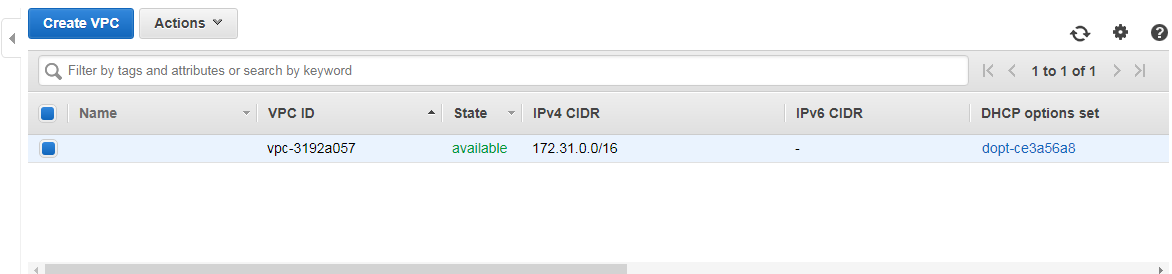
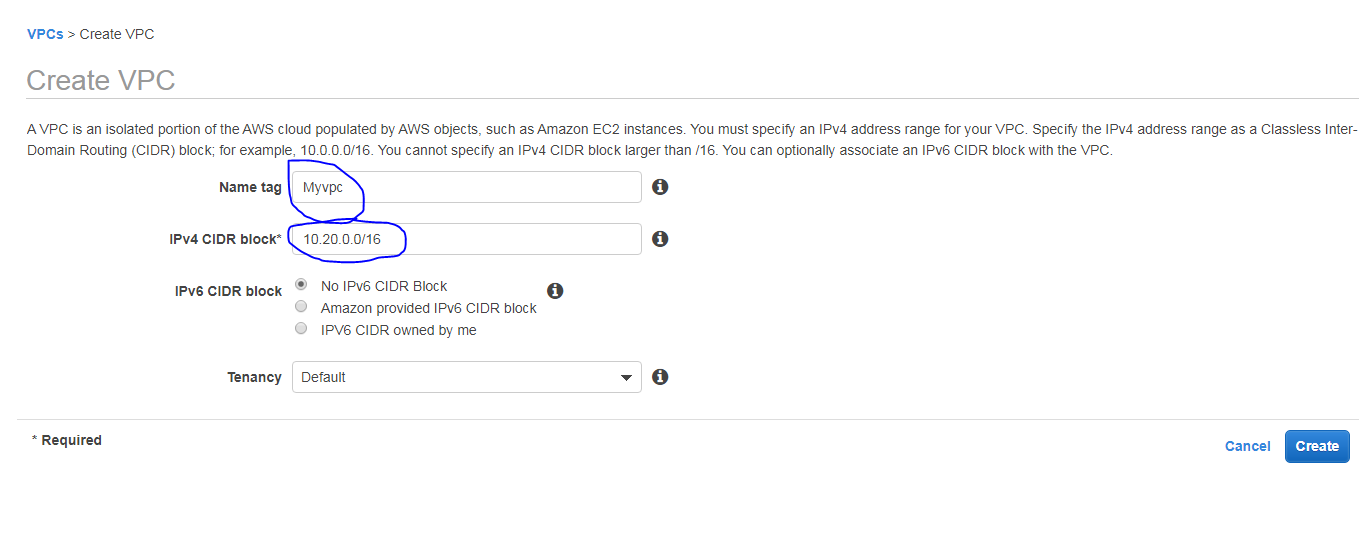
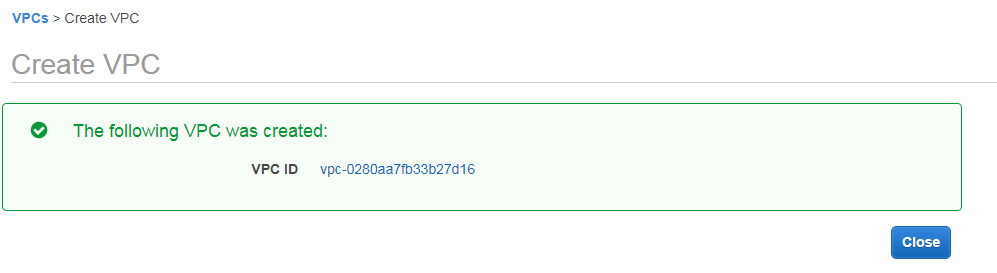
How to create a NAT Instance using Private and Public instance

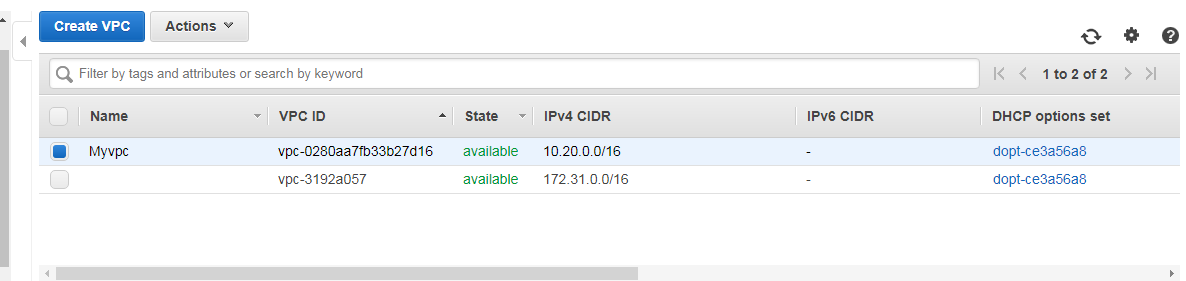
First create a VPC

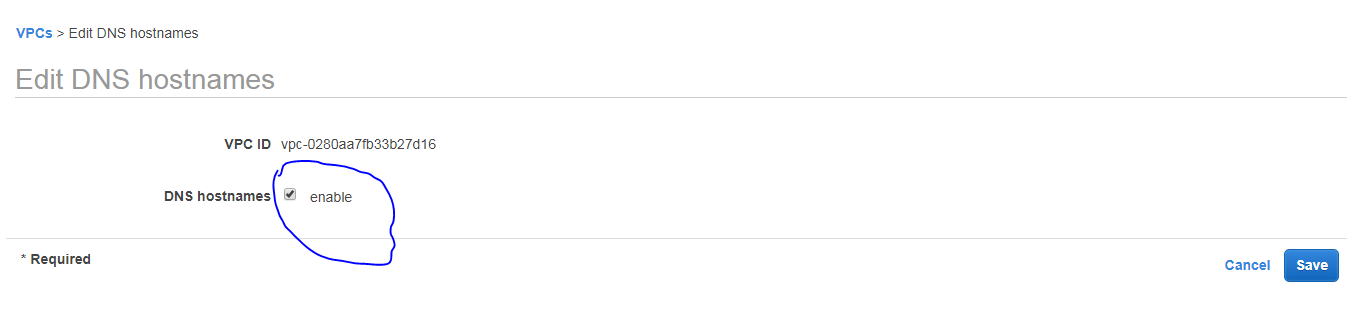
Ex: Myvpc





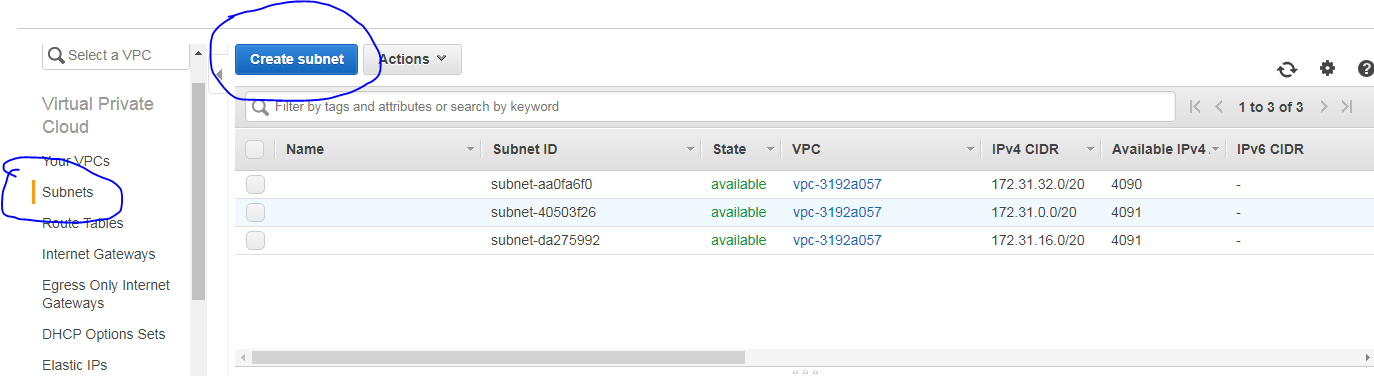


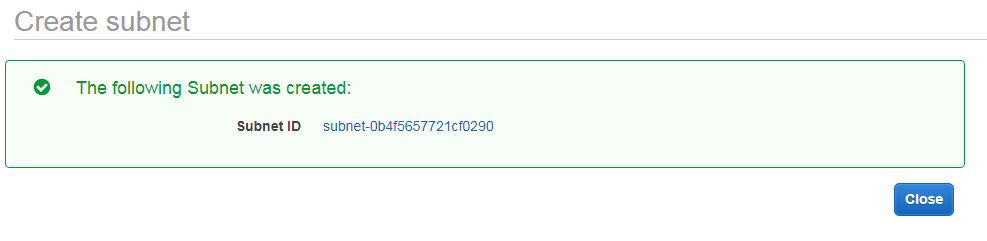
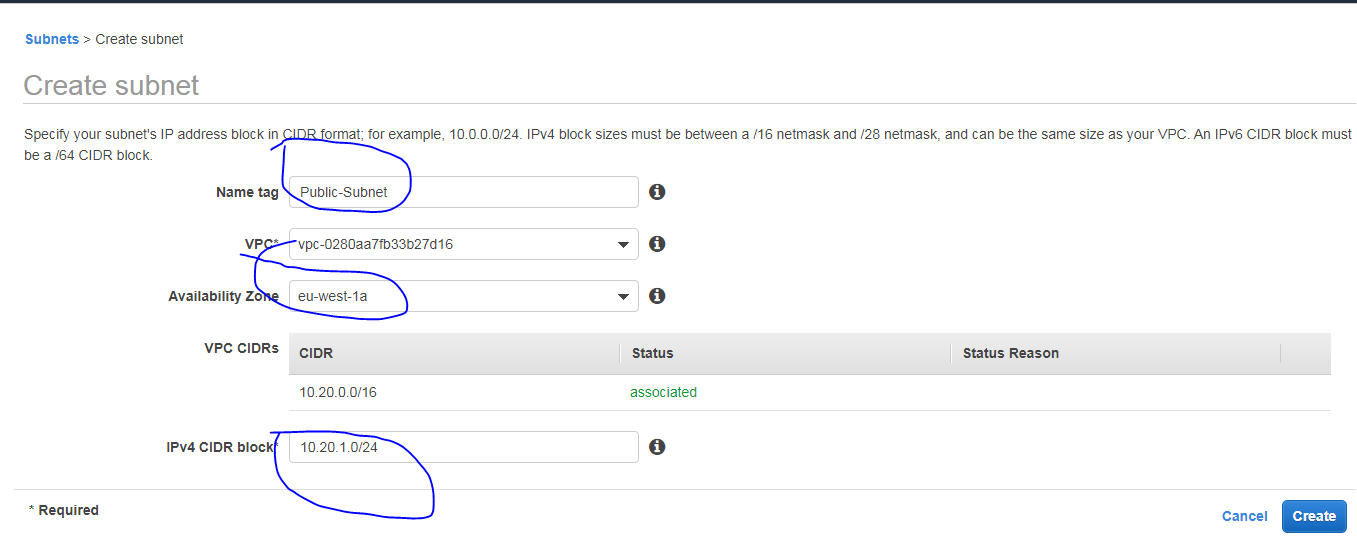




