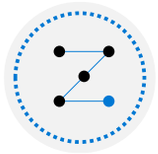
Microsoft Azure

AZ-104

Administer Intersite Connectivity

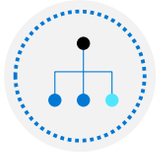
About this course: Course Outline

01: Administer Identity



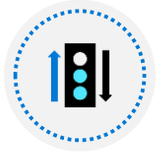
02: Administer Governance and Compliance

03: Administer Azure Resources



04: Administer Virtual Networking

05: Administer Intersite Connectivity



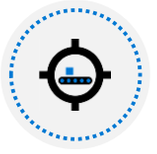
06: Administer Network Traffic Management

07: Administer Azure Storage

08: Administer Azure Virtual Machines

09: Administer PaaS Compute Options

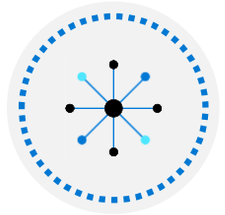
10: Administer Data Protection



11: Administer Monitoring

Administer Intersite Connectivity Introduction

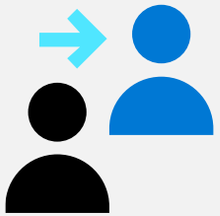
Configure VNet Peering



Configure Network Routing and Endpoints

