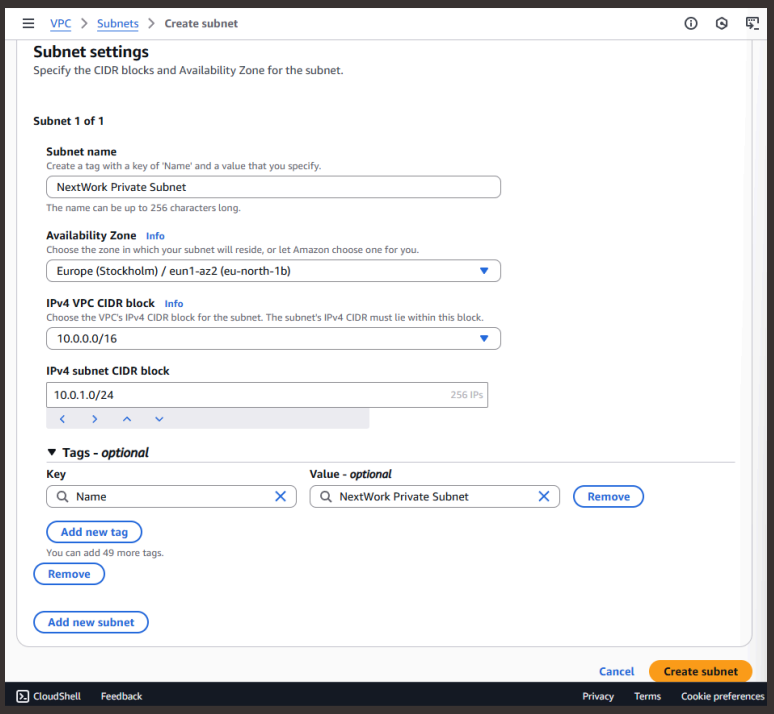
nextwork.org

Creating a Private Subnet

D Duc Thai



Duc Thai
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is your private network in AWS where you pick IP ranges, subnets, routes and firewalls. It isolates and secures resources, controls internet access, and lets you connect safely to your data center or office.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to set up the private subnet, private route table and private NACL to protect resources that need to be store secured and private.

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

One thing I didn't expect in this project is that you must allow both inbound and outbound in a stateless NACL — forgetting one side will block traffic even if security groups, NAT, and IGW are correct.

This project took me...

This project took me 60 mintutes.

D
Duc Thai
NextWork Student

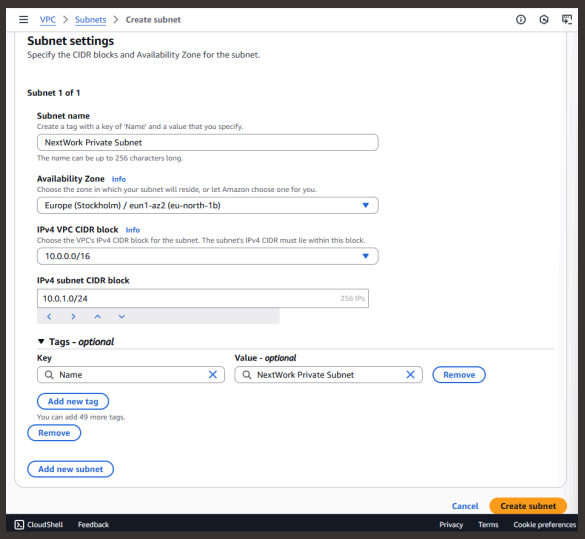
Private vs Public Subnets

The difference between public and private subnets is that Public subnet has a route to an Internet Gateway; resources with public IPs can be reached from the internet. Private subnet no IGW route, not reachable from the internet, uses a NAT to reach.

Having private subnets are useful because they to protect resources by keeping them off the internet. A private subnet has no IGW route, so it’s not publicly reachable. Instances can still reach out via a NAT, lowering attack surface.

My private and public subnets cannot have the same CIDR block Because subnets must be non-overlapping slices of the VPC IP range. Sharing CIDRs would cause duplicate IPs and routing conflicts. AWS enforces unique, non-overlapping subnet CIDR blocks.

Duc Thai
NextWork Student



A dedicated route table

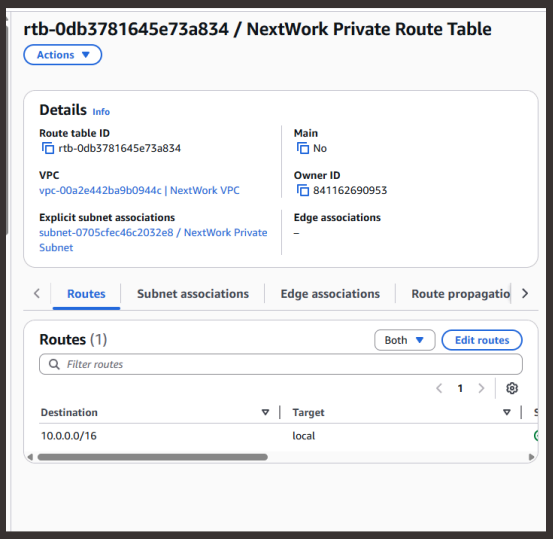
By default, my private subnet is associated with the route table that auto created by AWS when I set up my VPC.

I had to set up a new route table because the default route table was also used for public sub, which as the route the igw, that make my subnet public. Need to new one with no igw route to make the resources inside secure.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows lets instances talk to any IP inside the VPC. There’s no 0.0.0.0/0 to an IGW or NAT, so traffic won’t reach the internet—only intra-VPC communication.

D

Duc Thai
NextWork Student



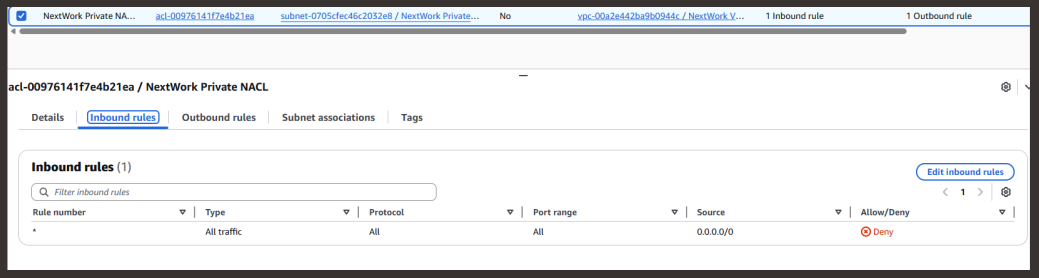
A new network ACL

By default, my private subnet is associated with default network ACL set up for every VPC. This default network ACL is associated with your private subnet, since I haven't set up an explicit association.

I set up a dedicated network ACL for my private subnet because the default ACL allows all traffic, which exposes your private subnet to unrestricted access from the internet or other untrusted networks. Need a new one that restricts traffic.

My new network ACL has two simple rules - denying all inbound and outbound traffic! I will leave these settings for now - let's customise them later in this project series,

Duc Thai
NextWork Student



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects