

# **SITE TO SITE**

## **Prepare R&D Document on How to setup Site to Site using Hyper-V**

### **1. What is Site-to-Site VPN?**

A Site-to-Site VPN connects two networks (like your on-premises office and Azure cloud) over the Internet securely. It's used for organizations with multiple branches or when you want to connect your local network to Azure.

---

### **2. What is Hyper-V?**

Hyper-V is Microsoft's virtualization platform that allows you to create virtual machines (VMs). In this project, your on-premises "network" will be simulated in a Hyper-V VM running Windows Server or a router OS like pfSense.

---

### **3. Overview of Project**

You're going to:

1. Create a Virtual Network Gateway in Azure.
  2. Create a Local Network Gateway in Azure (representing your on-premise).
  3. Simulate your local network using Hyper-V and a Virtual Router (e.g., pfSense).
  4. Connect them using a Site-to-Site VPN.
- 

### **4. What You Need**

<b>Component</b>	<b>Description</b>
Azure Subscription	Needed to set up Azure services
Hyper-V Enabled PC	Windows 10/11 Pro or Server edition
pfSense ISO (or RRAS on Windows Server)	Open-source router firewall for testing
Internet Connection	Required for VPN tunnel

---

## 5. Step-by-Step Configuration

---

### A. Azure Side Configuration

---

#### ◊ Step 1: Create a Virtual Network (VNet)

##### What is a VNet?

- A Virtual Network in Azure is like your own private network in the cloud.
- You use it to host virtual machines, connect services, or link with your on-premise network via VPN.

##### How to Do It:

1. Go to Azure Portal

Open a browser and go to: <https://portal.azure.com>

Log in using your Azure account.

2. Search for "Virtual Network" in the search bar and click "+ Create".

3. In the Basics tab:

- Subscription: Use your default subscription.

- Resource Group: Click "Create new" → Enter a name like SiteToSiteRG.

- Name: MyAzureVNet
- Region: Choose the one closest to your location.

4. In the IP Addresses tab:

- Address Space: 10.1.0.0/16 — This is the range of IPs Azure can assign inside the network.
- Subnet name: Enter GatewaySubnet (MUST use this exact name).
- Subnet address range: 10.1.0.0/24 — this subnet will be used by the VPN gateway.

5. Click Review + Create → then Create.

***Why GatewaySubnet?***

Azure requires a subnet named exactly GatewaySubnet to deploy the VPN Gateway.

## Create virtual network

...

Basics   Security   IP addresses   Tags   Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.

[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 *	<input type="text" value="Azure subscription 1"/> 
Resource group *	<input type="text" value="(New) SiteToSiteRG"/>  <a href="#">Create new</a>

### Instance details

Virtual network name *	<input type="text" value="MyAzureVNet"/>
Region * 	<input type="text" value="(US) East US"/>  <a href="#">Deploy to an Azure Extended Zone</a>

## Create virtual network

...

Basics Security IP addresses Tags Review + create

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. [Learn more ↗](#)

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. [Learn more ↗](#)

+ Add a subnet

10.0.0.0/16

 Delete address space

This address prefix overlaps with virtual network 'P2SVNNet'. If you intend to peer these virtual networks, change the address space. [Learn more ↗](#)

10.0.0.0

/16

10.0.0.0 - 10.0.255.255

65,536 addresses

Subnets

IP address range

Size

NAT gateway

default

10.0.0.0 - 10.0.0.255

/24 (256 addresses)

-



Add IPv4 address space | 

## Add a subnet



Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. [Learn more](#)

Subnet purpose i

Virtual Network Gateway



Name \* i

GatewaySubnet

### IPv4

Include an IPv4 address space



IPv4 address range i

10.0.0.0/16



10.0.0.0 - 10.0.255.255

Starting address \* i

10.0.1.0

Size i

/24 (256 addresses)



Subnet address range i

10.0.1.0 - 10.0.1.255

### IPv6

Include an IPv6 address space



This virtual network has no IPv6 address ranges.

### Private subnet

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. [Learn more](#)

Enable private subnet (no default outbound access)



### Security

Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. [Learn more](#)

NAT gateway i

None



[Create new](#)

**Add**

**Cancel**

[Give feedback](#)

## Create virtual network

...

