

A graphic element on the left side of the slide features a stylized map of Thailand. The map is composed of several overlapping triangles in shades of red, blue, and grey, creating a layered effect. The word "THAILAND" is overlaid on this graphic in large, white, sans-serif capital letters.

THAILAND

Cyber  
Security



 Microsoft Security

# Cloud SECURITY Intensive





# Network Security

Security Group 

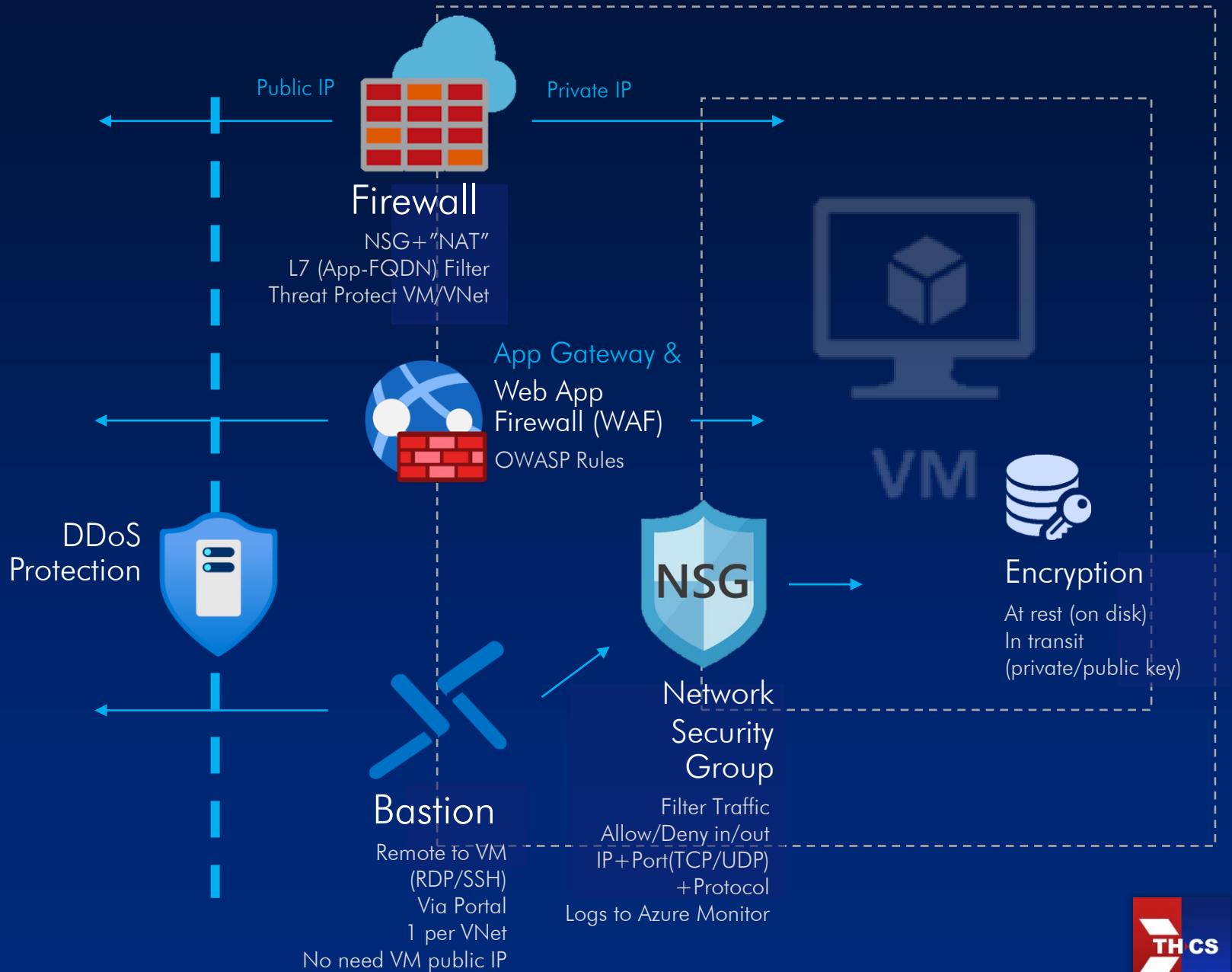
Virtual Network 

Bastion Host 



# SC-900

SECURITY  
COMPLIANCE  
IDENTITY



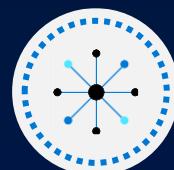
# AZ-104

NETWORK

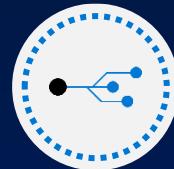
Module 4



Administer  
Virtual Network



01: Virtual Networks



02: Network Security Groups



03: Azure Firewall



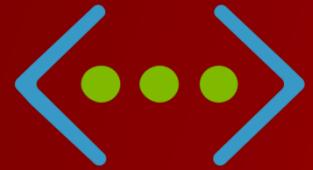
04: Azure DNS



05: Example Question

# AZ-104

## NETWORK



Virtual Networks



Plan Virtual Networks



Create Subnets



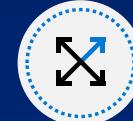
Create Virtual Networks



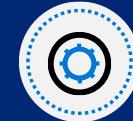
Plan IP Addressing



Create Public IP Addresses



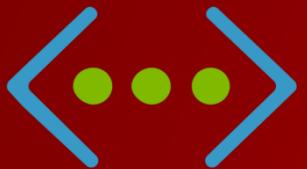
Associate Public IP Addresses



Associate Private IP Addresses

# AZ-104

NETWORK  
Virtual Networks



## Virtual Network

### Subnet



### Virtual Machines

On-premises

Virtual Network(s)

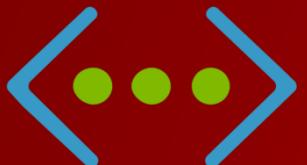
Logical representation  
of your own network

Create a dedicated  
private cloud-only  
virtual network

Securely extend  
your datacenter with  
virtual networks

Enable hybrid  
cloud scenarios





## Create virtual network

Basics IP Addresses Security Tags Review + create

### Project details

Subscription \* ⓘ

Visual Studio Enterprise ▾

Resource group \* ⓘ

Lab04 ▾

[Create new](#)

### Instance details

Name \*

VNet2 ✓

Region \*

(US) East US 2 ▾

Create new virtual networks  
at any time

Add virtual networks when  
you create a virtual machine

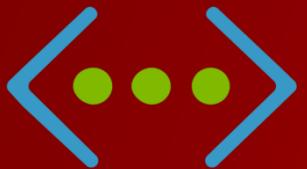
Need to define the address  
space, and at least one subnet

Be careful with overlapping  
address spaces

# AZ-104

## NETWORK

### Virtual Network



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

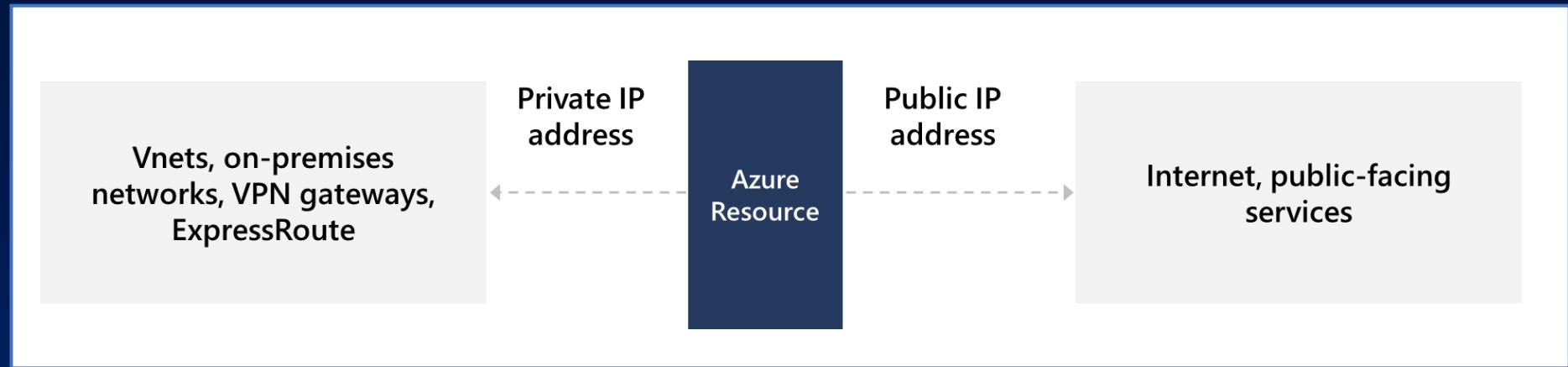
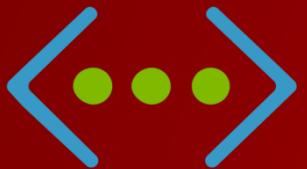
Each subnet must have a unique address range – cannot overlap with other subnets in the vnet in the subscription



