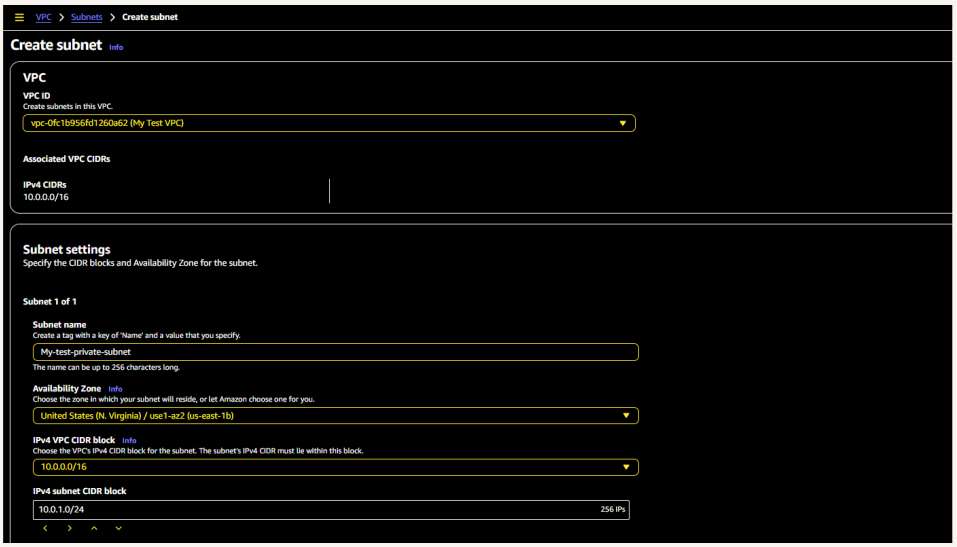
Creating a Private Subnet

Michael K.



Michael K.
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is a logically isolated virtual network withinAWS where i can launch and manage AWS resources (such as EC2 instances,RDS databases, and load balancers) using my own defined IP address range,subnets, route tables, and network gateways.

How I used Amazon VPC in this project

In today's project, I used my already created Amazon VPC and configured a more secure traffic within it, adding a private Neighborhood (subnet) for resources that are meant to be inaccessible from the internet.

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

One thing I didn't expect in this project is to have some deep understanding on the difference between a public and a private subnet.

Michael K.
NextWork Student

This project took me...

This project took me 30mins.

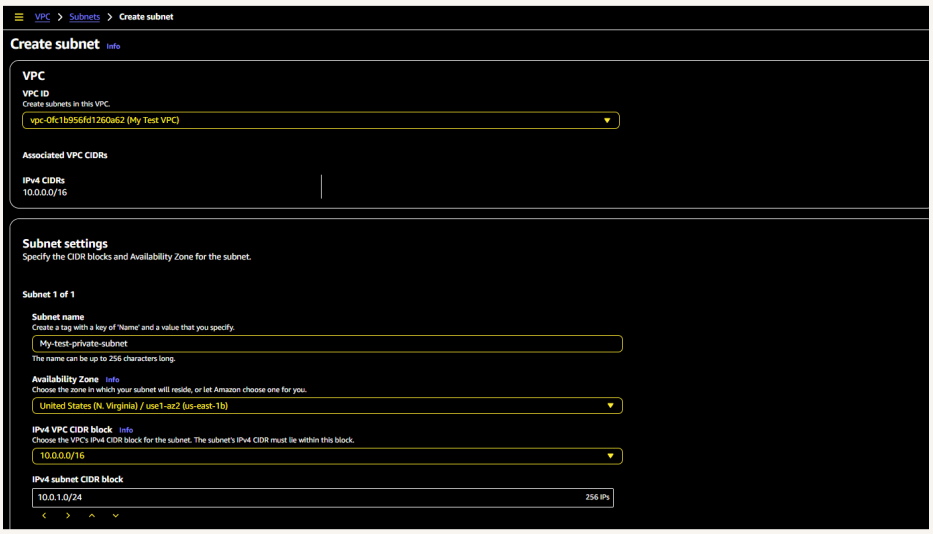
Michael K.
NextWork Student

Private vs Public Subnets

One of the difference between public and private subnets is in their CIDR Block range. Even though they might have the same number of available IP Adresse (because of the same number of changeable bits), their static bits will differ.

