Creating a VPC with a public subnet and a private subnet

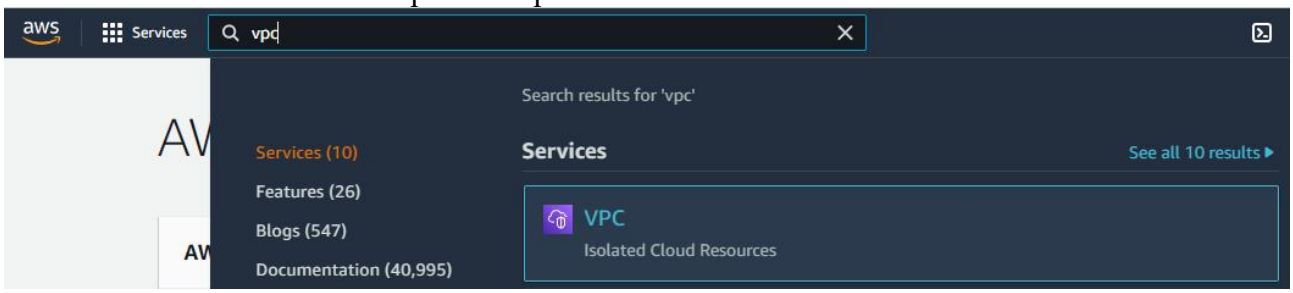
This document describes how to create a Virtual Private Cloud (VPC) in AWS. The VPC will have a public subnet and a private subnet. The public subnet will be connected to the Internet using an Internet Gateway. The Internet Gateway is designed to provide one to one NAT for the instances connected to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

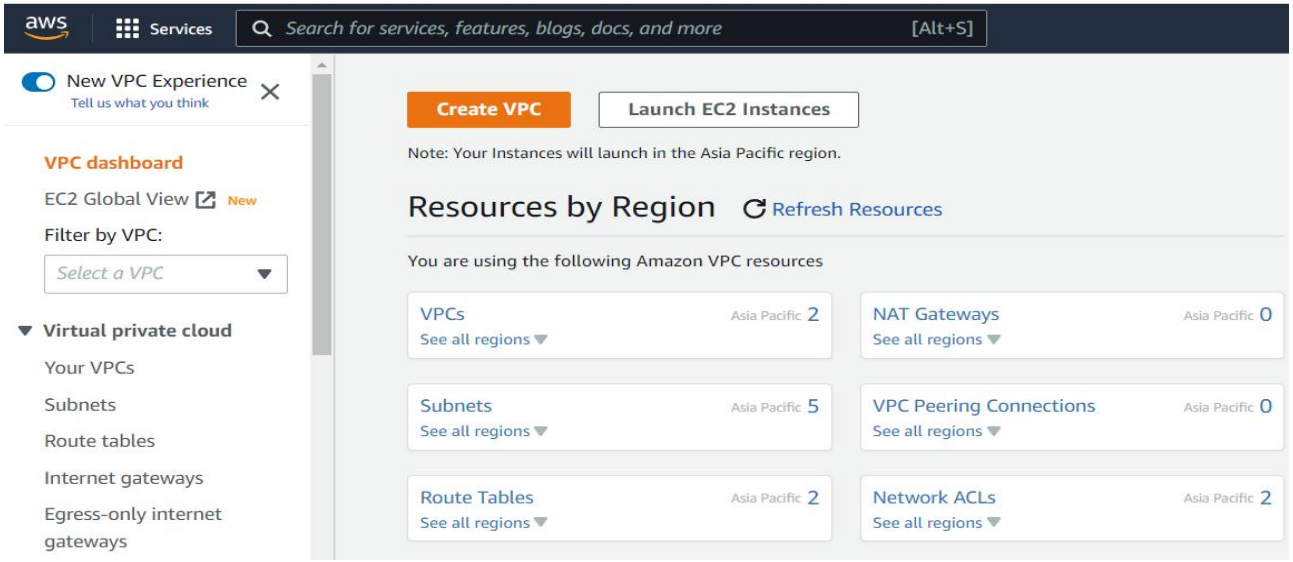
The private subnet can be provided Internet using a NAT gateway, however NAT Gateway is chargeable. Thus even though the step is included, do not perform if you don't want to pay charges.

