



nextwork.org

VPC Traffic Flow and Security

K

Katleo Rantle

The screenshot shows the AWS CloudFormation console with a success message: "Security group (sg-0079f7cf4050917cb | NextWork Security Group) was created successfully". Below the message is a table with details about the security group:

Details		Description		VPC ID
Security group name	NextWork Security Group	Security group ID	sg-0079f7cf4050917cb	vpc-0215ba78fb15cfd4
Owner	039612844657	Inbound rules count	1 Permission entry	
		Outbound rules count	1 Permission entry	

Below the table, there are tabs for "Inbound rules", "Outbound rules", "Sharing", "VPC associations", "Related resources - new", and "Tags". The "Inbound rules" tab is selected, showing a table with one rule:

Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
-	sgr-007bf35f71e48bc37	IPv4	HTTP	TCP	80	0.0.0.0/0	-



Katleo Rantle

NextWork Student

nextwork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is logical network boundary in the cloud and it is useful because it provides security and privacy to our resources on the cloud

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to setup multiple layers of security NACL at subnet level and security groups at resource level.

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

One thing I didn't expect in this project was being able to view all my VPC resources across multiple regions from a single screen

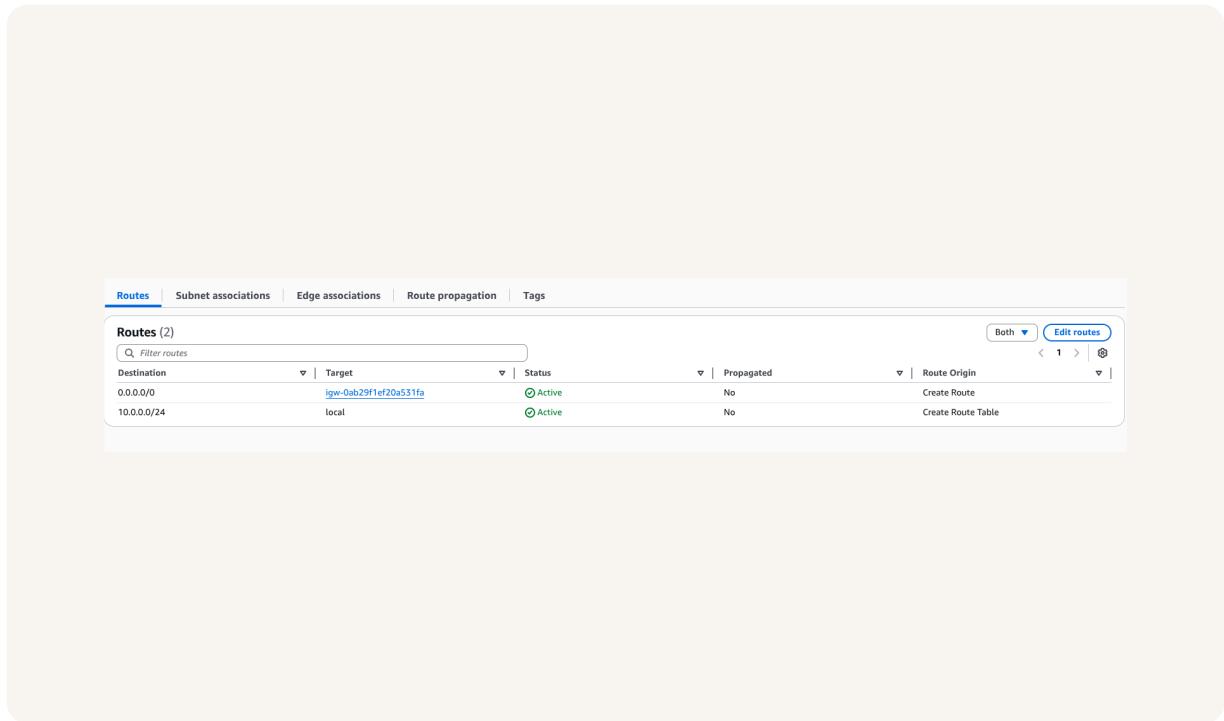
This project took me...

