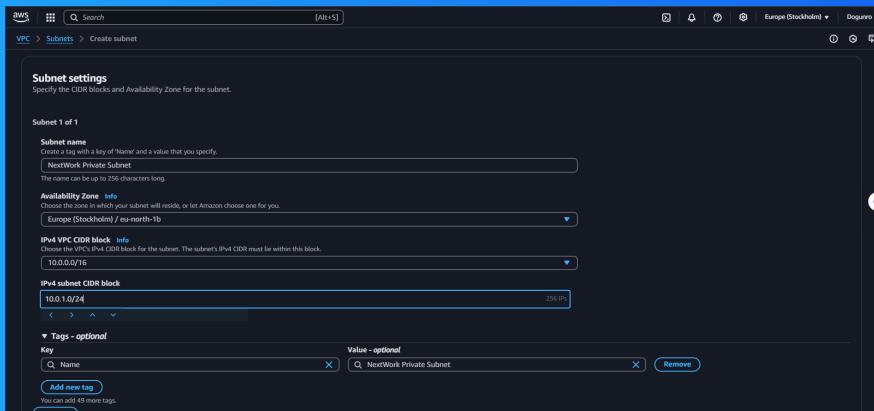




Creating a Private Subnet

 Honesty Dogunro





Introducing Today's Project!

What is Amazon VPC?

Amazon VPC provides a private, secure network on AWS, enabling control over traffic, IP ranges, and isolation for sensitive data.

How I used Amazon VPC in this project

I used Amazon VPC to create a secure network for today's project, customizing subnets and routing to control traffic flow and isolate resources for enhanced security.

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

I didn't expect how much fine-tuning was needed for VPC configurations, like setting up custom subnets and security groups to ensure seamless communication and security.

This project took me...

This project took me about 2 hours to complete, including planning, configuring the VPC, and testing the setup.

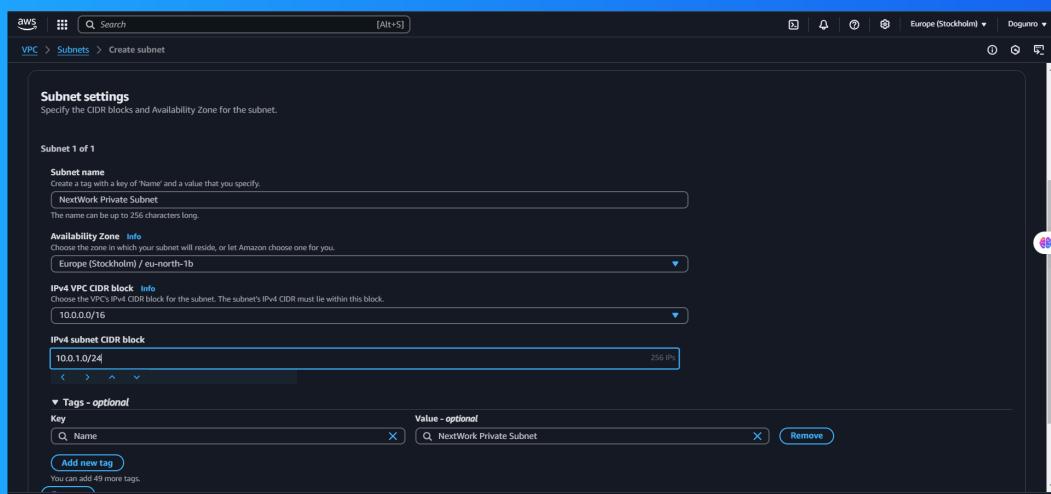


Private vs Public Subnets

The difference between public and private subnets is that public subnets are accessible from the internet, while private subnets are not and use private IP addresses for internal communication.

Having private subnets are useful because they enhance security by isolating resources from direct internet access, reducing exposure to threats, and allowing for better control over internal traffic and communication within a network.

My private and public subnets cannot have the same IP address range. This separation ensures proper routing, avoids conflicts, and maintains clear boundaries between internal and external network resources.





A dedicated route table

By default, my private subnet is associated with the main route table of the VPC. This route table includes local routes for communication within the VPC but does not have routes for internet access.

I had to set up a new route table because I needed to customize routing for specific subnets, enabling access to different resources or internet connectivity while isolating traffic according to security and performance requirements.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows local traffic within the VPC, enabling communication with other subnets while blocking internet access for enhanced security.

The screenshot shows the AWS VPC dashboard with the 'Route tables' section selected. A success message at the top indicates that subnet associations were updated for the new route table. The table lists three route tables: 'NextWork Public Route Table', 'rtb-004e925219a751b92', and 'NextWork Private Route Table'. The 'NextWork Private Route Table' is highlighted, showing its details: Route Table ID is 'rtb-04cc1b3fa1c3daf8d', it is associated with 'subnet-01e86d0d6b27165a2 / NextWork Private Subnet', and it is not the 'Main' route table. The 'Details' tab is selected, showing the VPC is 'vpc-04ff1496c16698071 | NextWork VPC' and the Owner ID is '851725458922'. The 'Routes' tab is also visible.



A new network ACL

By default, my private subnet is associated with the default Network Access Control List (NACL), which allows all inbound and outbound traffic. You can customize it for specific security needs later if required.

I set up a dedicated network ACL for my private subnet because I want to implement specific security rules to control inbound and outbound traffic, enhancing protection and managing access more effectively for my resources.

My new network ACL has two simple rules: denial of all inbound traffic and denial of all outbound traffic.

The screenshot shows the AWS VPC dashboard with the 'Network ACLs' section selected. A new NACL named 'NextWork Private NACL' is being created for a specific private subnet. The 'Inbound rules' tab is active, displaying a single rule that denies all traffic. The 'Outbound rules' tab is also visible.

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count
acl-001e8c945011e6956	-	3 Subnets	Yes	vpc-0b2879326ca84af93	2 Inbound rules
acl-05758fb088da5eb62	-	-	Yes	vpc-04f11495c16698071 / NextWork VPC	2 Inbound rules
NextWork Public NACL	acl-09a5abafcc02e611b	subnet-057f9a449b8206012 / NextWork Public...	No	vpc-04f11495c16698071 / NextWork VPC	2 Inbound rules
NextWork Private NACL	acl-0f490ec5698277f4a	subnet-01e86d0dfb27165a2 / NextWork Priva...	No	vpc-04f11495c16698071 / NextWork VPC	1 Inbound rule



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for
more projects

