



Startups at Microsoft

STARTUPS AT MICROSOFT

6 MIN READ

How to easily set up a VPN between Azure and AWS using managed services (Updated 2024)



rmmartins

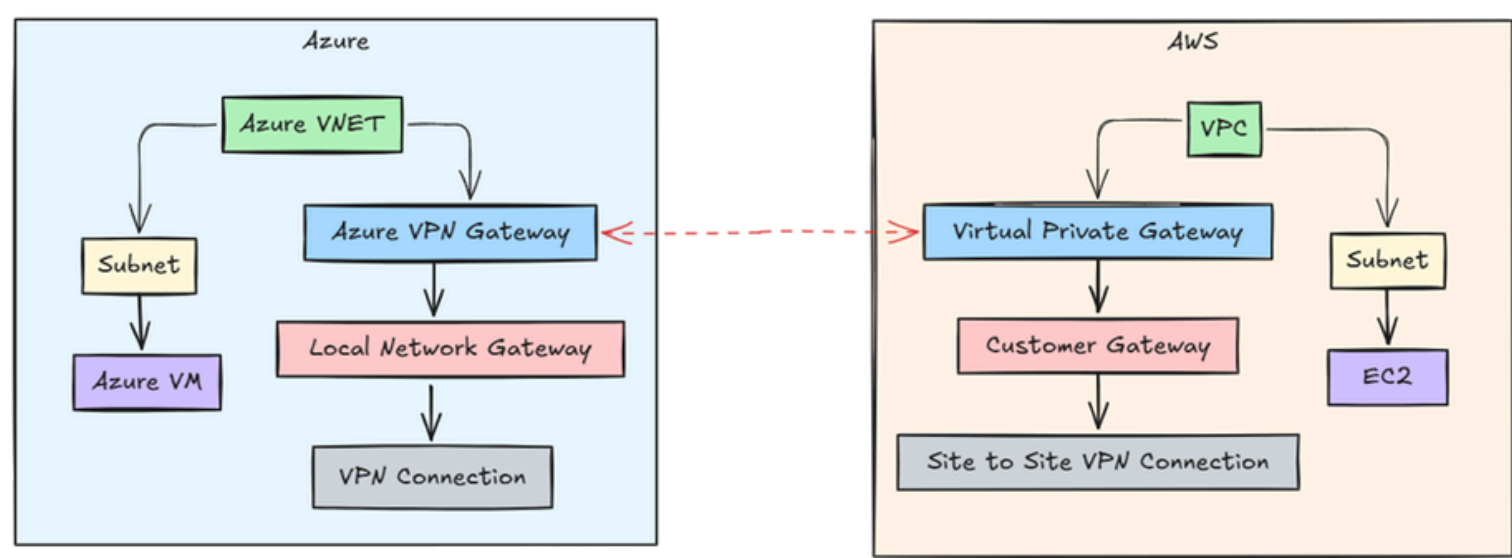
 MICROSOFT

Oct 25, 2024

Introduction

Setting up a secure VPN connection between **Azure** and **AWS** doesn't have to be complicated. In this guide, we'll demonstrate an easy and straightforward method to establish a multicloud static VPN using only **managed services**—no need to manage virtual machines or third-party appliances. This method provides a quick and reliable way to connect **Azure VPN Gateway** and **AWS Virtual Private Gateway** over IPsec tunnels (without BGP config), ensuring secure communication between the two environments.

This post is an updated version of a similar guide I [published three years ago](#), reflecting changes in services and adding valuable troubleshooting tips to streamline the process.



For more advanced scenarios, such as integrating dynamic routing with **BGP (Border Gateway Protocol)** to support automatic route exchanges, we recommend referring to the official [Azure VPN Gateway Documentation](#) for in-depth guidance.



1.1. Create a Resource Group

1. Go to **Azure Portal** > **Resource groups** > **Create**.
2. Select your subscription and region, and give the resource group a name like **RG-AzureAWSVPN**.

1.2. Create a Virtual Network (VNet) and Subnet

1. In the **Azure Portal**, go to **Virtual Networks** > **Create**.
2. Name the VNet **AzureVNet** and specify an address space of **172.16.0.0/16**.
3. Under **Subnets**, create a subnet named **Subnet-AzureVPN** with the address range **172.16.1.0/24**.
4. Add a **GatewaySubnet** with a /27 address block (e.g.,) for the VPN gateway.

