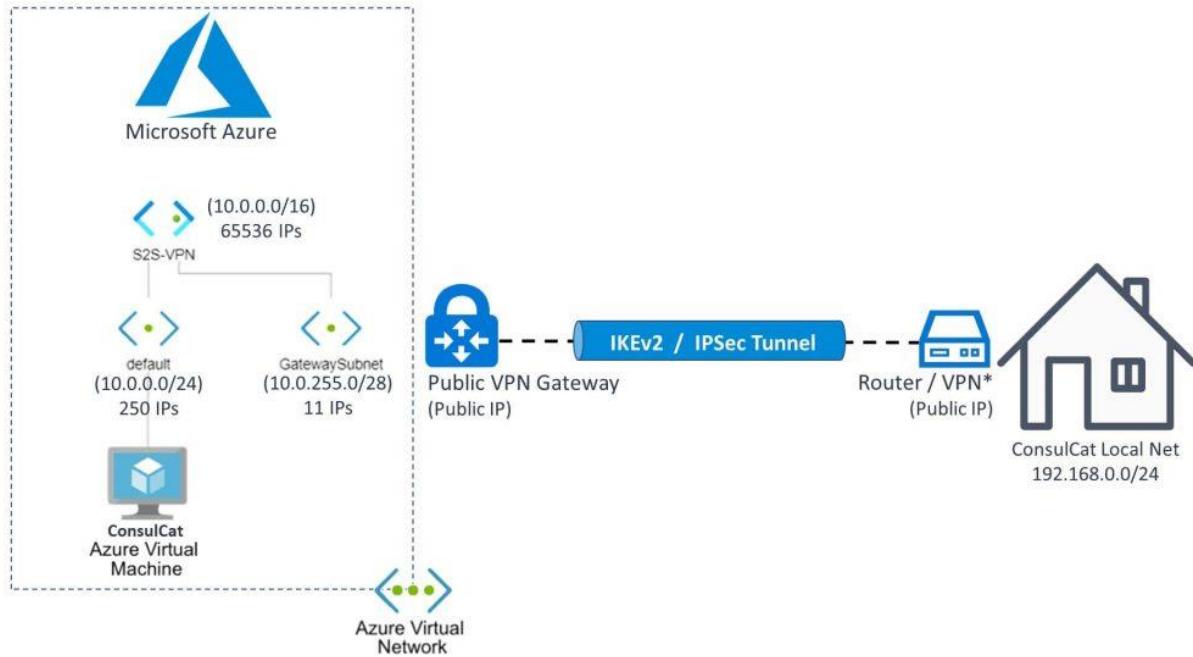


## SITE TO SITE VPN CONNECTION

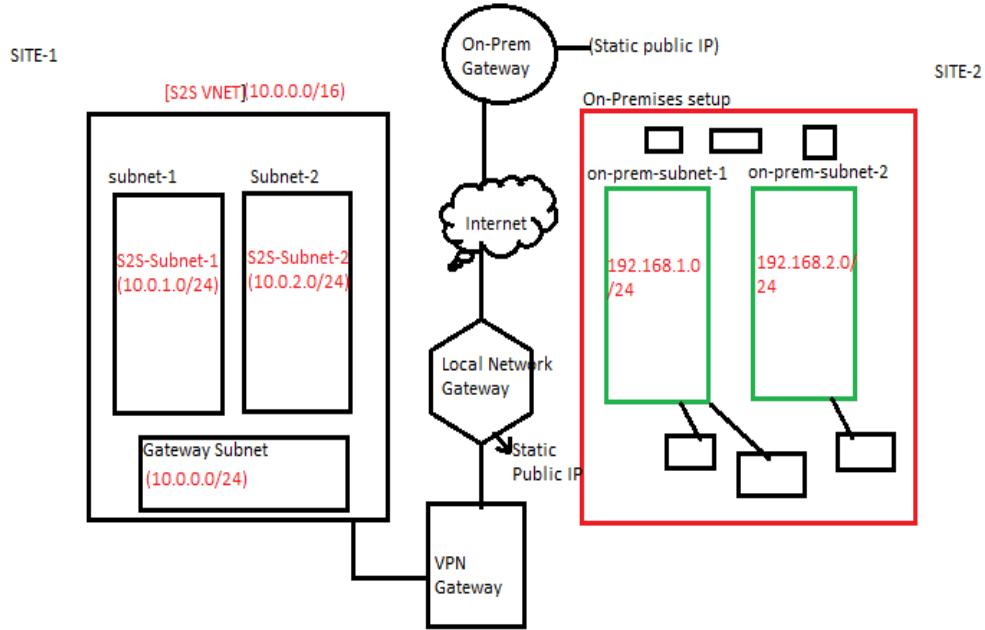


A Site-to-Site VPN gateway connection is used to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. This type of connection requires a VPN device located on-premises that has an externally facing public IP address assigned to it.

