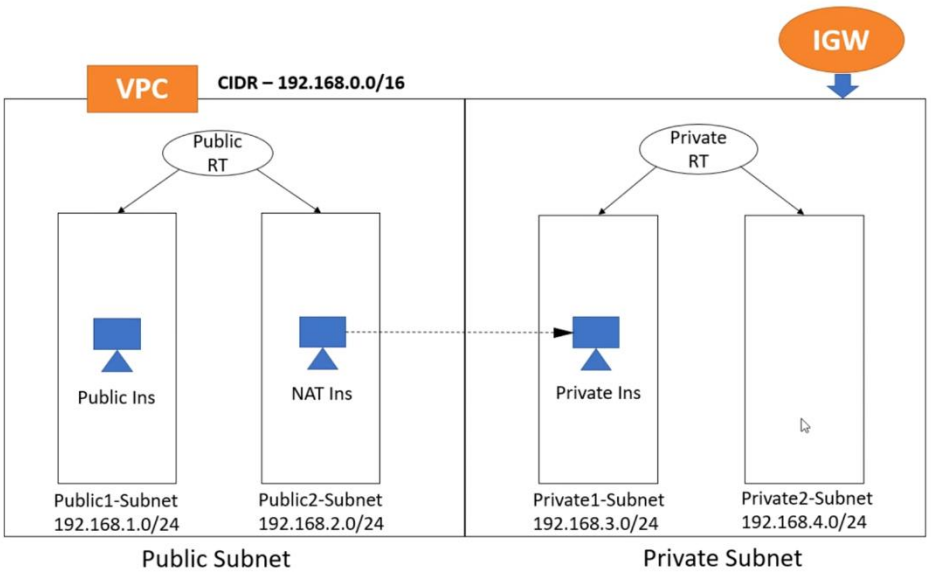
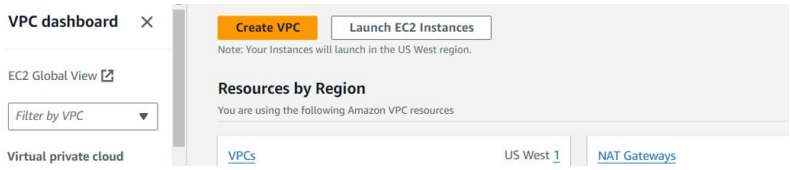
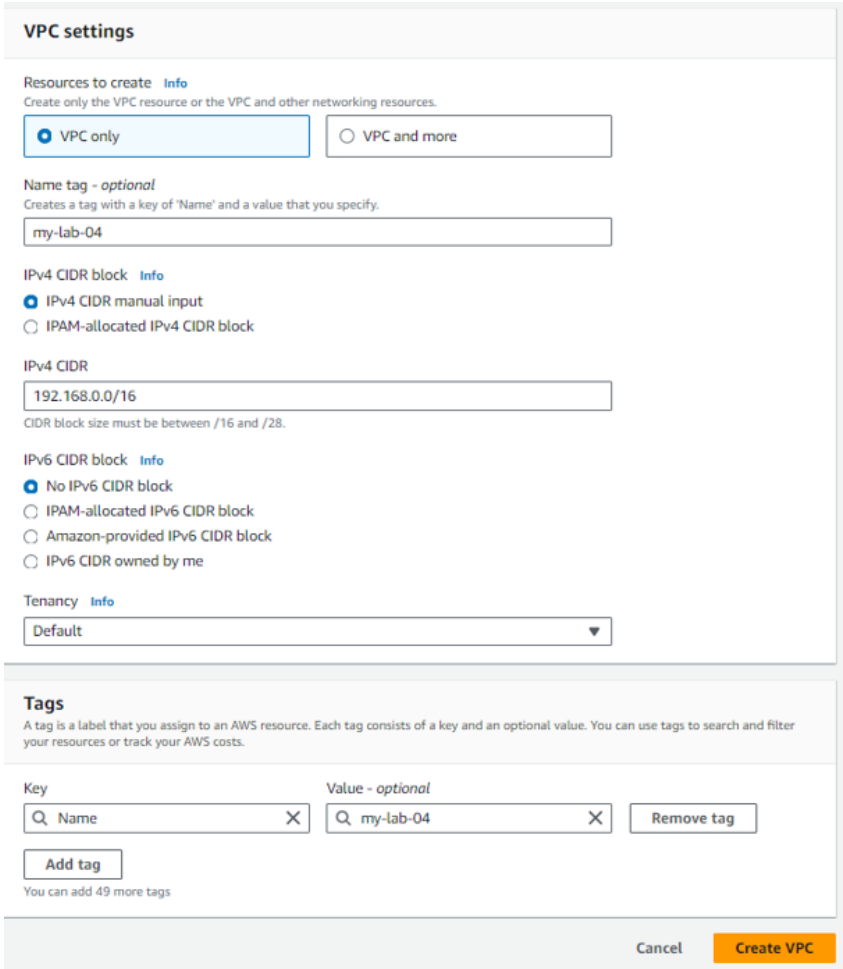
LAB 04: VPC Setup



Step 1: Create VPC: CIDR: 192.168.0.0/16

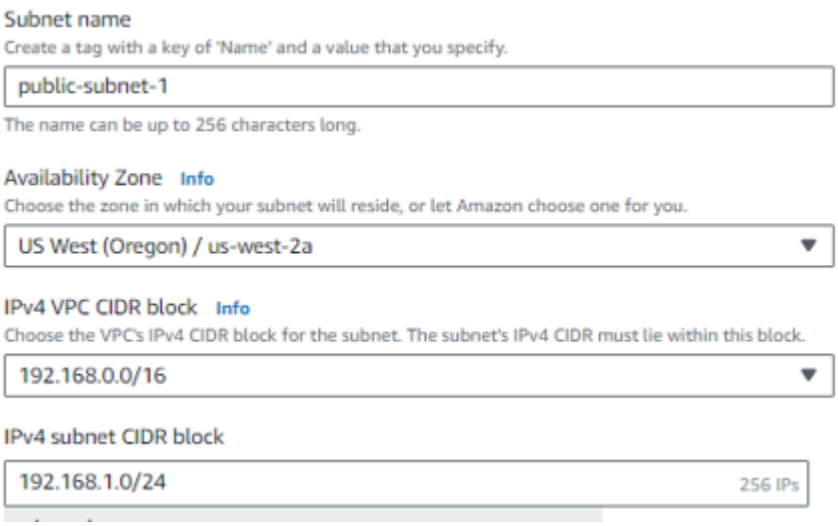




Step 2: Create Subnets:

