



[nextwork.org](https://nextwork.org)

# VPC Traffic Flow and Security



ucbethuel

The screenshot shows the AWS CloudFormation console with a modal dialog open. The title of the dialog is "sg-003927a6c939736ad - NextWork Security Group". The "Details" tab is selected. The modal contains the following information:

Details	Security group name	Security group ID	Description	VPC ID
NextWork Security Group	sg-003927a6c939736ad	A Security Group for the NextWork VPC	vpc-0d950959fc7e1d69	
Owner	190680267675	Inbound rules count	1 Permission entry	
		Outbound rules count	1 Permission entry	

OR

**ucbethuel**  
NextWork Student

[nextwork.org](http://nextwork.org)

# Introducing Today's Project!

## What is Amazon VPC?

Amazon VPC is Virtual Private Cloud and it is useful because it wrap all your amazon resources making them private and controllable by you.

## How I used Amazon VPC in this project

In today's project, I used Amazon VPC to connect traffic flow and add some security.

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

One thing I didn't expect in this project was it easy demonstration and practice.

## This project took me...

This project took me 2 hours.

OR

**ucbethuel**  
NextWork Student

[nextwork.org](http://nextwork.org)

# Route tables

Route tables are rules that direct how network traffic flows.

Routes tables are needed to make a subnet public because, it is right their we will be able to truly connect the subnet to the internet.

The screenshot shows the AWS VPC Route Tables interface. The URL in the browser is [VPC > Route tables > rtb-0d085ada6005e8060 > Edit routes](#). The main section is titled "Edit routes". It displays two routes:

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	CreateRouteTable
0.0.0.0/0	Internet Gateway	-	No	CreateRoute

Below the table, there is a "Remove" button next to the second route entry. At the bottom of the page are "Add route", "Cancel", "Preview", and "Save changes" buttons.

OR

**ucbethuel**  
NextWork Student

[nextwork.org](http://nextwork.org)

# Route destination and target

Routes are defined by their destination and target, which mean sources of network flow and the subnet or IP 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-xxxxxxxxxxxxxxxxxxxx

A screenshot of the AWS VPC Route Tables interface. The URL in the address bar is `VPC > Route tables > rtb-0d085ada6005e8060 > Edit routes`. The page title is "Edit routes".  
The table displays the following routes:

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	CreateRouteTable
Q 0.0.0.0/0 X	Internet Gateway	-	No	CreateRoute
Q igw-05a84f2637a89a4d1 X				Remove

Buttons at the bottom include "Add route", "Cancel", "Preview", and "Save changes".

OR

ucbethuel  
NextWork Student

[nextwork.org](http://nextwork.org)

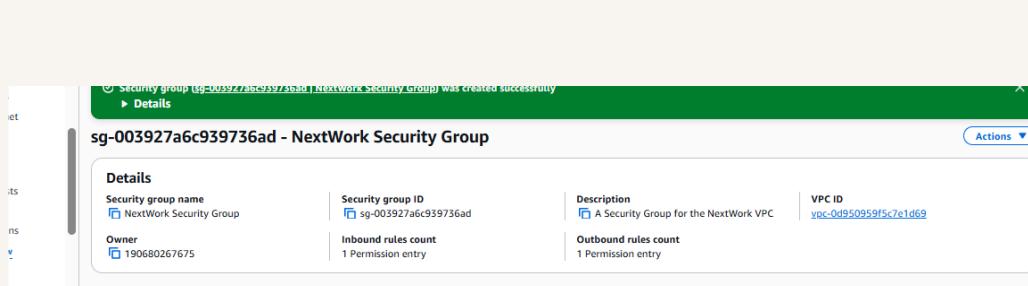
# Security groups

Security groups are like checkpoint which must first we meet before accessing a resources.

## Inbound vs Outbound rules

Inbound rules are rules concerned on how data coming in are to be treated, I configured an inbound rule that allow HTTP to access or interact with my resources.

Outbound rules are set public, By default, my security group's outbound rule allows sending data to all IP addresses whether in VPC or not.



 OR

**ucbethuel**  
NextWork Student

[nextwork.org](http://nextwork.org)

---

## Network ACLs

Network ACLs are securities located at your subnet, that checks for inbound and outbound traffic.

### Security groups vs. network ACLs

The difference between a security group and a network ACL is that, Security group is attached to resources while Network ACL is attached to Subnet.

OR

ucbethuel  
NextWork Student

[nextwork.org](http://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 whether inbound or outbound set at rule 100, while every other rule it denies, of which do not actually take effect.

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

Inbound rules (2)						
<input type="text"/> Filter inbound rules						
Rule number	Type	Protocol	Port range	Source	Allow/Deny	
100	All traffic	All	All	0.0.0.0/0	<input checked="" type="radio"/> Allow	
*	All traffic	All	All	0.0.0.0/0	<input type="radio"/> Deny	



[nextwork.org](https://nextwork.org)

# The place to learn & showcase your skills

Check out [nextwork.org](https://nextwork.org) for more projects

