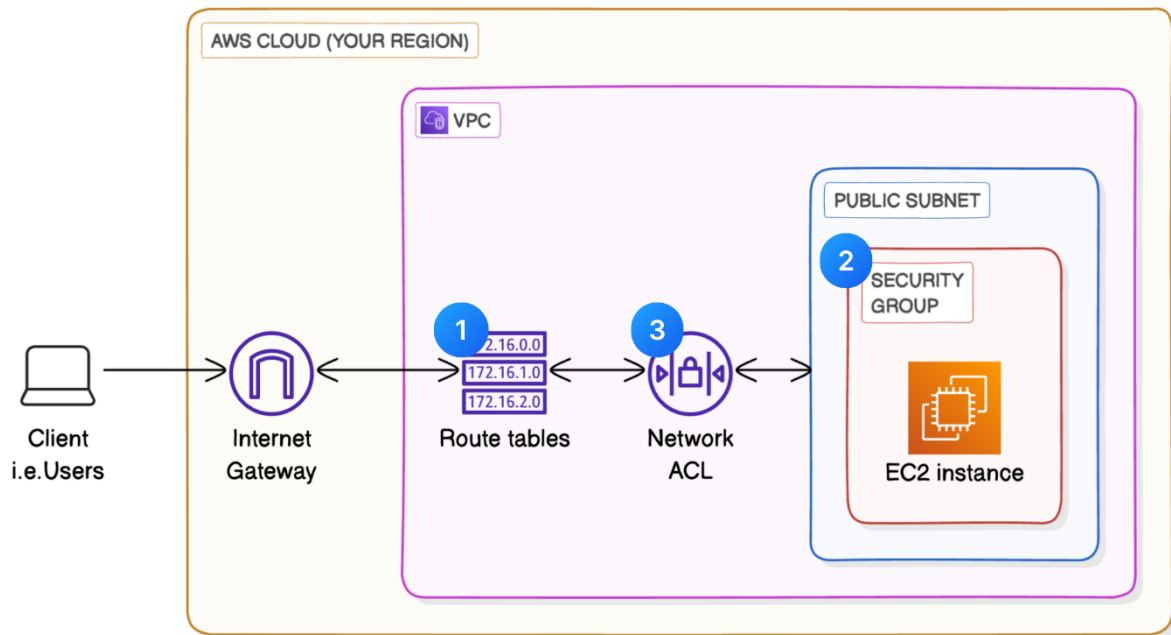


VPC Traffic Flow and Security

Get ready to:

1. Create a route table.
2. Create a security group.
3. Create a Network ACL (Network Access Control List).



Create a route table

In the left navigation pane, choose **Route tables**.

- Refresh your page.
- Two route tables! Why are there two?
 - Note: If you see more than two route tables, those route tables would've been set up in other projects that you've completed. Check the **VPC** column in the far-right side of the table to see where each route table belongs. Focus on the default route table and your VPC's route table.
- Let's investigate. Select one of the two route tables and select the **Routes** tab.
- Uncheck that route table, and switch to the other route table.
- Select the **Routes** tab again.
- Aha, the two tables have different routes!
- Let's rename your NextWork VPC route table so it's easier to recognise.
- Make sure you have your NextWork VPC route table selected - this is the route table with a single route to 10.0.0.0/16.
- Select the pencil icon in the **Name** column of your route table.
- Enter the name NextWork route table.
- Select **Save**.

- Select the **Routes** tab.
- Choose **Edit routes**.
- Choose **Add route** near the bottom of the page.
- Destination: 0.0.0.0/0
- Target: **Internet Gateway**.
- Select **NextWork IG**.
- Choose **Save changes**.
- Choose the **Subnet associations** tab.
- Under the **Explicit subnet associations** tab, choose **Edit subnet associations**
- Select **Public 1**.
- Choose **Save associations**.

VPCL > Route tables > rtb-0f9e7b436d4abfcd4 > Edit routes

Edit routes

Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
0.0.0.0/0	Internet Gateway	Active	No
0.0.0.0/0	Internet Gateway	-	No

Buttons: Add route, Cancel, Preview, Save changes

Create a security group

In this task, let's add a security group so that users can access resources in your VPC.

In the left navigation pane, choose **Security groups**.

Choose **Create security group**.

- Security group name: NextWork Security Group
- Description: A Security Group for the NextWork VPC.
- VPC: **NextWork VPC**
- Under the **Inbound rules** panel, choose **Add rule**.

VPCL > Security Groups > Create security group

VPC info

vpc-038bbbaa68b4dbf4d (NextWork VPC)

Inbound rules

Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	Anywhere...	

