AWS トランジットゲートウェイ

Amazon VPC

Amazon VPC: AWS トランジットゲートウェイ

Table of Contents

Transit Gateway とは

Transit Gateway は、仮想プライベートクラウド (VPC) とオンプレミスネットワークを相互接続するために使用できるネットワークの中継ハブです。クラウドインフラストラクチャがグローバルに拡張されるにつれて、リージョン間ピアリングはAWSグローバルインフラストラクチャ AWS データセンター間のすべてのネットワークトラフィックは、物理層で自動的に暗号化されます。

詳細については、「AWS Transit Gateway」を参照してください。

Transit Gateway の概念

Transit Gateway の主要な概念を次に示します。

- アタッチメント — 次をアタッチできます。
  - 1 つ以上の VPC
  - 接続 SD-WAN/サードパーティー製ネットワークアプライアンス
  - アンAWS Direct Connectゲートウェイ
  - 別のTransit Gateway とのピア接続
  - Transit Gateway への VPN 接続
- Transit Gateway の最大送信単位 (MTU) — ネットワーク接続の最大送信単位 (MTU) とは、接続を介して渡すことができる最大許容パケットサイズ (バイト単位) です。接続の MTU が大きいほど、より多くのデータを単一のパケットで渡すことができます。Transit Gateway は、VPC、AWS Direct Connect、Transit Gateway 接続、およびピアリングアタッチメント間のトラフィックに対して 8500 バイトの MTU をサポートします。VPN 接続を介したトラフィックは、1500 バイトの MTU を持つことができます。
- Transit Gateway ルートテーブル — Transit Gateway にはデフォルトのルートテーブルがあり、オプションで追加のルートテーブルを含めることができます。ルートテーブルには、パケットの宛先 IP アドレスに基づいてネクストホップを決定する動的ルートと静的ルートが含まれます。これらのルートのターゲットは、Transit Gateway のアタッチメントである場合があります。デフォルトでは、Transit Gateway アタッチメントはデフォルトの Transit Gateway ルートテーブルに関連付けられます。
- 関連付け — 各アタッチメントは、正確に 1 つのルートテーブルに関連付けられます。各アタッチメントは、正確に 1 つのルートテーブルに関連付けることができます。
- ルート伝達 — VPC、VPN 接続、または Direct Connect ゲートウェイは、Transit Gateway ルートテーブルに動的にルートを伝達できます。Connect アタッチメントでは、ルートはデフォルトで

Transit Gateway ルートテーブルに伝達されます。VPC では、Transit Gateway にトラフィックを送信するための静的ルートを作成する必要があります。VPN 接続では、ボーダーゲートウェイプロトコル (BGP) を使用してトランジットゲートウェイからオンプレミスのルーターにルートが伝達されます。Direct Connect ゲートウェイでは、許可されたプレフィックスが BGP を使用してオンプレミスルーターに送信されます。ピアリングアタッチメントでは、ピアリングアタッチメントをポイントする静的ルートをTransit Gateway のルートテーブルに作成する必要があります。

Transit Gateway の開始方法

次のリソースを使用して、Transit Gateway の作成と使用を支援します。

- Transit Gateway の動作
- 開始方法
- 設計のベストプラクティス

Transit Gateway の使用

次のインターフェイスのいずれかを使用して、Transit Gateway の作成、アクセス、管理を行うことができます。

- AWS Management Console — Transit Gateway へのアクセスに使用するウェブインターフェイスを提供します。
- AWSコマンドラインインターフェイス (AWS CLI CLI) — アマゾン VPC を含むさまざまな AWS のサービス用のコマンドが用意されており、Windows、macOS、および Linux でサポートされています。詳細については、「AWS Command Line Interface」を参照してください。
- AWSSDK — 言語固有の API オペレーションを提供し、署名の計算、リクエストの再試行処理、エラー処理など、接続のさまざまな詳細を処理します。詳細については、AWSSDK をご参照ください。
- クエリ API — HTTPS リクエストを使用して呼び出す低レベル API アクションを提供します。クエリ API の使用は、アマゾン VPC の最も直接的なアクセス方法ですが、リクエストに署名するハッシュの生成やエラー処理など、低レベルの詳細な作業をアプリケーションで処理する必要があります。詳細については、Amazon EC2 API リファレンスを参照してください。

料金

Transit Gateway 上のアタッチメントごとに時間単位で課金され、Transit Gateway で処理されたトラフィック量に対して課金されます。詳細については、AWS Transit Gateway の料金を参照してください。

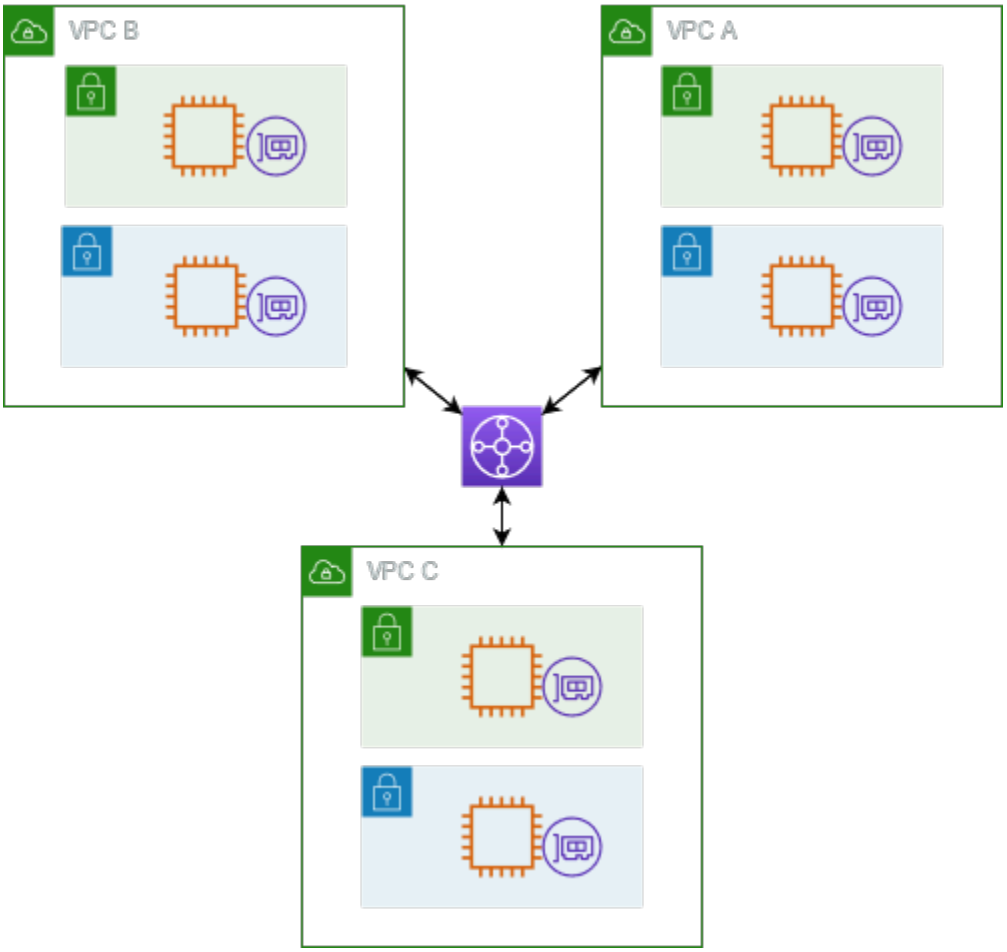
Transit Gateway の動作

Transit Gatewayは、仮想プライベートクラウド (VPC) とオンプレミスネットワークの間を流れるトラフィック用のリージョン仮想ルーターとして機能します。Transit Gateway は、ネットワークトラフィックの量に基づいて伸縮自在にスケーリングされます。Transit Gateway を介したルーティングは、レイヤー 3 で動作します。レイヤー 3 では、送信先 IP アドレスに基づいて、パケットが特定のネクストホップ接続に送信されます。

内容

アーキテクチャ図

次の図は、3 つの VPC が添付された Transit Gateway を示しています。これらの VPC のそれぞれのルートテーブルには、ローカルルートと、他の 2 つの VPC を宛先とするトラフィックを Transit Gateway に送信するルートが含まれます。



以下は、前の図に示されているアタッチメントのデフォルト Transit Gateway のルートテーブルの例です。各 VPC の CIDR ブロックがルートテーブルに伝播されます。したがって、各アタッチメントは他の 2 つのアタッチメントにパケットをルーティングできます。

デスティネーション	ターゲット	ルートタイプ
VPC A CIDR	*VPC A ########*	伝播済み
VPC B CIDR	*VPC B ########*	伝播済み
VPC C CIDR	*VPC C ########*	伝播済み

リソースアタッチメント

Transit Gateway アタッチメントは、パケットの送信元と送信先の両方です。次のリソースを Transit Gateway にアタッチできます。

- 1 つ以上の VPCs. AWS Transit Gateway は VPC サブネット内に Elastic Network Interface をデプロイし、Transit Gateway が選択したサブネットとの間でトラフィックをルーティングするために使用します。各アベイラビリティーゾーンには、少なくとも 1 つのサブネットが必要です。これにより、そのゾーンのすべてのサブネットのリソースにトラフィックが到達できるようになります。アタッチメントの作成時に、サブネットが同じゾーン内で有効になっている場合にだけ、特定のアベイラビリティーゾーン内のリソースが Transit Gateway に到達できます。サブネットルートテーブルに Transit Gateway へのルートがある場合、トラフィックが Transit Gateway に転送されるのは、Transit Gateway のアタッチメントが同じアベイラビリティーゾーンのサブネットにある場合のみです。
- 1 つ以上の VPN 接続
- 1 つ以上の AWS Direct Connect ゲートウェイ
- 1 つまたは複数の Transit Gateway Connect アタッチメント
- 1 つ以上の Transit Gateway ピアリング接続
- Transit Gateway アタッチメントは、パケットの送信元と送信先の両方です。

等コストマルチパスルーティング

AWS Transit Gateway は、ほとんどのアタッチメントで等コストマルチパス (ECMP) ルーティングをサポートしています。VPN アタッチメントの場合、Transit Gateway を作成または変更するときに、コンソールを使用して ECMP サポートを有効化または無効化できます。その他すべてのアタッチメントファイルについては、以下の ECMP 制限が適用されます。

- VPC - CIDR ブロックを重複させることは可能ではないため、VPC は ECMP をサポートしません。例えば、CIDR が 10.1.0.0/16 の VPC と、同じ CIDR を使用する 2 つ目の VPC を Transit Gateway にアタッチしてから、それらの間のトラフィックを負荷分散するようにルーティングをセットアップすることはできません。
- [VPN ECMP サポート] オプションが無効になっている場合、複数のパスで同等のプレフィックスが使用されていると、Transit Gateway は内部メトリクスを使用して優先パスを決定します。VPN アタッチメントに対する ECMP の有効化または無効化の詳細については、「the section called “Transit Gateway”」を参照してください。
- AWS Transit Gateway Connect - AWS Transit Gateway Connect アタッチメントは ECMP を自動的にサポートします。
- AWS Direct Connect Gateway - AWS Direct Connect Gateway アタッチメントは、ネットワークプレフィックス、プレフィックスの長さ、AS_PATH が完全に同じである場合、複数の Direct Connect Gateway アタッチメント間で ECMP を自動的にサポートします。

- Transit Gateway ピアリング - Transit Gateway ピアリングは、ダイナミックルーティングをサポートしておらず、2 つの異なるターゲットに対して同じ静的ルートを設定することもできないため、ECMP をサポートしません。

> **Note**
>
> - BGP マルチパスの AS-Path Relax はサポートされていないため、異なる AS 番号 (ASN) で ECMP を使用することはできません。
> - 異なるアタッチメントタイプ間では ECMP はサポートされません。例えば、VPN と VPC アタッチメント間で ECMP を有効にすることはできません。代わりに、Transit Gateway ルートが評価され、トラフィックは評価されたルートに従ってルーティングされます。詳細については、「the section called “ルートの評価順序”」を参照してください。
> - 単一の Direct Connect ゲートウェイは、複数のトランジット仮想インターフェイス全体で ECMP をサポートします。このため、Direct Connect ゲートウェイは 1 つだけ設定して使用し、ECMP を利用するために複数のゲートウェイを設定して使用しないことをお勧めします。Direct Connect ゲートウェイとパブリック仮想インターフェイスの詳細については、「パブリック仮想インターフェイスAWS から へのアクティブ/アクティブまたはアクティブ/パッシブ Direct Connect 接続を設定する方法」を参照してください。

アベイラビリティーゾーン

VPC を Transit Gateway に接続するときは、VPC サブネット内のリソースにトラフィックをルーティングするために、1 つ以上のアベイラビリティーゾーンを Transit Gateway で使用できるようにする必要があります。各アベイラビリティーゾーンを有効にするには、サブネットを 1 つだけ指定します。Transit Gateway は、サブネットから 1 つの IP アドレスを使用して、そのサブネット内にネットワークインターフェイスを配置します。アベイラビリティーゾーンを有効にすると、指定したサブネットやアベイラビリティーゾーンだけでなく、その VPC 内のすべてのサブネットにトラフィックをルーティングできます。ただし、Transit Gateway アタッチメントが存在するアベイラビリティーゾーンにあるリソースのみ、Transit Gateway に到達できます。

送信先アタッチメントが存在しないアベイラビリティーゾーンからトラフィックが発信された場合、AWS Transit Gateway はそのトラフィックをアタッチメントが存在するランダムなアベイラビリティーゾーンに内部的にルーティングします。このタイプのクロスアベイラビリティーゾーントラフィックには、Transit Gateway の追加料金はかかりません。

高可用性を確保するために、複数のアベイラビリティーゾーンを有効にすることをお勧めします。

アプライアンスモードサポートの使用

VPC でステートフルネットワークアプライアンスを設定する予定の場合は、アプライアンスが配置されているその VPC アタッチメントに対してアプライアンスモードサポートを有効にできます。これにより、Transit Gateway は、送信元と送信先の間のトラフィックフローの存続期間中、その VPC アタッチメントに対して同じアベイラビリティーゾーンを使用します。また、そのアベイラビリティーゾーンにサブネットの関連付けがある限り、Transit Gateway は VPC 内の任意のアベイラビリティーゾーンにトラフィックを送信できるようにします。詳細については、「例: 共有サービス VPC のアプライアンス」を参照してください。

ルーティング

Transit Gateway は、Transit Gateway ルートテーブルを使ってアタッチメント間で IPv4 と IPv6 パケットをルーティングします。これらのルートテーブルを設定して、アタッチされている VPC、VPN 接続、Direct Connect ゲートウェイのルートテーブルからルートを伝播できます。静的ルートを Transit Gateway ルートテーブルに追加することもできます。パケットが 1 つのアタッチメントから送信されると、宛先 IP アドレスと一致するルートを使用して別のアタッチメントにルーティングされます。

Transit Gateway のピアリングアタッチメントでは、静的ルートだけがサポートされます。

内容

ルートテーブル

Transit Gateway ではデフォルトのルートテーブルが自動的に使用されます。デフォルトでは、このルートテーブルはデフォルトの関連付けルートテーブルおよびデフォルトの伝達ルートテーブルです。または、ルート伝達とルートテーブルの関連付けを無効にした場合、 AWS は Transit Gateway のデフォルトルートテーブルを作成しません。

Transit Gateway に対して追加のルートテーブルを作成できます。これにより、アタッチメントのサブネットを分離できます。アタッチメントごとに 1 つのルートテーブルに関連付けることができます。アタッチメントでそのルートを 1 つ以上のルートテーブルに伝播できます。

ルートに一致するトラフィックを破棄する Transit Gateway ルートテーブルでは、ブラックホールルートを作成できます。

VPC を Transit Gateway にアタッチするときは、トラフィックが Transit Gateway を通過してルーティングするために、サブネットルートテーブルにルートを追加する必要があります。詳細については、Amazon VPC ユーザーガイドの「Transit Gateway のルーティング」を参照してください。

ルートテーブルの関連付け

Transit Gateway アタッチメントを単一のルートテーブルに関連付けることができます。各ルートテーブルは、ゼロから多数のアタッチメントに関連付けられ、パケットを他のアタッチメントに転送できます。

ルート伝達

各アタッチメントには、1 つ以上の Transit Gateway ルートテーブルにインストールできるルートが付属しています。アタッチメントが Transit Gateway ルートテーブルに伝播されると、これらのルートはルートテーブルにインストールされます。アドバタイズされたルートをフィルタリングすることはできません。

VPC アタッチメントの場合、VPC の CIDR ブロックは Transit Gateway のルートテーブルに伝達されます。

VPN アタッチメントまたは Direct Connect ゲートウェイアタッチメントで動的ルーティングを使用する場合、BGP 経由でオンプレミスルーターから学習されたルートを Transit Gateway ルートテーブルに伝播できます。

動的ルーティングを VPN アタッチメントで使用する場合、VPN アタッチメントに関連付けられたルートテーブル内のルートが BGP を介してカスタマーゲートウェイにアドバタイズされます。

Connect アタッチメントの場合、Connect アタッチメントに関連付けられたルートテーブル内のルートは、BGP を介して VPC で実行されているサードパーティの仮想アプライアンス (SD-WAN アプライアンスなど) にアドバタイズされます。

Direct Connect ゲートウェイアタッチメントの場合、許可されたプレフィックスインタラクションは、 からカスタマーネットワークにアドバタイズされるルートを制御します AWS。

静的ルートと伝達ルートが同じ送信先を持つ場合、静的ルートの優先度が高くなるため、伝達されたルートはルートテーブルに含まれません。静的ルートを削除すると、重複する伝達ルートがルートテーブルに含まれます。

ピアリングアタッチメントのルート

2 つの Transit Gateway をピアリングし、それらの間でトラフィックをルーティングできます。これを行うには、Transit Gateway にピアリングアタッチメントを作成し、ピアリング接続を行うピア Transit Gateway を指定します。次に、Transit Gateway ルートテーブルに静的ルートを作成し、トラフィックを Transit Gateway ピアリングアタッチメントにルーティングします。ピア Transit Gateway にルーティングされるトラフィックは、ピア Transit Gateway の VPC および VPN アタッチメントにルーティングできます。

詳細については、「例: ピア接続 Transit Gateway 」を参照してください。

ルートの評価順序

Transit Gateway のルートは、次の順序で評価されます。

- 送信先アドレスの最も具体的なルート。
- 同じ CIDR を持つが、異なるアタッチメントタイプのルートの場合、ルートの優先度は次のとおりです。
  - 静的ルート (例えば、Site-to-Site VPN 静的ルート)
  - プレフィックスリスト参照ルート
  - VPC が伝達したルート
  - Direct Connect ゲートウェイが伝達したルート
  - Transit Gateway Connect が伝達したルート
  - Site-to-Site VPN 伝達ルート
  - 伝播ルートをピアリングするトランジットゲートウェイ (クラウド WAN)

一部のアタッチメントは、BGP 経由のルートアドバタイズをサポートしています。同じ CIDR を持つルート、および同じアタッチメントタイプからのルートの場合、ルートの優先度は BGP 属性によって制御されます。

- AS パスの長さを短くする
- MED 値が低い

- アタッチメントでサポートされている場合は、iBGP ルートよりも eBGP が推奨されます

> **Important**
>
> AWS は、上記のものと同じ CIDR、アタッチメントタイプ、および BGP 属性を持つ BGP ルートの一貫したルート優先順位を保証することはできません。

AWS Transit Gateway には優先ルートのみが表示されます。バックアップルートは、そのルートがアドバタイズされなくなった場合にのみ Transit Gateway ルートテーブルに表示されます。例えば、Direct Connect ゲートウェイと Site-to-Site VPN を介して同じルートをアドバタイズする場合などです。 AWS Transit Gateway は、優先ルートである Direct Connect ゲートウェイルートから受信したルートのみを表示します。バックアップルートであるSite-to-Site VPN は、Direct Connect ゲートウェイがアドバタイズされなくなった場合にだけ表示されます。

VPC とトランジットゲートウェイのルートテーブルの違い

ルートテーブルの評価は、VPC ルートテーブルとトランジットゲートウェイルートテーブルのどちらを使用しているかによって異なります。

次の例は、VPC ルートテーブルを示しています。VPC ローカルルートが最も優先順位が高く、その後に最も具体的なルートが続きます。静的ルートと伝達されたルートの送信先が同じ場合は、静的ルートの方が優先度が高くなります。

送信先	ターゲット	優先度
10.0.0.0/16	ローカル	1
192.168.0.0/16	pcx-12345	2
172.31.0.0/16	vgw-12345 (静的) または tgw-12345 (静的)	2
172.31.0.0/16	vgw-12345 (伝播済み)	3
0.0.0.0/0	igw-12345	4

次の例は、トランジットゲートウェイルートテーブルを示しています。VPN アタッチメントよりも AWS Direct Connect ゲートウェイアタッチメントを好ましいと考える場合は、BGP VPN 接続を使用して Transit Gateway ルートテーブルにルートを伝達します。

送信先	アタッチメント (ターゲット)	リソースタイプ	ルートタイプ	優先度
10.0.0.0/16	tgw-attach-123 | vpc-1234	VPC	静的または伝播済み	1
192.168.0.0/16	tgw-attach-789 | vpn-5678	VPN	静的	2
172.31.0.0/16	tgw-attach-456 | dxgw_id	AWS Direct Connect ゲートウェイ	伝播済み	3
172.31.0.0/16	tgw-attach-789 | tgw-connect-peer-123	接続	伝播済み	4
172.31.0.0/16	tgw-attach-789 | vpn-5678	VPN	伝播済み	5

トランジットゲートウェイの開始方法

次のタスクは、トランジットゲートウェイに慣れるのに役立ちます。トランジットゲートウェイを作成し、トランジットゲートウェイを使用して 2 つの VPC を接続します。

タスク

- 前提条件
- ステップ 1: トランジットゲートウェイを作成する
- ステップ 2: VPC をトランジットゲートウェイに接続します
- ステップ 3: トランジットゲートウェイと VPC の間にルートを追加します
- ステップ 4: トランジットゲートウェイをテストする
- ステップ 5: トランジットゲートウェイを削除する

前提条件

- トランジットゲートウェイを使用する簡単な例を示すために、同じリージョンに 2 つの VPC を作成します。VPC は重複する CIDR を持つことはできません。各 VPC で 1 つの Amazon EC2 インスタンスを起動します。詳細については、アマゾン VPC ユーザーガイドの「Amazon VPC の使用を開始する」を参照してください。
- 同じルートを 2 つの異なる VPC に向けることはできません。トランジットゲートウェイのルートテーブルに同一のルートが存在する場合、トランジットゲートウェイは、新しくアタッチされた VPC の CIDR を伝達しません。
- トランジットゲートウェイを処理するために必要なアクセス許可があることを確認してください。詳細については、「Transit Gateway の ID およびアクセス管理」を参照してください。
- 各ホストセキュリティグループに ICMP ルールを追加していない場合は、ホスト間で ping を実行できません。詳細については、「Amazon VPC ユーザーガイド」の「セキュリティグループの操作」を参照してください。

ステップ 1: トランジットゲートウェイを作成する

トランジットゲートウェイを作成すると、デフォルトのトランジットゲートウェイルートテーブルが作成され、それをデフォルトの関連付けルートテーブルおよびデフォルトの伝達ルートテーブルとして使用します。

トランジットゲートウェイを作成するには

1. アマゾン VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. リージョンセレクターで、VPC を作成したときに使用したリージョンを選択します。
3. ナビゲーションペインで [Transit Gateways] を選択します。
4. [Transit Gateway の作成] を選択します。
5. (オプション) [名前タグ] に、トランジットゲートウェイの名前を入力します。これにより、キーとして「Name」、値として指定した名前を持つタグが作成されます。
6. (オプション) [説明] に、トランジットゲートウェイの説明を入力します。
7. [アマゾン 側の ASN] に、トランジットゲートウェイのプライベート自律システム番号 (ASN) を入力します。これは、ボーダーゲートウェイプロトコル (BGP) セッションの AWS 側の ASN になります。

   16 ビット ASN の場合、その範囲は 64512 ～ 65534 です。

   32 ビット ASN の場合、その範囲は 4200000000 ～ 4294967294 です。

   マルチリージョンのデプロイがある場合は、トランジットゲートウェイにそれぞれ、一意の ASN を使用することをお勧めします。
8. (オプション) DNS サポートを無効にする必要がある場合、またはデフォルトの関連付けルートテーブルまたはデフォルトの伝達ルートテーブルが不要な場合は、デフォルト設定を変更できます。
9. [Transit Gateway の作成] を選択します。ゲートウェイが作成されると、トランジットゲートウェイの初期状態は `pending` になります。

ステップ 2: VPC をトランジットゲートウェイに接続します

アタッチメントの作成に進む前に、前のセクションで作成したトランジットゲートウェイが使用可能として表示されるまで待ちます。各 VPC のアタッチメントを作成します。

「前提条件」で説明されているように、2 つの VPC を作成し、それぞれで EC2 インスタンスを起動したことを確認します。

VPC へのトランジットゲートウェイアタッチメントの作成

1. アマゾン VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。

3. [Transit Gateway アタッチメントの作成] を選択します。
4. (オプション) [名前タグ] にアタッチメントの名前を入力します。
5. [Transit Gateway ID] で、アタッチメントに使用するトランジットゲートウェイを選択します。
6. [アタッチメントタイプ] で、[VPC] を選択します。
7. [DNS サポート] を有効にするかどうかを選択します。この演習では、[IPv6 サポート] は有効にしません。
8. [VPC ID] で、トランジットゲートウェイにアタッチする VPC を選択します。
9. [サブネット ID] で、トラフィックをルーティングするためにトランジットゲートウェイが使用するアベイラビリティーゾーンごとに 1 つのサブネットを選択します。少なくとも 1 つのサブネットを選択する必要があります。アベイラビリティーゾーンごとに 1 つだけサブネットを選択できます。
10. [Transit Gateway アタッチメントの作成] を選択します。

各アタッチメントは常に 1 つのルートテーブルに関連付けられています。ルートテーブルは、ゼロから多数のアタッチメントに関連付けることができます。設定するルートを決定するには、トランジットゲートウェイのユースケースを決定し、ルートを設定します。詳細については、「ユースケースの例」を参照してください。

ステップ 3: トランジットゲートウェイと VPC の間にルートを追加します

ルートテーブルには、パケットの宛先 IP アドレスに基づいて関連する VPCのネクストホップを決定する、動的ルートと静的ルートが含まれます。非ローカルルートの送信先とトランジットゲートウェイのアタッチメント ID のターゲットを持つルートを設定します。詳細については、アマゾン VPC ユーザーガイドの「トランジットゲートウェイのルーティング」をご参照ください。

ルートを VPC ルートテーブルに追加するには

1. アマゾン VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[ルートテーブル] を選択します。
3. VPC に関連付けられているルートテーブルを選択します。
4. [ルート] タブを選択し、[ルート編集] を選択します。
5. [ルート追加] を選択します。

6. [送信先] 列に、送信先の IP アドレス範囲を入力します。ターゲットでは、トランジットゲートウェイを選択してから、トランジットゲートウェイ ID を選択します。
7. [Save changes] (変更の保存) をクリックします。

ステップ 4: トランジットゲートウェイをテストする

各 VPC の Amazon EC2 インスタンスに接続し、それらの間で ping コマンドなどのデータを送信することで、トランジットゲートウェイが正常に作成されたことを確認できます。詳細については、「Linux インスタンスへの接続」または「Windows インスタンスへの接続」を参照してください。

ステップ 5: トランジットゲートウェイを削除する

不要になったトランジットゲートウェイは削除できます。

リソースのアタッチメントがあるトランジットゲートウェイは削除できません。アタッチメント付きのトランジットゲートウェイを削除しようとすると、トランジットゲートウェイを削除する前に、まずそれらのアタッチメントを削除するように求められます。トランジットゲートウェイが削除されるとすぐに、そのゲートウェイに対する課金は停止します。

トランジットゲートウェイを削除するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway] を選択します。
3. トランジットゲートウェイを選択し、[アクション]、[トランジットゲートウェイの削除] を選択します。
4. 「**`delete`**」と入力し、[削除] を選択します。

   [Transit gateways] ページのトランジット ゲートウェイの State は [Deleting] です。削除すると、トランジットゲートウェイはページから削除されます。

Transit Gateway 設計のベストプラクティス

Transit Gateway 設計に関するベストプラクティスは次のとおりです:

- 各 Transit Gateway VPC アタッチメントに個別のサブネットを使用します。各サブネットに対して、小さな CIDR (/28 など) を使用して、EC2 リソースのアドレスが増えるようにします。別のサブネットを使用する場合は、次の項目を設定できます:
  - Transit Gateway サブネットに関連付けられたインバウンドおよびアウトバウンド NACL を開いたままにします。
  - トラフィックフローに応じて、ワークロードサブネットに NACL を適用できます。
- ネットワーク ACL を 1 つ作成し、Transit Gateway に関連付けられたすべてのサブネットに関連付けます。ネットワーク ACL は、インバウンド方向とアウトバウンド方向の両方で開いたままにします。
- ネットワーク設計で複数の VPC ルートテーブル (複数の NAT ゲートウェイを経由してトラフィックをルーティングする中間ボックス VPC など) を必要としない限り、同じ VPC ルートテーブルを Transit Gateway に関連付けられたすべてのサブネットに関連付けます。
- Border Gateway Protocol (BGP) Site-to-Site VPN 接続を使用します。接続用のカスタマーゲートウェイデバイスまたはファイアウォールがマルチパスをサポートしている場合は、機能を有効にします。
- AWS Direct Connect ゲートウェイアタッチメントと BGP Site-to-Site VPN アタッチメントのルート伝播を有効にします。
- VPC ピアリングからトランジットゲートウェイを使用するように移行する場合。VPC ピアリングと Transit Gateway 間の MTU サイズの不一致により、非対称トラフィックで一部のパケットがドロップされる可能性があります。サイズの不一致によりジャンボパケットがドロップされないように、両方の VPC を同時に更新してください。
- 設計上、Transit Gateway は可用性が高いため、高可用性を得るためにTransit Gateway を追加する必要はありません。
- 設計で複数のTransit Gateway ルートテーブルが必要でない限り、Transit Gateway ルートテーブルの数を制限します。
- 冗長性を確保するには、災害対策用に各リージョンで 1 つの Transit Gateway を使用します。
- 複数の Transit Gateway のデプロイを行う場合は、それぞれの Transit Gateway に固有の自律システム番号 (Amazon 側の ASN) を使用することをお勧めします。リージョン間のピアリングも使用できます。詳細については、「AWS Transit Gateway リージョン間ピアリングを使用したグローバルネットワークの構築」を参照してください。

Transit Gateway のユースケースの例

トランジットゲートウェイの一般的ユースケースは以下のとおりです。お客様のトランジットゲートウェイはこれらのユースケースに限定されません。

例

- 例: 集中型ルーター
- 例: 隔離された VPC
- 例: 共有サービスによる分離された VPC
- 例: ピア接続 Transit Gateway
- 例: インターネットへの一元的な発信ルーティング
- 例: 共有サービス VPC のアプライアンス

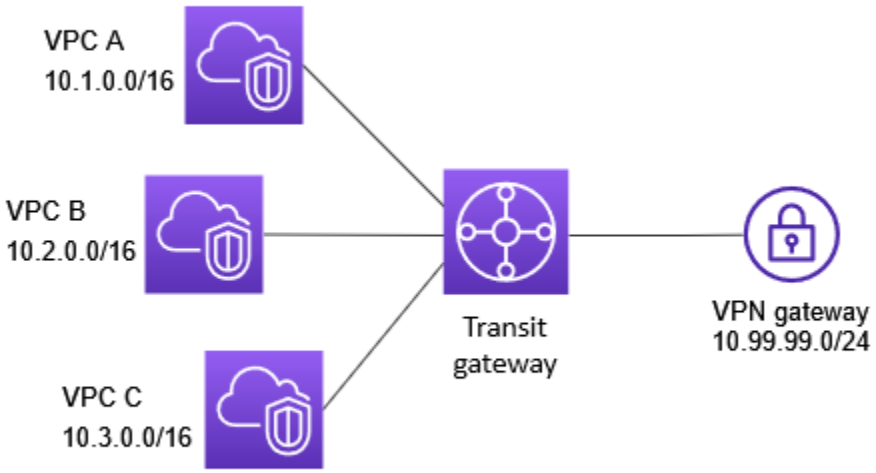
例: 集中型ルーター

すべての VPC、AWS Direct Connect 、および Site-to-Site VPN 接続を接続する集中型ルーターとしてトランジットゲートウェイを設定することができます。このシナリオでは、アタッチメントはすべて、トランジットゲートウェイのデフォルトルートテーブルに関連付けられ、トランジットゲートウェイのデフォルトルートテーブルに伝播されます。そのため、アタッチメントはすべて、単純なレイヤー 3 IP ルーターとしてトランジットゲートウェイを提供しながら、パケットを相互にルーティングできます。

目次

概要

次の図は、このシナリオの設定に重要なコンポーネントを示しています。このシナリオでは、トランジットゲートウェイへの 3 つの VPC のアタッチメントと 1 つの Site-to-Site VPN アタッチメントがあります。VPC A、VPC B、および VPC C のサブネットから、別の VPC のサブネットまたは VPN 接続を宛先とするパケットは、最初にトランジットゲートウェイを介してルーティングされます。



