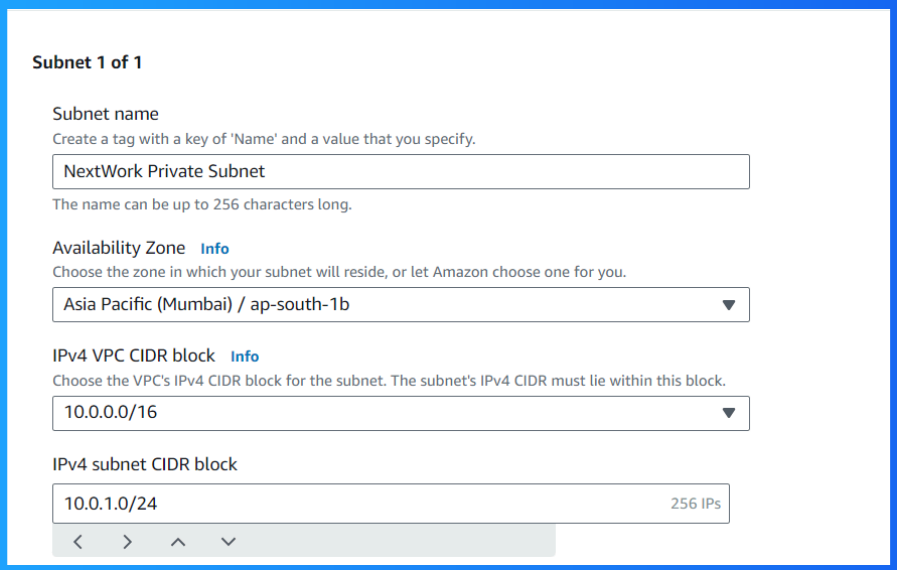
NextWork.org

Creating a Private Subnet

SH shravanirg03@gmail.com



SH
shravanirg03@gmail.com
NextWork Student
NextWork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC allows you to create an isolated, secure network in the AWS cloud, giving you control over IP ranges, subnets, etc. It is useful as it enhances security, and lets you scale resources while ensuring privacy and flexibility.

How I used Amazon VPC in this project

I set up public and private subnets in Amazon VPC. I created a private subnet with a dedicated route table and private network ACL. I also configured a public subnet with an Internet Gateway and necessary settings to manage traffic & ensure security.

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

This project provided valuable insights and deeper understanding of various networking concepts.

This project took me...

The entire process took me approximately 60 minutes.

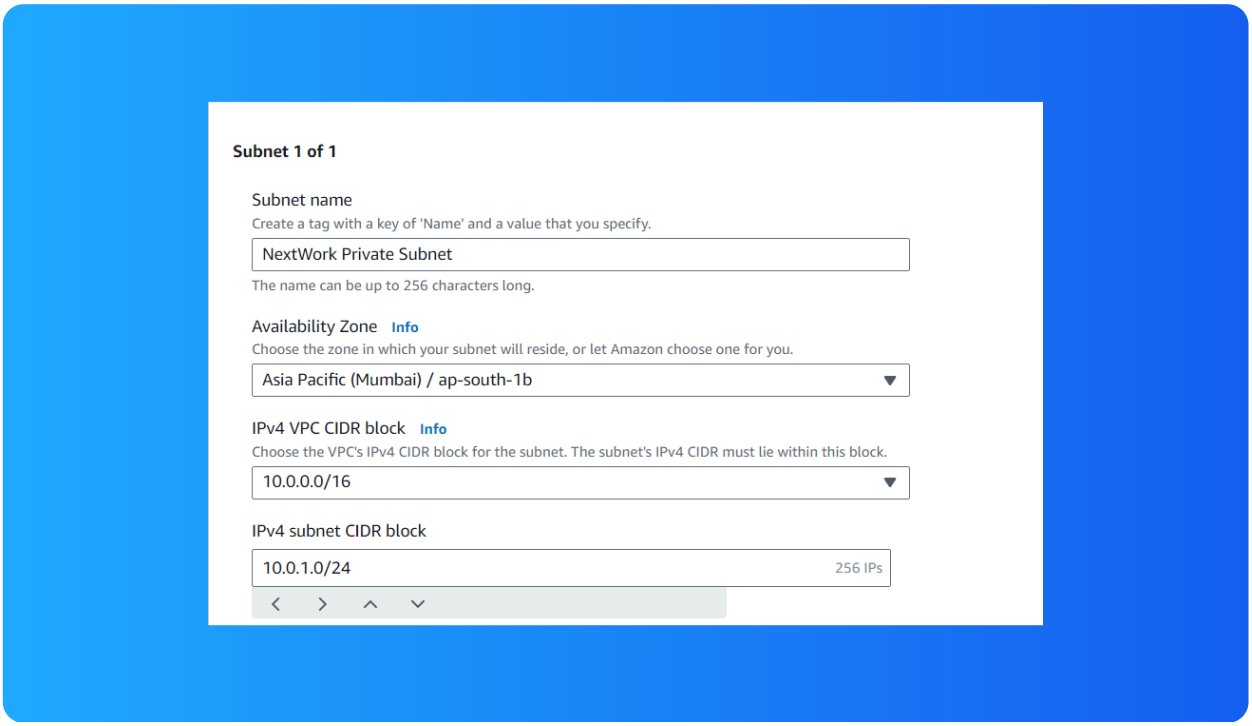
SH
shravanirg03@gmail.com
NextWork Student