Home > Virtual networks >

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

172.16.0.0/16 [Delete address space](#)

172.16.0.0/16 /16

172.16.0.0 - 172.16.255.255 65,536 addresses

Subnets	IP address range	Size	NAT gateway	
Subnet-AzureVPN	172.16.1.0 - 172.16.1.255	/24 (256 addresses)	-	Edit Delete
GatewaySubnet	172.16.254.0 - 172.16.254.31	/27 (32 addresses)	-	Edit Delete

1.3. Set Up the Azure VPN Gateway

1. Go to **+Create a resource**, search for **Virtual Network Gateway**, and select **Create**.
2. Fill in the details:
 - o **Name:** *AzureVPNGateway*
 - o **Gateway Type:** **VPN**
 - o **SKU:** **VpnGw1** (or higher if needed)
 - o **Public IP Address:** Create a new one and name it *AzureVPNGatewayPublicIP*.
 - o **Active-Active Mode:** Leave **disabled** unless high availability is required.
 - If you need to ensure High Availability, enabling the Active-Active mode will made needed the following additional configurations on the Azure side:
 - Create a second Public IP Address for the Virtual Network Gateway
 - Create a second Local Network Gateway pointing to the public IP address of the Tunnel 2 on AWS side
 - Create a second VPN connection pointing to the Tunnel 2 on AWS side
 - o **Configure BGP:** Leave disabled for this lab



[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 *

MyLab

Resource group ⓘ

RG-AzureAWSVPN (derived from virtual network's resource group)

Instance details

Name *

AzureVPNGateway

Region *

Central US

[Deploy to an Azure Extended Zone](#)

Gateway type * ⓘ

☒ VPN ☐ ExpressRoute

SKU * ⓘ

VpnGw1

Generation ⓘ

Generation1

Virtual network * ⓘ

AzureVNet

[Create virtual network](#)

Subnet ⓘ

GatewaySubnet (172.16.254.0/27)

ⓘ 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 *

AzureVPNGatewayPublicIP

Public IP address SKU

Standard

Assignment

☐ Dynamic ☒ Static

Enable active-active mode * ⓘ

☐ Enabled ☒ Disabled

Configure BGP * ⓘ

☐ Enabled ☒ Disabled

Authentication Information (Preview)

Enable Key Vault Access ⓘ

☐ Enabled ☒ Disabled

Step 2: Set Up Your AWS Environment

2.1. Create a VPC and Subnet in AWS

1. In the **AWS Console**, go to **VPC > Create VPC**.
2. Use an address space (e.g., *10.0.0.0/16*) for the **AWS-VPC**.



A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create [Info](#)

Create only the VPC resource or the VPC and other networking resources.

☒ VPC only

☐ VPC and more

Name tag - optional

Creates a tag with a key of 'Name' and a value that you specify.

AWS-VPC

IPv4 CIDR block [Info](#)

☒ IPv4 CIDR manual input

☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.0.0.0/16

CIDR block size must be between /16 and /28.

3. Under **Subnets**, create a subnet with a name like **Subnet-AWSVPN** and the address space **10.0.1.0/24** for your subnet.



Create subnet Info

VPC

VPC ID

Create subnets in this VPC.

vpc-0cba04b8819c978b0 (AWS-VPC)

Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

Subnet-AWSVPN

The name can be up to 256 characters long.

Availability Zone Info

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

No preference

IPv4 VPC CIDR block Info

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

10.0.0.0/16

IPv4 subnet CIDR block

10.0.1.0/24



2.2. Create an AWS Virtual Private Gateway (VGW)

1. In the **AWS VPC Console**, go to **Virtual Private Gateway** and create a new VGW named **AWS-VPN-VGW**.

Create virtual private gateway info

A virtual private gateway is the VPN concentrator on the Amazon side of the site-to-site VPN connection.

Details

Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.

AWS-VPN-VGW

Value must be 256 characters or less in length.

