



Creating a Private Subnet

SH

shravanirg03@gmail.com

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 Info

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

Asia Pacific (Mumbai) / ap-south-1b



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.

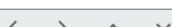
10.0.0.0/16



IPv4 subnet CIDR block

10.0.1.0/24

256 IPs



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC allows you to create an isolated, secure network in the AWS cloud, giving you control over IP ranges, subnets, etc. It is useful as it enhances security, and lets you scale resources while ensuring privacy and flexibility.

How I used Amazon VPC in this project

I set up public and private subnets in Amazon VPC. I created a private subnet with a dedicated route table and private network ACL. I also configured a public subnet with an Internet Gateway and necessary settings to manage traffic & ensure security.

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

This project provided valuable insights and deeper understanding of various networking concepts.

This project took me...

The entire process took me approximately 60 minutes.

Private vs Public Subnets

The difference between public and private subnets is that public subnets are accessible by and can access the internet, while private subnets are completely isolated from the internet by default.

Having private subnets are useful because they protect sensitive resources (like databases) from direct internet exposure, ensuring enhanced security by limiting access to internal traffic.

My private and public subnets cannot have the same IPv4 CIDR block i.e. the same range of IP addresses. The CIDR block for every subnet must be unique and cannot overlap with another 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 [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
Asia Pacific (Mumbai) / ap-south-1b

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
< > ^ v

A dedicated route table

By default, my private subnet is associated with the default route table i.e. a route table that has a route to an internet gateway.

I had to set up a new route table because my subnet cannot have a route to an internet gateway. Thus, I created a custom routing configuration for the private subnet.

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

rtb-0b3da3def7f05cf68 / NextWork Private Route Table					
Details	Routes	Subnet associations	Edge associations	Route propagation	Tags
Routes (1)					
<input type="text"/> Filter routes	Both	Edit routes			
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's 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 an event of security breach where traffic that has compromised a public subnet can get access to a private subnet if network ACL rules allow all traffic.

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

The screenshot shows the AWS Network ACL management interface. The title bar reads "acl-0960f5f0cd4f59cea / NextWork Private NACL". Below the title, there are tabs for "Details", "Inbound rules" (which is selected), "Outbound rules", "Subnet associations", and "Tags".

The "Inbound rules (1)" section displays a single rule:

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

On the right side of the "Inbound rules" section, there are buttons for "Edit inbound rules", navigation arrows, and a refresh icon.



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for
more projects