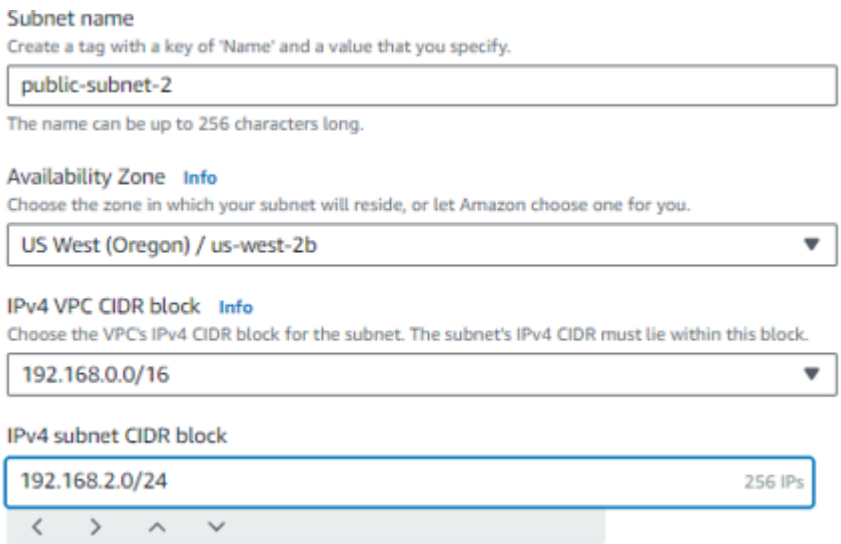
public-subnet-1

CIDR: 192.168.1.0/24 and check the availability zone also



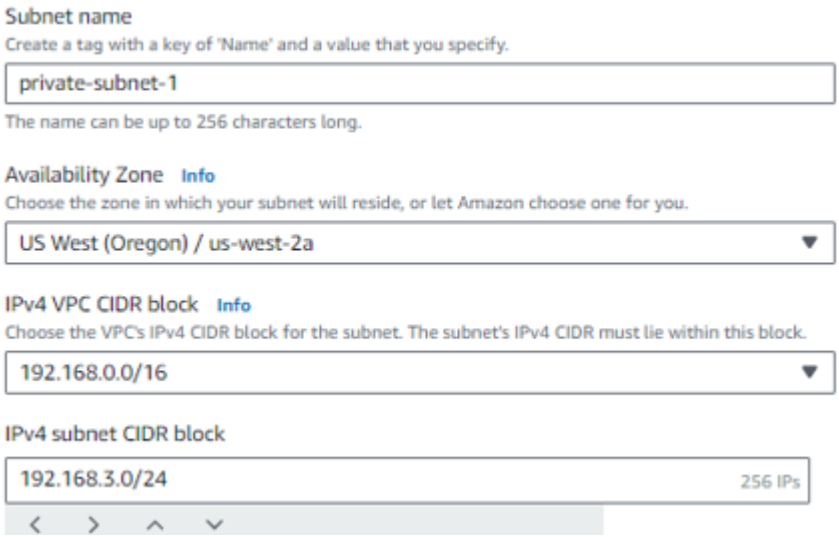
public-subnet-2

CIDR: 192.168.2.0/24 and check the availability zone also



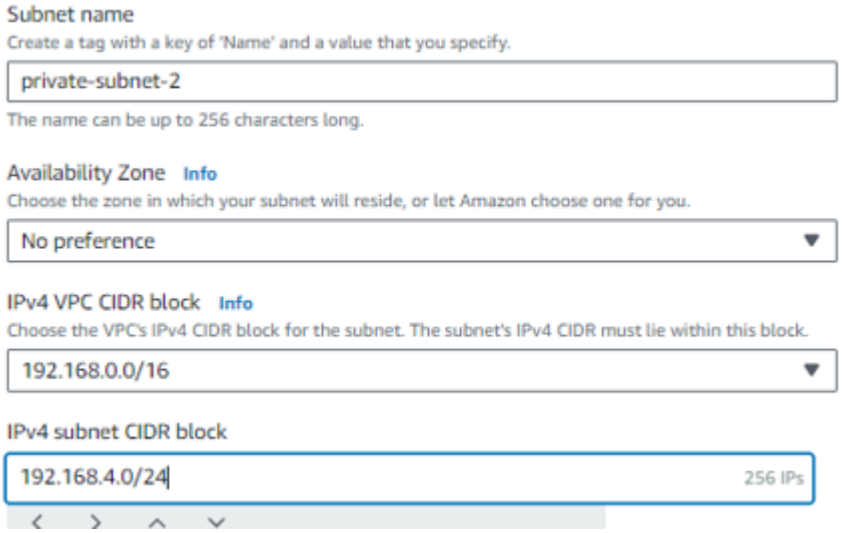
private-subnet-1

CIDR: 192.168.3.0/24 and check the availability zone also



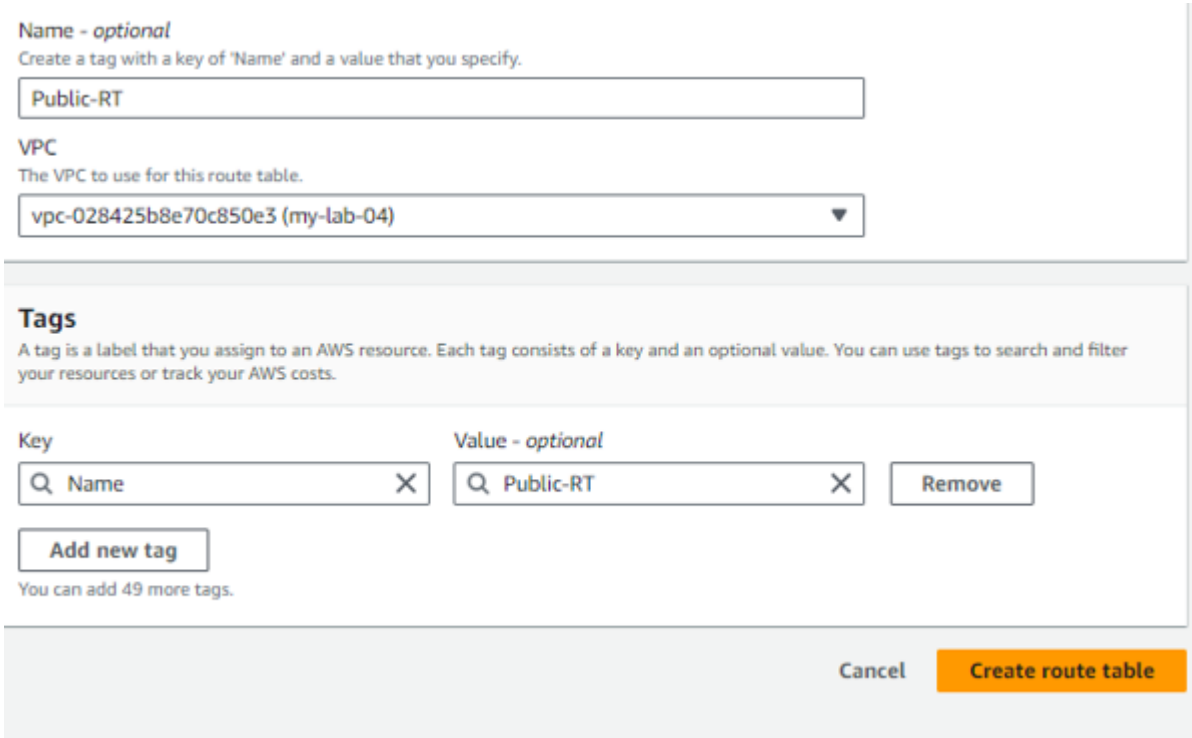
private-subnet-2

