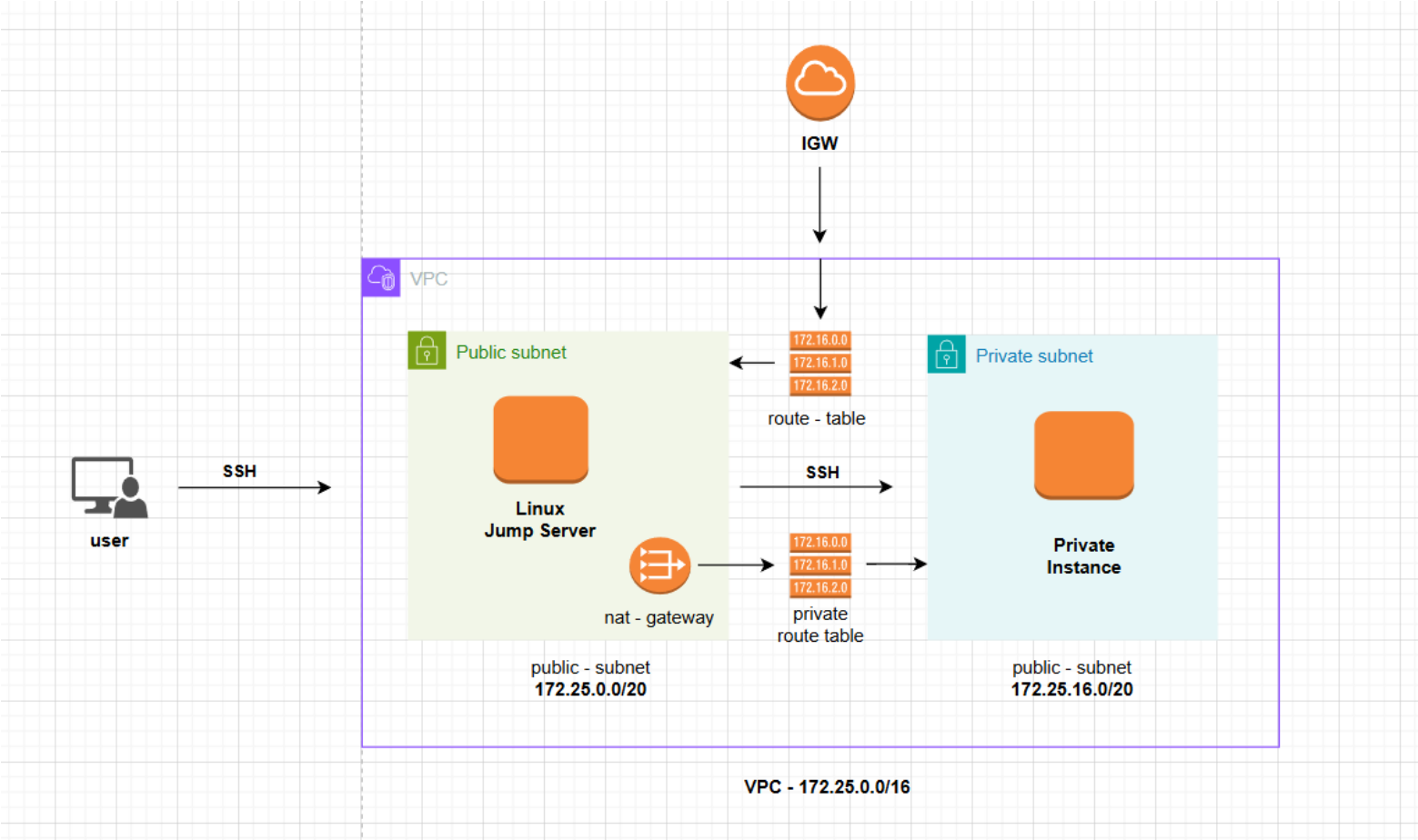
Project Title: Designing and Implementing a Private Network using VPC

Designing and Implementing a Private Network using AWS VPC:

This project demonstrates the design and implementation of a secure, scalable, and isolated private network architecture using Amazon Web Services (AWS) Virtual Private Cloud (VPC). The setup ensures efficient traffic routing, secure remote access, and controlled internet exposure for EC2 instances through strategic subnet design and access control mechanisms.



Key Components and Implementation

- **Virtual Private Cloud (VPC):**
  - Designed a custom VPC with CIDR block allocation to logically isolate network resources.
  - Created both **public** and **private subnets** to separate externally exposed and internal workloads.

- **Subnets & Route Tables:**
  - Configured separate route tables for public and private subnets to control traffic flow.
  - Enabled communication between subnets and managed routing to the internet where applicable.

- **Internet Gateway & NAT Gateway:**
  - Attached an Internet Gateway to the public subnet to allow internet traffic.
  - Set up a **NAT Gateway** to allow instances in the private subnet to access the internet **without exposing them publicly**.

- **EC2 Instances:**
  - Deployed an EC2 instance in the **private subnet** for secure and isolated computing.
  - Used AMIs, security groups, and IAM roles as per security and access requirements.

- **Bastion Host (Jump Box):**
  - Launched a Bastion Host in the public subnet to act as a secure bridge for accessing private instances.
  - Configured SSH key-based access, restricting remote access only via the Bastion Host to enhance security.

🔐 Security Configuration

- Configured **Security Groups** to:
    - Allow SSH only from trusted IPs to the Bastion Host.
    - Deny direct access to private subnet instances from the internet.
    - Permit only necessary inbound/outbound traffic per instance role.

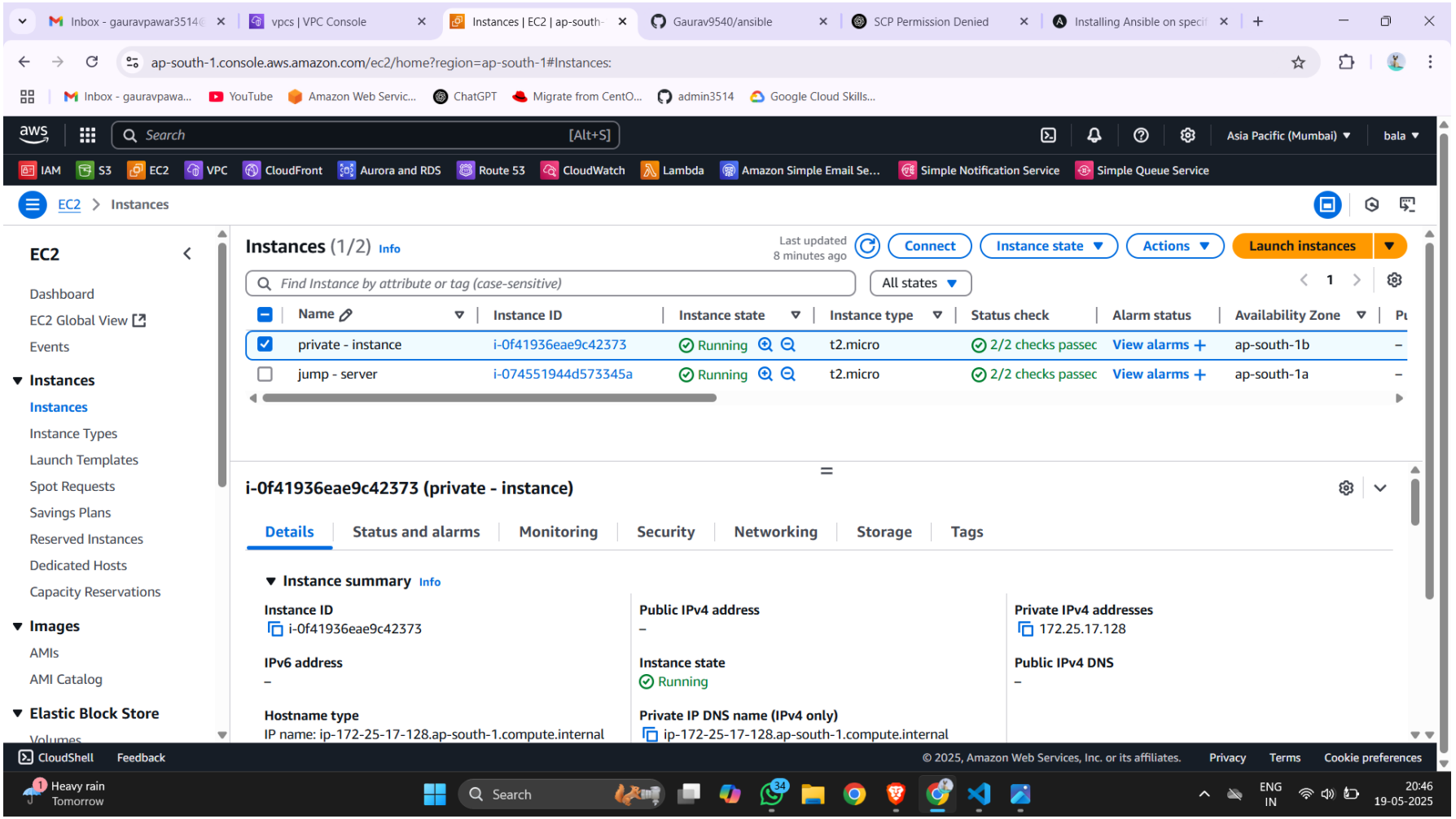
🧰 Skills & Tools Used

- **AWS Services:** EC2, VPC, Subnets, Internet Gateway, NAT Gateway, Route Tables, Bastion Host, Security Groups
- **Networking Concepts:** CIDR, NAT, SSH Tunneling, Network Isolation
- **Security Best Practices:** Principle of least privilege, restricted SSH access, private instance isolation

