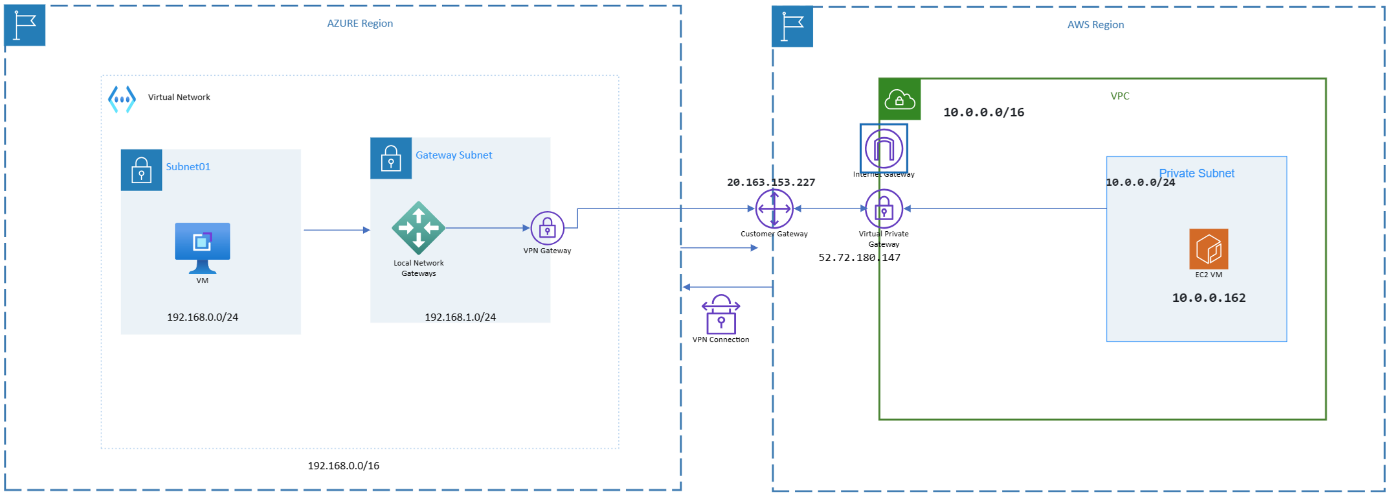
Contents

Architecture Diagram



AWS-Azure Site-to-Site VPN connection Setup:

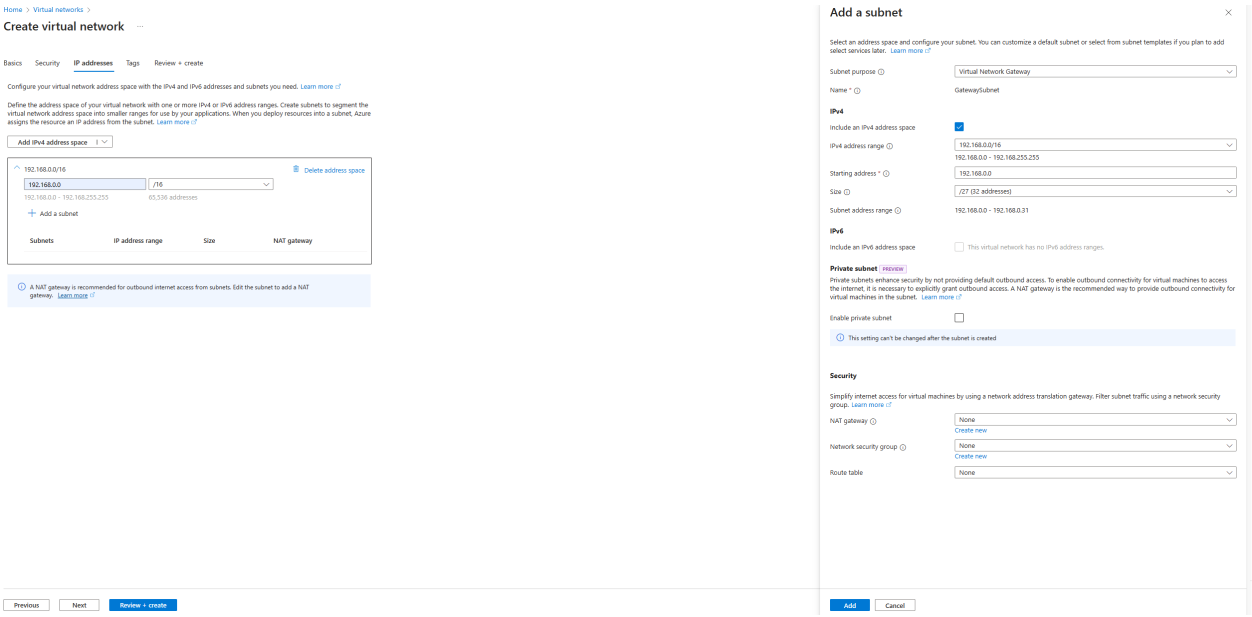
Configuring Azure

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

```
Resource Group Name: rg-azure-aws-conn
Region: East-US
```

2. Create Virtual Network

```
Resource Group Name: rg-azure-aws-conn
Region: East-US
VNet Name: vnet-azure
VNet IPv4 Address Space: 192.168.0.0/16
Subnet Name: GatewaySubnet
Subnet IPv4 Address Space: 192.168.1.0/24
```



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

192.168.0.0/16

192.168.0.0 /16

192.168.0.0 - 192.168.255.255 65,536 addresses

Subnets	IP address range	Size	NAT gateway

A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway. Learn more

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: Virtual Network Gateway

Name *: GatewaySubnet

IPv4

Include an IPv4 address space: ☑

IPv4 address range: 192.168.0.0/16

192.168.0.0 - 192.168.255.255

Starting address *: 192.168.0.0

Size: /27 (32 addresses)

Subnet address range: 192.168.0.0 - 192.168.0.31

IPv6

Include an IPv6 address space: □ This virtual network has no IPv6 address ranges.

Private subnet PREVIEW

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: □

This setting can't be changed after the subnet is created

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: None
Create new

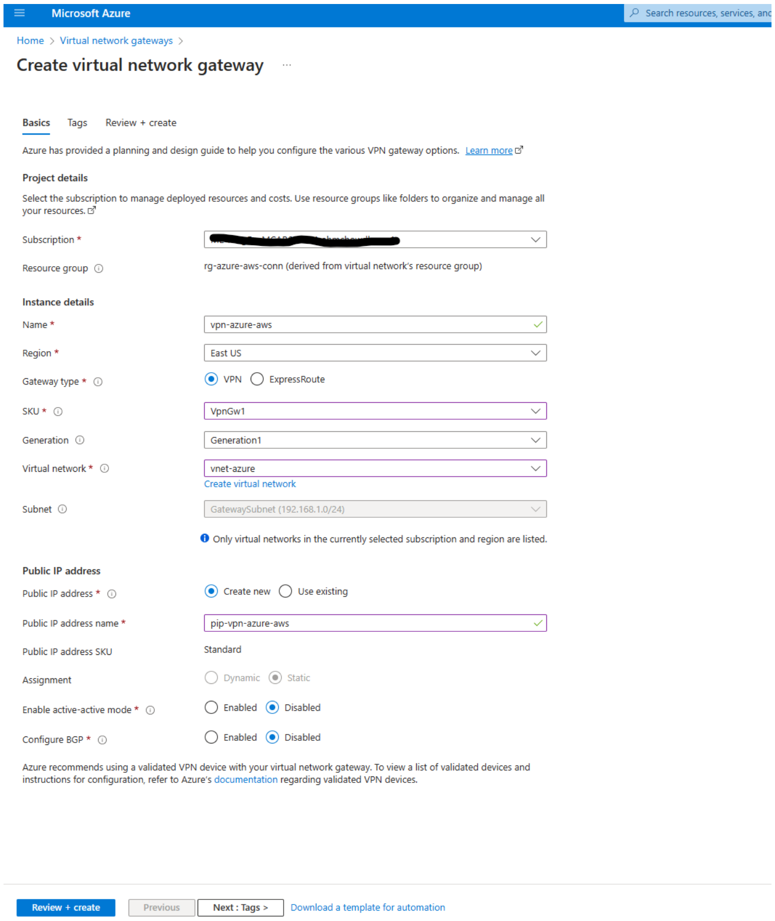
Network security group: None
Create new

Route table: None

3. Create the Virtual Network Gateway

```
VPN Gateway Name: vpn-azure-aws
Region: East-US
Gateway Type: VPN
SKU: VpnGw1
Generation: Generation 1
Virtual Network: vnet-azure

Public IP Address: pip-vpn-azure-aws
Public IP Address Type: Basic
Assignment: Dynamic
Enable active-active mode: Disabled
Configure BGP: Disabled
```


Microsoft Azure
Search resources, services, and
Home > Virtual network gateways >
Basics
Tags
Review + create
Review + create
Previous
Next : Tags >
Download a template for automation

Create virtual network gateway

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 *	[redacted]
Resource group	rg-azure-aws-conn (derived from virtual network's resource group)

Instance details

Name *	vpn-azure-aws
Region *	East US
Gateway type *	● VPN ○ ExpressRoute
SKU *	VpnGw1
Generation	Generation1
Virtual network *	vnet-azure Create virtual network
Subnet	GatewaySubnet (192.168.1.0/24)

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

Public IP address

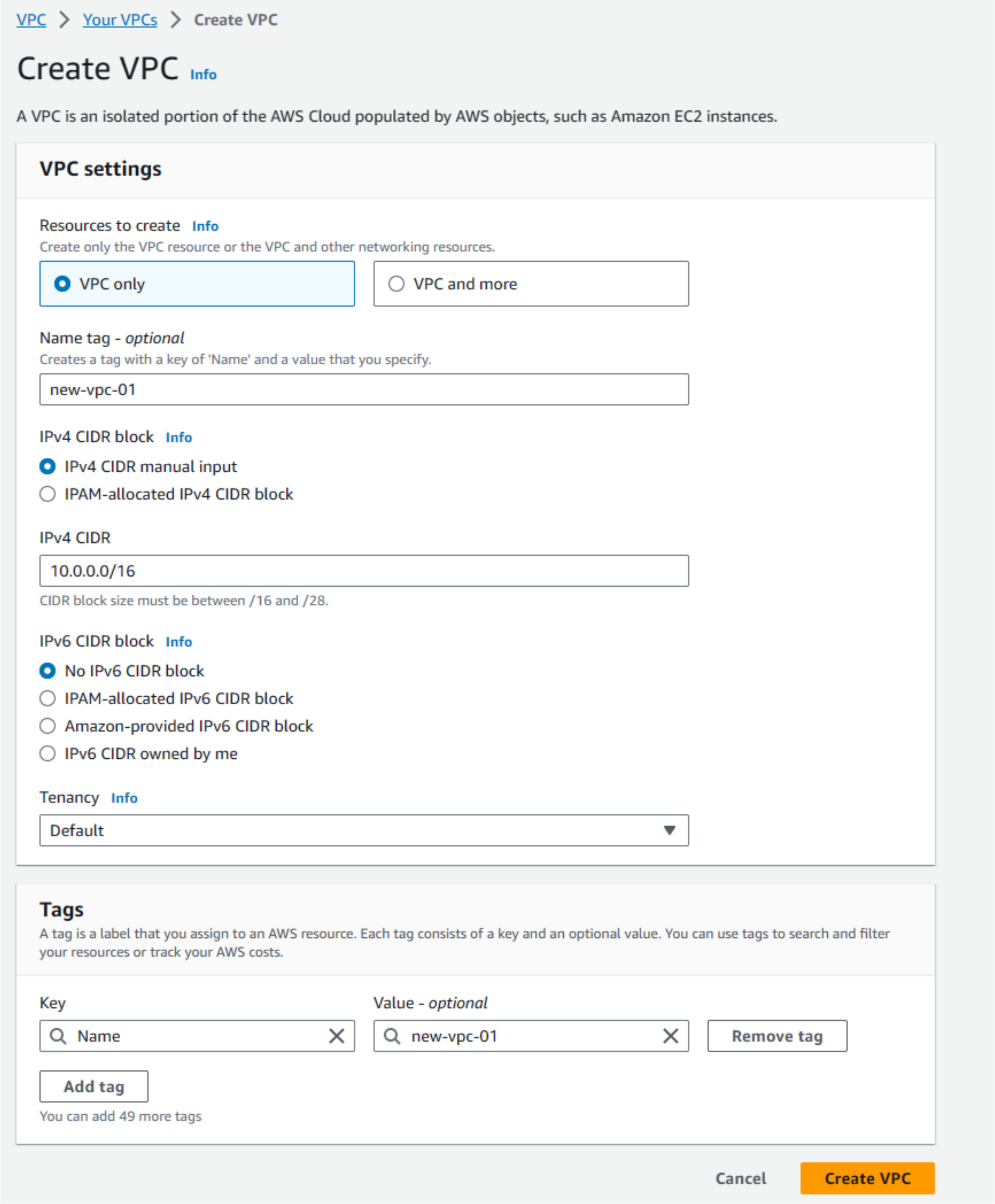
Public IP address *	● Create new ○ Use existing
Public IP address name *	pip-vpn-azure-aws
Public IP address SKU	Standard
Assignment	○ Dynamic ● Static
Enable active-active mode *	○ Enabled ● Disabled
Configure BGP *	○ Enabled ● Disabled

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

Configuring AWS

4. Create the Virtual Private Cloud (VPC) in AWS

```
Name: new-vpc-01
IPv4 CIDR: 10.0.0.0/16
```



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

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.
new-vpc-01

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.

IPv6 CIDR block Info
● No IPv6 CIDR block
○ IPAM-allocated 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.

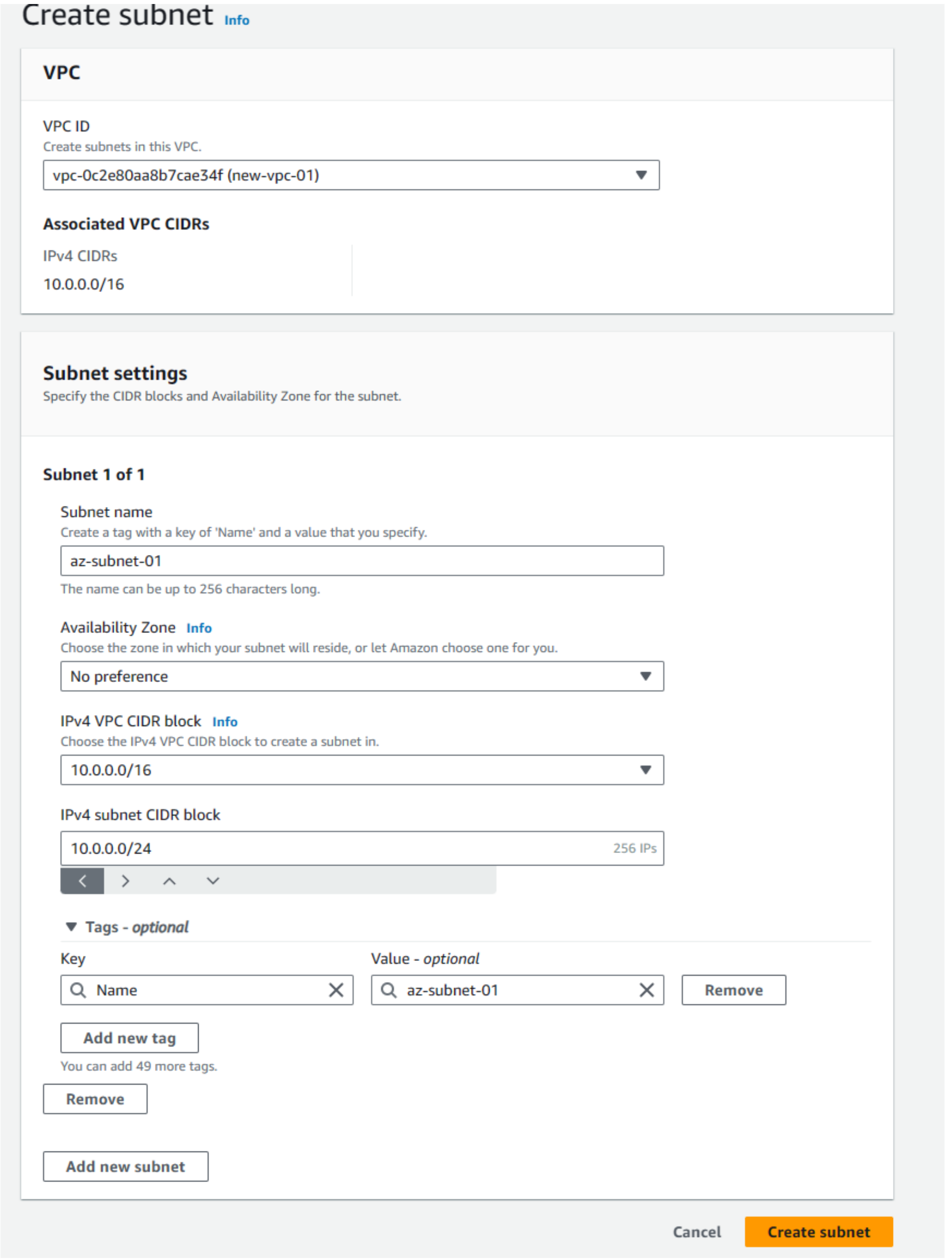
Key	Value - *optional*	
Name	new-vpc-01	Remove tag

Add tag
You can add 49 more tags

Cancel Create VPC

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

```
Name: az-subnet-01
VPC Name: new-vpc-01
VPC IPv4 CIDR: 10.0.0.0/16
IPv4 CIDR: 10.0.0.0/24
```



Create subnet Info

VPC

VPC ID
Create subnets in this VPC.
vpc-0c2e80aa8b7cae34f (new-vpc-01)

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.
az-subnet-01
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 IPv4 VPC CIDR block to create a subnet in.
10.0.0.0/16

IPv4 subnet CIDR block
10.0.0.0/24 256 IPs

Tags - *optional*

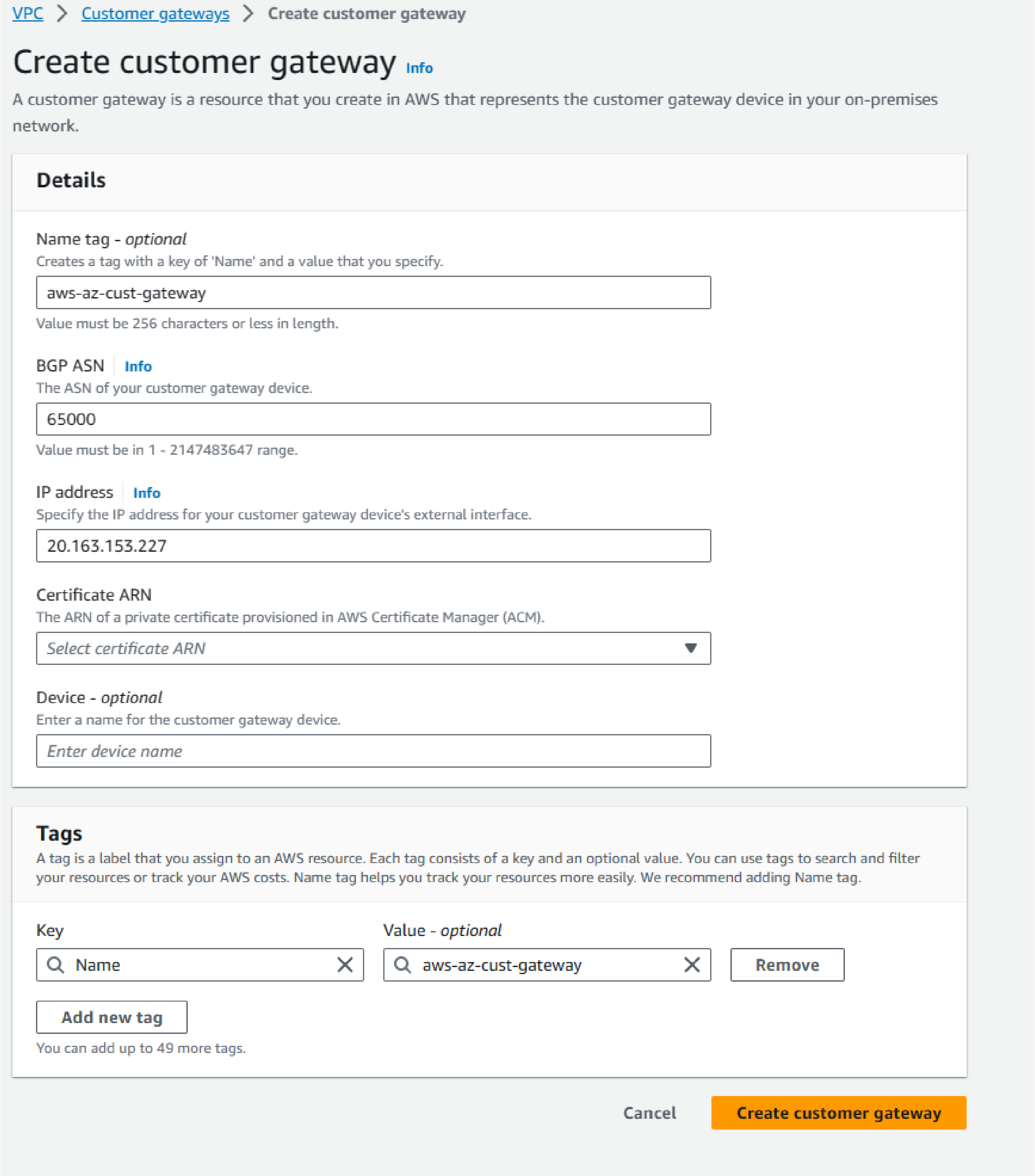
Key	Value - *optional*	
Name	az-subnet-01	Remove

You can add 49 more tags.

6. Create a customer gateway pointing to the Public IP Address of Azure VPN Gateway

   When you create a customer gateway, you provide information about your device to AWS. You or your network administrator must configure the device to work with the site-to-site VPN connection.

```
IP address: Public IP Address of Azure VPN Gateway 20.163.153.227 (pip-vpn-azure-aws)
Rest keep everything as default
```



VPC > Customer gateways > Create customer gateway

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.
aws-az-cust-gateway
Value must be 256 characters or less in length.

BGP ASN Info
The ASN of your customer gateway device.
65000
Value must be in 1 - 2147483647 range.

IP address Info
Specify the IP address for your customer gateway device's external interface.
20.163.153.227

Certificate ARN
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.
Enter device name

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. Name tag helps you track your resources more easily. We recommend adding Name tag.

Key	Value - *optional*	
Name	aws-az-cust-gateway	Remove

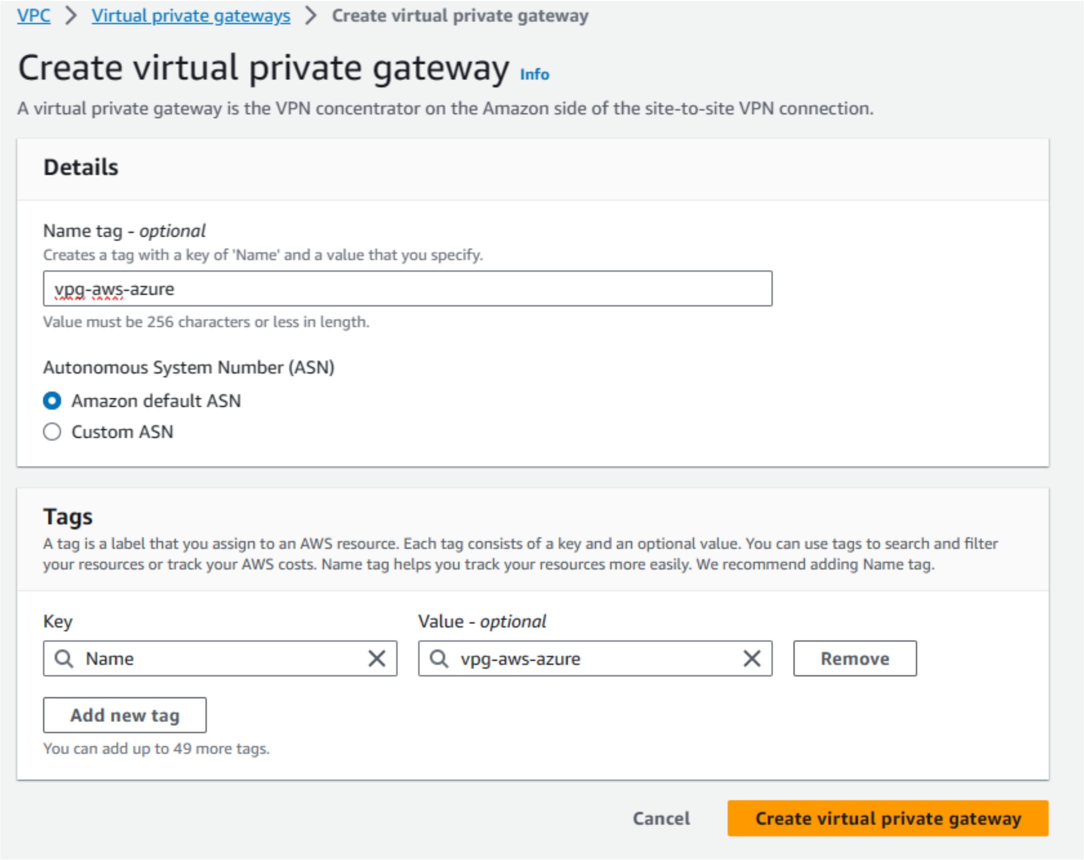
Add new tag

You can add up to 49 more tags.

