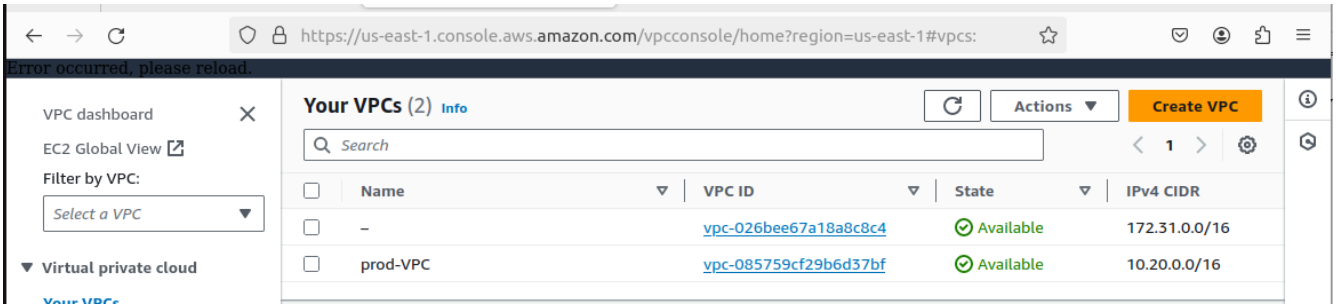
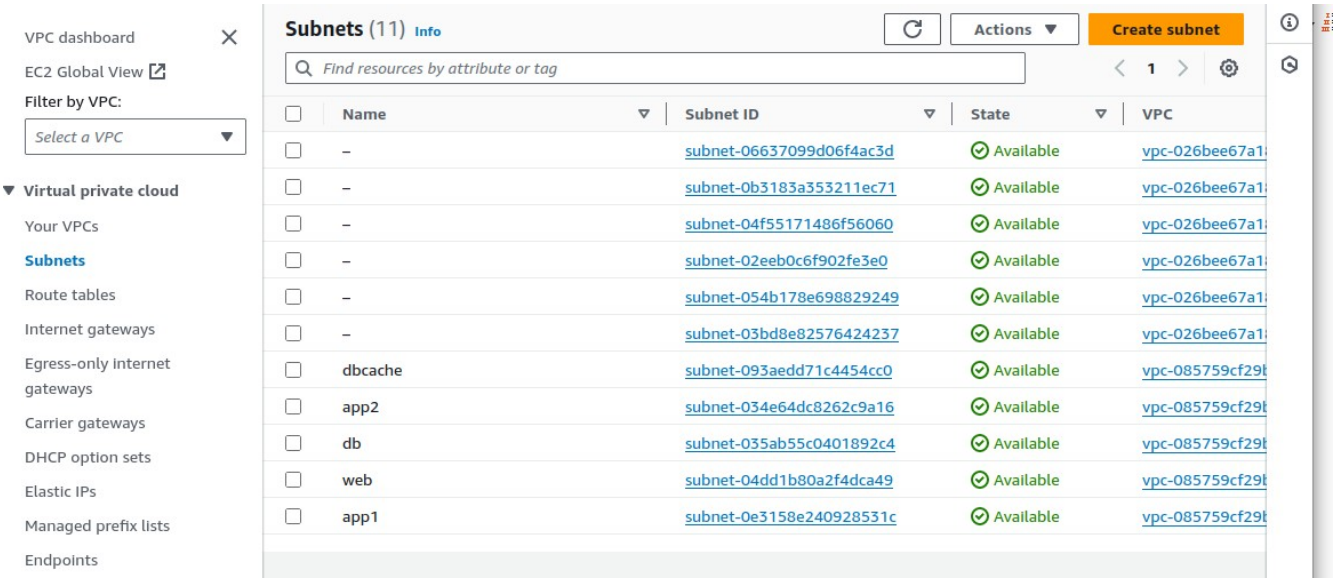
You work for XYZ Corporation, and based on the expansion requirements of your company, you have been asked to create and setup distinct Amazon VPCs for production and development teams.
You are expected to perform the following tasks for the respective VPCs:

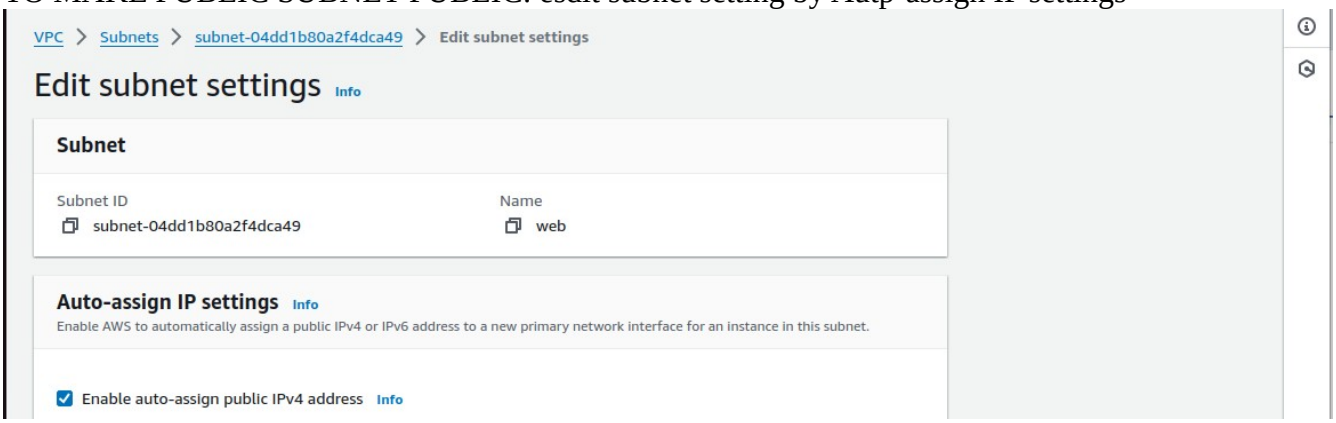
For the production network:
1. Design and build a four-tier architecture
2. Create five subnets. Among them, four should be private with names app1, app2, dbcache, and db, and the fifth one should be public with the name web
3. Launch instances in all subnets, and name them as per the subnet as they are launched in
4. Allow the dbcache instance and the app1 subnet to send Internet requests
5. Manage security groups and NACLs
6. Create a VPC Endpoint for the S3 service, and access the objects in any bucket from within the VPC

For the development network:
1. Design and build a two-tier architecture with two subnets named web and db, and launch instances in both subnets, naming them as per the subnet names
2. Make sure that only web subnet can send Internet requests
3. Create a peering connection between the production network and the development network
4. Setup a connection between the db subnets of both the production network and the development network, respectively