Private vs Public Subnets

The difference between public and private subnets is that public subnets are accessible by and can access the internet, while private subnets are completely isolated from the internet by default.

Having private subnets are useful because they protect sensitive resources (like databases) from direct internet exposure, ensuring enhanced security by limiting access to internal traffic.

My private and public subnets cannot have the same IPv4 CIDR block i.e. the same range of IP addresses. The CIDR block for every subnet must be unique and cannot overlap with another subnet.



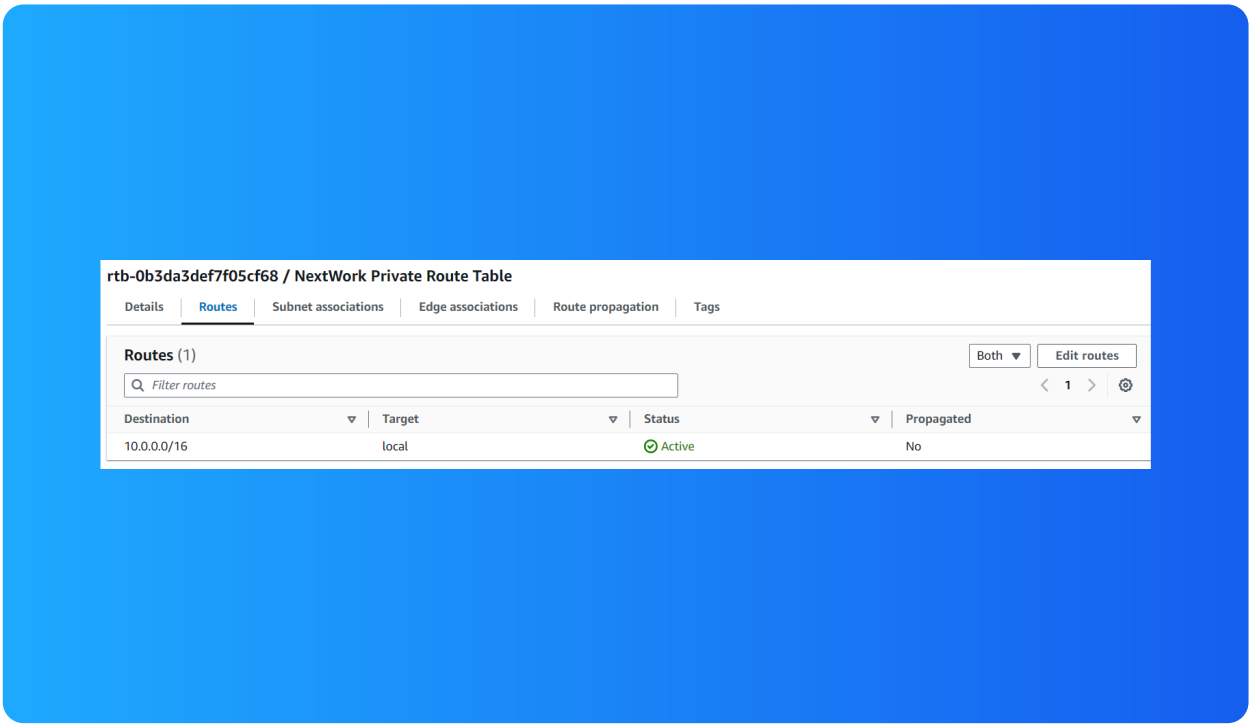
SH
shravanirg03@gmail.com
NextWork Student

A dedicated route table

By default, my private subnet is associated with the default route table i.e. a route table that has a route to an internet gateway.

I had to set up a new route table because my subnet cannot have a route to an internet gateway. Thus, I created a custom routing configuration for the private subnet.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows internal communication i.e. with a destination of another resource within my VPC.

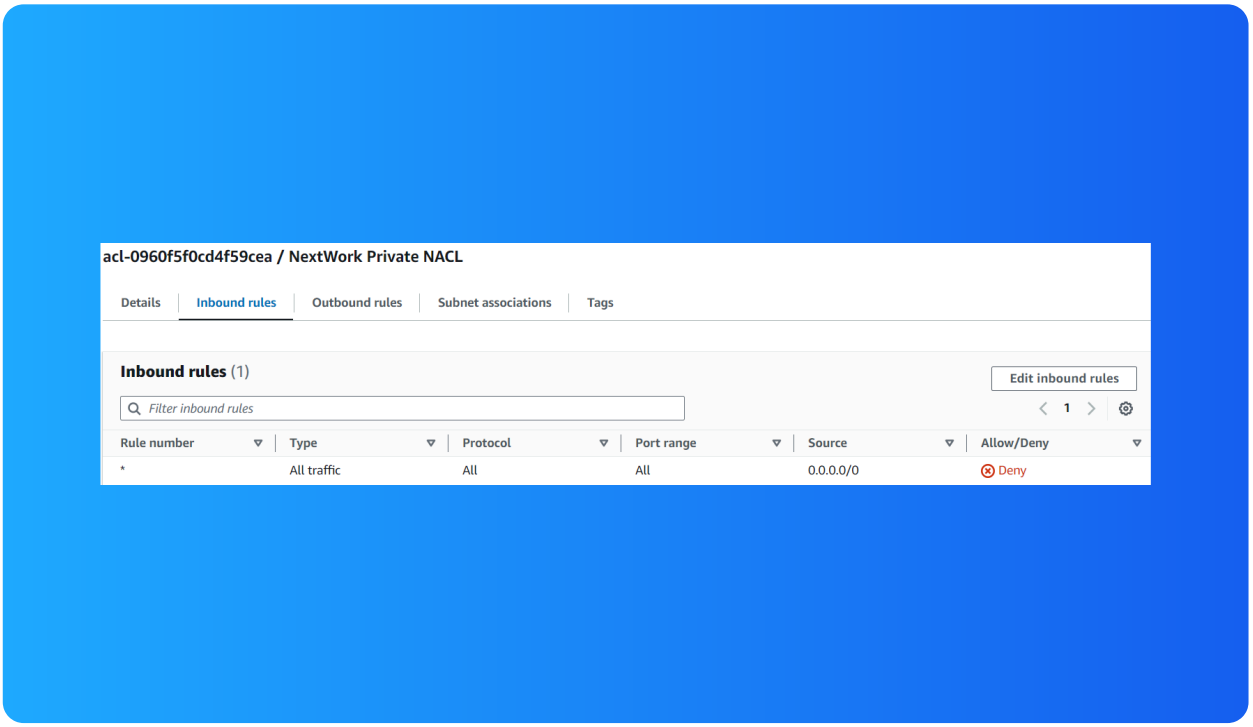


A new network ACL

By default, my private subnet is associated with the default network ACL that's set up for every VPC created in my AWS account.

I set up a dedicated network ACL for my private subnet because a network ACL becomes crucial in an event of security breach where traffic that has compromised a public subnet can get access to a private subnet if network ACL rules allow all traffic.

My new network ACL has two simple rules - deny all inbound and deny all outbound traffic.



Everyone should be in a job they love.

Check out nextwork.org for more projects