



# VPC Traffic Flow and Security



Ivan Delgadillo Fernandez

The screenshot shows the AWS EC2 Security Groups console. A green success message at the top states: "Security group (sg-05d456408acbf95c7 | NextWork Security Group) was created successfully". Below this, the "Details" tab is selected for the security group "sg-05d456408acbf95c7 - NextWork Security Group". The "Details" table includes columns for Security group name, Security group ID, Description, VPC ID, Owner, Inbound rules count, and Outbound rules count. Under "Inbound rules", there is one rule listed:

Inbound rules (1)				
Security group rule...	IP version	Type	Protocol	Port range
sgr-071ffcf6a6a37b007	IPv4	HTTP	TCP	80



Ivan Delgadillo Fernandez

NextWork Student

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

---

# Introducing Today's Project!

## What is Amazon VPC?

Amazon Virtual Private Cloud (Amazon VPC) gives you full control over your virtual networking environment, including resource placement, connectivity, and security

## How I used Amazon VPC in this project

I created VPC to put a subnet facing to internet

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

I didn't expect to configure the network ACL

## This project took me...

around 45 minutes



Ivan Delgadillo Fernandez

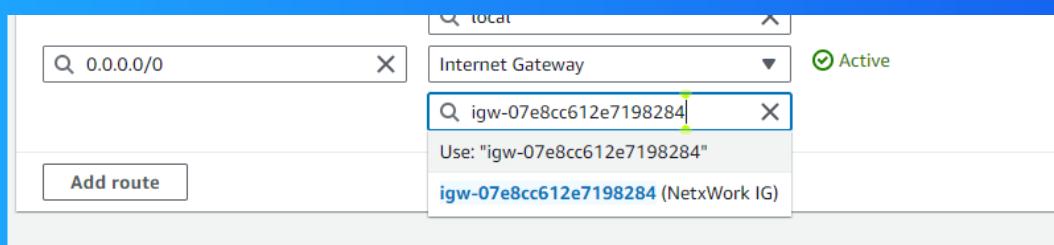
NextWork Student

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

# Route tables

Route table are a set of rules, known as routes that determines where network traffic is directed.

Route tables are needed to make a subnet public for Internet access.



Ivan Delgadillo Fernandez

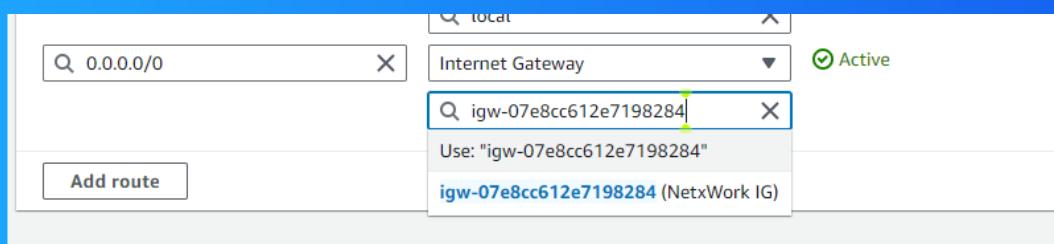
NextWork Student

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

# Route destination and target

Routes are defined by their destination and target, which mean network traffic can be redirected

The route in my route table that directed internet-bound traffic to my internet gateway had destination of anywhere, and a target of my internet gateway.





Ivan Delgadillo Fernandez

NextWork Student

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

# Security groups

Security groups are responsible for checking who comes in and out. They have strict rules about what kind of traffic can enter or leave the resource based on its IP address, protocols and port numbers.

## Inbound vs Outbound rules

Inbound rules control the data that can enter the resources in your security group, while outbound rules control that data that your resources can send out.

By default, AWS security groups already allow all outbound traffic. So unless you specify otherwise, any resource associated with the security group can access and send data to any IP address - whether it's in your VPC, other VPCs (if you have the ri

The screenshot shows the AWS EC2 Security Groups console. A green header bar at the top indicates that a security group was created successfully. Below this, the main interface displays the details of a security group named "sg-05d456408acbf95c7 - NextWork Security Group". The "Details" section provides information such as the security group name, ID, description, owner, and VPC ID. The "Inbound rules" tab is selected, showing one rule entry. The rule details include the source, IP version, type, protocol, and port range.



Ivan Delgadillo Fernandez

NextWork Student

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

---

# Network ACLs

Network ACL are a rules that either allow access to a network.

## Security groups vs. network ACLs

Security groups and network ACLs are similar in that they allow you to control access to AWS resources within your VPC. But security groups allow you to control inbound and outbound traffic at the instance level, while network ACLs offer similar capa

Ivan Delgadillo Fernandez

NextWork Student

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

# Default vs Custom Network ACLs

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

The default network ACL is configured to allow all traffic to flow in and out of the subnets with which it is associated. Each network ACL also includes a rule whose rule number is an asterisk (\*). This rule ensures that if a packet doesn't match any

The network ACL also includes inbound rules that allow SSH and RDP traffic into the subnet. Outbound rule 120 enables responses to leave the subnet. The network ACL has outbound rules (100 and 110) that allow outbound HTTP and HTTPS traffic out of th

The screenshot shows the AWS Network ACL Inbound Rules configuration page for an ACL named 'acl-024f24e16423f7b86'. The page has tabs for Details, Inbound rules (which is selected), Outbound rules, Subnet associations, and Tags. The Inbound rules section displays 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

