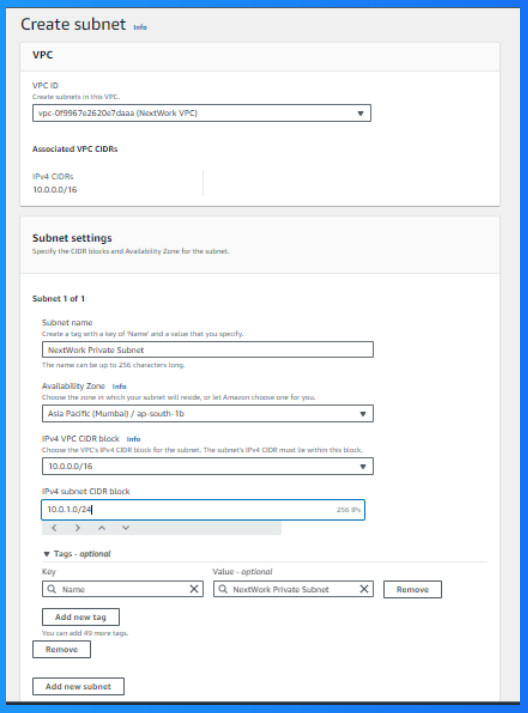
NextWork.org

Creating a Private Subnet

Roshan Thomas



Roshan Thomas
NextWork Student

NextWork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a service that lets you create isolated virtual networks within AWS. It's useful for securely managing and controlling resources, providing privacy, and ensuring customized network configurations tailored to your needs.

How I used Amazon VPC in this project

I used Amazon VPC to create a private subnet for securely hosting internal resources, while keeping them isolated from public internet access. This included setting up dedicated route tables and network ACLs for enhanced security.

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

I didn't expect that subnet CIDR blocks needed to be unique to avoid overlaps. It was surprising to see how critical it is to manage IP ranges to prevent routing conflicts within the VPC.

This project took me...

1 hour 40 minutes.

Roshan Thomas
NextWork Student

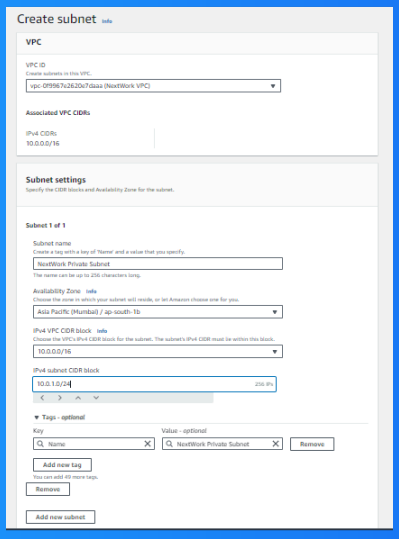
NextWork.org

Private vs Public Subnets

The difference between public and private subnets is that public subnets are like open streets connected to the internet, while private subnets are secluded neighborhoods, hidden away with no direct internet access!

Having private subnets is useful because they keep sensitive resources tucked away from the internet, like a secret hideout, allowing secure operations without public exposure!

My private and public subnets cannot have the same IP address range. It's like ensuring two neighborhoods don't share the same street names—each needs its own space to avoid confusion and traffic jams!



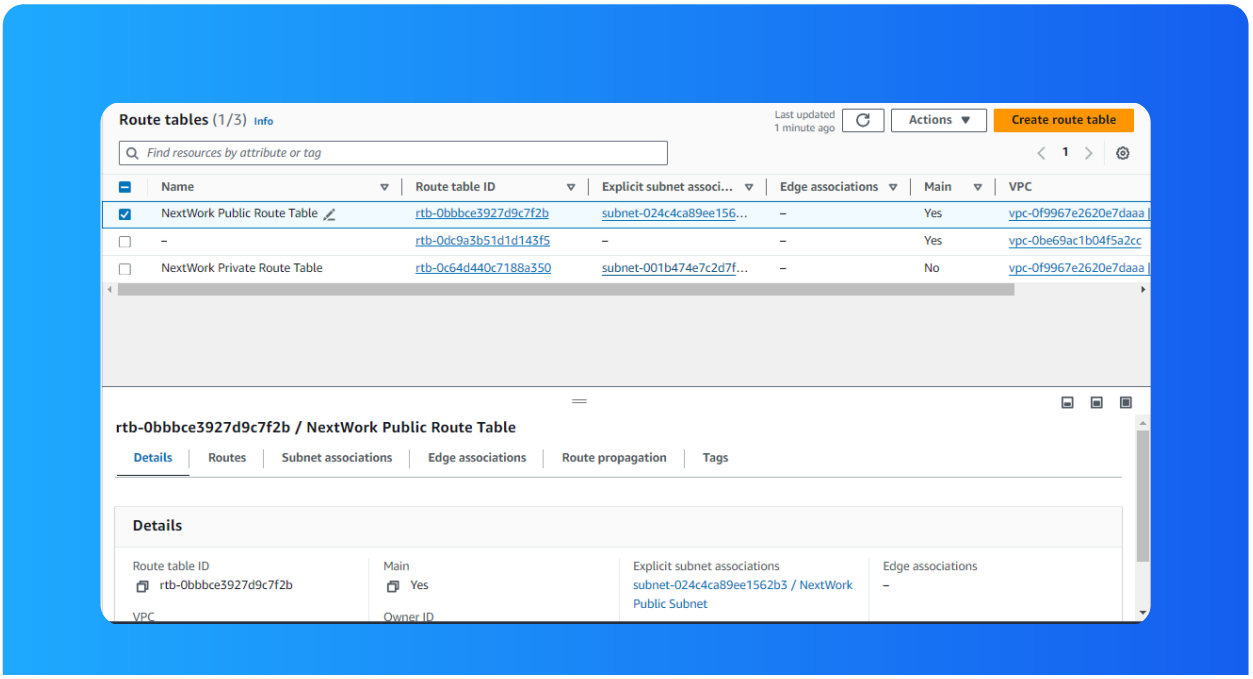
Roshan Thomas
NextWork Student

A dedicated route table

By default, my private subnet is associated with the main route table, which doesn't have a route to the internet. It's like a neighborhood with roads that don't lead outside, keeping it off the map!

I had to set up a new route table because I needed to give my public subnet a path to the internet. It's like adding a highway to connect my neighborhood to the rest of the world!

My private subnet's dedicated route table only has one inbound and one outbound rule that allows local traffic within the VPC. It's like a private road, only letting cars from the same neighborhood pass through!



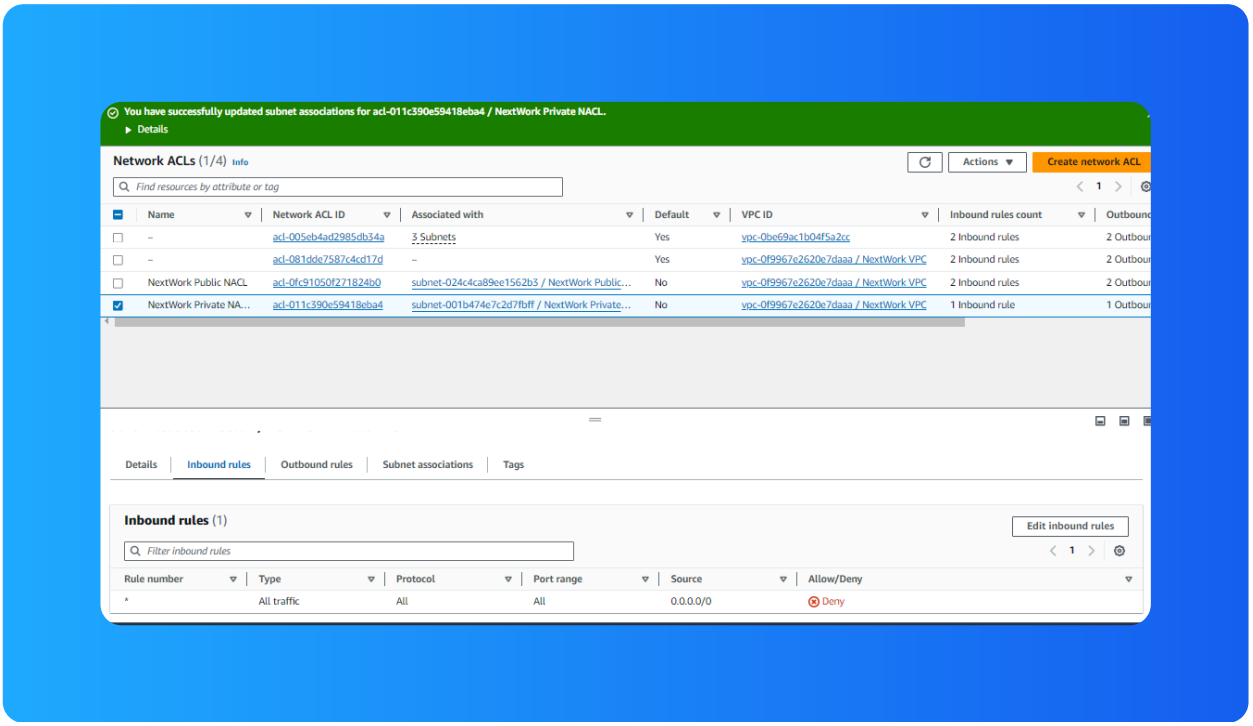
Roshan Thomas
NextWork Student

A new network ACL

By default, my private subnet is associated with the default NACL, which allows all traffic in and out. It's like a neighborhood gate that doesn't stop anyone, letting everything flow freely!

I set up a dedicated network ACL for my private subnet because I wanted tighter security. It's like hiring extra security guards to control who gets in and out of my exclusive neighborhood!

My new network ACL has two simple rules - allow inbound traffic from within the VPC and allow outbound traffic to the VPC. It's like letting neighbors visit but only allowing trips within the local area!



Everyone should be in a job they love.

Check out nextwork.org for more projects