Site – To – Site VPN

What is VPN?

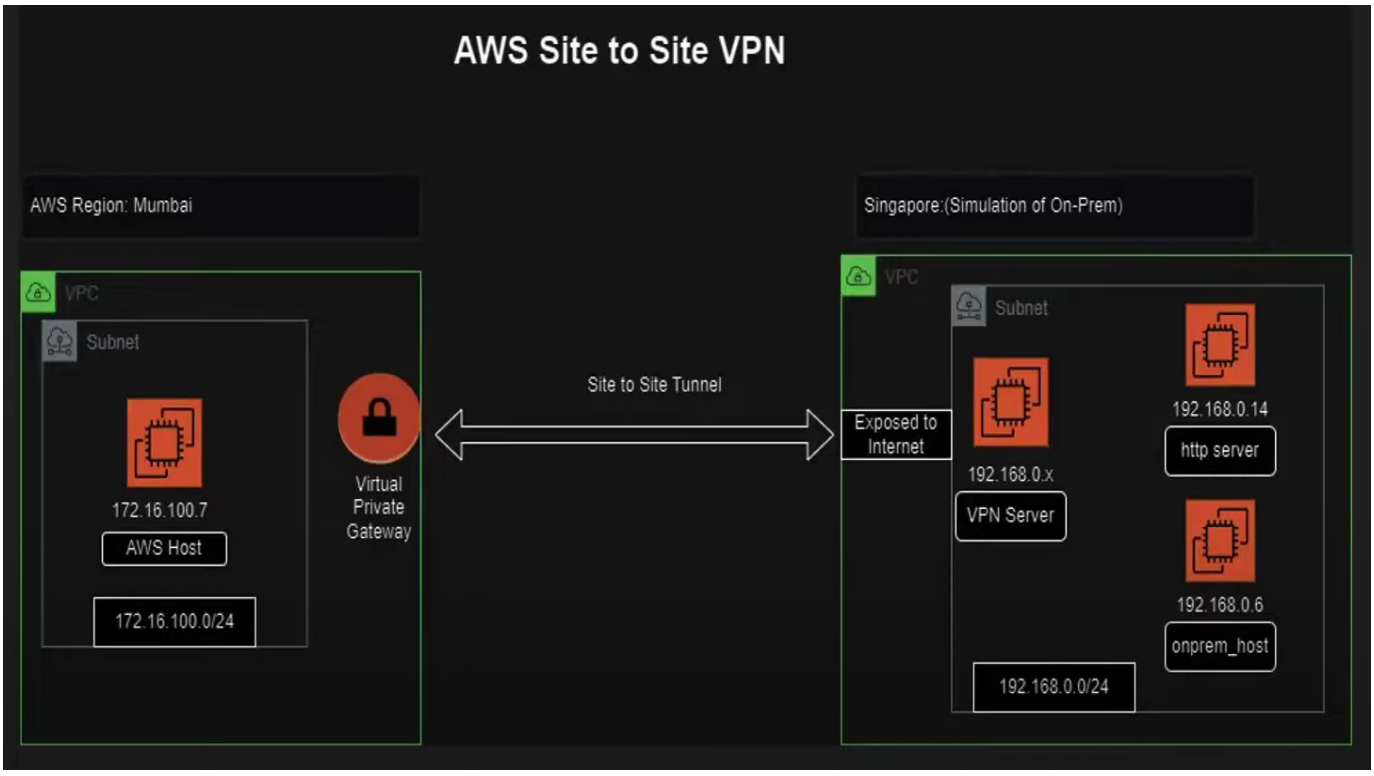
VPN Stants for “Virtual private network” - A service that helps you stay private online.

A Virtual Private Network (VPN) is a specialized virtual network that provides a secure connection over the Internet. It encrypts your internet traffic and hides your online identity, making it significantly harder for third parties to access your data or monitor your online activities.

What is SITE-TO-SITE VPN?

There are multiple ways you can connect your AWS infrastructure to an on-premise network. The Site-to-Site VPN connection is the easier and cost-effective way.

AWS Site-to-Site VPN connections are utilizing the public Internet to connect between AWS and on-premise networks “in general” due to the less cost. That does not mean that it cannot leverage any other connection options such as Direct Connect or Global Accelerated network.



Components

1. Virtual Private Gateway (VGW) — is a logical gateway object, which is a target of one or more Route Tables.

2. Customer Gateway (CGW) — is a logical configuration on AWS, which represents the configurations of the physical on-premises router where VPN is connected to

3. VPN Connection - By, default instances that you launch into an Amazon VPC Can't Communicate With your Own Network To enable the communicate, you have to establish,

Site-To-Site VPN Connection

1) VPN Connection -A secure Connection Between your On-premises equipment and your VPC

2) VPN Tunnel – An encrypted link Where data can pass from the Customer network to or from AWS Each VPN Connection include two VPN Tunnels Which You Can Simultaneously use for High Availability.

3) Customer Gateway – An Aws resource Which Provides Information to AWS about you Customer Gateway device.

4) Customer Gateway device – A physical app on Customer site.