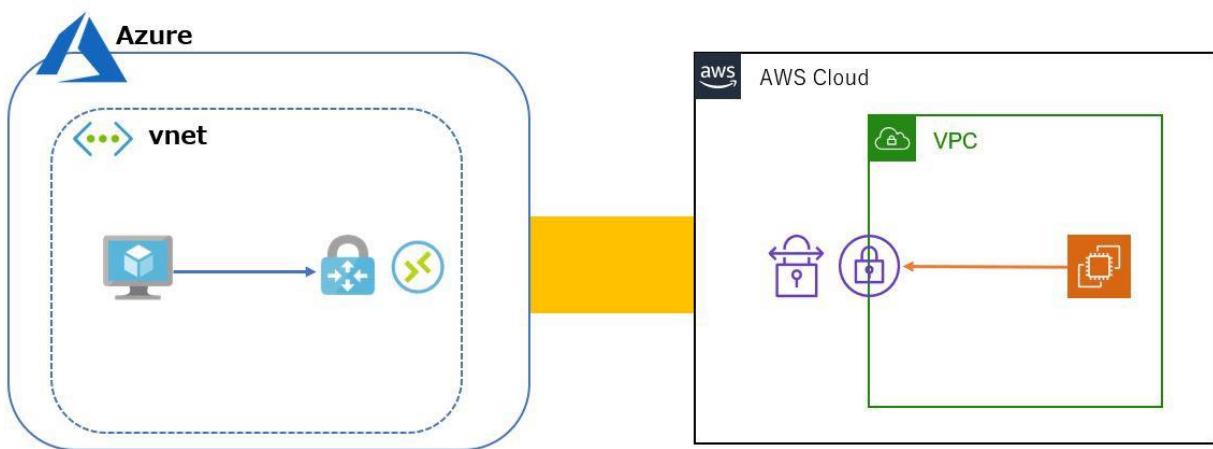
### About the gateway subnet

The virtual network gateway uses specific subnet called the gateway subnet. The gateway subnet is part of the virtual network IP address range that you specify when configuring your virtual network. It contains the IP addresses that the virtual network gateway resources and services use. The subnet must be named 'GatewaySubnet' in order for Azure to deploy the gateway resources. You can't specify a different subnet to deploy the gateway resources to. If you don't have a subnet named 'GatewaySubnet', when you create your VPN gateway, it will fail.

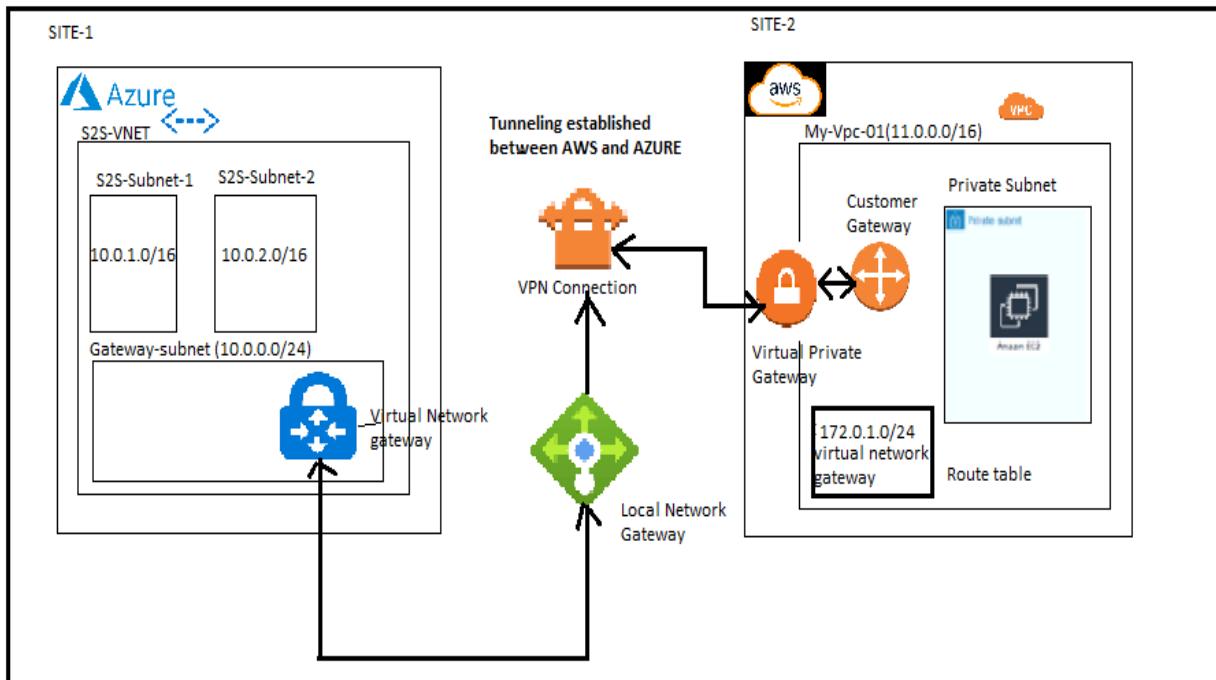
## Project Deployment Architecture:



## SITE TO SITE VPN CONNECTION BETWEEN AZURE AND AWS:



## PROJECT DEPLOYMENT ARCHITECTURE(S2S CONNECTIVITY BETWEEN AWS AND AZURE):



### AZURE SITE CONFIGURATION:

Screenshot of the Microsoft Azure "Create a resource group" wizard:

- Basics Step:**
  - Subscription: Azure for Students
  - Resource group: S2S-RG
  - Region: (US) Central US
- Next Step:** Tags >

Created a Resource group (S2S-RG).

## Create VNET (S2S-Vnet) with S2S-Subnet-1(10.0.1.0/24) and S2S-Subnet-2(10.0.2.0/24).

The screenshot shows the 'Create virtual network' wizard on the 'Basics' step. The 'Subscription' dropdown is set to 'Azure for Students'. The 'Resource group' dropdown is set to 'S2S-RG' with 'Create new' as an option. The 'Name' field is filled with 'S2S-Vnet'. The 'Region' dropdown is set to 'Central US'. At the bottom, there are buttons for 'Review + create', '< Previous', 'Next : IP Addresses >', and 'Download a template for automation'.

