Amazon Virtual Private Cloud

Transit Gateways

Amazon Virtual Private Cloud: Transit Gateways

Table of Contents

What is a transit gateway? ... 1
- Transit gateway concepts ... 1
- Working with transit gateways ... 1
- Pricing ... 2

How transit gateways work ... 3
- Resource attachments ... 3
- Availability Zones ... 3
- Routing ... 3
  - Route tables ... 3
  - Route table association ... 4
  - Route propagation ... 4
  - Routes for peering attachments ... 4
  - Route evaluation order ... 4

Getting started ... 6
- Prerequisites ... 6
- Step 1: Create the transit gateway ... 6
- Step 2: Attach your VPCs to your transit gateways ... 7
- Step 3: Add routes between the transit gateway and your VPCs ... 7
- Step 4: Testing the transit gateway ... 8
- Step 5: Delete the transit gateway ... 8

Examples ... 9
- Centralized router ... 9
  - Overview ... 9
  - Routing ... 10
- Isolated VPCs ... 11
  - Overview ... 11
  - Routing ... 12
- Isolated VPCs with shared services ... 12
  - Overview ... 13
  - Routing ... 14
- Peering ... 15
  - Overview ... 15
  - Routing ... 16

Working with transit gateways ... 17
- Transit gateways ... 17
  - Create a transit gateway ... 18
  - View your transit gateways ... 19
  - Add or edit tags for a transit gateway ... 19
  - Sharing a transit gateway ... 19
  - Accepting a resource share ... 20
  - Accepting a shared attachment ... 20
  - Delete a transit gateway ... 20
- Transit gateway attachments to a VPC ... 20
  - Create a transit gateway attachment to a VPC ... 21
  - Modify your VPC attachment ... 21
  - Modify your VPC attachment tags ... 22
  - View your VPC attachments ... 22
  - Delete a VPC attachment ... 22
- Transit gateway attachments to a Direct Connect gateway ... 22
- Transit gateway VPN attachments ... 23
  - Create a transit gateway attachment to a VPN ... 23
  - View your VPN attachments ... 24
- Transit gateway peering attachments ... 24
  - Create a peering attachment ... 24

Accept or reject a peering attachment request 25
Add a route to the transit gateway route table 25
View your transit gateway peering connection attachments 26
Delete a peering attachment 26
Transit gateway route tables 27
Create a transit gateway route table 27
Associate a transit gateway route table 27
Delete an association for a transit gateway route table 27
View transit gateway route tables 28
Propagate a route to a transit gateway route table 28
Disable route propagation 28
View route table propagations 29
Create a static route 29
Delete a static route 29
Export route tables to Amazon S3 30
Delete a transit gateway route table 31
Multicast on transit gateways 31
Multicast concepts 1
Considerations 32
Multicast routing 32
Working with multicast 33
Monitor your transit gateways 38
CloudWatch metrics 38
Transit gateway metrics 38
Metric dimensions for transit gateways 39
CloudTrail logs 39
Transit gateway information in CloudTrail 39
Understanding transit gateway log file entries 40
Authentication and access control 42
Example policies to manage transit gateways 42
Service-linked role 44
Permissions granted by the service-linked role 44
Create the service-linked role 44
Edit the service-linked role 44
Delete the service-linked role 44
Design best practices 45
Network ACLs 46
Same subnet for EC2 network interface workload and transit gateway association 46
Different subnet for EC2 network interface workload and transit gateway association 46
Best Practices 47
Quotas 48
General 48
Routing 48
Transit gateway attachments 48
Bandwidth 48
AWS Direct Connect gateways 48
Multicast 49
Additional quota resources 49
Sharing considerations 50
Unshare a transit gateway 51
Transit Gateway Network Manager 52
Network Manager concepts 1
Pricing 52
How Transit Gateway Network Manager works 52
Registering transit gateways 52
Defining and associating your on-premises network 54
Quotas 54

- Getting started 55
  - Prerequisites 55
  - Step 1: Create a global network 55
  - Step 2: Register your transit gateway 55
  - Step 3: (Optional) Define and associate your on-premises network resources 56
  - Step 4: View and monitor your global network 56
- Scenarios 56
  - AWS-only global network 57
  - Single device with a single VPN connection 57
  - Device with multiple VPN connections 58
  - Multi-device and multi-link site 59
  - SD-WAN connecting to AWS 60
- Working with Network Manager resources 62
  - Global networks 62
  - Transit gateway registrations 63
  - On-premises network 65
- Visualizing and monitoring your global network 72
  - Overview 73
  - Details 74
  - Geographic 75
  - Topology 76
  - Events 77
  - Monitoring 77
  - Route Analyzer 77
- Metrics and events 77
  - Monitoring with CloudWatch metrics 77
  - Monitoring with CloudWatch Events 79
- Route Analyzer 83
  - Route Analyzer basics 83
  - Performing a route analysis 83
  - Example: Route analysis for peered transit gateways 84
  - Example: Route analysis with a middlebox configuration 86
- Identity and access management for Transit Gateway Network Manager 88
  - How Network Manager works with IAM 88
  - Example policies to manage Transit Gateway Network Manager 89
  - Service-linked role 92
- Tagging your Network Manager resources 93
  - Supported resources 93
  - Tagging restrictions 93
- Logging Transit Gateway Network Manager API calls with AWS CloudTrail 94
  - Network Manager information in CloudTrail 94

Document history 96

What is a transit gateway?

A *transit gateway* is a network transit hub that you can use to interconnect your virtual private clouds (VPC) and on-premises networks.

For more information, see AWS Transit Gateway.

Transit gateway concepts

The following are the key concepts for transit gateways:

- **attachment** — You can attach a VPC, an AWS Direct Connect gateway, a peering connection with another transit gateway, or a VPN connection to a transit gateway.
- **transit gateway Maximum Transmission Unit (MTU)** — The maximum transmission unit (MTU) of a network connection is the size, in bytes, of the largest permissible packet that can be passed over the connection. The larger the MTU of a connection, the more data can be passed in a single packet. A transit gateway supports an MTU of 8500 bytes for traffic between VPCs, Direct 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. 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 a VPC or a VPN connection. 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 or VPN connection can dynamically propagate routes to a transit gateway route table. With a VPC, you must create static routes to send traffic to the transit gateway. With a VPN connection, 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.

Working 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 APIs and takes care of many of the connection details, such as calculating signatures, handling request retries, and error handling. 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 error handling. For more information, see the Amazon EC2 API Reference.

Pricing

You are charged based on each hour that your VPC or VPN connection are attached to the transit gateway. For more information, see AWS Transit Gateway pricing.

How transit gateways work

A *transit gateway* acts as a Regional virtual router for traffic flowing between your virtual private clouds (VPC) and VPN connections. 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
- One or more VPN connections
- One or more AWS Direct Connect gateways
- One or more transit gateway peering connections

If you attach a transit gateway peering connection, the transit gateway must be in a different Region.

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 Availability Zone, not just the specified subnet. Resources that reside in Availability Zones where there is no transit gateway attachment will not be able to reach the transit gateway.

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

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 and VPN connections. 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 table that matches the destination IP address.

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

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, we do 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 their 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 for traffic to route through the transit gateway. For more information, see Routing for a Transit Gateway 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 forward packets to other attachments.

Route propagation

Each attachment comes with routes that can be installed to 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.

For a VPN connection attachment, routes in the transit gateway route table propagate to and from the transit gateway and your on-premises router using Border Gateway Protocol (BGP). The prefixes that are advertised over the BGP session are propagated to the transit gateway 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 (p. 15).

Route evaluation order

Transit gateway routes are evaluated in the following order:

- The longest prefix route for the destination address.
- If routes are the same with different targets:
  - Static routes have a higher precedence than propagated routes.
  - Among propagated routes, VPC CIDRs have a higher precedence than Direct Connect gateways than Site-to-Site VPN.

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. When a static route and a propagated route have the same destination, the static route has a higher priority. If you want to use the AWS Direct Connect gateway attachment over the VPN attachment, then 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 | vpn-5678	VPN	Propagated	4

Getting started with transit gateways

The following tasks help you become familiar with transit gateways. You will create a transit gateway and then connect two of your VPCs using the transit gateway.

Tasks

- Prerequisites (p. 6)
- Step 1: Create the transit gateway (p. 6)
- Step 2: Attach your VPCs to your transit gateways (p. 7)
- Step 3: Add routes between the transit gateway and your VPCs (p. 7)
- Step 4: Testing the transit gateway (p. 8)
- Step 5: Delete the transit gateway (p. 8)

Prerequisites

- To demonstrate a simple example of using a transit gateway, create two VPCs in the same Region. The VPCs cannot have overlapping CIDRs. Launch one EC2 instance in each VPC. For more information, see Getting started with IPv4 for Amazon VPC in the *Amazon VPC User Guide*.
- You must enable resource sharing from the master account for your organization. For information about enabling resource sharing, see Enable sharing with AWS organizations in the *AWS RAM User Guide*.
- You cannot have identical routes pointing to two different VPCs. A transit gateway does not propagate the CIDRs of a newly attached VPC if an identical route exists in the transit gateway route tables.
- Verify that you have the permissions required to work with transit gateways. For more information, see Authentication and access control for your transit gateways (p. 42).

Step 1: Create the transit gateway

When you create a transit gateway, we create a default transit gateway route table and use it as the default association route table and the default propagation route table.

To create a transit gateway

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the Region selector, choose the Region that you used when you created the VPCs.
3. On the navigation pane, choose **Transit Gateways**.
4. Choose **Create Transit Gateway**.
5. (Optional) For **Name tag**, type a name for the transit gateway. This creates a tag with "Name" as the key and the name that you specified as the value.
6. (Optional) For **Description**, type a description for the transit gateway.
7. For **Amazon side ASN**, type the private Autonomous System Number (ASN) for your transit gateway. This should be the ASN for the AWS side of a Border Gateway Protocol (BGP) session.

The range is 64512 to 65534 for 16-bit ASNs.

The range is 4200000000 to 4294967294 for 32-bit ASNs.

If you have a multi-region deployment, we recommend that you use a unique ASN for each of your transit gateways.

8. (Optional) You can modify the default settings if you need to disable DNS support, or if you don't want the default association route table or default propagation route table.
9. Choose **Create Transit Gateway**.
10. After you see the message **Create Transit Gateway request succeeded**, choose **Close**. The initial state of the transit gateway is `pending`.

Step 2: Attach your VPCs to your transit gateways

Wait until the transit gateway you created in the previous section shows as available before proceeding with creating an attachment. Create an attachment for each VPC.

Confirm that you have created two VPCs and launched an EC2 instance in each, as described in Prerequisites (p. 6).

Create a transit gateway attachment to a VPC

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Attachments**.
3. Choose **Create Transit Gateway Attachment**.
4. For **Transit Gateway ID**, choose the transit gateway to use for the attachment.
5. For **Attachment type**, choose **VPC**.
6. (Optional) For **Attachment name tag**, type a name for the attachment.
7. Choose whether to enable **DNS support**. For this exercise, do not enable **IPv6 support**.
8. For **VPC ID**, choose the VPC to attach to the transit gateway.
9. For **Subnet IDs**, select one subnet for each Availability Zone to be used by the transit gateway to route traffic. You must select at least one subnet. You can select only one subnet per Availability Zone.
10. Choose **Create attachment**.

Each attachment is always associated with exactly one route table. Route tables can be associated with zero to many attachments. To determine the routes to configure, decide on the use case for your transit gateway, and then configure the routes. For more information, see *Examples* (p. 9).

Step 3: Add routes between the transit gateway and your VPCs

A route table includes dynamic and static routes that determine the next hop for associated VPCs based on the destination IP address of the packet.

To add a route to a VPC route table

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.

2. On the navigation pane, choose **Route Tables**.
3. Choose the route table associated with your VPC.
4. Choose the **Routes** tab, then choose **Edit routes**.
5. Choose **Add route**.
6. In the **Destination** column, enter the destination IP address range. For **Target**, choose the transit gateway that you used to create the transit gateway attachment.
7. Choose **Save routes**, then choose **Close**.

Step 4: Testing the transit gateway

You can confirm that the transit gateway was successfully created by connecting to an EC2 instance in each VPC, and then sending data between them, such as a ping command. For more information, see Connect to your Linux instance or Connecting to your Windows instance.

Step 5: Delete the transit gateway

When you no longer need a transit gateway, you can delete it. You cannot delete a transit gateway that has resource attachments. As soon as the transit gateway is deleted, you stop incurring charges for it.

To delete your transit gateway

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Attachments**.
3. Select the attachments and then choose **Actions**, **Delete**. When prompted for confirmation, choose **Delete**.
4. On the navigation pane, choose **Transit Gateways**.
5. Select the transit gateway and then choose **Actions**, **Delete**. When prompted for confirmation, choose **Delete**.

Examples

The following are common use cases for transit gateways. Your transit gateways are not limited to these use cases.

Topics

- Example: Centralized router (p. 9)
- Example: Isolated VPCs (p. 11)
- Example: Isolated VPCs with shared services (p. 12)
- Example: Peered transit gateways (p. 15)

Example: Centralized router

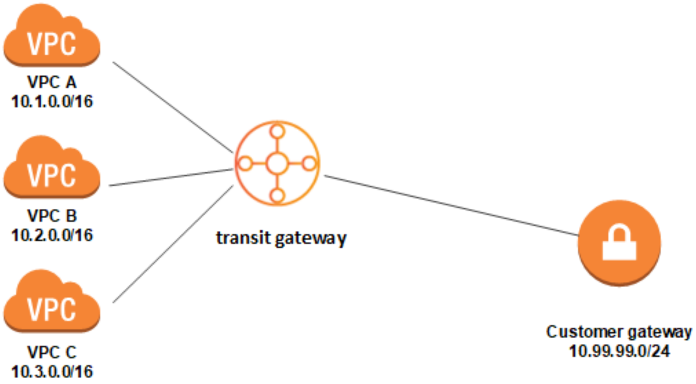
You can configure your transit gateway as a centralized router that connects all of your VPCs, AWS Direct Connect, and AWS Site-to-Site VPN connections. In this scenario, all attachments are associated with the transit gateway default route table and propagate to the transit gateway default route table. Therefore, all attachments can route packets to each other, with the transit gateway serving as a simple layer 3 IP router.

Contents

- Overview (p. 9)
- Routing (p. 10)

Overview

The following diagram shows the key components of the configuration for this scenario. In this scenario, there are three VPC attachments and one Site-to-Site VPN attachment to the transit gateway. Packets from the subnets in VPC, A, VPC B, and VPC C that have the internet as a destination, route first through the transit gateway and then route to the VPN. Packets from one VPC that have a destination of a subnet in another VPC, for example from 10.1.0.0 to 10.2.0.0, route through the transit gateway.



In this scenario, you create the following entities for this scenario::

- Three VPCs. For information about creating a VPC, see Creating a VPC in the *Amazon Virtual Private Cloud User Guide*.
- A transit gateway. For more information, see the section called “Create a transit gateway” (p. 18).

- Three VPC attachments on the transit gateway. For more information, see the section called "Create a transit gateway attachment to a VPC" (p. 21).
- A Site-to-Site VPN. For more information, see the following topics in the *AWS Site-to-Site VPN User Guide*:
  - Create a Site-to-Site VPN connection
  - Requirements for your customer gateway device
- A VPN attachment on the transit gateway. For more information, see the section called "Create a transit gateway attachment to a VPN" (p. 23).

When you create the VPC attachments, the CIDRs for each VPC propagate to the transit gateway route table. When the VPN is up, the BGP session is established and the Site-to-Site VPN CIDR propagates to the transit gateway route table and the VPC CIDRs are added to the customer gateway BGP table.

Routing

Each VPC has a route table and there is a route table for the transit gateway.

VPC route tables

Each VPC has a route table with 2 entries. The first entry is the default entry for local IPv4 routing in the VPC; this entry enables the instances in this VPC to communicate with each other. The second entry routes all other IPv4 subnet traffic to the transit gateway. The following table shows the VPC A routes.

Destination	Target
10.1.0.0/16	local
0.0.0.0/0	*tgw-id*

Transit gateway route table

The following is an example of a default route table for the attachments shown in the previous diagram, with route propagation enabled.

Destination	Target	Route type
10.1.0.0/16	`Attachment for VPC A`	propagated
10.2.0.0/16	`Attachment for VPC B`	propagated
10.3.0.0/16	`Attachment for VPC C`	propagated
10.99.99.0/24	`Attachment for VPN connection`	propagated

Customer gateway BGP table

The customer gateway BGP table contains the following VPC IP Addresses.

- 10.1.0.0/16
- 10.2.0.0/16
- 10.3.0.0/16

Example: Isolated VPCs

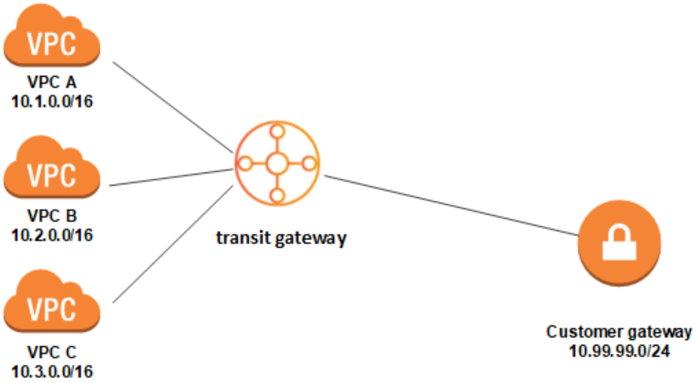
You can configure your transit gateway as multiple isolated routers. This is similar to using multiple transit gateways, but provides more flexibility in cases where the routes and attachments might change. In this scenario, each isolated router has a single route table. All attachments associated with an isolated router propagate and associate with its route table. Attachments associated with one isolated router can route packets to each other, but cannot route packets to or receive packets from the attachments for another isolated router.

Contents

- Overview (p. 11)
- Routing (p. 12)

Overview

The following diagram shows the key components of the configuration for this scenario. Packets from VPC A, VPC B, and VPC C route to the transit gateway. Packets from the subnets in VPC, A, VPC B, and VPC C that have the internet as a destination, route first through the transit gateway and then route to the Site-to-Site VPN. Packets from one VPC that have a destination of a subnet in another VPC, for example from 10.1.0.0 to 10.2.0.0, route through the transit gateway, where they are blocked because there is no route for them in the transit gateway route table.



In this scenario, you create the following entities:

- Three VPCs. For information about creating a VPC, see Creating a VPC in the *Amazon Virtual Private Cloud User Guide*.
- A transit gateway. For more information, see the section called "Create a transit gateway" (p. 18).
- Three attachments on the transit gateway for the three VPCs. For more information, see the section called "Create a transit gateway attachment to a VPC" (p. 21).
- A Site-to-Site VPN. For more information, see the following topics in the *AWS Site-to-Site VPN User Guide*:
  - Create a Site-to-Site VPN connection
  - Requirements for your customer gateway device
- A VPN attachment on the transit gateway. For more information, see the section called "Create a transit gateway attachment to a VPN" (p. 23).

When the VPN is up, the BGP session is established and the VPN CIDR propagates to the transit gateway route table and the VPC CIDRs are added to the gateway BGP table.

Routing

Each VPC has a route table and there is a VPC route table and a VPN route table in the transit gateway.

VPC route tables

Each VPC has a route table with 2 entries. The first entry is the default entry for local IPv4 routing in the VPC; this entry enables the instances in this VPC to communicate with each other. The second entry routes all other IPv4 subnet traffic to the transit gateway. The following table shows the VPC A routes.

Destination	Target
10.1.0.0/16	local
0.0.0.0/0	*tgw-id*

Transit gateway route table

This scenario uses a route table for the VPCs and a route table for the VPN. The route table for the VPC has an entry that points to the VPN attachment.

Destination	Target	Route type
10.99.99.0/24	*`Attachment for VPN connection`*	propagated

The route table for the VPN has entries for each of the VPCs

Destination	Target	Route type
10.1.0.0/16	*`Attachment for VPC A`*	propagated
10.2.0.0/16	*`Attachment for VPC B`*	propagated
10.3.0.0/16	*`Attachment for VPC C`*	propagated

Customer gateway BGP table

The customer gateway BGP table contains the following VPC IP Addresses.

- 10.1.0.0/16
- 10.2.0.0/16
- 10.3.0.0/16

Example: Isolated VPCs with shared services

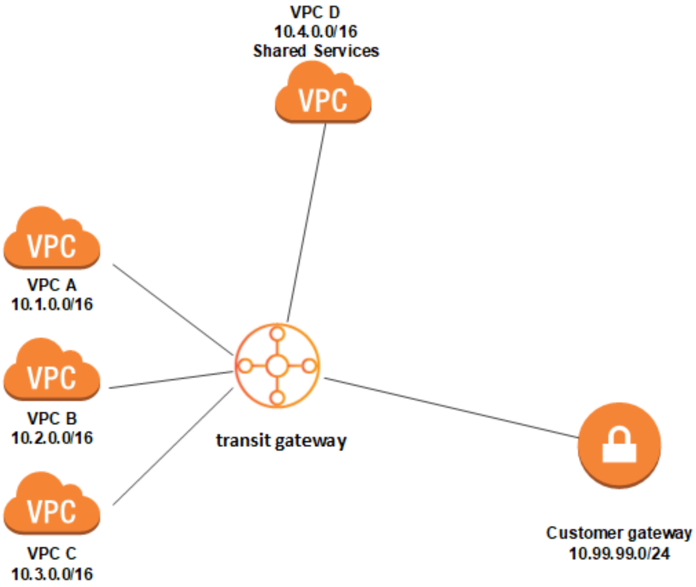
You can configure your transit gateway as multiple isolated routers that use a shared service. This is similar to using multiple transit gateways, but provides more flexibility in cases where the routes and attachments might change. In this scenario, each isolated router has a single route table. All attachments associated with an isolated router propagate and associate with its route table. Attachments associated with one isolated router can route packets to each other, but cannot route packets to or receive packets from the attachments for another isolated router. Attachments can route packets to or receive packets from the shared services. You can use this scenario when you have groups that need to be isolated, but use a shared service, for example a production system.

