



VPC Traffic Flow and Security

K

Kehinde Abiuwa

The screenshot shows the AWS VPC Security Groups console. A success message at the top right states: "Security group (sg-0aca2a369602a66e1 | NextWork Security Group) was created successfully". The main view displays the details of the "sg-0aca2a369602a66e1 - NextWork Security Group". The security group has the following details:

Security group name	Security group ID	Description	VPC ID
NextWork Security Group	sg-0aca2a369602a66e1	A Security Group for the Next Work VPC.	vpc-046f2acbf8531dc17
Owner	Inbound rules count	Outbound rules count	
511239431868	1 Permission entry	1 Permission entry	

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

Name	Security group rule ID	IP version	Type	Protocol
-	sgr-00d3922ab2107f616	IPv4	HTTP	TCP

The left sidebar includes navigation links for Virtual private cloud, Security, and PrivateLink and Lattice.

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a customizable virtual network in the AWS cloud that is useful because it gives you full control over networking, security, and connectivity for your cloud resources

How I used Amazon VPC in this project

I created an Amazon VPC and created subnets, route tables and internet gateway, i linked all of them together in the vpc and then created security groups for my resources and network acls for my subnets to control the inbound and outbound traffic flowing in my VPC

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

Nothing really

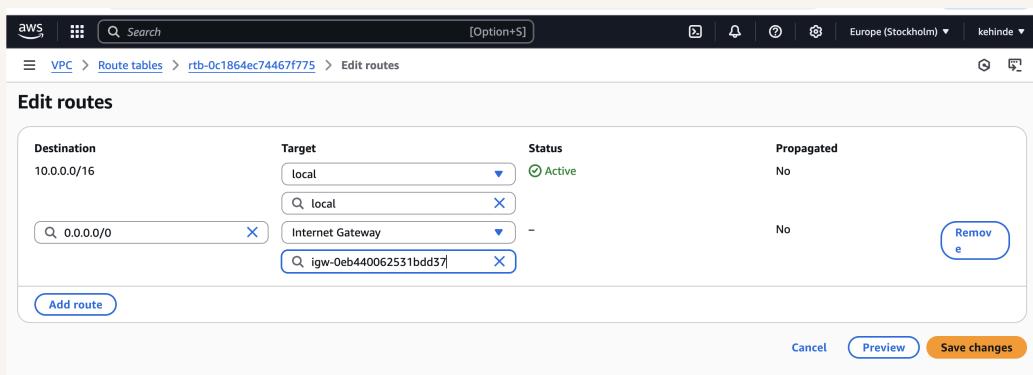
This project took me...

25 mins

Route tables

Route tables are a set of rules that determines how network traffic is directed within your VPC

Routes tables are needed to make a subnet public because they define how traffic from that subnet can reach the internet



Route destination and target

Routes are defined by their destination and target, which mean the destination specifies the IP address range of the traffic, and the target specifies where that traffic should be sent, such as an internet gateway

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-0eb440062531bdd37

The screenshot shows the AWS VPC Route Tables interface. The URL in the browser is `VPC > Route tables > rtb-0c1864ec74467f775 > Edit routes`. The page title is "Edit routes". There is a table with columns: Destination, Target, Status, and Propagated. One row is visible:

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	Internet Gateway	-	No

Below the table are "Add route" and "Remove" buttons. At the bottom are "Cancel", "Preview", and "Save changes" buttons.

Security groups

Security groups are virtual firewalls that control inbound and outbound traffic for your resources in a VPC (e.g ec2 instances)

Inbound vs Outbound rules

Inbound rules are rules that control the data that can enter the resources in your security group. I configured an inbound rule that allows any IP address to access your resource

Outbound rules are rules that control that data that your resources can send out. By default, my security group's outbound rule allows all outbound traffic



The screenshot shows the AWS VPC Security Groups console. A success message at the top right states: "Security group (sg-0aca2a369602a66e1 | 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-0aca2a369602a66e1	Description A Security Group for the Next Work VPC.	VPC ID vpc-046f2acbf8531dc17
Owner 511239431868	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Below the details, there are tabs for Inbound rules, Outbound rules, Sharing - new, VPC associations - new, and Tags. The Inbound rules section shows one rule:

Name	Security group rule ID	IP version	Type	Protocol
-	sgr-00d3922ab2107f616	IPv4	HTTP	TCP

Network ACLs

Network ACLs are used to set broad traffic rules that apply to 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

The difference between a security group and a network ACL is that security groups operate at the instance level and allow only specified traffic, while network ACLs operate at the subnet level and allow or deny traffic using stateless rules

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 if it's the default ACL, or deny all traffic if it's a custom ACL with no rules defined

In contrast, a custom ACL's inbound and outbound rules are automatically set to deny all traffic until you explicitly add allow or deny rules

The screenshot shows the AWS VPC Network ACLs page. A green success message box at the top right says: "You have successfully updated subnet associations for acl-0c12be776059a1b15 / NextWork Network ACL." Below this, the "Network ACLs (1/3) Info" table lists three entries:

Name	Network ACL ID	Associated with	Default	VPC ID
acl-0f175496a7de7b716	-	-	Yes	vpc-046f2acb
acl-01190da0eb15960e8	-	3 Subnets	Yes	vpc-042a1f6d
NextWork Network A...	acl-0c12be776059a1b15	subnet-040a1e1cb0bb74f13 / Public_1	No	vpc-046f2acb

Below the table, the "Inbound rules (2)" 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



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

