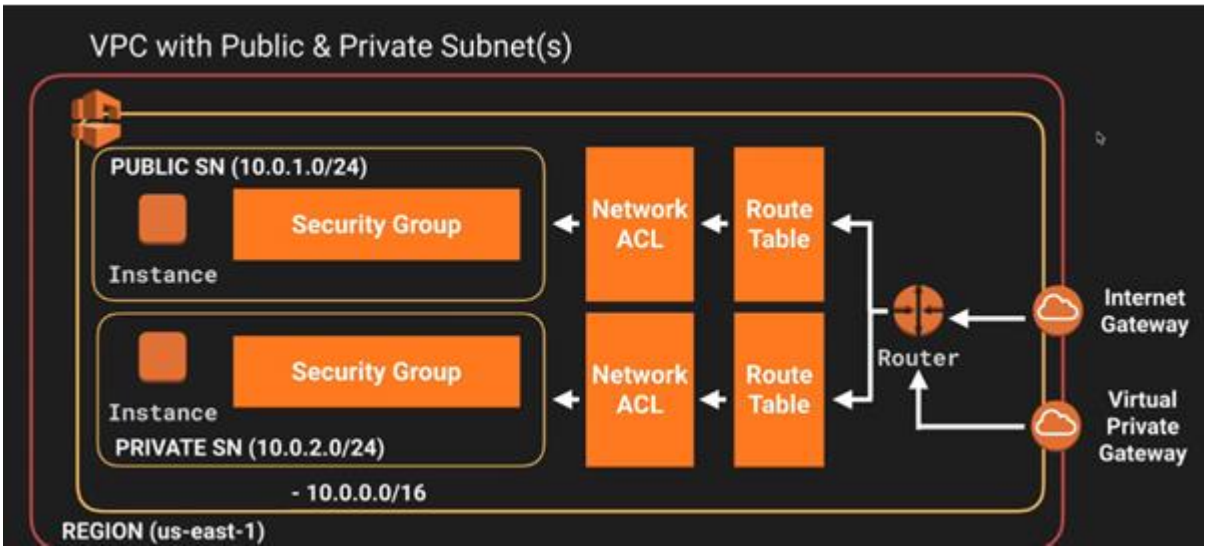
AWS Quick Start Guide: Amazon Virtual Private Cloud Documentation

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch Amazon Web Services (AWS) resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

The following are the key concepts for VPCs:

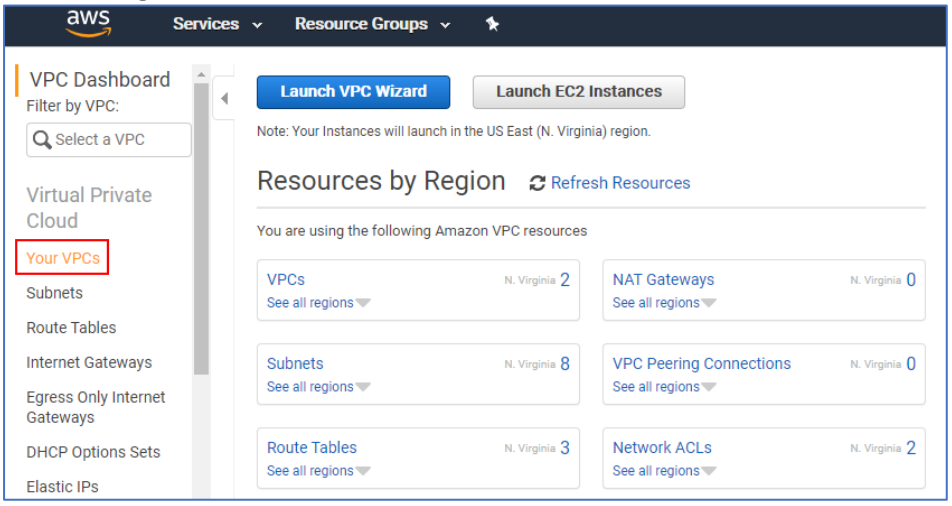
- A *virtual private cloud* (VPC) is a virtual network dedicated to your AWS account.
- A *subnet* is a range of IP addresses in your VPC.
- A *route table* contains a set of rules, called routes, that are used to determine where network traffic is directed.
- An *internet gateway* is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet. It therefore imposes no availability risks or bandwidth constraints on your network traffic.
- A *VPC endpoint* enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by Private Link without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.