The screenshot shows the 'Create virtual network' wizard on the 'IP Addresses' step. The 'IPv4 address space' is set to '10.0.0.0/16 10.0.0.0 - 10.0.255.255 (65536 addresses)'. There is a checkbox for 'Add IPv6 address space'. Below this, there is a table for adding subnets:

Subnet name	Subnet address range	NAT gateway
<input type="checkbox"/> S2S-Subnet-1	10.0.1.0/24	-
<input type="checkbox"/> S2S-Subnet-2	10.0.2.0/24	-

A note at the bottom states: 'Use of a NAT gateway is recommended for outbound internet access from a subnet. You can deploy a NAT gateway and assign it to a subnet after you create the virtual network.' with a link to 'Learn more'.

The screenshot shows the 'Create virtual network' wizard on the 'Security' step. It includes buttons for 'Review + create', '< Previous', 'Next : Security >', and 'Download a template for automation'.

## Create Gateway-Subnet (10.0.0.0/24)

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation pane is open with the following structure:

- Home > Virtual networks > S2S-Vnet
- Virtual network
- Subnets
- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Subnets** (selected)
- Bastion
- DDoS protection
- Firewall
- Microsoft Defender for Cloud
- Network manager
- DNS servers
- Peerings
- Service endpoints
- Private endpoints
- Properties
- Locks
- Monitoring

The main content area displays the 'S2S-Vnet | Subnets' page with two subnets listed:

Name	IPv4	IPv6	Available IPs
S2S-Subnet-1	10.0.1.0/24	-	251
S2S-Subnet-2	10.0.2.0/24	-	251

To the right, a modal dialog box titled 'Add subnet' is open, showing the configuration options for a new subnet:

- Name:** GatewaySubnet
- Subnet address range:** 10.0.0.0/24 (10.0.0.0 - 10.0.0.255 (251 + 5 Azure reserved addresses))
- Add IPv6 address space:** None
- NAT gateway:** None
- Network security group:** None
- Route table:** None
- SERVICE ENDPOINTS:** Services: 0 selected
- SUBNET DELEGATION:** Delegate subnet to a service: None
- NETWORK POLICY FOR PRIVATE ENDPOINTS:**

At the bottom of the dialog are 'Save' and 'Cancel' buttons.

Now let's configure Virtual network gateway.

Name	Vpn-AWS-AZ
Gateway Type	VPN
VPN Type	Route Based
SKU	VpnGw1AZ
Generation	Generation1
Virtual Network	S2S-Vnet
Public IP (create new)	Vpn-AWS-AZ-IP

Microsoft Azure Search resources, services, and docs (G+/-)

Home > Virtual network gateways > Create virtual network gateway

**Instance details**

Name \*: Vpn-AWS-AZ

Region \*: Central US

Gateway type \*: VPN

VPN type \*: Route-based

SKU \*: VpnGw1AZ

Generation: Generation1

Virtual network \*: S2S-Vnet

Subnet: GatewaySubnet (10.0.0.0/24)

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

**Public IP address**

Public IP address \*: Create new

Public IP address name \*: Vpn-AWS-AZ-IP

Public IP address SKU: Standard

Assignment: Static

Availability zone \*: Zone-redundant

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

Microsoft Azure Search resources, services, and docs (G+/-)

Home > Vpn-AWS-AZ

**Overview**

Resource group (move) : S2S-RG

Location : Central US

Subscription (move) : Azure for Students

Subscription ID :

Tags (edit) : Click here to add tags

**Essentials**

SKU : VpnGw1AZ

Gateway type : VPN

VPN type : Route-based

Virtual network : S2S-Vnet

Public IP address : 20.112.214.65 (Vpn-AWS-AZ-IP)

**Health check**

Perform a quick health check to detect possible gateway issues

**Documentation**

View guidance on helpful topics related to VPN gateway

Show data for last 1 hour 6 hours 12 hours 1 day 7 days 30 days

Total tunnel ingress

Total tunnel egress

## 1. AWS SITE CONFIGURATION:

Create a VPC “My-vpc-01” with CIDR 11.0.0.0/16.

[A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 address range when you create a VPC. Specify the IPv4 address range as a Classless Inter-Domain

Routing (CIDR) block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16.]

**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.  
My-vpc-01

**IPv4 CIDR block Info**  
 IPv4 CIDR manual input    IPAM-allocated IPv4 CIDR block  
11.0.0.0/16

**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.

**Feedback** Looking for language selection? Find it in the new [Unified Settings](#) Feedback

**You successfully created `vpc-05fb30927f8e39503 / My-vpc-01`**

**VPC > Your VPCs > `vpc-05fb30927f8e39503`**

**vpc-05fb30927f8e39503 / My-vpc-01**

**Actions ▼**

<b>Details <small>Info</small></b>			
<b>VPC ID</b> <code>vpc-05fb30927f8e39503</code>	<b>State</b> <input checked="" type="radio"/> Available	<b>DNS hostnames</b> Disabled	<b>DNS resolution</b> Enabled
<b>Tenancy</b> Default	<b>DHCP option set</b> <code>dopt-0109a4fb0f9f60085</code>	<b>Main route table</b> <code>rtb-009ec241785a9172f</code>	<b>Main network ACL</b> <code>acl-036606dda231db861</code>
<b>Default VPC</b> No	<b>IPv4 CIDR</b> <code>11.0.0.0/16</code>	<b>IPv6 pool</b> -	<b>IPv6 CIDR</b> -
<b>Route 53 Resolver DNS Firewall rule groups</b> -	<b>Owner ID</b> <code>739767204060</code>		

**CIDRs Info**

<b>Address type</b>	<b>CIDR</b>	<b>Pool</b>	<b>Status</b>
IPv4	<code>11.0.0.0/16</code>	-	<input checked="" type="radio"/> Associated

**Feedback** Looking for language selection? Find it in the new [Unified Settings](#) Feedback

Create a subnet “My-subnet-01” with CIDR (11.0.1.0/24) inside the VPC created.

