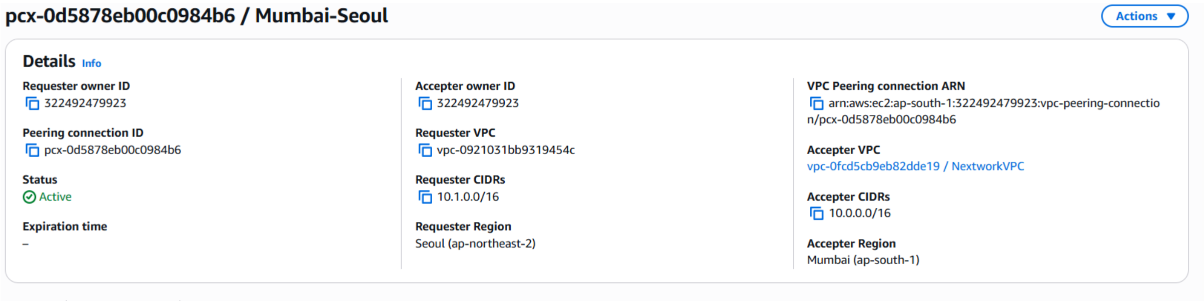
VPC Peering for Cross Region

Mohammed Amir

Introduction

In this project, configures a cross-region VPC peering connection between two Virtual Private Clouds (VPCs) — each hosted in different AWS regions — while maintaining secure communication between EC2 instances across both public and private subnets. The goal was to enable seamless SSH and ICMP (ping) communication between instances in both VPCs, following secure networking practices and AWS best architecture patterns.



pcx-0d5878eb00c0984b6 / Mumbai-Seoul

Details

Requester owner ID
322492479923

Peering connection ID
pcx-0d5878eb00c0984b6

Status
Active

Expiration time
–

Accepter owner ID
322492479923

Requester VPC
vpc-0921031bb9319454c

Requester CIDRs
10.1.0.0/16

Requester Region
Seoul (ap-northeast-2)

VPC Peering connection ARN
arn:aws:ec2:ap-south-1:322492479923:vpc-peering-connection/pcx-0d5878eb00c0984b6

Accepter VPC
vpc-0fcd5cb9eb82dde19 / NextworkVPC

Accepter CIDRs
10.0.0.0/16

Accepter Region
Mumbai (ap-south-1)

Topics Covered :-

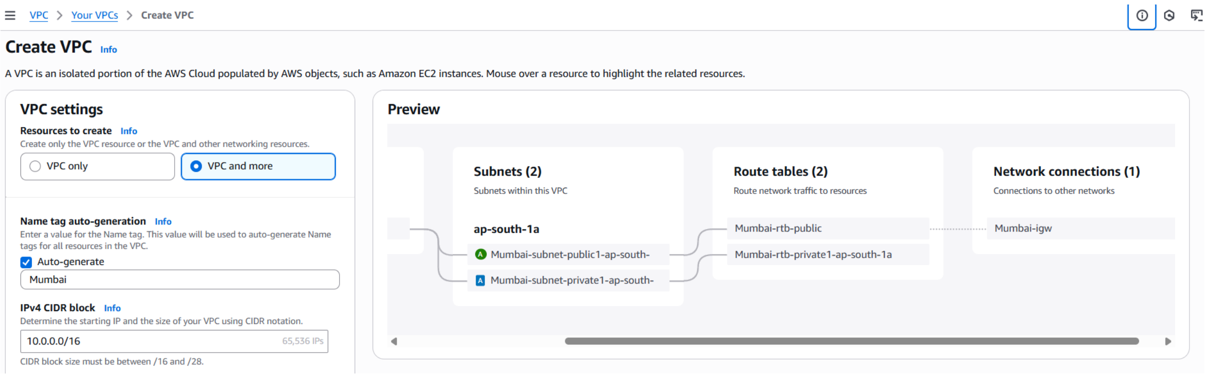
1. Amazon VPC (Virtual Private Cloud)

Amazon VPC lets you provision a logically isolated network in the AWS Cloud. You have complete control over your virtual networking environment, including IP address ranges, subnets, route tables, and network gateways.

VPC Design (Mumbai and Seoul) :-

Mumbai Region (ap-south-1)

- VPC CIDR: 10.0.0.0/16
- Public Subnet: 10.0.1.0/24
- Private Subnet: 10.0.2.0/24
- EC2: One in public subnet, one in private subnet
- Mumbai - VPC is configured with an Internet Gateway for public subnets.



Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to highlight the related resources.

VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.
○ VPC only ● VPC and more

Name tag auto-generation Info
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.
☑ Auto-generate
Mumbai

IPv4 CIDR block Info
Determine the starting IP and the size of your VPC using CIDR notation.
10.0.0.0/16 65,536 IPs
CIDR block size must be between /16 and /28.

Preview

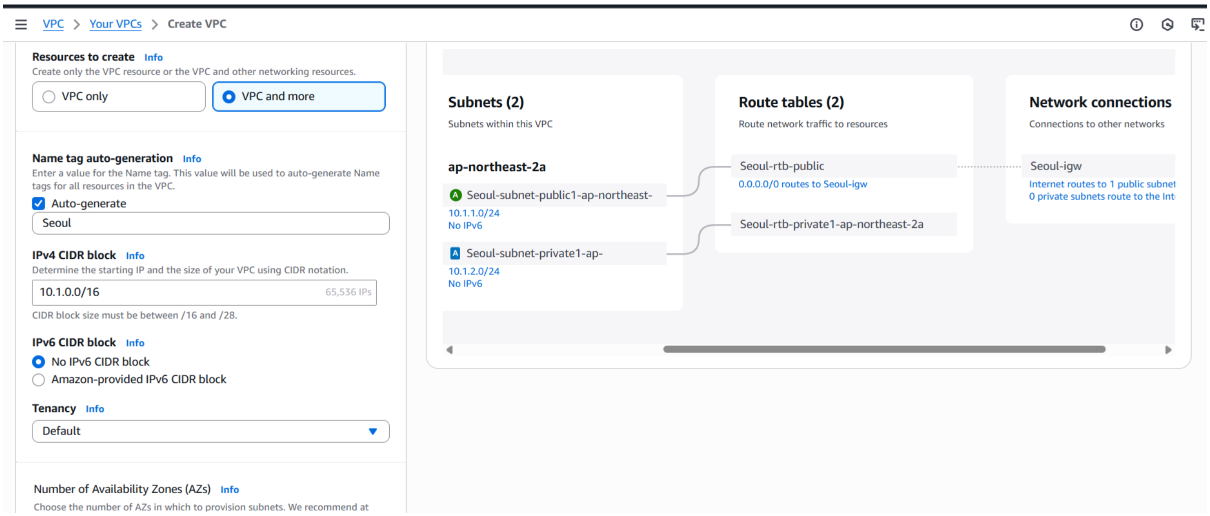
Subnets (2)
Subnets within this VPC
ap-south-1a
Mumbai-subnet-public1-ap-south-
Mumbai-subnet-private1-ap-south-

Route tables (2)
Route network traffic to resources
Mumbai-rtb-public
Mumbai-rtb-private1-ap-south-1a

Network connections (1)
Connections to other networks
Mumbai-igw

Seoul (ap-northeast-2)

- VPC CIDR: 10.1.0.0/16
- Public Subnet: 10.1.1.0/24
- Private Subnet: 10.1.2.0/24
- EC2: One in public subnet, one in private subnet
- Seoul - VPC is configured with an Internet Gateway for public subnets.



Resources to create Info
Create only the VPC resource or the VPC and other networking resources.
○ VPC only ● VPC and more

Name tag auto-generation Info
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.
☑ Auto-generate
Seoul

IPv4 CIDR block Info
Determine the starting IP and the size of your VPC using CIDR notation.
10.1.0.0/16 65,536 IPs
CIDR block size must be between /16 and /28.

IPv6 CIDR block Info
● No IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block

Tenancy Info
Default

Number of Availability Zones (AZs) Info
Choose the number of AZs in which to provision subnets. We recommend at

Subnets (2)
Subnets within this VPC
ap-northeast-2a
Seoul-subnet-public1-ap-northeast-
10.1.1.0/24
No IPv6
Seoul-subnet-private1-ap-
10.1.2.0/24
No IPv6

Route tables (2)
Route network traffic to resources
Seoul-rtb-public
0.0.0.0/0 routes to Seoul-igw
Seoul-rtb-private1-ap-northeast-2a

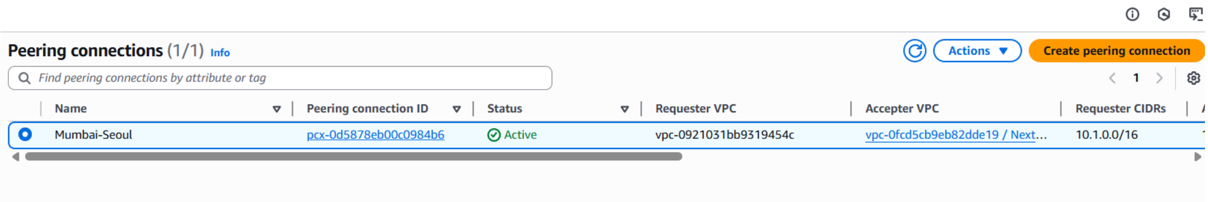
Network connections
Connections to other networks
Seoul-igw
Internet routes to 1 public subnet
0 private subnets route to the Int

2. VPC Peering (Cross-Region)

VPC peering is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses.

Peering Setup:

- Created a VPC peering connection from Seoul to Mumbai region.
- Accepted the request from the Mumbai side.



