



nextwork.org

Creating a Private Subnet



mohammed Furqanuddin

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.

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.

The name can be up to 256 characters long.

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.

IPv4 subnet CIDR block
 256 IPs
[Add more](#)

Tags - optional
Key Value - optional [Remove](#)



mohammed Furqanuddin

NextWork Student

nextwork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is a secure, isolated network in AWS where you launch and manage your resources. It's useful because it gives full control over networking, security, and internet access for your applications.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create a custom network where I set up public and private subnets, route tables, and a network ACL to securely manage resources and control their internet access.

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

One thing I didn't expect in this project was the need to create a separate route table and network ACL for the private subnet to keep it fully isolated from the internet.

This project took me...

This project took me around 1 hour to complete, including setting up the VPC, creating public and private subnets, configuring route tables, and setting up the network ACL.

mohammed Furqanuddin

NextWork Student

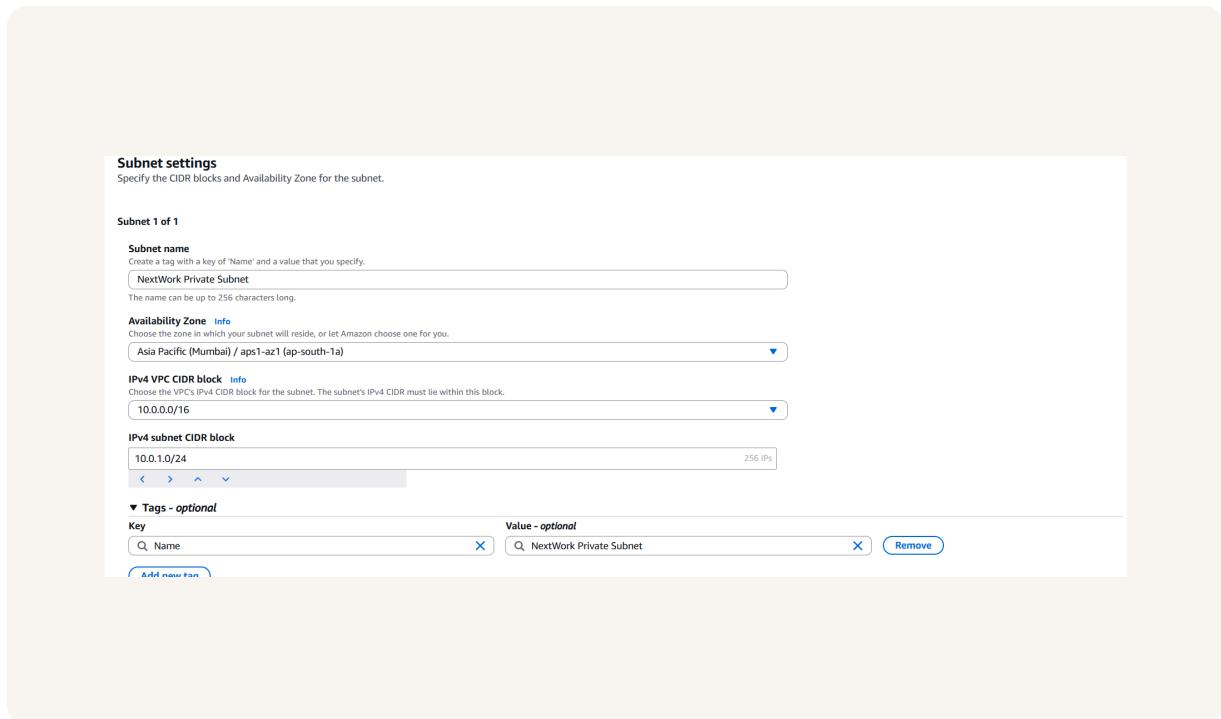
nextwork.org

Private vs Public Subnets

A public subnet is connected to the internet through an Internet Gateway, so its resources (like web servers) can be accessed publicly. A private subnet has no direct internet access, so its resources stay isolated and secure within the VPC.

Private subnets exist to keep sensitive resources (like databases) hidden from the internet, making them safer and more secure.

Your private and public subnets can't share the same route table they each need their own, since public subnets connect to the internet while private subnets stay isolated.



The screenshot shows the 'Subnet settings' configuration page for a VPC. The page is titled 'Subnet settings' and includes a note: 'Specify the CIDR blocks and Availability Zone for the subnet.' It displays the configuration for 'Subnet 1 of 1'.

Subnet name: NextWork Private Subnet

Availability Zone: Asia Pacific (Mumbai) / aps1-az1 (ap-south-1a)

IPv4 VPC CIDR block: 10.0.0.0/16

IPv4 subnet CIDR block: 10.0.1.0/24

Tags - optional:

Key	Value - optional
Name	NextWork Private Subnet

[Add new tag](#)

mohammed Furqanuddin

NextWork Student

nextwork.org

A dedicated route table

By default, Our private subnet is associated with the main (default) route table of the VPC in this case, the NextWork route table we renamed earlier.

We're setting up a new route table so our private subnet stays private.

Our private subnet's dedicated route table only has one local route that allows traffic within the VPC,It does not have a route to the Internet Gateway,so resources inside the private subnet can only talk to other resorces in the VPC,not the internet

The screenshot shows the AWS Route Tables page with the following details:

Route tables (3) [Info](#)

Last updated: 1 minute ago | Actions | [Create route table](#)

Find route tables by attribute or tag

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
-	rtb-0f37b166da93af1a7	-	-	Yes	vpc-0797aca4207a4fe8f
NextWork Public Route Table	rtb-0247db27ede02ebb1	subnet-0cf3c511a68c96c...	-	Yes	vpc-0243615189a967967 Ne
NextWork Private Route Table	rtb-06c615a0ecd6c160a	subnet-004e7c115fef340...	-	No	vpc-0243615189a967967 Ne

mohammed Furqanuddin

NextWork Student

nextwork.org

A new network ACL

By default, our private subnet is associated with the default network ACL that AWS automatically creates with our VPC.

I set up a dedicated network ACL for my private subnet because I need tighter security rules at the subnet level, ensuring sensitive resources (like databases) are protected from unwanted traffic.

My new network ACL has one inbound and one outbound rule that deny all traffic (all protocols, all ports) from anywhere (0.0.0.0/0).

The screenshot shows the AWS Network ACL Inbound Rules configuration page for the network ACL 'acl-0a8df407e08a2aaef / NextWork Private NACL'. The 'Inbound rules' tab is selected. There is one rule listed:

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



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

