

Project Title:

"Inter-Region Private Network Connectivity Using AWS VPC Peering Across Global Regions"

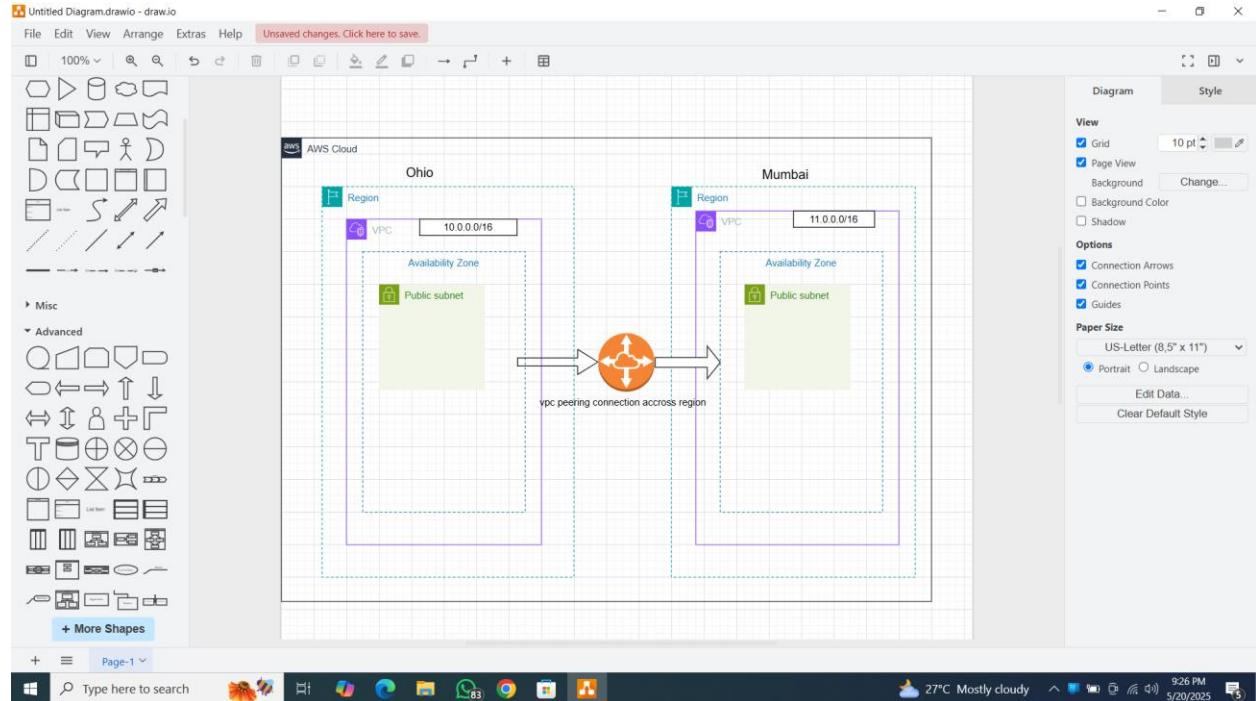
1. Project Overview

This project demonstrates secure and efficient inter-region connectivity between two Amazon Virtual Private Clouds (VPCs) hosted in different AWS regions (Ohio and Mumbai). VPC peering is used to enable private IP communication between EC2 instances across these regions without using public internet or VPNs.

2. Objectives

- Establish a **private, low-latency connection** between two VPCs across different AWS regions.
- Enable **EC2 instances** in both regions to communicate using **private IP addresses**.
- Ensure a **secure, cost-effective architecture** without public IPs or NAT Gateways.

3. Architecture Diagram



Regions:

- **Ohio (us-east-2)** → VPC A → CIDR: 10.0.0.0/16
- **Mumbai (ap-south-1)** → VPC B → CIDR: 11.0.0.0/16

Connection: Inter-region VPC Peering

Subnet Type: Public subnets in both regions

EC2 Communication: Private IP-based SSH/Ping

5. Implementation Steps

A. Create VPCs

- **Ohio:** 10.0.0.0/16
- **Mumbai:** 11.0.0.0/16

B. Create Subnets & Launch EC2 Instances

- Public subnets in both VPCs
- EC2 Instances with key pair & security group allowing:
 - **SSH (port 22)**
 - **ICMP (ping) / HTTP**

VPC-A

Screenshot of the AWS VPC Console showing the 'Your VPCs' dashboard.

