Cross-Account VPC Peering Through Transit Gateway in AWS

Executive Summary

This document outlines the implementation of secure, scalable connectivity between two AWS accounts using AWS Transit Gateway. The configuration enables seamless VPC-to-VPC communication across accounts.

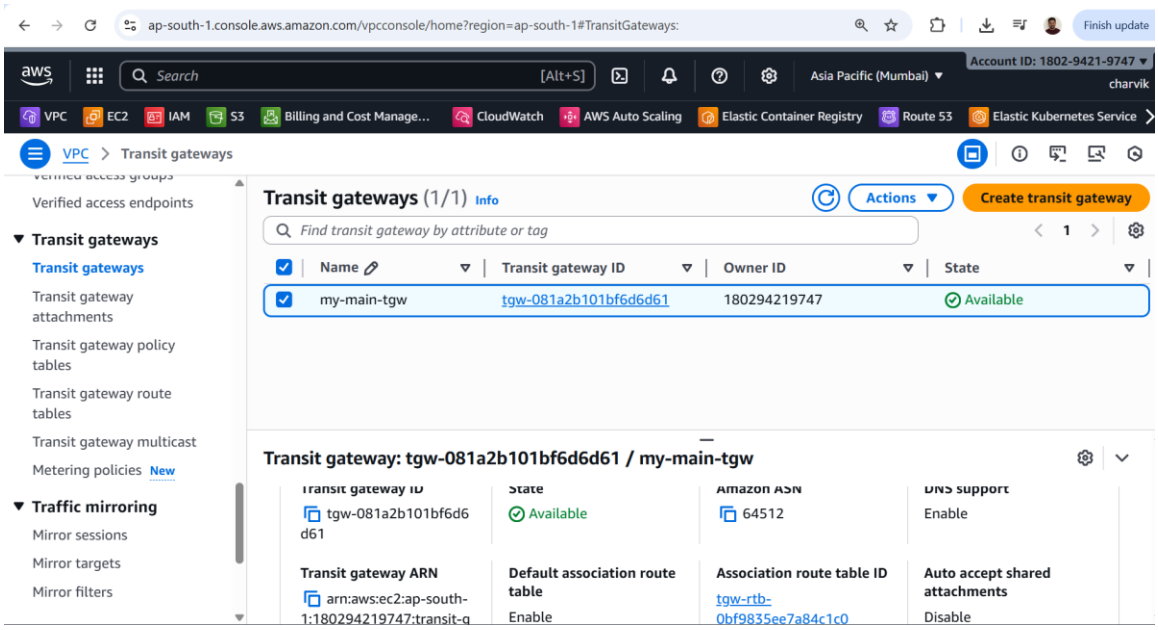
Environment Details

- Account A (Root Account): VPC-A (10.10.0.0/16)
- Account B (Dev Account): VPC-B (10.20.0.0/16)
- Transit Gateway shared from Account A → Account B
- EC2 instances placed in private subnets of each VPC.

Transit Gateway Creation (Account A)

Steps:

