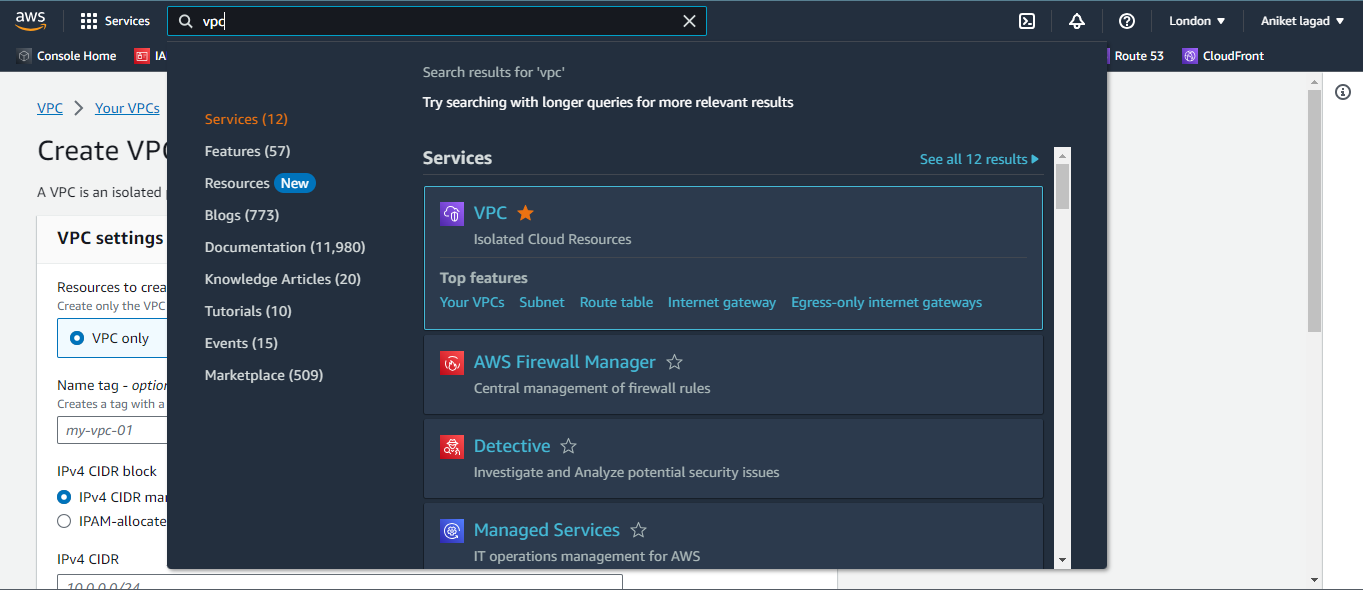
\*\*\*VPC TASK\*\*\*

Task: You've been tasked with setting up a VPC for a new project. The project requires an isolated network environment for security.

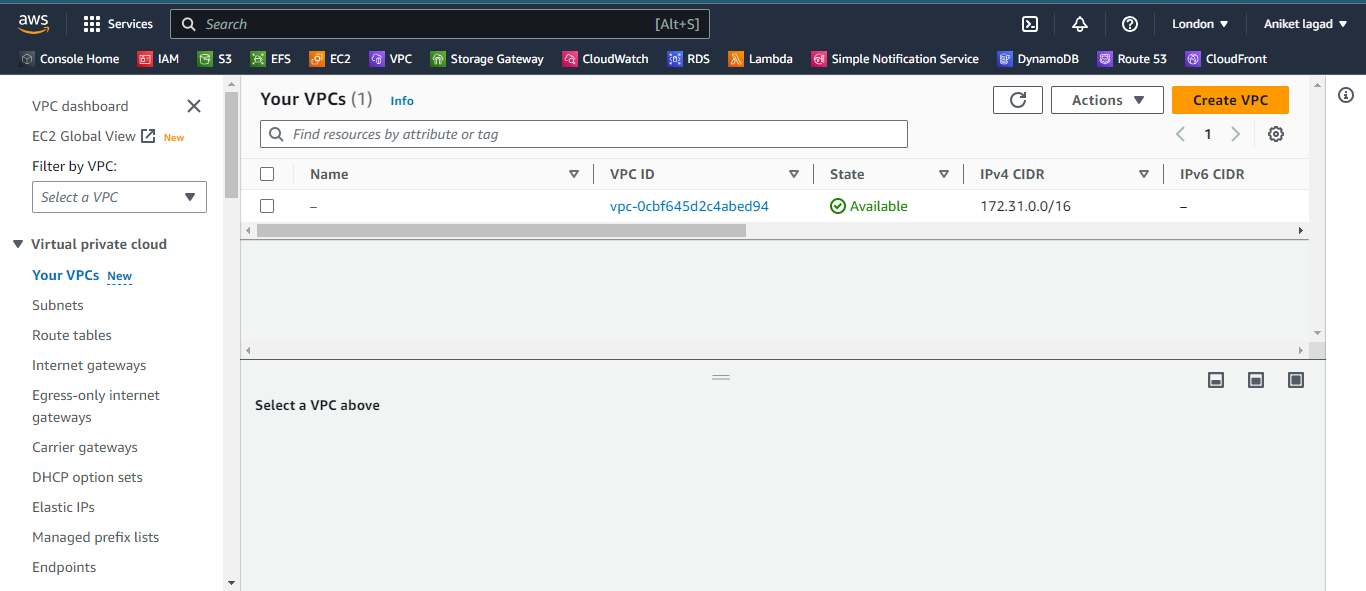
Action: Create a VPC named "ProjectVPC" with the IP address range 10.0.0.0/16.

🡺 step 1:- Login to aws account and go to vpc service .