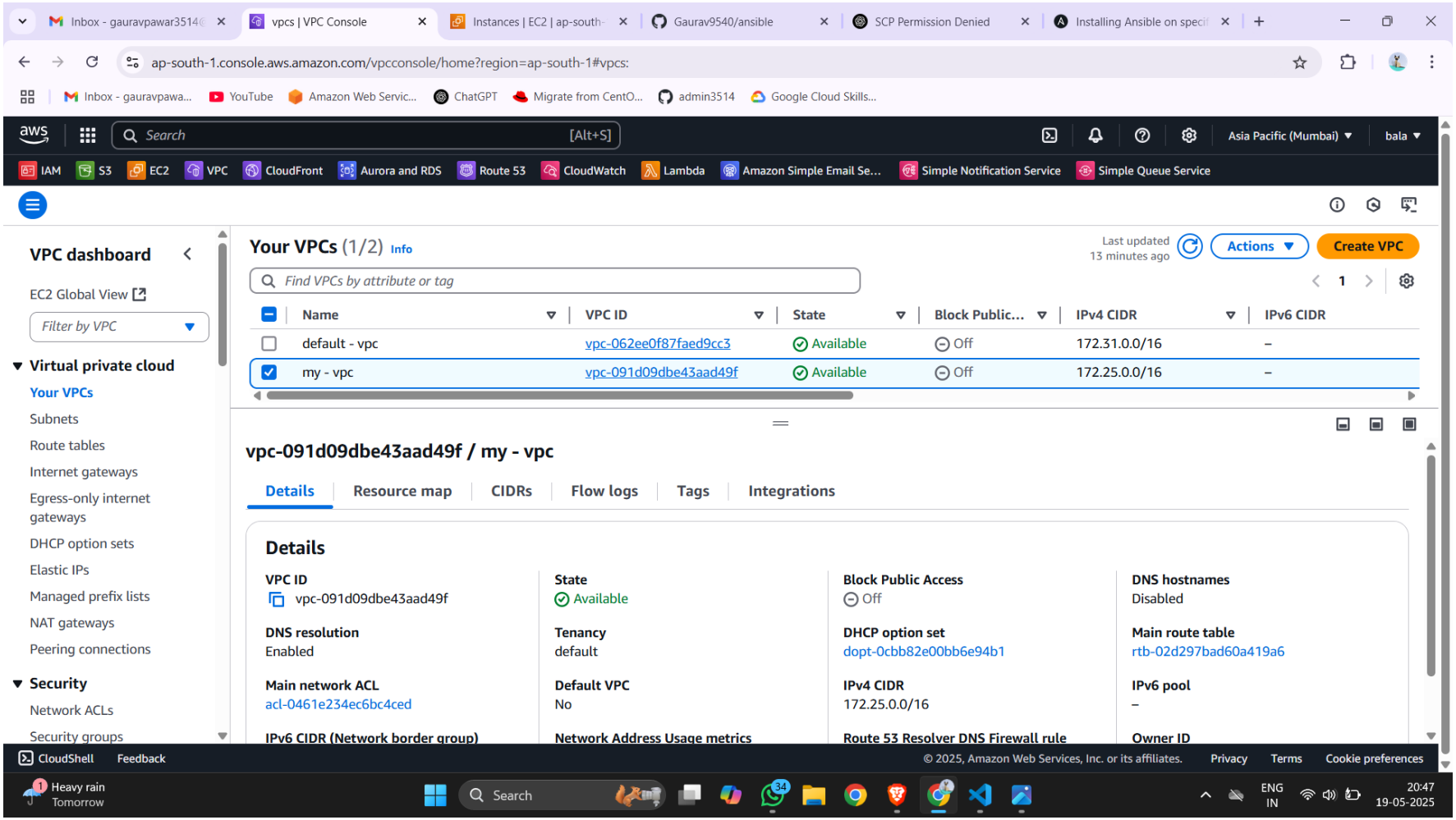
✅ Outcome

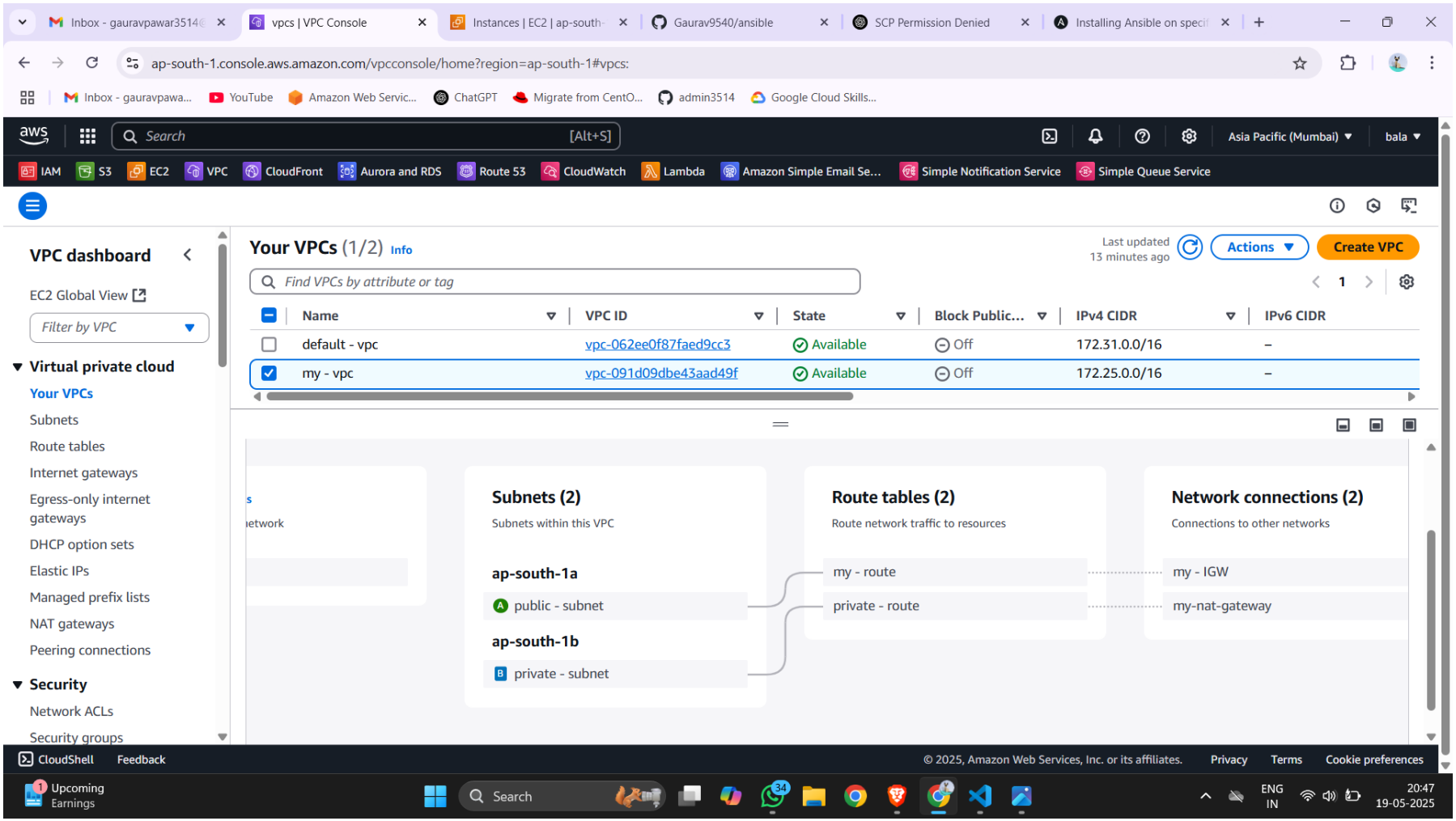
Successfully created a secure and robust private network environment in AWS. This design allows internal applications to run securely without public exposure while maintaining necessary external access through controlled and monitored pathways.

