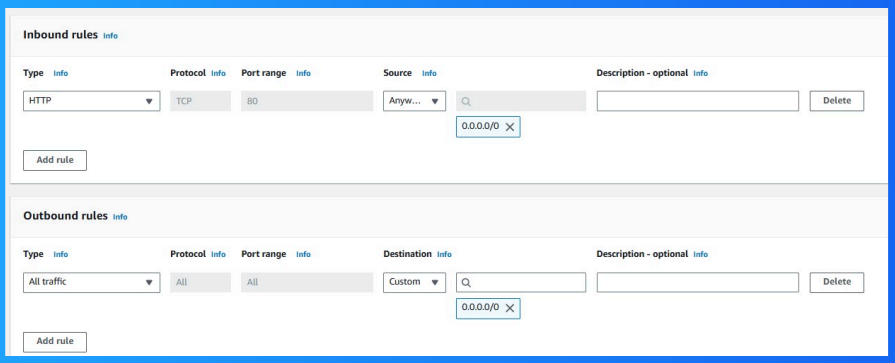
NextWork.org

VPC Traffic Flow and Security

Ronson Lobo



Ronson Lobo
NextWork Student

NextWork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon Virtual Private Cloud (VPC) Security It can be useful for: Security (Inbound outbound filtering), Scalability (scalable infrastructure) Customization (Own ip range, subnets and route tables)

How I used Amazon VPC in this project

I used VPC to check the Traffic Flow and Security of a data packet. A virtual private cloud was created to check the flow of data, security checks, the internet gateway etc

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

I wasn't expecting so many checks happen when a data flow is done

This project took me...

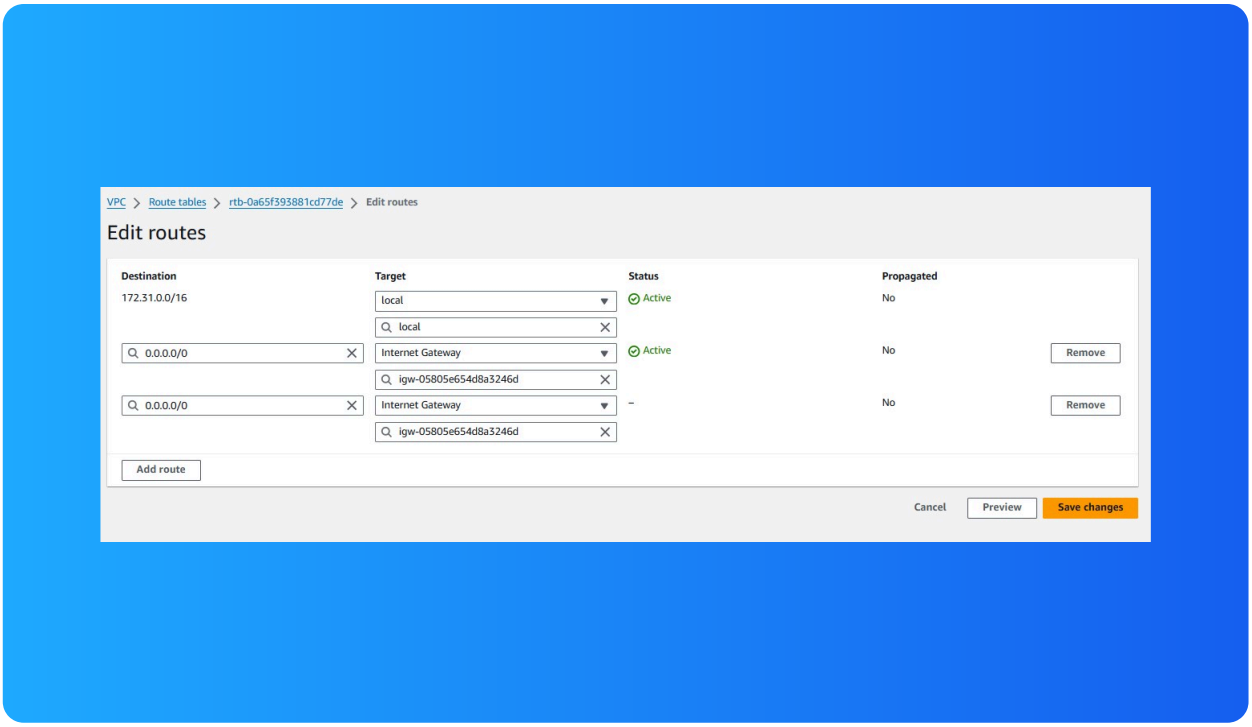
I was able to complete this project in 45 minutes

Ronson Lobo
NextWork Student

Route tables

A route table is a set of rules that help network devices determine the best path for data packets to travel from a source to a destination. Route tables are stored in routers and networked computers, and are often viewed in table format.

