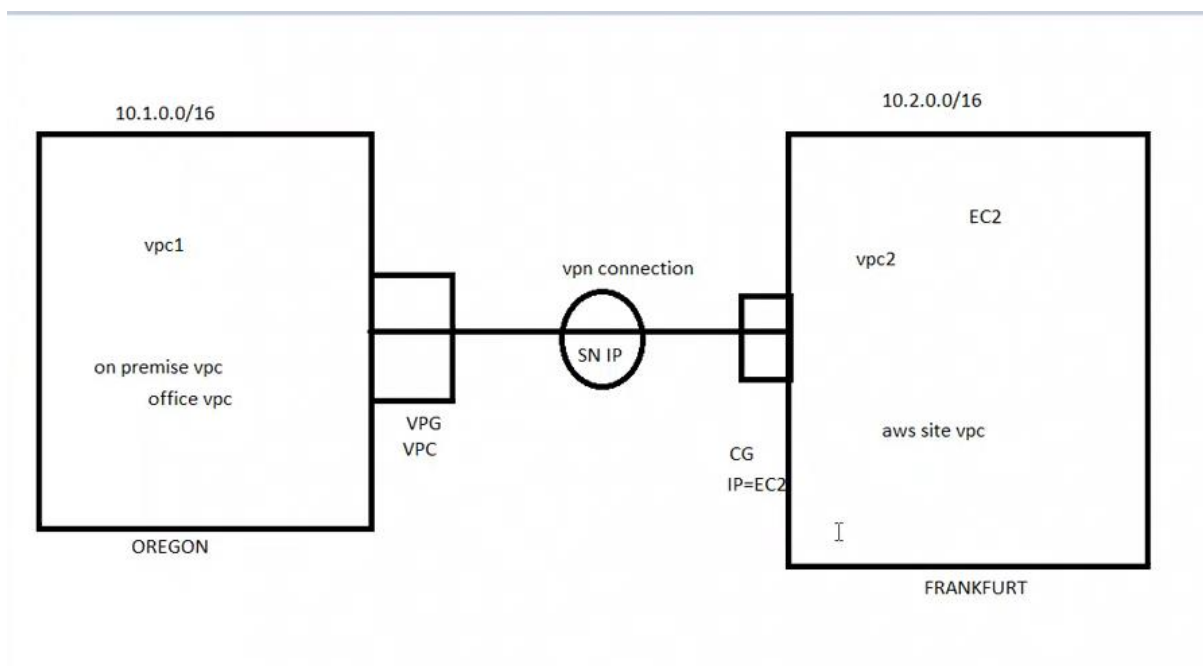


## **SITE-TO-SITE VPN**

---

By default, instances that you launch into an Amazon VPC can't communicate with your own (remote) network. You can enable access to your remote network from your VPC by creating an AWS Site-to-Site VPN (Site-to-Site VPN) connection and configuring routing to pass traffic through the connection.



- We have to create 2 VPC in two different regions. Let's Start by creating a 1<sup>st</sup> VPC in N.Virginia.

aws Services Search [Alt+S] N. Virginia

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.

IPv4 CIDR block [Info](#)  
☒ IPv4 CIDR manual input  
☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

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](#)

➤ Create Subnet.

aws Services Search [Alt+S] N. Virginia

VPC > Subnets > Create subnet

## Create subnet [Info](#)

### VPC

VPC ID  
Create subnets in this VPC.

Associated VPC CIDRs

IPv4 CIDRs  
10.1.0.0/16

### 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.  
  
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.

IPv4 CIDR block [Info](#)

➤ Create a internet gateway and attach it to the VPC.

The screenshot shows the AWS Management Console interface for creating an internet gateway. The top navigation bar includes the AWS logo, 'Services' menu, a search bar, and the region 'N. Virginia'. The breadcrumb trail is 'VPC > Internet gateways > Create internet gateway'. The main heading is 'Create internet gateway' with an 'Info' link. A descriptive paragraph states: '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.' Below this is a form section titled 'Internet gateway settings'. It contains a 'Name tag' field with the value 'batch7-igt1' and a description: 'Creates a tag with a key of 'Name' and a value that you specify.' At the bottom, there is a 'Tags - optional' section with a description: '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.'

- Create a Route table. And then edit the Route and make subnet association.

The screenshot shows the AWS Management Console interface for creating a route table. The top navigation bar includes the AWS logo, 'Services' menu, a search bar, and the region 'N. Virginia'. The breadcrumb trail is 'VPC > Route tables > Create route table'. The main heading is 'Create route table' with an 'Info' link. A descriptive paragraph states: 'A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.' Below this is a form section titled 'Route table settings'. It contains a 'Name - optional' field with the value 'batch-7-rt1' and a description: 'Create a tag with a key of 'Name' and a value that you specify.' Below that is a 'VPC' dropdown menu with the selected value 'vpc-02fe737b9cbb4b0a (batch-7-vpc1)'. At the bottom, there is a 'Tags' section with a description: '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.' The 'Tags' section shows a table with columns 'Key' and 'Value - optional'. It contains one tag with 'Key' 'Name' and 'Value' 'batch-7-rt1'. There are 'X' buttons to remove each tag and a 'Remove' button.

- Now we have to Create a Second a VPC in another Region (Oregon) steps are same so below we have the screenshot for the same.

aws Services Search [Alt+S] Oregon

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.

batch-7-vpc2

**IPv4 CIDR block** [Info](#)  
☒ IPv4 CIDR manual input  
☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR  
10.2.0.0/16

**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

aws Services Search [Alt+S] Oregon

VPC > Subnets > Create subnet

## Create subnet [Info](#)

### VPC

**VPC ID**  
Create subnets in this VPC.

vpc-0be1b757f912e1ad (batch-7-vpc2)

**Associated VPC CIDRs**  
IPv4 CIDRs  
10.2.0.0/16

### 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.

batch7-subnet-2  
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](#)  
10.2.0.0/16

➤ Creating the Internet gateway.

✓ The following internet gateway was created: igw-0e370648c920d2ad8 - batch-7-igt2. You can now attach to a VPC to enable the VPC to communicate with the internet. [Attach to a VPC](#) ✕

VPC > Internet gateways > igw-0e370648c920d2ad8

## igw-0e370648c920d2ad8 / batch-7-igt2 [Actions](#)

**Details** [Info](#)

Internet gateway ID	State	VPC ID	Owner
igw-0e370648c920d2ad8	Detached	-	528519205020

**Tags** [Manage tags](#)

### ➤ Attach the VPC

aws Services  [Alt+S] Oregon ▼

VPC > Internet gateways > Attach to VPC (igw-0e370648c920d2ad8)

## Attach to VPC (igw-0e370648c920d2ad8) [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.

**AWS Command Line Interface command**

[Cancel](#) [Attach internet gateway](#)

### ➤ Create Route table

aws Services  [Alt+S] Oregon ▼

VPC > Route tables > Create route table

## Create route table [Info](#)

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

**Route table settings**

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

**VPC**  
The VPC to use for this route table.

**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.

### ➤ Edit Route table.

VPC > Route tables > rtb-05639306bd8d28b7e > Edit routes

## Edit routes

Destination	Target	Status	Propagated
10.2.0.0/16	Q local X	Active	No
Q 0.0.0.0/0 X	Q igw- X igw-0e370648c920d2ad8 (batch-7-igt2)	-	No

Add route

Remove

Cancel Preview Save changes

### ➤ Edit Subnet association.

VPC > Route tables > rtb-05639306bd8d28b7e > Edit subnet associations

## Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/1)

Q Filter subnet associations

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
batch7-subnet-2	subnet-073781dcf53a8768e	10.2.0.0/16	-	Main (rtb-08248c6e78473011d)

Selected subnets

subnet-073781dcf53a8768e / batch7-subnet-2 X

Cancel Save associations

### ➤ Now We have to create EC2 in VPC2 and make changes in Network setting.

aws

Services

Search

[Alt+S]

Oregon

EC2 > Instances > Launch an instance

## Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name

batch-7-ec2

Add additional tags

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Q Search our full catalog including 1000s of application and OS images

Recents

Quick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

S

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

▼ Summary

Number of instances [Info](#)

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.0.2...[read more](#)

ami-0efa651876de2a5ce

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel

Launch instance

[Review commands](#)

aws

Services

Search

[Alt+S]

Oregon

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-0be1b757f912e1ad (batch-7-vpc2)

10.2.0.0/16

Subnet [Info](#)

subnet-073781dcf53a8768e

batch-7-subnet-2

VPC: vpc-0be1b757f912e1ad Owner: 528519205020 Availability Zone: us-west-2a IP addresses available: 65531 CIDR: 10.2.0.0/16

Create new subnet

Auto-assign public IP [Info](#)

Enable

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

Security group name - required

launch-wizard-2

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and \_-./!@#.%&\*~'

Description - required [Info](#)

launch-wizard-2 created 2023-04-05T07:41:07.470Z

Inbound security groups rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)

Remove

Type [Info](#)

Protocol [Info](#)

Port range [Info](#)

ssh

TCP

22

▼ Summary

Number of instances [Info](#)

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.0.2...[read more](#)

ami-0efa651876de2a5ce

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel

Launch instance

[Review commands](#)

➤ Create Virtual private gateway in VPC1 and attach the VPC.

VPC > Virtual private gateways > vgw-018f894b93f9c8866

## vgw-018f894b93f9c8866 / batch7-vpg

**Details**

Virtual private gateway ID	State	Type	VPC
vgw-018f894b93f9c8866	Detached	ipsec.1	-
Amazon ASN			
64512			

Actions ▲

- Attach to VPC
- Detach from VPC
- Manage tags
- Delete virtual private gateway

Taas

➤ Now create customer gateway in VPC1 and give the public ID of ec2.

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.

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).

Select certificate ARN ▼

**Device - optional**  
Enter a name for the customer gateway device.

Taas

➤ Create VPN connection.



# 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.

batch-7-vpn

Value must be 256 characters or less in length.

Target gateway type [Info](#)

☒ Virtual private gateway

☐ Transit gateway

☐ Not associated

Virtual private gateway

vgw-018f894b93f9c8866 / batch7-vpg

Customer gateway [Info](#)

☒ Existing

☐ New

Customer gateway ID

cgw-0e9c0c53cd24f1d1e / batch7-CGTW

Routing options [Info](#)

☐ Dynamic (requires BGP)

☒ Static

VPC > VPN connections > vpn-0fff03eac5be63137

vpn-0fff03eac5be63137 / batch-7-vpn

Download configurationActions

Details

VPN ID

vpn-0fff03eac5be63137

Transit gateway

-

VPC

-

Local IPv4 network CIDR

10.2.0.0/16

Core network ARN

-

State

Available

Customer gateway address

192.1.1.1

Routing

Dynamic

Remote IPv4 network CIDR

10.1.0.0/16

Core network attachment ARN

-

Virtual private gateway

vgw-018f894b93f9c8866

Type

ipsec.1

Acceleration enabled

False

Local IPv6 network CIDR

-

Gateway association state

associated

Customer gateway

cgw-0e9c0c53cd24f1d1e

Category

VPN

Authentication

Pre-shared key

Remote IPv6 network CIDR

-

Outside IP address type

PublicIpv4

Tunnel detailsTags

Tunnel state

Tunnel number	Outside IP address	Inside IPv4 CIDR	Inside IPv6 CIDR	Status	Last status change	Details	Pending maintenance	Maintenance auto a
Tunnel 1	3.218.69.83	169.254.175.220/30	-	Down	April 5, 2023, 13:31:16 (UTC+05:30)	IPSEC IS DOWN	-	-
Tunnel 2	52.5.65.46	169.254.146.240/30	-	Down	April 5, 2023, 13:31:16 (UTC+05:30)	IPSEC IS DOWN	-	-

In order to make the tunnel “UP” you have to configure the EC2 with customer gateway.

END