



VPC Traffic Flow and Security

SH

shilpa_i_kale@yahoo.com

The screenshot shows the AWS CloudFormation console with a success message: "Security group (sg-07eadf483f88a95a2 | NextWork Security Group) was created successfully". Below the message, the security group details are listed:

Security group name	sg-07eadf483f88a95a2	Security group ID	sg-07eadf483f88a95a2	Description	VPC ID
Owner	619071342657	Inbound rules count	1 Permission entry	A Security Group for the NextWork VPC.	vpc-0cbd831029ee63277

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

Name	Security group rule ID	IP version	Type	Protocol	Port range
-	sgr-0fa9661efe83cc110	IPv4	HTTP	TCP	80

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is an isolated section of AWS and it is useful because it is private i.e. resources deployed in a VPC are not public and private.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create a public subnet, internet gateway, route tables, security group, network ACL.

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

One thing I didn't expect in this project was there was default of everything like the default VPC, default subnet, default internet gateway, network ACL.

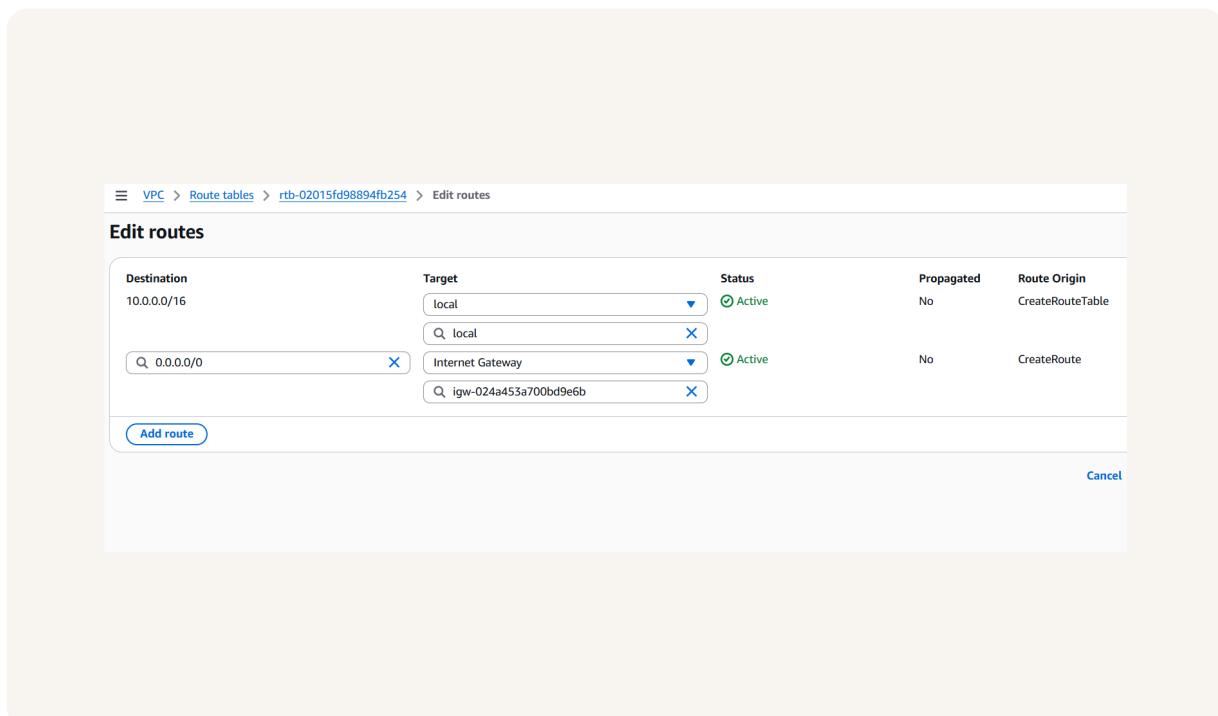
This project took me...

This project took me 2 and half hours including demo and understanding the concept.

Route tables

Route tables are like the GPS that directs traffic within my VPC to the correct destination.