Next we will create two Subnet's called **Public** and **Private** subnet

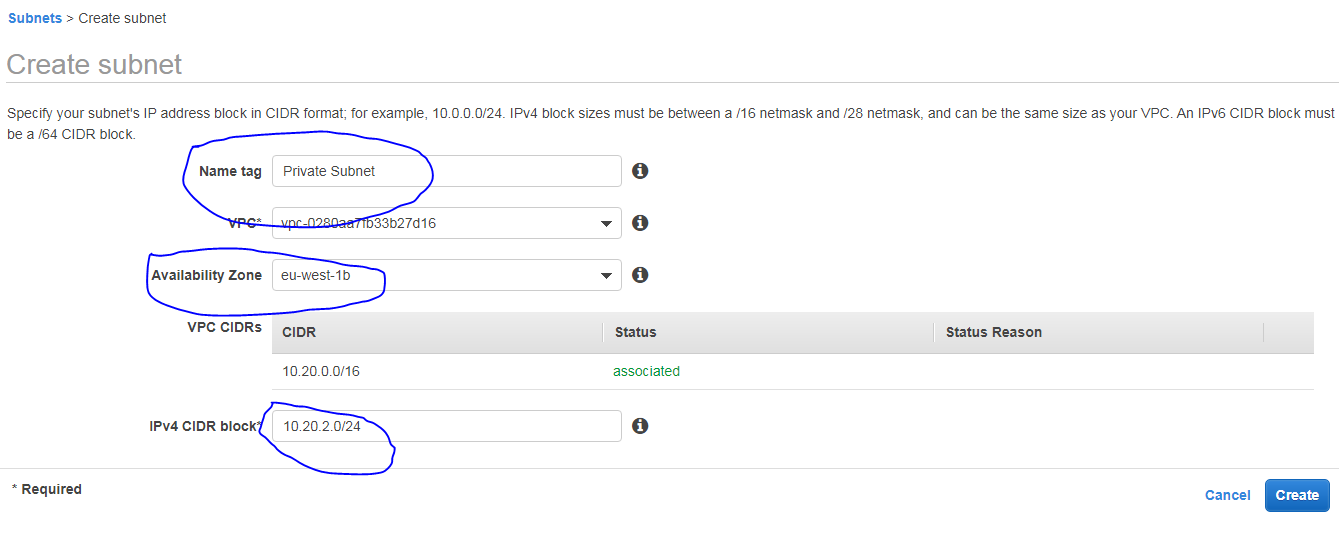
**Public Subnet** : 10.20.1.0/24

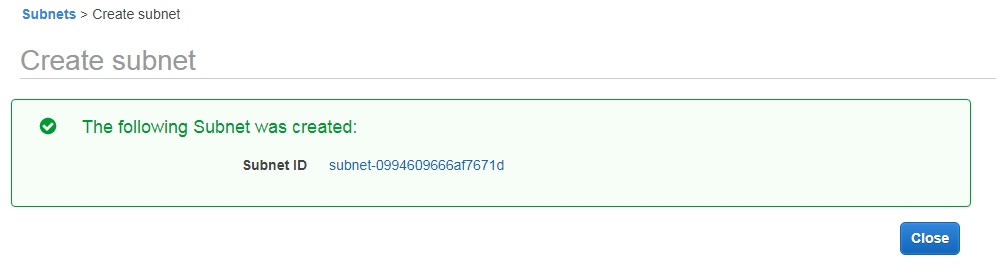


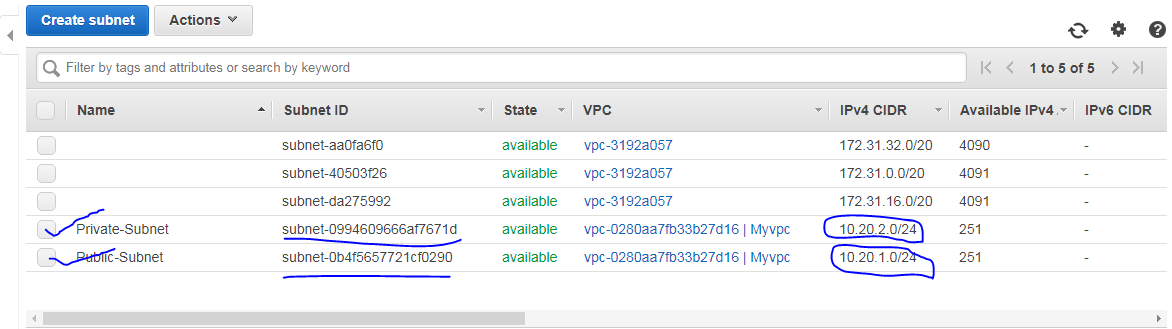


Next we will create a **Private Network**

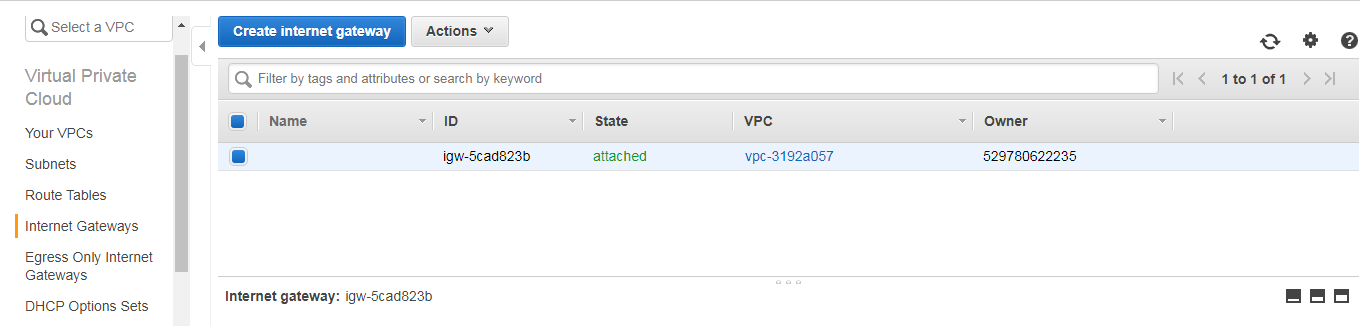
**Private Subnet** : 10.20.2.0/24

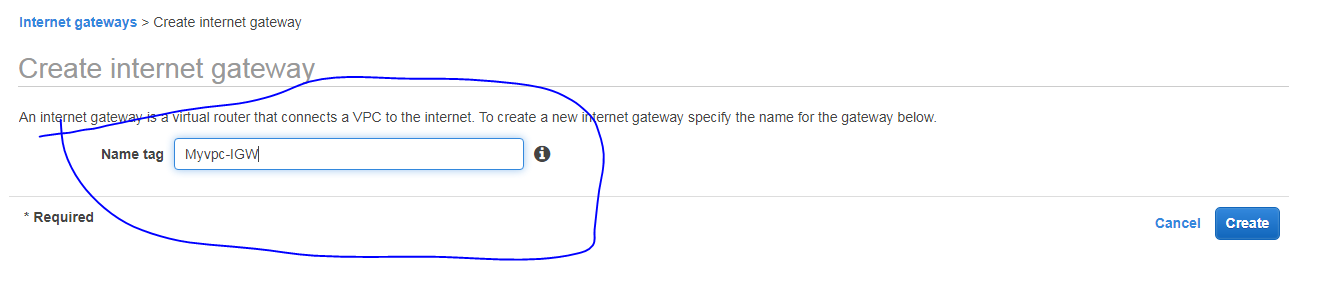


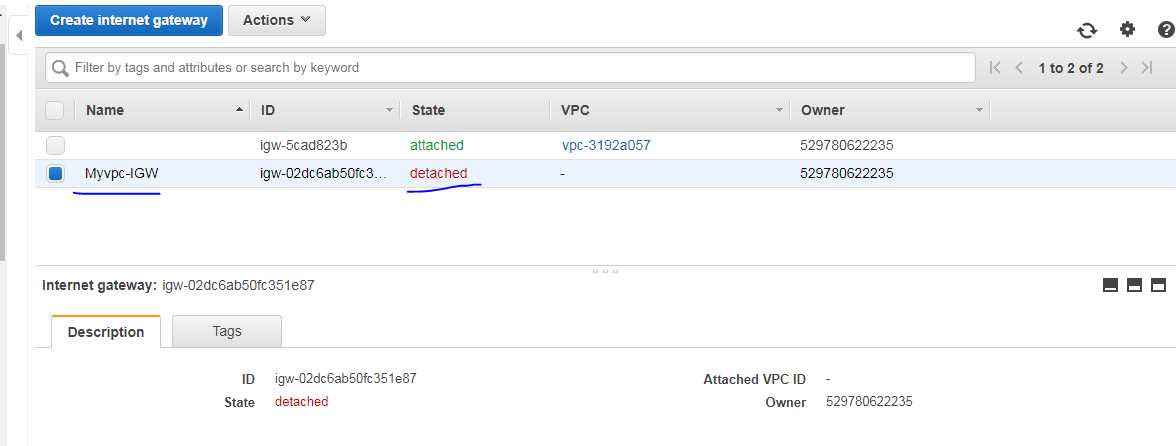


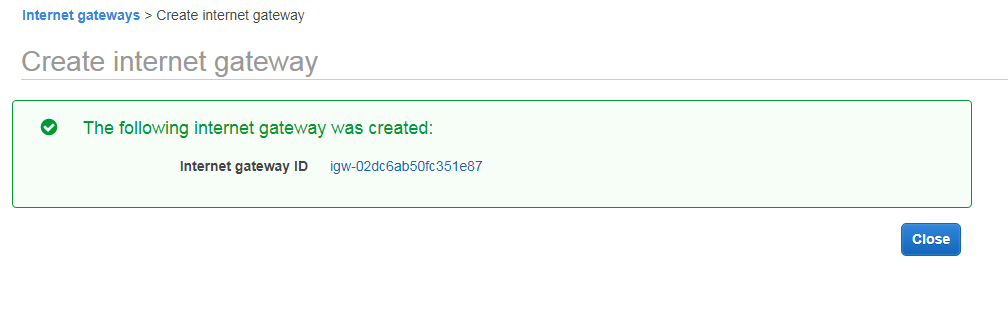


Create an internet Gateway

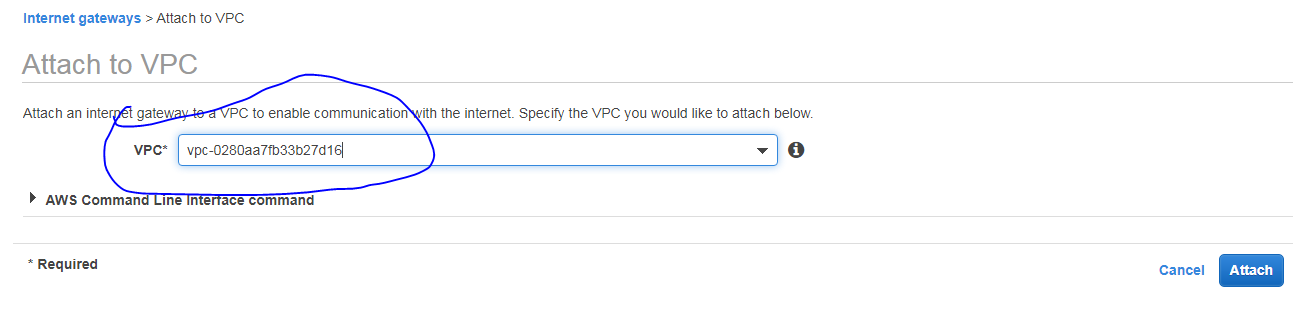


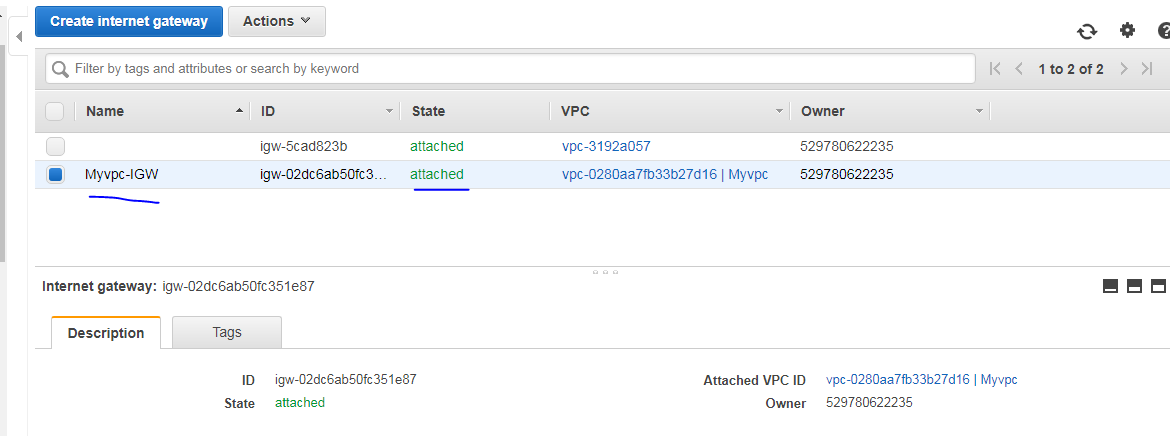






Next we have attach the **VPC** into the internet gateway

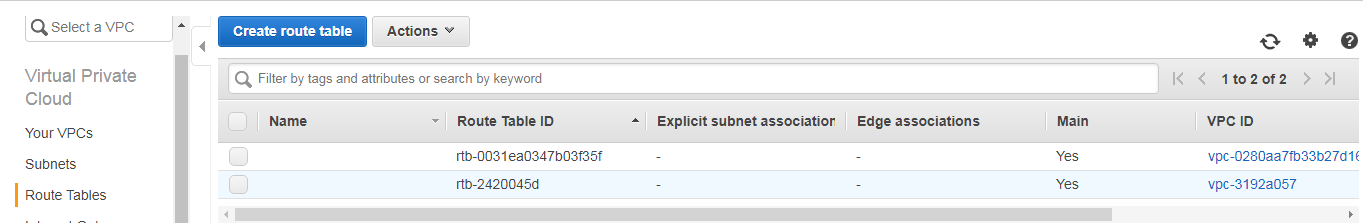


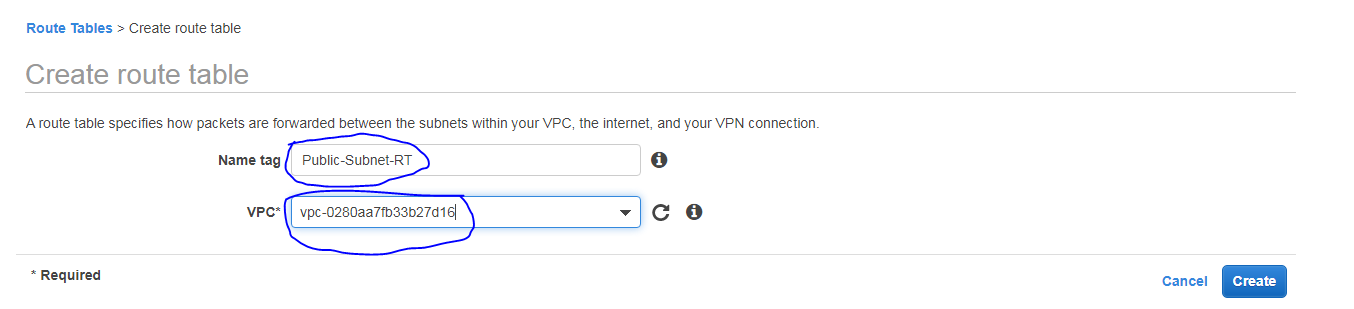


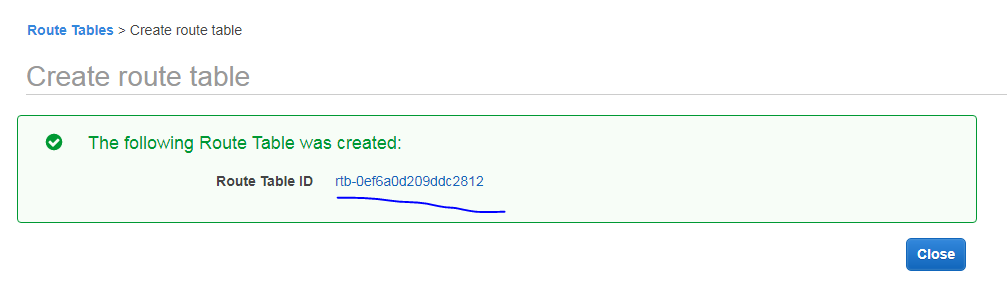
Next we have to create two diff route table for Public and Private subnets using the below naming standards,

