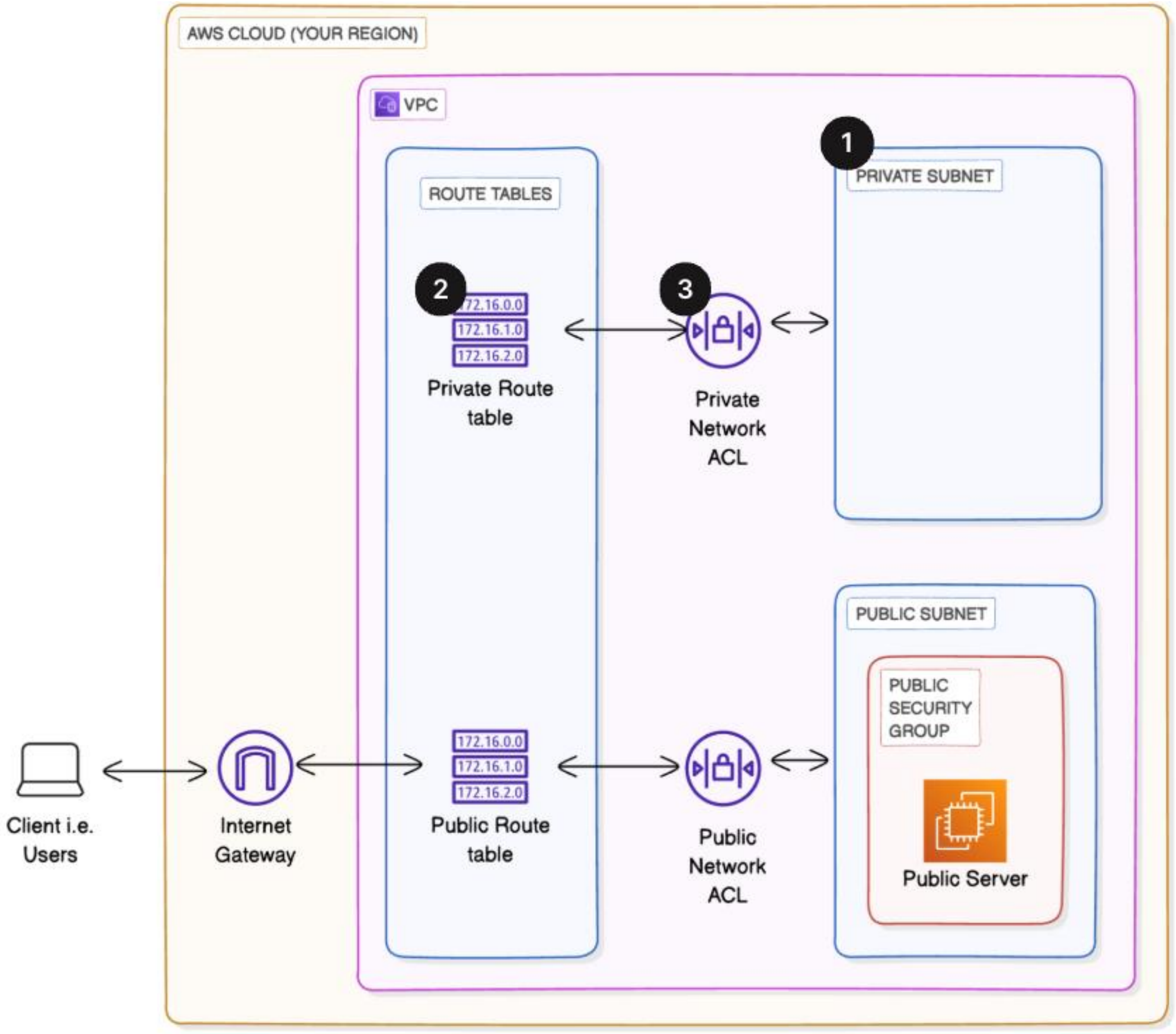
Creating a Private Subnet - Step-by-Step Documentation



This documentation provides a comprehensive, step-by-step process for setting up a private subnet in AWS. It builds on the earlier projects 'Build a Virtual Private Cloud' and 'VPC Traffic Flow and Security' and includes both the foundational steps and the new steps for configuring private networking in your VPC.

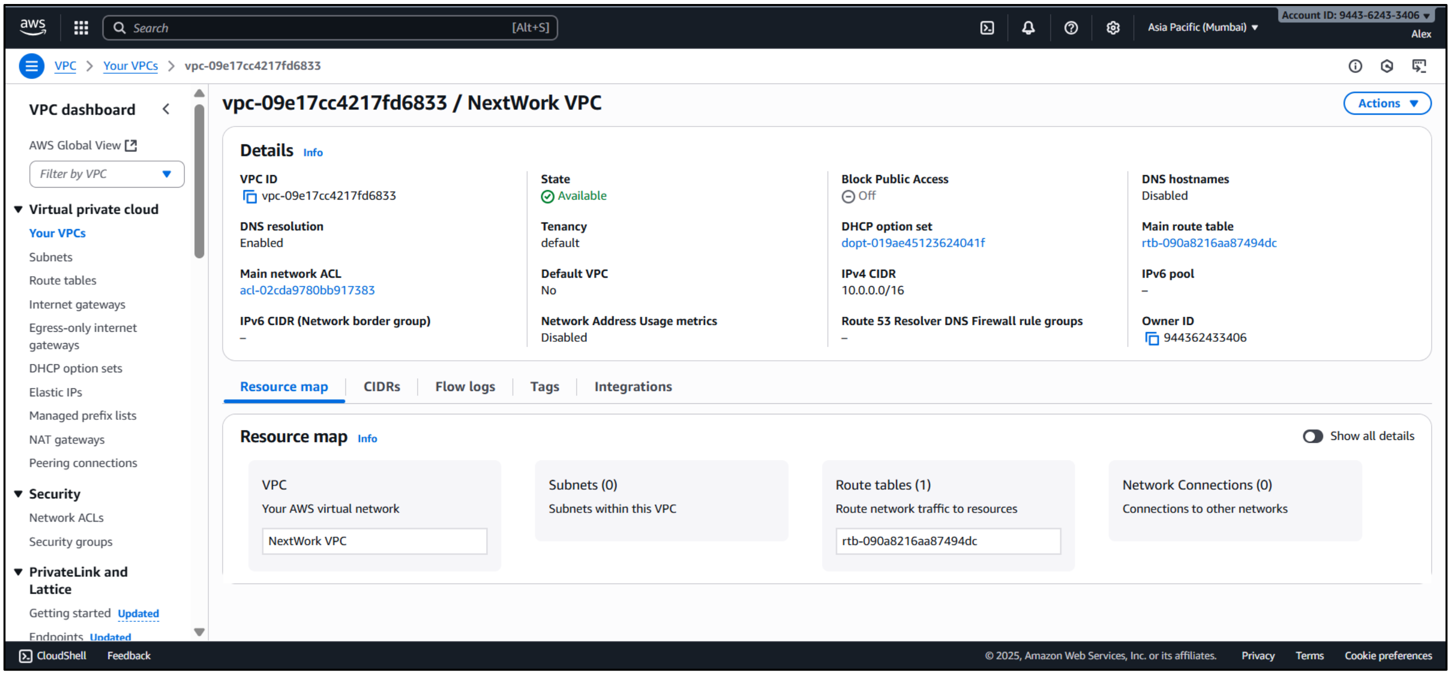
Step 1: Create a VPC

Set up a new Virtual Private Cloud in AWS.

Actions:

- - Log in to 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' option.
- - 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.



VPC > Your VPCs > vpc-09e17cc4217fd6833

vpc-09e17cc4217fd6833 / NextWork VPC

Details

VPC ID vpc-09e17cc4217fd6833	State Available	Block Public Access Off	DNS hostnames Disabled
DNS resolution Enabled	Tenancy default	DHCP option set dopt-019ae45123624041f	Main route table rtb-090a8216aa87494dc
Main network ACL acl-02cda9780bb917383	Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool –
IPv6 CIDR (Network border group) –	Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups –	Owner ID 944362433406

Resource map

VPC — Your AWS virtual network — NextWork VPC

Subnets (0) — Subnets within this VPC

Route tables (1) — Route network traffic to resources — rtb-090a8216aa87494dc

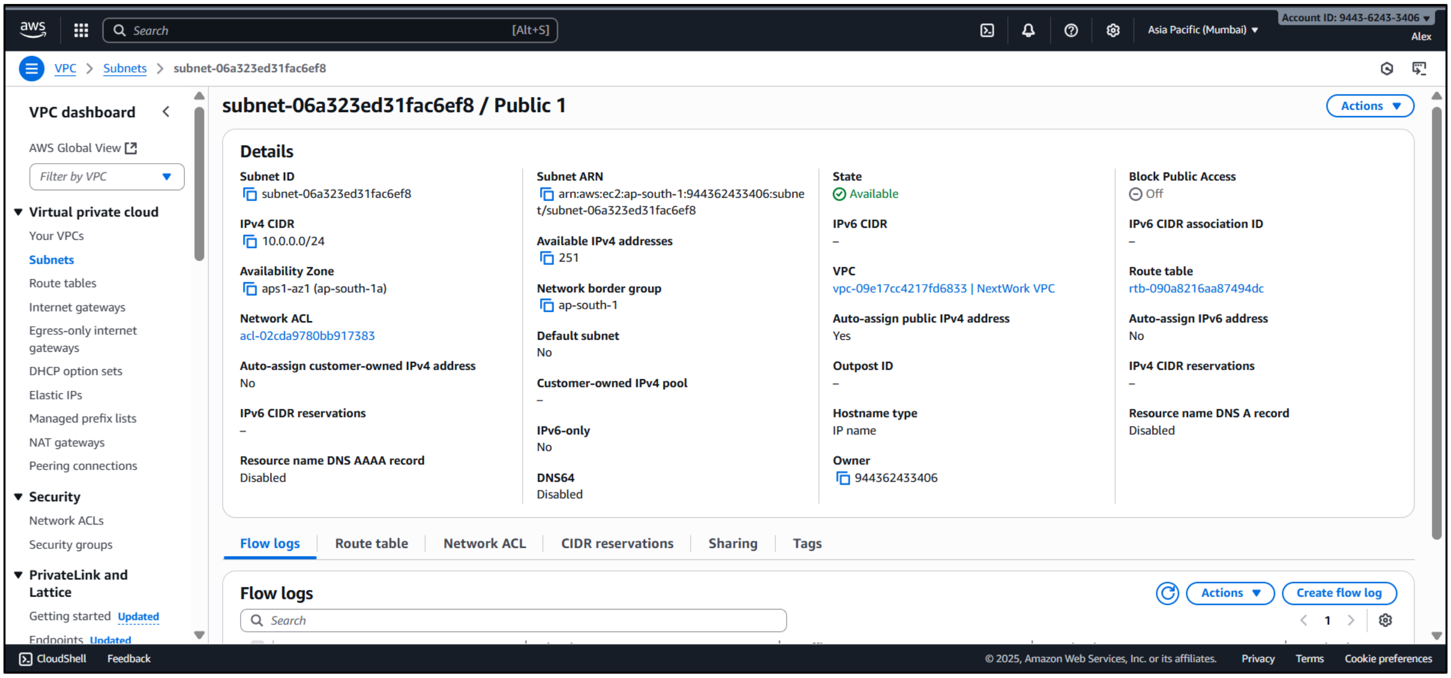
Network Connections (0) — Connections to other networks

Step 2: Create Subnets

Divide your VPC into subnets for better resource organization.

Actions:

- - From the VPC Dashboard, select 'Subnets' in the navigation pane.
- - Click 'Create subnet'.
- - Choose the VPC you just created (NextWork VPC).
- - Enter a Subnet name (e.g., Public 1).
- - Select an Availability Zone.
- - Enter an IPv4 CIDR block for the subnet (e.g., 10.0.0.0/24).
- - Click 'Create subnet'.
- - Select your new subnet and go to 'Edit subnet settings'.
- - Enable 'Auto-assign public IPv4 address'.
- - Click 'Save' to apply changes.



subnet-06a323ed31fac6ef8 / Public 1

Details

Subnet ID: subnet-06a323ed31fac6ef8

Subnet ARN: arn:aws:ec2:ap-south-1:944362433406:subnet/subnet-06a323ed31fac6ef8

State: Available

Block Public Access: Off

IPv4 CIDR: 10.0.0.0/24

Available IPv4 addresses: 251

IPv6 CIDR: –

IPv6 CIDR association ID: –

Availability Zone: aps1-az1 (ap-south-1a)

Network border group: ap-south-1

VPC: vpc-09e17cc4217fd6833 | NextWork VPC

Route table: rtb-090a8216aa87494dc

Network ACL: acl-02cda9780bb917383

Default subnet: No

Auto-assign public IPv4 address: Yes

Auto-assign IPv6 address: No

Auto-assign customer-owned IPv4 address: No

Customer-owned IPv4 pool: –

Outpost ID: –

IPv4 CIDR reservations: –

IPv6 CIDR reservations: –

IPv6-only: No

Hostname type: IP name

Resource name DNS A record: Disabled

Resource name DNS AAAA record: Disabled

DNS64: Disabled

Owner: 944362433406

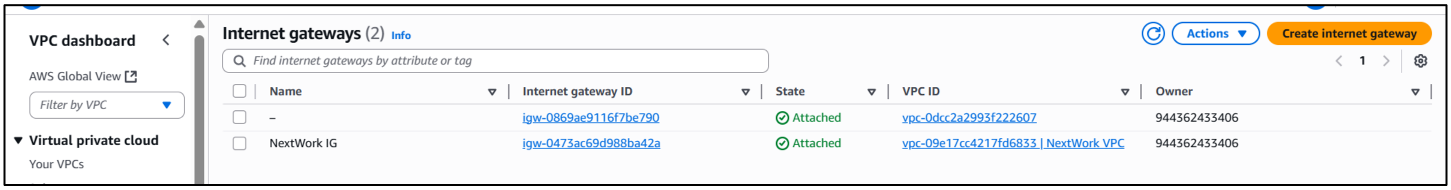
Flow logs

Step 3: Create an Internet Gateway

Attach an internet gateway to your VPC to enable internet access.

Actions:

- - In the VPC Dashboard, select 'Internet gateways' from the left-hand panel.
- - Click 'Create internet gateway'.
- - Enter a Name tag (e.g., NextWork IG).
- - Click 'Create internet gateway'.
- - Select your newly created gateway and choose 'Attach to VPC'.
- - Select your VPC (NextWork VPC) and confirm.
- - Your VPC is now connected to the internet.



Internet gateways (2)

☐	Name	Internet gateway ID	State	VPC ID	Owner
☐	–	igw-0869ae9116f7be790	Attached	vpc-0dcc2a2993f222607	944362433406
☐	NextWork IG	igw-0473ac69d988ba42a	Attached	vpc-09e17cc4217fd6833 | NextWork VPC	944362433406

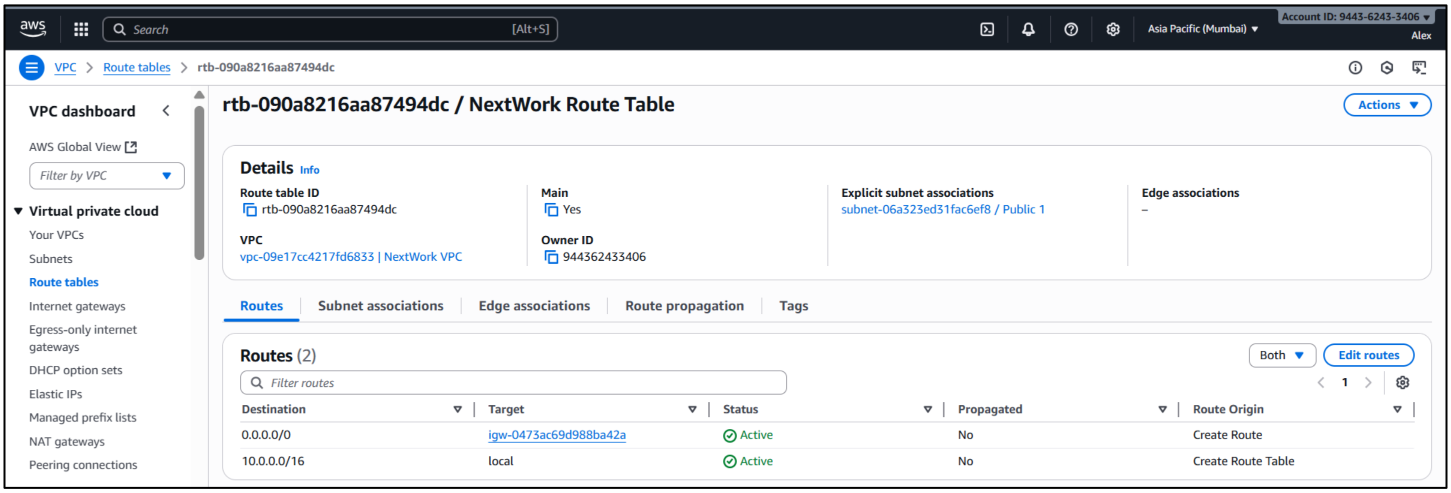
Step 4: Create a Route Table

Set up a route table to define how traffic flows in your VPC.

Actions:

- - In the VPC Dashboard, select 'Route tables' from the navigation pane.
- - Click 'Create route table'.
- - Enter a Name tag (e.g., NextWork-RouteTable).

- - Choose your VPC (NextWork VPC).
- - Click 'Create route table'.
- - Select your new route table and go to the 'Routes' tab.
- - Click 'Edit routes' and add a route with Destination = 0.0.0.0/0 and Target = your Internet Gateway.
- - Click 'Save changes'.
- - Associate the route table with your public subnet by going to the 'Subnet associations' tab and selecting 'Edit subnet associations'.
- - Choose your Public 1 subnet and save.



rtb-090a8216aa87494dc / NextWork Route Table

Details Info

Route table ID: rtb-090a8216aa87494dc

Main: Yes

Explicit subnet associations: subnet-06a323ed31fac6ef8 / Public 1

Edge associations: –

VPC: vpc-09e17cc4217fd6833 | NextWork VPC

Owner ID: 944362433406

Routes (2)

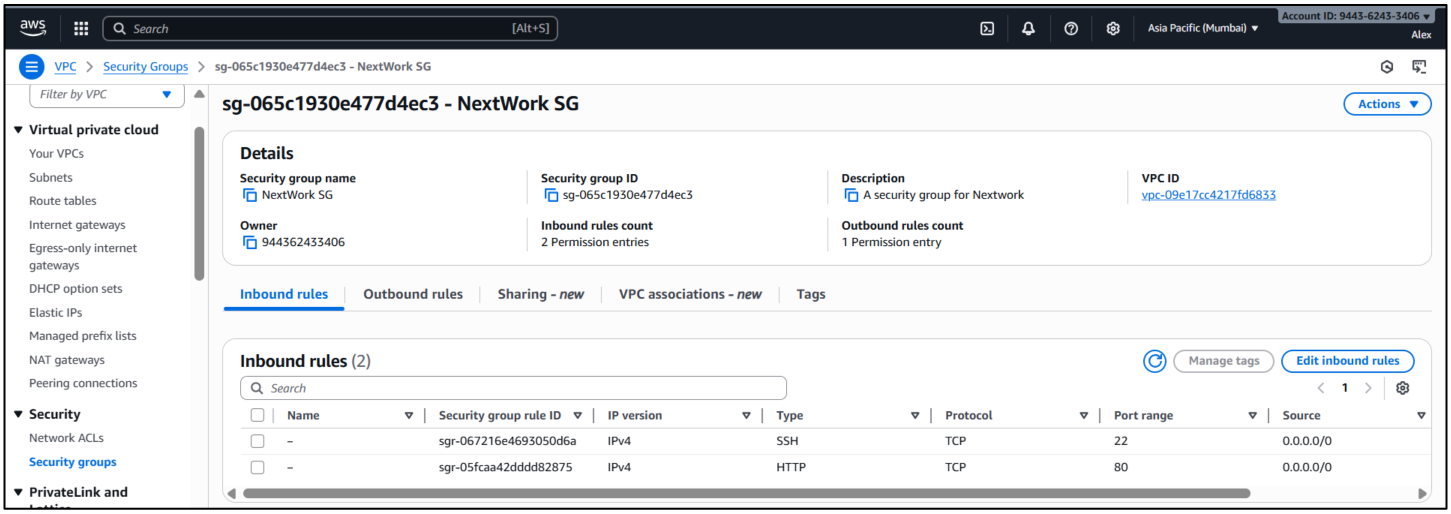
Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-0473ac69d988ba42a	Active	No	Create Route
10.0.0.0/16	local	Active	No	Create Route Table

