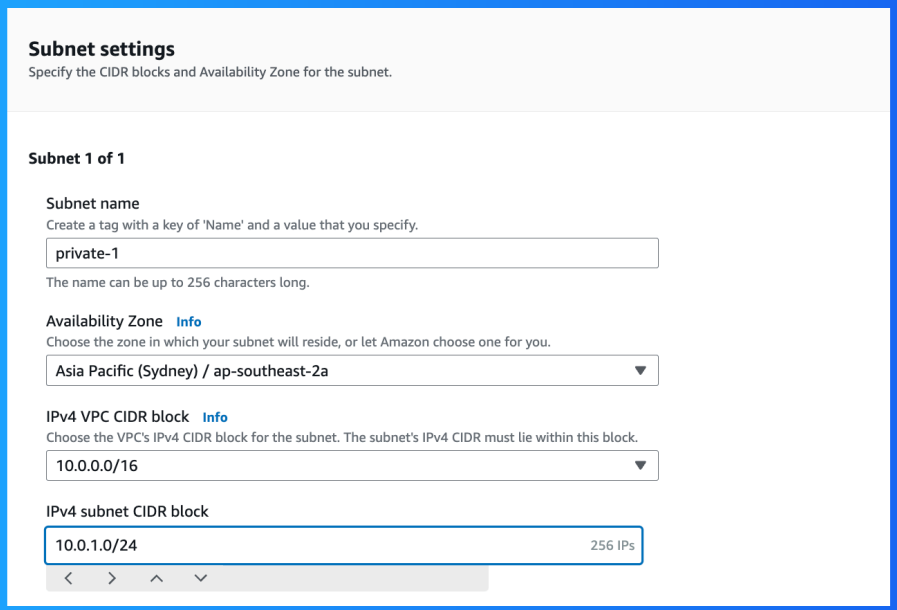
NextWork.org

Creating a Private Subnet

Juncheng Wang



Juncheng Wang
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC enables you to build a virtual network in the AWS cloud. You can define your own network space by controlling how your network and the Amazon EC2 resources inside your network are communicating with the internet.

How I used Amazon VPC in this project

I set up a private subnet with associated route table and network ACL.

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

Although setting up a route without an internet gateway would already prevent direct internet access to and from the subnet, setting up a dedicated network ACL is still a crucial practice to prevent internal traffic from public subnet.

This project took me...

