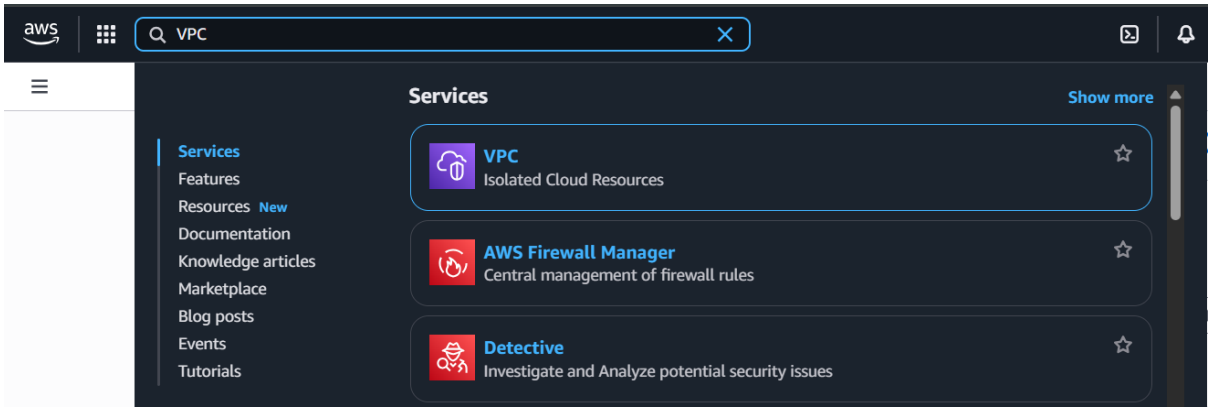
Day 24

“CLOUD SECURITY”

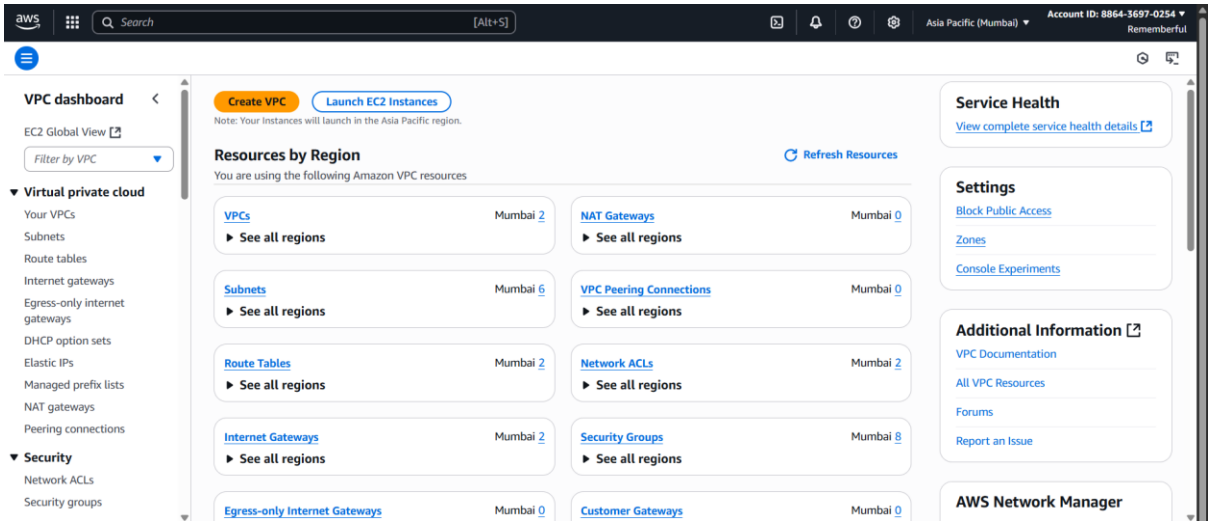
Creating secure EC2 Instances in AWS Virtual Private Cloud (VPC):

Steps:

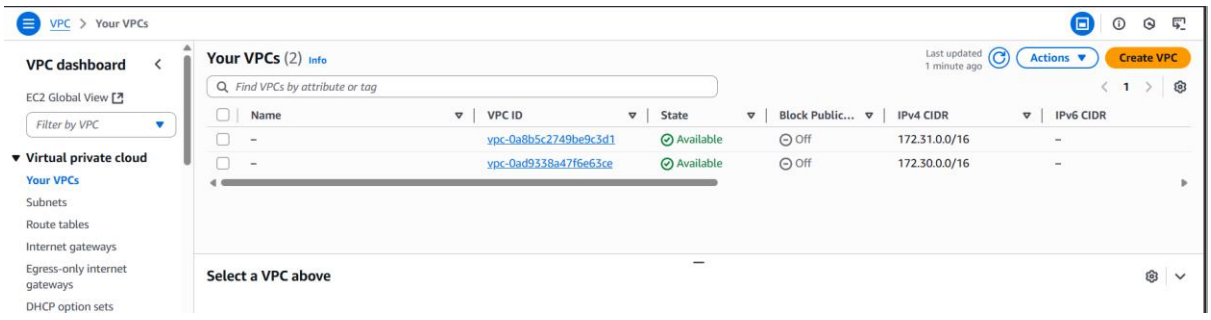
To create the VPC, first open the VPC:



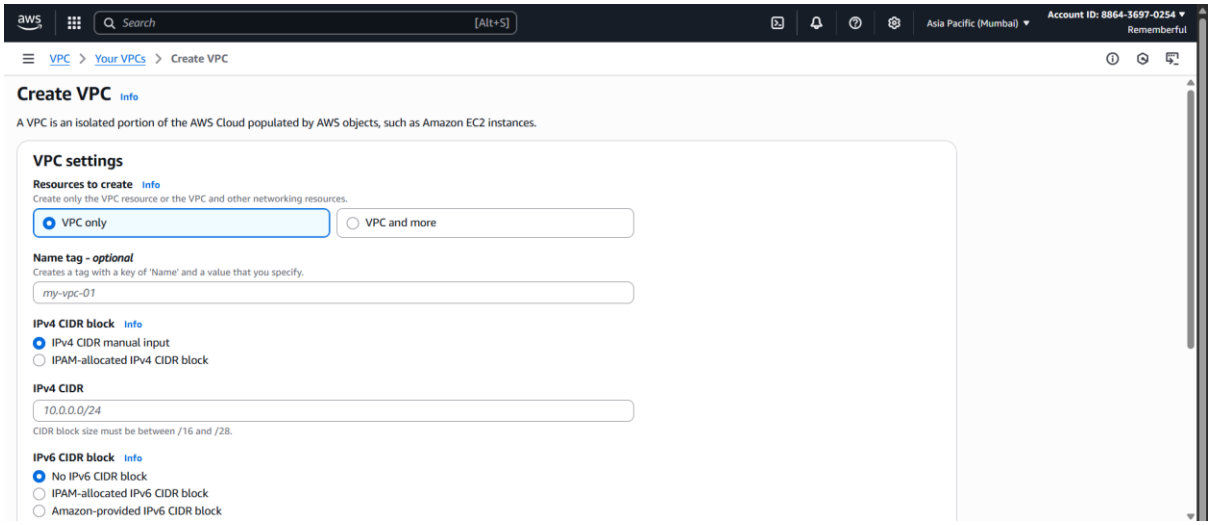
Following window will appear:



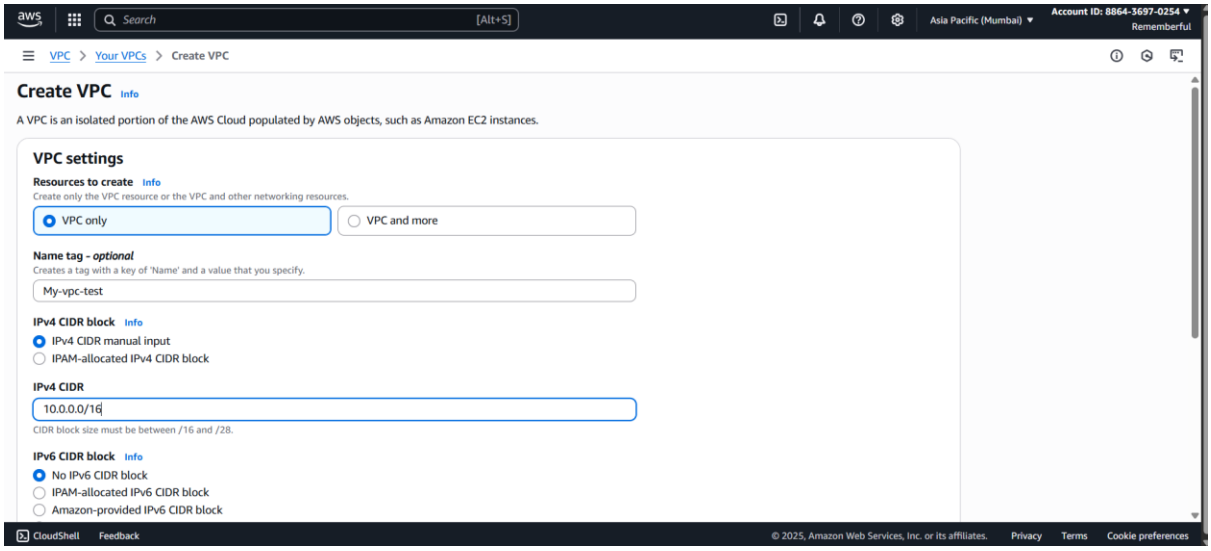
Under the “Your VPC” section: click on “Create VPC” button



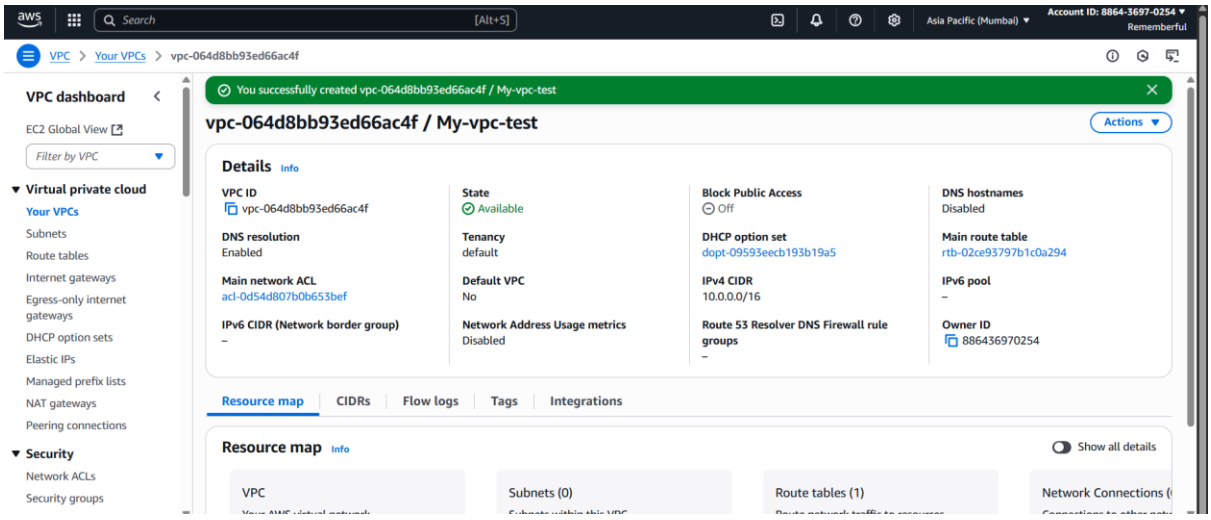
Following screen will appear:



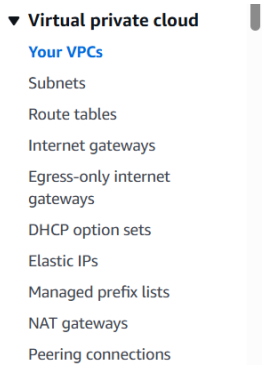
Fill the name, CIDR, don't change any other settings: then click on the "Create VPC" button.