Contents

- Overview (p. 13)
- Routing (p. 14)

Overview

The following diagram shows the key components of the configuration for this scenario. Packets from VPC A, VPC B, and VPC C route to the transit gateway. Packets from the subnets in VPC A, VPC B, and VPC C that have the internet as a destination, route first through the transit gateway and then route to the Site-to-Site VPN. Packets from one VPC that have a destination of a subnet in another VPC, for example from 10.1.0.0 to 10.2.0.0, route through the transit gateway, where they are blocked because there is no route for them in the transit gateway route table. Packets from VPC A, VPC B, and VPC C that have VPC D as the destination route through the transit gateway.



In this scenario, you create the following entities:

- Four VPCs. For information about creating a VPC, see Creating a VPC in the *Amazon Virtual Private Cloud User Guide*.
- A transit gateway. For more information, see Create a transit gateway.
- Four attachments on the transit gateway for the four VPCs. For more information, see the section called "Create a transit gateway attachment to a VPC" (p. 21).
- A Site-to-Site VPN. For more information, see the following topics in the *AWS Site-to-Site VPN User Guide*:
  - Create a Site-to-Site VPN connection
  - Requirements for your customer gateway device
- A VPN attachment on the transit gateway. For more information, see the section called "Create a transit gateway attachment to a VPN" (p. 23).

When the VPN is up, the BGP session is established and the VPN CIDR propagates to the transit gateway route table and the VPC CIDRs are added to the gateway BGP table.

Routing

Each VPC has a route table and there is a VPC route table and a Site-to-Site VPN route table in the transit gateway.

VPC A, VPC B, VPC C, and VPC D route tables

Each VPC has a route table with 2 entries. The first entry is the default entry for local IPv4 routing in the VPC; this entry enables the instances in this VPC to communicate with each other. The second entry routes all other IPv4 subnet traffic to the transit gateway. The following table shows the VPC A routes.

Destination	Target
10.1.0.0/16	local
0.0.0.0/0	*tgw-id*

Transit gateway route tables

This scenario uses two transit gateway route tables—one for the VPCs and one for the VPN. The route table for the VPCs has an entry that points to the VPN attachment and an entry that points to VPC D.

Destination	Target	Route type
10.99.99.0/24	*`Attachment for VPN connection`*	propagated
10.4.0.0/16	*`Attachment for VPC D`*	propagated

The route table for the Site-to-Site VPN connection is associated with the VPN attachment, and has entries that point to each of the VPCs. This enables communication to the VPCs from the VPN connection.

Destination	Target	Route type
10.1.0.0/16	*`Attachment for VPC A`*	propagated
10.2.0.0/16	*`Attachment for VPC B`*	propagated
10.3.0.0/16	*`Attachment for VPC C`*	propagated
10.4.0.0/16	*`Attachment for VPC D`*	propagated

Customer gateway BGP table

The customer gateway BGP table contains the following VPC IP Addresses.

- 10.1.0.0/16

- 10.2.0.0/16
- 10.3.0.0/16
- 10.4.0.0/16

Example: Peered transit gateways

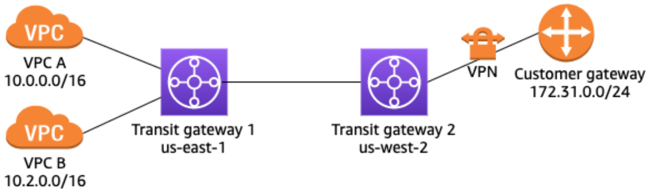
You can create a transit gateway peering connection between transit gateways in different Regions. You can then route traffic between the attachments for each of the transit gateways. In this scenario, VPC and VPN attachments are associated with the transit gateway default route tables, and they propagate to the transit gateway default route tables. Each transit gateway route table has a static route that points to the transit gateway peering attachment.

Contents

- Overview (p. 15)
- Routing (p. 16)

Overview

The following diagram shows the key components of the configuration for this scenario. Transit gateway 1 has two VPC attachments, and transit gateway 2 has one Site-to-Site VPN attachment. Packets from the subnets in VPC A and VPC B that have the internet as a destination first route through transit gateway 1, then transit gateway 2, and then route to the VPN.



You create the following entities for this scenario:

- Two VPCs. For information about creating a VPC, see Creating a VPC in the *Amazon Virtual Private Cloud User Guide*.
- Two transit gateways in different Regions. For more information, see the section called “Create a transit gateway” (p. 18).
- Two VPC attachments on the first transit gateway. For more information, see the section called “Create a transit gateway attachment to a VPC” (p. 21).
- A Site-to-Site VPN attachment on the second transit gateway. For more information, see the section called “Create a transit gateway attachment to a VPN” (p. 23) and Requirements for your customer gateway device in the *AWS Site-to-Site VPN User Guide*.
- A transit gateway peering attachment between the two transit gateways. For more information, see Transit gateway peering attachments (p. 24).

When you create the VPC attachments, the CIDRs for each VPC propagate to the route table for transit gateway 1. When the VPN is up, the following actions occur:

- The BGP session is established
- The Site-to-Site VPN CIDR propagates to the route table for transit gateway 2
- The VPC CIDRs are added to the gateway BGP table

Routing

Each VPC has a route table and each transit gateway has a route table.

VPC route tables

Each VPC has a route table with 2 entries. The first entry is the default entry for local IPv4 routing in the VPC. This default entry enables the resources in this VPC to communicate with each other. The second entry routes all other IPv4 subnet traffic to the transit gateway. The following table shows the VPC A routes.

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*tgw-1-id*

Transit gateway route tables

The following is an example of the default route table for transit gateway 1, with route propagation enabled.

Destination	Target	Route type
10.0.0.0/16	`Attachment ID for VPC A`	propagated
10.2.0.0/16	`Attachment ID for VPC B`	propagated
0.0.0.0/0	`Attachment ID for peering connection`	static

The following is an example of the default route table for transit gateway 2, with route propagation enabled.

Destination	Target	Route type
172.31.0.0/16	`Attachment ID for VPN connection`	propagated
10.0.0.0/16	`Attachment ID for peering connection`	static
10.2.0.0/16	`Attachment ID for peering connection`	static

Customer gateway BGP table

The customer gateway BGP table contains the following VPC IP Addresses.

- 10.0.0.0/16
- 10.2.0.0/16

Working with transit gateways

You can work with transit gateways using the Amazon VPC console or the AWS CLI.

Contents

- Transit gateways (p. 17)
- Transit gateway attachments to a VPC (p. 20)
- Transit gateway attachments to a Direct Connect gateway (p. 22)
- Transit gateway VPN attachments (p. 23)
- Transit gateway peering attachments (p. 24)
- Transit gateway route tables (p. 27)
- Multicast on transit gateways (p. 31)

Transit gateways

A transit gateway enables you to attach VPCs and VPN connections in the same Region and route traffic between them. A transit gateway works across AWS accounts, and you can use AWS Resource Access Manager to share your transit gateway with other accounts. After you share a transit gateway with another AWS account, the account owner can attach their VPCs to your transit gateway. A user from either account can delete the attachment at any time.

You can enable multicast on a transit gateway, and then create a transit gateway multicast domain that allows multicast traffic to be sent from your multicast source to multicast group members over VPC attachments that you associate with the domain.

You can also create a peering connection attachment between transit gateways in different AWS Regions. This enables you to route traffic between the transit gateways' attachments across different Regions.

Each VPC or VPN attachment is associated with a single route table. That route table decides the next hop for the traffic coming from that resource attachment. A route table inside the transit gateway allows for both IPv4 or IPv6 CIDRs and targets. The targets are VPCs and VPN connections. When you attach a VPC or create a VPN connection on a transit gateway, the attachment is associated with the default route table of the transit gateway.

You can create additional route tables inside the transit gateway, and change the VPC or VPN association to these route tables. This enables you to segment your network. For example, you can associate development VPCs with one route table and production VPCs with a different route table. This enables you to create isolated networks inside a transit gateway similar to virtual routing and forwarding (VRFs) in traditional networks.

Transit gateways support dynamic and static routing between attached VPCs and VPN connections. You can enable or disable route propagation for each attachment. Transit gateway peering attachments support static routing only.

Topics

- Create a transit gateway (p. 18)
- View your transit gateways (p. 19)
- Add or edit tags for a transit gateway (p. 19)
- Sharing a transit gateway (p. 19)

- Accepting a resource share (p. 20)
- Accepting a shared attachment (p. 20)
- Delete a transit gateway (p. 20)

Create a transit gateway

When you create a transit gateway, we create a default transit gateway route table and use it as the default association route table and the default propagation route table.

You must enable resource sharing from the master account for your organization. For information about enabling resource sharing, see Enable Sharing with AWS Organizations in the *AWS RAM User Guide*.

To create a transit gateway using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateways**.
3. Choose **Create Transit Gateway**.
4. For **Name tag**, optionally enter a name for the transit gateway. A name tag can make it easier to identify a specific gateway from the list of gateways. When you add a **Name tag**, a tag is created with a key of **Name** and with a value equal to the value you enter.
5. For **Description**, optionally enter a description for the transit gateway.
6. For **Amazon side ASN**, either leave the default value to use the default Autonomous System Number (ASN), or enter the private ASN for your transit gateway. This should be the ASN for the AWS side of a Border Gateway Protocol (BGP) session.

   The range is 64512 to 65534 for 16-bit ASNs.

   The range is 4200000000 to 4294967294 for 32-bit ASNs.

   If you have a multi-region deployment, we recommend that you use a unique ASN for each of your transit gateways.
7. For **DNS support**, choose **enable** if you need the VPC to resolve public IPv4 DNS host names to private IPv4 addresses when queried from instances in another VPC attached to the transit gateway.
8. For **VPN ECMP support**, choose **enable** if you need Equal Cost Multipath (ECMP) routing support between VPN connections. If connections advertise the same CIDRs, the traffic is distributed equally between them.

   When you select this option, the advertised BGP ASN, the BGP attributes such as the AS-path and the communities for preference must be the same.
9. For **Default route table association**, choose **enable** to automatically associate transit gateway attachments with the default route table for the transit gateway.
10. For **Default route table propagation**, choose **enable** to automatically propagate transit gateway attachments to the default route table for the transit gateway.
11. (Optional) To use the transit gateway as a router for multicast traffic, select **Multicast support**.
12. For **Auto accept shared attachments**, choose **enable** to automatically accept cross-account attachments.
13. Choose **Create Transit Gateway**.
14. After you see the message **Create Transit Gateway request succeeded**, choose **Close**.

To create a transit gateway using the AWS CLI

Use the create-transit-gateway command.

View your transit gateways

To view your transit gateways using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateways**. The details for the transit gateway are displayed below the list of gateways on the page.

To view your transit gateways using the AWS CLI

Use the describe-transit-gateways command.

Add or edit tags for a transit gateway

Add tags to your resources to help organize and identify them, such as by purpose, owner, or environment. You can add multiple tags to each transit gateway. Tag keys must be unique for each transit gateway. If you add a tag with a key that is already associated with the transit gateway, it updates the value of that tag. For more information, see Tagging your Amazon EC2 Resources.

Add tags to a transit gateway using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateways**.
3. Choose the transit gateway for which to add or edit tags.
4. Choose the **Tags** tab in the lower part of the page.
5. Choose **Add/Edit Tags**.
6. Choose **Create Tag**.
7. Enter a **Key** and **Value** for the tag.
8. Choose **Save**.

Sharing a transit gateway

You can use AWS Resource Access Manager (RAM) to share a transit gateway across accounts or across your organization in AWS Organizations. Use the following procedure to share a transit gateway that you own.

To share a transit gateway

1. Open the AWS Resource Access Manager console at https://console.aws.amazon.com/ram/.
2. Choose **Create a resource share**.
3. Under **Description**, for **Name**, type a descriptive name for the resource share.
4. For **Select resource type**, choose **Transit Gateways**. Select the transit gateway.
5. (Optional) For **Principals**, add principals to the resource share. For each AWS account, OU, or organization, specify its ID and choose **Add**.

   For **Allow external accounts**, choose whether to allow sharing for this resource with AWS accounts that are external to your organization.
6. (Optional) Under **Tags**, type a tag key and tag value pair for each tag. These tags are applied to the resource share but not to the transit gateway.
7. Choose **Create resource share**.

Accepting a resource share

If you were added to a resource share, you receive an invitation to join the resource share. You must accept the resource share before you can access the shared resources.

To accept a resource share

1. Open the AWS Resource Access Manager console at https://console.aws.amazon.com/ram/.
2. On the navigation pane, choose **Shared with me**, **Resource shares**.
3. Select the resource share.
4. Choose **Accept resource share**.
5. To view the shared transit gateway, open the **Transit Gateways** page in the Amazon VPC console.

Accepting a shared attachment

If you didn't enable the **Auto accept shared attachments** functionality when you created your transit gateway, you must manually accept cross-account (shared) attachments.

To manually accept a shared attachment

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Attachments**.
3. Select the transit gateway attachment that's pending acceptance.
4. Choose **Actions**, **Accept**.

To accept a shared attachment using the AWS CLI

Use the accept-transit-gateway-vpc-attachment command.

Delete a transit gateway

You can't delete a transit gateway with existing attachments. You need to delete all attachments before you can delete a transit gateway.

To delete a transit gateway using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. Choose the transit gateway to delete.
3. Choose **Actions**, **Delete**, then choose **Delete** to confirm the deltion.

To delete a transit gateway using the AWS CLI

Use the delete-transit-gateway command.

Transit gateway attachments to a VPC

When you attach a VPC to a transit gateway, you must specify one subnet from each Availability Zone to be used by the transit gateway to route traffic. Specifying one subnet from an Availability Zone enables traffic to reach resources in every subnet in that Availability Zone.

Limits

When you attach a VPC to a transit gateway, resources in Availability Zones where there is no transit gateway attachment cannot reach the transit gateway. If there is a route to the transit gateway in a subnet route table, traffic is only forwarded to the transit gateway when the transit gateway has an attachment in a subnet in the same Availability Zone.

The resources in a VPC attached to a transit gateway cannot access the security groups of a different VPC that is also attached to the same transit gateway.

A transit gateway does not support DNS resolution for custom DNS names of attached VPCs set up using private hosted zones in Amazon Route 53. To configure the name resolution for private hosted zones for all VPCs attached to a transit gateway, see Centralized DNS management of hybrid cloud with Amazon Route 53 and AWS Transit Gateway.

Create a transit gateway attachment to a VPC

To create a VPC attachment using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Attachments**.
3. Choose **Create Transit Gateway Attachment**.
4. For **Transit Gateway ID**, choose the transit gateway for the attachment. You can choose a transit gateway that you own or a transit gateway that was shared with you.
5. For **Attachment type**, choose **VPC**.
6. Under **VPC Attachment**, optionally type a name for **Attachment name tag**.
7. Choose whether to enable **DNS Support** and **IPv6 Support**.
8. For **VPC ID**, choose the VPC to attach to the transit gateway.

   This VPC must have at least one subnet associated with it.
9. For **Subnet IDs**, select one subnet for each Availability Zone to be used by the transit gateway to route traffic. You must select at least one subnet. You can select only one subnet per Availability Zone.
10. Choose **Create attachment**.

To create a VPC attachment using the AWS CLI

Use the create-transit-gateway-vpc-attachment command.

Modify your VPC attachment

To modify your VPC attachments using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Attachments**.
3. Select the VPC attachment, and then choose **Actions**, **Modify**.
4. To enable DNS support, select **DNS support**.
5. To add a subnet to the attachment, next to the subnet, select the box.
6. Choose **Modify attachment**.

To modify your VPC attachments using the AWS CLI

Use the modify-transit-gateway-vpc-attachment command.

Modify your VPC attachment tags

To modify your VPC attachment tags using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Attachments**.
3. Select the VPC attachment, and then choose **Actions**, **Add/Edit tags**.
4. [Add a tag] Choose **Add tag** and do the following:
   - For **Key**, enter the key name.
   - For **Value**, enter the key value.
5. [Remove a tag] Next to the tag, choose Delete ("X").
6. Choose **Modify attachment**.

View your VPC attachments

To view your VPC attachments using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Attachments**.
3. Choose the search bar, select **Resource type** from the menu, and then select **VPC**.
4. The VPC attachments are displayed. Choose an attachment to view its details.

To view your VPC attachments using the AWS CLI

Use the describe-transit-gateway-vpc-attachments command.

Delete a VPC attachment

To delete a VPC attachment using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Attachments**.
3. Select the VPC attachment.
4. Choose **Actions**, **Delete**.
5. When prompted for confirmation, choose **Delete**.

To delete a VPC attachment using the AWS CLI

Use the delete-transit-gateway-vpc-attachment command.

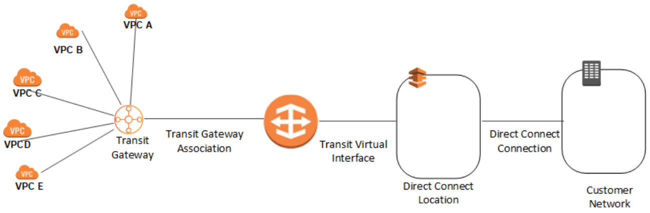
Transit gateway attachments to a Direct Connect gateway

Attach a transit gateway to a Direct Connect gateway using a transit virtual interface. This configuration offers the following benefits. You can:

- Manage a single connection for multiple VPCs or VPNs that are in the same Region.

- Advertise prefixes from on-premises to AWS and from AWS to on-premises.

The following diagram illustrates how the Direct Connect gateway enables you to create a single connection to your Direct Connect connection that all of your VPCs can use.



The solution involves the following components:

- A transit gateway.
- A Direct Connect gateway.
- An association between the Direct Connect gateway and the transit gateway.
- A transit virtual interface that is attached to the Direct Connect gateway.

For information about configuring Direct Connect gateways with transit gateways, see Transit gateway associations in the *AWS Direct Connect User Guide*.

Transit gateway VPN attachments

To attach a VPN connection to your transit gateway, you must specify the customer gateway. For more information about the requirements for a customer gateway device, see Requirements for your customer gateway device in the *AWS Site-to-Site VPN User Guide*.

For static VPNs, add the static routes to the transit gateway route table.

Create a transit gateway attachment to a VPN

To create a VPN attachment using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Attachments**.
3. Choose **Create Transit Gateway Attachment**.
4. For **Transit Gateway ID**, choose the transit gateway for the attachment. You can choose a transit gateway that you own.
5. For **Attachment type**, choose **VPN**.
6. For **Customer Gateway**, do one of the following:
   - To use an existing customer gateway, choose **Existing**, and then select the gateway to use.

     If your customer gateway is behind a network address translation (NAT) device that's enabled for NAT traversal (NAT-T), use the public IP address of your NAT device, and adjust your firewall rules to unblock UDP port 4500.
   - To create a customer gateway, choose **New**, then for **IP Address**, type a static public IP address and **BGP ASN**.

     For **Routing options**, choose whether to use **Dynamic** or **Static**. For more information, see Site-to-Site VPN Routing Options in the *AWS Site-to-Site VPN User Guide*.

7. For **Tunnel Options**, see Site-to-Site VPN Tunnel Options for your Site-to-Site VPN Connection in the *AWS Site-to-Site VPN User Guide*.
8. Choose **Create attachment**.

To create a VPN attachment using the AWS CLI

Use the create-vpn-connection command.

View your VPN attachments

To view your VPN attachments using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Attachments**.
3. Choose the search bar, select **Resource type** from the menu, and then select **VPN**.
4. The VPN attachments are displayed. Choose an attachment to view its details or to add tags.

To view your VPN attachments using the AWS CLI

Use the describe-transit-gateway-attachments command.

Transit gateway peering attachments

You can peer two transit gateways and route traffic between them, which includes IPv4 and IPv6 traffic. To do this, create a peering attachment on your transit gateway, and specify a transit gateway in another AWS Region. The peer transit gateway can be in your account or a different AWS account.

After you create a peering attachment request, the owner of the peer transit gateway (also referred to as the *accepter transit gateway*) must accept the request. To route traffic between the transit gateways, add a static route to the transit gateway route table that points to the transit gateway peering attachment.

We recommend using unique ASNs for the peered transit gateways to take advantage of future route propagation capabilities.

Transit gateway peering attachments are not supported in the following AWS Regions: Asia Pacific (Hong Kong), Asia Pacific (Osaka-Local), and Middle East (Bahrain).

Create a peering attachment

Before you begin, ensure that you have the ID of the transit gateway that you want to attach. If the transit gateway is in another AWS account, ensure that you have the AWS account ID of the owner of the transit gateway.

After you create the peering attachment, the owner of the accepter transit gateway must accept the attachment request.

To create a peering attachment using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Attachments**.
3. Choose **Create Transit Gateway Attachment**.
4. For **Transit Gateway ID**, choose the transit gateway for the attachment. You can choose a transit gateway that you own or a transit gateway that was shared with you.

5. For **Attachment type**, choose **Peering Connection**.
6. Optionally enter a name tag for the attachment.
7. For **Account**, do one of the following:
   - If the transit gateway is in your account, choose **My account**.
   - If the transit gateway is in different AWS account, choose **Other account**. For **Account ID**, enter the AWS account ID.
8. For **Region**, choose the Region that the transit gateway is located in.
9. For **Transit gateway ID (accepter)**, enter the ID of the transit gateway that you want to attach.
10. Choose **Create attachment**.

To create a peering attachment using the AWS CLI

Use the create-transit-gateway-peering-attachment command.

Accept or reject a peering attachment request

To activate the peering attachment, the owner of the accepter transit gateway must accept the peering attachment request. This is required even if both transit gateways are in the same account. The peering attachment must be in the `pendingAcceptance` state. Accept the peering attachment request from the Region that the accepter transit gateway is located in.

