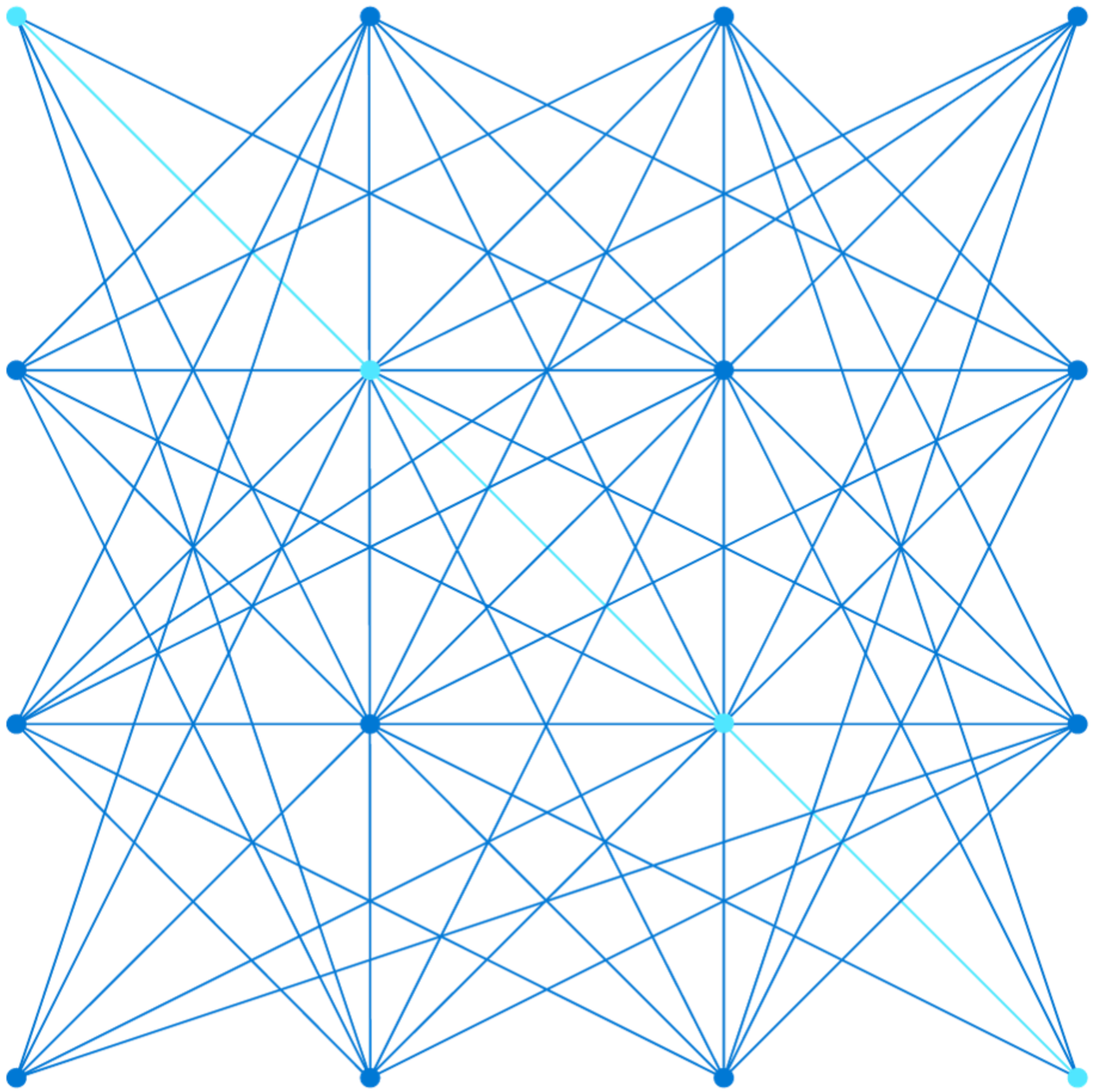
Microsoft Azure

AZ-700

Module 2

Design and Implement Hybrid Networking



Module Overview

- Design and implement Azure VPN Gateway
- Exercise - Create and configure a Virtual Network Gateway
- Connect networks with Site-to-site VPN connections
- Connect devices to networks with Point-to-site VPN connections
- Connect remote resources by using Azure Virtual WANs
- Exercise - Create a Virtual WAN by using the Azure Portal
- Create a network virtual appliance (NVA) in a virtual hub

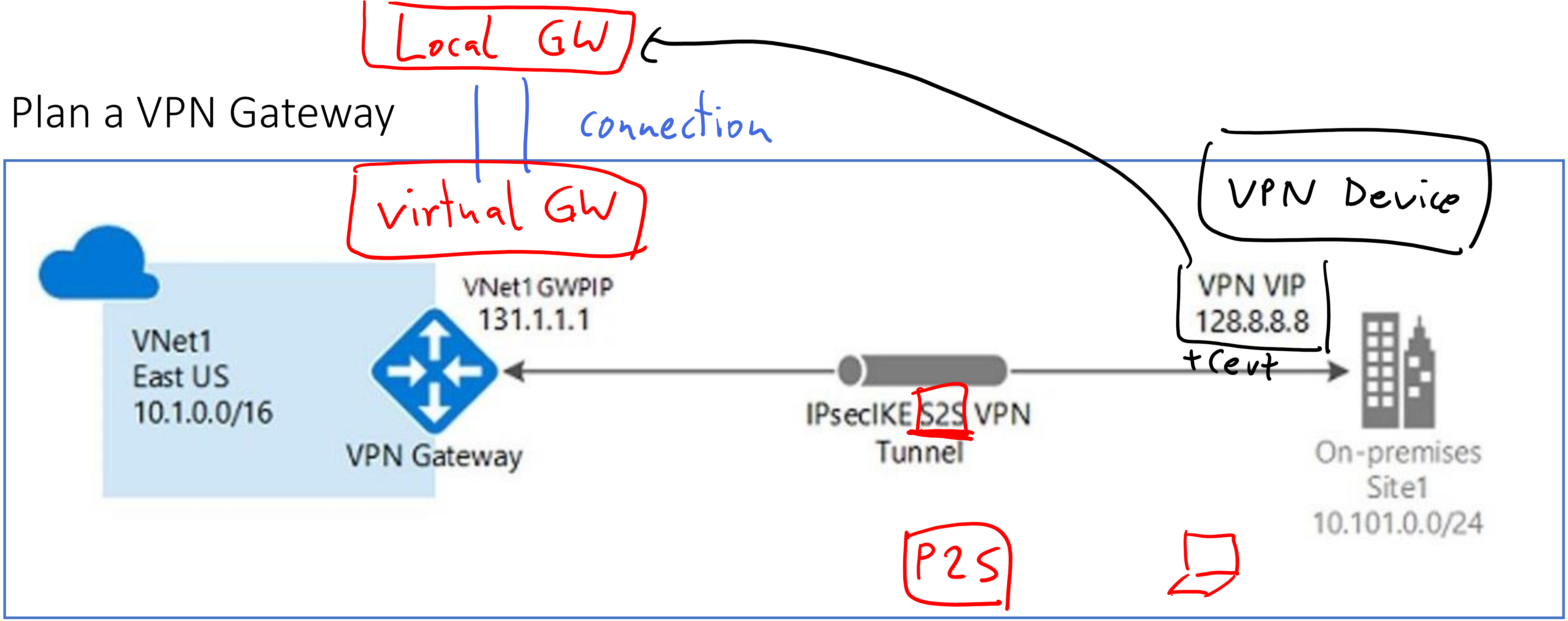
Design and implement Azure VPN gateway

Design and implement Azure VPN Gateway overview

- Plan a VPN Gateway
- Create the Gateway Subnet
- VPN Gateway Configuration requirements
- VPN Gateway Types
- Choose the appropriate Gateway SKU and Generation
- Create the Local Network Gateway
- Configure the on-premises VPN device
- Create the VPN connection
- Verify and troubleshoot the VPN connection
- High availability options for VPN connections
- Demonstration
- Review

Create a zone redundant VNET gateway in Azure Availability zones

Plan a VPN Gateway



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

VNet-to-VNet connections connect Azure virtual networks to each other

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

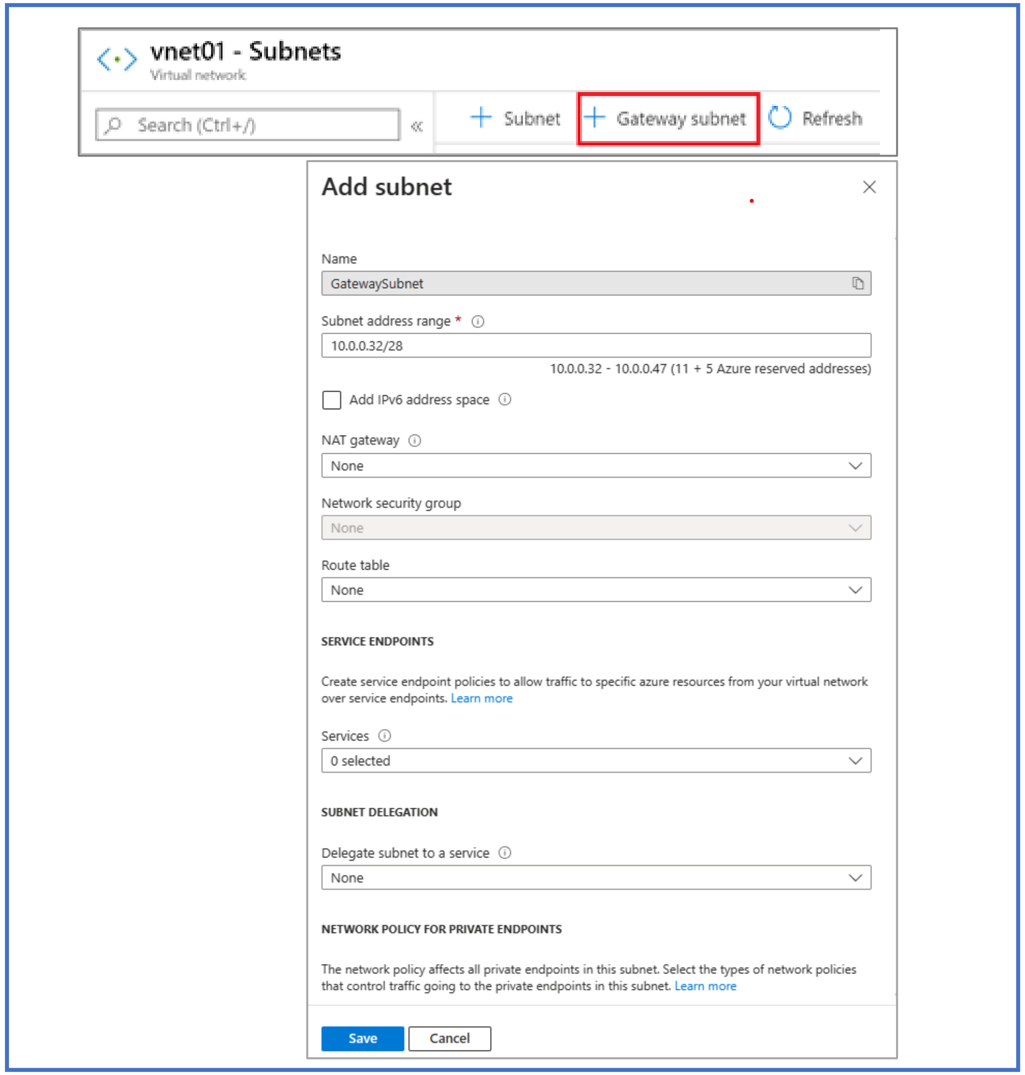
AzureFirewallSubnet
AzureBastionSubnet

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



Add subnet

Name
GatewaySubnet

Subnet address range *
10.0.0.32/28
10.0.0.32 - 10.0.0.47 (11 + 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 over service endpoints. Learn more

Services
0 selected

SUBNET DELEGATION

Delegate subnet to a service
None

NETWORK POLICY FOR PRIVATE ENDPOINTS

The network policy affects all private endpoints in this subnet. Select the types of network policies that control traffic going to the private endpoints in this subnet. Learn more