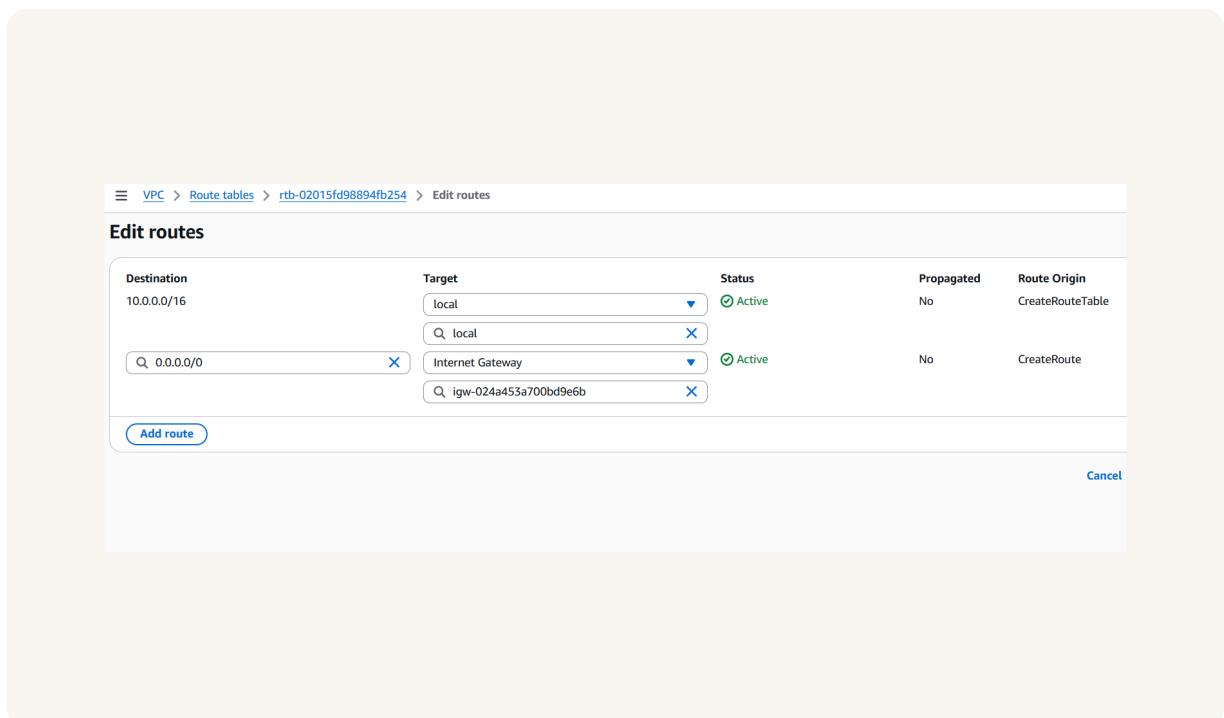
Routes tables are needed to make a subnet public because subnet needs to have route to an internet gateway in order to be considered public. A route table is the only way to establish this connection.



Route destination and target

Routes are defined by their destination and target, which mean the 'destination' is the range of IP addresses that traffic in my VPC is trying to reach. The 'target' is the road or the 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-NextWork IG.



Security groups

Security groups are like the security guards that monitor both inbound and outbound traffic at the resource level i.e every single resource in a subnet in a VPC has a security group.

Inbound vs Outbound rules

Inbound rules are the rules that monitor/restrict inbound traffic like what is coming inside the resource e.g. users visiting a web app I am hosting. I configured an inbound rule that allows all HTTP request.

Outbound rules are the rules that monitor/restrict outbound traffic like what is going outside e.g. my webapp requesting data from a public source. By default, my security group's outbound rule allows all type of traffic.

SH

shilpa_i_kale@yahoo.c...

NextWork Student

nextwork.org

sg-07eadf483f88a95a2 - NextWork Security Group

Security group (sg-07eadf483f88a95a2 | NextWork Security Group) was created successfully

Details

Security group name NextWork Security Group	Security group ID sg-07eadf483f88a95a2	Description A Security Group for the NextWork VPC. vpc-0cbd831029ee63277
Owner 619071342657	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)

Name	Security group rule ID	IP version	Type	Protocol	Port range
-	sgr-0fa9661efe85cc110	IPv4	HTTP	TCP	80

Network ACLs

Network ACLs are like cops that secure my network at subnet level.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that security group secures network at resource level(every single resource in my VPC is associated with a security group) and network ACL secures network at subnet level.

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.

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

The screenshot shows the AWS Network ACLs management interface. At the top, there is a search bar labeled "Find Network ACLs by attribute or tag". Below it is a table with two rows:

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound
-	acl-09ffbed0226302a5a	3 Subnets	Yes	vpc-09afe716642db711e	2 Inbound
<input checked="" type="checkbox"/> NextWork Network A...	acl-09fdc30d92c1dce4a	subnet-00fc3ed804da5e79b / Public 1	Yes	vpc-0cbd831029ee65277 / NextWork V...	2 Inbound

Below this, a modal window is open for the custom ACL "acl-09fdc30d92c1dce4a / NextWork Network ACL". The modal has tabs for "Details", "Inbound rules" (which is selected), "Outbound rules", "Subnet associations", and "Tags".

The "Inbound rules" section shows two rules:

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

At the bottom of the modal, there are links for "Mobile App", "© 2025, Amazon Web Services, Inc. or its affiliates.", "Privacy", "Terms", and "Cookie preferences".



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

