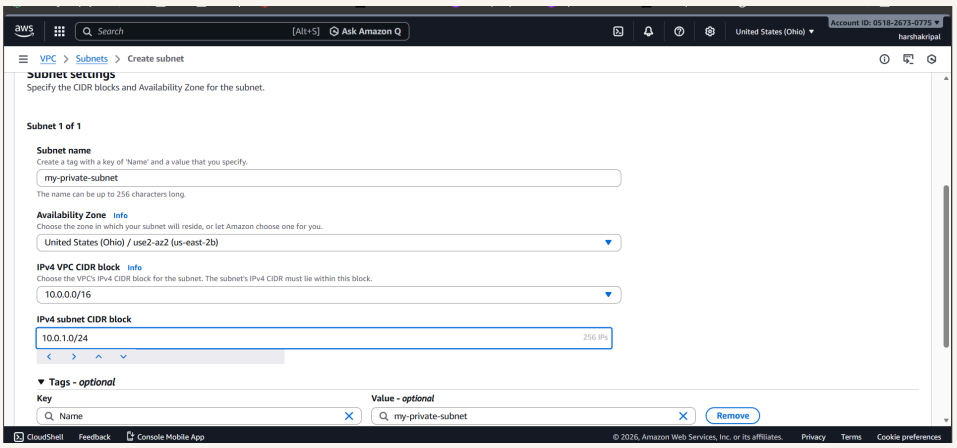
nextwork.org

Creating a Private Subnet

Harshada Kripal



Harshada Kripal
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a Virtual Private Cloud that allows you to set up a secure and isolated network environment within AWS. It is useful because it gives you complete control over network configuration, security, and traffic management, ensuring that resources can communicate safely and efficiently.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create a private subnet which further have private route tables and private Network ACL's which ensures security of my private subnet.

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

One thing I didn’t expect in this project is how much thought and configuration goes into securing private subnets. Creating private subnets, dedicated route tables, and custom Network ACLs gave me a deeper understanding of how traffic is carefully controlled and filtered within a VPC to protect resources while still allowing necessary communication.

Harshada Kripal
NextWork Student

This project took me...

This project took me 30 minutes to complete.

Harshada Kripal
NextWork Student

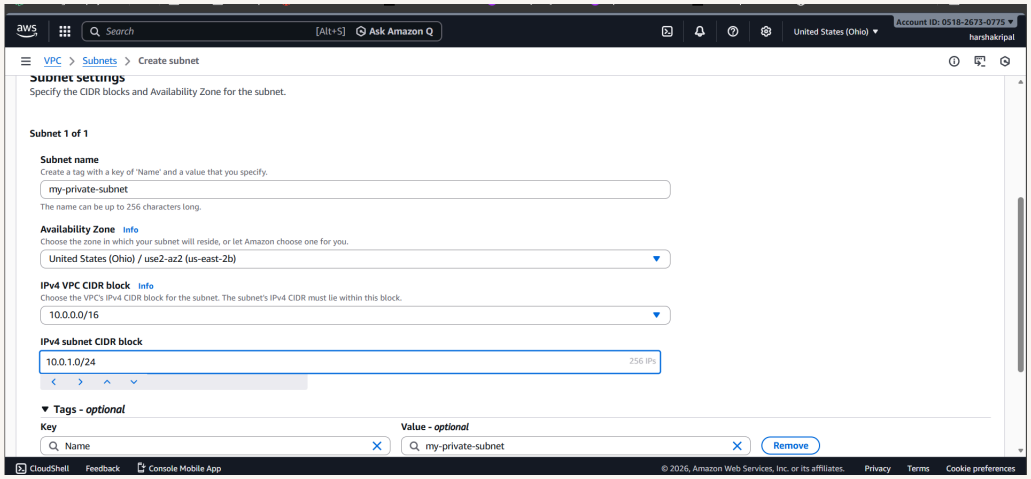
Private vs Public Subnets

The difference between public and private subnets is that a public subnet has a route to an Internet Gateway, allowing resources within it to communicate directly with the internet, while a private subnet does not have direct internet access and is used for resources that should remain isolated from public networks, such as databases or internal services.

Having private subnets is useful because it isolates the resources from public networks, enhancing security and reducing exposure to potential threats, while still allowing controlled access to other resources within the VPC or through a NAT gateway for internet connectivity when needed.

My private and public subnets cannot have the same.CIDR Block because that's what keeps each range complete separate from each other.

Harshada Kripal
NextWork Student



Harshada Kripal
NextWork Student

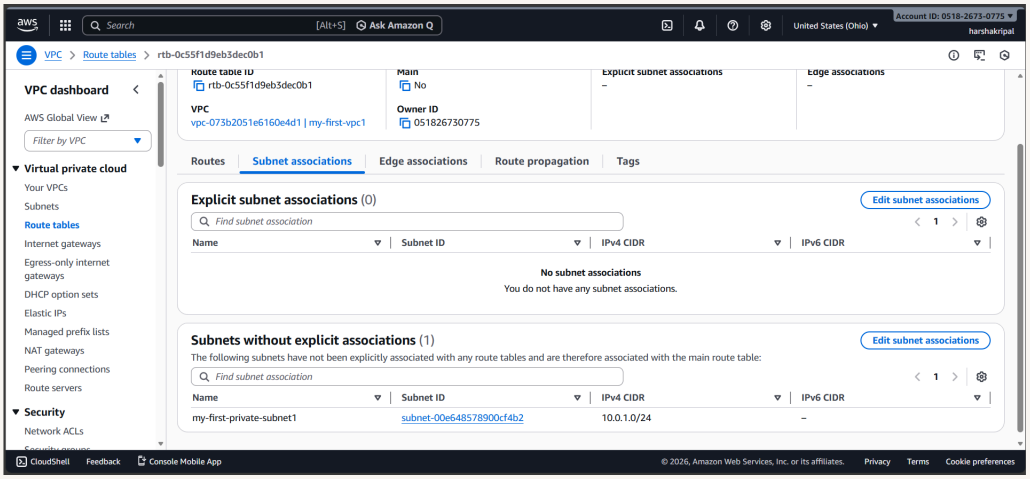
A dedicated route table

By default, my private subnet is associated with the main route table of the VPC, which controls the routing of traffic for that subnet unless a custom route table is explicitly associated.

I had to set up a new route table because I wanted to define custom routing rules for my private subnet, such as directing traffic through a NAT gateway instead of an Internet Gateway, to ensure secure and controlled communication.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows traffic to and from the VPC and necessary internal resources, while blocking direct access to the public internet.

Harshada Kripal
NextWork Student



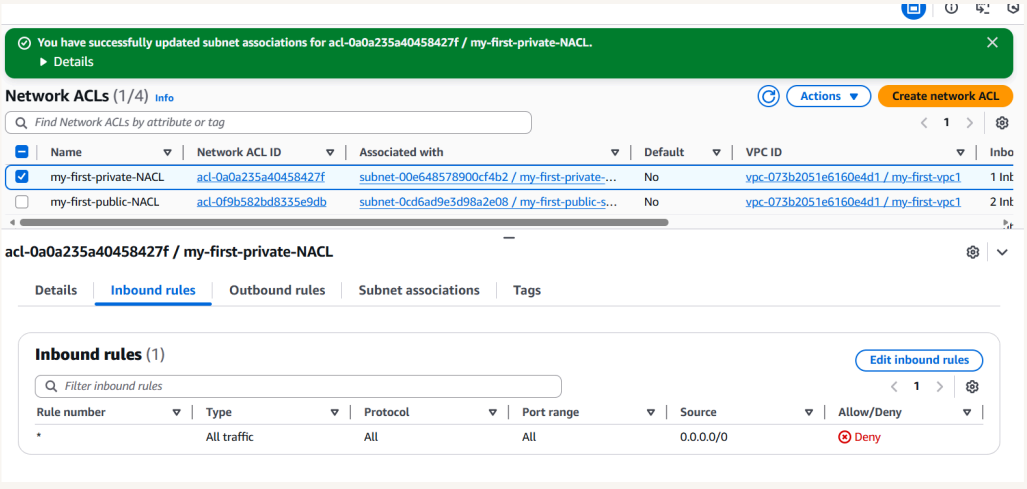
Harshada Kripal
NextWork Student

A new network ACL

By default, my private subnet is associated with the default Network ACL created by AWS, which allows all types of traffic into the subnet and could pose security risks.

I set up a dedicated network ACL for my private subnet to enhance security, I created a custom private Network ACL to serve as an additional layer of protection for my private subnet.

My new Network ACL has two simple rules – one inbound rule and one outbound rule that explicitly do not allow unauthorized access.



The place to learn & showcase your skills

Check out nextwork.org for more projects