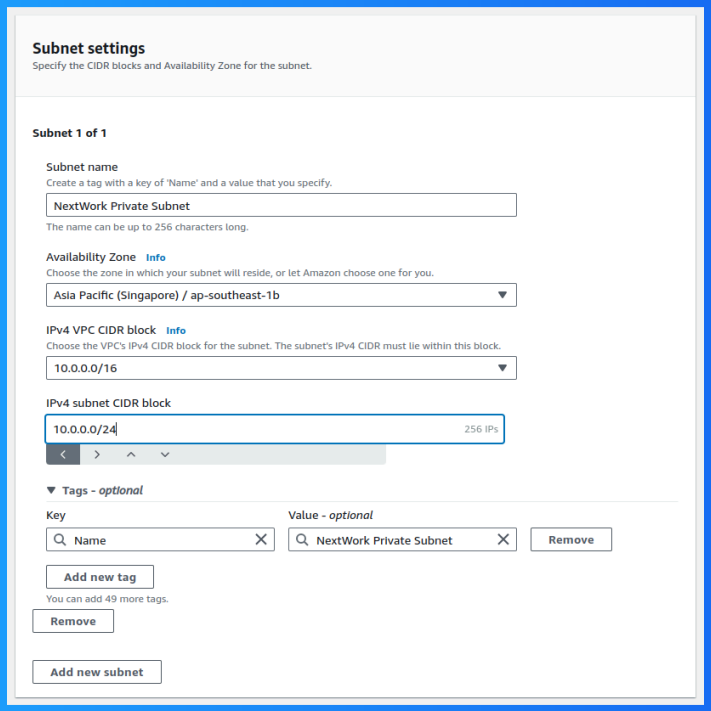
NextWork.org

Creating a Private Subnet

Emmanuel Enalpe III



Emmanuel Enalpe III
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC allows you to create a private, isolated network within AWS. It lets you control network resources, IP address ranges, and security, offering better control over traffic and enhancing security for your cloud resources.

How I used Amazon VPC in this project

I used Amazon VPC to create a secure network environment, defining subnets, route tables, and internet gateways for proper traffic flow. This ensured secure communication between instances while isolating them from the public internet.

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

One thing I didn’t expect in the VPC project was how crucial the proper configuration of route tables and security groups is for traffic flow. It’s easy to overlook these details, but they play a vital role in ensuring the network works smoothly.

This project took me...

It took me less than an hour to complete this AWS service project.

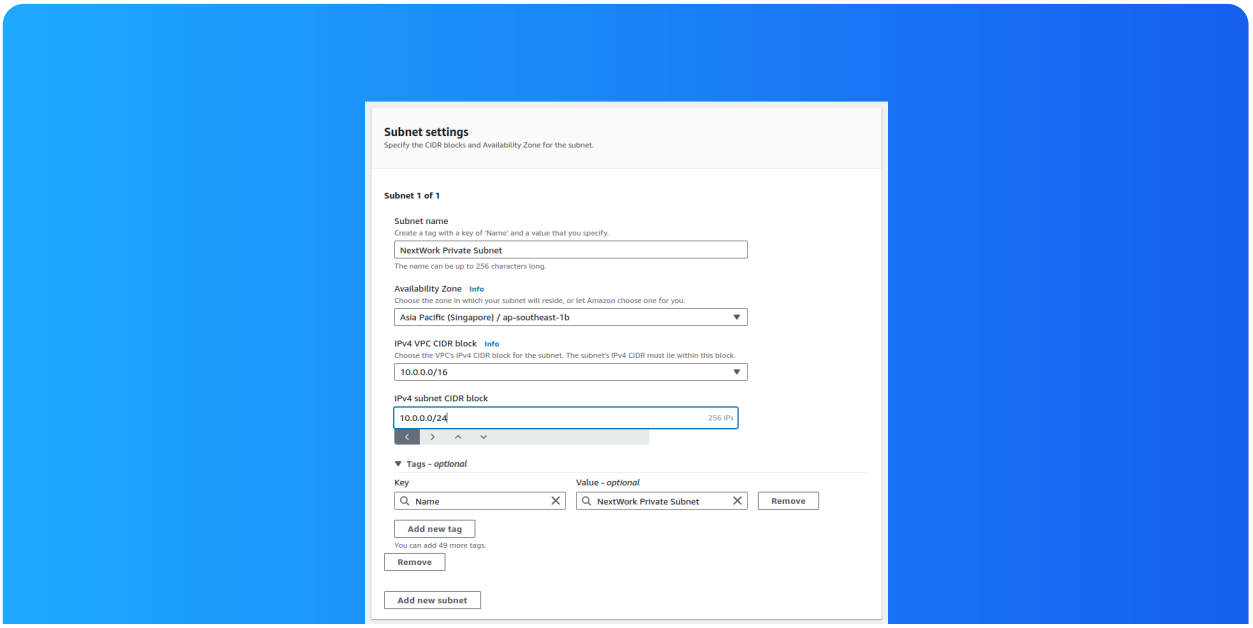
Emmanuel Enalpe III
NextWork Student

Private vs Public Subnets

The difference between public and private subnets is that public subnets have access to the internet via an Internet Gateway, while private subnets are isolated from direct internet access, often using a NAT Gateway for outbound traffic.

Having private subnets are useful because they enhance security by isolating resources from the internet, allowing only internal communication or controlled access via NAT gateways, VPNs, or bastion hosts, thus protecting sensitive data and systems.

My private and public subnets cannot have the same route table configurations, as public subnets require a route to an internet gateway, while private subnets route traffic through a NAT gateway or NAT instance for internet access.



Emmanuel Enalpe III
NextWork Student

A dedicated route table

By default, my private subnet is associated with the main route table of the VPC, which does not have a route to an internet gateway, ensuring it remains private.

I had to set up a new route table because I needed to customize the traffic flow for specific subnets in my VPC, ensuring proper routing for internet access, private connections, or specific peering arrangements.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows local traffic within the VPC. It does not route traffic to the internet or other external networks unless connected to a NAT gateway.

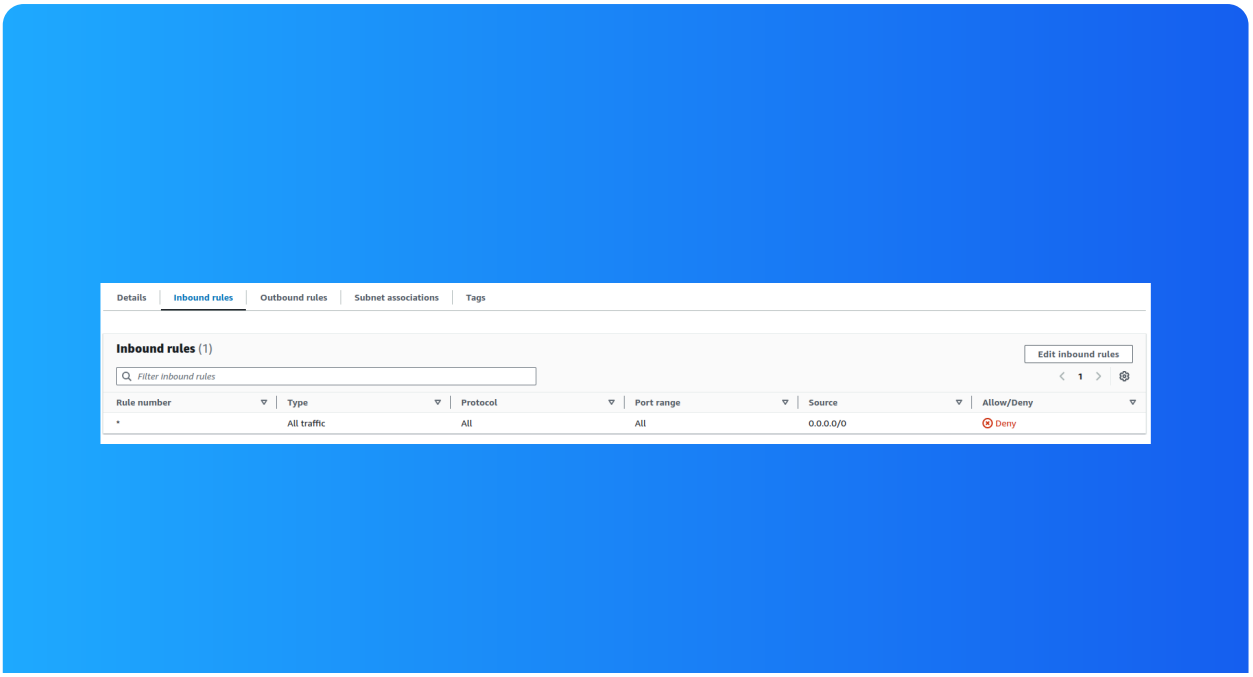
Emmanuel Enalpe III
NextWork Student

A new network ACL

By default, my private subnet is associated with the default Network ACL (NACL) for the VPC, which allows all inbound and outbound traffic unless explicitly modified.

I set up a dedicated network ACL for my private subnet because it provides granular control over inbound and outbound traffic, enhances security by isolating the subnet, and ensures compliance with specific access and filtering requirements.

My new network ACL has two simple rules – one inbound rule denying all traffic and one outbound rule denying all traffic. These rules effectively block both incoming and outgoing communication for enhanced security.



Everyone should be in a job they love.

Check out nextwork.org for more projects