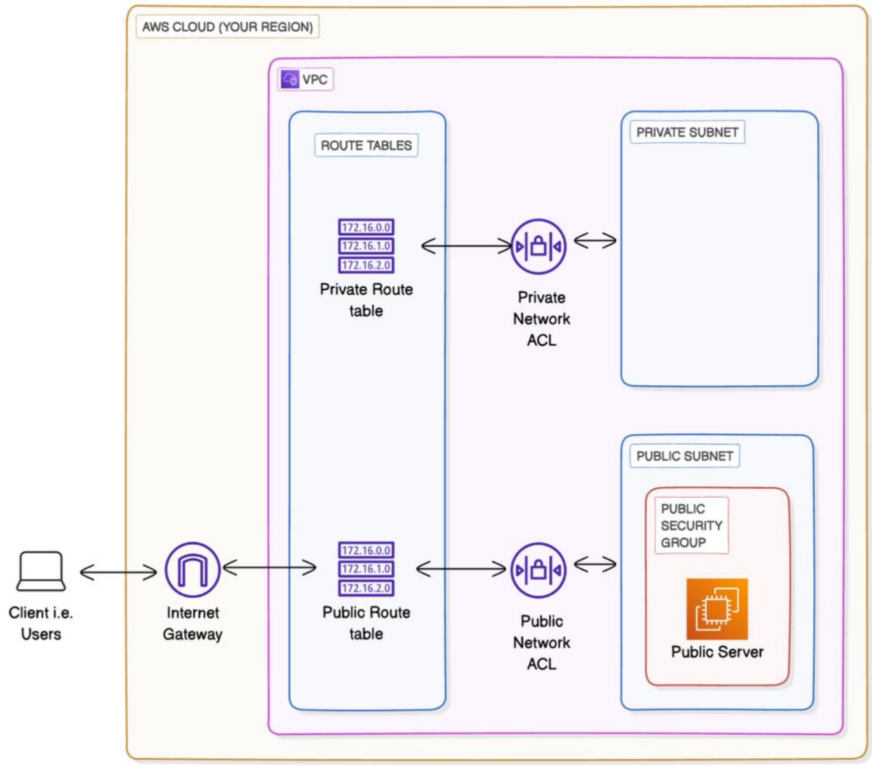
Creating a Private Subnet



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) allows you to create a private network within AWS, offering control over IP ranges, subnets, and security settings. It’s useful for securely managing resources and controlling connectivity and network isolation.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create a secure, isolated network. I set up public and private subnets, configured route tables for traffic flow, and applied network ACLs to control access, ensuring secure and efficient communication.

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

One thing I didn’t expect in this project was the level of detail required in configuring network ACLs and route tables. The need to carefully plan and customize these settings for security and efficient communication took more time than anticipated.

This project took me...

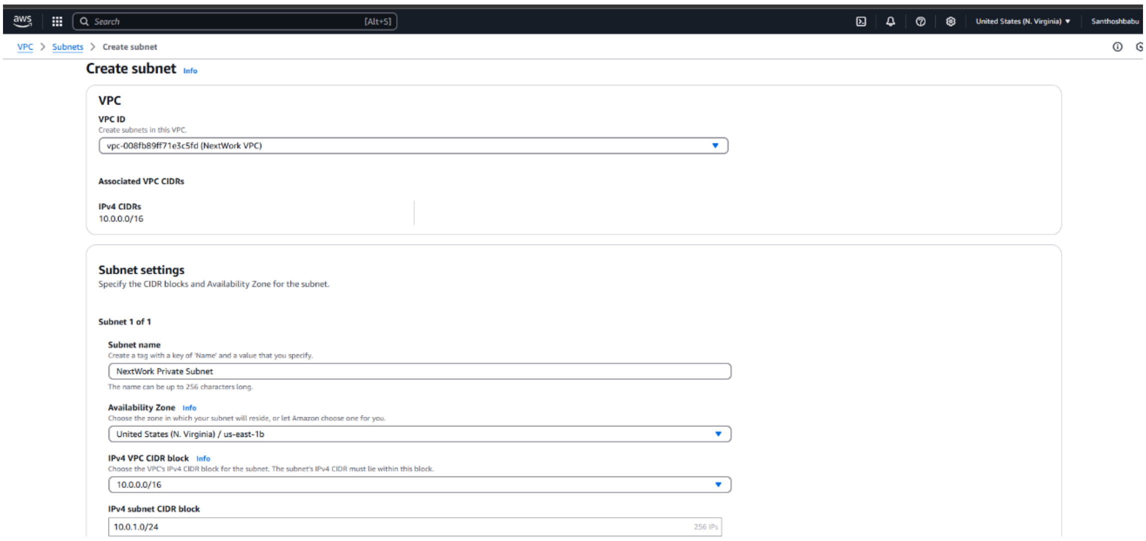
This project took an hour to complete. The most time-consuming tasks were setting up the VPC, configuring subnets, and adjusting route tables. Fine-tuning security settings and ensuring proper isolation and access control required extra attention.