1. **EC2 Instance Setup:** Launched a **Jump Server in the public subnet** to enable SSH access, and a **Private EC2 instance in the private subnet**, configured with security groups to allow access only via the Jump Server for enhanced security.



2. **VPC Setup:** Created a custom VPC (my-vpc) with CIDR block 172.25.0.0/16, enabling DNS resolution and subnet segmentation for secure and organized cloud networking.




Inbox - gauravpawar3514
vpcs | VPC Console
Instances | EC2 | ap-south
Gaurav9540/ansible
SCP Permission Denied
Installing Ansible on speci
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#vpcs:
Search [Alt+S]
Asia Pacific (Mumbai)
bala
IAM S3 EC2 VPC CloudFront Aurora and RDS Route 53 CloudWatch Lambda Amazon Simple Email Se... Simple Notification Service Simple Queue Service
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Security
Network ACLs
Security groups
Your VPCs (1/2) Info
Last updated 13 minutes ago
Actions
Create VPC
Find VPCs by attribute or tag
Name
VPC ID
State
Block Public...
IPv4 CIDR
IPv6 CIDR
default - vpc
vpc-062ee0f87faed9cc3
Available
Off
172.31.0.0/16
my - vpc
vpc-091d09dbe43aad49f
Available
Off
172.25.0.0/16
Subnets (2)
Subnets within this VPC
ap-south-1a
public - subnet
ap-south-1b
private - subnet
Route tables (2)
Route network traffic to resources
my - route
private - route
Network connections (2)
Connections to other networks
my - IGW
my-nat-gateway
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Upcoming Earnings
Search
ENG IN
20:47
19-05-2025

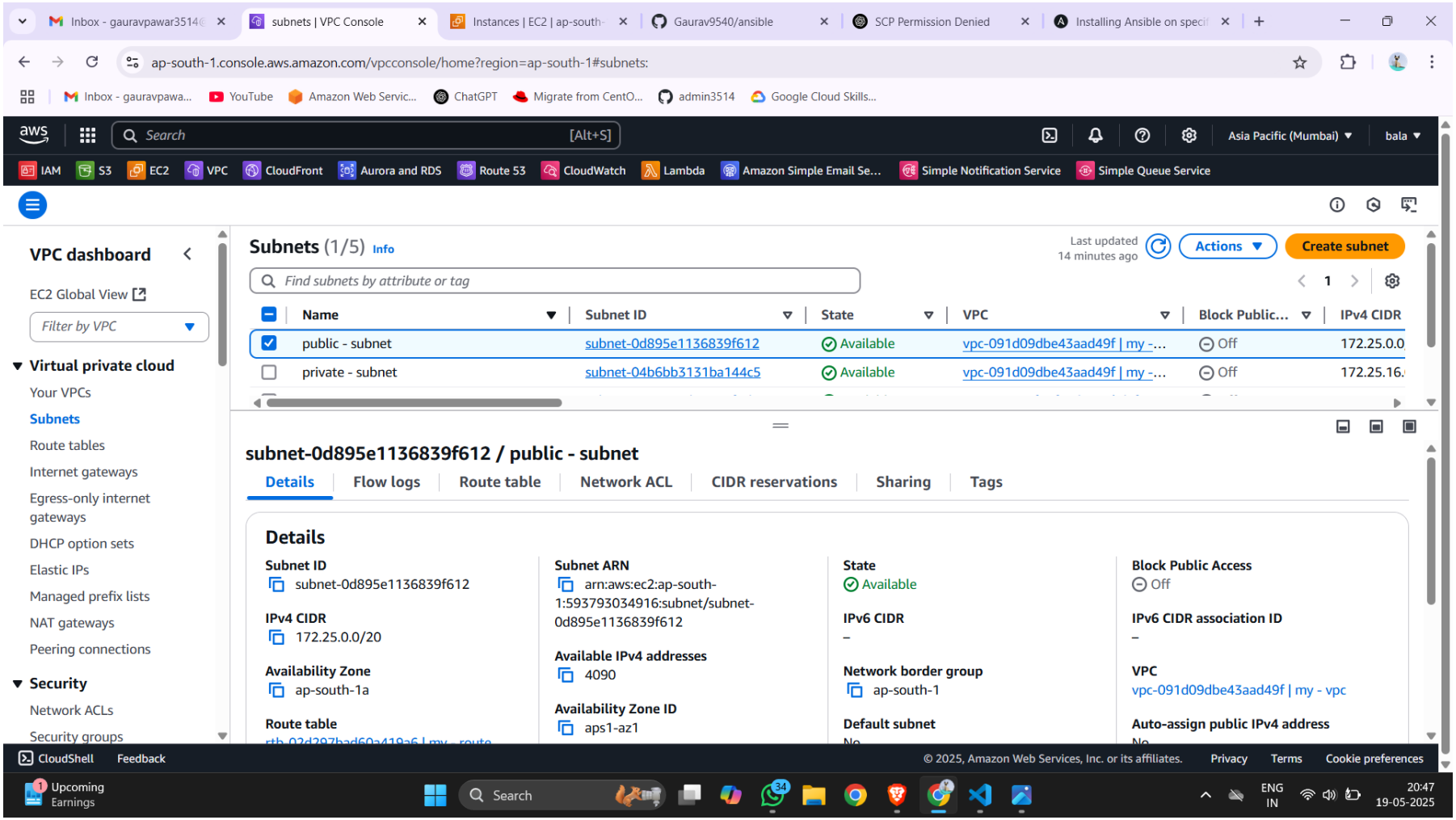
3. Subnet Creation in a Custom VPC:

In the custom VPC my-vpc, two subnets were created to support a secure and segregated network architecture:

- **Public Subnet:**
  A public subnet (public - subnet) with IPv4 CIDR block 172.25.0.0/20 was created in Availability Zone ap-south-1a. This subnet is designed to host resources that require internet access, such as a Bastion Host or NAT Gateway.

- **Private Subnet:**
  A private subnet (private - subnet) with IPv4 CIDR block 172.25.16.0/20 was created in the same VPC. This subnet is intended for resources that should not be directly accessible from the internet, such as backend servers or databases.

These subnets are key to enabling secure and organized routing within the VPC, with the public subnet facilitating controlled external access and the private subnet maintaining internal-only connectivity.


Inbox - gauravpawar3514
subnets | VPC Console
Instances | EC2 | ap-south-
Gaurav9540/ansible
SCP Permission Denied
Installing Ansible on speci
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#subnets:
Inbox - gauravpawa...
YouTube
Amazon Web Servic...
ChatGPT
Migrate from CentO...
admin3514
Google Cloud Skills...
Search
[Alt+S]
Asia Pacific (Mumbai)
bala
IAM
S3
EC2
VPC
CloudFront
Aurora and RDS
Route 53
CloudWatch
Lambda
Amazon Simple Email Se...
Simple Notification Service
Simple Queue Service
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Security
Network ACLs
Security groups
Subnets (1/5) Info
Last updated 14 minutes ago
Actions
Create subnet
Find subnets by attribute or tag
Name
Subnet ID
State
VPC
Block Public...
IPv4 CIDR
public - subnet
subnet-0d895e1136839f612
Available
vpc-091d09dbe43aad49f | my -...
Off
172.25.0.0
private - subnet
subnet-04b6bb3131ba144c5
Available
vpc-091d09dbe43aad49f | my -...
Off
172.25.16.
subnet-0d895e1136839f612 / public - subnet
Details
Flow logs
Route table
Network ACL
CIDR reservations
Sharing
Tags
Details
Subnet ID
subnet-0d895e1136839f612
IPv4 CIDR
172.25.0.0/20
Availability Zone
ap-south-1a
Route table
Subnet ARN
arn:aws:ec2:ap-south-1:593793034916:subnet/subnet-0d895e1136839f612
Available IPv4 addresses
4090
Availability Zone ID
aps1-az1
State
Available
IPv6 CIDR
–
Network border group
ap-south-1
Default subnet
Block Public Access
Off
IPv6 CIDR association ID
–
VPC
vpc-091d09dbe43aad49f | my - vpc
Auto-assign public IPv4 address
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Upcoming Earnings
Search
ENG IN
20:47
19-05-2025

4. Route Table Configuration in VPC

To enable proper routing and traffic management between public and private subnets in the my-vpc, two route tables were configured:

- **Public Route Table:**
  This route table is associated with the **public subnet**.