Having private subnets are useful because i can host resources which are meant to be private and not accessible from the internet there.

My private and public subnets cannot have the same CIDR Block range number.



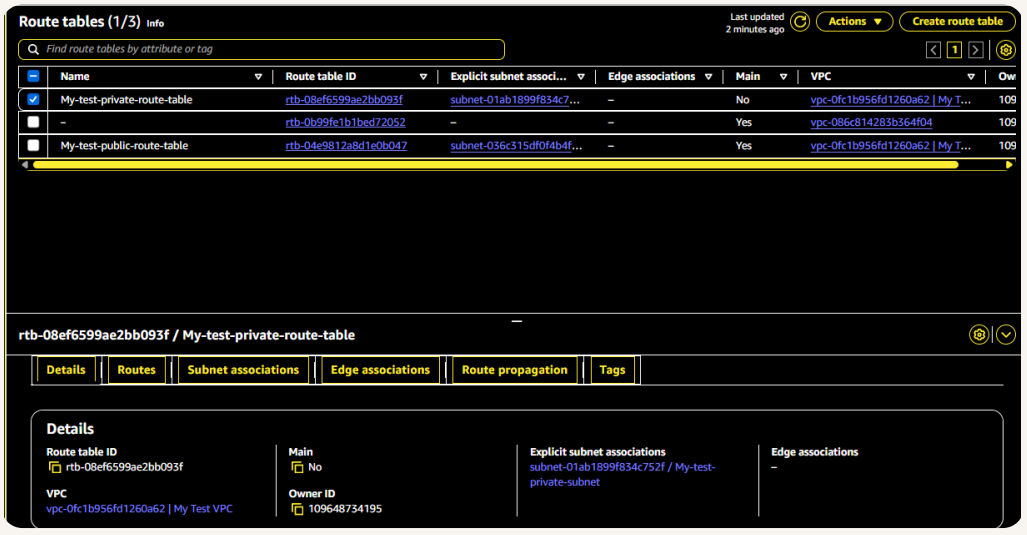
Michael K.
NextWork Student

A dedicated route table

By default, my private subnet is associated with with the public route table that AWS created as i created my VPC.

I had to set up a new route table because that public route table linked to my private subnet contains a route to an Internet gateway which would make my private subnet public if ever attached to it.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows traffic within the VPC.



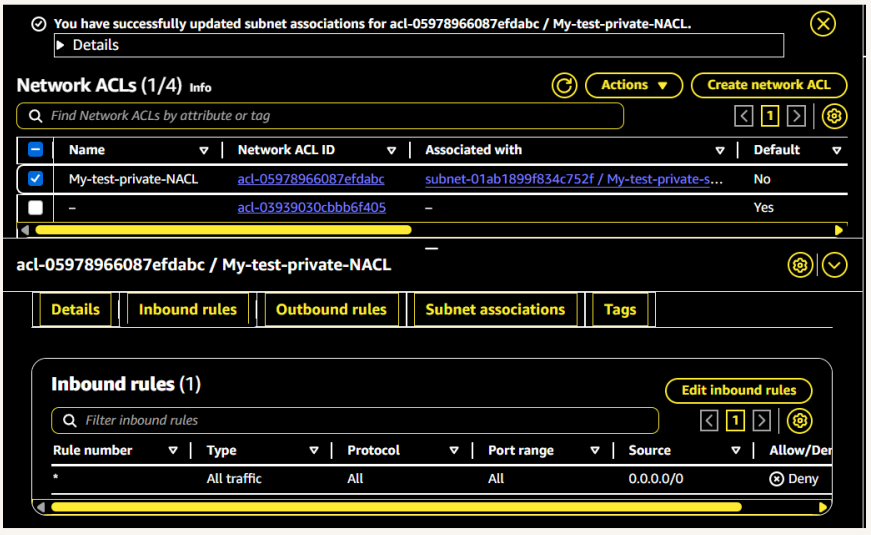
Michael K.
NextWork Student

A new network ACL

By default, my private subnet is associated with the public Network ACL created by AWS when my VPC was created.

I set up a dedicated network ACL for my private subnet because if i leave it attached to that public Network ACL and it later get compromised, an attacker can use its vulnerability to access resources in my private subnet.

My new network ACL has two simple rules - Deny all inbound and outbound traffic for NOW.



The place to learn & showcase your skills

Check out nextwork.org for more projects