

# AZ-104T00A

## Administer Intersite Connectivity

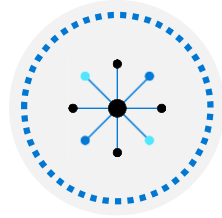


# Administer Intersite Connectivity Introduction



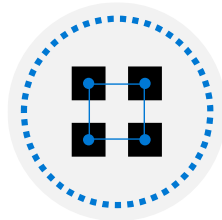
Configure VNet Peering

---



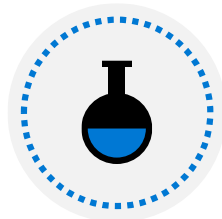
Configure VPN Gateway

---



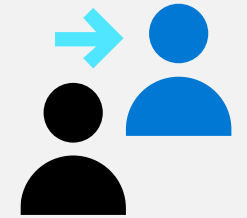
Configure ExpressRoute and Virtual WAN

---



Lab 05 - Implement Intersite Connectivity

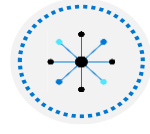
# Configure VNet Peering



# Configure VNet Peering Introduction



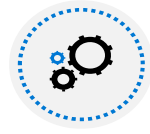
Determine VNet Peering Uses



Determine Gateway Transit and Connectivity Needs



Create VNet Peering



Determine Service Chaining Uses

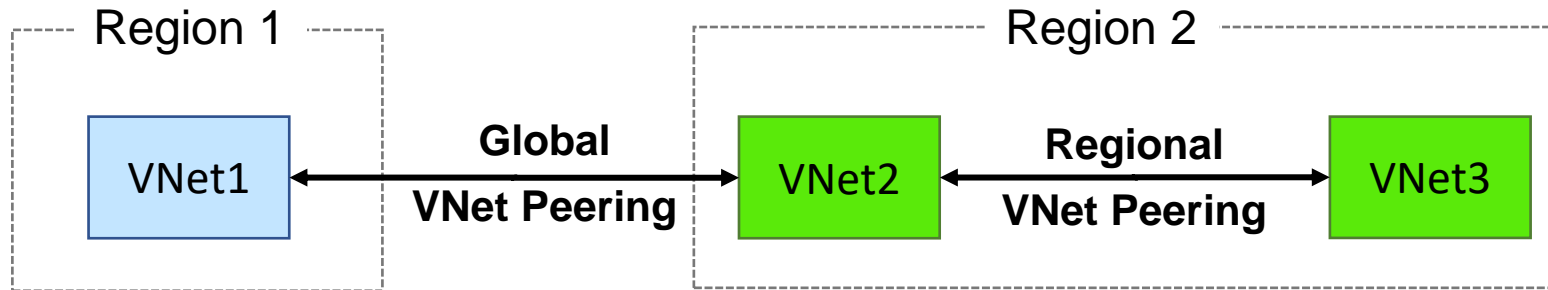


Demonstration – VNet Peering



Summary and Resources

# Determine VNet Peering Uses



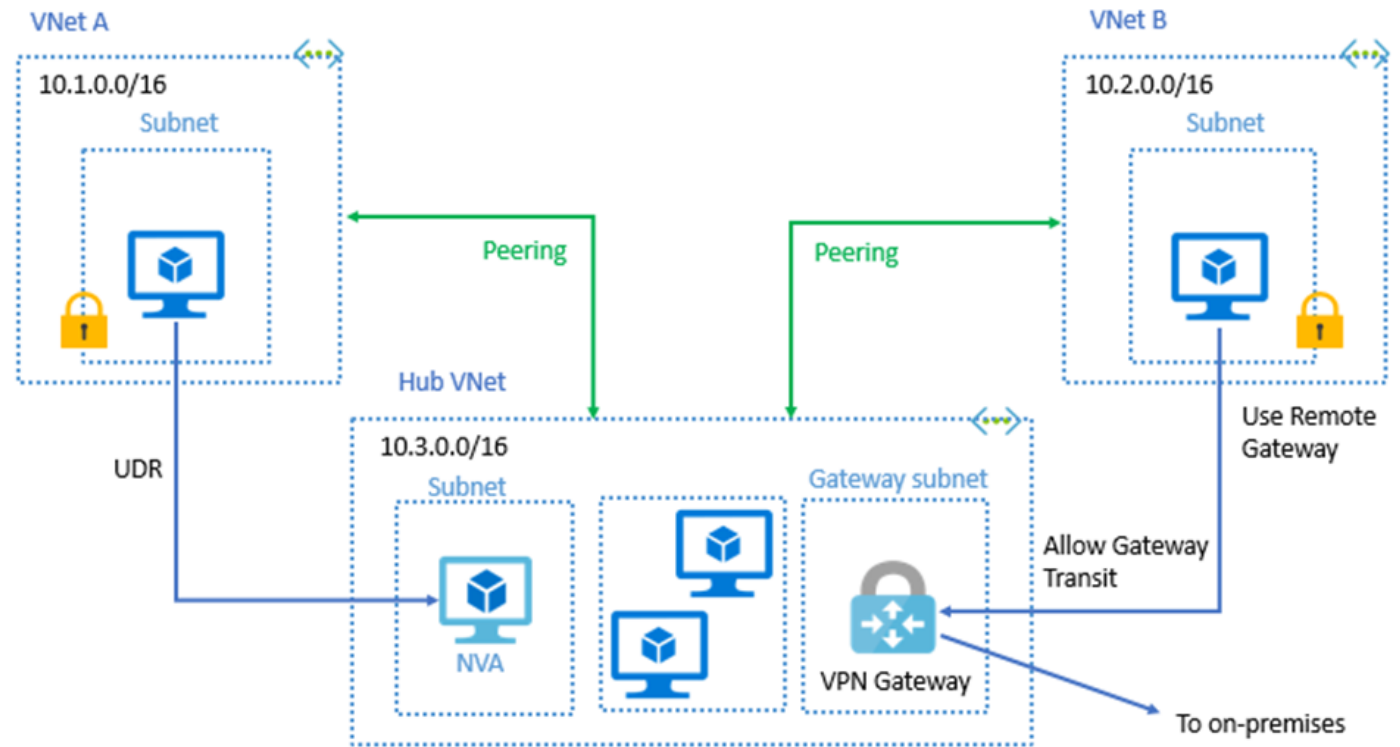
- Two types of peering: Global and Regional
- Connects two Azure virtual networks – you can peer across subscriptions and tenants
- Peered networks use the Azure backbone for privacy and isolation
- Easy to setup, seamless data transfer, and great performance

# Determine Gateway Transit and Connectivity Needs

Gateway transit allows peered virtual networks to share the gateway and get access to resources

No VPN gateway is required in the peered virtual network

Default VNet peering provides full connectivity



IP address spaces of connected networks can't overlap

# Create VNet Peering

Allow virtual network access settings

Configure forwarded traffic settings

This virtual network

Peering link name \*

Traffic to remote virtual network ⓘ

- ☒ Allow (default)
- ☐ Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ

- ☒ Allow (default)
- ☐ Block traffic that originates from outside this virtual network