Create one VPC in Mumbai Region

➔ Go to VPC

➔ VPC & more

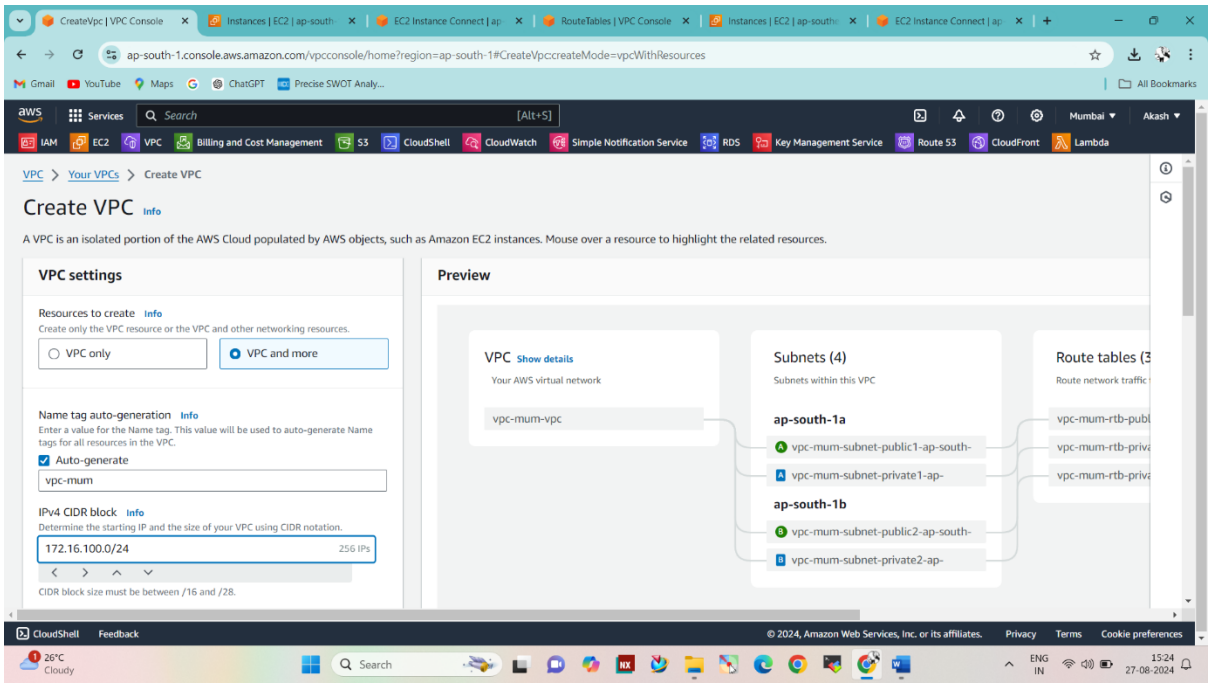
➔ Give CIDR Block as 172.16.100.0/24

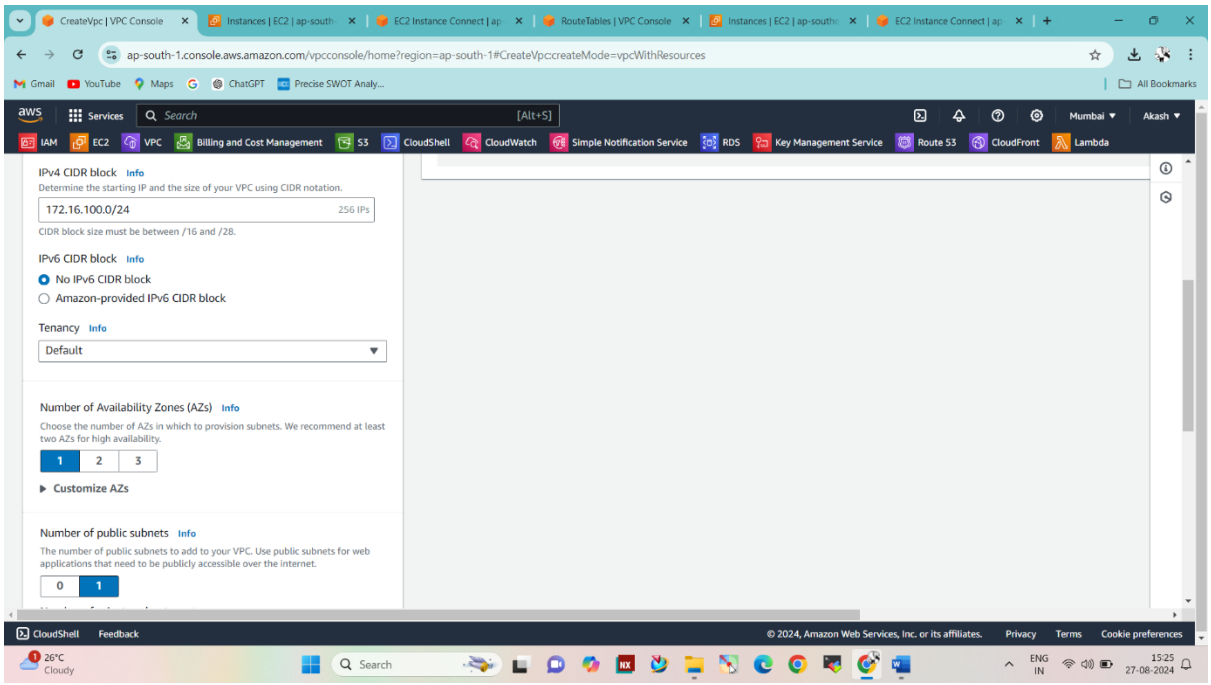
Create one VPC in Singapore Region

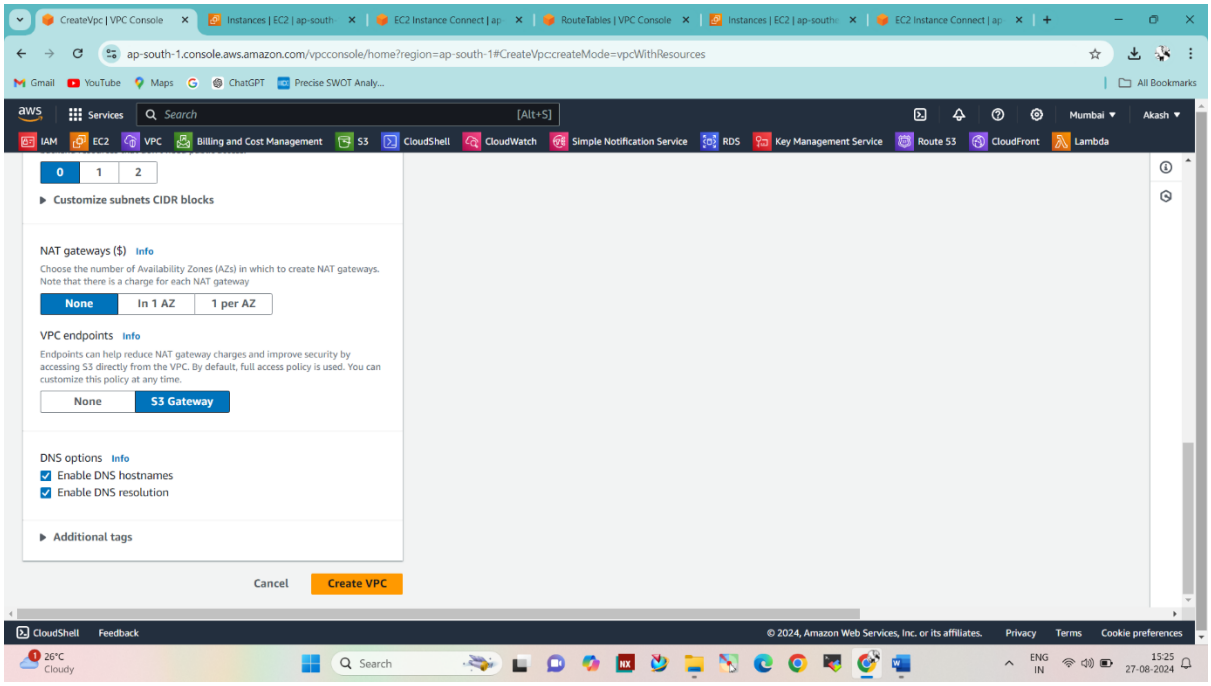
➔ Go to VPC

➔ VPC & more

➔ Give CIDR Block as 192.168.0.0/24


CreateVpc | VPC Console
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateVpc:createMode=vpcWithResources
Services
Search
[Alt+S]
Mumbai
Akash
IAM
EC2
VPC
Billing and Cost Management
S3
CloudShell
CloudWatch
Simple Notification Service
RDS
Key Management Service
Route 53
CloudFront
Lambda
VPC > Your VPCs > Create VPC
Create VPC Info
A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to highlight the related resources.
VPC settings
Resources to create Info
Create only the VPC resource or the VPC and other networking resources.
VPC only
VPC and more
Name tag auto-generation Info
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.
Auto-generate
vpc-mum
IPv4 CIDR block Info
Determine the starting IP and the size of your VPC using CIDR notation.
172.16.100.0/24
256 IPs
CIDR block size must be between /16 and /28.
Preview
VPC Show details
Your AWS virtual network
vpc-mum-vpc
Subnets (4)
Subnets within this VPC
ap-south-1a
vpc-mum-subnet-public1-ap-south-
vpc-mum-subnet-private1-ap-
ap-south-1b
vpc-mum-subnet-public2-ap-south-
vpc-mum-subnet-private2-ap-
Route tables (3
Route network traffic
vpc-mum-rtb-publ
vpc-mum-rtb-priv
vpc-mum-rtb-priv
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
26°C
Cloudy
Search
ENG
IN
15:24
27-08-2024


