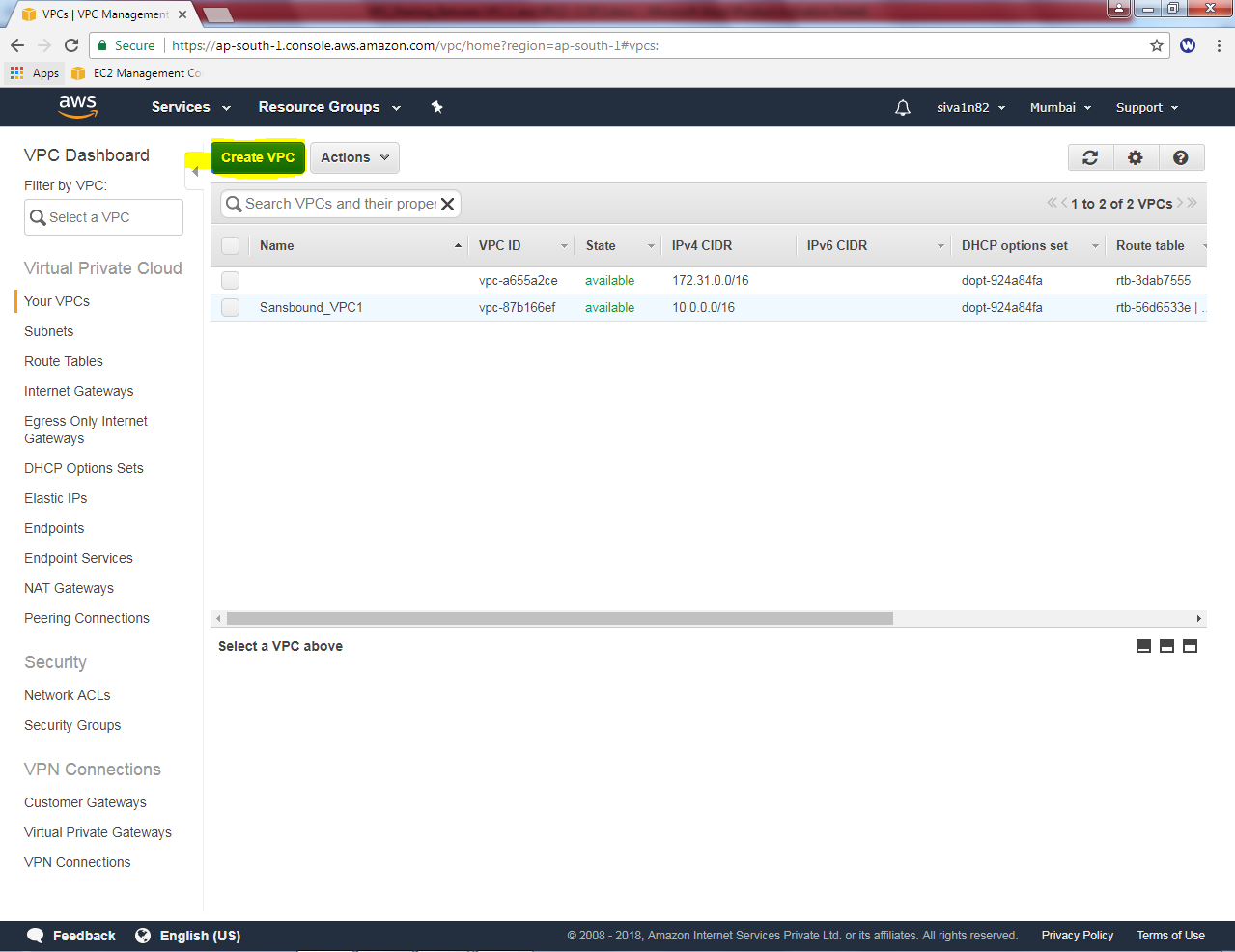
Lab 13

**Configure VPC Peering Between two VPC’s – 2 of 3**

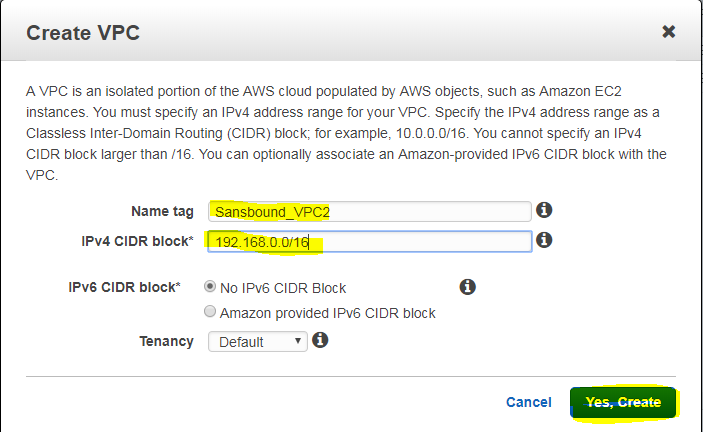
We need to create VPC2 in Mumbai region,

Click “create VPC”.



While creating VPC, name tag as “Sansbound\_VPC2”.

IPV4 CIDR block as 192.168.0.0/16 subnet



click “Yes, create”.

Then we need to create subnet for the Sansbound\_VPC2.

In VPC Dashboard, click Subnet, then click “create subnet”.

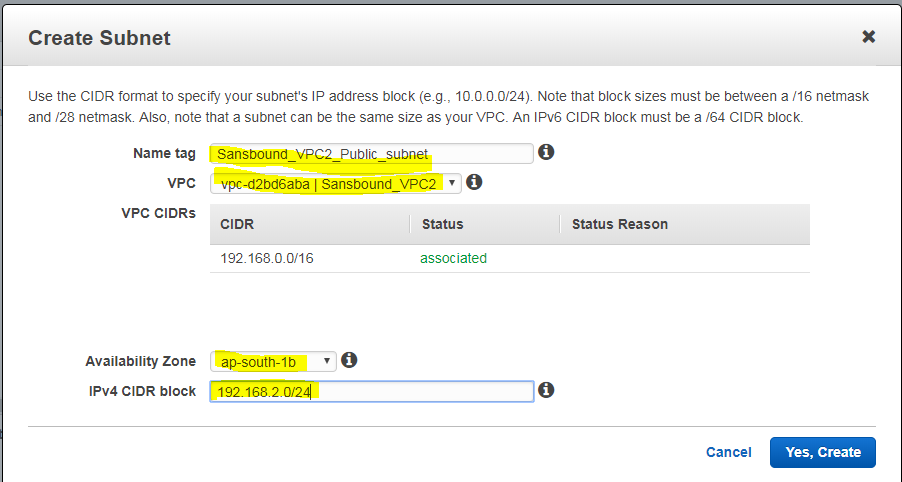
While creating subnet,

Name tag as “Sansbound\_VPC2\_Public\_Subnet”.

VPC as Sansbound\_VPC2.