Peering connections (1/1) Info
Actions ▼
Create peering connection
Find peering connections by attribute or tag

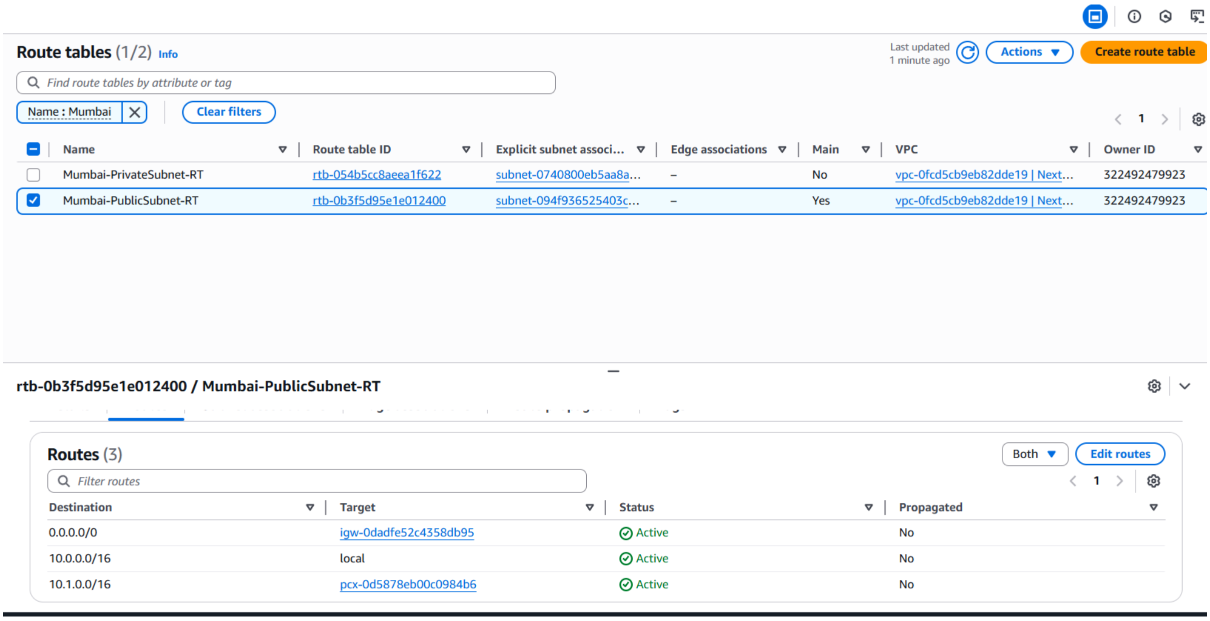
	Name	Peering connection ID	Status	Requester VPC	Accepter VPC	Requester CIDRs
●	Mumbai-Seoul	pcx-0d5878eb00c0984b6	✓ Active	vpc-0921031bb9319454c	vpc-0fcd5cb9eb82dde19 / Next...	10.1.0.0/16

3. Route Table Configuration

An AWS Route Table is a set of rules (called routes) that determines how network traffic is directed within a VPC (Virtual Private Cloud).

Mumbai Region

- Public and Private Route Tables updated to route traffic to 10.1.0.0/16 via peering connection.



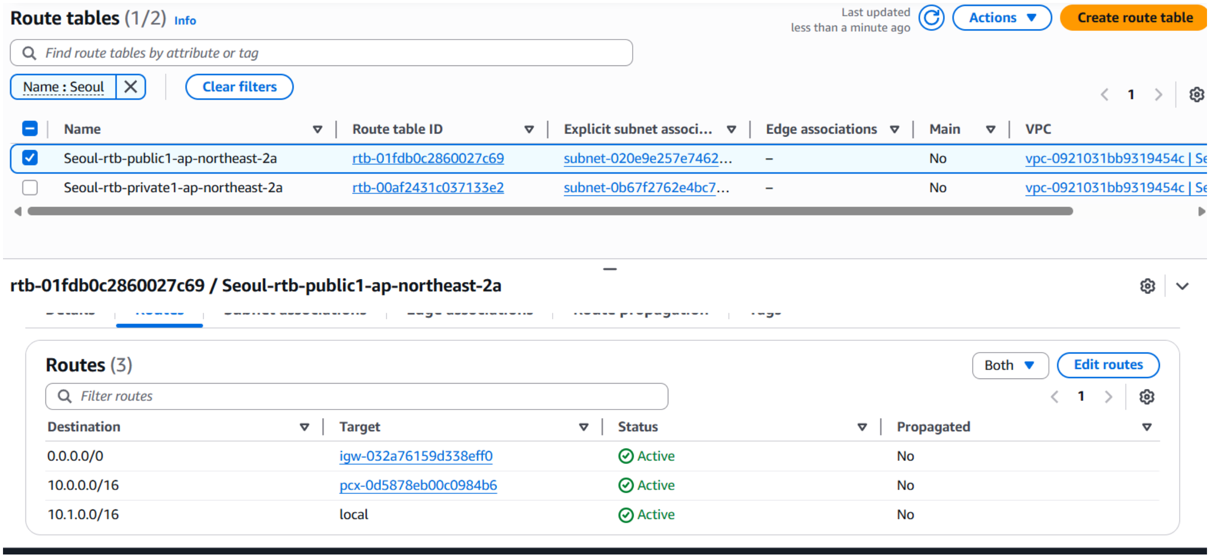
☐	Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC	Owner ID
☐	Mumbai-PrivateSubnet-RT	rtb-054b5cc8aeea1f622	subnet-0740800eb5aa8a...	–	No	vpc-0fcd5cb9eb82dde19 | Next...	322492479923
☑	Mumbai-PublicSubnet-RT	rtb-0b3f5d95e1e012400	subnet-094f936525403c...	–	Yes	vpc-0fcd5cb9eb82dde19 | Next...	322492479923

