

**School of Computer Science, Engineering and Applications (SCSEA)**

**B. Tech TY (CCSA)**

**Subject: Cloud Architecture And Protocol**

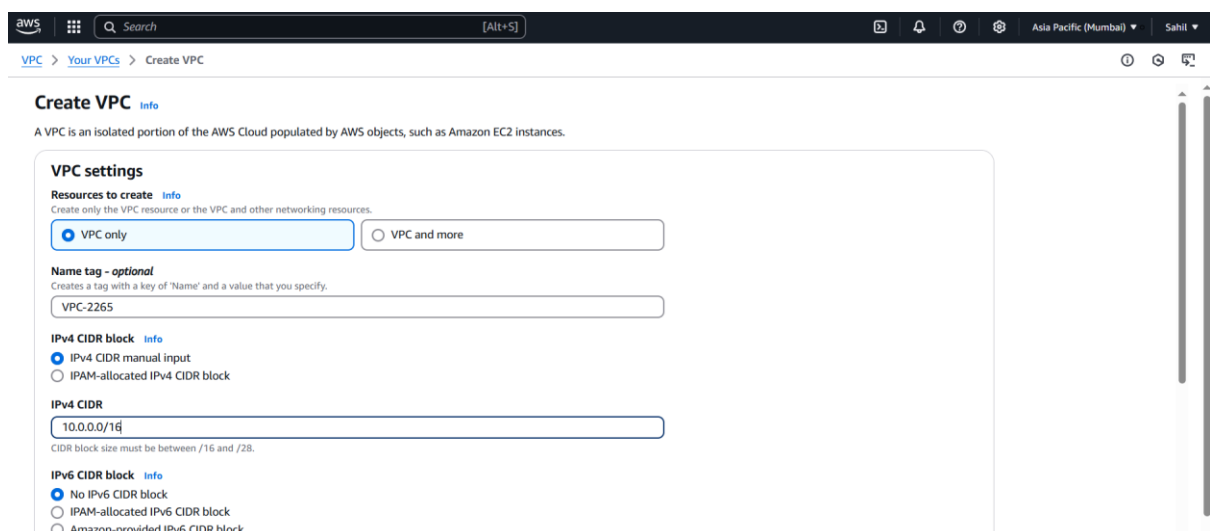
**Name of the Student: Sahil S. Mandawgade**

**PRN: 20220802265**

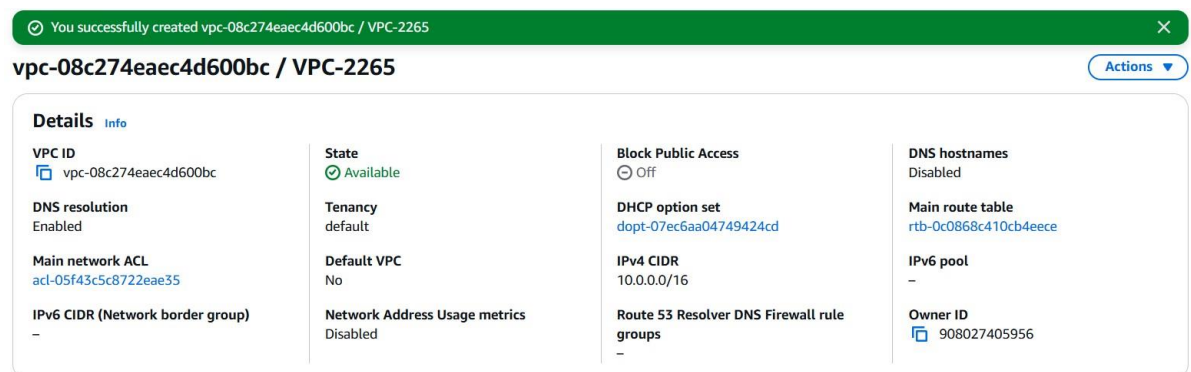
**Title of Practical: 2. Building a Dual-Subnet Architecture on AWS:  
Secure Communication Between Public and  
Private Instances with NAT Gateway.**

**Step 1: Create VPC.**

- Log-in to Your AWS Console.
- Search "VPC" in AWS search bar and enter VPC Dashboard.
- Go to "Your VPCs" - you will have your default VPC > Click on "Create VPC"
- Assign name & CIDR: 10.0.0.0/16 - Click "Create VPC".



- VPC Successfully Created.



**School of Computer Science, Engineering and Applications (SCSEA)**

**B. Tech TY (CCSA)**

**Subject: Cloud Architecture And Protocol**

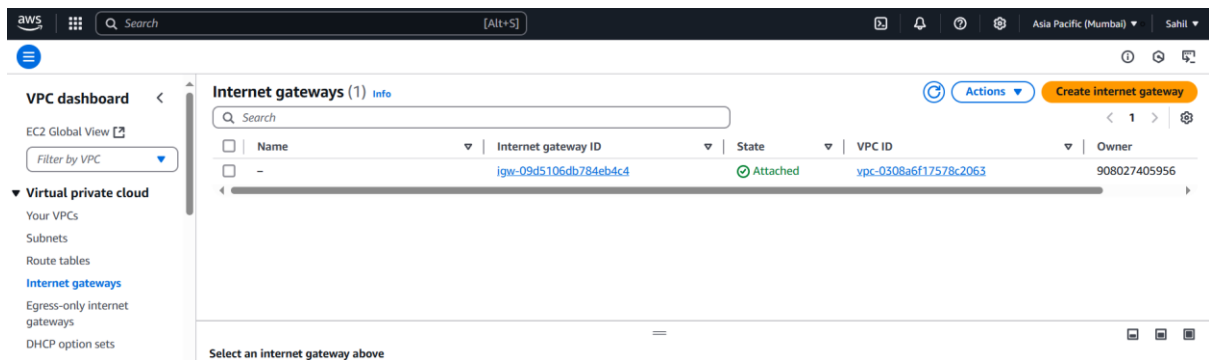
**Name of the Student: Sahil S. Mandawgade**

**PRN: 20220802265**

**Title of Practical: 2. Building a Dual-Subnet Architecture on AWS:  
Secure Communication Between Public and  
Private Instances with NAT Gateway.**

**Step 2: Creation of Internet Gateway (IGW).**

- Under Virtual Private Cloud (sidebar) - Internet Gateway - Create internet gateway.
- Note: There will be a default IGW to the default VPC, do not delete it.



- Assign IGW Name - Create IGW.

**Create internet gateway** [Info](#)

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

**Internet gateway settings**

**Name tag**

Creates a tag with a key of 'Name' and a value that you specify.

IGW-2265

**Tags - optional**

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

**Key**

Q Name

**Value - optional**

Q IGW-2265

Remove

Add new tag

You can add 49 more tags.

Cancel

Create internet gateway

- IGW Dashboard - Select your new IGW - Actions - Attach VPC.
- Select Your VPC - Attach IGW.