CreateVpc | VPC Console
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateVpc:createMode=vpcWithResources
Services
Search
[Alt+S]
Mumbai
Akash
IAM
EC2
VPC
Billing and Cost Management
S3
CloudShell
CloudWatch
Simple Notification Service
RDS
Key Management Service
Route 53
CloudFront
Lambda
IPv4 CIDR block Info
Determine the starting IP and the size of your VPC using CIDR notation.
172.16.100.0/24
256 IPs
CIDR block size must be between /16 and /28.
IPv6 CIDR block Info
No IPv6 CIDR block
Amazon-provided IPv6 CIDR block
Tenancy Info
Default
Number of Availability Zones (AZs) Info
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.
1
2
3
Customize AZs
Number of public subnets Info
The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.
0
1
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
26°C
Cloudy
Search
ENG
IN
15:25
27-08-2024



Create one Instance in Mumbai Region

➔ Launch Instance

➔Use image as “Amazon Linux 2”

➔Launch Instance

Create one Instance in Singapore Region

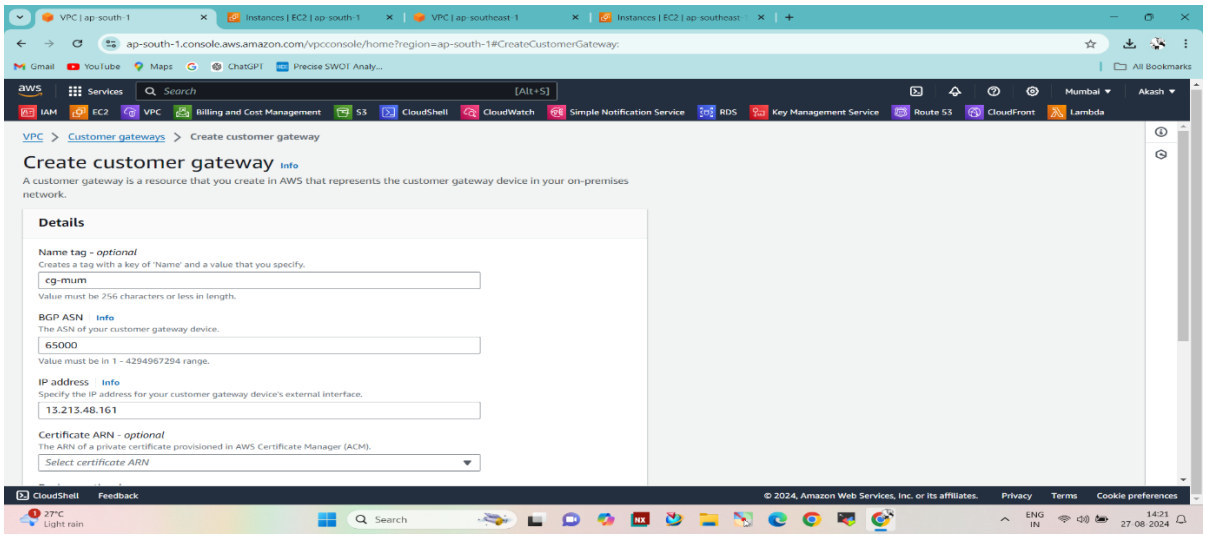
➔ Launch Instance

➔Use image as “Amazon Linux 2”

➔Launch Instance

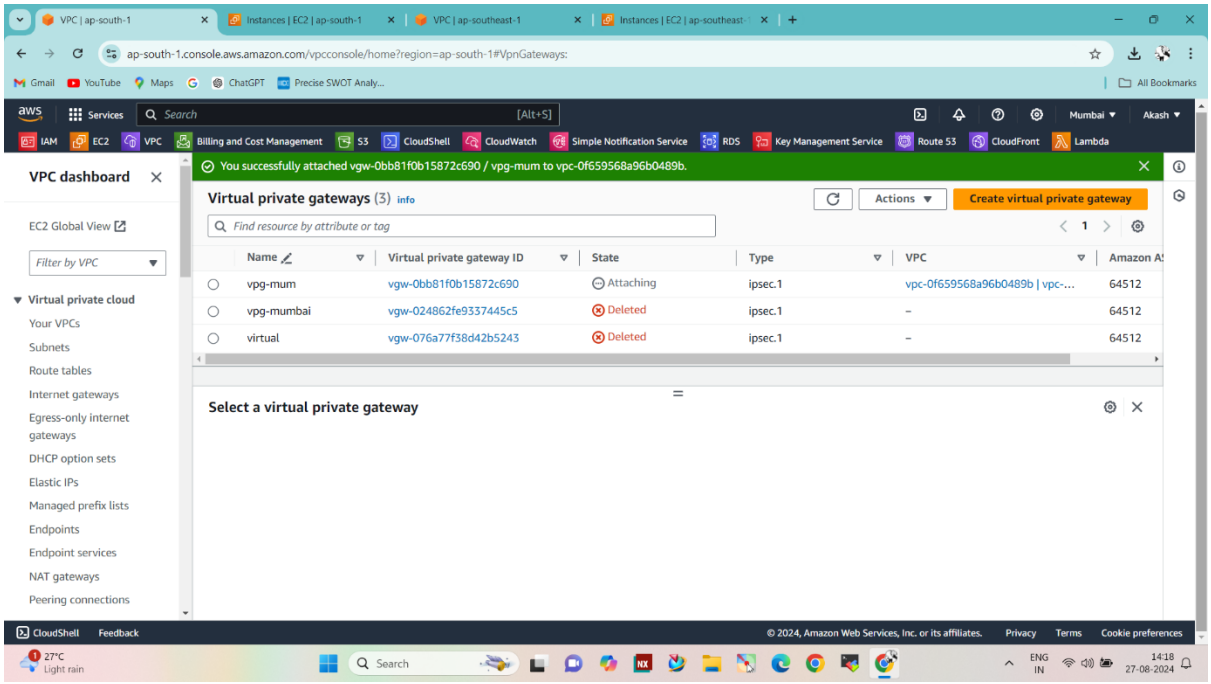
Create Customer Gateway in Mumbai Region

➔Use Public IP address of Singapore Region



Create Virtual Private Gateway in Mumbai Region

➔Attach Virtual Private Gateway to VPC

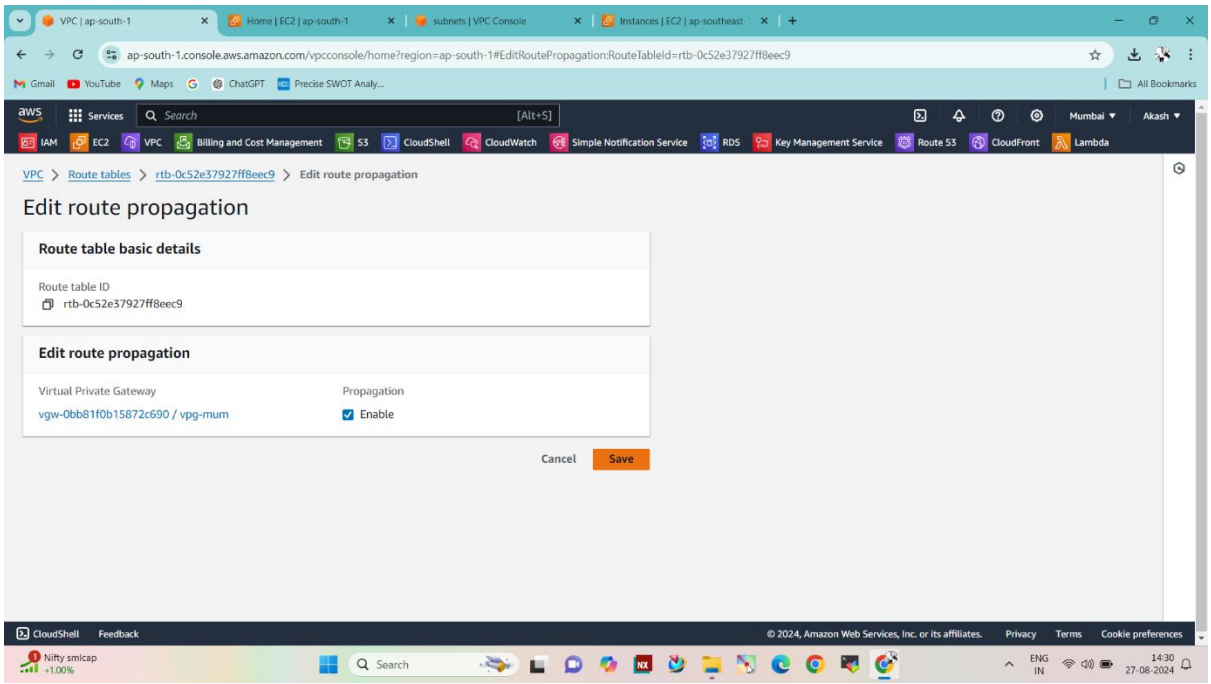


Go to Route Table

➔Actions

➔Edit rout Propagation

➔" Enable" & save



Create Site-to-Site VPN in Mumbai Region

➔Select Virtual Private Gateway

➔Select Customer Gateway

➔Routing Options

➔Static

➔Static IP prefix.

➔192.168.0.0/24

➔172.16.100.0/24

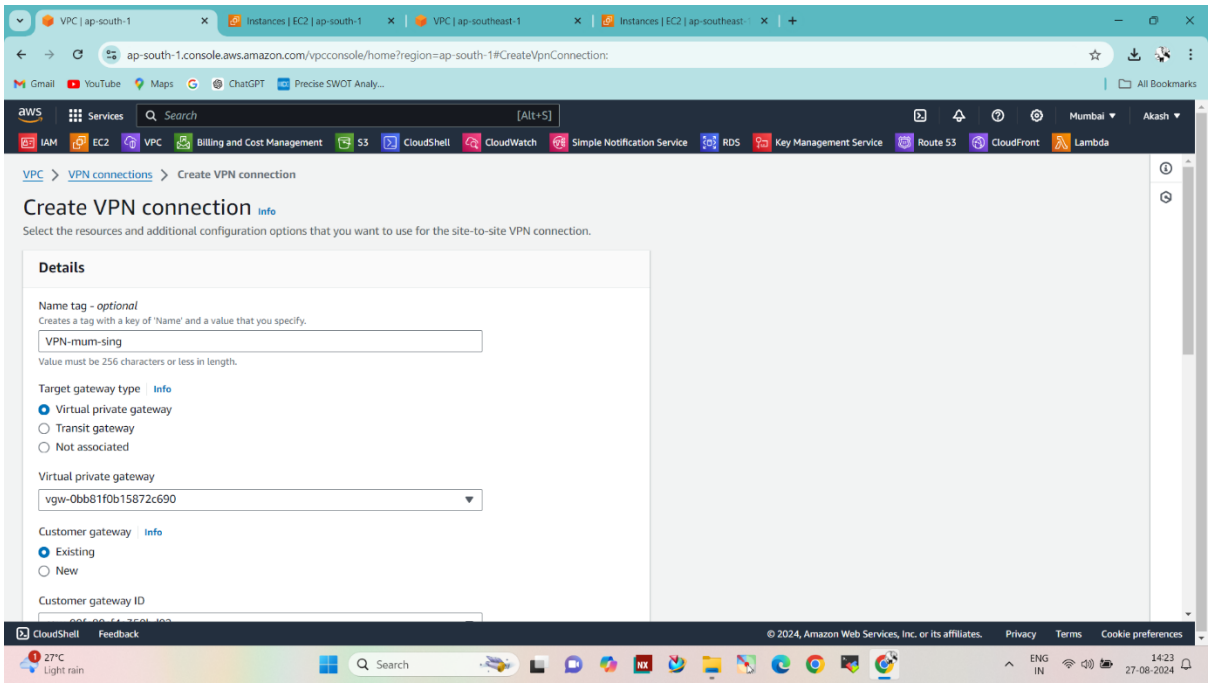
➔Local IPv4 network CIDR

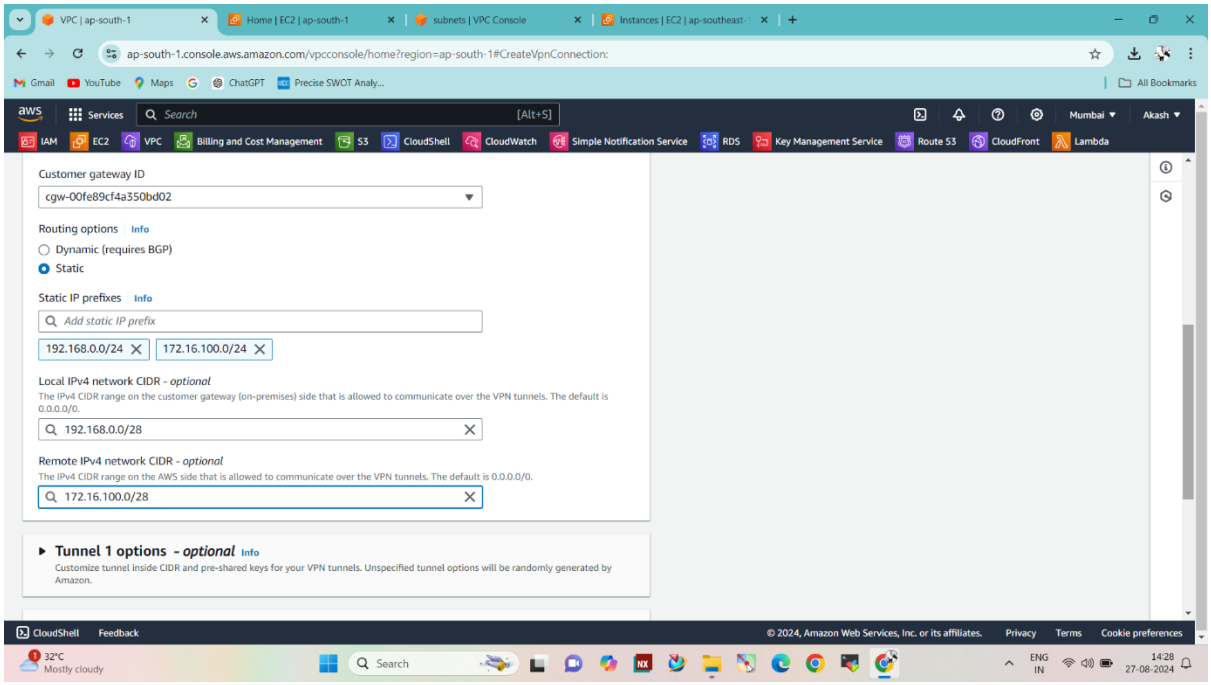
➔192.168.0.0/28 ..... Use Singapore Subnet CIDR