Lab 05 - Implement Intersite Connectivity

Configure VNet Peering



Configure VNet Peering Introduction

Determine VNet Peering Uses

Determine Gateway Transit and Connectivity Needs

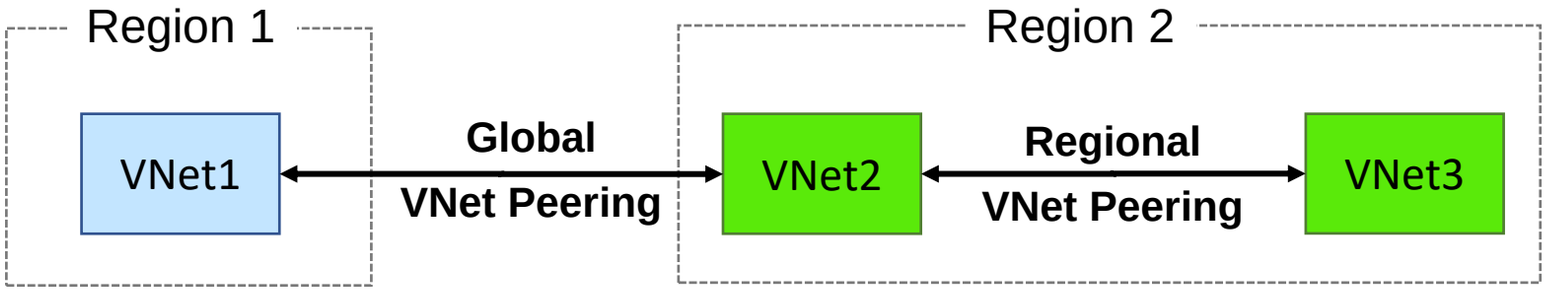
Create VNet Peering

Determine Service Chaining Uses

Demonstration – VNet Peering

Summary and Resources

Determine VNet Peering Uses



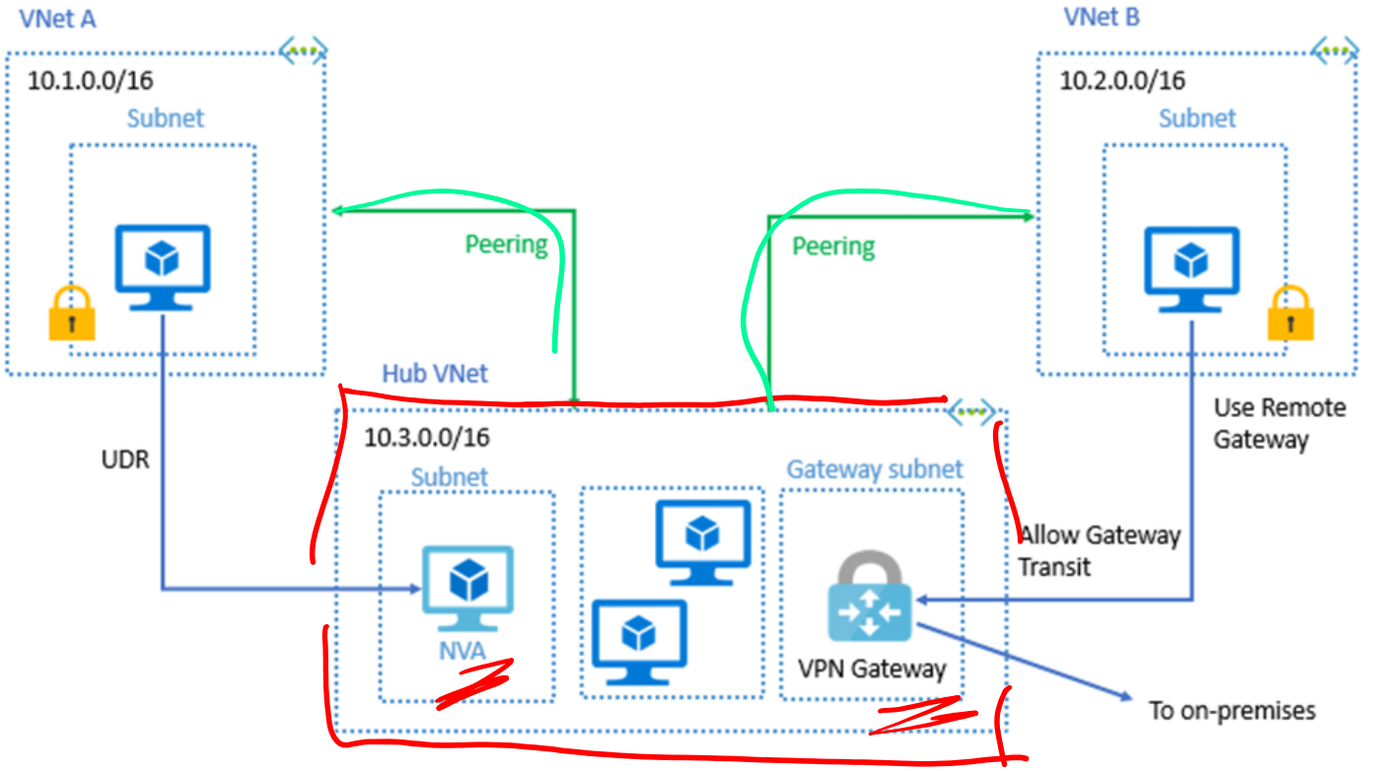
- Two types of peering: Global and Regional
- Connects two Azure virtual networks – you can peer across subscriptions and tenants
- Peered networks use the Azure backbone for privacy and isolation
- Easy to setup, seamless data transfer, and great performance

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



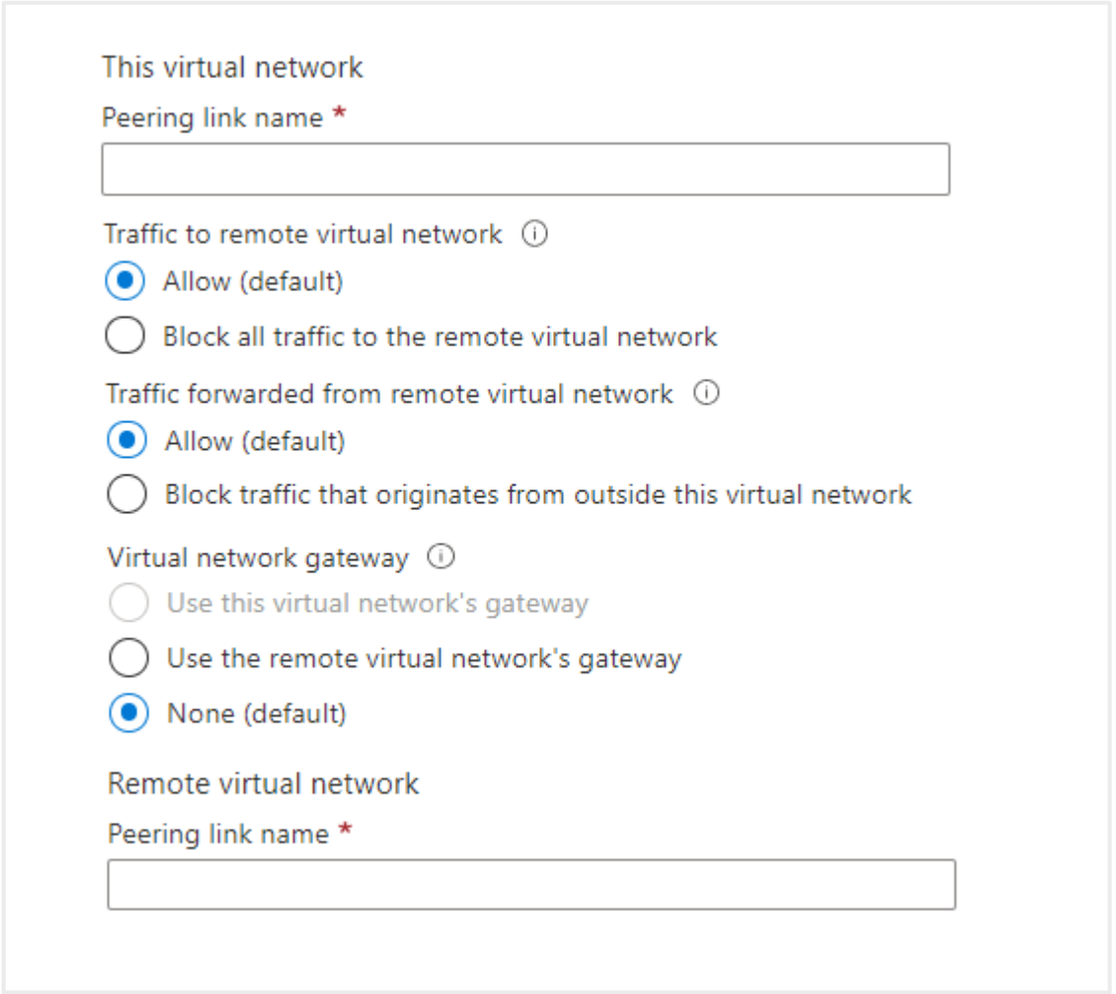
✓ **IP address spaces of connected networks can't overlap**