Basics Security IP addresses Tags Review + create

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. [Learn more](#)

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. [Learn more](#)

 Add a subnet

 10.0.0.0/16

 Delete address space

This address prefix overlaps with virtual network 'P2SVNet'. If you intend to peer these virtual networks, change the address space. [Learn more](#)

10.0.0.0

/16

10.0.0.0 - 10.0.255.255

65,536 addresses

Subnets

IP address range

Size

NAT gateway

[default](#)

10.0.0.0 - 10.0.0.255

/24 (256 addresses)

-

 

[GatewaySubnet](#)

10.0.1.0 - 10.0.1.255

/24 (256 addresses)

-

 

Add IPv4 address space



# Create virtual network

...

Basics

Security

IP addresses

Tags

[Review + create](#)

[View automation template](#)

## Basics

Subscription	Azure subscription 1
Resource Group	SiteToSiteRG
Name	MyAzureVNet
Region	East US

## Security

Azure Bastion	Disabled
Azure Firewall	Disabled
Azure DDoS Network Protection	Disabled

## IP addresses

Address space	10.0.0.0/16 (65,536 addresses)
Subnet	default (10.0.0.0/24) (256 addresses)
Subnet	GatewaySubnet (10.0.1.0/24) (256 addresses)

## Tags

Home >

 MyAzureVNet-1753349582070 | Overview

Deployment

Search X ⏪ Delete Cancel Redeploy Download Refresh

**Overview**

Inputs Outputs Template

Your deployment is complete

Deployment name : MyAzureVNet-1753349582070 Start time : 24/07/2025, 15:03:06  
Subscription : Azure subscription 1 Correlation ID : 9c5516b5-6eea-4916-b410-9d5629b42bf0  
Resource group : SiteToSiteRG

Deployment details

Resource	Type	Status	Operation details
MyAzureVNet	Virtual network	OK	Operation details

Next steps

Go to resource

Give feedback

## ◊ Step 2: Create a Virtual Network Gateway

### What is it?

- This is the VPN appliance in Azure that connects your virtual network to your on-premise network.

### How to Do It:

1. In Azure Portal, search for "Virtual Network Gateway" → click + Create.
2. In the Basics tab:
  - Name: MyAzureVPNGateway
  - Region: Same as your VNet (must match).

- **Gateway Type:** VPN
- **VPN Type:** Route-based (used for dynamic routing, preferred).
- **SKU:** VpnGw1 (you can choose Basic if cost is a concern, but features may be limited).
- **Virtual Network:** Select MyAzureVNet.
- **Public IP Address:** Click "Create new" → Name it AzureVPNPublicIP.

3. Click Review + Create → then Create.

## 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 \*

Azure subscription 1

Resource group [?](#)

SiteToSiteRG (derived from virtual network's resource group)

### Instance details

Name \*

MyAzureVPNGateway



Region \*

East US



[Deploy to an Azure Extended Zone ↗](#)

Gateway type \* [?](#)

VPN  ExpressRoute

SKU \* [?](#)

VpnGw1



Generation [?](#)

Generation1



Enable Advanced Connectivity [?](#)

Enabled  Disabled

Virtual network \* [?](#)

MyAzureVNet



[Create virtual network](#)

Subnet [?](#)

GatewaySubnet (10.0.1.0/24)



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

### Public IP address

Public IP address \* [?](#)

Create new  Use existing

[Review + create](#)

[Previous](#)

[Next : Tags >](#)

[Download a template for automation](#)

## Create virtual network gateway

Virtual network \* ⓘ

MyAzureVNet



[Create virtual network](#)

Subnet ⓘ

GatewaySubnet (10.0.1.0/24)



i 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 \*

AzureVPNPublicIP



Public IP address SKU

Standard

Assignment

Dynamic  Static

Enable active-active mode \* ⓘ

Enabled  Disabled

### SECOND PUBLIC IP ADDRESS

SECOND PUBLIC IP ADDRESS \* ⓘ

Create new  Use existing

Public IP address name \*

AzureVPNPublicIP1



Public IP address SKU

Standard

Configure BGP \* ⓘ

Enabled  Disabled

### Authentication Information (Preview)

Enable Key Vault Access ⓘ

Enabled  Disabled

Azure recommends using a validated VPN device with your virtual network gateway. To view a list of validated devices and instructions for configuration, refer to Azure's [documentation](#) regarding validated VPN devices.