The main table displays two VPCs:

Name	VPC ID	State	Block Public...	IPv4 CIDR	IPv6 CIDR
VPC-A	vpc-01d93e89f72231eb4	Available	Off	10.0.0.0/16	-
	vpc-0b25ccb2668ddec7f	Available	Off	172.31.0.0/16	-

The 'Details' tab is selected for VPC-A, showing the following configuration:

Setting	Value
VPC ID	vpc-01d93e89f72231eb4
State	Available
DNS resolution	Enabled
Tenancy	default
Block Public Access	Off
DHCP option set	dopt-0bce296af2077739
DNS hostnames	Disabled
Main route table	rtb-0658367da0c33295f

The browser address bar shows: https://us-east-2.console.aws.amazon.com/vpcconsole/home?region=us-east-2#vpcs

Screenshot of the AWS EC2 Instances page.

The main table displays one instance:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
EC2-Ubuntu...	i-0a860db30710ab46a	Running	t2.micro	Initializing	View alarms +	us-east-2a	-

The 'Select an instance' dropdown is open, showing the instance name: EC2-Ubuntu...

The browser address bar shows: https://us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#Instances

VPC Peering Communication | (352) Day 16 | Inter Region VPC | (352) AWS VPC Transit Gateway | vpcs | VPC Console | Instance details | EC2 | us-east-2 | EC2 Instance Connect | us-east-2 | +

https://us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#InstanceDetails:instanceId=i-0a860d830710ab46a

YouTube What is Subnet Mask? How to Build a Doc...

aws Search [Alt+S] United States (Ohio) Thauqiq @ thauqiq123-aws All Bookmarks

EC2 Instances i-0a860d830710ab46a

Instance summary for i-0a860d830710ab46a (EC2-Ubuntu-server-VPC-A) Info Updated 8 minutes ago

Instance ID i-0a860d830710ab46a Public IPv4 address 18.224.70.8 | open address

IPv6 address - Instance state Running

Hostname type IP name: ip-10-0-1-181.us-east-2.compute.internal Private IP DNS name (IPv4 only) ip-10-0-1-181.us-east-2.compute.internal

Answer private resource DNS name - Instance type t2.micro

Auto-assigned IP address 18.224.70.8 [Public IP] VPC ID vpc-01d93e89f72231eb4 (VPC-A)

IAM Role - Subnet ID subnet-0d7ffee942c82c5cf (PUB-SUB-2a)

IMDSv2 Required Instance ARN arn:aws:ec2:us-east-2:688567302802:instance/i-0a860d830710ab46a

Operator - Elastic IP addresses -

AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. | Learn more

Auto Scaling Group name - Managed false

Details Status and alarms Monitoring Security Networking Storage Tags

CloudShell Feedback Type here to search 131 AM 5/23/2025 © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

VPC Peering Communication | (352) Day 16 | Inter Region VPC | (352) AWS VPC Transit Gateway | vpcs | VPC Console | SecurityGroup | EC2 | us-east-2 | +

https://us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#SecurityGroup:group-id=sg-0bb97cc3d5576e6ce

YouTube What is Subnet Mask? How to Build a Doc...

aws Search [Alt+S] United States (Ohio) Thauqiq @ thauqiq123-aws All Bookmarks

EC2 Security Groups sg-0bb97cc3d5576e6ce - VPC-A-SG Actions

Capacity Reservations

Images AMIs AMI Catalog

Elastic Block Store Volumes Snapshots Lifecycle Manager

Network & Security Security Groups Placement Groups Key Pairs Network Interfaces

Load Balancing Load Balancers Target Groups Trust Stores

Auto Scaling Auto Scaling Groups

CloudShell Feedback Type here to search 121 AM 5/23/2025 © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

