Table of contents

Introduction to Public subnet and Private subnet :

- Now that we can create VPC,subnets ,route tables ,IGW and NACL, we'll see how do we diffrentiate between public subnet and private subet .
- Agenda for today we'll be understanding the subnet , NAT and VPC endpoint

How to diffrentiate between a public subnet and private subnet

Public Subnet

- The Public subnet hosts EC2 instances having public ip addresses .
- Since the instances are expected to have public ip ,generally the "**auto-assign public ip**" will be marked as **Yes**
- Also in order to reach the instances having public ip , we need IGW . This basically translates to having a route table attached to the subnet which must have a route to IGW.
- So 2 properties using which we can identify a public subnet is
  - "Auto assign public ip " setting to be turned to Yes
  - Subnet should have a route table assigned which should have a route to IGW
  - Now we can conclude , all the default subnets created under default VPC are public subnets.

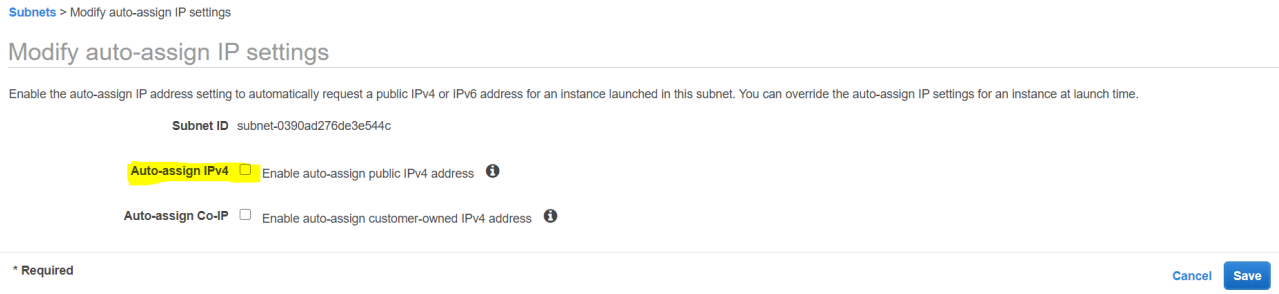
Private subnet

- Private subnet hosts instances which will only have private ip address .
- Naturally the "**auto assign public ip**" setting is kept as **No**
- Since the instances do not have public ip , they cannot utilize the IGW anyways . Hence a subnet has to have a seperate route table which does not have IGW associated with it.
- 2 properties which define a private subnet
  - "Auto assign public ip " setting to be turned to No
  - Subnet should have a seperate route table assigned which does not have a route to IGW

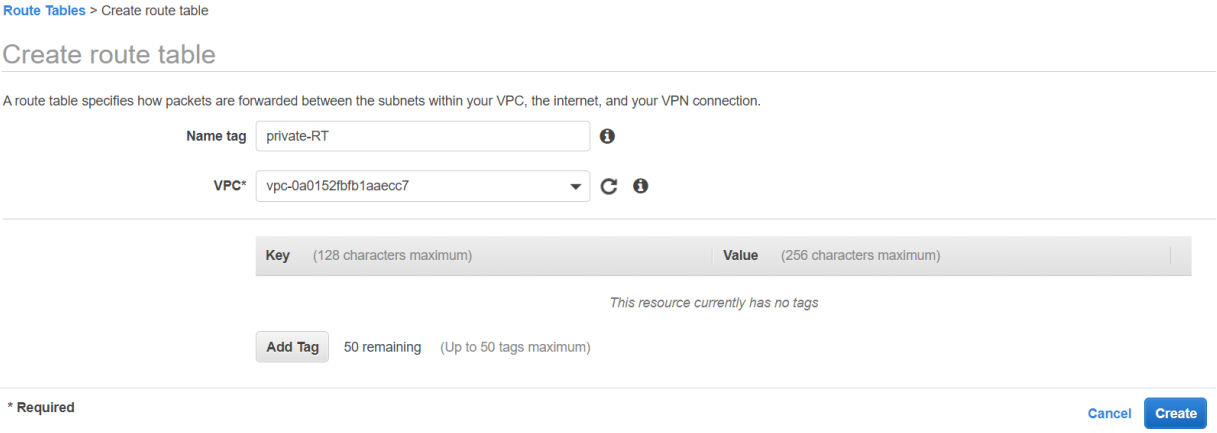
Creating private subnet

- We have already seen how to create a public subnet when we were replicating the default subnet under default VPC .