AWS Services Search for services, features, blogs, docs, and more [Alt+S] Mumbai Ashutosh

### Create subnet Info

**VPC**

VPC ID  
Create subnets in this VPC.  
vpc-05fb30927f8e39503 (My-vpc-01)

Associated VPC CIDRs  
IPv4 CIDRs  
11.0.0.0/16

**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.  
My-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 CIDR block Info  
Q 11.0.1.0/24 X

▼ Tags - optional

Key	Value - optional

Feedback Looking for language selection? Find it in the new Unified Settings ?

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

AWS Services Search for services, features, blogs, docs, and more [Alt+S] Mumbai Ashutosh

New VPC Experience Tell us what you think X

VPC Subnets subnet-0a952a89ea0a00f5f

### subnet-0a952a89ea0a00f5f / My-subnet-01

Actions ▼

**Details**

Subnet ID <a href="#">subnet-0a952a89ea0a00f5f</a>	Subnet ARN <a href="#">arn:aws:ec2:ap-south-1:739767204060:subnet/subnet-0a952a89ea0a00f5f</a>	State <span>Available</span>	IPv4 CIDR <a href="#">11.0.1.0/24</a>
Available IPv4 addresses <a href="#">251</a>		Availability Zone <a href="#">ap-south-1c</a>	Availability Zone ID <a href="#">aps1-az2</a>
VPC <a href="#">vpc-05fb30927f8e39503   My-vpc-01</a>	IPv6 CIDR -	Network ACL <a href="#">acl-036606gda231db861</a>	Default subnet No
Auto-assign public IPv4 address No	Route table <a href="#">rtb-009ec241785a9172f</a>	Auto-assign customer-owned IPv4 address No	Customer-owned IPv4 pool -
Outpost ID -	IPv4 CIDR reservations -	IPv6 CIDR reservations -	IPv6-only No
Hostname type IP name	Resource name DNS A record Disabled	Resource name DNS AAAA record Disabled	DNS64 Disabled
Owner <a href="#">739767204060</a>			

Flow logs Route table Network ACL CIDR reservations Sharing Tags

Feedback Looking for language selection? Find it in the new Unified Settings ?

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

## 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.

Screenshot of the AWS Management Console showing the creation of a Customer Gateway. The search bar at the top shows "customer gateways".

### 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 - 2147483647 range.
- IP address [Info](#)**  
Specify the IP address for your customer gateway device's external interface.
- Certificate ARN**  
The ARN of a private certificate provisioned in AWS Certificate Manager (ACM).
- Device - optional**  
Enter a name for the customer gateway device.

**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.

Feedback Looking for language selection? Find it in the new [Unified Settings](#) 

© 2022, Amazon Internet Services Private Ltd. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

New VPC Experience  Tell us what you think

You successfully created cgw-079e51110b3acbacd / CGW-AWS-AZ. 

### Customer gateways (1) [Info](#)

[Filter customer gateways](#)  Actions  Create customer gateway 

Name	Customer gateway ID	State	BGP ASN	IP address	Type
CGW-AWS-AZ	cgw-079e51110b3acbacd	Available	65000	20.185.83.40	ipsec.1

Select a customer gateway 

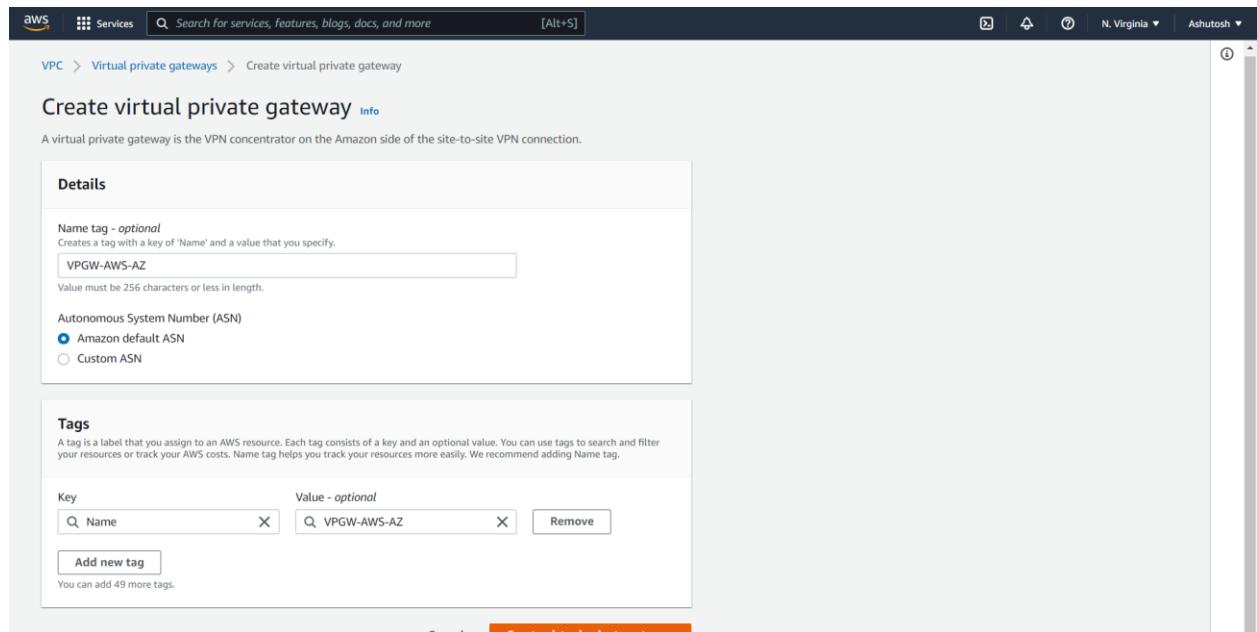
Feedback Looking for language selection? Find it in the new [Unified Settings](#) 

