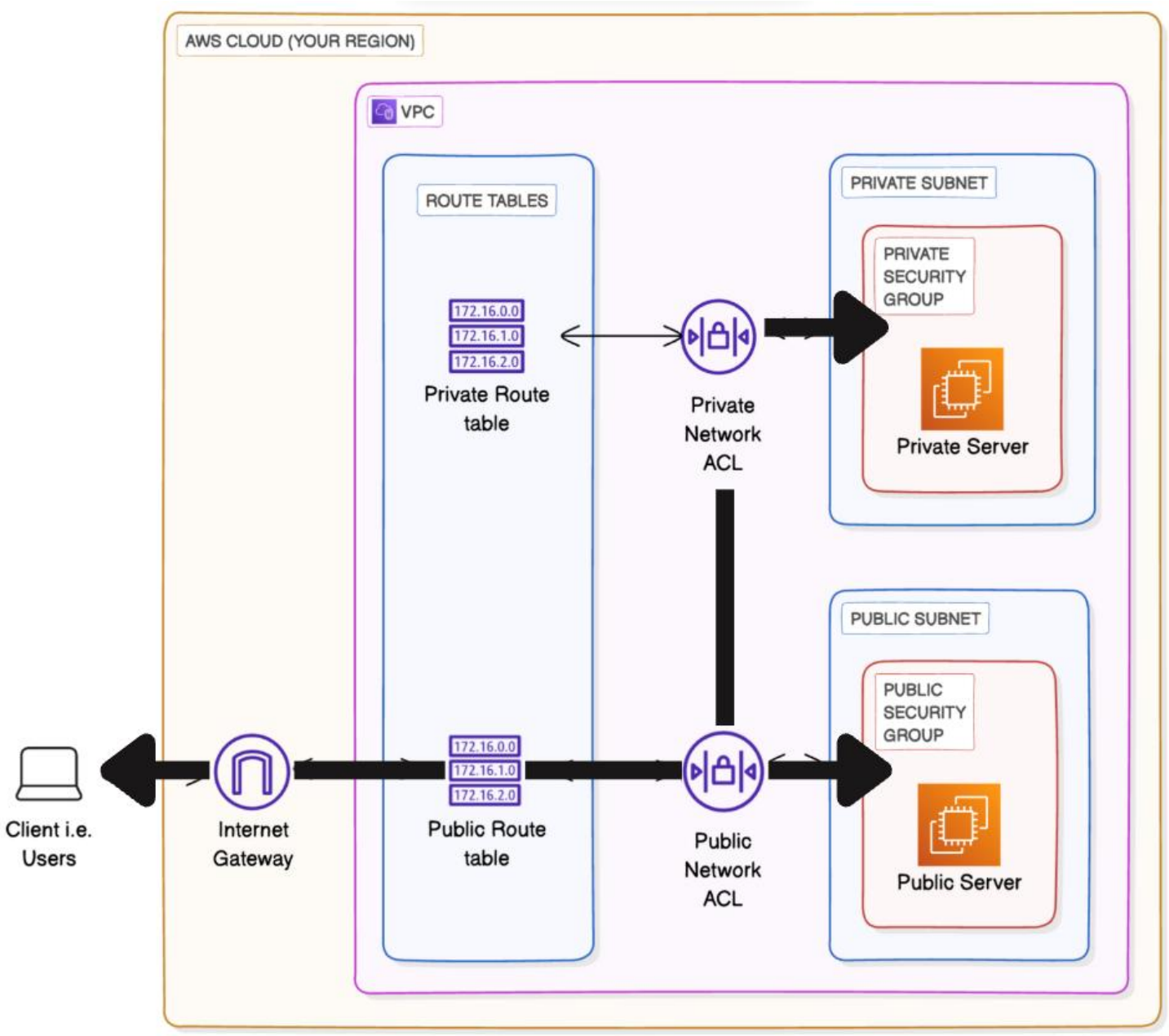
Testing VPC Connectivity - Step-by-Step Documentation



This documentation is a detailed, step-by-step guide to testing VPC connectivity for your AWS project. It is self-contained and includes a full recap of the prior VPC setup steps, followed by the connectivity tests you'll perform between public and private EC2 instances and to the internet.

Step 0: Before we start...

Make sure you've completed the earlier projects in this VPC networking series or have the following already set up:

- An AWS account and access to the AWS Management Console.

- A VPC (NextWork VPC) with Public and Private subnets.

- An Internet Gateway attached to the VPC.

- Route tables, Security Groups and Network ACLs configured.

- One EC2 instance in the Public Subnet (NextWork Public Server) and one in the Private Subnet (NextWork Private Server).

✍️ What are we here to do today? (Quick note for your documentation):

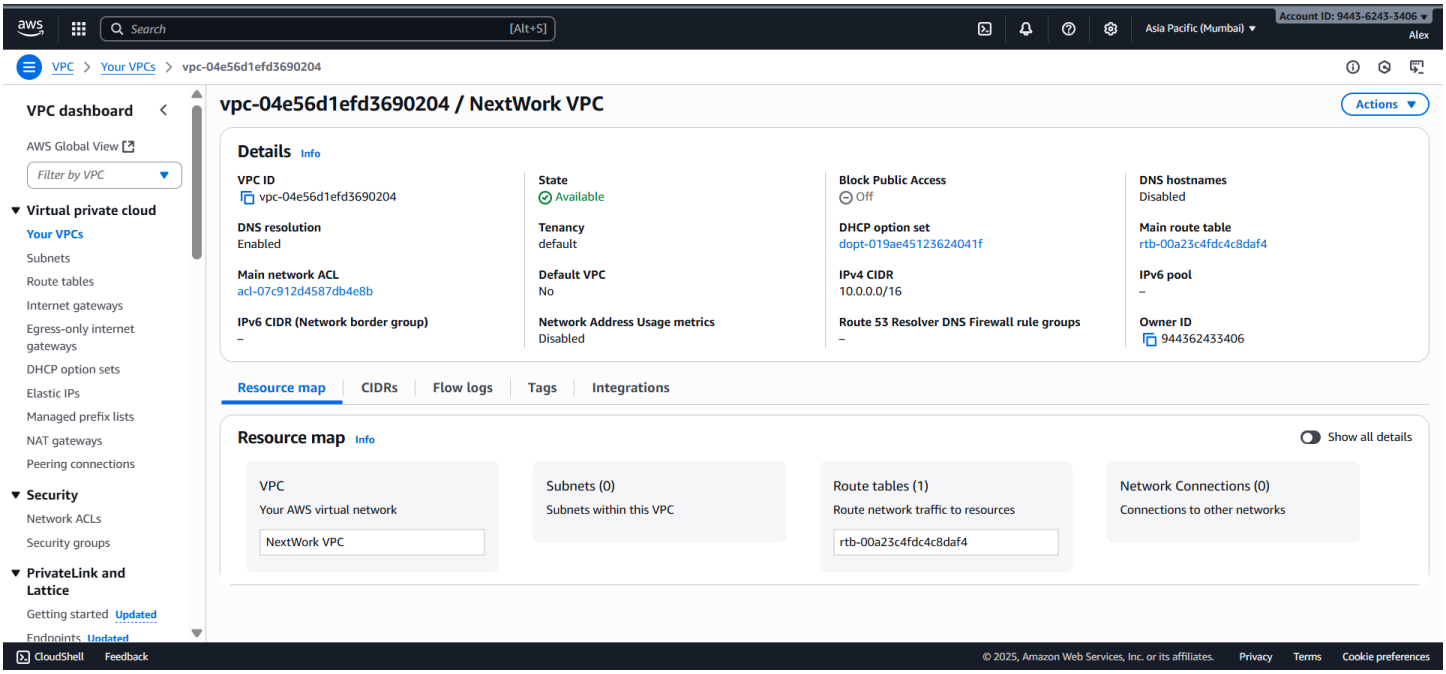
In this project I will verify connectivity between EC2 instances in my VPC and validate internet access from the public subnet.

