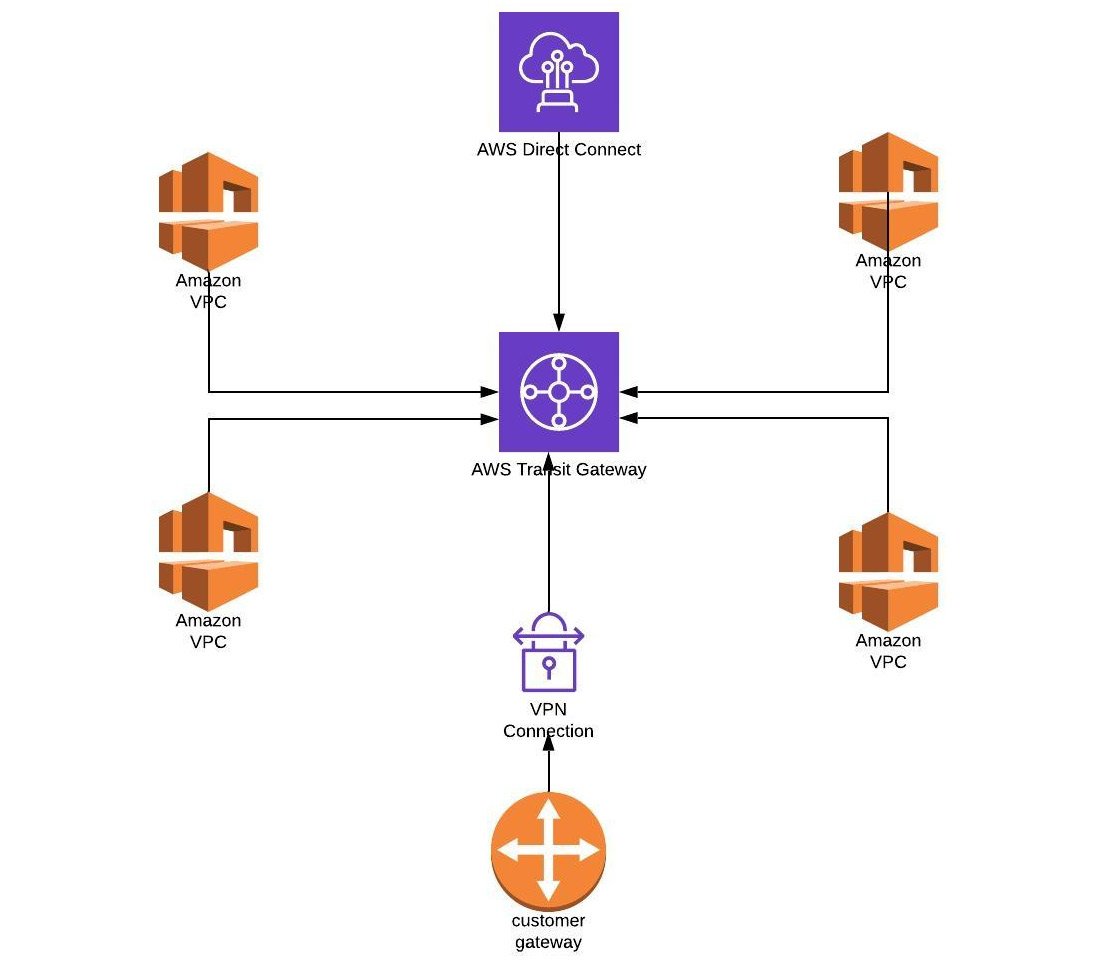
www

Assignment Documentation on AWS Transit Gateway Vs VPC Peering

Ritesh

Dated: 21-12-2022

**AWS Transit Gateway**



**What is a Transit Gateway?**

* A transit gateway is a network transit hub
* AWS Transit gateway connects VPCs and on-premises network through central hub
* This simplifies your network and puts an end to complex peering relationship it acts as a cloud router-each new connection is only made once
* Your data is automatically encrypted and never travels over the public internet.
* Inter Region peering connects AWS Transit Gateway together using AWS global network.

A transit gateway is a network transit hub that you can use to interconnect your virtual private clouds (VPCs) and on-premises networks. As your cloud infrastructure expands globally, inter-Region peering connects transit gateways together using the AWS Global Infrastructure.

* AWS Transit Gateway connects your Amazon Virtual Private Clouds (VPCs) and on-premises networks through a central hub.
* This connection simplifies your network and puts an end to complex peering relationships.
* Transit Gateway acts as a highly scalable cloud router—each new connection is made only once.
* AWS Transit Gateway helps you design and implement networks at scale by acting as a cloud router.
* As your network grows, the complexity of managing incremental connections can slow you down.
* AWS Transit Gateway connects VPCs and on-premises networks through a central hub.

**Benefits**

* It acts a Cloud router.
* With AWS Transit Gateway Network Manager, you can easily monitor your amazon VPCs and edge connection from a central console.
* Traffic between an Amazon VPC and AWS Transit Gateway remains on the AWS global private network and It’s not expose to the public internet.