## School of Computer Science, Engineering and Applications (SCSEA)

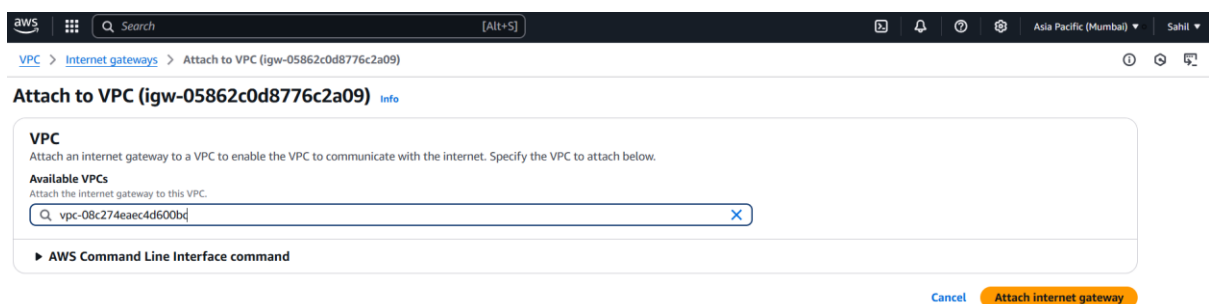
### B. Tech TY (CCSA)

### Subject: Cloud Architecture And Protocol

**Name of the Student:** Sahil S. Mandawgade

**PRN:** 20220802265

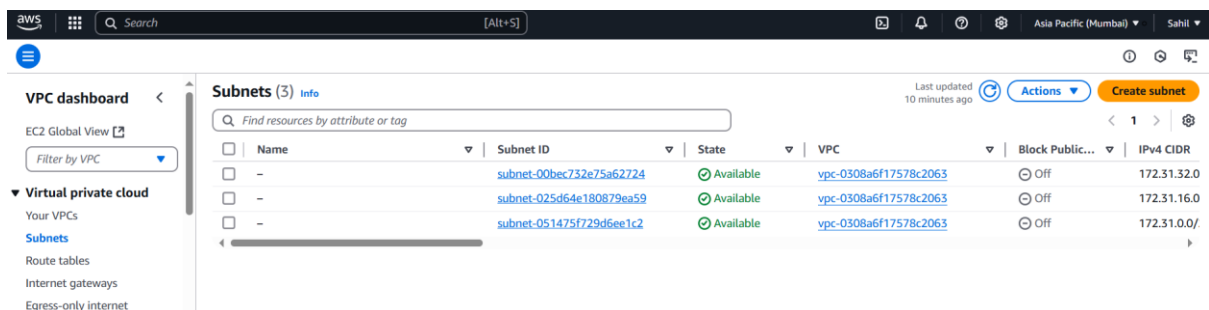
**Title of Practical:** 2. Building a Dual-Subnet Architecture on AWS:  
Secure Communication Between Public and  
Private Instances with NAT Gateway.



The screenshot shows the AWS console 'Attach to VPC' page. The breadcrumb trail is 'VPC > Internet gateways > Attach to VPC (igw-05862c0d8776c2a09)'. The main heading is 'Attach to VPC (igw-05862c0d8776c2a09)'. Below this, there's a section 'VPC' with the instruction 'Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.' Under 'Available VPCs', there's a search bar with the text 'vpc-08c274eae4d600bd' and a blue 'X' icon. At the bottom right, there are two buttons: 'Cancel' and 'Attach internet gateway'.

### Step 3: Create Public and Private Subnet.

- Under Virtual Private Cloud - Subnets - Create subnet.



The screenshot shows the AWS console 'Subnets' page. The breadcrumb trail is 'VPC dashboard > Subnets (3)'. The main heading is 'Subnets (3)'. Below this, there's a search bar with the text 'Find resources by attribute or tag'. The table below shows the following data:

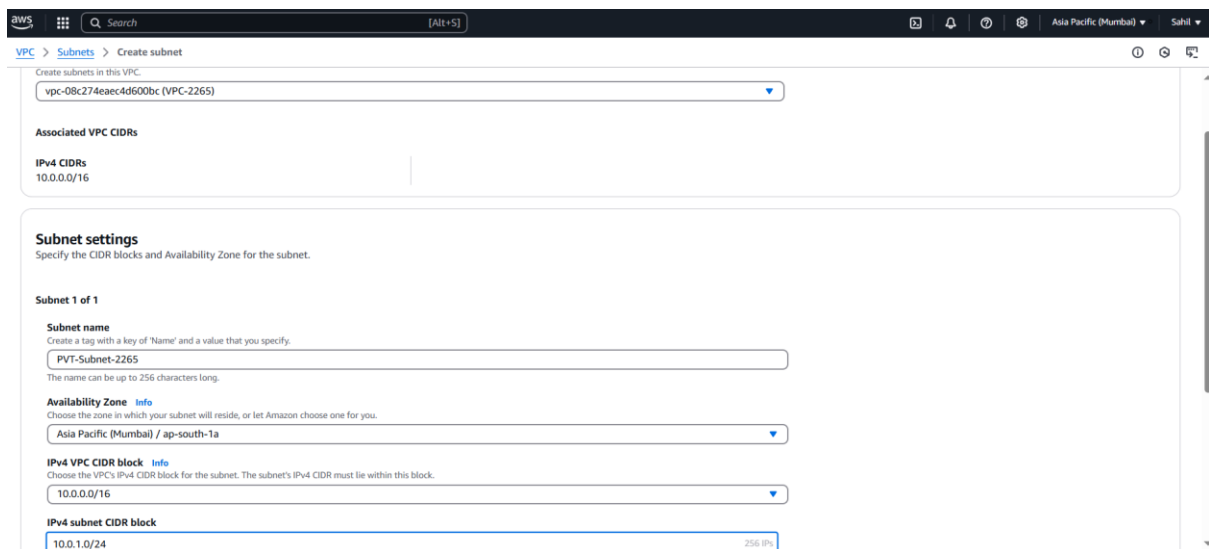
Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
-	subnet-00bec732e75a62724	Available	vpc-0308a6f17578c2063	Off	172.31.32.0
-	subnet-025d64e180879ea59	Available	vpc-0308a6f17578c2063	Off	172.31.16.0
-	subnet-051475f729d6ee1c2	Available	vpc-0308a6f17578c2063	Off	172.31.0.0

- Select your VPC - Assign Name: Private subnet - Assign CIDR: 10.0.1.0/24 - Create Subnet.

**School of Computer Science, Engineering and Applications (SCSEA)**  
**B. Tech TY (CCSA)**  
**Subject: Cloud Architecture And Protocol**

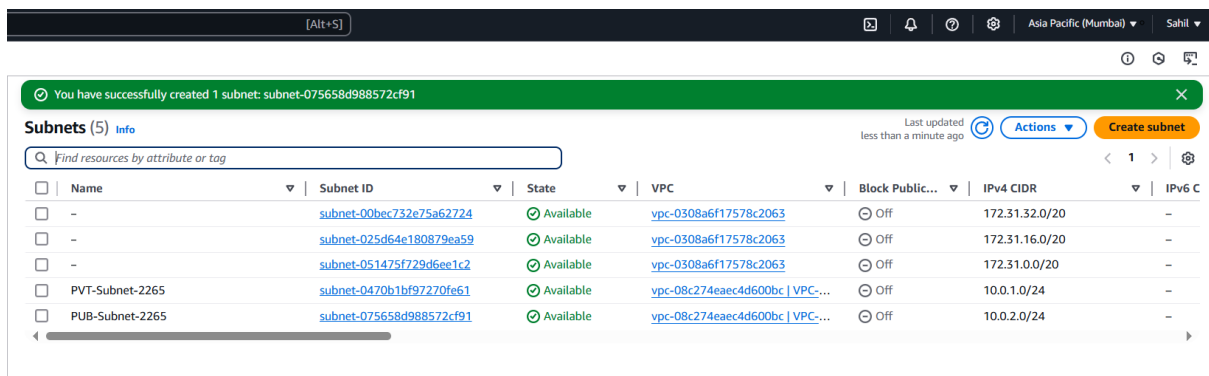
**Name of the Student: Sahil S. Mandawgade** **PRN: 20220802265**

**Title of Practical: 2. Building a Dual-Subnet Architecture on AWS:  
Secure Communication Between Public and  
Private Instances with NAT Gateway.**



The screenshot shows the 'Create subnet' page in the AWS Management Console. The 'Associated VPC' is 'vpc-08c274eae4d600bc (VPC-2265)'. The 'IPv4 CIDR' is '10.0.0/16'. Under 'Subnet settings', 'Subnet 1 of 1' is configured with the name 'PVT-Subnet-2265', 'Availability Zone' set to 'Asia Pacific (Mumbai) / ap-south-1a', and 'IPv4 VPC CIDR block' set to '10.0.0/16'. The 'IPv4 subnet CIDR block' is '10.0.1.0/24'.

