AWS VPC (Virtual Private Cloud)

It is related to Network and Security part

VPC provides isolated network for resources in AWS cloud

Is AWS a public or private cloud -> it is a public (anyone can access the AWS website, create acount, use resources)

Can anyone login and work with resources in AWS? Yes, then it is a public cloud

In that case, protecting my resources is very crucial. If I login into my account, can I access other accounts’ resources, answer is no

With my login, I shouldn’t access your resources and vice-versa. that’s called as isolated resources

With the help of VPC, we can protect our resources in AWS cloud

VPC provides flexible and secured network to maintain and manage our resources in AWS cloud

Can everyone access every resource available in your home? The answer is No. Mostly outsiders can access only up to front door

VPC is like our home, before creating the resources, first part is to create a VPC

Even though, we haven’t created our own VPC, still while creating other resources, we used the default VPC being created. Maximum we can create 65000 IPs, that many IPs we can allow within one VPC. Maximum approx 65000 IPs will be there in one VPC

VPC (approx 65000 IPs)

Subnet 1

Subnet 2  
(private)

Subnet 3 (public)

Internetworking Gateway

We can have any number of Subnets inside VPCs, we have something called as Public Subnet and Private Subnet

VPC terminology:

1. VPC
2. Subnet (Private or Public)
3. CIDR Block (IP ranges) -> VPC sizing
4. Route tables
5. Internet gateway
6. NAT gateway
7. VPC peering
8. Security groups --> at Resource level --> Rules (both Inbound [who can access] and Outbound [what we can access]) to allow who can access
9. NACL --> Subnet level --> but at Subnet level, we can have rules for allowing also and denying also

What’s one Subnet? Like a small network within VPC. We can allocate like 256 IPs in the subnet.

In Subnet SN2, we can allocate 124 IPs

Private Subnet is for the internal communication

Public subnet can be accessed through internetworking. Internetworking means outsiders can also access. Say if I attached an Internetworking Gateway (INW) to a public subnet, anyone can access. Any of the Subnet, if I attach Internet Gateway (INW), it becomes Public otherwise it is Private

Public subnet --> Internet Gateway, Private subnet --> NAT Gateway

IPs

There are several types of IPs (Internet Protocol) address used in a computer network. All devices like mobile phones, laptops, desktops etc all have IPs. If devices have to get connected over internet, IP address is a must

IPv4: 32 bits --> 4 sets of numbers

IPv4 ---> 32 bits numeric addresses written in four sets of numbers separated by periods: 192.168.1.1

It is most widely used IP version and supports approximately 4.3 billion unique addresses

IPv6: 128 bits, IPv6 is trying to solve the problem of IP shortage, which might occur in the future due to IPv4 --> 8 sets of four hexadecimal digits will be there

IPv6 uses hexadecimal notation with colons eg: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Supports 340 undecillion unique addresses

Public IP

Private IP

Static IP address

Dynamic IP

VPC Sizing: process of allocating IPs to VPC subnets. In general, allocating IPs is called as VPC sizing, within VPC how many IPs are required and within each subnet how many IPs are required. When we create a new VPC, that time we decide how many IPs we want --> Decision of allocating IPs to VPCs is only called as VPC sizing

IP Ranges we will be doing with CIDR --> Class less Inter domain Range

VPCs are regional-specific

Can VPCs interact? Yes that’s called as VPC peering

Any device, if it has to access resources of internet, is IP compusory? Yes

On a regular basis, number of new devices are rapidly increasing and are using internet, and any device if it has to use internet, then IP is mandatory and a must and there might be possibility of running out of IPs, which has to be unique. To overcome this issue, IPv6 was introduced

When we connect Internet Gateway to a Private Subnet, it becomes Public Subnet. Also Route Table (RT) will be there between INW and Public SN1 to make it public. Rules of routing, with the help of route tables, INW, outsiders can access resources within one Subnet

VPC sizing: Sizing will be calculated in 2 power or power of 2

**IPv4**

10.0.0.1/16 ==> means 2 power (32-16) ==> 2 power 16. 32 is the maximum . Maximum one VPC can have is 65,536

10.0.0.1/32 ==> 2 power (32-32) ==> 2 power 0 = 1 IPs address, not recommended to create VPC or Subnet with just one IP address

Therefore, AWS supports from 28

10.0.0.1/28 ==> 2 power (32-28) ==> 2 power 4 = 16. this is the minimum number of IPs AWS supports. AWS supports from 28 and less

AWS supports minimum 16 to maximum 65,536 IPs

Similarly, AWS does not support ==> 10.0.0.1/15 less than 16

Subnet ranges can be given from /16 to /28

Recommended to use /24

10.0.0.1/24 ==> 2 power (32-24) = 2 power 8 = 256 IPs that’s generally we use. In real-life scenario also 256 IP is more than enough for Subnets

VPC allows us to create and manage our own networks or isolated networks within AWS cloud

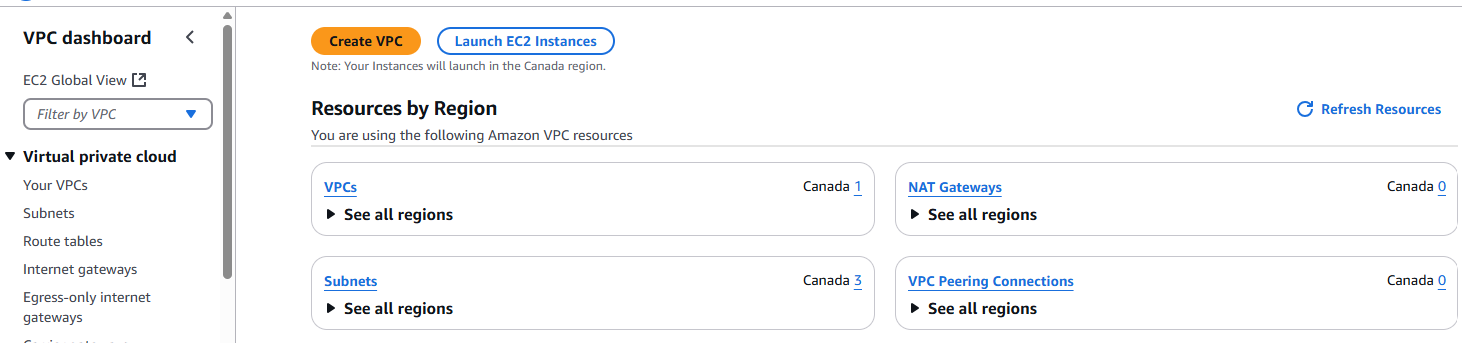
In VPC, users can define their own IP address range, subnets, route table and network gateways

It provides control over network configuration such as setting up access-control policies, firewall rules (security group rules) and network traffic routing

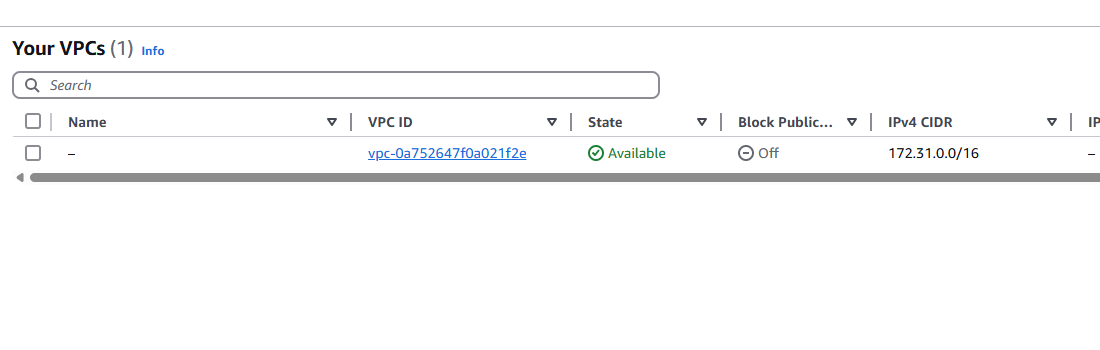
MobaXterm is an outsider, not part of AWS, if you are able to connect with MobaXTerm it is a public subnet, otherwise private subnet

Practical task:

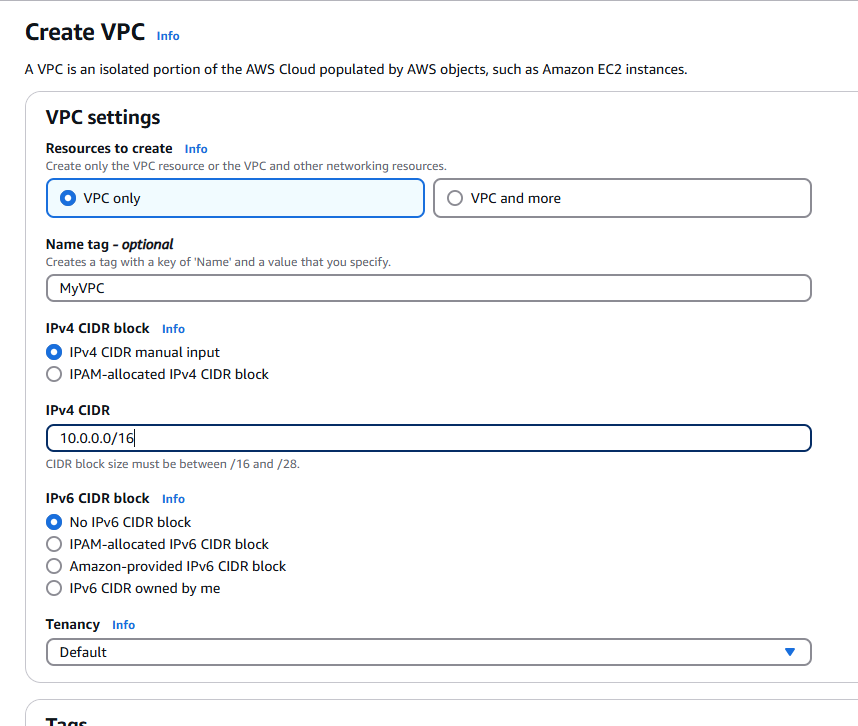
1. Create VPC
   1. CIDR block: 10.0.0.0/16
   2. Select No IPv6 CIDR block
   3. Rest select default options
   4. Click create VPC
   5. Note: One Route table will be created for VPC by default if necessary re-name
2. Create two subnets ->
   1. Create subnet-1
      1. Name: subnet-public
      2. CIDR block: 10.0.0.0/24 (it will take 256 IPs)
   2. Create subnet-2
      1. Name: subnet-private
      2. CIDR block: 10.0.1.0/24 (I will slightly change IP to avoid collision)
   3. Route tables: The moment we create VPC default route table will be created go to route table section and rename it to private
   4. Create a NEW Route table and name it to Public
   5. After Route tables are created, Edit and attach Subnet association
   6. Public RT attach to Public subnet
   7. Private RT Attach to Private subnet
   8. Create new Internet Gateway
   9. Click on Public-RT --> routes --> Add route ---> Internet Gateway and select the IGW we had created earlier and select 0.0.0.0/0 in the other input field
3. Create 2 EC2s
   1. One EC2 in public subnet and another in private subnet
   2. Tested by connect to EC2 of public subnet, it worked and we were NOT able to connect to Private EC2 / private subnet because no Internet Gateway was attached



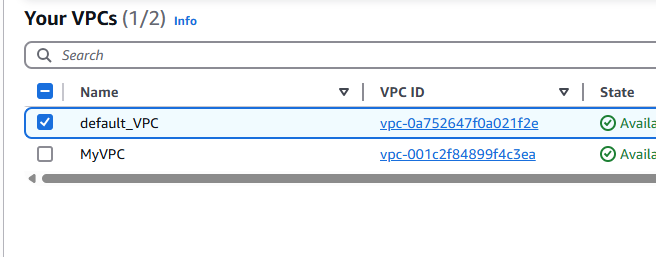
One default VPC is already there



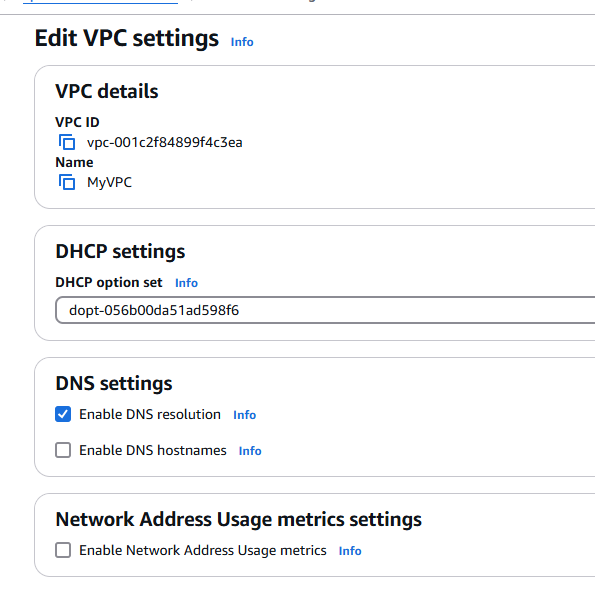
Use the following settings: create VPC



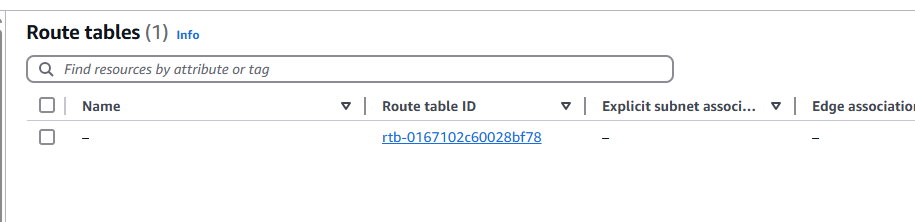
10.0.0.0/16 means almost 65000 IPs are allowed in this VPC



