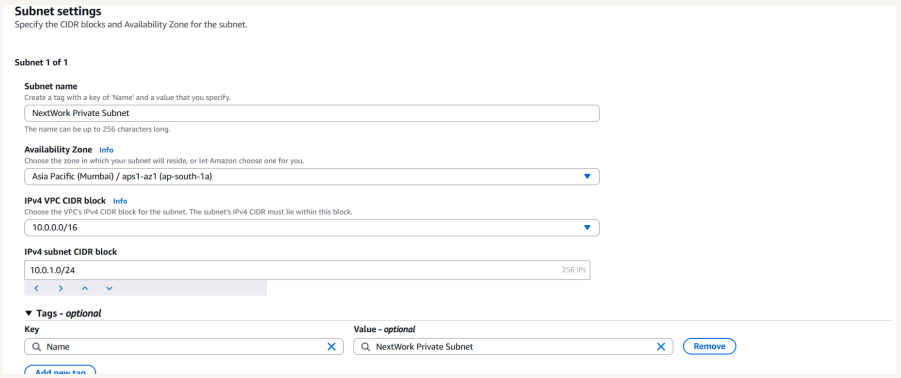
nextwork.org

Creating a Private Subnet

mohammed Furqanuddin



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is a secure, isolated network in AWS where you launch and manage your resources. It’s useful because it gives full control over networking, security, and internet access for your applications.

How I used Amazon VPC in this project

In today’s project, I used Amazon VPC to create a custom network where I set up public and private subnets, route tables, and a network ACL to securely manage resources and control their internet access.

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

One thing I didn’t expect in this project was the need to create a separate route table and network ACL for the private subnet to keep it fully isolated from the internet.

This project took me...

This project took me around 1 hour to complete, including setting up the VPC, creating public and private subnets, configuring route tables, and setting up the network ACL.

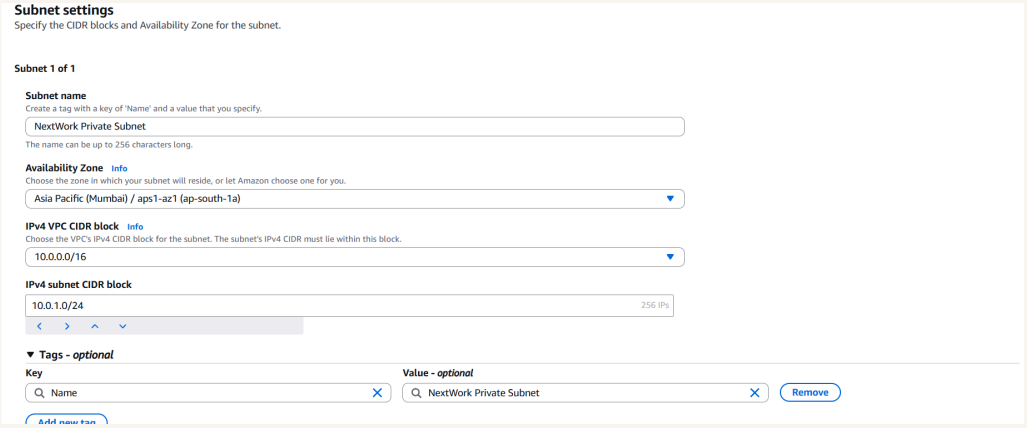
mohammed Furqanuddin
NextWork Student

Private vs Public Subnets

A public subnet is connected to the internet through an Internet Gateway, so its resources (like web servers) can be accessed publicly. A private subnet has no direct internet access, so its resources stay isolated and secure within the VPC.

Private subnets exist to keep sensitive resources (like databases) hidden from the internet, making them safer and more secure.

Your private and public subnets can’t share the same route table they each need their own, since public subnets connect to the internet while private subnets stay isolated.

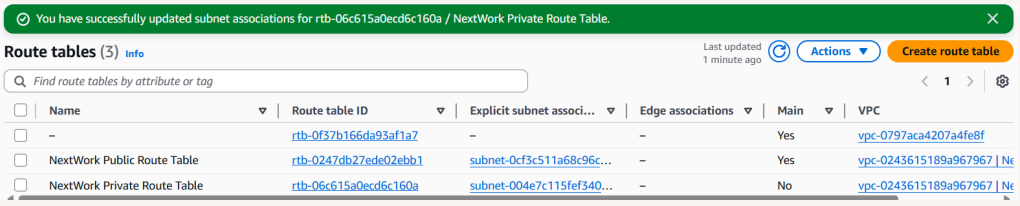


A dedicated route table

By default, Our private subnet is associated with the main (default) route table of the VPC in this case, the NextWork route table we renamed earlier.

We're setting up a new route table so our private subnet stays private.

Our private subnet's dedicated route table only has one local route that allows traffic within the VPC,It does not have a route to the Internet Gateway,so resources inside the private subnet can only talk to other resorces in the VPC,not the internet

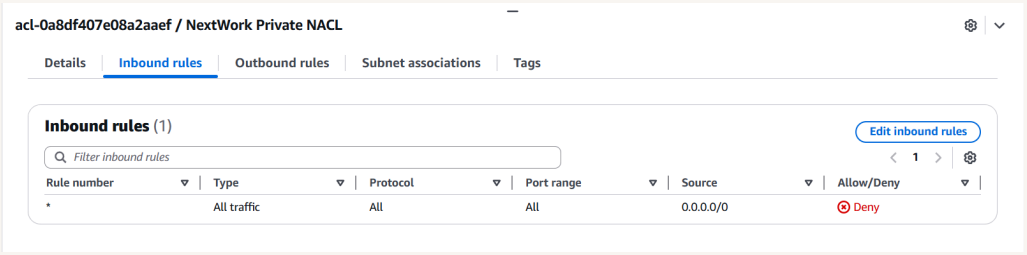


A new network ACL

By default, our private subnet is associated with the default network ACL that AWS automatically creates with our VPC.

I set up a dedicated network ACL for my private subnet because I need tighter security rules at the subnet level, ensuring sensitive resources (like databases) are protected from unwanted traffic.

My new network ACL has one inbound and one outbound rule that deny all traffic (all protocols, all ports) from anywhere (0.0.0.0/0).



The place to learn & showcase your skills

Check out nextwork.org for more projects