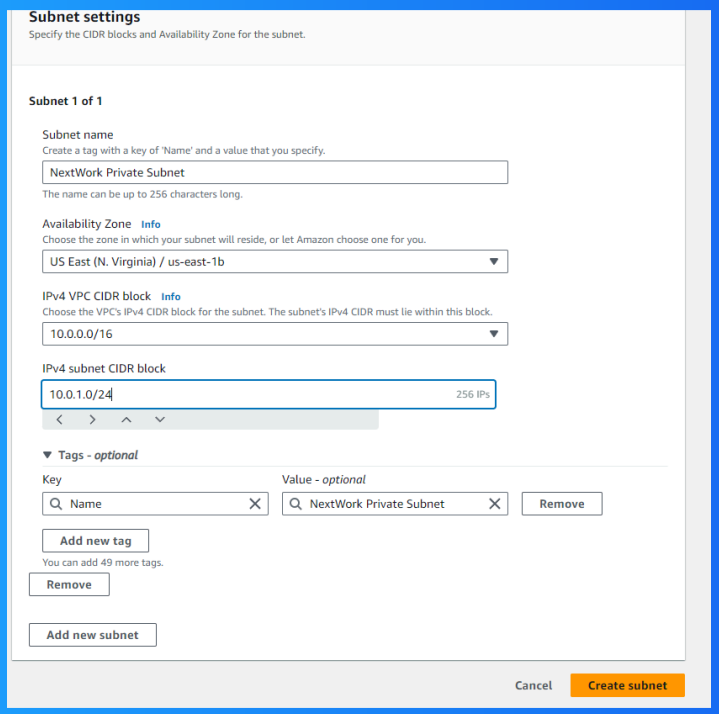
NextWork.org

# Creating a Private Subnet

Sai Prasanth Reddy



**Sai Prasanth Reddy**
NextWork Student



# Introducing Today's Project!

## What is Amazon VPC?

Amazon VPC is a service that lets you create isolated cloud networks in AWS. It’s useful because it provides control over networking, including IP ranges, subnets, and security, enabling secure, scalable, and customizable cloud infrastructure.

## How I used Amazon VPC in this project

I used Amazon VPC in today's project to create an isolated network, set up private subnets and configured route tables to ensure proper network access and security for my resources.

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

One thing I didn't expect in this project was encountering an error for assigning the same CIDR block to both subnets. I had to ensure each subnet had a unique CIDR range to avoid conflicts in routing traffic.

## This project took me...

This project took me about 45 minutes, with extra time spent resolving the CIDR block conflict and configuring the route tables and network ACLs for the private subnet.

