Student Name: **Weight: 3%**

Student ID: **Marks: /10**

Lab: Azure Network Services

Lab Objectives

In this lab, you'll explore how to create and manage Azure network services. You will:

1. Create an Azure Virtual Network.
2. Connect two virtual networks via peering.
3. Create a UDR (user defined route).
4. Edit a NSG (network security group).
5. Create a VPN gateway.
6. Create a point-to-site VPN gateway.

Lab Requirements

- Up to date browser
- Azure account
- Windows server virtual machine

Instructions

1. Working individually, follow the procedure below.
2. Take screenshots, as described in the *Marking Criteria* section.
3. Create a document that includes all screenshots appropriately titled and described, and then upload it to the Lab assignment drop box.
4. Be sure to include your name and student ID in the document.

Marking Criteria

Screenshots	Marks
Two networks and the ability to ping between them	/2
User defined routes	/2
Peered networks	/2
VPN gateway	/2
Point-to-site configuration and ping	/2
Total	/10

Note: This icon indicates when a screenshot is required.

📷

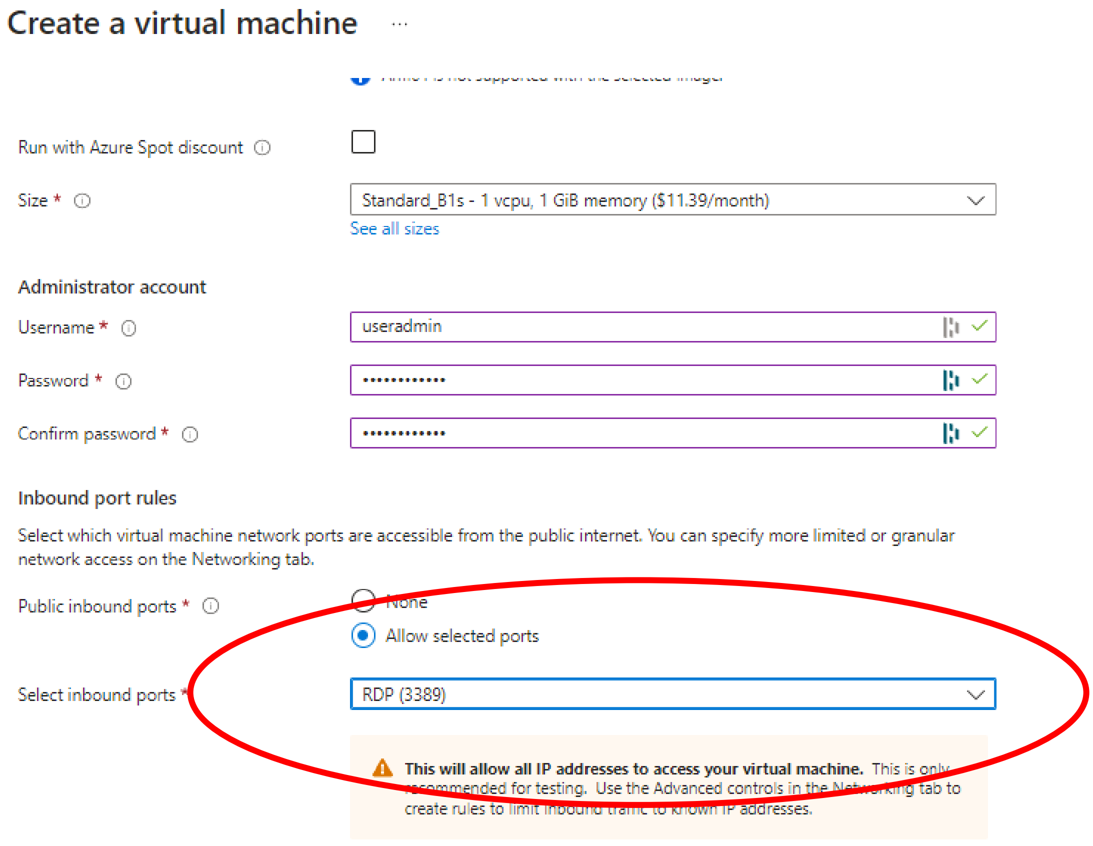
Source: Flatiron.com, Freepik, Image: screenshot_983871

Procedure

Part 1: Create an Azure Virtual Network

In a physical network, cables, switches, routers and network cards are required to communicate between computers. In virtual systems, virtual networking components are used to provide similar functions between virtual systems and resources. In previous labs, when you created a virtual machine, although several virtual components were automatically created, you do have control over those pieces.

- □ Navigate to **Virtual Machines** in the portal, click the **+ Create** button and fill out the resource group, name, availability options and type information for an inexpensive virtual machine.
- □ Scroll to the bottom of the page and note that for public inbound ports the default is to allow RDP on port 3389.



Create a virtual machine ...

Run with Azure Spot discount ☐

Size * Standard_B1s - 1 vcpu, 1 GiB memory ($11.39/month)

See all sizes

Administrator account

Username * useradmin

Password * •••••••••••••

Confirm password * •••••••••••••

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ○ None ● Allow selected ports

Select inbound ports * RDP (3389)

This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

© 2023, Microsoft Azure. Used with permission from Microsoft.

You’ve used this port in previous labs to talk to a virtual machine, but for communication, a virtual machine needs an IP address and a network card, and it needs to live in a network of some kind.

- □ Click **Next** and choose an inexpensive disk.
- □ Click **Next** to go to the *Networking* page.

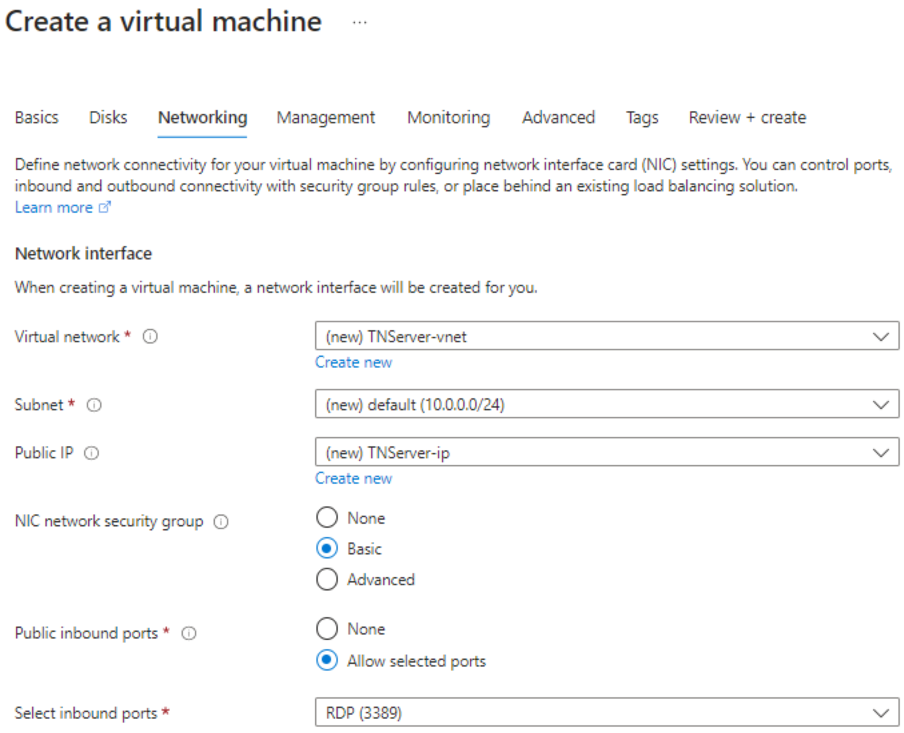
Azure has filled out the information to create a new set of network resources.

- A virtual network
- A subnet
- A public IP
- A network security group

Some of these resources have costs associated with them. For example, public IP addresses accrue costs.

Note: For more information, read: IP Address pricing (https://azure.microsoft.com/en-ca/pricing/details/ip-addresses/).

In the example below, the server is named **TNServer** and you can see the default names chosen for the components.



Create a virtual machine ...

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.
Learn more

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * : (new) TNServer-vnet
Create new

Subnet * : (new) default (10.0.0.0/24)

Public IP : (new) TNServer-ip
Create new

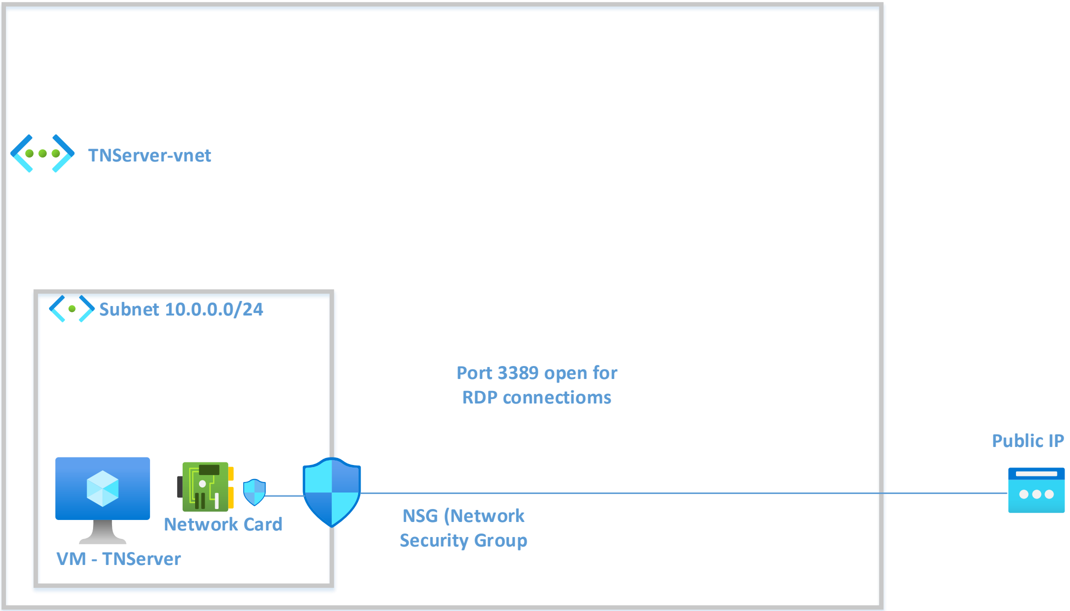
NIC network security group : ○ None ● Basic ○ Advanced

Public inbound ports * : ○ None ● Allow selected ports

Select inbound ports * : RDP (3389)

© 2023, Microsoft Azure. Used with permission from Microsoft.

The drawing below shows how the components fit together.



© 2023, Southern Alberta Institute of Technology.
This figure was designed with icons from Microsoft Azure.

□ Review and create the virtual machine.

□ When the resources are created, go to the main page for the resource group.

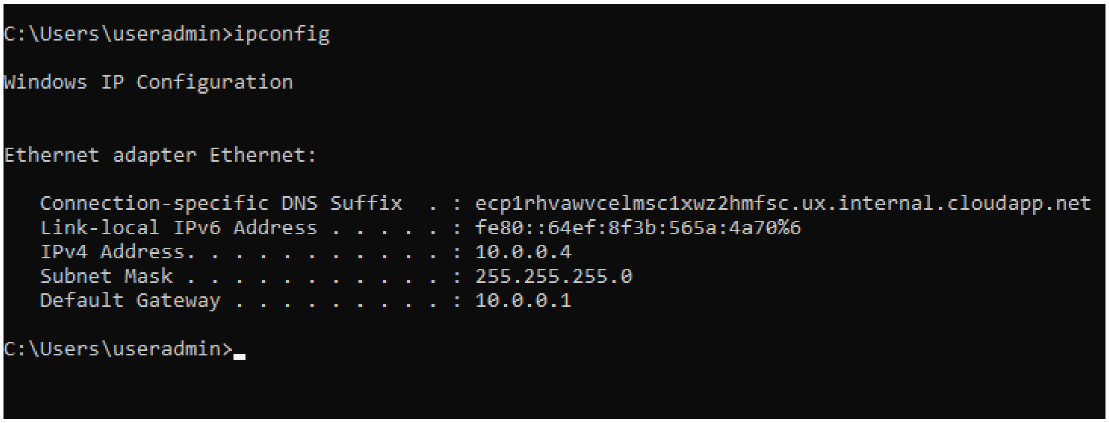
□ Select the Public IP Address, review the information and note the IP address.

□ Navigate to the main page for the virtual machine and select **Connect** from the top menu.

□ Download the RDP file, and then connect and log in to the virtual machine.

□ Check the IP information.

It is the only VM and has the address of 10.0.0.4. Note that the DG has taken 10.0.0.1.



```
C:\Users\useradmin>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : ecp1rhvawvcelmsc1xwz2hmfsc.ux.internal.cloudapp.net
   Link-local IPv6 Address . . . . . : fe80::64ef:8f3b:565a:4a70%6
   IPv4 Address. . . . . . . . . . . : 10.0.0.4
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.1

C:\Users\useradmin>_
```

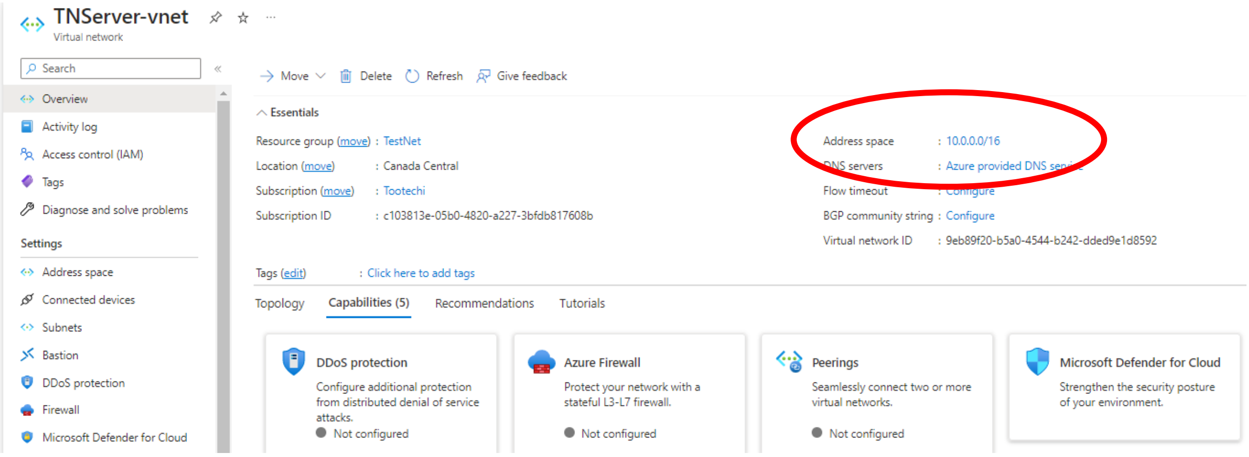
© 2023, Microsoft Azure. Used with permission from Microsoft.

Note: IP address for virtual machines start at 4 because Azure reserves 5 IP addresses within all subnets:

- 192.168.1.0: Network address
- 192.168.1.1: Reserved by Azure for the default gateway
- 192.168.1.2 and 192.168.1.3: Reserved by Azure to map the Azure DNS IPs to the Vnet space
- 192.168.1.255: Network broadcast address.

☐ Navigate to the **Virtual Networks** page in the Azure portal and select the virtual network that was created for your VM.

☐ On the main page for the virtual network, you can see the address space given to the network. You have a 10.0.0.0/16 network address and a 10.0.0.0/24 subnet address.



Resource group (move) : TestNet
Location (move) : Canada Central
Subscription (move) : Tootechi
Subscription ID : c103813e-05b0-4820-a227-3bfdb817608b
Tags (edit) : Click here to add tags

Address space : 10.0.0.0/16
DNS servers : Azure provided DNS service
Flow timeout : Configure
BGP community string : Configure
Virtual network ID : 9eb89f20-b5a0-4544-b242-dded9e1d8592

DDoS protection
Configure additional protection from distributed denial of service attacks.
● Not configured

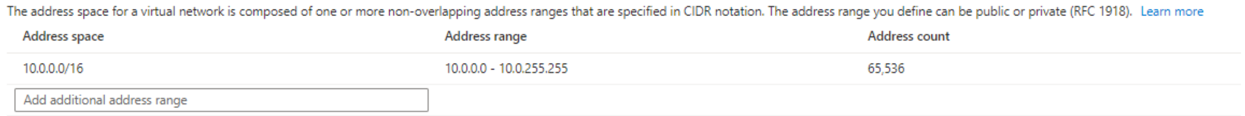
Azure Firewall
Protect your network with a stateful L3-L7 firewall.
● Not configured

Peerings
Seamlessly connect two or more virtual networks.
● Not configured

Microsoft Defender for Cloud
Strengthen the security posture of your environment.

© 2023, Microsoft Azure. Used with permission from Microsoft.

☐ Select **Address Space** from the blade menu and review all the information for the virtual network's address space, including the number of addresses in the space.



The address space for a virtual network is composed of one or more non-overlapping address ranges that are specified in CIDR notation. The address range you define can be public or private (RFC 1918). Learn more

Address space	Address range	Address count
10.0.0.0/16	10.0.0.0 - 10.0.255.255	65,536
Add additional address range		

© 2023, Microsoft Azure. Used with permission from Microsoft.

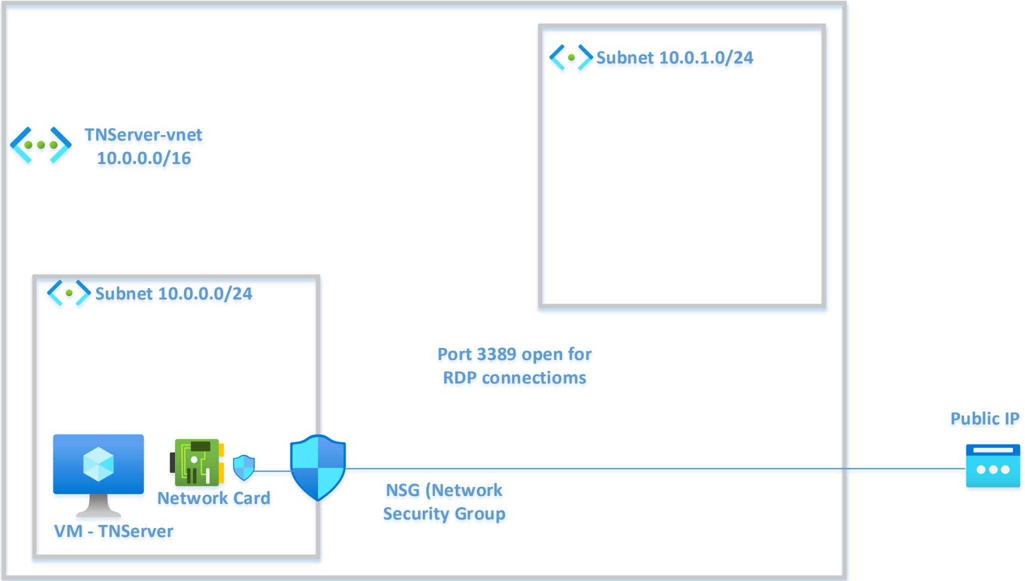
☐ Select **Subnets** from the blade menu and select **+ Subnet** from the top menu.

☐ Give the subnet a name. Note that it recommends an address of 10.0.1.0/24.

Subnet addresses within a virtual network cannot overlap, just like subnet addresses in a physical network cannot overlap.

☐ Save the new subnet.

You now have a second empty subnet within your virtual network.



© 2023, Southern Alberta Institute of Technology.
This figure was designed with icons from Microsoft Azure.

☐ Go back to the **Virtual Networks** main page and select **+ Create** from the top menu.

☐ Select the resource group you used to create the VM, give the network a name and select **Canada East** as the region.

☐ Click **Next** to go to the IP page.

Note: The recommended IP address for this network is 10.1.0.0/16.

Azure recommends you use IP addresses from RFC1918.

- 10.0.0.0 – 10.255.255.255 (10/8 prefix)
- 172.16.0.0 – 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 – 192.168.255.255 (192.168/16 prefix)

Note: For more information about networking limits, read: Azure Service limits (https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/azure-subscription-service-limits#networking-limits)

The portal has also recommended a subnet of 10.1.0.0/24. A /24 subnet has 256 addresses minus the 5 reserved mentioned above.

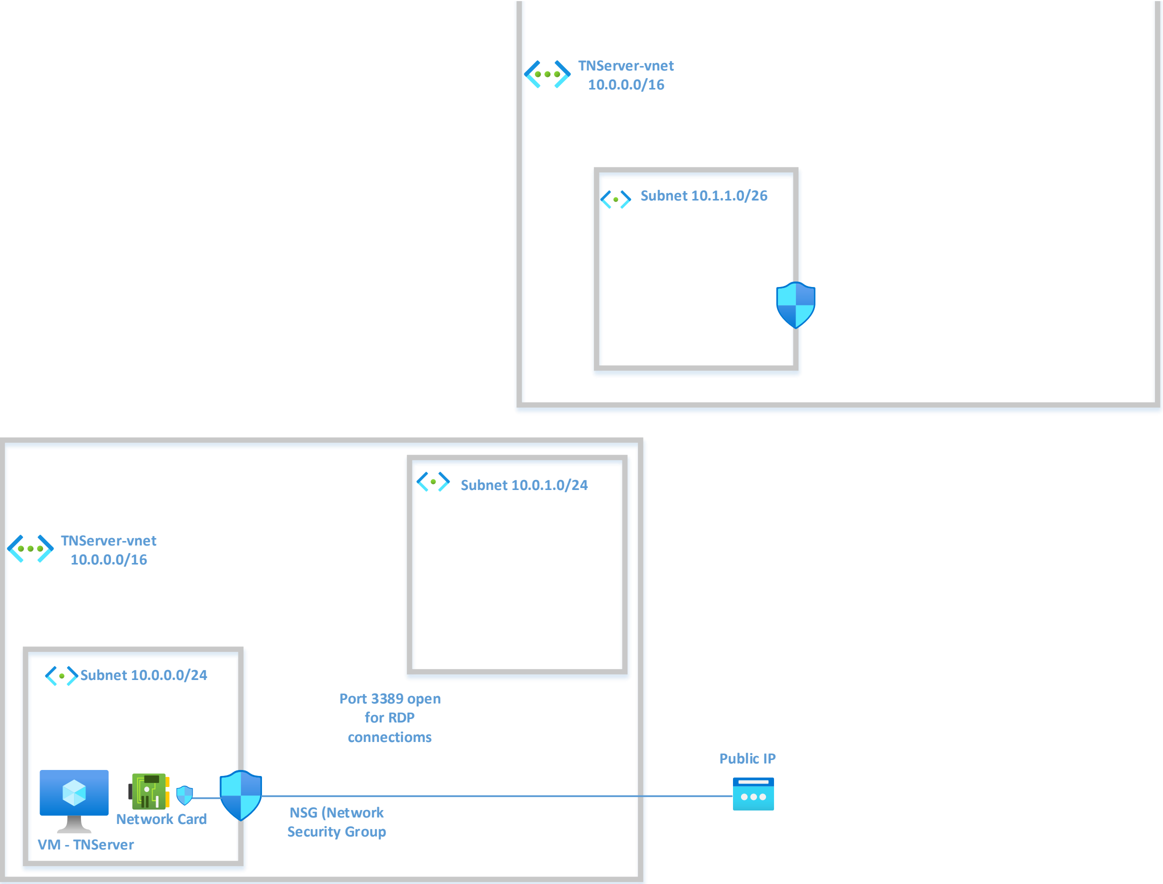
☐ Delete that subnet and add a new one.

☐ Type in **10.0.1.0/26** as the subnet range and it will warn you that this address is not within the network address space.

☐ Type in **10.1.1.0/26** and create the new subnet.

How many IP addresses will be in the new subnet?

☐ Review and create the network. You now have a second network in the cloud with a subnet.



© 2023, Southern Alberta Institute of Technology.
This figure was designed with icons from Microsoft Azure.

Part 2: Connect Two Virtual Networks via Peering

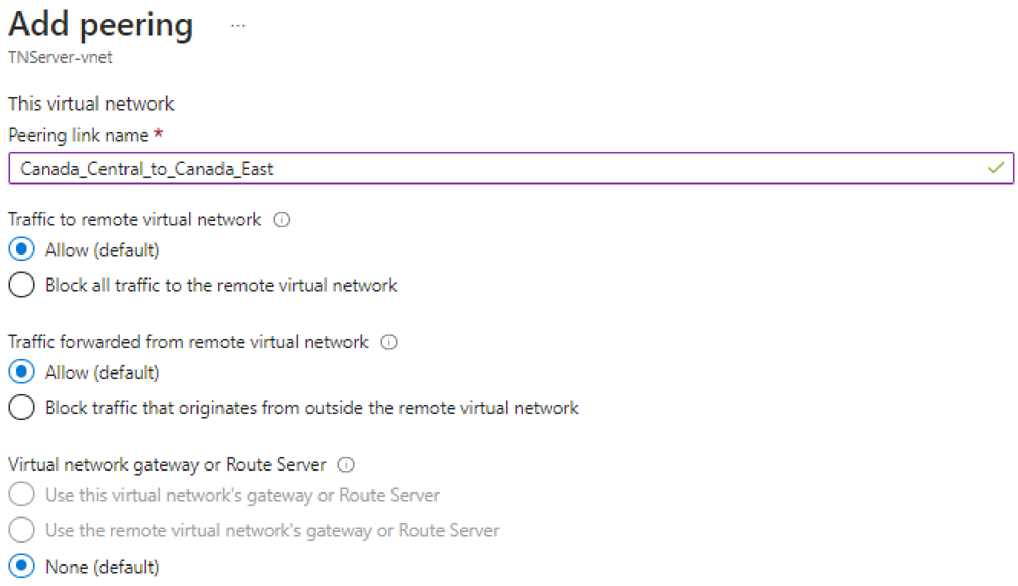
Azure virtual network peering allows you to connect virtual networks together to appear as a single network. The traffic between the networks runs on the Microsoft backbone. You can connect virtual networks in the same region together (Microsoft calls this Virtual Network Peering) and you can connect virtual networks in different regions (Microsoft calls this Global Virtual Network Peering).

The virtual networks you created in the previous section are in two different regions, so in this section you are going to connect them.

□ Go to the main page for the first network you created and select **Peerings** from the blade menu.

□ Click the **+ Add** button.

□ Name the connection and note the traffic options.



Add peering ...

TNServer-vnet

This virtual network

Peering link name *

Canada_Central_to_Canada_East ✓

Traffic to remote virtual network ⓘ

● Allow (default)

○ Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ

● Allow (default)

○ Block traffic that originates from outside the remote virtual network

Virtual network gateway or Route Server ⓘ

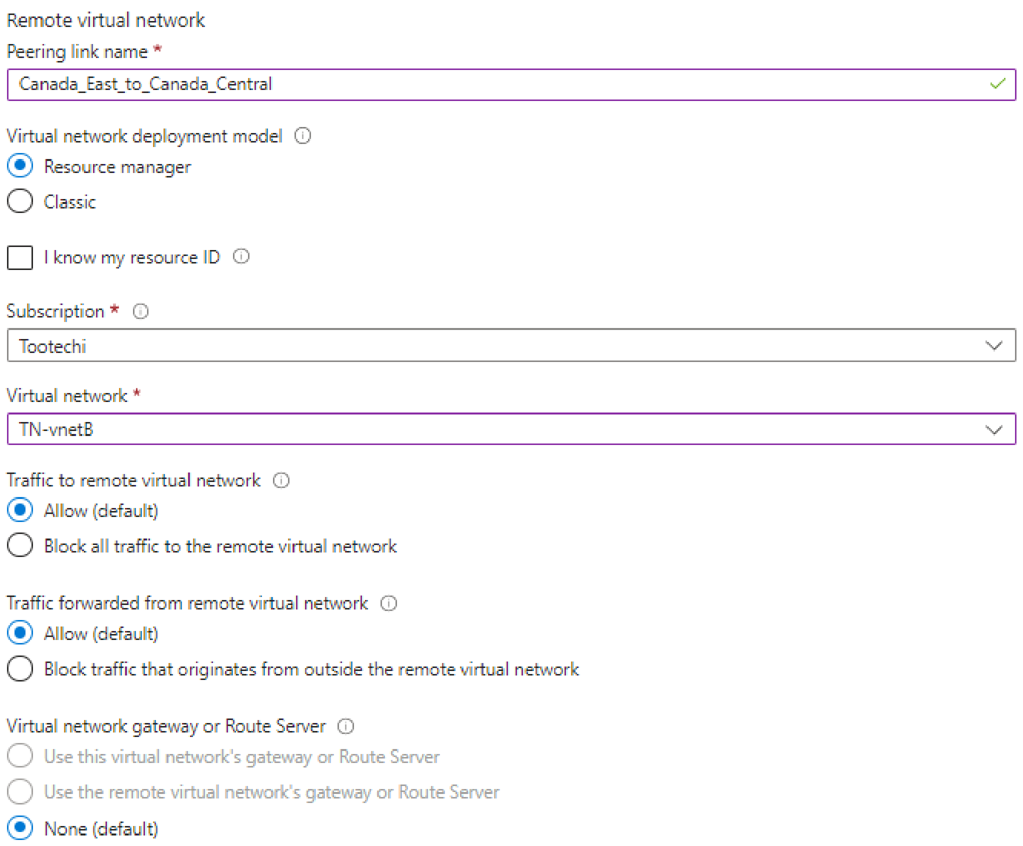
○ Use this virtual network's gateway or Route Server

○ Use the remote virtual network's gateway or Route Server

● None (default)

© 2023, Microsoft Azure. Used with permission from Microsoft.

□ Scroll down to the *Remote Virtual Network* section and configure the same information for your second network.



