nextwork.org

Creating a Private Subnet

L Louis Moyo

L
Louis Moyo
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a virtual private cloud that lets you isolate and control network resources in AWS. It's useful for customising security, IP ranges, and routing to fit your project needs.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create a private subnet for internal resources, ensuring they are isolated from the internet for security.

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

One thing I didn't expect was that the private subnet automatically linked to the main route table, requiring a separate one for full isolation.

This project took me...

This project took me about 45minutes, including creating the subnet, checking settings, and verifying its association with the correct route table.

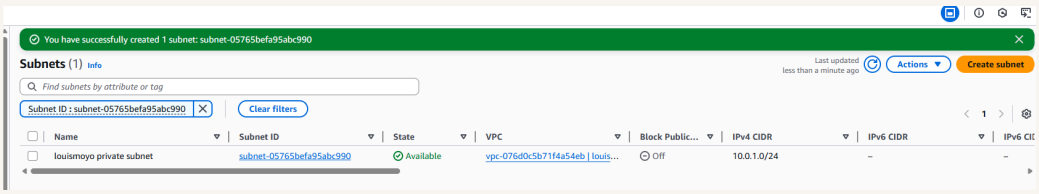
Louis Moyo
NextWork Student

Private vs Public Subnets

The difference between public and private subnets is that public subnets have a route to the internet via an internet gateway, while private subnets do not.

Having private subnets is useful because they isolate resources from direct internet access, improving security by reducing exposure to external threats.

My private and public subnets cannot have the same CIDR block within the same VPC, as each subnet must have a unique range of IP addresses.

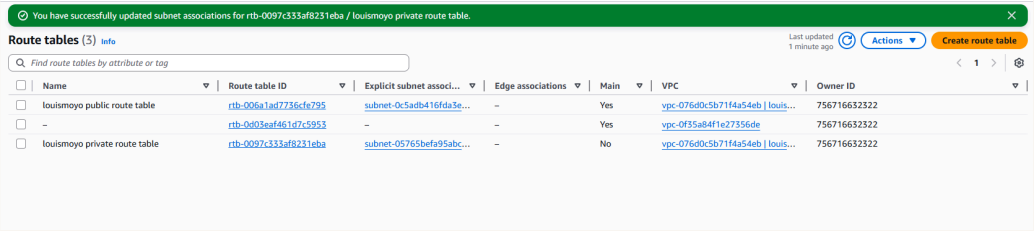


A dedicated route table

By default, my private subnet is associated with the main route table of the VPC, which handles routing until a custom route table is assigned.

I set up a new route table to isolate the private subnet's traffic, ensuring it routes internally without direct internet access for added security.

My private subnet's route table allows only internal VPC traffic via the local route, preventing any direct outbound internet connectivity.

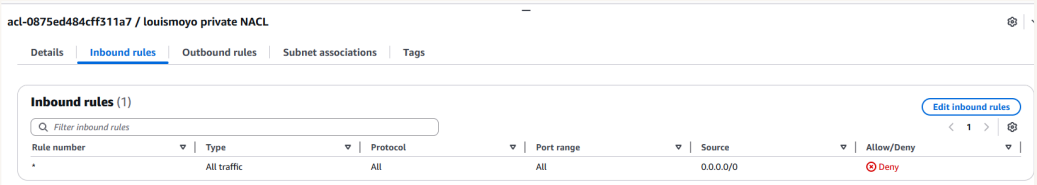


A new network ACL

By default, my private subnet is associated with the VPC's default NACL, which allows all inbound and outbound traffic unless explicitly modified.

I set up a dedicated network ACL for my private subnet to enforce stricter traffic control, separating it from the default NACL to better secure sensitive resources.

My new network ACL has two rules: inbound denies all traffic from any source (0.0.0.0/0) and outbound denies all traffic to any destination (0.0.0.0/0).



The place to learn & showcase your skills

Check out nextwork.org for more projects