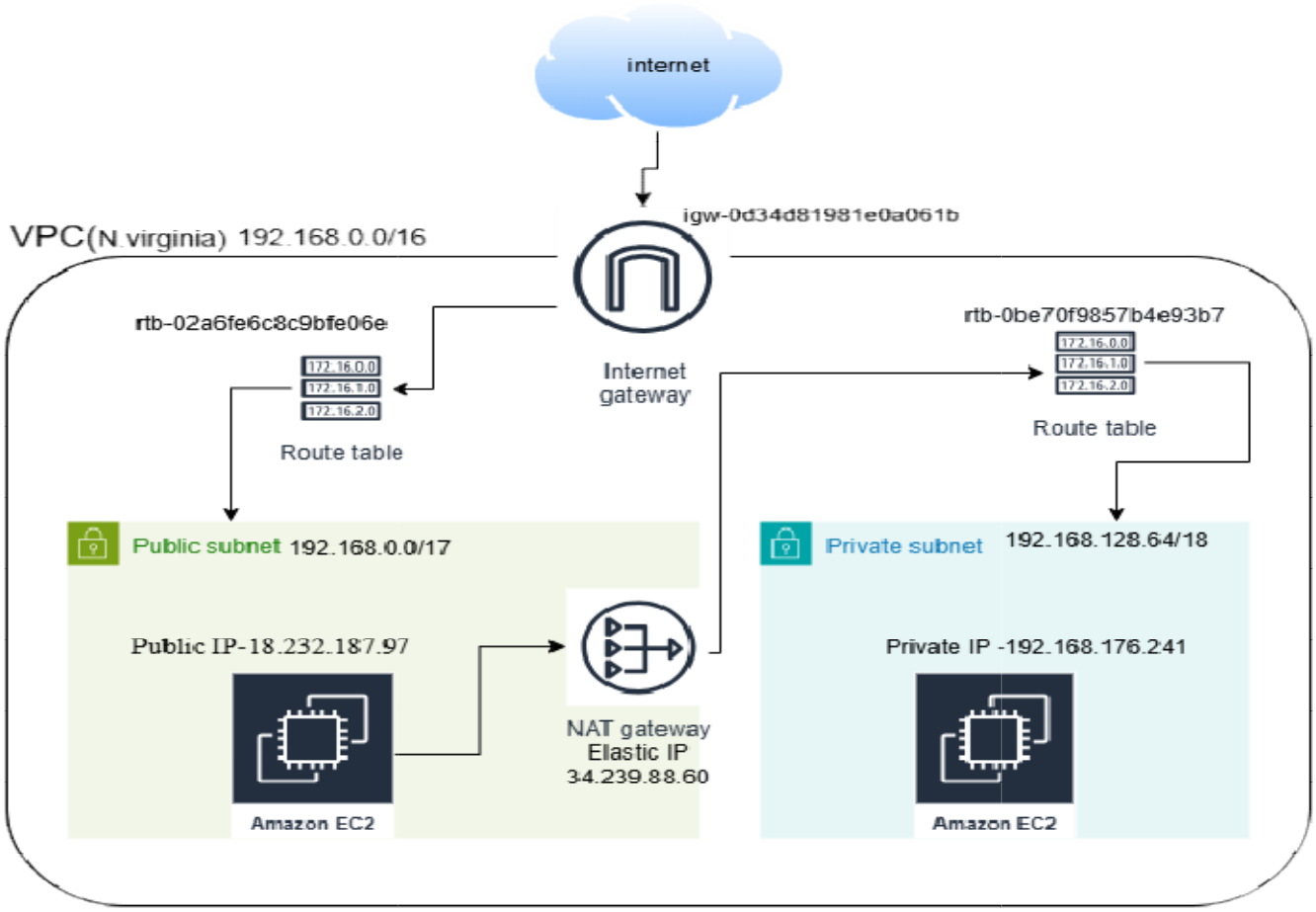
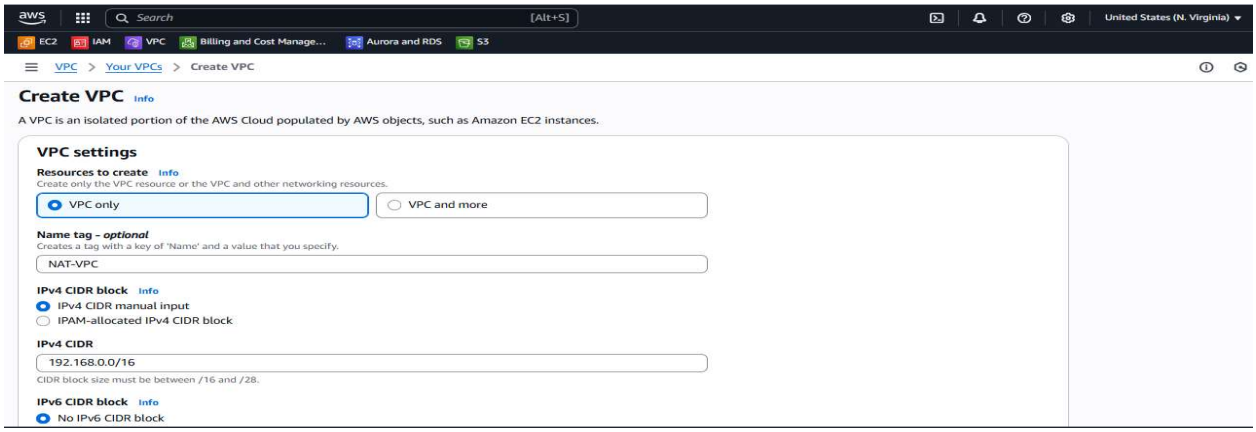
Connecting Public Server's(EC2) **Internet** to Private Server(EC2) Using NAT Gateway (VPC) security process endpoint will be public server

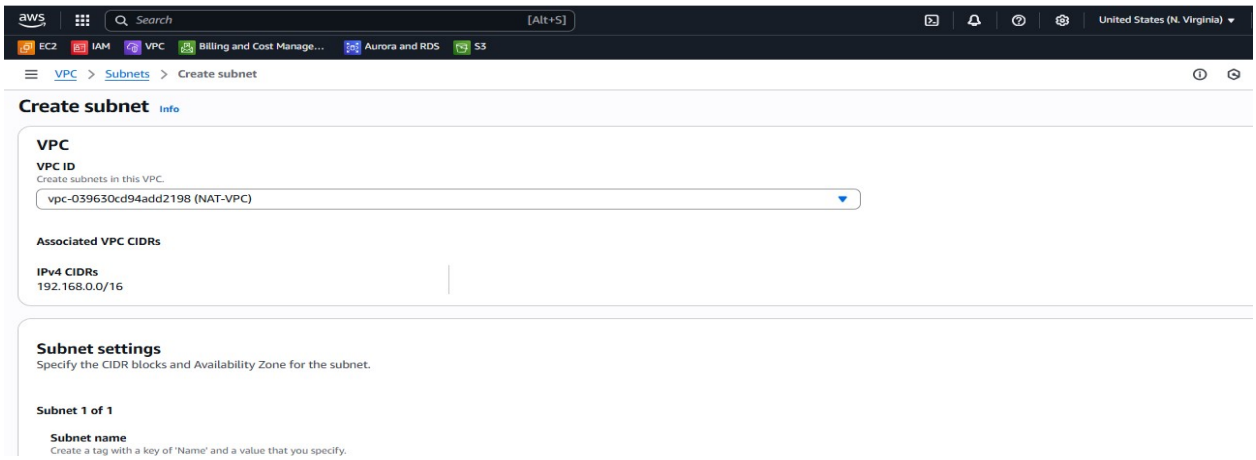


Issue : - For security reasons we have to not show our private server to everyone for that we will provide internet through public server.

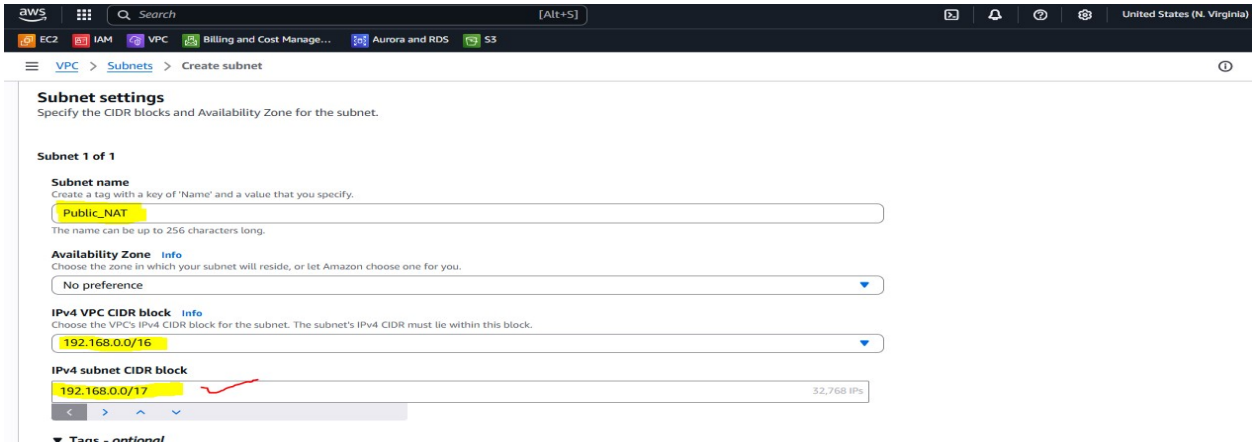
First we will create a VPC (CIDR-192.168.0.0/16)



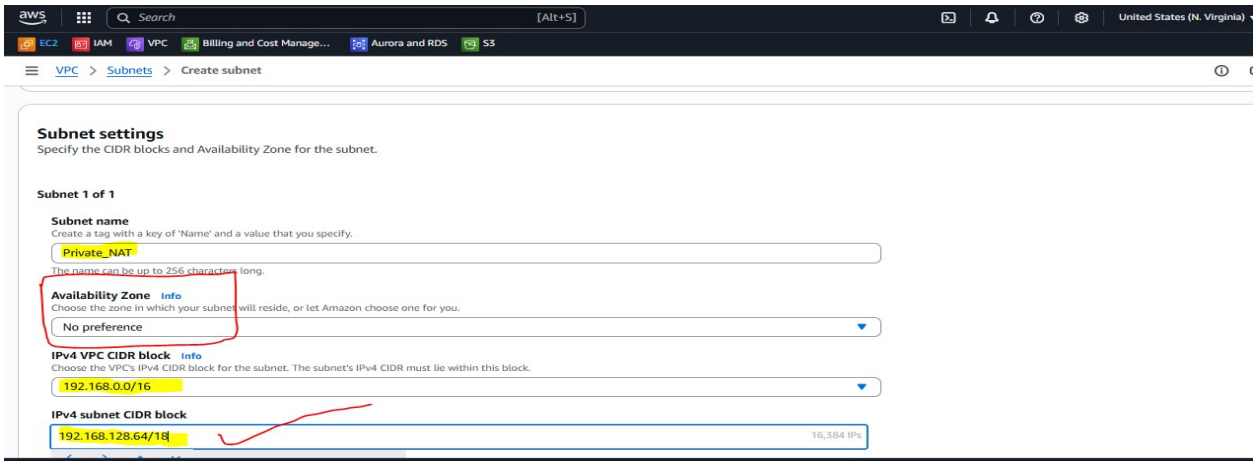
Now in that VPC we need create Subnets (Assigning IPs for subnet always check IPs Range in CIDRs /16)



Our Public subnet will be - 192.168.0.0/17



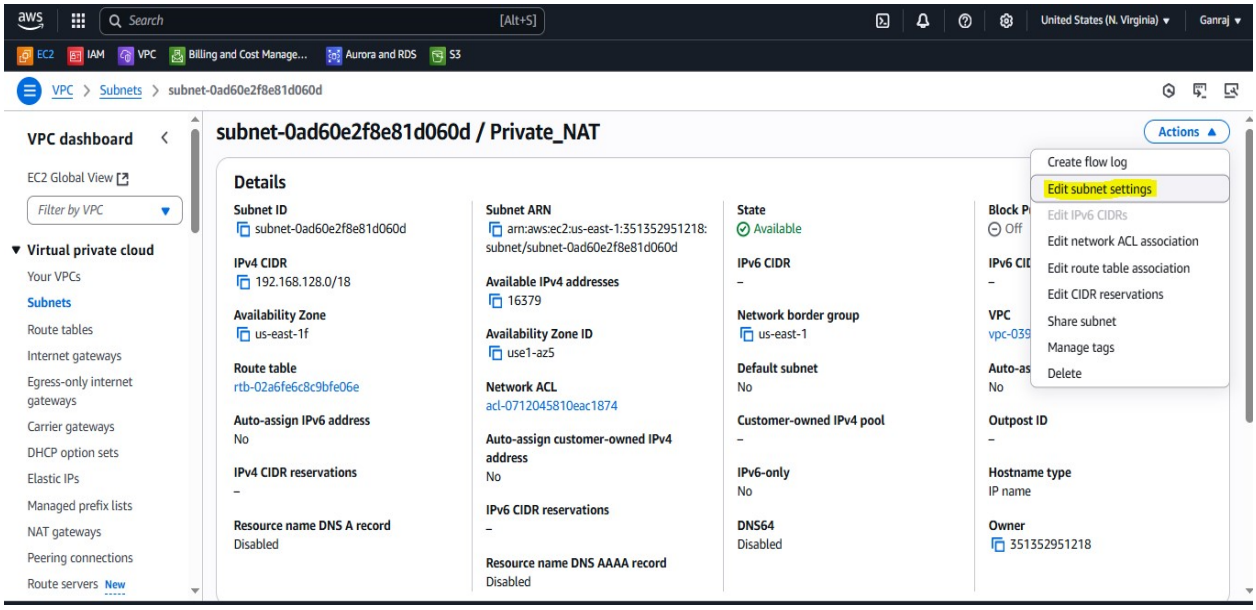
Private Subnet - 192.168.128.64/18

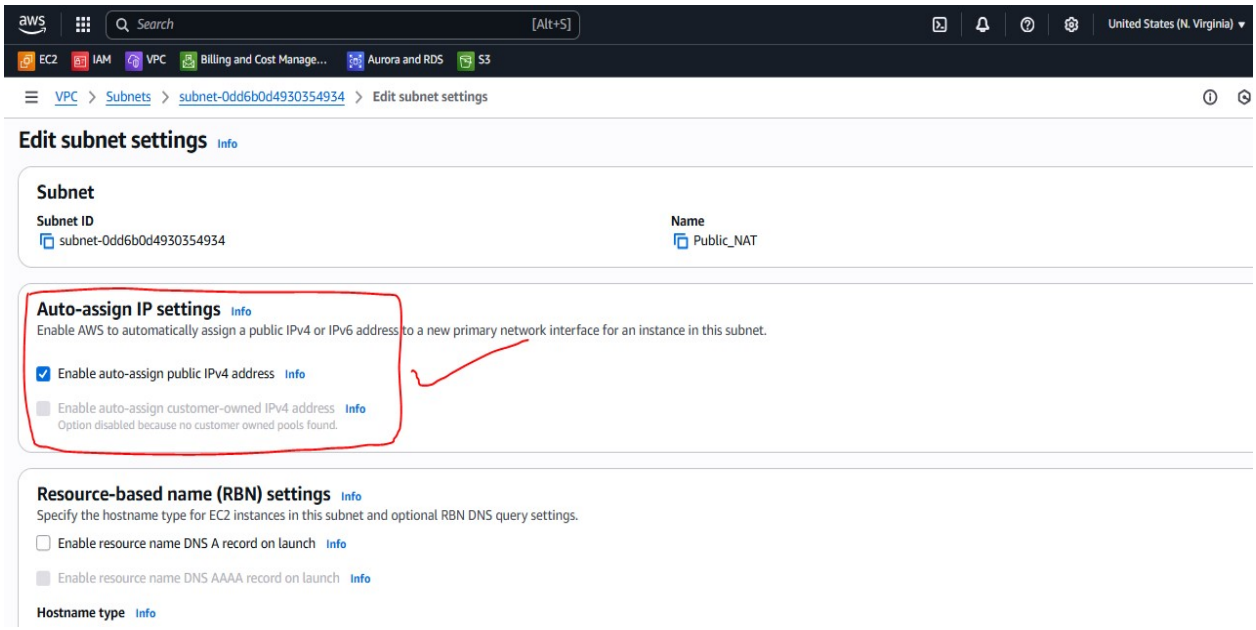


Here in the both you can set same availability zone also

Imp – if we need set a private subnet that's we need set that subnet auto assign public IP to be Disabled or off let me show you

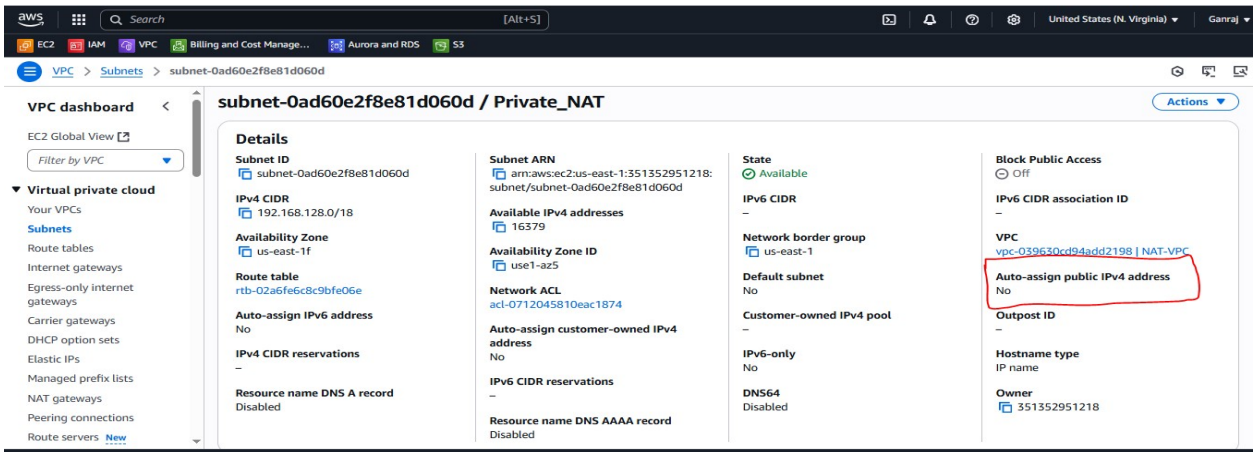
For public Subnet we will set On because we need that subnet accessible for internet



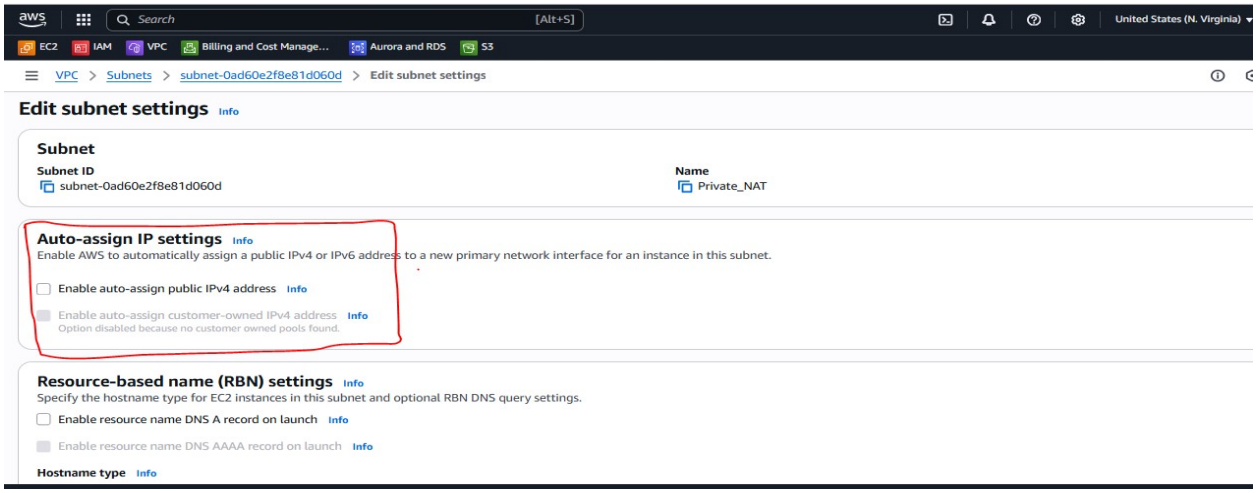


And Click on Save.

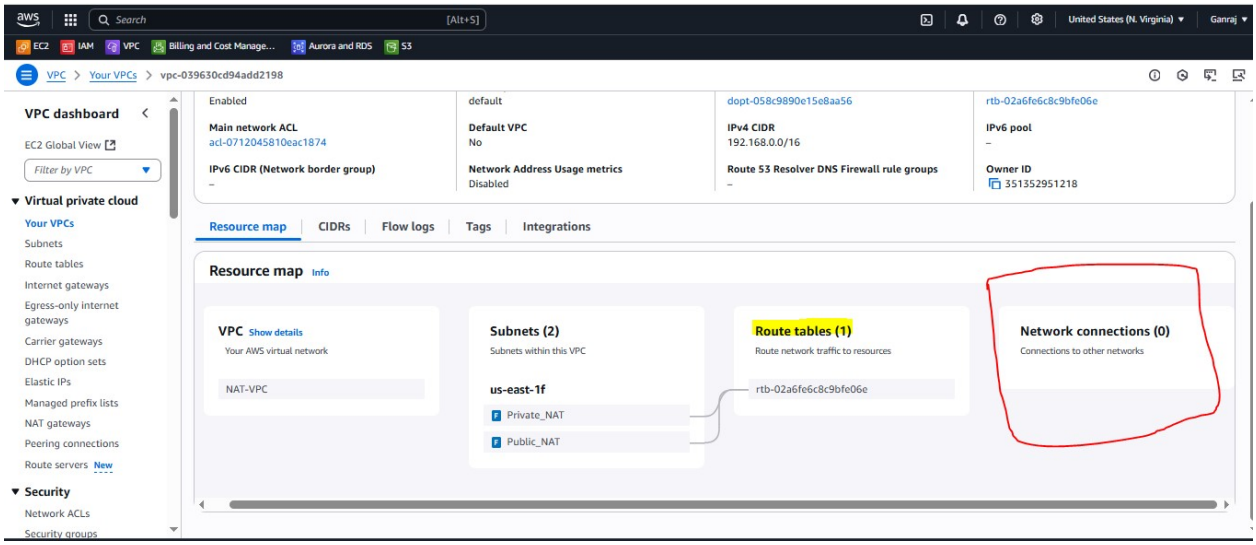
Now we have check for private subnet is auto assign IP is enabled or off .Need to set off because we are making private server using that subnet lets check It.



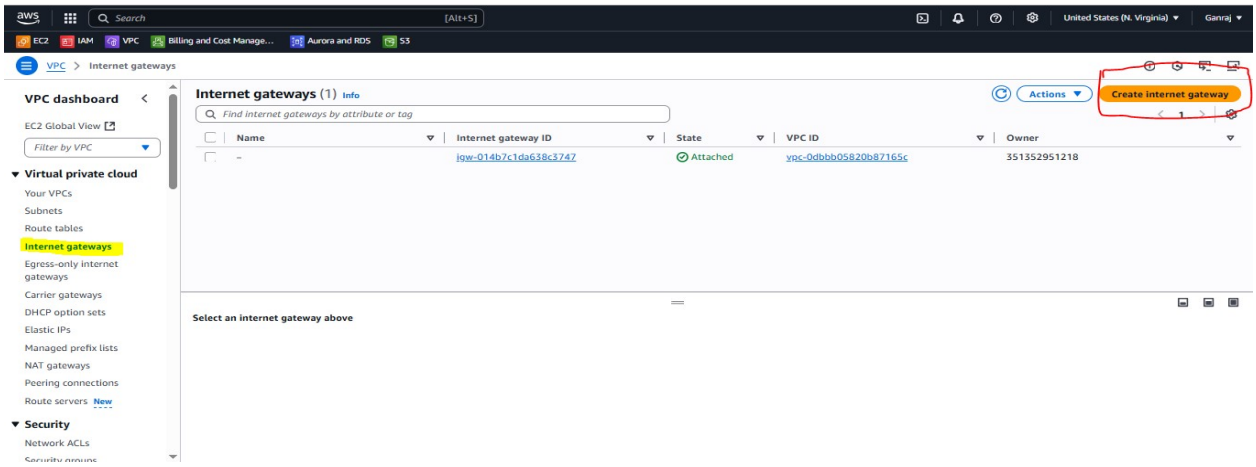
If here shows Yes go to actions and edit subnet settings and uncheck the box as shown in the snap.

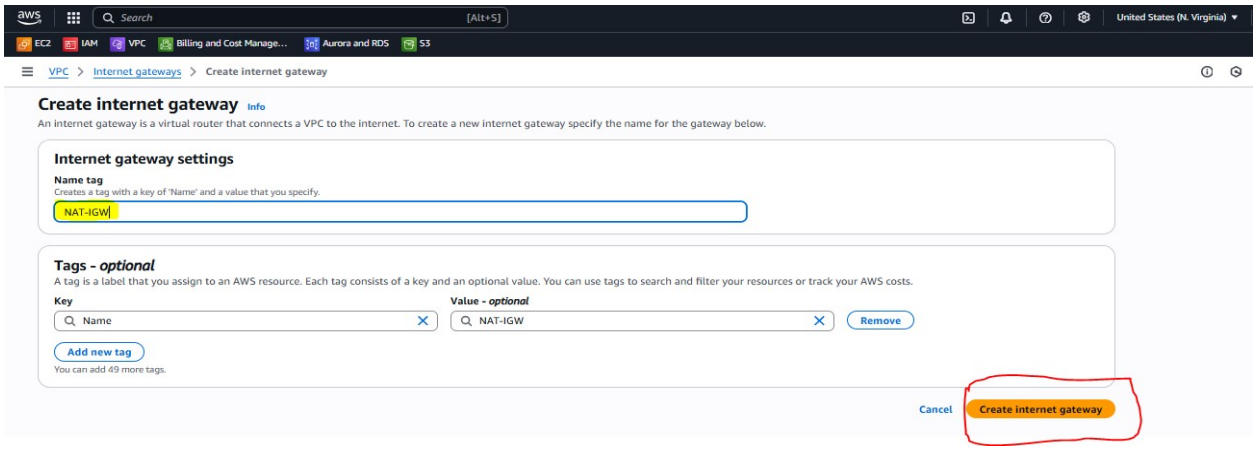


When create subnets in VPC it automatically gives us a route table as you can see in the snap.

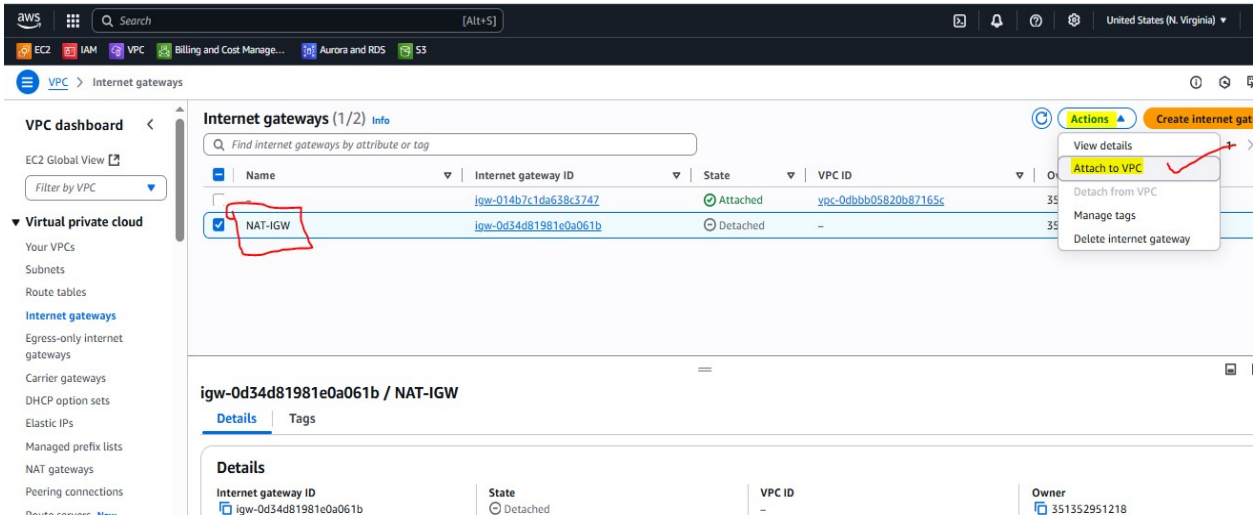


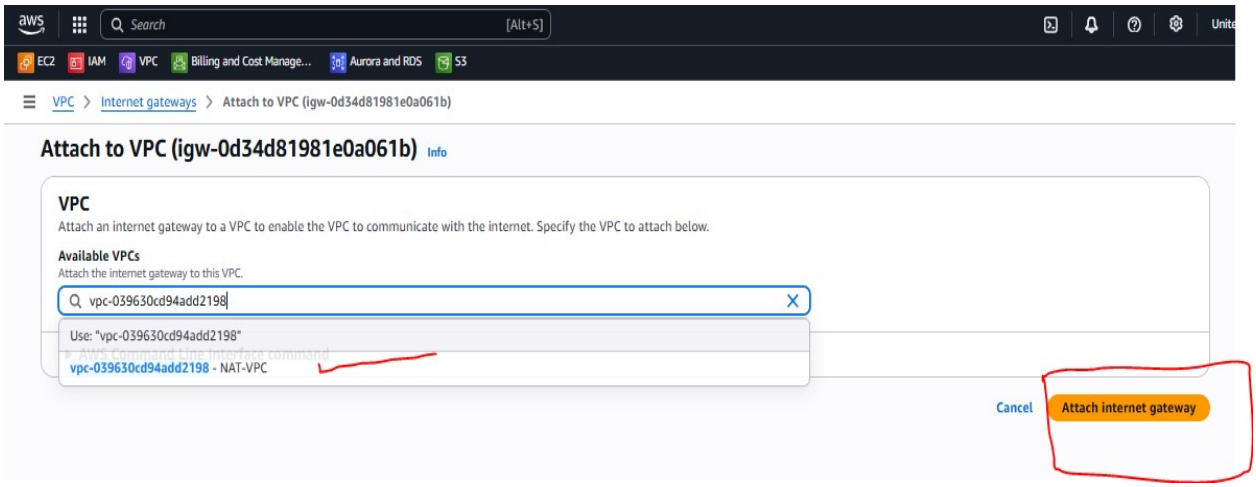
But you can see in the snap we don't have any internet gateway because we have created own vpc if we use default VPC we get automatically attached Internet gateway to our VPC .So now we have to create a internet gateway for our VPCs and for its Subnets which connects by route table.



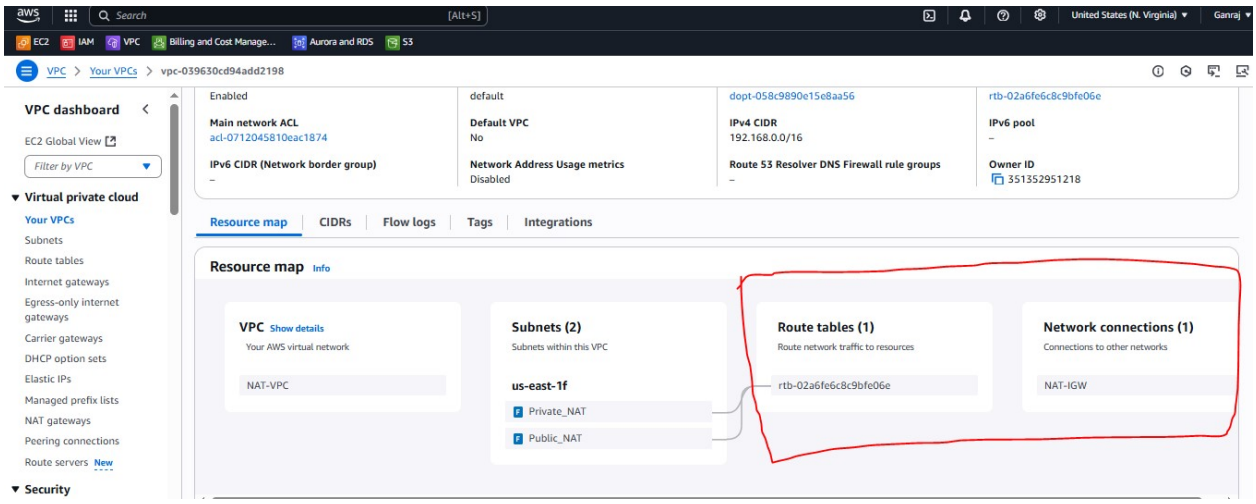


Now we need to attach that Internet gateway to our VPC

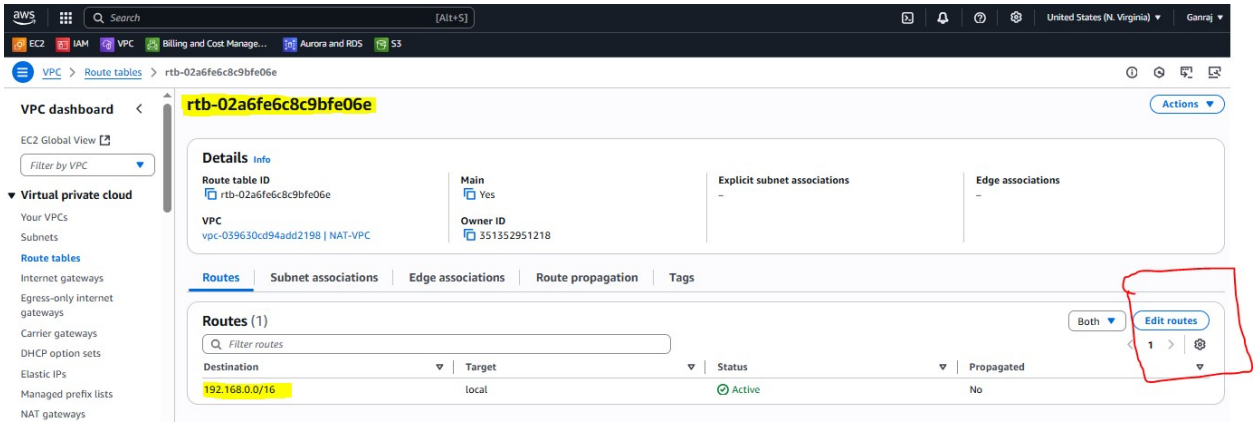


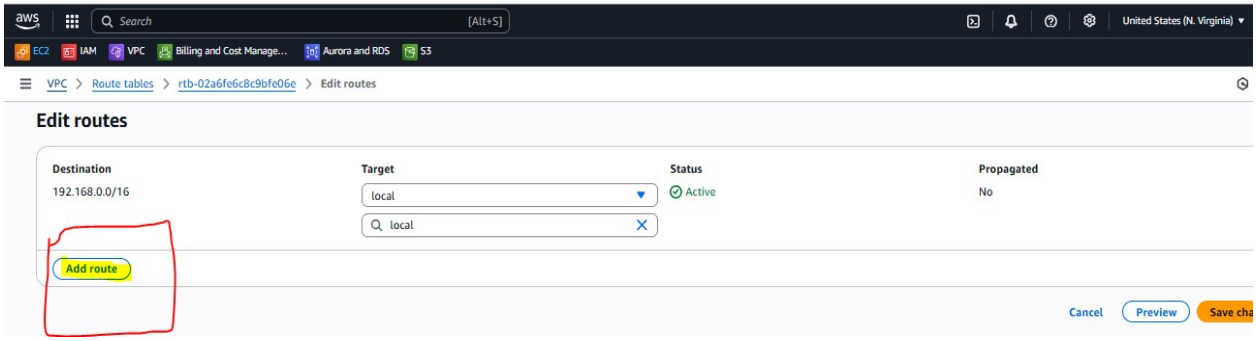


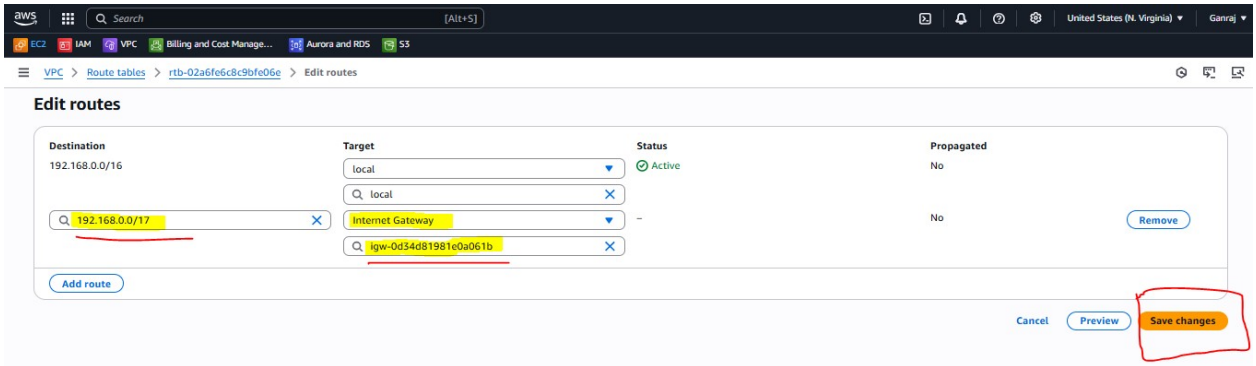
We have connect internet gateway to route table which we provide internet to out subnet later



Got to route table ID - rtb-02a6fe6c8c9bfe06e

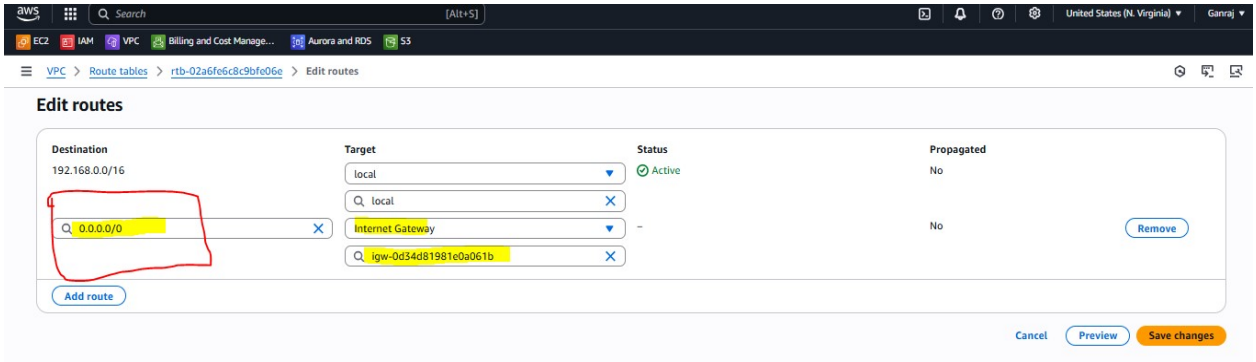


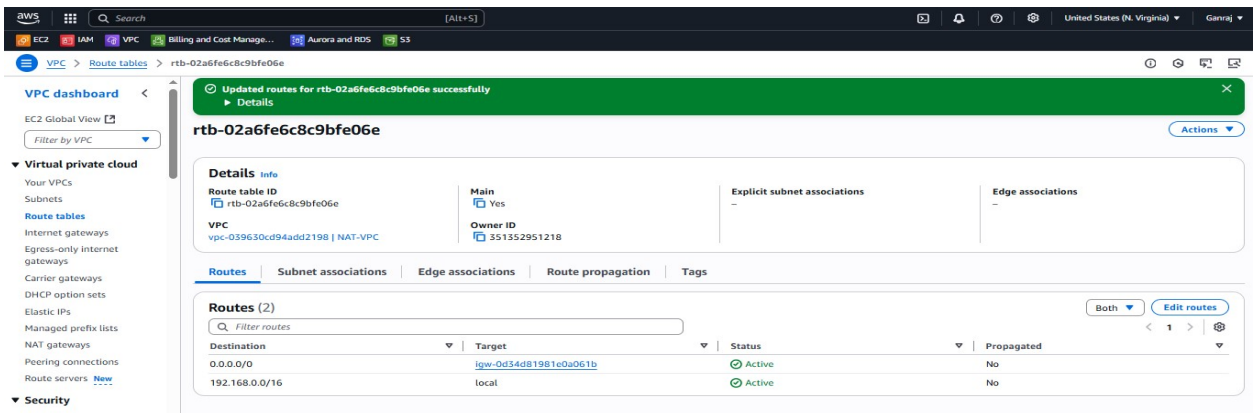




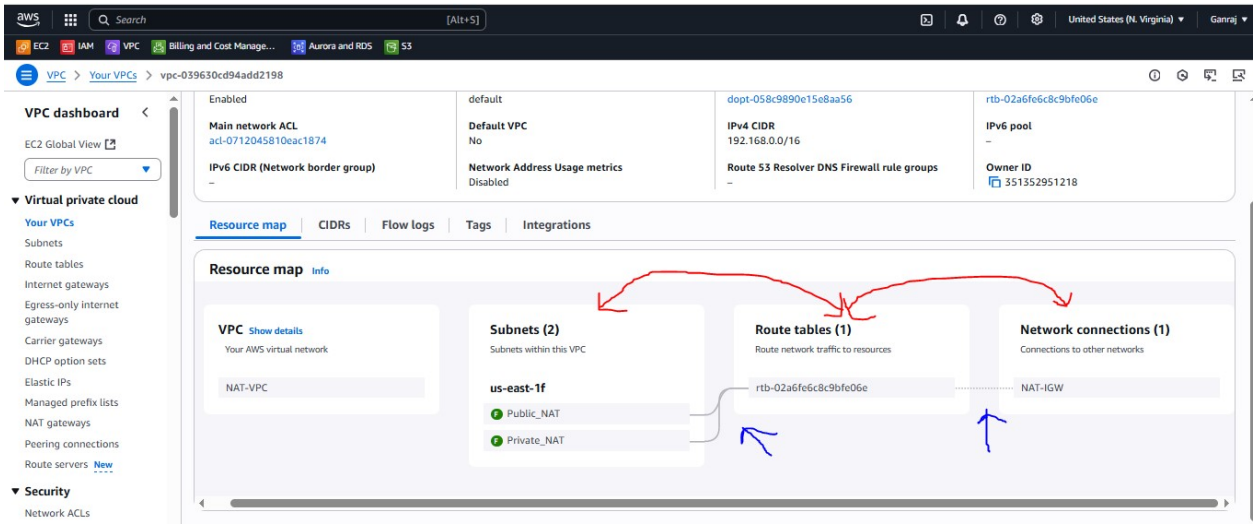
Here we have added specific IPs which shows internet only route on or over specific IPs or subnets.Because we have to isolate our server if you are testing you can set like default all (0.0.0.0/0) its your choice.

Save changes.

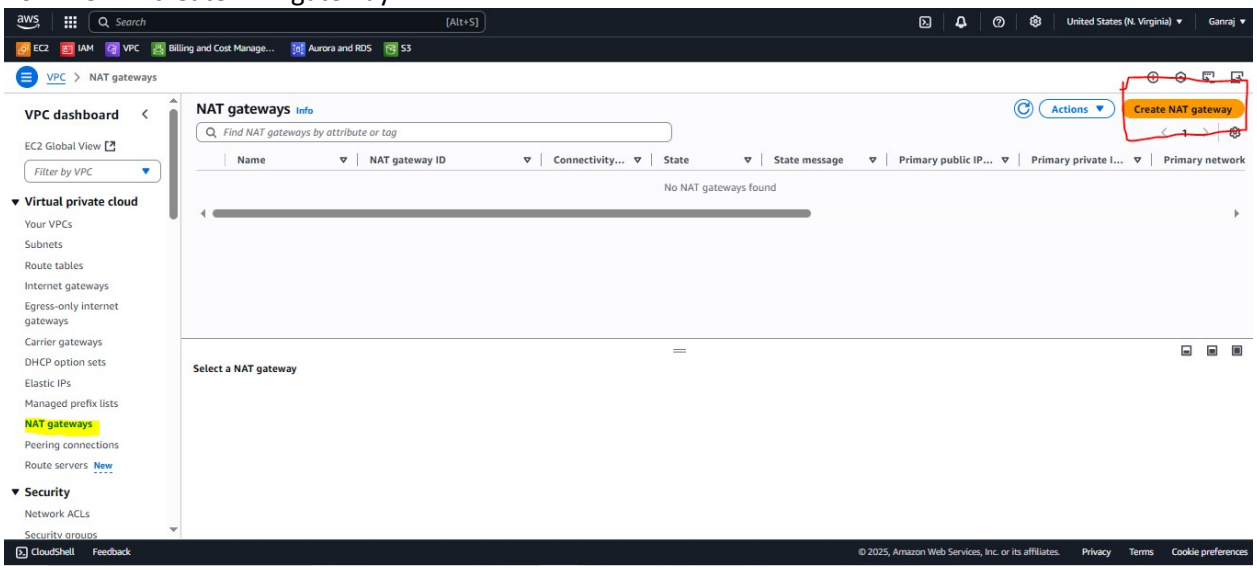




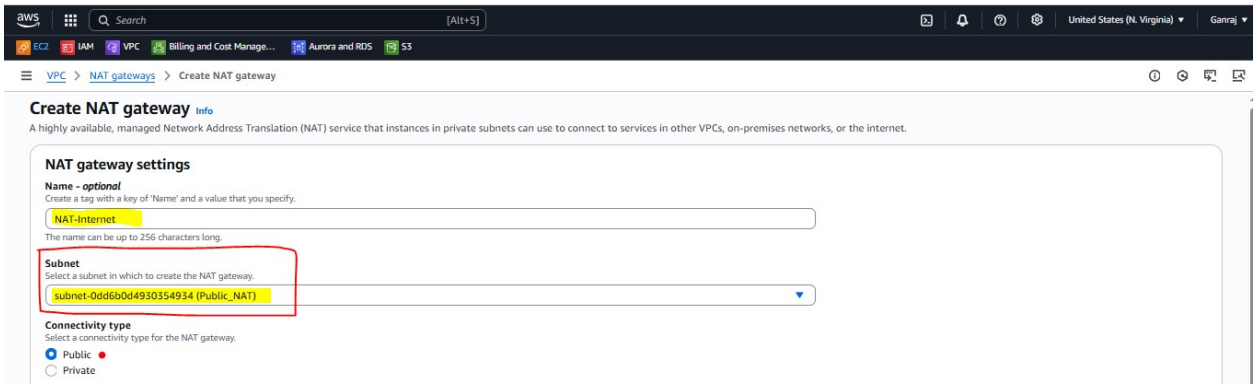
As we can see in the below snap connection between internet gateway to route table to subnets are made see but note if we made specific subnet ip connection then its will not same as below.



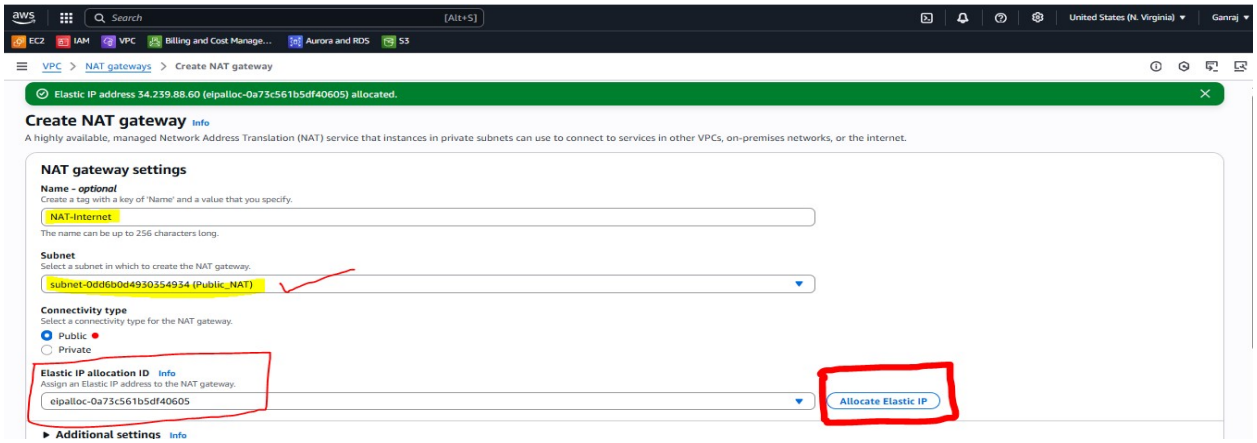
Now we will create NAT gateway

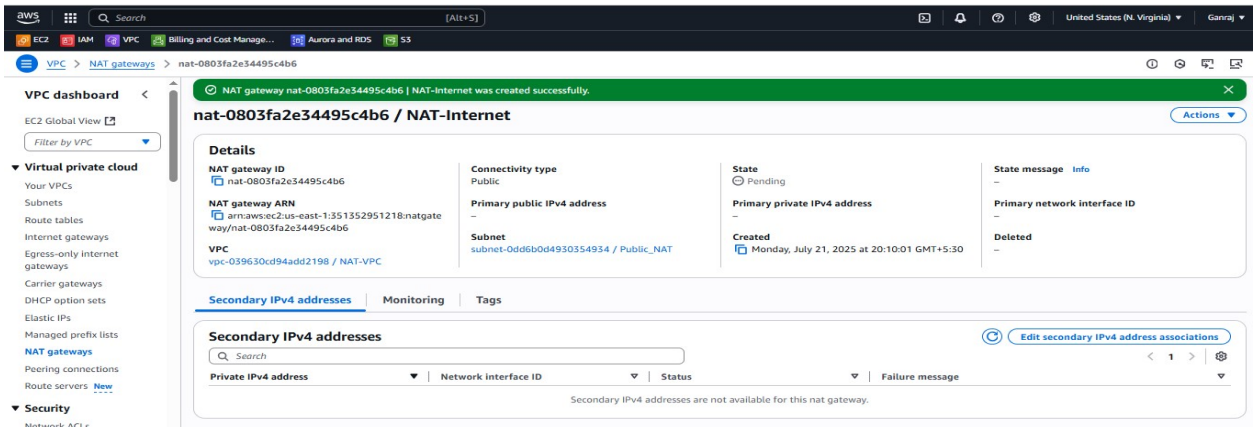


NAT gateway only Attached to Public Subnet because internet access is only available for Public subnet

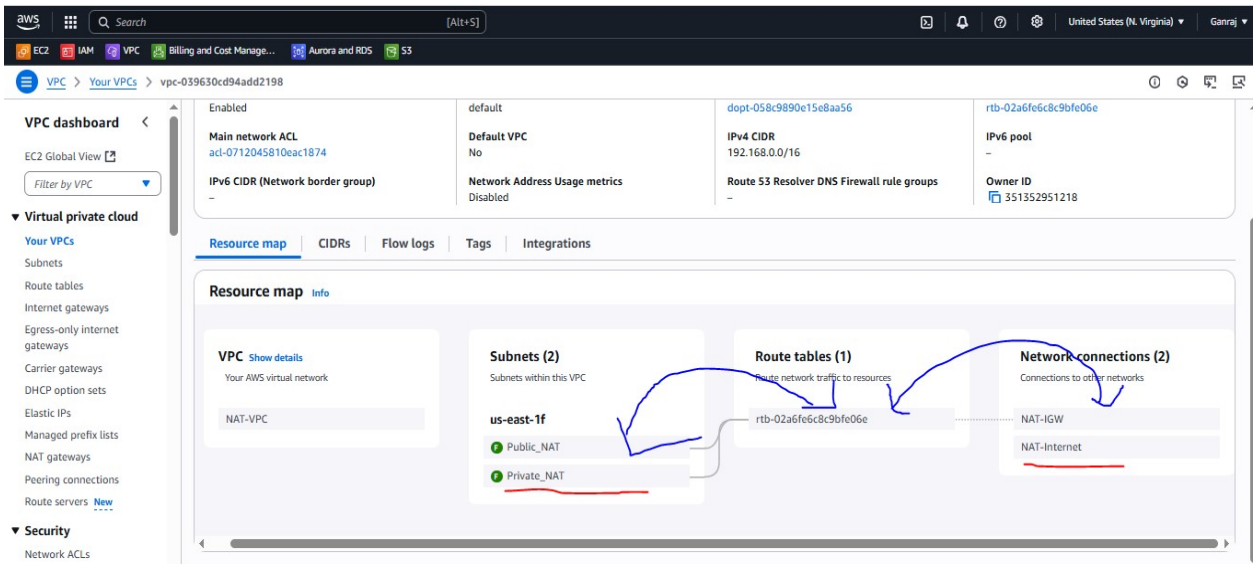


For NAT we need Elastic IP because it works on Static IP which is **fixed public IP**. Access the internet (outbound) but **Remain unreachable from the internet (inbound)** — for security

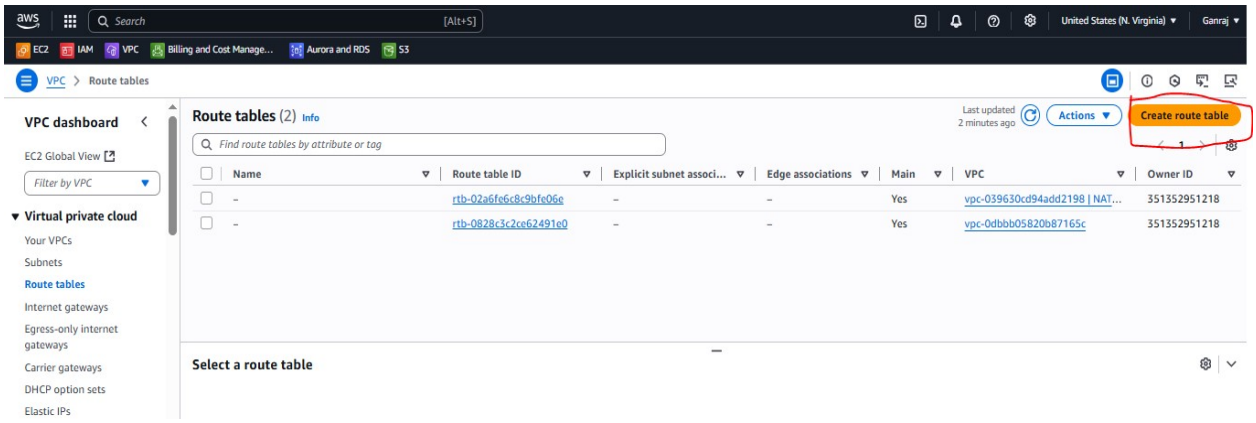


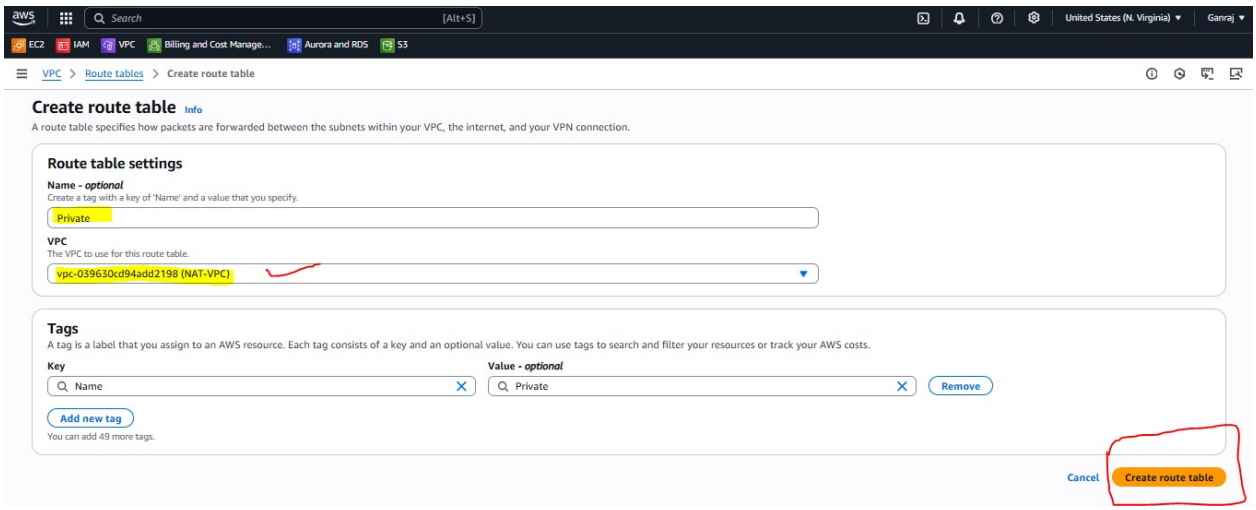


Here in the below snap we can see public subnet have internet but not for private because of route table for that we need to create another route table to make connection through NAT

