How transit gateways work

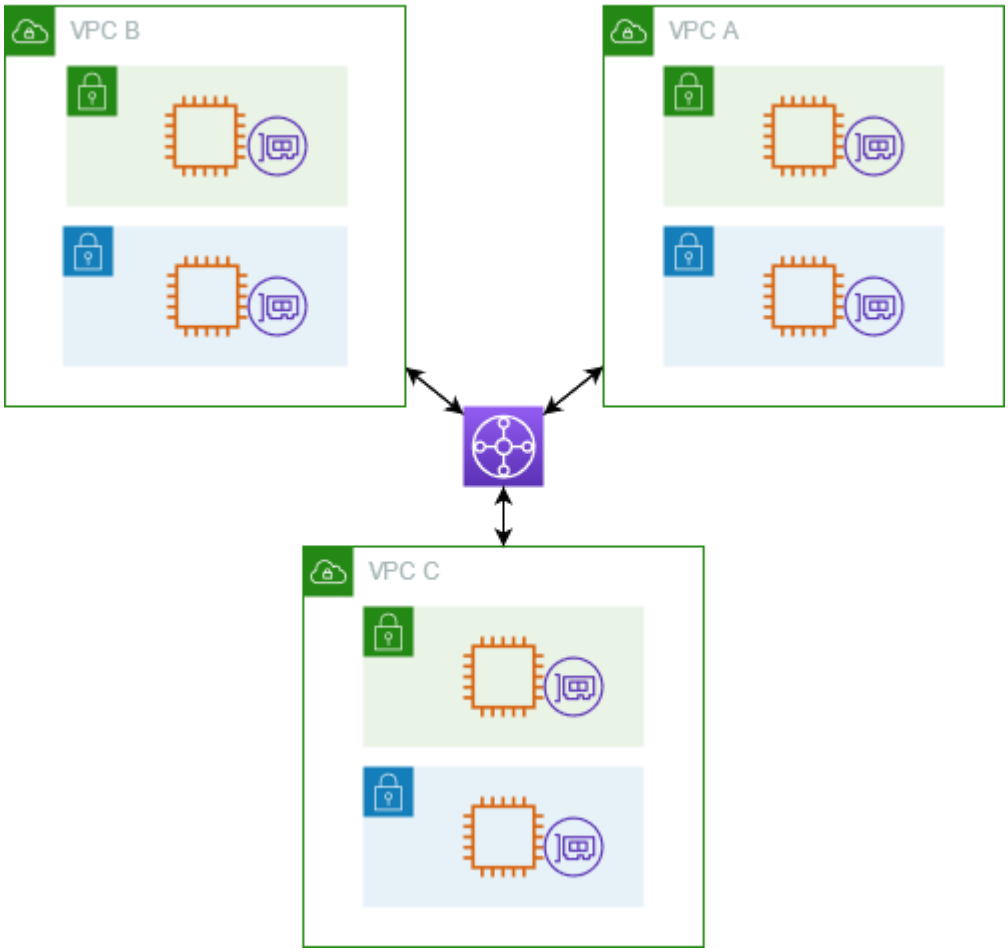
PDF (vpc-tgw.pdf#how-transit-gateways-work) | RSS (transit-gateway-release-notes.rss)

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.

Contents

Architecture diagram

The following diagram shows a transit gateway with three VPC attachments. The route table for each of these VPCs includes the local route and routes that send traffic destined for the other two VPCs to the transit gateway.



The following is an example of a default transit gateway route table for the attachments shown in the previous diagram. The CIDR blocks for each VPC propagate to the route table. Therefore, each attachment can route packets to the other two attachments.

Destination	Target	Route type
VPC A CIDR	*Attachment for VPC A*	propagated
VPC B CIDR	*Attachment for VPC B*	propagated
VPC C CIDR	*Attachment for VPC C*	propagated

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.

Availability Zones

When you attach a VPC to a transit gateway, you must enable one or more Availability Zones to be used by the transit gateway to route traffic to resources in the VPC subnets. To enable each Availability Zone, you specify exactly one subnet. The transit gateway places a network interface in that subnet using one IP address from the subnet. After you enable an Availability Zone, traffic can be routed to all subnets in that zone, not just the specified subnet. Resources that reside in Availability Zones where there is no transit gateway attachment cannot reach the transit gateway.

We recommend that you enable multiple Availability Zones to ensure availability.

Using appliance mode support

If you plan to configure a stateful network appliance in your VPC, you can enable appliance mode support for the VPC attachment in which the appliance is located. This ensures that the transit gateway uses the same Availability Zone for that VPC attachment for the lifetime of a flow of traffic between source and destination. It also allows the transit gateway to send traffic to any Availability Zone in the VPC, as long as there is a subnet association in that zone. For more information, see Example: Appliance in a shared services VPC (./transit-gateway-appliance-scenario.html) .

