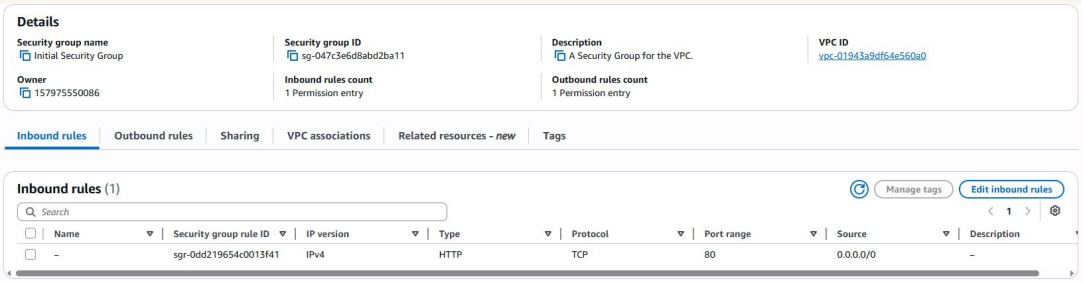
VPC Traffic Flow and Security

Melvin green



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a service that lets you create your own isolated virtual network within AWS, where you can launch and manage resources like EC2 instances, databases, and other services

in a secure environment. It is useful because it gives you full control over your network configuration, including IP ranges, subnets, route tables, and security settings, allowing you to design and protect your cloud infrastructure while keeping your resources isolated from other users in AWS.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create and manage my own isolated cloud network, where I set up subnets, route tables, an Internet Gateway, and security controls like a Security Group and a Network ACL. This allowed me to control how resources communicate with each other and with the internet, while keeping the environment secure and organized.

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

One thing I didn’t expect in this project was how many different networking components had to work together just to make a simple connection work properly. I thought setting up an Amazon VPC would mainly involve creating resources like EC2 instances, but I learned that I also needed to correctly configure subnets, route tables, an Internet Gateway, a Security Group, and a Network ACL. It was surprising how each part plays a specific role, and if even one setting is incorrect, the whole connection can fail.

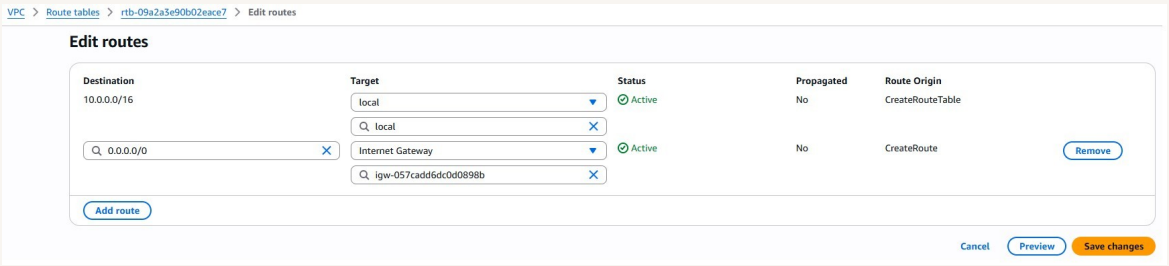
This project took me...

This project took me about 1 and a half hours, including demo time and additional learning about each component, which helped me build a better understanding of how everything works together in an Amazon VPC environment.

Route tables

Route tables are like a GPS (or road map) for network traffic in a subnet. It contains a set of rules, called routes, that tell data packets where to go next based on their destination address; whether that's within the VPC, to the internet, or to another network (like a VPN or peered VPC).

