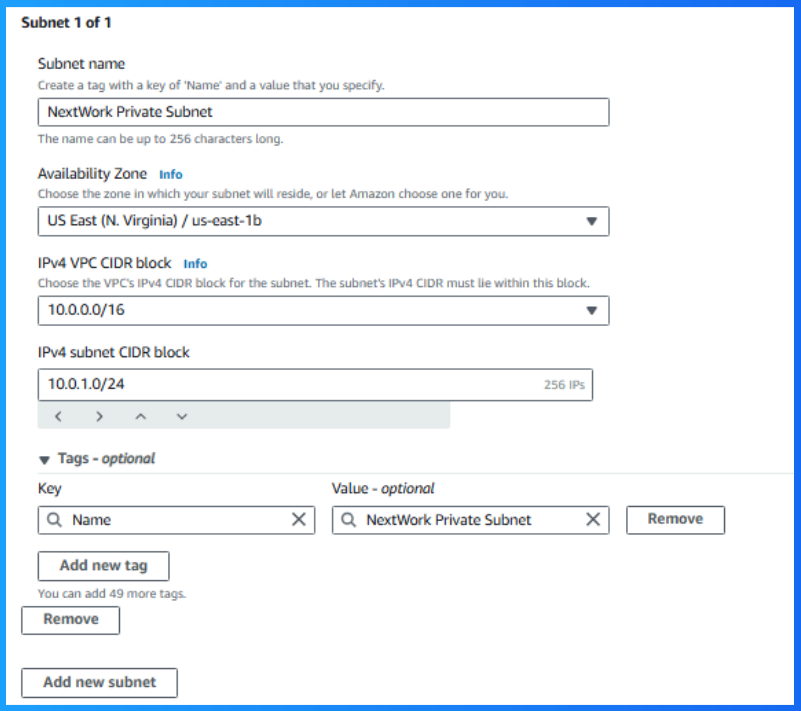
NextWork.org

Creating a Private Subnet

Gloria



G
Gloria
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is a secure, isolated network in AWS where you can launch resources like EC2 instances. It’s useful because it gives control over networking, such as IP ranges, subnets and security.

How I used Amazon VPC in this project

I used Amazon VPC in today's project to create a secure and isolated network, set up private and public subnets, configured route tables for traffic control, and implemented custom network ACLs to enhance security and manage traffic flow.

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

One thing I didn't expect in this project is how critical security is at every level. Configuring subnets, route tables, and network ACLs made me realize the importance of carefully managing traffic to ensure the environment remains secure.

This project took me...

This project took me 20 minutes to complete. With prior setups from earlier projects, the process was smooth and beginner-friendly, highlighting the importance of security configurations at every step.

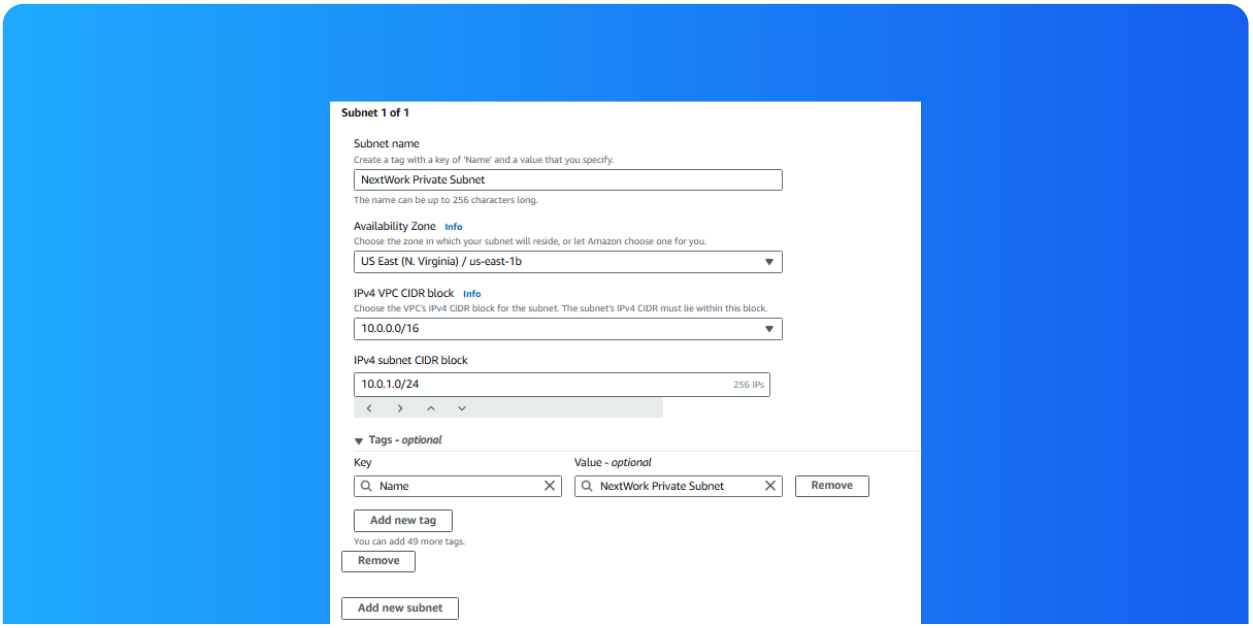
Gloria
NextWork Student

Private vs Public Subnets

The difference between public and private subnets is that a public subnet has a route to the internet through an internet gateway, allowing external access, while a private subnet does not, keeping its resources isolated and accessible only within.

Having private subnets are useful because they enhance security by isolating sensitive resources, like databases or application servers, from direct internet access. This reduces exposure to external threats while allowing controlled communication.

My private and public subnets cannot have the same CIDR block, as each subnet in a VPC must have a unique range of IP addresses to ensure proper routing and avoid conflicts within the network.



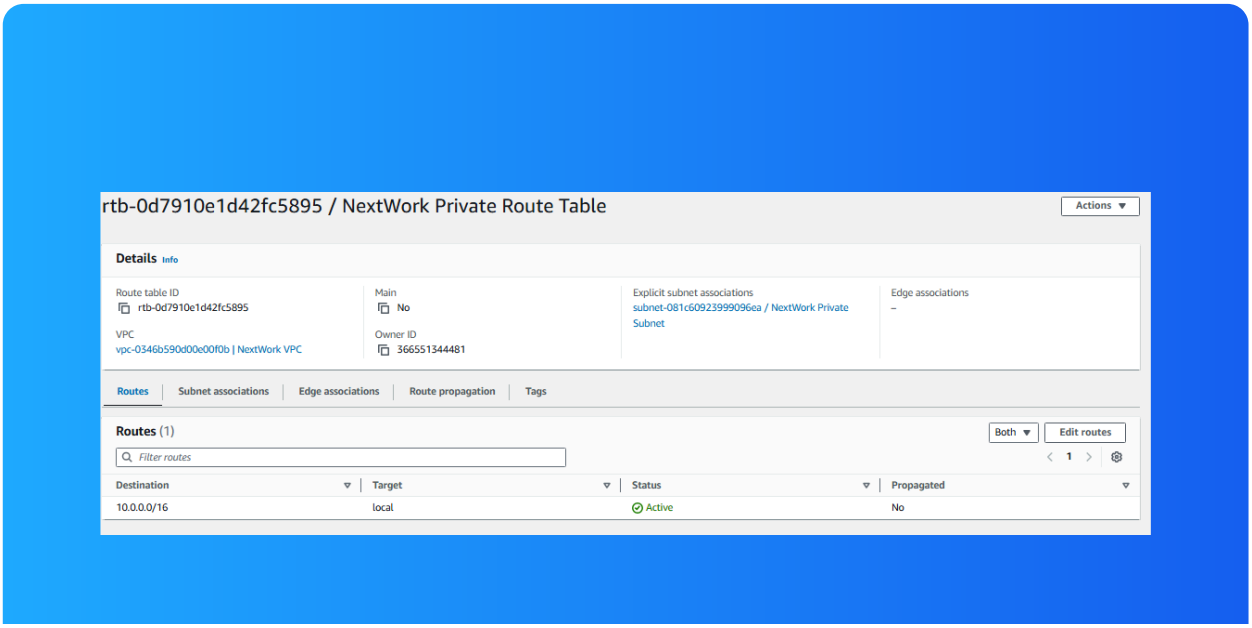
Gloria
NextWork Student

A dedicated route table

By default, my private subnet is associated with the main route table of the VPC, which the public subnet is already associated with. This setup could expose the private subnet to public internet routes, making it necessary to create a new one.

