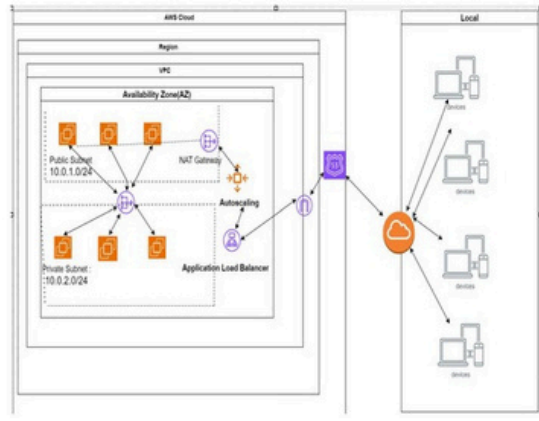


# Networking and Security in Cloud(Project)

Diagram:-

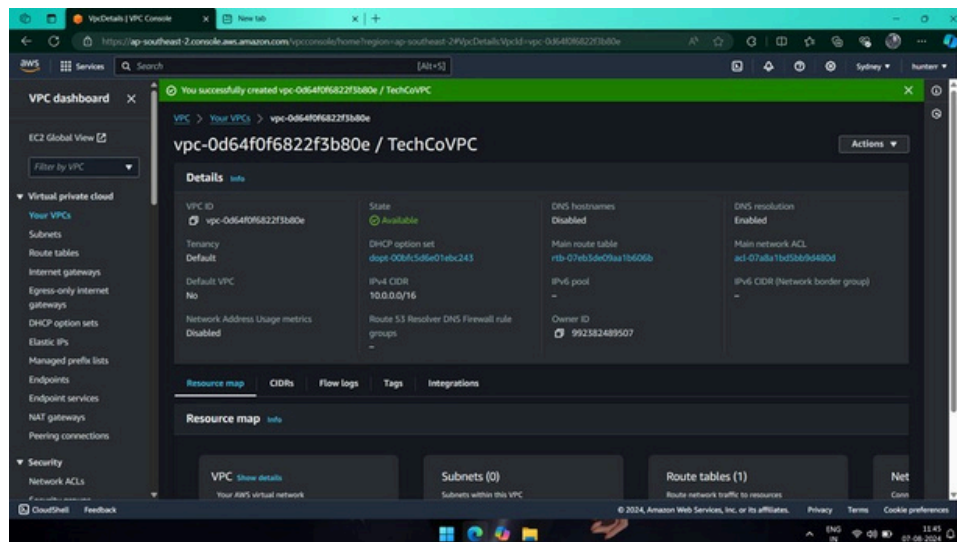


## Objectives:-

- Design a VPC architecture that meets the requirements of the organization's applications and services.
- Configure subnets within the VPC to logically isolate different components and control traffic flow.
- Implement security measures such as security groups and network ACLs to control inbound and outbound traffic.
- Establish connectivity to the internet gateway and enable secure communication with external resources.
- Ensure high availability and fault tolerance by distributing resources across multiple availability zones

## Task 1: VPC and Subnet Setup

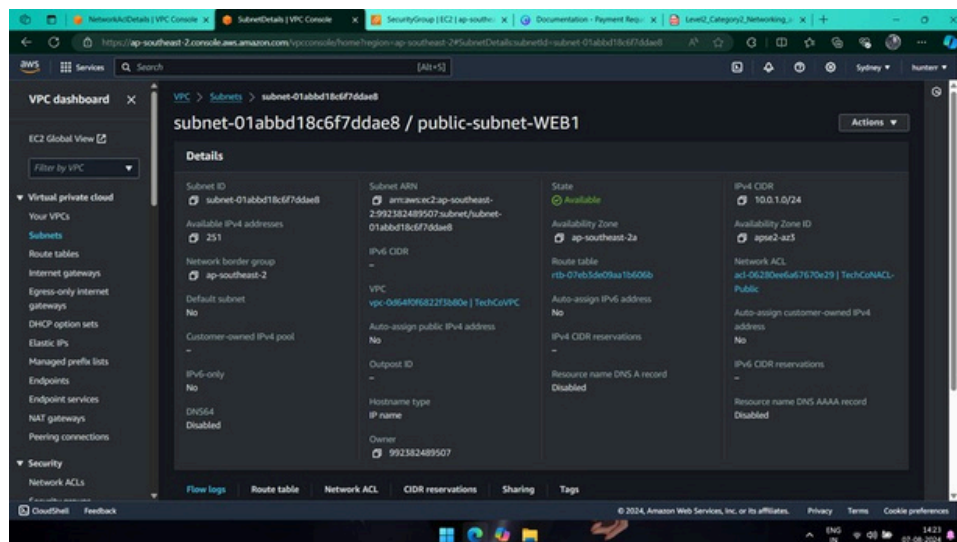
Step 1:- Create a VPC named "TechCoVPC" with CIDR block 10.0.0.0/16.