**Sai Prasanth Reddy**
NextWork Student

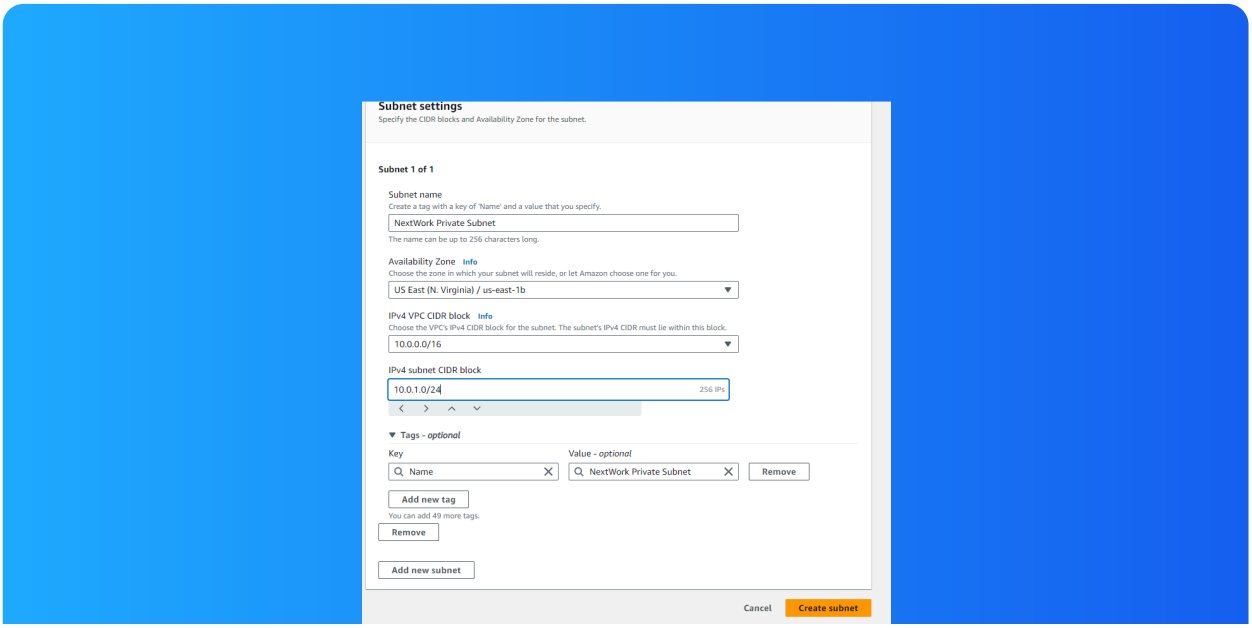


# Private vs Public Subnets

The difference between public and private subnets is that public subnets have a route to the internet through an internet gateway, allowing external access, while private subnets do not, restricting them to internal network communication.

Having private subnets are useful because they enhance security by isolating sensitive resources from direct internet access, allowing internal communication while still accessing the internet through a NAT gateway for outbound traffic.

My private and public subnets cannot have the same IP address range, as each subnet must have a unique CIDR block within the VPC to properly route traffic without conflicts.



**Sai Prasanth Reddy**
NextWork Student

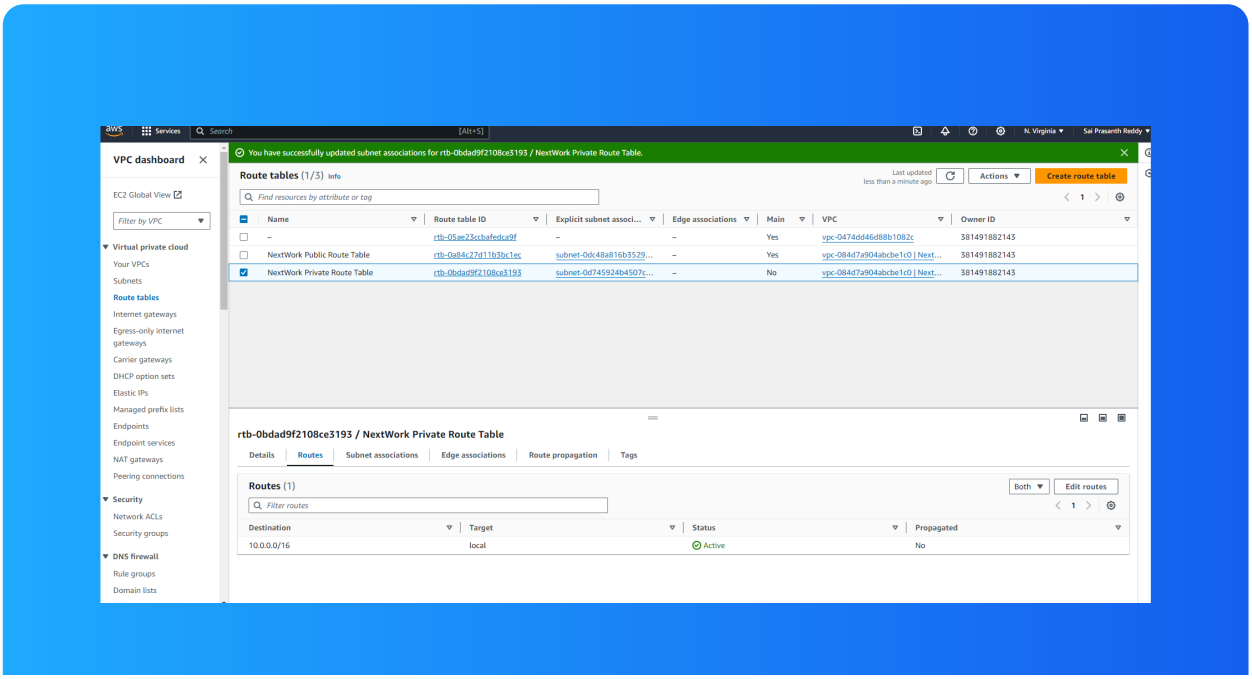


# A dedicated route table

By default, my private subnet is associated with the main route table of the VPC, which does not have a route to the internet gateway, ensuring it remains isolated from external internet access.

I had to set up a new route table because my private and public subnets need different routing configurations, with the public subnet requiring a route to the internet gateway and the private subnet remaining isolated.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows traffic within the VPC, enabling internal communication without allowing direct internet access.



**Sai Prasanth Reddy**
NextWork Student

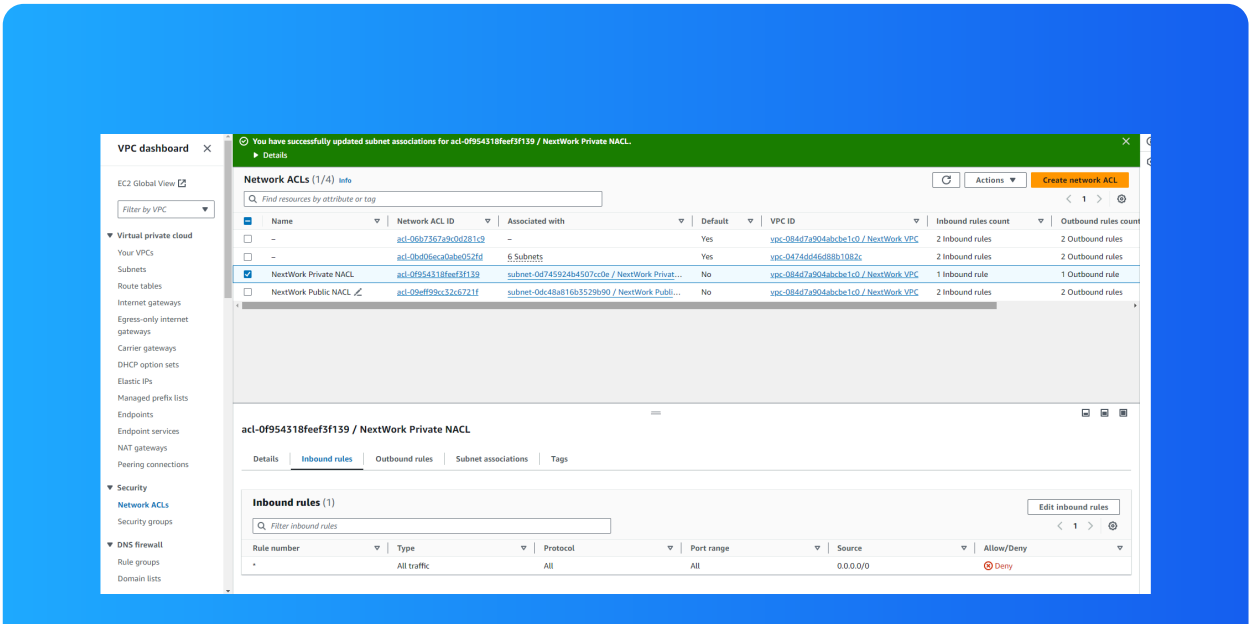


# A new network ACL

By default, my private subnet is associated with the VPC's default network ACL, which allows all inbound and outbound traffic unless custom rules are set to restrict it.

I set up a dedicated network ACL for my private subnet because I needed more granular control over inbound and outbound traffic, allowing me to enhance security by defining specific rules for traffic filtering at the subnet level.

My new network ACL has two simple rules — one inbound rule allowing internal VPC traffic and one outbound rule allowing traffic to other subnets within the VPC, while blocking all other unauthorized inbound and outbound traffic.



# Everyone should be in a job they love.

Check out nextwork.org for more projects