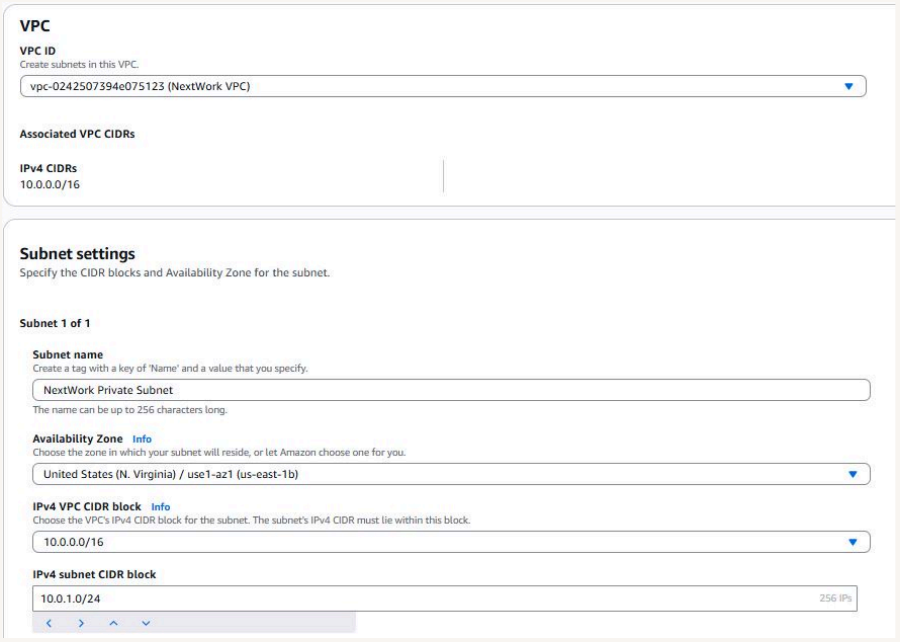
nextwork.org

Creating a Private Subnet

Mohammed Dawoud Mota



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a virtual private cloud that lets you launch AWS resources in a private, isolated network. It’s useful for controlling network configuration, security, and access to resources in the cloud.

How I used Amazon VPC in this project

In today’s project, I used Amazon VPC to create a custom network with public and private subnets, route tables, internet gateway, security groups, and NACLs to securely manage traffic and access for resources.

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

One unexpected thing was how creating a private subnet required a unique CIDR block and a separate route table and NACL to keep it isolated from the internet.

This project took me...

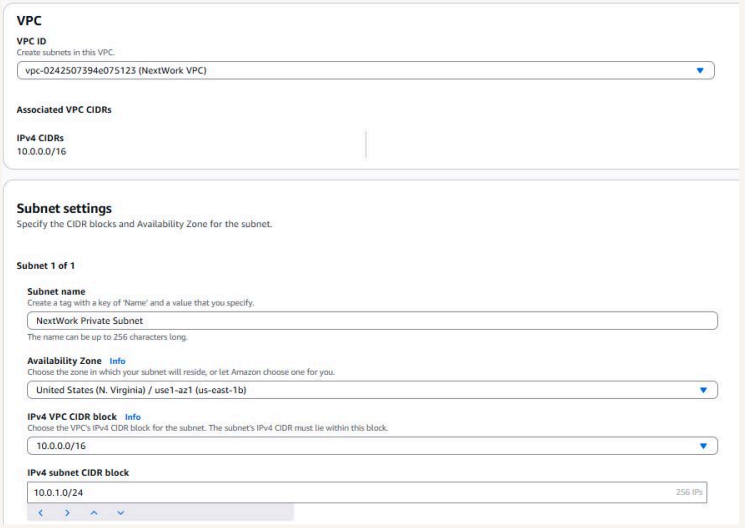
This project took me 35 minutes.

Private vs Public Subnets

A public subnet has a route to an internet gateway, allowing direct internet access. A private subnet has no direct internet route, keeping resources isolated from the internet for security.

Private subnets exist to securely host resources that shouldn’t be directly accessible from the internet, like databases or internal services, protecting sensitive data while still allowing controlled internal access.

Private and public subnets cannot share the same CIDR block. Each subnet must have a unique IP range to avoid address conflicts within the VPC.

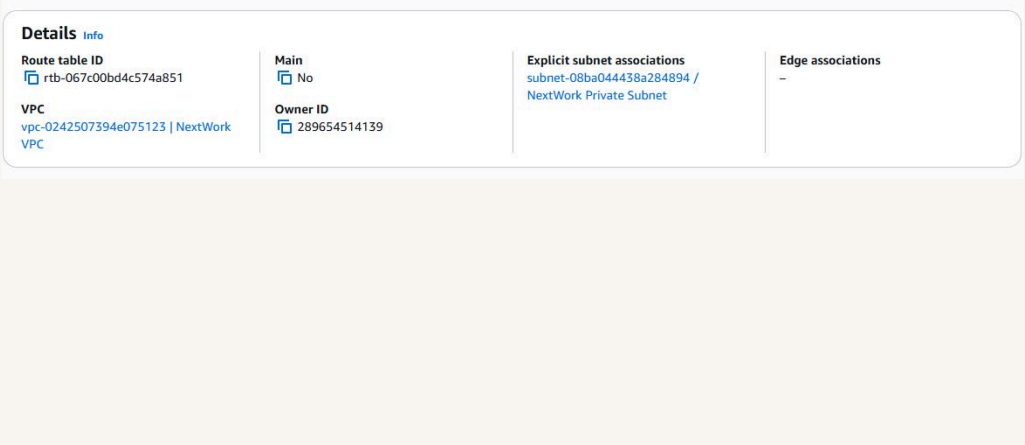

VPC
VPC ID
Create subnets in this VPC.
vpc-0242507394e075123 (NextWork VPC)
Associated VPC CIDRs
IPv4 CIDRs
10.0.0.0/16
Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.
Subnet 1 of 1
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
NextWork Private Subnet
The name can be up to 256 characters long.
Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
United States (N. Virginia) / use1-az1 (us-east-1b)
IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16
IPv4 subnet CIDR block
10.0.1.0/24
256 IPs

A dedicated route table

By default, a private subnet is associated with the VPC's main route table unless you create and assign a custom route table.

A new route table is set up so the private subnet can have custom routing that blocks internet access while allowing internal VPC communication.

The private subnet's route table allows only internal VPC traffic and does not route traffic to the internet.

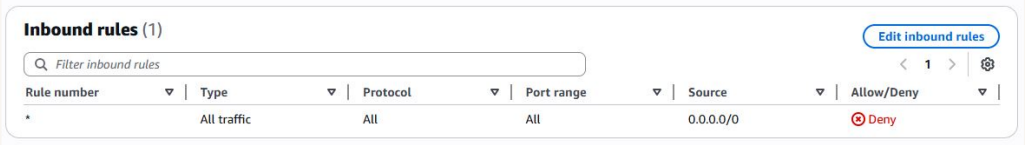


A new network ACL

By default, the VPC's default network ACL is associated with a private subnet unless a custom NACL is created and assigned.

A new network ACL is set up to secure the private subnet by explicitly controlling inbound and outbound traffic instead of relying on the default ACL, which allows all traffic.

In the new private NACL, all inbound and outbound traffic is denied by default until specific rules are added to allow certain traffic.



The place to learn & showcase your skills

Check out nextwork.org for more projects