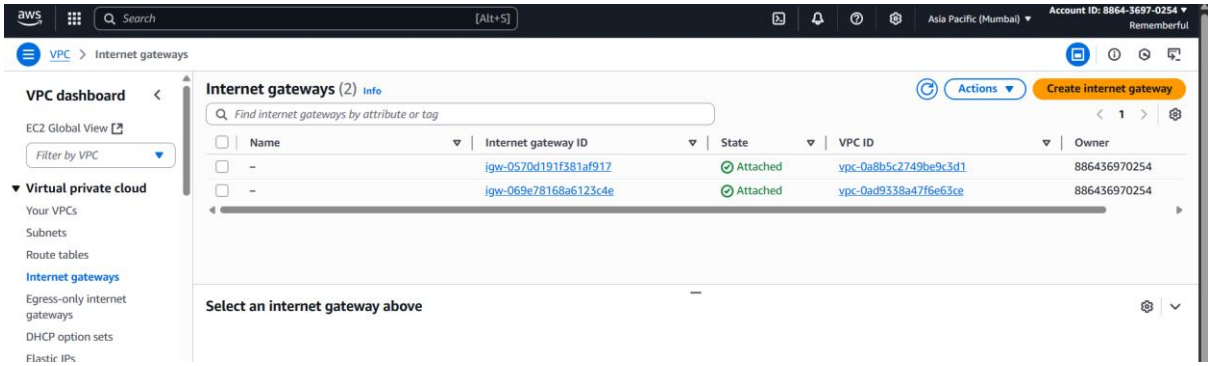
Following confirmation will occurs:



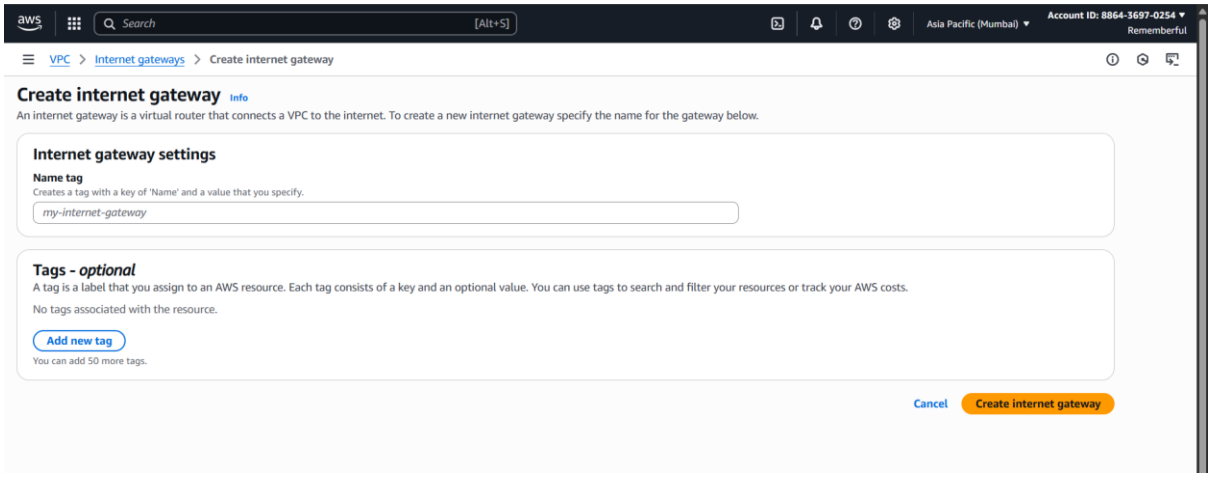
Now, we need to create an Internet Gateway:



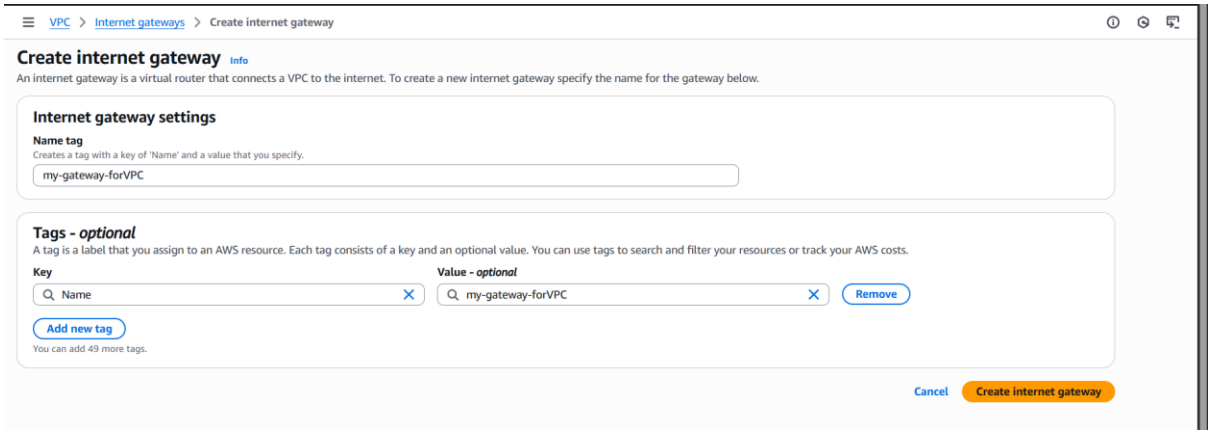
Following screen will appear:



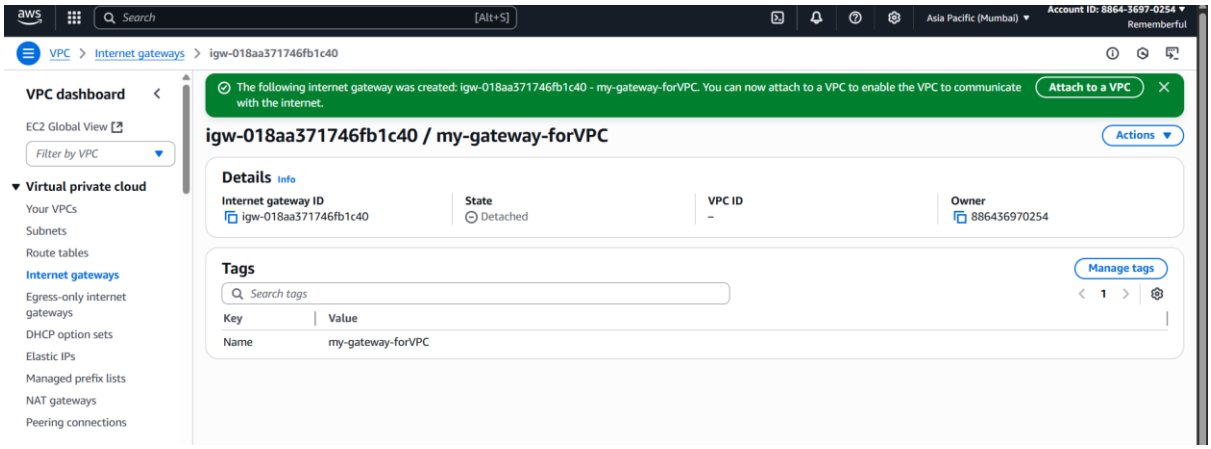
Click on the “Create Internet Gateway” Button: following screen will appear.



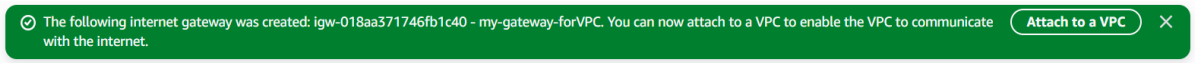
Fill it and rest of the things be default, and then click on “Create Internet Gateway” button:



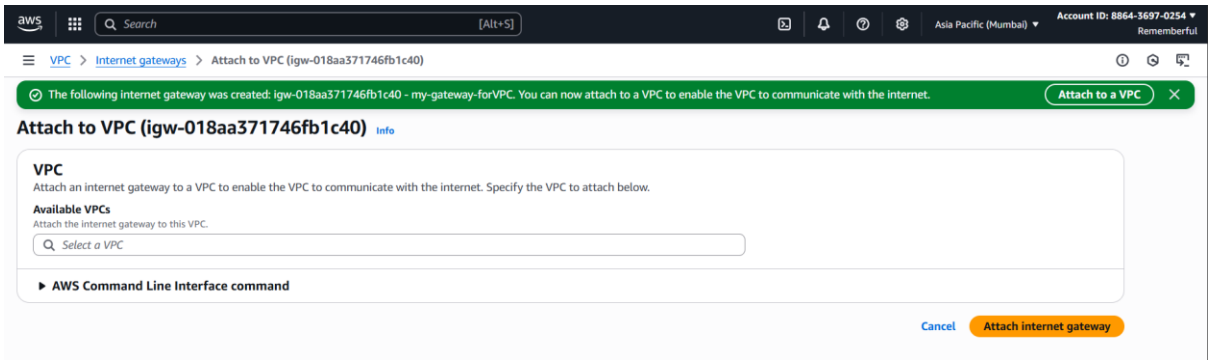
Following confirmation will show:



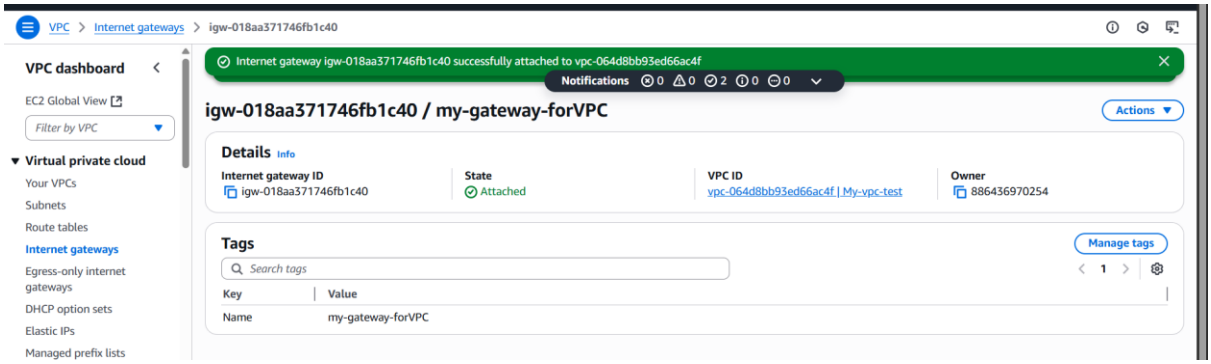
At the green confirmation, click on the “Attach to a VPC” button:



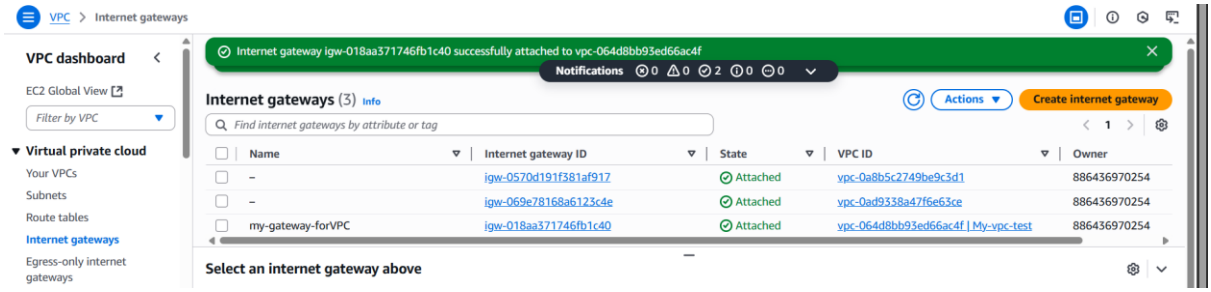
Following window will appear:



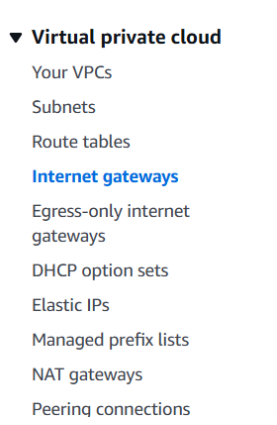
Select the required VPC: and then click on “Attach Internet Gateway” button, following confirmation will occur.



