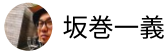


Transit Gatewayを利用してVPC間で通信してみた

Transit Gatewayは複数VPCや、オンプレミスを単一のゲートウェイで接続可能にするサービスです。Transit Gatewayの理解を深めるために、Transit Gatewayの用語を交えつつ、シンプルな構成で実際に構築してみたいと思います。

#Amazon VPC

#AWS



坂巻一義

2019.10.07



5



7



13

この記事は公開されてから1年以上経過しています。情報が古い可能性がありますので、ご注意ください。

Transit Gatewayは複数VPCや、オンプレミスを単一のゲートウェイで接続することができるサービスです。Transit Gateway登場以前は、接続先が増えるたびにピアリングや、Direct Connect等でフルメッシュ構成が必要でした。

そんなTransit Gatewayが先日、東京リージョンでDirect Connectサポートを発表しました。これによりTransit Gatewayの利用を検討する機会が増えそうです。（体感）

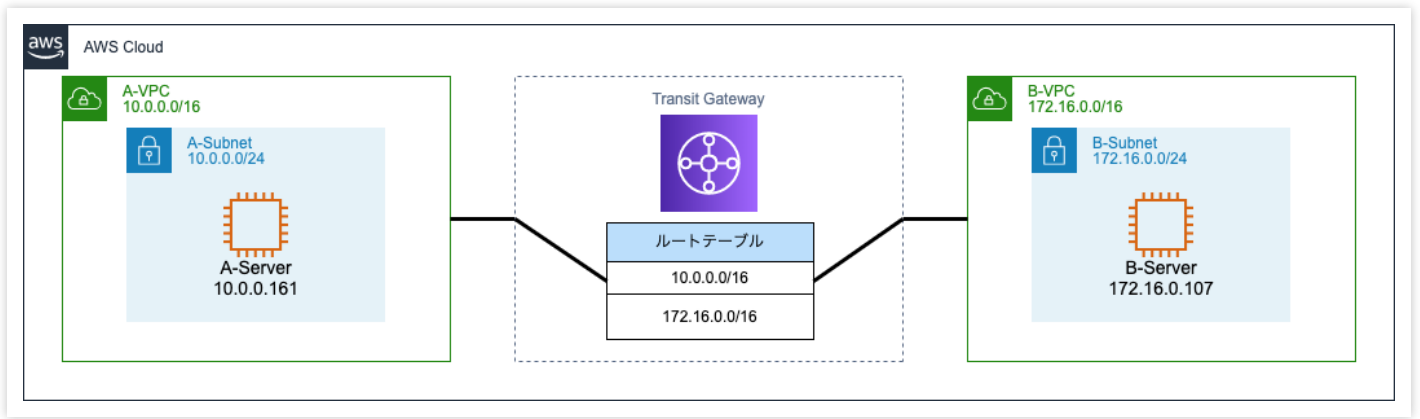
- [AWS Direct Connect の AWS Transit Gateway サポートが新たに 6 つのリージョンで利用可能に](#)

本エントリーでは、Transit Gatewayの理解を深めるために、Transit Gatewayの用語を交えつつ、シンプルな構成 ^{*1}で実際に構築してみたいと思います。

構成 & 前提

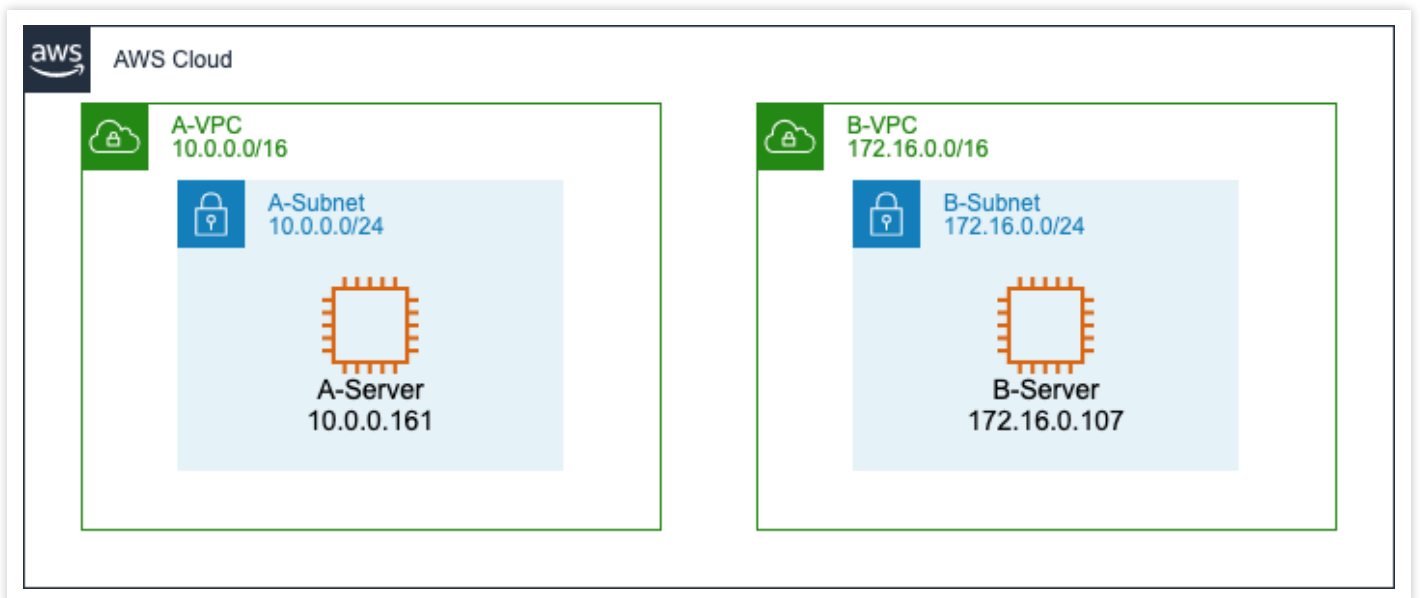
構成

最終的には以下のような構成で、各VPCから双方向に通信を実施してみたいと思います。



前提

以下VPC、EC2が作成済みであることを前提としています。



やってみた

Transit Gateway作成

VPCコンソールより[Transit Gateway]-[Create Transit Gateway]をクリックします。



ここでは、アソシエーション、プロパゲーション（後ほど手動で行います）等のデフォルトのチェックは外しました。[Name tag]に任意の名称を指定し[Create Transit Gateway]をクリックします。

Transit Gateways > Create Transit Gateway

Create Transit Gateway

A Transit Gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same account or across accounts.

Name tag ⓘ

Description ⓘ

Configure the Transit Gateway

Amazon side ASN ⓘ

DNS support ☒ enable ⓘ

VPN ECMP support ☐ enable ⓘ

Default route table association ☐ enable ⓘ

Default route table propagation ☐ enable ⓘ

Configure sharing options for cross account

Auto accept shared attachments ☐ enable ⓘ

* 必須

キャンセル **Create Transit Gateway**

「State」が「available」になることを確認してください。

タグや属性によるフィルター、またはキーワードによる検索				
1 中の 1 ~ 1				
<input checked="" type="checkbox"/>	Name	Transit Gateway ID	Owner account ID	State
<input checked="" type="checkbox"/>	TestTransitGateway	tgw-0ce242fdb5484073c	[REDACTED]	pending

タグや属性によるフィルター、またはキーワードによる検索				
1 中の 1 ~ 1				
<input checked="" type="checkbox"/>	Name	Transit Gateway ID	Owner account ID	State
<input checked="" type="checkbox"/>	TestTransitGateway	tgw-0ce242fdb5484073c	[REDACTED]	available