Alternatively, you can reject any peering connection request that you've received that's in the `pendingAcceptance` state. You must reject the request from the Region that the accepter transit gateway is located in.

To accept a peering attachment request using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Attachments**.
3. Select the transit gateway peering attachment that's pending acceptance.
4. Choose **Actions**, **Accept**.
5. Add the static route to the transit gateway route table. For more information, see the section called “Create a static route” (p. 29).

To reject a peering attachment request using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Attachments**.
3. Select the transit gateway peering attachment that's pending acceptance.
4. Choose **Actions**, **Reject**.

To accept or reject a peering attachment using the AWS CLI

Use the accept-transit-gateway-peering-attachment and reject-transit-gateway-peering-attachment commands.

Add a route to the transit gateway route table

To route traffic between the peered transit gateways, you must add a static route to the transit gateway route table that points to the transit gateway peering attachment. The owner of the accepter transit gateway must also add a static route to their transit gateway's route table.

To create a static route using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Route Tables**.
3. Select the route table for which to create a route.
4. Choose **Actions**, **Create route**.
5. On the **Create route** page, enter the CIDR block for which to create the route. For example, specify the CIDR block of a VPC that's attached to the peer transit gateway.
6. Choose the peering attachment for the route.
7. Choose **Create route**.

To create a static route using the AWS CLI

Use the create-transit-gateway-route command.

After you create the route, associate the transit gateway route table with the transit gateway peering attachment. For more information, see the section called "Associate a transit gateway route table" (p. 27).

View your transit gateway peering connection attachments

You can view your transit gateway peering attachments and information about them.

To view your peering attachments using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Attachments**.
3. Choose the search bar, select **Resource type** from the menu, and then select **peering**.
4. The peering attachments are displayed. Choose an attachment to view its details.

To view your transit gateway peering attachments using the AWS CLI

Use the describe-transit-gateway-peering-attachments command.

Delete a peering attachment

You can delete a transit gateway peering attachment. The owner of either of the transit gateways can delete the attachment.

To delete a peering attachment using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Attachments**.
3. Select the transit gateway peering attachment.
4. Choose **Actions**, **Delete**.
5. When prompted for confirmation, choose **Delete**.

To delete a peering attachment using the AWS CLI

Use the delete-transit-gateway-peering-attachment command.

Transit gateway route tables

Use transit gateway route tables to configure routing for your transit gateway attachments.

Create a transit gateway route table

To create a transit gateway route table using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Route Tables**.
3. Choose **Create Transit Gateway Route Table**.
4. (Optional) For **Name tag**, type a name for the transit gateway route table. This creates a tag with the tag key "Name", where the tag value is the name that you specify.
5. For **Transit Gateway ID**, select the transit gateway for the route table.
6. Choose **Create Transit Gateway Route Table**.

To create a transit gateway route table using the AWS CLI

Use the create-transit-gateway-route-table command.

Associate a transit gateway route table

You can associate a transit gateway route table with a transit gateway attachment.

To associate a transit gateway route table using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Route Tables**.
3. Select the route table.
4. In the lower part of the page, choose the **Associations** tab.
5. Choose **Create association**.
6. Choose the attachment to associate and then choose **Create association**.

To associate a transit gateway route table using the AWS CLI

Use the associate-transit-gateway-route-table command.

Delete an association for a transit gateway route table

You can disassociate a transit gateway route table from a transit gateway attachment.

To disassociate a transit gateway route table using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Route Tables**.
3. Select the route table.
4. In the lower part of the page, choose the **Associations** tab.
5. Choose the attachment to disassociate and then choose **Delete association**.

6. When prompted for confirmation, choose **Delete association**.

To disassociate a transit gateway route table using the AWS CLI

Use the disassociate-transit-gateway-route-table command.

View transit gateway route tables

To view transit gateway route tables using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Route Tables**.
3. To find a specific route table or set of tables, enter all or part of the name, keyword, or attribute in the filter field.

Choose a route table to display the settings for it.

To view transit gateway route tables using the AWS CLI

Use the describe-transit-gateway-route-tables command.

Propagate a route to a transit gateway route table

Use route propagation to add a route from a route table to an attachment.

To propagate a route to a transit gateway attachment route table

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Route Tables**.
3. Select the route table for which to create a propagation.
4. Choose **Actions**, **Create propagation**.
5. On the **Create propagation** page, choose the attachment.
6. Choose **Create propagation**.
7. Choose **Close**.

To enable route propagation using the AWS CLI

Use the enable-transit-gateway-route-table-propagation command.

Disable route propagation

Remove a propagated route from a route table attachment.

To disable route propagation using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Route Tables**.
3. Select the route table to delete the propagation from.
4. On the lower part of the page, choose the **Propagations** tab.
5. Select the attachment and then choose **Delete propagation**.
6. When prompted for confirmation, choose **Delete propagation**.

To disable route propagation using the AWS CLI

Use the disable-transit-gateway-route-table-propagation command.

View route table propagations

To view route propagations using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Route Tables**.
3. Select the route table to view propagations for.
4. On the lower part of the page, choose the **Propagations** tab.

To view route propagations using the AWS CLI

Use the get-transit-gateway-route-table-propagations command.

Create a static route

You can create a static route for a VPC, VPN, or transit gateway peering attachment, or you can create a blackhole route that drops traffic that matches the route.

To create a static route using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Route Tables**.
3. Select the route table for which to create a route.
4. Choose **Actions**, **Create route**.
5. On the **Create route** page, enter the CIDR block for which to create the route.
6. Choose the attachment for the route.
7. Choose **Create route**.

To create a blackhole route using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Route Tables**.
3. Select the route table for which to create a route.
4. Choose **Actions**, **Create route**.
5. On the **Create route** page, enter the CIDR block for which to create the route, and then choose **Blackhole**.
6. Choose **Create route**.

To create a static route or blackhole route using the AWS CLI

Use the create-transit-gateway-route command.

Delete a static route

You can create a static route for an attached VPC or VPN connection, or you can create a blackhole route that drops traffic that matches the route.

To delete a static route using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Route Tables**.
3. Select the route table for which to delete the route, and choose **Routes**.
4. Choose the route to delete.
5. Choose **Delete route**.
6. In the confirmation box, choose **Delete route**.

To delete a static route using the AWS CLI

Use the delete-transit-gateway-route command.

Export route tables to Amazon S3

You can export the routes in your transit gateway route tables to an Amazon S3 bucket. The routes are saved to the specified Amazon S3 bucket in a JSON file.

To export transit gateway route tables using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Route Tables**.
3. Choose the route table that includes the routes to export.
4. Choose **Actions**, **Export routes**.
5. On the **Export routes** page, for **S3 bucket name**, type the name of the S3 bucket.
6. To filter the routes exported, specify filter parameters in the **Filters** section of the page.
7. Choose **Export routes**.

To access the exported routes, open the Amazon S3 console at https://console.aws.amazon.com/s3/, and navigate to the bucket that you specified. The file name includes the AWS account ID, AWS Region, route table ID, and a timestamp. Select the file and choose **Download**. The following is an example of a JSON file that contains information about two propagated routes for VPC attachments.

```
{
  "filter": [
    {
      "name": "route-search.subnet-of-match",
      "values": [
        "0.0.0.0/0",
        "::/0"
      ]
    }
  ],
  "routes": [
    {
      "destinationCidrBlock": "10.0.0.0/16",
      "transitGatewayAttachments": [
        {
          "resourceId": "vpc-0123456abcd123456",
          "transitGatewayAttachmentId": "tgw-attach-1122334455aabbcc1",
          "resourceType": "vpc"
        }
      ],
      "type": "propagated",
      "state": "active"
    },
    {
      "destinationCidrBlock": "10.2.0.0/16",
      "transitGatewayAttachments": [
        {
          "resourceId": "vpc-abcabc123123abca",
          "transitGatewayAttachmentId": "tgw-attach-6677889900aabbcc7",
          "resourceType": "vpc"
        }
      ],
      "type": "propagated",
      "state": "active"
    }
  ]
}
```

Delete a transit gateway route table

To delete a transit gateway route table using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Route Tables**.
3. Select the route table to delete.
4. Choose **Actions**, **Delete route table**.
5. Choose **Delete** again to confirm the deletion.

To delete a transit gateway route table using the AWS CLI

Use the delete-transit-gateway-route-table command.

Multicast on transit gateways

Multicast is a communication protocol used for delivering a single stream of data to multiple receiving computers simultaneously. Transit Gateway supports routing multicast traffic between subnets of attached VPCs and serves as a multicast router for instances sending traffic destined for multiple receiving instances.

Multicast concepts

The following are the key concepts for multicast:

- **Multicast domain** — A Multicast domain allows segmentation of a multicast network into different domains and makes the transit gateway act as multiple multicast routers. You define multicast domain membership at the subnet level.
- **Multicast group** — A multicast group is used to identify a set of sources and receivers that will send and receive the same multicast traffic. A multicast group is identified by a group IP address. Sources use the group address as the IP destination address in their data packets. Receivers use this group address to inform the network that they are interested in receiving packets sent to that group. Transit gateway multicast group membership is defined by individual elastic network interfaces attached to EC2 instances.
- **Multicast source** — An elastic network interface associated with a supported EC2 instance that sends multicast traffic.
- **Multicast group member** — An elastic network interface associated with a supported EC2 instance that receives multicast traffic. A multicast group has multiple group members.

Considerations

- You must create a new transit gateway to enable multicast.
- You cannot share multicast-enabled transit gateways with other accounts (using AWS Resource Access Manager).
- Multicast group membership is managed using Amazon VPC Console or the AWS CLI.
- Internet Group Management Protocol (IGMP) (IGMP) support for managing group membership will come in the future.
- A subnet can only be in one multicast domain.
- If you use a non-Nitro instance, you must disable the **Source/Dest** check. For information about disabling the check, see Changing the source or destination checking in the *Amazon EC2 User Guide for Linux Instances*.
- A non-Nitro instance cannot be a multicast sender.

Multicast routing

Learn how route tables, network ACLs, and security groups handle multicast traffic.

Route tables

Route tables are not used to handle multicast traffic. Instead, we send all multicast traffic to the transit gateway that is associated with a multicast domain, when you add a subnet to that multicast domain.

Network ACLs

Network ACL rules operate at the subnet level and apply to multicast traffic, because transit gateways reside outside of the subnet. For information about network ACLs, see Network ACLs in the *Amazon VPC User Guide*.

To control multicast traffic, you can create allow and deny rules. For example, to allow outbound multicast traffic, create the following outbound rule using the console or CLI:

- **Rule number** - A rule number, for example 100.
- **CIDR block** - The CIDR block of the multicast group, for example 224.0.0.0/24.
- **Protocol** - The protocol that your multicast applications use.
- **Action** - Set this to **Allow**.
- **Description** - A description for the rule, for example, "Allow all outbound multicast traffic".

Security groups

Security group rules operate at the instance level and can be applied to both inbound and outbound multicast traffic. This behavior is the same as unicast traffic. For all group member instances, you must allow inbound traffic from the group source. For information about security groups, see Security groups in the *Amazon VPC User Guide*.

You can control traffic that multicast sources can send by adding inbound rules to the security group for the multicast traffic. Use the following values for the parameters.

- **Type** - The traffic type that your multicast applications use.
- **Port range** - The ports that your multicast applications use.
- **Protocol** - The protocol that your multicast applications use.

- **Source** - The multicast senders IP address, or CIDR. You cannot use a security group for the source.
- **Description** - A description for the rule, for example, "Allow all inbound multicast traffic".

For example, to allow receipt of multicast UDP traffic on port 143 from any multicast sender in a VPC with a CIDR of 10.0.0.0/16, create a security group, and then add the following inbound rule:

Type	Protocol	Source	Port Range	Description
Custom UDP Rule	UDP	Custom 10.0.0.0/16	143	UDP port 143 rule

Working with multicast

You can configure multicast on transit gateways using the Amazon VPC console or the AWS CLI.

Contents

- Create a transit gateway multicast domain (p. 33)
- Associate VPC attachments and subnets with a transit gateway multicast domain (p. 34)
- Register sources with a multicast group (p. 34)
- Register members with a multicast group (p. 34)
- Deregister sources from a multicast group (p. 35)
- Deregister members from a multicast group (p. 35)
- Disassociate subnets from a transit gateway multicast domain (p. 35)
- View your multicast groups (p. 36)
- View your transit gateway multicast domain associations (p. 36)
- Add or remove tags for a transit gateway multicast domain (p. 36)
- Delete a transit gateway multicast domain (p. 37)

Create a transit gateway multicast domain

To begin using multicast on a transit gateway, create a transit gateway multicast domain.

Before you create a multicast domain, create a new transit gateway that has multicast enabled. For more information, see the section called “Create a transit gateway” (p. 18).

To create a transit gateway multicast domain using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Multicast**.
3. Choose **Create Transit Gateway Multicast domain**.
4. (Optional) For **Name tag**, enter a name to identify the domain.
5. For **Transit Gateway ID**, select the transit gateway that processes the multicast traffic.
6. Choose **Create Transit Gateway multicast** domain.

To create a transit gateway multicast domain using the AWS CLI

Use the create-transit-gateway-multicast-domain command.

Associate VPC attachments and subnets with a transit gateway multicast domain

Use the following procedure to associate a VPC attachment with a multicast domain. When you create an association, you can then select the subnets to include in the multicast domain.

To associate VPC attachments with a transit gateway multicast domain using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Multicast**.
3. Select the transit gateway multicast domain, and then choose **Actions**, **Create association**.
4. For **Transit Gateway ID**, select the transit gateway attachment.
5. For **Choose subnets to associate**, select the subnets to include in the domain.
6. Choose **Create association**.

To associate VPC attachments with a transit gateway multicast domain using the AWS CLI

Use the associate-transit-gateway-multicast-domain command.

Register sources with a multicast group

Use the following procedure to register sources with a multicast group. The source is the network interface that sends multicast traffic.

You need the following information before you add a source:

- The ID of the transit gateway multicast domain
- The ID of the source network interface
- The multicast group IP address

To register sources using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Multicast**.
3. Select the transit gateway multicast domain, and then choose **Actions**, **Add group sources**.
4. For **Group IP address**, enter either the IPv4 CIDR block or IPv6 CIDR block to assign to the multicast domain.
5. Under **Choose network interfaces**, select the multicast senders' network interfaces.
6. Choose **Add sources**.

To register sources using the AWS CLI

Use the register-transit-gateway-multicast-group-sources command.

Register members with a multicast group

Use the following procedure to register group members with a multicast group. The members are the network interfaces that receive multicast traffic.

You need the following information before you add members:

- The ID of the transit gateway multicast domain

- The IDs of the group members' network interfaces
- The multicast group IP address

To register members using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Multicast**.
3. Select the transit gateway multicast domain, and then choose **Actions**, **Add group members**.
4. For **Group IP address**, enter either the IPv4 CIDR block or IPv6 CIDR block to assign to the multicast domain.
5. Under **Choose network interfaces**, select the multicast receivers' network interfaces.
6. Choose **Add members**.

To register members using the AWS CLI

Use the register-transit-gateway-multicast-group-sources command.

Deregister sources from a multicast group

Use the following procedure to remove a source from a multicast group.

To remove a source using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Multicast**.
3. Select the transit gateway multicast domain.
4. Choose the **Groups** tab.
5. Select the sources, and then choose **Remove source**.

To remove a source using the AWS CLI

Use the deregister-transit-gateway-multicast-group-sources command.

Deregister members from a multicast group

Use the following procedure to deregister members from a multicast group.

To deregister members using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Multicast**.
3. Select the transit gateway multicast domain.
4. Choose the **Groups** tab.
5. Select the members, and then choose **Remove member**.

To deregister members using the AWS CLI

Use the deregister-transit-gateway-multicast-group-members command.

Disassociate subnets from a transit gateway multicast domain

Use the following procedure to disassociate subnets from a transit gateway multicast domain.

To disassociate subnets using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Multicast**.
3. Select the transit gateway multicast domain.
4. Choose the **Associations** tab.
5. Select the subnet, and then choose **Remove association**.

To disassociate subnets using the AWS CLI

Use the disassociate-transit-gateway-multicast-domain command.

View your multicast groups

Use the following procedure to view your multicast groups.

To view multicast groups using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Multicast**.
3. Select the transit gateway multicast domain.
4. Choose the **Groups** tab.

To view multicast groups using the AWS CLI

Use the view multicast groups command.

View your transit gateway multicast domain associations

You can view your transit gateway multicast domains to verify that they are available, and that they contain the appropriate subnets and attachments.

To view a transit gateway multicast domain using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Multicast**.
3. Select the transit gateway multicast domain.

To view a transit gateway multicast domain using the AWS CLI

Use the describe-transit-gateway-multicast-domains command.

Add or remove tags for a transit gateway multicast domain

Add tags to your resources to help organize and identify them, such as by purpose, owner, or environment. You can add multiple tags to each transit gateway multicast domain. Tag keys must be unique for each transit gateway multicast domain. If you add a tag with a key that is already associated with the transit gateway multicast domain, it updates the value of that tag. For more information, see Tagging your Amazon EC2 Resources.

Add tags to a transit gateway using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.

2. On the navigation pane, choose **Transit Gateways Multicast**.
3. Choose the transit gateway multicast domain for which to add or edit tags.
4. Choose the **Tags** tab in the lower part of the page.
5. Choose **Add/Edit Tags**.
6. Choose **Create Tag**.
7. Enter a **Key** and **Value** for the tag.
8. Choose **Save**.

Delete a transit gateway multicast domain

Use the following procedure to delete a transit gateway multicast domain.

To delete a transit gateway multicast domain using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. On the navigation pane, choose **Transit Gateway Multicast**.
3. Select the transit gateway multicast domain, and then choose **Actions**, **Delete multicast domain**.
4. Choose **Delete**.

To delete a transit gateway multicast domain using the AWS CLI

Use the delete-transit-gateway-multicast-domain command.

Monitor your transit gateways

You can use the following features to monitor your transit gateways, analyze traffic patterns, and troubleshoot issues with your transit gateways.

CloudWatch metrics

You can use Amazon CloudWatch to retrieve statistics about data points for your transit gateways as an ordered set of time series data, known as *metrics*. You can use these metrics to verify that your system is performing as expected. For more information, see CloudWatch metrics for your transit gateways (p. 38).

VPC Flow Logs

You can use VPC Flow Logs to capture detailed information about the traffic going to and from the VPCs that are attached to your transit gateways. For more information, see VPC Flow Logs in the *Amazon VPC User Guide*.

CloudTrail logs

You can use AWS CloudTrail to capture detailed information about the calls made to the transit gateway API and store them as log files in Amazon S3. You can use these CloudTrail logs to determine which calls were made, the source IP address where the call came from, who made the call, when the call was made, and so on. For more information, see Logging API calls for your transit gateway using AWS CloudTrail (p. 39).

CloudWatch metrics for your transit gateways

Amazon VPC publishes data points to Amazon CloudWatch for your transit gateways. CloudWatch enables you to retrieve statistics about those data points as an ordered set of time series data, known as *metrics*. Think of a metric as a variable to monitor, and the data points as the values of that variable over time. Each data point has an associated timestamp and an optional unit of measurement.

You can use metrics to verify that your system is performing as expected. For example, you can create a CloudWatch alarm to monitor a specified metric and initiate an action (such as sending a notification to an email address) if the metric goes outside what you consider an acceptable range.

Amazon VPC reports metrics to CloudWatch only when requests are flowing through the transit gateway. If there are requests flowing through the transit gateway, Amazon VPC measures and sends its metrics in 60-second intervals. If there are no requests flowing through the transit gateway or no data for a metric, the metric is not reported.

For more information, see the Amazon CloudWatch User Guide.

Contents

- Transit gateway metrics (p. 38)
- Metric dimensions for transit gateways (p. 39)

Transit gateway metrics

The `AWS/TransitGateway` namespace includes the following metrics.

Metric	Description
`BytesIn`	The number of bytes received by the transit gateway.
`BytesOut`	The number of bytes sent from the transit gateway.
`PacketsIn`	The number of packets received by the transit gateway.
`PacketsOut`	The number of packets sent by the transit gateway.
`PacketDropCountBlackhole`	The number of packets dropped because they matched a blackhole route.
`PacketDropCountNoRoute`	The number of packets dropped because they did not match a route.

Metric dimensions for transit gateways

To filter the metrics for your transit gateways, use the following dimensions.

Dimension	Description
`TransitGateway`	Filters the metric data by transit gateway.

Logging API calls for your transit gateway using AWS CloudTrail

AWS CloudTrail is a service that provides a record of actions taken by a user, role, or an AWS service. CloudTrail captures all transit gateway API calls as events. The calls captured include calls from the AWS Management Console and code calls to the transit gateway API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for transit gateways. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to the transit gateway API, the IP address from which the request was made, who made the request, when it was made, and additional details.

For more information about transit gateway APIs, see the Transit Gateways section in the *Amazon EC2 API Reference*.

For more information about CloudTrail, see the AWS CloudTrail User Guide.

Transit gateway information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs through the transit gateway API, that activity is recorded in a CloudTrail event along with other AWS service events in **Event history**. You can view, search, and download recent events in your AWS account. For more information, see Viewing Events with CloudTrail Event History.

For an ongoing record of events in your AWS account, including events for the transit gateway API, create a trail. A *trail* enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following:

- Overview for Creating a Trail
- CloudTrail Supported Services and Integrations
- Configuring Amazon SNS Notifications for CloudTrail
- Receiving CloudTrail Log Files from Multiple Regions and Receiving CloudTrail Log Files from Multiple Accounts

All calls to transit gateway actions are logged by CloudTrail. For example, calls to the `CreateTransitGateway` action generates entries in the CloudTrail log files.

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the CloudTrail userIdentity Element.

Understanding transit gateway log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The log files include events for all AWS API calls for your AWS account, not just transit gateway API calls. You can locate calls to the transit gateway API by checking for `eventSource` elements with the value `ec2.amazonaws.com`. To view a record for a specific action, such as `CreateTransitGateway`, check for `eventName` elements with the action name.