CIDR: 192.168.4.0/24 and check the availability zone also

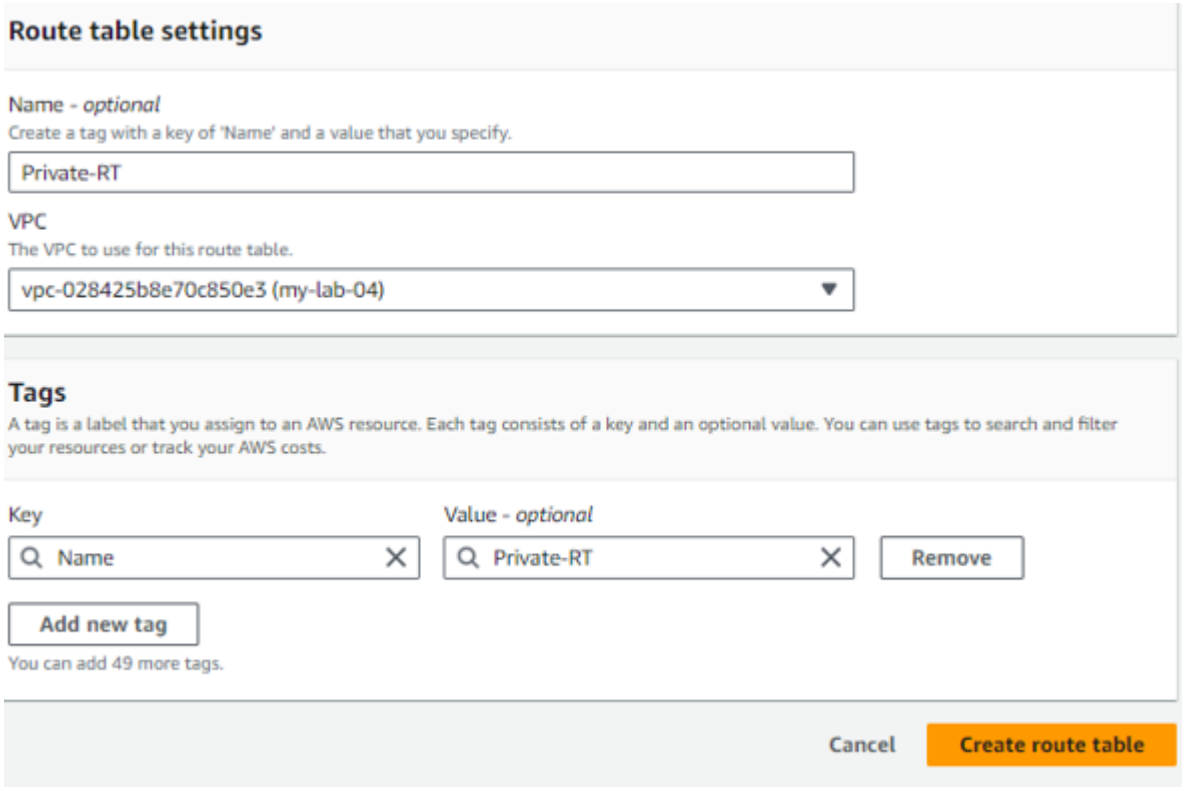


Step 3: Create Route Tables

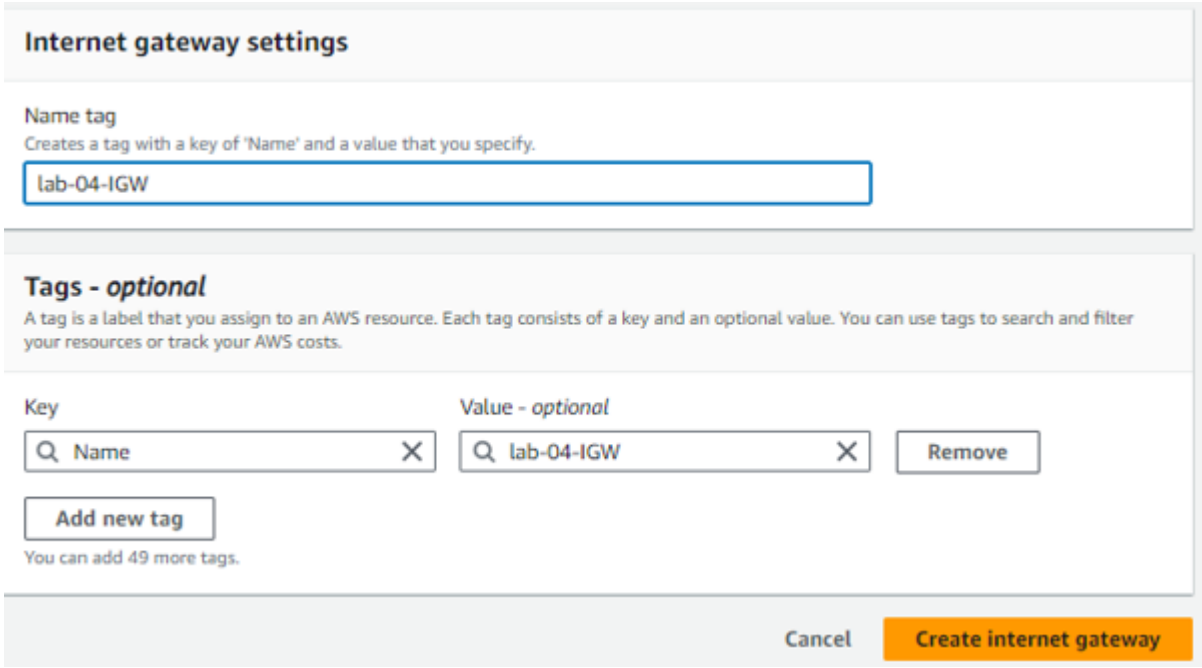
Public-RT -select your VPC



Private-RT -select your VPC



Step 4: Create Internet Gateway



Step 5: Launch an instance – Public Instance in Public Subnet - 01

Launch public EC2 instance:

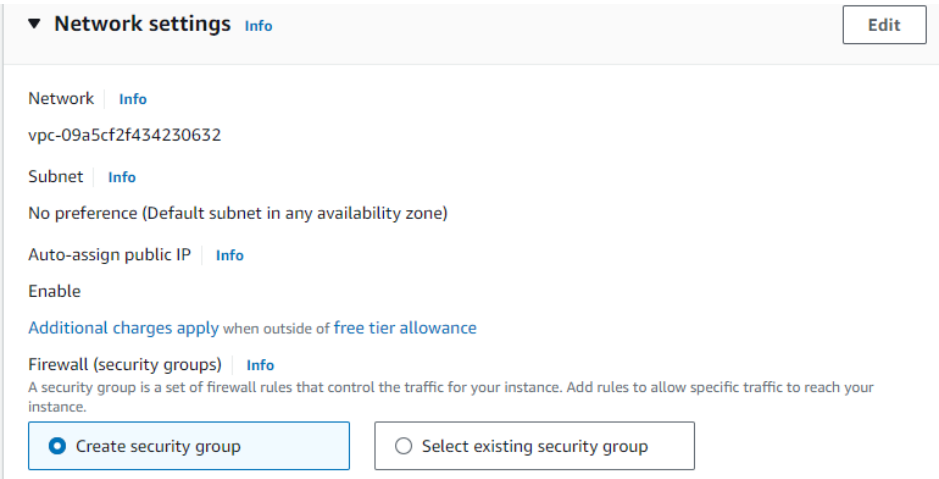
Amazon Machine Image (AMI)

+

Create a new key pair

+

Edit the network setting



By selecting your VPC and Choose public subnet-1

Enable the Auto-assign Public IP

Create security group

Check the inbound rules

Security group name - *required*

launch-wizard-9

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - *required* Info

launch-wizard-9 created 2024-09-04T17:05:32.749Z

Inbound Security Group Rules

Security group rule 1 (All, All, 0.0.0.0/0) Remove

Type Info	Protocol Info	Port range Info
All traffic	All	All

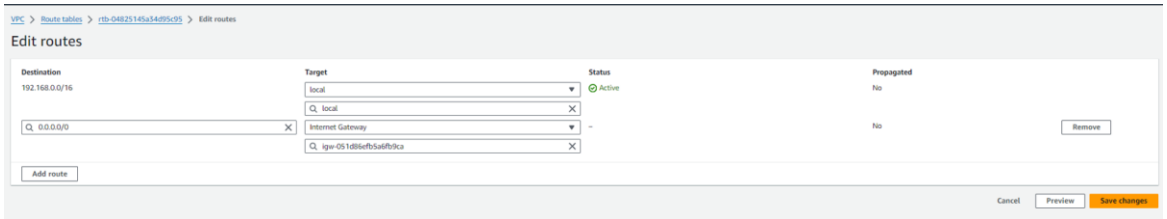
Source type Info	Source Info	Description - *optional* Info
Anywhere	Add CIDR, prefix list or security 0.0.0.0/0	e.g. SSH for admin desktop

And launch the public ec2 instance.

After launching the public EC2 instance -try to connect via EC2 instance connect…It won't work.

Step 6: To edit the routing table.

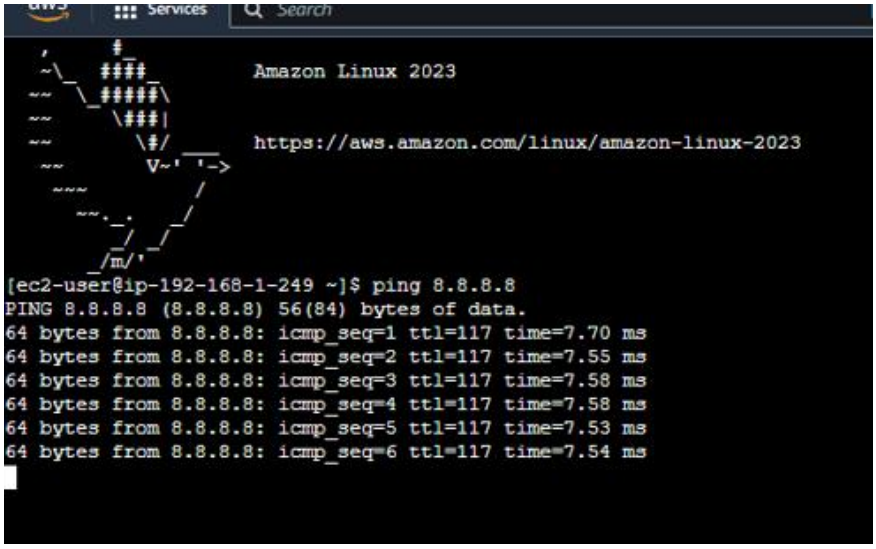
Select the Public-RT table and edit routes like 0.0.0.0/0 and select your Internet Gateway



Select the Subnet association and add both the public subnet and save the same.

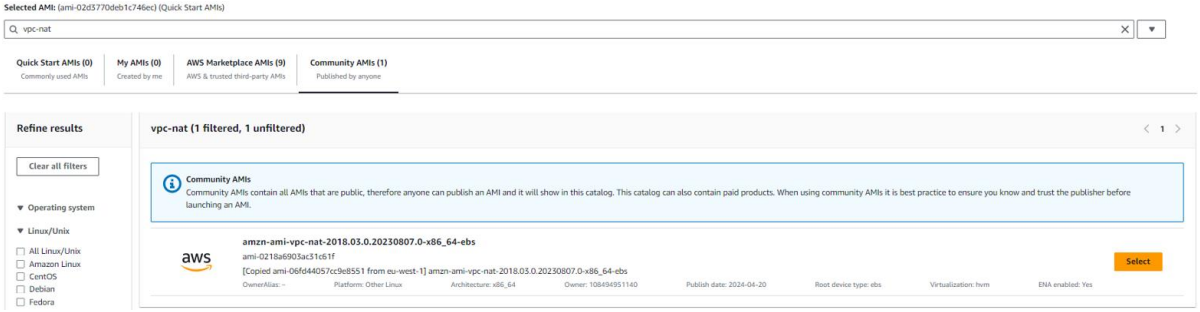
Now try to connect the public EC2 instance -try to connect via EC2 instance connect…It should work.

Use ping 8.8.8.8 to test our public instance connected to the internet via IGW (created by you – user)

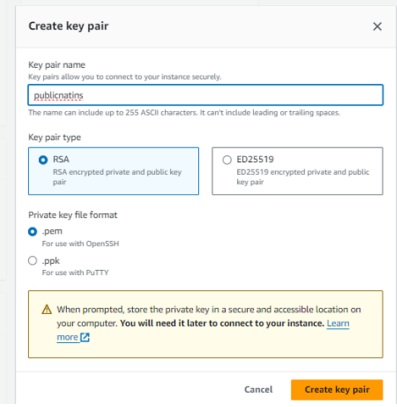


Step 7: Launch an NAT instance – Public NAT Instance in Public Subnet – 02

Select the custom AMIs as mentioned below…..

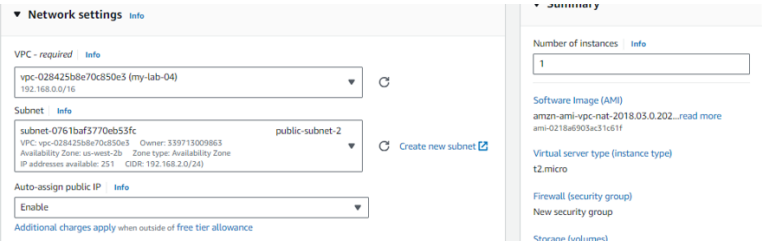


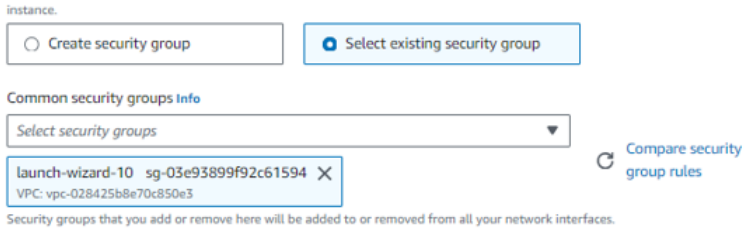
Create key-pair



Choose VPC as well as subnet-2 and enable the Auto-assign public IP

Select the existing security group(You have created while creating FIRST instance) by allowing all…..