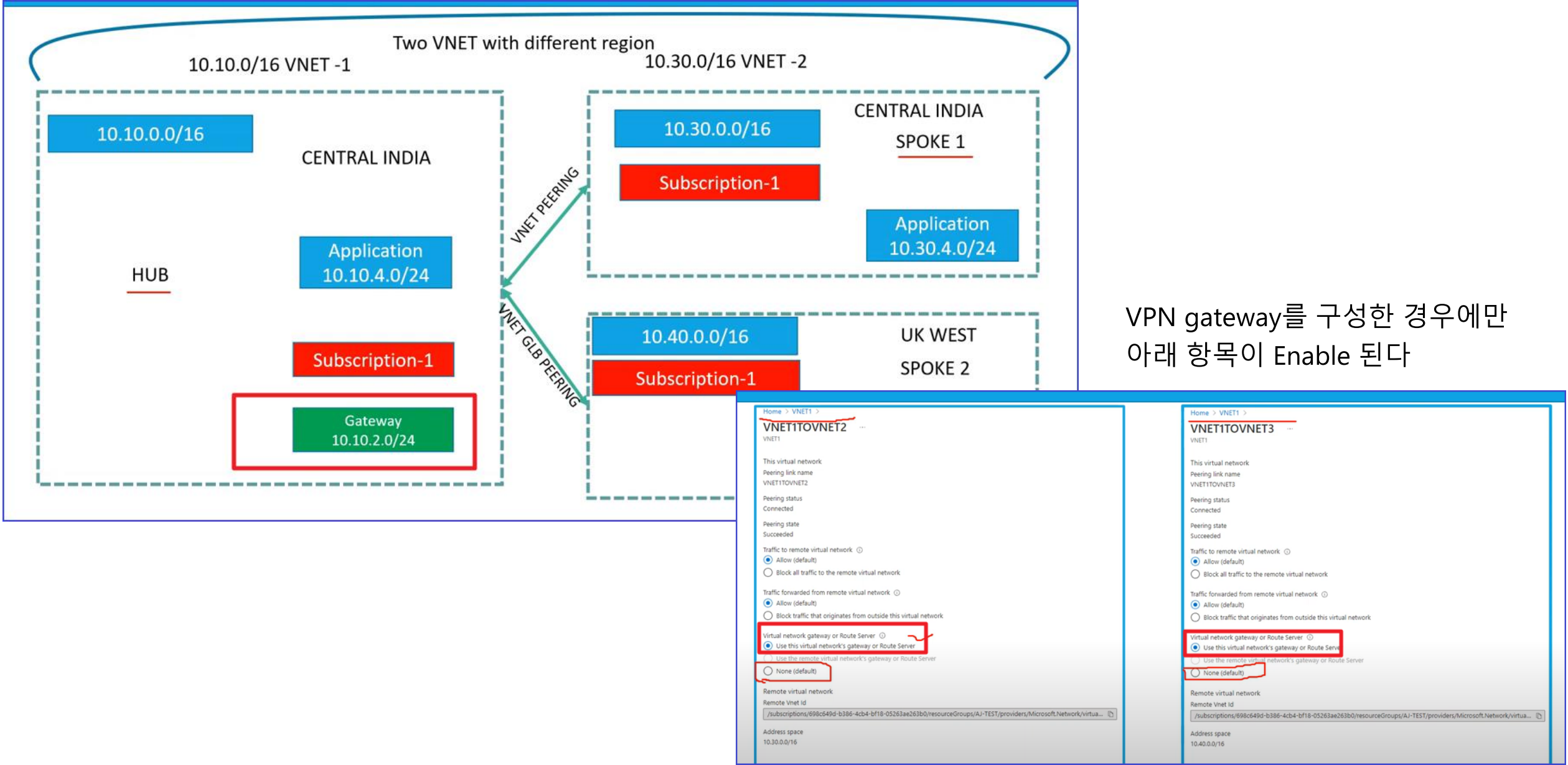
Virtual network gateway ⓘ

- ☐ Use this virtual network's gateway
- ☐ Use the remote virtual network's gateway
- ☒ None (default)

