THAILAND Cyber Security

Microsoft Security

Cloud

SECURITY

Intensive

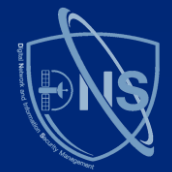
5

Network Security

Security Group

Virtual Network

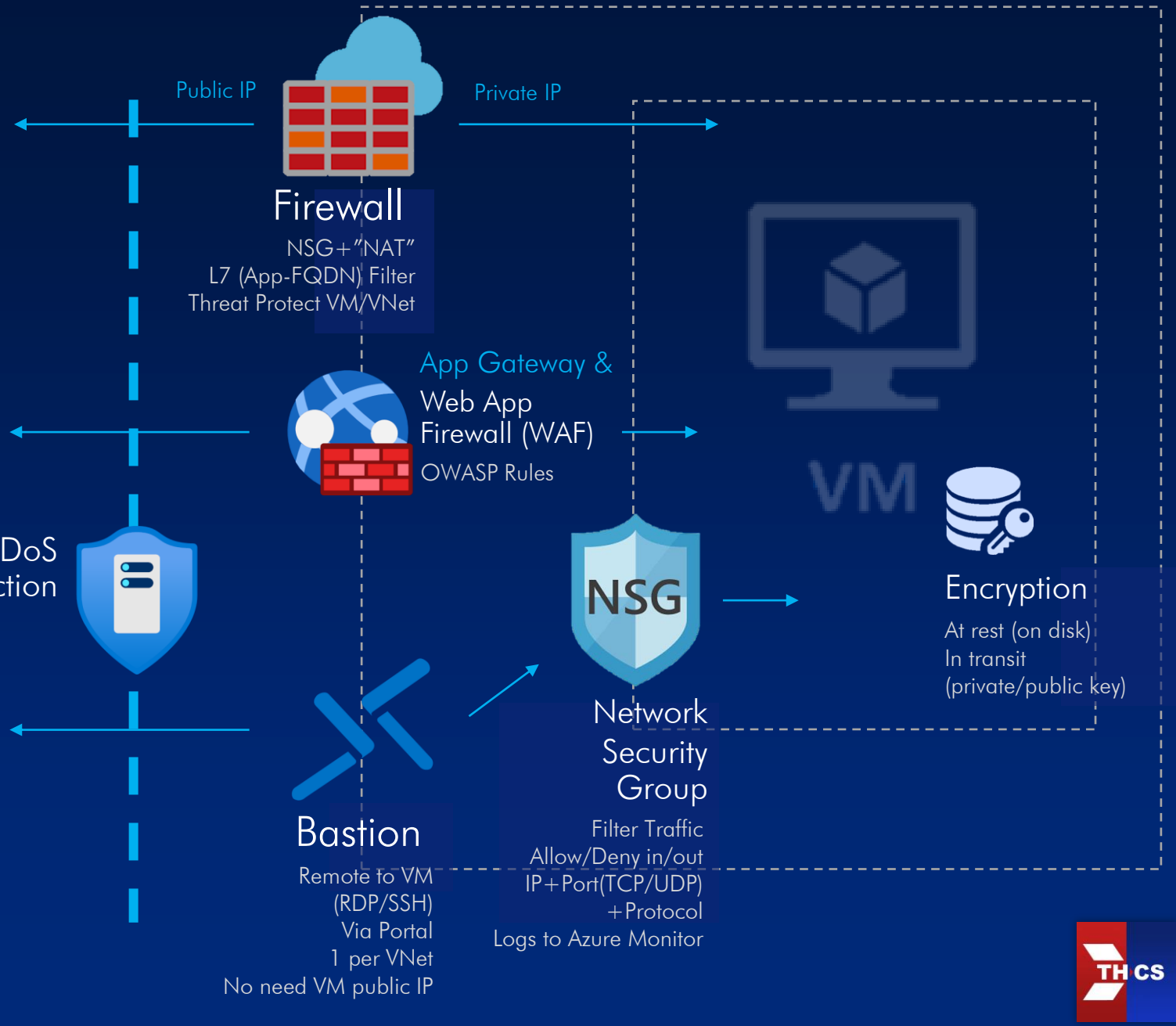
Bastion Host



SC-900

SECURITY
COMPLIANCE
IDENTITY

Microsoft CERTIFIED
SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS



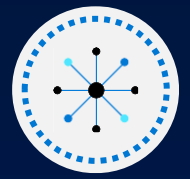
THCS

AZ-104

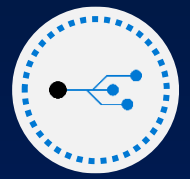
NETWORK

Module 4

Administer Virtual Network



01: Virtual Networks



02: Network Security Groups

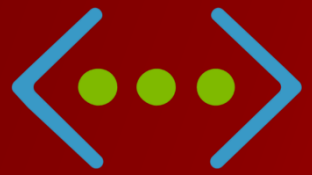
03: Azure Firewall

04: Azure DNS

05: Example Question

AZ-104

NETWORK



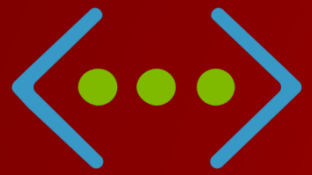
Virtual Networks

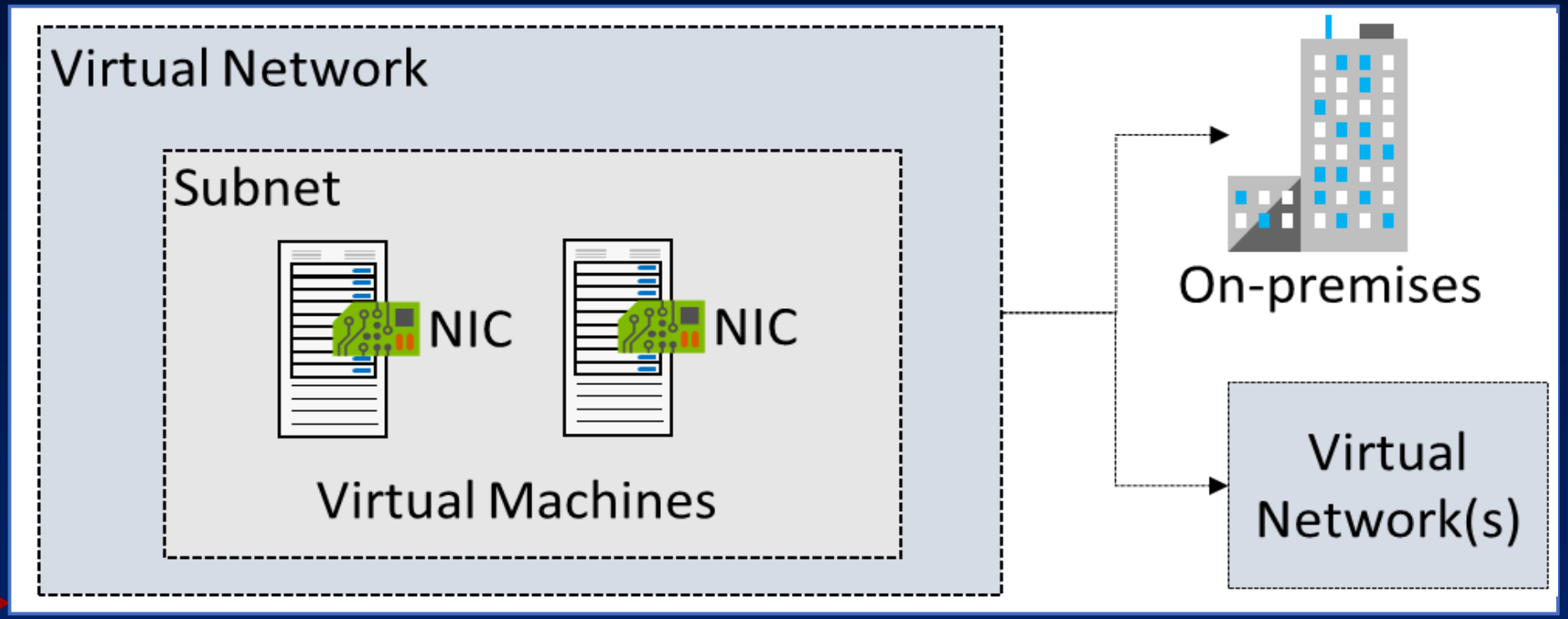
- Plan Virtual Networks
- Create Subnets
- Create Virtual Networks
- Plan IP Addressing
- Create Public IP Addresses
- Associate Public IP Addresses
- Associate Private IP Addresses

AZ-104

NETWORK

Virtual Networks





Logical representation of your own network

Create a dedicated private cloud-only virtual network

Securely extend your datacenter with virtual networks

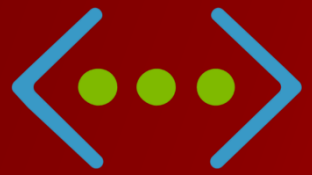
Enable hybrid cloud scenarios

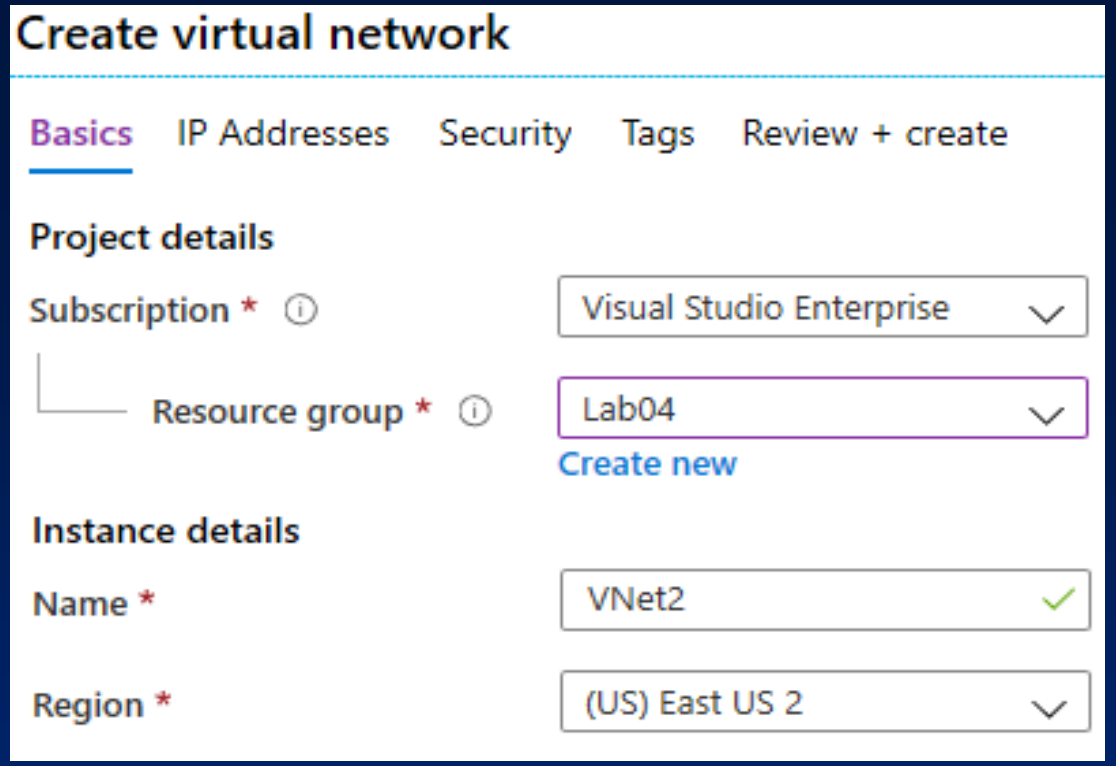
THCS

AZ-104

NETWORK

Virtual Network





Create new virtual networks at any time

Add virtual networks when you create a virtual machine

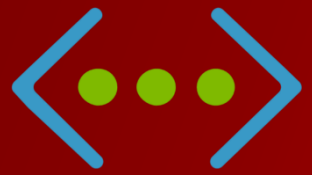
Need to define the address space, and at least one subnet

Be careful with overlapping address spaces

AZ-104

NETWORK

Virtual Network



+ Subnet | + Gateway subnet | Refresh | Manage users | Delete

Name	IPv4	IPv6	Available IPs	Delegated
subnet0	10.0.0.0/24	-	250	-
subnet1	10.0.1.0/24	-	251	-
subnet2	10.0.2.0/24	-	251	-
AzureBastionSubnet	10.0.30.0/27	-	27	-
GatewaySubnet	10.0.3.0/27	-	availability dependent on dynamic use	-

A virtual network can be segmented into one or more subnets

Subnets can help improve security, increase performance, and make it easier to manage the network

Subnets provide logical divisions within your network

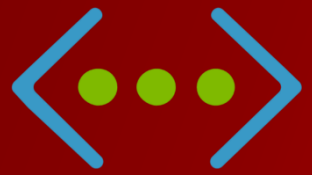
Each subnet must have a unique address range – cannot overlap with other subnets in the vnet in the subscription

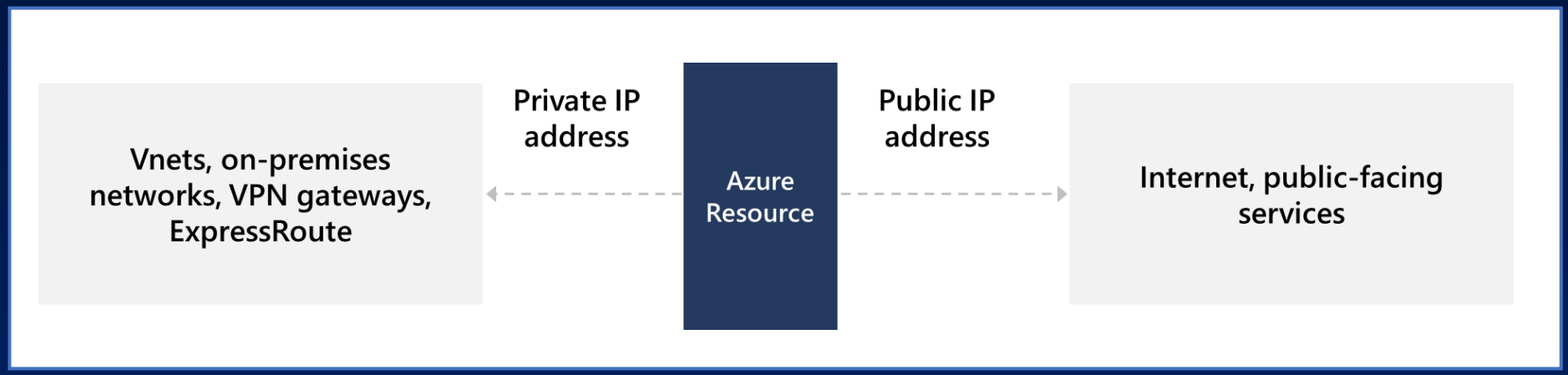
THCS

AZ-104

NETWORK

Virtual Network





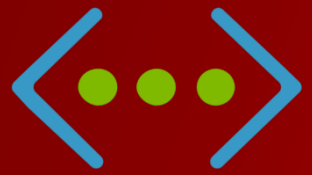
Private IP addresses - used within an Azure virtual network (VNet), and your on-premises network, when you use a VPN gateway or ExpressRoute circuit to extend your network to Azure

Public IP addresses - used for communication with the Internet, including Azure public-facing services

AZ-104

NETWORK

Virtual Network



Available in IPv4 or IPv6 or both

Basic vs Standard SKU

Dynamic vs Static

Zone redundant (Standard SKU)

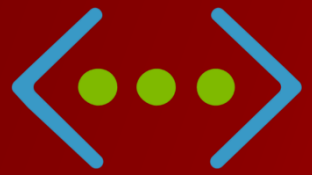
Range of contiguous addresses available as a prefix

THCS

AZ-104

NETWORK

Virtual Network



Public IP addresses	IP address association	Dynamic	Static
Virtual Machine	NIC	Yes	Yes
Load Balancer	Front-end configuration	Yes	Yes
VPN Gateway	Gateway IP configuration	Yes	Yes*
Application Gateway	Front-end configuration	Yes	Yes*

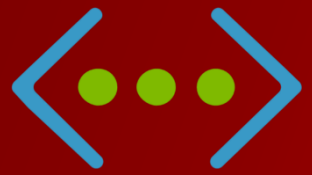
A public IP address resource can be associated with virtual machine network interfaces, internet-facing load balancers, VPN gateways, and application gateways

*Static IP addresses only available on certain SKUs.

AZ-104

NETWORK

Virtual Network



Private IP Addresses	IP address association	Dynamic	Static
Virtual Machine	NIC	Yes	Yes
Internal Load Balancer	Front-end configuration	Yes	Yes
Application Gateway	Front-end configuration	Yes	Yes

Dynamic (default). **Azure assigns the next available unassigned or unreserved IP address in the subnet's address range**

Static. **You select and assign any unassigned or unreserved IP address in the subnet's address range**

AZ-104

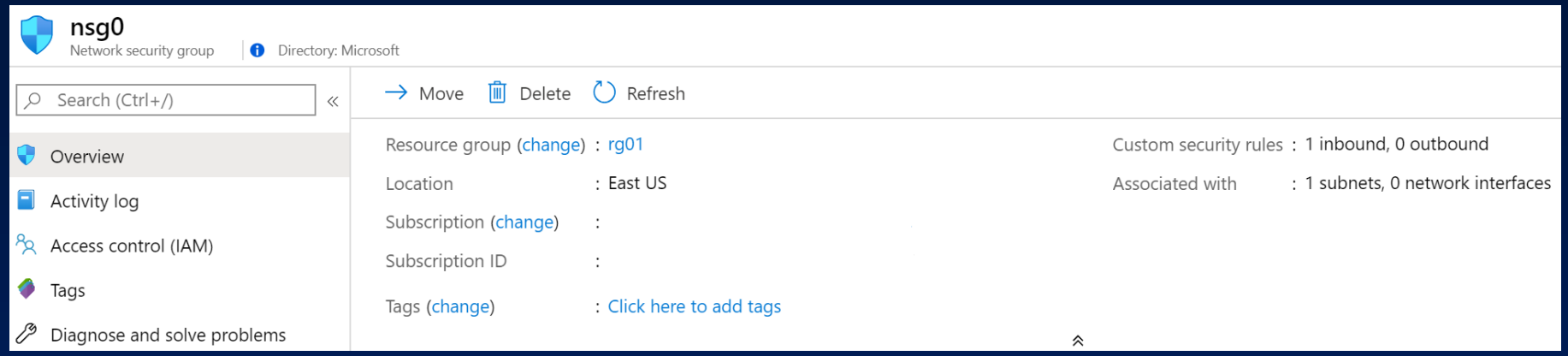
NETWORK

Network Security Groups

- Implement Network Security Groups (NSG)
- Determine NSG Rules
- Determine NSG Effective Rules
- Create NSG Rules

AZ-104

NETWORK
Network Security Groups



Limits network traffic to resources in a virtual network

Lists the security rules that allow or deny inbound or outbound network traffic

Associated to a subnet or a network interface

Can be associated multiple times

AZ-104

NETWORK
Network Security Groups

Inbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
100	⚠ RDP_Inbound	3389	Any	Any	Any	✔ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✔ Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✔ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✖ Deny

Outbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✔ Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	✔ Allow
65500	DenyAllOutBound	Any	Any	Any	Any	✖ Deny

Security rules in NSGs enable you to filter network traffic that can flow in and out of virtual network subnets and network interfaces

There are default security rules. You cannot delete the default rules, but you can add other rules with a higher priority