Remote virtual network

Peering link name *

Canada_East_to_Canada_Central ✓

Virtual network deployment model ⓘ

● Resource manager

○ Classic

□ I know my resource ID ⓘ

Subscription * ⓘ

Tootechi

Virtual network *

TN-vnetB

Traffic to remote virtual network ⓘ

● Allow (default)

○ Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ

● Allow (default)

○ Block traffic that originates from outside the remote virtual network

Virtual network gateway or Route Server ⓘ

○ Use this virtual network's gateway or Route Server

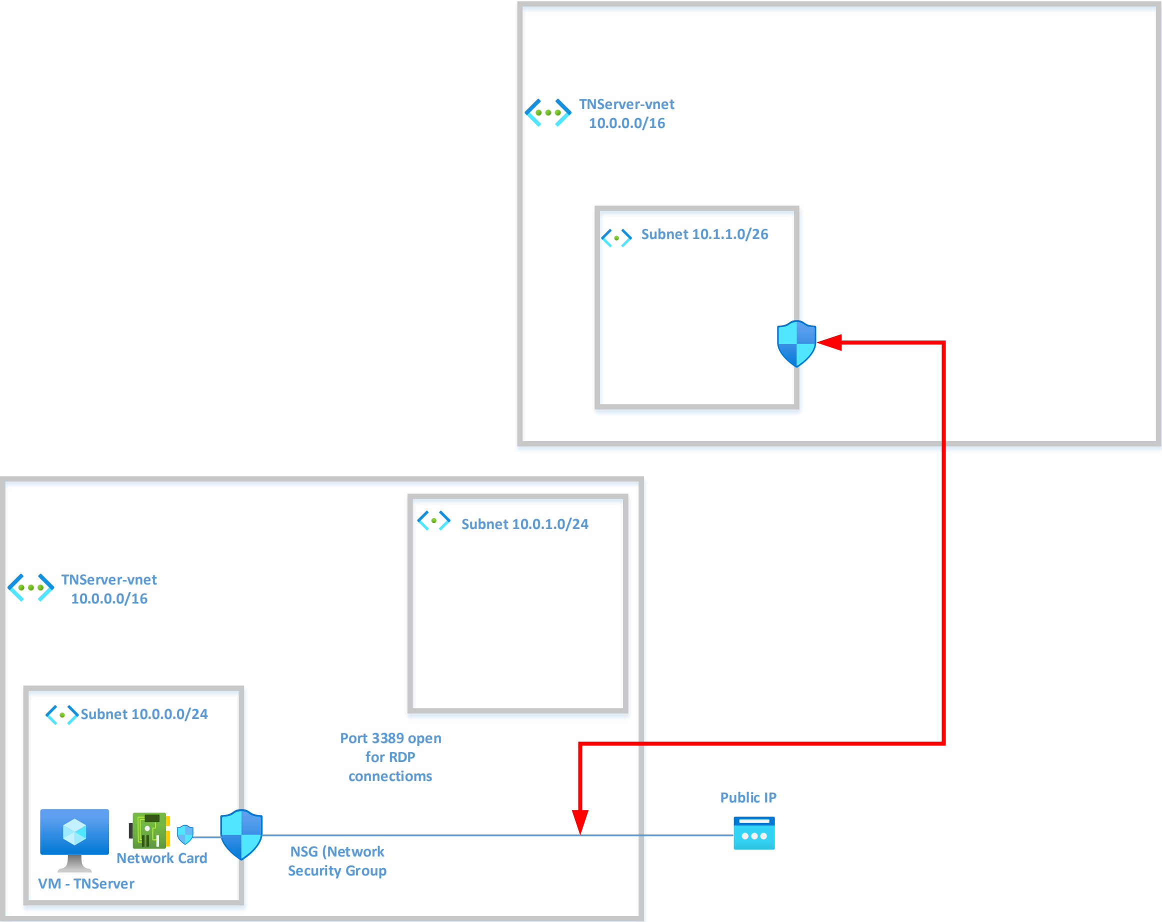
○ Use the remote virtual network's gateway or Route Server

● None (default)

© 2023, Microsoft Azure. Used with permission from Microsoft.

☐ Add the peering

☐ When the resource is complete, go to your second network. You should be able to see the peering in that network as well.



© 2023, Southern Alberta Institute of Technology.
This figure was designed with icons from Microsoft Azure.

☐ Create a second virtual machine. However, when you get to the networking page, select your second virtual subnet, so that you have one virtual machine in each subnet in each virtual network.

☐ Find the private IP addresses for each of the virtual machines and RDP into each of them.

☐ On each VM, set the operating system firewall to allow ICMP traffic.

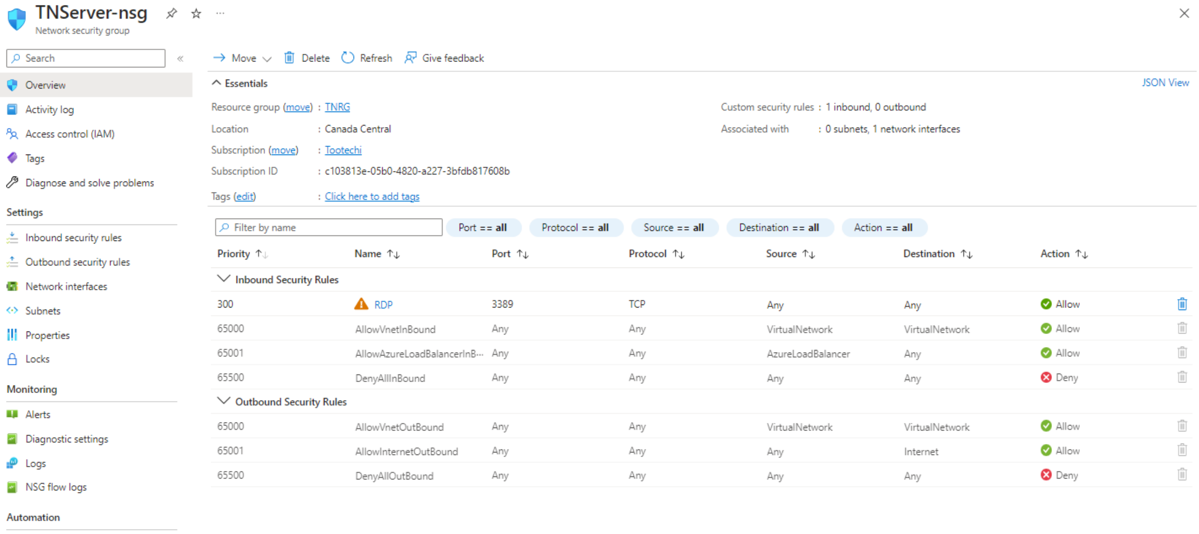
☐ Ping between the virtual machines by private IP address.

Part 3: Edit a Network Security Group (NSG)

A network security group (NSG) is a set of security rules that filter traffic between resources. An NSG can be applied to a network card or a subnet and can filter both inbound and outbound traffic. One of the major benefits of NSGs is that they can be associated more than once (in the same region), so you don’t need to repeat configurations.

- ☐ Go to the main page for each of your virtual machines and select **Networking** from the blade menu.
- ☐ In the *IP Configuration* box, choose a network interface to see the rules applied to that interface.
- ☐ In the search box, type **Network Security Groups** and go to the main page. You will see the two NSGs that were created by default.
- ☐ Select one of them and then select **Network Interfaces** from the blade menu. Note the network card it is connected to.
- ☐ Select **Subnets** from the blade menu and note that no NSGs were created by default for the subnets.

  This would be where you could attach an NSG to a subnet.
- ☐ Select **Overview** from the blade menu to see the full set of inbound and outbound rules in this NSG.



TNServer-nsg
Network security group

Essentials

Resource group (move) : TNRG
Location : Canada Central
Subscription (move) : Tootechi
Subscription ID : c103813e-05b0-4820-a227-3bfdb817608b
Tags (edit) : Click here to add tags
Custom security rules : 1 inbound, 0 outbound
Associated with : 0 subnets, 1 network interfaces

Port == all | Protocol == all | Source == all | Destination == all | Action == all

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
Inbound Security Rules						
300	⚠ RDP	3389	TCP	Any	Any	✓ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerInB···	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	✓ Allow
65500	DenyAllOutBound	Any	Any	Any	Any	✗ Deny

© 2023, Microsoft Azure. Used with permission from Microsoft.

Note: To see the default rules and the rule properties, read: Network security groups (https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview).

The rules are executed in numerical order, so look at the inbound security rules:

- 300 allows RDP to and from any source/destination
- 65000 allows all inbound traffic from inside the virtual network – this allows virtual machines in different subnets to communicate
- 65001 allows Azure load balancer traffic
- 65500 denies all other traffic – this includes traffic from your second virtual network, so this is the one denying our ping traffic.

Let’s suppose that for security reasons you want to block the ping traffic between the two machines. To do this, you need to deny inbound ICMP traffic.

☐ Select **Inbound Security Rules** from the blade menu.

☐ Click **+ Add** on the top menu.

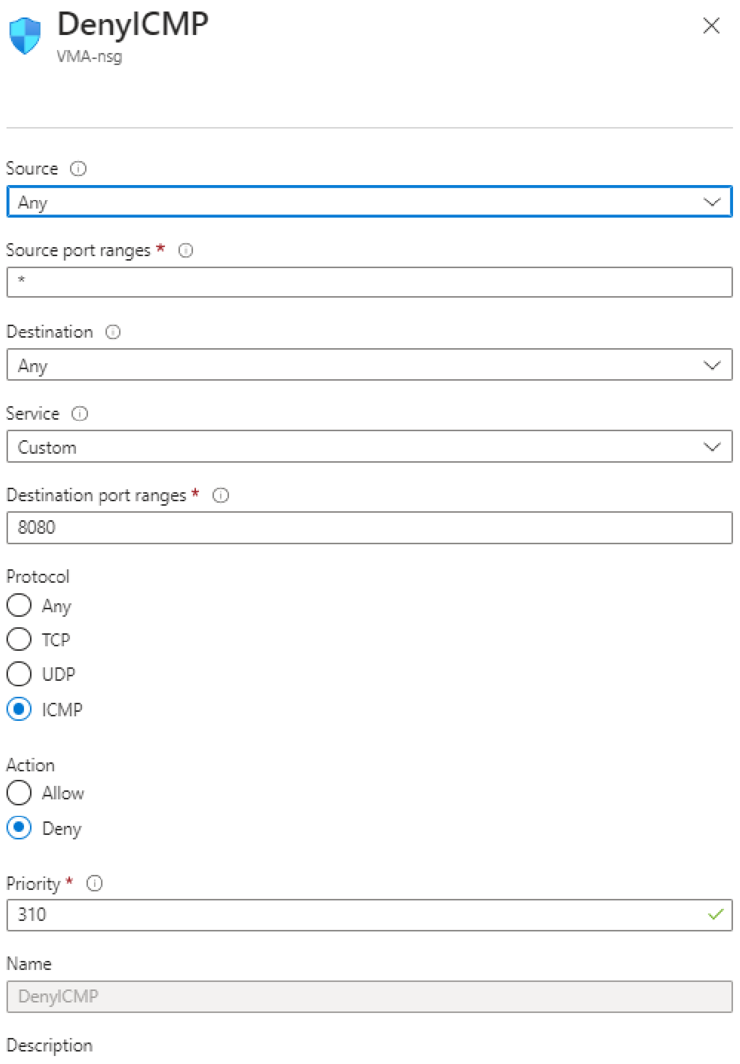
☐ Leave the Source and Destination as **Any**.

☐ Select the *Service* drop down arrow and see some of the pre-built rules you could add. ICMP is not one of them.

☐ Select **ICMP** under the *protocol* section and **Deny** in the *action* section.

The priority is set to 310 by default, but that means that rule is read and checked after the RDP rule.

☐ Name and add the rule.



DenyICMP

VMA-nsg

Source: Any

Source port ranges *: *

Destination: Any

Service: Custom

Destination port ranges *: 8080

Protocol

○ Any
○ TCP
○ UDP
● ICMP

Action

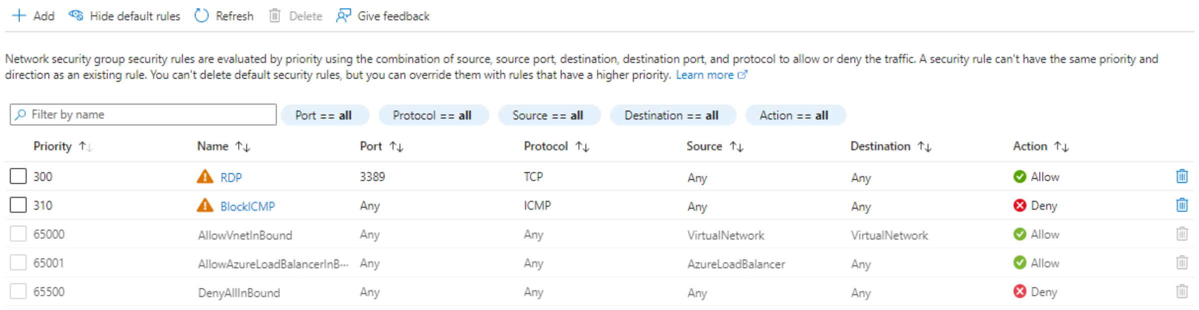
○ Allow
● Deny

Priority *: 310

Name: DenyICMP

Description

□ You should now be able to see the rule, although it may take several minutes before the rule takes effect.

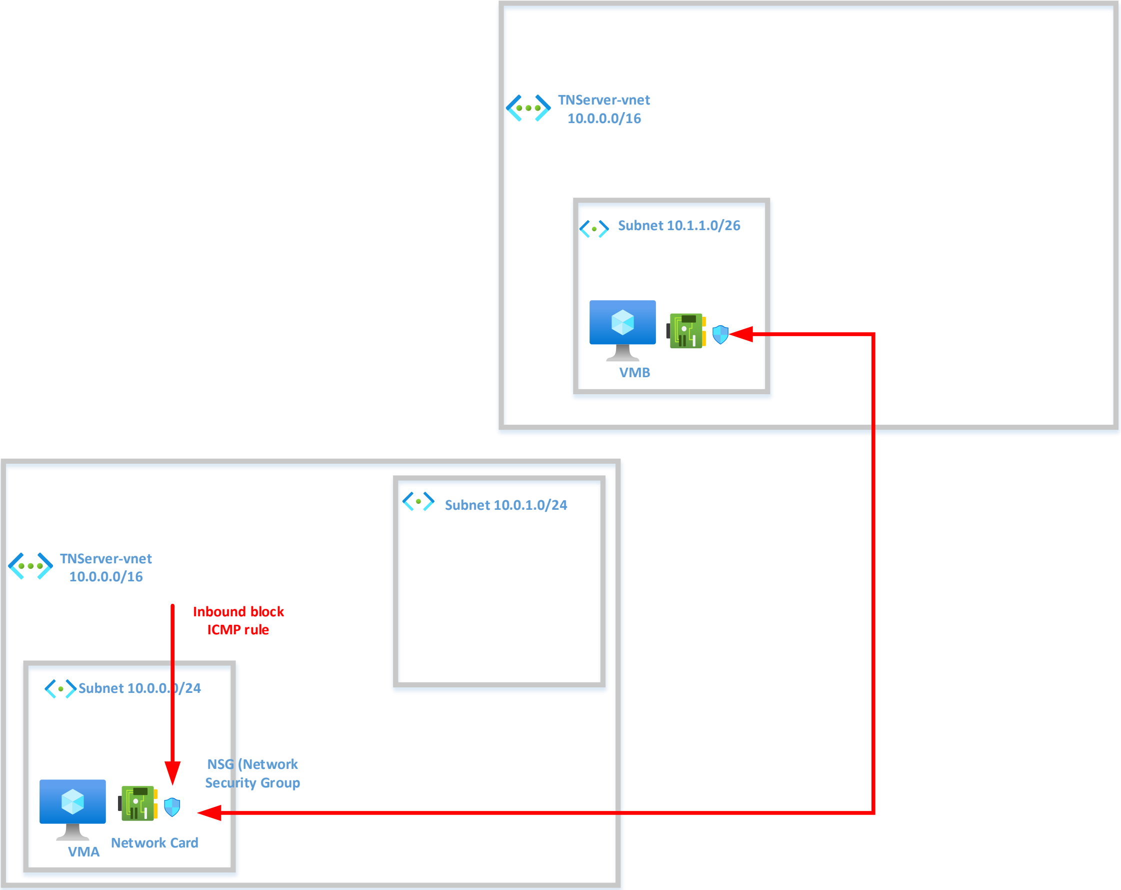


Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. Learn more

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
□ 300	⚠ RDP	3389	TCP	Any	Any	✓ Allow
□ 310	⚠ BlockICMP	Any	ICMP	Any	Any	✗ Deny
□ 65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
□ 65001	AllowAzureLoadBalancerInB···	Any	Any	AzureLoadBalancer	Any	✓ Allow
□ 65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny

Creating the security rule on VMA shown in the drawing below will block any ICMP traffic coming from VMB, and VMB won't be able to ping VMA but VMA will still be able to ping VMB.

☐ Test this with your VMs.



© 2023, Southern Alberta Institute of Technology.
This figure was designed with icons from Microsoft Azure.

You could go to the NSG on VMB and create the same rule to block incoming ICMP traffic. Instead, you'll create a new NSG and associate it to the 10.1.1.0/26 subnet.

☐ Go to the main page for the subnet and select **+ Create** from the top menu.

☐ Select your resource group, name it **BlockICMP**, put it in the same region as your 10.1.1.0/26 subnet, and then create the NSG.

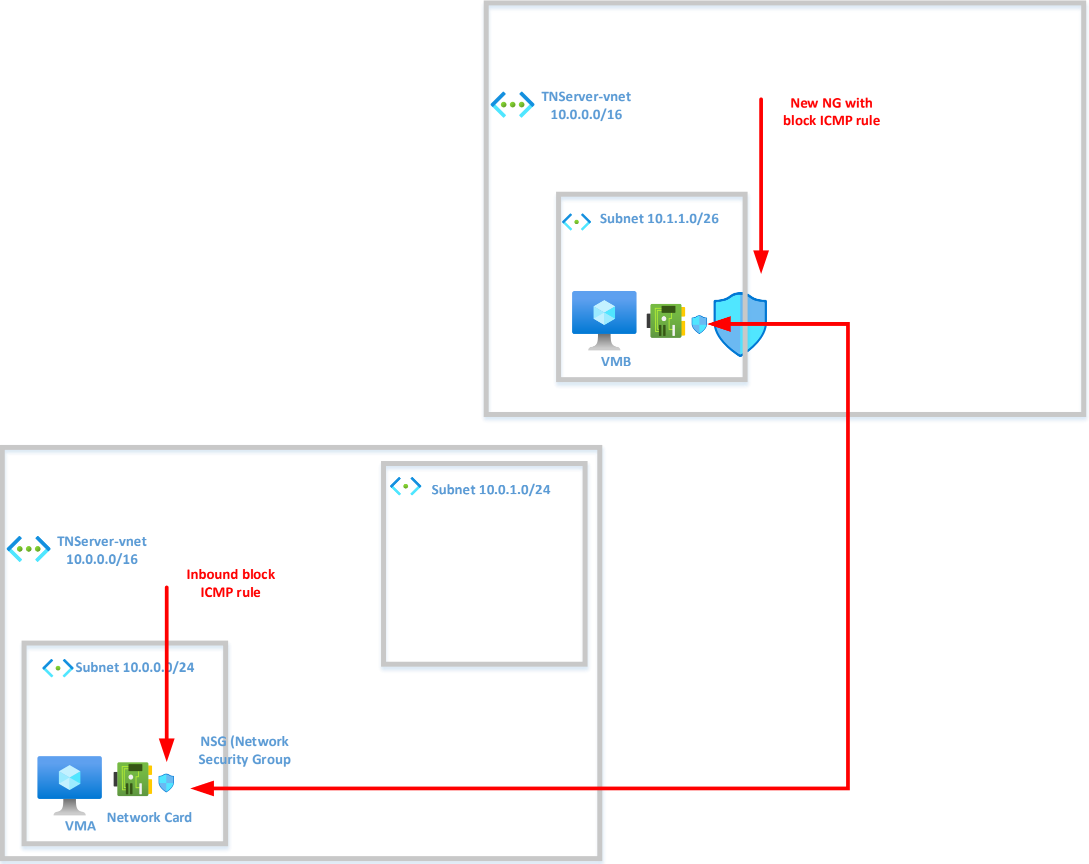
☐ When complete, add the block ICMP rule to the inbound traffic.

