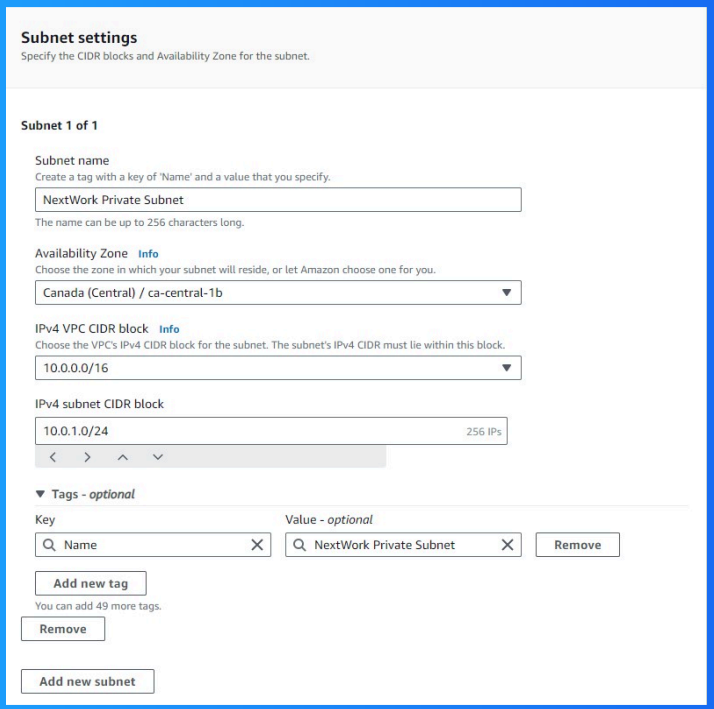
NextWork.org

Creating a Private Subnet

Nikhil Bhan



N

Nikhil Bhan
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. I used another 15 minutes to write my documentation.

