

# AZURE VIRTUAL NETWORK

By Aavisek Choudhury  
MCSE Cloud Platform &  
Infrastructure  
(<http://whyazure.in>)

# CHAPTERS

**01**

Walkthrough with the Azure VNET

**02**

Few use cases of Azure VNET

**03**

Creation of Azure VNET – Things you should know

**04**

Lab 1: Create VNETS – Quick Create

**05**

Lab 2: Create VNETS – Custom Create

**06**

Lab 3: Create VNETS with the XML configuration file

**07**

Site to Site VPN

**08**

Point to Site VPN with (Lab 4: Create point to site VPN)

**09**

Azure Express route

**10**

Lab 5: Create Azure VNET to VNET VPN

# WALKTHROUGH-AZURE VIRTUAL NETWORK

## What is a Azure virtual network or VNET?

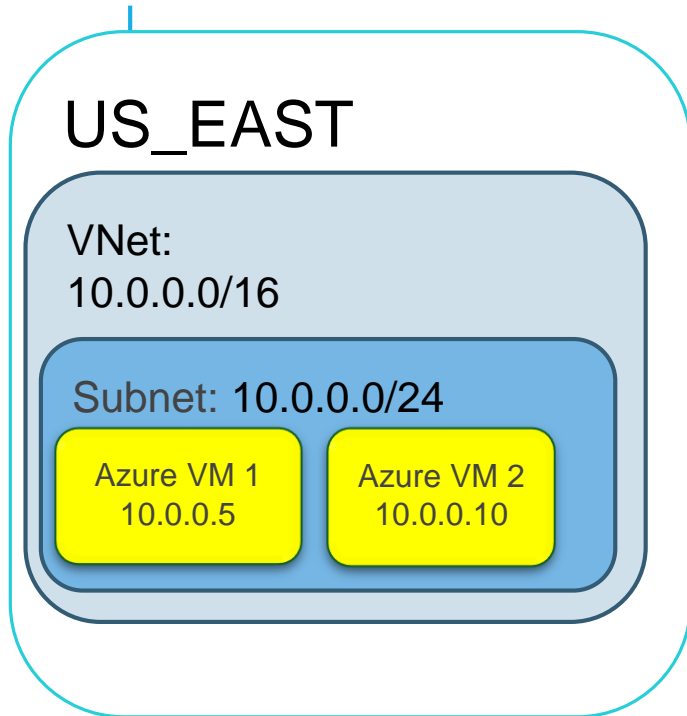
Virtual networks (**VNets**) are used in Azure to provide a layer of security and isolation to your services.

VMs and services that are part of the same virtual network can access each other.

By default, services outside the virtual network cannot connect to services within the virtual network. You can, however, configure the network to allow access to the external service.

Services that talk to each other within a virtual network do not travel through the Azure Load Balancer, which gives you better performance.

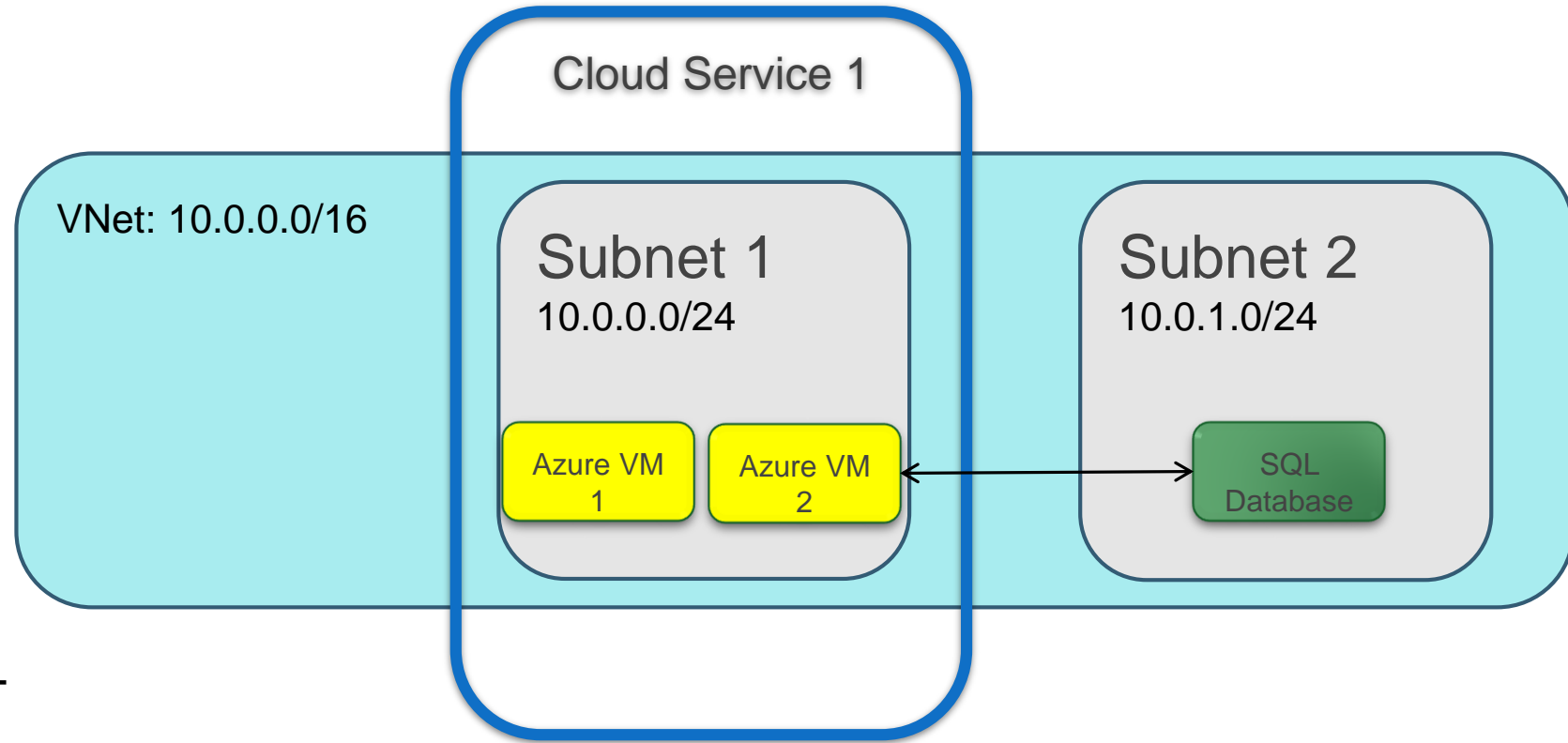
# COMMON EXAMPLE



Two VM's resides in the same VNET

## Business Requirement

Let's say you have a front-end web application running in a cloud service using a back-end database running in a virtual machine. You can put the back-end database in the same virtual network as the cloud service; the web application will access the database over the virtual network. This allows you to use the back-end database from the cloud service without the database being accessible on the public Internet.