rtb-0b3f5d95e1e012400 / Mumbai-PublicSubnet-RT

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0dadfe52c4358db95	✓ Active	No
10.0.0.0/16	local	✓ Active	No
10.1.0.0/16	pcx-0d5878eb00c0984b6	✓ Active	No

Seoul Region

- Public and Private Route Tables updated to route traffic to 10.0.0.0/16 via peering connection.



☑	Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
☑	Seoul-rtb-public1-ap-northeast-2a	rtb-01fdb0c2860027c69	subnet-020e9e257e7462...	–	No	vpc-0921031bb9319454c | Se
□	Seoul-rtb-private1-ap-northeast-2a	rtb-00af2431c037133e2	subnet-0b67f2762e4bc7...	–	No	vpc-0921031bb9319454c | Se

rtb-01fdb0c2860027c69 / Seoul-rtb-public1-ap-northeast-2a

Destination	Target	Status	Propagated
0.0.0.0/0	igw-032a76159d338eff0	✓ Active	No
10.0.0.0/16	pcx-0d5878eb00c0984b6	✓ Active	No
10.1.0.0/16	local	✓ Active	No

4. Security Groups

A Security Group (SG) in AWS is a virtual firewall that controls inbound and outbound traffic to EC2 instances and other resources at the instance level.

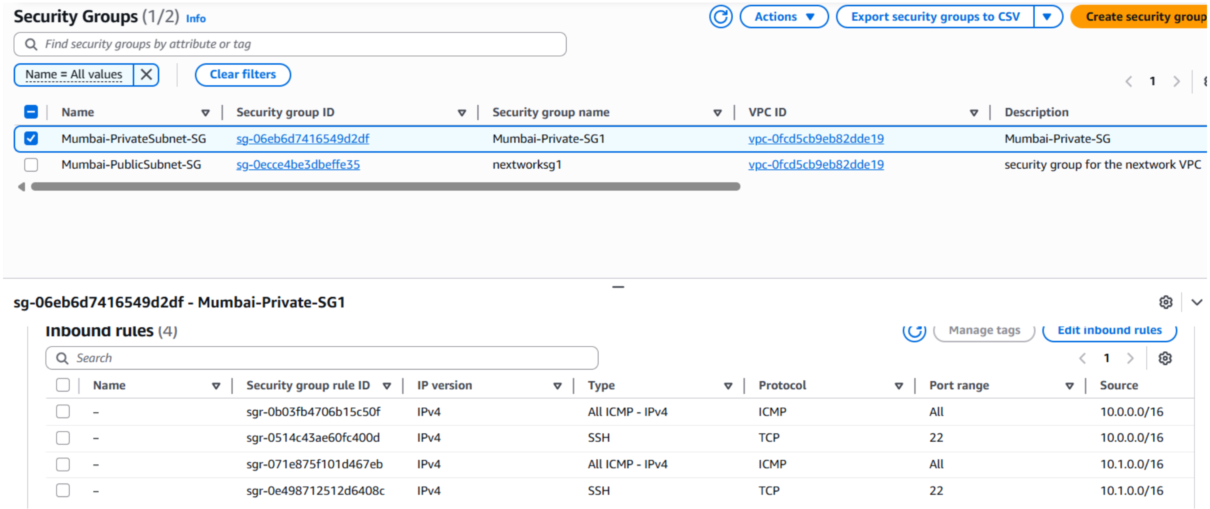
Security Groups (Applied to Public & Private Subnets in both VPC's)

Created individual Security Groups for:

- Public Subnets (Mumbai & Seoul)
- Private Subnets (Mumbai & Seoul)

Inbound Rules:

- SSH (Port 22) from 10.0.0.0/16 and 10.1.0.0/16
  → Allows secure SSH access from all instances across both VPCs.
- All ICMP - IPv4 from 10.0.0.0/16 and 10.1.0.0/16
  → Enables ping requests for connectivity checks across all subnets.