Remote virtual network

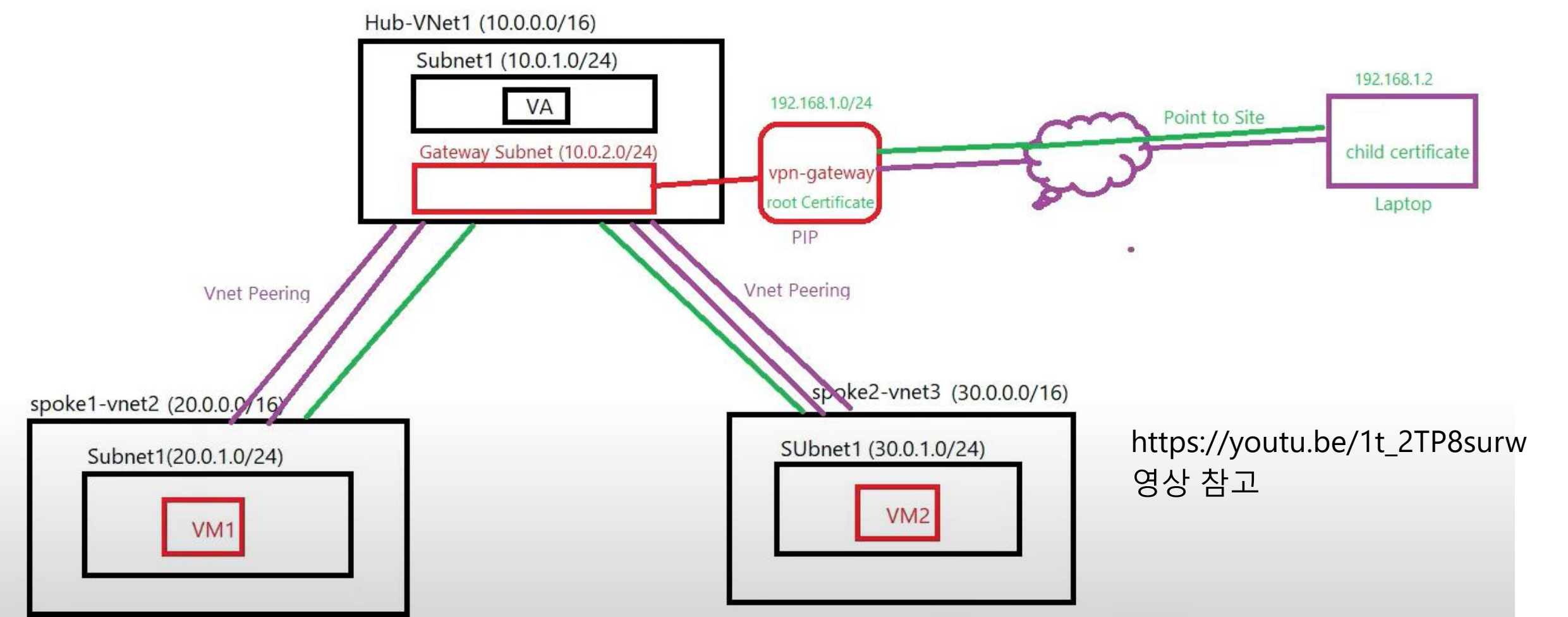
Peering link name \*

# Create VNet Peering-Configure a VPN gateway &Allow gateway transit





# Create VNet Peering-Configure a VPN gateway &Allow gateway transit



## 총 개념

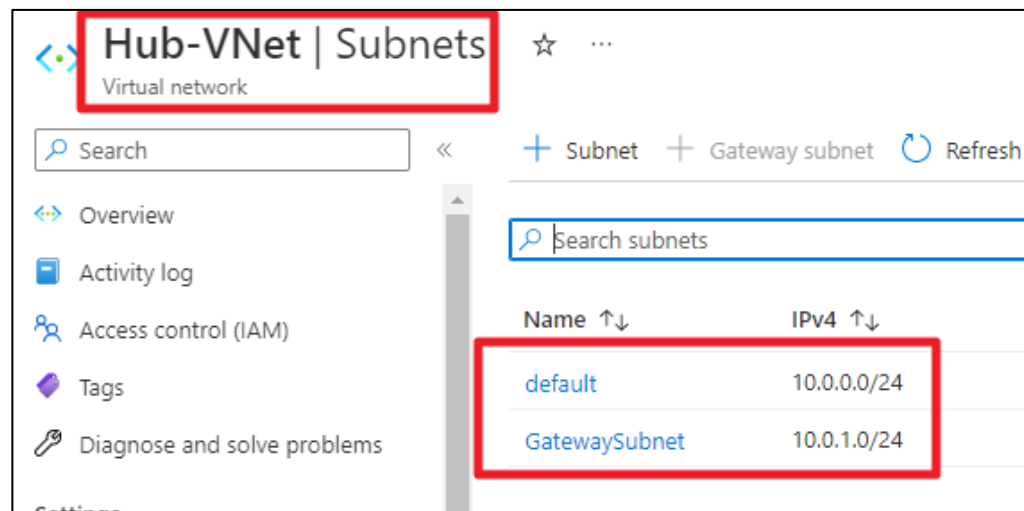
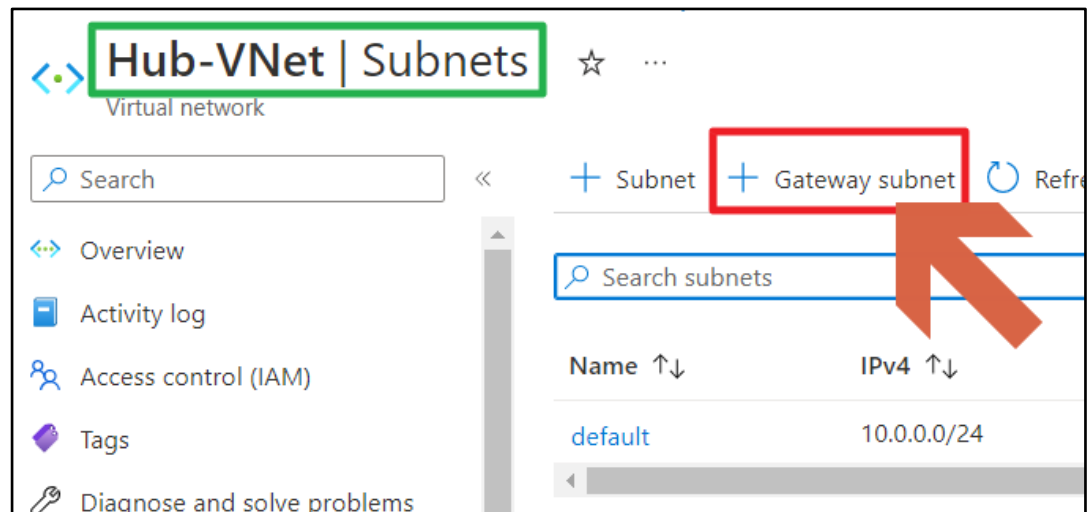
이렇게 구성하면 사내 컴퓨터에서 Point-to-Site VPN을 구성하면  
사내의 관리자 노트북에서 Vnet1, Vnet2, Hub-Vnet에 있는 VM들과  
LAN 통신이 가능하다(ping 등 모두 가능하다)

## 1) 3개 VNet 생성하기

**Hub-VNet:** HQ: 10.0.0.0/24  
GatewaySubnet: 10.0.1.0/24

**VNet1:** default: 10.1.0.0/24

**VNet2:** default: 10.2.0.0/24



## 2) 2개 VM 생성하기

**VM-VNet1:** CentOS  
VNet1에 연결  
NSG에서 ICMP allow

**VM-VNet2:** CentOS  
VNet2에 연결  
NSG에서 ICMP allow

Priority	Name	Port	Protocol	Source	Destination	Action
300	SSH	22	TCP	Any	Any	Allow
310	Allow-Ping	Any	ICMP	Any	Any	Allow

### 3) Virtual Network Gateway 생성하기

#### Create virtual network gateway ...

Subscription \*

Azure subscription 1

Resource group ⓘ

devRG (derived from virtual network's resource group)

#### Instance details

Name \*

VPNGW

Region \*

East US

Gateway type \* ⓘ

☒ VPN ☐ ExpressRoute

VPN type \* ⓘ

☒ Route-based ☐ Policy-based

SKU \* ⓘ

VpnGw1

Generation ⓘ

Generation1

Virtual network \* ⓘ

Hub-VNet

Create virtual network

Subnet ⓘ

GatewaySubnet (10.0.1.0/24)

<div></div>

Only virtual networks in the currently selected subscription listed.

Subnet ⓘ

GatewaySubnet (10.0.1.0/24)

<div></div>

Public IP Address Type \* ⓘ

☐ Basic ☒ Standard

#### Public IP address

Public IP address \* ⓘ

☒ Create new ☐ Use existing

Public IP address name \*

vpngw-pip

Public IP address SKU

Standard

Assignment

☐ Dynamic ☒ Static

Enable active-active mode \* ⓘ

☐ Enabled ☒ Disabled

Configure BGP \* ⓘ

☐ Enabled ☒ Disabled

## 4) VNet\_Hub에서 VNet1과 Peering 설정하기

This virtual network

Peering link name \*

Hub-VNet1

Traffic to remote virtual network ⓘ

☒ Allow (default)

☐ Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ

☒ Allow (default)

☐ Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ

☒ Use this virtual network's gateway or Route Server

☐ Use the remote virtual network's gateway or Route Server

☐ None (default)

Remote virtual network

Peering link name \*

VNet1-Hub

Virtual network deployment model ⓘ

☒ Resource manager

☐ Classic

☐ I know my resource ID ⓘ

Subscription \* ⓘ

Azure subscription 1

Virtual network \*

VNet1

Traffic to remote virtual network ⓘ

☒ Allow (default)

☐ Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ

☒ Allow (default)

☐ Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ

☐ Use this virtual network's gateway or Route Server

☐ Use the remote virtual network's gateway or Route Server

☒ None (default)

VNet1에서  
수정

VNet1-Hub ...