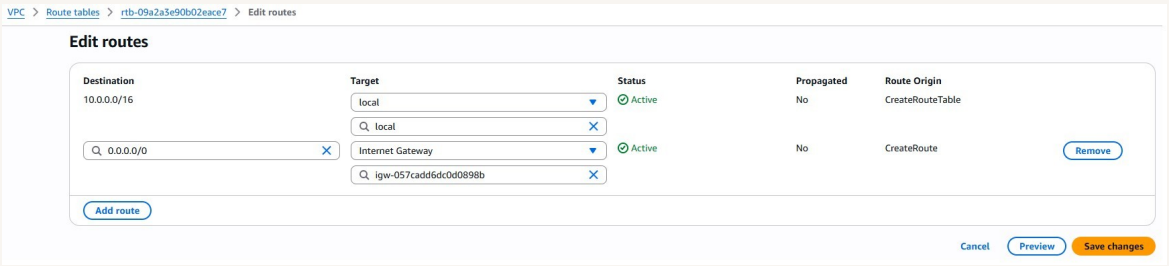
Route tables are needed to make a subnet public because a public subnet needs a route that sends internet-bound traffic to an Internet Gateway. A route table is the only way to establish this connection.



Route destination and target

A route in an AWS route table consists of a destination and a target. The destination is a range of IP addresses that traffic in my VPC is trying to reach. While the target is the path that the traffic will use to get to their 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 my internet gateway.



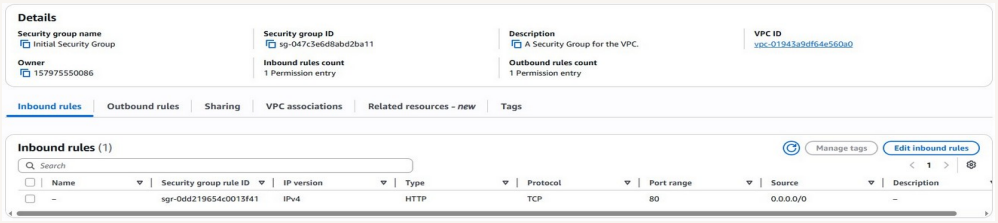
Security groups

A Security Group can be thought of as a security checkpoint at the entrance of each resource in your subnet. Just like a security guard controls who is allowed to enter or leave a building, a security group controls which inbound and outbound traffic is allowed to access your resources, helping keep your VPC secure by only permitting authorized connections.

Inbound vs Outbound rules

Inbound rules are the rules that monitor/restrict inbound traffic, e.g., users visiting a website app I’m hosting. I configured an inbound rule that allows all inbound HTTP traffic.

Outbound rules are the rules that monitor/restrict outbound traffic, for example, a web app requesting data from a public source. By default, my security group's outbound rule will allow all outbound traffic.



Network ACLs

Network ACLs are a set of rules that secure the network at the subnet level.

Security groups vs. network ACLs

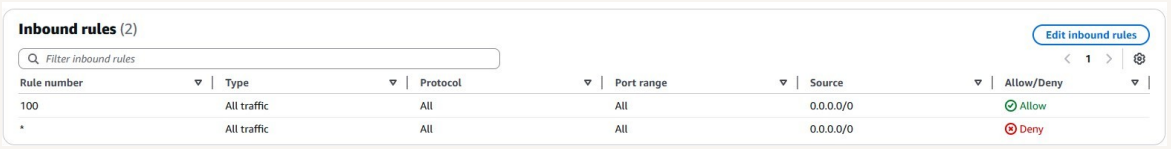
The main difference between a Security Group and a Network ACL is their scope. A security group protects your VPC at the resource level, meaning each individual resource, such as an EC2 instance, is associated with a security group that controls its inbound and outbound traffic. In contrast, a Network ACL protects your VPC at the subnet level, meaning each subnet is associated with a Network ACL that controls traffic entering and leaving the entire subnet. In simple terms, security groups act as protection for individual resources, while Network ACLs provide security for the whole subnet.

Default vs Custom Network ACLs

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

By default, a network ACL's inbound rule will allow all incoming traffic, and outbound rules will allow all outgoing traffic.

In contrast, a custom ACL’s inbound and outbound rules are automatically set to deny all incoming/outgoing traffic.

