# Basic Networking Topology Implementation

Design and implement a basic networking topology:

➢ Set up two VMs with private IPs.

➢ Configure one VM as a web server and the other as a client.

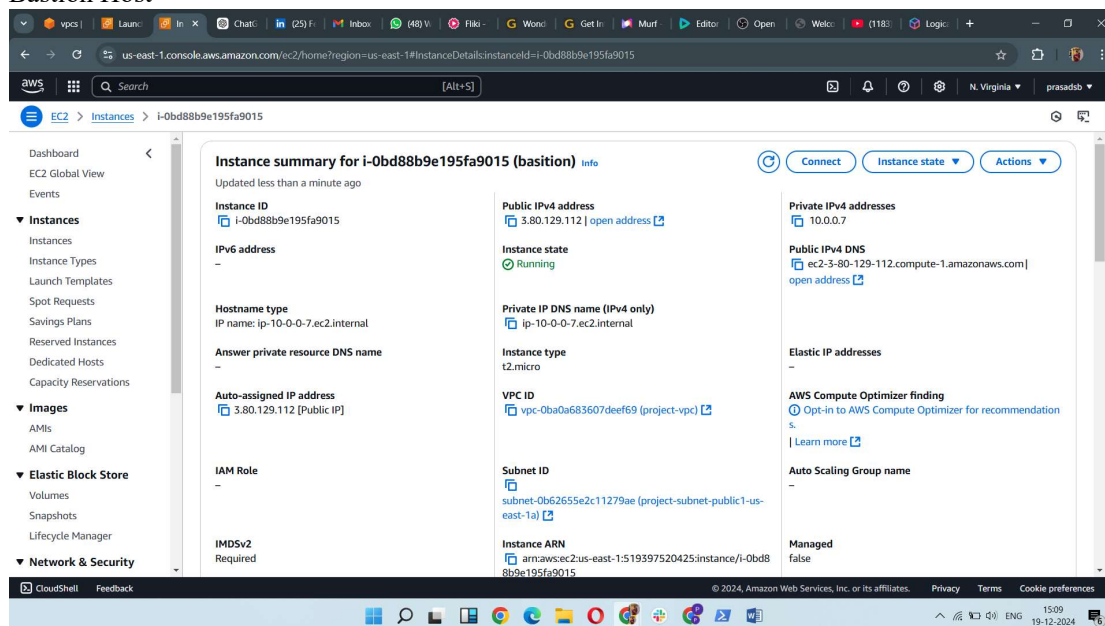➢ Use SSH to securely transfer files between them.