# FEW USES OF AZURE VNET

You can add a Virtual Network Gateway to a virtual network and use it to connect your on-premises network to Azure, effectively making the virtual network in Azure an extension of your on-premises network. This provides the ability to deploy hybrid cloud applications that securely connect to your on-premises datacenter. The Virtual Network Gateway is a fully managed service in Azure.

More complex features available include multisite VPNs, in-region VNet-to-VNet, and cross-region VNet-to-VNet.

Most cross-premises connections involve using a VPN device to create a secure connection to your virtual network in Azure.

# CREATION OF AZURE VNET- THINGS YOU SHOULD KNOW

## VNET COMPONENTS

ADDRESS SPACE

SUBNETS

DNS SERVERS

US\_EAST

VNet:  
10.0.0.0/16

Subnet: 10.0.0.0/24

Azure VM 1  
10.0.0.5

## WHEN VNET NEEDED TO BE CONNECTED TO OTHER VNET WHAT YOU SHOULD DO

Always select address ranges that are not overlapping.

VNET are private and you must use un routable IP addresses, specified in CIDR notation, such as 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16.

CIDR notation uses this format: xxx.xxx.xxx.xxx/n, where n is the number of leftmost '1' bits in the mask.

After specifying your virtual network address space(s), you can create one or more subnets for your virtual network.

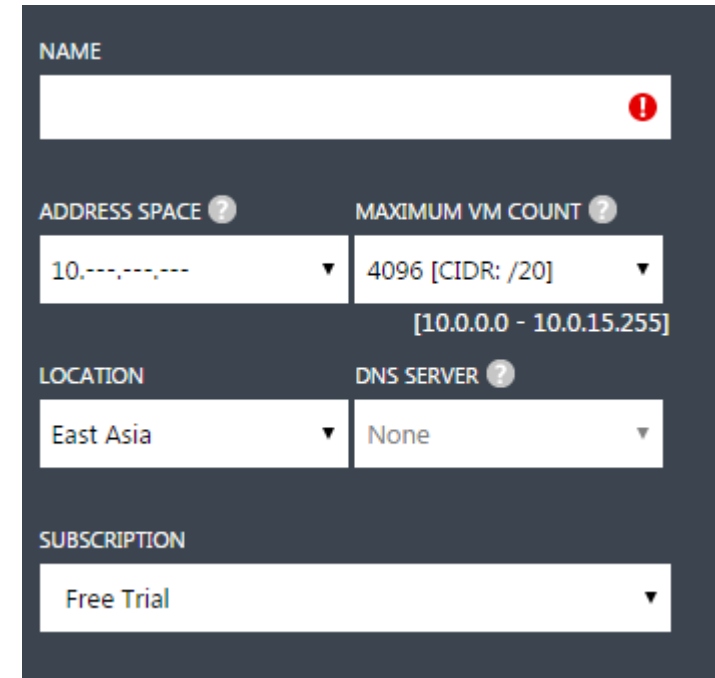
If you want to refer to your VMs or role instances by host name or fully qualified domain name (FQDN) directly, rather than using an IP address and port number, you need a DNS service to provide name Resolution.

There are two options: you can use the Azure-provided name resolution or you can specify a DNS server that is not maintained by Azure, such as one that is used by your on-premises infrastructure or one that you set up and maintain in an Azure VM.

# LAB 1: CREATE VNETS- QUICK CREATE

The MAXIMUM VM COUNT is the count of the range of IP addresses included for the selected CIDR. If you look at the values in the drop-down list, you will see the highest CIDR (and thus the fewest number of IP addresses) is 20, which gives you 4,096 addresses

For DNS SERVER, if you set this to None, the name resolution will be provided by Azure. If you want to have name resolution between this virtual network and your on-premises network, you should specify the DNS servers you are using for your on-premises name resolution. For this example, just leave it set to None.



A screenshot of the 'Quick Create' form for a new Virtual Network (VNet) in Azure. The form is dark-themed with white text and input fields. It includes sections for NAME, ADDRESS SPACE, MAXIMUM VM COUNT, LOCATION, DNS SERVER, and SUBSCRIPTION. The ADDRESS SPACE is set to '10.---.---.---' and MAXIMUM VM COUNT is set to '4096 [CIDR: /20]'. The LOCATION is 'East Asia' and DNS SERVER is 'None'. The SUBSCRIPTION is 'Free Trial'. A red exclamation mark icon is visible in the NAME field.

NAME	
<input type="text"/>	
ADDRESS SPACE ?	MAXIMUM VM COUNT ?
<input type="text" value="10.---.---.---"/>	<input type="text" value="4096 [CIDR: /20]"/>
[10.0.0.0 - 10.0.15.255]	
LOCATION	DNS SERVER ?
<input type="text" value="East Asia"/>	<input type="text" value="None"/>
SUBSCRIPTION	
<input type="text" value="Free Trial"/>	

# LAB 2: CREATE VNET - CUSTOM CREATE

## STEP 1

CREATE A VIRTUAL NETWORK

### Virtual Network Details

NAME

AAVINET

LOCATION

East Asia ▼

SUBSCRIPTION

Free Trial ▼

NETWORK PREVIEW

↔ AAVINET

## STEP 2

CREATE A VIRTUAL NETWORK

### DNS Servers and VPN Connectivity

DNS SERVERS ?

ENTER NAME

IP ADDRESS

POINT-TO-SITE CONNECTIVITY ?

☐ Configure a point-to-site VPN

SITE-TO-SITE CONNECTIVITY ?

☐ Configure a site-to-site VPN

NETWORK PREVIEW

↔ AAVINET



# CREATE VNET CUSTOM CREATE

## STEP 3

### Virtual Network Address Spaces

ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
10.0.0.0/28	10.0.0.0	/28 (16)	10.0.0.0 - 10.0.0.15
SUBNETS			
Subnet-1	10.0.0.0	/29 (8)	10.0.0.0 - 10.0.0.7
add subnet			

add address space

#### NETWORK PREVIEW

AAVINET

## STEP 4

### Virtual Network Address Spaces

ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
10.0.0.0/28	10.0.0.0	/28 (16)	10.0.0.0 - 10.0.0.15
SUBNETS			
MYVMS	10.0.0.8	/29 (8)	10.0.0.8 - 10.0.0.15
MYSERVICES	10.0.0.0	/29 (8)	10.0.0.0 - 10.0.0.7
add subnet			

add address space

#### NETWORK PREVIEW

AAVINET

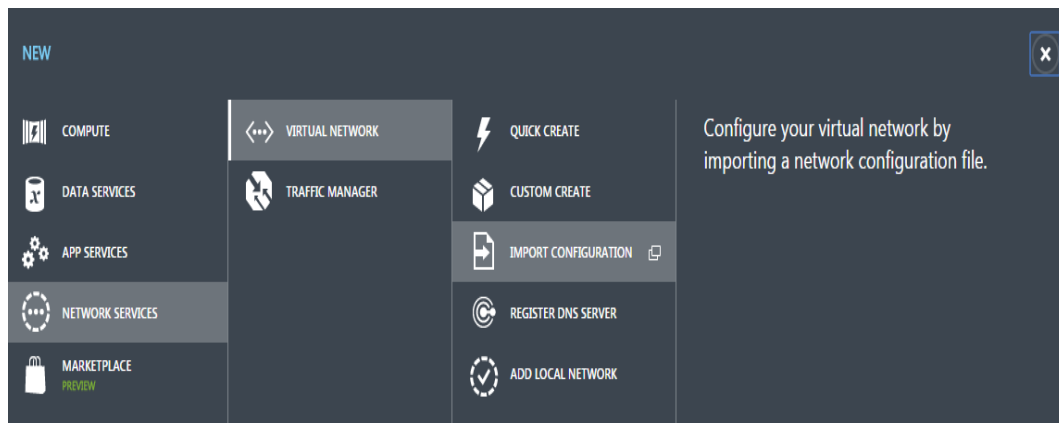
# LAB 3: CREATE VNET — WITH XML FILE

## STEP 1



By clicking on the export button on the bar showing above you can download the entire Azure network configuration to an XML file.

## STEP 2

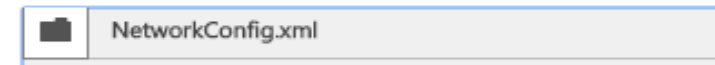


## STEP 3

### IMPORT NETWORK CONFIGURATION FILE

Import the network configuration file

#### CONFIGURATION FILE



#### SUBSCRIPTION



## STEP 4

### IMPORT NETWORK CONFIGURATION FILE

Building your network

This import will result in the following changes to your network configuration.

TYPE	NAME	ACTION
Virtual Network	AAVINET1	+ CREATE
Virtual Network	HWMVNET	+ CREATE
Virtual Network	AAVTNET2	+ CREATE



# RESULT OF THE VNET CREATION WITH XML FILE

## networks

VIRTUAL NETWORKS

LOCAL NETWORKS

DNS SERVERS

NAME		STATUS	SUBSCRIPTION	LOCATION	🔍
AAVINET1	→	✓ Created	Free Trial	East Asia	
AAVIVNET2		✓ Created	Free Trial	East Asia	
HWMVNET		✓ Created	Free Trial	South Central US	

This raises a lot of questions because you have to download the whole configuration for the subscription and cannot download just the configuration for one of the virtual networks defined in the subscription:

- Is there a way to modify the settings for one of the virtual networks?
- Can you add another virtual network?
- Can you remove one or more of the virtual networks?
- What if you already have VMs or services deployed into the virtual network?

# ADD & DELETE VNET WITH THE XML FILE

## What if you add a network?

IMPORT NETWORK CONFIGURATION FILE

### Building your network

This import will result in the following changes to your network configuration.

TYPE	NAME	ACTION
Virtual Network	AAVINET1	— No changes
Virtual Network	HWMVNET	— No changes
Virtual Network	AAVIVNET2	— No changes
Virtual Network	AAVIVNET3	+ CREATE



## What if you delete a network?

IMPORT NETWORK CONFIGURATION FILE

### Building your network

This import will result in the following changes to your network configuration.

TYPE	NAME	ACTION
Virtual Network	AAVINET1	— No changes
Virtual Network	HWMVNET	— No changes
Virtual Network	AAVIVNET2	— No changes
Virtual Network	AAVIVNET3	✗ DELETE



# UPDATE A VNET WITH THE XML FILE

## What if you update a network?

IMPORT NETWORK CONFIGURATION FILE

Building your network

This import will result in the following changes to your network configuration.

TYPE	NAME	ACTION
Virtual Network	AAVINET1	⬆ UPDATE
Virtual Network	HWMVNET	— No changes
Virtual Network	AAVINET2	— No changes

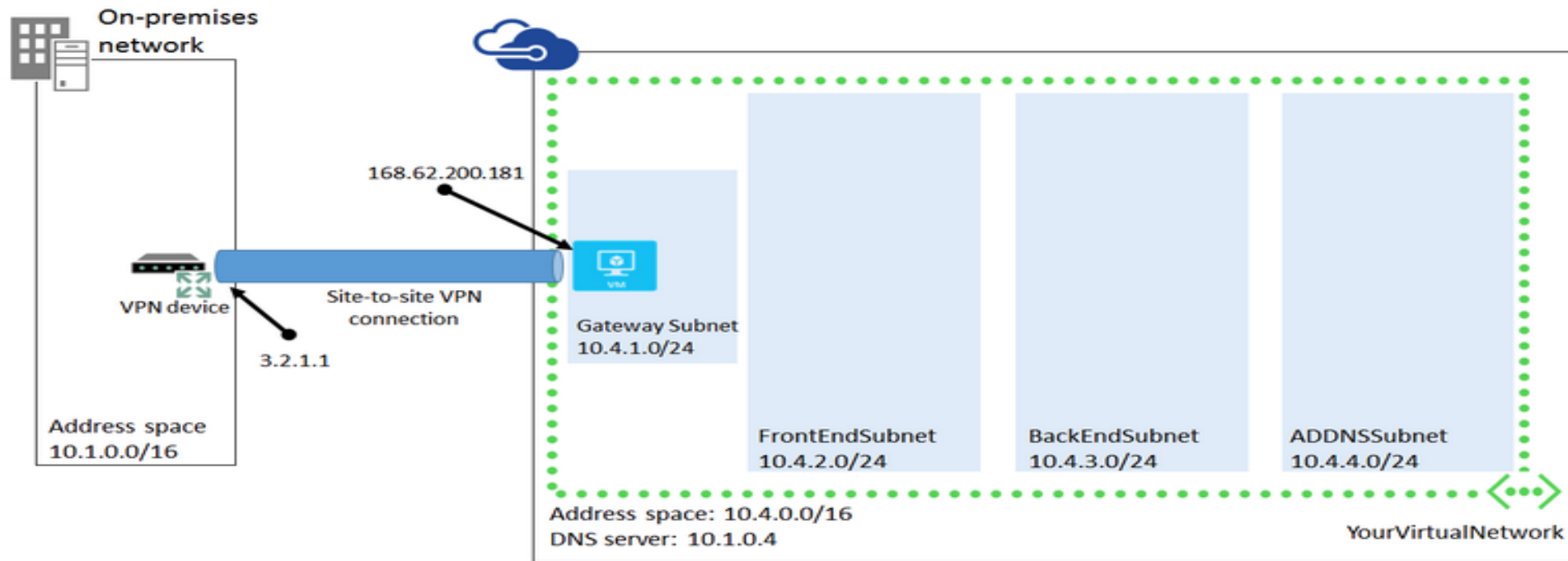
⬅

✓

QUESTIONS?

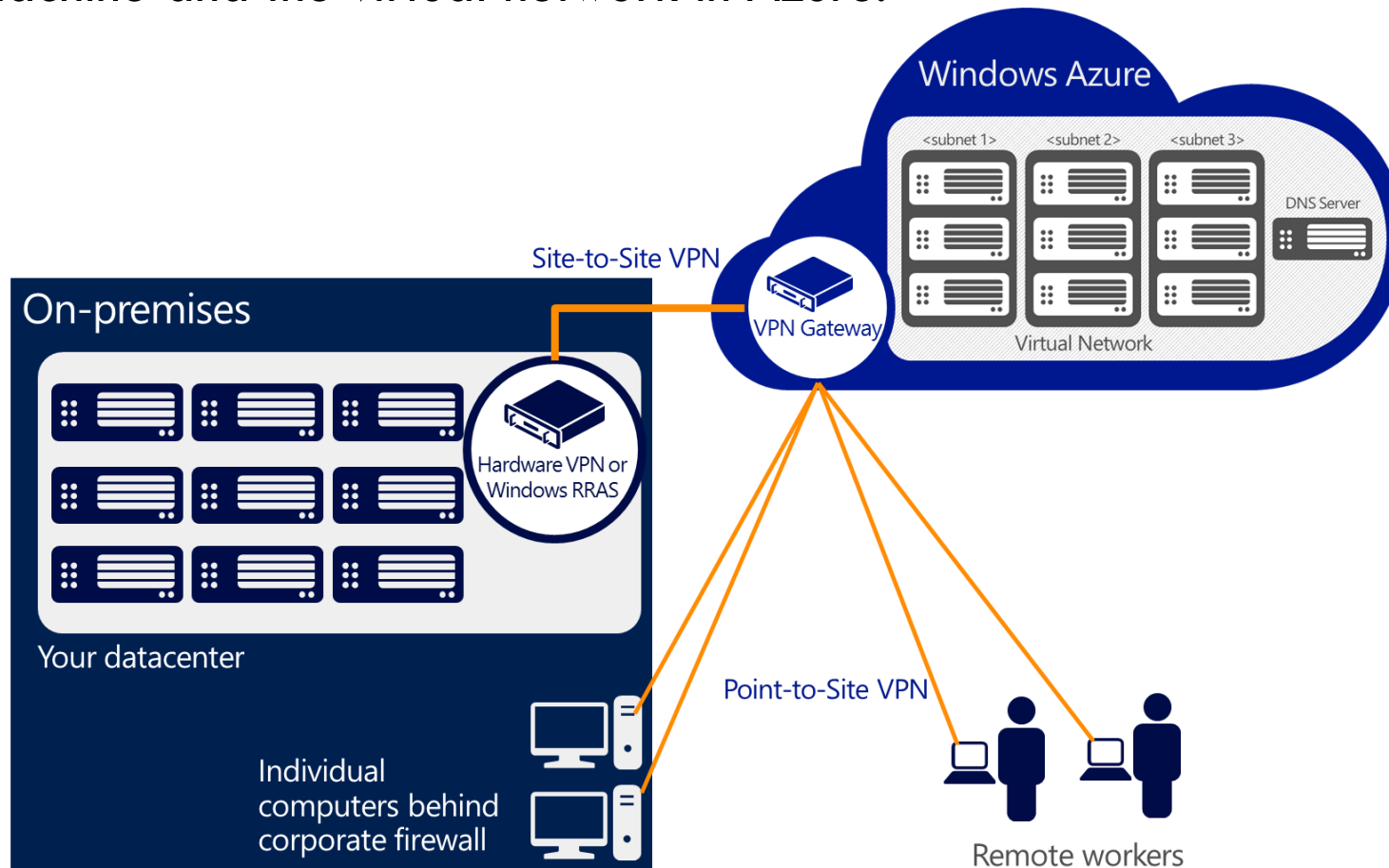
# SITE TO SITE VPN

A site-to-site VPN lets you connect securely from your on-premises network to your virtual network in Azure. You have to have a public-facing IPv4 IP address and a compatible VPN device.



# POINT TO SITE VPN

Point-to-site VPN enables you to connect from your local machine over a Secure Socket Tunneling Protocol (SSTP) tunnel to your virtual network in Azure. This uses certificate authentication between the client machine and the virtual network in Azure.



# LAB 4: SETUP A POINT TO SITE VPN

In this lab we see how to set up a point-to-site network and test it by deploying a VM into the network and connecting to it from the local machine.

## Step 1 : Create a custom VNET

CREATE A VIRTUAL NETWORK

### Virtual Network Details

NAME

AAVIP2S

LOCATION

East Asia

## Step 2: Configure a point to site VPN

CREATE A VIRTUAL NETWORK

### DNS Servers and VPN Connectivity

DNS SERVERS ?

ENTER NAME

IP ADDRESS

POINT-TO-SITE CONNECTIVITY ?

☒ Configure a point-to-site VPN

SITE-TO-SITE CONNECTIVITY ?

☐ Configure a site-to-site VPN



# LAB 4: SETUP A POINT TO SITE VPN

Step 3: Specify the IP address range from which your VPN clients will receive an IP address when connected. Here I have used the default 10.0.0.0/24

## Point-to-Site Connectivity

ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
10.0.0.0/24	10.0.0.0	/24 (254)	10.0.0.1 - 10.0.0.254
<a href="#">add address space</a>			

I have used starting IP 10.0.18.0 with a CIDR of /24. This gives us an address range of 10.0.18.0 through 10.0.18.255, I have also rename the subnet and added /27 CIDR, in my next step I will add a gateway.

Step 4: Now I will setup the address space used by the virtual network.

ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
10.0.18.0/24	10.0.18.0	/24 (256)	10.0.18.0 - 10.0.18.255
SUBNETS			
AAVIP2SVMs	10.0.18.0	/27 (32)	10.0.18.0 - 10.0.18.31
<a href="#">add subnet</a>	<a href="#">add gateway subnet</a>		

# LAB 4: SETUP A POINT TO SITE VPN

Step 5: Specify a gateway, here I have chosen the default gateway which is 10.0.18.32

ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
10.0.18.0/24	10.0.18.0	/24 (256)	10.0.18.0 - 10.0.18.255
SUBNETS			
AAVIP2SVMs	10.0.18.0	/27 (32)	10.0.18.0 - 10.0.18.31
Gateway	10.0.18.32	/29 (8)	10.0.18.32 - 10.0.18.39
add subnet		add gateway subnet	

Step 6: Now I will click on Check sign which will create the VNET for the point to site VNET and you can see in the screen.

NAME		STATUS	SUBSCRIPTION	LOCATION	
AAVINET1	→	✓ Created	Free Trial	East Asia	
AAVIP2S		✓ Created	Free Trial	East Asia	
AAVIVNET2		✓ Created	Free Trial	East Asia	
HWMVNET		✓ Created	Free Trial	South Central US	

# LAB 4: SETUP A POINT TO SITE VPN

Step 7: Now I will create a VM and will select an image from the Azure Gallery

VERSION RELEASE DATE ? 2/29/2016 ▼	CLOUD SERVICE ? Create a new cloud service ▼
VIRTUAL MACHINE NAME ? AAVIVM1	CLOUD SERVICE DNS NAME AAVIVM1SVC .cloudapp.net
TIER BASIC STANDARD	SUBSCRIPTION Free Trial ▼
SIZE ? A1 (1 core, 1.75 GB memory) ▼	REGION/AFFINITY GROUP/VIRTUAL NETWORK ? AAVIP2S ▼
NEW USER NAME Aavi1	VIRTUAL NETWORK SUBNETS AAVIP2SVMs(10.0.18.0/27) ▼
NEW PASSWORD ..... ✓	STORAGE ACCOUNT Use an automatically generated storage account ▼
CONFIRM .....	AVAILABILITY SET ? (None) ▼

# LAB 4: SETUP A POINT TO SITE VPN

## Step 8: Create the VPN Gateway

We will click on the + sign in the dashboard of the VNET to create the gateway. Once you click on this you will see something like this below.

virtual network



resources

NAME	ROLE	IP ADDRESS	SUBNET NAME	
AAVIVM1	Virtual Machine	10.0.18.4	AAVIP2SVMs	

# LAB 4: SETUP A POINT TO SITE VPN

## Step 9: Create the Certificate

Now we will create a self signed root certificate and a client certificate, This is because rather than use password authentication, which is fairly weak, point-to-site connectivity uses certificate authentication. Someone without the correct client certificate installed will not be able to connect to the virtual network, even if he or she somehow obtains the IP address of the network.

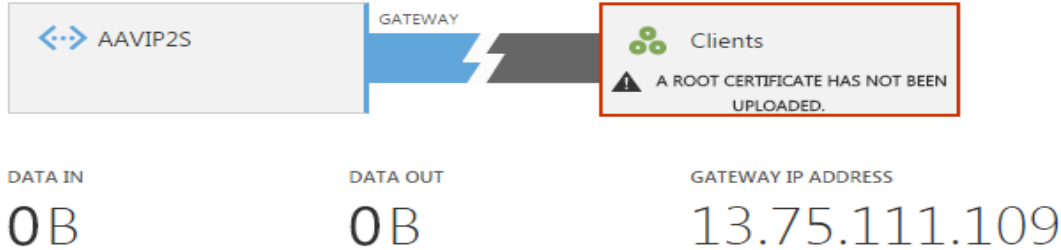
Here are the steps we follow for generating the certificates.

1. Generate a self-signed root certificate.
2. Upload the root certificate to the Azure Management Portal.
3. Generate a client certificate that uses the root certificate you just created.
4. Export and install the client certificate on the client machine that is going to connect to the network.

# LAB 4: SETUP A POINT TO SITE VPN

## Step 9: Create the Certificate and upload

virtual network




resources

NAME	ROLE	IP ADDRESS	SUBNET NAME
AAVIVM1	Virtual Machine	10.0.18.4	AAVIP2SVMs

## Upload Certificate

Point-to-site connectivity requires certificates for client authentication. You need to generate a self-signed root-certificate and upload it before you can download a VPN client. [Learn more.](#)

CERTIFICATE

 AaviP2SRoot.cer

```
makecert -sky exchange -r -n "CN=AaviP2SRoot" -pe -a sha1 -len 2048 -ss My .\AaviP2SRoot.cer
```

