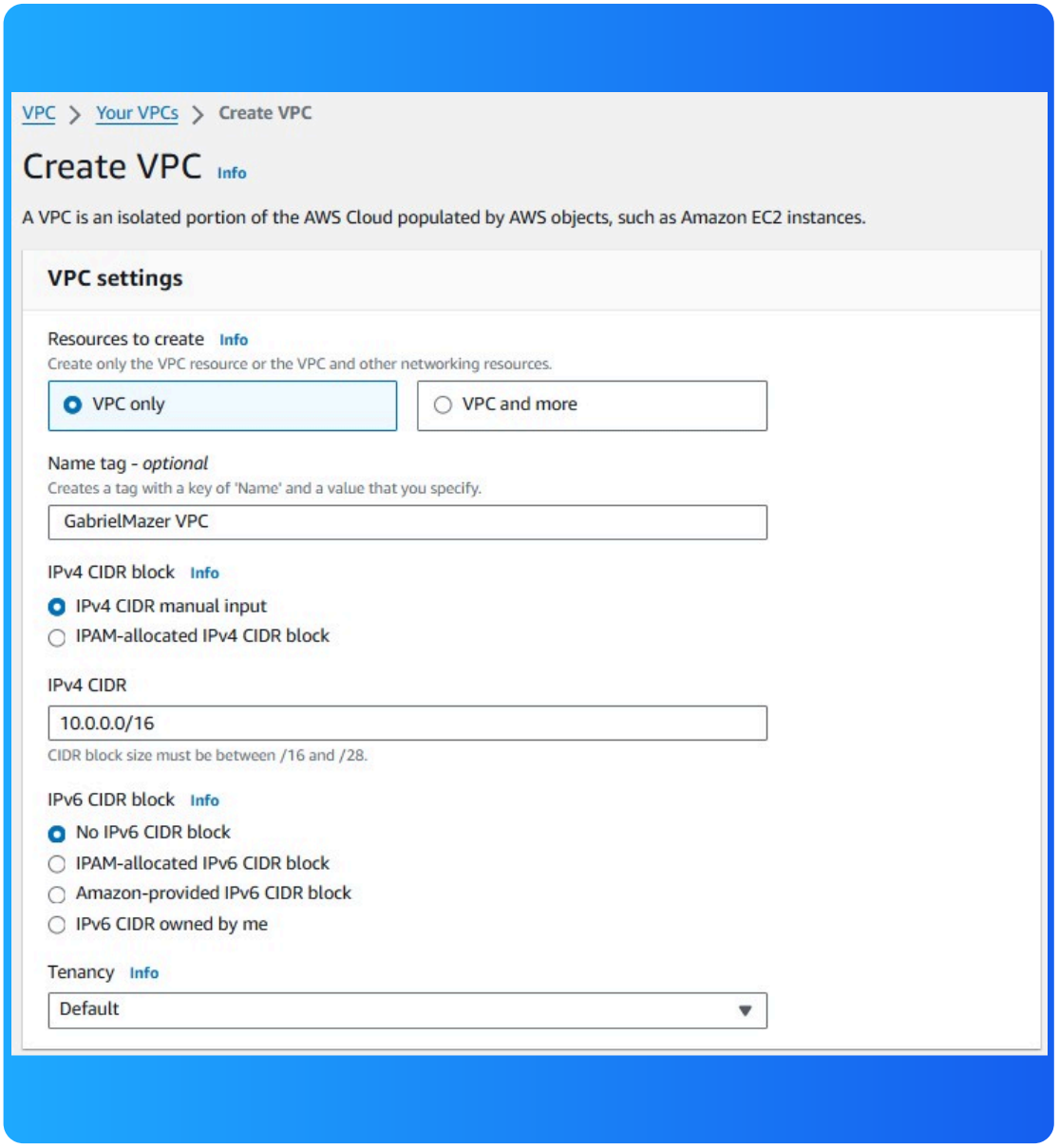
Build a Virtual Private Cloud

Gabriel Taveira Mazer



Gabriel Mazer

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is a private network that allows you to isolate and manage your resources in AWS, offering control over security, traffic flow, and network settings, making it essential for cloud infrastructure.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create a custom virtual network, set up subnets, and attached an internet gateway, enabling controlled access between my resources and the internet.

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

I didn’t expect how straightforward and visual the process of configuring a VPC would be, especially with the guided steps and AWS console layout.

This project took me...

This project took me about 2 hours to complete, including reading the instructions, creating the VPC, subnets, and configuring the internet gateway.

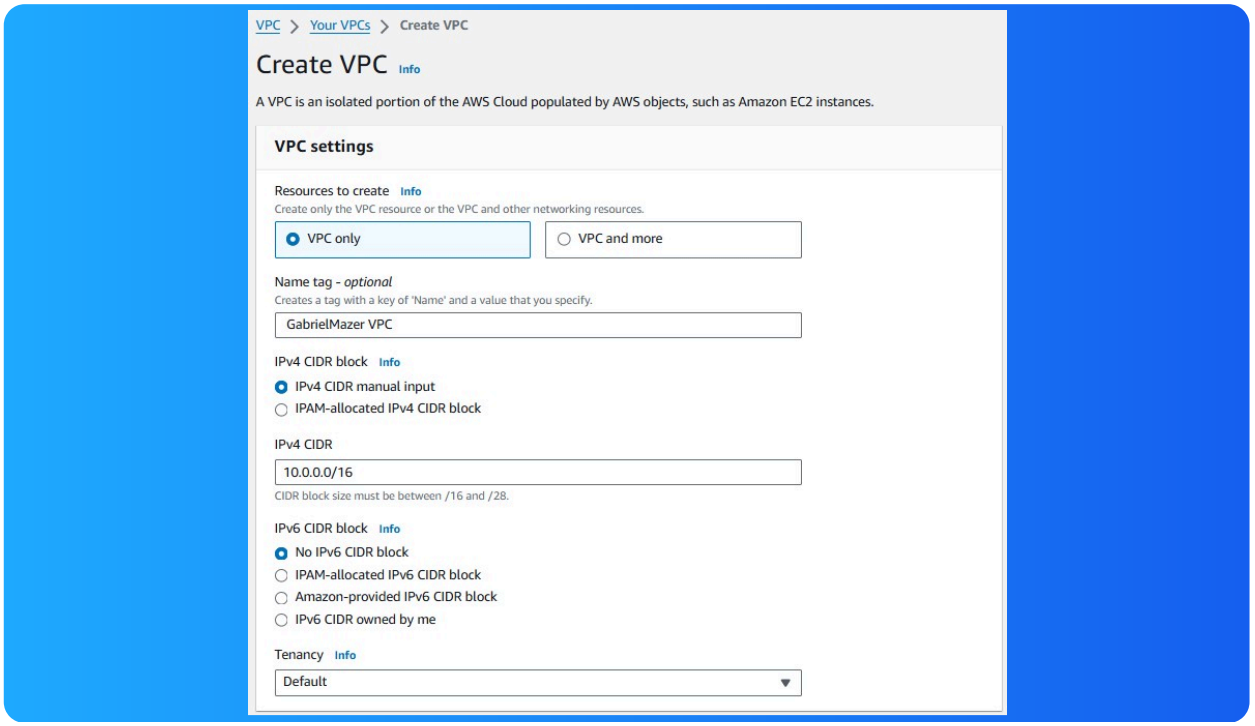
Gabriel Mazer

Virtual Private Clouds (VPCs)

VPCs are isolated virtual networks in AWS that allow you to control and manage resources, such as EC2 instances, with custom security, IP addressing, and networking configurations.

There was already a default VPC in my account ever since my AWS account was created. This is because AWS provides a default VPC for quick resource deployment without needing custom networking setup.

To set up my VPC, I had to define an IPv4 CIDR, which means specifying a range of IP addresses that can be assigned to resources within the VPC, ensuring no overlap with other networks.



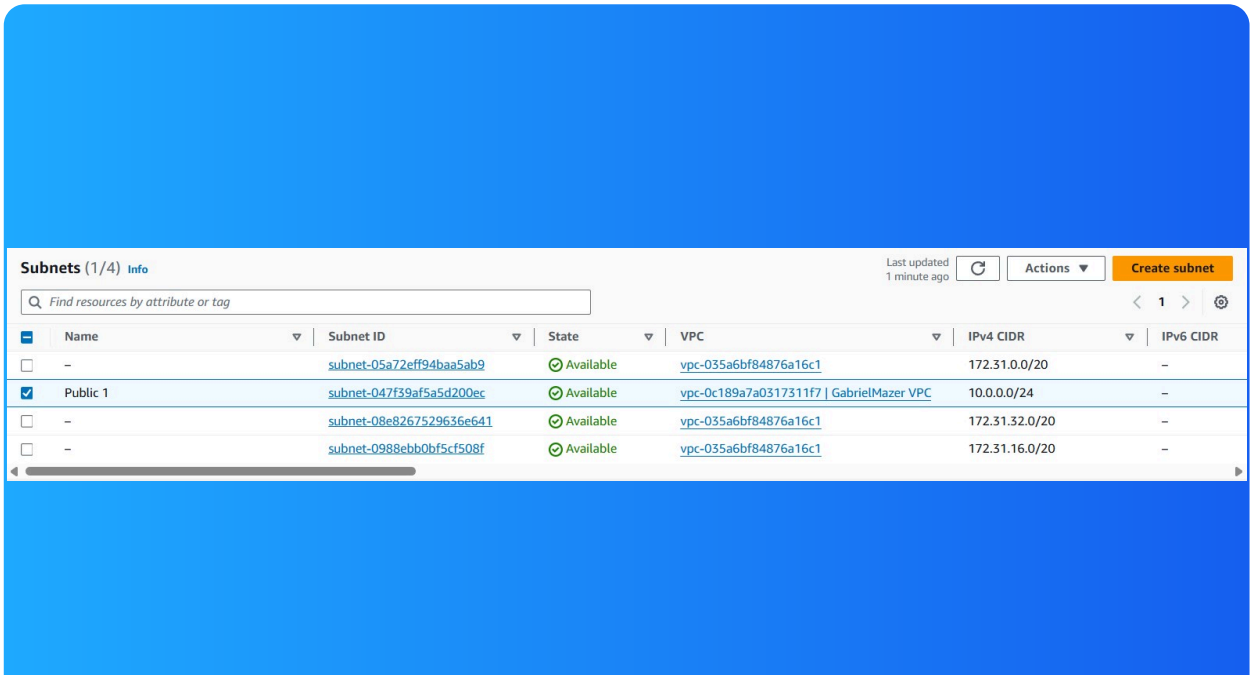
Gabriel Mazer

Subnets

Subnets are subdivisions of a VPC that allow you to segment your network. Each subnet hosts resources that can communicate within the subnet and with other subnets, while controlling traffic through network access control.

There are already subnets existing in my account, one for every Availability Zone in the selected AWS region, allowing me to launch resources without needing to manually create subnets from scratch.

I named my subnet Public 1, but that doesn't automatically make my subnet a public subnet. For a subnet to be considered public, it has to be associated with an Internet Gateway and have a route to the internet.

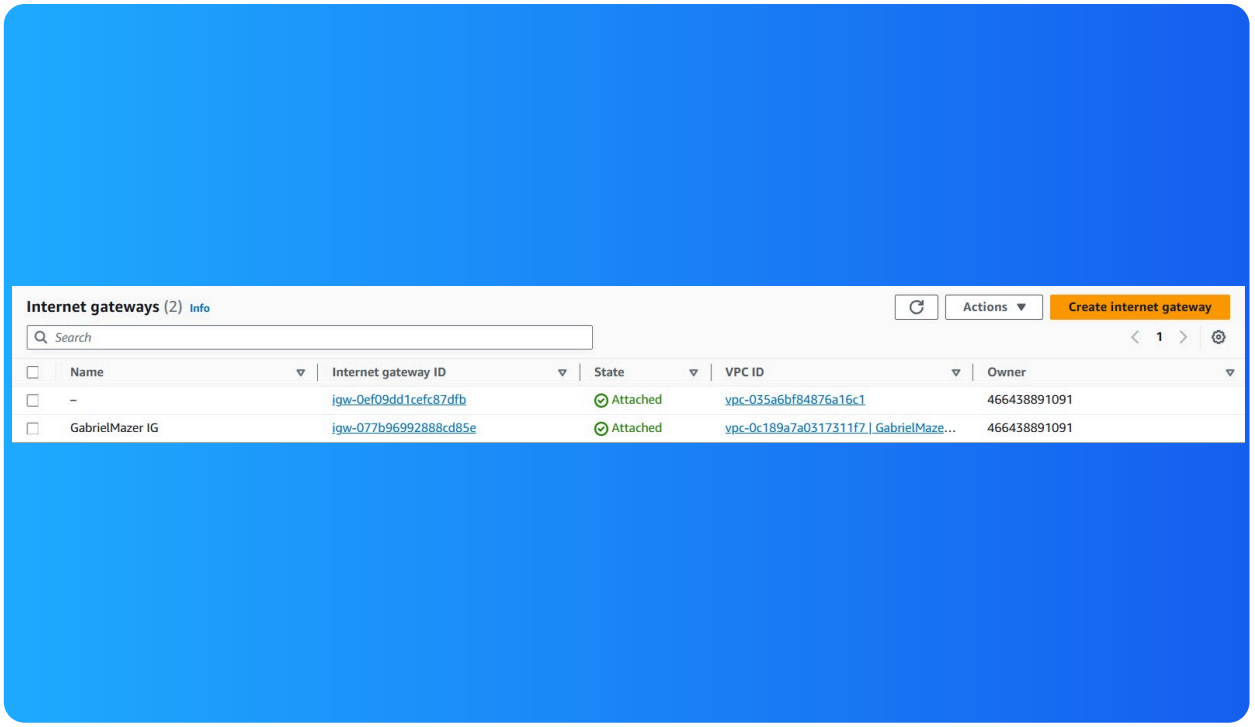


Gabriel Mazer

Internet gateways

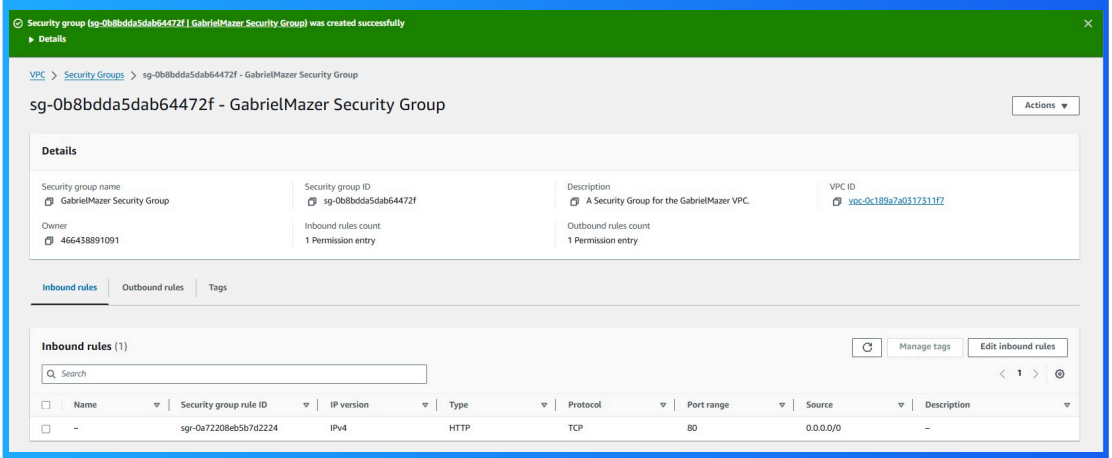
Internet gateways are horizontally scaled, redundant, and highly available gateways that allow communication between resources within a VPC and the internet.

Attaching an internet gateway to a VPC means the resources within the VPC can send and receive data to and from the internet, enabling public access when properly configured.



