



NextWork.org

# VPC Traffic Flow and Security



Sadeesha Perera

Security group name: NextWork Security Group  
Security group ID: sg-07e7890b915287bff  
Description: A Security Group for the NextWork VPC.  
VPC ID: vpc-03cc146bd20872eea  
Owner: 992362852391  
Inbound rules count: 1 Permission entry  
Outbound rules count: 1 Permission entry

Name	Security group rule...	IP version	Type	Protocol	Port range
-	sgr-0c905232057151...	IPv4	HTTP	TCP	80



Sadeesha Perera  
NextWork Student

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

# Introducing Today's Project!

## What is Amazon VPC?

Amazon VPC is a service that lets you create a logically isolated section within the AWS cloud, providing you with complete control over your virtual network. It offers enhanced security, scalability, flexibility, and cost-effectiveness.

## How I used Amazon VPC in this project

To build a secure application, I used Amazon VPC to create a virtual network. This involves creating a VPC, defining public and private subnets, configuring route tables, and creating security groups.

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

How easy to enable security measurements in the AWS environment

## This project took me...

50 minutes



# Route tables

Route tables are like a set of rules that determine how network traffic flows within your virtual network. Each subnet is associated with a route table, defining where specific IP traffic should be directed based on destination CIDR blocks.

Route tables are needed to make a subnet public because it determines how network traffic from that subnet is routed. To make a subnet public, you need to associate it with a route table that contains a route pointing to an internet gateway.

The screenshot shows the AWS VPC Route Table Details page for the route table 'rtb-0ecd4cb7170c6c102'. The 'Details' tab is selected, displaying the following information:

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-0ecd4cb7170c6c102	Yes	-	-
VPC	vpc-03cc146bd20872eea   NextWork	Owner ID: 9923582852391	VPC

The 'Routes' tab shows two routes:

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0fe04570fd654c36b4	Active	No
10.0.0.0/16	local	Active	No



# Route destination and target

A route in a route table consists of a destination and a target. The destination specifies the range of IP addresses the route applies to, while the target indicates where traffic matching that destination should be sent.

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-0fe534534b

The screenshot shows the AWS VPC console with the URL [us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#RouteTableDetails:RouteTableId=rtb-0ecd4cb7170c6c102](https://us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#RouteTableDetails:RouteTableId=rtb-0ecd4cb7170c6c102). A green banner at the top says "Updated routes for rtb-0ecd4cb7170c6c102 / NextWork route table successfully". The main content area is titled "rtb-0ecd4cb7170c6c102 / NextWork route table". It shows a "Details" section with route table ID, VPC, and owner information. Below is a "Routes" table:

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0fe0437d6d54c56b4	Active	No
10.0.0.0/16	local	Active	No



# Security groups

Security groups act as virtual firewalls for your EC2 instances, controlling both inbound and outbound traffic. They operate on a "deny all" principle, meaning that all traffic is blocked unless explicitly allowed by a specific rule.

## Inbound vs Outbound rules

An inbound rule in a security group defines the types of traffic allowed to enter an EC2 instance. It specifies the source IP address range, port range, and protocol for incoming traffic.

An outbound rule in a security group defines the types of traffic that an EC2 instance is allowed to send out. It specifies the destination IP address range, port range, and protocol for outgoing traffic.

The screenshot shows the AWS VPC Security Groups console. The main view displays the 'Details' for the 'sg-07e7890b915287bff - NextWork Security Group'. The 'Inbound rules' tab is selected, showing one rule: 'sgr-0c905232057151...'. This rule allows traffic from '0.0.0.0/0' to port 80 on TCP. The 'Outbound rules' tab is also visible. On the left, the 'VPC dashboard' sidebar is open, showing various network components like VPCs, Subnets, Route tables, and Internet gateways. The browser's address bar shows the URL: us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#SecurityGroup;groupid=sg-07e7890b915287bff.



**Sadeesha Perera**  
NextWork Student

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

# Network ACLs

Network Access Control Lists (NACLs) are another layer of security for your VPC. They act as a firewall for traffic entering or leaving a subnet. Unlike security groups, which are associated with individual instances, NACLs are associated with subnets.

## Security groups vs. network ACLs

Security groups and network ACLs are both used to control traffic within a VPC, but they differ in scope and operation. Security groups operate at the instance level, controlling traffic to and from individual EC2 instances.

Sadeesha Perera  
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, network ACLs allow all inbound and outbound traffic. This means that unless you explicitly add rules to deny specific traffic, all traffic will be permitted.

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

Inbound rules (2)							Edit inbound rules	
Rule number	Type	Protocol	Port range	Source	Allow/Deny		< 1 >	⚙️
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

