



nextwork.org

Creating a Private Subnet



MHM Aslam

The screenshot shows the AWS VPC Subnets creation interface. At the top, there's a breadcrumb navigation: [VPC](#) > [Subnets](#) > Create subnet. Below this, a sidebar titled "Associated VPC CIDRs" shows an IPv4 CIDR block of 10.0.0.0/16. The main content area is titled "Subnet settings" with the sub-instruction "Specify the CIDR blocks and Availability Zone for the subnet." It displays "Subnet 1 of 1" with a "Subnet name" field containing "NextWork Private Subnet". The "Availability Zone" dropdown is set to "Asia Pacific (Mumbai) / ap-south-1b". Under "IPv4 VPC CIDR block", it says "Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block." A dropdown menu shows "10.0.0.0/16". The "IPv4 subnet CIDR block" field contains "10.0.1.0/24" with a note "256 IPs".

A circular profile picture of a young man with dark hair, wearing a brown long-sleeved shirt and dark pants, sitting outdoors with a green landscape in the background.

MHM Aslam

NextWork Student

nextwork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is a virtual network dedicated to your AWS account where you can launch AWS resources in an isolated environment. It's useful because it gives you full control over your network settings, security, and traffic flow.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to isolate the private subnet from the internet and make the public subnet accessible by attaching an internet gateway, allowing external access only to the resources meant to be publicly available.

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

One thing I didn't expect in this project was how important route tables and network ACLs are in controlling access—small misconfigurations can completely block traffic or expose resources unintentionally.



MHM Aslam

NextWork Student

nextwork.org

This project took me...

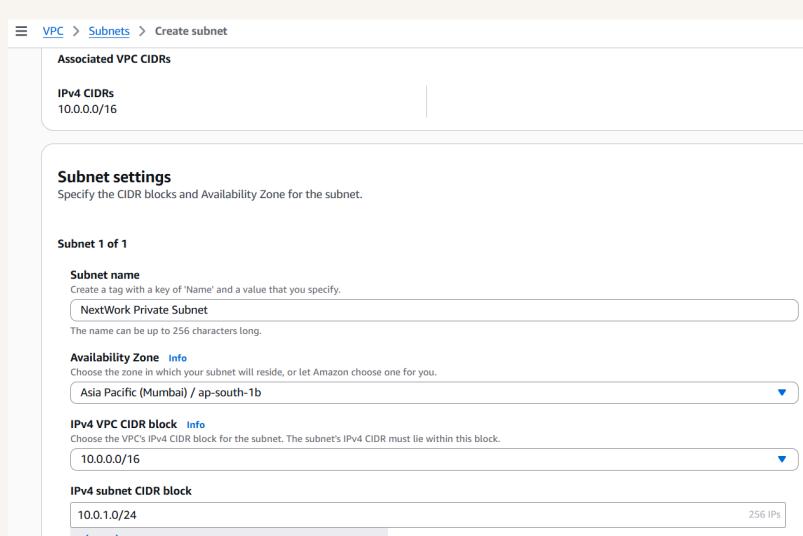
Another AWS Service done! This project took me around 1 hour since I had already learned about public subnet settings earlier and only needed to focus on configuring and securing the private subnet.

Private vs Public Subnets

The difference between public and private subnets is that public subnets are accessible from the internet, while private subnets are not accessible from the internet.

Having private subnets are useful because they enhance security by isolating sensitive resources from direct internet access, reducing the attack surface and allowing controlled communication through secure channels.

My private and public subnets cannot have the same IP address range (CIDR block), as each subnet in a VPC must have a unique range to avoid routing conflicts.



A circular profile picture of a young man with dark hair, wearing a brown long-sleeved shirt and dark pants, sitting outdoors with a body of water in the background.

A dedicated route table

By default, my private subnet is associated with the main route table, which does not have a route to an internet gateway.

I had to set up a new route table because I needed to control traffic flow differently, such as allowing internet access for a public subnet or isolating a private subnet from external networks.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows internal VPC traffic, enabling communication between subnets within the VPC but not with the internet.



MHM Aslam
NextWork Student

nextwork.org

rtb-071ecc61dc5360450 / NextWork Private Route Table

[Details](#) | [Routes](#) | [Subnet associations](#) | [Edge associations](#) | [Route propagation](#) | [Tags](#)

Details		Explicit subnet associations	Edge associations
Route table ID	rtb-071ecc61dc5360450	Main <input checked="" type="checkbox"/> No	-
VPC	vpc-08ab0049ef1b4e81a NextWork VPC	Owner ID 799227258538	subnet-0476b018275b8bd13 / NextWork Private Subnet

A circular profile picture of a young man with dark hair, wearing a brown long-sleeved shirt and dark pants, sitting outdoors with a body of water and trees in the background.

MHM Aslam
NextWork Student

nextwork.org

A new network ACL

By default, my private subnet is associated with the default Network ACL (NACL) of the VPC, which allows all inbound and outbound traffic.

I set up a dedicated network ACL for my private subnet to control inbound and outbound traffic more strictly, improving security by limiting access to trusted sources and blocking unwanted traffic to protect sensitive resources.

My new network ACL has two simple rules – it denies all inbound and outbound traffic to completely block any network communication, ensuring maximum isolation and security for the private subnet.



MHM Aslam
NextWork Student

nextwork.org

The screenshot shows a web-based interface for managing Network Access Control Lists (NACLs). The title bar indicates the specific NACL: "acl-0859527eb851df999 / NextWork Private NACL". Below the title, there are tabs for "Details", "Inbound rules" (which is currently selected), "Outbound rules", "Subnet associations", and "Tags".

The "Inbound rules" section displays one rule:

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

There are buttons for "Edit inbound rules" and navigation controls (back, forward, search, etc.).



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