1 hour

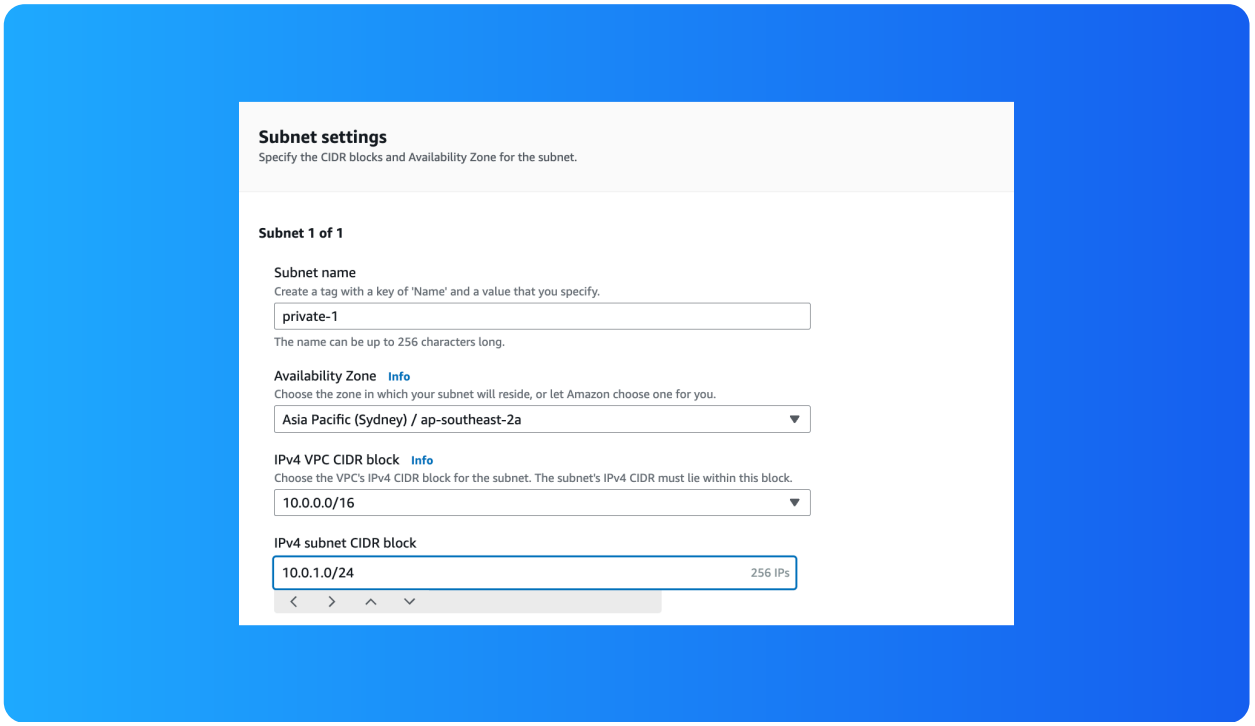
Juncheng Wang
NextWork Student

Private vs Public Subnets

The difference between public and private subnets is that public subnets are accessible by and can access the internet, while private subnets are completely isolated from the internet.

Having private subnets is useful because keeping resources away from the internet is very important for security when it contains confidential resources and data.

My private and public subnets cannot have the same IPv4 CIDR block (the same range of IP addresses). The CIDR block for every subnet must be unique and cannot overlap with another subnet.

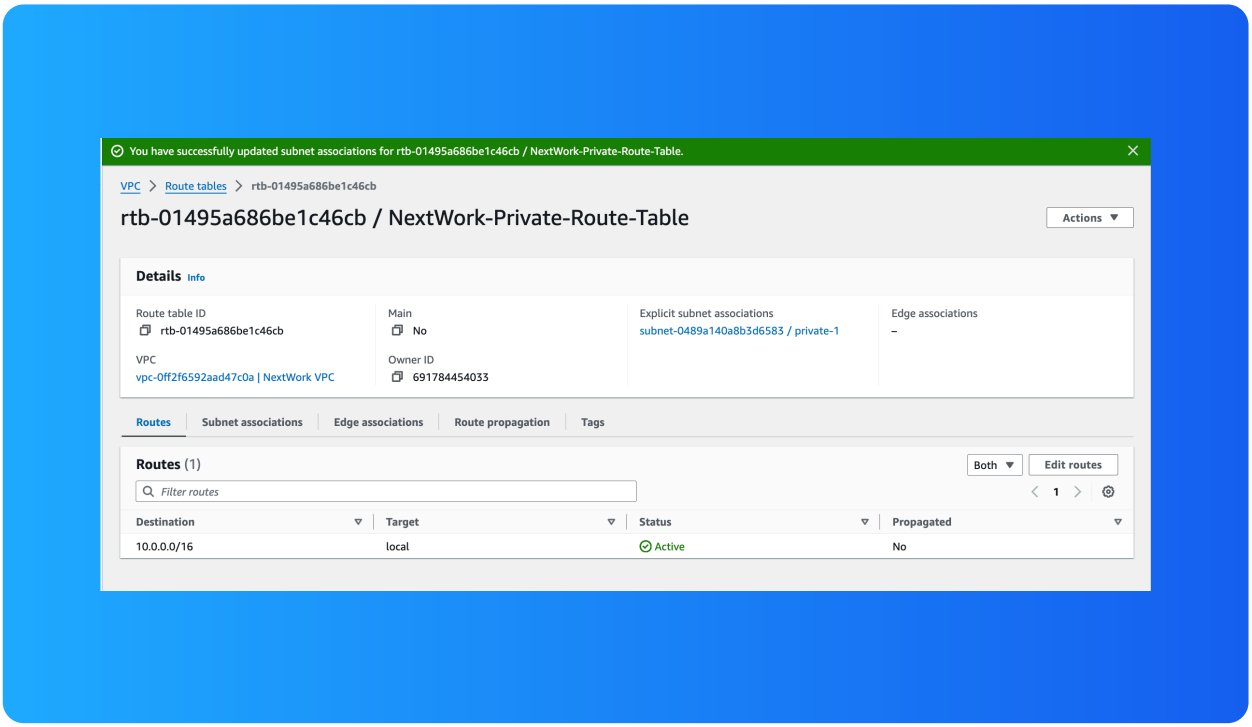


A dedicated route table

By default, my private subnet is associated with the default route table that AWS automatically created with my VPC.

I had to set up a new route table because my subnet can't have a route to an internet gateway. I need to make a new one to only allow the local target to make my subnet private.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows internal communication only i.e. with a destination of another resource within my VPC.



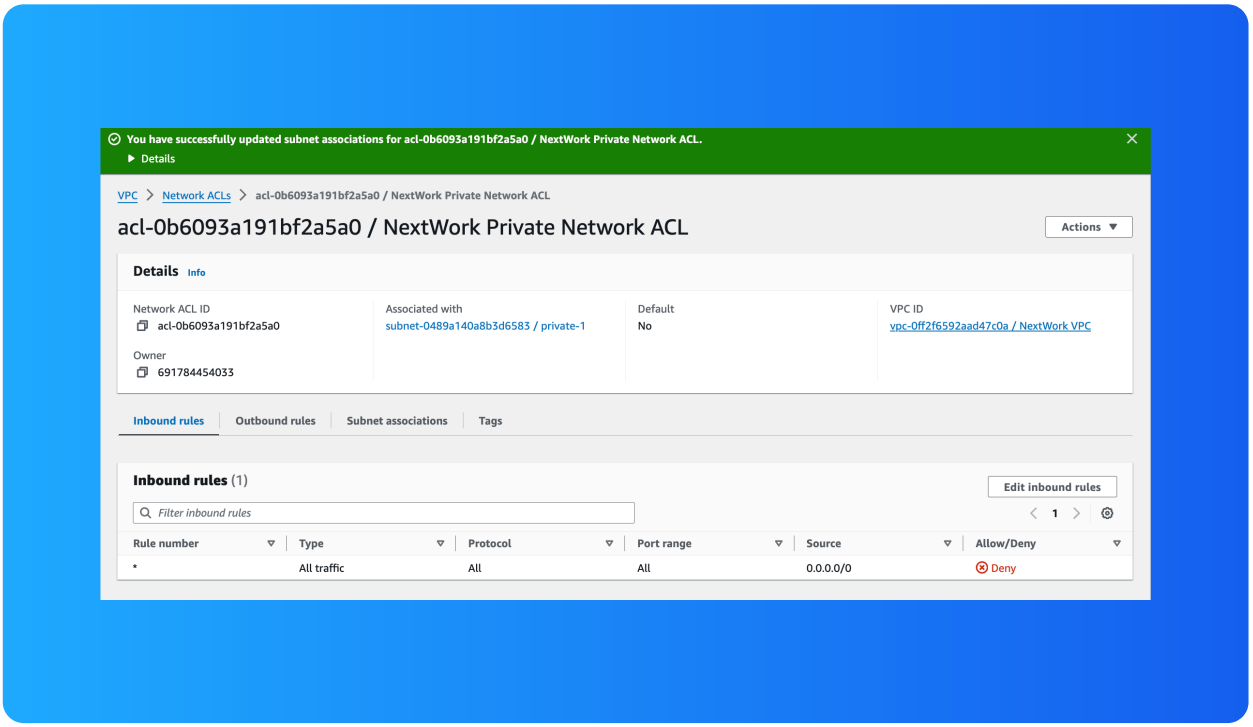
Juncheng Wang
NextWork Student

A new network ACL

By default, my private subnet is associated with the default network ACL that is set up for every VPC.

I setup a dedicated network ACL for my private subnet because a network ACL helps to prevent security breaches where traffic that has compromised my public subnet can get access to my private subnet if I have network ACL rules that allow all traffic.

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



Everyone should be in a job they love.

Check out nextwork.org for more projects