# AZ-104

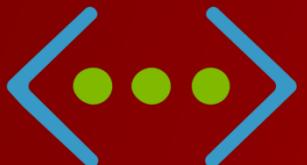
## NETWORK

### 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



#### Create public IP address

IP Version \*

- IPv4  IPv6  Both

SKU \*

- Basic  Standard

#### IPv4 IP Address Configuration

Name \*

IP address assignment \*

- Dynamic  Static

Available in IPv4 or IPv6 or both

Basic vs Standard SKU

Dynamic vs Static

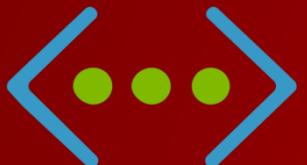
Zone redundant (Standard SKU)

Range of contiguous addresses available as a prefix

# 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*

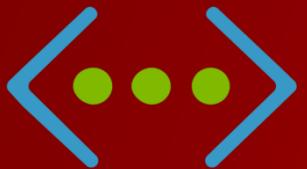
A public IP address resource can be associated with virtual machine network interfaces, internet-facing load balancers, VPN gateways, and application gateways

\*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



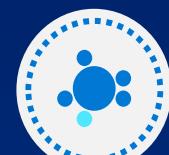
Implement Network Security Groups (NSG)



Determine NSG Rules



Determine NSG Effective Rules



Create NSG Rules

# AZ-104

## NETWORK Network Security Groups



The screenshot shows the Azure portal interface for a Network Security Group named "nsg0". The left sidebar includes options like Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The main content area displays resource details: Resource group (change) : rg01, Location : East US, Subscription (change) : , Subscription ID : , and Tags (change) : Click here to add tags. It also shows associated resources: Custom security rules : 1 inbound, 0 outbound, Associated with : 1 subnets, 0 network interfaces.

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

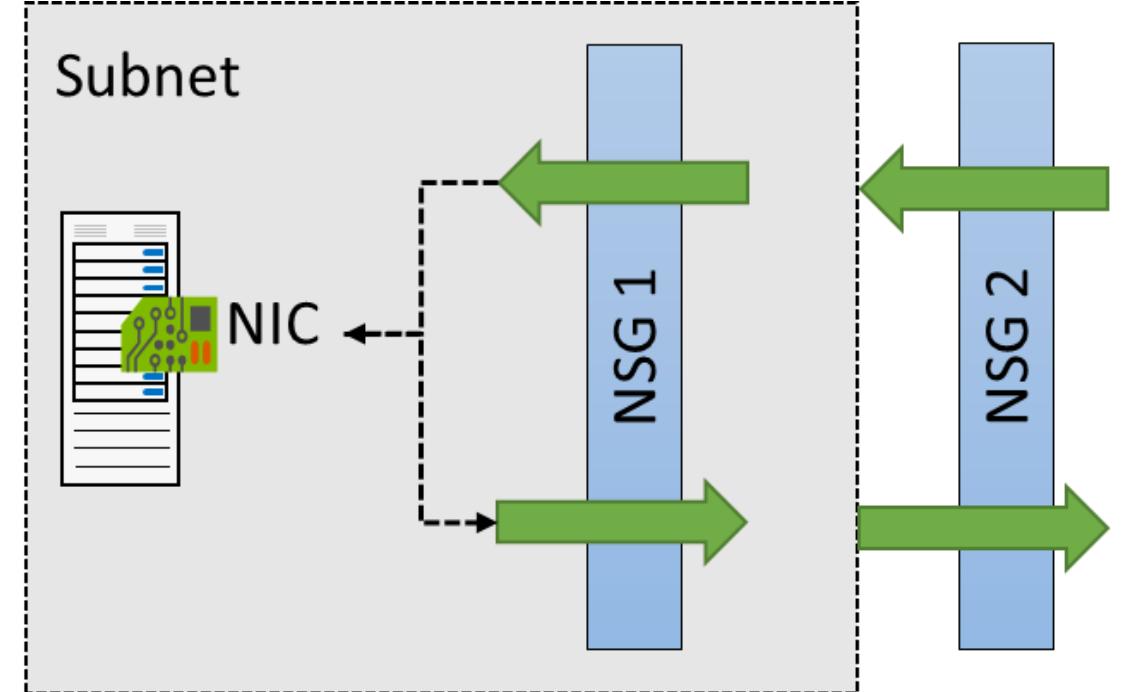
There are default security rules. You cannot delete the default rules, but you can add other rules with a higher priority



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



Network Interface: [vm01990](#)    Effective security rules    Topology  
Virtual network/subnet: [vnet01/subnet0](#)    NIC Public IP: -    NIC Private IP: **10.1.0.4**    Accelerated networking: **Disabled**

# AZ-104

## NETWORK

### Network Security Groups



Add inbound security rule  
az-vm

Source ⓘ  
Any

Source port ranges \* ⓘ  
\*

Destination ⓘ  
Any

Service ⓘ  
Custom

Destination port ranges \* ⓘ  
8080

Protocol  
 Any  
 TCP  
 UDP  
 ICMP

Action  
 Allow  
 Deny

Priority \* ⓘ  
310

Name \*  
Port\_8080

Description

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

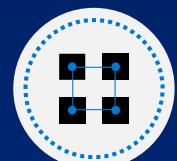
### Azure Firewall



Determine Azure Firewall Uses



Create Azure Firewalls

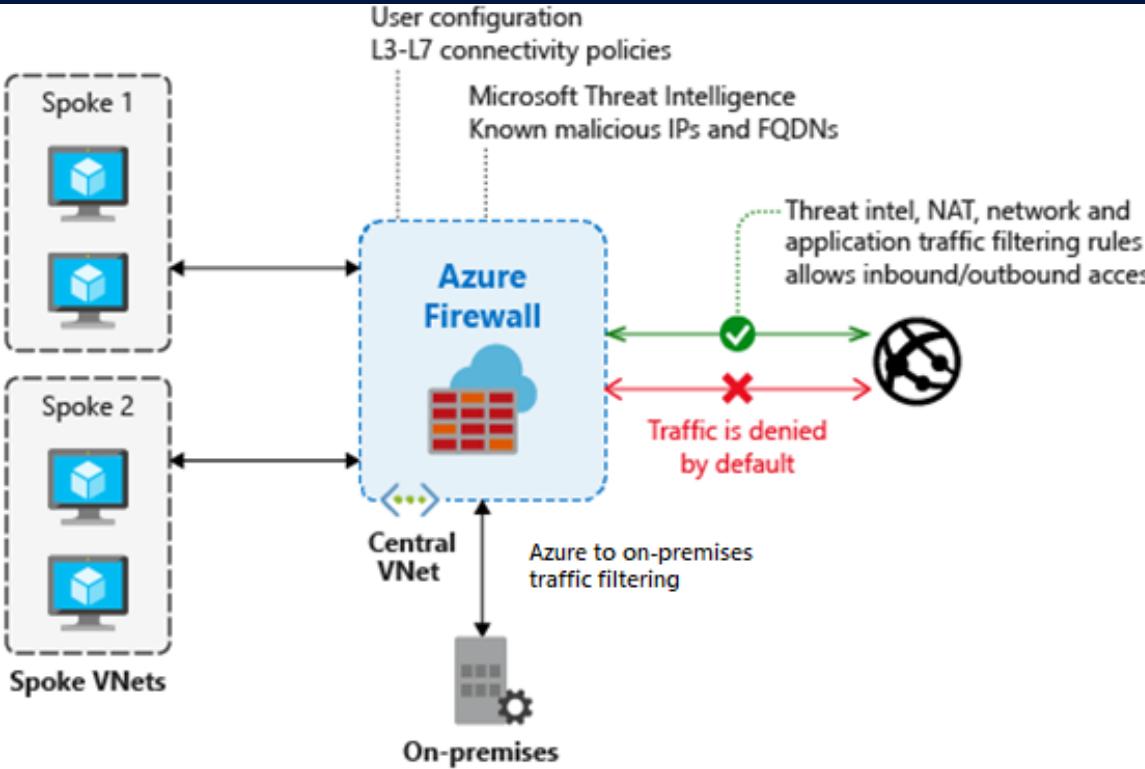
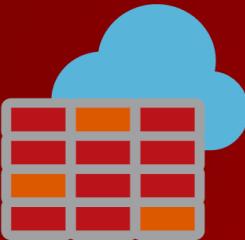


