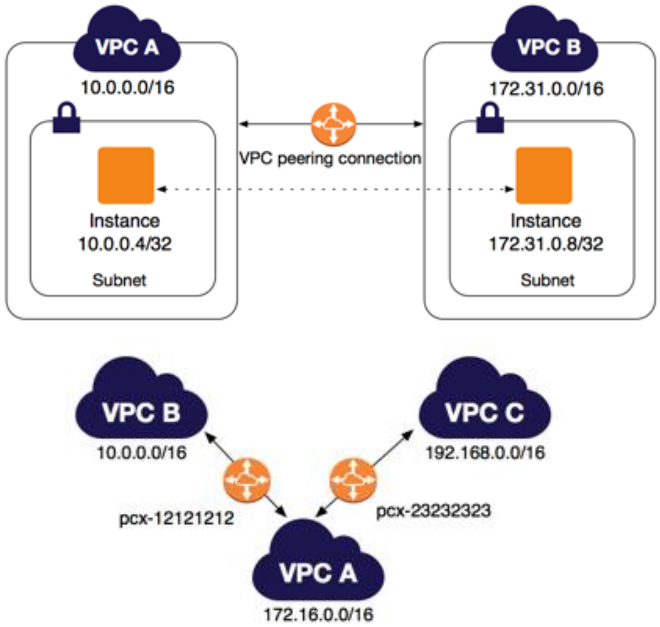
AWS Quick Start Guide: Amazon Virtual Private Cloud VPC Peering Connections Documentation

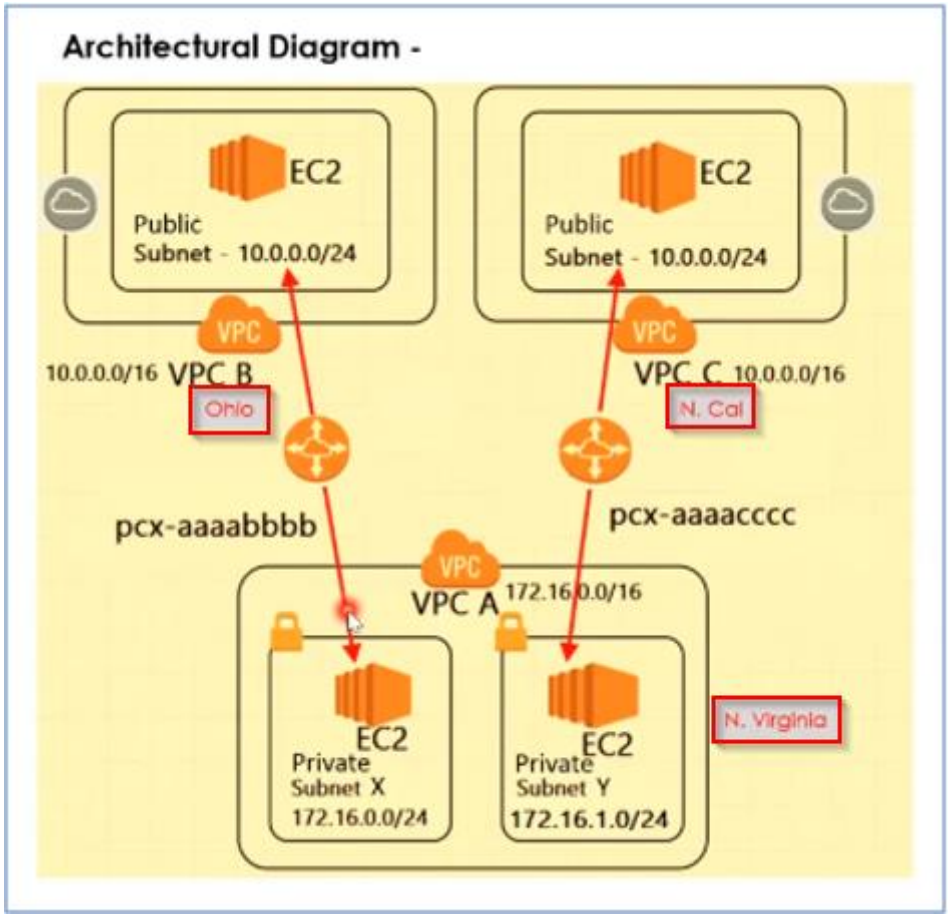
Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined.

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection).



Route Table	Destination	Target
VPC A -- Private Subnet X RT	172.16.0.0/16	Local
	10.0.0.0/16	PCX -AB
VPC B -- Private Subnet Y RT	172.16.0.0/16	Local
	10.0.0.0/16	PCX - AC
VPC B -- Public Subnet RT	10.0.0.0/16	Local
	172.16.0.0/24	PCX -AB
	0.0.0.0/0	IGW
VPC C -- Public Subnet RT	10.0.0.0/16	Local
	172.16.1.0/24	PCX -AB
	0.0.0.0/0	IGW

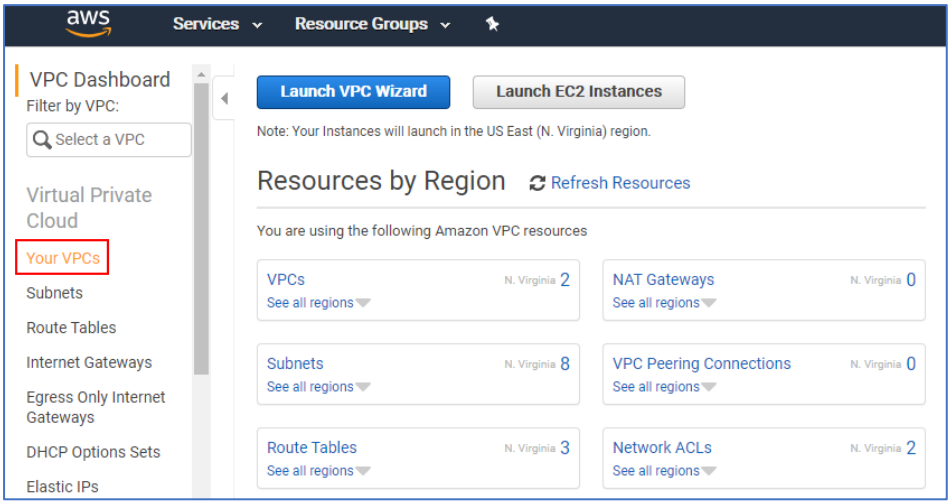
VPC A	**172.16.0.0/16**	
	Private Subnet X	172.16.0.0/24
	Private Subnet Y	172.16.1.0/24
VPC B	10.0.0.0/16	
	Public Subnet B	10.0.0.0/24
VPC C	10.0.0.0/16	
	Public Subnet C	10.0.0.0/24



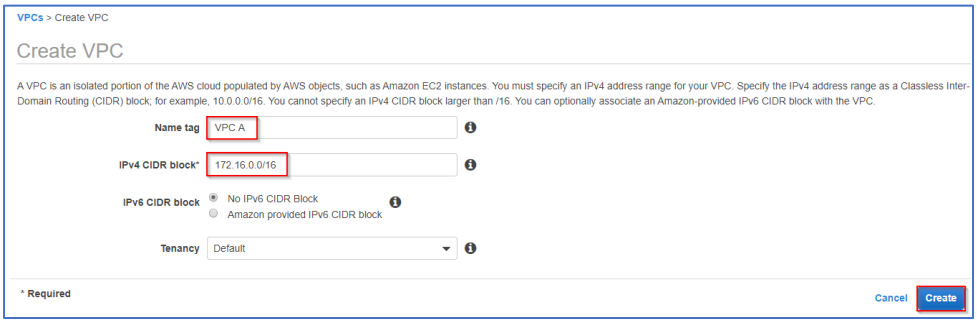
Accessing Amazon VPC

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

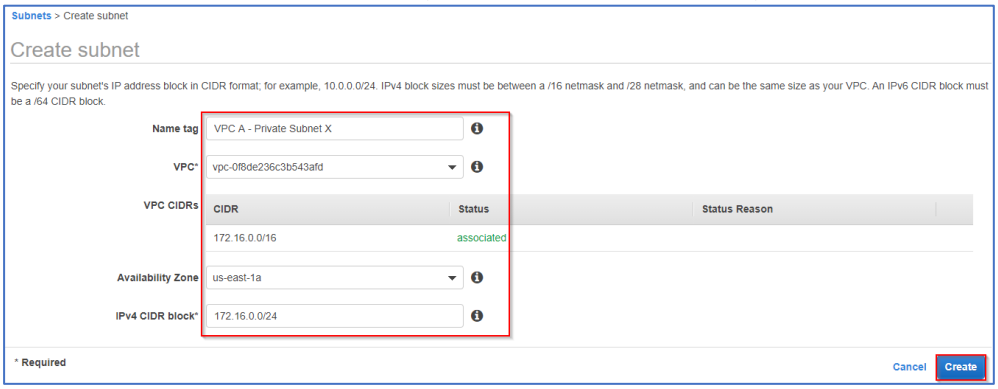
1. **AWS Management Console – N. Virginia - VPCs. -> Your VPCs**



