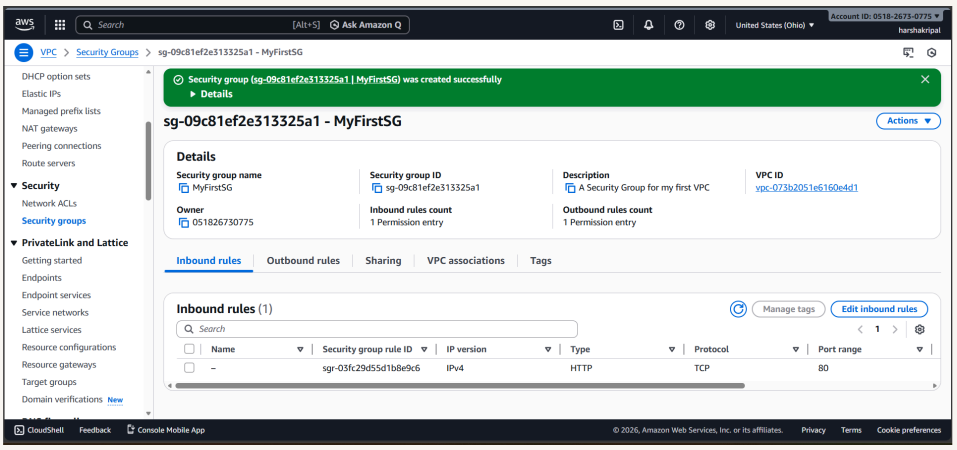
nextwork.org

VPC Traffic Flow and Security

H Harshada Kripal



Harshada Kripal
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a Virtual Private Cloud that allows you to create and customize isolated network environments and provision resources according to your requirements. It is useful because it provides full control over networking, security, and traffic flow, ensuring that resources are secure, organized, and able to communicate efficiently.

How I used Amazon VPC in this project

In today’s project, I used Amazon VPC to create a route table that directs internet-bound traffic to my Internet Gateway. I also created security groups to provide a layer of protection for individual resources within the VPC. Additionally, I configured Network ACLs to provide an extra layer of security at the subnet level, controlling traffic entering and leaving the subnets in my VPC.

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

One thing I didn’t expect in this project was how much control and flexibility AWS VPC provides in managing network traffic and security, even for a relatively simple setup.

Harshada Kripal
NextWork Student

This project took me...

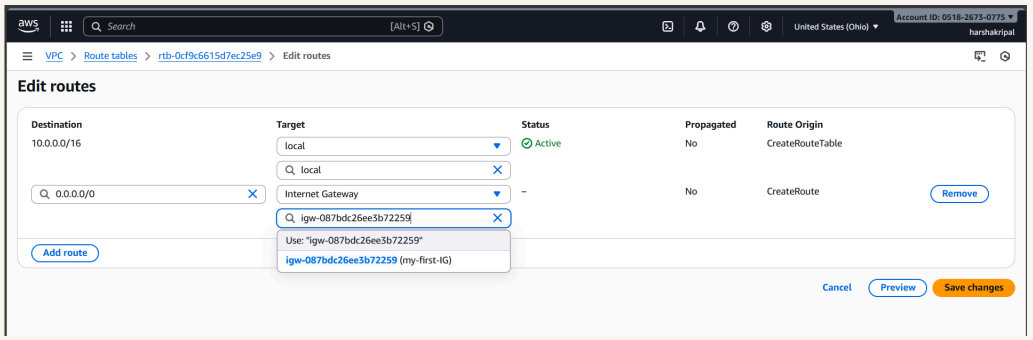
This project took me 30 minutes to complete and provided a valuable learning experience. I gained hands-on knowledge about VPCs, subnets, route tables, security groups, and Network ACLs, enhancing my understanding of AWS networking and security concepts.

Harshada Kripal
NextWork Student

Route tables

Route tables are a set of rules that determine where network traffic is directed within a VPC. They control how data moves between subnets, gateways, and other network resources.

Routes tables are needed to make a subnet public because they provide a route to directs internet-bound traffic to an Internet Gateway. Without this route, resources in the subnet cannot reach or be reached from the public internet.

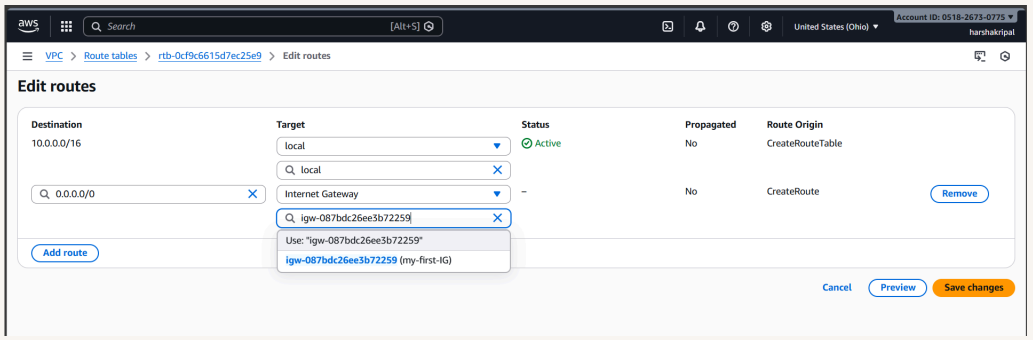


Harshada Kripal
NextWork Student

Route destination and target

Routes are defined by their destination and target, which means the destination specifies where the traffic is going such as an IP range, and the target specifies where that traffic should be sent such as an Internet Gateway, NAT Gateway, or another network resource.

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 internet gateway igw.



Harshada Kripal
NextWork Student

Security groups

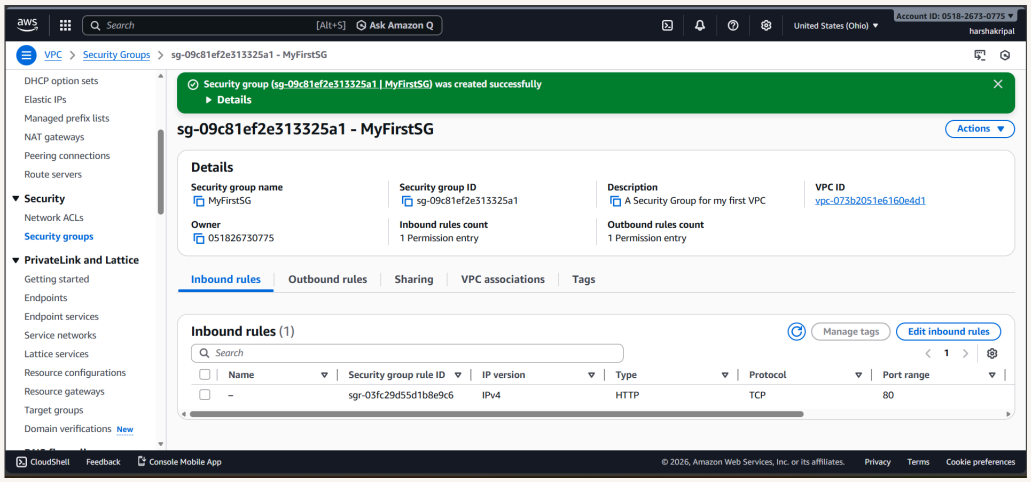
Security groups are virtual firewalls in our VPC which allows inbound and outbound traffic for resources in the VPC. They defone which type of traffic is allowed to reach or leave the resources such as EC2 Instances.

Inbound vs Outbound rules

Inbound rules are the rules which allows traffic to reach the resources within VPC. I configured an inbound rule that is 0.0.0.0/0 which means it will allows all kind of traffic to my resources within my VPC.

Outbound rules decides what data send by the resource within our VPC By default, my security group's outbound rule is 0.0.0.0/0 which means resource is allowed to send traffic to any destination on the internet, enabling it to communicate externally when required.

Harshada Kripal
NextWork Student



Harshada Kripal
NextWork Student

Network ACLs

Network ACLs sets broad traffic rule on an entire subnet. For example, blocking incoming traffic from a particular range of IP addresses or denying all outbound traffic to certain ports.

Security groups vs. network ACLs

Security groups are attached to individual resources (like EC2 instances) and act as stateful firewalls that control which inbound and outbound traffic is allowed. Network ACLs (NACLs) are attached to subnets and act as stateless firewalls that control traffic entering and leaving the subnet as a whole. i.e., Security Groups protect resources, while Network ACLs protect subnets.

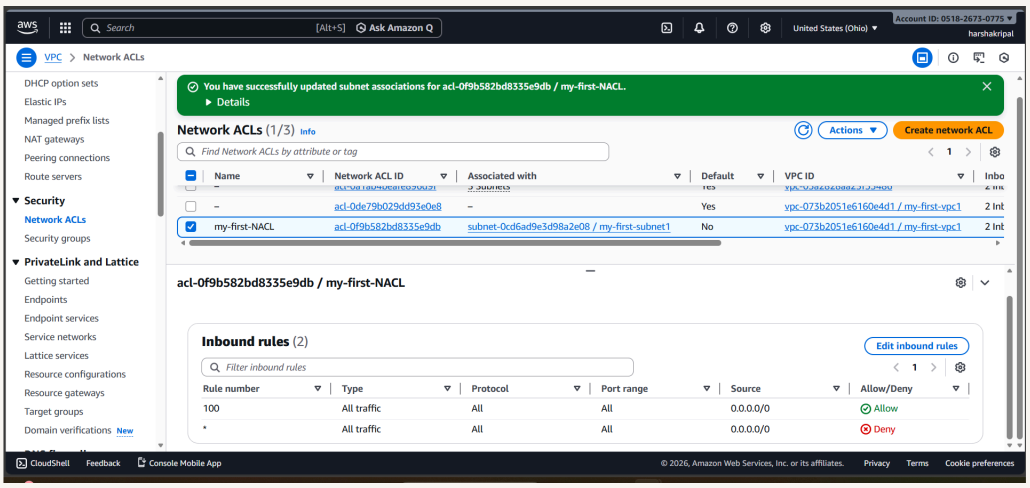
Harshada Kripal
NextWork Student

Default vs Custom Network ACLs

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

By default, a Network ACL allows all inbound and outbound traffic, meaning it does not block any communication unless we explicitly add rules to restrict it.

Inbound and outbound rules allow all traffic (0.0.0.0/0), just like the default ACL. However, we can modify these rules to allow or deny specific traffic.



The place to learn & showcase your skills

Check out nextwork.org for more projects