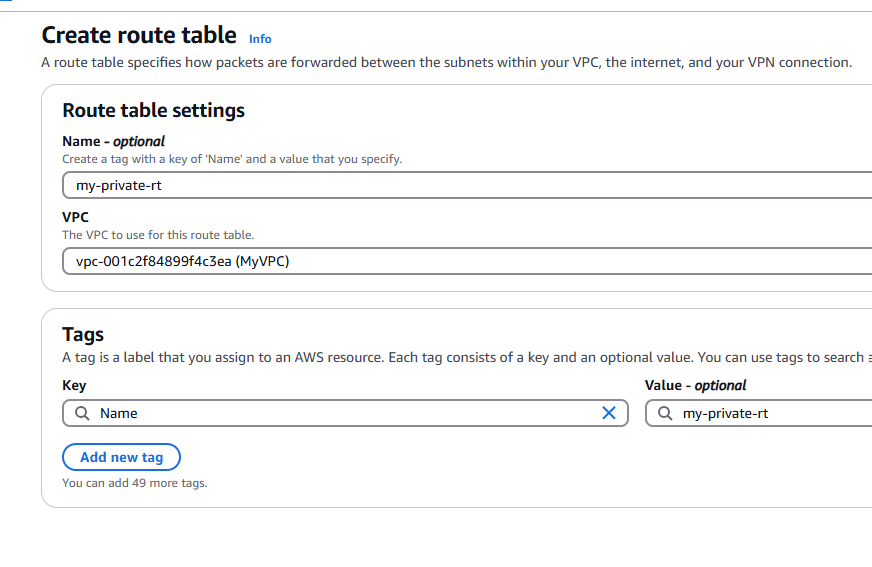
Edit VPC settings



Click Route tables

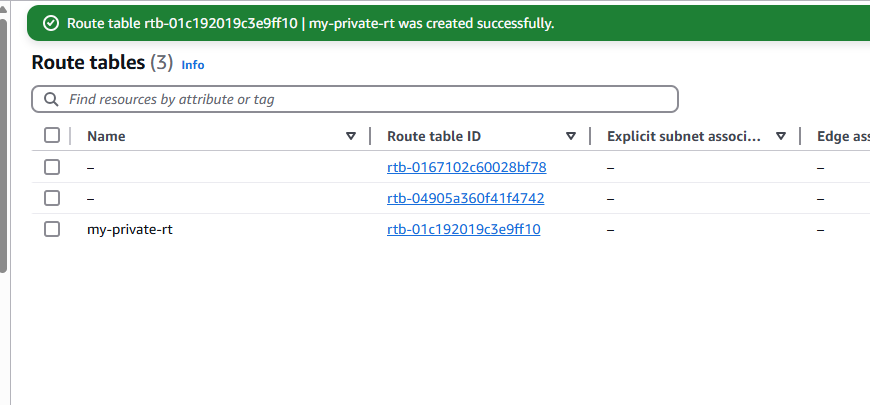


Create Route table



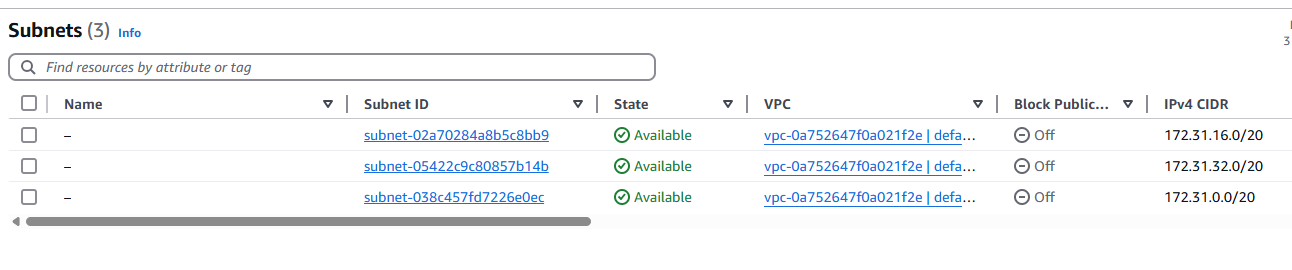
Click route table

Note: One Route table is created along with VPC by default

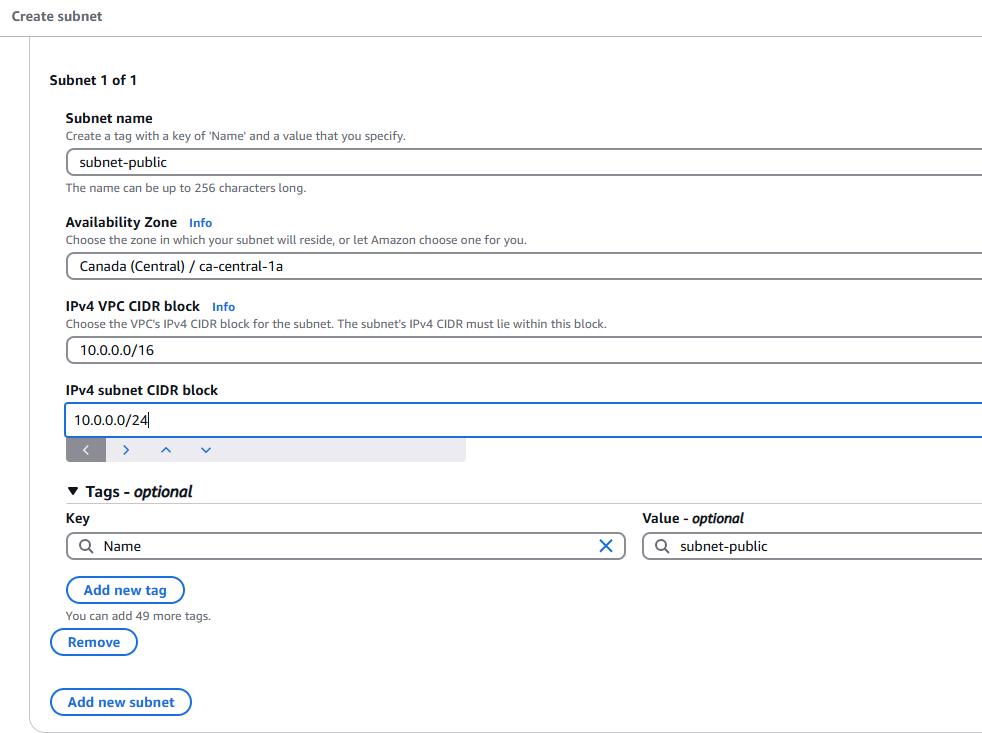


Go to Subnets

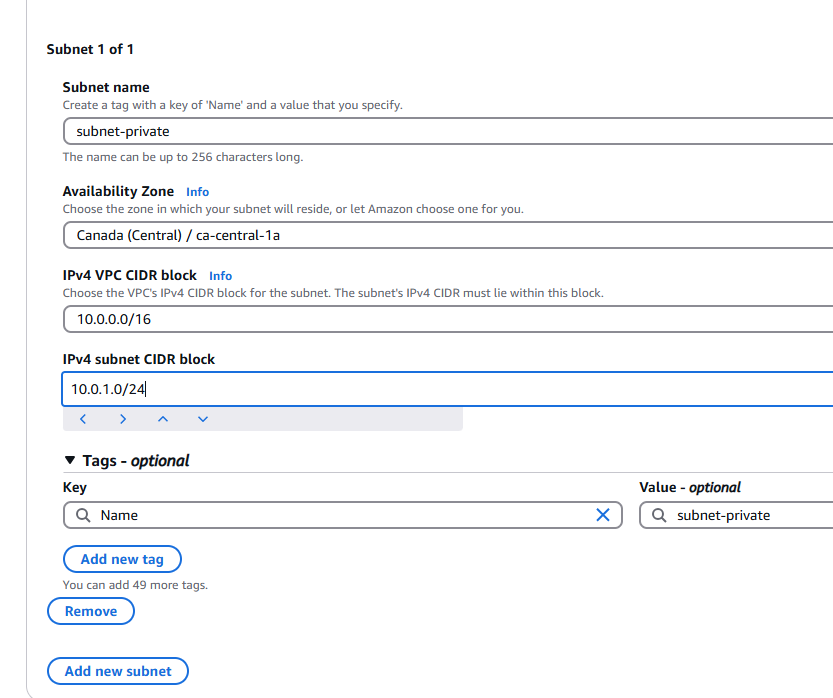
Default subnets are there

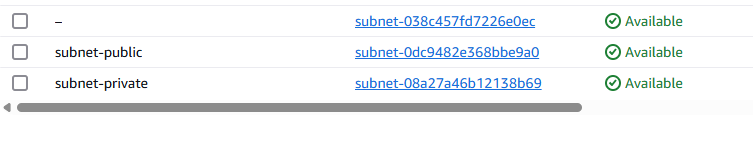


Create a new Subnet

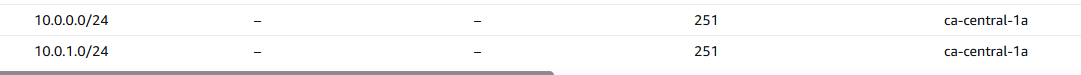


10.0.0.0/24 ---> IPv4 subnet CIDR block

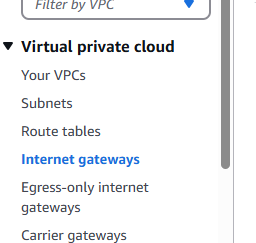




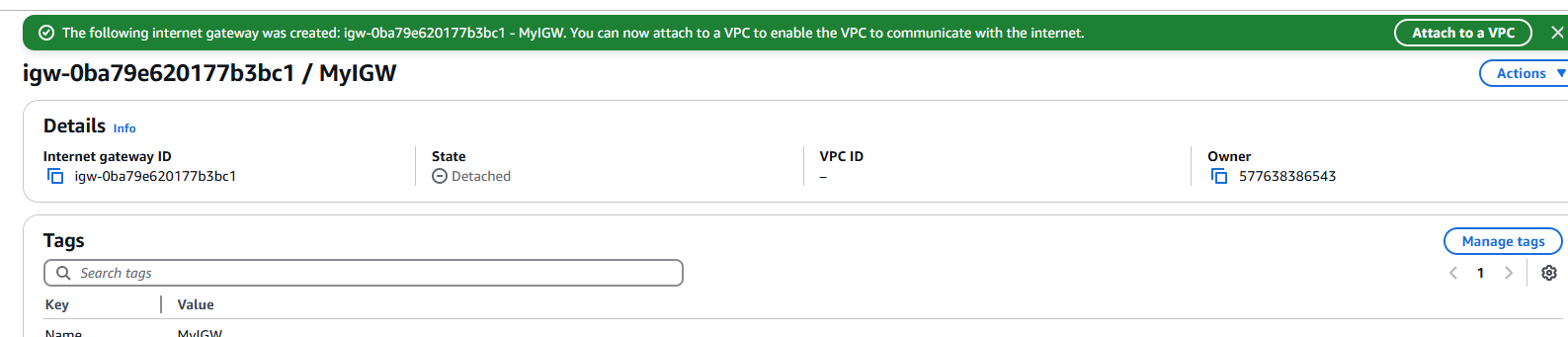
If you attach Internet gateway, it is public, if you don’t attach then it is private

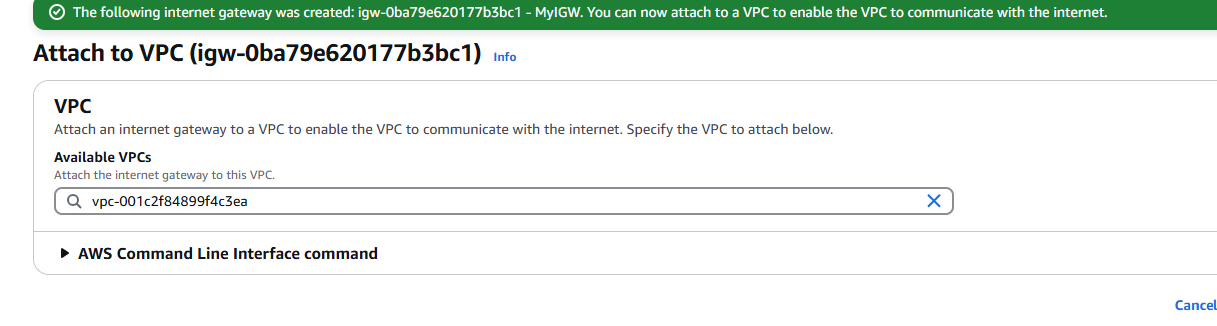
We have 251 IP addresses in our subnets: 

