



nextwork.org

Creating a Private Subnet



saqibh49@gmail.com

The screenshot shows the AWS VPC Subnets console with the following details:

Subnet ARN: arn:aws:ec2:us-east-1:510482603806:subnet/subnet-08346a1012c6eb532

IPv4 CIDR: 10.0.1.0/24

Available IPv4 addresses: 251

Network border group: us-east-1

Auto-assign customer-owned IPv4 address: No

IPv6 CIDR reservations: -

Resource name DNS AAAA record: Disabled

State: Available

IPv6 CIDR: -

VPC: vpc-099268cd4891b2c1f | network vpc

Default subnet: No

Customer-owned IPv4 pool: -

IPv6-only: No

Hostname type: IP name

Outpost ID: -

Owner: 510482603806

Block Public Access: Off

IPv6 CIDR association ID: -

Route table: rtb-0ba34292d39560cdd | NextWork route table

Auto-assign IPv6 address: No

IPv4 CIDR reservations: -

Resource name DNS A record: Disabled

Flow logs: No flow logs found

Actions: Create flow log

CloudShell Feedback Console Mobile App

saqibh49@gmail.com

NextWork Student

nextwork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a virtual network in AWS that lets you create an isolated cloud environment to launch and manage your resources, and it is useful because it gives you control over IP addressing, subnets, routing, and security to protect and organize your infrastructure.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create a private subnet, along with a route table, and network ACL.

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

One thing I didn't expect in this project is that a private subnet is exactly the same as a public subnet, just without the internet gateway.

This project took me...

This project took me 30 minutes

saqibh49@gmail.com

NextWork Student

nextwork.org

Private vs Public Subnets

The difference between public and private subnets is that private subnets do not have an internet gateway connected to their route tables, so outside access is not allowed or possible. Public subnets have an internet gateway attached to their route table so outside internet access is available.

Having private subnets are useful because they work as the backend for the frontend parts of VPC housed in public subnets. For example, an S3 site might be stored in a public subnet, but all the customer data might be stored in a private subnet.

My private and public subnets cannot have the same CIDR blocks.

saqibh49@gmail.com

NextWork Student

nextwork.org

AWS Global View [Option+Shift] United States (N. Virginia) Saqib Hossain (S104-8260-3806)

VPC > Subnets > subnet-08346a1012c6eb332

subnet-08346a1012c6eb332 / NextWork Private Subnet

Details

Subnet ID	arn:aws:ec2:us-east-1:510482603806:subnet/subnet-08346a1012c6eb332	State	Available
IPv4 CIDR	10.0.1.0/24	IPv6 CIDR	-
Availability Zone	use1-a2z (us-east-1b)	VPC	vpc-099268cd4891b2cf network route table rtb-0ba34292d39360cdd NextWork route table
Network ACL	acl-065ac8d720d41031e	Auto-assign public IPv4 address	No
Auto-assign customer-owned IPv4 address	No	Outpost ID	-
IPv6 CIDR reservations	-	Hostname type	IP name
Resource name DNS AAAA record	Disabled	Owner	510482603806
IPv6-only	No	IPv4 CIDR reservations	-
DNS64	Disabled	Resource name DNS A record	Disabled

Flow logs No flow logs found

© 2026, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

saqibh49@gmail.com

NextWork Student

nextwork.org

A dedicated route table

By default, my private subnet is associated with the public route table I built earlier, or if no route tables built by me exist, then it will use the default one that AWS includes in the account.

I had to set up a new route table because the public route table has a connection to an internet gateway, but the private subnet needs to be self contained so only internal traffic gets through.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows local traffic, nothing from the internet

saqibh49@gmail.com

NextWork Student

nextwork.org

The screenshot shows the AWS VPC Route Table configuration page. The route table ID is rtb-026b37bf87f82c944. The main section displays details such as the route table ID, owner ID, and explicit subnet associations. A single route entry is listed, pointing to a local target with an active status. The left sidebar provides navigation links for various VPC components like Route tables, Internet gateways, and Security groups.

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	Create Route Table

saqibh49@gmail.com

NextWork Student

nextwork.org

A new network ACL

By default, my private subnet is associated with the Network ACL associated with your private route subnet by default is the VPC's default Network ACL, which automatically allows all inbound and outbound traffic unless you modify it.

I set up a dedicated network ACL for my private subnet because this acts as an extra form of security alongside the route table not being connected to an internet gateway.

My new network ACL has two simple rules - All inbound traffic is blocked, and all outbound traffic is blocked.

The screenshot shows the AWS VPC Network ACL details page for 'acl-0f92b3b085bf500d0 / NextWork Private NACL'. The 'Inbound rules' section displays a single 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

