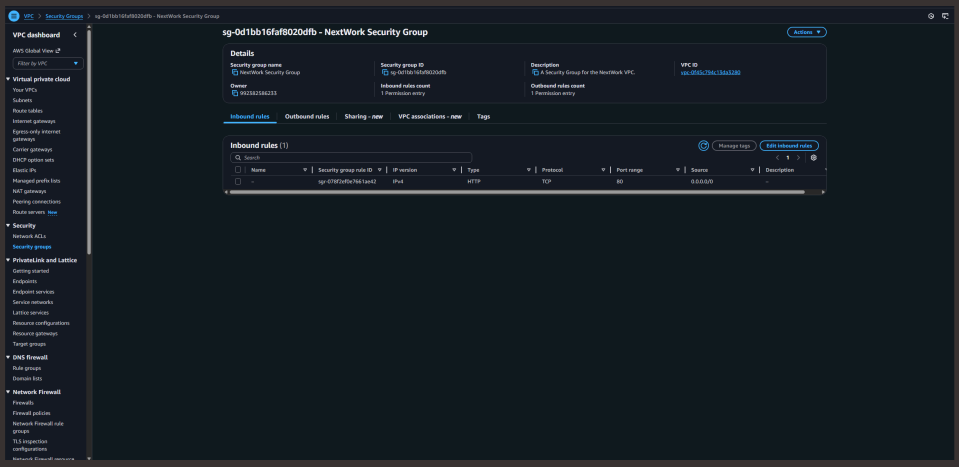
nextwork.org

VPC Traffic Flow and Security

Louis



Louis
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a virtual private network in the AWS cloud where you can launch and manage your resources in an isolated environment that you control, and it is useful because it lets you securely organise your applications, control network traffic, and connect to the internet only when you want to.

How I used Amazon VPC in this project

I used Amazon VPC by first creating a virtual private cloud with a 10.0.0.0/16 IP range, then creating a public subnet (10.0.0.0/24) for my resources. I configured route tables to direct internet traffic (0.0.0.0/0) to my internet gateway, set up security groups to allow HTTP traffic on port 80, and added Network ACLs for an extra layer of security on the subnet level. Then I used the AWS CLI to automate creating the same infrastructure in eu-west-1, and finally used EC2 Global View to see and manage all my resources across both regions in one dashboard.

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

One thing I didn't expect was how critical route tables are to making everything work. I thought creating a subnet and attaching an internet gateway would be enough for internet access, but I learned that without configuring the route table with the 0.0.0.0/0 route pointing to the IGW, nothing connects to the internet.

This project took me...

This project took me around an hour to complete, which included creating the VPC infrastructure manually through the console, setting up all the networking and security components, deploying resources in a second region using AWS CLI, and exploring EC2 Global View to manage everything.

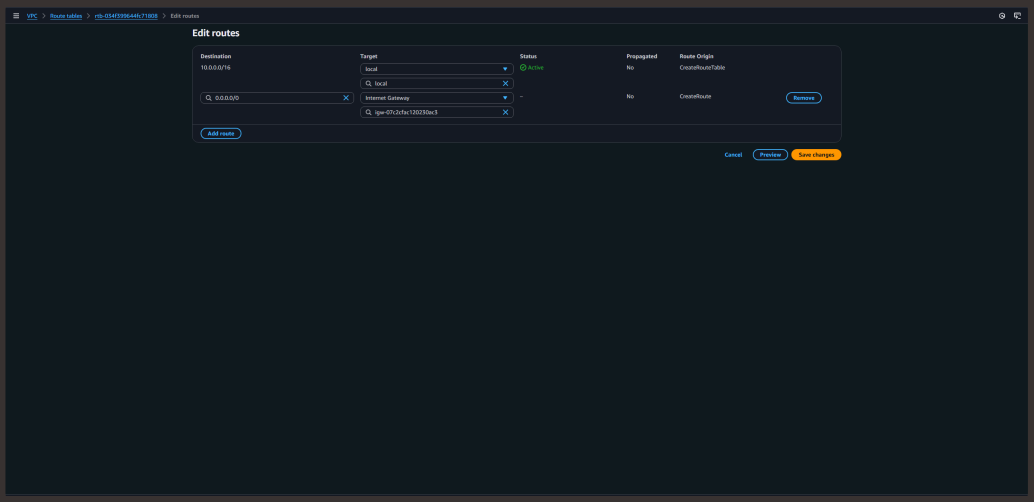
Louis
NextWork Student

nextwork.org

Route tables

Route tables are virtual routers within your VPC that contain a set of rules (routes) evaluated to determine where network traffic should be directed. Whether it stays within the VPC, goes to the internet, or routes to other connected networks.

