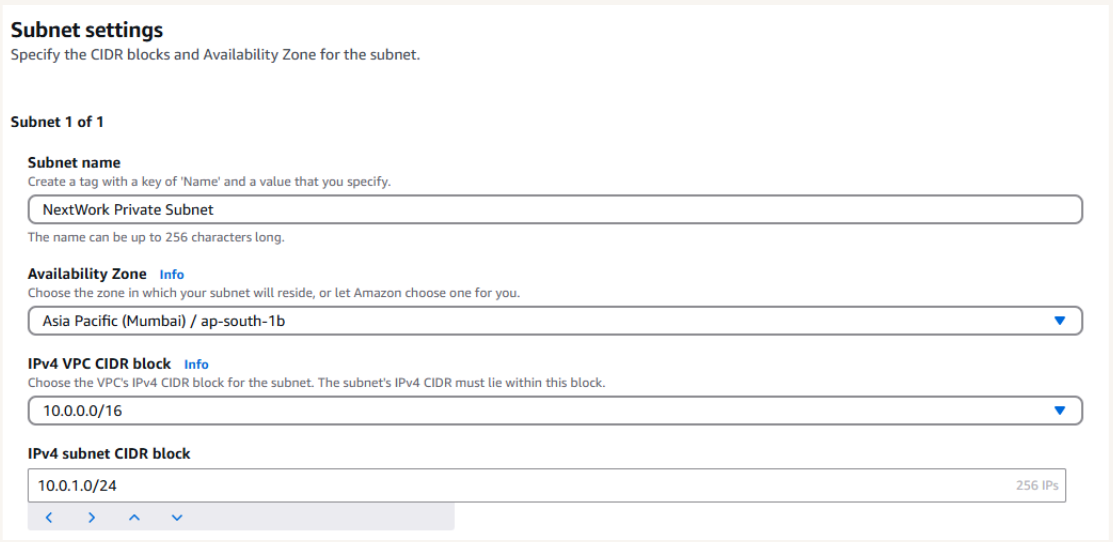
Creating a Private Subnet

RA **Ranjith D B**



RA
Ranjith D B
NextWork Student
NextWork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC lets you create a private, isolated network in AWS, giving full control over IP addressing, routing, and security. It’s useful for securely hosting applications and managing network access.

How I used Amazon VPC in this project

I used Amazon VPC to create a private subnet, set up a dedicated route table, and configured a network ACL to control traffic and enhance security for internal resources.

One thing I didn't expect in this project was...

I didn’t expect that custom network ACLs start by denying all traffic, requiring explicit rules to allow any communication within the VPC.

This project took me...

This project took me about 1 hour to complete.

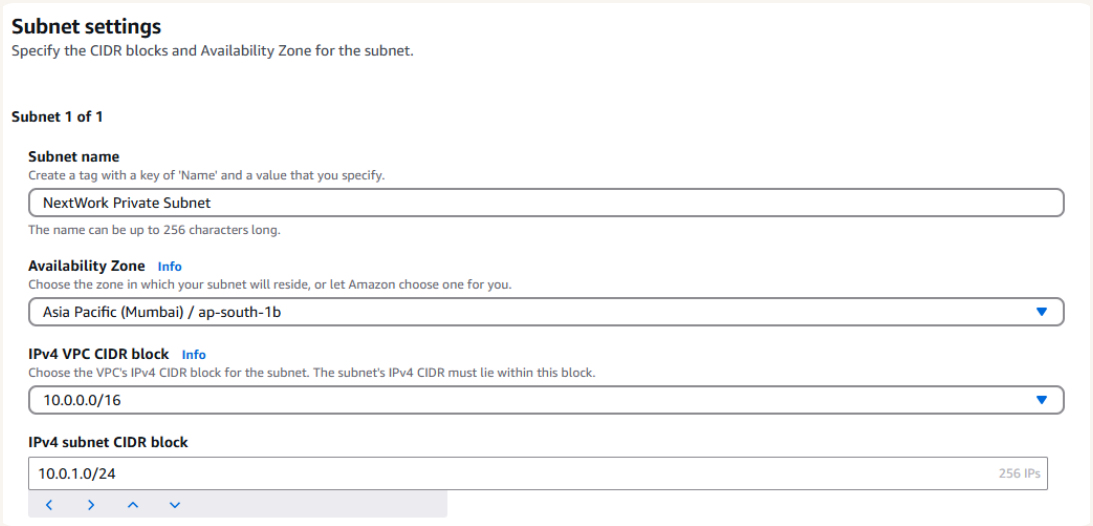
RA
Ranjith D B
NextWork Student

Private vs Public Subnets

The difference between public and private subnets is that public subnets have direct internet access via an internet gateway, while private subnets are isolated and can only access the internet through a NAT gateway or VPN.

Having private subnets are useful because they enhance security by keeping sensitive resources, like databases, protected from direct internet access, reducing exposure to attacks while still allowing internal communication.

My private and public subnets cannot have the same CIDR block because each subnet in a VPC must have a unique IP range to avoid conflicts and ensure proper traffic routing within the network.

