Module 9 – Transit Gateway

Transit Gateway with Site-Site VPN Setup.

It acts as a central hub that connects multiple virtual private clouds (VPCs), on-premises networks, and VPNs, enabling seamless communication between them.

So, in this practical again we will have three different regions which will behave like different AWS accounts.

US-EAST-1 – 192.168.255.0/24 – this will have VPN with Transit GW

Mumbai – 172.16.0.0/16 – VPN Client

Another AWS account – 192.168.254.0/24 – here we will see if we can ping US-EAST-1 instance via Transit GW.

So, let's start now.

First, we will configure all the services that are needed in US-EAST-1 region.

Step -1 VPC Setup

Step -2 VPC Setup for Mumbai region and install the Open Swan and configure it.

Step -3 Transit GW setup with VPN.

Step -4 Share the Transit GW with other AWS accounts.

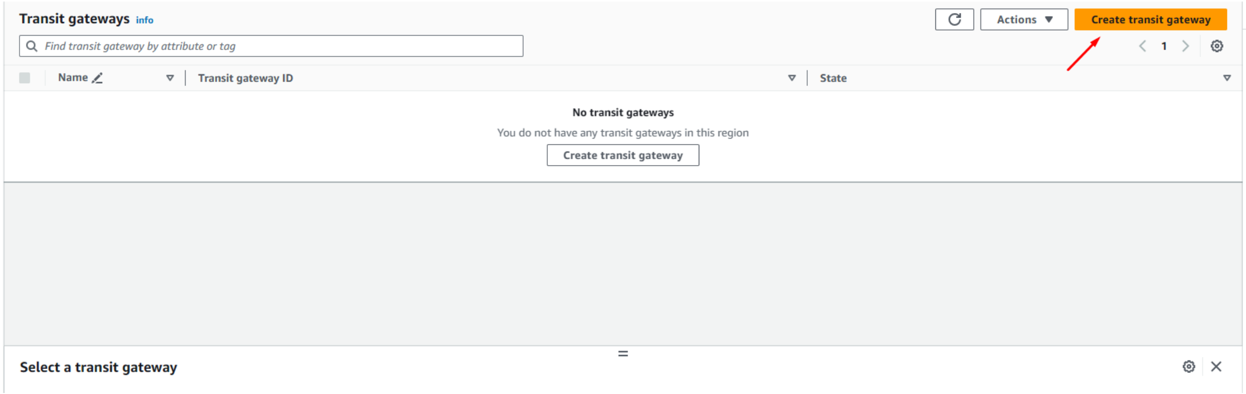
Step -5 VPC Setup in new AWS account.

Step -6 Transit GW Attachment in the AWS account.

Step – 7 Change the route table setting in US-EAST-1 and New AWS account.

Let's set up Transit GW first.

Click on Create transit gateway.



No transit gateways

You do not have any transit gateways in this region

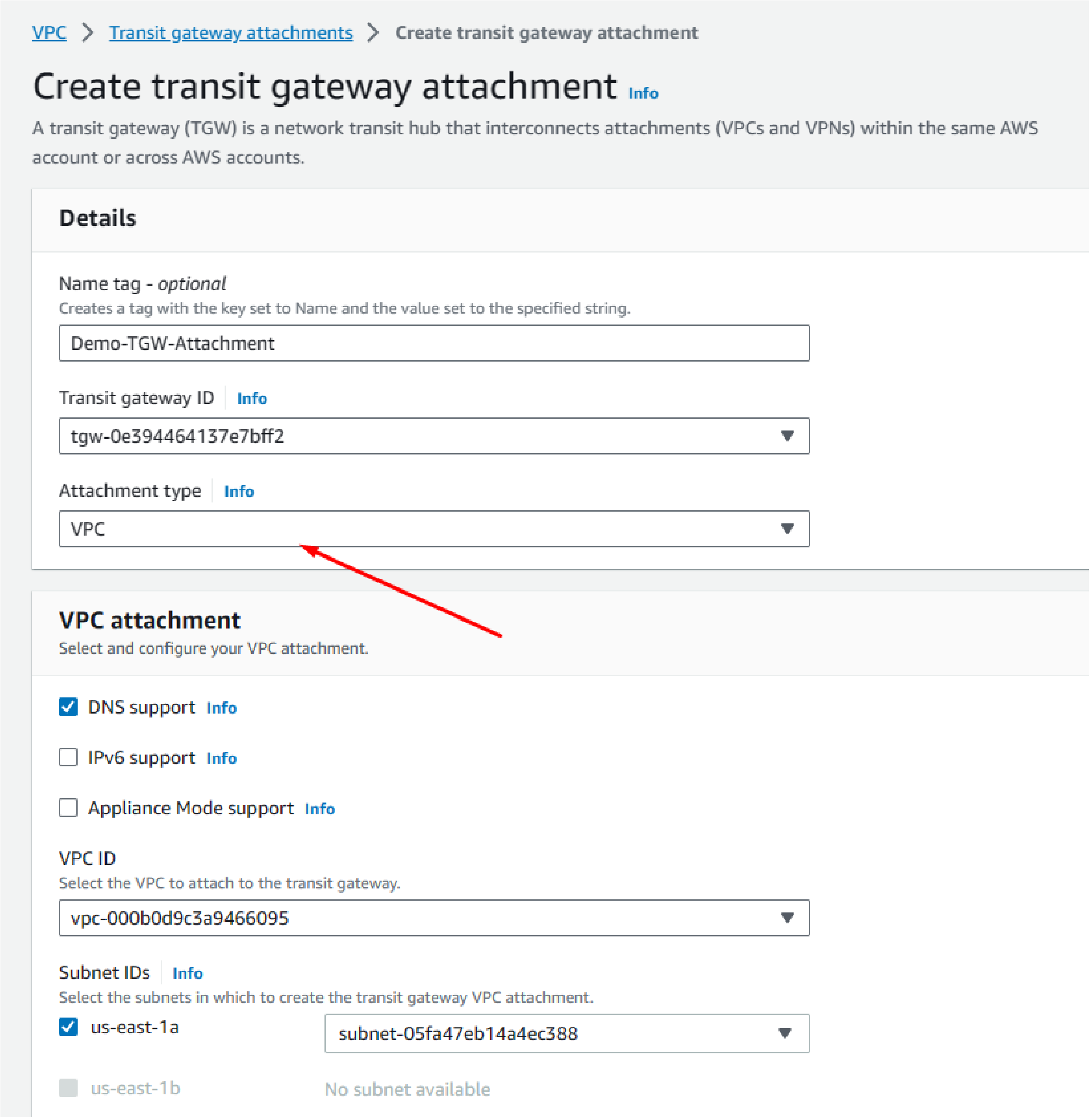
Fill in the details and keep the default setting and then click on create transit gateway.

Now create Customer Gateway.

Next step is to create the Site-Site VPN, make sure while creating the VPN we have to select Target Gateway as Transit Gateway.

Once the VPN is setup then configure OpenSwan.

Create Transit GW Attachment and attach to VPC, make sure to Select Attachment Type as VPC.



VPC > Transit gateway attachments > Create transit gateway attachment

Create transit gateway attachment Info

A transit gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same AWS account or across AWS accounts.

Details

Name tag - *optional*
Creates a tag with the key set to Name and the value set to the specified string.
Demo-TGW-Attachment

Transit gateway ID Info
tgw-0e394464137e7bff2 ▼

Attachment type Info
VPC ▼

VPC attachment
Select and configure your VPC attachment.

☑ DNS support Info

□ IPv6 support Info

□ Appliance Mode support Info

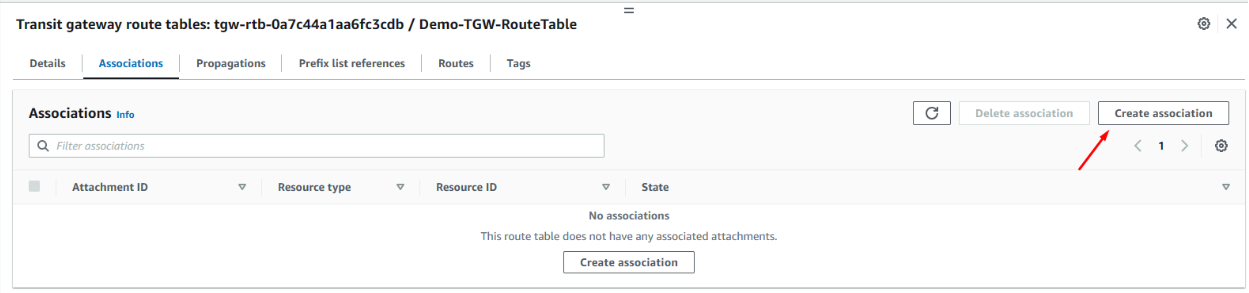
VPC ID
Select the VPC to attach to the transit gateway.
vpc-000b0d9c3a9466095 ▼

Subnet IDs Info
Select the subnets in which to create the transit gateway VPC attachment.

☑ us-east-1a	subnet-05fa47eb14a4ec388 ▼
□ us-east-1b	No subnet available

Next steps create Transit gateway route table.

Once the route table is created, then add Associations and Propagations.



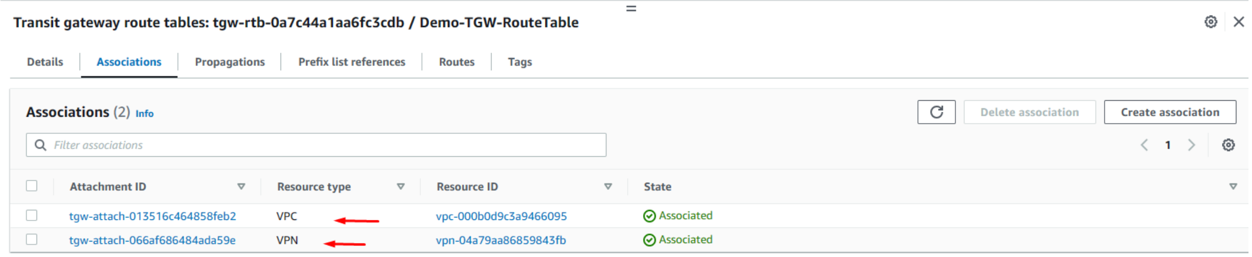
Transit gateway route tables: tgw-rtb-0a7c44a1aa6fc3cdb / Demo-TGW-RouteTable

Associations Info

□	Attachment ID	Resource type	Resource ID	State

No associations

This route table does not have any associated attachments.



Transit gateway route tables: tgw-rtb-0a7c44a1aa6fc3cdb / Demo-TGW-RouteTable

Associations (2) Info

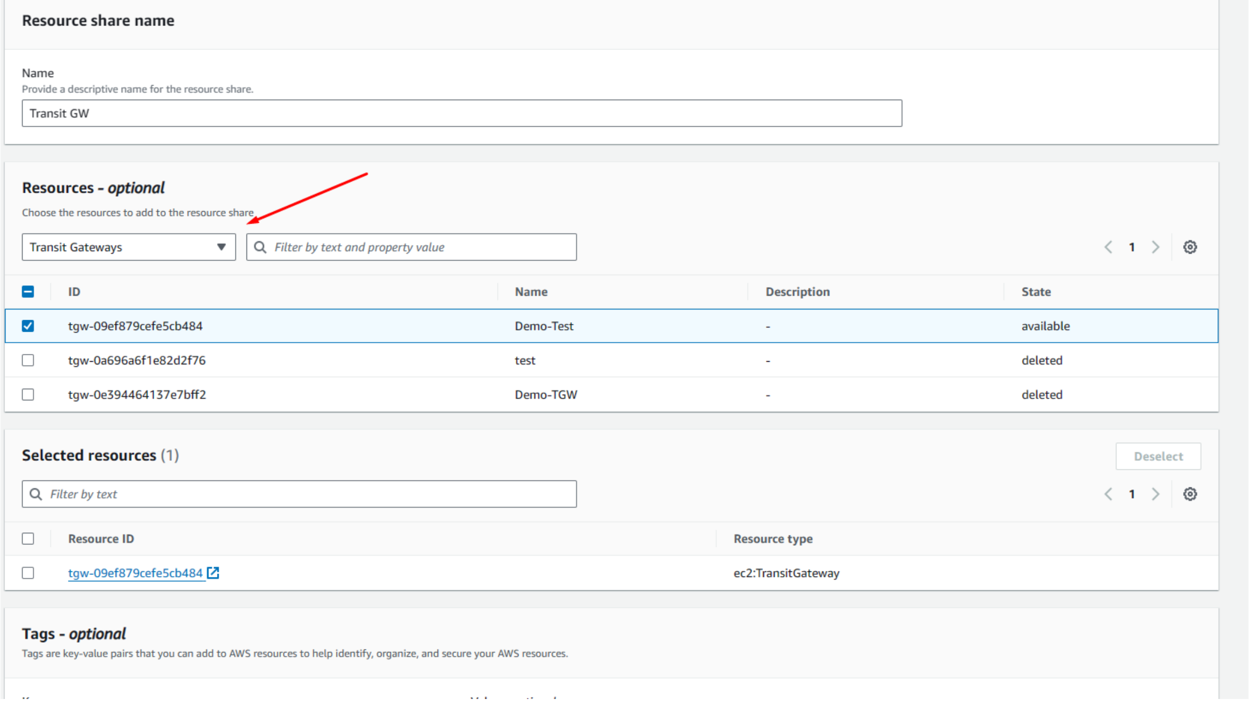
□	Attachment ID	Resource type	Resource ID	State
□	tgw-attach-013516c464858feb2	VPC	vpc-000b0d9c3a9466095	✓ Associated
□	tgw-attach-066af686484ada59e	VPN	vpn-04a79aa86859843fb	✓ Associated

Follow the same thing for propagation.

Then finally update the Route Table.

We have setup the Transit Gateway, now its time to share the Transit Gateway with Other AWS account, so that Spoke VPC can talk to On-Prem via a Transit Gateway.

Click on Share Transit GW.



Resource share name

Name

Provide a descriptive name for the resource share.

Transit GW

Resources - *optional*

Choose the resources to add to the resource share.

Transit Gateways ▼

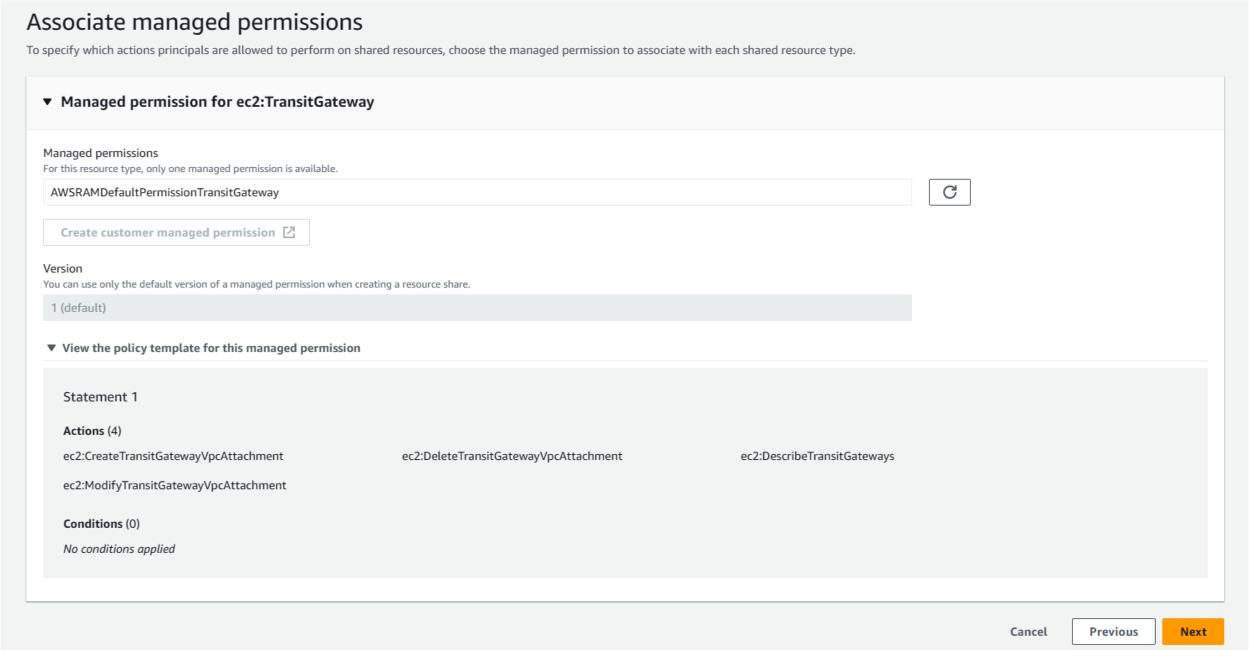
☑	ID	Name	Description	State
☑	tgw-09ef879cefe5cb484	Demo-Test	-	available
□	tgw-0a696a6f1e82d2f76	test	-	deleted
□	tgw-0e394464137e7bff2	Demo-TGW	-	deleted

Selected resources (1)

□	Resource ID	Resource type
□	tgw-09ef879cefe5cb484	ec2:TransitGateway

Tags - *optional*

Tags are key-value pairs that you can add to AWS resources to help identify, organize, and secure your AWS resources.



Associate managed permissions

To specify which actions principals are allowed to perform on shared resources, choose the managed permission to associate with each shared resource type.

▼ **Managed permission for ec2:TransitGateway**

Managed permissions
For this resource type, only one managed permission is available.
AWSRAMDefaultPermissionTransitGateway

Version
You can use only the default version of a managed permission when creating a resource share.
1 (default)

▼ **View the policy template for this managed permission**

Statement 1

Actions (4)

ec2:CreateTransitGatewayVpcAttachment
ec2:DeleteTransitGatewayVpcAttachment
ec2:DescribeTransitGateways
ec2:ModifyTransitGatewayVpcAttachment

Conditions (0)

No conditions applied

specify the AWS account number with whom you want to share.

Once it’s shared, go to the AWS account, and create the VPC attachment.