



VPC Traffic Flow and Security



Russell Geisler

The screenshot shows the AWS CloudFormation console with the URL <https://console.aws.amazon.com/cloudformation/home?region=us-east-1#/stacks/sg-009c479d0f5ae8cc0>. The page displays the details of a security group named "NextWork Security Group" (sg-009c479d0f5ae8cc0). The security group is associated with a VPC (vpc-0fbec0e0f993bfad) and has one inbound rule allowing HTTP traffic (TCP port 80) from the IP address sgr-031dce9a3b2b21815. The "Inbound rules" section shows this single rule.

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC are used to secure and protect resources.

How I used Amazon VPC in this project

I built a VPC with a security group and network ACL to set rules to control traffic and routing tables to designate IP address ranges.

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

I did not expect to get to get this in depth in building a secure VPC

This project took me...

I spent about an hour completing this project

Route tables

The route table is a table of rules, called routes, that decide where the data in your network should go.

Route tables are needed to make a subnet public so internet-bound traffic can reach the public internet

The screenshot shows a web-based interface for managing network routes. At the top, there's a navigation bar with links to 'ROUTE TABLES', 'RTD-03041410C112U002', and 'Edit routes'. Below the navigation is a title 'Edit routes'. The main area contains a table with four columns: 'Destination', 'Target', 'Status', and 'Propagated'. There are two rows in the table:

Destination	Target	Status	Propagated
10.0.0.0/16	local Q local	Active	No
Q 0.0.0.0/0	Internet Gateway Q igw-003cf3aa3a0fd0373	Active	No

At the bottom of the table, there are buttons for 'Add route' (highlighted in blue), 'Cancel', 'Preview', and 'Save changes' (highlighted in orange).

Route destination and target

Routes are defined by their destination and targets. A destination is the IP address range that traffic wants to get to. The target is the path the traffic will need to take.

The new routes destination is 0.0.0.0/0 and the target is the Internet Gateway

The screenshot shows a web-based interface for managing network routes. The top navigation bar includes links for 'VPL', 'Route tables', and 'Edit routes'. The main title is 'Edit routes'. Below the title, there is a table with four columns: 'Destination', 'Target', 'Status', and 'Propagated'. There are two rows in the table:

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	Internet Gateway	Active	No

At the bottom of the table, there is a 'Remove' button next to the second row. Below the table, there is a blue 'Add route' button. At the very bottom of the interface, there are three buttons: 'Cancel', 'Preview' (disabled), and 'Save changes'.

Security groups

Security groups check inbound and outbound traffic to and from a resource in the VPC.

Inbound vs Outbound rules

Inbound rules are rules for traffic coming into the VPC like visitor traffic. The inbound rule i created allows http traffic so all http traffic can access my resources

Outbound rules are for devices trying to access resources outside of the VPC. This outbound rule currently allows all traffic

The screenshot shows the AWS CloudFormation console with the following details:

Details

Security group name	sg-009c479d0f5ae8cc0	Description	VPC ID
Owner	022687721466	Inbound rules count	vpc-0fbecd0e0f993bfad
		1 Permission entry	
		Outbound rules count	
		1 Permission entry	

Inbound rules (1)

Name	Security group rule ID	IP version	Type	Protocol	Port range
-	sgr-031dce9a3b2b21815	IPv4	HTTP	TCP	80

Network ACLs

Network ACLs are access control lists that can allow or deny inbound and outbound traffic.

Security groups vs. network ACLs

Security groups define rules for inbound and outbound traffic to and from resources.
Network ACLs are broader rules for the whole subnet

Default vs Custom Network ACLs

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

By default, a network ACL will allow all network traffic inbound and outbound

A custom ACL will automatically deny all inbound and outbound traffic until rules are set

Edit inbound rules Info
Inbound rules control the incoming traffic that's allowed to reach the VPC.

Rule number	Type info	Protocol info	Port range info	Source info	Allow/Deny info
100	All traffic	All	All	0.0.0/0	Allow
*	All traffic	All	All	0.0.0/0	Deny

[Add new rule](#) [Sort by rule number](#)

[Cancel](#) [Preview changes](#) [Save changes](#)



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

