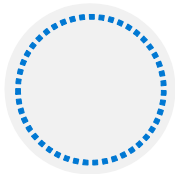
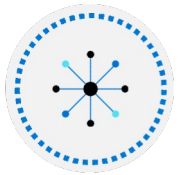
Microsoft Azure

AZ-104T00A
Module 05:
Intersite Connectivity

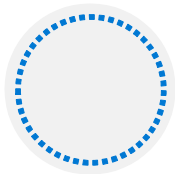
Module Overview



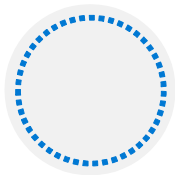
Lesson 01: VNet Peering



Lesson 02: VPN Gateway Connections



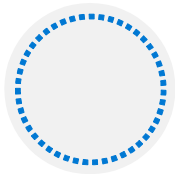
Lesson 03: ExpressRoute and Virtual WAN



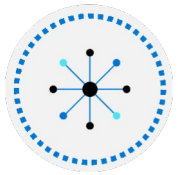
Lesson 04: Module 05 Lab and Review

Lesson 01: VNet Peering

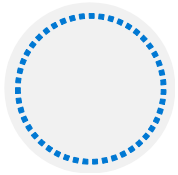
VNet Peering Overview



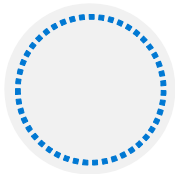
VNet Peering



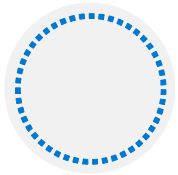
Gateway Transit and Connectivity



Configure VNet Peering



Service Chaining



Demonstration – VNet Peering

VNet Peering

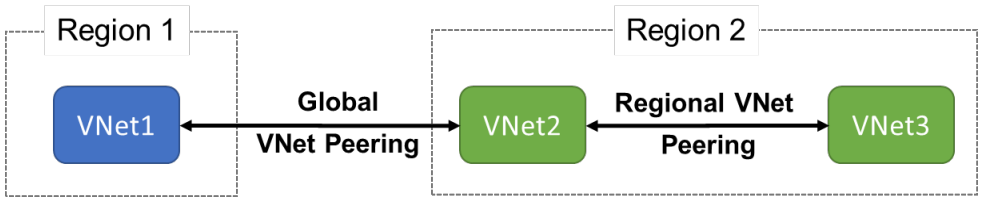
VNet peering connects two Azure virtual networks

Two types of peering: Regional and Global

Peered networks use the Azure backbone for privacy and isolation

You can peer across subscriptions and tenants

Easy to setup, seamless data transfer, and great performance

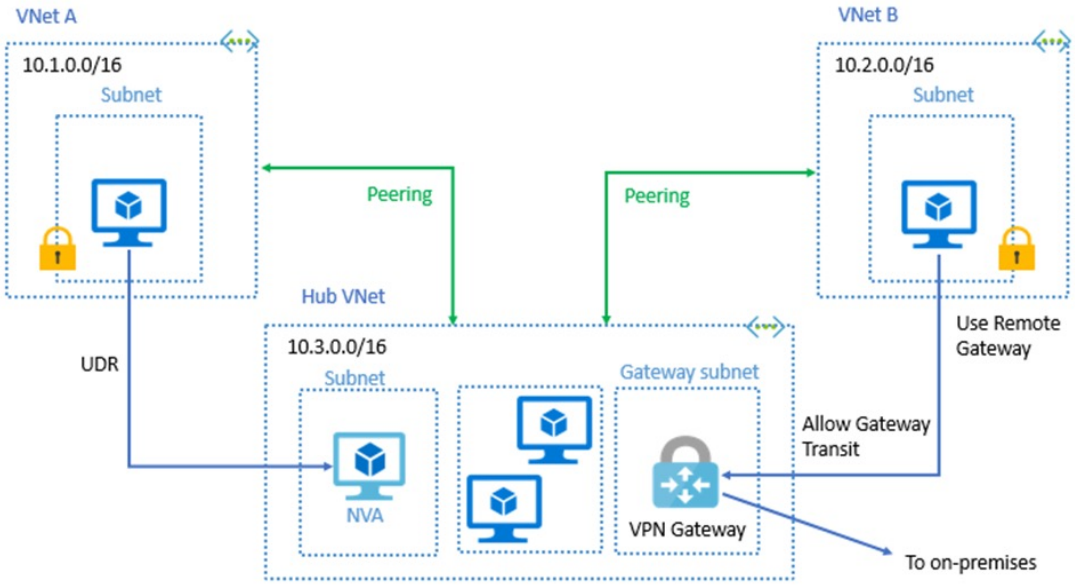


Gateway Transit and Connectivity

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

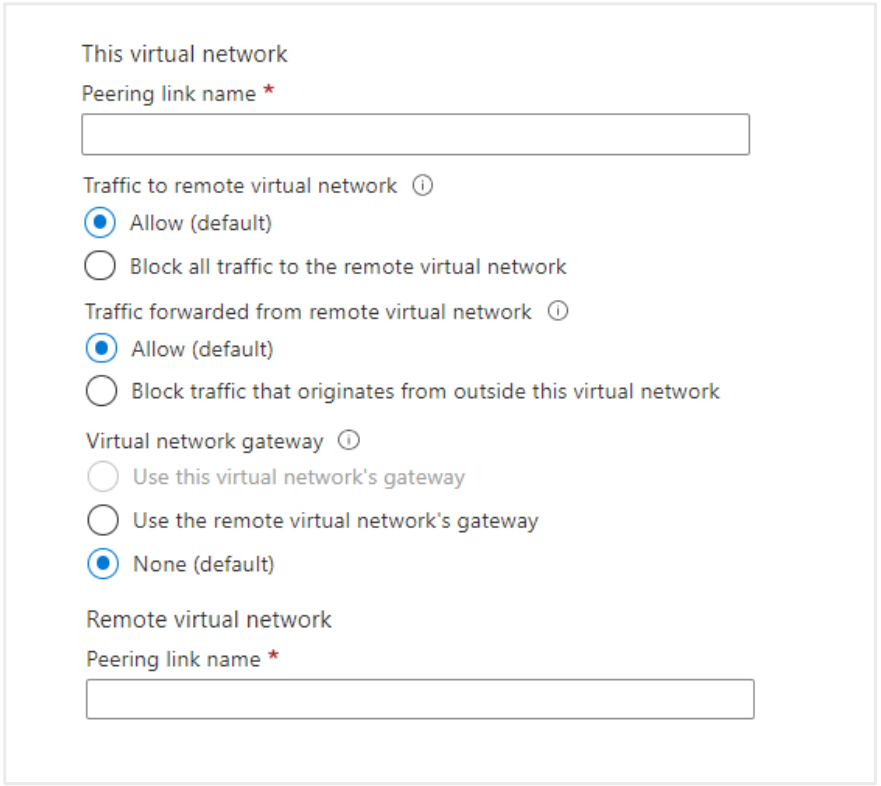


✓ **IP address spaces of connected networks can't overlap**

Configure VNet Peering

Allow virtual network access settings

Configure forwarded traffic settings

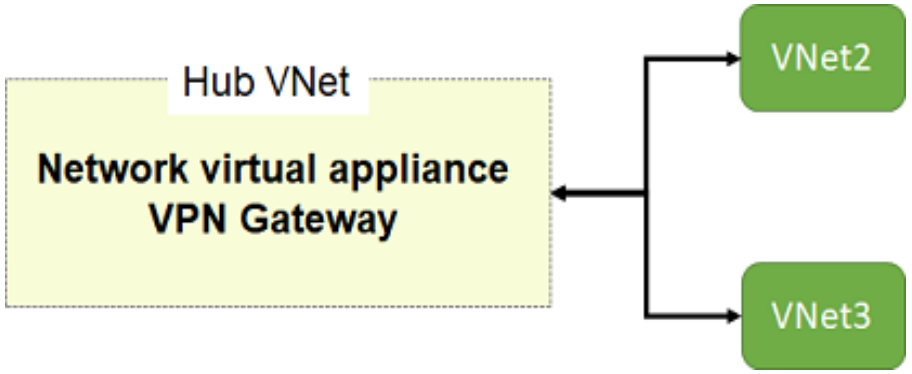


Service Chaining

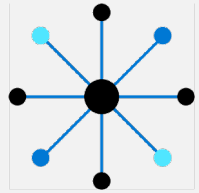
Leverage user-defined routes and service chaining to implement custom routing

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

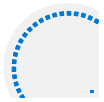
Service chaining enables you to direct traffic from one virtual network to a virtual appliance, or virtual network gateway, in a peered virtual network, through user-defined routes



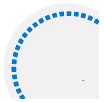
Lesson 02: VPN Gateway Connections



VPN Gateway Connections Overview

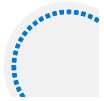


VPN Gateways

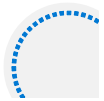


Implement Site-to-Site VPN Connections

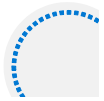
Create the Gateway Subnet



VPN Gateway Configuration

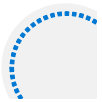


VPN Gateway Types

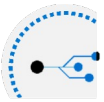


VPN Gateway SKU and Generation

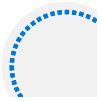
Create the Local Network Gateway



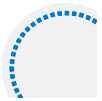
Configure the On-premises VPN Device



Create the VPN Connection

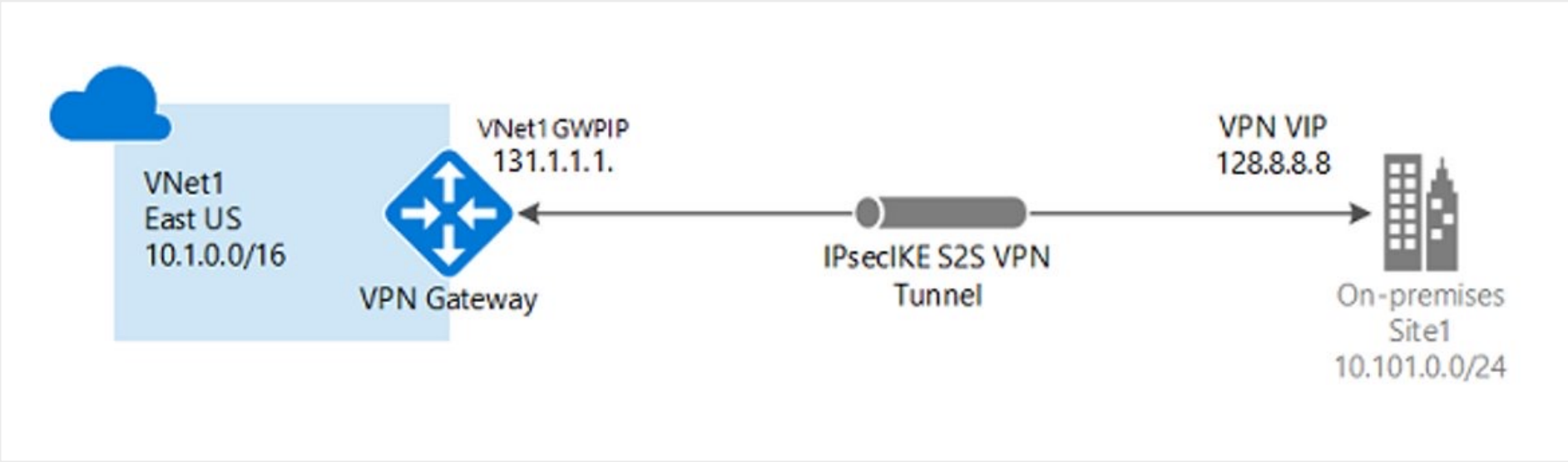


High Availability Scenarios



Demonstration – VPN Gateway

VPN Gateways

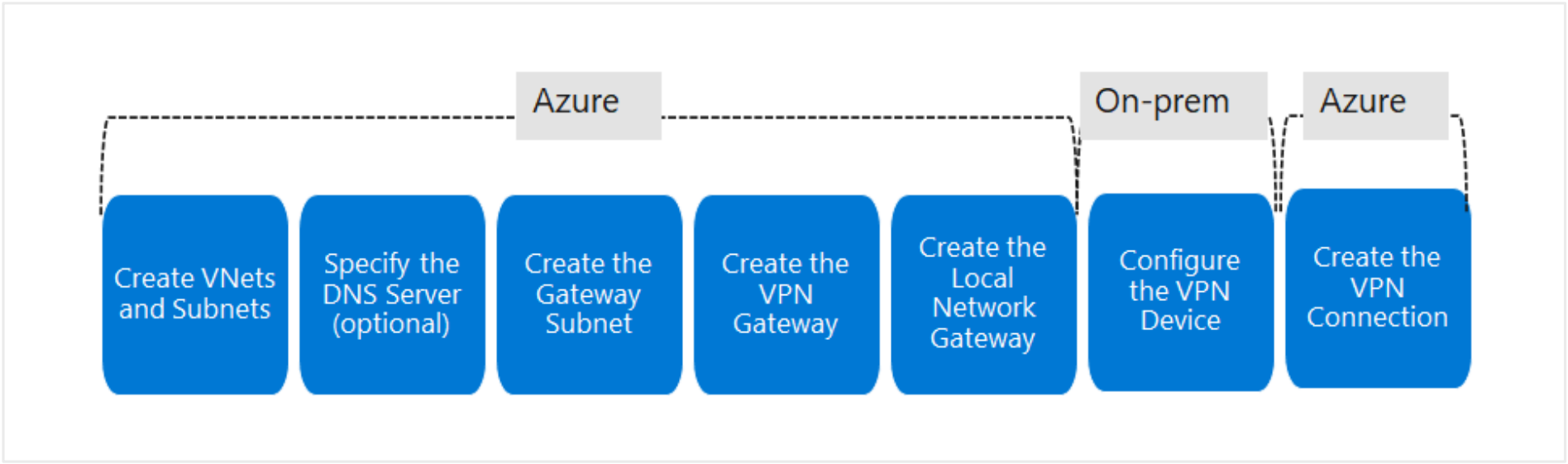


Site-to-site connections connect on-premises datacenters to Azure virtual networks

VNet-to-VNet connections connect Azure virtual networks (custom)

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

Implement 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

Point-to-site vs Site-to-site

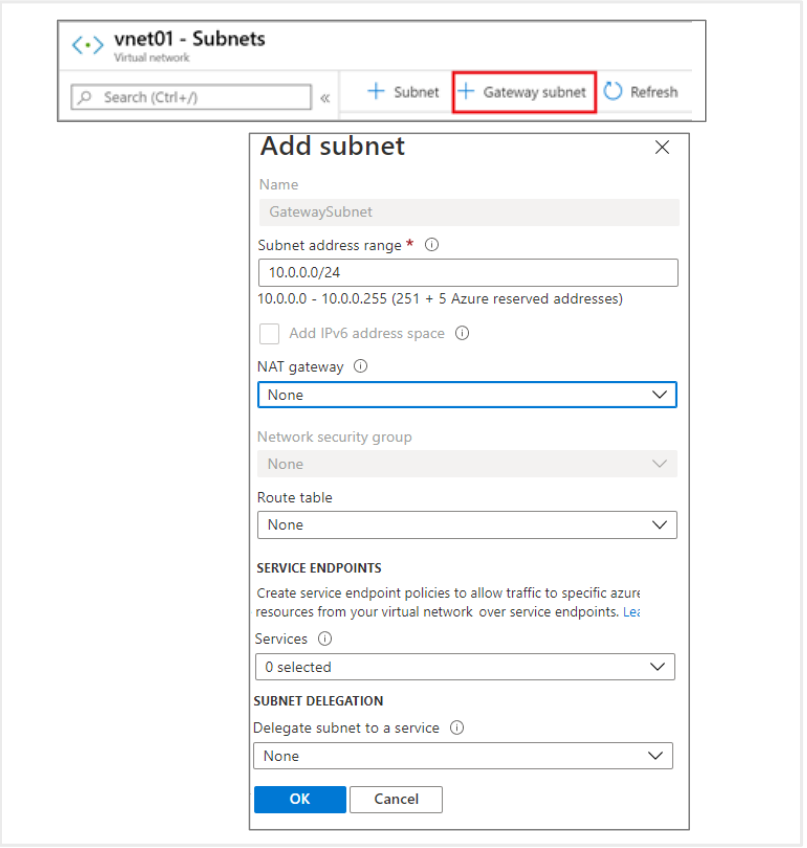
	Point-to-Site	Site-to-Site
Azure Supported Services	Cloud Services and Virtual Machines	Cloud Services and Virtual Machines
Typical Bandwidths	Based on the gateway SKU	Typically < 1 Gbps aggregate
Protocols Supported	Secure Sockets Tunneling Protocol (SSTP), OpenVPN and IPsec	IPsec
Routing	RouteBased (dynamic)	We support PolicyBased (static routing) and RouteBased (dynamic routing VPN)
Connection resiliency	active-passive	active-passive or active-active
Typical use case	Secure access to Azure virtual networks for remote users	Dev / test / lab scenarios and small to medium scale production workloads for cloud services and virtual machines