Route tables are needed to make a subnet public because they provide the instructions that tell traffic how to get to the internet gateway. Without this route, the subnet remains isolated.

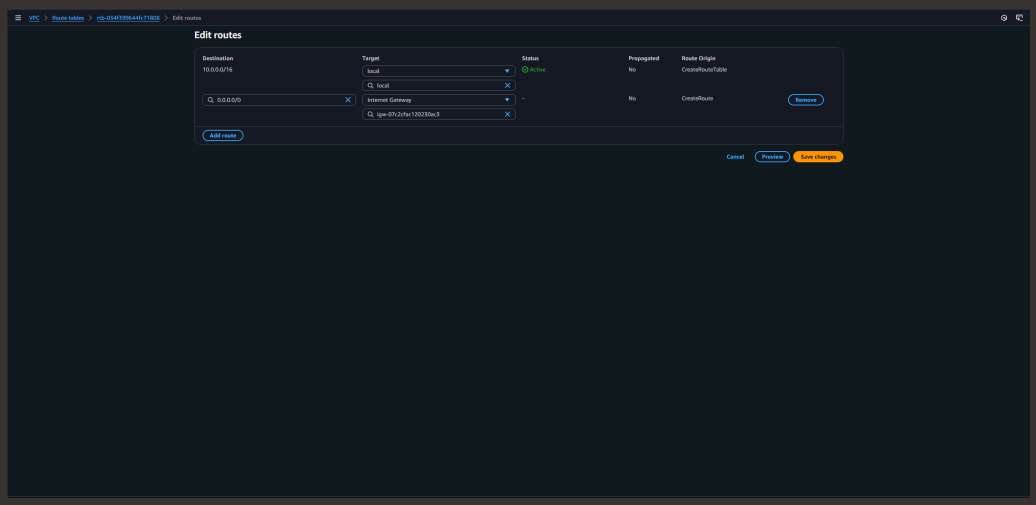


Louis
NextWork Student

Route destination and target

Routes are defined by their destination and target, which mean the destination is the IP address range you're trying to reach, and the target is the gateway or connection that will handle that traffic.

The route in my route table that directed internet-bound traffic to my internet gateway had a destination of 0.0.0.0/0, which is CIDR notation meaning “match any IP address on the internet.” The target was igw-07c2cfac120230ac3, which is the unique identifier of my Internet Gateway (IGW) that AWS uses to route packets between my VPC and the public internet.



Security groups

Security groups are AWS-managed access control mechanisms that act as virtual firewalls for EC2 instances and other resources. They evaluate each network packet against defined rules to determine whether to allow or deny traffic, and they automatically handle return traffic because they are stateful.

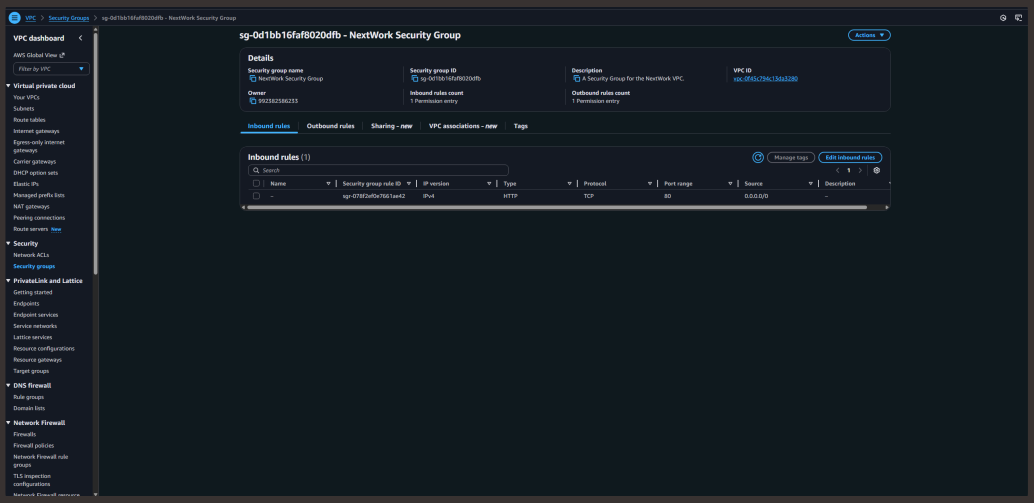
Inbound vs Outbound rules

Inbound rules are security group rules that control what incoming traffic is allowed to reach your resources, specifying which protocols, ports, and sources are permitted to establish connections to your instances. I configured an inbound rule that allows HTTP traffic from anywhere on the internet (0.0.0.0/0), enabling web browsers to access web content hosted on my instances.

Outbound rules are security group rules that control what outgoing traffic is allowed to leave your resources, specifying which protocols, ports, and destinations your instances are permitted to send traffic to. My security group's outbound rule allows all traffic (all protocols on all ports) to any destination (0.0.0.0/0), enabling my instances to communicate freely with any external service or resource on the internet.

Louis
NextWork Student

nextwork.org



Louis
NextWork Student

Network ACLs

Network ACLs are subnet-level firewalls that control what traffic can enter and leave your entire subnet, providing an additional layer of security beyond security groups.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that security groups protect individual instances and remember connections (stateful), while Network ACLs protect entire subnets and don't remember connections (stateless).

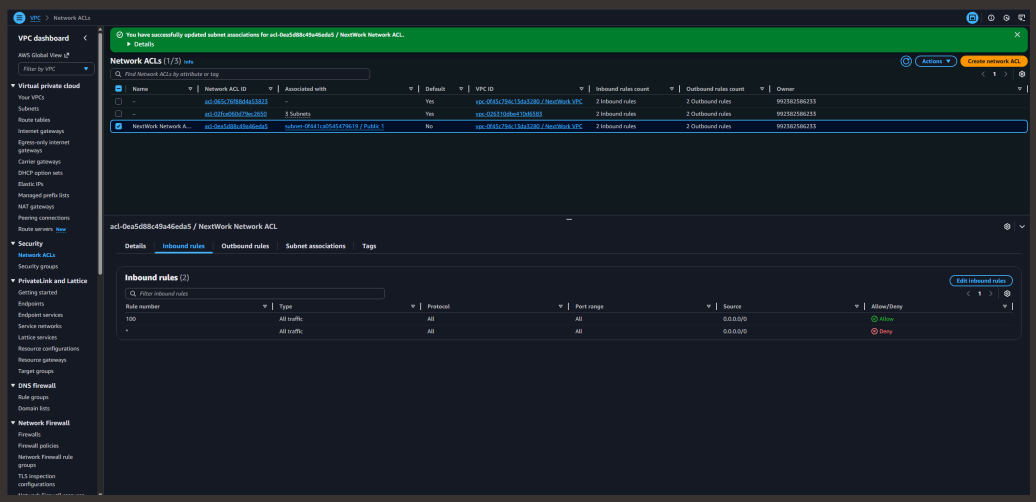
Louis
NextWork Student

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 allow all traffic.

When you create a custom network ACL, both its inbound and outbound rules deny all traffic until you explicitly add rules to allow specific traffic.



Louis
NextWork Student

Tracking VPC Resources

I created additional VPC networking resources (a VPC, an Internet Gateway, and a Security Group) using the AWS CLI in a new region. Instead of my usual region (London), I used eu-west-1 (Ireland). Where I had created resources through the console. Teams would use multiple regions to achieve high availability and disaster recovery, reduce latency for global users, comply with data residency regulations, and ensure business continuity if one region experiences an outage.

EC2 Global View is a tool where you can find all your AWS resources across every region in one place. I could even narrow down my search by region, making it easy to filter specific locations. Without EC2 Global View, you'd have to manually switch regions and check each one individually.

I would use EC2 Global View again whenever I need to quickly see all my AWS resources across multiple regions at once, find specific resources without remembering which region they're in, or check for unused resources that are costing money.

nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects