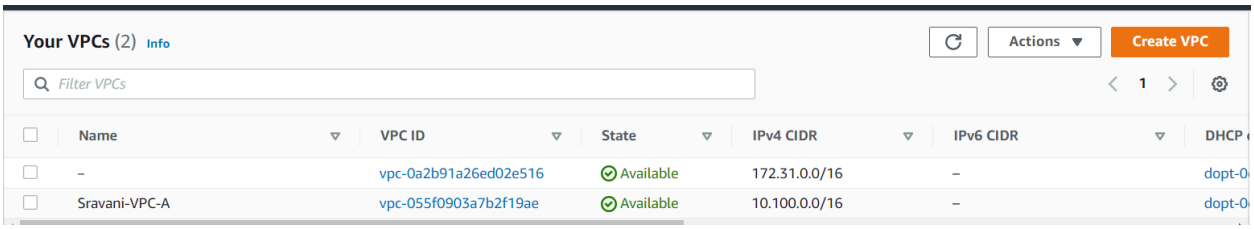
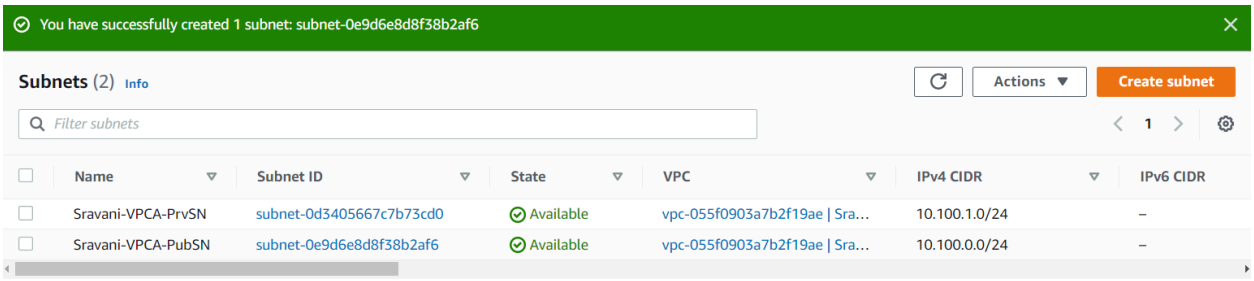
VPC-Peering

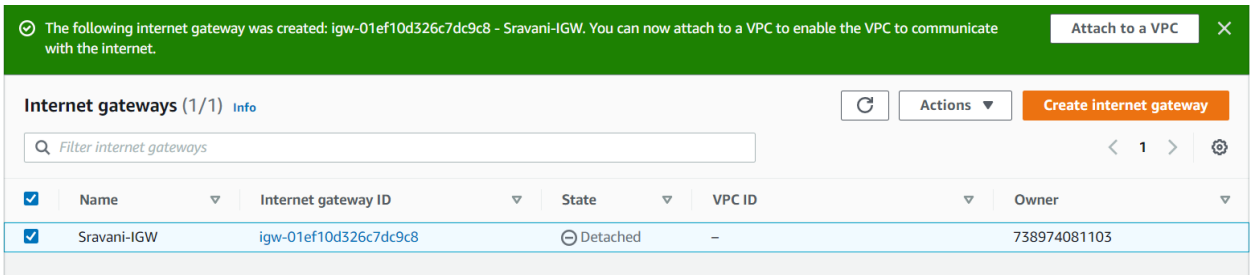
1. Create VPC-A



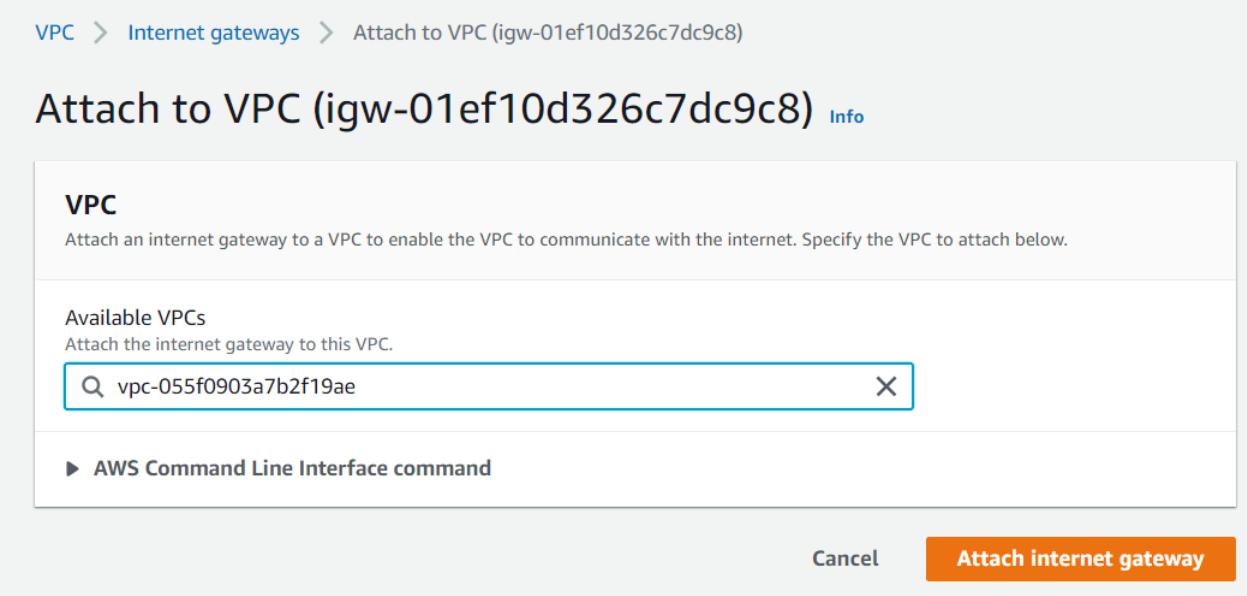
2. Create 2 subnets in VPC-A (One private subnet and one public subnet)