➔ Remote IPv4 network CIDR

➔172.16.100.0/28 ..... Use Mumbai Subnet CIDR

➔Create VPN Connection.



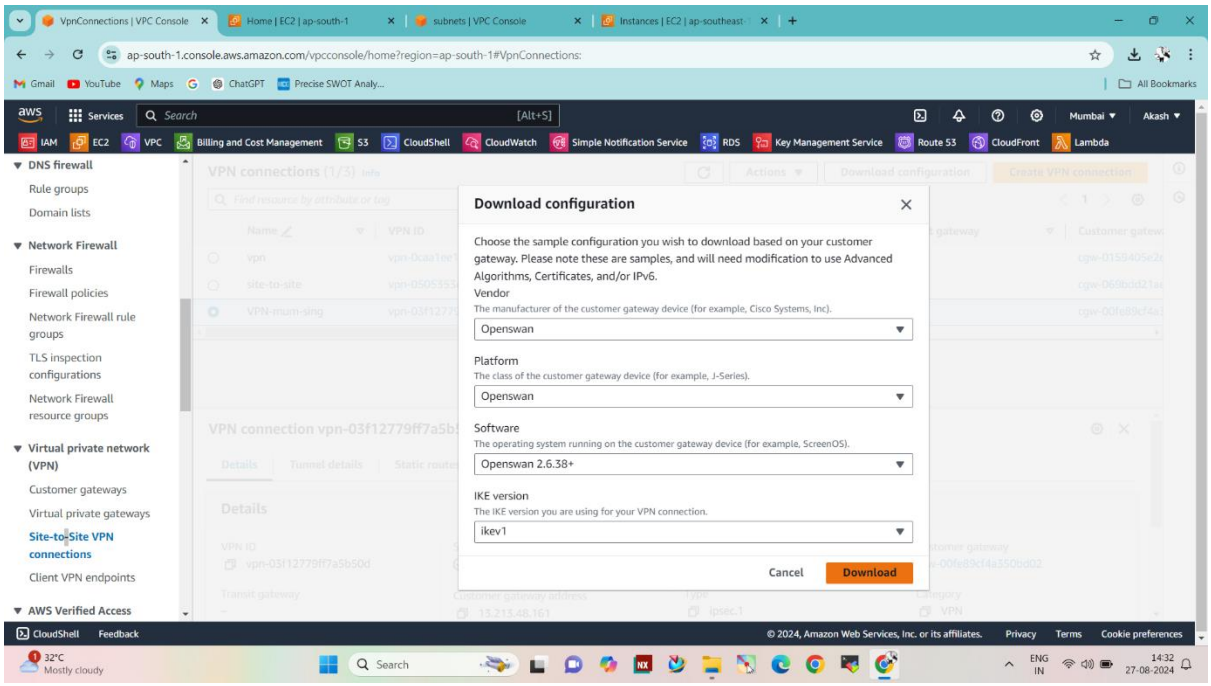


After Creating Site-to-Site VPN

➔Download Configuration

➔Download Openswan File

➔Close



Add Security Group

➔All TCP, SSH, HTTP, ICMP, IMAP Ports

Connect to Singapore Instance

sudo -i

yum install openswan -y

Note :- Open Downloaded Configuration File and Follow all the steps of openswan Configure File.

This configuration assumes that you already have a default openswan installation in place on the Amazon Linux operating system (but may also work with other distros as well)

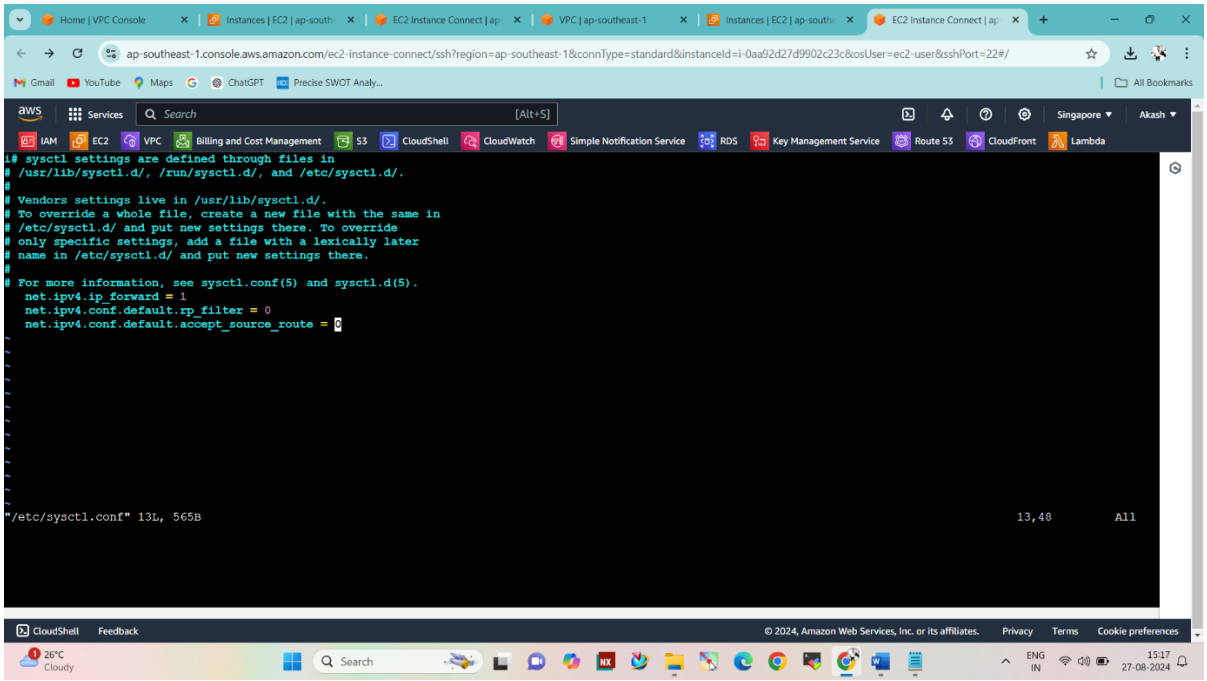
Steps :-

1) Open /etc/sysctl.conf and ensure that its values match the following:

