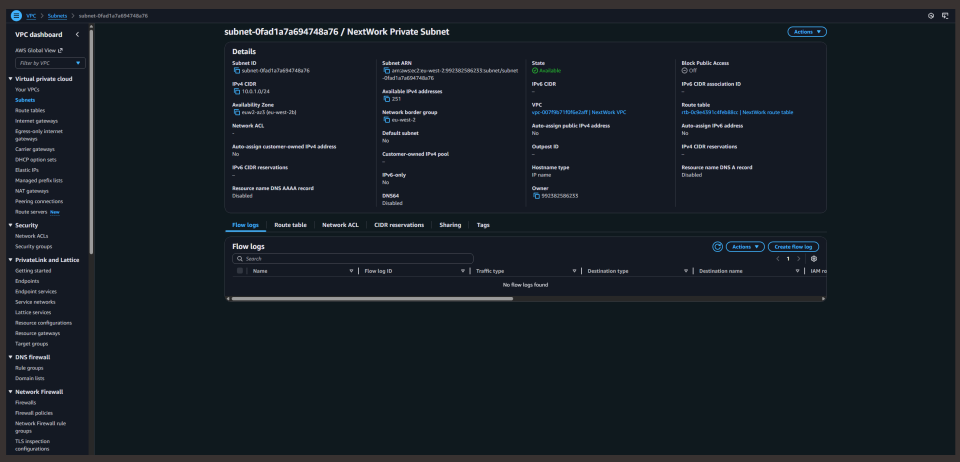
nextwork.org

Creating a Private Subnet

Louis



Louis
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is your own private network in AWS where you can launch and manage your cloud resources in an isolated environment that you control.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to build a multi-tier network architecture with proper security segmentation. I started by creating a VPC with the CIDR block 10.0.0.0/16, then created separate public and private subnets to isolate different types of resources. I configured route tables for each subnet type. The public route table with a route to the internet gateway for internet connectivity, and the private route table with only local routes to keep backend resources isolated. I also set up dedicated network ACLs for my private subnet to implement subnet-level access controls, creating multiple layers of security.

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

One thing I didn't expect in this project is how many separate components are needed to truly make a subnet private. I initially thought that just not having an internet gateway route would be enough, but I learned that I also need to create dedicated route tables, configure custom network ACLs with specific rules, and understand how all these layers work together.

This project took me...

This project took me just over an hour to work through, creating the basic VPC infrastructure and then building out the private subnet with all its associated components. The time was spent understanding the concepts behind public versus private subnets, carefully configuring the private route table to ensure no

Louis
NextWork Student

Private vs Public Subnets

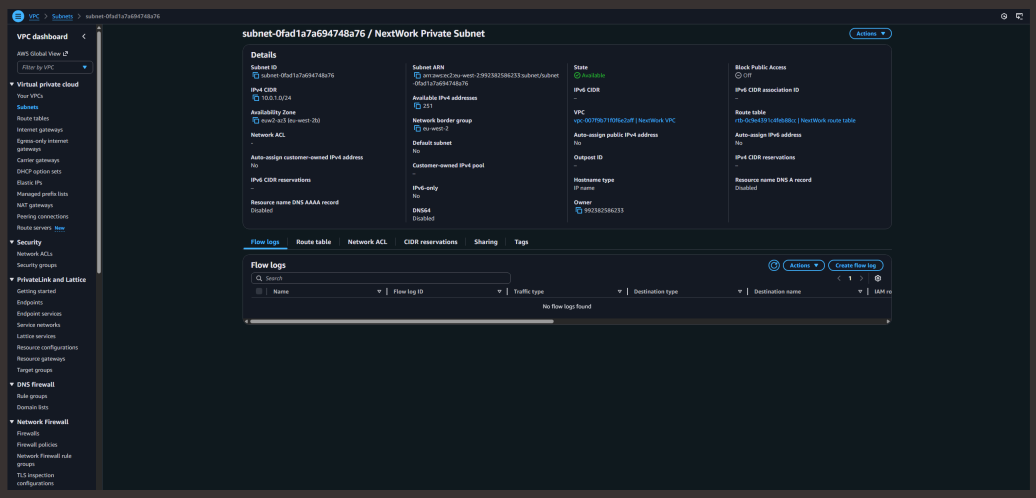
The difference between public and private subnets is that a public subnet has a route to an internet gateway in its route table, allowing resources within it to send and receive traffic directly from the internet, while a private subnet does not have this route and keeps its resources isolated from direct internet access. Public subnets are used for resources that need to be accessible from the internet like web servers, whereas private subnets are used for backend resources like databases that should only communicate within the VPC.