sg-0bb97cc3d5576e6ce - VPC-A-SG

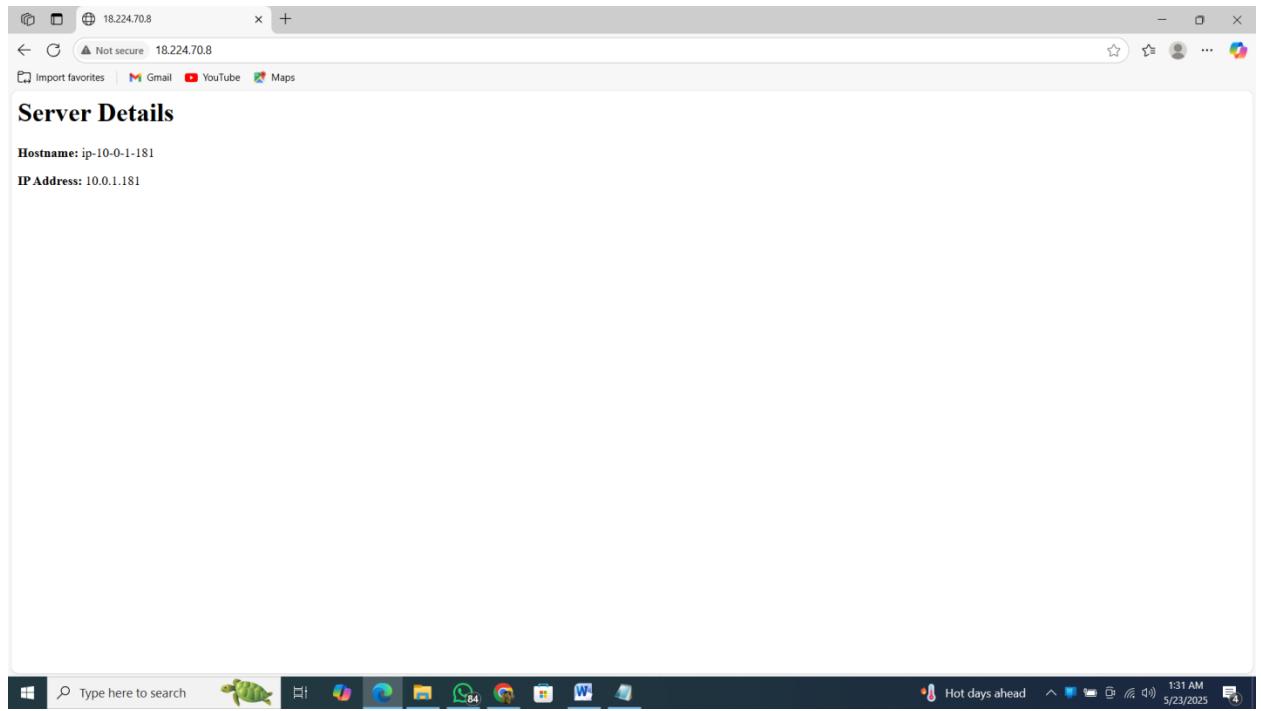
Details Security group ID sg-0bb97cc3d5576e6ce Description launch-wizard-1 created 2025-05-22T19:53:49.025Z VPC ID vpc-01d93e89f72231eb4

Owner 688567302802 Inbound rules count 3 Permission entries Outbound rules count 1 Permission entry

Inbound rules Outbound rules Sharing - new VPC associations - new Tags

Inbound rules (3) Manage tags Edit inbound rules

Name	Security group rule ID	IP version	Type	Protocol	Port range
-	sgr-0f67b825c24b503a5	IPv4	All ICMP - IPv4	ICMP	All
-	sgr-09b184f3eab3b3021	IPv4	HTTP	TCP	80
-	sgr-02acd9394985205f3	IPv4	SSH	TCP	22



VPC-B

VPC Peering Communication | (352) Day 16 | Inter Region VPC | (352) AWS VPC Transit Gateway | vpcs | VPC Console | Instances | EC2 | ap-south-1 | EC2 Instance Connect | us-east-1 | +

https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#vpcs:

aws Search [Alt+S] Asia Pacific (Mumbai) Thaufig @ thaufig123-aws

VPC > Your VPCs

Your VPCs (2) Info Last updated 31 minutes ago Actions Create VPC

Name	VPC ID	State	Block Public...	IPv4 CIDR	IPv6 CIDR
-	ypc-0487ffbb7ef8abc13	Available	Off	172.31.0.0/16	-
VPC-B	ypc-0b1a8d9526e233b02	Available	Off	11.0.0.0/16	-

Select a VPC above

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 30°C Partly cloudy 1:41 AM 5/23/2025

Type here to search

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 30°C Partly cloudy 1:41 AM 5/23/2025

VPC Peering Communication | (352) Day 16 | Inter Region VPC | (352) AWS VPC Transit Gateway | vpcs | VPC Console | Instances | EC2 | ap-south-1 | EC2 Instance Connect | us-east-1 | +

https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Instances:

aws Search [Alt+S] Asia Pacific (Mumbai) Thaufig @ thaufig123-aws

EC2 > Instances

Instances (1) Info Last updated less than a minute ago Connect Instance state Actions Launch instances

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
EC2-Ubuntu-s...	i-0cd1582013cb99f19	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1a	-

Select an instance

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 30°C Partly cloudy 1:42 AM 5/23/2025

Type here to search

Screenshot of the AWS EC2 Instance Details page for instance i-0cd1582013cb99f19.

Instance summary for i-0cd1582013cb99f19 (EC2-Ubuntu-server-VPC-B)

Attribute	Value
Public IPv4 address	13.127.167.147
Instance state	Running
Private IP DNS name (IPv4 only)	ip-11-0-1-136.ap-south-1.compute.internal
Instance type	t2.micro
VPC ID	vpc-0b1a8d9526e233b02 (VPC-B)
Subnet ID	subnet-0bfe5f1b3eff94428 (PUBLIC-SUB-VPC-B-1A)
Instance ARN	arn:aws:ec2:ap-south-1:688567302802:instance/i-0cd1582013cb99f19
Private IPv4 addresses	11.0.1.136
Public DNS	-
Elastic IP addresses	-
AWS Compute Optimizer finding	Opt-in to AWS Compute Optimizer for recommendation s.
Auto Scaling Group name	-
Managed	false

