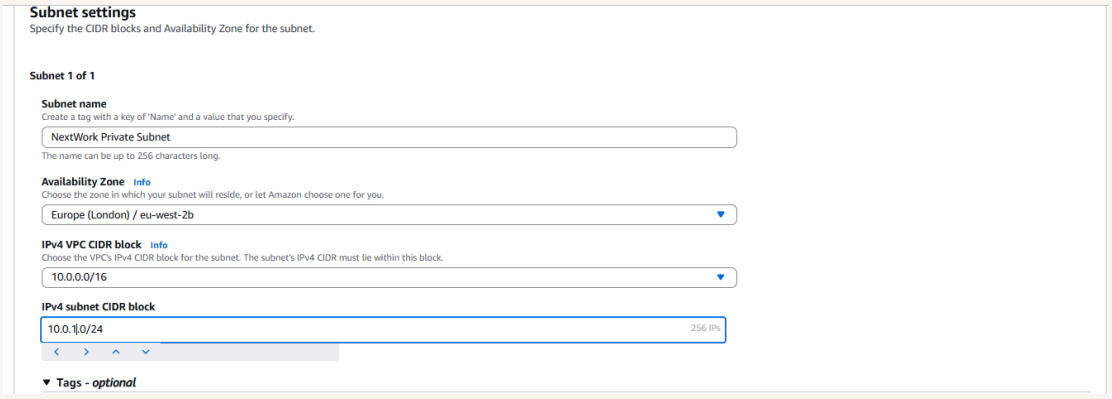
nextwork.org

Creating a Private Subnet

AM ampahben3@gmail.com



AM
ampahben3@gmail.com
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) lets you control access and resource availability in AWS. It enhances security by isolating sensitive data, defining network rules, and ensuring only authorized users can interact with specific services.

How I used Amazon VPC in this project

I used Amazon VPC to set up private and public subnets, configure route tables for traffic control, add an internet gateway for public access, and create network ACLs and security groups to manage resource security and regulate traffic flow.

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

Repeating steps with slight changes was unexpected, but it reinforced key AWS concepts. The level of detail required for each configuration and its impact on security was surprising too.

AM
ampahben3@gmail.com
NextWork Student
NextWork.org

This project took me...

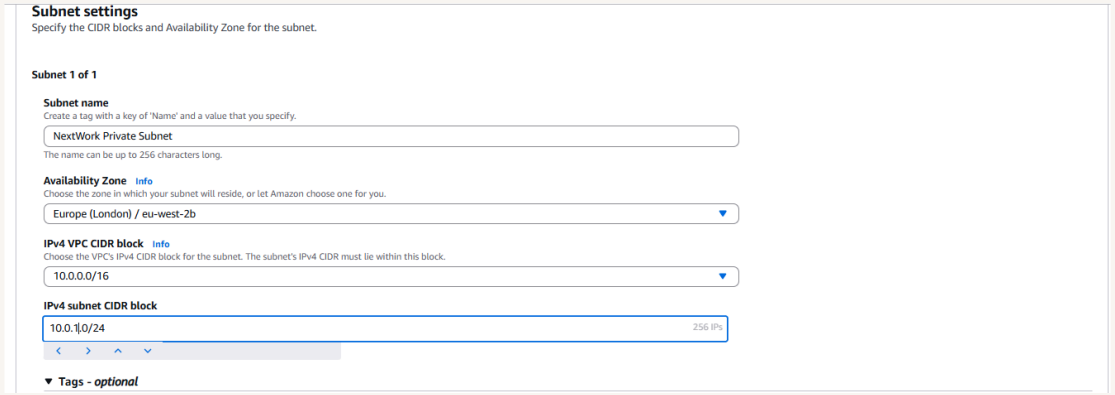
It took an hour because I focused on revising the first part, ensuring the Public Subnet was set up correctly and carefully configuring the CIDR block. Taking time on these foundational steps helped streamline the rest of the process.

Private vs Public Subnets

The difference between public and private subnets is that public subnets host resources accessible from the internet, while private subnets are isolated for security, housing sensitive data or internal applications without direct internet exposure.

Having private subnets are useful because they restrict internet access, protect sensitive data, and ensure controlled access. They enhance security, support internal applications, and minimize exposure to threats, keeping critical systems safe.

My private and public subnets cannot have the same CIDR block, as each subnet must have a unique IP range. This ensures proper network segmentation and avoids conflicts, enabling efficient routing and secure communication between resources.