Create VNet Peering

Allow virtual network access settings

Configure forwarded traffic settings

To peering links must be created and shown in "connected" status

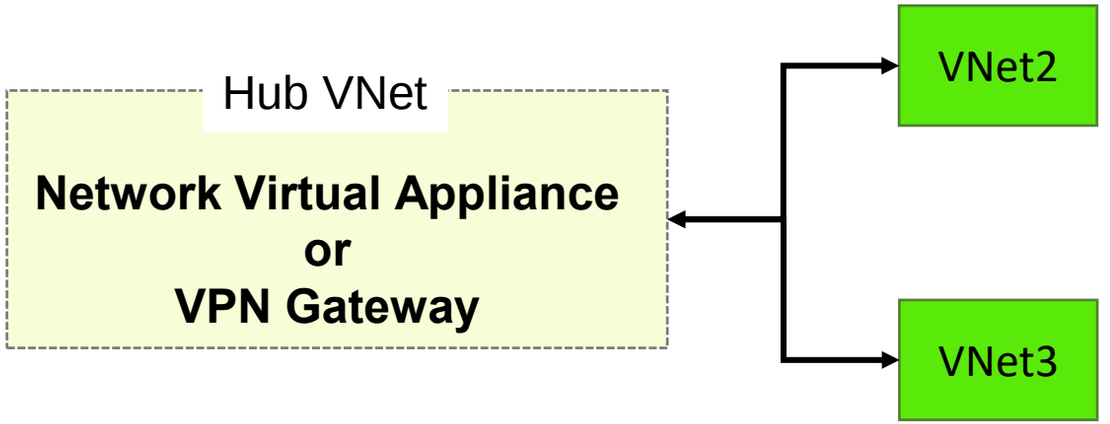


Determine Service Chaining Uses

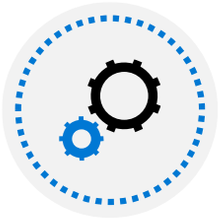
Leverage user-defined routes and service chaining to implement custom routing

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



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

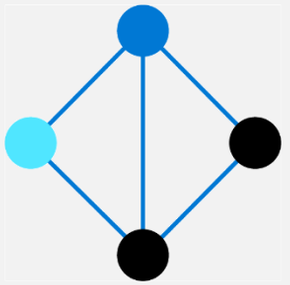
Knowledge Check Questions

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

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

A *sandbox* indicates a hands-on exercise.