リソース

このシナリオでは、次のリソースを作成します。

- 3 つの VPC。VPC の作成の詳細については、Amazon VPC ユーザーガイドの「VPC を作成する」をご参照ください。
- トランジットゲートウェイ。詳細については、「the section called “Transit Gateway を作成する”」を参照してください。
- トランジットゲートウェイ上の 3 つの VPC アタッチメント。詳細については、「the section called “VPC への Transit Gateway アタッチメントの作成”」を参照してください。
- トランジットゲートウェイ上の Site-to-Site VPN のアタッチメント。各 VPC の CIDR ブロックがトランジットゲートウェイルートテーブルに伝播されます。VPN 接続が起動すると、BGP セッションが確立され、Site-to-Site VPN CIDR がトランジットゲートウェイルートテーブルに伝播され、VPC CIDR がカスタマーゲートウェイの BGP テーブルに追加されます。詳細については、「the section called “VPN への Transit Gateway アタッチメントの作成”」を参照してください。

  Site-to-Site VPN AWS Site-to-Site VPNユーザーガイドで、カスタマーゲートウェイデバイスの要件を必ず確認してください。

ルーティング

各 VPC にはルートテーブルがあり、トランジットゲートウェイルートテーブルがあります。

VPC ルートテーブル

各 VPC には、2 つのエントリを持つルートテーブルがあります。最初のエントリは、VPC のローカル IPv4 ルーティングのデフォルトエントリです。このエントリによって、この VPC 内のインスタンスが相互に通信できるようになります。2 番目のエントリは、他のすべての IPv4 サブネットトラフィックをトランジットゲートウェイにルーティングします。次の表に VPC A のルートを示します。

送信先	ターゲット
10.1.0.0/16	ローカル
0.0.0.0/0	tgw-id

転送ゲートウェイルートテーブル

以下は、前の図に示されているアタッチメントのデフォルトルートテーブルの例で、ルート伝播が有効になっています。

送信先	ターゲット	ルートタイプ
10.1.0.0/16	*VPC A ########*	伝播済み
10.2.0.0/16	*VPC B ########*	伝播済み
10.3.0.0/16	*VPC C ########*	伝播済み
10.99.99.0/24	*VPN ##########*	伝播済み

カスタマーゲートウェイの BGP テーブル

カスタマーゲートウェイの BGP テーブルには、次の VPC CIDR が含まれています。

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

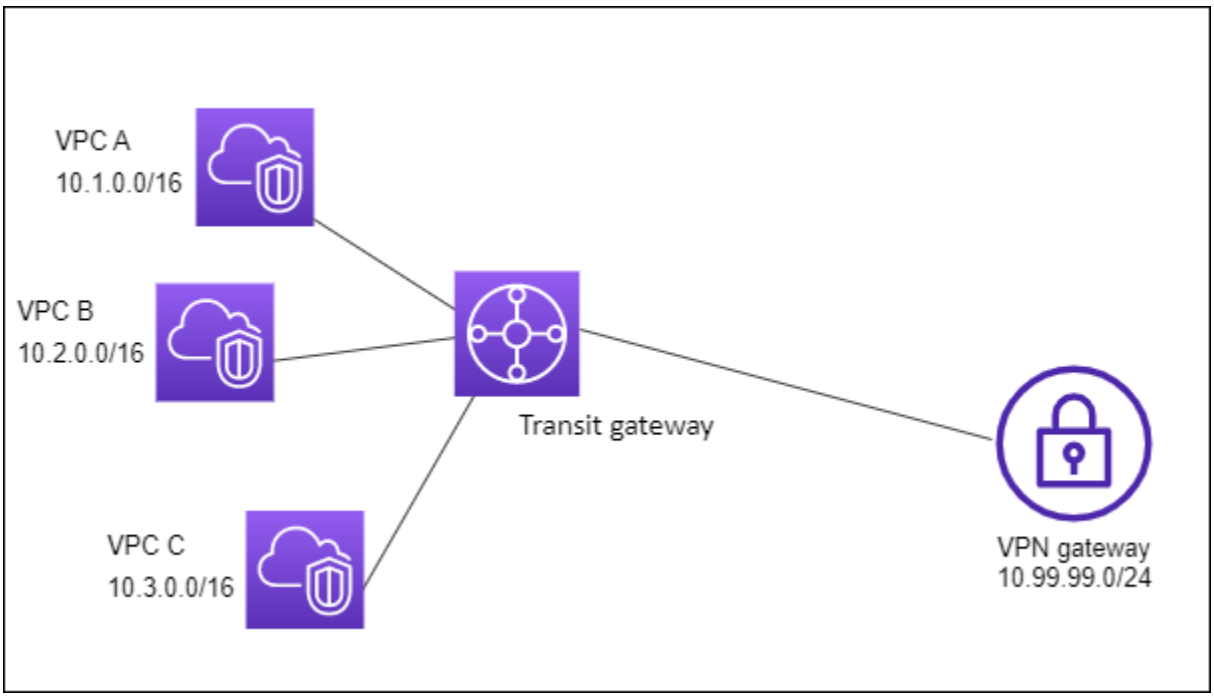
例: 隔離された VPC

複数の独立したルーターとしてトランジットゲートウェイを設定することができます。これは複数のトランジットゲートウェイを使用するのと似ていますが、ルートとアタッチメントが変わる可能性がある場合に、より高い柔軟性を提供します。このシナリオでは、独立した各ルーターに単一のルートテーブルがあります。独立したルーターに関連付けられているすべてのアタッチメントは、伝播されてそのルートテーブルに関連付けられます。1 つの独立したルーターに関連付けられているアタッチメントは、相互にパケットをルーティングできますが、別の独立したルーターのアタッチメントにパケットをルーティングしたり、アタッチメントからパケットを受信したりすることはできません。

目次

概要

次の図は、このシナリオの設定に重要なコンポーネントを示しています。VPC A、VPC B、および VPC C からのパケットは、トランジットゲートウェイにルーティングされます。インターネットを送信先とする VPC A、VPC B、および VPC C のサブネットからのパケットは、最初にトランジットゲートウェイを介してルーティングされ、次に Site-to-Site VPN 接続にルーティングされます (送信先がそのネットワーク内にある場合)。送信先が別の VPC のサブネットである VPC からのパケット (たとえば 10.1.0.0 から 10.2.0.0) はトランジットゲートウェイを経由してルーティングされますが、トランジットゲートウェイルートテーブルにはそれらのルートがないためブロックされます。



リソース

このシナリオでは、次のリソースを作成します。

- 3 つの VPC。VPC の作成の詳細については、Amazon VPC ユーザーガイドの「VPC を作成する」をご参照ください。
- トランジットゲートウェイ。詳細については、「the section called “Transit Gateway を作成する”」を参照してください。
- 3 つの VPC に使用するトランジットゲートウェイの 3 つのアタッチメント。詳細については、「the section called “VPC への Transit Gateway アタッチメントの作成”」を参照してください。
- Transit Gateway 上の Site-to-Site VPN のアタッチメント。詳細については、「the section called “VPN への Transit Gateway アタッチメントの作成”」(VPN への Transit Gateway アタッチメントの作成) を参照してください。Site-to-Site VPN AWS Site-to-Site VPNユーザーガイドで、カスタマーゲートウェイデバイスの要件を必ず確認してください。

VPN 接続が起動すると、BGP セッションが確立され、VPN CIDR がトランジットゲートウェイルートテーブルに伝播され、VPC CIDR がカスタマーゲートウェイの BGP テーブルに追加されます。

ルーティング

各 VPC にはルートテーブルがあり、トランジットゲートウェイには VPC 用と VPN 接続用の 2 つのルートテーブルがあります。

VPC A、VPC B、および VPC C ルートテーブル

各 VPC には、2 つのエントリを持つルートテーブルがあります。最初のエントリは、VPC のローカル IPv4 ルーティングのデフォルトエントリです。このエントリにより、この VPC 内のインスタンスが相互に通信できるようになります。2 番目のエントリは、他のすべての IPv4 サブネットトラフィックをトランジットゲートウェイにルーティングします。次の表に VPC A のルートを示します。

送信先	ターゲット
10.1.0.0/16	ローカル
0.0.0.0/0	tgw-id

トランジットゲートウェイルートテーブル

このシナリオでは、VPC に 1 つのルートテーブルを使用し、VPN 接続に 1 つのルートテーブルを使用します。

VPC アタッチメントは次のルートテーブルに関連付けられます。このテーブルには、VPN アタッチメントの伝播されるルートがあります。

送信先	ターゲット	ルートタイプ
10.99.99.0/24	*VPN ##########*	伝播済み

VPN アタッチメントは次のルートテーブルに関連付けられます。このテーブルには、各 VPC アタッチメントの伝播されるルートがあります。

送信先	ターゲット	ルートタイプ

送信先	ターゲット	ルートタイプ
10.1.0.0/16	*VPC A ########*	伝播済み
10.2.0.0/16	*VPC B ########*	伝播済み
10.3.0.0/16	*VPC C ########*	伝播済み

トランジットゲートウェイルートテーブルでのルート伝播の詳細については、「Transit Gateway ルートテーブルへのルートの伝達」を参照してください。

カスタマーゲートウェイの BGP テーブル

カスタマーゲートウェイの BGP テーブルには、次の VPC CIDR が含まれています。

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

例: 共有サービスによる分離された VPC

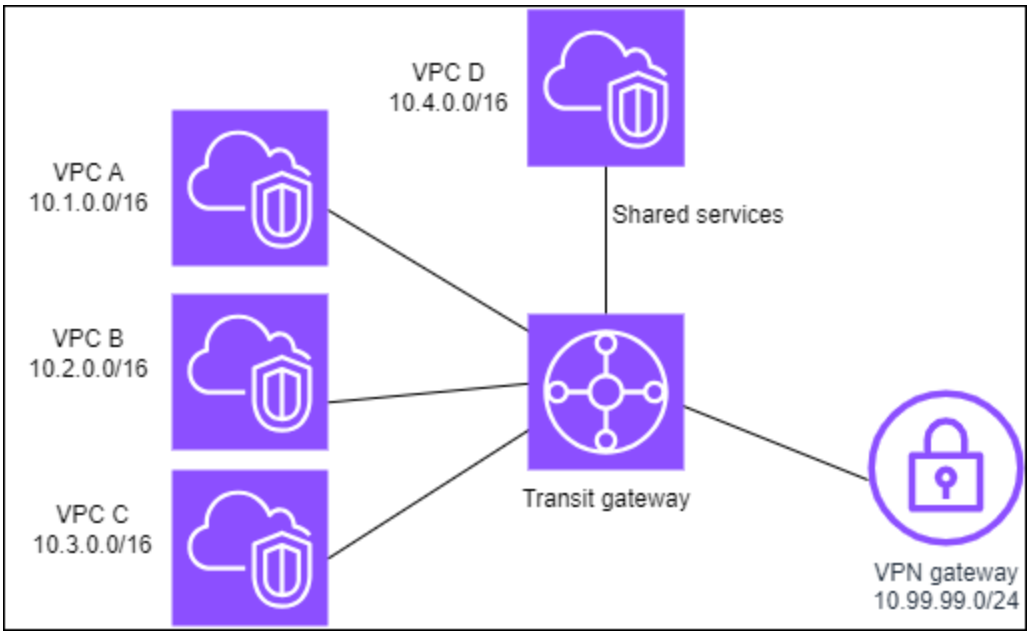
共有サービスを使用する複数の分離されたルーターとしてトランジットゲートウェイを設定できます。これは複数のトランジットゲートウェイを使用するのと似ていますが、ルートとアタッチメントが変わる可能性がある場合に、より高い柔軟性を提供します。このシナリオでは、独立した各ルーターに単一のルートテーブルがあります。独立したルーターに関連付けられているすべてのアタッチメントは、伝播されてそのルートテーブルに関連付けられます。1 つの独立したルーターに関連付けられているアタッチメントは、相互にパケットをルーティングできますが、別の独立したルーターのアタッチメントにパケットをルーティングしたり、アタッチメントからパケットを受信したりすることはできません。アタッチメントは、共有サービスとの間でパケットを送受信することができます。このシナリオは、分離する必要があるが、本番システムなどの共有サービスを使用する必要があるグループがある場合に使用できます。

目次

- ルーティング

概要

次の図は、このシナリオの設定に重要なコンポーネントを示しています。インターネットを送信先とする VPC A、VPC B、VPC C のサブネットからのパケットは、最初に Transit Gateway を介してルーティングされ、次に Site-to-Site VPN のカスタマーゲートウェイにルーティングされます。VPC A、VPC B、または VPC C のサブネットを送信先とする VPC A、VPC B、または VPC C のサブネットからのパケットは、Transit Gateway を介してルーティングされますが、Transit Gateway ルートテーブルにはそれらのルートがないためブロックされます。トランジットゲートウェイを経由した VPC D への送信先ルートとして VPC D を持つ VPC A、VPC B、および VPC C からのパケット。



リソース

このシナリオでは、次のリソースを作成します。

- 4 つの VPC。VPC の作成の詳細については、Amazon VPC ユーザーガイドの「VPC を作成する」をご参照ください。
- トランジットゲートウェイ。詳細については、「トランジットゲートウェイを作成する」を参照してください。

- Transit Gateway 上の 4 つのアタッチメント (VPC ごとに 1 つ)。詳細については、「the section called “VPC への Transit Gateway アタッチメントの作成”」(VPC への Transit Gateway アタッチメントの作成) を参照してください。
- Transit Gateway 上の Site-to-Site VPN のアタッチメント。詳細については、「the section called “VPN への Transit Gateway アタッチメントの作成”」(VPN への Transit Gateway アタッチメントの作成) を参照してください。

  Site-to-Site VPN AWS Site-to-Site VPNユーザーガイドで、カスタマーゲートウェイデバイスの要件を必ず確認してください。

VPN 接続が起動すると、BGP セッションが確立され、VPN CIDR がトランジットゲートウェイルートテーブルに伝播され、VPC CIDR がカスタマーゲートウェイの BGP テーブルに追加されます。

- 隔離された各 VPC は、隔離されたルートテーブルに関連付けられ、共有ルートテーブルに伝達されます。
- 共有された各 VPC は、共有されたルートテーブルに関連付けられ、両方のルートテーブルに伝達されます。

ルーティング

各 VPC にはルートテーブルがあり、トランジットゲートウェイには 2 つのルートテーブルがあります — 1 つは VPC 用、もう 1 つは VPN 接続および共有サービス VPC 用です。

VPC A、VPC B、VPC C、および VPC D ルートテーブル

各 VPC には、2 つのエントリを持つルートテーブルがあります。最初のエントリは、VPC のローカルルーティングのデフォルトエントリです。このエントリによって、この VPC 内のインスタンスが相互に通信できるようになります。2 番目のエントリは、他のすべての IPv4 サブネットトラフィックをTransit Gateway にルーティングします。

送信先	ターゲット
10.1.0.0/16	ローカル
0.0.0.0/0	*Transit Gateway ID*

トランジットゲートウェイルートテーブル

このシナリオでは、VPC に 1 つのルートテーブルを使用し、VPN 接続に 1 つのルートテーブルを使用します。

VPC A、B、および C のアタッチメントは次のルートテーブルに関連付けられます。このテーブルには、VPN アタッチメントの伝播されたルートと、VPC D のアタッチメントの伝播されたルートがあります。

送信先	ターゲット	ルートタイプ
10.99.99.0/24	*VPN ##########*	伝播済み
10.4.0.0/16	*VPC D ########*	伝播済み

VPN アタッチメントおよび共有サービス VPC (VPC D) アタッチメントは、次のルートテーブルに関連付けられています。このテーブルには、各 VPC アタッチメントを指すエントリがあります。これにより、VPN 接続および共有サービス VPC から VPC への通信が可能になります。

送信先	ターゲット	ルートタイプ
10.1.0.0/16	*VPC A ########*	伝播済み
10.2.0.0/16	*VPC B ########*	伝播済み
10.3.0.0/16	*VPC C ########*	伝播済み

詳細については、「Transit Gateway ルートテーブルへのルートの伝達」(Transit Gateway ルートテーブルへのルートの伝達) を参照してください。

カスタマーゲートウェイの BGP テーブル

カスタマーゲートウェイの BGP テーブルには、4 つの VPC すべての CIDR が含まれています。

例: ピア接続 Transit Gateway

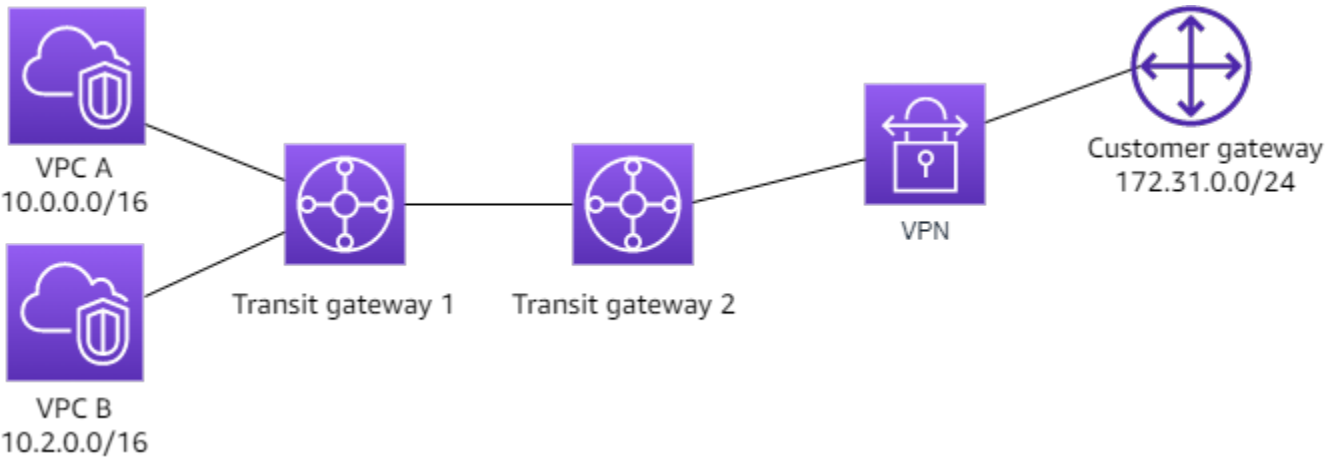
異なるリージョンで Transit Gateway 間に Transit Gateway ピアリング接続を作成できます。その後、各 Transit Gateway のアタッチメント間でトラフィックをルーティングできます。このシナリオ

では、VPC および VPN アタッチメントは、Transit Gateway のデフォルトルートテーブルに関連付けられ、Transit Gateway のデフォルトルートテーブルに伝播されます。各 Transit Gateway のルートテーブルには、ゲートウェイのピアリングアタッチメントを指す静的ルートがあります。

目次

概要

次の図は、このシナリオの設定に重要なコンポーネントを示しています。Transit Gateway 1 には 2 つの VPC アタッチメントがあり、Transit Gateway 2 には 1 つの Site-to-Site VPN アタッチメントがあります。送信先としてインターネット接続を持つ VPC A および VPC B のサブネットからのパケットは、最初にTransit Gateway 1 を介してルーティングされ、次にTransit Gateway 2 を介して VPN 接続にルーティングされます。



リソース

このシナリオでは、次のリソースを作成します。

- 2 つの VPC。VPC の作成の詳細については、Amazon VPC ユーザーガイドの「VPC を作成する」をご参照ください。
- 2 つの Transit Gateway。同じリージョン内に存在することも、異なるリージョン内に存在することもできます。詳細については、「the section called “Transit Gateway を作成する”」を参照してください。

- 最初のTransit Gateway の 2 つの VPC アタッチメント。詳細については、「the section called "VPC への Transit Gateway アタッチメントの作成"」を参照してください。
- 2 つ目の Transit Gateway 上の Site-to-Site VPN のアタッチメント。詳細については、「the section called "VPN への Transit Gateway アタッチメントの作成"」を参照してください。Site-to-Site VPN AWS Site-to-Site VPNユーザーガイドで、カスタマーゲートウェイデバイスの要件を必ず確認してください。
- 2 つのTransit Gateway 間のTransit Gateway ピアリングアタッチメント。詳細については、「Transit Gateway ピアリングアタッチメント」を参照してください。

VPC アタッチメントを作成すると、各 VPC の CIDR がTransit Gateway 1 のルートテーブルに伝播されます。VPN 接続がオンになると、次のアクションが発生します。

- BGP セッションが確立される
- Site-to-Site VPN CIDR がTransit Gateway 2 のルートテーブルに伝播される
- VPC CIDR がカスタマーゲートウェイ BGP テーブルに追加される

ルーティング

各 VPC にはルートテーブルがあり、各Transit Gateway にルートテーブルがあります。

VPC A および VPC B ルートテーブル

各 VPC には、2 つのエントリを持つルートテーブルがあります。最初のエントリは、VPC のローカル IPv4 ルーティングのデフォルトエントリです。このデフォルトエントリにより、この VPC 内のリソースが相互に通信できるようになります。2 番目のエントリは、他のすべての IPv4 サブネットトラフィックをTransit Gateway にルーティングします。次の表に VPC A のルートを示します。

送信先	ターゲット
10.0.0.0/16	ローカル
0.0.0.0/0	tgw-1-id

Transit Gateway ルートテーブル

次に、ルート伝播が有効になっているTransit Gateway 1 のデフォルトルートテーブルの例を示します。

送信先	ターゲット	ルートタイプ
10.0.0.0/16	*VPC A ######## ID*	伝播済み
10.2.0.0/16	*VPC B ######## ID*	伝播済み
0.0.0.0/0	*############ ID*	静的

次に、ルート伝播が有効になっているTransit Gateway 2 のデフォルトルートテーブルの例を示します。

送信先	ターゲット	ルートタイプ
172.31.0.0/24	*VPN ########## ID*	伝播済み
10.0.0.0/16	*############ ID*	static
10.2.0.0/16	*############ ID*	static

カスタマーゲートウェイの BGP テーブル

カスタマーゲートウェイの BGP テーブルには、次の VPC CIDR が含まれています。

- 10.0.0.0/16
- 10.2.0.0/16

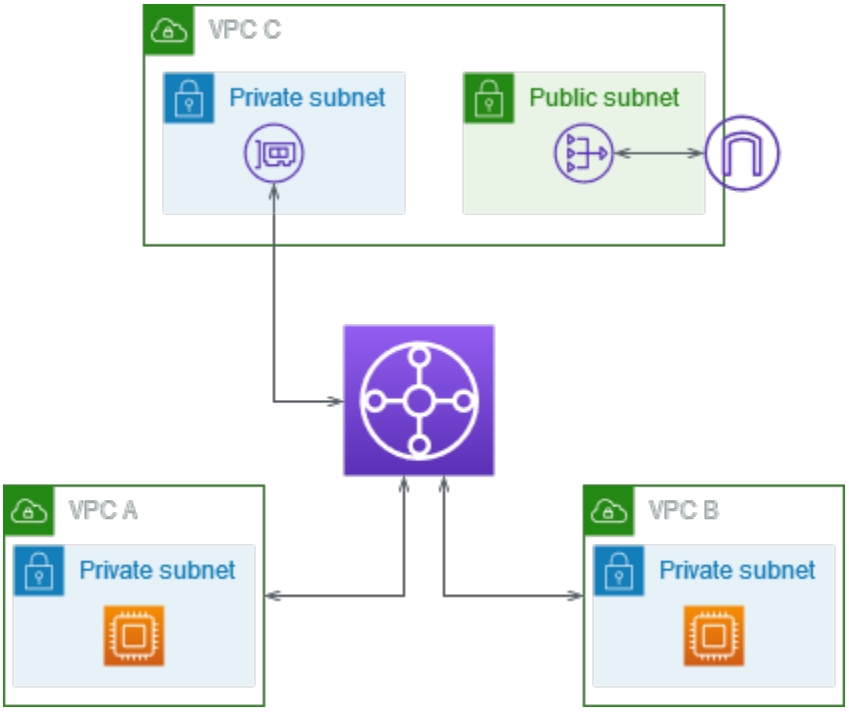
例: インターネットへの一元的な発信ルーティング

インターネットゲートウェイがない VPC からのアウトバウンドインターネットトラフィックを、NAT ゲートウェイとインターネットゲートウェイを含む VPC にルーティングするように、トランジットゲートウェイを設定できます。

目次

概要

次の図は、このシナリオの設定に重要なコンポーネントを示しています。VPC A と VPC B にインターネットアクセス (アウトバウンドのみ) が必要なアプリケーションがあります。パブリック NAT ゲートウェイとインターネットゲートウェイ、VPC アタッチメント用のプライベートサブネットを使用して VPC C を設定します。すべての VPC をトランジットゲートウェイに接続します。VPC A と VPC B からのアウトバウンドインターネットトラフィックが VPC C へのトランジットゲートウェイを通過するようにルーティングを設定します。VPC C の NAT ゲートウェイは、トラフィックをインターネットゲートウェイにルーティングします。



リソース

このシナリオでは、次のリソースを作成します。

- IP アドレス範囲が重複しない 3 つの VPC。詳細については、Amazon VPC ユーザーガイドの「VPC を作成する」を参照してください。
- VPC A と VPC B には、それぞれ EC2 インスタンスを持つプライベートサブネットがあります。
- VPC C には次のものがあります。
  - VPC にアタッチされたインターネットゲートウェイ。詳細については、Amazon VPC ユーザーガイドの「インターネットゲートウェイの作成とアタッチ」を参照してください。
  - NAT ゲートウェイを持つパブリックサブネット。詳細については、Amazon VPC ユーザーガイドの「NAT ゲートウェイの基本」を参照してください。
  - Transit Gateway アタッチメントのサブネット。プライベートサブネットは、パブリックサブネットと同じアベイラビリティーゾーンに設置する必要があります。
- 1 つのトランジットゲートウェイ。詳細については、「the section called “Transit Gateway を作成する”」を参照してください。
- トランジットゲートウェイ上の 3 つの VPC アタッチメント。各 VPC の CIDR ブロックがトランジットゲートウェイルートテーブルに伝播されます。詳細については、「the section called “VPC への Transit Gateway アタッチメントの作成”」を参照してください。VPC C には、プライベートサブネットを使用してアタッチメントを作成する必要があります。パブリックサブネットを使用してアタッチメントを作成すると、インスタンストラフィックはインターネットゲートウェイにルーティングされるものの、インターネットゲートウェイはそのトラフィックをドロップします。これは、インスタンスにパブリック IP アドレスがないためです プライベートサブネットにアタッチメントを配置することで、トラフィックが NAT ゲートウェイにルーティングされます。NAT ゲートウェイは、Elastic IP アドレスを送信元 IP アドレスとして使用して、トラフィックをインターネットゲートウェイに送信します

ルーティング

各 VPC には複数のルートテーブルがあり、トランジットゲートウェイには 1 つのルートテーブルがあります。

ルートテーブル

- VPC A のルートテーブル
- VPC B のルートテーブル

- VPC C のルートテーブル
- 転送ゲートウェイルートテーブル

VPC A のルートテーブル

ルートテーブルの例を次に示します。最初のエントリにより、VPC 内のインスタンスが相互に通信できるようになります。2 番目のエントリは、他のすべての IPv4 サブネットトラフィックをトランジットゲートウェイにルーティングします。

送信先	ターゲット
VPC A CIDR	ローカル
0.0.0.0/0	*transit-gateway-id*

VPC B のルートテーブル

ルートテーブルの例を次に示します。最初のエントリにより、VPC 内のインスタンスが相互に通信できるようになります。2 番目のエントリは、他のすべての IPv4 サブネットトラフィックをトランジットゲートウェイにルーティングします。

送信先	ターゲット
VPC B CIDR	ローカル
0.0.0.0/0	*transit-gateway-id*

VPC C のルートテーブル

インターネットゲートウェイにルートを追加することにより、NAT ゲートウェイを使用して、サブネットをパブリックサブネットとして構成します。もう一方のサブネットはプライベートサブネットのままにします。

パブリックサブネットのルートテーブルの例を次に示します。最初のエントリにより、VPC 内のインスタンスが相互に通信できるようになります。2 番目と 3 番目のエントリは、VPC A と VPC B のトラフィックをトランジットゲートウェイにルーティングします。最後のエントリは、他のすべての IPv4 サブネットトラフィックをインターネットゲートウェイにルーティングします。

送信先	ターゲット
VPC C CIDR	ローカル
VPC A CIDR	*transit-gateway-id*
VPC B CIDR	*transit-gateway-id*
0.0.0.0/0	*internet-gateway-id*

プライベートサブネットのルートテーブルの例を次に示します。最初のエントリにより、VPC 内のインスタンスが相互に通信できるようになります。2 番目のエントリは、他のすべての IPv4 サブネットトラフィックを NAT ゲートウェイにルーティングします。

送信先	ターゲット
VPC C CIDR	ローカル
0.0.0.0/0	*nat-gateway-id*

転送ゲートウェイルートテーブル

トランジットゲートウェイのルートテーブルの例を次に示します。各 VPC の CIDR ブロックがトランジットゲートウェイルートテーブルに伝播されます。静的ルートは、アウトバウンドインターネットトラフィックを VPC C に送信します。オプションとして、VPC CIDR ごとにブラックホールルートを追加することで、VPC 間の通信を防止することもできます。

CIDR	Attachment	ルートタイプ
VPC A CIDR	*VPC A ########*	伝播済み

CIDR	Attachment	ルートタイプ
VPC B CIDR	*VPC B ########*	伝播済み
VPC C CIDR	*VPC C ########*	伝播済み
0.0.0.0/0	*VPC C ########*	static

例: 共有サービス VPC のアプライアンス

共有サービス VPC でアプライアンス (セキュリティアプライアンスなど) を設定できます。トランジットゲートウェイアタッチメント間でルーティングされるすべてのトラフィックは、まず、共有サービス VPC のアプライアンスによって検査されます。アプライアンスモードが有効な場合、トランジットゲートウェイは、フローハッシュアルゴリズムを使用して、アプライアンス VPC 内の 1 つのネットワークインターフェイスを選択し、フローの有効期間中トラフィックを送信します。トランジットゲートウェイは、リターントラフィックに同じネットワークインターフェイスを使用します。これにより、双方向トラフィックは対称的にルーティングされます。つまり、フローの有効期間中、VPC アタッチメント内の同じアベイラビリティーゾーンを経由してルーティングされます。アーキテクチャ内に複数のトランジットゲートウェイがある場合、各トランジットゲートウェイは独自のセッションアフィニティを維持し、各トランジットゲートウェイは異なるネットワークインターフェイスを選択できます。

フローの維持を保証するには、1 つのトランジットゲートウェイをアプライアンス VPC に接続する必要があります。複数のトランジットゲートウェイを 1 つのアプライアンス VPC に接続しても、これらのトランジットゲートウェイはフロー状態情報を相互に共有しないので、フローの維持は保証されません。

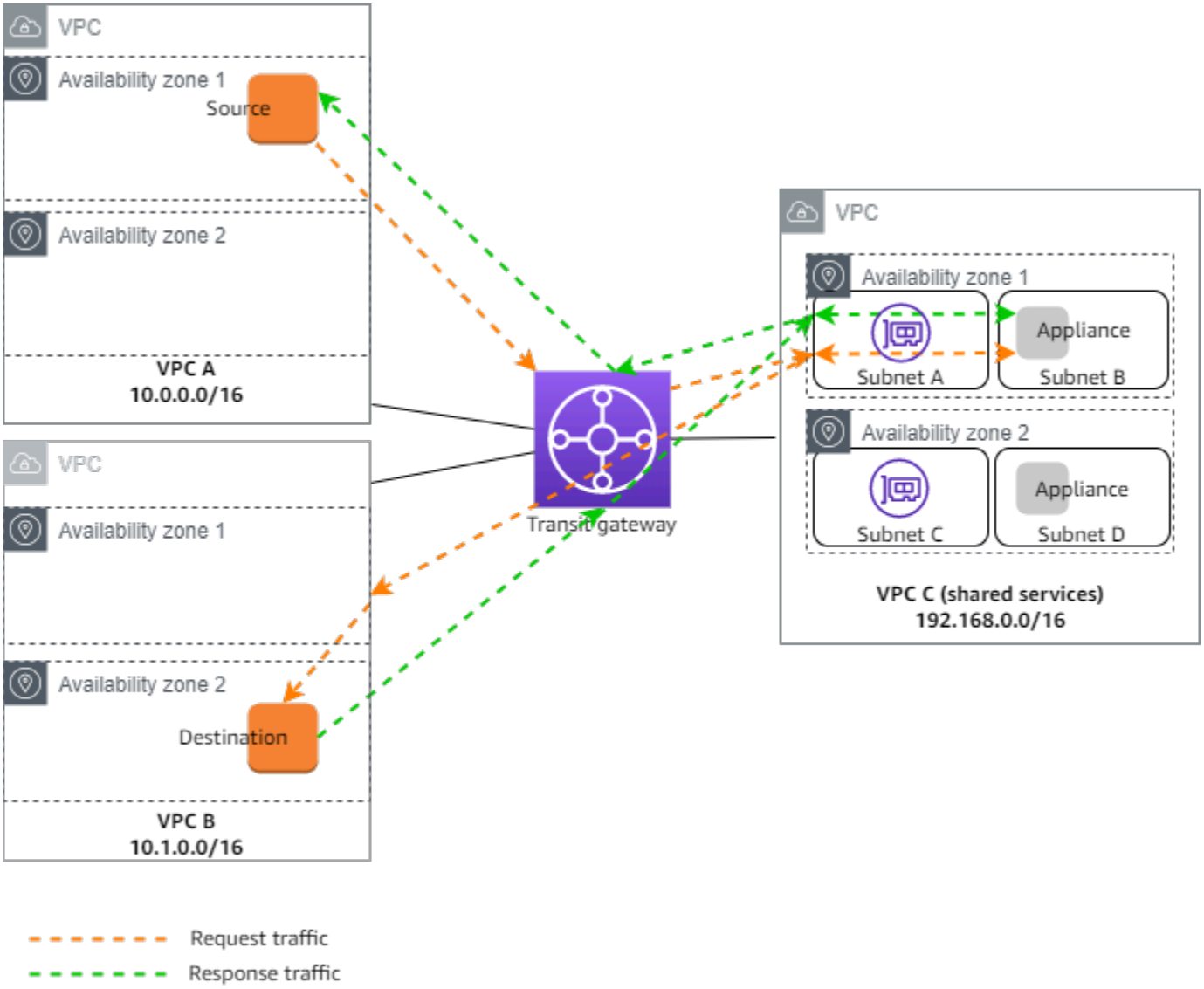
> **Important**
>
> - アプライアンスモードのトラフィックは、送信元と送信先のトラフィックが同じ Transit Gateway アタッチメントから集中型 VPC (インスペクション VPC) に到達する限り、正しくルーティングされます。送信元と送信先が 2 つの異なる Transit Gateway アタッチメントから入力されている場合、トラフィックが低下する可能性があります。アプライアンスモードは、VPN を介してネットワークに入るトラフィックには適用されません。
> - 既存のアタッチメントでアプライアンスモードを有効にすると、アタッチメントが任意のアベイラビリティーゾーンを流れる可能性があるため、そのアタッチメントの現在のルー

トに影響する可能性があります。アプライアンスモードが有効になっていない場合、トラフィックは発信元のアベイラビリティーゾーンに保持されます。

内容

概要

次の図は、このシナリオの設定に重要なコンポーネントを示しています。トランジットゲートウェイには、3 つの VPC アタッチメントがあります。VPC C は共有サービス VPC です。VPC A と VPC B 間のトラフィックはトランジットゲートウェイにルーティングされ、その後、最終的な宛先にルーティングされる前に、検査のために VPC C のセキュリティアプライアンスにルーティングされます。アプライアンスはステートフルアプライアンスであるため、リクエストトラフィックとレスポンストラフィックの両方が検査されます。高可用性を実現するために、VPC C の各アベイラビリティーゾーンにアプライアンスがあります。



このシナリオでは、次のリソースを作成します。

- 3 つの VPC。VPC の作成については、アマゾン仮想プライベートクラウド ユーザーガイドの「VPC を作成する」を参照してください。
- トランジットゲートウェイ。詳細については、「the section called “Transit Gateway を作成する”」を参照してください。
- 3 つの VPC アタッチメント、各 VPC に 1 つずつ。詳細については、「the section called “VPC への Transit Gateway アタッチメントの作成”」を参照してください。

  VPC アタッチメントごとに、各アベイラビリティーゾーンでサブネットを指定します。共有サービス VPC の場合、これらは、トラフィックがトランジットゲートウェイから VPC にルーティングされるサブネットです。前の例では、サブネット A と C です。

VPC C の VPC アタッチメントの場合、アプライアンスモードのサポートを有効にして、レスポンストラフィックがソーストラフィックと同じ VPC C のアベイラビリティーゾーンにルーティングされるようにします。

Amazon VPC コンソールはアプライアンスモードをサポートしていません。Amazon VPC API、AWS SDK、または AWS CLI を使用して、アプライアンスモードまたは AWS CloudFormation を有効にできます。例えば、-create-transit-gateway-vpcattachment コマンドまたは modify-transit-gateway-vpc-attachment コマンド`--options ApplianceModeSupport=enable`に を追加します。

> **Note**
>
> アプライアンスモードでのフロー維持が保証されるのは、インスペクション VPC に対する送信元トラフィックと宛先トラフィックのみです。

ステートフルアプライアンスおよびアプライアンスモード

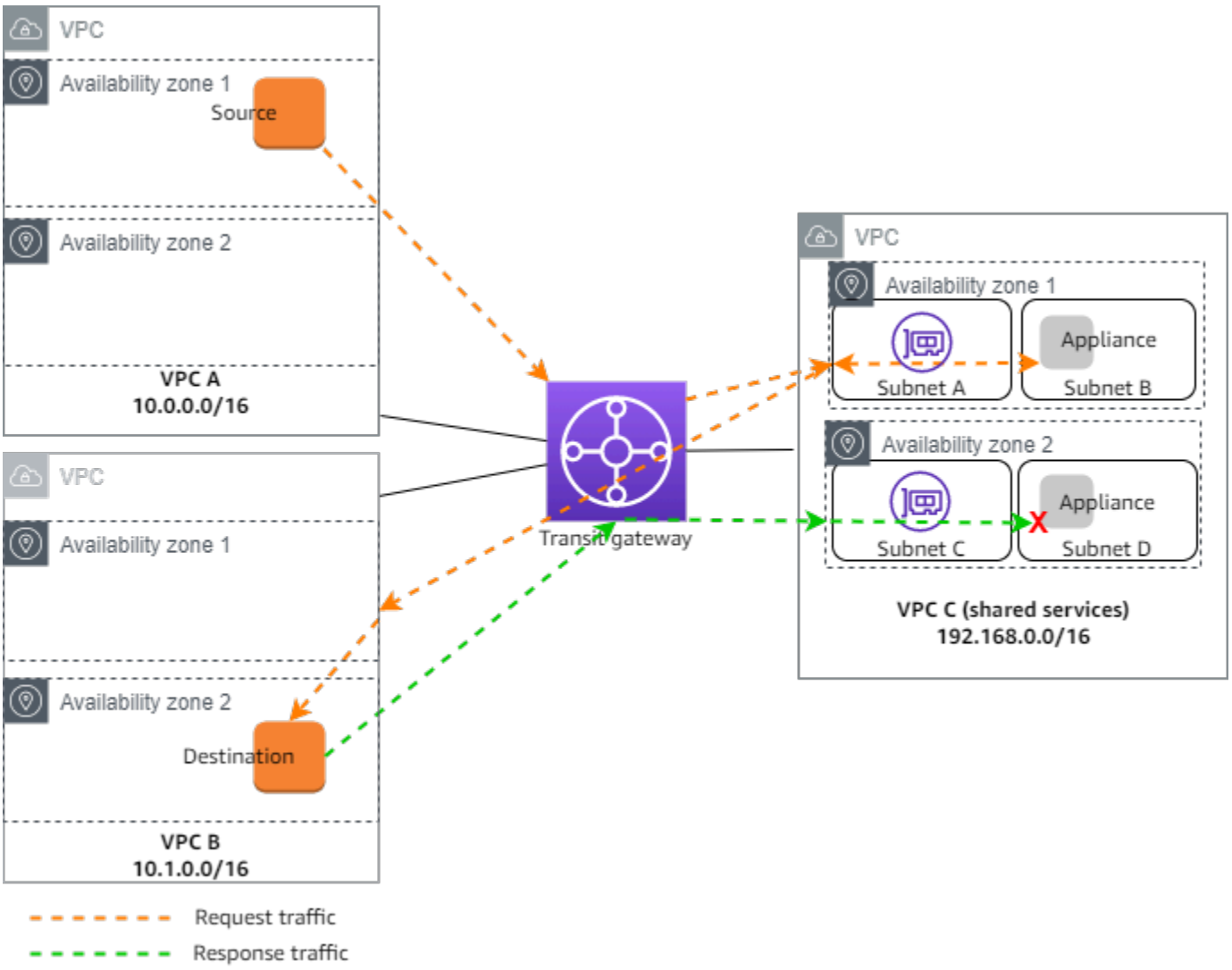
VPC アタッチメントが複数のアベイラビリティーゾーンにまたがっており、ステートフルな検査のために送信元ホストと送信先ホスト間のトラフィックを同じアプライアンスを介してルーティングする必要がある場合は、アプライアンスが配置されている VPC アタッチメントのアプライアンスモードサポートを有効にします。

詳細については、AWSブログの一元化された検査アーキテクチャを参照してください。

アプライアンスモードが有効でない場合の動作

アプライアンスモードが有効になっていない場合、トランジットゲートウェイは、送信元のアベイラビリティーゾーン内の VPC アタッチメント間でルーティングされたトラフィックが送信先に到達するまで維持しようとします。トラフィックは、アベイラビリティーゾーンに障害が発生した場合、またはそのアベイラビリティーゾーン内で VPC アタッチメントに関連付けられたサブネットがない場合にのみ、アタッチメント間でアベイラビリティーゾーンを通過します。

次の図は、アプライアンスモードサポートが有効でない場合のトラフィックフローを示しています。VPC B のアベイラビリティーゾーン 2 から発信されるレスポンストラフィックは、トランジットゲートウェイによって VPC C 内の同じアベイラビリティーゾーンにルーティングされます。したがって、アベイラビリティーゾーン 2 のアプライアンスは VPC A の送信元からの元のリクエストを認識しないため、トラフィックはドロップされます。



ルーティング

各 VPC には 1 つ以上のルートテーブルがあり、トランジットゲートウェイには 2 つのルートテーブルがあります。

VPC ルートテーブル

VPC A と VPC B

VPC A と B には、2 つのエントリを持つルートテーブルがあります。最初のエントリは、VPC のローカル IPv4 ルーティングのデフォルトエントリです。このデフォルトエントリにより、この VPC 内のリソースが相互に通信できるようになります。2 番目のエントリは、他のすべての IPv4 サブネットトラフィックをトランジットゲートウェイにルーティングします。以下は、VPC A のルートテーブルです。

送信先	ターゲット
10.0.0.0/16	ローカル
0.0.0.0/0	tgw-id

VPC C

共有サービス VPC (VPC C) には、サブネットごとに異なるルートテーブルがあります。サブネット A はトランジットゲートウェイによって使用されます (VPC アタッチメントの作成時にこのサブネットを指定します)。サブネット A のルートテーブルは、サブネット B のアプライアンスにすべてのトラフィックをルーティングします。

送信先	ターゲット
192.168.0.0/16	ローカル
0.0.0.0/0	appliance-eni-id

サブネット B (アプライアンスを含む) のルートテーブルは、トラフィックをトランジットゲートウェイにルーティングします。

送信先	ターゲット
192.168.0.0/16	ローカル
0.0.0.0/0	tgw-id

トランジットゲートウェイルートテーブル

このトランジットゲートウェイは、VPC A と VPC B に 1 つのルートテーブルを使用し、共有サービス VPC (VPC C) には 1 つのルートテーブルを使用します。

VPC A と VPC B のアタッチメントは、次のルートテーブルに関連付けられています。ルートテーブルは、すべてのトラフィックを VPC C にルーティングします。

送信先	ターゲット	ルートタイプ
0.0.0.0/0	*VPC C ######## ID*	静的

VPC C アタッチメントは、次のルートテーブルに関連付けられています。トラフィックを VPC A および VPC B にルーティングします。

送信先	ターゲット	ルートタイプ
10.0.0.0/16	*VPC A ######## ID*	伝播済み
10.1.0.0/16	*VPC B ######## ID*	伝播済み

Transit Gateway の使用

Amazon VPC コンソールまたは AWS CLI CLI を使用して、Transit Gateway を操作できます。

コンテンツ

Transit Gateway

Transit Gateway を使用すると、VPC と VPN 接続をアタッチして、それらの間でトラフィックをルーティングできます。トランジットゲートウェイは複数のアカウントで機能し AWS アカウント、AWS RAM 他のアカウントとトランジットゲートウェイを共有するために使用できます。トランジットゲートウェイを別のトランジットゲートウェイと共有すると AWS アカウント、アカウントオーナーは自分の VPC をトランジットゲートウェイに接続できます。どちらのアカウントのユーザーも、アタッチメントをいつでも削除できます。

トランジット・ゲートウェイ でマルチキャストを有効にしてから、ドメインに関連付ける VPC アタッチメントを介してマルチキャストソースからマルチキャストグループメンバーにマルチキャストトラフィックを送信できるようにする トランジット・ゲートウェイ マルチキャストドメインを作成できます。

各 VPC または VPN アタッチメントは、単一のルートテーブルに関連付けられています。そのルートテーブルは、そのリソースアタッチメントから来るトラフィックのネクストホップを決定します。Transit Gateway 内のルートテーブルは、IPv4 または IPv6 の両方の CIDR とターゲットを許可します。ターゲットは VPC と VPN 接続です。VPC をアタッチするか、Transit Gateway に VPN 接続を作成すると、その接続は Transit Gateway のデフォルトルートテーブルに関連付けられます。

Transit Gateway 内に追加のルートテーブルを作成し、VPC または VPN の関連付けをこれらのルートテーブルに変更できます。これにより、ネットワークをセグメント化することができます。たとえば、開発 VPC を 1 つのルートテーブルに関連付け、本番 VPC を別のルートテーブルに関連付けることができます。これにより、Transit Gateway 内に、従来のネットワークにおける仮想ルーティングおよび転送 (VRF) と同様の分離された複数のネットワークを作成できるようになります。

Transit Gateway では、アタッチされた VPC と VPN 接続間で動的および静的なルーティングをサポートしています。各アタッチメントのルートの伝播は有効または無効にできます。Transit Gateway ピアリングアタッチメントは、静的ルーティングのみをサポートします。ただし、同じリージョン内の 2 つのトランジットゲートウェイ間のピアリングを指す静的ルートは追加できません。

オプションで、1 つ以上の IPv4 または IPv6 CIDR ブロックを Transit Gateway に関連付けることができます。Transit Gateway Connect アタッチメント用の Transit Gateway Connect ピアを確立するときに、CIDR ブロックから IP アドレスを指定します。任意のパブリックまたはプライベート IP アドレス範囲 (169.254.0.0/16 範囲内のアドレス、ならびに VPC アタッチメントおよびオンプレミスネットワークのアドレスと重複する範囲を除く) を関連付けることができます。IPv4 CIDR ブロックと IPv6 CIDR ブロックの詳細については、「Amazon VPC ユーザーガイド」の「VPC とサブネット」を参照してください。

タスク

- Transit Gateway を作成する
- Transit Gateway の表示
- Transit Gateway のタグを追加または編集する
- Transit Gateway の変更
- Transit Gateway の共有
- リソース共有を受け入れる
- 共有アタッチメントを受け入れる
- Transit Gateway の削除

Transit Gateway を作成する

Transit Gateway を作成すると、デフォルトの Transit Gateway ルートテーブルが作成され、それをデフォルトの関連付けルートテーブルおよびデフォルトの伝達ルートテーブルとして使用します。デフォルトの Transit Gateway ルートテーブルを作成しない場合は、後で作成できます。ルートおよびルートテーブルについての詳細は、「???」を参照してください。

コンソールを使用して Transit Gateway を作成するには

1. アマゾン VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway] を選択します。
3. [Transit Gateway の作成] を選択します。
4. オプションで、[名前タグ] に Transit Gateway の名前を入力します。名前タグを使用すると、ゲートウェイのリストから特定のゲートウェイを識別しやすくなります。[名前タグ] を追加すると、[名前] というキーと、入力した値と同じ値のタグが作成されます。
5. オプションで、[説明] に、Transit Gateway の説明を入力します。
6. [Amazon 側の自律システム番号 (ASN)] は、デフォルト値のままにしてデフォルトの自律システム番号 (ASN) を使用するか、または Transit Gateway のプライベート ASN を入力します。これはボーダー・ゲートウェイ・プロトコル (BGP) AWS セッション側の ASN でなければなりません。

   16 ビット ASN の場合、その範囲は 64512 ー 65534 です。

   32 ビット ASN の場合、その範囲は 4200000000 ー 4294967294 です。

   マルチリージョンのデプロイがある場合は、Transit Gateway にそれぞれ、一意の ASN を使用することをお勧めします。
7. [DNS サポート] で、Transit Gateway にアタッチされている別のVPCのインスタンスから照会されたときに、パブリック IPv4 DNS ホスト名をプライベート IPv4 アドレスに解決するために VPC が必要な場合は、[有効] を選択します。
8. [VPN ECMP サポート] で、VPN トンネル間で 等コストマルチパス(ECMP) ルーティングサポートが必要な場合は、このオプションを選択します。接続が同じ CIDR をアドバタイズする場合、トラフィックは複数の接続間で均等に分散されます。

   このオプションを選択した場合、アドバタイズされた BGP ASN、AS パスなどの BGP 属性、およびコミュニティを同様に設定する必要があります。

   > **Note**
   >
   > ECMP を使用するには、動的ルーティングを使用する VPN 接続を作成する必要があります。静的ルーティングを使用する VPN 接続は、ECMP をサポートしません。
9. [デフォルトルートテーブルの関連付け]で、Transit Gateway アタッチメントを Transit Gateway のデフォルトルートテーブルに自動的に関連付けるには、このオプションを選択します。

10. [デフォルトルートテーブルの伝播] で、Transit Gateway アタッチメントを Transit Gateway のデフォルトルートテーブルに自動的に伝達するには、このオプションを選択します。
11. (オプション) トランジットゲートウェイをマルチキャストトラフィックのルーターとして使用するには、[マルチキャストのサポート] を選択します。
12. [共有アタッチメントを自動的に受け入れる]で、このオプションを選択して、アカウント間のアタッチメントを自動的に受け入れます。
13. (オプション) [Transit Gateway CIDR ブロック] で、[追加 CIDR] を選択し、Transit Gateway の IPv4 または IPv6 CIDR ブロックを 1 つ以上指定します。

    IPv4 の場合は /24 CIDR ブロック以上のサイズ (例: /23 または /22)、IPv6 の場合は /64 CIDR ブロック以上のサイズ (例: /63 または /62) を指定できます。任意のパブリックまたはプライベート IP アドレス範囲 (169.254.0.0/16 範囲内のアドレス、ならびに VPC アタッチメントおよびオンプレミスネットワークのアドレスと重複する範囲を除く) を関連付けることができます。
14. [Transit Gateway の作成] を選択します。

を使用してトランジットゲートウェイを作成するには AWS CLI

create-transit-gatewayコマンドを実行します。

Transit Gateway の表示

コンソールを使用して Transit Gateway を表示するには

1. アマゾン VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [トランジットゲートウェイ] を選択します。Transit Gateway の詳細は、ページのゲートウェイのリストの下に表示されます。

を使用してトランジットゲートウェイを表示するには AWS CLI

describe-transit-gatewaysコマンドを実行します。

Transit Gateway のタグを追加または編集する

目的、所有者、環境などに応じて、タグを整理して識別しやすくするために、リソースにタグを追加します。各 Transit Gateway に対して複数のタグを追加できます。タグキーは、各 Transit Gateway で一意である必要があります。すでに Transit Gateway に関連付けられているキーを持つタグを追

加すると、そのキーの値が更新されます。詳細については、「Amazon EC2 リソースにタグを付ける」を参照してください。

コンソールを使用して Transit Gateway にタグを追加する

1. アマゾン VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [トランジットゲートウェイ] を選択します。
3. タグを追加または編集する Transit Gateway を選択します。
4. ページ下部の [タグ] タブをクリックします。
5. [Manage tags (タグの管理)] を選択します。
6. 新しいタグを追加を選択します。
7. タグの [キー] と [値] を入力します。
8. [Save] を選択します。

Transit Gateway の変更

Transit Gateway の設定オプションを変更できます。Transit Gateway を変更すると、変更されたオプションは新しい Transit Gateway アタッチメントにのみ適用されます。既存の Transit Gateway アタッチメントは変更されず、サービスの中断も見られません。

共有されている Transit Gateway を変更することはできません。

現在 Connect ピアについて IP アドレスのいずれかが使用されている場合は、トランジットゲートウェイの CIDR ブロックを削除できません。

Transit Gateway を変更するには

1. アマゾン VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway] を選択します。
3. 変更するTransit Gatewayを選択します。
4. アクション、Transit Gateway の変更を選択します。
5. 必要に応じてオプションを変更し、[トランジットゲートウェイの変更] をクリックします。

を使用してトランジットゲートウェイを変更するには AWS CLI

modify-transit-gatewayコマンドを実行します。

Transit Gateway の共有

AWS RAM を使用して、のアカウント間または組織全体でトランジットゲートウェイを共有できます AWS Organizations。以下の手順に従って、所有する Transit Gateway を共有します。

組織の管理アカウントで、リソース共有を有効にしておく必要があります。リソース共有を有効にする方法については、AWS RAM ユーザーガイドの「AWS Organizations との共有を有効にする」を参照してください。

Transit Gateway を共有するには

1. https://console.aws.amazon.com/ram/ AWS RAM でコンソールを開きます。
2. [リソースの共有の作成] を選択します。
3. [名前] に、リソース共有のわかりやすい名前を入力します。
4. [リソースタイプの選択] で、[トランジットゲートウェイ] を選択します。Transit Gateway を選択します。
5. (オプション) [プリンシパル] で、リソース共有にプリンシパルを追加します。OU AWS アカウント、または組織ごとに ID を指定し、[追加] を選択します。

   [外部アカウントを許可] で、 AWS アカウント このリソースを組織外のユーザーと共有することを許可するかどうかを選択します。
6. (オプション) [タグ] に、各タグのキーと値のペアを入力します。これらのタグはリソース共有には適用されますが、Transit Gateway には適用されません。
7. [リソース共有の作成] を選択します。

リソース共有を受け入れる

ユーザーがリソース共有に追加された場合は、リソース共有に参加するための招待状を受け取ります。共有リソースにアクセスする前に、リソース共有を受け入れる必要があります。

リソース共有を受け入れるには

1. https://console.aws.amazon.com/ram/ AWS RAM でコンソールを開きます。
2. ナビゲーションペインで、[自分と共有]、[リソース共有] の順に選択します。
3. リソース共有を選択します。
4. [リソース共有を受け入れる] を選択します。

5. 共有された Transit Gateway を表示するには、Amazon VPC コンソールで [Transit Gateway] ページを開きます。

共有アタッチメントを受け入れる

トランジットゲートウェイの作成時に [共有アタッチメントの自動承諾] 機能を有効にしなかった場合は、クロスアカウント (共有) アタッチメントを手動で受け入れる必要があります。

共有アタッチメントを手動で受け入れるには

1. アマゾン VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. 承認保留中の Transit Gateway アタッチメントを選択します。
4. アクション、Transit Gateway アタッチメントを受け入れるを選択します。

を使用して共有添付ファイルを受け付けるには AWS CLI

accept-transit-gateway-vpc-attach コマンドを使用してください。

Transit Gateway の削除

既存のアタッチメントを含む Transit Gateway を削除することはできません。Transit Gateway を削除する前に、すべてのアタッチメントを削除する必要があります。

コンソールを使用して Transit Gateway を削除するには

1. アマゾン VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. 削除する Transit Gateway を選択します。
3. アクション,Transit Gateway の削除を選択します。「**delete**」と入力して、[Delete (削除)] を選択して削除を確認します。

を使用してトランジットゲートウェイを削除するには AWS CLI

delete-transit-gatewayコマンドを実行します。

VPC への Transit Gateway アタッチメント

Transit Gateway に VPC をアタッチするときは、トラフィックをルーティングするために Transit Gateway によって使用される各アベイラビリティーゾーンから 1 つのサブネットを指定する必要があります。1 つのアベイラビリティーゾーンから 1 つのサブネットを指定すると、そのアベイラビリティーゾーン内のすべてのサブネットのリソースにトラフィックが到達できるようになります。

制限

- VPC を Transit Gateway にアタッチしても、Transit Gateway のアタッチメントが存在しないアベイラビリティーゾーンのリソースは、Transit Gateway に到達できません。Transit Gateway へのルートがサブネットルートテーブルにある場合、トラフィックが Transit Gateway に転送されるのは、Transit Gateway のアタッチメントが同じアベイラビリティーゾーンのサブネットにある場合のみです。
- Transit Gateway にアタッチされている VPC 内のリソースは、同じ Transit Gateway にもアタッチされている別の VPC のセキュリティグループにはアクセスできません。
- Transit Gateway は、Amazon Route 53 でプライベートホストゾーンを使用してセットアップされた、アタッチされた VPC のカスタム DNS 名に対する DNS 解決をサポートしていません。トランジットゲートウェイに接続されたすべての VPC のプライベートホストゾーンの名前解決を設定するには、「Amazon Route 53 と AWS Transit Gateway によるハイブリッドクラウドの集中型 DNS 管理」を参照してください。
- Transit Gateway は、同じ CIDR を持つ VPC 間のルーティングをサポートしていません。VPC を Transit Gateway にアタッチし、その CIDR が Transit Gateway にすでにアタッチされている別の VPC の CIDR と同じ場合、新しくアタッチされた VPC のルートは Transit Gateway ルートテーブルに伝達されません。
- ローカルゾーンに存在する VPC サブネットのアタッチメントを作成することはできません。ただし、ローカルゾーンのサブネットを、親アベイラビリティーゾーンを介して Transit Gateway に接続できるようにネットワークを設定することが可能です。詳細については、「ローカルゾーンのサブネットを Transit Gateway に接続する」を参照してください。
- IPv6 のみのサブネットを使用して Transit Gateway アタッチメントを作成することはできません。Transit Gateway アタッチメントのサブネットは IPv4 アドレスもサポートする必要があります。
- Transit Gateway をルートテーブルに追加するには、Transit Gateway に少なくとも 1 つの VPC アタッチメントが必要です。

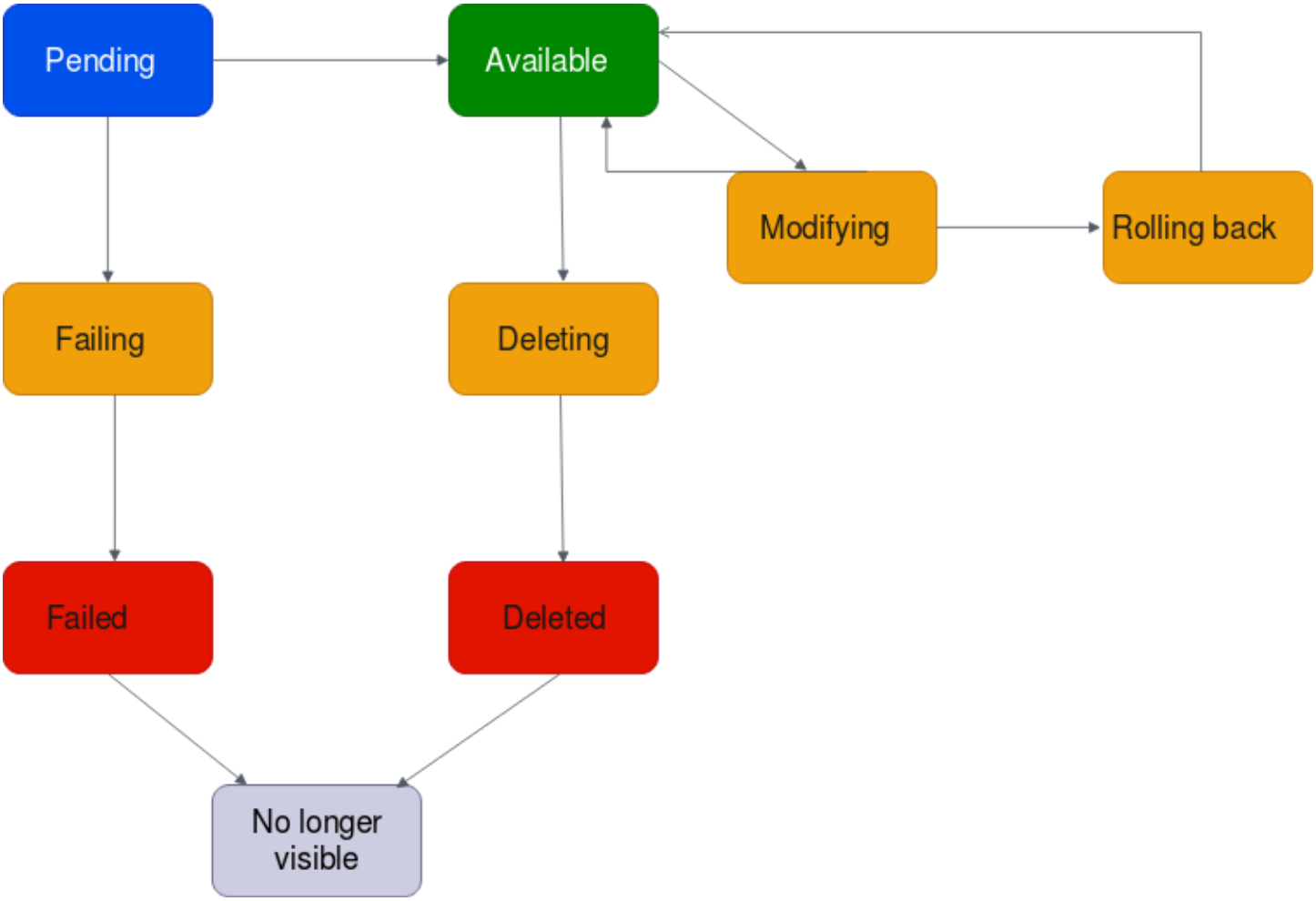
コンテンツ

- VPC アタッチメントのライフサイクル
- VPC への Transit Gateway アタッチメントの作成
- VPC アタッチメントを変更する
- VPC アタッチメントタグを変更する
- VPC アタッチメントの表示
- VPC アタッチメントの削除
- VPC アタッチメントの作成のトラブルシューティング

VPC アタッチメントのライフサイクル

VPC アタッチメントは、リクエストが開始された時点から、さまざまな段階を経ることになります。それぞれのステージで実行可能なアクションがあり、そのライフサイクルの最後で、VPC アタッチメントは Amazon Virtual Private Cloud Console と API またはコマンドライン出力に一定期間表示されます。

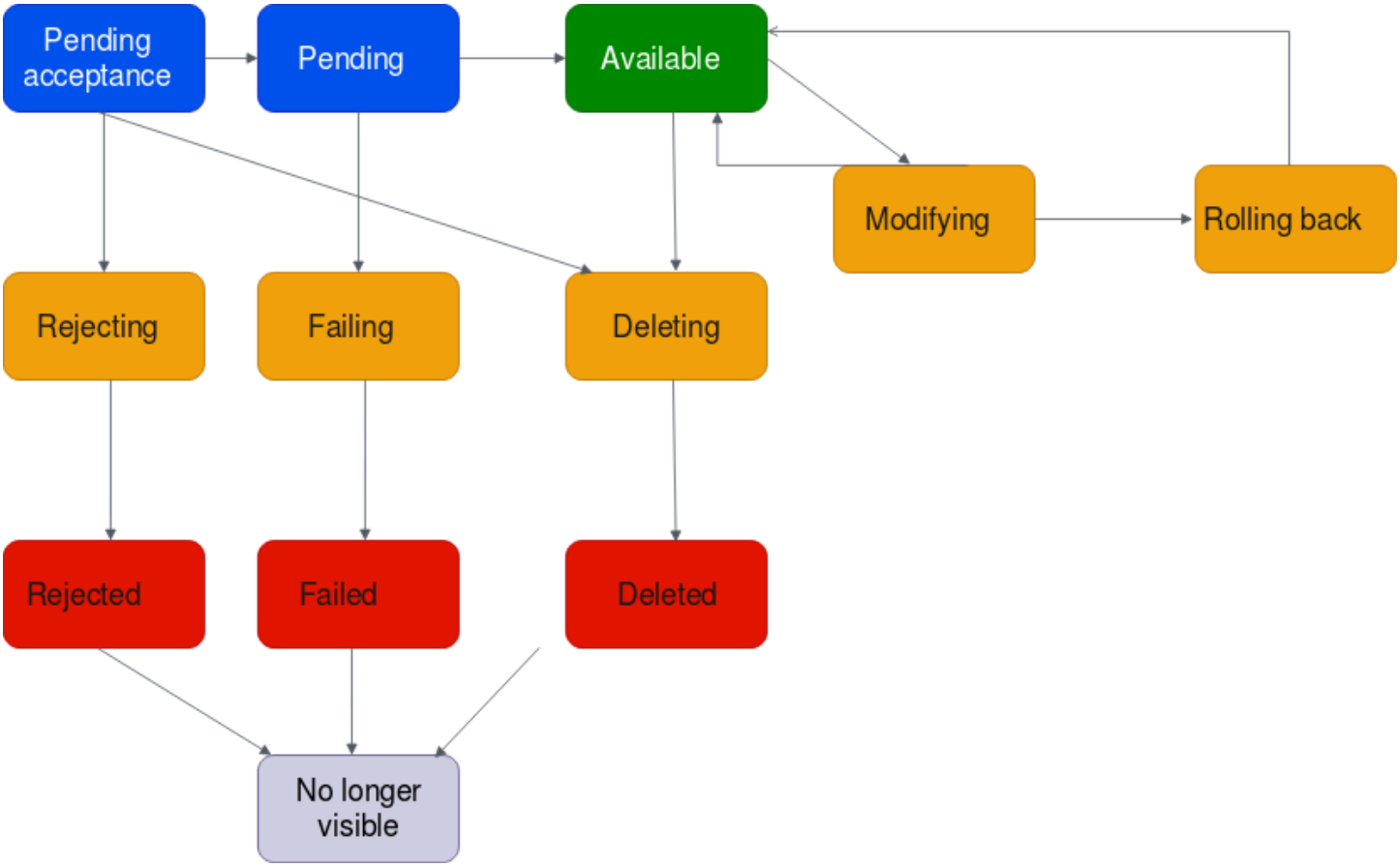
次の図は、単一のアカウント設定、または [共有アタッチメントを自動承諾] がオンになっているクロスアカウント設定で、アタッチメントが経る可能性のある状態を示しています。



