

[Back to Blog](#)[← Newer Article](#)[Older Article →](#)

## Co-Authors

[rmmartins](#)

## Version history

**Last update:** Aug 22 2022 04:50 PM

**Updated by:** [rmmartins](#)

## Labels

[Infra](#)

122

By [Ricardo Macedo Martins](#)

Published Jun 17 2021 12:48 PM

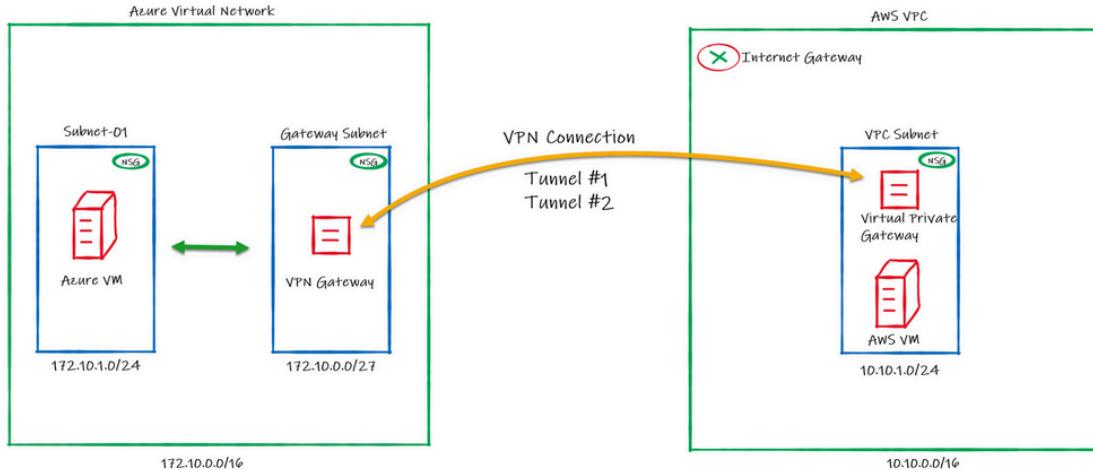
129K Views



What if you can establish a connection between Azure and AWS using only managed solutions instead to have to use virtual machines? This is exactly what we'll be covering on this article connecting AWS Virtual Private Gateway with the Azure VPN Gateway directly without worry to manage IaaS resources like virtual machines.

Below the draw of our lab:

[Skip for Main Navigation](#)



Share



Regarding the high availability, please note that on AWS, by default a VPN connection always will have 2 Public IPs, one per tunnel. On Azure it doesn't happen by default and in this case you will be using Active/Passive from Azure side.

This means that we will be setting only one "node" from Azure VPN Gateway to establish two VPN connections with AWS. In case of a failure, the second node from Azure VPN Gateway will connect to AWS in a Active/Passive mode.

## Configuring Azure

### 1. Create a resource group on Azure to deploy the resources on that

New - Microsoft Azure | +

← → ⌂ https://portal.azure.com/?feature.customportal=false#create/hub

Microsoft Azure

Dashboard >

Create a resource

Home

Dashboard

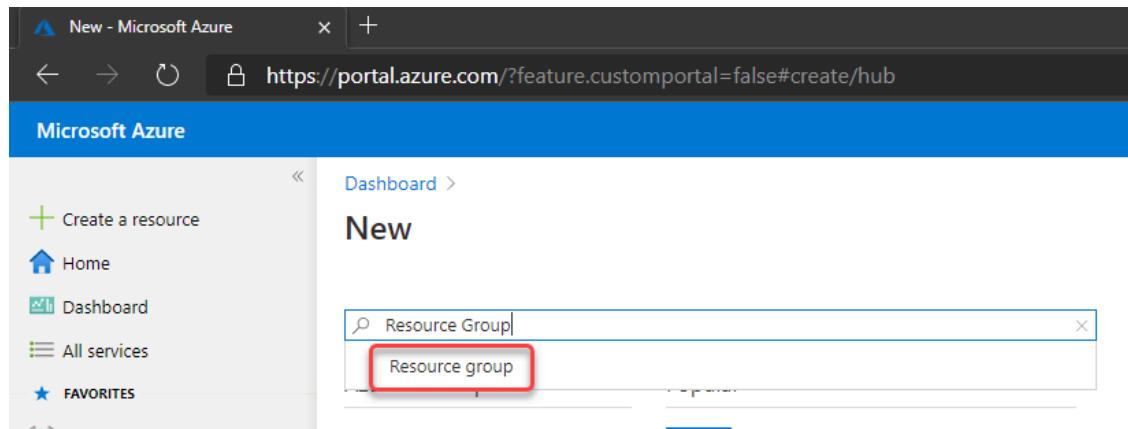
All services

FAVORITES

New

Resource Group

Resource group



Dashboard > New >

## Resource group

Microsoft



### Resource group

Save for later

Microsoft

Create

Choose the subscription, the name and the region to be deployed:

Skip for now Skip for later

## Create a resource group

Basics Tags Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

### Project details

Subscription \* ⓘ

Azure CXP FTA Internal Subscription RICMART

Resource group \* ⓘ

rg-azure-aws

### Resource details

Region \* ⓘ

(US) East US

## 2. Create a Virtual Network and a subnet

[Skip for now](#) [Save and continue](#)

New - Microsoft Azure

https://portal.azure.com/?feature.customportal=false#@microsoft.onmicrosoft.com/resource/subscri

Microsoft Azure

Create a resource

Home

Dashboard

All services

FAVORITES

Resource groups

Load balancers

All resources

Azure Synapse Analytics (f...)

Azure Cosmos DB

Virtual machines

Dashboard > rg-azure-aws >

New

Virtual Network

Virtual Network

Virtual network gateway

Azure Virtual Network Endpoints Management

KoçSistem Azure Virtual Network (VNet) Management

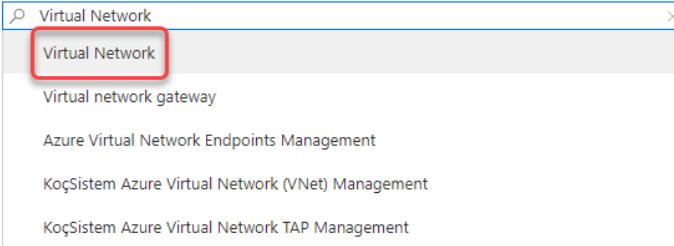
KoçSistem Azure Virtual Network TAP Management

Blockchain

Web App

Compute

Quickstarts + tutorials



## Virtual Network

Microsoft



## Virtual Network

Save for later

Microsoft

Azure benefit eligible

Create

Deploy with Resource Manager (change to Classic)

Define the subscription, resource group, name and region to be deployed:

Skip for now

## Create virtual network

Basics IP Addresses Security 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 about virtual network](#)

### Project details

Subscription \* ⓘ

Azure CXP FTA Internal Subscription RICMART

Resource group \* ⓘ

rg-azure-aws

[Create new](#)

### Instance details

Name \*

vnet-azure

Region \*

(US) East US

Set the address space for the virtual network and for the subnet. Here I'm defining the virtual network address space to **172.10.0.0/16**, changing the "default" subnet name to "**subnet-01**" and defining the subnet address range to **172.10.1.0/24**:

[Skip for now](#) [Next step](#)

## Create virtual network

Basics IP Addresses Security Tags Review + create

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

IPv4 address space

172.10.0.0/16		

Add IPv6 address space ⓘ

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

Add subnet Remove subnet

<input type="checkbox"/> Subnet name	Subnet address range
<input type="checkbox"/> subnet-01	172.10.1.0/24

[Skip for now](#) [Save and continue](#)

## Create virtual network

✓ Validation passed

Basics IP Addresses Security Tags **Review + create**

### Basics

Subscription Azure CXP FTA Internal Subscription RICMART  
Resource group rg-azure-aws  
Name vnet-azure  
Region East US

### IP addresses

Address space 172.10.0.0/16  
Subnet subnet-01 (172.10.1.0/24)

### Tags

None

### Security

BastionHost Disabled  
DDoS protection plan Basic  
Firewall Disabled

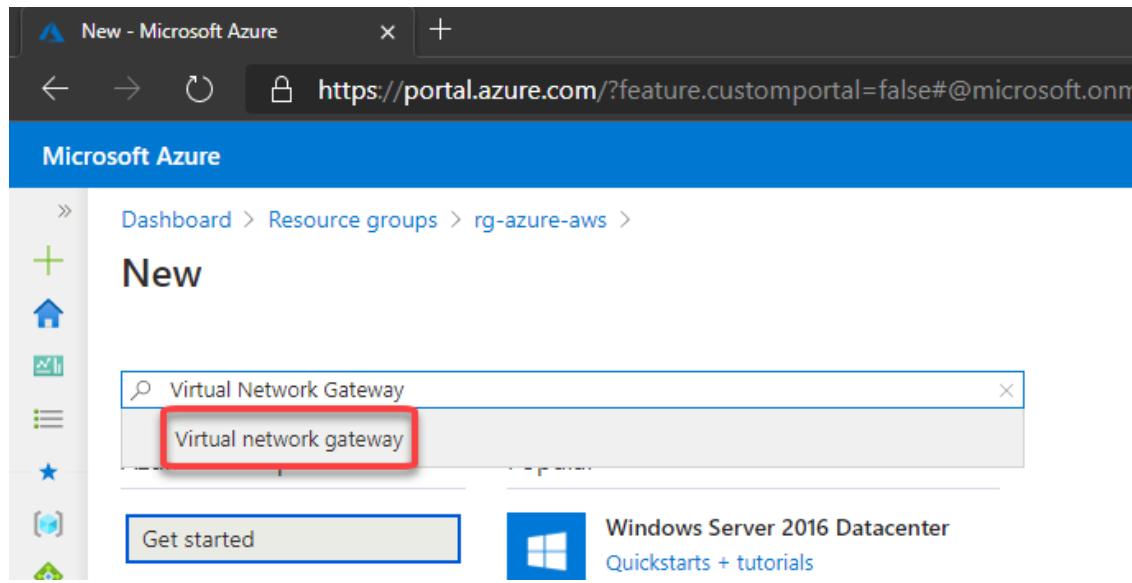
[Skip for now](#) [Save and continue](#)

### 3. Create the VPN Gateway

The Azure VPN Gateway is a resource composed of 2 or more VM's that are deployed to a specific subnet called Gateway Subnet where the recommendation is to use a /27. He contain routing tables and run specific gateway services. Note that you can't access those VM's.

To create, go to your Resource Group, then click to **+ Add**

The screenshot shows the Azure portal interface for a Resource Group named 'rg-azure-aws'. The 'Overview' tab is selected. At the top, there is a search bar, a '+ Add' button (which is highlighted with a red box), and other navigation links like 'Edit columns', 'Delete resource group', 'Refresh', and 'Export to CSV'. Below the search bar, the 'Essentials' section displays subscription information: 'Subscription (change) : Azure CXP FTA Internal Subscription RICMART' and 'Subscription ID : d9759156-c58b-4373-b08a-e7b28d114df4'. There is also a 'Tags' section with a link to 'Click here to add tags'. On the left, a sidebar lists 'Settings' with options like 'Quickstart', 'Deployments', 'Policies', 'Properties', and 'Locks'. The main content area shows a table with one record: 'Showing 1 to 1 of 1 records.' A filter bar at the bottom allows filtering by 'Name' and 'vnet-azure'.



Dashboard > Resource groups > rg-azure-aws > New >

## Virtual network gateway ↗

Microsoft

A screenshot of the 'Virtual network gateway' creation page. On the left is a blue sidebar with a three-dot icon. The main title is 'Virtual network gateway' in bold black font, followed by the Microsoft logo. Below the title is a purple button labeled 'Azure benefit eligible'. At the bottom of the sidebar is a large blue 'Create' button, which is also highlighted with a red box. To the right of the sidebar, there is a 'Save for later' button with a heart icon.

Then fill the fields like below:

[Skip for now](#) [Skip for later](#)

Create virtual network gateway - x + https://portal.azure.com/?feature.customportal=false#create/Microsoft.VirtualNetworkGateway-ARM

Microsoft Azure

Dashboard > Resource groups > rg-azure-aws > New > Virtual network gateway >

## 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 \*  (highlighted with red box)

Resource group

**Instance details**

Name \*  (highlighted with red box)

Region \*  (highlighted with red box)

Gateway type \*  VPN  ExpressRoute (highlighted with red arrow)

VPN type \*  Route-based  Policy-based (highlighted with red arrow)

SKU \*  (highlighted with red box)

Generation  (highlighted with red box)

Virtual network \*  (highlighted with red box)  
Only virtual networks in the currently selected subscription and region are listed.

Gateway subnet address range \*  (highlighted with red box)  
172.10.0.0 - 172.10.0.255 (256 addresses)

**Public IP address**

Public IP address \*  Create new  Use existing (highlighted with red arrow)

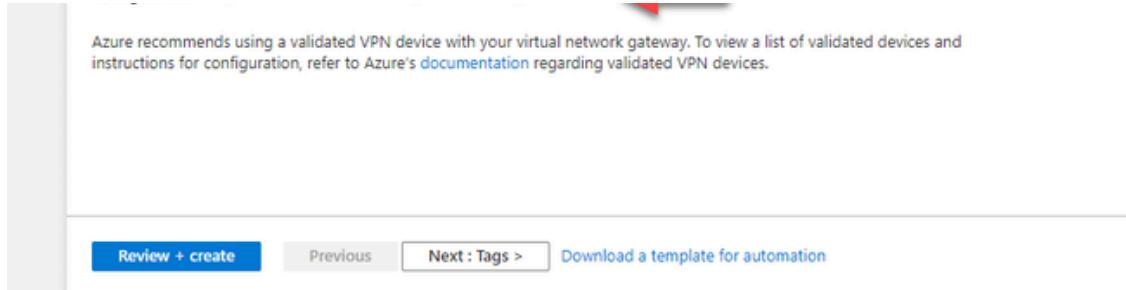
Public IP address name \*  (highlighted with red box)

Public IP address SKU Basic  
 Dynamic  Static

Assignment  
 Enabled  Disabled (highlighted with red arrow)

Configure BGP \*  Enabled  Disabled (highlighted with red arrow)

Skip to Primary Navigation



After click to Review + create, in a few minutes the Virtual Network Gateway will be ready:

vpn-azure-aws

Virtual network gateway

Resource group (change)  
rg-azure-aws

Location  
East US

Subscription (change)  
Azure CXP FTA Internal Subscription RICMART

SKU  
VpnGw1

Gateway type  
VPN

VPN type  
Route-based

Virtual network  
vnet-azure

Public IP address  
20.185.83.40 (pip-vpn-azure-aws)

## Configuring AWS

### 4. Create the Virtual Private Cloud (VPC)

Skip [For M&S Integration](#)

VPC Management Console x +

https://console.aws.amazon.com/vpc/home?region=us-east-1#CreateVpc:

aws Services ▾

VPC > Your VPCs > Create VPC

## Create VPC Info

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

**VPC settings**

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

my-vpc-01

IPv4 CIDR block Info  
10.10.0.0/16

IPv6 CIDR block Info  
 No IPv6 CIDR block  
 Amazon-provided IPv6 CIDR block  
 IPv6 CIDR owned by me

Tenancy Info  
Default

**Tags**  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

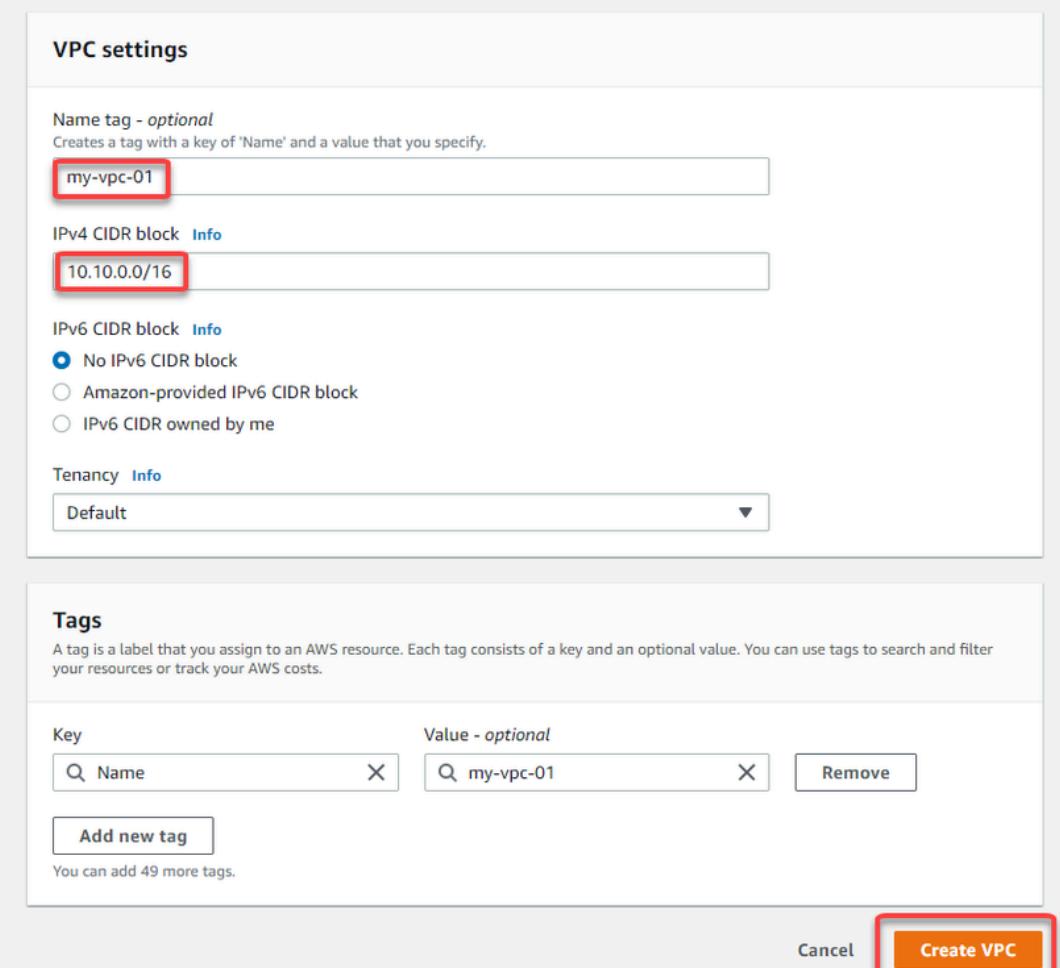
Key Value - *optional*

Name my-vpc-01 Remove

Add new tag

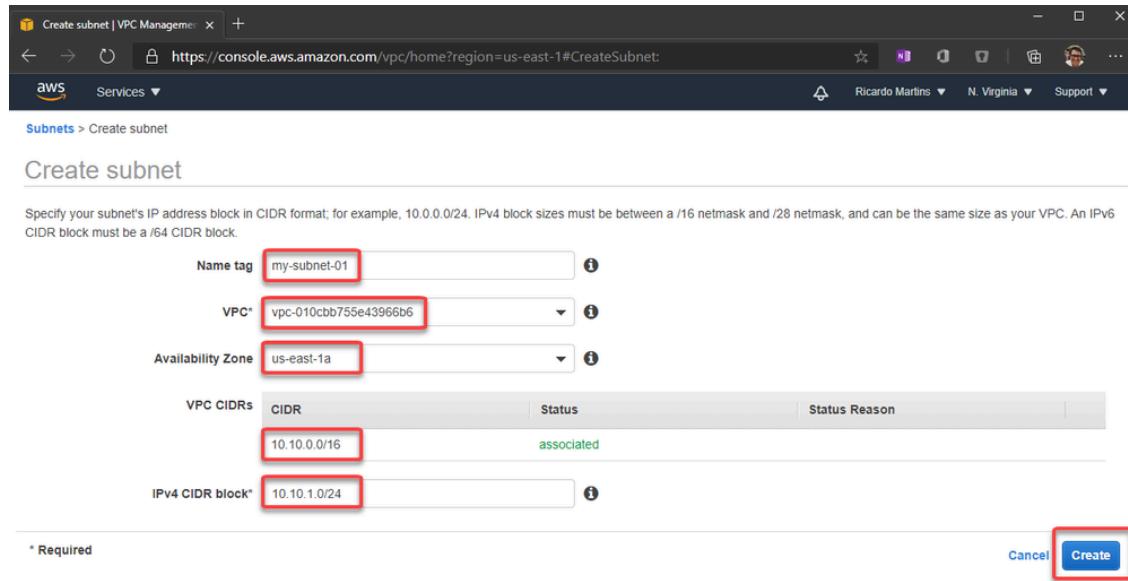
You can add 49 more tags.