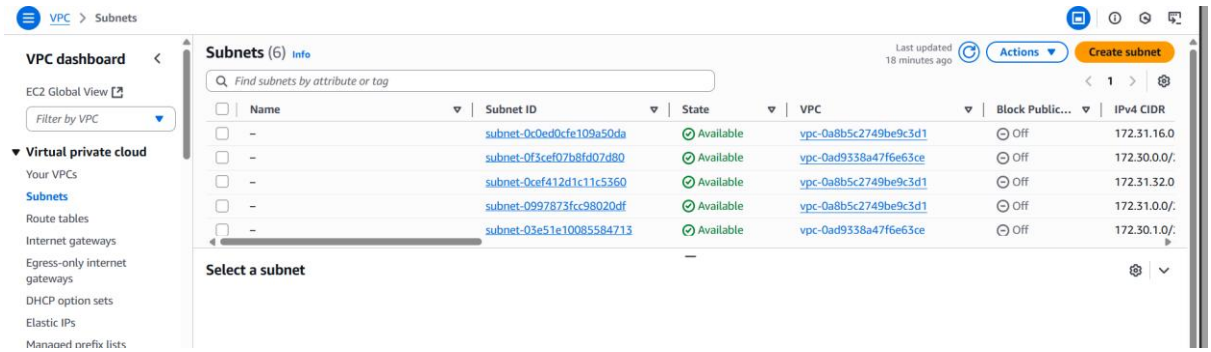
Make sure that it shows “attached”:



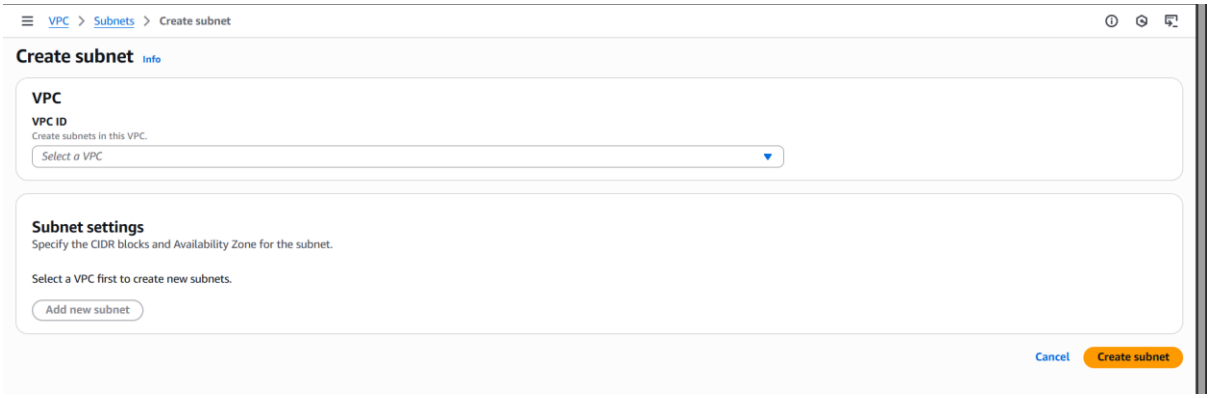
Next, we need to create private and public subnet in the VPC, to do so click on the “subnet” option available on the left menu:



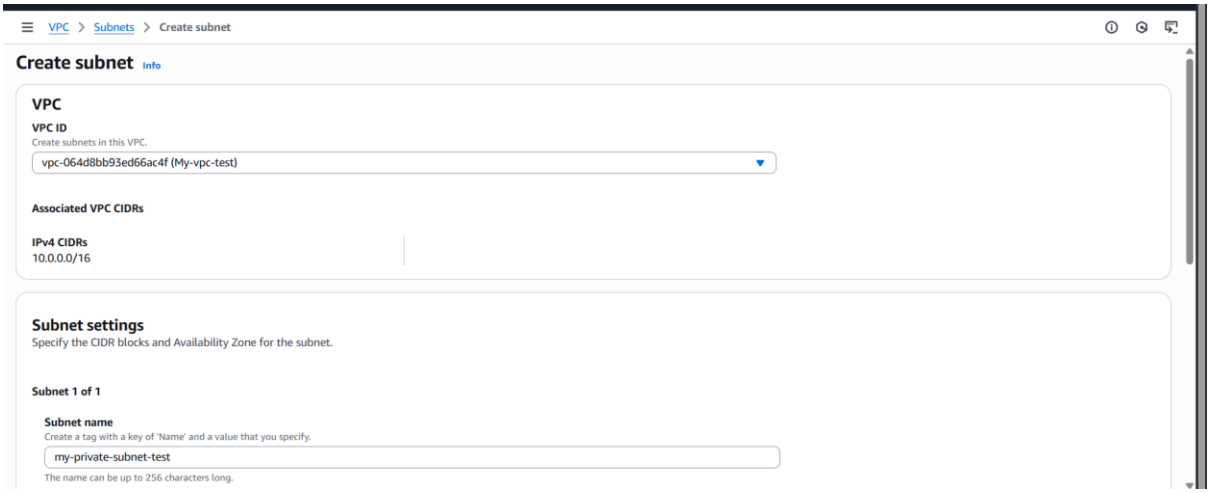
Following screen will appear:



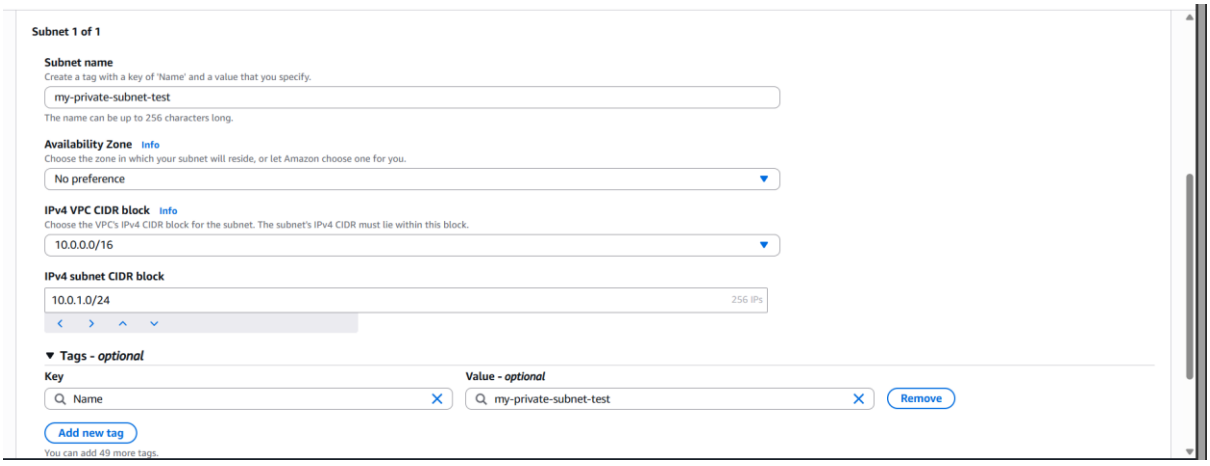
First, we will create a private subnet: click on the “Create subnet” button, following screen will appear.



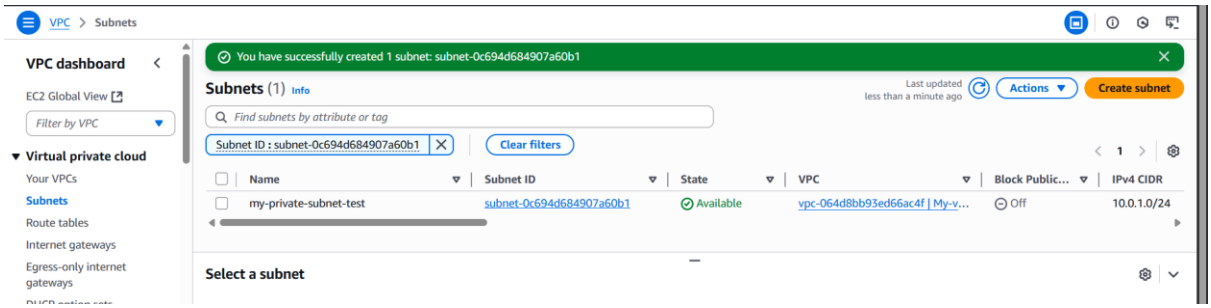
Select the VPC ID, and assign the name:



Scroll down and make sure to write the “IPV4 subnet CIDR block”:

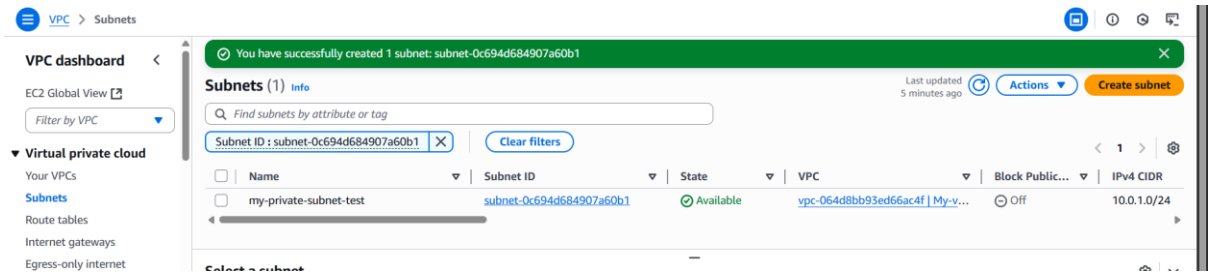


Leave rest of the settings as it is, and then click on the “create subnet” button: following confirmation will occur.

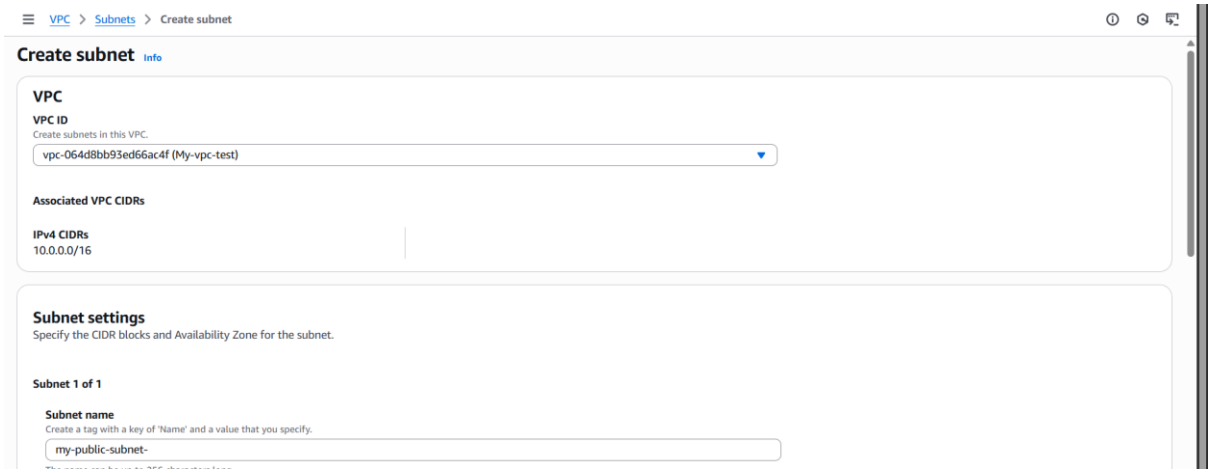


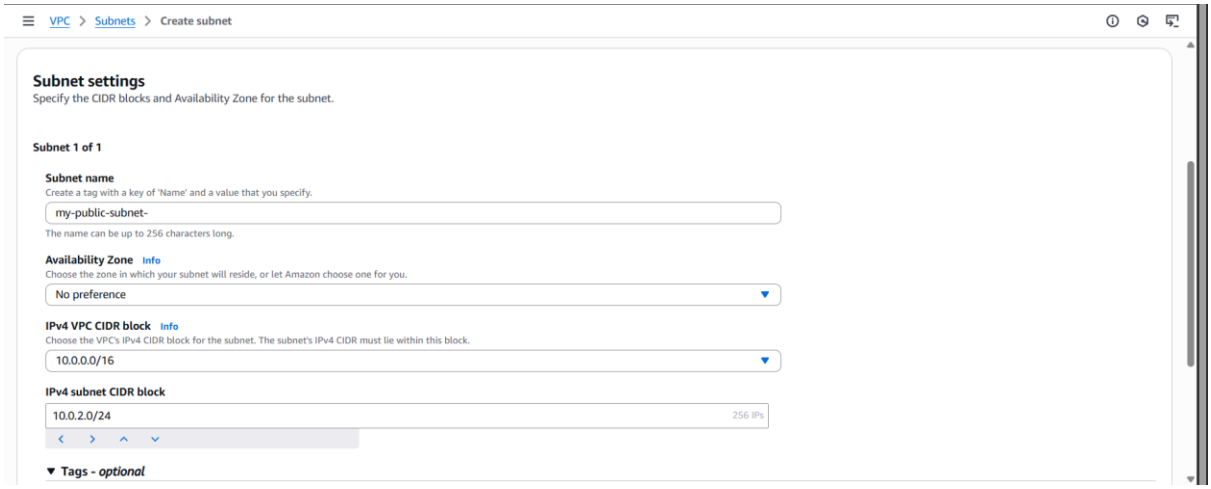
So a private subnet is created, now we need to create a public subnet.