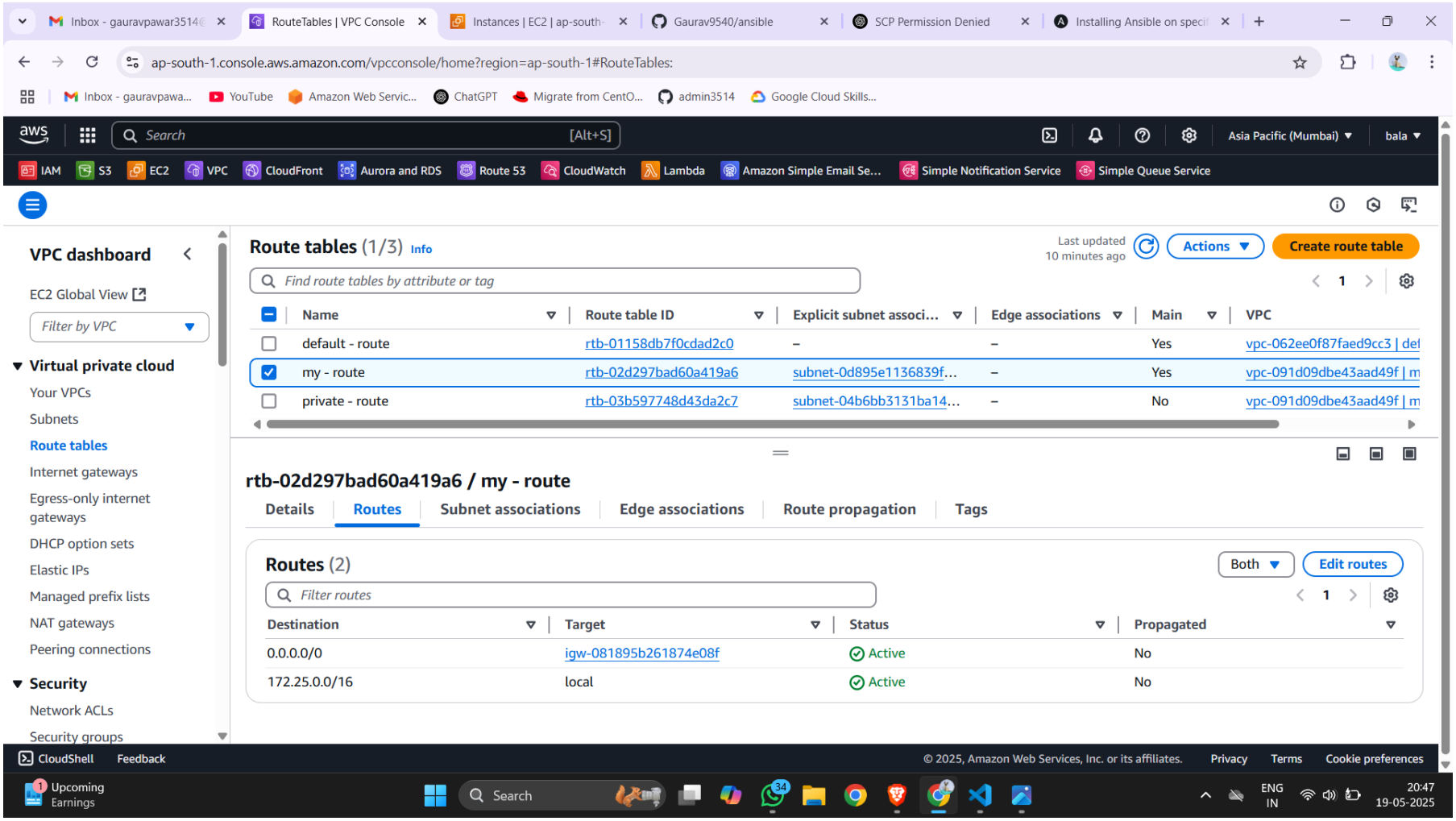
- **Destination:** 0.0.0.0/0

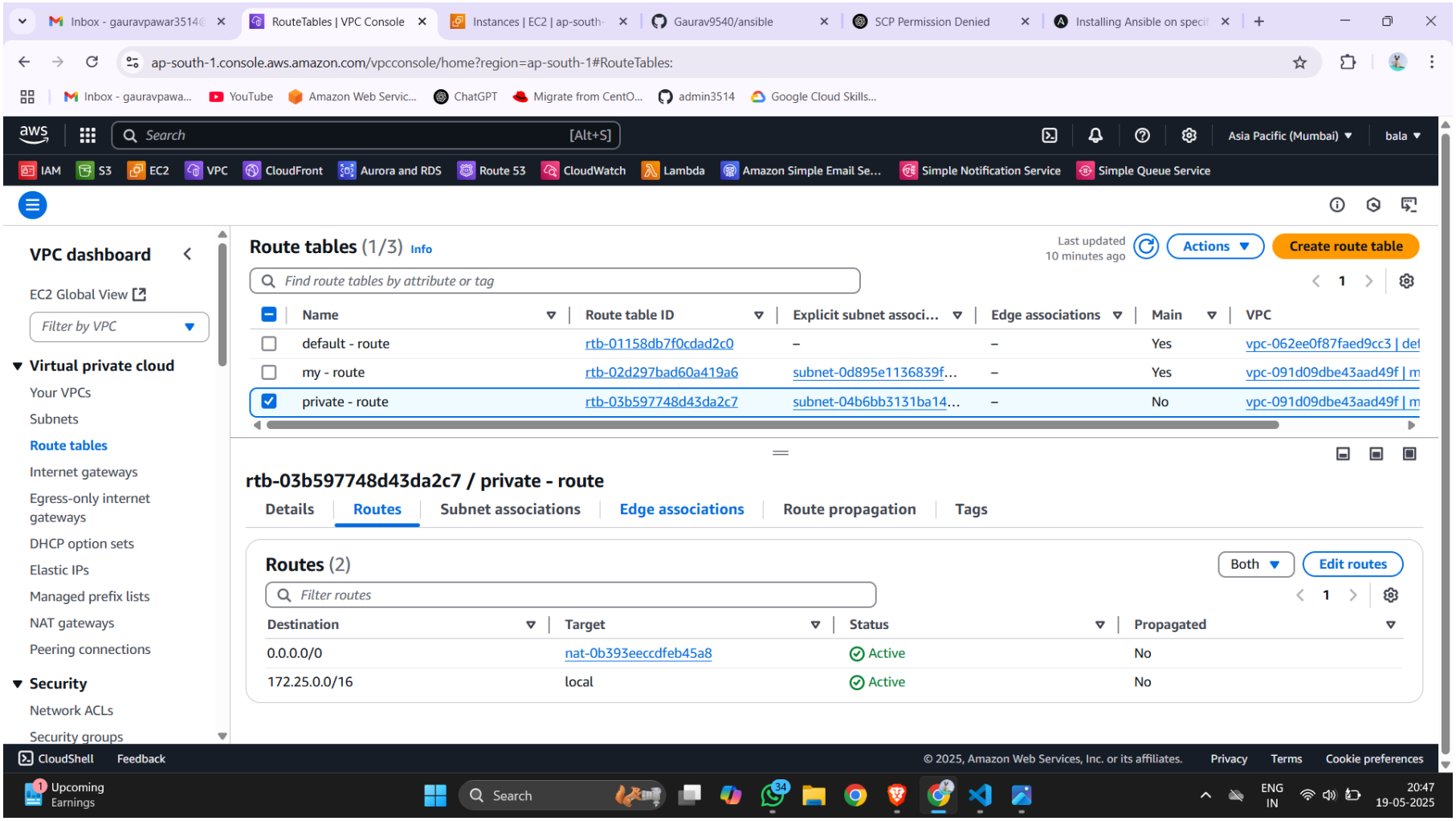
- **Target:** Internet Gateway (IGW)
  This configuration allows all outbound traffic from the public subnet to reach the internet via the Internet Gateway. It is typically used for resources like Bastion Hosts or NAT Gateways that require direct internet access.

- **Private Route Table:**
  This route table is associated with the **private subnet**.

- **Destination:** 0.0.0.0/0

- **Target:** NAT Gateway
  This allows resources in the private subnet (such as EC2 instances) to access the internet **for updates or external API calls**, while still keeping them **inaccessible from the internet**, thereby ensuring higher security.