Cancel | Create customer gateway

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

```
Name: vpg-aws-azure
```



VPC > Virtual private gateways > Create virtual private gateway

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.

vpg-aws-azure

Value must be 256 characters or less in length.

Autonomous System Number (ASN)

● Amazon default ASN

○ Custom ASN

Tags

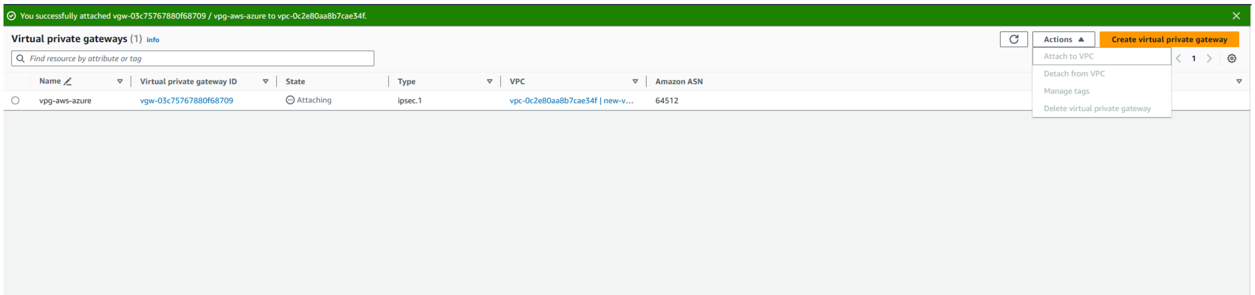
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs. Name tag helps you track your resources more easily. We recommend adding Name tag.

Key	Value - *optional*	
Name	vpg-aws-azure	Remove

Add new tag

You can add up to 49 more tags.

Attach with your VPC:



You successfully attached vgw-03c75767880f68709 / vpg-aws-azure to vpc-0c2e80aa8b7cae34f.

Virtual private gateways (1) info

Find resource by attribute or tag

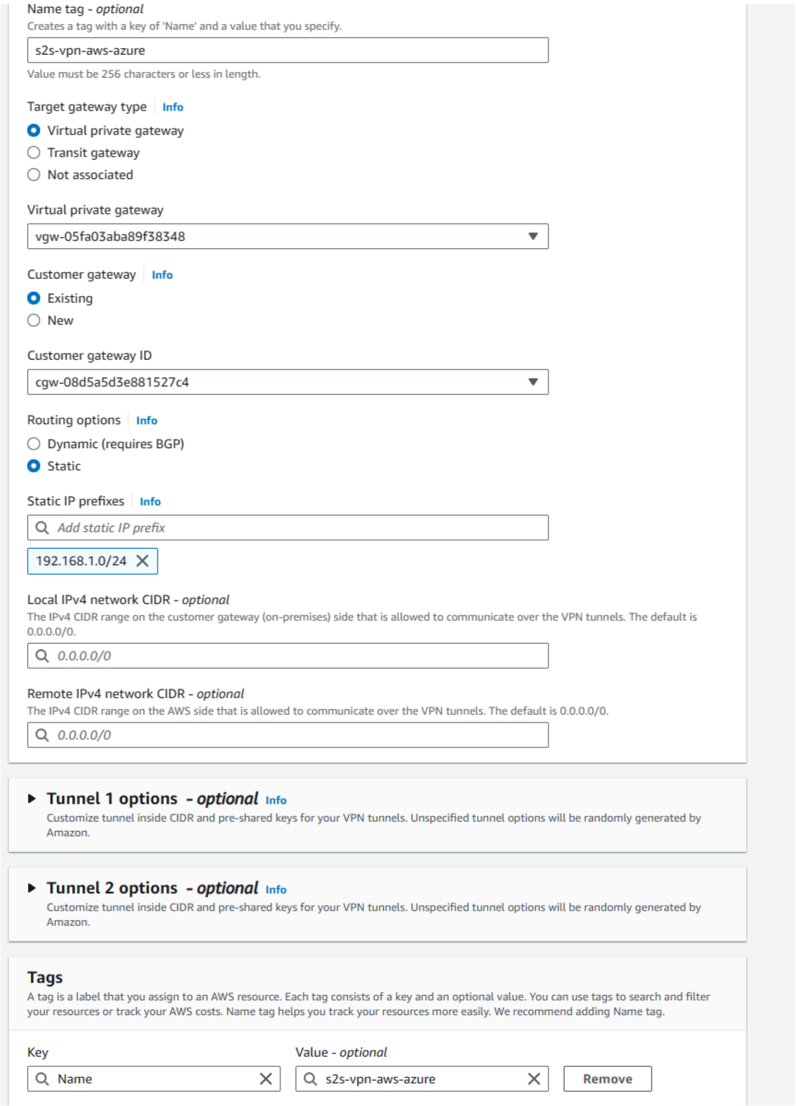
	Name	Virtual private gateway ID	State	Type	VPC	Amazon ASN
○	vpg-aws-azure	vgw-03c75767880f68709	Attaching	ipsec.1	vpc-0c2e80aa8b7cae34f | new-v...	64512

Actions
Create virtual private gateway
Attach to VPC
Detach from VPC
Manage tags
Delete virtual private gateway
1

8. Create a site-to-site VPN Connection

Name: s2s-vpn-aws-azure

```
Target gateway type: Virtual private gateway (Select your Virtual private gateway
created in 7)
Customer gateway: Existing (Select your VCustomer gateway created in 6)
Routing options: Static
Static IP prefixes: 192.168.1.0/24
Leave rest of them as default
```



Name tag - *optional*

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

s2s-vpn-aws-azure

Value must be 256 characters or less in length.

Target gateway type | Info

● Virtual private gateway

○ Transit gateway

○ Not associated

Virtual private gateway

vgw-05fa03aba89f38348

Customer gateway | Info

● Existing

○ New

Customer gateway ID

cgw-08d5a5d3e881527c4

Routing options | Info

○ Dynamic (requires BGP)

● Static

Static IP prefixes | Info

Add static IP prefix

192.168.1.0/24 ✕

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.

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.

0.0.0.0/0

▶ **Tunnel 1 options** - ***optional*** Info

Customize tunnel inside CIDR and pre-shared keys for your VPN tunnels. Unspecified tunnel options will be randomly generated by Amazon.

▶ **Tunnel 2 options** - ***optional*** Info

Customize tunnel inside CIDR and pre-shared keys for your VPN tunnels. Unspecified tunnel options will be randomly generated by Amazon.

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. Name tag helps you track your resources more easily. We recommend adding Name tag.