© 2022, Amazon Internet Services Private Ltd. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

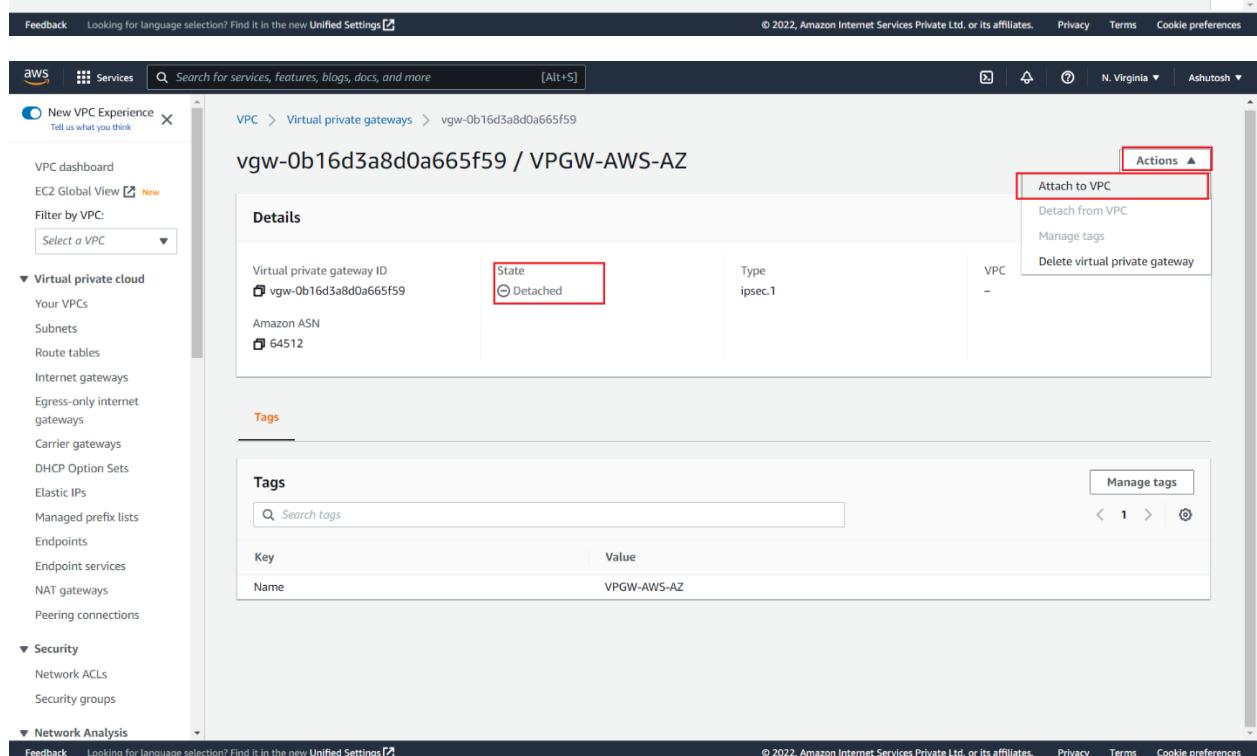
When you create a customer gateway, you provide information about your device to AWS. You or your network administrator must configure the device to work with the site-to-site VPN connection.

## Create the Virtual Private Gateway then attach to the VPC:

A virtual private gateway is the VPN concentrator on the Amazon side of the site-to-site VPN connection. You create a virtual private gateway and attach it to the VPC you want to use for the site-to-site VPN connection.



The screenshot shows the 'Create virtual private gateway' page in the AWS VPC console. In the 'Details' section, a name tag 'VPGW-AWS-AZ' is entered. Under 'Autonomous System Number (ASN)', the 'Amazon default ASN' option is selected. In the 'Tags' section, a single tag 'Name: VPGW-AWS-AZ' is added. At the bottom, the 'Create virtual private gateway' button is highlighted in orange.

The screenshot shows the 'vgw-0b16d3a8d0a665f59 / VPGW-AWS-AZ' details page. The 'State' is shown as 'Detached'. The 'Actions' menu on the right includes options like 'Attach to VPC' (which is highlighted with a red box), 'Detach from VPC', 'Manage tags', and 'Delete virtual private gateway'. The left sidebar shows the navigation path: VPC > Virtual private gateways > vgw-0b16d3a8d0a665f59.

Virtual private gateway ID: vgw-0b31641c1ba705d16

Available VPCs:

- vpc-04050da2dac1312b4
- vpc-05fb30927f8e39503 / My-vpc-01 (highlighted with a red box)

**Attach to VPC**

Feedback: Looking for language selection? Find it in the new Unified Settings.

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Virtual private gateway ID: vgw-0b31641c1ba705d16 / VPGW-AWS-AZ

Details

Virtual private gateway ID: vgw-0b31641c1ba705d16	State: Attached	Type: ipsec.1	VPC: vpc-05fb30927f8e39503   My-vpc-01 (highlighted with a red box)
---------------------------------------------------	-----------------	---------------	---------------------------------------------------------------------

Tags

Key	Value
Name	VPGW-AWS-AZ

Actions

Feedback: Looking for language selection? Find it in the new Unified Settings.

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

## Create a site-to-site VPN Connection:

A Site-to-Site VPN connection offers two VPN tunnels between a virtual private gateway or a transit gateway on the AWS side, and a customer gateway (which represents a VPN device) on the remote (on-premises) side.

**Create VPN connection** [Info](#)

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](#)

**Feedback** Looking for language selection? Find it in the new [Unified Settings](#)

© 2022, Amazon Internet Services Private Ltd. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

**Static IP prefixes** [Info](#)

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.

