



VPC Traffic Flow and Security



Lawrence T. Maguranye

The screenshot shows the AWS VPC Security Groups console. The left sidebar includes links for Your VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, Carrier gateways, DHCP option sets, Elastic IPs, Managed prefix lists, NAT gateways, Peering connections, Security (Network ACLs, Security groups), and PrivateLink and Lattice (Getting started, Updated Endpoints, Endpoint services). The main content area displays the details for the security group 'sg-06d07e8422ce95aad - NextWork Security Group'. The 'Details' section shows the security group name ('NextWork Security Group'), security group ID ('sg-06d07e8422ce95aad'), description ('A Security Group for the NextWork VP'), and VPC ID ('vpc-0da4c2e285eaf6cd'). It also shows the owner ('855955484490'), inbound rules count (1 Permission entry), and outbound rules count (1 Permission entry). The 'Inbound rules' tab is selected, showing one rule: a TCP port 80 rule from IP range sgr-0840x9x43820e93f to port 80. There are tabs for Outbound rules, Sharing - new, VPC associations - new, and Tags.

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC lets you create a private network within AWS where you control IP addresses, subnets, routing, and security. It's useful for securely hosting resources like EC2 instances and databases, with full control over traffic flow and access.

How I used Amazon VPC in this project

I used Amazon VPC to set up a secure network with a public subnet, routing, and access controls—perfect for organizing my project into isolated, manageable layers.

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

One thing I didn't expect in this project was how easily a small routing misconfiguration could block access between tiers—it was a great reminder that in cloud networking, even tiny details matter.

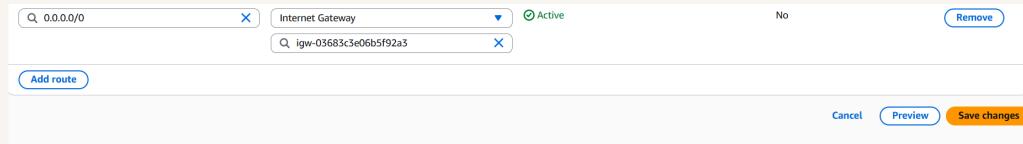
This project took me...

I took me about 2 hours to complete this task.

Route tables

It is a set of rules, called routes, used to determine where network traffic is directed. They are associated with subnets in a VPC and play a key role in controlling the flow of traffic within your cloud network and between the internet.

Routes tables are needed to make a subnet public because a subnet becomes public in AWS only when its route table contains a route to the Internet Gateway (IGW). Without this route, resources in the subnet cannot communicate with the internet.



Route destination and target

Routes are defined by their destination and target, which means the destination specifies the range of IP addresses the traffic is intended for, and the target is the gateway through which that traffic should be directed to reach its destination.

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 igw-03683c3e06b5f92a3.

A screenshot of a user interface for managing network routes. At the top, there are two input fields: 'Destination' containing '0.0.0.0/0' and 'Gateway' containing 'Internet Gateway'. Below these is a dropdown menu set to 'Active'. To the right of the gateway field is a 'Remove' button. Further down, there is another input field for 'Target' containing 'igw-03683c3e06b5f92a3', with a 'Remove' button next to it. At the bottom left is a blue 'Add route' button. On the far right are three buttons: 'Cancel', 'Preview' (in a light blue box), and 'Save changes' (in an orange box).

Security groups

Security groups are virtual firewalls in AWS that control inbound and outbound traffic for resources like EC2 instances. They act as gatekeepers, allowing or denying traffic based on rules you define.

Inbound vs Outbound rules

Inbound rules are access control settings that define which incoming traffic is allowed to reach an AWS resource, such as an EC2 instance. I configured an inbound rule that allows all inbound HTTP traffic.

Outbound rules are settings that control which types of traffic your AWS instance is allowed to send out to the internet or other network destinations. By default, my security group's outbound rule will allow all outbound traffic.

TA

Lawrence T. Maguranye

NextWork Student

nextwork.org

The screenshot shows the AWS VPC Security Groups console. On the left, there's a navigation sidebar with links like 'Your VPCs', 'Subnets', 'Route tables', etc., and sections for 'Security' (Network ACLs, Security groups), 'PrivateLink and Lattice' (Getting started, Endpoints, Endpoint services). The main area displays the details for a security group named 'sg-06d07e8422ce95aad - NextWork Security Group'. The 'Details' section includes fields for 'Security group name' (NextWork Security Group), 'Security group ID' (sg-06d07e8422ce95aad), 'Owner' (835955484490), 'Description' (A Security Group for the NextWork VP C.), 'VPC ID' (vpc-0da4c2e285eaf6ecd), 'Inbound rules count' (1 Permission entry), and 'Outbound rules count' (1 Permission entry). Below this, there are tabs for 'Inbound rules', 'Outbound rules', 'Sharing - new', 'VPC associations - new', and 'Tags'. The 'Inbound rules' tab shows one rule: sgr-084bc9c4382c0e93f, which is IPv4, HTTP, TCP, and port 80.

Network ACLs

Network ACLs are stateless, subnet-level firewalls in AWS that control inbound and outbound traffic in and out of your Virtual Private Cloud (VPC). Network ACLs evaluate every request independently—both coming in and going out.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that security groups are stateful and operate at the instance level, while network ACLs are stateless and work at the subnet level.

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 to flow in and out of the associated subnet. This means every protocol, every port range, and all IP addresses (0.0.0.0/0 for IPv4 and ::/0 for IPv6) are permitted.

In contrast, a custom ACL's inbound and outbound rules are set to deny all traffic by default. Until you define specific allow rules for certain ports, protocols, and IPs, no data can flow in or out of the subnet

The screenshot shows the AWS VPC Network ACLs interface. On the left, there's a navigation sidebar with options like VPC dashboard, EC2 Global View, Virtual private cloud (Your VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, Carrier gateways, DHCP option sets, Elastic IPs, Managed prefix lists, NAT gateways, Peering connections), and Security (Network ACLs). The main area displays 'Network ACLs (1/2) Info' with two entries:

Name	Network ACL ID	Associated with	Default	VPC ID	Inbo
-	acl-027d692168cf2e381	3 Subnets	Yes	vpc-084a586a7c2573023	2 Int
<input checked="" type="checkbox"/>	acl-0e2f8025a19463d71	subnet-090a031027cc88aaa / Public.1	Yes	vpc-0da4c2e285eaaf6ec0 / NextWork VPC	2 Int

Below this, the details for 'acl-0e2f8025a19463d71' are shown. The 'Outbound rules' tab is selected, displaying two rules:

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