☐ From the main page for that NSG, select **Subnets** from the blade menu.

☐ Select **+ Associate** from the top menu.

☐ Select the virtual network and subnet that you want to associate it to. In this case, you only have one virtual network and subnet in that region, so leave the defaults and click **OK**.

☐ Now, pings should be blocked on the network card of VMA and the subnet of VMB, so you should not be able to ping in either direction. Test it after a few minutes.



© 2023, Southern Alberta Institute of Technology.
This figure was designed with icons from Microsoft Azure.

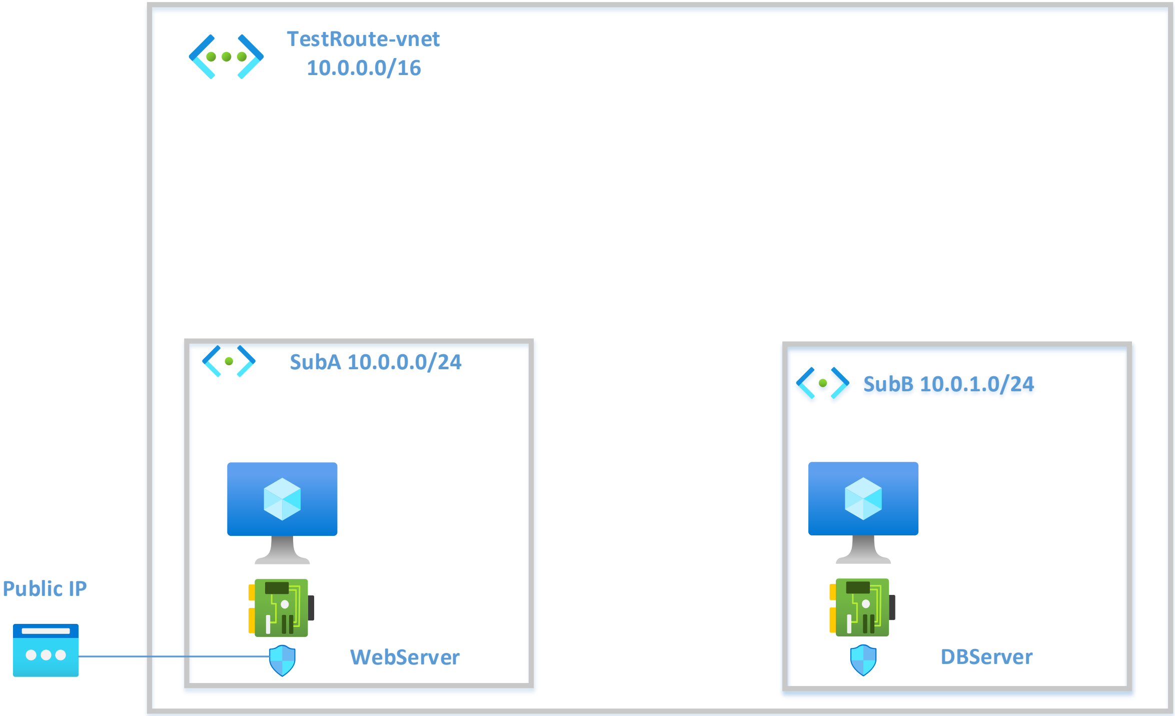
☐ Delete the resources to avoid accruing costs

Part 4: Create a User-Defined Route

Just like on-prem networks, Azure uses routes to determine the traffic flow between networks, subnets, the internet and virtual machines. In the last section you used NSGs to block or allow different types of traffic. Although this is an important security mechanism, a company may want to direct traffic between components in a very specific way.

In this part of the lab, you'll use as an example a scenario in which a small company has a web server that customers can log in to see a list of everything they have previously ordered, as well as a database server that contains all the orders. These are highly specialized applications and each needs to run on its own virtual machine. The web server will be public facing so the customers can access it but the database is accessed by the web server only, so you want it securely away from any public connection.

You are going to create a single network with two subnets. One of your subnets will contain the public-facing virtual machine that would contain a web server. The other subnet will contain the isolated back-end database server.



© 2023, Southern Alberta Institute of Technology.
This figure was designed with icons from Microsoft Azure.

☐ Create the network with the two subnets and VMs shown in the picture above.

Note: Don’t worry about the applications. Focus only on network connectivity.

☐ Configure both VM firewalls to allow ICMP traffic, and then ping between the two VMs’ private IP addresses.

You can ping between the VMs because, by default, Azure creates a route table with default routes for each subnet in a network. You can’t see the default route table, but if you want to override it, create a new route table.

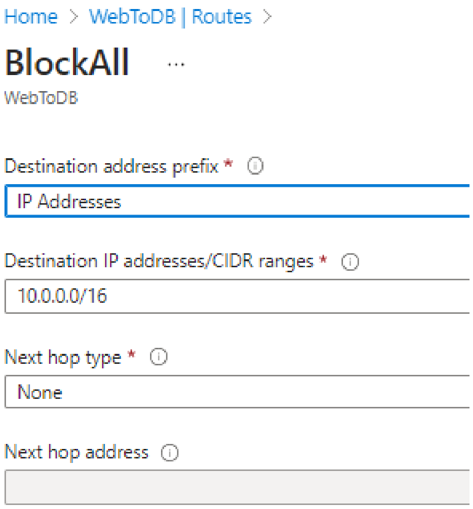
Note: To see the default routes, see: Virtual network traffic routing (https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview).

☐ In the Azure portal, search for and navigate to the **Route Tables** tool.

☐ Select **+ Create** and enter the resource group, region and name.

☐ Note the **Propagate Gateway Routes** selection and read the information.

- □ Create the route table.
- □ When the resource is created, go to its main page and notice that it has no routes or subnets associated with it yet.
- □ Select **Subnets** from the blade menu and associate your two subnets.
- □ Select **Routes** from the blade menu.
- □ Start by blocking all traffic between the subnets. Select **+ Add** from the top menu and create a BlockAll route.


Home > WebToDB | Routes >

BlockAll ...

WebToDB

Destination address prefix * : IP Addresses

Destination IP addresses/CIDR ranges * : 10.0.0.0/16

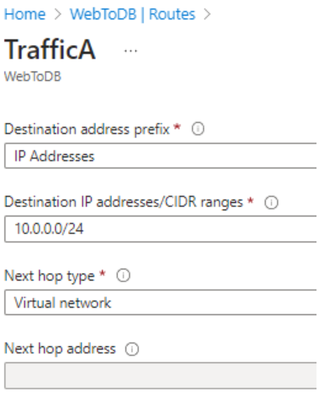
Next hop type * : None

Next hop address :

© 2023, Microsoft Azure. Used with permission from Microsoft.

This may take a few minutes to take effect.

- □ Now all traffic, by IP address, has no next hop. If you try pinging now it should fail.
- □ Create two routes, one for each of the subnets. (Only one of them is shown below.)


Home > WebToDB | Routes >

TrafficA ...

WebToDB

Destination address prefix * : IP Addresses

Destination IP addresses/CIDR ranges * : 10.0.0.0/24

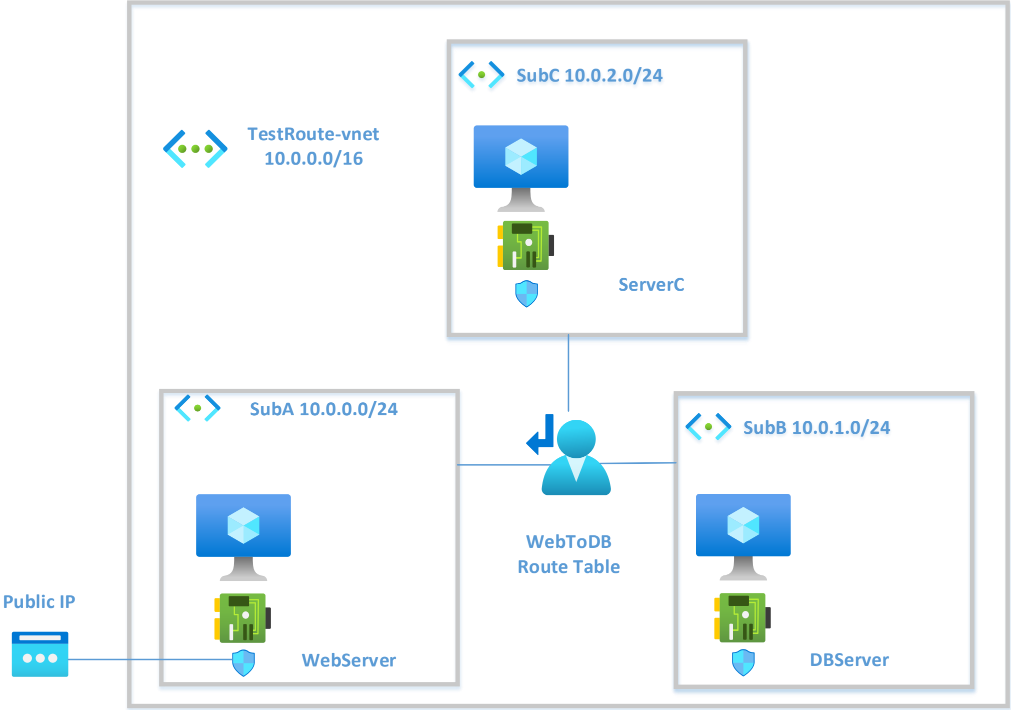
Next hop type * : Virtual network

Next hop address :

© 2023, Microsoft Azure. Used with permission from Microsoft.

☐ When the routes take effect, you should be able to ping between the subnets again.

☐ To test this further, create a third subnet in the network with a virtual machine and associate the subnet with the route table. Set the firewall in the new virtual machine to allow ICMP traffic.



© 2023, Southern Alberta Institute of Technology.
This figure was designed with icons from Microsoft Azure.

☐ Test that you are still able to ping between subnets A and B, but not subnet C.

☐ Delete your resources to avoid accruing costs.

