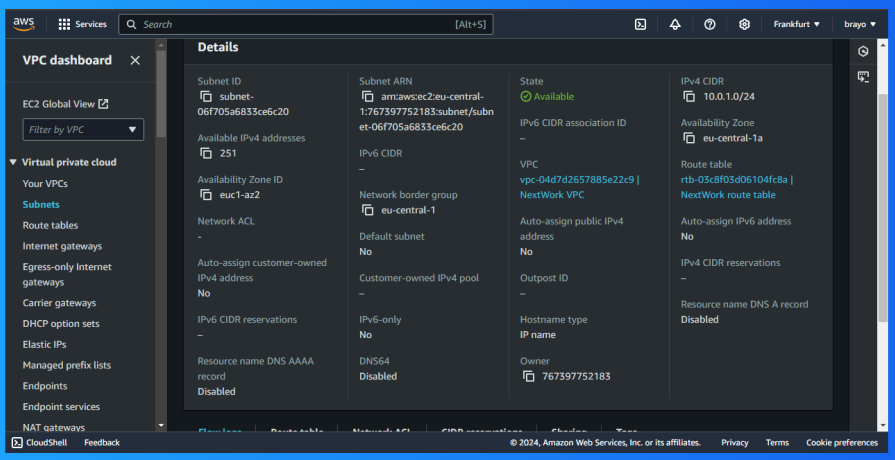
NextWork.org

Creating a Private Subnet

Brian Kimemia N



Brian Kimemia N
NextWork Student

NextWork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon Virtual Private Cloud enables users to create a logically isolated network in the AWS cloud, providing control over IP addressing, subnets, route tables, and security. It ensures secure, customizable network configurations for AWS resources.

How I used Amazon VPC in this project

I used Amazon VPC to design secure, isolated network environments for deploying AWS resources, configuring subnets, route tables, and security groups to control access and optimize data flow between instances and external services.

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

I didn’t expect the complexity of managing overlapping IP addresses across multiple VPCs, which required careful planning and adjustments to ensure seamless connectivity and avoid conflicts.

This project took me...

This project took approximately 1 hour , including planning, configuring the VPC, testing network settings, and troubleshooting connectivity issues.

Brian Kimemia N
NextWork Student

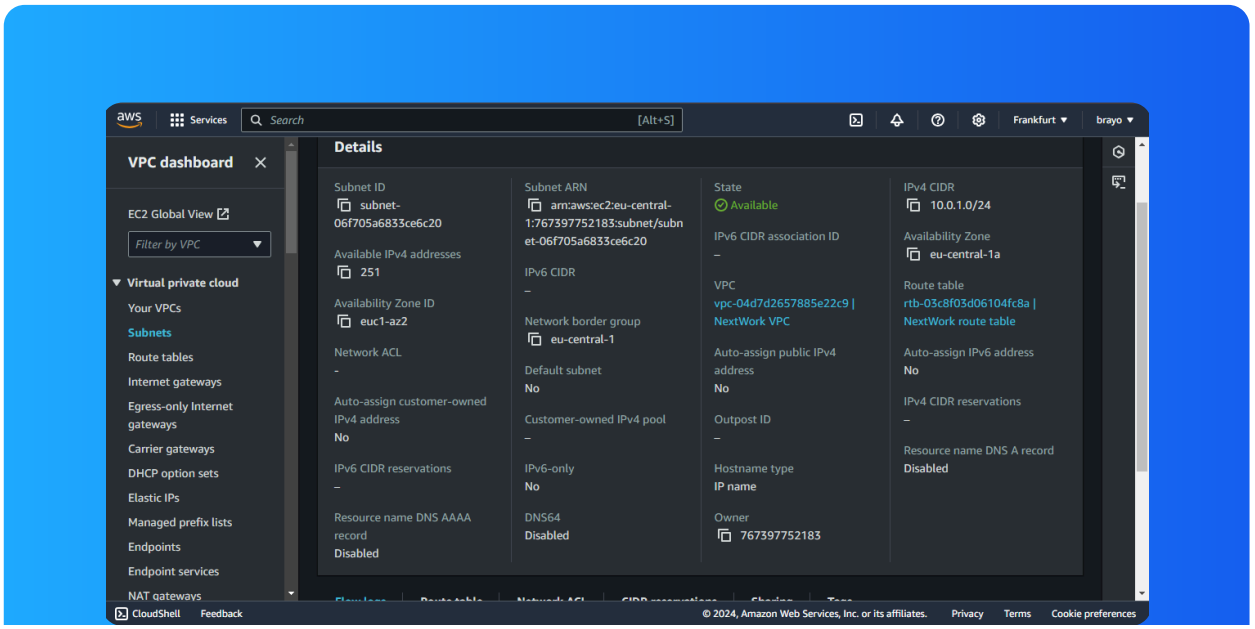
NextWork.org

Private vs Public Subnets

The difference between public and private subnets is that public subnets have routes to the internet through an internet gateway, allowing direct internet access, while private subnets do not, ensuring they remain isolated from external networks.

Having private subnets are useful because they provide enhanced security by isolating resources from direct internet access, making them ideal for sensitive workloads eg. databases and application servers that should not to be exposed to the internet

My private and public subnets cannot have the same route table or network ACL, as they require different configurations for managing internet access and security.