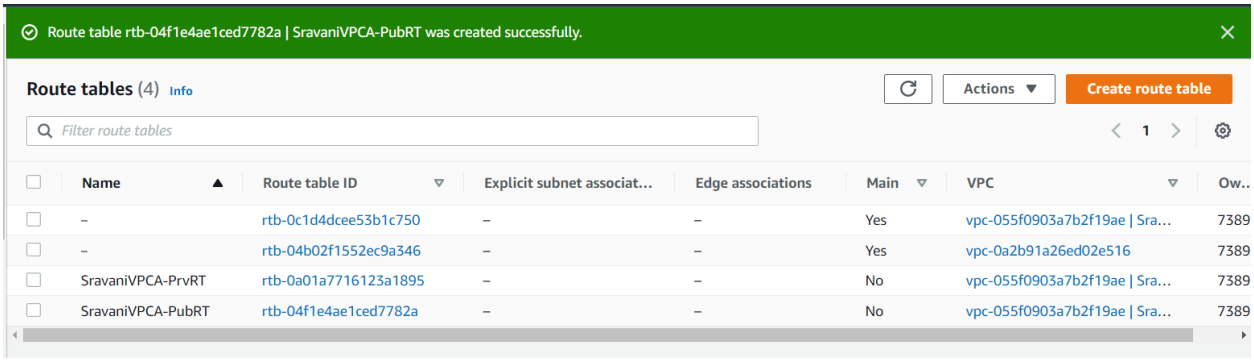
3. Create internet gateway



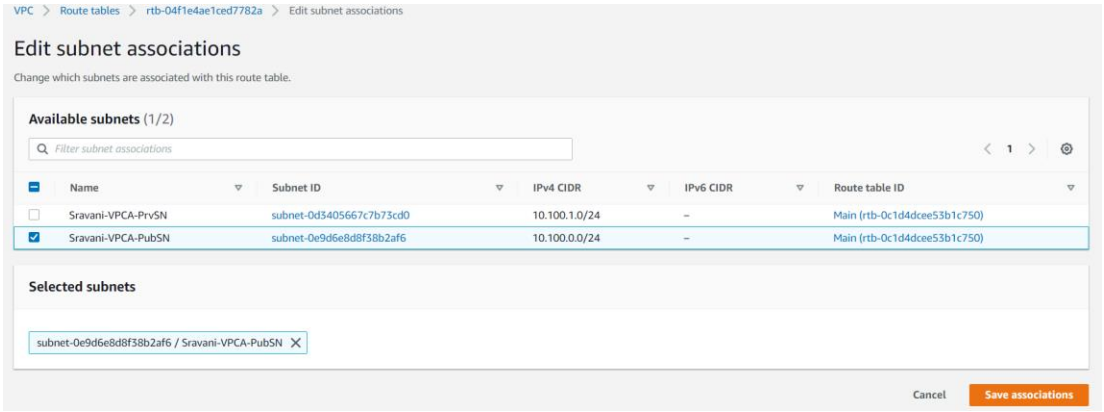
4. Attach internet gateway to a VPC

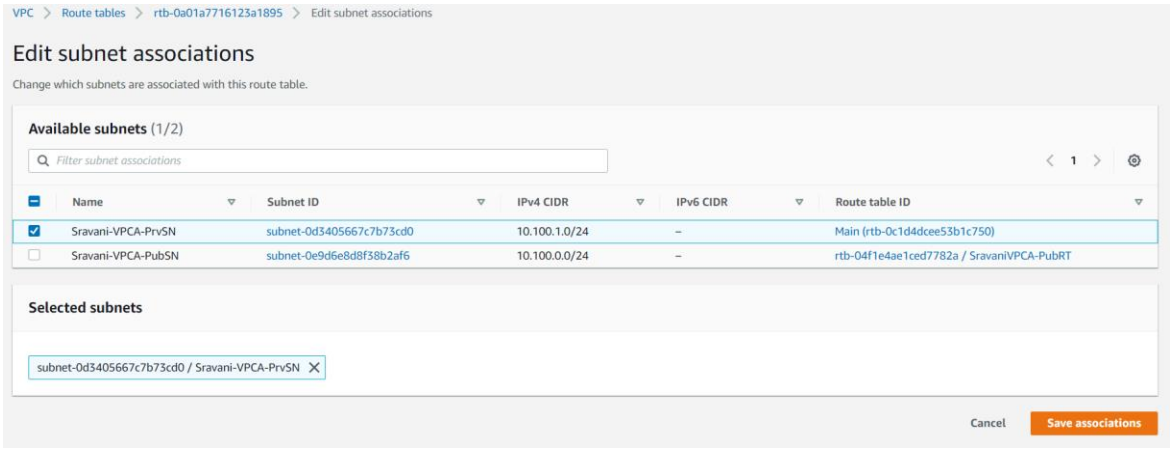


5. Create route tables

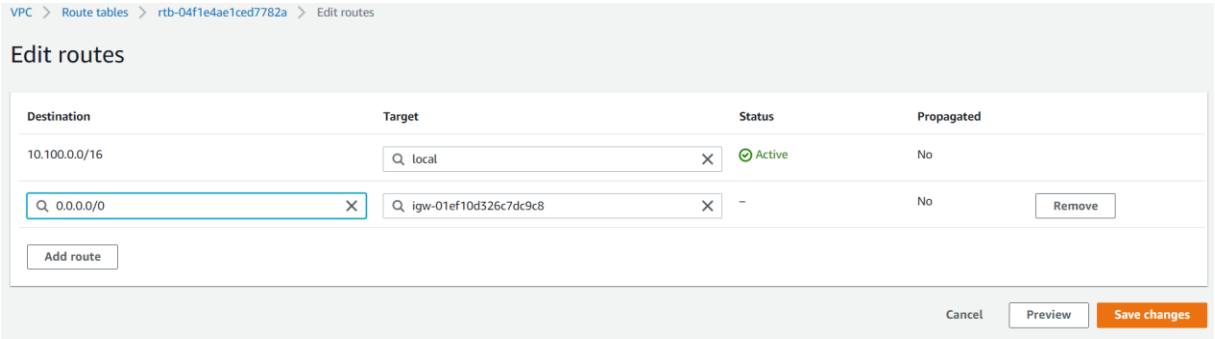


6. Associate subnets to route tables (Private-Private and Public-Public)