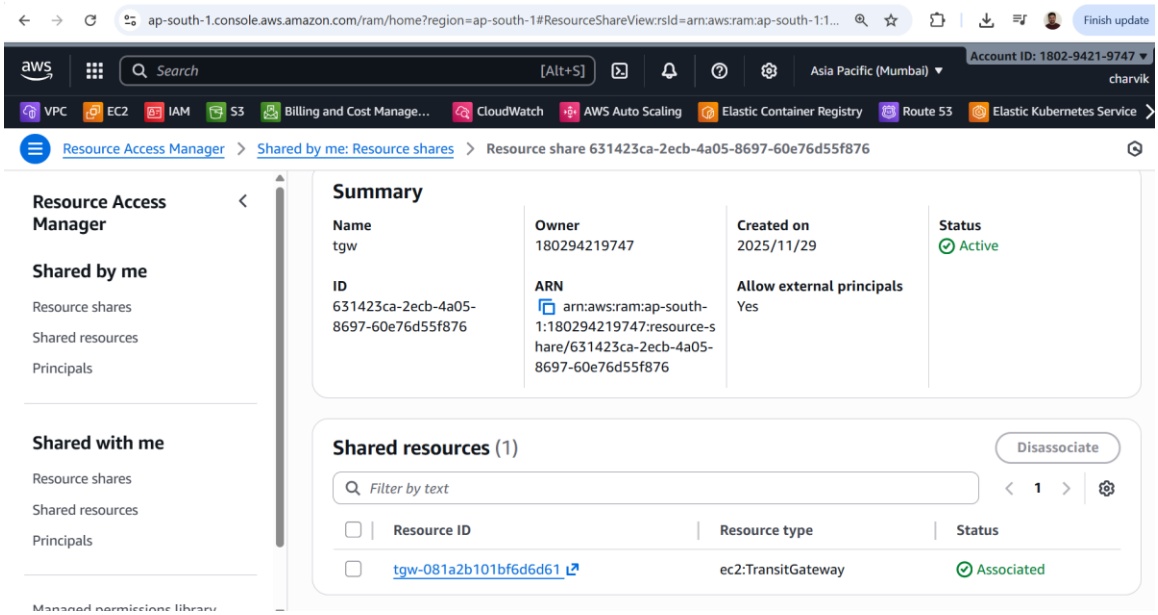
1. Navigate to VPC → Transit Gateways → Create TGW
2. Accept default settings or customize as per design

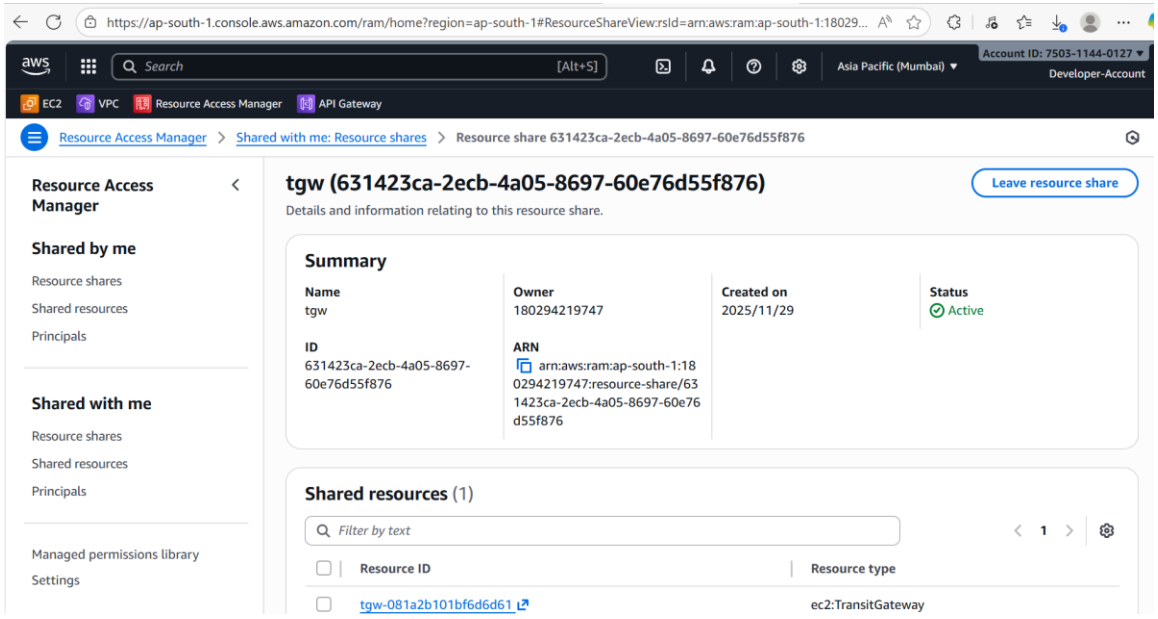


Resource Access Manager (RAM) Sharing

Steps:

1. Go to Resource Access Manager (RAM)
2. Create Resource Share → Add TGW
3. Add Account B as principal
4. Accept share from Account B

