



# Creating a Private Subnet



Katleo Rantle

Subnets (8) <a href="#">Info</a>								
	Name	Subnet ID	State	VPC	Action	IPv4 CIDR	IPv6 CIDR	Actions
	-	subnet-0c24ff07x73213121	Available	vpc-063a1x7ed0d2f17e6	<input type="radio"/> Off	17.23.1.48/0/20	-	<a href="#">Actions</a>
	-	subnet-02701414229592	Available	vpc-063a1x7ed0d2f17e6	<input type="radio"/> Off	17.23.1.0/0/20	-	<a href="#">Actions</a>
	-	subnet-07a0d0d9615e91	Available	vpc-063a1x7ed0d2f17e6	<input type="radio"/> Off	17.23.1.64/0/20	-	<a href="#">Actions</a>
	-	subnet-0338ab1eefce4783c	Available	vpc-063a1x7ed0d2f17e6	<input type="radio"/> Off	17.23.1.32/0/20	-	<a href="#">Actions</a>
	-	subnet-036a2711ed27d758db	Available	vpc-063a1x7ed0d2f17e6	<input type="radio"/> Off	17.23.1.16/0/20	-	<a href="#">Actions</a>
	public 1	subnet-0d8d4873c602ca9d81f	Available	vpc-063a1x7ed0d2f17e6	<input type="radio"/> Off	17.23.1.80/0/20	-	<a href="#">Actions</a>
	NextWork Private Subnet	subnet-0fe8c1849bcb768b	Available	vpc-0729d116258b2f8   NextWork VPC 260130	<input type="radio"/> Off	10.0.0.0/24	-	<a href="#">Actions</a>



**Katleo Rantle**

NextWork Student

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

# Introducing Today's Project!

## What is Amazon VPC?

Amazon VPC is a logical network boundary. It is useful because it provides a way for us to create isolated secure space for us to create resources on the cloud.

## How I used Amazon VPC in this project

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

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

One thing I didn't expect in this project is that private subnet needs its own dedicated route table and custom Network ACL (NACL) to function properly and maintain its private isolation.

## This project took me...

This project took me 1,5 hr

## Private vs Public Subnets

The difference between public and private subnets is that public subnets allow internet traffic where as private subnets only allow communication within the VPC

Having private subnets are useful because they allow us to restrict resource access from unauthorized connections and ensure internal apps dont have direct access to the internet

My private and public subnets cannot have the same CIDR block or range of ip addresses

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	IPv6 CIDR
-	subnet-0624ff07a7325121e	Available	vpc-063a1e7edd2f117e6	Off	172.31.48.0/20	-
-	subnet-007fd1c43f422a952	Available	vpc-063a1e7edd2f117e6	Off	172.31.0.0/20	-
-	subnet-07a0f0daff8616a91	Available	vpc-063a1e7edd2f117e6	Off	172.31.64.0/20	-
-	subnet-0d38d0be4ec4783cc	Available	vpc-063a1e7edd2f117e6	Off	172.31.32.0/20	-
-	subnet-036a271eed27a580b	Available	vpc-063a1e7edd2f117e6	Off	172.31.16.0/20	-
-	subnet-0b59ba9a7e8aaacb81f	Available	vpc-063a1e7edd2f117e6	Off	172.31.80.0/20	-
public 1	subnet-06dbd73d402c9ad28	Available	vpc-0c729d116268b2f10   NextWork VPC 260130	Off	10.0.0.0/24	-
NextWork Private Subnet	subnet-08e8c184919b769b	Available	vpc-0c729d116268b2f10   NextWork VPC 260130	Off	10.0.1.0/24	-

# A dedicated route table

By default, my private subnet is associated with the default route table that AWS automatically created with the VPC

I had to set up a new route table because the default route table has a route to the internet gateway which enables internet access

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

Route tables (1/4) <a href="#">Info</a>						
<input type="text"/> Find route tables by attribute or tag						
Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC	
-	rtb-00fc215e2666ec72	-	-	Yes	vpc-063a1e7eddd2f17e6	<a href="#">Actions</a>
-	rtb-05dcd41e2199f171	-	-	Yes	vpc-0c729d116268b2fc8   NextWork VPC 260130	<a href="#">Actions</a>
NextWork Public-rt	rtb-095662ea36326b016	subnet-0d6db73c602c9ad28 / NextWork Public Subnet	-	No	vpc-0c729d116268b2fc8   NextWork VPC 260130	<a href="#">Actions</a>
<input checked="" type="checkbox"/> NextWork Private-rt	rtb-0b0f4d66f19cf3f95	subnet-08e8c1849b9cb768b / NextWork Private Subnet	-	No	vpc-0c729d116268b2fc8   NextWork VPC 260130	<a href="#">Actions</a>



## A new network ACL

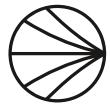
By default, my private subnet is associated with the default NACL which was created by AWS

I set up a dedicated network ACL for my private subnet because the default NACL allows all traffic and exposes our private subnet

My new network ACL has two simple rules - 100 inbound and out bound allowing traffic in and out the subnet

The screenshot shows the AWS Network ACL details page for 'acl-0f0bb384dceabf5ed / NextWork Private NACL'. The page has a header with 'Actions' and a 'Details' tab. Under 'Details', there are sections for 'Network ACL ID' (acl-0f0bb384dceabf5ed), 'Associated with' (subnet-08e8c1849b9cb768b / NextWork Private Subnet), 'Default' (No), and 'VPC ID' (vpc-0c729d116268b2fc8 / NextWork VPC 260130). Below this, there are tabs for 'Inbound rules', 'Outbound rules', 'Subnet associations' (which is selected), and 'Tags'. The 'Subnet associations' section shows one entry:

Name	Subnet ID	Associated with	Availability Zone	IPv4 CIDR	IPv6 CIDR
NextWork Private Subnet	<a href="#">subnet-08e8c1849b9cb768b</a>	acl-0f0bb384dceabf5ed / NextWork Pri...	use1-az6 (us-east-1b)	10.0.1.0/24	-



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

# The place to learn & showcase your skills

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