Autonomous System Number (ASN)

☒ Amazon default ASN

☐ Custom ASN

2. Attach the VGW to the **VPC**.

Virtual private gateways (1/1) info

Find resource by attribute or tag

Name <small>↗</small>	Virtual private gateway ID <small>▼</small>	State	Type
<div><div><div></div><div>AWS-VPN-VGW</div></div><div>Create virtual private gateway</div></div>	vgw-0465b5cf429d99a64	<div><div></div>Detached</div>	ipsec.1
<div><div>Actions</div><div><div>Attach to VPC</div><div>Detach from VPC</div><div>Manage tags</div><div>Delete virtual private gateway</div></div></div>			

VPC

>

Virtual private gateways

>

vgw-0465b5cf429d99a64

>

Attach to VPC

Attach to VPC info

Details

Virtual private gateway ID

vgw-0465b5cf429d99a64

Available VPCs
Attach the virtual private gateway to this VPC.

vpc-0cba04b8819c978b0 / AWS-VPC

Cancel

Attach to VPC

2.3. Set Up a Customer Gateway (CGW)

1. In the **AWS Console**, go to **Customer Gateway**, and create a CGW using the **public IP** of the Azure VPN Gateway. Name it **Azure-CGW**.



Create customer gateway Info

A customer gateway is a resource that you create in AWS that represents the customer gateway device in your on-premises network.

Details

Name tag - *optional*

Creates a tag with a key of 'Name' and a value that you specify.

Value must be 256 characters or less in length.

BGP ASN Info

The ASN of your customer gateway device.

Value must be in 1 - 4294967294 range.

IP address Info

Specify the IP address for your customer gateway device's external interface.

Certificate ARN - *optional*

The ARN of a private certificate provisioned in AWS Certificate Manager (ACM).

Select certificate ARN

▼

Device - *optional*

Enter a name for the customer gateway device.

2.4. Create the Site-to-Site VPN Connection

1. In **AWS Console**, go to **Site-to-Site VPN Connections** > **Create VPN Connection**.
2. Select the **Virtual Private Gateway** created earlier.
3. Select the **Customer Gateway** created earlier.
4. Set **Routing** as **Static**, and define the **Azure VNet subnet (172.16.1.0/24)** as the static route.



Select the resources and additional configuration options that you want to use for the site-to-site VPN connection.

Details

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.

Value must be 256 characters or less in length.

Target gateway type [Info](#)

☒ Virtual private gateway

☐ Transit gateway

☐ Not associated

Virtual private gateway

Customer gateway [Info](#)

☒ Existing

☐ New

Customer gateway ID

Routing options [Info](#)

☐ Dynamic (requires BGP)

☒ Static

Static IP prefixes [Info](#)

172.16.1.0/24

X

Local IPv4 network CIDR - *optional*
The IPv4 CIDR range on the customer gateway (on-premises) side that is allowed to communicate over the VPN tunnels. The default is 0.0.0.0/0.

Remote IPv4 network CIDR - *optional*
The IPv4 CIDR range on the AWS side that is allowed to communicate over the VPN tunnels. The default is 0.0.0.0/0.

5. Download the VPN Configuration File
1. After the VPN is set up, download the configuration file.

2. Select **Generic** for the platform and **Vendor agnostic** for the software.

3. Select **IKEv2** for the IKE version.

VPN connections (1/1) [Info](#)

Actions

Download configuration

Create VPN connection

< 1 >

Name	VPN ID	State	Virtual private gateway	Transit gateway
aws-azure-vpn	vpn-00f7a2573f74a6ce2	Available	vgw-0465b5cf429d99a64	-



Choose the sample configuration you wish to download based on your customer gateway. Please note these are samples, and will need modification to use Advanced Algorithms, Certificates, and/or IPv6.

Vendor

The manufacturer of the customer gateway device (for example, Cisco Systems, Inc).

Generic

Platform

The class of the customer gateway device (for example, J-Series).

Generic

Software

The operating system running on the customer gateway device (for example, ScreenOS).

Vendor Agnostic

IKE version

The IKE version you are using for your VPN connection.

ikev2

Cancel

Download

2.5. Enable Route Propagation

After creating the VPN connection, go to Route Tables > Select the existing route table > Route Propagation > Edit Route Propagation, and enable propagation for the VGW.

VPC > Route tables > rtb-0a2ffc4ba97c748d7

rtb-0a2ffc4ba97c748d7

Actions

Details

Info

Route table ID

rtb-0a2ffc4ba97c748d7

VPC

vpc-0cba04b8819c978b0 | AWS-VPC

Main

Yes

Owner ID

495599740128

Explicit subnet associations

-

Edge associations

-

Routes

Subnet associations

Edge associations

Route propagation

Tags

Route Propagation (1)

Edit route propagation

Find virtual private gateway

< 1 > ⚙

Virtual Private Gateway

vgw-0465b5cf429d99a64 | AWS-VPN-VGW

Propagation

No

https://techcommunity.microsoft.com/blog/startupsatmicrosoftblog/how-to-easily-set-up-a-vpn-between-azure-and-aws-using-managed-services-updated-/4278966

9/18



Edit route propagation

Route table basic details

Route table ID

rtb-0a2ffc4ba97c748d7

Edit route propagation

Virtual Private Gateway

vgw-0465b5cf429d99a64 / AWS-VPN-VGW

Propagation

☒ Enable

Step 3: Finish the Azure Side Configuration

3.1. Create the Local Network Gateway

1. In the **Azure Portal**, go to **Local Network Gateway** > **Create**.
2. Name the gateway **AWSLocalNetworkGateway**, and enter the **public IP** of the AWS VPN tunnel (from the configuration file).
3. Set the **AWS VPC CIDR block** (e.g., *10.0.0.0/16*) as the address space.
4. In the next tab (Advanced), leave the option **Configure BGP Settings** defined to **No**

[Home](#) > [Local network gateways](#) >

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 *

MyLab

Resource group *

RG-AzureAWSVPN

Create new

Instance details

Region *

Central US

Name *

AWSLocalNetworkGateway

Endpoint ⓘ

IP address

FQDN

IP address * ⓘ

3.12.233.181

Address Space(s) ⓘ

10.0.0.0/16

Add additional address range

https://techcommunity.microsoft.com/blog/startupsatmicrosoftblog/how-to-easily-set-up-a-vpn-between-azure-and-aws-using-managed-services-updated-/4278966

10/18



Create local network gateway

Basics

Advanced

Review + create

Configure BGP settings

Yes

No

3.2. Create the VPN Connection

1. Go to **Azure Portal** > **Virtual Network Gateway** > **Connections** > **+ Add**.
2. Configure the connection:
 - **Name:** *AzureAWSVPNConnection*
 - **Connection Type:** **Site-to-site (IPsec)**.
 - **Virtual Network Gateway:** Select **AzureVPNGateway**.
 - **Local Network Gateway:** Select **AWSLocalNetworkGateway**.
 - **Shared Key (PSK):** Use the shared key from the AWS VPN configuration file.
 - **IKE Protocol:** Set to **IKEv2**.
 - **IPsec/IKE Policy:** Use **Default**, or configure **custom policies** per AWS (AES128, SHA1, DH Group 2).
 - **DPD Timeout:** Set to **45 seconds**.
 - **Connection Mode:** Leave as **Default** unless specific behavior is required.

[Home](#) > [Virtual network gateways](#) > [AzureVPNGateway | Connections](#) >

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 *

MyLab

Resource group *

RG-AzureAWSVPN

Create new

Instance details

Connection type * ⓘ

Site-to-site (IPsec)

Name *

AzureAWSVPNConnection

Region *

Central 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 *

AzureVPNGateway

Local network gateway *

AWSLocalNetworkGateway

Authentication Method

☒ Shared Key(PSK)

☐ Key Vault Certificate (Preview)

Shared Key(PSK) *

.....

IKE Protocol

☐ IKEv1

☒ IKEv2

Use Azure Private IP Address

☐

Enable BGP

☐

IPsec / IKE policy

Default

Custom

Use policy based traffic selector

Enable

Disable

DPD timeout in seconds *

45

Connection Mode

☒ Default

☐ InitiatorOnly

☐ ResponderOnly

In about 5 minutes, you can check the VPN connection established.

3.3. Ensure the VPN is established

1. From Site-to-Site VPN connections on AWS, go to Tunnel details and check that the Tunnel 1 is UP:

Tunnel details					
Static routes					
Tags					
⚠ This VPN connection is not using both tunnels. This mode of operation is not highly available and we strongly recommend you configure your second tunnel.					
Tunnel state					
Tunnel number	Outside IP address	Inside IPv4 CIDR	Inside IPv6 CIDR	Status	Last status change
Tunnel 1	3.12.233.181	169.254.210.176/30	-	Up	October 24, 2024, 11:27:01 (UTC-04:00)
Tunnel 2	3.131.201.76	169.254.53.104/30	-	Down	October 24, 2024, 10:11:04 (UTC-04:00)

2. From Azure side, check if the status of the VPN connection is Connected:



Home > NoMarketplace-20241024111702 | Overview >

AzureAWSVPNConnection

Connection

Search

Refresh

Move

Download configuration

Delete

Overview

Activity log

Access control (IAM)

Tags

Settings

Authentication

Configuration

Essentials

Resource group (move)

RG-AzureAWSVPN

Status

Connected

Location

Central US

Subscription (move)

MyLab

Subscription ID

313dd062-1c1c-428a-afc4-4e271378679f

Tags (edit)

Add tags

Step 4: Add Routes and Configure Security

4.1. Check the Route for Azure Subnets in AWS Route Table

1. In the **AWS Console**, go to **VPC > Route Tables**.
2. Check if the AWS Route Table has a route for the **Azure VNet subnet (172.16.1.0/24)** with the **VGW** as the target. If the route propagation enabled before was done correctly, you should be able to see the routes to Azure subnet (172.16.1.0/24) automatically added:

VPC > Route tables > rtb-0a2ffc4ba97c748d7

rtb-0a2ffc4ba97c748d7

Details Info

Route table ID

rtb-0a2ffc4ba97c748d7

VPC

vpc-0cba04b8819c978b0 | AWS-VPC

Main

Yes

Owner ID

495599740128

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (2)

Filter routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
172.16.1.0/24	vgw-0465b5cf429d99a64	Active	Yes

4.2. Add an Internet Gateway (IGW)

Note: An Internet Gateway (IGW) is required for the EC2 instance to be accessible via its public IP address. Without the IGW, the EC2 instance won't be reachable over the public internet, preventing you from logging into the EC2 using their public IP address. This is the sole purpose of deploying the IGW.

https://techcommunity.microsoft.com/blog/startupsatmicrosoftblog/how-to-easily-set-up-a-vpn-between-azure-and-aws-using-managed-services-updated-/4278966

13/18

AWS-IGW, then attach it to the AWS VPC.

2. **Update Route Table:** Add a route to **0.0.0.0/0** pointing to the IGW for external connectivity.

Route 3

Destination

Q 0.0.0.0/0

X

Target

Internet Gateway

▼

Q igw-0d4c70834e45bee7c

X

After adding the new route, you should have 3 routes as below:

VPC > Route tables > rtb-0da0773bee897e432

rtb-0da0773bee897e432

Details Info

Route table ID

rtb-0da0773bee897e432

VPC

vpc-067efd80f35ea02a0

Main

Yes

Owner ID

495599740128

Explicit subnet associations

-

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (3)

Q Filter routes

Destination	Target	Status	Propagated
0.0.0.0/0	igw-07454628c6856af86	Active	No
10.0.0.0/16	local	Active	No
172.16.1.0/24	vgw-00df8b500a652cab9	Active	Yes

4.3. Set Security Group and NSG Rules

1. **AWS Security Group:** Ensure the **Security Group** for the AWS EC2 instance allows **ICMP (ping)** and other protocols (e.g., SSH) from Azure.
2. **Azure NSG:** Similarly, ensure the **NSG** attached to the Azure VM’s NIC allows inbound traffic from AWS.

Step 5: Test Connectivity Between Azure and AWS VMs

To test connectivity between Azure and AWS, first deploy a virtual machine in the appropriate subnet on each cloud provider—an EC2 instance on AWS and a VM on Azure. Once both machines are running, connect to each VM using their respective public IP addresses. After logging in, use the private IP addresses of both instances to run a ping test and verify private network connectivity between them.



the Azure VM using their public IP address and test unilaterally running the ping command against the private IP of the EC2 VM.

5.1. Ensure ICMP Traffic Is Allowed

Both the **AWS Security Group** and **Azure NSG** should allow ICMP (ping) traffic.