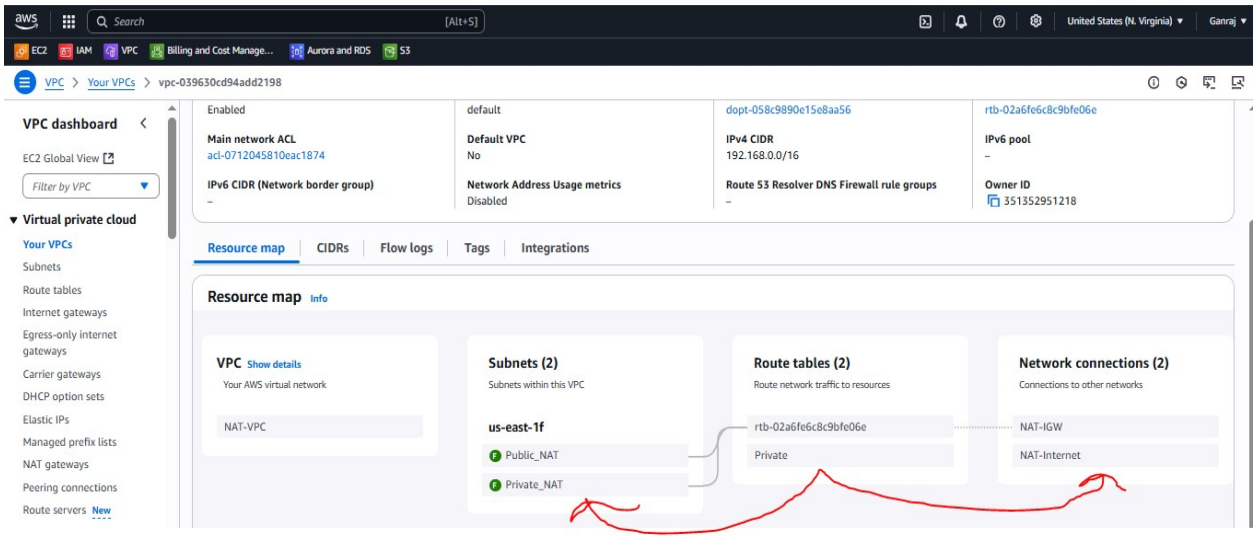


Now creating new route table for private

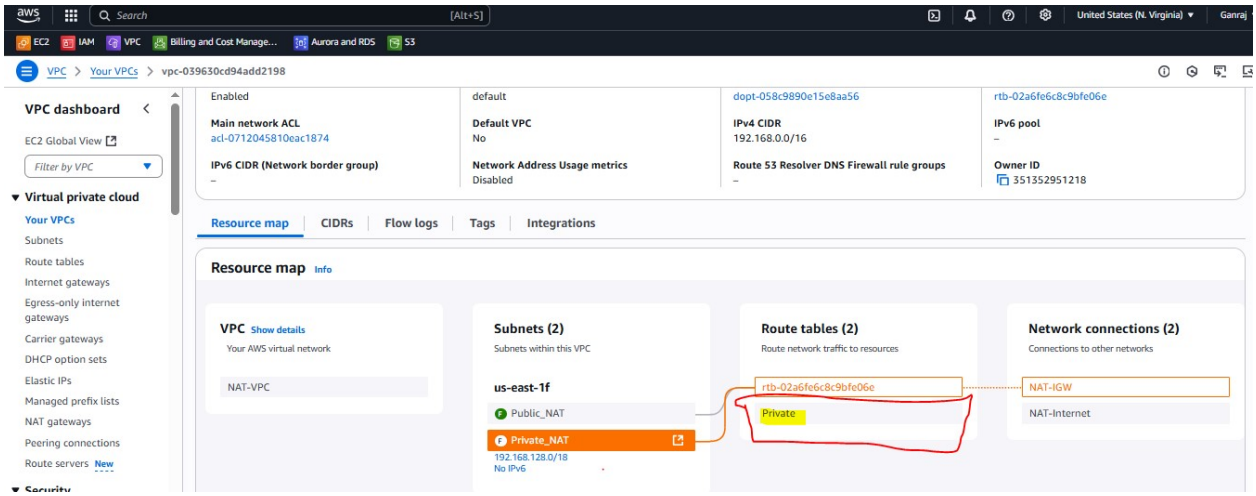


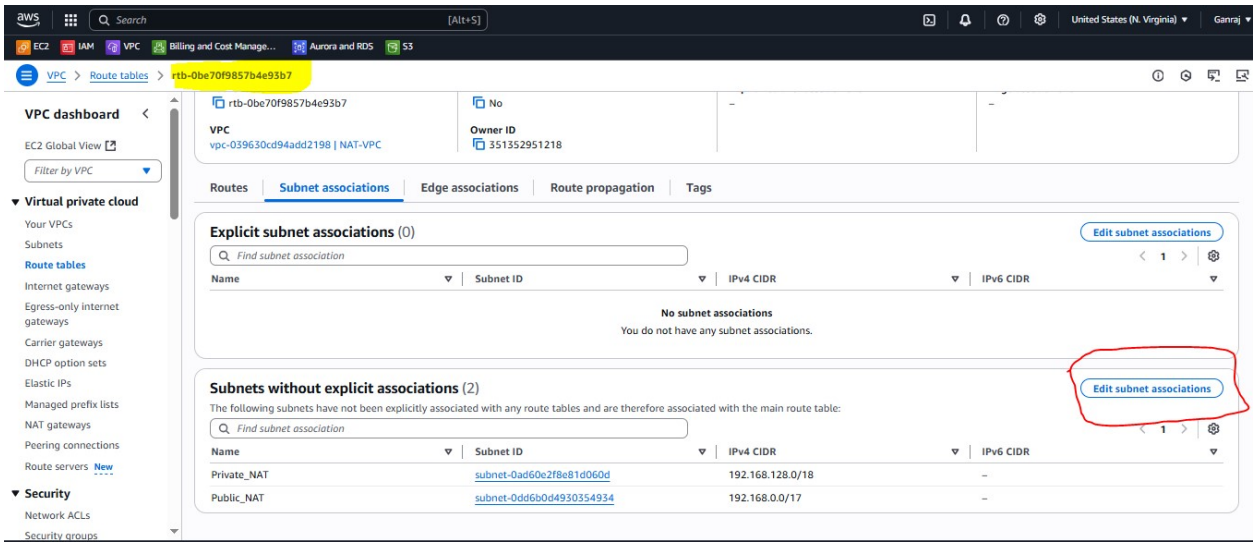


Now we have connect our private route table associated with only with Private Subnet later on NAT also

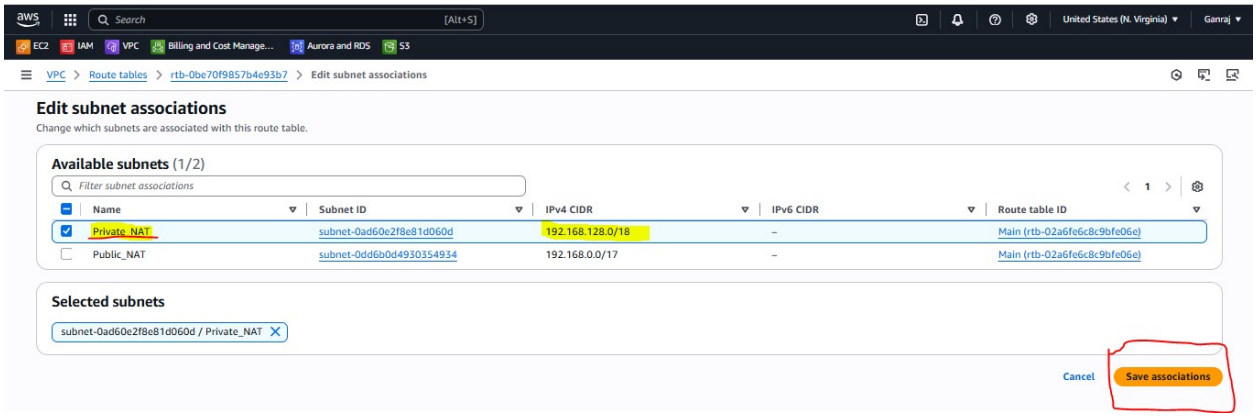


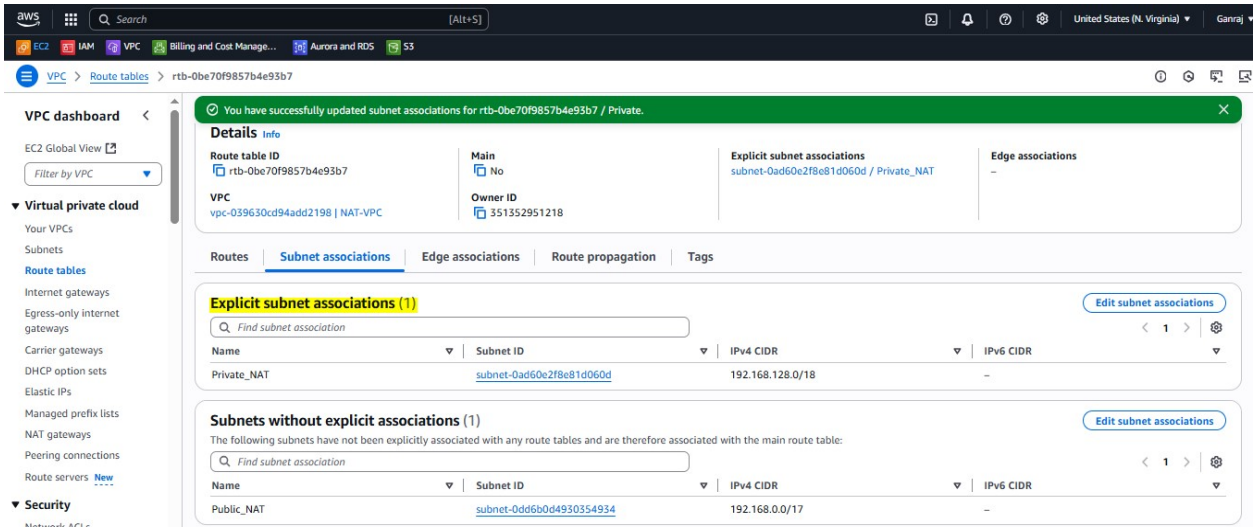
Now we will use private route to do subnet association and add NAT to be routed with Private Route table



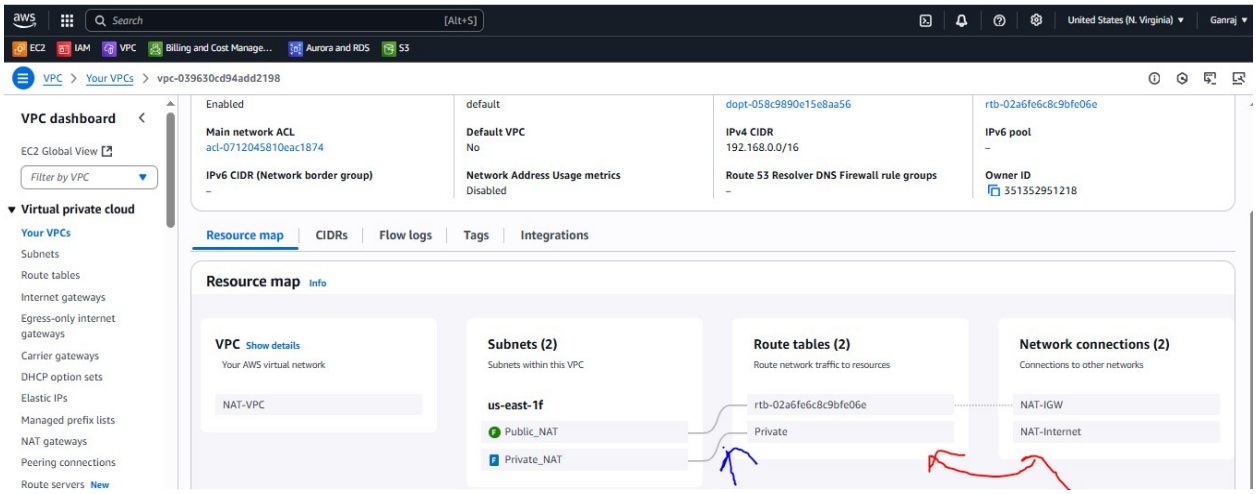


Here we have done the subnet association with route table for exclusive private route table will associated with Private Subnet (192.168.128.0/18)

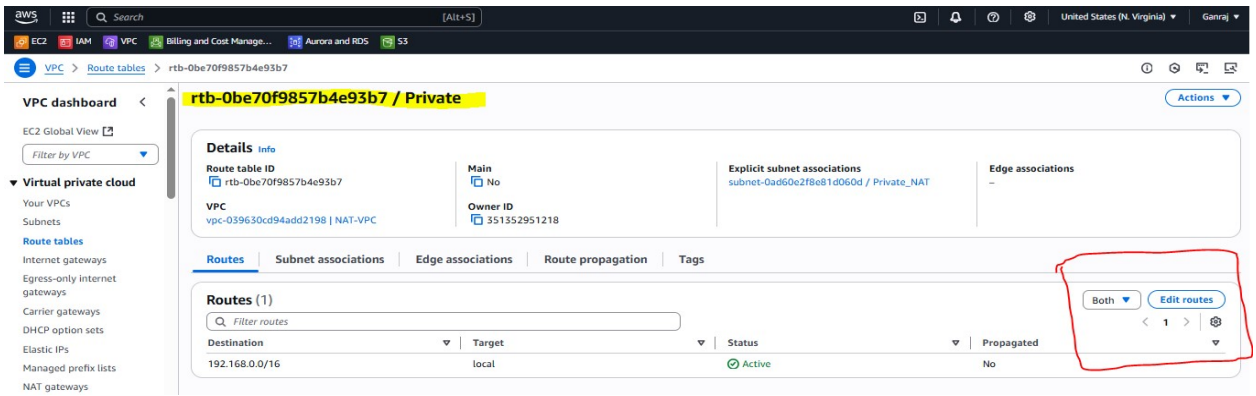


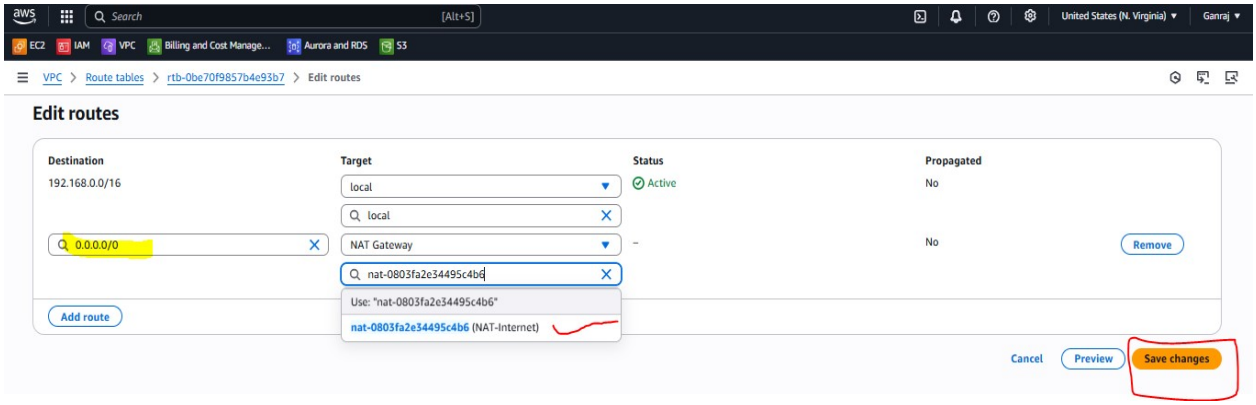


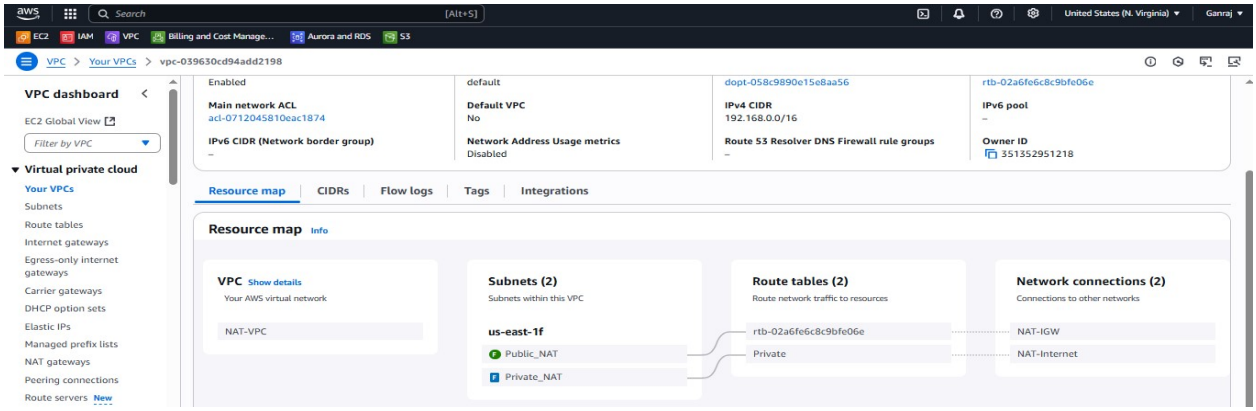
Now we will route the NAT towards Private subnet using Route table (Private) as you can see below snap