Cancel **Create VPC**



## 5. Create a subnet inside the VPC (Virtual Network)

Skip [For Lambda Function](#)



## 6. Create a customer gateway pointing to the public ip address of Azure VPN

### Gateway

The Customer Gateway is an AWS resource with information to AWS about the customer gateway device, which in this case is the Azure VPN Gateway.

Create Customer Gateway | VPC

https://console.aws.amazon.com/vpc/home?region=us-east-1#CreateCustomerGateway;CustomerGatewayId=cgw-0a4783b50da7a5630

aws Services ▾

Customer Gateways > Create Customer Gateway

### Create Customer Gateway

Specify the Internet-routable IP address for your gateway's external interface; the address must be static and may be behind a device performing network address translation (NAT). For dynamic routing, also specify your gateway's Border Gateway Protocol (BGP) Autonomous System Number (ASN); this can be either a public or private ASN (such as those in the 64512-65534 range).

VPNs can use either Pre-Shared Keys or Certificates for authentication. When using Certificate authentication, an IP address is optional. To use Certificate authentication, specify a Certificate ARN when you create your Customer Gateway. To use Pre-Shared Keys, only an IP address is required.

Name  ⓘ

Routing  Static  Dynamic

IP Address  ⓘ

Certificate ARN  ⓘ

Device  ⓘ

\* Required

Cancel **Create Customer Gateway**

## 7. Create the Virtual Private Gateway then attach to the VPC

Create Virtual Private Gateway | VPC

https://console.aws.amazon.com/vpc/home?region=us-east-1#CreateVirtualPrivateGateway;

aws Services ▾

Virtual Private Gateways > Create Virtual Private Gateway

### Create Virtual Private Gateway

A virtual private gateway is the router on the Amazon side of the VPN tunnel.

Name tag  ⓘ

ASN  Amazon default ASN  Custom ASN

\* Required

Cancel **Create Virtual Private Gateway**

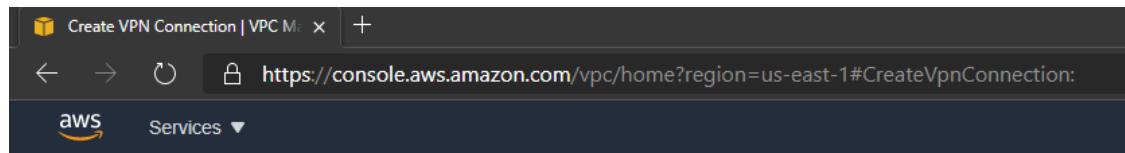
Skip [Skip for Manual Configuration](#)

The screenshot shows the AWS VPC console with the URL <https://console.aws.amazon.com/vpc/home?region=us-east-1#VpnGateways:sort=VpnGatewayId>. The left sidebar under 'CLOUD' shows 'Your VPCs New' with one entry: 'Subnets'. The main area displays a table of 'Virtual Private Gateways'. One row is selected, showing details: Name 'vgw-aws-azure', ID 'vgw-033b3758fae1f6443', State 'detached', Type 'ipsec.1', and VPC 'None'. A context menu is open over this row, with the 'Attach to VPC' option highlighted by a red box.

The screenshot shows the 'Attach to VPC' dialog box from the AWS VPC console. The URL is <https://console.aws.amazon.com/vpc/home?region=us-east-1#AttachVGWToVPC:VpnGatewayId=vgw-0...>. The dialog title is 'Attach to VPC'. It says 'Select the VPC to attach to the virtual private gateway.' Below is a dropdown labeled 'Virtual Private Gateway Id' with 'vgw-033b3758fae1f6443'. A dropdown labeled 'VPC\*' has 'my-vpc-01' selected. A 'Cancel' button and a 'Yes, Attach' button are at the bottom right. A red box highlights the 'my-vpc-01' selection in the dropdown.

## 8. Create a site-to-site VPN Connection

[Skip for now](#) [Next Step](#)



VPN Connections > Create VPN Connection

## Create VPN Connection

Select the target gateway and customer gateway that you would like to connect via a VPN connection. You must have entered the target gateway and customer gateway information in the previous step.

Name tag  ⓘ

Target Gateway Type  Virtual Private Gateway  Transit Gateway

Virtual Private Gateway\*  ⓘ

Customer Gateway  Existing  New

Customer Gateway ID\*  ⓘ

Filter by attributes

Customer Gateway ID	Name tag	IP Address	Certificate ARN
cgw-01c9644443bf20a28	cg-aws-azure	20.185.83.40	

Set the routing as static pointing to the azure subnet-01 prefix (172.10.1.0/24)

[Skip for Main Navigation](#)

Routing Options  Dynamic (requires BGP)  Static

IP Prefixes	Source	State	
172.10.1.0/24	-	-	X

Add Another Rule

Tunnel Inside Ip Version  IPv4  IPv6

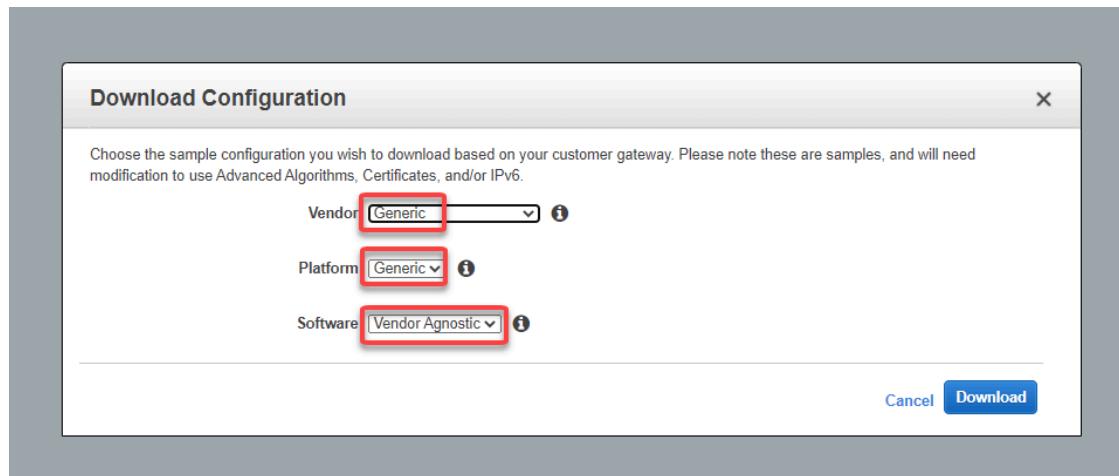
Local IPv4 Network Cidr: 0.0.0.0/0

Remote IPv4 Network Cidr: 0.0.0.0/0

After fill the options, click to create.

## 9. Download the configuration file

Please note that you need to change the Vendor, Platform and Software to Generic since Azure isn't a valid option:



In this configuration file you will note that there are the Shared Keys and the Public Ip Address for each of one of the two IPSec tunnels created by AWS:

[Skip to Formular Generation](#)

## IPSec Tunnel #1

### #1: Internet Key Exchange Configuration

Configure the IKE SA as follows:

Please note, these sample configurations are for the minimum requirement of AES128. Category "VPN" connections in the GovCloud region have a minimum requirement of AES256. You will need to modify these sample configuration files to take advantage of AES256. NOTE: If you customized tunnel options when creating or modifying your VPN connection, the tunnel may not work correctly.

Higher parameters are only available for VPNs of category "VPN," and not for "VPN". The address of the external interface for your customer gateway must be a static IP address. Your customer gateway may reside behind a device performing network address translation (NAT). To ensure that NAT traversal (NAT-T) can function, you must adjust your firewall settings.

- IKE version : IKEv1
- Authentication Method : Pre-Shared Key
- Pre-Shared Key : XXXXXXXXXX
- Authentication Algorithm : sha1
- Encryption Algorithm : aes-128-cbc
- Lifetime : 28800 seconds
- Phase 1 Negotiation Mode : main
- Diffie-Hellman : Group 2

## #2: IPSec Configuration

Configure the IPSec SA as follows:

Category "VPN" connections in the GovCloud region have a minimum requirement of AES-256-CBC-HMACSHA256. Please note, you may use these additionally supported IPSec parameters for encrypting traffic.

NOTE: If you customized tunnel options when creating or modifying your VPN connection, the following configuration will be used.

Higher parameters are only available for VPNs of category "VPN," and not for "VPN-Classic."

- Protocol : esp
- Authentication Algorithm : hmac-sha1-96
- Encryption Algorithm : aes-128-cbc-hmacsha256
- Lifetime : 3600 seconds
- Mode : tunnel
- Perfect Forward Secrecy : Diffie-Hellman Group 2

IPSec Dead Peer Detection (DPD) will be enabled on the AWS Endpoint. We recommend configuring DPD on your endpoint as follows:

- DPD Interval : 10
- DPD Retries : 3

IPSec ESP (Encapsulating Security Payload) inserts additional headers to transmit packets. These headers require additional space, which reduces the amount of space available to transmit application data.

To limit the impact of this behavior, we recommend the following configuration on your Customer Gateway:

- TCP MSS Adjustment : 1379 bytes
- Clear Don't Fragment Bit : enabled
- Fragmentation : Before encryption

## #3: Tunnel Interface Configuration

Your Customer Gateway must be configured with a tunnel interface that is associated with the IPSec tunnel. All traffic transmitted to the tunnel interface is encrypted and transmitted to the Virtual Private Gateway.

The Customer Gateway and Virtual Private Gateway each have two addresses that relate to this IPSec tunnel. Each contains an outside address, upon which encrypted traffic is exchanged. Each also contains an inside address associated with the tunnel interface.

[Skip to Primary Navigation](#)

The Customer Gateway outside IP address was provided when the Customer Gateway was created.

The customer gateway outside IP address was provided when the customer gateway was created. Changing the IP address requires the creation of a new Customer Gateway.

The Customer Gateway inside IP address should be configured on your tunnel interface.

