



Creating a Private Subnet



Jonathan Nutsugah

subnet-0874ceec16bc4dcf6 / Private 1

Details

Subnet ID	<input type="button" value="subnet-0874ceec16bc4dcf6"/>	Subnet ARN	<input type="button" value="arn:aws:ec2:us-east-1:248189930152:subnet/subnet-0874ceec16bc4dcf6"/>
IPv4 CIDR	<input type="button" value="192.168.1.16/28"/>	Available IPv4 addresses	<input type="button" value="11"/>
Availability Zone	<input type="button" value="us-east-1b"/>	Availability Zone ID	<input type="button" value="use1-az1"/>
Route table	<input type="button" value="rtb-0863f504d821dceb5 SacNet Route Table"/>	Network ACL	-
Auto-assign IPv6 address	No	Auto-assign customer-owned IPv4 address	No
IPv4 CIDR reservations	-	IPv6 CIDR reservations	-
Resource name DNS A record	Disabled	Resource name DNS AAAA record	Disabled



Jonathan Nutsugah

NextWork Student

nextwork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) lets you create a secure, isolated network in AWS where you control IP ranges, subnets, and traffic. It's useful for customizing network setup, enhancing security, and supporting hybrid cloud deployments.

How I used Amazon VPC in this project

Through the management console, I used it to virtually isolate a space to keep my resources away from external access.

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

How easy it is to navigate AWS.

This project took me...

40 minutes.

Jonathan Nutsugah

NextWork Student

nextwork.org

Private vs Public Subnets

The difference between public and private subnets is that public subnets have access to the internet through an internet gateway, while private subnets do not have direct internet access and are typically used for internal resources like databases.

Having private subnets is useful because they enhance security by isolating sensitive resources (like databases or internal services) from direct internet access, reducing the risk of external attacks.

My private and public subnets cannot have the same range of IP addresses.

subnet-0874ceec16bc4dcf6 / Private 1

Details

Subnet ID
[subnet-0874ceec16bc4dcf6](#)

IPv4 CIDR
[192.168.1.16/28](#)

Availability Zone
[us-east-1b](#)

Route table
[rtb-0863f504d821dceb5 | SacNet Route Table](#)

Auto-assign IPv6 address
No

IPv4 CIDR reservations
—

Resource name DNS A record
Disabled

Subnet ARN

[arn:aws:ec2:us-east-1:248189930152:subnet/subnet-0874ceec16bc4dcf6](#)

Available IPv4 addresses

[11](#)

Availability Zone ID

[use1-az1](#)

Network ACL

—

Auto-assign customer-owned IPv4 address
No

IPv6 CIDR reservations

—

Resource name DNS AAAA record
Disabled

Jonathan Nutsugah

NextWork Student

nextwork.org

A dedicated route table

By default, my private subnet is associated with the local target route.

I had to set up a new route table because the other route table will direct traffic to the internet, and we do not want that.

My private subnet's dedicated route table has only one inbound and one outbound rule, which allows traffic to flow only within the local network.

The screenshot shows the AWS Route Table details page for the route table **rtb-06627576642a3f56f / SacNet Private Route Table**. The page is divided into several sections:

- Details** (Info):
 - Route table ID: [rtb-06627576642a3f56f](#)
 - VPC: [vpc-0a80bd992fb168a73 | SacNet](#)
 - Main: No
 - Owner ID: [248189930152](#)
 - Explicit subnet associations:
 - [subnet-0874ceec16bc4dcf6 / Private 1](#)
- Routes**:
 - Routes (1)
 - Destination: 192.168.1.0/24
 - Target: local
 - Status: Active

Jonathan Nutsugah

NextWork Student

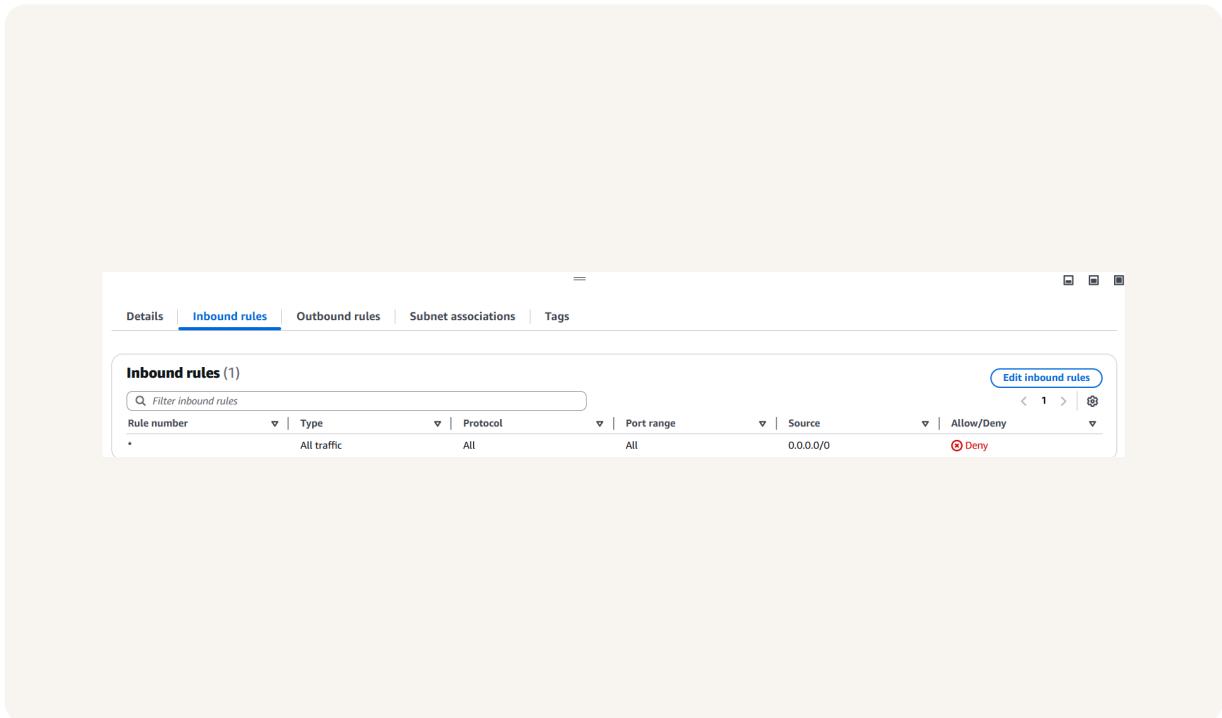
nextwork.org

A new network ACL

By default, my private subnet is associated with the default NACL created for the VPC.

I set up a dedicated network ACL for my private subnet because I want to deny all traffic for now until I am sure which traffic to allow.

My new network ACL has two simple rules - Deny all traffic, both inbound and outbound.





nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