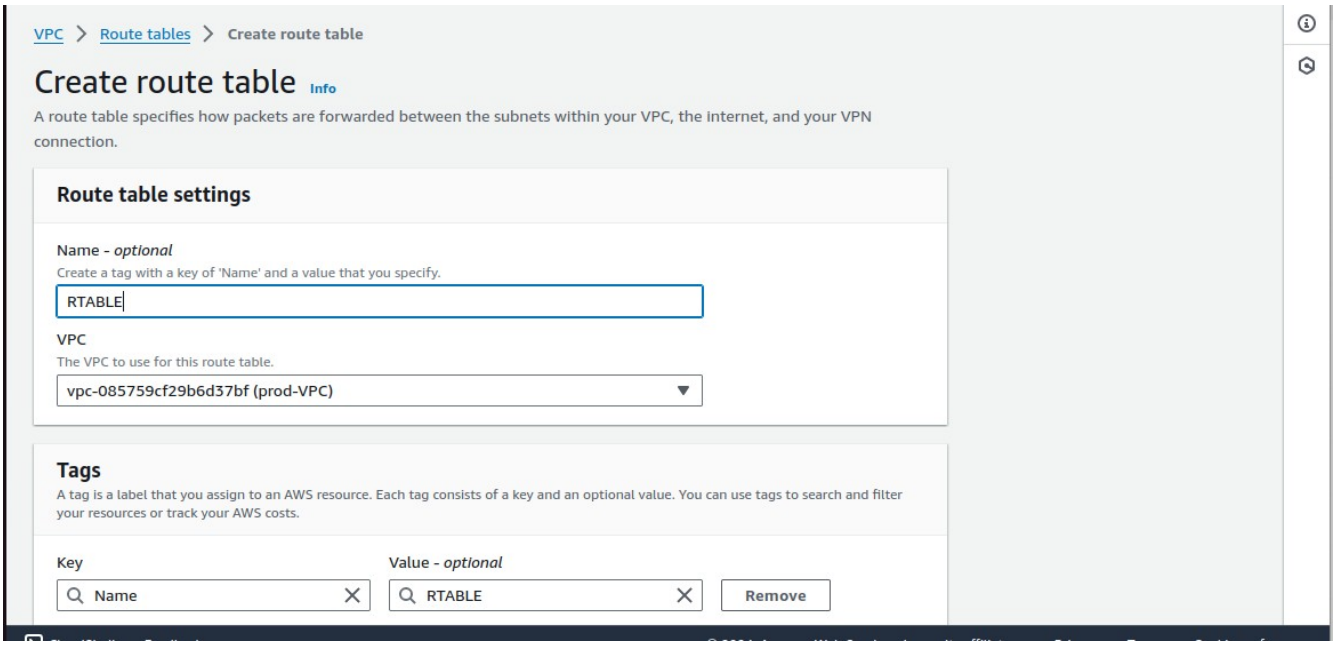


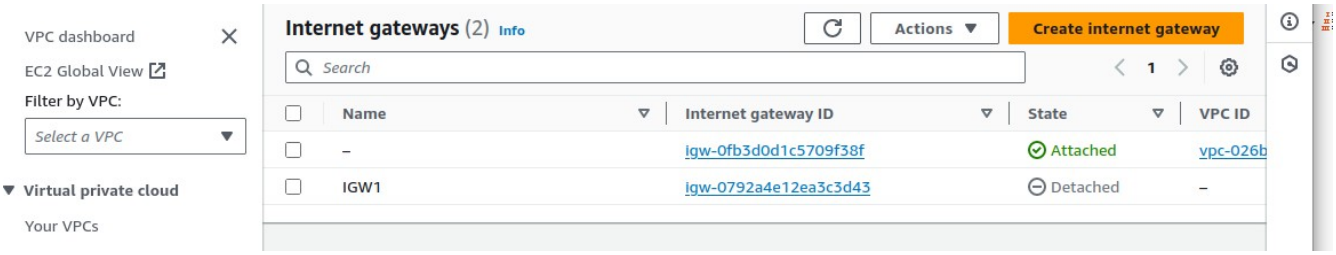


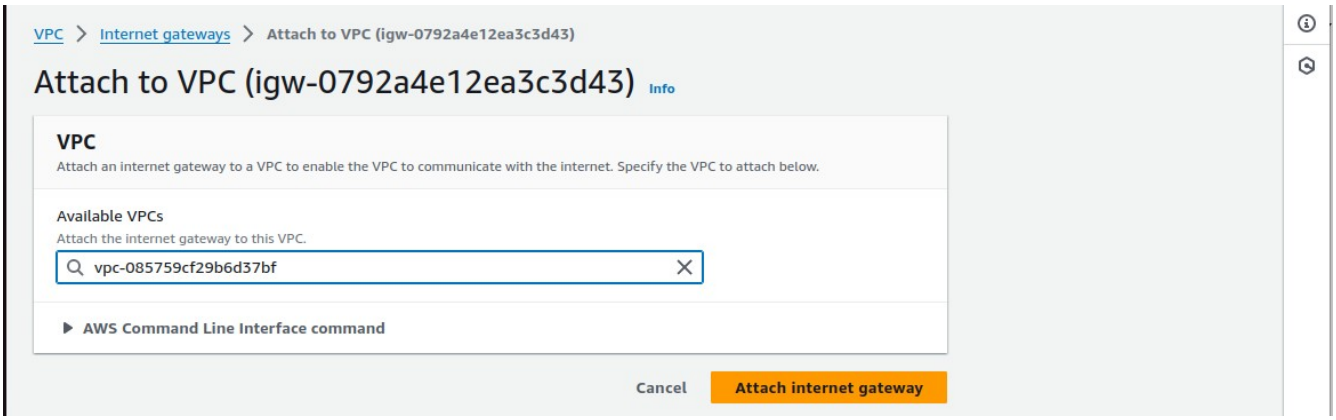
TO MAKE PUBLIC SUBNET PUBLIC: esdit subnet setting by Autp-assign IP settings



