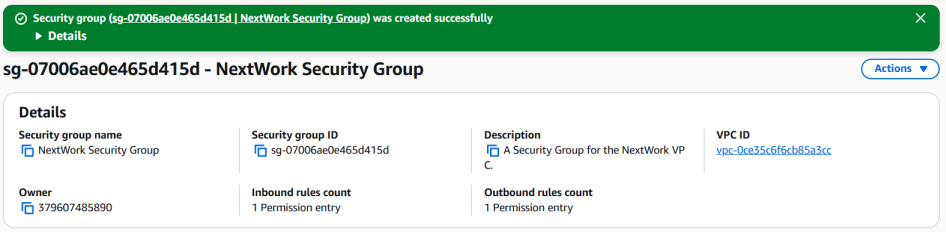
nextwork.org

VPC Traffic Flow and Security

SA sabastinemc@gmail.com



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a virtual private network in AWS that lets you launch AWS resources in an isolated, secure environment. It is useful because it gives you control over your network configuration, including IP addresses, subnets, route tables, and security settings, allowing you to securely run applications in the cloud.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create an isolated network in a new AWS Region, set up an Internet Gateway for external access, and configure a security group to control traffic to my resources.

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

One thing I didn't expect in this project was how easy it is to manage and view resources across multiple AWS Regions using tools like EC2 Global View, instead of manually checking each region.

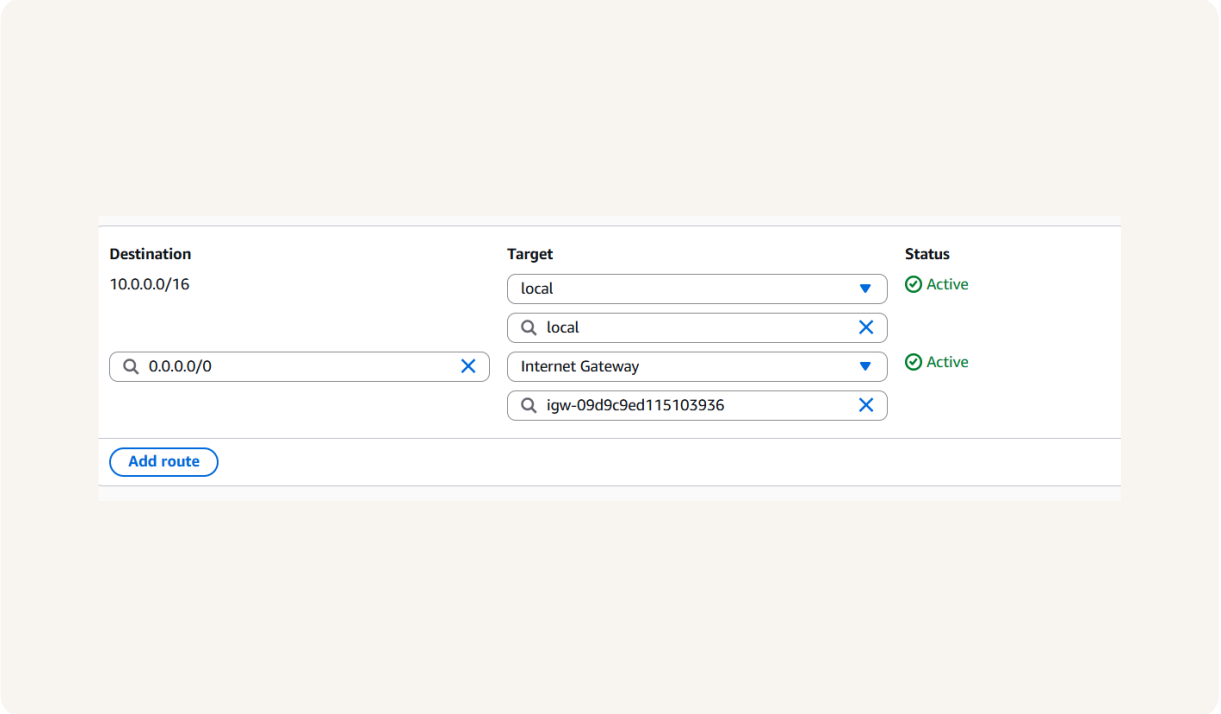
This project took me...

This project took me about 3 hours to complete, including creating the VPC, Internet Gateway, and Security Group in a new region and exploring EC2 Global View.

Route tables

Route tables are virtual routing rules within a VPC that determine how network traffic is directed. They control where traffic goes, whether to the internet gateway, another subnet, a NAT gateway, or other network connections, based on defined destination routes.