The following are example CloudTrail log records for the transit gateway API for a user who created a transit gateway using the console. You can identify the console using the `userAgent` element. You can identify the requested API call using the `eventName` elements. Information about the user (`Alice`) can be found in the `userIdentity` element.

Example Example: CreateTransitGateway

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2018-11-15T05:25:50Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "CreateTransitGateway",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "console.ec2.amazonaws.com",
    "requestParameters": {
        "CreateTransitGatewayRequest": {
            "Options": {
                "DefaultRouteTablePropagation": "enable",
                "AutoAcceptSharedAttachments": "disable",
                "DefaultRouteTableAssociation": "enable",
                "VpnEcmpSupport": "enable",
                "DnsSupport": "enable"
            },
            "TagSpecification": {
                "ResourceType": "transit-gateway",
                "tag": 1,
                "Tag": {
                    "Value": "my-tgw",
                    "tag": 1,
                    "Key": "Name"
                }
            }
        }
    },
    "responseElements": {
        "CreateTransitGatewayResponse": {
            "xmlns": "http://ec2.amazonaws.com/doc/2016-11-15/",
            "requestId": "a07c1edf-c201-4e44-bffb-3ce90EXAMPLE",
            "transitGateway": {
                "tagSet": {
                    "item": {
                        "value": "my-tgw",
                        "key": "Name"
                    }
                },
                "creationTime": "2018-11-15T05:25:50.000Z",
                "transitGatewayId": "tgw-0a13743bd6c1f5fcb",
                "options": {
                    "propagationDefaultRouteTableId": "tgw-rtb-0123cd602be10b00a",
                    "amazonSideAsn": 64512,
                    "defaultRouteTablePropagation": "enable",
                    "vpnEcmpSupport": "enable",
                    "autoAcceptSharedAttachments": "disable",
                    "defaultRouteTableAssociation": "enable",
                    "dnsSupport": "enable",
                    "associationDefaultRouteTableId": "tgw-rtb-0123cd602be10b00a"
                },
                "state": "pending",
                "ownerId": 123456789012
            }
        }
    },
    "requestID": "a07c1edf-c201-4e44-bffb-3ce90EXAMPLE",
    "eventID": "e8fa575f-4964-4ab9-8ca4-6b5b4EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

Authentication and access control for your transit gateways

AWS uses security credentials to identify you and to grant you access to your AWS resources. You can use features of AWS Identity and Access Management (IAM) to allow other users, services, and applications to use your AWS resources fully or in a limited way, without sharing your security credentials.

By default, IAM users don't have permission to create, view, or modify AWS resources. To allow an IAM user to access resources, such as a transit gateway, and perform tasks, you must create an IAM policy that grants the IAM user permission to use the specific resources and API actions they'll need, then attach the policy to the IAM user or the group to which the IAM user belongs. When you attach a policy to a user or group of users, it allows or denies the users permission to perform the specified tasks on the specified resources.

To work with a transit gateway, one of the following AWS managed policies might meet your needs:

- **PowerUserAccess**
- **ReadOnlyAccess**
- **AmazonEC2FullAccess**
- **AmazonEC2ReadOnlyAccess**

For more information, see IAM policies for Amazon EC2 in the *Amazon EC2 User Guide*.

Example policies to manage transit gateways

The following are example IAM policies for working with transit gateways.

Creating a tagged transit gateway

The following example enables users to create transit gateways. The `aws:RequestTag` condition key requires users to tag the transit gateway with the tag `stack=prod`. The `aws:TagKeys` condition key uses the `ForAllValues` modifier to indicate that only the key `stack` is allowed in the request (no other tags can be specified). If users don't pass this specific tag when they create the transit gateway, or if they don't specify tags at all, the request fails.

The second statement uses the `ec2:CreateAction` condition key to allow users to create tags only in the context of `CreateTransitGateway`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCreateTaggedTGWs",
            "Effect": "Allow",
            "Action": "ec2:CreateTransitGateway",
            "Resource": "arn:aws:ec2:region:account-id:transit-gateway/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/stack": "prod"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "stack"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:region:account-id:transit-gateway/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateTransitGateway"
                }
            }
        }
    ]
}
```

Working with transit gateway route tables

The following example enables users to create and delete transit gateway route tables for a specific transit gateway only (`tgw-11223344556677889`). Users can also create and replace routes in any transit gateway route table, but only for attachments that have the tag `network=new-york-office`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteTransitGatewayRouteTable",
                "ec2:CreateTransitGatewayRouteTable"
            ],
            "Resource": [
                "arn:aws:ec2:region:account-id:transit-gateway/tgw-11223344556677889",
                "arn:aws:ec2:*:*:transit-gateway-route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTransitGatewayRoute",
                "ec2:ReplaceTransitGatewayRoute"
            ],
            "Resource": "arn:aws:ec2:*:*:transit-gateway-attachment/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/network": "new-york-office"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTransitGatewayRoute",
                "ec2:ReplaceTransitGatewayRoute"
            ],
            "Resource": "arn:aws:ec2:*:*:transit-gateway-route-table/*"
        }
    ]
}
```

Transit gateway service-linked role

Amazon VPC uses service-linked roles for the permissions that it requires to call other AWS services on your behalf. For more information, see Using service-linked roles in the *IAM User Guide*.

Permissions granted by the service-linked role

Amazon VPC uses the service-linked role named **AWSServiceRoleForVPCTransitGateway** to call the following actions on your behalf when you work with a transit gateway:

- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterface`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:DeleteNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`

AWSServiceRoleForVPCTransitGateway trusts the `transitgateway.amazonaws.com` service to assume the role.

Create the service-linked role

You don't need to manually create the **AWSServiceRoleForVPCTransitGateway** role. Amazon VPC creates this role for you when you attach a VPC in your account to a transit gateway.

For Amazon VPC to create a service-linked role on your behalf, you must have the required permissions. For more information, see Service-linked role permissions in the *IAM User Guide*.

Edit the service-linked role

You can edit the description of **AWSServiceRoleForVPCTransitGateway** using IAM. For more information, see Editing a service-linked role in the *IAM User Guide*.

Delete the service-linked role

If you no longer need to use transit gateways, we recommend that you delete **AWSServiceRoleForVPCTransitGateway**.

You can delete this service-linked role only after you delete all transit gateway VPC attachments in your AWS account. This ensures that you can't inadvertently remove permission to access your VPC attachments.

You can use the IAM console, the IAM CLI, or the IAM API to delete service-linked roles. For more information, see Deleting a service-linked role in the *IAM User Guide*.

After you delete **AWSServiceRoleForVPCTransitGateway**, Amazon VPC creates the role again if you attach a VPC in your account to a transit gateway.

Transit gateway design best practices

The following are best practices for your transit gateway design:

- Use a separate subnet for each transit gateway VPC attachment. For each subnet, use a small CIDR, for example /28, so that you have more addresses for EC2 resources. When you use a separate subnet, you can configure the following:
  - Keep the inbound and outbound NACL associated with the transit gateway subnets open.
  - Depending on your traffic flow, you can apply NACLs to your workload subnets.
- Create one network ACL and associate it with all of the subnets that are associated with the transit gateway. 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 transit gateway, unless your network design requires multiple VPC route tables (for example, a middle-box VPC that routes traffic through multiple NAT gateways).
- Use Border Gateway Protocol (BGP) Site-to-Site VPN connections. If your 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.
- You do not need additional transit gateways for high availability, because transit gateways are highly available by design.
- Limit the number of transit gateway route tables unless your design requires multiple transit gateway route tables.
- For multiple Region deployments, we recommend that you use a unique Autonomous System Number (Amazon-side ASN) for each of your transit gateways.

How Network ACLs work with transit gateways

A network access control list (NACL) is an optional layer of security.

Network access control list (NACL) rules are applied differently, depending on the scenario:

- When you have the same subnet for your EC2 network interface workload and transit gateway association.
- When you have different subnets for your EC2 network interface workload and transit gateway association.

Same subnet for EC2 network interface workload and transit gateway association

Consider a configuration where you have an EC2 network interface workload and transit gateway association that have the same subnet. The same route table is used for both outbound and inbound traffic: the traffic from individual EC2 instances to the transit gateway, and the traffic that comes through the transit gateway to your VPC.

NACL rules are applied in the following way for traffic from individual EC2 instances to the transit gateway:

- Outbound rules use the destination IP address for evaluation.
- Inbound rules use the source IP address for evaluation.

NACL rules are applied in the following way for traffic from the transit gateway to your VPC:

- Inbound rules and outbound rules are not evaluated.

Different subnet for EC2 network interface workload and transit gateway association

Consider a configuration where you have an EC2 network interface workload and transit gateway association that have different subnets. In this configuration, each subnet is associated with a different NACL.

NACL rules are applied in the following way for traffic from individual EC2 instances to the transit gateway:

- Outbound rules for the EC2 instance subnet use the destination IP address for evaluation.
- Inbound rules for the transit gateway subnet use the source IP address for evaluation.
- Outbound rules for the transit gateway subnet are not evaluated.

NACL rules are applied in the following way for traffic from the transit gateway to your VPC:

- Outbound rules for the transit gateway subnet use the destination IP address for evaluation.
- Inbound rules for the transit gateway subnet are not evaluated.
- Inbound rules for the EC2 instance subnet use the source IP address for evaluation.

Best Practices

Use a separate subnet for each transit gateway VPC attachment. For each subnet, use a small CIDR, for example /28, so that you have more addresses for EC2 resources. When you use a separate subnet, you can configure the following:

- Keep the inbound and outbound NACL that is associated with the transit gateway subnets open.
- Depending on your traffic flow, you can apply NACLs to your workload subnets.

Quotas for your transit gateways

Your AWS account has the following service quotas (previously referred to as *limits*) related to transit gateways. Unless indicated otherwise, you can request an increase for a quota. For more information about service quotas, see AWS Service Quotas in the *Amazon Web Services General Reference*.

General

- Number of transit gateways per Region per account: 5

Routing

- Number of transit gateway route tables per transit gateway: 20
- Number of routes per transit gateway: 10,000

  For VPC route table quotas, see Amazon VPC quotas in the *Amazon VPC User Guide*.

Transit gateway attachments

- Total number of transit gateway attachments per transit gateway: 5,000
- Number of transit gateway attachments per VPC: 5

  This value cannot be increased.
- Number of transit gateway peering attachments per transit gateway: 50
- Number of pending transit gateway peering attachments transit gateway:10

Bandwidth

- Maximum bandwidth (burst) per VPC connection: 50 Gbps
- Maximum bandwidth per VPN connection: 1.25 Gbps

  This is a hard value. You can use ECMP to get higher VPN bandwidth by aggregating multiple VPN tunnels.

AWS Direct Connect gateways

- Number of AWS Direct Connect gateways per transit gateway: 20

  This value cannot be increased.
- Transit gateways per AWS Direct Connect gateway: 3

  This value cannot be increased.

Multicast

- Number of multicast domains per transit gateway: 20
- Number of multicast group members and sources per transit gateway: 1000
- Number of members per transit gateway multicast group: 100
- Number of multicast domain associations per VPC: 20
- Number of sources per transit gateway multicast group: 1

Additional quota resources

For information about quotas that apply to Site-to-Site VPN connections, see Site-to-Site VPN Quotas in the *AWS Site-to-Site VPN User Guide*.

For information about quotas that apply to VPC attachments see Amazon VPC Quotas in the *Amazon VPC User Guide*.

For information about quotas that apply to Direct Connect gateway attachments see AWS Direct Connect Quotas in the *AWS Direct Connect User Guide*.

For more information about service quotas for Transit Gateway Network Manager, see Network Manager quotas (p. 54).

Transit gateway sharing considerations

You can use AWS Resource Access Manager (RAM) to share a transit gateway for VPC attachments across accounts or across your organization in AWS Organizations. Take the following into account when you want to share a transit gateway.

An AWS Site-to-Site VPN attachment must be created in the same AWS account that owns the transit gateway.

An attachment to a Direct Connect gateway uses a transit gateway association and can be in the same AWS account as the Direct Connect gateway, or a different one from the Direct Connect gateway.

By default, IAM users do not have permission to create or modify AWS RAM resources. To allow IAM users to create or modify resources and perform tasks, you must create IAM policies that grant permission to use specific resources and API actions. You then attach those policies to the IAM users or groups that require those permissions.

Only the resource owner can perform the following operations:

- Create a resource share.
- Update a resource share.
- View a resource share.
- View the resources that are shared by your account, across all resource shares.
- View the principals with whom you are sharing your resources, across all resource shares. Viewing the principals with whom you are sharing enables you to determine who has access to your shared resources.
- Delete a resource share.
- Run all transit gateway, transit gateway attachment, and transit gateway route tables APIs.

You can perform the following operations on resources that are shared with you:

- Accept, or reject a resource share invitation.
- View a resource share.
- View the shared resources that you can access.
- View a list of all the principals that are sharing resources with you. You can see which resources and resource shares they have shared with you.
- Can run the `DescribeTransitGateways` API.
- Run the APIs that create and describe attachments, for example `CreateTransitGatewayVpcAttachment` and `DescribeTransitGatewayVpcAttachments`, in their VPCs.
- Leave a resource share.

A resource owner cannot create, modify, or delete the transit gateway route tables, or the transit gateway route table propagations and associations.

When you create a transit gateway, the transit gateway, is created in the Availability Zone that is mapped to your account and is independent from other accounts. When the transit gateway and the attachment entities are in different accounts, use the Availability Zone ID to uniquely and consistently identify the interface endpoint Availability Zone. For example, use1-az1 is an AZ ID for the us-east-1 Region and maps to the same location in every AWS account.

Unshare a transit gateway

When the share owner unshares the transit gateway, the following rules apply:

- The transit gateway attachment remains functional.
- The shared account can not describe the transit gateway.
- The transit gateway owner, and the share owner can delete the transit gateway attachment.

Transit Gateway Network Manager

Transit Gateway Network Manager (Network Manager) enables you to centrally manage your networks that are built around transit gateways. You can visualize and monitor your global network across AWS Regions and on-premises locations.

Network Manager concepts

The following are the key concepts for Network Manager:

- **global network** — A single, private network that acts as the high-level container for your network objects.
- **device** — Represents a physical or a virtual appliance that connects to a transit gateway over an IPsec tunnel (a VPN connection).
- **link** — Represents a single internet connection from a site.
- **site** — Represents a physical on-premises location. It could be a branch, office, store, campus, or a data center.

Pricing

There are no additional fees for using Network Manager. You are charged the standard fees for the network resources that you manage in your global network (such as transit gateways).

How Transit Gateway Network Manager works

To use Transit Gateway Network Manager (Network Manager), you create a *global network* to represent your network. Initially, the global network is empty. You then register your existing transit gateways and define your on-premises resources in the global network. This enables you to visualize and monitor your AWS resources and your on-premises networks.

After you create your global network, you can monitor your networks through a dashboard on the Network Manager console. You can view network activity and health using Amazon CloudWatch metrics and Amazon CloudWatch Events. The Network Manager console can help you identify whether issues in your network are caused by AWS resources, your on-premises resources, or the connections between them.

Network Manager does not create, modify, or delete your transit gateways and their attachments. To work with transit gateways, use the Amazon VPC console and the Amazon EC2 APIs.

Topics

- Registering transit gateways (p. 52)
- Defining and associating your on-premises network (p. 54)
- Network Manager quotas (p. 54)

Registering transit gateways

You can register transit gateways that are in the same AWS account as your global network. When you register a transit gateway, the following transit gateway attachments are automatically included in your global network:

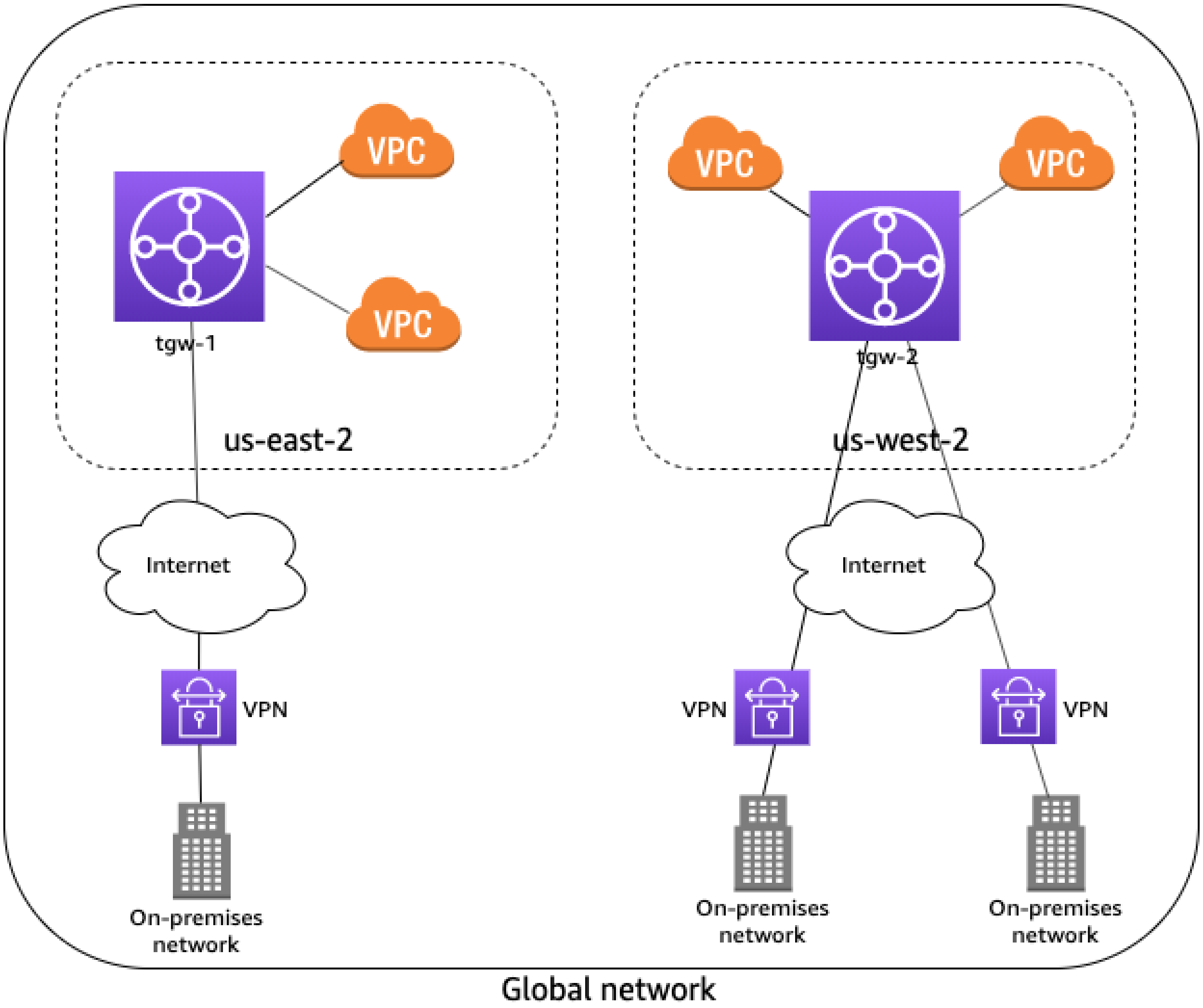
- VPCs
- Site-to-Site VPN connections
- AWS Direct Connect gateways
- Transit gateway peering connections

When you register a transit gateway that has a peering attachment, you can view the peer transit gateway in your global network, but you cannot view its attachments. If you own the peer transit gateway, you can register it in your global network to view its attachments.

If you delete a transit gateway, it's automatically deregistered from your global network.

Multi-region network

You can create a global network that includes transit gateways in multiple AWS Regions. This enables you to monitor the global health of your AWS network. In the following diagram, the global network includes a transit gateway in the `us-east-2` Region and a transit gateway in the `us-west-2` Region. Each transit gateway has VPC and VPN attachments. You can use the Network Manager console to view and monitor both of the transit gateways and their attachments.