[Review + create](#)

[Previous](#)

[Next : Tags >](#)

[Download a template for automation](#)

## Create virtual network gateway

 Validation passed

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

### Basics

Subscription	Azure subscription 1
Resource group	SiteToSiteRG
Name	MyAzureVPNGateway
Region	East US
SKU	VpnGw1
Generation	Generation1
Virtual network	MyAzureVNet
Subnet	GatewaySubnet (10.0.1.0/24)
Gateway type	Vpn
VPN type	RouteBased
Enable active-active mode	Enabled
Enable Advanced Connectivity	Disabled
Configure BGP	Disabled
Public IP address	AzureVPNPublicIP
SECOND PUBLIC IP ADDRESS	AzureVPNPublicIP1

### Tags

None

Home >

## Microsoft.VirtualNetworkGateway-20250724163727 | Overview

The screenshot shows the Azure portal's 'Overview' tab for a Virtual Network Gateway deployment. The deployment status is 'Deployment is in progress'. Deployment details include a name, subscription, and resource group. A table lists resources: two Public IP addresses, both marked as 'OK'.

Resource	Type	Status
AzureVPNPublicIP1	Public IP address	OK
AzureVPNPublicIP	Public IP address	OK

### ◊ Step 3: Create a Local Network Gateway

What is it?

- It represents your on-premises network (i.e., your Hyper-V lab with pfSense).
- You define the public IP and the internal network address of your local network here.

**How to Do It:**

1. Search for "Local Network Gateway" → click + Create.
2. Fill in:
  - Name: MyLocalNetwork
  - IP Address: This is the public IP of your on-prem router (pfSense). If you're testing, use your home's public IP or a placeholder for now.

- You can find your public IP by Googling “What is my IP?”
- Address Space: This is your internal subnet behind pfSense.  
Example: 192.168.1.0/24

### 3. Click Create.

Home > Hybrid connectivity

## Hybrid connectivity | Local network gateways

Preview

Search   Create Manage view Refresh Export to CSV Open query Assign tags

**Overview**

Filter for any field... Subscription equals all Resource group equals all Location equals all +

ExpressRoute

Showing 0 to 0 of 0 records.

Name ↑	Resource group
Set up ExpressRoute	
ExpressRoute circuits	
ExpressRoute directs	

WhatIsMyIP.com Search... News Pricing API Sign Up Login Help

What Is My IP? IP Address Lookup IP Whois Lookup IP Tools Privacy Tools Network Tools Email Tools Popular

### What Is My IP?

YOUR CURRENT IP INFO

My IPv4: [157.10.216.65](#)

My IPv6: Not Detected ⓘ

City: Pune ⓘ

State/Region: Maharashtra ⓘ

Postal Code: 412415 ⓘ

Country: India ⓘ

ISP: Advik Communication Pvt Ltd ⓘ

ASN: [137109](#)

Time Zone: UTC +05:30 ⓘ

## Create local network gateway

...

Basics   Advanced   Review + create

A local network gateway is a specific object that represents an on-premises location (the site) for routing purposes. [Learn more](#)

### Project details

Subscription \*

Azure subscription 1

Resource group \*

SiteToSiteRG

[Create new](#)

### Instance details

Region \*

East US

Name \*

MyLocalNetwork

Endpoint ⓘ

[IP address](#)   [FQDN](#)

IP address \* ⓘ

157.10.216.65

Address Space(s) ⓘ

192.168.1.0/24



...