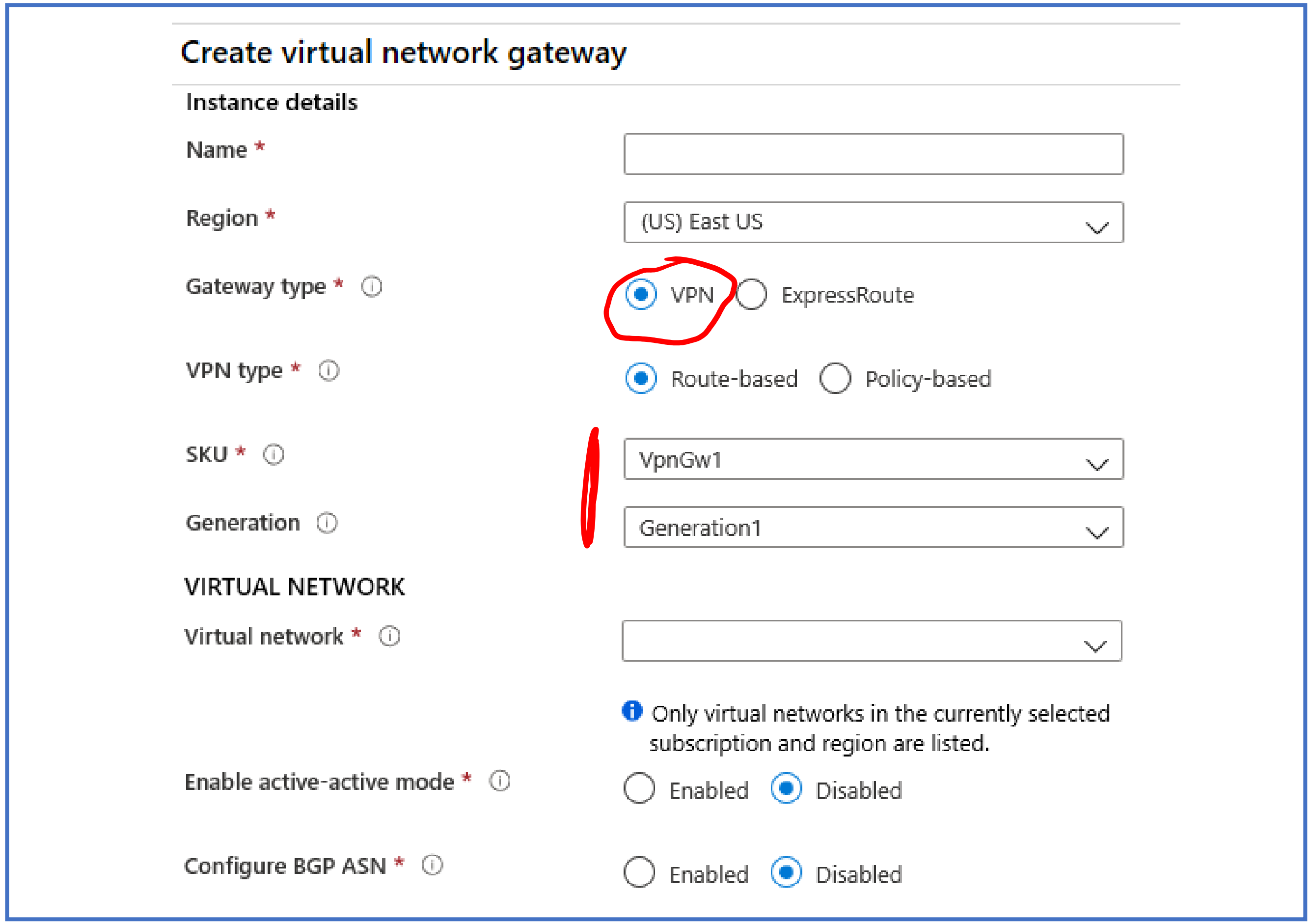
VPN Gateway Configuration requirements

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



Create virtual network gateway

Instance details

Name *

Region * (US) East US

Gateway type * ● VPN ○ ExpressRoute

VPN type * ● Route-based ○ Policy-based

SKU * VpnGw1

Generation Generation1

VIRTUAL NETWORK

Virtual network *

Only virtual networks in the currently selected subscription and region are listed.

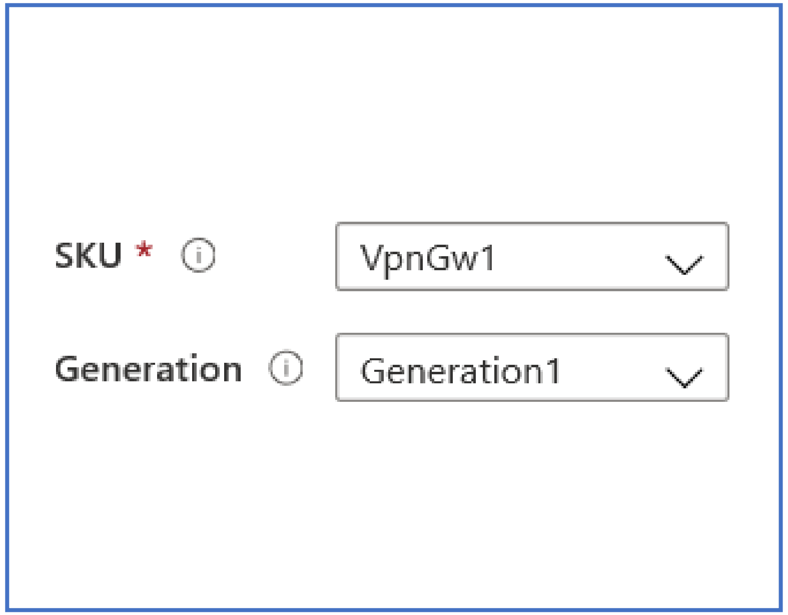
Enable active-active mode * ○ Enabled ● Disabled

Configure BGP ASN * ○ Enabled ● Disabled

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

Mariner Linux ?

Choose the appropriate 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	VpnGw1Az	Max. 30	Max. 250	650 Mbps
1	VpnGw2Az	Max. 30	Max. 500	1.0 Gbps
2	VpnGw2Az	Max. 30	Max. 500	1.25 Gbps
1	VpnGw3Az	Max. 30	Max. 1000	1.25 Gbps
2	VpnGw3Az	Max. 30	Max. 1000	2.5 Gbps
2	VpnGw4Az	Max. 100	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

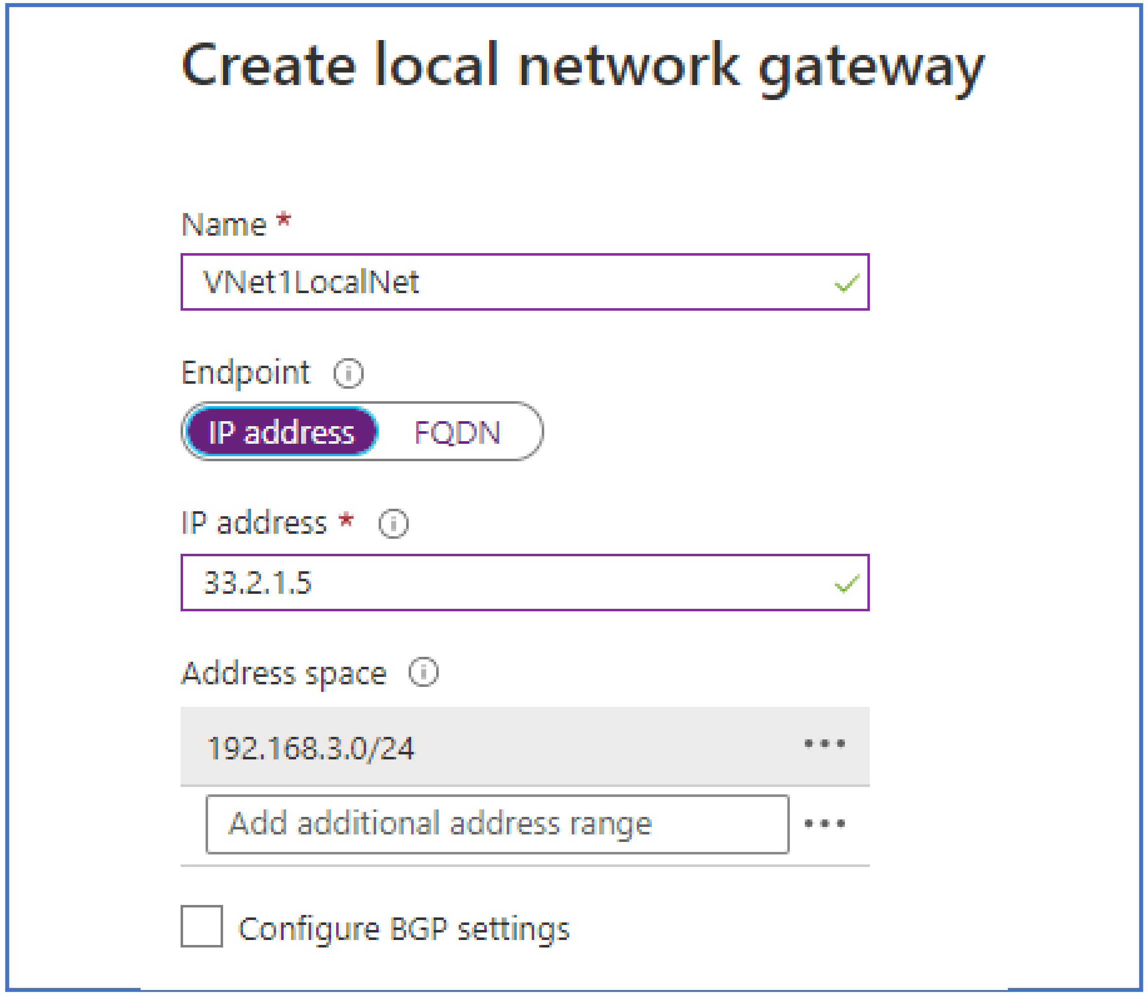
Create the Local Network Gateway

Reflects the on-premises network configuration and enables Azure to route to your on-premises network

