



Creating a Private Subnet

K

KELLY NKWAIN

The screenshot shows the AWS VPC Network ACLs configuration page. A green success message at the top states: "You have successfully updated subnet associations for acl-0aebd512564df2b61 / NextWork Network ACL." Below this, the "Details" section shows a table of Network ACLs:

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count
acl-01703ebd52f2467b	-	6 Subnets	Yes	vpc-082ee7556adcbff2	2 Inbound rules
acl-023fe28ef4acfbec	-	-	Yes	vpc-03133279a3f71ea1f / NextWork VPC	2 Inbound rules
NextWork Network A...	acl-0aebd512564df2b61	subnet-0690ec2d7ad4c7ba5 / Public 1	No	vpc-03133279a3f71ea1f / NextWork VPC	2 Inbound rules

Below the table, the specific Network ACL "acl-0aebd512564df2b61 / NextWork Network ACL" is selected. The "Inbound rules" tab is active, showing the following rule:

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is your own private network within a cloud infrastructure that helps you contain and control your own resources

How I used Amazon VPC in this project

I use Amazon VPC today to create a private subnet, a private Route table and a private Network ACL

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

This project went on as expected

This project took me...

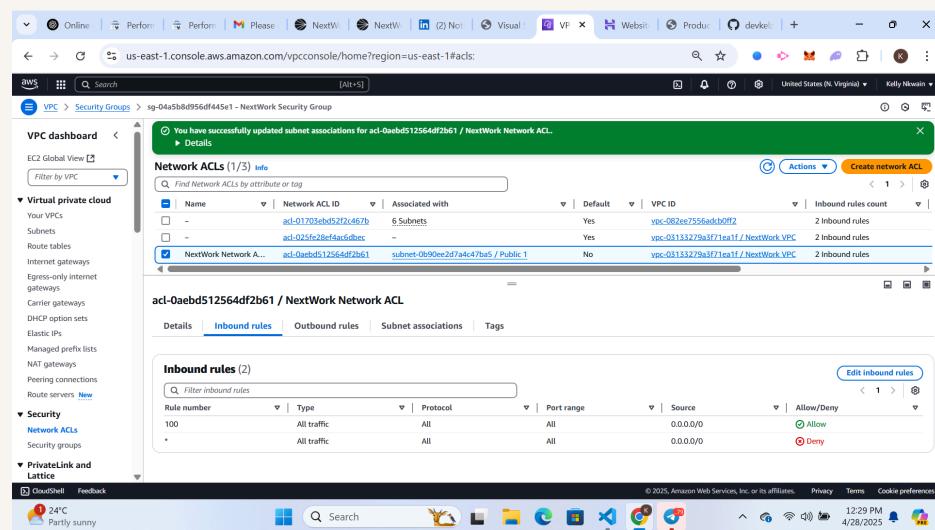
This project took me about 20 minutes

Private vs Public Subnets

The difference between public and private subnets is that the public subnet contains resources that can be accessed by the public while the private subnet contains resources that you want to keep private like databases which store clients details

Having private subnets are useful because they help store private resources therefore providing security. This helps so that only specific people can access your private resources

My private and public subnets cannot have the same network ACL, Route table and gateways



A dedicated route table

By default, my private subnet is associated with my default vpc route table

I had to set up a new route table because my private subnets needs a different route table that doesn't link directly to the internet but can have access to the internet in order to undergo updates and others

My private subnet's dedicated route table only has one inbound and one outbound rule that allows traffic within the VPC and to the internet through a NAT gateway

The screenshot shows the AWS VPC Route Tables page. A modal dialog box is open, indicating that subnet associations have been successfully updated for a specific route table. The table lists four route tables:

Name	Route table ID	Explicit subnet associations	Main	VPC	Owner ID
rtb-0c0e89550be137856	-	-	Yes	vpc-082ee7556ackb0f2	707345500788
NextWork Public route table	rtb-02d6c8d04717b3f5f	subnet-0b90ee2d7a4c47...	No	vpc-05133279a3f71ea1f Next... 	707345500788
-	rtb-05e54960b3102762c	-	Yes	vpc-05133279a3f71ea1f Next...	707345500788
-	rtb-0e25360e5bdff1661	subnet-0cb864499e5802...	No	vpc-05133279a3f71ea1f Next...	707345500788

Below the table, a detailed view of the selected route table (rtb-02d6c8d04717b3f5f) is shown. The 'Details' tab is selected, displaying information such as the route table ID, VPC association, and explicit subnet associations.

A new network ACL

By default, my private subnet is associated with the VPC's default Network ACL

I set up a dedicated network ACL for my private subnet because I want more control over the traffic allowed in and out such as: Restricting inbound access to only trusted IP ranges or services.

My new network ACL has two simple rules 1-Deny all other inbound traffic 2-Deny all other Outbound traffic

The screenshot shows the AWS VPC Network ACLs page. A green success message at the top states: "You have successfully updated subnet associations for acl-04b746c68ccfd320 / NextWork Private NACL." Below this, a table lists three Network ACLs:

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count
-	ad-025f628ef4ac5dbec	-	Yes	vpc-03133279a3f71ea1f / NextWork VPC	2 Inbound rules
NextWork Public NACL	ad-0aeb0512564df2b61	subnet-0b900e2d7a4c47ba5 / NextWork Public...	No	vpc-03133279a3f71ea1f / NextWork VPC	2 Inbound rules
NextWork Private NACL	ad-04b746c68ccfd320	subnet-0cb864499e5802030 / NextWork Privat...	No	vpc-03133279a3f71ea1f / NextWork VPC	1 Inbound rule

Below the table, a section titled "acl-04b746c68ccfd320 / NextWork Private NACL" shows the "Inbound rules" tab. It contains one 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

