

Creating a Private Subnet



Sanjana Tripathy

Create subnet info

VPC
VPC ID
Create subnet in this VPC.
vpc-0ac89301e96a4605 (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.
private-01
The name can be up to 255 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-1 ▼

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
10.0.1.0/24 255 IPs
◀ ▶ ↶ ↷

Tags - optional

Key	Value - optional	
<input type="text" value="Name"/>	<input type="text" value="private-01"/>	<input type="button" value="Remove"/>
<input type="button" value="Add new tag"/>		
<small>You can add 0-50 more tags.</small>		
<input type="button" value="Remove"/>		
<input type="button" value="Add new subnet"/>		

Cancel



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) lets you create a logically isolated network in the AWS cloud where you can launch resources like EC2 instances. It's useful because it gives you full control over networking, including IP ranges, subnets, routing.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to design a secure virtual network by creating a private subnet. I set up a custom route table, and configured a network ACL to control and restrict traffic flow for the private subnet.

This project took me...

This project took me 1 hour to complete.

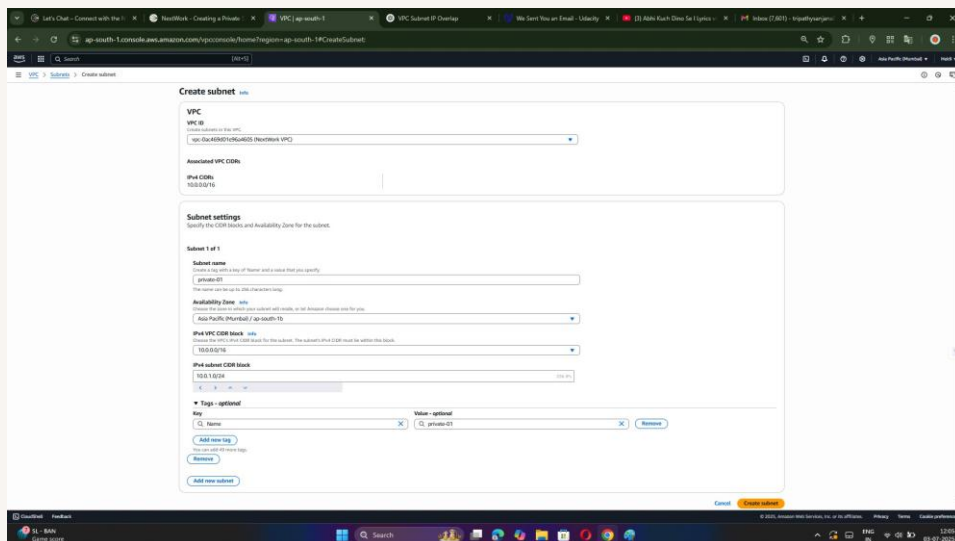


Private vs Public Subnets

A public subnet has a route to the internet via an Internet Gateway, allowing resources (like EC2) to be accessed from the internet. A private subnet has no direct internet route, keeping its resources isolated from public access.

Having private subnets is useful because they keep sensitive resources (like databases or internal servers) isolated from the internet, improving security and reducing exposure to external threats.

My private and public subnets cannot have the same same CIDR block. Each subnet in a VPC must have a unique, non-overlapping IP range to avoid routing conflicts.



The screenshot shows the 'Create subnet' page in the AWS Management Console. The page is titled 'Create subnet' and has a 'VPC' tab selected. The 'VPC ID' field is set to 'vpc-01a4b0c7d9c4b0d00'. The 'Associated VPC CIDRs' field shows '10.0.0.0/16'. The 'Subnet settings' section is expanded, showing 'Subnet 1 of 1'. The 'Subnet name' field is 'private-01'. The 'Availability Zone' is set to 'us-east-1a'. The 'IPv4 VPC CIDR block' is '10.0.0.0/16'. The 'IPv4 subnet CIDR block' is '10.0.0.0/16', which is highlighted with a red box. Below this, there are 'Tags - optional' and 'VPC - optional' sections. The 'VPC - optional' section has a 'Name' field set to 'private-01' and a 'Remove' button. The 'Tags - optional' section has an 'Add new tag' button. The 'Create subnet' button is at the bottom right.



A dedicated route table

By default, my private subnet is associated with the main route table that was created along with the VPC. This default route table applies to all subnets unless explicitly associated with a custom one.

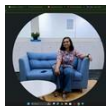
By default, my private subnet is associated with the main route table created with the VPC. However, to make it truly private, I create a new route table without a route to the internet, as the default table routes traffic to the Internet Gateway.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows local traffic within the VPC, ensuring the subnet remains isolated from the internet.

The screenshot shows the AWS Management Console interface for Route Tables. The top section displays a list of route tables, and the bottom section shows the details for a specific private route table.

Name	Route table ID	Explicit subnet assoc...	Edge associations	Main	VPC	Owner ID
-	rtb-02651556a3a91811	-	-	Yes	vpc-0775e14f1b1a14908	794038222820
NW Public Routetable	rtb-041372a60442a2f35	subnet-03278a4395a458b...	-	No	vpc-d0a469d71c95a4605 Next...	794038222820
-	rtb-0724a613a8d2313d9	-	-	Yes	vpc-d0a469d71c95a4605 Next...	794038222820
NW Private RouteTable	rtb-0001190cb9105094e	subnet-05c4e4a8270ca775 / private-01	-	No	vpc-d0a469d71c95a4605 Next...	794038222820

rtb-0001190cb9105094e / NW Private RouteTable			
Details			
Route table ID	Main	Explicit subnet associations	Edge associations
rtb-0001190cb9105094e	No	subnet-05c4e4a8270ca775 / private-01	-
VPC	Owner ID		
vpc-d0a469d71c95a4605 NextWork VPC	794038222820		



A new network ACL

By default, my private subnet is associated with with the default network ACL created when VPC was created.

I set up a dedicated network ACL for my private subnet because it allows me to define strict inbound and outbound rules, adding an extra layer of security to control traffic at the subnet level.

n my new NACL, the inbound rule denies all traffic by default (0.0.0.0/0). The outbound rule also denies all traffic. This ensures strict isolation, and I can add specific allow rules to permit only internal VPC communication as needed.

The screenshot shows the AWS Network ACLs console. The top section lists three Network ACLs:

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count	Outbound rules count	Owner
-	acl-0273b761c4f20830	3 Subnets	Yes	vpc-0f766c14b9a4f898	2 Inbound rules	2 Outbound rules	794038222820
NextWork NACL	acl-0a2073c417943222b7	subnet-012084-95d49d600 / Public-01	No	vpc-0ac469d71c06a8605 / NextWork V...	2 Inbound rules	2 Outbound rules	794038222820
-	acl-00af2927a457787de	-	Yes	vpc-0ac469d71c06a8605 / NextWork V...	2 Inbound rules	2 Outbound rules	794038222820
NextWork Private ACL	acl-0a06136d16d310d8	subnet-05d44488070ca75 / private-01	No	vpc-0ac469d71c06a8605 / NextWork V...	1 Inbound rule	1 Outbound rule	794038222820

The bottom section shows the details for the 'NextWork Private ACL' (acl-0a06136d16d310d8). It has tabs for Details, Inbound rules, Outbound rules, Subnet associations, and Tags. The 'Inbound rules' tab is active, showing a single rule:

Rule number	Type	Protocol	Port range	Source	Allow/Deny
-	All traffic	All	All	0.0.0.0/0	Deny



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