- Pending (保留中): VPC アタッチメントのリクエストが開始され、プロビジョニングプロセス中です。この段階では、アタッチメントは失敗するか、または `available` になる場合があります。
- Failing (失敗する可能性あり): VPC アタッチメントのリクエストが失敗する可能性があります。この段階では、VPC アタッチメントは `failed` になります。
- Failed (失敗): VPC アタッチメントのリクエストが失敗しました。この状態では、削除できません。失敗した VPC アタッチメントは 2 時間表示されたままになり、その後に表示されなくなります。
- Available (使用可能): VPC アタッチメントは使用可能で、トラフィックは VPC とトランジットゲートウェイ間でフローできます。この段階では、アタッチメントは `modifying` または `deleting` になる場合があります。
- Deleting (削除中): 削除中の VPC アタッチメント。この段階では、アタッチメントは `deleted` になる場合があります。

- Deleted (削除済み): `available` VPC アタッチメントが削除されました。この状態では、VPC アタッチメントは変更できません。VPC アタッチメントは 2 時間表示されたままになり、その後に表示されなくなります。
- Modifying (変更中): VPC アタッチメントのプロパティを変更するリクエストが作成されました。この段階では、アタッチメントは `available` または `rolling back` になる場合があります。
- Rolling back (ロールバック中): VPC アタッチメントの変更リクエストを完了できず、システムによって行われた変更がすべて元に戻されようとしています。この段階では、アタッチメントは `available` になる場合があります。

次の図は、[Auto accept shared attachments] (共有アタッチメントを自動承諾) がオフになっているクロスアカウント設定で、アタッチメントが経る可能性のある状態を示しています。



- Pending-acceptance (承諾の保留中): VPC アタッチメントのリクエストは承諾を待っています。この段階では、アタッチメントは `pending`、`rejecting`、または `deleting` になる場合があります。
- Rejecting (拒否中): 拒否処理中の VPC アタッチメント。この段階では、アタッチメントは `rejected` になる場合があります。

- Rejected (拒否): pending acceptance VPC アタッチメントが拒否されました。この状態では、VPC アタッチメントは変更できません。VPC アタッチメントは 2 時間表示されたままになり、その後に表示されなくなります。
- Pending (保留中): VPC アタッチメントが承諾され、プロビジョニングプロセス中です。この段階では、アタッチメントは失敗するか、または available になる場合があります。
- Failing (失敗する可能性あり): VPC アタッチメントのリクエストが失敗する可能性があります。この段階では、VPC アタッチメントは failed になります。
- Failed (失敗): VPC アタッチメントのリクエストが失敗しました。この状態では、削除できません。失敗した VPC アタッチメントは 2 時間表示されたままになり、その後に表示されなくなります。
- Available (使用可能): VPC アタッチメントは使用可能で、トラフィックは VPC とトランジットゲートウェイ間でフローできます。この段階では、アタッチメントは modifying または deleting になる場合があります。
- Deleting (削除中): 削除中の VPC アタッチメント。この段階では、アタッチメントは deleted になる場合があります。
- 削除した : available または pending acceptance VPC アタッチメントが削除されました。この状態では、VPC アタッチメントは変更できません。VPC アタッチメントは 2 時間表示されたままになり、その後に表示されなくなります。
- Modifying (変更中): VPC アタッチメントのプロパティを変更するリクエストが作成されました。この段階では、アタッチメントは available または rolling back になる場合があります。
- Rolling back (ロールバック中): VPC アタッチメントの変更リクエストを完了できず、システムによって行われた変更がすべて元に戻されようとしています。この段階では、アタッチメントは available になる場合があります。

VPC への Transit Gateway アタッチメントの作成

コンソールを使用して VPC アタッチメントを作成するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. [Transit Gateway アタッチメントの作成] を選択します。
4. オプションで、[名前タグ] に Transit Gateway アタッチメントの名前を入力します。
5. [Transit Gateway ID] で、アタッチメントの Transit Gateway を選択します。所有している Transit Gateway、または自分と共有された Transit Gateway を選択できます。

6. [添付タイプ] で、[VPC] を選択します。
7. DNS Support、IPv6 Support 、アプライアンスモードサポートを有効にするかどうかを選択します。

   アプライアンスモードが選択されている場合、送信元と宛先間のトラフィックフローは、そのフローの存続期間中、VPC アタッチメントに同じアベイラビリティーゾーンを使用します。
8. [VPC ID] で、Transit Gateway にアタッチする VPC を選択します。

   この VPC には少なくとも 1 つのサブネットが関連付けられている必要があります。
9. [サブネット ID] で、トラフィックをルーティングするためにトランジットゲートウェイが使用するアベイラビリティーゾーンごとに 1 つのサブネットを選択します。少なくとも 1 つのサブネットを選択する必要があります。アベイラビリティーゾーンごとに 1 つだけサブネットを選択できます。
10. [Transit Gateway アタッチメントの作成] を選択します。

を使用して VPC アタッチメントを作成するには AWS CLI

create-transit-gateway-vpc-attach コマンドを使用してください。

VPC アタッチメントを変更する

コンソールを使用して VPC アタッチメントを変更するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. VPC アタッチメントを選択後、アクション,Transit Gateway のアタッチメントの変更。
4. DNS サポートを有効にするには、[DNS サポート] を選択します。
5. サブネットをアタッチメントに追加するには、サブネットの横にあるボックスをオンにします。

   VPC アタッチメントサブネットを追加または変更すると、アタッチメントが変更状態のときにデータトラフィックに影響を与える可能性があります。
6. Transit Gateway のアタッチメントの変更を選択します。

を使用して VPC アタッチメントを変更するには AWS CLI

modify-transit-gateway-vpc-attach コマンドを使用してください。

VPC アタッチメントタグを変更する

コンソールを使用して VPC アタッチメントタグを変更するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. VPC アタッチメントを選択後、[アクション]、[タグの管理] の順に選択します。
4. [タグの追加] [新しいタグの追加] を選択して、以下を実行します。
   - [キー] にはキー名を入力します。
   - [値] にキー値を入力します。
5. [Remove a tag (タグの削除)] タグの横にある [削除] を選択します。
6. [Save] を選択します。

VPC アタッチメントタグは、コンソールを使用してのみ変更できます。

VPC アタッチメントの表示

コンソールを使用して VPC アタッチメントを表示するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. [リソースタイプ]列で、VPCを探します。これらは VPC アタッチメントです。
4. 詳細を表示するには、アタッチメントを選択します。

を使用して VPC アタッチメントを表示するには AWS CLI

describe-transit-gateway-vpc-attachments コマンドを使用してください。

VPC アタッチメントの削除

コンソールを使用して VPC アタッチメントを削除するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. VPC アタッチメントを選択します。

4. アクション、Transit Gateway のアタッチメントの削除を選択します。
5. 確認を求めるメッセージが表示されたら、「**delete**」と入力し、[削除] を選択します。

を使用して VPC アタッチメントを削除するには AWS CLI

delete-transit-gateway-vpc-attach コマンドを使用してください。

VPC アタッチメントの作成のトラブルシューティング

次のトピックは、VPC アタッチメントの作成時に発生する可能性のある問題のトラブルシューティングに役立ちます。

問題

VPC アタッチメントが失敗しました。

原因

原因は、次のいずれかである可能性があります。

1. VPC アタッチメントを作成しているユーザーは、サービスにリンクされたロールを作成するための適切なアクセス権限を持っていません。
2. IAM リクエストが多すぎるため、スロットリングの問題が発生しています。例えば、 AWS CloudFormation を使用してアクセス許可とロールを作成している場合などです。
3. サービスにリンクされたロールがアカウントにあり、サービスにリンクされたロールが変更されました。
4. トランジットゲートウェイは `available` 状態にありません。

ソリューション

原因に応じて、次をお試しください。

1. サービスにリンクされたロールを作成するための適切なアクセス権限がユーザーに付与されていることを確認します。詳細については、「IAM ユーザーガイド」の「サービスリンクロールのアクセス許可」を参照してください。ユーザーにアクセス権限が付与されたら、VPC アタッチメントを作成します。
2. コンソールまたは API を通じて VPC アタッチメントを手動で作成します。詳細については、「the section called “VPC への Transit Gateway アタッチメントの作成”」を参照してください。

3. サービスにリンクされたロールに正しいアクセス権限があることを確認します。詳細については、「the section called “Transit Gateway”」を参照してください。
4. トランジットゲートウェイが `available` 状態であることを確認します。詳細については、「the section called “Transit Gateway の表示”」を参照してください。

Transit Gateway VPN アタッチメント

VPN 接続を Transit Gateway にアタッチするには、カスタマーゲートウェイを指定する必要があります。カスタマーゲートウェイデバイスの要件の詳細については、「AWS Site-to-Site VPN ユーザーガイド」の「カスタマーゲートウェイデバイスの要件」を参照してください。

静的 VPN の場合は、静的ルートを Transit Gateway ルートテーブルに追加します。

VPN への Transit Gateway アタッチメントの作成

コンソールを使用して VPN アタッチメントを作成するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. [Transit Gateway アタッチメントの作成] を選択します。
4. [Transit Gateway ID] で、アタッチメントの Transit Gateway を選択します。所有している Transit Gateway を選択できます。
5. [アタッチメントタイプ] で、[VPN] を選択します。
6. [カスタマーゲートウェイ] で、以下のいずれかを実行します。
   - 既存のカスタマーゲートウェイを使用するには、[Existing (既存)] を選択してから、使用するゲートウェイを選択します。

     カスタマーゲートウェイが NAT トラバーサル (NAT-T) が有効になっているネットワークアドレス変換 (NAT) の内側にある場合は、NAT デバイスのパブリック IP アドレスを使用し、UDP ポート 4500 をブロックしないようにファイアウォールルールを調整します。
   - カスタマーゲートウェイを作成するには、[New] を選択し、[IP アドレス] に静的パブリック IP アドレスと [BGP ASN] を入力します。

     [ルーティング] オプションで、[動的] と [静的] のどちらを使用するかを選択します。詳細については、「AWS Site-to-Site VPN ユーザーガイド」の「Site-to-Site VPN のルーティングオプション」を参照してください。

7. [Tunnel Options] (トンネルオプション) で、トンネルの CIDR 範囲と事前共有キーを入力します。詳細については、Site-to-Site VPN アーキテクチャをご参照ください。
8. [Transit Gateway アタッチメントの作成] を選択します。

を使用して VPN アタッチメントを作成するには AWS CLI

create-vpn-connectionコマンドを実行します。

VPN アタッチメントの表示

コンソールを使用して VPN アタッチメントを表示するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. 左[リソースタイプ]列、探してVPN。これらは VPN アタッチメントです。
4. アタッチメントを選択して、詳細を表示したりタグを追加したりします。

を使用して VPN 添付ファイルを表示するには AWS CLI

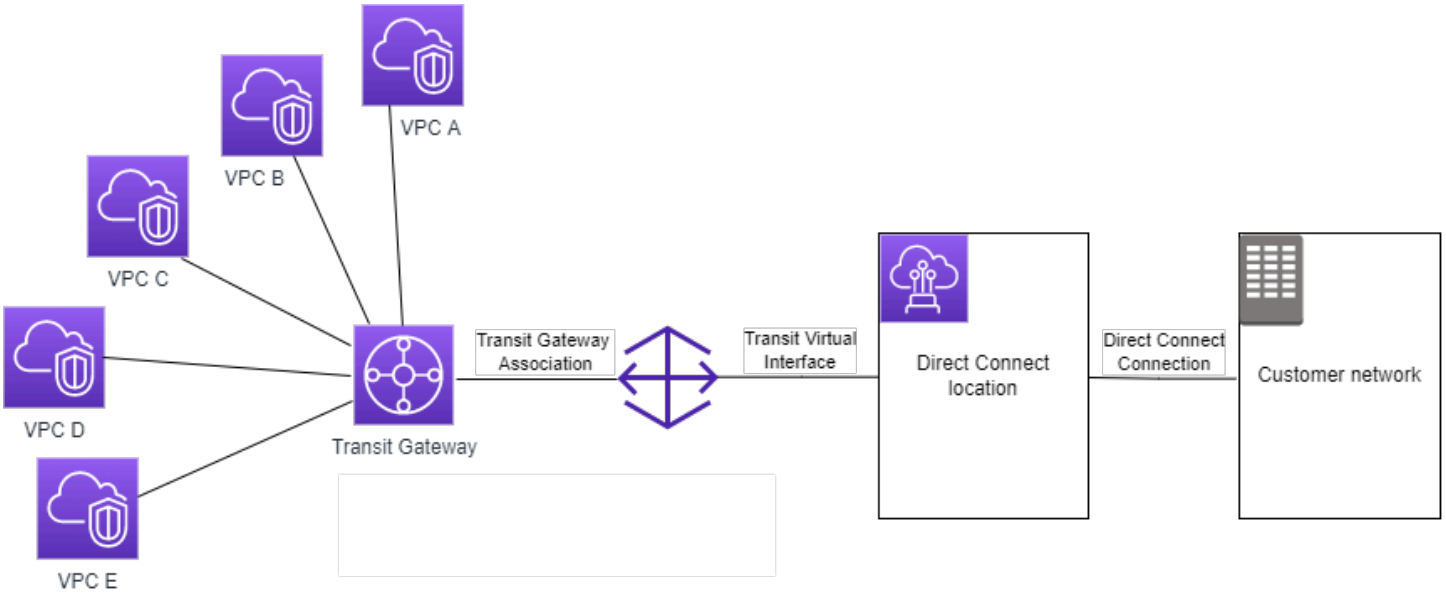
describe-transit-gateway-attachmentsコマンドを実行します。

Direct Connect ゲートウェイへのトランジットゲートウェイアタッチメント

トランジットゲートウェイで Direct Connect ゲートウェイアタッチメントを操作します。この設定には次のような利点があります。以下を実行できます。

- 同じリージョンにある複数の VPN または VPC に対して 1 つの接続を管理する。
- オンプレミスからAWSに、またはAWSからオンプレミスにプレフィックスをアドバタイズする。

次の図は、Direct Connect ゲートウェイによって、すべての VPC が使用できる Direct Connect 接続に 1 つの接続を作成する方法を示しています。



このソリューションには、次のコンポーネントが必要です。

- トランジットゲートウェイ。
- Direct Connect ゲートウェイ
- Direct Connect ゲートウェイと Transit Gateway の間の関連付け。
- トランジット仮想インターフェイスを使用して、Direct Connect ゲートウェイにトランジットゲートウェイをアタッチします。

トランジットゲートウェイを使用した Direct Connect ゲートウェイの設定の詳細については、AWS Direct Connectユーザーガイドの「トランジットゲートウェイの関連付け」を参照してください。

Transit Gateway ピアリングアタッチメント

リージョン内 Transit Gateway とリージョン間 Transit Gateway の両方をピアリングし、IPv4 および IPv6 トラフィックを含むそれらの間でトラフィックをルーティングできます。これを行うには、Transit Gateway にピアリングアタッチメントを作成し、Transit Gateway を指定します。ピアトランジットゲートウェイは、お客様のアカウントまたは別の AWS アカウント にある場合があります。

ピアリングアタッチメントリクエストを作成した後、ピアTransit Gateway（アクセプタTransit Gateway とも呼ばれる）の所有者がリクエストを受け入れる必要があります。Transit Gateway 間でトラフィックをルーティングするには、Transit Gateway のピアリングアタッチメントをポイントする静的ルートをTransit Gateway のルートテーブルに追加します。

将来のルート伝達機能を利用するために、ピアリングされたTransit Gateway に一意の ASN を使用することをお勧めします。

トランジットゲートウェイ ピアリングは、別のリージョンの Amazon Route 53 Resolver を使用してトランジットゲートウェイピアリングアタッチメントのどちらかの側の VPC 全体で、パブリックまたはプライベート IPv4 DNS ホスト名をプライベート IPv4 アドレスに解決することをサポートしていません。Route 53 リゾルバーの詳細については、「Amazon Route 53 デベロッパーガイド」の「Route 53 Resolver の使用開始」を参照してください。

リージョン間のゲートウェイピアリングでは、VPC ピアリングと同じネットワークインフラストラクチャを使用します。したがって、トラフィックはリージョン間を移動する際、仮想ネットワークレイヤーで AES-256 暗号化を使用して暗号化されます。トラフィックが AWS の物理的な制御の外部にあるネットワークリンクを通過する場合は、物理レイヤーで AES-256 暗号化を使用して暗号化されます。その結果、トラフィックは、AWS の物理的な制御の外部にあるネットワークリンク上で二重に暗号化されます。同じリージョン内では、トラフィックは、AWS の物理的な制御の外部にあるネットワークリンクを通過する場合にのみ、物理レイヤーで暗号化されます。

Transit Gateway ピアリングアタッチメントがサポートされているリージョンについては、AWS Transit Gateway に関するよくある質問のページを参照してください。

ピアリングアタッチメントの作成

開始する前に、アタッチするTransit Gateway の ID があることを確認します。Transit Gateway が別の AWS アカウントにある場合は、Transit Gateway の所有者の AWS アカウント ID を持っていることを確認します。

ピアリングアタッチメントを作成した後、アクセプタTransit Gateway の所有者はアタッチメントリクエストを受け入れる必要があります。

コンソールを使用して、ピアリングアタッチメントを作成するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. [Transit Gateway アタッチメントの作成] を選択します。
4. [Transit Gateway ID] で、アタッチメントの Transit Gateway を選択します。所有している Transit Gateway 、または自分と共有されたTransit Gateway を選択できます。
5. [アタッチメントの種類] で、[ピア接続] を選択します。
6. 必要に応じて、アタッチメントの名前タグを入力します。

7. [アカウント] で、次のいずれかを実行します。
   - Transit Gateway がアカウントにある場合は、[マイアカウント] を選択します。
   - Transit Gateway が別の AWS アカウントにある場合は、[他のアカウント] を選択します。[アカウント ID] に AWS アカウント ID を入力します。
8. [リージョン] で、Transit Gateway があるリージョンを選択します。
9. [Transit Gateway ID (アクセプタ)] に、アタッチする Transit Gateway の ID を入力します。
10. [Transit Gateway アタッチメントの作成] を選択します。

AWS CLI を使用して、ピアリングアタッチメントを作成するには

create-transit-gateway-peering-attachment コマンドを使用します。

ピアリングアタッチメントリクエストの承諾または拒否

ピアリングアタッチメントをアクティブにするには、アクセプタ Transit Gateway の所有者がピアリングアタッチメントリクエストを受け入れる必要があります。これは、両方の Transit Gateway が同じアカウントにある場合でも必要です。ピアリングアタッチメントは `pendingAcceptance` 状態である必要があります。アクセプタ Transit Gateway が配置されているリージョンからのピアリングアタッチメントリクエストを受け入れます。

または、受信した VPC ピア接続リクエストで `pendingAcceptance` 状態にあるものを拒否できます。アクセプタ Transit Gateway があるリージョンからのリクエストを拒否する必要があります。

コンソールを使用して、ピアリングアタッチメントリクエストを受け入れるには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. 承認保留中の Transit Gateway ピアリングアタッチメントを選択します。
4. アクション、Transit Gateway アタッチメントを受け入れるを選択します。
5. 静的ルートを Transit Gateway のルートテーブルに追加します。詳細については、「the section called “静的ルートを作成する”」を参照してください。

コンソールを使用して、ピアリングアタッチメントリクエストを拒否するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。

2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. 承認保留中の Transit Gateway ピアリングアタッチメントを選択します。
4. アクション、Transit Gateway アタッチメントを拒否するを選択します。

AWS CLI を使用して、ピアリングアタッチメントを承諾または拒否するには

accept-transit-gateway-peering-attachment コマンドおよび reject-transit-gateway-peering-attachment コマンドを使用します。

Transit Gateway のルートテーブルへのルートの追加

ピアリングされた Transit Gateway 間でトラフィックをルーティングするには、Transit Gateway のピアリングアタッチメントをポイントする静的ルートを Transit Gateway のルートテーブルに追加する必要があります。アクセプタTransit Gateway の所有者も、Transit Gateway ルートテーブルに静的ルートを追加する必要があります。

コンソールを使用して静的ルートを作成するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway ルートテーブル] を選択します。
3. ルートを作成するルートテーブルを選択します。
4. [アクション]、[静的ルートの作成] の順に選択します。
5. [静的ルートの作成] ページに、ルートを作成する CIDR ブロックを入力します。たとえば、ピア Transit Gateway にアタッチされている VPC の CIDR ブロックを指定します。
6. ルートのピアリングアタッチメントを選択します。
7. [静的ルートの作成] を選択します。

AWS CLI を使用して静的ルートを作成するには

create-transit-gateway-route コマンドを使用します。

> **Important**
>
> ルートを作成したら、Transit Gateway ルートテーブルをTransit Gateway ピアリングアタッチメントに関連付けます。詳細については、「the section called “Transit Gateway ルートテーブルの関連付け”」を参照してください。

Transit Gateway ピアリング接続アタッチメントの表示

Transit Gateway のピアリングアタッチメントとその情報を表示できます。

コンソールを使用して、ピアリングアタッチメントを表示するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. [リソースタイプ]列で、ピアリングを探します。これらはピアリングアタッチメントです。
4. 詳細を表示するには、アタッチメントを選択します。

AWS CLI を使用して、Transit Gateway ピアリングアタッチメントを表示するには

describe-transit-gateway-peering-attachments コマンドを使用します。

ピアリングタッチメントを削除する

Transit Gateway ピアリングアタッチメントを削除できます。いずれかの Transit Gateway の所有者は、アタッチメントを削除できます。

コンソールを使用して、ピアリングアタッチメントを削除するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. Transit Gateway ピアリングアタッチメントを選択します。
4. アクション,Transit Gateway のアタッチメントの削除を選択します。
5. 「**`delete`**」と入力し、[Delete (削除)] を選択します。

AWS CLI を使用して、ピアリングアタッチメントを削除するには

delete-transit-gateway-peering-attachment コマンドを使用します。

オプトインAWSリージョンに関する考慮事項

オプトインリージョンの境界を越えて Transit Gateway をピアリングできます。これらのリージョンの詳細とオプトイン方法については、「Amazon Web Services 全般のリファレンス」の「AWS リージョンの管理」を参照してください。これらのリージョンで Transit Gateway ピアリングを使用する場合は、次の点を考慮に入れてください。

- ピアリングアタッチメントを受け入れるアカウントがそのリージョンにオプトインされている限り、オプトインリージョンにピアリングできます。
- リージョンのオプトインステータスにかかわらず、AWSは、ピアリングアタッチメントを受け入れるアカウントと次のアカウントデータを共有します。
  - AWS アカウント ID
  - 転送ゲートウェイ ID
  - リージョンコード
- Transit Gateway のアタッチメントを削除すると、上記のアカウントデータが削除されます。
- リージョンをオプトアウトする前に、Transit Gateway ピアリングのアタッチメントを削除することを推奨します。ピアリングアタッチメントを削除しないと、トラフィックがアタッチメントを通過し続け、引き続き課金される可能性があります。アタッチメントを削除しない場合は、オプトインし直し、アタッチメントを削除できます。
- 一般に、Transit Gateway には送信者支払いモデルがあります。オプトイン境界を越えて Transit Gateway ピアリングアタッチメントを使用すると、アタッチメントを受け入れるリージョン (オプトインしていないリージョンを含む) で料金が発生する可能性があります。詳細については、AWSTransit Gateway の料金を参照してください。

Transit Gateway Connect アタッチメントと Transit Gateway Connect ピア

Transit Gateway Connect アタッチメントを作成して、Transit Gateway と VPC で実行されているサードパーティー仮想アプライアンス (SD-WAN アプライアンスなど) 間の接続を確立できます。Connect アタッチメントは、総称ルーティングカプセル化 (GRE)トンネルプロトコルをサポートして高パフォーマンスを実現し、ボーダーゲートウェイプロトコル (BGP) をサポートして動的ルーティングをサポートします。Connect アタッチメントを作成したら、Connect アタッチメントに 1 つ以上の GRE トンネル (Transit Gateway Connect ピアとも呼ばれます) を作成して、Transit Gateway とサードパーティーアプライアンスを接続できます。ルーティング情報を交換するために、GRE トンネル上で 2 つの BGP セッションを確立します。

> **Important**
>
> Transit Gateway Connect ピアは、AWS が管理するインフラストラクチャで終了する 2 つの BGP ピアリングセッションで構成されます。2 つの BGP ピアリングセッションによってルーティングプレーンに冗長性が備わり、1 つの BGP ピアリングセッションが失われてもルーティング操作に影響しないようになります。両方の BGP セッションから受信したルー

ティング情報は、指定された Connect ピアに対して蓄積されます。BGP ピアリングセッションが 2 つあることで、日常的なメンテナンス、パッチ適用、ハードウェアのアップグレード、交換などの AWS インフラストラクチャ運用に対しても保護されます。Connect ピアが、冗長性のために設定することが推奨されているデュアル BGP ピアリングセッションなしで動作している場合、AWS インフラストラクチャ運用中に接続が一時的に失われる可能性があります。Connect ピアで、BGP ピアリングセッションを両方設定することを強くお勧めします。アプライアンス側で高可用性をサポートするように複数の Connect ピアを設定している場合は、各 Connect ピアに両方の BGP ピアリングセッションを設定することをお勧めします。

Connect アタッチメントは、基盤となるトランスポートメカニズムとして、既存の VPC または Direct Connect アタッチメントを使用します。これは、トランスポートアタッチメントと呼ばれます。トランジットゲートウェイは、サードパーティーアプライアンスからの一致した GRE パケットを 接続 アタッチメントからのトラフィックとして識別します。送信元または送信先情報が正しくない GRE パケットを含む、その他のパケットは、トランスポートアタッチメントからのトラフィックとして扱われます。

> **Note**
>
> Direct Connect アタッチメントを転送メカニズムとして使用するには、まず Direct Connect を AWS Transit Gateway と統合する必要があります。この統合を作成する手順については、「Integrate SD-WAN devices with AWS Transit Gateway and AWS Direct Connect」を参照してください。

目次

Connect ピア

Connect ピア (GRE トンネル) は以下のコンポーネントで構成されます。

内部の CIDR ブロック (BGP アドレス)

BGP ピアリングに使用される内部 IP アドレス。IPv4 の 169.254.0.0/16 範囲から /29 CIDR ブロックを指定する必要があります。オプションで、IPv6 の fd00::/8 範囲から /125 CIDR ブロックを指定できます。以下の CIDR ブロックは予約済みで使用できません。

- 169.254.0.0/29
- 169.254.1.0/29
- 169.254.2.0/29
- 169.254.3.0/29
- 169.254.4.0/29
- 169.254.5.0/29
- 169.254.169.248/29

アプライアンスの IPv4 範囲の最初のアドレスを BGP IP アドレスとして設定する必要があります。IPv6 を使用する場合、内部 CIDR ブロックが fd00::/125 の場合は、アプライアンスのトンネルインターフェイスでこの範囲 (fd00::1) の最初のアドレスを設定する必要があります。

BGP アドレスは、トランジットゲートウェイ上のすべてのトンネルで一意である必要があります。

ピア IP アドレス

Connect ピアのアプライアンス側のピア IP アドレス (GRE 外部 IP アドレス)。これは任意の IP アドレスにすることができます。IP アドレスは IPv4 アドレスまたは IPv6 アドレスとすることができますか、トランジットゲートウェイアドレスと同じ IP アドレスファミリーである必要があります。

トランジットゲートウェイアドレス

Connect ピアのトランジットゲートウェイ側のピア IP アドレス (GRE 外部 IP アドレス)。IP アドレスは、トランジットゲートウェイ CIDR ブロックから指定される必要があります。また、トランジットゲートウェイの 接続 アタッチメント全体で一意である必要があります。IP アドレスを指定しない場合、トランジットゲートウェイ CIDR ブロックから最初に使用可能なアドレスが使用されます。

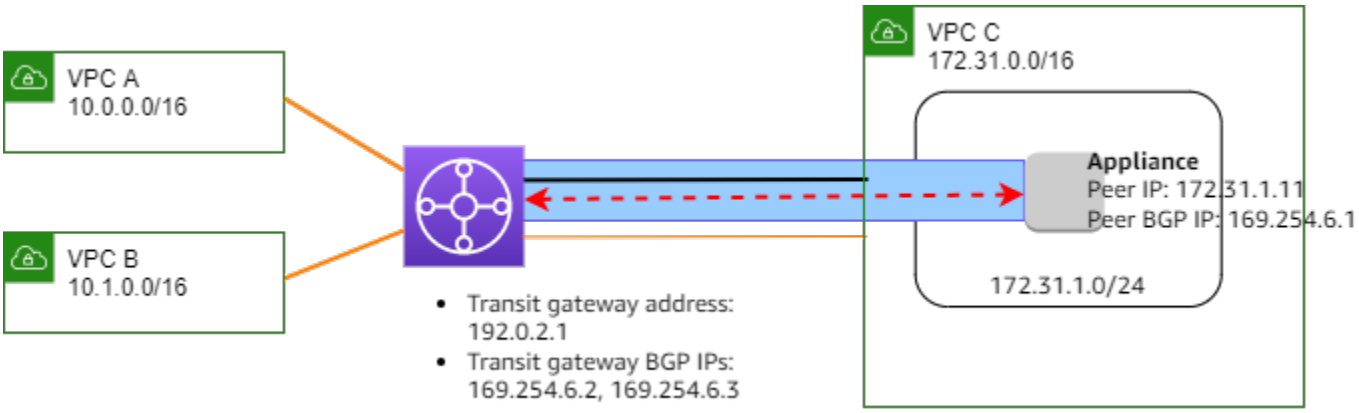
トランジットゲートウェイを作成または変更するときに、トランジットゲートウェイ CIDR ブロックを追加できます。

IP アドレスは IPv4 アドレスまたは IPv6 アドレスとすることができますか、ピア IP アドレスと同じ IP アドレスファミリーである必要があります。

ピア IP アドレスとトランジットゲートウェイアドレスは、GRE トンネルを一意に識別するために使用されます。複数のトンネル全体でいずれかのアドレスを再利用することはできますが、同じトンネル内で両方を再利用することはできません。

BGP ピアリングの Transit Gateway Connect は、マルチプロトコル BGP (MP-BGP) のみをサポートします。ここで、IPv6 ユニキャストの BGP セッションを確立するために IPv4 ユニキャストアドレスも必要です。GRE 外部 IP アドレスには IPv4 と IPv6 の両方のアドレスを使用できます。

次の例は、VPC 内の Transit Gateway とアプライアンスの間の Connect アタッチメントを示しています。



図のコンポーネント	説明
	VPC アタッチメント
	Connect アタッチメント
	GRE トンネル (Connect ピア)
	BGP ピアリングセッション

前の例では、既存の VPC アタッチメント (トランスポートアタッチメント) に Connect アタッチメントが作成されます。Connect ピアが Connect アタッチメントに作成され、VPC 内のアプライアンスへの接続を確立します。トランジットゲートウェイアドレスは 192.0.2.1 で、BGP アドレスの範囲は 169.254.6.0/29 です。範囲 (169.254.6.1) 内の最初の IP アドレスは、ピア BGP IP アドレスとしてアプライアンス上で設定されます。

VPC C のサブネットルートテーブルには、トランジットゲートウェイ CIDR ブロックを送信先とするトラフィックをトランジットゲートウェイにポイントするルートがあります。

送信先	ターゲット
172.31.0.0/16	ローカル
192.0.2.0/24	tgw-id

要件と考慮事項

Connect アタッチメントの要件と考慮事項は次のとおりです。

- Connect アタッチメントをサポートするリージョンについては、「AWS Transit Gateway よくある質問」を参照してください。
- サードパーティーアプライアンスは、接続 アタッチメントを使用して、GRE トンネルを介してトランジットゲートウェイとの間でトラフィックを送受信するように設定される必要があります。
- 動的ルートアップデートおよび正常性チェックに BGP を使用するようにサードパーティーアプライアンスを設定する必要があります。
- 次のタイプの BGP がサポートされています。
  - エクステリア BGP (eBGP): トランジットゲートウェイとは異なる自律システムにあるルーターへの接続に使用されます。eBGP を使用する場合は、存続可能時間 (TTL) 値 2 で ebgp-multihop を設定する必要があります。
  - インテリア BGP (iBGP): トランジットゲートウェイと同じ自律システムにあるルーターへの接続に使用されます。トランジットゲートウェイは、ルートが eBGP ピアを起点とし、next-hop-self が設定されている必要がある場合を除き、iBGP ピア (サードパーティーアプライアンス) からのルートをインストールしません。iBGP ピアリングを介してサードパーティーアプライアンスによってアドバタイズされるルートには、ASN が必要です。
  - MP-BGP (BGP 用のマルチプロトコル拡張): IPv4 および IPv6 アドレスファミリーなど、複数のプロトコルタイプをサポートするために使用されます。

- デフォルトの BGP キープアライブタイムアウトは 10 秒で、デフォルトのホールドタイマーは 30 秒です。
- IPv6 BGP ピアリングはサポートされていません。IPv4 ベースの BGP ピアリングのみがサポートされます。IPv6 プレフィクスは、MP-BGP を使用して IPv4 BGP ピアリングを介して交換されます。
- 双方向フォワーディング検出 (BFD) はサポートされていません。
- BGP グレースフルリスタートはサポートされていません。
- トランジットゲートウェイピアを作成するときに、ピア ASN 番号を指定しない場合、トランジットゲートウェイ ASN 番号が選択されます。つまり、アプライアンスとトランジットゲートウェイは、iBGP を実行する同じ自律システム内に存在することになります。
- Connect ピアが 2 つある場合は、BGP AS-PATH 属性を使用する Connect ピアが優先ルートになります。

