

# Private S3 Access via Gateway VPC Endpoint (No NAT Gateway)

**Created by:** *Manilka Shalinda*

**Purpose:** Access S3 from a private subnet without using NAT Gateway or Internet Gateway

## Overview

This setup demonstrates how to enable secure, private access to an **Amazon S3 bucket** from an **EC2 instance located in a private subnet**, without using a **NAT Gateway** or **Internet Gateway**. Instead, a **Gateway VPC Endpoint** is used to route S3 traffic privately within the AWS network.

## Goals

To securely access an Amazon S3 bucket from an EC2 instance located in a private subnet **without using a NAT Gateway or Internet Gateway**, by configuring a **Gateway VPC Endpoint**.

This setup ensures that all S3 traffic remains within the AWS network, improving **security** and **cost-efficiency**.

### 1. VPC Configuration

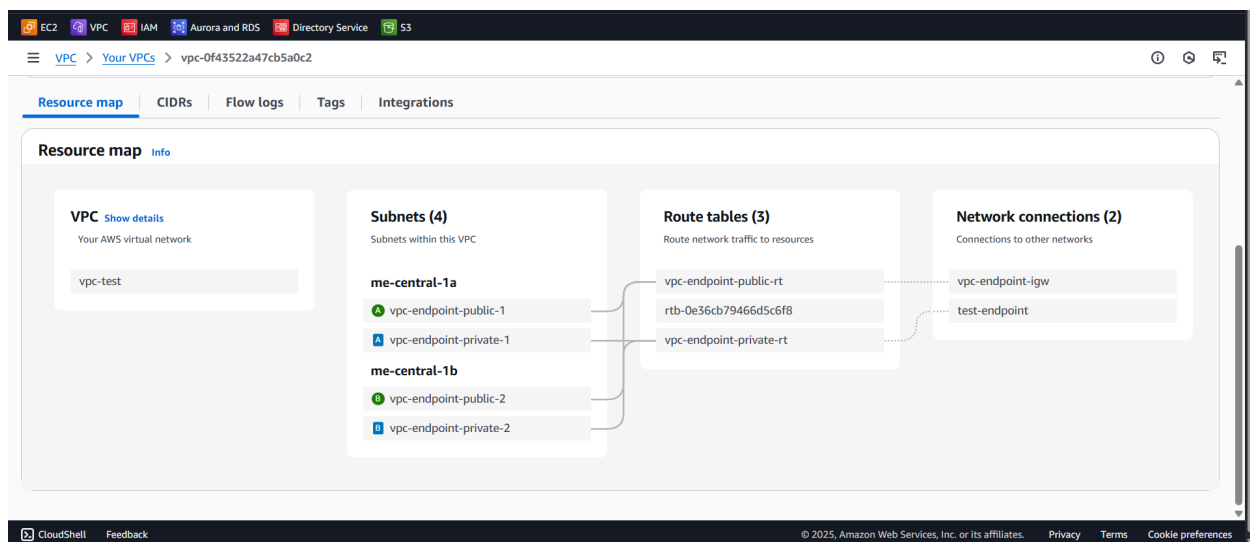
- **VPC CIDR:** 10.0.0.0/16
- **Subnets:**

Subnet Name	Type	CIDR
vpc-endpoint-public-1	Public	10.0.1.0/24
vpc-endpoint-public-2	Public	10.0.2.0/24
vpc-endpoint-private-1	Private	10.0.3.0/24
vpc-endpoint-private-2	Private	10.0.4.0/24

The screenshot shows the AWS Management Console interface for a VPC. The top navigation bar includes links for EC2, VPC, IAM, Aurora and RDS, Directory Service, and S3. The breadcrumb trail indicates the path: VPC > Your VPCs > vpc-0f43522a47cb5a0c2. The main heading is 'vpc-0f43522a47cb5a0c2 / vpc-test' with an 'Actions' button. Below this is a 'Details' section with a grid of information:

