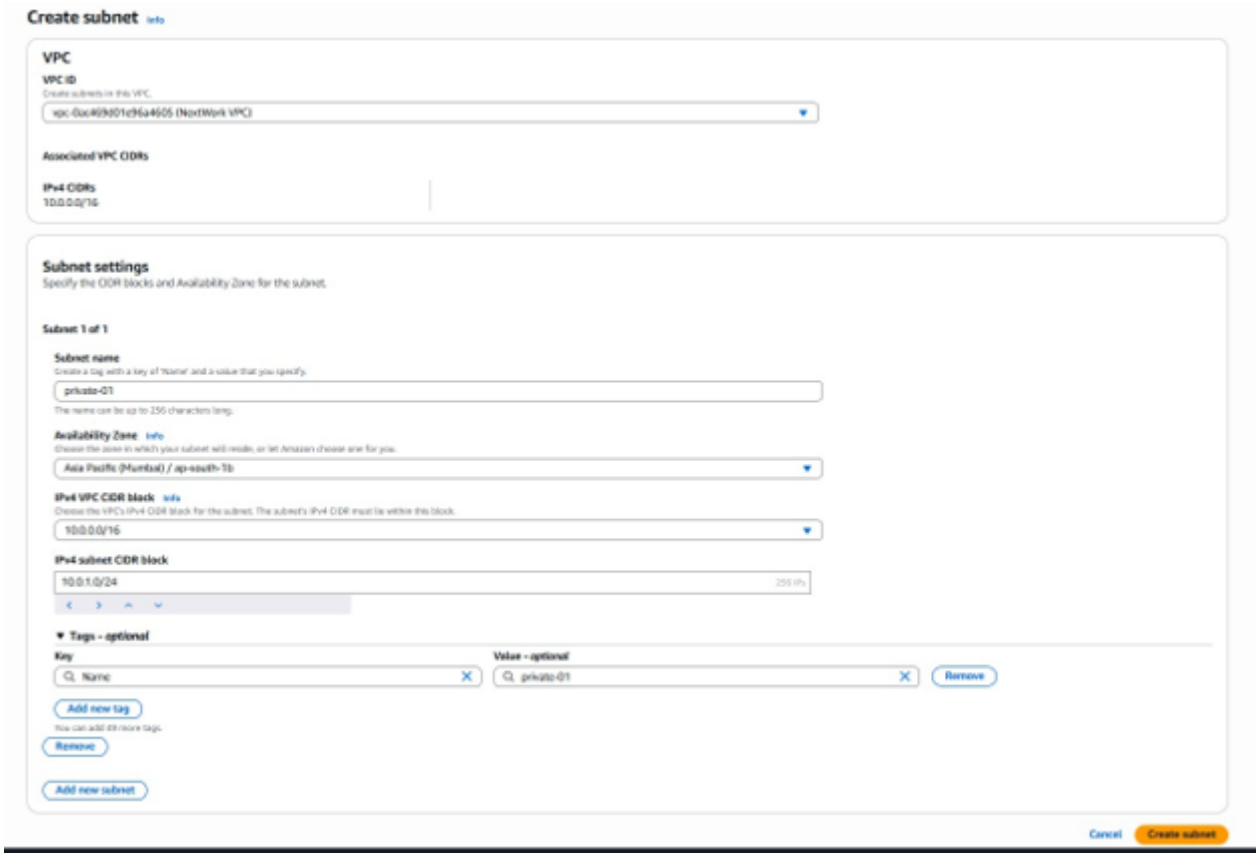
Creating a Private Subnet

Sanjana Tripathy



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) lets you create a logically isolated network in the AWS cloud where you can launch resources like EC2 instances. It's useful because it gives you full control over networking, including IP ranges, subnets, routing.

How I used Amazon VPC in this project

In today’s project, I used Amazon VPC to design a secure virtual network by creating a private subnet. I set upa custom route table, and configured a network ACL to control and restrict traffic flow for the private subnet.

This project took me...

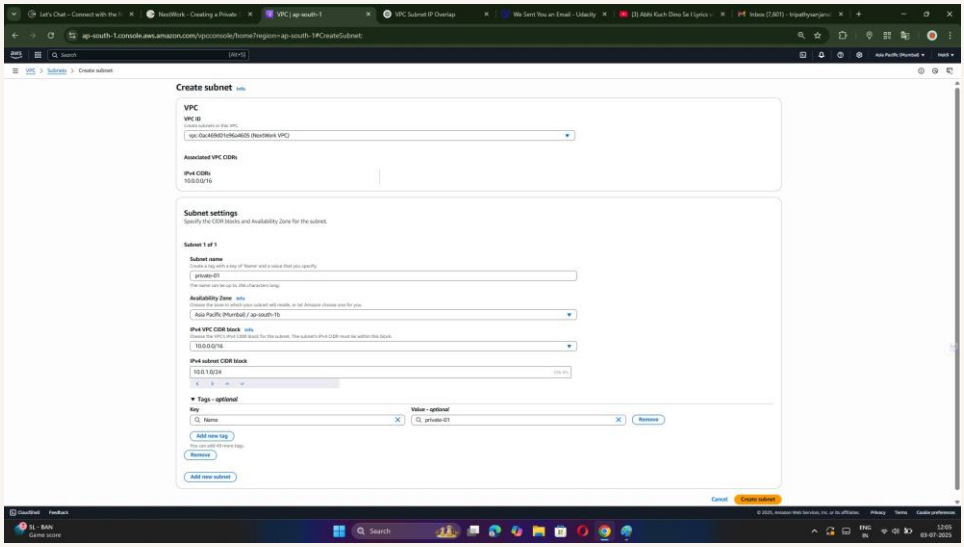
This project took me 1 hour to complete.