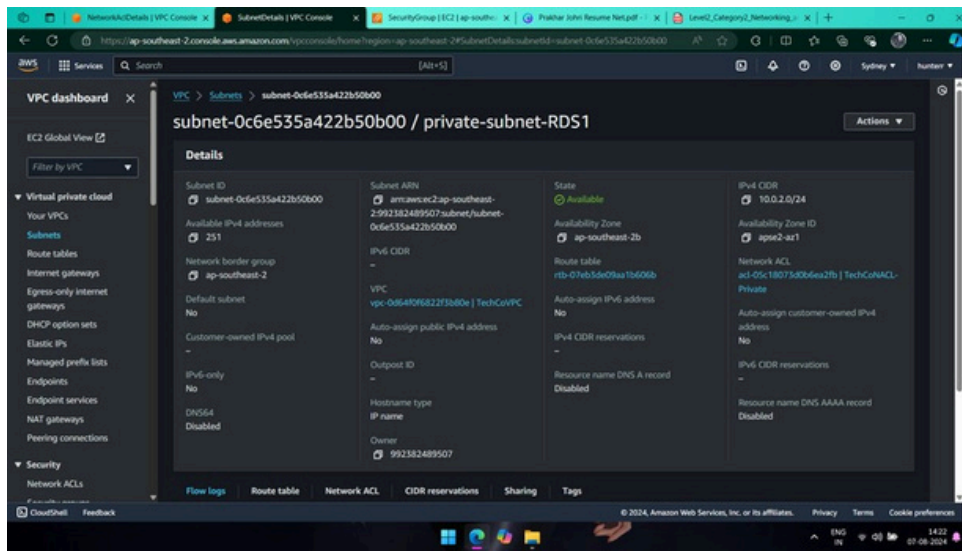
Step 1:- Created a VPC named "TechCoVPC".

## Task 1.2:- Create two subnets:

- Step 1.2.1:- Public Subnet: 10.0.1.0/24 (for web servers)
- Step 1.2.2:- Private Subnet: 10.0.2.0/24 (for database servers)



Step 1.2.1:- Created a Public Subnet.

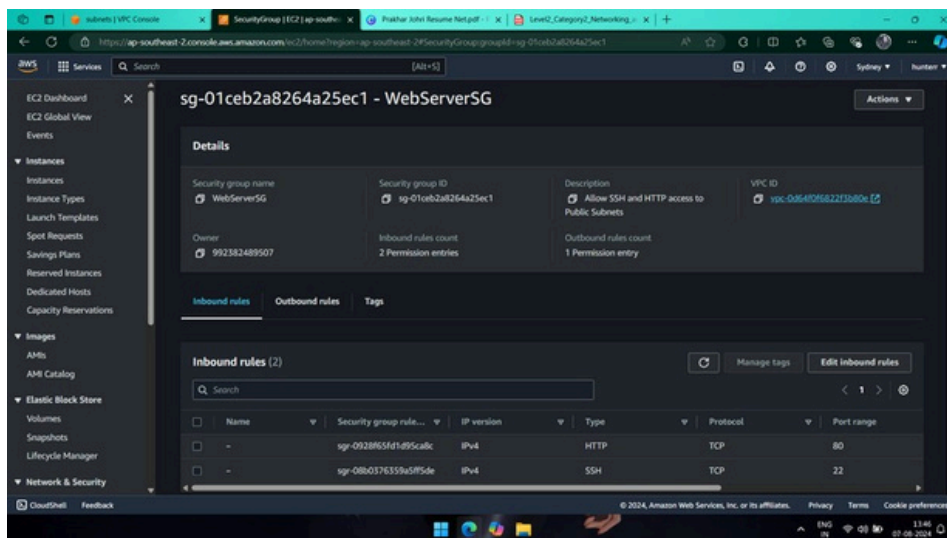


Step 1.2.2:- Created a Private Subnet.

## Task 2: Security Configuration

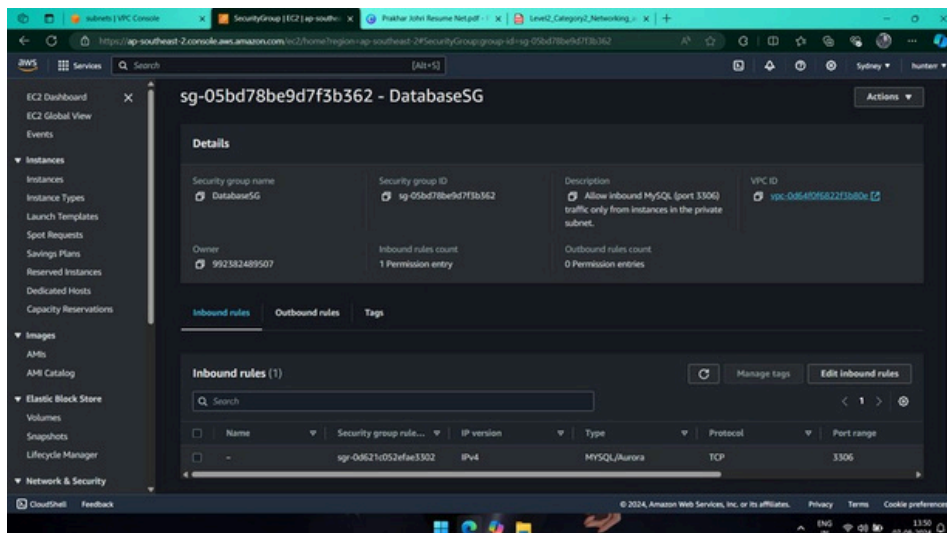
### Configure Security Groups:

**Step 1:- “WebServerSG”:** Allow inbound HTTP (port 80) and SSH (port 22) traffic from the internet to instances in the public subnet.



Step 1:- Created a Security Group named “WebServerSG” with ports 80 and 22 as allowed ports.

**Step 2:- “DatabaseSG”:** Allow inbound MySQL (port 3306) traffic only from instances in the private subnet.

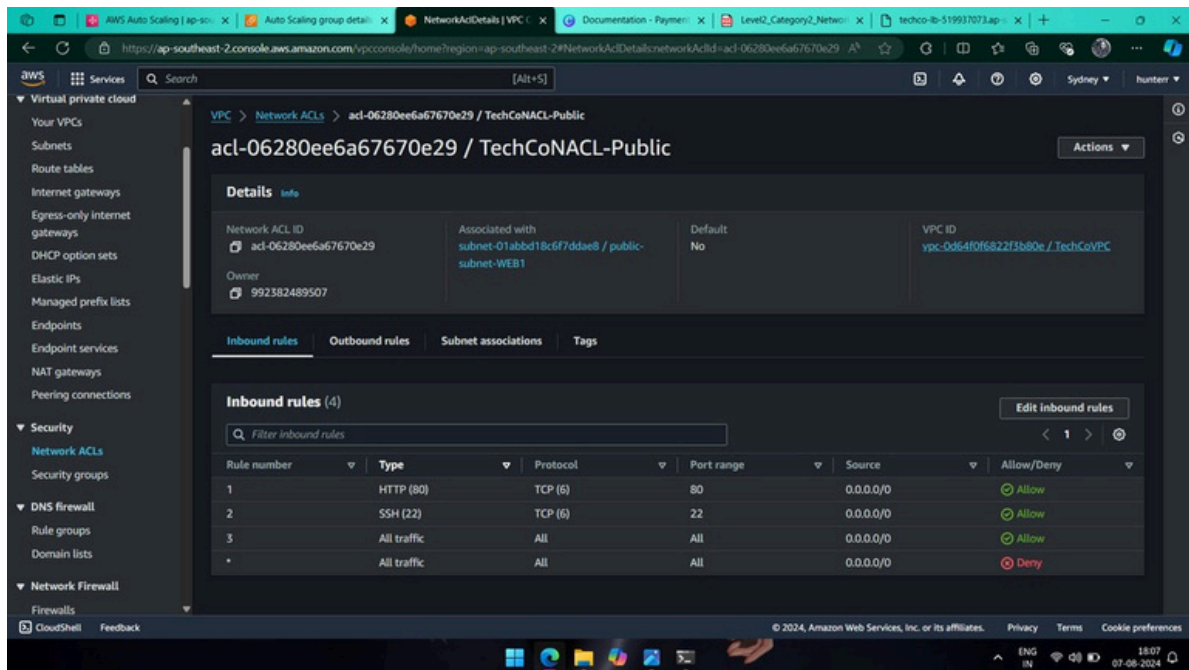


Step 2:- Created a Security Group named “DatabaseSG” with port 3306 as allowed port.

