AWS TRANSIT GATEWAY AND PEERING

AWS TG

Presented By
SHUBHAM

OOGLELABS

What is AWS transit gateway?

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.

Connect Amazon VPCs, AWS accounts, and on-premises networks to a single gateway

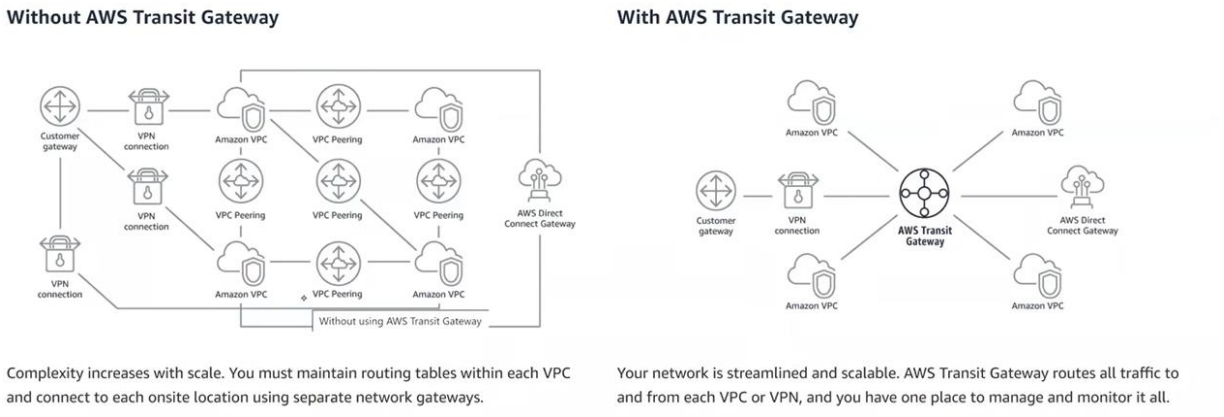
- A transit gateway is a network transit hub
- AWS Transit Gateway connects VPCs and on-premises networks through a central hub
- This simplifies your network and puts an end to complex peering relationships. It acts as a cloud router - each new connection is only made once
- A transit gateway scales elastically based on the volume of network traffic
- Your data is automatically encrypted and never travels over the public internet
- Inter-regional peering connects AWS Transit Gateways together using the AWS global network.
- Routing through a transit gateway operates at layer 3 (OSI Model), where the packets are sent to a specific next-hop attachment, based on their destination IP addresses

How it works

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.

Why AWS Transit Gateway?

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.



What is the difference between VPC peering and transit gateway?

TGWs across different regions can peer with each other to enable VPC communications across regions. Each spoke VPC only needs to connect to the TGW to gain access to other connected VPCs. provides simpler VPC-to-VPC communication management over VPC Peering with a large number of VPCs.