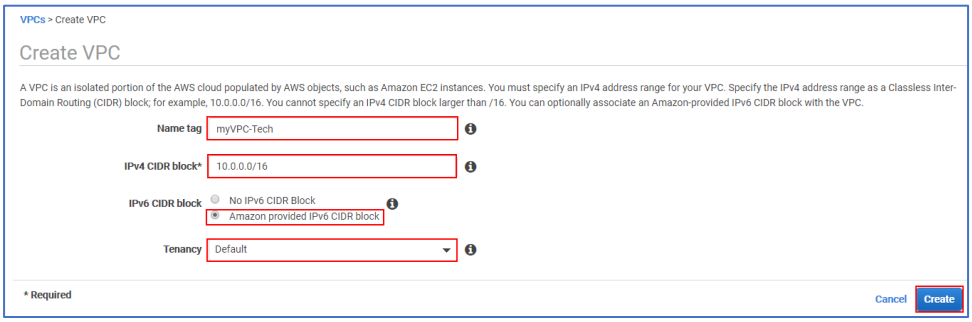
Accessing Amazon VPC

You can create, access, and manage your VPCs using any of the following interfaces:

1. **AWS Management Console – VPCs. -> Your VPCs**



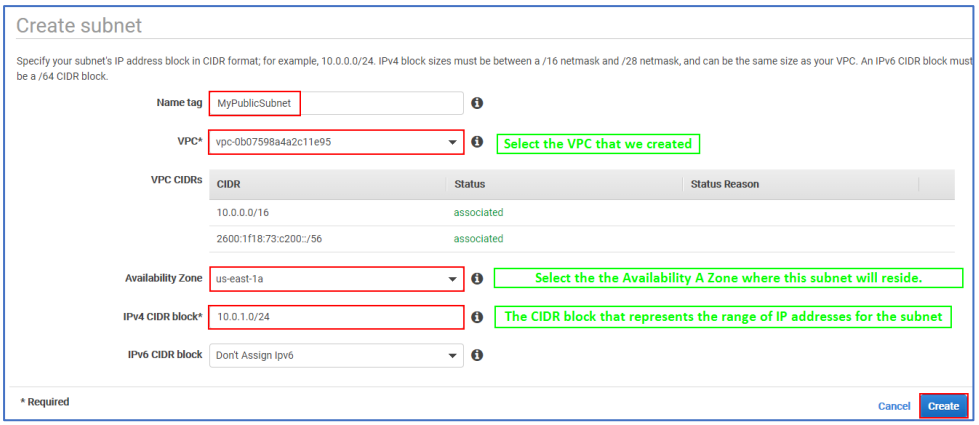
2. Create VPC as below:



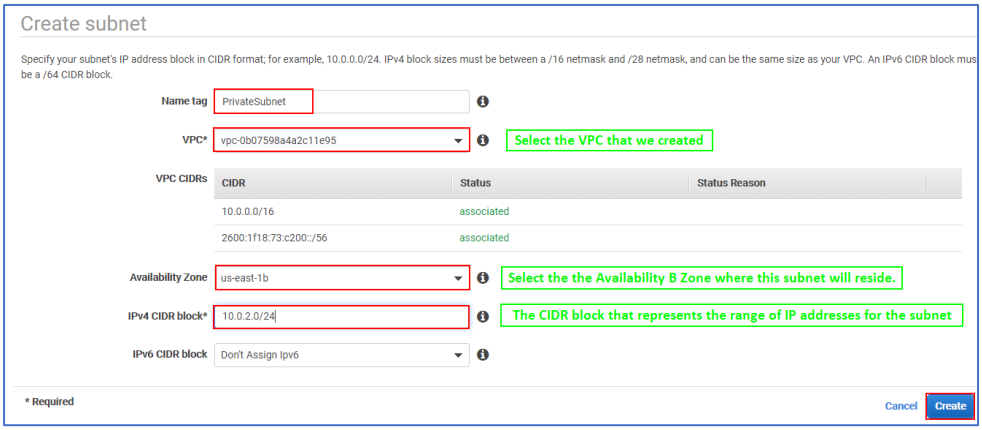
Note: Route tables, NACLS, security groups are created by default after creation of VPC

