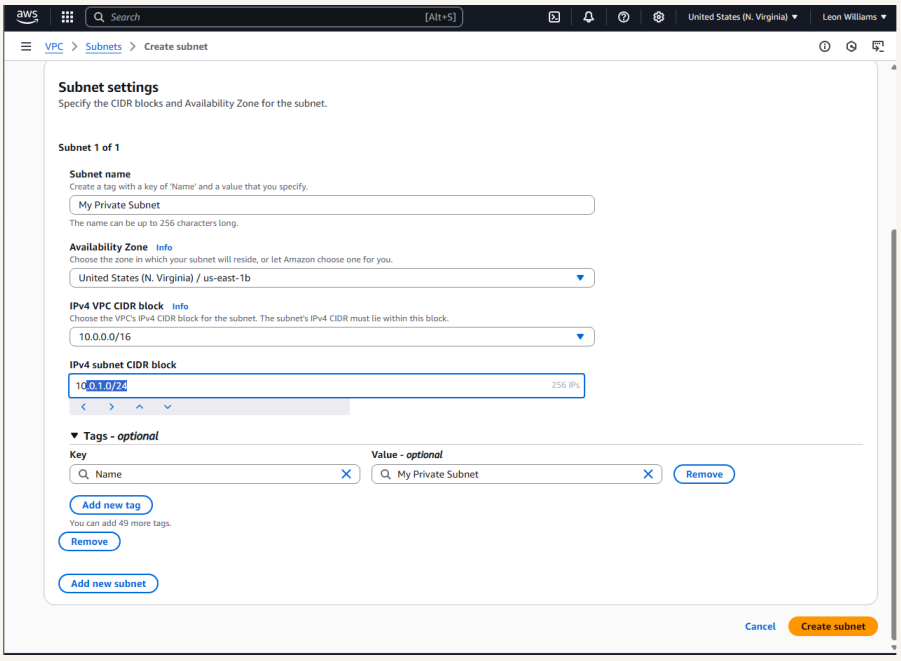
nextwork.org

Creating a Private Subnet

Leon Williams



Leon Williams
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC lets you create a private and isolated network in the cloud. It is useful because it gives you full control over networking, such as IP ranges, subnets, route tables, and gateways, to securely run AWS resources.

How I used Amazon VPC in this project

I used Amazon VPC to build a secure network environment by creating public and private subnets, setting up route tables to control traffic flow, and configuring network ACLs to manage access. This setup keeps sensitive resources protected.

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

One thing I didn't expect in this project was that the default network ACL allows all traffic, even to private subnets. I thought removing internet access in the route table was enough, but the ACL had to be secured too.

Leon Williams
NextWork Student

This project took me...

It took me just over 33 minutes to complete. The estimate was 60 minutes, but reusing my AWS setup from the last project definitely cut my time in half.

Leon Williams
NextWork Student

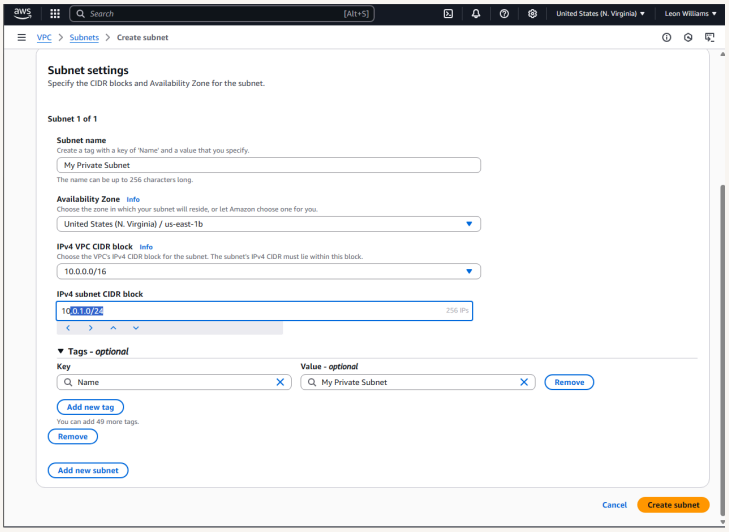
Private vs Public Subnets

The difference between public and private subnets is that public subnets can access the internet through an internet gateway, while private subnets are isolated and used for sensitive resources like databases.

Having private subnets is useful because they let you separate resources, like databases, from the public internet. This prevents unauthorized access and keeps your network organized using unique IP ranges that avoid overlap with public subnets.

My private and public subnets cannot have the same CIDR block, because each subnet in a VPC must have a unique IP range to avoid conflicts and ensure traffic is routed correctly.

Leon Williams
NextWork Student



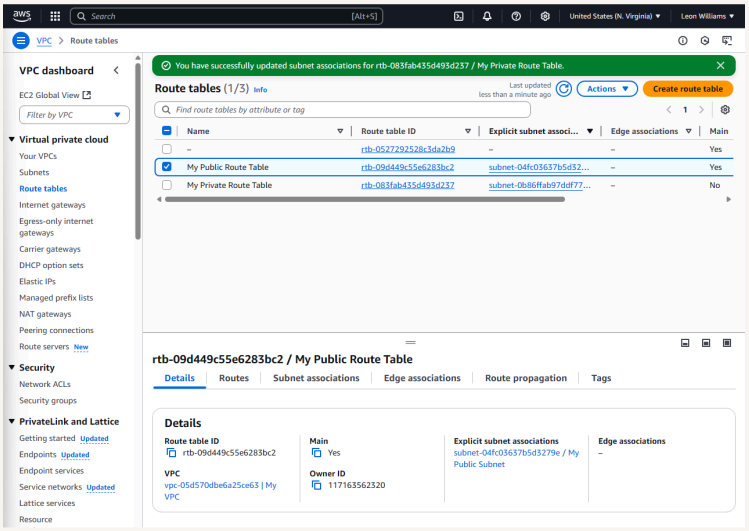
A dedicated route table

By default, my private subnet is associated with the already created Route Table, which is the default route table AWS created with my VPC. This happens because subnets not linked to another route table automatically use the default one.

I had to set up a new route table because the default route table has a route to an internet gateway, which would make my private subnet public. To keep it isolated, I created a separate route table without internet access.

My private subnet's route table only allows local traffic within the VPC. It has no route to the internet gateway, so it keeps the subnet isolated by restricting traffic to internal resources and blocking any direct internet access.

Leon Williams
NextWork Student



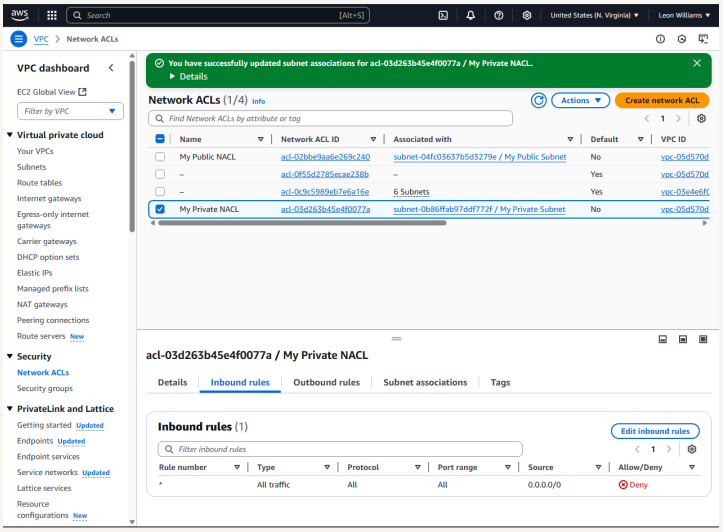
A new network ACL

By default, my private subnet is associated with the VPC's default network ACL, which allows all traffic. This happens because I haven't explicitly linked the private subnet to a custom-made private Network ACL yet.

I set up a dedicated private network ACL for my private subnet because the default ACL allows all traffic, which is insecure. A custom ACL lets me control inbound and outbound traffic, adding an extra layer of protection for sensitive resources.

My new network ACL has two simple rules: it denies all inbound and all outbound traffic by default. Custom NACLs start this way to ensure nothing gets through until specific rules are added to allow trusted traffic.

Leon Williams
NextWork Student



The place to learn & showcase your skills

Check out nextwork.org for more projects