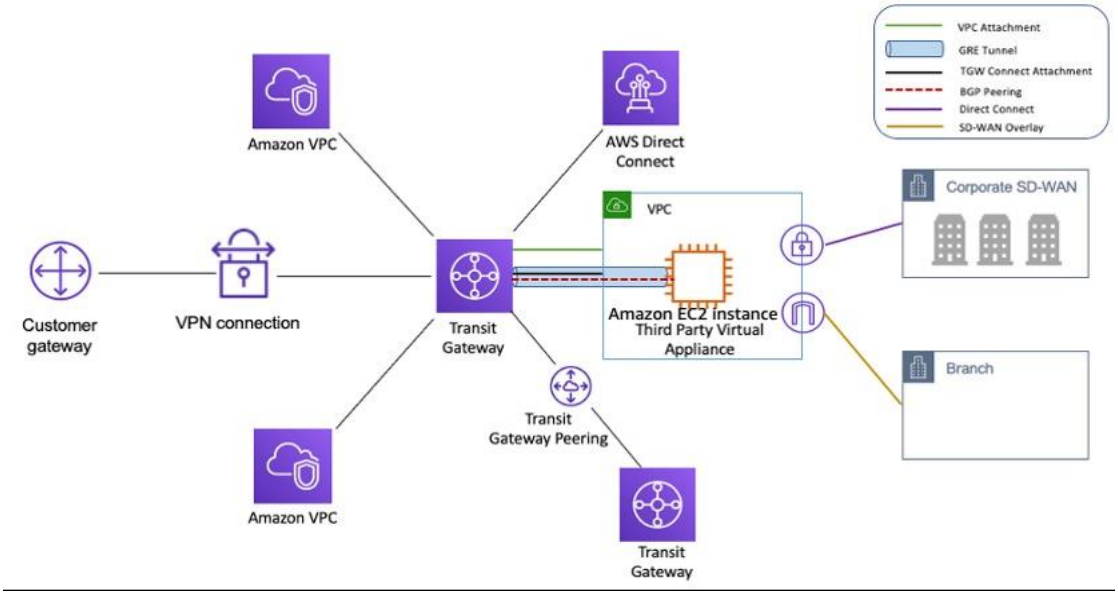
Work with transit gateways

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, see AWS Command Line Interface.
- AWS SDKs — Provides language-specific API operations and takes care of many of the connection details, such as calculating signatures, handling request retries, and handling errors. For more information, see AWS SDKs.
- Query API — Provides low-level API actions that you call using HTTPS requests. Using the Query API is the most direct way to access Amazon VPC, but it requires that your application handle low-level details such as generating the hash to sign the request, and handling errors. For more information, see the Amazon EC2 API Reference.

AWS Transit Gateway – TGW

- AWS Transit Gateway – TGW is a highly available and scalable service to consolidate the AWS VPC routing configuration for a region with a hub-and-spoke architecture.
- acts as a Regional virtual router and is a network transit hub that can be used to interconnect VPCs and on-premises networks.
- traffic always stays on the global AWS backbone, data is automatically encrypted, and never traverses the public internet, thereby reducing threat vectors, such as common exploits and DDoS attacks.
- is a regional resource and can connect VPCs within the same AWS Region.
- TGWs across different regions can peer with each other to enable VPC communications across regions.
- Each spoke VPC only needs to connect to the TGW to gain access to other connected VPCs.
- provides simpler VPC-to-VPC communication management over VPC Peering with a large number of VPCs.
- scales elastically based on the volume of network traffic.
- TGW routing operates at layer 3, where the packets are sent to a specific next-hop attachment, based on their destination IP addresses.
- AWS Resource Access Manager – RAM can be used to share the TGW with other accounts.



Transit Gateway Attachments

- Transit Gateway attachment is the connection between resources like VPC, VPN, Direct Connect, and the TGW.
- YGW attachment is both a source and a destination of packets.
- TGW supports the following attachments

1. One or more VPCs
2. One or more VPN connections
3. One or more AWS Direct Connect Gateways
4. One or more Transit Gateway Connect attachments
5. One or more Transit Gateway peering connections
6. One of more Connect SD-WAN/third-party network appliance

Transit Gateway Routing

- Transit Gateway routes IPv4 and IPv6 packets between attachments using transit gateway route tables.
- Route tables can be configured to propagate routes from the route tables for the attached VPCs, VPN connections, and Direct Connect gateways.
- When a packet comes from one attachment, it is routed to another attachment using the route that matches the destination IP address.
- VPC attached to a TGW must be added a route to the subnet route table in order for traffic to route through the TGW.

Transit Gateway Peering

- AWS Transit Gateway supports the ability to establish peering connections between Transit Gateways in the same and different AWS Regions.
- Inter-region peering enables customers to extend this connectivity and build global networks spanning multiple AWS Regions.
- Intra-region peering simplifies routing and inter-connectivity between VPCs and on-premises networks that are serviced and managed via separate Transit Gateways
- Traffic using inter-region Transit Gateway peering always stays on the AWS global network and never traverses the public internet, thereby reducing threat vectors, such as common exploits and DDoS attacks.
- Inter-region Transit Gateway peering encrypts inter-region traffic with no single point of failure.

Transit Gateway High Availability

- Transit Gateway must be enabled with multiple AZs to ensure availability and to route traffic to the resources in the VPC subnets.
- AZ can be enabled by specifying exactly one subnet within the AZ
- TGW places a network interface in that subnet using one IP address from the subnet.
- TGW can route traffic to all the subnets and not just the specified subnet within the enabled AZ.
- Resources that reside in AZs where there is no TGW attachment cannot reach the TGW.

Transit Gateway Appliance Mode

- For stateful network appliances in the VPC, appliance mode support for the VPC attachment can be enabled in which the appliance is located.
- Appliance Mode ensures that network flows are symmetrically routed to the same AZ and network appliance
- Appliance Mode ensures that the same AZ for that VPC attachment is used for the lifetime of a flow of traffic between source and destination.
- Appliance Mode also allows the TGW to send traffic to any AZ in the VPC, as long as there is a subnet association in that zone.

