

Build a Private Subnet

By Haroon Zaman | November 2025

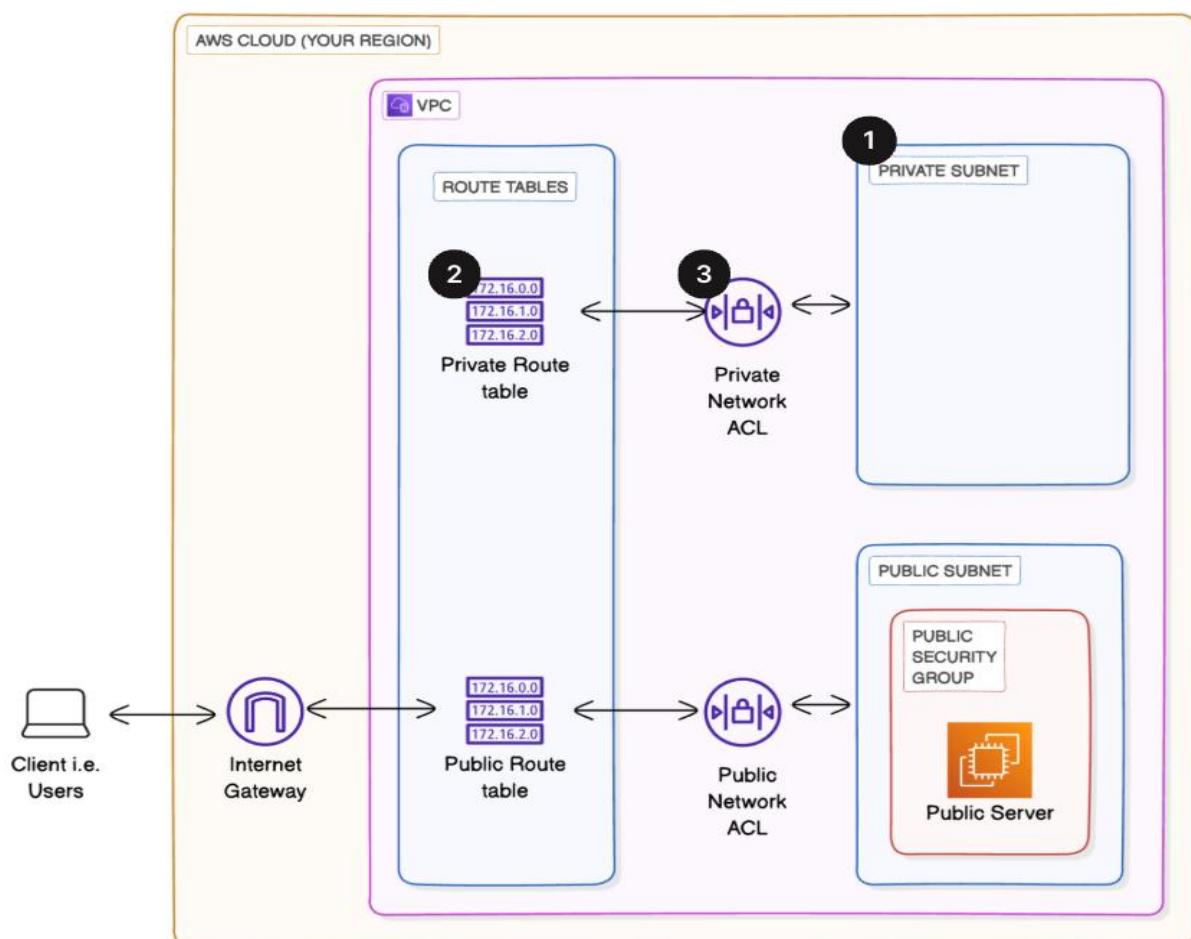
Introduction

I completed this project to deepen my understanding of AWS networking and secure cloud design. After building a public subnet and enabling internet access, my goal was to learn how to create a **private network** inside AWS where resources are **not exposed to the internet** and can only communicate internally.

