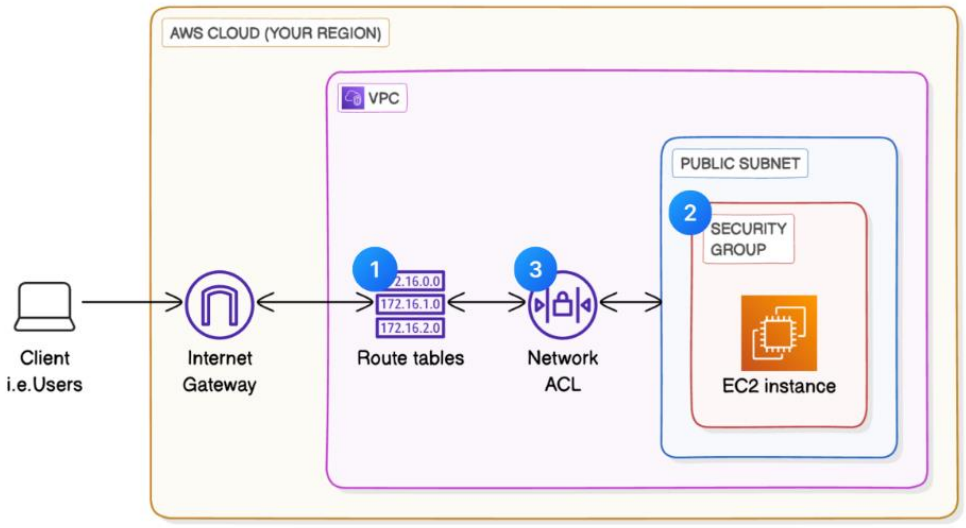
VPC Traffic Flow and Security



Today's game plan.

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) allows you to create a private, isolated network in AWS. It gives control over IP ranges, subnets, routing, and security, enabling secure communication, internet access, and connections to onpremises networks.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create a secure, isolated network for resources. I set up subnets, route tables, and security groups to manage traffic flow, ensuring secure communication between instances and controlled internet access.

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

One thing I didn't expect in this project was the complexity of configuring network security settings, like security groups and network ACLs. It required careful attention to detail to ensure proper access while maintaining strong security controls.

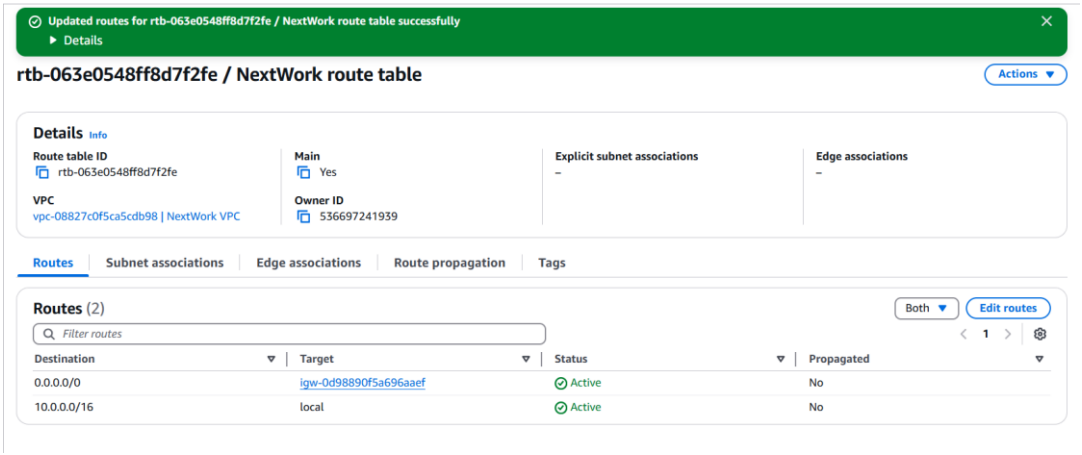
This project took me...

This project took me half an hour to complete.

Route tables

Route tables are data structures that define how network traffic is directed. They contain rules specifying destination IP ranges and the next hop for routing traffic, ensuring proper data flow between subnets, networks, and external destinations.

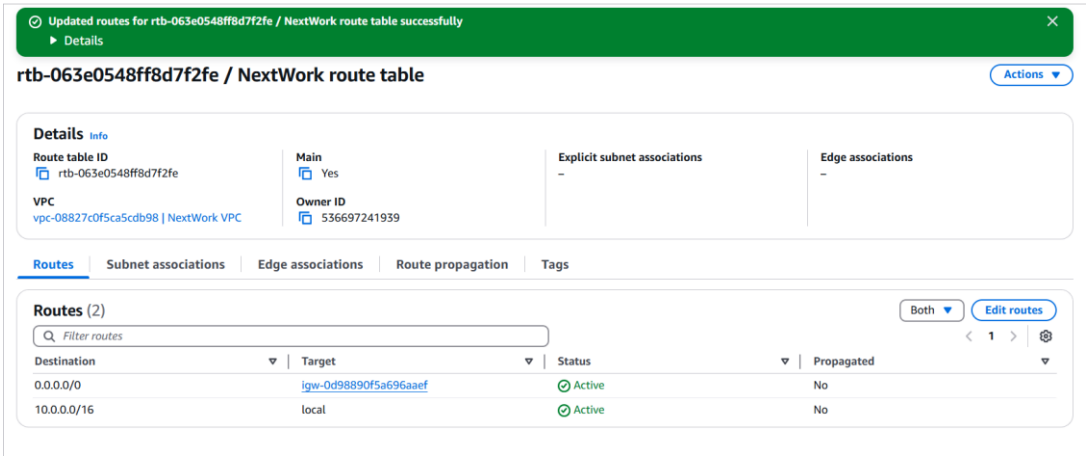
Route tables are needed to make a subnet public because they control how traffic is routed. By adding a route to the internet gateway, traffic from the subnet can reach external destinations, allowing it to be accessed from the internet.