<b>VPC ID</b> vpc-0f43522a47cb5a0c2	<b>State</b> Available	<b>Block Public Access</b> Off	<b>DNS hostnames</b> Disabled
<b>DNS resolution</b> Enabled	<b>Tenancy</b> default	<b>DHCP option set</b> dopt-0db374882e4f2c606	<b>Main route table</b> rtb-0e36cb79466d5c6f8
<b>Main network ACL</b> acl-0c102fead2fbb8117	<b>Default VPC</b> No	<b>IPv4 CIDR</b> 10.0.0.0/16	<b>IPv6 pool</b> -
<b>IPv6 CIDR</b> -	<b>Network Address Usage metrics</b> Disabled	<b>Route 53 Resolver DNS Firewall rule groups</b> -	<b>Owner ID</b> 475721339759

Below the details is a 'Resource map' section with tabs for CIDRs, Flow logs, Tags, and Integrations. The 'Resource map' tab is active, showing a diagram with four main components: VPC (vpc-test), Subnets (4), Route tables (3), and Network connections (2). The VPC component is labeled 'Your AWS virtual network'. The Subnets component is labeled 'Subnets within this VPC'. The Route tables component is labeled 'Route network traffic to resources'. The Network connections component is labeled 'Connections to other networks'.



## 2. Route Table Setup

### Public Route Table:

- Associated with **PublicSubnet1** and **PublicSubnet2**
- Route:
  - **0.0.0.0/0** → **Internet Gateway (IGW)**

## Private Route Table:

- Associated with **PrivateSubnet1** and **PrivateSubnet2**
- No internet route (no NAT)

## Public Route Table

EC2 VPC IAM Aurora and RDS Directory Service S3

VPC > Route tables > rtb-0d1d4ba9429d55146

### rtb-0d1d4ba9429d55146 / vpc-endpoint-public-rt

Actions

**Details** info

Route table ID rtb-0d1d4ba9429d55146	Main No	Explicit subnet associations 2 subnets	Edge associations -
VPC vpc-0f43522a47cb5a0c2   vpc-test	Owner ID 475721339759		

Routes Subnet associations Edge associations Route propagation Tags

**Routes (2)** Both Edit routes

Filter routes

Destination	Target	Status	Propagated
0.0.0.0/0	igw-06c8dc3da6702d826	Active	No
10.0.0.0/16	local	Active	No

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

EC2 VPC IAM Aurora and RDS Directory Service S3

VPC > Route tables > rtb-0d1d4ba9429d55146

### rtb-0d1d4ba9429d55146 / vpc-endpoint-public-rt

Actions

**Details** info

Route table ID rtb-0d1d4ba9429d55146	Main No	Explicit subnet associations 2 subnets	Edge associations -
VPC vpc-0f43522a47cb5a0c2   vpc-test	Owner ID 475721339759		

Routes Subnet associations Edge associations Route propagation Tags

**Explicit subnet associations (2)** Edit subnet associations

Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
vpc-endpoint-public-1	subnet-030c636483b0e27b6	10.0.1.0/24	-
vpc-endpoint-public-2	subnet-052c6b4fe9688d9bc	10.0.2.0/24	-

**Subnets without explicit associations (0)** Edit subnet associations

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

## Private Route Table

The screenshot shows the AWS Management Console interface for a private route table. The breadcrumb navigation is VPC > Route tables > rtb-09443026045d08fa6. The title is "rtb-09443026045d08fa6 / vpc-endpoint-private-rt". The "Details" section shows the route table ID, VPC, main status, owner ID, explicit subnet associations (2 subnets), and edge associations. The "Routes" tab is selected, showing a table with 2 routes. The first route has destination pl-1fbc5976 and target vpce-00270dd1c72af39f1, both active. The second route has destination 10.0.0/16 and target local, also active.

