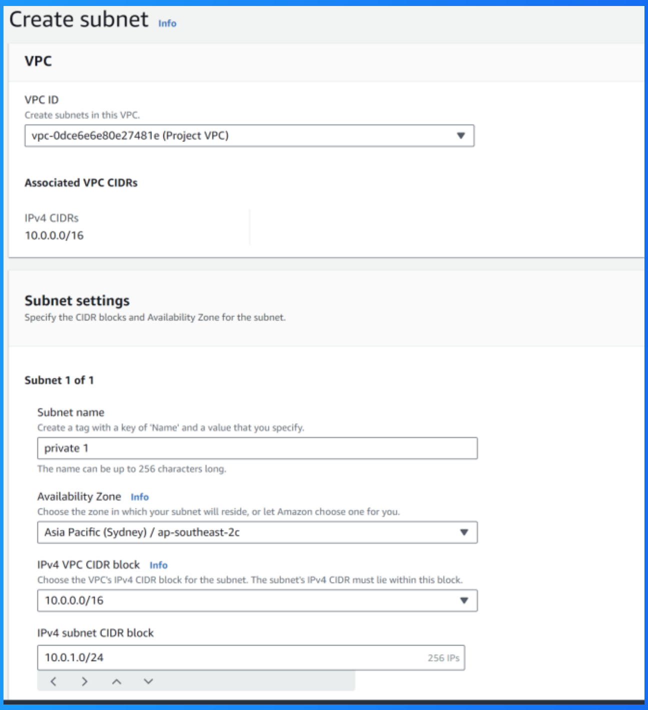
Creating a Private Subnet

V Prajit Venkatachalam

https://www.linkedin.com/in/prajit-venkatachalam-435b2a150/



Create subnet Info

VPC

VPC ID
Create subnets in this VPC.
vpc-0dce6e6e80e27481e (Project 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.
private 1
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.
Asia Pacific (Sydney) / ap-southeast-2c

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

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) exists within an AWS region and is used to build a private and secure connection for resources in the subnets. Through an internet gateway, these resources and users can access the internet to communicate with each other.

How I used Amazon VPC in this project

In today's project, I used my Amazon VPC to build the private subnet, including a private route table and a private network ACL.

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

One thing I did not expect in this project was learning the differences between public and private route tables, as well as the differences in inbound and outbound rules between private and public network ACLs.

This project took me...

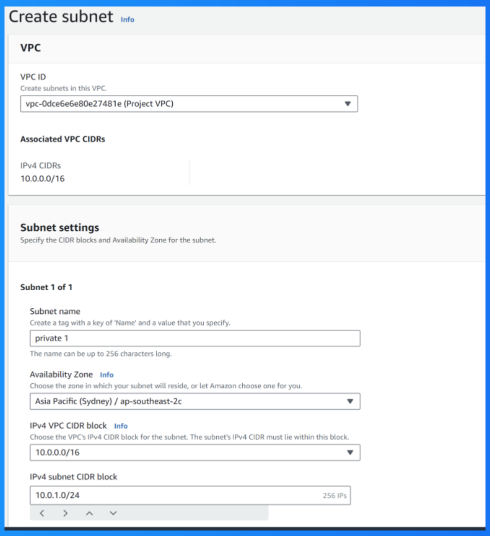
This project took me one and a half hours to complete, including writing the report.

Private vs Public Subnets

The differences between public and private subnets is that public subnets allowboth resources in VPC and users to access each other using internet via an internet gateway, while private subnets are completely isolated from the internet by default.

Having private subnets is useful because keeping resources away from the internet is crucial for ensuring the security of confidential resources and data.

My private and public subnets cannot have the same CIDR block, meaning they cannot share the same range of IP addresses. The CIDR block for each subnet must be unique and cannot overlap with any other subnet.



Create subnet Info

VPC

VPC ID
Create subnets in this VPC.
vpc-0dce6e6e80e27481e (Project 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.
private 1
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.
Asia Pacific (Sydney) / ap-southeast-2c