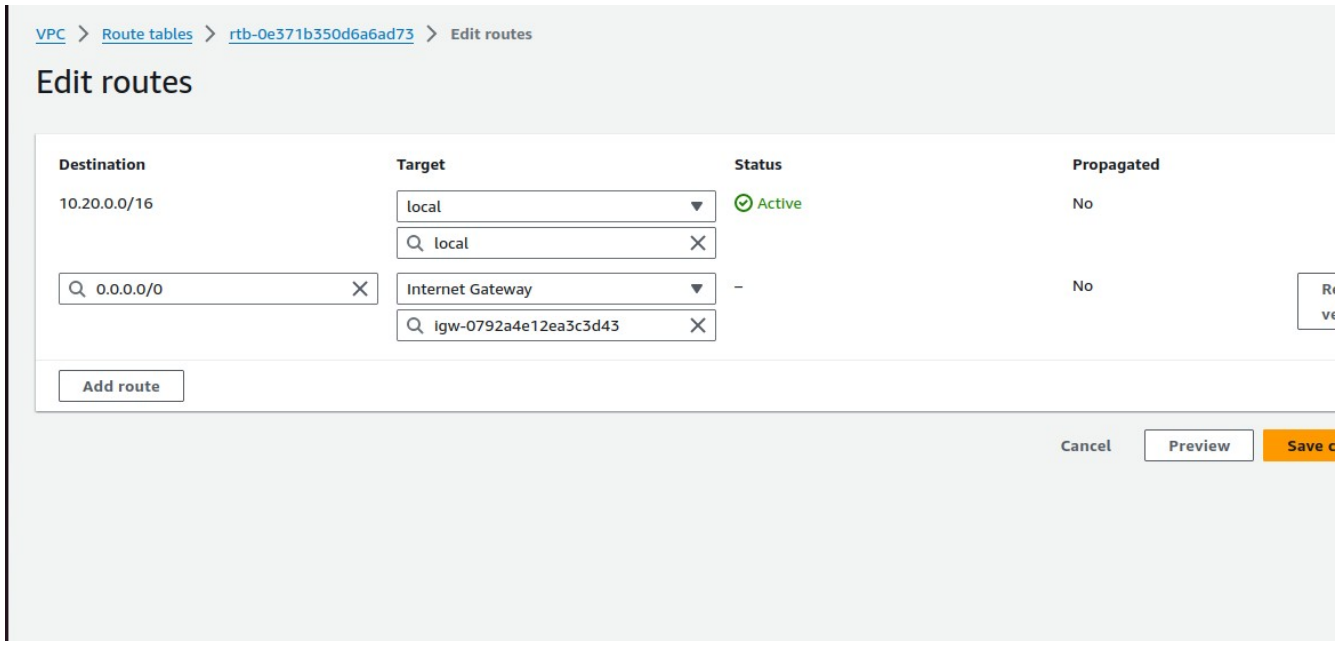
CREATE ROUTE-TABLE: ASS THE VPC CREATED WITH IT



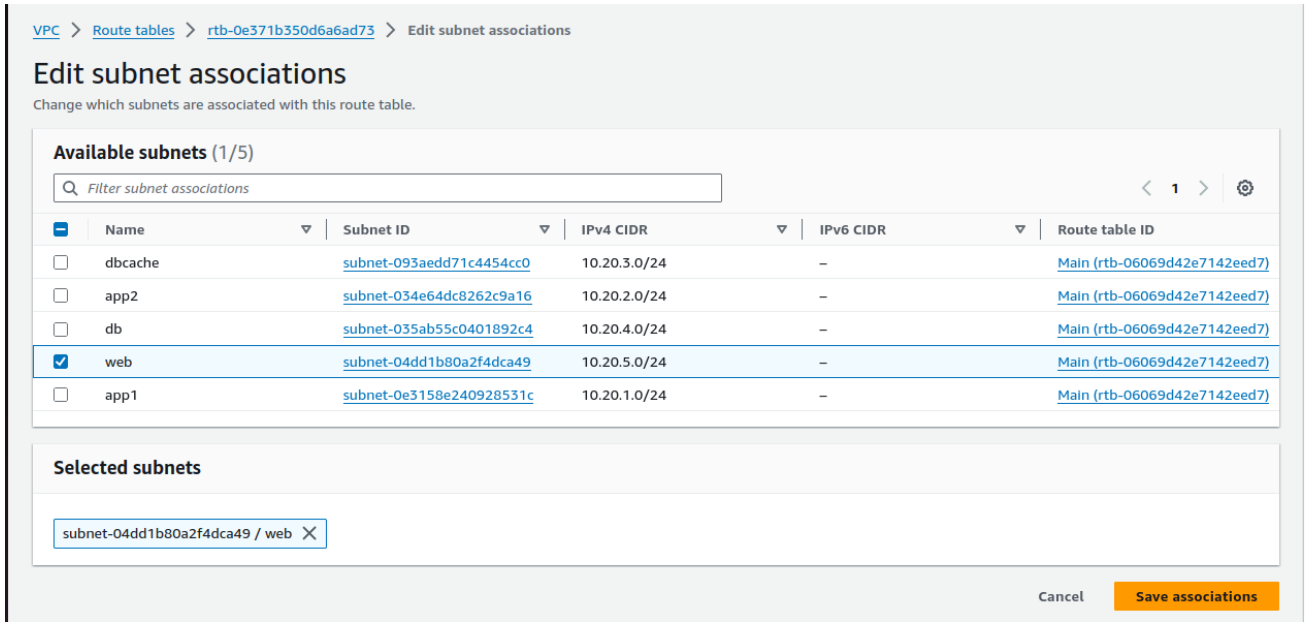


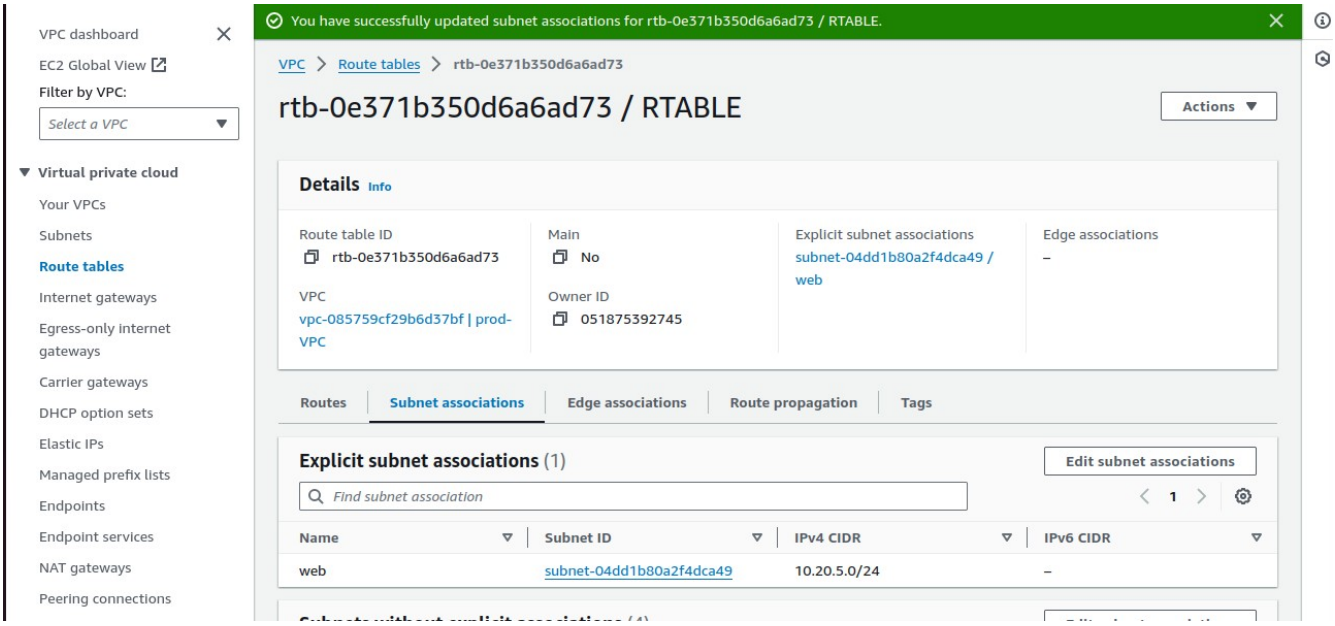


ASSOCIATE IGW with route table created



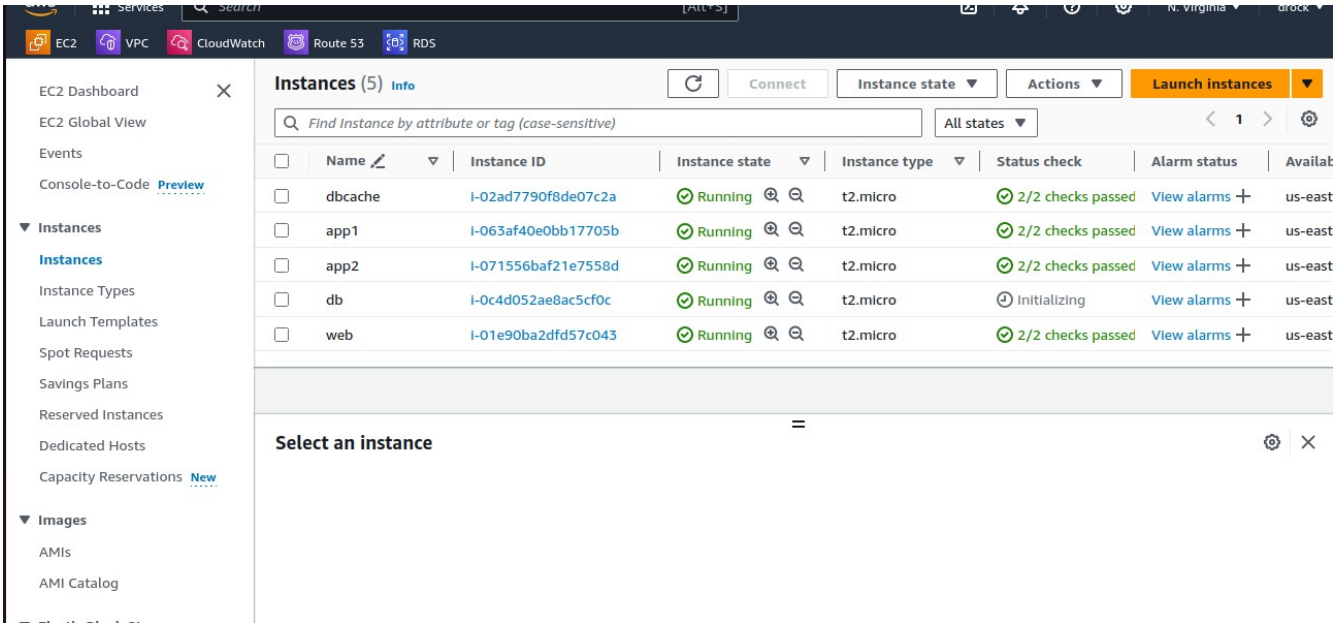
ASSOCIATE ONLY PUBLIC SUBNET TO THE RT





Now five subnets are created. app1, app2, dbcache, and db are private, and the fifth one: web is public.

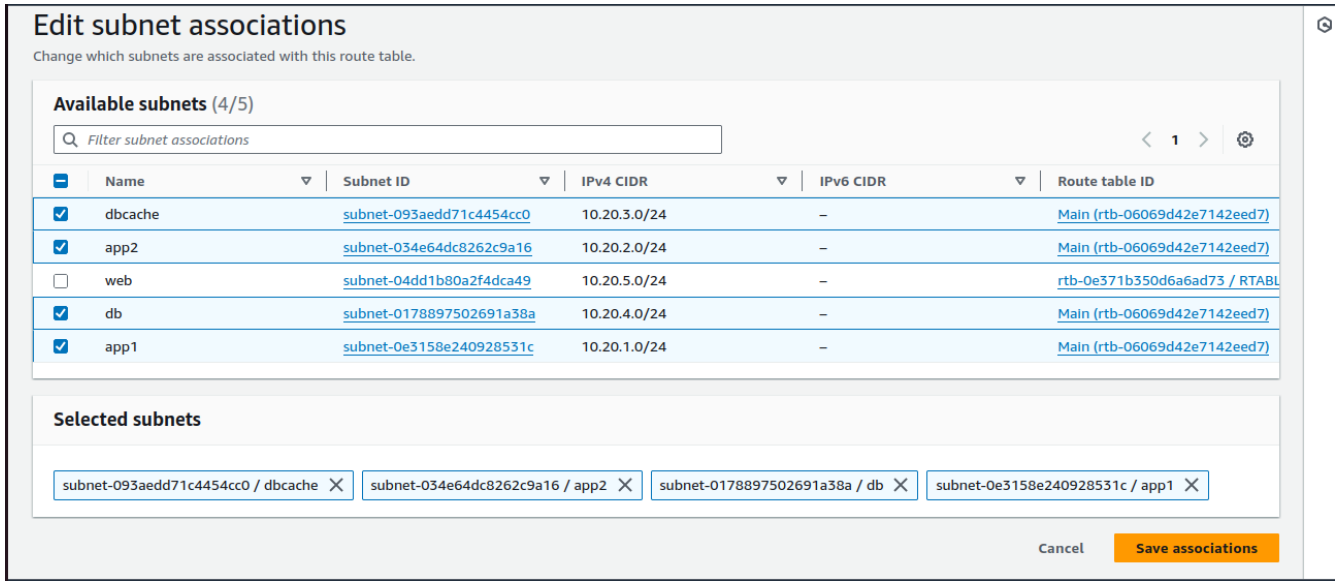
3. Launch instances in all subnets, and name them as per the subnet as they are launched in