Step 1: Create a VPC

Set up a new Virtual Private Cloud in AWS.

Actions:

- - Log in to the AWS Management Console.
- - Search for 'VPC' in the search bar and select it.
- - In the left-hand navigation pane, choose 'Your VPCs'.
- - Click 'Create VPC'.
- - Select 'VPC only'.
- - Enter a Name tag (e.g., NextWork VPC).
- - Enter an IPv4 CIDR block (e.g., 10.0.0.0/16).
- - Click 'Create VPC' to finalize.

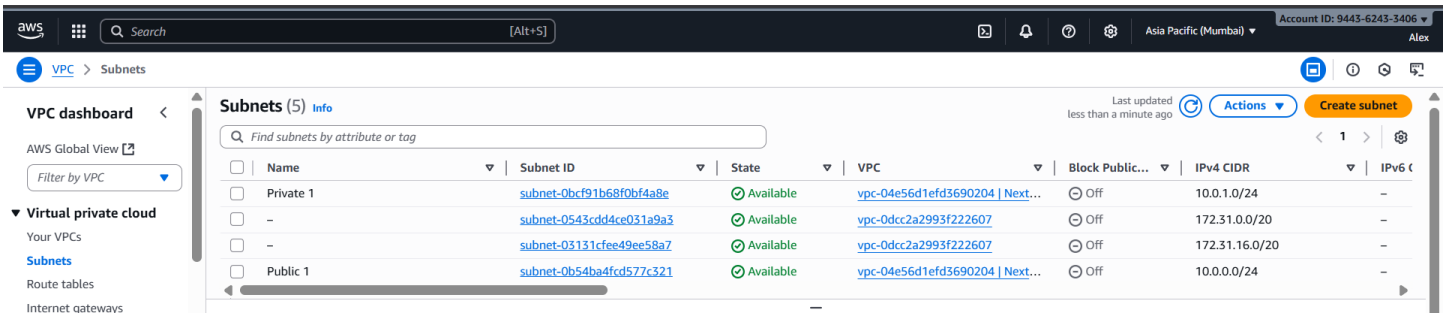


Step 2: Create Subnets

Create public and private subnets inside your VPC.

Actions:

- - From the VPC Dashboard, choose 'Subnets'.
- - Click 'Create subnet'.
- - Choose the VPC you created (NextWork VPC).
- - Enter a Subnet name (e.g., Public 1).
- - Select an Availability Zone.
- - Enter an IPv4 subnet CIDR block (e.g., 10.0.0.0/24).
- - Click 'Create subnet'.
- - Select the subnet, choose 'Edit subnet settings', and enable 'Auto-assign public IPv4 address' for the public subnet.
- - Repeat to create a private subnet (e.g., 10.0.1.0/24) and leave auto-assign public IPv4 disabled.

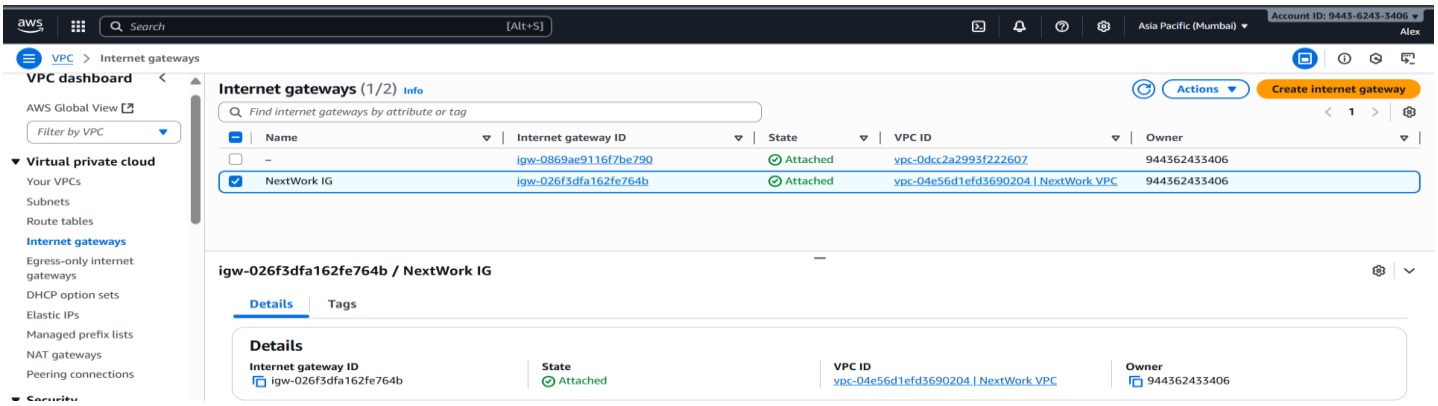


Step 3: Create an Internet Gateway

Attach an Internet Gateway to provide internet access for public subnets.

Actions:

- - In the VPC Dashboard, choose 'Internet gateways'.
- - Click 'Create internet gateway'.
- - Enter a Name tag (e.g., NextWork IG).
- - Click 'Create internet gateway'.
- - Select the gateway, choose 'Actions' → 'Attach to VPC'.
- - Select your VPC (NextWork VPC) and confirm.

