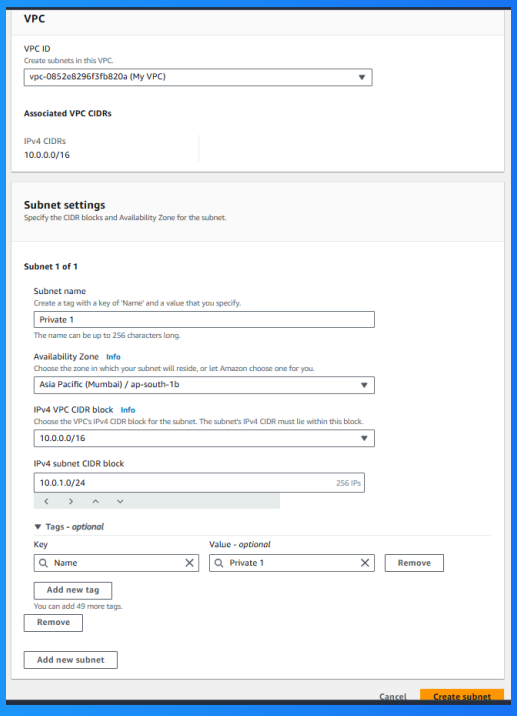
NextWork.org

Creating a Private Subnet

RAJARSHI VERMA



R
RAJARSHI VERMA
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) allows you to create a private, isolated section of the AWS cloud where you can launch AWS resources in a virtual network. It's useful for controlling network settings, enhancing security, and managing traffic.

How I used Amazon VPC in this project

In today's project I created a private subnet in case of keeping resources private like in case of database or sensitive data. Along with that I created private route table, private NACL.

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

It is quiet easy to make a private subnet and by default everything is pointing to open access to internet so it becomes necessary to check every aspect while setting up private subnet because you don't want anyone to sneak inside your machine.

This project took me...

It took me around 60 minutes to set everything from scratch that including creating VPC, public and private subnets, internet gateway, public and private routetable and public and private network acces control list.