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

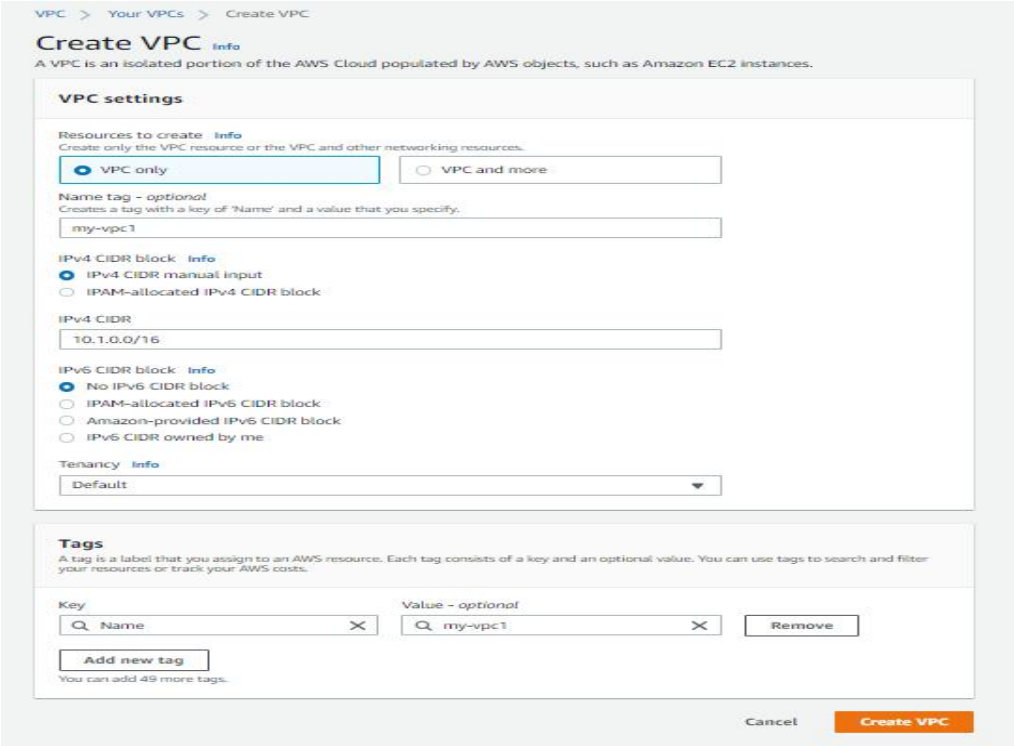
2. Search VPC and click VPC option to open VPC dashboard.



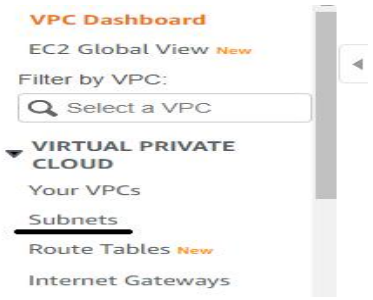
3. Once the VPC dashboard opens ,click Create VPC button shown in orange colour..



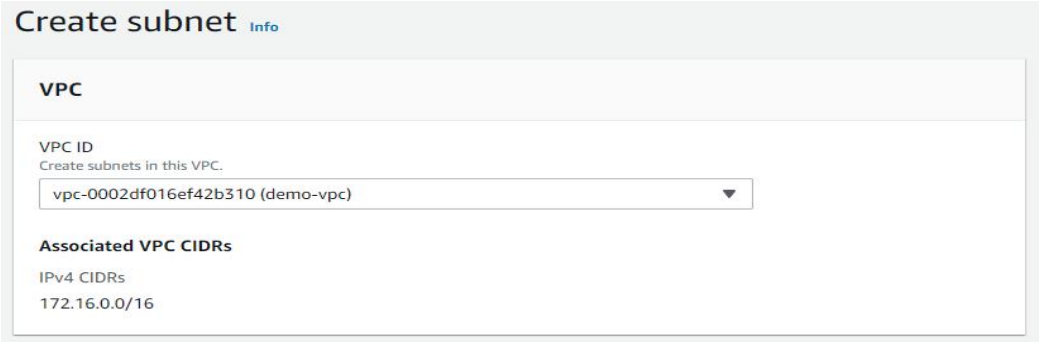
4. On the next page that opens click VPC only button. In the Name-tag field provide a name for the VPC. In the IPV4 CIDR block type 10.1.0.0/16 (for each VPC it should be different like 10.2.0.0/16 , 10.3.0.0/16 etc.)
Keep all other settings as default and click Create VPC.
It is shown in the following image.