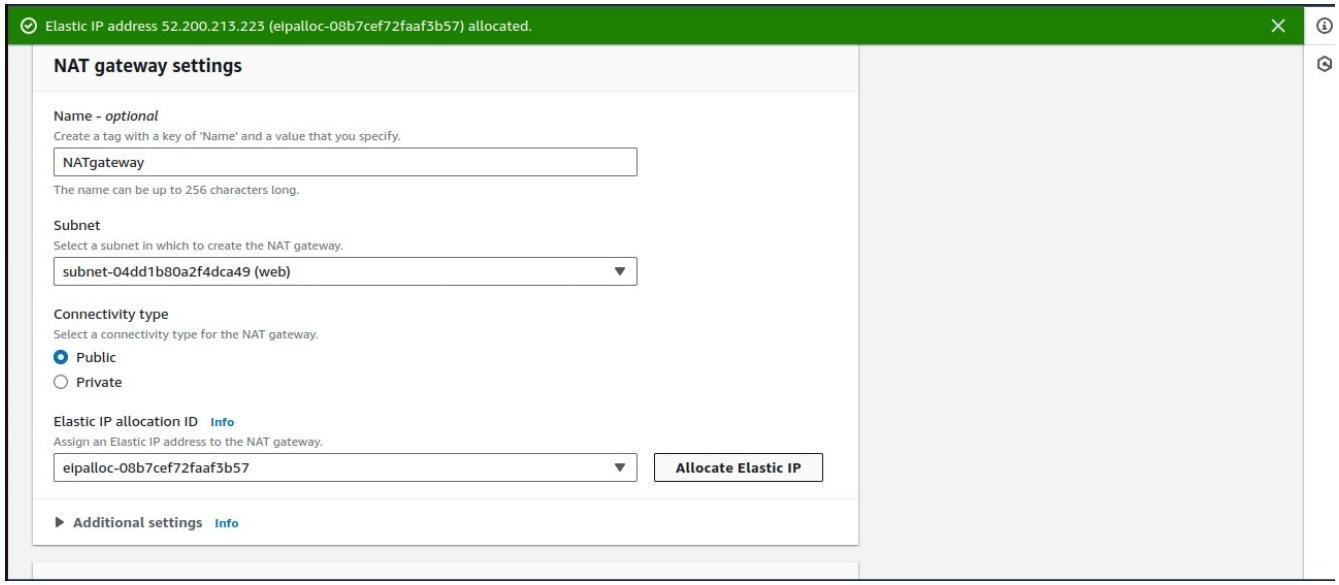
4. Allow the dbcache instance and the app1 subnet to send Internet requests

The private instance in the private subnets need NATgateway to be able to have access to internet.
1: CREATE PRIVATE RT

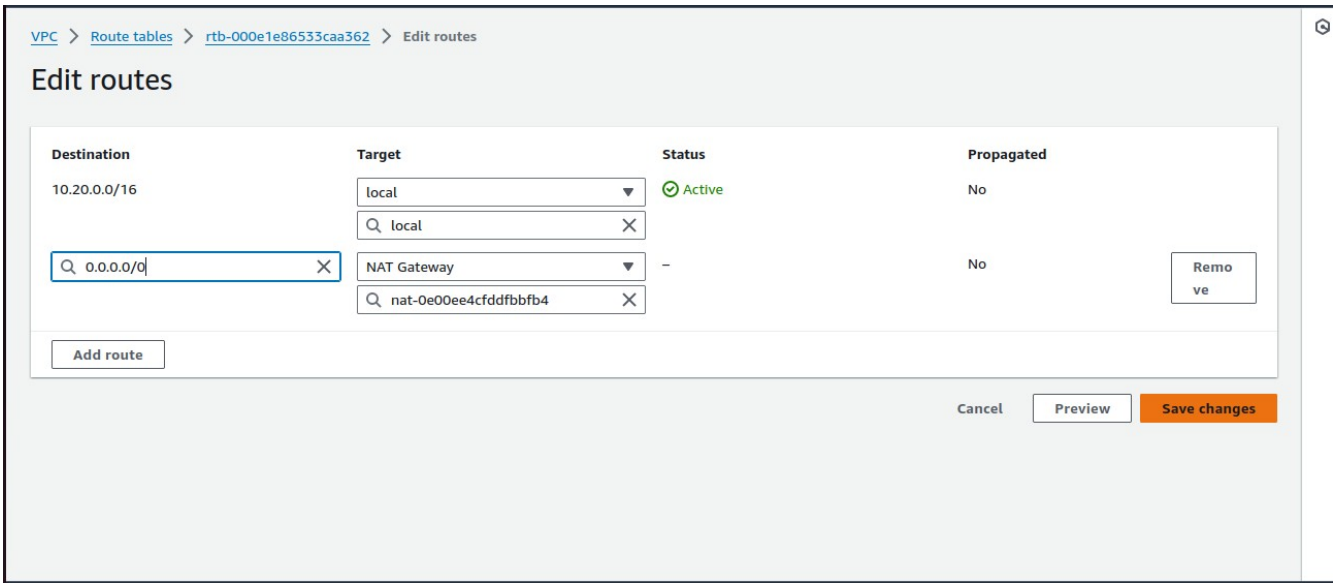
ASSOCIATE PRIVATE SUBNETS TO IT



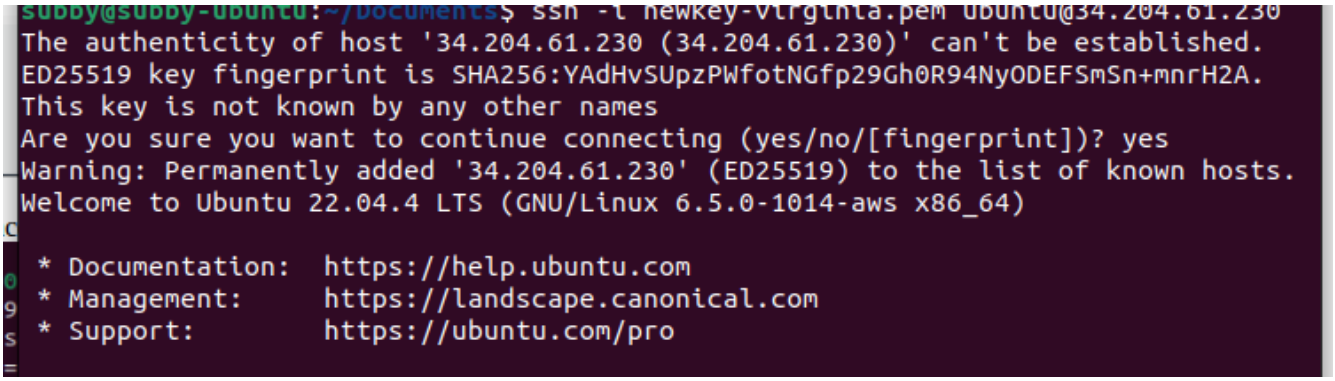
CREATE NAT-gateway
-- pick public subnet
-- EIP allocate



In Private RT: edit annd pit NAT-gateway



TEST ‘web’ instances



```
ubuntu@ip-10-20-5-123:~$ sudo ping aws.com
PING aws.com (99.84.108.3) 56(84) bytes of data.
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=
1 ttl=245 time=0.780 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=
2 ttl=245 time=0.789 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=
3 ttl=245 time=0.845 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=
4 ttl=245 time=0.836 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=
5 ttl=245 time=0.864 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=
6 ttl=245 time=0.898 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=
7 ttl=245 time=0.828 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=
8 ttl=245 time=0.914 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=
9 ttl=245 time=0.899 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=
10 ttl=245 time=0.828 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=
```

PublicIPs: 18.206.81.213 PrivateIPs: 20.0.1.228

CloudShell Feedback © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie pref

4. Allow the dbcache instance and the app1 subnet to send Internet requests

~/Documents: being location of keypair on my local pc

scp -i ~/Documents/newkey-virginia.pem ~/Documents/newkey-virginia.pem ubuntu@34.204.61.230:/home/ubuntu/newkey-virginia.pem

scp (secure copy) command to securely transfer the private key file from local device to the instance.

ssh -i ~/Documents/newkey-virginia.pem ubuntu@34.204.61.230 : public ip

After running this command, the private key file should be securely transferred to the specified location on the remote instance.