Security Groups (1/2) Info
Actions
Export security groups to CSV
Create security group
Find security groups by attribute or tag
Name = All values
Clear filters

☑	Name	Security group ID	Security group name	VPC ID	Description
☑	Mumbai-PrivateSubnet-SG	sg-06eb6d7416549d2df	Mumbai-Private-SG1	vpc-0fcd5cb9eb82dde19	Mumbai-Private-SG
□	Mumbai-PublicSubnet-SG	sg-0ecce4be3dbeffe35	nextworksg1	vpc-0fcd5cb9eb82dde19	security group for the nextwork VPC

sg-06eb6d7416549d2df - Mumbai-Private-SG1

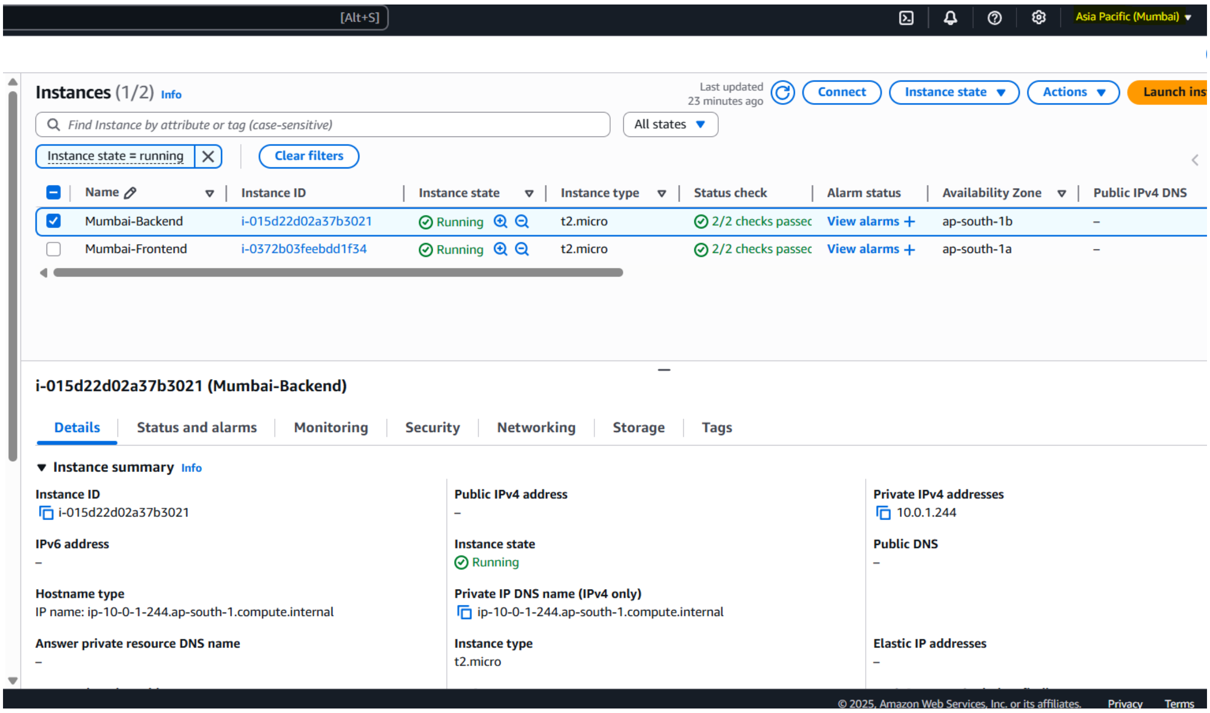
□	Name	Security group rule ID	IP version	Type	Protocol	Port range	Source
□	–	sgr-0b03fb4706b15c50f	IPv4	All ICMP - IPv4	ICMP	All	10.0.0.0/16
□	–	sgr-0514c43ae60fc400d	IPv4	SSH	TCP	22	10.0.0.0/16
□	–	sgr-071e875f101d467eb	IPv4	All ICMP - IPv4	ICMP	All	10.1.0.0/16
□	–	sgr-0e498712512d6408c	IPv4	SSH	TCP	22	10.1.0.0/16

5. EC2 Instance

An EC2 (Elastic Compute Cloud) instance is a virtual server provided by Amazon Web Services (AWS) that lets you run applications and workloads in the cloud.Deployed an EC2 instance in a public subnet with a configured Security Group, Network ACL, and Route Table to allow secure SSH and HTTP access while ensuring controlled inbound and outbound traffic flow.

Mumbai Region:

- Public instances have auto-assigned public IP
- Private instances are only reachable via public EC2 **(Bastion Host)** or VPC peering



Instances (1/2)

Last updated 23 minutes ago

Instance state = running

☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
☑	Mumbai-Backend	i-015d22d02a37b3021	✓ Running	t2.micro	✓ 2/2 checks passec	View alarms +	ap-south-1b	–
☐	Mumbai-Frontend	i-0372b03feebdd1f34	✓ Running	t2.micro	✓ 2/2 checks passec	View alarms +	ap-south-1a	–

i-015d22d02a37b3021 (Mumbai-Backend)

▼ Instance summary Info

Instance ID
i-015d22d02a37b3021

IPv6 address
–

Hostname type
IP name: ip-10-0-1-244.ap-south-1.compute.internal

Answer private resource DNS name
–

Public IPv4 address
–

Instance state
✓ Running

Private IP DNS name (IPv4 only)
ip-10-0-1-244.ap-south-1.compute.internal

Instance type
t2.micro

Private IPv4 addresses
10.0.1.244

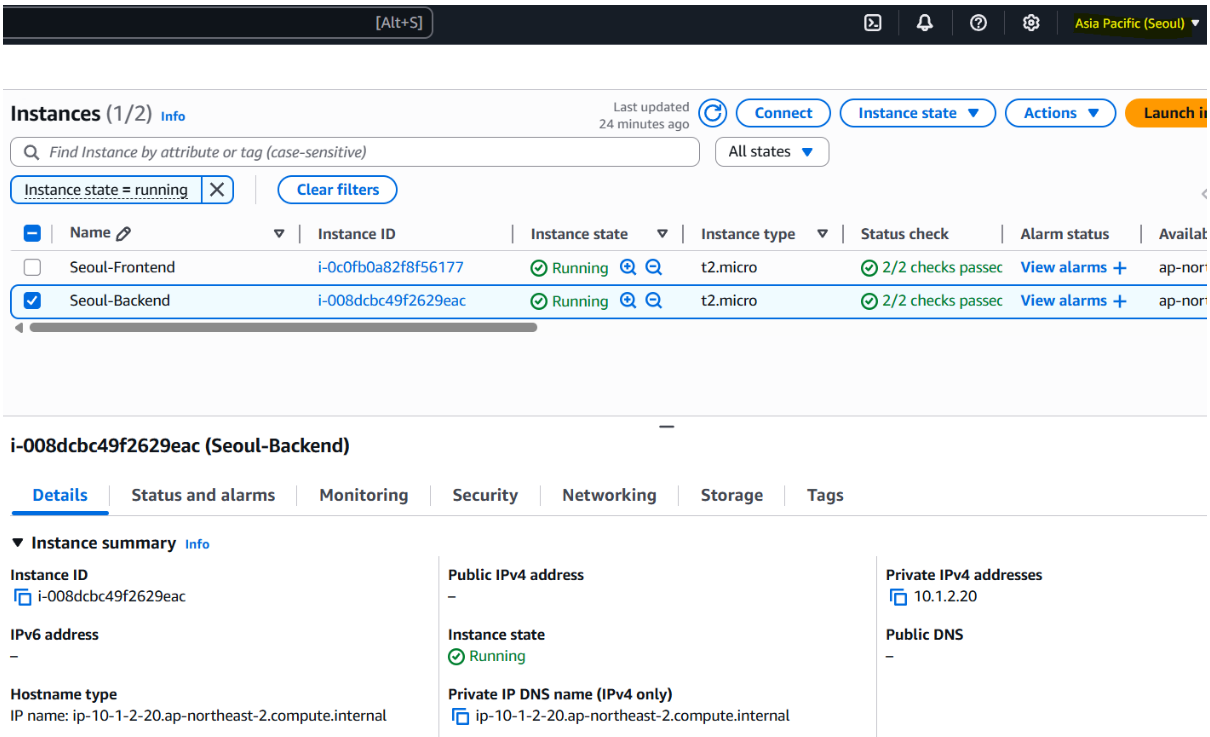
Public DNS
–

Elastic IP addresses
–

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

Seoul Region:

- Public instances have auto-assigned public IP
- Private instances are only reachable via public EC2 **(Bastion Host)** or VPC peering



Instances (1/2) Info

Last updated 24 minutes ago

Find Instance by attribute or tag (case-sensitive)

All states ▼

Instance state = running ✕

Clear filters

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availab
□	Seoul-Frontend	i-0c0fb0a82f8f56177	✓ Running	t2.micro	✓ 2/2 checks passec	View alarms +	ap-nor
☑	Seoul-Backend	i-008dcbc49f2629eac	✓ Running	t2.micro	✓ 2/2 checks passec	View alarms +	ap-nor

i-008dcbc49f2629eac (Seoul-Backend)