net.ipv4.ip_forward = 1

net.ipv4.conf.default.rp_filter = 0

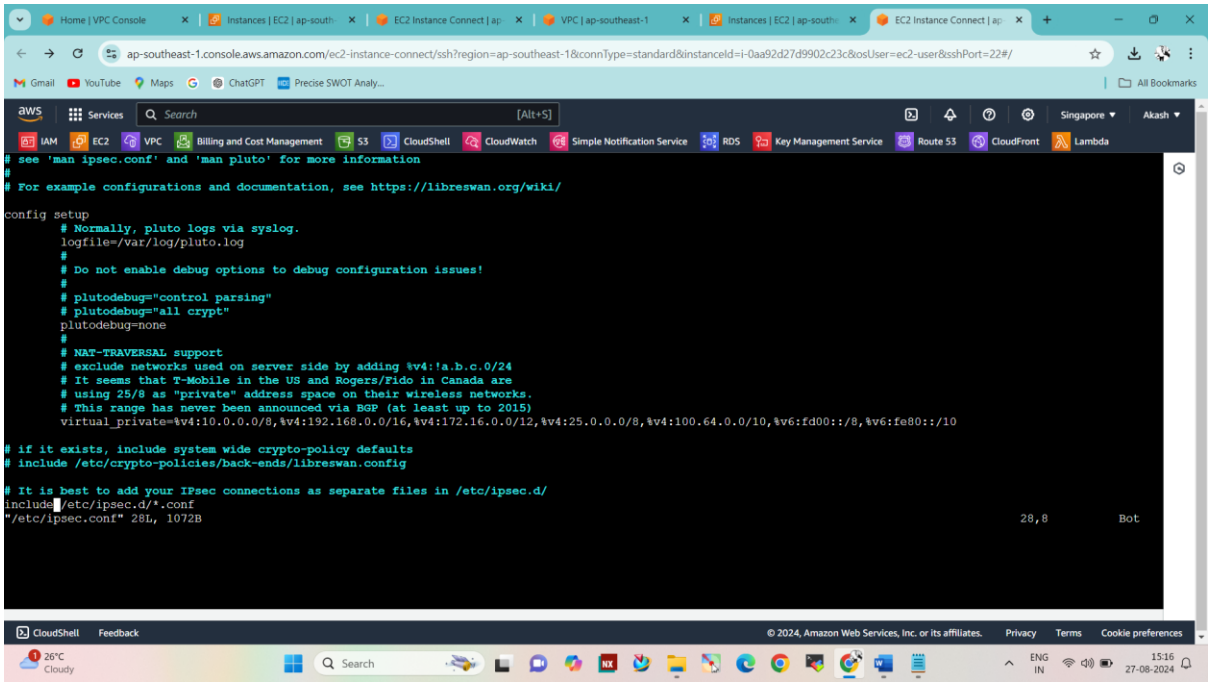
net.ipv4.conf.default.accept_source_route = 0



2) Apply the changes in step 1 by executing the command 'sysctl -p'

3) Open /etc/ipsec.conf and look for the line below. Ensure that the # in front of the line has been removed, then save and exit the file.

#include /etc/ipsec.d/*.conf



4) Create a new file at /etc/ipsec.d/aws.conf if doesn't already exist, and then open it. Append the following configuration to the end in the file:

#leftsubnet= is the local network behind your openswan server, and you will need to replace the <LOCAL NETWORK> below with this value (don't include the brackets). If you have multiple subnets, you can use 0.0.0.0/0 instead.

#rightsubnet= is the remote network on the other side of your VPN tunnel that you wish to have connectivity with, and you will need to replace <REMOTE NETWORK> with this value (don't include brackets).

<u>Note :</u>- Remove “auth=esp ”

conn Tunnel1

authby=secret

auto=start

left=%defaultroute

leftid=13.213.48.161

right=13.126.30.31

type=tunnel

ikelifetime=8h

keylife=1h

phase2alg=aes128-sha1;modp1024

ike=aes128-sha1;modp1024

auth=esp

keyingtries=%forever

keyexchange=ike

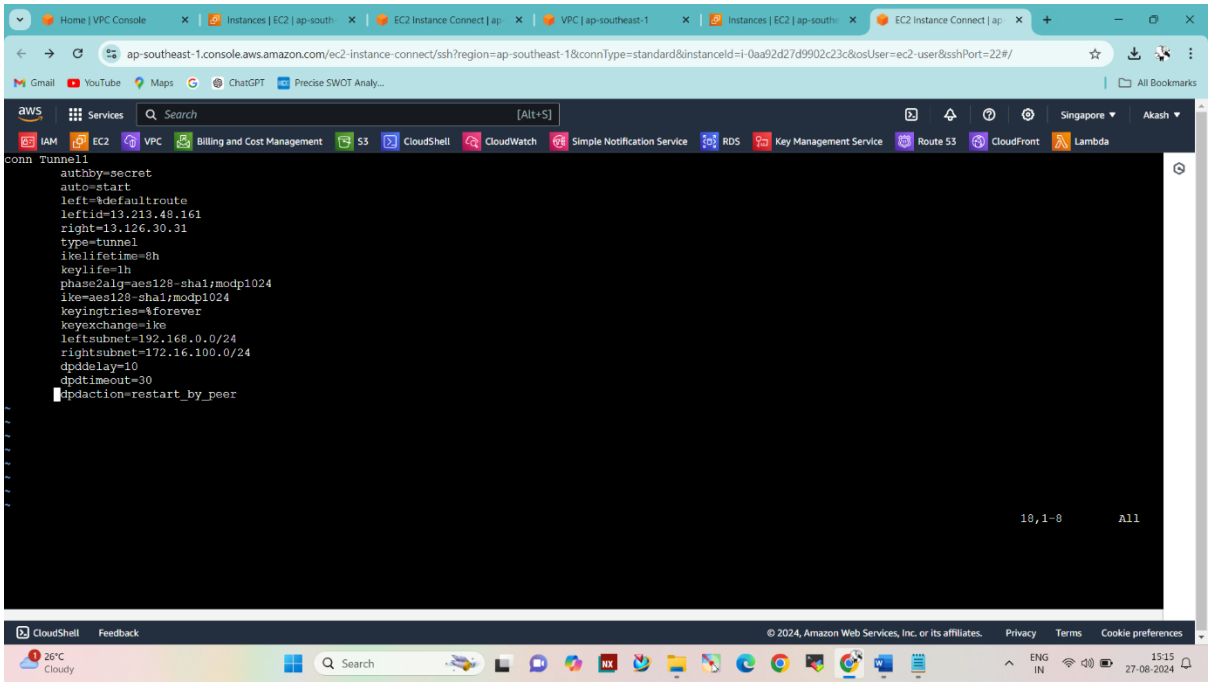
leftsubnet=<LOCAL NETWORK> ……. Use Singapore VPC CIDR

