

Creating a Private Subnet

A

Antonio C

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](#)



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is a service that lets you create a private, isolated network within AWS. It's useful for securely hosting resources, controlling network traffic, and customizing IP address ranges, subnets, and routing for enhanced

How I used Amazon VPC in this project

Create a private subnet. Create a private route table. Create a private network ACL.

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

I did not expect the various security changes in ACL

This project took me...

This project took me about an hour to complete.



Private vs Public Subnets

Public subnets have a route to the internet via an Internet Gateway, allowing direct access. Private subnets lack this route, so resources within them can't be accessed directly from the internet, enhancing security for sensitive data.

Private subnets exist to protect sensitive resources, like databases or internal apps, from direct internet access. This enhances security by limiting exposure and allowing only controlled communication through NAT or internal networking.

Private and public subnets can't share the same IP address range (CIDR block) or the same route to the Internet Gateway. Public subnets need a route to the IGW, while private ones use a NAT or no internet route at all for security.

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



A dedicated route table

By default, your private subnet is associated with the main route table of the VPC, which does not have a route to the Internet Gateway—keeping the subnet private and restricting direct internet access.

I had to set up a new route table because I am making sure it can only direct traffic to another internal resource (instead of the public internet).

A private subnet's route table allows internal VPC traffic (e.g., to other subnets) and, if configured, outbound internet traffic through a NAT Gateway or NAT instance. It blocks direct internet access by not routing through an Internet Gateway.

Route tables (1/3) Info						
Create route table						
Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC	Owner ID
<input checked="" type="checkbox"/> NextWork Public Route Table Edit	rtt-009c4020b006d5a#9a	subnet-06c009c36f94200...	-	Yes	vpc-0964d9fa772d8631b Next...	06685549#373
<input type="checkbox"/> -	rtt-0e748c28c2ef415b	-	-	Yes	vpc-0d04ad6ca0ccdf58	06685549#373
<input type="checkbox"/> NextWork Private Route Table	rtt-0a82b6065bdccfc1a	subnet-0dd5b215af87915...	-	No	vpc-0964d9fa772d8631b Next...	06685549#373

A new network ACL

A VPC's default network ACL allows all traffic, which exposes your private subnet to unrestricted access from the internet or other untrusted networks.

I set up a dedicated network ACL for my private subnet because it restricts traffic and protects your private subnet!

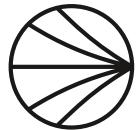
I set up a custom network NACLs to control inbound and outbound traffic for this private subnet - denying all traffic by default.

The screenshot shows the AWS Network ACLs interface. At the top, there is a search bar and a 'Create network ACL' button. Below is a table listing four Network ACLs:

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count	Outbound rules count
ad-06095f5ceee825a86	ad-06095f5ceee825a86	6 Subnets	Yes	vpc-0d04a66ca0ccdf158	2 Inbound rules	2 Outbound rules
ad-05cf148c783d46af	ad-05cf148c783d46af	subnet-0dd5b213af87915bf / NextWork Private ...	Yes	vpc-0984d9faf72e8631b / NextWork VPC	2 Inbound rules	2 Outbound rules
NextWork Network ACL	ad-0ef6f014de1ae27e504	subnet-06c009c36fb94200d3 / NextWork Public ...	No	vpc-09564d9faf72e8631b / NextWork VPC	2 Inbound rules	2 Outbound rules
NextWork Private NACL	ad-051a86bd533da560f	-	No	vpc-0984d9faf72e8631b / NextWork VPC	1 Inbound rule	1 Outbound rule

Below the table, the details for the selected 'ad-051a86bd533da560f / NextWork Private NACL' are shown. The 'Inbound rules' tab is active, displaying one rule:

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