**Tunnel 1 options** - *optional* [Info](#)

**Tunnel 2 options** - *optional* [Info](#)

**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 - <i>optional</i>
<input type="text" value="Name"/>	<input type="text" value="Vpn-AWS-AZ"/> <input type="button" value="Remove"/>
<input type="button" value="Add new tag"/>	

You can add 49 more tags.

**Feedback** Looking for language selection? Find it in the new [Unified Settings](#)

© 2022, Amazon Internet Services Private Ltd. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Download the configuration file.

The screenshot shows the AWS VPC console with a 'VPN connections (1/1)' list. A 'Download configuration' dialog is open over the list. The dialog has the following fields:

- Vendor:** Generic
- Platform:** Generic
- Software:** Vendor Agnostic
- IKE version:** ikev1

At the bottom right of the dialog are 'Cancel' and 'Download' buttons.

## Amazon Web Services Virtual Private Cloud

### VPN Connection Configuration

---

AWS utilizes unique identifiers to manipulate the configuration of a VPN Connection. Each VPN Connection is assigned a VPN Connection Identifier and is associated with two other identifiers, namely the Customer Gateway Identifier and the Virtual Private Gateway Identifier.

Your VPN Connection ID	:	vpn-01501acef5f22d92c
Your Virtual Private Gateway ID	:	vgw-0b31641c1ba705d16
Your Customer Gateway ID	:	cgw-079e51110b3acbacd

A VPN Connection consists of a pair of IPSec tunnel security associations (SAs). It is important that both tunnel security associations be configured.

**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, SHA1, and DH Group 2.

Category "VPN" connections in the GovCloud region have a minimum requirement of AES128, SHA2, and DH Group 14.

You will need to modify these sample configuration files to take advantage of AES256, SHA256, or other DH groups like 2, 14-18, 22, 23, and 24.

NOTE: If you customized tunnel options when creating or modifying your VPN connection, you may need to modify these sample configurations to match the custom settings for your tunnels.

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

The address of the external interface for your customer gateway must be a static 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 rules to unblock UDP port 4500.

If not behind NAT, and you are not using an Accelerated VPN, we recommend disabling NAT-T. If you are using an Accelerated VPN, make sure that NAT-T is enabled.

- 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 AES128, SHA2, and DH Group 14.

Please note, you may use these additionally supported IPsec parameters for encryption like AES256 and other DH groups like 2, 5, 14-18, 22, 23, and 24.

NOTE: If you customized tunnel options when creating or modifying your VPN connection, you may need to modify these sample configurations to match the custom settings for your tunnels.

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
- 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

**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, SHA1, and DH Group 2.

Category "VPN" connections in the GovCloud region have a minimum requirement of AES128, SHA2, and DH Group 14.

You will need to modify these sample configuration files to take advantage of AES256, SHA256, or other DH groups like 2, 14-18, 22, 23, and 24.

NOTE: If you customized tunnel options when creating or modifying your VPN connection, you may need to modify these sample configurations to match the custom settings for your tunnels.

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

The address of the external interface for your customer gateway must be a static 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 rules to unblock UDP port 4500.

If not behind NAT, and you are not using an Accelerated VPN, we recommend disabling NAT-T. If you are using an Accelerated VPN, make sure that NAT-T is enabled.

- 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 AES128, SHA2, and DH Group 14.

Please note, you may use these additionally supported IPsec parameters for encryption like AES256 and other DH groups like 2, 5, 14-18, 22, 23, and 24.

NOTE: If you customized tunnel options when creating or modifying your VPN connection, you may need to modify these sample configurations to match the custom settings for your tunnels.

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
- Lifetime : 3600 seconds
- Mode : tunnel
- Perfect Forward Secrecy : Diffie-Hellman Group 2

### #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.

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 : 13.127.225.111

#### Inside IP Addresses

- Customer Gateway : 169.254.62.238/30
- Virtual Private Gateway : 169.254.62.237/30

Configure your tunnel to fragment at the optimal size:

- Tunnel interface MTU : 1436 bytes

### #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.

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 : 65.1.105.70

#### Inside IP Addresses

- Customer Gateway : 169.254.161.38/30
- Virtual Private Gateway : 169.254.161.37/30

Configure your tunnel to fragment at the optimal size:

- Tunnel interface MTU : 1436 bytes

After the creation, you should have something like this:

Details

VPN ID vpn-01501acef5f22d92c	State Available	Virtual private gateway vgw-0b31641c1ba705d16	Customer gateway cgw-079e51110b3acbad
Transit gateway -	Customer gateway address 20.185.83.40	Type ipsec.1	Category VPN
VPC -	Routing Static	Acceleration enabled False	Authentication Pre-shared key
Local IPv4 network CIDR 0.0.0.0/0	Remote IPv4 network CIDR 0.0.0.0/0	Local IPv6 network CIDR -	Remote IPv6 network CIDR -
Core network ARN -	Core network attachment ARN -	Gateway association state associated	Outside IP address type PublicIPv4

Tunnel state

Tunnel number	Outside IP address	Inside IPv4 CIDR	Inside IPv6 CIDR	Status	Last status change	Details	Cert
Tunnel 1	13.127.225.111	169.254.62.236/30	-	Down	July 18, 2022, 11:13:13 (UTC+05:30)	-	-

# Adding the AWS information on Azure Configuration:

Now let's create the Local Network Gateway.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and a user profile. The main content area is titled "LNG-AZ-AWS" and "Local network gateway".