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

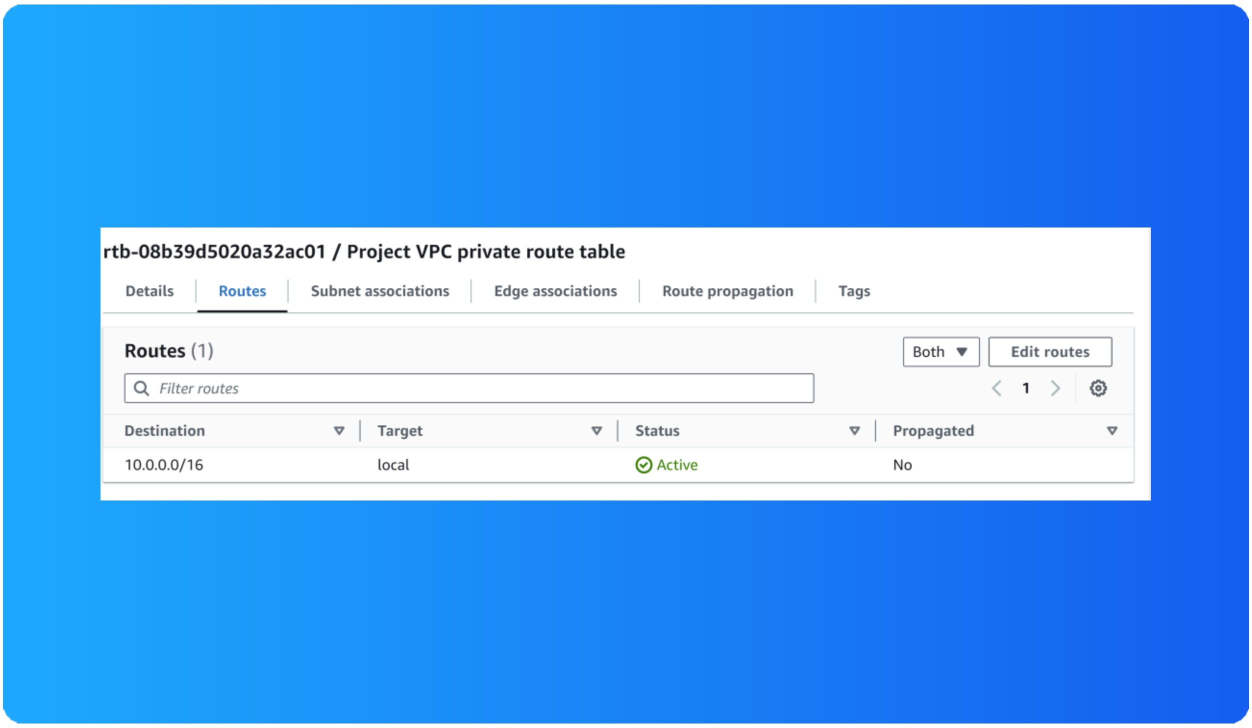
IPv4 subnet CIDR block
10.0.1.0/24 256 IPs

A dedicated route table

By default, my private subnet is associated with the default route table, which routes traffic to an internet gateway.

I had to set up a new route table because my private subnet should not have a route to an internet gateway.

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



rtb-08b39d5020a32ac01 / Project VPC private route table

Routes (1)

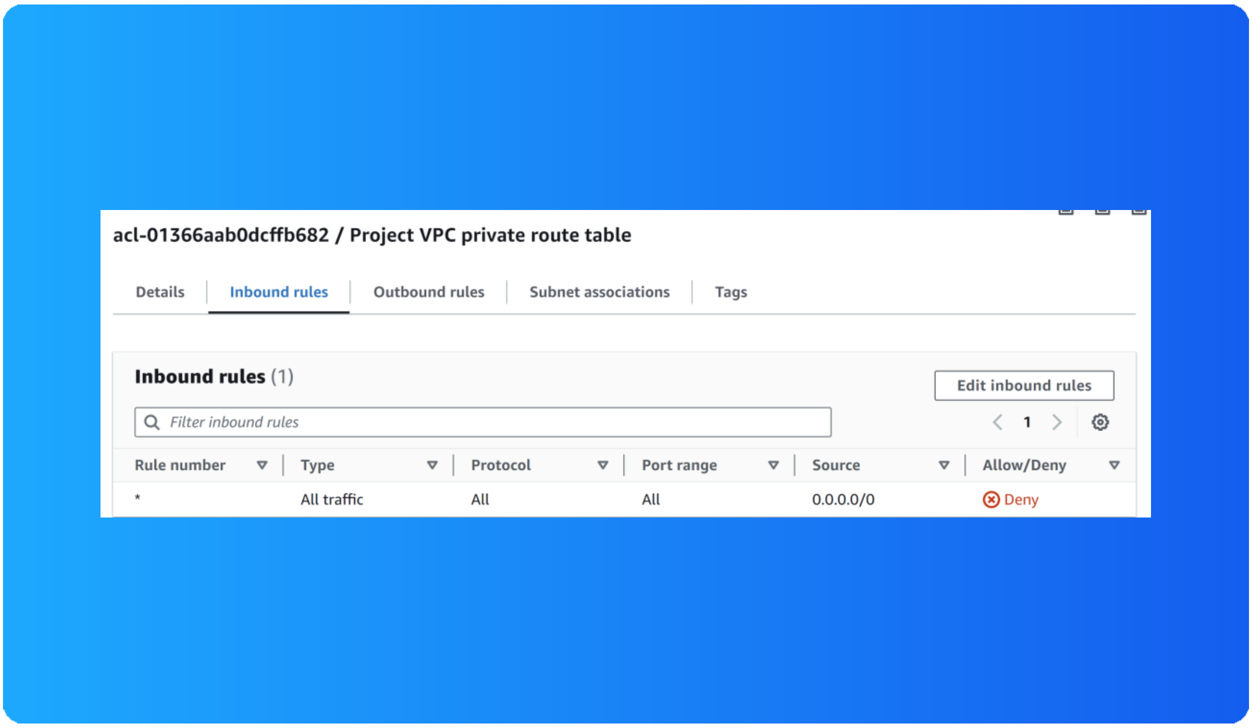
Destination	Target	Status	Propagated
10.0.0.0/16	local	✓ Active	No

A new network ACL

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

I set up a dedicated (Network) ACL for my private subnet because a network ACL becomes crucial in the event of security breaches. Traffic that compromises my public subnet could potentially access the private subnet if the NACL rules allow traffic.

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



acl-01366aab0dcffb682 / Project VPC private route table

Inbound rules (1)

Rule number	Type	Protocol	Port range	Source	Allow/Deny
*	All traffic	All	All	0.0.0.0/0	⊗ Deny

Everyone should be in a job they love.

Check out nextwork.org for more projects