



Creating a Private Subnet

DI

dineshrajdhanapathy@gmail.com

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.
`vpc-05aa66f04efc1f04ce (NextWork VPC)`

Associated VPC CIDRs

IPv4 CIDRs
`10.0.0.0/16`

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.
`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-1a`

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`

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

Cancel **Create subnet**

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is a service to create isolated, customizable networks in AWS. It's useful for controlling resource access, enhancing security, and managing traffic within a cloud.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create isolated subnets for public and private resources, set up route tables for traffic management, and configured security with NACLs to control access.

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

One thing I didn't expect in this project was the complexity of configuring network ACLs and route tables to ensure proper security and traffic flow, as it required careful planning to avoid misconfigurations.

This project took me...

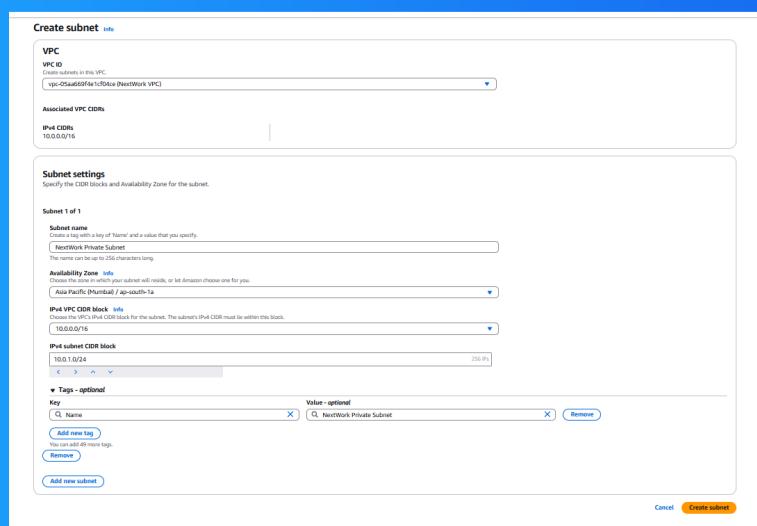
This project took me several hours to complete, including time spent setting up the VPC, configuring subnets, creating route tables, and adjusting network ACLs to ensure everything was secure and working properly.

Private vs Public Subnets

The difference between public and private subnets is that public subnets allow direct access to the internet via a public IP, while private subnets restrict access and require NAT or VPN for the internet.

Having private subnets are useful because they enhance security by isolating sensitive resources from the internet, reduce attack surface, and enable controlled access through NAT, VPN, or bastion hosts.

My private and public subnets cannot have the same CIDR block, as each must have unique IP ranges to avoid conflicts and ensure proper routing within the network.



A dedicated route table

By default, my private subnet is associated with the main route table, which does not have a route to an internet gateway, ensuring the subnet remains isolated from direct internet access.

I had to set up a new route table because I needed to customize traffic routing, such as directing internet-bound traffic through a NAT gateway for private subnets or isolating specific subnet communication.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows local VPC traffic and outbound internet access through a NAT gateway, maintaining security and isolation.

| You have successfully updated subnet associations for rtb-0496550d05b1bd191 / NextWork Private Route Table. | | | | | | | |
|---|-----------------------|---------------------------|-------------------|------|---------------------------------|--------------|--------------|
| Route tables (1/3) Info | | | | | | | |
| <input type="text"/> Find resources by attribute or tag | | | | | | | |
| Name | Route table ID | Explicit subnet associ... | Edge associations | Main | VPC | Owner ID | Last updated |
| - | rtb-05e2319c27e2b91e | - | - | Yes | vpc-0f1668c25a9f51658 | 466742534146 | 1 minute ago |
| <input checked="" type="checkbox"/> NextWork Public Route Table | rtb-5dd9226b23605505c | subnet-08570650ef4763... | - | Yes | vpc-05aa669f4e1cf04ce Next... | 466742534146 | |
| <input type="checkbox"/> NextWork Private Route | rtb-0496550d05b1bd191 | subnet-09be8e26e7d86e... | - | No | vpc-05aa669f4e1cf04ce Next... | 466742534146 | |

A new network ACL

By default, my private subnet is associated with the VPC's default Network ACL, which allows all inbound and outbound traffic until explicitly modified for enhanced security.

I set up a dedicated network ACL for my private subnet because it allows me to define granular rules to control inbound and outbound traffic, enhancing security and isolating the subnet from unwanted access.

My new network ACL has two simple rules: an inbound rule allowing VPC traffic and specific ports and an outbound rule permitting traffic to a NAT gateway or other necessary destinations.

| Network ACLs (1/4) Info | | | | | | | | |
|--|------------------------|--|---------|--------------------------------------|---------------------|----------------------|--------------|--|
| <input type="text"/> Find resources by attribute or tag | | Actions Create network ACL | | | | | | |
| Name | Network ACL ID | Associated with | Default | VPC ID | Inbound rules count | Outbound rules count | Owner | |
| - | acl-004cd4abed61dad59 | - | Yes | vpc-05aa669f4e1cf04ce / NextWork VPC | 2 Inbound rules | 2 Outbound rules | 46674253414f | |
| <input checked="" type="checkbox"/> NextWork Public NACL | awl-08ed1ad5e4097bdc | subnet-08570d60ef47d3fad / NextWork Public ... | No | vpc-05aa669f4e1cf04ce / NextWork VPC | 2 Inbound rules | 2 Outbound rules | 46674253414f | |
| - | acl-0ad28f6600351830f4 | 3. Subnets | Yes | vpc-0f1658c2599f51658 | 2 Inbound rules | 2 Outbound rules | 46674253414f | |
| - | acl-0xe9657eaab013e1c | subnet-09be8e26e7d86eaa4 / NextWork Privat... | No | vpc-05aa669f4e1cf04ce / NextWork VPC | 1 Inbound rule | 1 Outbound rule | 46674253414f | |



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for
more projects