Create Azure Firewall Rules

# 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

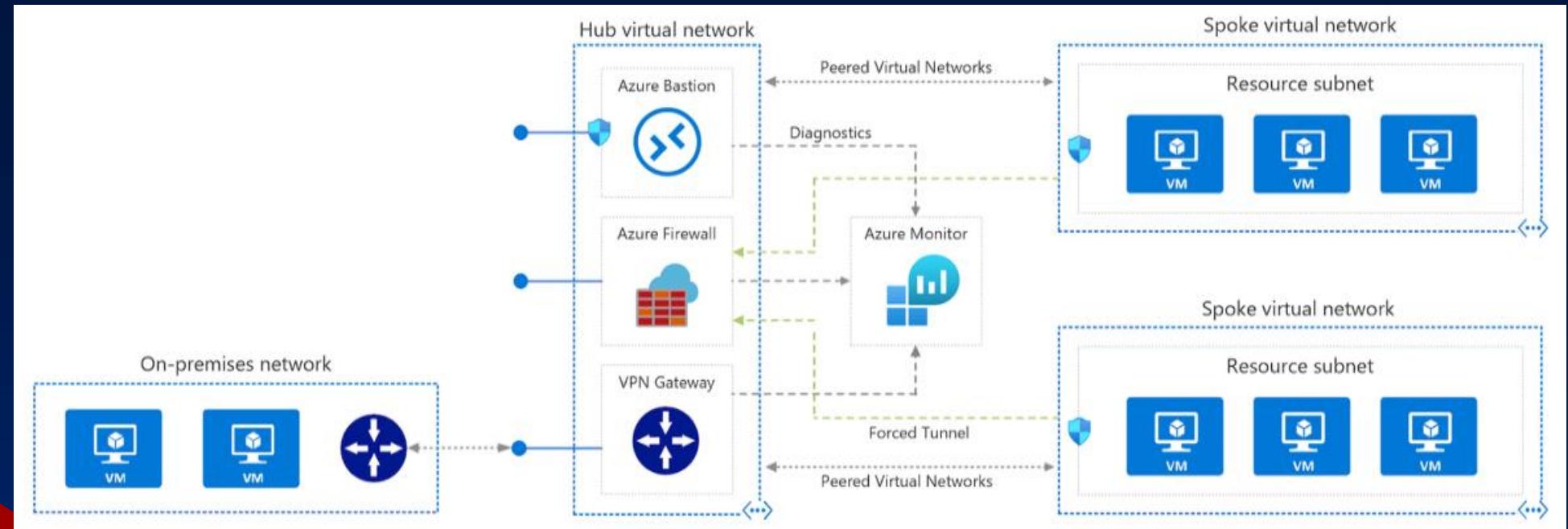
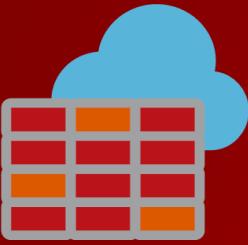
Create, enforce, and log application and network connectivity policies

Support for hybrid connectivity through deployment behind VPN and ExpressRoute Gateways



# AZ-104

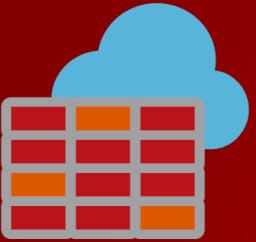
## NETWORK Azure Firewall



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



Settings

Rules

Public IP configuration

NAT rule collection

Network rule collection

Application rule collection

+ Add application rule collection

**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



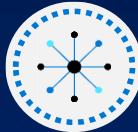
Identify Domains and Custom Domains



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



Create a directory  
Azure Active Directory

Basics \* Configuration \* Review + create

Directory details  
Configure your new directory

Organization name \* ⓘ  
Azure Administrator Incorporated ✓

Initial domain name \* ⓘ  
azureadminincorg ✓  
azurereadminincorg.onmicrosoft.com

Country/Region ⓘ  
United States

**Review + create** < Previous Next : Review + create >

Custom domain name  
Azure Administrator Incorporated

Custom domain name \* ⓘ  
azureadmininc.org ✓

**Add domain**

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)



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

azureadmininc.org

Custom domain name

Delete | Got feedback?

To use azureadmininc.org with your Azure AD, create a new TXT record with your domain name registrar using the info below.

Record type

TXT  MX

Alias or host name

@

Destination or points to address

MS=ms79094380

TTL

3600

[Share these settings via email](#)

Verification will not succeed until you have configured your domain with your registrar as described above.

# AZ-104

## NETWORK

### Azure DNS



Create DNS zone X

[Basics](#) [Tags](#) [Review + create](#)

A DNS zone is used to host the DNS records for a particular domain. For example, the domain 'contoso.com' may contain a number of DNS records such as 'mail.contoso.com' (for a mail server) and 'www.contoso.com' (for a web site). Azure DNS allows you to host your DNS zone and manage your DNS records, and provides name servers that will respond to DNS queries from end users with the DNS records that you create. [Learn more](#).

**Project details**

Subscription \* MSDN Platforms Subscription

Resource group \* rg-dns [Create new](#)

**Instance details**

Name \* azureadmininc.org

Resource group location East US

[Review + create](#) [Previous](#) [Next : Tags >](#) [Download a template for automation](#)

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

# AZ-104

## NETWORK

### Azure DNS



azureadmininc.org  
DNS zone

+ Record set → Move 🗑 Delete zone ⏪ Refresh

Resource group ([change](#))  
rg-dns

Subscription ([change](#))  
[MSDN Platforms Subscription](#)

Subscription ID

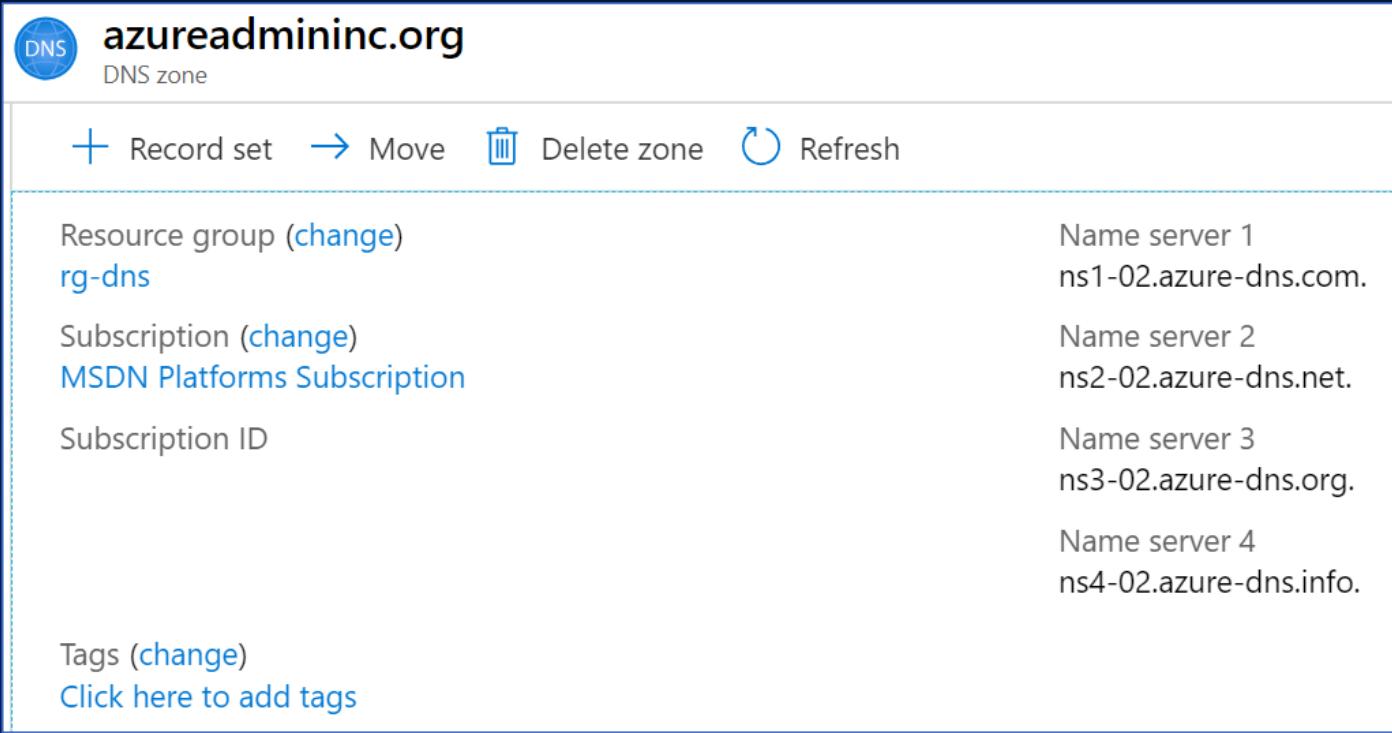
Name server 1  
ns1-02.azure-dns.com.

Name server 2  
ns2-02.azure-dns.net.

Name server 3  
ns3-02.azure-dns.org.

Name server 4  
ns4-02.azure-dns.info.

Tags ([change](#))  
[Click here to add tags](#)