Go to Internet Gateways



Create Internet Gateway then Attach to VPC

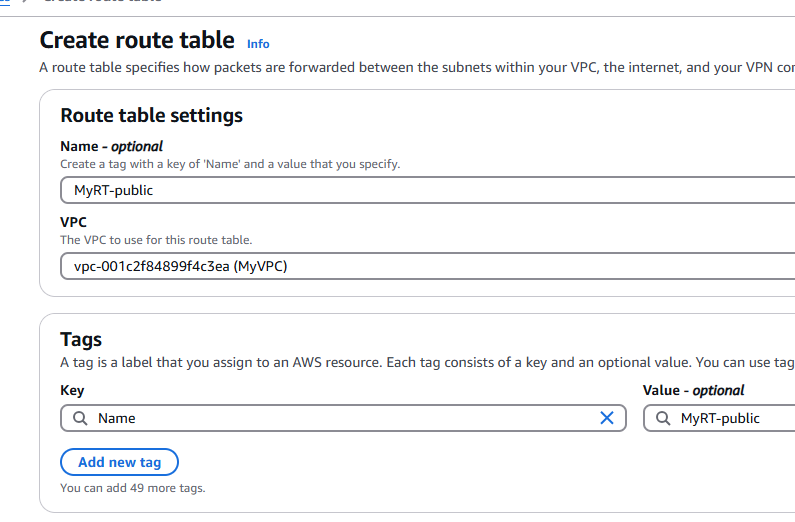


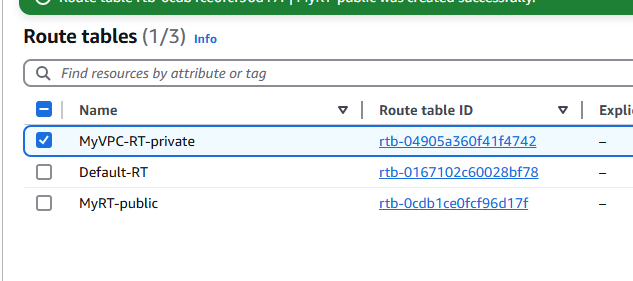


Select MyVPC

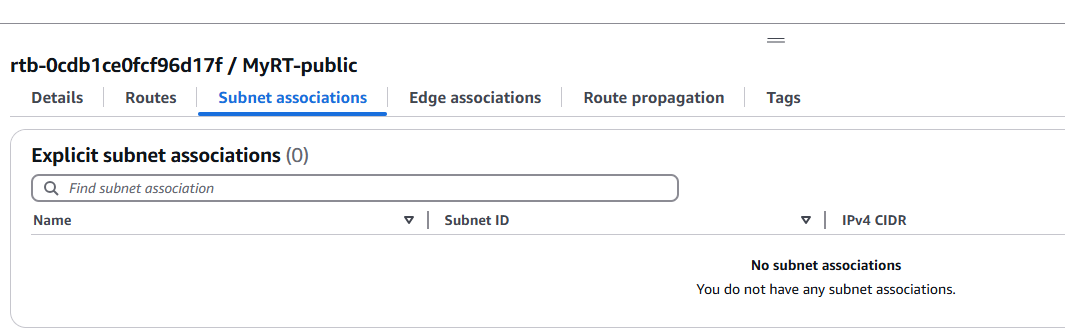
Click Attach internet gateway

Create a public route table

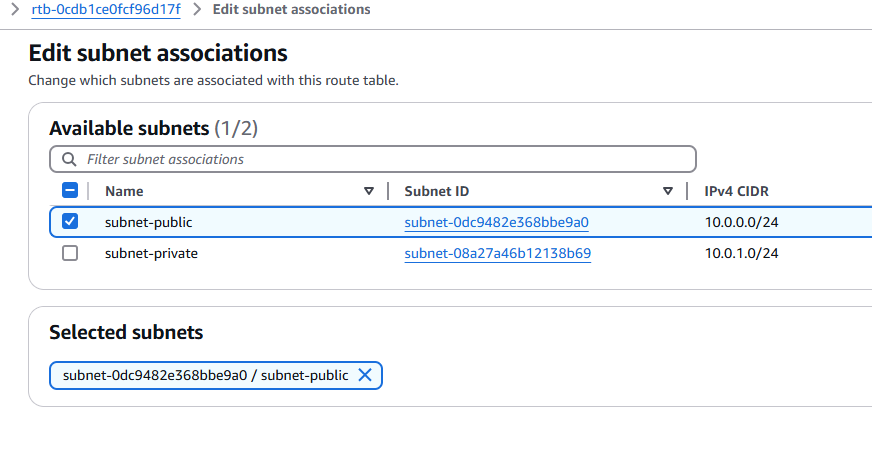




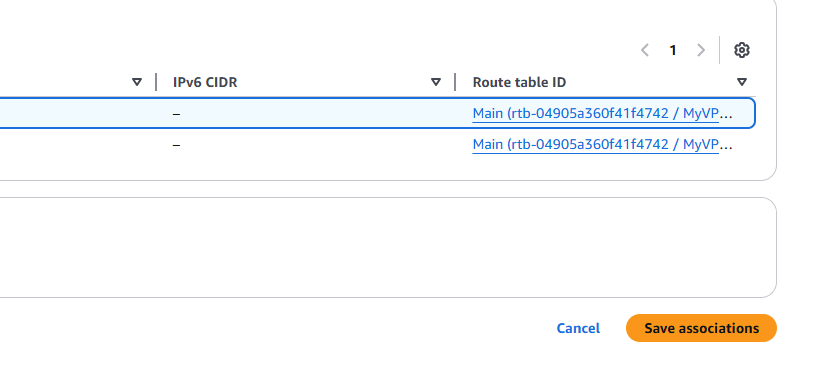
No subnet associations for Route table public