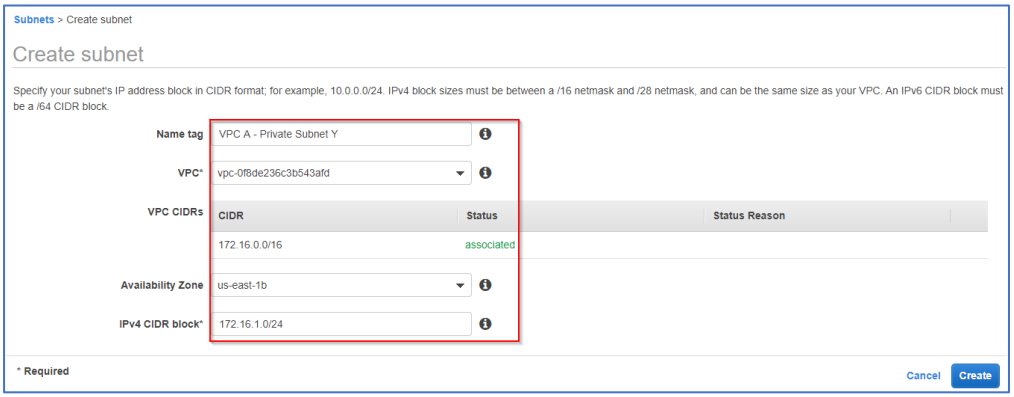
2. Create VPC as below:



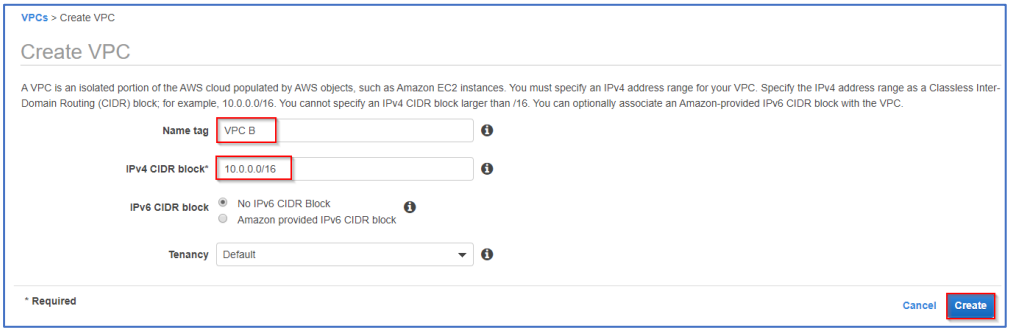
3. Now we can create two Subnet -> 1)**VPC A - Private Subnet X** 2)**VPC A - Private Subnet Y**



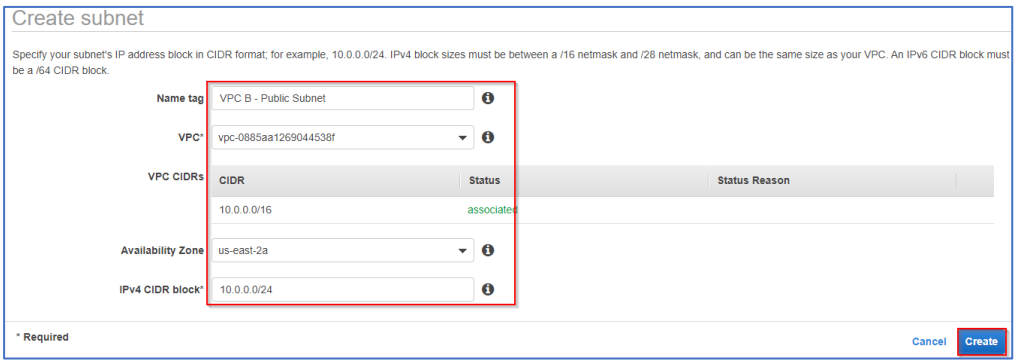
2)**VPC A - Private Subnet Y**



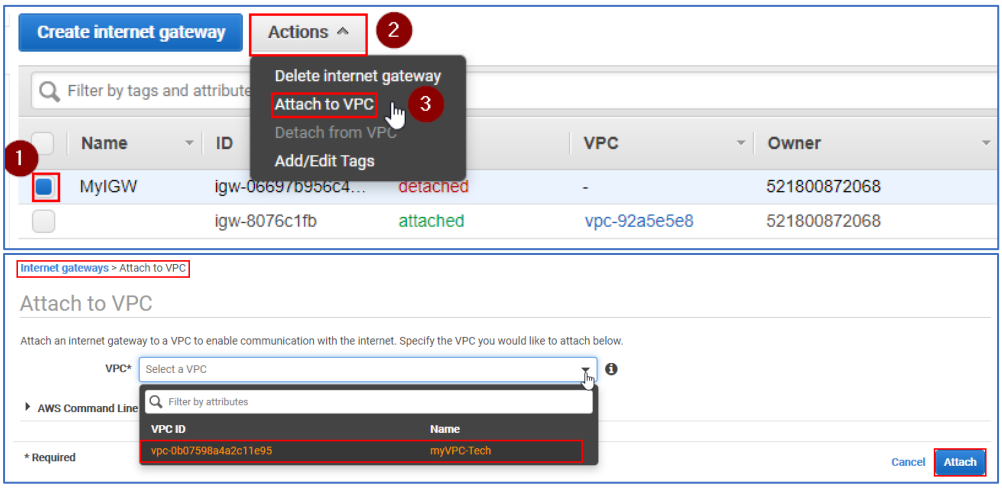
4. Now switch region to '**OHIO**'
5. Create VPC **'VPC B'**



Create a Subnet '**VPC B – Public Subnet**'