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



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

### Add record set

azureadmininc.org

Name

helloworld

.azureadmininc.org

Type

A

Alias record set i

Yes  No

TTL \*

1

TTL unit

Hours

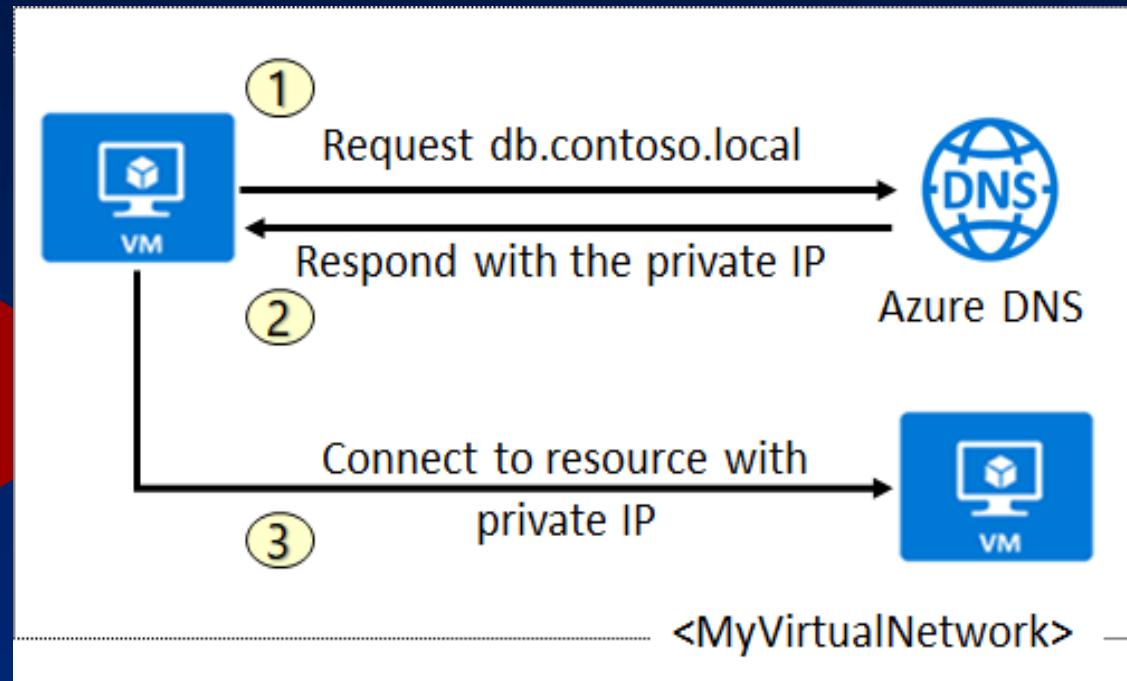
IP address

0.0.0.0

# 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

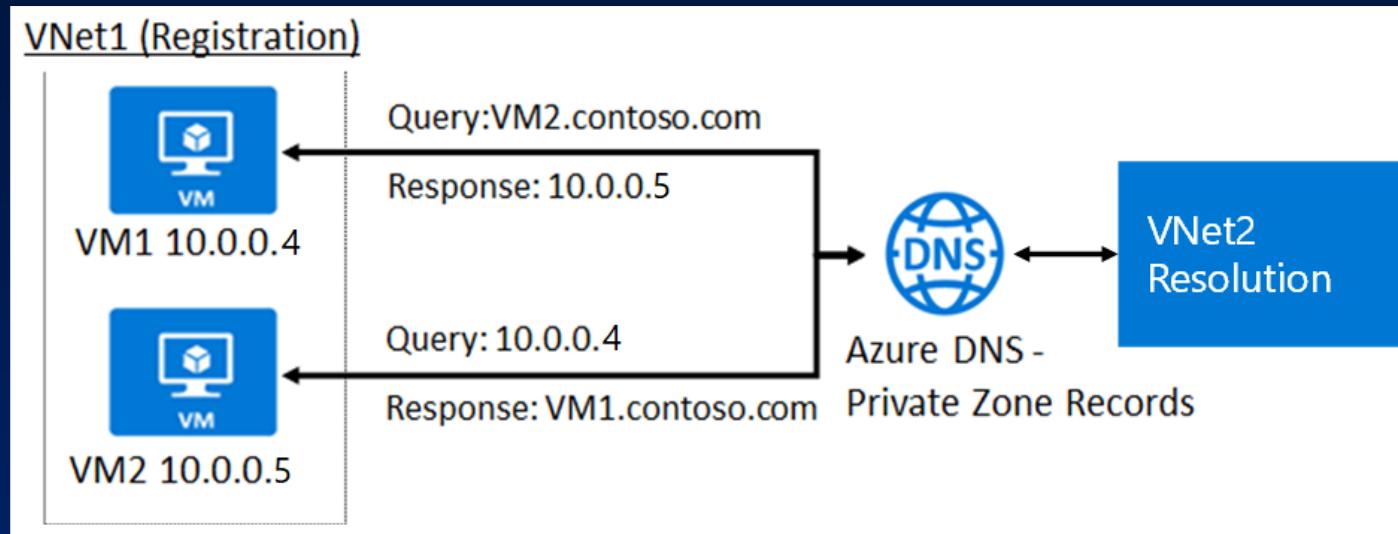
Use all common DNS records types

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

2.  A  B  C  D  E
3.  A  B  C  D  E
4.  A  B  C  D  E
5.  A  B  C  D  E
6.  A  B  C  D  E
7.  A  B  C  D  E
8.  A  B  C  D  E
9.  A  B  C  D  E
10.  A  B  C  D  E
11.  A  B  C  D  E
12.  A  B  C  D  E
13.  A  B  C  D  E
14.  A  B  C  D  E
15.  A  B  C  D  E
16.  A  B  C  D  E
17.  A  B  C  D  E
18.  A  B  C  D  E
19.  A  B  C  D  E
20.  A  B  C  D  E
21.  A  B  C  D  E
22.  A  B  C  D  E
23.  A  B  C  D  E
24.  A  B  C  D  E
25.  A  B  C  D  E
26.  A  B  C  D  E
27.  A  B  C  D  E
28.  A  B  C  D  E
29.  A  B  C  D  E
30.  A  B  C  D  E
31.  A  B  C  D  E
32.  A  B  C  D  E
33.  A  B  C  D  E
34.  A  B  C  D  E
35.  A  B  C  D  E
36.  A  B  C  D  E
37.  A  B  C  D  E
38.  A  B  C  D  E
39.  A  B  C  D  E
40.  A  B  C  D  E
41.  A  B  C  D  E
42.  A  B  C  D  E
43.  A  B  C  D  E
44.  A  B  C  D  E
45.  A  B  C  D  E
46.  A  B  C  D  E
47.  A  B  C  D  E
48.  A  B  C  D  E
49.  A  B  C  D  E



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:

1
2
3



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	Value
Name	ALLOW_HTTPS
Id	/subscriptions/09d06b22-ff51-48b7-a8be-947f15cbd69d/resourceGroups/RG1/providers/Microsoft.Network/networkSecurityGroups/NSG1/securityRules/ALLOW_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/DENY_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
Any	
10.1.0.10	
10.1.0.11	
10.1.0.10; 10.1.0.11	
10.1.0.0/28	

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	



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

Add a record to the public contoso.com DNS zone

Add an Azure AD tenant

Configure company branding

Create an Azure DNS zone

Add a custom name

Verify the domain

#### Answer Area

Add a custom name

Add a record to the public contoso.com DNS zone

Verify the domain



# 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.

Microsoft  
CERTIFIED

AZURE  
ADMINISTRATOR  
ASSOCIATE



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

# 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.

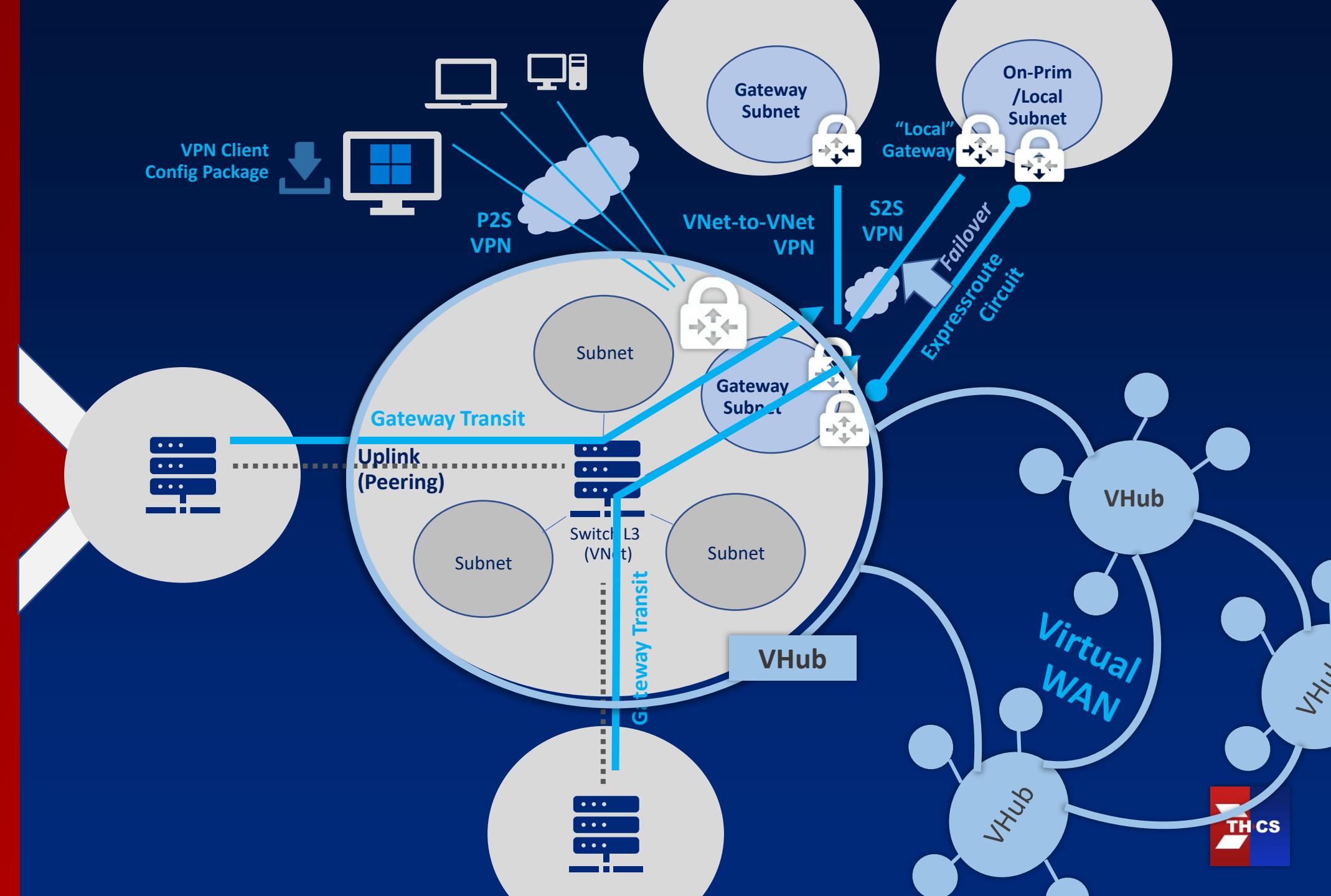
You need to ensure that Azure can verify the domain name.

