



# Creating a Private Subnet

R

Roshan Shrestha

subnet-00f477c03b9630fe2 / NextWork Private Subnet

| Details           |  | Actions                         |  |
|-------------------|--|---------------------------------|--|
| Subnet ID         | <a href="#">subnet-00f477c03b9630fe2</a> | Subnet ARN                      | <a href="#">arn:aws:ec2:us-east-2:321775682595:subnet/subnet-00f477c03b9630fe2</a> |
| IPv4 CIDR         | <a href="#">10.0.1.0/24</a>              | State                           | <span>Available</span>   |
| Availability Zone | <a href="#">us-east-2a</a>               | IPv6 CIDR                       | -  |
| Network ACL       |  | VPC                             | <a href="#">vpc-05d211b97b315a41b   NextWork VPC</a>                               |
|                   |  | Auto-assign public IPv4 address | Auto-assign IPv6 address   |
|                   |  | Block Public Access             | <input checked="" type="radio"/> Off   |
|                   |  | IPv6 CIDR association ID        | -  |
|                   |  | Route table                     | <a href="#">rtb-0cf805cf4241a2c   NextWork route table</a>                         |
|                   |  |                                 | Auto-assign IPv6 address   |



# Introducing Today's Project!

## What is Amazon VPC?

Amazon VPC is a section of the amazon cloudspace that is distinguishable from the rest, like a town within a country. It is useful because it helps us identify and isolate our resources.

## How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create a private subnet, a route table and a NACL for the private subnet.

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

One thing I didn't expect in this project is how easy it is to setup a private network ACL considering how important it is for security.

## This project took me...

This project took me about an hour.



# Private vs Public Subnets

The difference between public and private subnets is that public subnets are connected to the internet via an internet gateway whereas the private subnet is meant for resources that we want to isolate from the internet and need local communication.

Having private subnets are useful because we can keep resources like databases and user credentials private from the internet while maintaining access to resources local to the VPC.

My private and public subnets cannot have the same addresses. Similar to how two sections of the same city do not have the same address, we don't assign the same IP range to private and public subnets.



subnet-00f477c03b9630fe2 / NextWork Private Subnet

| Details           |  | Block Public Access      |  |
|-------------------|--|--------------------------|--|
| Subnet ID         | <a href="#">subnet-00f477c03b9630fe2</a> | Subnet ARN               | <a href="#">arn:aws:ec2:us-east-2:521775682595:subnet/subnet-00f477c03b9630fe2</a> |
| IPv4 CIDR         | <a href="#">10.0.1.0/24</a>              | Available IPv4 addresses | <a href="#">251</a>  |
| Availability Zone | <a href="#">us-east-2b</a>               | Availability Zone ID     | <a href="#">use2-sz2</a>   |
| Network ACL       |  | VPC                      | <a href="#">vpc-05d211b97b315a41b   NextWork VPC</a>                               |
|                   |  |                          | Auto-assign public IPv4 address  |
|                   |  |                          | Block Public Access  |
|                   |  |                          | <input type="radio"/> Off  |
|                   |  |                          | IPv6 CIDR association ID   |
|                   |  |                          | -  |
|                   |  | Route table              | <a href="#">rtb-0cf805cff4c241a2c   NextWork route table</a>                       |
|                   |  |                          | Auto-assign IPv6 address   |



# A dedicated route table

By default, my private subnet is associated with the default VPC route table.

I had to set up a new route table because by default the private subnet was associated with the VPC route table which lead traffic to the internet gateway making my private subnet publicly accessible. So, new route with local access only.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows local traffic

The screenshot shows the AWS VPC Route Tables interface. In the main pane, a message indicates successful subnet association for the route table 'rtb-0409828d95d4fa096 / NextWork Private Route Table'. The table lists three route tables:

| Name                                | Route table ID               | Explicit subnet associations              | Main     | VPC       | Owner ID                                     |                     |
|-------------------------------------|------------------------------|---|----------|-----------|--|---------------------|
| -                                   | rtb-0b2a53676db10a5c         | -   | -        | Yes       | vpc-014d0f52d7fd0e7                          | 321775682595        |
| NextWork Public Route Table         | rtb-0ef805cff4c241a2c        | subnet-0092f5fd72258453 / Next...         | -        | Yes       | vpc-05d211b897b315a41b   NextWork VPC        | 321775682595        |
| <b>NextWork Private Route Table</b> | <b>rtb-0409828d95d4fa096</b> | <b>subnet-00f477c03b9630fe2 / Next...</b> | <b>-</b> | <b>No</b> | <b>vpc-05d211b897b315a41b   NextWork VPC</b> | <b>321775682595</b> |

In the bottom details pane, the 'Main' status is set to 'No' and the 'Owner ID' is listed as '321775682595'. The 'Explicit subnet associations' section shows the association with 'subnet-00f477c03b9630fe2 / NextWork Private Subnet'.

# A new network ACL

By default, my private subnet is associated with the default NACL that AWS creates for each subnet. This NACL allows all inbound and outbound traffic.

I set up a dedicated network ACL for my private subnet because I want to control access to my resources in the private subnet. Not allow all traffic.

My new network ACL has two simple rules - Deny all inbound and outbound traffic.

The screenshot shows the AWS VPC Network ACLs page. On the left, there's a navigation sidebar with options like VPC dashboard, EC2 Global View, Virtual private cloud, Security, and PrivateLink and Lattice. The main area displays a table of Network ACLs:

| Name                  | Network ACL ID       | Associated with                                    | Default | VPC ID                              | Inbound rules count | Outbound rules count |
|-----------------------|----------------------|--|---------|-------------------------------------|---------------------|----------------------|
| NextWork Private NACL | ac-0b9281a40ee7aea6e | subnet-00f477c03b9530fe2 / NextWork Private Subnet | No      | vpc-05d21b97b315a41b / NextWork VPC | 1 Inbound rule      | 1 Outbound rule      |
| -                     | ac-d0723ea439fb08066 | 3 Subnets  | Yes     | vpc-014df052402f60e7                | 2 Inbound rules     | 2 Outbound rules     |
| NextWork Public NACL  | ac-02223ea416d20ad9  | subnet-09275e6d72258453 / NextWork Public Subnet   | No      | vpc-05d21b97b315a41b / NextWork VPC | 2 Inbound rules     | 2 Outbound rules     |
| -                     | ac-0fc73bc658e095b4  | -  | Yes     | vpc-05d21b97b315a41b / NextWork VPC | 2 Inbound rules     | 2 Outbound rules     |

Below this, a detailed view of the 'NextWork Private NACL' is shown. It has tabs for Details, Inbound rules, Outbound rules, Subnet associations, and Tags. The Inbound rules section shows one rule:

| Rule number | Type        | Protocol | Port range | Source    | Allow/Deny |
|-------------|-------------|----------|------------|-----------|------------|
| *           | 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