VPC Traffic Flow and Security

Gabriel Taveira Mazer

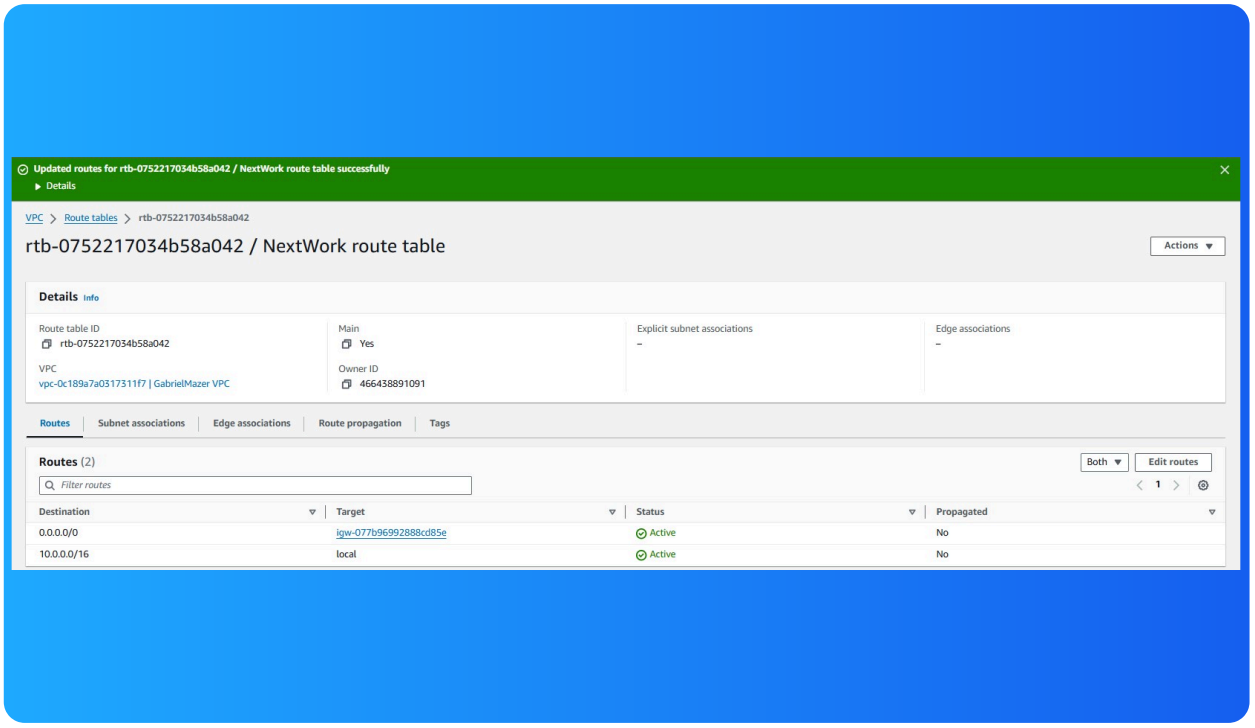


Gabriel Mazer

Route tables

Route tables are a set of rules that direct network traffic. They guide data on where to go within or outside a VPC, like a GPS for resources in a subnet.

Route tables are needed to make a subnet public because they must include a route directing traffic to an internet gateway. This allows communication with external networks.

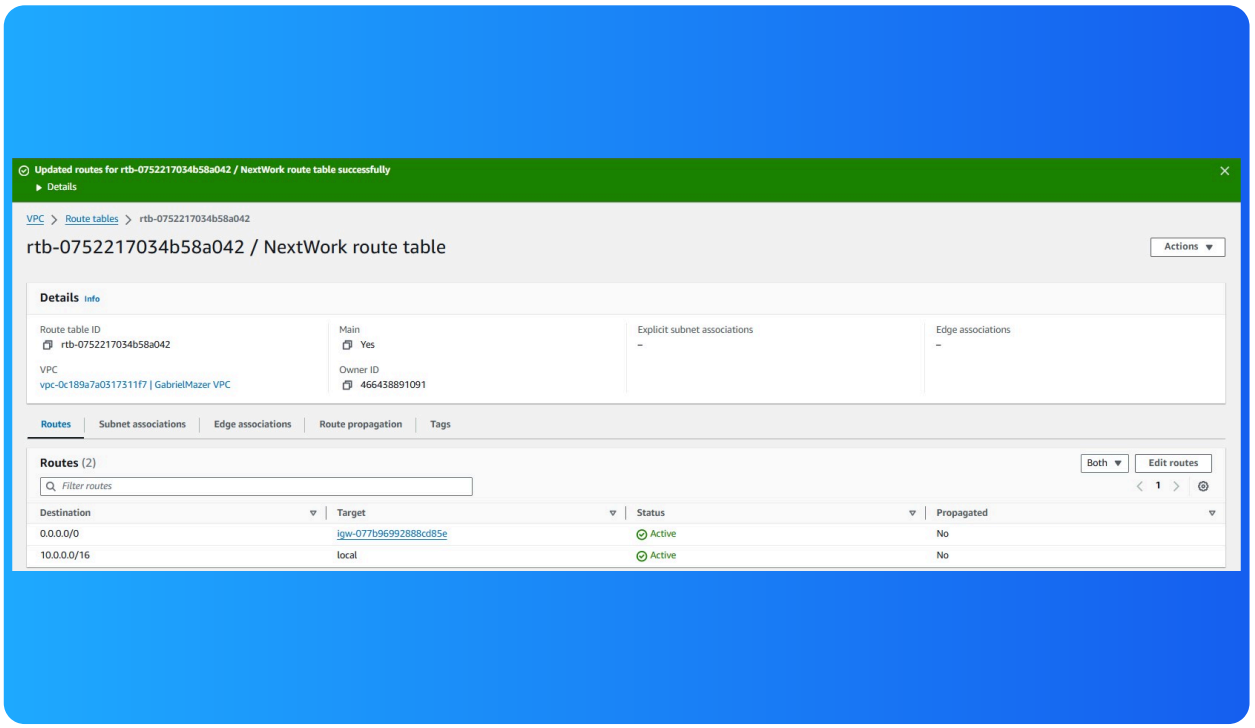


Gabriel Mazer

Route destination and target

Routes are defined by their destination (the IP range traffic wants to reach) and target (the path or resource traffic will use to get there).