**Advantages of AWS Transit Gateway**

* Allows for more VPCs per region compared to VPC peering
* Better visibility (network manager, CloudWatch metrics, and flow logs) compared to VPC peering
* TGW Route Tables per attachment allow for fine-grained routing
* Complexity is based on region count

**Disadvantages of AWS Transit Gateway**

* Additional hop (hop is **an intermediate connection in a string of connections linking two devices**.) will introduce some latency.
* Potential bottlenecks around regional peering links.
* Priced on hourly cost per attachment, data processing, and data transfer.

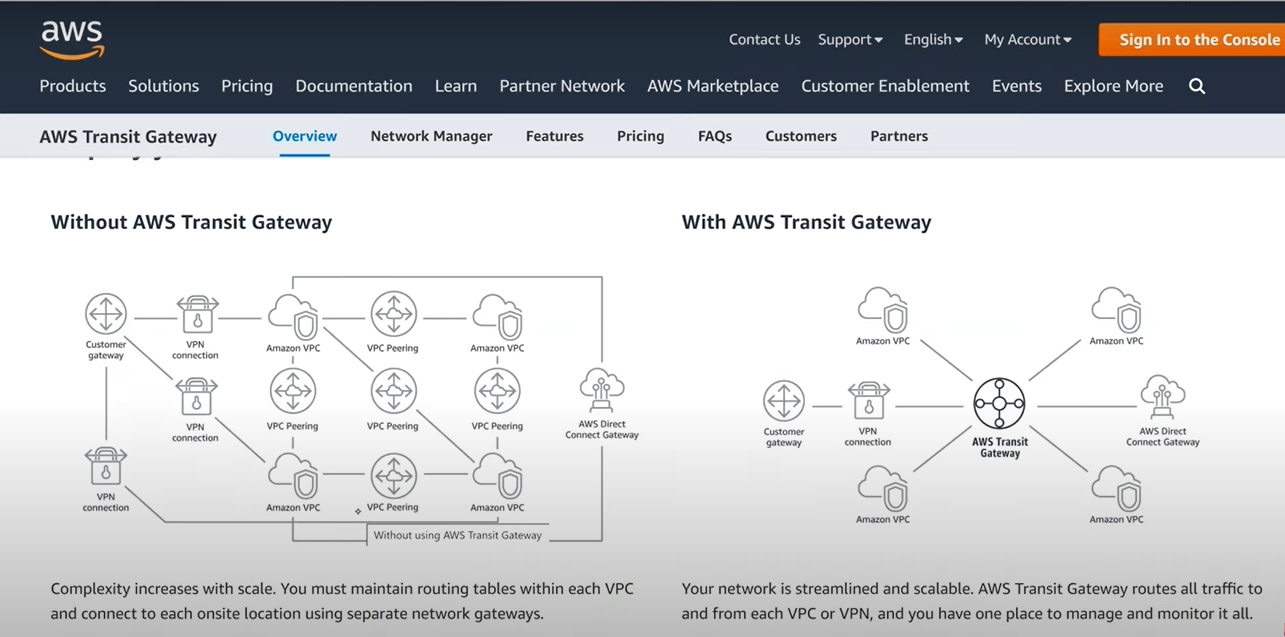
**Transit Gateway Concepts**

* **Attachments** — You can attach the following:
  + One or more VPCs
  + An AWS Direct Connect gateway
  + A peering connection with another transit gateway
  + A VPN connection to a transit gateway
* **Transit gateway route table** — A transit gateway has a default route table and can optionally have additional route tables. A route table includes dynamic and static routes that decide the next hop based on the destination IP address of the packet. The target of these routes could be any transit gateway attachment. By default, transit gateway attachments are associated with the default transit gateway route table.
* **Associations** — Each attachment is associated with exactly one route table. Each route table can be associated with zero to many attachments.
* **Route propagation** — A VPC, VPN connection, or Direct Connect gateway can dynamically propagate routes to a transit gateway route table. With a Connect attachment, the routes are propagated to a transit gateway route table by default. With a VPC, you must create static routes to send traffic to the transit gateway. With a VPN connection or a Direct Connect gateway, routes are propagated from the transit gateway to your on-premises router using Border Gateway Protocol (BGP). With a peering attachment, you must create a static route in the transit gateway route table to point to the peering attachment.