- Create Another Subnet named “Public Subnet” with CIDR: 10.0.2.0/24.
- Successful Creation of 2 Subnets.



The screenshot shows the 'Subnets' list in the AWS Management Console. A green notification bar at the top states: 'You have successfully created 1 subnet: subnet-075658d988572cf91'. The table below lists 5 subnets.

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	IPv6 C
-	subnet-00bec732e75a62724	Available	vpc-0308a6f17578c2063	Off	172.31.32.0/20	-
-	subnet-025d64e180879ea59	Available	vpc-0308a6f17578c2063	Off	172.31.16.0/20	-
-	subnet-051475f729d6ee1c2	Available	vpc-0308a6f17578c2063	Off	172.31.0.0/20	-
PVT-Subnet-2265	subnet-0470b1bf927270fe61	Available	vpc-08c274eae4d600bc   VPC-...	Off	10.0.1.0/24	-
PUB-Subnet-2265	subnet-075658d988572cf91	Available	vpc-08c274eae4d600bc   VPC-...	Off	10.0.2.0/24	-

**Step 4: Attaching NACL.**

- Under security - Network ACLs - Create NACL.
- Select your VPC & Assign NACL Name - Create NACL.

## School of Computer Science, Engineering and Applications (SCSEA)

### B. Tech TY (CCSA)

### Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

### Title of Practical: 2. Building a Dual-Subnet Architecture on AWS: Secure Communication Between Public and Private Instances with NAT Gateway.

#### Create network ACL Info

A network ACL is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet.

##### Network ACL settings

###### Name - optional

Creates a tag with a key of 'Name' and a value that you specify.

NACL-2265

###### VPC

VPC to use for this network ACL.

vpc-08c274eac4d600bc (VPC-2265)

##### Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

###### Key

Q Name

###### Value - optional

Q NACL-2265

Remove tag

Add tag

You can add 49 more tags

Cancel

Create network ACL

- Select your NACL - Inbound Rules - Edit Inbound Rules.
- Assign Rule Number: 100 - Allow all traffic - Save Changes.



- Select your NACL - Outbound Rules - Edit Outbound Rules.
- Assign Rule Number: 100 - Allow all traffic - Save Changes.

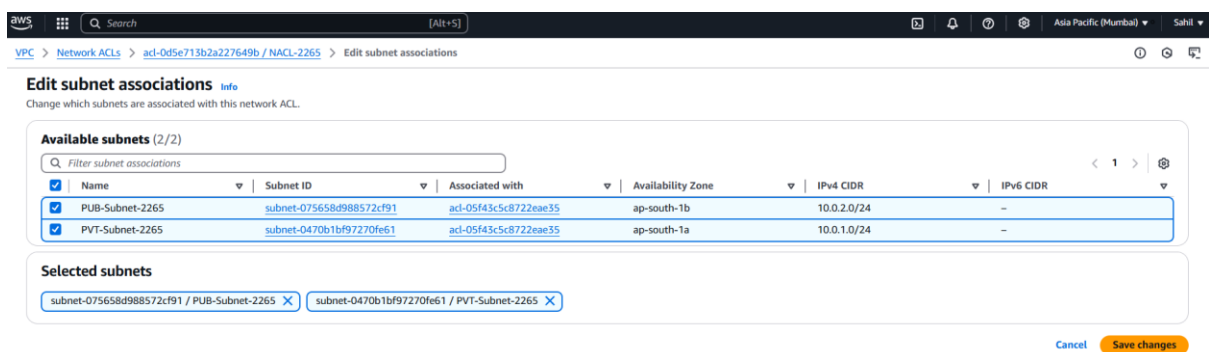


- Keep NACL Selected - Subnet Association – Edit subnet associations.
- Select Both Subnets & Save Changes.

**School of Computer Science, Engineering and Applications (SCSEA)**  
**B. Tech TY (CCSA)**  
**Subject: Cloud Architecture And Protocol**

**Name of the Student:** Sahil S. Mandawgade **PRN:** 20220802265

**Title of Practical:** 2. Building a Dual-Subnet Architecture on AWS:  
Secure Communication Between Public and  
Private Instances with NAT Gateway.

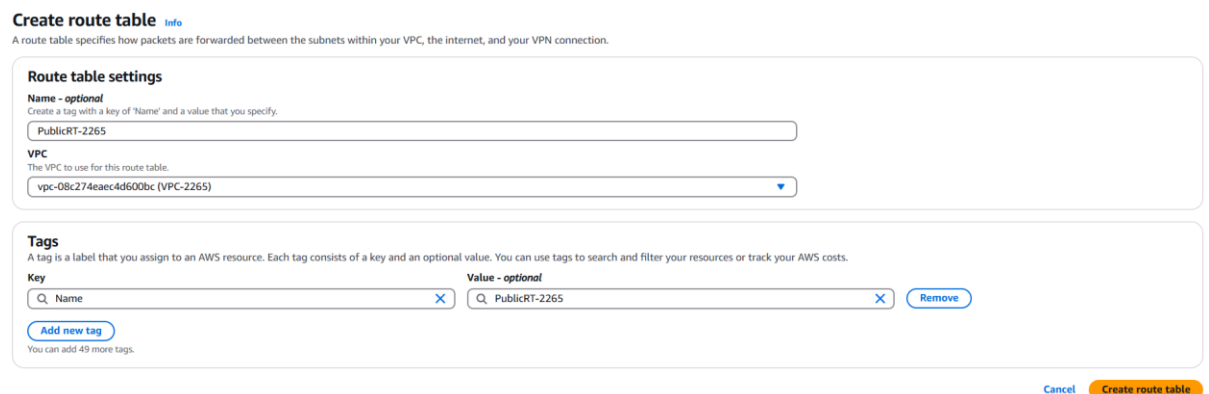


The screenshot shows the AWS console interface for editing subnet associations. The breadcrumb trail is: VPC > Network ACLs > acl-0d5e713b2a227649b / NACL-2265 > Edit subnet associations. The page title is 'Edit subnet associations' with an info icon. Below the title is a subtitle: 'Change which subnets are associated with this network ACL.' The main content area is titled 'Available subnets (2/2)' and contains a table with columns: Name, Subnet ID, Associated with, Availability Zone, IPv4 CIDR, and IPv6 CIDR. Two subnets are listed: PUB-Subnet-2265 (subnet-075658d988572cf91) and PVT-Subnet-2265 (subnet-0470b1bf97270fe61). Both are associated with acl-05f43c5c8722eae35 and are in the ap-south-1b availability zone. Below the table is a 'Selected subnets' section showing the same two subnets. At the bottom right are 'Cancel' and 'Save changes' buttons.

Name	Subnet ID	Associated with	Availability Zone	IPv4 CIDR	IPv6 CIDR
PUB-Subnet-2265	subnet-075658d988572cf91	acl-05f43c5c8722eae35	ap-south-1b	10.0.2.0/24	-
PVT-Subnet-2265	subnet-0470b1bf97270fe61	acl-05f43c5c8722eae35	ap-south-1a	10.0.1.0/24	-

**Step 5: Route Table.**

- Sidebar - VPC - Route Table - Create 2 Route Table, 1 for Public & 1 for Private.
- Assign name and select your VPC.



The screenshot shows the AWS console interface for creating a new route table. The breadcrumb trail is: VPC > Route Tables > Create route table. The page title is 'Create route table' with an info icon. Below the title is a subtitle: 'A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.' The main content area is titled 'Route table settings' and contains three sections: 'Name - optional' with a text input field containing 'PublicRT-2265', 'VPC' with a dropdown menu showing 'vpc-08c274eae4d600bc (VPC-2265)', and 'Tags' with a table for adding tags. The tags table has columns 'Key' and 'Value - optional'. One tag is added with Key 'Name' and Value 'PublicRT-2265'. At the bottom right are 'Cancel' and 'Create route table' buttons.

Key	Value - optional
Name	PublicRT-2265

- Do the same for Private Route Table.

**School of Computer Science, Engineering and Applications (SCSEA)**

**B. Tech TY (CCSA)**

**Subject: Cloud Architecture And Protocol**

**Name of the Student: Sahil S. Mandawgade**

**PRN: 20220802265**

**Title of Practical: 2. Building a Dual-Subnet Architecture on AWS:  
Secure Communication Between Public and  
Private Instances with NAT Gateway.**

**Create route table** Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

**Route table settings**

**Name - optional**

Create a tag with a key of 'Name' and a value that you specify.

PrivateRT-2265

**VPC**

The VPC to use for this route table.

vpc-08c274eac4d600bc (VPC-2265)

**Tags**

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

**Key**

Q Name

**Value - optional**

Q PrivateRT-2265

Remove

Add new tag

You can add 49 more tags.

Cancel

Create route table

- Select Public Route Table - Routes - Edit Routes.
- Select Destination: 0.0.0.0/0(all to any IP/ All IP) and choose your IGW - as we want internet connectivity for Public Subnet.

**Edit routes**

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
Q 0.0.0.0/0	Q local		
	Internet Gateway		No
	Q igw-05862c0d8776c2a09		
	Use: "igw-05862c0d8776c2a09"		
	igw-05862c0d8776c2a09 (IGW-2265)		

Add route

Cancel Preview Save changes

- Keep Public Route Table Selected - Subnet Association - Edit Subnet Association (Associate the Public Route Table to It's Public Subnet).
- Select Public Subnet - Save Association.

**Edit subnet associations**

Change which subnets are associated with this route table.

Available subnets (1/2)

Filter subnet associations

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input type="checkbox"/> PVT-Subnet-2265	subnet-0470b1bf97270fe61	10.0.1.0/24	-	Main (rtb-0c0868c410cb4eece)
<input checked="" type="checkbox"/> PUB-Subnet-2265	subnet-075658d988572cf91	10.0.2.0/24	-	Main (rtb-0c0868c410cb4eece)

Selected subnets

subnet-075658d988572cf91 / PUB-Subnet-2265

Cancel Save associations

- Select Private Route Table - Routes - Edit Routes.

## School of Computer Science, Engineering and Applications (SCSEA)

### B. Tech TY (CCSA)

### Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

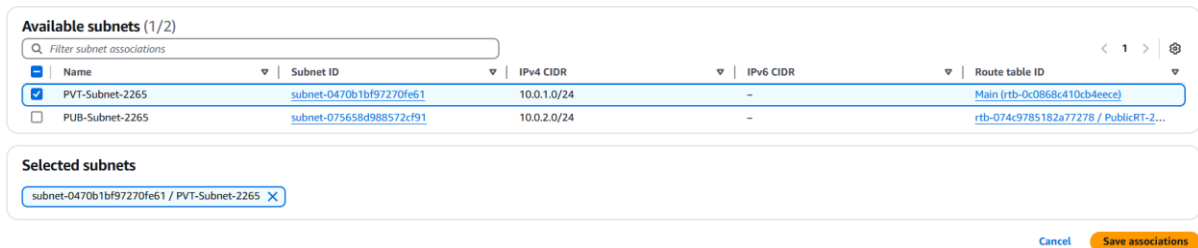
PRN: 20220802265

### Title of Practical: 2. Building a Dual-Subnet Architecture on AWS: Secure Communication Between Public and Private Instances with NAT Gateway.

- Keep local only and save changes - we later attach it with public subnet's NAT Gateway.
- Select Private Route Table - Subnet Association - edit subnet association - Add Private Subnet - Save Changes.

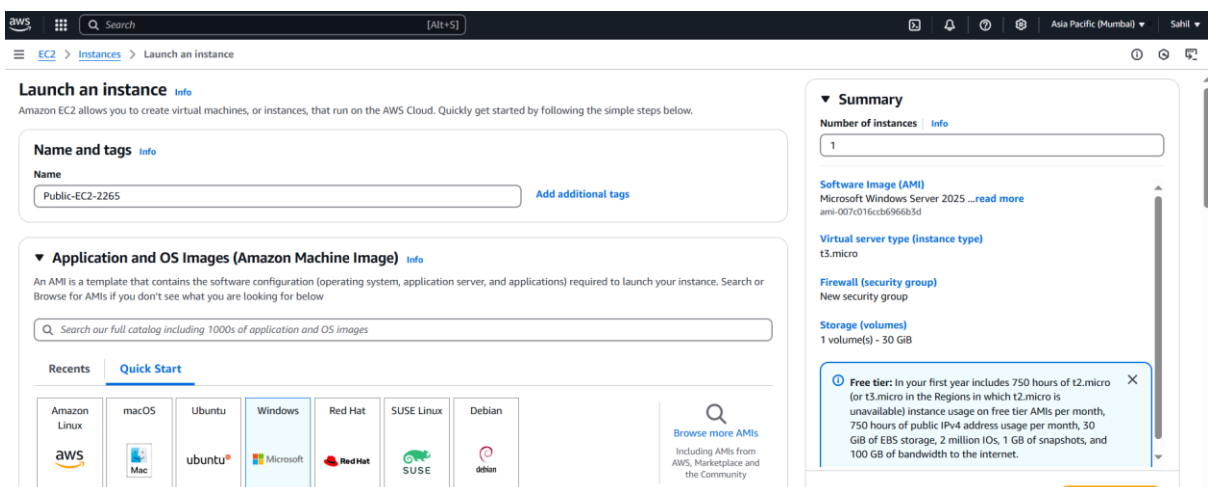
#### Edit subnet associations

Change which subnets are associated with this route table.



### Step 6: Create 2 EC2 Instances: Public and Private.

- Type EC2 in Search bar - EC2 Dashboard - First Create Public Instance.
- Assign Name - Choose Windows as AMI.



- Choose 4Gb t3.medium Instance for speed and use existing key pair.



**School of Computer Science, Engineering and Applications (SCSEA)**  
**B. Tech TY (CCSA)**  
**Subject: Cloud Architecture And Protocol**

**Name of the Student:** Sahil S. Mandawgade **PRN:** 20220802265

**Title of Practical:** 2. Building a Dual-Subnet Architecture on AWS:  
Secure Communication Between Public and Private Instances with NAT Gateway.