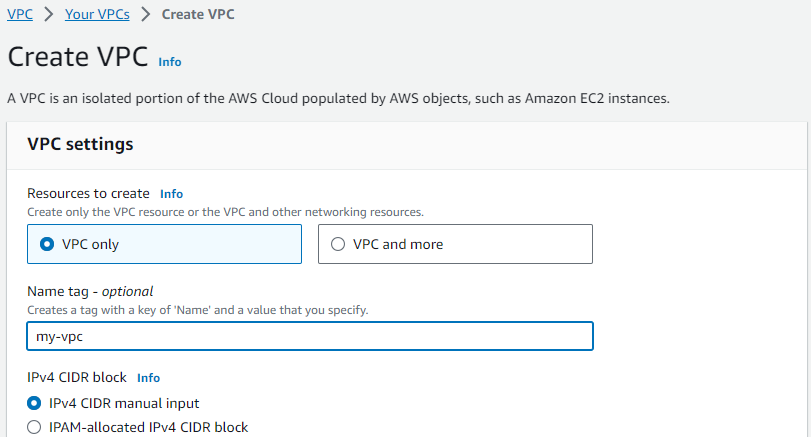
Step 2:-

Now click on vpc session and then click on create vpc.



Step 3:-

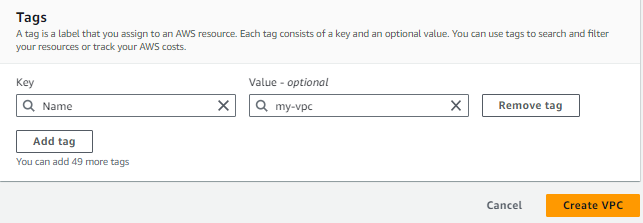
Now you have see the create vpc setting then select vpc only and then gave name it and select ipv4.



Step 4:-

Now gave ip address class I which class range you have to create subnet range. And then leave all as it is and then click click on create vpc. And your vpc was ready.





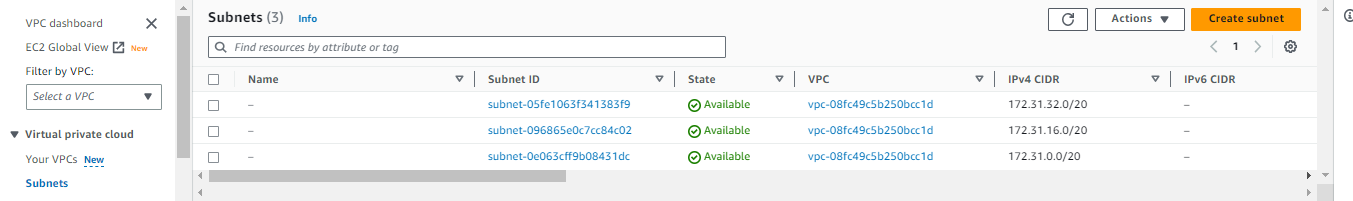
Scenario 2: Subnet Configuration

Task: Your application needs to be highly available, so you need to set up subnets across multiple availability zones within your VPC.

Action: Create three subnets – "SubnetA," "SubnetB," and "SubnetC" – each in a different availability zone, with IP address ranges 10.0.0.0/24, 10.0.1.0/24, and 10.0.2.0/24, respectively.

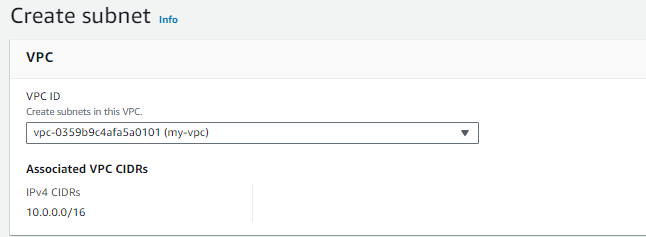
🡺

Step 1:-

now you have to create three subnets so click on subnet session and then click on create subnet.

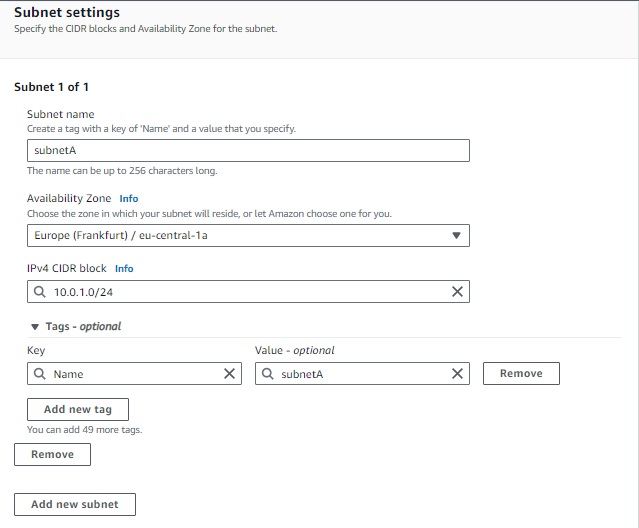
Step 2:-

And then you have see the vpc selecting column in that select your vpc and then scroll down.



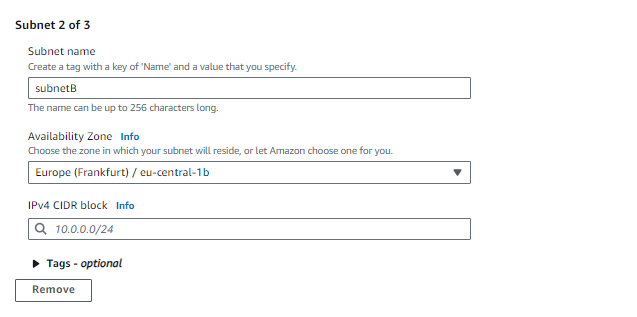
Step 3:-

And then gave first subnet name “subnetA” and then select one availability zone. Next you have to gave ip address range and then scroll down.



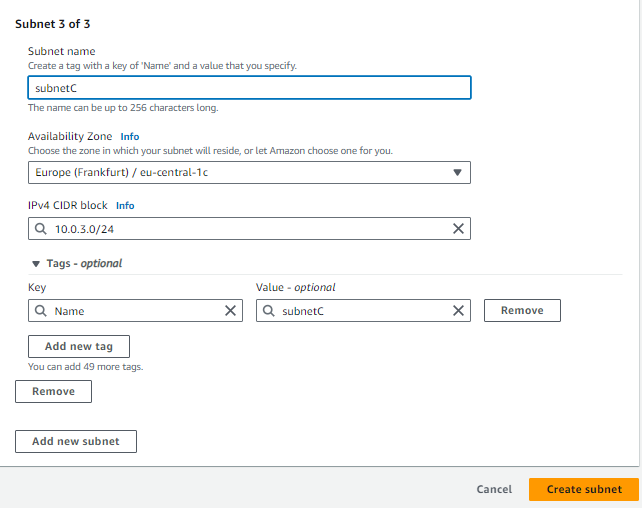
Step 4:-

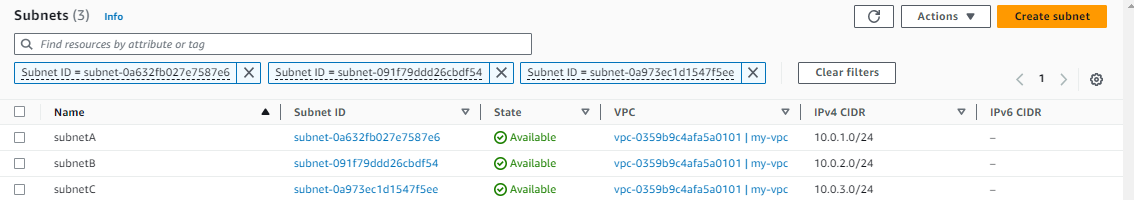
Now gave second subnet name “subnetB”. And then select availability zone and next you have to gave next ip range.and then scroll down.



Step 5:-

now gave 3rd subnet name and then select availability zone. After that gave next ip range to it. And click on create subnet. And your subnet was ready.





Scenario 3: Internet Gateway Setup

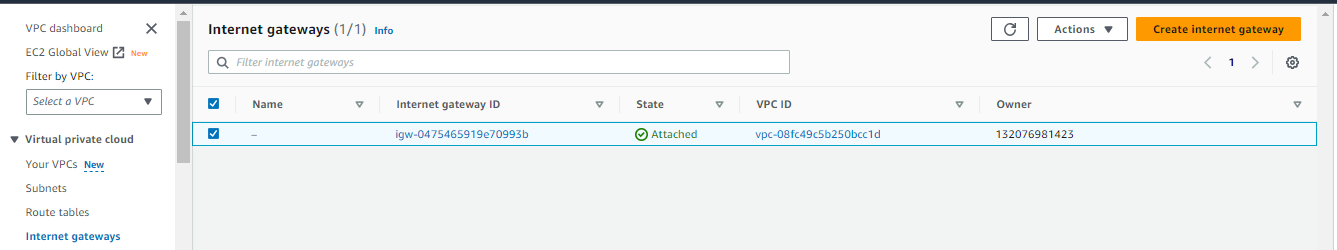
Task: Your application requires internet access for updates and external services.

Action: Attach an Internet Gateway to your VPC so that resources within it can communicate with the internet.

🡺

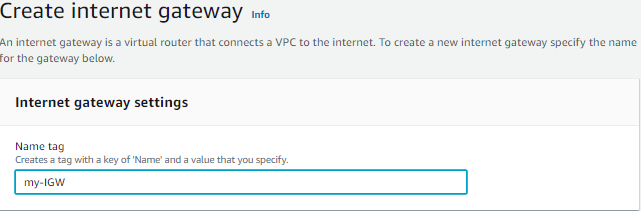
Step 1:-

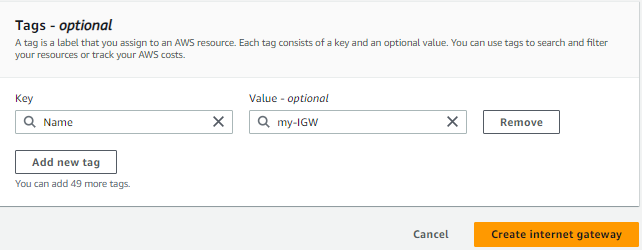
Now selct internet gateway session and then you have to click on create internet gateway.



Step 2:-

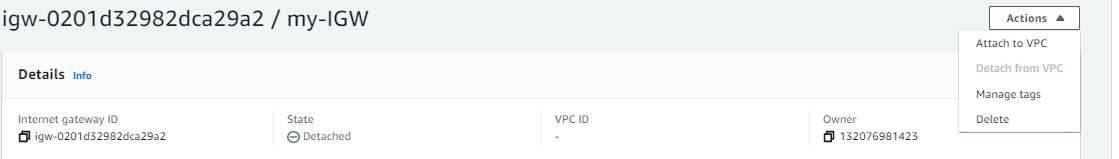
Now you have see the create internet gateway setting so gave your IGW and then leave all as it is and click on create internet gateway.

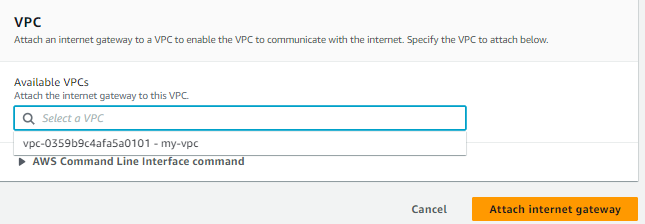




Step 3:-

Now click on your IGW and then click on actions and click on attach to vpc. After that select your vpc and click on attach internet gateway.





Scenario 4: Security Group Configuration

Task: You're launching a web server and a database server that should only communicate as needed. The web server should be accessible from anywhere on the internet, but the database server should only be accessible from the web server.