3. Now we can create two Subnet -> 1) PublicSubnet 2)PrivateSubnet

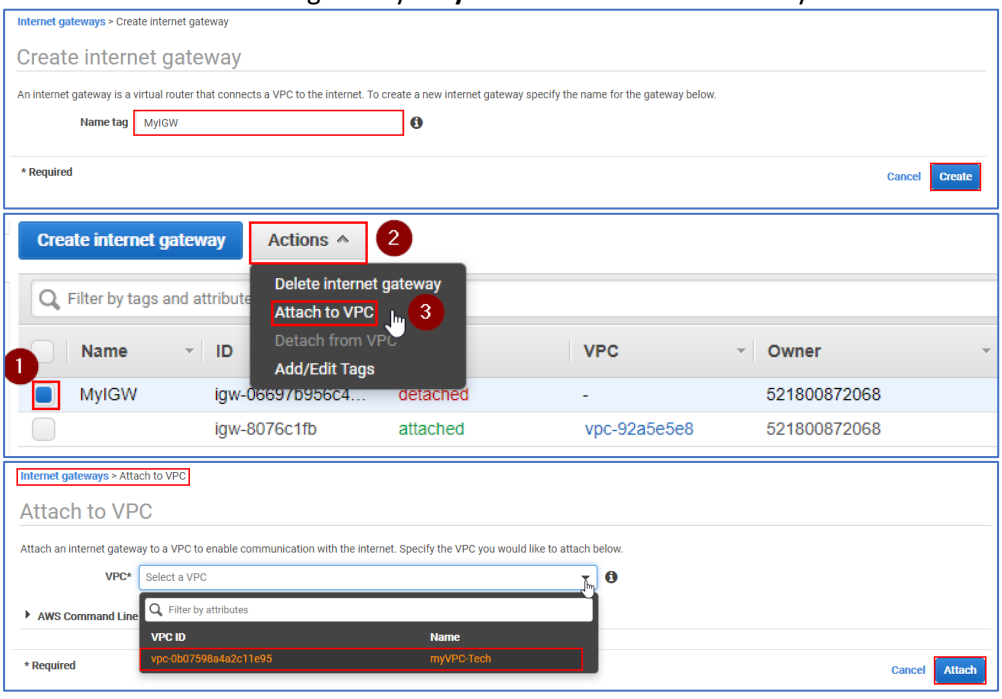
PublicSubnet



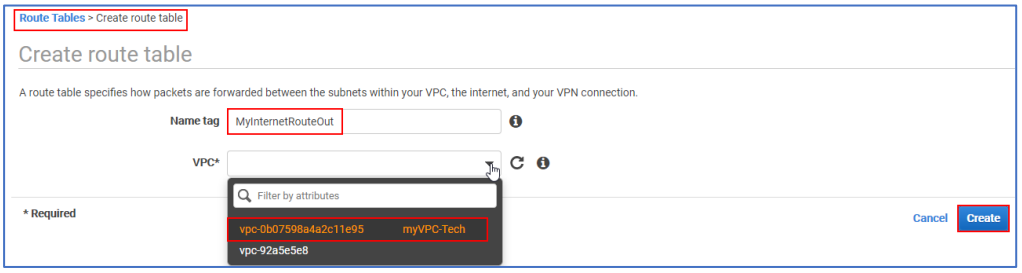
PrivateSubnet



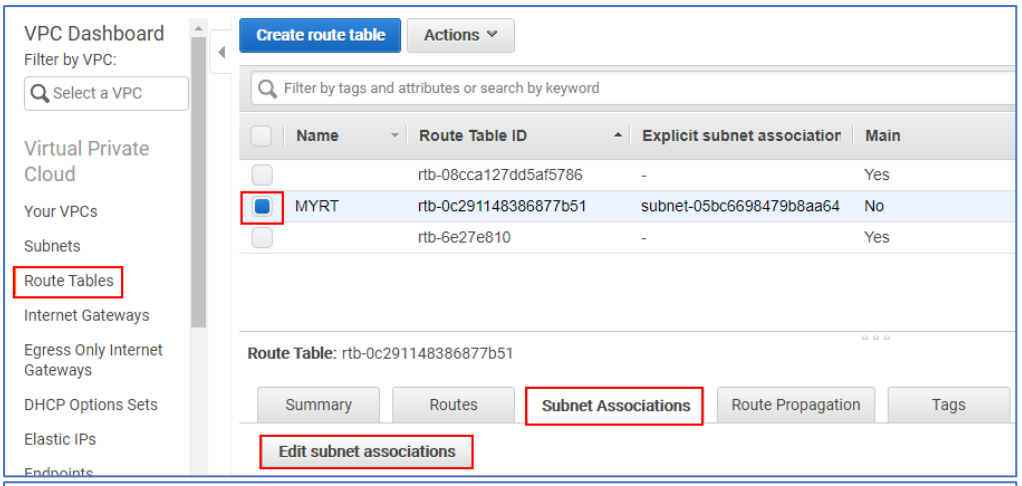
4. Please create an Internet gateway "**MyIGW**" and then attached to your VPC

