

Creating a VPC with a public subnet and a private subnet

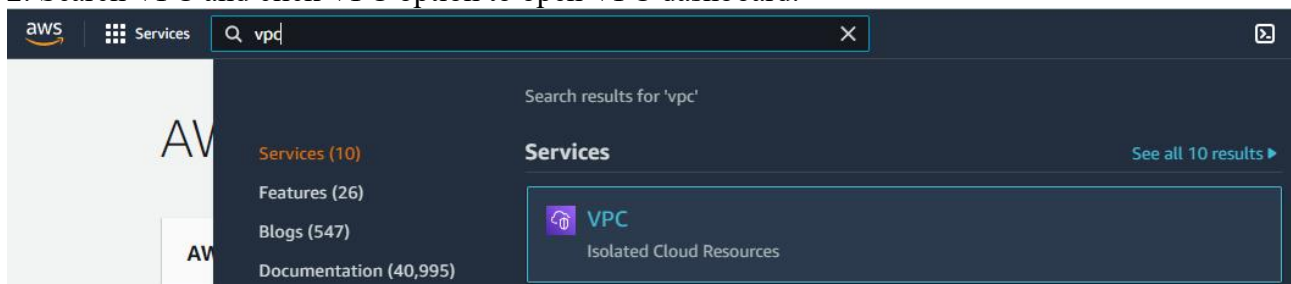
This document describes how to create a Virtual Private Cloud (VPC) in AWS. The VPC will have a public subnet and a private subnet. The public subnet will be connected to the Internet using an Internet Gateway. The Internet Gateway is designed to provide one to one NAT for the instances connected to the public subnet. This will assign public IP address to the instances connected to the public subnet.

The private subnet will not be connected to Internet. Thus the VM's in the private subnet will have no access to Internet. To access these VM's you need to access the VM in the public subnet. Then from that vm you access these private VM's.

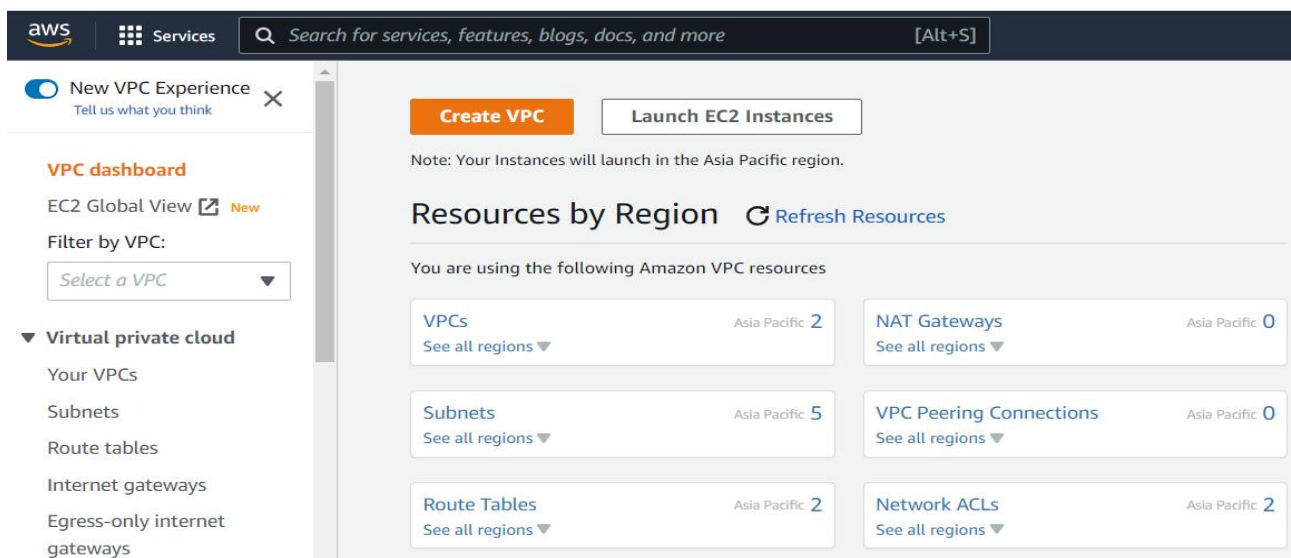
The private subnet can be provided Internet using a NAT gateway, however NAT Gateway is chargeable. Thus even though the step is included, do not perform if you don't want to pay charges.