[Add additional address range](#)

Home > Hybrid connectivity | Local network gateways >

## Create local network gateway

Validation passed

Basics Advanced Review + create

### Summary

Name	MyLocalNetwork
Subscription	Azure subscription 1
Resource group	SiteToSiteRG
Region	East US
Endpoint	IP address
IP address	157.10.216.65
Address Space(s)	192.168.1.0/24

Home >



LocalNetworkGatewayCreate-20250724165012 | Overview

Deployment

Search X <<

Delete Cancel Redeploy Download Refresh

Overview

Inputs

Outputs

Template

Your deployment is complete

Deployment name : LocalNetworkGatewayCreate-20250724165012  
Subscription : Azure subscription 1  
Resource group : SiteToSiteRG

Start time : 24/07/2025, 16:50:18

Correlation ID : 488eb090-aec-4ec0-ad87-13bd689fcfbe

Deployment details

Resource

Type

Status

MyLocalNetwork

Local network gateway

OK

## ◊ Step 4: Create the VPN Connection

Now, you will link the Azure Gateway to your on-prem router (represented by the local network gateway).

### How to Do It:

1. Go to the Virtual Network Gateway (MyAzureVPNGateway)
2. Click on "Connections" (left-side menu)
3. Click "+ Add"
4. Fill in:
  - o Name: MySiteToSiteConnection
  - o Connection Type: Site-to-Site (IPSec)
  - o Local Network Gateway: Select MyLocalNetwork
  - o Shared Key: Choose a password/key (e.g. 12345678vpn)
    - You'll use this same key on the pfSense side
  - o IPSec/IKE Policy: Leave blank for now
5. Click OK

Azure will now wait for your on-prem router to connect.

The screenshot shows the Azure portal interface for managing a Virtual Network Gateway named 'MyAzureVPNGateway'. The left sidebar has a 'Connections' section selected. The main area displays a table with one row: 'No results'. At the top right, there is a 'Connect' button. The URL in the browser bar is 'Home > MyAzureVPNGateway'.

## Create connection

...

Basics   Settings   Tags   Review + create

Create a secure connection to your virtual network by using VPN Gateway or ExpressRoute.

[Learn more about VPN Gateway](#) ↗

[Learn more about ExpressRoute](#) ↗

### Project details

Subscription \*

Azure subscription 1

Resource group \*

SiteToSiteRG

[Create new](#)

### Instance details

Connection type \* ⓘ

Site-to-site (IPsec)

Name \*

MySiteToSiteConnection

Region \*

East US

## Create connection

Basics    **Settings**    Tags    Review + create

### Virtual network gateway

To use a virtual network with a connection, it must be associated to a virtual network gateway.

Virtual network gateway * ⓘ	<input type="text" value="MyAzureVPNGateway"/>
Local network gateway * ⓘ	<input type="text" value="MyLocalNetwork"/>
Authentication Method ⓘ	<input checked="" type="radio"/> Shared Key(PSK) <input type="radio"/> Key Vault Certificate (Preview)
Shared Key(PSK) * ⓘ	<input type="text" value="12345678vpn"/>
IKE Protocol ⓘ	<input type="radio"/> IKEv1 <input checked="" type="radio"/> IKEv2
Use Azure Private IP Address ⓘ	<input type="checkbox"/>
Enable BGP ⓘ	<input type="checkbox"/>
IPsec / IKE policy ⓘ	<input type="radio" value="Default"/> Default <input type="radio" value="Custom"/> Custom
Use policy based traffic selector ⓘ	<input type="radio" value="Enable"/> Enable <input checked="" type="radio" value="Disable"/> Disable
DPD timeout in seconds * ⓘ	<input type="text" value="45"/>
Connection Mode ⓘ	<input checked="" type="radio"/> Default <input type="radio"/> InitiatorOnly <input type="radio"/> ResponderOnly

## Create connection

 Validation passed

Basics    Settings    Tags    **Review + create**

### Basics

Subscription	Azure subscription 1
Resource Group	SiteToSiteRG
Region	East US
Connection type	Site-to-site (IPsec)
Connection name	MyAzureVPNGateway

### Settings

Virtual network gateway	MyAzureVPNGateway
Local network gateway	MyLocalNetwork
IKE Protocol	IKEv2
IPsec / IKE policy	Default
Use policy based traffic selector	Disable
DPD timeout in seconds	45
Connection Mode	Default
Shared Key(PSK)	12345678vpn

### Tags

None

Home >

## NoMarketplace-20250724171354 | Overview

Deployment

Search  Delete  Cancel  Redeploy  Download  Refresh

- Overview
- Inputs
- Outputs
- Template

✓ Your deployment is complete

Deployment name : NoMarketplace-20250724171354  
Subscription : Azure subscription 1  
Resource group : SiteToSiteRG

