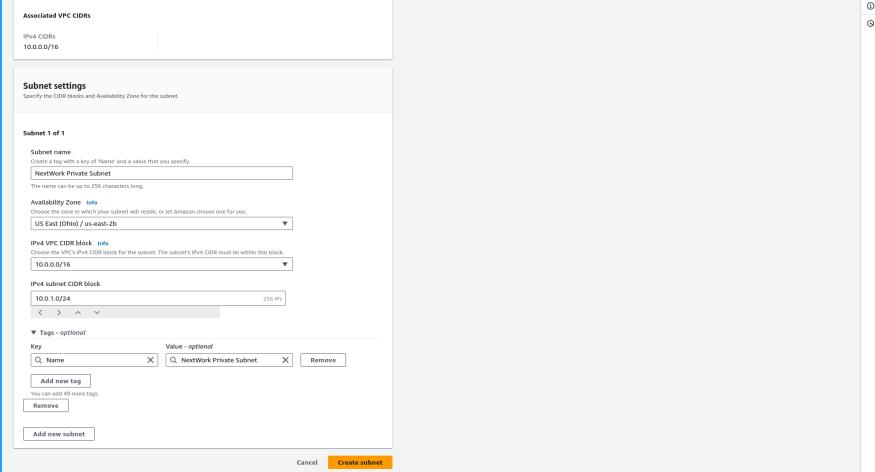


[NextWork.org](https://nextwork.org)

# Creating a Private Subnet



phogan2886@gmail.com



The screenshot shows the "Create a new subnet" step of the AWS VPC Subnet creation wizard. The interface includes fields for Associated VPC CIDR, Subnet settings (Subnet name: NextWork Private Subnet, Availability Zone: US East (Ohio) / us-east-2b), and IPv4 subnet CIDR block (10.0.1.0/24). A Tags section is also present, showing a single tag named "Name" with the value "NextWork Private Subnet". The "Create subnet" button is highlighted in orange at the bottom right.



phogan2886@gmail.com  
NextWork Student

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

# Introducing Today's Project!

## What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is a service that creates Isolated Networks. Allows you to set up a private, isolated network within AWS for your resources. Enhances Security and Control, providing fine-grained control over network config.

## How I used Amazon VPC in this project

Created a VPC which incorporate a public and private subnet to separate traffic. Customized ACLs to properly route traffic from the internet and set gates for the traffic flow

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

The ease it was to set the tables and gate for traffic flow and the separation of the subnets

## This project took me...

The project took me about 30 mins.



phogan2886@gmail.com  
NextWork Student

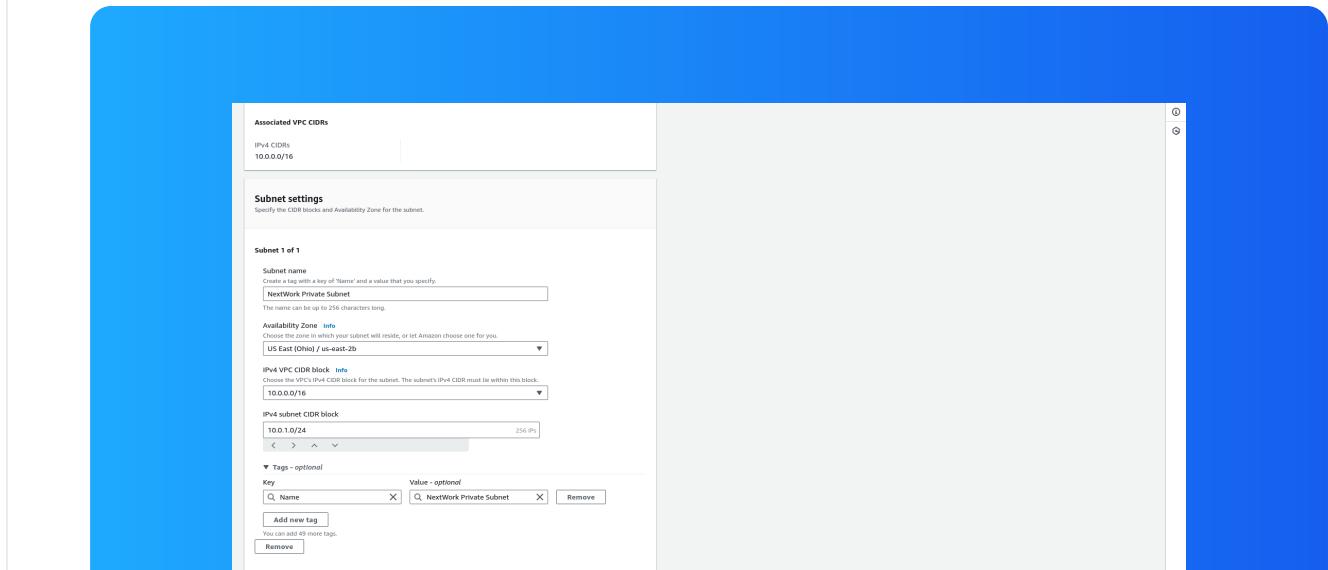
[NextWork.org](https://NextWork.org)