Details | **Status and alarms** | **Monitoring** | **Security** | **Networking** | **Storage** | **Tags**

Security details

- IAM Role: -
- Owner ID: 688567302802
- Launch time: Fri May 23 2025 01:12:05 GMT+0530 (India Standard Time)

Security groups

- sg-02f19b92d5c2f5911 (VPC-B-SG)

Inbound rules

Name	Security group rule ID	Port range	Protocol	Source	Security groups
-	sgr-0e281145a1f88055c	22	TCP	0.0.0.0/0	VPC-B-SG
-	sgr-00130a988a8db6ac0	All	ICMP	0.0.0.0/0	VPC-B-SG
-	sgr-0f245f77981525b37	80	TCP	0.0.0.0/0	VPC-B-SG

Outbound rules

Name	Security group rule ID	Port range	Protocol	Source	Security groups
-	sgr-0e281145a1f88055c	22	TCP	0.0.0.0/0	VPC-B-SG
-	sgr-00130a988a8db6ac0	All	ICMP	0.0.0.0/0	VPC-B-SG
-	sgr-0f245f77981525b37	80	TCP	0.0.0.0/0	VPC-B-SG

Screenshot of the AWS EC2 Instance Details page for instance i-0cd1582013cb99f19, focusing on the Security tab.

Security tab selected.

Security details

- IAM Role: -
- Owner ID: 688567302802
- Launch time: Fri May 23 2025 01:12:05 GMT+0530 (India Standard Time)

Security groups

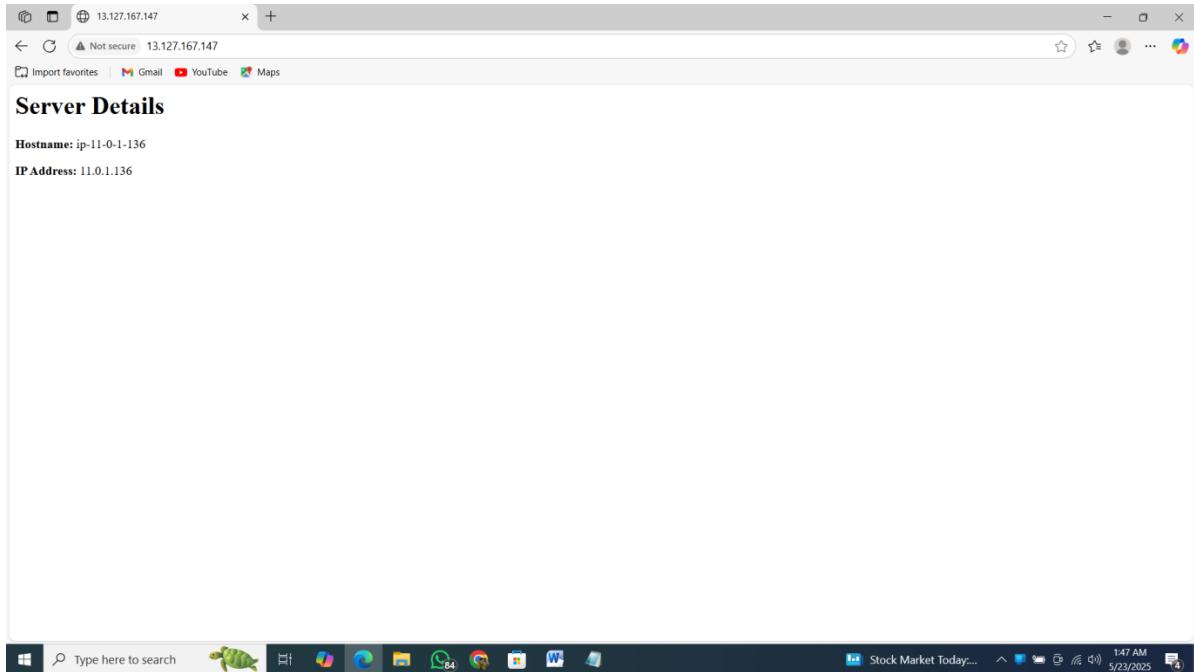
- sg-02f19b92d5c2f5911 (VPC-B-SG)

Inbound rules

Name	Security group rule ID	Port range	Protocol	Source	Security groups
-	sgr-0e281145a1f88055c	22	TCP	0.0.0.0/0	VPC-B-SG
-	sgr-00130a988a8db6ac0	All	ICMP	0.0.0.0/0	VPC-B-SG
-	sgr-0f245f77981525b37	80	TCP	0.0.0.0/0	VPC-B-SG