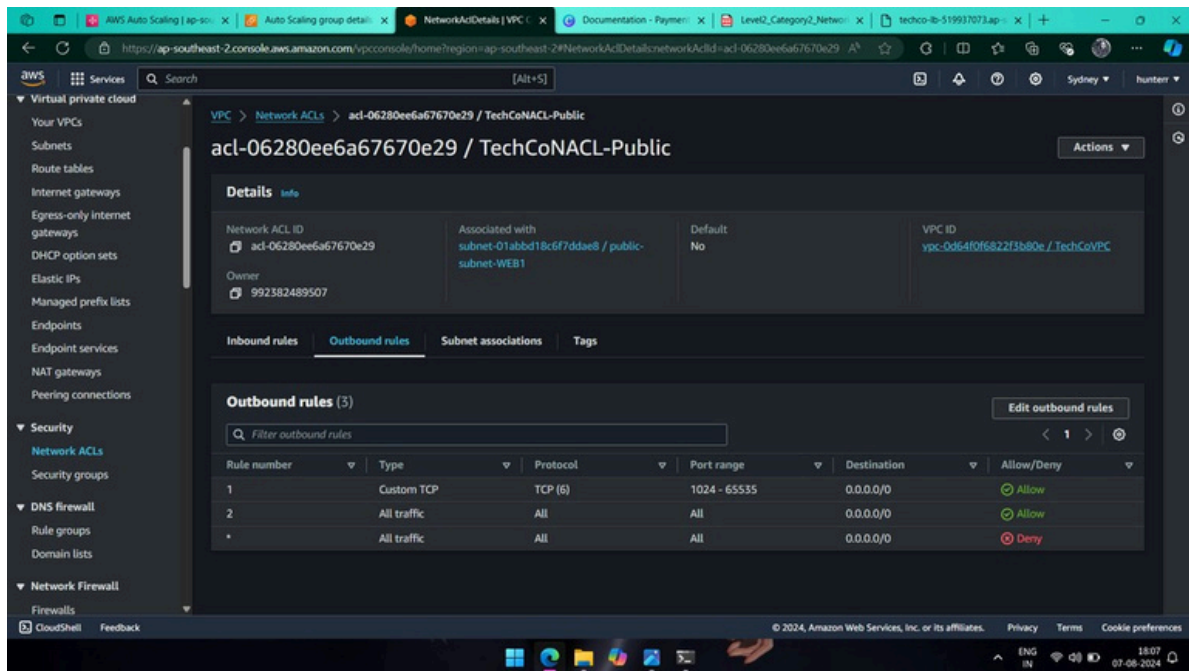
## Configure Network ACLs:

### Step 3:- For Public Subnet -

- Inbound: Allow HTTP (80) and SSH (22).
- Outbound: Allow all
- NACL Range : Open from 1024-65535



Step 3.1:- Created inbound rules for allowing port 80 and SSH.

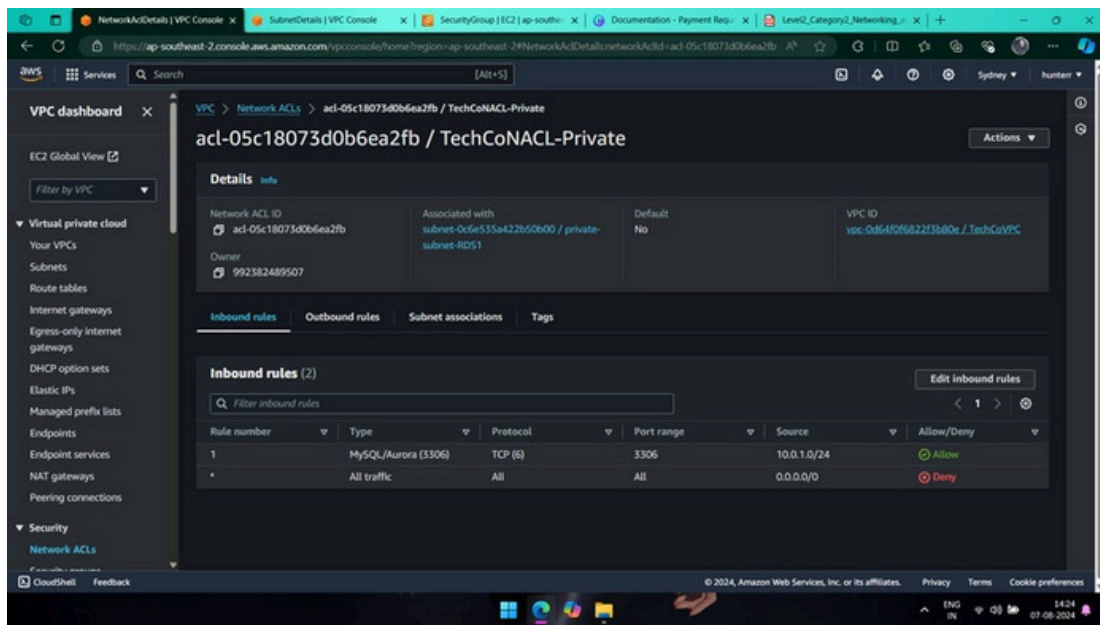


Step 3.1:- Created outbound rules for allowing port range from 1024 to 65535 and all traffic.

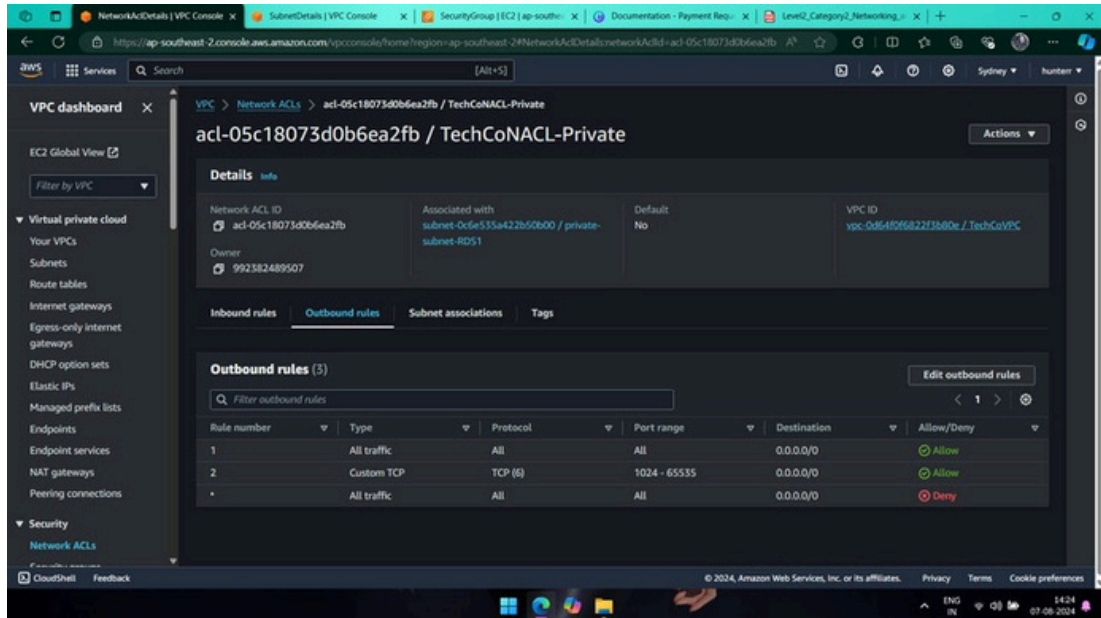
### Step 4:- For Private Subnet -

- Inbound: Allow MySQL (3306) from public subnet.
- Outbound: Allow all.
- NACL Range : Open from 1024-65535





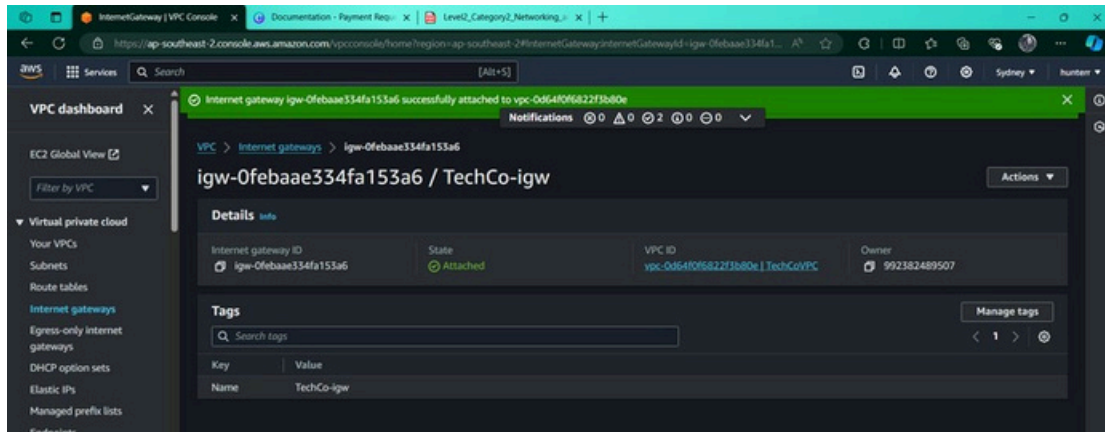
Step 4.1:- Created inbound rules for allowing port 3306.



Step 4.2:- Created outbound rules for allowing port range from 1024 to 65535 and all traffic.