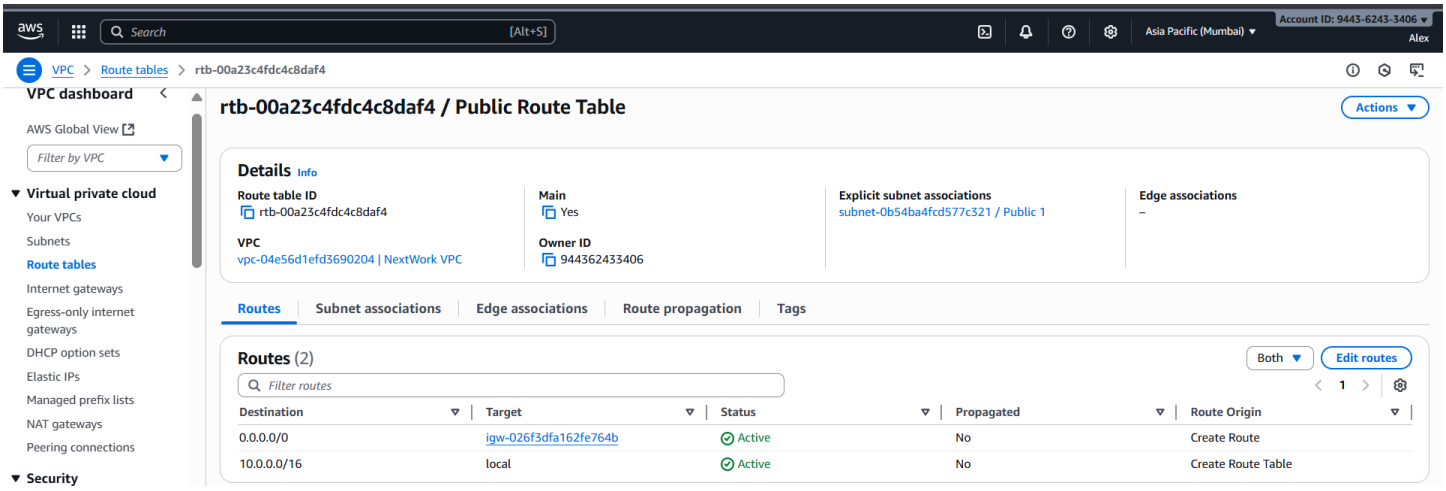


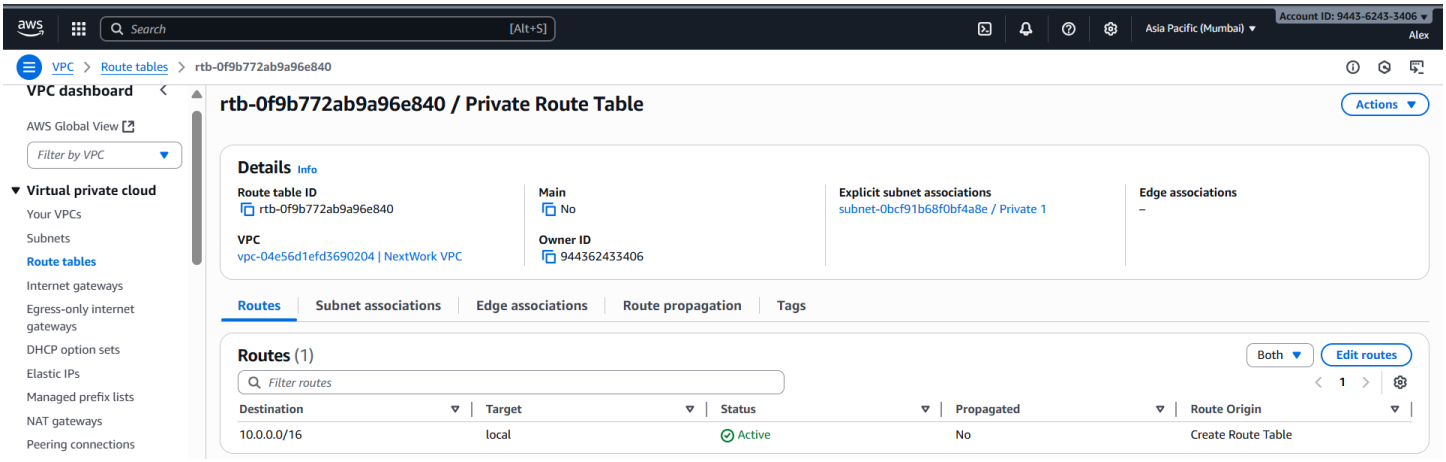
Step 4: Create/Configure Route Tables

Create route tables and associate them with subnets.

Actions:

- - Go to 'Route tables' in the VPC Dashboard.
- - Create a public route table and associate it with your Public subnet.
- - Edit the routes and add Destination = 0.0.0.0/0 with Target = Internet Gateway.
- - Create a private route table and associate it with your Private subnet.
- - Do not add a route to the Internet Gateway for the private route table.