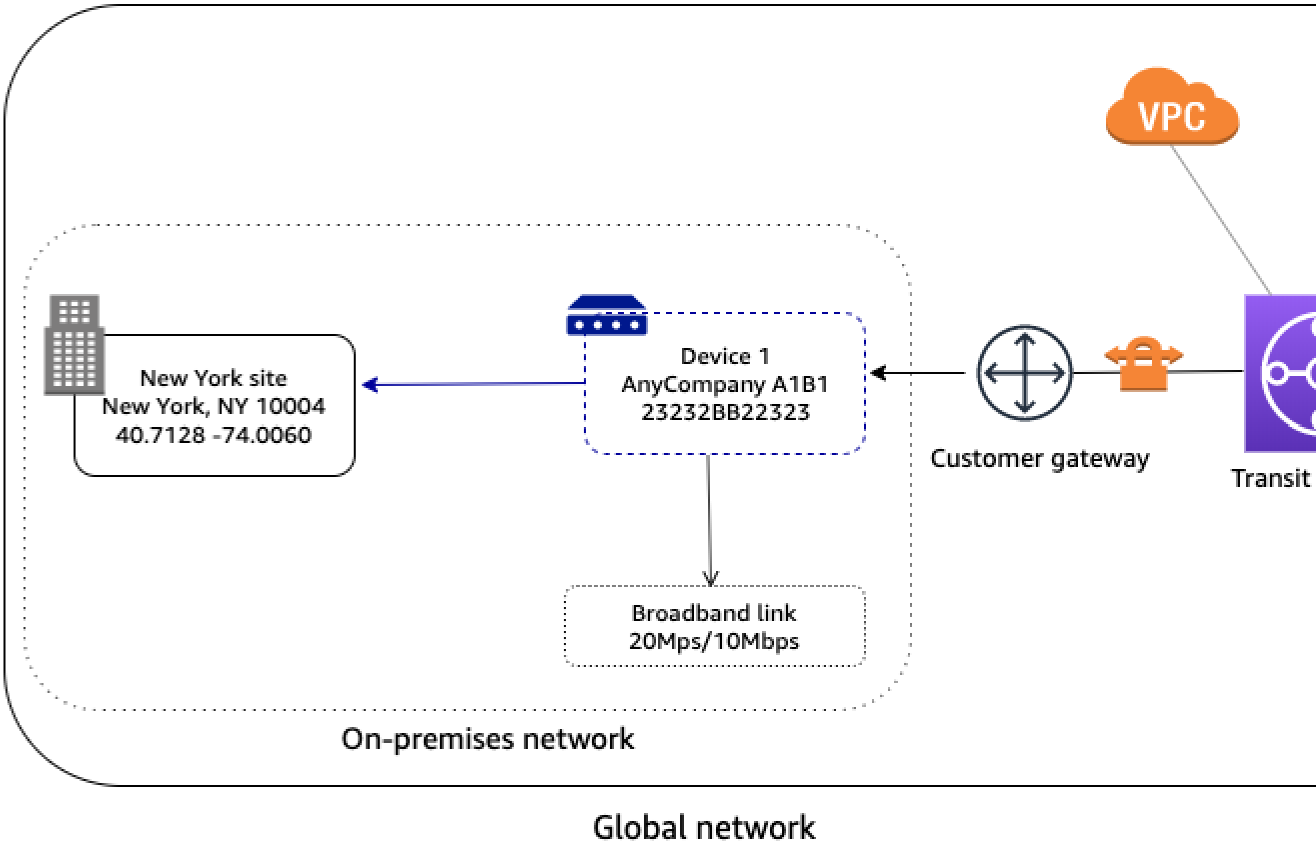
Defining and associating your on-premises network

To represent your on-premises network, you add *devices*, *links*, and *sites* to your global network. A site represents the physical location of your branch, office, store, campus, data center, and so on. When you add a site, you can specify the location information, including the physical address and coordinates.

A device represents the physical or virtual appliance that establishes connectivity with a transit gateway over an IPsec tunnel. A link represents a single outbound internet connection used by a device, for example, a 20 Mbps broadband link.

When you create a device, you can specify its physical location, and the site where it's located. A device can have a more specific location than the site, for example, a building in a campus or a floor in a building. When you create a link, you create it for a specific site. You can then associate a device with a link.

To connect your on-premises network to your AWS resources, associate a customer gateway that's in your global network with the device. In the following diagram, the on-premises network is connected to a transit gateway through a Site-to-Site VPN connection.



You can have multiple devices in a site, and you can associate a device with multiple links. For examples, see Scenarios for Transit Gateway Network Manager (p. 56).

You can work with one of our Partners in the AWS Partner Network (APN) to provision and connect your on-premises networks. For more information, see Transit Gateway Network Manager.

Network Manager quotas

Your AWS account has the following quotas related to Network Manager:

- Global networks per AWS account: 5
- Devices per global network: 200
- Links per global network: 200
- Sites per global network: 200

The Service Quotas console provides information about Network Manager quotas. You can use the Service Quotas console to view default quotas and request quota increases for adjustable quotas.

For more information about Site-to-Site VPN quotas, see Site-to-Site VPN Quotas in the *AWS Site-to-Site VPN User Guide*.

Getting started with Transit Gateway Network Manager

The following tasks help you become familiar with Transit Gateway Network Manager (Network Manager).

In this example, you create a global network and register your transit gateway with the global network. You can also define and associate your on-premises network resources with the global network.

Tasks

- Prerequisites (p. 55)
- Step 1: Create a global network (p. 55)
- Step 2: Register your transit gateway (p. 55)
- Step 3: (Optional) Define and associate your on-premises network resources (p. 56)
- Step 4: View and monitor your global network (p. 56)

Prerequisites

Before you begin, ensure that you have a transit gateway with attachments in your account. For more information, see Getting Started with Transit Gateways.

The transit gateway must be in the same AWS account as the global network.

Step 1: Create a global network

Create a global network as a container for your transit gateway.

To create a global network

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**.
3. Choose **Create global network**.
4. Enter a name and description for the global network, and choose **Create global network**.

Step 2: Register your transit gateway

Register your transit gateway in your global network.

To register the transit gateway

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**.
3. Choose the ID of your global network.
4. In the navigation pane, choose **Transit gateways**. Choose **Register transit gateway**.
5. Select the transit gateway in the list, and choose **Register transit gateway**.

Step 3: (Optional) Define and associate your on-premises network resources

You can define your on-premises network by creating sites, links, and devices to represent objects in your network. For more information, see the following procedures:

- Creating a site (p. 65)
- Creating a link (p. 66)
- Creating a device (p. 68)

You associate the device with a specific site, and with one or more links. For more information, see Device associations (p. 69).

Finally, create a Site-to-Site VPN connection attachment on your transit gateway, and associate the customer gateway with the device. For more information, see Customer gateway associations (p. 70).

You can also work with one of our Partners in the AWS Partner Network (APN) to provision and connect your on-premises network. For more information, see Transit Gateway Network Manager.

Step 4: View and monitor your global network

The Network Manager console provides a dashboard for you to view and monitor the network objects in your global network.

To access the dashboard for your global network

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**.
3. Choose the ID of your global network.
4. The **Overview** page provides an inventory of the objects in your global network. For more information about the pages in the dashboard, see Visualizing and monitoring your global network using the Network Manager console (p. 72).

Scenarios for Transit Gateway Network Manager

The following are common use cases and scenarios for Network Manager.

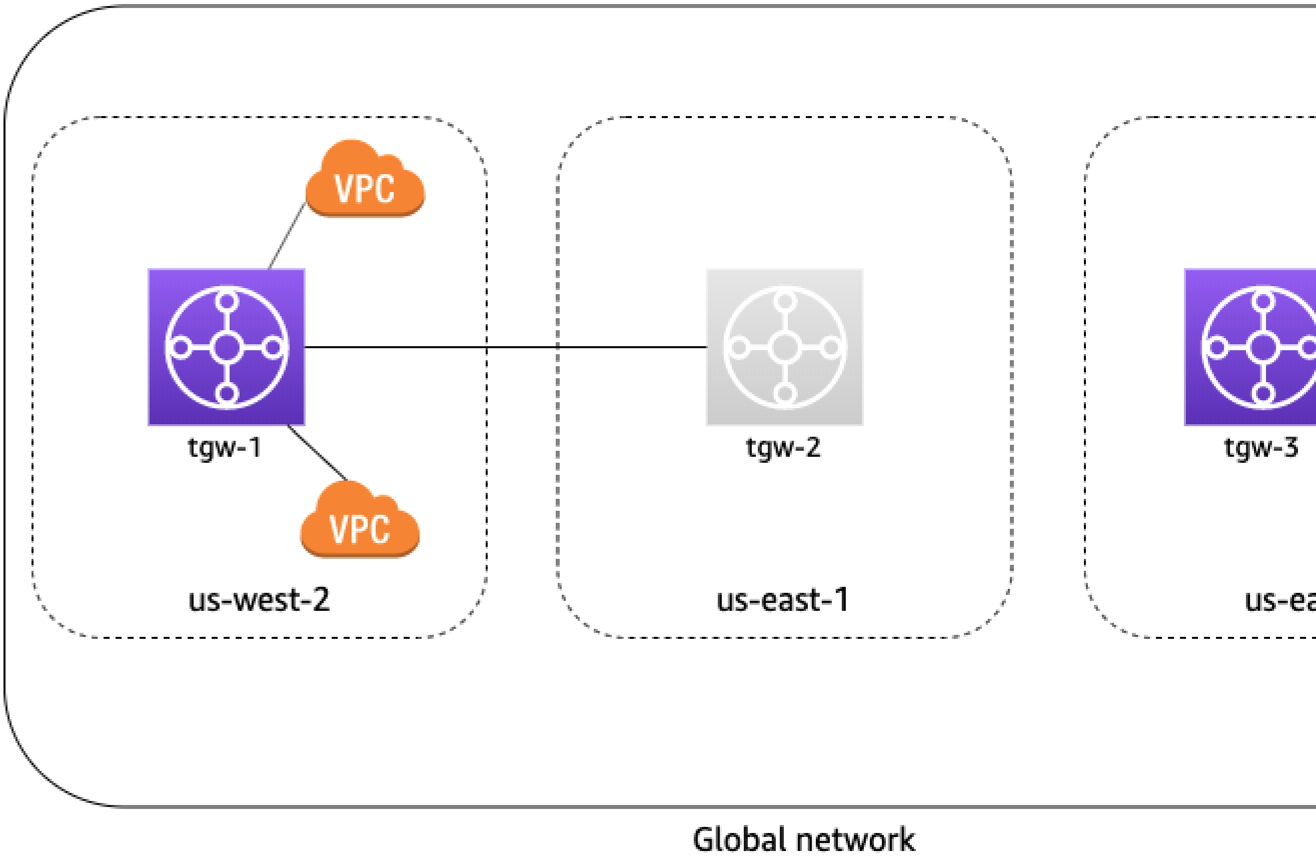
Topics

- AWS-only global network (p. 57)
- Single device with a single VPN connection (p. 57)
- Device with multiple VPN connections (p. 58)

- Multi-device and multi-link site (p. 59)
- SD-WAN connecting to AWS (p. 60)

AWS-only global network

In this scenario, your AWS network consists of three transit gateways. You own transit gateways `tgw-1` and `tgw-3`. Transit gateway `tgw-1` has a peering attachment with transit gateway `tgw-2` that's in a different AWS account. Your entire network is within AWS, and does not consist of on-premises resources.



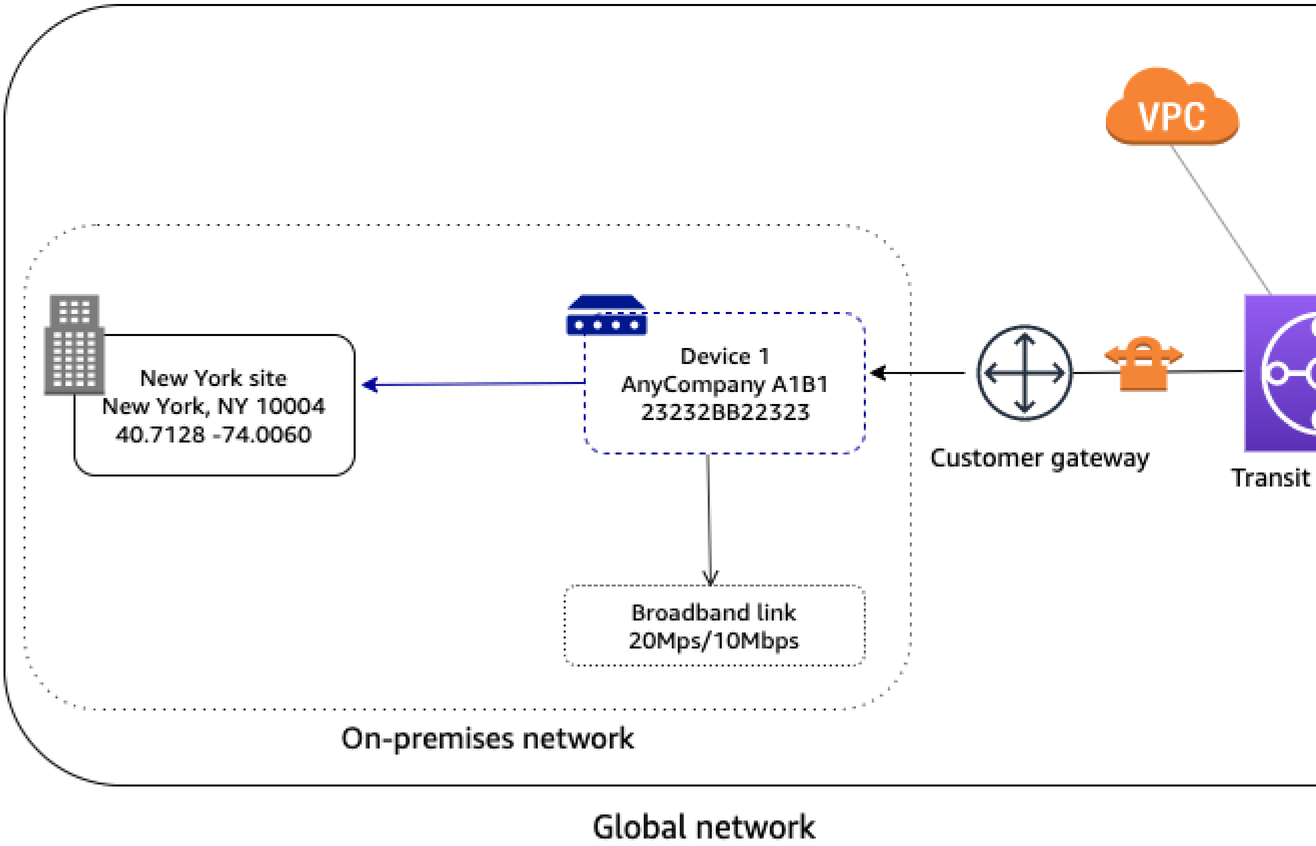
For this scenario, do the following in Network Manager:

- Create a global network. For more information, see Creating a global network (p. 62).
- Register the transit gateways `tgw-1` and `tgw-3` with your global network. For more information, see Registering a transit gateway (p. 64).

  When you register `tgw-1`, the transit gateway peering attachment is included in the global network and you can see information about `tgw-2`. However, any attachments for `tgw-2` are not included in your global network.

Single device with a single VPN connection

In the following scenario, your global network consists of a single site with a single device and link. The site is connected to your AWS network through a Site-to-Site VPN attachment on a transit gateway. Your transit gateway also has two VPC attachments.

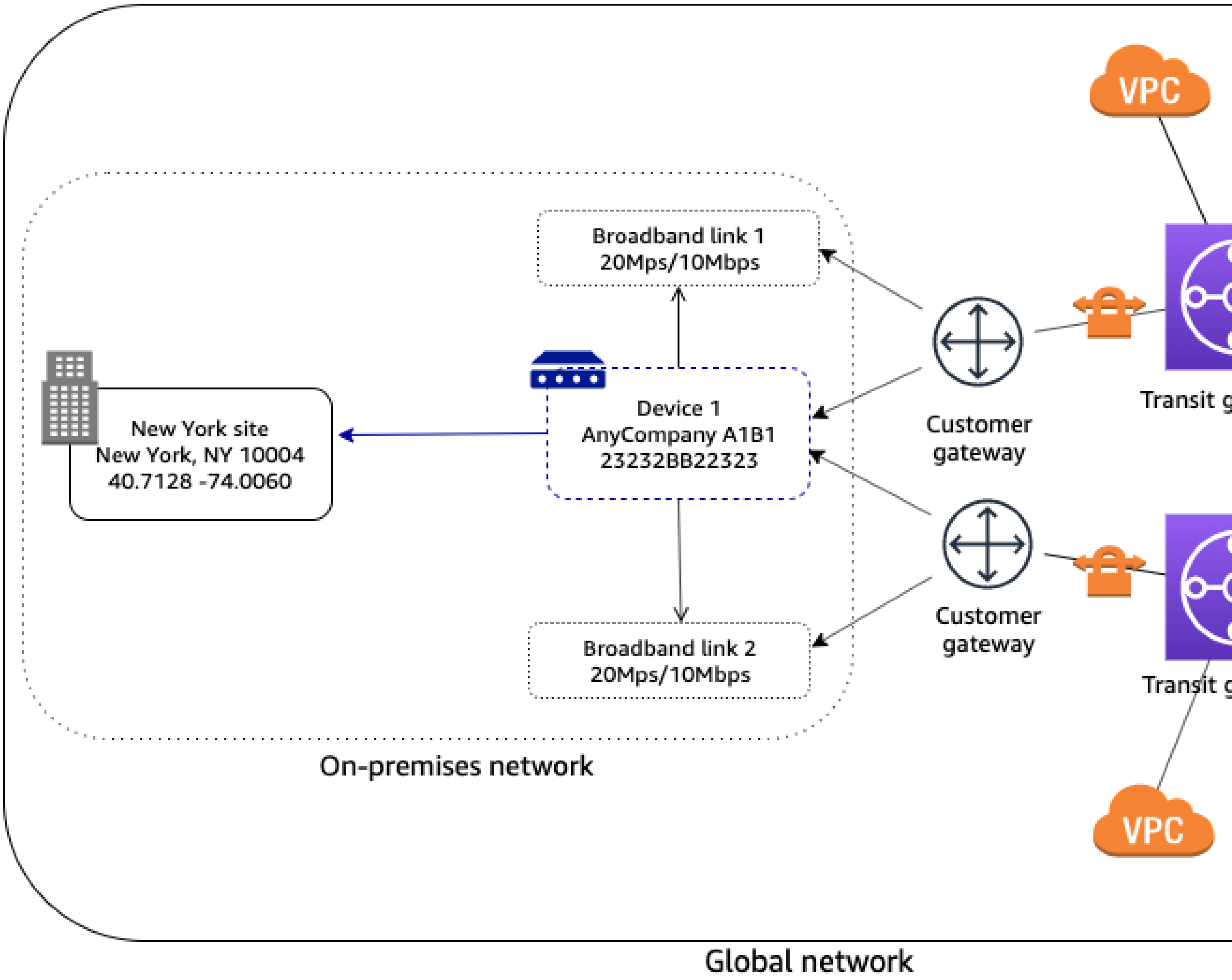


For this scenario, do the following in Network Manager:

- Create a global network. For more information, see Creating a global network (p. 62).
- Register the transit gateway. For more information, see Registering a transit gateway (p. 64).
- Create a site, device, and link. For more information, see Working with sites (p. 65), Working with devices (p. 68), and Working with links (p. 66).
- Associate the device with the site and with the link. For more information, see Device associations (p. 69).
- Associate the customer gateway (for the transit gateway Site-to-Site VPN attachment) with the device, and optionally, the link. For more information, see Customer gateway associations (p. 70).

Device with multiple VPN connections

In the following scenario, your on-premises network consists of a device with two Site-to-Site VPN connections to AWS. The device is associated with two customer gateways on two different transit gateways. Each VPN connection uses a separate link. To indicate which link applies to which VPN connection, you associate the customer gateway with both the device and the corresponding link.



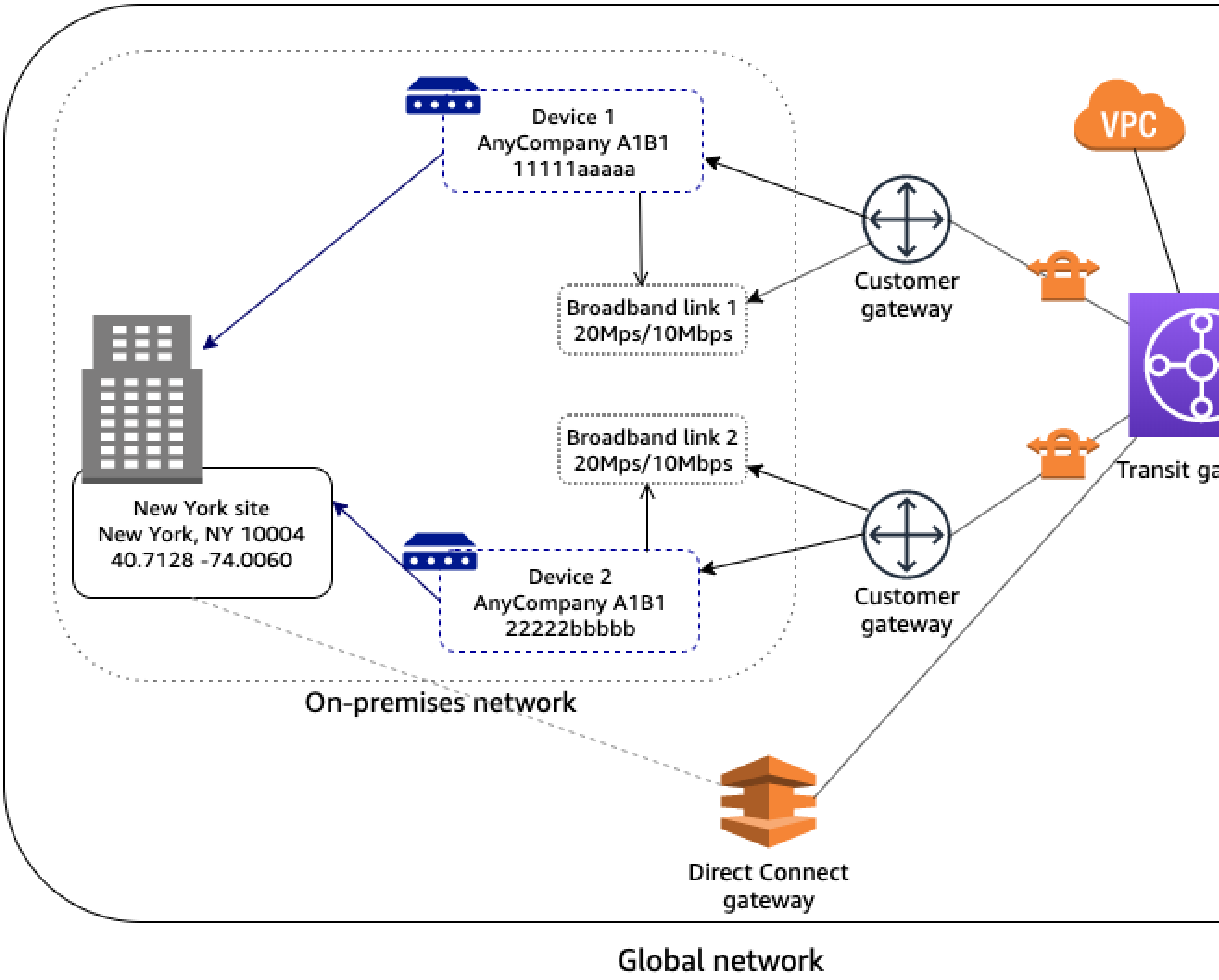
For this scenario, do the following in Network Manager:

- Create a global network. For more information, see Creating a global network (p. 62).
- Register the transit gateways. For more information, see Registering a transit gateway (p. 64).
- Create a site, device, and link. For more information, see Working with sites (p. 65), Working with devices (p. 68), and Working with links (p. 66).
- Associate the device with the site and both links. For more information, see Device associations (p. 69).
- Associate each customer gateway with the device and the corresponding link. For more information, see Customer gateway associations (p. 70).