Create the Gateway Subnet

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

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

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



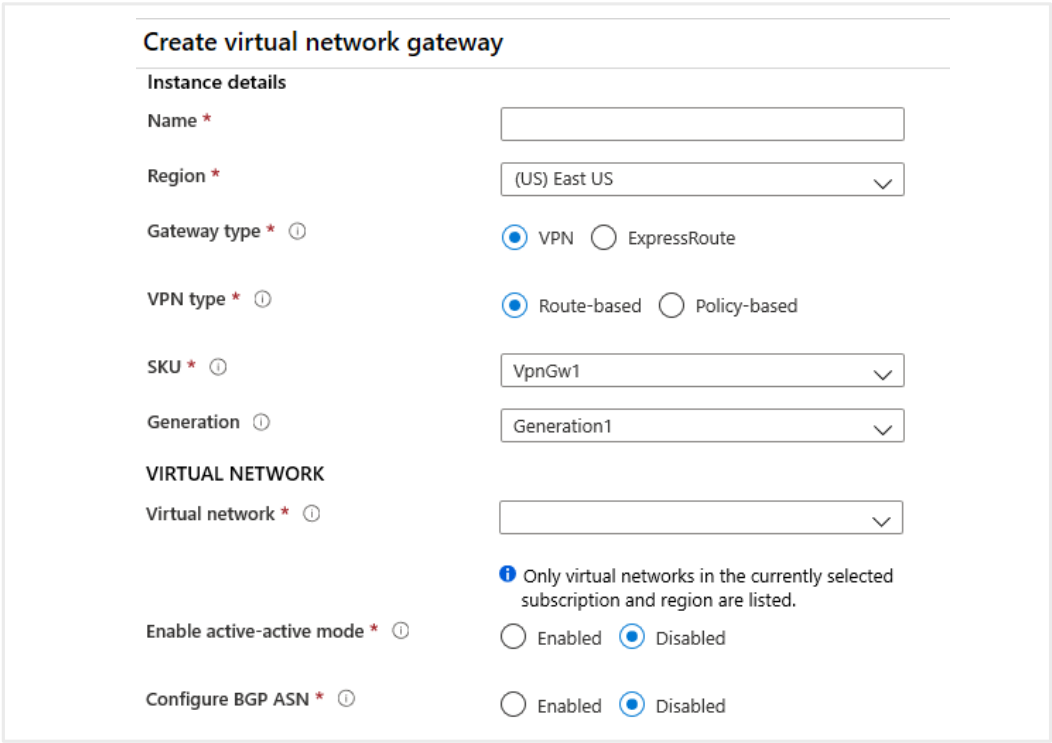
VPN Gateway Configuration

Most VPN types are Route-based

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

Associate a virtual network that includes the gateway subnet

The gateway needs a public IP address



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

VPN Gateway Types

Route-based VPNs use routes in the IP forwarding or routing table to direct packets:

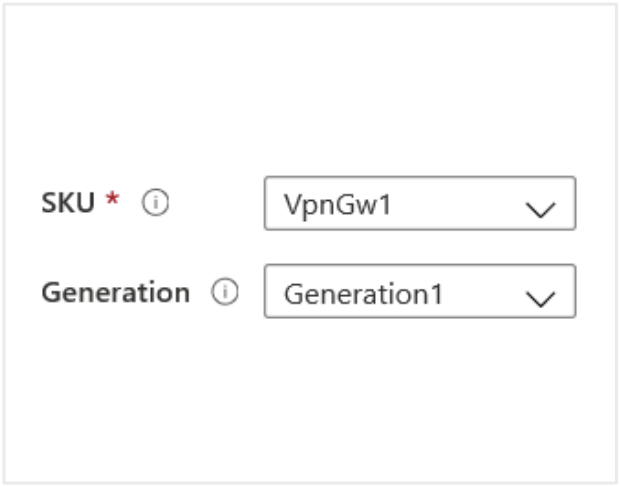
- Support for IKEv2
- Can use dynamic routing protocols

Policy-based VPNs encrypt and direct packets through IPsec tunnels based on the IPsec policies:

- Support for IKEv1 only
- Legacy on-premises VPN devices

Most VPN gateway configurations require a Route-based VPN

Gateway SKU and Generation



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. 30	Max. 5000	5.0 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