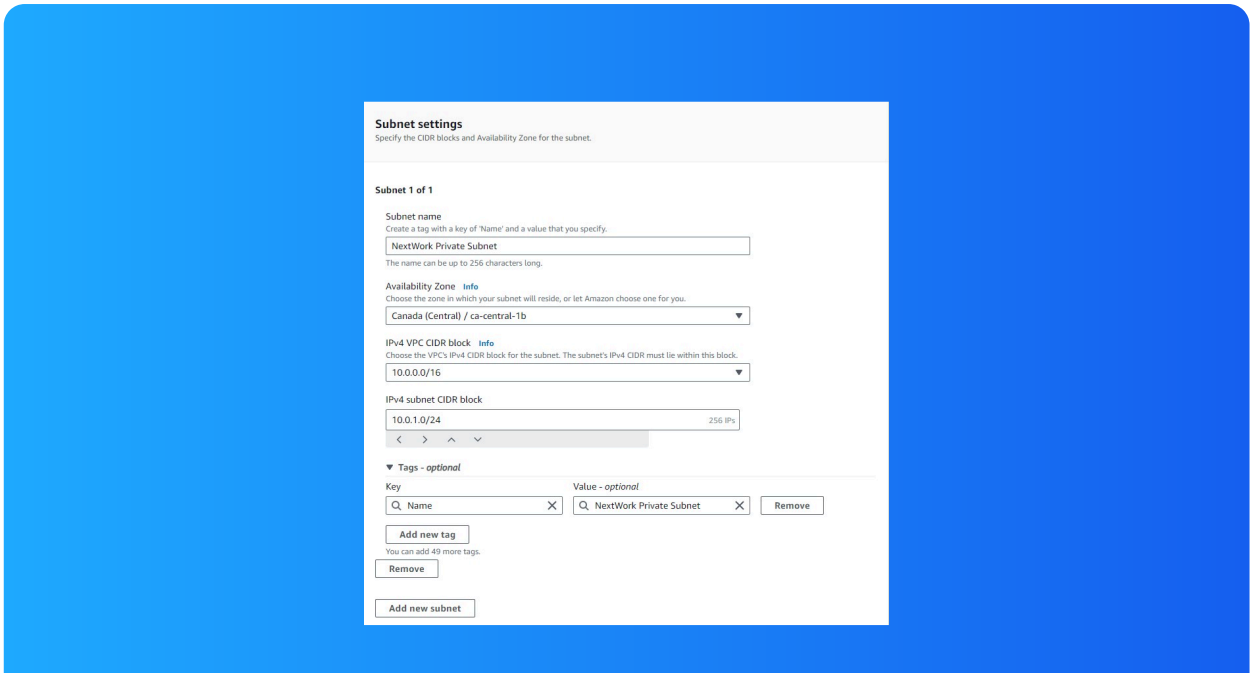
Nikhil Bhan
NextWork Student

Private vs Public Subnets

The difference between public and private subnets is that the public subnet is able to receive traffic from the Internet and send traffic out the network. The private subnet is not able to send or receive traffic as it's an isolated network.

Having private subnets are useful because the user's resources are protected and secured against any access outside of the subnet. Private subnets are useful if the user wants to secure sensitive information like databases containing credentials.

My private and public subnets cannot have the same IPv4 Subnet CIDR Block; this means that the range of IP addresses assigned to the public and private subnet have to be unique so it eliminates the issue of duplicate IP addresses.



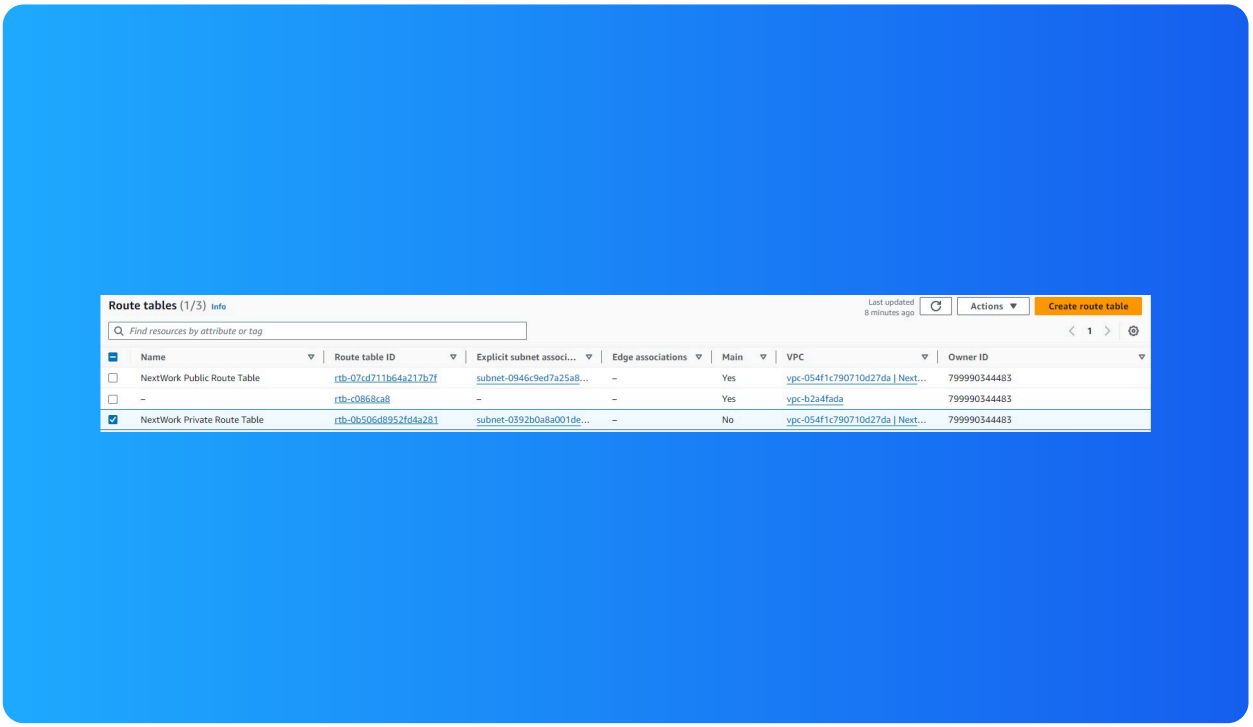
Nikhil Bhan
NextWork Student

A dedicated route table

By default, my private subnet is associated with my public route table.