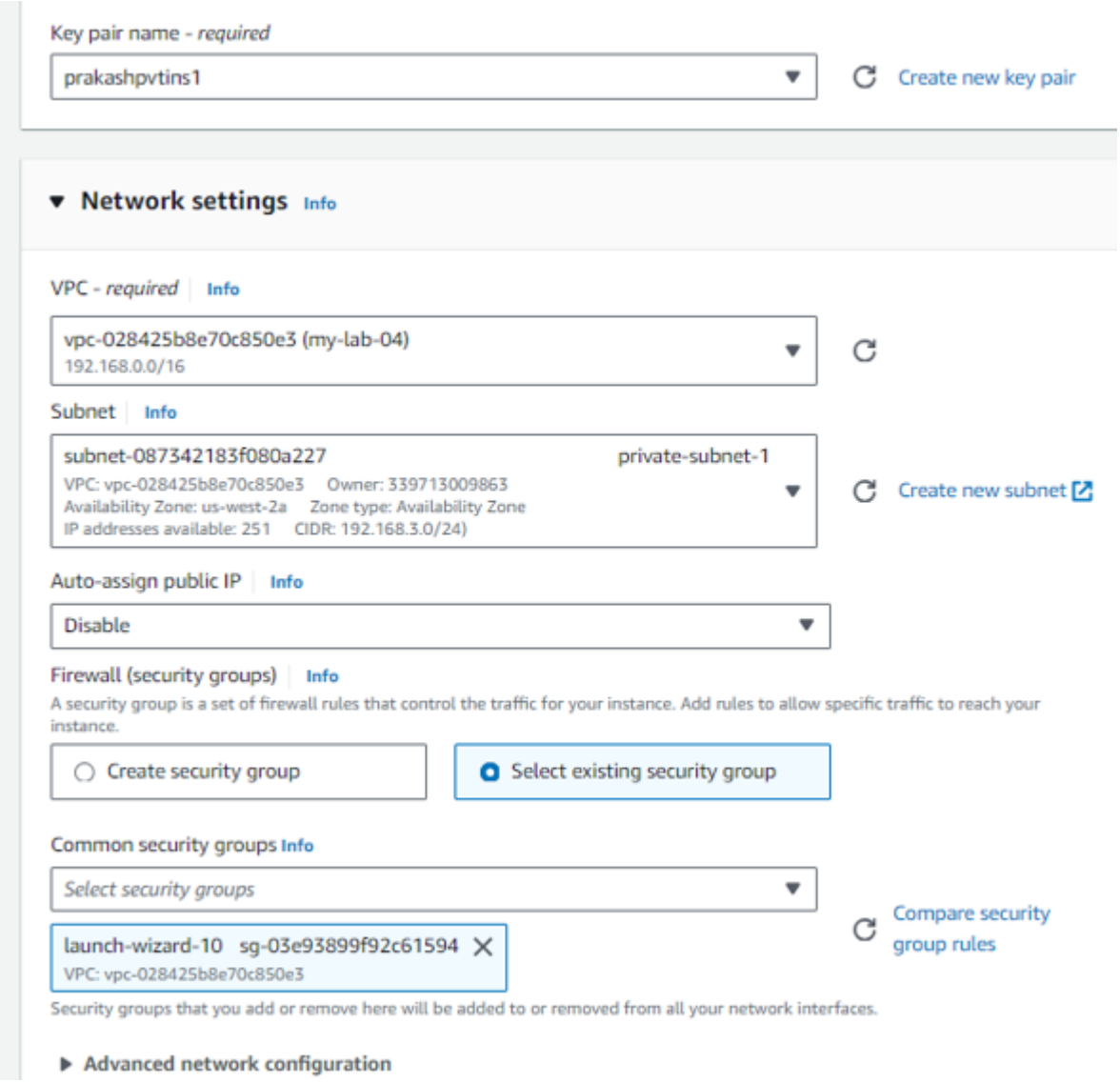




Public NAT Instance is ready ,will try to connect later after creating the private instance .

Step 8: Launch an ec2 instance – private Instance in Private Subnet – 01

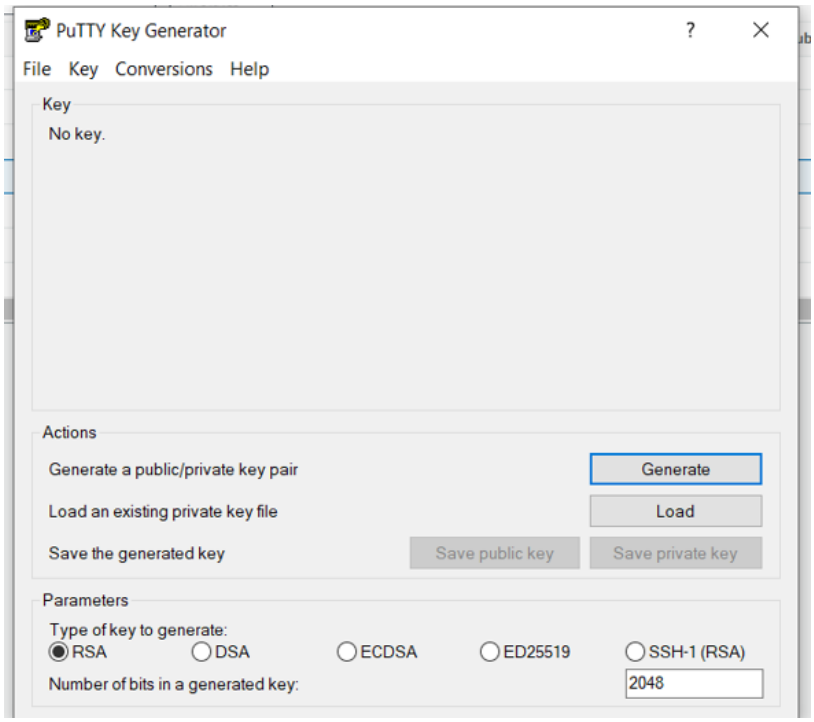
Choose appropriate VPC , Subnet , Disable the Auto assign public IP and selecting the already created security group.

