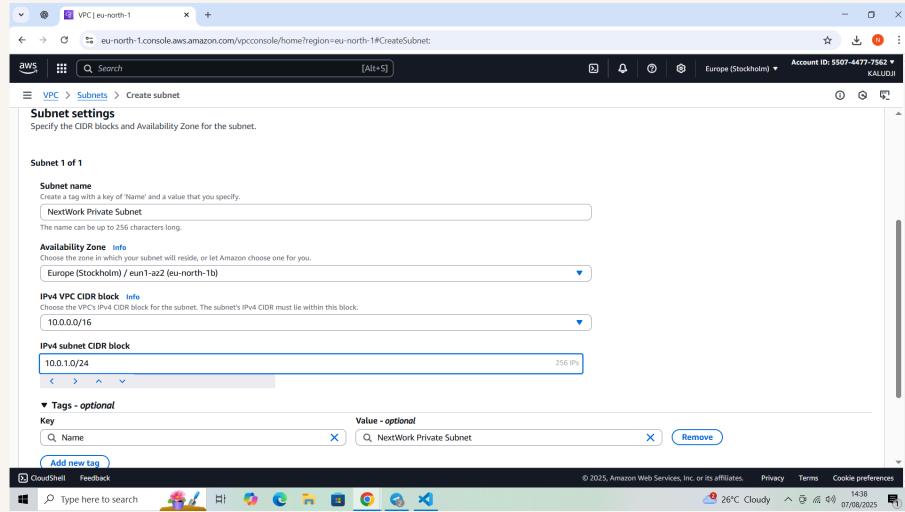




Creating a Private Subnet

N

Nchindo Boris





Introducing Today's Project!

What is Amazon VPC?

Amazon Virtual Private is a service that lets you create your own private, isolated network within the cloud. It is useful to control internet access

How I used Amazon VPC in this project

Amazon VPC was used in today's project to create; Private subnets Routing Security (via security groups and NACLs) Internet access (via gateways)

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

I did not expect that this project will be this easy

This project took me...

It took me 1hr to complete this project

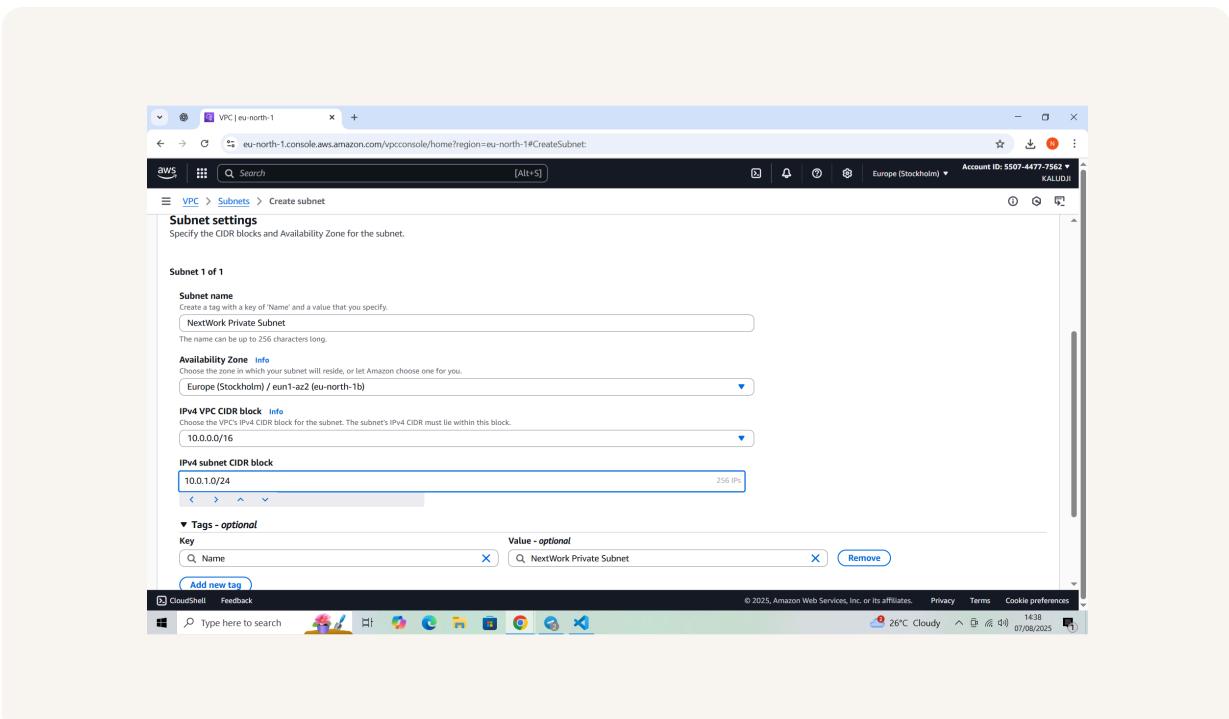


Private vs Public Subnets

The difference between public and private subnets internet access. Public Subnet has direct internet access while Private Subnet does not have direct internet access