Having private subnets are useful because they provide a secure layer of isolation for backend resources that don't need direct internet access, reducing the attack surface of your infrastructure. By keeping databases, application servers, and internal APIs in private subnets, you ensure that these critical components can't be directly targeted by external threats while still allowing them to communicate with other resources inside your VPC.

My private and public subnets cannot have the same CIDR block because each subnet needs its own unique set of IP addresses within the VPC. They also cannot share the same route table if you want them to act differently. Public subnets require a route table with an internet gateway route, while private subnets should not have this route. Additionally, they typically shouldn't share the same network ACL if you want different traffic filtering rules for each subnet type.

Louis
NextWork Student

nextwork.org



A dedicated route table

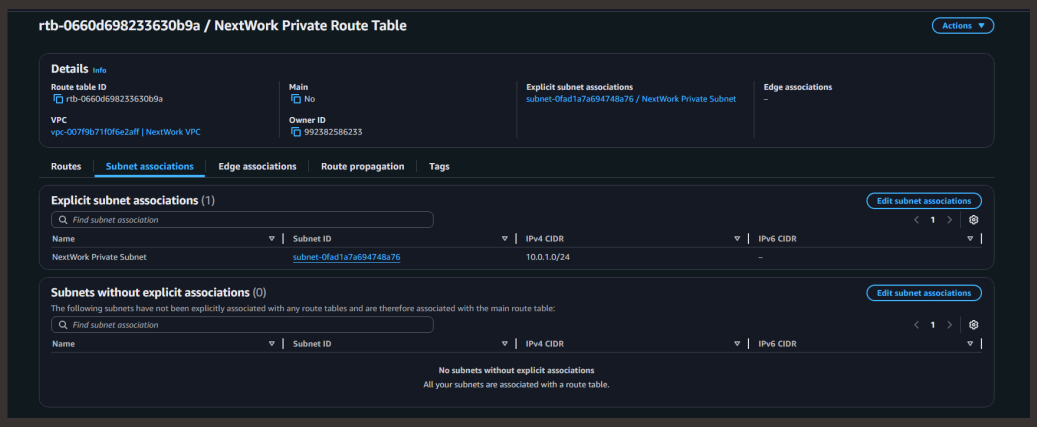
By default, my private subnet is associated with the default route table that was automatically created when I set up my VPC. This main route table is automatically assigned to any subnet that doesn't have an explicit custom route table association. That's why I need to create a separate private route table and manually associate it with my private subnet to ensure it has the correct routing rules without internet gateway access.

I had to set up a new route table because the default route table doesn't provide the routing configuration I need for my private subnet. By creating a dedicated private route table, I can ensure that traffic from my private subnet stays within the VPC and doesn't have a route to the internet gateway. This separation allows me to maintain different routing behaviours for my public and private subnets. The public subnet can access the internet while the private subnet remains isolated and secure.

My private subnet's dedicated route table only has one route that allows all traffic within the 10.0.0.0/16 VPC to communicate locally, which means my NextWork Private Subnet 10.0.1.0/24 can talk to other subnets in the VPC but not the internet.

Louis
NextWork Student

nextwork.org



A new network ACL

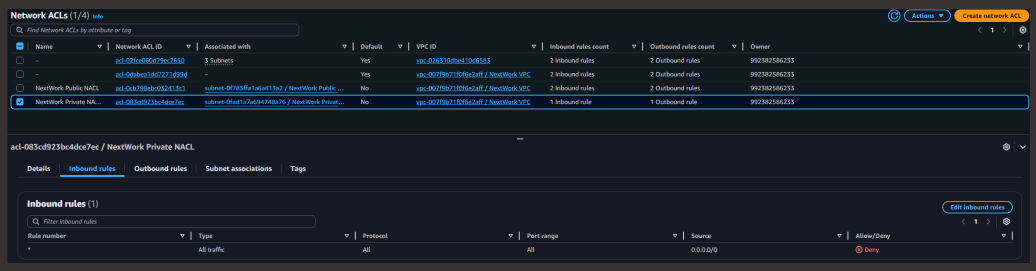
By default, my private subnet is associated with the default network ACL that was automatically created when I set up my VPC. This default network ACL allows all inbound and outbound traffic by default, which means it doesn't provide any traffic filtering at the subnet level. That's why I need to create a custom private network ACL with more restrictive rules and associate it with my private subnet to add proper security controls.

I set up a dedicated network ACL for my private subnet because the default network ACL allows all traffic, and I need more rules to secure my private subnet.

My new network ACL has two simple rules. One inbound rule and one outbound rule that both deny all traffic by default (rule * denying all protocols from 0.0.0.0/0).

Louis
NextWork Student

nextwork.org



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects