

CREATE THE VPC'S AND CONNECT THE THREE VPC'S USING TRANSIT GATEWAY

AWS announced this network resource during it's 2018 re:Invent conference. Simply put, a Transit Gateway is a simple mechanism that allows VPCs to communicate with each other. It also allows these VPCs to be connected to on-site networks via Direct Connect or VPN connections.

Table 1

If you've read any documentation about Transit Gateways, you'll learn about attachments, route tables, associations, and propagations. All of it may seem intimidating at first, but if you break it down by components, it may not seem so complex.

Here are the components that will be covered in the following sections:

- VPC Prerequisites and Organizations Trusted Access
- Creating the Transit Gateway
- Sharing the Transit Gateway using the Resource Access Manager
- Creating Transit Gateway Attachments

- Creating Transit Gateway Route Tables, Associations, and Propagations
- Using Direct Connect with Transit Gateway
- Using VPN to Transit Gateway
- Making VPC changes for Transit Gateway

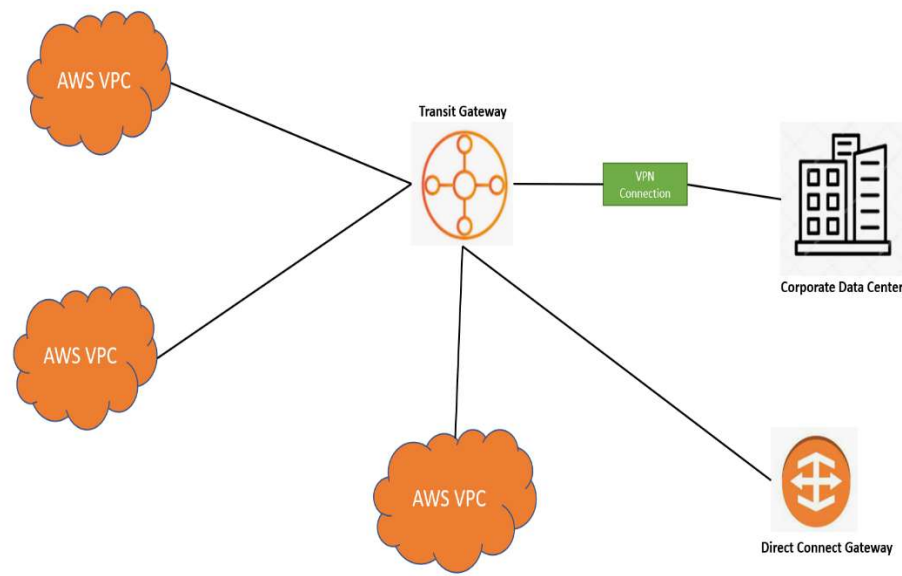
I won't get into the design decisions of using Transit Gateway versus designs using Transit VPC and/or VPC Peering, as there are other resources and blog postings that can help you make that determination. This series will assume that you want to move forward with a Transit Gateway solution.

In addition, all the instructions will be with the assumption that you are creating all the Transit Gateway resources via the web console. Although this helps better understand the concepts, I highly recommend that your Production-based solution uses an automated configuration approach, like using CloudFormation or Terraform. Our organization has coded our entire VPC and network infrastructure using Terraform, which is triggered by a Jenkins pipeline.

Here are assumptions about the implementation to be used:

- The Transit Gateway and all VPCs are in the same region.
- Each participating VPC will be in its own separate account.

- All accounts will be associated to each other using AWS Organizations.
- The Direct Connect connections will be dedicated, not hosted.



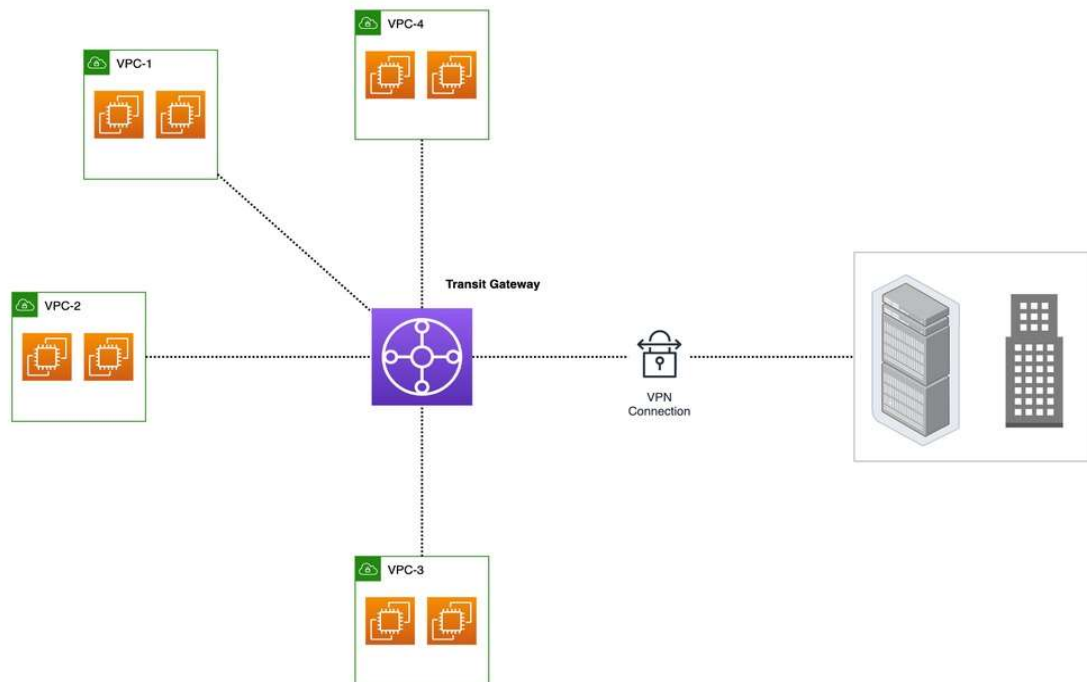
•

AWS announced this network resource during it's 2018 re:Invent conference. Simply put, a Transit Gateway is a simple mechanism that allows VPCs to communicate with each other. It also allows these VPCs to be connected to on-site networks via Direct Connect or VPN connections.

If you've read any documentation about Transit Gateways, you'll learn about attachments, route tables, associations, and propagations. All of it may seem intimidating at first, but if you break it down by components, it may not seem so complex.

Here are the components that will be covered in the following sections:

- VPC Prerequisites and Organizations Trusted Access
- Creating the Transit Gateway
- Sharing the Transit Gateway using the Resource Access Manager
- Creating Transit Gateway Attachments
- Creating Transit Gateway Route Tables, Associations, and Propagations
- Using Direct Connect with Transit Gateway
- Using VPN to Transit Gateway



- Making VPC changes for Transit Gateway

I won't get into the design decisions of using Transit Gateway versus designs using Transit VPC and/or VPC Peering, as there are other resources and blog postings that can help you make that determination. This series will assume that you want to move forward with a Transit Gateway solution.

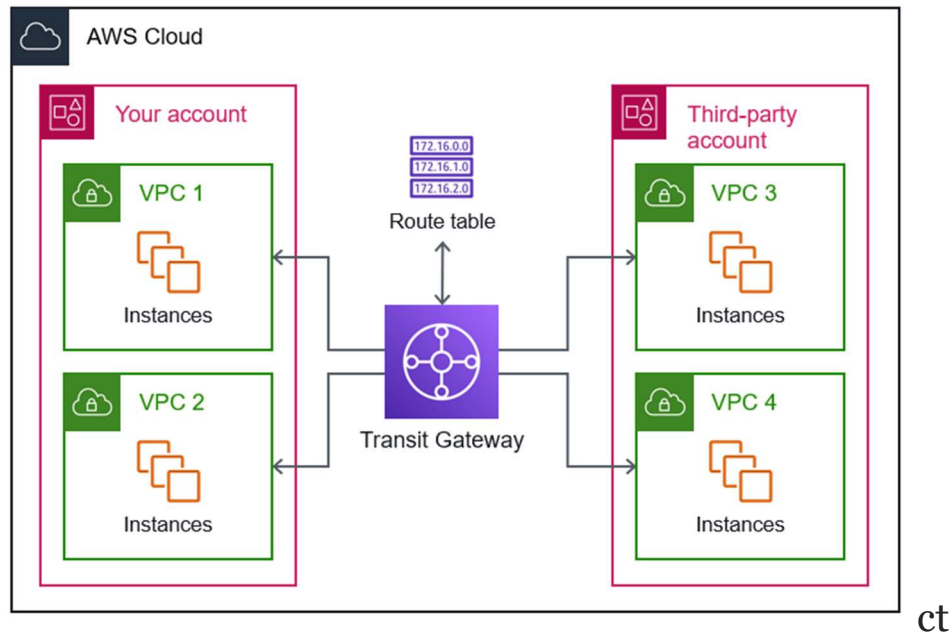
In addition, all the instructions will be with the assumption that you are creating all the Transit Gateway resources via the web console. Although this helps better understand the concepts, I highly

Recommend that your Production-based solution uses an automated configuration approach, like using CloudFormation or Terraform. Our organization has coded our entire VPC and network infrastructure using Terraform, which is triggered by a Jenkins pipeline.

Here are assumptions about the implementation to be used:

- The Transit Gateway and all VPCs are in the same region.
- Each participating VPC will be in its own separate account.
- All accounts will be associated to each other using AWS Organizations.

- The Direct Conne



connections will be dedicated, not hosted.

BENEFITS OF TRANSIT GATEWAY

- Simplified connectivity — AWS resources in geographically dispersed VPCs need access to a wide variety of on-prem or remote infrastructure. Now, you can connect all of your VPCs across thousands of AWS accounts and merge everything into a centrally-managed gateway.
- On-demand bandwidth — You can expand your network quickly to get the bandwidth requirements in order to transfer large amounts of data for your applications, to scale edge devices, or to enable your migration to the cloud.