1. Login to <https://console.aws.amazon.com> with your credentials.

2. Search VPC and click VPC option to open VPC dashboard.



3. Once the VPC dashboard opens ,click Create VPC button shown in orange colour..



4. On the next page that opens click VPC only button. In the Name-tag field provide a name for the VPC. In the IPV4 CIDR block type 10.1.0.0/16 (for each VPC it should be different like 10.2.0.0/16 , 10.3.0.0/16 etc.)

Keep all other settings as default and click Create VPC.

It is shown in the following image.

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.

my-vpc1

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

IPv4 CIDR
10.1.0.0/16

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 your resources or track your AWS costs.

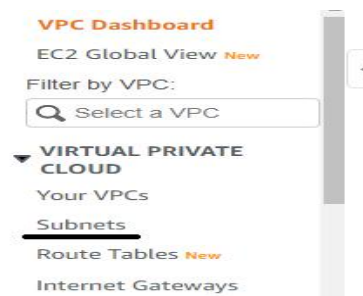
Key	Value - optional	
Q Name	Q my-vpc1	Remove

[Add new tag](#)

You can add 49 more tags.

Cancel [Create VPC](#)

5. Now create 2 subnets in the above VPC. For that click on the subnets option on the left side.



6. Click Create Subnet button. The page that opens first select the VPC created above.

Create subnet [Info](#)

VPC

VPC ID
Create subnets in this VPC.

vpc-0002df016ef42b310 (demo-vpc)

Associated VPC CIDRs

IPv4 CIDRs
172.16.0.0/16

Below this enter subnet details like subnet name, Availability zone, IPv4 CIDR block etc. The IPv4 CIDR block should be a subnet of the VPC CIDR.

If you are working in Mumbai region, then **do not select ap-south-1c availability zone**, as it does not support free tier instance t2.micro.

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.
demo-vpc-public
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.
Asia Pacific (Mumbai) / ap-south-1a

IPv4 CIDR block [Info](#)
172.16.1.0/24

▼ **Tags - optional**

We need to create one more subnet as private subnet. Thus click Add New Subnet button below. Enter details for the new subnet similar to the above.

Subnet 2 of 2

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
demo-vpc-private
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.
Asia Pacific (Mumbai) / ap-south-1a

IPv4 CIDR block [Info](#)
172.16.5.0/24

▼ **Tags - optional**

Key	Value - optional	
Name	demo-vpc-private	Remove

Add new tag
You can add 49 more tags.

Click Create Subnet.

7. Create an Internet Gateway. Click Internet Gateways option on the left side menu.



8. Click Create Internet Gateway button. In the Name tag provide a name. Then click Create Internet Gateway button.

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.
demo-vpc-igw

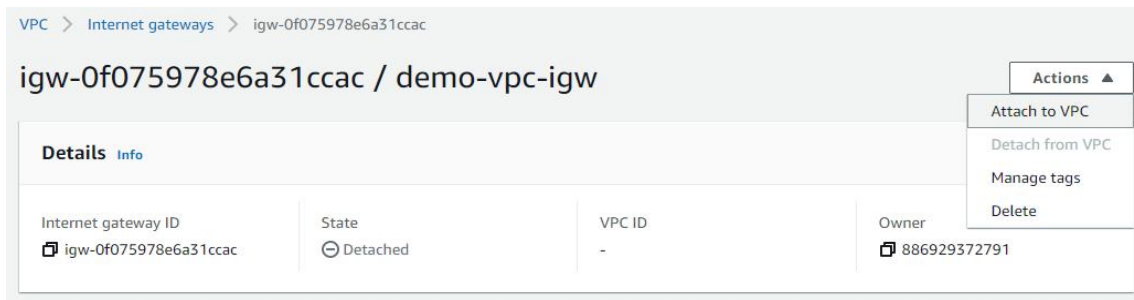
Tags - optional
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional	
Name	demo-vpc-igw	Remove

Add new tag
You can add 49 more tags.