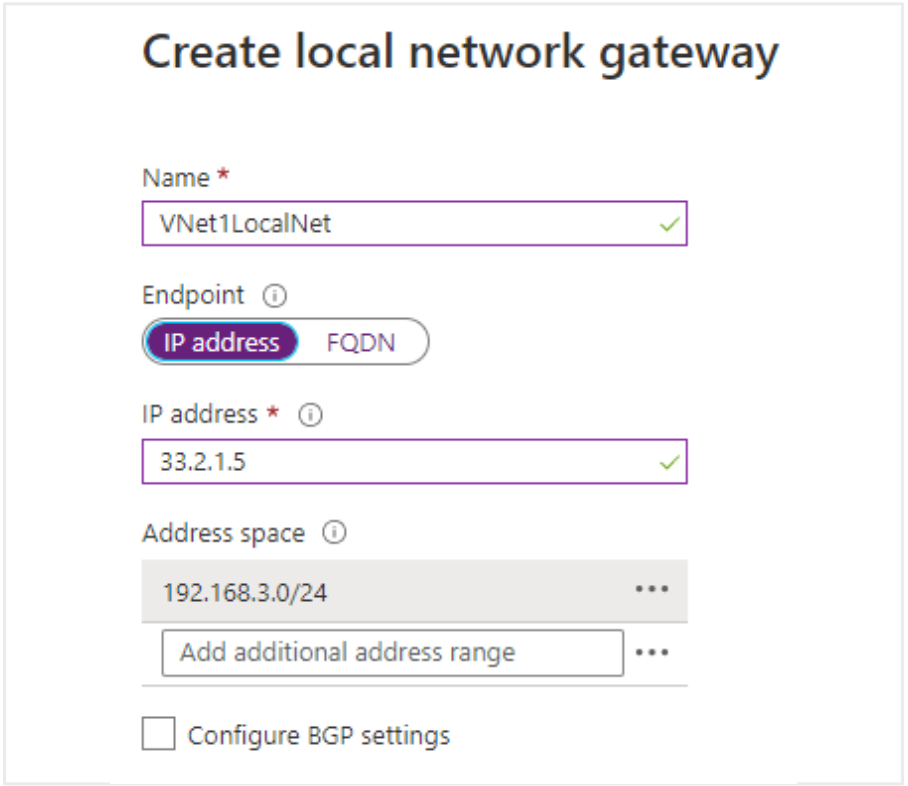
Create the Local Network Gateway

Defines the on-premises network configuration

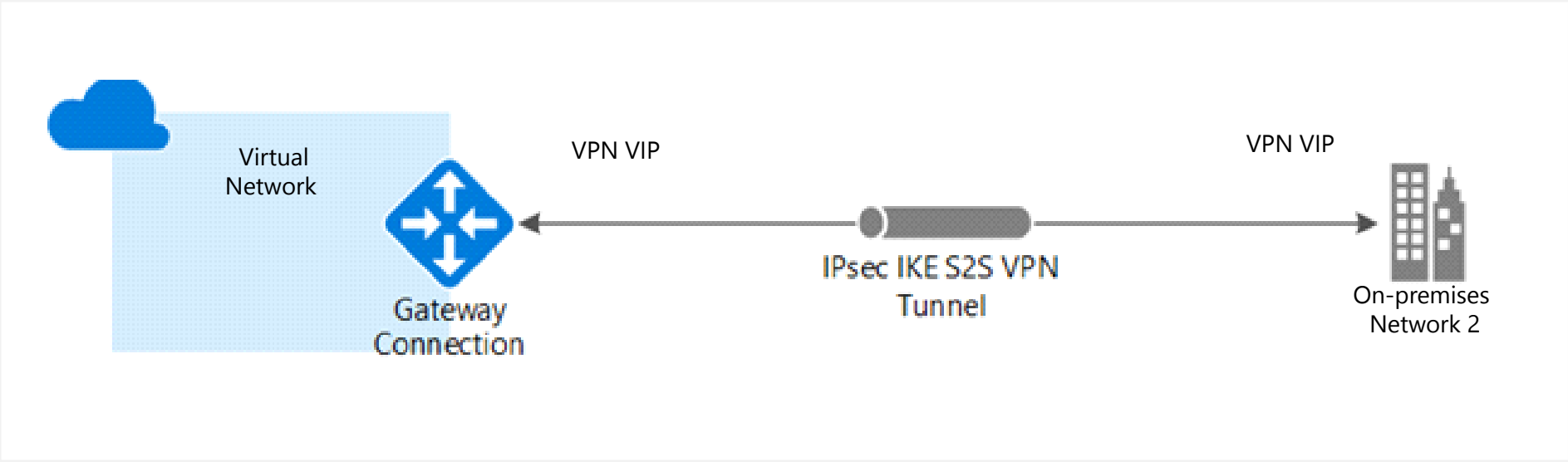
Give the site a name by which Azure can refer to it

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



Configure the On-premises VPN Device



Consult the list of supported VPN devices (Cisco, Juniper, Ubiquiti, Barracuda Networks)

A VPN device configuration script may be available

Remember the shared key for the Azure connection (next step)

Specify the public IP address (previous step)

