



Creating a Private Subnet

D

Duc Thai

VPC > Subnets > Create subnet

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
< > ^ ^

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.

CloudShell Feedback Privacy Terms Cookie preferences

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is your private network in AWS where you pick IP ranges, subnets, routes and firewalls. It isolates and secures resources, controls internet access, and lets you connect safely to your data center or office.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to set up the private subnet, private route table and private NACL to protect resources that need to be stored secured and private.

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

One thing I didn't expect in this project is that you must allow both inbound and outbound in a stateless NACL — forgetting one side will block traffic even if security groups, NAT, and IGW are correct.

This project took me...

This project took me 60 minutes.

Private vs Public Subnets

The difference between public and private subnets is that Public subnet has a route to an Internet Gateway; resources with public IPs can be reached from the internet. Private subnet no IGW route, not reachable from the internet, uses a NAT to reach.

Having private subnets are useful because they protect resources by keeping them off the internet. A private subnet has no IGW route, so it's not publicly reachable. Instances can still reach out via a NAT, lowering attack surface.

My private and public subnets cannot have the same CIDR block. Because subnets must be non-overlapping slices of the VPC IP range. Sharing CIDRs would cause duplicate IPs and routing conflicts. AWS enforces unique, non-overlapping subnet CIDR blocks.

D

Duc Thai

NextWork Student

nextwork.org

VPC > Subnets > Create subnet

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

Tags - optional

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="NextWork Private Subnet"/>

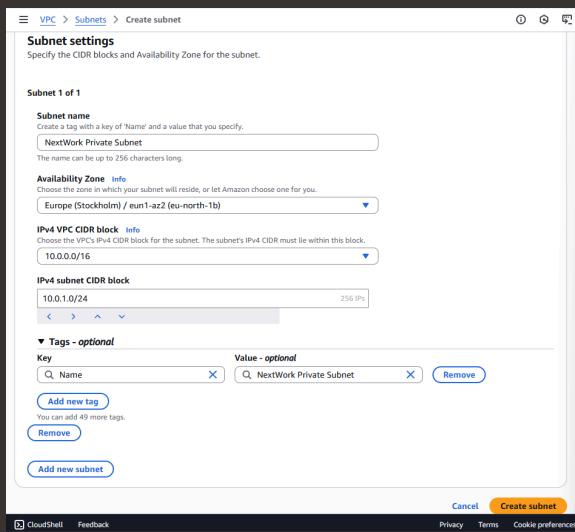
[Add new tag](#) You can add 49 more tags.
[Remove](#)

[Add new subnet](#)

[Cancel](#) [Create subnet](#)

[CloudShell](#) [Feedback](#)

[Privacy](#) [Terms](#) [Cookie preferences](#)



A dedicated route table

By default, my private subnet is associated with the route table that auto created by AWS when I set up my VPC.

I had to set up a new route table because the default route table was also used for public sub, which as the route the igw, that make my subnet public. Need to new one with no igw route to make the resources inside secure.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows lets instances talk to any IP inside the VPC. There's no 0.0.0.0/0 to an IGW or NAT, so traffic won't reach the internet—only intra-VPC communication.

D

Duc Thai
NextWork Student

nextwork.org

rtb-0db3781645e73a834 / NextWork Private Route Table

[Actions ▾](#)

Details [Info](#)

Route table ID	rtb-0db3781645e73a834	Main	<input checked="" type="checkbox"/> No
VPC	vpc-00a2e442ba9b0944c NextWork VPC	Owner ID	841162690953
Explicit subnet associations	subnet-0705cfec46c2032e8 / NextWork Private Subnet	Edge associations	-

[Routes](#) [Subnet associations](#) [Edge associations](#) [Route propagation](#)

Routes (1)

[Edit routes](#)

Destination	Target
10.0.0.0/16	local

A new network ACL

By default, my private subnet is associated with default network ACL set up for every VPC. This default network ACL is associated with your private subnet, since I haven't set up an explicit association.

I set up a dedicated network ACL for my private subnet because the default ACL allows all traffic, which exposes your private subnet to unrestricted access from the internet or other untrusted networks. Need a new one that restricts traffic.

My new network ACL has two simple rules - denying all inbound and outbound traffic! I will leave these settings for now - let's customise them later in this project series,

D

Duc Thai
NextWork Student

nextwork.org

The screenshot shows a network configuration interface for a 'NextWork Private NACL' named 'acl-00976141f7e4b21ea'. The interface includes tabs for 'Details', 'Inbound rules' (which is selected), 'Outbound rules', 'Subnet associations', and 'Tags'. Under the 'Inbound rules' tab, there is a table with one row:

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