This step is essential for hosting secure resources such as **databases, backend services, or internal applications**.

In this project, I completed the following tasks:

- **Created a Private Subnet** – A subnet that does not provide internet access, ensuring security and isolation for internal resources.
- **Created a Private Route Table** – I set up routing rules so that resources in the private subnet only communicate within the VPC.
- **Created a Private Network ACL** – I added extra security to control inbound and outbound traffic using allow/deny rules.



Private Subnet

A **private subnet** is a subnet inside a VPC that **does not have direct access to the internet**. It is used to host services that should remain internal and secure—for example, databases or backend servers that should not be publicly reachable.

Unlike a public subnet, a private subnet **does not route traffic to an internet gateway**.

To build my private subnet, I had to:

- Select my existing VPC.
- Define a new IPv4 CIDR block for the private subnet.
- Ensure that **no public IPs are automatically assigned**.
- Create a **private route table** that prevents internet access.
- Add a **custom network ACL** to control inbound and outbound traffic securely.

This setup helps maintain strong security and teaches how real-world cloud architectures separate **public and private resources** for best practices.

The screenshot shows the AWS VPC Subnets creation interface. At the top, there's a breadcrumb navigation: **VPC > Subnets > Create subnet**. The main section is titled **VPC**, with a **VPC ID** dropdown containing `vpc-0e69c4b80354b0e63 (My_Network_VPC)`. Below this is a **Associated VPC CIDRs** section with an **IPv4 CIDRs** dropdown containing `10.0.0.0/16`. The next section is titled **Subnet settings**, which says "Specify the CIDR blocks and Availability Zone for the subnet". It contains a **Subnet 1 of 1** section with a **Subnet name** input field containing `My_Private_Subnet`. Below it is an **Availability Zone** dropdown set to `No preference`. Under **IPv4 VPC CIDR block**, the dropdown shows `10.0.0.0/16`. Under **IPv4 subnet CIDR block**, the dropdown shows `10.0.1.0/24` with a note indicating 256 IPs available. There are also navigation arrows for selecting CIDR blocks.

First, I went to the **VPC console** and selected **Subnets** from the left panel. Then I clicked on **Create subnet**.

- I selected my existing VPC: **MY_NETWORK_VPC**.
- I named the subnet **My_Private_Subnet**.
- For **Availability Zone**, I chose **No Preference**, which allows AWS to automatically assign a zone.

- In the **IPv4 subnet CIDR block**, I used **10.0.1.0/24**, which is part of my main VPC CIDR range (10.0.0.0/16), ensuring the subnet stays within the VPC network.

After configuring these settings, I clicked on **Create Subnet** to successfully create my private subnet.

Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - optional
Create a tag with a key of 'Name' and a value that you specify.

VPC
The VPC to use for this route table.

Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
<input type="text" value="Q_Name"/>	<input type="text" value="Q_My_Private_RTable"/> <input type="button" value="Remove"/>

You can add 49 more tags.

Creating a Private Route Table

After creating **My_Private_Subnet**, I proceeded to set up a private route table for it. I opened the **VPC console** and selected **Route Tables** from the left-side panel. Then I clicked on **Create route table**.

- I named it **My_Private_RTable**.
- I selected my VPC: **MY_NETWORK_VPC**.

Once the details were filled, I clicked **Create route table** to complete the setup.

rtb-0650e5a316b4c94bd / My_Private_RTable Actions ▾

Details Info

Route table ID <input type="text" value="rtb-0650e5a316b4c94bd"/>	Main <input checked="" type="checkbox"/> No	Explicit subnet associations —	Edge associations —
VPC <input type="text" value="vpc-0e69c4b80354b0e63 My_Network_VPC"/>	Owner ID <input type="text" value="377721963177"/>		

Routes **Subnet associations** **Edge associations** **Route propagation** **Tags**

Routes (1) Both ▾ Edit routes

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	<input checked="" type="checkbox"/> Active	No	Create Route Table

After creating **My_Private_RTable**, I checked the routes inside it. I noticed that there was already a default route with **Destination: 10.0.0.0/16** and **Target: local**.