Outside IP Addresses:

- Customer Gateway : 20.185.83.40
- Virtual Private Gateway : 3.209.186.24

IPSec Tunnel #2

#1: Internet Key Exchange Configuration

Configure the IKE SA as follows:

Please note, these sample configurations are for the minimum requirement of AES128. Category "VPN" connections in the GovCloud region have a minimum requirement of AES256. You will need to modify these sample configuration files to take advantage of AES256. NOTE: If you customized tunnel options when creating or modifying your VPN connection,

Higher parameters are only available for VPNs of category "VPN," and not for "VPN". The address of the external interface for your customer gateway must be a static IP address. Your customer gateway may reside behind a device performing network address translation (NAT). To ensure that NAT traversal (NAT-T) can function, you must adjust your firewall settings.

- IKE version : IKEv1
- Authentication Method : Pre-Shared Key
- Pre-Shared Key : [REDACTED]
- Authentication Algorithm : sha1
- Encryption Algorithm : aes-128-cbc
- Lifetime : 28800 seconds
- Phase 1 Negotiation Mode : main
- Diffie-Hellman : Group 2

## #2: IPsec Configuration

Configure the IPsec SA as follows:

Category "VPN" connections in the GovCloud region have a minimum requirement of AH + ESP. Please note, you may use these additionally supported IPsec parameters for encryption.

NOTE: If you customized tunnel options when creating or modifying your VPN connection, the following parameters will be used.

Higher parameters are only available for VPNs of category "VPN," and not for "VPN with IPsec."

- Protocol : esp
- Authentication Algorithm : hmac-sha1-96
- Encryption Algorithm : aes-128-cbc
- Lifetime : 3600 seconds
- Mode : tunnel
- Perfect Forward Secrecy : Diffie-Hellman Group 2

IPSec Dead Peer Detection (DPD) will be enabled on the AWS Endpoint. We recommend configuring DPD on your endpoint as follows:

- DPD Interval : 10
- DPD Retries : 3

IPSec ESP (Encapsulating Security Payload) inserts additional headers to transmit packets. These headers require additional space, which reduces the amount of space available to transmit application data.

To limit the impact of this behavior, we recommend the following configuration on your Customer Gateway:

- TCP MSS Adjustment : 1379 bytes
- Clear Don't Fragment Bit : enabled
- Fragmentation : Before encryption

## #3: Tunnel Interface Configuration

Your Customer Gateway must be configured with a tunnel interface that is associated with the IPsec tunnel. All traffic transmitted to the tunnel interface is encrypted and transmitted to the Virtual Private Gateway.

The Customer Gateway and Virtual Private Gateway each have two addresses that relate to this IPsec tunnel. Each contains an outside address, upon which encrypted traffic is exchanged. Each also contain an inside address associated with the tunnel interface.

[Skip to Primary Navigation](#)

The Customer Gateway outside IP address was provided when the Customer Gateway was created. Changing the IP address requires the creation of a new Customer Gateway.

The Customer Gateway inside IP address should be configured on your tunnel interface.

#### Outside IP Addresses:

- Customer Gateway : 20.185.83.40
- Virtual Private Gateway : 52.70.171.101

After the creation, you should have something like this:

The screenshot shows the AWS VPC Dashboard with the 'Create VPN Connection' button highlighted. A table lists the created VPN connection: Name: vpn-aws-azure, VPN ID: vpn-0ca74f7bd72086f4b, State: available, Virtual Private Gateway: vgw-033b3758fae1f6443 | vpg-aws-azure, Transit Gateway: -, Inside IP Version: IPv4, Type: ipsec.1, Category: VPN, and VPC: vpc-01ccb755e439. Below the table, the 'Details' tab of the VPN connection configuration is selected, displaying various parameters such as VPN ID, Virtual Private Gateway, Customer Gateway Address, and Authentication Type.

## Adding the AWS information on Azure Configuration

### 10. Now let's create the Local Network Gateway

The Local Network Gateway is an Azure resource with information to Azure about the customer gateway device, in this case the AWS Virtual Private Gateway

Skip for now

New - Microsoft Azure    x | +

← → ⏪ 🔒 https://portal.azure.com/?feature.customportal=false#create/hub

Microsoft Azure

Dashboard >

**New**

Local Network Gateway

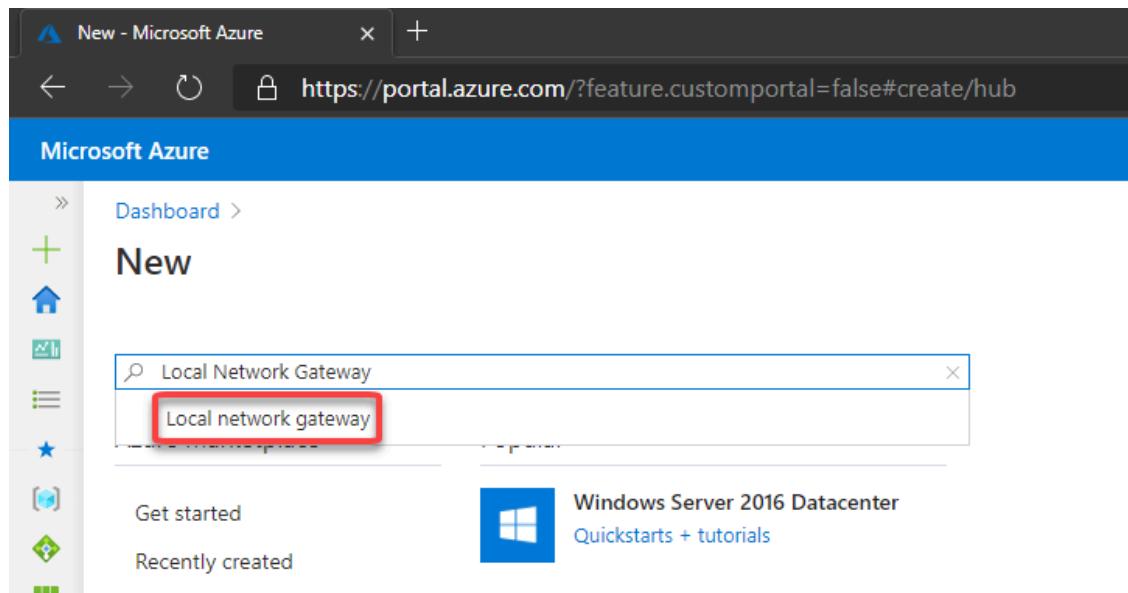
Local network gateway

Get started

Windows Server 2016 Datacenter

Recently created

Quickstarts + tutorials



Local network gateway - Microsoft    x | +

← → ⏪ 🔒 https://portal.azure.com/?feature.customportal=false#create

Microsoft Azure

Dashboard > New >

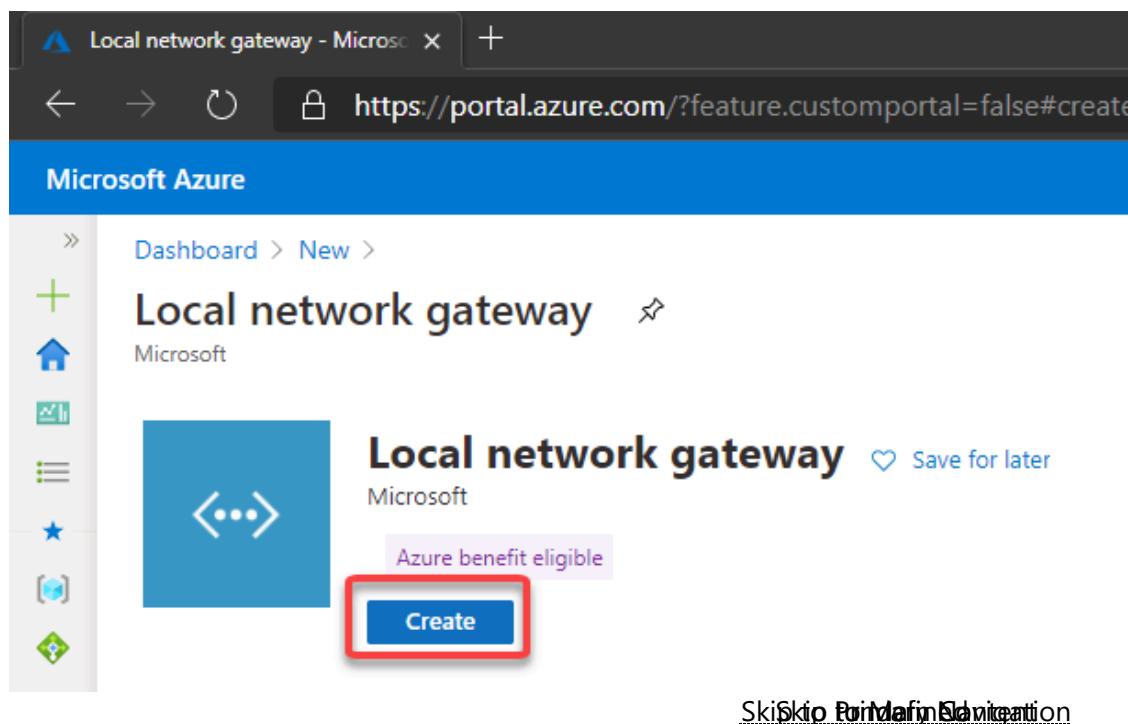
**Local network gateway** ⚡

Microsoft

Azure benefit eligible

Create

Skip for now



Now you need to specify the public ip address from the AWS Virtual Private Gateway and the VPC CIDR prefix.

Please note that the public address from the AWS Virtual Private Gateway is described at the configuration file you have downloaded.

As mentioned earlier, AWS creates two IPSec tunnels to high availability purposes. I'll use the public ip address from the IPSec Tunnel #1 for now.

Create local network gateway - Microsoft Azure

https://portal.azure.com/?feature.customportal=false#crea

Microsoft Azure

Search resources, services, and docs (G+)

Dashboard > New > Local network gateway >

## Create local network gateway

Name \*

 ✓

Endpoint ⓘ

IP address FQDN

IP address \* ⓘ

 ✓

Address space ⓘ

10.10.0.0/16 ...

Add additional address range ...

Configure BGP settings

Subscription \*

Azure CXP FTA Internal Subscription Rl... ▼

Resource group \* ⓘ

rg-azure-aws ▼

Create new

Location \*

East US Skip to Primary Navigation

Create a resource

Home

Dashboard

All services

FAVORITES

Resource groups

Load balancers

All resources

Azure Synapse Analytics (f...)