Route destination and target

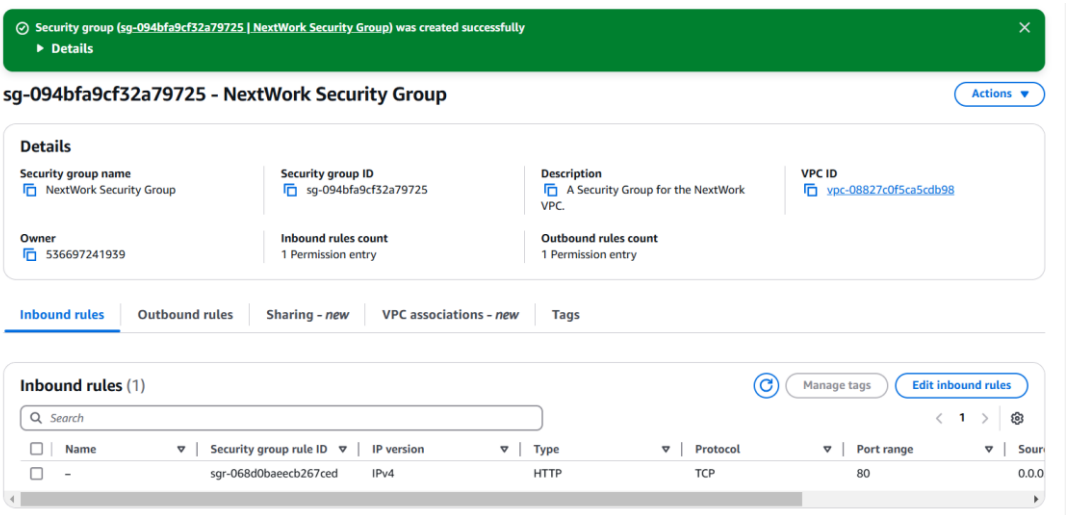
Routes are defined by their destination and target, which mean the destination is the IP address range the route applies to, and the target is where the traffic should be sent, such as an internet gateway, virtual machine, or another network device.

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 (e.g., igw-xxxxxxxx), routing all traffic from the subnet to the internet.



Security groups

Security groups are virtual firewalls that control inbound and outbound traffic to resources in a cloud environment. They define rules based on IP addresses, ports, and protocols, allowing, or denying traffic to secure instances and other resources.



Inbound vs Outbound rules

Inbound rules are rules that control the incoming traffic to a resource, specifying which traffic is allowed to reach the resource. I configured an inbound rule that allows traffic on port 80 (HTTP) from any IP address (0.0.0.0/0) to my EC2 instance.

Outbound rules are rules that control outgoing traffic from a resource, specifying which traffic can leave. By default, my security group's outbound rule allows all traffic to leave the instance, with no restrictions on destination IPs or ports.

Network ACLs

Network ACLs are security layers that control inbound and outbound traffic at the subnet level in a VPC. They consist of a set of rules that allow or deny traffic based on IP address, protocol, and port, providing an additional layer of security.

Security groups vs. network ACLs

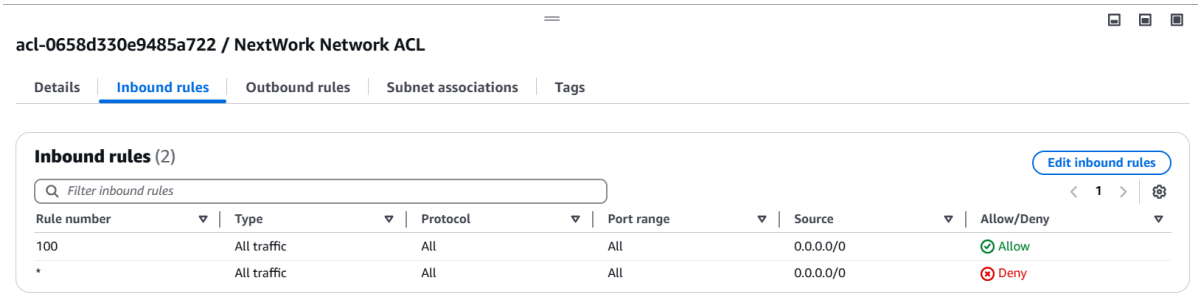
The difference between a security group and a network ACL is that security groups control traffic at the instance level and are stateful, while network ACLs control traffic at the subnet level and are stateless, requiring rules for both directions.

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 (0.0.0.0/0) to enter and leave the subnet, meaning no restrictions on any IP address, port, or protocol. This allows full access unless custom rules are defined.

In contrast, a custom ACL’s inbound and outbound rules are automatically set to deny all traffic by default. You must manually configure rules to allow specific traffic, defining IP addresses, ports, and protocols to control access to resources.



Today you've learnt how to:

- 🪠 **Set up route tables:** You configured a route table in your VPC to send Internet-bound traffic to your internet gateway, turning your subnet into a public subnet.
- 👮 **Implement security groups:** You created a security group to control inbound and outbound traffic at a resource level, specifying allowed IP addresses, protocols, and ports.
- 📋 **Deploy network ACLs:** You set up network ACLs as an additional layer of security, managing both incoming and outgoing traffic at the subnet level.