Multi-device and multi-link site

In the following scenario, your on-premises network consists of a site with two devices and two separate Site-to-Site VPN connections to AWS. For example, in a single building or campus, you might have multiple devices connected to AWS resources. Each device is associated with a customer gateway that's attached to your transit gateway.

Your AWS network is also connected to your on-premises network though an AWS Direct Connect gateway, which is an attachment on your transit gateway.



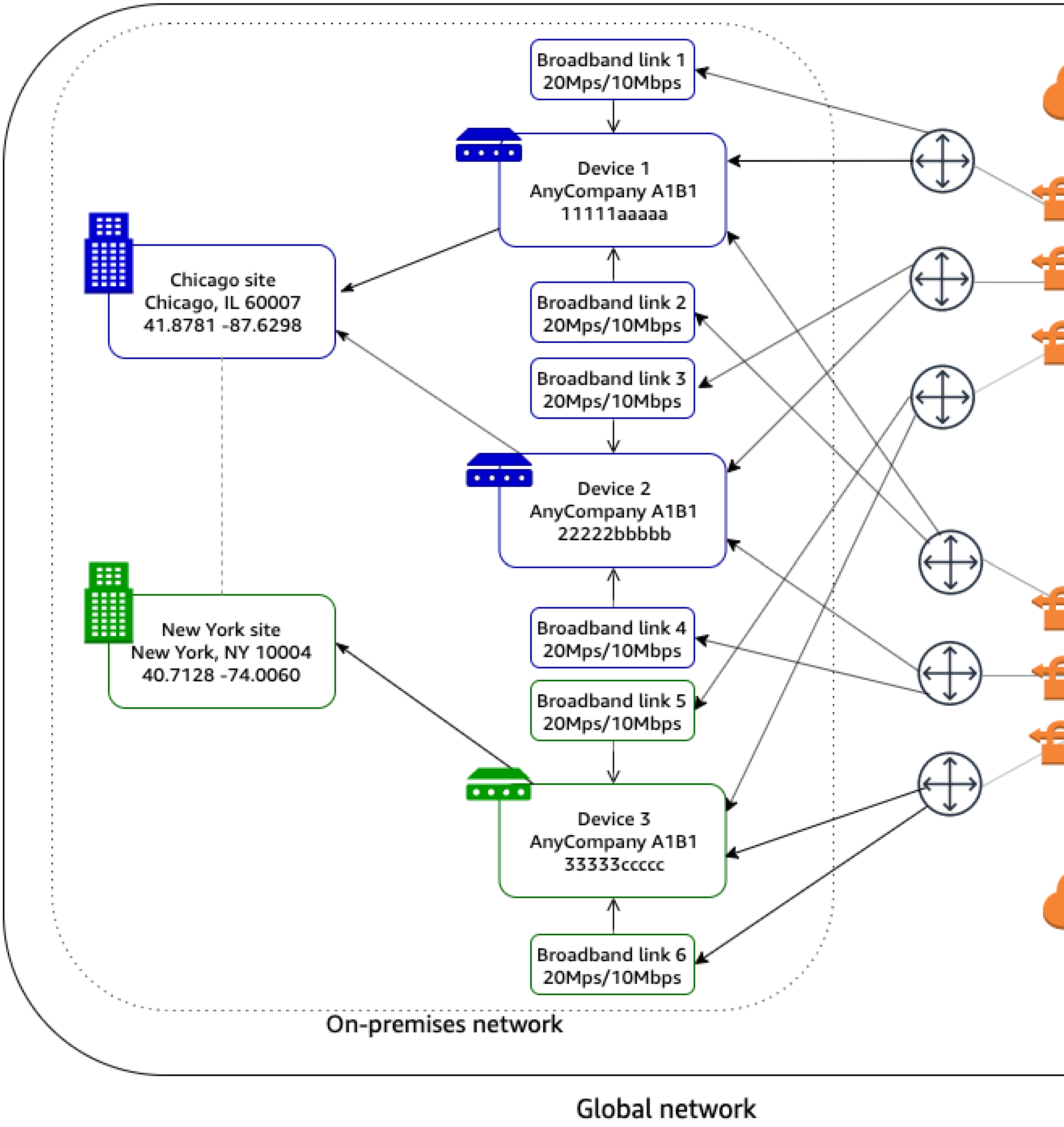
For this scenario, do the following in Network Manager:

- Create a global network. For more information, see Creating a global network (p. 62).
- Register the transit gateway. For more information, see Registering a transit gateway (p. 64).
- Create one site, two devices, and two links. For more information, see Working with sites (p. 65), Working with devices (p. 68), and Working with links (p. 66).
- Associate each device with the corresponding link. For more information, see Device associations (p. 69).
- Associate each customer gateway with the corresponding device and link. For more information, see Customer gateway associations (p. 70).

SD-WAN connecting to AWS

In the following example, your on-premises network consists of two sites. The Chicago site has two devices and the New York site has one device. Your AWS network consists of two transit gateways. All devices are associated with customer gateways (Site-to-Site VPN attachments) on both transit gateways.

Your on-premises network is managed using SD-WAN. The SD-WAN controller creates Site-to-Site VPN connections to the transit gateways, and creates the device, site, and link resources in Network Manager. This automates connectivity and enables you to get a full view of your network in Network Manager. The SD-WAN controller can also use Network Manager events and metrics to enhance its dashboard.



For more information about Partners who can help you set up your Site-to-Site VPN connections, see Transit Gateway Network Manager.

Working with Network Manager resources

You can work with Network Manager using the Network Manager console or the AWS CLI.

Contents

- Global networks (p. 62)
- Transit gateway registrations (p. 63)
- On-premises network (p. 65)

Global networks

A global network is a container for your network objects. When you create a global network, it's empty. After you create it, you can register your transit gateways and define your on-premises networks in the global network.

Topics

- Creating a global network (p. 62)
- Viewing a global network (p. 62)
- Updating a global network (p. 63)
- Deleting a global network (p. 63)

Creating a global network

Create a global network.

To create a global network

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**.
3. Choose **Create global network**.
4. Enter a name and description for the global network.
5. (Optional) Expand **Additional settings**. To add a tag, enter a **Key** and **Value** and choose **Add tag**.
6. Choose **Create global network**.

To create a global network using the AWS CLI

Use the create-global-network command.

Viewing a global network

You can view the details of your global network and information about the network objects in your global network.

To view your global network information

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**.
3. Choose the ID of your global network.
4. The **Overview** page contains information about the network objects in your global network. To view details about the global network resource (such as its ARN), choose **Details**. For more information

about the other pages on the dashboard, see Visualizing and monitoring your global network using the Network Manager console (p. 72).

To view global network details using the AWS CLI

Use the describe-global-networks command.

Updating a global network

You can modify the description or tags for a global network.

To update your global network

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**.
3. Choose your global network and choose **Edit**.
4. For **Description**, enter a new description for the global network.
5. For **Tags**, choose **Remove tag** to remove an existing tag, or choose **Add tag** to add a new tag.
6. Choose **Edit global network**.

To update a global network using the AWS CLI

Use the update-global-network command to update the description. Use the tag-resource and untag-resource commands to update the tags.

Deleting a global network

You cannot delete a global network if there are any network objects in the global network, including transit gateways, links, devices, and sites. You must first deregister or delete the network objects.

To delete your global network

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**.
3. Choose your global network and choose **Delete**.
4. In the confirmation dialog box, choose **Delete**.

To delete a global network using the AWS CLI

Use the delete-global-network command.

Transit gateway registrations

You can register your existing transit gateways with a global network. Any transit gateway attachments (such as VPCs, VPN connections, and AWS Direct Connect gateways) are automatically included in your global network.

You cannot create, delete, or modify your transit gateways and their attachments using the Network Manager console or APIs. To work with transit gateways, use the Amazon VPC console or the Amazon EC2 APIs.

You can register a transit gateway with one global network only. You can register transit gateways that are in the same AWS account as the global network.

Topics

- Registering a transit gateway (p. 64)
- Viewing your registered transit gateways (p. 64)
- Deregistering a transit gateway (p. 64)

Registering a transit gateway

Register a transit gateway with a global network. You cannot register a transit gateway with more than one global network.

To register a transit gateway

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**.
3. Choose the ID for your global network.
4. In the navigation pane, choose **Transit gateways**. Choose **Register transit gateway**.
5. Select the transit gateway in the list, and choose **Register transit gateway**.

To register a transit gateway using the AWS CLI

Use the register-transit-gateway command.

Viewing your registered transit gateways

View the registered transit gateways in your global network.

To view your registered transit gateways

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**.
3. Choose the ID for your global network.
4. In the navigation pane, choose **Transit gateways**.
5. The **Transit gateways** page lists your registered transit gateways. Choose the ID of transit gateway to view its details.

To view your registered transit gateways using the AWS CLI

Use the get-transit-gateway-registrations command.

Deregistering a transit gateway

Deregister a transit gateway from a global network.

To deregister a transit gateway

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**.
3. Choose the ID for your global network.
4. In the navigation pane, choose **Transit gateways**.
5. Select your transit gateway, and choose **Deregister**.

To deregister a transit gateway using the AWS CLI

Use the deregister-transit-gateway command.

On-premises network

You can represent your on-premises network in your global network through sites, devices, and links. For more information, see Defining and associating your on-premises network (p. 54). You then associate a device with a site and one or more links.

To add your on-premises network to your global network, you associate a customer gateway with your device.

All sites, devices, and links are created for a specific global network and cannot be shared with other global networks.

Topics

- Working with sites (p. 65)
- Working with links (p. 66)
- Working with devices (p. 68)
- Device associations (p. 69)
- Customer gateway associations (p. 70)

Working with sites

The following procedures show you how to create, update, and delete sites.

Topics

- Creating a site (p. 65)
- Updating a site (p. 66)
- Deleting a site (p. 66)

Creating a site

Create a site to represent the physical location of your network. The location information is used for visualization in the Network Manager console.

To create a site

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**.
3. Choose the ID of your global network.
4. In the navigation pane, choose **Sites**. Choose **Create site**.
5. For **Name** and **Description**, enter a name and description for the site.
6. For **Address**, enter the physical address of the site, for example, `New York, NY 10004`.
7. For **Latitude**, enter the latitude coordinates for the site, for example, `40.7128`.
8. For **Longitude**, enter the longitude coordinates for the site, for example, `-74.0060`.
9. Choose **Create site**.

Creating and viewing a site using the AWS CLI

Use the following commands:

- To create a site: create-site
- To view your sites: get-sites

Updating a site

You can update the details of your site, including the description, address, latitude, and longitude.

To update your site

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**.
3. Choose the ID for your global network.
4. In the navigation pane, choose **Sites**, and select your site.
5. Choose **Edit**.
6. Update the description, address, latitude, longitude, and tags as needed.
7. Choose **Edit site**.

Updating a site using the AWS CLI

Use the update-site command.

Deleting a site

If you no longer need a site, you can delete it. You must first disassociate the site from any devices and delete any links for the site.

To delete a site

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**.
3. Choose the ID of your global network.
4. In the navigation pane, choose **Sites**.
5. Select the site and choose **Delete**.
6. In the confirmation dialog box, choose **Delete**.

Deleting a site using the AWS CLI

Use the delete-site command.

Working with links

The following procedures show you how to create, update, and delete links.

Topics

- Creating a link (p. 66)
- Updating a link (p. 67)
- Deleting a link (p. 67)

Creating a link

Create a link to represent an internet connection from a device. A link is created for a specific site, therefore you must create a site before you create a link.

To create a link

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**.
3. Choose the ID of your global network.
4. In the navigation pane, choose **Sites**. Choose the ID of the site for which to create the link, and the choose **Links**.
5. Choose **Create link**.
6. For **Name** and **Description**, enter a name and description for the link.
7. For **Upload speed**, enter the upload speed in Mbps.
8. For **Download speed**, enter the download speed in Mbps.
9. For **Provider**, enter the name of the service provider.
10. For **Type**, enter the type of link, for example, `broadband`.
11. Choose **Create link**.

Creating and viewing a link using the AWS CLI

Use the following commands:

- To create a link: create-link
- To view your links: get-links

Updating a link

You can update the details of your link, including the bandwidth information, description, provider, and type.

To update a link

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**.
3. Choose the ID of your global network.
4. In the navigation pane, choose **Sites** and choose the ID for the site. Choose **Links**.
5. Select the link and choose **Edit**.
6. Update the link details as needed, then choose **Edit link**.

Updating a link using the AWS CLI

Use the update-link command.

Deleting a link

If you no longer need a link, you can delete it. You must first disassociate the link from any devices and customer gateways.

To delete a link

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**.
3. Choose the ID of your global network.
4. In the navigation pane, choose **Sites** and choose the ID for the site. Choose **Links**.

5. Select the link and choose **Delete**.
6. In the confirmation dialog box, choose **Delete**.

Deleting a link using the AWS CLI

Use the delete-link command.

Working with devices

The following procedures show you how to create, update, and delete devices.

Topics

- Creating a device (p. 68)
- Updating a device (p. 68)
- Deleting a device (p. 69)

Creating a device

Create a device to represent a physical or virtual appliance.

To create a device

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**.
3. Choose the ID of your global network.
4. In the navigation pane, choose **Devices**. Choose **Create device**.
5. For **Name** and **Description**, enter a name and description for the device.
6. For **Model**, enter the device model number.
7. For **Serial number**, enter the serial number for the device.
8. For **Type**, enter the device type.
9. For **Vendor**, enter the name of the vendor, for example, `Cisco`.
10. For **Address**, enter the physical address of the site, for example, `New York, NY 10004`.
11. For **Latitude**, enter the latitude coordinates for the site, for example, `40.7128`.
12. For **Longitude**, enter the longitude coordinates for the site, for example, `-74.0060`.
13. Choose **Create device**.

Creating and viewing a device using the AWS CLI

Use the following commands:

- To create a device: create-device
- To view your devices: get-devices

Updating a device

You can update the details of your device, including the description, model, serial number, type, vendor, and location information.

To update a device

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.

2. In the navigation pane, choose **Global networks**.
3. Choose the ID of your global network.
4. In the navigation pane, choose **Devices** and select the device.
5. Choose **Edit**.
6. Update the device details as needed, then choose **Edit device**.

Updating a device using the AWS CLI

Use the update-device command.

Deleting a device

If you no longer need a device, you can delete it. You must first disassociate the device from any sites, links, and customer gateways.

To delete a device

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**.
3. Choose the ID of your global network.
4. In the navigation pane, choose **Devices**.
5. Select the site and choose **Delete**.
6. In the confirmation dialog box, choose **Delete**.

Deleting a device using the AWS CLI

Use the delete-device command.

Device associations

You can associate a device with a site, and a device with one or more links.

Topics

- Device and site associations (p. 69)
- Device and link associations (p. 70)

Device and site associations

A site can have multiple devices associated with it, but a device can only be associated with a single site.

To associate a device and site

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**.
3. Choose the ID of your global network.
4. In the navigation pane, choose **Devices**, and choose the ID of your device.
5. Choose **Associate site**.
6. For **Site**, choose the name of your site from the list.
7. Choose **Edit site association**.

You can remove the association between a device and a site.

To disassociate a device and site

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**.
3. Choose the ID of your global network.
4. In the navigation pane, choose **Devices**, and choose the ID of your device.
5. Choose **Disassociate site**.

Working with device and site associations using the AWS CLI

When you create a new device using the create-device AWS CLI command, you can specify the site to associate with the device. For an existing device, you can use the update-device AWS CLI command to associate or disassociate a site.

Device and link associations

A link can be associated with more than one device. The device must be associated with a site.

To associate a link and a device

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**.
3. Choose the ID of your global network.
4. In the navigation pane, choose **Devices**, and choose the ID of your device.
5. Choose **Links**.
6. Choose **Associate link**.
7. Choose the link to associate, then choose **Associate link**.

You can remove the association between a link and a device.

To disassociate a link and a device

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**.
3. Choose the ID of your global network.
4. In the navigation pane, choose **Devices**, and choose the ID of your device.
5. Choose **Links**.
6. Select the link and choose **Disassociate**.

Working with device and link associations using the AWS CLI

You can work with device associations using the following commands.

- To associate a link with a device: associate-link
- To view your link associations: get-link-associations
- To disassociate a link from a device: disassociate-link

Customer gateway associations

You can associate a customer gateway with your on-premises network by associating it with a device, and optionally, a link. The customer gateway must already be in your global network as part of a VPN attachment in your transit gateway. If you specify a link, it must already be associated with the specified device.

For more information about creating a customer gateway, see Create a Customer Gateway in the *AWS Site-to-Site VPN User Guide*. For more information about creating a VPN attachment to a transit gateway, see Transit Gateway VPN Attachments in *Amazon VPC Transit Gateways*.

You can associate a customer gateway with a device and link in one of the following ways:

- On the **Transit gateways** page
- On the **Devices** page

Transit gateways page

To associate a customer gateway using the Transit gateways page

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**.
3. Choose the ID of your global network.
4. In the navigation pane, choose **Transit gateways**, and then choose the ID of your transit gateway.
5. Choose **On-premises associations**.
6. Select your customer gateway and choose **Associate**.
7. For **Device**, select the ID of the device to associate. For **Link**, select the ID of the link to associate.
8. Choose **Edit on-premises association**.

Devices page

To associate a customer gateway using the Devices page

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**.
3. Choose the ID of your global network.
4. In the navigation pane, choose **Devices**, and then choose the ID of your device.
5. Choose **On-premises associations**.
6. Choose **Associate**.
7. For **Customer gateway**, select the ID of the customer gateway to associate. For **Link**, select the ID of the link to associate.
8. Choose **Create on-premises association**.

You can disassociate a customer gateway from a device or link in one of the following ways:

- On the **Transit gateways** page
- On the **Devices** page

Transit gateways page

To disassociate a customer gateway using the Transit gateways page

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.

2. In the navigation pane, choose **Global networks**.
3. Choose the ID of your global network.
4. In the navigation pane, choose **Transit gateways**, and then choose **On-premises associations**.
5. Select your customer gateway and choose **Disassociate**.

Devices page

To disassociate a customer gateway using the Devices page

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**.
3. Choose the ID of your global network.
4. In the navigation pane, choose **Devices**, and then choose the ID of your device.
5. Choose **On-premises associations**.
6. Select your customer gateway and choose **Disassociate**.

Working with customer gateway associations using the AWS CLI

You can work with customer gateway associations using the following commands.

- To associate a customer gateway with a device and link: associate-customer-gateway
- To view your customer gateway associations: get-customer-gateway-associations
- To disassociate a customer gateway from a device and link: disassociate-customer-gateway

Visualizing and monitoring your global network using the Network Manager console

The Network Manager console provides a dashboard that enables you to visualize and monitor your global network. It includes information about the resources in your global network, their geographic location, the network topology, Amazon CloudWatch metrics and events, and enables you to perform route analysis.

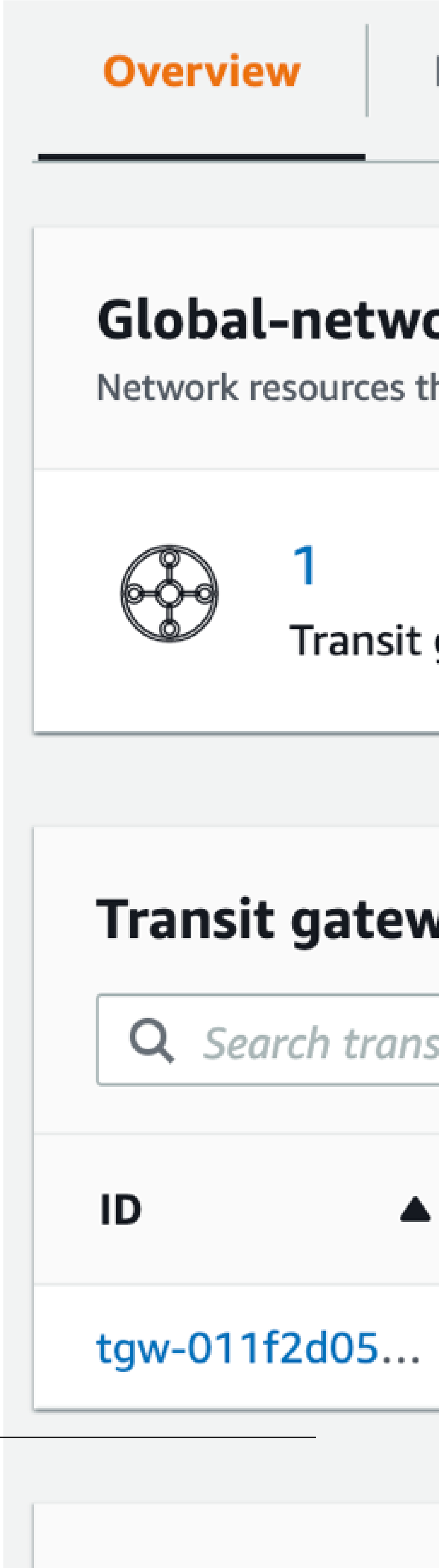
To access the dashboard for your global network

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. Choose the ID for your global network.