rightsubnet=<REMOTE NETWORK> …… Use Mumbai VPC CIDR

dpddelay=10

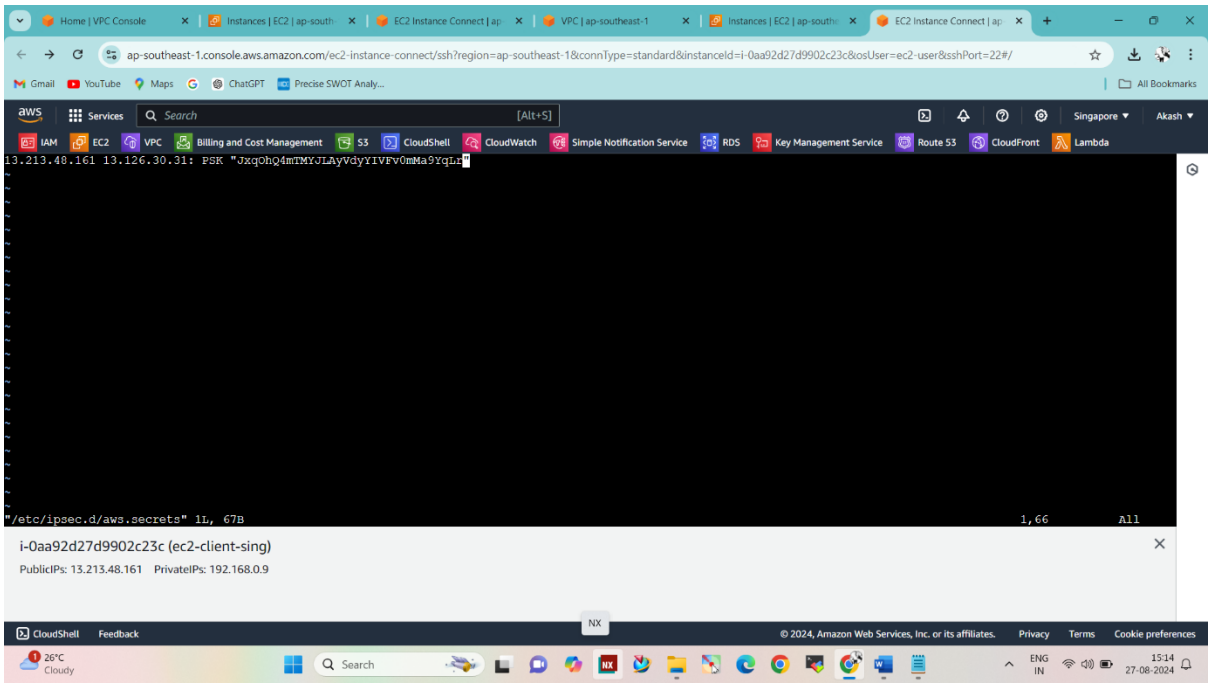
dpdtimeout=30

dpdaction=restart_by_peer



5) Create a new file at /etc/ipsec.d/aws.secrets if it doesn't already exist, and append this line to the file (be mindful of the spacing!):

13.213.48.161 13.126.30.31: PSK "JxqOhQ4mTMYJLAyVdyYIVFv0mMa9YqLr"