RouteTables | VPC Console
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#RouteTables:
Search [Alt+S]
Asia Pacific (Mumbai)
bala
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Security
Network ACLs
Security groups
Route tables (1/3) Info
Last updated 10 minutes ago
Actions
Create route table
Find route tables by attribute or tag
Name
Route table ID
Explicit subnet associ...
Edge associations
Main
VPC
default - route
rtb-01158db7f0cdad2c0
Yes
my - route
rtb-02d297bad60a419a6
subnet-0d895e1136839f...
Yes
private - route
rtb-03b597748d43da2c7
subnet-04b6bb3131ba14...
No
rtb-02d297bad60a419a6 / my - route
Details
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (2)
Both
Edit routes
Filter routes
Destination
Target
Status
Propagated
0.0.0.0/0
igw-081895b261874e08f
Active
No
172.25.0.0/16
local
Active
No
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Upcoming Earnings
Search
ENG IN
20:47
19-05-2025


Inbox - gauravpawar3514
RouteTables | VPC Console
Instances | EC2 | ap-south-
Gaurav9540/ansible
SCP Permission Denied
Installing Ansible on specif
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#RouteTables:
Inbox - gauravpawa...
YouTube
Amazon Web Servic...
ChatGPT
Migrate from CentO...
admin3514
Google Cloud Skills...
aws
Search
[Alt+S]
Asia Pacific (Mumbai)
bala
IAM
S3
EC2
VPC
CloudFront
Aurora and RDS
Route 53
CloudWatch
Lambda
Amazon Simple Email Se...
Simple Notification Service
Simple Queue Service
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Security
Network ACLs
Security groups
Route tables (1/3) Info
Last updated 10 minutes ago
Actions
Create route table
Find route tables by attribute or tag
Name
Route table ID
Explicit subnet associ...
Edge associations
Main
VPC
default - route
rtb-01158db7f0cdad2c0
–
–
Yes
vpc-062ee0f87faed9cc3 | def
my - route
rtb-02d297bad60a419a6
subnet-0d895e1136839f...
–
Yes
vpc-091d09dbe43aad49f | m
private - route
rtb-03b597748d43da2c7
subnet-04b6bb3131ba14...
–
No
vpc-091d09dbe43aad49f | m
rtb-03b597748d43da2c7 / private - route
Details
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (2)
Both
Edit routes
Filter routes
Destination
Target
Status
Propagated
0.0.0.0/0
nat-0b393eeccdfeb45a8
Active
No
172.25.0.0/16
local
Active
No
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Upcoming Earnings
Search
ENG IN
20:47
19-05-2025

5. Internet Gateway (IGW) Configuration

As part of the VPC setup, an **Internet Gateway** was created and attached to the custom VPC (my-vpc) to enable internet access for resources in the public subnet.

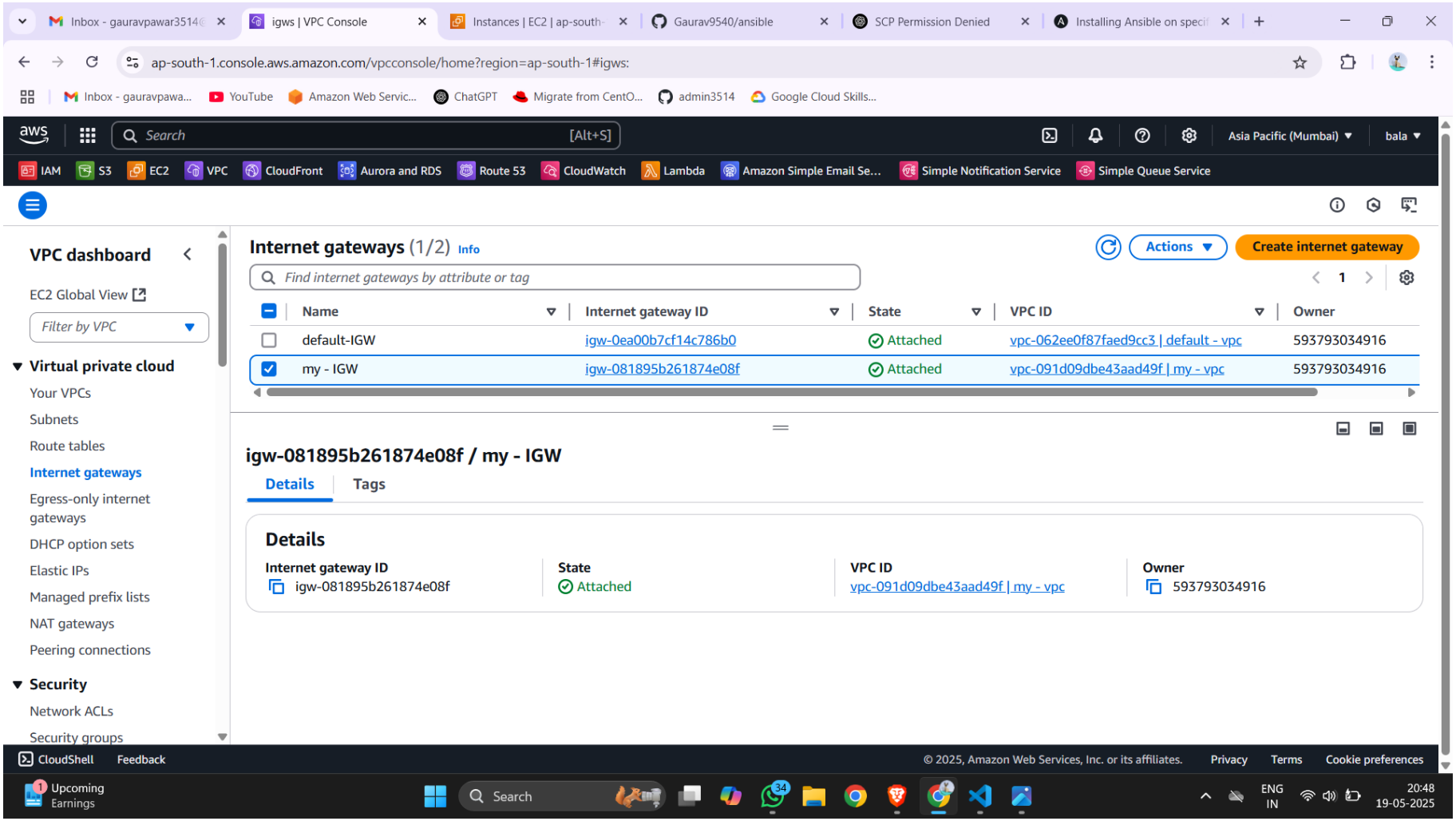
- Purpose: The Internet Gateway allows instances in the **public subnet** to **send and receive traffic to and from the internet**. It is a **highly available, horizontally scaled, and redundant VPC component** that acts as the bridge between the VPC and the internet.
- Attachment: The IGW was **attached to my-vpc** and associated with the **public route table**.
- Route Table Entry:

  In the **public route table**, a route was added with:

  Destination: 0.0.0.0/0

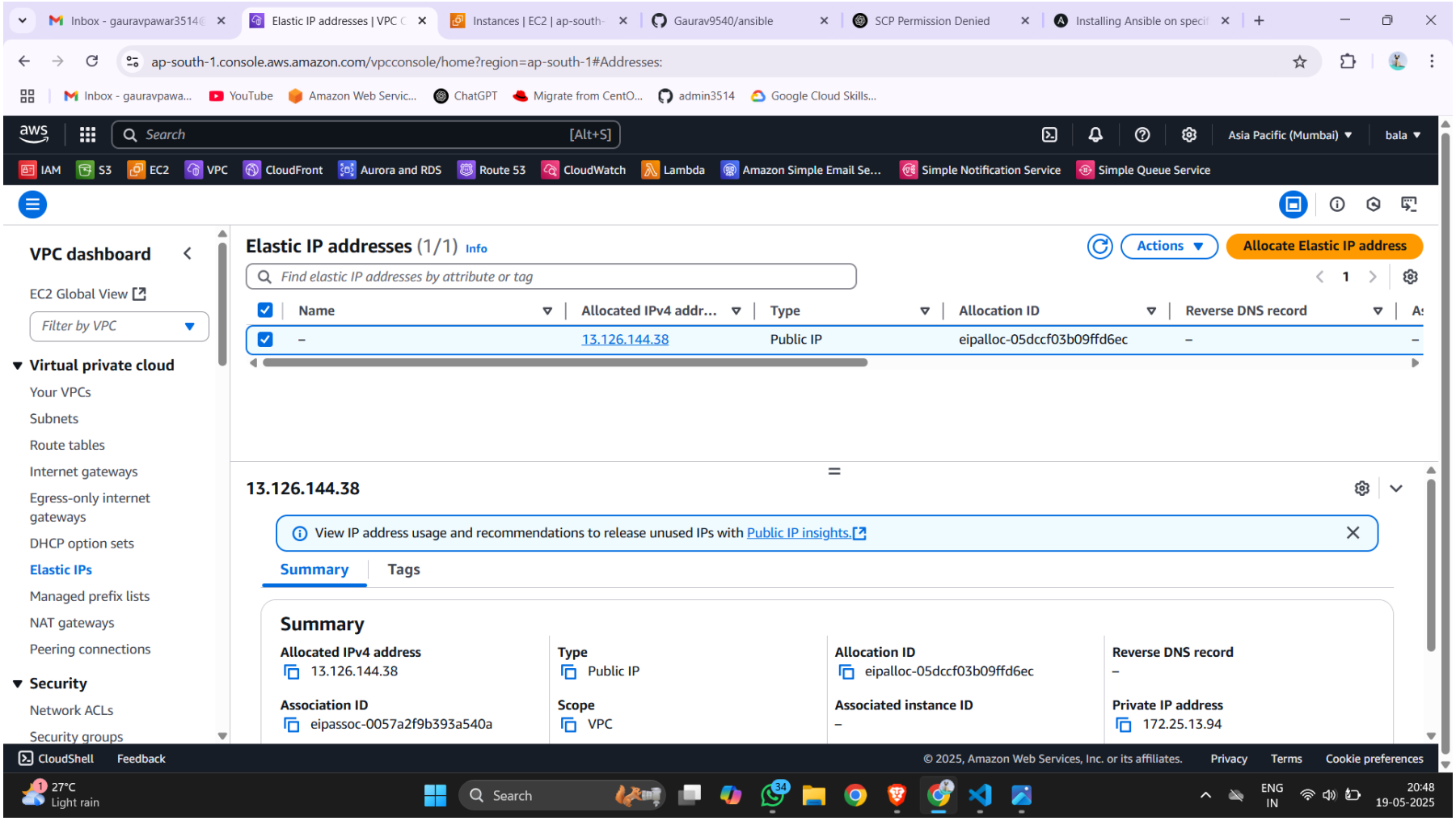
  Target: The attached **Internet Gateway**
  This route enables all outbound internet traffic from instances in the public subnet to go through the IGW.

  The Internet Gateway is essential for services like **bastion hosts**, **public-facing web servers**, or any resources that require **direct access to and from the internet**.


Inbox - gauravpawar3514
igws | VPC Console
Instances | EC2 | ap-south-
Gaurav9540/ansible
SCP Permission Denied
Installing Ansible on speci
ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#igws:
Inbox - gauravpawa...
YouTube
Amazon Web Servic...
ChatGPT
Migrate from CentO...
admin3514
Google Cloud Skills...
aws
Search
[Alt+S]
Asia Pacific (Mumbai)
bala
IAM
S3
EC2
VPC
CloudFront
Aurora and RDS
Route 53
CloudWatch
Lambda
Amazon Simple Email Se...
Simple Notification Service
Simple Queue Service
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Security
Network ACLs
Security groups
Internet gateways (1/2) Info
Actions
Create internet gateway
Find internet gateways by attribute or tag
Name
Internet gateway ID
State
VPC ID
Owner
default-IGW
igw-0ea00b7cf14c786b0
Attached
vpc-062ee0f87faed9cc3 | default - vpc
593793034916
my - IGW
igw-081895b261874e08f
Attached
vpc-091d09dbe43aad49f | my - vpc
593793034916
igw-081895b261874e08f / my - IGW
Details
Tags
Details
Internet gateway ID
igw-081895b261874e08f
State
Attached
VPC ID
vpc-091d09dbe43aad49f | my - vpc
Owner
593793034916
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Upcoming Earnings
Search
ENG IN
20:48
19-05-2025

6. Elastic IP (EIP) Address Configuration

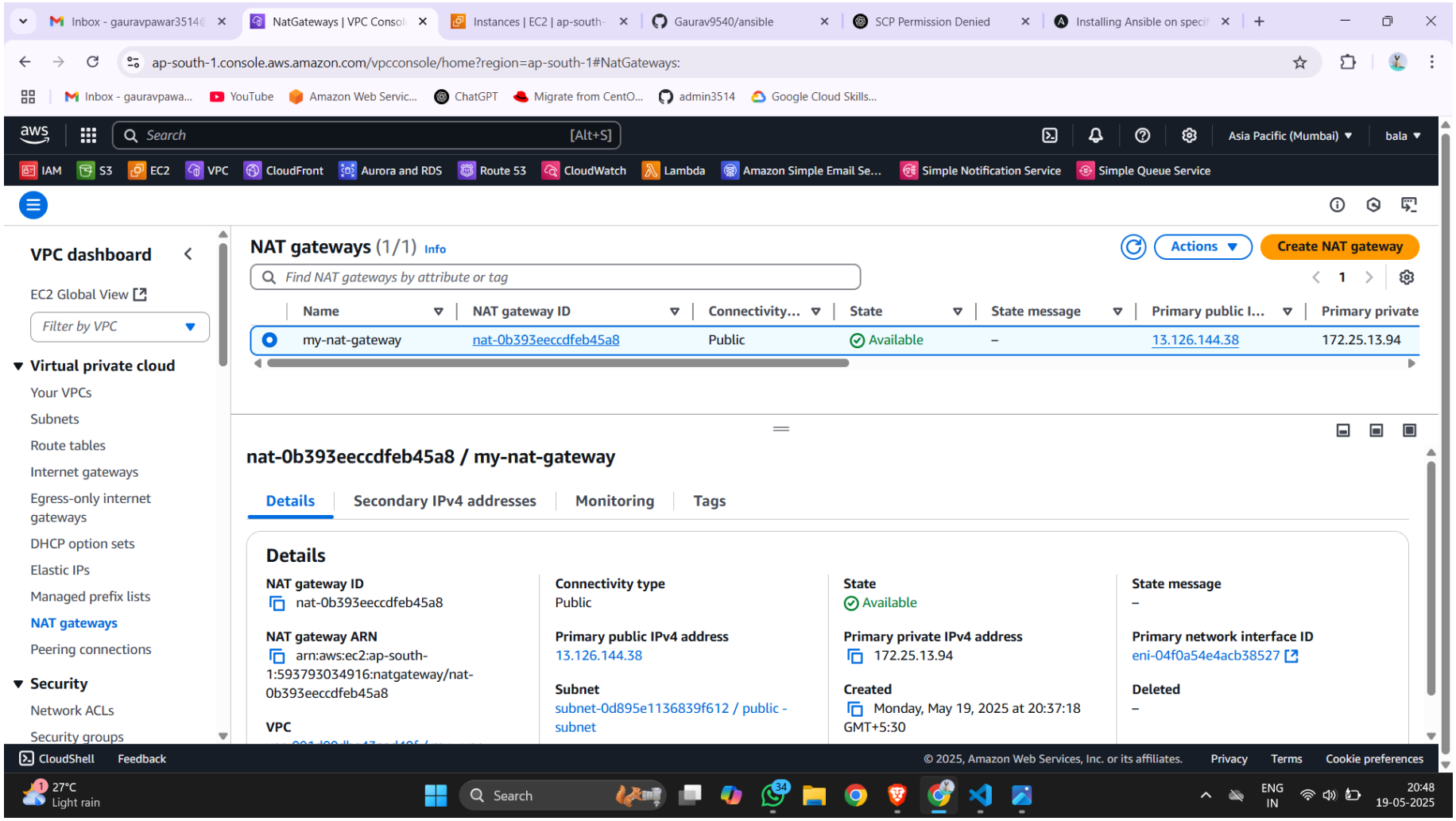
Elastic IP provides a static, public IPv4 address for dynamic cloud computing, allowing consistent access to an EC2 instance even after restarts.



7. NAT Gateway Configuration

A NAT Gateway is deployed in a public subnet with an Elastic IP to enable private subnet instances to access the internet securely, without allowing inbound traffic.

This involves allocating an Elastic IP, selecting a public subnet for deployment, and updating route tables for private subnets to forward internet-bound traffic through the NAT Gateway.