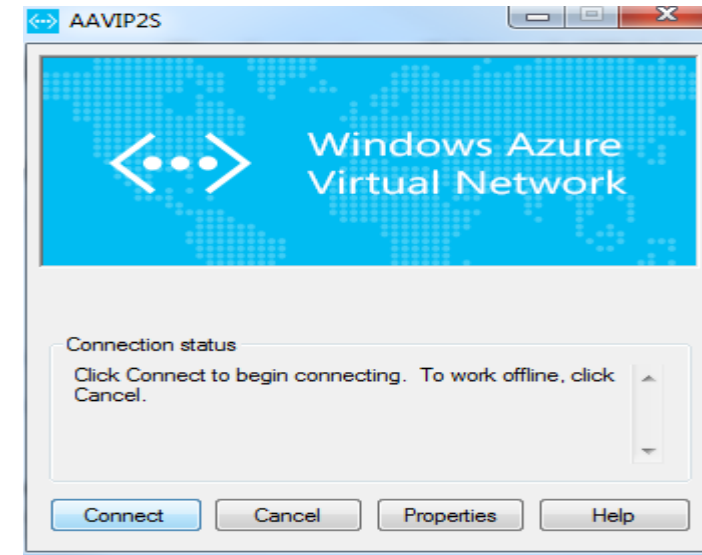
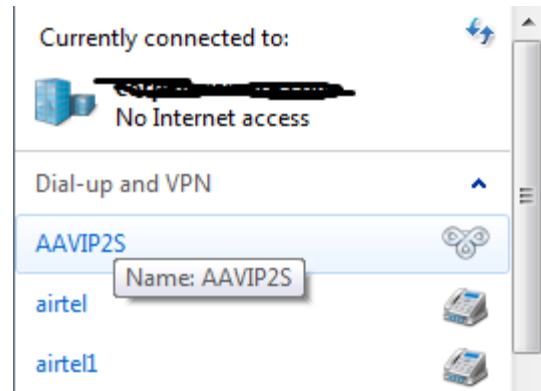
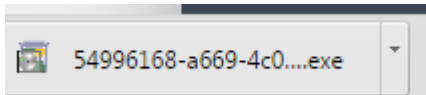
```
makecert.exe -n "CN=AaviP2SClient" -pe -sky exchange -m 96 -ss My -in "AaviP2SRoot" -is my -a sha1
```

# LAB 4: SETUP A POINT TO SITE VPN

Step 10: Download and install client VPN package from the Azure Portal and connect to VPN from your local computer

## quick glance

- Download the 64-bit Client VPN Package
- Download the 32-bit ClientVPN Package



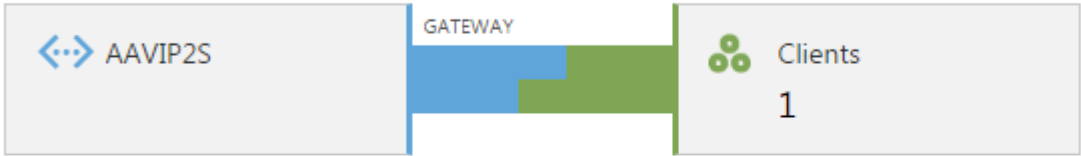
Access type: No Internet access  
Connections: AAVIP2S

# LAB 4: SETUP A POINT TO SITE VPN

aavip2s

[DASHBOARD](#) [CONFIGURE](#) [CERTIFICATES](#)

virtual network



DATA IN	DATA OUT	GATEWAY IP ADDRESS
248.01 KB	691.06 KB	13.75.111.109

resources

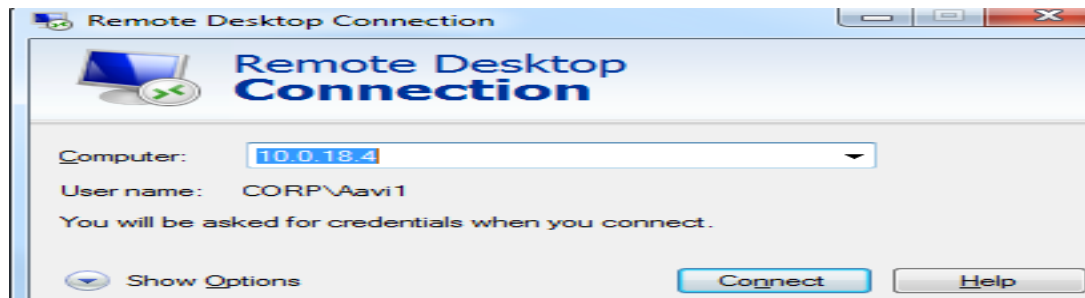
NAME	ROLE	IP ADDRESS	SUBNET NAME	
AAV1VM1	Virtual Machine	10.0.18.4	AAVIP2SVMs	

Out details



# LAB 4: SETUP A POINT TO SITE VPN

Step 12: RDP to the VM which we have created earlier with the help of the private IP address.

