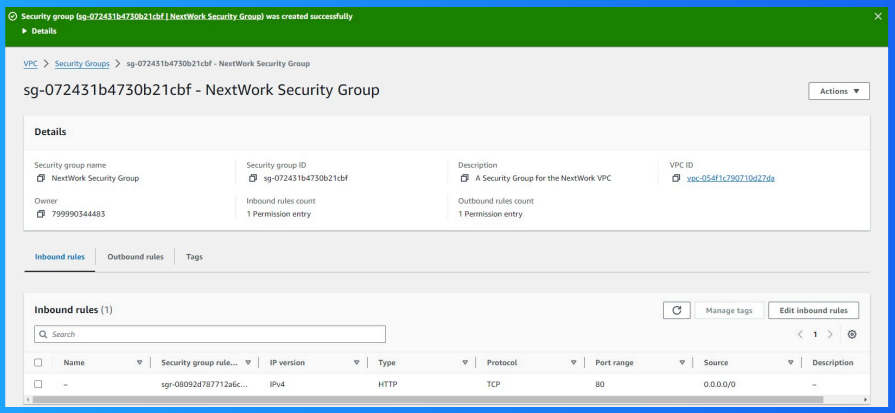
NextWork.org

VPC Traffic Flow and Security

Nikhil Bhan



N

Nikhil Bhan
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) allows users to create a private and isolated network in their AWS account. They can manage and organize resources as well as configure permissions and access to those resources.

How I used Amazon VPC in this project

In this project I created a route table, added a route to it and associated it with my subnet. I also created a Security Group that accepts incoming HTTP traffic from any IP address as well as a Network ACL that accepts all traffic to the subnet.

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

I wasn't expecting how important it is to attach a Route Table and Network ACL to my subnet; I can see what issues can happen if these steps are overlooked.

This project took me...

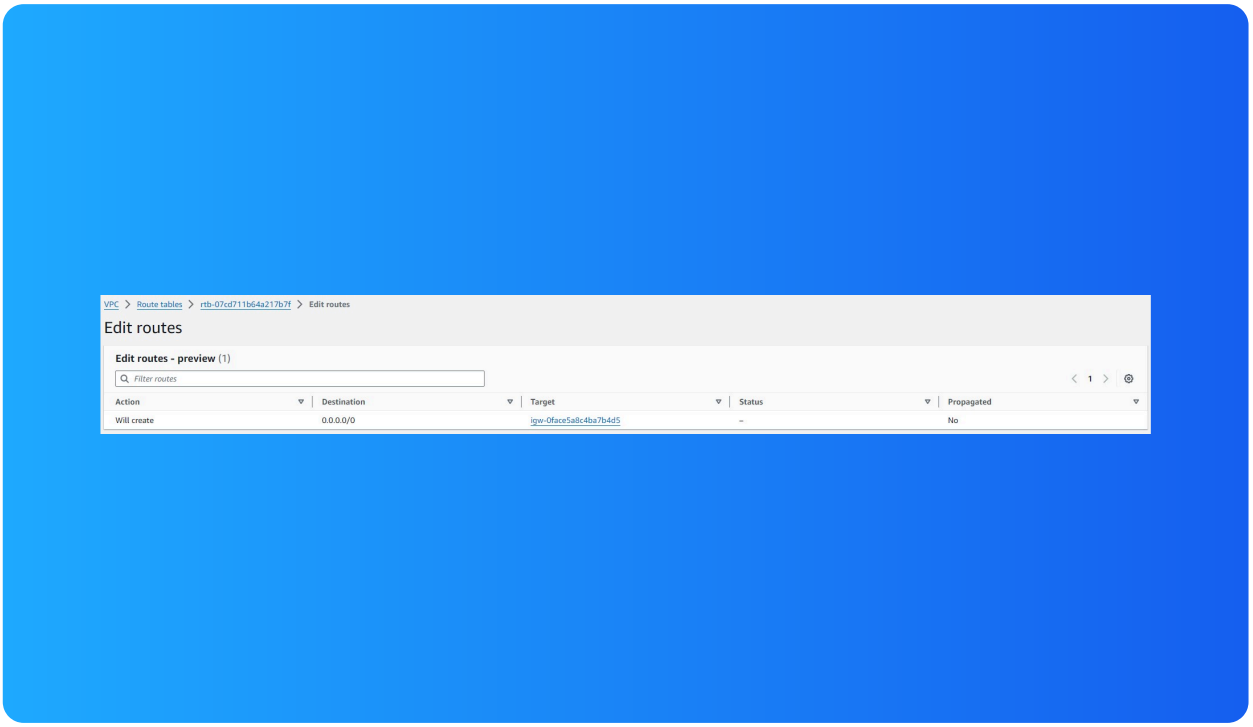
This project took me almost an hour to complete. I took an additional 15 minutes to write my documentation.

Nikhil Bhan
NextWork Student

Route tables

Route tables are a list of rules that provide the directions on where to send data in your network.