Azure Cosmos DB

Virtual machines

Storage accounts

Virtual networks

Azure Active Directory

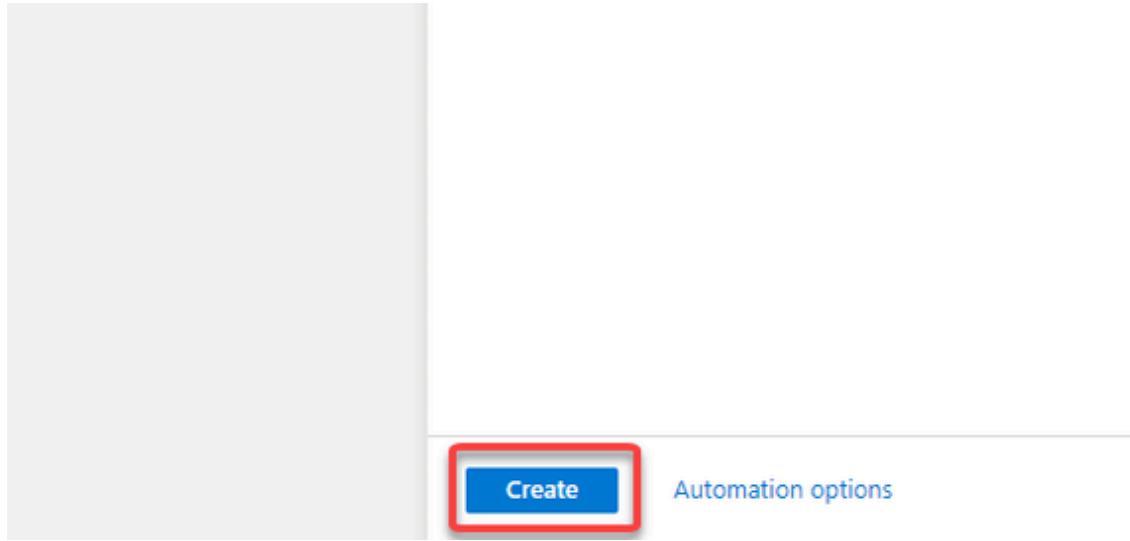
Monitor

Advisor

Security Center

Help + support

Cost Management + Billing



## 11. Then let's create the connection on the Virtual Network Gateway

A screenshot of the Microsoft Azure portal showing the 'rg-azure-aws' resource group details page. The URL in the browser is https://portal.azure.com/?feature.customportal=false#@microsoft.onmicrosoft.com/resource/subscriptions/d975. The left sidebar shows various service categories like Home, Dashboard, All services, and Resource groups. The main content area shows the 'rg-azure-aws' resource group overview, including sections for Overview, Activity log, Access control (IAM), Tags, Settings, and Cost Management. A list of resources is displayed, including 'vnet-azure' and 'vpn-azure-aws'. A red box highlights the 'rg-azure-aws' resource group name at the top of the page. A red box also highlights the 'Skip to Primary Navigation' link at the bottom of the page.

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a navigation menu with various options like 'Create a resource', 'Home', 'Dashboard', 'All services', 'FAVORITES' (which includes 'Resource groups', 'Load balancers', 'All resources', 'Azure Synapse Analytics', 'Azure Cosmos DB', 'Virtual machines', 'Storage accounts', 'Virtual networks', 'Azure Active Directory', 'Monitor', 'Advisor', and 'Security Center'). The main content area is titled 'vpn-azure-aws | Connections' and shows a 'Virtual network gateway' with 'Directory: Microsoft'. It includes a search bar ('Search (Ctrl+/)'), a '+ Add' button (highlighted with a red box), a 'Refresh' button, and a 'Search connections' input field. Below these are links for 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', and a 'Settings' section with 'Configuration' (highlighted with a red box) and 'Connections' (also highlighted with a red box). Other settings include 'Point-to-site configuration', 'Properties', 'Locks', 'Monitoring', and 'Logs'.

You should fill the fields according below. Please note that the Shared key was obtained at the configuration file downloaded earlier and In this case, I'm using the Shared Key for the Ipsec tunnel #1 created by AWS and described at the configuration file.

[Skip](#) [For Main Navigation](#)

Add connection - Microsoft Azure +

https://portal.azure.com/?feature.customportal=false#@microsoft.onmicrosoft.com

Microsoft Azure

Dashboard > Resource groups > rg-azure-aws > vpn-azure-aws >

Create a resource

Home

Dashboard

All services

FAVORITES

Resource groups

Load balancers

All resources

Azure Synapse Analytics (f...)

Azure Cosmos DB

Virtual machines

Storage accounts

Virtual networks

Azure Active Directory

Monitor

Advisor

Security Center

Help + support

Cost Management + Billing

## Add connection

vpn-azure-aws | Directory: Microsoft

Name \*

connection-azure-aws

Connection type ⓘ

Site-to-site (IPsec)

\*Virtual network gateway ⓘ

vpn-azure-aws

\*Local network gateway ⓘ

Ing-azure-aws

Shared key (PSK) \*

[REDACTED]

Use Azure Private IP Address ⓘ

Enable BGP ⓘ

IKE Protocol ⓘ

IKEv1  IKEv2

Subscription ⓘ

Azure CXP FTA Internal Subscription Rl...

Resource group ⓘ

rg-azure-aws

Create new

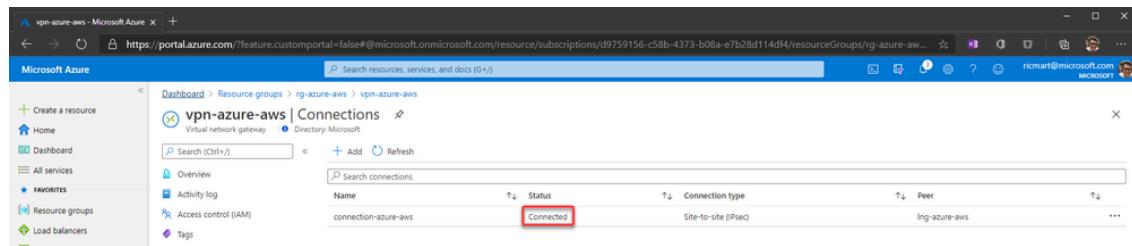
Location ⓘ

East US

Skip to Primary Navigation

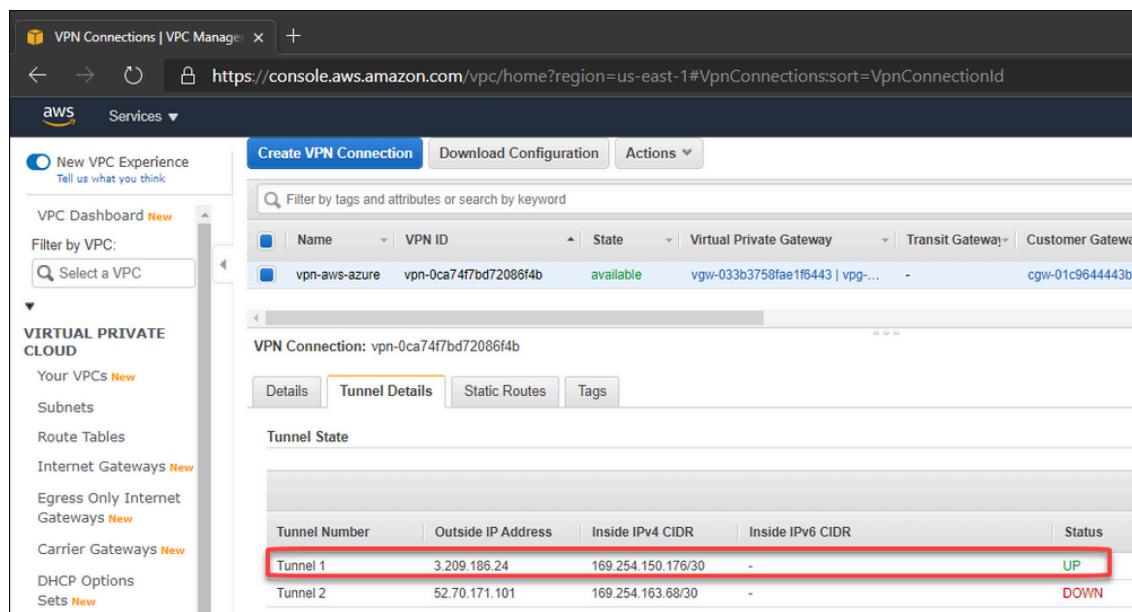
The screenshot shows the 'Add connection' wizard in the Microsoft Azure portal. The 'Name' field is set to 'connection-azure-aws'. The 'Connection type' dropdown is set to 'Site-to-site (IPsec)'. Under 'Virtual network gateway', the value 'vpn-azure-aws' is entered. Under 'Local network gateway', the value 'Ing-azure-aws' is entered. The 'Shared key (PSK)' field is empty. The 'IKE Protocol' section shows 'IKEv2' selected (indicated by a red arrow). The 'Subscription' dropdown is set to 'Azure CXP FTA Internal Subscription Rl...'. The 'Resource group' dropdown is set to 'rg-azure-aws'. The 'Location' dropdown is set to 'East US'.

After a few minutes, you can see the connection established:



The screenshot shows the Microsoft Azure portal interface. The user is in the 'Connections' section of a resource group named 'vpn-azure-aws'. A single connection named 'connection-azure-aws' is listed, and its status is highlighted with a red box, showing 'Connected'. The connection type is 'Site-to-site (IPsec)' and the peer is 'ing-azure-aws'.

In the same way, we can check on AWS that the 1st tunnel is up:



The screenshot shows the AWS VPC Manager interface. The user is viewing a 'VPN Connections' page. A single connection named 'vpn-aws-azure' is listed with the status 'available'. The 'Tunnel Details' tab is selected, showing two tunnels. Tunnel 1 has an 'Outside IP Address' of 3.209.186.24, an 'Inside IPv4 CIDR' of 169.254.150.176/30, and a 'Status' of 'UP', which is highlighted with a red box. Tunnel 2 has an 'Outside IP Address' of 52.70.171.101, an 'Inside IPv4 CIDR' of 169.254.163.68/30, and a 'Status' of 'DOWN'.

Now let's edit the route table associated with our VPC

The screenshot shows the AWS VPC Management console with the URL <https://console.aws.amazon.com/vpc/home?region=us-east-1#RouteTables:sort=routeTableId>. On the left, there's a sidebar with 'Route Tables' highlighted. The main area shows a table of route tables. A context menu is open over the first row, listing options like 'Set Main Route Table', 'Delete Route Table', 'Edit subnet associations', 'Edit edge associations', 'Edit route propagation', 'Edit routes' (which is highlighted with a red box), and 'Add/Edit Tags'. The table has columns for Name, Route Table ID, Explicit subnet association, Edge associations, and Main.

And add the route to Azure subnet through the Virtual Private Gateway:

The screenshot shows the 'Edit routes' page with the URL <https://console.aws.amazon.com/vpc/home?region=us-east-1#EditRoutes:routeTableId=rtb-03e2fd026035b7d69>. It displays a table of existing routes and a form for adding a new route. The new route being added has a destination of '172.10.1.0/24', a target of 'vgw-', and a gateway of 'vgw-033b3758fae1f6443'. The 'Save routes' button at the bottom right is highlighted with a red box.

## 12. Adding high availability

Now we can create a 2nd connection to ensure high availability. To do this let's create another Local Network Gateway which we will point to the public ip address of the IPSec tunnel #2 on the AWS

[Skip for now](#) [Next](#)

Create local network gateway - Microsoft Azure

https://portal.azure.com/?feature.customportal=false#cre

Microsoft Azure

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

Dashboard > New > Local network gateway >

## Create local network gateway

Name \*

 ✓

Endpoint ⓘ

IP address FQDN

IP address \* ⓘ

 ✓

Address space ⓘ

10.10.0.0/16 ...

Add additional address range ...

Configure BGP settings

Subscription \*

Azure CXP FTA Internal Subscription RI... ▼

Resource group \* ⓘ

rg-azure-aws ▼

[Create new](#)

Location \*

East US ▼

[Skip to Primary Navigation](#)

Create a resource

Home

Dashboard

All services

FAVORITES

Resource groups

Load balancers

All resources

Azure Synapse Analytics (f...)

Azure Cosmos DB

Virtual machines

Storage accounts

Virtual networks

Azure Active Directory

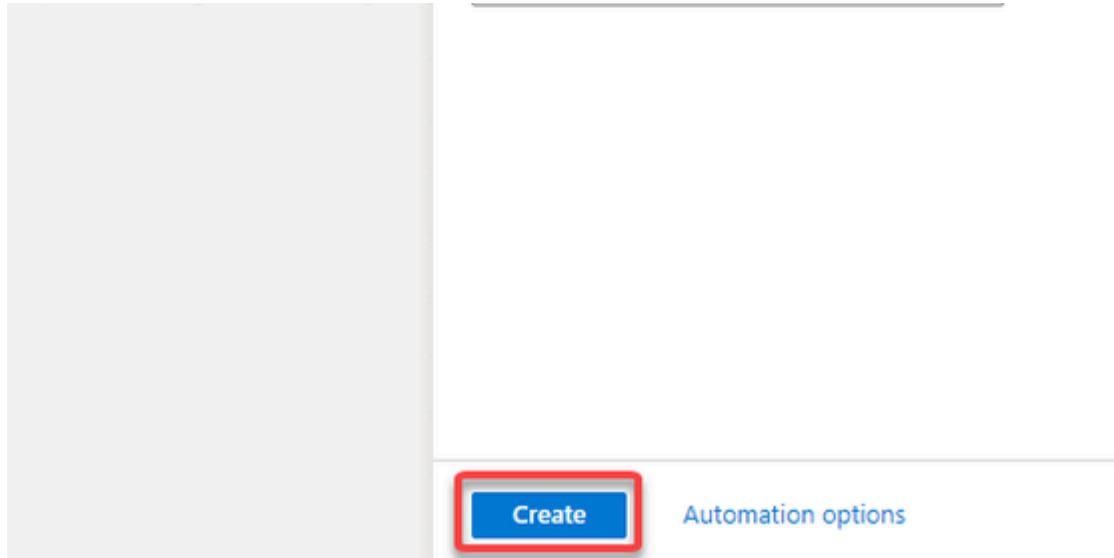
Monitor

Advisor

Security Center

Help + support

Cost Management + Billing



Then we can create the 2nd connection on the Virtual Network Gateway:

[Skip for now](#) [Get started](#)

Add connection - Microsoft Azure x +

← → ⌂ https://portal.azure.com/?feature.customportal=false#@microsoft.onmicrosoft.com

Microsoft Azure

Dashboard > Resource groups > rg-azure-aws > vpn-azure-aws >

**Add connection**

vpn-azure-aws | Directory: Microsoft

Name \*  

Connection type ⓘ  

\*Virtual network gateway ⓘ  

\*Local network gateway ⓘ  

Shared key (PSK) \* ⓘ  

Use Azure Private IP Address ⓘ

Enable BGP ⓘ

IKE Protocol ⓘ  IKEv1  IKEv2 

Subscription ⓘ  

Resource group ⓘ  

Create new

Location ⓘ

Skip to Primary Navigation

Create a resource

Home

Dashboard

All services

FAVORITES

Resource groups

Load balancers

All resources

Azure Synapse Analytics (f...)

Azure Cosmos DB

Virtual machines

Storage accounts

Virtual networks

Azure Active Directory

Monitor

Advisor

Security Center

Help + support

Cost Management + Billing



And in a few moments we'll have:

The image contains two screenshots side-by-side.

**Microsoft Azure Screenshot:** The URL is https://portal.azure.com/?feature.customportal=false#@microsoft.onmicrosoft.com/resource/subscripti... . It shows the 'Connections' page for a 'Virtual network gateway'. There are two entries in the table:

Name	Status	Connection type	Peer
connection-azure-aws	Connected	Site-to-site (IPsec)	Ing-azure-aws
connection-azure-aws-standby	Connected	Site-to-site (IPsec)	Ins-azure-aws-standby

**AWS VPC Manager Screenshot:** The URL is https://console.aws.amazon.com/vpc/home?region=us-east-1#VpnConnections:VpnConnectionId=vpn-0ca74f7bd72086f4b . It shows the 'VPN Connections' page. A single connection is listed:

Name	VPN ID	State	Virtual Private Gateway	Transit Gateway	Customer Gateway
vpn-aws-azure	vpn-0ca74f7bd72086f4b	available	vgw-033b3758fae1f6443   vpg-...	-	cgw-01c9644443

Below the table, under 'Tunnel Details', there is a 'Tunnel State' table:

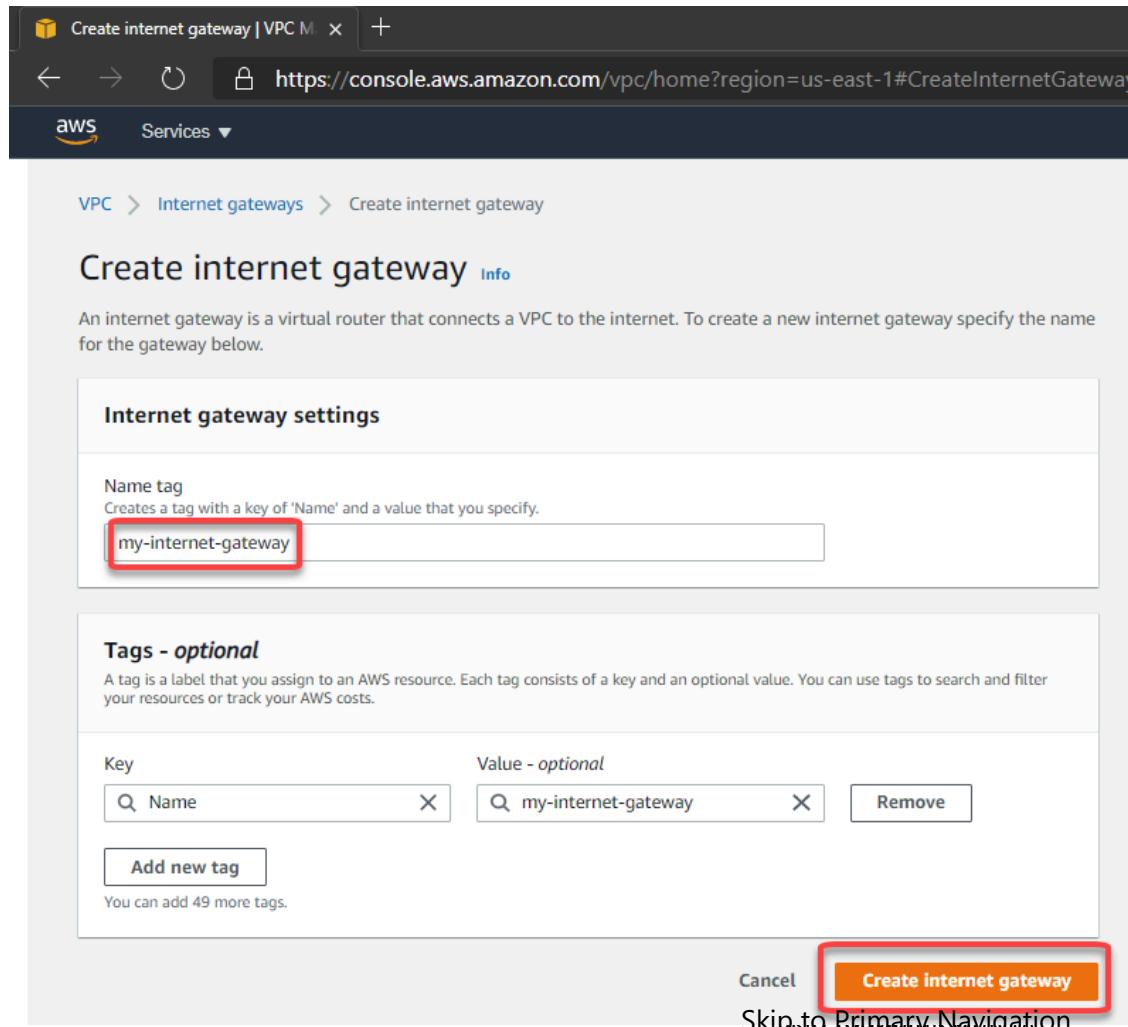
Tunnel Number	Outside IP Address	Inside IPv4 CIDR	Inside IPv6 CIDR	Status
Tunnel 1	3.209.186.24	169.254.150.176/30	-	UP
Tunnel 2	52.70.171.101	169.254.163.68/30	-	UP

With this, our VPN connection is established on both sides and the work is done.

