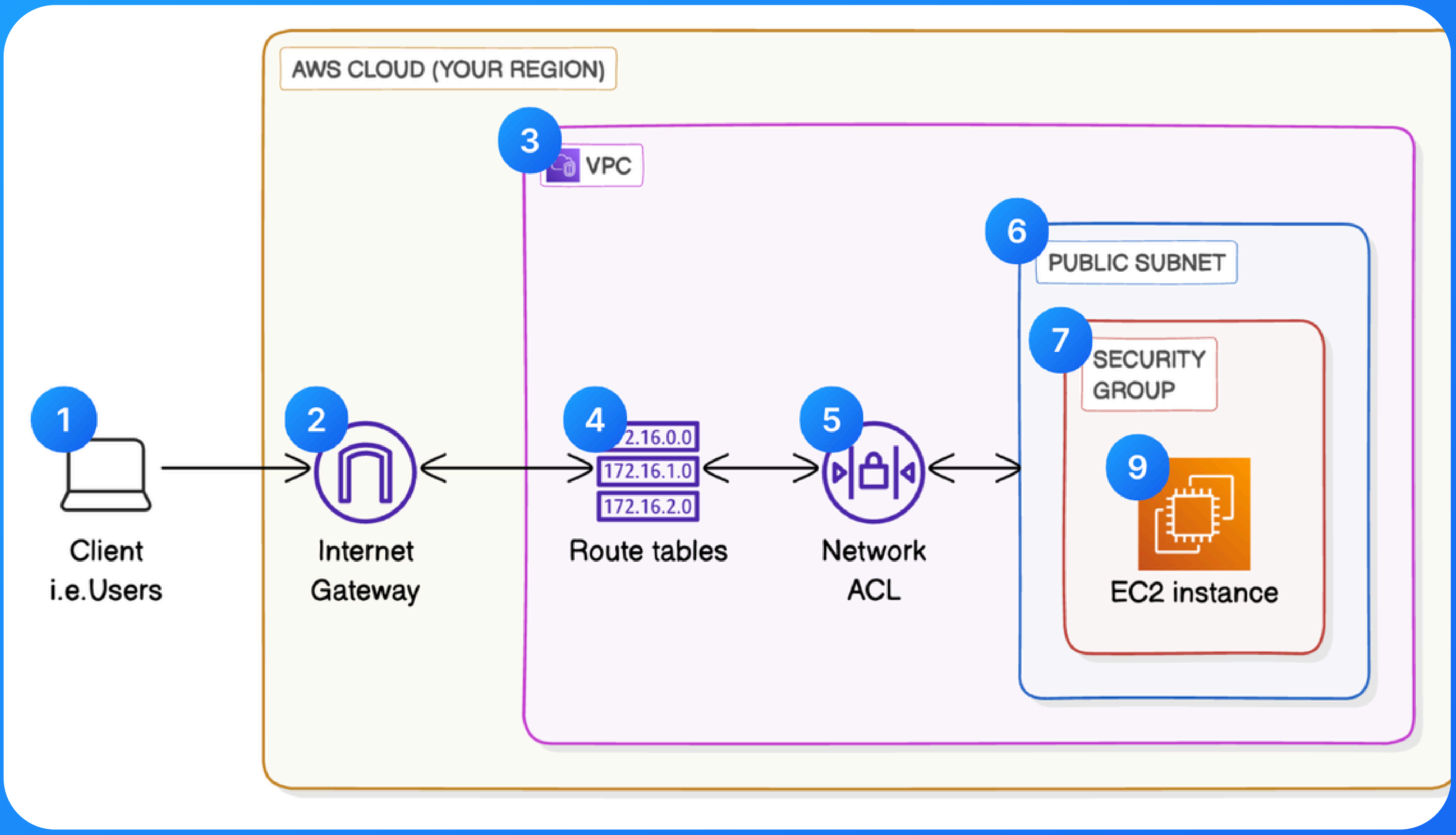
NextWork.org

VPC Traffic Flow and Security

Hassan Gachoka



Introducing Amazon VPC!

What it does & how it’s useful

Amazon VPC (Virtual Private Cloud) is a service that lets you provision a logically isolated section of the AWS cloud where you can launch AWS resources in a virtual network you define. Developers and teams use Amazon VPC for enhanced security, control, and network customization.

How I’m using it in today’s project

In today's project, we're using Amazon VPC to manage traffic flow and security with three key components: Route Tables for directing traffic, Network Access Control Lists (NACLs) for stateless filtering, and Security Groups for stateful filtering at the instance level.

