

Creating a Private Subnet

AM

ampahben3@gmail.com

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

Tags - optional

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) lets you control access and resource availability in AWS. It enhances security by isolating sensitive data, defining network rules, and ensuring only authorized users can interact with specific services.

How I used Amazon VPC in this project

I used Amazon VPC to set up private and public subnets, configure route tables for traffic control, add an internet gateway for public access, and create network ACLs and security groups to manage resource security and regulate traffic flow.

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

Repeating steps with slight changes was unexpected, but it reinforced key AWS concepts. The level of detail required for each configuration and its impact on security was surprising too.



AM

ampahben3@gmail.com

NextWork Student

NextWork.org

This project took me...

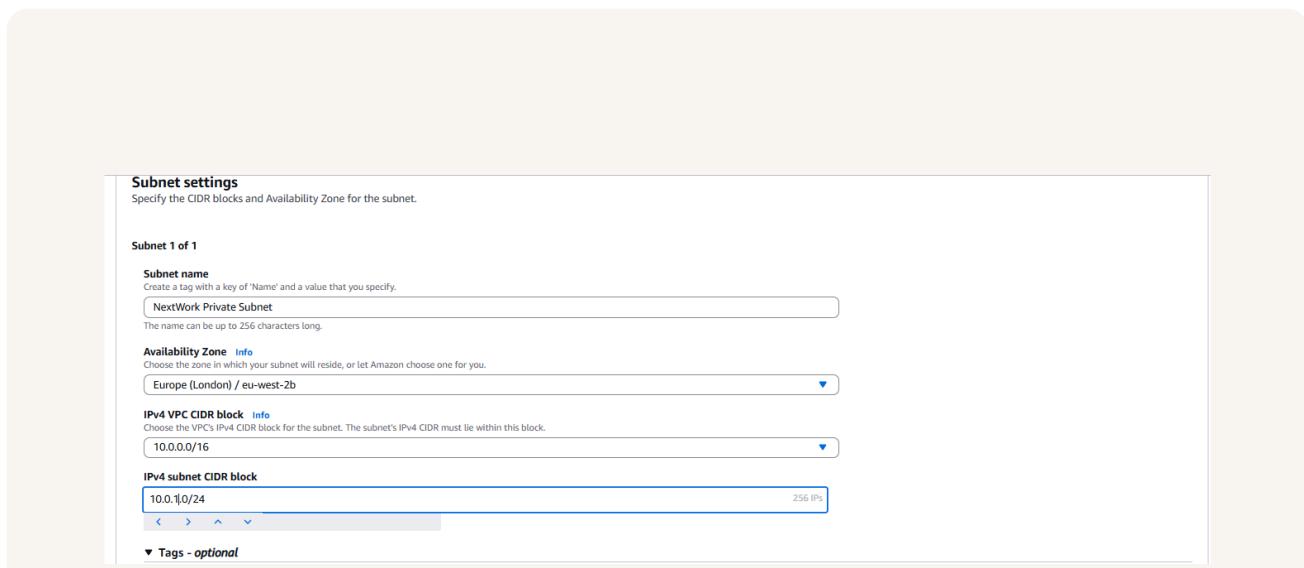
It took an hour because I focused on revising the first part, ensuring the Public Subnet was set up correctly and carefully configuring the CIDR block. Taking time on these foundational steps helped streamline the rest of the process.

Private vs Public Subnets

The difference between public and private subnets is that public subnets host resources accessible from the internet, while private subnets are isolated for security, housing sensitive data or internal applications without direct internet exposure.

Having private subnets are useful because they restrict internet access, protect sensitive data, and ensure controlled access. They enhance security, support internal applications, and minimize exposure to threats, keeping critical systems safe.

My private and public subnets cannot have the same CIDR block, as each subnet must have a unique IP range. This ensures proper network segmentation and avoids conflicts, enabling efficient routing and secure communication between resources.



A dedicated route table

By default, my private subnet is associated with the main route table of the custom VPC I created. This ensures internal communication while maintaining controlled access and preventing direct exposure to the public subnet.

I had to set up a new route table because the initial one was for a public subnet. This ensures private subnet traffic stays isolated, preventing unintended access and maintaining secure network segmentation.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows traffic within the VPC. It ensures secure internal communication while preventing direct external access, maintaining isolation for private resources.

The screenshot shows the AWS VPC Route Tables page. The interface includes a top navigation bar with the AWS logo, search bar, and various icons. On the left, there's a sidebar with 'VPC dashboard' and 'Virtual private cloud' sections, including 'Route tables'. The main content area displays a table titled 'Route tables (3) Info'. The table has columns for Name, Route table ID, Explicit subnet associ..., Edge associations, Main, and VPC. The table shows three entries:

Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
-	rtb-0ae822b7798d4e244	-	-	Yes	vpc-00f5730b761a0bf47
NextWork Public Route Table	rtb-084740138f109f4e3	subnet-06926b1047ac9a...	-	Yes	vpc-015438e332be14bdf h
NextWork Private Route Table	rtb-0dccfe5e05d10a2f0	subnet-0fba4566005822...	-	No	vpc-015438e332be14bdf h

Below the table, there's a section titled 'Select a route table' with three options: 'rtb-0ae822b7798d4e244', 'rtb-084740138f109f4e3', and 'rtb-0dccfe5e05d10a2f0'.

A new network ACL

By default, my private subnet is associated with the default network ACL of the VPC. This ACL automatically applies basic inbound and outbound rules, but a custom ACL can be configured to enforce stricter security controls for private resources.

I set up a dedicated network ACL for my private subnet because the default ACL is linked to the public subnet. The private subnet needs stricter security, so a separate ACL ensures controlled inbound and outbound rules, preventing unnecessary access.

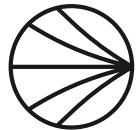
My new network ACL has two simple rules—one inbound and one outbound. The inbound rule denies all traffic from any source, ensuring no unauthorized access. Similarly, the outbound rule denies all traffic, preventing any data from leaving the subnet.

The screenshot shows the AWS VPC dashboard with the 'Network ACLs' section selected. There are four Network ACLs listed:

Name	Network ACL ID	Associated with	Default	VPC ID
NextWork Public NACL	acl-035ccb6053cede8fa	subnet-06926b1047ac9a4d9 / NextWork Publ...	No	vpc-015438e332be14bdf / NextWork V...
NextWork Private NA...	acl-0ce8bf19696e9b10f	subnet-0f8a4566005822623 / NextWork Privat...	No	vpc-015438e332be14bdf / NextWork V...
-	acl-03c5c3f94c16c608a	3 Subnets	Yes	vpc-0ff5730b761a0bf47
-	acl-0971cb504c7304062	-	Yes	vpc-015438e332be14bdf / NextWork V...

The 'Subnet associations' tab is selected, showing one association:

Name	Subnet ID	Associated with	Availability Zone	IPv4 CIDR	IPv6 CIDR
NextWork Private Subnet	subnet-0f8a456600582...	acl-0ce8bf19696e9b10f / NextWork Pri...	eu-west-2b	10.0.1.0/24	-



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for
more projects