A route table is needed to make a subnet public because it controls the routing of network traffic to an internet gateway, which connects the subnet to the internet and other AWS services:

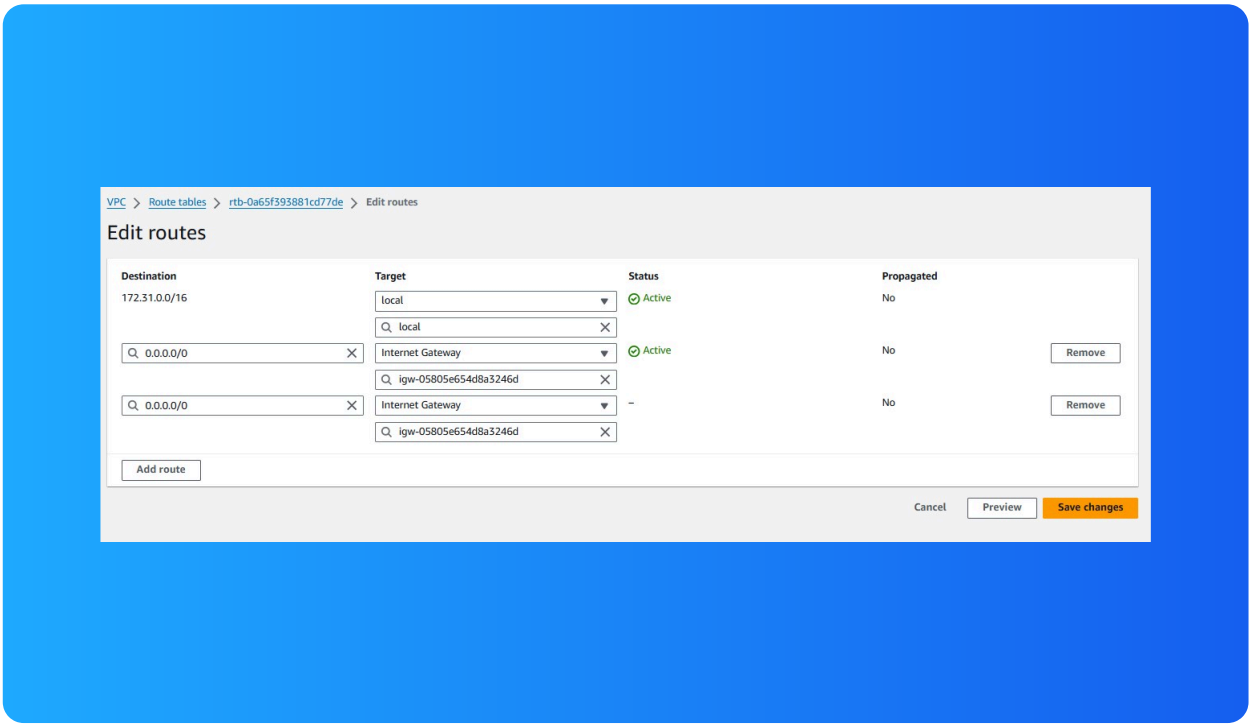


Ronson Lobo
NextWork Student

Route destination and target

In a route table, a route's destination is the range of IP addresses where traffic is to go, and the target is the network device used to reach that destination:

The route in my route table that directed internet-bound traffic to my internet gateway had a destination of all ip and a target of my VPC