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

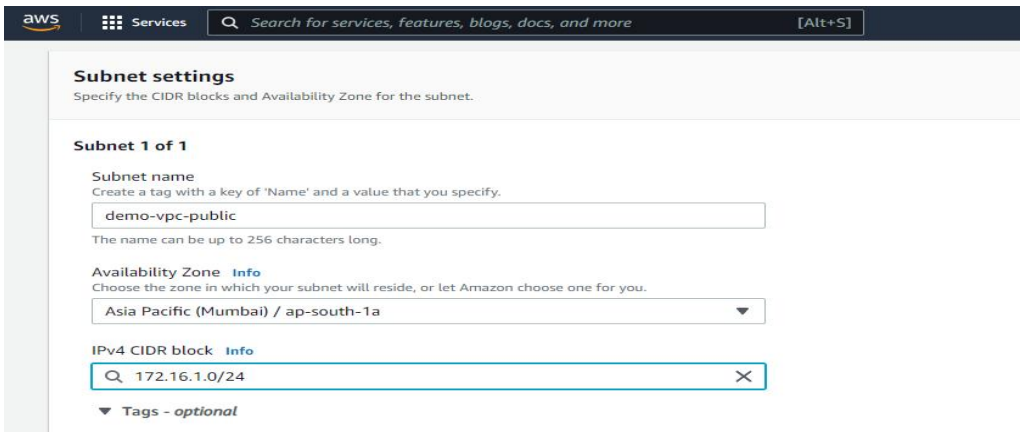


6. Click Create Subnet button. The page that opens first select the VPC created above.



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.

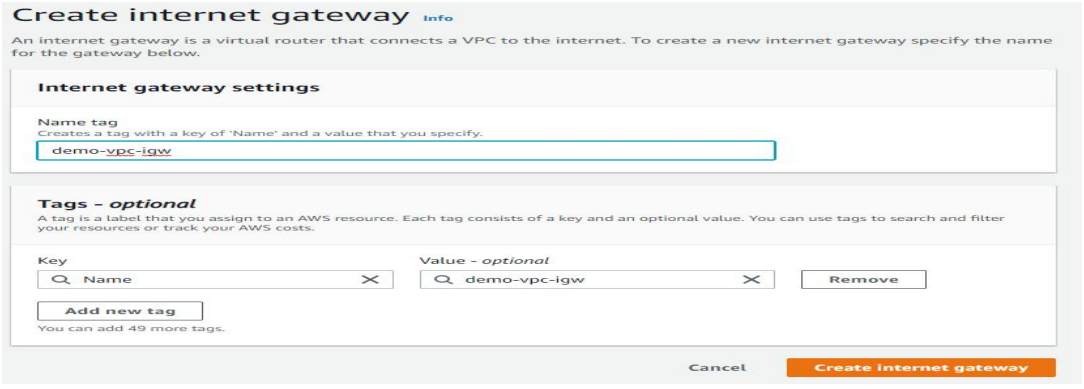


We need to create one more subnet as private subnet. Thus click Add New Subnet button below. Enter details for the new subnet similar to the above.

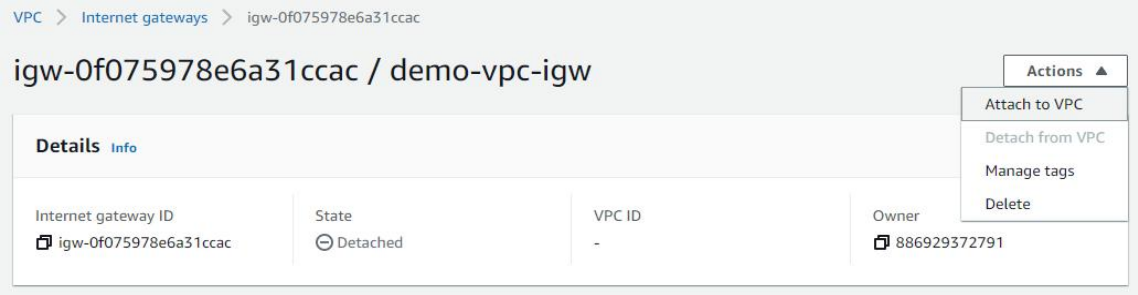
Click Create Subnet.

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

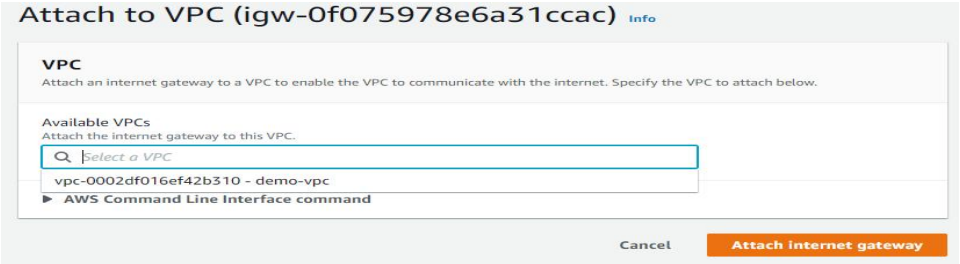
8. Click Create Internet Gateway button. In the Name tag provide a name. Then click Create Internet Gateway button.