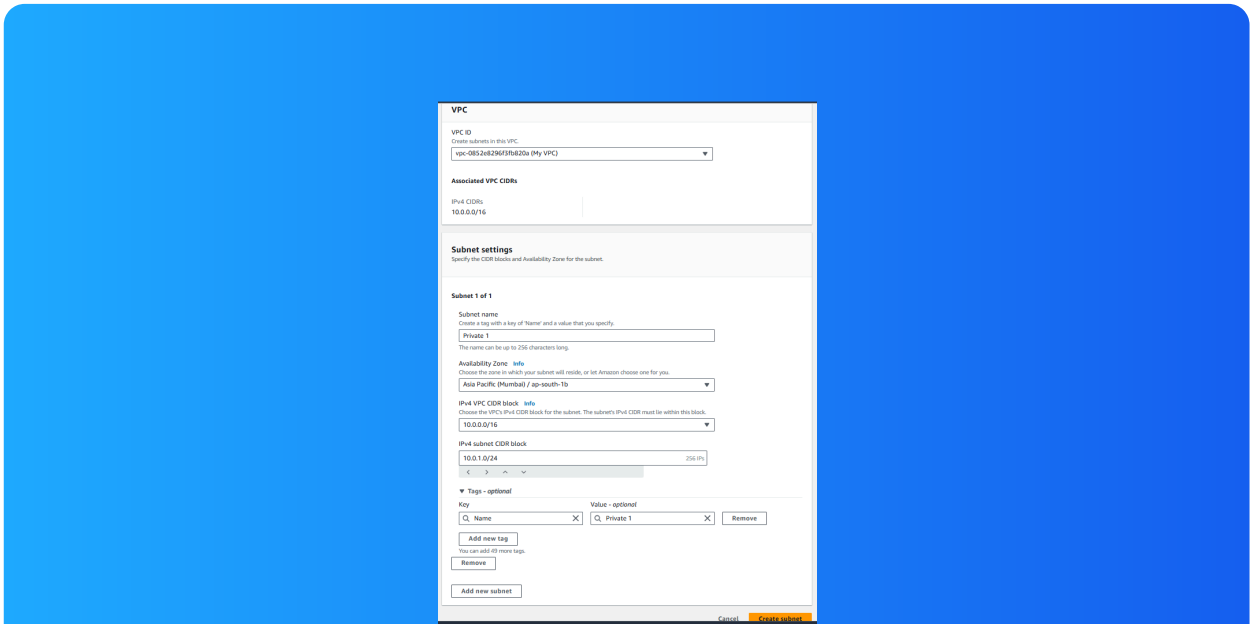
RAJARSHI VERMA
NextWork Student

Private vs Public Subnets

The difference between public and private subnets is that public subnets have direct access to the internet via an internet gateway, while private subnets do not. Private subnets are used for resources that should not be directly accessible.

Having private subsets are useful because there are always resources which do not require the direct access to internet and it is not best practice to place them in public subnet like database or any sensitive information.

My private and public subnets cannot have the same CIDR block. Each subnet in a VPC must have a unique CIDR block to avoid IP address conflicts and ensure proper routing of traffic within the network. For public-1 10.0.0.0/24 and for private 10.0.1.0

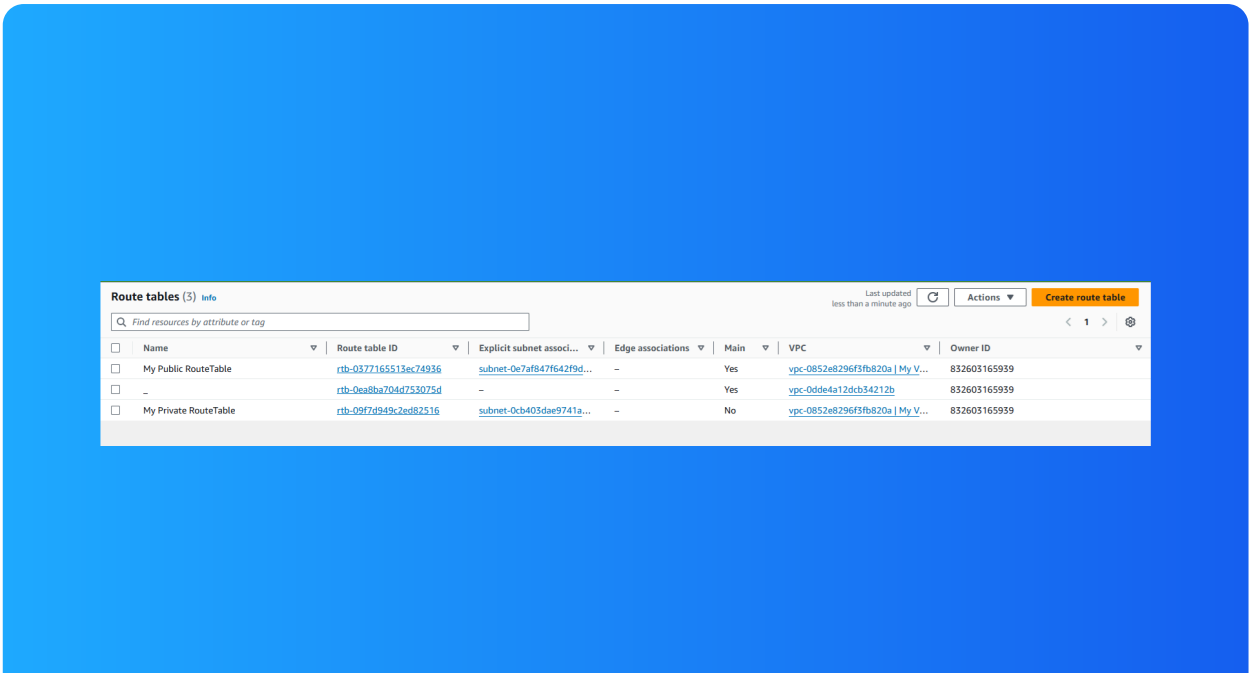


A dedicated route table

By default, my private subnet is associated with the main route table of the VPC. This route table does not have a route to an internet gateway, ensuring that the subnet remains private and isolated from direct internet access.