Having private subnets are useful because improve security, control, and architectural design in cloud environments. This protects sensitive data

My private and public subnets cannot have the same Internet Gateway and route table





A dedicated route table

By default, my private subnet is associated with the VPC's main route table

I had to set up a new route table because I want to control routing separately from public subnets and keep the Private Subnet Isolated From the Internet

My private subnet's dedicated route table only has one inbound and one outbound rule that allows Local Traffic Inside the VPC and No Internet Access by Default

The screenshot shows the AWS VPC Route Tables console. The left sidebar navigation includes 'VPC dashboard', 'EC2 Global View', 'Virtual private cloud' (with 'Your VPCs', 'Subnets', 'Route tables' selected), 'Egress-only Internet gateways', 'DHCP option sets', 'Elastic IP', 'Managed prefix lists', 'NAT gateways', 'Peering connections', 'Security' (with 'Network ACLs' and 'Security groups'), and 'PrivateLink and Lattice' (with 'Getting started: Updated'). The main content area displays 'Route tables (1/3) info' with three entries:

Name	Route table ID	Explicit subnet associations	Main	VPC
Network Public route table	rtb-04e2497f9e1c0cae8	subnet-07810e0f963f458a2	-	vpc-09994b3a50dd7108f Ne
rtb-08c1fa56bd07642fb	-	-	Yes	vpc-0691831b77710e62f7
NextWork Private Route Table	rtb-0f9a7616b8f4446cb	subnet_028387e4fb88c8...	-	No vpc-09994b3a50dd7108f Ne

Below this, the details for the 'rtb-04e2497f9e1c0cae8 / Network Public route table' are shown:

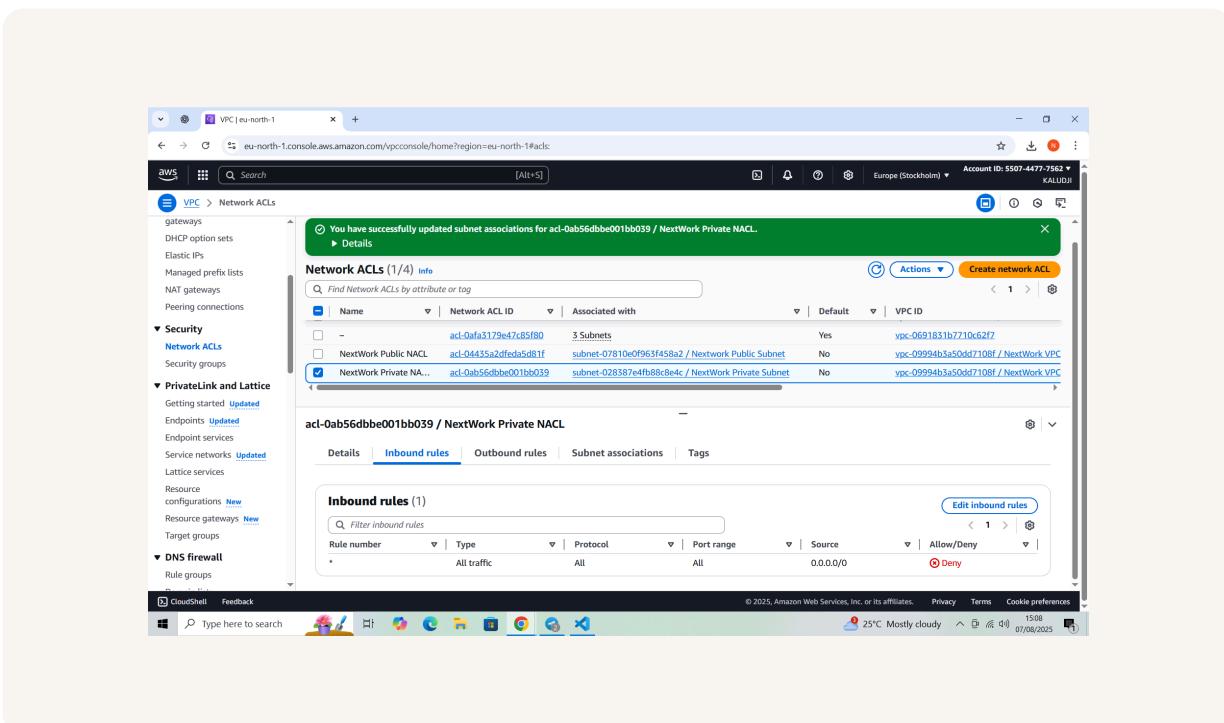
Details			
Route table ID rtb-04e2497f9e1c0cae8	Main Yes	Explicit subnet associations subnet-07810e0f963f458a2 / NextWork Public Subnet	Edge associations -
VPC vpc-09994b3a50dd7108f NextWork VPC	Owner ID 55074477562		

A new network ACL

By default, my private subnet is associated with default network ACL of the VPC

I set up a dedicated network ACL for my private subnet because it will restrict traffic and protect my private subnet

My new network ACL has two simple rules; All inbound and outbound traffic is denied





nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

