



Creating a Private Subnet



Emmanuel Enalpe III

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.

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
[Edit](#) [Delete](#)

Tags - optional

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="NextWork Private Subnet"/>

[Add new tag](#)
You can add 49 more tags.
[Remove](#)

[Add new subnet](#)



Emmanuel Enalpe III

NextWork Student

NextWork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC allows you to create a private, isolated network within AWS. It lets you control network resources, IP address ranges, and security, offering better control over traffic and enhancing security for your cloud resources.

How I used Amazon VPC in this project

I used Amazon VPC to create a secure network environment, defining subnets, route tables, and internet gateways for proper traffic flow. This ensured secure communication between instances while isolating them from the public internet.

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

One thing I didn't expect in the VPC project was how crucial the proper configuration of route tables and security groups is for traffic flow. It's easy to overlook these details, but they play a vital role in ensuring the network works smoothly.

This project took me...

It took me less than an hour to complete this AWS service project.



Private vs Public Subnets

The difference between public and private subnets is that public subnets have access to the internet via an Internet Gateway, while private subnets are isolated from direct internet access, often using a NAT Gateway for outbound traffic.

Having private subnets are useful because they enhance security by isolating resources from the internet, allowing only internal communication or controlled access via NAT gateways, VPNs, or bastion hosts, thus protecting sensitive data and systems.

My private and public subnets cannot have the same route table configurations, as public subnets require a route to an internet gateway, while private subnets route traffic through a NAT gateway or NAT instance for internet access.

The screenshot shows the 'Subnet settings' configuration page for a subnet named 'NextWork Private Subnet'. The subnet is associated with the 'Asia Pacific (Singapore) / ap-southeast-1b' availability zone and has an IPv4 CIDR block of '10.0.0.0/16'. The IPv4 subnet CIDR block is set to '10.0.0.0/24'. There are no tags added to this subnet.

Setting	Value
Subnet name	NextWork Private Subnet
Availability Zone	Asia Pacific (Singapore) / ap-southeast-1b
IPv4 VPC CIDR block	10.0.0.0/16
IPv4 subnet CIDR block	10.0.0.0/24
Tags - optional	None

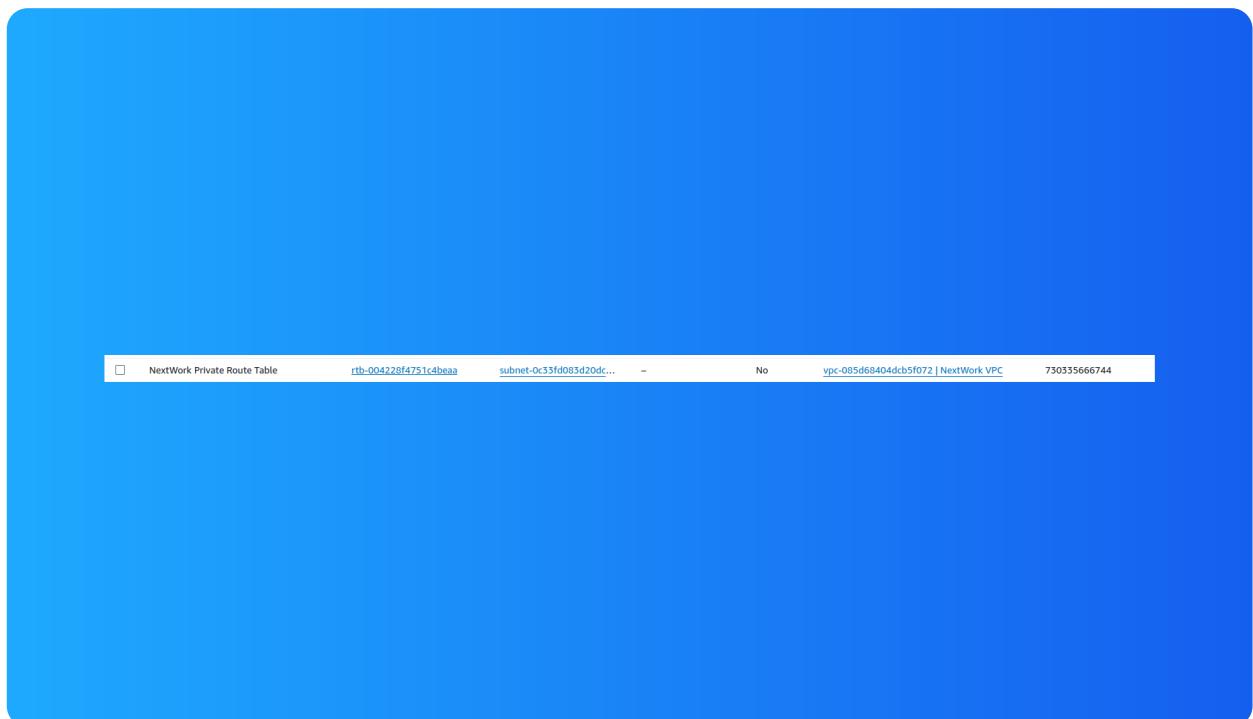


A dedicated route table

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

I had to set up a new route table because I needed to customize the traffic flow for specific subnets in my VPC, ensuring proper routing for internet access, private connections, or specific peering arrangements.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows local traffic within the VPC. It does not route traffic to the internet or other external networks unless connected to a NAT gateway.





A new network ACL

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

I set up a dedicated network ACL for my private subnet because it provides granular control over inbound and outbound traffic, enhances security by isolating the subnet, and ensures compliance with specific access and filtering requirements.

My new network ACL has two simple rules – one inbound rule denying all traffic and one outbound rule denying all traffic. These rules effectively block both incoming and outgoing communication for enhanced security.

The screenshot shows the AWS Network ACL Inbound Rules configuration page. At the top, there are tabs for Details, Inbound rules (which is selected), Outbound rules, Subnet associations, and Tags. Below the tabs, the title 'Inbound rules (1)' is displayed. A search bar labeled 'Filter inbound rules' is present. A table lists the single rule: Rule number * (All traffic), Type All, Protocol All, Port range All, Source 0.0.0.0/0, Allow/Deny Deny. To the right of the table is a button labeled 'Edit inbound rules' with a value of 1. The entire screenshot is overlaid with a large blue rectangular shape.



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for
more projects

