



VPC Traffic Flow and Security



vishnu vardhan gurram

The screenshot shows the AWS VPC Security Groups console. A success message at the top states: "Security group (sg-01bad8016e9f1d339 | NextWork Security Group) was created successfully". The main card displays the details of the new security group:

Security group name	NextWork Security Group	Security group ID	sg-01bad8016e9f1d339	Description	A Security Group for the NextWork VPC.
Owner	557690612623	Inbound rules count	1 Permission entry	Outbound rules count	1 Permission entry
Actions					

The "Inbound rules" tab is selected, showing one rule:

Name	Security group rule ID	IP version	Type	Protocol	Port range
-	sgr-09daf2e126fedfa5	IPv4	HTTP	TCP	80

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a private virtual network in AWS that lets you securely run and control your resources. It's useful for managing network settings and protecting your data.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create a secure network with subnets, route tables, and an internet gateway. I also set up security groups to control instance traffic and network ACLs to protect the subnets.

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

One thing I didn't expect was how much impact proper network and security settings have on making sure everything works smoothly and stays protected.

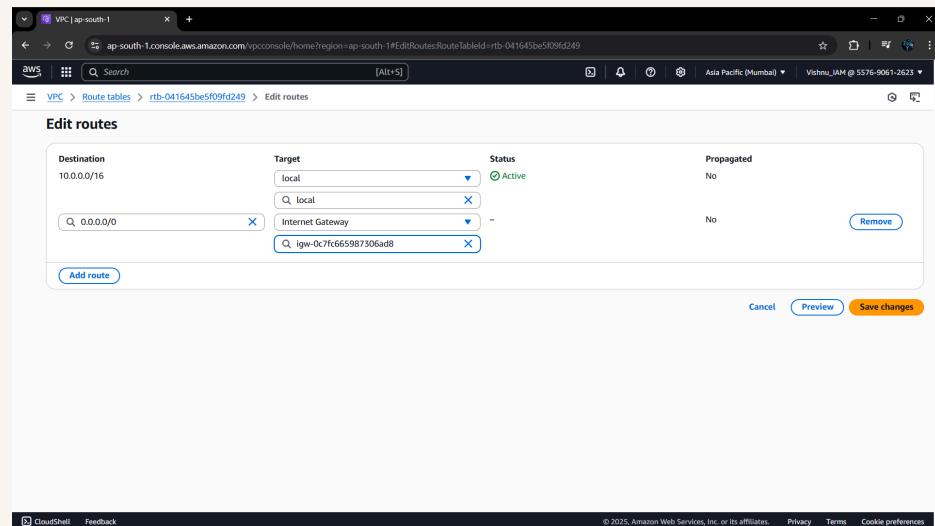
This project took me...

This project took me around 45 minutes to set up the VPC, subnets, route tables, internet gateway, and configure basic security groups and network ACLs.

Route tables

Route tables are a set of rules in a VPC that determine how network traffic is directed. They control the flow of traffic within the VPC and between the VPC and external networks like the internet.

