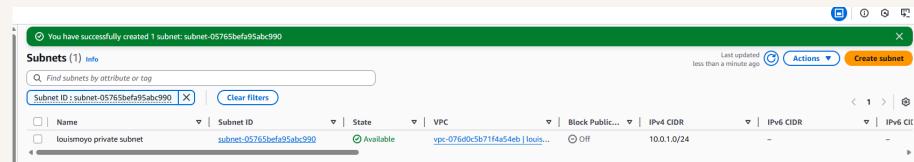




Creating a Private Subnet



Louis Moyo





Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a virtual private cloud that lets you isolate and control network resources in AWS. It's useful for customising security, IP ranges, and routing to fit your project needs.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create a private subnet for internal resources, ensuring they are isolated from the internet for security.

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

One thing I didn't expect was that the private subnet automatically linked to the main route table, requiring a separate one for full isolation.

This project took me...

This project took me about 45minutes, including creating the subnet, checking settings, and verifying its association with the correct route table.



Private vs Public Subnets

The difference between public and private subnets is that public subnets have a route to the internet via an internet gateway, while private subnets do not.

Having private subnets is useful because they isolate resources from direct internet access, improving security by reducing exposure to external threats.

My private and public subnets cannot have the same CIDR block within the same VPC, as each subnet must have a unique range of IP addresses.

You have successfully created 1 subnet: subnet-05765befa95abc990

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	IPv6 CIDR	IPv6 Cidr
louismoyo private subnet	subnet-05765befa95abc990	Available	vpc-076d0c5b71f4a54eb Louis...	Off	10.0.1.0/24	-	-



A dedicated route table

By default, my private subnet is associated with the main route table of the VPC, which handles routing until a custom route table is assigned.

I set up a new route table to isolate the private subnet's traffic, ensuring it routes internally without direct internet access for added security.

My private subnet's route table allows only internal VPC traffic via the local route, preventing any direct outbound internet connectivity.

Route tables (3) Info						
	Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
<input type="checkbox"/>	touismoyo public route table	rtb-009a1ad7736fe795	subnet-0c5adab416fd45e...	-	Yes	vpc-076d0c5b71f4a54eb louis...
<input type="checkbox"/>	-	rtb-0d03aef461d7c5953	-	-	Yes	vpc-0f35a84f1e27356de 756716632322
<input type="checkbox"/>	touismoyo private route table	rtb-0097c333af8231eba	subnet-05765befa95abc...	-	No	vpc-076d0c5b71f4a54eb louis...

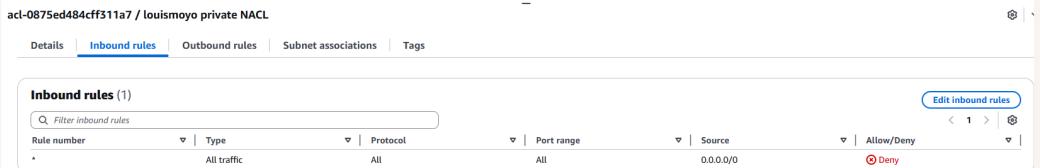


A new network ACL

By default, my private subnet is associated with the VPC's default NACL, which allows all inbound and outbound traffic unless explicitly modified.

I set up a dedicated network ACL for my private subnet to enforce stricter traffic control, separating it from the default NACL to better secure sensitive resources.

My new network ACL has two rules: inbound denies all traffic from any source (0.0.0.0/0) and outbound denies all traffic to any destination (0.0.0.0/0).



The screenshot shows the 'Inbound rules' section of the AWS Network ACL configuration. It displays one 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

