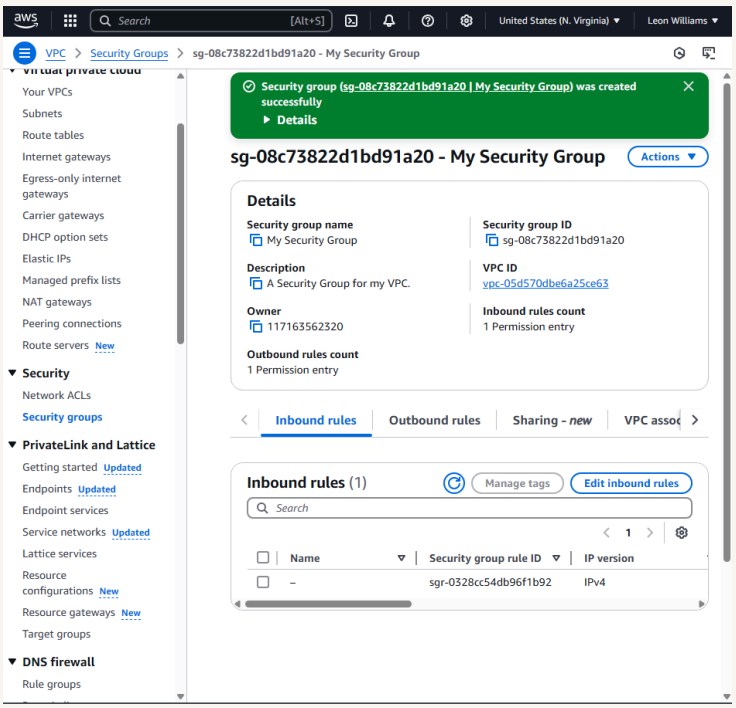
nextwork.org

VPC Traffic Flow and Security

Leon Williams



Leon Williams
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a private, isolated virtual network in AWS where you launch resources like servers and databases. It lets you control network settings, improving security and customizing your cloud environment to fit your needs.

How I used Amazon VPC in this project

I used Amazon VPC to create a secure virtual network for my resources. I set up subnets, route tables, security groups, and network ACLs to control traffic flow and protect my cloud environment.

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

One thing I didn’t expect in this project was how hands-on and detailed configuring inbound and outbound rules would be to control network traffic precisely. It gave me a deeper understanding of cloud security.

Leon Williams
NextWork Student

This project took me...

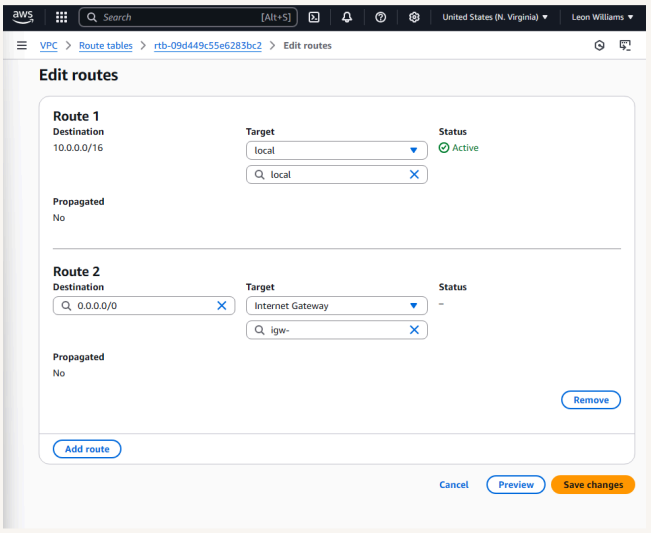
This project took me about 40 minutes in total. I stayed focused throughout and gained a better understanding of how networking works in the cloud.

Leon Williams
NextWork Student

Route tables

Route tables are like a GPS for your VPC, guiding traffic within the network and to the internet. I used one to create a public subnet by adding a route to the internet gateway, allowing external access while keeping internal traffic secure.

Route tables are needed to make a subnet public because they guide traffic flow. Adding a route to the internet gateway lets traffic reach external networks, allowing the subnet to send and receive data from the internet.

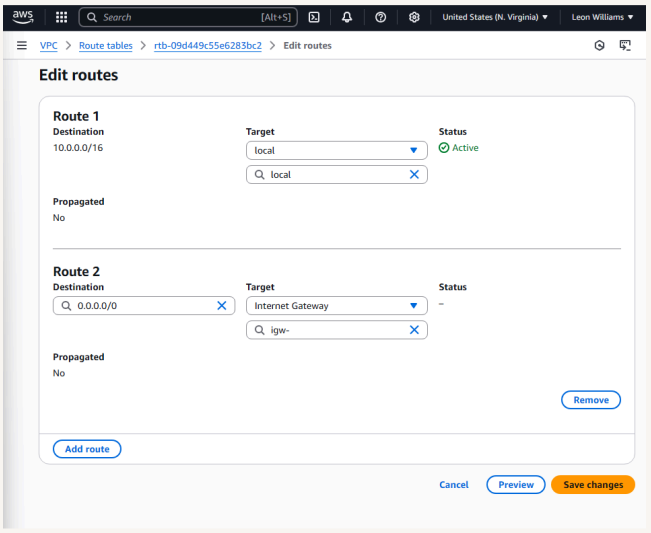


Leon Williams
NextWork Student

Route destination and target

Routes are defined by destination and target, which mean where traffic goes and how. Destination is the IP range to reach, and target is the path or device like an internet gateway or local network that directs the traffic.

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 the internet gateway ID, allowing all traffic not meant for the VPC to flow to the internet.



Leon Williams
NextWork Student

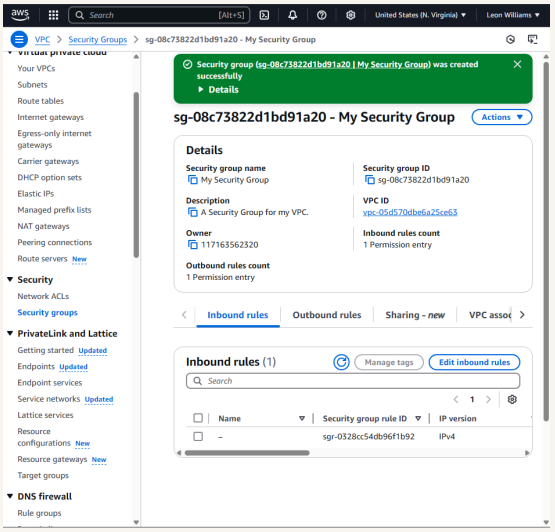
Security groups

Security groups are like guards for each resource in your VPC. They control traffic in and out using rules based on IP addresses, protocols, and ports to keep resources secure while allowing necessary communication inside and outside the network.

Inbound vs Outbound rules

Inbound rules control what incoming traffic is allowed to reach your resources. I configured an inbound rule that permits HTTP traffic from any IP address so users can securely access my web server from anywhere on the internet.

Outbound rules are settings that control what traffic your resources can send out. By default, my security group's outbound rule allows all outbound traffic, enabling resources to communicate freely with other networks and services outside the VPC.


Search
[Alt+S]
United States (N. Virginia)
Leon Williams
VPC
Security Groups
sg-08c73822d1bd91a20 - My Security Group
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
Route servers
Security
Network ACLs
Security groups
PrivateLink and Lattice
Getting started
Endpoints
Endpoint services
Service networks
Lattice services
Resource configurations
Resource gateways
Target groups
DNS firewall
Rule groups
Security group (sg-08c73822d1bd91a20 | My Security Group) was created successfully
Details
sg-08c73822d1bd91a20 - My Security Group
Actions
Details
Security group name
My Security Group
Security group ID
sg-08c73822d1bd91a20
Description
A Security Group for my VPC.
VPC ID
vpc-05d570dbe6a25ce63
Owner
117163562320
Inbound rules count
1 Permission entry
Outbound rules count
1 Permission entry
Inbound rules
Outbound rules
Sharing - new
VPC assoc
Inbound rules (1)
Manage tags
Edit inbound rules
Search
Name
Security group rule ID
IP version
sgr-0328cc54db96f1b92
IPv4

Leon Williams
NextWork Student

Network ACLs

Network ACLs are virtual firewalls for your subnet that control inbound and outbound traffic. They check data packets against rules to allow or deny access, adding a strong security layer alongside security groups.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that security groups control traffic at the resource level with stateful rules, while network ACLs control traffic at the subnet level with stateless rules, offering subnet protection.

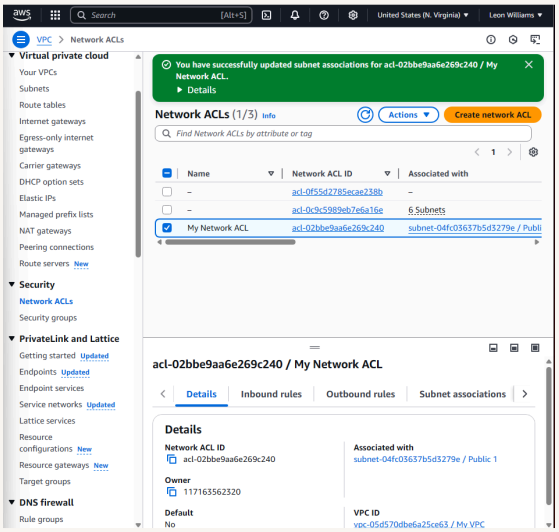
Leon Williams
NextWork Student

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 freely in and out of the associated subnet until you customize the rules to restrict specific traffic.

In contrast, a custom ACL's inbound and outbound rules are automatically set to deny all traffic until you add specific rules that allow certain types of traffic in or out of the subnet.



The place to learn & showcase your skills

Check out nextwork.org for more projects