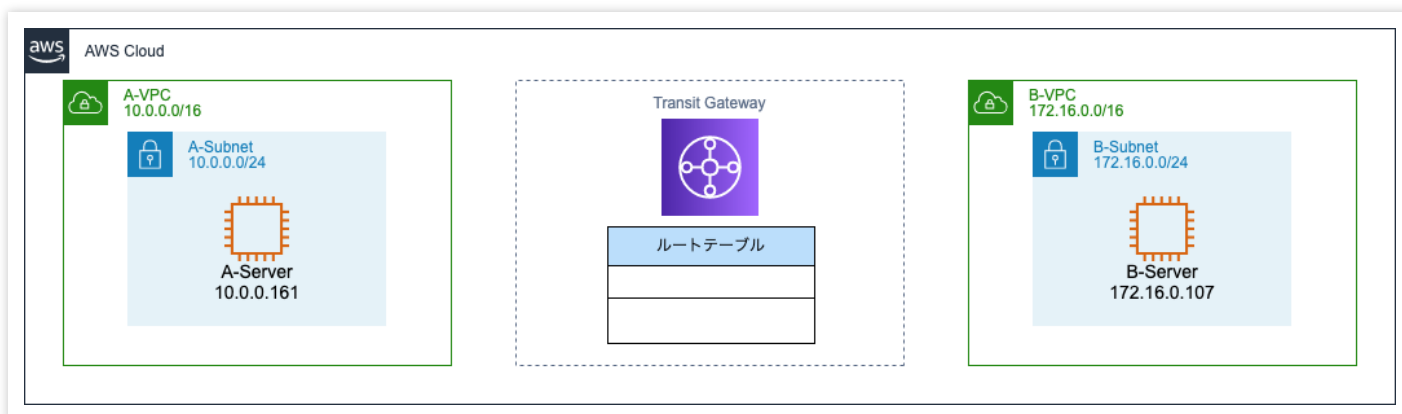
Transit Gatewayが作成できると、以下のようなイメージになります。



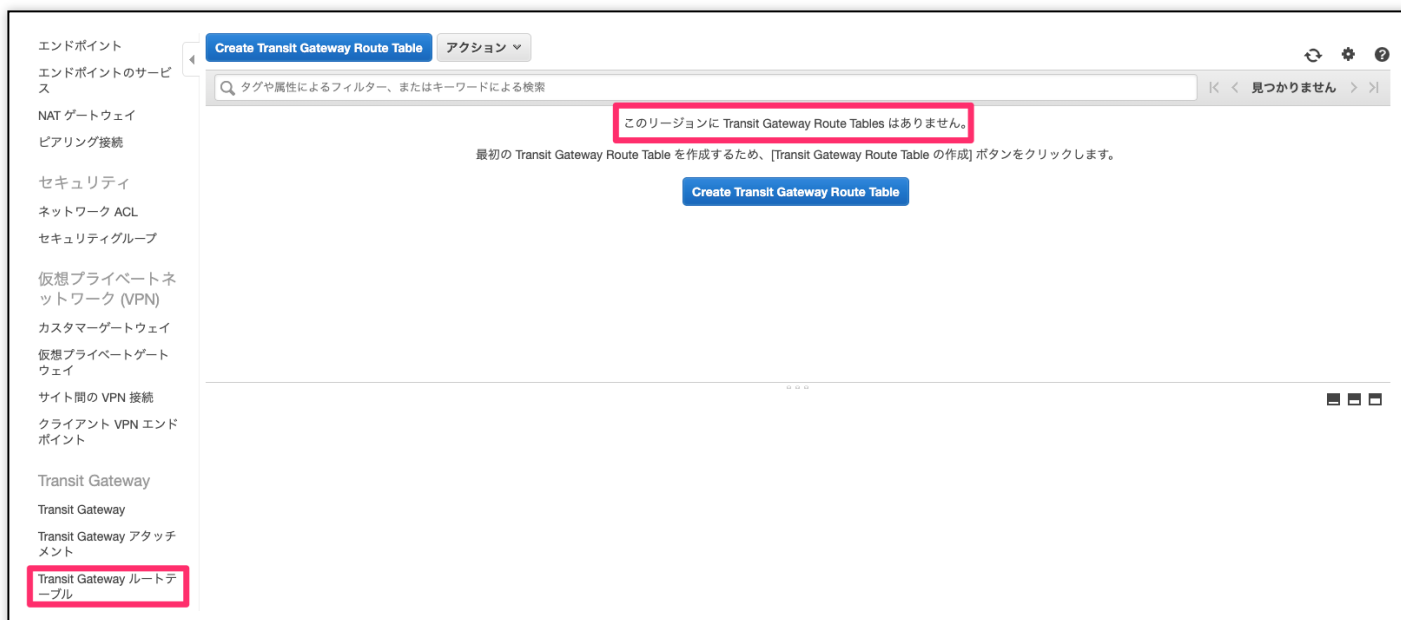
- 参考：[Create a Transit Gateway](#)

ルートテーブル作成

Transit Gatewayが持つ経路情報テーブル（ルートテーブル）を作成します。このルートテーブルは、通信のネクストホップの決定に利用されます。Transit Gatewayはルートテーブルを複数作成できますが、ここでは単一のルートテーブルを作成します。以下は、ルートテーブル作成後のイメージです。



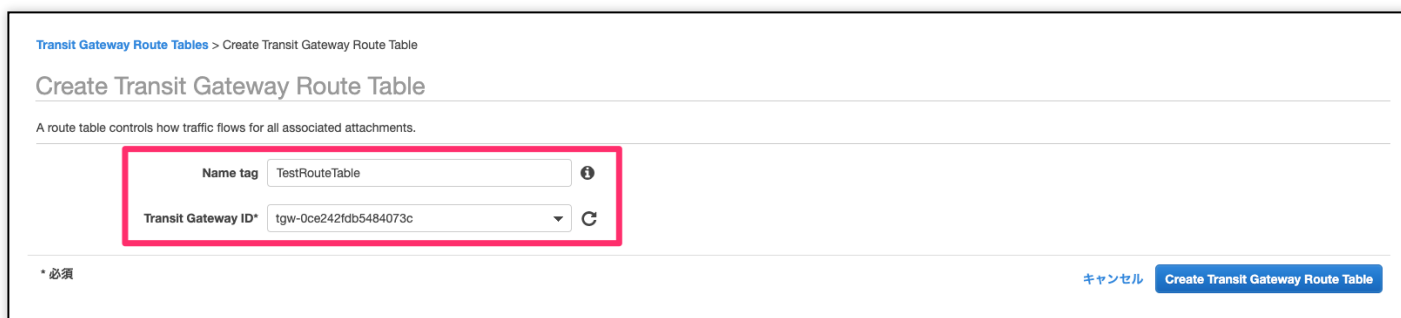
Transit Gateway作成時にデフォルトのチェックを外していたため、現時点でルートテーブルは存在しません。



「Create Transit Gateway Route Table」をクリックします。



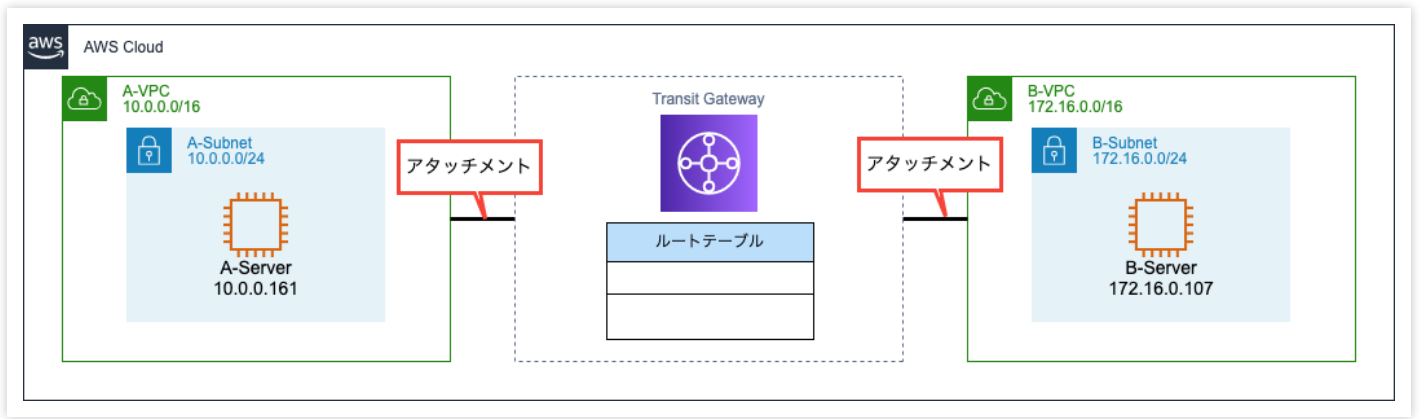
ルートテーブルに任意の名称を付け、さきほど作成したTransit Gatewayを指定します。



- 参考：[Create a Transit Gateway Route Table](#)

アタッチメント

VPCやDirect Connect等をTransit Gatewayに紐付ける作業を行います。アタッチメント後は、以下のようなイメージになります。



A-VPC

A-VPC（イメージ左）をアタッチメントします。[Create Transit Gateway Attachment]をクリックします。



さきほど作成したTransit Gatewayをアタッチメント先に指定します。アタッチメントするVPC、サブネットを指定し[Create attachment]をクリックします。

Transit Gateway Attachments > Create Transit Gateway Attachment

Create Transit Gateway Attachment

Select a Transit Gateway and the type of attachment you would like to create.

Transit Gateway ID*

Attachment type ☒ VPC ☐ VPN

VPC Attachment

Select and configure your VPC attachment.

Attachment name tag

DNS support ☒ enable

IPv6 support ☐ enable

VPC ID*

Subnet IDs*

Availability Zone	Subnet ID
<input checked="" type="checkbox"/> ap-northeast-1a	subnet-0bf41baf29a3b9c5e (A-Subnet)
<input type="checkbox"/> ap-northeast-1c	No subnet available
<input type="checkbox"/> ap-northeast-1d	No subnet available

* 必須

キャンセル [Create attachment](#)

「State」が「available」になるとアタッチメントは完了です。

🔍 タグや属性によるフィルター、またはキーワードによる検索

1 中の 1 ~ 1

<input type="checkbox"/>	Name	Transit Gateway attachment ID	Transit Gateway ID	Resource type	Resource ID	State
<input checked="" type="checkbox"/>	A-VPC_Attachment	tgw-attach-0545937fcc2a06466	tgw-0ce242fdb5484073c	VPC	vpc-023f33593198ab891	pending

タグや属性によるフィルター、またはキーワードによる検索

<

1 中の 1 ~ 1

>

<div></div>	Name	Transit Gateway attachment ID	Transit Gateway ID	Resource type	Resource ID	State
<div></div>	A-VPC_Attachment	tgw-attach-0545937fcc2a06466	tgw-0ce242fdb5484073c	VPC	vpc-023f33593198ab891	available

B-VPC

B-VPC（イメージ右）をアタッチメントします。作業手順は同様です。アタッチメントするVPCにB-VPC、サブネットを指定し[Create attachment]をクリックします。

Transit Gateway Attachments > Create Transit Gateway Attachment

Create Transit Gateway Attachment

Select a Transit Gateway and the type of attachment you would like to create.

Transit Gateway ID*

Attachment type ☒ VPC ☐ VPN

VPC Attachment

Select and configure your VPC attachment.

Attachment name tag

DNS support ☒ enable

IPv6 support ☐ enable

VPC ID*

Subnet IDs*

Availability Zone	Subnet ID
<input checked="" type="checkbox"/> ap-northeast-1a	subnet-05bb711f394476331 (B-Subnet)
<input type="checkbox"/> ap-northeast-1c	No subnet available
<input type="checkbox"/> ap-northeast-1d	No subnet available

* 必須

キャンセル Create attachment

「State」が「available」になるとアタッチメントは完了です。

タグや属性によるフィルター、またはキーワードによる検索							2 中の 1 ~ 2	
<input type="checkbox"/>	Name	Transit Gateway attachment ID	Transit Gateway ID	Resource type	Resource ID	State		
<input checked="" type="checkbox"/>	B-VPC_Attachment	tgw-attach-0fd117a8c6fccf4ac	tgw-0ce242fdb5484073c	VPC	vpc-09a13eae057f4c779	pending		
<input type="checkbox"/>	A-VPC_Attachment	tgw-attach-0545937fcc2a06466	tgw-0ce242fdb5484073c	VPC	vpc-023f33593198ab891	available		