▼ Instance summary Info

Instance ID
i-008dcbc49f2629eac

Public IPv4 address
–

Private IPv4 addresses
10.1.2.20

IPv6 address
–

Instance state
✓ Running

Public DNS
–

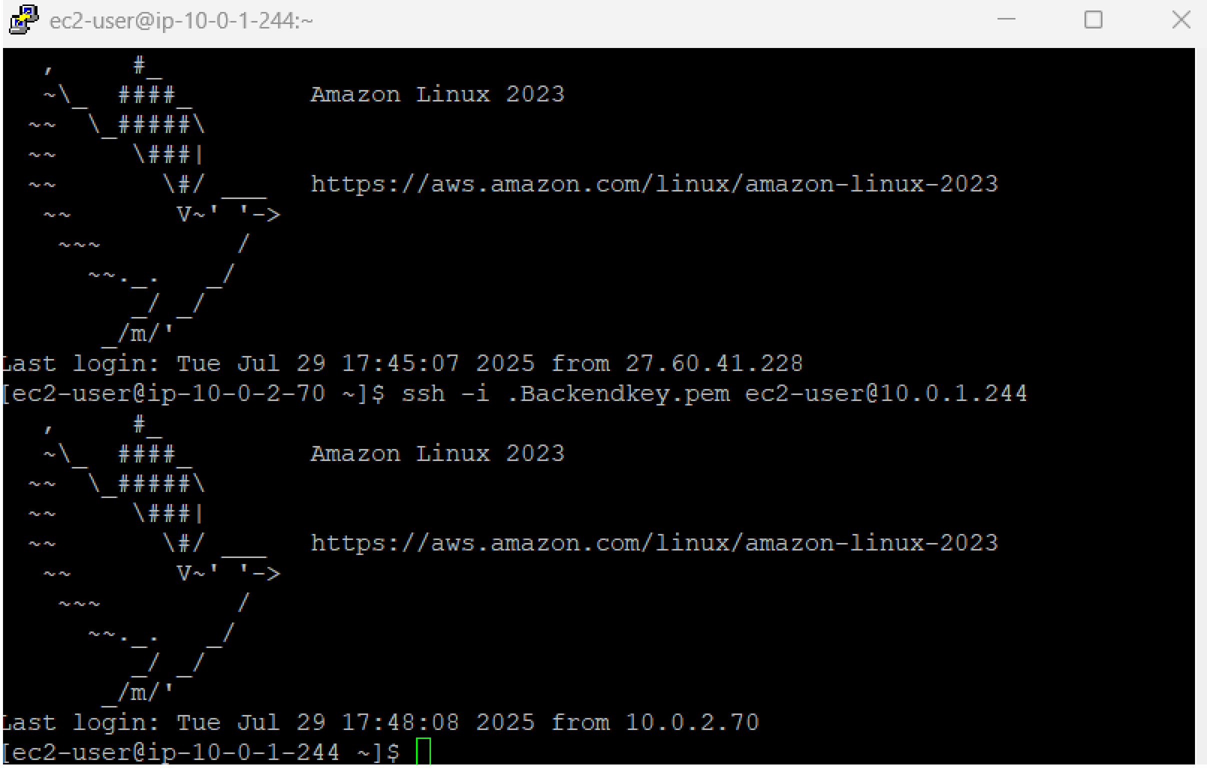
Hostname type
IP name: ip-10-1-2-20.ap-northeast-2.compute.internal

Private IP DNS name (IPv4 only)
ip-10-1-2-20.ap-northeast-2.compute.internal

6. Bastion Host (Jump Box)

A Bastion Host (also known as a Jump Box) is a special-purpose EC2 instance used to securely access private instances in a private subnet (inside a VPC) that do not have public IP addresses.

- Accessed private EC2s in both Mumbai and Seoul via internal IP
- Verified all EC2s were reachable over internal IP through ping and SSH

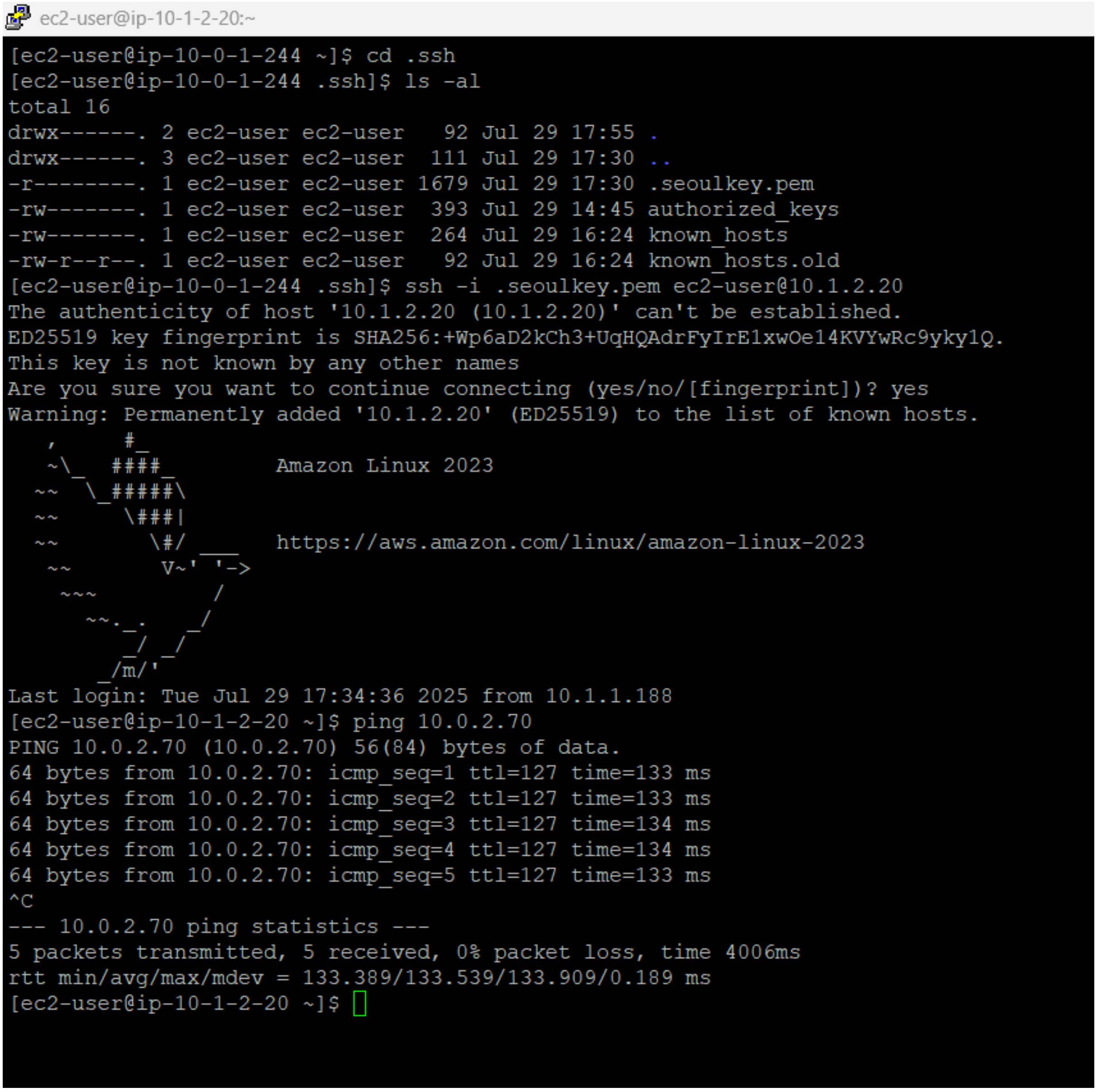


ec2-user@ip-10-0-1-244:~

```
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Tue Jul 29 17:45:07 2025 from 27.60.41.228
[ec2-user@ip-10-0-2-70 ~]$ ssh -i .Backendkey.pem ec2-user@10.0.1.244
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Tue Jul 29 17:48:08 2025 from 10.0.2.70
[ec2-user@ip-10-0-1-244 ~]$ 
```

Conclusion

In this project, successfully implemented cross-region VPC peering between two AWS regions — Mumbai and Seoul. The setup included properly configured public and private subnets, route tables, security groups, and EC2 instances. By using a bastion host, I ensured secure SSH access to private instances, and verified complete network connectivity using ping and internal IP communication. This architecture follows AWS best practices for secure and scalable VPC communication across regions.



```
[ec2-user@ip-10-0-1-244 ~]$ cd .ssh
[ec2-user@ip-10-0-1-244 .ssh]$ ls -al
total 16
drwx------. 2 ec2-user ec2-user   92 Jul 29 17:55 .
drwx------. 3 ec2-user ec2-user  111 Jul 29 17:30 ..
-r--------. 1 ec2-user ec2-user 1679 Jul 29 17:30 .seoulkey.pem
-rw-------. 1 ec2-user ec2-user  393 Jul 29 14:45 authorized_keys
-rw-------. 1 ec2-user ec2-user  264 Jul 29 16:24 known_hosts
-rw-r--r--. 1 ec2-user ec2-user   92 Jul 29 16:24 known_hosts.old
[ec2-user@ip-10-0-1-244 .ssh]$ ssh -i .seoulkey.pem ec2-user@10.1.2.20
The authenticity of host '10.1.2.20 (10.1.2.20)' can't be established.
ED25519 key fingerprint is SHA256:+Wp6aD2kCh3+UqHQAdrFyIrE1xwOe14KVYwRc9yky1Q.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.1.2.20' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Tue Jul 29 17:34:36 2025 from 10.1.1.188
[ec2-user@ip-10-1-2-20 ~]$ ping 10.0.2.70
PING 10.0.2.70 (10.0.2.70) 56(84) bytes of data.
64 bytes from 10.0.2.70: icmp_seq=1 ttl=127 time=133 ms
64 bytes from 10.0.2.70: icmp_seq=2 ttl=127 time=133 ms
64 bytes from 10.0.2.70: icmp_seq=3 ttl=127 time=134 ms
64 bytes from 10.0.2.70: icmp_seq=4 ttl=127 time=134 ms
64 bytes from 10.0.2.70: icmp_seq=5 ttl=127 time=133 ms
^C
--- 10.0.2.70 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 133.389/133.539/133.909/0.189 ms
[ec2-user@ip-10-1-2-20 ~]$ 
```