Ronson Lobo
NextWork Student

NextWork.org

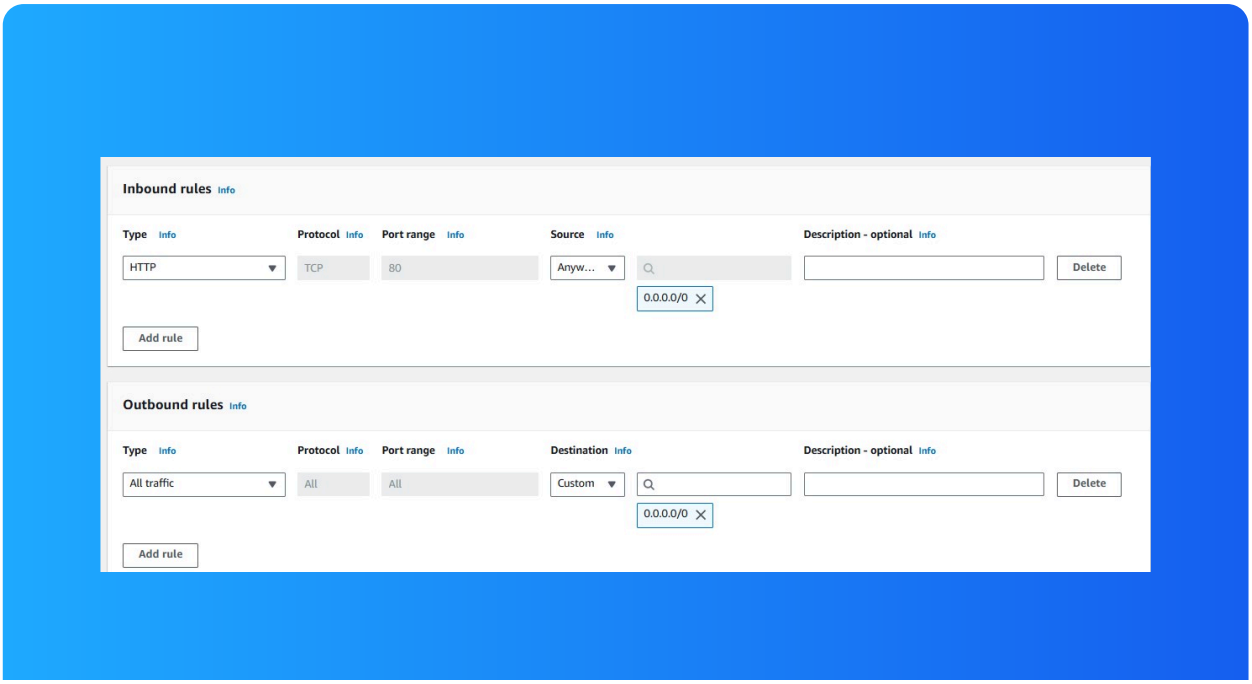
Security groups

Security groups are a way to control traffic to resources and assign permissions to users:

Inbound vs Outbound rules

An inbound rule is a firewall rule that controls traffic coming into a network from other networks or the internet. Inbound rules protect a network from unauthorized access by filtering incoming requests based on criteria like: IP addresses, Port num

Outbound rules control the traffic that leaves a network, and are a type of firewall policy that helps protect internal network resources:



Ronson Lobo
NextWork Student

Network ACLs

A network access control list (ACL) is a set of rules that controls access to a network, allowing or denying specific traffic:

Security groups vs. network ACLs

Security groups control traffic at the instance level, while NACLs control traffic at the subnet level. Security groups are associated with an EC2 instance, while NACLs are associated with a subnet.

Ronson Lobo
NextWork Student

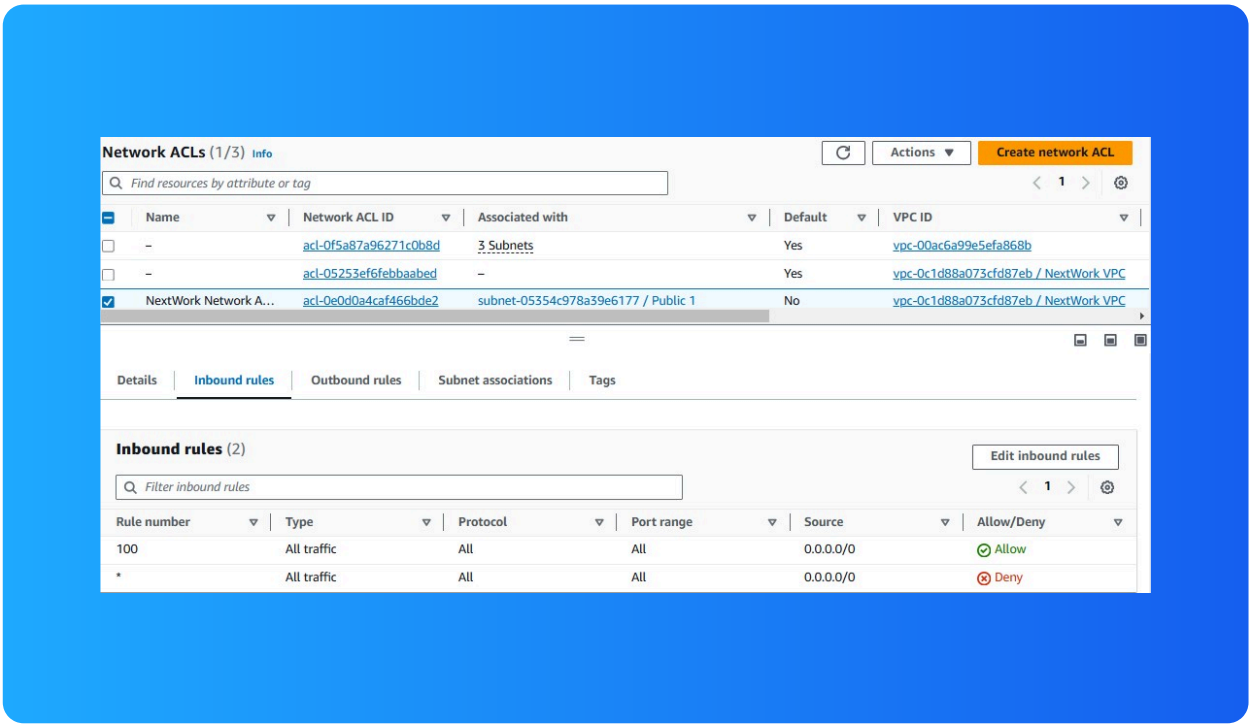
NextWork.org

Default vs Custom Network ACLs

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

The default rule for all inbound and outbound rules in a network access control list (ACL) is to deny all traffic:

A custom network access control list (ACL) inbound or outbound rule allows or denies specific traffic to a subnet:



Everyone should be in a job they love.

Check out nextwork.org for more projects