Brian Kimemia N
NextWork Student

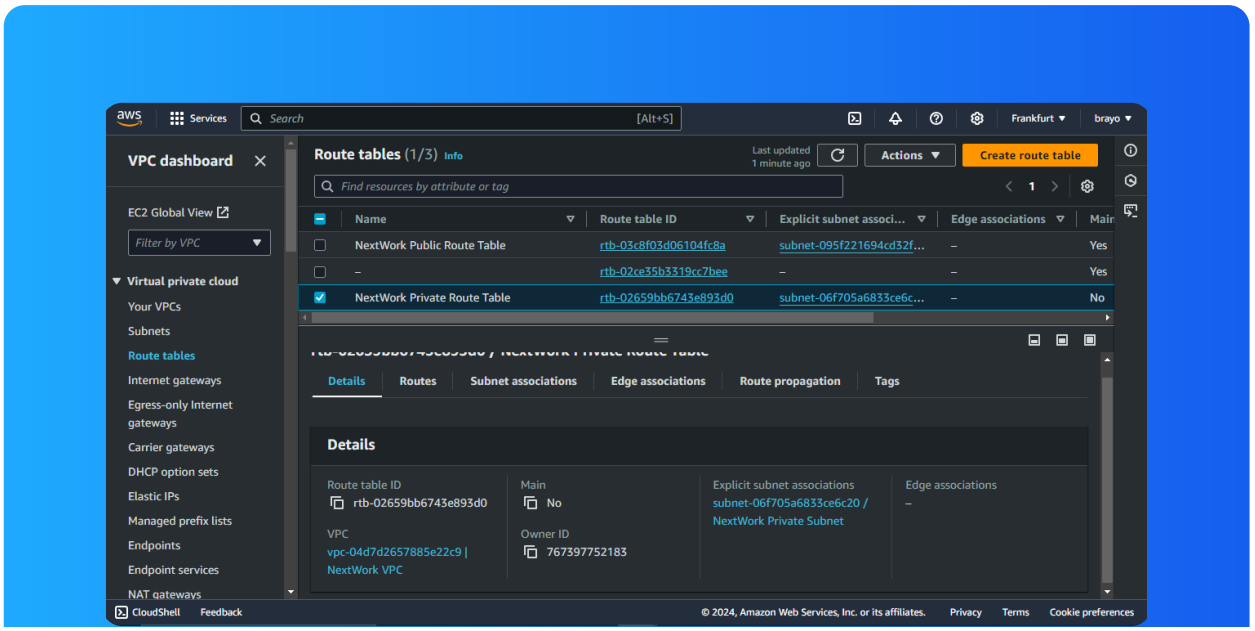
NextWork.org

A dedicated route table

By default, my private subnet is associated with the main route table of the VPC. This route table allows traffic based on the VPC's default routing settings, including the removal of the internet gateway route to prevent internet access.

I had to set up a new route table because the default route table allows traffic to flow unrestricted, including potentially allowing access to the internet,and I needed to ensure private subnet remains isolated from the internet for better security

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



Brian Kimemia N
NextWork Student

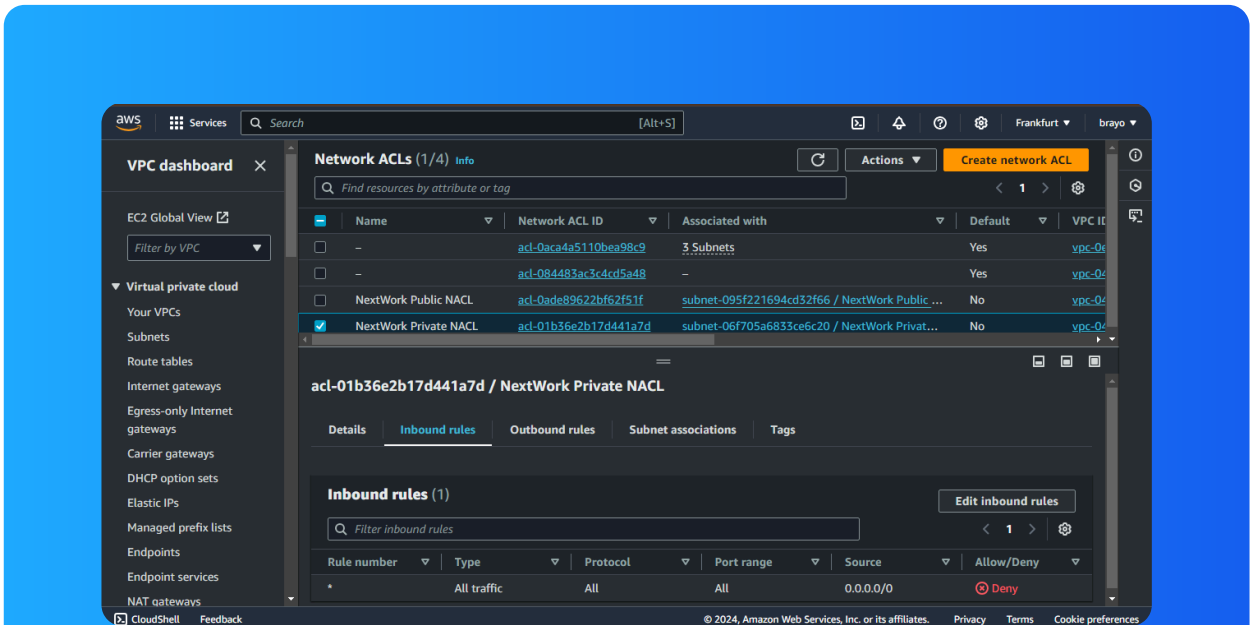
NextWork.org

A new network ACL

By default, my private subnet is associated with the default Network ACL for the VPC. This default ACL allows all inbound and outbound traffic, which could expose the subnet to unrestricted access.

I set up a dedicated network ACL for my private subnet because the default NACL allows all traffic, which could expose the subnet to potential security risks. By creating a custom ACL, I can restrict traffic and enhance security of my private subnet.

My new network ACL has two simple rules - the inbound and outbound rules are initially set to deny all traffic. This ensures that no traffic is allowed until we customize the rules to specify which sources of traffic we want to permit later in proect



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for more projects