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

Configure the On-premises VPN Device

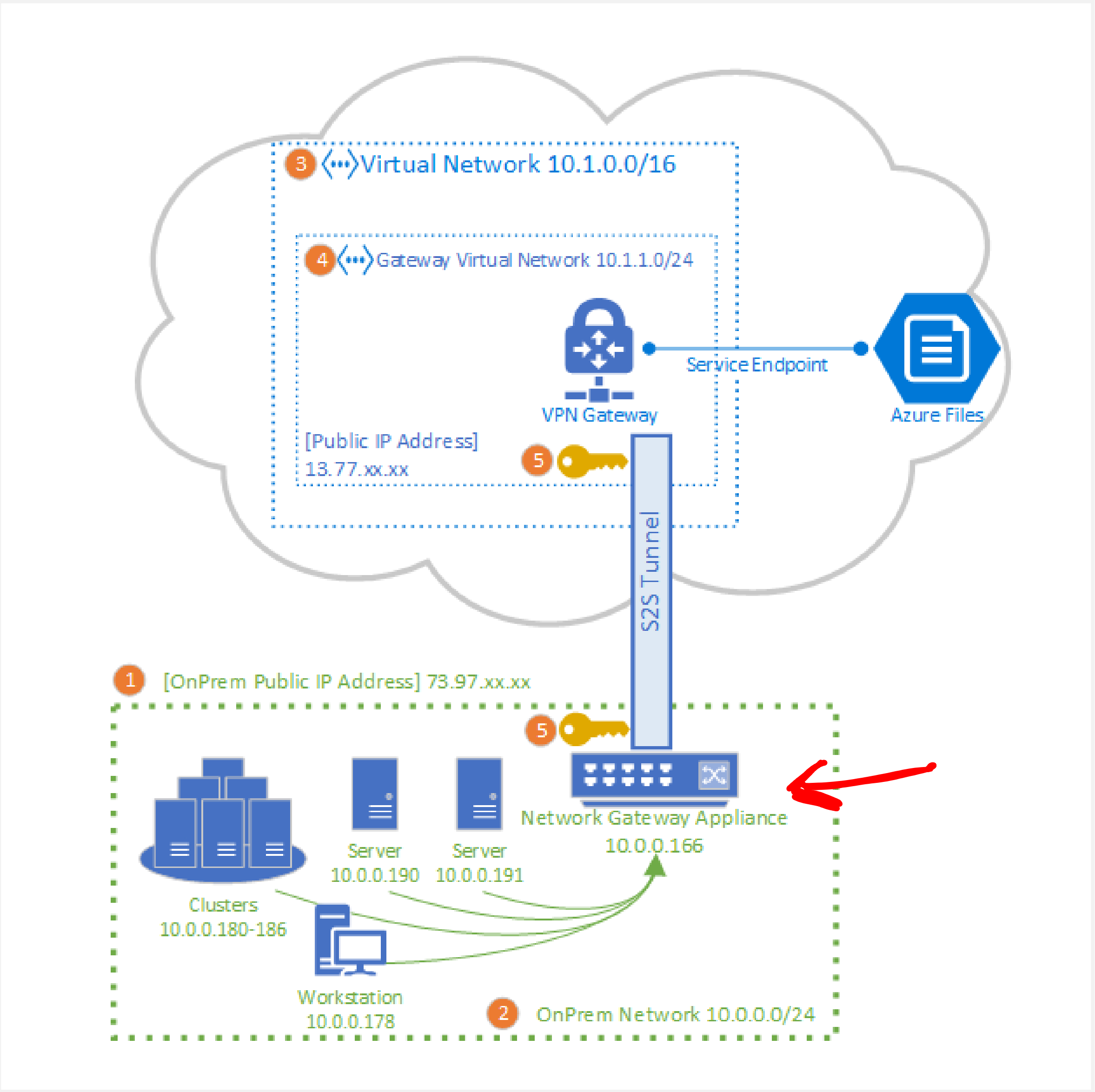
IKE v1
v2

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

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

Specify the public IP address (previous step)

A VPN device configuration script may be available



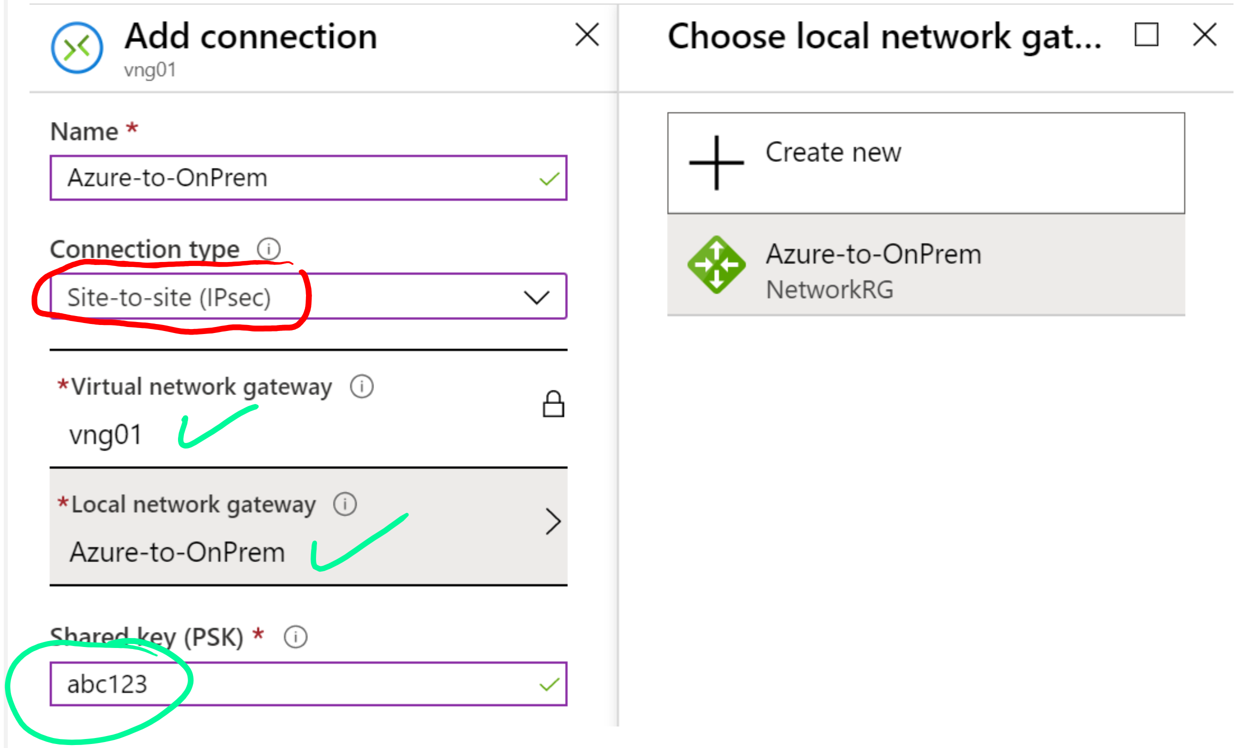
Create the VPN Connection

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 Pre-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 ✓

Choose local network gat...

Azure-to-OnPrem
NetworkRG

Verify and troubleshoot the VPN connection

Validate VPN throughput to a VNet

Utilize Network Watcher

Troubleshoot Azure VPN Gateway using diagnostic logs

Check UDR and NSGs on the gateway subnet

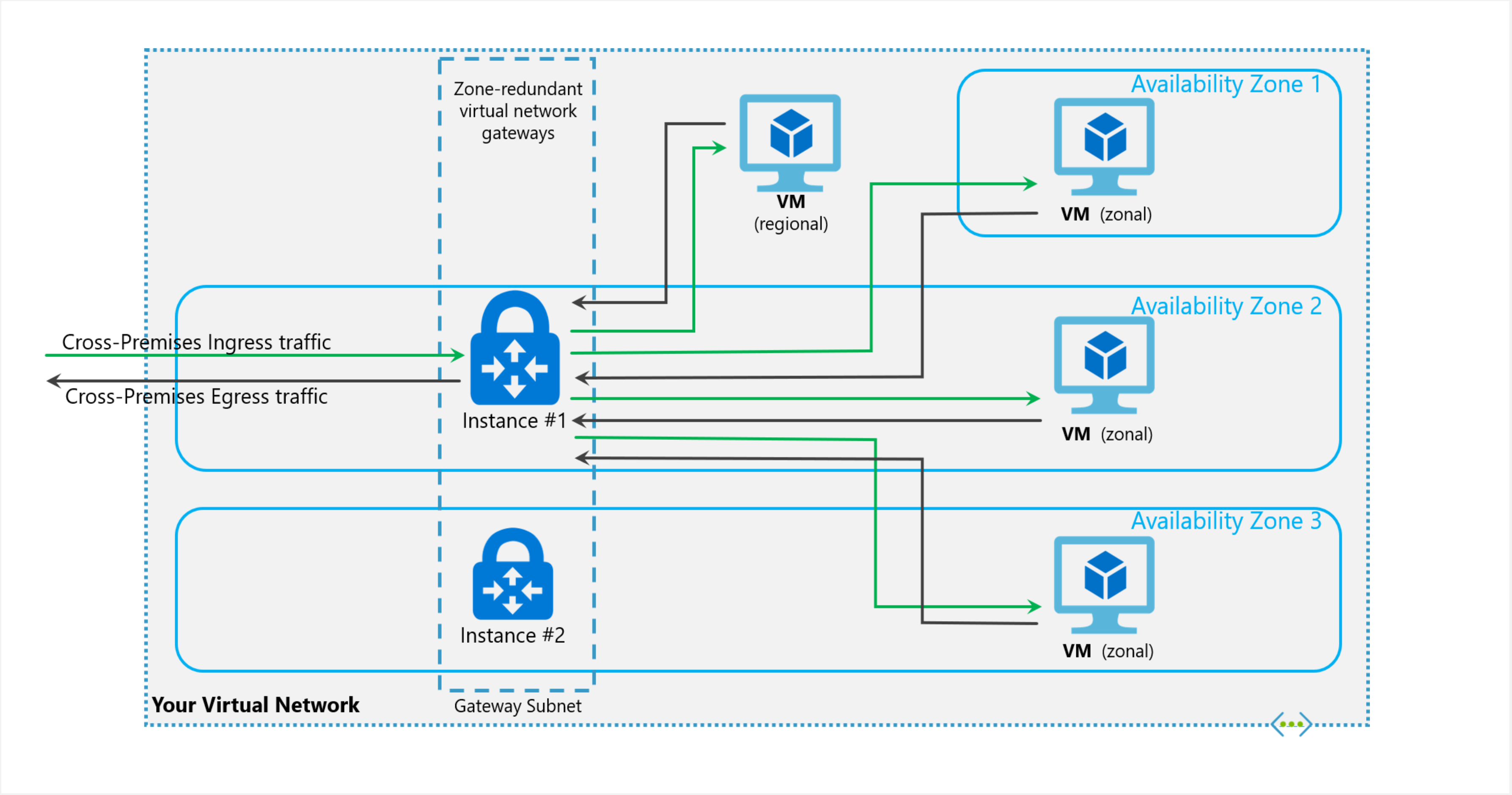
Check whether the on-premises VPN device is validated

Verify the Azure gateway health probe

Verify the shared key and the VPN peer IPs

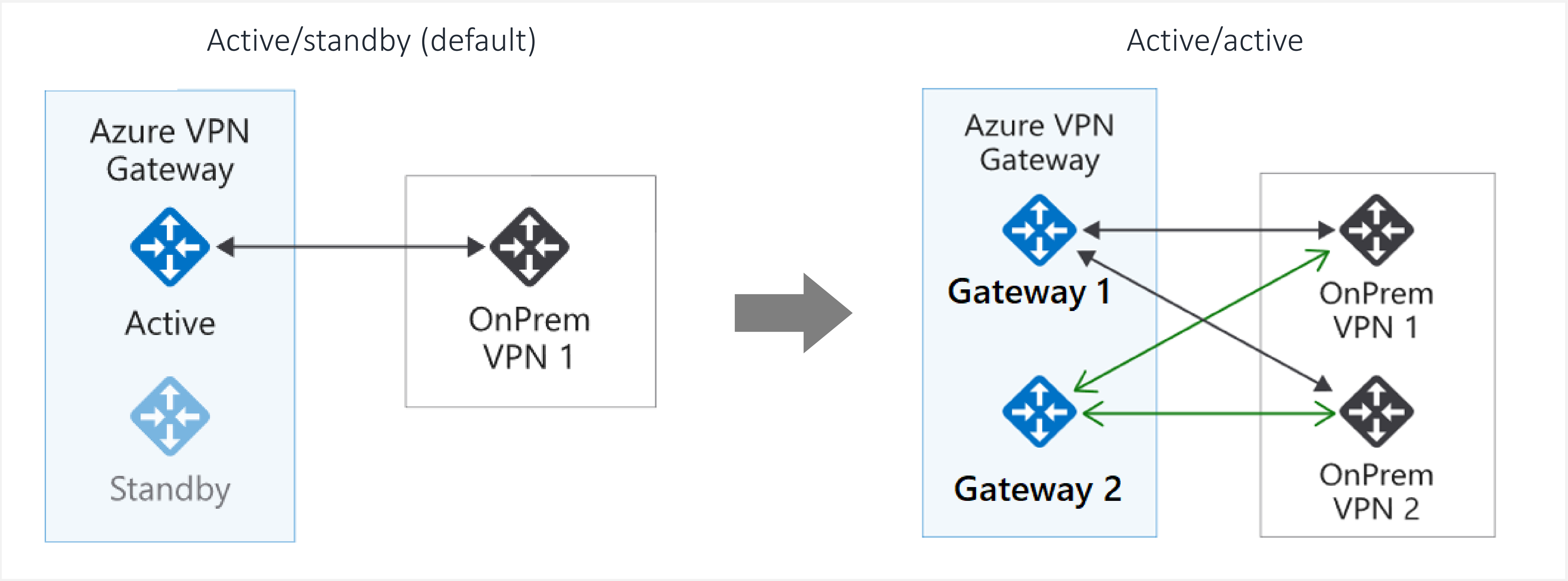
Check whether the on-premises VPN device has the perfect forward secrecy feature enabled