Routing

Your transit gateway routes IPv4 and IPv6 packets between attachments using transit gateway route tables. You can configure these route tables to propagate routes from the route tables for the attached VPCs, VPN connections, and Direct Connect gateways. You can also add static

routes to the transit gateway route tables. When a packet comes from one attachment, it is routed to another attachment using the route that matches the destination IP address.

For transit gateway peering attachments, only static routes are supported.

Contents

Route tables

Your transit gateway automatically comes with a default route table. By default, this route table is the default association route table and the default propagation route table. Alternatively, if you disable route propagation and route table association, AWS does not create a default route table for the transit gateway.

You can create additional route tables for your transit gateway. This enables you to isolate subnets of attachments. Each attachment can be associated with one route table. An attachment can propagate its routes to one or more route tables.

You can create a blackhole route in your transit gateway route table that drops traffic that matches the route.

When you attach a VPC to a transit gateway, you must add a route to your subnet route table in order for traffic to route through the transit gateway. For more information, see Routing for a Transit Gateway (https://docs.aws.amazon.com/vpc/latest/userguide/route-table-options.html#route-tables-tgw) in the *Amazon VPC User Guide*.

Route table association

You can associate a transit gateway attachment with a single route table. Each route table can be associated with zero to many attachments and can forward packets to other attachments.

Route propagation

Each attachment comes with routes that can be installed in one or more transit gateway route tables. When an attachment is propagated to a transit gateway route table, these routes are installed in the route table.

For a VPC attachment, the CIDR blocks of the VPC are propagated to the transit gateway route table.

When dynamic routing is used with a VPN attachment or a Direct Connect gateway attachment, you can propagate the routes learned from the on-premises router through BGP to any of the transit gateway route tables.

When dynamic routing is used with a VPN attachment, the routes in the route table associated with the VPN attachment are advertised to the customer gateway through BGP.

For a Connect attachment, routes in the route table associated with the Connect attachment are advertised to the third-party virtual appliances, such as SD-WAN appliances, running in a VPC through BGP.

For a Direct Connect gateway attachment, allowed prefixes interactions (https://docs.aws.amazon.com/directconnect/latest/UserGuide/allowed-to-prefixes.html) control which routes are advertised to the customer network from AWS.

When a static route and a propagated route have the same destination, the static route has the higher priority, so the propagated route is not included in the route table. If you remove the static route, the overlapping propagated route is included in the route table.

Routes for peering attachments

You can peer two transit gateways, and route traffic between them. To do this, you create a peering attachment on your transit gateway, and specify the peer transit gateway with which to create the peering connection. You then create a static route in your transit gateway route table to route traffic to the transit gateway peering attachment. Traffic that's routed to the peer transit gateway can then be routed to the VPC and VPN attachments for the peer transit gateway.

For more information, see Example: Peered transit gateways (./transit-gateway-peering-scenario.html) .

Route evaluation order

Transit gateway routes are evaluated in the following order:

- The most specific route for the destination address.
- For routes with the same destination IP address but different targets, the route priority is as follows:
  - Static routes (for example, Site-to-Site VPN static routes)
  - Prefix list referenced routes
  - VPC propagated routes
  - Direct Connect gateway propagated routes
  - Transit Gateway Connect propagated routes
  - Site-to-Site VPN propagated routes

Transit Gateway only shows a preferred route. A backup route will only appear in the Transit Gateway route table if that route is no longer advertised. For example, if you are advertising the same routes over the Direct Connect gateway and over Site-to-Site VPN. AWS Transit Gateway will only shows the routes received from the Direct Connect gateway route, which is the preferred route. The Site-to-Site VPN, which is the backup route, will only display when the Direct Connect gateway is no longer advertised.

Consider the following VPC route table. The VPC local route has the highest priority, followed by the routes that are the most specific. When a static route and a propagated route have the same destination, the static route has a higher priority.

Destination	Target	Priority
10.0.0.0/16	local	1
192.168.0.0/16	pcx-12345	2
172.31.0.0/16	vgw-12345 (static) or tgw-12345 (static)	2
172.31.0.0/16	vgw-12345 (propagated)	3
0.0.0.0/0	igw-12345	4

Consider the following transit gateway route table. If you prefer the AWS Direct Connect gateway attachment to the VPN attachment, use a BGP VPN connection and propagate the routes in the transit gateway route table.

Destination	Attachment (Target)	Resource type	Route type	Priority
10.0.0.0/16	tgw-attach-123 | vpc-1234	VPC	Static or propagated	1
192.168.0.0/16	tgw-attach-789 | vpn-5678	VPN	Static	2
172.31.0.0/16	tgw-attach-456 | dxgw_id	AWS Direct Connect gateway	Propagated	3
172.31.0.0/16	tgw-attach-789 | tgw-connect-peer-123	VPN	Propagated	4
172.31.0.0/16	tgw-attach-789 | vpn-5678	VPN	Propagated	5