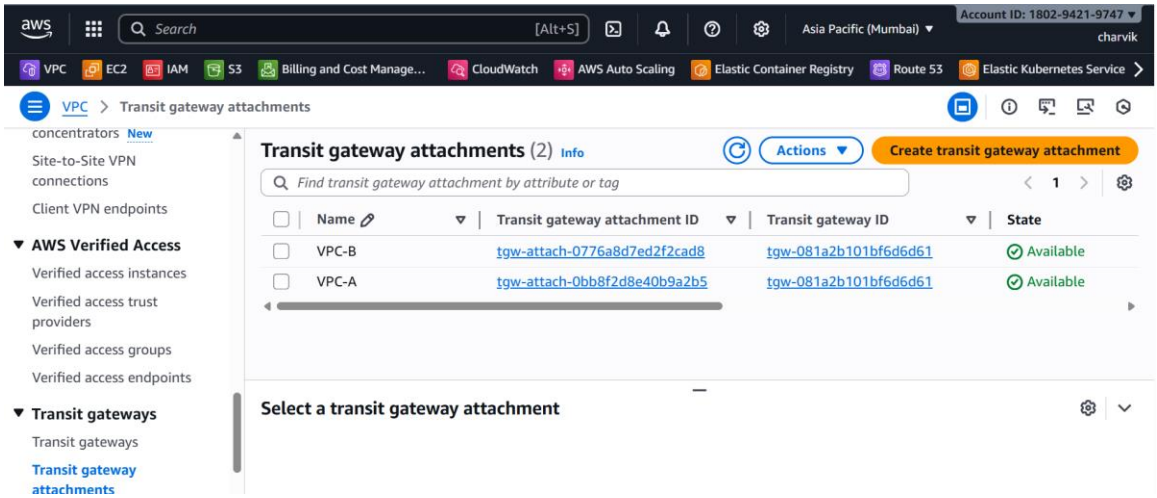


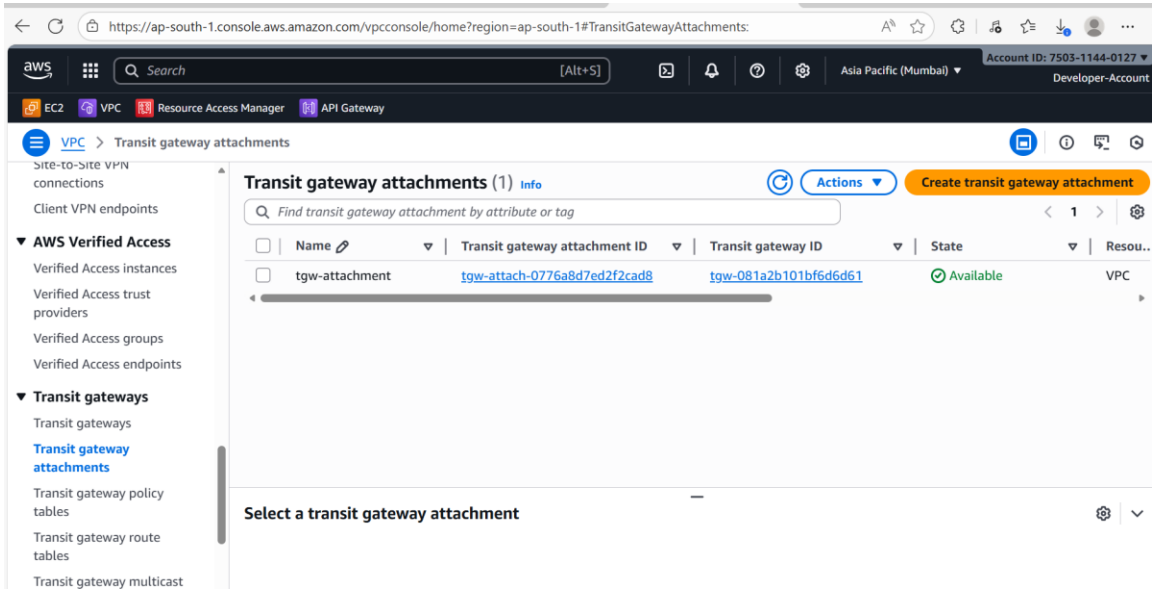


Transit Gateway Attachments

Steps:

1. Create VPC-A attachment in Account A
2. Create VPC-B attachment in Account B
3. Accept required attachments

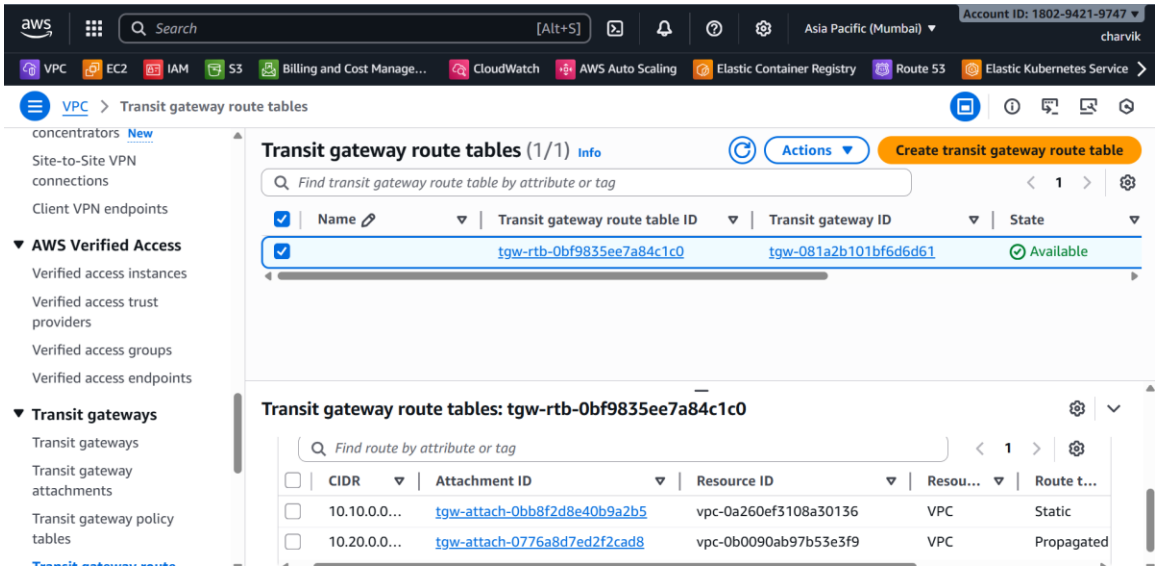




VPC Route Table Configuration

Each VPC Route Table must include:

- VPC-A → 10.20.0.0/16 → TGW
- VPC-B → 10.10.0.0/16 → TGW

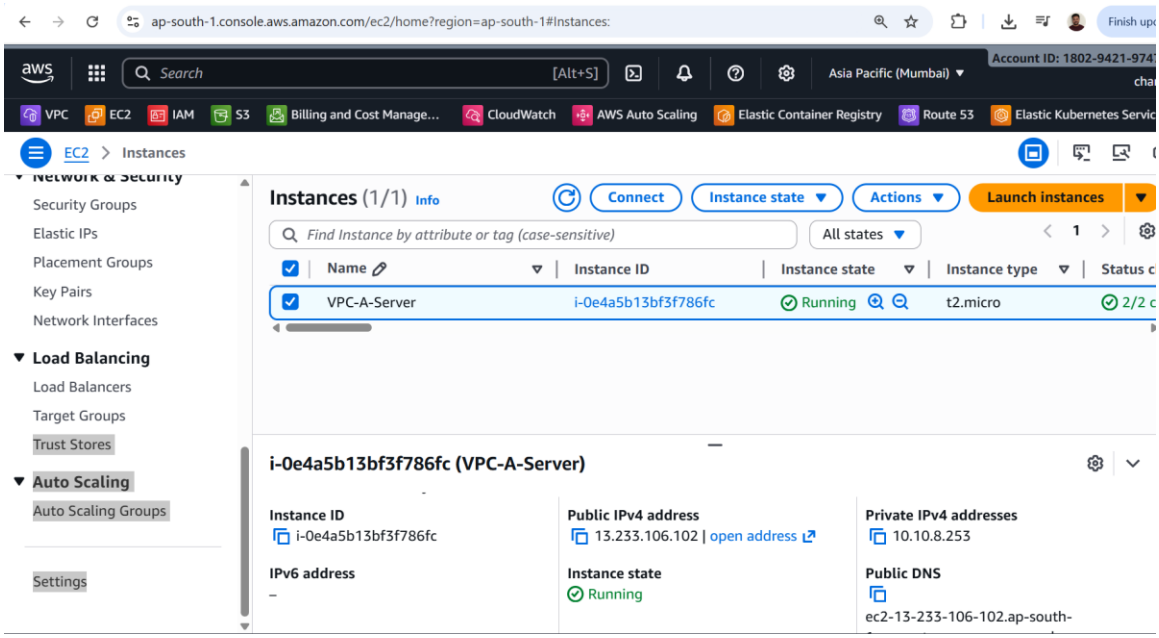


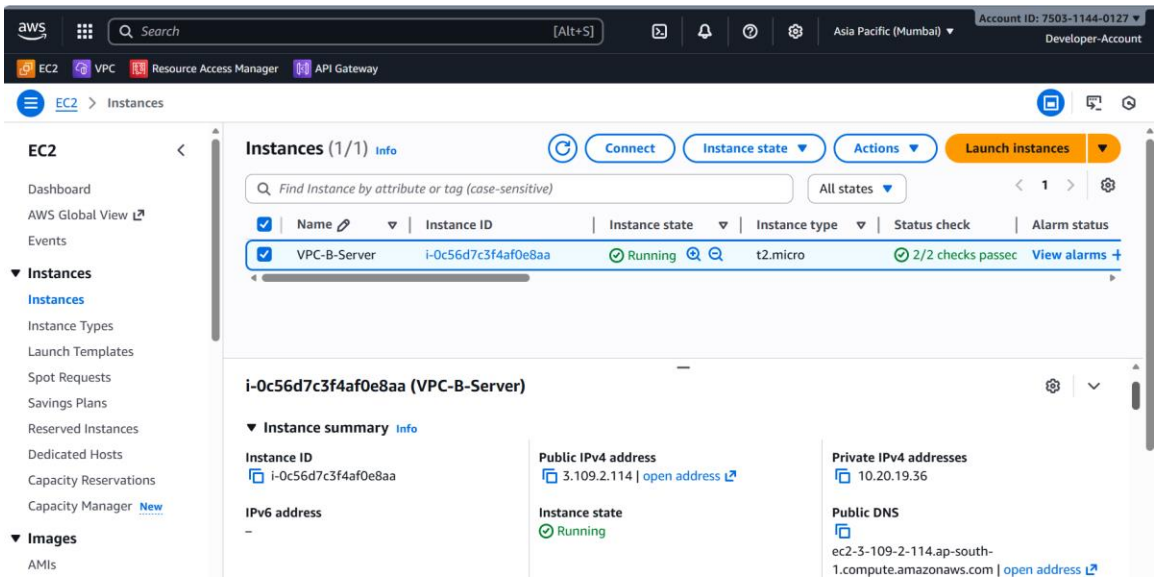
EC2 Deployment in Both VPCs

Launch EC2 instances in respective subnets.

