**DOCUMENTATION 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. Your data is automatically encrypted and never travels over the public internet.

**How transit gateways work**

A transit gateway acts as a Regional virtual router for traffic flowing between your virtual private clouds (VPCs) and on-premises networks. A transit gateway scales elastically based on the volume of network traffic. Routing through a transit gateway operates at layer 3, where the packets are sent to a specific next-hop attachment, based on their destination IP addresses.

## Resource attachments

A transit gateway attachment is both a source and a destination of packets. You can attach the following resources to your transit gateway:

* One or more VPCs. AWS Transit Gateway deploys an elastic network interface within VPC subnets, which is then used by the transit gateway to route traffic to and from the chosen subnets. You must have at least one subnet for each Availability Zone, which then enables traffic to reach resources in every subnet of that zone. During attachment creation, resources within a particular Availability Zone can reach a transit gateway only if a subnet is enabled within the same zone. If a subnet route table includes a route to the transit gateway, traffic is only forwarded to the transit gateway if the transit gateway has an attachment in the subnet of the same Availability Zone.
* One or more VPN connections
* One or more AWS Direct Connect gateways
* One or more Transit Gateway Connect attachments
* One or more transit gateway peering connections

Intra-region peering connections are supported. You can have different transit gateways in different Regions.

**Transit gateway concepts**

Transit gateways following key concepts :

* 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 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.