Skip to [Final Navigation](#)

### 13. Let's test!

First, let's add an Internet Gateway to our VPC at AWS. The Internet Gateway is a logical connection between an Amazon VPN and the Internet. This resource will allow us to connect through the test VM from their public ip through internet. This is not required for the VPN connection, is just for our test:

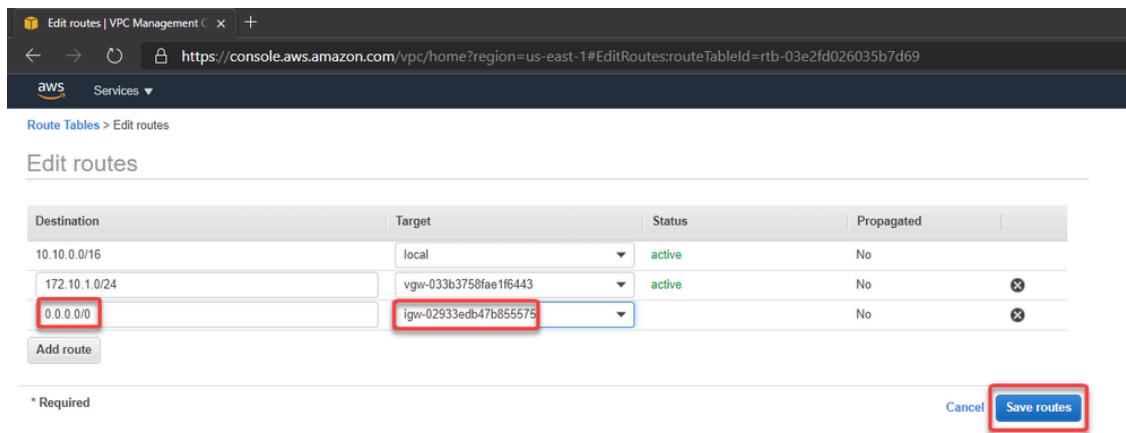


After create, let's attach to the VPC:

The screenshot shows the AWS VPC Management Console. On the left, there is a navigation sidebar with options like 'New VPC Experience', 'VPC Dashboard', 'Internet Gateways', 'Egress Only Internet Gateways', 'Carrier Gateways', 'DHCP Options Sets', and 'Route Tables'. The main content area is titled 'igw-02933edb47b855575 / my-internet-gateway'. It displays the Internet gateway ID (igw-02933edb47b855575), state (Detached), VPC ID (empty), and Owner (29263880518). Below this is a 'Tags' section with one tag: 'Name' set to 'my-internet-gateway'. On the right, there is an 'Actions' menu with options: 'Attach to VPC' (highlighted with a red box), 'Detach from VPC', 'Manage tags', and 'Delete'.

The screenshot shows the 'Attach internet gateway' wizard. The title bar says 'Attach internet gateway | VPC M...' and the URL is 'https://console.aws.amazon.com/vpc/home?region=us-east-1#AttachInternetGateway'. The breadcrumb navigation shows 'VPC > Internet gateways > Attach to VPC (igw-02933edb47b855575)'. The main section is titled 'Attach to VPC (igw-02933edb47b855575)' with a 'Info' link. It has a 'VPC' heading and a sub-instruction: 'Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.' Below this is a 'Available VPCs' section with the instruction: 'Attach the internet gateway to this VPC.' A search bar labeled 'Select a VPC' contains the text 'vpc-010ccb755e43966b6 - my-vpc-01', which is also highlighted with a red box. At the bottom right is a large orange 'Attach internet gateway' button, also highlighted with a red box. There are 'Cancel' and 'Skip to Primary Navigation' buttons at the bottom.

Now we can create a route to allow connections to **0.0.0.0/0** (Internet) through the Internet Gateway:



The screenshot shows the 'Edit routes' page in the AWS VPC Management Console. The URL is [https://console.aws.amazon.com/vpc/home?region=us-east-1#EditRoutes\\$routeTableId=rtb-03e2fd026035b7d69](https://console.aws.amazon.com/vpc/home?region=us-east-1#EditRoutes$routeTableId=rtb-03e2fd026035b7d69). The page displays a table of existing routes:

Destination	Target	Status	Propagated
10.10.0.0/16	local	active	No
172.10.1.0/24	vgw-033b3750fae1f6443	active	No
0.0.0.0/0	igw-02933edb47b855575	active	No

An 'Add route' button is visible below the table. At the bottom, there are 'Cancel' and 'Save routes' buttons, with 'Save routes' being highlighted by a red box.

On Azure the route was automatically created. You can check selecting the Azure VM > Networking > Network Interface > Effective routes. Note that we have 2 (1 per connection):

The screenshot shows the Azure portal interface for managing network interfaces. The left sidebar lists various services like Resource groups, Virtual machines, and Storage accounts. The main content area is titled 'vm-azure672 | Effective routes' and shows a table of 'Effective routes'. The table has columns for Source, State, Address Prefixes, Next Hop Type, and Next Hop Type IF. Two specific rows are highlighted with a red box: both are 'Virtual network gateway' entries with source '10.10.0.0/16' and next hop type 'Virtual network gateway' pointing to IP '20.185.83.40'. Other rows include a 'Default' entry with source '0.0.0.0/0' and next hop type 'Internet', and several other internal routes.

Source	State	Address Prefixes	Next Hop Type	Next Hop Type IF
Default	Active	172.10.0.0/16	Virtual network	-
Virtual network gateway	Active	10.10.0.0/16	Virtual network gateway	20.185.83.40
Virtual network gateway	Active	10.10.0.0/16	Virtual network gateway	20.185.83.40
Default	Active	0.0.0.0/0	Internet	-
Default	Active	10.0.0.0/8	None	-
Default	Active	100.64.0.0/10	None	-
Default	Active	192.168.0.0/16	None	-
Default	Active	25.33.80.0/20	None	-
Default	Active	25.41.3.0/25	None	-

Now I've created a Linux VM on Azure and our environment looks like this:

The screenshot shows the Microsoft Azure portal interface. The left sidebar is filled with various service icons under categories like Home, All services, Favorites, and Monitoring. The main content area is titled 'rg-azure-aws' and shows the 'Overview' tab for this resource group. Key details include:

- Subscription: Azure CXP FTA Internal Subscription RICMA... (Subscription ID: d9759156-c58b-4373-b08a-e7b28d114df4)
- Deployments: 7 Succeeded
- Tags: Click here to add tags

A search bar at the top allows filtering by name, type, and location. The main list view displays 12 records, all of which are located in the 'East US' region. The columns are Name, Type, and Location. The list includes:

Name	Type	Location
connection-azure-aws	Connection	East US
connection-azure-aws-standby	Connection	East US
ing-azure-aws	Local network gateway	East US
ins-azure-aws-standby	Local network gateway	East US
pip-vpn-azure-aws	Public IP address	East US
vm-azure	Virtual machine	East US
vm-azure-ip	Public IP address	East US
vm-azure-nsg	Network security group	East US
vm-azure672	Network interface	East US
vm-azure_disk1_bf051bb8caff4ec8a5071cf...	Disk	East US
vnet-azure	Virtual network	East US
vpn-azure-aws	Virtual network gateway	East US

And I did the same VM creation on AWS that looks like this:

Skip for now in Slides

The screenshot shows the AWS Resource Groups Management console. The URL in the browser is <https://console.aws.amazon.com/resource-groups/group/rg-aws-azure?region=us-east-1>. The left sidebar has sections for 'AWS Resource Groups' (selected), 'Resources' (Create Resource Group, Saved Resource Groups), and 'Tagging' (Tag Editor, Tag Policies). The main content area shows the 'rg-aws-azure' group. It includes a 'Group type and grouping criteria' section with 'Group type' set to 'Tag based' and 'Resource types' set to 'All supported resource types'. A 'Tags' section shows a single tag 'Lab: AWS-Azure'. Below this is a 'Group resources (9)' section with a table:

Identifier	Tag: Name	Service	Type	Region
cgw-01c9644443bf20a28	cg-aws-azure	EC2	CustomerGateway	us-east-1
i-04702ec1719c28a52	vm-aws	EC2	Instance	us-east-1
igw-02933edb47b855575	my-internet-gateway	EC2	InternetGateway	us-east-1
rtb-03e2fd026035b7d69	my-rt	EC2	RouteTable	us-east-1
sg-03cf3921c165a2c15	my-sg	EC2	SecurityGroup	us-east-1
subnet-081f287fc4638903c	my-subnet-01	EC2	Subnet	us-east-1
vpc-010cbb755e43966b6	my-vpc-01	EC2	VPC	us-east-1
vpn-0ca74f7bd72086f4b	vpn-aws-azure	EC2	VPNConnection	us-east-1
vgw-033b3758fae1f6443	vgw-aws-azure	EC2	VPNGateway	us-east-1

Then we can test the connectivity between Azure and AWS through our VPN connection:

Azure Linux VM

```
rmmartins@vm-azure:~$ curl ifconfig.co  
52.146.16.129  
rmmartins@vm-azure:~$ ifconfig eth0  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
      inet 172.10.1.4 netmask 255.255.255.0 broadcast 172.10.1.255  
        inetb fe80::20d:3aff:fe8d:1be9 prefixlen 64 scopeid 0x20<link>  
          ether 00:0d:3a:8d:1b:e9 txqueuelen 1000 (Ethernet)  
            RX packets 159702 bytes 200792484 (200.7 MB)  
            RX errors 0 dropped 0 overruns 0 frame 0  
            TX packets 32116 bytes 7050453 (7.0 MB)  
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
rmmartins@vm-azure:~$ ping 10.10.1.49 -c 5  
PING 10.10.1.49 (10.10.1.49) 56(84) bytes of data.  
64 bytes from 10.10.1.49: icmp_seq=1 ttl=64 time=4.89 ms  
64 bytes from 10.10.1.49: icmp_seq=2 ttl=64 time=4.18 ms  
64 bytes from 10.10.1.49: icmp_seq=3 ttl=64 time=3.74 ms  
64 bytes from 10.10.1.49: icmp_seq=4 ttl=64 time=4.70 ms  
64 bytes from 10.10.1.49: icmp_seq=5 ttl=64 time=5.09 ms  
  
--- 10.10.1.49 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4007ms  
rtt min/avg/max/mdev = 3.746/4.526/5.097/0.492 ms  
rmmartins@vm-azure:~$
```

AWS Linux VM

```
ubuntu@ip-10-10-1-49:~$ curl ifconfig.co  
3.94.96.168  
ubuntu@ip-10-10-1-49:~$ ifconfig eth0  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001  
      inet 10.10.1.49 netmask 255.255.255.0 broadcast 10.10.1.255  
        inetb fe80::20d:92ff:fe9b:a2bd prefixlen 64 scopeid 0x20<link>  
          ether 0e:d3:92:9b:a2:bd txqueuelen 1000 (Ethernet)  
            RX packets 2637 bytes 246854 (246.8 KB)  
            RX errors 0 dropped 0 overruns 0 frame 0  
            TX packets 3374 bytes 366476 (366.4 KB)  
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
ubuntu@ip-10-10-1-49:~$ ping 172.10.1.4 -c5  
PING 172.10.1.4 (172.10.1.4) 56(84) bytes of data.  
64 bytes from 172.10.1.4: icmp_seq=1 ttl=64 time=3.91 ms  
64 bytes from 172.10.1.4: icmp_seq=2 ttl=64 time=3.63 ms  
64 bytes from 172.10.1.4: icmp_seq=3 ttl=64 time=4.67 ms  
64 bytes from 172.10.1.4: icmp_seq=4 ttl=64 time=4.56 ms  
64 bytes from 172.10.1.4: icmp_seq=5 ttl=64 time=3.42 ms  
  
--- 172.10.1.4 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4006ms  
rtt min/avg/max/mdev = 3.426/4.043/4.677/0.500 ms  
ubuntu@ip-10-10-1-49:~$
```

**Update:** If you want to deploy a solution more resilient and using BGP, follow this documentation: <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-aws-bgp>

4 Likes

## 20 Comments

---



Néstor Reverón Iron Contributor

...