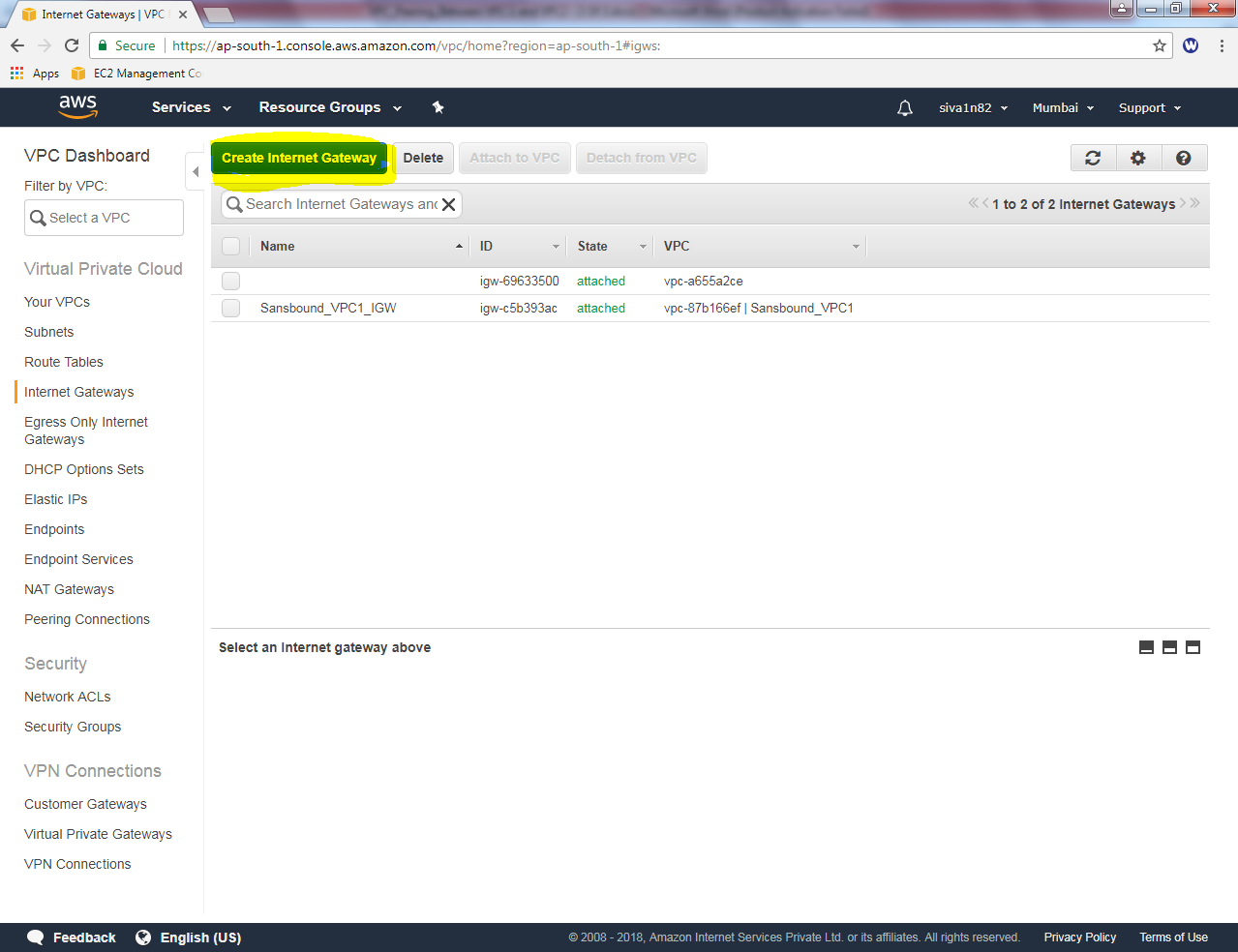
Availability Zone – 1B (Optional)

IPv4 CIDR Block – 192.168.2.0/24 subnet.

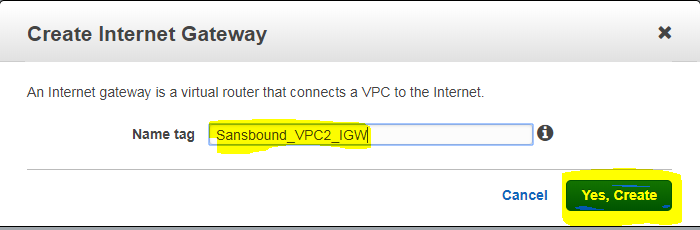


Click “Yes, create”.

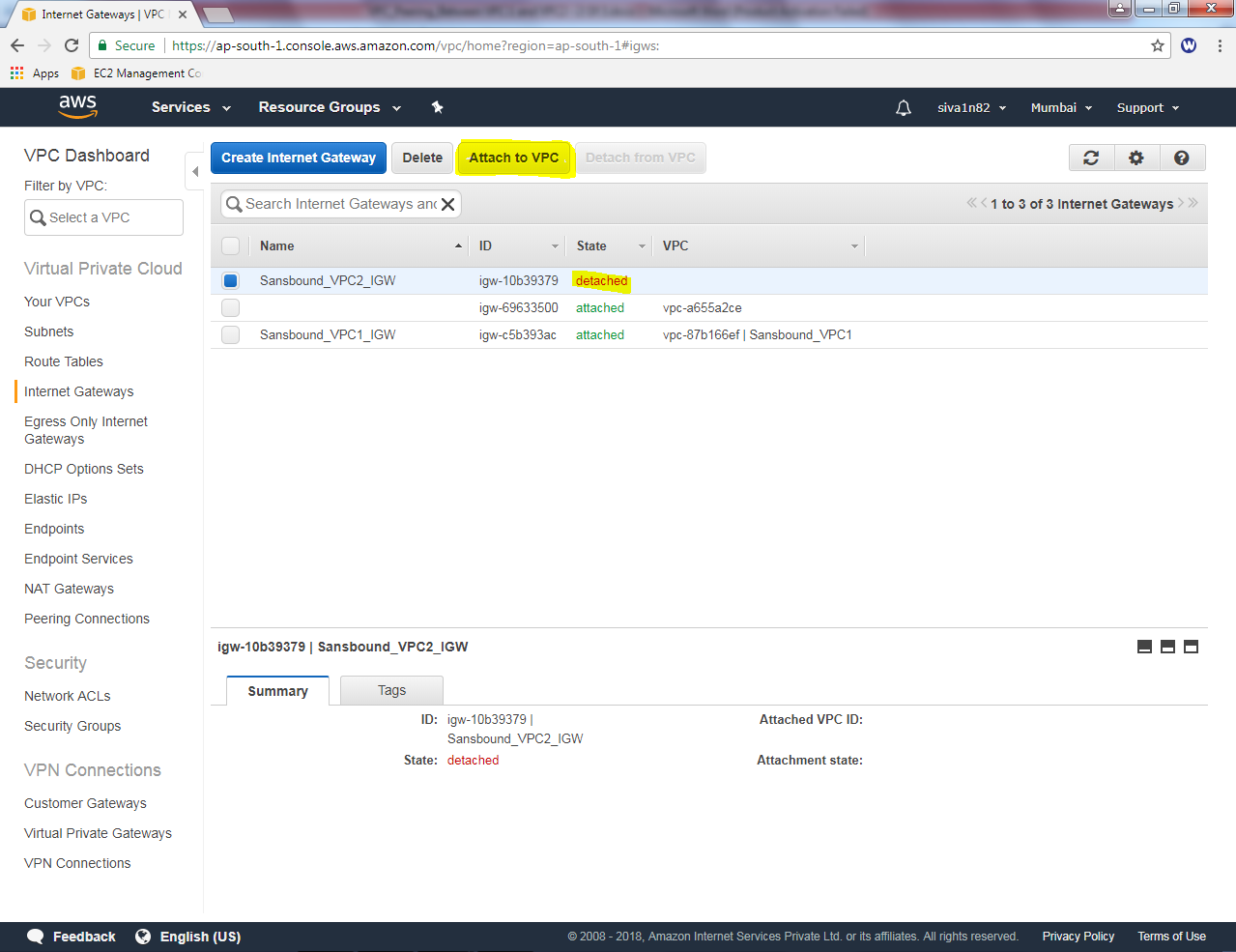
Then we need to create an internet gateway, click “create Internet Gateway”.

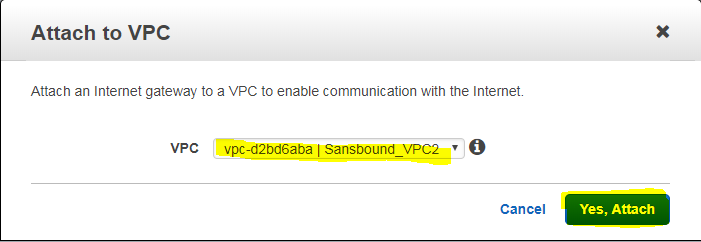


While creating internet gateway Name tag as “Sansbound\_VPC2\_IGW”.



