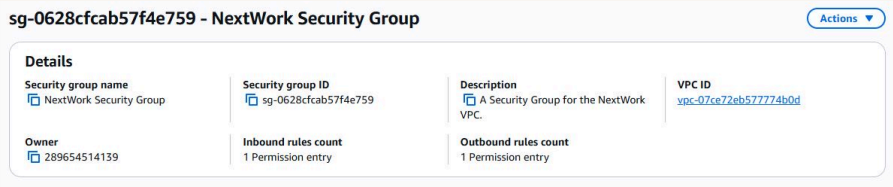
nextwork.org

VPC Traffic Flow and Security

Mohammed Dawoud Mota



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a virtual private cloud that isolates your resources in the AWS cloud. It’s useful because it gives you full control over network configuration, subnets, security, and internet access.

How I used Amazon VPC in this project

I used Amazon VPC to create a private network for my resources. I set up a VPC, added a public subnet, attached an internet gateway, configured a route table, security group, and network ACL to control traffic and access.

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

One thing I didn’t expect was how many layers of security are involved. Between route tables, security groups, and network ACLs, it was interesting to see how AWS controls traffic at both the subnet and resource levels.

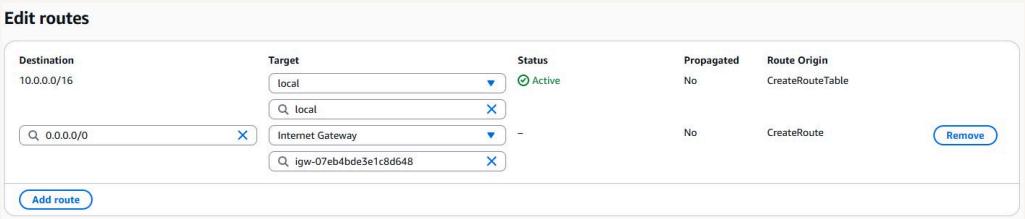
This project took me...

This project took me 30 minutes to complete.

Route tables

A route table is a set of rules in AWS that direct subnet traffic. Routes define a destination IP range and a target, such as “local” for VPC traffic or an internet gateway for external traffic.

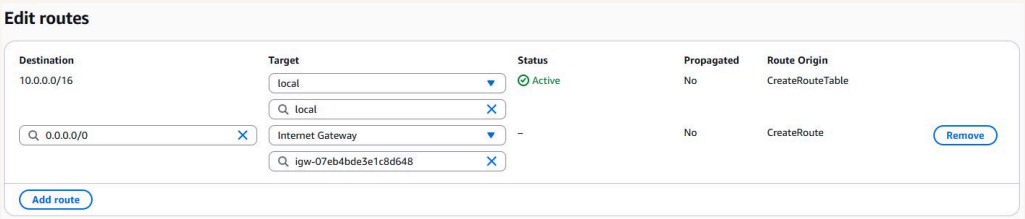
A subnet becomes public only if its route table has a route (0.0.0.0/0) pointing to an internet gateway. This route lets resources in the subnet send and receive traffic from the internet. Without it, the subnet stays private.



Route destination and target

In a route, the destination is the IP range the traffic wants to reach, and the target is where that traffic is sent, like an internet gateway for external traffic or “local” for traffic inside the VPC.

The new route’s destination is 0.0.0.0/0, meaning all IPv4 addresses, and the target is the internet gateway, which sends traffic from the subnet to the internet.



Security groups

A security group is a virtual firewall for AWS resources. It controls inbound and outbound traffic at the resource level, allowing specific IPs, protocols, and ports while blocking all other traffic by default.

Inbound vs Outbound rules

An inbound rule controls the traffic that can enter a resource. My security group's inbound rule allows HTTP traffic (port 80) from anywhere (0.0.0.0/0) so users can access.

An outbound rule controls the traffic that can leave a resource. My security group's outbound rules allow all traffic by default, so my resources can send data anywhere without restrictions.


sg-0628cfcab57f4e759 - NextWork Security Group
Actions
Details
Security group name
NextWork Security Group
Security group ID
sg-0628cfcab57f4e759
Description
A Security Group for the NextWork VPC.
VPC ID
vpc-07ce72eb577774b0d
Owner
289654514139
Inbound rules count
1 Permission entry
Outbound rules count
1 Permission entry

Network ACLs

Network ACLs are like traffic cops for a subnet. They control inbound and outbound traffic at the subnet level, checking each data packet against rules before allowing it to pass, adding an extra layer of security.

Security groups vs. network ACLs

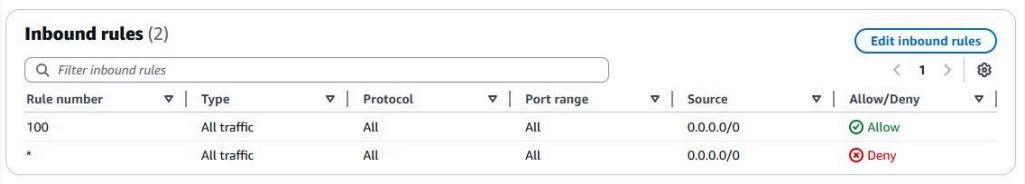
Security groups control traffic at the resource level, managing which IPs, protocols, and ports can access specific resources. Network ACLs control traffic at the subnet level, applying broader rules to all resources in the subnet.

Default vs Custom Network ACLs

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

The default network ACL allows all inbound and outbound traffic. This means every data packet can enter and leave the subnet unless you create custom rules to restrict it.

A custom network ACL starts by denying all traffic by default. You must add rules to explicitly allow or deny specific inbound or outbound traffic, controlling what enters or leaves the subnet.



The place to learn & showcase your skills

Check out nextwork.org for more projects