Public-Subnet-RT

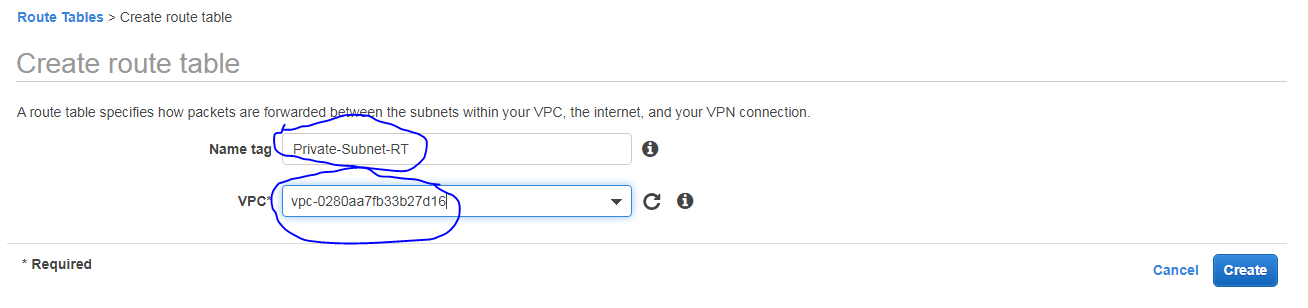
Private-Subnet-RT

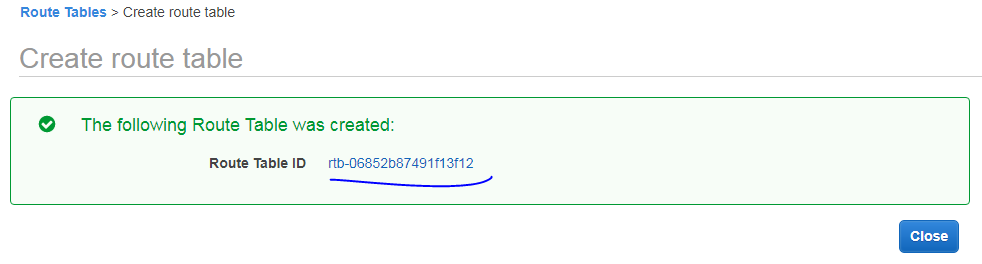


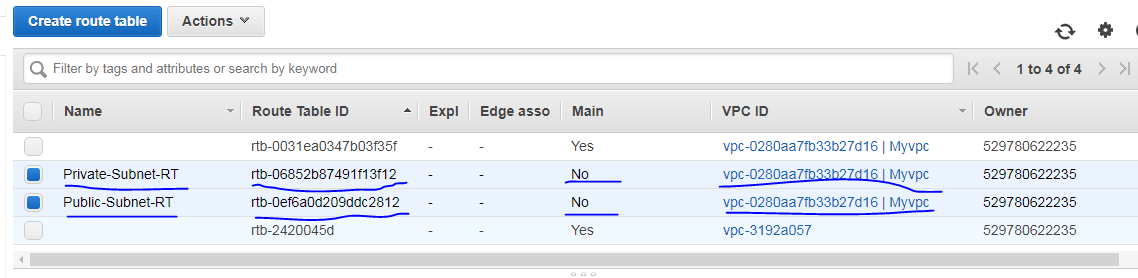




Next create Private Route table





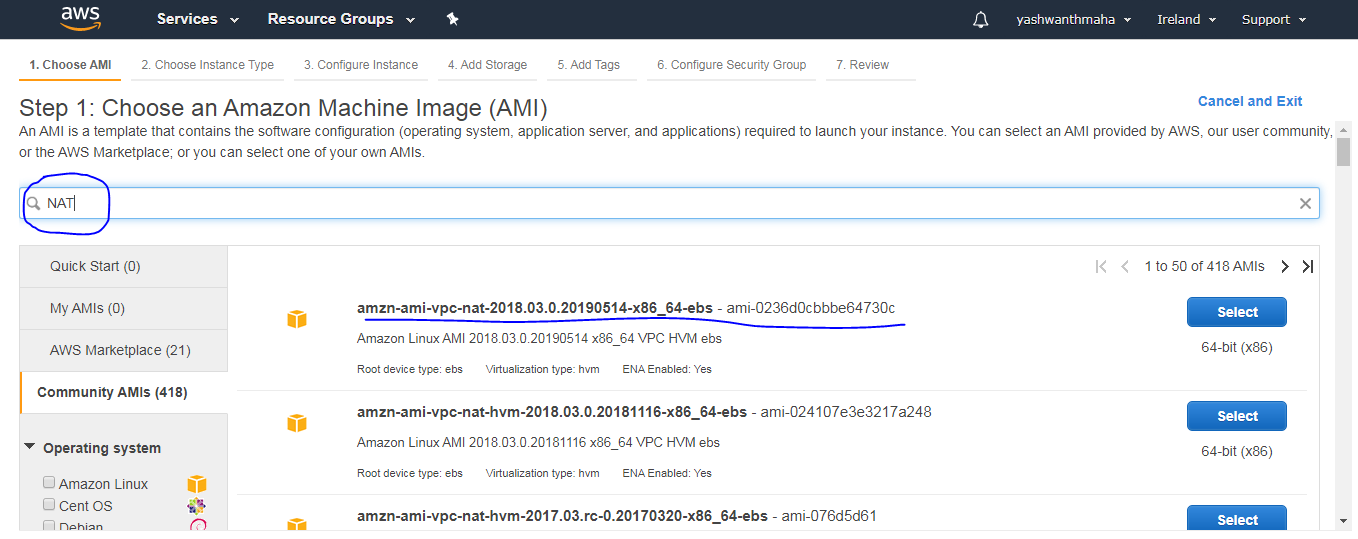


Next we have to create **three Linux ec2** instance

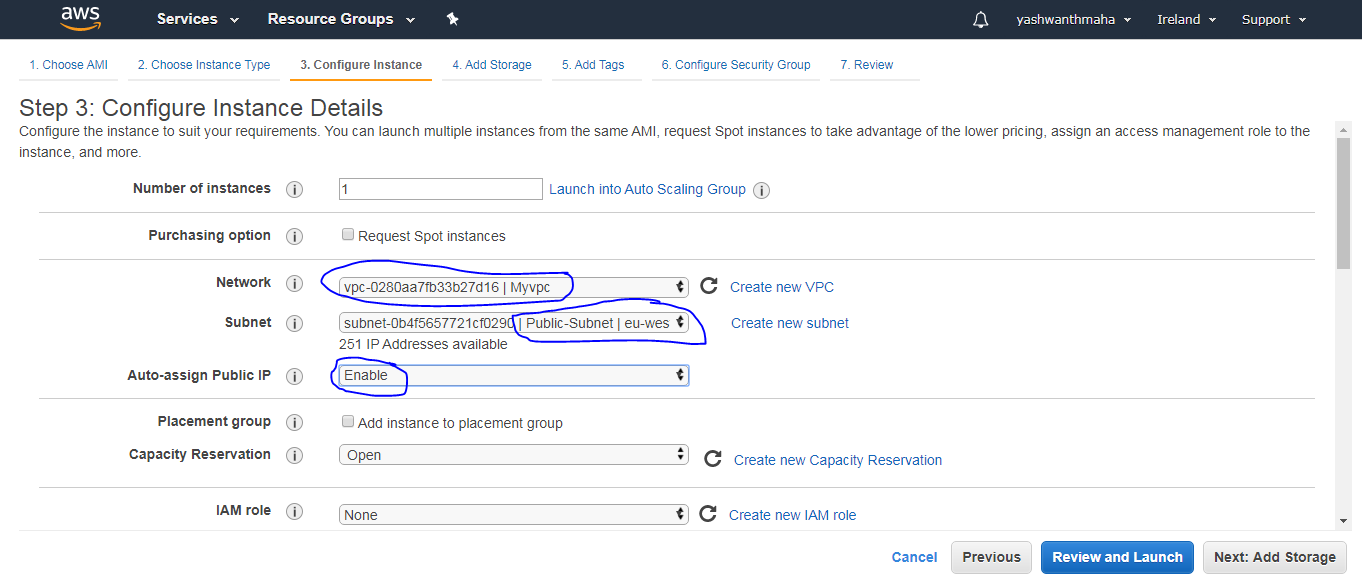
**NAT** =1 EC2 |**Public-Subnet-Instance** =1EC2

**Private-Subnet-Instance**=1EC2

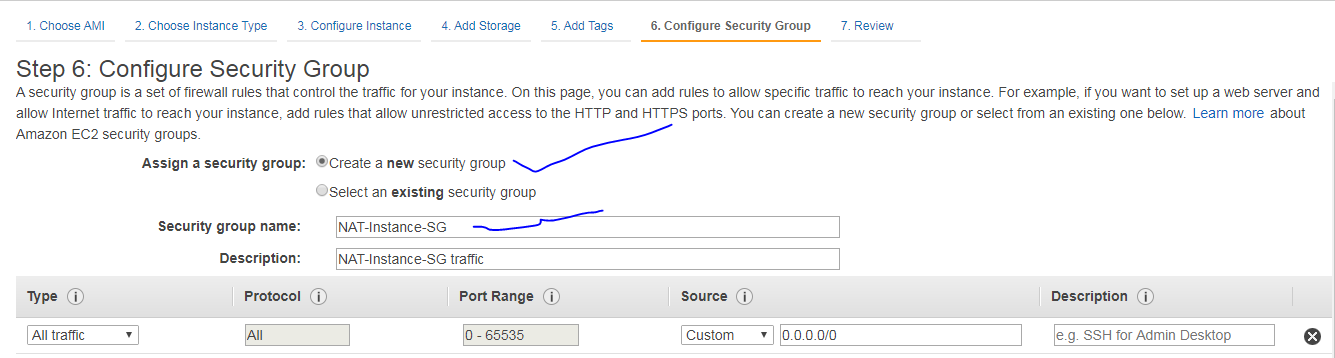
**NAT instance creation**



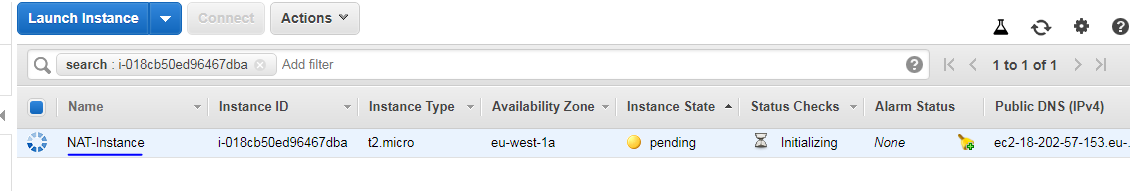


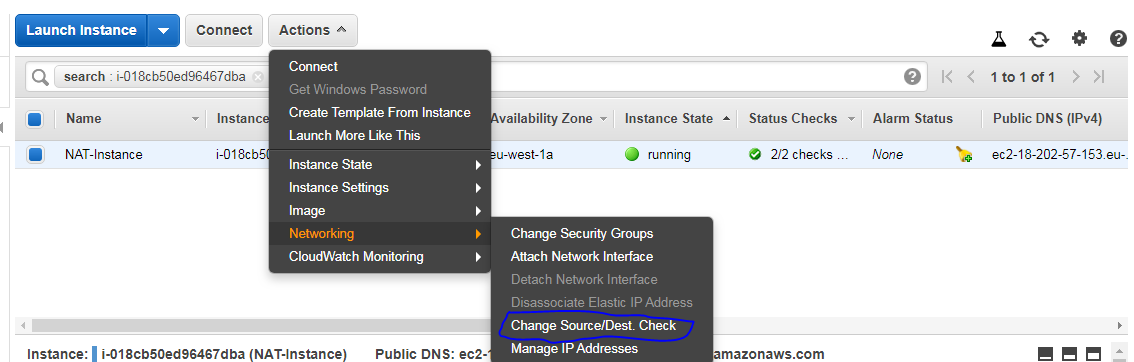


Select you **VPC** and it should be **Public Subnet** and assign the Public for the **NAT instance**. Once instance create you have to **disable source and destination check** = disable.

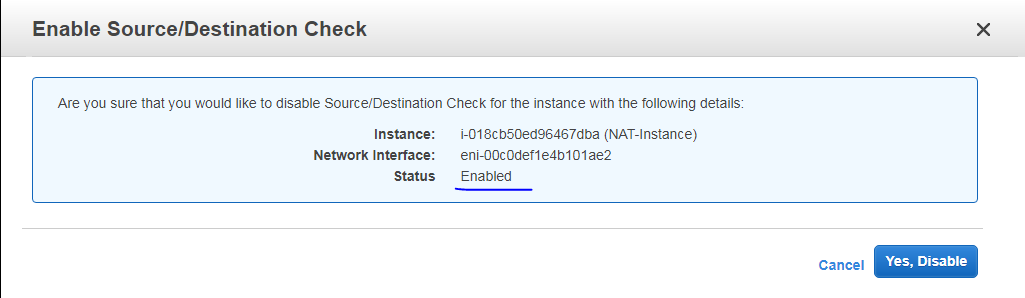


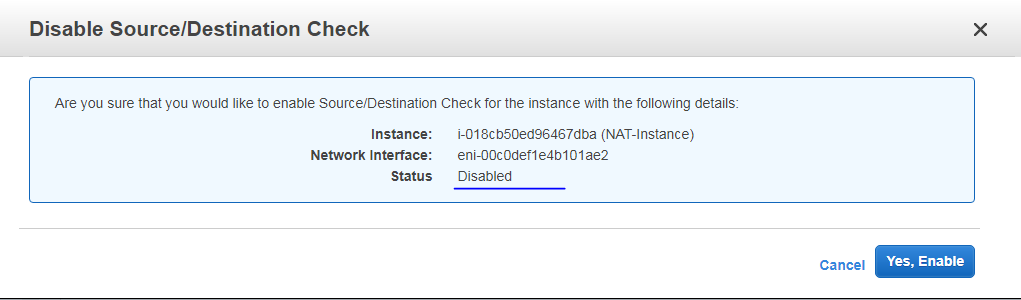
Created a new security group for the NAT instance.



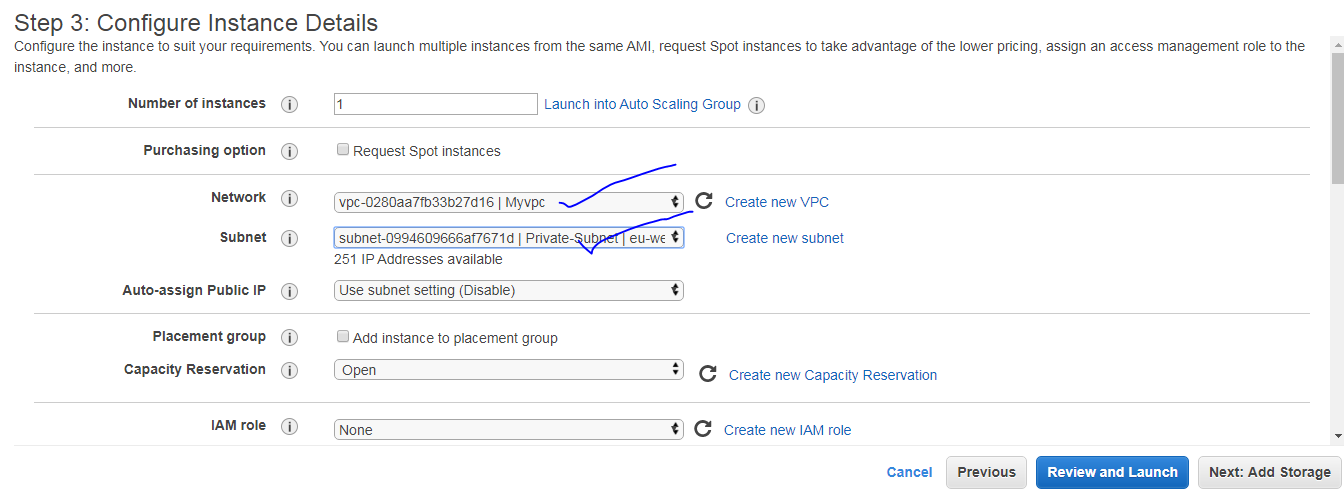


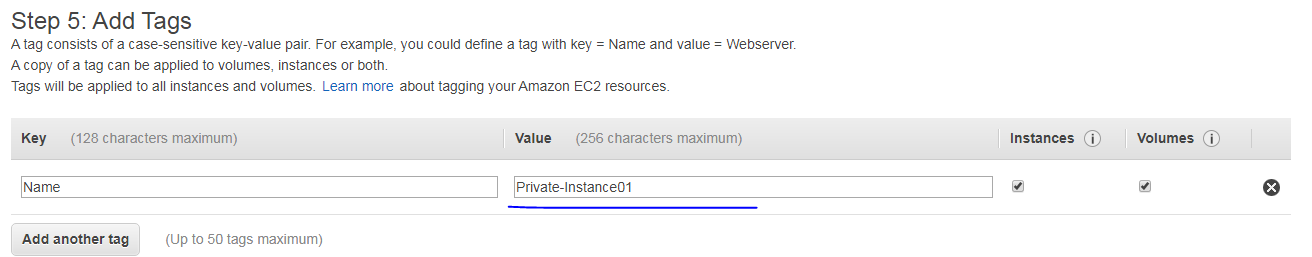
By default is enabled we have to make disable





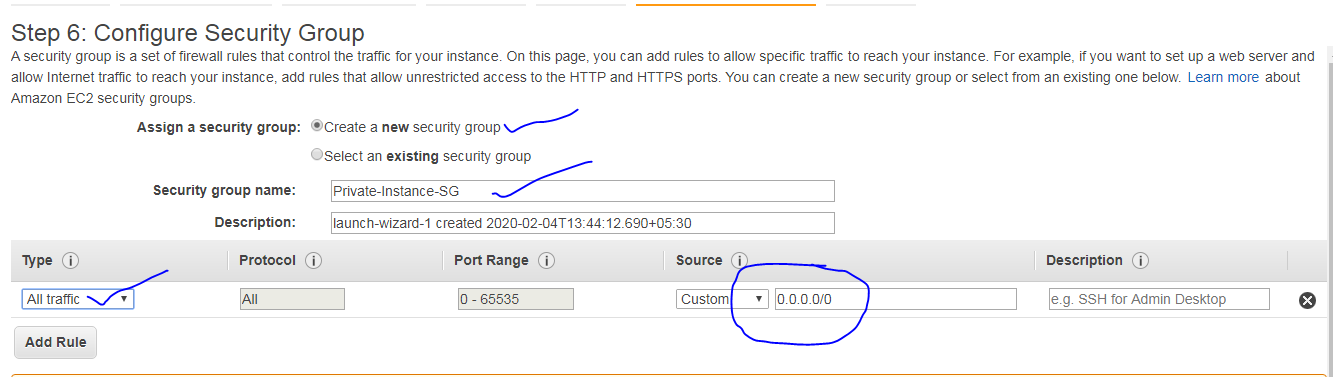
Create two more ec2 instance , one is private subnet and another one is public subnet