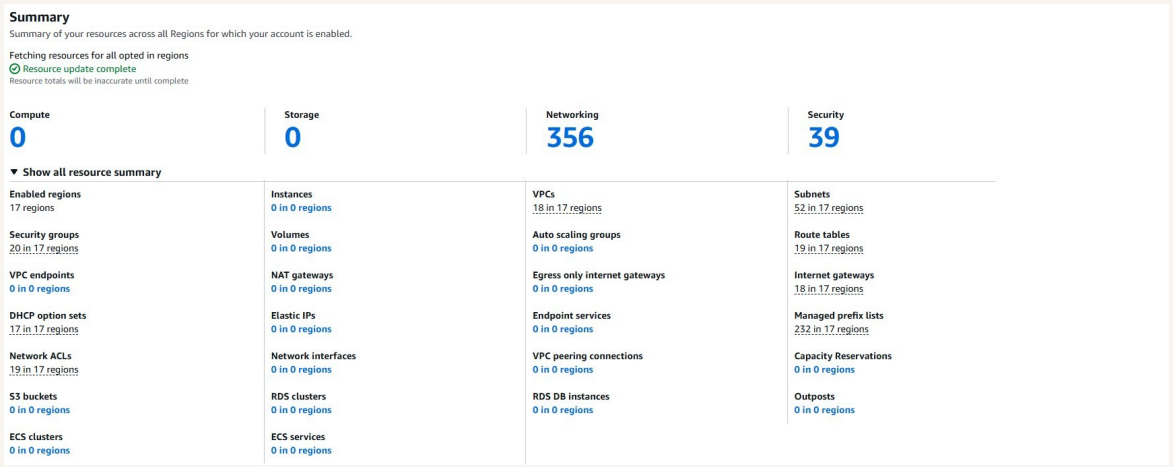


Tracking VPC Resources

I created an additional Amazon VPC, an Internet Gateway, and a Security Group in a different region, specifically us-west-1, instead of my usual region. Using multiple regions helps improve latency for end users because resources can be deployed closer to their physical location, making applications run faster and more responsive. It also improves reliability and disaster recovery, since if one region experiences an outage or failure, other regions can continue running and keep the application available.

Amazon EC2 Global View is a tool that lets you see and manage your EC2 and VPC resources across all AWS Regions from a single dashboard. It allows you to quickly find resources like instances, Amazon VPCs, and Security Groups, and you can even filter or narrow your search by specific categories such as VPCs or security groups. Without EC2 Global View, you would need to manually switch between different AWS Regions to track your resources, which can be time-consuming and harder to manage. This unified view makes it much easier to monitor everything running across multiple regions, especially in multi-region deployments.

Now that I've learned about Amazon EC2 Global View, I would use it again to quickly monitor and manage all my EC2 and Amazon VPC resources across multiple AWS Regions from one place. It would help me verify that my resources are correctly deployed, troubleshoot any issues faster, and ensure my multiregional setup is consistent and running smoothly without needing to switch between regions manually.


Summary
Summary of your resources across all Regions for which your account is enabled.
Fetching resources for all opted in regions
Resource update complete
Resource totals will be inaccurate until complete
Compute
0
Storage
0
Networking
356
Security
39
Show all resource summary
Enabled regions
17 regions
Security groups
20 in 17 regions
VPC endpoints
0 in 0 regions
DHCP option sets
17 in 17 regions
Network ACLs
19 in 17 regions
S3 buckets
0 in 0 regions
ECS clusters
0 in 0 regions
Instances
0 in 0 regions
Volumes
0 in 0 regions
NAT gateways
0 in 0 regions
Elastic IPs
0 in 0 regions
Network interfaces
0 in 0 regions
RDS clusters
0 in 0 regions
ECS services
0 in 0 regions
VPCs
18 in 17 regions
Auto scaling groups
0 in 0 regions
Egress only internet gateways
0 in 0 regions
Endpoint services
0 in 0 regions
VPC peering connections
0 in 0 regions
RDS DB instances
0 in 0 regions
Subnets
52 in 17 regions
Route tables
19 in 17 regions
Internet gateways
18 in 17 regions
Managed prefix lists
232 in 17 regions
Capacity Reservations
0 in 0 regions
Outposts
0 in 0 regions