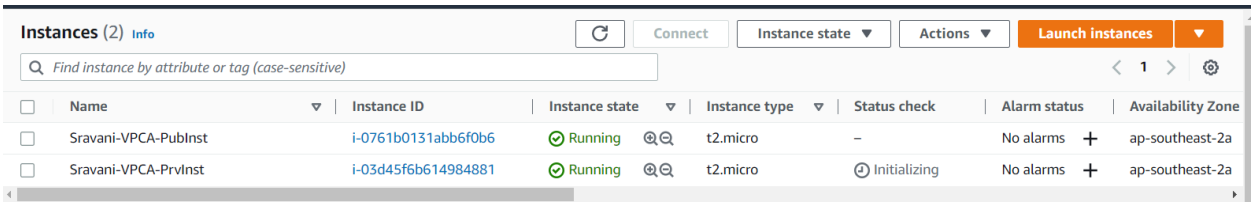




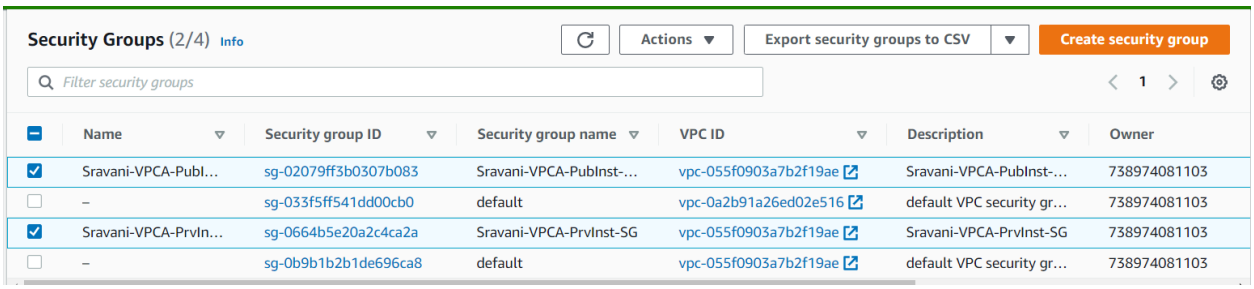
7. Connect the public route table to internet gateway



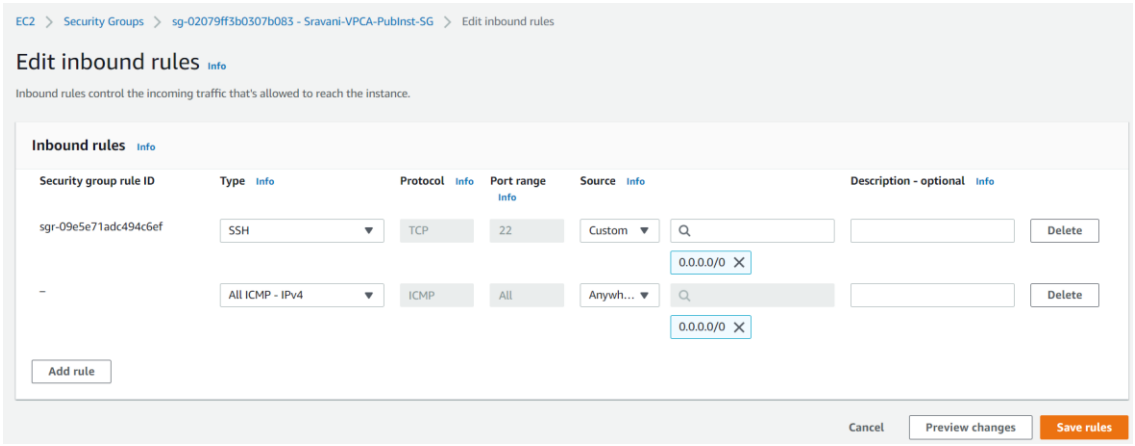
8. Create EC2 instances in public subnet and private subnet of first VPC, create security groups and select enable public ip along with instance creation:



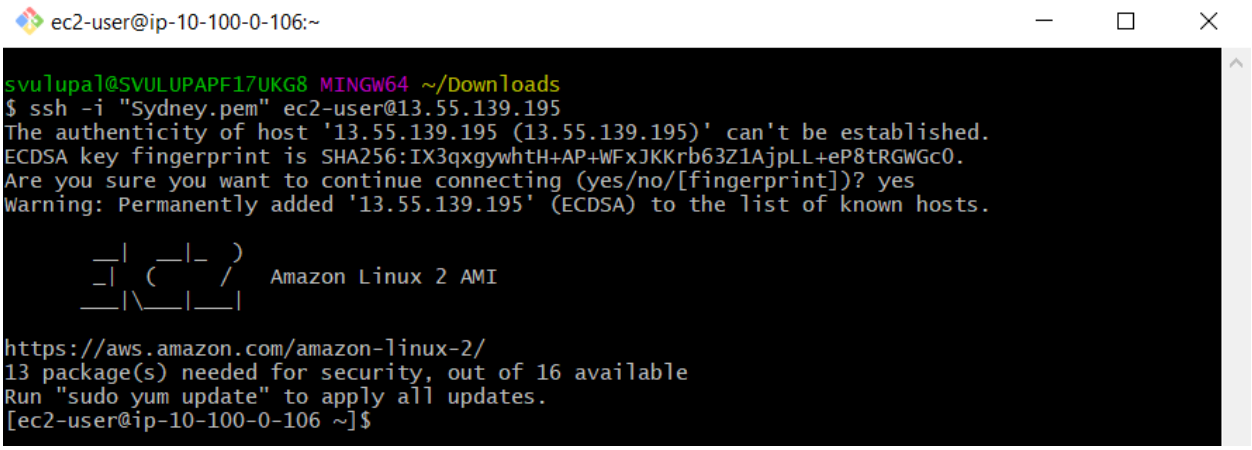
9. Security groups created along with instances:



10. Edit inbound rules of security groups to have All ICMP-IPV4

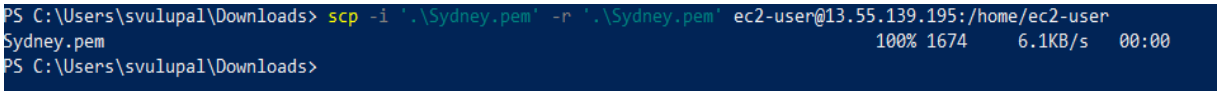


11. Connect to the public instance in the first VPC

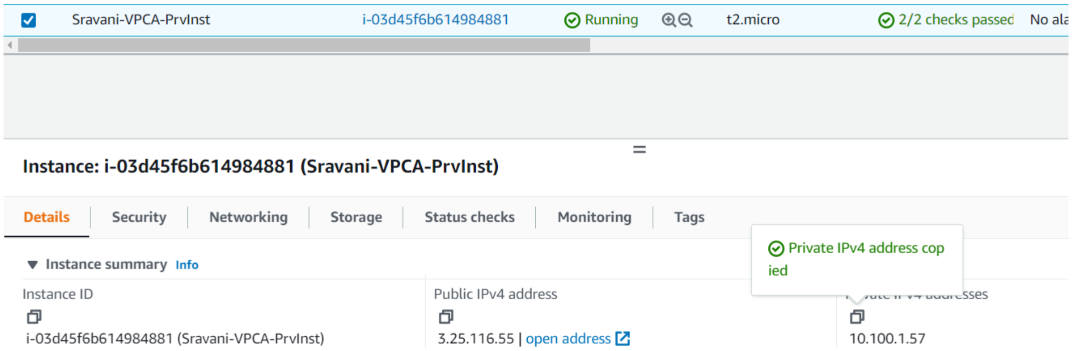


12. Connect to private instance in the first VPC from within the public instance since private instance is not connected to the internet:

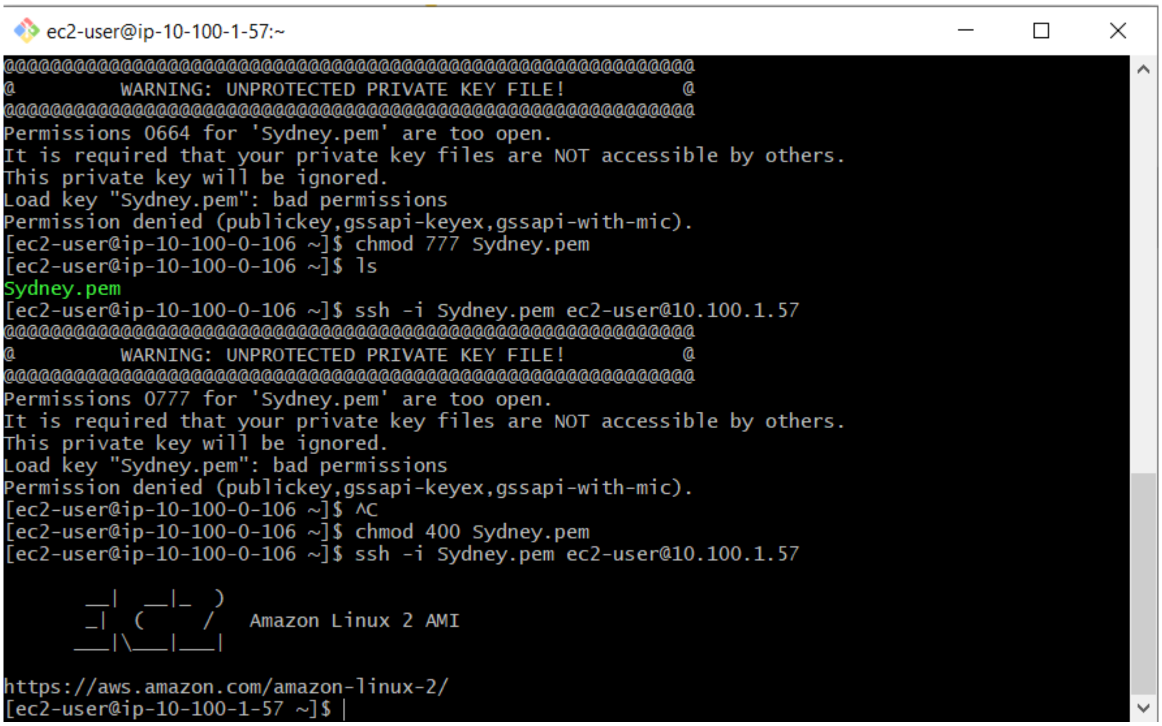
- Copy the pem file to the public instance:



- Connect to the private instance from public instance using the public ip of the private instance

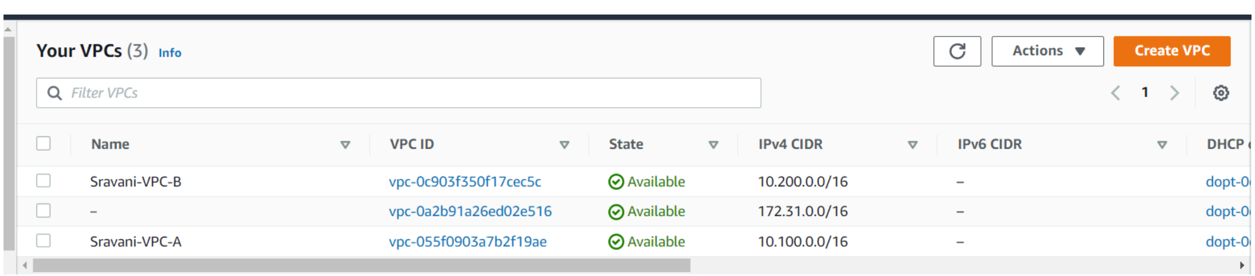


- Modify key permissions and connect to private instance using private ip:

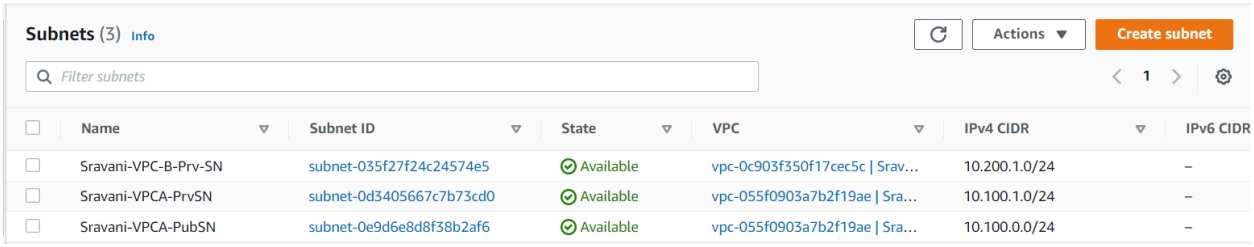


-

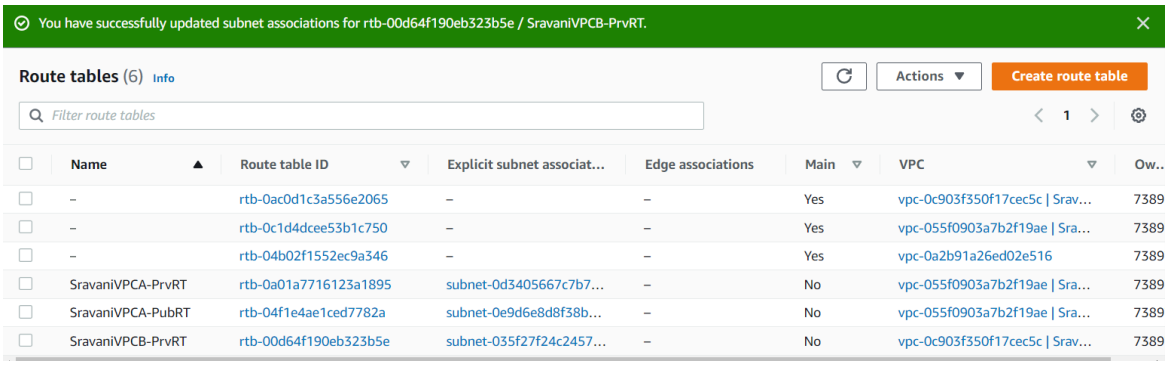
