



# VPC Traffic Flow and Security



tahirgroot@gmail.com

sg-05905d19d38f809e0 - Groot279 Security Group

Actions ▾

Details	
Security group name Groot279 Security Group	Security group ID sg-05905d19d38f809e0
Description A Security Group for the Groot279.	VPC ID <a href="#">vpc-053d27d591d13b581</a>
Owner 058264334031	Inbound rules count 1 Permission entry
	Outbound rules count 1 Permission entry

Inbound rules | Outbound rules | Tags

Inbound rules (1)

Manage tags | Edit inbound rules

Name	Security group rule...	IP version	Type	Protocol	Port range
-	sgr-0fa759052573e8034	IPv4	HTTP	TCP	80

 TA

tahirgroot@gmail.com

NextWork Student

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

---

# Introducing Today's Project!

## What is Amazon VPC?

Amazon Virtual Private Cloud (Amazon VPC) is a virtual network within the AWS cloud that gives you full control over your virtual networking environment. It allows you to create a private, isolated network within the public cloud.

## How I used Amazon VPC in this project

Designing VPC architectures based on specific requirements. by creating a route table, create a security group and create a network acl.

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

inbound and outbound traffic

## This project took me...

30 minutes

# Route tables

Route tables are databases used by routers to determine the best path for data packets to their destination, based on network addresses and associated metrics.

Route tables are needed to make a subnet public because they define the path network traffic takes. To access the public internet, a subnet requires a route pointing to an internet gateway within its route table.



# Route destination and target

Routes are defined by their destination and target, which mean:

- Destination: The network address or range of addresses where the traffic is headed
- Target: The next hop or device where the traffic should be sent to reach its destination

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 Groot279 IG (Internet Gateway)





tahirgroot@gmail.com

NextWork Student

NextWork.org

# Security groups

Security groups are virtual firewalls that control inbound and outbound traffic at resource level. They act as a barrier, allowing or denying traffic based on specified rules, ensuring only authorized access.

## Inbound vs Outbound rules

Inbound rules are permissions that dictate which traffic can enter a resource. They define the source, port, protocol, and allowed traffic. I configured an inbound rule that permits SSH traffic (port 80) from my IP address to enable secure access

Outbound rules are permissions that dictate which traffic can exit an EC2 instance. They define the destination, port, protocol, and allowed traffic. By default, my security group's outbound rule allows all outbound traffic.

The screenshot shows the AWS Security Groups console for the 'Groot279 Security Group'. The 'Details' tab is selected, displaying the following information:

Security group name	Security group ID	Description	VPC ID
Groot279 Security Group	sg-05905d19d38f809e0	A Security Group for the Groot279.	vpc-053d27d591d13b581
Owner	Inbound rules count	Outbound rules count	
058264334031	1 Permission entry	1 Permission entry	

Below the details, there are tabs for 'Inbound rules', 'Outbound rules', and 'Tags'. The 'Inbound rules' tab is selected, showing one rule:

Name	Security group rule...	IP version	Type	Protocol	Port range
-	snr-0fa75902573e004	IPv4	HTTP	TCP	80

# Network ACLs

Network ACLs are stateful firewalls that control inbound and outbound traffic at the subnet level. They provide an additional layer of security by filtering traffic before it reaches security groups.

## Security groups vs. network ACLs

The difference between a security group and a network ACL is that a security group acts as a firewall at the resource level, while a network ACL is a firewall at the subnet level, controlling traffic in and out of entire subnets.

# 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 create a dual layer of security that make sure inbound/outbound traffic go through at least two checks.

In contrast, a custom ACL's inbound and outbound rules are automatically set to deny all traffic. This means you must explicitly define rules to allow specific traffic, providing granular control over network access

Inbound rules (2)							Edit inbound rules	
Filter inbound rules		Type	Protocol	Port range	Source	Allow/Deny		
Rule number		All traffic	All	All	0.0.0.0/0	<input checked="" type="radio"/> Allow		
*		All traffic	All	All	0.0.0.0/0	<input type="radio"/> Deny		



NextWork.org

**Everyone  
should be in a  
job they love.**

Check out nextwork.org for  
more projects