Configure Network Routing and Endpoints



Configure Network Routing and Endpoints Introduction

Review System Routes

Identify User-Defined Routes

Demonstration – Custom Routing tables

Determine Service Endpoint Uses

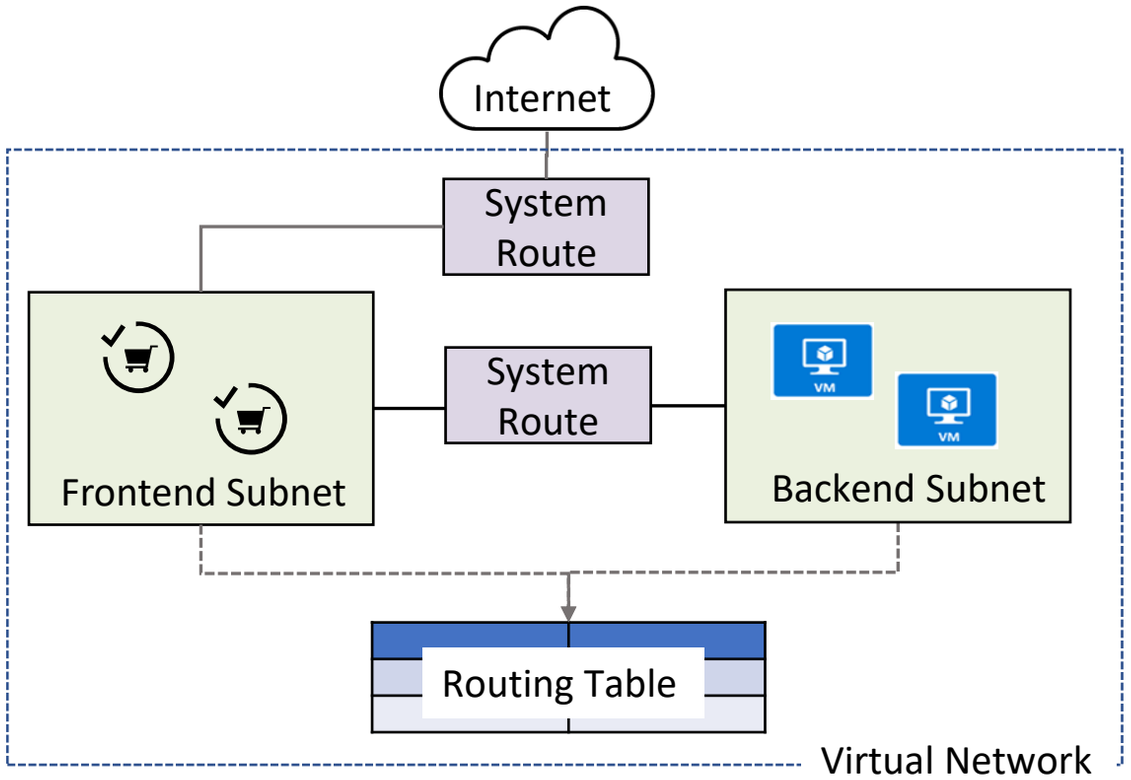
Identify Private Link Uses

Summary and Resources

Review System Routes

System routes direct network traffic between virtual machines, on-premises networks, and the internet:

- Traffic between VMs in the same subnet
- Between VMs in different subnets in the same virtual network
- Data flow from VMs to the internet
- Communication between VMs using a VNet-to-VNet VPN
- Site-to-Site and ExpressRoute communication through the VPN gateway

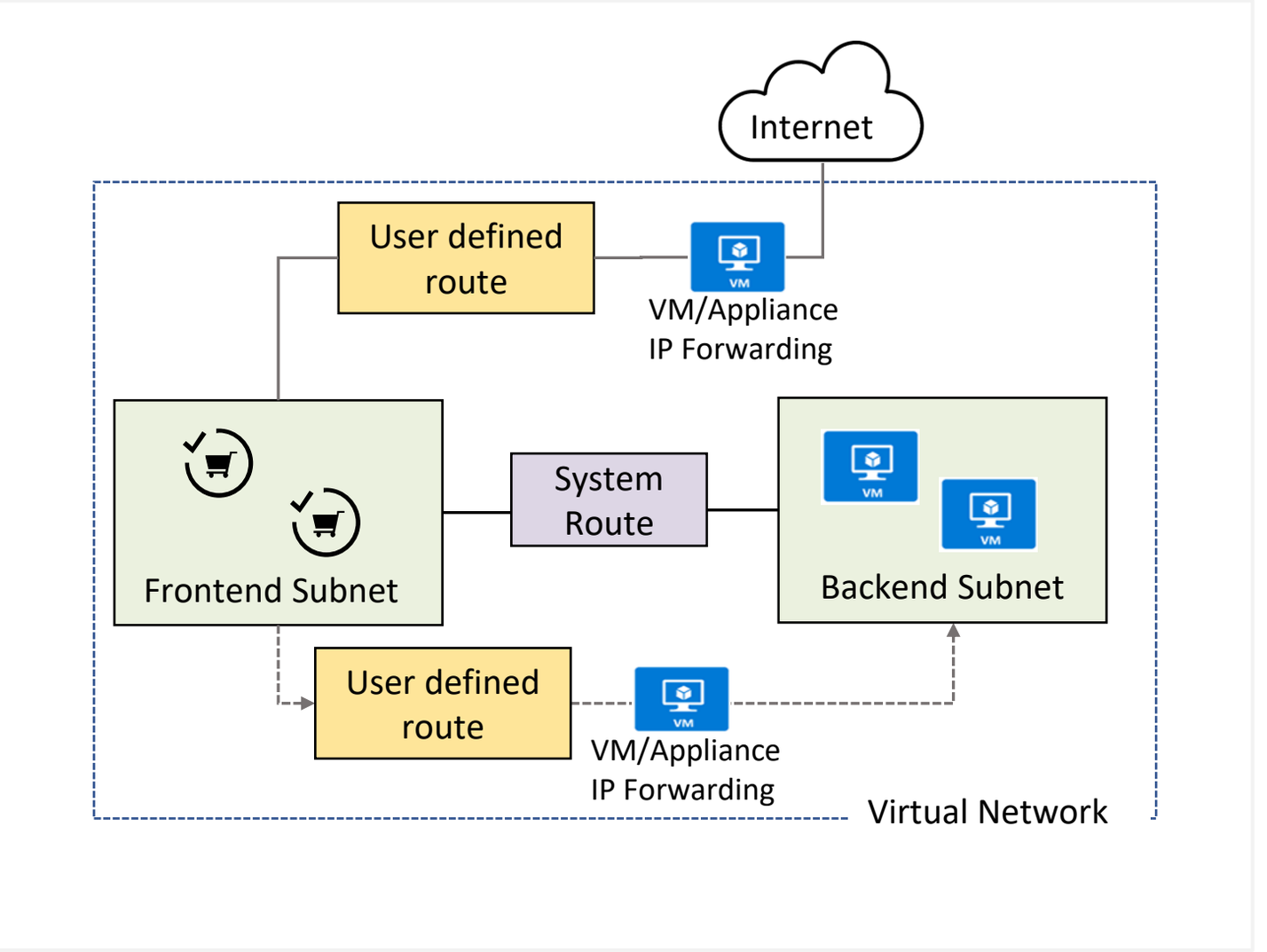


Identify User-Defined Routes

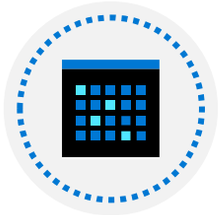
A route table contains a set of rules, called routes, that specifies how packets should be routed in a virtual network

User-defined routes are custom routes that control network traffic by defining routes that specify the next hop of the traffic flow

The next hop can be a virtual network gateway, virtual network, internet, or virtual appliance



