



AZ-700

Module 02

Design and Implement  
Hybrid Networking



# AZ-700 Agenda

Module 01: Introduction to Azure Virtual Networks

Module 02: Designing and Implementing Hybrid Networking 

Module 03: Designing and Implementing Azure ExpressRoute

Module 04: Load balance non-HTTP(S) traffic in Azure

Module 05: Load balance HTTP(S) traffic in Azure 

Module 06: Design and Implement Network Security

Module 07: Design and Implement private access to Azure Services

Module 08: Design and Implement Network Monitoring

# Module Overview

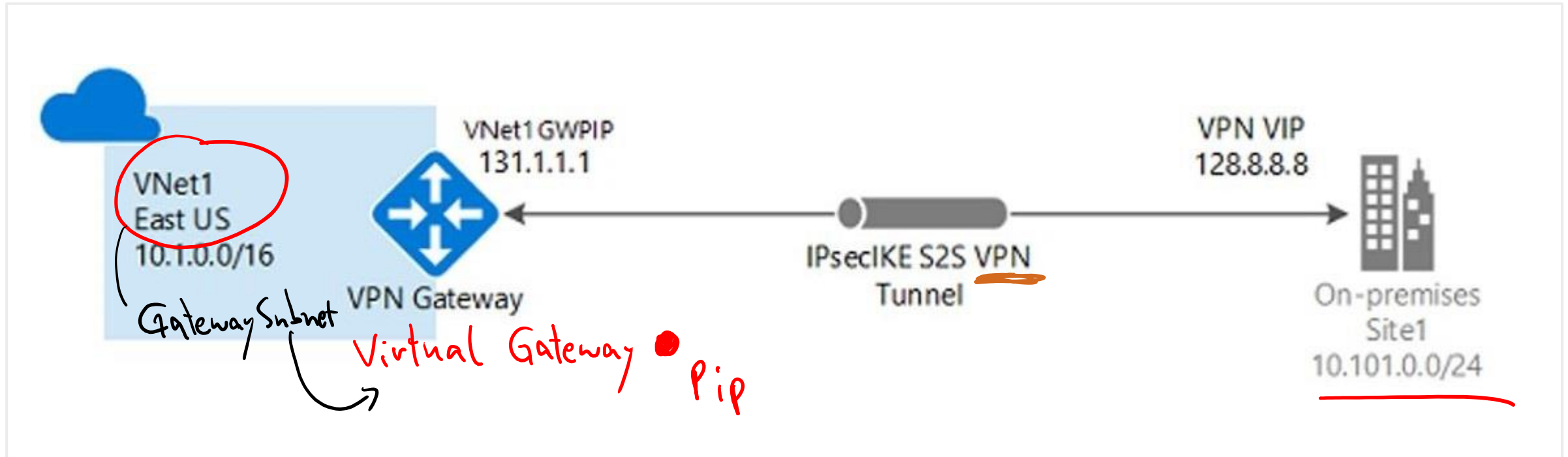
- Design and implement Azure VPN Gateway
- Exercise – Create and configure a Virtual Network Gateway
- Connect networks with Site-to-site VPN connections
- Connect devices to networks with Point-to-site VPN connections
- Connect remote resources by using Azure Virtual WANs
- Exercise – Create a Virtual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

# Design and implement Azure VPN gateway



→ Express Route

## 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  
*verschlüsselt*

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

Peering: unverschlüsselt

# 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

The screenshot shows the Azure portal interface for creating a new subnet. At the top, the page title is 'vnet01 - Subnets'. Below the title bar, there are three buttons: '+ Subnet', '+ Gateway subnet' (highlighted with a red box), and 'Refresh'. A red arrow points from the '+ Gateway subnet' button to the 'Name' field in the 'Add subnet' dialog. The 'Name' field contains 'GatewaySubnet' and is also highlighted with a red box. The 'Subnet address range' field is set to '10.0.0.32/28'. Below this, there is a checkbox for 'Add IPv6 address space' which is unchecked. The 'NAT gateway' is set to 'None'. The 'Network security group' is set to 'None'. The 'Route table' is set to 'None'. The 'SERVICE ENDPOINTS' section is expanded, showing 'Services' set to '0 selected'. The 'SUBNET DELEGATION' section is also expanded, showing 'Delegate subnet to a service' set to 'None'. The 'NETWORK POLICY FOR PRIVATE ENDPOINTS' section is expanded, showing a description of the policy. At the bottom of the dialog, there are 'Save' and 'Cancel' buttons.

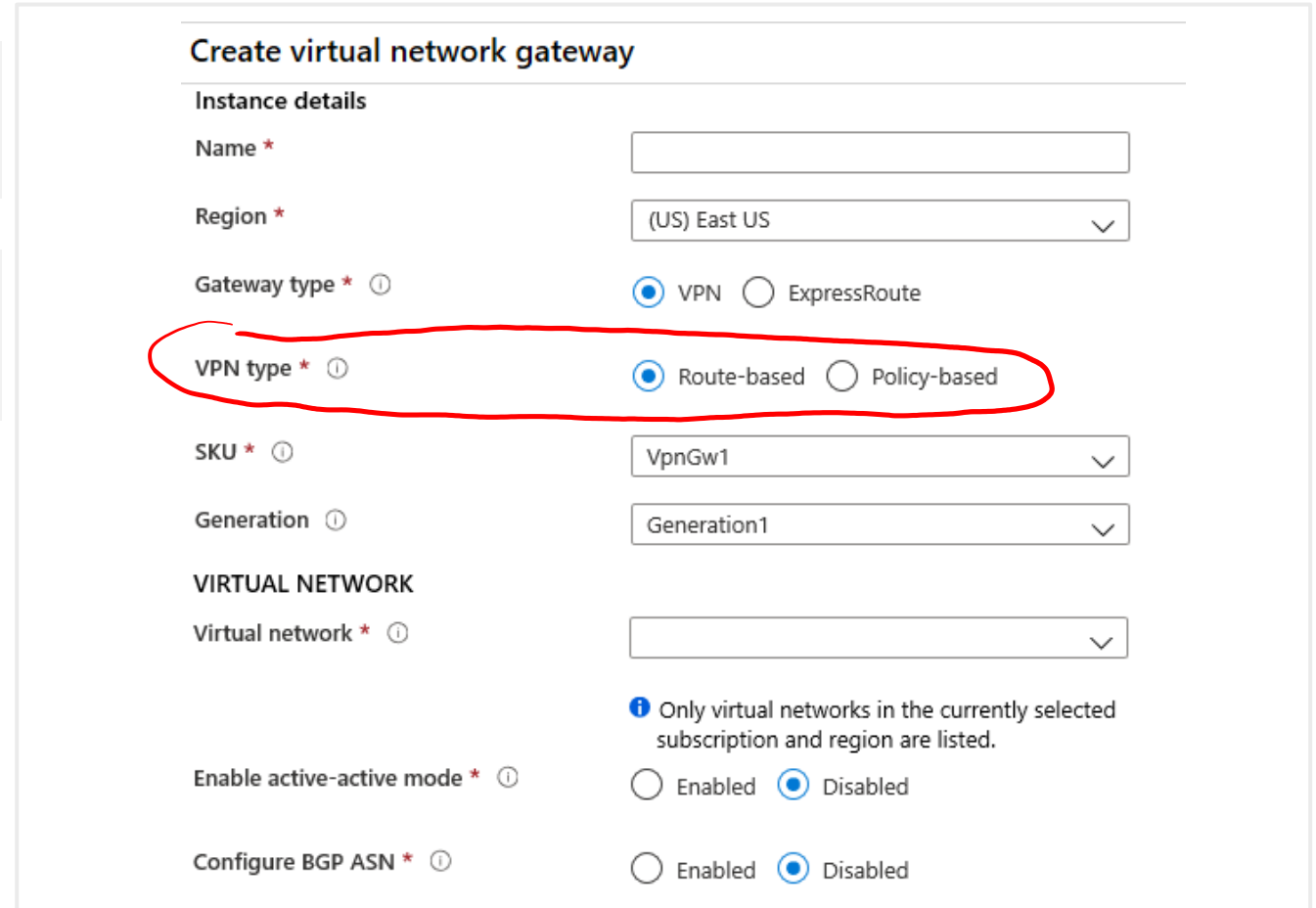
# VPN Gateway Configuration requirements

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 \*

Gateway type \* ☒ VPN ☐ ExpressRoute

**VPN type \* ☒ Route-based ☐ Policy-based**

SKU \*

Generation

**VIRTUAL NETWORK**

Virtual network \*

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

Enable active-active mode \* ☐ Enabled ☒ Disabled

Configure BGP ASN \* ☐ Enabled ☒ Disabled

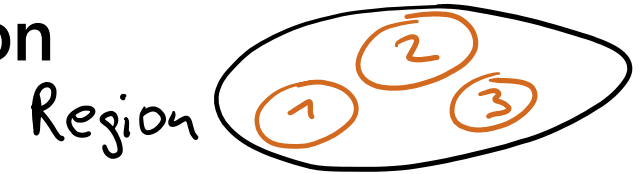


It can take up to 45 minutes to provision the VPN gateway

30

# Choose the appropriate Gateway SKU and Generation

Az Avail Zone = DC



## Sampling of available SKUs

SKU \* ⓘ

Generation ⓘ

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



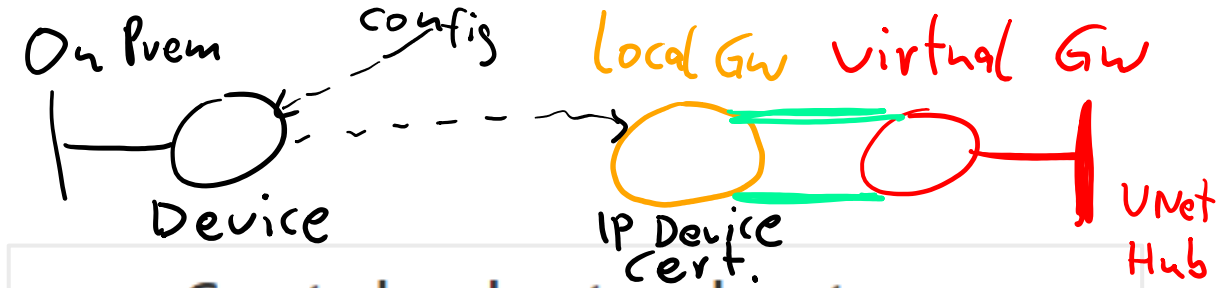
# Create the Local Network Gateway

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

Connection

Name \*

VNet1LocalNet

Endpoint ⓘ

IP address

FQDN

IP address \* ⓘ

33.2.1.5

Address space ⓘ

192.168.3.0/24

Transfer net

Add additional address range

☐ Configure BGP settings

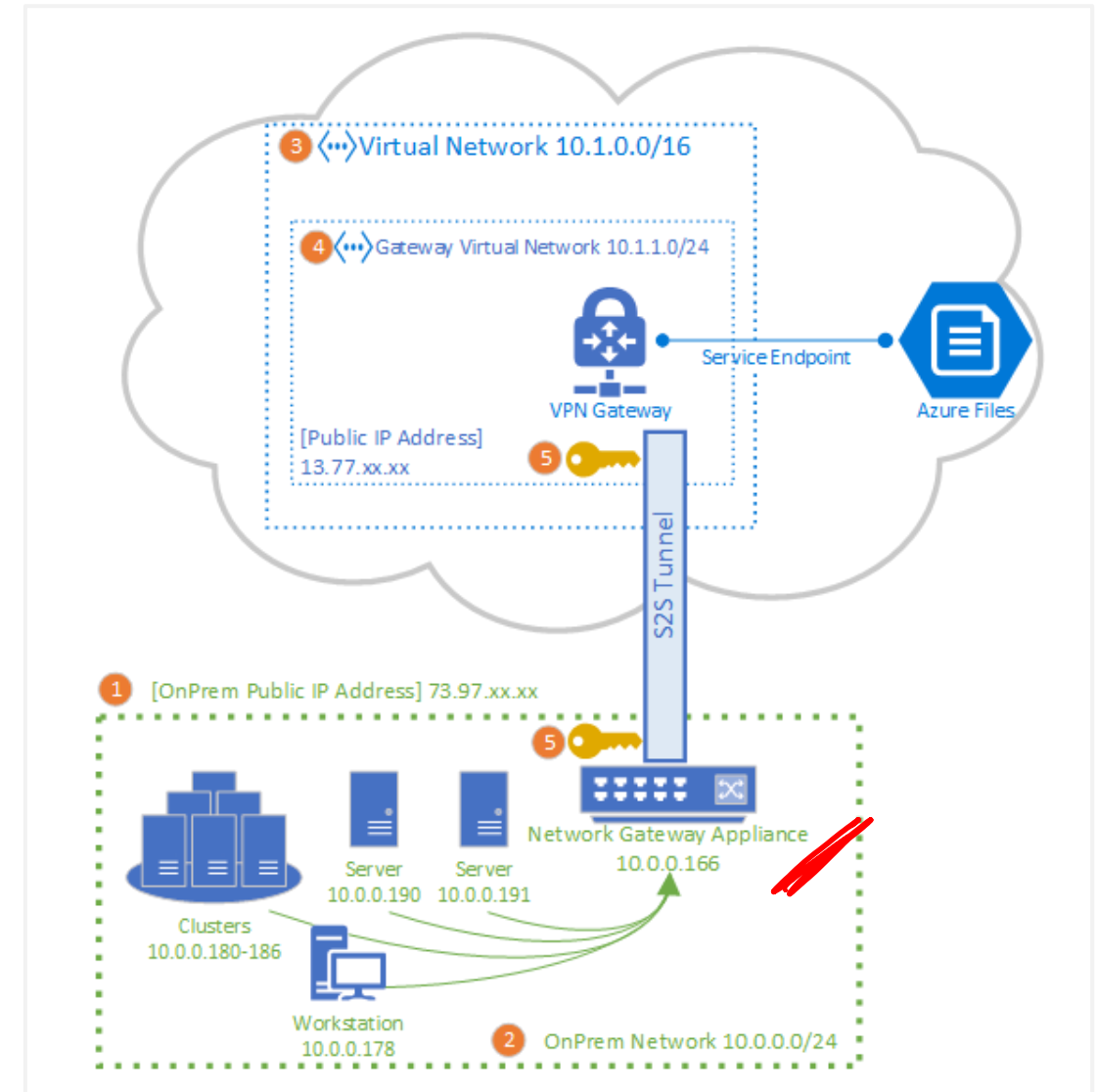
# Configure the On-premises VPN Device

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 gateway 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...** □ ×