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 route. This route shows that traffic in the private subnet can reach any resources in that subnet that have an IP address that's within the IP address range, which is 10.0.0.0/16.



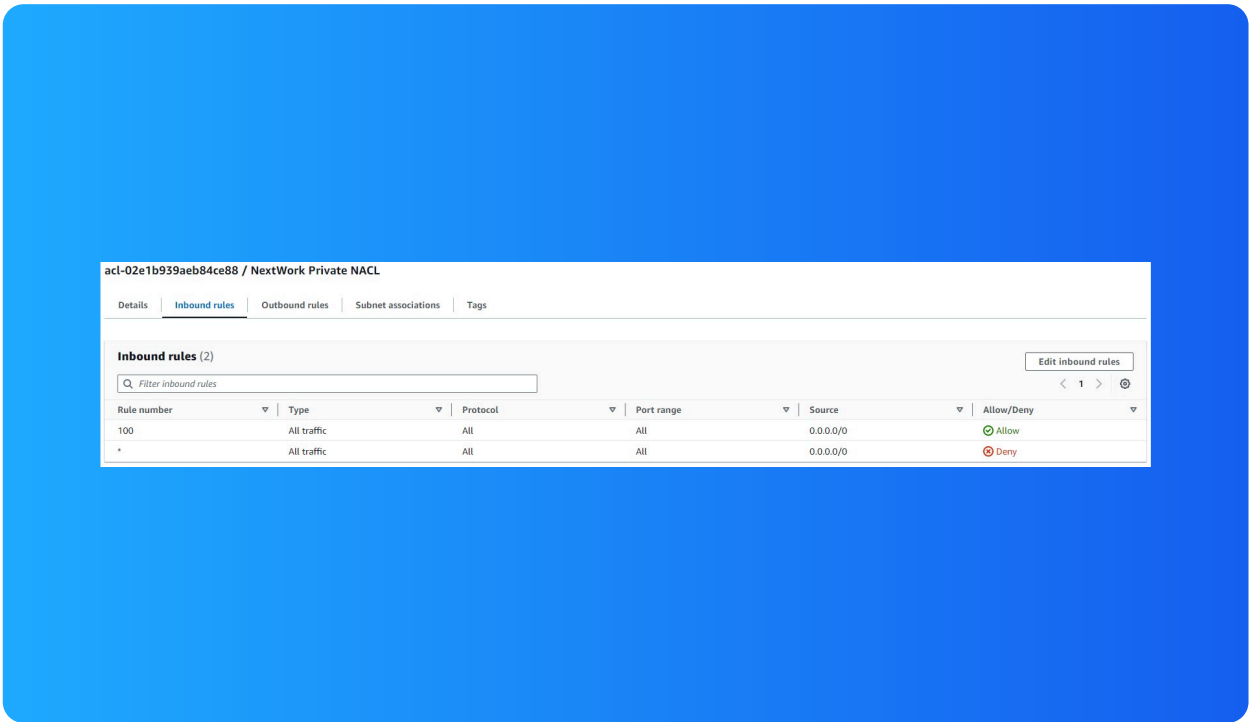
Nikhil Bhan
NextWork Student

A new network ACL

By default, my private subnet is associated with the default Network ACL in my VPC. It remains this way until I make an explicit association between that private subnet and another Network ACL.

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: Inbound: Deny all traffic that come from any IP addresses Outbound: Deny all traffic going to any IP addresses



Everyone should be in a job they love.

Check out nextwork.org for more projects