I created the Virtual private cloud (VPC) with 1 public subnet and 1 private subnet to ensure network isolation and secure communication between the instances.
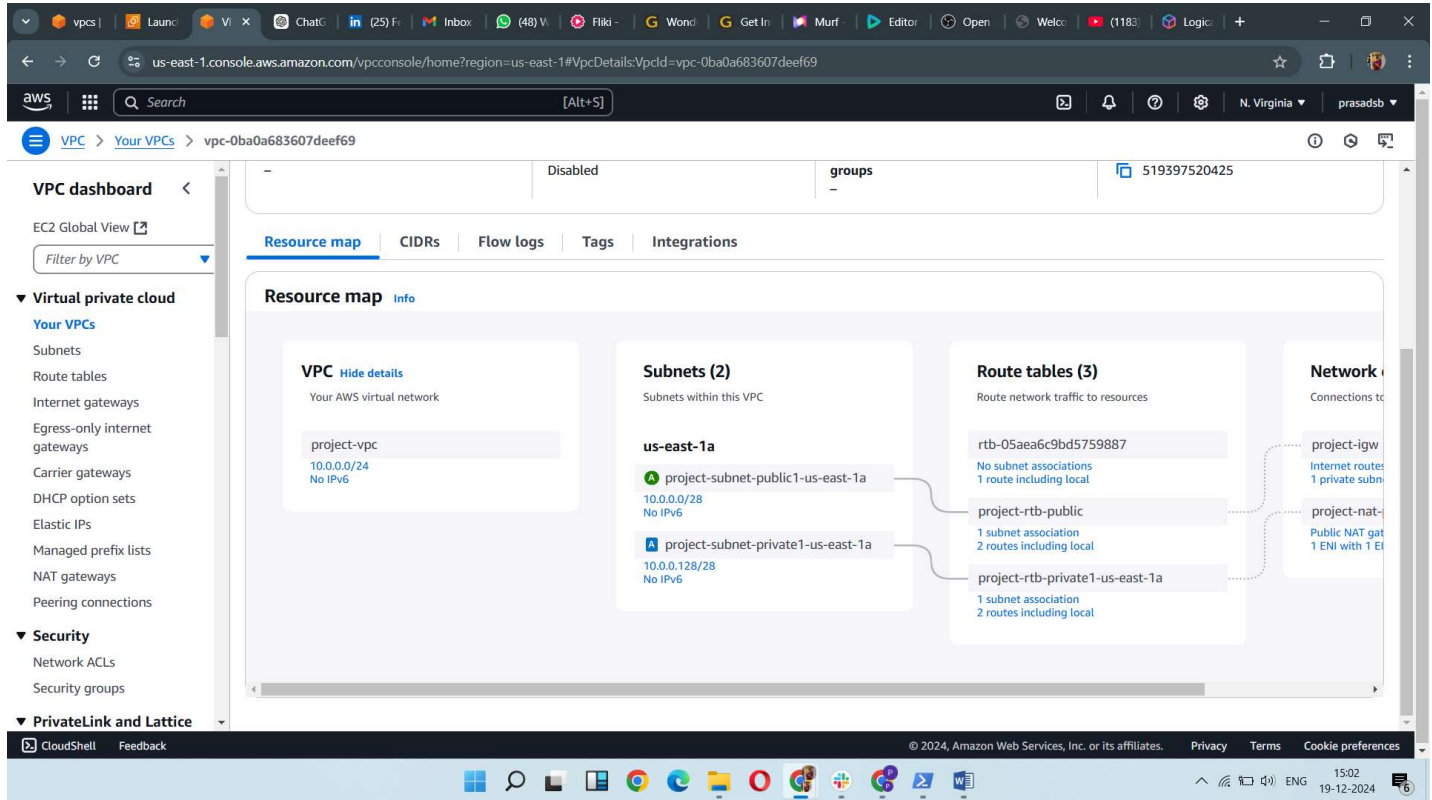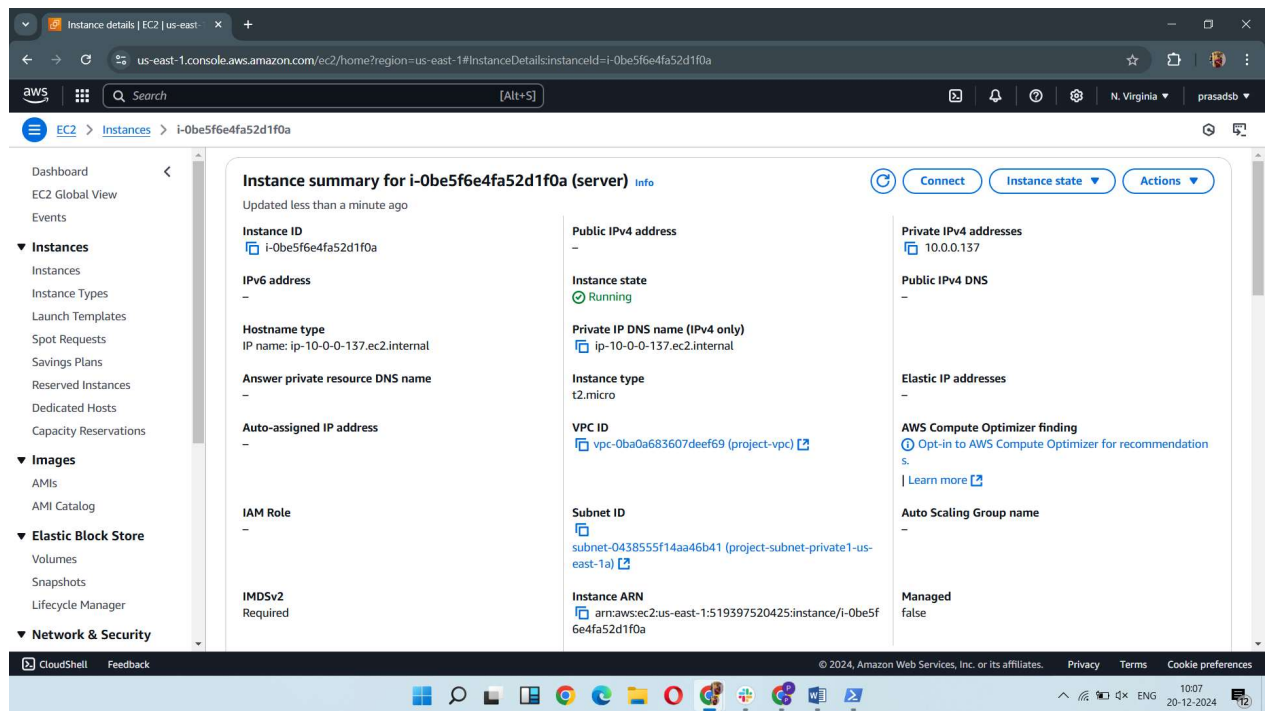

Three EC2 instances were created:

- **Bastion Host (Public IP)**: An EC2 instance created in the public subnet, with a public IP for access.
- **Web Server (Private IP)**: An EC2 instance created in the private subnet, configured as a web server.
- **Client (Private IP)**: Another EC2 instance created in the private subnet, configured as the client.
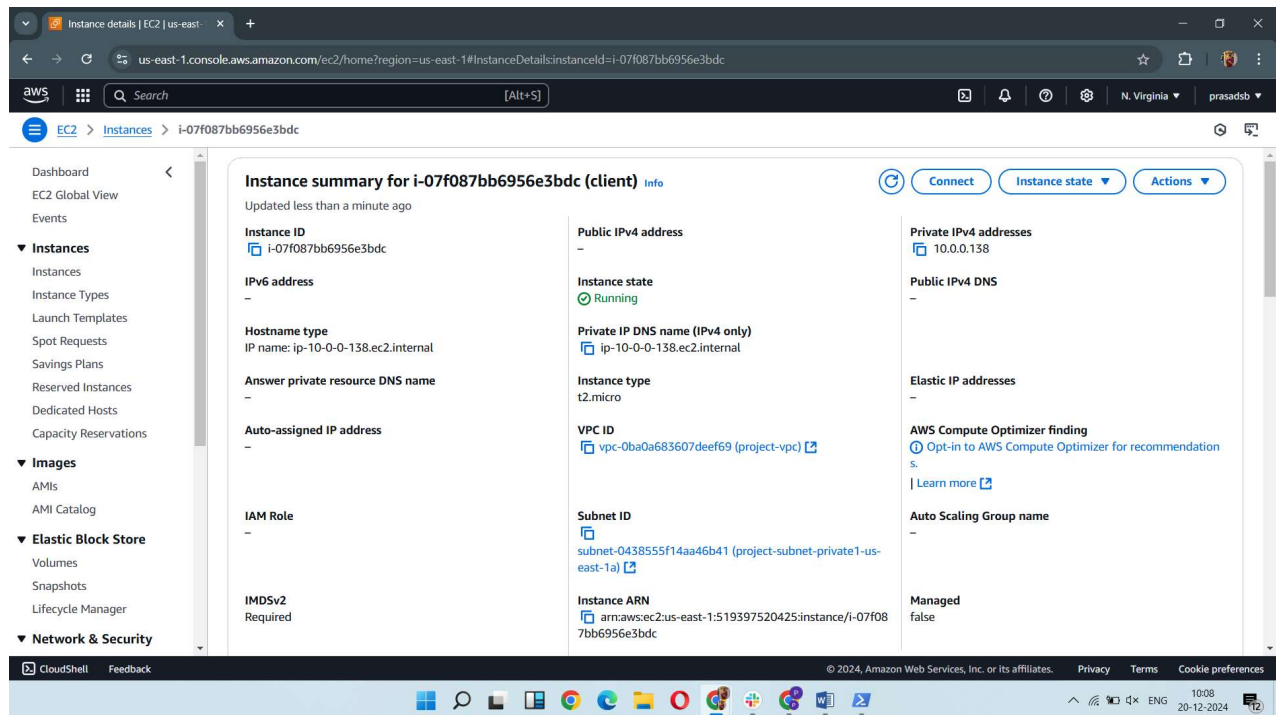 .
- Bastion Host

- ## Web server

- ## Client

- SSH keys were securely transferred from the local machine to the bastion host using SCP.
- The bastion host used as an intermediary to access the private instances (web server and client), bypassing the lack of public IPs on those machines.

- Nginx was installed on the web server, and the appropriate firewall rules (HTTP/80) were added to the security group, enabling the client to access the web page hosted on the server.

- Security Groups
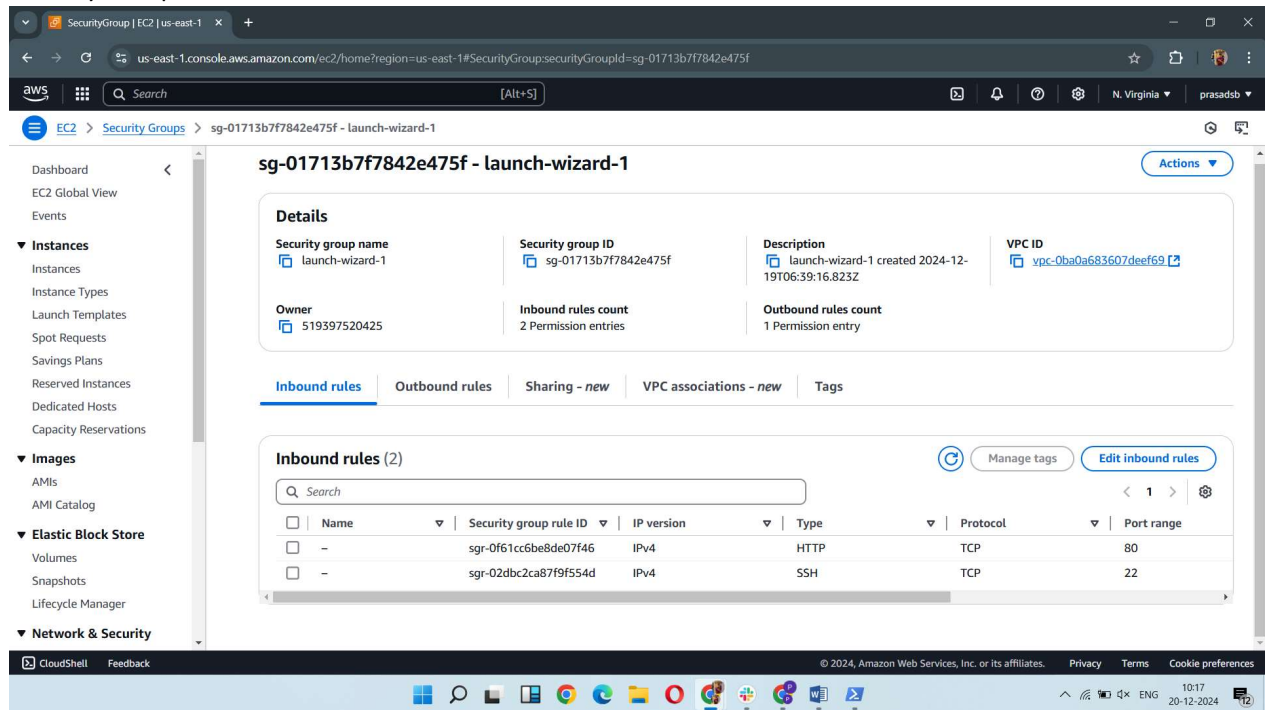
- Web server virtual machine

- Client virtual machine.

- The file transfer process was carried out using SCP, both from the client to the server and vice versa. This demonstrated the use of secure file transfer over SSH.

Basic Architecture

User

VPC: 10.0.0.0/16

PUBLIC SUBNET: 10.0.1.0/24

Internet Gateway

SSH connection

Bastion Host

SSH access

SSH access

PRIVATE SUBNET: 10.0.2.0/24

EC2 Instance 1

EC2 Instance 2

NAT Gateway

Internet