13. Create a second VPC

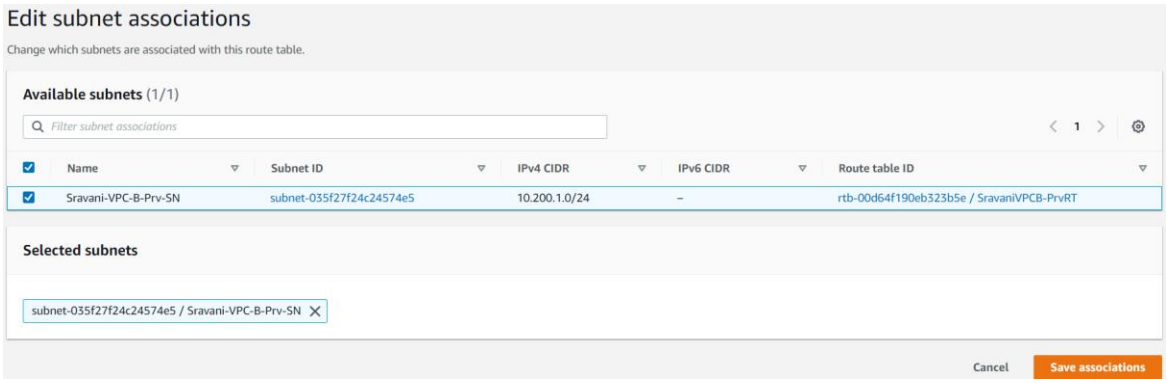


14. Create a private subnet in the above VPC

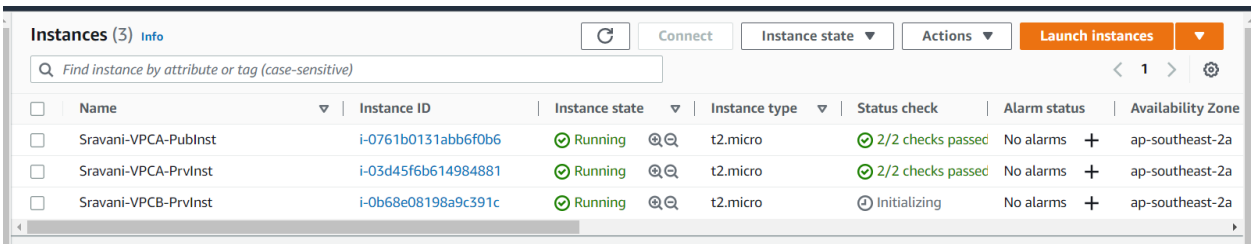


15. Create a route table and associate the private subnet above to the route table from the subnet associations menu:

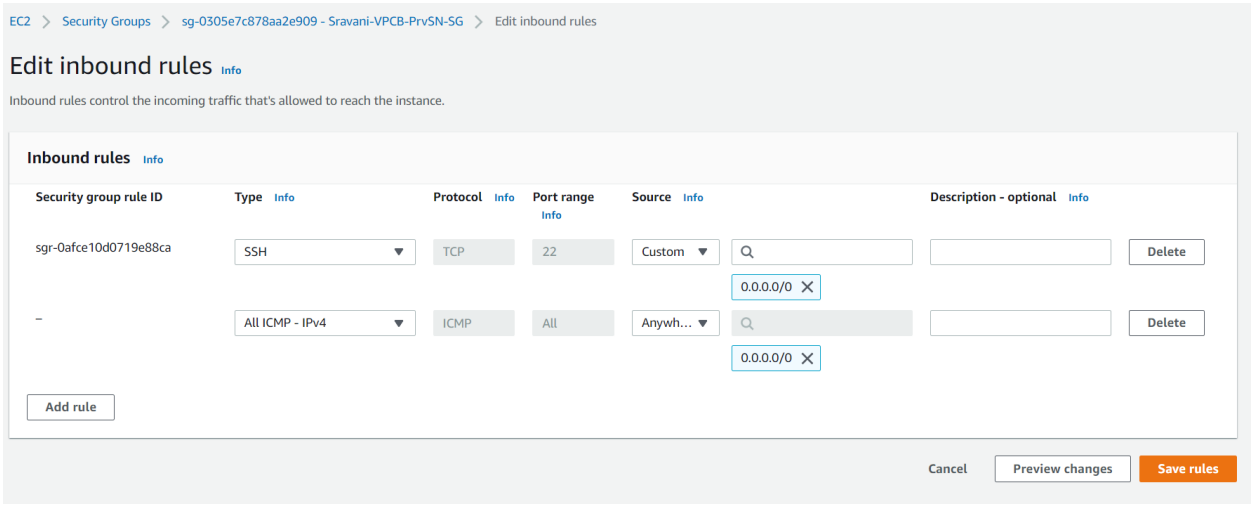




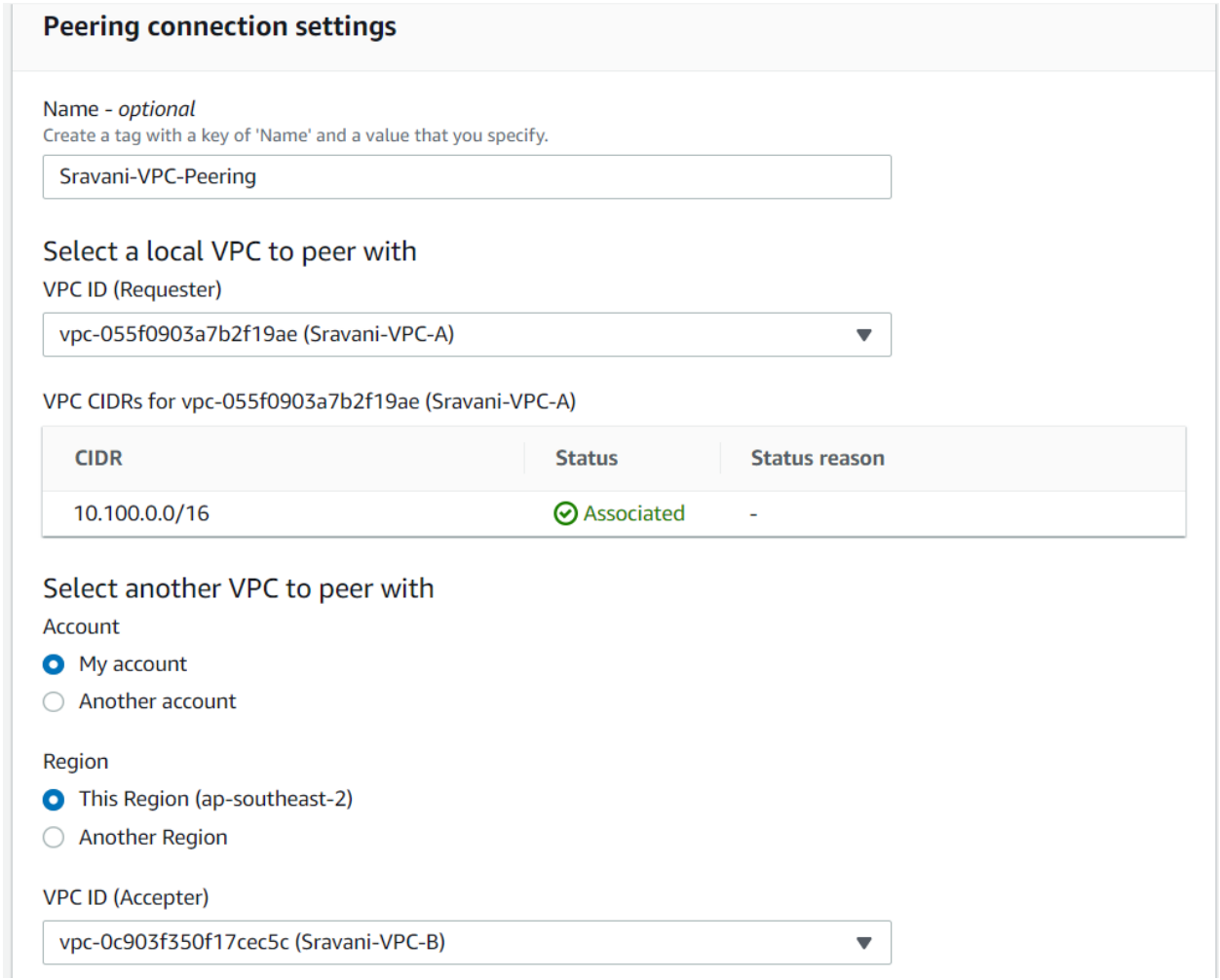
16. Create instance in the second VPC using the auto enable ip and creating a new security group:



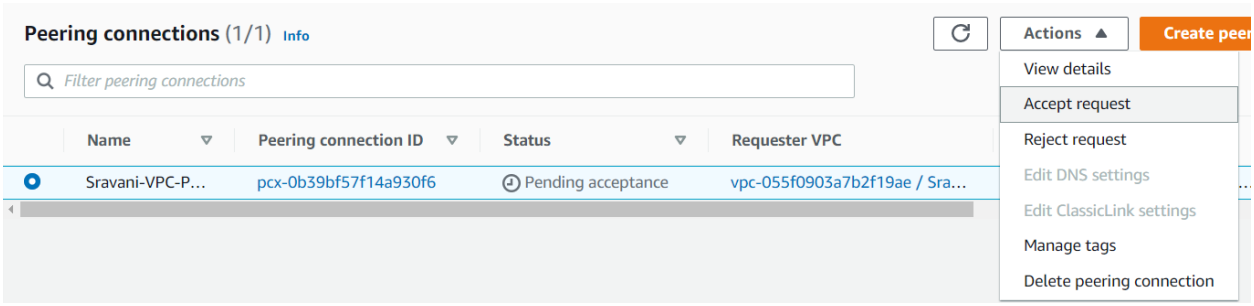
17. Edit the security group to enable All ICMPIPV4