## Task 3: Internet Connectivity

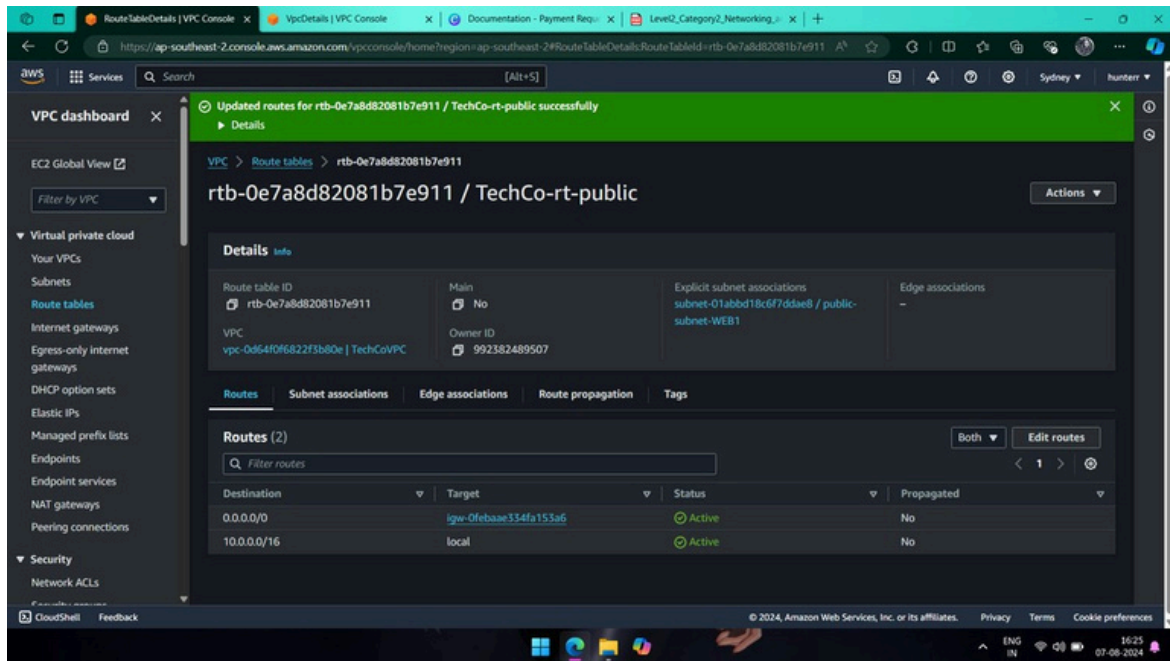
### Step 1:- Attach an Internal Gateway to the VPC “TechCoVPC”



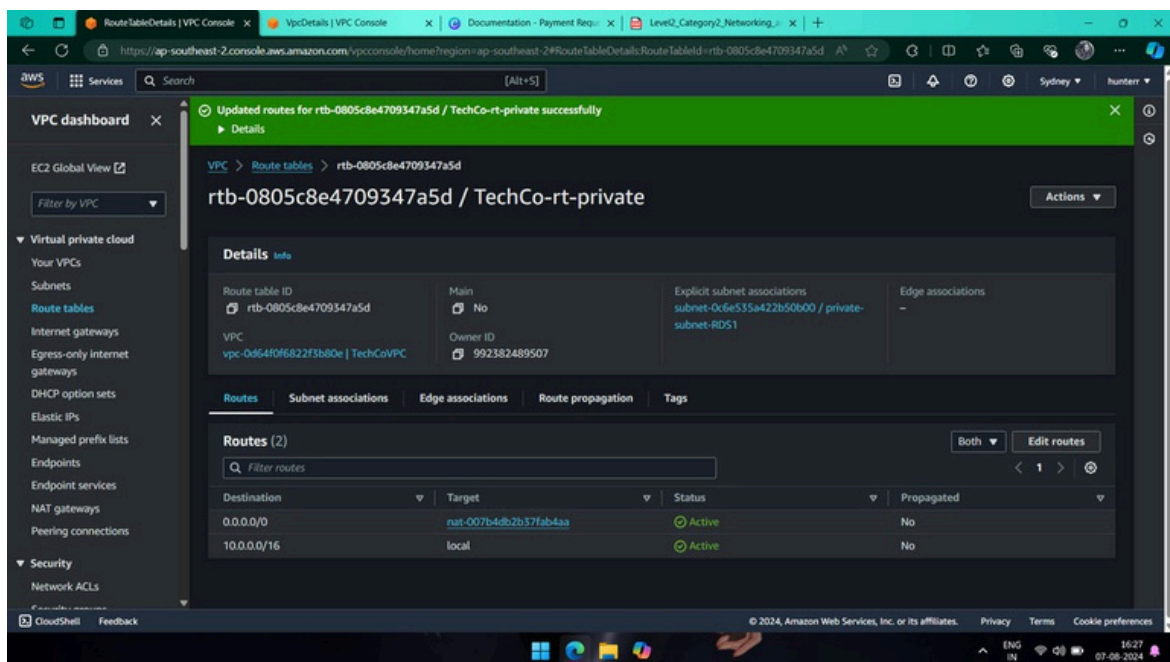
Step 1:- Attached an internet gateway for our VPC.

## Step 2:- Update route tables -

- Step 2.1:- Direct public subnet traffic to the Internet Gateway.
- Step 2.2:- Keep private subnet routes internal or through a NAT Gateway for outbound access.



Step 2.1

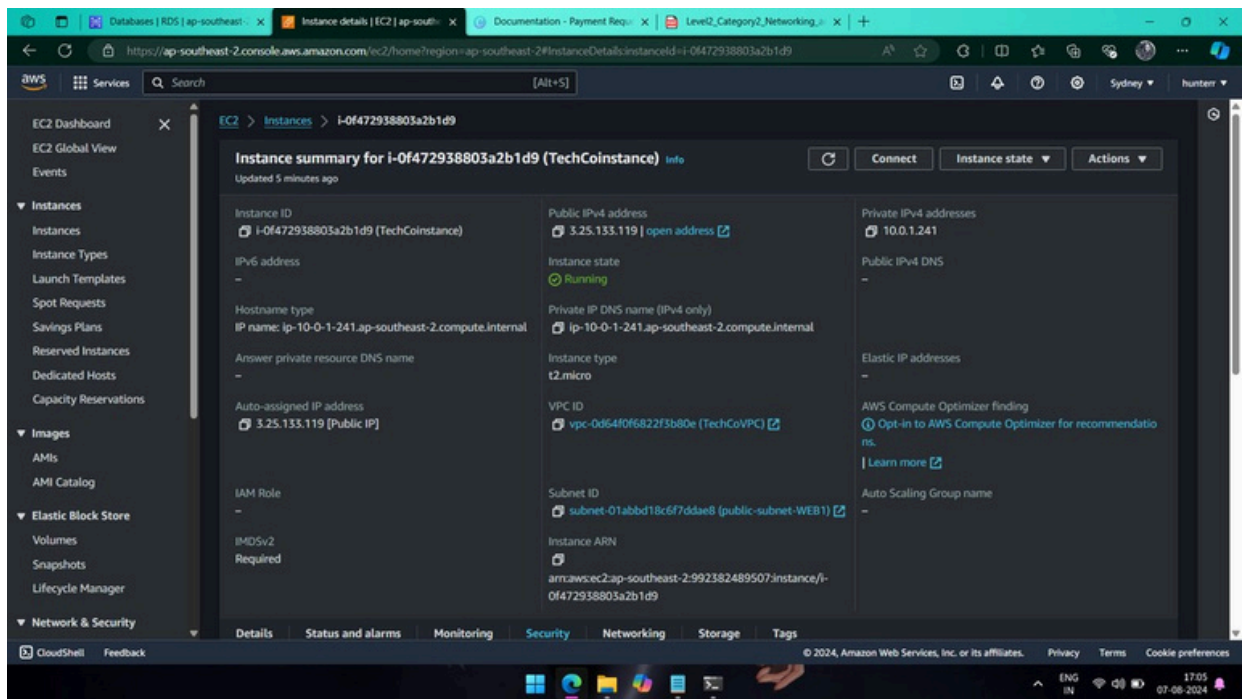


Step 2.2

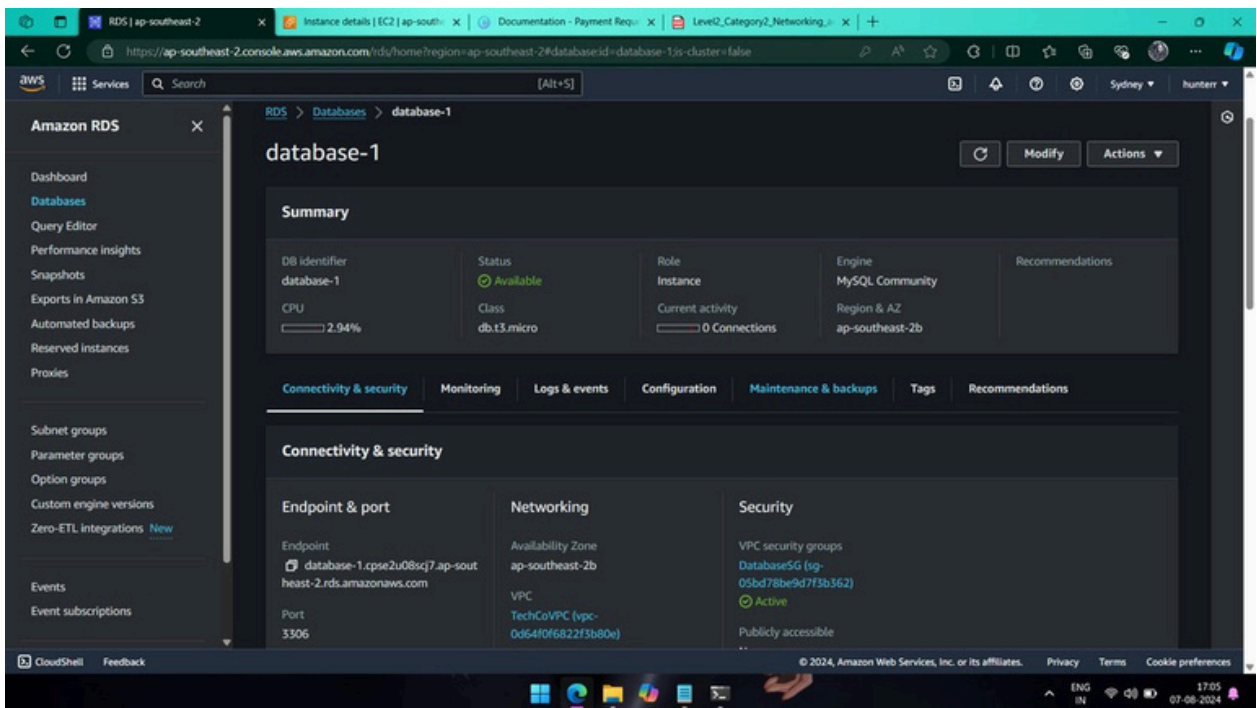
## Task 4: Application Deployment

### Step 1:- Launch EC2 instances:

- Step 1.1:- Deploy web server instances (e.g., Amazon Linux) in the public subnet.
- Step 1.2:- Deploy database server instances (e.g., Amazon RDS MySQL) in the private subnet.



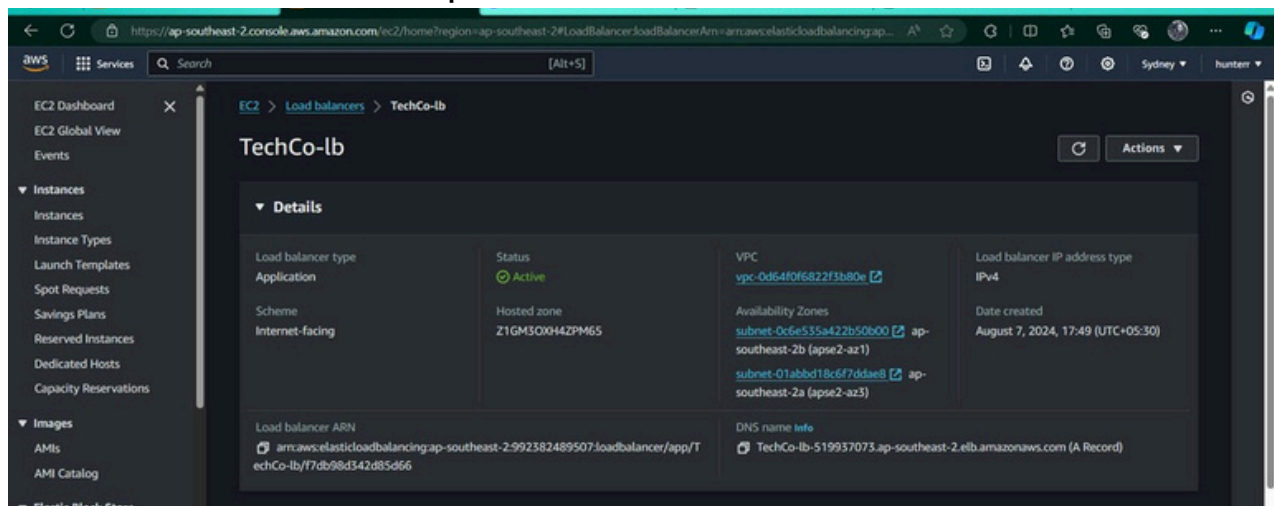
Step 1.1



Step 1.2

## Step 2:- Set up Application Load Balancer (ALB):

- Configure ALB to distribute incoming HTTP traffic across web server instances in multiple AZs.



Step 2