Routes **Subnet associations** **Edge associations** **Route propagation** **Tags**

Explicit subnet associations (1) Edit subnet associations

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
My_Private_Subnet	<input type="text" value="subnet-09751e0e45a3b4fd"/>	10.0.1.0/24	—

I selected **My_Private_RTable**, went to the **Subnet Associations** tab, clicked **Edit associations**, and selected **My_Private_Subnet**. After saving, the subnet was officially using this private route table — confirming it as a **private subnet** with no internet access.

Create network ACL Info

A network ACL is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet.

Network ACL settings

Name - optional
Creates a tag with a key of 'Name' and a value that you specify.

VPC
VPC to use for this network ACL.

Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
<input type="text" value="Q Name"/>	<input type="text" value="Q My_Private_ACL"/> X Remove tag
Add tag	

You can add 49 more tags

Cancel Create network ACL

Creating a Private Network ACL

- Next, I created the **private ACL** for my subnet.
- In the **VPC console**, I went to **Network ACLs** and clicked **Create Network ACL**.
- I entered the name **My_Private_ACL**.
- I selected the appropriate **VPC (MY_Network_VPC)**.
- Finally, I clicked **Create** to finish the setup.

acl-0e46cd94eee7b8c99 / My_Private_ACL Actions ▾

Details		Associated with	Default	VPC ID
Network ACL ID acl-0e46cd94eee7b8c99	Associated with —	Default No	VPC ID vpc-0e69c4b80354b0e63 / My_Network_VPC	
Owner 377721963177				

Inbound rules Outbound rules Subnet associations Tags

Inbound rules (1)

Edit inbound rules						
Filter inbound rules						
Rule number	Type	Protocol	Port range	Source	Allow/Deny	
*	All traffic	All	All	0.0.0.0/0	Deny	✖

- After creating the **My_Private_ACL**, I reviewed the rules section.
- Both the **inbound and outbound rules were set to DENY by default**.
- I did **not modify any rules** because this subnet is meant to be fully private.
- Later, if I deploy resources inside this subnet, I will **add rules according to my needs**.
- For now, the subnet remains **fully isolated and not accessible from the internet** — which is the purpose of a private subnet.

The screenshot shows the AWS Network ACL details page for 'acl-0e46cd94eee7b8c99 / My_Private_ACL'. It includes sections for Details, Info, and Subnet associations. The Subnet associations tab is selected, showing one association between the ACL and the 'My_Private_Subnet' (subnet-09751e0e45a3b4fd3). The VPC ID is 'vpc-0e69c4b80354b0e63 / My_Network_VPC'. The table lists the subnet ID, associated ACL, availability zone, and IPv4 CIDR.

Name	Subnet ID	Associated with	Availability Zone	IPv4 CIDR	IPv6 CIDR
My_Private_Subnet	subnet-09751e0e45a3b4fd3	acl-0e46cd94eee7b8c99 / My_Private_...	eun1-a21 (eu-north-1a)	10.0.1.0/24	-

- After creating the **My_Private_ACL**, I went to the **Subnet Associations** tab.
- I clicked on **Edit subnet associations**.
- A list of subnets appeared — from there, I selected **My_Private_Subnet**.
- Then I clicked **Save** to confirm the association.
- Now, **My_Private_Subnet is protected by my custom Private NACL**, keeping it fully secure and isolated.

Conclusion

Through this project, I successfully created a **private subnet**, a **private route table**, and a **custom network ACL**, strengthening the security of my VPC. This helped me understand how resources can be **fully isolated from the internet** while still existing inside the same VPC. I also learned the difference between **public and private subnets**, and how routing and access rules control communication in AWS.

Working with custom ACLs and route tables gave me hands-on experience with **network segmentation, access control, and secure architecture design**. This project taught me how to build a **secure cloud environment**, preparing me for more advanced AWS networking and real-world cloud deployments.