Outbound rules

Name	Security group rule ID	Port range	Protocol	Source	Security groups
-	sgr-0e281145a1f88055c	22	TCP	0.0.0.0/0	VPC-B-SG
-	sgr-00130a988a8db6ac0	All	ICMP	0.0.0.0/0	VPC-B-SG
-	sgr-0f245f77981525b37	80	TCP	0.0.0.0/0	VPC-B-SG



C. Create VPC Peering Connection

- Initiate peering from VPC A (Ohio) to VPC B (Mumbai)
 - Accept the request in the same account
-
- **Navigate to the VPC Dashboard:**
 - Go to the AWS Console → **VPC** → In the left-hand menu, click on "**Peering Connections**".
-
- **Initiate Peering from Ohio (VPC A):**
 - Click "**Create Peering Connection**".
 - Under **Name tag**, give it a recognizable name (e.g., VPC-A - TO - VPC-B Peering Connection).
 - Under **VPC Requester**, select the VPC in **Ohio** (VPC A with CIDR 10.0.0.0/16).
 - For **VPC Acceptor**, select **Another region**.
 - Choose **ap-south-1 (Mumbai)**.
 - Choose the VPC in Mumbai (VPC B with CIDR 11.0.0.0/16).
 - Select **My account** (since both VPCs are in the same AWS account).
 - Click "**Create Peering Connection**".

The screenshot shows the AWS VPC Peering connections page. The left sidebar is expanded, showing sections for Virtual private cloud, Security, and PrivateLink and Lattice. Under Peering connections, there is a link to 'Create peering connection'. The main content area is titled 'Peering connections' with a search bar. It displays a table with columns for Name, Peering connection ID, Status, Requester VPC, and Acceptor VPC. A message at the top right says 'No peering connection found'. Below the table, a note says 'Select a peering connection above'. At the bottom of the page, there are three small icons.

The screenshot shows the 'Create peering connection' wizard, step 1: 'Peering connection settings'. The title is 'Create peering connection'. A note says 'A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately.' There is a link to 'Info'. The section is titled 'Peering connection settings' with a note 'Name - optional'. A text input field contains 'VPC-A - TO - VPC-B Peering Connection'. Below it, 'Select a local VPC to peer with' has a dropdown for 'VPC ID (Requester)' set to 'vpc-01d93e89f72231eb4 (VPC-A)'. A table for 'VPC CIDRs for vpc-01d93e89f72231eb4 (VPC-A)' shows one row: CIDR 10.0.0.0/16, Status Associated, and Status reason -. At the bottom, 'Select another VPC to peer with' has 'Account' set to 'My account' (radio button checked) and 'Region' set to 'Ohio' (dropdown). The status bar at the bottom right shows 'Cannot contact provisioning server. Click here for more information.'

Screenshot of the AWS VPC Peering connections creation page in the AWS Management Console.

Select another VPC to peer with

- Account:** My account (radio button selected)
- Region:** Another Region (radio button selected)
- VPC ID (Acceptor):** vpc-0b1a8d9526e233b02

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
Name	VPC-A - TO - VPC-B Peering Connection

Create peering connection

Screenshot of the AWS VPC Peering connection details page in the AWS Management Console.

pcx-0da73d2e220289e6c / VPC-A - TO - VPC-B Peering Connection

Details

Requester owner ID	688567302802	Acceptor owner ID	688567302802	VPC Peering connection ARN	arn:aws:ec2:us-east-2:688567302802:vpc-peering-connection/pcx-0da73d2e220289e6c
Peering connection ID	pcx-0da73d2e220289e6c	Requester VPC	vpc-01d93e89f72231eb4 / VPC-A	Acceptor VPC	vpc-0b1a8d9526e233b02
Status	Initiating Request to 688567302802	Requester CIDRs	10.0.0.0/16	Acceptor CIDRs	-
Expiration time	Friday, May 30, 2025 at 01:58:32 GMT+5:30	Requester Region	Ohio (us-east-2)	Acceptor Region	Mumbai (ap-south-1)

DNS

Requester VPC ([vpc-01d93e89f72231eb4 / VPC-A](#)) Info

Allow accepter VPC to resolve DNS of hosts in requester VPC to private IP addresses

Actions

Accept the Peering Request (Mumbai Region):

- Switch to the **Mumbai region** in the AWS Console.
- Go to **VPC → Peering Connections**.
- You'll see the pending request.
- Select the request → Click "Actions" → "Accept Request".

The screenshot shows the AWS VPC Peering Connections page. In the center, there is a table titled "Peering connections (1/1) Info". The table has columns for Name, Peering connection ID, Status, and Requester VPC. One row is listed: "pcx-0da73d2e220289e6c" (Status: Pending acceptance, Requester VPC: vpc-01d93e89f72231e). To the right of the table, a context menu is open under the heading "Actions". The menu includes options: View details, Accept request (which is highlighted with a blue border), Reject request, Edit DNS settings, Manage tags, and Delete peering connection. Below the table, a modal window for "pcx-0da73d2e220289e6c" is displayed, stating "Pending acceptance" and providing instructions: "You can accept or reject this peering connection request using the 'Actions' menu. You have until Friday, May 30, 2025 at 01:58:32 GMT+5:30 to accept or reject the request, otherwise it expires." At the bottom of the page, there are tabs for Details, DNS, Route tables, and Tags, with "Details" selected. The "Details" section shows Requester owner ID (688567302802) and Acceptor owner ID (688567302802). The VPC Peering connection ARN is also listed as arn:aws:vpc:ap-south-1:688567302802:vpc-peering-connection/pcx-0da73d2e220289e6c. The bottom of the screen shows the Windows taskbar with various pinned icons like File Explorer, Edge, and File Manager.

The screenshot shows the AWS VPC Peering Connections page. A modal dialog box is open, prompting the user to accept a VPC peering connection request. The modal displays the following details:

- Requester VPC:** vpc-01d93e89f72231eb4
- Acceptor VPC:** vpc-0b1a8d9526e233b02 / VPC-B
- Requester CIDR:** 10.0.0.0/16
- Requester Region:** Ohio (us-east-2)
- Requester owner ID:** 688567302802 (This account)
- Acceptor CIDR:** 10.0.0.0/16
- Acceptor Region:** Mumbai (ap-south-1)
- Acceptor owner ID:** 688567302802 (This account)

The modal includes a "Pending acceptance" note and two buttons: "Cancel" and "Accept request".

The screenshot shows the AWS VPC Peering Connections page after the connection has been accepted. A green banner at the top indicates that the connection has been established.

The table lists the peering connection details:

Name	Peering connection ID	Status	Requester VPC	Acceptor VPC
VPC-B - TO - VPC-B Peering Connection	pcx-0da73d2e220289e6c	Active	vpc-01d93e89f72231eb4	vpc-0b1a8d9526e233b02 / VPC-B

The modal dialog box is no longer visible, indicating the connection is now active.

Peering Connection Status:

- Once accepted, the peering connection status should change to "**Active**"

D. Update Route Tables

- Add route to 11.0.0.0/16 in Ohio VPC's route table via peering
- Add route to 10.0.0.0/16 in Mumbai VPC's route table via peering

The screenshot shows the AWS VPC Route Tables page. The left sidebar is the VPC dashboard with sections for EC2 Global View, Virtual private cloud (Your VPCs, Subnets, Route tables selected), Security (Network ACLs, Security groups), and PrivateLink and Lattice. The main content area shows a table of route tables:

Name	Route table ID	Explicit subnet assoc...	Main	VPC
<input checked="" type="checkbox"/> VPC-A-RT	rtb-0fb9181d82d38ad4	subnet-0d7ffee942c82c5...	-	vpc-01d93e89f72231eb4 V
<input type="checkbox"/>	rtb-0658367da0c33295f	-	-	vpc-01d93e89f72231eb4 V
<input type="checkbox"/>	rtb-0f10a72b1baa98f52	-	-	vpc-0b25cb2668dec7f

Below the table, a specific route table is selected: **rtb-0fb9181d82d38ad4 / VPC-A-RT**. The Details tab is selected, showing:

- Route table ID: rtb-0fb9181d82d38ad4
- Main: No
- Owner ID: 688567302802
- Explicit subnet associations: subnet-0d7ffee942c82c5cf / PUB-SUB-2a
- Edge associations: -

The screenshot shows the AWS VPC Route Tables page for the selected route table: **rtb-0fb9181d82d38ad4 / VPC-A-RT**. The left sidebar is the VPC dashboard. The main content area shows the Details tab and the Routes tab.

Details tab (selected):

- Route table ID: rtb-0fb9181d82d38ad4
- Main: No
- Owner ID: 688567302802
- Explicit subnet associations: subnet-0d7ffee942c82c5cf / PUB-SUB-2a
- Edge associations: -

Routes tab:

Destination	Target	Status	Propagated
0.0.0.0/0	igw-09c9532d91eddfab2	Active	No
10.0.0.0/16	local	Active	No

Screenshot of the AWS VPC Route Tables configuration page for a specific route table.

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
Q 0.0.0.0/0	Internet Gateway	Active	No
Q 11.0.0.0/16	Peering Connection	-	No
	Q pcv-0da73d2e220289e6c	X	

Add route

Buttons: Cancel, Preview, Save changes



Screenshot of the AWS VPC Route Tables management interface.

Route tables (1/3) Info

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
-	rtb-014f95c2483c6cff4	-	-	Yes	vpc-0b1a8d9526e233b02 v
-	rtb-0cdff4ac3f1bd84fe1	-	-	Yes	vpc-0487ffbb7ef8abcf13
<input checked="" type="checkbox"/> VPC-B-RT	rtb-0f97856549bd96d26	subnet-0bfe3f1b3eff94428	-	No	vpc-0b1a8d9526e233b02 v

rtb-0f97856549bd96d26 / VPC-B-RT

Details | Routes | Subnet associations | Edge associations | Route propagation | Tags

Details

Route table ID rtb-0f97856549bd96d26	Main No	Explicit subnet associations subnet-0bfe3f1b3eff94428 / PUBLIC-SUB-VPC-B-1A	Edge associations -
VPC vpc-0b1a8d9526e233b02 VPC-B	Owner ID 688567302802		

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

The screenshot shows the AWS VPC console with the URL <https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#RouteTableDetails:RouteTableId=rtb-0f97856549bd96d26>. The page displays the details of a route table named 'rtb-0f97856549bd96d26 / VPC-B-RT'. The 'Details' tab is selected, showing the Route table ID (rtb-0f97856549bd96d26), Main status (No), Owner ID (vpc-0b1a8d9526e233b02 | VPC-B), and explicit subnet associations (subnet-0fe3fb3eff94428 / PUBLIC-SUB-VPC-B-1A). The 'Routes' tab shows two routes: one to 'igw-0f78a0a9e237026fb' (Status: Active, Propagated: No) and another to 'local' (Status: Active, Propagated: No). The left sidebar includes sections for EC2 Global View, Virtual private cloud (Your VPCs, Subnets, Route tables), Security (Network ACLs, Security groups), and PrivateLink and Lattice.

The screenshot shows the 'Edit routes' dialog for the route table 'rtb-0f97856549bd96d26'. The table lists existing routes and allows for adding new ones. One route to 'local' is marked as 'Active'. Another route to 'Internet Gateway' (target 'igw-0f78a0a9e237026fb') is also active. A third route to 'Peering Connection' (target 'pcx-0da73d2e220289e6d') is listed but has a status of '-' and is not propagated. Buttons for 'Add route', 'Cancel', 'Preview', and 'Save changes' are at the bottom.



Test the Setup

After successfully establishing the VPC peering connection and updating the route tables and security groups, it's essential to test connectivity between the two EC2 instances located in Ohio and Mumbai.

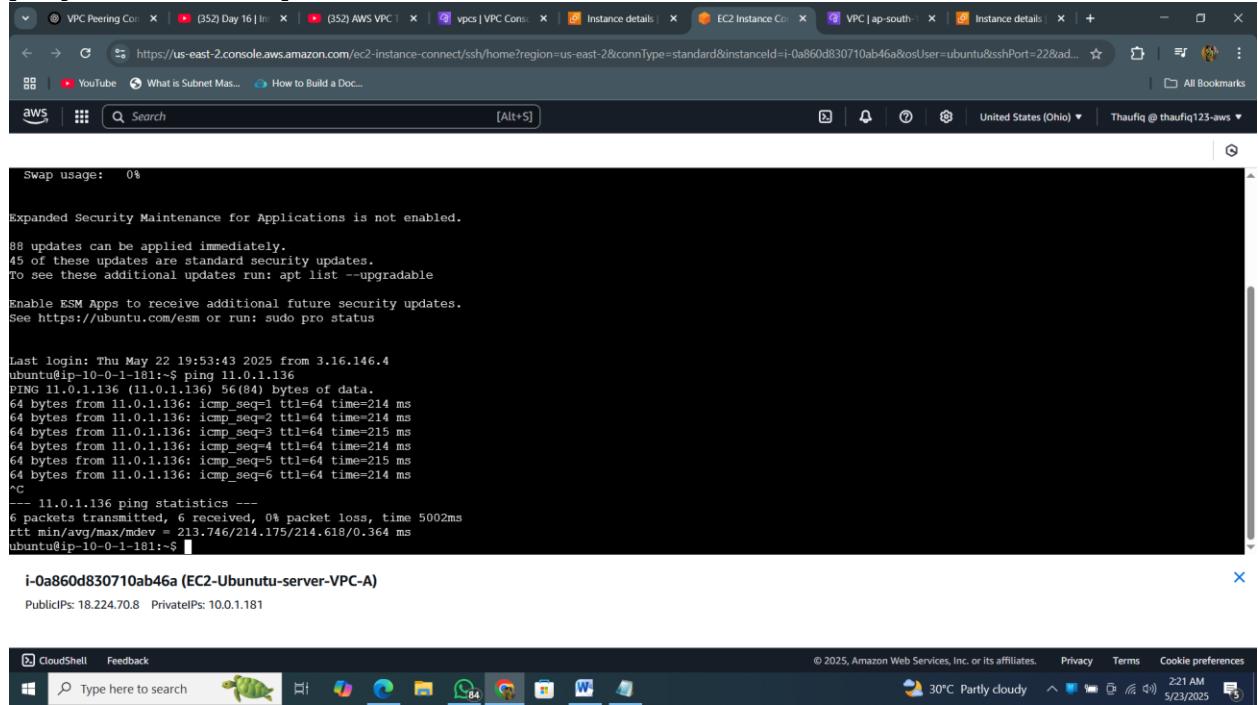
Step-by-Step Testing Instructions:

1. **Obtain the Private IP Addresses:**
 - Go to the **EC2 Dashboard** in the AWS Console for each region.
 - Note down the **private IP address** of the EC2 instance in **Ohio** and **Mumbai**.
2. **SSH into the Ohio EC2 Instance:**
 - From your local terminal or using EC2 Instance Connect (if allowed), SSH into the EC2 instance in the Ohio region:

Ping the EC2 Instance in Mumbai:

- From the Ohio EC2 instance, run the following command using the private IP of the Mumbai EC2:

```
ping <Mumbai-EC2-private-IP> (11.0.1.136)
```



The screenshot shows a terminal window with the following content:

```
Swap usage:  0%  
  
Expanded Security Maintenance for Applications is not enabled.  
88 updates can be applied immediately.  
45 of these updates are standard security updates.  
To see these additional updates run: apt list --upgradable  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
  
Last login: Thu May 22 19:53:43 2025 from 3.16.146.4  
ubuntu@ip-10-0-1-181:~$ ping 11.0.1.136  
PING 11.0.1.136 (11.0.1.136) 56(84) bytes of data:  
64 bytes from 11.0.1.136: icmp_seq=1 ttl=64 time=214 ms  
64 bytes from 11.0.1.136: icmp_seq=2 ttl=64 time=214 ms  
64 bytes from 11.0.1.136: icmp_seq=3 ttl=64 time=215 ms  
64 bytes from 11.0.1.136: icmp_seq=4 ttl=64 time=214 ms  
64 bytes from 11.0.1.136: icmp_seq=5 ttl=64 time=215 ms  
64 bytes from 11.0.1.136: icmp_seq=6 ttl=64 time=214 ms  
^C  
--- 11.0.1.136 ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 5002ms  
rtt min/avg/max/mdev = 213.746/214.175/214.618/0.364 ms  
ubuntu@ip-10-0-1-181:~$  
  
i-0a860d830710ab46a (EC2-Ubuntu-server-VPC-A)  
Public IPs: 18.224.70.8 Private IPs: 10.0.1.181
```

The terminal window is part of a desktop environment, with a taskbar at the bottom showing various application icons like CloudShell, Feedback, File Explorer, Edge, and others. The system tray indicates a temperature of 30°C, partly cloudy weather, and the date/time as 221 AM 5/23/2025.

SSH from Ohio to Mumbai (optional):

- If port 22 is allowed in the Mumbai EC2 security group from Ohio's CIDR range, you can also SSH into the Mumbai instance using its private IP

Confirm Bidirectional Communication:

- Repeat the steps in reverse by SSH'ing into the Mumbai EC2 instance and pinging the Ohio EC2's private IP.
- If both instances can ping each other via private IPs, then the VPC peering setup is working correctly.

The screenshot shows a CloudShell terminal window with the following content:

```
compliance features.

https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

85 updates can be applied immediately.
45 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Thu May 22 20:13:48 2025 from 13.233.177.4
ubuntu@ip-11-0-1-136:~$ ping 10.0.1.181
PING 10.0.1.181 (10.0.1.181) 56(84) bytes of data.
64 bytes from 10.0.1.181: icmp_seq=1 ttl=64 time=214 ms
64 bytes from 10.0.1.181: icmp_seq=2 ttl=64 time=214 ms
64 bytes from 10.0.1.181: icmp_seq=3 ttl=64 time=213 ms
64 bytes from 10.0.1.181: icmp_seq=4 ttl=64 time=213 ms
64 bytes from 10.0.1.181: icmp_seq=5 ttl=64 time=214 ms
^C
--- 10.0.1.181 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 213.286/213.574/213.893/0.232 ms
ubuntu@ip-11-0-1-136:~$
```

i-0cd1582013cb99f19 (EC2-Ubuntu-server-VPC-B)

Public IPs: 13.127.167.147 Private IPs: 11.0.1.136

The terminal also displays the AWS CloudShell interface with various tabs and navigation buttons at the top.

Expected Result:

- Successful ping replies from both directions.
- Optional SSH session initiated using private IP (if allowed in security group rules).
- No need for public IPs or internet access — all traffic flows through AWS's internal network.

Benefits

- **Cost-efficient:** No NAT or VPN required
- **Low latency:** AWS backbone routing
- **Secure:** Private IP-based communication

Conclusion

This project validates the feasibility and simplicity of using AWS VPC Peering for secure, private connectivity across global regions within the same AWS account, making it an ideal solution for distributed architectures and hybrid workloads.

