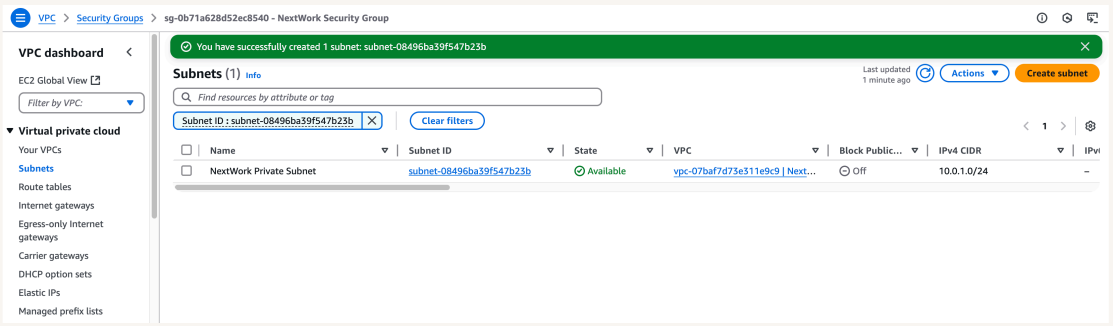
nextwork.org

Creating a Private Subnet

ralphgibendi01@gmail.com



ralphgibendi01@gmail.com
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a virtual network in AWS. It lets you define your isolated network, control traffic, and enhance security. It's useful for secure, flexible, and scalable cloud environments.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create a private subnet with a custom Network ACL, enhancing security by controlling traffic flow to and from the subnet.

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

I didn't expect the initial complexity of fine-tuning the Network ACL rules for optimal security and connectivity between private and public subnets.

This project took me...

30 minutes

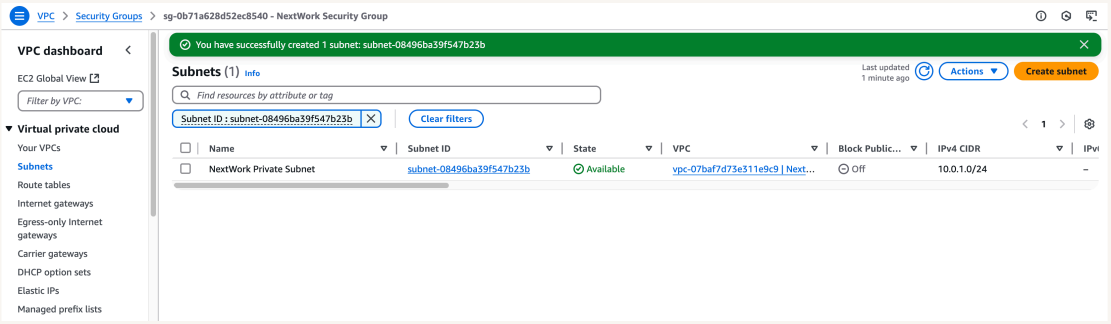
ralphgibendi01@gmail.com
NextWork Student

Private vs Public Subnets

The difference between public and private subnets is that public subnets have direct internet access, while private subnets do not, relying on NAT gateways for outbound traffic.

Having private subnets are useful because they enhance security by isolating resources from direct internet exposure, protecting sensitive data and applications.

My private and public subnets cannot have the same CIDR block, as they must reside within distinct IP address ranges within the VPC.



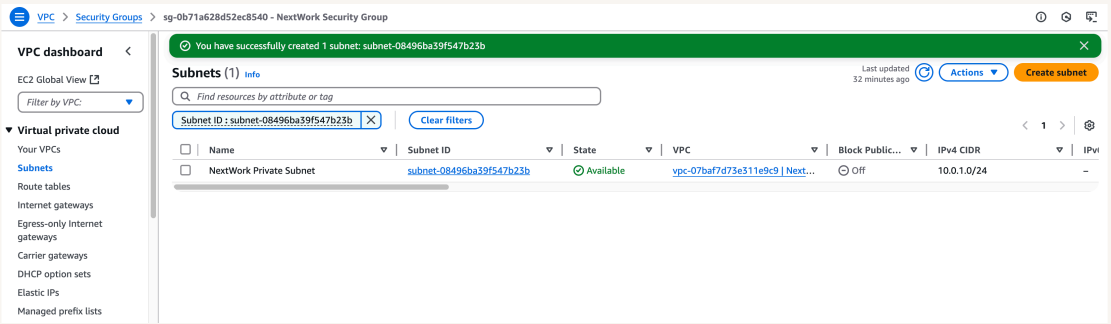
ralphgibendi01@gmail.com
NextWork Student

A dedicated route table

By default, my private subnet is associated with the main route table of the VPC, which includes a local route for internal communication but no routes for internet access, keeping the subnet private.

I had to set up a new route table because I needed specific routing rules to direct traffic appropriately, such as allowing instances in the private subnet to access the internet through a NAT gateway while maintaining 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. There are no rules for internet access, ensuring that the subnet remains isolated while facilitating internal communication



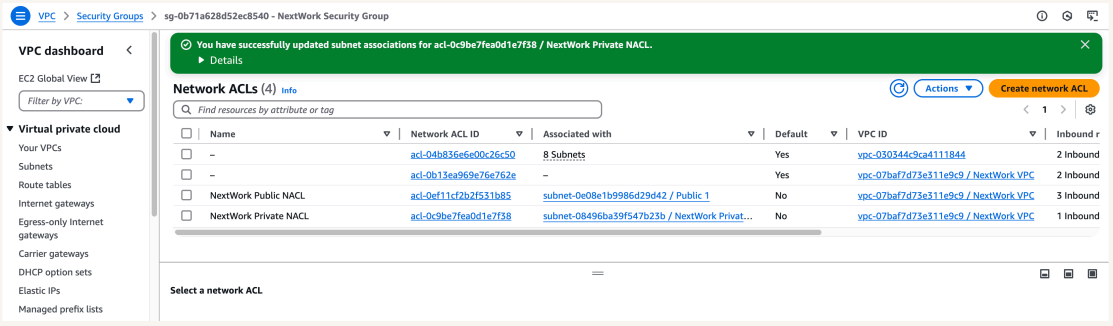
ralphgibendi01@gmail.com
NextWork Student

A new network ACL

By default, my private subnet is associated with the default Network ACL of the VPC. This default NACL allows all inbound and outbound traffic.

I set up a dedicated network ACL for my private subnet because I need to enforce specific security rules that differ from the default NACL, allowing for granular control over inbound and outbound traffic.

My new network ACL has two simple rules: it allows inbound traffic from the subnet's own CIDR block and outbound traffic to the NAT gateway's IP range.



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for more projects