ssh -i /home/ubuntu/newkey-virginia.pem ubuntu@10.20.1.211 : private ip

```
ubuntu@ip-10-20-1-211:~$ sudo ping aws.com
PING aws.com (99.84.108.37) 56(84) bytes of data.
64 bytes from server-99-84-108-37.iad79.r.cloudfront.net (99.84.108.37): icmp_seq=1 ttl=243 time=1.68 ms
64 bytes from server-99-84-108-37.iad79.r.cloudfront.net (99.84.108.37): icmp_seq=2 ttl=243 time=1.47 ms
64 bytes from server-99-84-108-37.iad79.r.cloudfront.net (99.84.108.37): icmp_seq=3 ttl=243 time=1.40 ms
64 bytes from server-99-84-108-37.iad79.r.cloudfront.net (99.84.108.37): icmp_seq=4 ttl=243 time=1.46 ms
64 bytes from server-99-84-108-37.iad79.r.cloudfront.net (99.84.108.37): icmp_seq=5 ttl=243 time=1.41 ms
64 bytes from server-99-84-108-37.iad79.r.cloudfront.net (99.84.108.37): icmp_seq=6 ttl=243 time=1.40 ms
64 bytes from server-99-84-108-37.iad79.r.cloudfront.net (99.84.108.37): icmp_seq=7 ttl=243 time=1.60 ms
64 bytes from server-99-84-108-37.iad79.r.cloudfront.net (99.84.108.37): icmp_seq=8 ttl=243 time=1.51 ms
64 bytes from server-99-84-108-37.iad79.r.cloudfront.net (99.84.108.37): icmp_seq=9 ttl=243 time=1.46 ms
```

OR

EC2 Instance Connect to Public instance and from there; ssh into private instance.
ssh -i newkey-virginia.pem ubuntu@10.20.1.211 :…….. private ip

app1 server

```
ubuntu@ip-10-20-5-123:~$ ssh -i newkey-virginia.pem ubuntu@10.20.1.211
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-1014-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

  System information as of Fri Apr 19 20:02:13 UTC 2024

  System load:  0.0               Processes:             98
  Usage of /:   20.7% of 7.57GB   Users logged in:       1
```

```
ubuntu@ip-10-20-1-211:~$ sudo ping aws.com
PING aws.com (99.84.108.3) 56(84) bytes of data.
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=1 ttl=244 time=1.65 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=2 ttl=244 time=1.53 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=3 ttl=244 time=1.43 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=4 ttl=244 time=1.42 ms
64 bytes from server-99-84-108-3.iad79.r.cloudfront.net (99.84.108.3): icmp_seq=5 ttl=244 time=1.42 ms
^C
--- aws.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 1.421/1.489/1.645/0.088 ms
```

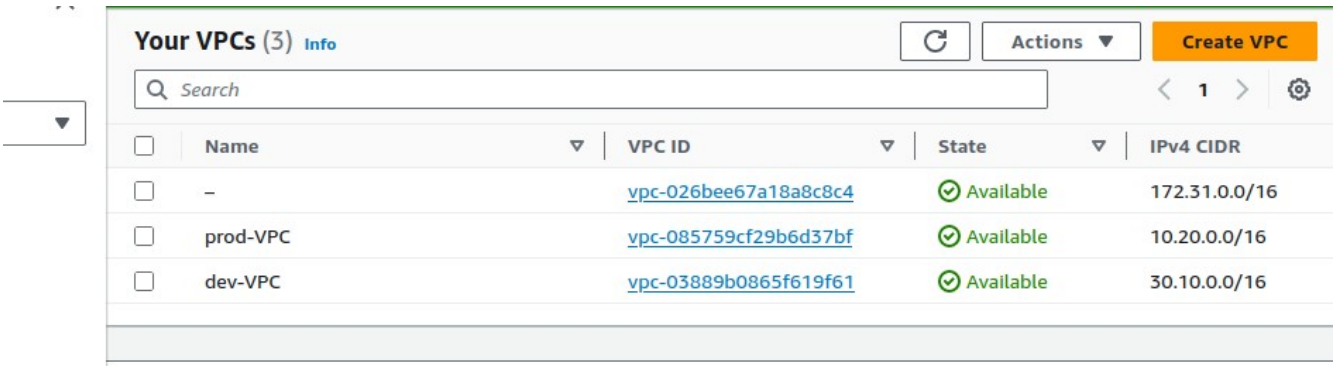
dbcache server

```
ubuntu@ip-10-20-5-123:~$ ssh -i newkey-virginia.pem ubuntu@10.20.3.244
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-1014-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

  System information as of Fri Apr 19 20:19:44 UTC 2024

  System load:  0.0               Processes:             97
  Usage of /:   20.4% of 7.57GB   Users logged in:       0
```

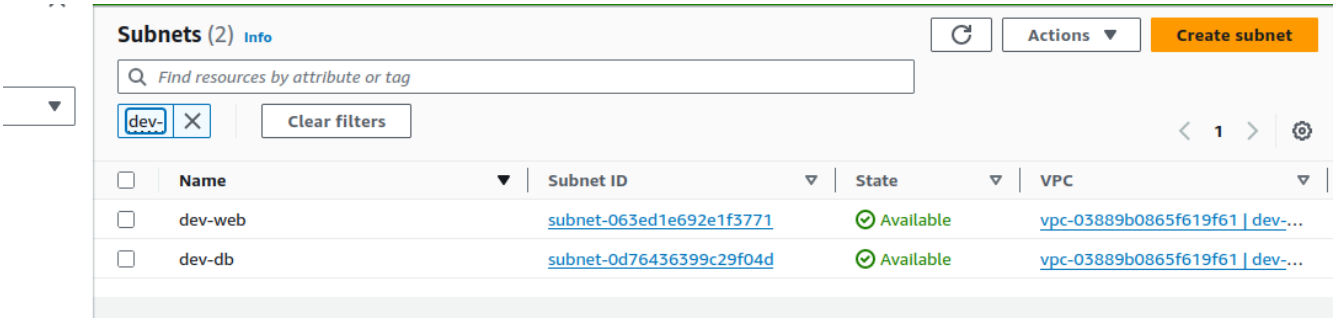
```
ubuntu@ip-10-20-3-244:~$ sudo ping google.com
PING google.com (172.253.122.139) 56(84) bytes of data.
64 bytes from bh-in-f139.1e100.net (172.253.122.139): icmp_seq=1 ttl=101 time=2.99 ms
64 bytes from bh-in-f139.1e100.net (172.253.122.139): icmp_seq=2 ttl=101 time=2.76 ms
64 bytes from bh-in-f139.1e100.net (172.253.122.139): icmp_seq=3 ttl=101 time=2.66 ms
64 bytes from bh-in-f139.1e100.net (172.253.122.139): icmp_seq=4 ttl=101 time=2.66 ms
64 bytes from bh-in-f139.1e100.net (172.253.122.139): icmp_seq=5 ttl=101 time=2.70 ms
64 bytes from bh-in-f139.1e100.net (172.253.122.139): icmp_seq=6 ttl=101 time=2.81 ms
c64 bytes from bh-in-f139.1e100.net (172.253.122.139): icmp_seq=7 ttl=101 time=2.66 ms
64 bytes from bh-in-f139.1e100.net (172.253.122.139): icmp_seq=8 ttl=101 time=2.77 ms
64 bytes from bh-in-f139.1e100.net (172.253.122.139): icmp_seq=9 ttl=101 time=2.71 ms
```

For the development network:
1. Design and build a two-tier architecture with two subnets named web and db, and launch instances in both subnets, naming them as per the subnet names

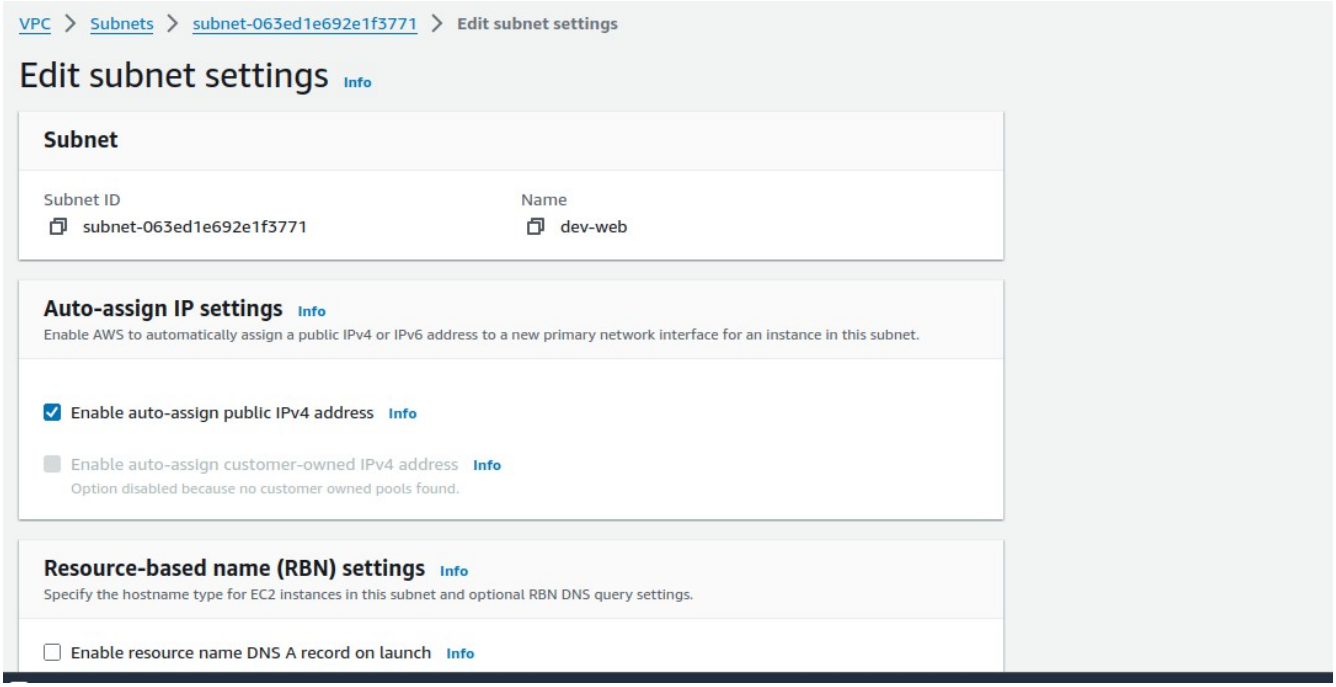
DEV-VPC



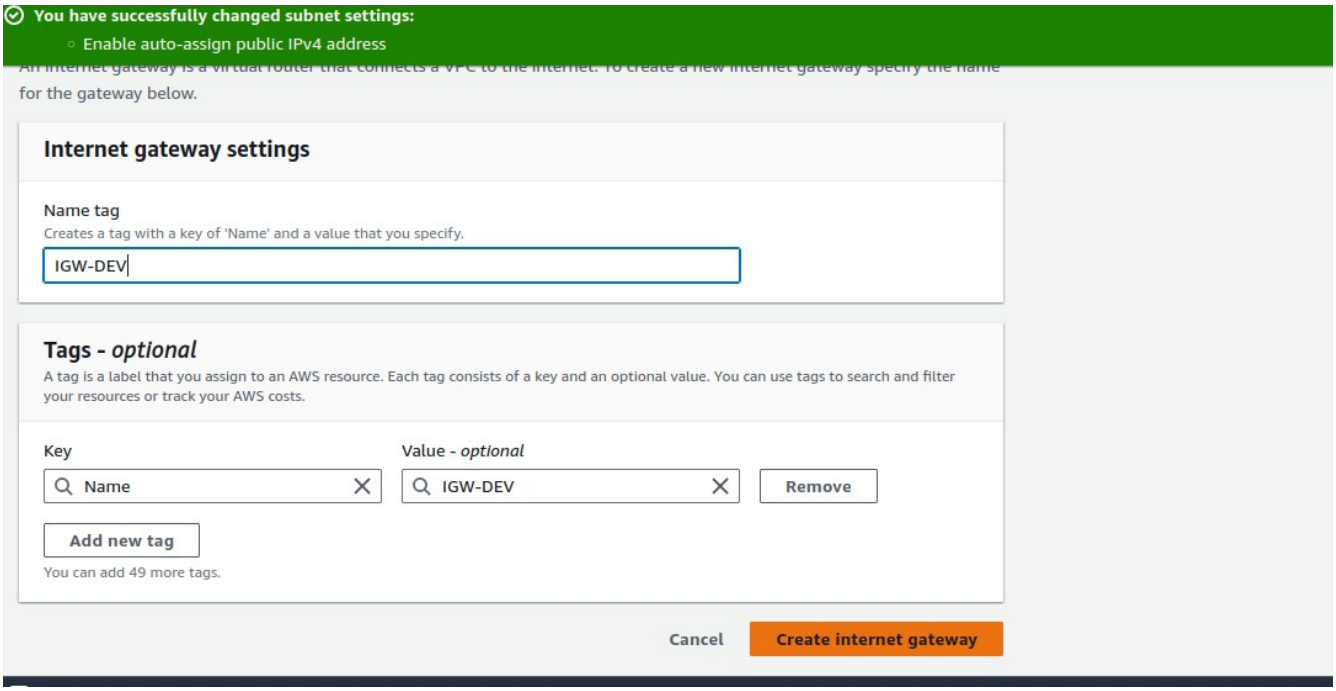
2SUBNETS: WEB AND DB



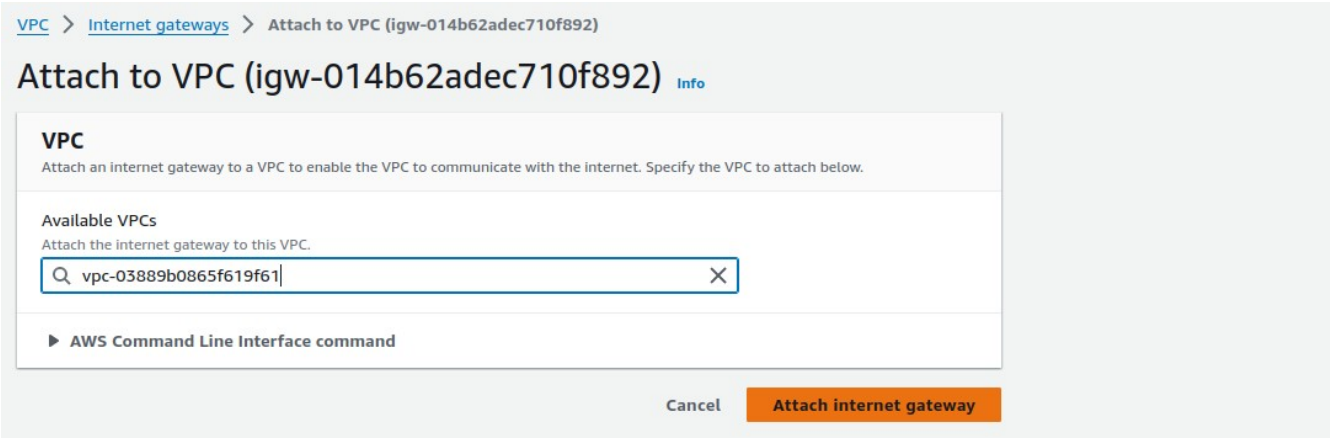
AUTO ASSIGN IP TO THE PUB SUBNET



CREATE IGW

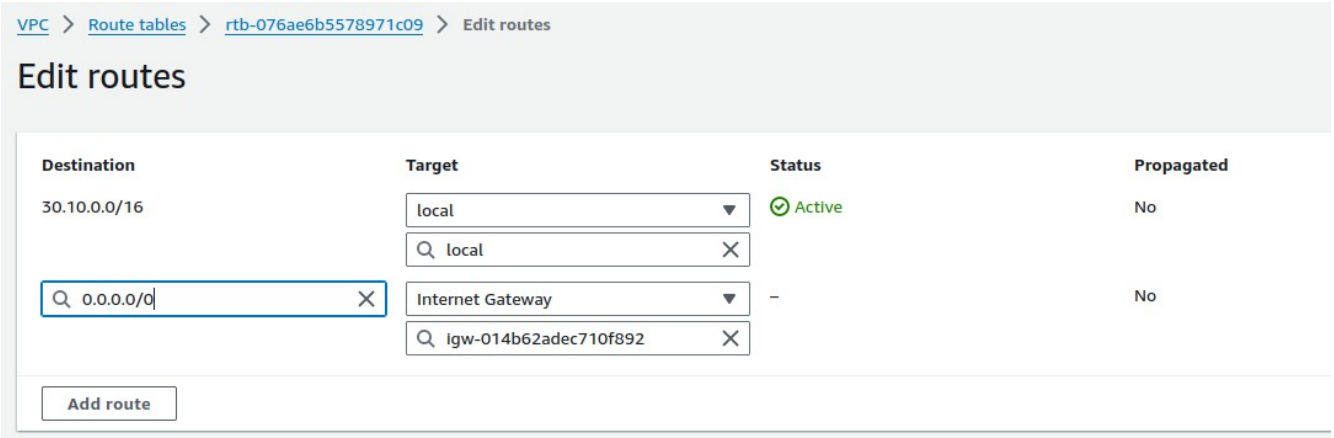


ATTACH IGW TO VPC

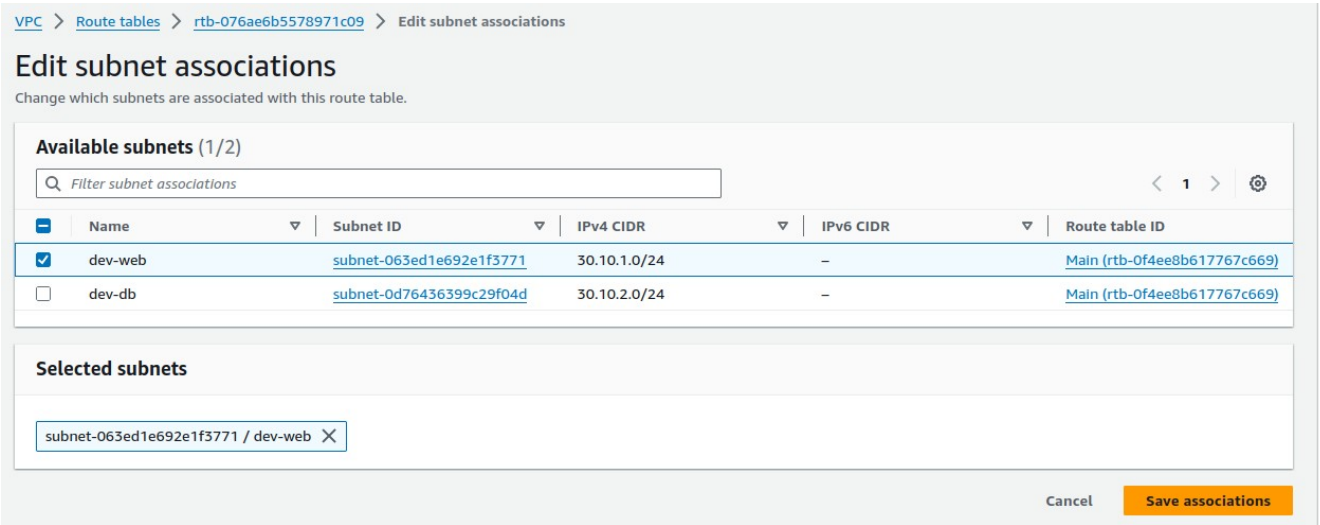