I had to set up a new route table because my private subnet needs routing rules specific to internal communication, like directing traffic to a NAT gateway, while avoiding public internet access routes to maintain security and isolation

My private subnet's dedicated route table only has one inbound and one outbound rule that allows local traffic within the VPC, ensuring secure communication between internal resources while blocking direct access to and from the internet.

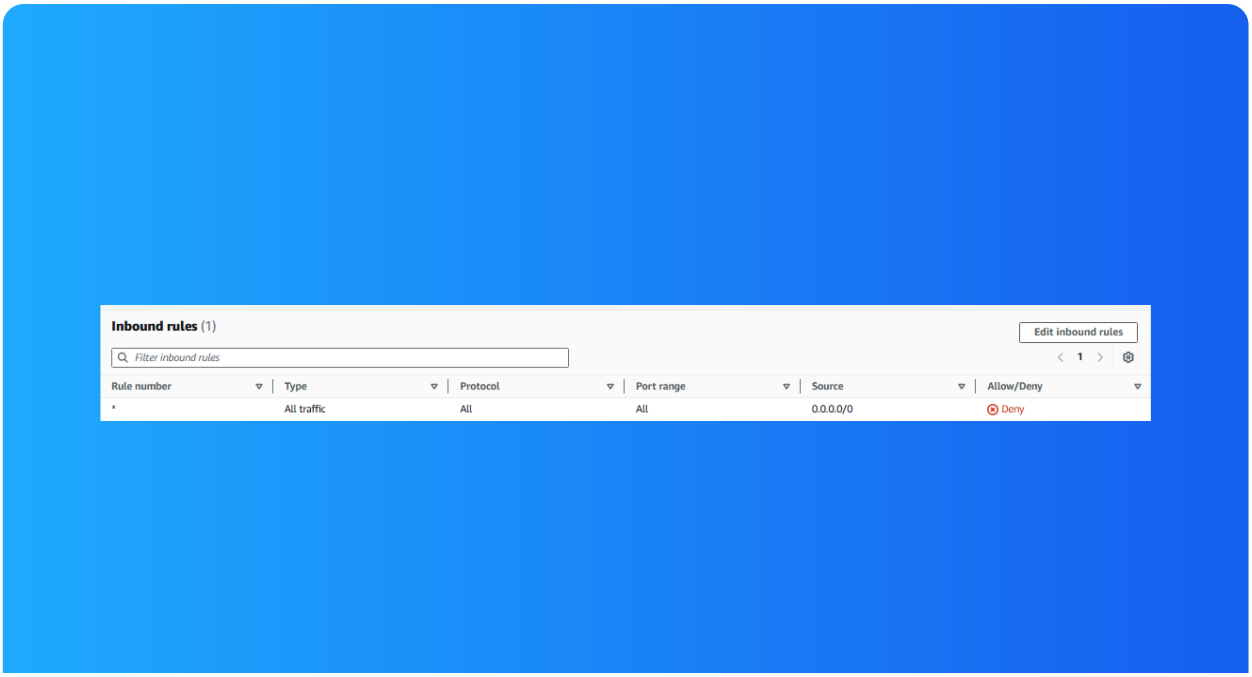


A new network ACL

By default, my private subnet is associated with the default network ACL provided by AWS, which allows all inbound and outbound traffic unless specific deny rules are added.

I set up a dedicated network ACL for my private subnet because it allows me to define custom rules for controlling inbound and outbound traffic, enhancing security by restricting access and isolating the subnet from unwanted traffic.

My new network ACL has two simple rules - an inbound rule that denies all traffic (`0.0.0.0/0`) across all protocols and ports to block unauthorized access, and an outbound rule that also denies all traffic to prevent any data from leaving the subnet



Everyone should be in a job they love.

Check out nextwork.org for more projects