  複数のアプライアンス間で 等コストマルチパス (ECMP) ルーティングを使用するには、同じ BGP AS-PATH 属性を使用してトランジットゲートウェイに同じプレフィクスをアドバタイズするように、アプライアンスを設定する必要があります。トランジットゲートウェイが使用可能なすべての ECMP パスを選択するには、AS-PATH と自律システム番号 (ASN) が一致している必要があります。トランジットゲートウェイは、同じ Connect アタッチメントの Connect ピア間、または同じトランジットゲートウェイ上の Connect アタッチメント間で ECMP を使用できます。Transit Gateway では、1 つのピアが確立する両方の冗長 BGP ピア接続間で ECMP を使用できません。
- Connect アタッチメントでは、ルートはデフォルトで Transit Gateway ルートテーブルに伝達されます。
- 静的ルートはサポートされていません。
- サードパーティーアプライアンス外部インターフェイス (トンネルソース) の最大送信単位 (MTU) が次のいずれかであることを確認してください。
  - GRE トンネルインターフェイスの MTU と一致する
  - GRE トンネルインターフェイスの MTU よりも大きい

Connect アタッチメントの作成

Connect アタッチメントを作成するには、トランスポートアタッチメントとして既存のアタッチメントを指定する必要があります。VPC アタッチメントまたは Direct Connect アタッチメントをトランスポートアタッチメントとして指定できます。

コンソールを使用して Connect アタッチメントを作成するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. [Transit Gateway アタッチメントの作成] を選択します。
4. (オプション) [名前タグ] でアタッチメントの名前タグを指定します。
5. [Transit Gateway ID] で、アタッチメントのトランジットゲートウェイを選択します。
6. [アタッチメントタイプ] で、[接続] を選択します。
7. [トランスポートアタッチメント ID] で、既存のアタッチメント の ID を選択します。
8. [Transit Gateway アタッチメントの作成] を選択します。

AWS CLI CLI を使用して Connect アタッチメントを作成するには

create-transit-gateway-connect コマンドを使用します。

Connect ピア (GRE トンネル) を作成する

既存の Connect アタッチメントについて、Connect ピア (GRE トンネル) を作成できます。開始する前に、トランジットゲートウェイ CIDR ブロックが設定されていることを確認してください。トランジットゲートウェイを作成または変更するときに、トランジットゲートウェイ CIDR ブロックを設定できます。

Connect ピアを作成するときは、Connect ピアのアプライアンス側で GRE 外部 IP アドレスを指定する必要があります。

コンソールを使用して Connect ピアを作成するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. Connect アタッチメントを選択し、[アクション] 、[Connect ピアを作成] の順に選択します。
4. (オプション) [名前タグ] に、Connect ピアの名前タグを指定します。
5. (オプション) [Transit Gateway GRE アドレス] に、Transit Gateway の GRE 外部 IP アドレスを指定します。デフォルトでは、トランジットゲートウェイ CIDR ブロックから最初に使用可能なアドレスが使用されます。
6. [ピア GRE アドレス] で、Connect ピアのアプライアンス側の GRE 外部 IP アドレスを指定します。

7. [BGP 内部 CIDR ブロック IPv4] で、BGP ピアリングに使用される内部 IPv4 アドレスの範囲を指定します。169.254.0.0/16 の範囲から /29 CIDR ブロックを指定します。
8. (オプション) [BGP 内部 CIDR ブロック IPv6] で、BGP ピアリングに使用される内部 IPv6 アドレスの範囲を指定します。fd00::/8 の範囲から /125 CIDR ブロックを指定します。
9. (オプション) [ピア ASN] で、アプライアンスのボーダーゲートウェイプロトコル (BGP) 自律システム番号 (ASN) を指定します。ネットワークに割り当てられている既存の ASN を使用できます。既存の ASN がない場合は、64512〜65534 (16ビットASN) または 4200000000〜4294967294 (32ビットASN) の範囲でプライベート ASN を使用できます。

   デフォルトは、トランジットゲートウェイと同じ ASN です。ピア ASN をトランジットゲートウェイ ASN (eBGP) とは異なるように設定する場合は、存続可能時間 (TTL) 値 2 で ebgp-multihop を設定する必要があります。
10. 選択接続ピアの作成を選択します。

AWS CLI を使用して Connect ピアを作成するには

create-transit-gateway-connect-保存 コマンドを使用します。

Connect アタッチメントと Connect ピアを表示する

Connect アタッチメントと Connect ピアを表示できます。

コンソールを使用して Connect アタッチメントと Connect ピアを表示するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. Connect アタッチメントを選択します。
4. アタッチメントの Connect ピアを表示するには、[Connect ピア] タブを選択します。

AWS CLI を使用して Connect アタッチメントと Connect ピアを表示するには

describe-transit-gateway-connects および describe-transit-gateway-connect-ピア コマンドを使用します。

Connect アタッチメントおよび Connect ピアのタグを変更する

Connect アタッチメントのタグを変更できます。

コンソールを使用して Connect アタッチメントタグを変更するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. 接続 アタッチメントを選択後、[アクション]、[タグの管理] の順に選択します。
4. タグを追加するには、新しいタグを追加を選択し、キー名とキーバリューを指定します。
5. タグを削除するには、[削除] を選択します。
6. [保存] を選択します。

Connect ピアのタグは変更できます。

コンソールを使用して Connect ピアのタグを変更するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. 接続 アタッチメントを選択し、[接続 ピア] を選択します。
4. Connect ピアを選択後、[アクション]、[タグの管理] の順に選択します。
5. タグを追加するには、新しいタグを追加を選択し、キー名とキーバリューを指定します。
6. タグを削除するには、[削除] を選択します。
7. [Save (保存)] を選択します。

AWS CLI を使用して Connect アタッチメントおよび Connect ピアのタグを変更するには

create-tags および delete-tags コマンドを使用します。

Connect ピアを削除する

Connect ピアが不要になった場合には、それを削除することができます。

コンソールを使用して Connect ピアを削除するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. Connect アタッチメントを選択します。
4. [Connect ピア] タブで、Connect ピアを選択し、[アクション]、[Connect ピアを削除] の順に選択します。

AWS CLI を使用して Connect ピアを削除するには

delete-transit-gateway-connect-保存 コマンドを使用します。

Connect アタッチメントを削除する

Connect アタッチメントが不要になった場合は、削除できます。まず、アタッチメントの Connect ピアをすべて削除する必要があります。

コンソールを使用して Connect アタッチメントを削除するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway アタッチメント] を選択します。
3. Connect アタッチメントを選択後、[アクション]、[Transit Gateway アタッチメントの削除]を選択します。
4. 「**`delete`**」と入力し、[削除] を選択します。

AWS CLI CLI を使用して Connect アタッチメントを削除するには

delete-transit-gateway-connect コマンドを使用します。

Transit Gateway ルートテーブル

Transit Gateway ルートテーブルを使用して、Transit Gateway アタッチメントのルーティングを設定します。

Transit Gateway ルートテーブルの作成

コンソールを使用して Transit Gateway ルートテーブルを作成するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway ルートテーブル] を選択します。
3. [Transit Gateway ルートテーブルの作成] を選択します。
4. (オプション) [名前タグ] に、トランジットゲートウェイルートテーブルの名前を入力します。これにより、タグキー「名前」を持つタグが作成されます。タグ値は指定した名前です。
5. [Transit Gateway ID] で、ルートテーブルの Transit Gateway を選択します。
6. [Transit Gateway ルートテーブルの作成] を選択します。

を使用してトランジットゲートウェイルートテーブルを作成するには AWS CLI

create-transit-gateway-route-table コマンドを使用します。

Transit Gateway ルートテーブルの表示

コンソールを使用して Transit Gateway ルートテーブルを表示するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway ルートテーブル] を選択します。
3. (オプション) 特定のルートテーブルまたはテーブルのセットを検索するには、フィルターフィールドに名前、キーワード、または属性の全部または一部を入力します。
4. ルートテーブルのチェックボックスを選択するか、ID を選択して、関連付け、伝達、ルート、タグに関する情報を表示します。

を使用してトランジットゲートウェイのルートテーブルを表示するには AWS CLI

describe-transit-gateway-route-tables コマンドを使用してください。

を使用してトランジットゲートウェイのルートテーブルのルートを表示するには AWS CLI

search-transit-gateway-routesコマンドを実行します。

を使用してトランジットゲートウェイのルートテーブルのルート伝達を表示するには AWS CLI

get-transit-gateway-route-table-propagations コマンドを使用してください。

を使用してトランジットゲートウェイのルートテーブルの関連付けを表示するには AWS CLI

get-transit-gateway-route-table-associations コマンドを使用してください。

Transit Gateway ルートテーブルの関連付け

Transit Gateway ルートテーブルを、Transit Gateway アタッチメントに関連付けることができます。

コンソールを使用して Transit Gateway ルートテーブルを関連付けるには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway ルートテーブル] を選択します。

3. ルートテーブルを選択します。
4. ページ下部で、[Associations (関連付け)] タブを選択します。
5. [関連付けの作成] を選択します。
6. 関連付けるアタッチメントを選択してから、[Create association (関連付けの作成)] を選択します。

を使用してトランジットゲートウェイのルートテーブルを関連付けるには AWS CLI

associate-transit-gateway-route-table コマンドを使用します。

Transit Gateway ルートテーブルの関連付けの削除

Transit Gateway アタッチメントから Transit Gateway ルートテーブルの関連付けを解除できます。

コンソールを使用して Transit Gateway ルートテーブルの関連付けを解除するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway ルートテーブル] を選択します。
3. ルートテーブルを選択します。
4. ページ下部で、[Associations (関連付け)] タブを選択します。
5. 関連付けを解除するアタッチメントを選択してから、[Delete association (関連付けの解除)] を選択します。
6. 確認を求めるメッセージが表示されたら、[Delete association (関連付けの解除)] を選択します。

を使用してトランジットゲートウェイのルートテーブルの関連付けを解除するには AWS CLI

disassociate-transit-gateway-route-table コマンドを使用します。

Transit Gateway ルートテーブルへのルートの伝達

ルート伝達を使用して、アタッチメントからルートテーブルへのルートを追加します。

Transit Gateway アタッチメントルートテーブルにルートを伝達するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway ルートテーブル] を選択します。
3. 伝播を作成するルートテーブルを選択します。

4. [Actions (アクション)]、[Create propagation (伝播の作成)] の順に選択します。
5. [Create propagation (伝播の作成)]ページで、アタッチメントを選択します。
6. 伝播の作成] を選択します。

を使用してルート伝播を有効にするには AWS CLI

enable-transit-gateway-route-table-propagation コマンドを使用してください。

ルート伝達の無効化

ルートテーブルアタッチメントからルート伝達を削除します。

コンソールを使用してルート伝達を無効にするには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway ルートテーブル] を選択します。
3. 伝播を削除するルートテーブルを選択します。
4. ページ下部で、[Propagations (伝播)] タブを選択します。
5. アタッチメントを選択し、次に[Delete propagation (伝播の削除)] を選択します。
6. 確認を求めるメッセージが表示されたら、[Delete propagation (伝播の削除)] を選択します。

を使用してルートプロパゲーションを無効にするには AWS CLI

disable-transit-gateway-route-table-propagation コマンドを使用してください。

静的ルートを作成する

VPC、VPN、または Transit Gateway ピアリングアタッチメントの静的ルートを作成するか、ルートに一致するトラフィックを切断するブラックホールルートを作成できます。

VPN アタッチメントをターゲットとする Transit Gateway ルートテーブル内の静的ルートは Site-to-Site VPN によってフィルターされません。これにより、BGP ベースの VPN を使用すると意図しないアウトバウンドトラフィックフローが発生する可能性があります。

コンソールを使用して静的ルートを作成するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。

2. ナビゲーションペインで [Transit Gateway ルートテーブル] を選択します。
3. ルートを作成するルートテーブルを選択します。
4. [アクション]、[静的ルートの作成] の順に選択します。
5. [ルートの作成] ページに、ルートを作成する CIDR ブロックを入力し、[アクティブ] を選択します。
6. ルートのアタッチメントを選択します。
7. [静的ルートの作成] を選択します。

コンソールを使用してブラックホールルートを作成するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway ルートテーブル] を選択します。
3. ルートを作成するルートテーブルを選択します。
4. [アクション]、[静的ルートの作成] の順に選択します。
5. [静的ルートの作成] ページに、ルートを作成する CIDR ブロックを入力し、[ブラックホール] を選択します。
6. [静的ルートの作成] を選択します。

を使用してスタティックルートまたはブラックホールルートを作成するには AWS CLI

create-transit-gateway-routeコマンドを実行します。

静的ルートを削除する

Transit Gateway ルートテーブルから静的ルートを削除できます。

コンソールを使用して静的ルートを削除するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway ルートテーブル] を選択します。
3. ルートを削除するルートテーブルを選択し、[ルート] を選択します。
4. 削除するルートを選択します。
5. 選択静的ルートを削除する。
6. 確認ボックスで [静的ルートの削除] を選択します。

を使用してスタティックルートを削除するには AWS CLI

delete-transit-gateway-routeコマンドを実行します。

スタティックルートの置換

トランジットゲートウェイルートテーブル内のスタティックルートを別のスタティックルートに置き換えることができます。

コンソールを使用してスタティックルートを置き換えるには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway ルートテーブル] を選択します。
3. ルートテーブルで置換するルートを選択します。
4. 詳細セクションで、[ルート] タブを選択します。
5. [アクション]、[スタティックルートの置換] を選択します。
6. [タイプ] では、[アクティブ] または [ブラックホール] を選択します。
7. [アタッチメントの選択] ドロップダウンから、ルートテーブル内の現在のゲートウェイを置き換えるトランジットゲートウェイを選択します。
8. [スタティックルートの置換] を選択します。

を使用してスタティックルートを置き換えるには AWS CLI

replace-transit-gateway-routeコマンドを実行します。

Amazon S3 にルートテーブルをエクスポートする

Transit Gateway のルートテーブルのルートを Amazon S3 バケットにエクスポートできます。ルートは、JSON ファイルの指定された Amazon S3 バケットに保存されます。

コンソールを使用して Transit Gateway ルートテーブルをエクスポートするには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway ルートテーブル] を選択します。
3. エクスポートするルートを含むルートテーブルを選択します。
4. [Actions (アクション)]、[Export routes (ルートのエクスポート)] を選択します。

5. [Export routes (ルートのエクスポート)] ページの [S3 bucket name (S3バケット名)]に、S3 バケットの名前を入力します。
6. エクスポートされたルートをフィルタリングするには、ページの [フィルター] セクションでフィルターパラメータを指定します。
7. [Export routes (ルートのエクスポート)] を選択します。

エクスポートされたルートにアクセスするには、https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開き、指定したバケットに移動します。ファイル名には AWS アカウント ID、 AWS リージョン、ルートテーブル ID、タイムスタンプが含まれます。ファイルを選択し、[ダウンロード] を選択します。VPC アタッチメントの 2 つの伝達ルートに関する情報を含む JSON ファイルの例を次に示します。

```
{
  "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"
      }
    ]
}
```

Transit Gateway ルートテーブルの削除

コンソールを使用して Transit Gateway ルートテーブルを削除するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway ルートテーブル] を選択します。
3. 削除するルートテーブルを選択します。
4. アクション、Transit Gateway ルートテーブルの削除を選択します。
5. **delete** と入力して、[Delete (削除)] を選択して削除を確認します。

を使用してトランジットゲートウェイのルートテーブルを削除するには AWS CLI

delete-transit-gateway-route-table コマンドを使用します。

プレフィックスリストリファレンス

トランジットゲートウェイルートテーブルでプレフィックスリストを参照できます。プレフィックスリストは、定義および管理する 1 つ以上の CIDR ブロックエントリのセットです。プレフィックスリストを使用すると、ネットワークトラフィックをルーティングするためにリソースで参照する IP アドレスの管理を簡素化できます。例えば、複数の Transit Gateway ルートテーブルにわたって同じ送信先 CIDR を頻繁に指定する場合、各ルートテーブルで同じ CIDR を繰り返し参照するのではなく、これらの CIDR を 1 つのプレフィックスリストで管理できます。送信先 CIDR ブロックを削除する必要がある場合は、影響を受けるすべてのルートテーブルからルートを削除する代わりに、プレフィックスリストからエントリを削除できます。

Transit Gateway ルートテーブルにプレフィックスリストリファレンスを作成すると、プレフィックスリストの各エントリは、Transit Gateway ルートテーブルにルートとして表示されます。

プレフィックスリストの詳細については、Amazon VPC ユーザーガイドの「プレフィックスリスト」を参照してください。

プレフィックスリストリファレンスの作成

Transit Gateway ルートテーブルにプレフィックスリストへの参照を作成できます。

コンソールを使用してプレフィックスリストリファレンスを作成するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway ルートテーブル}] をクリックします。
3. Transit Gateway ルートテーブルを選択します。
4. [アクション]、[プレフィックスリスト参照を作成] の順にクリックします。
5. [プレフィックスリスト ID] で、プレフィックスリストの ID を選択します。
6. を使用する場合タイプで、このプレフィクスリストへのトラフィックを許可するかどうかを選択します (アクティブ) またはドロップ (ブラックホール)。
7. [Transit Gateway アタッチメント ID] で、トラフィックをルーティングする先のアタッチメントの ID を選択します。
8. [プレフィックスリスト参照を作成] をクリックします。

AWS CLI を使用してプレフィックスリストリファレンスを作成するには

[create-transit-gateway-prefix-list-reference] コマンドを使用します。

プレフィックスリストリファレンスの表示

Transit Gateway ルートテーブルにプレフィックスリストリファレンスを表示できます。プレフィックスリストの各エントリを、Transit Gateway ルートテーブルに個別のルートとして表示することもできます。プレフィックスリストルートのルートタイプは `propagated` です。

コンソールを使用してプレフィックスリストリファレンスを表示するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway ルートテーブル}] をクリックします。
3. Transit Gateway ルートテーブルを選択します。
4. 下部のペインで、[プレフィックスリストリファレンス] をクリックします。プレフィックスリストリファレンスが一覧表示されます。
5. [ルート] をクリックします。プレフィックスリストの各エントリが、ルートテーブルにルートとして表示されます。

AWS CLI CLI を使用してプレフィックスリストリファレンスを表示するには

[get-transit-gateway-prefix-list-references] コマンドを使用します。

プレフィックスリストリファレンスの変更

プレフィックスリストリファレンスを変更するには、トラフィックのルーティング先のアタッチメントを変更します。または、ルートに一致するトラフィックを削除するかどうかを指定します。

プレフィックスリストの各ルートを [ルート] タブで変更することはできません。プレフィックスリストのエントリを変更するには、[マネージドプレフィックスリスト] 画面を使用します。詳細については、Amazon VPC ユーザーガイドの「プレフィックスリストの変更」を参照してください。

コンソールを使用してプレフィックスリストリファレンスを変更するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway ルートテーブル}] をクリックします。
3. Transit Gateway ルートテーブルを選択します。
4. 下部のペインで、[プレフィックスリストリファレンス] をクリックします。
5. プレフィックスリストリファレンスを選択し、[リファレンスの変更] をクリックします。
6. を使用する場合タイプで、このプレフィクスリストへのトラフィックを許可するかどうかを選択します (アクティブ) またはドロップ (ブラックホール)。
7. [Transit Gateway アタッチメント ID] で、トラフィックをルーティングする先のアタッチメントの ID を選択します。
8. [プレフィックスリスト参照の変更] をクリックします。

AWS CLI を使用してプレフィックスリストリファレンスを変更するには

[modify-transit-gateway-prefix-list-reference] コマンドを使用します。

プレフィックスリストリファレンスの削除

プレフィックスリストリファレンスが不要になった場合は、Transit Gateway ルートテーブルから削除できます。参照を削除しても、プレフィックスリストは削除されません。

コンソールを使用してプレフィックスリストリファレンスを削除するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway ルートテーブル}] をクリックします。

3. Transit Gateway ルートテーブルを選択します。
4. プレフィックスリストリファレンスを選択し、[リファレンスの削除] をクリックします。
5. [リファレンスの削除] を選択します。

AWS CLI を使用してプレフィックスリストリファレンスを削除するには

[delete-transit-gateway-prefix-list-reference] コマンドを使用します。

Transit Gateway ポリシーテーブル

Transit Gateway の動的ルーティングでは、ポリシーテーブルを使用してネットワークトラフィックが AWS Cloud WAN にルーティングされます。このテーブルには、ポリシー属性によってネットワークトラフィックを照合するためのポリシールールが含まれ、ルールに一致するトラフィックがターゲットルートテーブルにマッピングされます。

Transit Gateway に動的ルーティングを使用して、ルーティングおよび到達可能性の情報をピアリングされた Transit Gateway と自動的に情報交換できます。静的ルートとは異なり、パスの障害や輻輳などのネットワーク状態に基づいて、別のパスを経由してトラフィックをルーティングできます。また、動的ルーティングは、ネットワークの侵害や侵入が発生した場合にトラフィックを簡単に再ルーティングできるという点で、セキュリティの強化につながります。

> **Note**
>
> トランジットゲートウェイポリシーテーブルは現在、トランジットゲートウェイピア接続を作成するときに、Cloud WAN でのみサポートされています ピアリング接続を作成するときに、そのテーブルを接続に関連付けることができます。その後、アソシエーションはポリシールールを自動的にテーブルに入力します。
> Cloud WAN でのピアリング接続の詳細については、「AWS Cloud WAN ユーザーガイド」の「 Peerings」を参照してください。

Transit Gateway ポリシーテーブルの作成

コンソールを使用して Transit Gateway ポリシーテーブルを作成するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit gateway policy table] (Transit Gateway ポリシーテーブル) を選択します。

3. [Create transit gateway policy table] (Transit Gateway ポリシーテーブルの作成) を選択します。
4. (オプション) [Name tag] (名前タグ) に、Transit Gateway ポリシーテーブルの名前を入力します。これによりタグが作成され、タグの値は指定した名前になります。
5. [Transit gateway ID] (Transit Gateway の ID) で、ポリシーテーブルの Transit Gateway を選択します。
6. [Create transit gateway policy table] (Transit Gateway ポリシーテーブルの作成) を選択します。

を使用してトランジットゲートウェイポリシーテーブルを作成するには AWS CLI

create-transit-gateway-policy-table コマンドを使用します。

Transit Gateway ポリシーテーブルの削除

Transit Gateway ポリシーテーブルを削除します。テーブルが削除されると、そのテーブル内のすべてのポリシールールが削除されます。

コンソールを使用して Transit Gateway ポリシーテーブルを削除するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit gateway policy tables] (Transit Gateway ポリシーテーブル) を選択します。
3. 削除する Transit Gateway ポリシーテーブルを選択します。
4. [Actions] (アクション) を選択してから、[Delete policy table] (ポリシーテーブルの削除) を選択します。
5. テーブルを削除することを確認します。

を使用してトランジットゲートウェイポリシーテーブルを削除するには AWS CLI

delete-transit-gateway-policy-table コマンドを使用します。

Transit Gateway でのマルチキャスト

マルチキャストは、単一のデータストリームを複数の受信コンピュータに同時に配信するために使用される通信プロトコルです。Transit Gateway は、接続された VPC のサブネット間のマルチキャストトラフィックのルーティングをサポートし、複数の受信インスタンス宛てのトラフィックを送信するインスタンスのマルチキャストルーターとして機能します。

マルチキャストの概念

マルチキャストの主な概念は次のとおりです。

- マルチキャストドメイン — 異なるドメインへのマルチキャストネットワークのセグメント化が可能になり、Transit Gateway が複数のマルチキャストルーターとして機能するようになります。サブネットレベルでマルチキャストドメインのメンバーシップを定義します。
- マルチキャストグループ — 同じマルチキャストトラフィックを送受信するホストセットを識別します。マルチキャストグループは、グループ IP アドレスによって識別されます。マルチキャストグループのメンバーシップは、EC2 インスタンスにアタッチされた個々の 弾性ネットワークインタフェース によって定義されます。
- インターネットグループ管理プロトコル (IGMP) — ホストとルーターがマルチキャストグループメンバーシップを動的に管理できるようにするインターネットプロトコル。IGMP マルチキャストドメインには、IGMP プロトコルを使用してメッセージを結合、終了、送信するホストが含まれています。 は IGMPv2 プロトコルと IGMP および静的 (API ベース) グループメンバーシップマルチキャストドメインの両方 AWS をサポートします。

- マルチキャスト送信元 — マルチキャストトラフィックを送信するよう静的に設定された、サポートされている EC2 インスタンスに関連付けられた elastic network interface。マルチキャスト送信元は、静的な送信元の設定のみに適用されます。

  静的な送信元のマルチキャストドメインには、メッセージの参加、脱退、および送信を行うために IGMP プロトコルを使用しないホストが含まれます。を使用して AWS CLI 、ソースメンバーとグループメンバーを追加します。静的に追加された送信元は、マルチキャストトラフィックを送信し、メンバーはマルチキャストトラフィックを受信します。
- マルチキャストグループメンバー — マルチキャストトラフィックを受信する、サポートされている EC2 インスタンスに関連付けられた elastic network interface。マルチキャストグループには複数のグループメンバーがあります。静的な送信元のグループメンバーシップの設定では、マルチキャストグループメンバーはトラフィックだけを受信できます。IGMP グループ設定では、メンバーはトラフィックを送受信できます。

考慮事項

- サポートされるリージョンについては、 AWS Transit Gateway よくある質問を参照してください。
- マルチキャストをサポートするには、新しいTransit Gateway を作成する必要があります。

- マルチキャストグループのメンバーシップは、、 AWS CLI、または IGMP を使用して管理 Amazon Virtual Private Cloud Console されます。
- マルチキャストドメインに存在するサブネットは 1 つだけです。
- Nitro 以外のインスタンスを使用する場合は、[送信元/送信先チェック] を無効にする必要があります。チェックを無効にする方法については、「Amazon EC2 ユーザーガイド」の「送信元または送信先のチェックの変更」を参照してください。 Amazon EC2
- ニトロ以外のインスタンスをマルチキャスト送信元にすることはできません。
- マルチキャストルーティングは、 AWS Direct Connect、Site-to-Site VPN、ピアリングアタッチメント、または Transit Gateway Connect アタッチメントではサポートされていません。
- Transit Gateway は、マルチキャストパケットのフラグメント化をサポートしていません。フラグメント化されたマルチキャストパケットはドロップされます。詳細については、「最大送信単位 (MTU)」を参照してください。
- 起動時に、IGMP ホストは複数の IGMP JOIN メッセージを送信してマルチキャストグループに参加します (通常は 2 ~ 3 回の再試行)。万一、すべての IGMP JOIN メッセージが失われた場合、ホストはトランジットゲートウェイマルチキャストグループの一部になりません。このようなシナリオでは、アプリケーション固有の方法を使用して、ホストから IGMP JOIN メッセージを再トリガーする必要があります。
- グループメンバーシップは Transit Gateway からの IGMPv2 JOIN メッセージの受信から始まり、IGMPv2 LEAVE メッセージ の受信で終わります。Transit Gateway は、グループに正常に参加したホストを追跡します。クラウドマルチキャストルーターとして、Transit Gateway は 2 分ごとにメンバー全員に IGMPv2 QUERY メッセージを発行します。各メンバーは 応答中に IGMPv2 JOIN メッセージを送信します。これはメンバーがメンバーシップを更新する方法です。メンバーが 3 つの連続するクエリに応答できない場合、Transit Gateway は、参加したすべてのグループからこのメンバーシップを削除します。ただし、メンバーを to-be-queried リストから完全に削除するまで、12 時間このメンバーにクエリを送信し続けます。明示的な igMPv2 LEAVE メッセージは、それ以降のマルチキャスト処理からホストを即座かつ永続的に削除します。
- Transit Gateway は、グループに正常に参加したホストを追跡します。Transit Gateway が停止した場合、Transit Gateway は、IGMP JOIN メッセージが最後に正常に終了してから 7 分 (420 秒) 間、マルチキャストデータをホストに送信し続けます。Transit Gateway は、最長 12 時間、またはホストから IGMP LEAVE メッセージを受信するまで、メンバーシップクエリをホストに送信し続けます。
- Transit Gateway は、マルチキャストグループメンバーシップを追跡できるように、メンバーシップクエリパケットをすべての IGMP メンバーに送信します。これらの IGMP クエリパケットの送信元 IP は 0.0.0.0/32、送信先 IP は 224.0.0.1/32、プロトコルは 2 です。IGMP ホスト (インスタ

ンス) 上のセキュリティグループ設定、およびホストサブネット上の任意の ACL 設定で、これらの IGMP プロトコルメッセージを許可する必要があります。

- マルチキャストの送信元と送信先が同じ VPC 内にある場合、セキュリティグループ参照を使用して、送信元のセキュリティグループからのトラフィックを受け入れるように送信先セキュリティグループを設定することはできません。
- 静的なマルチキャストグループとソースの場合、Amazon VPC Transit Gateways は、もう存在しない ENI の静的グループとソースを自動的に削除します。これは、アカウント内の ENI を説明する Transit Gateway サービスにリンクされた役割を定期的に引き受けることによって行われます。
- 静的マルチキャストのみが IPv6 をサポートします。動的マルチキャストはそうではありません。

Windows Server でマルチキャストする

Windows Server 2019 または 2022 上の Transit Gateway と連携するようにマルチキャストを設定する場合は、追加の手順を実行する必要があります。を使用して PowerShell、次のコマンドを実行します。

1. TCP/IP スタックに IGMPv3 ではなく IGMPv2 を使用するように Windows サーバーを変更します。

   ```
   PS C:\> New-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services
   \Tcpip\Parameters -Name IGMPVersion -PropertyType DWord -Value 3
   ```

   > **Note**
   >
   > `New-ItemProperty` は、IGMP バージョンを指定するプロパティインデックスです。IGMP v2 はマルチキャストでサポートされているバージョンであるため、 プロパティは `Value`である必要があります3。Windows レジストリを編集する代わりに、次のコマンドを実行して IGMP バージョンを 2 に設定できます。
   > `Set-NetIPv4Protocol -IGMPVersion Version2`

2. Windows ファイアウォールでは、ほとんどの UDP トラフィックがデフォルトでドロップされます。まず、どの接続プロファイルがマルチキャストに使用されているかを確認する必要があります。

   ```
   PS C:\> Get-NetConnectionProfile | Select-Object NetworkCategory

   NetworkCategory
   ```

```
---------------
         Public
```

3. 前のステップで確認した接続プロファイルを更新して、必要な UDP ポートへのアクセスを許可します。

```
PS C:\> Set-NetFirewallProfile -Profile Public -Enabled False
```

4. EC2 インスタンスを再起動します。
5. マルチキャストアプリケーションをテストして、トラフィックのフローが予期したとおりのものであることを確認します。

マルチキャストのルーティング

トランジットゲートウェイは、マルチキャストを有効にすると、マルチキャストルーターとして動作します。サブネットをマルチキャストドメインに追加すると、そのマルチキャストドメインに関連付けられたトランジットゲートウェイにすべてのマルチキャストトラフィックが送信されます。

ネットワーク ACL

ネットワーク ACL ルールは、サブネットレベルで動作します。トランジットゲートウェイはサブネットの外部に存在するため、マルチキャストトラフィックに適用されます。詳細については、Amazon VPC ユーザーガイドの「ネットワーク ACL」を参照してください。

IGMP マルチキャストトラフィックの場合、最小インバウンドルールは次のとおりです。リモートホストは、マルチキャストトラフィックを送信するホストです。

タイプ	プロトコル	送信元	説明
カスタムプロトコル	IGMP(2)	0.0.0.0/32	IGMP クエリ
カスタム UDP プロトコル	UDP	リモートホストの IP アドレス	着信マルチキャストトラフィック

IGMP の最小アウトバウンドルールは次のとおりです。

タイプ	プロトコル	送信先	説明
カスタムプロトコル	IGMP(2)	224.0.0.2/32	IGMP 脱退

タイプ	プロトコル	送信先	説明
カスタムプロトコル	IGMP(2)	マルチキャストグループの IP アドレス	IGMP 参加
カスタム UDP プロトコル	UDP	マルチキャストグループの IP アドレス	アウトバウンドマルチキャストトラフィック

セキュリティグループ

セキュリティグループルールは、インスタンスレベルで動作します。これらのトラフィックは、インバウンドマルチキャストトラフィックとアウトバウンドマルチキャストトラフィックの両方に適用できます。動作は、ユニキャストトラフィックと同じです。すべてのグループメンバーインスタンスで、グループソースからのインバウンドトラフィックを許可する必要があります。詳細については、Amazon VPC ユーザーガイドの「セキュリティグループ」を参照してください。

IGMP マルチキャストトラフィックの場合は、少なくとも次のインバウンドルールが必要です。リモートホストは、マルチキャストトラフィックを送信するホストです。UDP インバウンドルールのソースとしてセキュリティグループを指定することはできません。

タイプ	プロトコル	送信元	説明
カスタムプロトコル	2	0.0.0.0/32	IGMP クエリ
カスタム UDP プロトコル	UDP	リモートホストの IP アドレス	着信マルチキャストトラフィック

IGMP マルチキャストトラフィックの場合は、少なくとも次のアウトバウンドルールが必要です。

タイプ	プロトコル	送信先	説明
カスタムプロトコル	2	224.0.0.2/32	IGMP 脱退
カスタムプロトコル	2	マルチキャストグループの IP アドレス	IGMP 参加

タイプ	プロトコル	送信先	説明
カスタム UDP プロトコル	UDP	マルチキャストグループの IP アドレス	アウトバウンドマルチキャストトラフィック

マルチキャストの操作

Amazon VPC コンソールまたは AWS CLI を使用して、トランジットゲートウェイでマルチキャストを設定できます。

マルチキャストドメインを作成する前に、ホストがマルチキャストトラフィックにインターネットグループ管理プロトコル (IGMP) プロトコルを使用しているかどうかを確認する必要があります。