EC2 VPC IAM Aurora and RDS Directory Service S3

VPC > Route tables > rtb-09443026045d08fa6

rtb-09443026045d08fa6 / vpc-endpoint-private-rt

**Details** info

Route table ID  
rtb-09443026045d08fa6

VPC  
vpc-0f43522a47cb5a0c2 | vpc-test

Main  
No

Owner ID  
475721339759

Explicit subnet associations  
2 subnets

Edge associations  
-

Routes Subnet associations Edge associations Route propagation Tags

**Routes (2)**

Filter routes

Destination	Target	Status	Propagated
pl-1fbc5976	vpce-00270dd1c72af39f1	Active	No
10.0.0/16	local	Active	No

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS Management Console interface for the same private route table, but with the "Subnet associations" tab selected. The "Explicit subnet associations (2)" section shows a table with 2 associations. The first association is for vpc-endpoint-private-1 with subnet ID subnet-070ff7fca44353699 and IPv4 CIDR 10.0.3.0/24. The second association is for vpc-endpoint-private-2 with subnet ID subnet-0f3f7263ff9ea97f7 and IPv4 CIDR 10.0.4.0/24. The "Subnets without explicit associations (0)" section is empty.

EC2 VPC IAM Aurora and RDS Directory Service S3

VPC > Route tables > rtb-09443026045d08fa6

rtb-09443026045d08fa6 / vpc-endpoint-private-rt

**Details** info

Route table ID  
rtb-09443026045d08fa6

VPC  
vpc-0f43522a47cb5a0c2 | vpc-test

Main  
No

Owner ID  
475721339759

Explicit subnet associations  
2 subnets

Edge associations  
-

Routes Subnet associations Edge associations Route propagation Tags

**Explicit subnet associations (2)**

Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
vpc-endpoint-private-1	subnet-070ff7fca44353699	10.0.3.0/24	-
vpc-endpoint-private-2	subnet-0f3f7263ff9ea97f7	10.0.4.0/24	-

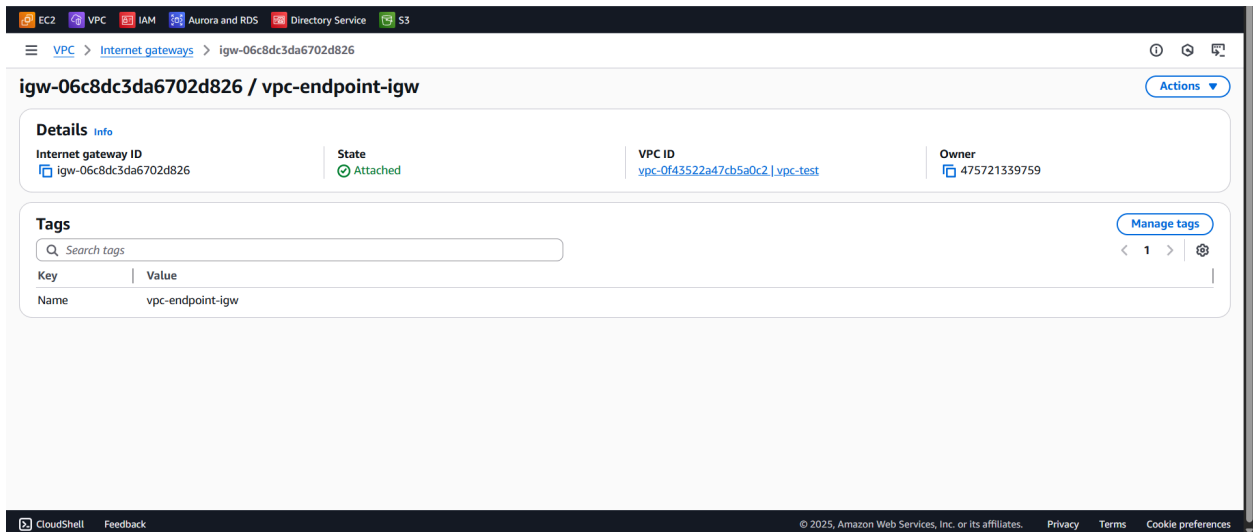
**Subnets without explicit associations (0)**

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

### 3. Internet Gateway

- **Created IGW** and attached it to the VPC
- Used **only** for public subnet routing



The screenshot shows the AWS Management Console interface for an Internet Gateway. The breadcrumb navigation indicates the path: VPC > Internet gateways > igw-06c8dc3da6702d826. The main heading is "igw-06c8dc3da6702d826 / vpc-endpoint-igw".

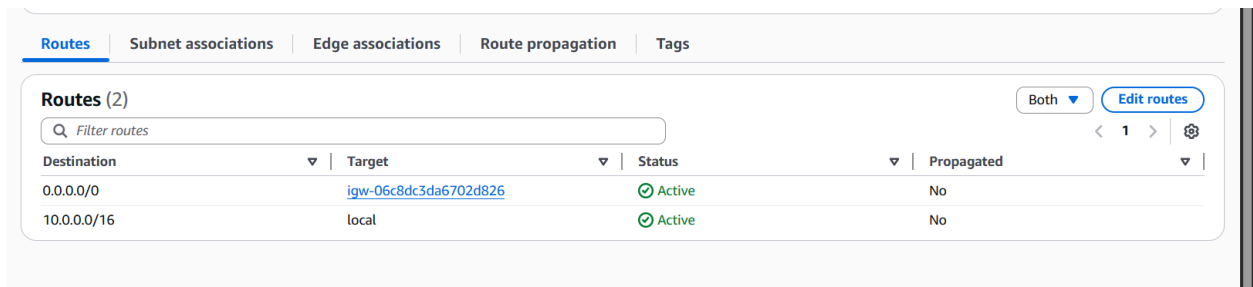
**Details** (info icon)

Internet gateway ID igw-06c8dc3da6702d826	State Attached	VPC ID vpc-0f43522a47cb5a0c2   vpc-test	Owner 475721339759
--	-------------------	--	-----------------------

**Tags** (Manage tags)

Key	Value
Name	vpc-endpoint-igw

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



The screenshot shows the "Routes" tab for the Internet Gateway. The breadcrumb navigation indicates the path: Routes > Subnet associations > Edge associations > Route propagation > Tags. The main heading is "Routes (2)".

Both Edit routes

Destination	Target	Status	Propagated
0.0.0.0/0	igw-06c8dc3da6702d826	Active	No
10.0.0.0/16	local	Active	No

## 4. EC2 Instances

### Public EC2

**Instance summary for i-02c38209c0c218800 (public ec2)** Info

Updated less than a minute ago

[Connect](#) [Instance state](#) [Actions](#)

<b>Instance ID</b> i-02c38209c0c218800	<b>Public IPv4 address</b> 3.28.191.177   <a href="#">open address</a>	<b>Private IPv4 addresses</b> 10.0.1.160
<b>IPv6 address</b> -	<b>Instance state</b> Running	<b>Public DNS</b> -
<b>Hostname type</b> IP name: ip-10-0-1-160.me-central-1.compute.internal	<b>Private IP DNS name (IPv4 only)</b> ip-10-0-1-160.me-central-1.compute.internal	<b>Elastic IP addresses</b> -
<b>Answer private resource DNS name</b> -	<b>Instance type</b> t3.micro	<b>AWS Compute Optimizer finding</b> <a href="#">Opt-in to AWS Compute Optimizer for recommendations.</a>   <a href="#">Learn more</a>
<b>Auto-assigned IP address</b> 3.28.191.177 [Public IP]	<b>VPC ID</b> vpc-0f43522a47cb5a0c2 (vpc-test)	<b>Auto Scaling Group name</b> -
<b>IAM Role</b> -	<b>Subnet ID</b> subnet-030c636483b0e27b6 (vpc-endpoint-public-1)	<b>Managed</b> false
<b>IMDSv2</b> Required	<b>Instance ARN</b> arn:aws:ec2:me-central-1:475721339759:instance/i-02c38209c0c218800	

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

### Private EC2

**Instance summary for i-023a3e5f44cee6b6d (private ec2)** Info

Refreshing instance data

[Connect](#) [Instance state](#) [Actions](#)

