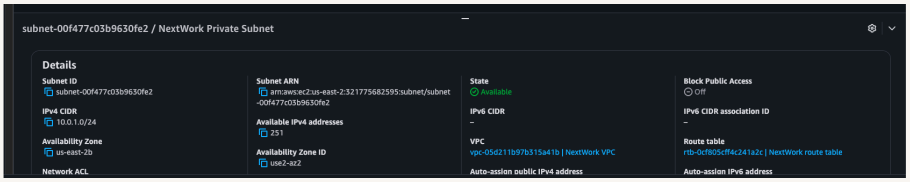
nextwork.org

Creating a Private Subnet

Roshan Shrestha



R
Roshan Shrestha
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a section of the amazon cloudspace that is distinguishable from the rest, like a town within a country. It is useful because it helps us identify and isolate our resources.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create a private subnet, a route table and a NACL for the private subnet.

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

One thing I didn't expect in this project is how easy it is to setup a private network ACL considering how important it is for security.

This project took me...

This project took me about an hour.

R
Roshan Shrestha
NextWork Student

Private vs Public Subnets

The difference between public and private subnets is that public subnets are connected to the internet via an internet gateway wheres the private subnet is meant for resources that we want to isolate from the internet and need local communication

Having private subnets are useful because we can keep resources like databases and user credentials private from the internet while maintaining access to resources local to the VPC

My private and public subnets cannot have the same addresses. Similar to how two sections of the same city do not have the same address, we don't assign the same IP range to private and pubic subnets.


subnet-00f477c03b9630fe2 / NextWork Private Subnet
Details
Subnet ID
subnet-00f477c03b9630fe2
IPv4 CIDR
10.0.1.0/24
Availability Zone
us-east-2b
Network ACL
Subnet ARN
arn:aws:ec2:us-east-2:321775682595:subnet/subnet-00f477c03b9630fe2
Available IPv4 addresses
251
Availability Zone ID
use2-az2
State
Available
IPv6 CIDR
–
VPC
vpc-05d211b97b315a41b | NextWork VPC
Auto-assign public IPv4 address
Block Public Access
Off
IPv6 CIDR association ID
–
Route table
rtb-0cf805cff4c241a2c | NextWork route table
Auto-assign IPv6 address

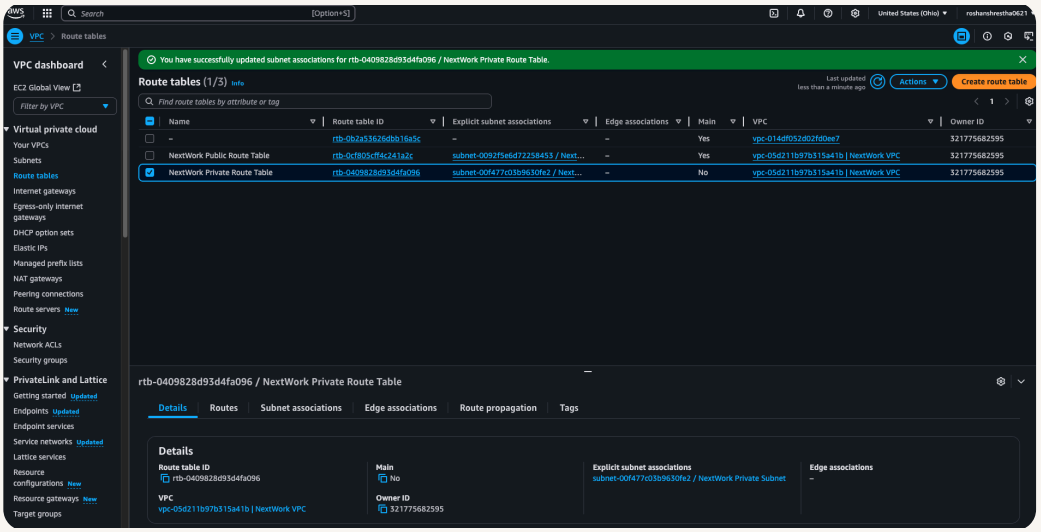
Roshan Shrestha
NextWork Student

A dedicated route table

By default, my private subnet is associated with the default VPC route table.

I had to set up a new route table because by default the private subnet was associated with the VPC route table which lead traffic to the internet gateway making my private subnet publicly accessible. So, new route with local access only.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows local traffic

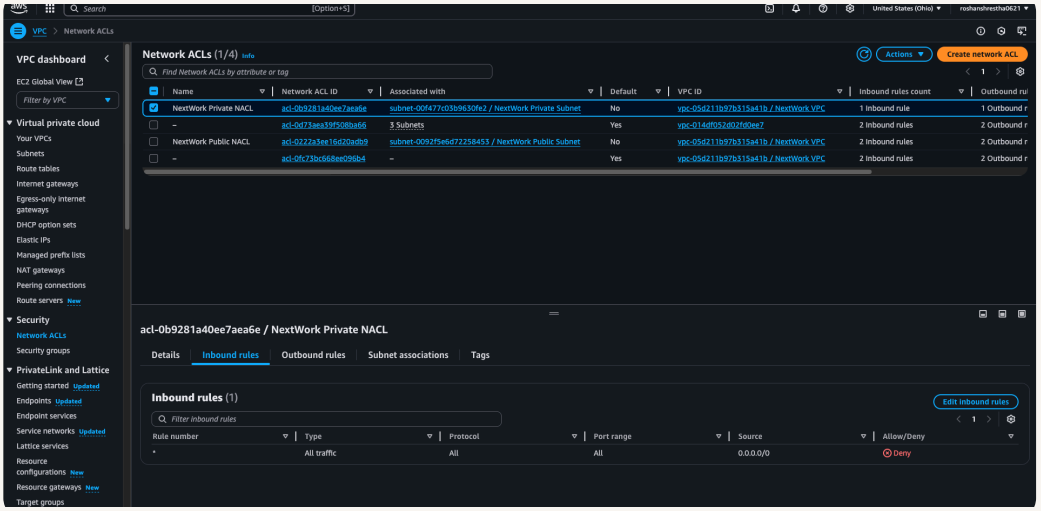


A new network ACL

By default, my private subnet is associated with the default NACL that AWS creates for each subnet. This NACL allows all inbound and outbound traffic.

I set up a dedicated network ACL for my private subnet because I want to control access to my resources in the private subnet. Not allow all traffic.

My new network ACL has two simple rules - Deny all inbound and outbound traffic.



The place to learn & showcase your skills

Check out nextwork.org for more projects