Which type of DNS record should you create?

- A. MX
- B. NSEC
- C. SRV
- D. NSEC3

# AZ-104

## NETWORK Intersite Connectivity



# AZ-104

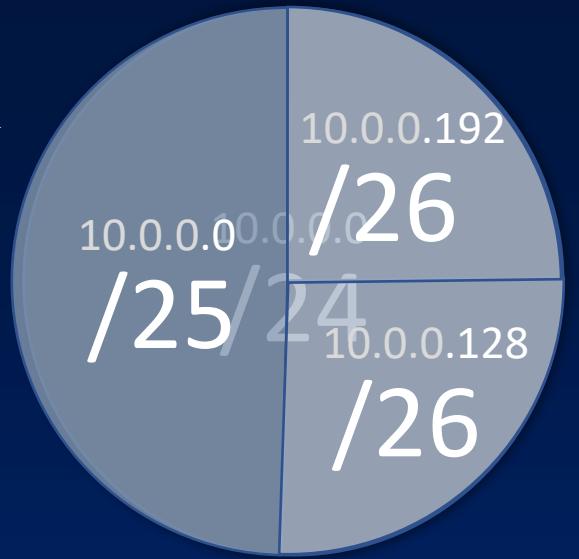
## NETWORK

### 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

# AZ-104

## NETWORK

### Intersite Connectivity



## Address Space IP Subnetting

Microsoft Azure Search resources, services, and docs (G+)

Home > Virtual networks >

### Create virtual network

Basics IP Addresses Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

10.0.0.0/16 10.0.0.0 - 10.0.255.255 (65536 addresses)

10.0.1.0/16

10.0.1.0/16 is not a valid CIDR block. Use 10.0.0.0/16 instead. Address space '10.0.1.0/16 (10.0.0.0 - 10.0.255.255)' overlaps with address space '10.0.0.0/16 (10.0.0.0 - 10.0.255.255)'. Address spaces within a virtual network cannot overlap.

Add subnet

Subnet name \* TestVNetSub1

Subnet address range \* 10.0.1.0/24

10.0.1.0 - 10.0.1.255 (251 + 5 Azure reserved addresses)

The subnet address range '10.0.1.0/24' is not contained in this virtual network's address spaces.

Basics IP Addresses Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

10.0.0.0/8

Address space '10.0.0.0/8 (10.0.0.0 - 10.255.255.255)' overlaps with address space '10.1.0.0/16 (10.1.0.0 - 10.1.255.255)' of virtual network 'SarahTestVNet1'. Virtual networks with overlapping address space cannot be peered. If you intend to peer these virtual networks, change address space '10.0.0.0/8 (10.0.0.0 - 10.255.255.255)'. [Learn more](#)

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

THCS

# AZ-104

## NETWORK

### Intersite Connectivity



Microsoft Azure Search

Home > Virtual networks >

## Virtual networks

Default Directory

**Create** Manage view ...

Filter for any field...

Name ↑↓

Basics IP Addresses Security Tags Review + create

Azure Virtual Network (VNet) is the fundamental building block for connecting Azure resources, such as Azure Virtual Machines (VM), to secure external networks. VNet is similar to a traditional network that you'd operate in your data center, but it benefits from Azure's infrastructure such as scale, availability, and security.

Project details

Subscription \*  Visual Studio Enterprise  TestVNetPeering  Create new

Resource group \*  TestVNetPeering  Create new

Instance details

Name \*  SarahTestVNet1  West US 2

Region \*  West US 2

Basics IP Addresses Security Tags Review + create

### Create virtual network ...

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

10.0.0.0/16 10.0.0.0 - 10.0.255.255 (65536 addresses)

The value must not be empty. Invalid argument: 'A non-null address range is required.'

Add IPv6 address space

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

Add subnet  Remove subnet

Subnet name  default Subnet address range 10.0.0.0/24

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

Review + create < Previous Next : Security > Download a template for automation

How to  
Peer VNet



# AZ-104

## NETWORK

### Intersite Connectivity



## How to Peer VNet

The screenshot illustrates the process of creating a VNet peering between two virtual networks: SarahTestVNet1 and TestVNet2.

**Step 1: SarahTestVNet1 | Peerings**

In the Azure portal, navigate to the "SarahTestVNet1" virtual network and select the "Peerings" blade. The "Add" button is highlighted with a red box.

**Step 2: Add peering**

The "Add peering" blade for "SarahTestVNet1" is shown. It includes an informational message about creating two-way peering links, a "Peering link name" field set to "VNet1-to-2", and configuration options for traffic to and from the remote network.

**Step 3: Add peering**

The "Add peering" blade for "TestVNet2" is shown. It includes a "Virtual network" dropdown set to "TestVNet2", configuration options for traffic to and from the remote network, and a "Subscription" dropdown set to "Visual Studio Enterprise Subscription".

**Summary:** Create once, get both (two-way) peering links.



# AZ-104

## NETWORK

### Intersite Connectivity



Home > Virtual networks > SarahTestVNet1

## SarahTestVNet1 | Peerings

Virtual network

Add Refresh Sync

Filter by name... Peering status == all

Name ↑↓	Peering status ↑↓	Peer ↑↓	Gateway transit ↑↓
VNet1-to-2	Connected	TestVNet2	Disabled

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

Home > Virtual networks > TestVNet2

## TestVNet2 | Peerings

Virtual network

Add Refresh Sync

Filter by name... Peering status == all

Name ↑↓	Peering status ↑↓	Peer ↑↓	Gateway transit ↑↓
VNet2-to-1	Connected	SarahTestVNet1	Disabled

Create once, get both direction peerings!

How to  
Peer VNet



# AZ-104

## NETWORK

### Intersite Connectivity



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

### Create a virtual machine

Networking tab selected.

Virtual network: (new) TestPeeringEastUS-vnet [Create new](#) (highlighted with red box)

Subnet: (new) default (10.0.0.0/24) (highlighted with red box)

Public inbound ports: Allow selected ports (highlighted with red box)

Select inbound ports: RDP (3389)

Warning message: This will allow all IP addresses to a recommended for testing. Use the A create rules to limit inbound traffic to

### Create virtual network

The Microsoft Azure Virtual Network service ensures logical isolation of the Azure cloud dedicated to your premises network. [Learn more](#)

Name: TestPeeringEastUS-vnet

Address space:

Address range	Addresses	Overlap
<input type="checkbox"/> 10.0.0.0/16	10.0.0.0 - 10.0.255.255 (65536 addresses)	None
<input checked="" type="checkbox"/> 10.1.128.0/17	10.1.128.0 - 10.1.255.255 (32768 addresses)	None
	(0 Addresses)	

Subnets:

Subnet name	Address range	Addresses
<input type="checkbox"/> default	10.0.0.0/24	10.0.0.0 - 10.0.0.255 (256 addresses)
<input type="checkbox"/> SarahSubTest	10.1.64.0/25	10.1.64.0 - 10.1.64.127 (128 addresses)

Your subnet is not contained within the address space for this virtual network: 10.0.0.0/16, 10.1.128.0/17.

## How to Peer VNet



# AZ-104

## NETWORK

### Intersite Connectivity



TestVM2-Sub2 | Connection troubleshoot

Search (Ctrl+ /)

Give feedback

Configuration management (Preview)

Policies

Run command

Monitoring

- Insights
- Alerts
- Metrics
- Diagnostic settings
- Logs
- Connection monitor (classic)
- Workbooks

Automation

- Tasks (preview)
- Export template

Support + troubleshooting

- Resource health
- Boot diagnostics
- Performance diagnostics
- Reset password
- Redeploy + reapply
- Serial console
- Connection troubleshoot
- New Support Request

Use Network Watcher for detailed connection tracing

Inbound connections   Outbound connections

Check connection source

Connection source \* My IP address

VM destination port

Service \* SSH

Port \* 22

Protocol \* TCP

Test connection

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

Microsoft Azure

Home > Network Watcher

## Network Watcher | Connection troubleshoot

Microsoft

Search (Ctrl+ /)

Overview

Get started

Monitoring

- Topology
- Connection monitor (classic)
- Connection monitor
- Network Performance Monitor

Network diagnostic tools

- IP flow verify
- NSG diagnostic
- Next hop
- Effective security rules
- VPN troubleshoot
- Packet capture
- Connection troubleshoot

Metrics

No virtual machines found

Source

Subscription \* Pay-As-You-Go

Resource group \*

Filter by Resource Group

Source type \*

Destination

Select a virtual machine  Specify manually

Resource group \*

Filter by Resource Group

Virtual machine \* No virtual machines found

Probe Settings

Preferred IP Version

Check Connection?  
Use Network Watcher



# AZ-104

## NETWORK

### Intersite Connectivity



Microsoft Azure

Home > Virtual machines > TestVM2-Sub2 >

### Connection troubleshoot

Network Watcher Connection Troubleshoot provides the capability to check a direct TCP connection from a virtual machine (VM) to a VM, fully qualified domain name (FQDN), URI, or IPv4 address. To start, choose a source to start the connection from, and the destination you wish to connect to and select "Check". [Learn more.](#)

Source

Subscription [Visual Studio Enterprise Subscription](#)

Resource group [TESTVNPEER](#)

Source type Virtual machine

Virtual machine [TestVM2-Sub2](#)

Destination

Select a virtual machine  Specify manually

Resource group \* [SarahTestPeering-New](#)

Virtual machine \* [vm1-sub1](#)

Probe Settings

Preferred IP Version [\(1\)](#)

Protocol [TCP](#) [ICMP](#)

Destination port \* [3389](#)

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

Check Connection?  
Use Network Watcher

Check

Status [Reachable](#)

Agent extension version 1.4

Source virtual machine [TestVM2-Sub2](#)

Grid view Topology view

Hops

Name	IP address	Status	Next hop IP address	RTT
<a href="#">TestVM2-Sub2</a>	10.1.2.4	<a href="#">Green</a>	10.1.1.4	-
<a href="#">vm1-sub1</a>	10.1.1.4	<a href="#">Green</a>	-	-

Average Latency in milliseconds 1

Minimum Latency in milliseconds 1

Maximum Latency in milliseconds 4

Probes Sent 66

Probes Failed 0

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



# 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)

Across regions with “Global” Peering

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 <sup>1</sup>	Zone 2 <sup>1</sup>	Zone 3 <sup>1</sup>	US Gov <sup>1</sup>
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

<sup>1</sup>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.

<sup>1</sup>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.

# AZ-104

## NETWORK

### Intersite Connectivity



Microsoft Azure Search resources, services, and docs (G+)

Home > Virtual network gateways > Create virtual network gateway

Basics Tags Review + create

Azure has provided a planning and design guide to help you configure the various VPN gateway options. [Learn more.](#)

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* Visual Studio Enterprise Subscription

Resource group TestVNetPeering (derived from virtual network's resource group)

**Instance details**

Name \* SarahGWTest

Region \* East US 2

Gateway type \*  VPN  ExpressRoute

VPN type \*  Route-based  Policy-based

SKU \* VpnGw2AZ

Generation Generation2

Virtual network \* SarahTestVNet [Create virtual network](#)

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

Gateway subnet address range \* 10.1.0.0/24  
10.1.0.0 - 10.1.0.255 (256 addresses)

An ExpressRoute gateway is used to send traffic between your Azure virtual network and your on-premises network over your ExpressRoute circuit. [Learn more](#)

A VPN gateway is used to send encrypted traffic between your Azure virtual networks or between Azure and your on-premises network. [Learn more](#)

Gateway type \*  VPN  ExpressRoute

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

# AZ-104

## NETWORK Intersite Connectivity



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)

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

The type of VPN you can choose depends on the make and model of your VPN device, and the kind of VPN connection you intend to create. Choose a route-based gateway if you intend to use point-to-site, inter-virtual network, or multiple site-to-site connections; if you are creating a VPN type gateway to coexist with an ExpressRoute gateway; or if you need to use IKEv2. Policy-based gateways support only IKEv1.

VPN type \*  Route-based  Policy-based

SKU \*  Basic  VpnGw2AZ

If the current SKU is Basic, Standard, or High performance, it can be upgraded or downgraded to a Basic, Standard, or High performance SKU. If the current SKU is VpnGw1, VpnGw2, or VpnGw3, it can be upgraded or downgraded to VpnGw1, VpnGw2, or VpnGw3. If the gateway is being created to coexist with an ExpressRoute gateway, choose any SKU except for Basic.

## Many kinds of VNet (VPN) Gateway

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

VPN type \*  Route-based  Policy-based

SKU \*  Basic  VpnGw2AZ

Generation  Generation1

SKU \*  Basic  VpnGw2AZ

Policy-based VPN gateway types are offered only in the Basic SKU. [Learn more](#)

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



# AZ-104

## NETWORK Intersite Connectivity



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.

Microsoft Azure Search resources, services, and docs (G+)

Home > Virtual network gateways > Create virtual network gateway

Basics Tags Review + create

Azure has provided a planning and design guide to help you configure the various VPN gateway options. [Learn more.](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* Visual Studio Enterprise Subscription

Resource group TestVNetPeerin

Instance details

Name \* SarahGWTest

Region \* East US 2

Gateway type \*  VPN  Route-based

VPN type \*  VpnGw1AZ  VpnGw2AZ  VpnGw3AZ

SKU \* VpnGw2AZ

Generation Generation2

Generation of VPN gateway, changing Generation or changing SKU across generation is not allowed. Basic and VpnGw1 SKUs are supported on Generation1 only, VpnGw4 and VpnGw5 SKUs are supported on Generation2 only. [Learn more.](#)

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

Many kinds  
of VNet (VPN) Gateway

VPN Gateway Generation	SKU	S2S/VNet-to-VNet Tunnels	P2S SSTP Connections	P2S IKEv2/OpenVPN Connections	Aggregate Throughput	BGP Benchmark
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
Generation1	VpnGw2AZ	Max. 30	Max. 128	Max. 500	1 Gbps	Supported
Generation1	VpnGw3AZ	Max. 30	Max. 128	Max. 1000	1.25 Gbps	Supported
Generation2	VpnGw2	Max. 30	Max. 128	Max. 500	1.25 Gbps	Supported
Generation2	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

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



# AZ-104

## NETWORK

### Intersite Connectivity



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

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

If select  
VpnGW\*”AZ”  
[Availability Zone]  
SKU, or choose  
“Standard” public  
IP, min /27 size  
GatewaySubnet is  
required.

Virtual network 'SarahTestVNetFull' doesn't contain a gateway subnet, and one must be configured before creating a virtual network gateway. Specify a subnet address range in CIDR notation which falls within the virtual network's address space: 192.168.0.0/24. If the gateway is an ExpressRoute type and you plan on creating a VPN gateway to coexist with it, the prefix of the CIDR notation must be 27 or smaller.

Gateway subnet address range \* 192.168.0.0/29  
192.168.0.0 - 192.168.0.7 (8 addresses)

The specified address space overlaps with subnet 'SarahSub1' which has a range of '192.168.0.0/25'. To deploy a zone-redundant/zonal gateway, the GatewaySubnet must be /27 or larger.

Instance details

- Name \* SarahGWTest
- Region \* East US 2
- Gateway type \*  VPN  ExpressRoute

The virtual network that will be able to send and receive traffic through this virtual network gateway. To associate a virtual network with a gateway, it must first contain a valid gateway subnet. A virtual network can't be associated with more than one gateway.

Virtual network \* SarahTestVNet1

Virtual network \* SarahTestVNet1  
Create virtual network  
Only virtual networks in the currently selected subscription and region are listed.

Gateway subnet address range \* 10.1.0.0/24  
10.1.0.0 - 10.1.0.255 (256 addresses)

SarahTestVNet1 | Subnets

Add subnet

- Name
- Subnet address range \* 10.1.0.0/24
- Add IPv6 address space
- NAT gateway  None
- Network security group

No NSG on GatewaySubnet !

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

Many kinds of VNet (VPN) Gateway

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



# AZ-104

## NETWORK

Intersite Connectivity



When adding connection, you have to choose “second” VNet GW, even on-prim GW! (that has to create local GW as logical ref)

**Microsoft Azure**

Home > Microsoft.VirtualNetworkGateway-20220416220302 > OnPrimGW

**OnPrimGW | Connections**

Virtual network gateway

+ Add Refresh

Search (Ctrl+ /) Search connections

Name	Status	Connection type
OnPrim2VNetPeer	Unknown	VNet-to-VNet

Must add connection on both GW (2-way)

S2S, PSK has to be the same

**Add connection**

OnPrimGW

Name \*  ✓

Connection type ⓘ  ✓

\*First virtual network gateway ⓘ  ➤

\*Second virtual network gateway ⓘ  ➤

Shared key (PSK) \* ⓘ  ✓

Use Azure Private IP Address ⓘ

Enable BGP ⓘ

IKE Protocol ⓘ  IKEv1  IKEv2

Subscription ⓘ  ✓

**Notifications**

More events in the activity log → Dismiss all

✓ Create connection Successfully created connection ‘OnPrim2VNetPeer’ a few seconds ago

✗ Failed to create connection

**Add connection**

GWVNet1

Name \*  ✓

Connection type ⓘ  ✓

\*First virtual network gateway ⓘ  ➤

\*Second virtual network gateway ⓘ  ➤

Shared key (PSK) \* ⓘ  ✓

Use Azure Private IP Address ⓘ

Enable BGP ⓘ

IKE Protocol ⓘ  IKEv1  IKEv2

Subscription ⓘ  ✓

Resource group ⓘ

OK

Create VNet-to-VNet  
or S2S connection

# AZ-104

## NETWORK Intersite Connectivity



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

Microsoft Azure Search resources, services, and docs (G+/)

Home > GWVNet1

## GWVNet1 | Connections

Virtual network gateway

Search (Ctrl+ /) Add Refresh

Name	Status	Connection type	Peer	...
OnPrim2VNetPeer	Not connected	VNet-to-VNet	OnPrimGW	...
VNetPeer2OnPrim	Updating	VNet-to-VNet	OnPrimGW	...

Search connections

Name	Status	Connection type	Peer	...
OnPrim2VNetPeer	Connected	VNet-to-VNet	OnPrimGW	...
VNetPeer2OnPrim	Connected	VNet-to-VNet	OnPrimGW	...

Add Refresh

Search connections

Name	Status	Connection type	Peer	...
OnPrim2VNetPeer	Connected	VNet-to-VNet	OnPrimGW	...
VNetPeer2OnPrim	Connected	VNet-to-VNet	OnPrimGW	...

Create VNet-to-VNet  
or S2S connection

# 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



# AZ-104

## NETWORK

### Intersite Connectivity



Home > Microsoft.VirtualNetworkGateway-20220430055453 > SarahTestVNetGW

### SarahTestVNetGW | Point-to-site configuration

Virtual network gateway

Search (Ctrl+ /) Save Discard Delete Download VPN client

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.)

Certmgr - [Certificates - Current User\Personal\Certificates]

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
P2SRootCert	P2SRootCert	2/2/2019	Client Authentication	<None>
P2SChildCert	P2SRootCert	2/2/2019	Client Authentication	<None>

PowerShell 7 (x64)

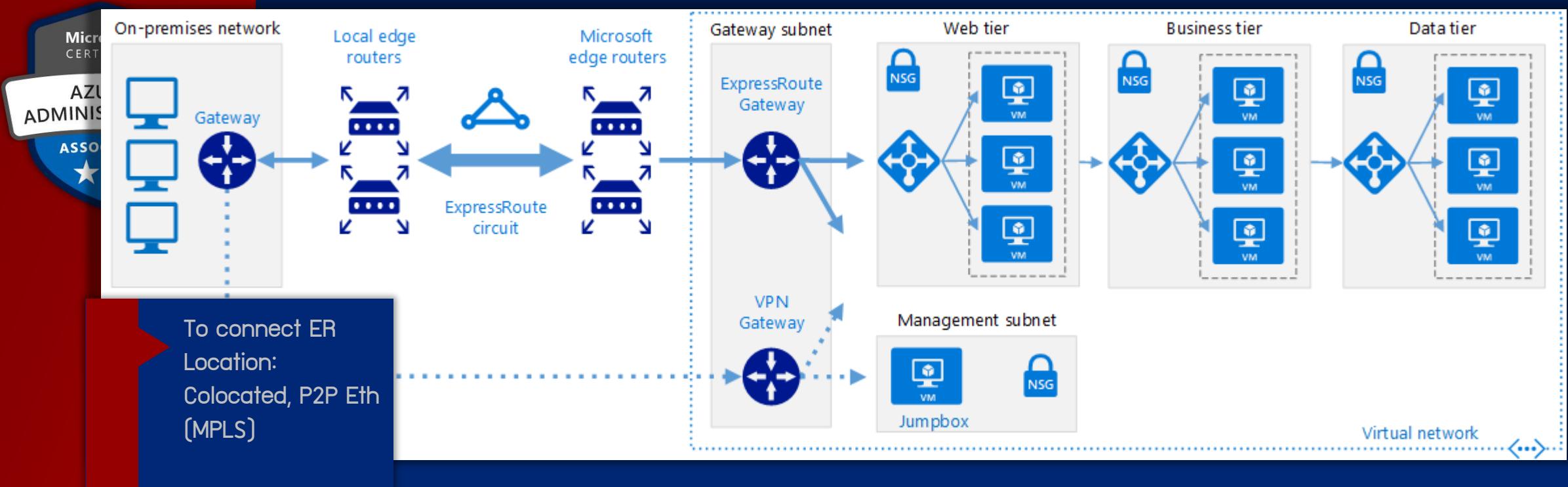
```
PS C:\Users\nol12> $cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature -Subject "CN=P2SRootCert" -KeyExportPolicy Exportable -HashAlgorithm sha256 -KeyLength 2048 -CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign -Subj "CN=P2SChildCert" -KeyExportPolicy Exportable -HashAlgorithm sha256 -KeyLength 2048 -CertStoreLocation "Cert:\CurrentUser\My" -Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")
```

Thumbprint F76C4147532C2CDE25F57BCD956414CFE1718613 Subject CN=P2SChildCert EnhancedKeyUsageList Client Authentication

## Create P2S Connection with Config Package



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



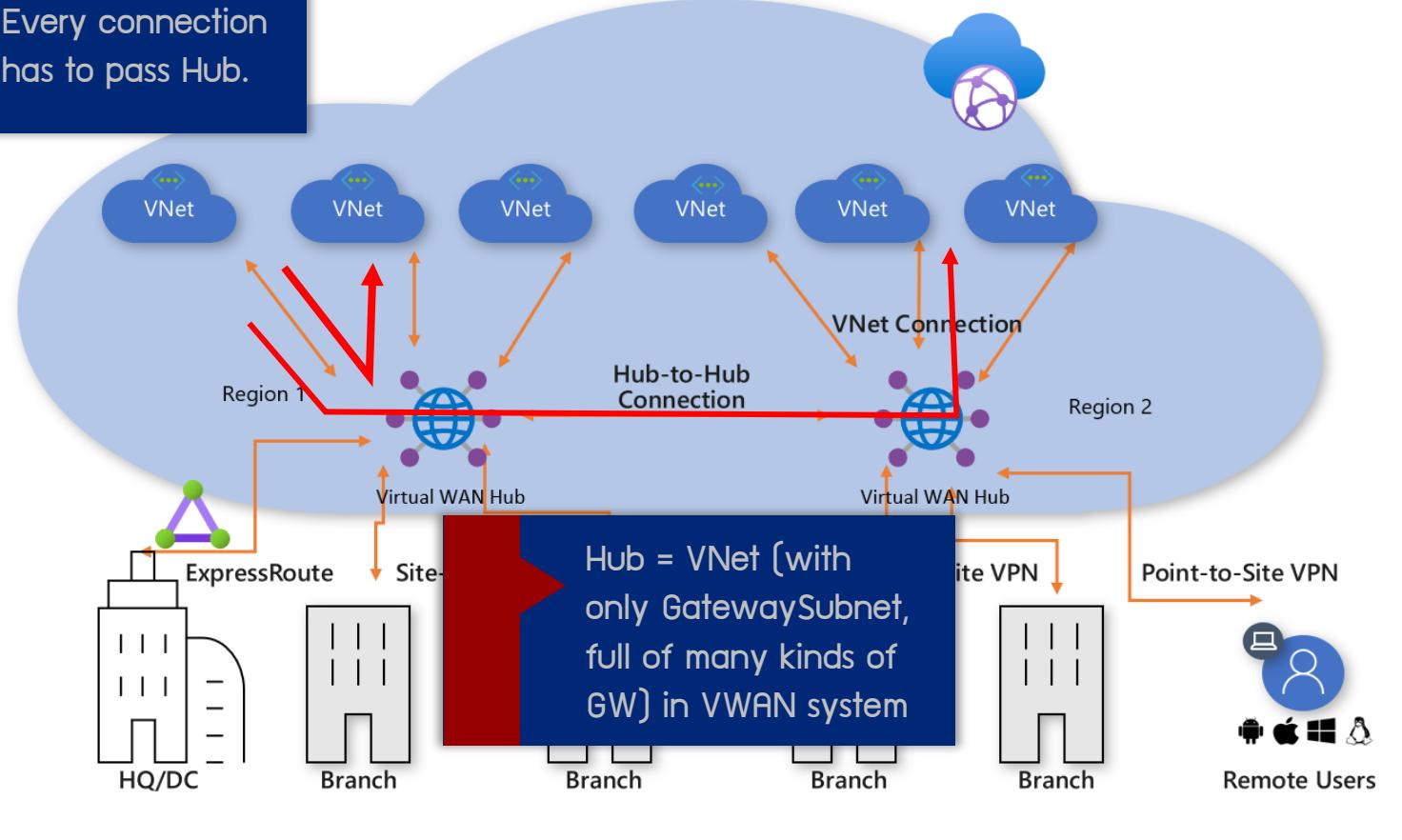
**ExpressRoute (ER)**  
With S2S as backup

# AZ-104

## NETWORK Intersite Connectivity



Every connection has to pass Hub.



One Virtual WAN  
With many Virtual Hubs

# AZ-104

NETWORK

Intersite Connectivity



# Example Questions

2.  A  B  C  D  E
3.  A  B  C  D  E
4.  A  B  C  D  E
5.  A  B  C  D  E
6.  A  B  C  D  E
7.  A  B  C  D  E
8.  A  B  C  D  E
9.  A  B  C  D  E
10.  A  B  C  D  E
11.  A  B  C  D  E
12.  A  B  C  D  E
13.  A  B  C  D  E
14.  A  B  C  D  E
15.  A  B  C  D  E
16.  A  B  C  D  E
17.  A  B  C  D  E
18.  A  B  C  D  E
19.  A  B  C  D  E
20.  A  B  C  D  E
21.  A  B  C  D  E
22.  A  B  C  D  E
23.  A  B  C  D  E
24.  A  B  C  D  E
25.  A  B  C  D  E
26.  A  B  C  D  E
27.  A  B  C  D  E
28.  A  B  C  D  E
29.  A  B  C  D  E
30.  A  B  C  D  E
31.  A  B  C  D  E
32.  A  B  C  D  E
33.  A  B  C  D  E
34.  A  B  C  D  E
35.  A  B  C  D  E
36.  A  B  C  D  E
37.  A  B  C  D  E
38.  A  B  C  D  E
39.  A  B  C  D  E
40.  A  B  C  D  E
41.  A  B  C  D  E
42.  A  B  C  D  E
43.  A  B  C  D  E
44.  A  B  C  D  E
45.  A  B  C  D  E
46.  A  B  C  D  E
47.  A  B  C  D  E
48.  A  B  C  D  E
49.  A  B  C  D  E

# AZ-104

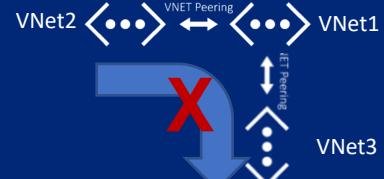
## NETWORK Intersite Connectivity



Home > SarahTestPeerVNet2

### SarahTestPeerVNet2 | Peerings

Peer ไป Transitive  
(ไม่โอดข้าม Vnet)



+ Add Refresh

Filter by name...

Name ↑↓

VNet2-VNet1

Peering status ↑↓

Connected

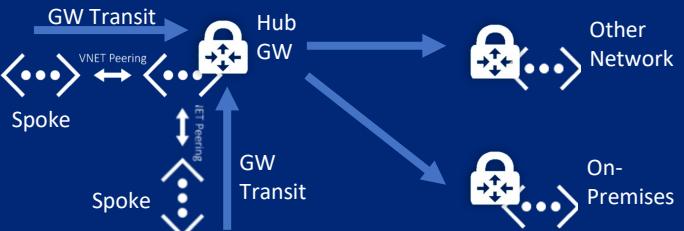
Peer ↑↓

SarahTestPeerVNet1

Gateway transit ↑↓

Disabled

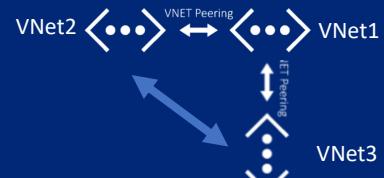
problems



Gateway Transit ไม่เกี่ยว ไม่ใช้การทำ Transitive ก็  
จะ Enable ก็แค่ให้กราฟิกที่ Peer ให้ล็อกอิน Hub ก็มีเกต  
เวย์อยู่ข้างไปเกตเวย์ที่ Net/OnPrim อื่นๆ เก่าบ้าน

### SarahTestPeerVNet3 | Peerings

ถ้าอยากคุยกับได้ มีวิธี  
เดียวคือ Peer เป็น



+ Add Refresh Sync

Filter by name...

Peering status == all

Name ↑↓

VNet3-VNet1

Peering status ↑↓

Connected

Peer ↑↓

SarahTestPeerVNet1

Gateway transit ↑↓

Disabled

From SarahTestPeerVNet1,  
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

# AZ-104

## NETWORK Intersite Connectivity



VNet1 can be peered with?

Peer ໄດ້ ໄວີ (Address Space/Prefix) ຕ້ອງໄປກັບກັນ (Overlapped) ເຊັ່ນ ດ້າ /16 [ສອງໃບຕໍແຮກ] ກີ່ຕ້ອງໄປກັບກັບ /16+ ຂອງVNet ວິນ

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

ເຄົາ Peer ຊ້າມຮັບເຈັຍນັກນ (Global Peering) ກັນໄດ້ແລ້ວ ໄນໄດ້ດູກຈຳກັດແກ່ຕ້ອງຮັບເຈັຍນເດືອນວັນອີກ

ດັ່ງນັ້ນ Region ໄປເກົ່າຍວ

# AZ-104

## NETWORK Intersite Connectivity



VNet "Sarah1" has no any VM or resource.

Sarah1 Virtual network

Search (Ctrl+ /) Overview Activity log Access control (IAM) Tags Diagnose and solve problems

Resource group (move) SarahTestPeering-New Location (move) West US 2 Subscription (move) Visual Studio Enterprise Subscription Subscription ID a909f5b5-790e-4d54-9a8d-597b124cc3cf

Address space 192.168.0.0/16 DNS servers Azure provided DNS service Flow timeout Configure BGP community string Configure Virtual network ID a45752b6-1596-463b-aa92-5cef

Tags (edit) Test : VNetPeering

Peer ได้ ไอพี (Address Space) ต้องไม่เก็บกัน (Overlapped) เช่น ก้า /16 (สองไปต่อแรก) ก็ ต้องไม่เก็บกัน /16+ ของ VNet อื่น

Peering ก้าไอพีไม่เก็บ เพียงรึได้เลย เป็นระบบกี่ ออกแบบมาให้ไปต้องฟัง เกตเวย์ ขับเบ็ต หรือใส่ NVA รีชอร์สจะได้ก่อน อยู่แล้ว

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



ถ้าสร้าง Peer แล้ว จะล็อกไม่ให้เพิ่มหรือแก้ Address Space (เหมือนเอาไปเขียนต่างหาก แล้ว) ดังนั้นต้องลบเพย์ร ก่อนก็จะได้



From this info:

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

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

Peering ถ้าไอพีไม่ทับเพย์รได้เลย เป็นระบบที่อุดแบบมาให้ไปต้องผ่านเกตเวย์ ซับเน็ต หรือไส NVN รีชอร์สจะไม่ถูกอนุญาตแล้ว



Gateway ต้องมีชับเบ็ต  
ของตัวเองแยกต่างหาก ถ้า  
VNet ใหม่ไม่เหลือ Space  
ให้พิมพ์สร้างชับเบ็ตเพิ่ม  
(อย่างต่ำ /29) ก็สร้างเกต  
เวย์ไม่ได้



Subscription: Sarah1, has VNets/Subnets as follows:

VNet	Address Space	Location	Subnet	Address Space	in VNet
VNet1	10.0.0.0/16	WestUS2	Sub11	10.0.0.0/17	VNet1
VNet2	172.168.128.0/17	SEA	Sub12	10.0.128.0/17	VNet1

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

VNet1 and 3 can establish Site-to-Site VPN?

Yes      No

VNet1 and 2 can be peered?

Yes      No

VNet2 and 3 can be peered?

Yes      No

# AZ-104

## NETWORK

### Intersite Connectivity



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

ໄປວ່າຈະເພີຍຮອບເຂົ້ມ  
ຝ່ານເກຕເວຍ ໄວພິສເປັບໃນ  
ກັ້ສອງ VNet ກີ່ຕ້ອງໄປໂວ  
ເວອຣແລປກັນ ຖອນນີ້  
VPN Gateway ຍັງກໍາ  
NAT ໄປໄດ້)

ດ້າໄວພິໄປໂວເວອຣແລປ ດ້າຈະ  
ເຂົ້ມກັນງ່າຍສຸດຄື້ອກໍາ  
ເພີຍຮົງ ແຕ່ດ້າຂອຍສິ່ນເນັດ  
ຄື້ອສຮ້າງ VNet (VPN)  
Gateway ໂດຍ VNet-  
to-Vnet

VPN ໂດຍ VNet-to-VNet ກີ່ຄົວ  
S2S ອຢ່າງນິ້ງ ດັ່ງນັ້ນຕ້ອງນິເກຕເວຍ  
ກີ່ແຕ່ລະໃຫຕ/VNet ດ້ວຍ ຕ່າງຝ່າຍ  
ຕ່າງສຮ້າງຄອນເບັກຊັ້ນໄປວັດຟັ້ງ



# AZ-104

## NETWORK

### Intersite Connectivity



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) และเปลี่ยนกีฬัง ไม่ได้ จึงต้องลบและสร้าง Gateway ใหม่เป็นแบบ Route-based ปกติ



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 ก้าวแรกเดรสสเปช  
เหลือ แล้วเรา gland สร้าง  
VPN Gateway สำหรับ  
VNet นั้น โดยยังไม่มี  
GatewaySubnet ก่อน  
หน้า ก็จะสร้างให้อัตโนมัติ

Site-to-Site เราต้อง  
สร้างเกตเวย์ก่อน ส่วนฟิ่งเพื่อ  
สร้าง Connection หาดัน



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

Expressroute เป็นลิงค์ส่วนตัว ไม่ได้ over internet จึงตัดออกไปได้เลย

**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

Office to VNet คือ Site-to-Site เราต้องสร้างเกตเวย์ทั้งสองฝั่งเพื่อสร้าง Connection หาก



#### 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 ไม่รองรับ failover คู่กับ Expressroute จึงต้องเลือกตั้งแต่ VpnGw1 ขึ้นไป

Gateway  
Expressroute ใช้  
GatewaySubnet  
เดียวกับ VPN Gateway  
ที่ทำ Failover จึงไม่ต้อง<sup>สร้างขับเน็ตเพิ่ม</sup>

ขั้นตอนการทำ Site-to-Site ก็แค่สร้าง Gateway กันสองฝ่าย แล้วแต่ละฝ่าย สร้าง Connection หาดัน (ตั้ง Key ให้ตรงกัน)

# AZ-104

## NETWORK

### Intersite Connectivity



#### Virtual WAN

3 offices: NY, LA, Seattle, all have 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

เราไม่ใช่เชอร์วิส Virtual WAN เดียว ในนั้นจะสร้าง  
กี่ Hub ก็ได้ ข้ามรีเจ็ยบ  
กันได้