systemctl start ipsec.service

systemctl status ipsec.service

systemctl restart ipsec.service

Go to Instance in Singapore Region

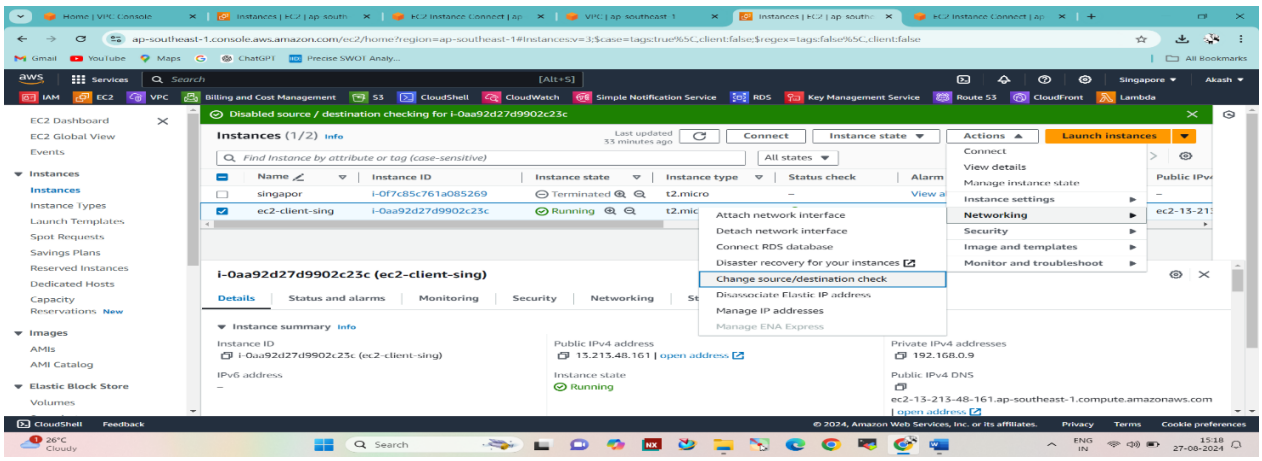
➔Select Instance

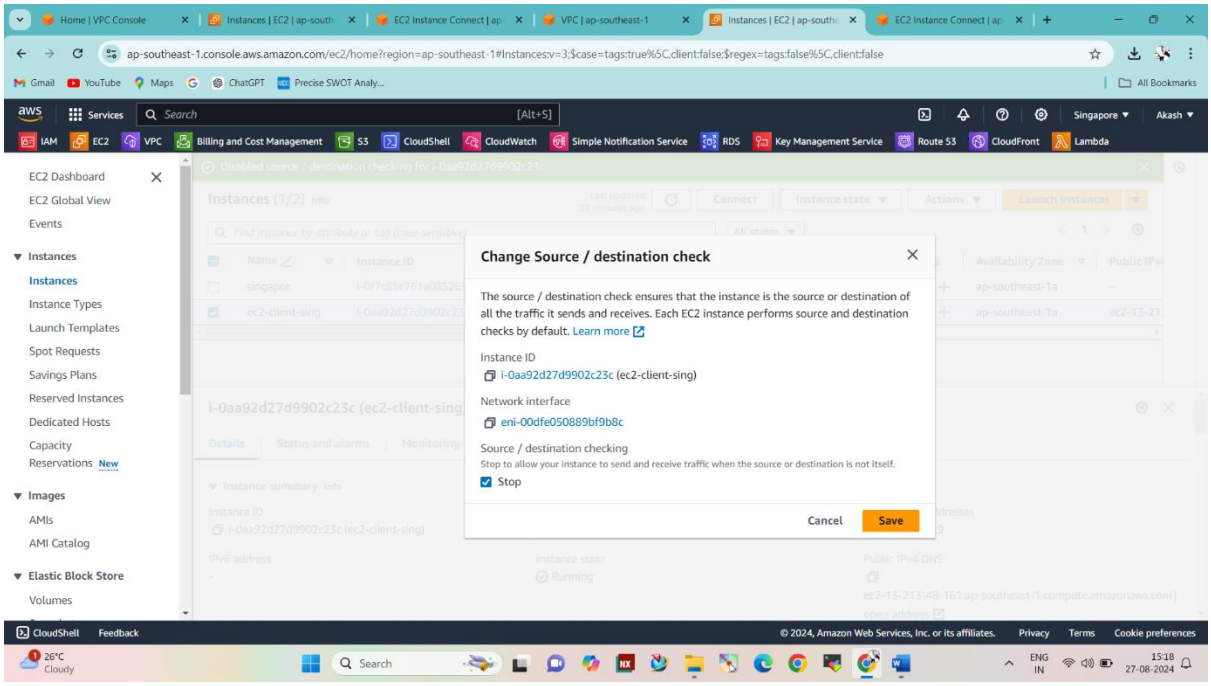
➔Actions

➔Networking

➔Change source / Destination Check

➔ " Stop" And Save





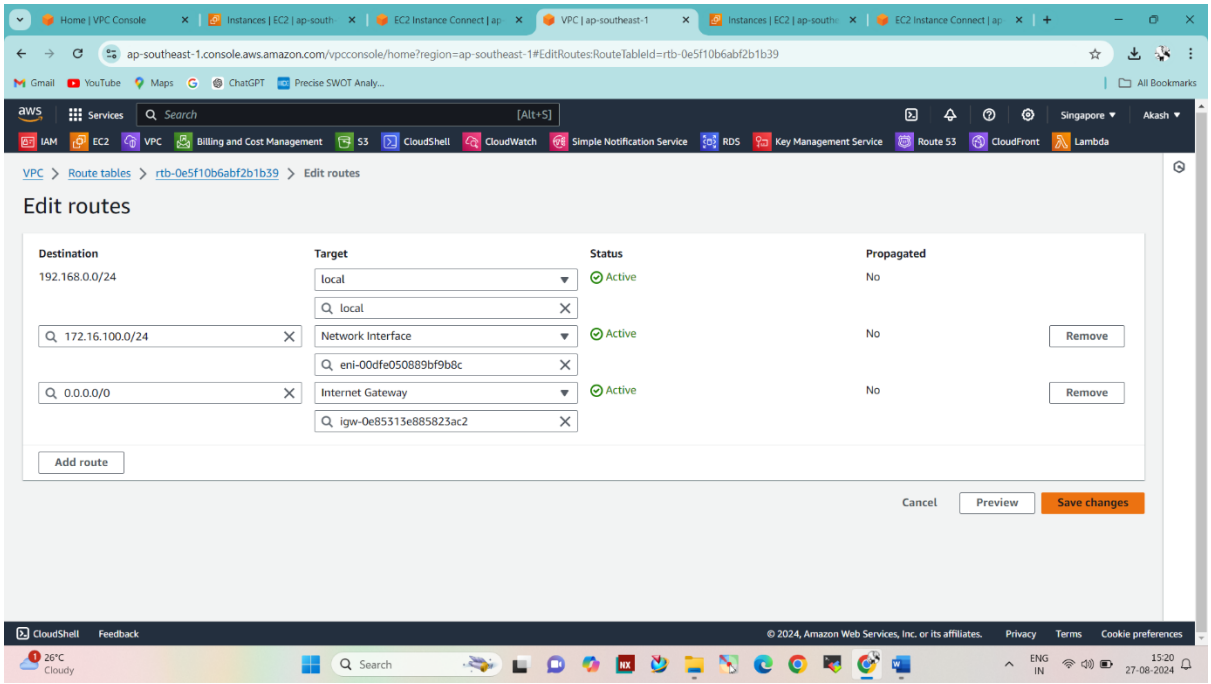
Go to Route Table

➔Edit Rout

➔Destination = 172.16.100.0/24

➔Target = Instance

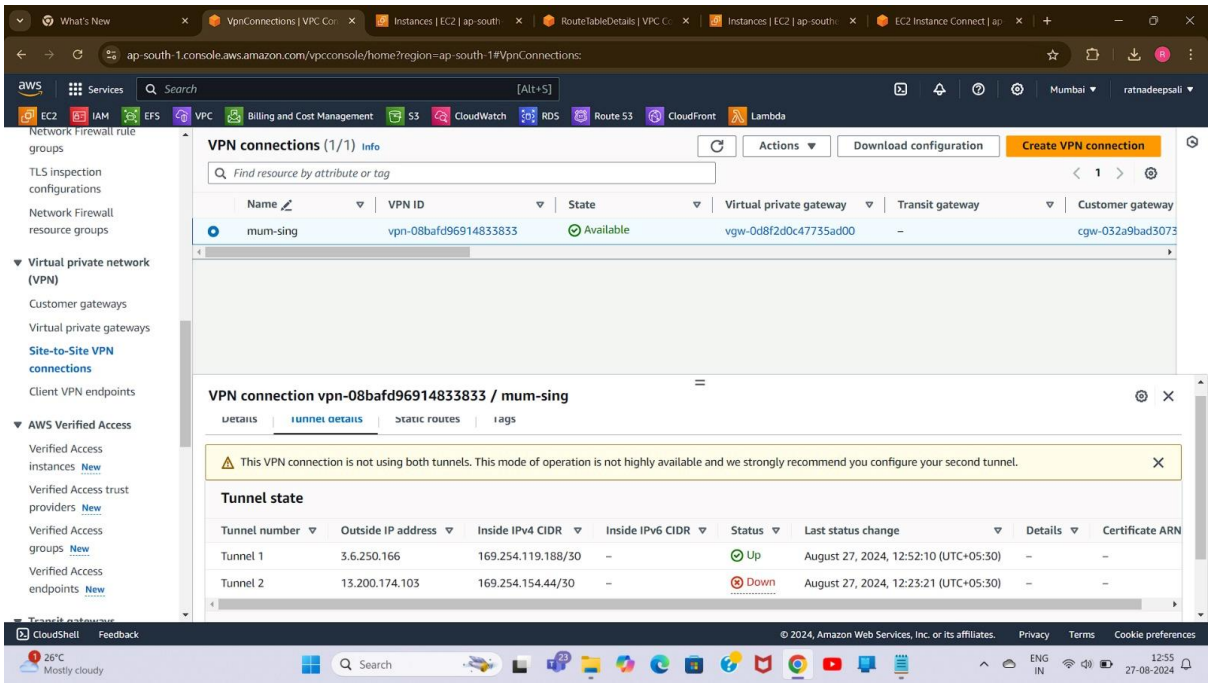
➔Save Changes



Go to Site – To – Site VPN

➔Chek the Tunnel Status

➔The status should be “UP”



Ping the Private IP of Mumbai Instance to the Singapore Instance

Go to Singapore Instance

➔# ping < Mumbai Instance Private IP >