



# VPC Traffic Flow and Security



RAJARSHI VERMA

The screenshot shows the AWS VPC Security Groups console. A success message at the top states: "Security group sg-0edb958575ed4a2c | MySecurityGroup was created successfully". The main view displays the details of the newly created security group "sg-0edb958575ed4a2c - MySecurityGroup". The details include:

- Security group name: MySecurityGroup
- Security group ID: sg-0edb958575ed4a2c
- Description: A security group for my VPC
- VPC ID: vpc-0ddeda17eab34212b
- Owner: 832603165939
- 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, and Tags. The Inbound rules section shows one rule:

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
-	sgr-080a3d7a5d73be...	IPv4	HTTP	TCP	80	0.0.0.0/0	-



# Introducing Today's Project!

## What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) allows you to create a private, isolated network within the AWS cloud. It provides security, customization, and scalability, enabling you to control inbound and outbound traffic, connect to the internet, and manage.

## How I used Amazon VPC in this project

I created a VPC with subnet and internet gateway. Then further I created a route table and then created a security group and at last created a network ACL.

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

Already created security groups and default rules and ACI. Moreover it is easy to create and set our rules but understanding of address and ports is necessary.

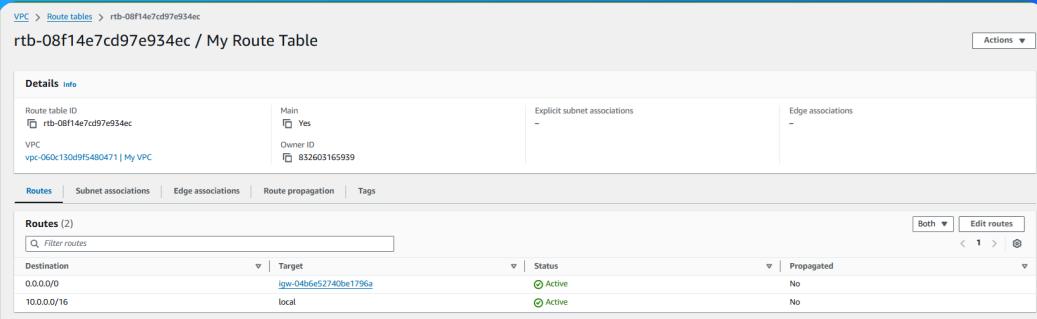
## This project took me...

It took me not more than 15 minutes for all the progress.

# Route tables

A route table in a VPC acts like a GPS, guiding data to its destination. Each subnet needs a route table to direct traffic. Without it, resources can't send or receive data. Multiple subnets can share one route table, but each subnet can only use one

Route tables are needed to make a subnet public because they direct traffic to the internet gateway. Without a route table, the subnet wouldn't know where to send or receive data, making it impossible for resources to communicate with the internet.



# Route destination and target

Routes are defined by their destination and target, which mean the IP address range that traffic wants to reach and the path it takes to get there. Example, `0.0.0.0/0` as a destination means all IP addresses, and `igw-xxxx` as target means IG.

New routes destination is 10.0.0.0/16 and target as local and if not found we have added a 0.0.0.0/0 destination whose target is internet gateway and it will search on web.

Details				Actions	
Route table ID	rtb-08f14e7cd97e934ec	Main	Yes	Explicit subnet associations	-
VPC	vpc-060c130d9f5480471   My VPC	Owner ID	832603165939	Edge associations	-
Routes	Subnet associations	Edge associations	Route propagation	Tags	
<b>Routes (2)</b>					
Destination	Target	Status	Propagated	Both	
0.0.0.0/0	igw-04b6e52740be1796a	Active	No	<	1
10.0.0.16	local	Active	No	>	Both