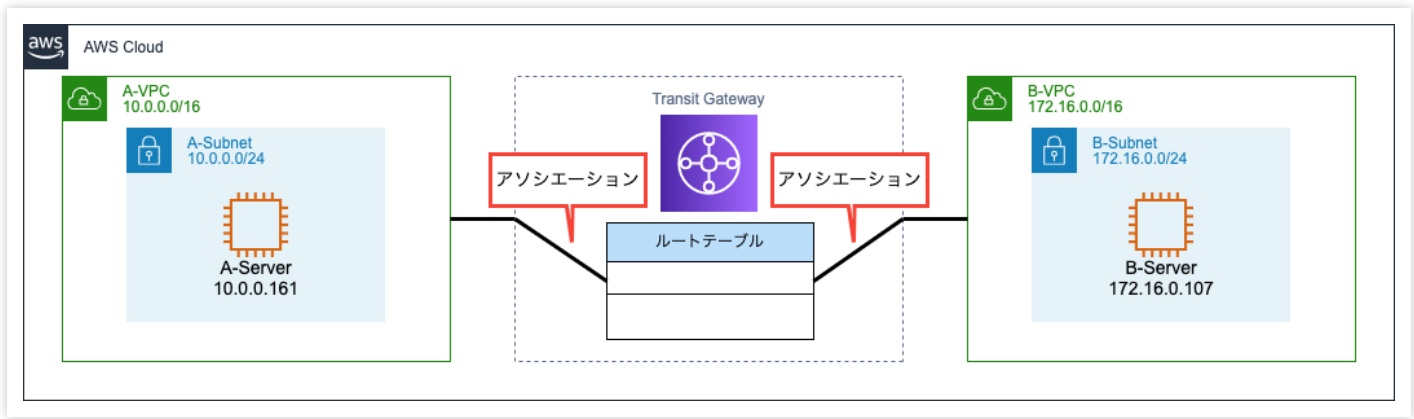
タグや属性によるフィルター、またはキーワードによる検索							2 中の 1 ~ 2	
<input type="checkbox"/>	Name	Transit Gateway attachment ID	Transit Gateway ID	Resource type	Resource ID	State		
<input checked="" type="checkbox"/>	B-VPC_Attachment	tgw-attach-0fd117a8c6fccf4ac	tgw-0ce242fdb5484073c	VPC	vpc-09a13eae057f4c779	available		
<input type="checkbox"/>	A-VPC_Attachment	tgw-attach-0545937fcc2a06466	tgw-0ce242fdb5484073c	VPC	vpc-023f33593198ab891	available		

- 参考：[Create a Transit Gateway Attachment to a VPC](#)

アタッチメントは完了しましたが、これだけでは通信を行うことができません。

アソシエーション

アタッチメントしたVPC等をルートテーブルに紐付けます。それにより、ルートテーブルにパケットが送信されるようになります。アソシエーション後のイメージです。



A-VPC

A-VPC（イメージ左）をアソシエーションします。[Create association]をクリックします。

Egress Only インターネット ゲートウェイ
DHCP オプションセット
Elastic IP
エンドポイント
エンドポイントのサービス
NAT ゲートウェイ
ピアリング接続
セキュリティ
ネットワーク ACL
セキュリティグループ
仮想プライベートネットワーク (VPN)
カスタマーゲートウェイ
仮想プライベートゲートウェイ
サイト間の VPN 接続
クライアント VPN エンドポイント
Transit Gateway
Transit Gateway
Transit Gateway アタッチメント
Transit Gateway ルートテーブル

Create Transit Gateway Route Table アクション

タグや属性によるフィルター、またはキーワードによる検索

Name	Transit Gateway route table ID	Transit Gateway ID	State	Default association route table	Default propagation route table
TestRouteTable	tgw-rtb-062bd59381532f0c9	tgw-0ce242fdb5484073c	available	No	No

Transit Gateway Route Table: tgw-rtb-062bd59381532f0c9

Details Associations Propagations Routes Tags

Create association Delete association

属性によるフィルター、またはキーワードによる検索

Attachment ID	Resource type	Resource ID	State
This route table does not have any associated attachments			

A-VPCのアタッチメントを指定し、[Create association]をクリックします。

Transit Gateway Route Tables > Create association

Create association

Associating an attachment to a route table allows traffic to be sent from the attachment to the target route table. An attachment can only be associated to one route table.

Transit Gateway ID tgw-0ce242fdb5484073c

Transit Gateway route table ID tgw-rtb-062bd59381532f0c9

Choose attachment to associate*

* 必須

キャンセル Create association

アソシエーションが確認できました。

Create Transit Gateway Route Table アクション

タグや属性によるフィルター、またはキーワードによる検索

Name	Transit Gateway route table ID	Transit Gateway ID	State	Default association route table	Default propagation route table
TestRouteTable	tgw-rtb-062bd59381532f0c9	tgw-0ce242fdb5484073c	available	No	No

Transit Gateway Route Table: tgw-rtb-062bd59381532f0c9

Details Associations Propagations Routes Tags

Create association Delete association

属性によるフィルター、またはキーワードによる検索

Attachment ID	Resource type	Resource ID	State
tgw-attach-0545937fcc2a06466	VPC	vpc-023f33593198ab891	associated

B-VPC

B-VPC（イメージ右）をアソシエーションします。作業手順は同様です。B-VPCのアタッチメントを指定し、[Create association]をクリックします。

Transit Gateway Route Tables > Create association

Create association

Associating an attachment to a route table allows traffic to be sent from the attachment to the target route table. An attachment can only be associated to one route table.

Transit Gateway ID tgw-0ce242fdb5484073c

Transit Gateway route table ID tgw-rtb-062bd59381532f0c9

Choose attachment to associate* tgw-attach-0fd117a8c6fcc4ac

* 必須

キャンセル Create association

アソシエーションが確認できました。

Create Transit Gateway Route Table アクション

タグや属性によるフィルター、またはキーワードによる検索

Name	Transit Gateway route table ID	Transit Gateway ID	State	Default association route table	Default propagation route table
TestRouteTable	tgw-rtb-062bd59381532f0c9	tgw-0ce242fdb5484073c	available	No	No

Transit Gateway Route Table: tgw-rtb-062bd59381532f0c9

Details Associations Propagations Routes Tags

Create association Delete association

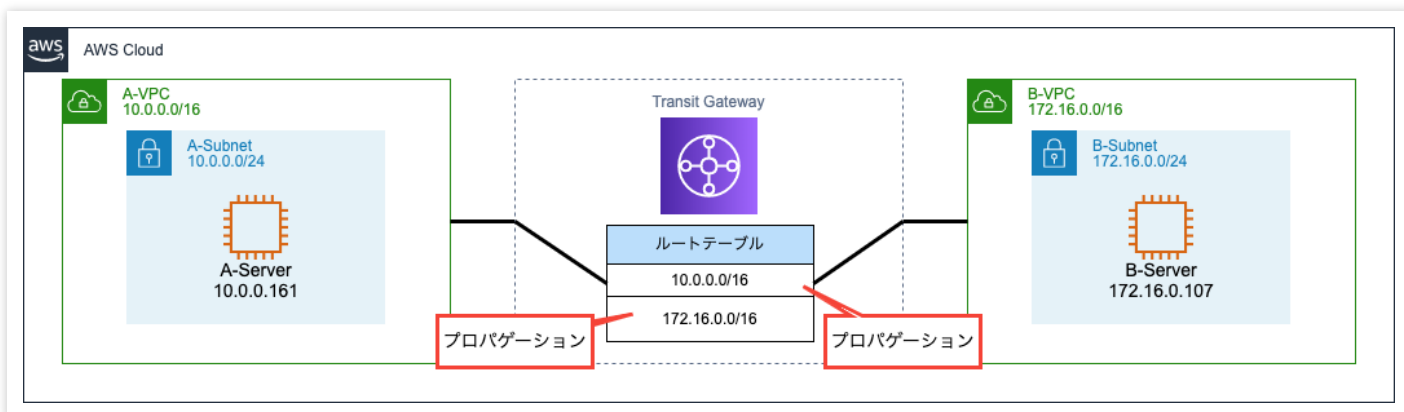
属性によるフィルター、またはキーワードによる検索

Attachment ID	Resource type	Resource ID	State
tgw-attach-0fd117a8c6fcc4ac	VPC	vpc-09a13eae057f4c779	associated
tgw-attach-0545937fcc2a06466	VPC	vpc-023f33593198ab891	associated

- 参考：[Associate a Transit Gateway Route Table](#)

プロパゲーション

アタッチメントしたVPCからルートテーブルに経路を伝播します。アソシエートしたVPCからプロパゲーションされることでルートテーブルが完成し、アタッチメントしたリソース間（ここではVPC）で通信が可能になります。プロパゲーションが実施後のイメージです。



A-VPC

A-VPC（イメージ左）をプロパゲーションします。[Create propagation]をクリックします。

The screenshot shows the AWS Management Console interface for creating a Transit Gateway Route Table. The 'Create Transit Gateway Route Table' page is displayed, with the 'Propagations' tab selected. The 'Create propagation' button is highlighted with a red box. The left sidebar shows the 'Transit Gateway ルートテーブル' (Transit Gateway Route Table) link highlighted with a red box.

Name	Transit Gateway route table ID	Transit Gateway ID	State	Default association route table	Default propagation route table
TestRouteTable	tgw-rtb-062bd59381532f0c9	tgw-0ce242fdb5484073c	available	No	No

Transit Gateway Route Table: tgw-rtb-062bd59381532f0c9

Details Associations **Propagations** Routes Tags

Create propagation Delete propagation

属性によるフィルター、またはキーワードによる検索

Attachment ID	Resource type	Resource ID	State
This route table does not have any propagated attachments			

A-VPCのアタッチメントを指定し、[Create propagation]をクリックします。


Transit Gateway Route Tables > Create propagation

Create propagation

Adding a propagation will allow routes to be propagated from an attachment to the target Transit Gateway route table. An attachment can be propagated to multiple route tables.

Transit Gateway ID `tgw-0ce242fdb5484073c`

Transit Gateway route table ID `tgw-rtb-062bd59381532f0c9`

Choose attachment to propagate* `tgw-attach-0545937fcc2a06466` 

* 必須 キャンセル Create propagation

「State」が「enabled」になると、ルートテーブルに経路が追加されます。

Create Transit Gateway Route Table アクション

タグや属性によるフィルター、またはキーワードによる検索

Name	Transit Gateway route table ID	Transit Gateway ID	State	Default association route table	Default propagation route table
TestRouteTable	tgw-rtb-062bd59381532f0c9	tgw-0ce242fdb5484073c	available	No	No

Transit Gateway Route Table: tgw-rtb-062bd59381532f0c9

Details Associations **Propagations** Routes Tags

Create propagation Delete propagation

属性によるフィルター、またはキーワードによる検索

Attachment ID	Resource type	Resource ID	State
tgw-attach-0545937fcc2a06466	VPC	vpc-023f33593198ab891	enabled

Create Transit Gateway Route Table アクション

タグや属性によるフィルター、またはキーワードによる検索

Name	Transit Gateway route table ID	Transit Gateway ID	State	Default association route table	Default propagation route table
TestRouteTable	tgw-rtb-062bd59381532f0c9	tgw-0ce242fdb5484073c	available	No	No

Transit Gateway Route Table: tgw-rtb-062bd59381532f0c9

Details Associations Propagations **Routes** Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create route Replace route Delete route

属性によるフィルター、またはキーワードによる検索

CIDR	Attachment	Resource type	Route type	Route state
10.0.0.0/16	tgw-attach-0545937fcc2a06466 vpc-023f33593198ab891	VPC	propagated	active

B-VPC

B-VPC（イメージ右）をプロパゲーションします。作業手順は同様です。B-VPCのアタッチメントを指定し、[Create propagation]をクリックします。


Transit Gateway Route Tables > Create propagation

Create propagation

Adding a propagation will allow routes to be propagated from an attachment to the target Transit Gateway route table. An attachment can be propagated to multiple route tables.

Transit Gateway ID `tgw-0ce242fdb5484073c`

Transit Gateway route table ID `tgw-rtb-062bd59381532f0c9`

Choose attachment to propagate* `tgw-attach-0fd117a8c6fccf4ac` 

* 必須 キャンセル Create propagation

「State」が「enabled」になると、ルートテーブルに経路が追加されます。

Create Transit Gateway Route Table アクション

タグや属性によるフィルター、またはキーワードによる検索 1 中の 1 ~ 1

Name	Transit Gateway route table ID	Transit Gateway ID	State	Default association route table	Default propagation route table
TestRouteTable	tgw-rtb-062bd59381532f0c9	tgw-0ce242fdb5484073c	available	No	No

Transit Gateway Route Table: tgw-rtb-062bd59381532f0c9

Details Associations **Propagations** Routes Tags

Create propagation Delete propagation

属性によるフィルター、またはキーワードによる検索 2 中の 1 ~ 2

Attachment ID	Resource type	Resource ID	State
tgw-attach-0545937fcc2a06466	VPC	vpc-023f33593198ab891	enabled
tgw-attach-0fd117a8c6fccf4ac	VPC	vpc-09a13eae057f4c779	enabled

Create Transit Gateway Route Table アクション

タグや属性によるフィルター、またはキーワードによる検索 1 中の 1 ~ 1

Name	Transit Gateway route table ID	Transit Gateway ID	State	Default association route table	Default propagation route table
TestRouteTable	tgw-rtb-062bd59381532f0c9	tgw-0ce242fdb5484073c	available	No	No

Transit Gateway Route Table: tgw-rtb-062bd59381532f0c9

Details Associations Propagations **Routes** Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create route Replace route Delete route

属性によるフィルター、またはキーワードによる検索 2 中の 1 ~ 2

CIDR	Attachment	Resource type	Route type	Route state
10.0.0.0/16	tgw-attach-0545937fcc2a06466 vpc-023f33593198ab891	VPC	propagated	active
172.16.0.0/16	tgw-attach-0fd117a8c6fccf4ac vpc-09a13eae057f4c779	VPC	propagated	active

なお、プロパゲートはアソシエートに関係なく、複数ルートテーブルに設定可能です。

- 参考：[Propagate a Route to a Transit Gateway Route Table](#)

サブネットのルートテーブルに経路追加

通信を行いたい各サブネットのルートテーブルに、Transit Gatewayへの経路を追加します。

A-Subnet

B-Subnetへの経路を追加します。送信先にB-SubnetのCIDR、ターゲットには作成したTransit Gatewayを指定します。

VPC ダッシュボード
VPC でフィルタリング:
VPC の選択

Virtual Private Cloud
VPC
サブネット
ルートテーブル
インターネットゲートウェイ
Egress Only インターネットゲートウェイ
DHCP オプションセット
Elastic IP
エンドポイント
エンドポイントのサービス
NAT ゲートウェイ

サブネットの作成 アクション

search: A-Subnet フィルターの追加

Name	サブネット ID	状態	VPC	IPv4 CIDR	利用可能な IPv4	IPv6 CIDR
A-Subnet	subnet-0bf41baf29a3b9c5e	available	vpc-023f33593198ab891 ...	10.0.0.0/24	249	-

サブネット: subnet-0bf41baf29a3b9c5e

説明 フローログ ルートテーブル ネットワーク ACL タグ 共有

ルートテーブルの関連付けの編集

ルートテーブル: rtb-05edf7b0a65482156 | A-Public-RTB

送信先	ターゲット
172.16.0.0/24	tgw-0ce242fdb5484073c
10.0.0.0/16	local
0.0.0.0/0	igw-057f852adc0e0d257

B-Subnet

A-Subnetへの経路を追加します。送信先にA-SubnetのCIDR、ターゲットには作成したTransit Gatewayを指定します。

VPC ダッシュボード
VPC でフィルタリング:
VPC の選択

Virtual Private Cloud
VPC
サブネット
ルートテーブル
インターネットゲートウェイ
Egress Only インターネットゲートウェイ
DHCP オプションセット
Elastic IP
エンドポイント
エンドポイントのサービス
NAT ゲートウェイ

サブネットの作成 アクション

search: B-Subnet フィルターの追加

Name	サブネット ID	状態	VPC	IPv4 CIDR	利用可能な IPv4	IPv6 CIDR
B-Subnet	subnet-05bb711f394476331	available	vpc-09a13eae057f4c779 ...	172.16.0.0/24	249	-

サブネット: subnet-05bb711f394476331

説明 フローログ ルートテーブル ネットワーク ACL タグ 共有

ルートテーブルの関連付けの編集

ルートテーブル: rtb-08c18e6d4725ae613 | B-Public-RTB

送信先	ターゲット
10.0.0.0/24	tgw-0ce242fdb5484073c
172.16.0.0/16	local
0.0.0.0/0	igw-038277bb9c3d2b322

セキュリティグループ編集

各セキュリティグループで通信を許可します。

セキュリティグループの作成 アクション ▼

search : A-Server フィルターの追加

Name	グループ ID	グループ名	VPC ID	所有者	説明
A-Server	sg-04c16072ab30dfac7	A-Server	vpc-023f33593198ab891		A-Server

セキュリティグループ: sg-04c16072ab30dfac7

説明 インバウンド アウトバウンド タグ

編集

タイプ	プロトコル	ポート範囲	ソース	説明
SSH	TCP	22		
すべての ICMP - IPv4	すべて	該当なし	172.16.0.0/24	

セキュリティグループの作成 アクション ▼

search : B-Server フィルターの追加

Name	グループ ID	グループ名	VPC ID	所有者	説明
B-Server	sg-0e8e5c05901e4cd8e	B-Server	vpc-09a13eae057f4c779		B-Server

セキュリティグループ: sg-0e8e5c05901e4cd8e

説明 インバウンド アウトバウンド タグ

編集

タイプ	プロトコル	ポート範囲	ソース	説明
SSH	TCP	22		
すべての ICMP - IPv4	すべて	該当なし	10.0.0.0/24	

アクセス確認

Transit Gatewayにアタッチメントしたリソース間で通信を確認してみます。

A-Server → B-Server

```
[ec2-user@ip-10-0-0-161 ~]$ ping -c 3 172.16.0.107
PING 172.16.0.107 (172.16.0.107) 56(84) bytes of data.
64 bytes from 172.16.0.107: icmp_seq=1 ttl=254 time=0.955 ms
64 bytes from 172.16.0.107: icmp_seq=2 ttl=254 time=0.595 ms
64 bytes from 172.16.0.107: icmp_seq=3 ttl=254 time=0.674 ms

--- 172.16.0.107 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2018ms
rtt min/avg/max/mdev = 0.595/0.741/0.955/0.156 ms
```

B-Server → A-Server

```
[ec2-user@ip-172-16-0-107 ~]$ ping -c 3 10.0.0.161
PING 10.0.0.161 (10.0.0.161) 56(84) bytes of data.
64 bytes from 10.0.0.161: icmp_seq=1 ttl=254 time=0.992 ms
64 bytes from 10.0.0.161: icmp_seq=2 ttl=254 time=0.639 ms
64 bytes from 10.0.0.161: icmp_seq=3 ttl=254 time=0.759 ms

--- 10.0.0.161 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2025ms
rtt min/avg/max/mdev = 0.639/0.796/0.992/0.150 ms
```

想定通りの通信が確認できました。

さいごに

Transit Gatewayの理解を深めるためにシンプルな構成で構築を実施してみました。VPC、VPN、Direct Connectなど、接続するポイントが多く想定される場合は、Transit Gatewayの利用を検討してみてくださいはいかがでしょうか。

以上、坂巻（@nochi251）でした！

参考

- [「Transit Gateway Deep Dive アーキテクチャガイド」 | AWS Summit Tokyo 2019](#)
- [Transit Gateways](#)
- [新機能 – トランジットゲートウェイでネットワークアーキテクチャをシンプルに](#)

脚注

1. 単一のVPC間通信でTransit Gatewayを利用することはないと思いますが.. [↩](#)