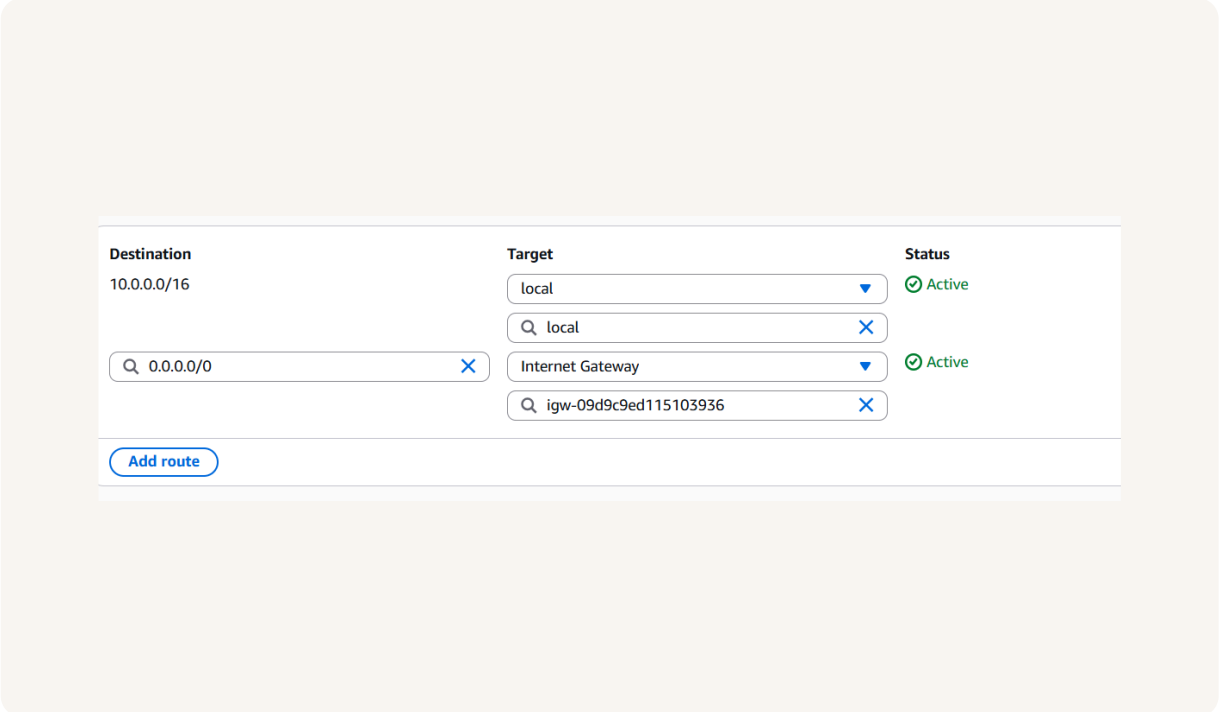
Route tables are needed to make a subnet public because they define a route (0.0.0.0/0) that directs internet-bound traffic to an Internet Gateway. Without this route, the subnet has no path to the internet and remains private.



Route destination and target

Routes are defined by their destination and target, which mean the destination is the IP address range where the traffic is going (for example, 0.0.0.0/0 for all internet traffic), and the target is the resource that handles that traffic (such as an Internet Gateway, NAT Gateway, VPC Peering connection, or Transit Gateway).

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 (igw-09d9c9ed115103936).



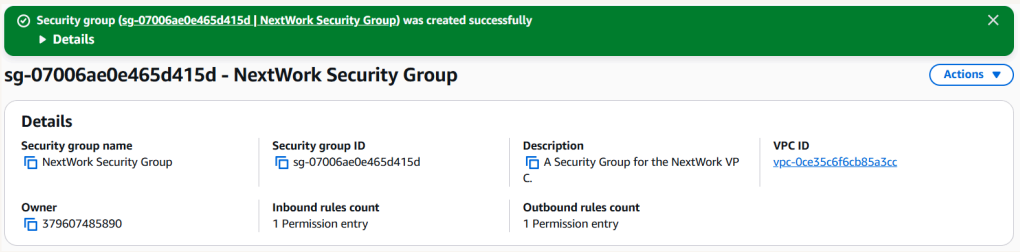
Security groups

Security groups are virtual firewalls that control inbound and outbound traffic for specific AWS resources. They define which traffic is allowed based on IP address, protocol, and port number, helping secure resources within a VPC.

Inbound vs Outbound rules

Inbound rules are rules that control what incoming traffic is allowed to reach a resource. They specify the source (IP address range), protocol, and port number that are permitted to access the resource. I configured an inbound rule that allows HTTP traffic on port 80 from 0.0.0.0/0 so that web traffic from the internet can reach my resource.

Outbound rules are rules that control what traffic is allowed to leave a resource. They define the destination, protocol, and port number that outbound traffic can use. By default, my security group's outbound rule allows all traffic (0.0.0.0/0) to leave the resource, meaning it can send traffic to any destination unless I modify the rule.


Security group (sg-07006ae0e465d415d | NextWork Security Group) was created successfully
Details
sg-07006ae0e465d415d - NextWork Security Group
Actions
Details
Security group name
NextWork Security Group
Security group ID
sg-07006ae0e465d415d
Description
A Security Group for the NextWork VPC.
VPC ID
vpc-0ce35c6f6cb85a3cc
Owner
379607485890
Inbound rules count
1 Permission entry
Outbound rules count
1 Permission entry

Network ACLs

Network ACLs are optional, stateless security layers that control inbound and outbound traffic at the subnet level. They use numbered rules to explicitly allow or deny traffic based on IP address, protocol, and port number, providing an additional layer of security beyond security groups.

Security groups vs. network ACLs

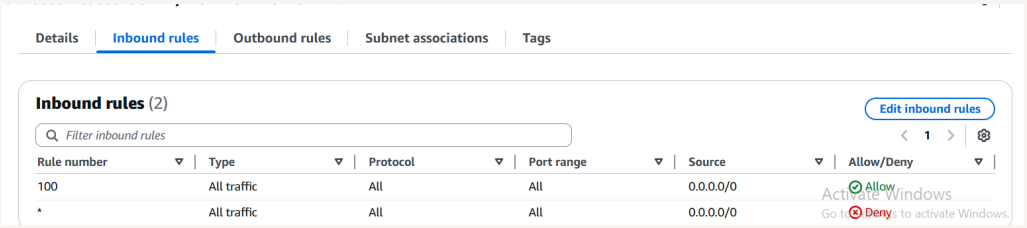
The difference between a security group and a network ACL is that ACLs are used to set broad traffic rules that apply to an entire subnet. For example, blocking incoming traffic from a particular range of IP addresses or denying all outbound traffic to certain ports. Whereas, Security groups allow for more granular control, managing access to individual resource. You can specify which ports and protocols are allowed for each connected resource.

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. The default network ACL permits all inbound and outbound traffic until you modify the rules to explicitly allow or deny specific traffic.

In contrast, a custom ACL’s inbound and outbound rules are automatically set to deny all traffic until you add rules to explicitly allow specific inbound or outbound traffic.

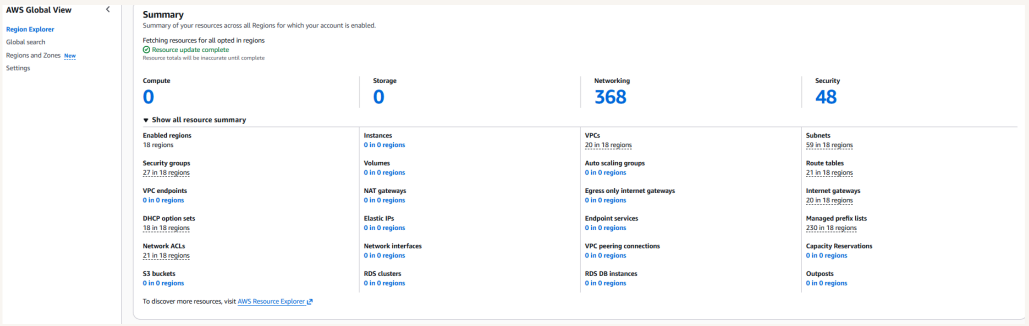


Tracking VPC Resources

I created additional a VPC, an Internet Gateway, and a Security Group. Instead of my usual region, I used a different AWS Region (for example, us-east-1 or eu-central-1). Teams would use multiple regions to improve latency for users, increase fault tolerance in case of outages or disasters, and gain global deployment experience.

EC2 Global View is a tool where you can find all your EC2 resources across multiple AWS Regions in one centralized dashboard. I could even narrow down my search by Region, instance type, or resource ID. Without EC2 Global View, you'd have to log in to each region separately and manually check each resource, which can be time-consuming and error-prone.

Now that I've learnt about EC2 Global View, I'd use it again to quickly see all my EC2 resources across multiple regions, monitor usage and statuses in one place, and troubleshoot issues without switching between regions.


AWS Global View
Region Explorer
Global search
Regions and Zones New
Settings
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
368
Security
48
Show all resource summary
Enabled regions
18 regions
Security groups
27 in 18 regions
VPC endpoints
0 in 0 regions
DHCP option sets
18 in 18 regions
Network ACLs
21 in 18 regions
S3 buckets
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
VPCs
20 in 18 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
59 in 18 regions
Route tables
21 in 18 regions
Internet gateways
20 in 18 regions
Managed prefix lists
230 in 18 regions
Capacity Reservations
0 in 0 regions
Outposts
0 in 0 regions
To discover more resources, visit AWS Resource Explorer

The place to learn & showcase your skills

Check out nextwork.org for more projects