Route tables are needed to make a subnet public because the resources in that subnet need the directions to the Internet Gateway to send Internet-bound traffic. From the gateway, that traffic would get sent out to the Internet.

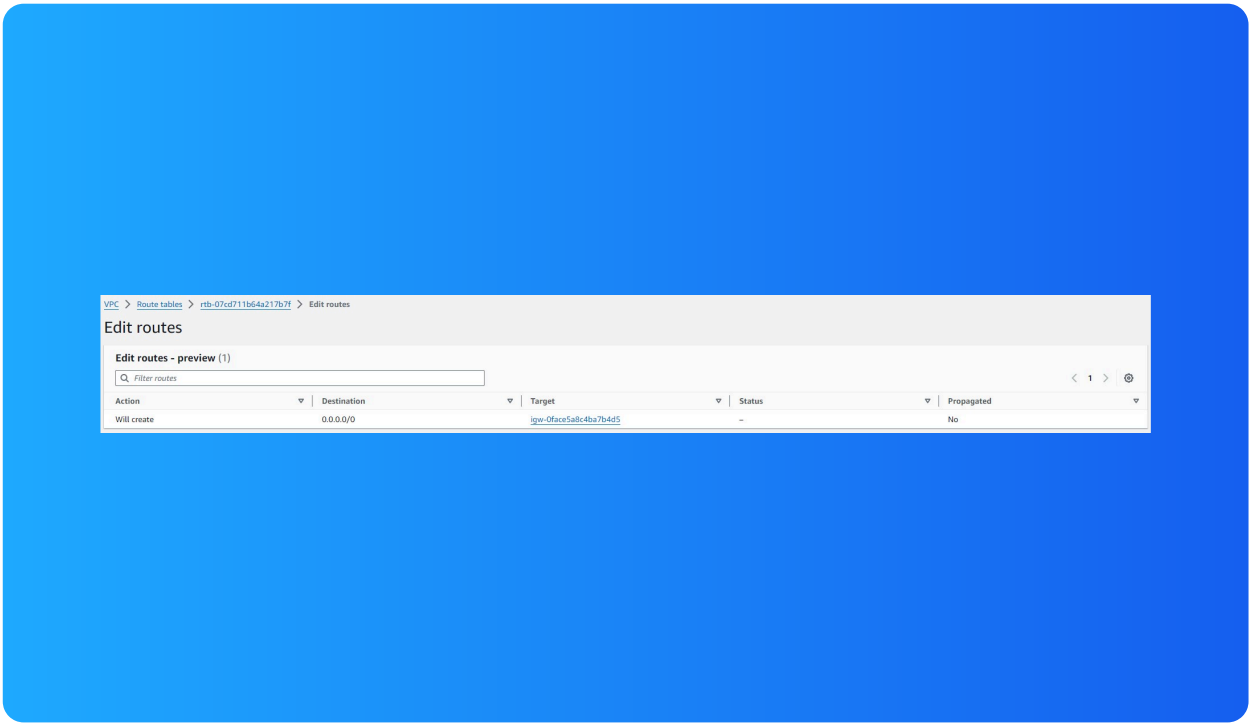


Nikhil Bhan
NextWork Student

Route destination and target

Routes are defined by their destination and target, which mean that the traffic will use the target as a pathway to reach its destination. The destination in this case would a range of IP addresses, like a highway connecting to a street of houses.

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 "igw-0face5a8c4ba7b4d5", which is the Internet Gateway I created and attached to my VPC.



Nikhil Bhan
NextWork Student

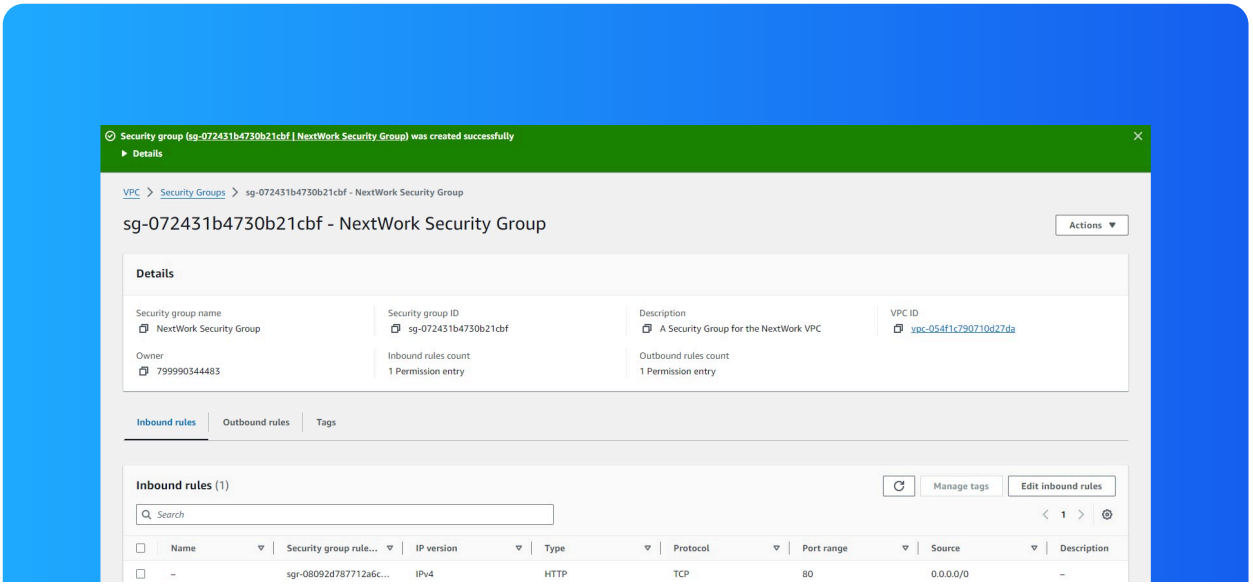
Security groups

Security groups are like security guards; they protect resources in your AWS account by checking the traffic that comes in and out. These traffic rules can restrict traffic based on their IP addresses, protocols and port numbers used.

Inbound vs Outbound rules

Inbound rules are rules that determine what incoming traffic can access the resources in the security group. I configured an inbound rule that allows any external IPv4 address to access the resources in the security group by using the HTTP protocol.

Outbound rules are rules that determine what data traffic the resources in the security group can send out. By default, my security group's outbound rule allows any traffic to be sent out to any external IP address on the Internet.



N
Nikhil Bhan
NextWork Student

Network ACLs

Network ACLs are like traffic security; they are placed at the entrance and exiting points of the subnet. They check every data packet in the traffic against a list of access control rules before allowing that packet through.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that the security group manages access to individual resources in the subnet. The network ACL uses rules that applies to the whole subnet, which consists of all the resources.

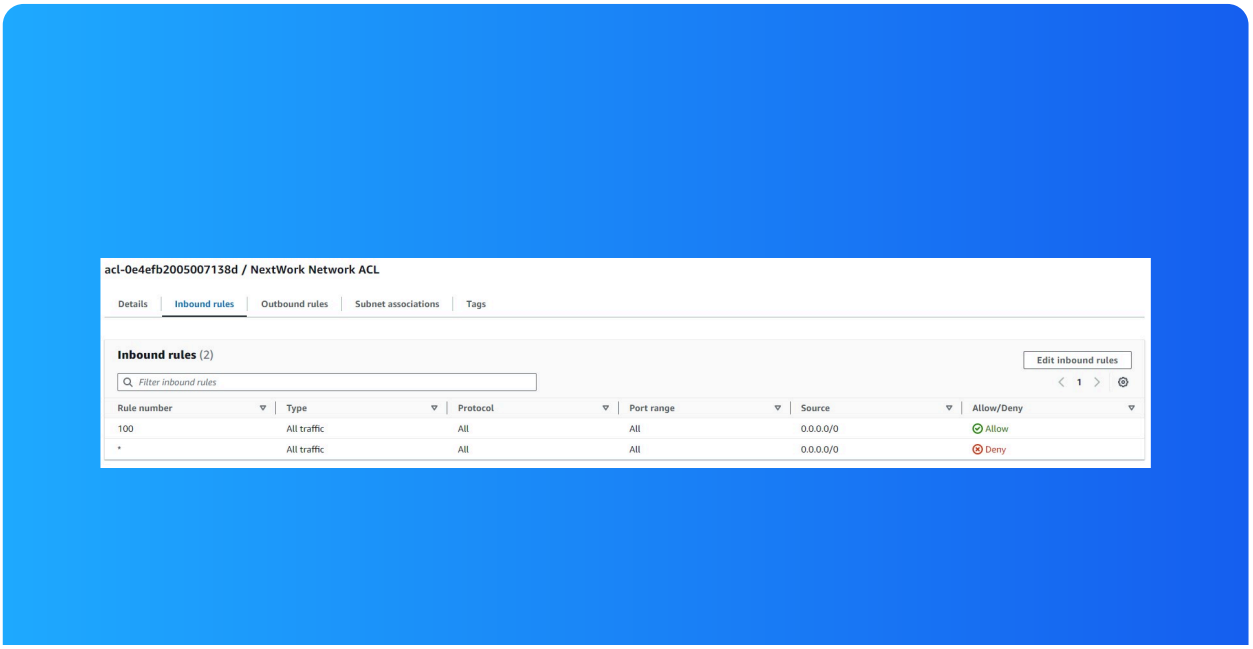
N
Nikhil Bhan
NextWork Student

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 coming into the network, as well as going out to the Internet. This works well for a public subnet with a website hosted on an EC2 instance, but not for private data!

In contrast, a custom ACL's inbound and outbound rules are automatically set to deny any traffic coming from the Internet and it also restricts any traffic from exiting the subnet. This is a perfect way to secure private resources like databases.



Everyone should be in a job they love.

Check out nextwork.org for more projects