Transit Gateway Connect Attachment

- Transit Gateway Connect attachment can help establish a connection between a TGW and third-party virtual appliances (such as SD-WAN appliances) running in a VPC.
- A Connect attachment supports the Generic Routing Encapsulation (GRE) tunnel protocol for high performance and Border Gateway Protocol (BGP) for dynamic routing.

Transit Gateway Network Manager

- AWS Transit Gateway Network Manager provides a single global view of the private network.
- includes events and metrics to monitor the quality of the global network, both in AWS and on-premises.
- Event alerts specify changes in the topology, routing, and connection status. Usage metrics provide information on up/down connection, bytes in/out, packets in/out, and packets dropped. seamlessly integrates with SD-WAN solutions

Transit Gateway Best Practices

- Use a separate subnet for each transit gateway VPC attachment.
- Create one network ACL and associate it with all of the subnets that are associated with the TGW. Keep the network ACL open in both the inbound and outbound directions.
- Associate the same VPC route table with all of the subnets that are associated with the YGW, unless your network design requires multiple VPC route tables (for example, a middle-box VPC that routes traffic through multiple NAT gateways).
- Use BGP Site-to-Site VPN connections, if the customer gateway device or firewall for the connection supports multipath, enable the feature.
- Enable route propagation for AWS Direct Connect gateway attachments and BGP Site-to-Site VPN attachments.
- are highly available by design and do not need additional TGWs for high availability,
- Limit the number of TGW route tables unless your design requires multiple transit gateway route tables.
- For redundancy, use a single TGW in each Region for disaster recovery.
- For deployments with multiple TGWs, it is recommended to use a unique ASN for each of them.
- supports intra-Region peering.

Transit Gateway vs Transit VPC vs VPC Peering

VPC Peering vs Transit VPC vs Transit Gateway

Criteria	VPC Peering	Transit VPC	Transit Gateway
Architecture	Full mesh - One to One mapping	VPN-based hub-and-spoke	Attachments-based hub-and-spoke. Can be peered with other TGWs.
Hybrid Connectivity	Not Supported - Only VPC to VPC	Supported	Supported
Complexity	Increases with VPC count	Customer needs to maintain EC2 instance/HA	AWS managed service; increases with Transit Gateway count
Transitive Routing	Not Supported	Supported	Supported
Scale	125 active Peers/VPC (keeps on changing)	Depends on virtual router/EC2	5000 attachments per Region
Segmentation	Security groups	Customer managed	Transit Gateway route tables
Latency	Lowest	Extra, due to VPN encryption overhead	Additional Transit Gateway hop
Bandwidth limit	No limit	Subject to EC2 instance bandwidth limits based on size/family	Up to 50 Gbps (burst)/attachment
Visibility	VPC Flow Logs	VPC Flow Logs and CloudWatch Metrics	Transit Gateway Network Manager, VPC Flow Logs, CloudWatch Metrics
Cross-referencing Security group	Supported	Not supported	Not supported
Cost	Data transfer	EC2 hourly cost, VPN tunnels cost and data transfer	Hourly per attachment, data processing, and data transfer

Attachments — You can attach the following:

- One or more VPCs
- A Connect SD-WAN/third-party network appliance
- An AWS Direct Connect gateway
- A peering connection with another transit gateway
- A VPN connection to a transit gateway

Transit gateway Maximum Transmission Unit (MTU) —

The largest permissible packet that can be passed over the connection in bytes. The larger the MTU of a connection, the more data that can be passed in a single packet

A transit gateway supports an MTU of 8500 bytes for traffic between VPCs, AWS Direct Connect, Transit Gateway Connect, and peering attachments. Traffic over VPN connections can have an MTU of 1500 bytes

Transit gateway route table —

- A transit gateway has a default route table and can optionally have additional route tables. 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
- Acts as a cloud router
- with AWS Transit Gateway Network Manager, you can easily monitor your Amazon VPCs and edge connections from a central console

- Traffic between an Amazon VPC and AWS Transit Gateway remains on the AWS global private network and is not exposed to the public internet. This helps protect against distributed denial of service (DDoS) attacks and other common exploits
- AWS Transit Gateway multicast support distributes the same content to multiple specific destinations

Use-cases

El Deliver global applications spanning thousands of Amazons VPCs. Transit Gateways aids you to deploy new applications without updating massive route tables to create peering relationships