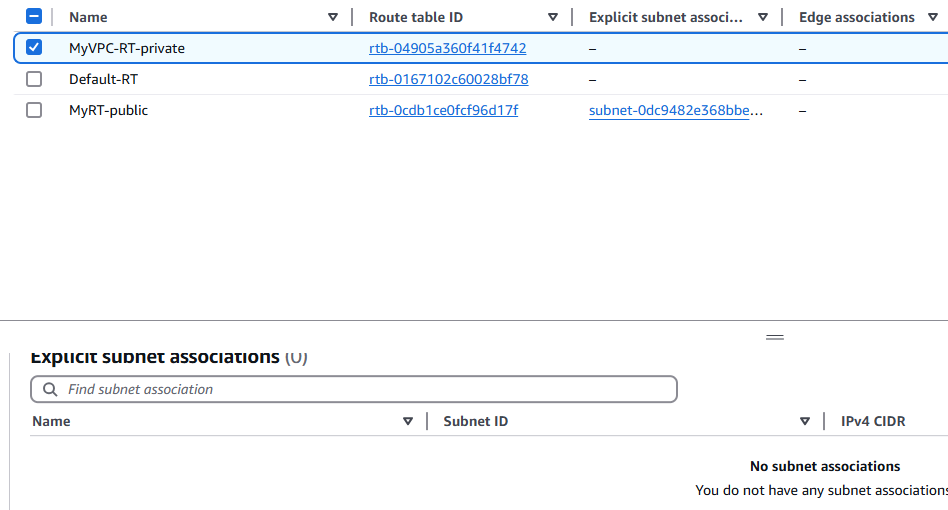
Click Public subnet for public VPC

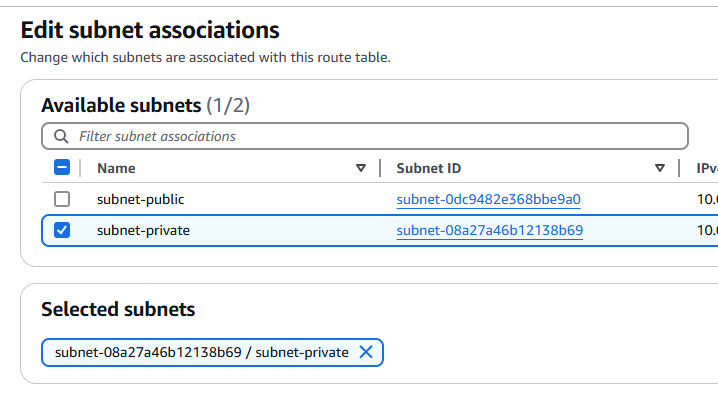


Click Save associations

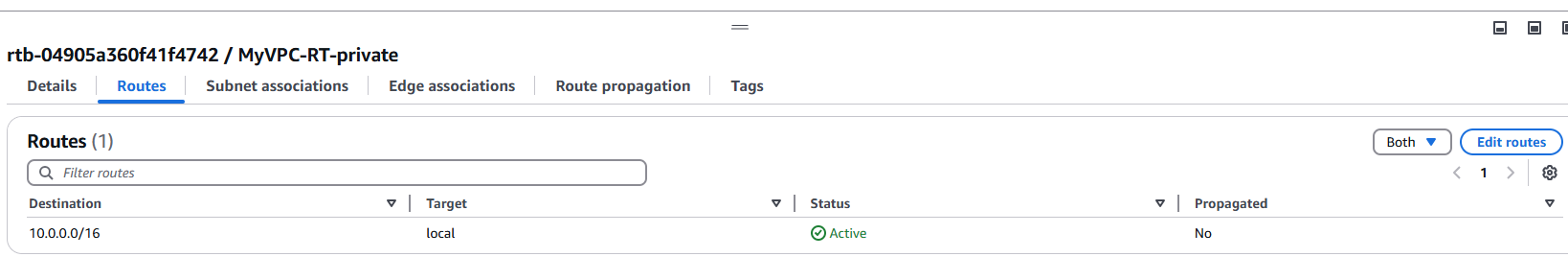


Same thing click on Private subnet --> no associations at the moment

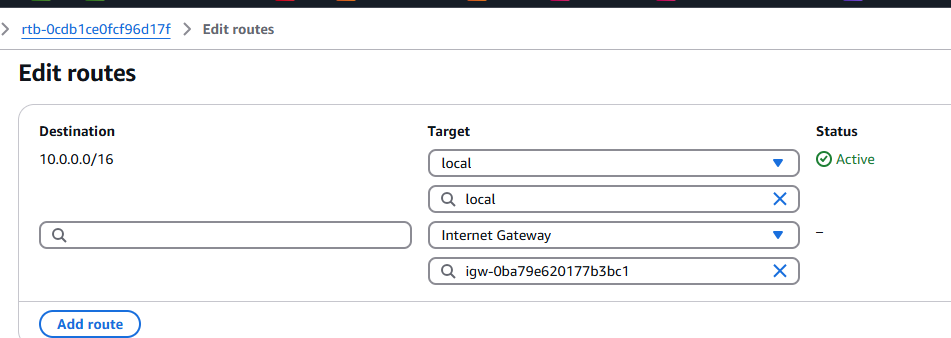


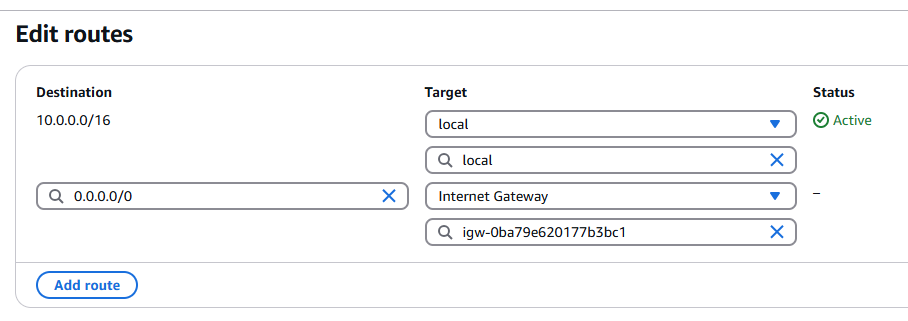


Click on edit routes --> it is done only for the PUBLIC subnet



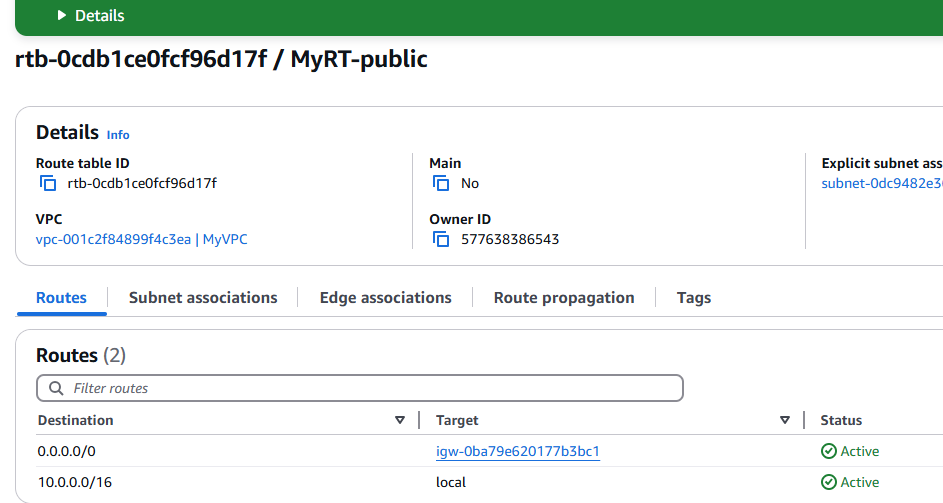
Add route ---> select Internet Gateway





Click Save changes

Internet Gateway associated only with the Public route table



VPC (approx 65000 IPs)

Subnet 1

Subnet 2  
(private) EC2

Subnet 3 (public) EC2

Internetworking Gateway

RouteTable

Private IP

Note:

We have created a Public subnet, then Route tables --> then we have attached Internet gateway to RT

Route tables: The moment we create VPC default route table will be created go to route table section and rename it to private

Then Create a NEW Route table and name it to Public

After Route tables are created, Edit and attach Subnet association

Public RT attach to Public subnet

Private RT Attach to Private subnet

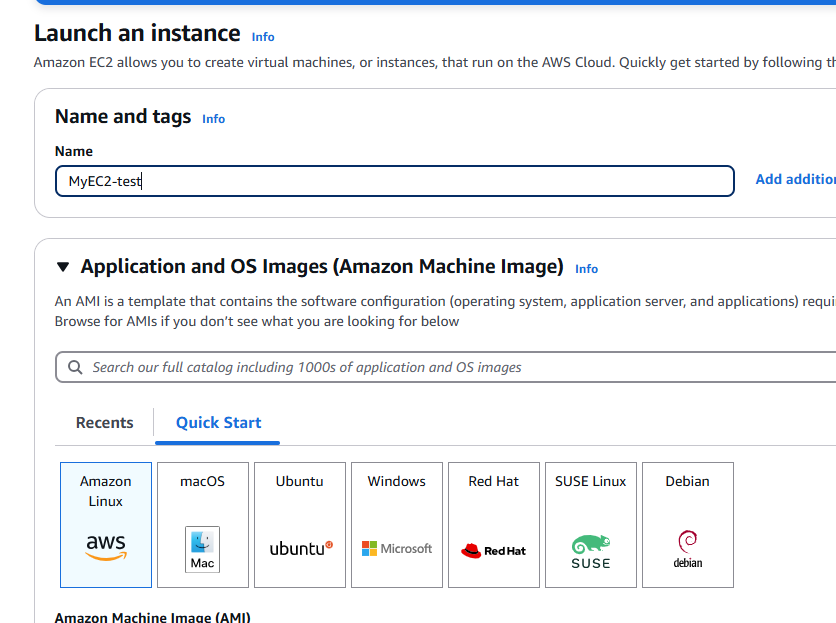
Create new Internet Gateway

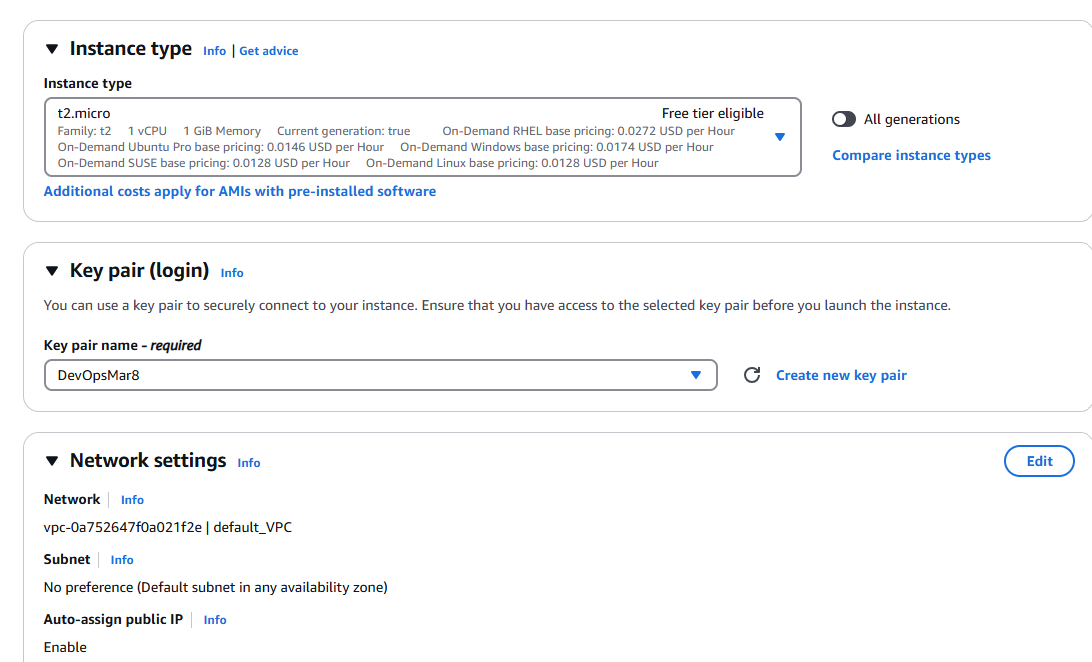
Click on Public-RT --> routes --> Add route ---> Internet Gateway and select the IGW we had created earlier

Summary

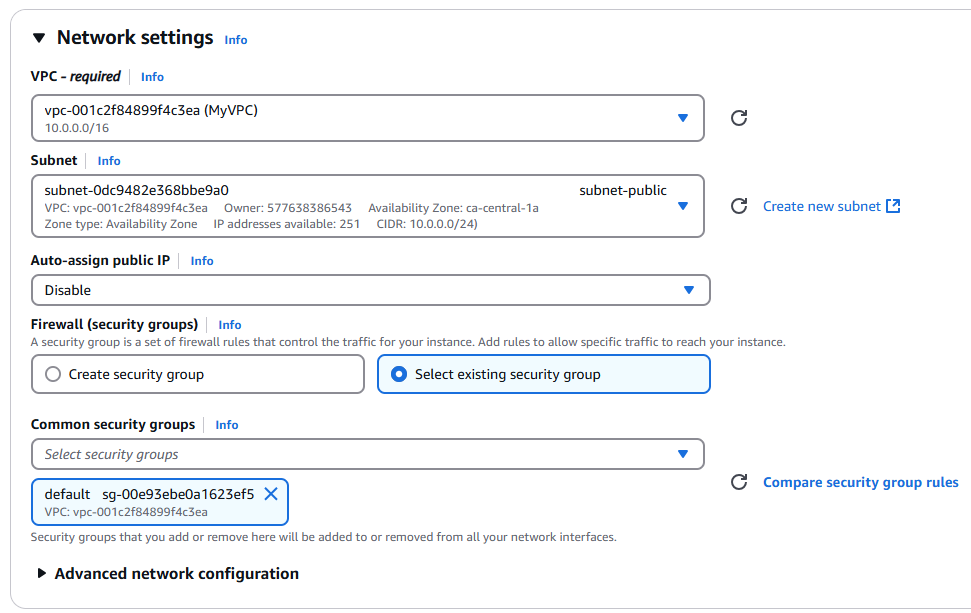
1. Create VPC
2. Create 2 subnets
3. Create IGW
4. Create Route tables
5. Associate RT to respective Subnets
6. Attach IGW to Public RT
7. One EC2 in public subnet and another in private subnet
8. Tested by connect to EC2 of public subnet, it worked and we were NOT able to connect to Private EC2 / private subnet because no Internet Gateway was attached

Now go to EC2





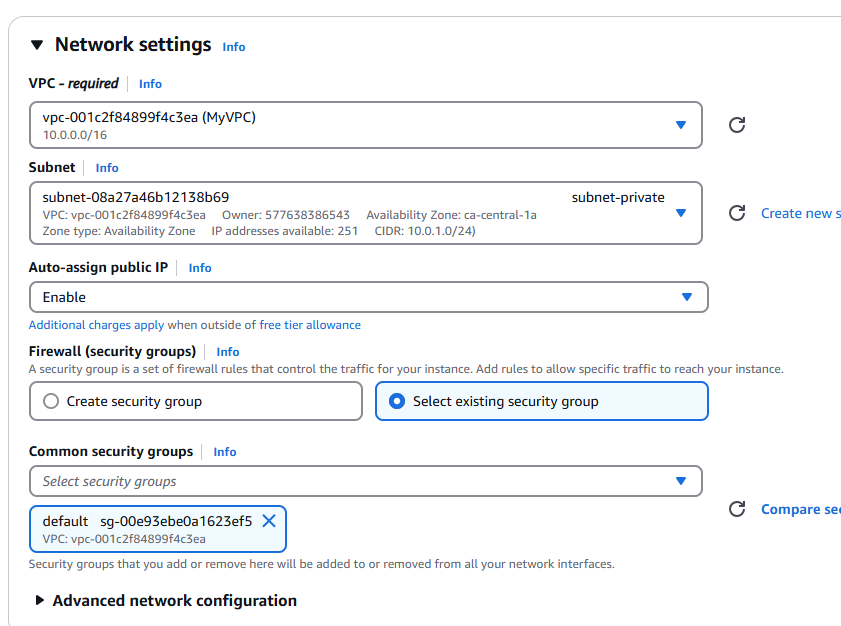
Change VPC to MyVPC, Select subnet-public, Security group default