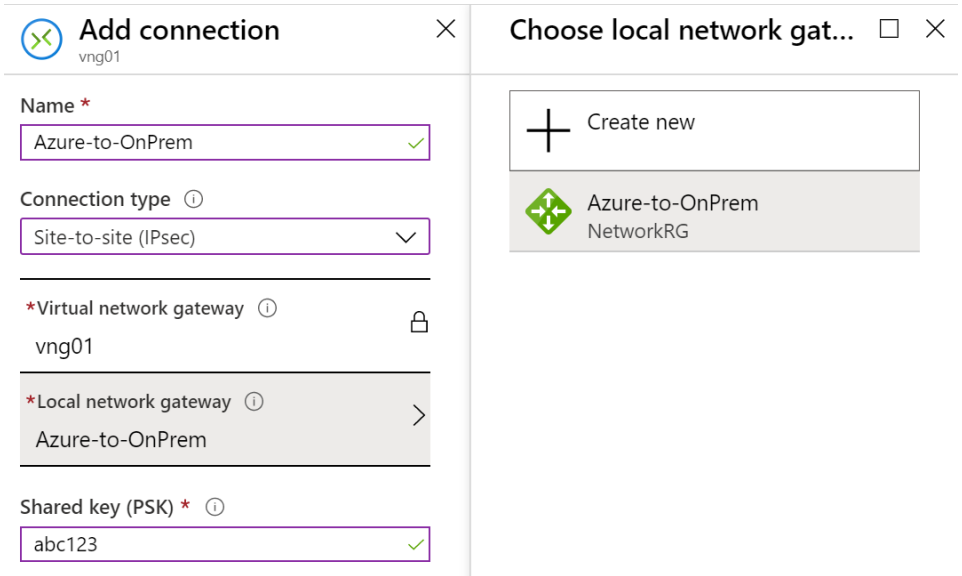
Create the VPN Connection

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

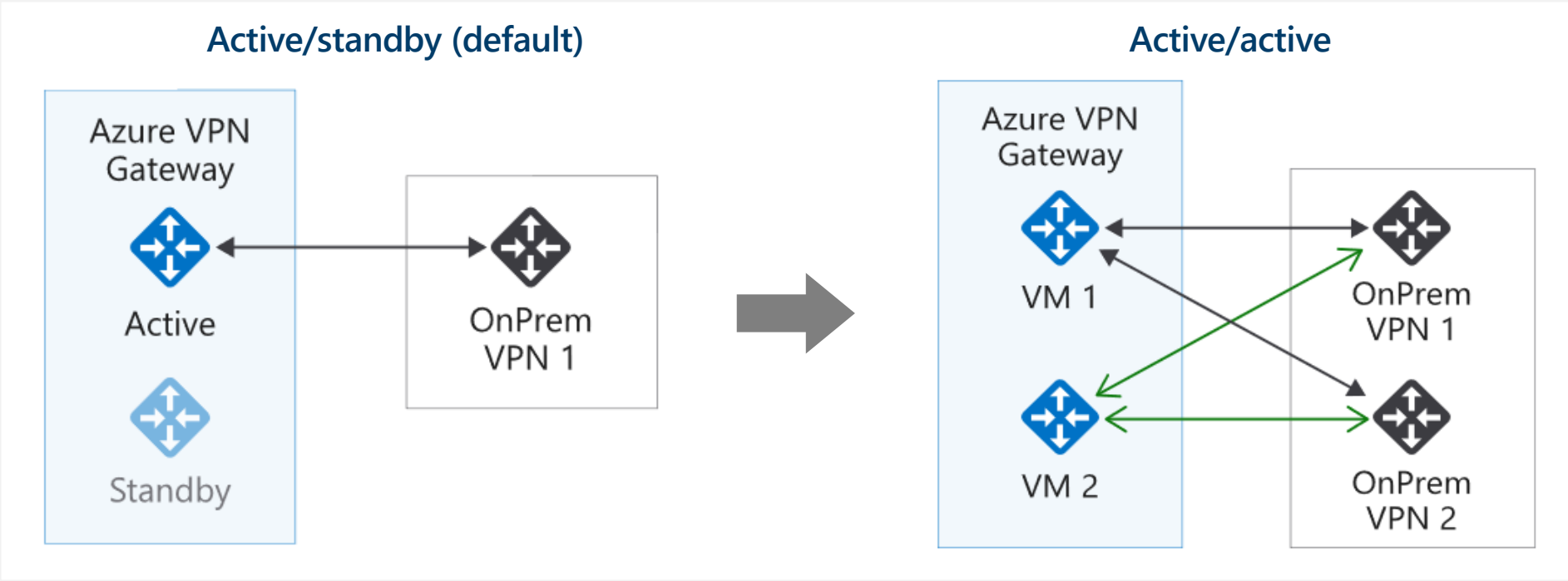
Configure a name for the connection and specify the type as Site-to-site (IPsec)

Select the VPN gateway and the Local Network Gateway

Enter the Shared key for the connection



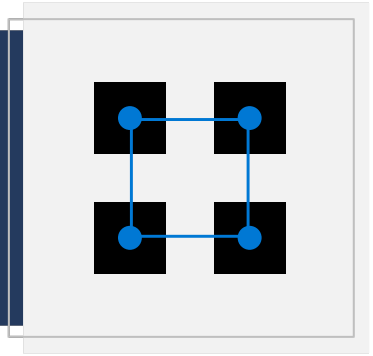
High Availability Scenarios



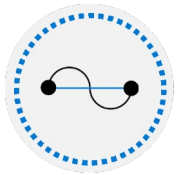
VPN gateways are deployed as two instances