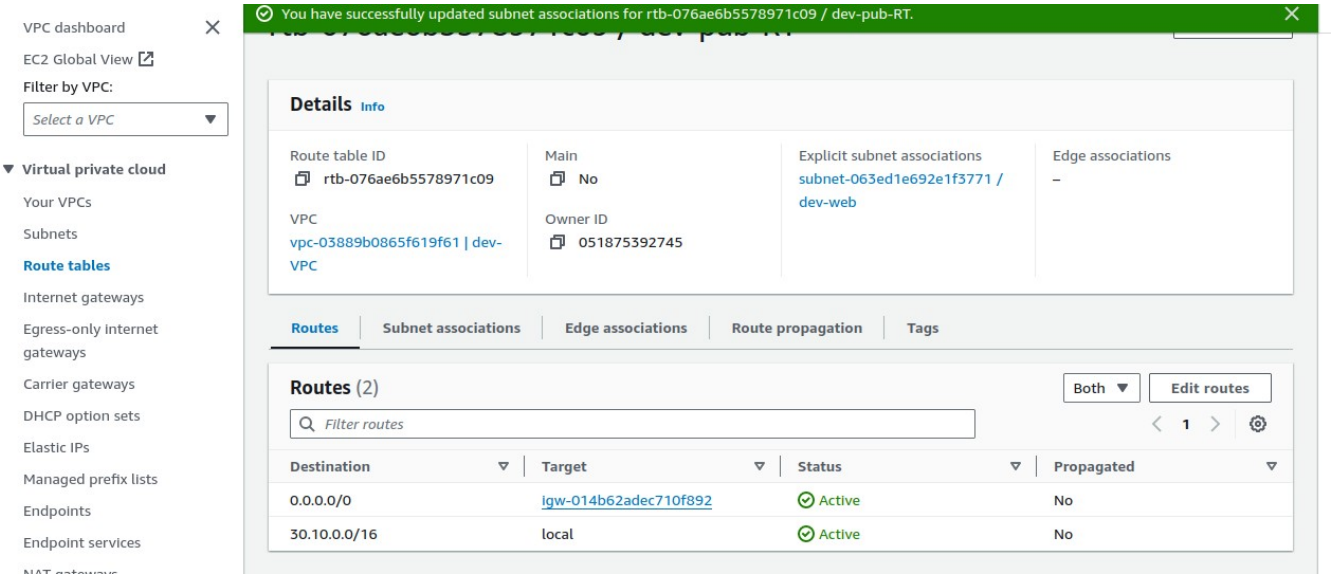
CREATE RT

& edit RT and pick target as igw

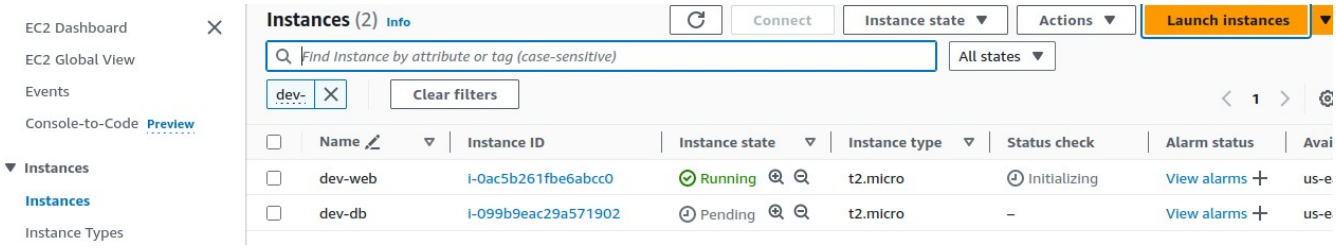


RT association with public subnet

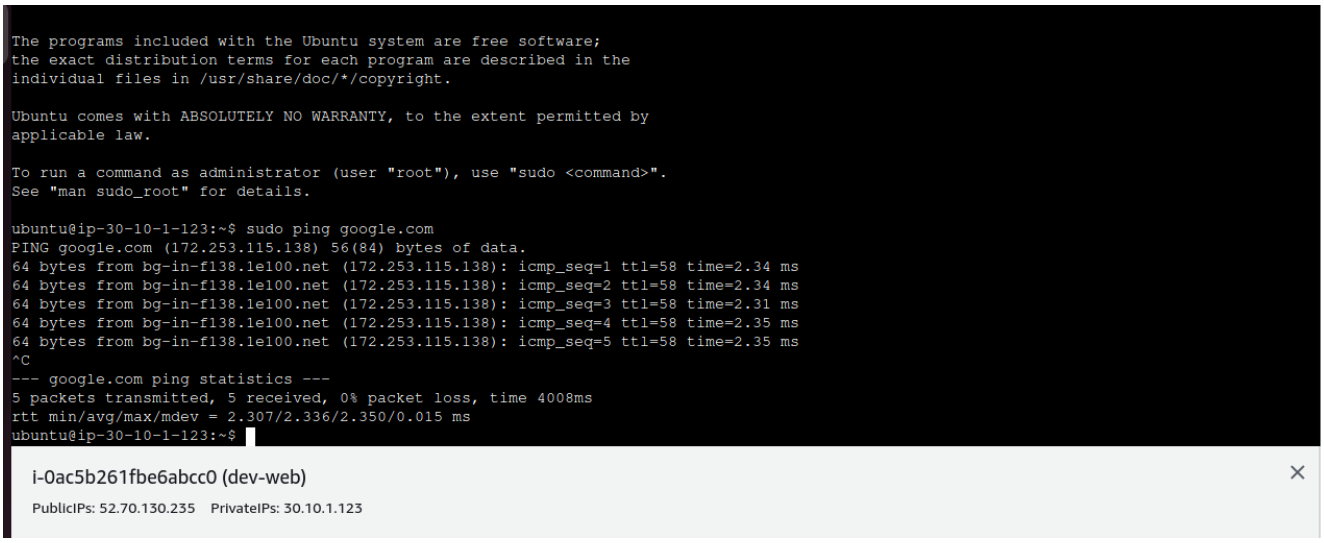




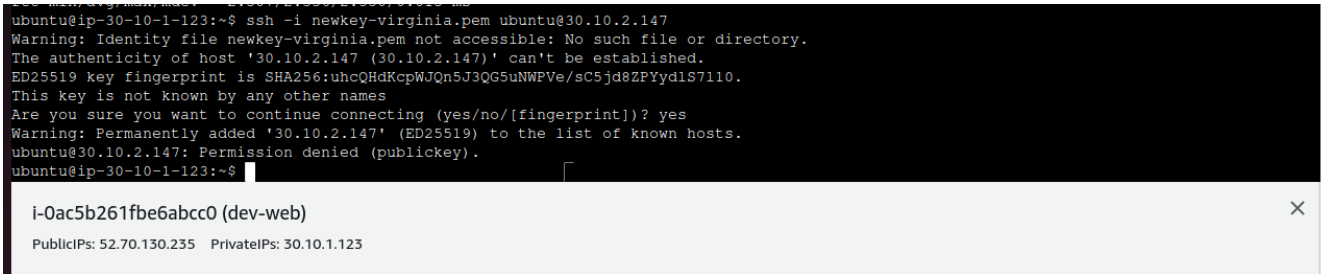
launch instances in both subnets, naming them as per the subnet names



