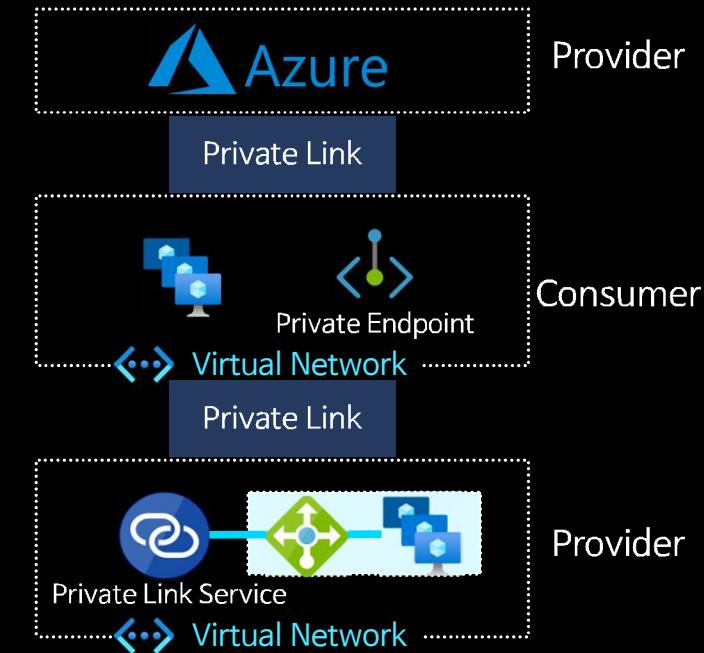
# Azure Private Link

# Private Link

Highly secure and private connectivity to Azure services

## Private Link

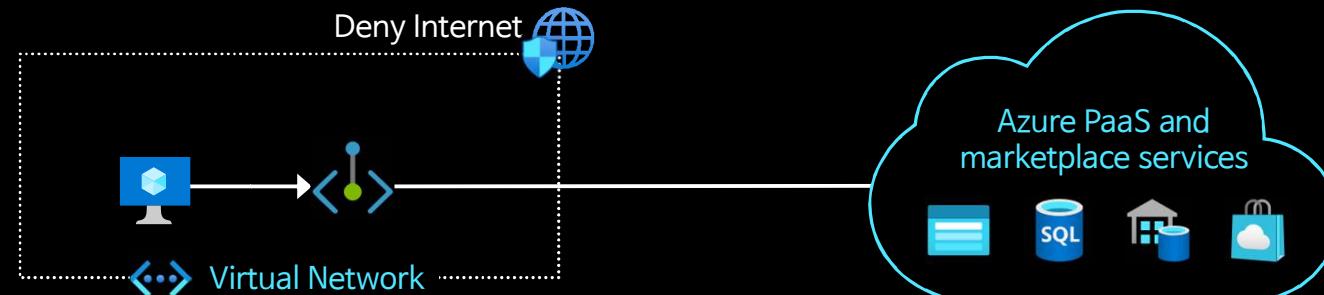
- Azure 가상 네트워크의 Private Endpoint를 이용해서 Azure PaaS Service(Azure Storage, Cosmos DB, SQL Database 등)와 Azure에 올린 사용자/파트너 서비스에 접근 할 수 있도록 하는 서비스
- Private Link를 이용하는 경우 Azure 가상 네트워크는 인터넷 경로를 사용하지 않고, Microsoft Backbone 네트워크를 사용



# Private Link

## Private Endpoints

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

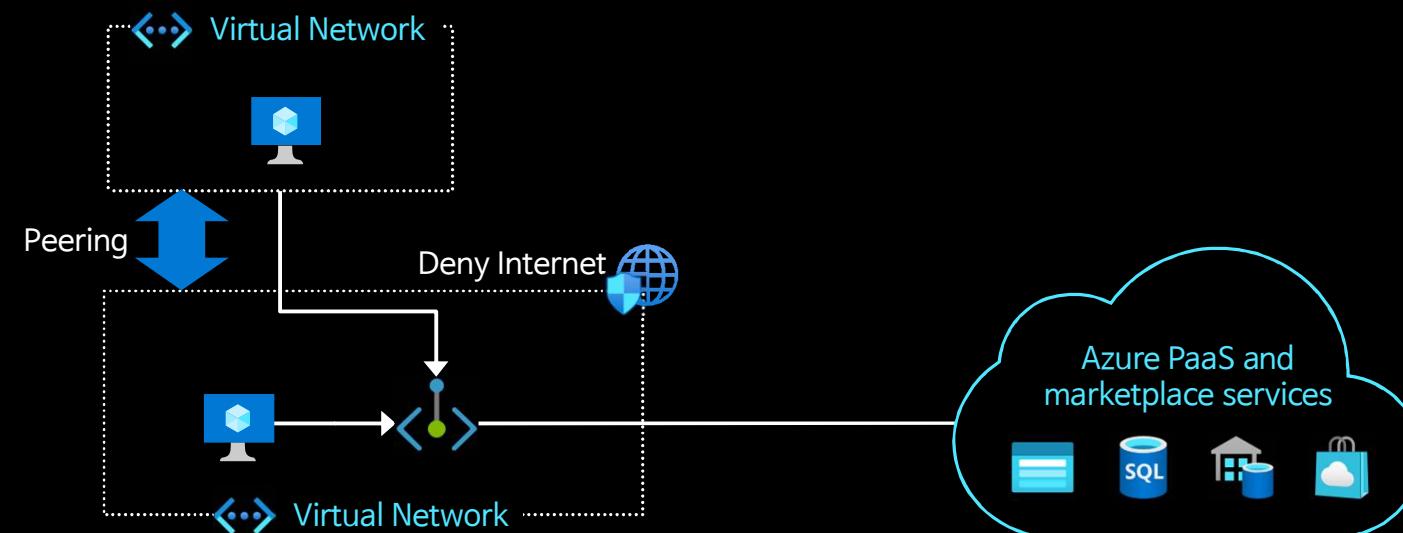


# Private Link

Private Link를 이용하여 Peered Networks에서 서비스 호출

## Private Endpoints

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

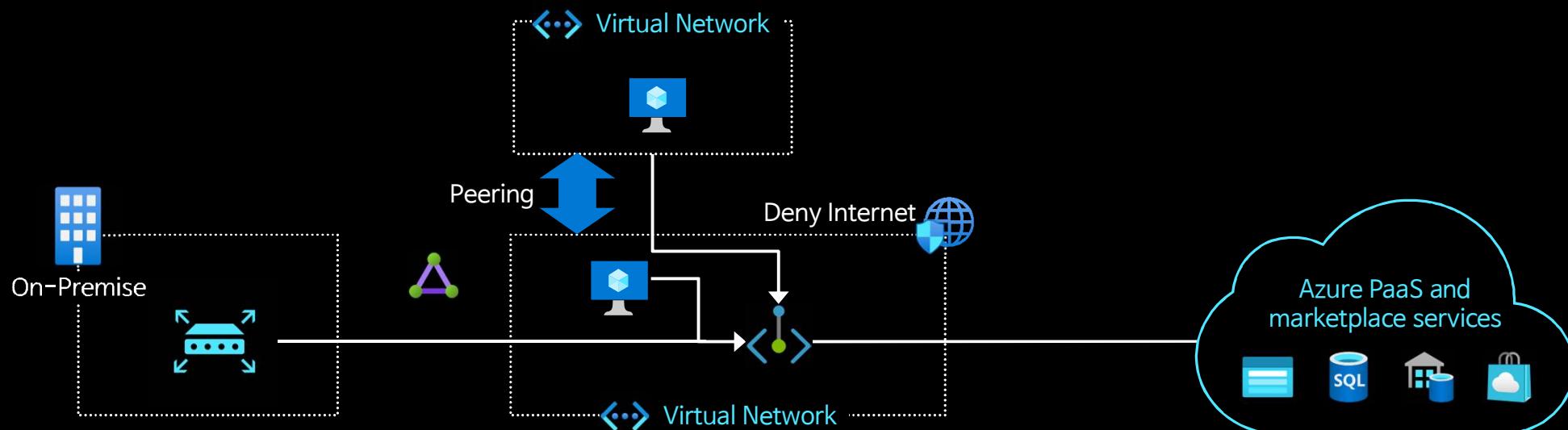


# Private Link

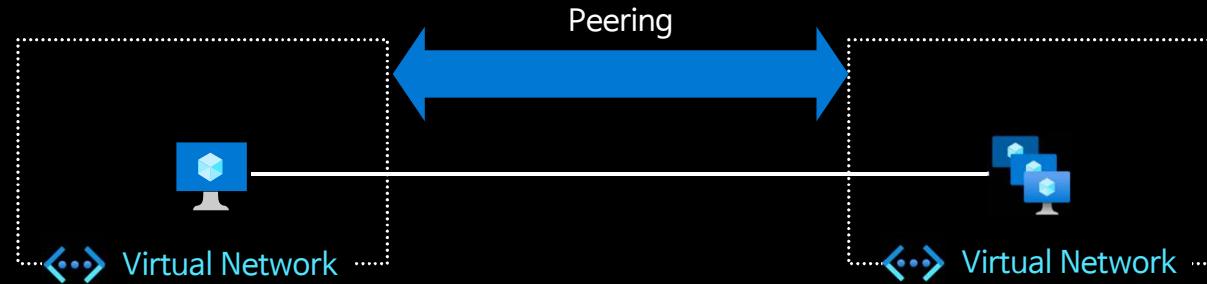
Private Link를 이용하여 On-Premise에서 서비스 호출

## Private Endpoints

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



# Virtual Network 간의 서비스 호출



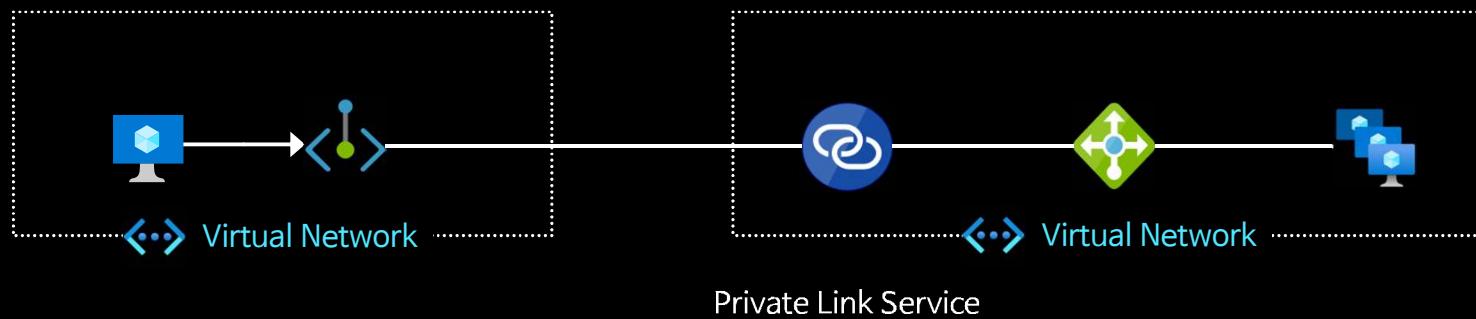


# Private Link

Private Link Service

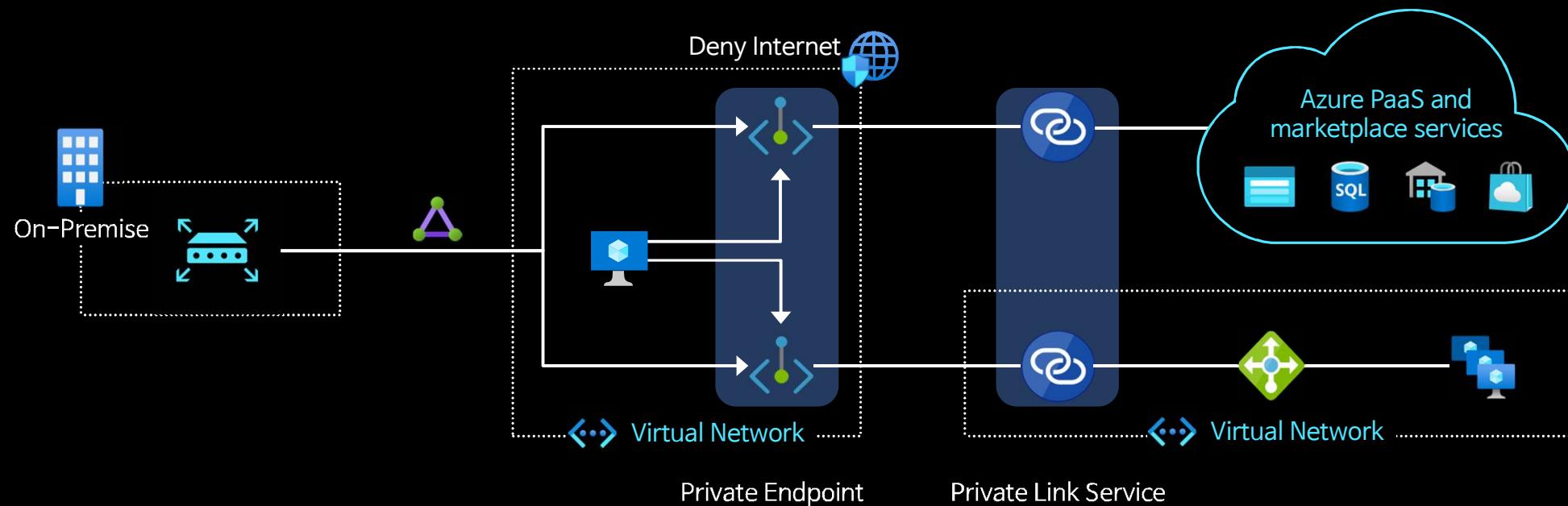
## Private Link Service

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



# Private Link

Highly secure and private connectivity to Azure services





# Private Link

지원되는 서비스 리스트

Supported services	Available regions	Status
Private Link services behind standard Azure Load Balancer	All public regions	GA
Azure Storage	All public regions	GA
Azure Data Lake Storage Gen2	All public regions	GA
Azure SQL Database	All public regions	GA
Azure Synapse Analytics (SQL Data Warehouse)	All public regions	GA
Azure Cosmos DB	All public regions	GA
Azure Database for PostgreSQL - Single server	All public regions	GA
Azure Database for MySQL	All public regions	GA
Azure Database for MariaDB	All public regions	GA
Azure Key Vault	All public regions	GA
Azure Kubernetes Service - Kubernetes API	All public regions	GA
Azure Search	EAST US, WEST US 2, SOUTH CENTRAL US	Preview
Azure Container Registry	All public regions	Preview
Azure App Configuration	All public regions	Preview
Azure Backup	EAST US, WEST US 2, SOUTH CENTRAL US	Preview
Azure Event Hub	All public regions	Preview
Azure Service Bus	All public regions	Preview
Azure Relay	All public regions	Preview
Azure Event Grid	EAST US, WEST US 2, SOUTH CENTRAL US	Preview
Azure Web Apps	EAST US, WEST US 2, SOUTH CENTRAL US	Preview
Azure Machine Learning	EAST US, WEST US 2, SOUTH CENTRAL US	Preview

정리하며..



**Thank You**