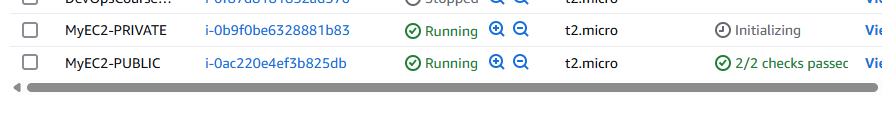


Next create a Private-VM

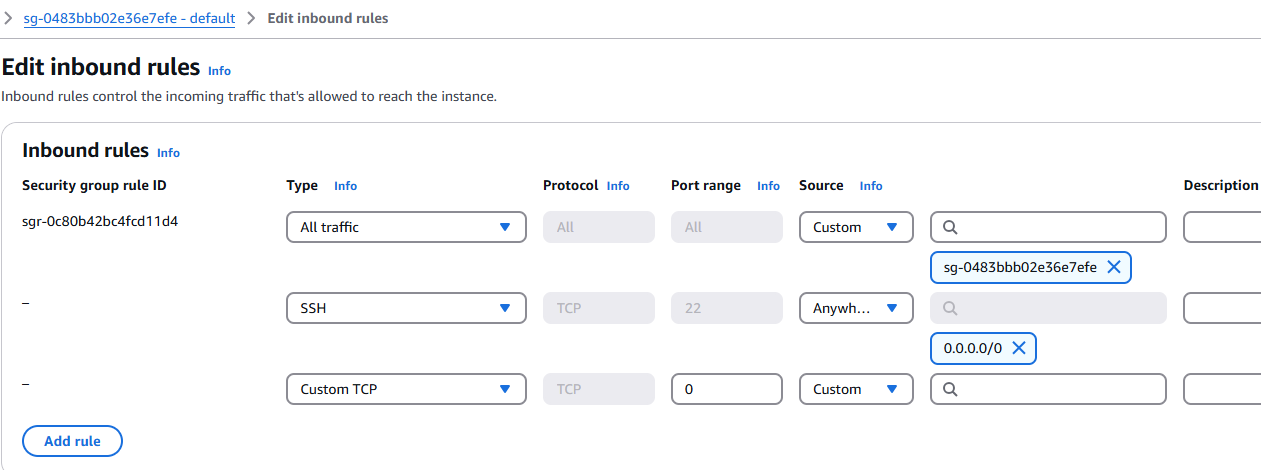
Use the following settings

Auto-assign public IP is ‘Enable’

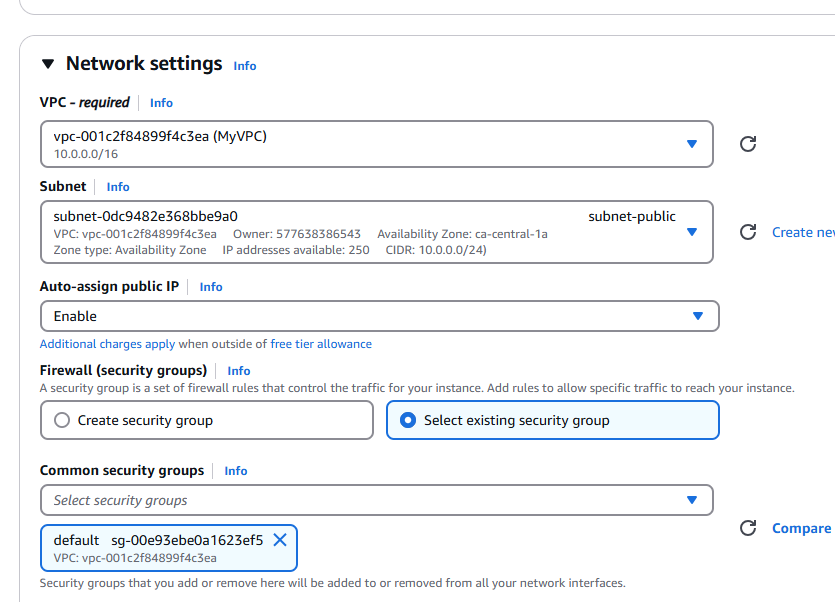




Edit Security Group --> Inbound rules of VPC default SG



For public EC2 also make sure Auto-assign public IP is enabled

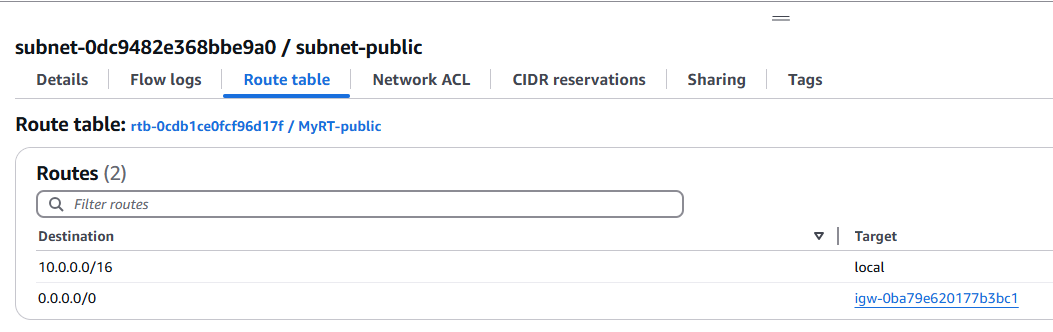


Copy Public IP then connect using MobaXTerm

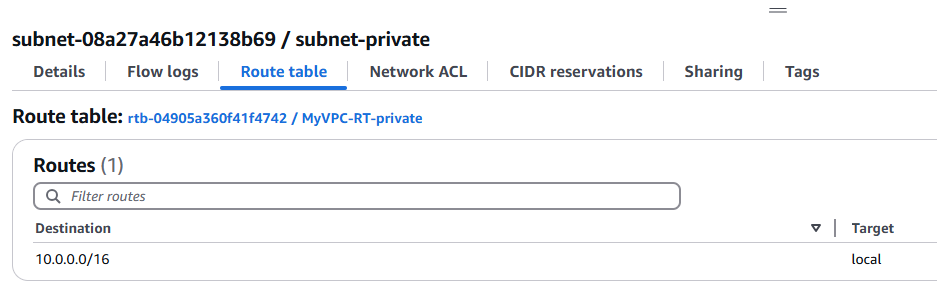
It should connect



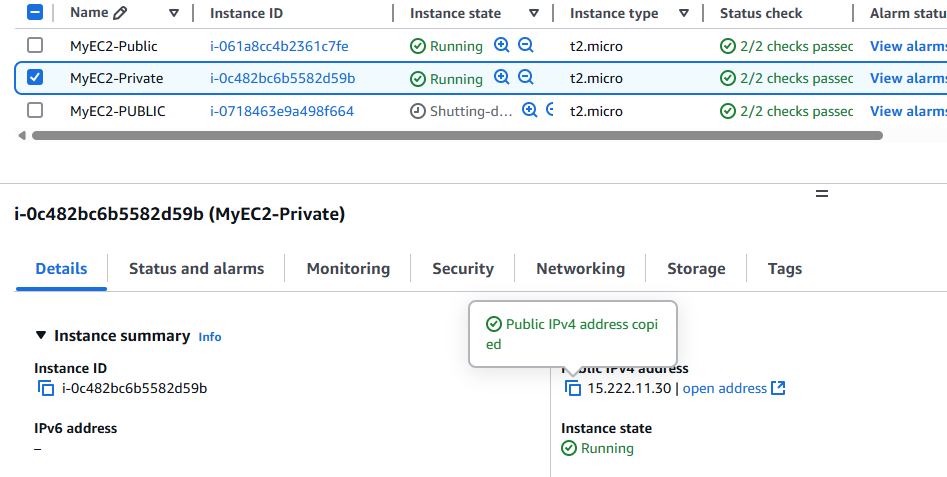
Keep in mind for subnet-public, we have attached igw



For subnet-private, we have local

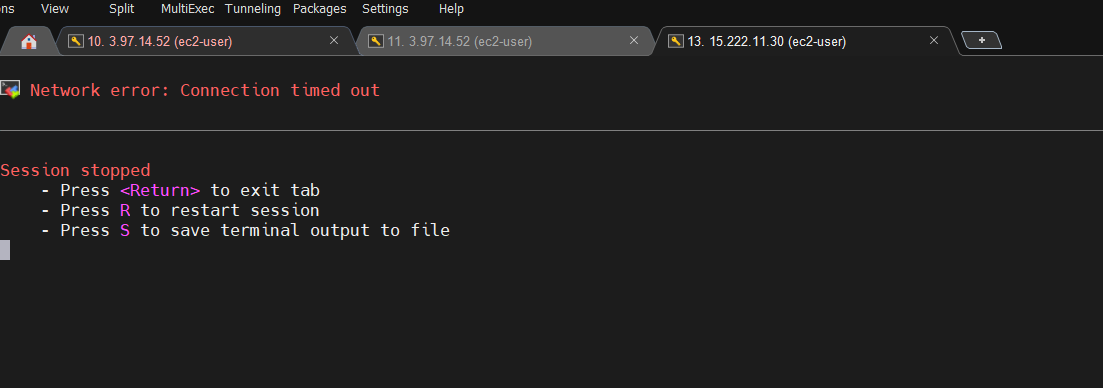


Go back to EC2, connect to private-EC2



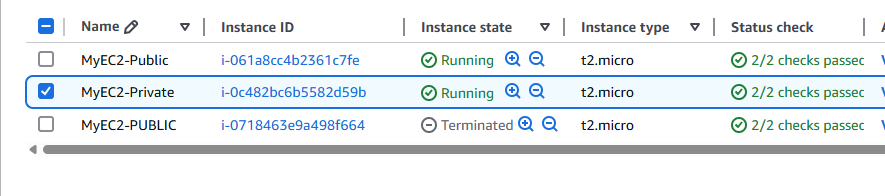
MyEC2-private

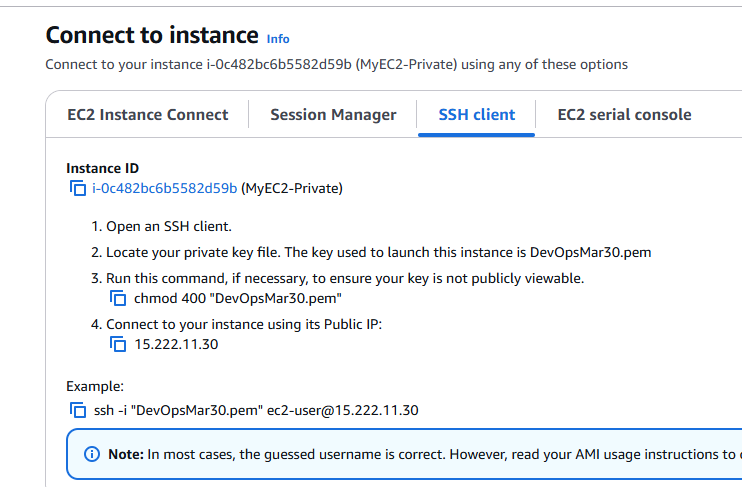
We are not able to establish the connection for private VM



**Connect with Private EC2 of Private Subnet from Public EC2 of Public Subnet using SSH connection:**

Select Private EC2, click Connect

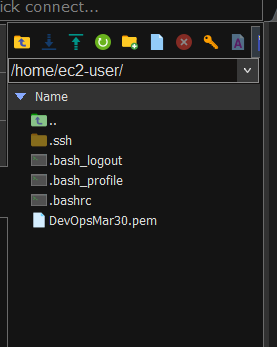


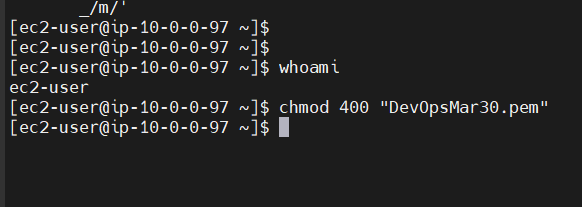


Copy this and paste in EC2

chmod 400 "DevOpsMar30.pem"

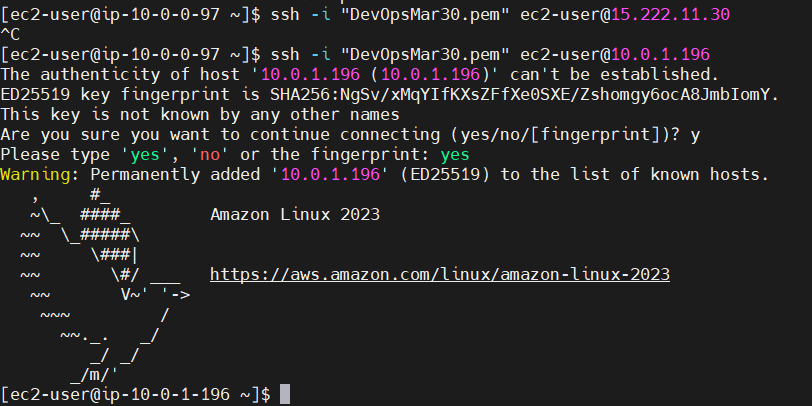
Upload key first





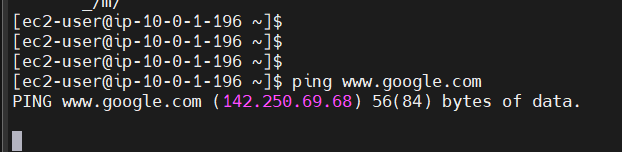
To Connect to Private EC2 from Public EC2

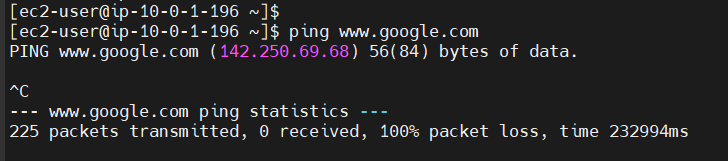
Use PRIVATE IP of Private EC2 Not Public IP then connect



When it comes to public EC2, there is no issues with both Incoming and Outgoing. With Private EC2, for Outgoing service to be enabled, we need NatGateway is a must. Without NatGateway it is not possible. It is paid

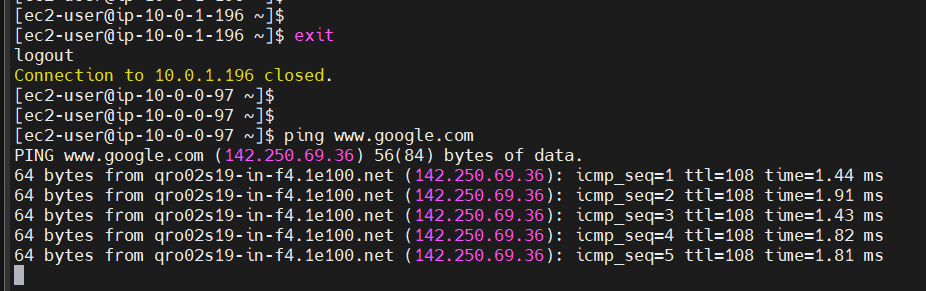
Now I am on Private EC2 on Private Subnet and outgoing services wont work without NatGateway



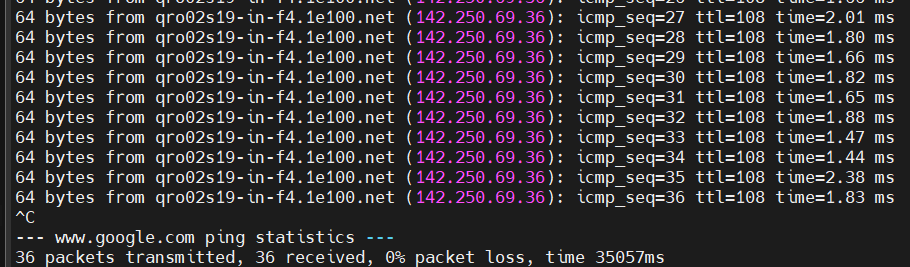


Now go back to Public EC2

I exit out of Private EC2 then do the same thing

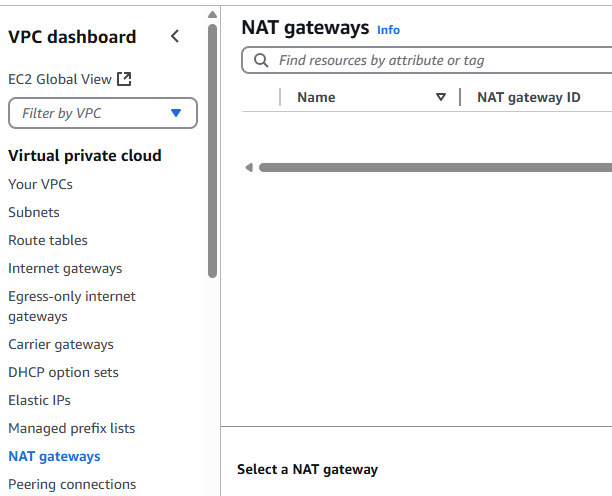


It works! From Public EC2 on Public Subnet



See Packet loss is 0% from Public Subnet

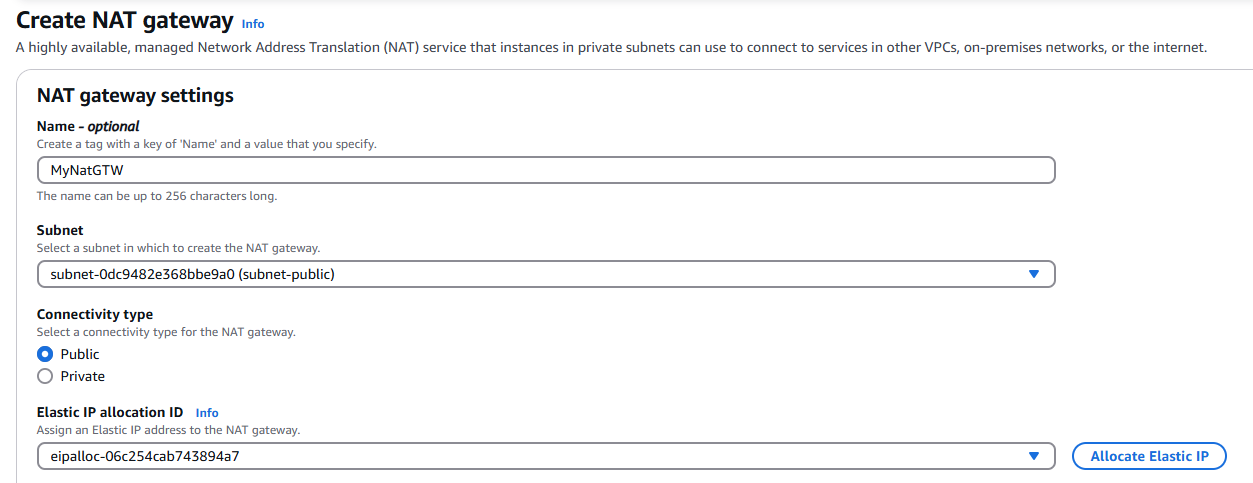
If you go back to VPC, you will see NAT gateways