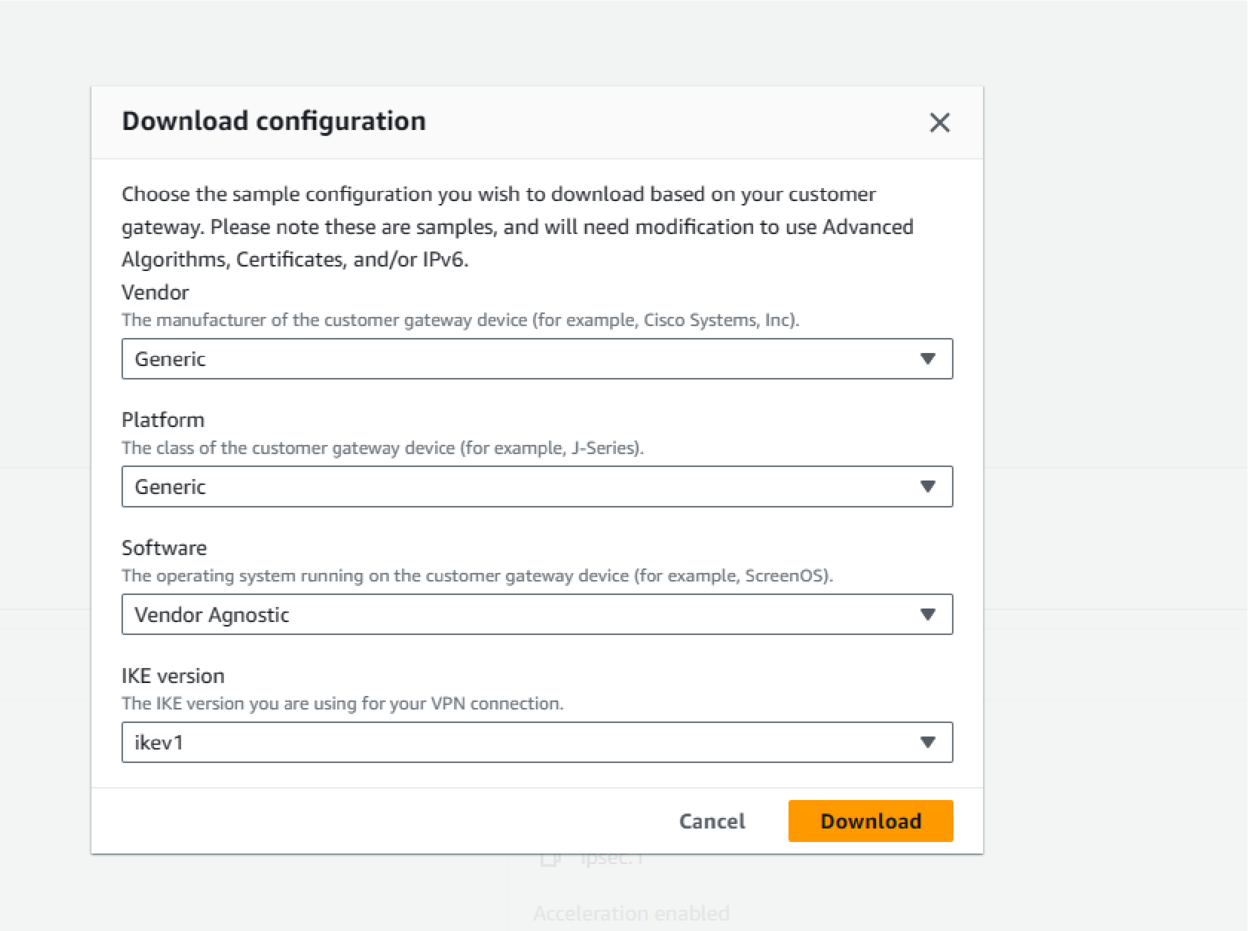
Key: Name

Value - *optional*: s2s-vpn-aws-azure

9. Download the configuration file

```
Vendor: Generic
```

```
Platform: Generic
Software: Vendor Agnostic
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.
```



Download configuration

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

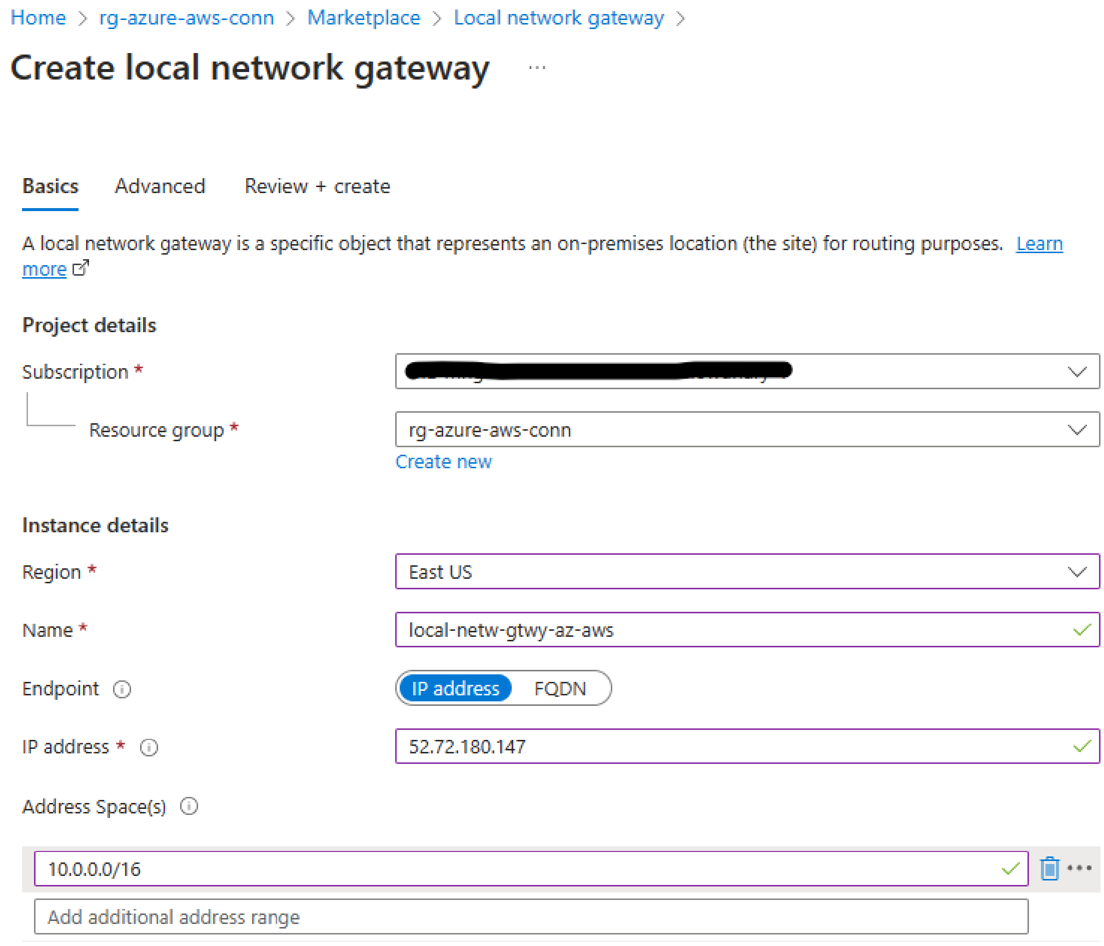
IKE version
The IKE version you are using for your VPN connection.
ikev1

Connecting Azure and AWS

10. Create the Local Network Gateway in Azure

```
Name: local-netw-gtwy-az-aws
```

Resource Group Name: rg-azure-aws-conn
Region: East-US
IP address: Get the Outside IP address from the configuration file downloaded in 9.
Should be the Virtual Private Gateway address Extrenal. 52.72.180.147
Address Space(s): 10.0.0.0/16 (from AWS VPC main CIDR)



Home > rg-azure-aws-conn > Marketplace > Local network gateway >

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 * [redacted]

Resource group * rg-azure-aws-conn
Create new

Instance details

Region * East US

Name * local-netw-gtwy-az-aws ✓

Endpoint ⓘ [✓ IP address] FQDN

IP address * ⓘ 52.72.180.147 ✓

Address Space(s) ⓘ

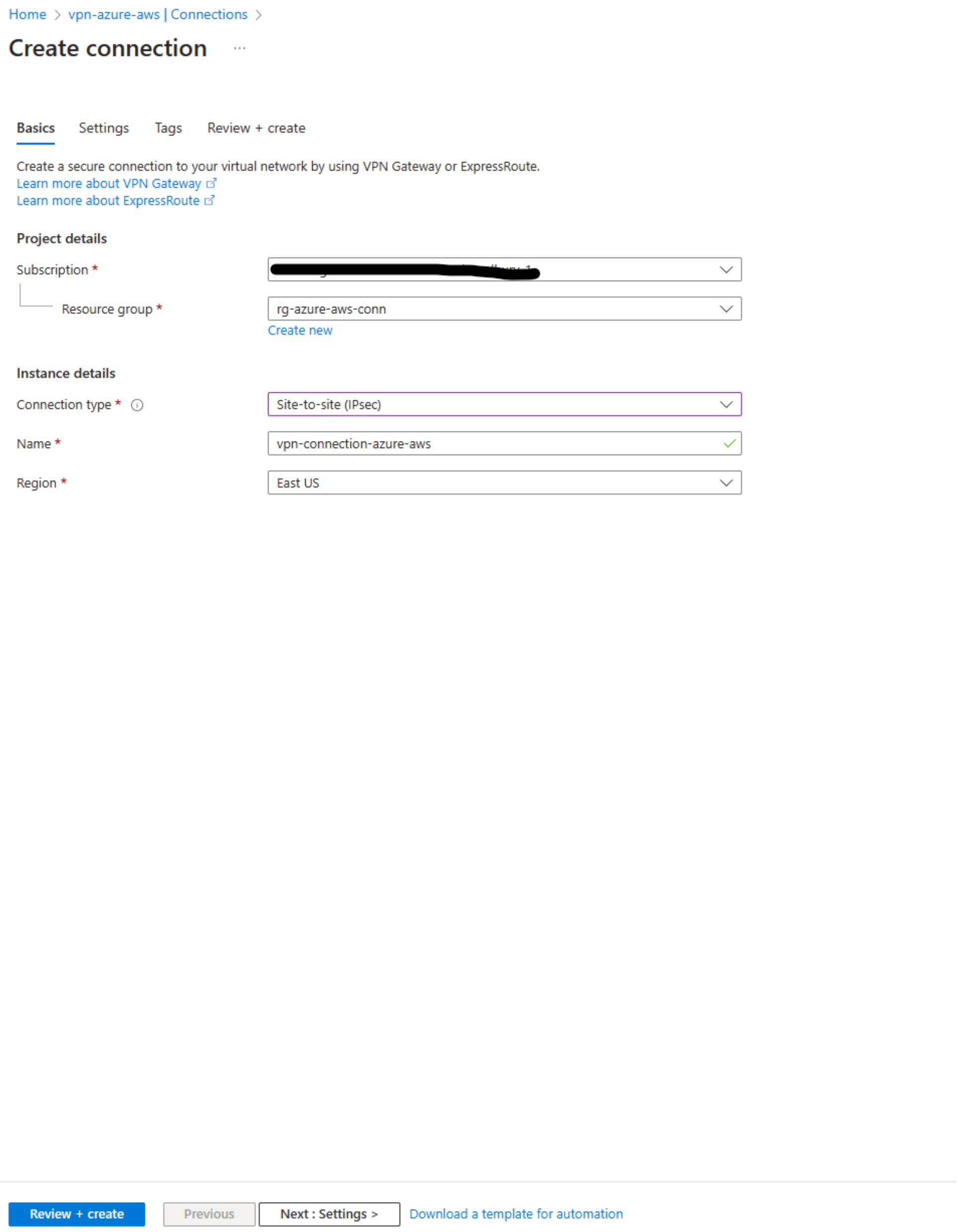
10.0.0.0/16 ✓

Add additional address range

11. Create the connection on the Virtual Network Gateway in Azure

Name: vpn-connection-azure-aws
Connection Type: Site-to-Site
Shared Key: Get the Pre-shared key from the downloaded vpn configuration file (pick the right tunnel)

Local Network Gateway: Select the Local Network Gateway which you created in 10.
Shared Key: Get the Shared Key from the configuration file downloaded in 9.
IKE Protocol: leave it as IKEv2
Wait till the Connection Status changes to - Connected
In the same way, check in AWS Console wheather the 1st tunnel of Virtual Private Gateway UP.



Home > vpn-azure-aws | 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 * [redacted]

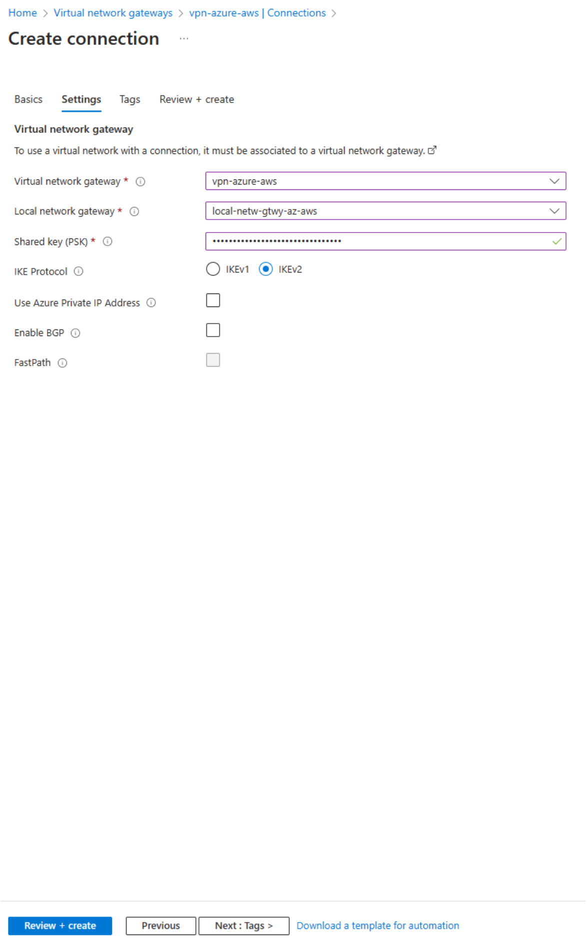
Resource group * rg-azure-aws-conn
Create new

Instance details

Connection type * Site-to-site (IPsec)

Name * vpn-connection-azure-aws

Region * East US



Home > Virtual network gateways > vpn-azure-aws | Connections >
Create connection ...
Basics
Settings
Tags
Review + create

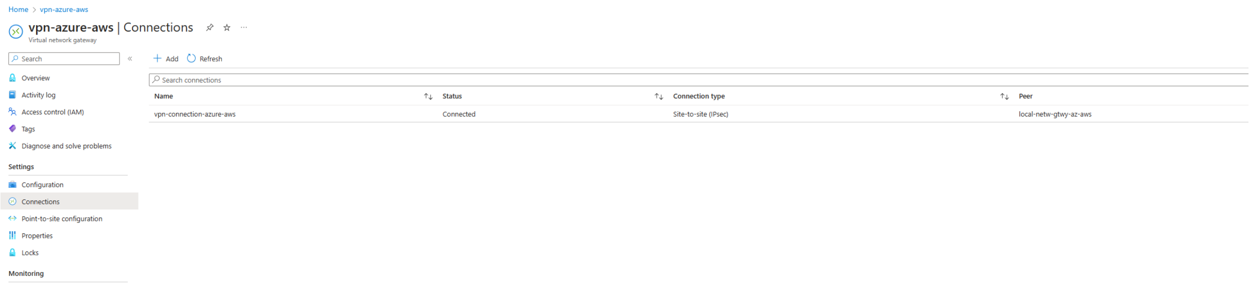
Virtual network gateway

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

Virtual network gateway *	vpn-azure-aws
Local network gateway *	local-netw-gtwy-az-aws
Shared key (PSK) *	••••••••••••••••••••••••••••••••
IKE Protocol	○ IKEv1 ● IKEv2
Use Azure Private IP Address	□
Enable BGP	□
FastPath	□

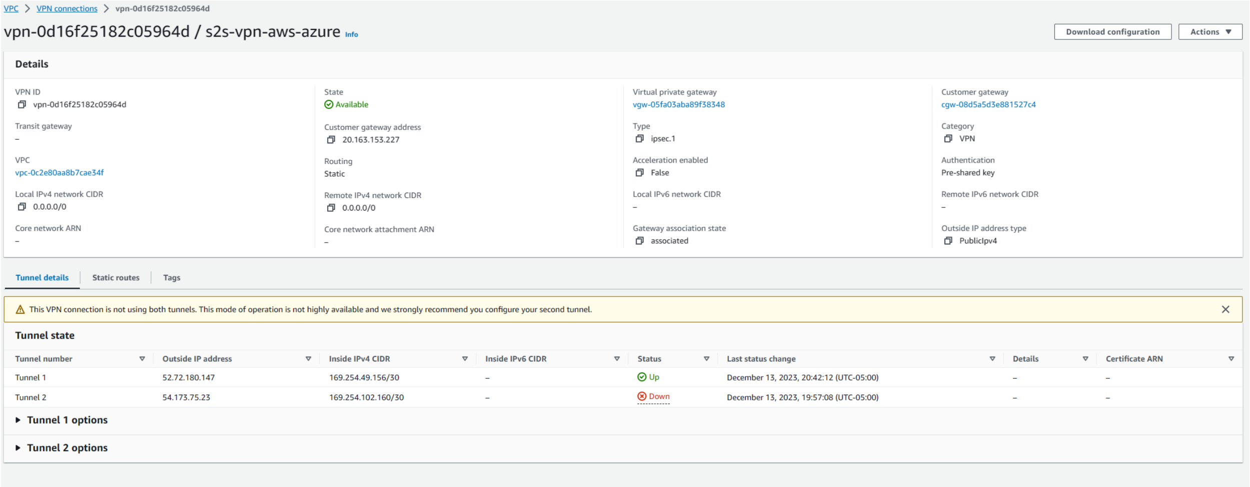
Review + create
Previous
Next : Tags >
Download a template for automation

Connectivity tab under Virtual Network Gateway must show Connected on Azure side and



Name	Status	Connection type	Peer
vpn-connection-azure-aws	Connected	Site-to-site (IPsec)	local-netw-gtwy-az-aws

Tunnel should be up on AWS side:



vpn-0d16f25182c05964d / s2s-vpn-aws-azure

Details

VPN ID
vpn-0d16f25182c05964d

Transit gateway
–

VPC
vpc-0c2e80aa8b7cae34f

Local IPv4 network CIDR
0.0.0.0/0

Core network ARN
–

State
✓ Available

Customer gateway address
20.163.153.227

Routing
Static

Remote IPv4 network CIDR
0.0.0.0/0

Core network attachment ARN
–

Virtual private gateway
vgw-05fa03aba89f38348

Type
ipsec.1

Acceleration enabled
False

Local IPv6 network CIDR
–

Gateway association state
associated

Customer gateway
cgw-08d5a5d3e881527c4

Category
VPN

Authentication
Pre-shared key

Remote IPv6 network CIDR
–

Outside IP address type
PublicIpv4

⚠ 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

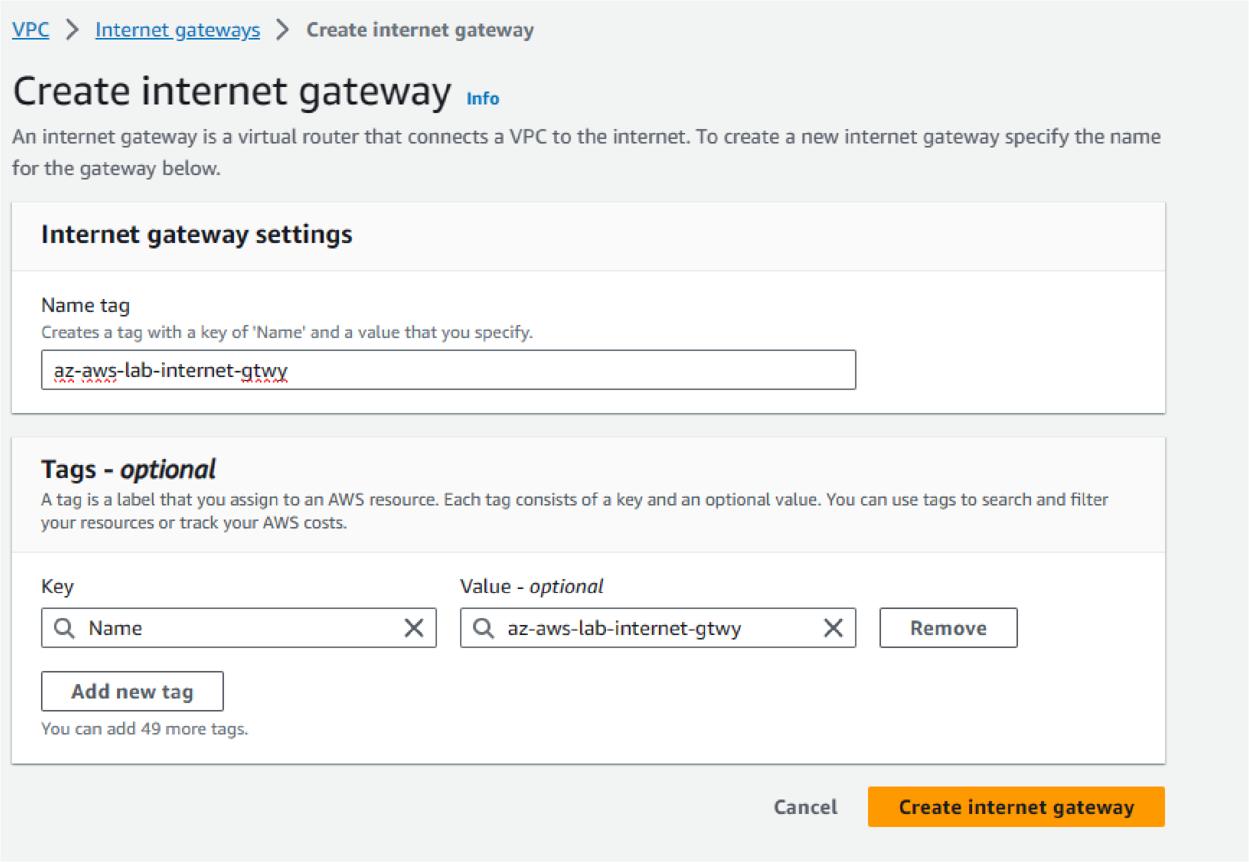
Tunnel number	Outside IP address	Inside IPv4 CIDR	Inside IPv6 CIDR	Status	Last status change	Details	Certificate ARN
Tunnel 1	52.72.180.147	169.254.49.156/30	–	✓ Up	December 13, 2023, 20:42:12 (UTC-05:00)	–	–
Tunnel 2	54.173.75.23	169.254.102.160/30	–	⊗ Down	December 13, 2023, 19:57:08 (UTC-05:00)	–	–

▶ Tunnel 1 options

▶ Tunnel 2 options

12. Create Internet Gateway and Attach it to VPC in AWS

`Name:` az-aws-lab-internet-gtwy



VPC > Internet gateways > Create internet gateway

Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag

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

az-aws-lab-internet-gtwy

Tags - *optional*

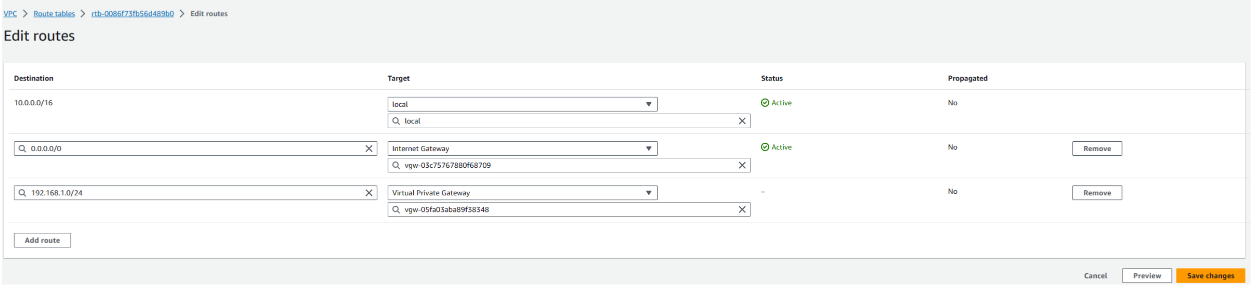
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*
Name	az-aws-lab-internet-gtwy

You can add 49 more tags.