The route in my route table that directed internet-bound traffic had a destination of 0.0.0.0/0 (all IPs) and a target of the internet gateway.



Gabriel Mazer

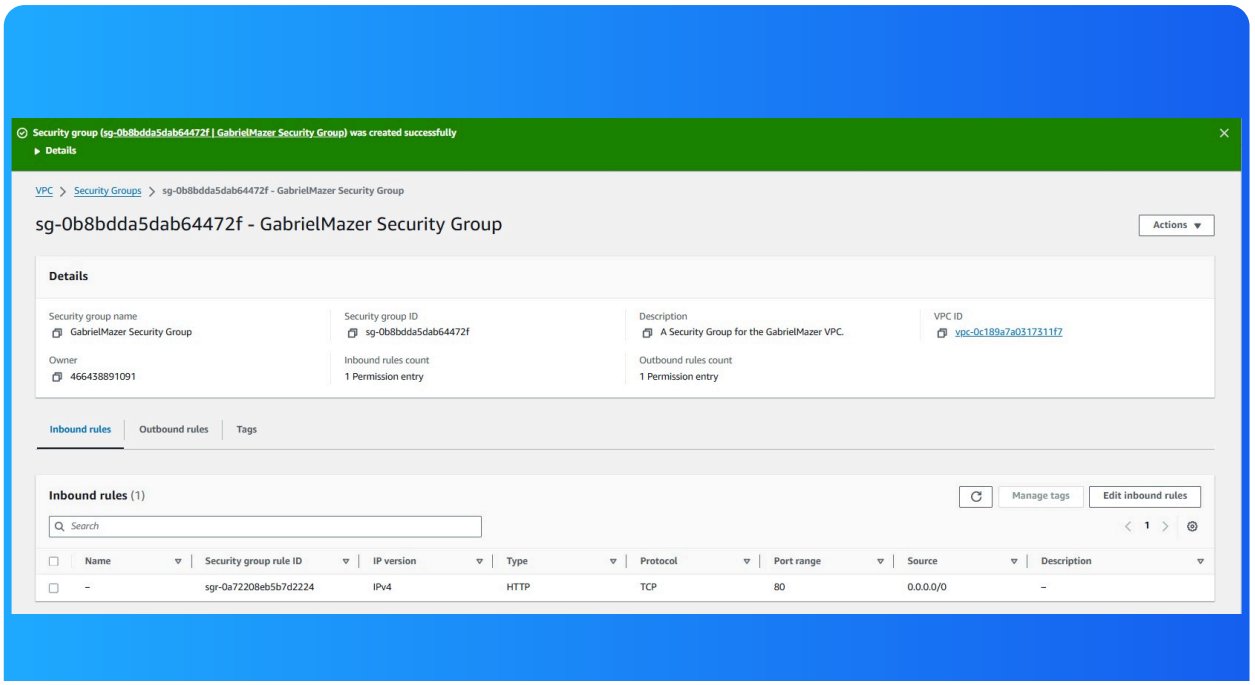
Security groups

Security groups are virtual firewalls that control incoming and outgoing traffic for resources in a VPC, based on defined rules.

Inbound vs Outbound rules

Inbound rules are settings that allow specific traffic to enter a resource. I configured an inbound rule that allows HTTP traffic (port 80) from anywhere (IPv4).

Outbound rules are settings that allow specific traffic to leave a resource. By default, my security group's outbound rule allows all traffic to leave the instance.



Gabriel Mazer

Network ACLs

Network ACLs are like community watchmen that secure traffic at the subnet level in a VPC, controlling inbound/outbound traffic for all resources in the subnet.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that security groups secure resources at the resource level, while network ACLs secure traffic at the subnet level.

Gabriel Mazer

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 in both directions for any protocol.

In contrast, a custom ACL’s inbound and outbound rules are automatically set to deny all traffic until specific allow rules are added.