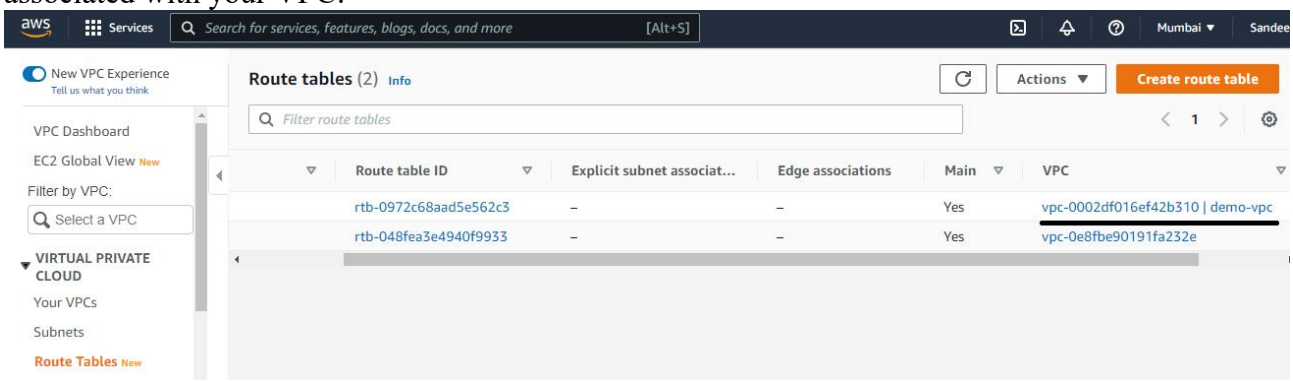
9. Once the Internet Gateway is created, on the screen that is displayed, click Actions button and click Attach to VPC.



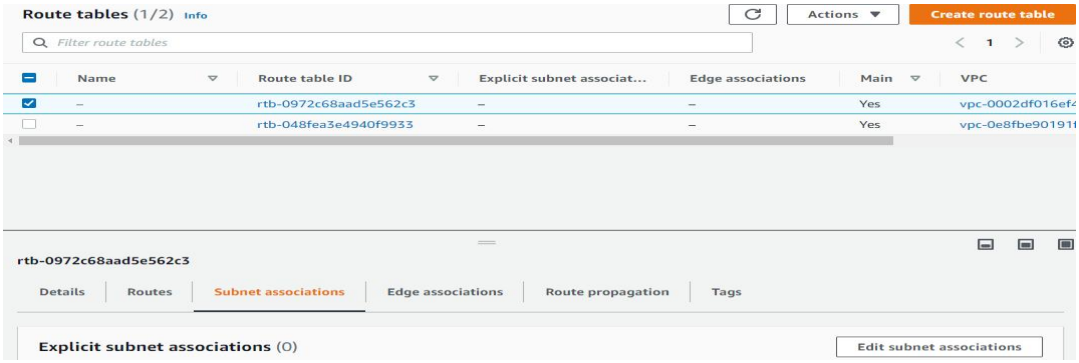
In the page that opens click and select your VPC. Click Attach Internet Gateway.



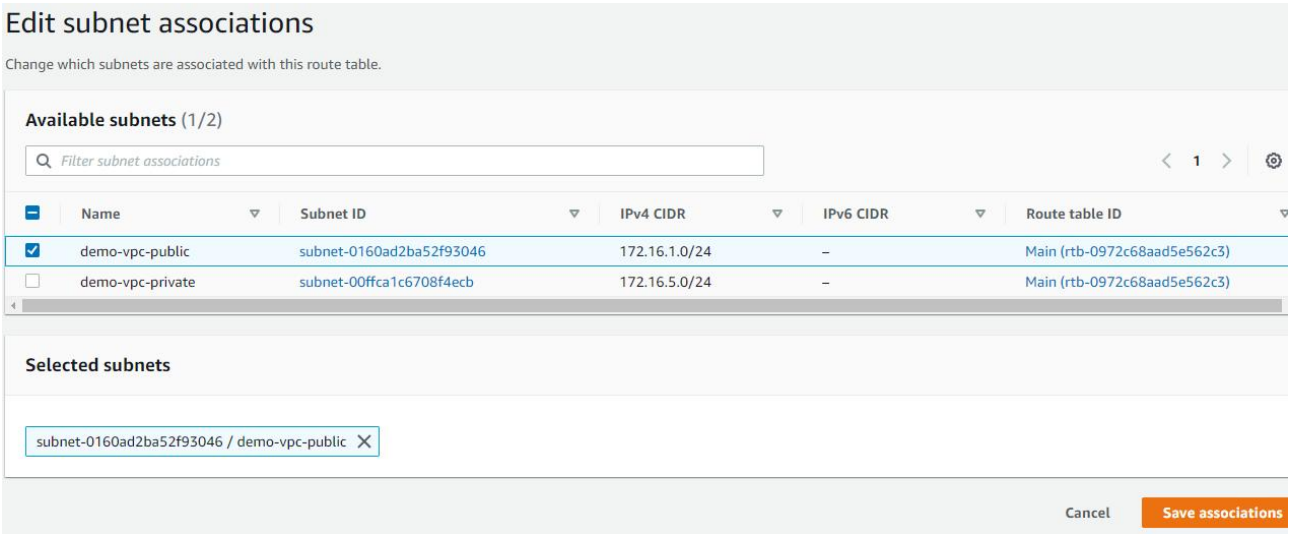
10. Now add entry into the route table to send all traffic through Internet Gateway.
Click on the Route tables option on the left side above Internet Gateways. Find the route table associated with your VPC.



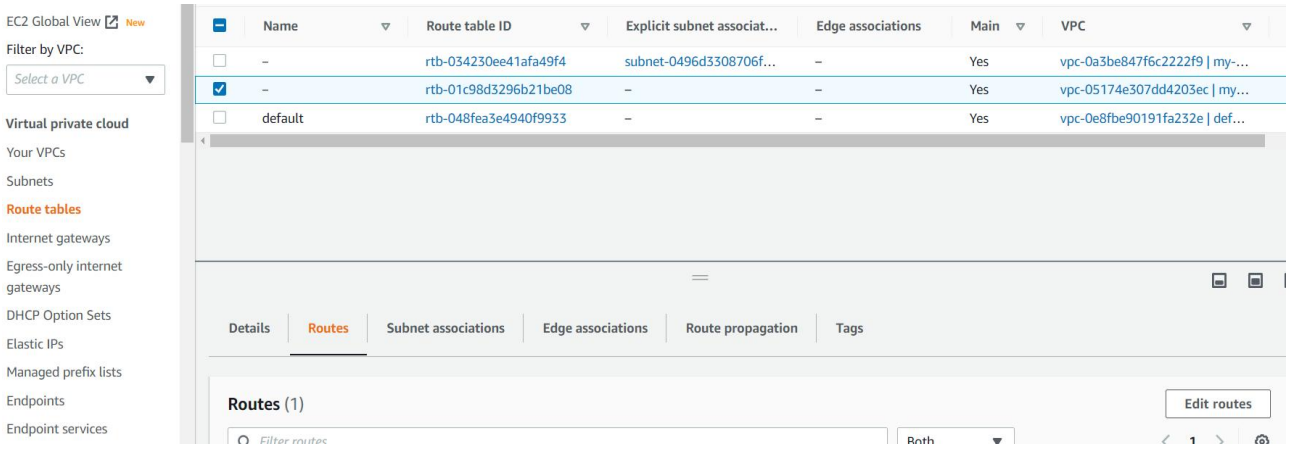
Select that subnet check box. Then select subnet association below. Then click Edit subnet association button.



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

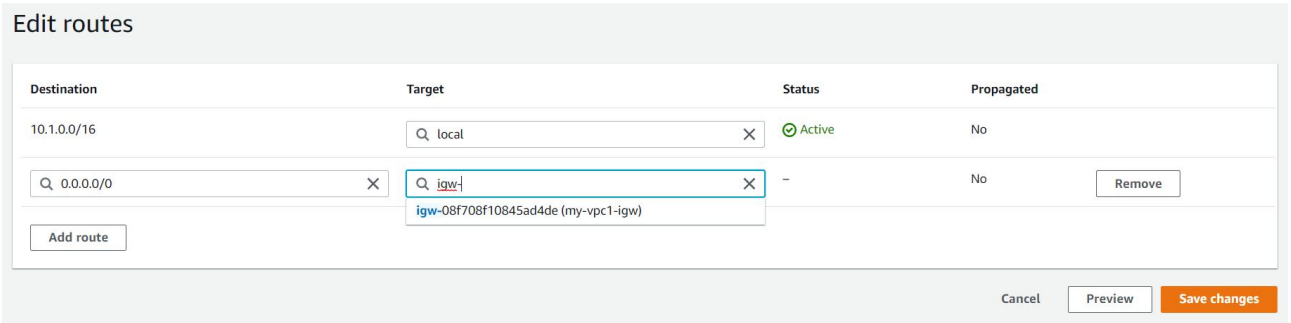


Now make sure the route table associated with your VPC is selected. Below click the R**outes** option as shown in the orange colour in the following image.

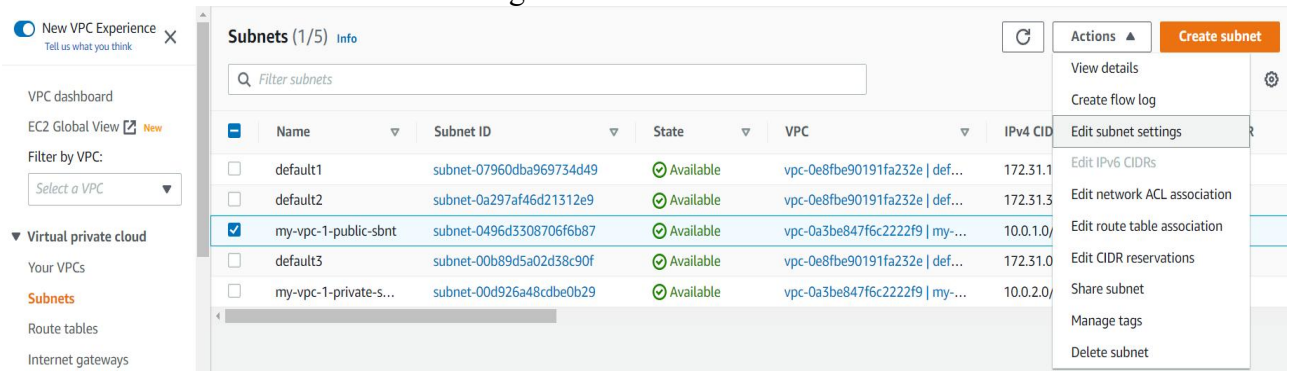


Then click Edit Routes button , in the right bottom of the screen.

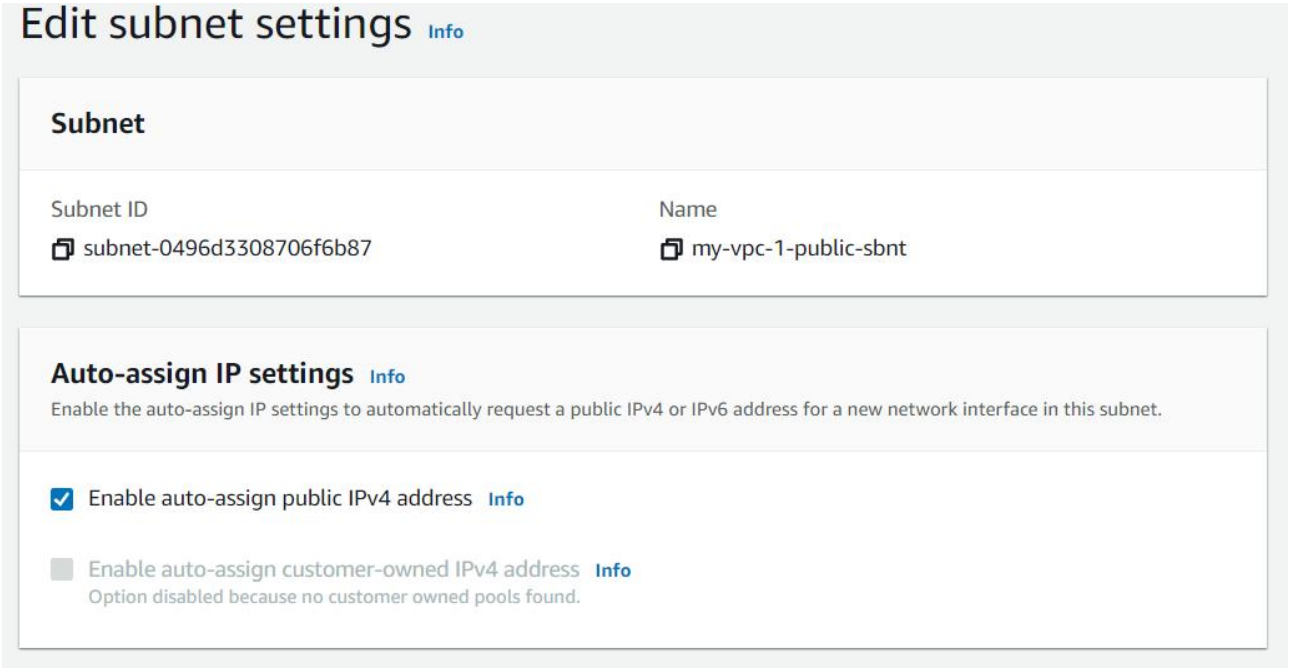
In the Edit Routes window that opens, click Add Route button. In the new route option that is shown select 0.0.0.0/0 in the destination field. Then below target click and select Internet Gateway option. This will display the Internet Gateway name as shown below. Select it. Then Click Save Changes.



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.



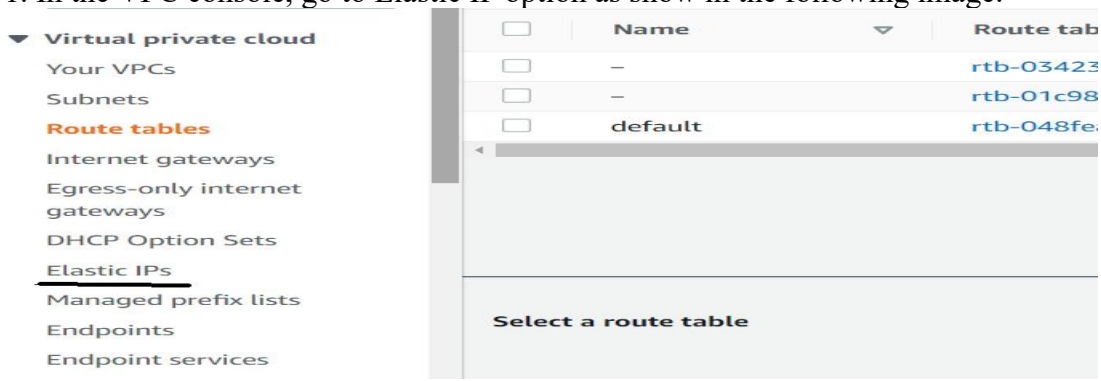
Then click Save.

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.

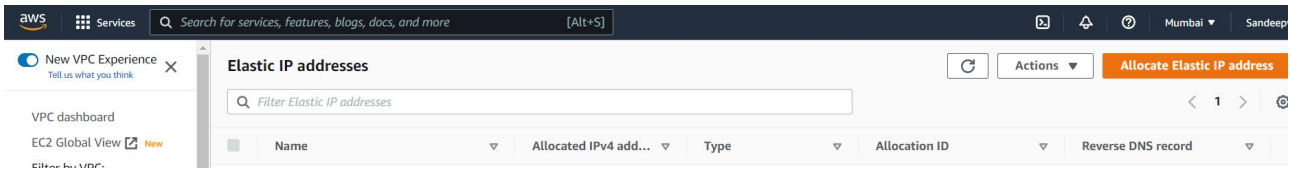
Following steps will have charges applied. The NAT gateway is not free. It has per hour charges of around $0.045/hr. However it may change so confirm before using it.

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

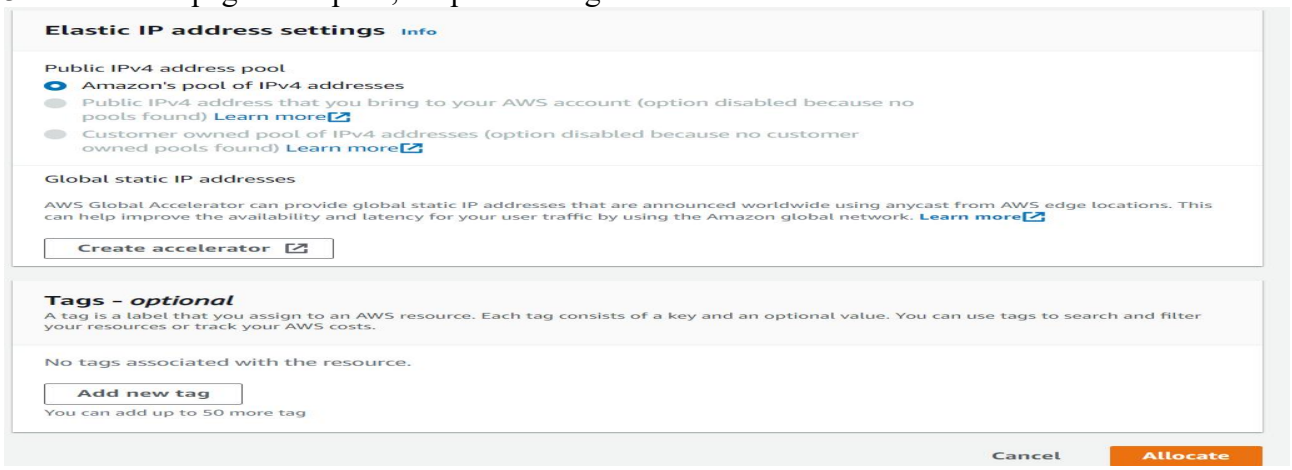
1. In the VPC console, go to Elastic IP option as show in the following image.