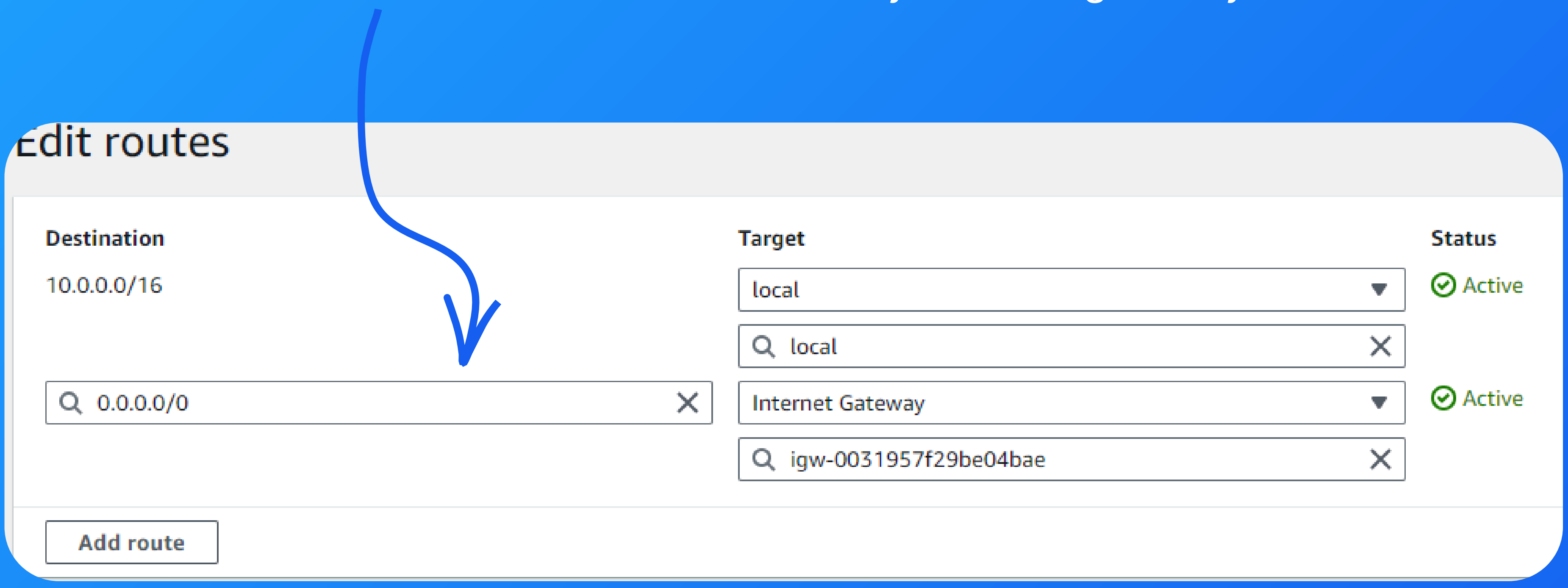
This project took me...

This project took me 20 minutes to complete, creating a VPC then focusing on configuring Route Tables, Network Access Control Lists, and Security Groups within the VPC. Documentation took me half an hour to thoroughly detail the setup and security measures implemented.

Route tables

- Route tables are used in Amazon VPC to determine where network traffic is directed
- Route tables are needed to make a subnet public because they define the routes that allow traffic to flow between subnets and the internet.
- A route table is made up of routes, which are defined by its destination and target:
  - The **destination** is the CIDR block to which the traffic is directed.
  - The target is the gateway, instance, or network interface that traffic is routed to.
- 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 the Internet Gateway.

This route directs Internet-bound traffic to my internet gateway



Edit routes

Destination	Target	Status
10.0.0.0/16	local local	✓ Active
0.0.0.0/0	Internet Gateway igw-0031957f29be04bae	✓ Active

