



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

# VPC Traffic Flow and Security



Jonathan Nutsugah

sg-03e7a2e351d21a4c3 - SacNet Security Group

[Actions](#)

Details		Description	VPC ID
Security group name	SacNet Security Group	Security group ID	sg-03e7a2e351d21a4c3
Owner	248189930152	Inbound rules count	1 Permission entry
		Outbound rules count	1 Permission entry
			vpc-0a80bd992fb168a73

[Inbound rules](#)   [Outbound rules](#)   [Sharing - new](#)   [VPC associations - new](#)   [Tags](#)

**Inbound rules (1)**

Name	Security group rule ID	IP version	Type	Protocol	Port range	Source
-	sgr-03e8d49b0ae0b7ceb	IPv4	HTTP	TCP	80	0.0.0.0/0



**Jonathan Nutsugah**

NextWork Student

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

---

# Introducing Today's Project!

## What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) lets you create a secure, isolated network in AWS where you control IP ranges, subnets, and traffic. It's useful for customizing network setup, enhancing security, and supporting hybrid cloud deployments.

## How I used Amazon VPC in this project

I used it through the management console to create a virtually isolated environment for my resources.

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

The ease navigating the UI.

## This project took me...

60 minutes.

# Route tables

Route tables are tables that contain destination and target information for a network. A system would refer to a routing table to select the best route for passing network traffic.

Route tables are needed to make a subnet public because it will contain the route to the internet as an entry.

The screenshot shows a user interface for managing network routes. At the top, there are tabs: 'Routes' (which is selected and highlighted in blue), 'Subnet associations', 'Edge associations', 'Route propagation', and 'Tags'. Below the tabs, the title 'Routes (2)' is displayed. There is a search bar with the placeholder 'Filter routes'. The main area contains a table with three columns: 'Destination', 'Target', and 'Status'. The table has two rows:

Destination	Target	Status
0.0.0.0/0	<a href="#">igw-0e0c34249a14f3da7</a>	Active
192.168.1.0/24	local	Active

**Jonathan Nutsugah**  
NextWork Student

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

# Route destination and target

Routes are defined by their destination and target, which means a specific destination and target must be specified for a router to be able to direct traffic through the most appropriate path.

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 Internet Gateway.

The screenshot shows a user interface for managing network routes. At the top, there are tabs: **Routes** (which is selected), **Subnet associations**, **Edge associations**, **Route propagation**, and **Tags**. Below the tabs, a section titled **Routes (2)** displays a table of routes. The table has columns for **Destination**, **Target**, and **Status**. There is also a **Filter routes** input field above the table. The data in the table is as follows:

Destination	Target	Status
0.0.0.0/0	<a href="#">igw-0e0c34249a14f3da7</a>	Active
192.168.1.0/24	local	Active

A circular profile picture of a young man with dark hair, wearing a black t-shirt, standing indoors.

**Jonathan Nutsugah**

NextWork Student

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

---

# Security groups

Security groups are firewalls that either deny or allow traffic based on inbound and outbound rules at the instance level.

## Inbound vs Outbound rules

Inbound rules are rules that regulate incoming traffic. I configured an inbound rule that allows only HTTP traffic coming in from anywhere.

Outbound rules are rules that regulate outgoing traffic from an instance. By default, my security group's outbound rule is set to allow all traffic to go out of the instance.



**Jonathan Nutsugah**  
NextWork Student

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

**sg-03e7a2e351d21a4c3 - SacNet Security Group**

[Actions ▾](#)

Details		Description	VPC ID
Security group name <a href="#">SacNet Security Group</a>	Security group ID <a href="#">sg-03e7a2e351d21a4c3</a>	Description <a href="#">A Security Group for the SacNet VPC</a>	VPC ID <a href="#">vpc-0a80bd992fb168a73</a>
Owner <a href="#">248189930152</a>	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

[Inbound rules](#) | [Outbound rules](#) | [Sharing - new](#) | [VPC associations - new](#) | [Tags](#)

**Inbound rules (1)**

Name	Security group rule ID	IP version	Type	Protocol	Port range	Source
-	sgr-03e8d49b0ae0b7ceb	IPv4	HTTP	TCP	80	0.0.0.0/0

[Edit inbound rules](#)

A circular profile picture of a young man with dark hair, wearing a black t-shirt, standing indoors.

**Jonathan Nutsugah**  
NextWork Student

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

# Network ACLs

Network ACLs are similar to security groups, but they filter traffic at the subnet level.

## Security groups vs. network ACLs

The difference between a security group and a network ACL is that security groups are stateful and NACLs are stateless. Also, security groups operate at the instance level while NACLs operate at the subnet level.

**Jonathan Nutsugah**  
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.

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

The screenshot shows the 'Inbound rules' tab of a CloudFormation stack configuration. There are two rules listed:

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](https://nextwork.org)

# The place to learn & showcase your skills

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