Cancel **Create internet gateway**

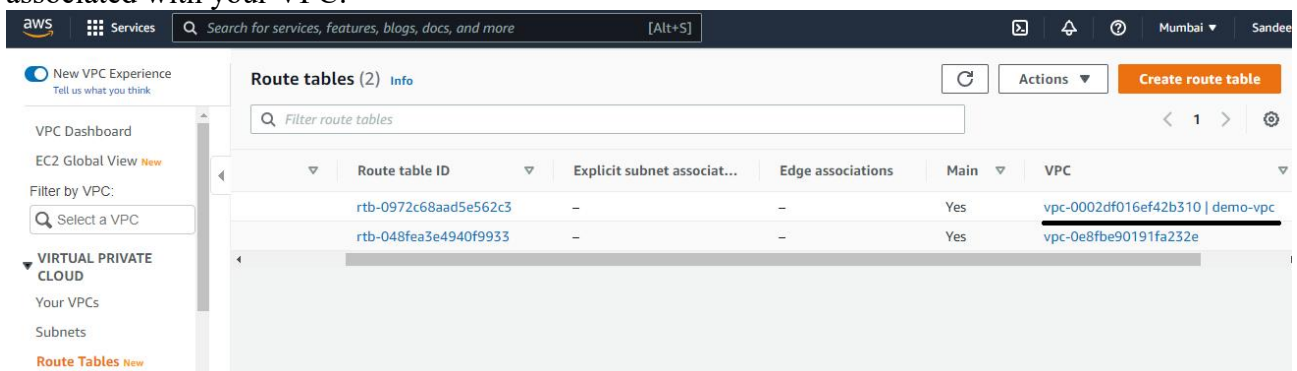
9. Once the Internet Gateway is created, on the screen that is displayed, click Actions button and click Attach to VPC.



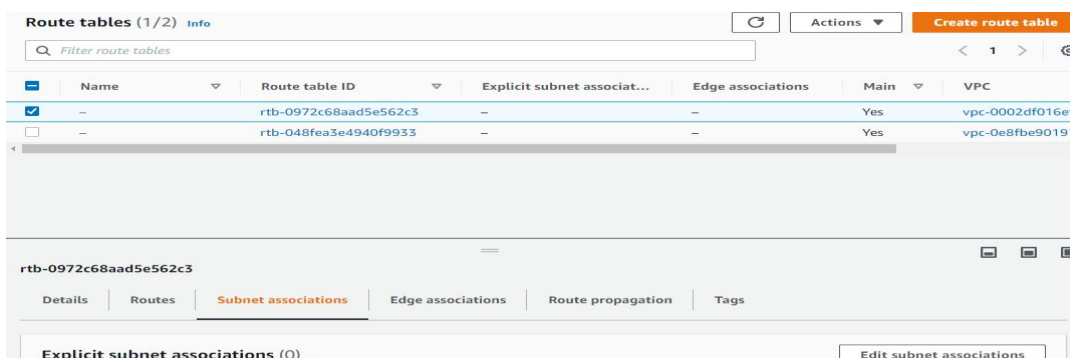
In the page that opens click and select your VPC. Click Attach Internet Gateway.



10. Now add entry into the route table to send all traffic through Internet Gateway. Click on the Route tables option on the left side above Internet Gateways. Find the route table associated with your VPC.



Select that subnet check box. Then select subnet association below. Then click Edit subnet association button.



In the list of subnets displayed, select the public subnet. Then click Save associations.

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/2)

Filter subnet associations

	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/>	demo-vpc-public	subnet-0160ad2ba52f93046	172.16.1.0/24	–	Main (rtb-0972c68aad5e562c3)
<input type="checkbox"/>	demo-vpc-private	subnet-00ffca1c6708f4ecb	172.16.5.0/24	–	Main (rtb-0972c68aad5e562c3)

Selected subnets

subnet-0160ad2ba52f93046 / demo-vpc-public

Cancel Save associations

Now make sure the route table associated with your VPC is selected. Below click the **Routes** option as shown in the orange colour in the following image.

EC2 Global View New

Filter by VPC:

Select a VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

DHCP Option Sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC
<input type="checkbox"/>	–	rtb-034230ee41afa49f4	subnet-0496d3308706f...	–	Yes	vpc-0a3be847f6c2222f9 my...
<input checked="" type="checkbox"/>	–	rtb-01c98d3296b21be08	–	–	Yes	vpc-05174e307dd4203ec my...
<input type="checkbox"/>	default	rtb-048fea3e4940f9933	–	–	Yes	vpc-0e8fbe90191fa232e def...

Details Routes Subnet associations Edge associations Route propagation Tags

Routes (1)

Filter routes

Both

Edit routes

Then click Edit Routes button , in the right bottom of the screen.

In the Edit Routes window that opens, click Add Route button. In the new route option that is shown select 0.0.0.0/0 in the destination field. Then below target click and select Internet Gateway option. This will display the Internet Gateway name as shown below. Select it. Then Click Save Changes.