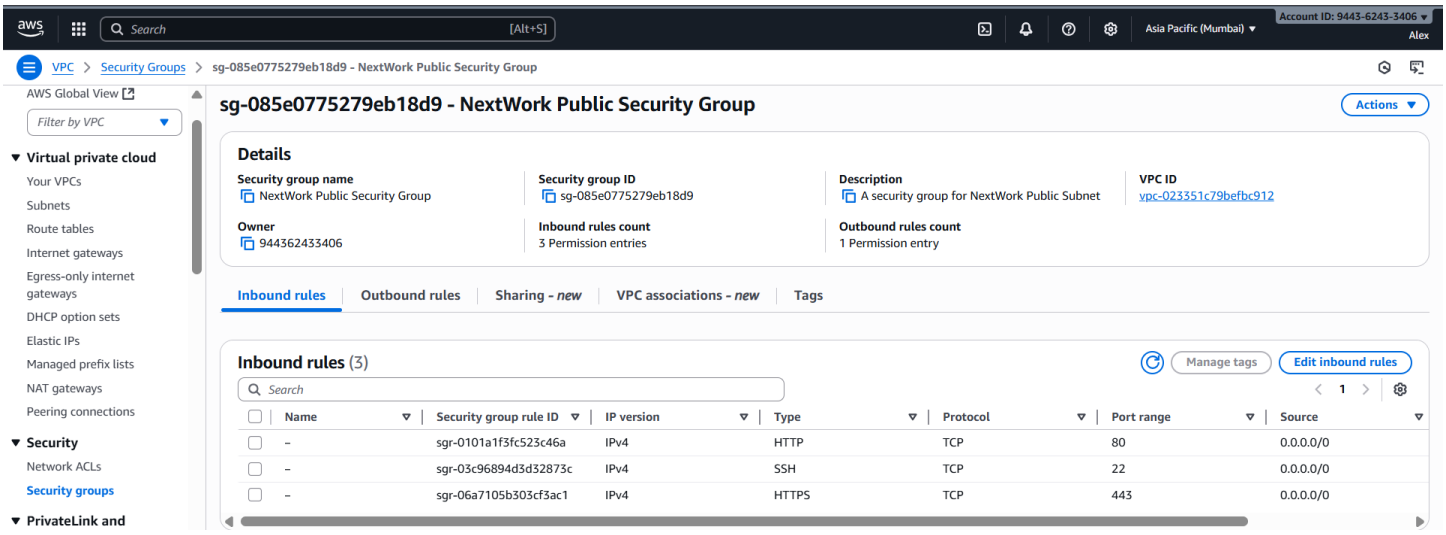
Step 5: Create Security Groups

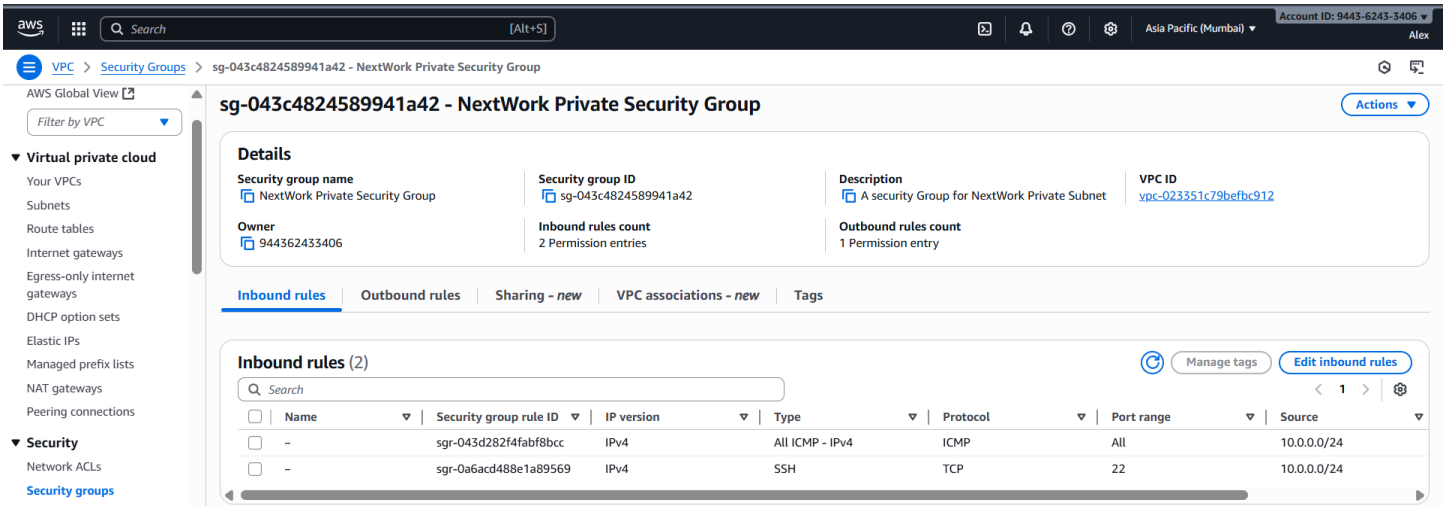
Create Security Groups to control instance-level traffic.

Actions:

- - In the VPC Dashboard, select 'Security groups'.
- - Click 'Create security group'.
- - Enter a Name tag (e.g., NextWork Public Security Group) and select your VPC.
- - Add inbound rules for HTTP (80) and any required ports (e.g., SSH 22 for management).
- - Create a separate Security Group for the Private subnet (e.g., NextWork Private Security Group) with limited inbound rules.

- - Attach the appropriate security groups to your EC2 instances.



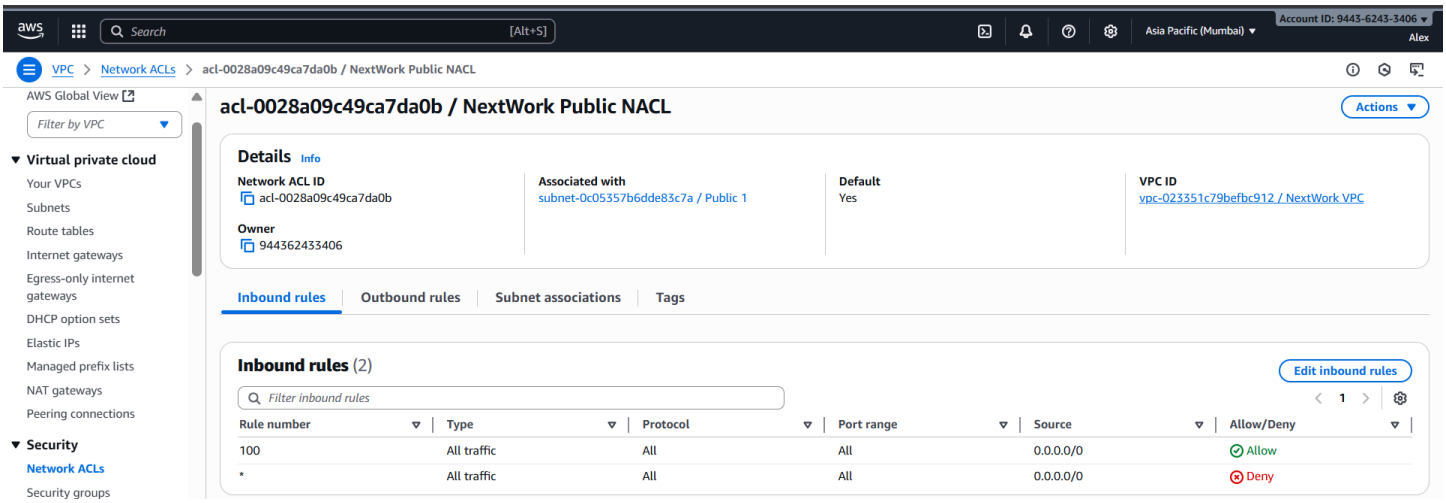


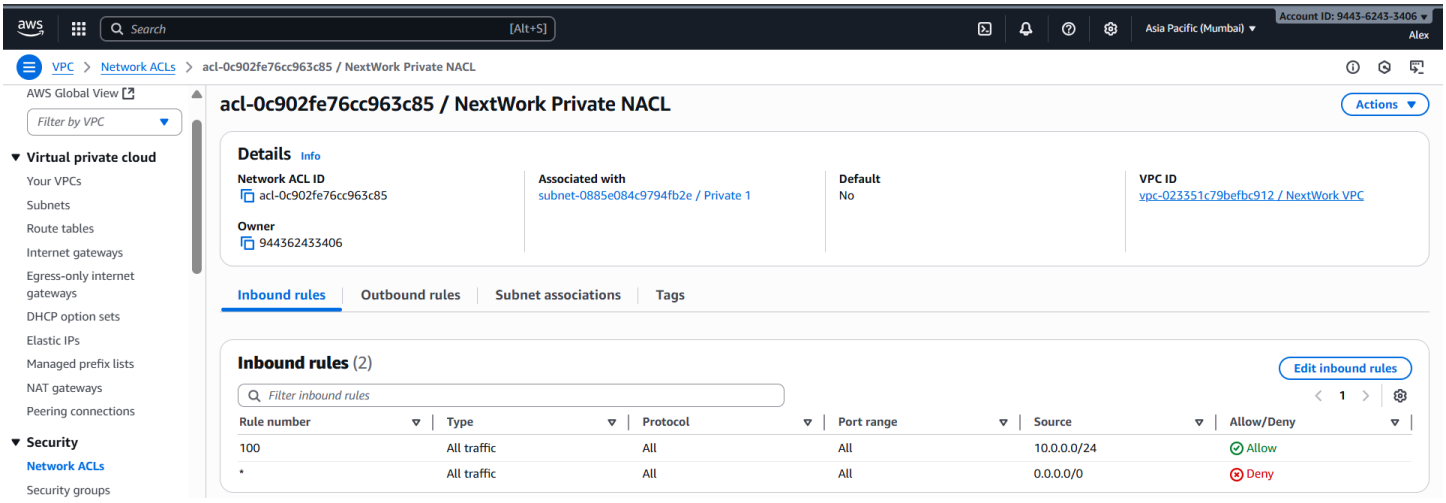
Step 6: Create Network ACLs

Create Network ACLs (NACLs) to control subnet-level traffic.

Actions:

- - In the VPC Dashboard, choose 'Network ACLs'.
- - Create or select a Network ACL for the Public subnet and review its inbound/outbound rules.
- - Rename the default NACL associated with Public subnet (optional) to 'NextWork Public NACL'.
- - Create a new Network ACL for the Private subnet (NextWork Private NACL).
- - Note: custom NACLs start with all traffic denied; you'll add rules to allow required traffic.