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

```
Add the route to Azure subnet through the Virtual Private Gateway
Destination: 192.168.1.0/24
Target: Virtual Private Gateway in AWS that was created
Also-
Destination: 0.0.0.0/0
Target: Internet Gateway that we created in 12.
```



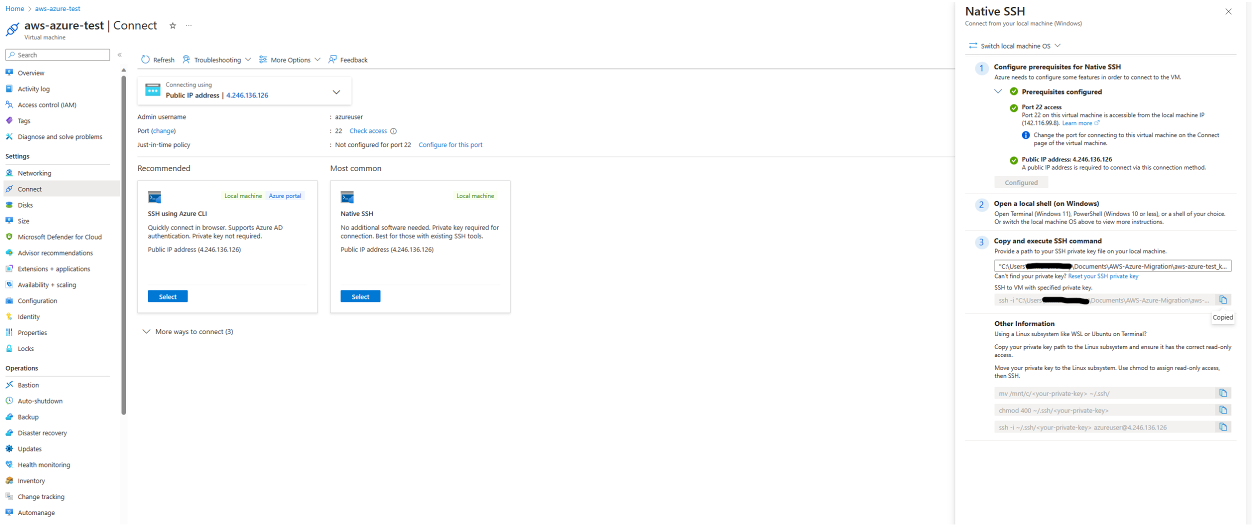
Edit routes

Destination	Target	Status	Propagated	
10.0.0.0/16	local local	Active	No	
0.0.0.0/0	Internet Gateway vgw-03c75767880f68709	Active	No	Remove
192.168.1.0/24	Virtual Private Gateway vgw-05fa03aba89f38348	–	No	Remove

14. Create VMs in both Azure and AWS and Test the connection.

    Make sure you can ping each other by SSH into each VM's in Azure and AWS environment.

AZURE VM Setup



Connecting using
Public IP address | 4.246.136.126

Admin username : azureuser
Port (change) : 22 Check access
Just-in-time policy : Not configured for port 22 Configure for this port

Recommended

Local machine Azure portal
SSH using Azure CLI
Quickly connect in browser. Supports Azure AD authentication. Private key not required.
Public IP address (4.246.136.126)
Select

Most common

Local machine
Native SSH
No additional software needed. Private key required for connection. Best for those with existing SSH tools.
Public IP address (4.246.136.126)
Select

More ways to connect (3)

Native SSH
Connect from your local machine (Windows)

Switch local machine OS

1 **Configure prerequisites for Native SSH**
Azure needs to configure some features in order to connect to the VM.

✓ **Prerequisites configured**

✓ **Port 22 access**
Port 22 on this virtual machine is accessible from the local machine IP (142.116.99.8). Learn more

Change the port for connecting to this virtual machine on the Connect page of the virtual machine.

✓ **Public IP address: 4.246.136.126**
A public IP address is required to connect via this connection method.

Configured

2 **Open a local shell (on Windows)**
Open Terminal (Windows 11), PowerShell (Windows 10 or less), or a shell of your choice. Or switch the local machine OS above to view more instructions.

3 **Copy and execute SSH command**
Provide a path to your SSH private key file on your local machine.

```
"C:\Users[redacted]\Documents\AWS-Azure-Migration\aws-azure-test_k...
```

Can't find your private key? Reset your SSH private key

SSH to VM with specified private key.

```
ssh -i "C:\Users[redacted]\Documents\AWS-Azure-Migration\aws-...
```

Copied

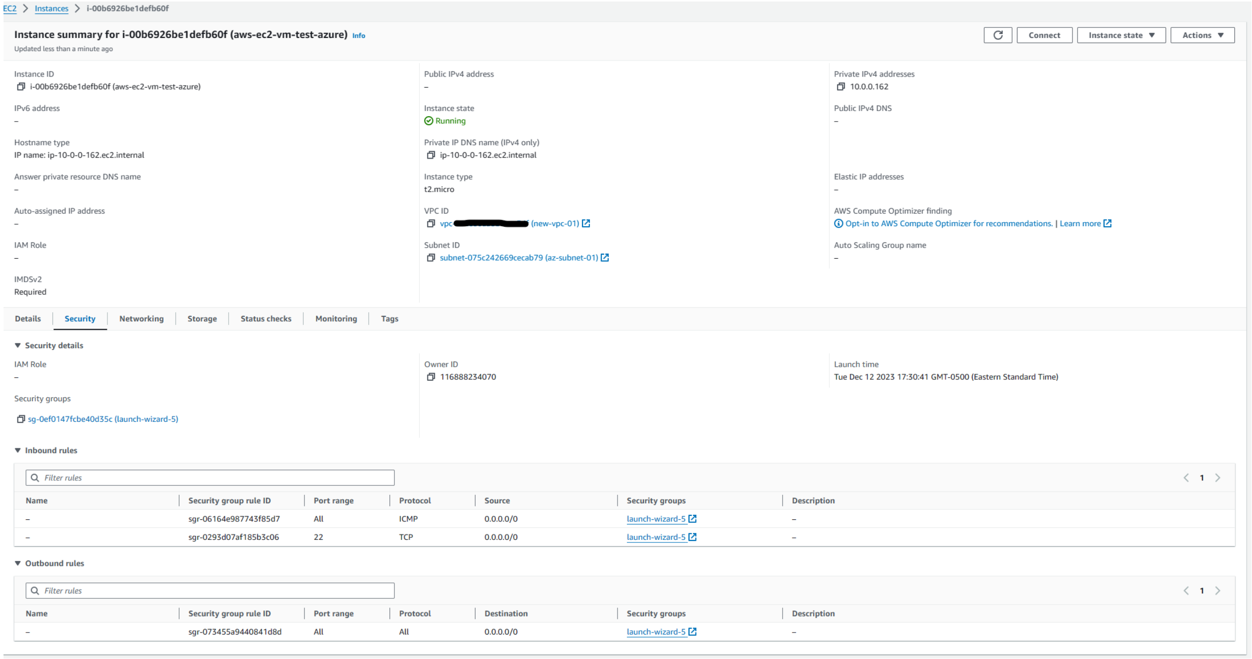
Other Information
Using a Linux subsystem like WSL or Ubuntu on Terminal?

Copy your private key path to the Linux subsystem and ensure it has the correct read-only access.

Move your private key to the Linux subsystem. Use chmod to assign read-only access, then SSH.

```
mv /mnt/c/<your-private-key> ~/.ssh/
chmod 400 ~/.ssh/<your-private-key>
ssh -i ~/.ssh/<your-private-key> azureuser@4.246.136.126
```

AWS VM Setup



Instance summary for i-00b6926be1defb60f (aws-ec2-vm-test-azure) Info
Updated less than a minute ago

Instance ID
i-00b6926be1defb60f (aws-ec2-vm-test-azure)

Public IPv4 address
–

Private IPv4 addresses
10.0.0.162

IPv6 address
–

Instance state
Running

Public IPv4 DNS
–

Hostname type
IP name: ip-10-0-0-162.ec2.internal

Private IP DNS name (IPv4 only)
ip-10-0-0-162.ec2.internal

Answer private resource DNS name
–

Instance type
t2.micro

Elastic IP addresses
–

Auto-assigned IP address
–

VPC ID
vpc[redacted] (new-vpc-01)

AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more

IAM Role
–

Subnet ID
subnet-075c242669cecab79 (az-subnet-01)

Auto Scaling Group name
–

IMDSv2
Required

▼ **Security details**

IAM Role
–

Owner ID
116888234070

Launch time
Tue Dec 12 2023 17:30:41 GMT-0500 (Eastern Standard Time)

Security groups
sg-0ef0147fcbe40d35c (launch-wizard-5)

▼ **Inbound rules**

Filter rules

Name	Security group rule ID	Port range	Protocol	Source	Security groups	Description
–	sgr-06164e987743f85d7	All	ICMP	0.0.0.0/0	launch-wizard-5	–
–	sgr-0293d07af185b3c06	22	TCP	0.0.0.0/0	launch-wizard-5	–

▼ **Outbound rules**

Filter rules

Name	Security group rule ID	Port range	Protocol	Destination	Security groups	Description
–	sgr-073455a9440841d8d	All	All	0.0.0.0/0	launch-wizard-5	–