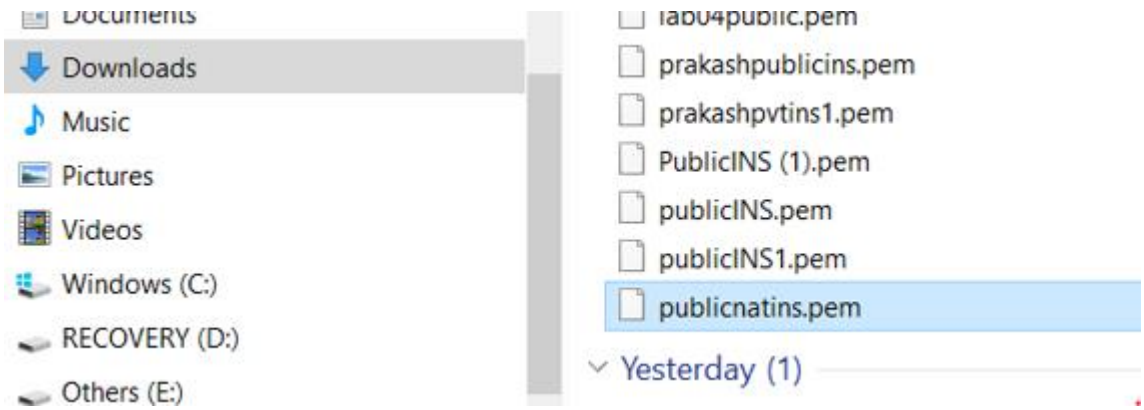


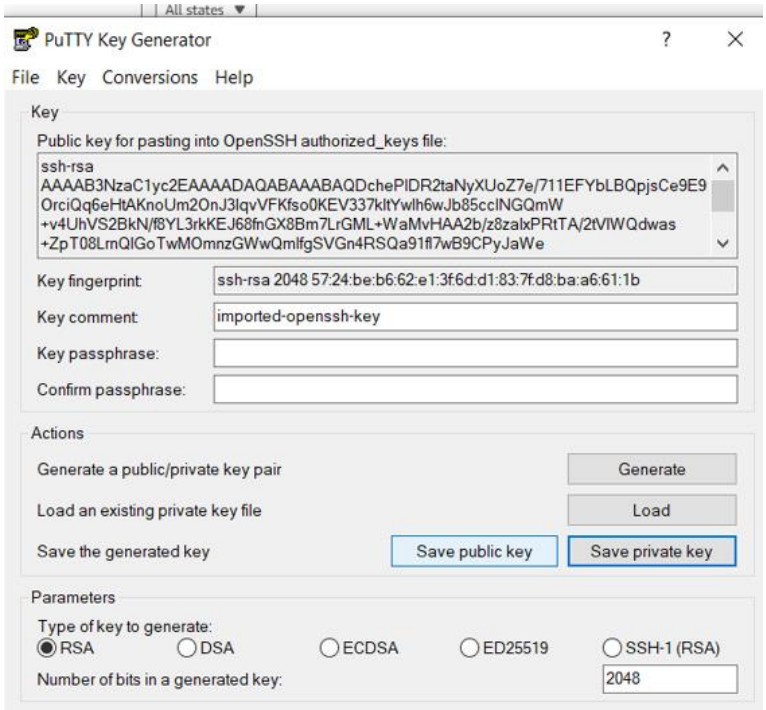
Private instance is ready.

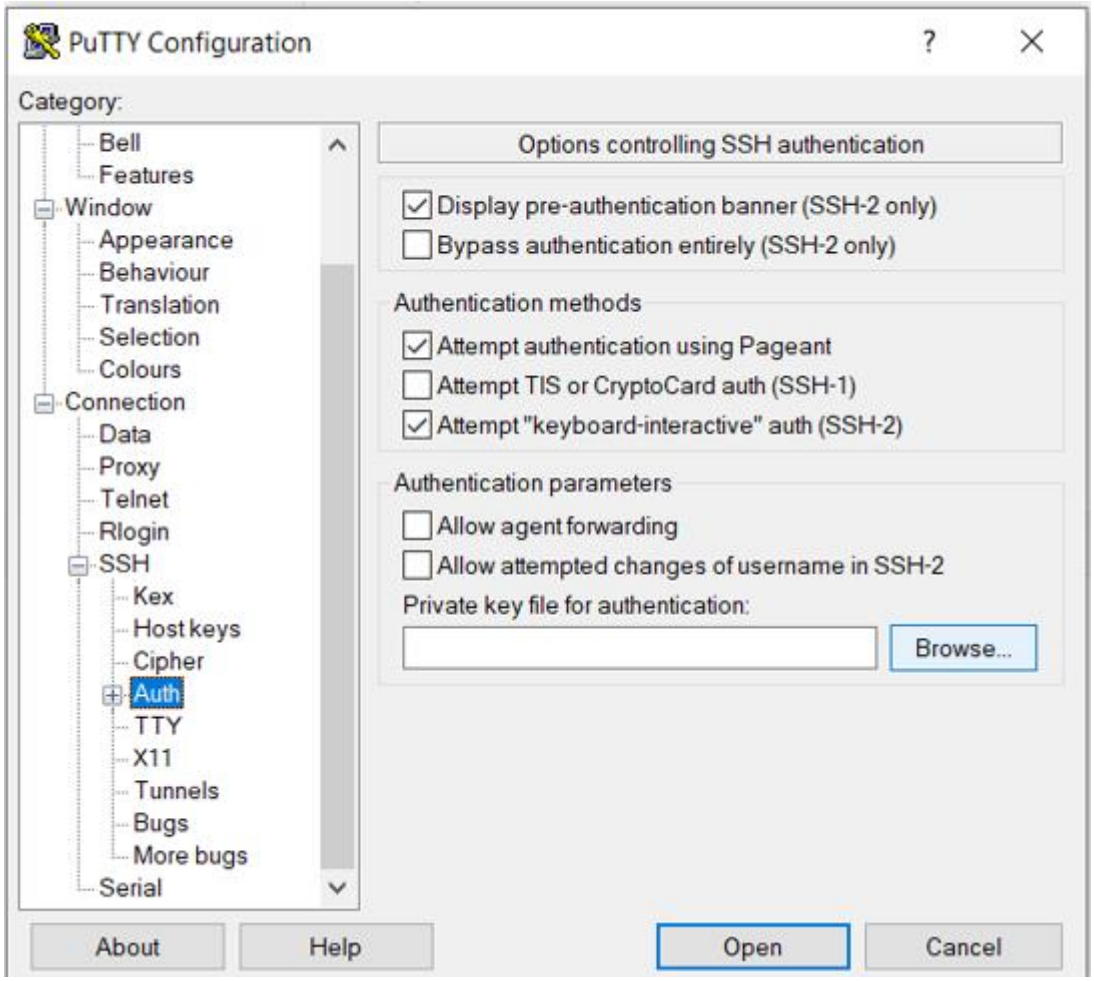
Step 09: Run a NAT instance using PUTTY Connection.

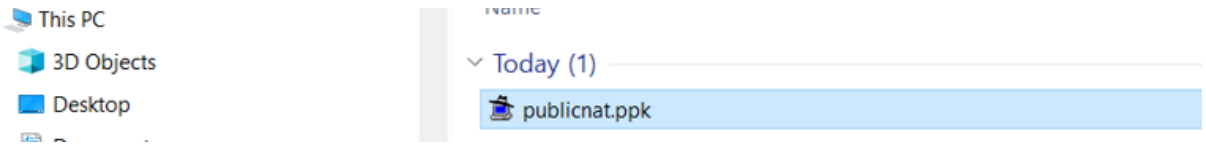
Create a KEY for NAT with the key compatibility

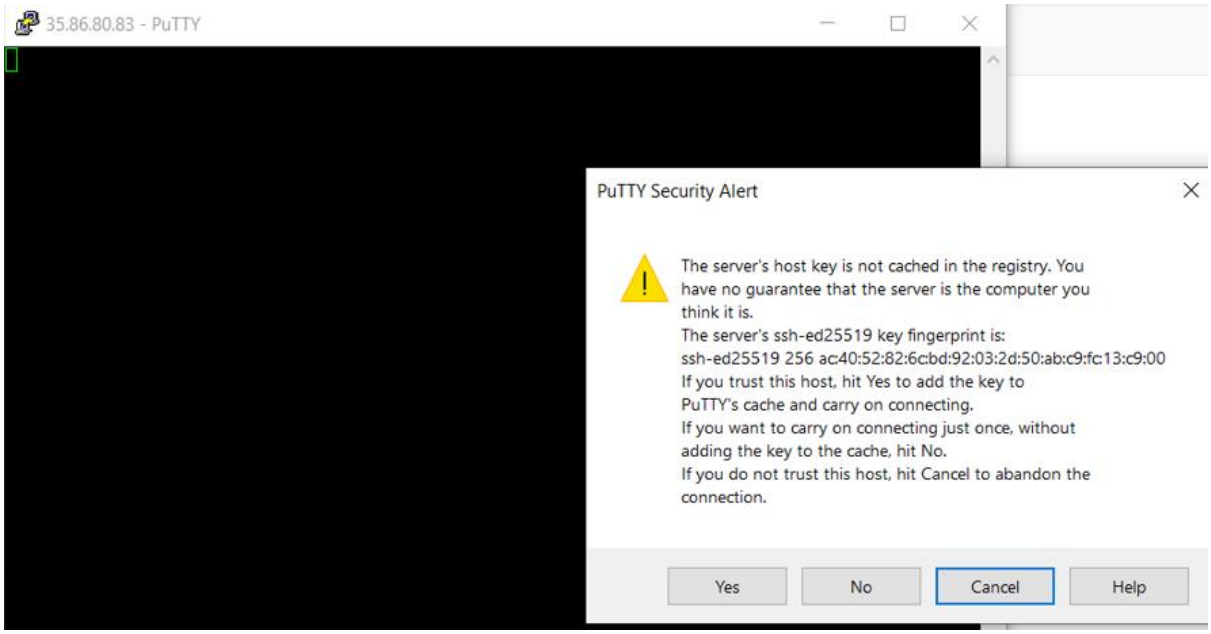




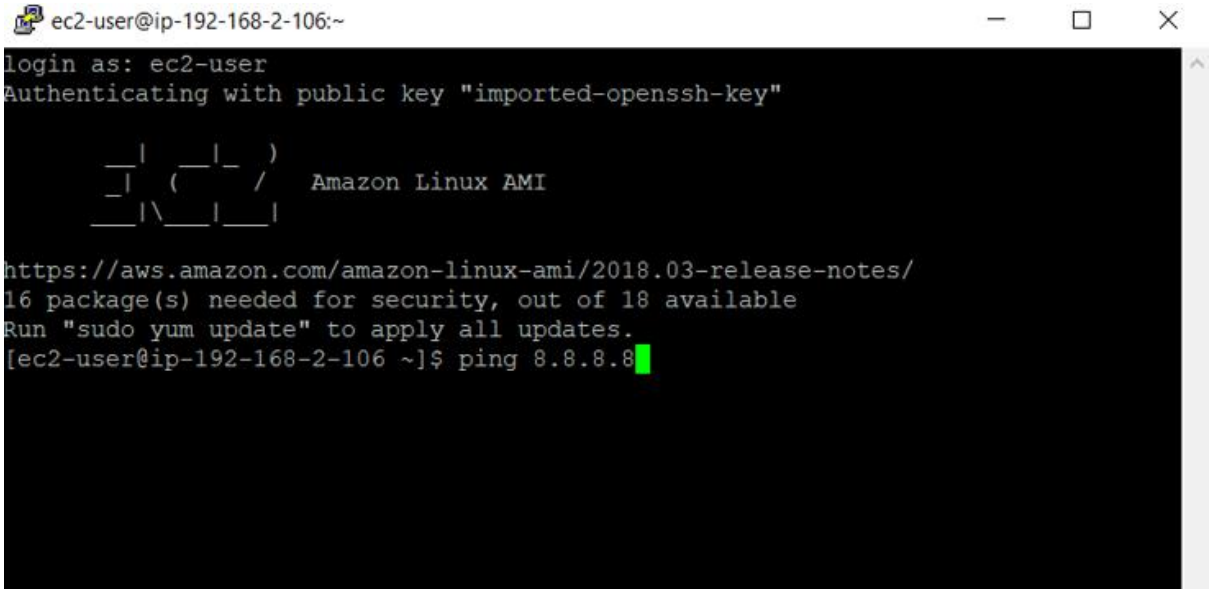

All states
PuTTY Key Generator
File Key Conversions Help
Key
Public key for pasting into OpenSSH authorized_keys file:
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDchePlDR2taNyXUoZ7e/711EFYbLBQpjsCe9E9
OrciQq6eHtAKnoUm2OnJ3lqvVFKfso0KEV337kltYwlh6wJb85ccINGQmW
+v4UhVS2BkN/f8YL3rkKEJ68fnGX8Bm7LrGML+WaMvHAA2b/z8zalxPRtTA/2tVlWQdwas
+ZpT08LrnQlGoTwMOmnzGWwQmlfgSVGn4RSQa91fl7wB9CPyJaWe
Key fingerprint:
ssh-rsa 2048 57:24:be:b6:62:e1:3f:6d:d1:83:7f:d8:ba:a6:61:1b
Key comment:
imported-openssh-key
Key passphrase:
Confirm passphrase:
Actions
Generate a public/private key pair
Generate
Load an existing private key file
Load
Save the generated key
Save public key
Save private key
Parameters
Type of key to generate:
RSA
DSA
ECDSA
ED25519
SSH-1 (RSA)
Number of bits in a generated key:
2048


PuTTY Configuration
Category:
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Host keys
Cipher
Auth
TTY
X11
Tunnels
Bugs
More bugs
Serial
Options controlling SSH authentication
Display pre-authentication banner (SSH-2 only)
Bypass authentication entirely (SSH-2 only)
Authentication methods
Attempt authentication using Pageant
Attempt TIS or CryptoCard auth (SSH-1)
Attempt "keyboard-interactive" auth (SSH-2)
Authentication parameters
Allow agent forwarding
Allow attempted changes of username in SSH-2
Private key file for authentication:
Browse...
About
Help
Open
Cancel





Login as ec2-user



ec2-user@ip-192-168-2-106:~

```
login as: ec2-user
Authenticating with public key "imported-openssh-key"

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

https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
16 package(s) needed for security, out of 18 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-192-168-2-106 ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=58 time=7.32 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=58 time=7.39 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=58 time=7.43 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=58 time=7.44 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=58 time=7.36 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=58 time=7.37 ms
```

NAT instance also connected successfully.

Step 10: Connect IGW via private ec2 instance

Need to place key private pem file into NAT instance, then only NAT will help private instance to connect internet gateway.

```
C:\Users\Prakash P\Downloads>pscp -i publicnat.ppk prakashpvtins1.pem ec2-user@35.86.80.83:/home/ec2-user
```

publicnat.ppk – ppk file for nat instance

*******.pem is key for private instance

ec2-user is a default user

@followed by public IP of NAT Instance

:/home/ec2-user is the destination directory where *******.pem to be kept.

//PSCP (PuTTY Secure Copy Protocol) is a command-line tool for transferring files and folders from a Windows computer to a Linux computer

ec2-user@ip-192-168-2-106:~

```
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Last login: Wed Sep  4 16:08:32 2024 from 183.82.205.138

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

https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
16 package(s) needed for security, out of 18 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-192-168-2-106 ~]$ ls
prakashpvtins1.pem
```

Follow the given steps in

Connect to instance Info

Connect to your instance i-002a1eaa9576a98fc (prakashpvtINS1) using any of these options

EC2 Instance Connect | Session Manager | SSH client | EC2 serial console

Instance ID

i-002a1eaa9576a98fc (prakashpvtINS1)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is prakashpvtins1.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
   chmod 400 "prakashpvtins1.pem"
4. Connect to your instance using its Private IP:
   192.168.3.150

Example:

ssh -i "prakashpvtins1.pem" ec2-user@192.168.3.150

Note: In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

```
https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
16 package(s) needed for security, out of 18 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-192-168-2-106 ~]$ ls
prakashpvtins1.pem
[ec2-user@ip-192-168-2-106 ~]$ chmod 400 "prakashpvtins1.pem"
[ec2-user@ip-192-168-2-106 ~]$ ssh -i "prakashpvtins1.pem" ec2-user@192.168.3.150
The authenticity of host '192.168.3.150 (192.168.3.150)' can't be established.
ECDSA key fingerprint is SHA256:tqAnNgga5PKwFIuGnVd3FW92HLwqB3dJQMvyY7sWu8A.
ECDSA key fingerprint is MD5:c0:a9:fa:ba:44:78:1c:be:53:f6:ae:fb:05:1d:36:36.
Are you sure you want to continue connecting (yes/no)?
```