+ Create new

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

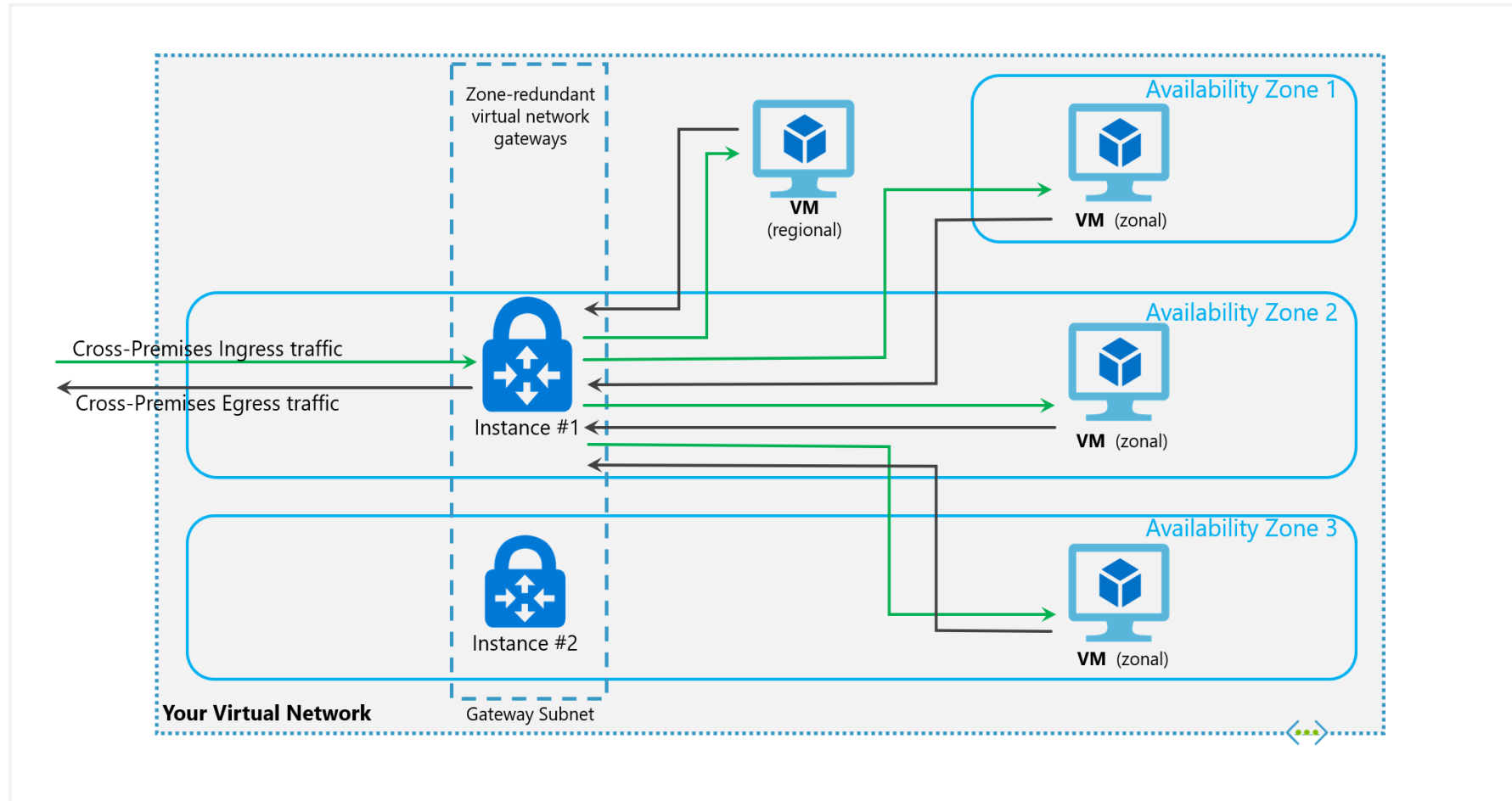
Check whether the on-premises VPN device is validated

Verify the Azure gateway health probe

Verify the shared key and the VPN peer IPs

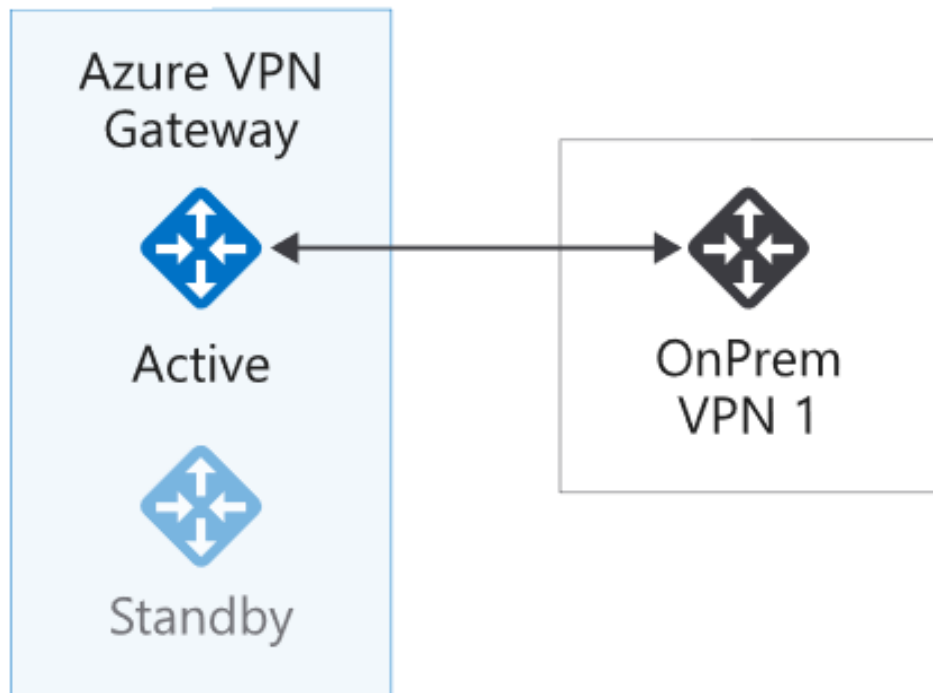
Check whether the on-premises VPN device has the perfect forward secrecy feature enabled

# Create a zone redundant VNET gateway in Azure Availability zones

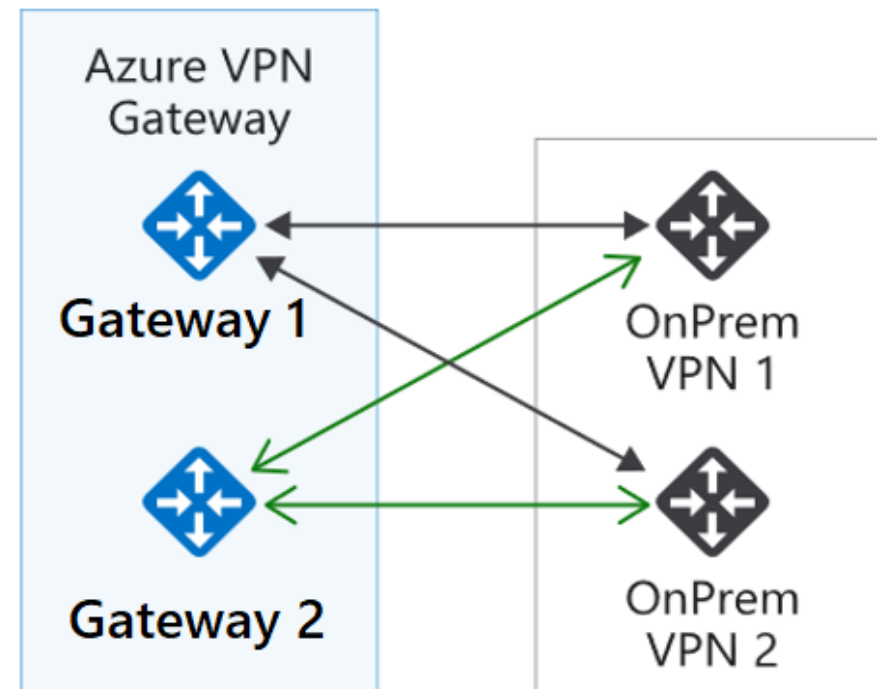


# High availability options for VPN connections

Active/standby (default)



Active/active



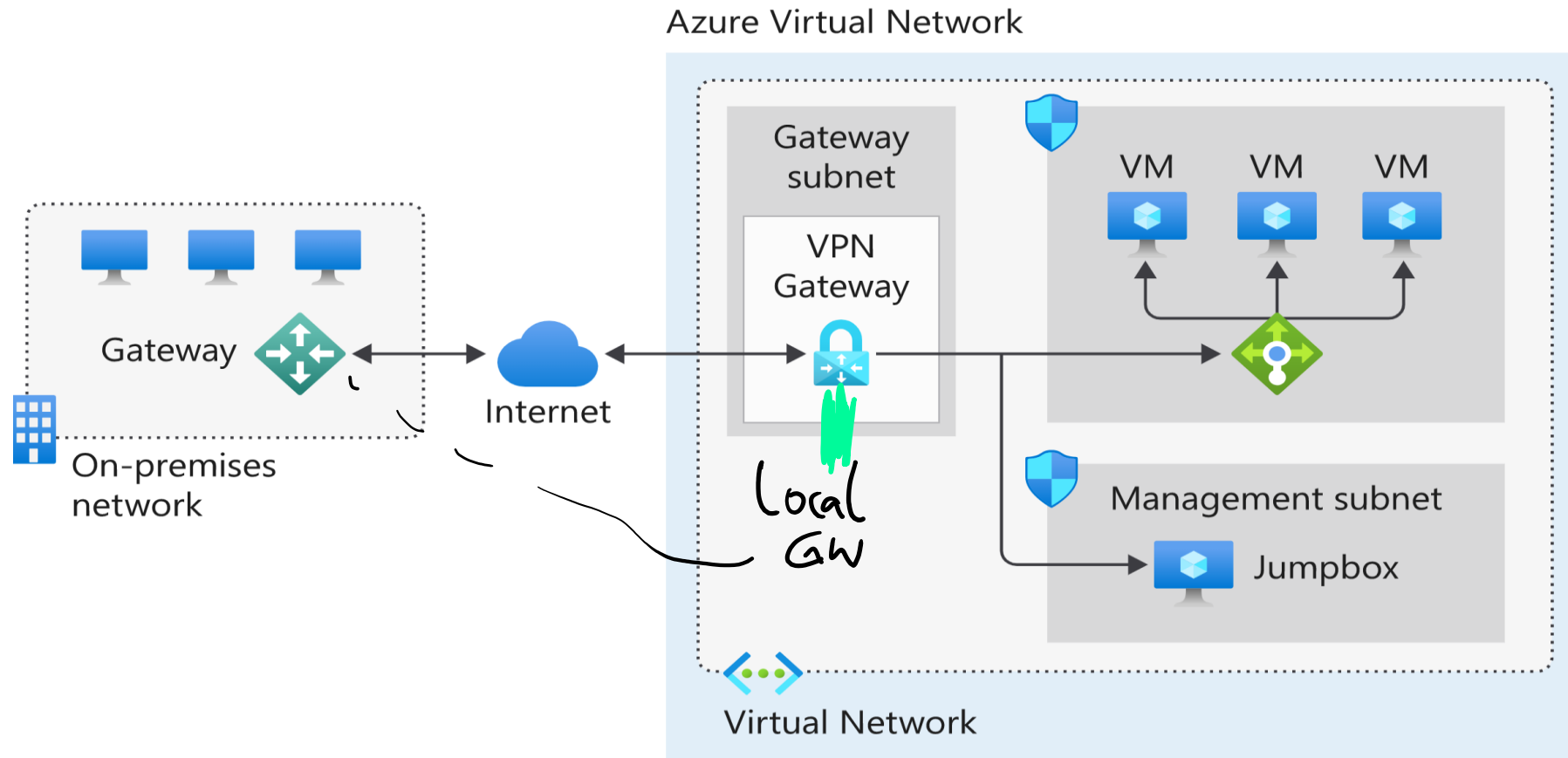
VPN gateways are deployed  
as two instances

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

# Connect Networks with Site-to-site VPN Connections



# Site-to-site VPN connections





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

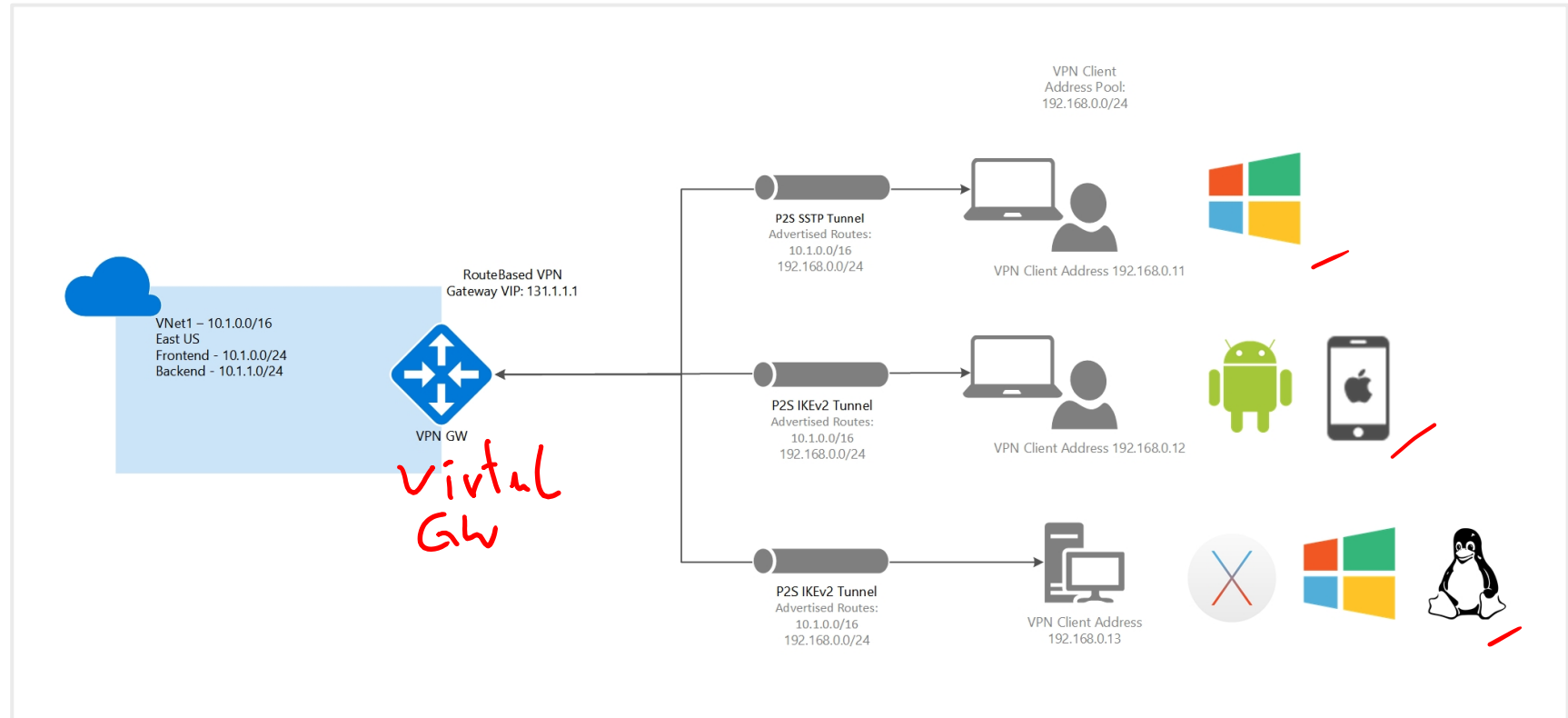


# Point-to-site protocols

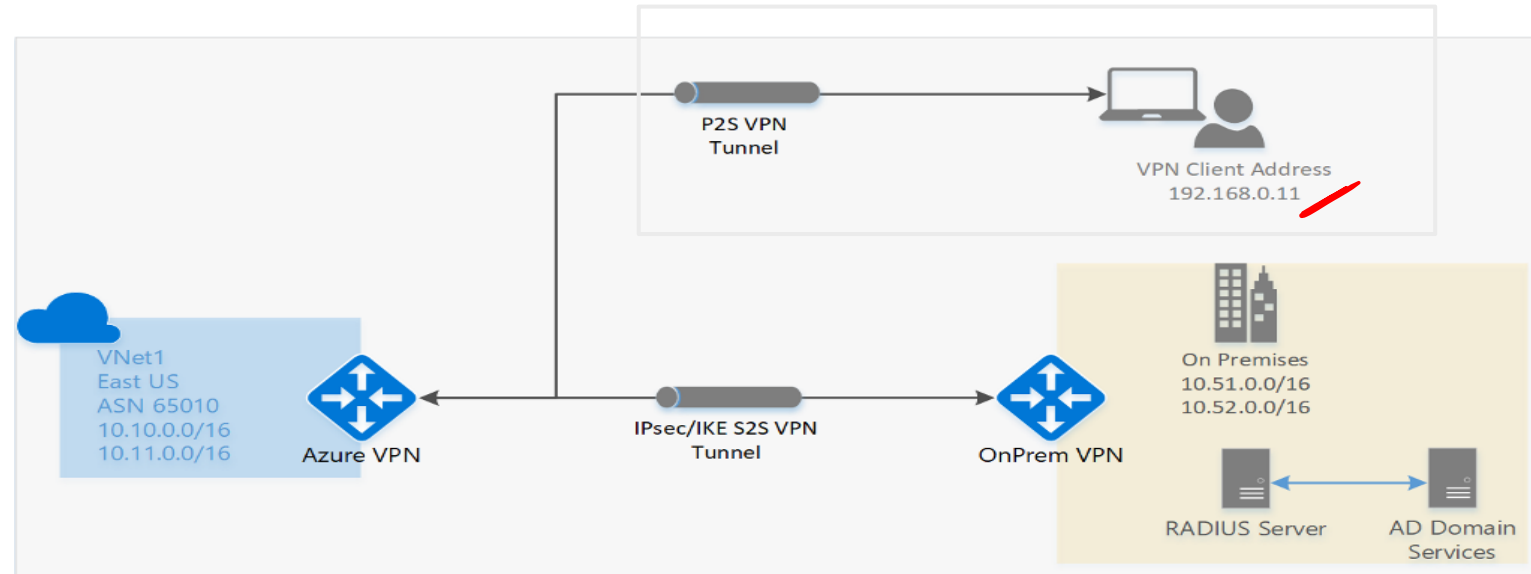
OpenVPN® Protocol

Secure Socket Tunneling Protocol (SSTP)

IKEv2 VPN



# Point-to-site authentication methods



Azure certificate authentication

Native Azure Active Directory authentication

Active Directory (AD) Domain Server

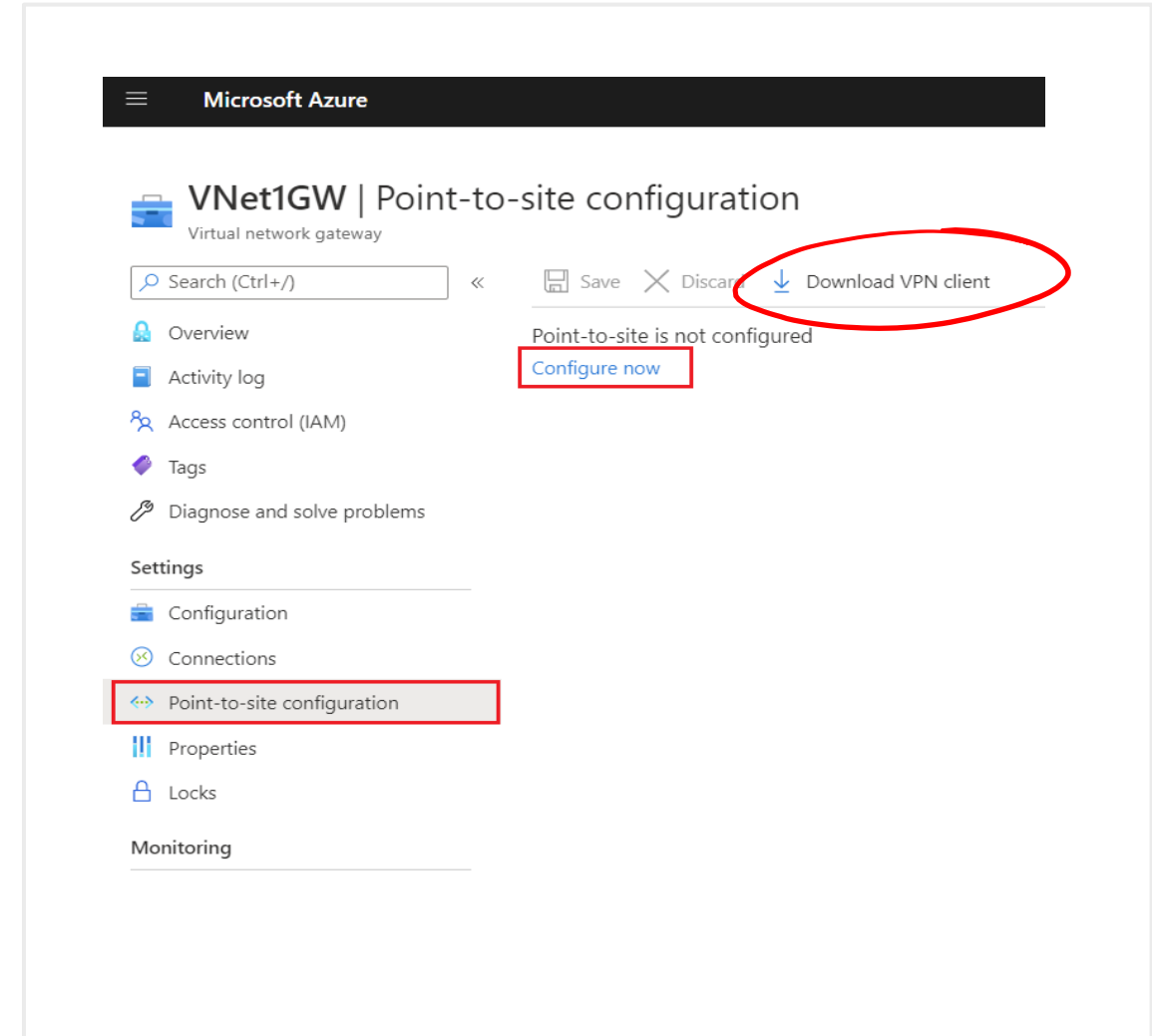
# Prepare Point-to-site configuration in Azure

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.



# Connect remote resources by using Azure Virtual WANs

+ Firewall Policy Manager



# What is Azure Virtual WAN?

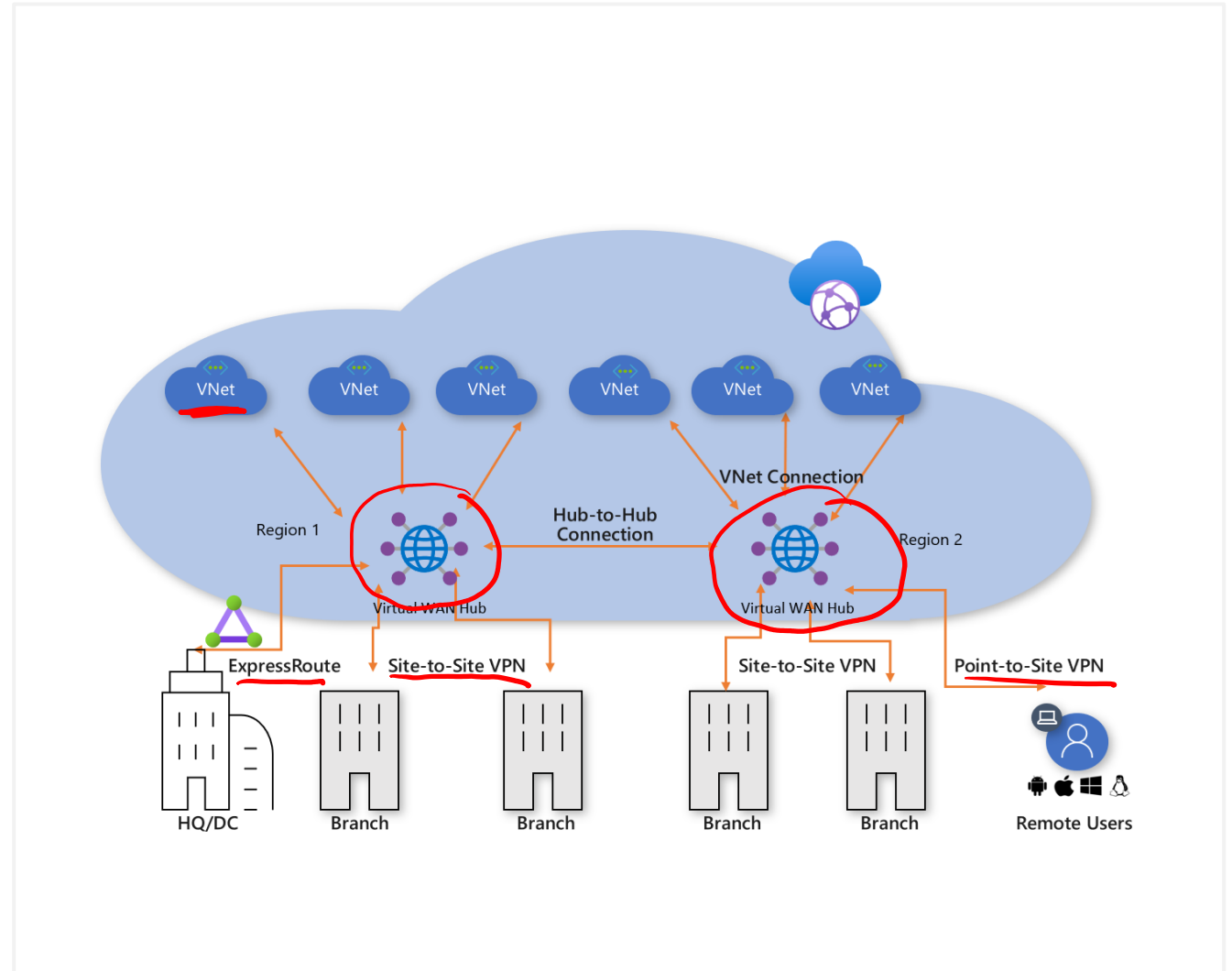
Brings together S2S, P2S, and ExpressRoute

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

Basics

[Review + create](#)

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 ⓘ

© Copyright Microsoft Corporation. All rights reserved.

# 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

Basics Site to site Point to site ExpressRoute Routing Tags Review + create

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 \*

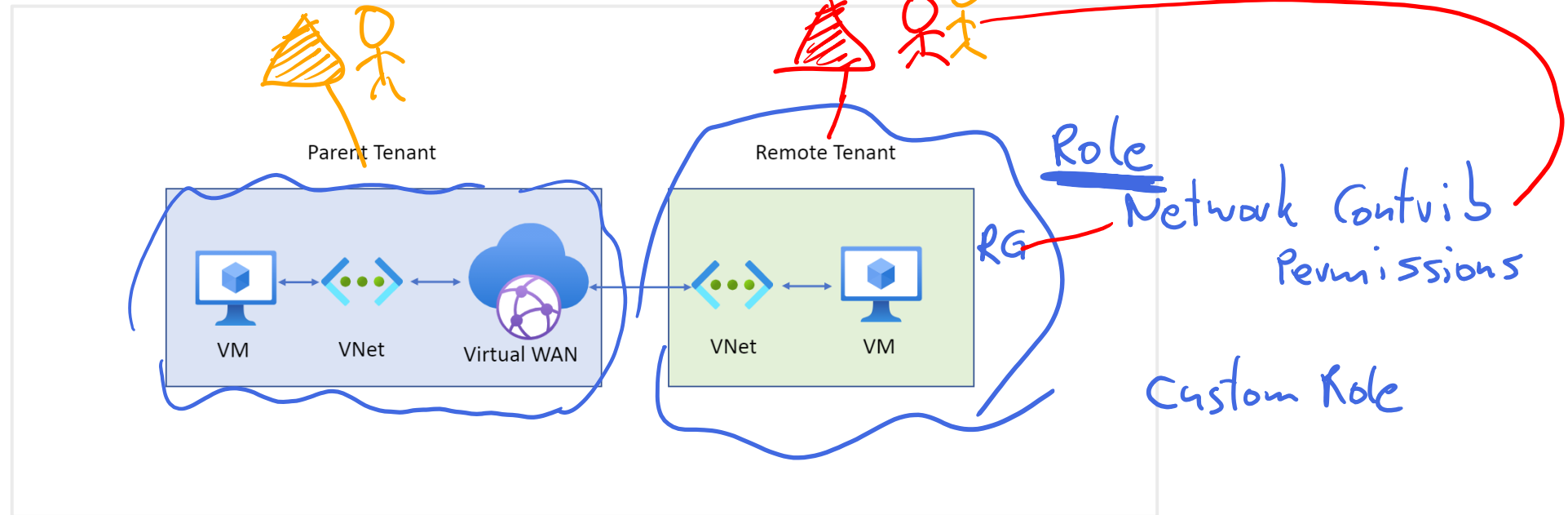
Hub private address space \* ⓘ e.g. 10.0.0.0/24

Creating a hub with a gateway will take 30 minutes.

Review + create Previous Next : Site to site >



# 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

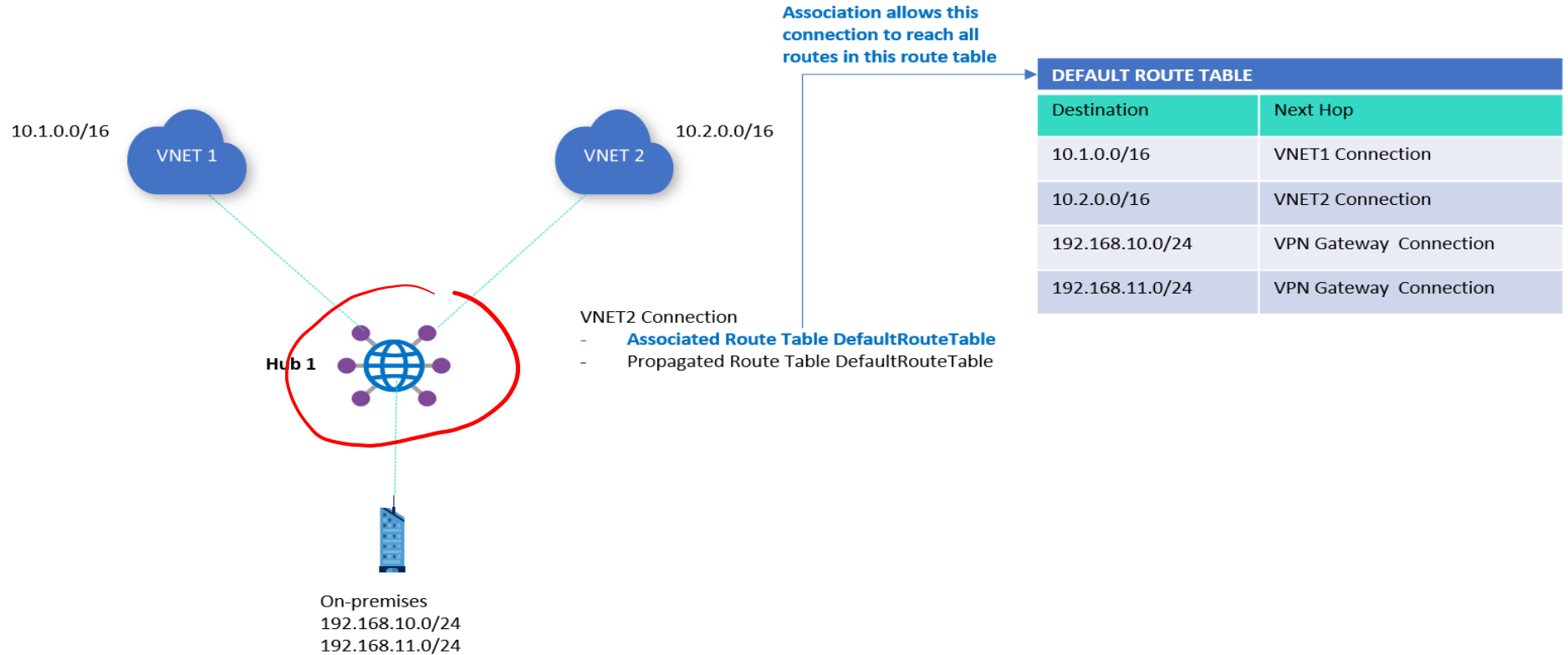
Connections

Association

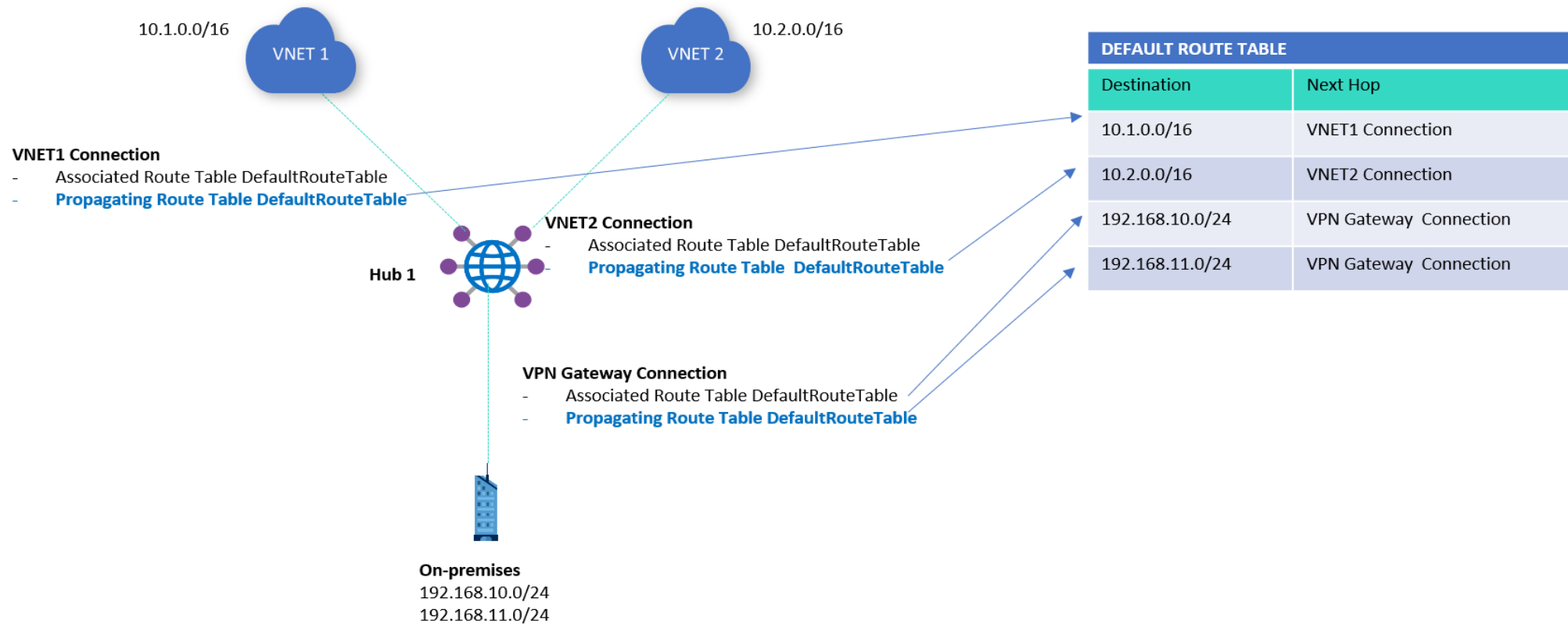
Propagation

Labels

Static routes



# Virtual Hub Routing – continued



UDR

User defined routing

Route Table  
Route

NVA

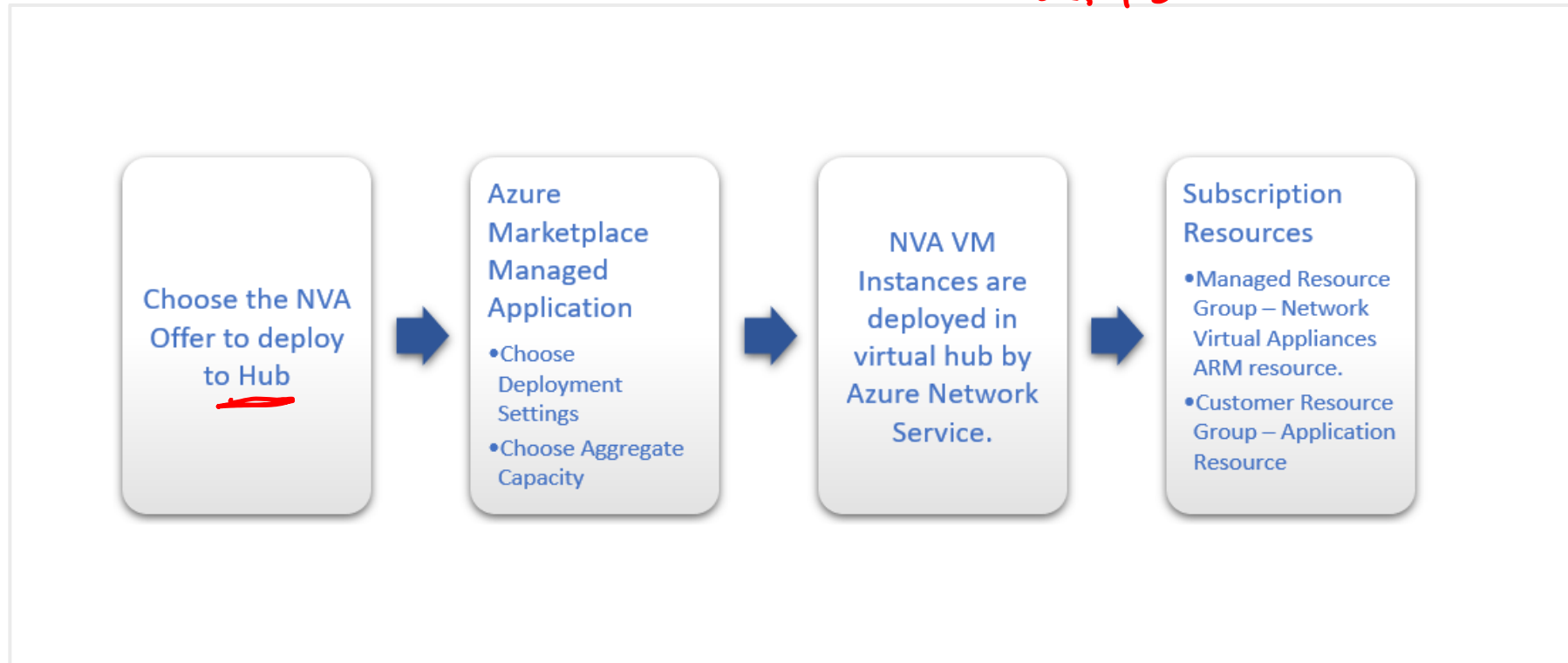
Next Hop

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

# Manage an NVA in a Virtual Hub

IaaS  
PaaS  
SaaS

CaaS



# 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

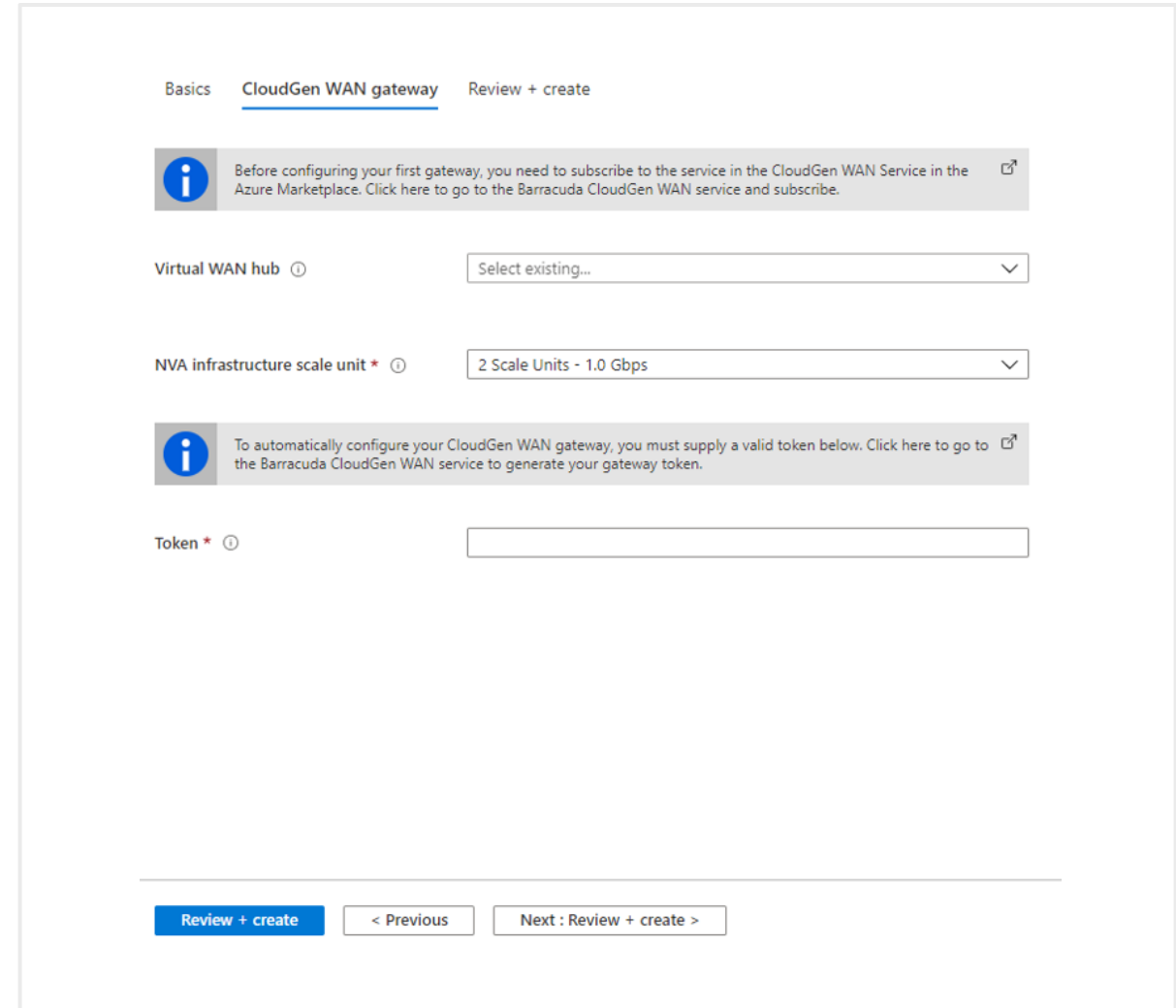
arubaedgeconnectenterprise  
barracudasdwanrelease  
checkpoint  
ciscosdwan  
fortinet-ngfw  
fortinet-sdwan-and-ngfw  
fortinet-sdwan  
fortinet  
versanetworks  
vmwaresdwaninvwan

# 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.



The screenshot shows the 'CloudGen WAN gateway' configuration page in the Azure portal. The page has three tabs: 'Basics', 'CloudGen WAN gateway' (which is selected), and 'Review + create'. Below the tabs, there are two informational messages: one about subscribing to the service in the Azure Marketplace, and another about providing a valid token for automatic configuration. The configuration fields include 'Virtual WAN hub' (a dropdown menu with 'Select existing...' as the current selection), 'NVA infrastructure scale unit' (a dropdown menu with '2 Scale Units - 1.0 Gbps' as the current selection), and 'Token' (a text input field). At the bottom, there are three buttons: 'Review + create' (highlighted in blue), '< Previous', and 'Next : Review + create >'.

# Lab – Create and configure a Virtual Network Gateway

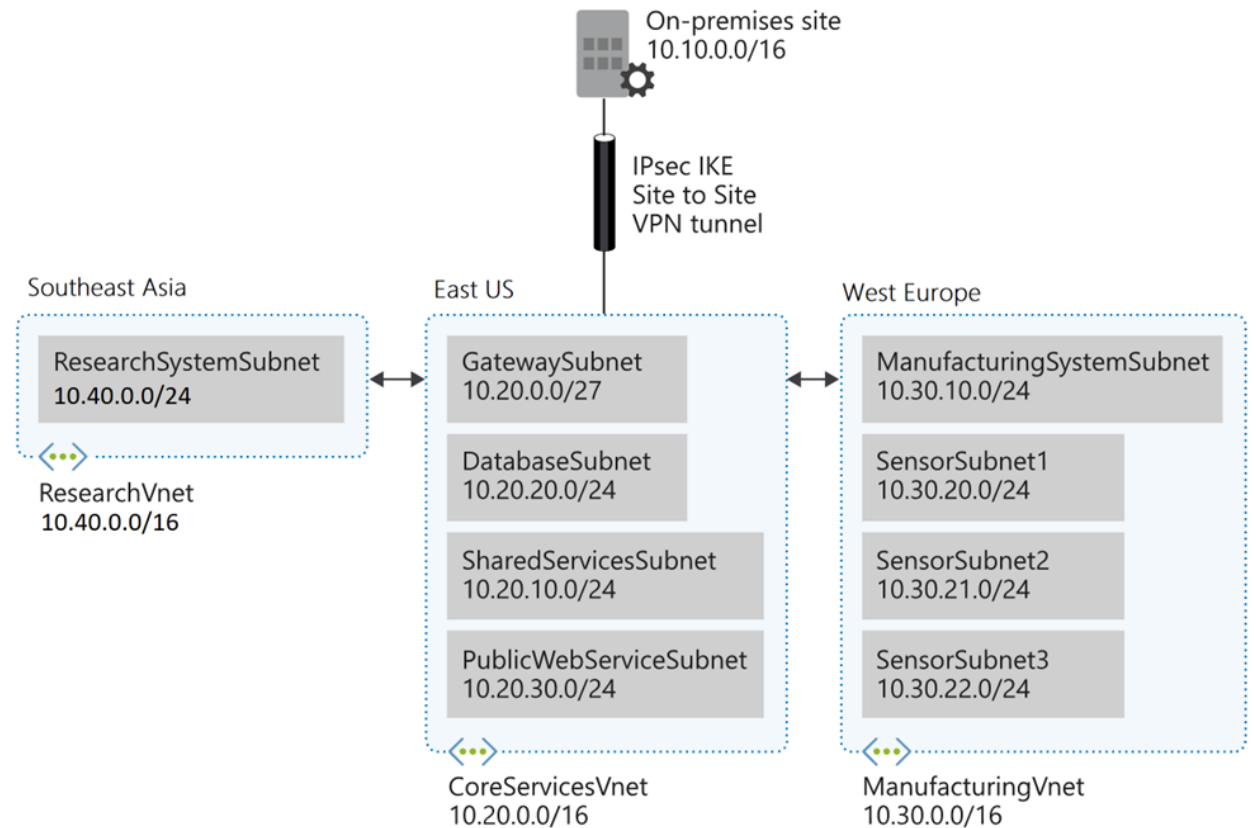




# Exercise – Create and Configure a Virtual Network Gateway



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



# Lab – Create a virtual WAN by using the Azure portal



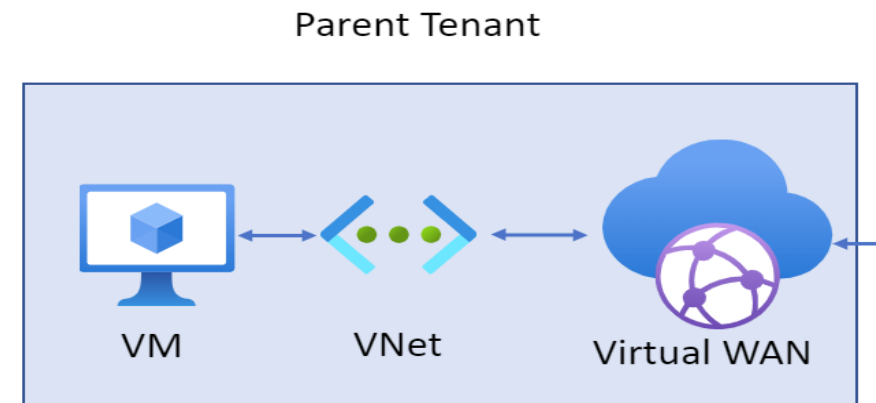
# Exercise – Create a Virtual WAN by Using Azure Portal



Task 1: Create a Virtual WAN

Task 2: Create a hub

Task 3: Connect a VNet to the Virtual Hub



# End of presentation

