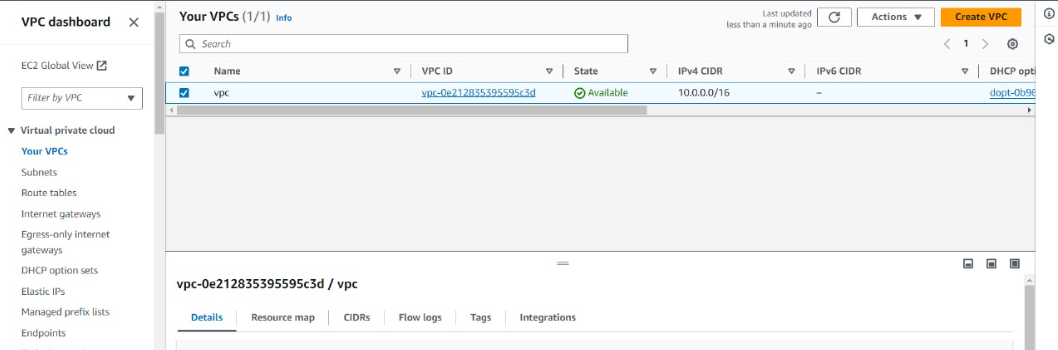
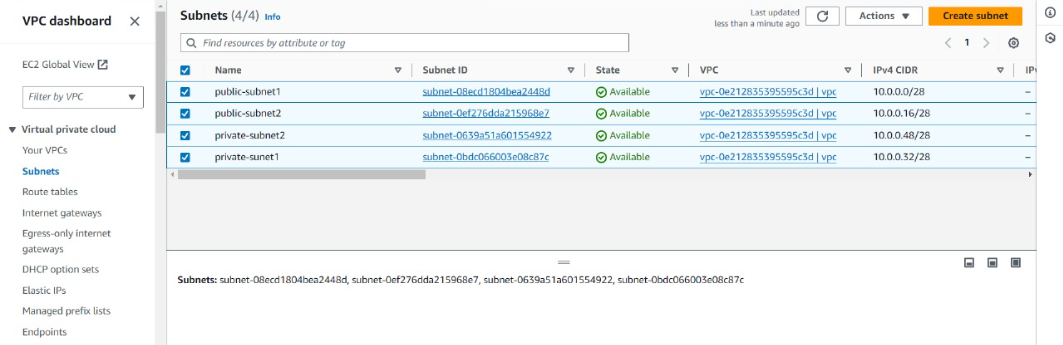
DESIGNING A SECURE NETWORK ARCHITECTURE USING VPC

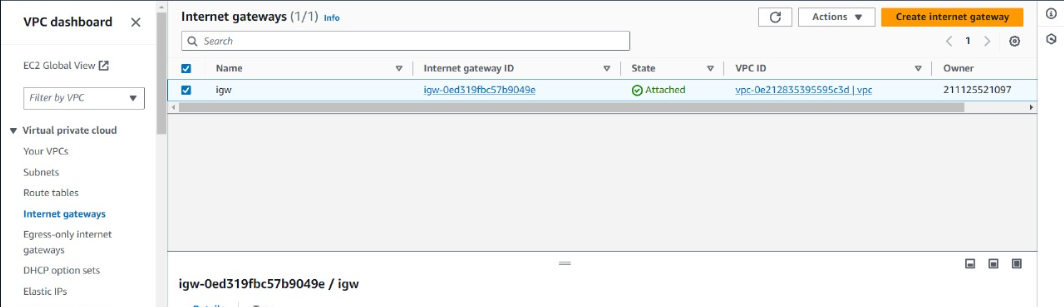
As the project is mostly done in the AWS console I’m providing the screenshots of the steps we followed and here and there we used some commands so I’ll mention them at that particular step.