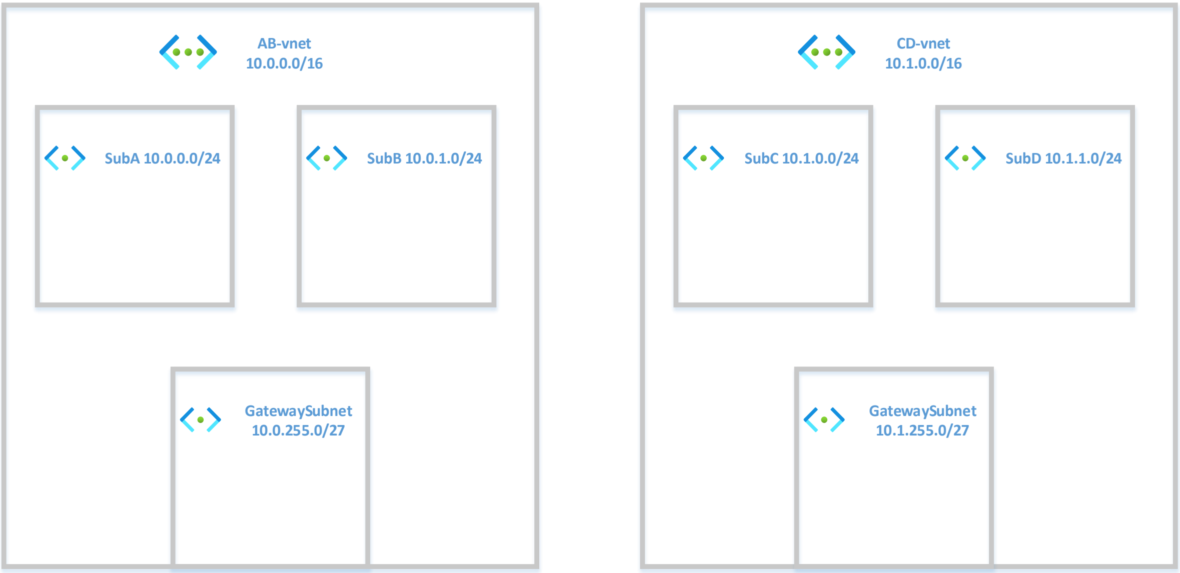
Section 5: Create a VPN Gateway

Earlier in this lab, you created a peering connection between two virtual networks in the cloud. Those connections run over the Microsoft backbone and, while the traffic is private, it is not encrypted. Another way to connect two cloud networks is through a VPN gateway that uses an encrypted tunnel.

To do this, each network requires a gateway subnet. Every network connected to the VPN gateway requires a gateway subnet that has the IP addresses that will be used by the virtual network gateway resources. That subnet must be named **GatewaySubnet** and Microsoft recommends you use a /27 or /28 for the IP addresses.

☐ Create the networks and subnets shown in the diagram below. Make sure you name the gateway subnet correctly.

It's common to put the gateway subnet at the end of the IP address range to allow more subnets to be created easily if necessary.



© 2023, Southern Alberta Institute of Technology.
This figure was designed with icons from Microsoft Azure.

The next step is to deploy a VPN gateway in each of the gateway subnets.

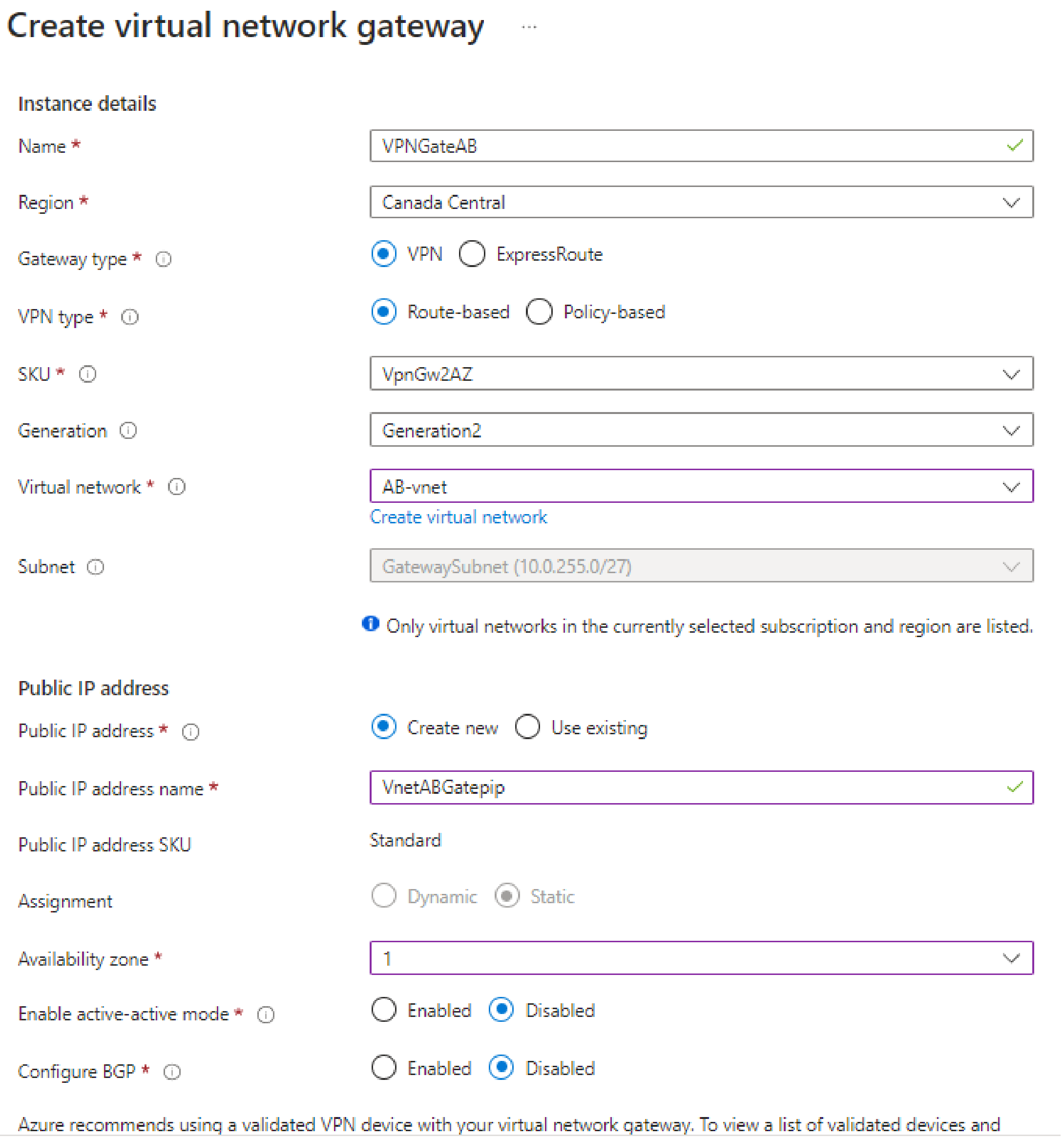
☐ Search for and navigate to the **Virtual Network Gateways** tool.

☐ Select **+ Create** from the top menu, name it and set the region.

☐ Next select **VPN**, **Route Based** and the **VpnGw2AZ** SKU**.**

Note: Read more about these selections at: [About VPN Gateway configuration settings](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings) (https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings).

☐ Select the appropriate virtual network and fill out the information as shown below.



Create virtual network gateway ...

Instance details

Name *	VPNGateAB ✓
Region *	Canada Central
Gateway type * ⓘ	● VPN ○ ExpressRoute
VPN type * ⓘ	● Route-based ○ Policy-based
SKU * ⓘ	VpnGw2AZ
Generation ⓘ	Generation2
Virtual network * ⓘ	AB-vnet Create virtual network
Subnet ⓘ	GatewaySubnet (10.0.255.0/27)

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

Public IP address

Public IP address * ⓘ	● Create new ○ Use existing
Public IP address name *	VnetABGatepip ✓
Public IP address SKU	Standard
Assignment	○ Dynamic ● Static
Availability zone *	1
Enable active-active mode * ⓘ	○ Enabled ● Disabled
Configure BGP * ⓘ	○ Enabled ● Disabled

Azure recommends using a validated VPN device with your virtual network gateway. To view a list of validated devices and

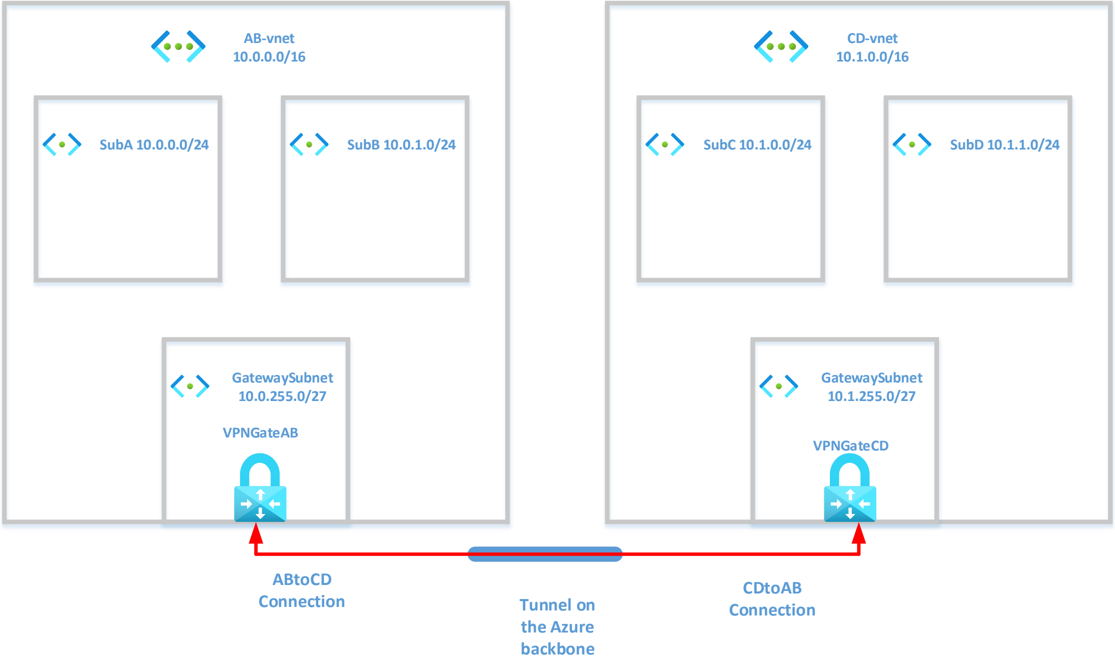
© 2023, Microsoft Azure. Used with permission from Microsoft.