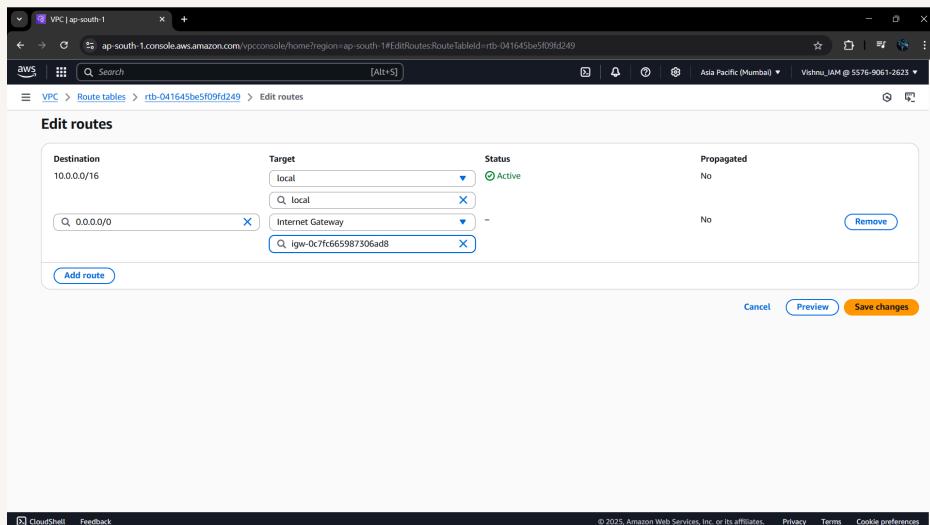
Route tables are needed to make a subnet public because they define how traffic is routed. To make a subnet public, the route table must have a route that directs internet-bound traffic (0.0.0.0/0) to the internet gateway.



Route destination and target

Routes are defined by their destination and target, which mean the destination is the IP range the traffic is going to, and the target is where that traffic should be sent, such as an internet gateway, NAT gateway, or another subnet.

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 (igw-xxxxxxxx).



Security groups

Security groups are virtual firewalls in AWS that control inbound and outbound traffic for resources like EC2 instances. They work at the instance level and allow you to define rules based on IP addresses, protocols, and ports.

Inbound vs Outbound rules

Inbound rules are settings in a security group that control the traffic allowed to enter your resource. I configured an inbound rule that allowed HTTP traffic (port 80) from anywhere so that my web server could be accessed publicly.

Outbound rules are settings in a security group that control the traffic allowed to leave your resource. By default, my security group's outbound rule allowed all traffic to any destination

The screenshot shows the AWS VPC console with the URL <https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup;groupId=sg-01bad8016e9f1d339>. A green success message at the top states: "Security group (sg-01bad8016e9f1d339 | NextWork Security Group) was created successfully". The main page displays the details of the newly created security group "sg-01bad8016e9f1d339 - NextWork Security Group". The "Details" section includes:

- Security group name:** NextWork Security Group
- Security group ID:** sg-01bad8016e9f1d339
- Description:** A Security Group for the NextWork VPC.
- VPC ID:** vpc-00fc4205e3b82af1d
- Owner:** 557690612623
- Inbound rules count:** 1 Permission entry
- Outbound rules count:** 1 Permission entry

The "Inbound rules" tab is selected, showing one rule:

Name	Security group rule ID	IP version	Type	Protocol	Port range
-	sgr-09daf2e126fedfd5	IPv4	HTTP	TCP	80

Network ACLs

Network ACLs are stateless firewalls at the subnet level in a VPC that control inbound and outbound traffic. They allow or deny traffic based on rules and apply to all resources within the associated subnet.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that security groups are stateful and apply to instances, while network ACLs are stateless and apply to subnets.

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 pass through. This means no restrictions are applied unless you create specific rules to block or limit traffic for added security.

In contrast, a custom ACL's inbound and outbound rules are automatically set to deny all traffic by default, so you must create specific rules to allow or deny traffic based on IP addresses, protocols, and ports.

The screenshot shows the AWS VPC Network ACLs console. On the left, there is a navigation sidebar with sections for VPC dashboard, Virtual private cloud, Security (Network ACLs selected), and PrivateLink and Lattice. The main area displays a table of Network ACLs:

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound Rules
acl-08eecc09b072c473d9	acl-08eecc09b072c473d9	3 Subnets	Yes	vpc-04c27eea08c079335	2 Int
NextWork Network A...	acl-0dc1771bf434ff1ff	subnet-0beab943cc440698f / Public_1	No	vpc-04c27eea08c079335	2 Int

Below the table, there are tabs for Details, Inbound rules (selected), Outbound rules, Subnet associations, and Tags. Under the Inbound rules tab, there is another table:

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