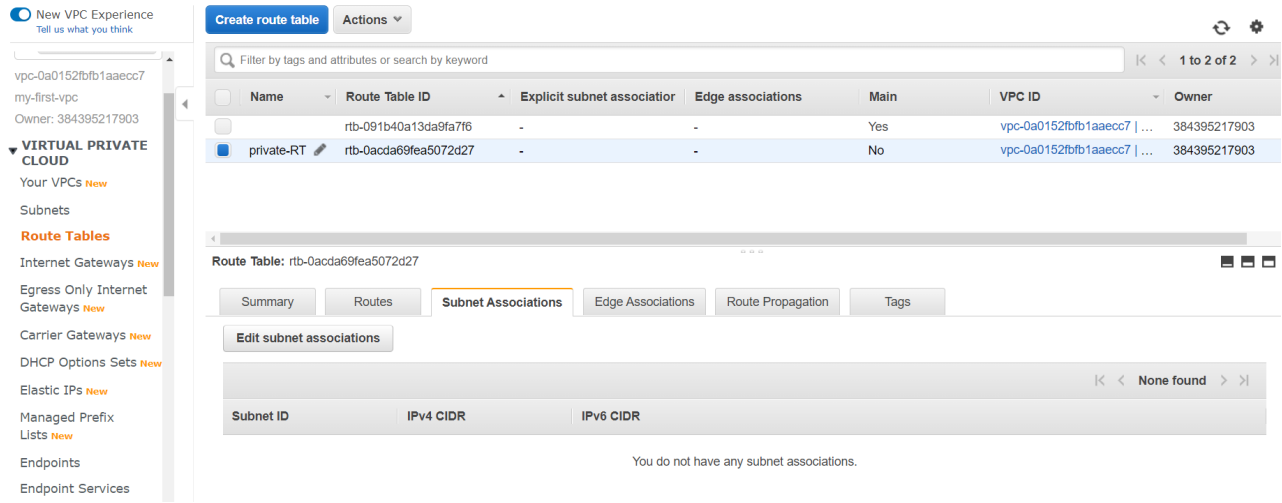
- Let us now create a private subnet
- Create a VPC create a sudbnet under the same
- Once created , click on subnet , go to actions and click on "modify auto-assign IP settings "



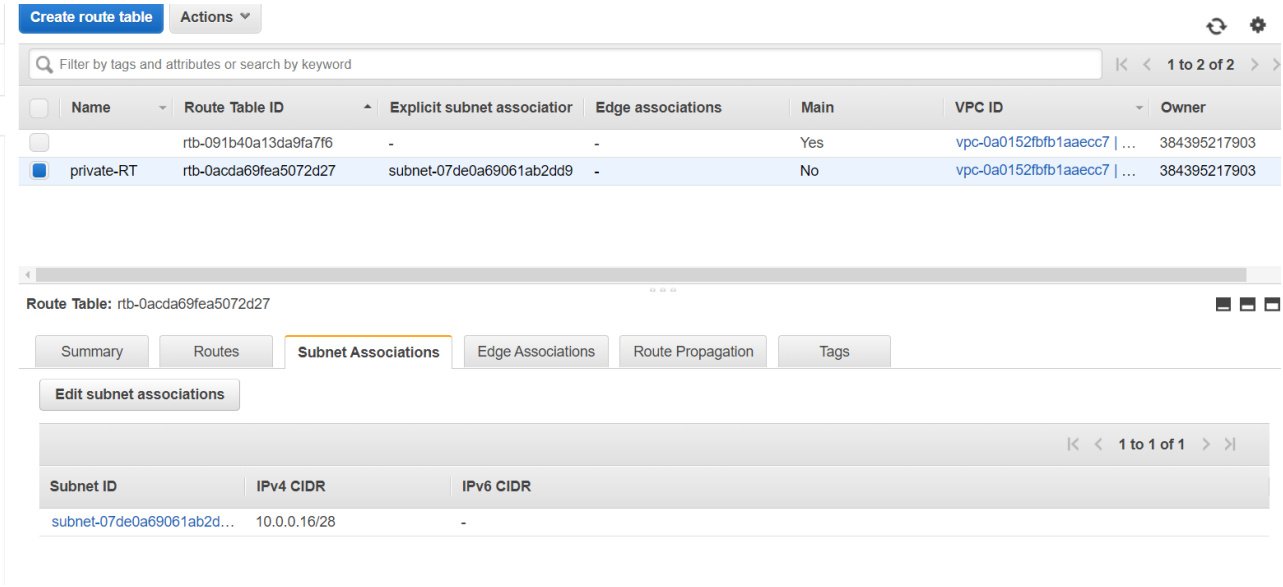
- Make sure the "Enable auto-assign public IPv4 address" is unticked like above .
- Now that we have enabled the 1st setting let us move to the 2nd criteria
- We need to create a seperate route table which needs to be associated with the subnet
- Navigate to route table and click on create route table



- Provide a name for Route table and select the VPC as above and click on create route table .
- Once the route table is created , click on the created route table and navigate to subnet associations



- click on edit subnet associations , check the private subnet and click on save .



- Since this route table by default does not have an IGW attached , and is attached to our subnet . This fulfills our second criteria of private subnet .
- All the instances launched in this subnet will not have a public ip as well as they will not have internet access from and to the instances.

How to access instances in private subnet i.e. which only have a private ip address

- We have seen till now that private ip addresses can only be accessed from within a network
- Since our VPC is a network , this can proivide us a way to connect to our instances .
- In order to acheive this , we need to have a VPC with one public sunet and one private subnet .
- Launch 1 EC2 instance in each subnet so that we will have 2 instances in total. Make sure you use different security group for each.
- We will refer the instance launched in public subnet as public instance and similarly instance launched in the private subnet will be termed as private instance.
- The pem key which we have assigned to our private instance need to copied on the public instance
    - Note : You can upload the key in any S3 bucket , use an IAM role to copy the file on the public instance
- Now the goal here is to access the private instance using public instance
- Login to public instance and use below command

```
ssh -i keyname.pem ec2-user@private-ip-address-of-private-instance
```

- If you receive **bad permissions** error then perform below command and try again

```
sudo chmod 400 keyname.pem
```

- There will be a connection timed out error now. in order to resolve it , it the security group of private instance , add a rule granting ssh access from private ip of public instance .
- Once this is setup try again and it should work .

NAT gateway

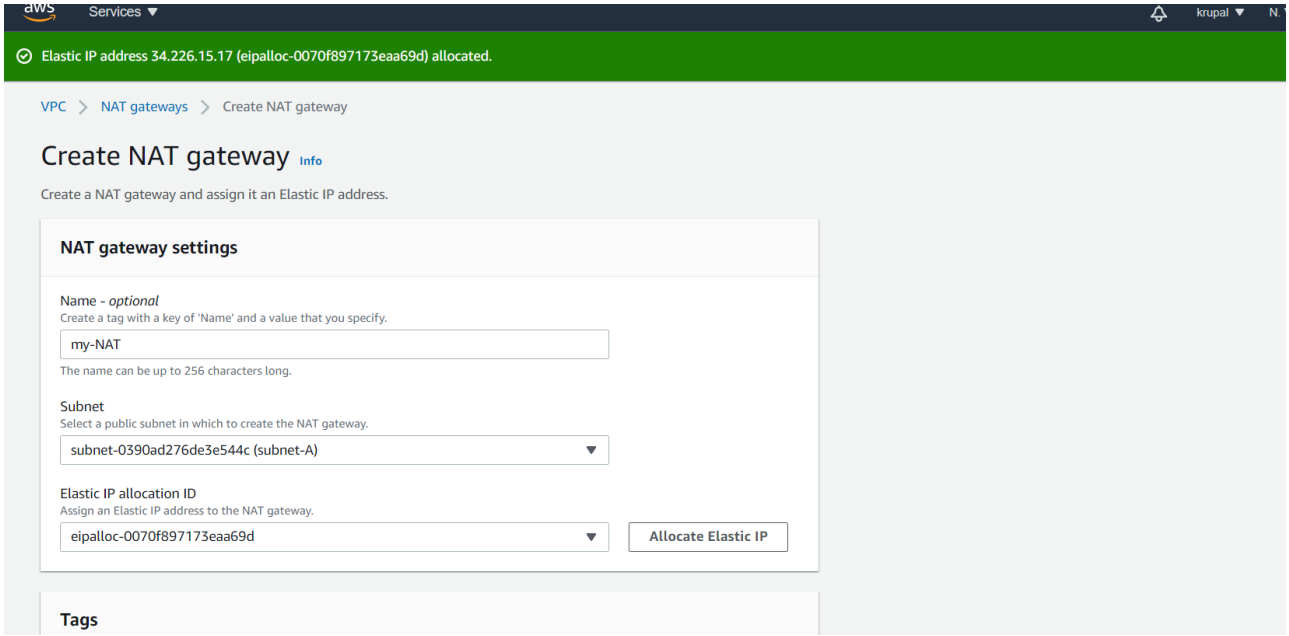
- Once we are connected to the private instance, let us check if we have internet connectivity from the instance

```
ping www.google.com
```

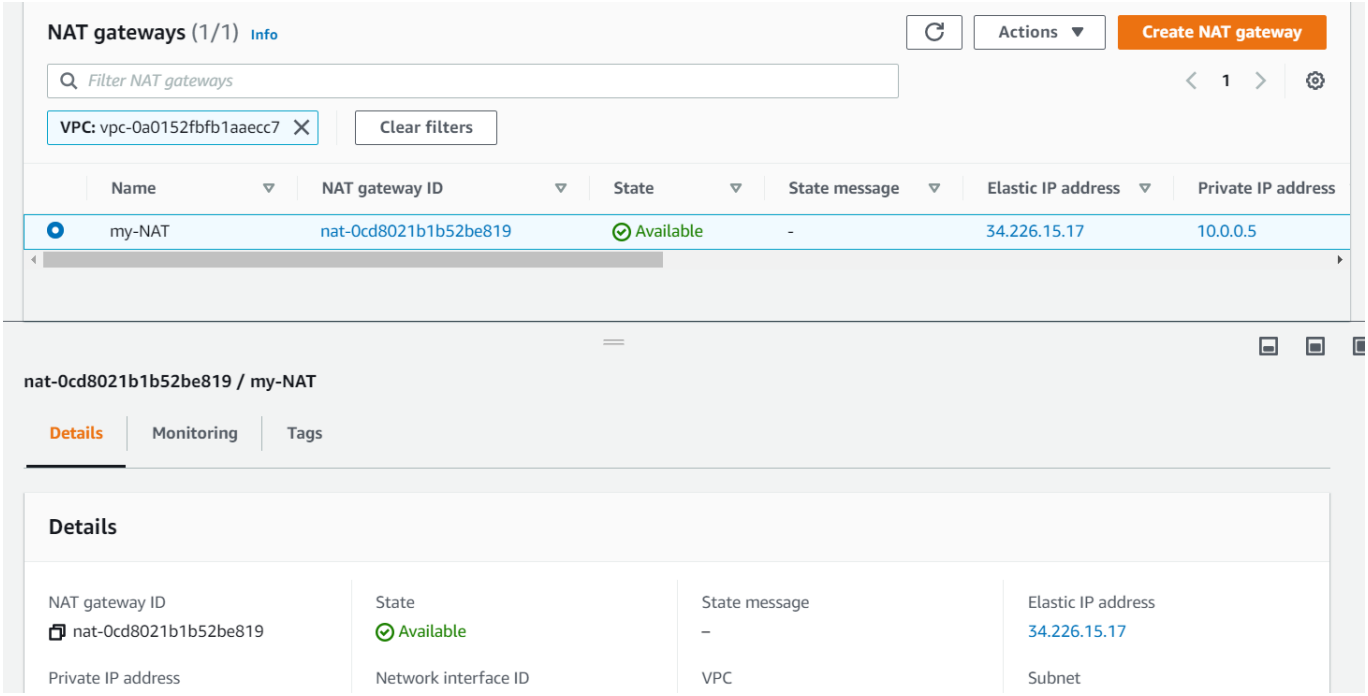
- Since we do not have a route table which has an IGW , we will not be having internet connectivity and above command will fail
- NAT gateway stands for Network Address Translation , it is basically used for bringing internet to instances which do not have public ip address .

Creating and using a NAT gateway

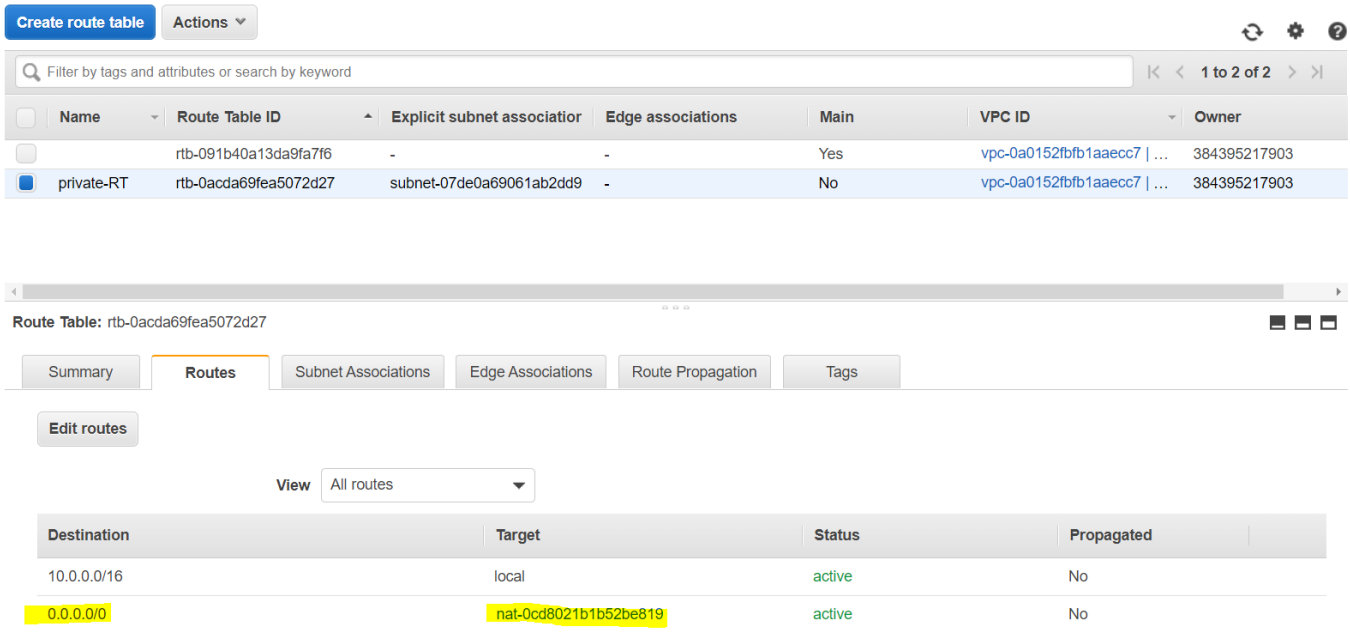
- Navigate to "NAT gateways" in VPC
- Click on "Create NAT gateway"
- Name the NAT gateway
- In the subnet tab select the **Public subnet **
- Reason for selecting public subnet is , NAT gateway relies on IGW to bring internet . Since public subnet has access to IGW , we need to create NAT in public subnet
- Click on allocate Elastic Ip . This creates a elastic ip which will be associated to our NAT . We need a static public IP because without a public IP IGW cannot get us internet . Hence we require a EIP



- Click on create NAT gateway
- Wait for the NAT gateway to become available



- Once this NAT is created , similar to IGW , in order to use it We must add a route to internet using route table
- We had created a didcated route table for our private subnet . Let us add a entry in the route table like below



- In order to add the above entry , Select our private route table . Click on add route
- In destination add 0.0.0.0/0
- in target select "NAT gateway" and select the newly created nat gateway id .
- Click on save .
- Once this is done login to the privat einstance again and try below command again

```
ping www.gooogle.com
```

Points to consider

- Post practice make sure to delete the components inside the VPC , i.e. igw ,NACL,NAT.elastic ip etc before deleting the VPC. Without that VPC will not be deleted
- Public instance used for jumping to private instances is termed as jump host or bastian host
- While whitelisting traffic for within a VPC , always use private ip address
- Always remember , NAT gateway is created in public subnet but is used by a private subnet