<b>Instance ID</b> i-023a3e5f44cee6b6d	<b>Public IPv4 address</b> -	<b>Private IPv4 addresses</b> 10.0.3.94
<b>IPv6 address</b> -	<b>Instance state</b> Running	<b>Public DNS</b> -
<b>Hostname type</b> IP name: ip-10-0-3-94.me-central-1.compute.internal	<b>Private IP DNS name (IPv4 only)</b> ip-10-0-3-94.me-central-1.compute.internal	<b>Elastic IP addresses</b> It is taking a bit longer than usual to fetch your data
<b>Answer private resource DNS name</b> -	<b>Instance type</b> t3.micro	<b>AWS Compute Optimizer finding</b> <a href="#">Opt-in to AWS Compute Optimizer for recommendations.</a>   <a href="#">Learn more</a>
<b>Auto-assigned IP address</b> It is taking a bit longer than usual to fetch your data	<b>VPC ID</b> vpc-0f43522a47cb5a0c2 (vpc-test)	<b>Auto Scaling Group name</b> -
<b>IAM Role</b> No roles attached to instance profile: EC2S3AccessRole	<b>Subnet ID</b> subnet-070ff7fca44353699	<b>Managed</b> false
<b>IMDSv2</b> Required	<b>Instance ARN</b> arn:aws:ec2:me-central-1:475721339759:instance/i-023a3e5f44cee6b6d	

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

### SSH Flow:

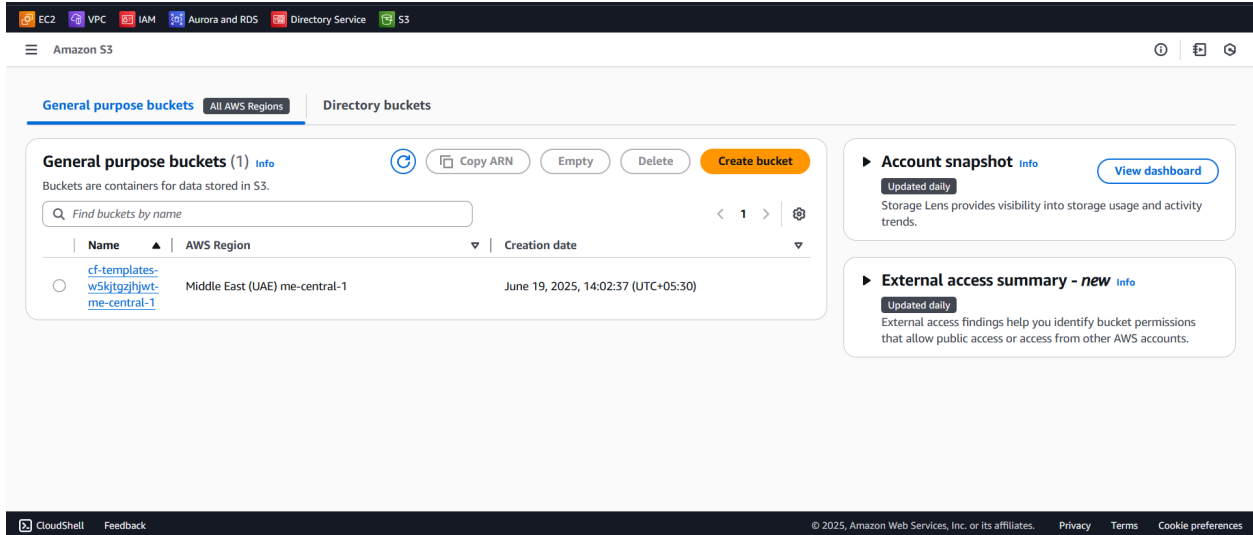
Local machine → PublicEC2 → PrivateEC2

(No NAT Gateway or public IP for private EC2)