For this, again click on the “Create subnet” button:

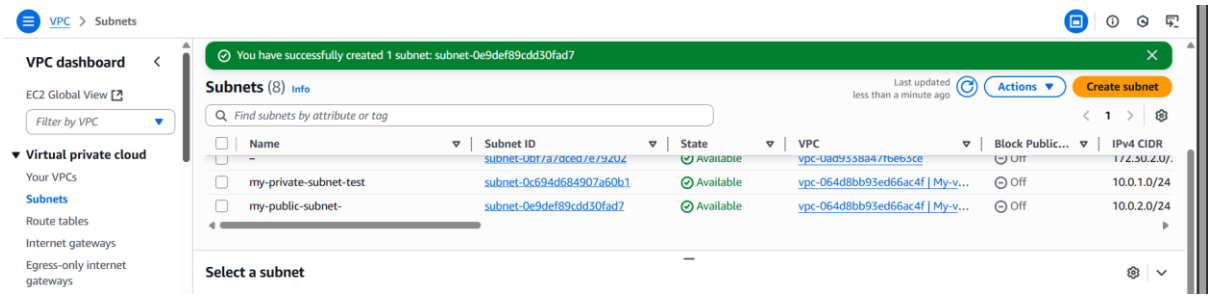


Again, do the same process we did above, just make sure to specify the different subnet block.



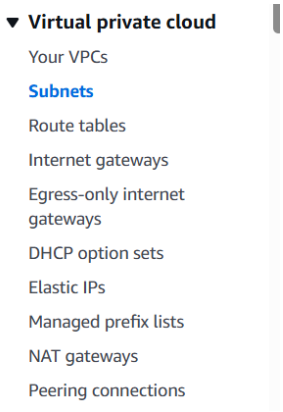


Click on the “create subnet” button, following confirmation will occur.

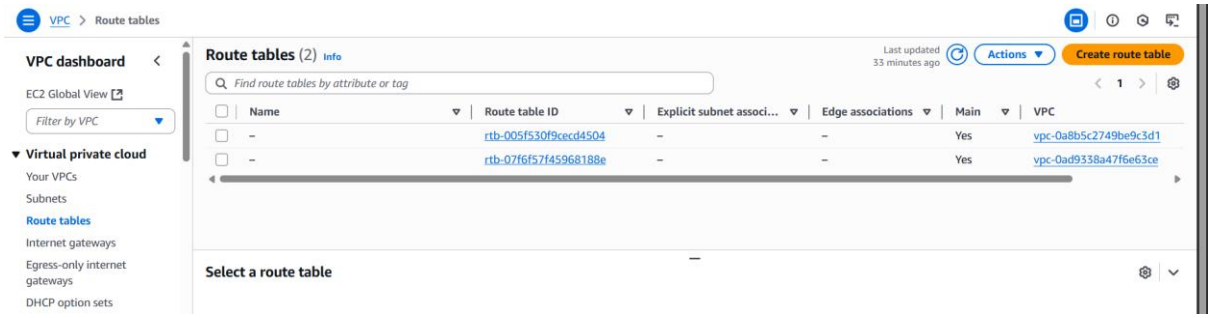


Thus, we have two subnets for private and public access.

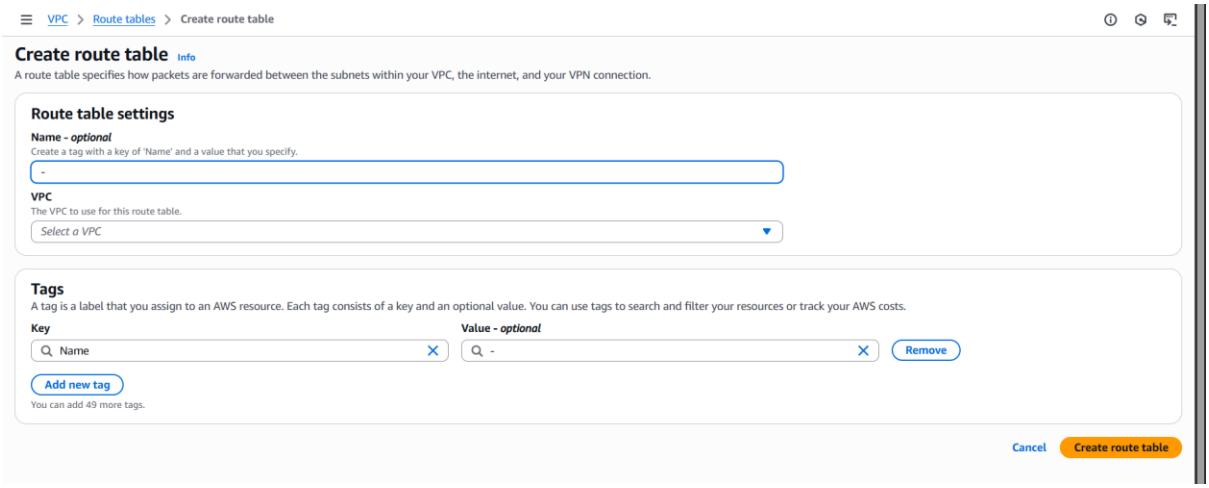
Next, we will create the route tables to route the network traffic: where to find this route table?



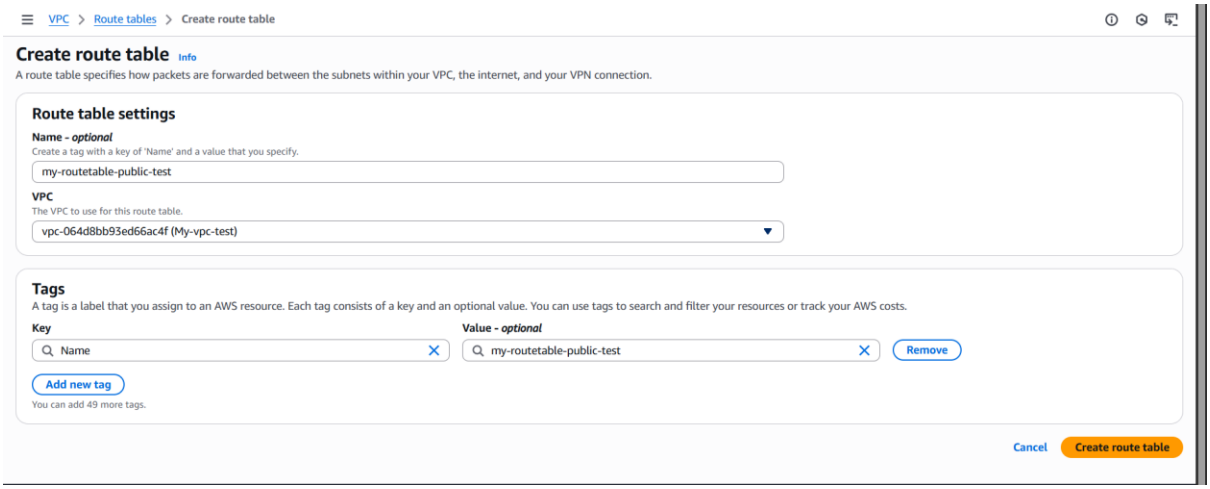
Following screen will appear:



To create a route table for the public subnet, click on the “Create route table” button: following screen will appear.

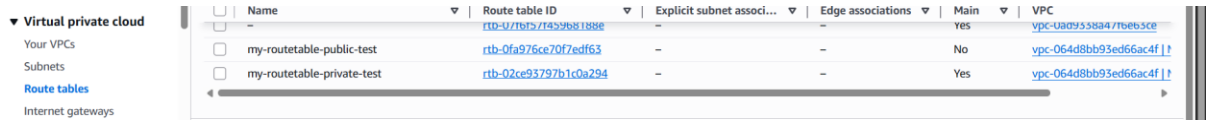


Fill the details and then click on the orange button:



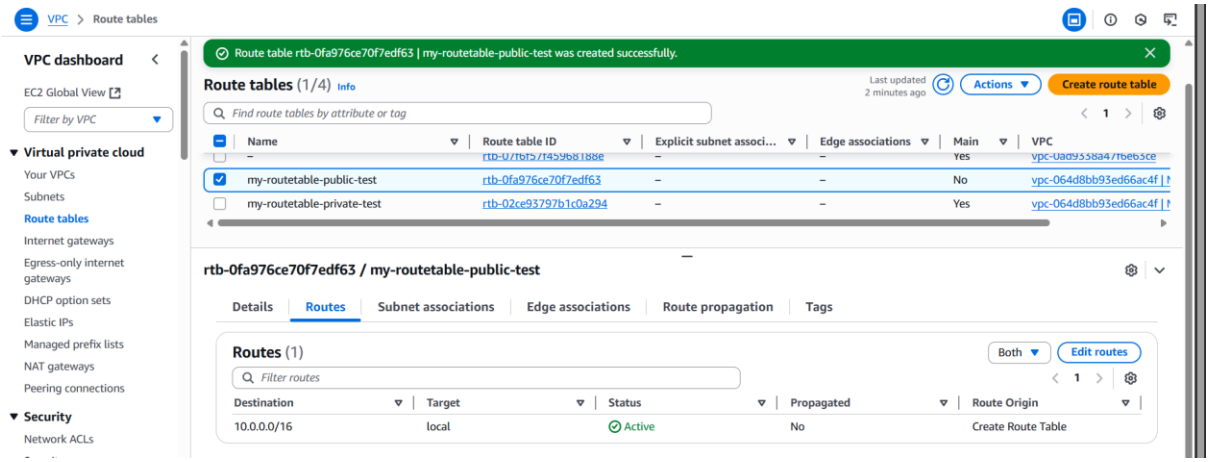
Following confirmation will occur:

Go back to the section of “Route Tables”, make sure to edit the name of default route table created or the VPC to identify the private route table:

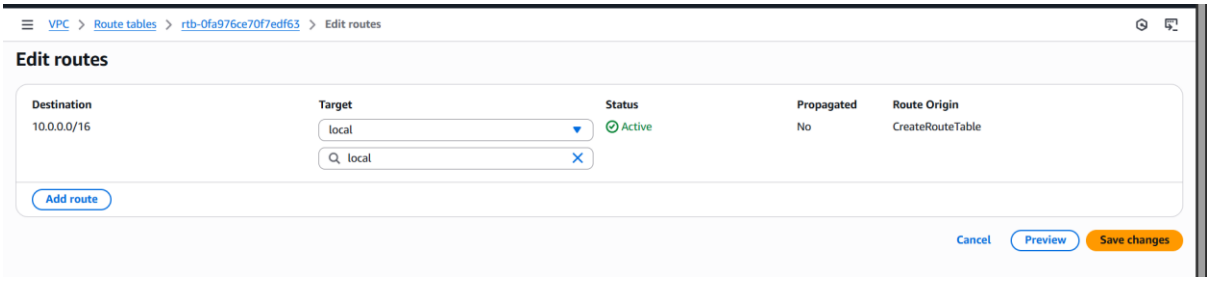


Now, we will configure the public route table as public and add the public subnet and internet gateway.

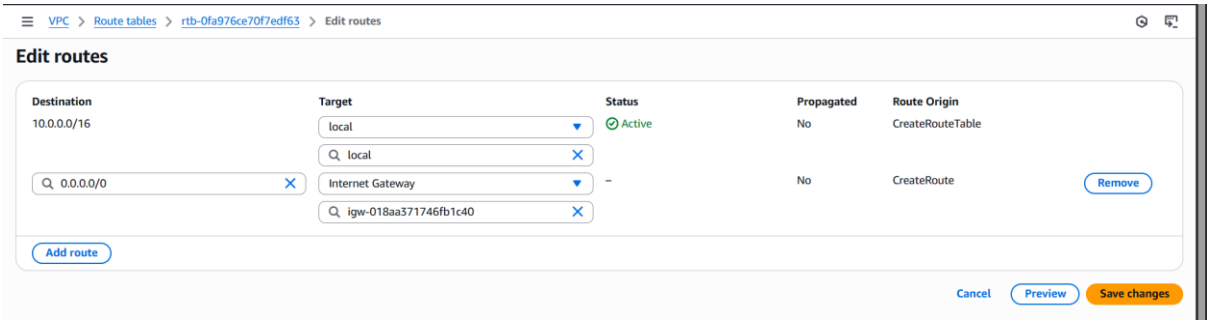
Click on the public route table: and click on the “routes” section.