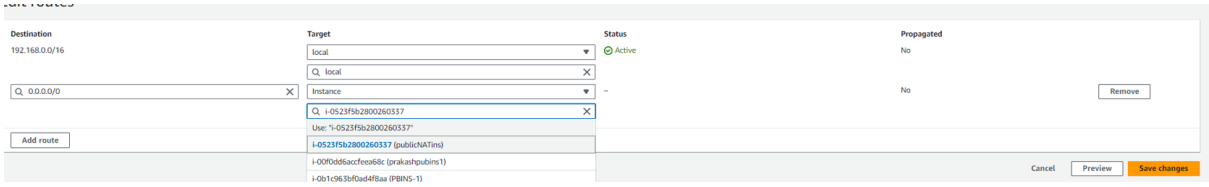
Try to ping suing ping 8.8.8.8

```
https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
16 package(s) needed for security, out of 18 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-192-168-2-106 ~]$ ls
prakashpvtins1.pem
[ec2-user@ip-192-168-2-106 ~]$ chmod 400 "prakashpvtins1.pem"
[ec2-user@ip-192-168-2-106 ~]$ ssh -i "prakashpvtins1.pem" ec2-user@192.1
The authenticity of host '192.168.3.150 (192.168.3.150)' can't be establi
ECDSA key fingerprint is SHA256:tqAnNgga5PKwFIuGnVd3FW92HLwqB3dJQMvyY7sWu
ECDSA key fingerprint is MD5:c0:a9:fa:ba:44:78:1c:be:53:f6:ae:fb:05:1d:36
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.3.150' (ECDSA) to the list of known h
       ,     #_
       ~\_  ####_        Amazon Linux 2023
      ~~  \_#####\
      ~~     \###|
      ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
       ~~       V~' '->
        ~~~         /
          ~~._.   _/
             _/ _/
           _/m/'
[ec2-user@ip-192-168-3-150 ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
```

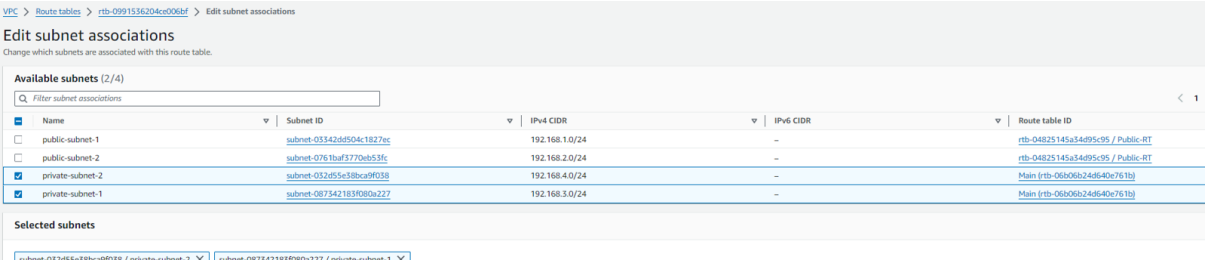
It may/may not work.

Go to Private RT table and do the route changes.

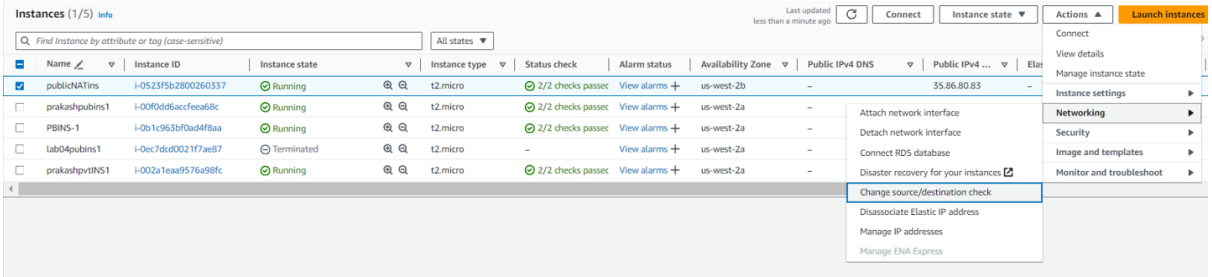
Choose 0.0.0.0/0 and select an instance as public Nat Instance and save the changes.

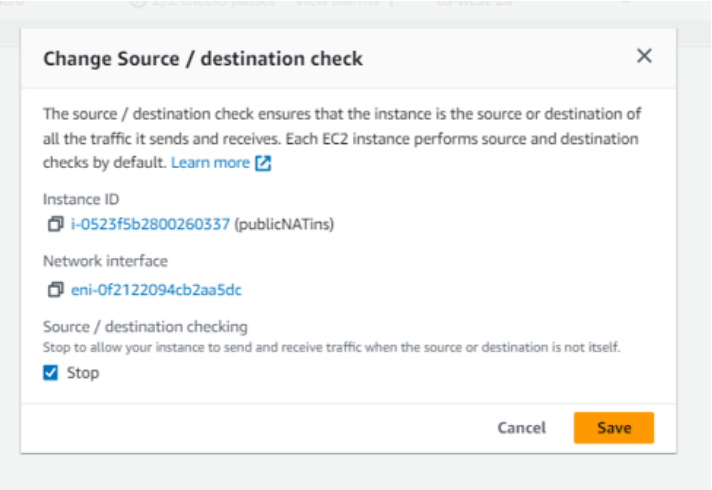


Edit the subnet associations -by adding private subnet



Go to NAT instance change the source and destination check by enabling the STOP.





Try to ping

```
ec2-user@ip-192-168-3-150:~
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Last login: Wed Sep  4 16:14:55 2024 from 183.82.205.138

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

https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
16 package(s) needed for security, out of 18 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-192-168-2-106 ~]$ ls
prakashpvtins1.pem
[ec2-user@ip-192-168-2-106 ~]$ chmod 400 "prakashpvtins1.pem"
[ec2-user@ip-192-168-2-106 ~]$ ssh -i "prakashpvtins1.pem" ec2-user@192.1
0
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Wed Sep  4 16:16:18 2024 from 192.168.2.106
[ec2-user@ip-192-168-3-150 ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=89 ttl=57 time=10.1 ms
64 bytes from 8.8.8.8: icmp_seq=90 ttl=57 time=8.20 ms
64 bytes from 8.8.8.8: icmp_seq=91 ttl=57 time=8.16 ms
64 bytes from 8.8.8.8: icmp_seq=92 ttl=57 time=8.20 ms
64 bytes from 8.8.8.8: icmp_seq=93 ttl=57 time=8.17 ms
64 bytes from 8.8.8.8: icmp_seq=94 ttl=57 time=8.21 ms
64 bytes from 8.8.8.8: icmp_seq=95 ttl=57 time=8.20 ms
64 bytes from 8.8.8.8: icmp_seq=96 ttl=57 time=8.30 ms
64 bytes from 8.8.8.8: icmp_seq=97 ttl=57 time=8.15 ms
64 bytes from 8.8.8.8: icmp_seq=98 ttl=57 time=8.23 ms
64 bytes from 8.8.8.8: icmp_seq=99 ttl=57 time=8.22 ms
64 bytes from 8.8.8.8: icmp_seq=100 ttl=57 time=8.13 ms
```

From private instance the internet is accessed with the help of – NAT gate way

Still error, there may be issue in security group…