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

Lesson 03: ExpressRoute and Virtual WAN



ExpressRoute and Virtual WAN Overview

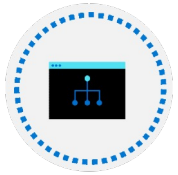


ExpressRoute

ExpressRoute Capabilities

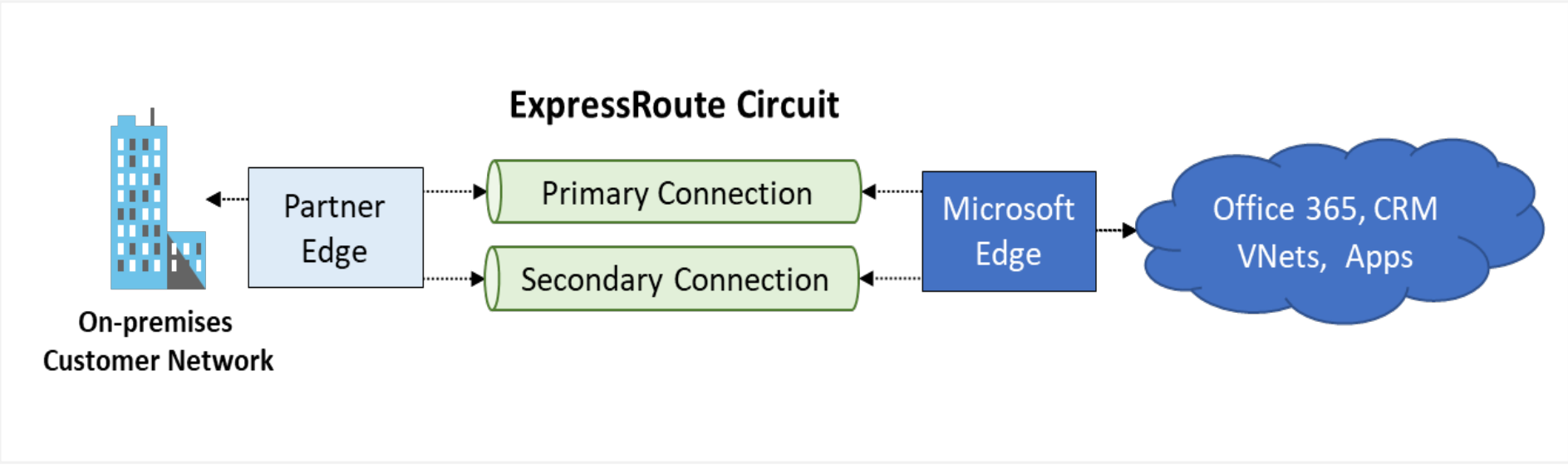
Coexisting Site-to-Site and ExpressRoute

Intersite Connection Comparisons



Virtual WANs

ExpressRoute



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

ExpressRoute Capabilities

Layer 3 connectivity with redundancy

Connectivity to all regions within a geography

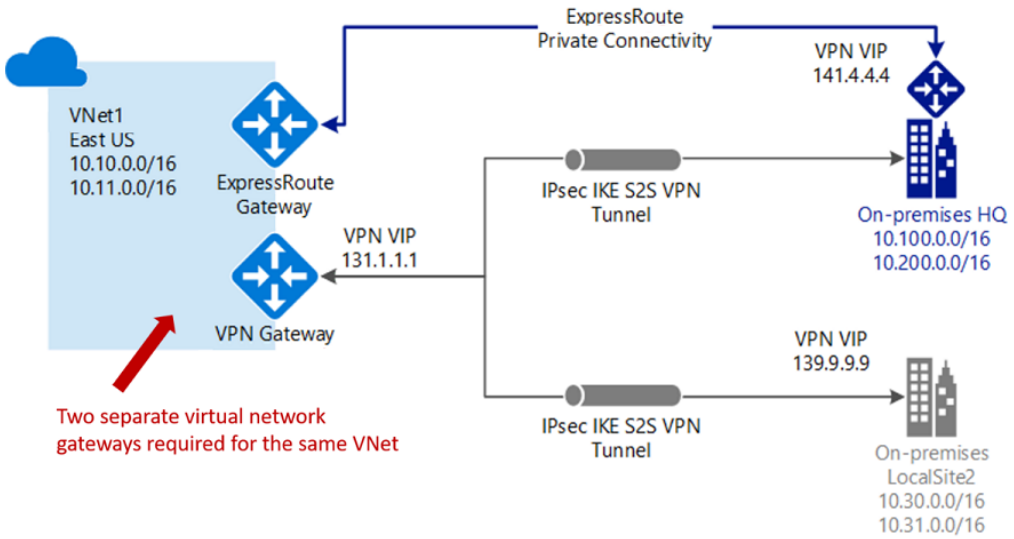
Global connectivity with ExpressRoute premium add-on