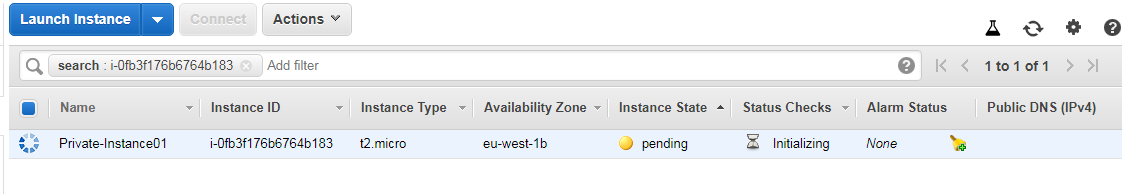




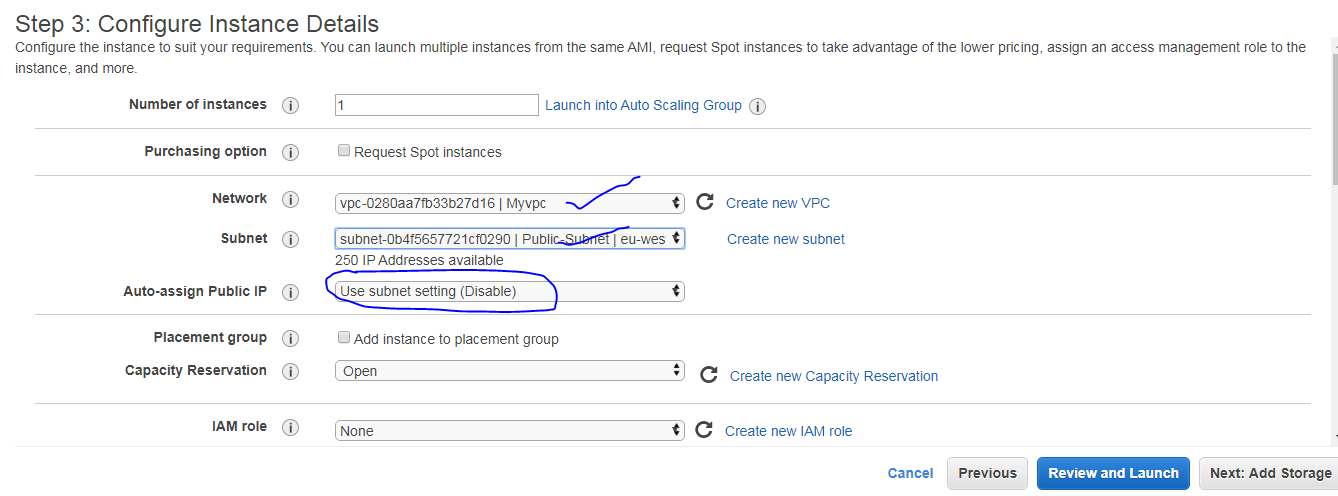
Create private instance as given below vpc and subnet and no public ip

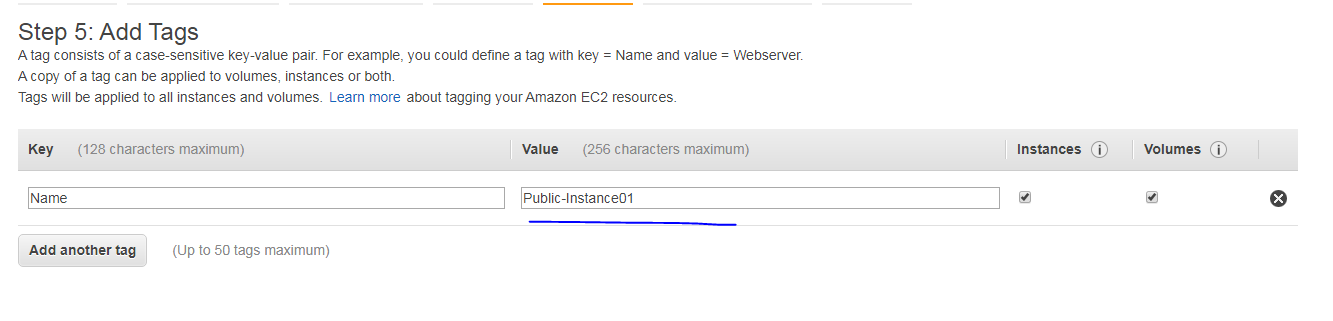
and all traffic but should not change source 0.0.0.0/0 , leave it the default source.

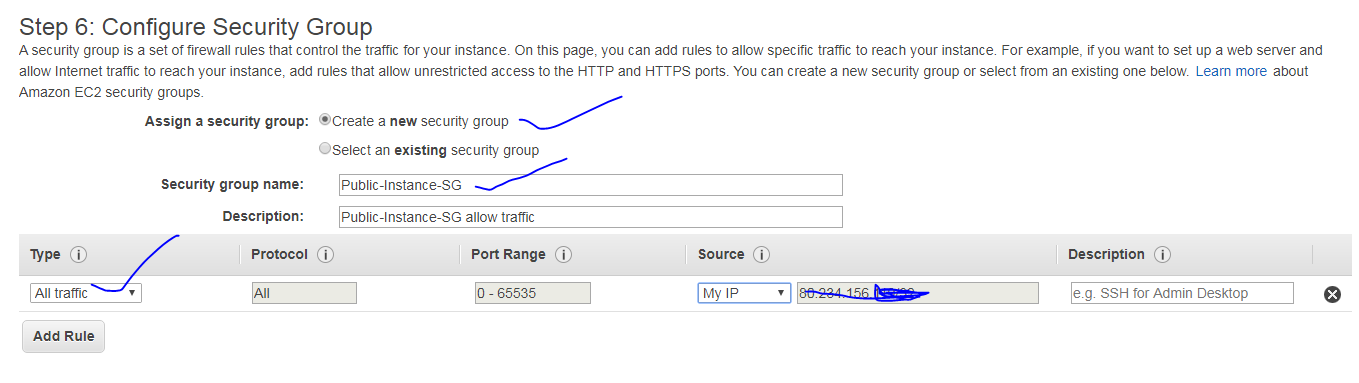


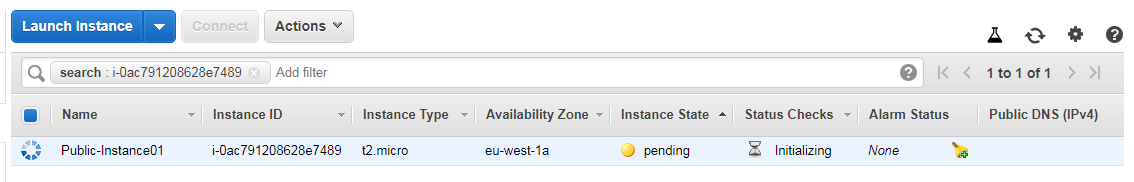


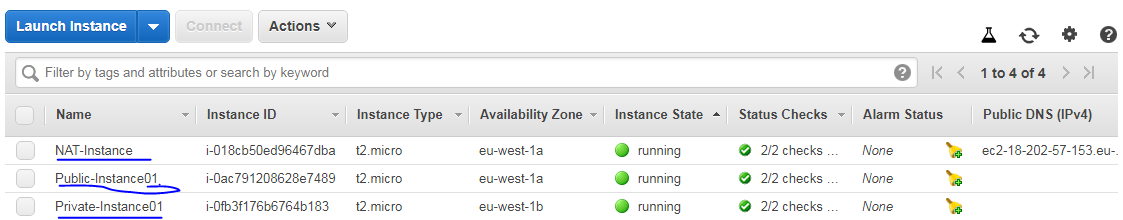
Create a public instance using the below descriptive way,