THCS

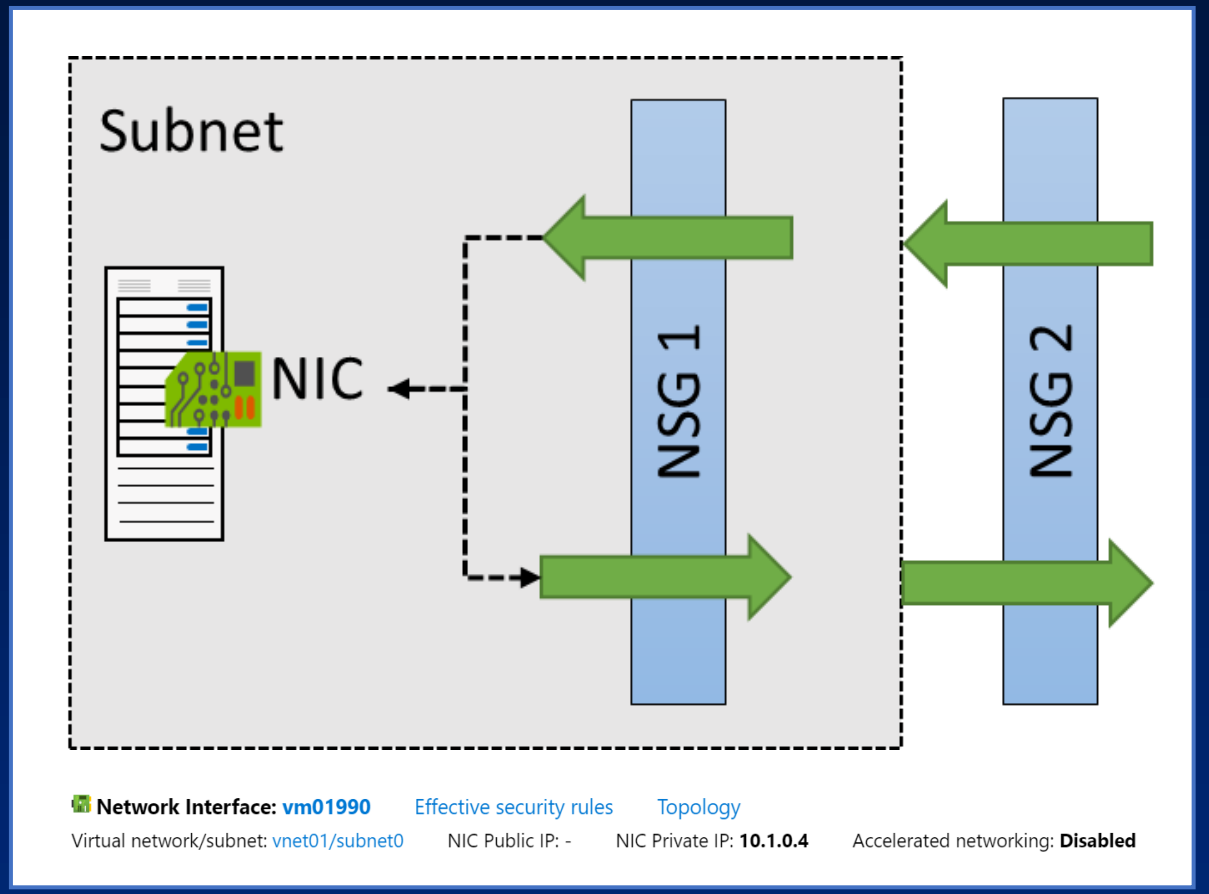
AZ-104

NETWORK
Network Security Groups

NSGs are evaluated independently for the subnet and NIC

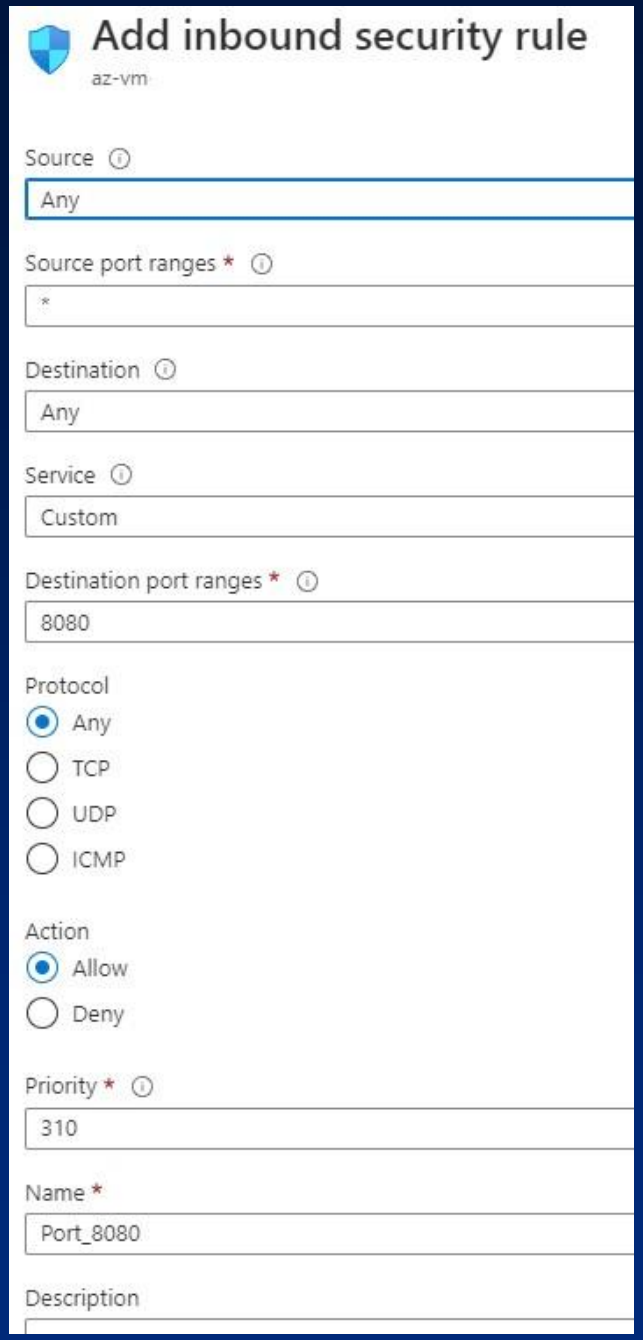
An “allow” rule must exist at both levels for traffic to be admitted

Use the Effective Rules link if you are not sure which security rules are being applied



AZ-104

NETWORK
Network Security Groups



Select from a large variety of services

Service – The destination protocol and port range for this rule

Port ranges – Single port or multiple ports

Priority – The lower the number, the higher
the priority

AZ-104

NETWORK

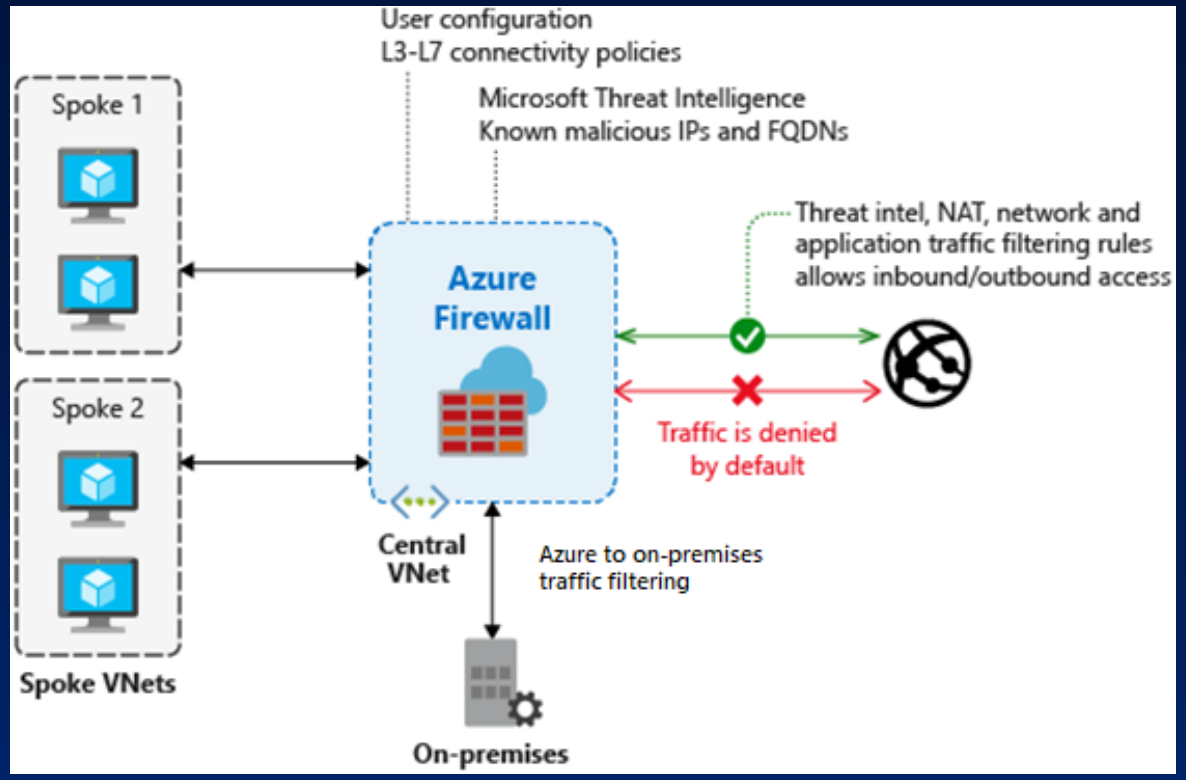
Azure Firewall

- Determine Azure Firewall Uses
- Create Azure Firewalls
- Create Azure Firewall Rules

AZ-104

NETWORK

Azure Firewall



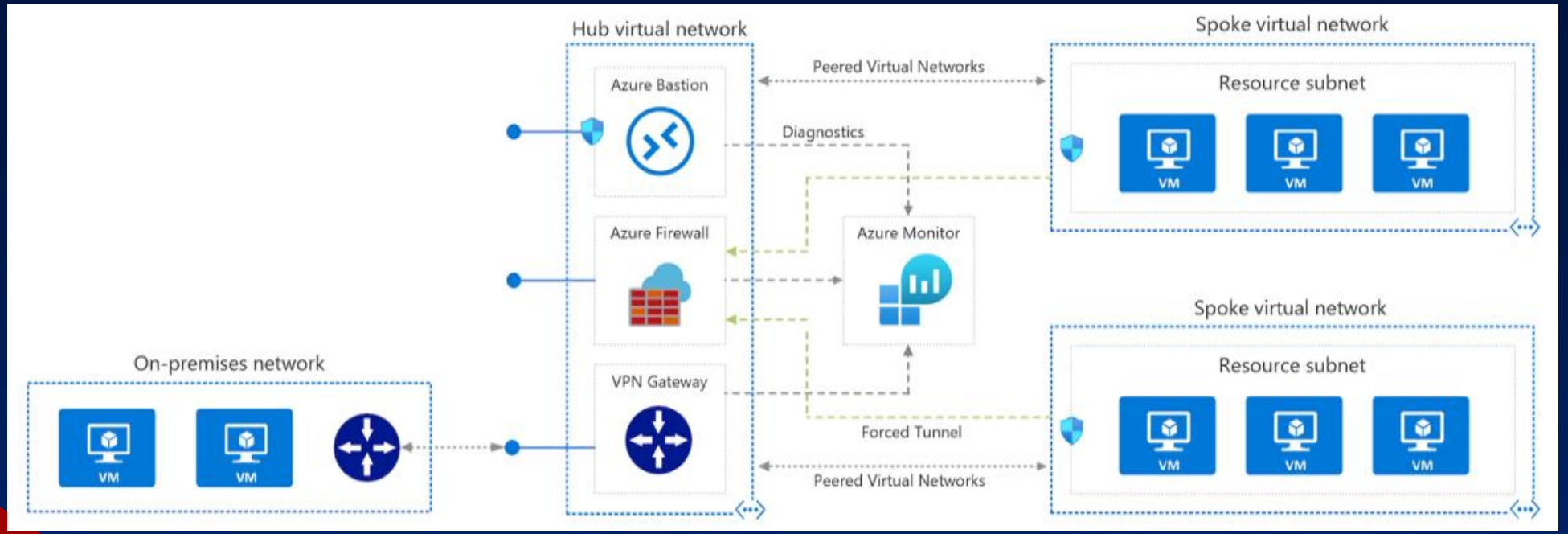
- Stateful firewall as a service
- Threat intelligence-based filtering
- Built-in high availability with unrestricted cloud scalability
- Fully integrated with Azure Monitor for logging and analytics
- Create, enforce, and log application and network connectivity policies
- Support for hybrid connectivity through deployment behind VPN and ExpressRoute Gateways

THCS

AZ-104

NETWORK

Azure Firewall



A Hub-Spoke network topology is recommended

Shared services are placed in the hub virtual network

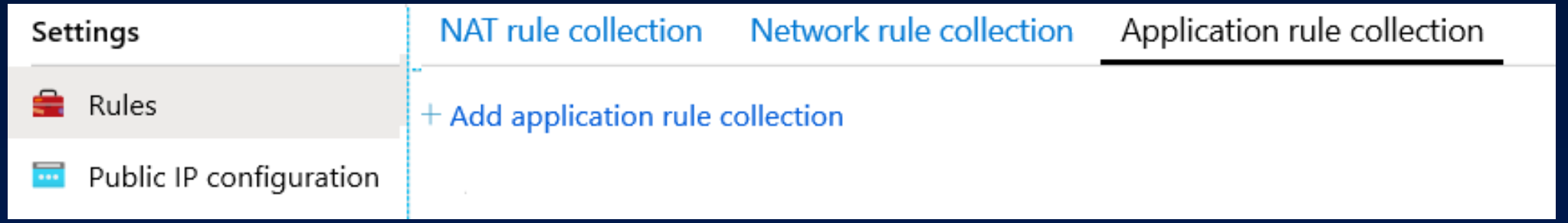
Each environment is deployed to a spoke to maintain isolation

THCS

AZ-104

NETWORK

Azure Firewall



NAT rules. Configure DNAT rules to allow incoming connections

Network rules. Configure rules that contain source addresses, protocols, destination ports, and destination addresses

Application rules. Configure fully qualified domain names (FQDNs) that can be accessed from a subnet

AZ-104

NETWORK

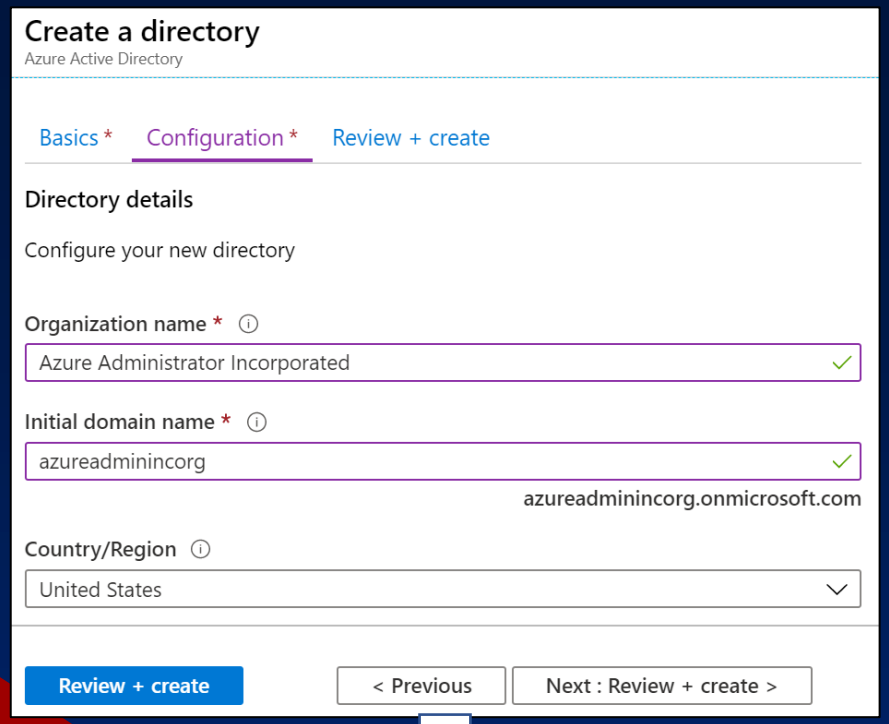
Azure DNS

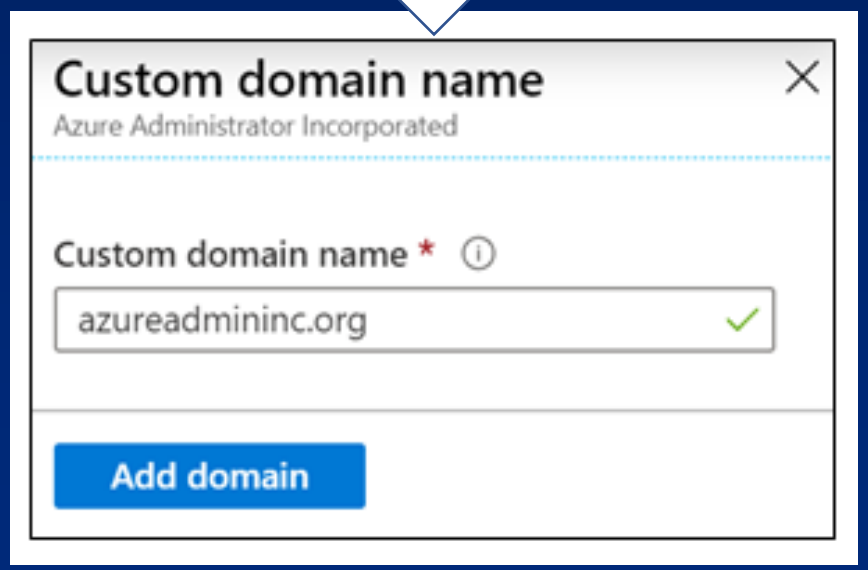
- Identify Domains and Custom Domains
- Verify Custom Domain Names
- Create Azure DNS Zones
- Delegate DNS Domains
- Add DNS Record Sets
- Plan for Private DNS Zones
- Determine Private Zone Scenarios

AZ-104

NETWORK

Azure DNS





When you create an Azure subscription an Azure AD domain is created for you

The domain has initial domain name in the form *domainname.onmicrosoft.com*

You can customize/change the name

After the custom name is added it must be verified (next topic)

THCS

AZ-104

NETWORK

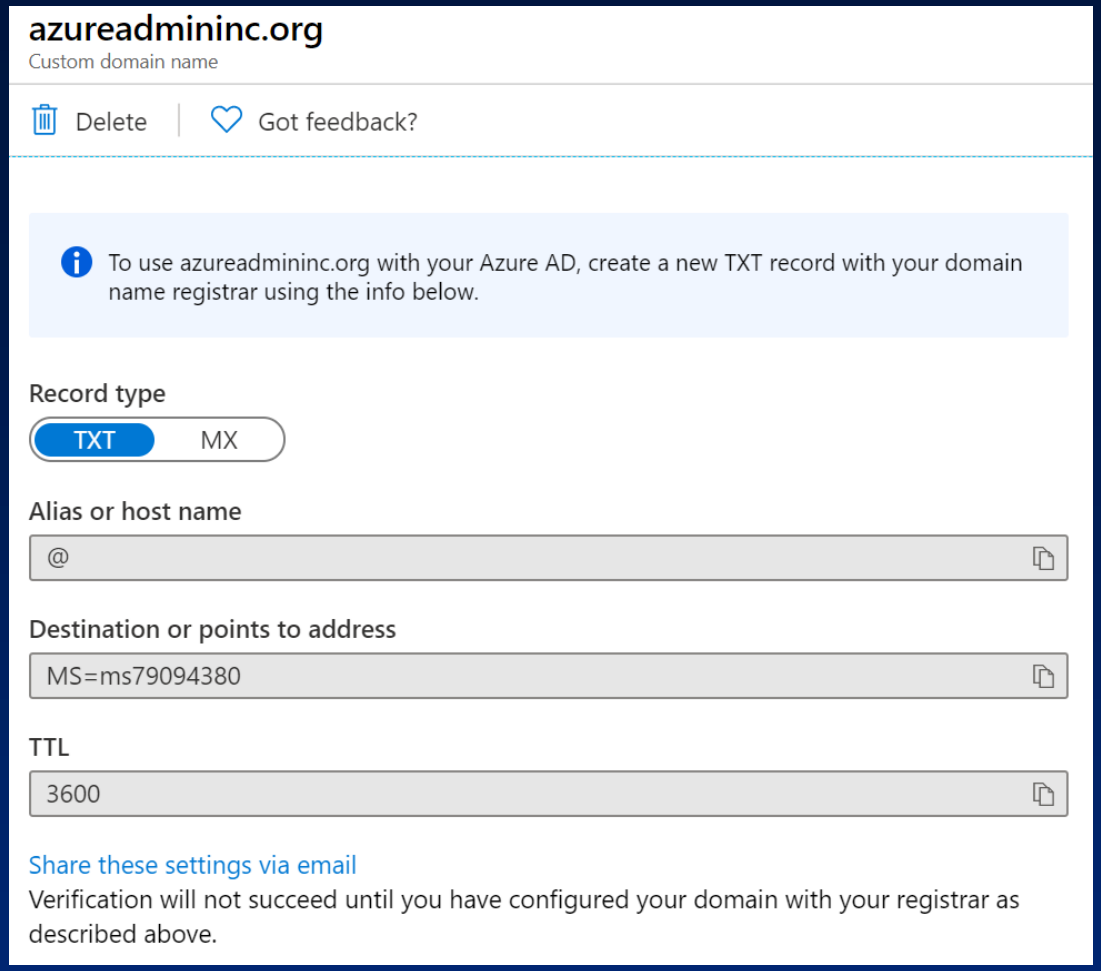
Azure DNS

Verification demonstrates ownership of the domain name

Add a DNS record (MX or TXT) that is provided by Azure into your company's DNS zone

Azure will query the DNS domain for the presence of the record

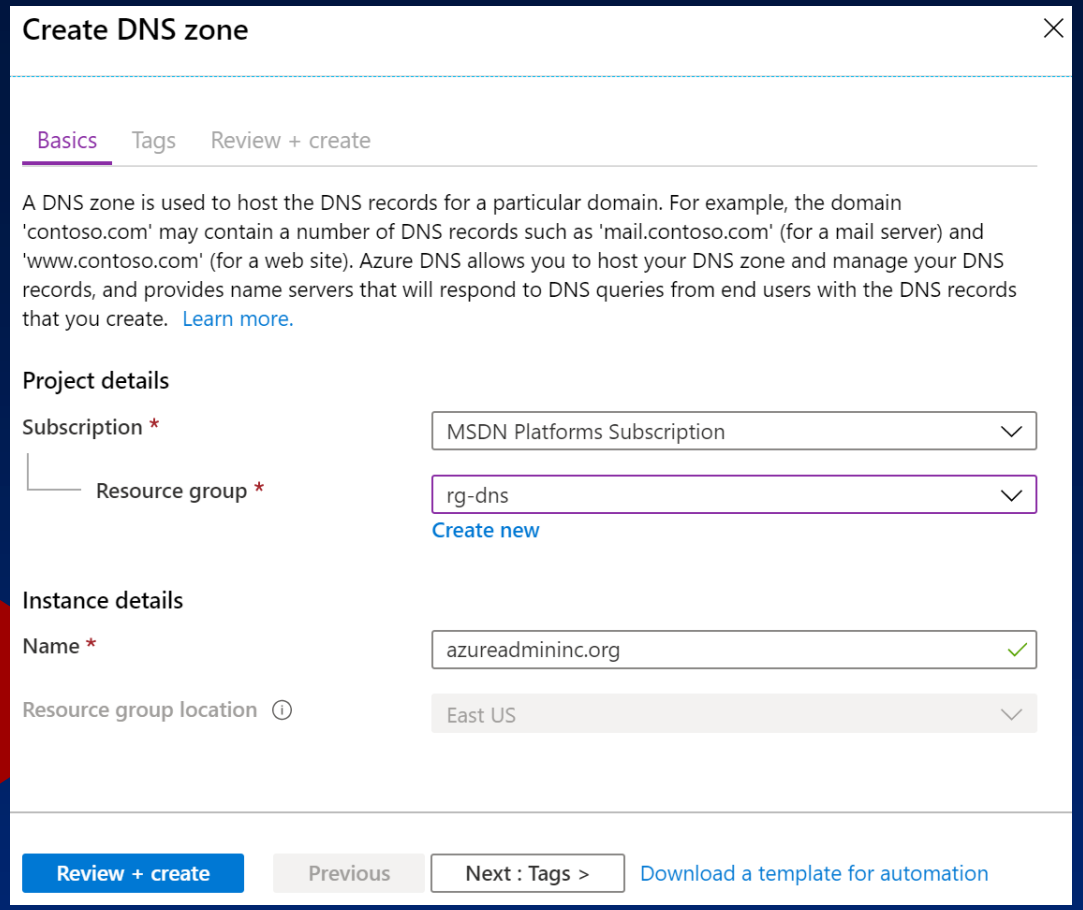
This could take several minutes or several hours



AZ-104

NETWORK

Azure DNS



A DNS zone hosts the DNS records for a domain

Where multiple zones share the same name, each instance is assigned different name server addresses

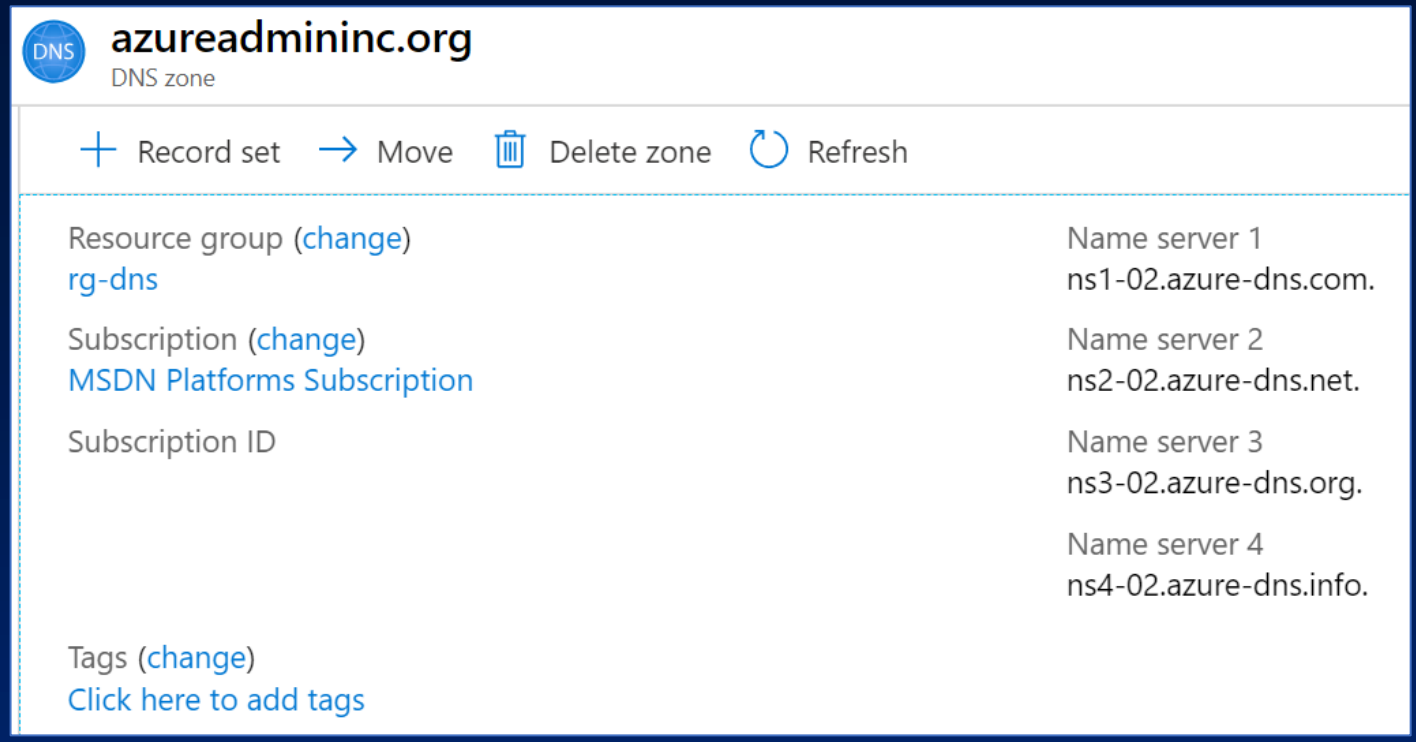
Root/Parent domain is registered at the registrar and pointed to Azure NS

THCS

AZ-104

NETWORK

Azure DNS



When delegating a domain to Azure DNS, you must use the name server names provided by Azure DNS – use all four

Once the DNS zone is created, update the parent registrar

For child zones, register the NS records in the parent domain

AZ-104

NETWORK

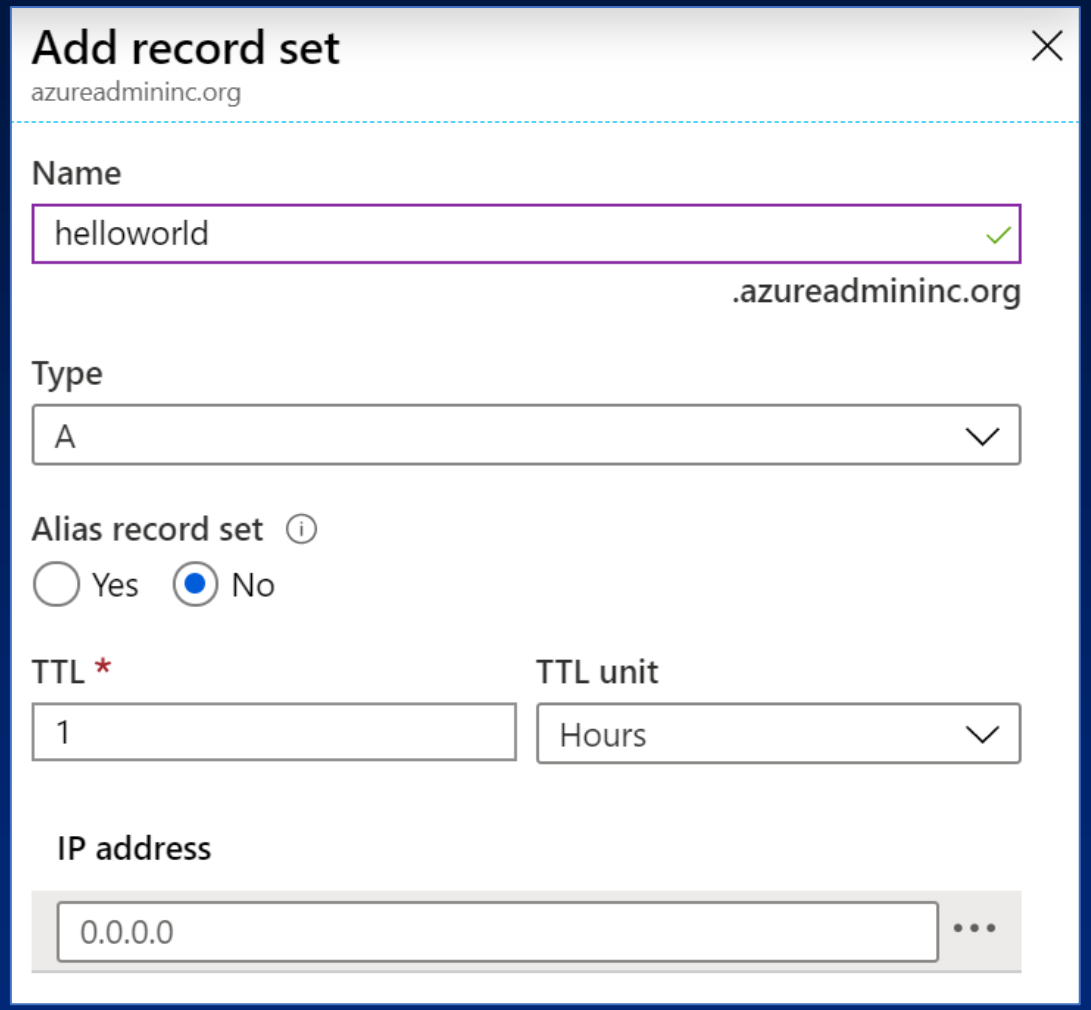
Azure DNS

A record set is a collection of records in a zone that have the same name and are the same type

You can add up to 20 records to any record set

A record set cannot contain two identical records

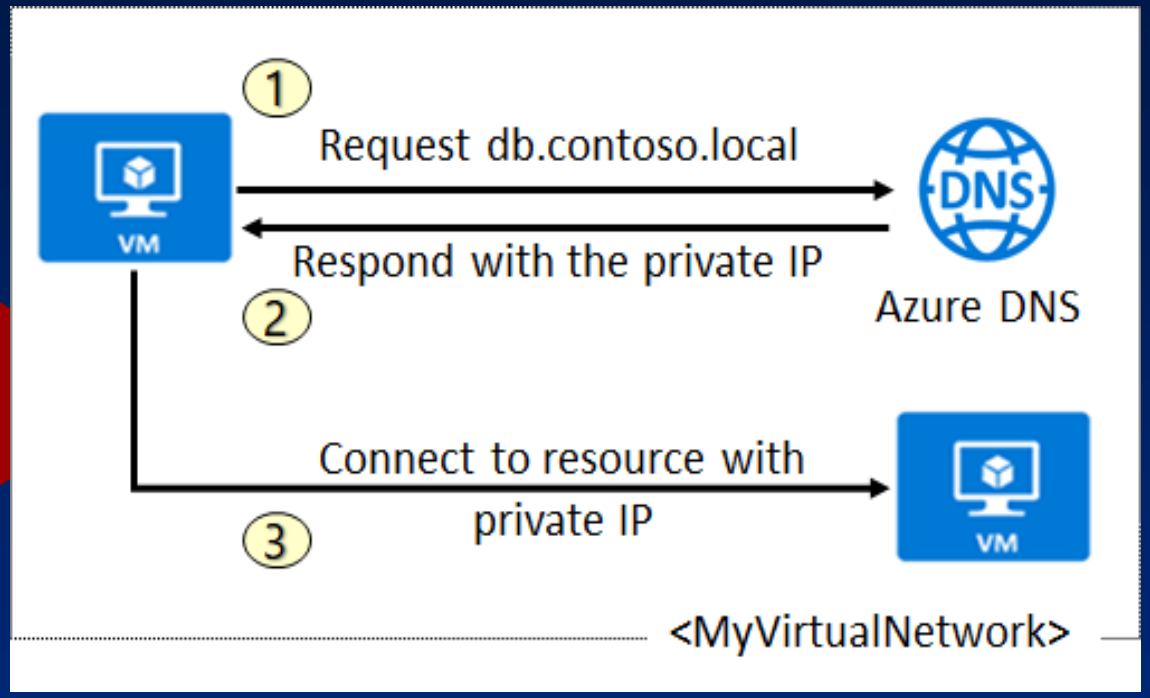
Changing the drop-down Type, changes the information required



AZ-104

NETWORK

Azure DNS

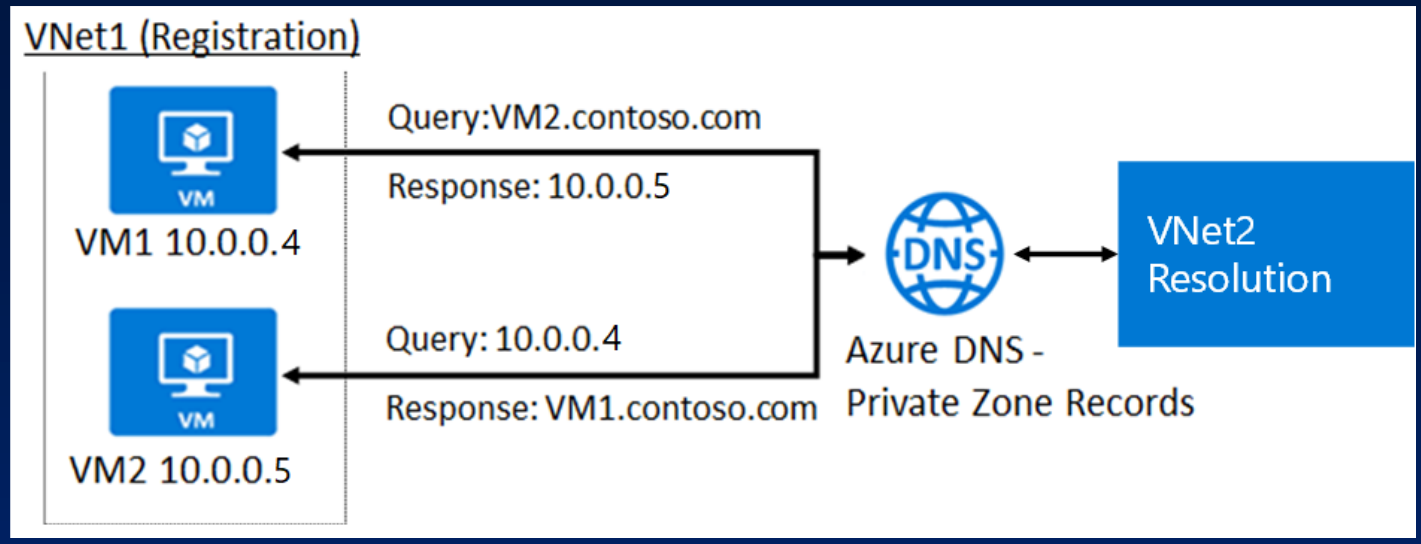


- Use your own custom domain names
- Provides name resolution for VMs within a VNet and between VNets
- Automatic hostname record management
- Removes the need for custom DNS solutions
- Use all common DNS records types
- Available in all Azure regions

AZ-104

NETWORK

Azure DNS



DNS resolution in VNet1 is private and not accessible from the Internet

DNS queries across the virtual networks are resolved

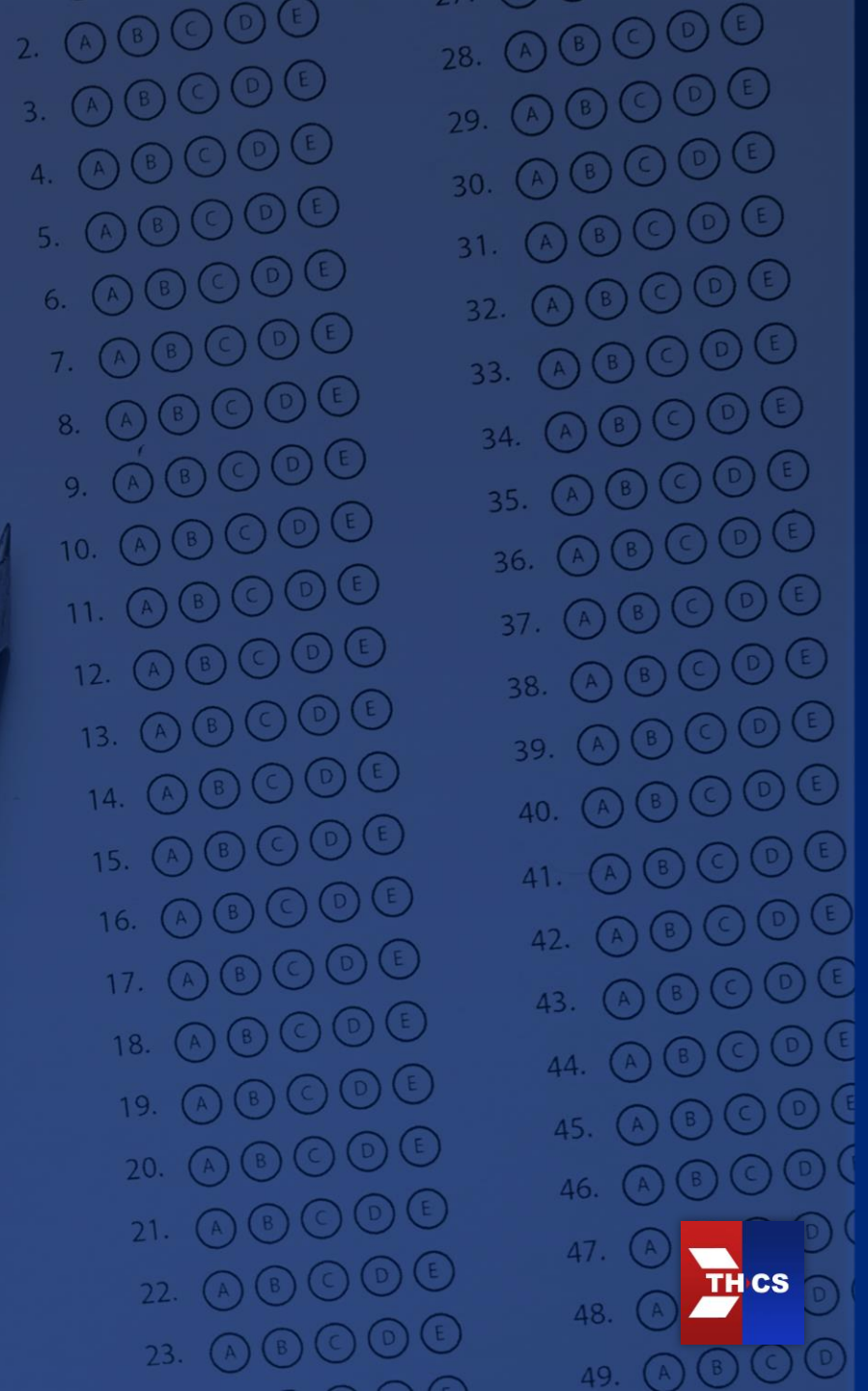
Reverse DNS queries are scoped to the same virtual network

AZ-104

NETWORK

Intersite Connectivity

Example Questions



AZ-104

NETWORK

Azure DNS

Scenario: You have a public-facing application named App1. App1 is comprised of the following three tiers:

- A SQL database
- A web front end
- A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Technical requirements include:

- Move all the virtual machines for App1 to Azure.
- Minimize the number of open ports between the App1 tiers.

HOTSPOT -

You need to recommend a solution for App1. The solution must meet the technical requirements.

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Number of virtual networks: 1 (2, 3)

Number of subnets per virtual network: 3 (1, 2)

AZ-104

NETWORK

Azure DNS

You plan to deploy five virtual machines to a virtual network subnet.

Each virtual machine will have a public IP address and a private IP address.

Each virtual machine requires the same inbound and outbound security rules.

What is the minimum number of network interfaces and network security groups that you require? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Minimum number of network interfaces:

- 5
- 10
- 15
- 20

Minimum number of network security groups:

- 1
- 2
- 5
- 10

AZ-104

NETWORK

Azure DNS

You have an Azure subscription that contains the virtual machines shown in the following table:

Name	Operating system	Connects to
VM1	Windows Server 2019	Subnet1
VM2	Windows Server 2019	Subnet2

VM1 and VM2 use public IP addresses. From Windows Server 2019 on VM1 and VM2, you allow inbound Remote Desktop connections.

Subnet1 and Subnet2 are in a virtual network named VNET1.

The subscription contains two network security groups (NSGs) named NSG1 and NSG2. NSG1 uses only the default rules.

NSG2 uses the default rules and the following custom incoming rule:

- Priority: 100
- Name: Rule1
- Port: 3389
- Protocol: TCP
- Source: Any
- Destination: Any
- Action: Allow

NSG1 is associated to Subnet1. NSG2 is associated to the network interface of VM2.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
From the Internet, you can connect to VM1 by using Remote Desktop.	○	○
From the Internet, you can connect to VM2 by using Remote Desktop.	○	○
From VM1, you can connect to VM2 by using Remote Desktop	○	○

AZ-104

NETWORK

Azure DNS

You have a network security group (NSG) named NSG1 that has the rules defined in the exhibit. (Click the Exhibit tab.)

```
PS C:\> Get-AzNetworkSecurityGroup -Name "NSG1" -ResourceGroupName "RG1" | Select -ExpandProperty SecurityRules

Name                                 : ALLOW_HTTPS
Id                                   : /subscriptions/09d06b22-ff51-48b7-a8be-947f15cbd69d/resourceGroups/RG1/
                                       providers/Microsoft.Network/networkSecurityGroups/NSG1/securityRules/AL
                                       LOW_HTTPS
Etag                                 : W/"8e3e9995-aa78-41e2-bfea-44b50c389873"
ProvisioningState                    : Succeeded
Description                          :
Protocol                             : TCP
SourcePortRange                      : {*}
DestinationPortRange                 : {443}
SourceAddressPrefix                  : {*}
DestinationAddressPrefix             : {*}
SourceApplicationSecurityGroups      : []
DestinationApplicationSecurityGroups : []
Access                               : Allow
Priority                             : 100
Direction                            : Inbound


Name                                 : DENY_PING
Id                                   : /subscriptions/09d06b22-ff51-48b7-a8be-947f15cbd69d/resourceGroups/RG1/
                                       providers/Microsoft.Network/networkSecurityGroups/NSG1/securityRules/DE
                                       NY_PING
Etag                                 : W/"8e3e9995-aa78-41e2-bfea-44b50c389873"
ProvisioningState                    : Succeeded
Description                          :
Protocol                             : ICMP
SourcePortRange                      : {*}
DestinationPortRange                 : {*}
SourceAddressPrefix                  : {VirtualNetwork}
DestinationAddressPrefix             : {*}
SourceApplicationSecurityGroups      : []
DestinationApplicationSecurityGroups : []
Access                               : Deny
Priority                             : 111
Direction                            : Outbound
```

NSG1 is associated to a subnet named Subnet1. Subnet1 contains the virtual machines shown in the following table.

Name	IP address
VM1	10.1.0.10
VM2	10.1.0.11

You need to add a rule to NSG1 to ensure that VM1 can ping VM2. The solution must use the principle of least privilege.

How should you configure the rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Direction:

- Inbound
- Outbound

Source:

- Any
- 10.1.0.10
- 10.1.0.11
- 10.1.0.10; 10.1.0.11
- 10.1.0.0/28

Destination:

- Any
- 10.1.0.10
- 10.1.0.11
- 10.1.0.10; 10.1.0.11
- 10.1.0.0/28

Priority:

- 110
- 111
- 112

AZ-104

NETWORK

Azure DNS

You have an Azure Active Directory (Azure AD) tenant that has the contoso.onmicrosoft.com domain name.

You have a domain name of contoso.com registered at a third-party registrar.

You need to ensure that you can create Azure AD users that have names containing a suffix of @contoso.com.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Actions		Answer Area
Add a record to the public contoso.com DNS zone		Add a custom name
Add an Azure AD tenant		Add a record to the public contoso.com DNS zone
Configure company branding	>	Verify the domain
Create an Azure DNS zone	<	
Add a custom name		
Verify the domain		

THCS

AZ-104

NETWORK

Azure DNS

You have an Azure subscription that contains the resources in the following table.

Name	Type	Azure region	Resource group
VNet1	Virtual network	West US	RG2
VNet2	Virtual network	West US	RG1
VNet3	Virtual network	East US	RG1
NSG1	Network security group (NSG)	East US	RG2

To which subnets can you apply NSG1?

A. the subnets on VNet1 only

B. the subnets on VNet2 and VNet3 only

C. the subnets on VNet2 only

D. the subnets on VNet3 only

E. the subnets on VNet1, VNet2, and VNet3

AZ-104

NETWORK

Azure DNS

Your company has an Azure Active Directory (Azure AD) subscription.

You need to deploy five virtual machines (VMs) to your company's virtual network subnet.

The VMs will each have both a public and private IP address. Inbound and outbound security rules for all of these virtual machines must be identical.

Which of the following is the least amount of network interfaces needed for this configuration?

A. 5

B. 10

C. 20

D. 40

AZ-104

NETWORK

Azure DNS

Your company has an Azure Active Directory (Azure AD) subscription.

You need to deploy five virtual machines (VMs) to your company's virtual network subnet.

The VMs will each have both a public and private IP address. Inbound and outbound security rules for all of these virtual machines must be identical.

Which of the following is the least amount of security groups needed for this configuration?

A. 4

B. 3

C. 2

D. 1

AZ-104

NETWORK

Azure DNS

You have a registered DNS domain named contoso.com.

You create a public Azure DNS zone named contoso.com.

You need to ensure that records created in the contoso.com zone are resolvable from the internet.

What should you do?

A. Create NS records in contoso.com.

B. Modify the SOA record in the DNS domain registrar.

C. Create the SOA record in contoso.com.

D. Modify the NS records in the DNS domain registrar.

AZ-104

NETWORK

Azure DNS

You have Azure virtual machines that run Windows Server 2019 and are configured as shown in the following table.

Name	Private IP address	Public IP address	Virtual network name	DNS suffix configured in Windows Server
VM1	10.1.0.4	52.186.85.63	VNET1	Adatum.com
VM2	10.1.0.5	13.92.168.13	VNET1	Contoso.com

You create a private Azure DNS zone named adatum.com. You configure the adatum.com zone to allow auto registration from VNET1.

Which A records will be added to the adatum.com zone for each virtual machine? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

A records for VM1:

- None
- **Private IP address only**
- Public IP address only
- Private IP address and public IP address

A records for VM2:

- None
- **Private IP address only**
- Public IP address only
- Private IP address and public IP address

THCS

AZ-104

NETWORK

Azure DNS

You have an Azure Active Directory (Azure AD) tenant named contosocloud.onmicrosoft.com.

Your company has a public DNS zone for contoso.com.

You add contoso.com as a custom domain name to Azure AD.

You need to ensure that Azure can verify the domain name.

Which type of DNS record should you create?

A. MX

B. NSEC

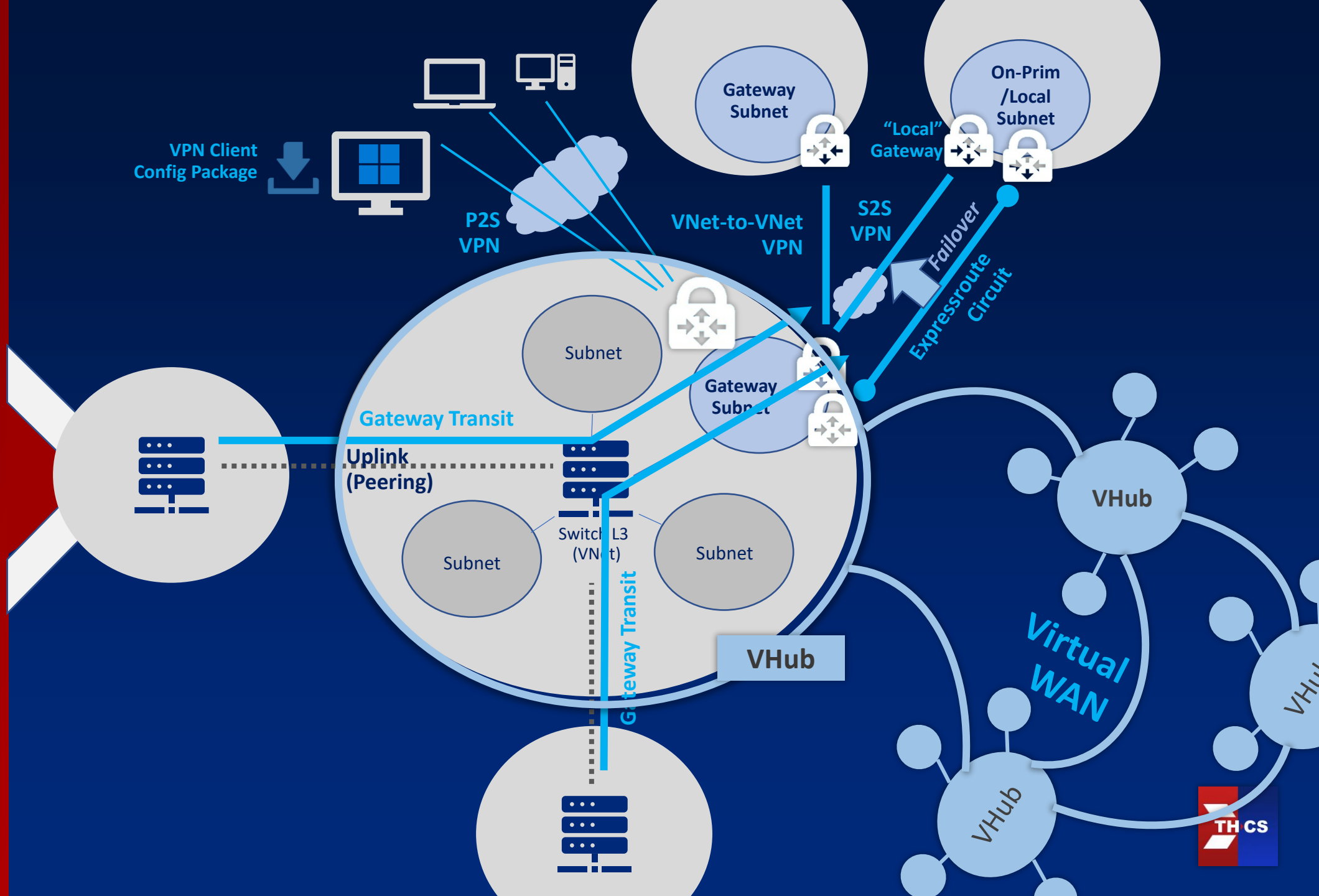
C. SRV

D. NSEC3

AZ-104

NETWORK

Intersite Connectivity



AZ-104

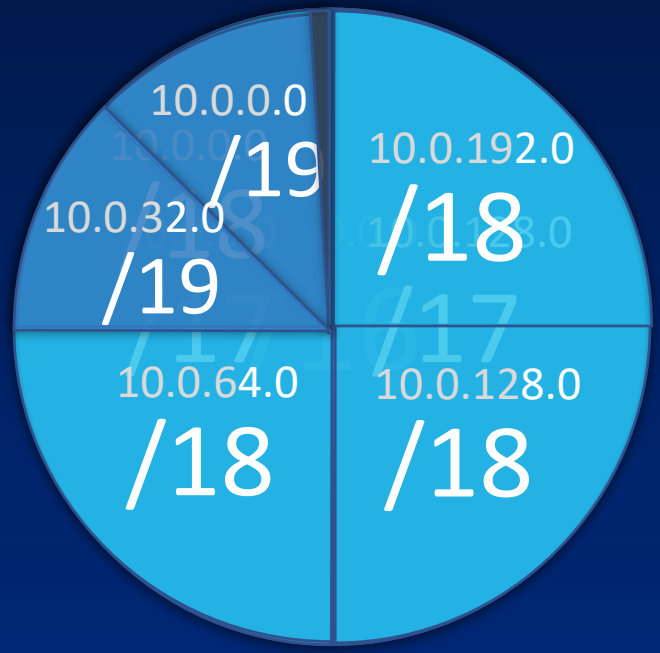
NETWORK

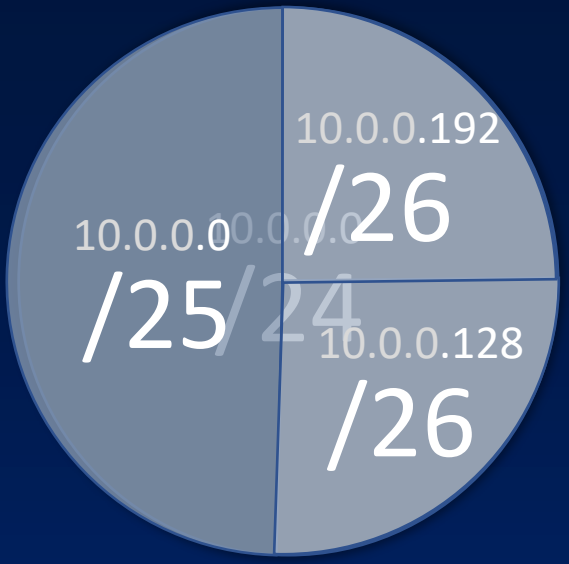
Intersite Connectivity

Address Space

"Overlapped"

Cannot be peered or connect via Vnet (VPN) Gateway





Any VNet has no any Address Space left for create GatewaySubnet, cannot create Gateway!

Address Space

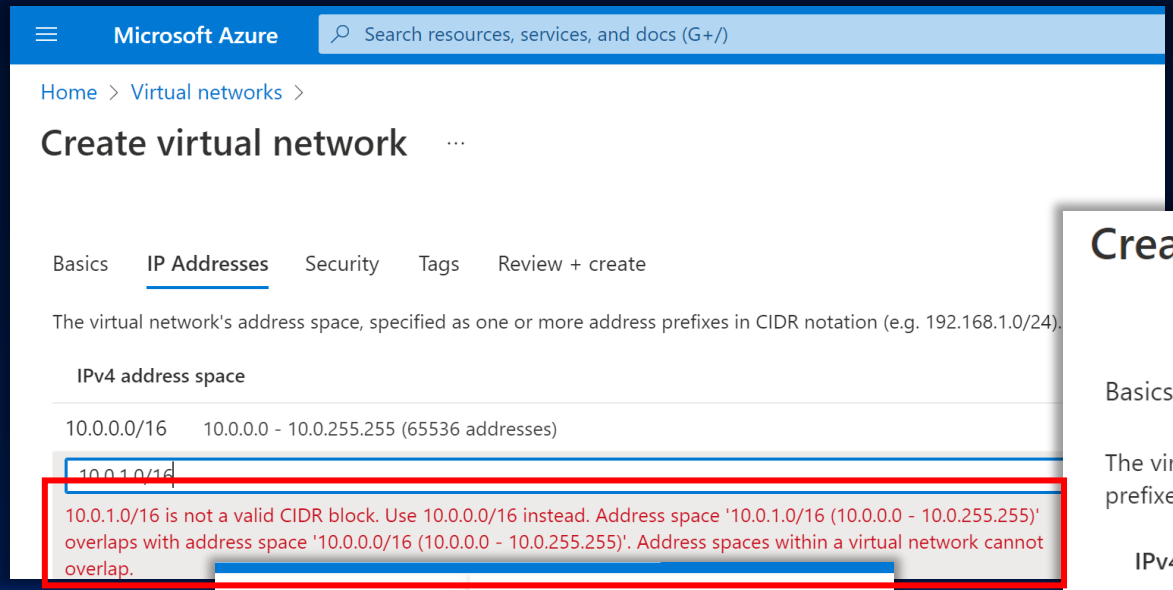
IP Subnetting

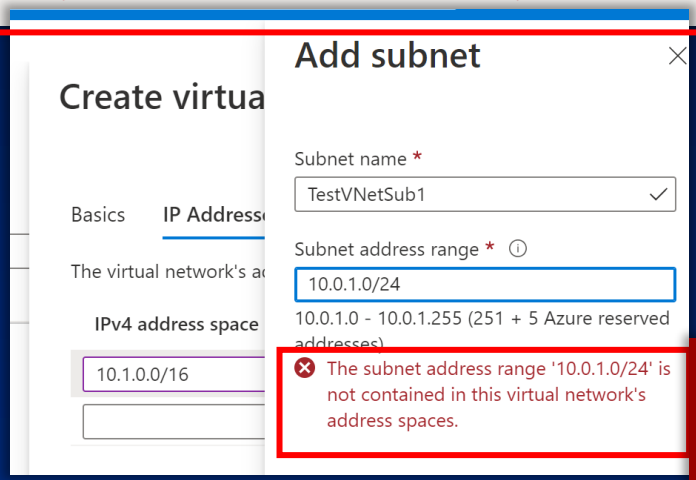
THCS

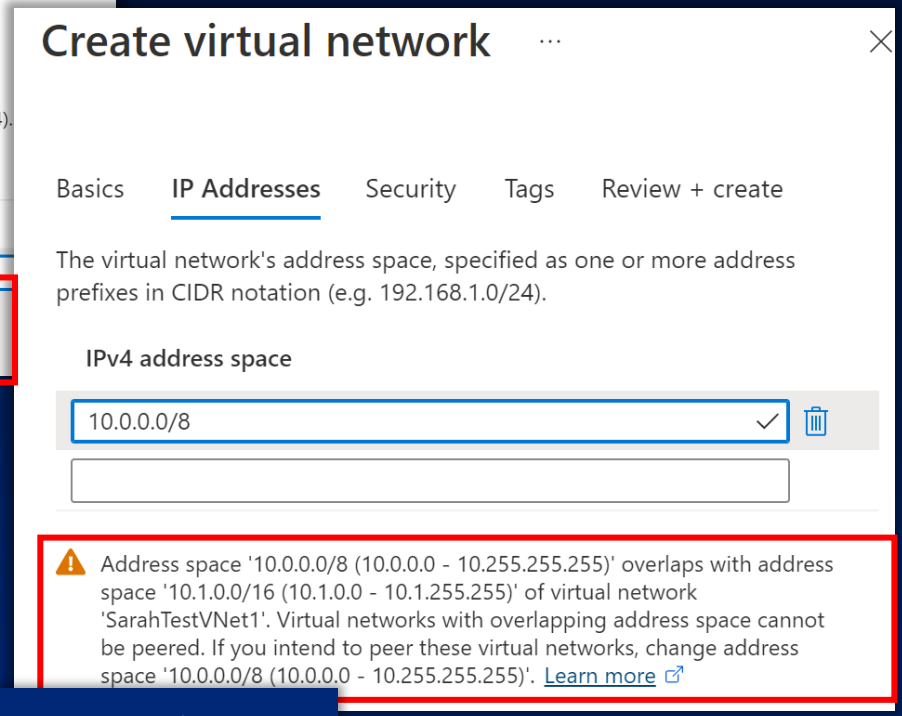
AZ-104

NETWORK

Intersite Connectivity







Azure alerts ⚠ you from creating VNet stage, both subnetting error and peering conflict probability

Address Space

IP Subnetting

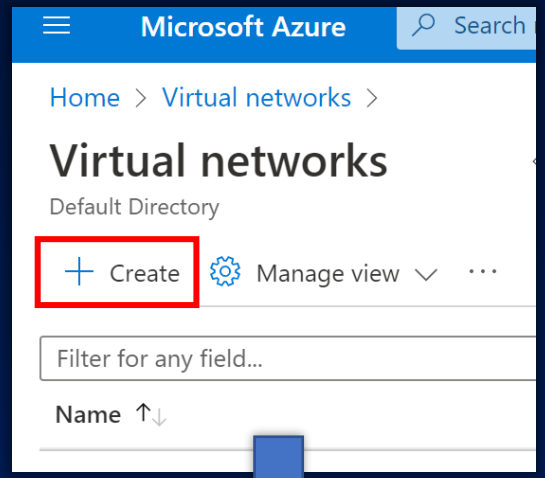
THCS

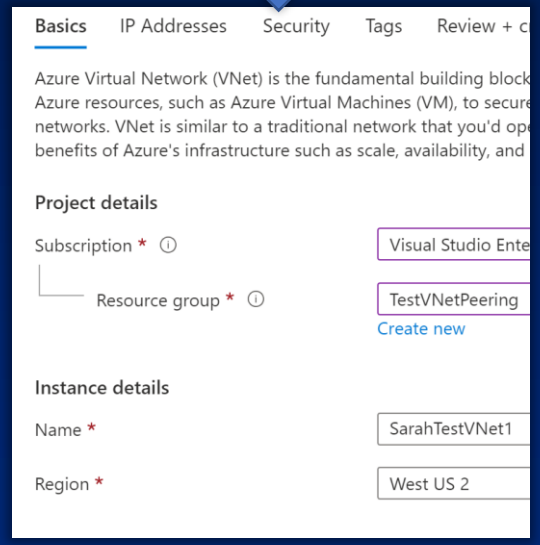
AZ-104

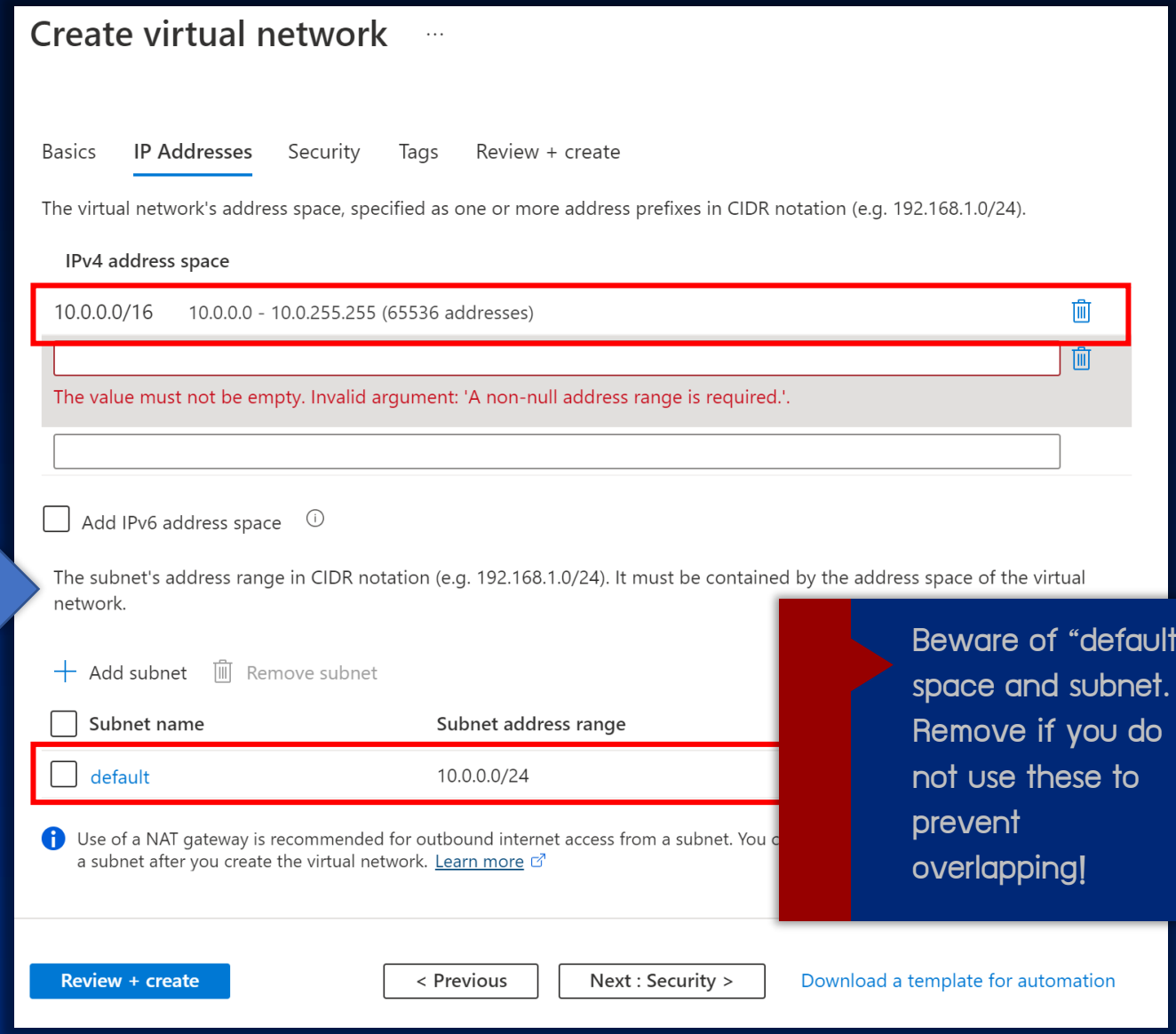
NETWORK

Intersite Connectivity

Microsoft CERTIFIED AZURE ADMINISTRATOR ASSOCIATE







Beware of “default” space and subnet. Remove if you do not use these to prevent overlapping!

How to

Peer VNet

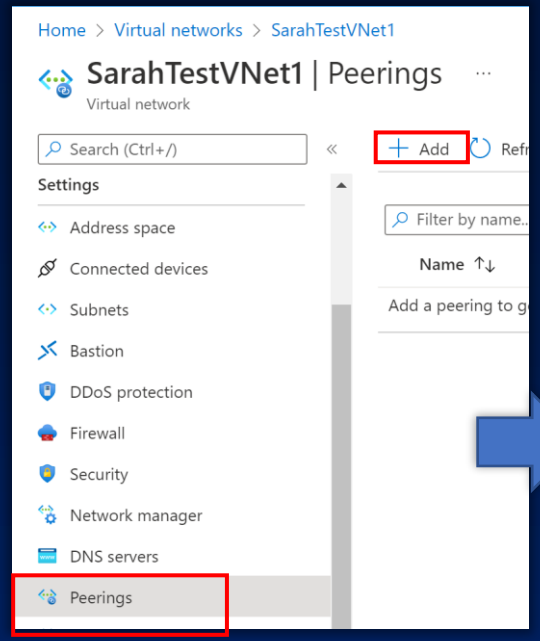
THCS

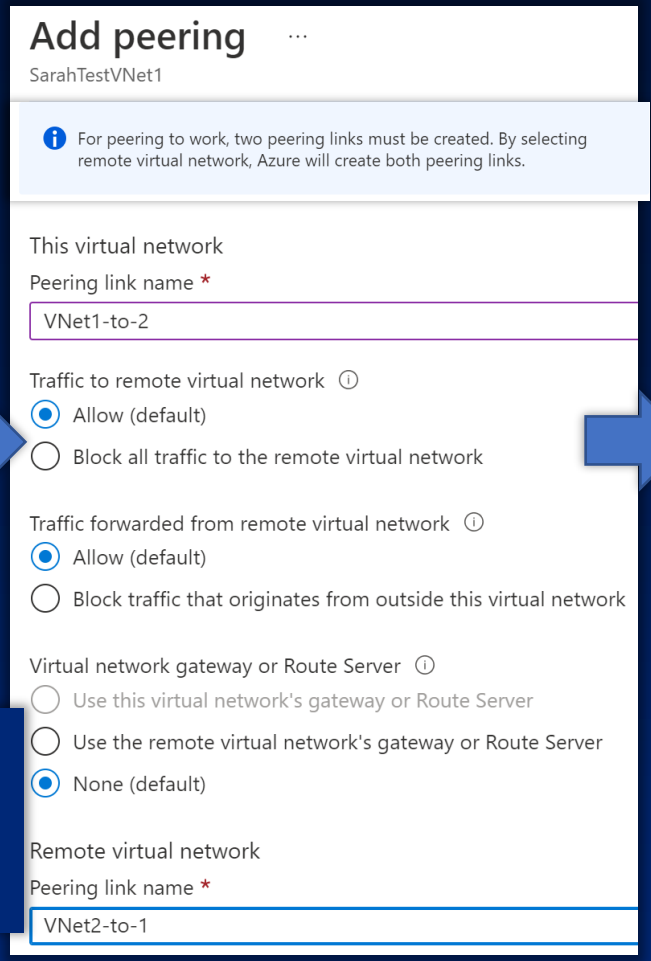
AZ-104

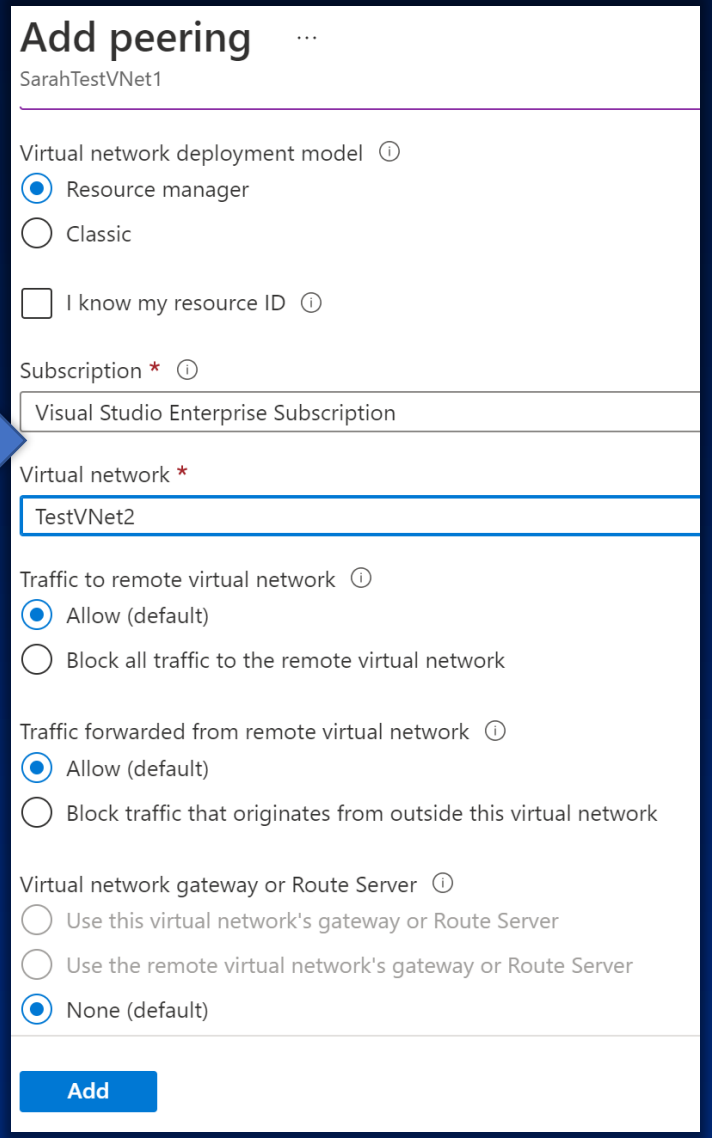
NETWORK

Intersite Connectivity

Microsoft CERTIFIED
AZURE ADMINISTRATOR
ASSOCIATE







Create once, get both (two-way) peering links

How to

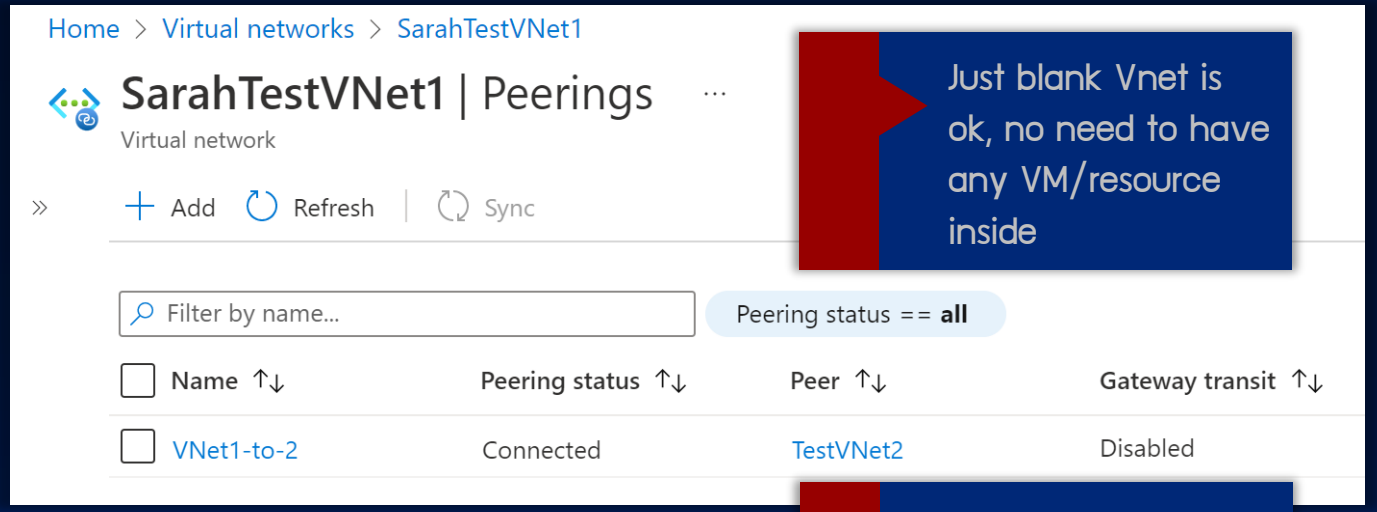
Peer VNet

THCS

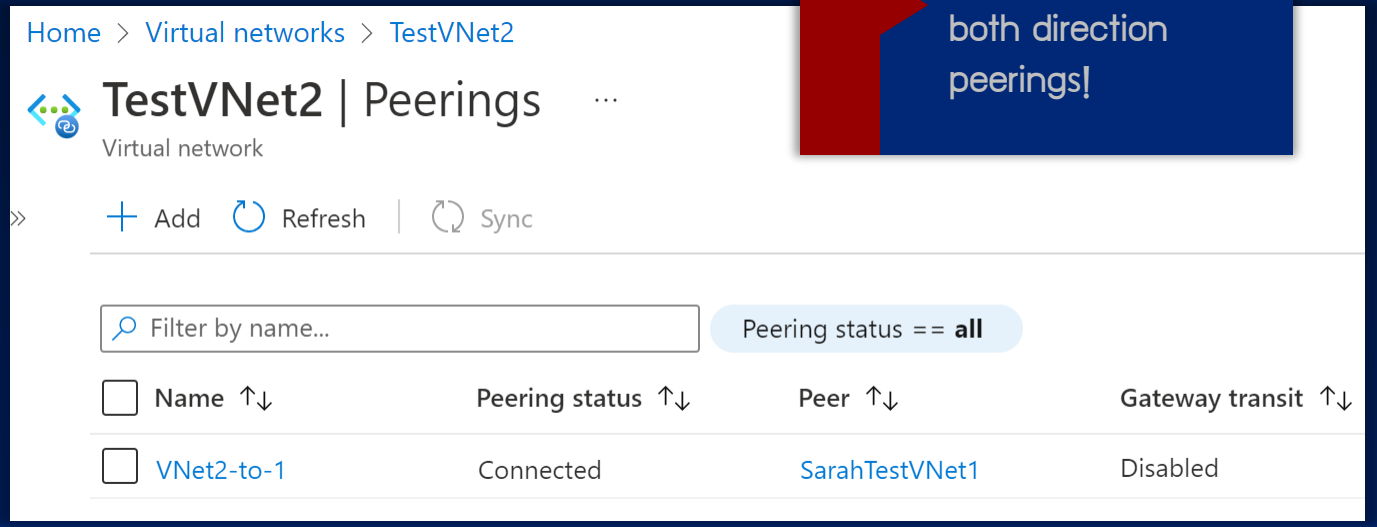
AZ-104

NETWORK

Intersite Connectivity



Just blank Vnet is ok, no need to have any VM/resource inside



Create once, get both direction peerings!

How to

Peer VNet

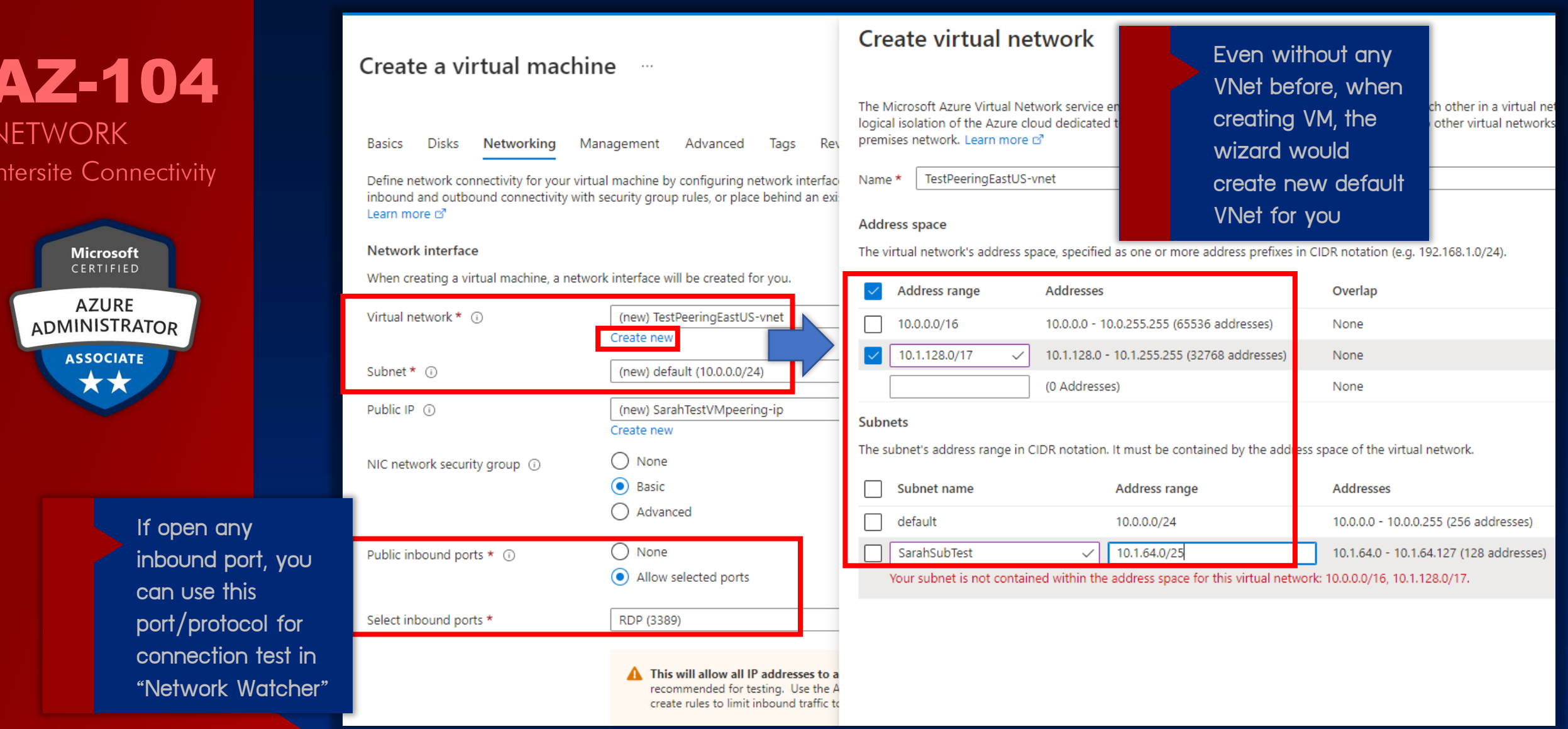
THCS

AZ-104

NETWORK

Intersite Connectivity

Microsoft CERTIFIED AZURE ADMINISTRATOR ASSOCIATE



Even without any VNet before, when creating VM, the wizard would create new default VNet for you

If open any inbound port, you can use this port/protocol for connection test in “Network Watcher”

How to

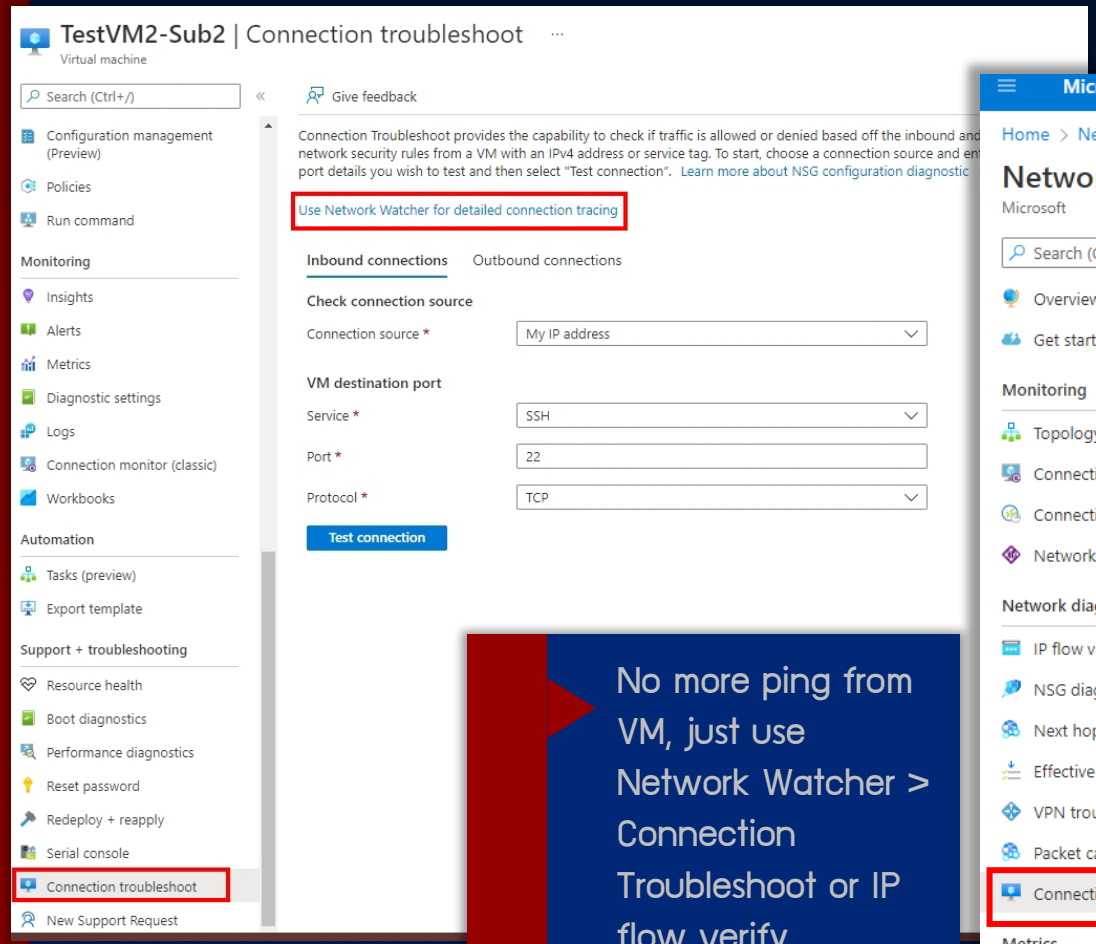
Peer VNet

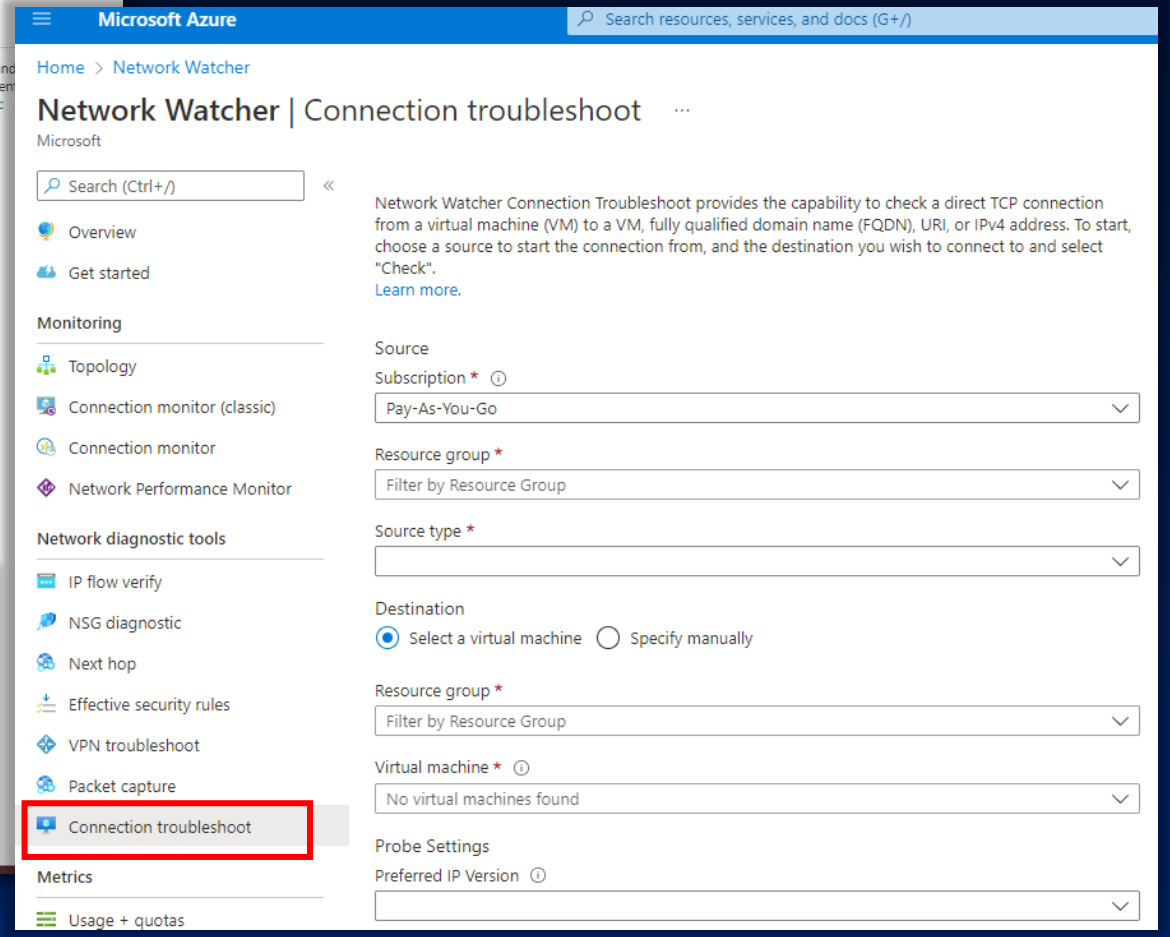
THCS

AZ-104

NETWORK

Intersite Connectivity





No more ping from VM, just use Network Watcher > Connection Troubleshoot or IP flow verify

Check Connection?

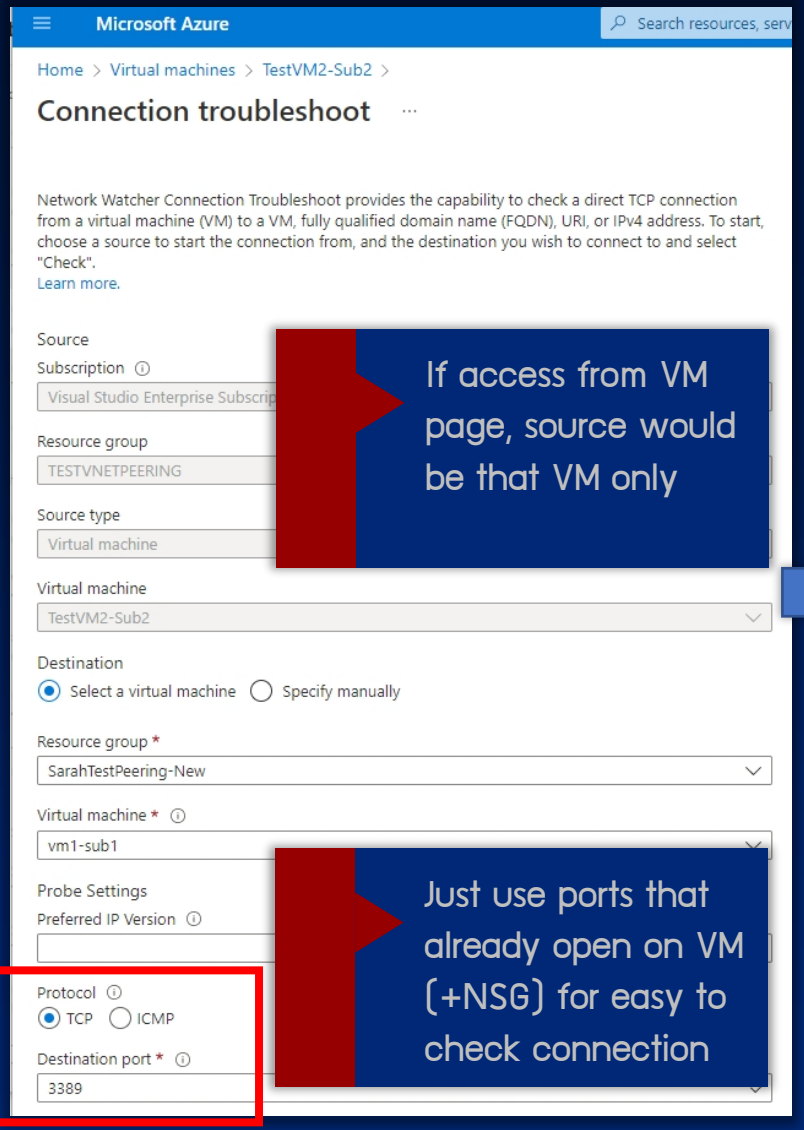
Use **Network Watcher**

THCS

AZ-104

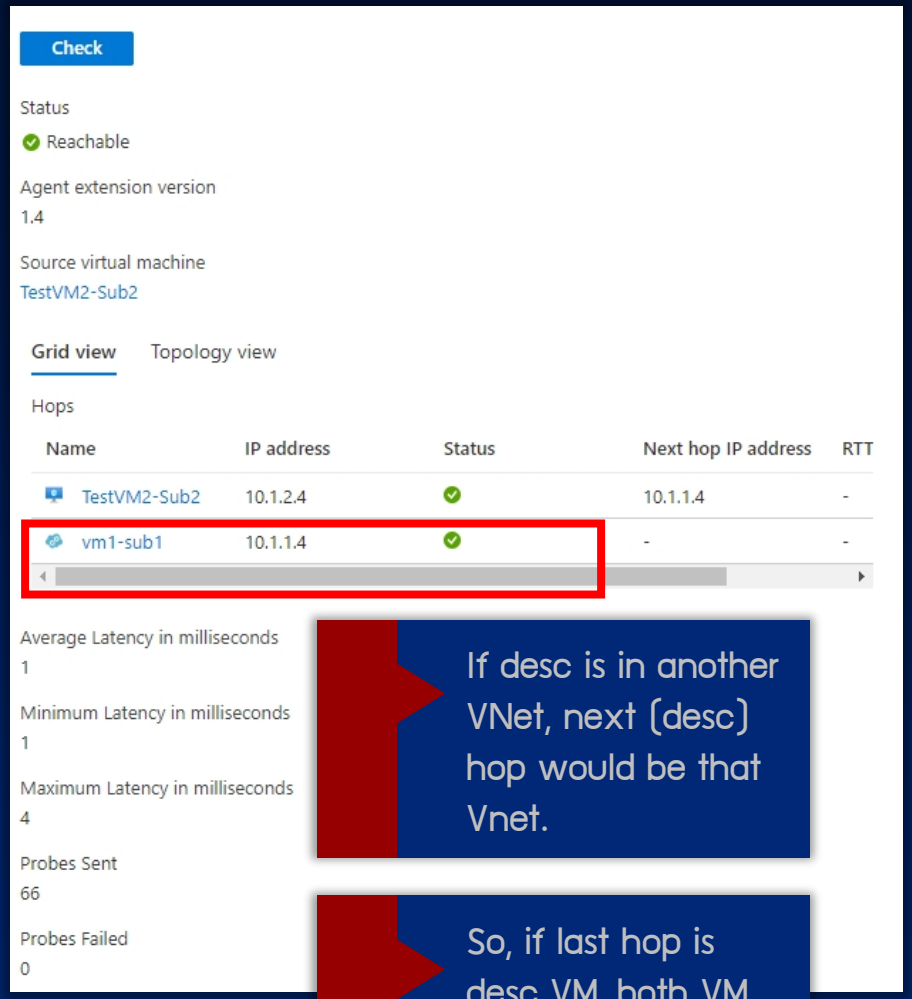
NETWORK

Intersite Connectivity



If access from VM page, source would be that VM only

Just use ports that already open on VM (+NSG) for easy to check connection



If desc is in another VNet, next (desc) hop would be that Vnet.

So, if last hop is desc VM, both VM should be in the same VNet

Check Connection?

Use **Network Watcher**

THCS

AZ-104

NETWORK

Intersite Connectivity

Yes! Now we can peer with VNet in different region with no any difference.

Except the “Price”, more expensive esp. regions in Aus/Asia zone (Zone 2)

azure.microsoft.com/en-us/pricing/details/virtu... Incognito

Virtual network peering

Virtual network peering links virtual networks, enabling you to route traffic between them using private IP addresses. Ingress and egress traffic is charged at both ends of the peered networks.

VNET Peering within the same region

Inbound data transfer	**$0.01** per GB
Outbound data transfer	**$0.01** per GB

Global VNET Peering

	Zone 1[1]	Zone 2[1]	Zone 3[1]	US Gov[1]
Inbound data transfer	**$0.035** per GB	**$0.09** per GB	**$0.16** per GB	**$0.044** per GB
Outbound data transfer	**$0.035** per GB	**$0.09** per GB	**$0.16** per GB	**$0.044** per GB

*Global VNET Peering pricing is based on a zonal structure. For instance, if data is being transferred from a VNET in zone 1 to a VNET in zone 2, customers will incur outbound data transfer rates for zone 1 and inbound data transfer rates for zone 2.

[1]Regions that correspond to Zone 1, Zone 2, Zone 3 and Gov can be found at this documentation.

The Virtual Network Peering charge applies to the traffic volume via the connectivity created by Azure Virtual Network Manager.

Across regions

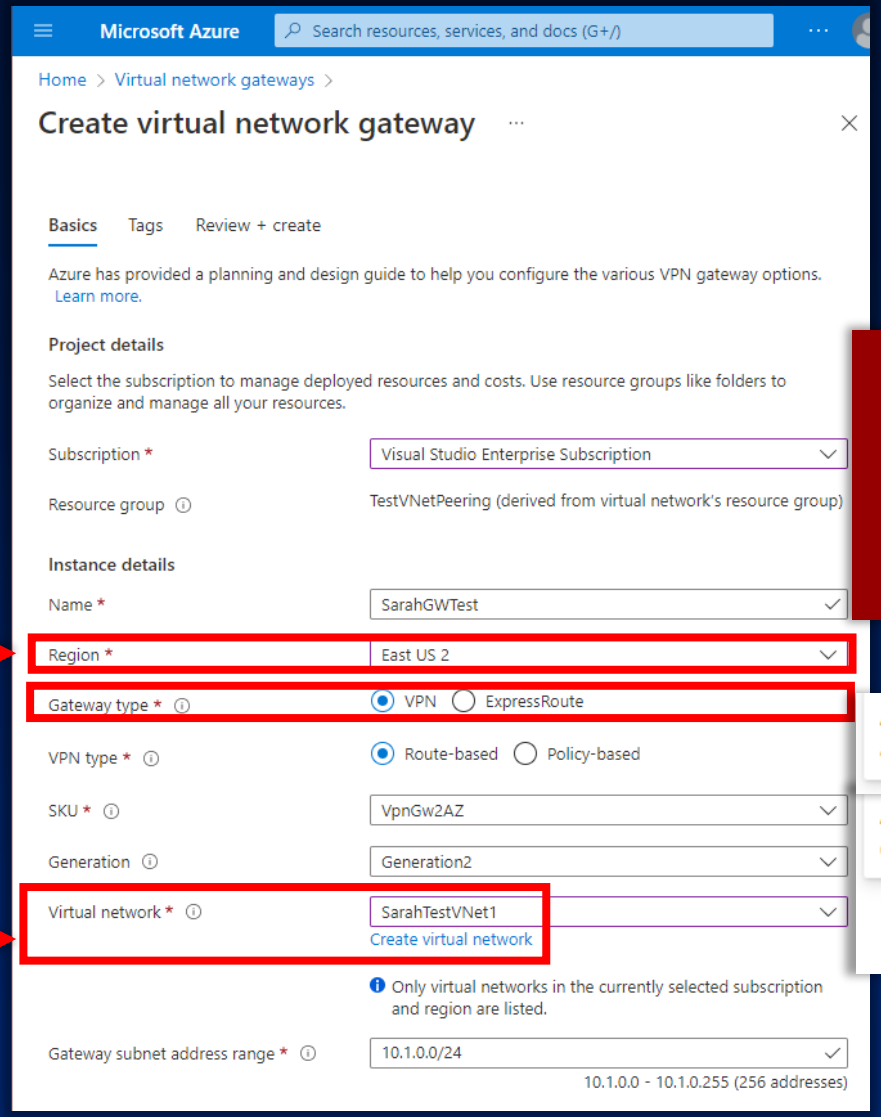
with “Global” Peering

THCS

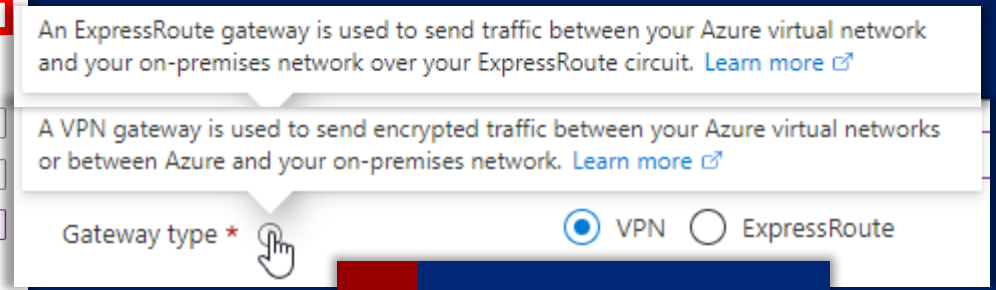
AZ-104

NETWORK

Intersite Connectivity



Choose Region that the VNet exists. (GW has to be in the same region as VNet, of course)



So you cannot create connection as over-internet VPN and private Expressroute circuit/link on the same gateway.

Many kinds

of VNet (VPN) Gateway

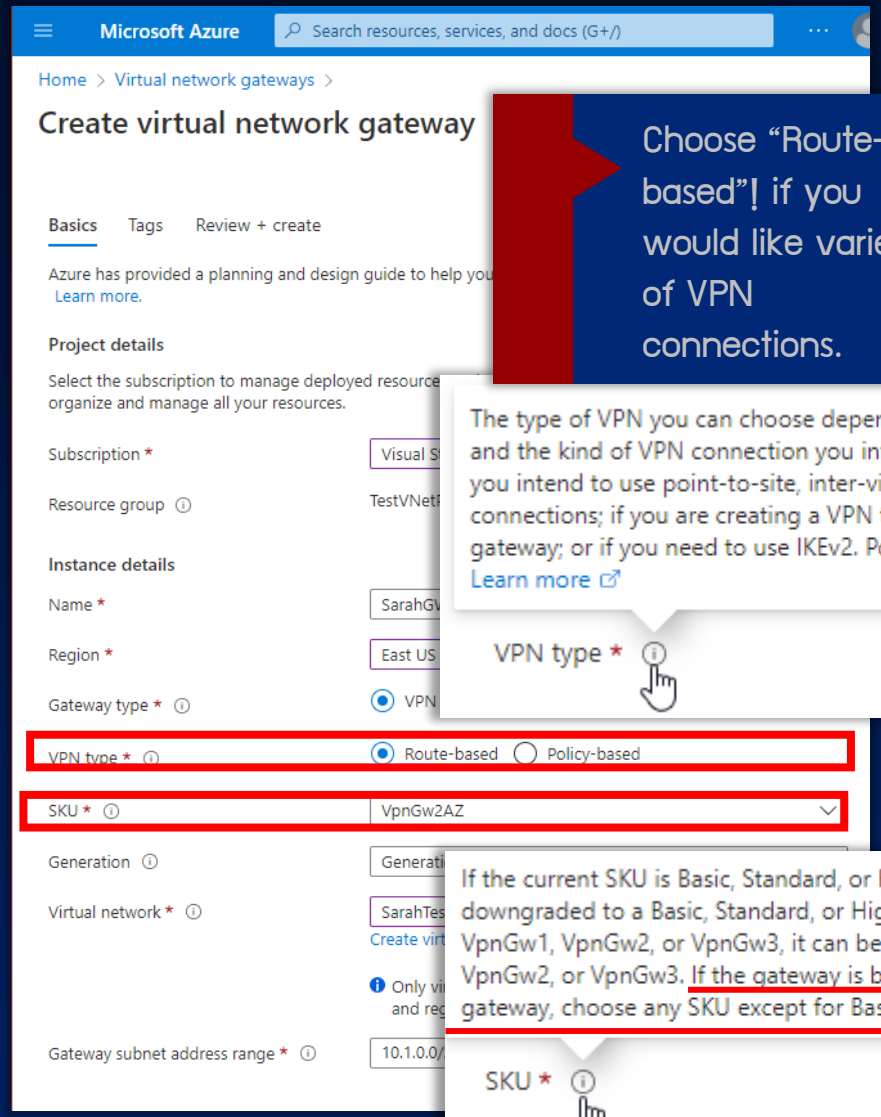
THCS

AZ-104

NETWORK

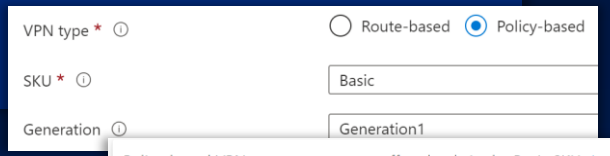
Intersite Connectivity

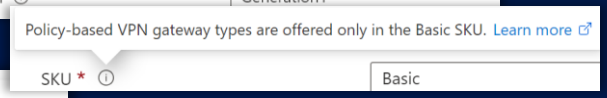
Microsoft CERTIFIED AZURE ADMINISTRATOR ASSOCIATE

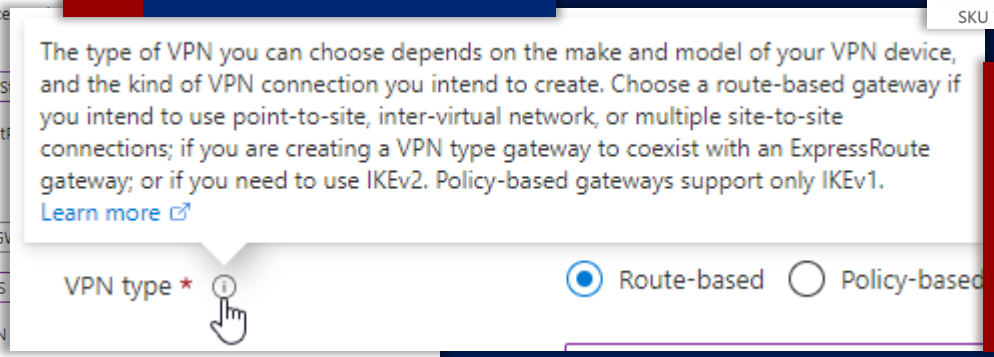


Choose "Route-based"! if you would like variety of VPN connections.

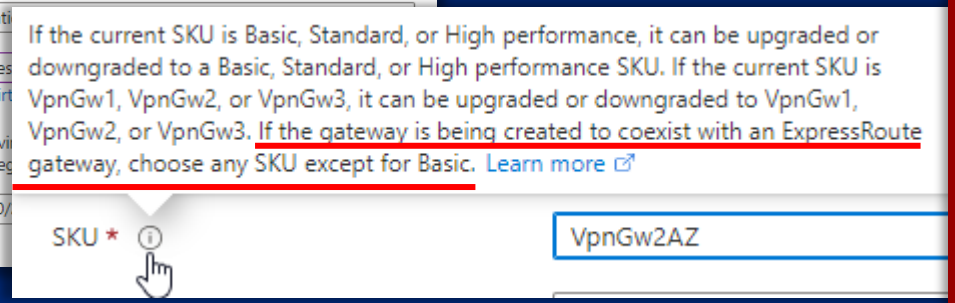
To use "Policy-based" ("Static" Traffic Selector), use Basic SKU with one S2S connection only.







Policy-based GW does not support P2S, multi S2S, failover with Expressroute, IKEv2.



So in most cases, please do not choose "Basic" SKU. Basic SKU do not support failover with Expressroute GW in the same GWsubnet

Policy-based = Static Routing (Table) = Add route (and encryption method) per prefix by your own

Route-based = Dynamic Routing (with protocol, but can use with static Routing Table also)

Many kinds of VNet (VPN) Gateway

THCS

AZ-104

NETWORK

Intersite Connectivity

Microsoft CERTIFIED

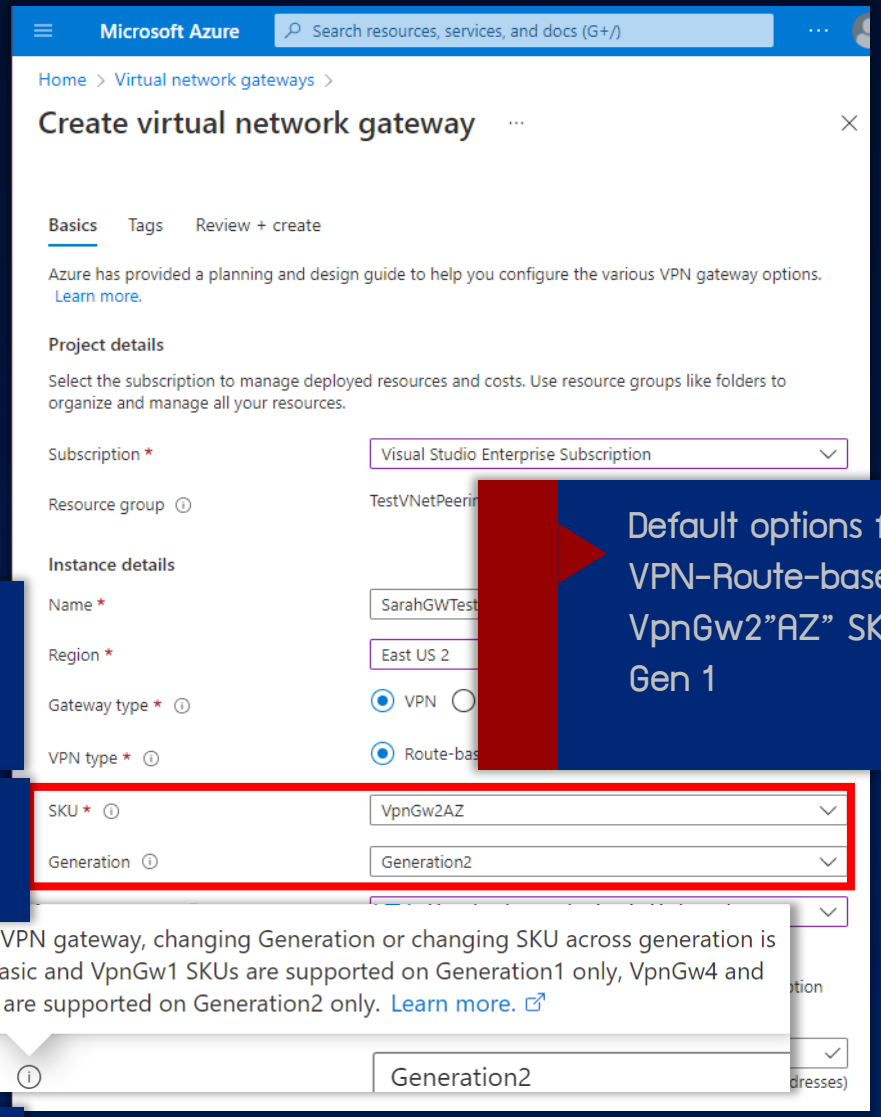
AZURE ADMINISTRATOR

ASSOCIATE

Gen 2 = Gen 1 + More Throughput (for VpnGw2, 3)

Basic and VpnGw1 are in Gen1 only

VpnGw4,5 are in Gen2 only, are top SKU that support max 100 S2S connections.



Default options for VPN-Route-based is VpnGw2"AZ" SKU - Gen 1

VPN Gateway Generation	SKU	S2S/VNet-to-VNet Tunnels	P2S SSTP Connections	P2S IKEv2/OpenVPN Connections	Aggregate Throughput Benchmark	BGP
Generation1	Basic	Max. 10	Max. 128	Not Supported	100 Mbps	Not Supported
Generation1	VpnGw1	Max. 30	Max. 128	Max. 250	650 Mbps	Supported
Generation1	VpnGw2	Max. 30	Max. 128	Max. 500	1 Gbps	Supported
Generation1	VpnGw3	Max. 30	Max. 128	Max. 1000	1.25 Gbps	Supported
Generation1	VpnGw1AZ	Max. 30	Max. 128	Max. 250	650 Mbps	Supported
ration1	VpnGw2AZ	Max. 30	Max. 128	Max. 500	1 Gbps	Supported
ration1	VpnGw3AZ	Max. 30	Max. 128	Max. 1000	1.25 Gbps	Supported
ration2	VpnGw2	Max. 30	Max. 128	Max. 500	1.25 Gbps	Supported
ration2	VpnGw3	Max. 30	Max. 128	Max. 1000	2.5 Gbps	Supported
Generation2	VpnGw4	Max. 100*	Max. 128	Max. 5000	5 Gbps	Supported
Generation2	VpnGw5	Max. 100*	Max. 128	Max. 10000	10 Gbps	Supported
Generation2	VpnGw2AZ	Max. 30	Max. 128	Max. 500	1.25 Gbps	Supported
Generation2	VpnGw3AZ	Max. 30	Max. 128	Max. 1000	2.5 Gbps	Supported
Generation2	VpnGw4AZ	Max. 100*	Max. 128	Max. 5000	5 Gbps	Supported
Generation2	VpnGw5AZ	Max. 100*	Max. 128	Max. 10000	10 Gbps	Supported

Many kinds of VNet (VPN) Gateway

If you wish for more than 100 S2S tunnels, use Virtual WAN

THCS

AZ-104

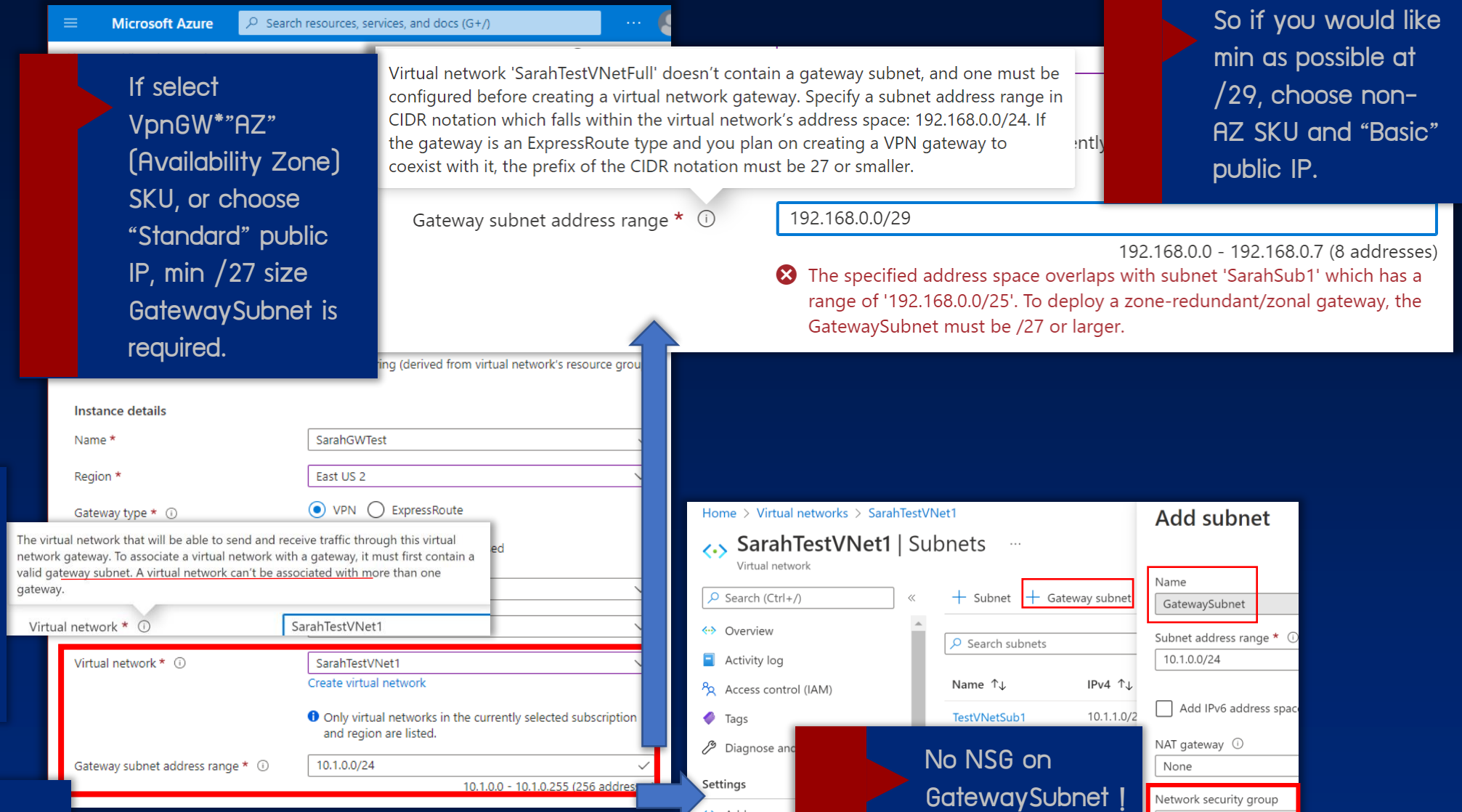
NETWORK

Intersite Connectivity

Microsoft CERTIFIED AZURE ADMINISTRATOR ASSOCIATE

One GW "per Type!" VpnGW and ExpressRoute GW can be coexists (for failover) in the same Vnet.

If select VpnGW*"AZ" (Availability Zone) SKU, or choose "Standard" public IP, min /27 size GatewaySubnet is required.



So if you would like min as possible at /29, choose non-AZ SKU and "Basic" public IP.

No NSG on GatewaySubnet !

If no any GatewaySubnet before, this wizard will let you create new one now.

You can create GatewaySubnet beforehand in Vnet page. Note that subnet name must be "GatewaySubnet"

Many kinds of VNet (VPN) Gateway

THCS

AZ-104

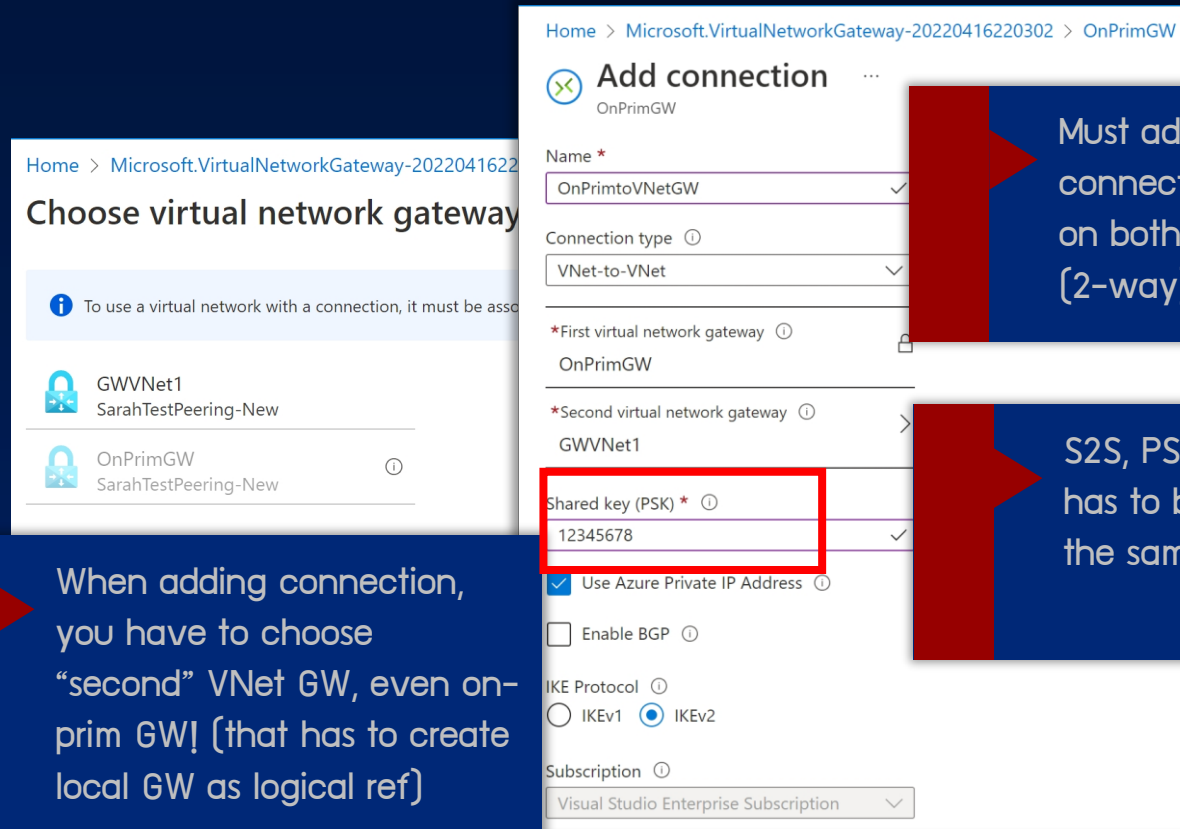
NETWORK

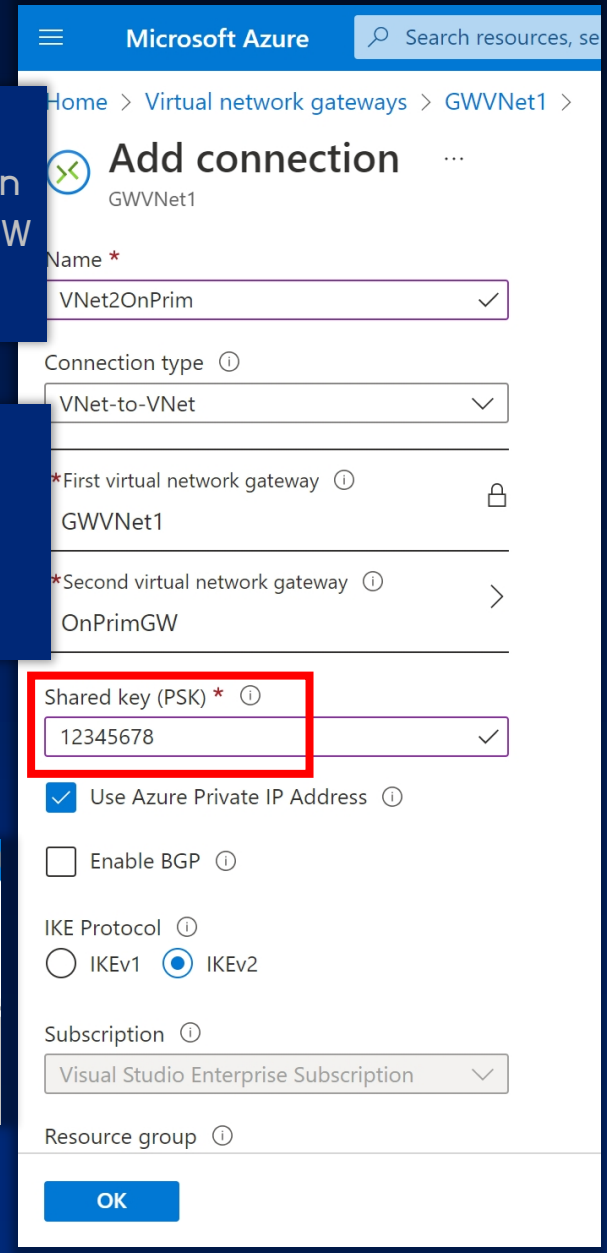
Intersite Connectivity

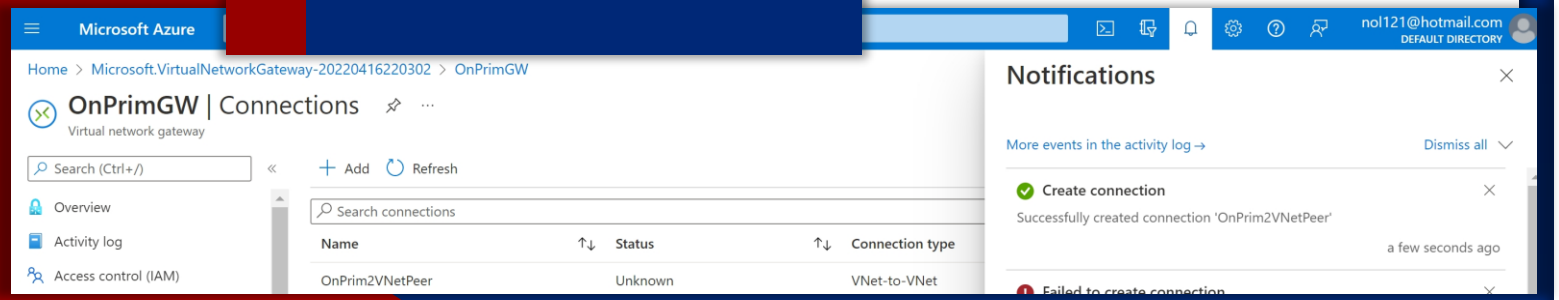
Microsoft CERTIFIED

AZURE ADMINISTRATOR

ASSOCIATE







Create **VNet-to-VNet**

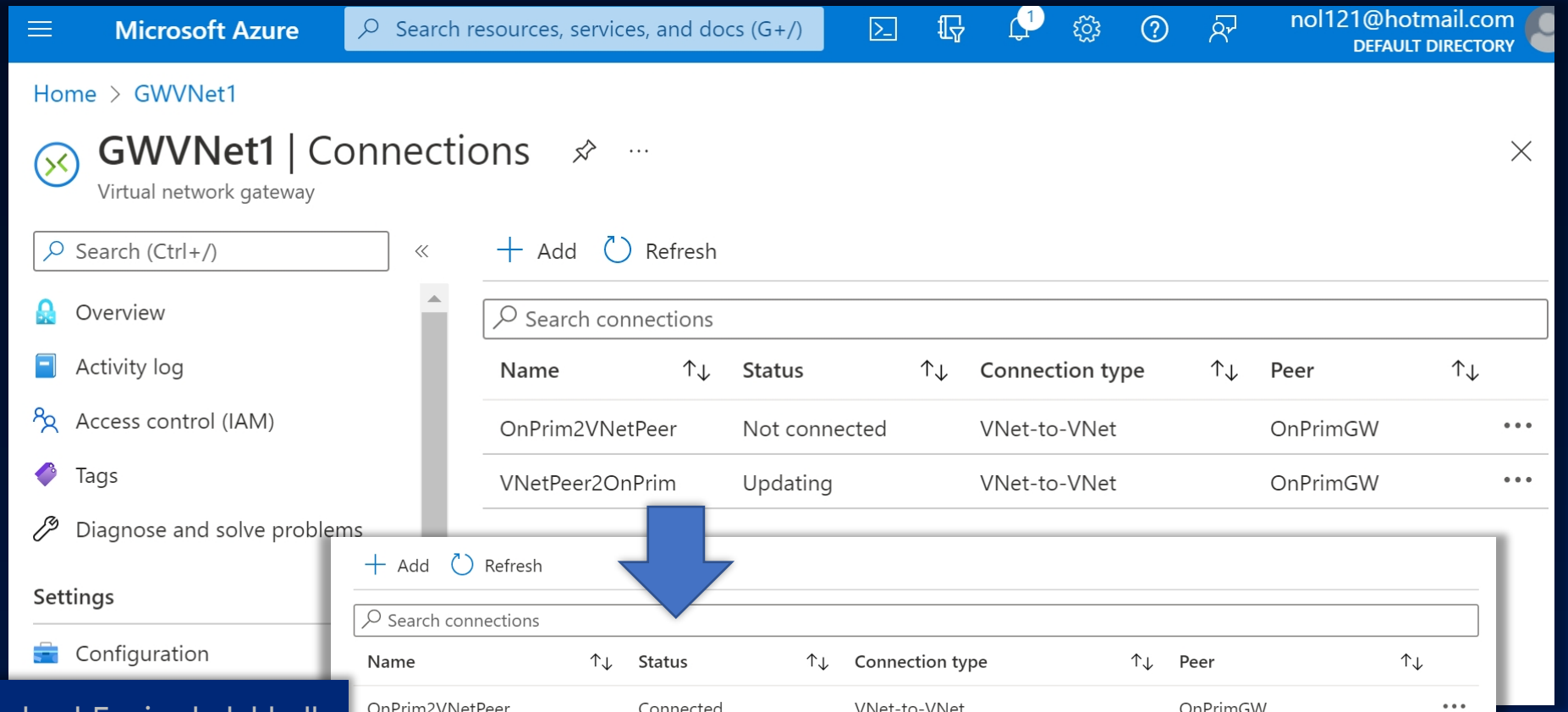
or S2S connection

THCS

AZ-104

NETWORK

Intersite Connectivity



Wait about 5 mins to let both connections sync and show status as “Connected” in the end.

Create VNet-to-VNet

or S2S connection

THCS

AZ-104

NETWORK

Intersite Connectivity

Home > Virtual machines > OnPrimTest >

Connection troubleshoot ...

Status

Reachable

Agent extension version

1.4

Source virtual machine

OnPrimTest

Grid view | Topology view

Hops

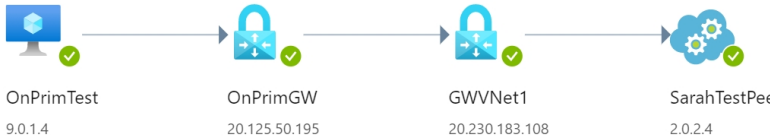
Name	IP address	Status	Next hop IP address	RTT
OnPrimTest	9.0.1.4	✓	20.125.50.195	-
OnPrimGW	20.125.50.195	✓	20.230.183.108	-
GWVNet1	20.230.183.108	✓	2.0.2.4	-
SarahTestPeerV...	2.0.2.4	✓		

Home > Virtual machines > OnPrimTest >

Connection troubleshoot ...

Grid view | Topology view

Note that VPN Gateway use Public IP as next hop, even in VNet-to-VNet



See each hop as GW > GW > Desc. VNet

Create **VNet-to-VNet**

or S2S connection

THCS

AZ-104

NETWORK

Intersite Connectivity

Microsoft CERTIFIED AZURE ADMINISTRATOR ASSOCIATE

Home > Microsoft.VirtualNetworkGateway-20220430055453 > SarahTestVNetGW

SarahTestVNetGW | Point-to-site configuration

Virtual network gateway

Search (Ctrl+/)

Save Discard Delete Download VPN client

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Configuration
- Connections
- Point-to-site configuration
- Properties
- Locks

Monitoring

- Logs
- Alerts
- Metrics
- BGP peers

Automation

Address pool *: 10.0.0.0/24

Tunnel type: OpenVPN (SSL)

Authentication type: 3 selected

- Azure certificate
- RADIUS authentication
- Azure Active Directory

Public IP address * ⓘ

Create new / Use existing

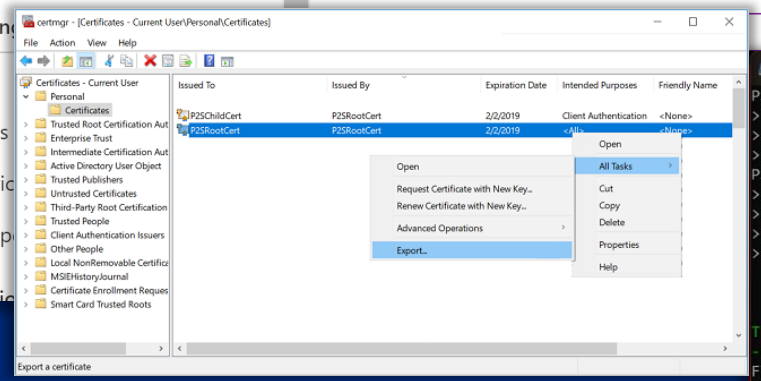
Root certificates

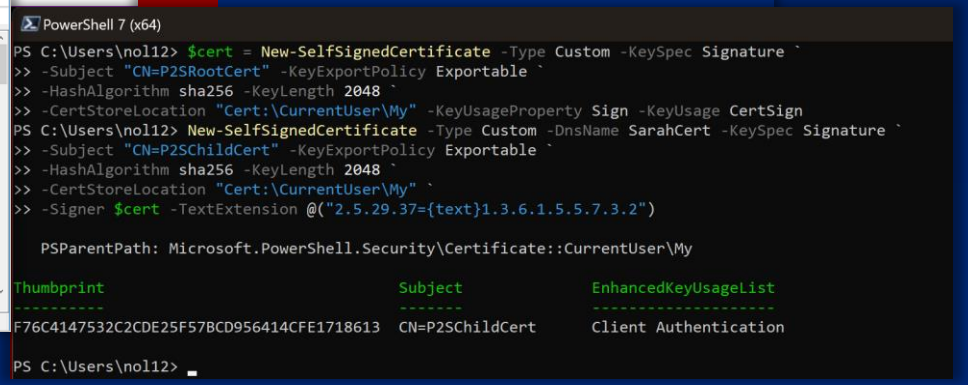
Name	Public certificate data

Revoked certificates

Name	Thumbprint

In case using cert, you must generate root certificate (of course, with private from device first and then copy to this field.





Create P2S

Connection with Config Package

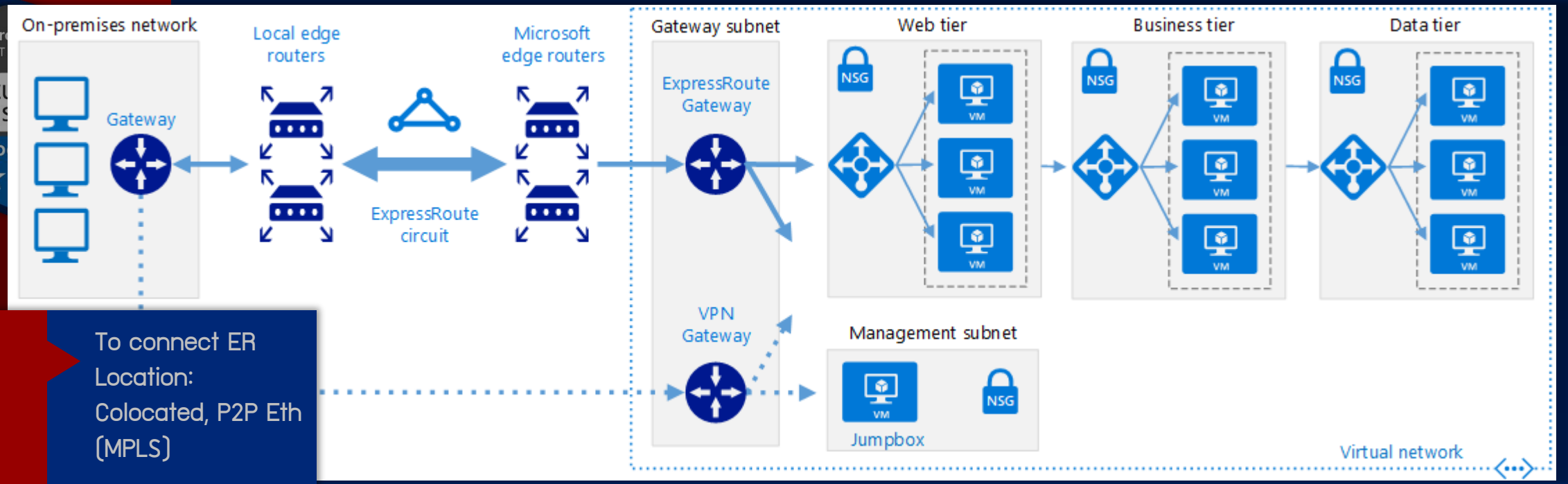
THCS

AZ-104

NETWORK

Intersite Connectivity

Each circuit has two (active/ active) channels, each for each MSEE (MS Router.)



