



Creating a Private Subnet



nikhil7_94@hotmail.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
◀ ▶ ⌂ ⌃

Introducing Today's Project!

What is Amazon VPC?

A VPC is a private isolated network in the cloud where you can securely run resources like servers and databases. It's useful because it gives full control over network settings, security, and connectivity to the internet.

How I used Amazon VPC in this project

Today I used Amazon VPC to create a public subnet.

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

One thing I didnt expect was subnets that arent associated with another route table automatically use NextWork Public Route Table.

This project took me...

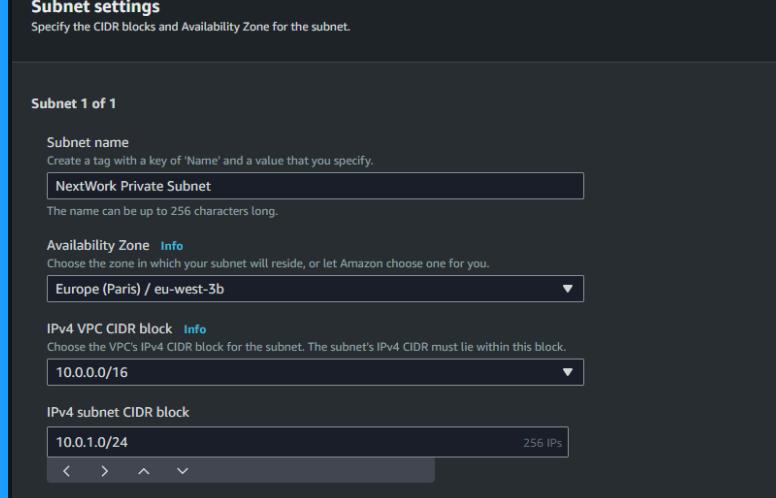
I took a round 1 hour with this project.

Private vs Public Subnets

The difference between public and private subnets is that public subnets have routes to the internet through an internet gateway, while private subnets do not keeping their resources isolated from direct internet access.

Having private subnets are useful because you can isolate resources from direct internet access reducing exposure to potential threats.

My private and public subnets cannot have the same IP address range as each subnet must be uniquely identifiable within the VPC.



A dedicated route table

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

I had to set up a new route table because I want to isolate my VPC subnet and don't have access to internet.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows all traffic to internal resources instead of internet.

The screenshot shows the AWS Route Tables page with the following details:

Name	Route Table ID	Explicit subnet associations	Main
-	rtb-0299e6034ddaf8ad2	-	Yes
NextWork Public Route Table	rtb-0bd19c9ae0a788bdf	subnet-02be28d7b12314...	Yes
NextWork Private Route Table	rtb-05dfb76f155b1a004	subnet-0bc389ba11bcf3a...	No

Below the table, the details for the selected route table (rtb-05dfb76f155b1a004) are shown:

Details			
Route table ID: rtb-05dfb76f155b1a004	Main: No	Explicit subnet associations: subnet-0bc389ba11bcf3a91 /	Edge associations: -

A new network ACL

By default, my private subnet is associated with default network ACL, since you haven't set up an explicit association between your private subnet and another network ACL.

I set up a dedicated network ACL for my private subnet because I want to restrict traffic and protect my private subnet.

My new network ACL has two simple rules which are the inbound rules and outbound rules to define exactly which traffic source allow. At this step I have denied all access in both of this rules.

Inbound rules (1)							Edit inbound rules	
Rule number		Type	Protocol	Port range	Source	Allow/Deny		
*	All traffic	All	All	0.0.0.0/0		Deny		



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for
more projects