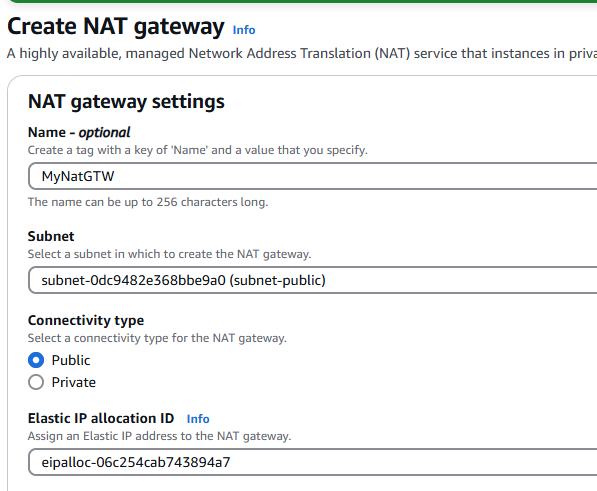


To use Nat Gateway in Private Subnet you have to create in a PUBLIC Subnet, internet should be accessible. Select subnet-public

Click Allocate Elastic IP

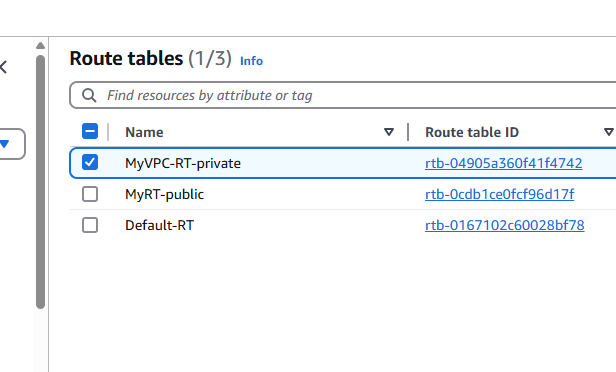
Elastic IPs and Nat Gateway are paid services. Please delete after practicing



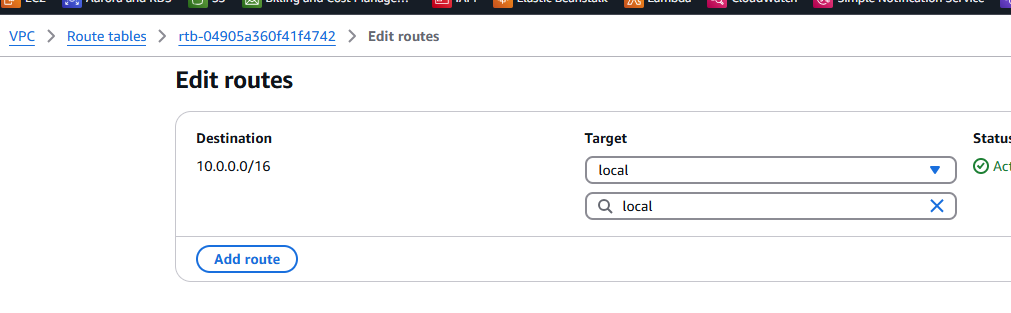


Click Create Nat Gateway

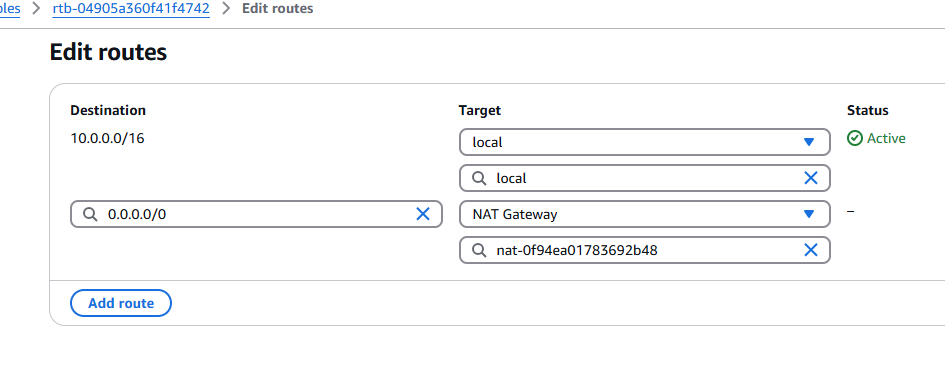
Go back to Route tables



For Private RT, click Edit Routes



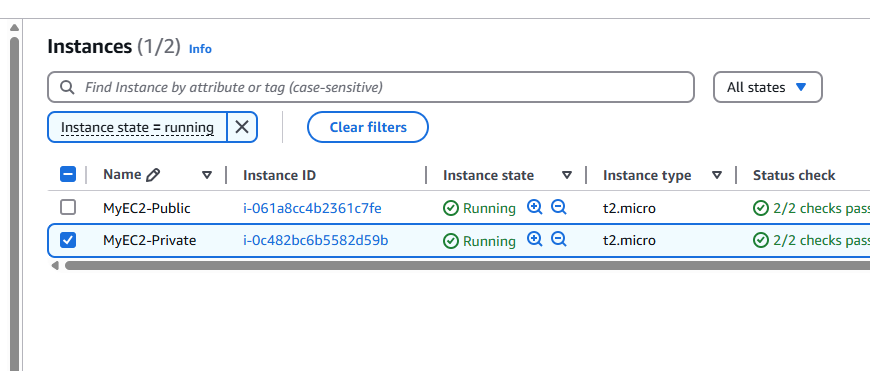
Add route



Select 0.0.0.0/0 then NAT Gateway ---> Select the one we have created

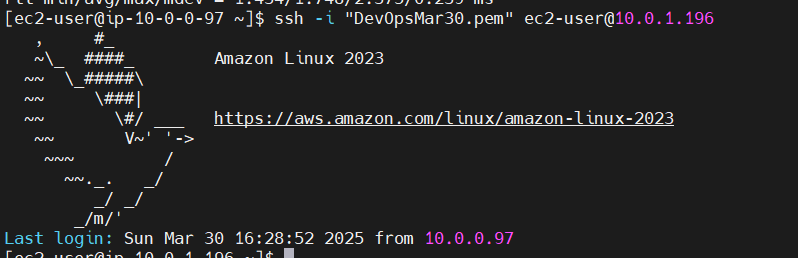
Click Save changes

Go back to EC2

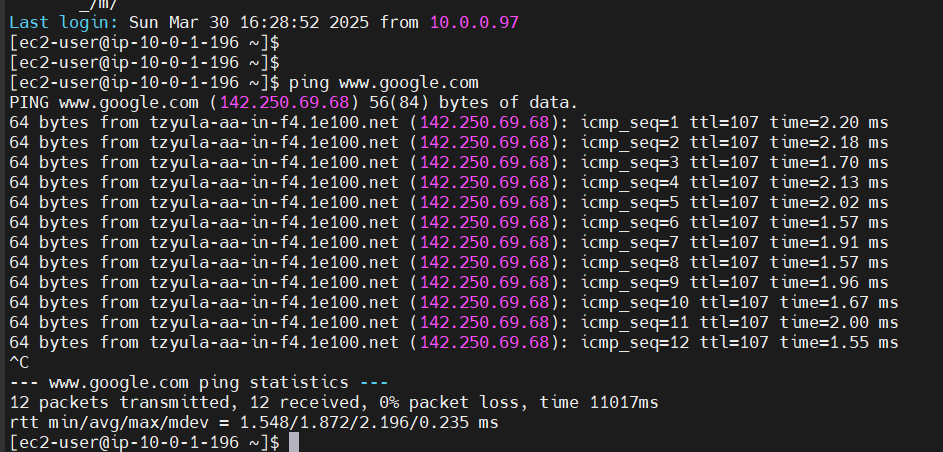


MyEC2-Private --> Connect

Connect to Private EC2 from Public EC2 again

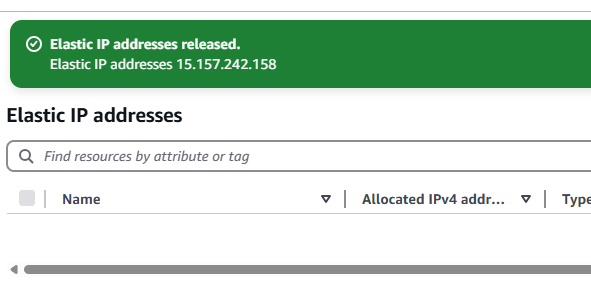


Now ping from Private EC2 and 0% packet loss



Please delete NAT Gateways immediately

Delete Elastic IP also --> Release Elastic IP



Right now we established connection between different Subnets within the same VPC

Say you have two different VPCs, owned by two different Users

Can we connect EC2s between them and perform operations?

VPC2

VPC Peering

VM2

VM1

That’s where VPC peering comes into Picture

VPC1