To connect ER Location: Colocated, P2P Eth (MPLS)

ExpressRoute (ER)

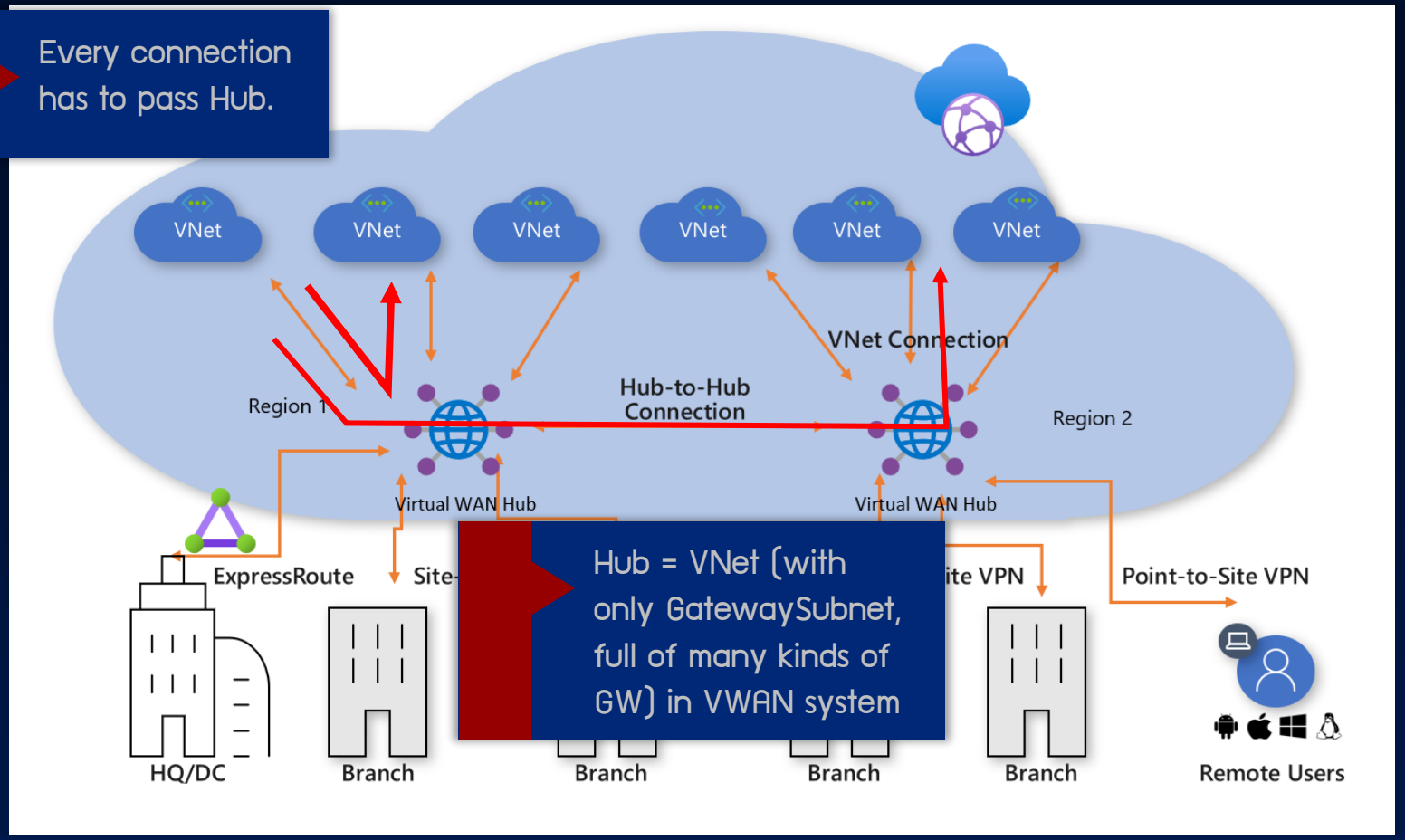
With S2S as backup

AZ-104

NETWORK

Intersite Connectivity

Every connection has to pass Hub.



Hub = VNet (with only GatewaySubnet, full of many kinds of GW) in VWAN system

One Virtual WAN

With many Virtual Hubs

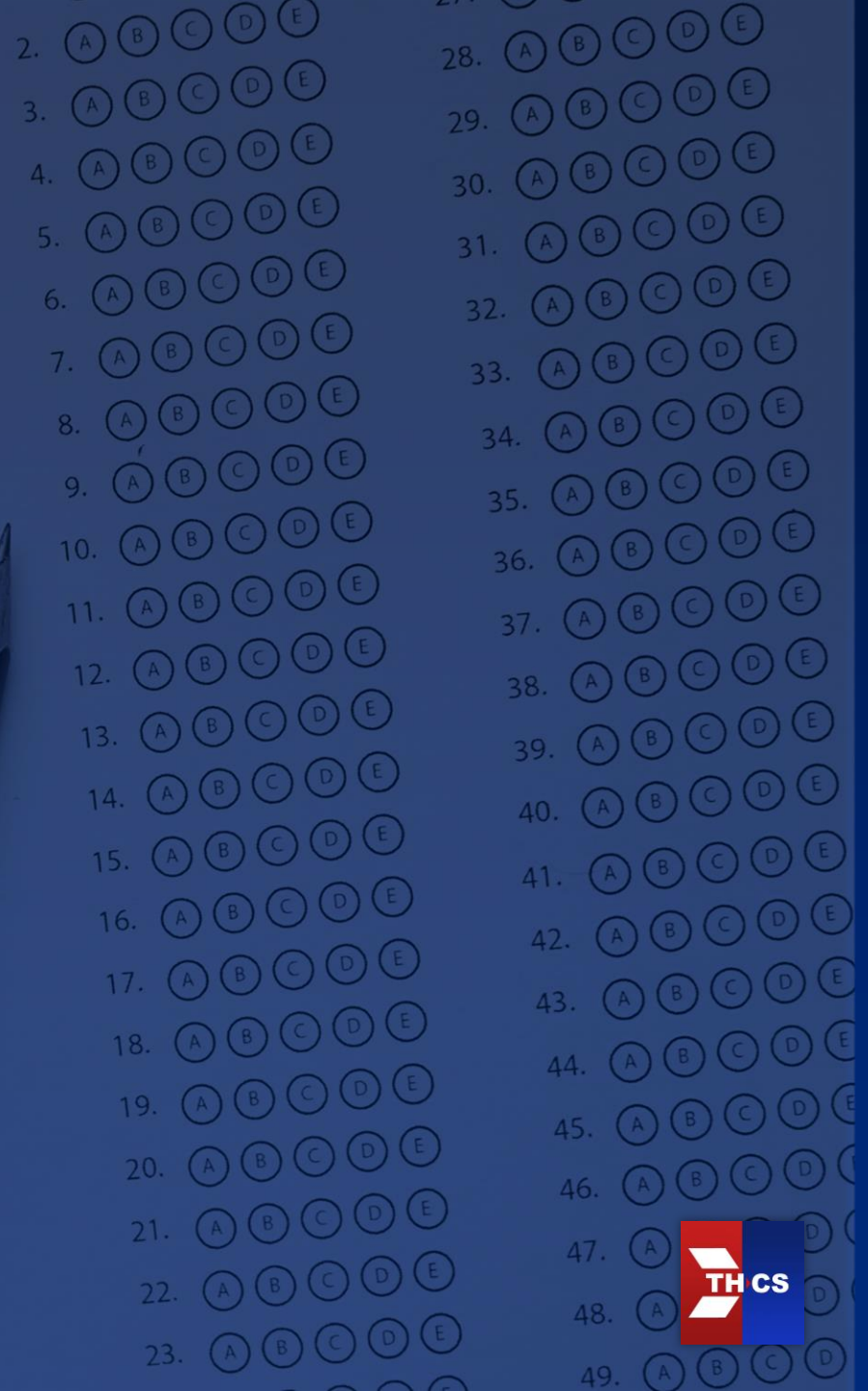
THCS

AZ-104

NETWORK

Intersite Connectivity

Example Questions

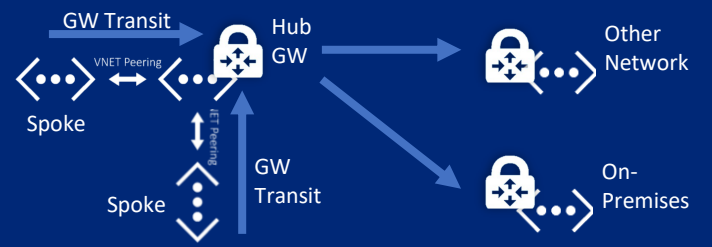


AZ-104

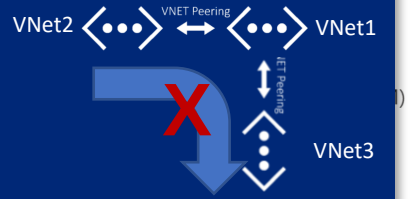
NETWORK

Intersite Connectivity

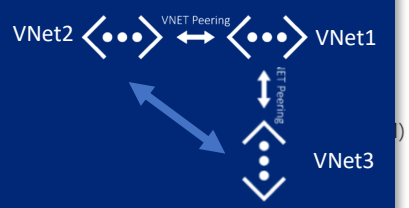
Gateway Transit ไม่เกี่ยว ไม่ใช่การทำ Transitive ถึง จะ Enable ก็แค่ให้ทราฟิกที่ Peer ไหลออก Hub ที่มีเกตเวย์ยิงข้ามไปเกตเวย์ที่ Net/OnPrim อื่นเท่านั้น



Peer ไม่ Transitive (ไม่โดดข้าม Vnet)



ถ้าอยากคุยกันได้ มีวิธีเดียวคือ Peer เพิ่ม



From SarahTestPeer**VNet1**, packets can be routed to:

A. SarahTestPeerVNet2 only
B. SarahTestPeerVNet3 only
C. SarahTestPeerVNet2 and 3

From SarahTestPeerVNET2, packets can be routed to:

A. SarahTestPeerVNet1 only
B. SarahTestPeerVNet3 only
C. SarahTestPeerVNet1 and 3

THCS

AZ-104

NETWORK

Intersite Connectivity

VNet1 can be peered with?

Peer ได้ ไอพี (Address Space/Prefix) ต้องไม่ทับกัน (Overlapped) เช่น ถ้า /16 (สองไบต์แรก) ก็ต้องไม่ทับกับ /16+ ของVNet อื่น

Name	Address Space	Subnet	Region
VNet1	10.0.0.0/16	10.0.1.0/24	East US
VNet2	10.0.128.0/17	10.0.192.0/24	West US2
VNet3	192.168.0.0/16	192.168.2.0/24	East US
VNet4	192.169.0.0/17	192.169.2.0/24	Southeast Asia

A. VNet2,3,4
B. VNet3,4
C. VNet4
D. VNet2,4

เค้า Peer ข้ามรีเจี้ยนกัน (Global Peering) กันได้แล้ว ไม่ได้ถูกจำกัดแค่ต้องรีเจี้ยนเดียวกันอีก

ดังนั้น Region ไม่เกี่ยว

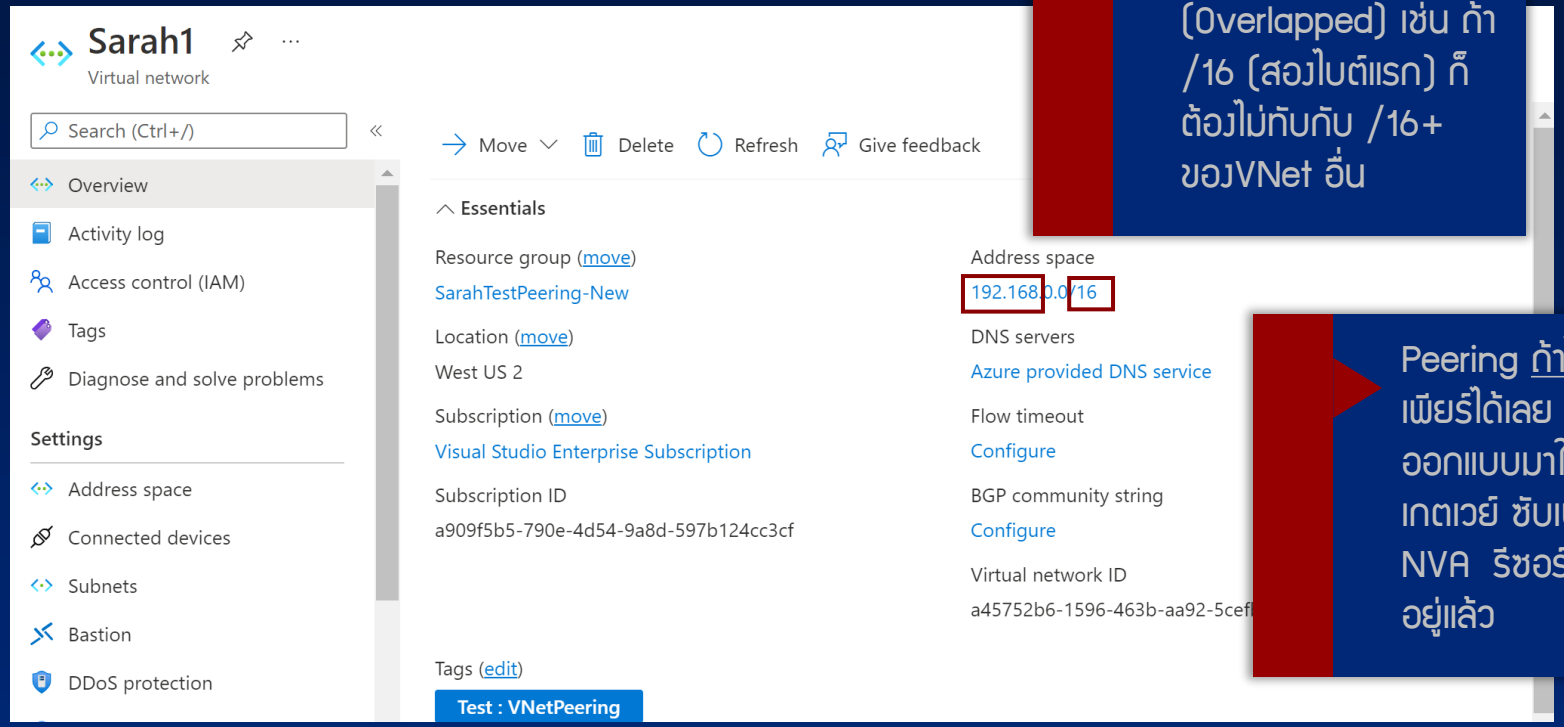
THCS

AZ-104

NETWORK

Intersite Connectivity

VNet “Sarah1” has no any VM or resource.



Peer ได้ ไอพี (Address Space) ต้องไม่ทับกัน (Overlapped) เช่น ถ้า /16 (สองไบต์แรก) ก็ต้องไม่ทับกับ /16+ ของVNet อื่น

Peering ถ้าไอพีไม่ทับ เพียร์ได้เลย เป็นระบบที่ออกแบบมาให้ไม่ต้องพึ่งเกตเวย์ ซับเน็ต หรือใส่ NVA รีซอร์สอะไรก่อนอยู่แล้ว

If you would like to peer this with Vnet “Sarah2” that has address space as “192.168.128.0/17”, what do you have to do first?

A. Add VM or any resource
B. Be sure that two VNets are in the same region
C. Change address space of Sarah1
D. Add gateways
E. Create service endpoint
F. Create subnets that are not overlapped
G. Nothing to do, just peer

THCS

AZ-104

NETWORK

Intersite Connectivity

From this info:

VNet	Address Space	Subnet	Peered with
Sarah1	10.0.0.0/16	10.0.1.0/24 10.0.2.0/24	Sarah2
Sarah2	10.1.128.0/17	10.1.192.0/24	Sarah1

Peering ถ้าไอพีไม่ทับ เพียร์ได้เลย เป็นระบบที่ออกแบบมาให้ไม่ต้องพึ่งเกตเวย์ ซับเน็ต หรือใส่ NVA รีซอร์สอะไรก่อนอยู่แล้ว

If we would like to add address space: 10.2.0.0/16 to Sarah1, which 3 steps from these instructions you should do respectively:

A. Delete Sarah1
B. Create new Sarah1
C. Modify Address Space, adding 10.2.0.0/16
D. Remove Peering
E. Recreate Peering
F. Allow Gateway transit
G. Create Gateway subnet
H. Create VPN Gateway
I. Create Gateway Connection

Step1: D. Remove Peering

Step2: C. Modify Address Space, adding 10.2.0.0/16

Step3: E. Recreate Peering

ถ้าสร้าง Peer แล้ว จะล็อกไม่ให้เพิ่มหรือแก้ Address Space (เหมือนเอาไปเขียนตารางเราท์แล้ว) ดังนั้นต้องลบเพียร์ก่อนถึงแก้ได้

THCS

AZ-104

NETWORK

Intersite Connectivity

VPN Gateway

Subscription: Sarah1, has VNets/Subnets as follows:

VNet	Address Space	Location
VNet1	10.0.0.0/16	WestUS2
VNet2	172.168.128.0/17	SEA

Subnet	Address Space	in VNet
Sub11	10.0.0.0/17	VNet1
Sub12	10.0.128.0/17	VNet1
Sub21	172.168.128.0/24	VNet2
Sub22	172.168.192.0/24	VNet2

Subscription: Sarah2, has VNet:

- name: VNet3
- Address Space: 10.2.0.0/16
- Location: Japan East
- has subnets as follows:

Subnet	Address Space
Sub31	10.2.1.0/24
Sub32	10.2.2.0/24

Gateway ต้องมีซับเน็ตของตัวเองแยกต่างหาก ถ้า VNet ไหนไม่เหลือ Space ไอพีให้สร้างซับเน็ตเพิ่ม (อย่างต่ำ /29) ก็สร้างเกตเวย์ไม่ได้

VNet1 and 3 can established Site-to-Site VPN? Yes **No**

VNet1 and 2 can be peered? **Yes** No

VNet2 and 3 can be peered? **Yes** No

THCS

AZ-104

NETWORK

Intersite Connectivity

VPN Gateway

There are two subscriptions: Sarah1 and Sarah2

In Sarah1, there are VNet1. In VNet1, there are VM1 and Subnet1 (10.0.1.128/25.) VNet1 address space is 10.0.1.0/24.

In Sarah2, there are VNet2. In VNet2, there are VM2 and Subnet2 (10.0.2.128/25.) VNet1 address space is 10.0.2.0/24.

What should you do first to connect VNet1 and 2?

A. Add more subnets
B. Provision Gateway only in VNet1
C. Provision Gateways for each VNet
D. Modify address space of VNet1 or 2
E. Move VNet into the same subscription

ไม่ว่าจะเพียร์หรือเชื่อมผ่านเกตเวย์ ไอพีสเปซในทั้งสอง VNet ก็ต้องไม่โอเวอร์แลปกัน (ตอนนี้ VPN Gateway ยังทำ NAT ไม่ได้)

ถ้าไอพีไม่โอเวอร์แลป ถ้าจะเชื่อมกันง่ายสุดคือทำเพียริ่ง แต่ถ้าชอยส์ไม่มีก็คือสร้าง VNet (VPN) Gateway แบบ VNet-to-Vnet

VPN แบบ VNet-to-VNet ก็คือ S2S อย่างนึง ดังนั้นต้องมีเกตเวย์ที่แต่ละไซต์/VNet ด้วย ต่างฝ่ายต่างสร้างคอนเนคชั่นไปอีกฟั่ง

THCS

AZ-104

NETWORK

Intersite Connectivity

VPN Gateway

In VNet Sarah1, there is policy-based gateway called GW1. If we want on-premises computers to connect to Sarah1 via Point-to-Site connection, which first two steps we have to do?

A. Create gateway at on-premises/local site network
B. Create the connections
C. Install VPN agents on computers
D. Delete GW1
E. Create virtual firewall
F. Recreate GW1 as route-based VPN gateway
G. Reset GW1
H. Create public IP address space in Sarah1

Policy-based ไม่รองรับ Point-to-Site (ได้แต่ S2S) และเปลี่ยนทีหลังไม่ได้ จึงต้องลบและสร้าง Gateway ใหม่เป็นแบบ Route-based ปกติ

THCS

AZ-104

NETWORK

Intersite Connectivity

VPN Gateway

Which first 4 steps to create site-to-site VPN to Vnet Sarah1 in Azure that has address space 192.168.0.0/16 and one subnet 192.168.2.0/24?

A. Create VPN Gateway
B. Create Connections
C. Create Load Balancer
D. Create Proxy Server
E. Create GatewaySubnet
F. Create VM
G. Create at least two subnets
H. Create local gateway
I. Create DNS server
J. Create CDN profile

Step1: E. Create GatewaySubnet

Step2: A. Create VPN Gateway

Step3: H. Create local gateway

Step4: B. Create connections

ปกติ ถ้าแอดเดรสสเปซเหลือ แล้วเรากดสร้าง VPN Gateway สำหรับ VNet นั้น โดยยังไม่มี GatewaySubnet ก่อนหน้า ก็จะสร้างให้อัตโนมัติ

Site-to-Site เราก็ต้องสร้างเกตเวย์ทั้งสองฝั่งเพื่อสร้าง Connection หากัน

THCS

AZ-104

NETWORK

Intersite Connectivity

VPN Gateway

We want to connect on-premises Silom office network to VNet Sarah1 in Azure cloud as encrypted connection over the internet, So what should we do in the cloud portal and on-premises site?

Portal:

A. Create policy-based gateway
B. Create Expressroute gateway/circuit
C. Establish virtual Firewall
D. Create route-based Virtual Network gateway and local network gateway
E. Create Expressroute circuit and on-premises data gateway

On-premises:

A. Install VPN configuration client package on all clients
B. Deploy Expressroute
C. Deploy DirectAccess server
D. Configure Site-to-Site VPN connection
E. Implement Proxy server

Expressroute เป็นลิงค์ส่วนตัว ไม่ได้ over internet จึงตัดออกไปได้เลย

Office to VNet คือ Site-to-Site เราก็ต้องสร้างเกตเวย์ทั้งสองฝั่งเพื่อสร้าง Connection หากัน

THCS

AZ-104

NETWORK

Intersite Connectivity

Expressroute

VNet Sarah1 connects to on-premises with Azure Expressroute. If we would like to create the backup connection as automatic failover site-to-site VPN, which three actions should you do, as to reduce cost as possible?

A. Create gateway at on-premises/local network
B. Create a connection
C. Install VPN agents on computers
D. Create VPN Gateway with VpnGw2 sku
E. Create VPN Gateway with Basic sku
F. Create Gateway subnet
G. Reset Expressroute
H. Create public IP address space in Sarah1

Basic sku ไม่รองรับทำ Failover คู่กับ Expressroute จึงต้องเลือกตั้งแต่ VpnGw1 ขึ้นไป

Gateway Expressroute ใช้ GatewaySubnet เดียวกับ VPN Gateway ที่ทำ Failover จึงไม่ต้องสร้างซับเน็ตเพิ่ม

ขั้นตอนการทำ Site-to-Site ก็แค่สร้าง Gateway ทั้งสองฝั่ง แล้วแต่ละฝั่งสร้าง Connection หากัน (ตั้ง Key ให้ตรงกัน)

THCS

AZ-104

NETWORK

Intersite Connectivity

Virtual WAN

3 offices: NY, LA, Seattle, all has their own datacenter. We also have VNet in each region: East and West US. Both VNets are peered. Which solution can connect all with least latency?

A. Use CDN with Application Proxy
B. Use 3 Virtual WANs and one Virtual Hub
C. Use Site-to-Site VPN Gateways
D. Use Peering for all connections
E. Use 3 Virtual Hubs in one Virtual WAN

เรามักเช่าเซอร์วิส Virtual WAN เดียว ในนั้นจะสร้างกี่ Hub ก็ได้ ข้ามรีเจี้ยนกันได้

THCS