**Transit gateways working**

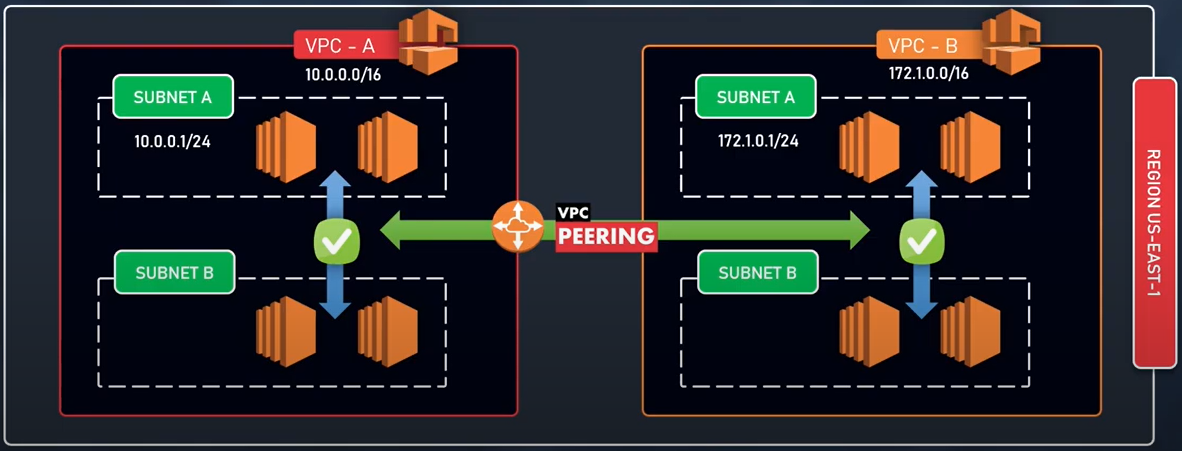
You can create, access, and manage your transit gateways using any of the following interfaces:

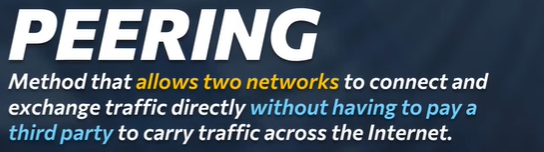
* **AWS Management Console** — Provides a web interface that you can use to access your transit gateways.
* **AWS Command Line Interface (AWS CLI)** — Provides commands for a broad set of AWS services, including Amazon VPC, and is supported on Windows, macOS, and Linux. For more information.



**AWS VPC Peering**

A VPC Peering connection is a networking connection between two VPCs that enable you to route traffic between them using private IPV4 addresses or IPV6 addresses



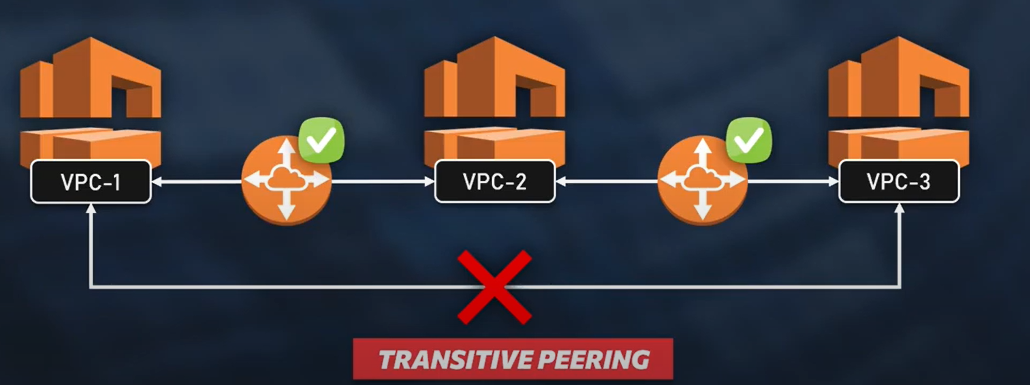
AWS uses the existing infrastructure of a VPC to create a VPC peering connection:

* Sharing data across accounts become easier.
* Sharing data across instance across vpc becomes easier.
* We can establish peering relationship between VPCs across different AWS Regions (also called Inter-Region VPC Peering)
* Can communicate with EC2, RDS, Lambda without needing:
* Gateways
* VPN connections
* Separate network appliances.
* All traffics remains in the Private IP space.

**MULTIPLE VPC PEERING CONNECTION**

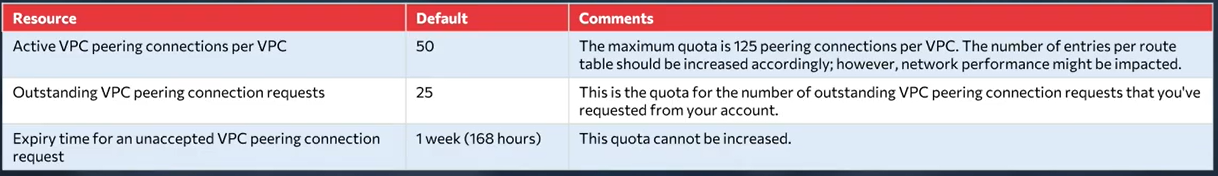
It is a One -To- One relationship between 2VPC.

There is no support for TRANSITIVE relationships or connections.



**VPC** PEERING (Points to Remember)

1. You cannot create a VPC peering connection between VPCs that have matching or overlapping IPV4 or IPV6 CIDR blocks.



1. VPC peering does not support transitive peering relationships.
2. You cannot have more than one VPC peering connection between the same two VPCs at the same time.
3. Any tags that you create for your VPC peering connection are only applied in the account or region in which you create them.
4. You cannot connect to or query the Amazon DNS server in peer VPC.