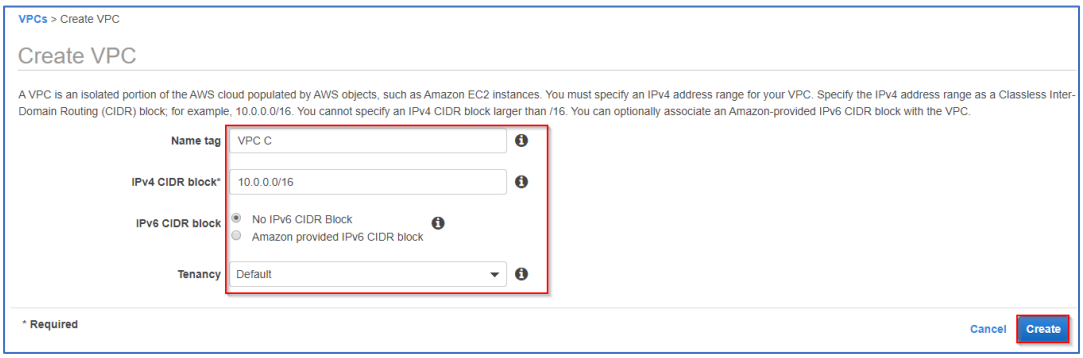


6. Please create an Internet gateway "**VPC-B IGW**" and then attached to your VPC

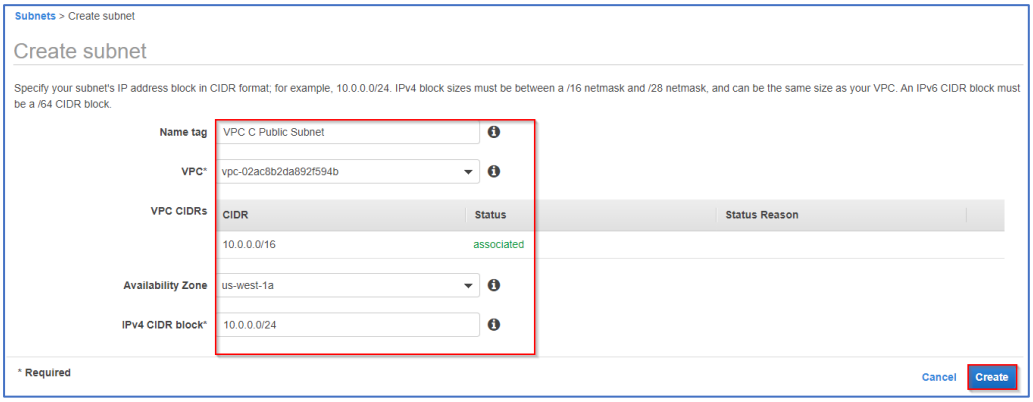


7. Switch to **N.California**

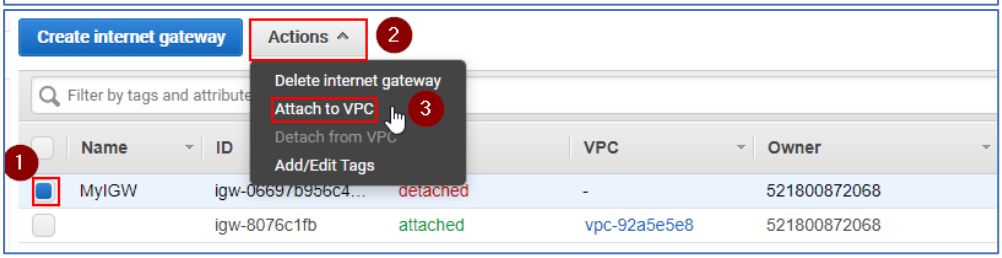
Create **VPC C**

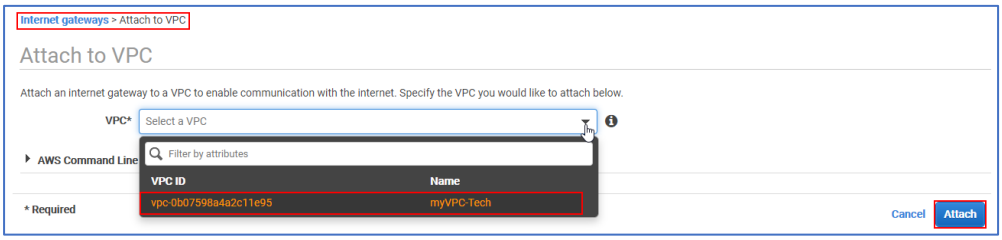


8. Create a Subnet '**VPC C – Public Subnet'**

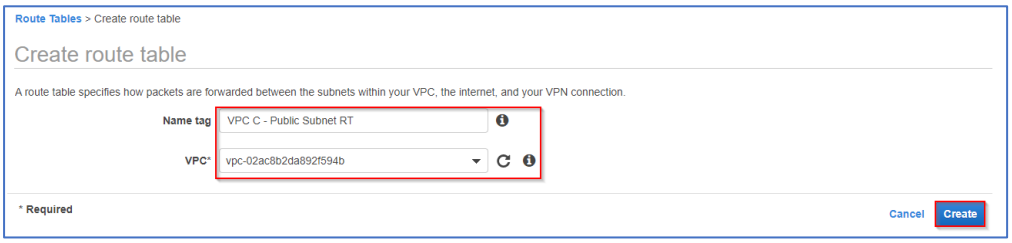


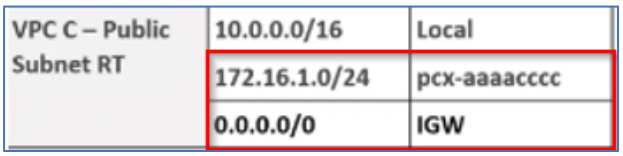
9. Please create an Internet gateway "**VPC - C IGW**" and then attached to your VPC

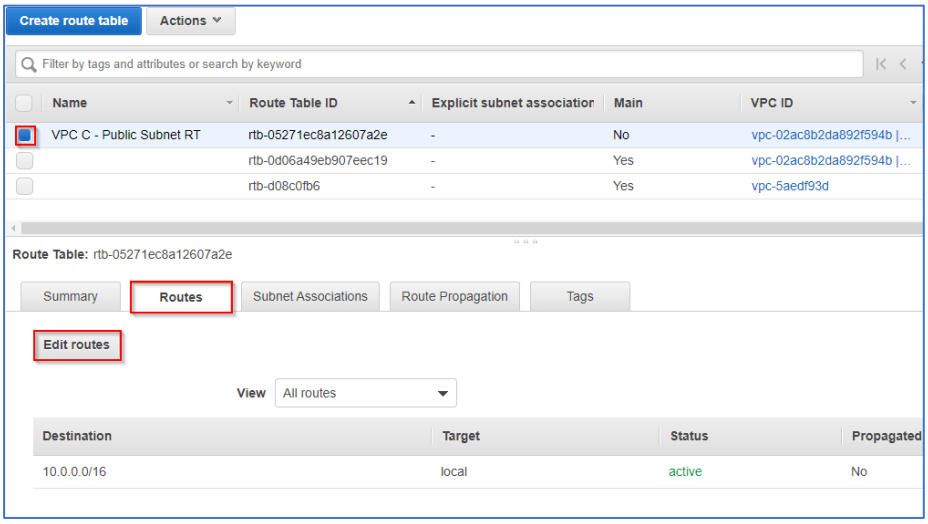




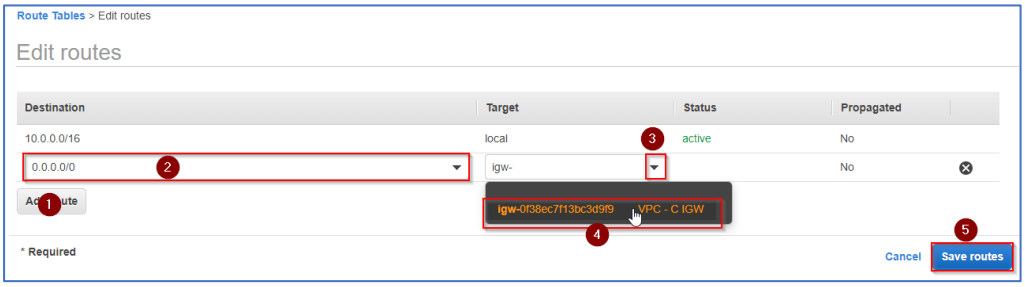
10. Create '**Route Table**'