Step 5: Create a Security Group

Create a security group to control inbound and outbound traffic for your resources.

Actions:

- - In the VPC Dashboard, select 'Security groups'.
- - Click 'Create security group'.
- - Enter a Name tag (e.g., NextWork-SG).
- - Select your VPC (NextWork VPC).
- - Add inbound rules (e.g., allow HTTP on port 80, SSH on port 22).
- - Add outbound rules (default allows all traffic).
- - Click 'Create security group' to save.



sg-065c1930e477d4ec3 - NextWork SG

Details

Security group name: NextWork SG
Security group ID: sg-065c1930e477d4ec3
Description: A security group for Nextwork
VPC ID: vpc-09e17cc4217fd6833
Owner: 944362433406
Inbound rules count: 2 Permission entries
Outbound rules count: 1 Permission entry

Inbound rules (2)

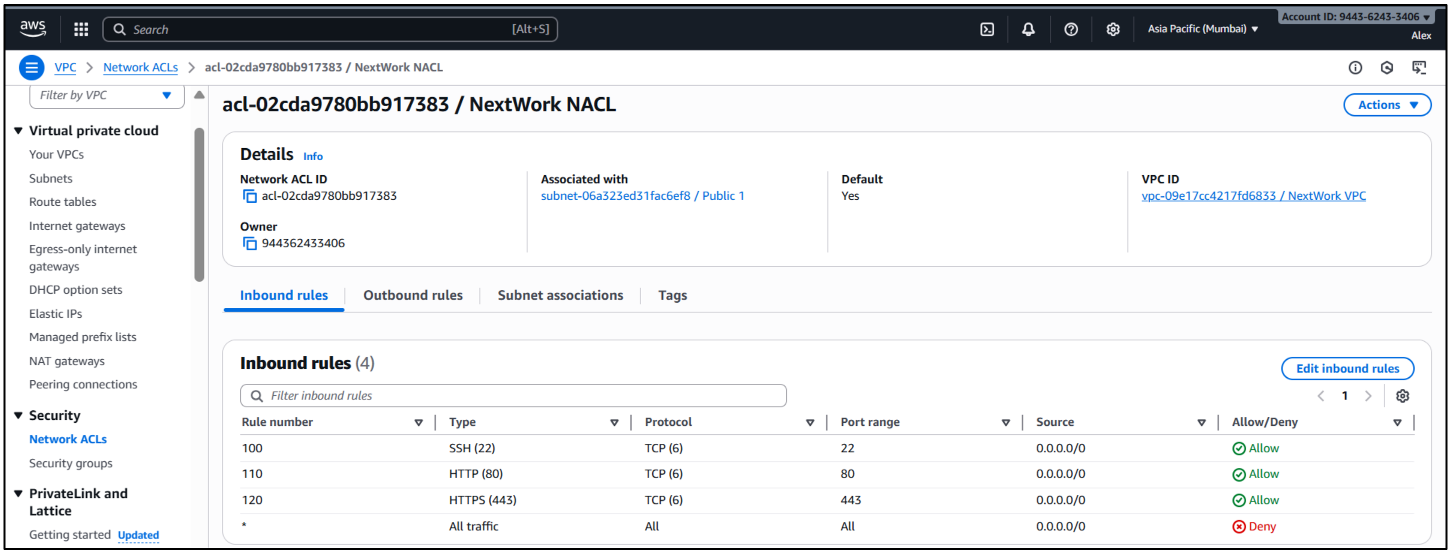
Name	Security group rule ID	IP version	Type	Protocol	Port range	Source
–	sgr-067216e4693050d6a	IPv4	SSH	TCP	22	0.0.0.0/0
–	sgr-05fcaa42dddd82875	IPv4	HTTP	TCP	80	0.0.0.0/0

Step 6: Create a Network ACL (Access Control List)

Set up a network ACL to provide an additional layer of security at the subnet level.

Actions:

- - In the VPC Dashboard, select 'Network ACLs' from the navigation pane.
- - Click 'Create network ACL'.
- - Enter a Name tag (e.g., NextWork-NACL).
- - Choose your VPC (NextWork VPC).
- - Click 'Create network ACL'.
- - Select your new NACL and go to the 'Inbound rules' tab. Add rules (e.g., allow HTTP, HTTPS, and SSH).
- - Go to the 'Outbound rules' tab and configure rules (e.g., allow all traffic).
- - Associate your NACL with the public subnet by selecting 'Subnet associations'.
- - Click 'Edit subnet associations', select your Public 1 subnet, and save.



acl-02cda9780bb917383 / NextWork NACL

Details

Network ACL ID: acl-02cda9780bb917383
Associated with: subnet-06a323ed31fac6ef8 / Public 1
Default: Yes
VPC ID: vpc-09e17cc4217fd6833 / NextWork VPC
Owner: 944362433406

Inbound rules (4)

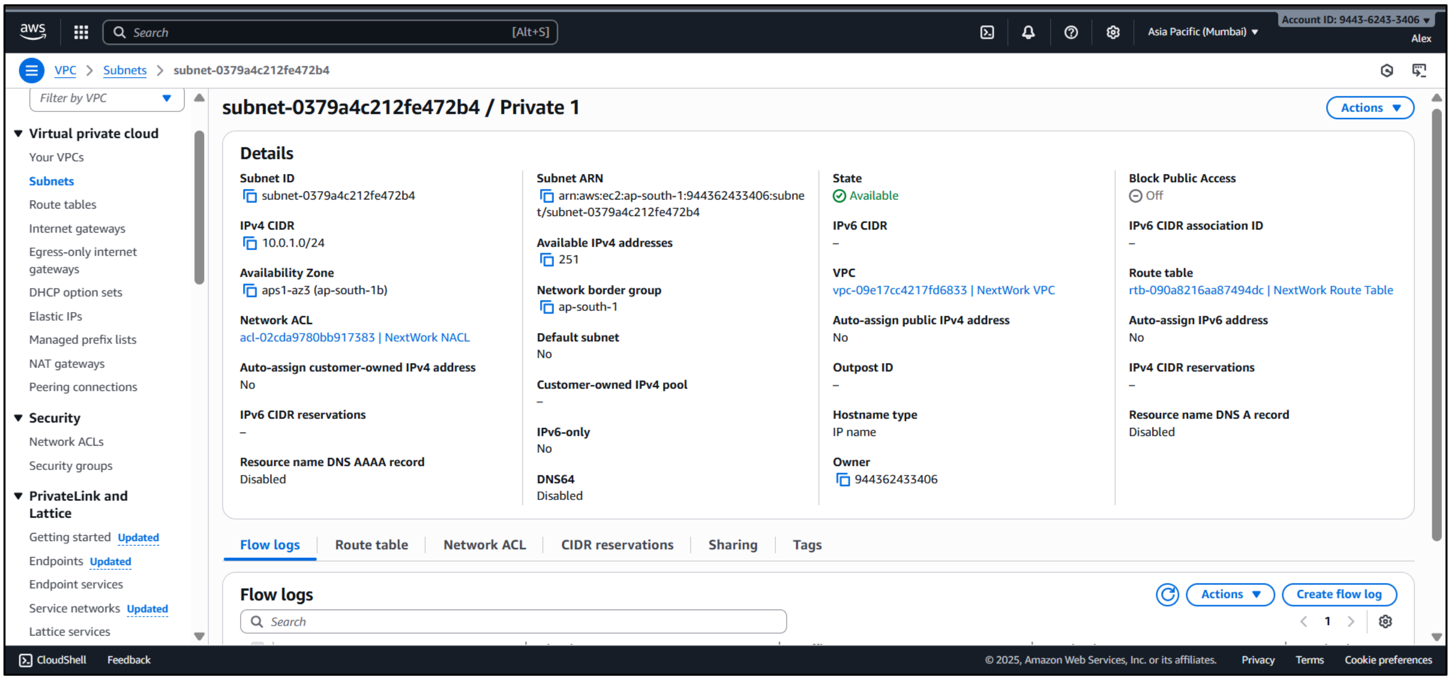
Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	SSH (22)	TCP (6)	22	0.0.0.0/0	✓ Allow
110	HTTP (80)	TCP (6)	80	0.0.0.0/0	✓ Allow
120	HTTPS (443)	TCP (6)	443	0.0.0.0/0	✓ Allow
*	All traffic	All	All	0.0.0.0/0	⊗ Deny

Step 7: Create a Private Subnet

Set up a private subnet inside your VPC.

Actions:

- - In the VPC Dashboard, choose 'Subnets'.
- - Click 'Create subnet'.
- - Select your VPC (NextWork VPC).
- - Enter a Subnet name (e.g., Private 1).
- - Select an Availability Zone (different from your public subnet for redundancy).
- - Enter an IPv4 CIDR block (e.g., 10.0.1.0/24).
- - Click 'Create subnet'.
- - Leave auto-assign public IPv4 address disabled (to keep it private).



subnet-0379a4c212fe472b4 / Private 1

Details

Subnet ID
subnet-0379a4c212fe472b4

IPv4 CIDR
10.0.1.0/24

Availability Zone
aps1-az3 (ap-south-1b)

Network ACL
acl-02cda9780bb917383 | NextWork NACL

Auto-assign customer-owned IPv4 address
No

IPv6 CIDR reservations
–

Resource name DNS AAAA record
Disabled

Subnet ARN
arn:aws:ec2:ap-south-1:944362433406:subnet/subnet-0379a4c212fe472b4

Available IPv4 addresses
251

Network border group
ap-south-1

Default subnet
No

Customer-owned IPv4 pool
–

IPv6-only
No

DNS64
Disabled

State
Available

IPv6 CIDR
–

VPC
vpc-09e17cc4217fd6833 | NextWork VPC

Auto-assign public IPv4 address
No

Outpost ID
–

Hostname type
IP name

Owner
944362433406

Block Public Access
Off

IPv6 CIDR association ID
–

Route table
rtb-090a8216aa87494dc | NextWork Route Table

Auto-assign IPv6 address
No

IPv4 CIDR reservations
–

Resource name DNS A record
Disabled

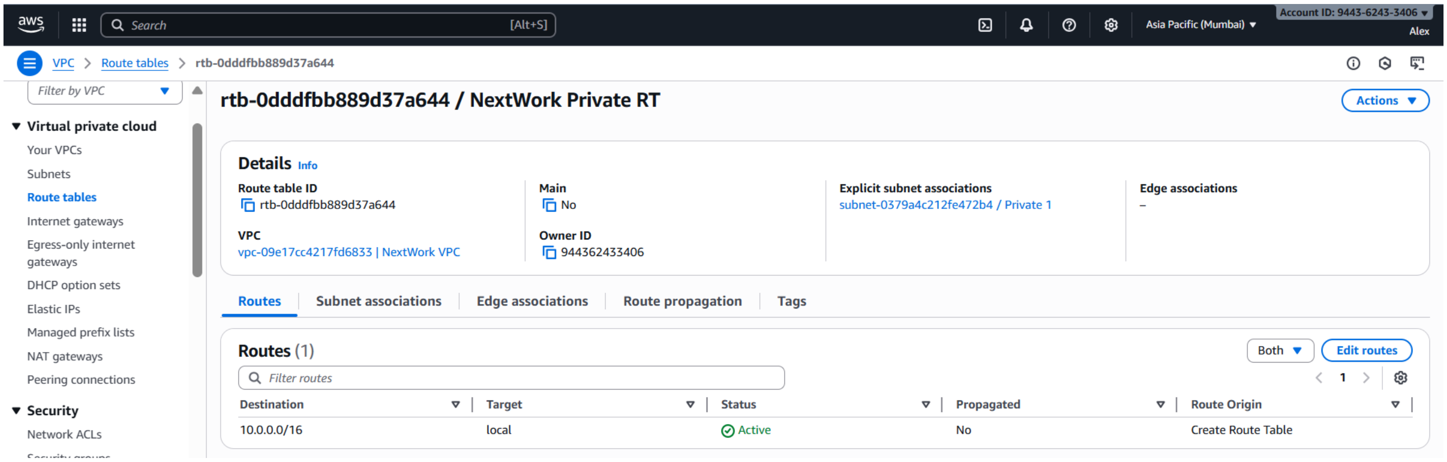
Flow logs

Step 8: Create a Private Route Table

Define routing rules for your private subnet.

Actions:

- - In the VPC Dashboard, select 'Route tables'.
- - Click 'Create route table'.
- - Enter a Name tag (e.g., NextWork-Private-RT).
- - Select your VPC (NextWork VPC).
- - Click 'Create route table'.
- - Associate this route table with your Private 1 subnet by going to 'Subnet associations'.
- - Click 'Edit subnet associations', select Private 1 subnet, and save.
- - Do not add a route to the internet gateway – keeping the subnet private.



rtb-0dddfbb889d37a644 / NextWork Private RT

Details Info

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-0dddfbb889d37a644	No	subnet-0379a4c212fe472b4 / Private 1	–
VPC	Owner ID		
vpc-09e17cc4217fd6833 | NextWork VPC	944362433406		

Routes (1)

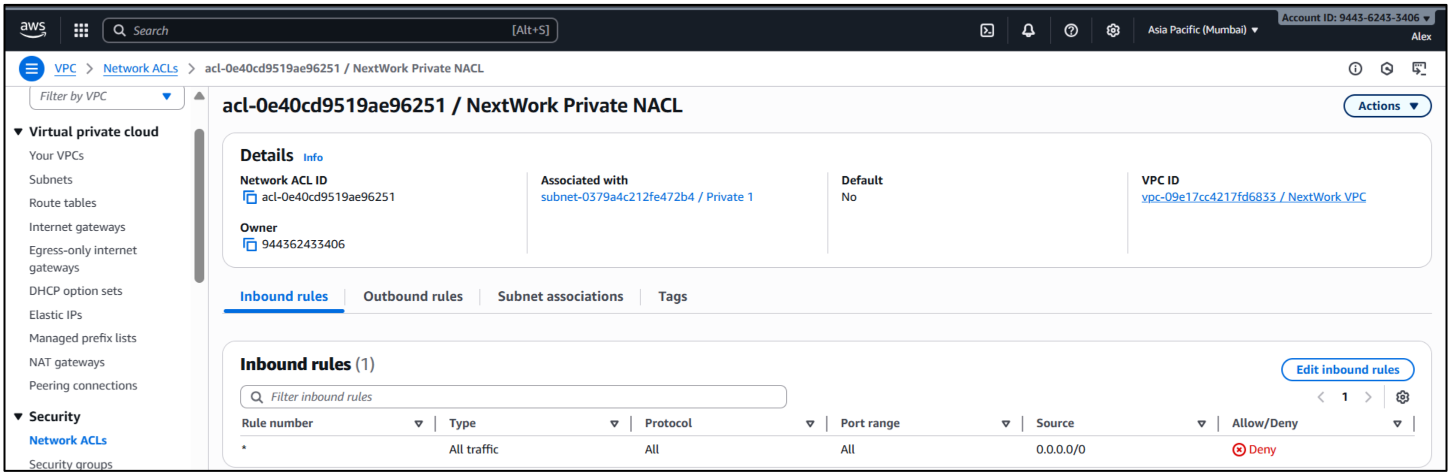
Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	✓ Active	No	Create Route Table

Step 9: Create a Private Network ACL

Configure a network ACL for your private subnet for additional security.

Actions:

- - In the VPC Dashboard, select 'Network ACLs'.
- - Click 'Create network ACL'.
- - Enter a Name tag (e.g., NextWork-Private-NACL).
- - Choose your VPC (NextWork VPC).
- - Click 'Create network ACL'.
- - In 'Inbound rules', allow only necessary internal traffic (e.g., from your public subnet or specific IP ranges).
- - In 'Outbound rules', restrict access to prevent internet connectivity.
- - Associate your new NACL with your Private 1 subnet by selecting 'Subnet associations'.
- - Click 'Edit subnet associations', select Private 1 subnet, and save.



acl-0e40cd9519ae96251 / NextWork Private NACL

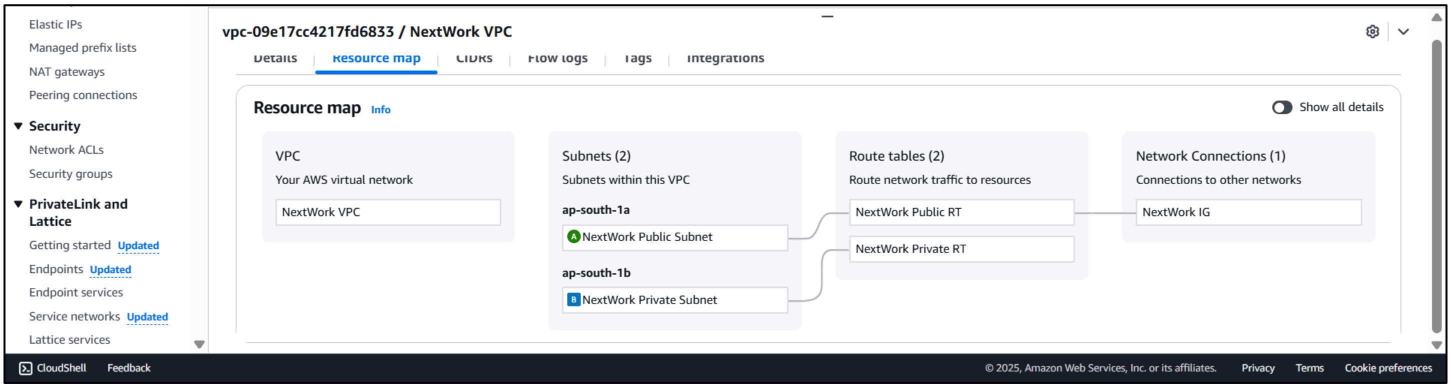
Details Info

Network ACL ID	Associated with	Default	VPC ID
acl-0e40cd9519ae96251	subnet-0379a4c212fe472b4 / Private 1	No	vpc-09e17cc4217fd6833 / NextWork VPC
Owner			
944362433406			

Inbound rules (1)

Rule number	Type	Protocol	Port range	Source	Allow/Deny
*	All traffic	All	All	0.0.0.0/0	⊗ Deny

Final VPC Resource Map:



vpc-09e17cc4217fd6833 / NextWork VPC

Resource map

VPC
Your AWS virtual network
NextWork VPC

Subnets (2)
Subnets within this VPC
ap-south-1a
A NextWork Public Subnet
ap-south-1b
B NextWork Private Subnet

Route tables (2)
Route network traffic to resources
NextWork Public RT
NextWork Private RT

Network Connections (1)
Connections to other networks
NextWork IG