Private vs Public Subnets

The difference between public and private subnets is that public subnets have direct internet access via an Internet Gateway, while private subnets don’t. They rely on a NAT Gateway or VPN for external communication, offering more security.

Having private subnets are useful because they add security by isolating sensitive resources, like databases and application servers, from direct internet access. This reduces exposure to threats while still allowing controlled communication.

My private and public subnets cannot have the same internet access. Public subnets can access the internet directly via an Internet Gateway, whereas private subnets rely on a NAT Gateway or VPN for external communication, ensuring more security.



Create subnet

VPC

VPC ID
Create subnets in this VPC.
vpc-008fb89ff71e3c5fd (NextWork 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.
NextWork Private Subnet
The name can be up to 256 characters long.

Availability Zone
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
United States (N. Virginia) / us-east-1b

IPv4 VPC CIDR block
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

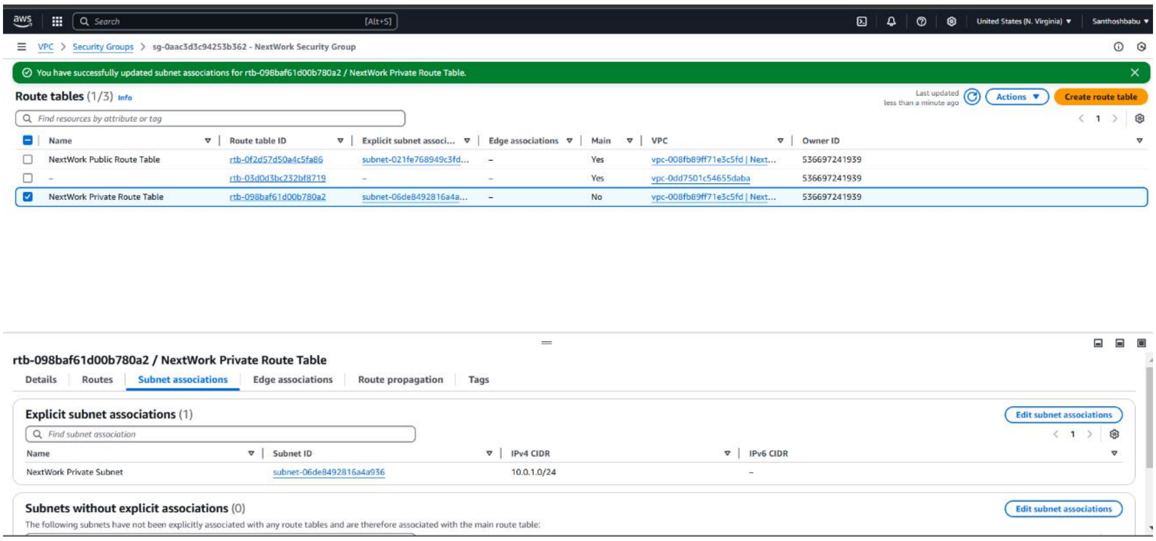
IPv4 subnet CIDR block
10.0.1.0/24 256 IPs

A dedicated route table

By default, my private subnet is associated with the main route table. This table includes routes for local VPC traffic but does not provide internet access. To enable external communication, a NAT Gateway or VPN must be added to the route table.

I had to set up a new route table because I needed to customize routing for specific subnets. This allows me to direct traffic from private subnets through a NAT Gateway for internet access while keeping public and private subnet traffic separate.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows traffic within the VPC. Outbound traffic is routed through a NAT Gateway to access the internet, while inbound traffic is restricted for security.



You have successfully updated subnet associations for rtb-098baf61d00b780a2 / NextWork Private Route Table.

Route tables (1/3)

	Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC	Owner ID
□	NextWork Public Route Table	rtb-0f2d57d50a4c5fa86	subnet-021fe768949c3fd...	–	Yes	vpc-008fb89ff71e3c5fd | Next...	536697241939
□	–	rtb-03d0d3bc232bf8719	–	–	Yes	vpc-0dd7501c54655daba	536697241939
☑	NextWork Private Route Table	rtb-098baf61d00b780a2	subnet-06de8492816a4a...	–	No	vpc-008fb89ff71e3c5fd | Next...	536697241939

rtb-098baf61d00b780a2 / NextWork Private Route Table

Explicit subnet associations (1)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
NextWork Private Subnet	subnet-06de8492816a4a936	10.0.1.0/24	–

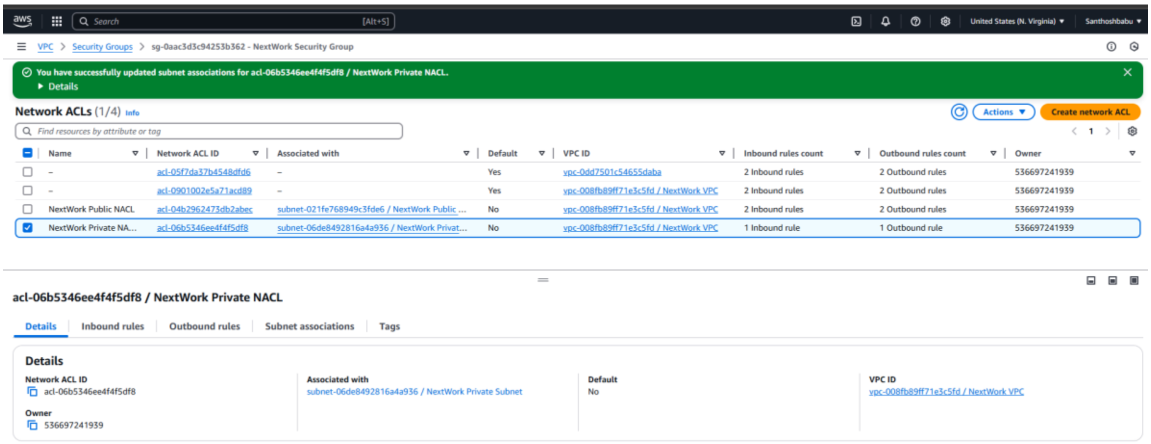
Subnets without explicit associations (0)
The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

A new network ACL

By default, my private subnet is associated with the default Network ACL (NACL). This NACL allows all inbound and outbound traffic. However, it can be customized to restrict or allow specific types of traffic for better security and control.

I set up a dedicated network ACL for my private subnet because I wanted better control over inbound and outbound traffic. It allows me to apply specific security rules, restrict unnecessary access, and protect sensitive resources within the subnet.

My new network ACL has two simple rules – one inbound rule that allows traffic from trusted sources within the VPC, and one outbound rule that allows traffic to the internet via a NAT Gateway, ensuring secure communication while limiting exposure.


aws
Search [Alt+S]
United States (N. Virginia) ▾
Santhoshbabu ▾

VPC > Security Groups > sg-0aac3d3c94253b362 - NextWork Security Group

You have successfully updated subnet associations for acl-06b5346ee4f4f5df8 / NextWork Private NACL.
▸ Details

Network ACLs (1/4) Info

Actions ▾
Create network ACL
Find resources by attribute or tag

	Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count	Outbound rules count	Owner
□	–	acl-05f7da37b4548dfd6	–	Yes	vpc-0dd7501c54655daba	2 Inbound rules	2 Outbound rules	536697241939
□	–	acl-0901002e5a71acd89	–	Yes	vpc-008fb89ff71e3c5fd / NextWork VPC	2 Inbound rules	2 Outbound rules	536697241939
□	NextWork Public NACL	acl-04b2962473db2abec	subnet-021fe768949c3fde6 / NextWork Public ...	No	vpc-008fb89ff71e3c5fd / NextWork VPC	2 Inbound rules	2 Outbound rules	536697241939
☑	NextWork Private NA...	acl-06b5346ee4f4f5df8	subnet-06de8492816a4a936 / NextWork Privat...	No	vpc-008fb89ff71e3c5fd / NextWork VPC	1 Inbound rule	1 Outbound rule	536697241939

acl-06b5346ee4f4f5df8 / NextWork Private NACL

Details

Network ACL ID: acl-06b5346ee4f4f5df8
Associated with: subnet-06de8492816a4a936 / NextWork Private Subnet
Default: No
VPC ID: vpc-008fb89ff71e3c5fd / NextWork VPC
Owner: 536697241939

Today we've learnt how to:

- 🚷 **Create a private subnet:** You created a new subnet and set its CIDR block to avoid an overlap with your public subnet.
- 🚧 **Create a private route table:** You also made this subnet private by assigning it to a dedicated route table that doesn't route traffic to an internet gateway!
- 🚔 **Create a private network ACL:** Then, you set up custom network ACLs to control inbound and outbound traffic for this private subnet - denying all traffic by default.