Edit routes

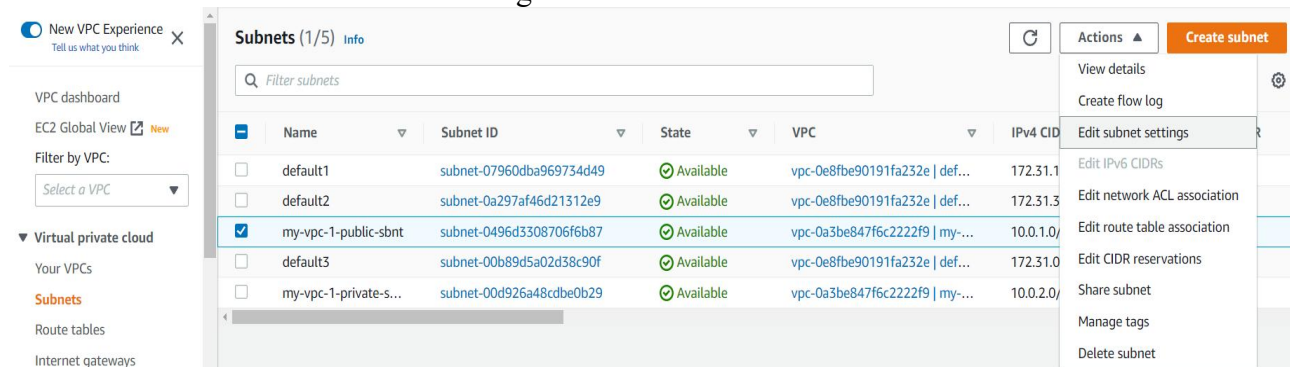
Destination	Target	Status	Propagated
10.1.0.0/16	local	Active	No
0.0.0.0/0	igw-	–	No
	igw-08f708f10845ad4de (my-vpc1-igw)		

Add route

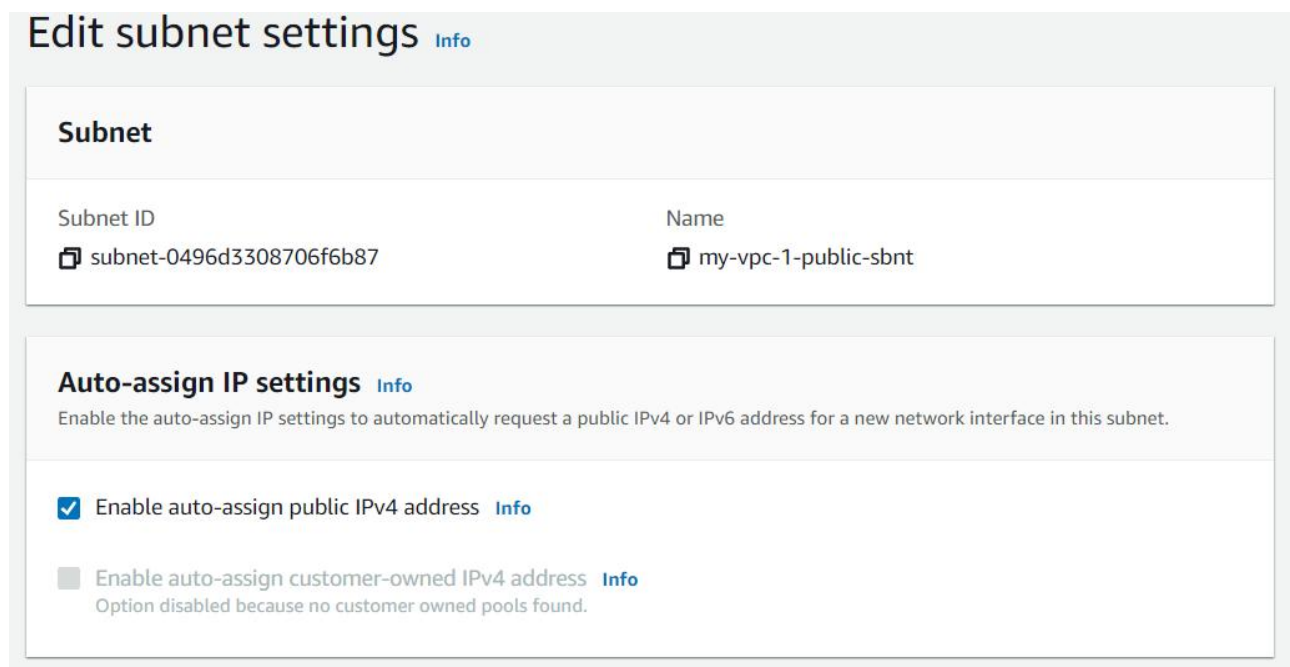
Remove

Cancel Preview Save changes

11. Now enable auto public IP assignment for the EC2 instances connected to the public subnet. For this go to subnets in the VPC console. Click the check box of the public subnet then go to the Actions tab and click Edit Subnet settings.



In the new page that opens, select the check box for Enable auto-assign public IPV4 address.



Then click Save.

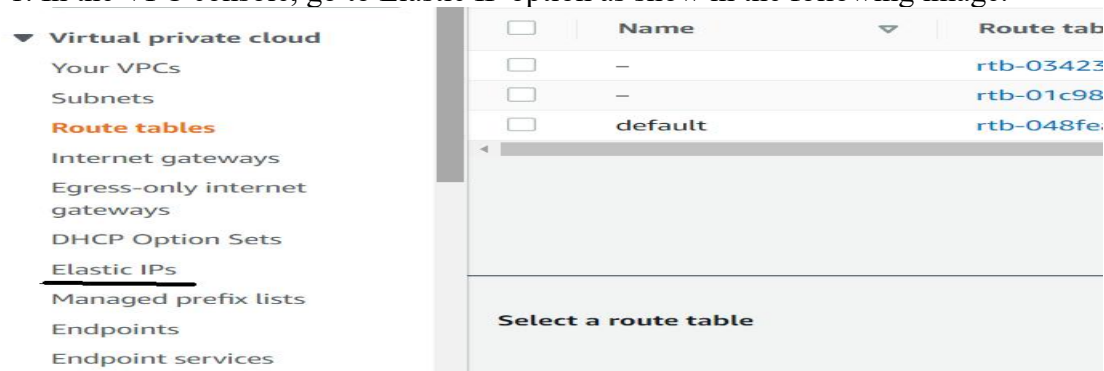
This is how you have successfully created a VPC with a public subnet and a private subnet. Public subnet VM's will have access to and from Internet. However the private subnet VM's will not have any Internet access.

To provide oneway Internet access to private subnet VM's perform following steps.

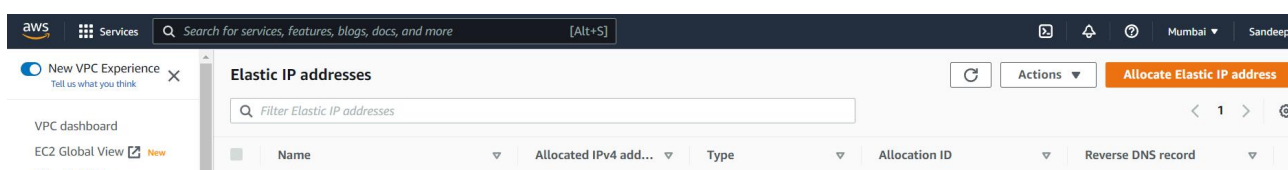
Following steps will have charges applied. The NAT gateway is not free. It has per hour charges of around \$0.045/hr. However it may change so confirm before using it.

Following steps will provide Internet (one way I.e from VM to Internet). But VM's can not be accessed from over Internet directly.

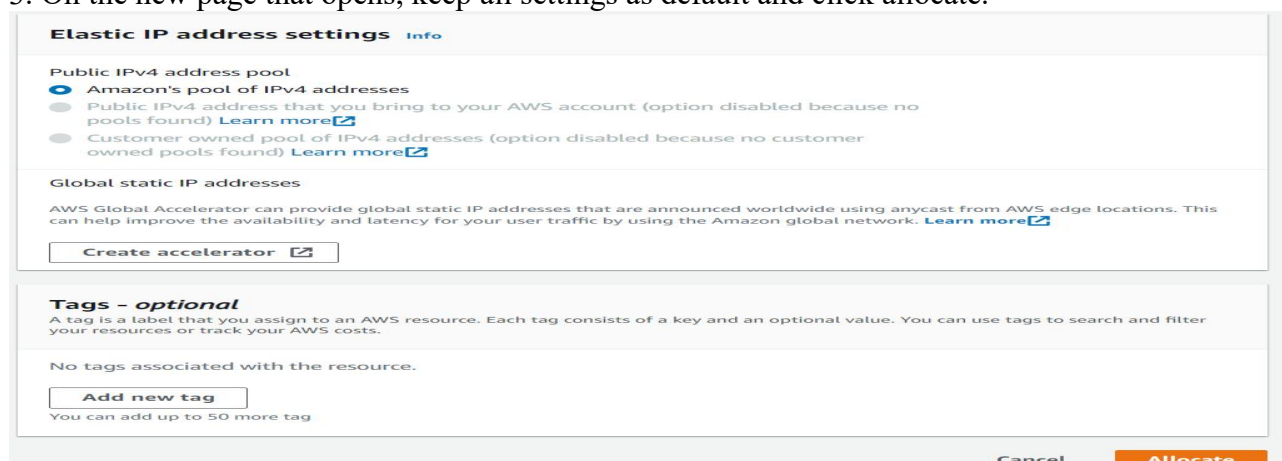
1. In the VPC console, go to Elastic IP option as show in the following image.



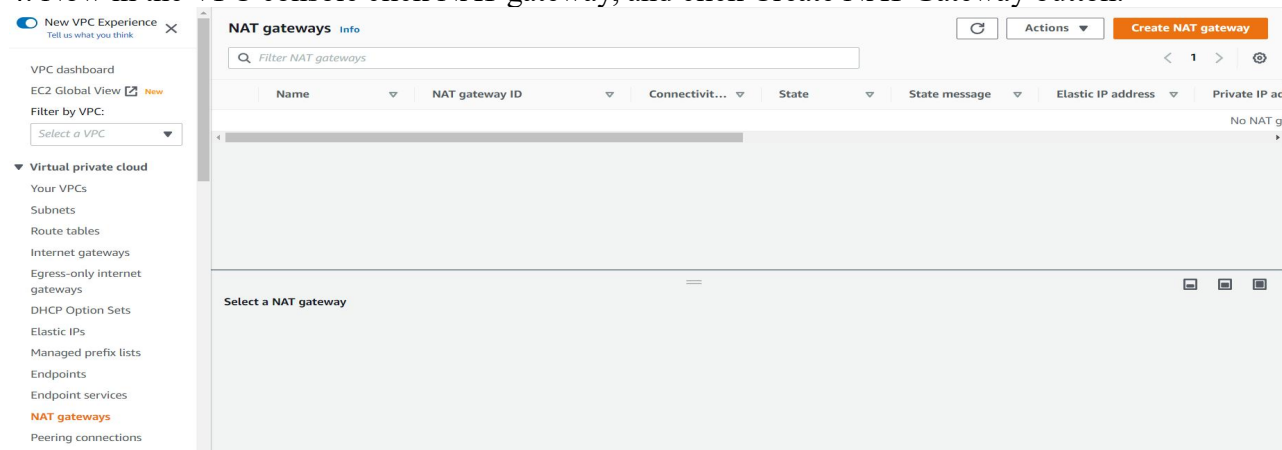
2. In the page that opens, click Allocate Elastic IP.



3. On the new page that opens, keep all settings as default and click allocate.



4. Now in the VPC console click NAT gateway, and click Create NAT Gateway button.



5. In the Create NAT Gateway page, Provide a name to the NAT Gateway. Then in the Subnet field, click drop down arrow and select your private subnet created in the VPC. Select the Elastic IP created above in the Elastic IP allocation field. Then click Create NAT Gateway button.

Create NAT gateway [Info](#)

A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the internet.

NAT gateway settings

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

The name can be up to 256 characters long.

Subnet
Select a subnet in which to create the NAT gateway.

Connectivity type
Select a connectivity type for the NAT gateway.
☒ Public
☐ Private

Elastic IP allocation ID [Info](#)
Assign an Elastic IP address to the NAT gateway.

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	
<input type="text" value="Name"/>	<input type="text" value="My-vpc1-NG"/>	<input type="button" value="Remove"/>

You can add 49 more tags.

Now you have successfully created a new VPC with one public subnet and one private subnet.

Now create 2 Linux Instances. While creating attach one VM in public subnet and other in Private subnet. Try to access private subnet VM from public subnet VM.

Do not forget to delete NAT Gateway first. Once the NAT Gateway is deleted then go to Elastic IP. Select the elastic IP checkbox. Click actions tab and click Release Elastic IP.