Start time : 24/07/2025, 17:15:37  
Correlation ID : b049475a-454d-4fd3-a166-59bf3c9c3694

Deployment details

Resource	Type	Status
<input checked="" type="checkbox"/> MyAzureVPNGateway	Connection	OK

## B. On-Premises (Hyper-V) Configuration

### What is pfSense?

pfSense is a free, open-source firewall and router operating system based on FreeBSD. You can use it to:

- Act like a home/office router
- Build VPN connections
- Control traffic between networks
- Simulate an "on-premises router" in lab setups like yours

In this project, pfSense is the on-prem device that will connect to Azure via Site-to-Site VPN.

### What is Hyper-V?

Hyper-V is a virtualization tool built into Windows 10/11 Pro and Windows Server. It allows you to create Virtual Machines (VMs) to simulate real computers.

You'll install pfSense inside a VM on Hyper-V and use that VM as a virtual router for your local network.

Now we simulate your on-prem network using Hyper-V and a pfSense firewall.

---

#### ◊ **Step 5: Download & Install pfSense in Hyper-V**

##### **How to Do It:**

###### 1. Download pfSense:

- Visit: <https://www.pfsense.org/download/>
- Choose:
  - Architecture: AMD64 (64-bit)
  - Installer: ISO Installer
  - Mirror: Choose one close to you

###### 2. Open Hyper-V Manager

If Hyper-V is not enabled:

1. Search "**Turn Windows features on or off**"
2. Check **Hyper-V** and reboot.

Then:

- Search and open **Hyper-V Manager**
- On the right-hand side, click "**New**" > "**Virtual Machine**"
  - Create a new Virtual Machine:
    - Name: pfSense-Router

- Generation: Choose based on ISO (Gen 1 is safest)
- RAM: Allocate 1–2 GB
- Virtual Hard Disk: 10–20 GB
- Install OS from Bootable CD: Choose the pfSense ISO

### 3. Create Two Network Adapters:

- External NIC: Connects to the internet (e.g., shared with your PC)
- Internal NIC: Connects to a virtual internal network (your simulated LAN)

#### ***General Settings:***

<b>Option</b>	<b>Setting</b>
Name	pfSense-Router
Generation	<b>Generation 1</b> (works best with ISO images)
RAM	<b>1024–2048 MB (1–2 GB)</b>
Hard Disk	<b>20 GB</b> (you can use 10 GB for testing)
Boot from	<b>Image file (.iso)</b> and select your downloaded pfSense ISO

#### ***Virtual Network Settings:***

You need to create **two virtual network adapters**:

### 4. Start the VM and follow installation steps:

- Use defaults
- pfSense will ask to assign WAN and LAN interfaces
  - WAN: External adapter

- LAN: Internal adapter

## Create Virtual Switches in Hyper-V (First Time Only)

Go to **Virtual Switch Manager** (in Hyper-V Manager) and create:

### 1. External Switch (Internet-facing)

- Click **New virtual network switch > External**
- Name: WAN-Switch
- Connect it to your **physical network adapter**
- This lets the VM access the internet

### 2. Internal Switch (your LAN simulation)

- Click **New virtual network switch > Internal**
- Name: LAN-Switch
- This creates a private network between pfSense and your other lab VMs

Once switches are created, you can assign them to VM NICs.

## 5. Attach the Two Network Adapters to the VM

In **VM Settings**:

- **Network Adapter 1:**
  - Connect to: WAN-Switch
  - This is the **WAN (Internet)** interface in pfSense
- **Network Adapter 2:**
  - Connect to: LAN-Switch
  - This is the **LAN (internal lab network)** interface in pfSense

Think of it like:

css

CopyEdit

[Internet] ←→ [WAN Interface pfSense LAN Interface] ←→ [Other VMs]

## 6. Start pfSense VM and Install OS

1. Click **Start** on the VM
2. Click **Connect** to open the virtual console

### **pfSense Installation Steps:**

- When the boot menu appears, press **Enter** for default boot
- Select **Install pfSense**
- Use default options:
  - Auto-partition
  - Use entire disk
  - Accept all defaults
- Reboot after installation