5.2. Test Connectivity with ping

1. From the **Azure VM**, ping the **AWS VM** using its private IP:

```
rmmartins@vm01:~$ ping 10.0.1.177
PING 10.0.1.177 (10.0.1.177) 56(84) bytes of data.
64 bytes from 10.0.1.177: icmp_seq=1 ttl=64 time=21.9 ms
64 bytes from 10.0.1.177: icmp_seq=2 ttl=64 time=22.9 ms
64 bytes from 10.0.1.177: icmp_seq=3 ttl=64 time=21.3 ms
64 bytes from 10.0.1.177: icmp_seq=4 ttl=64 time=21.3 ms
^C
--- 10.0.1.177 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 21.306/21.875/22.941/0.663 ms
rmmartins@vm01:~$
```

2. From the **AWS VM**, ping the **Azure VM** using its private IP:

```
ubuntu@ip-10-0-1-177:~$ ping 172.16.1.4
PING 172.16.1.4 (172.16.1.4) 56(84) bytes of data.
64 bytes from 172.16.1.4: icmp_seq=1 ttl=64 time=20.8 ms
64 bytes from 172.16.1.4: icmp_seq=2 ttl=64 time=21.7 ms
64 bytes from 172.16.1.4: icmp_seq=3 ttl=64 time=21.7 ms
64 bytes from 172.16.1.4: icmp_seq=4 ttl=64 time=21.4 ms
^C
--- 172.16.1.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 20.837/21.401/21.736/0.351 ms
ubuntu@ip-10-0-1-177:~$ |
```

Troubleshooting Common Issues

1. Missing Static Route in AWS VPN

- Ensure that the **static route** for the **Azure VNet subnet (172.16.1.0/24)** is added in the AWS VPN configuration. Without this route, AWS will not know to send traffic to Azure through the VPN.

2. No Inbound Traffic on Azure VPN Gateway



3. Custom IPsec/IKE Policies

- If the default policies aren’t working, apply **custom IPsec/IKE policies** based on AWS configuration (AES128, SHA1, DH Group 2 for Phase 1 and Phase 2).

4. Further Troubleshooting

- For additional troubleshooting guidance, refer to the official Azure VPN diagnostics documentation: [Troubleshoot VPN with Azure Diagnostics](#).

Conclusion

By following this guide, you’ve successfully set up a VPN connection between **Azure** and **AWS** using managed services. Ensuring that the route for Azure’s subnet is added to the AWS Route Table is crucial for proper communication between the two clouds. If you need more advanced configurations, such as **BGP** for dynamic routing, consult the [Azure VPN Gateway documentation](#).

Updated Oct 28, 2024

VERSION 3.0

2

Comment



rmmartins MICROSOFT

Joined June 01, 2017

[View Profile](#)



[Startups at Microsoft](#)

Follow this blog board to get notified when there's new activity

Share



What's new

- Surface Pro 9
- Surface Laptop 5
- Surface Studio 2+
- Surface Laptop Go 2
- Surface Laptop Studio
- Surface Duo 2



Microsoft Store

- Account profile
- Download Center
- Microsoft Store support
- Returns
- Order tracking
- Virtual workshops and training
- Microsoft Store Promise
- Flexible Payments

Education

- Microsoft in education
- Devices for education
- Microsoft Teams for Education
- Microsoft 365 Education
- Education consultation appointment
- Educator training and development
- Deals for students and parents
- Azure for students

Business

- Microsoft Cloud
- Microsoft Security
- Dynamics 365
- Microsoft 365
- Microsoft Power Platform
- Microsoft Teams
- Microsoft Industry
- Small Business

Developer & IT

- Azure
- Developer Center
- Documentation
- Microsoft Learn
- Microsoft Tech Community
- Azure Marketplace
- AppSource
- Visual Studio

Company

- Careers
- About Microsoft
- Company news



[Register](#)

[Sign In](#)

- Diversity and inclusion
- Accessibility
- Sustainability



Your Privacy Choices

[Sitemap](#)

[Contact Microsoft](#)

[Privacy](#)

[Manage cookies](#)

[Terms of use](#)

[Trademarks](#)

[Safety & eco](#)

[About our ads](#)

© Microsoft 2024