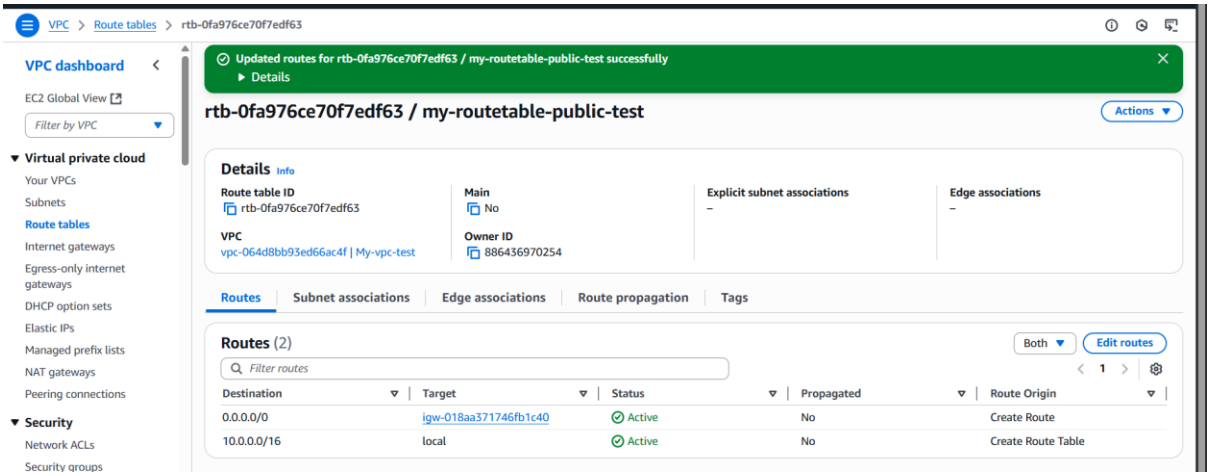
Click on the “Edit Routes” button: following screen will appear



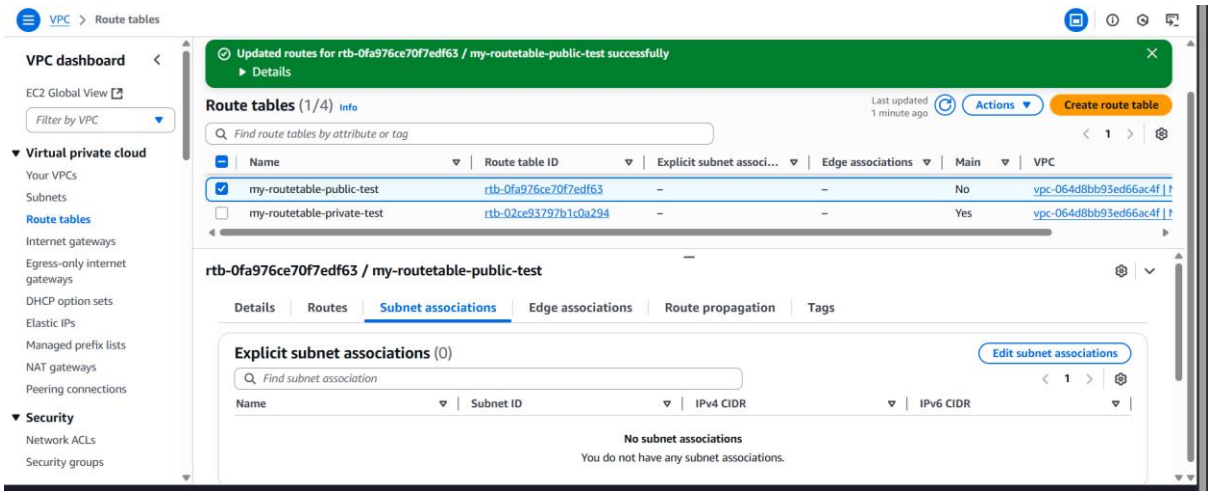
Click on “add route” button to add the IP: write 0.0.0.0/0 for allowing traffic from any source, and then select the Internet gateway option from the target section.



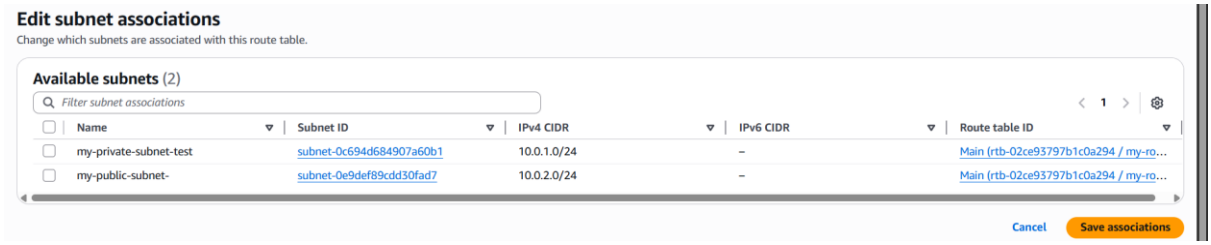
Click on “save changes” button: following confirmation will occur.



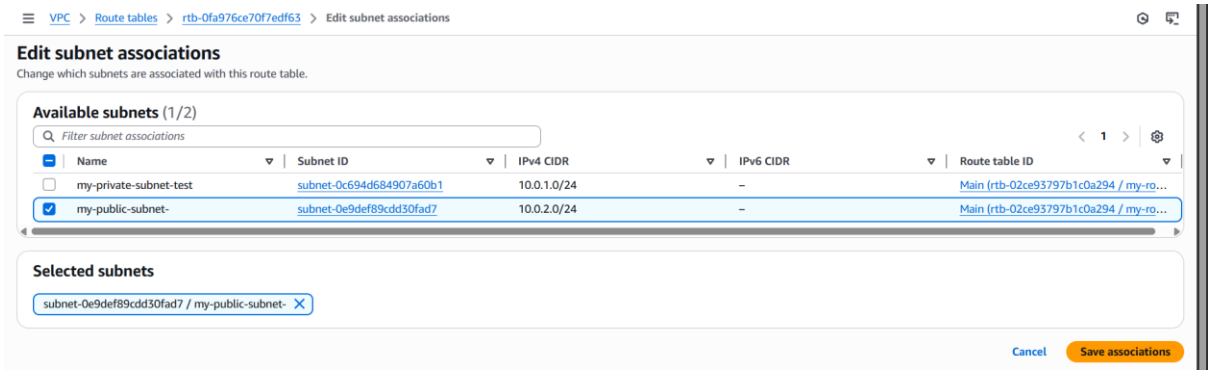
Now, again select the public route table and then go to the “Subnet association” section:



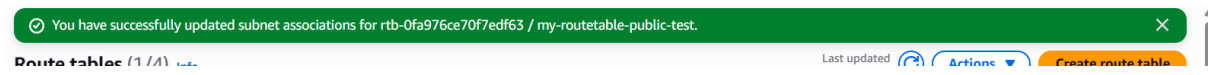
Click on the “Edit subnet association” button: following window will appear



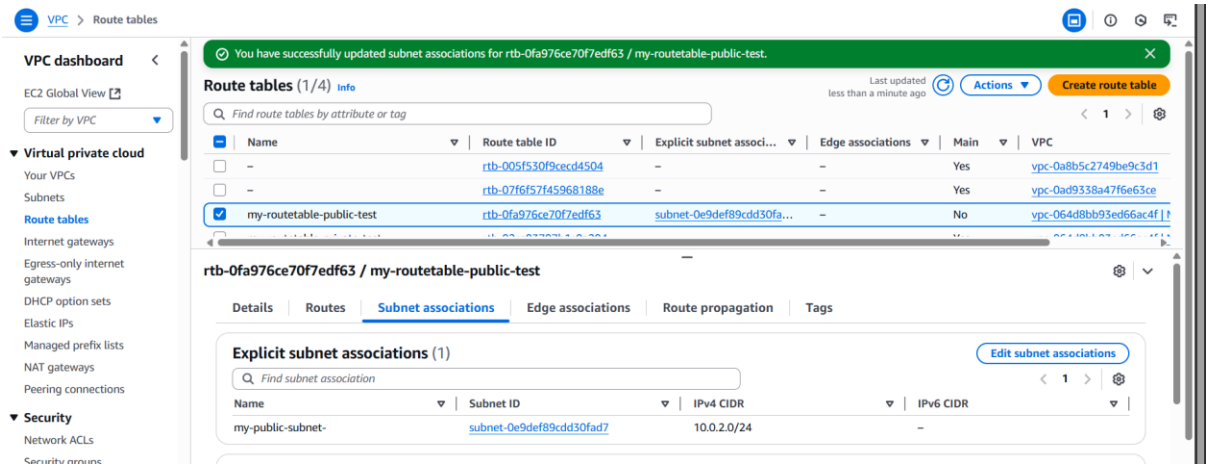
Select the subnet for public association:



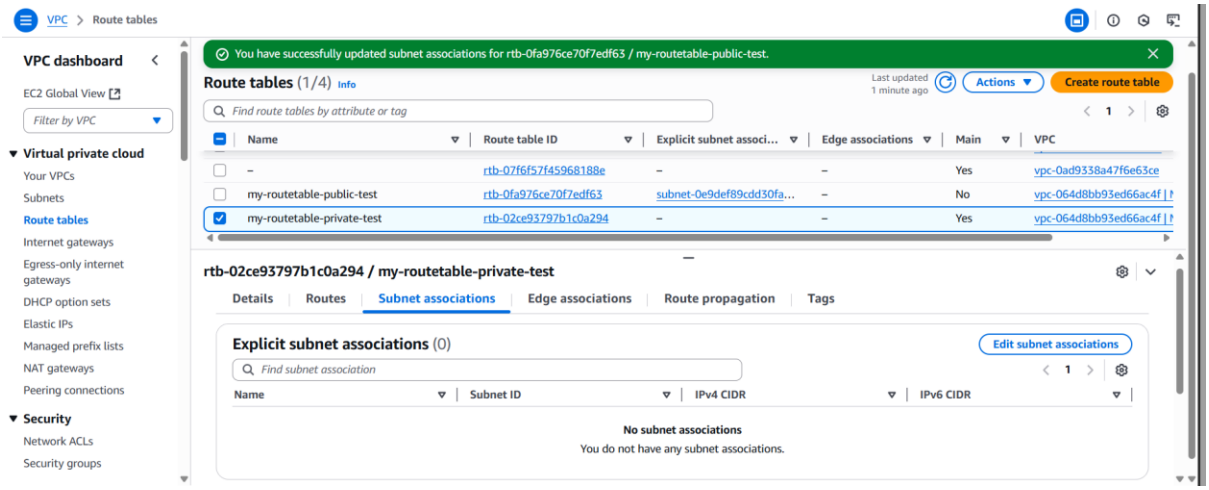
Click on the “Save association” button: following confirmation will occur.



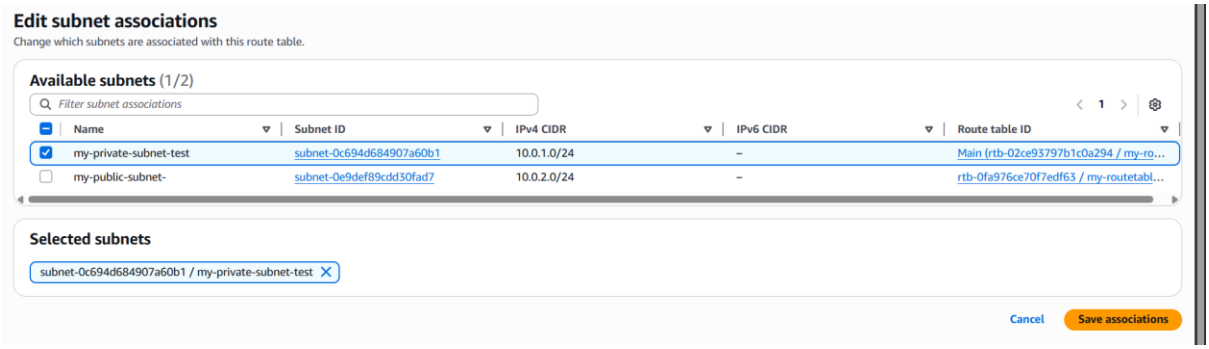
Clearly the association is added successfully:



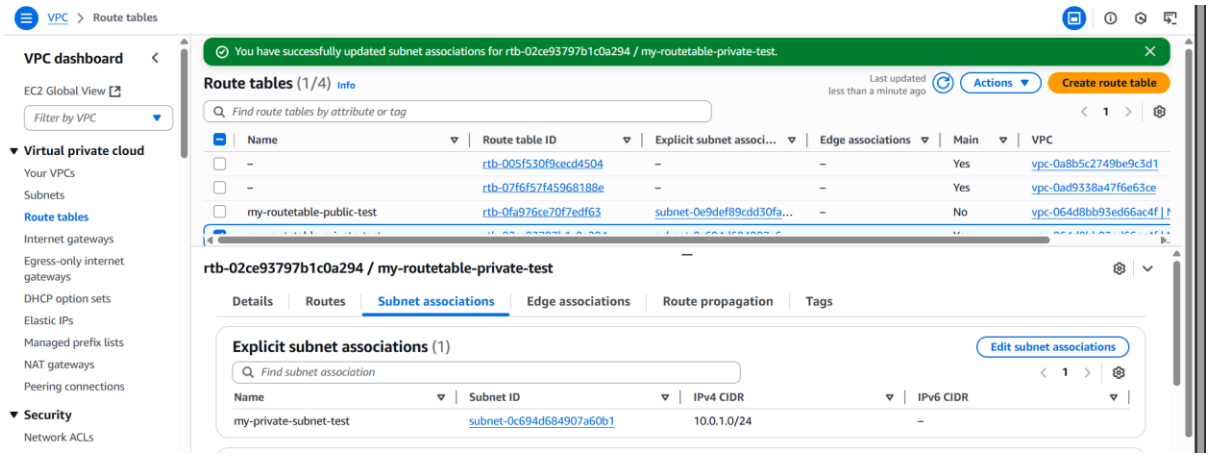
Now, we will add the subnet for the private route table:



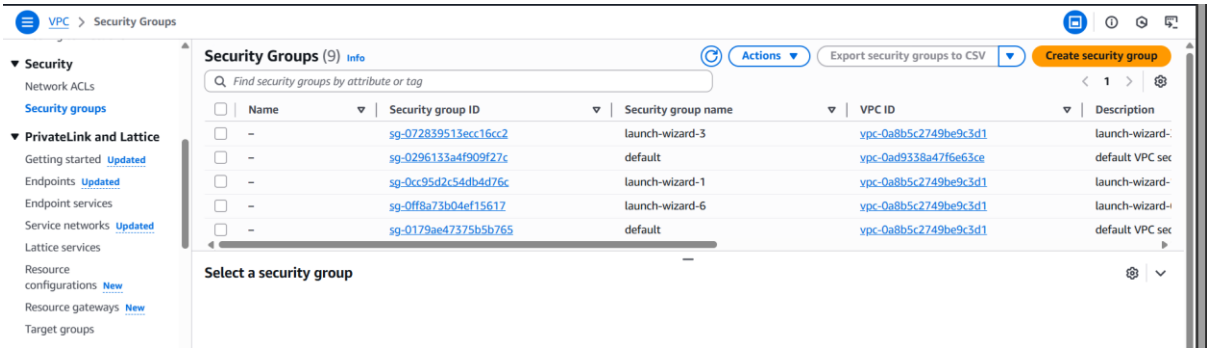
Then,



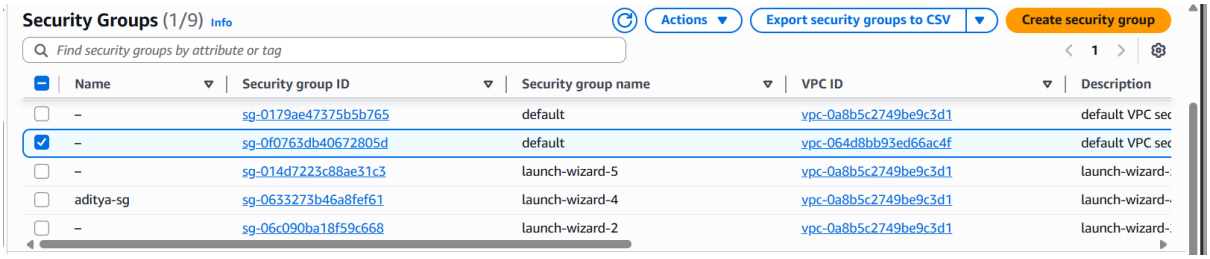
Following confirmation will occur:



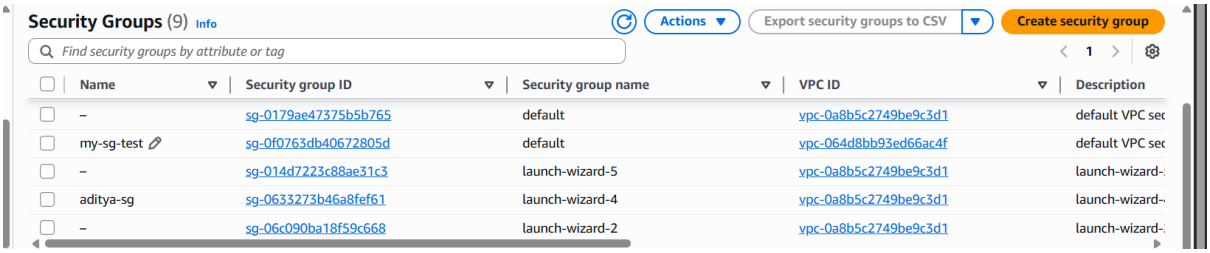
Now, we will configure the traffic from the internet, using the “Security Groups” section: following window will occur.



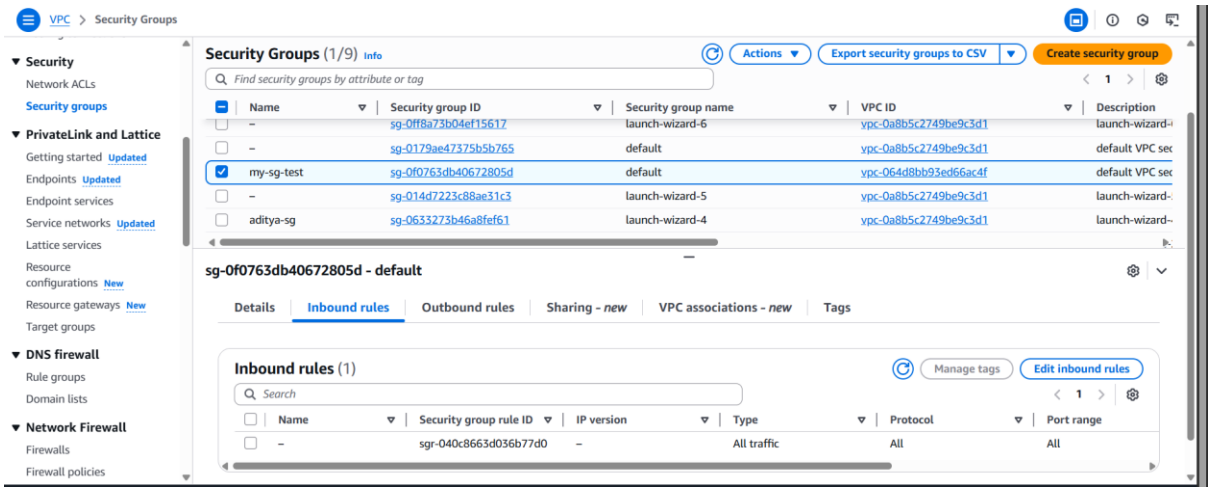
We can actually see the default security group created for our VPC:



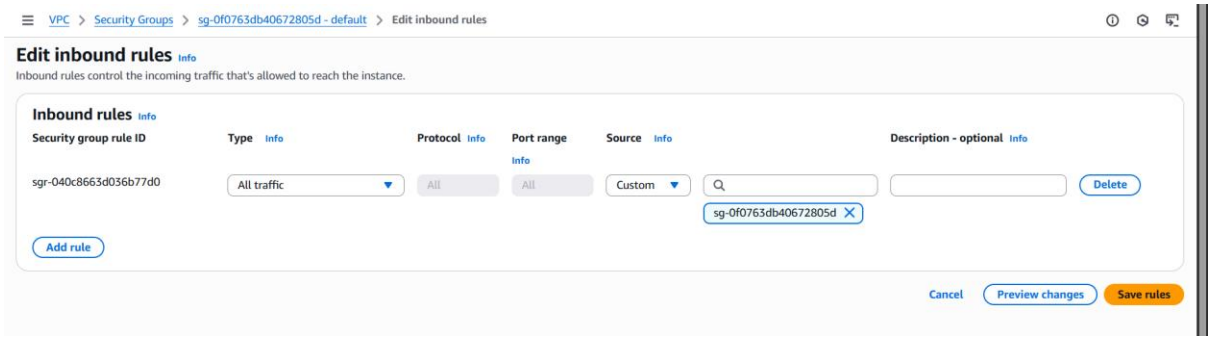
Edit its name:



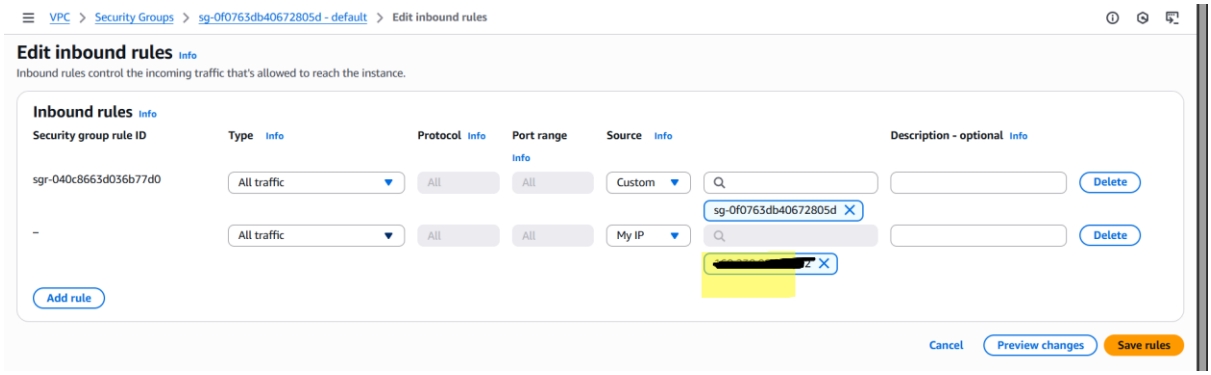
Now, we will configure the inbound traffic for that security group:



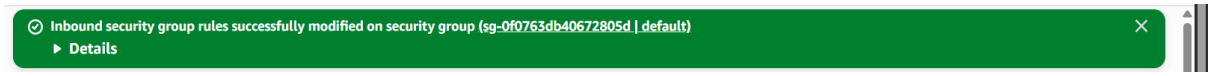
Click on the “Edit Inbound rules” button: following screen will appear.



Click on “add rule” button, and select the type as “All traffic” , and in source “My IP” to make sure only your IP can access.

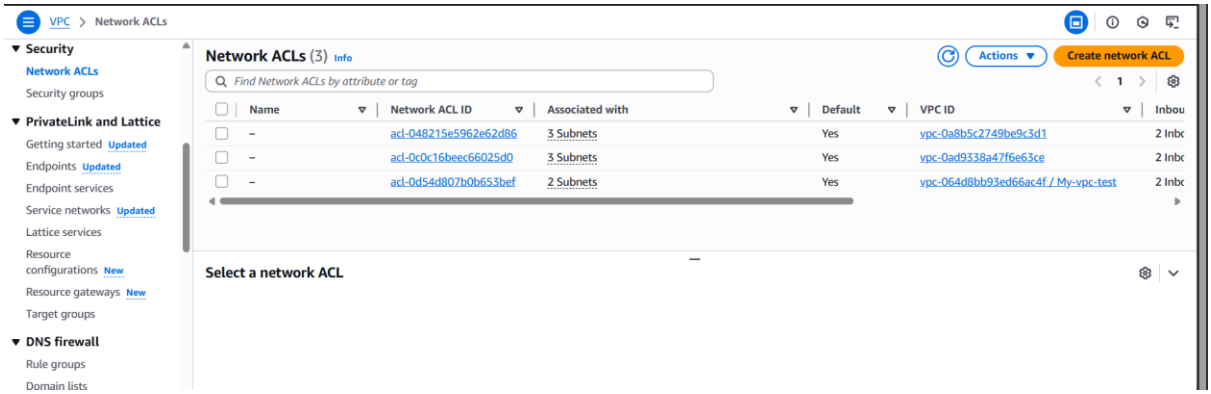


Then click on the “save rules” button: following confirmation will occur.

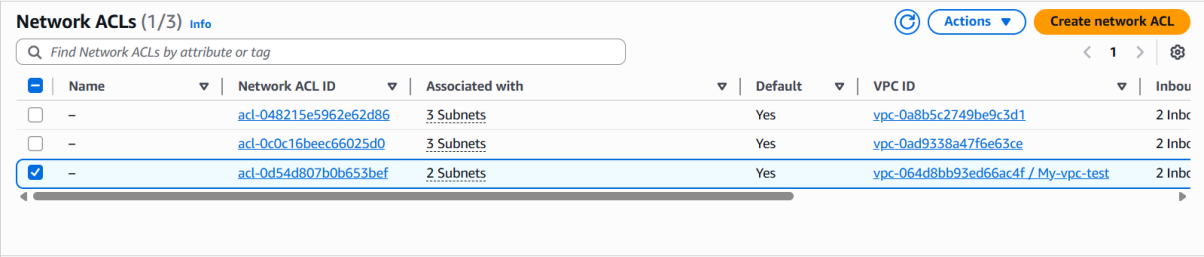


So, inbound rules is set for the Security groups.

