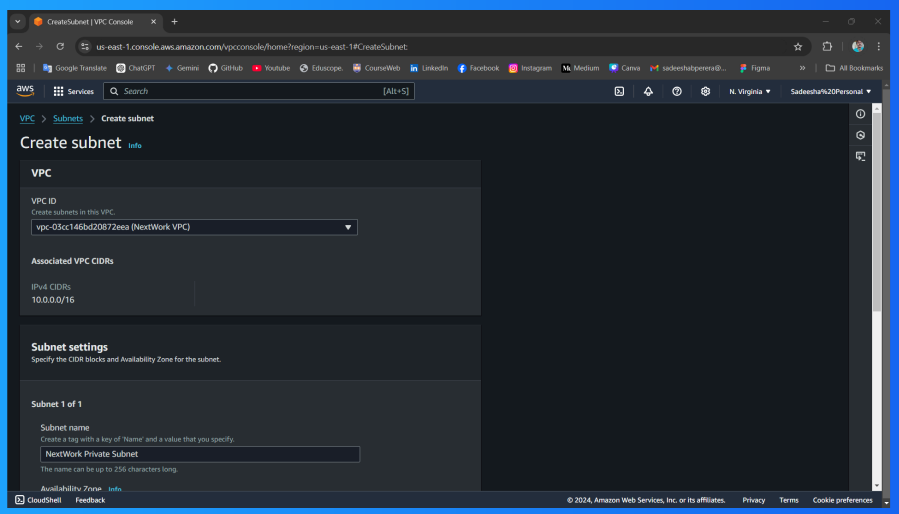
NextWork.org

Creating a Private Subnet

Sadeesha Perera



Sadeesha Perera
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon Virtual Private Cloud (VPC) is a service that allows you to launch Amazon Web Services (AWS) resources into a virtual network that you define. This virtual network resembles a traditional network you'd operate in your own data centre.

How I used Amazon VPC in this project

I used private subnet, create a VPC, define a private subnet, configure a route table with a NAT Gateway, create security groups to control traffic and launch EC2 instances within the subnet.

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

How easy is to create private subnet to secure resources in AWS.

This project took me...

30 minutes

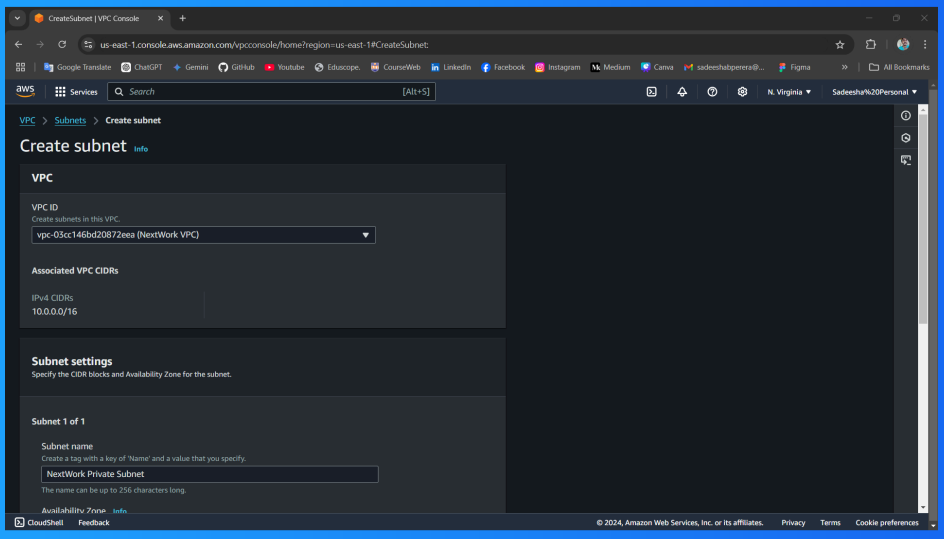
Sadeesha Perera
NextWork Student

Private vs Public Subnets

Public subnets are directly connected to the internet gateway, allowing resources within them to access the public internet. Private subnets, on the other hand, do not have direct internet access.

Private subnets exist to enhance the security and isolation of resources within a VPC. By preventing direct internet access to resources in private subnets, you can significantly reduce the risk of unauthorized access and attacks.

Private and public subnets within a VPC cannot directly share public IP addresses. Public subnets can have public IP addresses assigned to their instances, allowing them to be accessed directly from the internet.