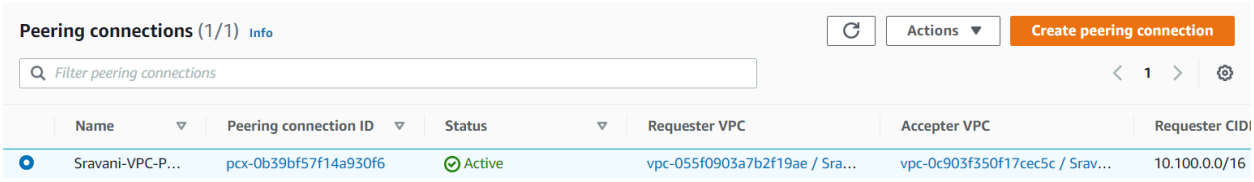


18. Create Peering connection using the following settings:

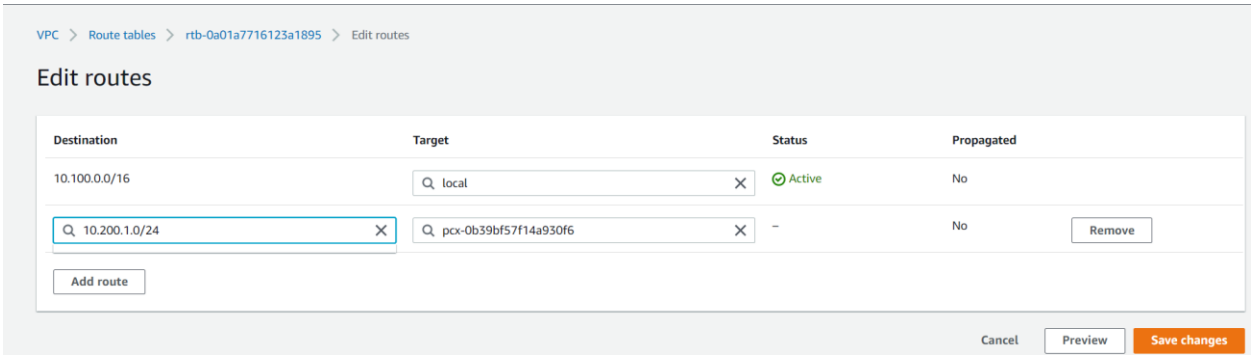


19. Accept the pending request for the peering connection:

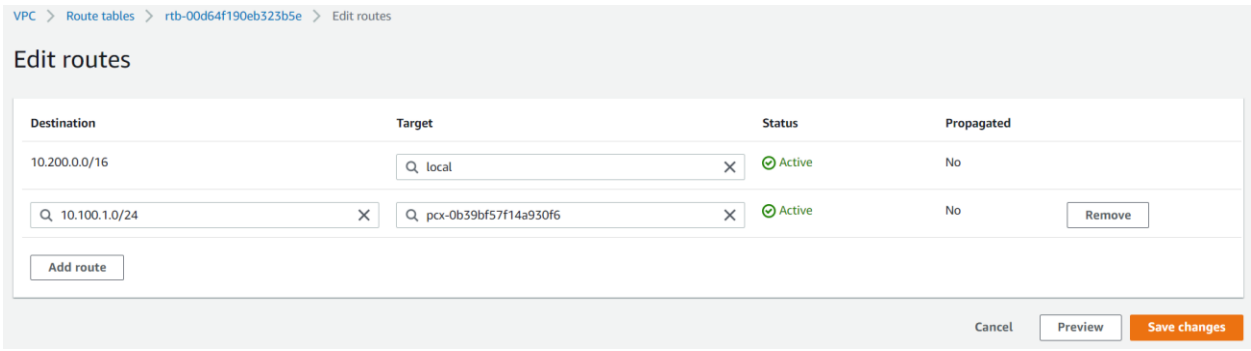




20. Update the route tables of both the private subnets of first and second VPC to make a connection from one to the other
    a. Route table of first VPC private subnet



    b. Route table of second VPC private subnet



21. Ping the private subnet instance of the second VPC from the private subnet instance of the first VPC now after adding the routes.

```
[ec2-user@ip-10-100-1-57 ~]$ pwd
/home/ec2-user
[ec2-user@ip-10-100-1-57 ~]$ ping 10.200.1.103
PING 10.200.1.103 (10.200.1.103) 56(84) bytes of data.
64 bytes from 10.200.1.103: icmp_seq=1 ttl=255 time=0.460 ms
64 bytes from 10.200.1.103: icmp_seq=2 ttl=255 time=0.507 ms
64 bytes from 10.200.1.103: icmp_seq=3 ttl=255 time=0.483 ms
64 bytes from 10.200.1.103: icmp_seq=4 ttl=255 time=0.442 ms
64 bytes from 10.200.1.103: icmp_seq=5 ttl=255 time=0.445 ms
64 bytes from 10.200.1.103: icmp_seq=6 ttl=255 time=0.500 ms
64 bytes from 10.200.1.103: icmp_seq=7 ttl=255 time=0.481 ms
64 bytes from 10.200.1.103: icmp_seq=8 ttl=255 time=0.654 ms
64 bytes from 10.200.1.103: icmp_seq=9 ttl=255 time=0.445 ms
64 bytes from 10.200.1.103: icmp_seq=10 ttl=255 time=0.506 ms
64 bytes from 10.200.1.103: icmp_seq=11 ttl=255 time=0.448 ms
^C
--- 10.200.1.103 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10239ms
rtt min/avg/max/mdev = 0.442/0.488/0.654/0.059 ms
[ec2-user@ip-10-100-1-57 ~]$
```

22. Connect from the instance in first VPC private subnet1 to the instance in second VPC private subnet 1
    a. Copy the pem file from the instance in public subnet of the first VPC to the instance in private subnet of the first VPC

```
[ec2-user@ip-10-100-0-106 ~]$ scp -i Sydney.pem -r Sydney.pem ec2-user@10.100.1.57:/home/ec2-use
r
Sydney.pem                                    100% 1674    495.2KB/s   00:00
```

    b. Connect to the private subnet machine of the first VPC from public subnet of the first VPC

```
ec2-user@ip-10-100-0-106 ~]$ ssh -i Sydney.pem ec2-user@10.100.1.57
ast login: Fri Oct 28 06:04:18 2022 from 10.100.0.106

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

ttps://aws.amazon.com/amazon-linux-2/
ec2-user@ip-10-100-1-57 ~]$ cd /home/ec2-user/
ec2-user@ip-10-100-1-57 ~]$ ls
ydney.pem
ec2-user@ip-10-100-1-57 ~]$ chmod 400 Sydney.pem
ec2-user@ip-10-100-1-57 ~]$
```

c. Now, connect to the private subnet machine of the first VPC to the private subnet instance of the second VPC using the private ip