VNet1

This virtual network

Peering link name

VNet1-Hub

Peering status

Fully Synchronized

Peering state

Succeeded

Traffic to remote virtual network ⓘ

☒ Allow (default)

☐ Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ

☒ Allow (default)

☐ Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ

☐ Use this virtual network's gateway or Route Server

☒ Use the remote virtual network's gateway or Route Server

☐ None (default)

## 4) VNet\_Hub에서 VNet2와 Peering 설정하기

This virtual network

Peering link name \*

Hub-VNet2

Traffic to remote virtual network ⓘ

☒ Allow (default)

☐ Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ

☒ Allow (default)

☐ Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ

☒ Use this virtual network's gateway or Route Server

☐ Use the remote virtual network's gateway or Route Server

☐ None (default)

Remote virtual network

Peering link name \*

Vnet2-Hub

Virtual network deployment model ⓘ

☒ Resource manager

☐ Classic

☐ I know my resource ID ⓘ

Subscription \* ⓘ

Azure subscription

Virtual network \*

VNet2

Traffic to remote virtual network ⓘ

☒ Allow (default)

☐ Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ

☒ Allow (default)

☐ Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ

☐ Use this virtual network's gateway or Route Server

☐ Use the remote virtual network's gateway or Route Server

☒ None (default)

VNet2에서  
수정

Vnet2-Hub

VNet2

This virtual network

Peering link name

Vnet2-Hub

Peering status

Fully Synchronized

Peering state

Succeeded

Traffic to remote virtual network ⓘ

☒ Allow (default)

☐ Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ

☒ Allow (default)

☐ Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ

☐ Use this virtual network's gateway or Route Server

☒ Use the remote virtual network's gateway or Route Server

☐ None (default)

## 5) VPNGW에서 Point-Site-VPN 구성

Win10의 PowerShell에서 인증서를 만들어서 VPN Gateway에서 설정하고  
다시 VPN Gateway에서 VPN Client 프로그램을 다운로드하여 Win10에 설치하여  
VPN 연결을 한다

VPN 연결 후에는 Win10에서 VNet1에 있는 VM과 Ping 통신을 하여 성공시킨다

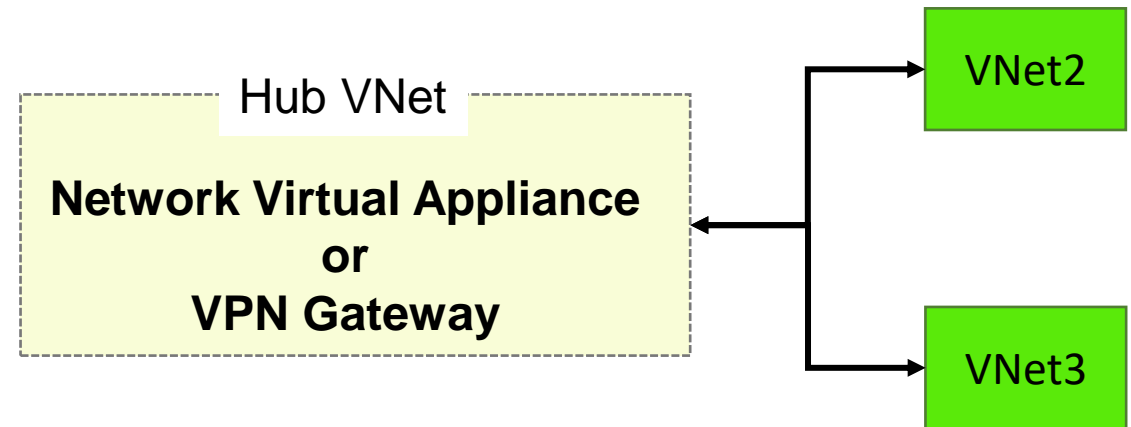


# Determine Service Chaining Uses

Leverage user-defined routes and service chaining to implement custom routing

Implement a VNet hub with a network virtual appliance or a VPN gateway

Service chaining enables you to direct traffic from one virtual network to a virtual appliance, or virtual network gateway, in a peered virtual network, through user-defined routes

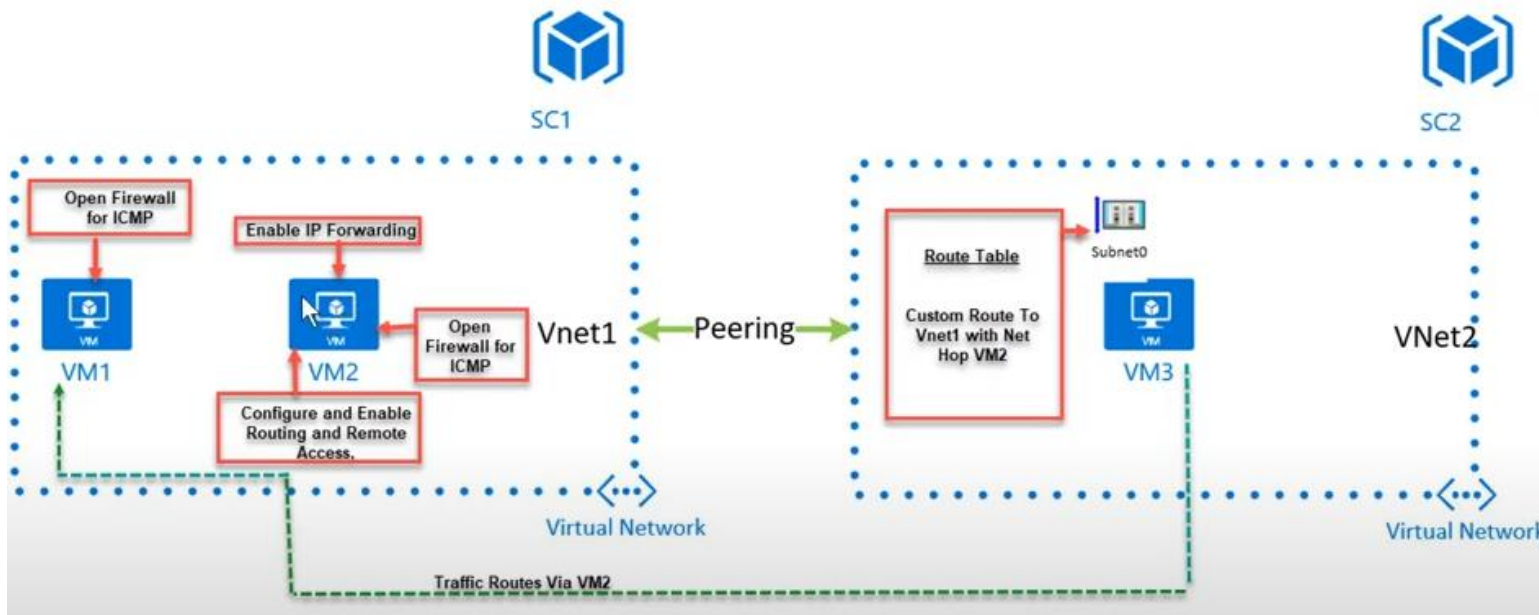


# Determine Service Chaining Uses

참고 영상: <https://youtu.be/KpzpkBAETJ8>

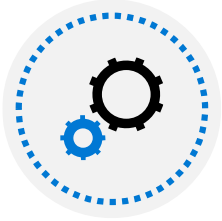
실습 파일:

<https://rajanieshkaushikk.com/2020/03/12/how-to-setup-service-chaining-in-azure/>



작업 할 내용이 많음  
- Windows에서 Router 설정

# Demonstration – VNet Peering



Configure VNet peering on the first virtual network

---



Configure a VPN gateway

---



Allow gateway transit

---



Confirm VNet peering on the second virtual network

# Summary and Resources – Configure VNet Peering

Knowledge Check Questions



Microsoft Learn Modules ([docs.microsoft.com/Learn](https://docs.microsoft.com/Learn))

[Distribute your services across Azure virtual networks and integrate them by using virtual network peering \(Sandbox\)](#)

*A sandbox* indicates a hands-on exercise.

# Lesson 02: Configure VPN Gateway



# Configure VPN Gateway Introduction



Determine VPN Gateway Uses



Create Site-to-Site Connections



Demonstration- VPN Gateway

- Create the Gateway Subnet
- Create the VPN Gateway
- Determine Gateway SKU and Generation
- Create the Local Network Gateway
- Setup the On-premises VPN Device
- Create the VPN Connection

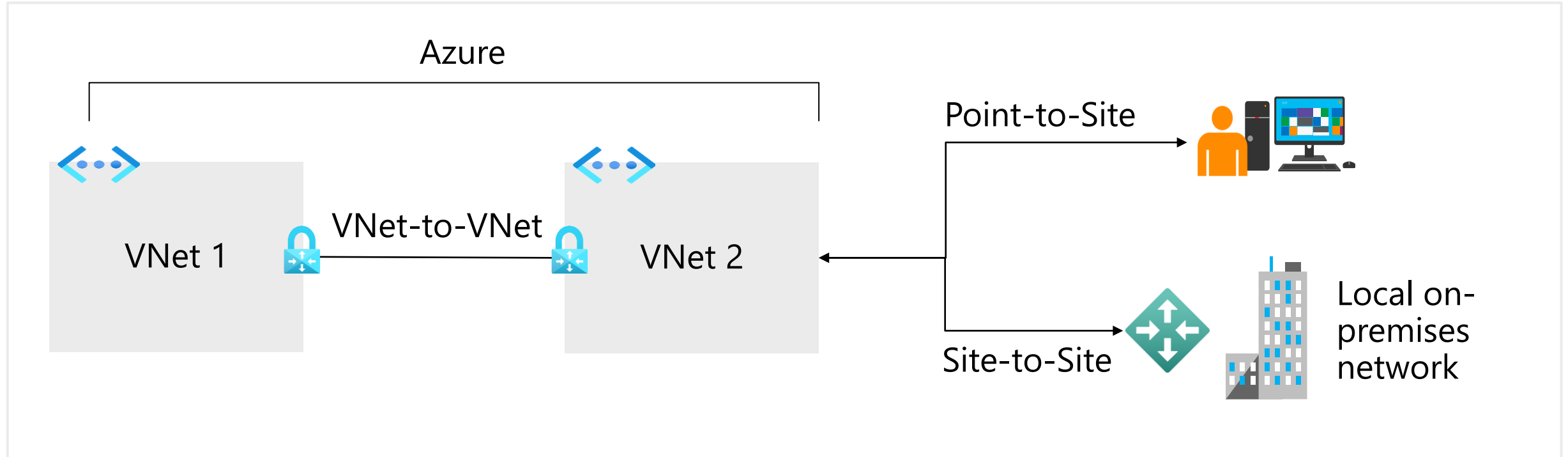


Determine High Availability Scenarios



Summary and Resources

# Determine VPN Gateway Uses

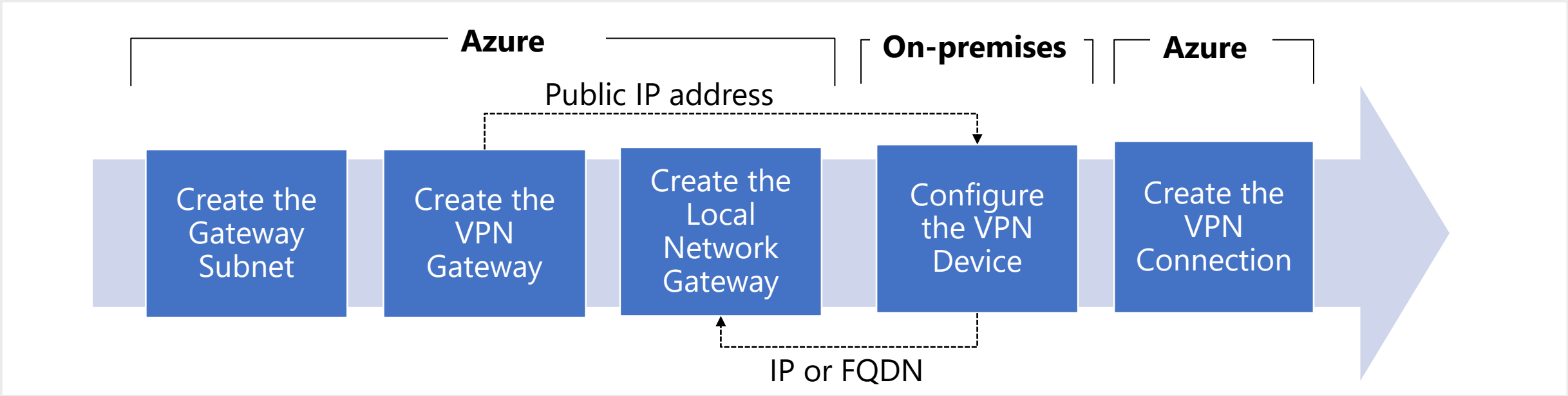


VNet-to-VNet connections connect Azure virtual networks – VNet peering or custom

Point-to-Site (User VPN) connections connect individual devices to Azure virtual networks

Site-to-Site connections connect on-premises datacenters to Azure virtual networks

# Create Site-to-Site VPN Connections



Take time to carefully plan your network configuration

The on-premises part is necessary only if you are configuring Site-to-Site

Always verify and test your connections



# Demonstration – VPN gateways



Explore the Gateway subnet blade

---



Explore the Connected Devices blade

---



Explore adding a virtual network gateway

---



Explore adding a connection between the virtual networks

# Create the Gateway Subnet

When you create your gateway subnet, gateway VMs are deployed to the gateway subnet and configured with the required VPN gateway settings

The gateway subnet contains the IP addresses; if possible, use a CIDR block of /28 or /27

Never deploy other resources (for example, additional VMs) to the gateway subnet

+ Subnet + Gateway subnet

Name  
GatewaySubnet

Subnet address range \* ⓘ  
10.0.1.0/24  
10.0.1.0 - 10.0.1.255 (251 + 5 Azure reserved addresses)

☐ Add IPv6 address space ⓘ

NAT gateway ⓘ  
None

Network security group  
None

Route table  
None

**SERVICE ENDPOINTS**  
Create service endpoint policies to allow traffic to specific azure resources from your virtual network service endpoints. [Learn more](#)

Services ⓘ  
0 selected

**SUBNET DELEGATION**  
Delegate subnet to a service ⓘ  
None

# Create the VPN Gateway

Most VPN Gateways are Route-based

Your choice of gateway SKU affects the number of connections you can have and the aggregate throughput benchmark

Associate the virtual network that includes the Gateway Subnet – need a public IP address

It can take up to 45 minutes to provision the VPN gateway

## Create virtual network gateway ...

Basics Tags Review + create

Subscription \*

ASC DEMO

Resource group ⓘ

Select a virtual network to get resource group

### Instance details

Name \*

Region \*

East US 2

Gateway type \* ⓘ

☒ VPN ☐ ExpressRoute

VPN type \* ⓘ

☒ Route-based ☐ Policy-based

SKU \* ⓘ

VpnGw2AZ

Generation ⓘ

Generation2

Virtual network \* ⓘ

[Create virtual network](#)