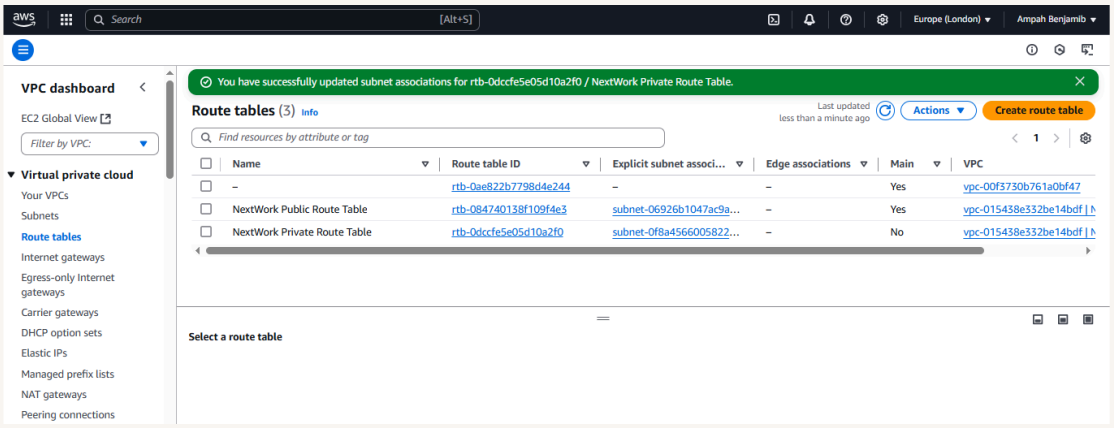


A dedicated route table

By default, my private subnet is associated with the main route table of the custom VPC I created. This ensures internal communication while maintaining controlled access and preventing direct exposure to the public subnet.

I had to set up a new route table because the initial one was for a public subnet. This ensures private subnet traffic stays isolated, preventing unintended access and maintaining secure network segmentation.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows traffic within the VPC. It ensures secure internal communication while preventing direct external access, maintaining isolation for private resources.

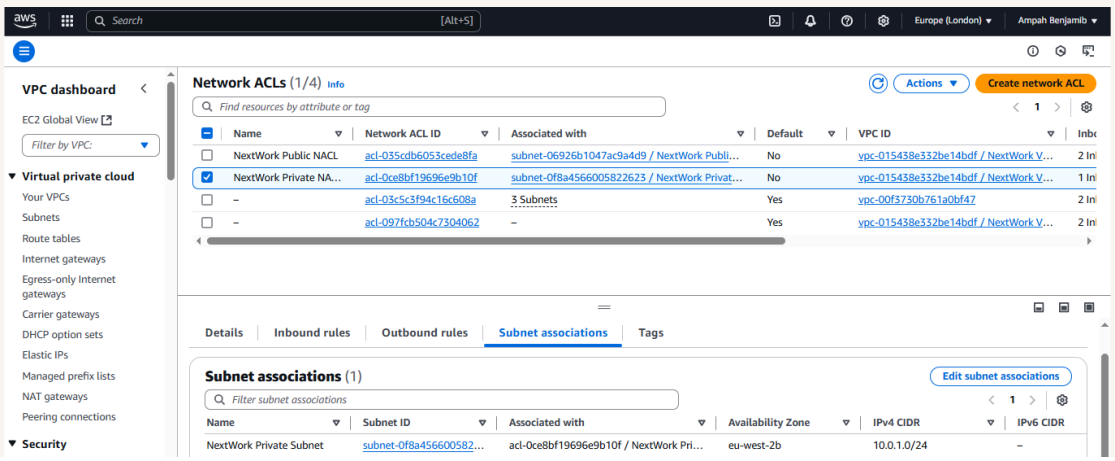


A new network ACL

By default, my private subnet is associated with the default network ACL of the VPC. This ACL automatically applies basic inbound and outbound rules, but a custom ACL can be configured to enforce stricter security controls for private resources.

I set up a dedicated network ACL for my private subnet because the default ACL is linked to the public subnet. The private subnet needs stricter security, so a separate ACL ensures controlled inbound and outbound rules, preventing unnecessary access.

My new network ACL has two simple rules-one inbound and one outbound. The inbound rule denies all traffic from any source, ensuring no unauthorized access. Similarly, the outbound rule denies all traffic, preventing any data from leaving the subnet.



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for more projects