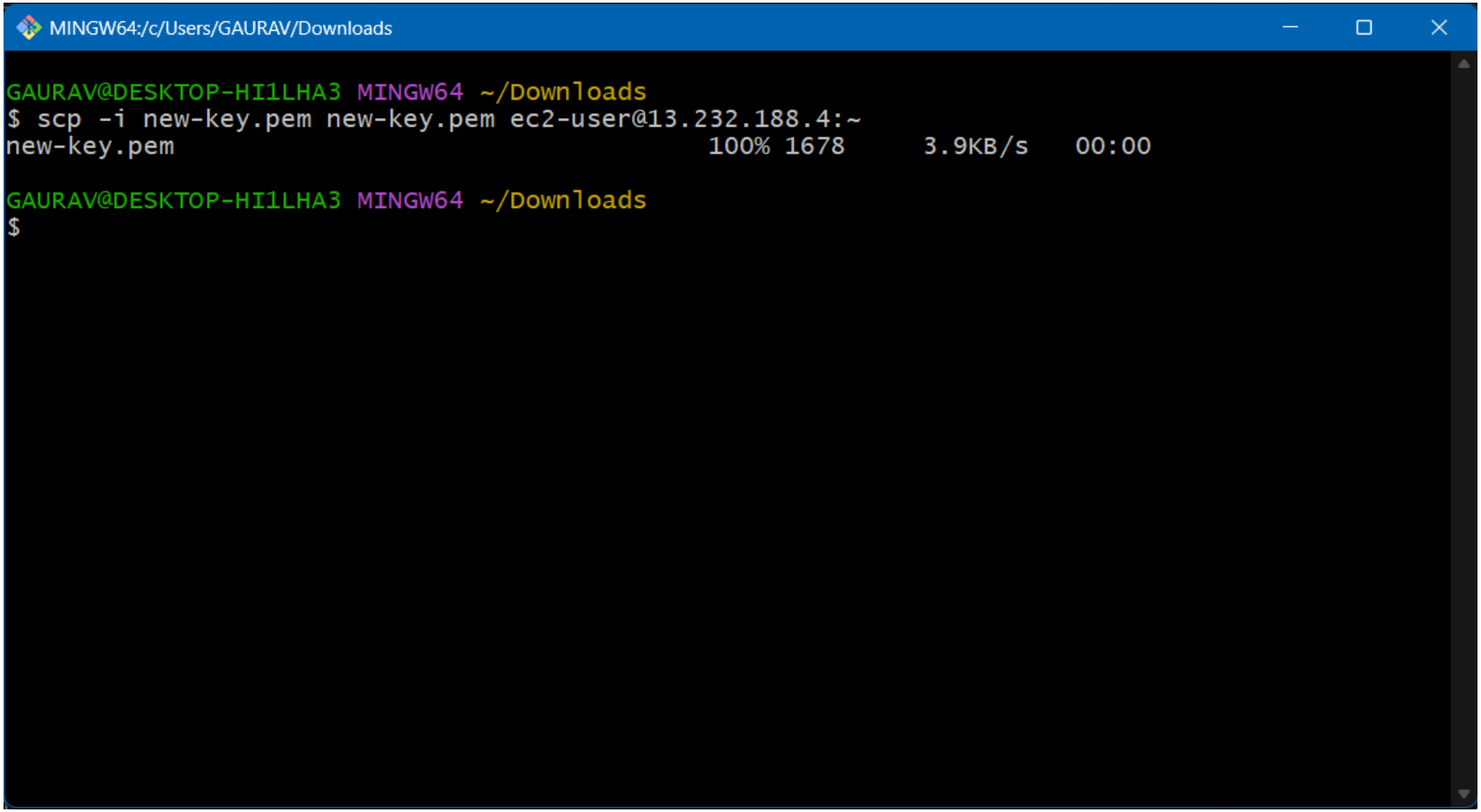
8. Transferring SSH Key to Jump Server for Private Instance Access

To securely access a private EC2 instance, the SSH private key is copied from the local machine to the jump server (bastion host) using the **scp** command. This allows the jump server to act as an intermediary for SSH connections into the private instance via key-based authentication.

The key transfer can be done with:

scp -i <local-private-key.pem> <key-to-transfer.pem> ubuntu@<jump-server-ip>:/home/ubuntu/

This command authenticates using the local key and securely transfers the private key to the jump server's home directory.

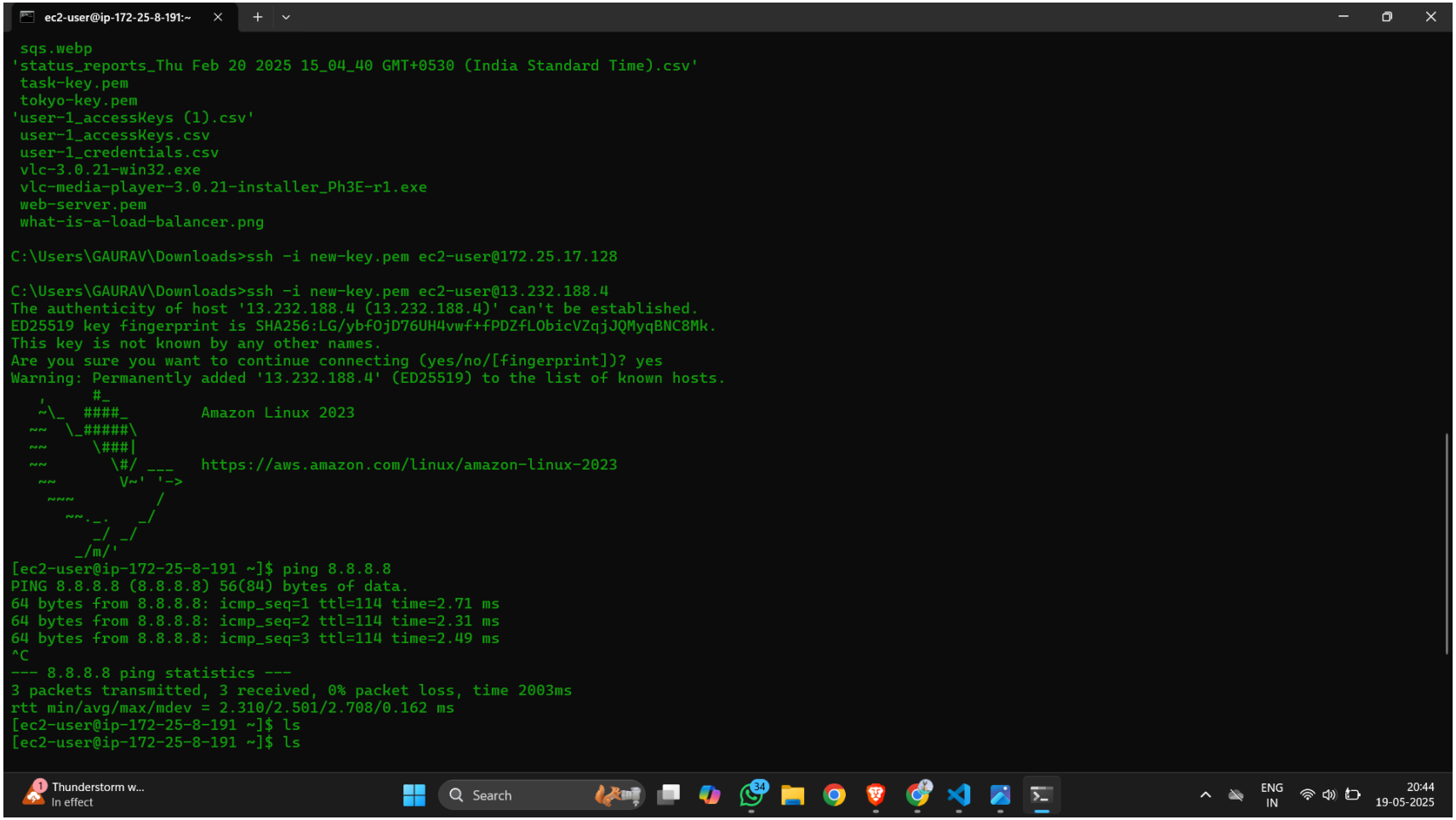


9. SSH Access to Jump Server from Local Machine

To initiate a secure connection to the jump server (bastion host), SSH is used from the local machine with the appropriate private key. This allows access to internal network resources by forwarding traffic through the jump server. It's essential to ensure the private key permissions are correctly set (typically chmod 600) to prevent unauthorized access.

Here’s the SSH command to connect to a jump server (bastion host) using a private key:

ssh -i <local-private-key.pem> ubuntu@<jump-server-ip>

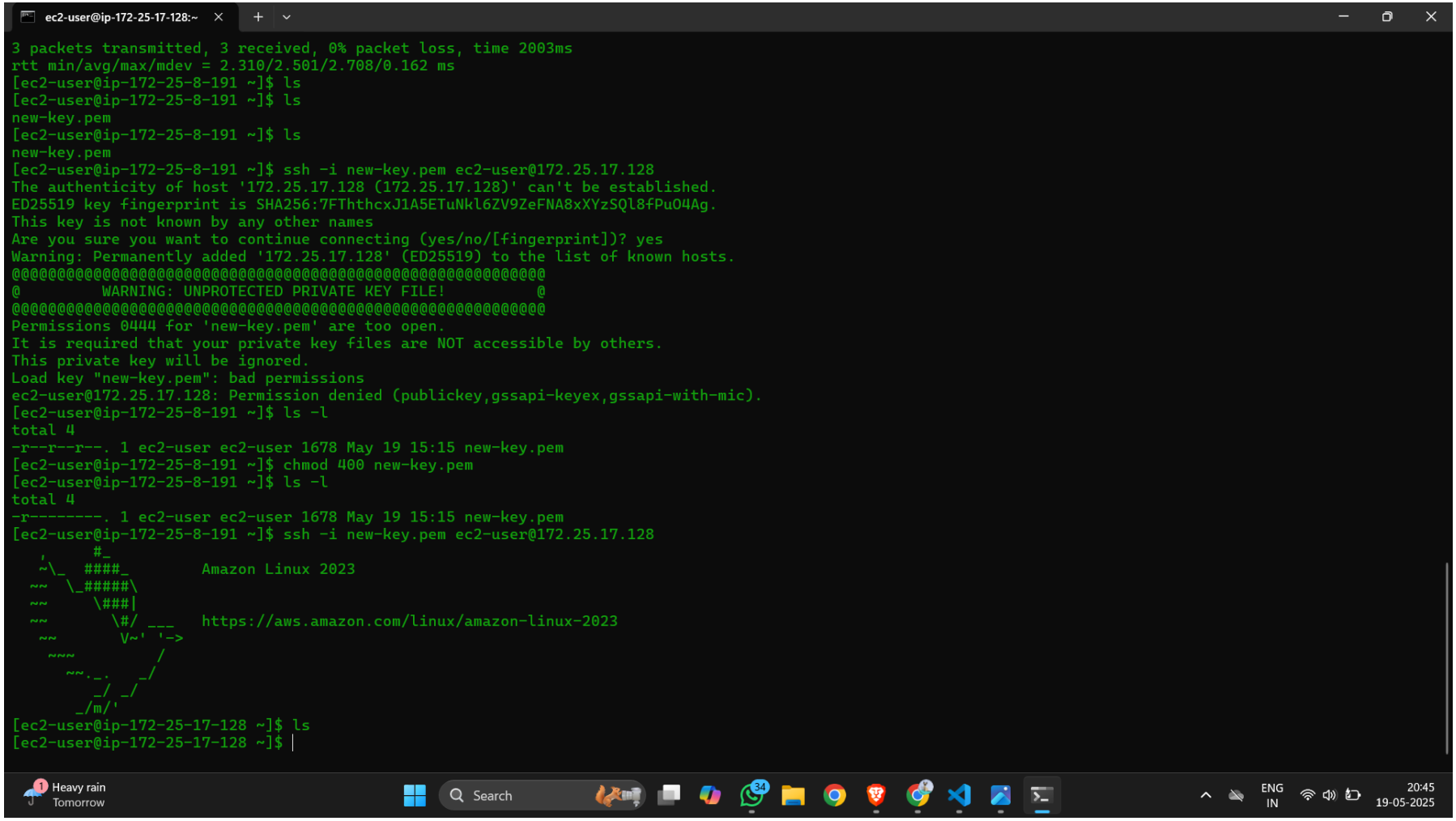


10. SSH into a Private EC2 Instance via a Jump Server (Bastion Host)

To securely connect to a private EC2 instance (not publicly accessible), you can route your SSH session through a public-facing bastion host (jump server). This setup allows indirect access to the private instance without exposing it to the internet.

Here's how to do it using SSH agent forwarding or a ProxyJump:

ssh -i /path/to/private_key.pem -J user@bastion_host user@private_instance_ip

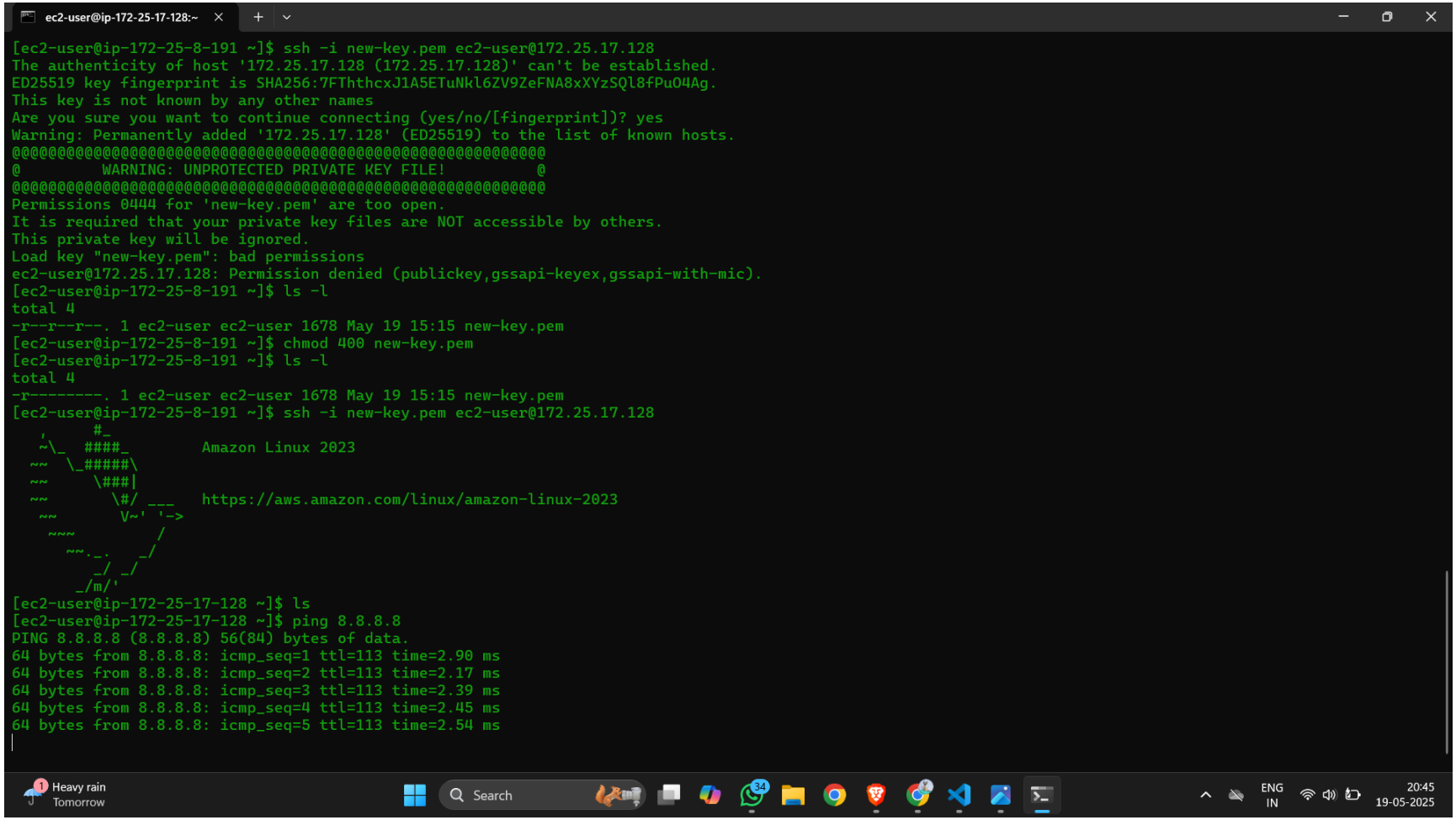


11. Verifying Internet Connectivity on a Private Instance Using ping

After successfully SSH into the private instance through the jump server, it's important to confirm that the instance has internet access—especially if it's within a private subnet. This ensures that it can reach external services, download updates, or connect to APIs.

✅ Step to Check Internet Connectivity Once you're logged into the private instance:

ping 8.8.8.8 or ping www.google.com



12. Performing Installations and Updates on a Private Instance After Verifying Internet Access

Once internet connectivity has been confirmed on the private instance using the ping command, you can proceed with various system operations that require external access. These include installing software packages, updating system dependencies, and downloading necessary files or configurations from the internet.