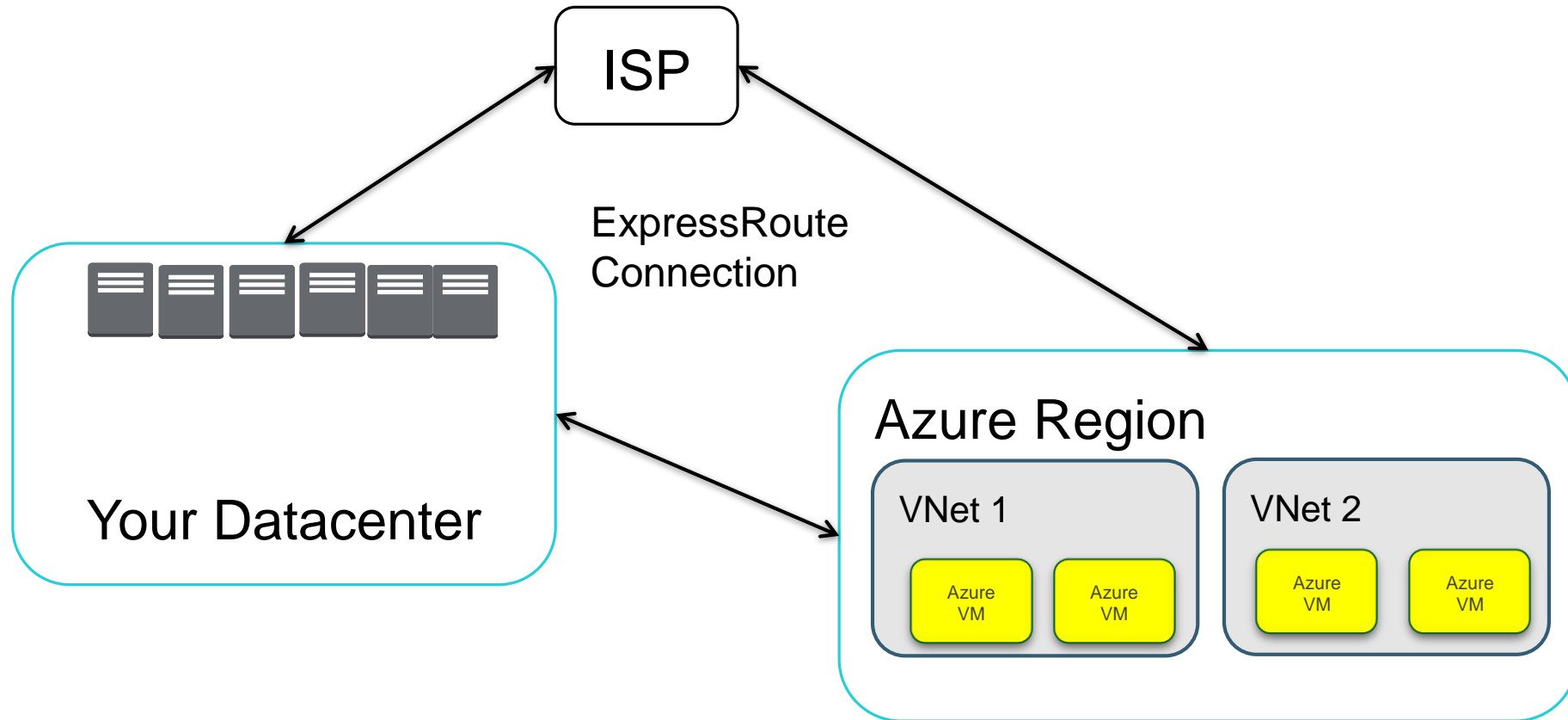


You should be able to see something like this.

```
Deployment Id:      1746399588d742e0acc75fe7a462c431
Internal IP:       10.0.18.4
Public IP:         13.75.107.177
Boot Time:         4/6/2016 3:18 AM
Free Space:        C:\ 116.21 GB NTFS
                   D:\ 68.77 GB NTFS
Host Name:         AAVIVM1
Memory:            1792 MB
OS Version:        Windows Server 2012 R2 Datacenter
User Name:         Aavi1
```

# PRIVATE SITE-TO-SITE CONNECTIVITY (EXPRESSROUTE)

Private site-to-site connectivity, which in Azure means ExpressRoute. This is called private because the network traffic occurs over your network provider and does not go across the public Internet as it does with both site-to-site and point-to-site connectivity



# LAB 5 — CREATE A VNET TO VNET CONNECTION

Connecting a virtual network to another virtual network (VNet-to-VNet) is very similar to connecting a virtual network to an on-premises site location. Both connectivity types use a VPN gateway to provide a secure tunnel using IPsec/IKE. The VNets you connect can be in different subscriptions and different regions. You can even combine VNet to VNet communication with multi-site configurations.

Step 1 & 2: Plan the IP address range.

Virtual Network	Virtual Network Site Definition	Local Network Site Definition
AZUREVNET	AZUREVNET(10.1.0.0/16)	AZURELOCAL(10.1.0.0/16)
ONPREVNET	ONPREMVNET(192.168.1.0/29)	ONPREMLOCAL(192.168.1.0/28)

# LAB 5 — CREATE A VNET TO VNET CONNECTION

Virtual Network	Location	Starting IP	Subnet
AZUREVNET	East Asia	10.1.0.0/16	10.1.0.0/19
ONPREMVNET	South East Asia	192.168.1.0/29	192.168.1.0/29

## AZUREVNET

ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
10.1.0.0/16	10.1.0.0	/16 (65531)	10.1.0.4 - 10.1.255.254
SUBNETS			
VM	10.1.0.0	/19 (8187)	10.1.0.4 - 10.1.31.254
Gateway	10.1.32.0	/29 (3)	10.1.32.4 - 10.1.32.6
add subnet		add gateway subnet	

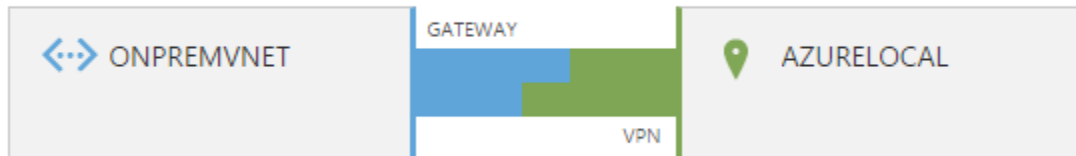
## ONPREMVNET

ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
192.168.1.0/28	192.168.1.0	/28 (11)	192.168.1.4 - 192.168.1.14
SUBNETS			
VMS	192.168.1.0	/29 (3)	192.168.1.4 - 192.168.1.6
Gateway	192.168.1.8	/29 (3)	192.168.1.12 - 192.168.1.14
add subnet		add gateway subnet	

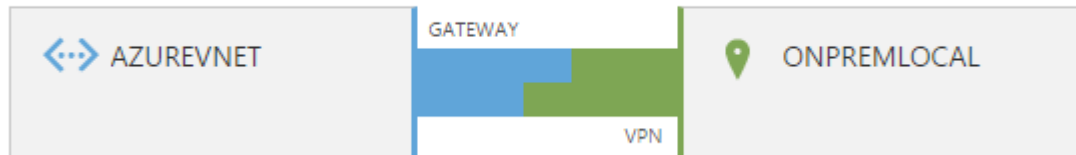
# LAB 5 — CREATE A VNET TO VNET CONNECTION

## Step 3: Create the Gateway

virtual network



virtual network



## Step 4: Configure the LAN with the public IP of the Gateway

Specify your local network details

NAME

AZURELOCAL

VPN DEVICE IP ADDRESS (OPTIONAL)