**Overview** tab selected:

- Name: LNG-AZ-AWS
- Resource group: S2S-RG
- Location: Central US
- Subscription ID: 9dbeb810-be7d-4dd9-9a12-0f2dd16c41aa
- Tags: Click here to add tags

**Essentials** section:

- IP address: 13.127.225.111
- Address Space(s): 11.0.0.0/16, 11.0.1.0/24, 172.10.1.0/24

**Settings** sidebar:

- Configuration
- Connections (selected)
- Properties
- Locks

**Automation** section:

- Tasks (preview)
- Export template

**Support + troubleshooting** section:

- New Support Request

Page navigation: Page 1 of 1

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and a user profile. The main content area is titled "Vpn-AWS-AZ | Connections" and "Virtual network gateway".

**Connections** tab selected:

- + Add (button highlighted with a red box)
- Refresh (button)

**Search connections** input field:

No results

**Settings** sidebar:

- Configuration
- Connections (selected)
- Point-to-site configuration
- Properties
- Locks

**Monitoring** section:

- Logs
- Alerts
- Metrics
- BGP peers

**Automation** section:

- Tasks (preview)
- Export template

**Support + troubleshooting** section:

- Common health

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.

The screenshot shows the 'Add connection' dialog box in the Microsoft Azure portal. The 'Name' field is set to 'Connection-AWS-AZ'. The 'Connection type' is 'Site-to-site (IPsec)'. The 'Virtual network gateway' is 'Vpn-AWS-AZ' and the 'Local network gateway' is 'LNG-AZ-AWS'. The 'Shared key (PSK)' field contains the placeholder 'Add your shared key for IPsec Tunnel #1'. The 'OK' button is highlighted with a red border.

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

The screenshot shows the 'Connections' page in the Microsoft Azure portal for the 'vpn-azure-aws' resource group. It displays a single connection named 'connection-azure-aws' with a status of 'Connected'. The 'Status' column is highlighted with a red border.

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

The screenshot shows the AWS VPC Connections page. At the top, there's a search bar and a table header with columns: Name, VPN ID, State, Virtual Private Gateway, Transit Gateway, and Customer Gateway. A single row is listed: vpn-aws-azure, vpn-0ca74f7bd72086f4b, available, vgw-033b3758fae1f6443 | vpg..., and cgw-01c9644443bf. Below the table, a section titled "VPN Connection: vpn-0ca74f7bd72086f4b" contains tabs for Details, Tunnel Details (which is selected), Static Routes, and Tags. Under "Tunnel Details", there's a table for "Tunnel State" with columns: Tunnel Number, Outside IP Address, Inside IPv4 CIDR, Inside IPv6 CIDR, and Status. Two tunnels are listed: Tunnel 1 (Status UP) with IP 3.209.186.24 and CIDRs 169.254.150.176/30 and -; and Tunnel 2 (Status DOWN) with IP 52.70.171.101 and CIDRs 169.254.163.68/30 and -.

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

The screenshot shows the AWS Route Tables page. The left sidebar has a "Route Tables" item highlighted with a red box. In the main area, there's a table with columns: Name, Route Table ID, Explicit subnet association, Edge associations, and Main. Two route tables are listed: rtb-03e2fd026035b7d69 (Main Yes) and rtb-bc6db3c5 (Main Yes). A context menu is open over the first route table, listing options: Set Main Route Table, Delete Route Table, Edit subnet associations, Edit edge associations, Edit route propagation, and Edit routes (which is highlighted with a red box). There's also an option for Add/Edit Tags.

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

The screenshot shows the AWS VPC Management console with the URL <https://console.aws.amazon.com/vpc/home?region=us-east-1#EditRoutes:routeTableId=rtb-03e2fd026035b7d69>. The 'Edit routes' page is displayed, showing a table with one existing route (10.10.0.0/16 to local) and one new route being added (172.10.1.0/24 to vgw-). The new route is associated with route table vgw-033b3758fae1f6443 and gateway vpg-aws-azure. The 'Save routes' button 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

The screenshot shows the Microsoft Azure portal with the URL <https://portal.azure.com/?feature.customportal=false#/create>. The 'Create local network gateway' page is displayed, showing fields for Name (Ing-azure-aws-standby), Endpoint (IP address), IP address (10.10.1.1), Address space (10.10.0.0/16), Subscription (Azure CXP FTA Internal Subscription RI...), Resource group (rg-azure-aws), and Location (East US). The 'Create' button is highlighted with a red box.

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

The screenshot shows the 'Add connection' wizard in the Microsoft Azure portal. The left sidebar lists various services like Home, Dashboard, Resource groups, and Virtual networks. The main form is titled 'Add connection' and is configured for a 'Site-to-site (IPsec)' connection. It specifies a 'Virtual network gateway' of 'vpn-azure-aws' and a 'Local network gateway' of 'Lng-azure-aws-standby'. The 'IKE Protocol' is set to 'IKEv2', indicated by a red arrow pointing to the radio button. Other fields include a 'Shared key (PSK)', a subscription of 'Azure CXP FTA Internal Subscription RI...', a resource group of 'rg-azure-aws', and a location of 'East US'. The URL in the browser is <https://portal.azure.com/?feature.customportal=false#@microsoft.onmicrosoft.com>.

And in a few moments we'll have:

The screenshot displays two browser windows side-by-side, illustrating the configuration of a Site-to-Site VPN connection between Microsoft Azure and Amazon AWS.

**Microsoft Azure (Top Window):**

- URL:** https://portal.azure.com/?feature.customportal=false#@microsoft.onmicrosoft.com/resource/su...
- Page Title:** vpn-azure-aws | Connections
- Left Sidebar:** Create a resource, Home, Dashboard, All services, FAVORITES, Resource groups, Load balancers, All resources.
- Content Area:** Shows the connection status for "connection-azure-aws" and "connection-azure-aws-stan...". Both are listed as "Connected".

