



VPC Traffic Flow and Security



Michael Emeruwa

The screenshot shows the AWS VPC Security Groups console. A green success message at the top states: "Security group (sg-0517d7b867b90f0a9 | NextWork Security Group) was created successfully". Below this, the security group details are listed:

Details	
Security group name NextWork Security Group	Security group ID sg-0517d7b867b90f0a9
Owner 41827279624	Description A Security Group for the NextWork VPC
Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry

Below the details, there are tabs for Inbound rules, Outbound rules, Sharing - new, VPC associations - new (which is selected), and Tags.

At the bottom of the screenshot, there is a search bar for VPC associations and buttons for Disassociate VPC and Associate VPC.



Michael Emeruwa
NextWork Student

NextWork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a private network in the cloud. It provides a means to control traffic interaction with data on the network.

How I used Amazon VPC in this project

I created my own Amazon VPC and set up traffic flow and security.

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

I didn't expect the inbound and outbound rules to decline all traffic by default.

This project took me...

40mins



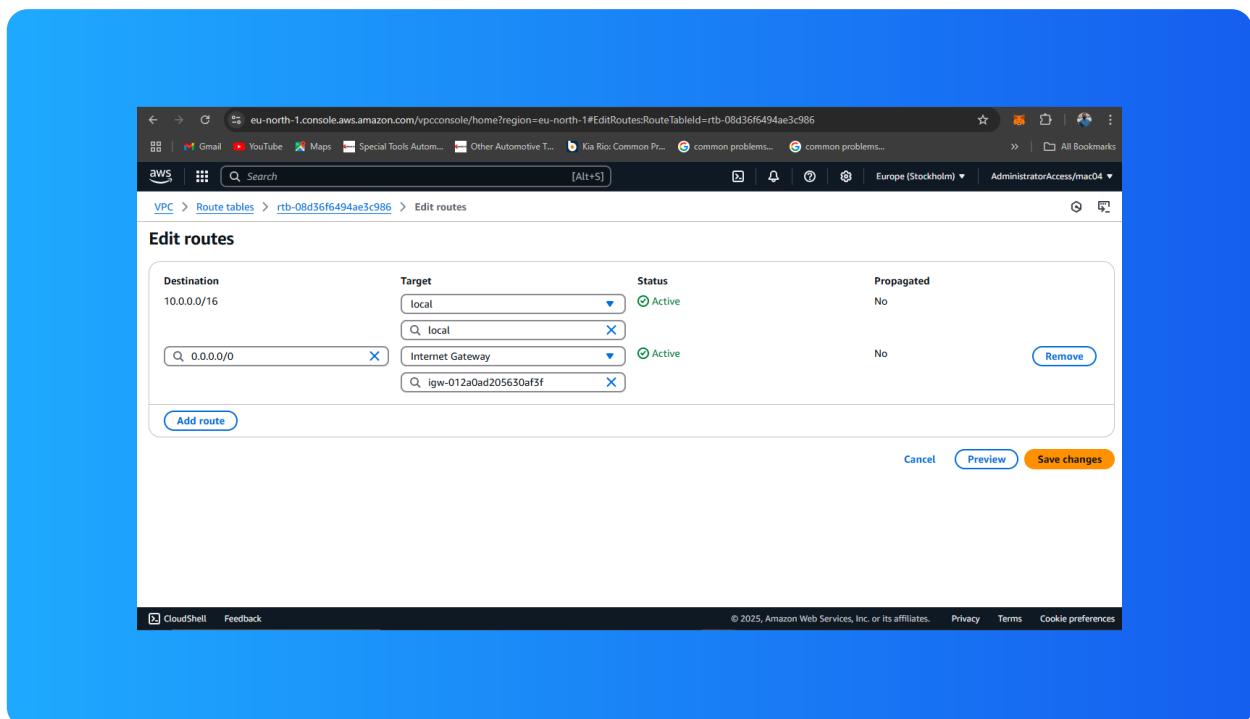
Michael Emeruwa
NextWork Student

NextWork.org

Route tables

Route tables are path ways for resources within the network to share and receive data.

Routes tables are needed to make a subnet public because without it, there's no pathway for incoming traffic. External users would not be able to accesss the data.





Michael Emeruwa
NextWork Student

NextWork.org

Route destination and target

Routes are defined by their destination and target, which mean the IP address range for traffic and the path traffic has to take to get there. The target can either route traffic to the internet or keep traffic within the VPC.

The route in my route table that directed internet-bound traffic to my internet gateway had a destination of 0.0.0.0/0 and a target of igw-012a0ad20563af3f

The screenshot shows the 'Edit routes' interface for a specific route table. A single route is listed:

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	Internet Gateway	Active	No
	igw-012a0ad20563af3f		

Buttons at the bottom include 'Add route', 'Cancel', 'Preview', and 'Save changes' (which is highlighted).

Michael Emeruwa
NextWork Student

NextWork.org

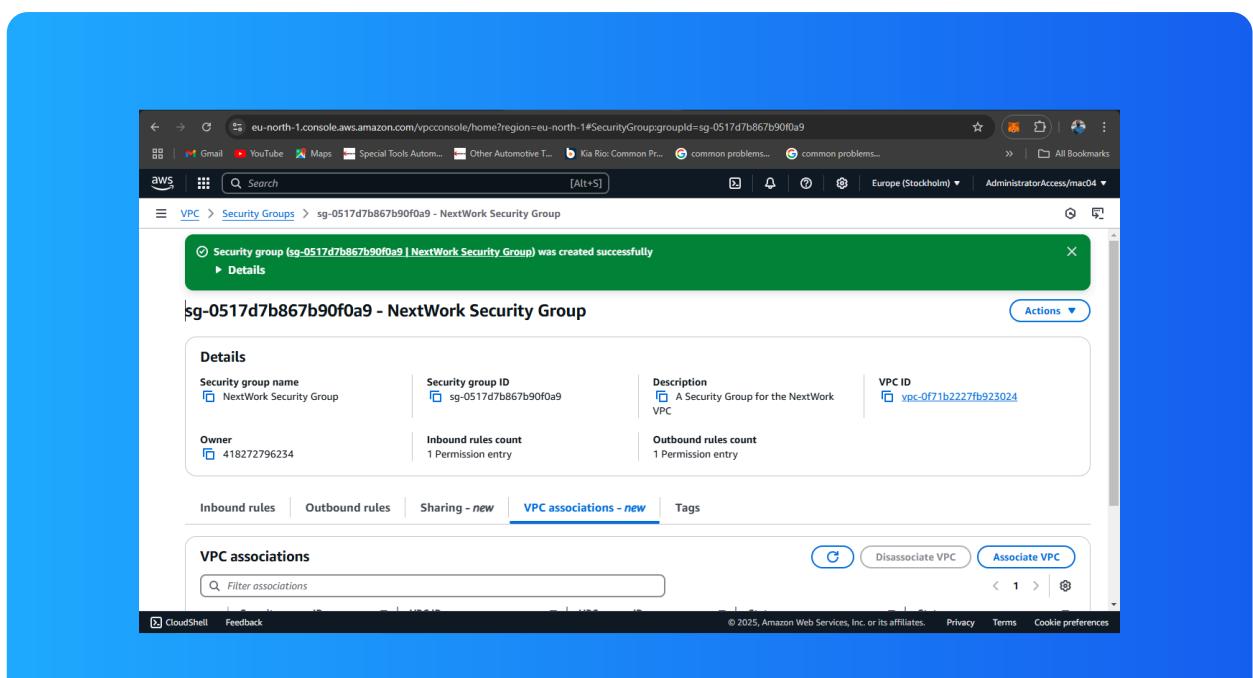
Security groups

Security groups are a means of checking that only protocols, IP addresses that are allowed, are permitted to interact with the resource within a resources.

Inbound vs Outbound rules

Inbound rules are rules that control the data that can enter resources in the security group. I configured an inbound rule that Type: HTTP and Source: Anywhere-IPv4. This means anyone in the public can access my resource.

Outbound rules are rules that control the data the resources send out. By default, my security group's outbound rule allows my resources to send out data.





Michael Emeruwa
NextWork Student

NextWork.org

Network ACLs

Network ACLs are used to set broad traffic rule that apply to entire subnet.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that a Security group is used to control traffic on a granular level, how traffic interacts with a resource, while network ACL controls how traffic interacts with an entire subnet



Michael Emeruwa
NextWork Student

NextWork.org

Default vs Custom Network ACLs

Similar to security groups, network ACLs use inbound and outbound rules

By default, a network ACL's inbound and outbound rules will allow all traffic to enter and leave the subnet.

In contrast, a custom ACL's inbound and outbound rules are automatically set to deny all traffic unless customized.

The screenshot shows the AWS VPC Network ACL details page. A green success message at the top states: "You have successfully updated subnet associations for acl-0052c331d3c8f85c4 / NextWork Network ACL." Below this, the "Details" section shows the Network ACL ID (acl-0052c331d3c8f85c4), Associated with (subnet-0a7a6600f994f1c / Public 1), Owner (418272796234), and VPC ID (vpc-065456fcbb2344458c / NextWork VPC). The "Inbound rules" tab is selected, displaying two rules:

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



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for
more projects