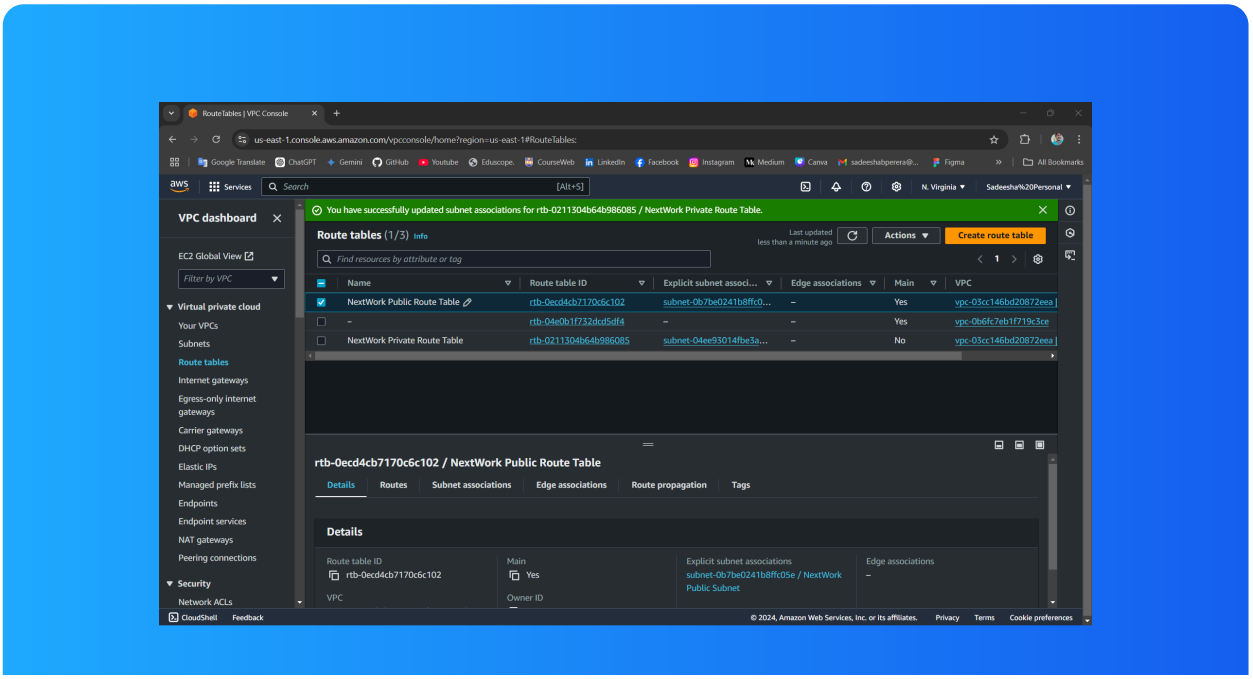
Sadeesha Perera
NextWork Student

A dedicated route table

By default, a private subnet is associated with the main route table of the VPC. This main route table typically contains a default route that directs traffic to a NAT Gateway. This allows instances in the private subnet to access the internet.

I created new route tables to achieve network segmentation, custom routing, and enhanced security. By isolating traffic, and defining specific routes.

A private subnet's route table typically allows traffic to a NAT Gateway for internet access, other private subnets for internal communication, and VPC endpoints for private AWS service access.



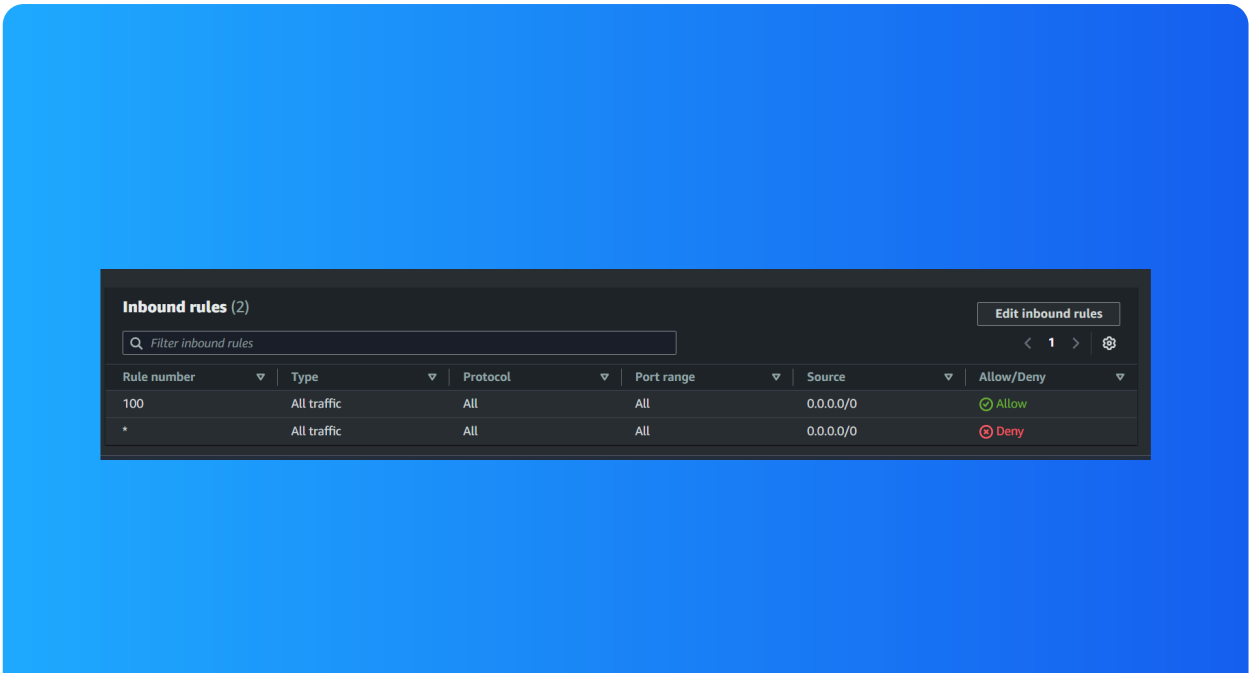
Sadeesha Perera
NextWork Student

A new network ACL

By default, a private subnet is associated with the default network ACL of the VPC. This default NACL allows all inbound and outbound traffic, which can pose a security risk if not configured properly.

I set up a new network ACL to enhance security and control traffic flow within our VPC. By creating a custom network ACL with specific allow and deny rules, we can restrict access to our private subnet and prevent unauthorized traffic.

Inbound rules typically include a default deny rule and specific allow rules for SSH and RDP traffic from trusted IP addresses. Outbound rules often allow all traffic by default but can be customized to restrict specific outbound connections.



Everyone should be in a job they love.

Check out nextwork.org for more projects