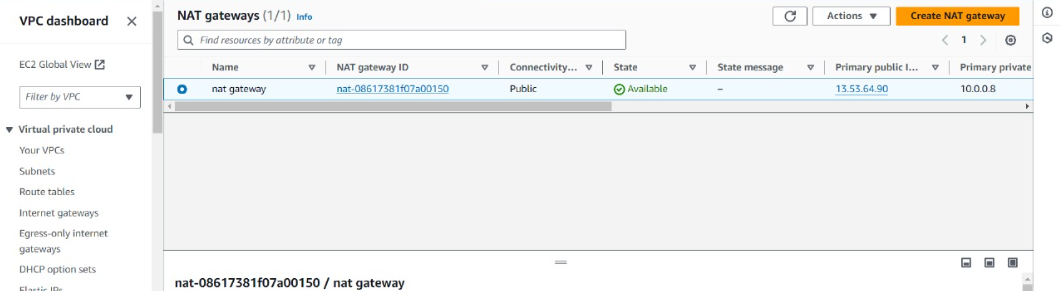


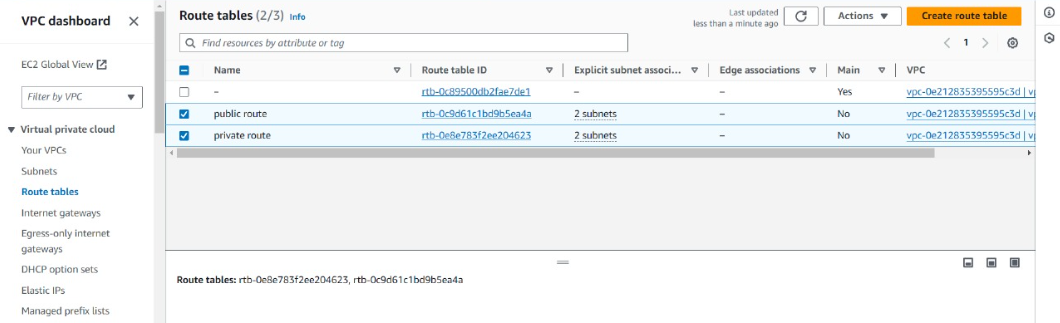
Creating a VPC after configuration

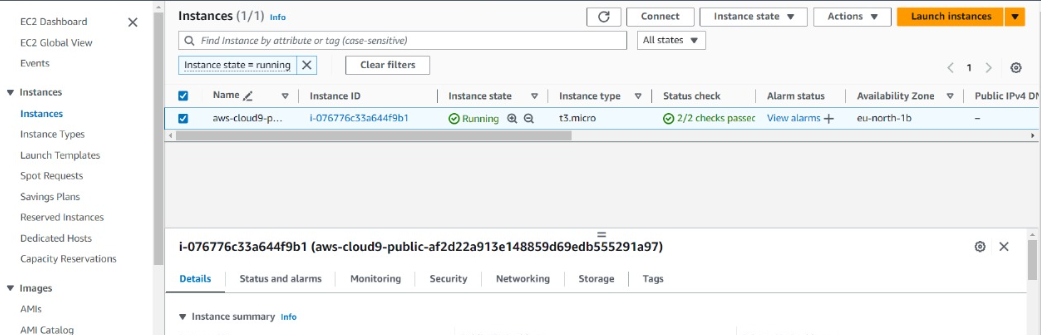


Creating the subnets and connecting then to VPC and configuring them

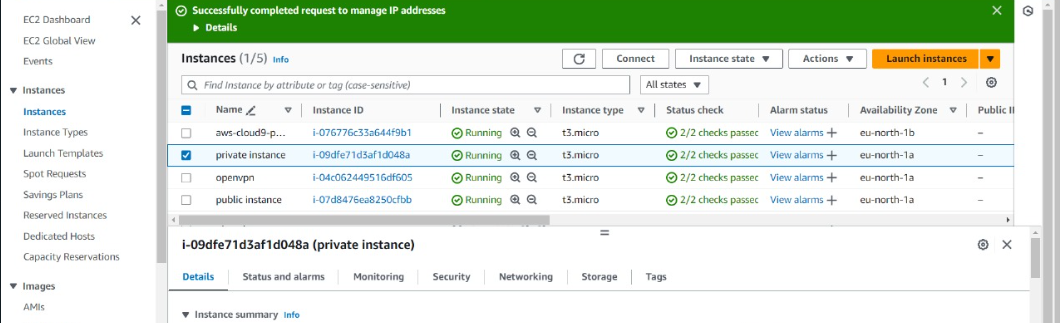




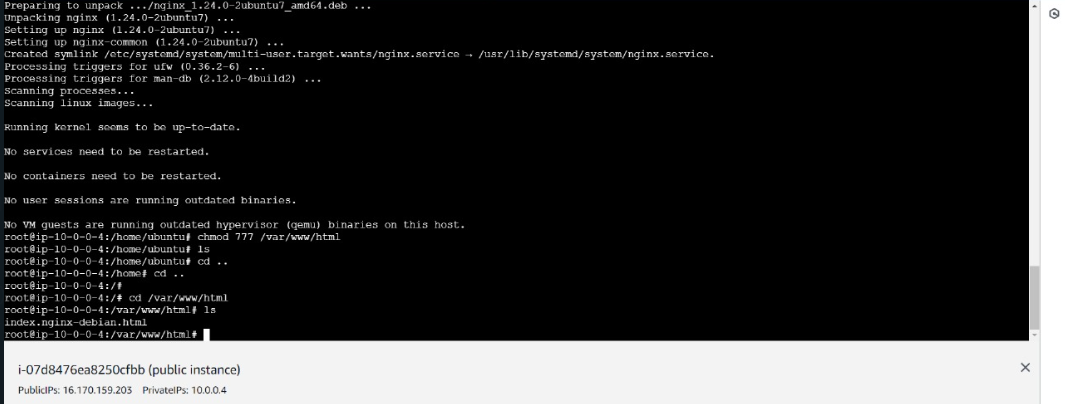
We used a IGW for public route table and NAT gateway for public route table



Launched a AWS cloud9 environment

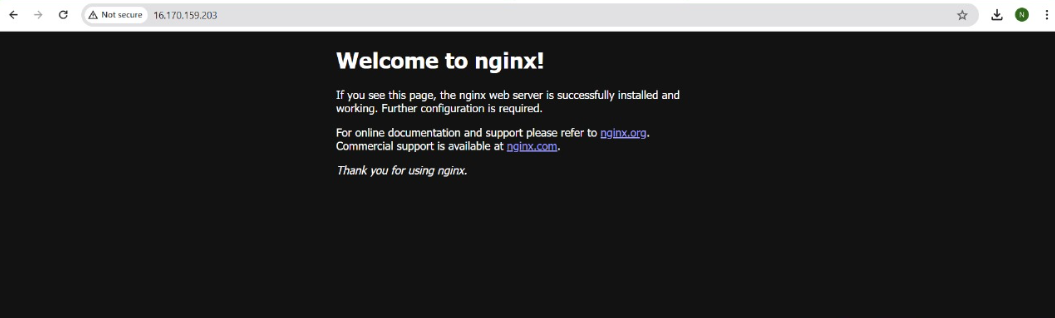


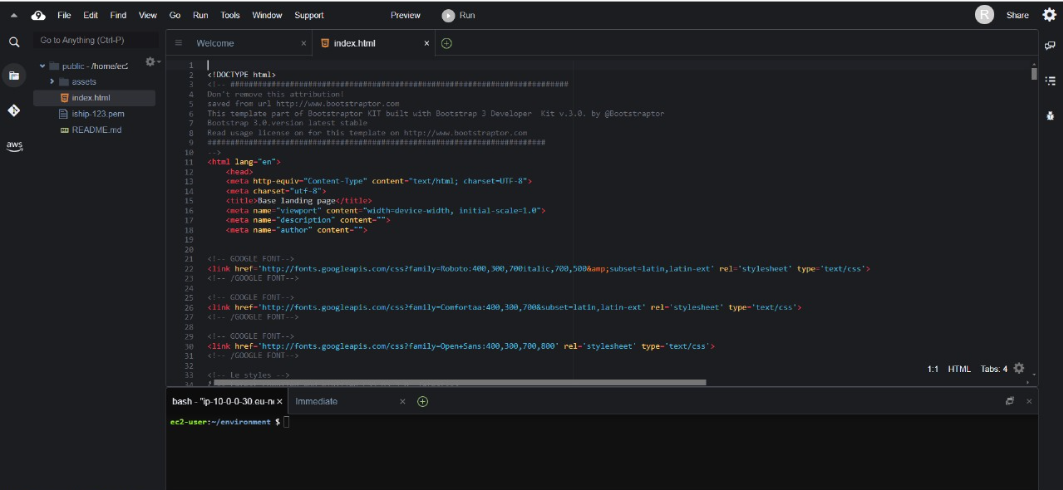
Launched a public ec2 ubuntu instance and a private ec2 ubuntu instance and finally an instance named OpenVPN by using IAM.



Connecting the public instance to ec2 and given the following commands

1. sudo su
2. apt-get update
3. apt-get install nginx -y
4. chmod 777 /var/www/html
5. cd /var/www/html
6. ls





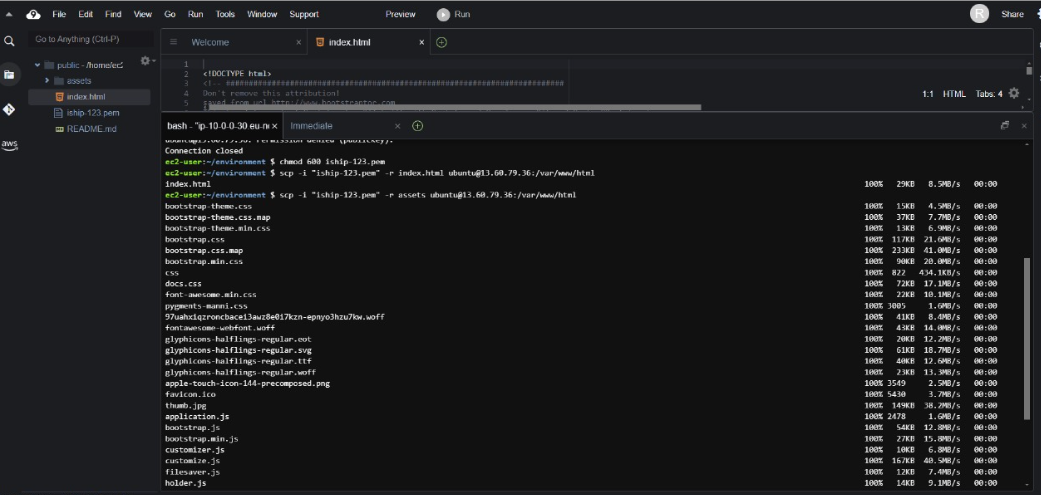
Uploading the sample template and the pem file to the cloud9 environment.

Then given the required commands

1.chmod 600 name.pem

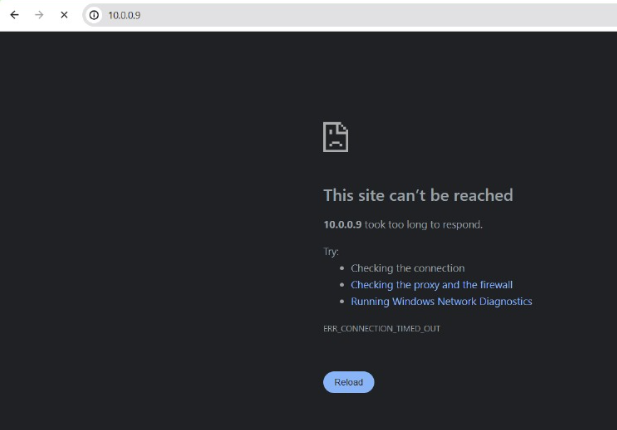
2. scp -i “name.pem” -r index.html source-path ec2-user@IP:/destination-path

3. scp -i “name.pem” -r assets source-path ec2-user@IP:/destination-path

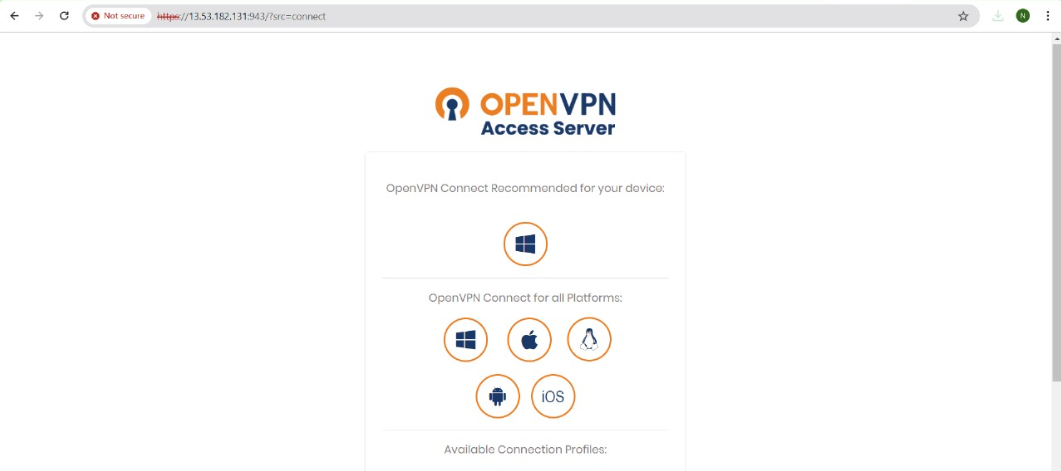


Now the private instance is connected to ec2 and removed the public IP.

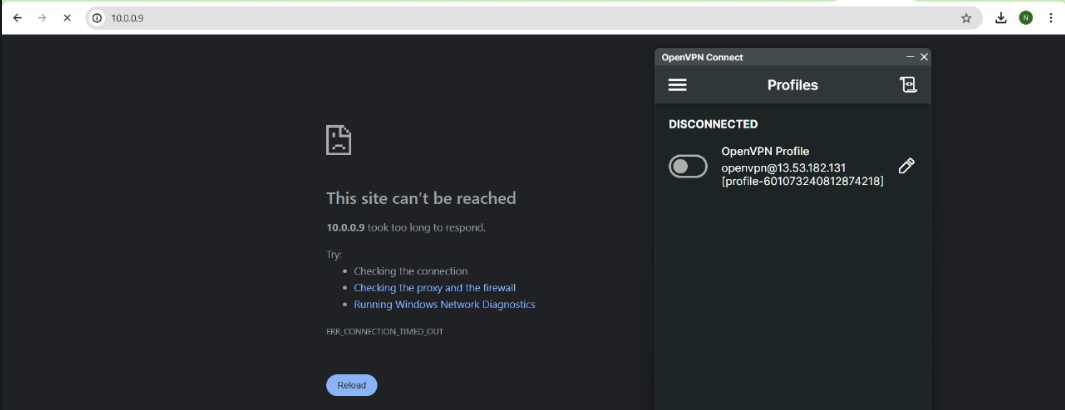
Now taken the private IP and passed it in the new tab

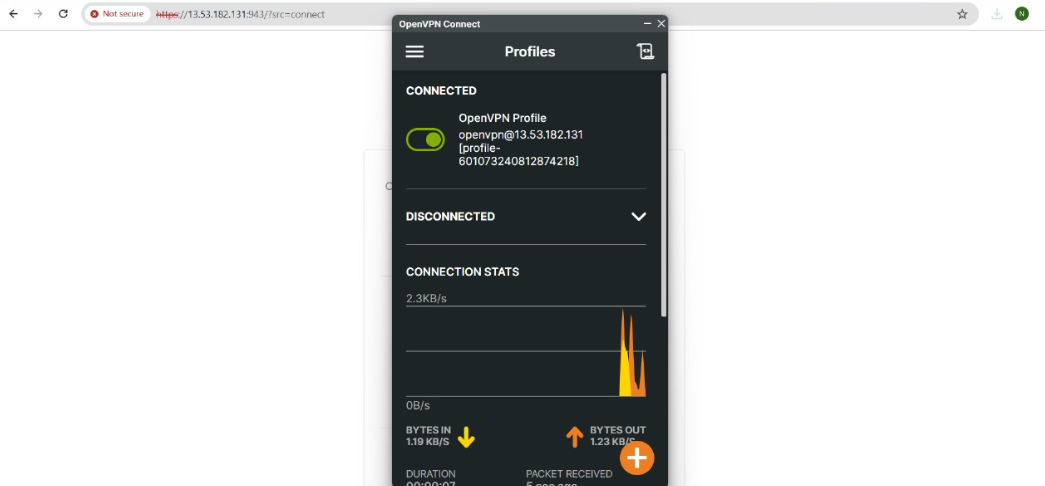


Now download and configure the OpenVPN which is a third party access control.

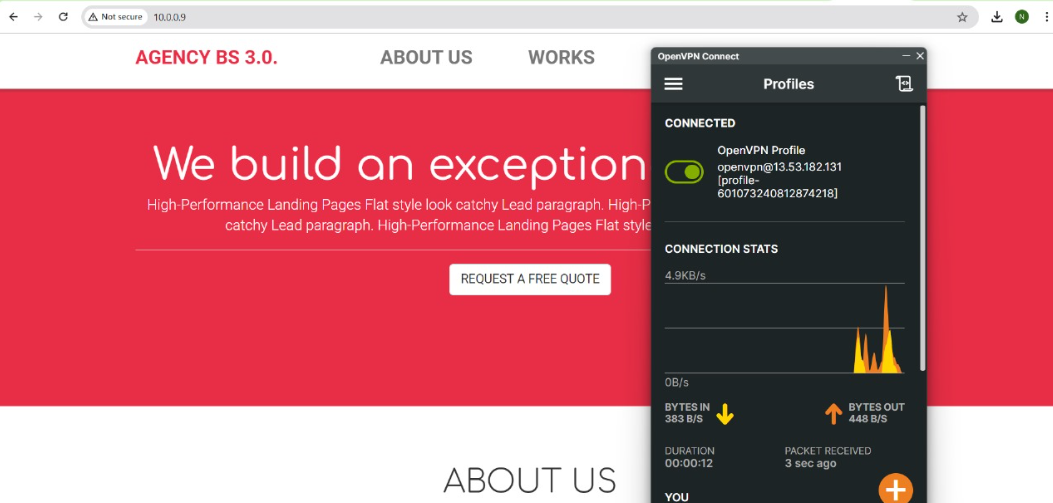


We can’t still access so let’s connect with the OpenVPN





Now we can access the sample website using private IP and pasting it in the new tab



Here with this we designed a secure network architecture using VPC and third party access control OpenVPN.

The basic architecture design is the below one