This project took me 2.5hrs

Route tables

Route tables are rules that determine where data in our network should go

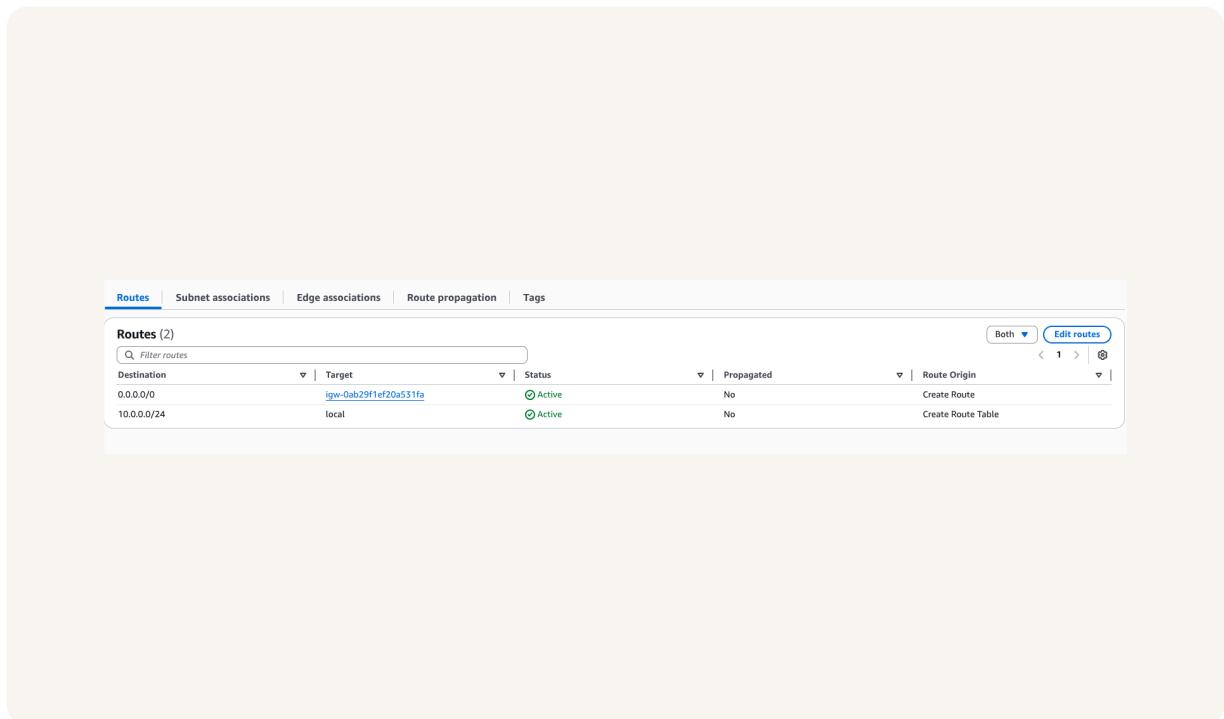
Routes tables are needed to make a subnet public because internet bound traffic needs a route that directs that traffic to the IGW without it that traffic will not be allowed to leave the VPC thus it cannot be public



Route destination and target

Routes are defined by their destination and target, which mean where the traffic wants to go, ip address range (destination) and how the traffic will get there, the path (target)

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-0ab29f1ef20a531fa



A screenshot of a network configuration interface, likely a web-based management tool. The top navigation bar includes tabs for 'Routes' (which is selected), 'Subnet associations', 'Edge associations', 'Route propagation', and 'Tags'. Below the navigation is a search bar labeled 'Filter routes'. A table displays two routes:

Routes (2)					
Destination	Target	Status	Propagated	Route Origin	
0.0.0.0/0	igw-0ab29f1ef20a531fa	Active	No	Create Route	
10.0.0.0/24	local	Active	No	Create Route Table	

Buttons for 'Edit routes' and a page number '1' are visible at the top right of the table area.