---

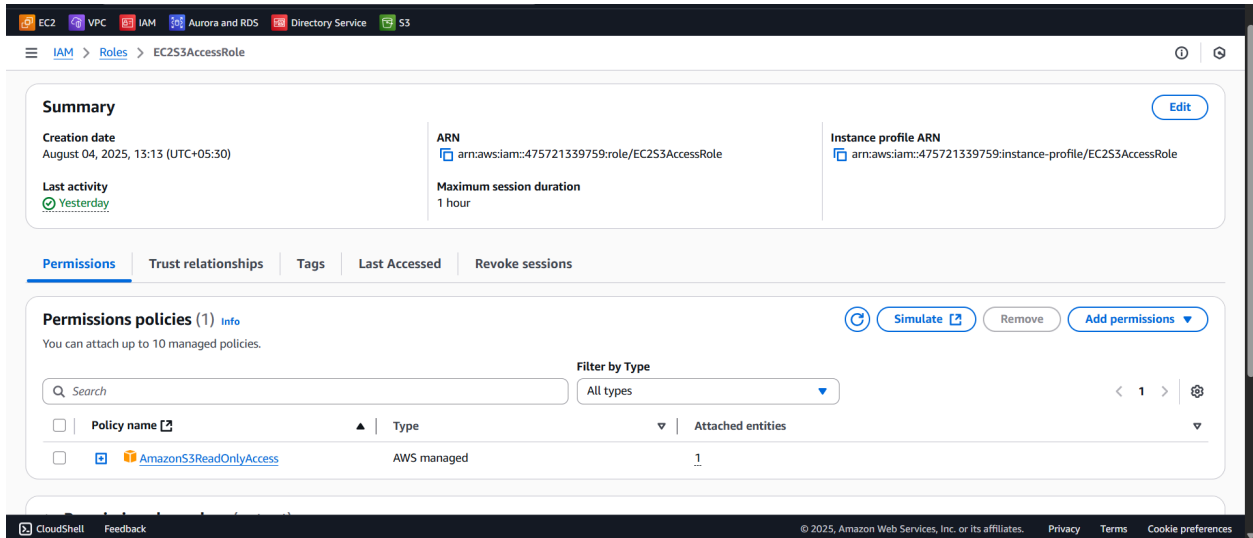


## S3 Bucket



The screenshot shows the Amazon S3 console interface. At the top, there's a navigation bar with various AWS services. The main content area is titled 'General purpose buckets (1)'. Below this, there's a search bar and a table of buckets. The table has columns for Name, AWS Region, and Creation date. One bucket is listed: 'cf-templates-w5kjtqzjhwt-me-central-1' in the 'me-central-1' region, created on 'June 19, 2025, 14:02:37 (UTC+05:30)'. To the right of the table, there are two informational cards: 'Account snapshot' and 'External access summary - new'. The footer of the console shows 'CloudShell', 'Feedback', and copyright information for Amazon Web Services, Inc.

## IAM Role with S3 Policy



The screenshot shows the AWS IAM console interface for the 'EC2S3AccessRole'. The 'Summary' tab is active, displaying the role's details: 'Creation date' (August 04, 2025, 13:13 (UTC+05:30)), 'ARN' (arn:aws:iam:475721339759:role/EC2S3AccessRole), and 'Instance profile ARN' (arn:aws:iam:475721339759:instance-profile/EC2S3AccessRole). Below the summary, there are tabs for 'Permissions', 'Trust relationships', 'Tags', 'Last Accessed', and 'Revoke sessions'. The 'Permissions' tab is active, showing a list of permissions policies. One policy is listed: 'AmazonS3ReadOnlyAccess' of type 'AWS managed'. The footer of the console shows 'CloudShell', 'Feedback', and copyright information for Amazon Web Services, Inc.

## 6. Gateway Endpoint Setup

- **Type:** Gateway Endpoint
- **VPC:** 10.0.0.0/16
- **Route Table attached:** Private Route Table

### Endpoint

EC2VPCIAMAurora and RDSDirectory ServiceS3

VPC>Endpoints>vpce-00270dd1c72af39f1

vpce-00270dd1c72af39f1 / test-endpoint

Details

Endpoint ID

vpce-00270dd1c72af39f1

VPC ID

vpce-0f43522a47cb5a0c2 (vpc-test)

Service region

me-central-1

Status

Available

Status message

-

Creation time

Monday 4 August 2025 at 13:00:43 GMT+5:30

Service name

com.amazonaws.me-central-1.s3

Endpoint type

Gateway

Private DNS names enabled

No

Route tables

Policy

Tags

Route tables (1)

Search

Name	Route Table ID	Main	Associated Id
vpce-endpoint-private-rt	rtb-09443026045d08fa6 (vpce-endpoint...	No	2 subnets

Manage route tables

### Route (Private Route Table)

Routes (2)

Both

Edit routes

Filter routes

Destination	Target	Status	Propagated
pl-1fbc5976	vpce-00270dd1c72af39f1	Active	No
10.0.0.0/16	local	Active	No

---