Create a new security group for public instance as given below

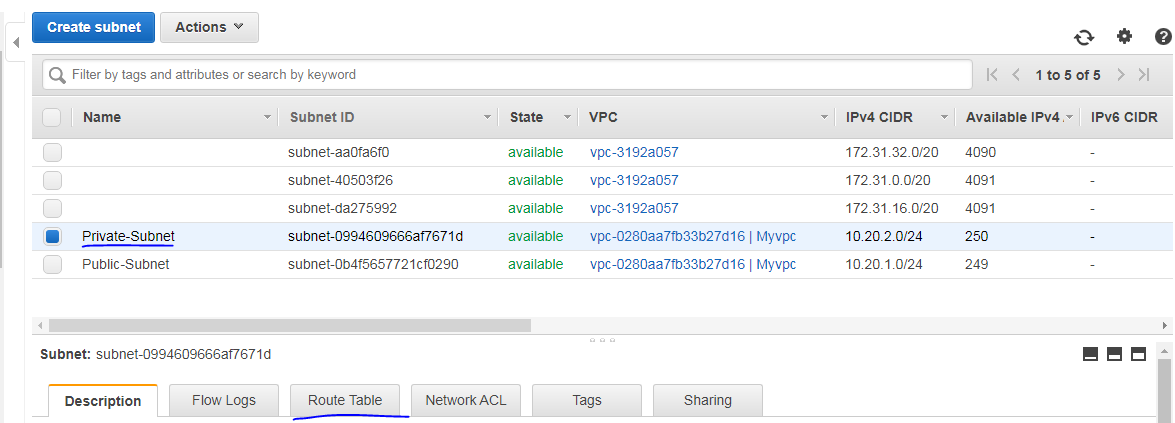


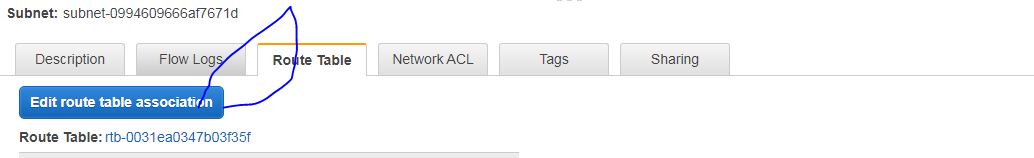


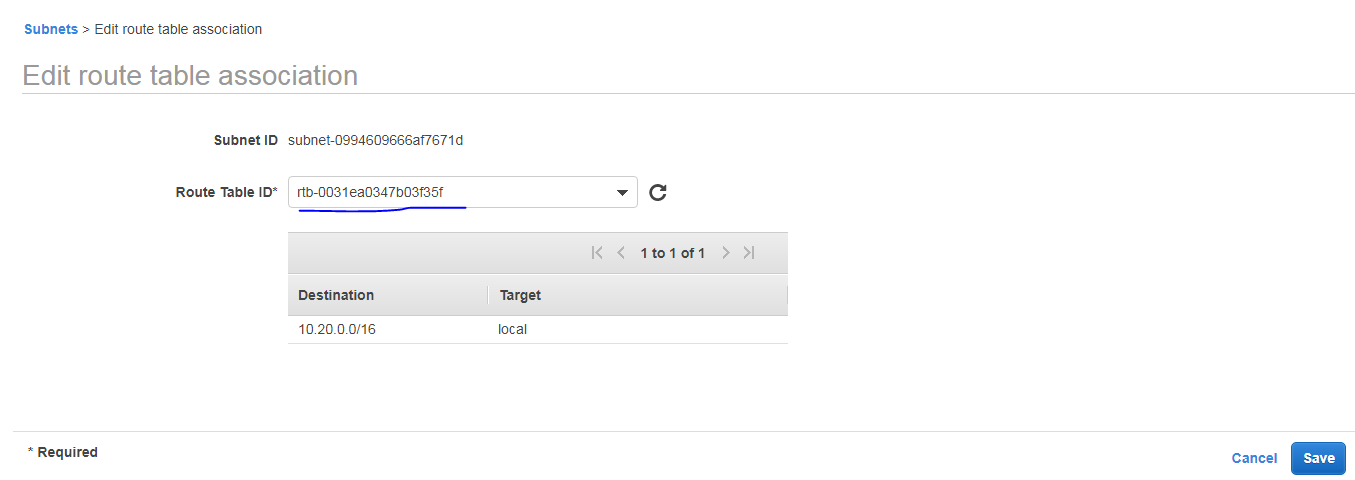
Now , associate the **route tables** in the **respective route tables**

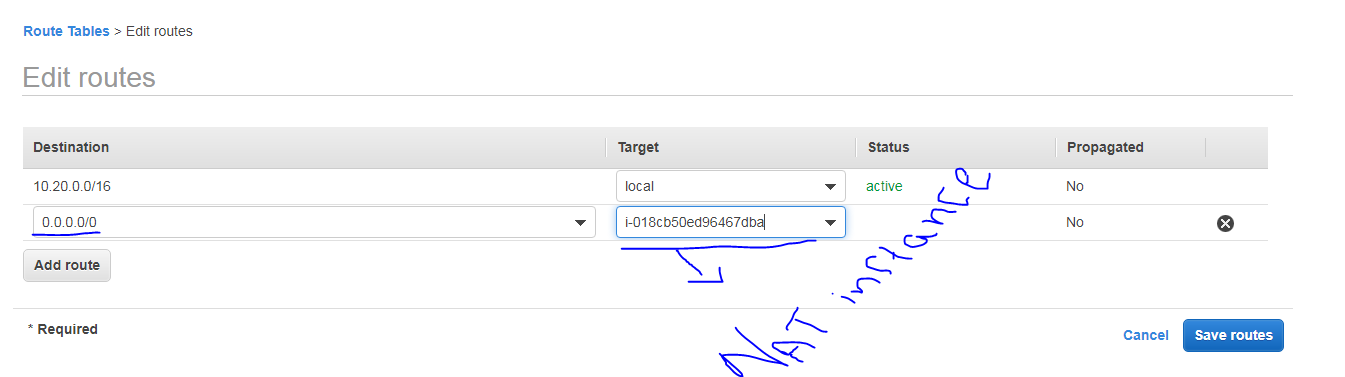
Private route table = **NAT instance**

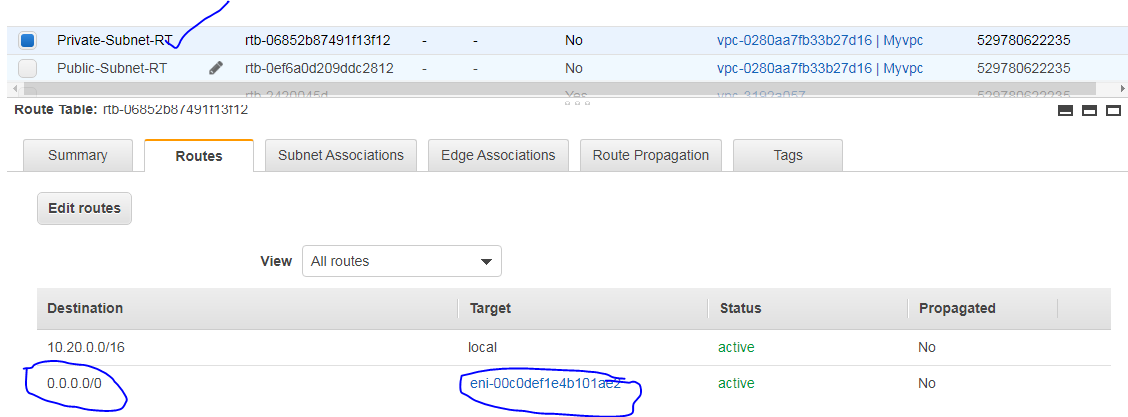
Public route table = **IGW**



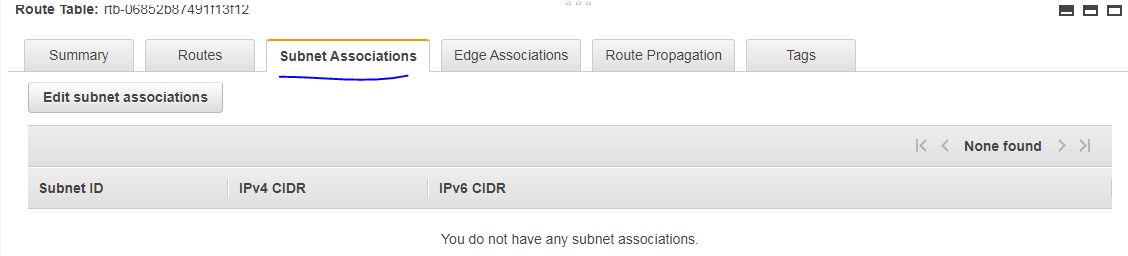


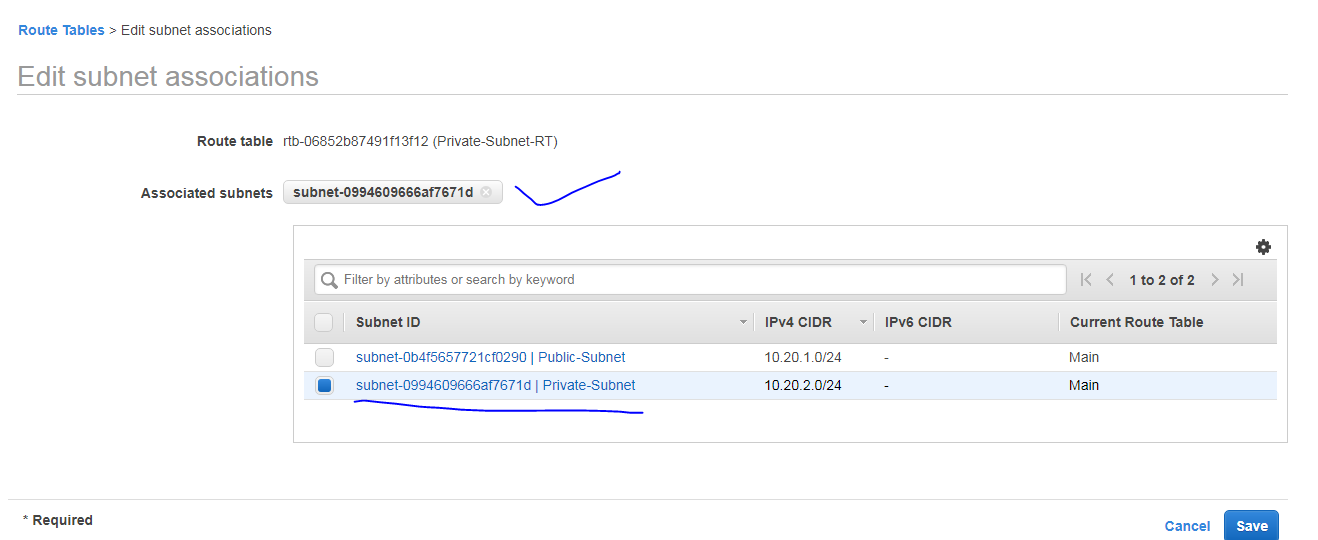


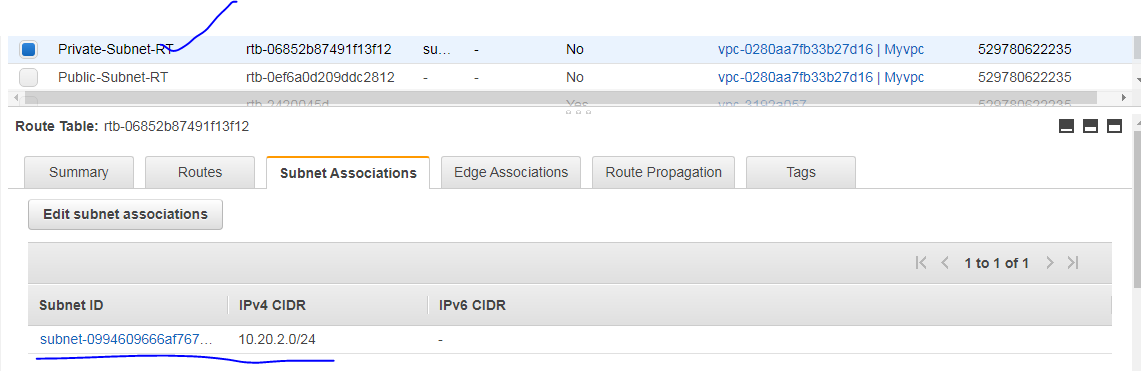




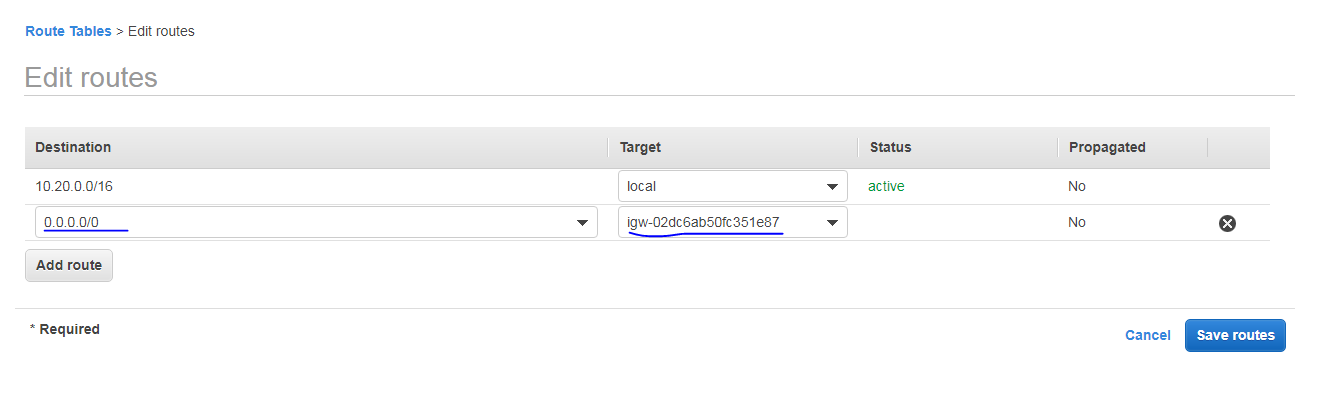
Next associate the private subnet in the next section,

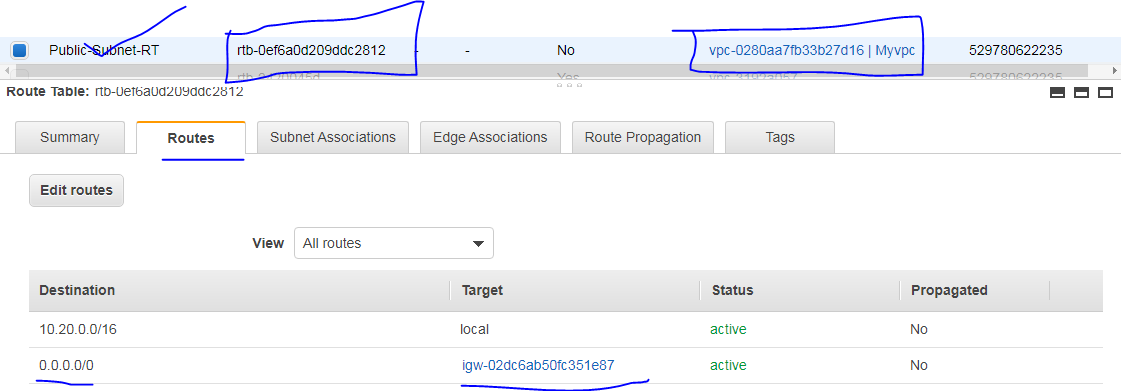


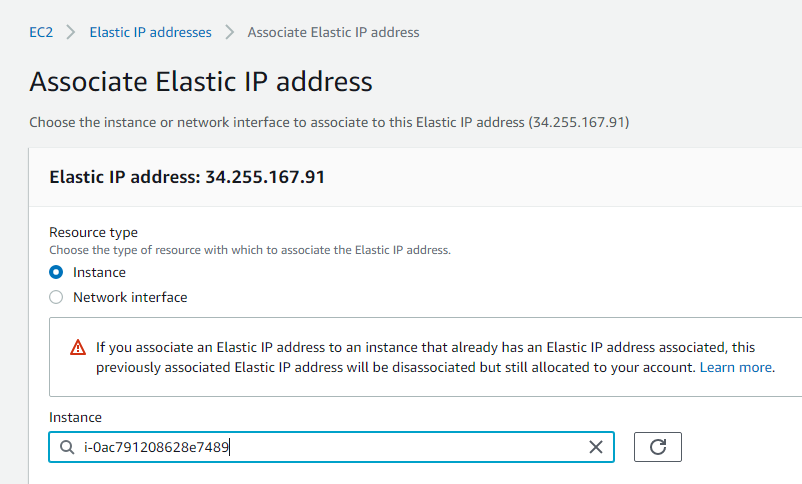


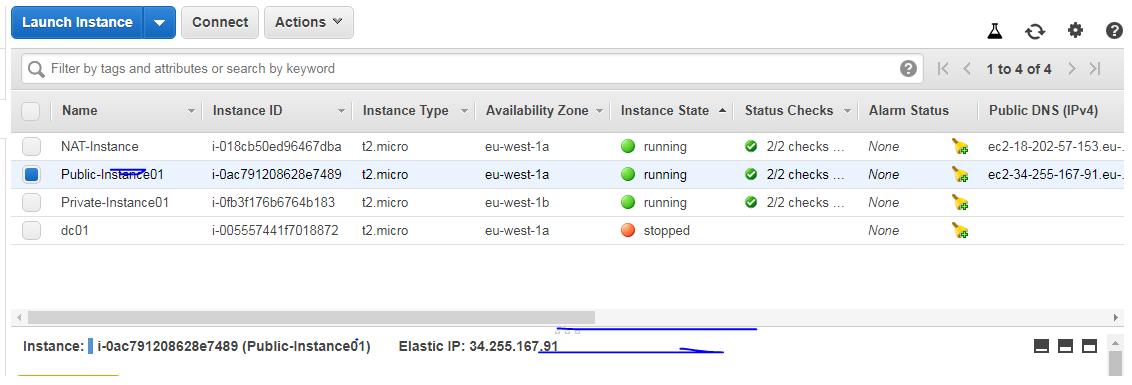


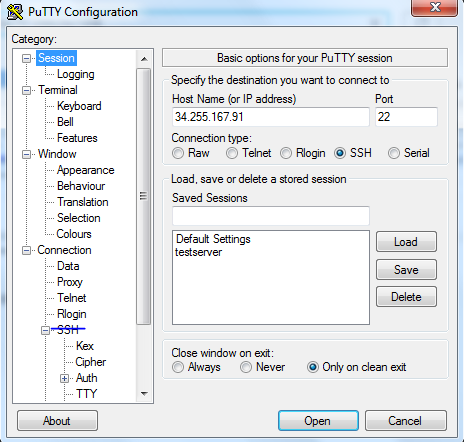
For public subnet we have to select the IGW



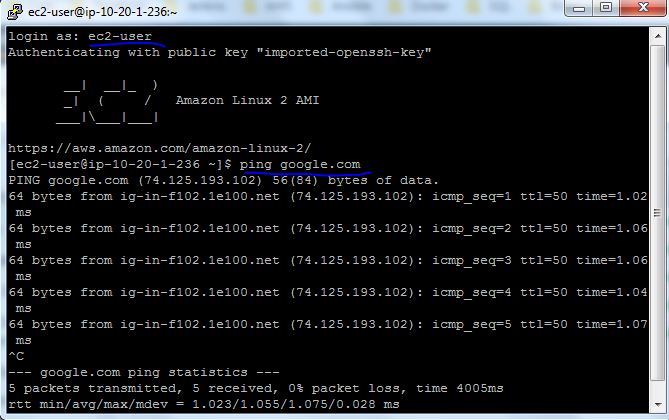


Assign the EIP into the public instance 



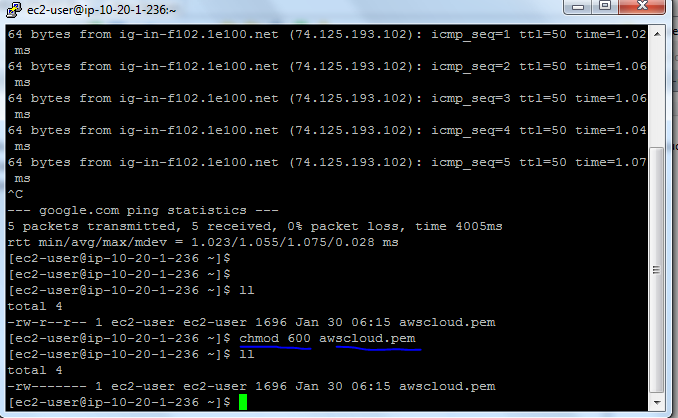
Connect the public instance using the EIP using putty

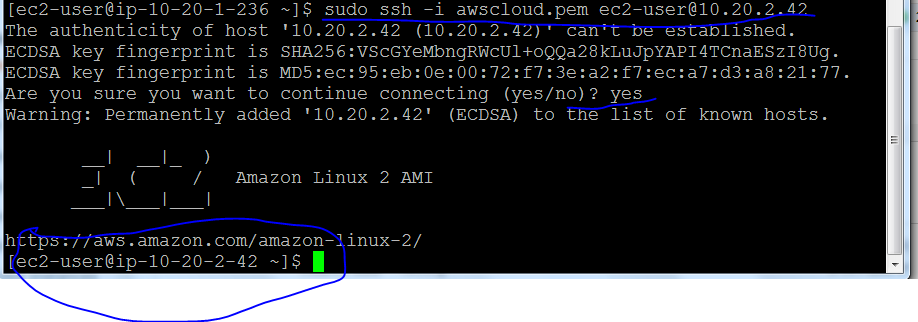
SSh >> select auth and select your .ppk file there



Next connect the private instance , first login the public instance and connect using ssh,

syntax: sudo ssh -i XXXXXXXXXXXpemkeyfileXXXXXXXXXX ec2-user@XXXXXXXXXXXXXipadress(private)





next we will ping google.com in the private instance, you will get the internet connection via NAT instance . This is what we will get the private instance internet and patching and other actives...