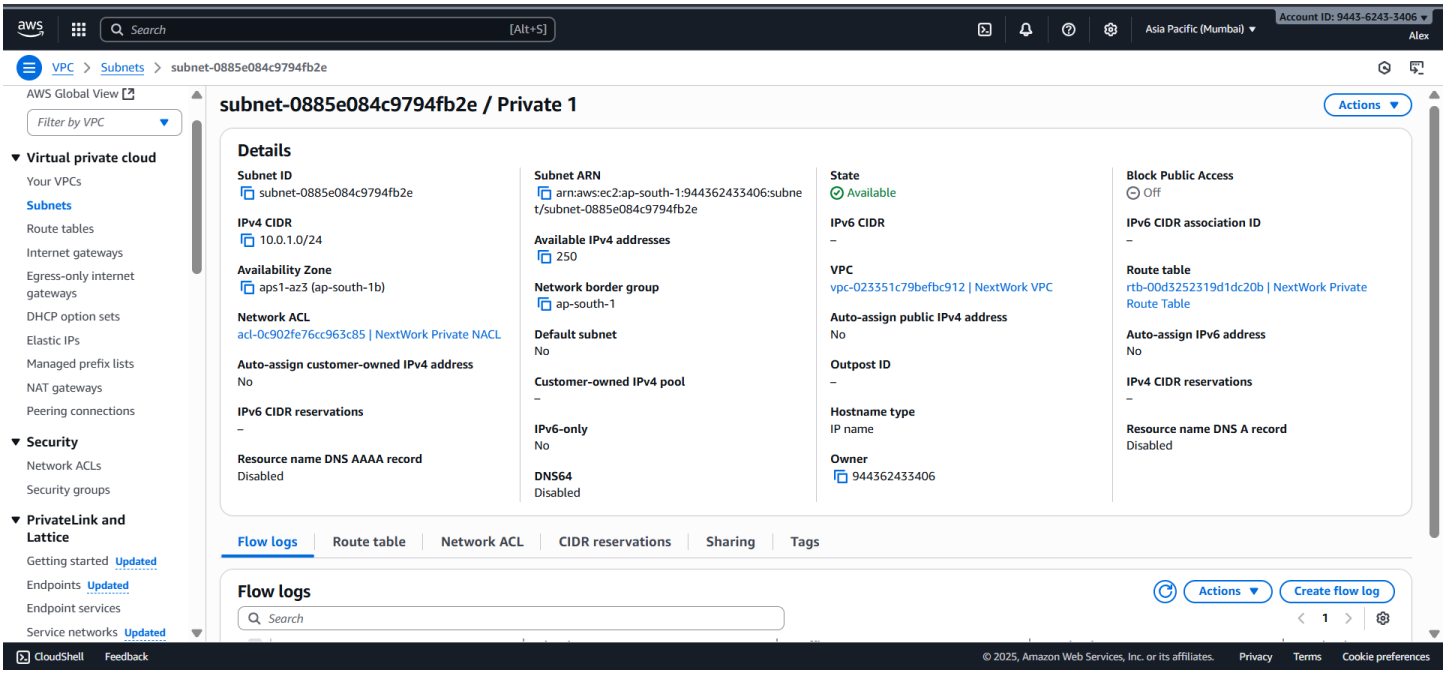


Step 7: Create a Private Subnet

Add a private subnet to your VPC for internal resources.

Actions:

- - In the VPC Dashboard, choose 'Subnets' → 'Create subnet'.
- - Select NextWork VPC and enter Subnet name (e.g., Private 1).
- - Select an Availability Zone different from the public subnet for redundancy.
- - Enter an IPv4 CIDR block (e.g., 10.0.1.0/24).
- - Click 'Create subnet' and leave auto-assign public IPv4 disabled.

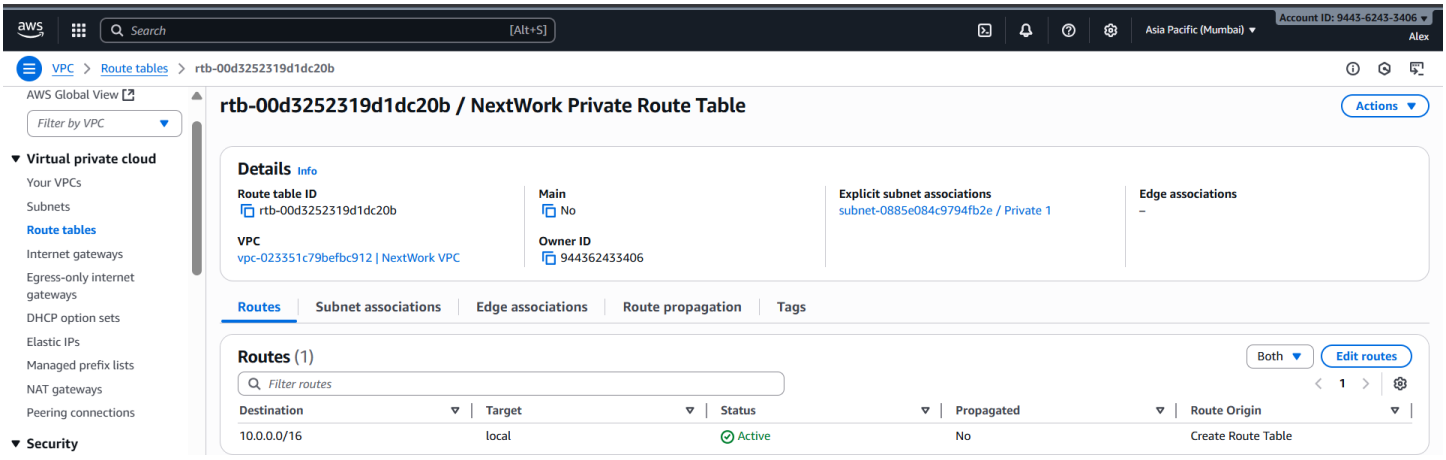


Step 8: Create a Private Route Table

Create and associate a route table for private subnet routing.

Actions:

- - In 'Route tables', click 'Create route table'.
- - Enter a Name tag (e.g., NextWork Private RT) and select your VPC.
- - Create the route table and go to 'Subnet associations'.
- - Edit subnet associations and select your Private 1 subnet.
- - Do not add routes to an Internet Gateway.

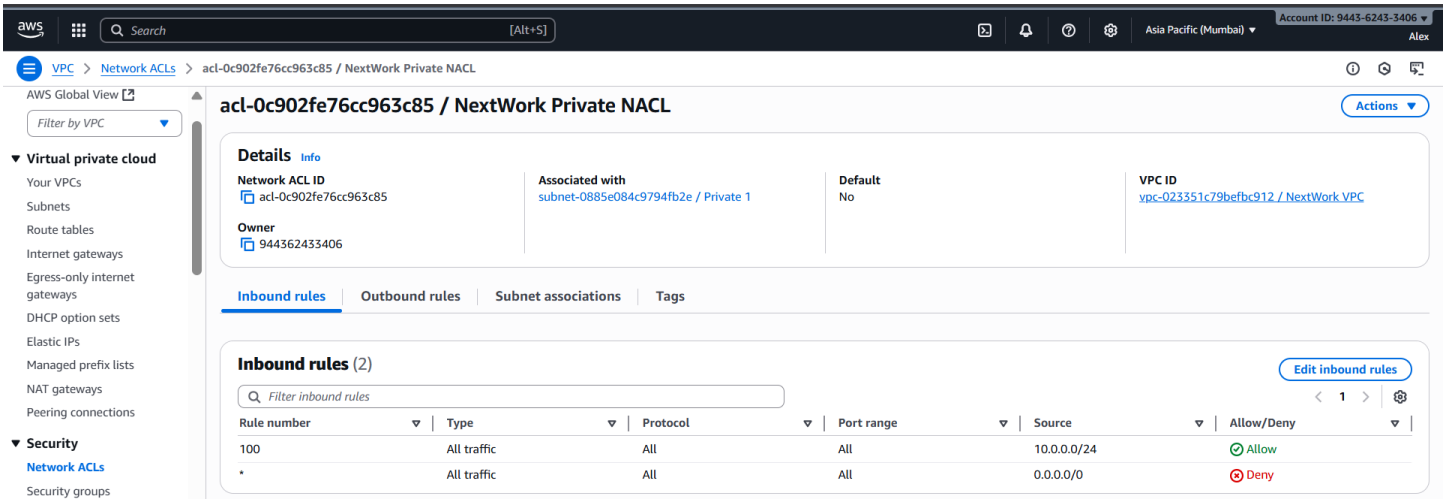


Step 9: Create a Private Network ACL

Add a subnet-level NACL protecting your private subnet.

Actions:

- - In 'Network ACLs', click 'Create network ACL'.
- - Name it (e.g., NextWork Private NACL) and choose your VPC.
- - Create inbound rules to allow necessary internal traffic (e.g., ICMP from public subnet) as required.
- - Configure outbound rules appropriately to restrict internet-bound access.
- - Associate the NACL with your Private subnet under 'Subnet associations'.

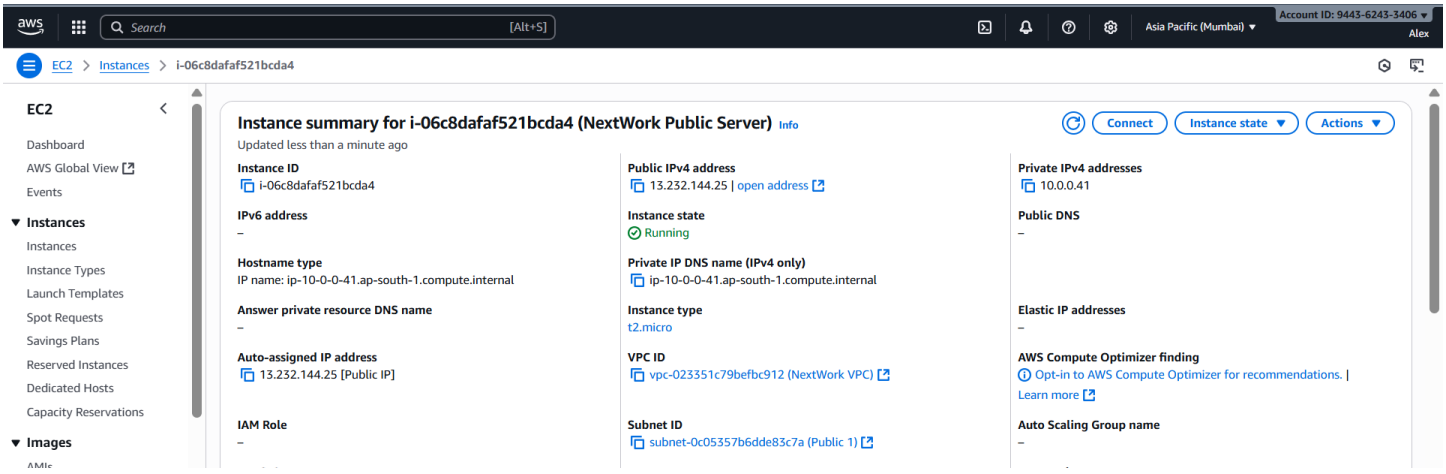


Step 10: Launch EC2 Instance in Public Subnet

Launch a public EC2 instance with a public IP and public security group.

Actions:

- - Open EC2 Console → Instances → Launch Instance.
- - Enter a Name tag (e.g., NextWork Public Server).
- - Select an AMI (e.g., Amazon Linux 2023 AMI) and instance type (t2.micro).
- - Under Network settings, select NextWork VPC and the Public subnet.
- - Enable Auto-assign Public IP.
- - Choose or create a Key pair (NextWork key pair) and download the private key (.pem).
- - Select the NextWork Public Security Group.
- - Click 'Launch' and wait for the instance to reach 'running' state.

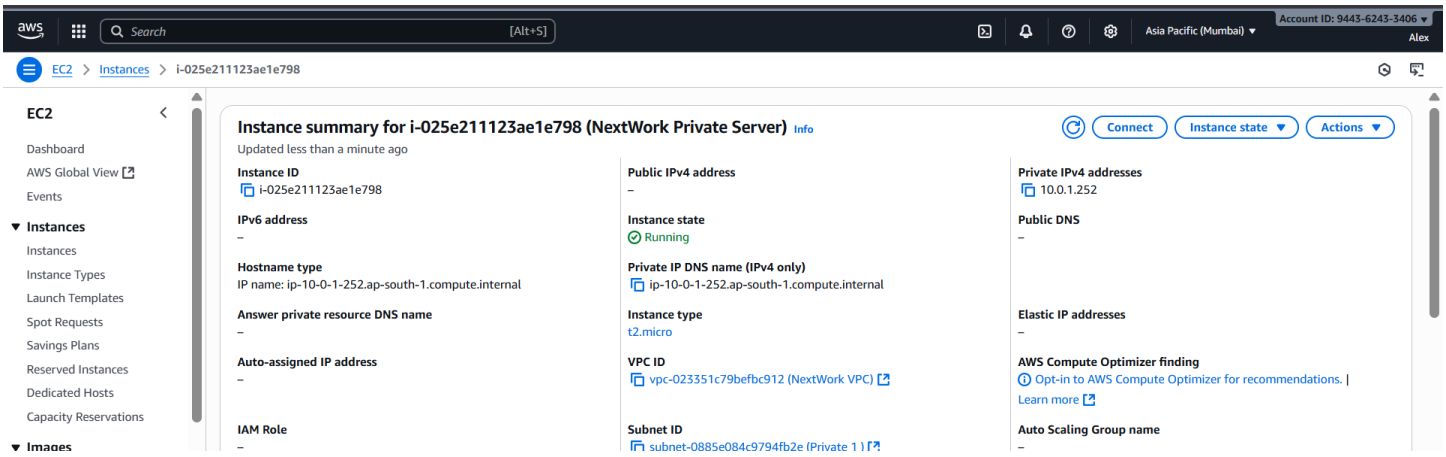


Step 11: Launch EC2 Instance in Private Subnet

Launch a private EC2 instance that has no public IP.

Actions:

- - EC2 Console → Launch Instance.
- - Enter Name tag (e.g., NextWork Private Server).
- - Choose the same AMI and instance type (t2.micro).
- - Under Network settings, select NextWork VPC and the Private subnet.
- - Disable Auto-assign Public IP.
- - Create/select a private security group (NextWork Private Security Group).
- - Click 'Launch' and wait for the instance to become 'running'. Note: connect via Bastion/Jump host from Public subnet if needed.

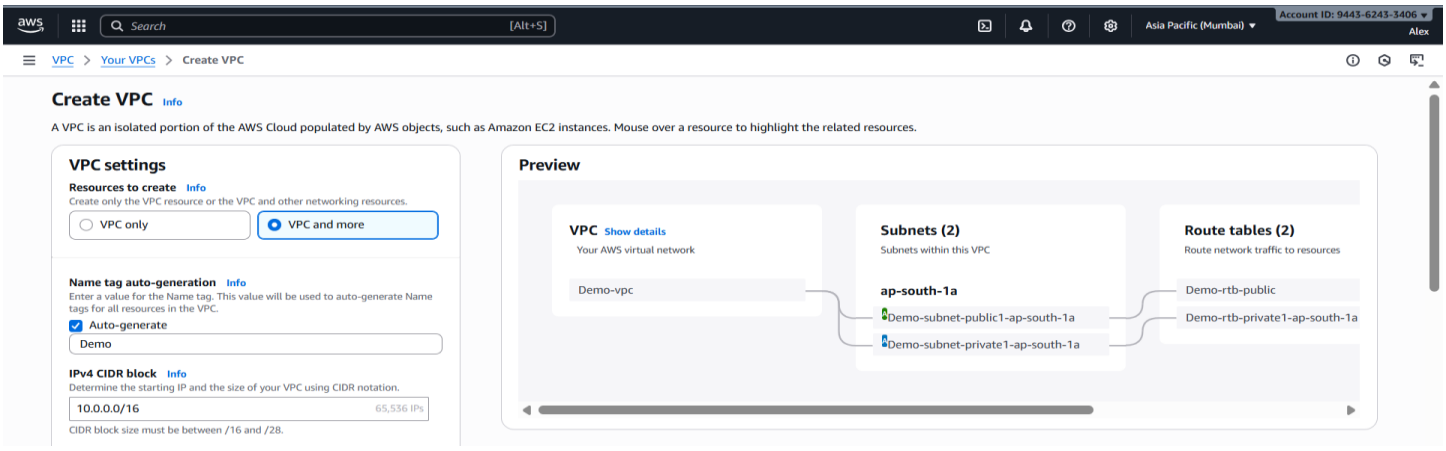


Step 12: Use Amazon VPC Wizard (Optional)

Use the VPC Wizard to create a pre-configured VPC and resources quickly.

Actions:

- - In the VPC Dashboard, click 'Launch VPC Wizard' or 'Create VPC' → 'VPC and more'.
- - Choose a template (e.g., VPC with Public and Private Subnets).
- - Review resource map (subnets, route tables, IGW, NACLs) and configuration.
- - Adjust AZ count, subnet CIDRs, and naming as needed and create the VPC.



Step 13: Set up your VPC basics (verify)

Confirm that prior project resources are present and running.

Actions:

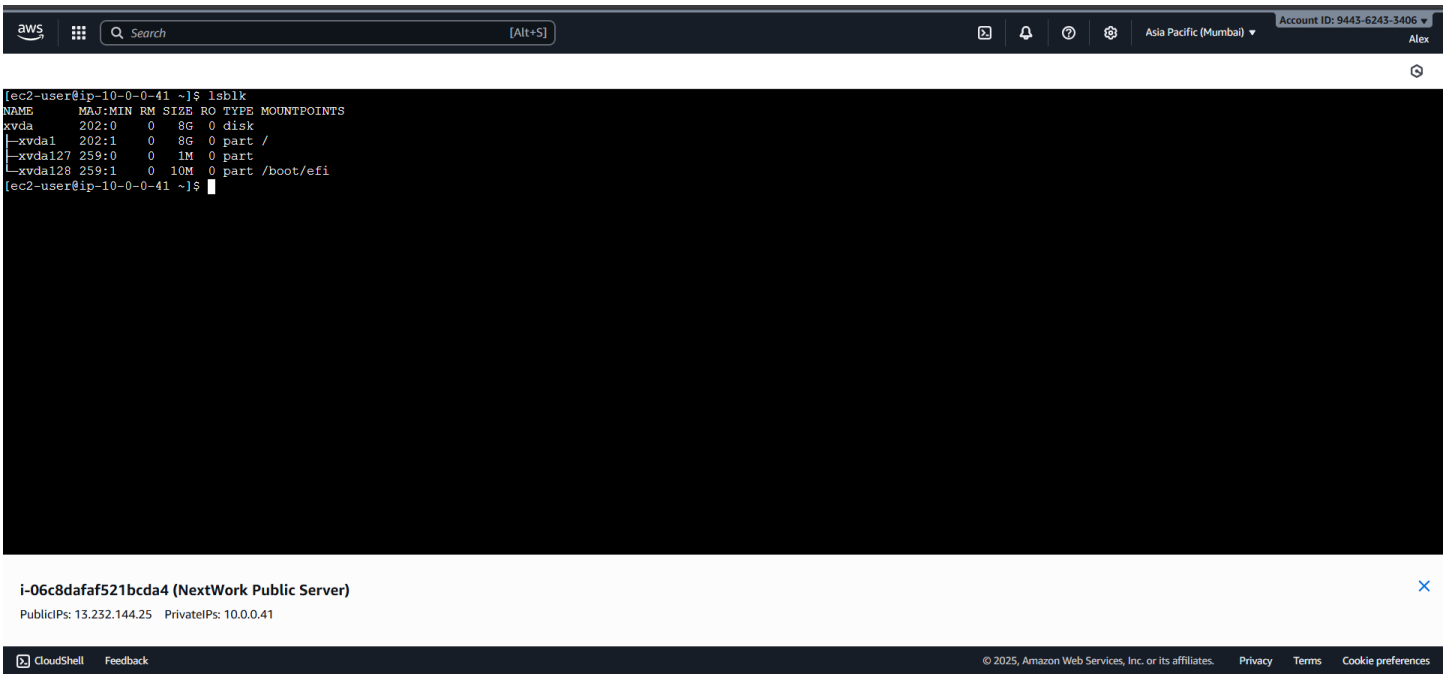
- - Open the VPC console and confirm NextWork VPC exists.
- - Verify Public and Private subnets are present.
- - Confirm the Internet Gateway is attached to NextWork VPC.
- - Check route tables (public RT has 0.0.0.0/0 → IGW).
- - Ensure NACLs and Security Groups exist and are named appropriately.
- - Verify EC2 instances (NextWork Public Server and NextWork Private Server) are running.

Step 14: Connect to NextWork Public Server (EC2 Instance Connect)

Use EC2 Instance Connect from the AWS Console to SSH into the public EC2 instance.

Actions:

- - Open EC2 Console → Instances and select NextWork Public Server.
- - Click 'Connect' → 'EC2 Instance Connect'.
- - Keep default username (ec2-user) and public IP pre-filled, then click 'Connect'.
- - If connection fails, inspect the NextWork Public Security Group inbound rules and ensure SSH (port 22) is allowed.
- - Temporarily allow SSH from Anywhere-IPv4 to ensure EC2 Instance Connect can reach your instance (note: restrict later for security).

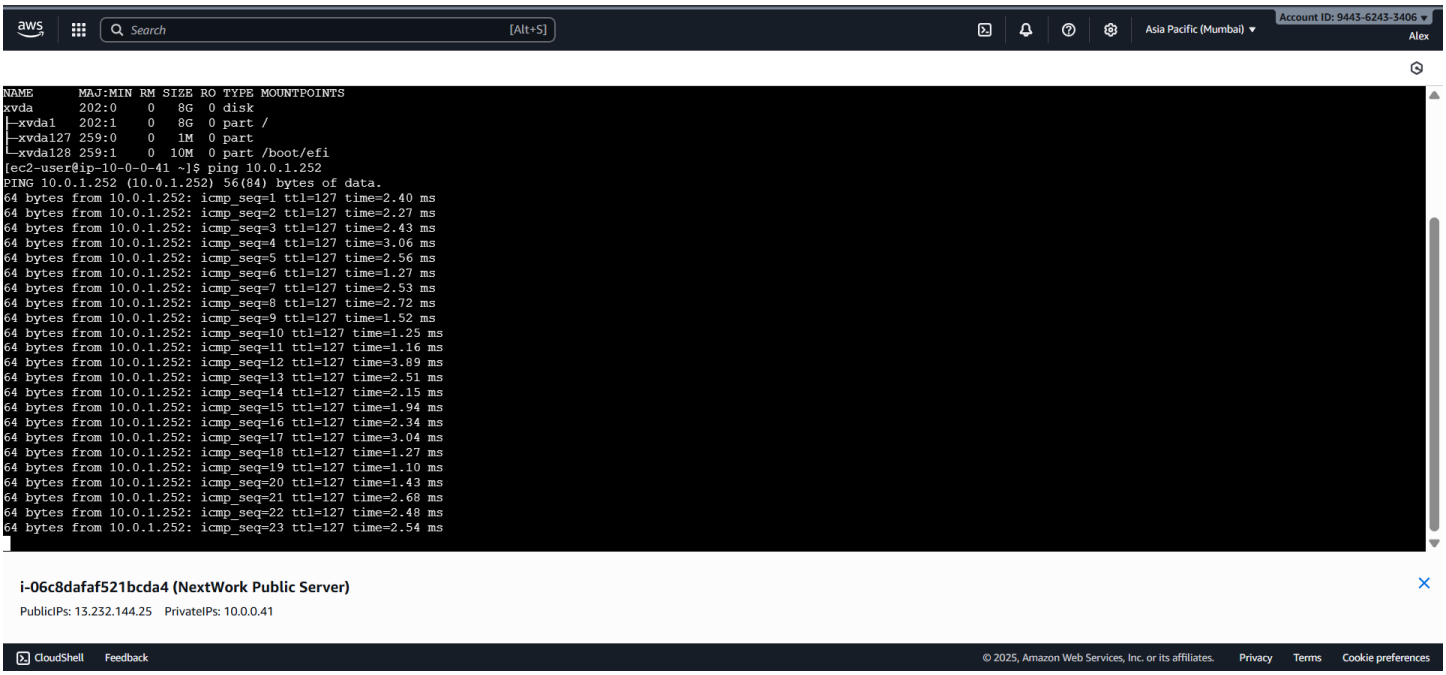


Step 15: Test connectivity between your EC2 instances (ping)

From the Public Server, ping the Private Server's private IP and troubleshoot if needed.

Actions:

- - On the EC2 console, copy the Private IPv4 address of the NextWork Private Server.
- - In the Public Server terminal (EC2 Instance Connect), run: ping <Private IPv4 Address>
- - If you receive no replies, inspect the NextWork Private NACL rules—ensure ICMP (All ICMP - IPv4) is allowed inbound from 10.0.0.0/24 and outbound to 10.0.0.0/24.
- - Inspect NextWork Private Security Group inbound rules—add All ICMP - IPv4 with Source = NextWork Public Security Group.
- - After updates, run ping again and confirm multiple replies are received.

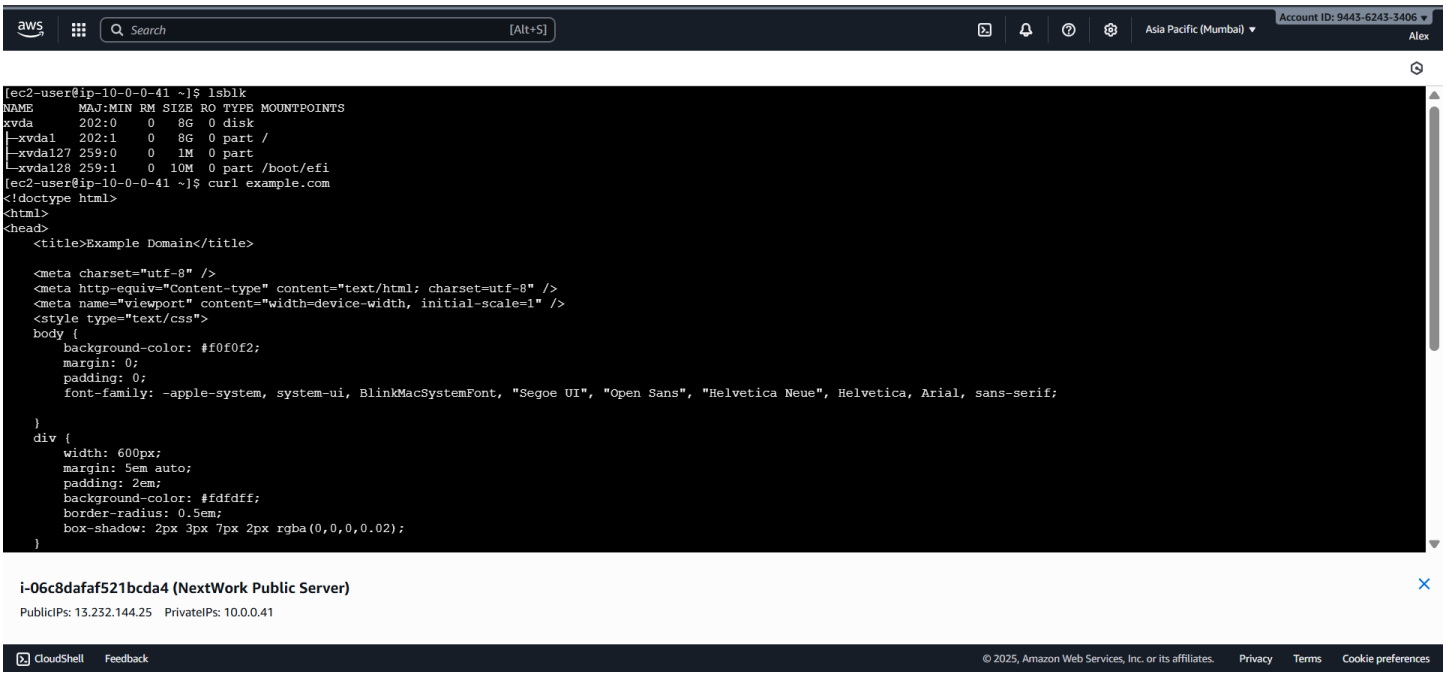


Step 16: Test VPC connectivity with the internet (curl)

From the Public Server, use curl to verify external HTTP connectivity.

Actions:

- - In the Public Server terminal, stop any running ping (Ctrl+C).
- - Run: curl example.com and confirm you receive HTML output.
- - Run: curl learn.nextwork.org and follow redirects if necessary (curl will show redirect responses).
- - Use the returned URLs to curl the final page (e.g., curl https://learn.nextwork.org/projects/...).
- - Confirm the HTML output appears—this verifies outbound internet connectivity from the public subnet.



i-06c8dafaf521bcda4 (NextWork Public Server)

PublicIPs: 13.232.144.25 PrivateIPs: 10.0.0.41