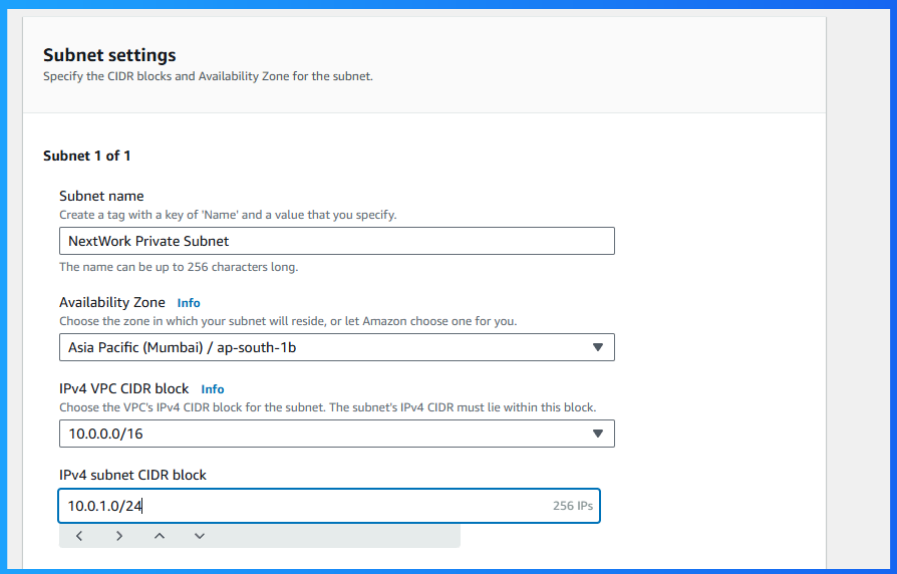
NextWork.org

Creating a Private Subnet

Saish Nar



Saish Nar
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) allows users to create a private and isolated network in their AWS account. They can manage and organize resources as well as configure permissions and access to those resources.

How I used Amazon VPC in this project

In this project I used my NextWork VPC to create a private subnet in another Availability Zone and associated it to a new route table I made. I also created a new network ACL to set access restrictions for my private subnet.

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

I wasn't expecting how simple it would be to associate and disassociate a subnet from a route table to another one.

This project took me...

This project took me about an hour to complete.

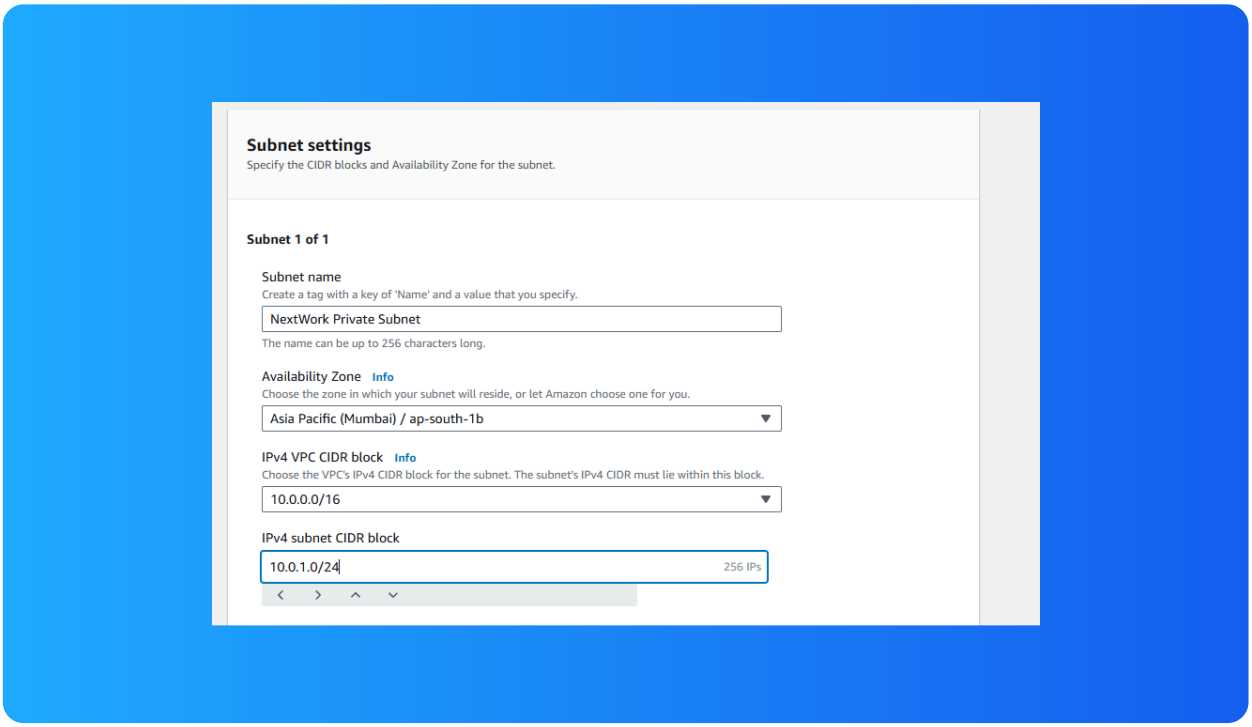
Saish Nar
NextWork Student

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 keeping resources away from the internet is extremely important for the security of confidential resources/data.

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.