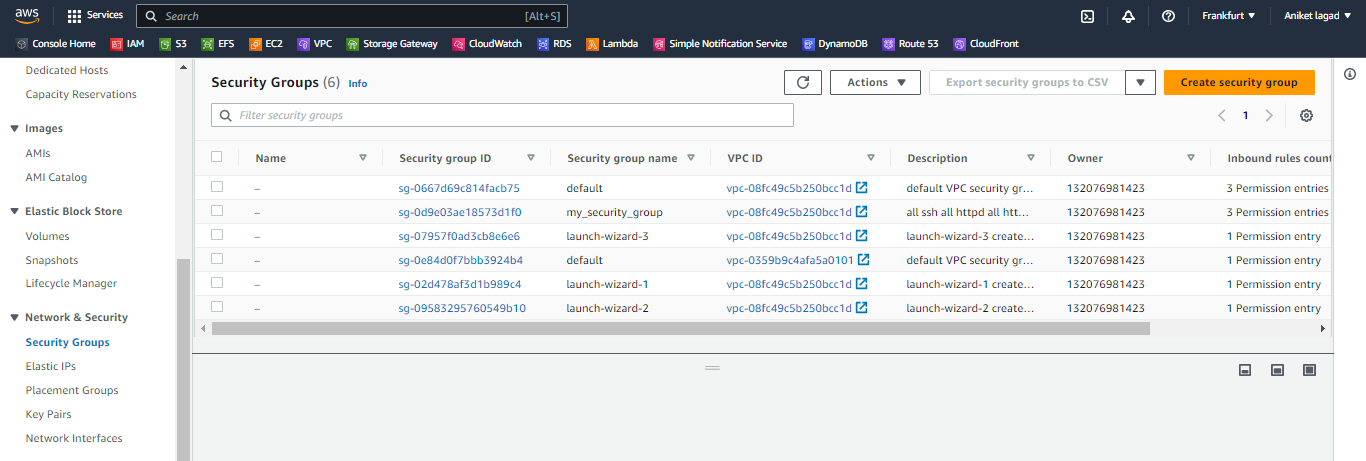
Action: Create a Security Group for the web server allowing incoming HTTP (port 80) and HTTPS (port 443) traffic from anywhere.

Create a Security Group for the database server allowing incoming traffic only from the Security Group of the web server on the database port (e.g., 3306 for MySQL).

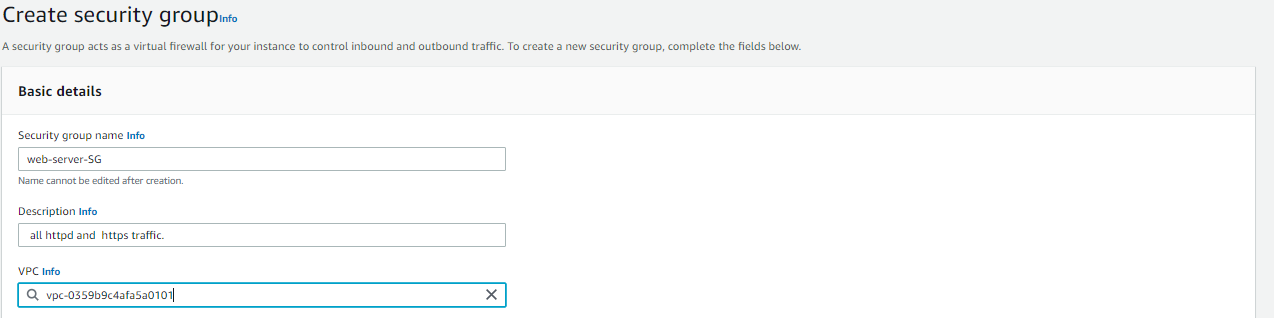
🡺

Step 1:-

Now you have to create security groups as mention in question for security base. So you have to go too ec2 service. So go to service and click on security group session and then click on create security group.

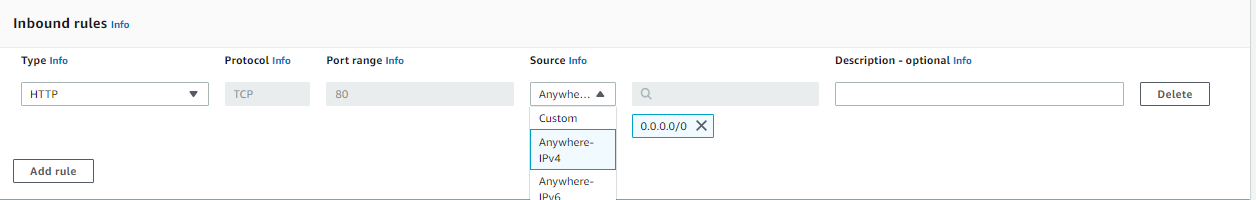


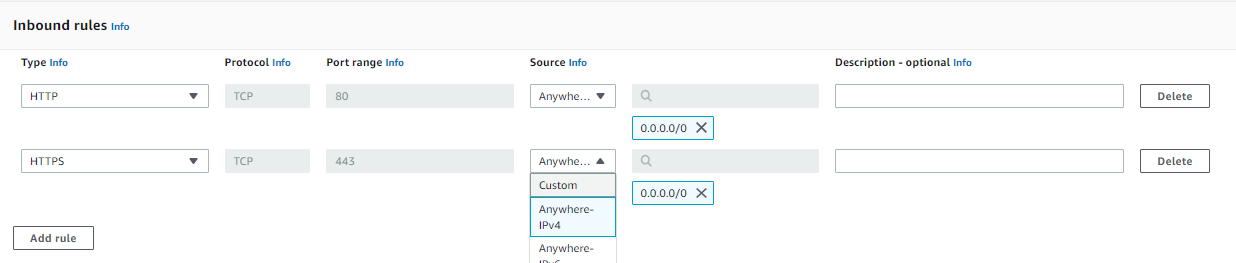
Step 2:-

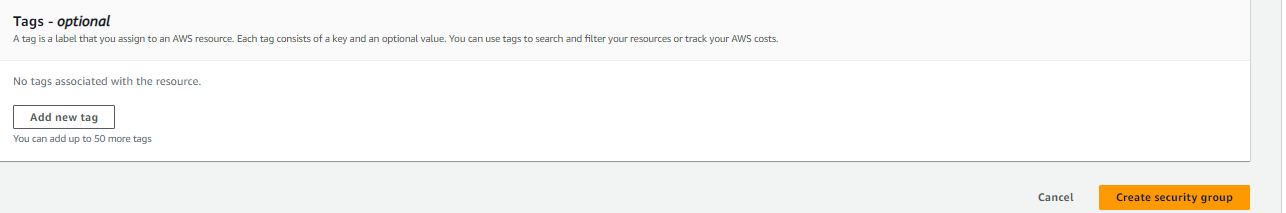
Now you see create security group setting so gave it name and then describe and next select your VPC. And after then scroll down. 

Step 3:-

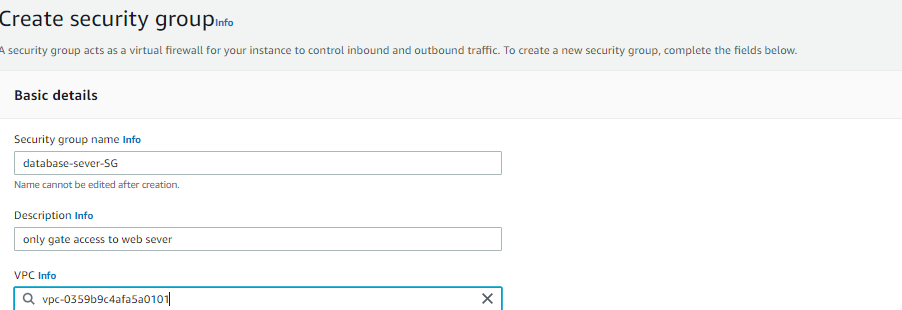
Now you have to select inbound rules so first add http service and port 80/tcp of it and then click on source and select anywhere ipv4. And then if you have to describe the describe. And next you have to add httpd service and port 443/tcp of it and then select anywhere ipv4 and as it is if you want describe it describe. And next you have click on create security group.





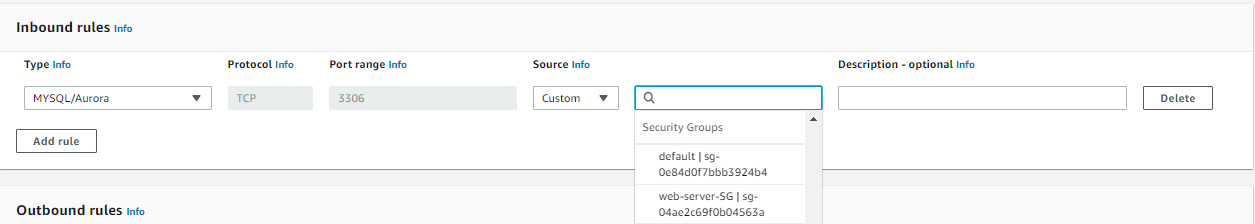


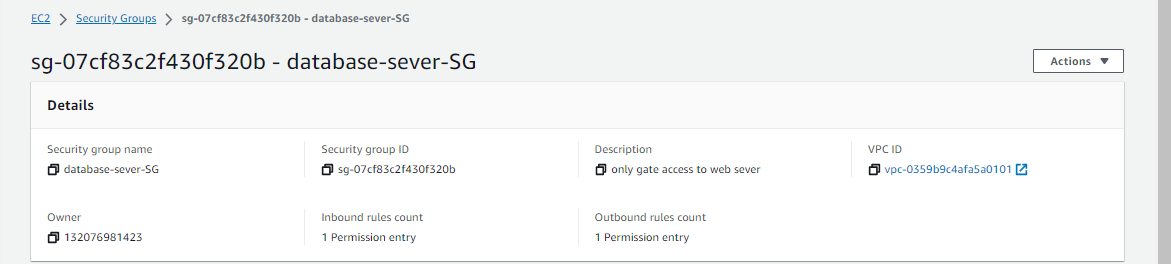
Step 4:-

Next you have to create 2nd security group for database server. So click on create SG and then gave name and gave description and after that select your vpc. Then scroll down. 

Step 5:-

Now select inbound rules of mysql service and port 3306 of it. And then gave describtion if you want next click on create security group. And your SG was ready to attach to web and database sever.





Scenario 5: Network ACLs

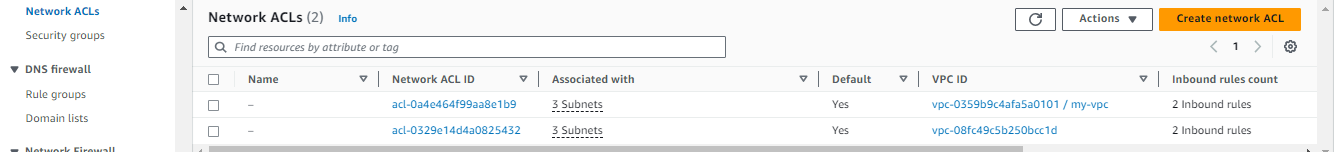
Task: Your company has strict security requirements. They want to control inbound and outbound traffic at the subnet level.

Action: Configure a Network ACL for "SubnetA" that allows incoming HTTP traffic (port 80) and outgoing SSH traffic (port 22), but blocks all other inbound and outbound traffic.