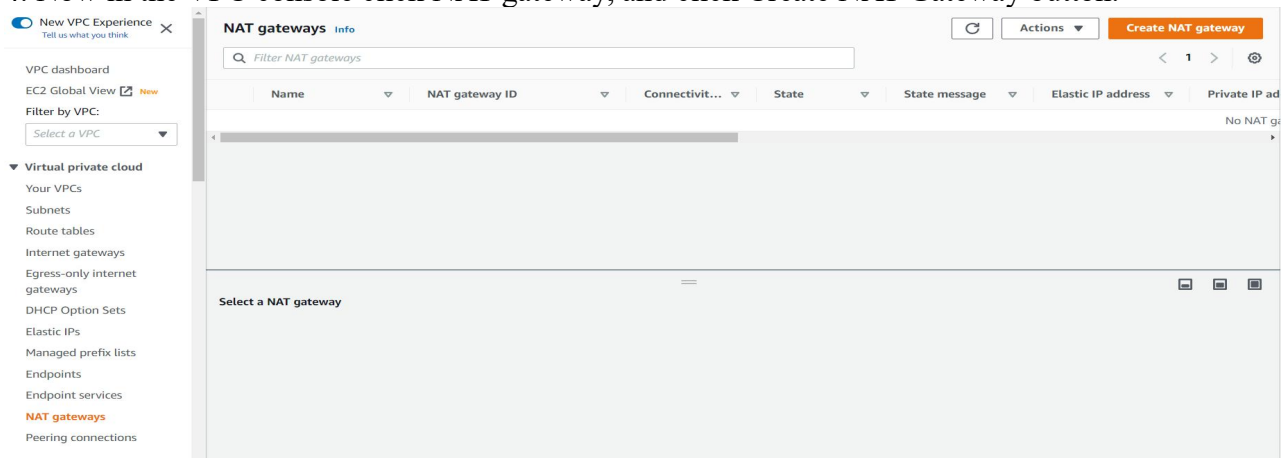
2. In the page that opens, click Allocate Elastic IP.



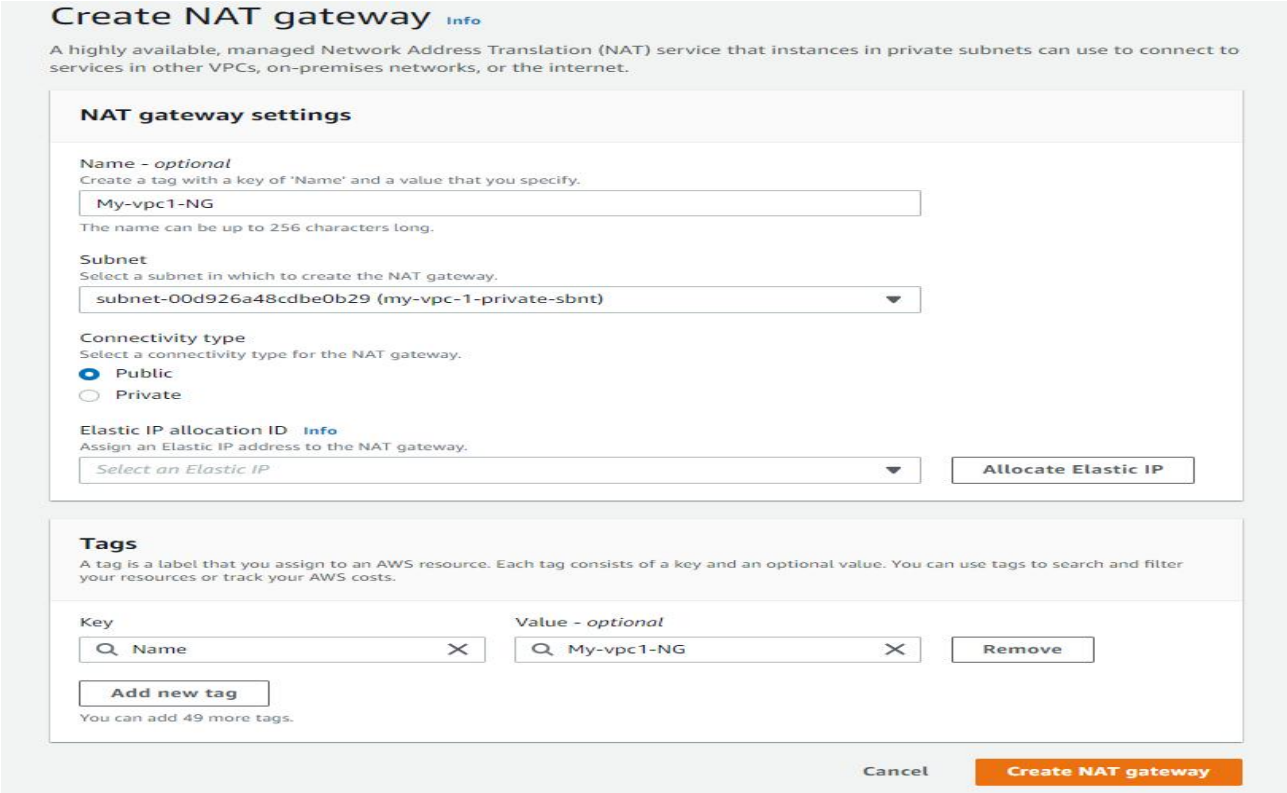
3. On the new page that opens, keep all settings as default and click allocate.



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.



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.