# Private vs Public Subnets

The difference between public and private subnets is that Public have a route to an Internet Gateway, allowing resources to access the internet directly. Private do not have direct internet access

Having private subnets are useful because enhance security to keep internal resources, like databases, isolated from direct internet access, reducing exposure to potential threats.

My private and public subnets cannot have the same Internet Access: Public subnets have direct internet access, while private subnets rely on NAT for outbound access. Security Exposure: Private subnets are not directly exposed to the internet





phogan2886@gmail.com  
NextWork Student

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

# A dedicated route table

By default, my private subnet is associated with 10.0.0.0/16 local/VPC

I had to set up a new route table because the default subnet table is accessible to the internet. I needed to make the entire table private.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows traffic from within the VPC private network

The screenshot shows the AWS Route Tables interface. At the top, a message says "You have successfully updated subnet associations for rtb-08e52544dd694e1c / NextWork Private Route Table". Below this, the "Route tables (1/3) Info" section lists three route tables:

Name	Route table ID	Explicit subnet assoc...	Main	VPC	Owner ID
NextWork Public Route Table	rtb-0baab132a89ff25d	subnet-03f7ef0669f20...	No	ycp-031e997da0ff5e2ba   NextWork VPC	02484845236
-	rtb-0ed92bb121340d5d	-	Yes	ycp-0f7293b7e539430x	02484845236
<b>NextWork Private Route Table</b>	<b>rtb-08e52544dd694e1c</b>	<b>subnet-01ae4de95f94eb...</b>	<b>No</b>	<b>ycp-0a1e997da0ff5e2ba   NextWork VPC</b>	<b>02484845236</b>

The main content area shows the details for the "rtb-08e52544dd694e1c / NextWork Private Route Table". The "Subnet associations" tab is selected. It shows one explicit association:

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
NextWork Private Subnet	subnet-01a4dd695f94eb0fd	10.0.1.0/24	-

Below this, a note states: "The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table." A table shows these subnets:

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
-	-	-	-



phogan2886@gmail.com  
NextWork Student

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

# A new network ACL

By default, my private subnet is associated with my private subnet

I set up a dedicated network ACL for my private subnet because we can make sure to deny all traffic to prevent attacks from the default ACL

My new network ACL has two simple rules, deny all traffic

The screenshot shows the NextWork interface for managing Network ACLs. At the top, a message indicates successful subnet associations for a specific ACL. Below this, the 'Network ACLs (1/4) Info' section lists four entries:

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count
-	acl-0f0e24008d9c87dc	3 Subnets	Yes	vpc-0f7293b7e5334520c	2 Inbound rules
-	acl-0e908a1b09295c9ba	-	Yes	vpc-0a1e9974a0fffe2ba / NextWork VPC	2 Inbound rules
NextWork Public NACL	acl-0e08650df05eb79d	subnet-057fe0669912d03114 / NextWork Public...	No	vpc-0a1e9974a0fffe2ba / NextWork VPC	2 Inbound rules
<b>NextWork Private NACL</b>	<b>acl-02359b7701690c0bf</b>	<b>subnet-01aae4de95f94ab9fd / NextWork Privat...</b>	<b>No</b>	<b>vpc-0a1e9974a0fffe2ba / NextWork VPC</b>	<b>1 Inbound rule</b>

Below this, a detailed view of the 'acl-02359b7701690c0bf / NextWork Private NACL' is shown. The 'Inbound rules' tab is selected, displaying a single rule:

Rule number	Type	Protocol	Port range	Source	Allow/Deny
1	All traffic	All	All	0.0.0.0/0	<b>Deny</b>



NextWork.org

# Everyone should be in a job they love.

Check out nextwork.org for  
more projects