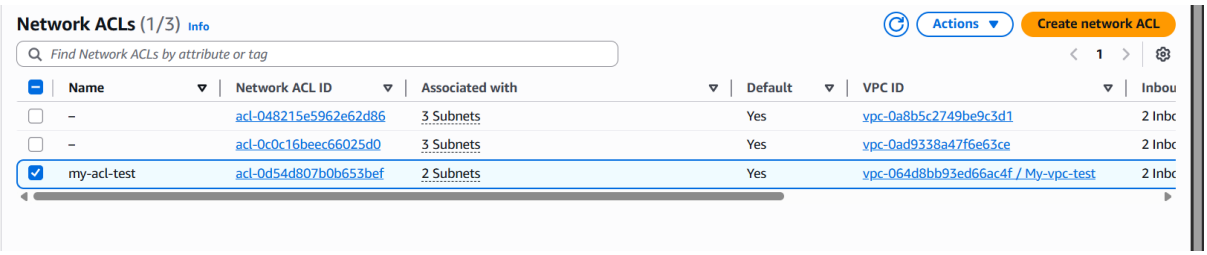
Now, open the ACL:



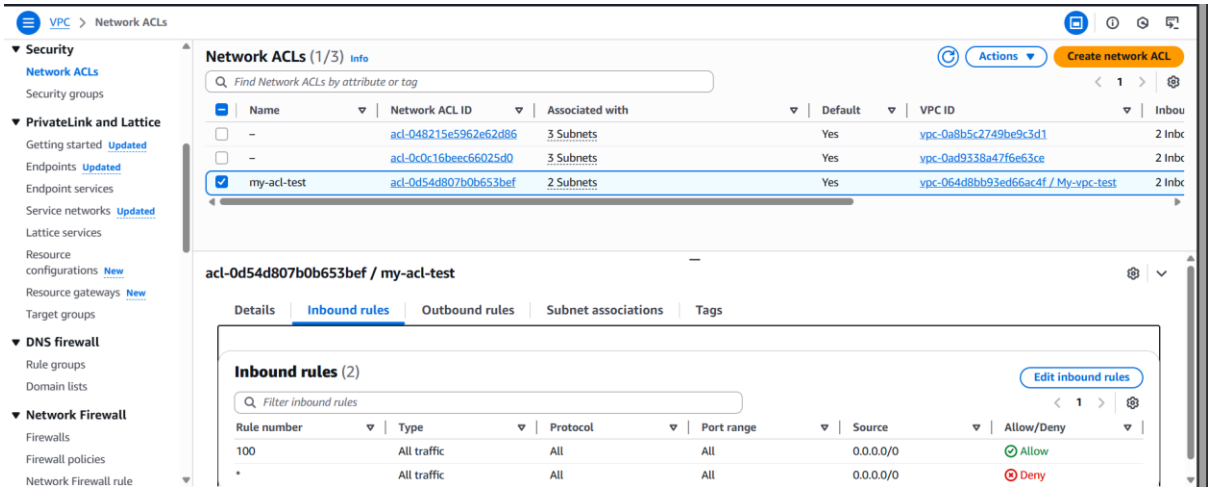
Identify the default Network ACL:



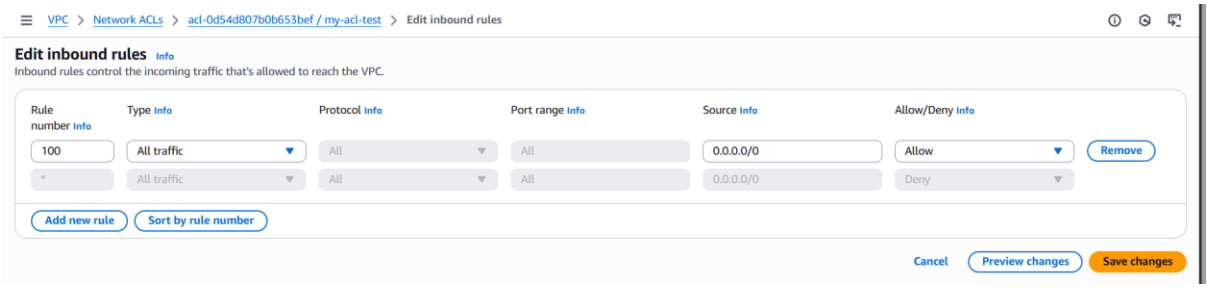
Change its name:



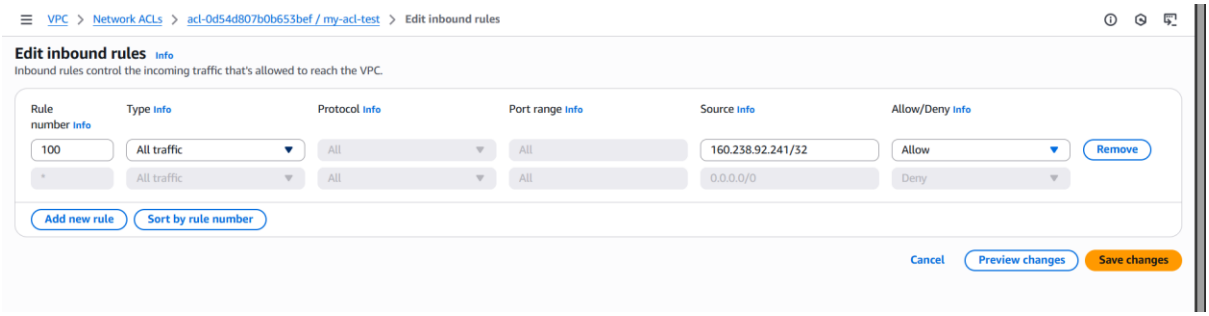
Next, click on the “Inbound rule” section: clearly all the traffic is allowed, but we need only traffic from our IP.



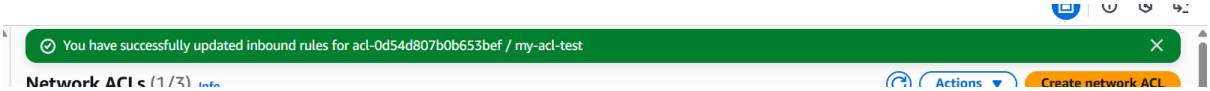
Click on the “Edit Inbound rules” button: following screen will appear.



Specify your IP, in the Source:

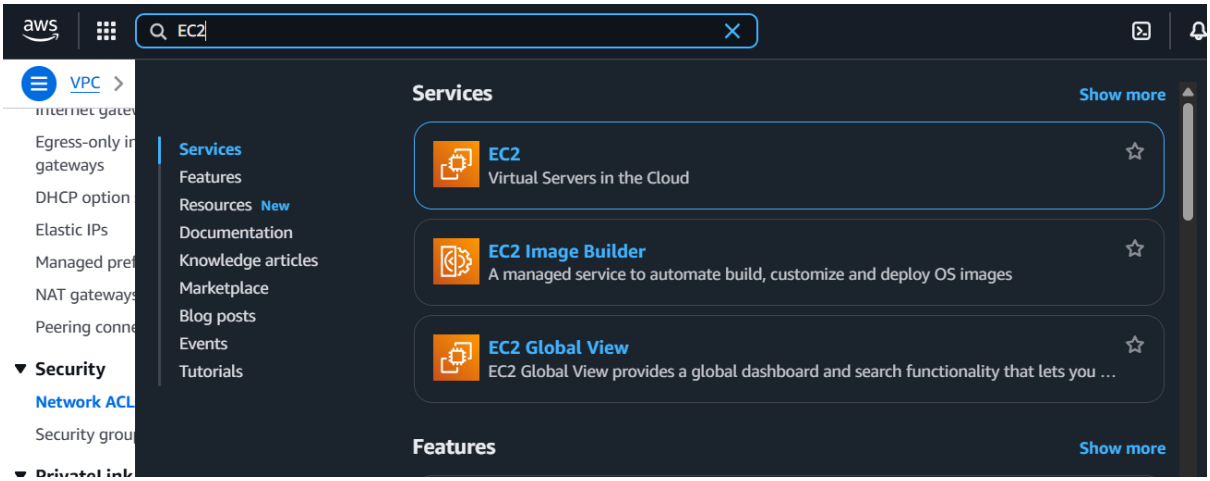


Click on the Save changes button: following confirmation will occur.

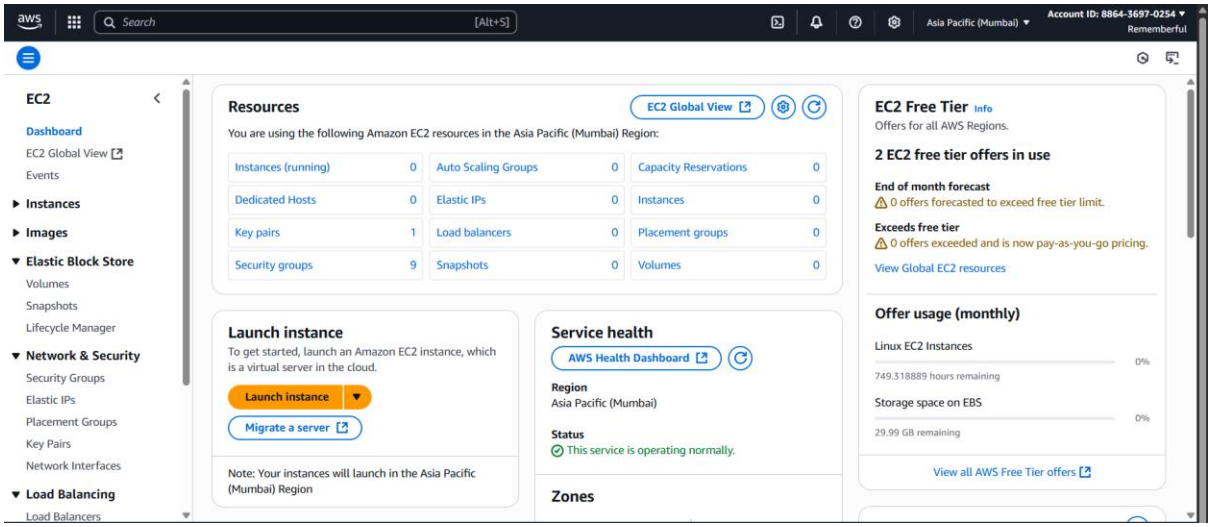


So, till now, ACL is also configured properly.

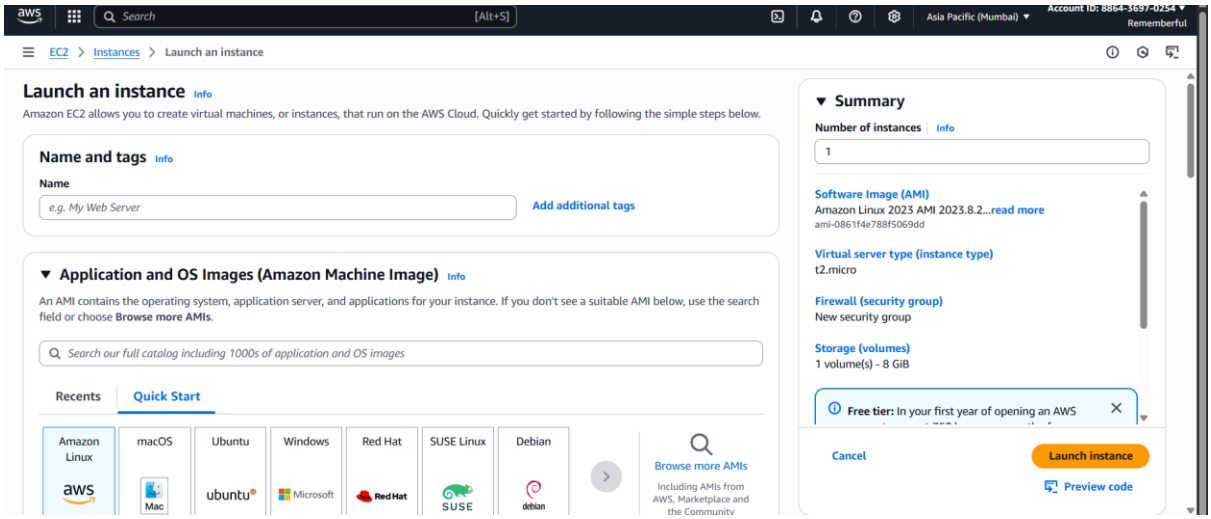
Now, we will move towards the EC2 Instance creation:



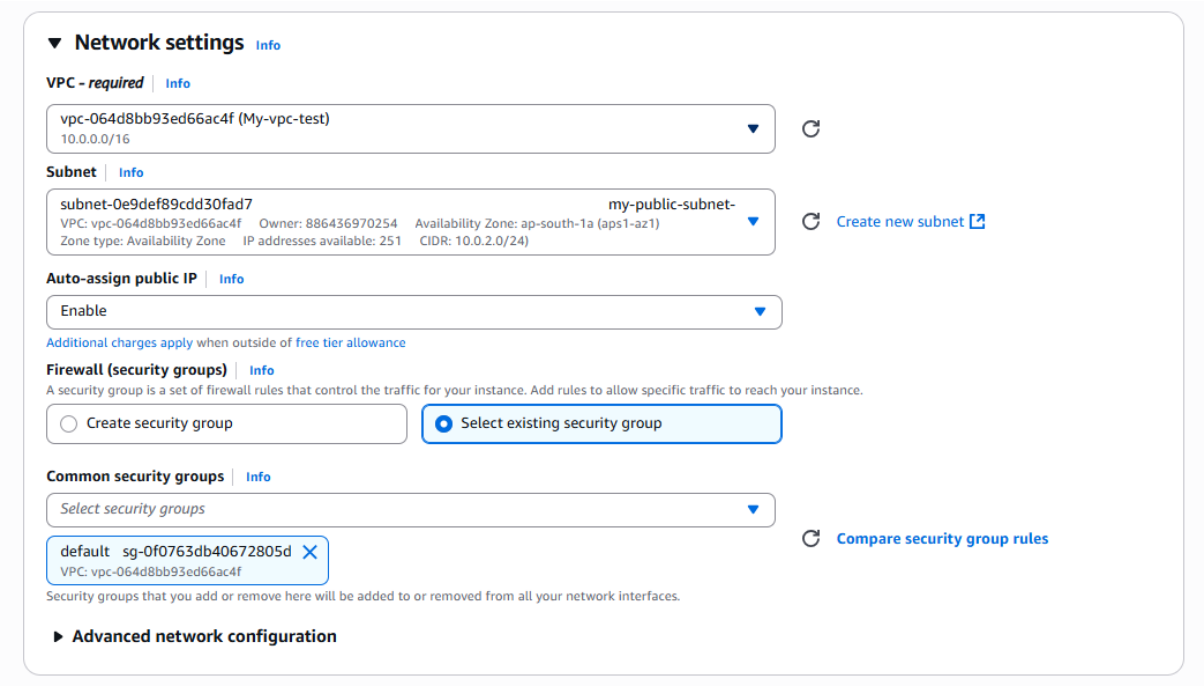
Following screen will appear:



Click on launch instance button: following screen appears.

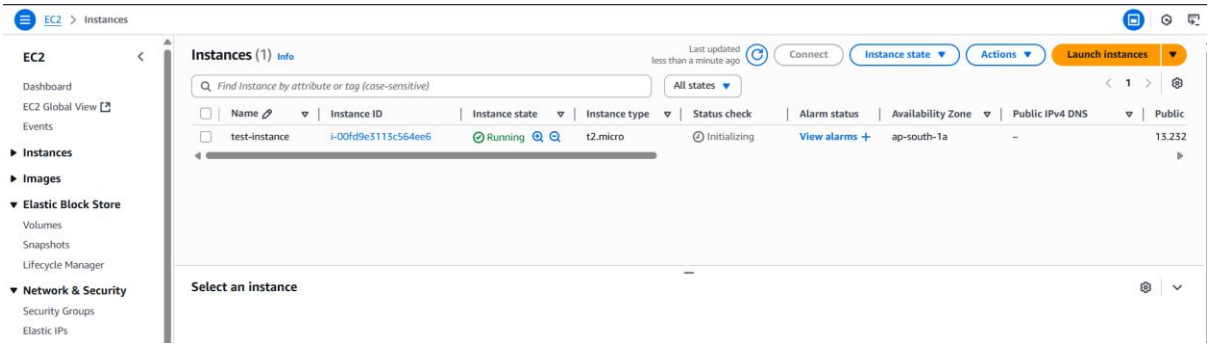


Scroll down, keep other things as it is, just make the following changes in the “network settings” section:

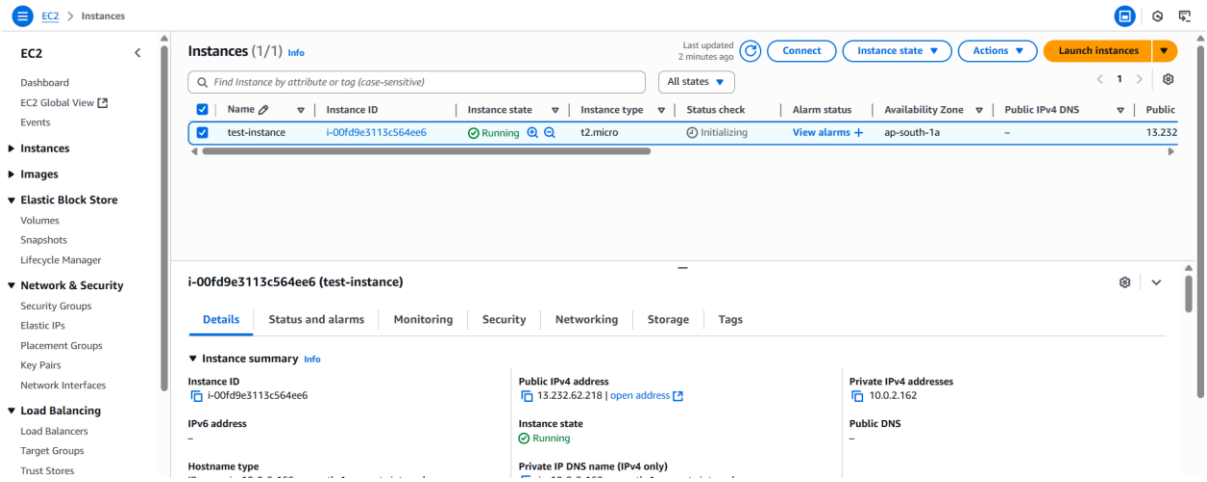


Click on “launch instance” button: following confirmation will occur.

We may recheck the status of the instance here:

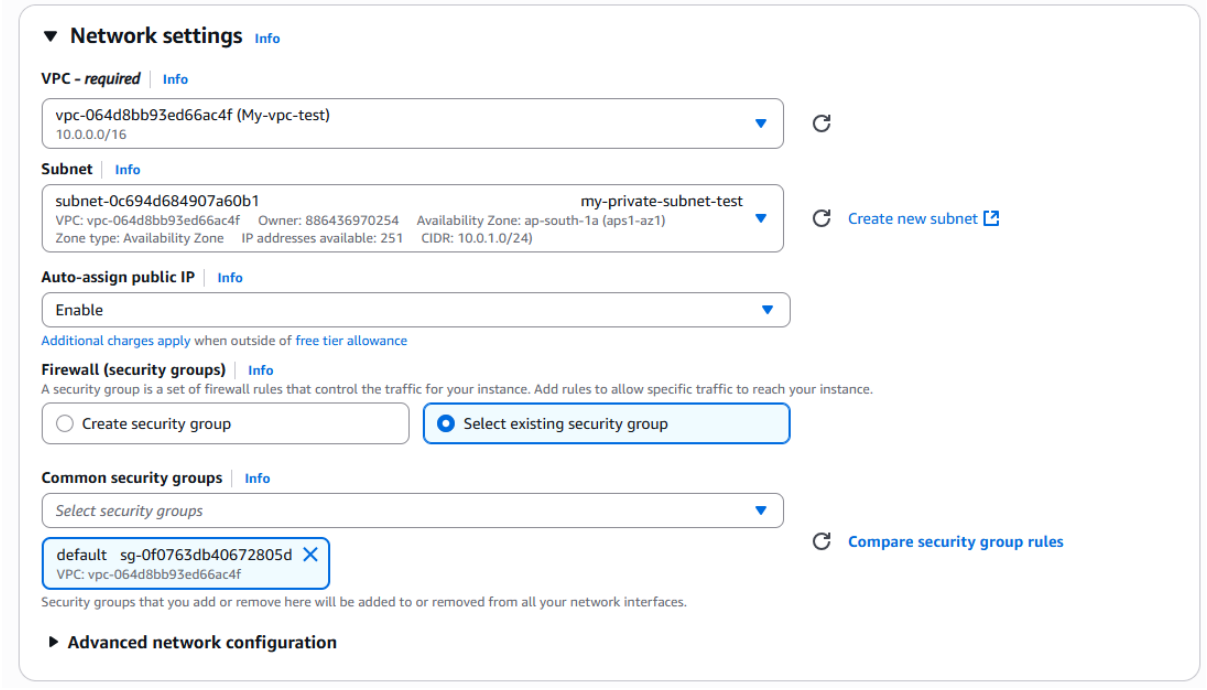


Click on the instance and note the Public IP address:

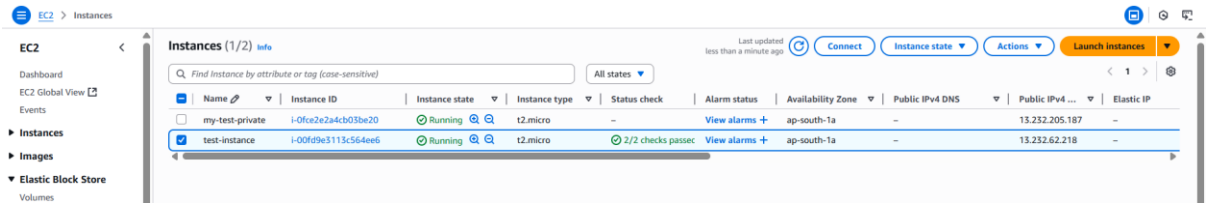


Now, we will create another instance for the private subnet: click on “launch instance” button again.

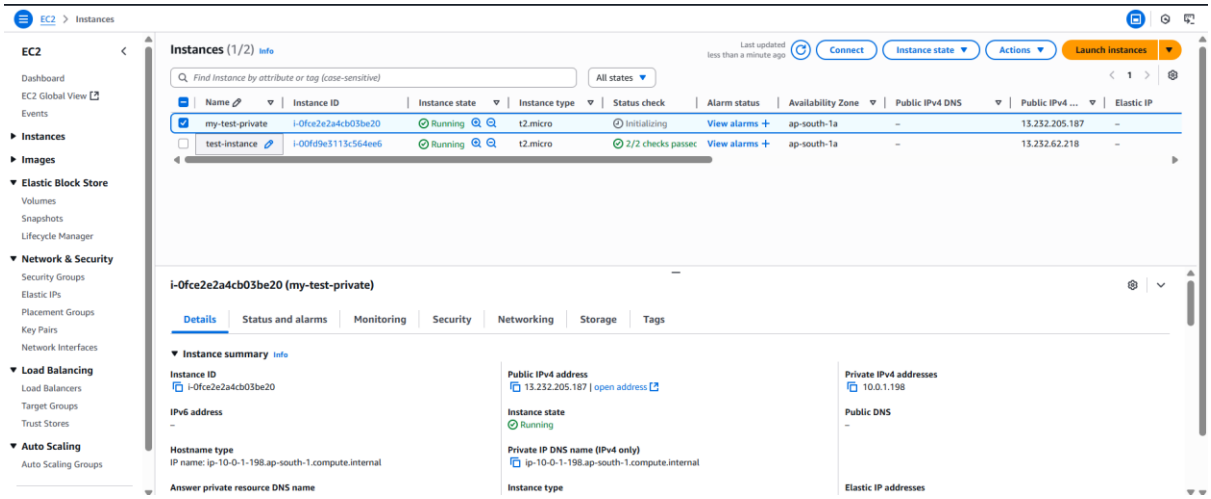
For this new instance, keep things as default, just change the “network settings” section as:



Then click on the “Launch instance” button: clearly “my-test-private” is created.



We can also see the details of the private instance :



Now, we will check if we are able to achieve our goal or not, for which we will ping the Public IP of the non-private instance: clearly it is working.

```
C:\Users\Aditya>ping 13.232.62.218

Pinging 13.232.62.218 with 32 bytes of data:
Reply from 13.232.62.218: bytes=32 time=44ms TTL=120
Reply from 13.232.62.218: bytes=32 time=44ms TTL=120
Reply from 13.232.62.218: bytes=32 time=44ms TTL=120
Reply from 13.232.62.218: bytes=32 time=43ms TTL=120

Ping statistics for 13.232.62.218:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 43ms, Maximum = 44ms, Average = 43ms

C:\Users\Aditya>
```

Similarly, pinging private instance will not work:

```
C:\Users\Aditya>ping 13.232.205.187

Pinging 13.232.205.187 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 13.232.205.187:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

--The End--