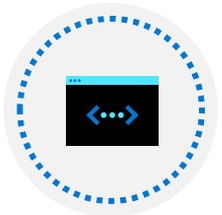
Demonstration – Custom Routing Tables



Create a route table

Add a route

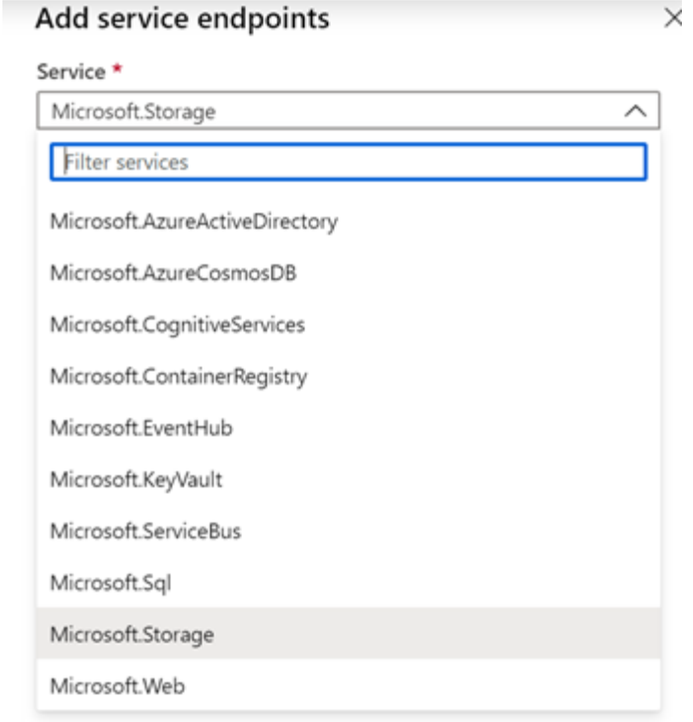
Associate a route table to a subnet

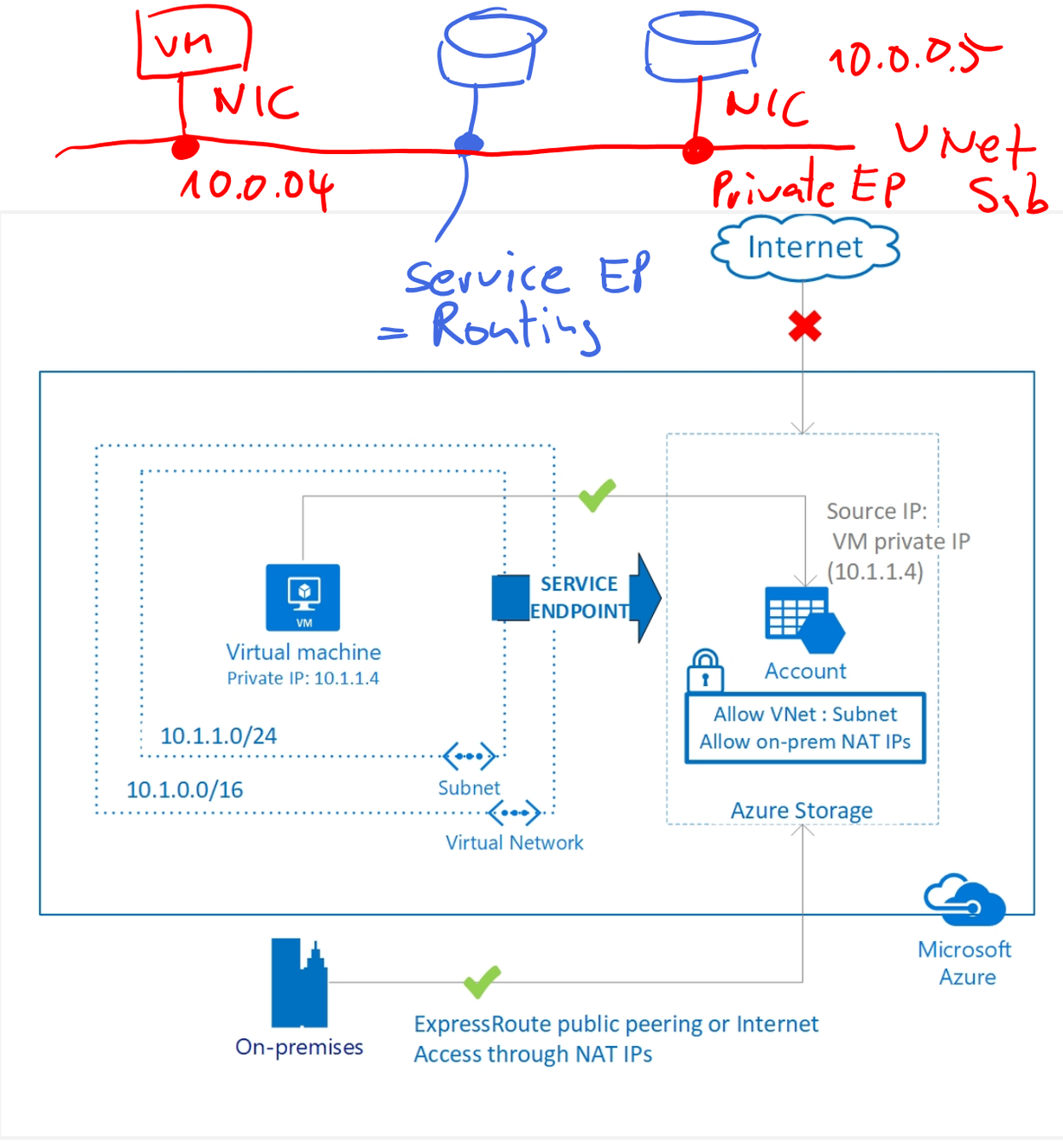


Use PowerShell to view your routing information (optional)

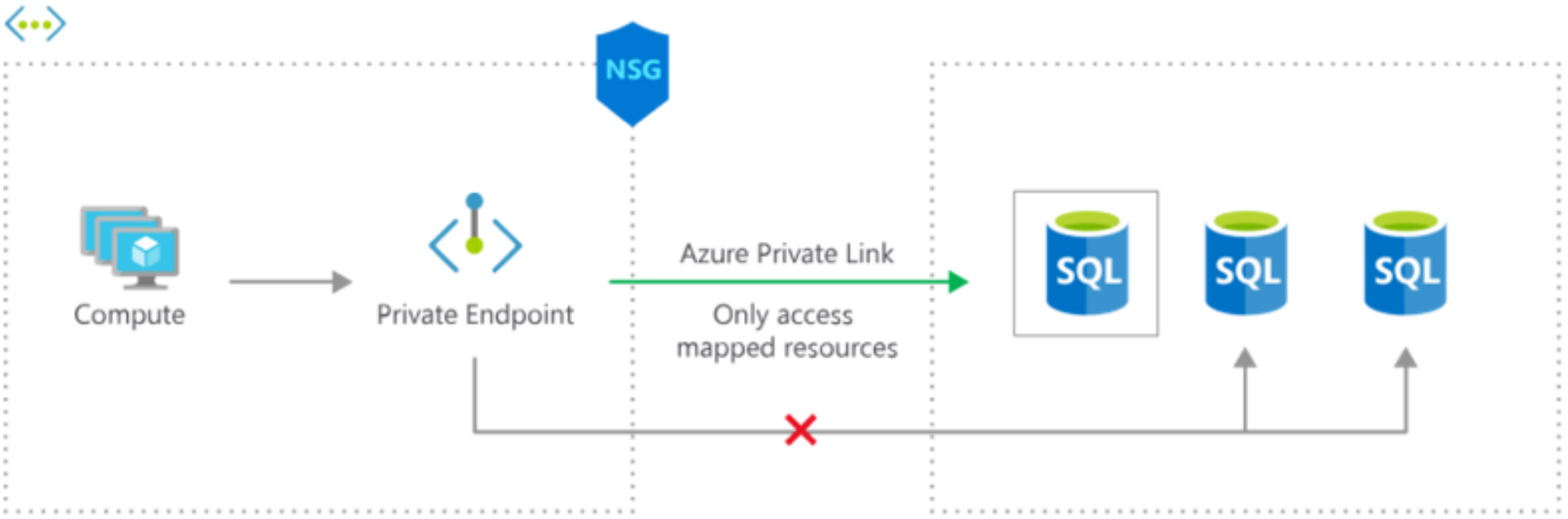
Determine Service Endpoint Uses

Endpoints limit network access to specific services -Adding service endpoints can take up to 15 minutes to complete





Identify Private Link Uses



Private connectivity to services on Azure. Traffic remains on the Microsoft network, with no public internet access

Integration with on-premises and peered networks

In the event of a security incident within your network, only the mapped resource would be accessible

Summary and Resources – Configure Network Routing and Endpoints

Knowledge Check Questions

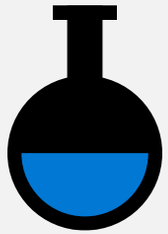
Microsoft Learn Modules (docs.microsoft.com/Learn)

Manage and control traffic flow in your Azure deployment with routes (Sandbox)

Introduction to Azure Private Link

A *sandbox* indicates a hands-on exercise.

