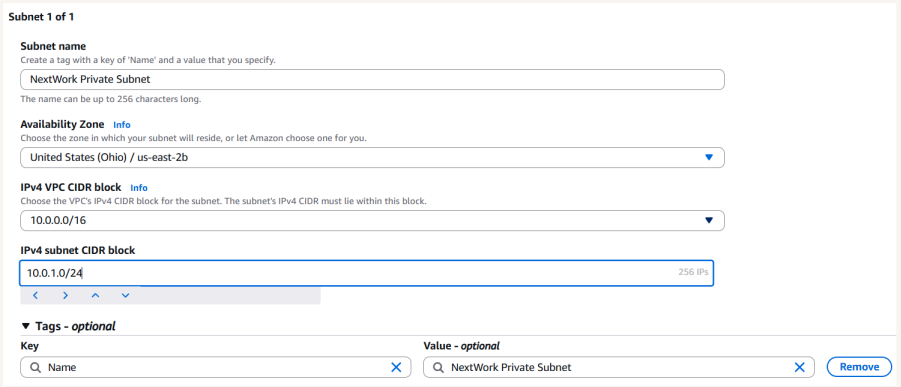
nextwork.org

Creating a Private Subnet

Joba Amunigun
https://www.linkedin.com/in/dvoice



Joba Amunigun
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is a secure, isolated section of the AWS cloud where I can launch and manage resources like EC2 instances, subnets, and route tables. It's useful because it gives me full control over my network — including IP addressing, internet access, routing, and security — so I can design how my cloud environment communicates and stays protected. It's like building your own private neighborhood in the cloud, with your own roads, gates, and security guards.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to design and secure a full network setup in the cloud. I created public and private subnets, configured route tables, added internet gateways, and set up both security groups and custom network ACLs. I also used the AWS CLI to deploy resources across regions and tracked everything using EC2 Global View.

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

One thing I didn't expect was how detailed and layered cloud network security really is. From configuring route tables to setting strict rules in security groups and network ACLs — every layer requires intentional setup. I also didn't expect how careful I'd need to be when using the CLI to clean up resources — one missing step could stop the whole process.

Joba Amunigun
NextWork Student

This project took me...

This project took me about 60 minutes — including time to set up resources, test configurations, troubleshoot CLI cleanup, and reflect on how everything connected.

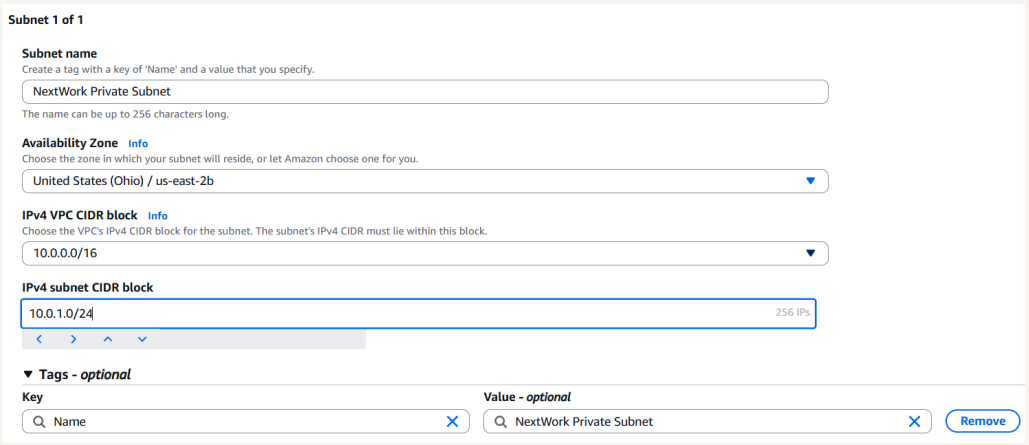
Joba Amunigun
NextWork Student

Private vs Public Subnets

The difference between public and private subnets is that public subnets have a route to the internet through an internet gateway, while private subnets do not. Resources in a public subnet can send and receive traffic from the internet, while those in a private subnet are isolated and typically used for internal services that don't need direct internet access, like databases or backend applications

Having private subnets are useful because they keep sensitive resources — like databases or internal services — hidden from direct internet access. This adds an important layer of security by reducing exposure and limiting access only to trusted, internal systems or public-facing components in other subnets.

My private and public subnets cannot have the same CIDR block— each subnet must have a unique IP address range within the VPC. This ensures that traffic can be routed correctly, without conflicts or overlap, and that each subnet can serve its own purpose (public or private) clearly and securely.