Security groups

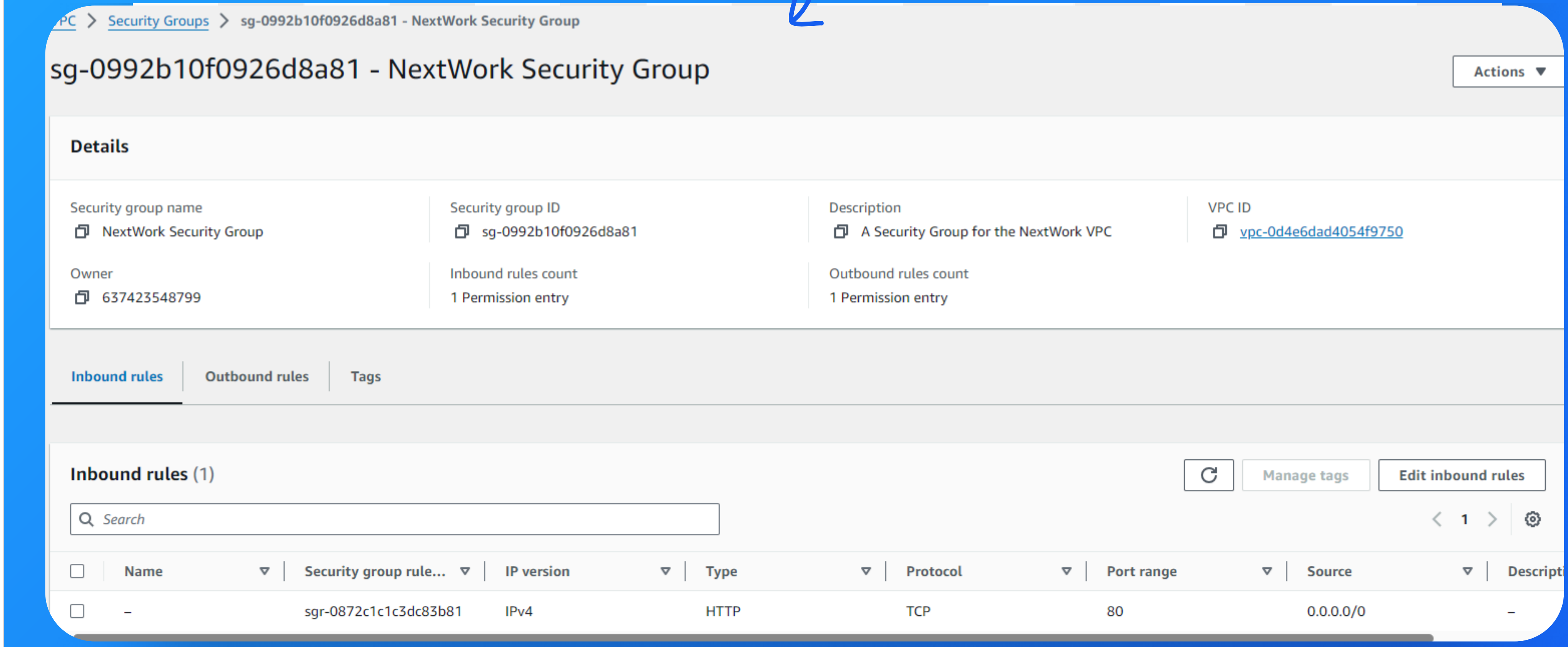
- Security groups are virtual firewalls for your Amazon EC2 instances to control inbound and outbound traffic.

- Security groups control traffic flow using two types of rules:
  - **Inbound rules** are used to control the incoming traffic to your instances.
  - **Outbound rules** are used to control the outgoing traffic from your instances.

- By default, an outbound rule allows all outbound traffic.

- I also configured an inbound rule that allows all traffic.

My configured security group



PC > Security Groups > sg-0992b10f0926d8a81 - NextWork Security Group

sg-0992b10f0926d8a81 - NextWork Security Group

Details

Security group name
NextWork Security Group

Security group ID
sg-0992b10f0926d8a81

Description
A Security Group for the NextWork VPC

VPC ID
vpc-0d4e6dad4054f9750

Owner
637423548799

Inbound rules count
1 Permission entry

Outbound rules count
1 Permission entry

Inbound rules (1)

□	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Descripti
□	–	sgr-0872c1c1c3dc83b81	IPv4	HTTP	TCP	80	0.0.0.0/0	–

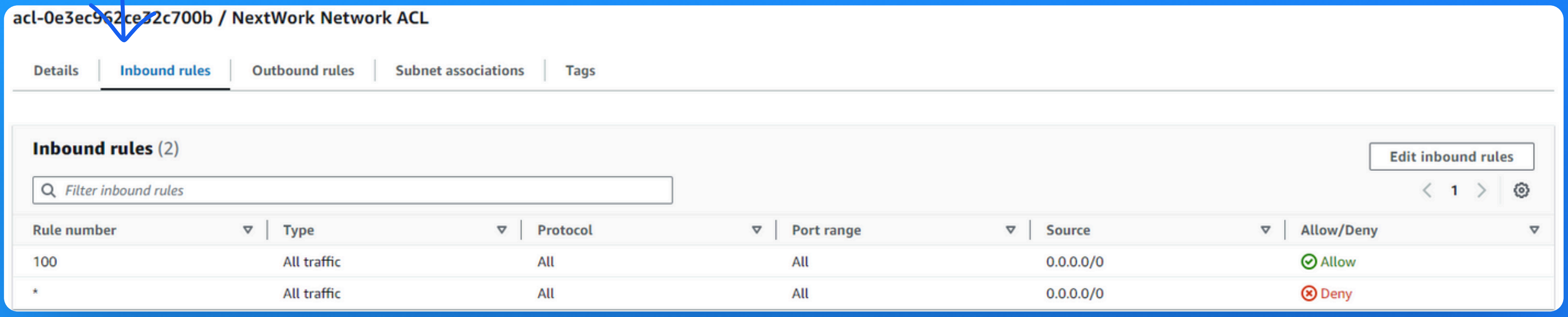
Network ACLs

- Network ACLs are used to set broad traffic rules that apply to an entire subnet. For example, blocking incoming traffic from a particular range of IP addresses or denying all outbound traffic to certain ports.
- Security groups allow for more granular control, managing access to individual resource. You can specify which ports and protocols are allowed for each connected resource.

- Having both is a great security practice! You can set broad restrictions at the subnet level with ACLs, and more specific limits at the resource level through security groups. This dual layer takes security to the next level as traffic must pass through multiple checks, which reduces the chances of unwanted access.

- Similar to security groups, network ACLs use inbound and outbound rules:
    - A default network ACL's inbound rule is set up to allow all inbound traffic by default
    - A default network ACL's outbound rule is set up to allow all outbound traffic by default
    - In contrast, a custom ACL's inbound and outbound rules are automatically set to deny all traffic, requiring explicit rules to be added to allow desired traffic flows

My network ACL’s inbound rules

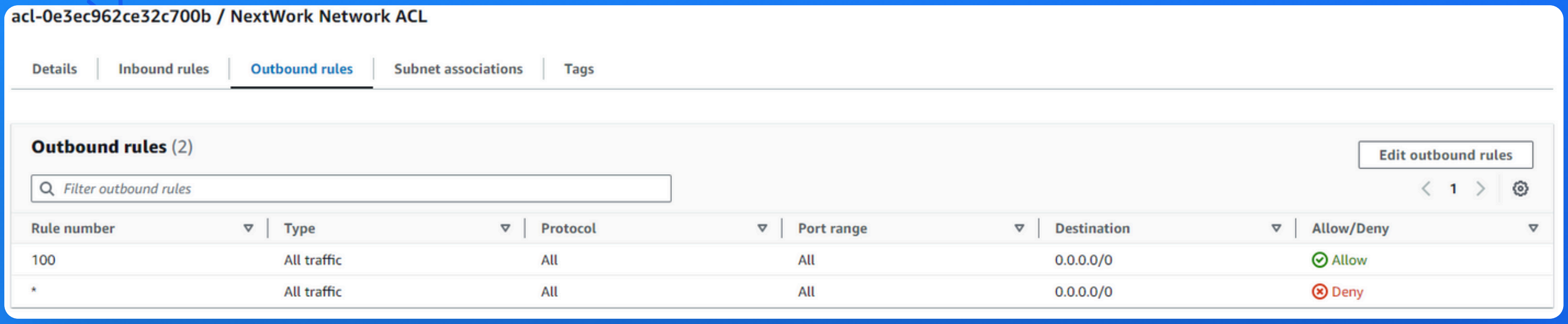


acl-0e3ec962ce32c700b / NextWork Network ACL

Inbound rules (2)

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

My network ACL’s outbound rules



acl-0e3ec962ce32c700b / NextWork Network ACL

Outbound rules (2)

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	✓ Allow
*	All traffic	All	All	0.0.0.0/0	⊗ Deny

My key learnings

1. I can use a route table to make a subnet public by adding a route with a destination CIDR block of 0.0.0.0/0 and a target of an internet gateway.

2. Protocols and port numbers define rules for communication between network devices. Protocols specify how data is exchanged, while port numbers designate specific endpoints within those protocols.

3. The default settings for default ACLs are to allow all inbound and outbound traffic until explicitly configured with rules.

4. One thing I didn’t expect was the complexity and impact of network ACLs on traffic flow within the VPC, requiring careful configuration to avoid unintended restrictions or vulnerabilities.