Create a zone redundant VNET gateway in Azure Availability zones



Tables LA workspace KQL Kusto

High availability options for VPN connections



VPN gateways are deployed as two instances

Enable active/active mode for higher availability

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

Summary – Design and implement Azure VPN Gateway

Check your knowledge

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

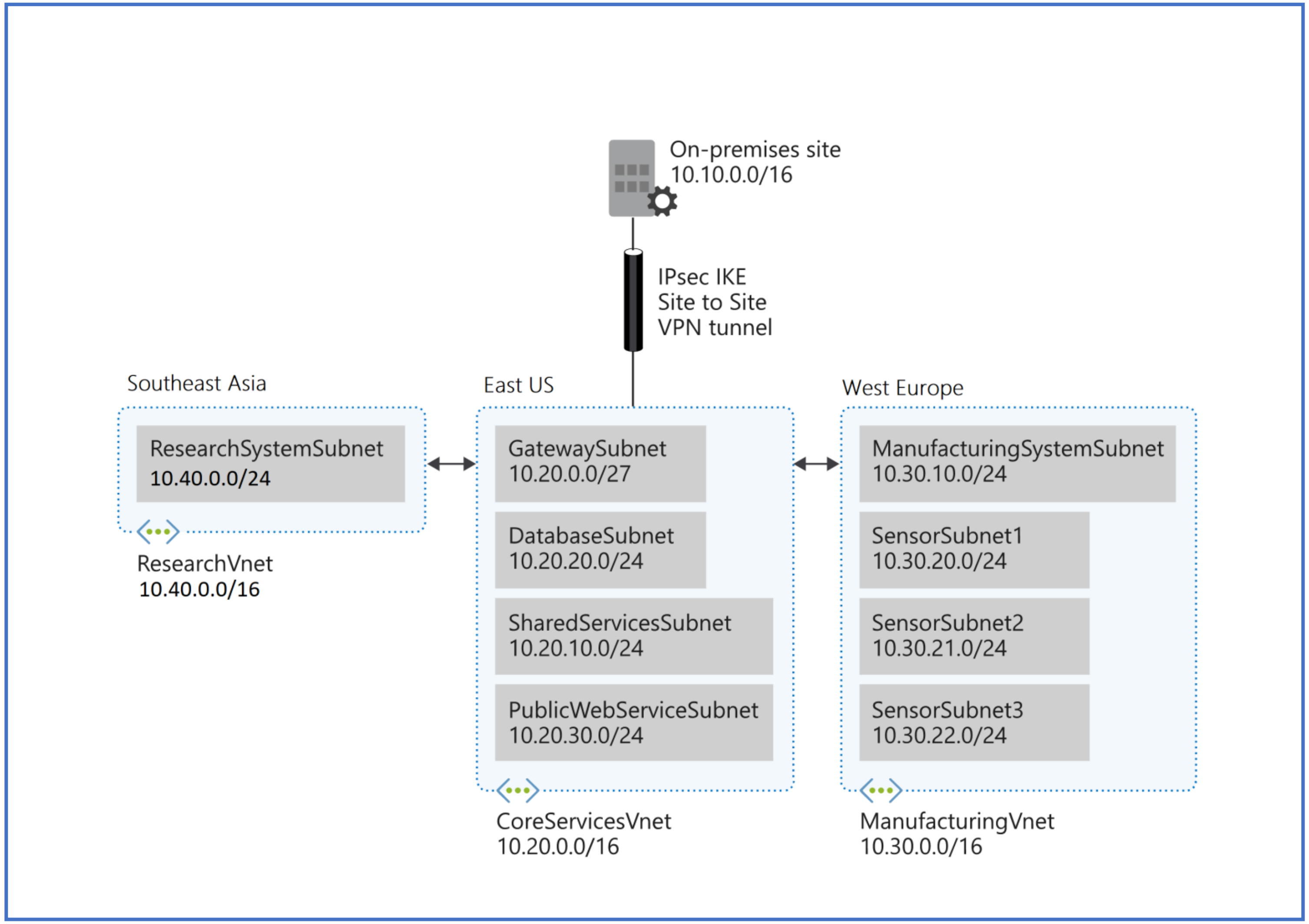
[VPN Gateway documentation | Microsoft Docs]

[Introduction to Azure VPN Gateway - Training | Microsoft Learn]

Exercise - Create and configure a Virtual Network Gateway

Exercise –Create and configure a virtual network gateway

Configure a virtual network gateway to connect the Contoso Core Services VNet and Manufacturing VNet



Connect Networks with Site-to-site VPN Connections

Connect Networks with Site-to-site VPN Connections overview

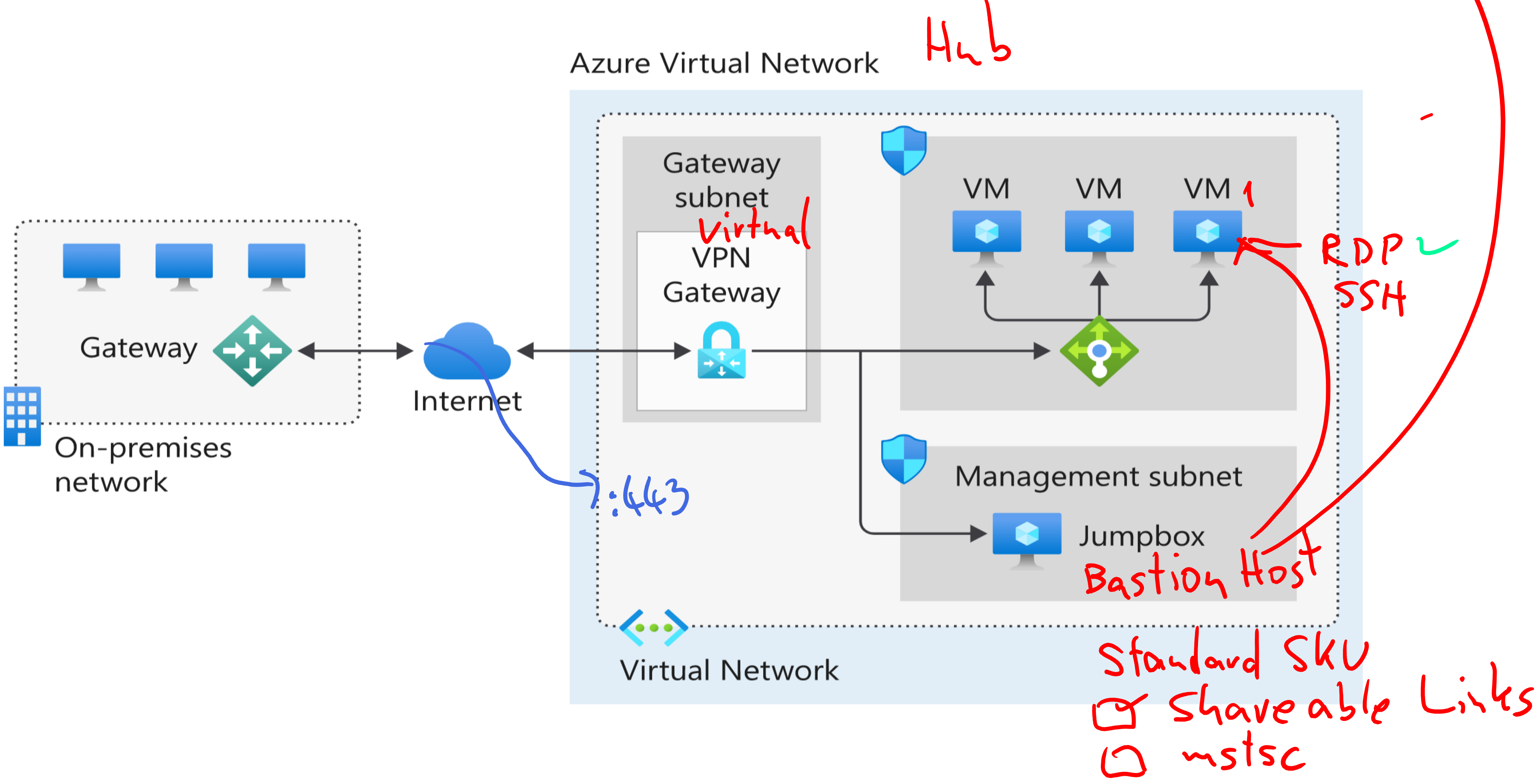
Site-to-site VPN Connections

Review

Site-to-site VPN connections

Spoke VM2

Peering



Summary – Site-to-Site VPN Connections

Check your knowledge

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

[Tutorial - Connect on-premises network to virtual network: Azure portal - Azure VPN Gateway | Microsoft Docs]()

Connect devices to networks with Point-to-site VPN connections

Connect devices to networks with Point-to-site VPN connections overview

Point-to-site protocols

Point-to-site authentication methods

Configure Point-to-site clients

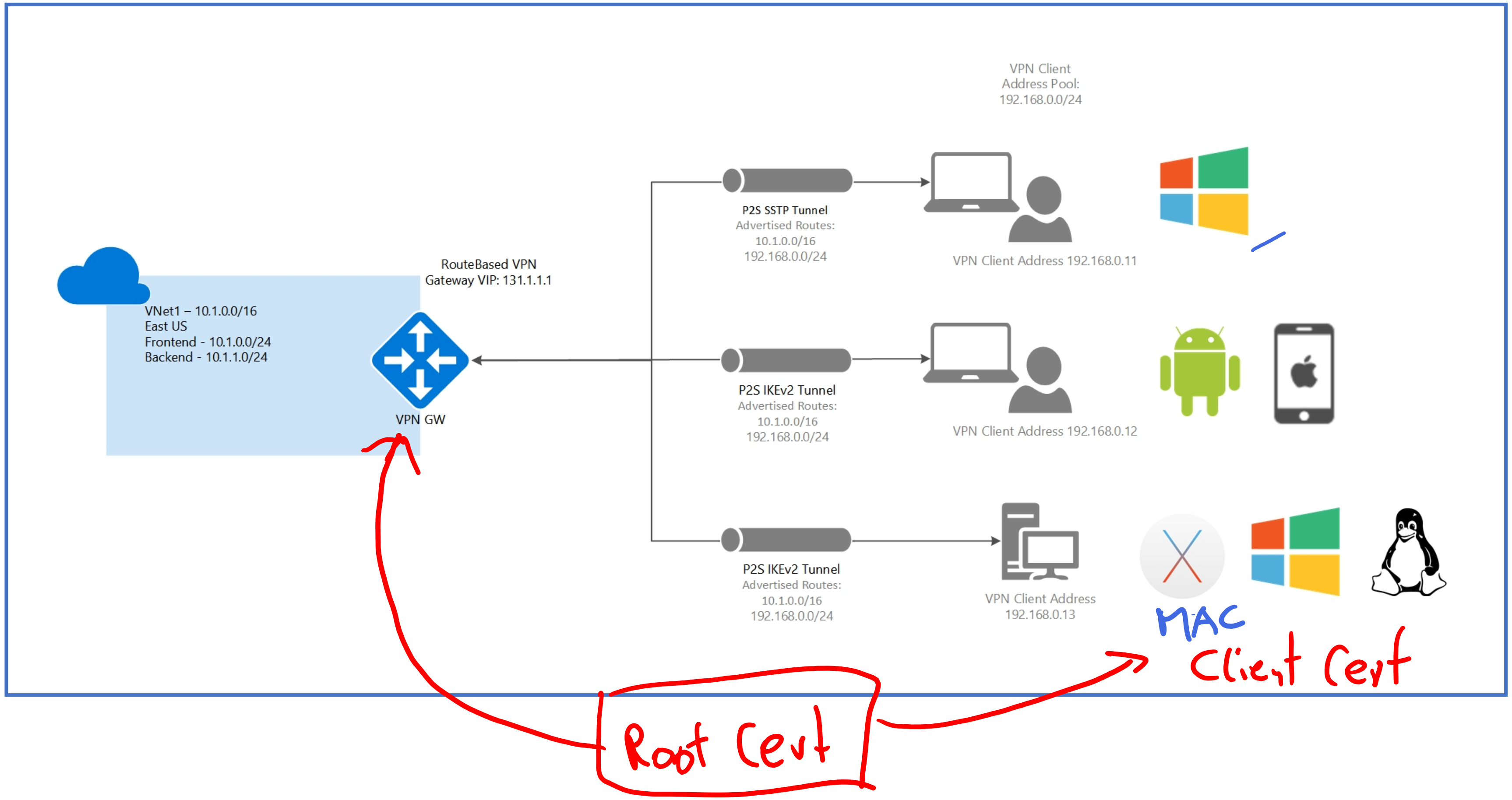
Review

Point-to-site protocols

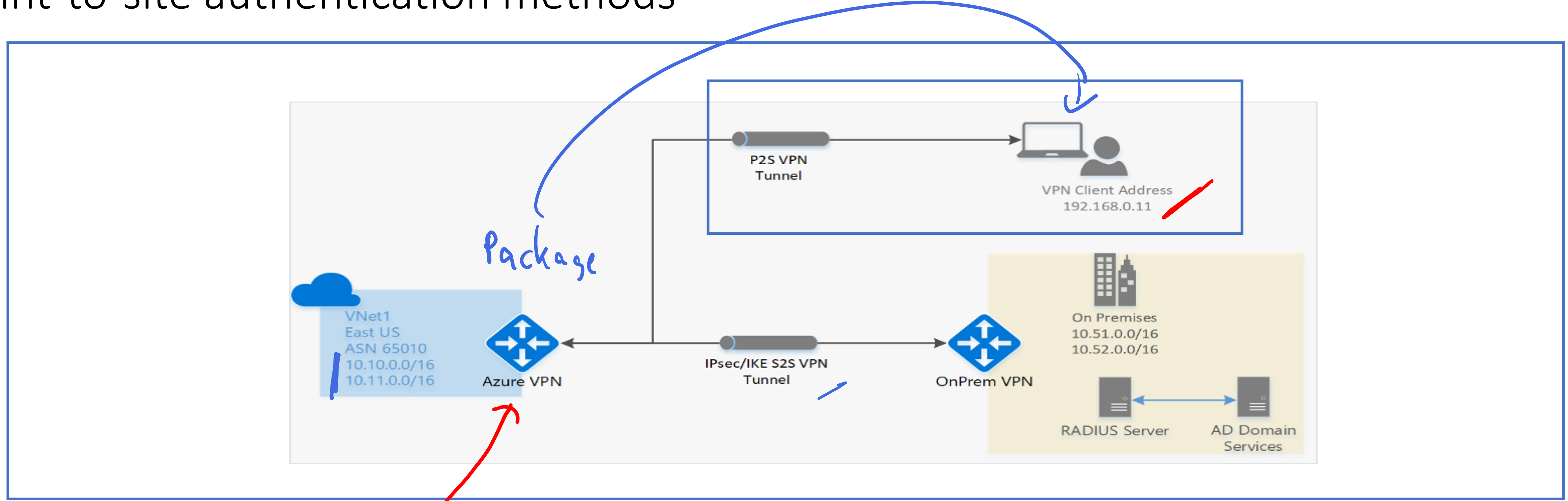
OpenVPN® Protocol

Secure Socket Tunneling Protocol (SSTP)

IKEv2 VPN



Point-to-site authentication methods



Azure certificate authentication

Self Signed

Native Azure Active Directory authentication

Active Directory (AD) Domain Server

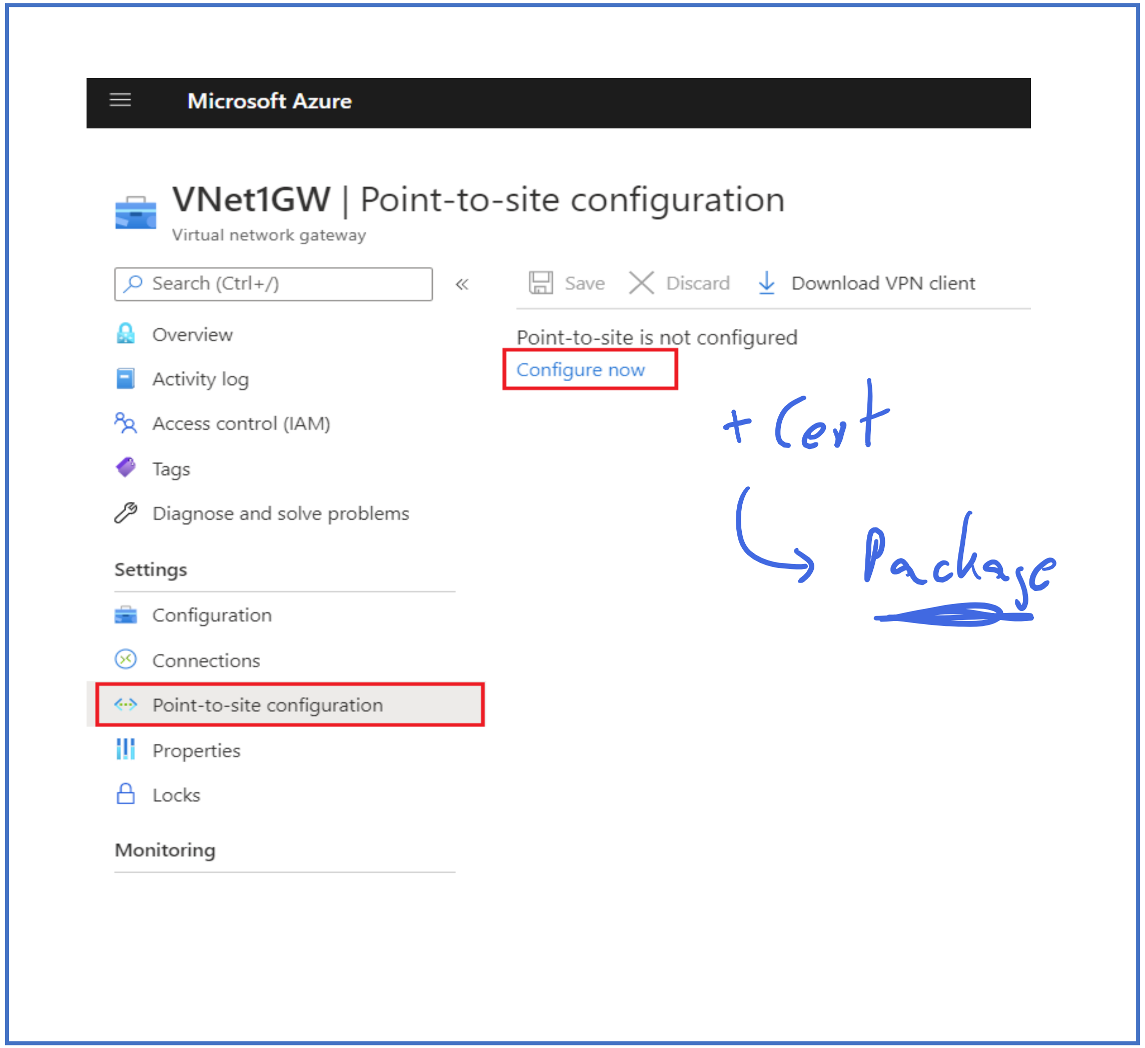
Prepare Point-to-site configuration in Azure

Navigate to the **Settings** section of the virtual network gateway page

Select **Point-to-site configuration**.
Select **Configure now** to open the configuration page

On the **Point-to-site configuration** page, in the **Address pool** box, add the private IP address range that you want to use

VPN clients dynamically receive an IP address from the range that you specify. The minimum subnet mask is 29 bit for active/passive and 28 bit for active/active configuration.



Point-to-site is not configured

+ Cert

Package

© Copyright Microsoft Corporation. All rights reserved.

Summary – Point-to-Site VPN Connections

Check your knowledge

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

Connect to a VNet using P2S VPN & certificate authentication: portal - Azure VPN Gateway | Microsoft Docs

Configure an Always-On VPN tunnel - Azure VPN Gateway | Microsoft Docs

Connect remote resources by using Azure Virtual WANs

Connect remote resources by using Azure Virtual WANs overview

- What is Azure Virtual WAN?
- Choose a Virtual WAN SKU
- Hub private address space
- Connect cross-tenant VNets to a virtual WAN hub
- Virtual Hub routing
- Demonstration
- Review

What is Azure Virtual WAN?

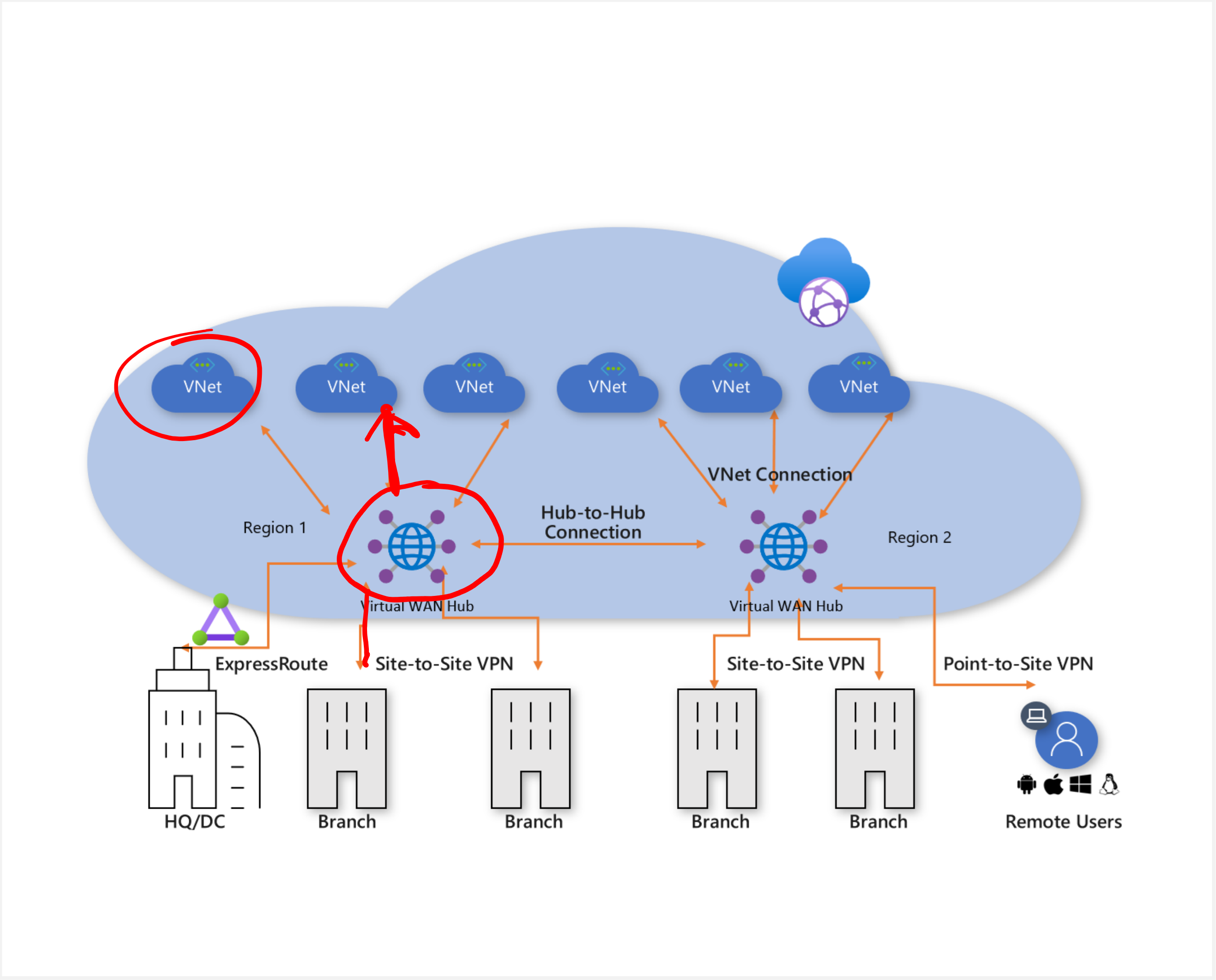
Brings together S2S, P2S, and ExpressRoute

Integrated connectivity using a hub-and-spoke connectivity model

Connect virtual networks and workloads to the Azure hub automatically

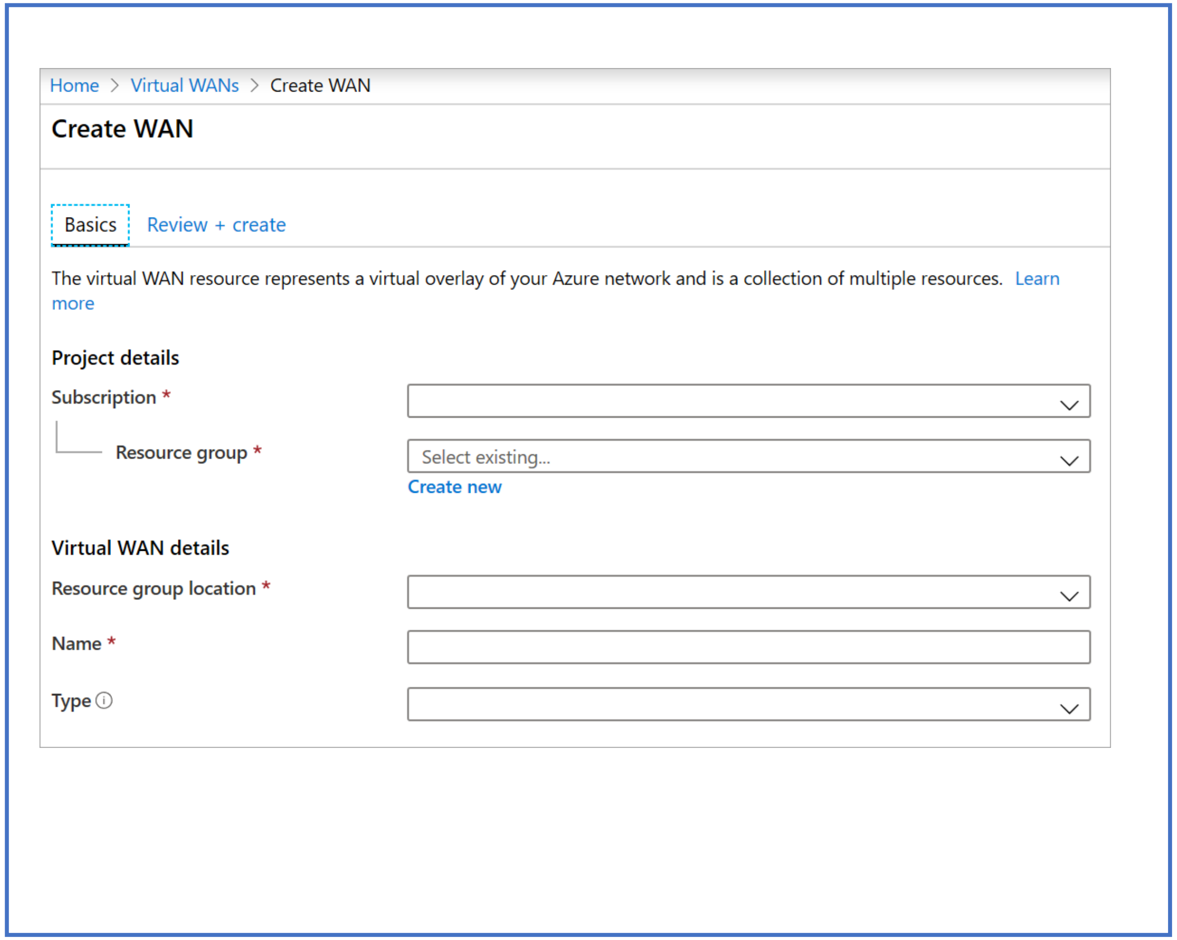
Visualize the end-to-end flow within Azure

Two types: Basic and Standard



Choose Virtual WAN SKU

Virtual WAN type	Hub type	Available configuration
Basic	Basic	Site-to-site VPN only
Standard	Standard	ExpressRoute User VPN (P2S) VPN (Site-to-site) Inter-hub and VNet-to-VNet transiting through the virtual hub



Home > Virtual WANs > Create WAN

Create WAN

The virtual WAN resource represents a virtual overlay of your Azure network and is a collection of multiple resources. Learn more

Project details

Subscription *

Resource group * Select existing...

Create new

Virtual WAN details

Resource group location *

Name *

Type ⓘ

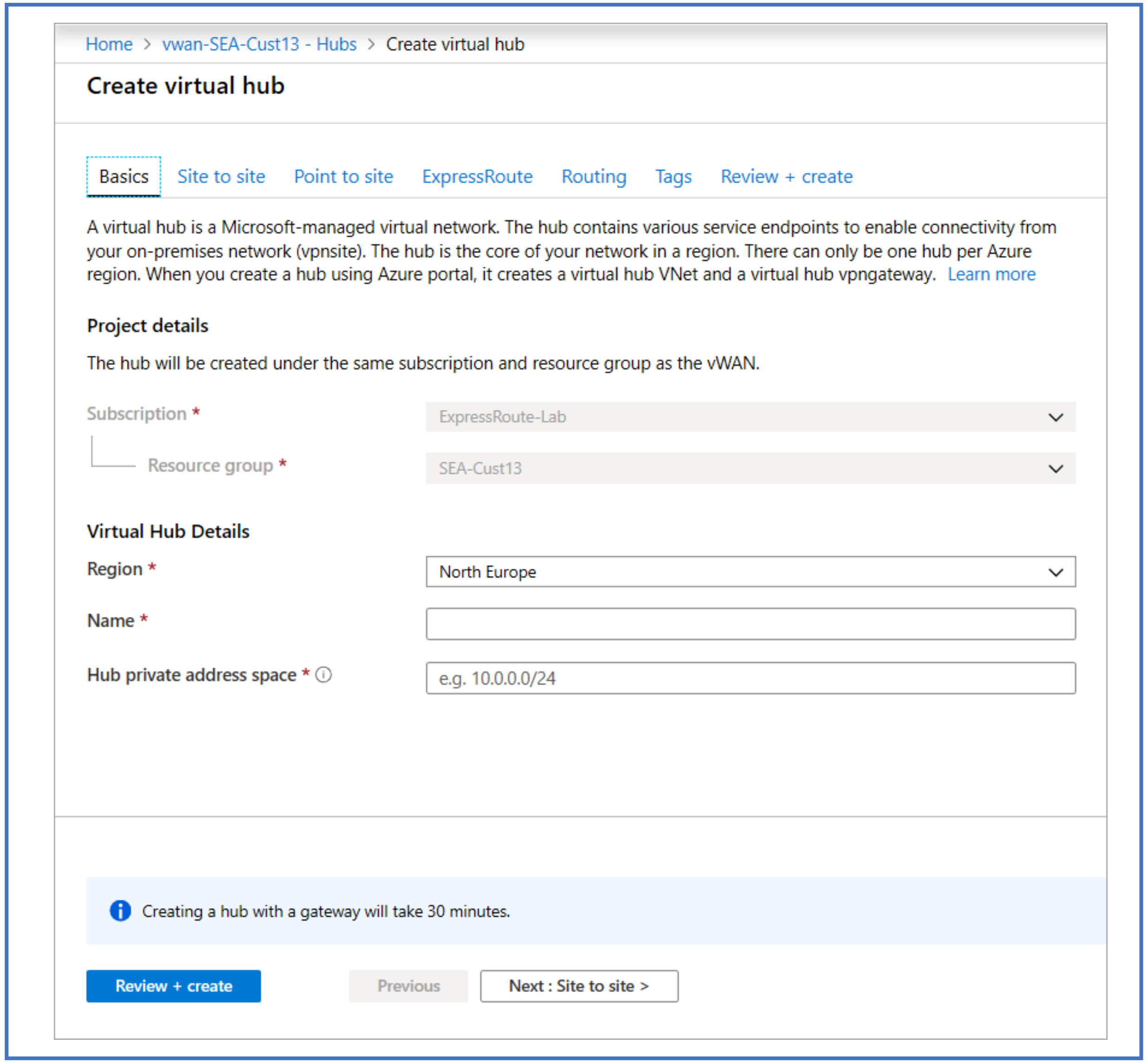
Hub private address space

Minimum address space is /24 to create a hub

No need to explicitly plan the subnet address space for the services in the virtual hub

Azure Virtual WAN is a managed service, it creates the appropriate subnets in the virtual hub for the different gateways/services

For example, VPN gateways, ExpressRoute gateways, User VPN Point-to-site gateways, Firewall, routing, etc.



Home > vwan-SEA-Cust13 - Hubs > Create virtual hub

Create virtual hub

A virtual hub is a Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity from your on-premises network (vpnsite). The hub is the core of your network in a region. There can only be one hub per Azure region. When you create a hub using Azure portal, it creates a virtual hub VNet and a virtual hub vpngateway. Learn more

Project details

The hub will be created under the same subscription and resource group as the vWAN.

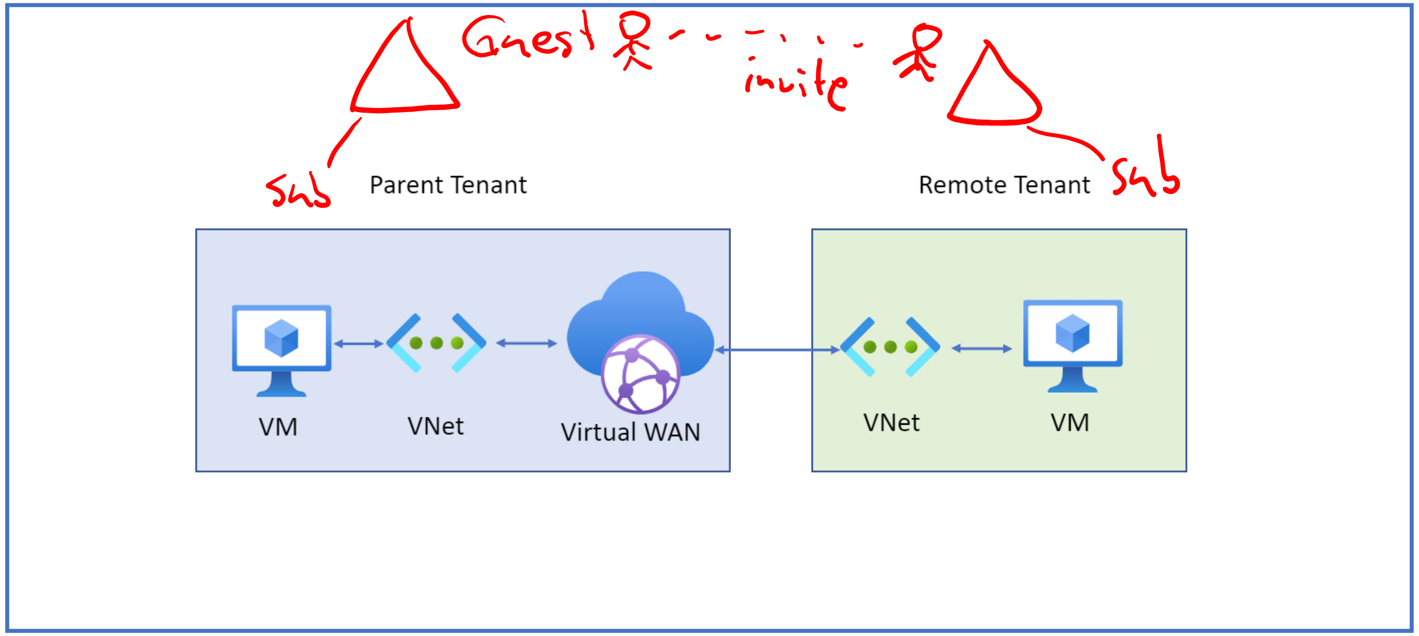
Subscription *	ExpressRoute-Lab
Resource group *	SEA-Cust13

Virtual Hub Details

Region *	North Europe
Name *	
Hub private address space * ⓘ	e.g. 10.0.0.0/24

Creating a hub with a gateway will take 30 minutes.

Connect cross-tenant VNets to a Virtual WAN hub



A Virtual WAN and virtual hub in the parent subscription

A virtual network configured in a subscription in the remote tenant

Non-overlapping address spaces in the remote tenant and address spaces within any other VNets already connected to the parent virtual hub

Virtual Hub Routing

Hub route table

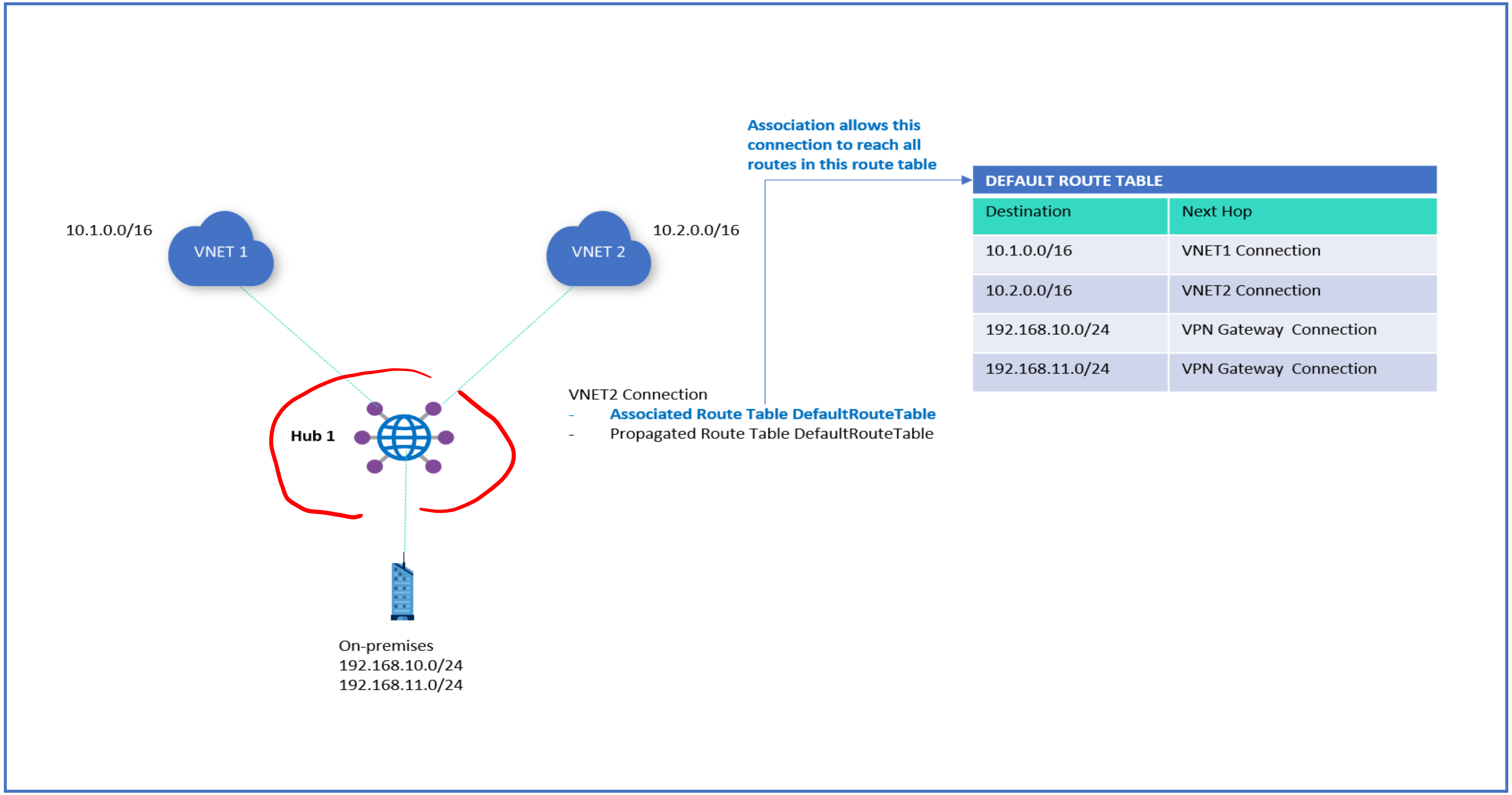
Connections

Association

Propagation

Labels

Static routes



Association allows this connection to reach all routes in this route table

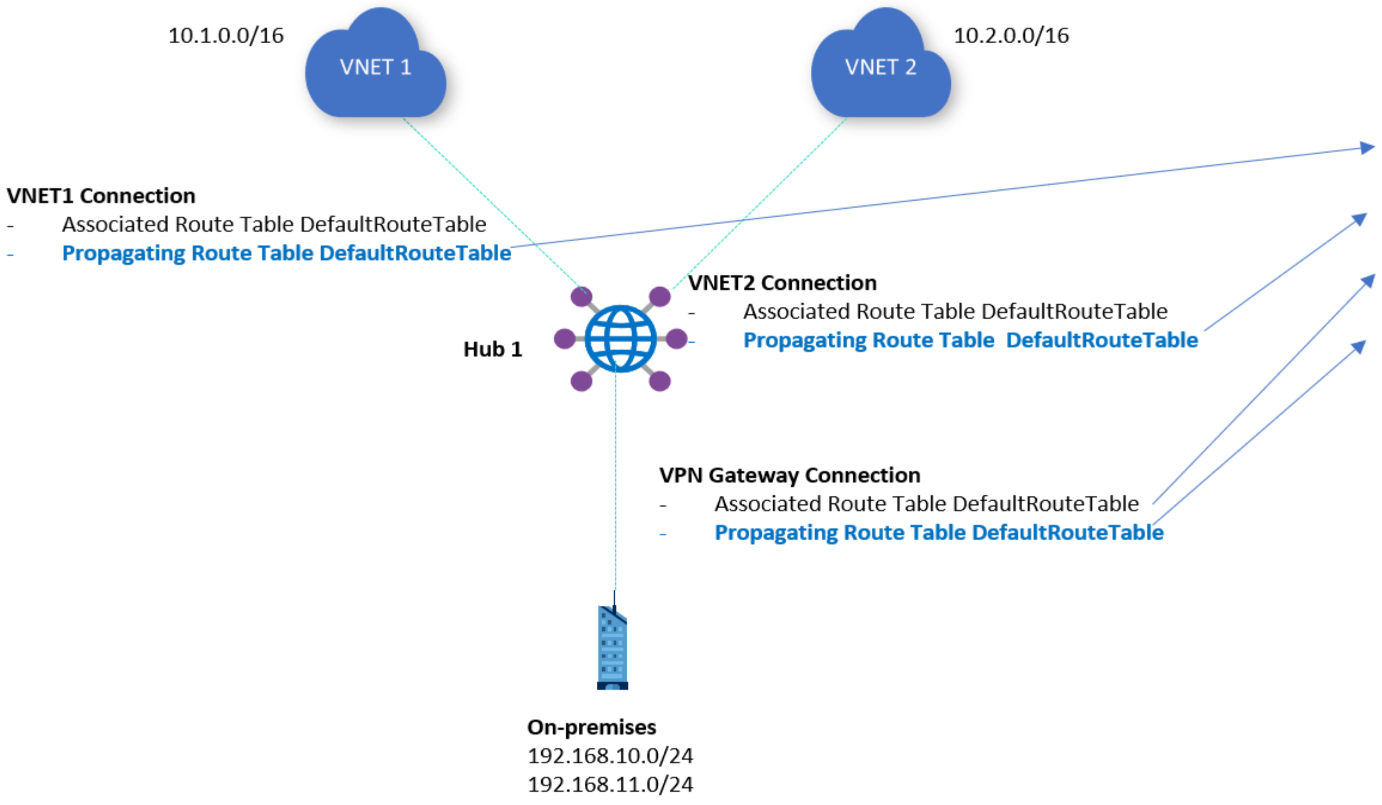
VNET2 Connection

- **Associated Route Table DefaultRouteTable**
- Propagated Route Table DefaultRouteTable

DEFAULT ROUTE TABLE

Destination	Next Hop
10.1.0.0/16	VNET1 Connection
10.2.0.0/16	VNET2 Connection
192.168.10.0/24	VPN Gateway Connection
192.168.11.0/24	VPN Gateway Connection

Virtual Hub Routing – continued



VNET1 Connection

- Associated Route Table DefaultRouteTable
- **Propagating Route Table DefaultRouteTable**

VNET2 Connection

- Associated Route Table DefaultRouteTable
- **Propagating Route Table DefaultRouteTable**

VPN Gateway Connection

- Associated Route Table DefaultRouteTable
- **Propagating Route Table DefaultRouteTable**

On-premises
192.168.10.0/24
192.168.11.0/24

DEFAULT ROUTE TABLE

Destination	Next Hop
10.1.0.0/16	VNET1 Connection
10.2.0.0/16	VNET2 Connection
192.168.10.0/24	VPN Gateway Connection
192.168.11.0/24	VPN Gateway Connection

Demonstration – route to shared services using an ARM template

Review and deploy the ARM template

Complete the hybrid configuration

Connect remote resources by using Azure Virtual WANs Review

Knowledge Check Questions

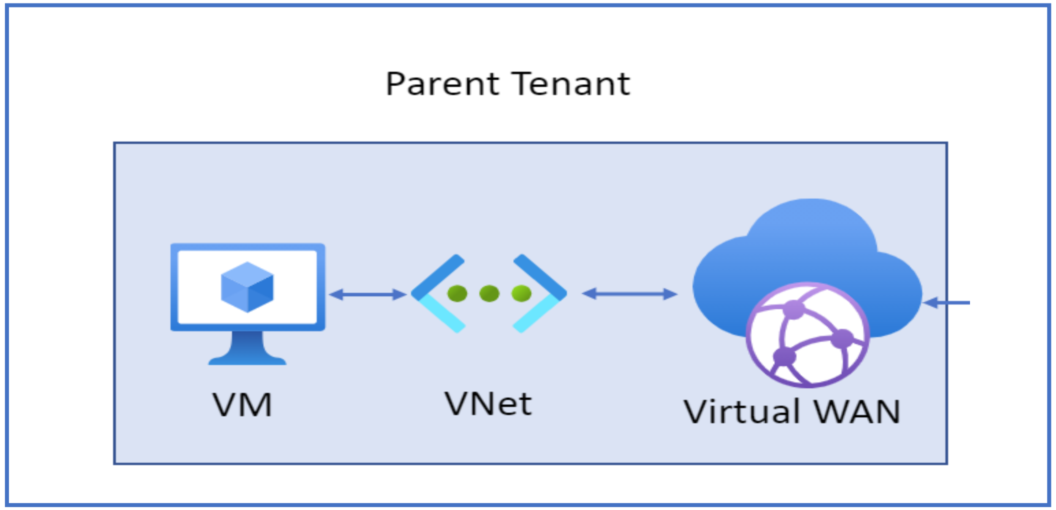
Microsoft Learn Modules (docs.microsoft.com/Learn)

[Virtual WAN documentation | Microsoft Docs](#)

[Azure Virtual WAN Overview | Microsoft Docs](#)

Exercise: create a virtual WAN by using the Azure portal

Exercise – Create a Virtual WAN by using Azure Portal



Objectives

Task 1:

Create a Virtual WAN

Task 2:

Create a hub

Task 3:

Connect a VNet to the Virtual Hub

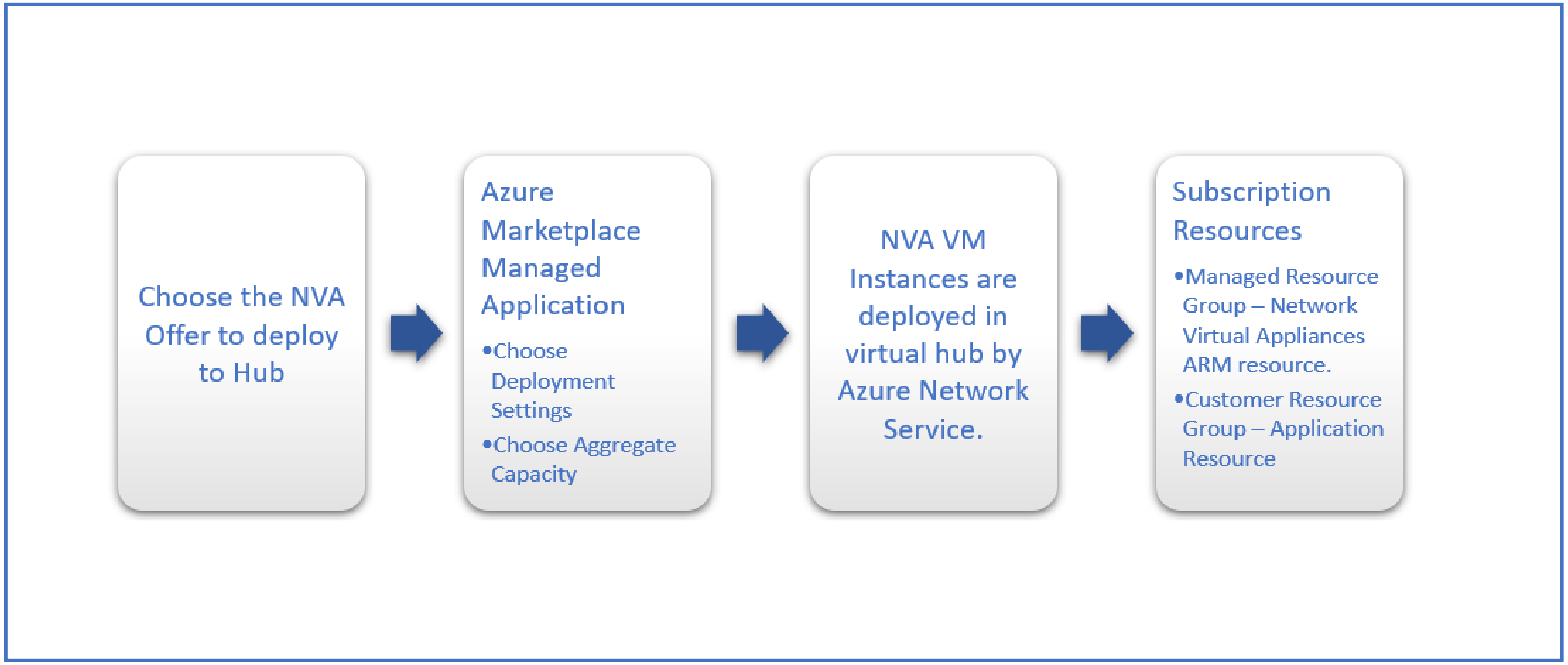
Create a network virtual appliance (NVA) in a virtual hub

UDR

Create a network virtual appliance (NVA) in a virtual hub overview

- Manage an NVA in a Virtual Hub
- Deploy an NVA in your Virtual Hub
- Review

Manage an NVA in a Virtual Hub



Choose the NVA Offer to deploy to Hub

Azure Marketplace Managed Application

- Choose Deployment Settings
- Choose Aggregate Capacity

NVA VM Instances are deployed in virtual hub by Azure Network Service.

Subscription Resources

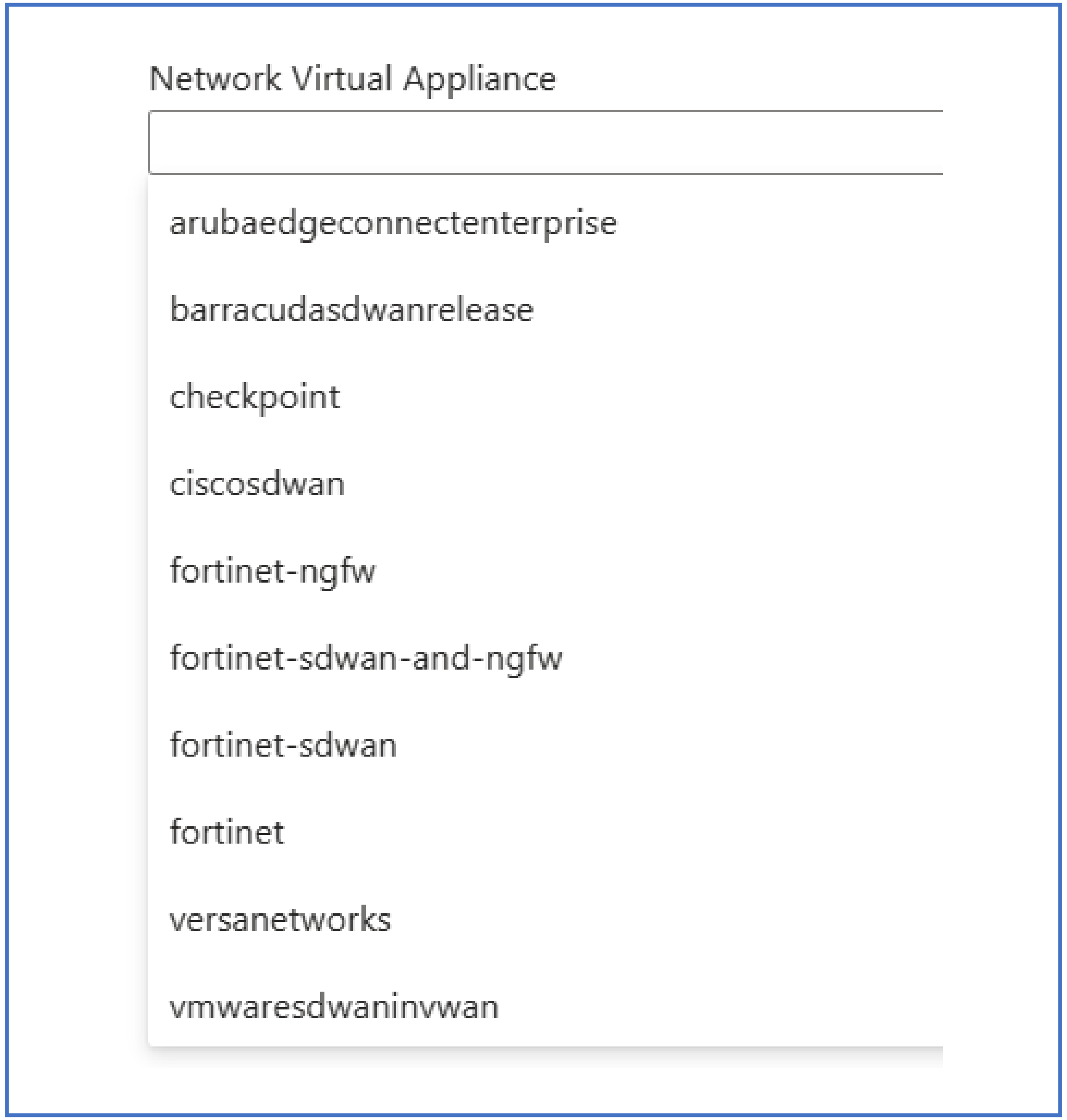
- Managed Resource Group – Network Virtual Appliances ARM resource.
- Customer Resource Group – Application Resource

Deploy an NVA in your Virtual Hub

Locate the Virtual WAN hub you created in the previous step and open it

Find the Network Virtual Appliances tile and select the Create link.

On the **Network Virtual Appliance** blade, select your preferred provider based on available selections, then select the **Create** button



Network Virtual Appliance

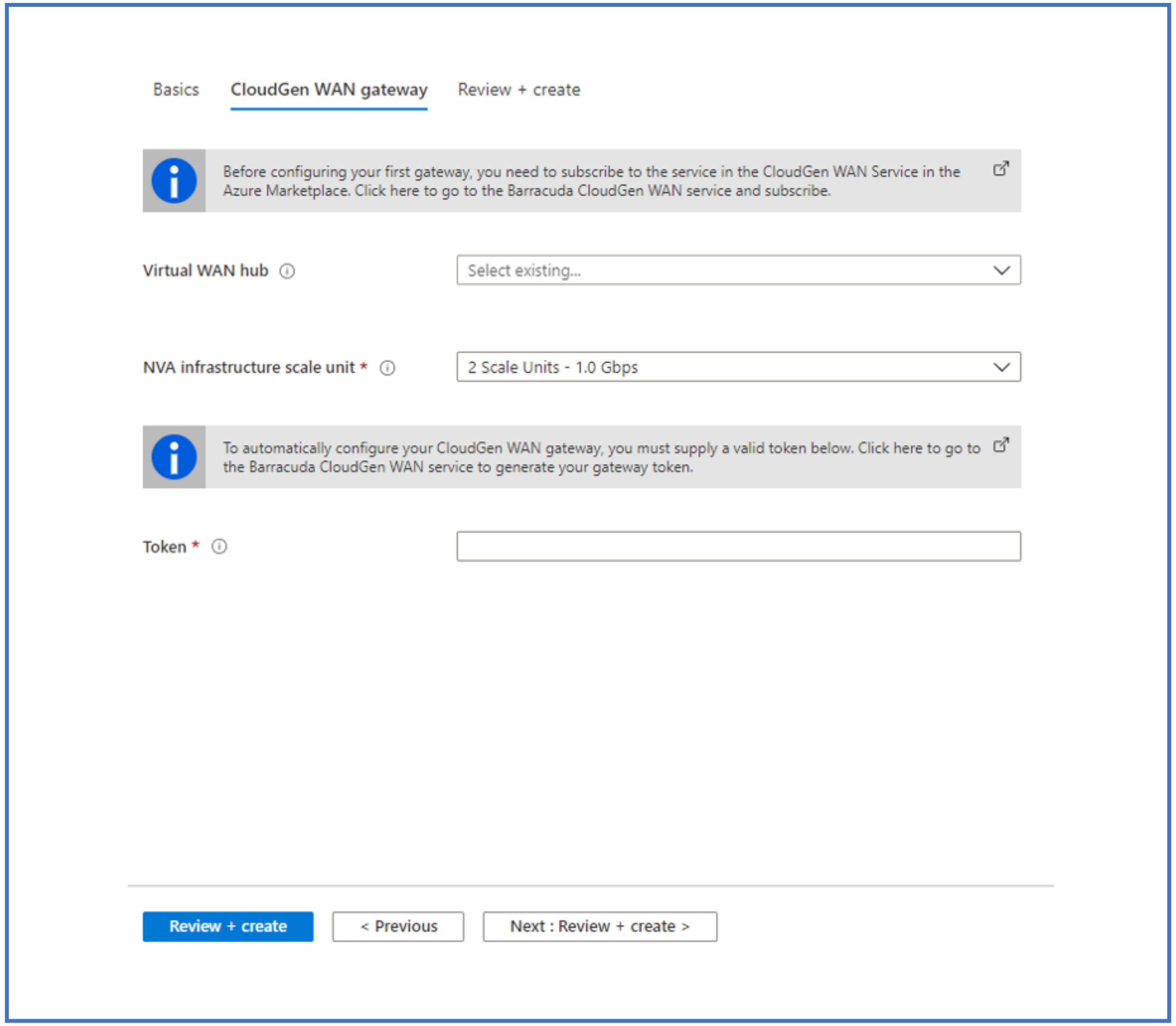
- arubaedgeconnectenterprise
- barracudasdwanrelease
- checkpoint
- ciscosdwan
- fortinet-ngfw
- fortinet-sdwan-and-ngfw
- fortinet-sdwan
- fortinet
- versanetworks
- vmwaresdwaninvwan

Deploy an NVA in your Virtual Hub Cont.

Virtual WAN Hub - The Virtual WAN hub you want to deploy this NVA into

NVA Infrastructure Units - Indicate the number of NVA Infrastructure Units you want to deploy this NVA with. Choose the amount of aggregate bandwidth capacity you want to provide across all the branch sites that will be connecting to this hub through this NVA.

Token - Barracuda requires that you provide an authentication token here in order to identify yourself as a registered user of this product. You'll need to obtain this from Barracuda.



Before configuring your first gateway, you need to subscribe to the service in the CloudGen WAN Service in the Azure Marketplace. Click here to go to the Barracuda CloudGen WAN service and subscribe.

Virtual WAN hub: Select existing...

NVA infrastructure scale unit *: 2 Scale Units - 1.0 Gbps

To automatically configure your CloudGen WAN gateway, you must supply a valid token below. Click here to go to the Barracuda CloudGen WAN service to generate your gateway token.

Token *:

Create a network virtual appliance (NVA) in a virtual hub - Review

Knowledge Check Questions

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

Azure Virtual WAN: About Network Virtual Appliance in the hub | Microsoft Docs

What is a secured virtual hub? | Microsoft Docs

End of presentation