🡺

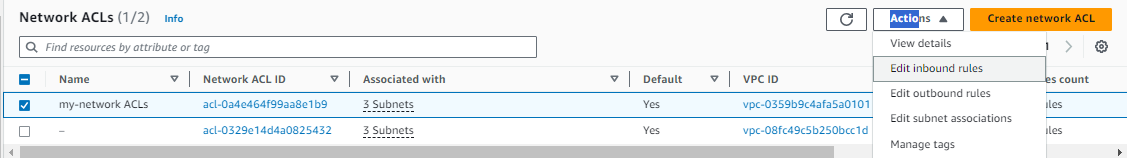
Step 1:-

First we have to go vpc service and then go to network ACL. You have see there created network ACl which associated with your vpc subnets.

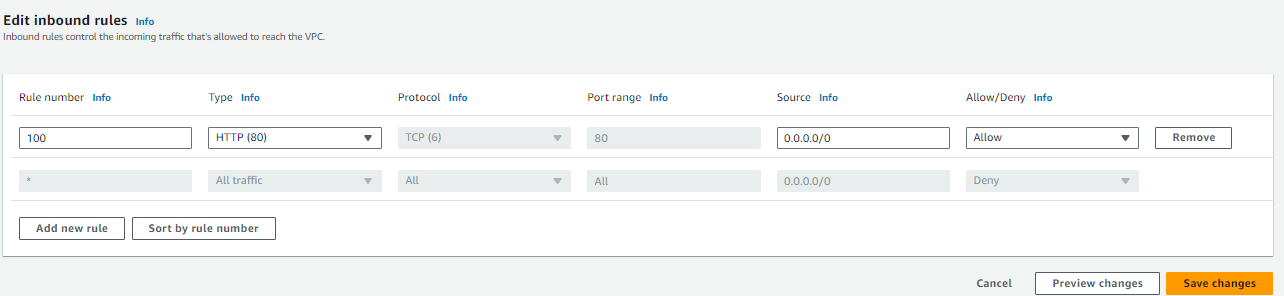


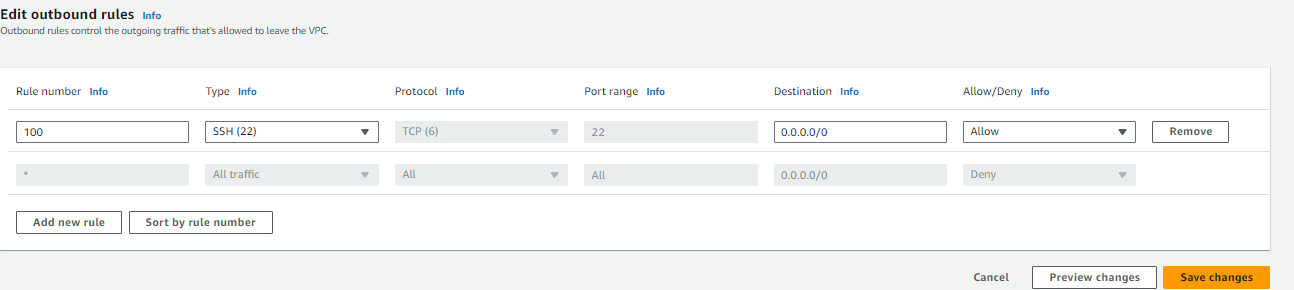
Step 2:-

Now you have to select your network ACLs and then click on actions and then click on edit inbound rules option.



Step 3:-

Then you have see the information of edit inbound rule so you have to only change type httpd(80) and then click on save change. And then select oout bond rules and then select in type ssh(22) and save changes. 



Scenario 6: Route Table Management

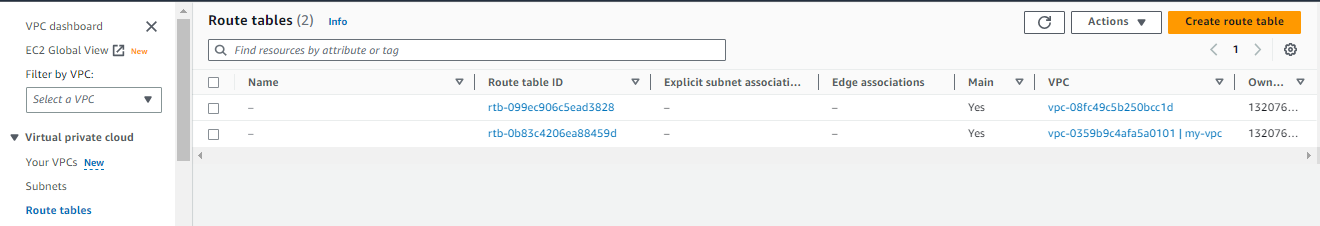
Task: You have multiple subnets, and you want to ensure traffic flows correctly between them.

Action: Create a custom route table named "ProjectRouteTable" and associate it with "SubnetB." Add a route to direct traffic destined for the internet (0.0.0.0/0) through the Internet Gateway.

🡺

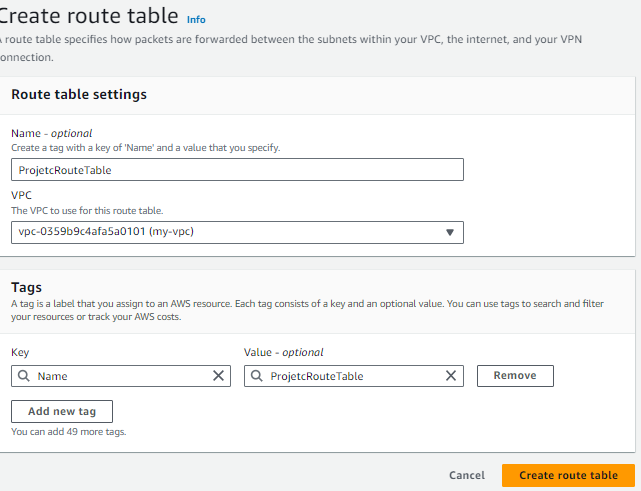
Step 1:-

You have to go route table session to create route table named “ProjectRouteTable”. And click on create route table option.



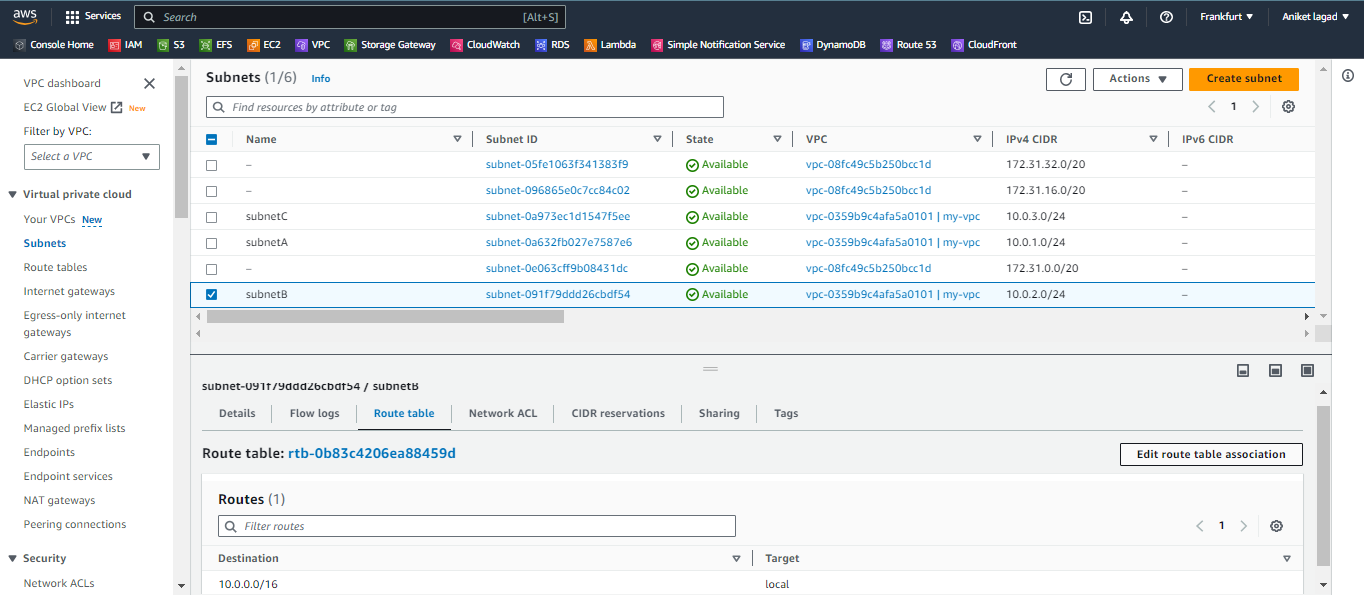
Step 2:-

Now you see the create route table setting so gave it name as ProjectRouteTable and then select your VPC. And click on create route table .



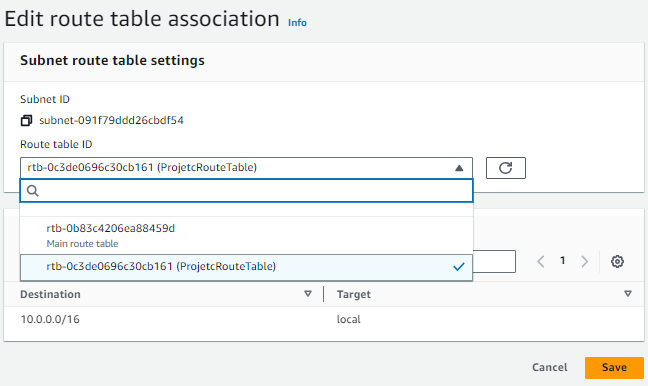
Step 3:-

Now you have associate the route table to subnet named as “subnetB”. So go to subnet session and select subnetB and then click on route table option and then click on edit route table association.



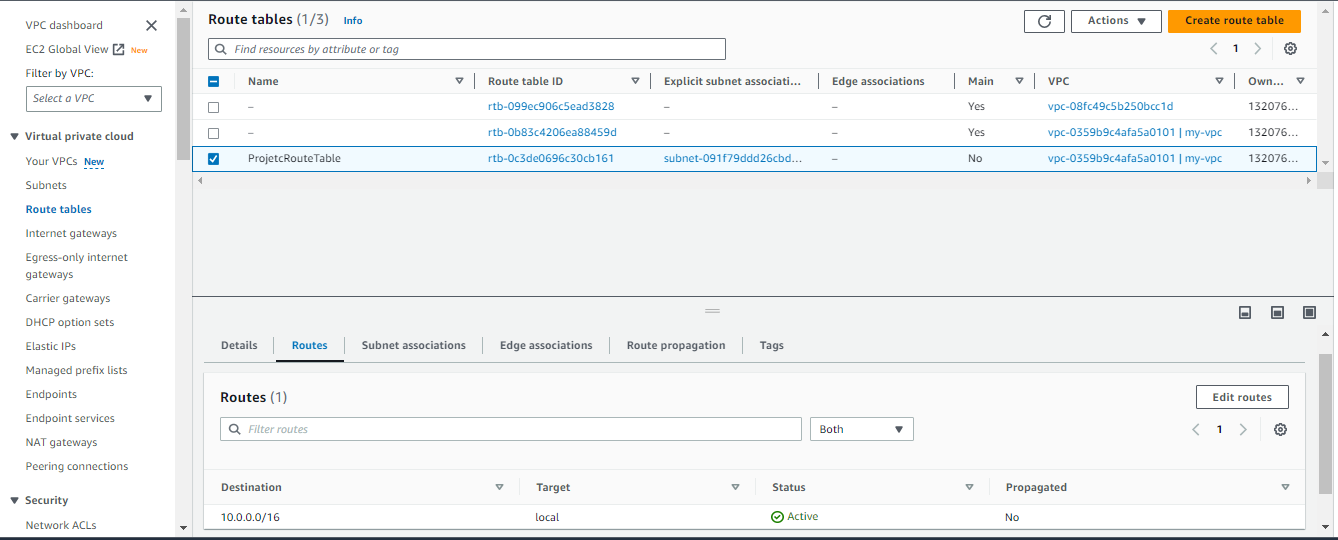
Step 4:-

Now you see the subnet route table settings so select your route table and then save it.



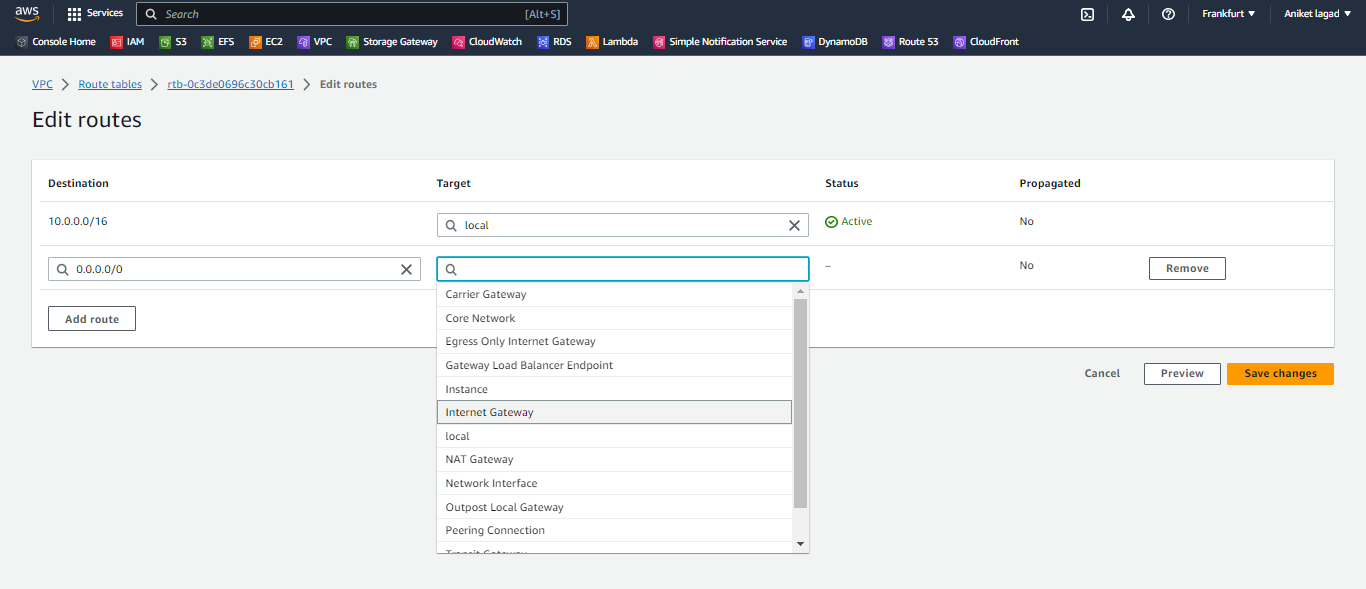
Step 5:-

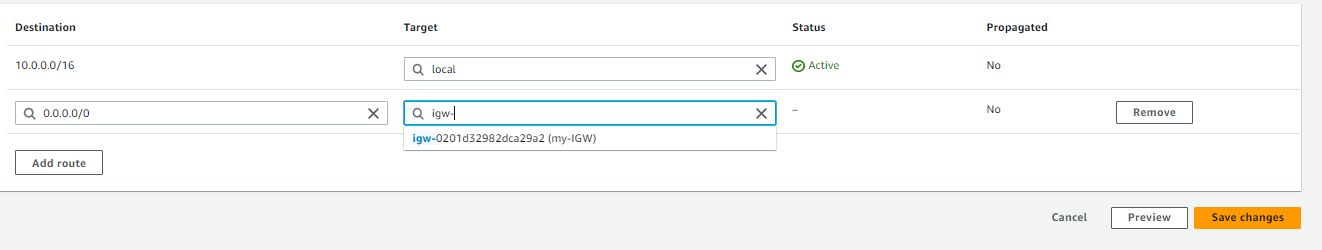
Now you have to attach IGW to route table so your instance get access of internet. So go to route table session and then click on your route table named as ProjectRouteTable and then click on edit routes.

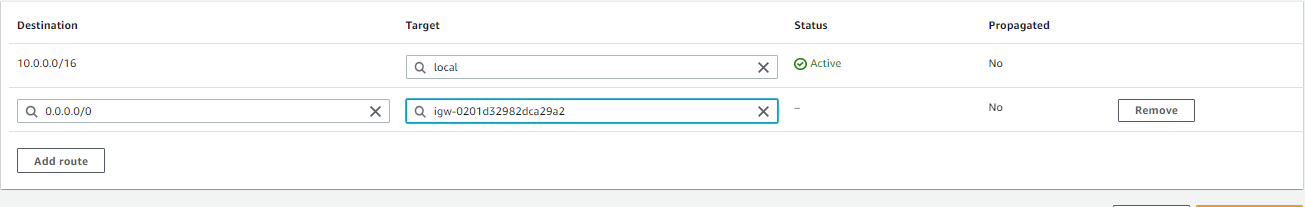


Step 6:-

Now see the edit route setting so click on add route and then select 0.0.0.0/0 destination and then click on target and then select internet gateway option and then select your IGW. And then click save changes.







Scenario 7: VPN Connection

Task: Your company needs a secure connection between its on-premises network and the VPC for data exchange.

Action: Set up a VPN Connection between your VPC and your company's on-premises network. Configure the necessary parameters like VPN tunnel endpoints and security settings.