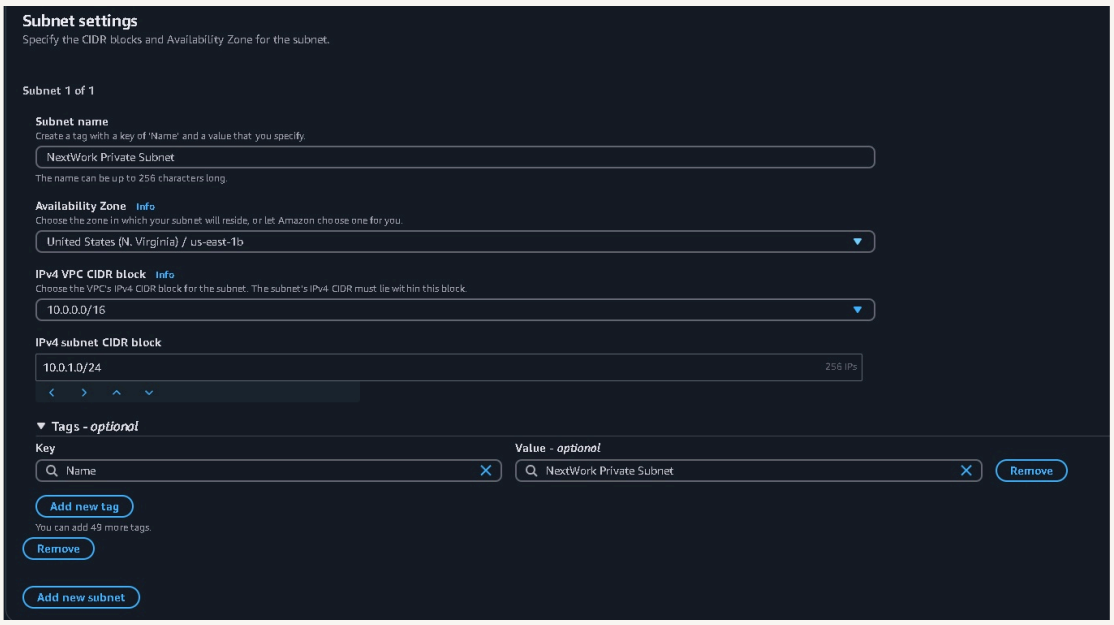
Creating a Private Subnet

Antonio C



Antonio C
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is a service that lets you create a private, isolated network within AWS. It’s useful for securely hosting resources, controlling network traffic, and customizing IP address ranges, subnets, and routing for enhanced

How I used Amazon VPC in this project

 Create a private subnet. Create a private route table. Create a private network ACL.

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

I did not expect the various security changes in ACL

This project took me...

This project took me about an hour to complete.

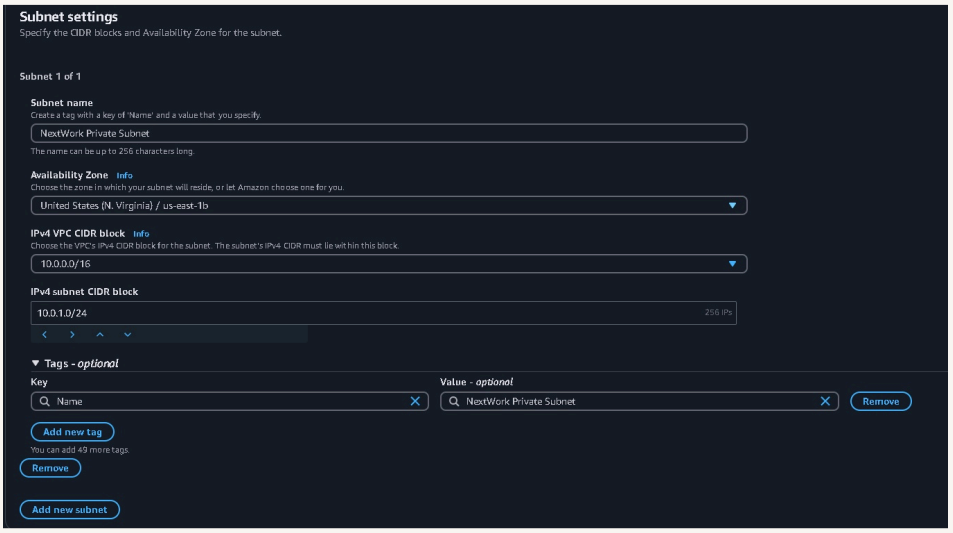
Antonio C
NextWork Student

Private vs Public Subnets

Public subnets have a route to the internet via an Internet Gateway, allowing direct access. Private subnets lack this route, so resources within them can't be accessed directly from the internet, enhancing security for sensitive data.

Private subnets exist to protect sensitive resources, like databases or internal apps, from direct internet access. This enhances security by limiting exposure and allowing only controlled communication through NAT or internal networking.

Private and public subnets can't share the same IP address range (CIDR block) or the same route to the Internet Gateway. Public subnets need a route to the IGW, while private ones use a NAT or no internet route at all for security.



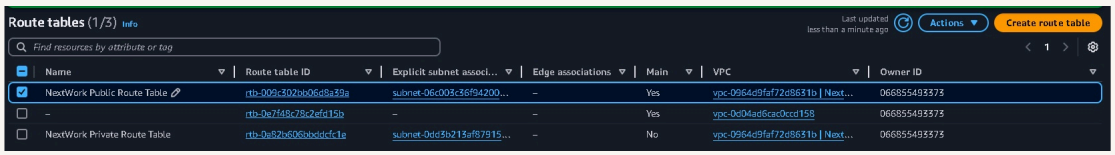
Antonio C
NextWork Student

A dedicated route table

By default, your private subnet is associated with the main route table of the VPC, which does not have a route to the Internet Gateway—keeping the subnet private and restricting direct internet access.

I had to set up a new route table because I am making sure it can only direct traffic to another internal resource (instead of the public internet).

A private subnet's route table allows internal VPC traffic (e.g., to other subnets) and, if configured, outbound internet traffic through a NAT Gateway or NAT instance. It blocks direct internet access by not routing through an Internet Gateway.



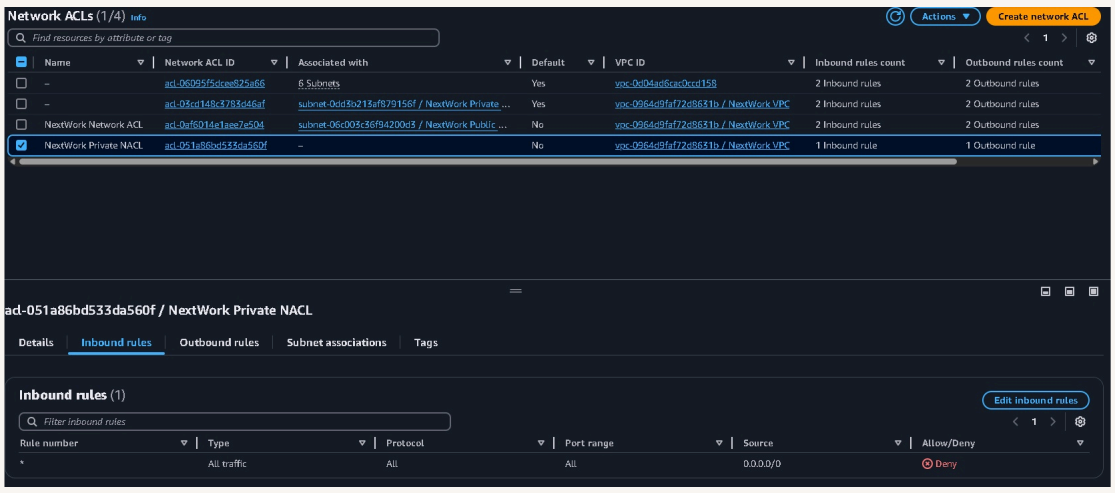
Antonio C
NextWork Student

A new network ACL

A VPC's default network ACL allows all traffic, which exposes your private subnet to unrestricted access from the internet or other untrusted networks.

I set up a dedicated network ACL for my private subnet because it restricts traffic and protects your private subnet!

I set up a custom network NACLs to control inbound and outbound traffic for this private subnet - denying all traffic by default.



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for more projects