Private vs Public Subnets

A public subnet has a route to the internet via an Internet Gateway, allowing resources (like EC2) to be accessed from the internet. A private subnet has no direct internet route, keeping its resources isolated from public access.

Having private subnets is useful because they keep sensitive resources (like databases or internal servers) isolated from the internet, improving security and reducing exposure to external threats.

My private and public subnets cannot have the same same CIDR block. Each subnet in a VPC must have a unique, non-overlapping IP range to avoid routing conflicts.

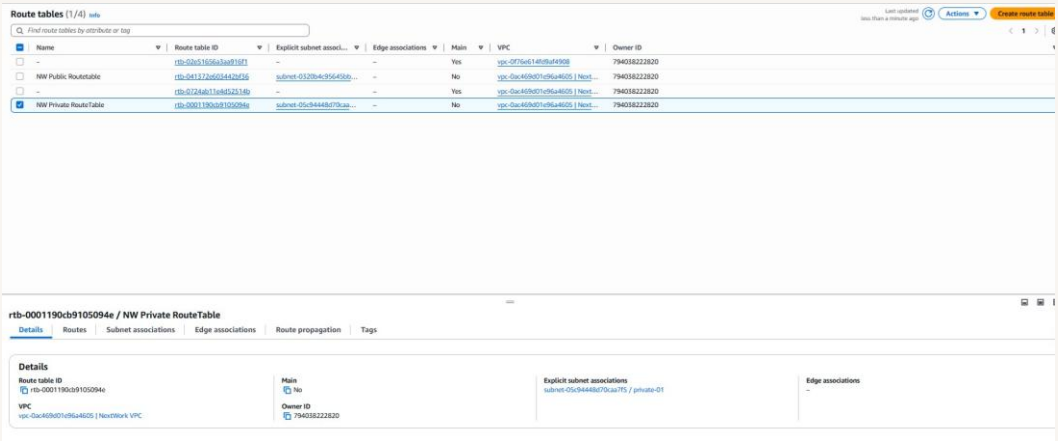


A dedicated route table

By default, my private subnet is associated with the main route table that was created along with the VPC. This default route table applies to all subnets unless explicitly associated with a custom one.

By default, my private subnet is associated with the main route table created with the VPC. However, to make it truly private, I create a new route table without a route to the internet, as the default table routes traffic to the Internet Gateway.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows local traffic within the VPC, ensuring the subnet remains isolated from the internet.

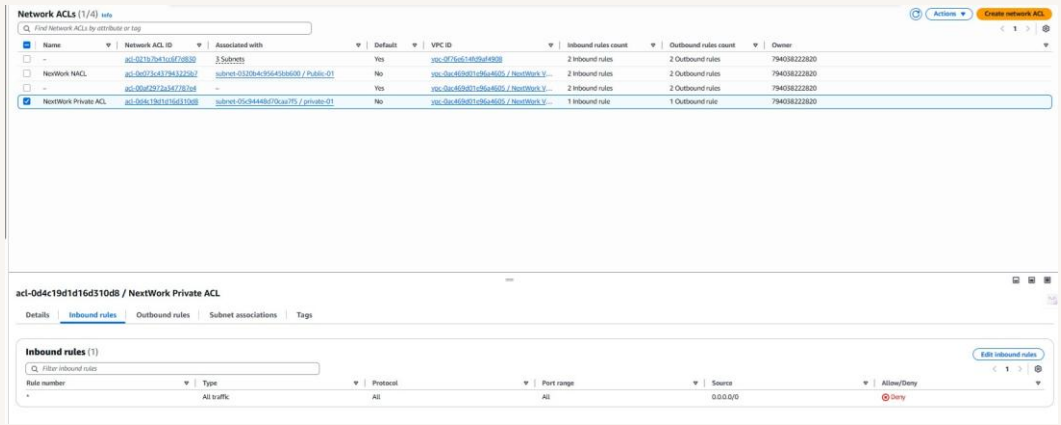


A new network ACL

By default, my private subnet is associated with with the default network ACL created when VPC was created.

I set up a dedicated network ACL for my private subnet because it allows me to define strict inbound and outbound rules, adding an extra layer of security to control traffic at the subnet level.

n my new NACL, the inbound rule denies all traffic by default (0.0.0.0/0). The outbound rule also denies all traffic. This ensures strict isolation, and I can add specific allow rules to permit only internal VPC communication as needed.



The place to learn & showcase your skills

Check out nextwork.org for more projects