Ensure:

- Correct VPC selection
- Security groups allow ICMP & SSH from the opposite CIDR





Connectivity Verification (Ping & SSH)

Validation tests:

- Ping VPC-A → VPC-B
- Ping VPC-B → VPC-A
- SSH from laptop into both EC2s
- SSH EC2-A → EC2-B and EC2-B → EC2-A

```
ubuntu@ip-10-10-8-253:~$ ping 10.20.19.36
PING 10.20.19.36 (10.20.19.36) 56(84) bytes of data.
64 bytes from 10.20.19.36: icmp_seq=1 ttl=63 time=1.46 ms
64 bytes from 10.20.19.36: icmp_seq=2 ttl=63 time=1.73 ms
64 bytes from 10.20.19.36: icmp_seq=3 ttl=63 time=1.07 ms
```

```
ubuntu@ip-10-10-8-253:~$ ssh -i tgw-key.pem ubuntu@10.20.19.36
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-1015-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sun Nov 30 02:56:02 UTC 2025

  System load:  0.0               Processes:             113
  Usage of /:   28.4% of 6.71GB   Users logged in:       1
  Memory usage: 22%               IPv4 address for enX0: 10.20.19.36
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Sun Nov 30 02:54:31 2025 from 49.37.169.142
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-20-19-36:~$
```

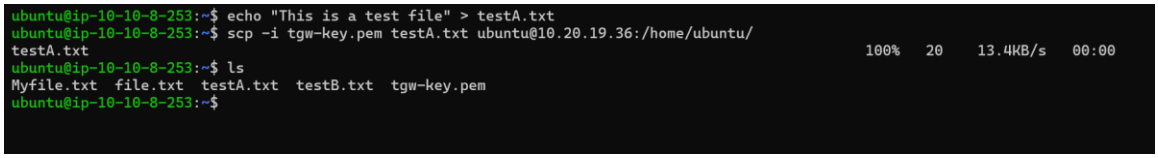
```
ubuntu@ip-10-20-19-36:~$ ping 10.10.8.253
PING 10.10.8.253 (10.10.8.253) 56(84) bytes of data.
64 bytes from 10.10.8.253: icmp_seq=1 ttl=63 time=1.59 ms
64 bytes from 10.10.8.253: icmp_seq=2 ttl=63 time=1.39 ms
64 bytes from 10.10.8.253: icmp_seq=3 ttl=63 time=0.885 ms
^C
--- 10.10.8.253 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.885/1.287/1.589/0.295 ms
ubuntu@ip-10-20-19-36:~$
```

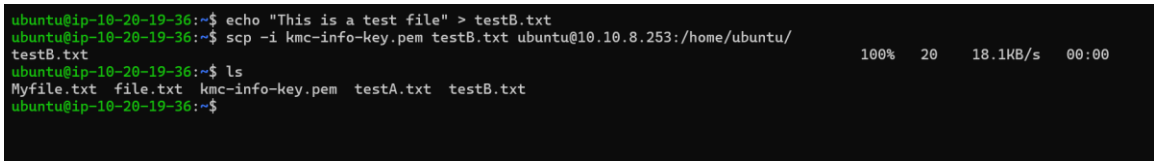
```
ubuntu@ip-10-20-19-36:~$ ssh -i kmc-info-key.pem ubuntu@10.10.8.253
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-1015-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sun Nov 30 03:00:53 UTC 2025

  System load:  0.0               Processes:             112
  Usage of /:   26.6% of 6.71GB   Users logged in:       1
  Memory usage: 21%               IPv4 address for enX0: 10.10.8.253
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Sun Nov 30 02:54:39 2025 from 49.37.169.142
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-10-8-253:~$
```

Internal EC2-to-EC2 File Transfer (SCP)

Examples:
EC2-A → EC2-B:
scp -i tgw-key.pem file.txt ubuntu@10.20.x.x:/home/ubuntu/

EC2-B → EC2-A:
scp -i kmc-info-key.pem file.txt ubuntu@10.10.x.x:/home/ubuntu/





Final Validation Checklist

✓ TGW Created
✓ Share Accepted by Account B
✓ Attachments in 'Available' state
✓ TGW Route Table configured
✓ VPC Routes configured
✓ Ping works both ways
✓ SSH works both ways
✓ SCP transfers successful

12. Conclusion

The cross-account TGW setup is fully functional and validated. Both VPCs are securely connected using a scalable hub-and-spoke architecture.