Across on-premises connectivity with ExpressRoute Global Reach

Bandwidth options – 50 Mbps to 100 Gbps

Billing models – Unlimited, metered, premium

Coexisting 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

Intersite Connections Comparison

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

Virtual WANs

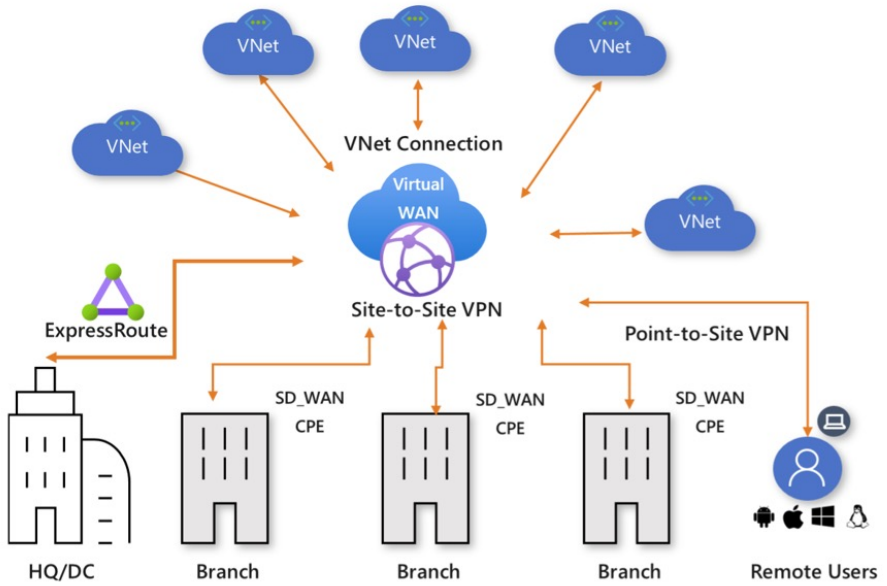
Brings together S2S, P2S, and ExpressRoute

Integrated connectivity using a hub-and-spoke connectivity model

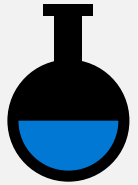
Connect virtual networks and workloads to the Azure hub automatically

Visualize the end-to-end flow within Azure

Two types: Basic and Standard



Lesson 04: Module 05 Lab and Review



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

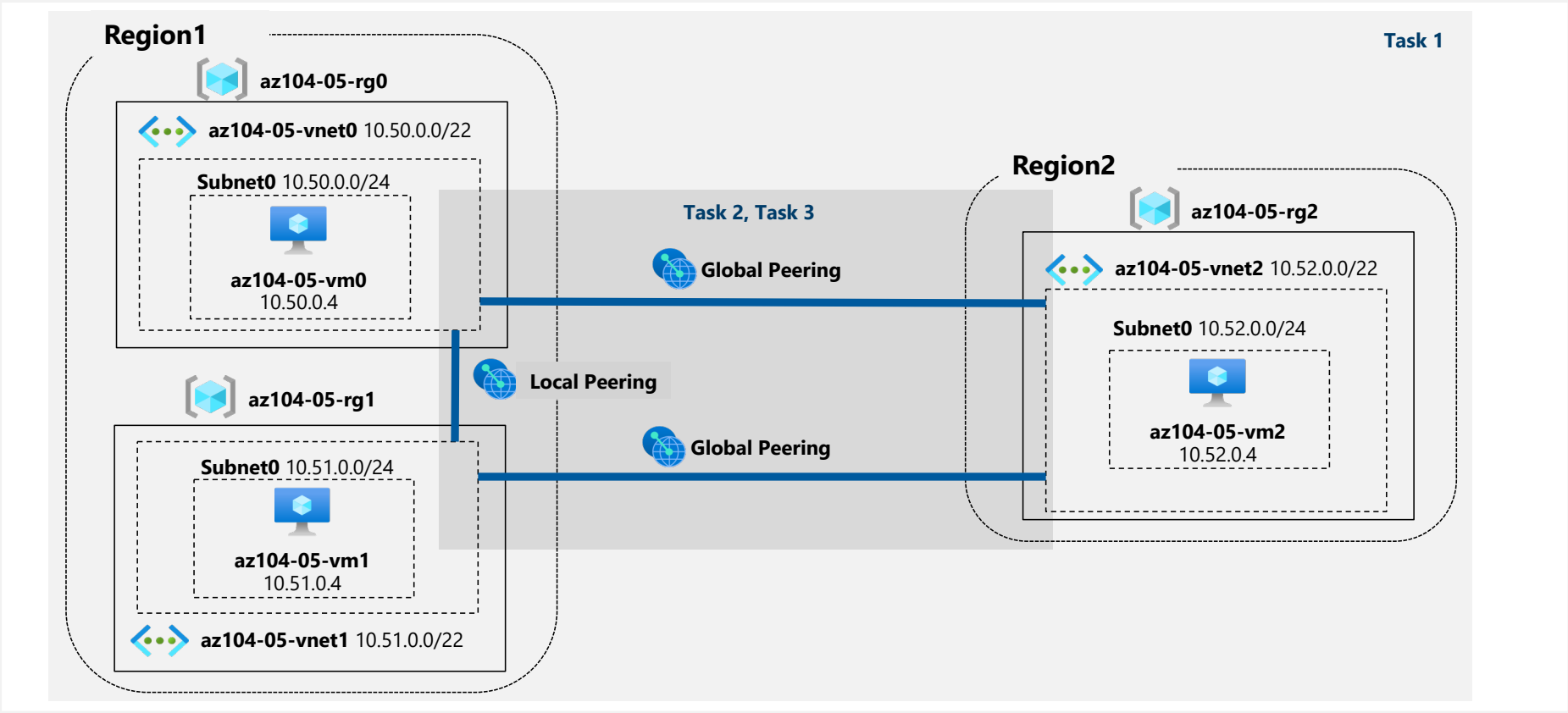
Task 1:
Provision the lab environment

Task 2:
Configure local and global virtual network peering

Task 3:
Test intersite connectivity

Next slide for an architecture diagram

Lab 05 – Architecture diagram



Module Review

Module Review Questions

Microsoft Learn Modules (docs.microsoft.com/Learn)

Distribute your services across Azure virtual networks and integrate them by using virtual network peering

Connect your on-premises network to Azure with VPN gateway

Connect your on-premises network to the Microsoft global network by using ExpressRoute

End of presentation