Security groups

Security groups are rules that can control what kind of data or traffic is allowed to enter or leave a resource

Inbound vs Outbound rules

Inbound rules are rules that control what kind of traffic can enter the resource in the security group I configured an inbound rule that allows any external device to communicate with our resource

Outbound rules are rules that define or control data that our resource can send By default, my security group's outbound rule allow any resource within our security group to send data to any ip address



Security group (sg-0079f7cf4050917cb | NextWork Security Group) was created successfully

Details

sg-0079f7cf4050917cb - NextWork Security Group

Actions ▾

Details		Description	VPC ID
Security group name <input checked="" type="checkbox"/> NextWork Security Group	Security group ID <input checked="" type="checkbox"/> sg-0079f7cf4050917cb	Description <input checked="" type="checkbox"/> A Security Group for NextWork VPC	VPC ID <input checked="" type="checkbox"/> vpc-0f2156af76f615cf4
Owner <input checked="" type="checkbox"/> 039612844657	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Inbound rules | Outbound rules | Sharing | VPC associations | Related resources - new | Tags

Inbound rules (1)

Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
-	sgr-007bf35f71e48bc37	IPv4	HTTP	TCP	80	0.0.0.0/0	-

Manage tags | Edit inbound rules | < | 1 | > | ⌂ | ⌂



Katleo Rantle

NextWork Student

nextwork.org

Network ACLs

Network ACLs are rules that control traffic or check data packets at subnet level to see what may or may not enter

Security groups vs. network ACLs

The difference between a security group and a network ACL is that NACLs work at a subnet level and can block entire classes of ip addresses and security groups work at resource 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 inbound and out bound traffic

In contrast, a custom ACL's inbound and outbound rules are automatically set to deny all traffic until we add the rules for what kind of traffic we allow

acl-043f168b697393844 / NextWork NACL

Details [Info](#)

Network ACL ID acl-043f168b697393844	Associated with -	Default No	VPC ID vpc-0f2156af76f615cf4 / NextWork VPC
---	----------------------	---------------	--

[Actions ▾](#)

[Inbound rules](#) [Outbound rules](#) [Subnet associations](#) [Tags](#)

Inbound rules (2)

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

[Edit inbound rules](#)



Katleo Rantle

NextWork Student

nextwork.org

Tracking VPC Resources

I created additional VPC, internet gateway and security group Instead of my usual region, I used eu-west-2, london Teams would use multiple regions to improve latency and make apps more highly available ie protect from natural diasters and other things that can go wrong from working only in one geographical location

EC2 Global View is a tool where you can find and manage all ec2 and VPC resources accross all regions I could even narrow down my search by specific region Without EC2 Global View, you'd have to go into the specific region to be able to see resources in that region

Now that I've learnt about EC2 Global View, I'd use it again in cases where Ec2 and VPC resources have been delpoyed accross multiple regions



Katleo Rantle

NextWork Student

nextwork.org

AWS Global View <

Region Explorer

Global search

Regions and Zones [New](#)

Settings

Resource update complete

Resource totals will be inaccurate until complete

Compute	Storage	Networking	Security
0	1	368	55

Show all resource summary

Region explorer (34)

The region explorer lists your resources across all Regions for which your account is enabled.

Updated 8 minutes ago

Open selected Region

View Region details

View Region resources

Region	Instances	VPCs	Subnets	Security Groups	Volumes	Auto Scaling Gr...	Route Tables	VPC Endpoints
Africa (Cape Town) af-south-1	2	3	6	-	-	2	-	-
Asia Pacific (Mumbai) ap-south-1	1	3	4	-	-	1	-	-
Asia Pacific (Osaka) ap-northeast-3	1	3	1	-	-	1	-	-
Asia Pacific (Seoul) ap-northeast-2	1	4	1	-	-	1	-	-
Asia Pacific (Singapore) ap-southeast-1	1	3	1	-	-	1	-	-
Asia Pacific (Sydney) ap-southeast-2	1	3	1	-	-	1	-	-
Asia Pacific (Tokyo) ap-northeast-1	1	3	1	-	-	1	-	-
Canada (Central) ca-central-1	1	3	1	-	-	1	-	-
Europe (Frankfurt) eu-central-1	1	3	1	-	-	1	-	-
Europe (Ireland) eu-west-1	1	3	1	-	-	1	-	-
Europe (London) eu-west-2	2	3	3	-	-	2	-	-



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