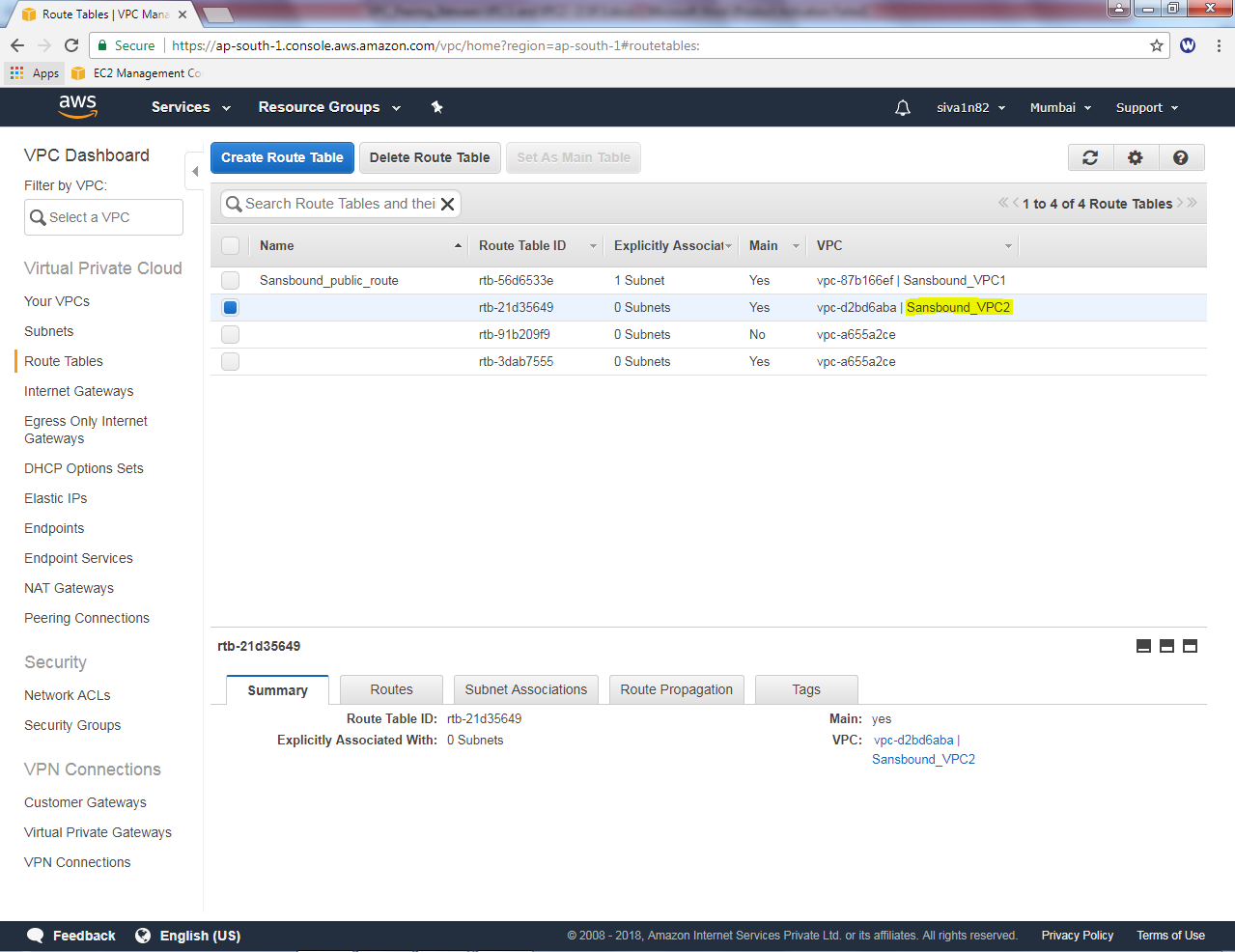
It shows, IGW in detached state, we need to attach VPC.

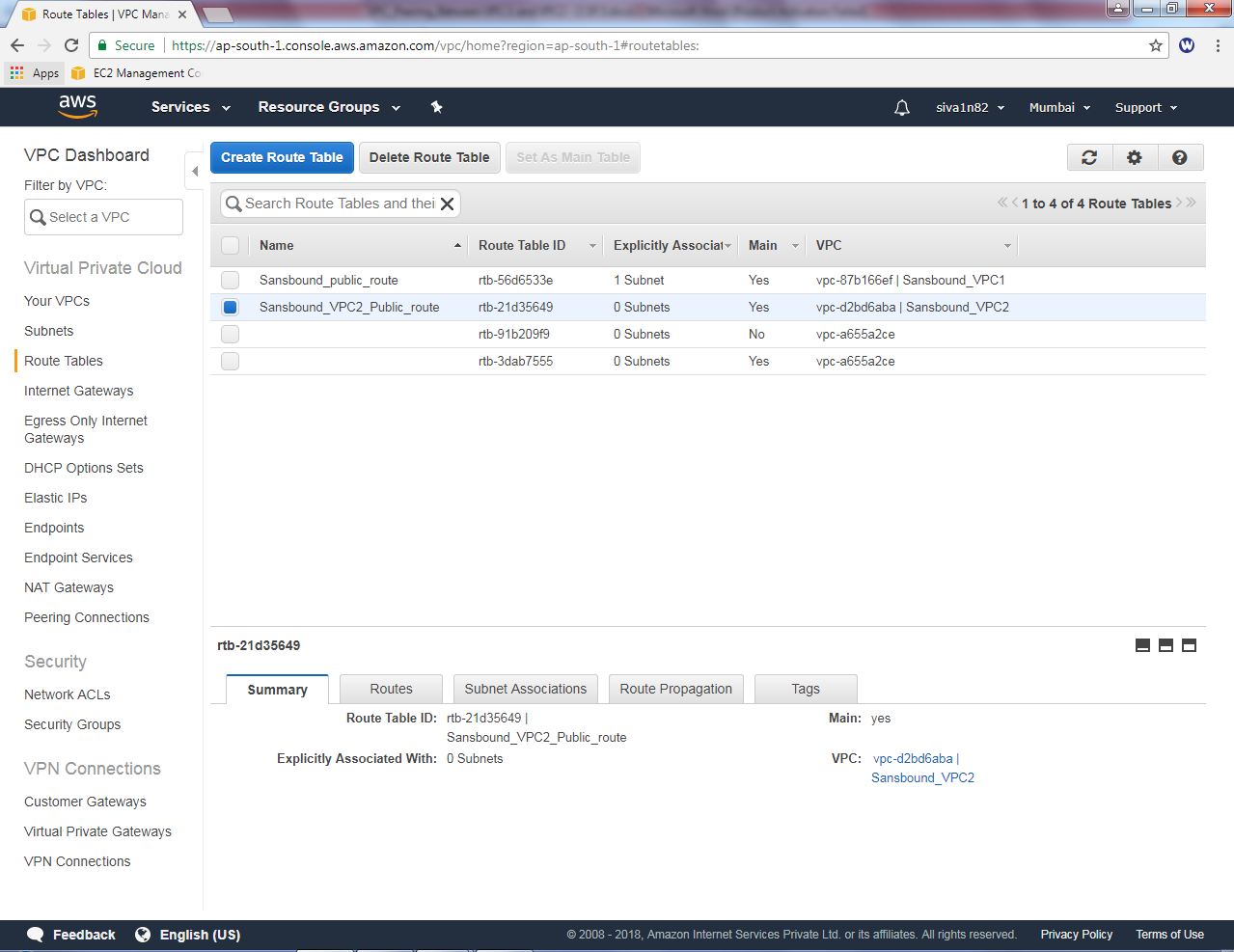




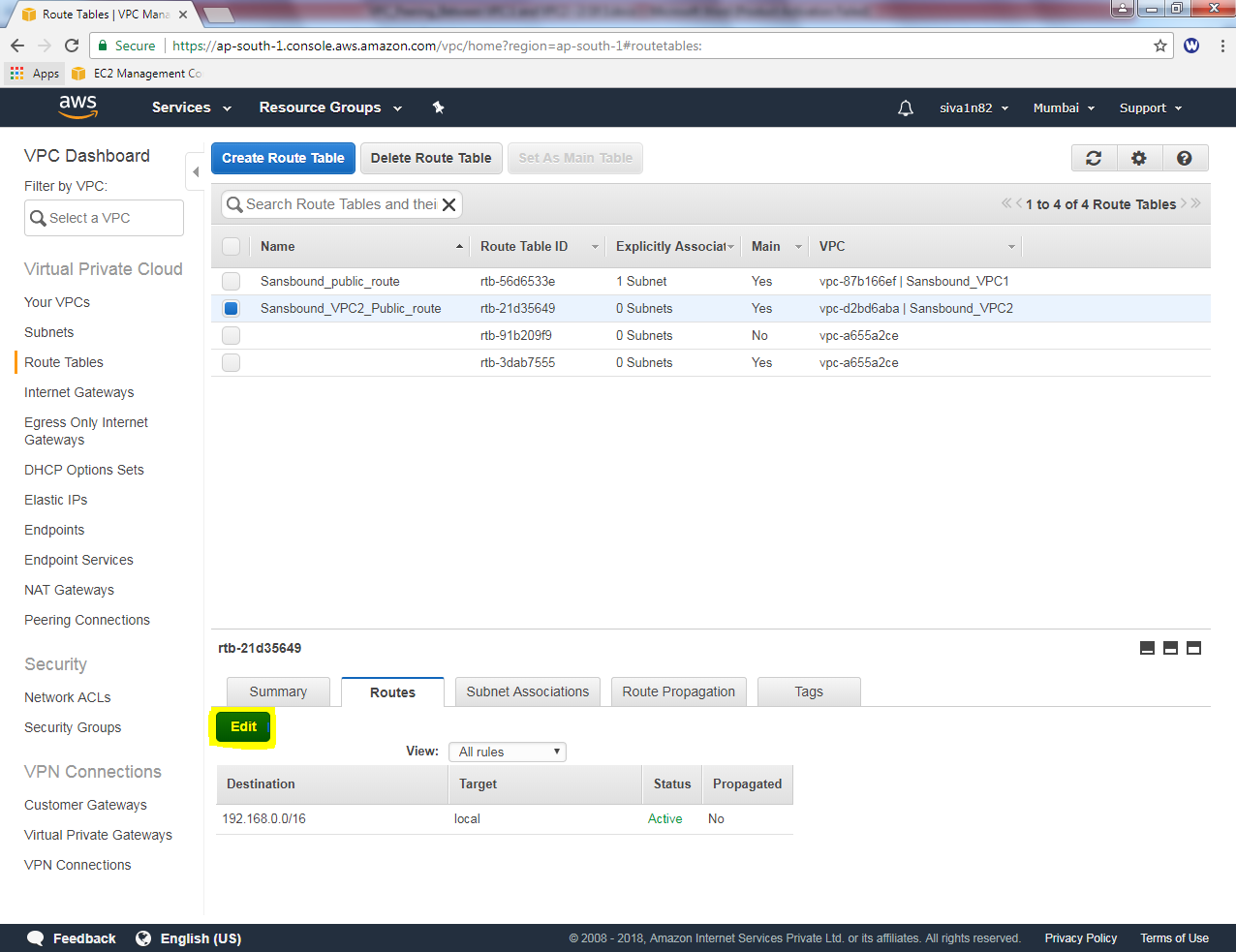
Click “Yes, Attach”.

Rename the Sansbound\_VPC1 route table as sansbound\_VPC2\_public\_route.

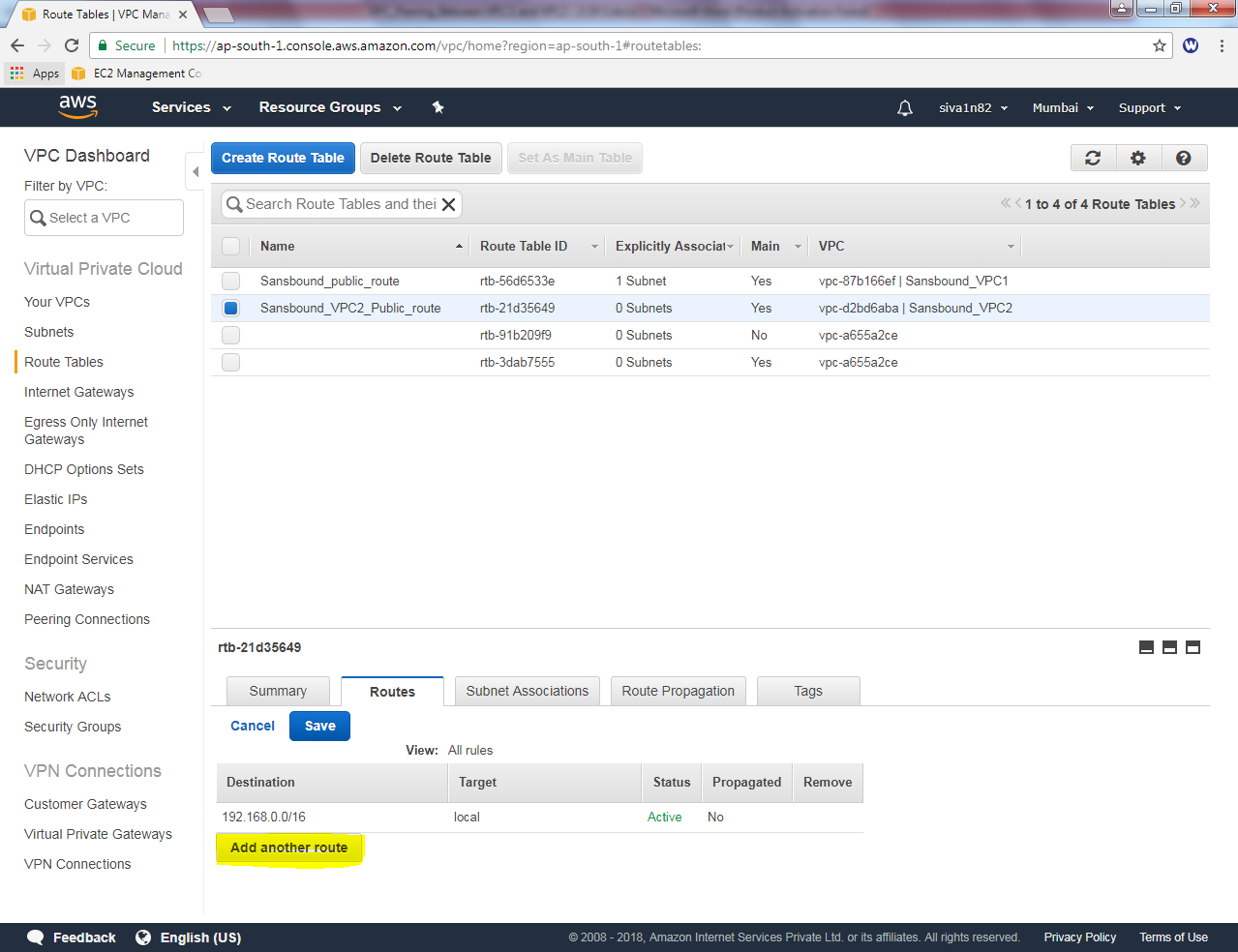




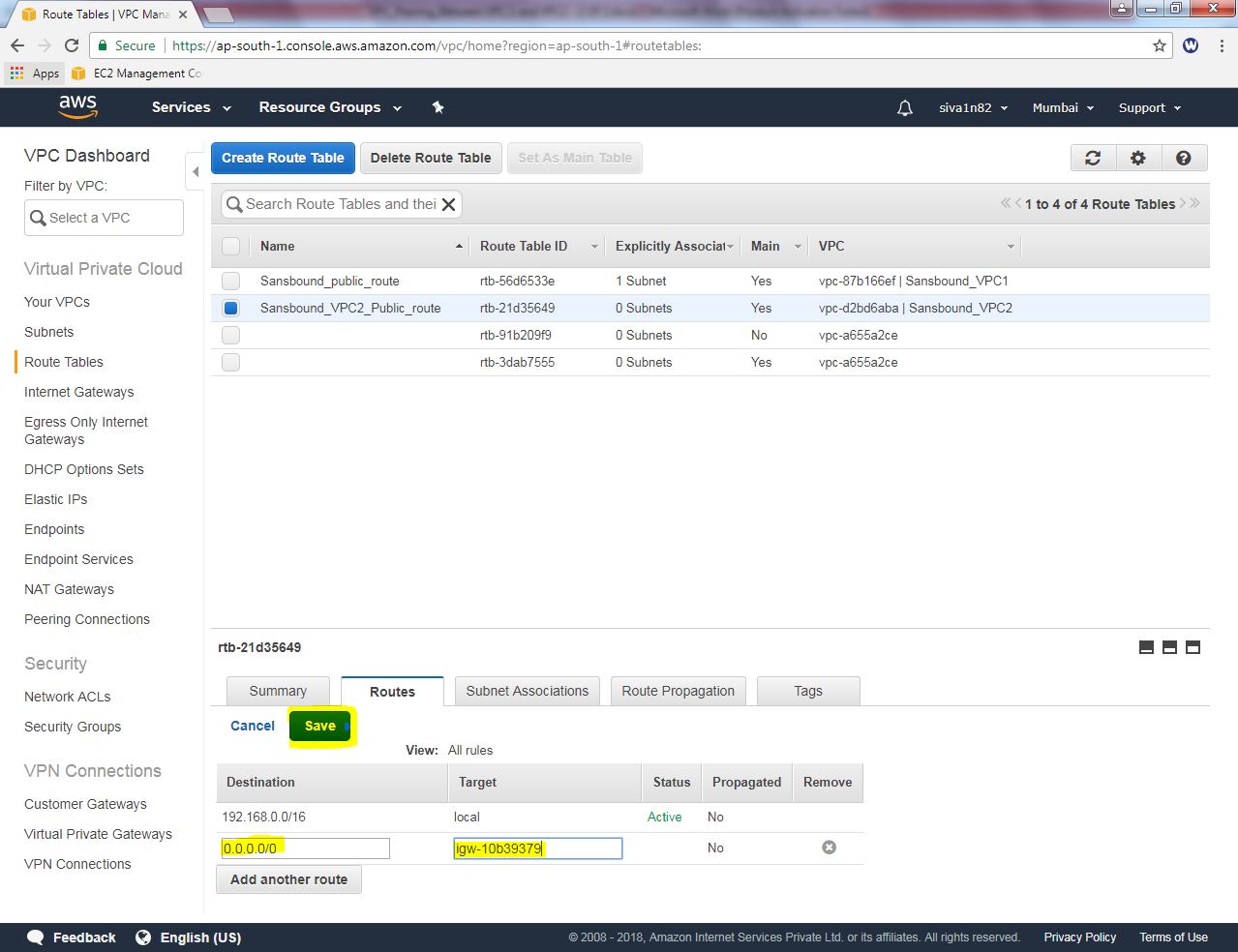
InSanbound\_VPC2\_Public\_route table, select route tab then click “Edit” option.



Click “Add another route”button.

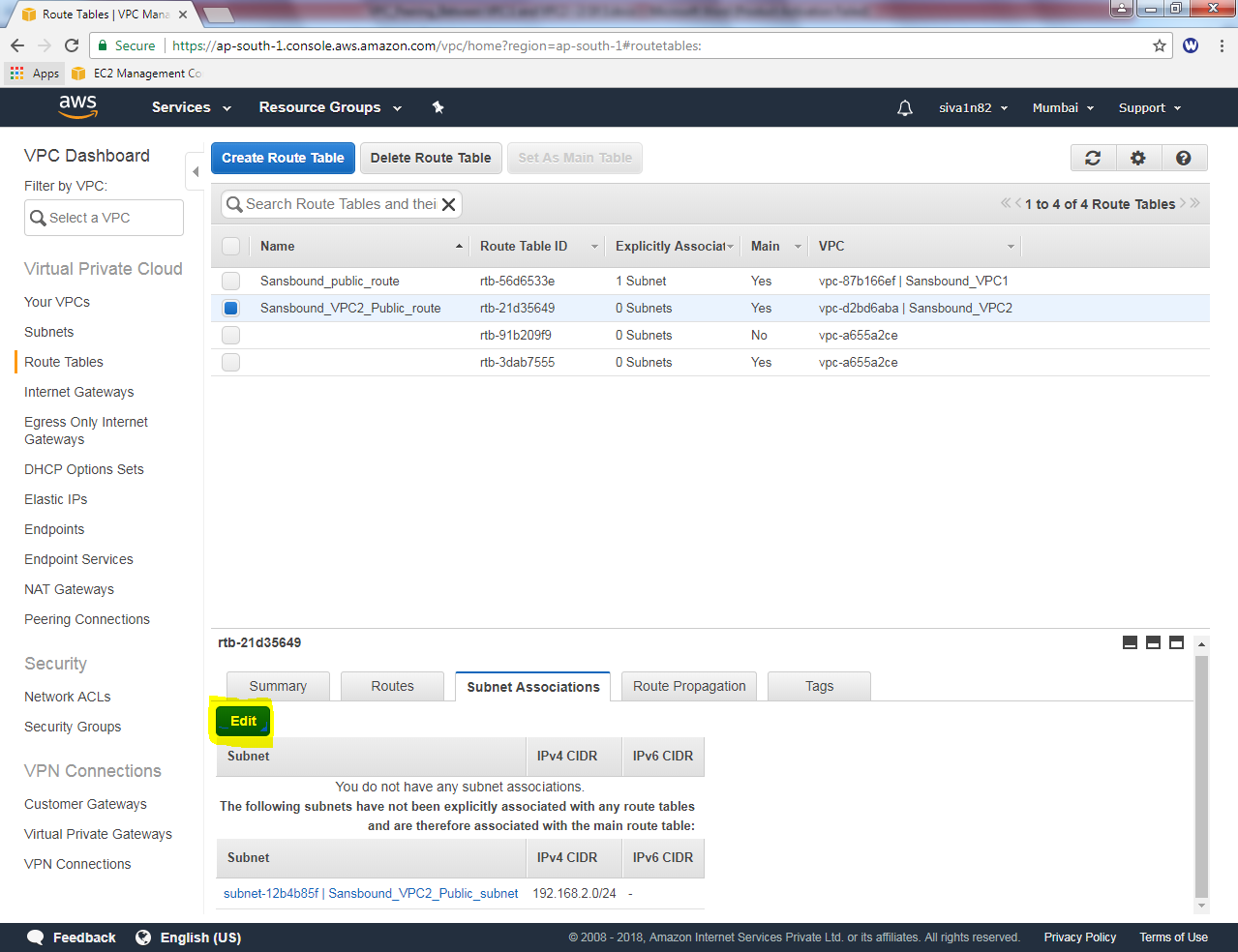


Add default route 0.0.0.0/0 and select **”igw-\*”** as target.

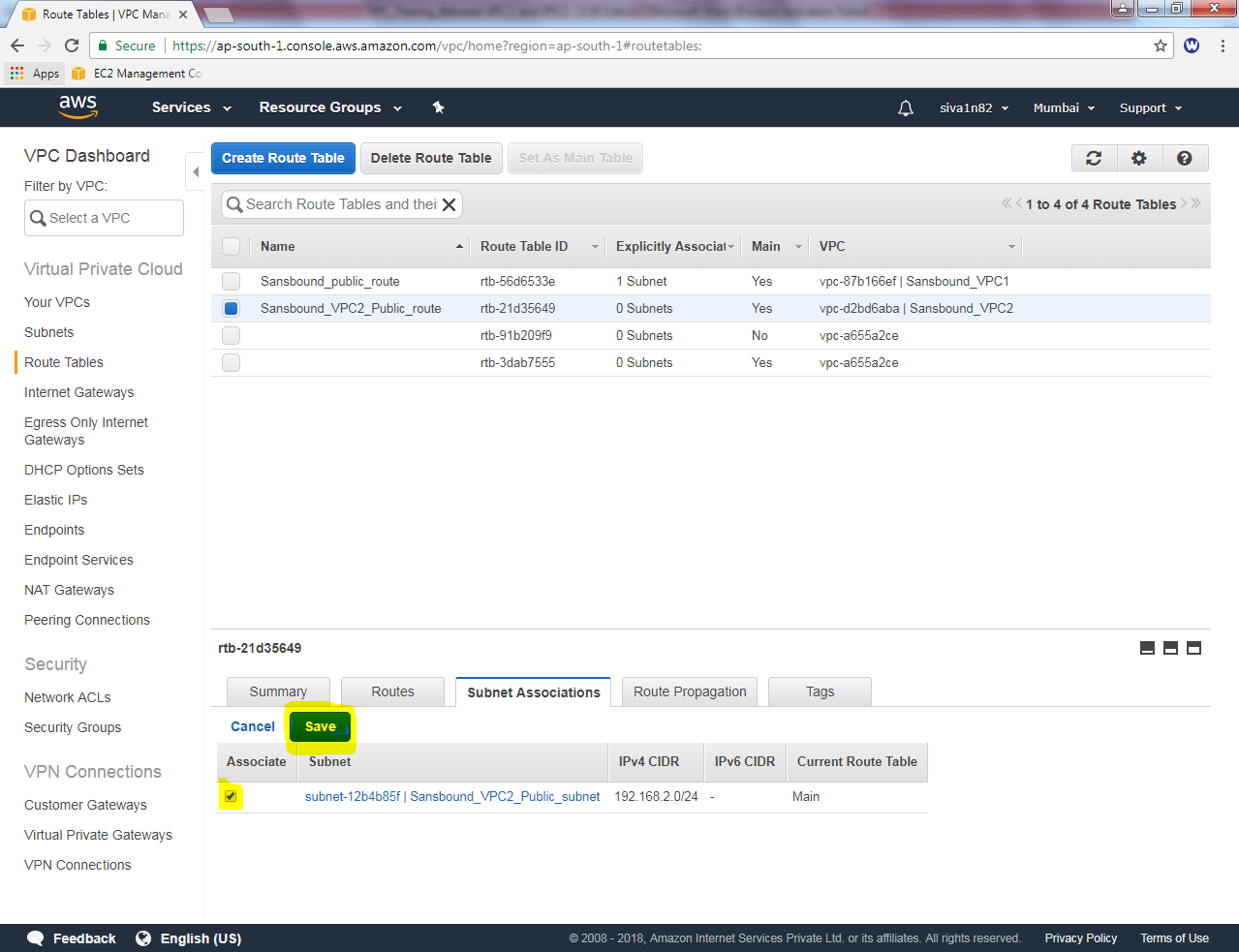


Then click “save”.

Then we need to associate the subnet. Click “Subnet associations” tab, then click “Edit” option.