After reboot, remove the ISO from the DVD drive under **VM Settings > DVD Drive > None**, or it may boot again into the installer

## 7. Assign WAN and LAN Interfaces

Once pfSense boots up fully, it will show:

kotlin

CopyEdit

Valid interfaces are:

em0, em1

Do you want to set up VLANs? No

Enter WAN interface name: em0

Enter LAN interface name: em1

Assign like this (your names may be em0, em1, hn0, etc.):

- WAN: the adapter connected to **WAN-Switch**
- LAN: the adapter connected to **LAN-Switch**

You will see something like:

vbnetwork

CopyEdit

WAN: 192.168.1.10 (from your home router or DHCP)

LAN: 192.168.1.1

## 8. Access pfSense Web UI

From your host PC (or another VM on LAN-Switch):

1. Open browser
2. Visit: **http://192.168.1.1**
3. Login:
  - **Username:** admin
  - **Password:** pfsense

You now have full access to the pfSense firewall!

## What You've Accomplished

- You created a **virtual router** using pfSense
- It has:

- A **WAN** side with internet access (like your home router)
  - A **LAN** side to simulate your internal network
  - This pfSense router is now ready to be configured for a **Site-to-Site VPN**
- 

#### ◊ **Step 6: Configure pfSense for Site-to-Site VPN**

Now you configure the VPN tunnel in pfSense.

#### **Access pfSense Web UI:**

1. Open browser → enter LAN IP of pfSense (e.g., 192.168.1.1)
  2. Default login:
    - Username: admin
    - Password: pfSense
- 

#### **Configure Phase 1 (Main VPN Connection):**

1. Go to VPN > IPsec > Tunnels
2. Click + Add P1

#### **Settings:**

<b>Field</b>	<b>Value</b>
Key Exchange	IKEv2
Remote Gateway	The Public IP of your Azure VPN Gateway
Authentication	Mutual PSK
Pre-Shared Key	Same as Azure (e.g., 12345678vpn)

Field	Value
Encryption	AES 256, SHA256, DH Group 2 or 14

Click Save, then Apply Changes

---

### **Configure Phase 2 (Define Traffic Allowed in VPN):**

1. Click + Add P2 under Phase 1

#### **Settings:**

Field	Value
Local Subnet	192.168.1.0/24
Remote Subnet	10.1.0.0/16 (Azure VNet address space)
Protocol	ESP
Encryption	AES 256, SHA256

Click Save, then Apply Changes

---

#### **◊ Step 7: (Optional) Add Static Route**

Only needed if internal routing is not working.

1. Go to System > Routing > Static Routes
2. Add a new route:
  - Destination Network: 10.1.0.0/16
  - Gateway: Select the IPsec tunnel

## **How to Know It's Working:**

- Azure Portal:  
Go to VPN Gateway > Connections > Status = *Connected*
- pfSense:  
Go to Status > IPsec → Status = *Established*

## **Test Connectivity:**

From a VM inside your Hyper-V LAN, try to:

- Ping an Azure VM
  - RDP into a server
  - Use tracert or pathping to verify routing
- 

## **6. Testing and Validation**

Once both sides are configured:

On Azure:

1. Go to VPN Gateway > Connections
2. You should see the status: Connected

On pfSense:

1. Go to Status > IPsec
2. Tunnel should show as Established

Ping Test:

- Try to ping an Azure VM from your Hyper-V VM (and vice versa).
  - If successful, VPN is working.
- 

## **7. Troubleshooting**

<b>Issue</b>	<b>Possible Fix</b>
VPN not connecting	Check shared key, IP addresses, ensure ports UDP 500, 4500 are open
Can't ping Azure	Check Azure NSG rules, route table
pfSense tunnel down	Review logs under Status > System Logs > IPsec

---

## **8. Security Considerations**

- Use strong PSK (Pre-Shared Key)
  - Restrict NSG rules in Azure to allow only required IPs
  - Enable monitoring and alerts in Azure for VPN Gateway
- 

## **9. Conclusion**

You have now created a secure Site-to-Site VPN tunnel between your simulated on-premises network using Hyper-V and pfSense, and Microsoft Azure. This kind of setup is essential for hybrid cloud deployments, remote branch office connectivity, or lab testing.