Topics

- Overview (p. 73)
- Details (p. 74)
- Geographic (p. 75)
- Topology (p. 76)
- Events (p. 77)
- Monitoring (p. 77)
- Route Analyzer (p. 77)

Overview



Overview

Global-netwo

Network resources th

1

Transit g

Transit gatew

Search trans

ID ▲

tgw-011f2d05…

On the **Overview** page, you can view the following information:

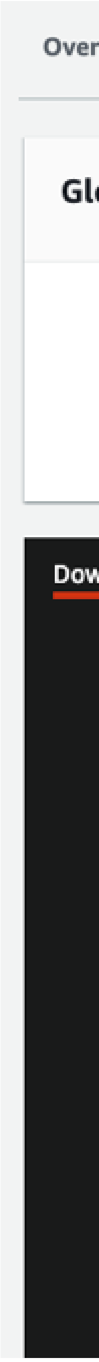
- The inventory of your global network.
- A list of the transit gateways that are registered in your global network, and the overall status of the VPN connection attachments for those transit gateways. To visualize and monitor an individual transit gateway, choose the transit gateway ID, or choose **Transit gateways** in the navigation pane.
- A summary of network events, for example, topology changes in your global network.

Details

On the **Details** page, you can view information about the global network resource, including the following:

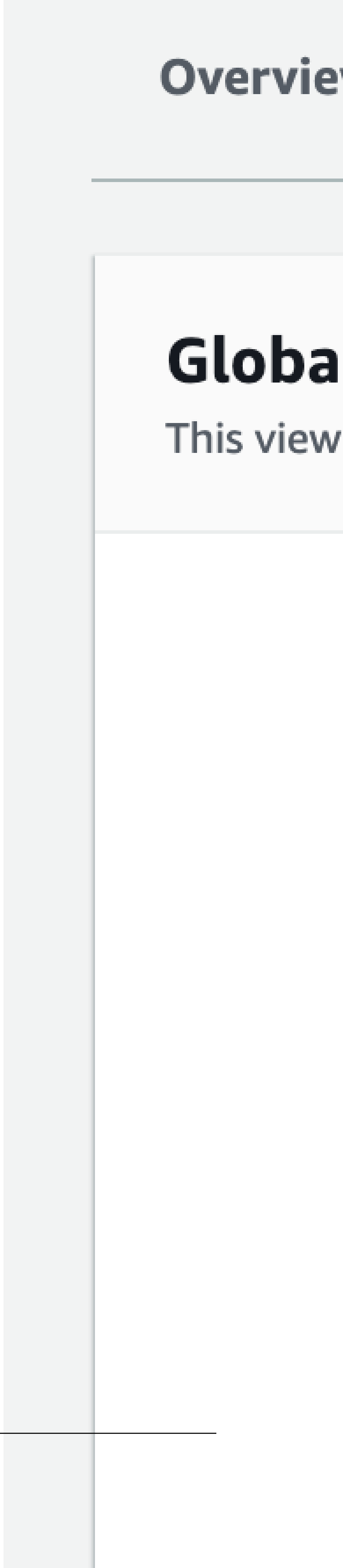
- The Amazon Resource Name (ARN)
- The name and description
- The state
- The AWS account ID
- The assigned tags

Geographic



On the **Geographic** page, you can view the locations of the resources that are registered in your global network on a map. Lines on the map represent connections between the resources, and the line colors represent the type of connection and their state. You can choose any of the location points to view information about the resources in that location.

Topology



Overvie

Globa

This view

On the **Topology** page, you can view the network tree for your global network. By default, the page displays all resources in your global network and the logical relationships between them. You can filter the network tree by resource type, and you can choose any of the nodes to view information about the specific resource it represents. The line colors represent the state of the relationships between AWS and the on-premises resources.

Events

On the **Events** page, you can view the system events that describe changes in your global network. For more information, see Monitoring your global network with CloudWatch Events (p. 79).

Monitoring

On the **Monitoring** page, you can view CloudWatch metrics for the transit gateways, VPN connections, and on-premises resources in your global network. For more information, see Monitoring your global network with Amazon CloudWatch metrics (p. 77).

Route Analyzer

On the **Route Analyzer** page, you can perform an analysis of the routes in your transit gateway route tables. This enables to you visualize routing paths and troubleshoot route-related connectivity issues. For more information, see Route Analyzer (p. 83).

Using Amazon CloudWatch metrics and events with your global network

AWS provides the following monitoring tools to watch the resources in your global network, report when something is wrong, and take automatic actions when appropriate.

- *Amazon CloudWatch* monitors your AWS resources and the applications that you run on AWS in real time. You can collect and track metrics, create customized dashboards, and set alarms that notify you or take actions when a specified metric reaches a threshold that you specify. For more information, see the Amazon CloudWatch User Guide.
- *Amazon CloudWatch Events* delivers a near-real-time stream of system events that describe changes in AWS resources. CloudWatch Events enables automated event-driven computing, as you can write rules that watch for certain events and trigger automated actions in other AWS services when these events happen. For more information, see the Amazon CloudWatch Events User Guide.

Monitoring your global network with Amazon CloudWatch metrics

You can monitor Network Manager using CloudWatch, which collects raw data and processes it into readable, near-real-time metrics. These statistics are kept for 15 months, so that you can access historical information and gain a better perspective on how your web application or service is performing. You can also set alarms that watch for certain thresholds, and send notifications or take actions when those thresholds are met. For more information, see the Amazon CloudWatch User Guide.

You can view CloudWatch metrics in your global network for your registered transited gateways, your associated Site-to-Site VPN connections, and your on-premises resources. You can view metrics per transit gateway, per global network.

For more information about the supported metrics, see the following topics:

- CloudWatch metrics for your transit gateways
- Monitoring VPN tunnels using Amazon CloudWatch
- CloudWatch metrics for on-premises resources (p. 78)

For examples of creating alarms, see Creating Amazon CloudWatch Alarms in the *Amazon CloudWatch User Guide*.

CloudWatch metrics for on-premises resources

Network Manager publishes data points to Amazon CloudWatch for your on-premises resources, including devices and links. CloudWatch enables you to retrieve statistics about those data points as an ordered set of time series data, known as metrics. Each data point has an associated timestamp and an optional unit of measurement.

You can use metrics to verify that your system is performing as expected. For example, you can create a CloudWatch alarm to monitor a specified metric and initiate an action (such as sending a notification to an email address) if the metric goes outside what you consider an acceptable range.

Device metrics

The `AWS/NetworkManager` namespace includes the following metrics for devices.

Metric	Description
`BytesIn`	The number of bytes received by the device.
`BytesOut`	The number of bytes sent by the device.
`VpnTunnelsDown`	The number of VPN tunnels on the device that have a DOWN status. Static VPN tunnels with a DOWN status, and BGP VPN tunnels with any state other than ESTABLISHED, are included in the count.

Metric dimensions for devices

To filter the metrics for your devices, use the following dimensions.

Dimension	Description
`DeviceId`	Filters the metric data by the device.

Link metrics

The `AWS/NetworkManager` namespace includes the following metrics for links.

Metric	Description
`BytesIn`	The number of bytes received by the on-premises network using this link.

Metric	Description
`BytesOut`	The number of bytes sent from the on-premises network using this link.

Metric dimensions for links

To filter the metrics for your links, use the following dimensions.

Dimension	Description
`LinkId`	Filters the metric data by the link.

Viewing global network CloudWatch metrics

There are various options for viewing CloudWatch metrics for your global network, including the following:

- Viewing metrics for the global network and filtering by transit gateway
- Viewing metrics for a specific transit gateway

To view metrics for your global network and filter by transit gateway

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**, and choose the ID for your global network.
3. Choose **Monitoring**. On this page, you can filter by transit gateway to view metrics for that transit gateway.

To view metrics for a specific transit gateway

1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.
2. In the navigation pane, choose **Global networks**, and choose the ID for your global network.
3. In the navigation pane, choose **Transit gateways**, and choose the ID for your transit gateway.
4. Choose **Monitoring**. On this page, you can view metrics for your transit gateway.

> **Note**
> On the **Monitoring** page, the **Add to dashboard** option only works if your registered transit gateway is in the US West (Oregon) Region.

Monitoring your global network with CloudWatch Events

CloudWatch Events delivers a near-real-time stream of system events that describe changes in your resources. Using simple rules that you can quickly set up, you can match events and route them to one or more target functions or streams. For more information, see the Amazon CloudWatch Events User Guide.

Transit Gateway Network Manager sends the following types of events to CloudWatch Events:

- Topology changes

- Routing updates
- Status updates

Getting started

Before you can view events for your global network, you must onboard to CloudWatch Logs Insights. In the Network Manager console, choose the ID of your global network. In the **Network events summary** section, choose **Onboard to CloudWatch Log Insights**.

An IAM principal in your account, such as an IAM user, must have sufficient permissions to onboard to CloudWatch Logs Insights. Ensure that the IAM policy contains the following permissions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "events:PutTargets",
                "events:DescribeRule",
                "logs:PutResourcePolicy",
                "logs:DescribeLogGroups",
                "logs:DescribeResourcePolicies",
                "events:PutRule",
                "logs:CreateLogGroup"
            ],
            "Resource": "*"
        }
    ]
}
```

The preceding policy does not grant permission to create, modify, or delete Network Manager resources. For more information about IAM policies for working with Network Manager, see Identity and access management for Transit Gateway Network Manager (p. 88).

When you onboard to CloudWatch Logs Insights, the following occurs:

- A CloudWatch event rule with the name `DON_NOT_DELETE_networkmanager_rule` is created in the US West (Oregon) Region.
- A CloudWatch Logs log group with the name `/aws/events/networkmanagerloggroup` is created in the US West (Oregon) Region.
- The CloudWatch event rule is configured with the CloudWatch Logs log group as a target.
- A CloudWatch resource policy with the name `DON_NOT_DELETE_networkmanager_TrustEventsToStoreLogEvents` is created in the US West (Oregon) Region. To view this policy, use the following AWS CLI command: `aws logs describe-resource-policies --region us-west-2`

To view events for your global network in the Network Manager console, choose the ID of your global network, and choose **Events**.

Topology change events

Topology change events occur when there have been changes to the resources in your global network. These events include the following:

- A transit gateway was registered in the global network
- A transit gateway was deregistered from the global network

- A transit gateway in the global network was deleted
- A VPN connection was created for a transit gateway
- A VPN connection was deleted on a transit gateway
- The customer gateway for a VPN connection was changed
- The target gateway for a VPN connection was changed
- A VPC was attached to a transit gateway
- A VPC was detached from a transit gateway
- An AWS Direct Connect gateway was attached to a transit gateway
- An AWS Direct Connect gateway was detached from a transit gateway
- A transit gateway peering connection attachment was created
- A transit gateway peering connection attachment was deleted

The following is an example of an event where a transit gateway VPC attachment was deleted (the VPC was detached from the transit gateway).

```
{
  "account": "123456789012",
  "region": "us-west-2",
  "detail-type": "Network Manager Topology Change",
  "source": "aws.networkmanager",
  "version": "0",
  "time": "2019-06-30T23:18:50Z",
  "id": "fb1d3015-c091-4bf9-95e2-d9example",
  "resources": [
     "arn:aws:networkmanager::123456789012:global-network/global-
network-08eb4a99cb6example",
     "arn:aws:ec2:us-east-1:123456789012:transit-gateway/tgw-11111111111122222"
  ],
  "detail": {
     "change-type": "VPC-ATTACHMENT-DELETED",
     "change-description": "A VPC attachment has been deleted.",
     "region": "us-east-1",
     "transit-gateway-arn": "arn:aws:ec2:us-east-1:123456789012:transit-gateway/
tgw-11111111111122222",
     "transit-gateway-attachment-arn": "arn:aws:ec2:us-east-1:123456789012:transit-gateway-
attachment/tgw-attach-012345678abc12345",
     "vpc-arn": "arn:aws:ec2:us-east-1:123456789012:vpc/vpc-11223344556677aab"
  }
}
```

Routing update events

Routing update events occur when there have been changes to the transit gateway route tables in your global network. These events include the following:

- A transit gateway attachment's route table association changed
- A route was created in a transit gateway route table
- A route was deleted in a transit gateway route table

The following is an example of an event where a transit gateway route table was associated with an attachment.

```
{
  "account": "123456789012",
  "region": "us-west-2",
  "detail-type": "Network Manager Routing Update",
  "source": "aws.networkmanager",
  "version": "0",
  "time": "2019-06-30T23:18:50Z",
  "id": "fb1d3015-c091-4bf9-95e2-d9852example",
  "resources": [
     "arn:aws:networkmanager::123456789012:global-network/global-
network-08eb4a99cb6example",
     "arn:aws:ec2:us-east-1:123456789012:transit-gateway/tgw-11111111111122222"
  ],
  "detail": {
     "change-type": "TGW-ROUTE-TABLE-ASSOCIATED",
     "change-description": "A Transit Gateway attachment has been associated to a route
 table.",
     "region": "us-east-1",
     "transit-gateway-arn": "arn:aws:ec2:us-east-1:123456789012:transit-gateway/
tgw-11111111111122222",
     "transit-gateway-attachment-arn": "arn:aws:ec2:us-east-1:123456789012:transit-gateway-
attachment/tgw-attach-012345678abc12345",
     "transit-gateway-route-table-arn": "arn:aws:ec2:us-east-1:123456789012:transit-
gateway-route-table/tgw-rtb--123abc123abc123ab"
  }
}
```

Status update events

Status update events occur when there have been changes to the status of the connectivity of your VPN connections in the global network. These events include the following:

- A VPN tunnel's IPsec session went down
- A VPN tunnel's IPsec session went up (after being down)
- A VPN tunnel's BGP session went down
- A VPN tunnel's BGP session went up (after being down)

The following is an example of an event where a VPN tunnel's IPsec session came up.