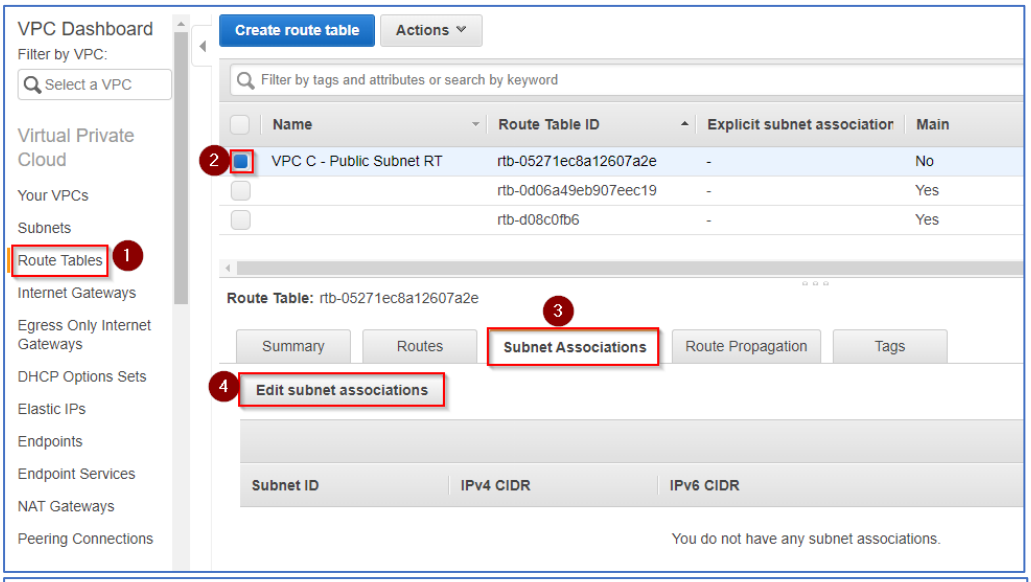


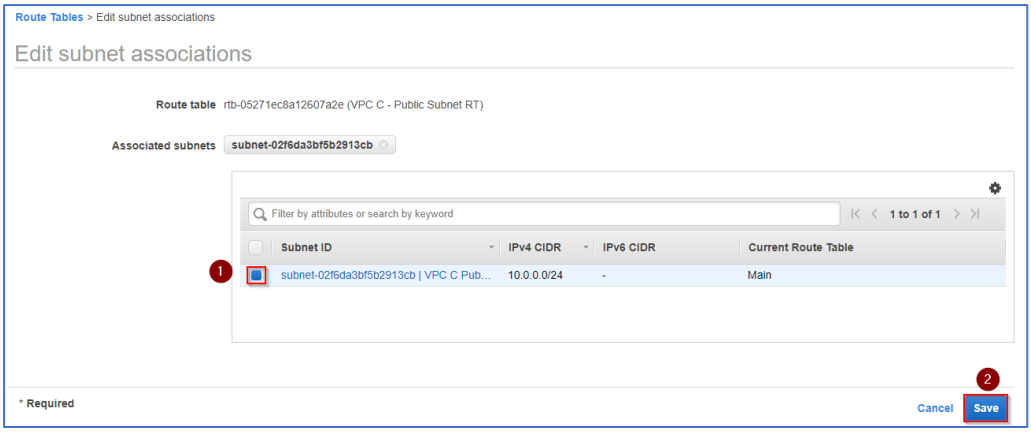


11. Add route table –



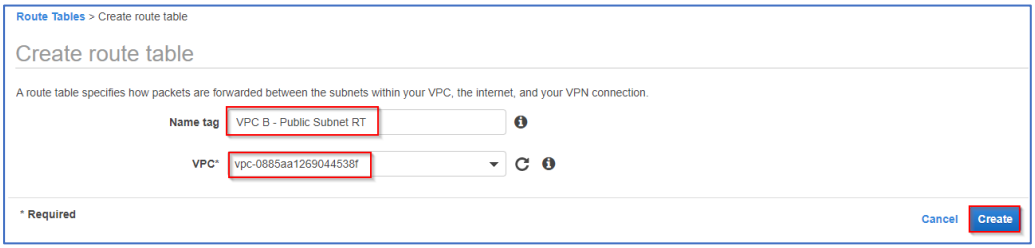
12. Now we have to do **'Subnet Associations'**

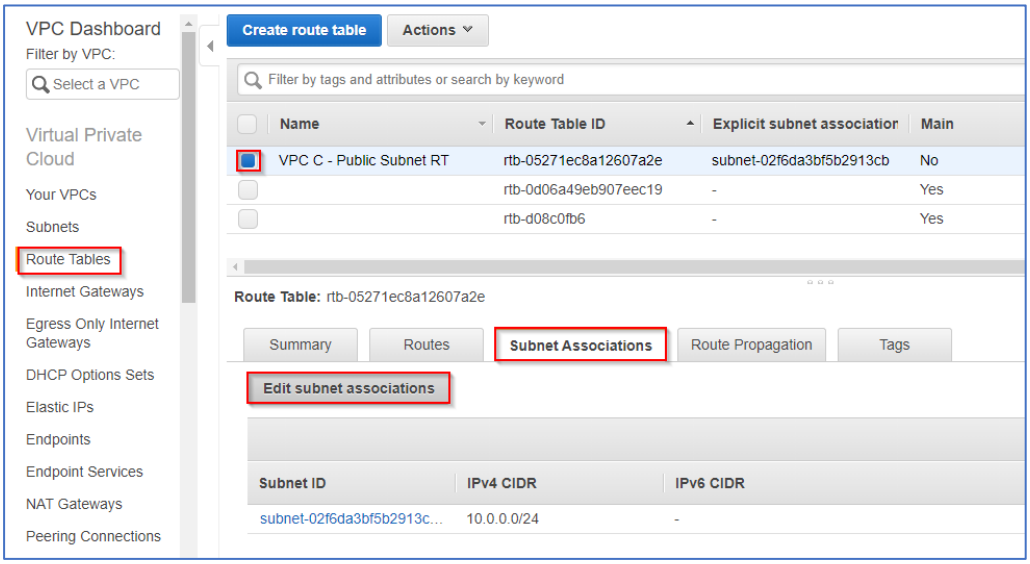


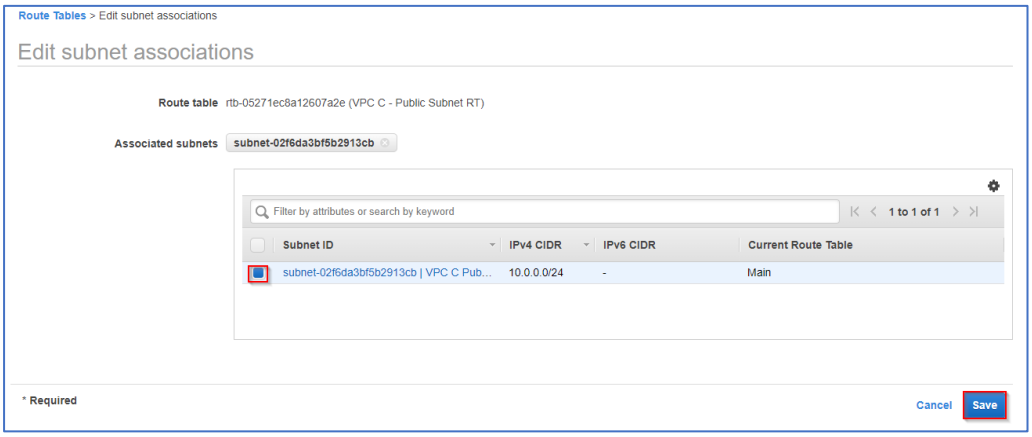


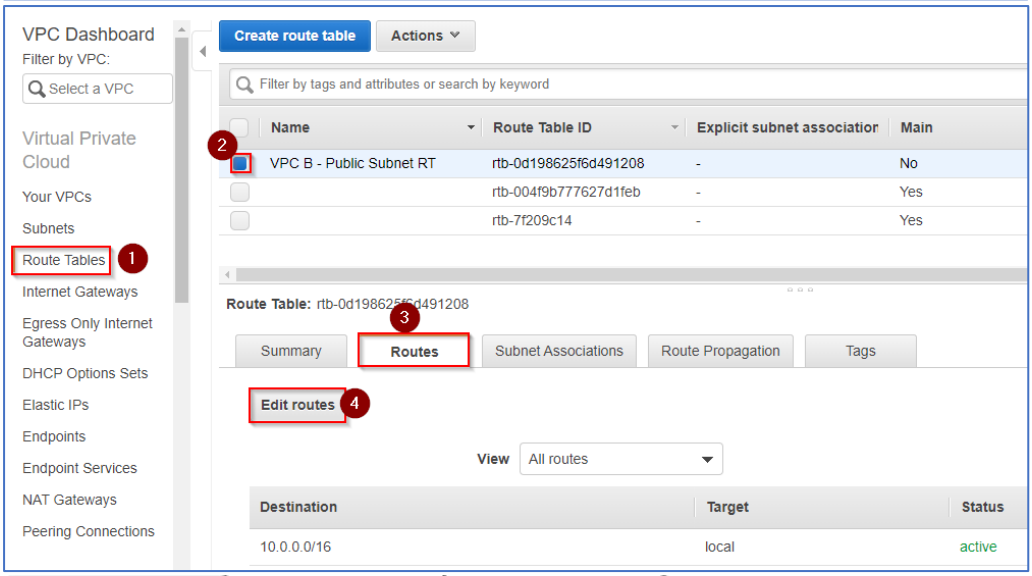
13. Switch to **Ohio** and do the (10-12) same activities for **VPC-B**

Create 'Route Table' VPC B – Public Subnet RT

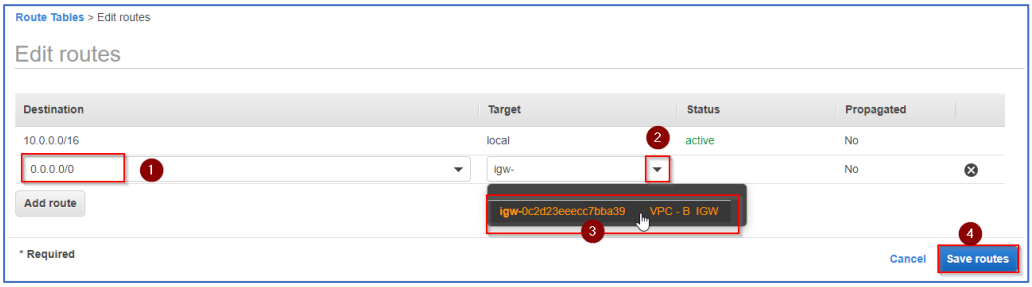






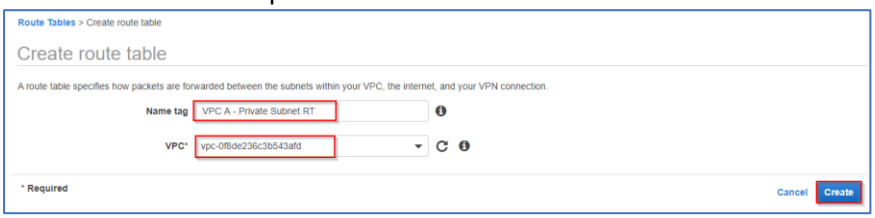


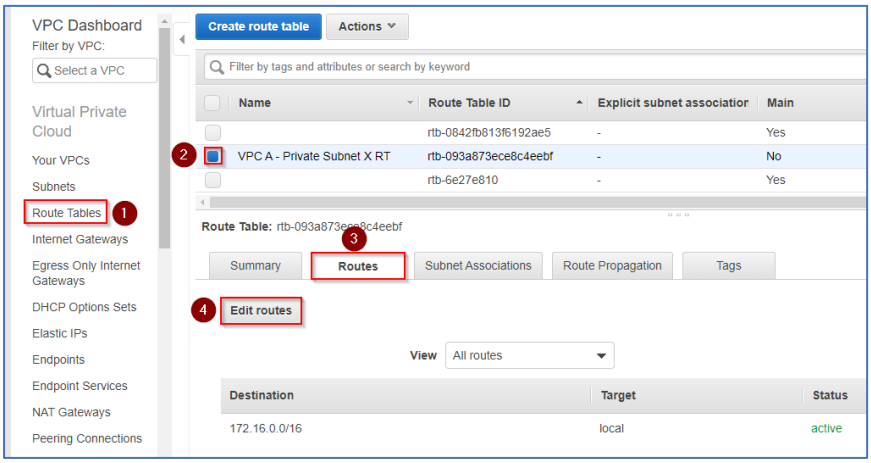
VPC B - Public Subnet RT	10.0.0.0/16	Local
	172.16.0.0/24	pcx-aaaabbbb
	0.0.0.0/0	IGW



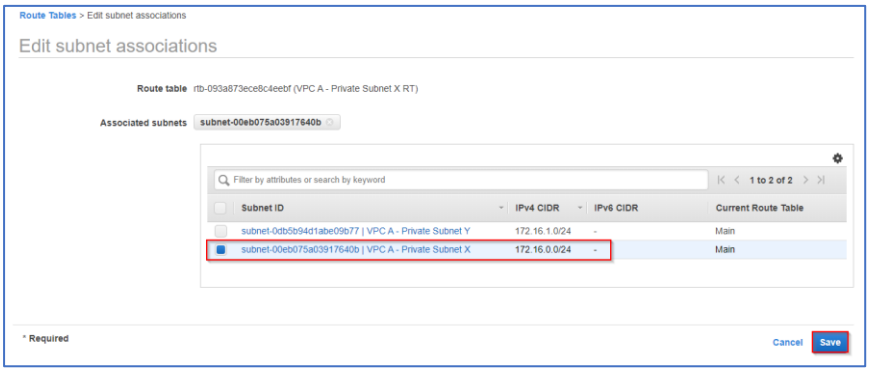
Switch to **N. Virginia** and Create route table, This Subnet is private, and we will not have any internet gateway routing

14. Create Route Table as per below:



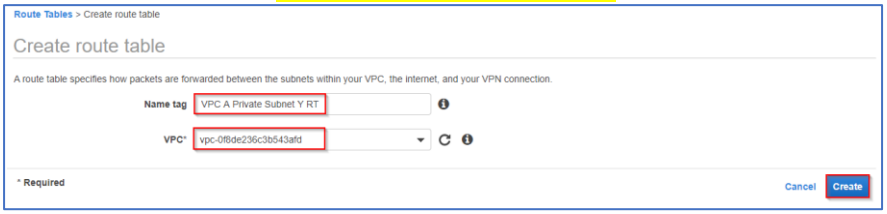


15. Do the **Subnet Associations**

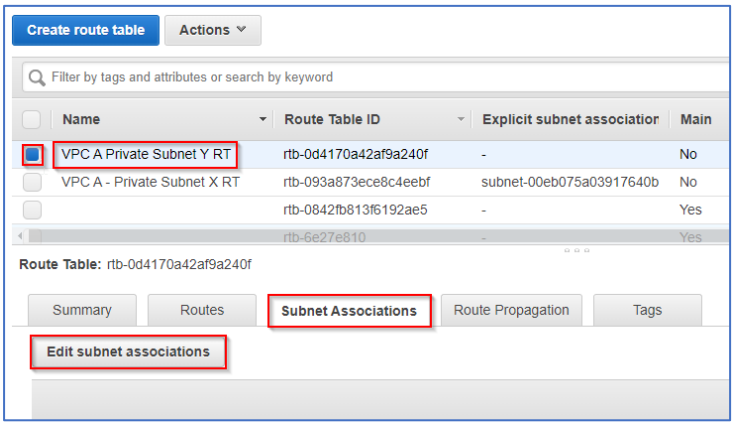


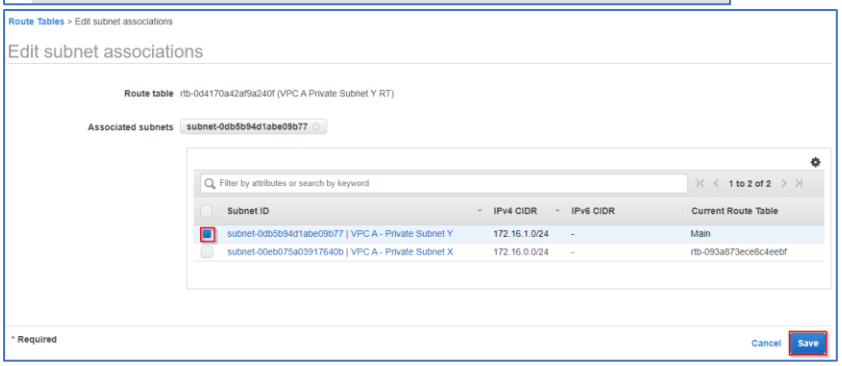
PCX A '**N.Verginia**'

16. Create a **'Route Table'** **VPC A – Private Subnet Y RT**

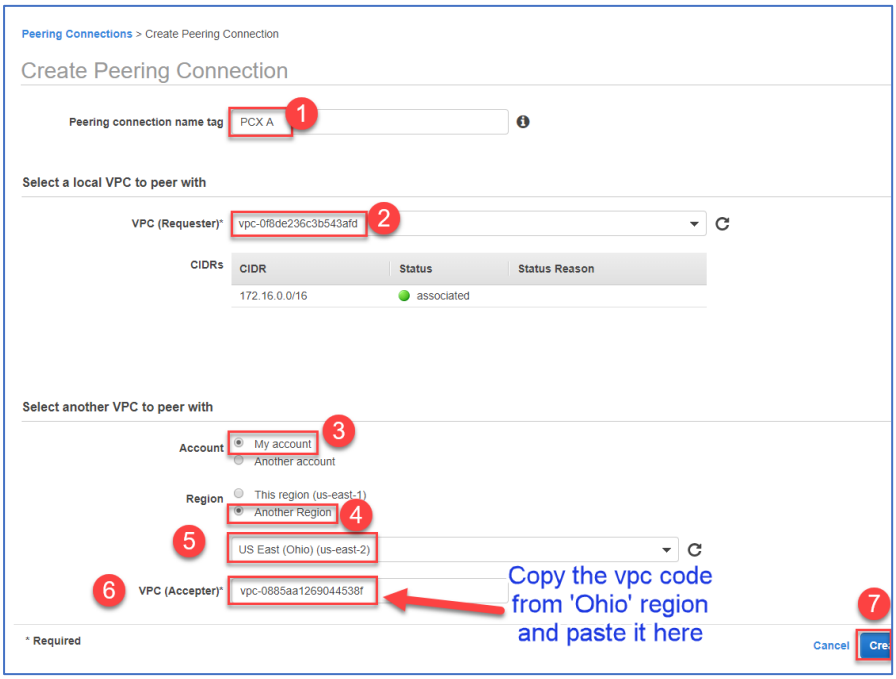


17. Do the '**Subnet Association**'

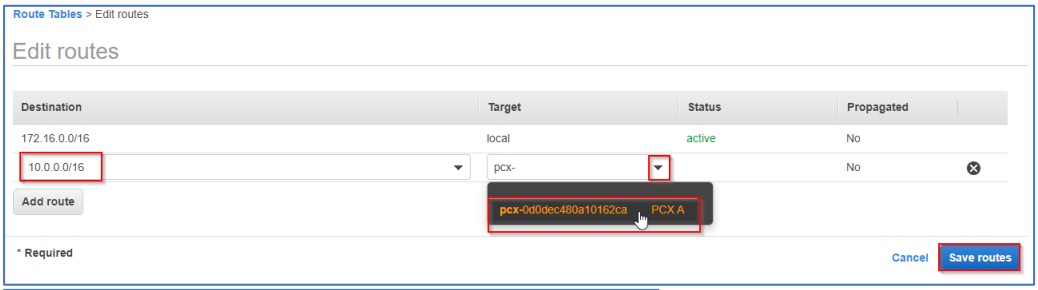




18. Now in same region **N.Virginia**, go to vpc peering and create peering connection

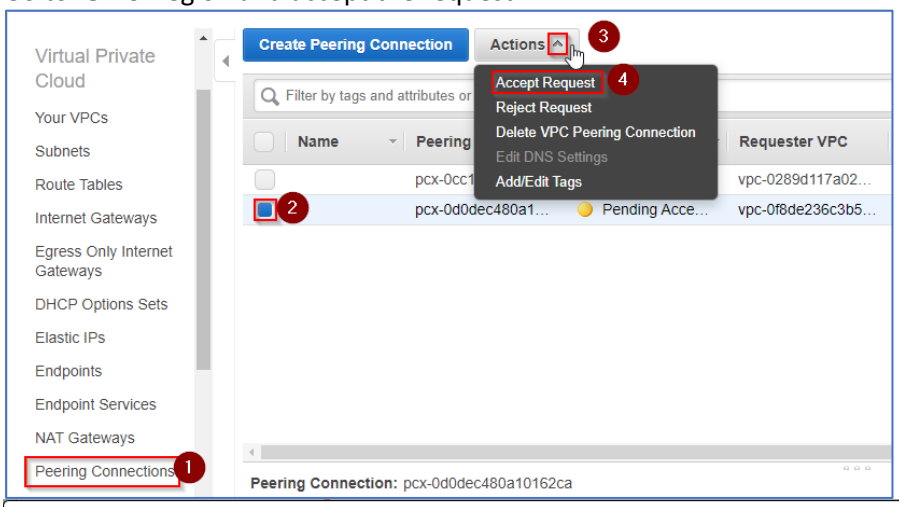


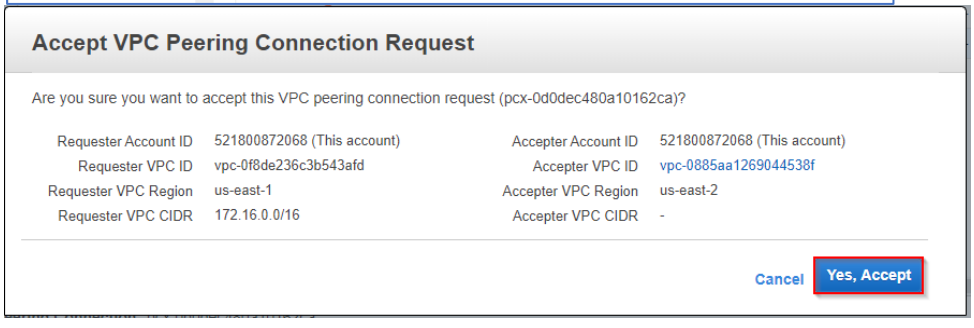
19. Now we can add '**Route Table**'

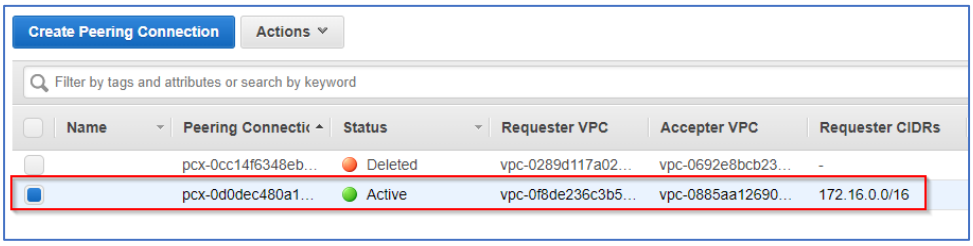


Route Table	Destination	Target
VPC A – Private Subnet X RT	172.16.0.0/16	Local
	10.0.0.0/16	pcx-aaaabbbb
VPC A – Private Subnet Y RT	172.16.0.0/16	Local
	10.0.0.0/16	pcx-aaaaccccc

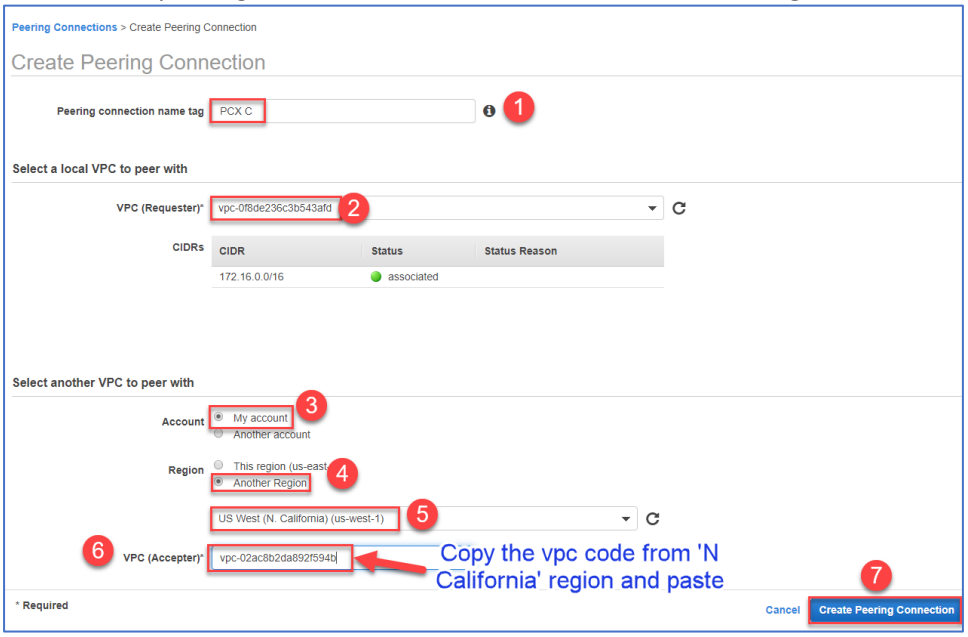
Go to '**Ohio**' region and accept the request.



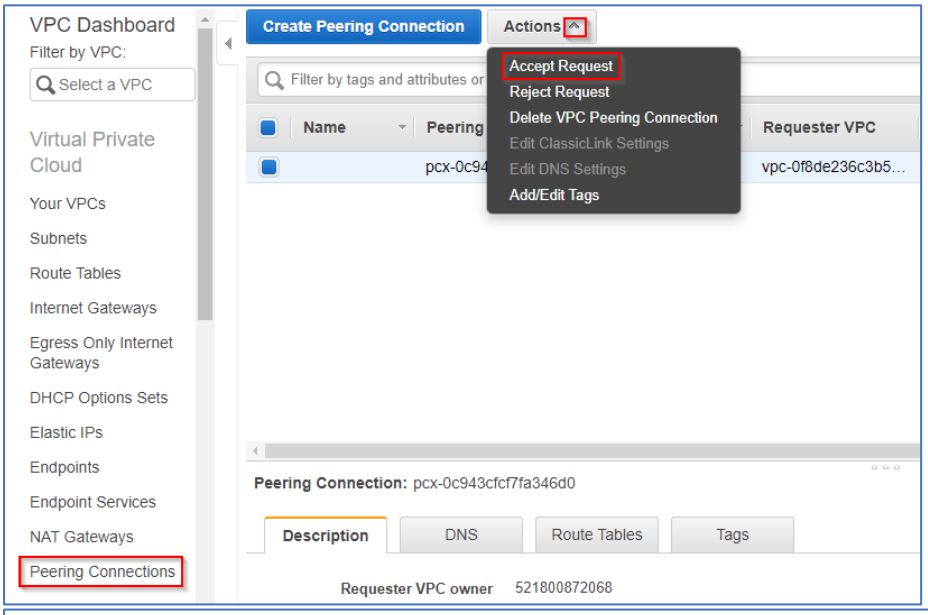


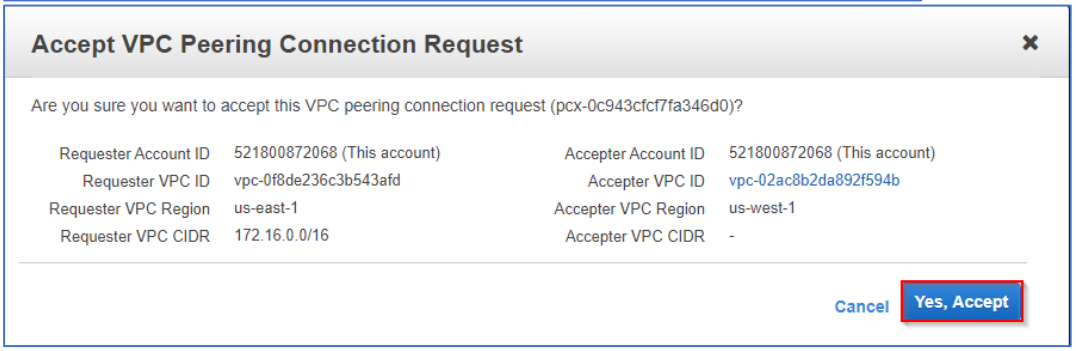


20. Do the same peering for VPC C **'PCX C'** of **N. California from N. Virginia'**

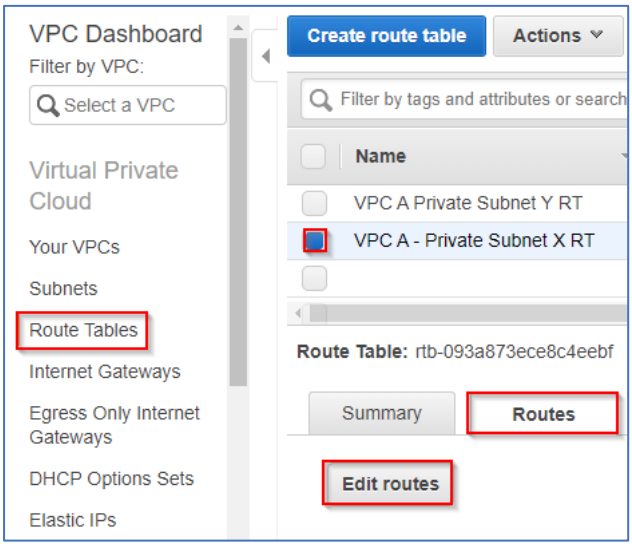


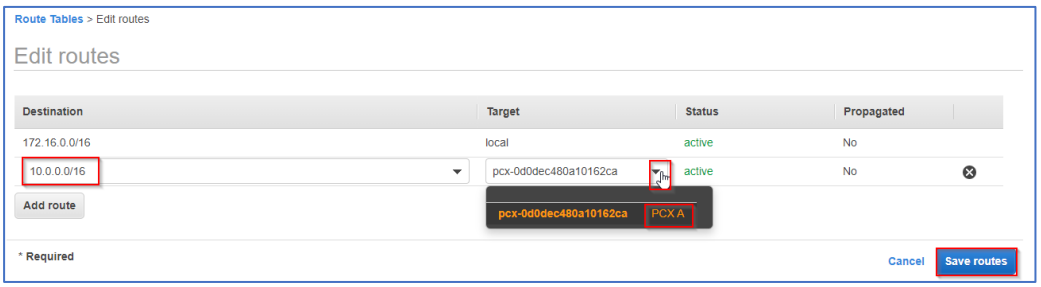
Go to '**N. California**' region and accept the request.



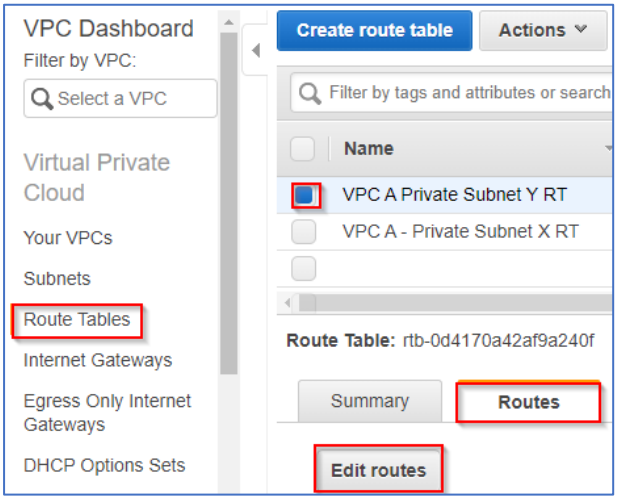


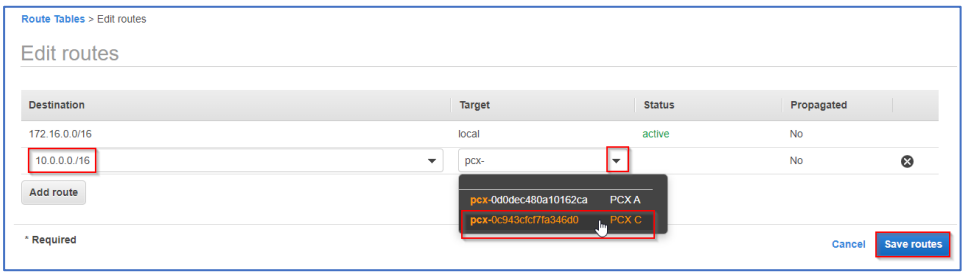
21. After this we need to add routes to Route table, switch to N virgina and do the routes association.



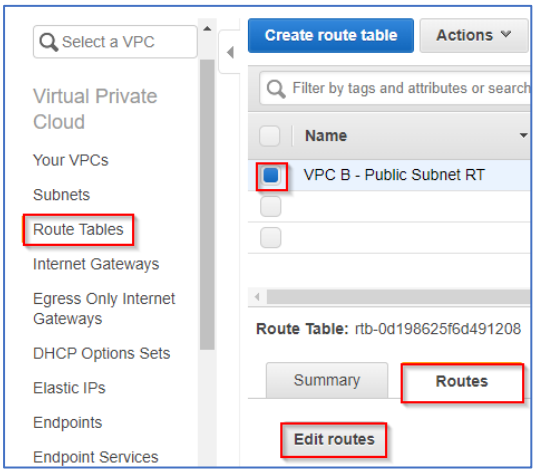


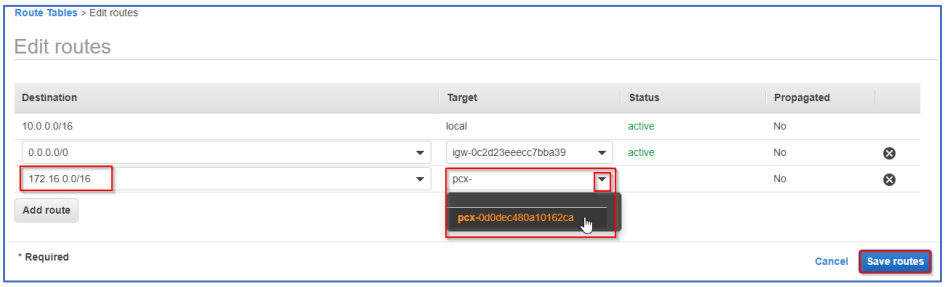
22. Now modify the route for VPC A '**Private Subnet Y RT'**.





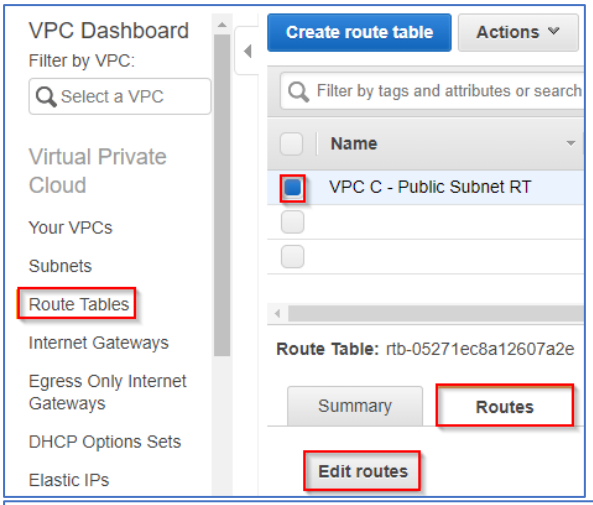
23. Now go to **Ohio** and we need to modify '**Route Table'** for **VPC B** to add peering connection route.

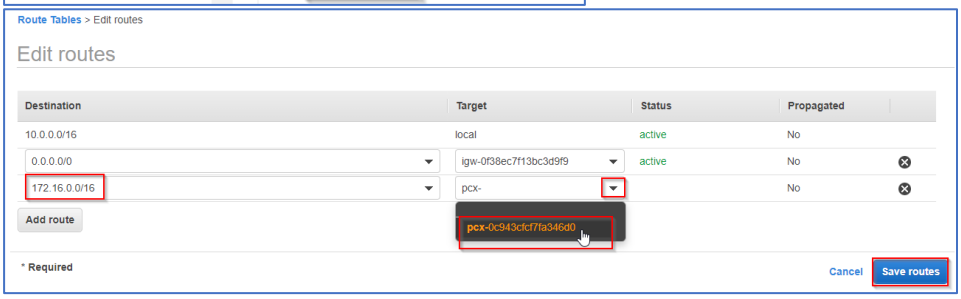




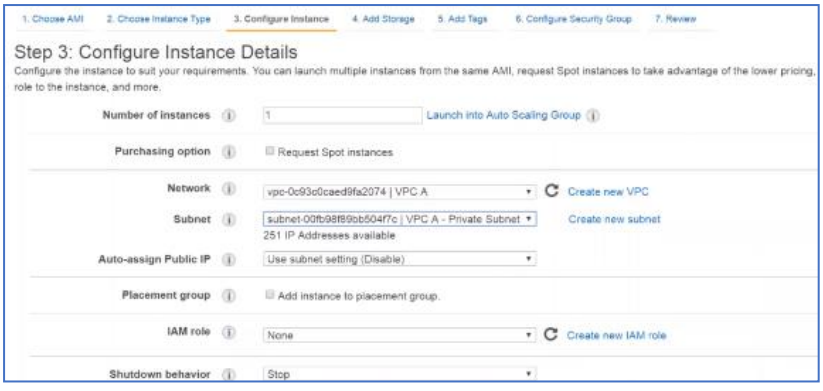
24. Switch to **N.California** and do the same for it.

Edit '**Route Table**'



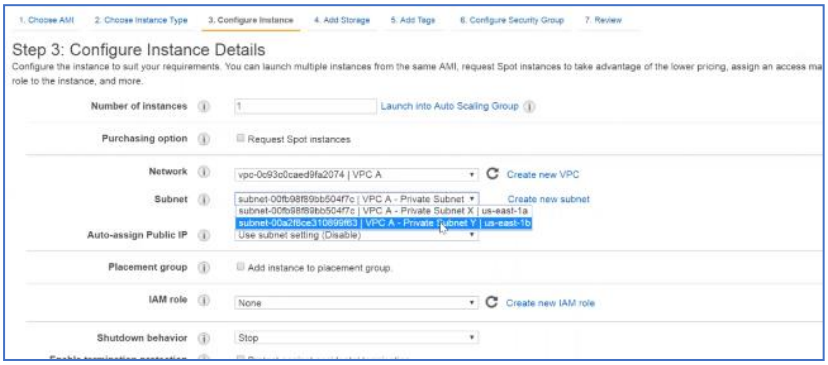


25. Now Launch **EC2 in N.Virginia** using **VPC A - Private Subnet X**

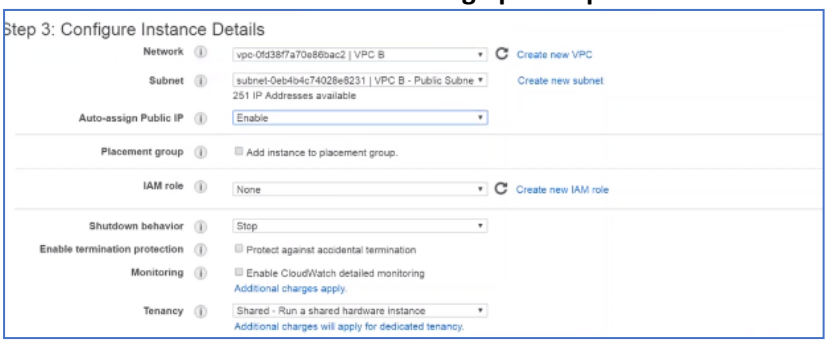


Keep traffic in Security grp as ssh only

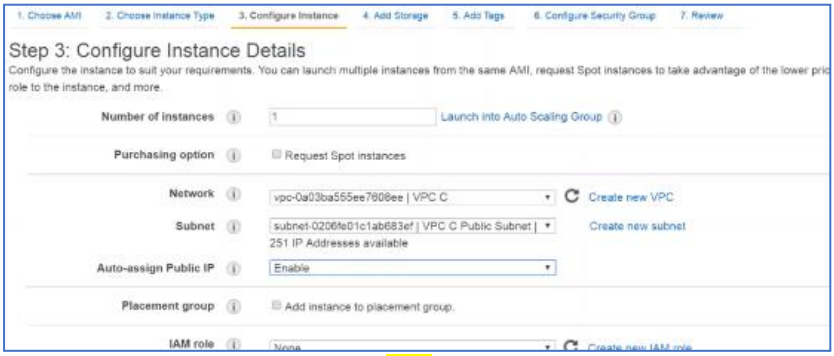
26. Now launch another **EC2** in **N.Virginia VPC A - Private Subnet Y** with security group as ssh only.



27. Now launch **EC2** in **Ohio** with **auto assign public ip** enable and **ssh as security group**.



28. Launch another Public instance in **N. California** with **ssh as security grp**



Now check the connectivity via ssh.

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