



Creating a Private Subnet

G

Gaurav Balpande

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

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.

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.

IPv4 subnet CIDR block
 256 IPs

Tags - optional

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="dray-private-subnet"/>

[Add new tag](#) You can add 49 more tags.
[Remove](#)

[Add new subnet](#)

[Cancel](#) [Create subnet](#)

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is the foundation networking tool in AWS used to create private space within the Amazon region to provide security and to easily manage the resources.

How I used Amazon VPC in this project

In today's project, I had created private subnet, private ACL and private route table.

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

One thing I didn't expect was to provide different route table and ACL for private subnet.

This project took me...

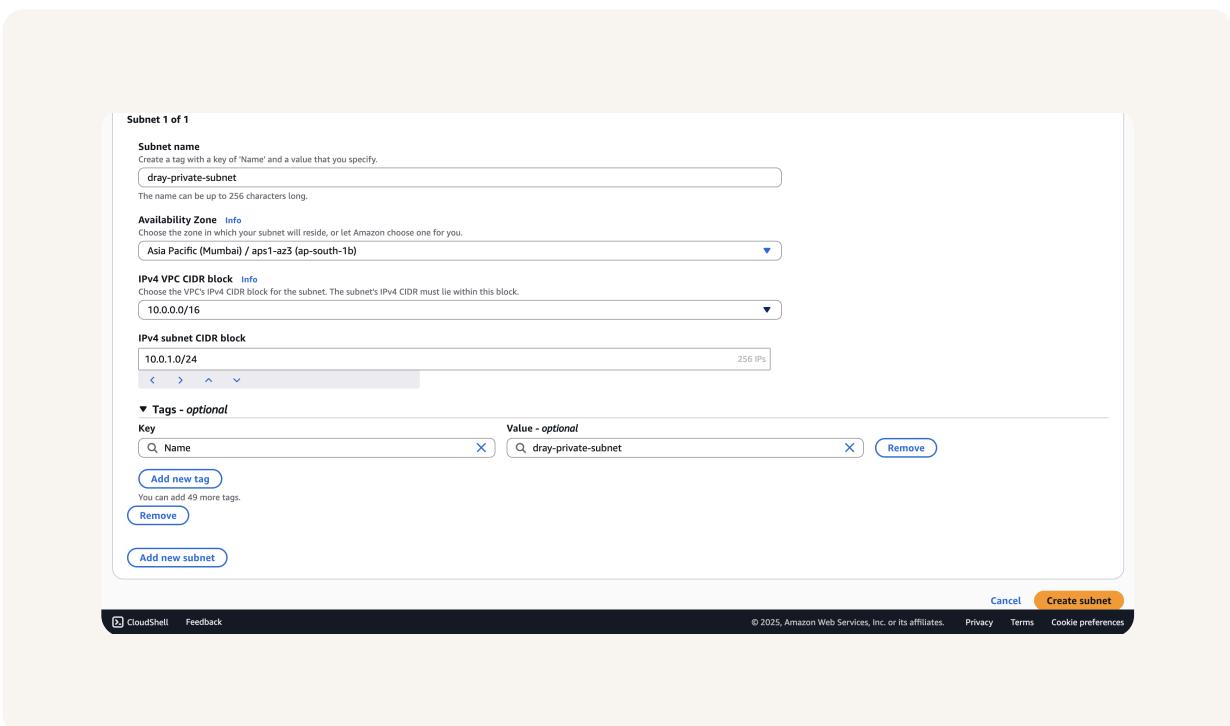
It's an easy project, took nearly 1 hr.

Private vs Public Subnets

The difference between public and private subnets is that public subnet resources are directly accessed by internet but private subnet resources can't.

Having private subnets are useful because there might be some services where we want security and don't want to be available to all through internet.

My private and public subnets cannot have the same IPv4 VPC CIDR block because it's like having same name for address which will cause conflict.



A dedicated route table

By default, my private subnet is associated with the VPC for the local connection.

I had to set up a new route table because public and private cant have the same route table as in public there is connection for internet but in private it has local connection for connection between resources.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows the connection between local resources.