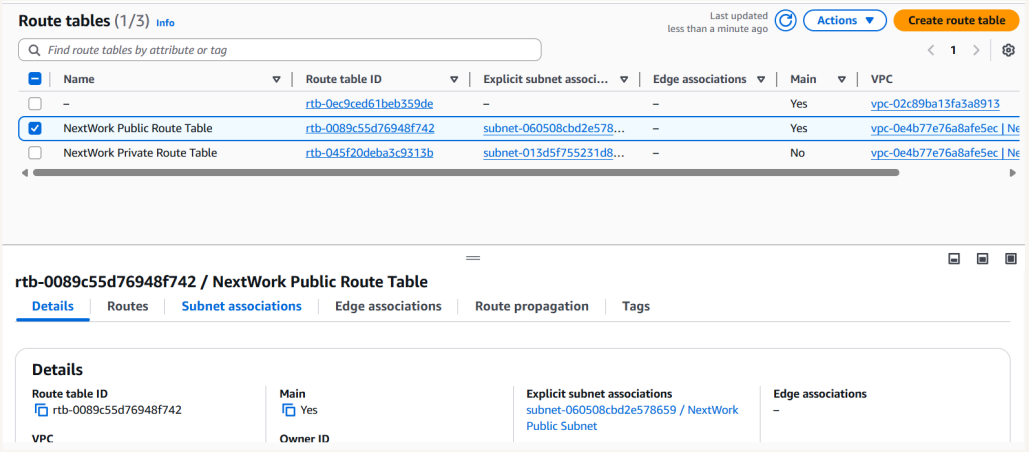

Subnet 1 of 1
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
NextWork Private Subnet
The name can be up to 256 characters long.
Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
United States (Ohio) / us-east-2b
IPv4 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
256 IPs
Tags - optional
Key
Value - optional
Name
NextWork Private Subnet
Remove

A dedicated route table

By default, my private subnet is associated with the main route table of the VPC — which, in my case, is the renamed "NextWork route table". Since this table includes a route to an internet gateway, using it for my private subnet would unintentionally make it public. That's why I needed to create and associate a new route table with no internet routes to keep my private subnet secure.

I had to set up a new route table because my private subnet should not use the default route table — it includes a route to an internet gateway, which would make the subnet public. By creating a separate route table without any internet routes, I can keep the subnet isolated and secure, making it a true private subnet for internal resources.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows local traffic within the VPC — meaning communication between resources inside the same VPC is allowed, but there's no internet access. This keeps the subnet private and isolated, perfect for backend services or sensitive data that shouldn't be exposed to the public.


Route tables (1/3) Info
Last updated less than a minute ago
Actions
Create route table
Find route tables by attribute or tag
1
Name
Route table ID
Explicit subnet associ...
Edge associations
Main
VPC
– rtb-0ec9ced61beb359de – – Yes vpc-02c89ba13fa3a8913
NextWork Public Route Table rtb-0089c55d76948f742 subnet-060508cbd2e578... – Yes vpc-0e4b77e76a8afe5ec | Ne
NextWork Private Route Table rtb-045f20deba3c9313b subnet-013d5f755231d8... – No vpc-0e4b77e76a8afe5ec | Ne
rtb-0089c55d76948f742 / NextWork Public Route Table
Details
Routes
Subnet associations
Edge associations
Route propagation
Tags
Details
Route table ID
rtb-0089c55d76948f742
Main
Yes
Explicit subnet associations
subnet-060508cbd2e578659 / NextWork Public Subnet
Edge associations
–
VPC
Owner ID

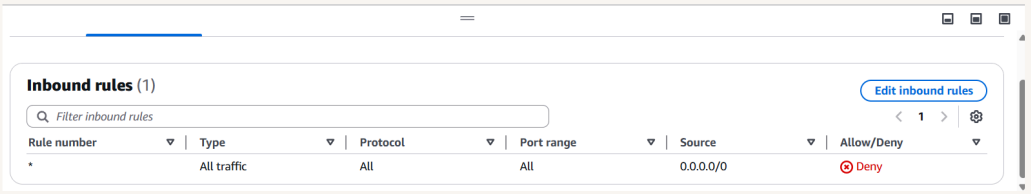
A new network ACL

By default, my private subnet is associated with the default Network ACL that came with my VPC. This default NACL allows all inbound and outbound traffic, unless I choose to modify its rules. While it doesn't block traffic initially, it's good practice to create a custom NACL later for stricter control over what enters and leaves the subnet.

I set up a dedicated network ACL for my private subnet because the default network ACL allows all inbound and outbound traffic, which leaves the subnet exposed to unrestricted access. Since I hadn't explicitly associated my private subnet with any other ACL, it was still using the default one. Creating a new custom network ACL gives me tighter control over what traffic is allowed — helping me protect my private subnet from unnecessary exposure

My new network ACL has two simple rules — both set to deny all traffic: Inbound Rule: Denies all incoming traffic, blocking access to the subnet from external sources. Outbound Rule: Denies all outgoing traffic, preventing the subnet from initiating any external communication.

Joba Amunigun
NextWork Student



The place to learn & showcase your skills

Check out nextwork.org for more projects