☐ Create the VPN gateway in the other network with the appropriate names and the same selections.

It takes up to 45 minutes for the resources to be created.

The last step is to create the connection between the two VPN gateways.

□ Go to the main page for one of the VPN gateways and select **Connections** from the blade menu.



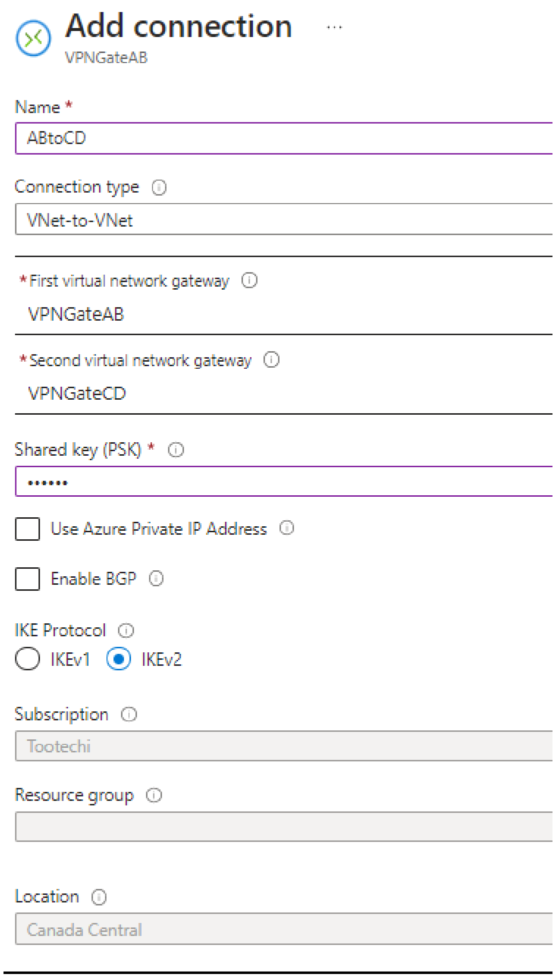
© 2023, Southern Alberta Institute of Technology.
This figure was designed with icons from Microsoft Azure.

□ Select **+ Add** from the top menu and select **Vnet to Vnet** connection.

□ In the second virtual network gateway box, select your other gateway.

Note: If it is grayed out, then the resource hasn't been created yet.

□ Use **abc123** as the shared key. This is a common test value.



Add connection ...
VPNGateAB

Name *
ABtoCD

Connection type ⓘ
VNet-to-VNet

*First virtual network gateway ⓘ
VPNGateAB

*Second virtual network gateway ⓘ
VPNGateCD

Shared key (PSK) * ⓘ
••••••

☐ Use Azure Private IP Address ⓘ

☐ Enable BGP ⓘ

IKE Protocol ⓘ
○ IKEv1 ● IKEv2

Subscription ⓘ
Tootechi

Resource group ⓘ

Location ⓘ
Canada Central

© 2023, Microsoft Azure. Used with permission from Microsoft.

☐ Go to the other VPN gateway and create the connection in the other direction.

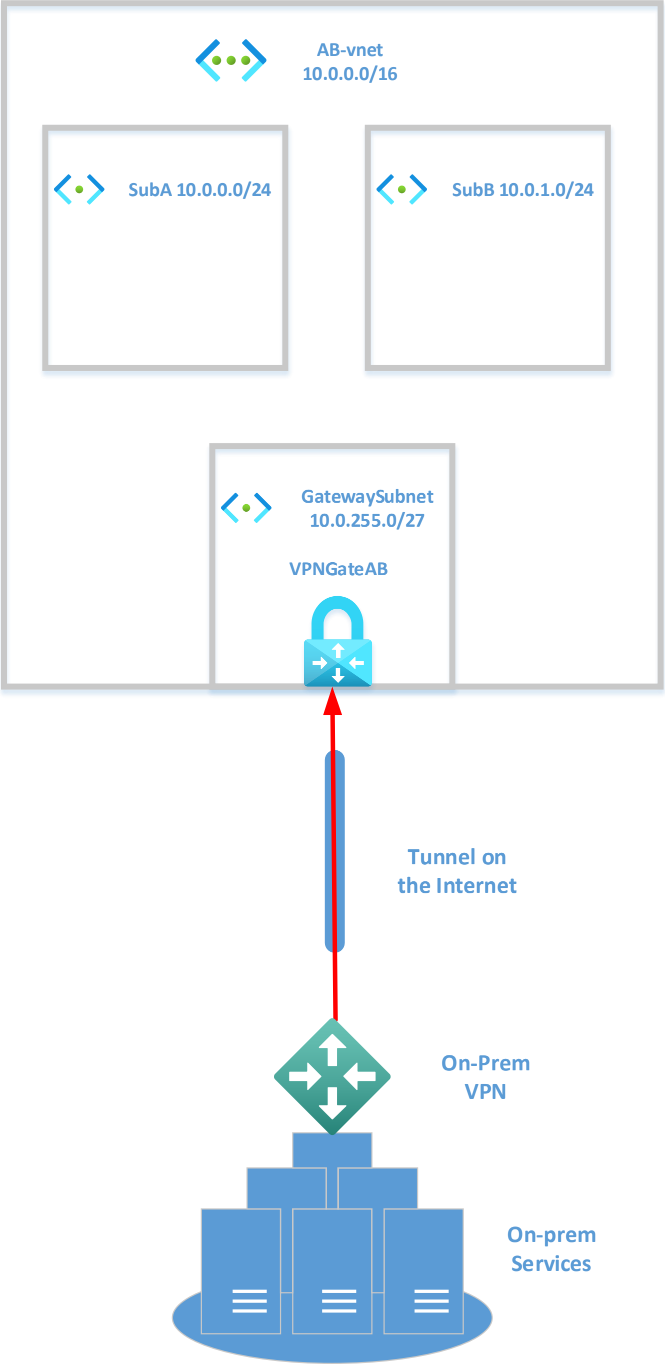
☐ Test the connection when the state of the connections changes from *updating* or *unknown*, to *connected*.

☐ Create a virtual machine in each network and test the connection.

Part 6: Create a Point-to-Site VPN Gateway

The networks that you have created so far have all been on the cloud but many companies use a hybrid model and have resources in both the cloud and on-prem. For example, if want to connect to your cloud network from your on-prem data center but you don't want to buy a dedicated line, an Azure VPN Gateway would allow you to talk between your on-prem data center and cloud networks through an encrypted tunnel on the public internet. If you have a single device in a remote location, you can use the VPN gateway to create a point-to-site connection between that device and your Azure networks.

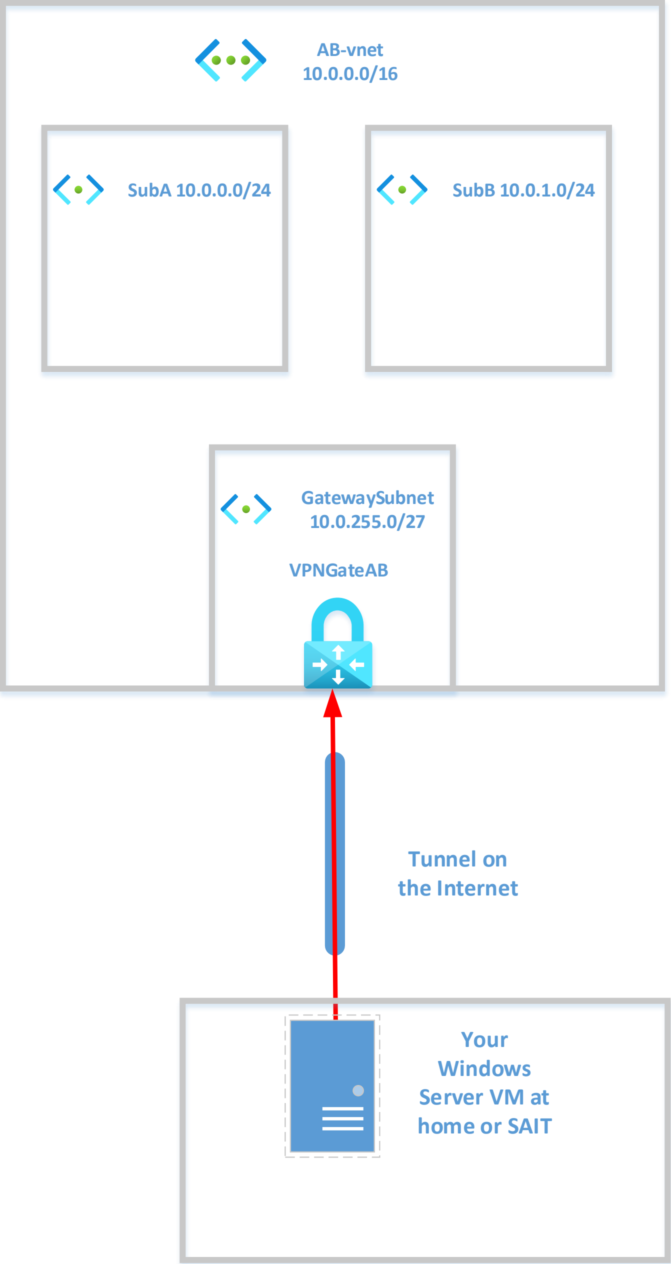
For more information on these configurations, see: Tutorial: Create a site-to-site VPN connection in the Azure portal (https://learn.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal).



© 2023, Southern Alberta Institute of Technology.
This figure was designed with icons from Microsoft Azure.

☐ Create a point-to-site connection between your Windows server virtual machine and your cloud network using certificates.

Note: Use the article: Configure server settings for P2S VPN Gateway connections (https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal) for help.



© 2023, Southern Alberta Institute of Technology.
This figure was designed with icons from Microsoft Azure.