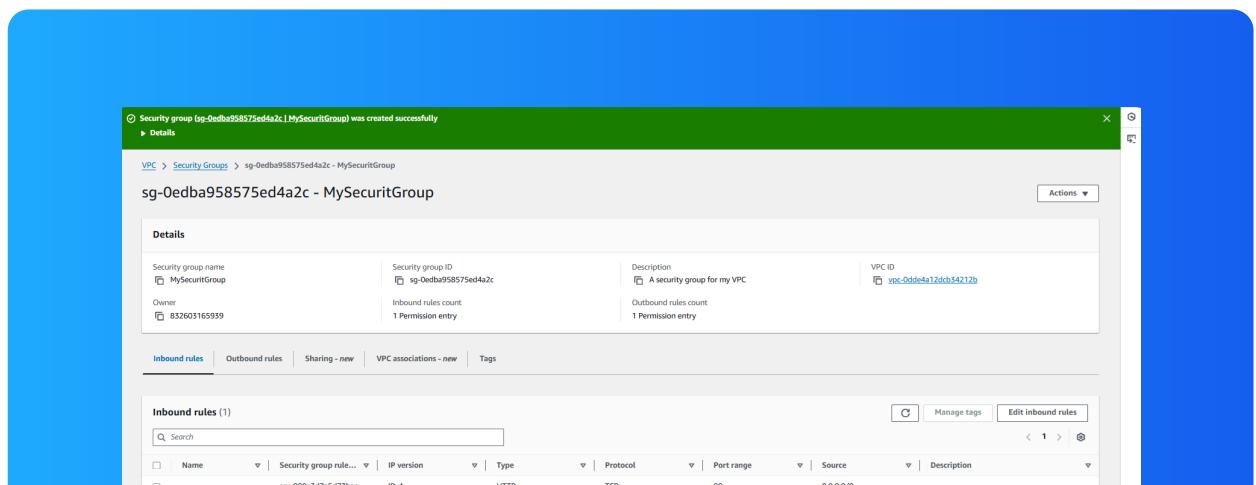
# Security groups

Security groups are virtual firewalls for your AWS resources. They control inbound and outbound traffic to and from your resources based on rules you define. Each security group acts at the instance level and allows which traffic to interact.

## Inbound vs Outbound rules

Inbound rules are rules that control the incoming traffic to your resources. They specify which traffic is allowed to enter your resources based on criteria like IP address, protocol, and port number. I added type HTTP and Source type anywhere IPv-4.

Outbound rules are rules that control the outgoing traffic from your resources. By default, my security group's outbound rule allows all outbound traffic, meaning any resource associated with the security group can send data to any IP address.





# Network ACLs

A Network Access Control List (ACL) are set of rules that control network traffic in and out of a subnet.. Imagine a traffic cop standing at the entrance and exit of your subnet. Each time a data packet tries to enter or leave, the traffic cop check

## Security groups vs. network ACLs

The difference between a security group and a network ACL is that ACL is a firewall that controls traffic for an entire subnet. And Security groups are more granular than ACLs. They control traffic for individual resources, such as EC2 instance.

# 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. This means that all incoming and outgoing traffic is permitted unless you specifically add rules to deny certain types of traffic or restrict access to specific IP address

In contrast, a custom ACL's inbound and outbound rules are automatically set to \*\*deny all traffic\*\*. This means that no data can enter or leave the associated subnets until specific rules are added. By default, all traffic is blocked.

The screenshot shows the AWS Network ACLs management interface. At the top, there is a table listing three Network ACLs:

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count	Outbound rules count	Owner
-	acl-011d10ce681738a60	-	Yes	vpc-060c130d9f548047f / My_VPC	2 Inbound rules	2 Outbound rules	832603165939
-	acl-0e0a173371bc11c8	3 Subnets	Yes	vpc-0dd64a12dc634212b	2 Inbound rules	2 Outbound rules	832603165939
<input checked="" type="checkbox"/> MyACL	acl-07e115b5f598c4473	subnet-0e56503f12592a483 / Public v1	No	vpc-060c130d9f548047f / My_VPC	2 Inbound rules	2 Outbound rules	832603165939

The 'MyACL' row is selected. Below the table, the details for 'acl-07e115b5f598c4473 / MyACL' are shown. 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