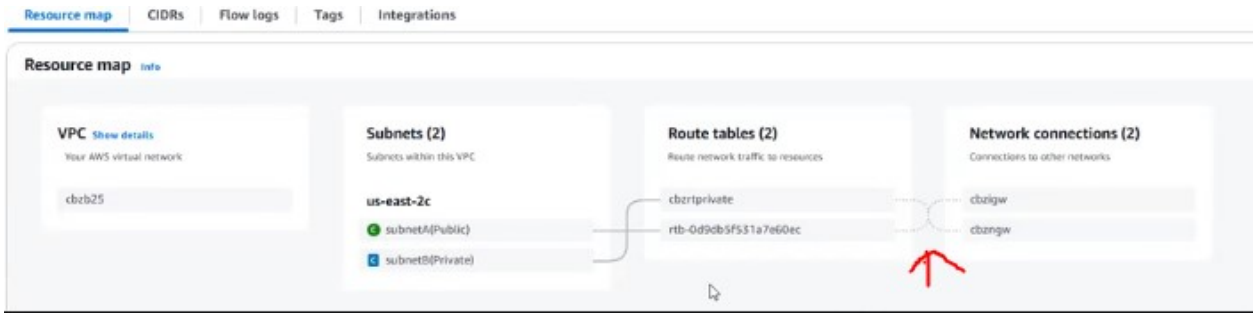
So go to route table's Routes







Its will show connection like this also its depends on representation of AWS.

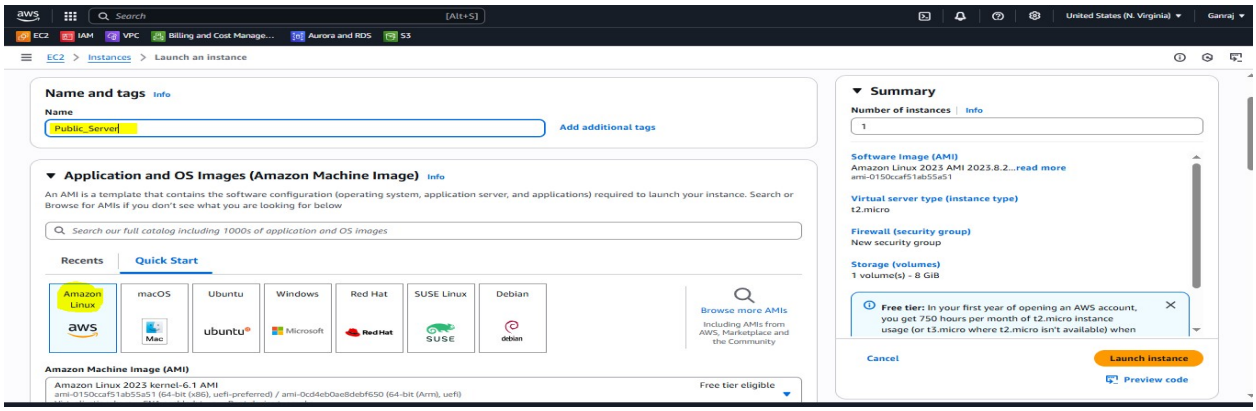


See we have made connection between NAT to Internet now we have create Instance to check whether our process giving internet of Publice server to private server and the private server access only through public server

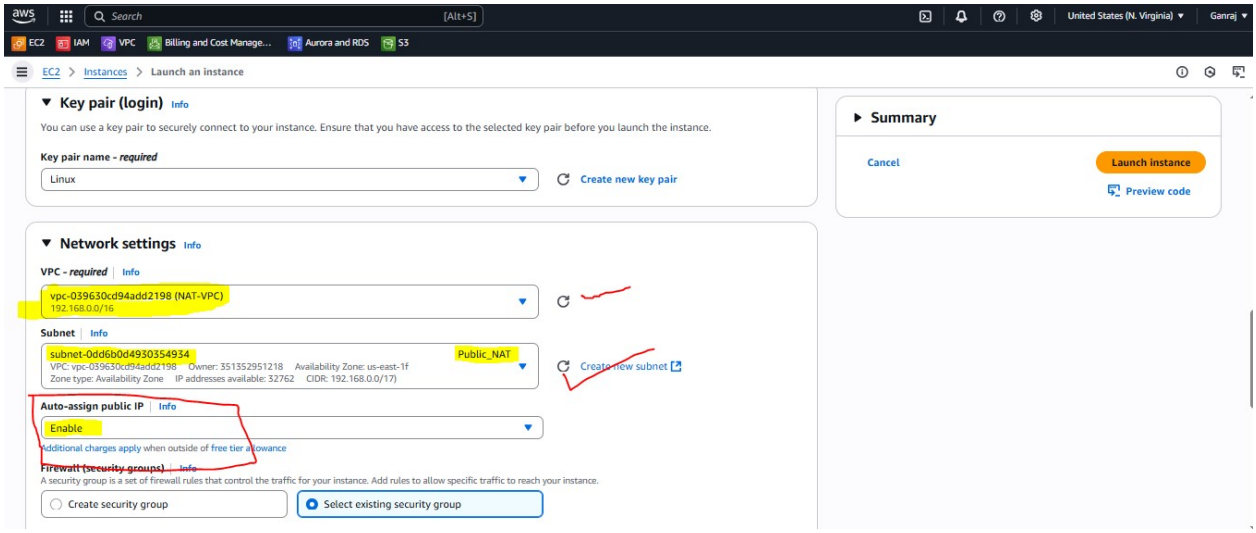
Note : - Private Server

- **Cannot be accessed directly** (no public IP, no IGW route)
- Can only go **out to the internet** using **NAT Gateway**
- Must be accessed via:
  - **Bastion Host** (jump box in public subnet)
  - **Public-facing server** (with SSH access + internal connectivity)
  - **VPN / Direct Connect** if you want private access from outside AWS

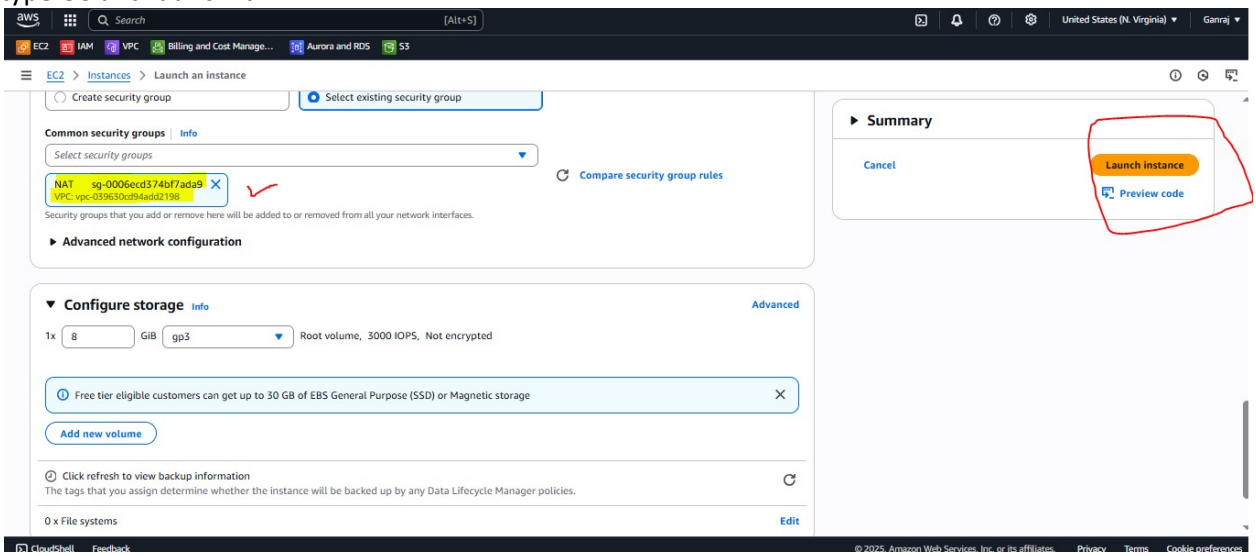
Now lets create Public and private servers in their specific subnets using VPC



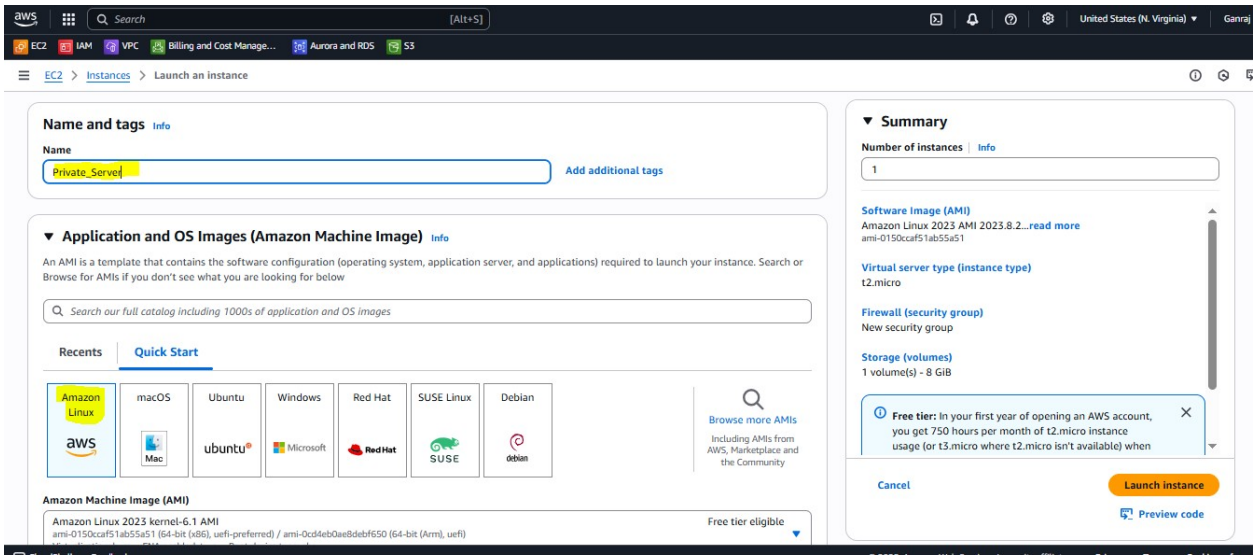
Here while selecting VPC click on our VPC and change subnet to public subnet it important change for our process also check Auto assign IP is Enable because we creating Public server.



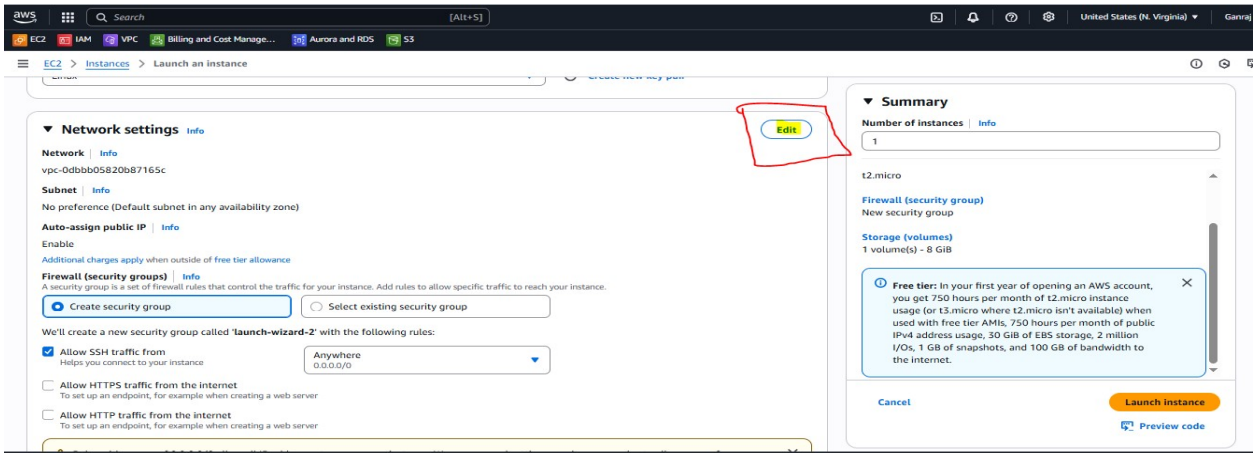
Create security group which have allowed inbound rule for internet and SSH protocol for accessing Linux type OS and launch it.



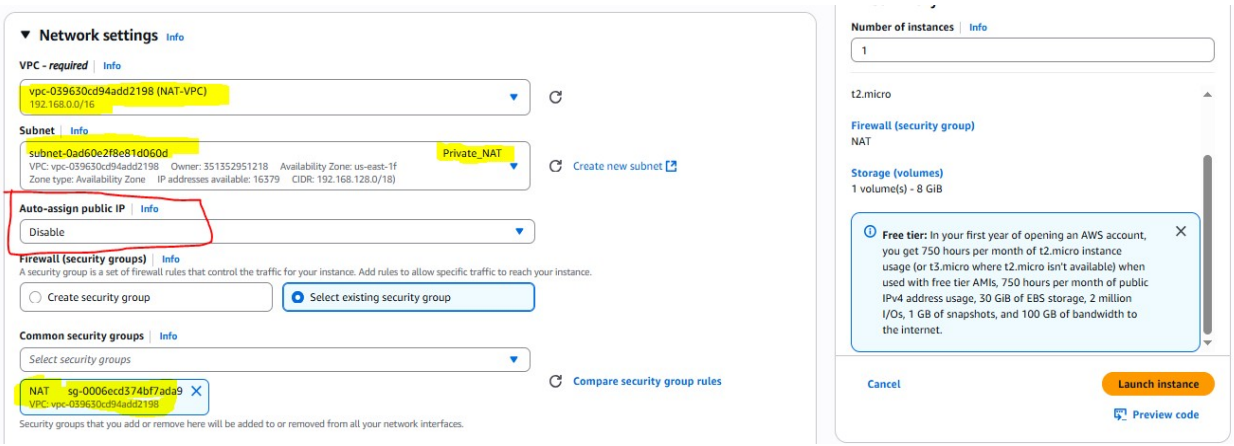
Now We will create private server



Here also we have change Default VPC to our VPC that we have created and Private Subnet



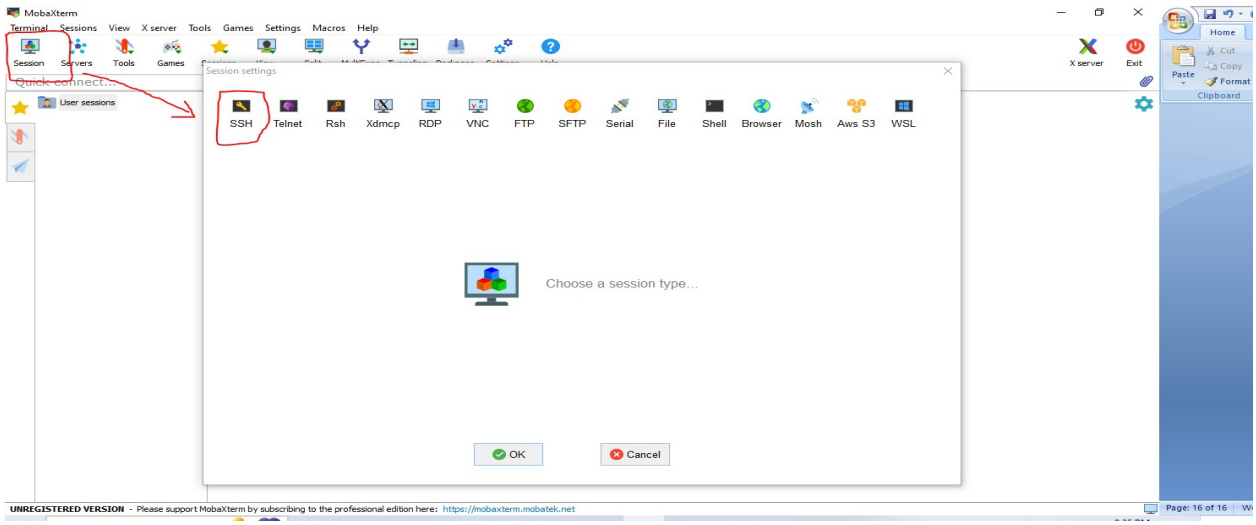
Here we can see auto assign IP need to disabled because we have set our private server to isolated from direct access through internet.

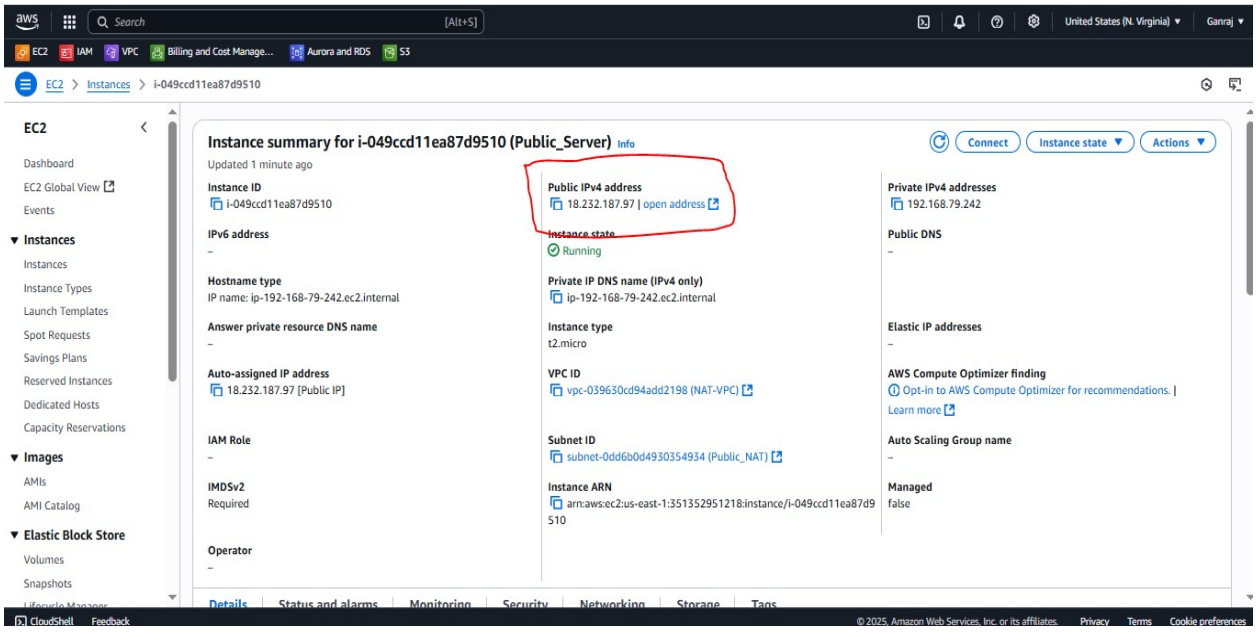


See we have created Public server and Private Server but if we want to access out private we need to go through Public so lets do process using Mobaxtrem because we need to add Private Key to our Public server which will access to Private Server

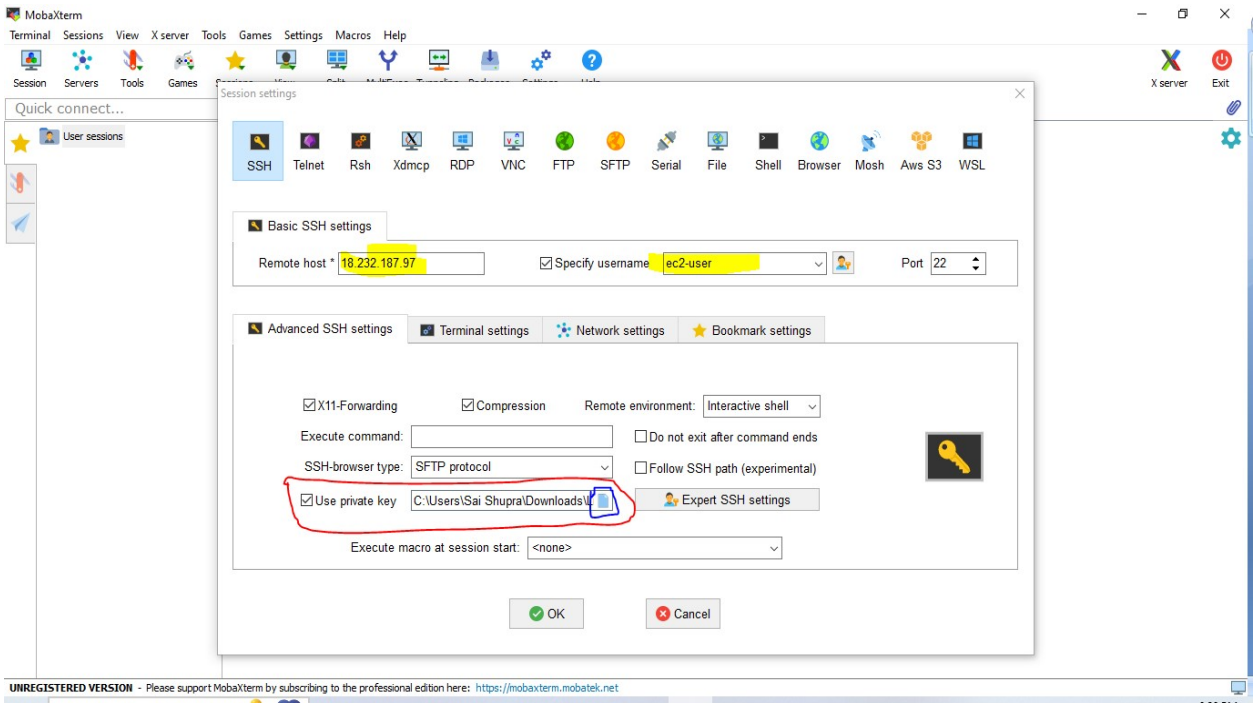
You can download MobaXtrem form here Free

https://mobaxterm.mobatek.net/download.html

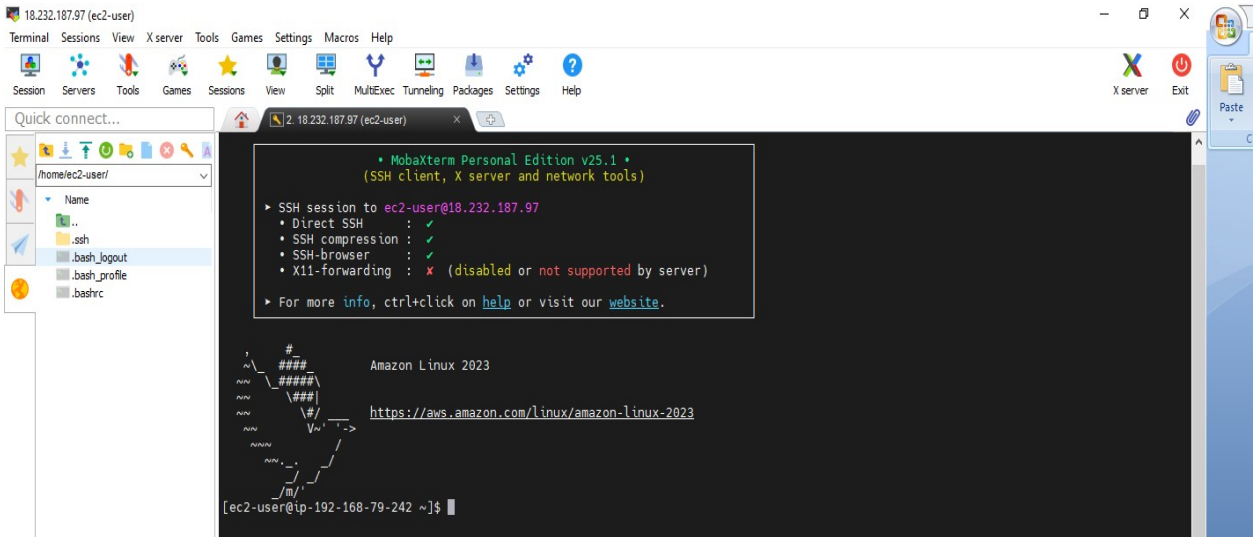




Copy the Public IP of Public server mention specific user for amazon we put ec2-user and in the advance option of MobXterm open saved Private key of public server then we can access public server using MobaXtrem .



Click OK.

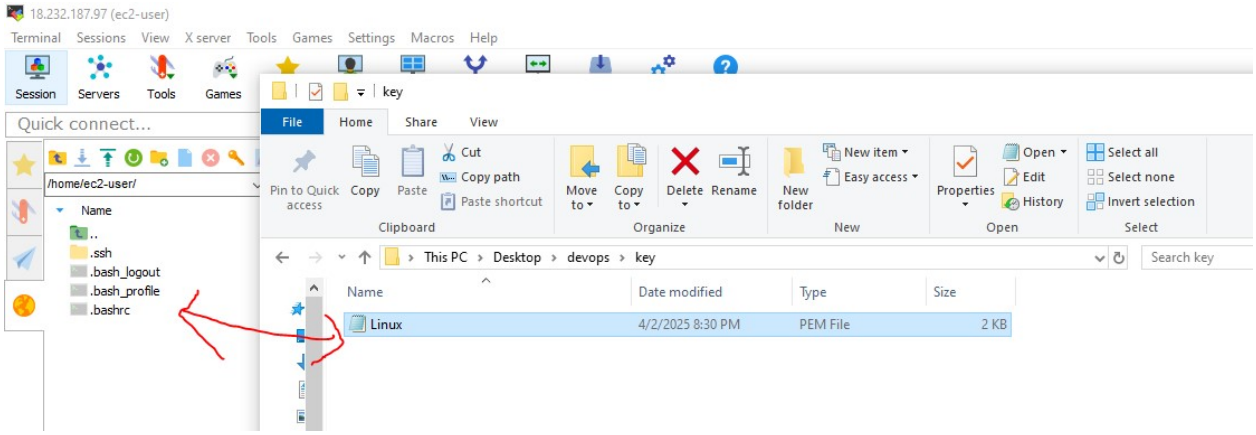


See we now connected to our public server which has intenet access now we have connect to Private server using a command

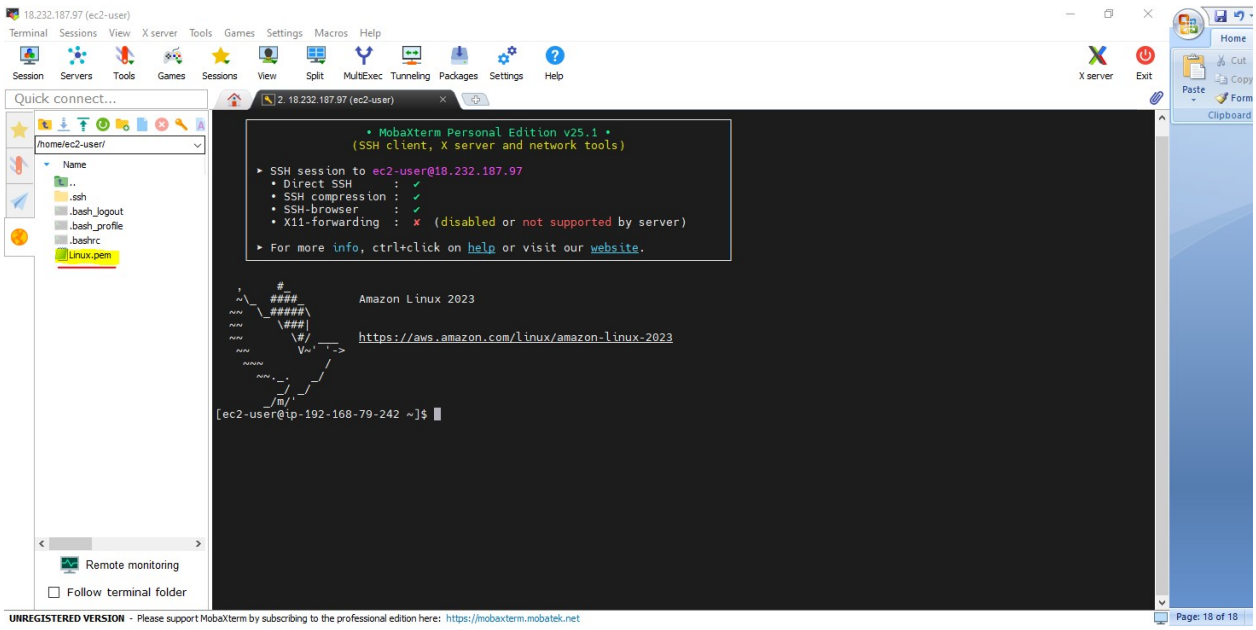
ssh –i ‘Private-key’ ec2-user@private-IP

for that we have to add private server’s private key lets add it

In the MobaXterm we have one advantage that we can drag drop data files from our local machine to VM(EC2 Instances)



As you can see copied it from our machine to EC2 instance

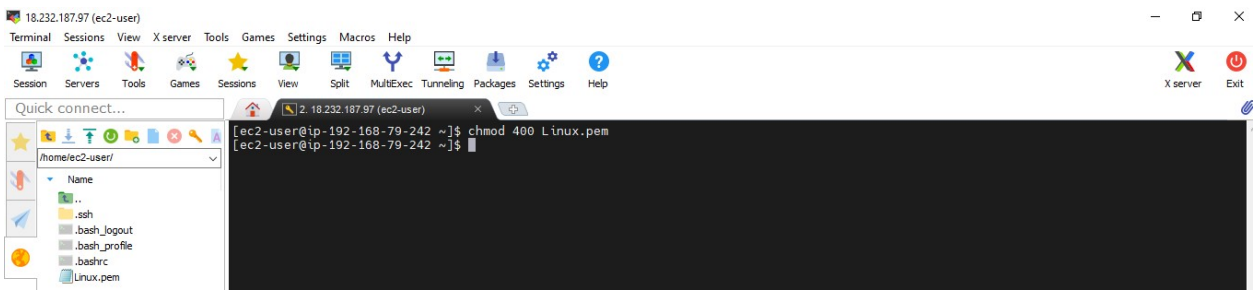


Now we will use that command and connect Private Server on Public Server

But first we need to give access to that file for Public server user

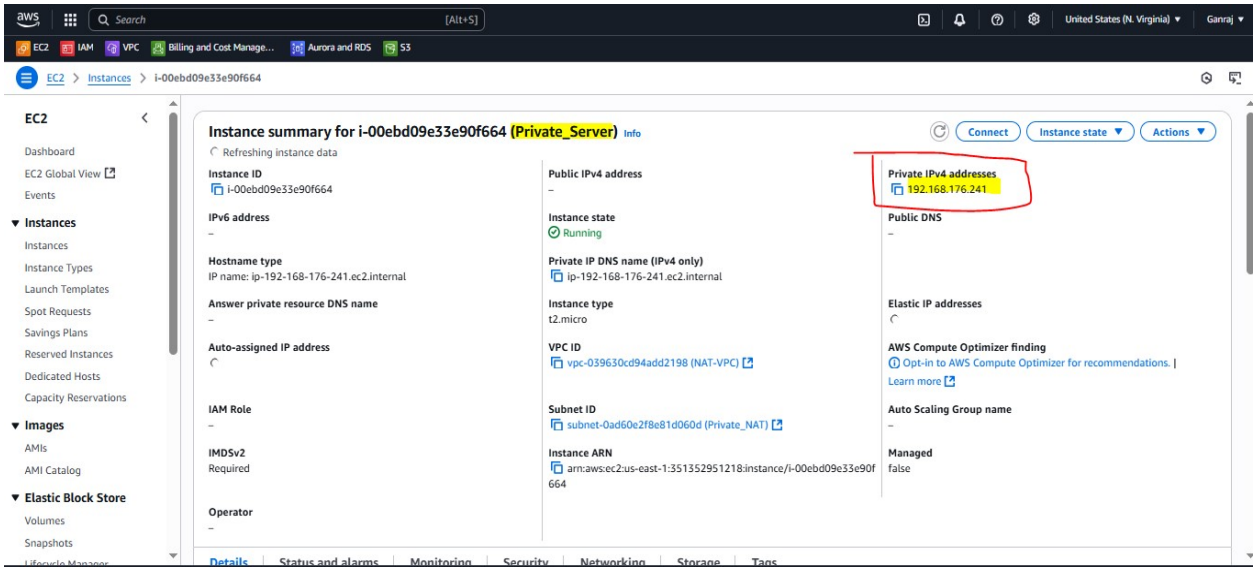
Using : - chmod 400 privatekeyname

chmod 400 Linux.pem



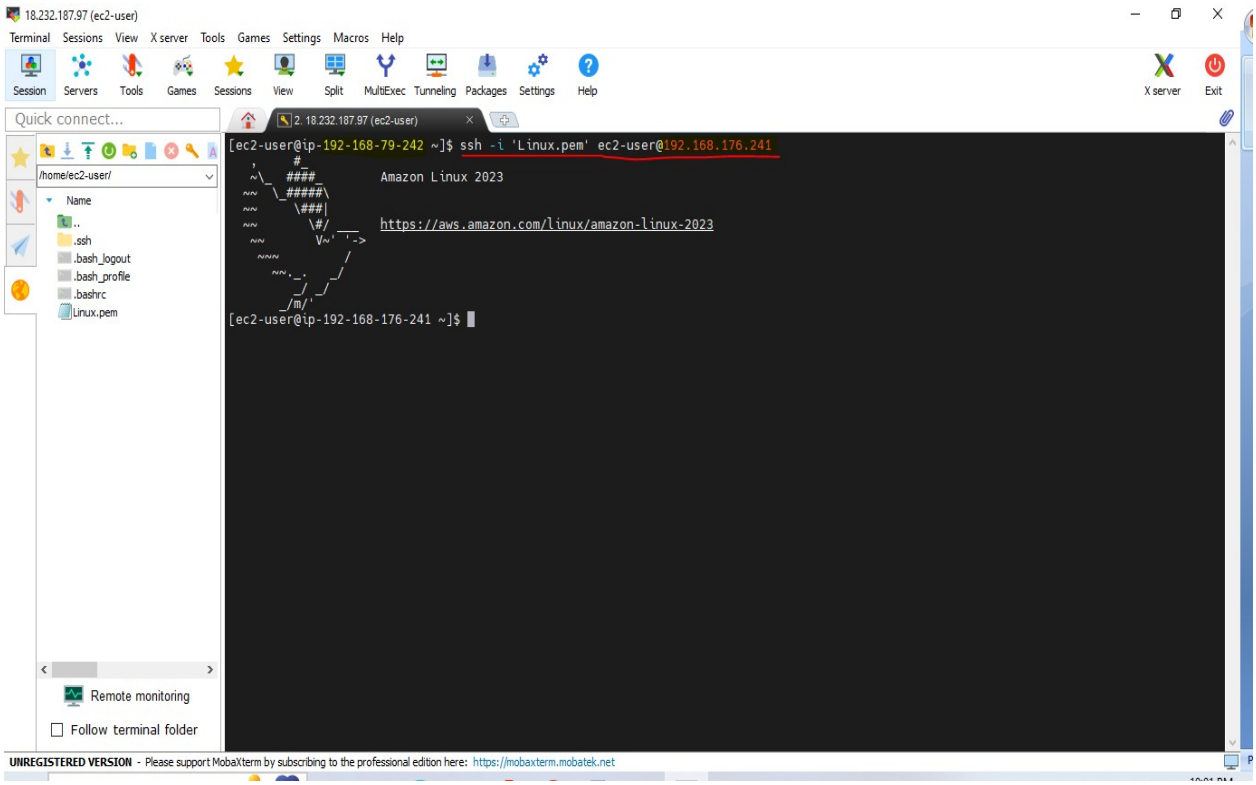
Now use this command to connect private server

ssh -i 'Linux.pem' ec2-user@192.168.176.241

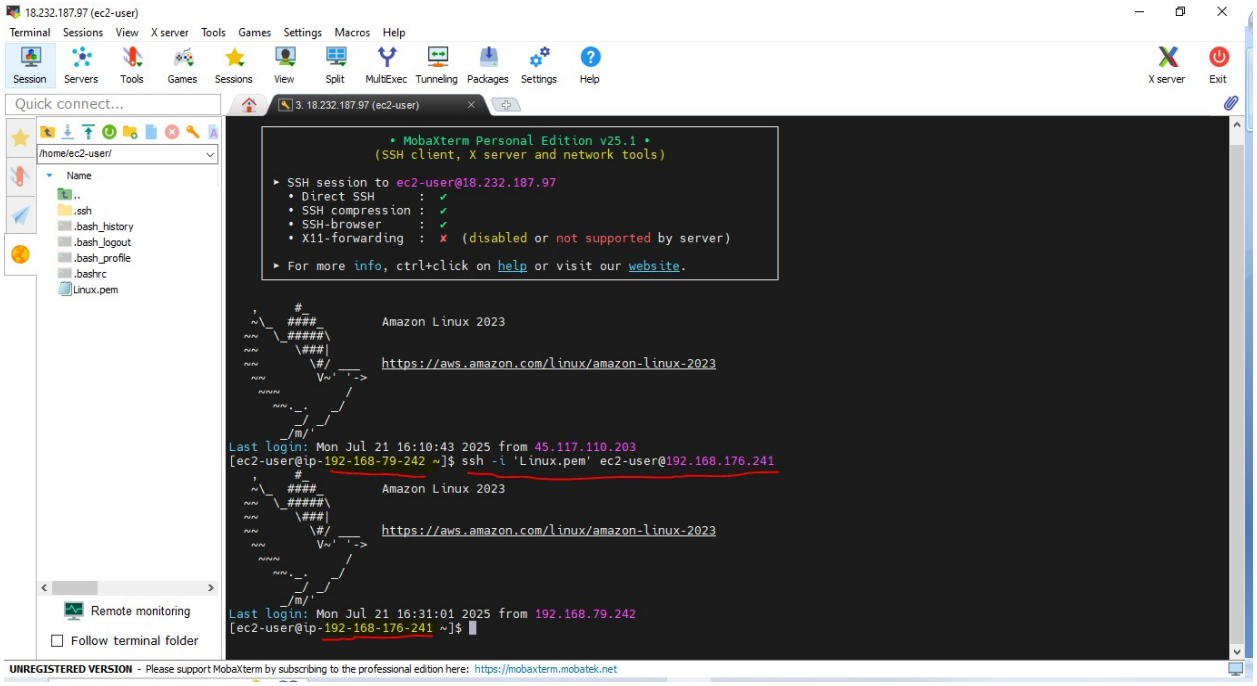


Copying related private IP from Private server Instance and Private key name

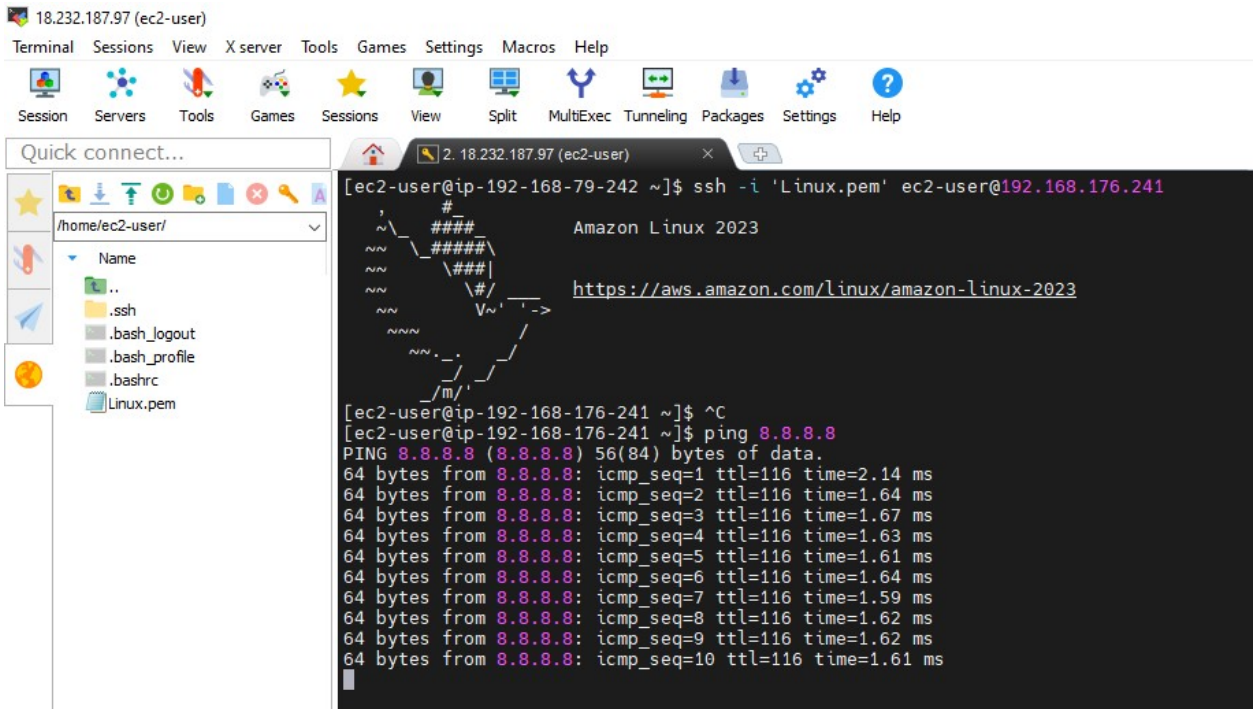
ssh -i 'Linux.pem' ec2-user@192.168.176.241



This screenshot shows reconnection of Private server using Public server



As you can see in the snap we have connected to private server using Public server, Now we will check Internet Access .



See in this scenario we have achieved process of NAT which provides internet access Public Server(EC2) to Private Server(EC2) and The access will provide only through Public Server