**AWS VPC Manager (Bottom Window):**

- URL:** https://console.aws.amazon.com/vpc/home?region=us-east-1#VpnConnection
- Page Title:** VPN Connections | VPC Manager
- Left Sidebar:** New VPC Experience, VPC Dashboard, Filter by VPC (Select a VPC), VIRTUAL PRIVATE CLOUD (Your VPCs, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, Carrier Gateways, DHCP Options Sets).
- Content Area:** Shows the creation of a new VPN connection named "vpn-aws-azure". The "Tunnel Details" tab is selected, displaying two tunnels:

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

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

### 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:

The screenshot shows the 'Create internet gateway' wizard in the AWS VPC console. The URL in the browser is <https://console.aws.amazon.com/vpc/home?region=us-east-1#CreateInternetGateway>. The page title is 'Create internet gateway'. The breadcrumb navigation shows 'VPC > Internet gateways > Create internet gateway'. The main section is titled 'Internet gateway settings'.

**Name tag**  
Creates a tag with a key of 'Name' and a value that you specify.  
 (The input field is highlighted with a red border.)

**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
<input type="text" value="Name"/>	<input type="text" value="my-internet-gateway"/> <span style="border: 1px solid #ccc; padding: 2px;">X</span> <span style="border: 1px solid #ccc; padding: 2px;">Remove</span>

**Add new tag**  
You can add 49 more tags.

At the bottom right are 'Cancel' and 'Create internet gateway' buttons. The 'Create internet gateway' button is highlighted with a red border.

After create, let's attach to the VPC:

New VPC Experience  
Tell us what you think

VPC Dashboard New  
Filter by VPC:  
Select a VPC

VIRTUAL PRIVATE CLOUD  
Your VPCs New  
Subnets  
Route Tables  
**Internet Gateways New**  
Egress Only Internet Gateways New  
Carrier Gateways New  
DHCP Options Sets New

igw-02933edb47b855575 / my-internet-gateway

Details Info

Internet gateway ID igw-02933edb47b855575	State Detached	VPC ID -	Owner 292638880518
----------------------------------------------	-------------------	-------------	-----------------------

Actions ▾

- Attach to VPC (highlighted)
- Detach from VPC
- Manage tags
- Delete

Tags

Key	Value
Name	my-internet-gateway

Manage tags

Attach internet gateway | VPC M x +

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

aws Services ▾

VPC > Internet gateways > Attach to VPC (igw-02933edb47b855575)

## Attach to VPC (igw-02933edb47b855575) Info

**VPC**  
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs  
Attach the internet gateway to this VPC.

Select a VPC

vpc-010cbb755e43966b6 - my-vpc-01 (highlighted)

AWS Command Line Interface command

Cancel **Attach internet gateway** (highlighted)

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

The screenshot shows the AWS VPC Management interface under the Route Tables > Edit routes section. A new route is being added to a specific route table. The destination is set to 0.0.0.0/0, and the target is set to igw-02933edb47b855575. Both the destination and target fields are highlighted with red boxes. The status of the route is active. The 'Save routes' button at the bottom right is also highlighted with a red box.

Destination	Target	Status	Propagated
10.10.0.0/16	local	active	No
172.10.1.0/24	vgw-033b3758fae1f6443	active	No
0.0.0.0/0	igw-02933edb47b855575		No

\* Required

Cancel Save routes

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 under the Microsoft Azure section. The user is viewing the effective routes for a specific network interface. The table lists several routes, but two specific ones are highlighted with red boxes. Both routes point to a virtual network gateway with a next hop type of 'Virtual network gateway' and a next hop IP of '20.185.83.40'. The first highlighted route has a source of 'Virtual network gateway' and a state of 'Active'. The second highlighted route also has a source of 'Virtual network gateway' and a state of 'Active'.

Source	State	Address Prefixes	Next Hop Type	Next Hop IP
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 Azure Resource Groups blade for the 'rg-azure-aws' group. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Settings, Cost Management, Monitoring, and Workbooks. The main area displays a table of resources with columns for Name, Type, Location, and three-dot ellipsis actions. The table includes entries for various Azure services like Connection, Local network gateway, Public IP address, Virtual machine, Network security group, Network interface, Disk, Virtual network, and Virtual network gateway, all located in the East US region.

Name	Type	Location	Actions
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-nsq	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:

The screenshot shows the AWS Resource Groups Management blade for the 'rg-aws-azure' group. The left sidebar has sections for Resources (Create Resource Group, Saved Resource Groups), Tagging (Tag Editor, Tag Policies), and AWS Lambda. The main area shows a table of resources under the 'Group resources' section. The table includes entries for EC2 instances, CustomerGateways, InternetGateways, RouteTables, SecurityGroups, Subnets, VPCs, VPNConnections, and VPNGateways, all located in the us-east-1 region. A filter bar at the top allows searching by Identifier, Tag: Name, Service, Type, and Region.

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-02933ed47b855575	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-010ccb755e43966b6	my-vpc-01	EC2	VPC	us-east-1
vpn-0ca74f7bd72086f4b	vpn-aws-azure	EC2	VPNConnection	us-east-1
vgw-033b3758fae1f6443	vgp-aws-azure	EC2	VPNGateway	us-east-1

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

11.0.0.0/16

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.10.1.4 brd 172.10.1.255 netm 255.255.255.0
    ineto fe80::20a:3aff:fe8d:1be9 brd 172.10.1.255
    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)
    ... dropped 0 overruns 0 carrier 0 collisions 0
```

```
mmartins@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
```

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
    inet 10.10.1.49 brd 10.10.1.255 netm 255.255.255.0
    ineto fe80::10a:92ff:fe9b:a2bd brd 10.10.1.255
    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
```

```
mmartins@aws-vm:~$ 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
```

AWS Linux VM