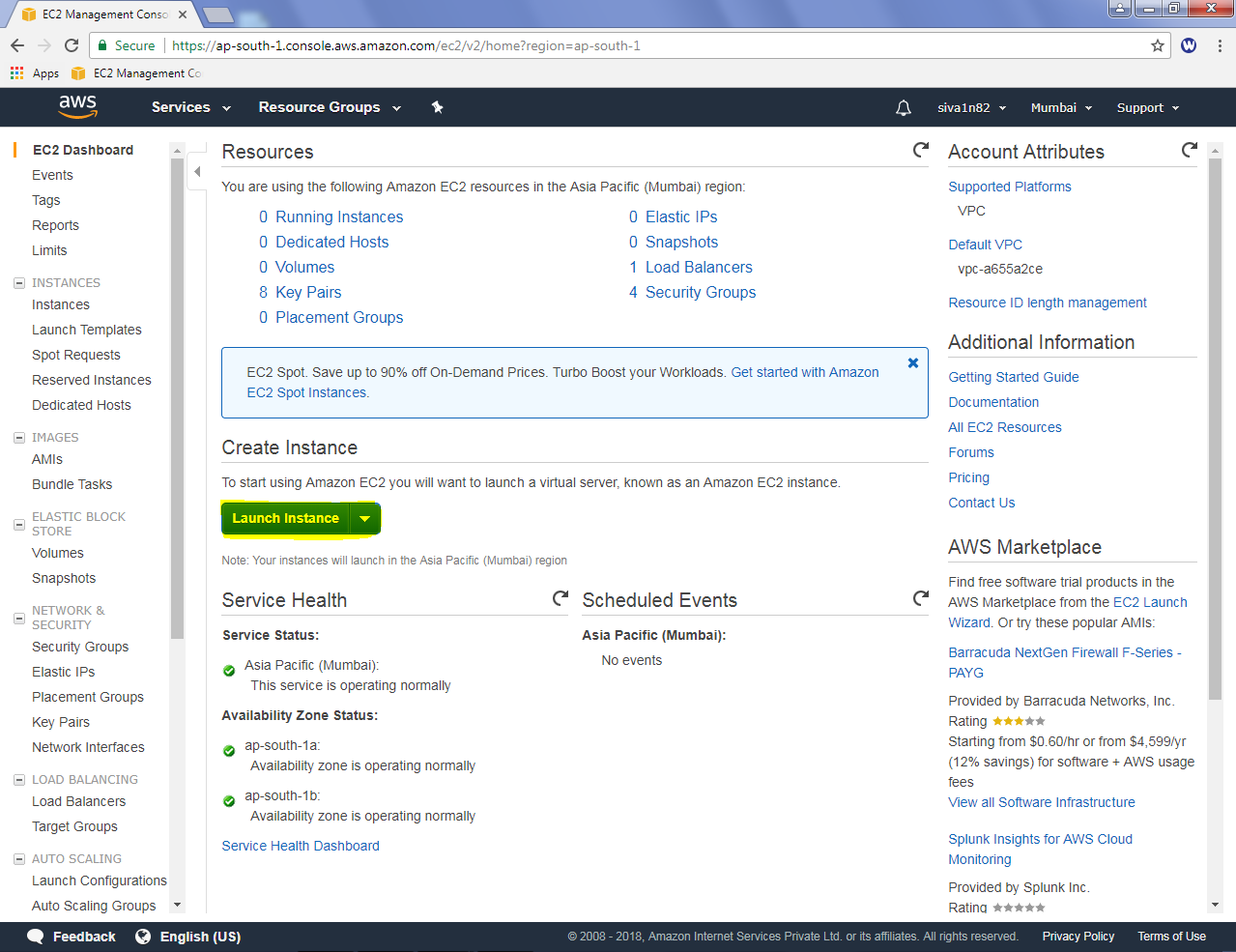


Select option check box option to select “sansbound\_VPC2\_Public\_subnet”.

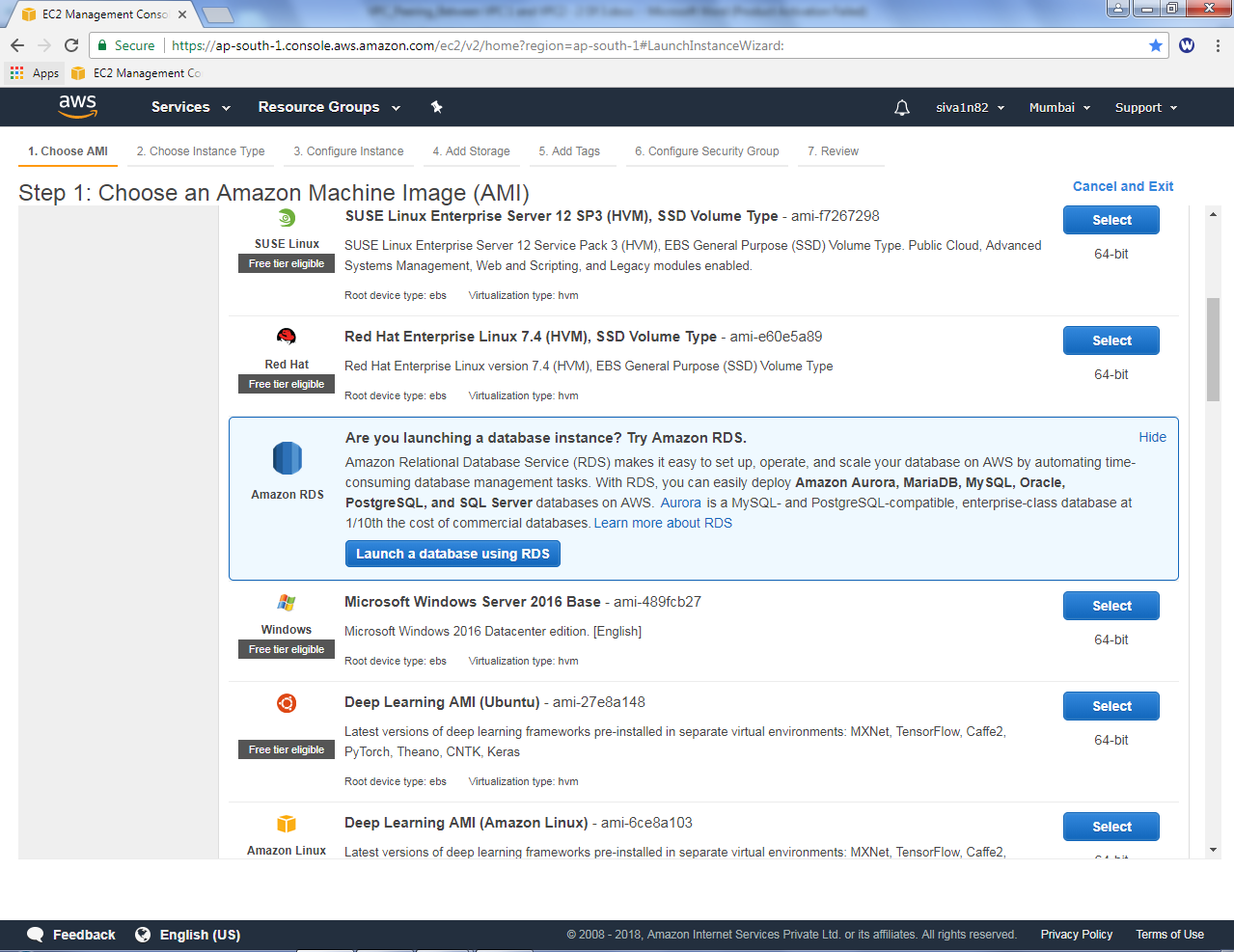


Then click “Save”.

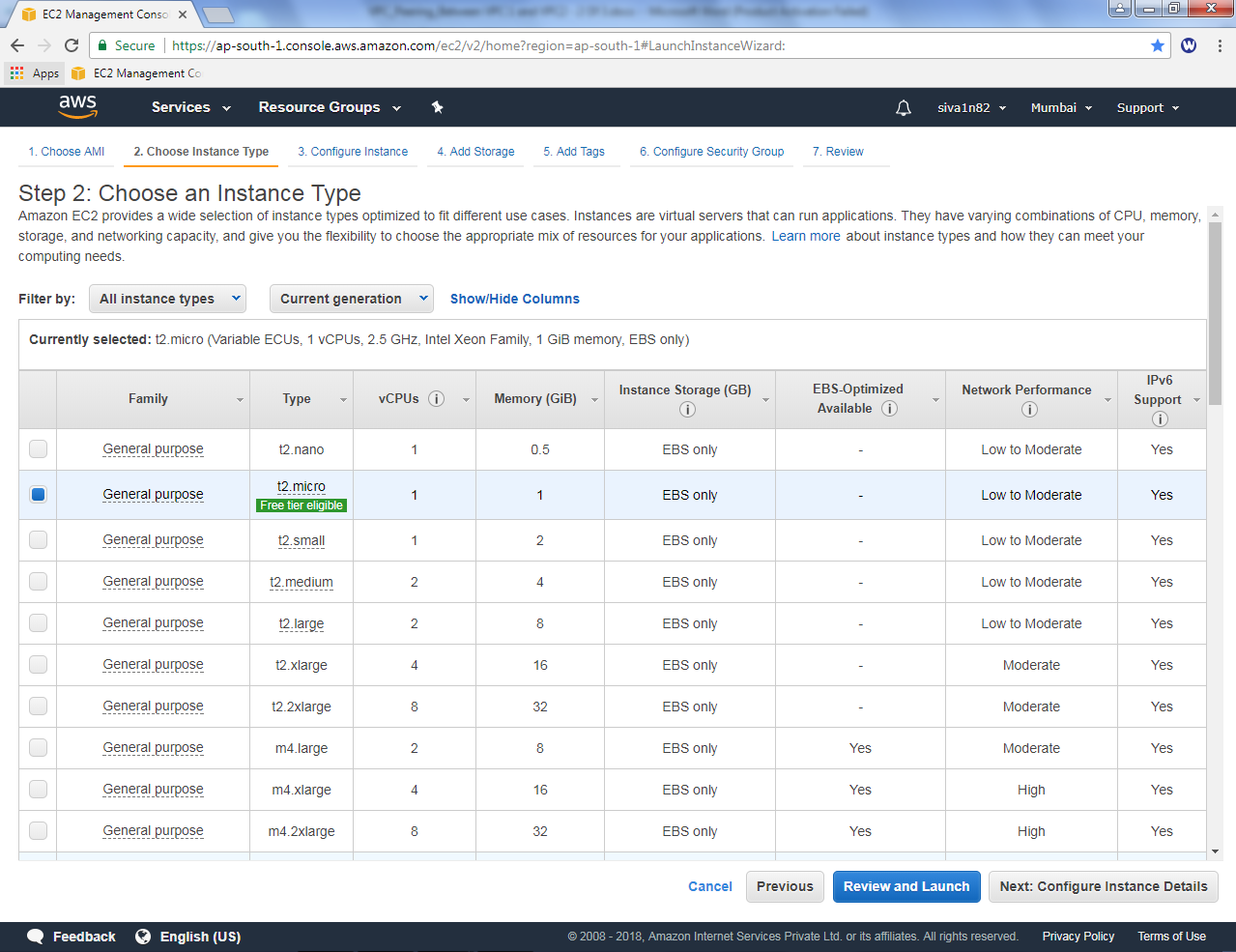
Then we need to create an instance for VPC2. Click “Launch Instance”.