I had to set up a new route table because the default route table is associated with the public subnet and has a route to the internet gateway. To keep the private subnet isolated, it needs a separate route table without internet access.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows internal VPC traffic. This ensures that the subnet remains isolated from the internet while still enabling communication within the VPC.



R

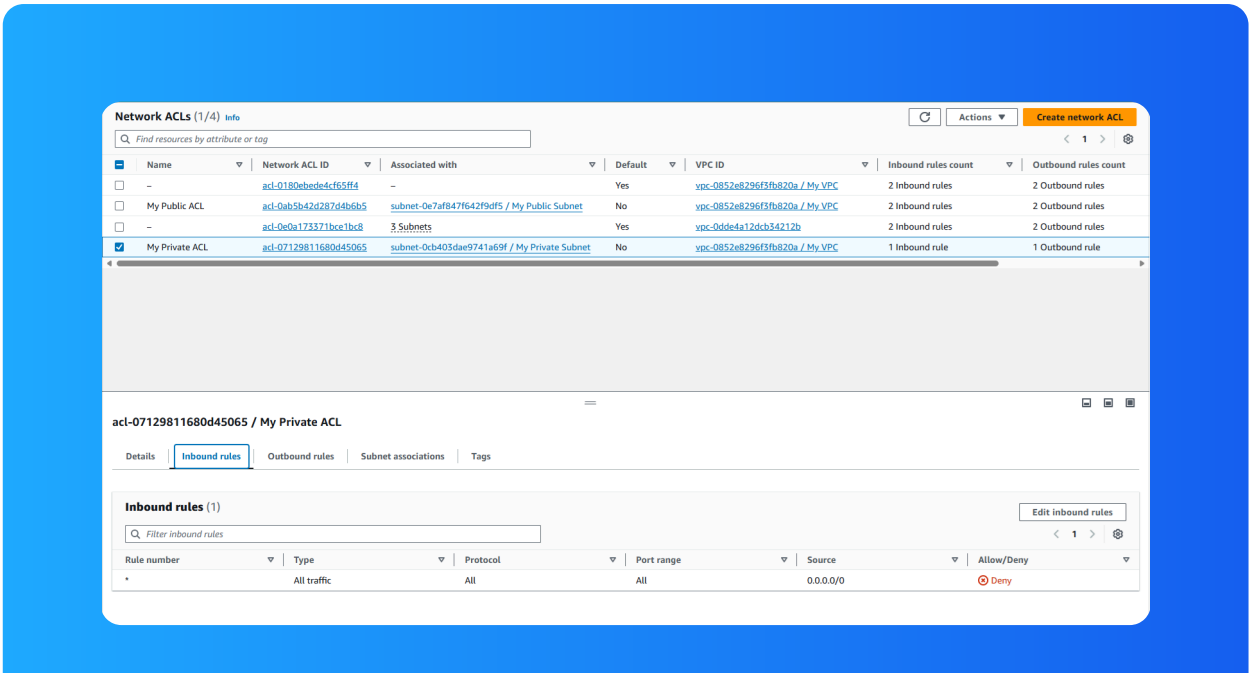
RAJARSHI VERMA
NextWork Student

A new network ACL

By default, my private subnet is associated with the default network ACL of the VPC. This default ACL allows all inbound and outbound traffic, which is why it's important to create a custom ACL to restrict traffic and enhance security.

I set up a dedicated network ACL for my private subnet because the default ACL allows all traffic, which poses security risks. A custom ACL restricts inbound and outbound traffic, enhancing the security of my private subnet.

My new network ACL has two simple rules - one inbound and one outbound rule. Both rules deny all traffic by default. Custom network ACLs start with denying all inbound and outbound traffic. We'll customize them later to allow specific traffic sources



Everyone should be in a job they love.

Check out nextwork.org for more projects