Buttons: Add rule, Delete

- Type: HTTP
- Source: Anywhere-IPv4
- At the bottom of the screen, choose **Create security group**.

sg-06e886aa6631ccfee - NextWork Security Group Actions ▾

Details

Security group name
 NextWork Security Group

Security group ID
 sg-06e886aa6631ccfee

Description
 A Security Group for the NextWork VPC.

VPC ID
 vpc-038bbbaa68b4dbf4d

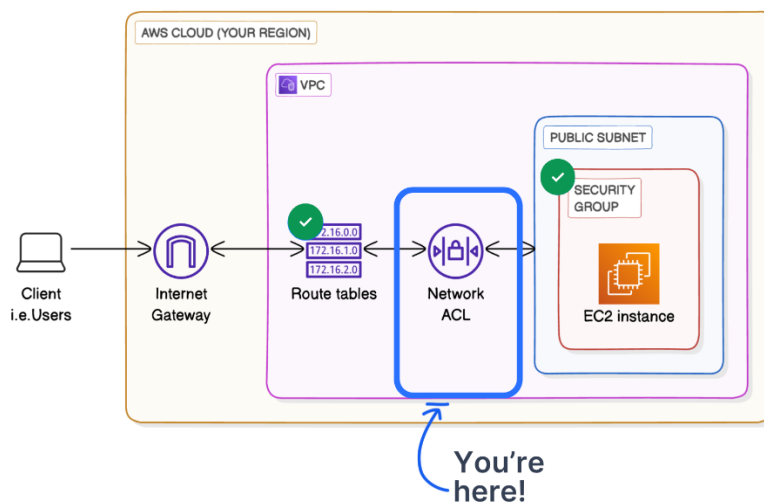
Owner
 329599662468

Inbound rules count
 1 Permission entry

Outbound rules count
 1 Permission entry

[Inbound rules](#)
[Outbound rules](#)
[Sharing - new](#)
[VPC associations - new](#)
[Tags](#)

Create a Network ACL



In the left navigation pane, choose **Network ACLs**.

Choose the network ACL that's associated with your **Public 1** subnet, and check out the tabs for **Inbound rules** and **Outbound rules**.

NextWork VPC [acl-0ef9f322640394c58](#) - No [vpc-038bbbaa68b4dbf4d / NextWork V...](#) 1 Inbound rule

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

Inbound rules (1) Edit inbound rules



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

Your default ACL has everything we need, but it's great practice to set up everything from scratch.

- Select **Create new network ACL**.
- Name: NextWork Network ACL

- VPC: **NextWork VPC**
- Select **Create network ACL**.
- Uncheck the default network ACL you've selected.
- Select the checkbox next to **NextWork Network ACL**
- Select the **Inbound rules** tab.
- Select **Edit inbound rules**.
- Select **Add new rule**.
- Rule number: 100
- Type: **All traffic**.
- Source: 0.0.0.0/0
- Click **Save changes**.

acl-0ef9f322640394c58 / NextWork VPC Actions ▾

Details info
Network ACL ID
 acl-0ef9f322640394c58
Owner
 329599662468

Associated with
-



Default
No

VPC ID
[vpc-038bbbaa68b4dbf4d / NextWork VPC](#)

Inbound rules | Outbound rules | Subnet associations | Tags

Inbound rules (2) Edit inbound rules

< 1 > ⚙

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

- Select the **Outbound rules** tab.
- Select **Edit outbound rules**.
- Select **Add new rule**.
- Rule number: 100
- Type: **All traffic**.
- Destination: 0.0.0.0/0
- Select the **Subnet associations** tab, which should be right next to the Outbound rules tab.
- The subnet associations tab is empty
- Under the **Subnet associations** tab, select **Edit subnet associations**.
- Select your **Public 1** subnet.
- Select **Save changes**.

Details

Info

Network ACL ID

acl-0ef9f322640394c58

Associated with

-

Default

No

VPC ID

[vpc-038bbbaa68b4dbf4d / NextWork VPC](#)

Owner

329599662468

Outbound rules (2)

Edit outbound rules

Filter outbound rules

< 1 >

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

Details

Info

Network ACL ID

acl-0ef9f322640394c58

Associated with

[subnet-08cf7637b8146a1a7 / Public 1](#)

Default

No

VPC ID

[vpc-038bbbaa68b4dbf4d / NextWork VPC](#)

Owner

329599662468

Subnet associations (1)

Edit subnet associations

Filter subnet associations

< 1 >

Name	Subnet ID	Associated with	Availability Zone	IPv4 CIDR	IPv6 CIDR
Public 1	subnet-08cf7637b8146a1...	acl-0ef9f322640394c58 / NextWork VPC	us-east-1a	10.0.0.0/24	-