Public IP address \* ⓘ

☒ Create new ☐ Use existing

Enable active-active mode \* ⓘ

☐ Enabled ☒ Disabled

Configure BGP \* ⓘ

☐ Enabled ☒ Disabled

# Determine Gateway SKU and Generation

SKU \* ⓘ

VpnGw1 ▾

Generation ⓘ

Generation1 ▾

Sampling of available SKUs

Gen	SKU	S2S/VNet-to-VNet Tunnels	P2S IKEv2 Connections	Throughput Benchmark
1	VpnGw1/Az	Max. 30	Max. 250	650 Mbps
1	VpnGw2/Az	Max. 30	Max. 500	1.0 Gbps
2	VpnGw2/Az	Max. 30	Max. 500	1.25 Gbps
1	VpnGw3/Az	Max. 30	Max. 1000	1.25 Gbps
2	VpnGw3/Az	Max. 30	Max. 1000	2.5 Gbps
2	VpnGw4/Az	Max. 100	Max. 5000	5.0 Gbps
2	VpnGw5/Az	Max. 100	Max. 10000	10.0 Gbps

The Gateway SKU affects the connections and the throughput

Resizing is allowed within the generation

The Basic SKU (not shown) is legacy and should not be used

# Create the Local Network Gateway

Reflects the on-premises network configuration

Give the site a name by which Azure can refer to it

Use a public IP address or FQDN for Local Network Gateway Endpoint

Specify the IP address prefixes that will be routed through the gateway to the VPN device

## Create local network gateway

Name \*

VNet1LocalNet



Endpoint ⓘ

IP address

FQDN

IP address \* ⓘ

33.2.1.5



Address space ⓘ

192.168.3.0/24



Add additional address range



☐ Configure BGP settings

# Create the On-premises VPN Device

Consult the list of supported VPN devices

A VPN device configuration script may be available

Remember the shared key for the Azure connection

Specify the public IP address of the VPN Gateway

## Sampling of supported VPN devices

Vendor	Device Family
Barracuda Networks, Inc.	Barracuda CloudGen Firewall
Cisco	ASA, ASR, ISR
Citrix	NetScaler MPX, SDX, VPX
Juniper	SRX, J-Series, ISG, SSG
F5	BIG-IP Series
Palo Alto Networks	All devices running PAN-OS


# Create the VPN Connection

Once your VPN gateways is created and the on-premises device is configured, create a connection object

Configure a name for the connection and specify the type as Site-to-site (IPsec)

Select the VPN gateway and the Local Network Gateway

Enter the Shared key for the connection

 **Add connection** ✕

vng01

Name \*

Azure-to-OnPrem ✓

Connection type ⓘ

Site-to-site (IPsec) ▼

\*Virtual network gateway ⓘ

vng01 🔒

\*Local network gateway ⓘ

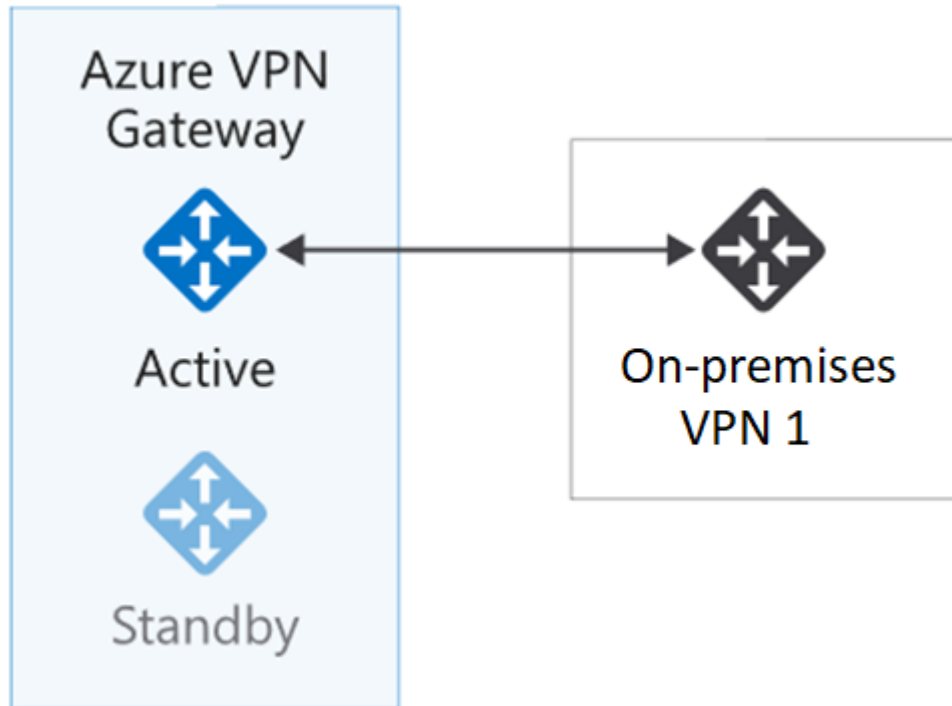
Azure-to-OnPrem >

Shared key (PSK) \* ⓘ

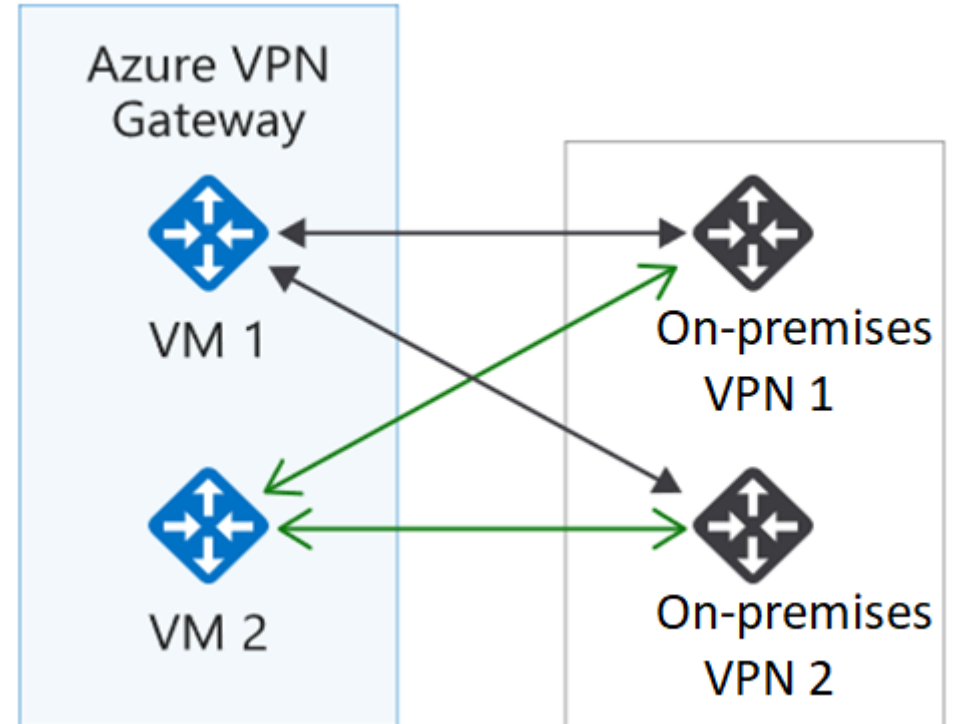
abc123 ✓

# Determine High Availability Scenarios

Active/standby (default)



Active/active



VPN gateways are deployed as two instances

Enable **active/active mode** for higher availability



# Summary and Resources – Configure VPN Gateway

Knowledge Check Questions



Microsoft Learn Modules ([docs.microsoft.com/Learn](https://docs.microsoft.com/Learn))

[Introduction to Azure VPN Gateway](#)

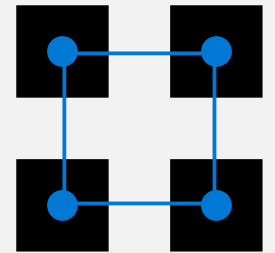
---

[Connect your on-premises network to Azure with VPN Gateway \(Sandbox\)](#)

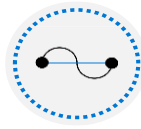
---

*A sandbox* indicates a hands-on exercise.

# Lesson 03: Configure ExpressRoute and Virtual WAN



# Configure ExpressRoute and Virtual WAN Introduction



Determine ExpressRoute Uses



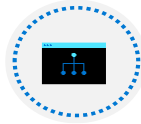
Determine ExpressRoute Capabilities



Coexist Site-to-Site and ExpressRoute



Compare Intersite Connection Options

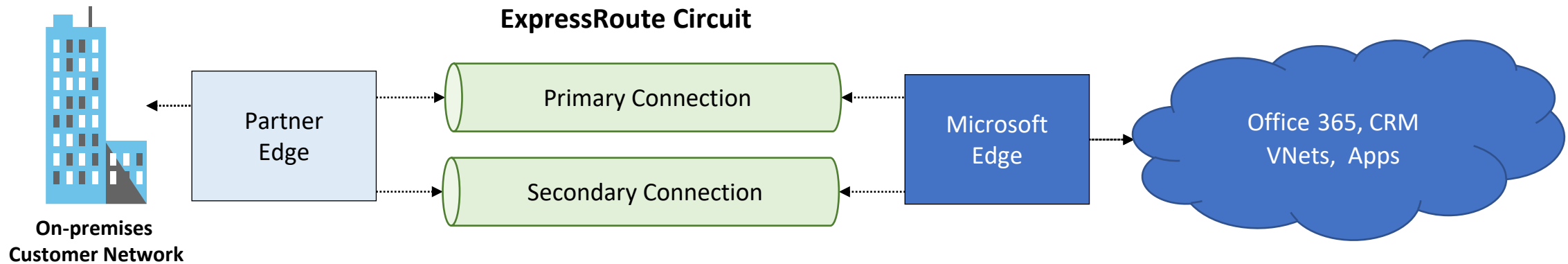


Determine Virtual WAN Uses



Summary and Resources

# Determine ExpressRoute Uses



Private connections  
between your on-premises  
network and Microsoft  
datacenters

Connections do not go  
over the public  
Internet – Partner network

Secure, reliable,  
low latency, high speed  
connections

# Determine ExpressRoute Capabilities

Layer 3 connectivity with redundancy

Connectivity to all regions within a geography

Global connectivity with ExpressRoute premium add-on

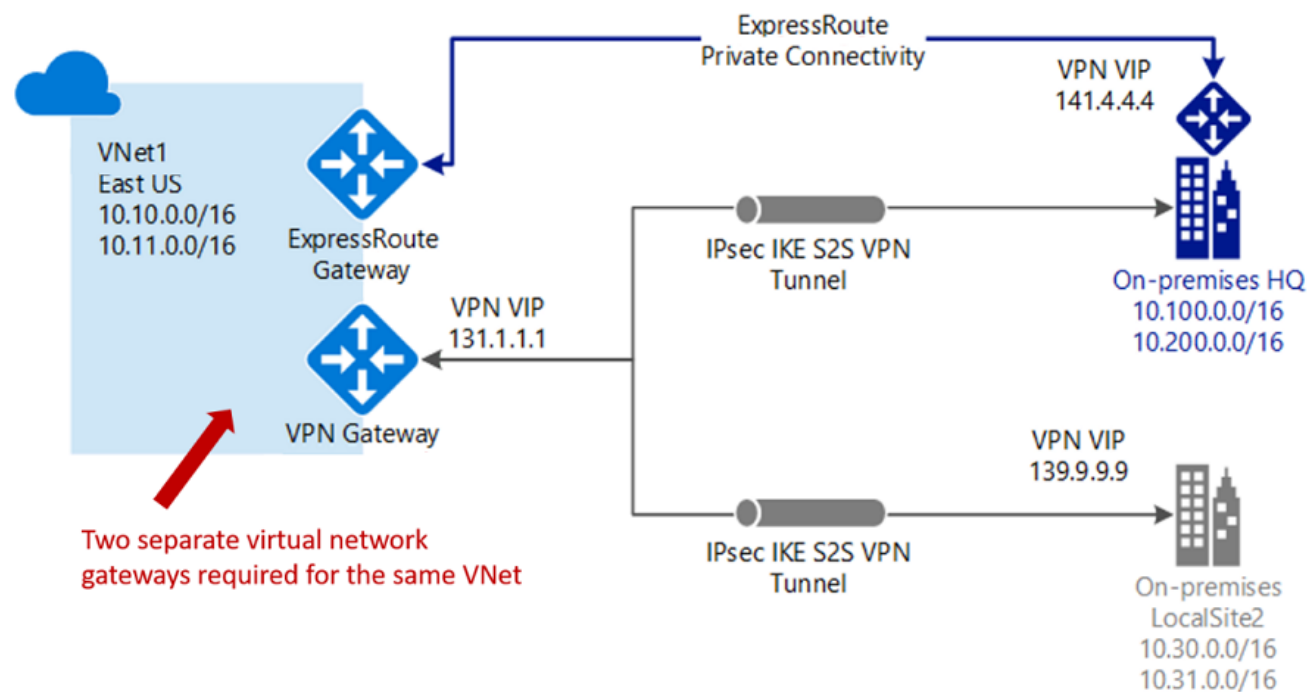
Across on-premises connectivity with ExpressRoute Global Reach

Bandwidth options – 50 Mbps to 100 Gbps

Billing models – Unlimited, metered, premium



# Coexist Site-to-Site and ExpressRoute



Use S2S VPN as a secure failover path for ExpressRoute

Use S2S VPNs to connect to sites that are not connected with ExpressRoute

Notice two VNet gateways for the same virtual network

# Compare Intersite Connection Options

Connection	Azure services supported	Bandwidth	Protocols	Typical use case
Virtual network, point-to-site	Azure IaaS services, Azure Virtual Machines	Based on the gateway SKU	Active/passive	Dev, test, and lab environments for cloud services and virtual machines
Virtual network, site-to-site	Azure IaaS services, Azure Virtual Machines	Typically, <1 Gbps aggregate	Active/passive Active/active	Dev, test, and lab environments. Small-scale production workloads and virtual machines
ExpressRoute	Azure IaaS and PaaS services, Microsoft 365 services	50 Mbps up to 100 Gbps	Active/active	Enterprise-class and mission-critical workloads. Big data solutions

# Determine Virtual WAN Uses

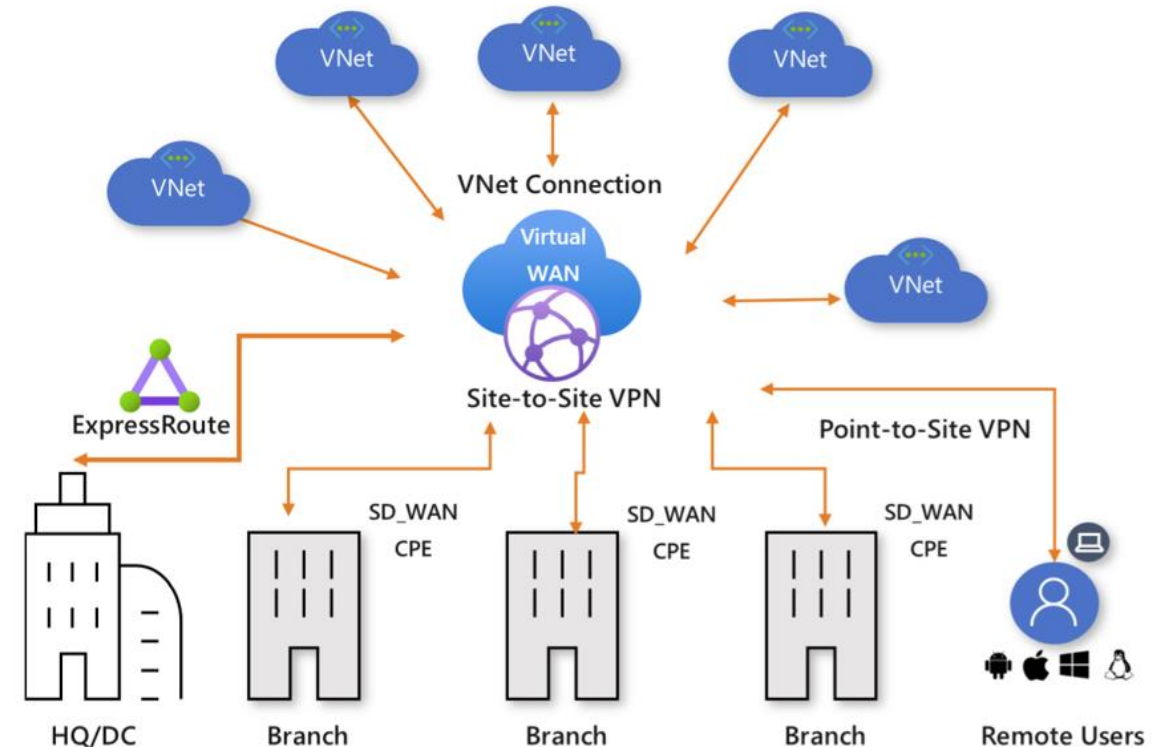
Brings together S2S, P2S, and ExpressRoute

Integrated connectivity using a hub-and-spoke connectivity model

Connect virtual networks and workloads to the Azure hub automatically

Visualize the end-to-end flow within Azure

Two types: Basic and Standard





# Summary and Resources – Configure ExpressRoute and Virtual WANs

Knowledge Check Questions



Microsoft Learn Modules ([docs.microsoft.com/Learn](https://docs.microsoft.com/Learn))

[Introduction to Azure ExpressRoute](#)

---

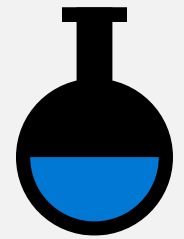
[Design and implement Azure ExpressRoute](#)

---

[Introduction to Azure Virtual WAN](#)

---

# Lab 05 - Implement Intersite Connectivity



# Lab 05 – Implement intersite connectivity

## Lab scenario

Contoso has its datacenters in Boston, New York, and Seattle offices connected via a mesh wide-area network links, with full connectivity between them. You need to implement a lab environment that will reflect the topology of the Contoso's on-premises networks and verify its functionality

## Objectives

### Task 1:

Provision the lab environment

### Task 2:

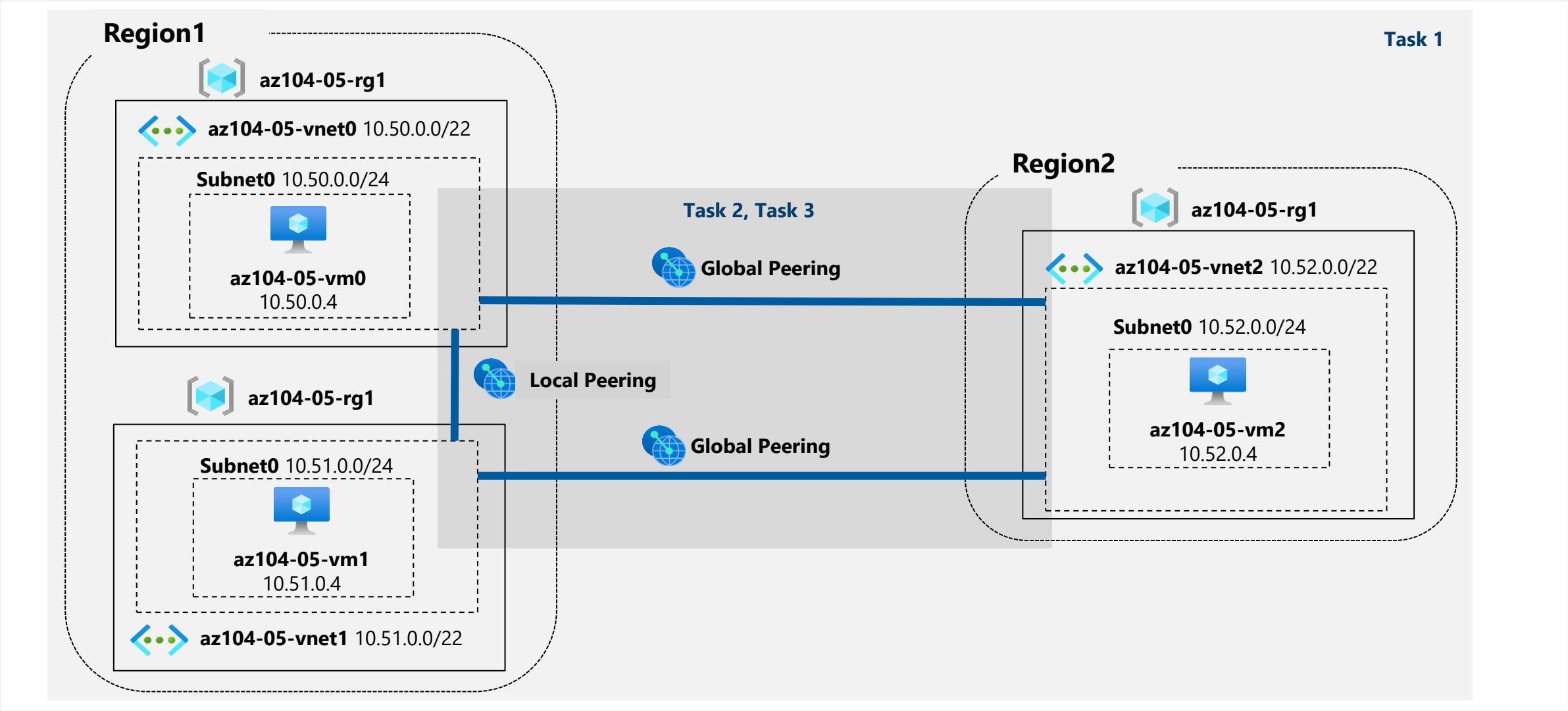
Configure local and global virtual network peering

### Task 3:

Test intersite connectivity

Next slide for an architecture diagram 

# Lab 05 – Architecture diagram



# End of presentation