dev-web instance can access internet

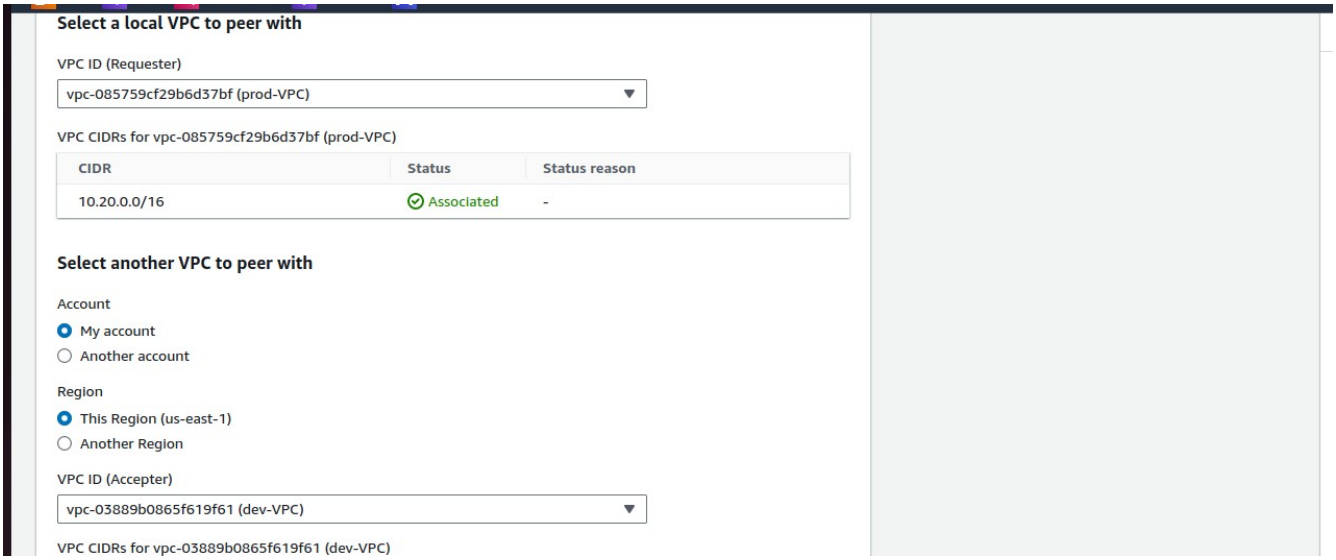


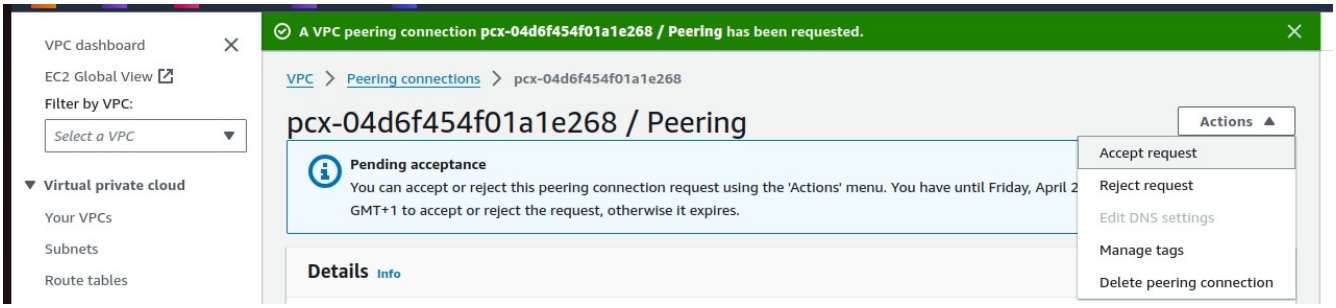
dev-db can not access internet (not even when ssh from public instance)NATgateway was not created



3. Create a peering connection between the production network and the development network

CREATE PEERING CONNECTION BETWEEN PROD-VPC AND DEV-VPC

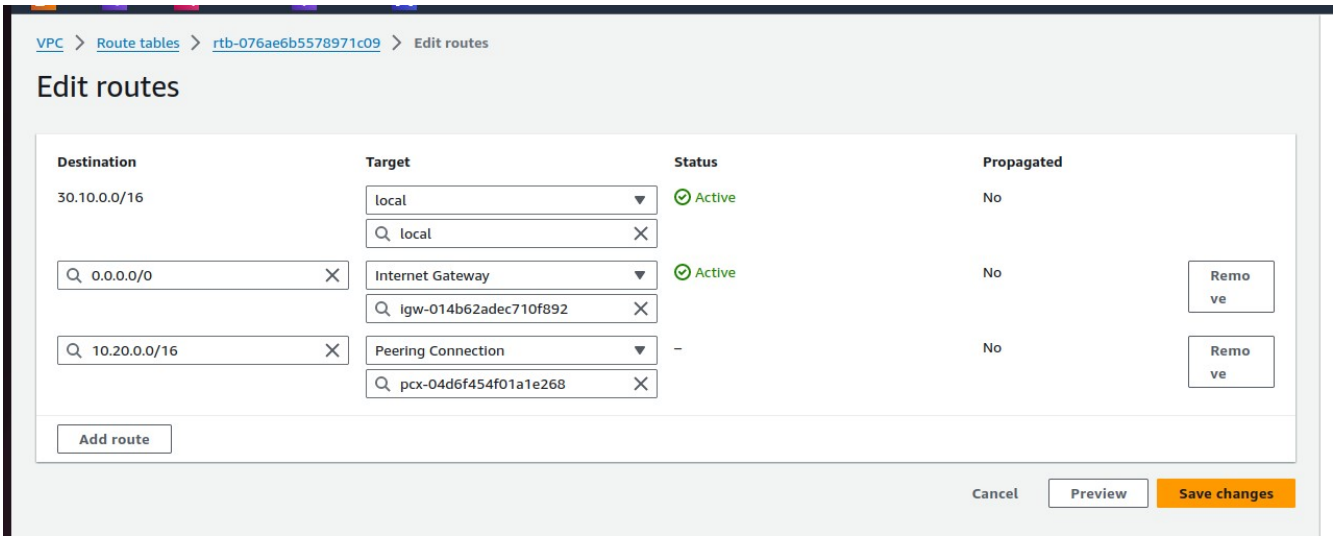




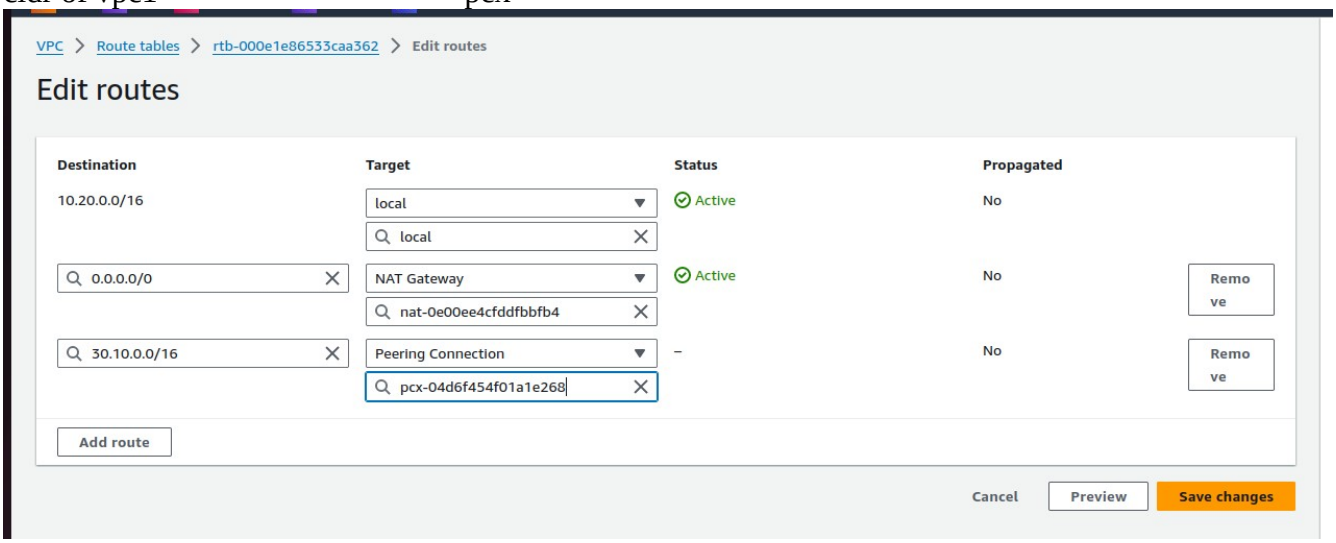
EDIT RT OF THE VPC

PUBLIC RT VPC2 I.e dev

cidr of vpc1 ---------- pcx



PRIVATE RT OF VPC1 I.e production
cidr of vpc1 ---------- pcx



NOW, connect to public instance of a VPC and from their attempt to connect to private instance of another VPC / ping private instance from public instances