40.83.123.72

Specify your local network details

NAME

ONPREMLOCAL

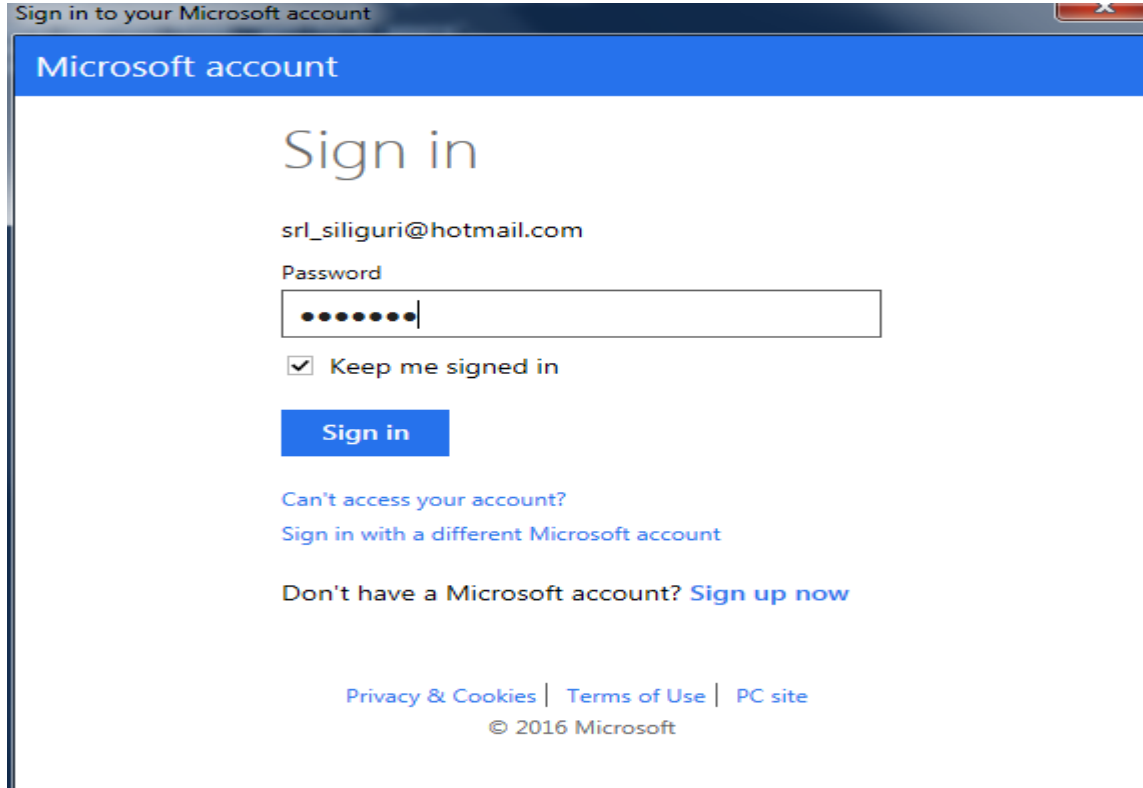
VPN DEVICE IP ADDRESS (OPTIONAL)

13.76.138.68

# LAB 5 — CREATE A VNET TO VNET CONNECTION

Step 4: Connect to Azure subscription from PowerShell

Add-AzureAccount



Step 5: Connect to appropriate subscription and setup the shared key.

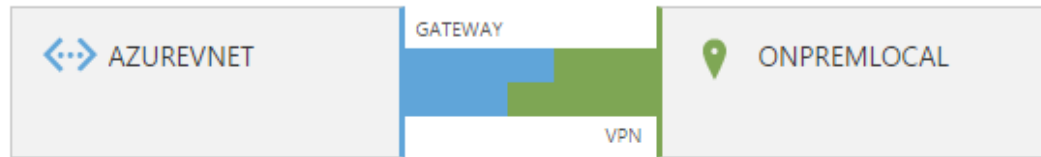
```
Set-AzureVNetGatewayKey -VNetName  
AZUREVNET -LocalNetworkSiteName  
ONPREMLOCAL -SharedKey A1b2C3D5
```

```
Set-AzureVNetGatewayKey -VNetName  
ONPREMVNET -LocalNetworkSiteName  
AZURELOCAL -SharedKey A1b2C3D5
```

# LAB 5 — CREATE A VNET TO VNET CONNECTION

Step 6: Connect the Gateway in AzureVNET

virtual network



DATA IN

14.22 KB

DATA OUT

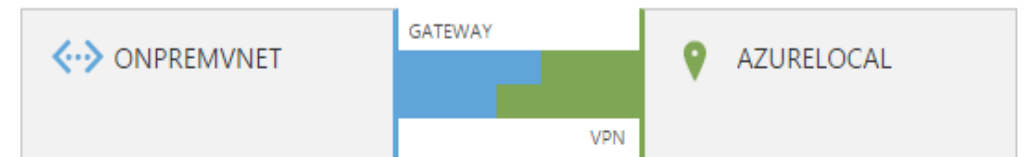
14.59 KB

GATEWAY IP ADDRESS

40.83.123.72

Step 7: Connect the Gateway in ONPREMVNET

virtual network



DATA IN

14.55 KB

DATA OUT

14.22 KB

GATEWAY IP ADDRESS

13.76.138.68

# LAB 5 — CREATE A VNET TO VNET CONNECTION

## Step 8: Create a VM in AzureVNET

CREATE A VIRTUAL MACHINE

Choose an Image



## Step 9: Select the appropriate VNET

REGION/AFFINITY GROUP/VIRTUAL NETWORK ?

AZUREVNET ▼

VIRTUAL NETWORK SUBNETS

VM(10.1.0.0/19) ▼

## Step 10: Create a VM in ONPREMVNET

CREATE A VIRTUAL MACHINE

Choose an Image



## Step 10: Select the appropriate VNET

REGION/AFFINITY GROUP/VIRTUAL NETWORK ?

ONPREMVNET ▼

VIRTUAL NETWORK SUBNETS

VMS(192.168.1.0/29) ▼



# LAB 5 — CREATE A VNET TO VNET CONNECTION

Step 11: Allow the network discovery of the VM

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers. [What is network discovery?](#)

- ☒ Turn on network discovery
- ☐ Turn off network discovery

Step 12: Stop the Windows Firewall



Step 13: Run the PING command from AZUREVM1 to ONPREMVM1

```
C:\Users\aaavi1>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:
Reply from 192.168.1.4: bytes=32 time=39ms TTL=126
Reply from 192.168.1.4: bytes=32 time=36ms TTL=126
Reply from 192.168.1.4: bytes=32 time=35ms TTL=126
Reply from 192.168.1.4: bytes=32 time=37ms TTL=126

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 35ms, Maximum = 39ms, Average = 36ms
```

Step 14: Run the PING command from ONPREMVM1 to AZUREVM1

```
C:\Users\aaavi1>ping 10.1.0.4

Pinging 10.1.0.4 with 32 bytes of data:
Reply from 10.1.0.4: bytes=32 time=38ms TTL=126
Reply from 10.1.0.4: bytes=32 time=37ms TTL=126
Reply from 10.1.0.4: bytes=32 time=39ms TTL=126
Reply from 10.1.0.4: bytes=32 time=36ms TTL=126

Ping statistics for 10.1.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 36ms, Maximum = 39ms, Average = 37ms
```



Thank You