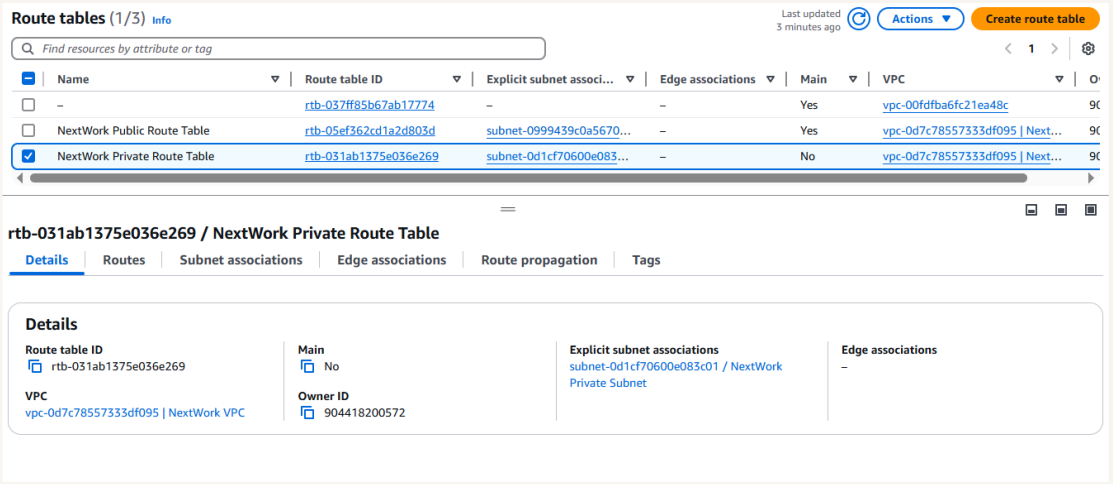

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.
Subnet 1 of 1
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
NextWork Private Subnet
The name can be up to 256 characters long.
Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
Asia Pacific (Mumbai) / ap-south-1b
IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16
IPv4 subnet CIDR block
10.0.1.0/24
256 IPs

A dedicated route table

By default, my private subnet is associated with the VPC's main route table, which initially allows all traffic within the VPC but does not provide external internet access unless explicitly configured.

I had to set up a new route table because my private subnet should not have a route to an internet gateway, ensuring that resources within it remain isolated from the public internet.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows internal traffic within the VPC while blocking direct access to the internet.


Route tables (1/3) Info
Last updated 3 minutes ago
Actions
Create route table
Find resources by attribute or tag
Name
Route table ID
Explicit subnet associ...
Edge associations
Main
VPC
– rtb-037ff85b67ab17774 – – Yes vpc-00fdfba6fc21ea48c
NextWork Public Route Table rtb-05ef362cd1a2d803d subnet-0999439c0a5670... – Yes vpc-0d7c78557333df095 | Next...
NextWork Private Route Table rtb-031ab1375e036e269 subnet-0d1cf70600e083... – No vpc-0d7c78557333df095 | Next...
rtb-031ab1375e036e269 / NextWork Private Route Table
Details
Routes
Subnet associations
Edge associations
Route propagation
Tags
Details
Route table ID
rtb-031ab1375e036e269
Main
No
Explicit subnet associations
subnet-0d1cf70600e083c01 / NextWork Private Subnet
Edge associations
–
VPC
vpc-0d7c78557333df095 | NextWork VPC
Owner ID
904418200572

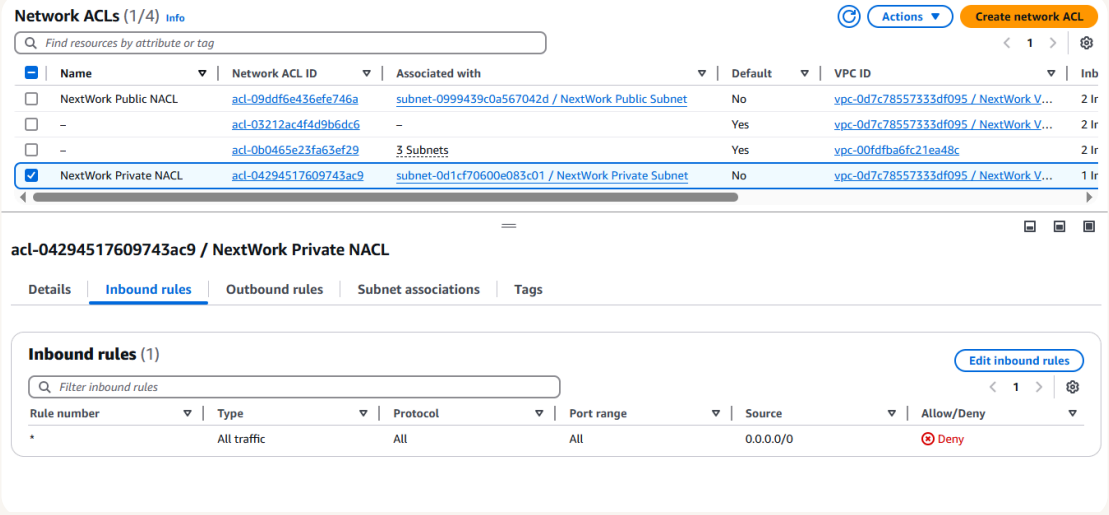
RA
Ranjith D B
NextWork Student

A new network ACL

By default, my private subnet is associated with the VPC's default network ACL, which allows all inbound and outbound traffic unless explicitly restricted.

I set up a dedicated network ACL for my private subnet because the default ACL permits all traffic, and I want to enforce stricter security controls to limit access.

My new network ACL has two simple rules—by default, it denies all inbound and outbound traffic until specific rules are added to allow necessary communication.



Everyone should be in a job they love.

Check out nextwork.org for more projects