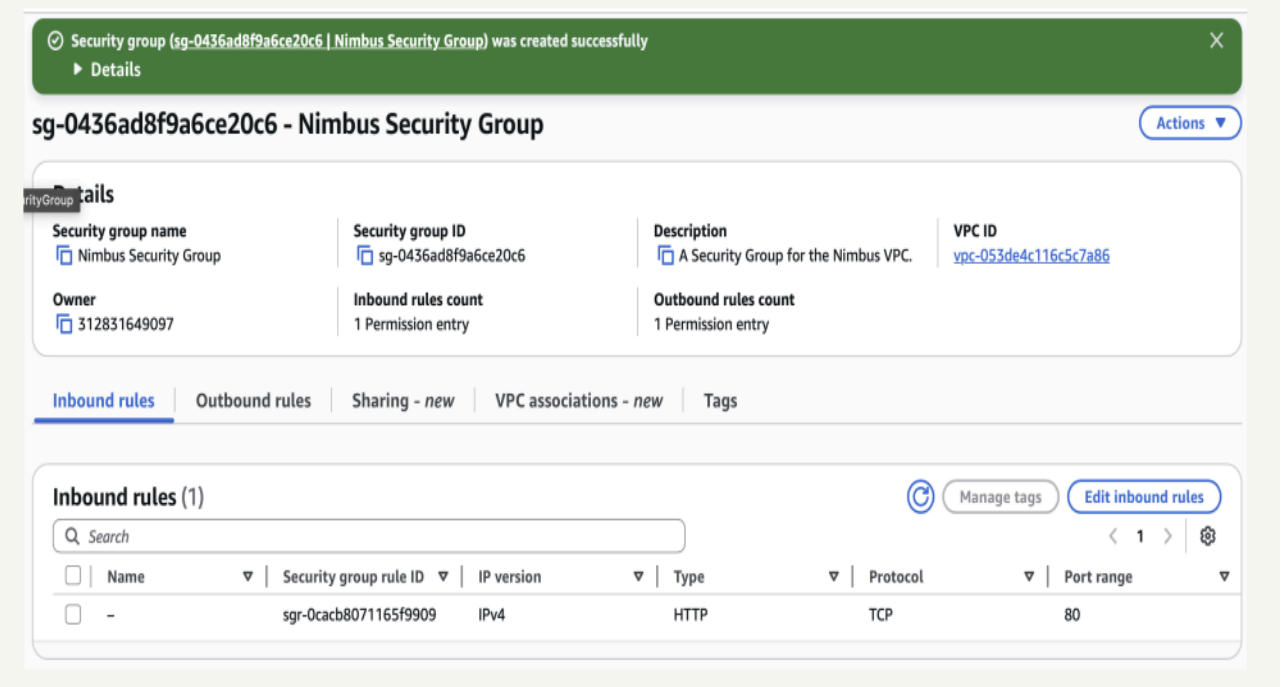
VPC Traffic Flow and Security



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is Amazon VPC is your own private network in AWS where you can place and control your cloud resources (like EC2 instances, databases, and load balancers). It is very useful if a user wants total agency over their resources.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create subnets, create a route table, and create a network.

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

One thing I didn't expect in this project was that by default, inbound and outbound rules have contrasting results whether it is custom-built or not. Custom builds deny all traffic for example.

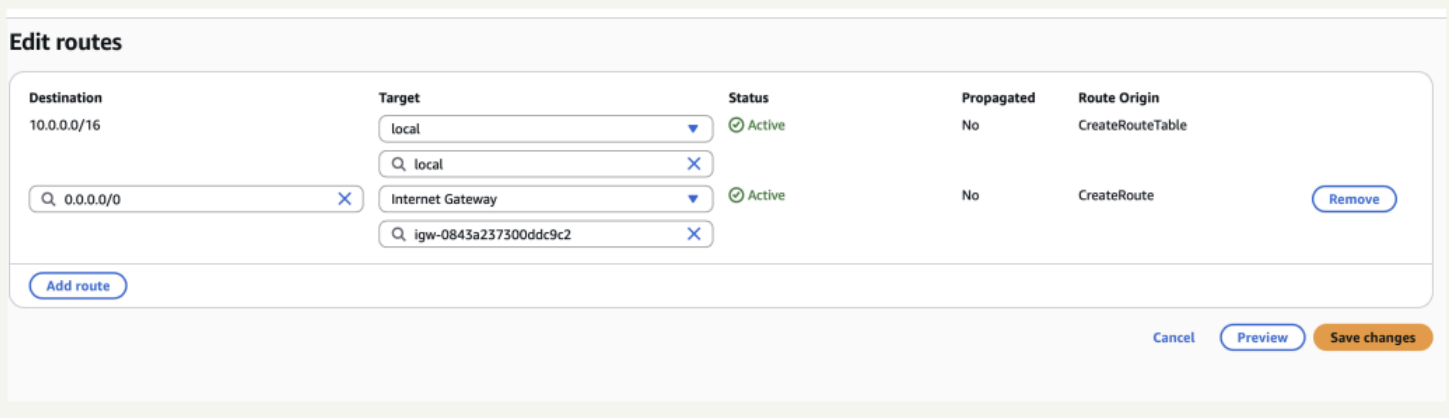
This project took me...

This project took me about an hour to complete.

Route tables

Think of a route table as a GPS for the resources in your subnet. Just like a GPS helps people get to their destination in a city, a route table is a table of rules, called routes, that decide where the data in your network should go.

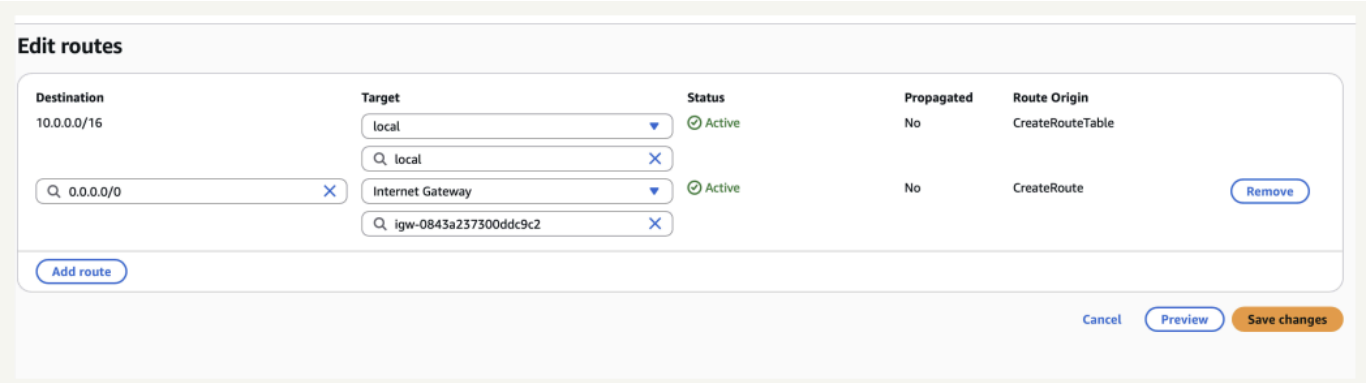
When a subnet's route table has a route that directs internet-bound traffic to the internet gateway, the subnet becomes a public subnet. This means your subnet can communicate with the internet.



Route Destination and Target

Routes are defined by their destination and target, which means the range of IP addresses that traffic in the VPC is trying to reach, and the road/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 Nimbus IG (gateway).



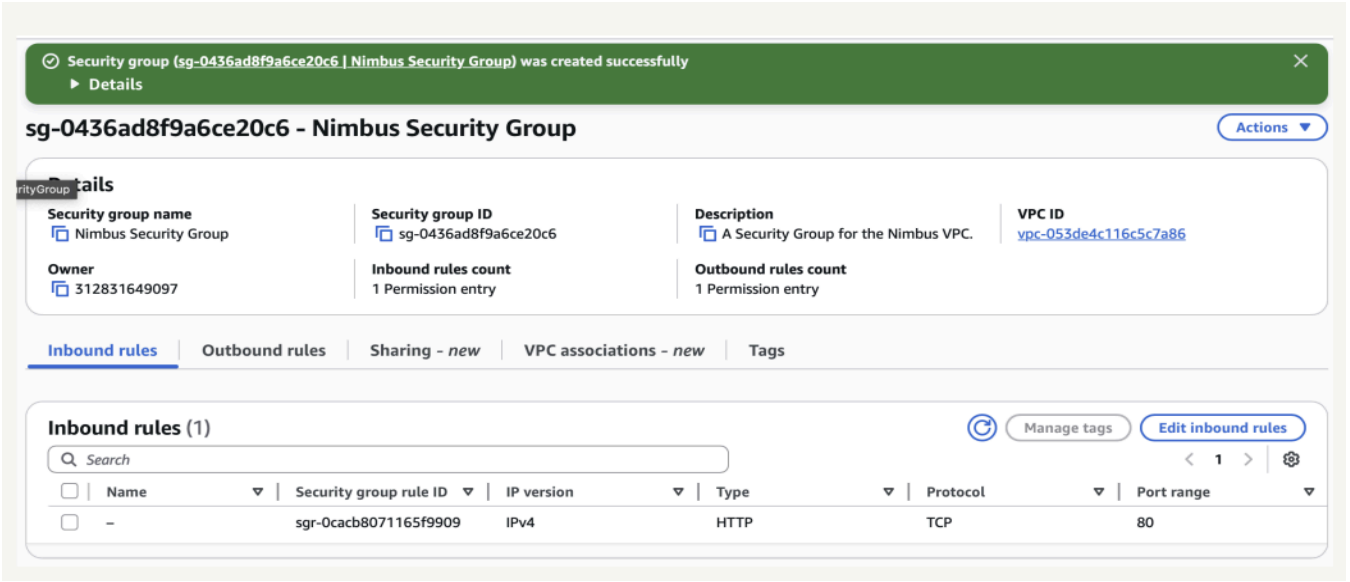
Security Groups

Security groups are responsible for checking who comes in and who comes out. They have strict rules about what kind of traffic can enter or leave the resource based on its IP address, protocols and port numbers.

Inbound vs Outbound rules

Inbound rules control the data that can enter the resources in your security group. I configured an inbound rule that allows all HTTP traffic.

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


Security group (sg-0436ad8f9a6ce20c6 | Nimbus Security Group) was created successfully
Details
sg-0436ad8f9a6ce20c6 - Nimbus Security Group
Actions
Details
Security group name
Nimbus Security Group
Security group ID
sg-0436ad8f9a6ce20c6
Description
A Security Group for the Nimbus VPC.
VPC ID
vpc-053de4c116c5c7a86
Owner
312831649097
Inbound rules count
1 Permission entry
Outbound rules count
1 Permission entry
Inbound rules
Outbound rules
Sharing - new
VPC associations - new
Tags
Inbound rules (1)
Manage tags
Edit inbound rules
Search
1
Name
Security group rule ID
IP version
Type
Protocol
Port range
–
sgr-0cacb8071165f9909
IPv4
HTTP
TCP
80

Network ACLs

Network ACLs are a list of rules that controls traffic flow by permitting or denying data based on criteria like IP addresses, protocols, and port numbers.

Security groups vs. network ACLs

The difference between a security group and a network ACL is their scope. A security group secures my network at the resource level (so every single resource in my VPC is associated with a security group), while network ACLs secure my network at the subnet level (every single subnet in my VPC is associated with a network ACL).

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 incoming and outgoing traffic, respectively.

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