Select “Microsoft Windows server 2016 Base “option.



Select “t2.micro”.

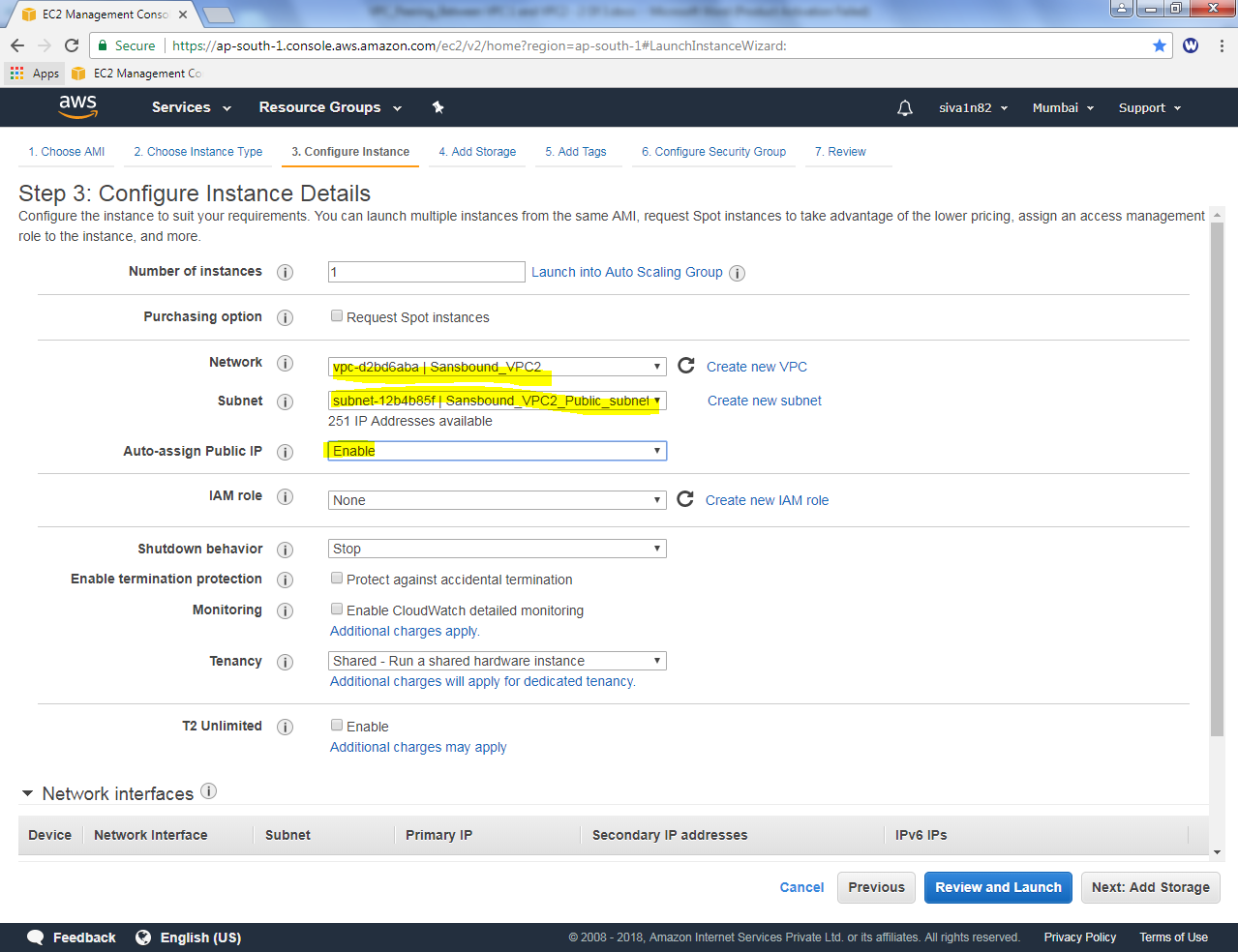


Click “Next”.

Select network as “Sansbound\_VPC2”

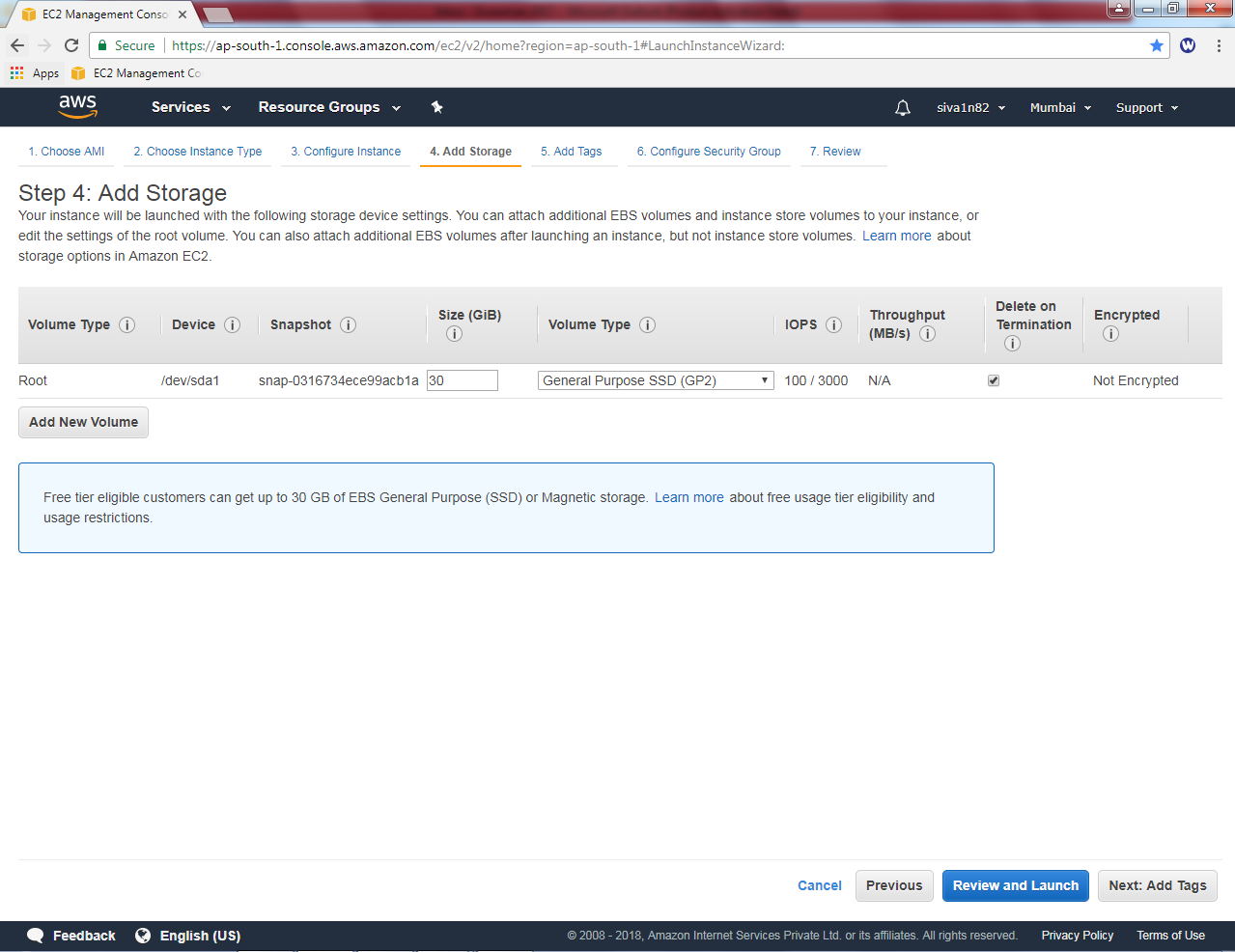
Select subnet as Sansbound\_VPC2\_public\_Subnet

