



# Creating a Private Subnet



Mohamed Galole

☰ [VPC](#) > [Subnets](#) > Create 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**

255 IPs

< > ^ v

▼ Tags - optional



# Introducing Today's Project!

## What is Amazon VPC?

Amazon VPC is a Virtual Private Cloud that lets you create and manage your own isolated network within the AWS cloud. It is useful because it gives you full control over your networking environment.

## How I used Amazon VPC in this project

In today's project, I used Amazon VPC to set up public and private subnets, configured route tables and a network ACL, and defined how traffic flows, ensuring the private subnet stays protected from direct internet access.

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

One thing I didn't expect in this project is how many interconnected components like route tables, gateways, and NACLs are required to make a subnet truly private. It showed me how important proper configuration and associations are for securing VPC.



**Mohamed Galole**

NextWork Student

[nextwork.org](https://nextwork.org)

This project took me...

This project took me one hour to complete.



## Private vs Public Subnets

The difference between public and private subnets is that public subnet has a route to the Internet Gateway, allowing resources to access and be accessed from the internet. A private subnet has no direct internet route, keeping resources isolated.

Having private subnets are useful because it keeps sensitive resources isolated from the internet, reducing security risks. They ensure critical systems like databases or internal servers are accessible only within the VPC.

My private and public subnets cannot have the same CIDR block. Each subnet in a VPC must have a unique, non-overlapping CIDR block so AWS can correctly route traffic between them within the VPC.



☰ [VPC](#) > [Subnets](#) > Create 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.

United States (N. Virginia) / use1-az2 (us-east-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

▼ Tags - optional

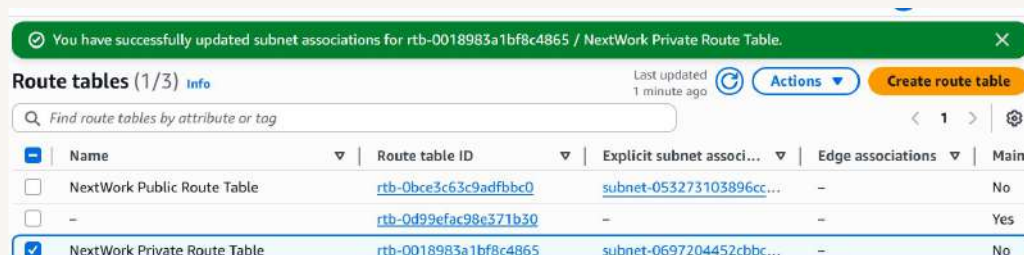


## A dedicated route table

By default, my private subnet is associated with the main route table by default unless I manually associate it with NextWork Private Route Table.

I had to set up a new route table to control traffic specifically for the private subnet. This ensures that the private subnet doesn't use the main or public route table.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows local VPC traffic (10.0.0.0/16) this means resources inside the subnet can communicate with other resources within the same VPC



You have successfully updated subnet associations for rtb-0018983a1bf8c4865 / NextWork Private Route Table.

Route tables (1/3) [Info](#) Last updated 1 minute ago [Actions](#) [Create route table](#)

Find route tables by attribute or tag

	Name	Route table ID	Explicit subnet associ...	Edge associations	Main
<input type="checkbox"/>	NextWork Public Route Table	<a href="#">rtb-0bce3c63c9adfbbc0</a>	<a href="#">subnet-053273103896cc...</a>	-	No
<input type="checkbox"/>	-	<a href="#">rtb-0d999efac98e371b30</a>	-	-	Yes
<input checked="" type="checkbox"/>	NextWork Private Route Table	<a href="#">rtb-0018983a1bf8c4865</a>	<a href="#">subnet-0697204452cbbc...</a>	-	No



## A new network ACL

By default, my private subnet is associated with VPC's default Network ACL. This default NACL allows all inbound and outbound traffic unless you create a custom NACL and explicitly associate it with your private subnet to apply stricter network rules

I set up a dedicated network ACL for my private subnet to tighten security at the subnet level by defining specific inbound and outbound rules. This ensures my private subnet is protected from unwanted traffic providing an additional security layer.

My new network ACL has two simple rules My new Network ACL has two simple rules one inbound and one outbound that both allow all traffic (0.0.0.0/0). This ensures resources in the private subnet can communicate freely within the VPC.



✓ You have successfully updated outbound rules for acl-0e3b6aef883ec0bf3 / NextWork Private NACL

**Network ACLs (1/3)** [Info](#) [Actions](#) [Create network ACL](#)

Find Network ACLs by attribute or tag

	Name	Network ACL ID	Associated with	Default	VPC ID
<input type="checkbox"/>	-	<a href="#">acl-04c8c60ef971d111f</a>	-	Yes	<a href="#">vpc-05dc</a>
<input checked="" type="checkbox"/>	NextWork Private NA...	<a href="#">acl-0e3b6aef883ec0bf3</a>	<a href="#">subnet-0697204452cbbc9b6 / NextWork Privat...</a>	No	<a href="#">vpc-05dc</a>

**acl-0e3b6aef883ec0bf3 / NextWork Private NACL**

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



[nextwork.org](https://nextwork.org)

# The place to learn & showcase your skills

Check out [nextwork.org](https://nextwork.org) for more projects