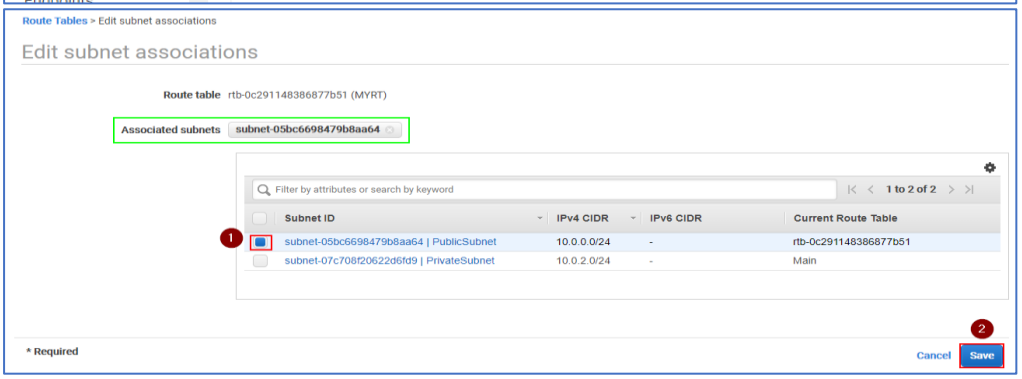


5. Create route table - A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

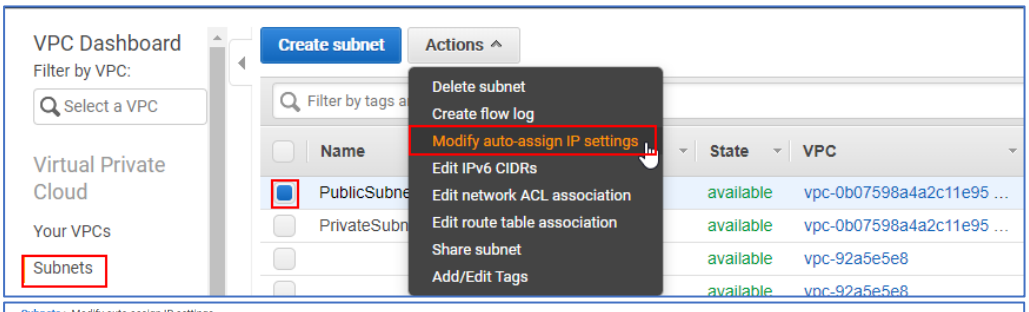


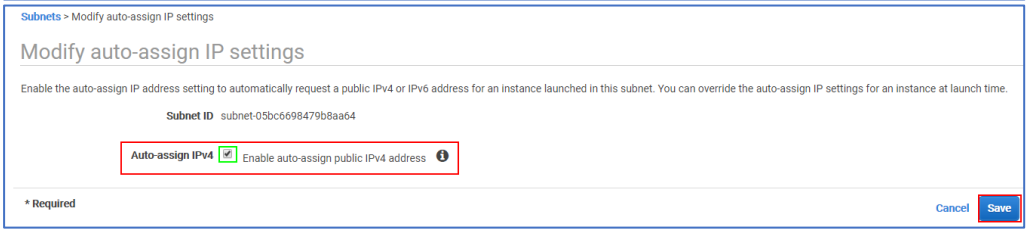
6. Now we have to **Subnet Associations**





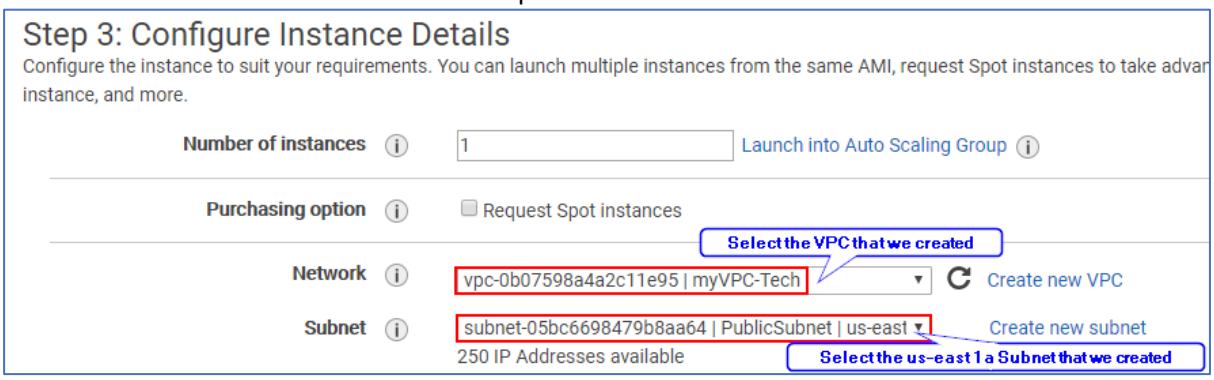
7. After this go to Subnets and make your public subnet as auto assign public IP





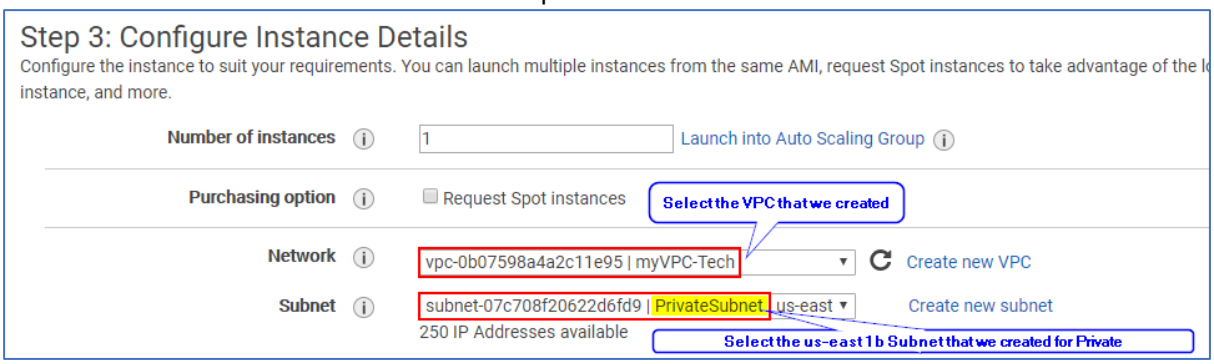
8. After this launch EC2 instances, in configuration instance tab, choose your **VPC** in network, choose your public subnet.

EC2 – First Instance 10.0.1.0 –us east-1a as public subnet



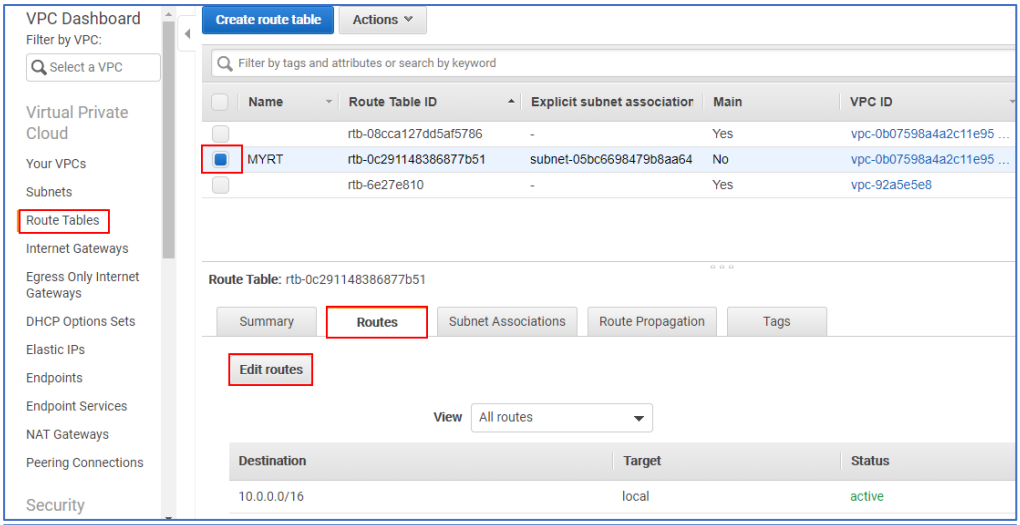
After this create new security group “SG-1”, ssh and http, HTTPS
Choose new key pair or you can use the existing one.

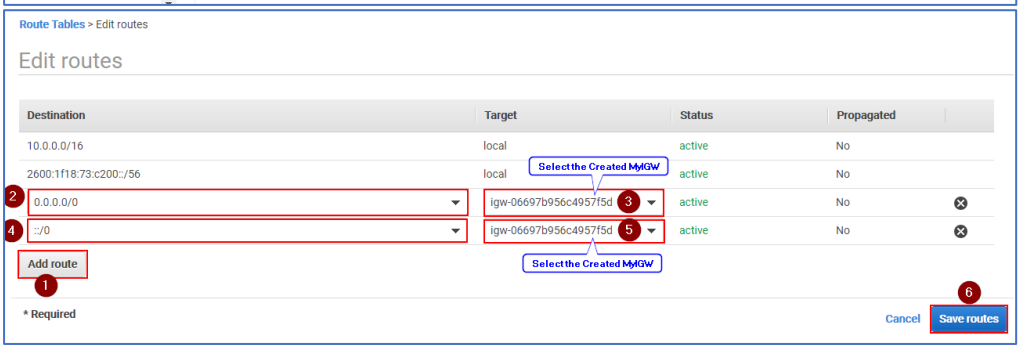
EC2- Second Instance 10.0.2.0 –us east-1a as private subnet



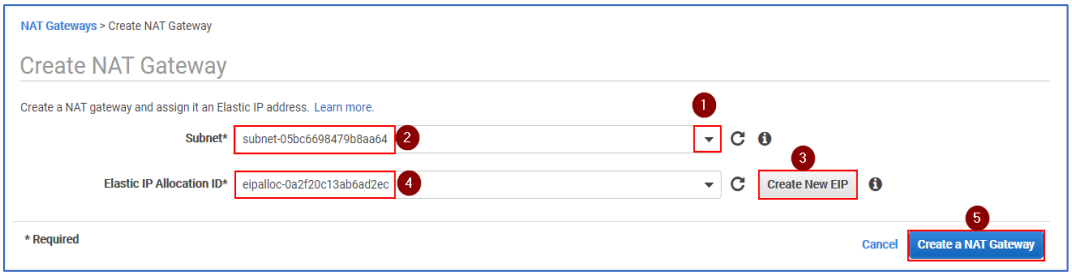
After this create new security group “SG-1”, ssh and http, HTTPS
Choose new key pair or you can use the existing one.

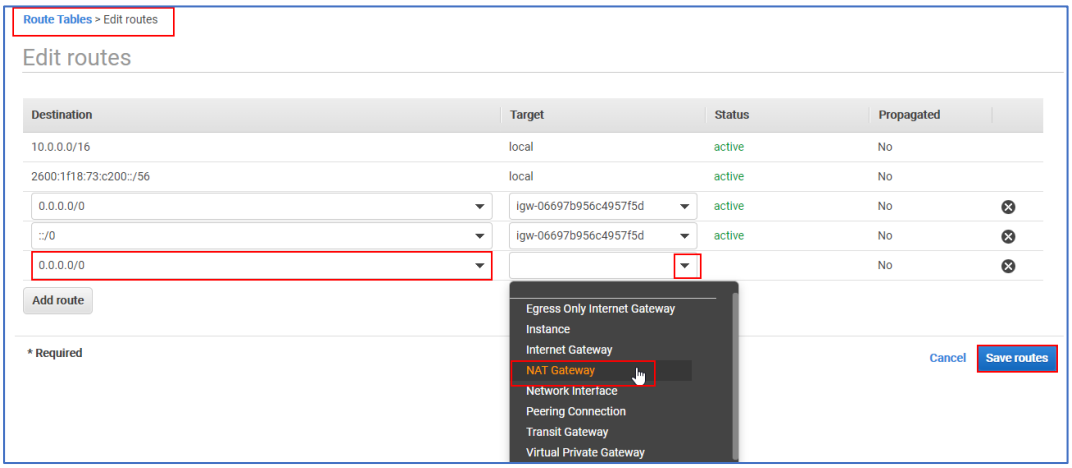
9. After this connect to public machine **EC2- First Instance** and try to check if it is internet connected or working. By Ping google.com
If Internet is not working, then do below the steps.
We need to enable Internet access.

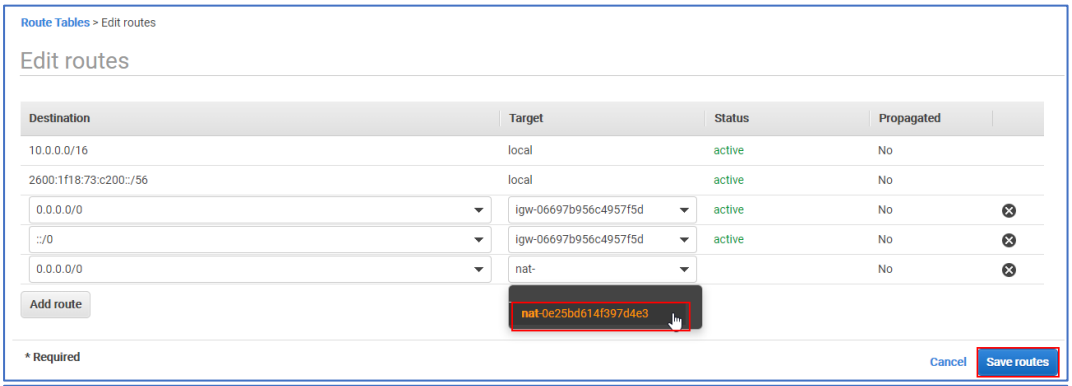


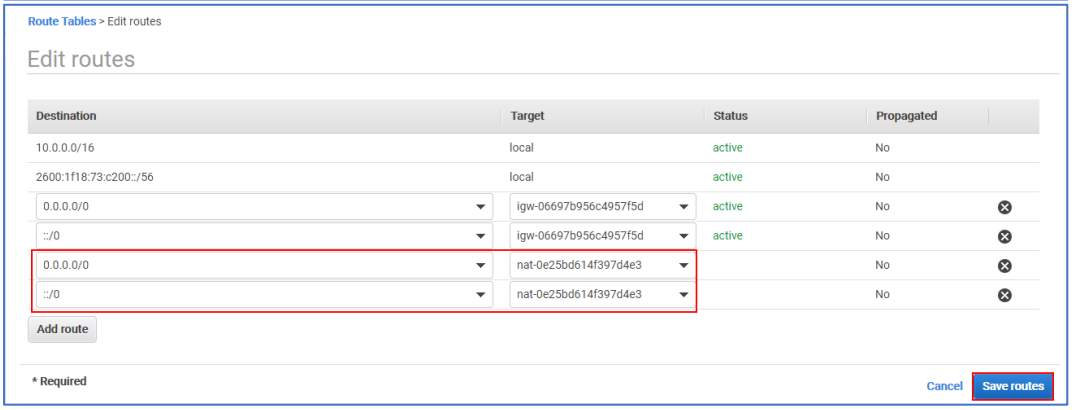


10. Now try to access your EC2-Second System (PrivateServer) from EC2-First System (PublicServer)
11. [ec2-user@ip-10-0-1-167 ~]$ vi mynewkey.pem (copy and paste the code from .pem key)
12. [ec2-user@ip-10-0-1-167 ~]$ chmod 400 mynewkey.pem (Set the permission)
13. [ec2-user@ip-10-0-1-167 ~]$ ssh -i mynewkey.pem ec2-user@<private_ip_address>
14. After connectivity, elevate privileges and check for command yum update -y
    If the Internet is not working on PrivateServer then do below the steps.









Done