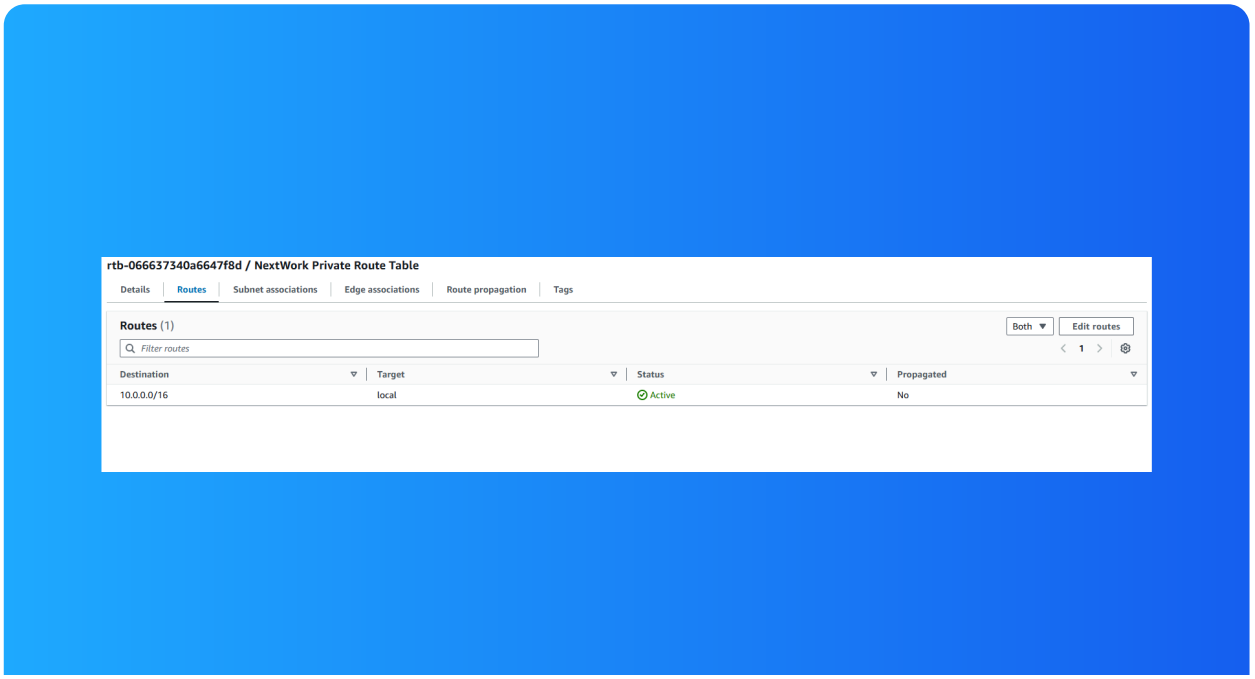
Saish Nar
NextWork Student

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 other route table is public and I want to keep some resources and subnets private in my AWS environment. This new route table I created is private, therefore when I attach my subnet it would be private.

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.



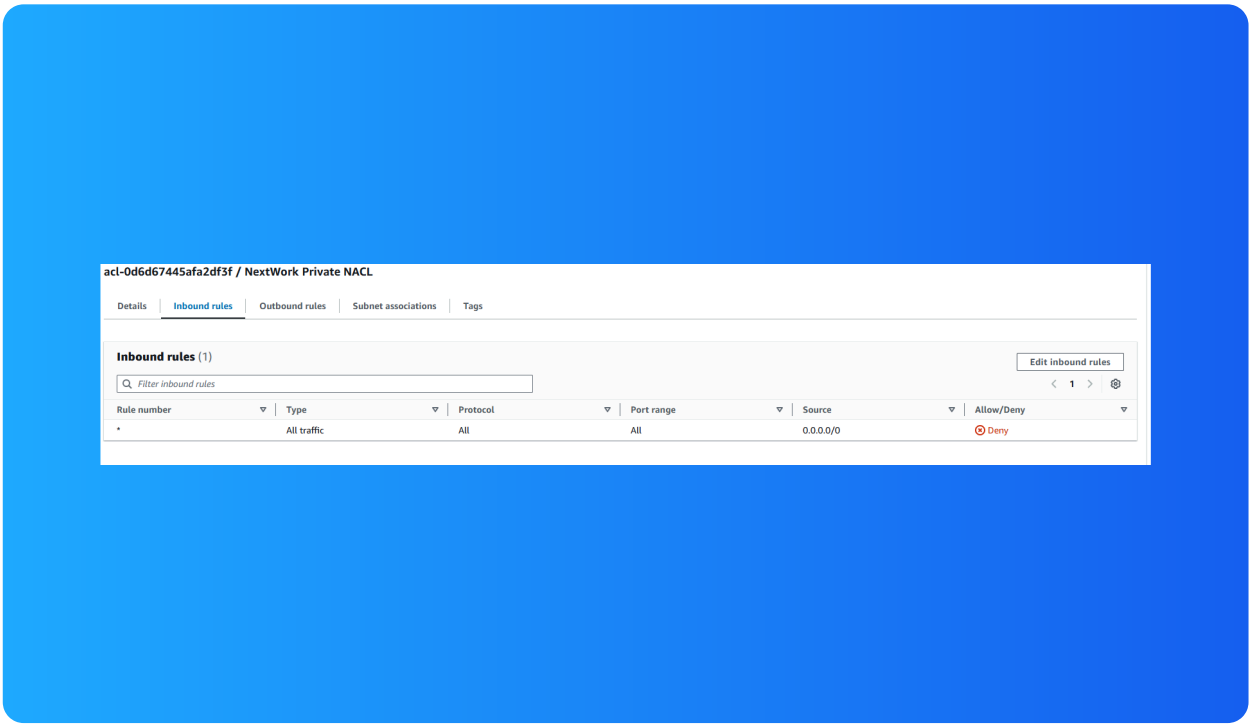
Saish Nar
NextWork Student

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 I want to set strict access controls; these access controls will protect my resources from being accessed from external users and to prevent traffic from leaving my private subnet.

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