Jul 12 2021 05:21 AM

Thanks [@rmmartins](#)

0 Likes



Chandu P Copper Contributor

...

Aug 01 2021 03:04 AM

[@rmmartins](#)

Thank you very much for the steps.

I need some high level guidance for our use-case, if you don't mind please.

Ours is a early stage startup company. We are trying to setup secure employees login/connections to our AWS environment.

We have all our 10 employees using office365. We do have Azure subscription too.

How could I setup this use-case:-

[Skip](#) [For My Information](#)

Create Azure VNet Gateway and Azure VPN (I think we know steps for this).

Create a Virtual Desktop (either Ubuntu or Windows, in AWS or within Azure) for Multi-User session mode.

All our employees should login to Azure VPN client on their own personal laptops using Azure AD(O365) login; after that employees should login to the Virtual Desktop using SSO via Azure AD. After logging in to Virtual Desktop only our engineers should be able to connect to our AWS resources like AWS EKS or AWS RDS or anything which is in our AWS private subnet using AWS SSO via Azure AD.

Please provide some high level steps or point me to some resources which could help. Please & Thank you.

1 Like



[Fabio Jourdan](#) Copper Contributor

...

Aug 19 2021 06:58 AM

[@Chandu P](#) , use Azure AD Application Proxy to publish Private Web Applications, without using VPN or connections between Azure and AWS, you only need to deploy a proxy Machine in your AWS VPC with Internet Connection.

For AWS administrative tasks, in management console, use

AWS SSO + Azure AD

[Skip Form Factor Navigation](#)

 1 Like



**microworker** Copper Contributor

Dec 15 2021 09:09 AM

...

During step 11 while creating the connection in Azure, I'm getting the "Unknown" status on the connection. I'm getting something similar in AWS. Configuration seems like it is correct, although clearly I'm doing something wrong. Does anyone know what causes the "Unknown" status? I'm not seeing any clear documentation on it anywhere.

 0 Likes



**stefanalex2360** Copper Contributor

...

Dec 21 2021 09:27 AM

hi microworker

check public ip addresses in both ends of the tunnel and secret key again.

And wait. sometimes i wait for like 5 to 10 minutes for tunnels to go up, sometimes it is almost instant

 0 Likes

[Skip to main content](#)



[microworker](#) Copper Contributor

Dec 21 2021 01:02 PM

...

[@stefanalex2360](#)

I did do that, but they were definitely correct. I did upgrade the gateway from vpngw1 to vpngw2 and tunnel 1 immediately came up. But now I can't get the second tunnel up.

↳ 0 Likes



[Rajarshi1590](#) Copper Contributor

May 09 2022 07:34 PM

...

Hi,

Thank you for the nice step-by-step article! I just tried the steps mentioned in the article. So, from the Azure side when we are creating a virtual network gateway, we are disabling BGP. But, from AWS side when we are creating a customer gateway with the public IP of the Azure Virtual network gateway, we cannot disable BGP. If BPP related text field is left blank, then it is asking me to enter something, as shown in the screenshot below. So, It cannot be left blank. Not sure how BGP did not appear in the screenshot that you provided for configuring CGW in AWS.

[Skip](#) [For Main Navigation](#)

Now, if I enable BGP ( by providing a BGP ASN as 65001) then will it be able to communicate with Azure once the Virtual private gateway is set up and attached to the corresponding VPC? If not, then how to make the connectivity work?

The screenshot shows the 'Details' section of an AWS Customer Gateway configuration. It includes fields for:

- Name tag - optional:** CG-ILRS-Azure
- BGP ASN:** Enter BGP ASN (65001)
- IP address:** 20.213.3.226
- Certificate ARN:** Select certificate ARN

↳ 0 Likes



**jdewitt66** Copper Contributor

Aug 02 2022 02:15 PM

...

Hello,

Bottom line up front: Need assistance moving DB from AWS to Azure

Thanks for the article above. I am working on a project in which we are trying to transfer several existing PostgreSQL DB from AWS to Azure. We have followed all directions that we can find online to use the Azure DMS but we cannot establish a successful connection between the DMS and AWS. The problem occurs on the 'Select Source' page of the Azure DMS. During the validation step I get an error stating 'Failed to connect'. I have been working on this for a few weeks trying different solutions. I get a different error if I purposely enter incorrect source info, so I believe that Azure is talking to AWS, but not creating the required connection.

I followed all of the steps in the above article and can see that both AWS tunnels are up and the connection in Azure shows connected. However, I still can't get a connection to allow transfer of the DBs from AWS to Azure. Can anyone help?

✍ 0 Likes



AlexT330 Copper Contributor

Dec 04 2022 06:58 PM

...

In your examples you use **172.10.0.0/16**, but those are public IP addresses assigned to AT&T. Configuring them on a private subnet is likely to cause connectivity issues with parts of the internet. Recently some members of my team configured a VPN

Skip Forum Navigation

using those values copied from your tutorial and now I'm asking them to redo their work to use private address space instead.

May I suggest switching your tutorial to **172.16.0.0/16** which is an appropriate private space instead.

↳ 0 Likes



Anoop Singh Copper Contributor

...

Apr 05 2023 01:59 PM

It's very precise and clear content. Loved it.

I have successfully completed my use case for VPN connectivity with high availability between Azure and AWS cloud.

Thanks Once again for your great content.

Thanks,

Anoop Singh

↳ 1 Like



mileytores Copper Contributor

...

May 05 2023 03:30 PM

Muchas gracias! funcionó a la perfección, pero si tuve que cambiar a sku VpnGW2

Skip for Main Navigation

 1 Like



**sonali335** Copper Contributor

...

Jun 08 2023 07:52 AM

I did all the setup as mentioned in above step my tunnel is also up and vpn is also connected.

but when im doing the ping from aws to azure and azure to aws its not working  
showing

--- 10.34.0.4 ping statistics ---

3 packets transmitted, 0 received, 100% packet loss, time  
2052ms

 0 Likes



**vsk2023** Copper Contributor

...

Oct 21 2023 10:36 PM

Hi @sonali335 ,  
Could you pls try the below

In AWS side of the config, in the Site-to-Site VPN connections,  
under "Static routes" add the IP prefix of the Azure VM's IP.

Skip in Production Environment

172.10.1.0/24

Also ensure the route propagation is enabled in the route table config.

Hope this helps.

拇指图标 1 Like



[David2075](#) Copper Contributor

Dec 11 2023 03:10 PM

...

Saw this after many hours of pulling my hair out...."Also ensure the route propagation is enabled in the route table config."

After enabling, my issues were resolved.

FYI: Great article !

拇指图标 0 Likes



[mshah1525](#) Copper Contributor

...

Jan 18 2024 12:13 PM

I am able to ssh from AWS to Azure, but not from Azure to AWS. On both end, the tunnel connectivity shows as connected.

Also if we plan to add another Azure region, is there a way to use existing tunnel or do I need to setup another tunnel between Azure East to AWS.

[Skip to main content](#)

 0 Likes



Dan1232275 Copper Contributor

...

Feb 07 2024 04:47 PM

@rmmartins @mshah1525 Were you able to resolve it? I am having same issue.

I can ssh from AWS to Azure but not the other way.

I can ping both ways.

 0 Likes



Dan1232275 Copper Contributor

...

Feb 12 2024 10:56 PM

If your GatewaySubnet have a route table, ensure Propagate gateway routes is set to true for the gateway.

 1 Like



mshah1525 Copper Contributor

...

Feb 20 2024 11:39 AM

Yes, we were configuring the route table and hence the "Propagate gateway routes" which the VPN was configuring were invalidated. Once we deleted our routing configuration, it started working fine.

[Skip Forum Navigation](#)

We see the VPN routing configuration, once we create a VM and look at the Network config. Is there any other place we can see all the routing configuration?

↳ 0 Likes



jlewis Copper Contributor

Mar 28 2024 07:06 AM

...

@rmmartins

Thank you very much for the steps.

↳ 0 Likes



venkatesh00hotmailco Copper Contributor

...

Jul 02 2024 01:27 PM

Super helpful!!

↳ 0 Likes

You must be a registered user to add a comment. If you've already registered, sign in. Otherwise, register and sign in.



[Comment](#)

## **What's new**

Surface Pro 9

Surface Laptop 5

Surface Studio 2+

Surface Laptop Go 2

Surface Laptop Studio

Surface Duo 2

Microsoft 365

Windows 11 apps

## **Microsoft Store**

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Virtual workshops and training

Microsoft Store Promise

Flexible Payments

## **Education**

[Skip to main content](#)

[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](#)

[Skip for main navigation](#)

[Documentation](#)

[Microsoft Learn](#)

[Microsoft Tech Community](#)

[Azure Marketplace](#)

[AppSource](#)

[Visual Studio](#)

## **Company**

[Careers](#)

[About Microsoft](#)

[Company news](#)

[Privacy at Microsoft](#)

[Investors](#)

[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