Auto-assign Public IP: Enable

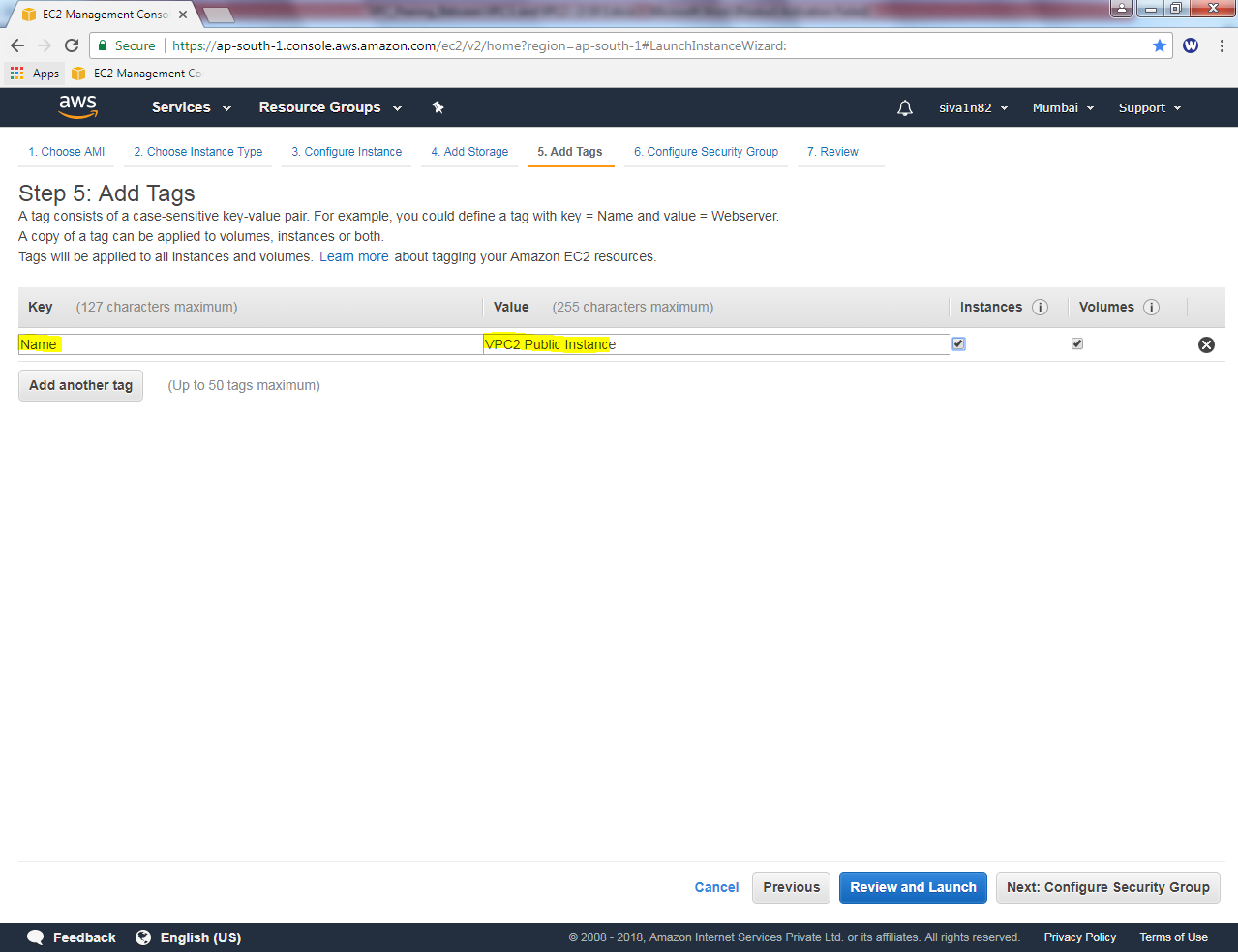


Click “Next”.

Leave default and click “Next”.

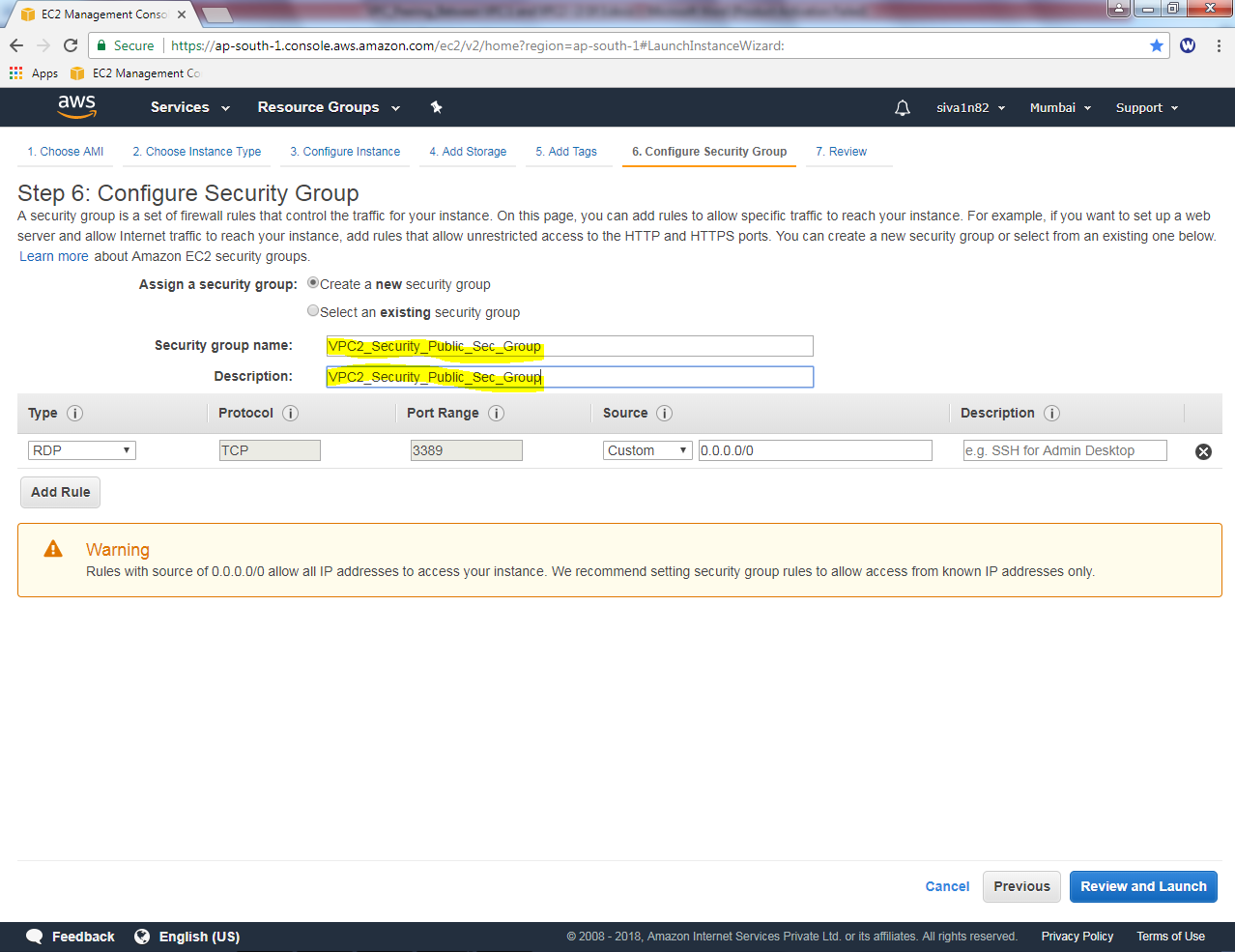


Type key as “name”and Value as VPC2 Public Instance.



Click “Next”.

Create a new security group as “VPC2\_Security\_Public\_Sec\_Group”. Allow RDP (3389 Port).



Click “Review and Launch”.

Click “Launch”.