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:

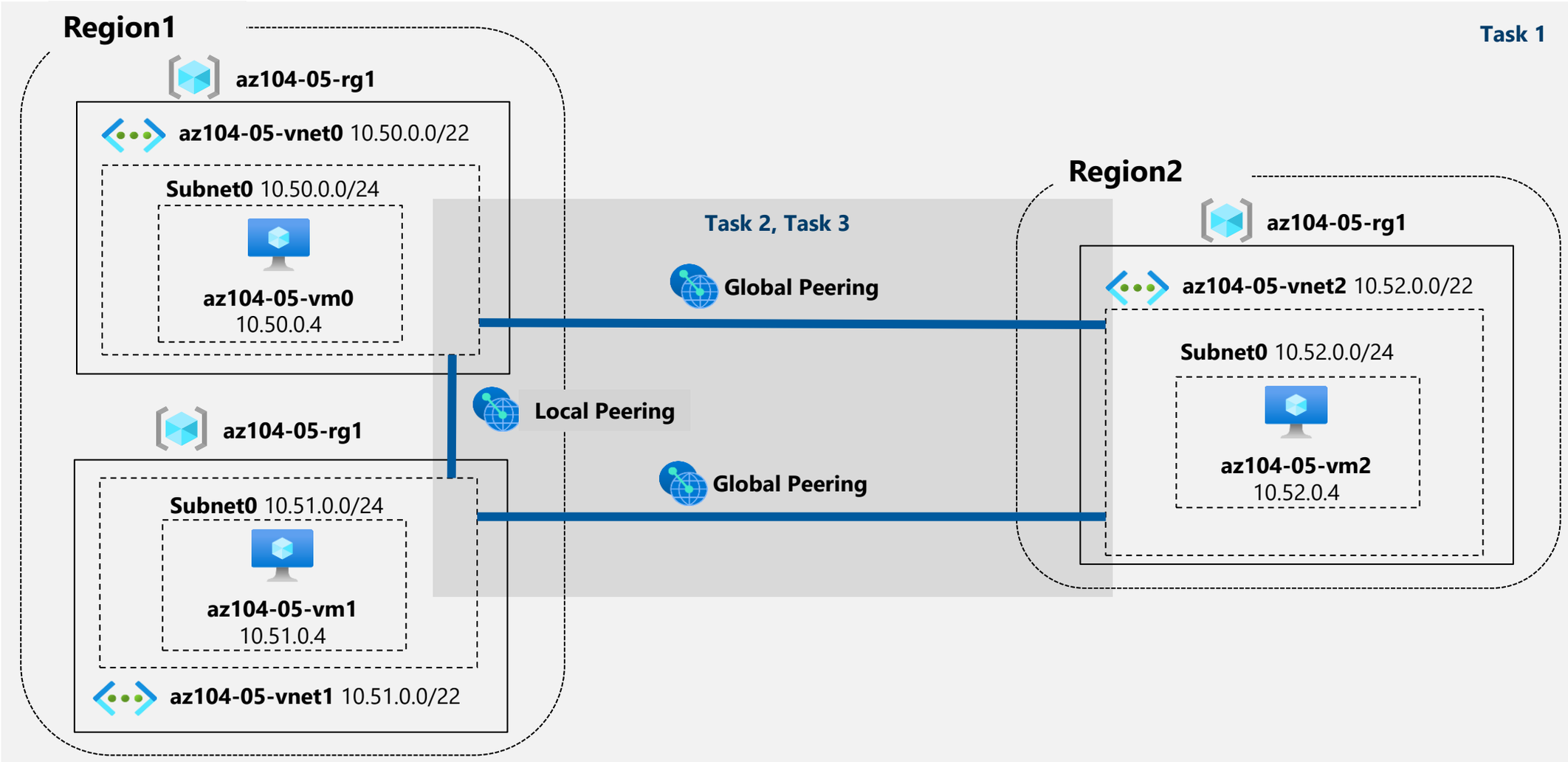
Configure local and global virtual network peering

Task 3:

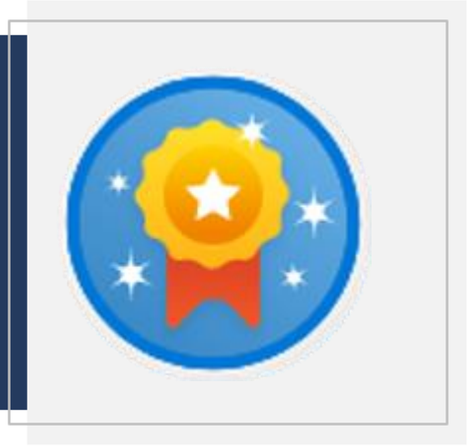
Test intersite connectivity

Next slide for an architecture diagram

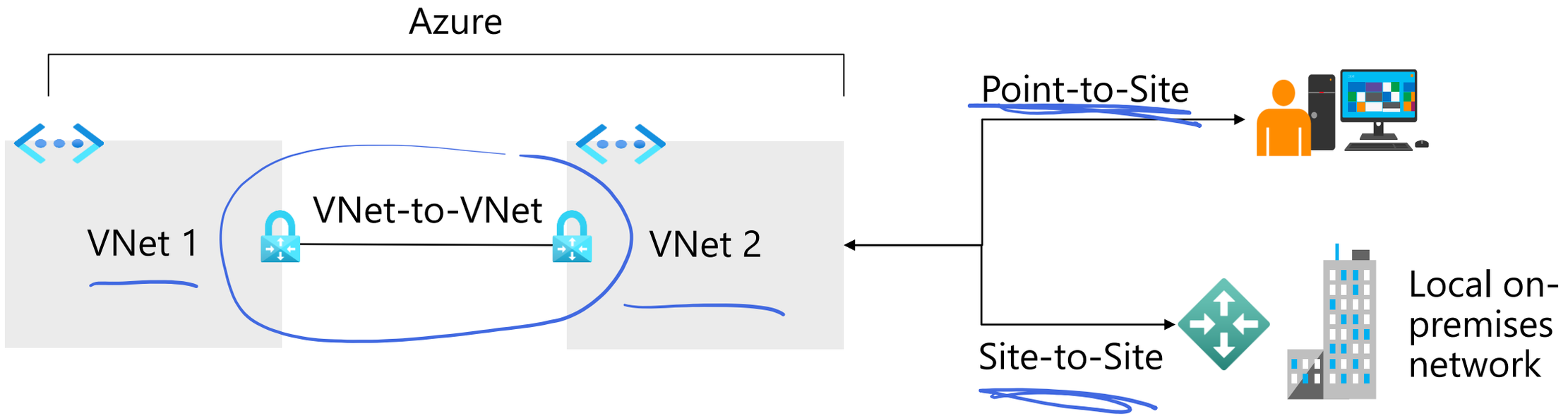
Lab 05 – Architecture diagram



End of presentation



Determine VPN Gateway Uses

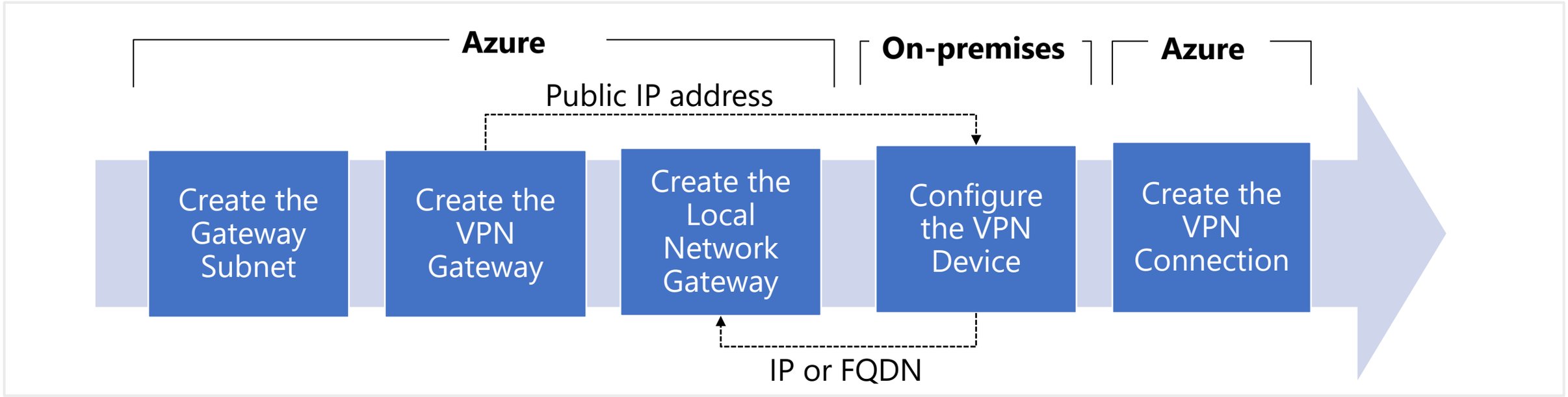


VNet-to-VNet connections connect Azure virtual networks – VNet peering or custom

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