```
{
  "account": "123456789012",
  "region": "us-west-2",
  "detail-type": "Network Manager Status Update",
  "source": "aws.networkmanager",
  "version": "0",
  "time": "2019-06-30T23:18:50Z",
  "id": "fb1d3015-c091-4bf9-95e2-d98example",
  "resources": [
     "arn:aws:networkmanager::123456789012:global-network/global-
network-08eb4a99cb6example",
     "arn:aws:ec2:us-east-1:123456789012:vpn-connection/vpn-33333333333344444"
  ],
  "detail": {
     "status-change": "VPN-CONNECTION-IPSEC-UP",
     "change-description": "IPsec for a VPN connection has come up.",
     "region": "us-east-1",
     "transit-gateway-arn": "arn:aws:ec2:us-east-1:123456789012:transit-gateway/
tgw-11111111111122222",
     "transit-gateway-attachment-arn": "arn:aws:ec2:us-east-1:123456789012:transit-gateway-
attachment/tgw-attach-1122334455aaaaaaa",
     "vpn-connection-arn": "arn:aws:ec2:us-east-1:123456789012:vpn-connection/
vpn-33333333333344444",
     "outside-ip-address": "198.51.100.3"
  }
}
```

Route Analyzer

In your global network, you can use the Route Analyzer to perform an analysis of the routes in your transit gateway route tables. The Route Analyzer analyzes the routing path between a specified source and destination, and returns information about the connectivity between components. You can use the Route Analyzer to do the following:

- Verify that the transit gateway route table configuration will work as expected before you start sending traffic.
- Validate your existing route configuration.
- Diagnose route-related issues that are causing traffic disruption in your global network.

Topics

- Route Analyzer basics (p. 83)
- Performing a route analysis (p. 83)
- Example: Route analysis for peered transit gateways (p. 84)
- Example: Route analysis with a middlebox configuration (p. 86)

Route Analyzer basics

To use the Route Analyzer, you indicate the path for the traffic from a source to a destination. For the source, you specify the transit gateway, the transit gateway attachment from which the traffic originates, and a source IPv4 or IPv6 address. The Route Analyzer analyzes the routes in the associated transit gateway route table for the transit gateway attachment. For the destination, you specify a target IPv4 or IPv6 address, and the destination transit gateway and transit gateway attachment.

If you've configured a middlebox appliance in your VPC, you can indicate the location of the appliance in the route analysis. This enables you to specify multiple network hops in a route between a source and destination, to help you analyze the route of the traffic.

You can also analyze the return path for traffic from the specified destination back to the source.

The following rules apply when using the Route Analyzer:

- The Route Analyzer analyzes routes in transit gateway route tables only. It does not analyze routes in VPC route tables or in your customer gateway devices.
- The transit gateways must be registered in your global network.
- The Route Analyzer does not analyze security group rules or network ACL rules. To capture information about accepted and rejected IP traffic in your VPC, you can use VPC flow logs.
- The Route Analyzer only returns information for the return path if it can successfully return information for the forward path.

Performing a route analysis

To use the Route Analyzer, you must use the Network Manager console.

To analyze your routes

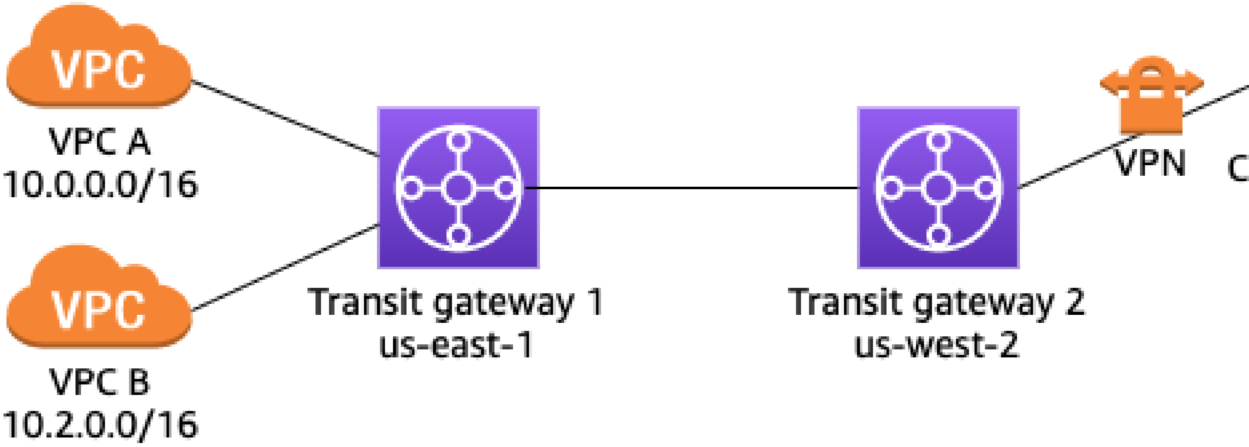
1. Open the Network Manager console at https://console.aws.amazon.com/networkmanager/.

2. Choose the ID for your global network, and then choose **Route Analyzer**.
3. Under **Source**, do the following:
   - Choose the transit gateway and the transit gateway attachment.
   - For **IP address**, enter a source IPv4 or IPv6 address.
4. Under **Destination**, do the following:
   - Choose the transit gateway and the transit gateway attachment.
   - For **IP address**, enter a target IPv4 or IPv6 address.
5. (Optional) To analyze the return path, ensure that you enable **Include return path in results**. If enabled, you must specify an IP address under **Source**.
6. To specify middlebox appliances in the routing path, choose **Middlebox appliance?**.
7. Choose **Run route analysis**.
8. The results are displayed under **Results of route analysis**. If you specified **Middlebox appliance?** in step 6, choose **Yes** or **No** for each of the attachments to indicate the location of the appliances and to complete the route analysis.

   You can choose the ID of any of the resources in the path to view more information about the resources.

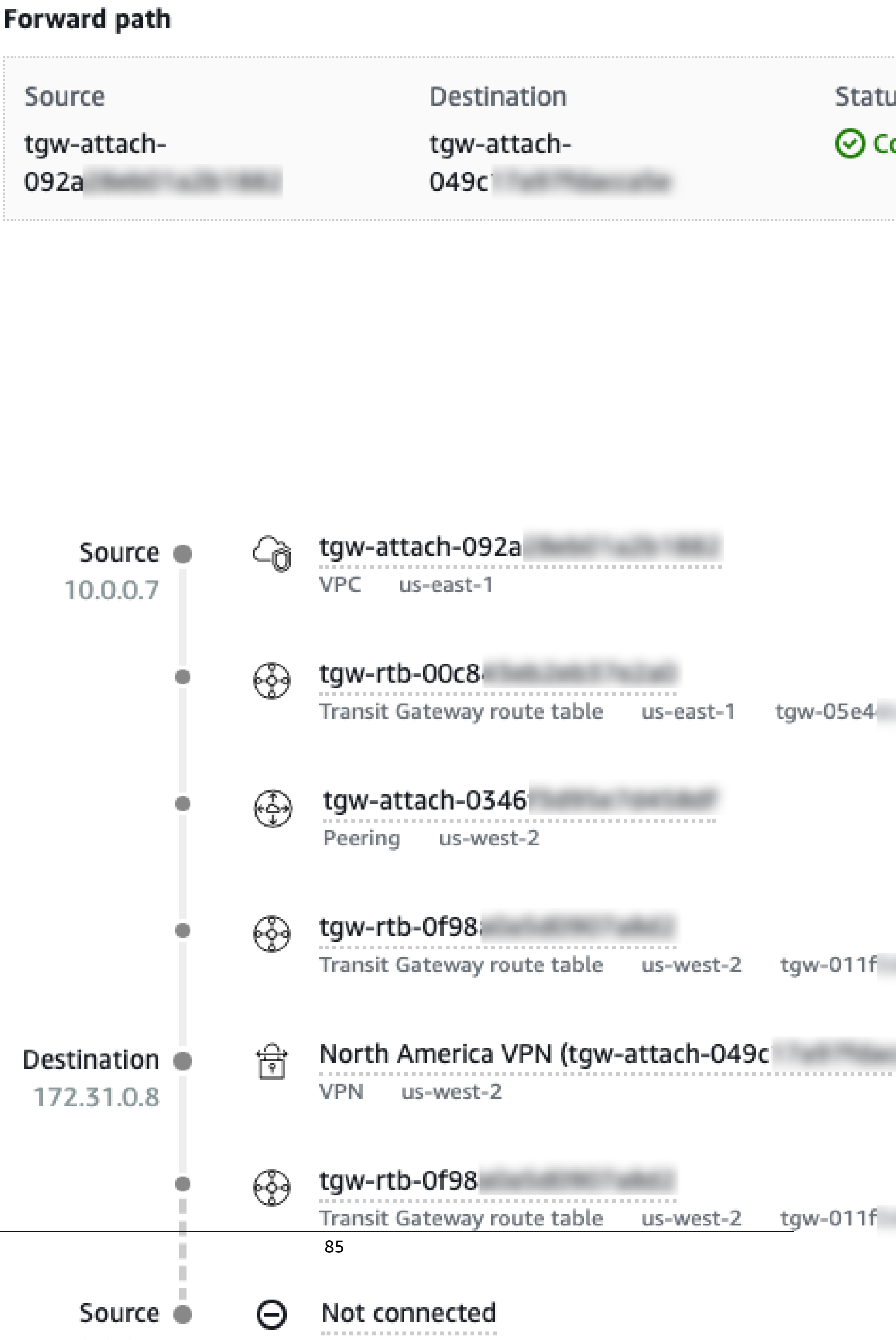
Example: Route analysis for peered transit gateways

In the following example, transit gateway 1 has two VPC attachments, and a peering attachment to transit gateway 2. Transit gateway 2 has a Site-to-Site VPN attachment to your on-premises network. You want to use the Route Analyzer to ensure that the VPCs and Site-to-Site VPN connections can route traffic to each other through the transit gateways.



In the Route Analyzer, do the following:

1. Under **Source**, specify transit gateway 1 and the transit gateway attachment for VPC A. Specify an IP address from the CIDR block of VPC A, for example, `10.0.0.7`.
2. Under **Destination**, specify transit gateway 2 and the VPN attachment. Specify an IP address from the range of the on-premises network, for example, `172.31.0.8`.
3. Ensure that **Include return path in results** is selected.
4. Run the route analysis. In the results, verify the path between the source and destination. For example, the following results indicate that there is a forward path from transit gateway 1 to transit gateway 2, but no return path. Check the route table for transit gateway 2, and ensure that there is a static route that points to the peering attachment.



Forward path

Source	Destination	Statu
tgw-attach-092a[redacted]	tgw-attach-049c[redacted]	✓ Co

Source 10.0.0.7 — tgw-attach-092a[redacted]
VPC us-east-1

tgw-rtb-00c8[redacted]
Transit Gateway route table us-east-1 tgw-05e4[redacted]

tgw-attach-0346[redacted]
Peering us-west-2

tgw-rtb-0f98[redacted]
Transit Gateway route table us-west-2 tgw-011f[redacted]

Destination 172.31.0.8 — North America VPN (tgw-attach-049c[redacted]
VPN us-west-2

tgw-rtb-0f98[redacted]
Transit Gateway route table us-west-2 tgw-011f[redacted]

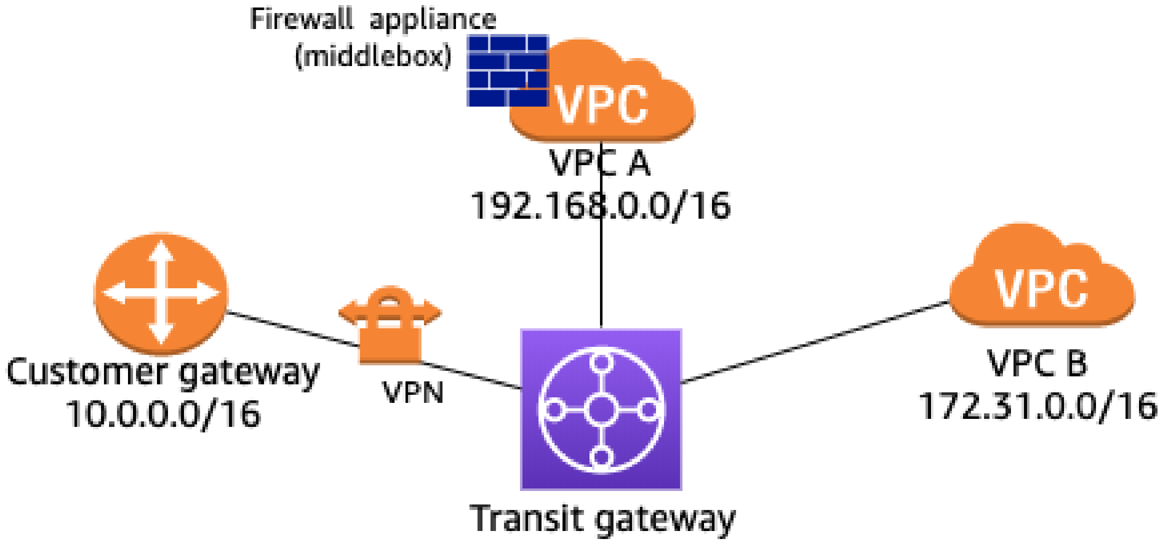
Source — Not connected

5. To run the analysis between VPC B and the VPN connection, modify the information under **Source**. Choose the transit gateway attachment for VPC B, and specify an IP address from the CIDR block of VPC B, for example, `10.2.0.9`.
6. Reload the results and verify the path between the source and destination.

For more information about the routing configuration for this scenario, see the transit gateway peering example (p. 15).

Example: Route analysis with a middlebox configuration

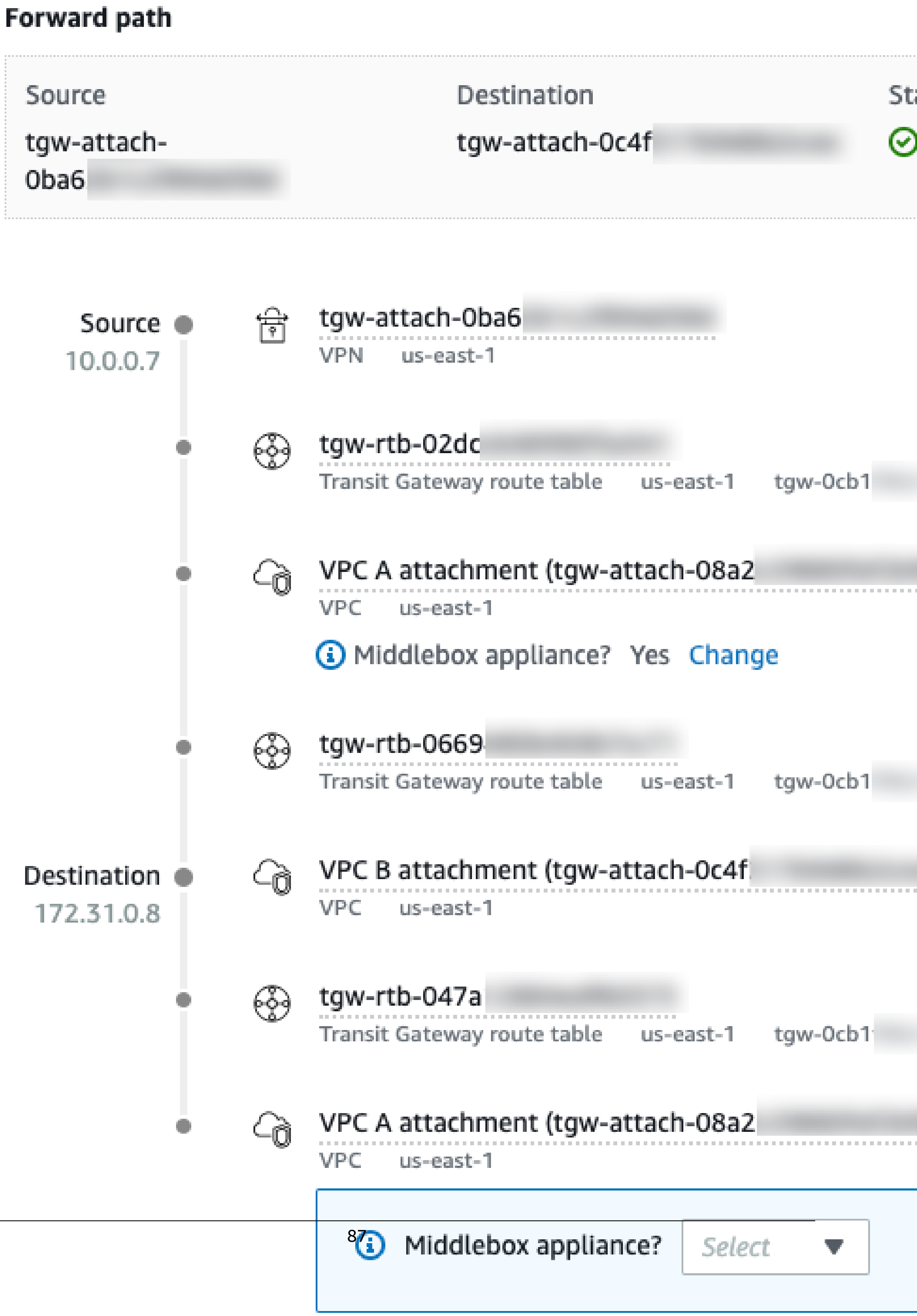
If you've configured a VPC to act as a middlebox appliance for inspecting traffic that flows to other parts of your network, you can indicate the location of the appliance in the route analysis. In the following example, the transit gateway has two VPC attachments and a VPN attachment. VPC A runs a firewall appliance (middlebox) that inspects the traffic that flows between the VPN connection and VPC B.



In the Route Analyzer, you can specify the location of the middlebox appliance as follows:

1. Under **Source**, specify the transit gateway and the VPN attachment. Specify an IP address from the range of the on-premises network, for example, `10.0.0.7`.
2. Under **Destination**, specify the transit gateway and the attachment for VPC B. Specify an IP address from the CIDR block of VPC B, for example, `172.31.0.8`.
3. For **Middlebox appliance?**, choose **Include**.
4. Run the route analysis.
5. For the **Middlebox appliance?** sections for the transit gateway attachment for VPC A, choose **Yes**.

   You can choose the ID of any resource in the path to view more information about that resource.



Forward path

Source: tgw-attach-0ba6[redacted]

Destination: tgw-attach-0c4f[redacted]

St

Source 10.0.0.7
tgw-attach-0ba6[redacted]
VPN us-east-1

tgw-rtb-02dc[redacted]
Transit Gateway route table us-east-1 tgw-0cb1[redacted]

VPC A attachment (tgw-attach-08a2[redacted]
VPC us-east-1
Middlebox appliance? Yes Change

tgw-rtb-0669[redacted]
Transit Gateway route table us-east-1 tgw-0cb1[redacted]

Destination 172.31.0.8
VPC B attachment (tgw-attach-0c4f[redacted]
VPC us-east-1

tgw-rtb-047a[redacted]
Transit Gateway route table us-east-1 tgw-0cb1[redacted]

VPC A attachment (tgw-attach-08a2[redacted]
VPC us-east-1

Middlebox appliance? Select ▼

Identity and access management for Transit Gateway Network Manager

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be *authenticated* (signed in) and *authorized* (have permissions) to use Transit Gateway Network Manager (Network Manager) resources. IAM is an AWS service that you can use with no additional charge. You can use features of IAM to allow other users, services, and applications to use your AWS resources fully or in a limited way, without sharing your security credentials.

By default, IAM users don't have permission to create, view, or modify AWS resources. To allow an IAM user to access resources, such as a global network, and perform tasks, you must:

- Create an IAM policy that grants the IAM user permission to use the specific resources and API actions they need
- Attach the policy to the IAM user or to the group to which the IAM user belongs

When you attach a policy to a user or group of users, it allows or denies the user permissions to perform the specified tasks on the specified resources.

Topics

- How Network Manager works with IAM (p. 88)
- Example policies to manage Transit Gateway Network Manager (p. 89)
- Transit Gateway Network Manager service-linked role (p. 92)

How Network Manager works with IAM

With IAM identity-based policies, you can specify allowed or denied actions and resources, and specify the conditions under which actions are allowed or denied. Network Manager supports specific actions, resources, and condition keys. For a complete list, see Actions, Resources, and Condition Keys for Network Manager in the *IAM User Guide*.

To learn about all of the elements that you use in a JSON policy, see IAM JSON Policy Elements Reference in the *IAM User Guide*.

Actions

Policy actions in Network Manager use the following prefix before the action: `networkmanager:`. For example, to grant someone permission to create a global network with the `CreateGlobalNetwork` API operation, you include the `networkmanager:CreateGlobalNetwork` action in their policy.

For a list of Network Manager actions, see the Network Manager API Reference.

Resources

The Resource element specifies the object or objects to which the action applies. Statements must include either a Resource or a NotResource element. You specify a resource using an ARN or using the wildcard (*) to indicate that the statement applies to all resources.

The global network resource has the following ARN.

```
arn:${Partition}:networkmanager::${Account}:global-network/${GlobalNetworkId}
```

For example, to specify the `global-network-1122334455aabbccd` global network in your statement, use the following ARN.

```
"Resource": "arn:aws:networkmanager::123456789012:global-network/global-
network-1122334455aabbccd"
```

For more information about the format of ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces.

Condition keys

The `Condition` element (or `Condition` *block*) lets you specify conditions in which a statement is in effect. The `Condition` element is optional. You can build conditional expressions that use condition operators, such as equals or less than, to match the condition in the policy with values in the request.

If you specify multiple `Condition` elements in a statement, or multiple keys in a single `Condition` element, AWS evaluates them using a logical `AND` operation. If you specify multiple values for a single condition key, AWS evaluates the condition using a logical `OR` operation. All of the conditions must be met before the statement's permissions are granted.

You can also use placeholder variables when you specify conditions. For example, you can grant an IAM user permission to access a resource only if it is tagged with their IAM user name. For more information, see IAM Policy Elements: Variables and Tags in the *IAM User Guide*.

You can attach tags to Network Manager resources or pass tags in a request to Network Manager. To control access based on tags, you provide tag information in the condition element of a policy using the `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, or `aws:TagKeys` condition keys.

To see all AWS global condition keys, see AWS Global Condition Context Keys in the *IAM User Guide*.

Network Manager also supports the following condition keys:

- `networkmanager:tgwArn`—Controls which transit gateways can be registered or deregistered in your global network.
- `networkmanager:cgwArn`—Controls which customer gateways can be associated or disassociated from devices and links in your global network.

Example policies to manage Transit Gateway Network Manager

The following are example IAM policies for working with Network Manager.

Administrator access

The following IAM policy grants full access to the Amazon EC2, Network Manager, AWS Direct Connect, and CloudWatch APIs. This enables administrators to create and manage transit gateways and their attachments (such as VPCs and AWS Direct Connect gateways), create and manage Network Manager resources, and monitor global networks using CloudWatch metrics and events. The policy also grants user permissions to create any required service-linked roles.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "networkmanager:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "cloudwatch:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "events:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "directconnect:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/*"
        }
    ]
}
```

Read-only access

The following IAM policy grants read-only access to the Amazon EC2, Network Manager, AWS Direct Connect, CloudWatch, and CloudWatch Events APIs. This enables users to use the Network Manager console to view and monitor global networks and their associated resources, and view metrics and events for the resources. Users cannot create or modify any resources.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:Get*",
                "ec2:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "networkmanager:Get*",
                "networkmanager:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:List*",
                "cloudwatch:Get*",
                "cloudwatch:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:Describe*",
                "logs:Get*",
                "logs:List*",
                "logs:StartQuery",
                "logs:StopQuery",
                "logs:TestMetricFilter",
                "logs:FilterLogEvents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "events:List*",
                "events:TestEventPattern",
                "events:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "directconnect:Describe*",
            "Resource": "*"
        }
    ]
}
```

Controlling the use of transit gateways and customer gateways

The following IAM policy enables users to work with Network Manager resources, but they are explicitly denied permission to do the following:

- Register or deregister a specific transit gateway (`tgw-aabbccdd112233445`) in the global network.
- Associate or disassociate a specific customer gateway (`cgw-11223344556677abc`) in the global network.

The policy uses the `networkmanager:tgwArn` and `networkmanager:cgwArn` condition keys to enforce these conditions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "networkmanager:*"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Deny",
            "Action": [
                "networkmanager:RegisterTransitGateway",
                "networkmanager:DeregisterTransitGateway"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "networkmanager:tgwArn": "arn:aws:ec2:<region>:<account-id>:transit-
gateway/tgw-aabbccdd112233445"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": [
                "networkmanager:AssociateCustomerGateway",
                "networkmanager:DisassociateCustomerGateway"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "networkmanager:cgwArn": "arn:aws:ec2:<region>:<account-id>:customer-
gateway/cgw-11223344556677abc"
                }
            }
        }
    ]
}
```

Transit Gateway Network Manager service-linked role

Network Manager uses service-linked roles for the permissions that it requires to call other AWS services on your behalf. For more information about service-linked roles, see Using Service-Linked Roles in the *IAM User Guide*.

Permissions granted by the service-linked role

Network Manager uses the service-linked role named **AWSServiceRoleForNetworkManager** to call the actions on your behalf when you work with global networks. The following IAM policy is attached to the role.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "directconnect:DescribeConnections",
                "directconnect:DescribeDirectConnectGatewayAttachments",
                "directconnect:DescribeLocations",
                "directconnect:DescribeVirtualInterfaces",
                "ec2:DescribeCustomerGateways",
                "ec2:DescribeTransitGatewayAttachments",
                "ec2:DescribeTransitGatewayRouteTables",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeVpnConnections",
                "ec2:GetTransitGatewayRouteTableAssociations",
                "ec2:SearchTransitGatewayRoutes"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Create the service-linked role

You don't need to manually create the **AWSServiceRoleForNetworkManager** role. Network Manager creates this role for you when you create your first global network.

For Network Manager to create a service-linked role on your behalf, you must have the required permissions. For more information, see Service-Linked Role Permissions in the *IAM User Guide*.

Edit the service-linked role

You can edit the description of **AWSServiceRoleForNetworkManager** using IAM. For more information, see Editing a Service-Linked Role in the *IAM User Guide*.

Delete the service-linked role

If you no longer need to use Network Manager, we recommend that you delete the **AWSServiceRoleForNetworkManager** role.

You can delete this service-linked role only after you delete your global network.

You can use the IAM console, the IAM CLI, or the IAM API to delete service-linked roles. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

After you delete **AWSServiceRoleForNetworkManager**, Network Manager will create the role again when you create a new global network.

Tagging your Network Manager resources

A *tag* is a metadata label that either you or AWS assigns to an AWS resource. Each tag consists of a *key* and a *value*. For tags that you assign, you define the key and the value. For example, you might define the key as `purpose` and the value as `test` for one resource.

Tags help you do the following:

- Identify and organize your AWS resources. Many AWS services support tagging, so you can assign the same tag to resources from different services to indicate that the resources are related.
- Control access to your AWS resources. For more information, see Controlling Access Using Tags in the IAM User Guide.

Supported resources

The following Network Manager resources support tagging:

- Global networks
- Devices
- Sites
- Links

Tagging restrictions

The following basic restrictions apply to tags on Network Manager resources:

- Maximum number of tags that you can assign to a resource: 200
- Maximum key length: 128 Unicode characters
- Maximum value length: 256 Unicode characters
- Valid characters for key and value: a-z, A-Z, 0-9, space, and the following characters: _ . : / = + - and @
- Keys and values are case sensitive
- You cannot use `aws:` as a prefix for keys; it's reserved for AWS use

Logging Transit Gateway Network Manager API calls with AWS CloudTrail

Transit Gateway Network Manager (Network Manager) works together with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Network Manager. CloudTrail captures all API calls for Network Manager as events. The calls that are captured include calls from the Network Manager console and code calls to the Network Manager API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Network Manager. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to Network Manager, the IP address from which the request was made, who made the request, when it was made, and additional details.

To learn more about CloudTrail, see the AWS CloudTrail User Guide.

Network Manager information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in Network Manager, that activity is recorded in a CloudTrail event along with other AWS service events in **Event history**. You can view, search, and download recent events in your AWS account. For more information, see Viewing Events with CloudTrail Event History.

For an ongoing record of events in your AWS account, including events for Network Manager, create a trail. A *trail* enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all Regions in the AWS partition, and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following:

- Overview for Creating a Trail
- CloudTrail Supported Services and Integrations
- Configuring Amazon SNS Notifications for CloudTrail
- Receiving CloudTrail Log Files from Multiple Regions and Receiving CloudTrail Log Files from Multiple Accounts

All Network Manager actions are logged by CloudTrail and are documented in the Network Manager API Reference. For example, calls to the `CreateGlobalNetwork` action generate entries in the CloudTrail log files.

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials

- Whether the request was made with temporary security credentials for a role or federated user
- Whether the request was made by another AWS service

For more information, see the CloudTrail userIdentity Element.

Document history for transit gateways

The following table describes the releases for transit gateways.

Feature	Description	Release date
Network Manager Route Analyzer	You can analyze the routes in your transit gateway route tables in your global network. For more information, see Route Analyzer (p. 83).	2020-05-04
Transit Gateway Network Manager	You can visualize and monitor your global networks that are built around transit gateways. For more information, see Transit Gateway Network Manager (p. 52).	2019-12-03
Peering attachments	You can create a peering connection with a transit gateway in another AWS Region. For more information, see Transit gateway peering attachments (p. 24).	2019-12-03
Multicast support	Transit Gateway supports routing multicast traffic between subnets of attached VPCs and serves as a multicast router for instances sending traffic destined for multiple receiving instances. For more information, see the section called "Multicast on transit gateways" (p. 31).	2019-12-03
AWS Direct Connect Support for AWS Transit Gateway	You can use an *AWS Direct Connect gateway* to connect your AWS Direct Connect connection over a transit virtual interface to the VPCs or VPNs attached to your transit gateway You associate a Direct Connect gateway with the transit gateway Then, create a transit virtual interface for your AWS Direct Connect connection to the Direct Connect gateway. For information, see the section called "Transit gateway attachments to a Direct Connect gateway" (p. 22).	2019-03-27
Initial release	This release introduces transit gateways.	26 November 2018