▼ **Instance type** [Info](#) | [Get advice](#)

**Instance type**

t3.medium

Family: t3 2 vCPU 4 GiB Memory Current generation: true  
On-Demand Windows base pricing: 0.0632 USD per Hour On-Demand Ubuntu Pro base pricing: 0.0483 USD per Hour  
On-Demand SUSE base pricing: 0.1011 USD per Hour On-Demand RHEL base pricing: 0.0736 USD per Hour  
On-Demand Linux base pricing: 0.0448 USD per Hour

☐ All generations

[Compare instance types](#)

[Additional costs apply for AMIs with pre-installed software](#)

▼ **Key pair (login)** [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

**Key pair name - required**

KY-CCSA-TY-2265

[Create new key pair](#)

For Windows instances, you use a key pair to decrypt the administrator password. You then use the decrypted password to connect to your instance.

- Network Settings - Edit - Choose your VPC - Choose Public Subnet - Enable Auto-assign IP - Create SG which allows RDP - Launch Instance.

▼ **Network settings** [Info](#)

**VPC - required** [Info](#)

vpc-08c274eae4d600bc (VPC-2265)  
10.0.0.0/16



**Subnet** [Info](#)

subnet-075658d988572cf91 PUB-Subnet-2265  
VPC: vpc-08c274eae4d600bc Owner: 908027405956 Availability Zone: ap-south-1b  
Zone type: Availability Zone IP addresses available: 251 CIDR: 10.0.2.0/24



[Create new subnet](#)

**Auto-assign public IP** [Info](#)

Enable

[Additional charges apply when outside of free tier allowance](#)

**Firewall (security groups)** [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group

☐ Select existing security group

**Security group name - required**

VPC-SG-RDP

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and \_-./[]#,@!+=&()!\$\*

**Description - required** [Info](#)

RDP Access

**Inbound Security Group Rules**

▼ Security group rule 1 (TCP, 3389, 0.0.0.0/0)

[Remove](#)

**Type** [Info](#)

rdp

**Protocol** [Info](#)

TCP

**Port range** [Info](#)

3389

**School of Computer Science, Engineering and Applications (SCSEA)**

**B. Tech TY (CCSA)**

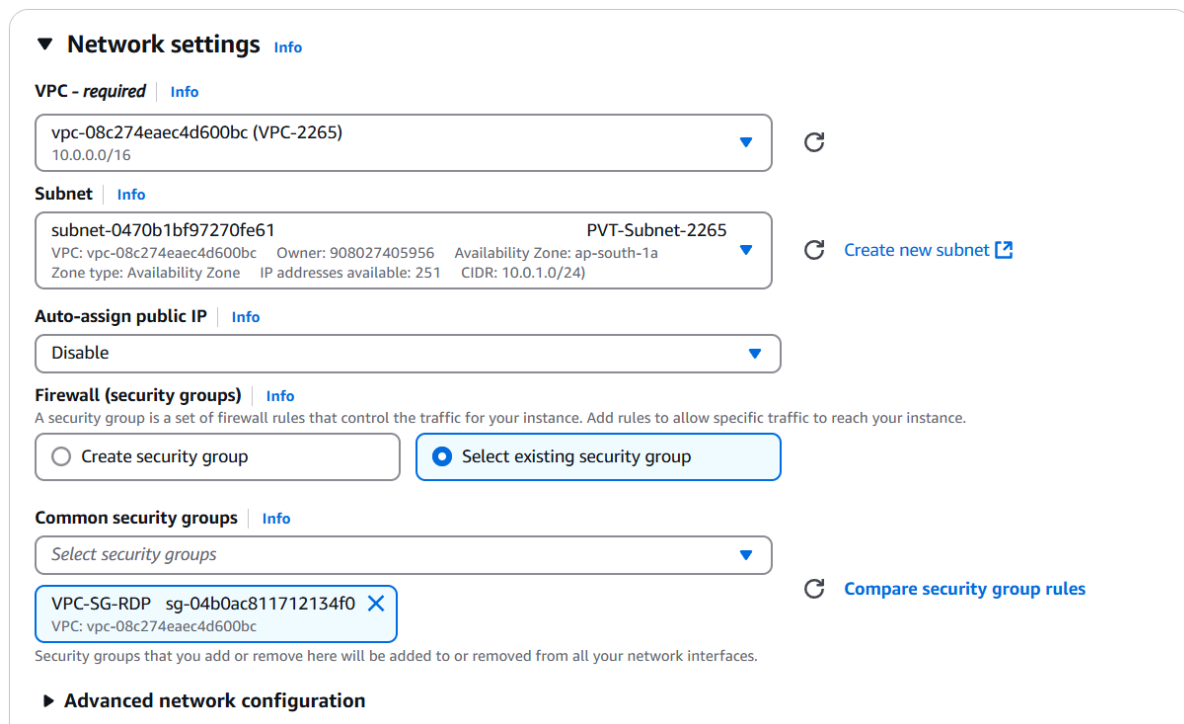
**Subject: Cloud Architecture And Protocol**

**Name of the Student: Sahil S. Mandawgade**

**PRN: 20220802265**

**Title of Practical: 2. Building a Dual-Subnet Architecture on AWS:  
Secure Communication Between Public and  
Private Instances with NAT Gateway.**

- Create Another instance - Use Same SG, follow same steps - Choose Private Subnet - Don't Add Auto Assign to it.



The screenshot shows the AWS Network settings console for a VPC. The 'Network settings' section is expanded, showing the VPC ID 'vpc-08c274eaec4d600bc (VPC-2265)' and its CIDR block '10.0.0.0/16'. Below this, the 'Subnet' section shows a selected private subnet 'subnet-0470b1bf97270fe61' (PVT-Subnet-2265) with details: VPC: vpc-08c274eaec4d600bc, Owner: 908027405956, Availability Zone: ap-south-1a, Zone type: Availability Zone, IP addresses available: 251, and CIDR: 10.0.1.0/24. The 'Auto-assign public IP' is set to 'Disable'. In the 'Firewall (security groups)' section, the 'Select existing security group' option is chosen. Under 'Common security groups', the group 'VPC-SG-RDP sg-04b0ac811712134f0' is selected. A link to 'Compare security group rules' is visible. At the bottom, there is a link to 'Advanced network configuration'.

**Step 7:** Check Internet Access in your Public and Private Instances - Private should not have internet access.

- Copy public IP of Public Subnet - Open RDP Client - paste IP in PC Name - Click on Credentials - Add Credentials - Username: Administrator.

**School of Computer Science, Engineering and Applications (SCSEA)**

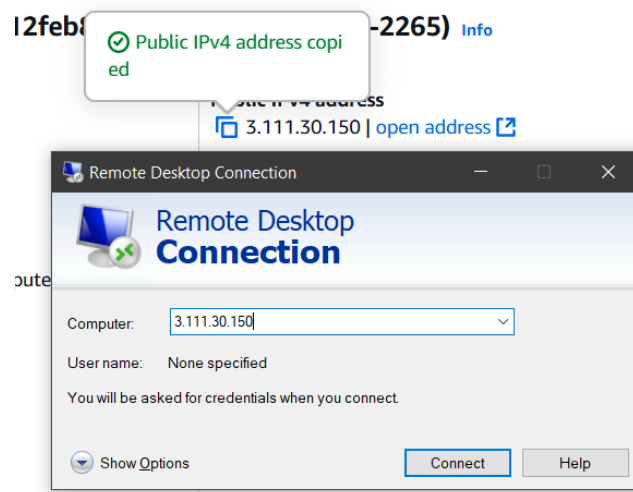
**B. Tech TY (CCSA)**

**Subject: Cloud Architecture And Protocol**

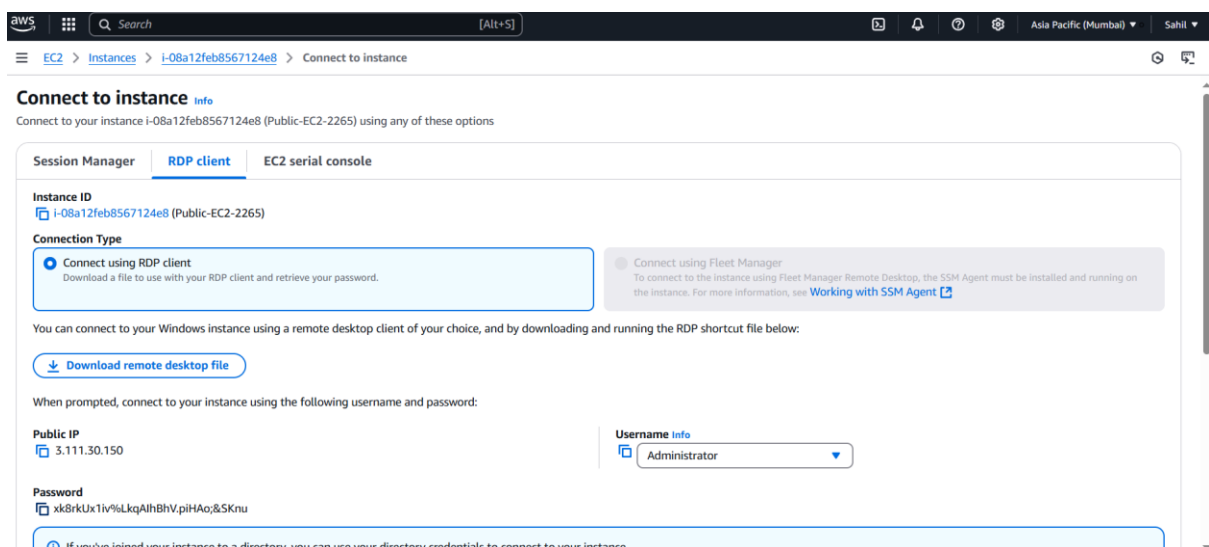
**Name of the Student: Sahil S. Mandawgade**

**PRN: 20220802265**

**Title of Practical: 2. Building a Dual-Subnet Architecture on AWS:  
Secure Communication Between Public and  
Private Instances with NAT Gateway.**



- Go Back to AWS Public Instance – Connect - RDP Client - Get Password - Upload Your .pem Key and Decrypt Password.



- Copy Password - Paste in RDP . Press Yes.
- Public Instance Successfully Accessed.
- As we can see the internet access is there.

**School of Computer Science, Engineering and Applications (SCSEA)**

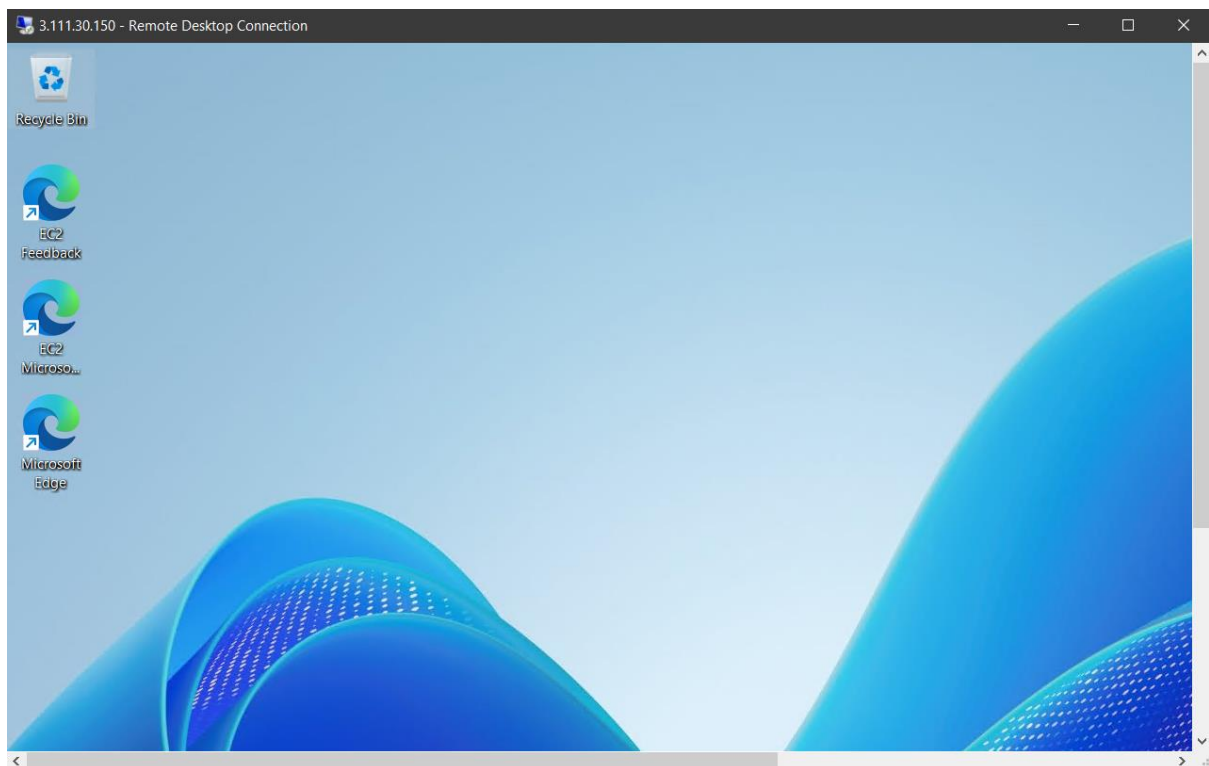
**B. Tech TY (CCSA)**

**Subject: Cloud Architecture And Protocol**

**Name of the Student: Sahil S. Mandawgade**

**PRN: 20220802265**

**Title of Practical: 2. Building a Dual-Subnet Architecture on AWS:  
Secure Communication Between Public and  
Private Instances with NAT Gateway.**



- Now we open RDP in Public Instance - Do the same process with Private Instance.



**D Y PATIL  
INTERNATIONAL  
UNIVERSITY**  
AKURDI PUNE

**School of Computer Science, Engineering and Applications (SCSEA)**

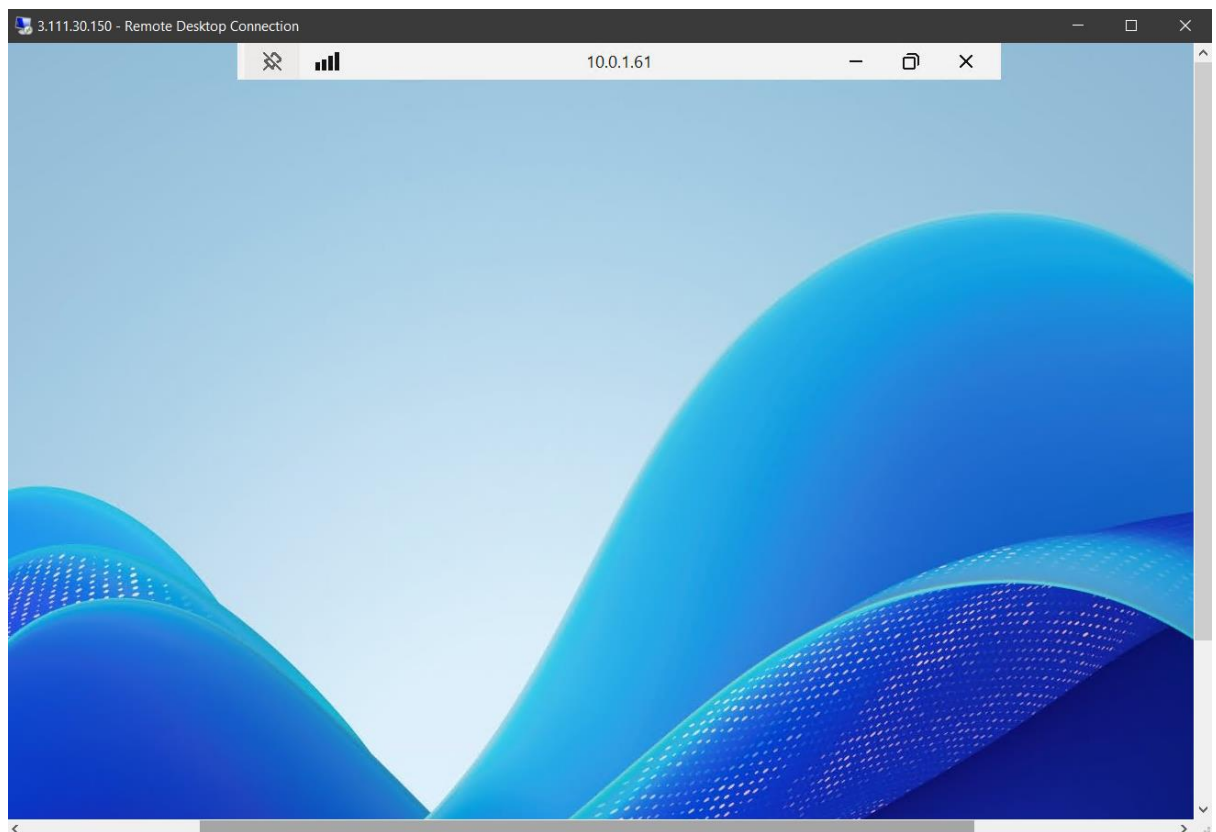
**B. Tech TY (CCSA)**

**Subject: Cloud Architecture And Protocol**

**Name of the Student: Sahil S. Mandawgade**

**PRN: 20220802265**

**Title of Practical: 2. Building a Dual-Subnet Architecture on AWS:  
Secure Communication Between Public and  
Private Instances with NAT Gateway.**



- We are in Private Instance - verify with the IP the top - as we can see we don't have internet access and we also tried opening google which failed as we don't have internet access in Private Instance.

**School of Computer Science, Engineering and Applications (SCSEA)**

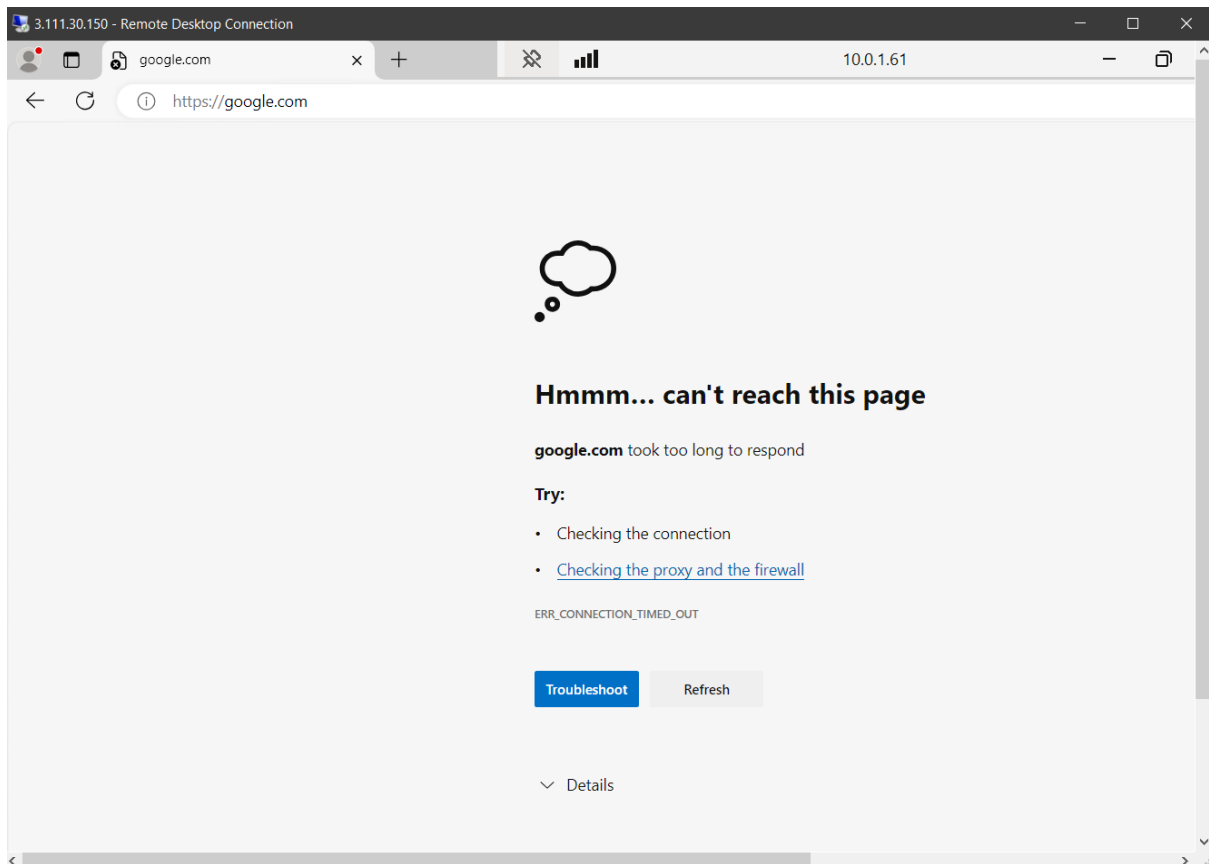
**B. Tech TY (CCSA)**

**Subject: Cloud Architecture And Protocol**

**Name of the Student: Sahil S. Mandawgade**

**PRN: 20220802265**

**Title of Practical: 2. Building a Dual-Subnet Architecture on AWS:  
Secure Communication Between Public and  
Private Instances with NAT Gateway.**



- Now we will Close these sessions - and attach NAT with Public Subnet and update it in Private Subnet's Route Table so we can access internet in Private Instance without attaching it to IGW.

**Step 8: NAT Gateway.**

- Open AWS - VPC - NAT - Create Nat Gateway.
- Assign Name - Public Subnet - Connectivity: Public - Allocate Elastic IP - Create NAT Gateway.

## School of Computer Science, Engineering and Applications (SCSEA)

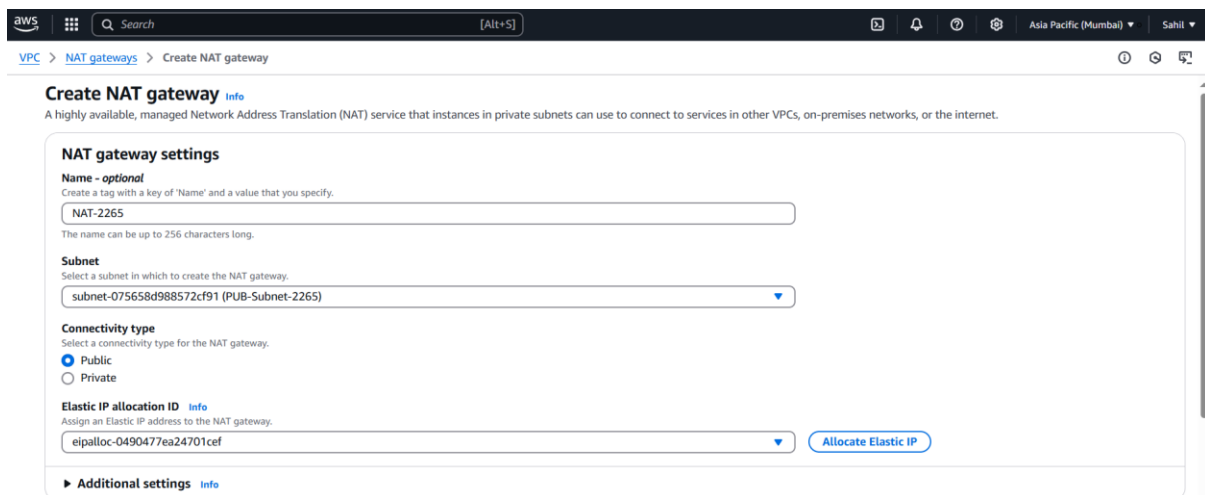
### B. Tech TY (CCSA)

### Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

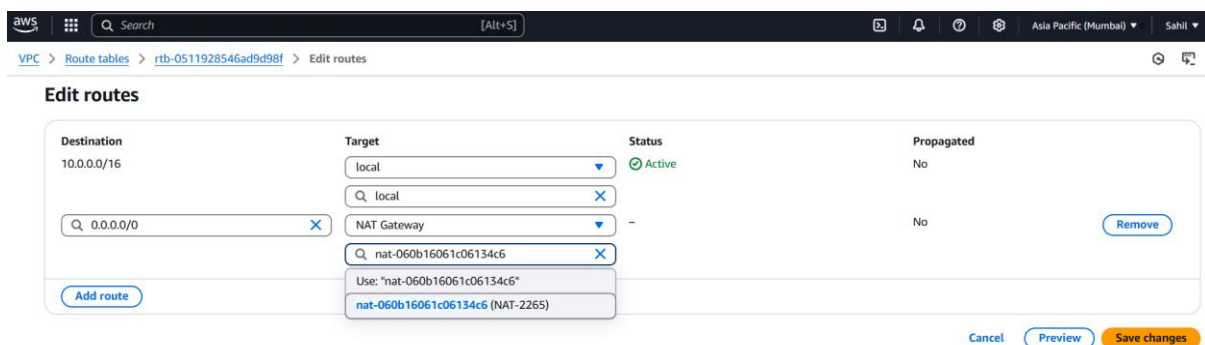
PRN: 20220802265

### Title of Practical: 2. Building a Dual-Subnet Architecture on AWS: Secure Communication Between Public and Private Instances with NAT Gateway.



The screenshot shows the 'Create NAT gateway' page in the AWS Management Console. The page title is 'Create NAT gateway' with an 'info' link. Below the title is a description: 'A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the internet.' The 'NAT gateway settings' section includes: 'Name - optional' with a text input field containing 'NAT-2265'; 'Subnet' with a dropdown menu showing 'subnet-075658d988572cf91 (PUB-Subnet-2265)'; 'Connectivity type' with radio buttons for 'Public' (selected) and 'Private'; and 'Elastic IP allocation ID' with a dropdown menu showing 'eipalloc-0490477ea24701cef' and an 'Allocate Elastic IP' button. There is also an 'Additional settings' section with an 'info' link.

- Go to Routes Tables - Select Private Route Table - Routes - Edit Routes.
- Add Destination: 0.0.0.0/0 - Select NAT Gateway and choose your created NAT - Save Changes.



The screenshot shows the 'Edit routes' page in the AWS Management Console. The page title is 'Edit routes'. The 'Destination' field shows '10.0.0.0/16'. The 'Target' field shows 'local'. The 'Status' field shows 'Active'. The 'Propagated' field shows 'No'. There is a search bar for destinations, and a list of routes is shown below. The first route has a destination of '0.0.0.0/0' and a target of 'NAT Gateway'. The second route has a destination of 'nat-060b16061c06134c6' and a target of 'nat-060b16061c06134c6 (NAT-2265)'. There are 'Add route', 'Remove', 'Cancel', 'Preview', and 'Save changes' buttons.

### Step 9: Network Access into Private EC2 Instance Accessing from Public EC2.

- Open RDP – Connect to Your Public Instance.
- Open RDP in Public instance windows - Connect Private Instance - Open Google in Microsoft Edge in Private instance.

**School of Computer Science, Engineering and Applications (SCSEA)**

**B. Tech TY (CCSA)**

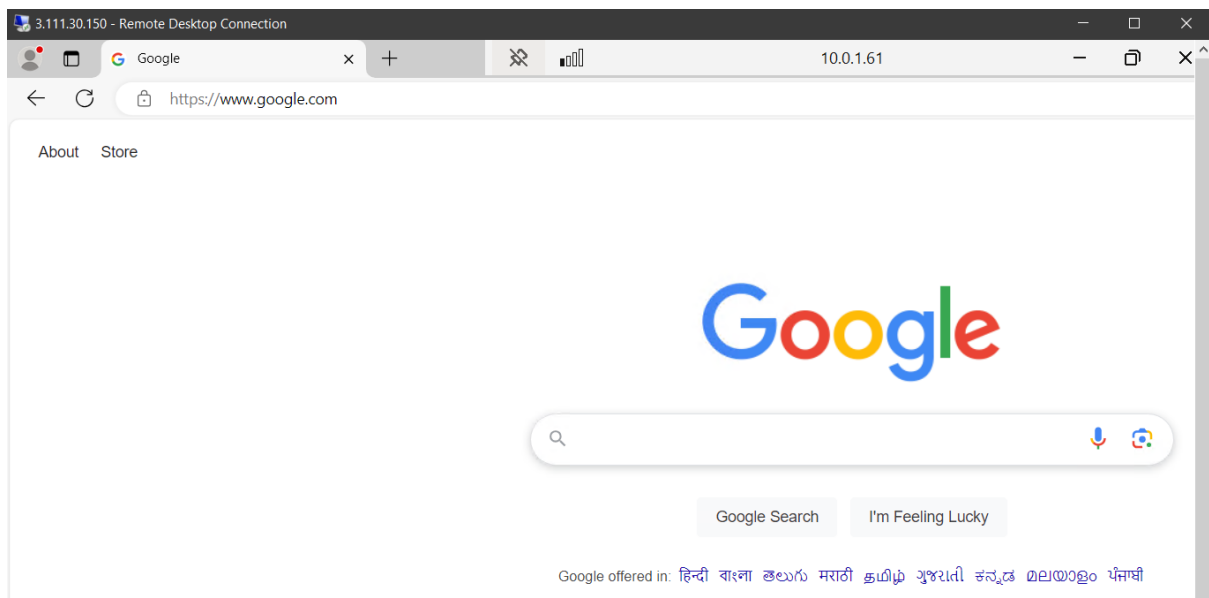
**Subject: Cloud Architecture And Protocol**

**Name of the Student: Sahil S. Mandawgade**

**PRN: 20220802265**

**Title of Practical: 2. Building a Dual-Subnet Architecture on AWS:  
Secure Communication Between Public and  
Private Instances with NAT Gateway.**

- As we can see successful internet access into the private EC2 instance -  
Successfully accessed internet in private ec2 in private subnet without connect it  
to IGW.



**Step 10: Deletion Of Resources.**

- Delete the resources in a manner where they don't leave any dependencies not to cause complications later.
- Order of Deletion of Resources:

EC2 instances - Delete Security Groups from VPC Dashboard - delete NAT Gateway - Release Elastic IP - de-associate subnets from route tables and delete route tables - de-associate subnets from NACL and delete NACL - Delete Subnets - Detach IGW from VPC & Delete IGW - Delete VPC.