The screenshot shows the AWS VPC Route Tables page. On the left, the navigation pane includes links for VPC dashboard, EC2 Global View, Filter by VPC, Virtual private cloud (Your VPCs, Subnets, Route tables), Security (Network ACLs, Security groups), and PrivateLink and Lattice (Getting started, Endpoints, Endpoint services, Service networks). The main content area displays the 'Route tables (1/3) Info' section. A table lists three route tables:

Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
-	rtb-04de95d9cb7d5388	-	-	Yes	vpc-0e31a0fce5945ca
<input checked="" type="checkbox"/> dray-private-route-table	rtb-0785a3eae5585ef3f	-	-	No	vpc-09c10688fa32c7c
-	rtb-08c201ec03f502946	-	-	Yes	vpc-09c10688fa32c7c

The 'dray-private-route-table' row is selected. Below it, the details for 'rtb-0785a3eae5585ef3f / dray-private-route-table' are shown. The 'Routes' tab is active, displaying one route:

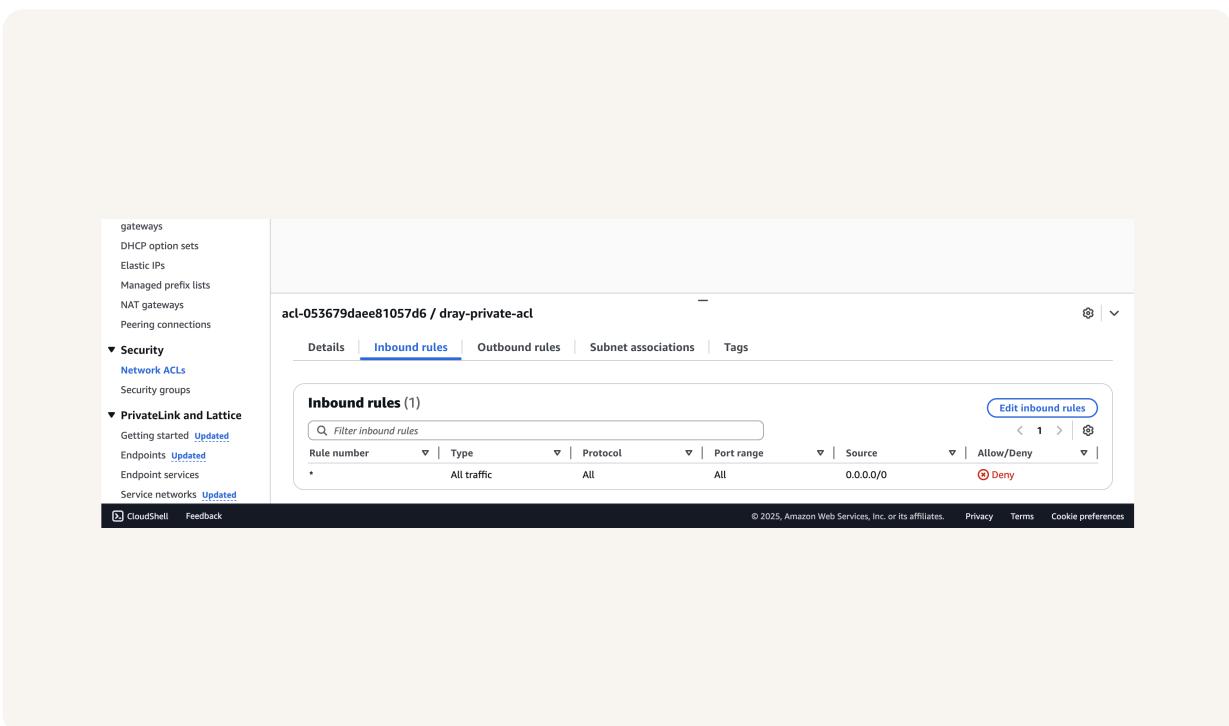
Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

A new network ACL

By default, my private subnet is associated with default ACL which deny all inbound and outbound traffic.

I set up a dedicated network ACL for my private subnet because we don't want any connection with the internet and for ACL of public subnet there is internet connection.

My new network ACL has two simple rules - 1. deny all inbound traffic.. 2. deny all outbound traffic.





nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