コンテンツ

マルチキャストドメイン属性

次の表は、マルチキャストドメイン属性の詳細を示しています。両方の属性を同時に有効にすることはできません。

属性	説明
`Igmpv2Support` (AWS CLI) IGMPv2 のサポート(コンソール)	この属性は、グループメンバーがマルチキャストグループの参加または脱退を行う方法を決定します。 この属性が無効の場合は、ドメインにグループメンバーを手動で追加する必要があります。

属性	説明
	少なくとも 1 つのメンバーが IGMP プロトコルを使用する場合、この属性を [有効] にします。メンバーは、次のいずれかの方法でマルチキャストグループに参加します。 • IGMP をサポートするメンバーは、JOIN および LEAVE メッセージを使用します。 • IGMP をサポートしないメンバーは、Amazon VPC コンソールまたは AWS CLI を使用してグループに追加または削除される必要があります。 マルチキャストグループメンバーを登録する場合は、登録を解除する必要があります。トランジットゲートウェイは、手動で追加されたグループメンバーによって送信された IGMP LEAVE メッセージを無視します。
StaticSourcesSupport (AWS CLI) 静的ソースサポート(コンソール)	この属性は、グループに静的なマルチキャスト送信元があるかどうかを決定します。 この属性が有効になっている場合は、register-transit-gateway-multicast-group-sources を使用してマルチキャストドメインのソースを追加する必要があります。マルチキャストトラフィックを送信できるのは、マルチキャスト送信元のみです。 この属性を無効にした場合、指定されたマルチキャスト送信元はありません。マルチキャストドメインに関連付けられたサブネットにあるインスタンスはすべて、マルチキャストトラフィックを送信でき、グループメンバーはマルチキャストトラフィックを受信します。

IGMP 設定を管理する

マルチキャストトラフィックに IGMP プロトコルを使用するホストが少なくとも 1 つある場合、AWS はインスタンスから IGMP JOIN メッセージを受信したときにマルチキャストグループを自動的に作成し、そのインスタンスをこのグループのメンバーとして追加します。を使用して、非 IGMP ホストをメンバーとしてグループに静的に追加することもできます AWS CLI。マルチキャストドメ

インに関連付けられたサブネットにあるインスタンスはすべて、トラフィックを送信でき、グループメンバーはマルチキャストトラフィックを受信します。

設定を完了するには、次の手順を実行します。

1. VPC を作成します。VPC の作成の詳細については、Amazon VPC ユーザーガイドの「VPC を作成する」を参照してください。
2. VPC 内にサブネットを作成します。サブネットの作成の詳細については、Amazon VPC ユーザーガイドの「VPC でサブネットを作成する」を参照してください。
3. マルチキャストトラフィック用に設定されたトランジットゲートウェイを作成します。詳細については、「the section called “Transit Gateway を作成する”」を参照してください。
4. VPC アタッチメントを作成します。詳細については、「the section called “VPC への Transit Gateway アタッチメントの作成”」を参照してください。
5. IGMP サポート用に設定されたマルチキャストドメインを作成します。詳細については、「the section called “IGMP マルチキャストドメインを作成する”」を参照してください。

   以下の設定を使用します。

   - IGMPv2 のサポートを有効にします。
   - 静的ソースサポートを無効にします。
6. トランジットゲートウェイ VPC アタッチメント内のサブネットとマルチキャストドメイン間の関連付けを作成します。詳細については、「the section called “VPC アタッチメントとサブネットをマルチキャストドメインに関連付ける”」を参照してください。
7. EC2 のデフォルトの IGMP バージョンは IGMPv3 です。すべての IGMP グループメンバーのバージョンを変更する必要があります。以下のコマンドを実行できます。

   ```
   sudo sysctl net.ipv4.conf.eth0.force_igmp_version=2
   ```
8. IGMP プロトコルを使用しないメンバーをマルチキャストグループに追加します。詳細については、「the section called “マルチキャストグループにメンバーを登録する”」を参照してください。

静的な送信元の設定を管理する

この設定では、マルチキャスト送信元をグループに静的に追加する必要があります。ホストは、マルチキャストグループの参加または脱退を行うために IGMP プロトコルを使用しません。マルチキャストトラフィックを受信するグループメンバーを静的に追加する必要があります。

設定を完了するには、次の手順を実行します。

1. VPC を作成します。VPC の作成の詳細については、Amazon VPC ユーザーガイドの「VPC を作成する」を参照してください。
2. VPC 内にサブネットを作成します。サブネットの作成の詳細については、Amazon VPC ユーザーガイドの「VPC でサブネットを作成する」を参照してください。
3. マルチキャストトラフィック用に設定されたトランジットゲートウェイを作成します。詳細については、「the section called “Transit Gateway を作成する”」を参照してください。
4. VPC アタッチメントを作成します。詳細については、「the section called “VPC への Transit Gateway アタッチメントの作成”」を参照してください。
5. IGMP サポートなしでマルチキャストドメインを作成し、送信元の静的な追加をサポートします。詳細については、「the section called “静的な送信元のマルチキャストドメインを作成する”」を参照してください。

   以下の設定を使用します。

   - IGMPv2 のサポートを無効にします。
   - 手動で送信元を追加するには、[Static sources support] (静的な送信元のサポート) を有効にします。

     属性が有効になっている場合、マルチキャストトラフィックを送信できる唯一のリソースは送信元です。その他の場合は、マルチキャストドメインに関連付けられたサブネットにあるインスタンスはすべて、マルチキャストトラフィックを送信でき、グループメンバーはマルチキャストトラフィックを受信します。
6. トランジットゲートウェイ VPC アタッチメント内のサブネットとマルチキャストドメイン間の関連付けを作成します。詳細については、「the section called “VPC アタッチメントとサブネットをマルチキャストドメインに関連付ける” 」を参照してください。
7. [Static sources support] (静的な送信元のサポート) を有効にした場合は、送信元をマルチキャストグループに追加します。詳細については、「the section called “マルチキャストグループにソースを登録する”」を参照してください。
8. メンバーをマルチキャストグループに追加します。詳細については、「the section called “マルチキャストグループにメンバーを登録する”」を参照してください。

静的なグループメンバーの設定を管理する

この設定では、マルチキャストメンバーをグループに静的に追加する必要があります。ホストは、マルチキャストグループの参加または脱退を行うために IGMP プロトコルを使用できません。マルチキャストドメインに関連付けられたサブネットにあるインスタンスはすべて、マルチキャストトラフィックを送信でき、グループメンバーはマルチキャストトラフィックを受信します。

設定を完了するには、次の手順を実行します。

1. VPC を作成します。VPC の作成の詳細については、Amazon VPC ユーザーガイドの「VPC を作成する」を参照してください。
2. VPC 内にサブネットを作成します。サブネットの作成の詳細については、Amazon VPC ユーザーガイドの「VPC でサブネットを作成する」を参照してください。
3. マルチキャストトラフィック用に設定されたトランジットゲートウェイを作成します。詳細については、「the section called “Transit Gateway を作成する”」を参照してください。
4. VPC アタッチメントを作成します。詳細については、「the section called “VPC への Transit Gateway アタッチメントの作成”」を参照してください。
5. IGMP サポートなしでマルチキャストドメインを作成し、送信元の静的な追加をサポートします。詳細については、「the section called “静的な送信元のマルチキャストドメインを作成する”」を参照してください。

   以下の設定を使用します。

   - IGMPv2 のサポートを無効にします。
   - 静的ソースサポートを無効にします。
6. トランジットゲートウェイ VPC アタッチメント内のサブネットとマルチキャストドメイン間の関連付けを作成します。詳細については、「the section called “VPC アタッチメントとサブネットをマルチキャストドメインに関連付ける”」を参照してください。
7. メンバーをマルチキャストグループに追加します。詳細については、「the section called “マルチキャストグループにメンバーを登録する”」を参照してください。

マルチキャストドメインを管理する

トランジットゲートウェイでマルチキャストの使用を開始するには、マルチキャストドメインを作成し、サブネットをドメインに関連付けます。

目次

- IGMP マルチキャストドメインを作成する
- 静的な送信元のマルチキャストドメインを作成する
- VPC アタッチメントとサブネットをマルチキャストドメインに関連付ける
- マルチキャストドメインの関連付けを表示する
- マルチキャストドメインからのサブネットの関連付けを解除する
- マルチキャストドメインにタグを追加する
- マルチキャストドメインを削除する

IGMP マルチキャストドメインを作成する

まだ確認していない場合は、使用可能なマルチキャストドメイン属性を確認します。詳細については、「the section called “マルチキャストの操作”」を参照してください。

Console

コンソールを使用して IGMP マルチキャストドメインを作成するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway マルチキャスト] を選択します。
3. [Transit Gateway マルチキャストドメインの作成] をクリックします。
4. [名前タグ] に、ドメインの名前を入力します。
5. [トランジットゲートウェイ ID] で、マルチキャストトラフィックを処理するトランジットゲートウェイを選択します。
6. [IGMPv2 support] (IGMPv2 サポート) で、チェックボックスをオンにします。
7. [Static sources support] (静的な送信元のサポート) で、チェックボックスをオフにします。
8. このマルチキャストドメインについてクロスアカウントサブネットの関連付けを自動的に受け入れるには、[Auto accept shared associations] (共有されている関連付けを自動的に受け入れる) を選択します。
9. [Transit Gateway マルチキャストドメインの作成] をクリックします。

Command line

を使用して IGMP マルチキャストドメインを作成するには AWS CLI

create-transit-gateway-multicast-domain コマンドを使用します。

```
aws ec2 create-transit-gateway-multicast-domain --transit-gateway-
id tgw-0xexampleid12345 --options StaticSourcesSupport=disable,Igmpv2Support=enable
```

静的な送信元のマルチキャストドメインを作成する

まだ確認していない場合は、使用可能なマルチキャストドメイン属性を確認します。詳細については、「the section called “マルチキャストの操作”」を参照してください。

Console

コンソールを使用して静的なマルチキャストドメインを作成するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway マルチキャスト] を選択します。
3. [Transit Gateway マルチキャストドメインの作成] をクリックします。
4. [Name tag] (名前タグ) に、ドメインを識別する名前を入力します。
5. [トランジットゲートウェイ ID] で、マルチキャストトラフィックを処理するトランジットゲートウェイを選択します。
6. [IGMPv2 support] (IGMPv2 サポート) で、チェックボックスをオフにします。
7. [Static sources support] (静的な送信元のサポート) で、チェックボックスをオンにします。
8. このマルチキャストドメインについてクロスアカウントサブネットの関連付けを自動的に受け入れるには、[Auto accept shared associations] (共有されている関連付けを自動的に受け入れる) を選択します。
9. [Transit Gateway マルチキャストドメインの作成] をクリックします。

Command line

を使用して静的マルチキャストドメインを作成するには AWS CLI

create-transit-gateway-multicast-domain コマンドを使用します。

```
aws ec2 create-transit-gateway-multicast-domain --transit-gateway-
id tgw-0xexampleid12345 --options StaticSourcesSupport=enable,Igmpv2Support=disable
```

VPC アタッチメントとサブネットをマルチキャストドメインに関連付ける

VPC アタッチメントをマルチキャストドメインに関連付けるには、以下の手順に従います。関連付けを作成するときに、マルチキャストドメインに含めるサブネットを選択できます。

開始する前に、トランジットゲートウェイで VPC アタッチメントを作成する必要があります。詳細については、「VPC への Transit Gateway アタッチメント」を参照してください。

Console

コンソールを使用して VPC アタッチメントをマルチキャストドメインに関連付けるには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway マルチキャスト] を選択します。
3. マルチキャストドメインを選択し、[Actions] (アクション)、[Create association] (関連付けの作成) の順に選択します。
4. 関連付ける添付ファイルを選択で、トランジットゲートウェイアタッチメントを選択します。
5. [Choose subnets to associate] (関連付けるサブネットを選択する) で、マルチキャストドメインに含めるサブネットを選択します。
6. [関連付けの作成] を選択します。

Command line

を使用して VPC アタッチメントをマルチキャストドメインに関連付けるには AWS CLI

associate-transit-gateway-multicast-domain コマンドを使用します。

マルチキャストドメインの関連付けを表示する

マルチキャストドメインを表示して、使用可能なこと、および適切なサブネットとアタッチメントが含まれていることを確認できます。

Console

コンソールを使用してマルチキャストドメインを表示するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。

2. ナビゲーションペインで [Transit Gateway マルチキャスト] を選択します。
3. マルチキャストドメインを選択します。
4. [Associations (関連付け)] タブを選択します。

Command line

を使用してマルチキャストドメインを表示するには AWS CLI

describe-transit-gateway-multicast-domains コマンドを使用します。

マルチキャストドメインからのサブネットの関連付けを解除する

サブネットとマルチキャストドメインの関連付けを解除するには、次の手順を実行します。

Console

コンソールを使用して、サブネットの関連付けを解除するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway マルチキャスト] を選択します。
3. マルチキャストドメインを選択します。
4. [Associations (関連付け)] タブを選択します。
5. サブネットに続いて、アクション、関連付けを削除の順に選択します。

Command line

を使用してサブネットの関連付けを解除するには AWS CLI

disassociate-transit-gateway-multicast-domain コマンドを使用します。

マルチキャストドメインにタグを追加する

目的、所有者、環境などに応じて、タグを整理して識別しやすくするために、リソースにタグを追加します。各マルチキャストドメインに複数のタグを追加できます。タグキーは、マルチキャストドメインごとに一意である必要があります。既にマルチキャストドメインに関連付けられているキーを持つタグを追加すると、そのキーの値が更新されます。詳細については、「Amazon EC2 リソースにタグを付ける」を参照してください。

Console

コンソールを使用してマルチキャストドメインにタグを追加するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway マルチキャスト] を選択します。
3. マルチキャストドメインを選択します。
4. [Actions] (アクション)、[Manage tags] (タグの管理) を選択します。
5. タグごとに、[Add new tag] (新しいタグの追加)を選択し、キーの名前と値を入力します。
6. [保存] を選択します。

Command line

を使用してマルチキャストドメインにタグを追加するには AWS CLI

create-tags コマンドを使用します。

マルチキャストドメインを削除する

マルチキャストドメインを削除するには、次の手順に従います。

Console

コンソールを使用してマルチキャストドメインを削除するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway マルチキャスト] を選択します。
3. マルチキャストドメインを選択し、[Actions] (アクション)、[Delete multicast domain] (マルチキャストドメインの削除) の順に選択します。
4. 確認を求められたら、**delete**と入力し、[削除] を選択します。

Command line

を使用してマルチキャストドメインを削除するには AWS CLI

delete-transit-gateway-multicast-domain コマンドを使用します。

マルチキャストグループを管理する

目次

マルチキャストグループにソースを登録する

> **Note**
>
> この手順は、[Static sources support] (静的な送信元のサポート) 属性を [enable] (有効) に設定している場合にのみ必要です。

次の手順に従って、ソースをマルチキャストグループに登録します。ソースは、マルチキャストトラフィックを送信するネットワークインターフェイスです。

ソースを追加する前に、次の情報が必要です。

- マルチキャストドメインの ID
- 送信元のネットワークインターフェイスの ID
- マルチキャストグループの IP アドレス

Console

コンソールを使用して、ソースを登録するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway マルチキャスト] を選択します。
3. マルチキャストドメインを選択し、[Actions] (アクション)、[Add group sources] (グループソースの追加) の順に選択します。
4. [Group IP address (グループ IP アドレス)] に、マルチキャストドメインに割り当てる IPv4 CIDR ブロックまたは IPv6 CIDR ブロックのいずれかを入力します。

5. [Choose network interfaces (ネットワークインターフェイスの選択)] で、マルチキャスト送信者のネットワークインターフェイスを選択します。
6. 「ソースを追加」 を選択します。

Command line

を使用してソースを登録するには AWS CLI

register-transit-gateway-multicast-group-sources コマンドを使用します。

マルチキャストグループにメンバーを登録する

グループメンバーをマルチキャストグループに登録するには、次の手順を実行します。

メンバーを追加する前に、次の情報が必要です。

- マルチキャストドメインの ID
- グループメンバーのネットワークインターフェイスの ID
- マルチキャストグループの IP アドレス

Console

コンソールを使用して、メンバーを登録するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway マルチキャスト] を選択します。
3. マルチキャストドメインを選択し、[Actions] (アクション)、[Add group members] (グループメンバーの追加) の順に選択します。
4. [Group IP address (グループ IP アドレス)] に、マルチキャストドメインに割り当てる IPv4 CIDR ブロックまたは IPv6 CIDR ブロックのいずれかを入力します。
5. [Choose network interfaces (ネットワークインターフェイスの選択)] で、マルチキャスト受信者のネットワークインターフェイスを選択します。
6. [Add members (メンバーの追加)] を選択します。

Command line

を使用してメンバーを登録するには AWS CLI

register-transit-gateway-multicast-group-members コマンドを使用します。

マルチキャストグループからソースを登録解除する

マルチキャストグループに手動で送信元を追加していない限り、この手順を実行する必要はありません。

Console

コンソールを使用して、ソースを削除するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway マルチキャスト] を選択します。
3. マルチキャストドメインを選択します。
4. [グループ] タブを選択します。
5. ソースを選択し、[Remove source (ソースを削除)] を選択します。

Command line

を使用してソースを削除するには AWS CLI

deregister-transit-gateway-multicast-group-sources コマンドを使用します。

マルチキャストグループからメンバーを登録解除する

マルチキャストグループに手動でメンバーを追加していない限り、この手順を実行する必要はありません。

Console

コンソールを使用して、メンバーの登録を解除するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway マルチキャスト] を選択します。
3. マルチキャストドメインを選択します。
4. [グループ] タブを選択します。
5. メンバーを選択し、[Remove member (メンバーの削除)] を選択します。

Command line

を使用してメンバーの登録を解除するには AWS CLI

deregister-transit-gateway-multicast-group-members コマンドを使用します。

マルチキャストグループを表示する

マルチキャストグループに関する情報を表示して、IGMPv2 プロトコルを使用してメンバーが検出されたことを確認できます。メンバータイプ (コンソールの場合) 、または MemberType (の場合 AWS CLI) は、 がプロトコルを持つメンバー AWS を検出したときに IGMP を表示します。

Console

コンソールを使用して、マルチキャストグループを表示するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Transit Gateway マルチキャスト] を選択します。
3. マルチキャストドメインを選択します。
4. [グループ] タブを選択します。

Command line

を使用してマルチキャストグループを表示するには AWS CLI

search-transit-gateway-multicast-groups コマンドを使用します。

次の例は、IGMP プロトコルがマルチキャストグループメンバーを検出したことを示しています。

```
aws ec2 search-transit-gateway-multicast-groups --transit-gateway-multicast-
domain tgw-mcast-domain-000fb24d04EXAMPLE
{
    "MulticastGroups": [
        {
            "GroupIpAddress": "224.0.1.0",
            "TransitGatewayAttachmentId": "tgw-attach-0372e72386EXAMPLE",
            "SubnetId": "subnet-0187aff814EXAMPLE",
            "ResourceId": "vpc-0065acced4EXAMPLE",
            "ResourceType": "vpc",
```

```
            "NetworkInterfaceId": "eni-03847706f6EXAMPLE",
            "MemberType": "igmp"
        }
    ]
}
```

共有マルチキャストドメインを使用する

マルチキャストドメイン共有を使用すると、マルチキャストドメイン所有者は、その組織内の AWS アカウント、または AWS Organizations 内の組織全体とドメインを共有できます。マルチキャストドメイン所有者は、マルチキャストドメインを一元的に作成および管理できます。コンシューマーは、共有マルチキャストドメインで次の操作を実行できます。

- マルチキャストドメイン内のグループメンバーまたはグループソースを登録および登録解除する
- サブネットをマルチキャストドメインに関連付けたり、サブネットとマルチキャストドメインとの関連付けを解除したりする

マルチキャストドメイン所有者は、マルチキャストドメインを次のユーザーと共有できます。

- 組織内 (または AWS Organizations 内の組織内) の AWS アカウント
- AWS Organizationsの組織内の組織単位
- AWS Organizations の組織全体
- AWS Organizations 外の AWS アカウント。

  マルチキャストドメインを組織外の AWS アカウントと共有するには、AWS Resource Access Manager を使用してリソース共有を作成し、マルチキャストドメインを共有するプリンシパルを選択するときに [すべてのユーザーとの共有を許可] を選択します。リソース共有の作成の詳細については、AWS RAM ユーザーガイドの「AWS RAM でのリソース共有の作成」を参照してください。

内容

- 共有マルチキャストドメインの共有を解除する
- 共有マルチキャストドメインを識別する
- 共有マルチキャストドメインのアクセス許可
- 請求と使用量測定
- クォータ

マルチキャストドメインを共有するための前提条件

- マルチキャストドメインを共有するには、それを AWS アカウント内で所有している必要があります。自身が共有を受けているマルチキャストドメインは共有できません。
- AWS Organizations の組織や組織単位とマルチキャストドメインを共有するには、AWS Organizations との共有を有効にする必要があります。詳細については、AWS RAM ユーザーガイドの「Enable Sharing with AWS Organizations」を参照してください。

関連する のサービス

マルチキャストドメイン共有は AWS Resource Access Manager (AWS RAM) と連携します。AWS RAM は、AWS リソースを任意の AWS アカウントと共有したり、AWS Organizations を介して共有したりするためのサービスです。AWS RAM を使用したリソース共有。これにより、自身が所有するリソースを共有できます。リソース共有は、共有するリソースと、それらを共有するコンシューマーを指定します。コンシューマーには、個々の AWS アカウントとする、あるいは AWS Organizations 内の組織単位または組織全体を指定できます。

AWS RAM の詳細については、AWS RAM ユーザーガイドを参照してください。

アベイラビリティーゾーン間での共有

リソースがリージョンの複数のアベイラビリティーゾーンに分散されるようにするために、アベイラビリティーゾーンは各 アカウントの名前に個別にマッピングされます。このため、アカウントが異なると、アベイラビリティーゾーンの命名方法が異なる場合があります。たとえば、us-east-1a アカウントのアベイラビリティーゾーン AWS の場所は、別の us-east-1a アカウントのアベイラビリティーゾーン AWS の場所と異なる可能性があります。

自己のアカウントを基準にしてマルチキャストドメインの場所を特定するには、アベイラビリティーゾーン ID (AZ ID) を使用する必要があります。AZ ID は、すべての AWS アカウントで同じアベイラビリティーゾーンを一貫して示すための一意の識別子です。例えば、use1-az1 は us-east-1 リージョンの AZ ID であり、すべての AWS アカウントで同じ場所を示します。

アカウントのアベイラビリティーゾーンの AZ ID を表示するには

1. AWS RAM コンソール (https://console.aws.amazon.com/ram) を開きます。
2. 現在のリージョンの AZ ID は、画面の右側にある [お客様の AZ ID] パネルに表示されます。

マルチキャストドメインを共有する

所有者がコンシューマーとマルチキャストドメインを共有する場合、コンシューマーは次のことを行うことができます。

- グループメンバーまたはグループソースを登録および登録解除する
- サブネットの関連付けおよび関連付けの解除を行う

マルチキャストドメインを共有するには、そのマルチキャストドメインをリソース共有に追加する必要があります。リソース共有とは、AWS RAM アカウント間で自身のリソースを共有するための AWS リソースです。リソース共有では、共有対象のリソースと、共有先のコンシューマーを指定します。Amazon Virtual Private Cloud Consoleを使用してマルチキャストドメインを共有する場合は、既存のリソース共有にそのマルチキャストドメインを追加します。マルチキャストドメインを新しいリソース共有に追加するには、最初にAWS RAMコンソールを使用してリソース共有を作成する必要があります。

AWS Organizations の組織に属している場合、組織内での共有が有効になっていると、組織内のコンシューマーには共有マルチキャストドメインへのアクセス許可が自動的に付与されます。それ以外の場合、コンシューマーはリソース共有への参加の招待を受け取り、その招待を受け入れた後で、共有マルチキャストドメインへのアクセス許可が付与されます。

*Amazon Virtual Private Cloud Console、AWS RAM コンソール、または AWS CLI を使用して、所有しているマルチキャストドメインを共有できます。

*Amazon Virtual Private Cloud Console を使用して所有しているマルチキャストドメインを共有するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Multicast Domains] (マルチキャストドメイン) を選択します。
3. マルチキャストドメインを選択し、[Actions] (アクション)、[Share multicast domain] (マルチキャストドメインの共有) の順に選択します。
4. リソース共有を選択してから、[Share multicast domain] (マルチキャストドメインの共有) を選択します。

AWS RAM コンソールを使用して所有しているマルチキャストドメインを共有するには

「AWS RAM ユーザーガイド 」の「リソース共有の作成」を参照してください。

AWS CLI を使用して所有しているマルチキャストドメインを共有するには

create-resource-share コマンドを使用します。

共有マルチキャストドメインの共有を解除する

共有マルチキャストドメインの共有が解除されると、コンシューマーマルチキャストドメインリソースについて次の事項が生じます。

- コンシューマーサブネットは、マルチキャストドメインとの関連付けが解除されます。サブネットは、コンシューマーアカウントに残ります。
- コンシューマーグループソースおよびグループメンバーは、マルチキャストドメインとの関連付けが解除され、コンシューマーアカウントから削除されます。

マルチキャストドメインの共有を解除するには、リソース共有からそのマルチキャストドメインを削除する必要があります。これは、AWS RAM コンソールまたは AWS CLI から行うことができます。

自己所有の共有マルチキャストドメインを共有解除するには、それをリソース共有から削除する必要があります。これを行うには、*Amazon Virtual Private Cloud Console、AWS RAM コンソール、または AWS CLI を使用します。

*Amazon Virtual Private Cloud Console を使用して所有している共有マルチキャストドメインの共有を解除するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Multicast Domains] (マルチキャストドメイン) を選択します。
3. マルチキャストドメインを選択し、[Actions] (アクション)、[Stop sharing] (共有を停止) の順に選択します。

AWS RAM コンソールを使用して所有している共有マルチキャストドメインの共有を解除するには

「AWS RAM ユーザーガイド」の「リソース共有の更新」を参照してください。

AWS CLI を使用して所有している共有マルチキャストドメインの共有を解除するには

disassociate-resource-share コマンドを使用します。

共有マルチキャストドメインを識別する

所有者とコンシューマーは、*Amazon Virtual Private Cloud Consoleおよび AWS CLI を使用して、共有マルチキャストドメインを特定できます

*Amazon Virtual Private Cloud Console を使用して共有マルチキャストドメインを識別するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Multicast Domains] (マルチキャストドメイン) を選択します。
3. マルチキャストドメインを選択します。
4. [Transit Multicast Domain Details] (トランジットマルチキャストドメインの詳細) ページで、[Owner ID] (所有者 ID) を表示して、マルチキャストドメインの AWS アカウント ID を識別します。

AWS CLI を使用して共有マルチキャストドメインを識別するには

describe-transit-gateway-multicast-domains コマンドを使用します。このコマンドは、所有しているマルチキャストドメインと、自分と共有されているマルチキャストドメインを返します。`OwnerId` は、マルチキャストドメイン所有者の AWS アカウント ID を示しています。

共有マルチキャストドメインのアクセス許可

所有者のアクセス許可

所有者は、マルチキャストドメインと、ドメインに登録または関連付けたメンバーとアタッチメントの管理に責任を負います。所有者は、いつでも共有アクセスを変更または取り消すことができます。AWS Organizations を使用して、コンシューマーが共有マルチキャストドメイン上に作成したリソースを表示、変更、および削除できます。

コンシューマーのアクセス許可

コンシューマーは、作成したマルチキャストドメインにおけるのと同じ方法で、共有マルチキャストドメインに対して次の操作を実行できます。

- マルチキャストドメイン内のグループメンバーまたはグループソースを登録および登録解除する
- サブネットをマルチキャストドメインに関連付けたり、サブネットとマルチキャストドメインとの関連付けを解除したりする

コンシューマーは、共有マルチキャストドメイン上に作成するリソースの管理に責任を負います。

お客様は、他のコンシューマーまたはマルチキャストドメイン所有者が所有するリソースを表示または変更することはできません。また、それらの者と共有されているマルチキャストドメインを変更することもできません。

請求と使用量測定

所有者またはコンシューマーのマルチキャストドメインを共有するための追加料金は発生しません。

クォータ

共有マルチキャストドメインは、所有者およびコンシューマーのマルチキャストドメインクォータにカウントされます。

トランジットゲートウェイの共有に関する考慮事項

AWSResource Access Manager (RAM) を使用して、アカウント全体、またはAWS Organizations の組織全体で VPC アタッチメントの Transit Gateway を共有できます。RAM を有効にし、リソースを組織と共有する必要があります。詳細については、「AWS RAM ユーザーガイド」の「AWS Organizations でリソース共有を有効にする」を参照してください。

トランジットゲートウェイを共有する場合は、以下の点を考慮してください。

- AWS Site-to-Site VPN Site-to-Site VPN アタッチメントは、トランジットゲートウェイを所有する同じ AWS アカウントで作成する必要があります。
- Direct Connect ゲートウェイへのアタッチメントは Transit Gateway の関連付けを使用し、Direct Connect ゲートウェイと同じAWSアカウントと、別のアカウントのどちらにも存在することができます。

デフォルトでは、ユーザーには AWS RAM リソースを作成または変更するためのアクセス許可はありません。ユーザーがリソースを作成または変更してタスクを実行できるようにするには、特定のリソースと API アクションを使用するアクセス許可を付与する IAM ポリシーを作成する必要があります。そのため、そのようなアクセス許可が必要な IAM ユーザーまたはグループにそのポリシーをアタッチします。

リソース所有者のみ次のオペレーションを実行できます。

- リソース共有を作成します。
- リソース共有を更新します。
- リソース共有を表示します。
- アカウントによって共有されているリソースをすべてのリソース共有間で表示できます。
- すべてのリソース共有で、リソースを共有しているプリンシパルを表示します。お客様の共有相手のプリンシパルを表示することで、お客様の共有リソースにアクセスできるプリンシパルを判別できます。
- リソース共有を削除します。
- トランジットゲートウェイ、トランジットゲートウェイアタッチメント、およびトランジットゲートウェイルートテーブル API をすべて実行します。

共有されているリソース上で次のオペレーションを実行することができます。

- リソースの共有の招待を承認または拒否します。
- リソース共有を表示します。
- お客様がアクセスできる共有リソースを表示します。
- リソースを共有しているすべてのプリンシパルのリストを表示します。共有されているリソースおよびリソース共有を確認することができます。
- `DescribeTransitGateways` API を実行できます。
- アタッチメントを作成して示している API を実行します (例: `CreateTransitGatewayVpcAttachment` および `DescribeTransitGatewayVpcAttachments` (VPC 内))。
- リソース共有を終了します。

Transit Gateway が共有されている場合、Transit Gateway ルートテーブルまたは Transit Gateway ルートテーブルの伝達および関連付けを作成、変更、削除することはできません。

トランジットゲートウェイを作成した場合、トランジットゲートウェイは自分のアカウントにマップされているアベイラビリティーゾーンに作成され、他のアカウントからは独立しています。トランジットゲートウェイおよびアタッチメントエンティティが異なるアカウントにある場合、アベイラビリティーゾーン ID を使用してアベイラビリティーゾーンを一意に一貫して識別します。例えば、use1-az1 は、us-east-1 リージョンの AZ ID で、すべてのAWSアカウントで同じ場所にマッピングされます。

トランジットゲートウェイの共有解除

共有所有者がトランジットゲートウェイの共有を解除する場合、次のルールが適用されます。

- トランジットゲートウェイアタッチメントは、機能し続けます。
- 共有アカウントでトランジットゲートウェイを示すことはできません。
- トランジットゲートウェイの所有者および共有所有者は、トランジットゲートウェイアタッチメントを削除できます。

トランジットゲートウェイが別の AWS アカウントと共有されていない場合、またはトランジットゲートウェイが共有されている AWS アカウントが組織から削除された場合、トランジットゲートウェイ自体は影響を受けません。

共有サブネット

VPC 所有者は、共有 VPC サブネットにトランジットゲートウェイを接続できます。参加者はできません。参加者のリソースからのトラフィックは、VPC 所有者が共有 VPC サブネットに設定したルートに応じて、アタッチメントを使用できます。

詳細については、「Amazon VPC ユーザーガイド」の「VPC を他のアカウントと共有する」を参照してください。

Transit Gateway Flow Logs を使用したネットワークトラフィックのログ記録

Transit Gateway Flow Logs は、Transit Gateway 間で行き来する IP トラフィックに関する情報をキャプチャできるようにする機能です。フローログデータは、Amazon CloudWatch Logs、Amazon S3、または Firehose に発行できます。フローログを作成したら、選択した送信先でそのデータを取得して表示できます。フローログデータはネットワークトラフィックのパスの外で収集されるため、ネットワークのスループットやレイテンシーには影響しません。ネットワークパフォーマンスに影響を与えるリスクなしに、フローログを作成または削除できます。Transit Gateway フローログは、「the section called “Transit Gateway Flow Log のレコード”」で説明されている Transit Gateway のみに関連する情報をキャプチャします。VPC 内のネットワークインターフェイスとの間で送受信される IP トラフィックに関する情報をキャプチャする場合は、VPC フローログを使用します。詳細については、「Amazon VPC ユーザーガイド」の「VPC フローログを使用した IP トラフィックのログ記録」を参照してください。

> **Note**
>
> トランジットゲートウェイフローログを作成するには、トランジットゲートウェイの所有者である必要があります。お客様が所有者でない場合は、トランジットゲートウェイの所有者からアクセス許可が付与される必要があります。

モニタリングされる Transit Gateway のフローログデータは、フローログレコードとして記録されます。これは、トラフィックフローについて説明するフィールドで構成されるログイベントです。詳細については、「Transit Gateway Flow Log のレコード」を参照してください。

フローログを作成するには、以下の内容を指定します。

- フローログを作成するリソース
- フローログデータを発行する送信先

フローログを作成後、データ収集と選択された送信先へのデータ発行が開始されるまでに数分かかる場合があります。フローログで、Transit Gateway のリアルタイムのログストリームはキャプチャされません。詳細については、「フローログの作成」を参照してください。

フローログにタグを適用できます。タグはそれぞれ、1 つのキーとオプションの 1 つの値で構成されており、どちらもお客様側が定義します。タグは、目的や所有者などによって、フローログを整理するのに役立ちます。

フローログが不要になった場合には、それを削除することができます。フローログを削除すると、リソースのフローログサービスは無効になり、新しいフローログレコードは作成されず、 CloudWatch ログまたは Amazon S3 に発行されません。フローログを削除しても、トランジットゲートウェイの既存のフローログレコードまたはログストリーム (CloudWatch Logs の場合) またはログファイルオブジェクト (Amazon S3 の場合) は削除されません。既存のログストリームを削除するには、 CloudWatch ログコンソールを使用します。既存のログファイルオブジェクトを削除するには、Amazon S3 コンソールを使用します。フローログを削除した後で、データの収集が中止するまでに数分かかる場合があります。詳細については、「フローログの削除」を参照してください。

制限事項

Transit Gateway フローログには、次の制限が適用されます。

- マルチキャストトラフィックはサポートされていません。
- Connect アタッチメントはサポートされていません。すべての Connect フローログはトランスポートアタッチメントの下に表示されるため、トランジットゲートウェイまたは Connect トランスポートアタッチメントで有効にする必要があります。

Transit Gateway Flow Log のレコード

フローログレコードは、Transit Gateway のネットワークフローを表します。各レコードは、スペースで区切られたフィールドから成る文字列です。送信元、送信先、プロトコルなど、レコードにはトラフィックフローのさまざまなコンポーネントの値が含まれています。

フローログを作成するときは、フローログレコードのデフォルトの形式を使用するか、カスタム形式を指定できます。

内容

デフォルトの形式

デフォルトの形式では、フローログレコードには、使用可能なフィールドテーブルに表示される順序でバージョン 2 から 6 のフィールドが含まれます 。デフォルトの形式をカスタマイズまたは変更することはできません。使用可能なすべてのフィールドまたはフィールドの異なるサブセットをキャプチャするには、代わりにカスタム形式を指定します。

カスタム形式

カスタム形式を使用して、フローログレコードに含めるフィールドと順序を指定します。これにより、ニーズに合ったフローログを作成し、関連のないフィールドを省略できます。カスタム形式を使用すると、発行されたフローログから特定の情報を抽出する別個のプロセスが不要になります。使用可能なフローログフィールドは任意の数指定できますが、少なくとも 1 つ指定する必要があります。

使用可能なフィールド

次の表に、Transit Gateway フローログレコードの使用可能なすべてのフィールドを示します。Version 列には、フィールドが導入されたバージョンが表示されます。

Amazon S3 にフローログデータを公開する場合、フィールドのデータ型はフローログ形式によって異なります。形式がプレーンテキストの場合、すべてのフィールドは STRING 形式です。形式が Parquet の場合は、フィールドのデータ型の表を参照してください。

フィールドが特定のレコードに該当しないか、特定のレコードに対して計算できなかった場合、レコードでそのエントリには「-」記号が表示されます。パケットヘッダーから直接取得されないメタデータフィールドは、ベストエフォート近似値であり、値が欠落しているか、不正確である可能性があります。

フィールド	説明	Version
version	フィールドが導入されたバージョンを示します。デフォルトの形式には、すべてのバージョン 2 フィールドが含まれ、順番はテーブルと同じです。 Parquet データ型: INT_32	2
resource-type	サブスクリプションが作成されるリソースのタイプ。Transit Gateway フローログの場合、これは になりますTransitGateway。	6

フィールド	説明	Version
	Parquet データ型: STRING	
account-id	ソーストランジットゲートウェイの所有者の AWS アカウント ID。 Parquet データ型: STRING	2
tgw-id	トラフィックが記録される Transit Gateway の ID。 Parquet データ型: STRING	6
tgw-attachment-id	トラフィックが記録される Transit Gateway アタッチメントの ID。 Parquet データ型: STRING	6
tgw-src-vpc-account-id	ソース VPC トラフィックの AWS アカウント ID。 Parquet データ型: STRING	6
tgw-dst-vpc-account-id	送信先 VPC トラフィックの AWS アカウント ID。 Parquet データ型: STRING	6
tgw-src-vpc-id	Transit Gateway の送信元 VPC の ID。 Parquet データ型: STRING	6
tgw-dst-vpc-id	Transit Gateway の送信先 VPC の ID。 Parquet データ型: STRING	6
tgw-src-subnet-id	Transit Gateway 送信元トラフィックのサブネットの ID。 Parquet データ型: STRING	6
tgw-dst-subnet-id	Transit Gateway 送信先トラフィックのサブネットの ID。 Parquet データ型: STRING	6
tgw-src-eni	フローの送信元 Transit Gateway アタッチメント ENI の ID。 Parquet データ型: STRING	6

フィールド	説明	Version
tgw-dst-eni	フローの送信先 Transit Gateway アタッチメント ENI の ID。 Parquet データ型: STRING	6
tgw-src-az-id	トラフィックが記録される Transit Gateway を含むアベイラビリティーゾーンの ID。トラフィックがサブロケーションからの場合、レコードにはこのフィールドに「-」記号が表示されます。 Parquet データ型: STRING	6
tgw-dst-az-id	トラフィックが記録される送信先 Transit Gateway を含むアベイラビリティーゾーンの ID。 Parquet データ型: STRING	6
tgw-pair-attachment-id	フローの方向に応じて、これはフローの出力または入力のアタッチメント ID になります。 Parquet データ型: STRING	6
srcaddr	受信トラフィックの送信元アドレス。 Parquet データ型: STRING	2
dstaddr	送信トラフィックの送信先アドレス。 Parquet データ型: STRING	2
srcport	トラフィックの送信元ポート。 Parquet データ型: INT_32	2
dstport	トラフィックの送信先ポート。 Parquet データ型: INT_32	2
protocol	トラフィックの IANA プロトコル番号。詳細については、「割り当てられたインターネットプロトコル番号」を参照してください。 Parquet データ型: INT_64	2

フィールド	説明	Version
packets	フロー中に転送されたパケットの数。 Parquet データ型: INT_64	2
bytes	フロー中に転送されたバイト数。 Parquet データ型: INT_64	2
start	集約間隔内にフローの最初のパケットが受信された時間 (UNIX 秒)。これは、パケットが Transit Gateway 上で送信または受信されてから最大 60 秒になる場合があります。 Parquet データ型: INT_64	2
end	集約間隔内にフローの最後のパケットが受信された時間 (UNIX 秒)。これは、パケットが Transit Gateway 上で送信または受信されてから最大 60 秒になる場合があります。 Parquet データ型: INT_64	2
log-status	フローログのステータス。 • OK — データは選択された送信先に正常にログ記録されます。 • NODATA — 集約間隔内にネットワークインターフェイスとの間で行き来するネットワークトラフィックはありませんでした。 • SKIPDATA — 集約間隔内に一部のフローログレコードがスキップされました。これは、内部的なキャパシティー制限、または内部エラーが原因である可能性があります。 Parquet データ型: STRING	2
type	トラフィックの種類。指定できる値は、IPv4 | IPv6 | EFA です。詳細については、「Amazon EC2 ユーザーガイド」の「Elastic Fabric Adapter」を参照してください。 Amazon EC2 Parquet データ型: STRING	3

フィールド	説明	Version
packets-lost-no-route	ルートが指定されていないためにパケットが失われました。 Parquet データ型: INT_64	6
packets-lost-blackhole	ブラックホールのためにパケットが失われました。 Parquet データ型: INT_64	6
packets-lost-mtu-exceeded	MTU を超えるサイズのためにパケットが失われました。 Parquet データ型: INT_64	6
packets-lost-ttl-expired	の有効期限が切れたためにパケットが失われました time-to-live。 Parquet データ型: INT_64	6

フィールド	説明	Version
tcp-flags	次の TCP フラグのビットマスク値: • FIN — 1 • SYN — 2 • RST — 4 • PSH — 8 • ACK — 16 • SYN-ACK — 18 • URG — 32 **Important** フローログエントリが ACK パケットのみで構成されている場合、フラグ値は 16 ではなく 0 になります。 TCP フラグの一般的な情報 (FIN、SYN、ACK などのフラグの意味など) については、Wikipedia の「TCP セグメント構造」を参照してください。 TCP フラグは、集約間隔内に OR 処理することができます。短い接続の場合、フラグがフローログレコードの同じ行に設定されることがあります (例えば、SYN-ACK と FIN の場合は 19、SYN と FIN の場合は 3 など)。 Parquet データ型: INT_32	3
region	トラフィックが記録される Transit Gateway を含むリージョン。 Parquet データ型: STRING	4
flow-direction	トラフィックがキャプチャされるインターフェイスに対するフローの方向。指定できる値は次のとおりです: ingress | egress。 Parquet データ型: STRING	5

フィールド	説明	Version
pkt-src-aws-service	送信元 IP アドレスが サービスのものである場合の、 の IP アドレス範囲のサブセットの名前。 srcaddr AWS 指定可能な値は次のとおりです:AMAZON |AMAZON_APPFLOW |AMAZON_CONNECT |API_GATEWAY |CHIME_MEETINGS |CHIME_VOICECONNECTOR |CLOUD9 |CLOUDFRONT |CODEBUILD |DYNAMODB |EBS |EC2 |EC2_INSTANCE_CONNECT |GLOBALACCELERATOR |KINESIS_VIDEO_STREAMS |ROUTE53 |ROUTE53_HEALTHCHECKS |ROUTE53_HEALTHCHECKS_PUBLISHING |ROUTE53_RESOLVER |S3 |WORKSPACES_GATEWAYS。 Parquet データ型: STRING	5
pkt-dst-aws-service	送信先 IP アドレスが AWS サービスのものである場合、 dstaddr フィールドの IP アドレス範囲のサブセットの名前。可能な値の一覧については、pkt-src-aws-service フィールドをご参照ください。Parquet データ型: STRING	5

Transit Gateway Flow Logs の料金

Transit Gateway フローログを発行すると、提供されたログに対するデータインジェスト料金とアーカイブ料金が適用されます。発行されたログを発行する際の料金の詳細については、Amazon CloudWatch 料金表 を開き、有料階層 でログ を選択し、発行されたログ を見つけます。

ログに発行するフロー CloudWatch ログを作成する

フローログは、フローログデータを Amazon に直接発行できます CloudWatch。

CloudWatch Logs に発行されると、フローログデータはロググループに発行され、各トランジットゲートウェイにはロググループに一意のログストリームがあります。ログストリームにはフローログレコードが含まれます。同じロググループにデータを公開する複数のフローログを作成できます。同じ Transit Gateway が同じロググループの 1 つまたは複数のフローログに存在する場合、1 つの組み合わされたログストリームがあります。1 つのフローログで、拒否されたトラフィックをキャプチャし、別のフローログで、許可されたトラフィックをキャプチャするよう指定した場合、組み合わされたログストリームですべてのトラフィックがキャプチャされます。

フローログを CloudWatch Logs に発行すると、提供されたログのデータ取り込み料金とアーカイブ料金が適用されます。詳細については、「Amazon CloudWatch の料金」を参照してください。

CloudWatch Logs のタイムスタンプフィールドは、フローログレコードにキャプチャされた開始時刻に対応します。ingestionTime フィールドには、フローログレコードが CloudWatch Logs によって受信された日時が表示されます。タイムスタンプは、フローログレコードでキャプチャされた終了時刻より後になります。

CloudWatch ログの詳細については、「Amazon Logs ユーザーガイド」の CloudWatch 「ログに送信されたログ」を参照してください。 CloudWatch

内容

フローログを Logs に発行するための IAM CloudWatch ロール

フローログに関連付けられている IAM ロールには、 CloudWatch Logs で指定されたロググループにフローログを発行するための十分なアクセス許可が必要です。IAM ロールは に属している必要があります AWS アカウント。

IAM ロールにアタッチされた IAM ポリシーには、少なくとも以下のアクセス許可が含まれている必要があります。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource": "*"
```

```
    }
  ]
}
```

フローログサービスがロールを引き受けることができる信頼関係がロールにあることも確認します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Confused Deputy Problem (混乱した使節の問題) から自分を守るために、aws:SourceAccount および aws:SourceArn の条件キーを使用することをお勧めします。例えば、前述の信頼ポリシーに次の条件ブロックを追加できます。ソースアカウントはフローログの所有者であり、ソース ARN はフローログ ARN です。フローログ ID が不明な場合は、ARN の不明部分をワイルドカード (*) に置き換え、フローログ作成後にポリシーを更新できます。

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account_id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:region:account_id:vpc-flow-log/flow-log-id"
    }
}
```

フローログの IAM ロールを作成または更新する

既存ロールを更新するか、次の手順を使用してフローログで使用する新しいロールを作成できます。

フローログの IAM ロールを作成するには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。

2. ナビゲーションペインで [ロール]、[ロールの作成] の順に選択します。
3. 信頼できるエンティティの種類の選択 で、AWS サービス を選択します。[ユースケース] で、[EC2] を選択します。[次へ] をクリックします。
4. [アクセス権限を追加] ページで、[次へ: レビュー] を選択し、オプションでタグを追加します。[次へ] をクリックします。
5. 名前、確認、作成ページで、ロールの名前を入力し、オプションで説明を入力します。[ロールの作成] を選択します。
6. ロールの名前を選択します。[アクセス許可] で [インラインポリシーの作成] を選択してから、[JSON] タブを選択します。
7. 「フローログを Logs に発行するための IAM CloudWatch ロール」から最初のポリシーをコピーして、ウィンドウに貼り付けます。[ポリシーの確認] を選択します。
8. ポリシーの名前を入力し、[ポリシーの作成] を選択します。
9. ロールの名前を選択します。[信頼関係] で、[信頼関係の編集] を選択します。既存のポリシードキュメントで、サービスを `ec2.amazonaws.com` から `vpc-flow-logs.amazonaws.com` に変更します。[信頼ポリシーの更新] を選択します。
10. [概要] ページで、ロールの ARN を書き留めます。フローログを作成するときに、この ARN が必要になります。

IAM ユーザーがロールを渡すためのアクセス許可

フローログに関連付けられた IAM ロール用に `iam:PassRole` アクションを使用するアクセス許可もユーザーに必要です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["iam:PassRole"],
      "Resource": "arn:aws:iam::account-id:role/flow-log-role-name"
    }
  ]
}
```

ログに発行するフロー CloudWatch ログを作成する

Transit Gateway のフローログを作成できます。これらのステップを IAM ユーザーとして実行する場合は、`iam:PassRole` アクションを使用するアクセス許可があることを確認してください。詳細については、「IAM ユーザーがロールを渡すためのアクセス許可」を参照してください。

コンソールを使用して Transit Gateway フローログを作成するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/vpc/ で Amazon VPC コンソールを開きます。
2. ナビゲーションペインで、[Transit Gateway] を選択します。
3. 1 つまたは複数の Transit Gateway のチェックボックスを選択し、[アクション]、[フローログの作成] の順に選択します。
4. 送信先 で、ログに送信 CloudWatch を選択します。
5. [送信先ロググループ] で、現在の送信先ロググループの名前を選択します。

   > **Note**
   >
   > 送信先ロググループがまだ存在しない場合は、このフィールドに新しい名前を入力すると、新しい送信先ロググループが作成されます。

6. IAM ロール では、ログを CloudWatch Logs に発行するアクセス許可を持つロールの名前を指定します。
7. [Lログレコードの形式] で、フローログレコードの形式を選択します。
   - デフォルトの形式を使用するには、[AWS のデフォルト形式] を選択します。
   - カスタム形式を使用するには、[カスタム形式] を選択し、[ログ形式] からフィールドを選択します。
8. (オプション) フローログにタグを適用するには、[新規タグを追加] を選択します。
9. [フローログの作成] を選択します。

コマンドラインを使用してフローログを作成するには

以下のいずれかのコマンドを使用します。

- create-flow-logs (AWS CLI)

- New-EC2FlowLogs (AWS Tools for Windows PowerShell)
- CreateFlowログ (Amazon EC2 クエリ API)

次の AWS CLI 例では、トランジットゲートウェイ情報をキャプチャするフローログを作成します。フローログは、IAM ロール を使用してmy-flow-logs、アカウント 123456789101 の CloudWatch というログのロググループに配信されますpublishFlowLogs。

```
aws ec2 create-flow-logs --resource-type TransitGateway --resource-ids
 tgw-1a2b3c4d --log-group-name my-flow-logs --deliver-logs-permission-arn
 arn:aws:iam::123456789101:role/publishFlowLogs
```

CloudWatch Logs でフローログレコードを処理する

Logs によって収集された他のログイベントと同様に、フロー CloudWatch ログレコードを操作できます。ログデータとメトリクスフィルターのモニタリングの詳細については、「Amazon ユーザーガイド」の「ログデータの検索とフィルタリング」を参照してください。 CloudWatch

例: フローログの CloudWatch メトリクスフィルターとアラームを作成する

この例では、tgw-123abc456bca のフローログがあります。1 時間以内の期間に TCP ポート 22 (SSH) 経由でインスタンスに接続しようとする試みが 10 個以上拒否された場合に、アラームを作成するとします。最初に、アラームを作成するトラフィックのパターンと一致するメトリクスフィルターを作成する必要があります。次に、メトリクスフィルターのアラームを作成できます。

拒否された SSH トラフィックのメトリクスフィルターを作成し、フィルタのアラームを作成するには

1. https://console.aws.amazon.com/cloudwatch/ で CloudWatch コンソールを開きます。
2. ナビゲーションペインで、[ログ]、[ロググループ] の順に選択します。
3. ロググループのチェックボックスをオンにしてから、[アクション]、[メトリクスフィルターの作成] を選択します。
4. [フィルターパターン] で、次のように入力します。

```
[version, resource_type, account_id,tgw_id="tgw-123abc456bca”, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr= "10.0.0.1", dstaddr,
 srcport=“80”, dstport, protocol=“6”, packets, bytes,start,end, log_status,
```

```
type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
pkt_dst_aws_service]
```

5. [テストするログデータの選択] で、Transit Gateway のログストリームを選択します。(オプション) フィルターパターンと一致するログデータの行を表示するには、[テストパターン] を選択します。準備ができたら、[次へ] を選択します。
6. フィルター名、メトリクス名前空間、およびメトリック名を入力します。メトリクス値の設定を「**1**」にします。完了したら、[次へ] を選択し、その後 [メトリクスフィルターの作成] を選択します。
7. ナビゲーションペインで、[アラーム]、[すべてのアラーム] の順に選択します。
8. [アラームの作成] を選択します。
9. 作成したメトリクスフィルターの名前空間を選択します。

   新しいメトリクスがコンソールに表示されるまでに数分かかる場合があります。
10. 作成したメトリクス名を選択し、その後 [メトリクスの選択] を選択します。
11. アラームを以下のように設定して、[次へ] をクリックします。

    - [統計] で、[合計] を選択します。これにより、指定された期間のデータポイントの総数をキャプチャしていることを確認できます。
    - [期間] で、[1 時間] を選択します。
    - [随時] で、[以上] を選択し、しきい値は「**10**」と入力します。
    - [追加設定]、[警告を出すデータポイント数] はデフォルトの「**1**」のままにしておきます。
12. [通知] で、既存の SNS トピックを選択するか、[新しいトピックを作成] を選択して新しいトピックを作成します。[次へ] をクリックします。
13. 次のページで、アラームの名前と説明を入力し、[次へ] を選択します。
14. アラームの設定が終わったら、[アラームを作成] を選択します。

Amazon S3 に発行するフローログの作成

フローログはフローログデータを Amazon S3 に発行できます。

Amazon S3 に発行した場合、フローログデータは、指定する既存の Amazon S3 バケットに発行されます。モニタリングされるすべての Transit Gateway のフローログレコードが、バケットに保存された一連のログファイルオブジェクトに発行されます。

フローログを Amazon S3 に発行すると、 Amazon CloudWatch データインジェスト料金とアーカイブ料金が によって提供されるログに適用されます。発行されたログの CloudWatch 料金の詳細については、Amazon CloudWatch の料金 を開き、ログ を選択してから、発行されたログ を見つけます。

フローログに使用する Amazon S3 バケットの作成方法については、Amazon Simple Storage Service ユーザーガイドの「バケットの作成」を参照してください。

複数のアカウントログの詳細については、「AWS ソリューションライブラリの中央ロギング」を参照してください。

CloudWatch ログの詳細については、Amazon S3 に送信された CloudWatch ログ」を参照してください。

内容

フローログファイル

VPC Flow Logs は、フローログレコードを収集し、ログファイルに統合して、5 分間隔でログファイルを Amazon S3 バケットに発行する機能です。各ログファイルには、前の 5 分間に記録された IP トラフィックのフローログレコードが含まれています。

ログファイルの最大ファイルサイズは 75 MB です。ログファイルが 5 分以内にファイルサイズの上限に達した場合、フローログはフローログレコードの追加を停止します。次に、フローログを Amazon S3 バケットに発行してから、新しいログファイルを作成します。

Amazon S3 では、フローログファイルの [最終更新日時] フィールドに、ファイルが Amazon S3 バケットにアップロードされた日時が表示されます。これは、ファイル名のタイムスタンプより後で、Amazon S3 バケットにファイルをアップロードするのにかかった時間によって異なります。

ログファイル形式

ログファイルに指定できる形式は次のとおりです。各ファイルは 1 つの Gzip ファイルに圧縮されます。

- [Text] - プレーンテキスト。これがデフォルトの形式です。
- [Parquet] - Apache Parquet は列指向データ形式です。Parquet 形式のデータに対するクエリは、プレーンテキストのデータに対するクエリに比べて 10 ~ 100 倍高速です。Gzip 圧縮を使用した Parquet 形式のデータは、Gzip 圧縮を使用したプレーンテキストよりもストレージスペースが 20% 少なくなります。

ログファイルオプション

オプションで、次のオプションを指定できます。

- [Hive-compatible S3 prefixes] - Hive 互換ツールにパーティションをインポートする代わりに、Hive 互換プレフィックスを有効にします。クエリを実行する前に、[MSCK REPAIR TABLE] コマンドを使用します。
- [Hourly partitions] - 大量のログがあり、通常は特定の時間にクエリをターゲットにしている場合、ログを時間単位で分割することで、より高速な結果が得られ、クエリコストを節約できます。

ログファイル S3 バケット構造

ログファイルでは、フローログの ID、リージョン、作成日、および送信先オプションに基づくフォルダ構造を使用して、指定された Amazon S3 バケットに保存されます。

デフォルトでは、ファイルは次の場所に配信されます。

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/
```

Hive 互換の S3 プレフィックスを有効にすると、ファイルは次の場所に配信されます。

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/service=vpcflowlogs/aws-region=region/year=year/month=month/day=day/
```

時間単位のパーティションを有効にすると、ファイルは次の場所に配信されます。

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/hour/
```

Hive 互換パーティションを有効にして 1 時間あたりのフローログをパーティション化すると、ファイルは次の場所に配信されます。

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/service=vpcflowlogs/aws-region=region/year=year/month=month/day=day/hour=hour/
```

ログファイル名

ログファイルのファイル名は、フローログ ID、リージョン、および作成日時に基づきます。ファイル名は、次の形式です。

```
aws_account_id_vpcflowlogs_region_flow_log_id_YYYYMMDDTHHmmZ_hash.log.gz
```

以下は、us-east-1 リージョンで June 20, 2018 の 16:20 UTC に、リソースに対して AWS アカウント「123456789012」で作成されたフローログのログファイルの例です。ファイルには、終了時刻が 16:20:00 から 16:24:59 の間のフローログレコードが含まれます。

```
123456789012_vpcflowlogs_us-east-1_fl-1234abcd_20180620T1620Z_fe123456.log.gz
```

フローログを Amazon S3 にパブリッシュする IAM プリンシパルの IAM ポリシー

フローログを作成する IAM プリンシパルには、フローログを宛先の Amazon S3 バケットに公開するために、以下のアクセス許可が付与されている必要があります。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
        ],
      "Resource": "*"
    }
  ]
}
```

フローログのための Amazon S3 バケットのアクセス許可

デフォルトでは、Amazon S3 バケットとそれに含まれているオブジェクトはプライベートです。バケット所有者のみが、そのバケットとそれに含まれているオブジェクトにアクセスできます。ただし、バケット所有者は、アクセスポリシーを記述することで他のリソースおよびユーザーにアクセス権限を付与することができます。

フローログを作成するユーザーがバケットを所有し、そのバケットに PutBucketPolicy および GetBucketPolicy 許可を持っている場合、次のポリシーが自動的にそのバケットにアタッチされます。このポリシーは、バケットにアタッチされている既存のポリシーを上書きします。

それ以外の場合は、バケット所有者が、フローログ作成者の AWS アカウント ID を指定して、このポリシーをバケットに追加しなければ、フローログの作成は失敗します。詳細については、Amazon Simple Storage Service ユーザーガイドのバケットポリシーの使用を参照してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource": "my-s3-arn",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": account_id
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:region:account_id:*"
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryCheck",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": ["s3:GetBucketAcl", "s3:ListBucket"],
            "Resource": "arn:aws:s3:::bucket_name",
            "Condition": {
                "StringEquals": {
```

```
                    "aws:SourceAccount": account_id
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:region:account_id:*"
                }
            }
        }
    ]
}
```

my-s3-arn に指定する ARN は、Hive と互換性のある S3 のプレフィックスを使用するかどうかによって異なります。

- デフォルトのプレフィックス

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/account_id/*
```

- Hive 互換の S3 プレフィックス

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/aws-account-id=account_id/*
```

ベストプラクティスとして、個々の AWS アカウント ARNs ではなく、ログ配信サービスプリンシパルにこれらのアクセス許可を付与することをお勧めします。また、aws:SourceAccount および aws:SourceArn 条件キーを使用して、混乱した使節の問題から保護することもベストプラクティスです。ソースアカウントはフローログの所有者であり、ソース ARN は、ログサービスのワイルドカード (*) ARN です。

SSE-KMS に使用する必須のキーポリシー

Amazon S3 バケット内のデータを保護するには、Amazon S3 マネージドキーを使用したサーバー側の暗号化 (SSE-S3)、または に格納された KMS キーを使用したサーバー側の暗号化 (SSE-KMS) のいずれかを有効にします。詳細については、Amazon S3 ユーザーガイドの「サーバー側の暗号化を使用したデータの保護」をご参照ください。

SSE-KMS では、 AWS マネージドキーまたはカスタマーマネージドキーを使用できます。 AWS マネージドキーでは、クロスアカウント配信を使用できません。フローログはログ配信アカウントから配信されるため、クロスアカウント配信のアクセス権を付与する必要があります。S3 バケットへのクロスアカウントアクセス権を付与するには、カスタマーマネージドキーを使用し、バケット暗号化を有効にするときに、カスタマーマネージドキーの Amazon リソースネーム (ARN) を指定します。

詳細については、Amazon S3 ユーザーガイドの「AWS KMSによるサーバー側の暗号化の指定」をご参照ください。

カスタマーマネージドキーで SSE-KMS を使用する場合、VPC Flow Logs が S3 バケットに書き込めるように、キーのキーポリシー (S3 バケットのバケットポリシーではありません) に以下を追加する必要があります。

```
{
    "Sid": "Allow Transit Gateway Flow Logs to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "delivery.logs.amazonaws.com"
        ]
    },
   "Action": [
       "kms:Encrypt",
       "kms:Decrypt",
       "kms:ReEncrypt*",
       "kms:GenerateDataKey*",
       "kms:DescribeKey"
    ],
    "Resource": "*"
}
```

Amazon S3 ログファイルのアクセス許可

Amazon S3 は、必須のバケットポリシーに加えて、アクセスコントロールリスト (ACL) を使用して、フローログによって作成されたログファイルへのアクセスを管理します。デフォルトでは、バケット所有者が各ログファイルで FULL_CONTROL 権限を持ちます。ログ配信の所有者 (バケット所有者とは異なる場合) は、許可を持ちません。ログ配信アカウントには、READ および WRITE 許可があります。詳細については、Amazon Simple Storage Service ユーザーガイドの「アクセスコントロールリスト (ACL) の概要」を参照してください。

Amazon S3 に発行するフローログの作成

Amazon S3 バケットを作成して設定した後は、Transit Gateway のフローログを作成できます。

コンソールを使用して Amazon S3 に発行される Transit Gateway フローログを作成するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。

2. ナビゲーションペインで、[Transit Gateways]、[Transit Gateway アタッチメント] の順に選択します。
3. 1 つまたは複数の Transit Gateway または Transit Gateway アタッチメントのチェックボックスを選択します。
4. [アクション]、[フローログの作成] を選択します。
5. フローログ設定を構成します。詳細については、「フローログ設定を構成するには」を参照してください。

コンソールを使用してフローログ設定を構成するには

1. [送信先] で、[S3 バケットへの送信] を選択します。
2. [S3 バケット ARN] で、既存の Amazon S3 バケットの Amazon リソースネーム (ARN) を指定します。オプションで、サブフォルダを含めることができます。例えば、`my-logs` というバケットで `my-bucket` というサブフォルダを指定するには、次の ARN を使用します。

   ```
   arn:aws::s3:::my-bucket/my-logs/
   ```

   `AWSLogs` は予約語であるため、バケットでサブフォルダ名として使用することはできません。

   バケットを所有している場合は、リソースポリシーが自動的に作成され、バケットにアタッチされます。詳細については、「フローログのための Amazon S3 バケットのアクセス許可」を参照してください。
3. [ログレコード形式] で、フローログレコードの形式を指定します。
   - デフォルトのフローログレコード形式を使用するには、[AWS のデフォルト形式] を選択します。
   - カスタム形式を作成するには、[カスタム形式] を選択します。[ログの形式] で、フローログレコードに含めるフィールドを選択します。
4. [ログファイル形式] で、ログファイルの形式を指定します。
   - [Text] - プレーンテキスト。これがデフォルトの形式です。
   - [Parquet] - Apache Parquet は列指向データ形式です。Parquet 形式のデータに対するクエリは、プレーンテキストのデータに対するクエリに比べて 10 ~ 100 倍高速です。Gzip 圧縮を使用した Parquet 形式のデータは、Gzip 圧縮を使用したプレーンテキストよりもストレージスペースが 20% 少なくなります。

5. (オプション) Hive 互換の S3 プレフィックスを使用するには、[Hive-compatible S3 prefix]、[有効化] を選択します。
6. (オプション) 1 時間あたりのフローログを分割するには、[Every 1 hour (60 mins)] を選択します。
7. (オプション) フローログにタグを追加するには、[新しいタグを追加] を選択し、タグのキーと値を指定します。
8. [フローログの作成] を選択します。

コマンドラインツールを使用して Amazon S3 に発行されるフローログを作成するには

以下のいずれかのコマンドを使用します。

- create-flow-logs (AWS CLI)
- New-EC2FlowLogs (AWS Tools for Windows PowerShell)
- CreateFlowログ (Amazon EC2 クエリ API)

次の AWS CLI 例では、VPC のすべてのトランジットゲートウェイトラフィックをキャプチャするフローログ`tgw-00112233344556677`を作成し、フローログを というの Amazon S3 バケットに配信します`flow-log-bucket`。`--log-format` パラメータにより、フローログレコードのカスタム形式が指定されます。

```
aws ec2 create-flow-logs --resource-type TransitGateway --resource-ids
 tgw-00112233344556677 --log-destination-type s3 --log-destination arn:aws:s3:::flow-
log-bucket/my-custom-flow-logs/'
```

Amazon S3 でのフローログレコードの処理

ログファイルは圧縮されます。Amazon S3 コンソールを使用してログファイルを開くと、ファイルは解凍され、フローログレコードが表示されます。ファイルをダウンロードする場合、フローログレコードを表示するには解凍する必要があります。

Firehose へのフローログの発行

トピック

- クロスアカウント配信のための IAM ロール
- Firehose に発行するフローログを作成する

フローログは、フローログデータを Firehose に直接発行できます。フローログの発行先は、リソースモニターと同じアカウント、または別のアカウントを選択できます。

前提条件

Firehose に発行する場合、フローログデータはプレーンテキスト形式で Firehose 配信ストリームに発行されます。まず、Firehose 配信ストリームを作成しておく必要があります。配信ストリームを作成する手順については、「Amazon Data Firehose デベロッパーガイド」の「Amazon Data Firehose 配信ストリームの作成」を参照してください。

料金表

標準の取り込み料金と配信料金が適用されます。詳細については、Amazon CloudWatch 料金表 を開き、ログ を選択して、提供されたログ を見つけます。

クロスアカウント配信のための IAM ロール

Kinesis Data Firehose に発行する場合、監視するリソースと同じアカウント (ソースアカウント) または別のアカウント (送信先アカウント) にある配信ストリームを選択できます。Firehose へのフローログのクロスアカウント配信を有効にするには、ソースアカウントに IAM ロールを作成し、宛先アカウントに IAM ロールを作成する必要があります。

ロール

- ソースアカウントロール
- 送信先アカウントロール

ソースアカウントロール

ソースアカウントで、次のアクセス許可を付与するロールを作成します。この例のロールの名前は `mySourceRole` ですが、このロールには別の名前を選択できます。最後のステートメントにより、送信先アカウントのロールがこのロールを引き受けることができるようになります。条件ステートメントにより、このロールは指定されたリソースを監視する場合に限り、ログ配信サービスだけに渡されます。ポリシーを作成するときに、監視する VPC、ネットワークインターフェイス、またはサブネットを条件キー `iam:AssociatedResourceARN` で指定します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::source-account:role/mySourceRole",
      "Condition": {
          "StringEquals": {
              "iam:PassedToService": "delivery.logs.amazonaws.com"
          },
          "StringLike": {
              "iam:AssociatedResourceARN": [
                  "arn:aws:ec2:region:source-account:transit-gateway/
tgw-0fb8421e2da853bf"
              ]
          }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
          "logs:CreateLogDelivery",
          "logs:DeleteLogDelivery",
          "logs:ListLogDeliveries",
          "logs:GetLogDelivery"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::destination-account:role/
AWSLogDeliveryFirehoseCrossAccountRole"
    }
  ]
}
```

このロールに以下の信頼ポリシーがあることを確認します。これにより、ログ配信サービスがロールを引き受けることができます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
```

```
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

ソースアカウントから、以下に説明する手順に従ってロールを作成します。

ソースアカウントロールを作成するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/iam/ で IAM コンソールを開きます。
2. ナビゲーションペインで、ポリシー を選択します。
3. [ポリシーの作成] を選択します。
4. [ポリシーの作成] ページで、次の操作を行います。
   1. [JSON] を選択します。
   2. このウィンドウのコンテンツを、このセクションの冒頭にあるアクセス許可ポリシーに置き換えてください。
   3. [次へ: タグ]、[次へ: 確認] の順に選択します。
   4. ポリシーの名前と説明 (省略可能) を入力し、[ポリシーの作成] を選択します。
5. ナビゲーションペインで [ロール] を選択します。
6. [ロールの作成] を選択します。
7. [信頼されたエンティティのタイプ] には、[カスタム信頼ポリシー] を選択します。[カスタム信頼ポリシー] で、`"Principal": {},` を次のように置き換え、ログ配信サービスを指定します。[次へ] をクリックします。

   ```
   "Principal": {
      "Service": "delivery.logs.amazonaws.com"
   },
   ```

8. [Add permissions] (アクセス許可の追加) ページで、この手順で先ほど作成したポリシーの横にあるチェックボックスを選択し、[Next] (次へ) を選択します。
9. ロールの名前を入力し、オプションで説明を入力します。
10. [ロールの作成] を選択します。

送信先アカウントロール

送信先アカウントで、 で始まる名前のロールを作成しますAWSLogsDeliveryFirehoseCrossAccountRole。このロールには、以下のアクセス許可が必要です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
          "iam:CreateServiceLinkedRole",
          "firehose:TagDeliveryStream"
      ],
      "Resource": "*"
    }
  ]
}
```

このロールに次の信頼ポリシーがあることを確認します。これにより、ソースアカウントで作成したロールがこのロールを引き受けることができます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
          "AWS": "arn:aws:iam::source-account:role/mySourceRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

送信先アカウントから、以下に説明する手順に従ってロールを作成します。

送信先アカウントロールを作成するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/iam/ で IAM コンソールを開きます。

2. ナビゲーションペインで、ポリシー を選択します。
3. [ポリシーの作成] を選択します。
4. [ポリシーの作成] ページで、次の操作を行います。
   1. [JSON] を選択します。
   2. このウィンドウのコンテンツを、このセクションの冒頭にあるアクセス許可ポリシーに置き換えてください。
   3. [次へ: タグ]、[次へ: 確認] の順に選択します。
   4. で始まるポリシーの名前を入力しAWSLogDeliveryFirehoseCrossAccountRole、ポリシーの作成 を選択します。
5. ナビゲーションペインで Roles (ロール) を選択します。
6. [ロールの作成] を選択します。
7. [信頼されたエンティティのタイプ] には、[カスタム信頼ポリシー] を選択します。[カスタム信頼ポリシー] で、`"Principal": {},` を次のように置き換え、ログ配信サービスを指定します。[次へ] をクリックします。

```
"Principal": {
   "AWS": "arn:aws:iam::source-account:role/mySourceRole"
},
```

8. [Add permissions] (アクセス許可の追加) ページで、この手順で先ほど作成したポリシーの横にあるチェックボックスを選択し、[Next] (次へ) を選択します。
9. ロールの名前を入力し、オプションで説明を入力します。
10. [ロールの作成] を選択します。

Firehose に発行するフローログを作成する

コンソールを使用して Firehose に発行する Transit Gateway フローログを作成するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Transit Gateways]、[Transit Gateway アタッチメント] の順に選択します。
3. 1 つまたは複数の Transit Gateway または Transit Gateway アタッチメントのチェックボックスを選択します。
4. [アクション]、[フローログの作成] を選択します。

5. [送信先] には、[Firehose 配信システム] への送信を選択します。
6. [Firehose 配信ストリーム ARN] には、フローログの発行先として作成した配信ストリームの ARN を選択します。
7. [ログレコード形式] で、フローログレコードの形式を指定します。
   - デフォルトのフローログレコード形式を使用するには、[AWS のデフォルト形式] を選択します。
   - カスタム形式を作成するには、[カスタム形式] を選択します。[ログの形式] で、フローログレコードに含めるフィールドを選択します。
8. (オプション) フローログにタグを追加するには、[新しいタグを追加] を選択し、タグのキーと値を指定します。
9. [フローログの作成] を選択します。

コマンドラインツールを使用して Firehose に発行するフローログを作成するには

以下のいずれかのコマンドを使用します。

- create-flow-logs (AWS CLI)
- New-EC2FlowLogs (AWS Tools for Windows PowerShell)
- CreateFlowログ (Amazon EC2 クエリ API)

次の AWS CLI の例では、トランジットゲートウェイ情報をキャプチャし、フローログを指定された Firehose 配信ストリームに配信するフローログを作成します。

```
aws ec2 create-flow-logs \
                --resource-type TransitGateway \
                --resource-ids tgw-1a2b3c4d \
                --log-destination-type kinesis-data-firehose \
                --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream:flowlogs_stream
```

次の AWS CLI の例では、トランジットゲートウェイ情報をキャプチャし、フローログをソースアカウントとは異なる Firehose 配信ストリームに配信するフローログを作成します。

```
aws ec2 create-flow-logs  \
  --resource-type TransitGateway \
```

```
  --resource-ids gw-1a2b3c4d \
  --log-destination-type kinesis-data-firehose \
  --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream:flowlogs_stream \
  --deliver-logs-permission-arn arn:aws:iam::source-account:role/mySourceRole \
  --deliver-cross-account-role arn:aws:iam::destination-account:role/
AWSLogDeliveryFirehoseCrossAccountRole
```

Transit Gateway Flow Logs の操作

Amazon EC2、Amazon VPC、および Amazon S3 コンソールを使用して CloudWatch、Transit Gateway フローログを操作できます。 Amazon S3

タスク

- フローログの使用の管理
- フローログの作成
- フローログを表示する
- フローログのタグを追加または削除する
- フローログレコードを表示する
- フローログレコードの検索
- フローログの削除
- API と CLI の概要と制限事項

フローログの使用の管理

デフォルトでは、 ユーザーにはフローログを使用するためのアクセス許可がありません。フローログを作成、説明、削除するアクセス権限をユーザーに付与するユーザーポリシーを作成できます。詳細については、Amazon EC2 API リファレンスの「IAM ユーザーに対する Amazon EC2 リソースに対するアクセス許可の付与」を参照してください。

フローログを作成、説明、削除する完全なアクセス許可をユーザーに付与するポリシー例を次に示します。

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteFlowLogs",
        "ec2:CreateFlowLogs",
        "ec2:DescribeFlowLogs"
      ],
      "Resource": "*"
    }
  ]
}
```

CloudWatch Logs または Amazon S3 のどちらに発行するかに応じて、追加の IAM ロールとアクセス許可の設定が必要です。詳細については、「ログに発行するフロー CloudWatch ログを作成する」および「Amazon S3 に発行するフローログの作成」を参照してください。

フローログの作成

データを CloudWatch Logs、Amazon S3、または Firehose に発行できるトランジットゲートウェイのフローログを作成できます。

詳細については、次を参照してください。

- ログに発行するフロー CloudWatch ログを作成する
- Amazon S3 に発行するフローログの作成
- Firehose に発行するフローログを作成する

フローログを表示する

Amazon VPC コンソールでフローログに関する情報を表示するには、特定のリソースの [フローログ] タブを表示します。リソースを選択すると、そのリソースのすべてのフローログが表示されます。表示される情報には、フローログの ID、フローログの設定、およびフローログのステータスに関する情報が含まれます。

Transit Gateway のフローログに関する情報を表示するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Transit Gateways]、[Transit Gateway アタッチメント] の順に選択します。

3. Transit Gateway または Transit Gateway アタッチメントを選択し、[フローログの削除] を選択します。フローログに関する情報がタブに表示されます。[送信先タイプ] 列は、フローログを発行する送信先を示します。

フローログのタグを追加または削除する

Amazon EC2 および Amazon VPC コンソールで、フローログのタグを追加または削除できます。

Transit Gateway フローログのタグを追加または削除するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Transit Gateways]、[Transit Gateway アタッチメント] の順に選択します。
3. Transit Gateway または Transit Gateway アタッチメントを選択します。
4. 必要なフローログの [タグの管理] を選択します。
5. 新しいタグを追加するには、[タグの作成] を選択します。タグを削除するには、削除アイコンを選択します (x)。
6. [保存] を選択します。

フローログレコードを表示する

選択した送信先タイプに応じて、 CloudWatch ログコンソールまたは Amazon S3 コンソールを使用してフローログレコードを表示できます。フローログを作成してからコンソールに表示されるまでに、数分かかる場合があります。

CloudWatch Logs に発行されたフローログレコードを表示するには

1. https://console.aws.amazon.com/cloudwatch/ で CloudWatch コンソールを開きます。
2. ナビゲーションペインで、[ログ] を選択し、フローログを含むロググループを選択します。各 Transit Gateway のログストリームのリストが表示されます。
3. フローログレコードを表示する Transit Gateway の ID を含むログストリームを選択します。詳細については、「Transit Gateway Flow Log のレコード」を参照してください。

Amazon S3 に対して発行されたフローログレコードを表示するには

1. Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。

2. [バケット名] で、フローログを発行するバケットを選択します。
3. [名前] で、ログファイルの横にあるチェックボックスを選択します。オブジェクトの概要パネルで、[ダウンロード] を選択します。

フローログレコードの検索

Logs コンソールを使用して、 CloudWatch ログに発行されるフロー CloudWatch ログレコードを検索できます。メトリクスフィルターを使用すると、フローログレコードをフィルタリングできます。フローログレコードはスペースで区切られます。

Logs コンソールを使用してフロー CloudWatch ログレコードを検索するには

1. https://console.aws.amazon.com/cloudwatch/ で CloudWatch コンソールを開きます。
2. ナビゲーションペインで、[ログ]、[ロググループ] の順に選択します。
3. フローログを含むロググループを選択します。各 Transit Gateway のログストリームのリストが表示されます。
4. 検索する Transit Gateway がわかっている場合は、個々のログストリームを選択します。または、[ロググループの検索] を選択して、ロググループ全体を検索します。ロググループに多数の Transit Gateway がある場合、または選択した時間範囲によっては、この処理に時間がかかる場合があります。
5. [イベントをフィルター] で、次の文字列を入力します。これは、フローログレコードで デフォルトの形式が使用されていることを前提としています。

```
[version, resource_type, account_id,tgw_id, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr, dstaddr, srcport, dstport,
 protocol, packets, bytes,start,end, log_status, type,packets_lost_no_route,
 packets_lost_blackhole, packets_lost_mtu_exceeded, packets_lost_ttl_expired,
 tcp_flags,region, flow_direction, pkt_src_aws_service, pkt_dst_aws_service]
```

6. 必要に応じてフィールドの値を指定して、フィルターを変更します。次の例では、特定の送信元 IP アドレスでフィルタリングします。

```
[version, resource_type, account_id,tgw_id, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr= 10.0.0.1, dstaddr,
```

```
 srcport, dstport, protocol, packets, bytes,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
 packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
 pkt_dst_aws_service]
[version, resource_type, account_id,tgw_id, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr= 10.0.2.*, dstaddr,
 srcport, dstport, protocol, packets, bytes,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
 packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
 pkt_dst_aws_service]
```

次の例では、Transit Gateway ID tgw-123abc456bca、宛先ポート、およびバイト数でフィルタリングします。

```
[version, resource_type, account_id,tgw_id=tgw-123abc456bca, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr, dstaddr, srcport, dstport =
 80 || dstport = 8080, protocol, packets, bytes >= 500,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
 packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
 pkt_dst_aws_service]
```

フローログの削除

Amazon VPC コンソールを使用して Transit Gateway フローログを削除できます。

これらの手順では、リソースのフローログサービスが無効になります。フローログを削除しても、Amazon S3 の CloudWatch ログまたはログファイルから既存のログストリームは削除されません。既存のフローログデータは、それぞれのサービスのコンソールを使用して削除する必要があります。さらに、Amazon S3 に公開するフローログを削除しても、バケットポリシーとログファイルのアクセスコントロールリスト (ACL) は削除されません。

Transit Gateway のフローログを削除するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Transit Gateway] を選択します。
3. [Transit Gateway ID] を選択します。

4. [フローログ] セクションで、削除するフローログを選択します。
5. [アクション] を選択してから、[フローログの削除] を選択します。
6. [削除] を選択してフローを削除することを確認します。

API と CLI の概要と制限事項

このページで説明しているタスクは、コマンドラインまたは API を使用して実行できます。

`CreateFlowLogs` API または `create-flow-logs` CLI を使用する場合、次の制限が適用されます。

- `--resource-ids` の最大制約は、`TransitGateway` または `TransitGatewayAttachment` リソースタイプが 25 です。
- `--traffic-type` はデフォルトでは必須フィールドではありません。これを Transit Gateway リソースタイプに指定すると、エラーが返されます。この制限は Transit Gateway リソースタイプにのみ適用されます。
- `--max-aggregation-interval` には、`60` のデフォルトの値があります。これは、Transit Gateway リソースタイプで唯一受け入れられる値です。他の値を渡そうとすると、エラーが返されます。この制限は Transit Gateway リソースタイプにのみ適用されます。
- `--resource-type` で、`TransitGateway` と `TransitGatewayAttachment` の 2 つの新しいリソースタイプがサポートされています。
- 含めるフィールドを設定しない場合、`--log-format` には Transit Gateway リソースタイプのすべてのログフィールドが含まれます。これは、Transit Gateway リソースタイプにのみ適用されます。

フローログの作成

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)
- CreateFlowログ (Amazon EC2 クエリ API)

フローログの説明

- describe-flow-logs (AWS CLI)
- Get-EC2FlowLog (AWS Tools for Windows PowerShell)

- DescribeFlow口グ (Amazon EC2 クエリ API)

フローログレコード (ログイベント) の表示

- get-log-events (AWS CLI)
- Get-CWLLogEvent (AWS Tools for Windows PowerShell)
- GetLogイベント (CloudWatch API)

フローログの削除

- delete-flow-logs (AWS CLI)
- Remove-EC2FlowLog (AWS Tools for Windows PowerShell)
- DeleteFlow口グ (Amazon EC2 クエリ API)

Transit Gateway のモニタリング

Transit Gateway をモニタリングするには、次の機能を使用して、トラフィックパターンの分析や Transit Gateway のトラブルシューティングを行います。

CloudWatch メトリクス

Amazon CloudWatch を使用して、Transit Gateway のデータポイントに関する統計情報を、メトリクスと呼ばれる時系列データの時間順のセットとして取得できます。これらのメトリクスを使用して、システムが正常に実行されていることを確認できます。詳細については、「Transit Gateway 用の CloudWatch メトリクス」を参照してください。

Transit Gateway Flow Logs

Transit Gateway Flow Logs を使用して、Transit Gateway のネットワークトラフィックに関する詳細情報を取得できます。詳細については、「Transit Gateway Flow Logs 」を参照してください。

VPC Flow Logs

VPC Flow Logs を使用して、Transit Gateway にアタッチされている VPC の間で送受信されるトラフィックに関する詳細情報を取得できます。詳細については、アマゾン VPC ユーザーガイドの「VPC フローログを使用した IP トラフィックのログ記録」を参照してください。

CloudTrail ログ

AWS CloudTrailを使用して、 Transit Gateway API に対して行われた呼び出しに関する詳細情報をキャプチャし、Amazon S3 でログファイルとして保存できます。これらの CloudTrail ログを使用して、行われた呼び出し、呼び出し元のソース IP アドレス、呼び出し元、呼び出し時間などを判断できます。詳細については、「AWS CloudTrailを使用した転送ゲートウェイの API 呼び出しのログ記録。」を参照してください。

Network Manager を使用する CloudWatch イベント

AWS Network Manager を使用してイベントを CloudWatch に転送し、それらのイベントをターゲット関数またはストリームにルーティングできます。Network Manager は、トポロジーの変更、ルーティングの更新、ステータスの更新に関するイベントを生成します。これらはすべて、Transit Ggateway の変更を確認するために使用できます。詳細については、「AWS Global Networks for Transit Gateways ユーザーガイド」の「CloudWatch Events を使用してグローバルネットワークをモニタリングする」を参照してください。

Transit Gateway 用の CloudWatch メトリクス

アマゾン VPC は、Transit Gateway および Transit Gateway アタッチメントに関するデータポイントを Amazon CloudWatch に発行します。CloudWatch では、それらのデータポイントについての統計を、順序付けられた時系列データのセット (メトリクスと呼ばれる) として取得できます。メトリクスは監視対象の変数、データポイントは時間の経過と共に変わる変数の値と考えることができます。各データポイントには、タイムスタンプと、オプションの測定単位が関連付けられています。

メトリクスを使用して、システムが正常に実行されていることを確認できます。メトリクスを使用して、システムが正常に実行されていることを確認できます。例えば、指定のメトリクスを監視する CloudWatch アラームを作成し、メトリクスが許容範囲外になった場合にアクション (E メールアドレスに通知を送信するなど) を開始することができます。

アマゾン VPC が 60 秒間隔でメトリクスを測定し、CloudWatch に送信します。

詳細については、Amazon CloudWatch ユーザーガイドを参照してください。

目次

Transit Gateway メトリクス

AWS/TransitGateway 名前空間には、次のメトリクスが含まれます。

メトリクス	説明
BytesDropCountBlackhole	blackhole ルートと一致したためにドロップされたバイトの数。
BytesDropCountNoRoute	ルートと一致しなかったためにドロップされたバイトの数。
BytesIn	Transit Gateway あたりの受信バイト数。
BytesOut	Transit Gateway からの送信バイト数。
PacketsIn	Transit Gateway によって受信されたパケットの数。

メトリクス	説明
PacketsOut	Transit Gateway によって送信されたパケットの数。
PacketDropCountBlackhole	blackhole ルートと一致したためにドロップされたパケットの数。
PacketDropCountNoRoute	ルートと一致しなかったためにドロップされたパケットの数。

アタッチメントレベルのメトリクス

Transit Gateway アタッチメントでは、次のメトリクスを使用できます。すべてのアタッチメントメトリクスは、Transit Gateway 所有者のアカウントに発行されます。すべてのアタッチメントメトリクスは、 所有者のアカウントに公開されます。アタッチメントの所有者は、自分のアタッチメントのメトリクスのみを表示できます。サポートされているアタッチメントタイプの詳細については、「the section called “リソースアタッチメント”」を参照してください。

メトリクス	説明
BytesDropCountBlackhole	Transit Gateway アタッチメント上の blackhole ルートに一致したためにドロップされたバイトの数。
BytesDropCountNoRoute	Transit Gateway アタッチメント上のルートと一致しなかったためにドロップされたバイトの数。
BytesIn	Transit Gateway によってアタッチメントから受信されたバイト数。
BytesOut	Transit Gateway からアタッチメントに送信されたバイト数。
PacketsIn	Transit Gateway によってアタッチメントから受信されたパケット数。
PacketsOut	Transit Gateway によってアタッチメントに送信されたパケットの数。
PacketDropCountBlackhole	Transit Gateway アタッチメント上の blackhole ルートに一致したためにドロップされたパケットの数。

メトリクス	説明
PacketDropCountNoRoute	Transit Gateway アタッチメント上のルートと一致しなかったためにドロップされたパケットの数。

Transit Gateway のメトリクスディメンション

Transit Gateway のメトリクスをフィルタリングするには、次のディメンションを使用します。

ディメンション	説明
TransitGateway	Transit Gateway によってメトリクスデータをフィルタリングします。
TransitGatewayAttachment	Transit Gateway アタッチメントによってメトリクスデータをフィルタリングします。

AWS CloudTrailを使用した転送ゲートウェイの API 呼び出しのログ記録。

AWS CloudTrailは、ユーザーやロール、AWSサービスによって実行されたアクションを記録するサービスです。CloudTrail は、すべてのTransit Gateway API コールをイベントとしてキャプチャします。キャプチャされた呼び出しには、AWS Management Consoleからの呼び出しとTransit Gateway API オペレーションへのコード呼び出しが含まれます。証跡を作成すると、Transit Gateway のイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。証跡を設定しない場合でも、CloudTrail コンソールの [イベント履歴] で最新のイベントを表示できます。CloudTrail で収集された情報を使用して、Transit Gateway API に対するリクエスト、リクエスト元の IP アドレス、リクエストの実行者、リクエスト日時などの詳細を確認できます。

Transit Gateway API の詳細については、「Amazon EC2 API リファレンス」の「AWS Transit Gateway アクション」を参照してください。

CloudTrail の詳細については、AWS CloudTrail ユーザーガイドを参照してください。

CloudTrail のTransit Gateway 情報

CloudTrail は、アカウントを作成すると AWS アカウントで有効になります。Transit Gateway API を経由してアクティビティが発生すると、そのアクティビティはイベント履歴のAWSの他のサービスのイベントとともに CloudTrail イベントに記録されます。最近のイベントは、AWS アカウントで表示、検索、ダウンロードできます。詳細については、「CloudTrail イベント履歴でのイベントの表示」を参照してください。

Transit Gateway API のイベントなど、 AWSアカウントのイベントの継続的な記録については、証跡を作成します。証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで追跡を作成するときに、追跡がすべての リージョンに適用されます。追跡は、AWSパーティションのすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集したイベントデータをより詳細に分析し、それに基づく対応するためにその他の AWS のサービスを設定できます。詳細については、次を参照してください。

- 追跡を作成するための概要
- CloudTrail のサポート対象サービスと統合
- Amazon SNS の CloudTrail の通知の設定
- 複数のリージョンから CloudTrail ログファイルを受け取る、および複数のアカウントから CloudTrail ログファイルを受け取る

Transit Gateway アクションへのすべての呼び出しが CloudTrail により ログに記録されます。たとえば、`CreateTransitGateway` アクションを呼び出すと、CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。同一性情報は次の判断に役立ちます。

- リクエストが、ルートと AWS Identity and Access Management ユーザー認証情報のどちらを使用して送信されたか。
- リクエストがロールまたはフェデレーションユーザーの一時的なセキュリティ認証情報を使用して行われたかどうか。
- リクエストが、別の AWS のサービスによって送信されたかどうか。

詳細については、「CloudTrail userIdentity エレメント」を参照してください。

Transit Gateway のログファイルエントリを理解する

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルには、単一か複数のログエントリがあります。イベントはあらゆるソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストのパラメータなどの情報が含まれます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

このログファイルには、Transit Gateway API 呼び出しだけでなく、ご使用のAWSアカウントのすべての API 呼び出しに関するイベントが含まれます。`eventSource` の値を使用して `ec2.amazonaws.com` 要素を確認することで、Transit Gateway API に対する呼び出しを見つけることができます。`CreateTransitGateway` などの特定のアクションのレコードを表示するには、アクション名で `eventName` 要素を確認します。

次の例は、コンソールを使用して Transit Gateway を作成したユーザーのTransit Gateway API に関する、CloudTrail ログレコードを示しています。`userAgent` 要素を使用してコンソールを特定できます。`eventName` 要素を使用して、リクエストされた API コールを特定できます。ユーザーに関する情報 (`Alice`) は `userIdentity` 要素で確認できます。

Example 例 : 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"
}
```

Transit Gateway の ID およびアクセス管理

AWS ではセキュリティ認証情報を使用して、ユーザーを識別し、AWS リソースへのアクセスを付与します。AWS Identity and Access Management (IAM)の機能を使用して、他のユーザー、サービス、およびアプリケーションが完全にまたは制限付きでお客様の AWS リソースを使用できるようにします。その際、お客様のセキュリティ認証情報は共有されません。

デフォルトでは、IAM ユーザーには、AWSリソースを作成、表示、変更するためのアクセス許可はありません。ユーザーが Transit Gateway などのリソースにアクセスして、タスクを実行できるようにするには、特定のリソースや必要となる API アクションを使用するための許可をユーザーに付与する IAM ポリシーを作成してから、そのポリシーをそのユーザーが属するグループにアタッチする必要があります。ポリシーをユーザーまたはユーザーのグループにアタッチする場合、ポリシーによって特定リソースの特定タスクを実行するユーザーの権限が許可または拒否されます。

Transit Gateway を使用するには、以下のAWS管理ポリシーのいずれかがニーズを満たす場合があります。

- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess
- PowerUserAccess
- ReadOnlyAccess

Transit Gateway を管理するためのポリシー例

以下は Transit Gateway を使用するための IAM ポリシーの例です。

必要なタグを持つ Transit Gateway を作成する

以下の例で、ユーザーは Transit Gateway を作成できるようになります。`aws:RequestTag` 条件キーでは、ユーザーは Transit Gateway をタグ `stack=prod` にタグ付けすることが求められます。`aws:TagKeys` 条件キーは、`ForAllValues` 修飾子を使用し、キー `stack` のみがリクエストで許可されることを指定します (他のタグは指定できません)。ユーザーが Transit Gateway の作成時にこの指定のタグを渡さない場合、またはタグを指定しない場合、リクエストは却下されます。

2 番目のステートメントは、`ec2:CreateAction` 条件キーを使用して、ユーザーが `CreateTransitGateway` のコンテキストでみタグを使用できるようにします。

```
{
    "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"
                }
            }
        }
    ]
}
```

Transit Gateway ルートテーブルの操作

以下の例では、ユーザーが特定の Transit Gateway のみ（`tgw-11223344556677889`）に対して Transit Gateway ルートテーブルを作成および削除できるようにします。ユーザーは、任意の Transit Gateway のルートテーブルでルートの作成や置き換えができますが、タグ `network=new-york-office` の付いたアタッチメントに対してのみ可能です。

```
{
```

```
    "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/*"
        }
    ]
}
```

AWS Network Manager を管理するポリシーの例

ポリシーの例については、「AWS Global Networks for Transit Gateways User Guide」の「Example policies to manage Network Manager」を参照してください。

Transit Gateway サービスにリンクされたロール

Amazon VPC は、ユーザーに代わって他のAWSサービスを呼び出すために必要なアクセス許可のために、サービスにリンクされたロールを使用します。詳細については、IAM ユーザーガイドの「サービスにリンクされたロールの使用」を参照してください。

Transit Gateway サービスにリンクされたロール

Amazon VPC は、他のを呼び出すために必要なアクセス許可を持つ、サービスにリンクされたロールを使用します。AWSサービスは、Transit Gateway を操作するときにユーザーに代わって提供されます。

サービスにリンクされたロールによって付与されるアクセス許可

Amazon VPC は、Transit Gateway を使用するときに、AWSServiceRoleForVPCTransitGateway という名前のサービスにリンクされたロールを使用して、ユーザーに代わって次のアクションを呼び出します。

- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:DeleteNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`
- `ec2:AssignIpv6Addresses`
- `ec2:UnAssignIpv6Addresses`

AWSServiceRoleForVPCTransitGateway ロールでは、以下のサービスを信頼してロールを引き受けます。

- `transitgateway.amazonaws.com`

AWSServiceRoleForVPCTransitGateway はマネージドポリシー AWSVPCTransitGatewayServiceRolePolicy を使用します。

サービスにリンクされたロールの作成、編集、削除をIAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、許可を設定する必要があります。詳細については、「IAM User

Guide」(IAM ユーザーガイド) の「Service-linked role permissions」(サービスにリンクされたロールのアクセス権限) を参照してください。

サービスにリンクされたロールの作成

AWSServiceRoleForVPCTransitGateway ロールを手動で作成する必要はありません。このロールは、アカウント内の VPC を Transit Gateway にアタッチするときに、Amazon VPC によって作成されます。

Amazon VPC がお客様に代わってサービスにリンクされたロールを作成するには、必要なアクセス許可がお客様に付与されていなければなりません。詳細については、IAM ユーザーガイド の「サービスにリンクされたロールのアクセス許可」を参照してください。

サービスにリンクされたロールを編集する

IAM を使用して、AWSServiceRoleForVPCTransitGateway の説明を編集できます。詳細については、IAM ユーザーガイドの「サービスにリンクされたロールの編集」を参照してください。

サービスにリンクされたロールを削除する

Transit Gateway を使用する必要がなくなった場合は、AWSServiceRoleForVPCTransitGateway を削除することをお勧めします。

このサービスにリンクされたロールを削除するには、AWSアカウントの Transit Gateway VPC アタッチメントをすべて削除する必要があります。これにより、VPC アタッチメントへのアクセス許可を誤って削除することがなくなります。

サービスにリンクされたロールは、IAM コンソール、IAM CLI、または IAM API を使用して削除することができます。詳細については、IAM ユーザーガイド の「サービスにリンクされたロールの削除」を参照してください。

AWSServiceRoleForVPCTransitGateway を削除すると、アカウントの VPC を Transit Gateway にアタッチするときに、Amazon VPC によってロールがもう一度作成されます。

Transit Gateway の AWS マネージドポリシー

AWS マネージドポリシーは、AWS が作成および管理するスタンドアロンポリシーです。AWS マネージドポリシーは、多くの一般的なユースケースでアクセス許可を提供できるように設計されているため、ユーザー、グループ、ロールへのアクセス許可の割り当てを開始できます。

AWS マネージドポリシーは、ご利用の特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることにご注意ください。AWS のすべてのお客様が使用できるようになるのを避けるためです。ユースケース別にカスタマー管理ポリシーを定義することで、アクセス許可を絞り込むことをお勧めします。

AWS 管理ポリシーで定義したアクセス権限は変更できません。AWS が AWS マネージドポリシーに定義されているアクセス許可を更新すると、更新はポリシーがアタッチされているすべてのプリンシパルアイデンティティ (ユーザー、グループ、ロール) に影響します。新しい AWS のサービスを起動するか、既存のサービスで新しい API オペレーションが使用可能になると、AWS が AWS マネージドポリシーを更新する可能性が最も高くなります。

詳細については、「IAM ユーザーガイド」の「AWS 管理ポリシー」を参照してください。

Transit Gateway を使用するには、以下のAWS管理ポリシーのいずれかがニーズを満たす場合があります。

- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess
- PowerUserAccess
- ReadOnlyAccess

AWS マネージドポリシー: AWSVPCTransitGatewayServiceRolePolicy

このポリシーはロール AWSServiceRoleForVPCTransitGateway にアタッチされます。これにより、Amazon VPC は Transit Gateway アタッチメント用のリソースを作成および管理できます。

このポリシーに対する許可を確認するには、「AWS マネージドポリシーリファレンス」の「AWSVPCTransitGatewayServiceRolePolicy」を参照してください。

AWS 管理ポリシーに対する Transit Gateway の更新

Transit Gateway の AWS 管理ポリシーに対する更新の詳細について、Amazon VPC がこれらの変更の追跡を開始した 2021 年 3 月以降のものを表示します。

変更	説明	日付
Amazon VPC が変更の追跡をスタートしました	Amazon VPC が AWS 管理ポリシーの変更の追跡を開始しました。	2021 年 3 月 1 日

ネットワーク ACL とトランジットゲートウェイの動作

ネットワークアクセスコントロールリスト (NACL) は、オプションのセキュリティレイヤーです。

ネットワークアクセスコントロールリスト (NACL) のルールは、シナリオに応じて異なる方法で適用されます。

- the section called “EC2 インスタンスおよび Transit Gateway の関連付け用の同じサブネット”
- the section called “EC2 インスタンスと Transit Gateway の関連付け用の異なるサブネット”

EC2 インスタンスおよび Transit Gateway の関連付け用の同じサブネット

同じサブネット内に、EC2 インスタンスと Transit Gateway の関連付けがある設定について考えてみます。EC2 インスタンスから Transit Gateway へのトラフィックと、Transit Gateway からインスタンスへのトラフィックの両方に、同じネットワーク ACL が使用されます。

インスタンスから Transit Gateway へのトラフィックに対して、次のように NACL ルールが適用されています。

- アウトバウンドルールでは、評価に送信先 IP アドレスを使用します。
- インバウンドルールでは、評価に送信元 IP アドレスを使用します。

Transit Gateway からインスタンスへのトラフィックに対して、次のように NACL ルールが適用されています。

- アウトバウンドルールは評価されません。
- インバウンドルールは評価されません。

EC2 インスタンスと Transit Gateway の関連付け用の異なるサブネット

あるサブネットに EC2 インスタンスがあり、別のサブネットに Transit Gateway の関連付けがあり、各サブネットが異なるネットワーク ACL に関連付けられている設定について考えてみましょう。

EC2 インスタンスのサブネットに対して、次のようにネットワーク ACL ルールが適用されています。

- アウトバウンドルールでは、送信先 IP アドレスを使用して、インスタンスから Transit Gateway へのトラフィックを評価します。
- インバウンドルールでは、送信元 IP アドレスを使用して、Transit Gateway からインスタンスへのトラフィックを評価します。

Transit Gateway のサブネットに対して、次のように NACL ルールが適用されています。

- アウトバウンドルールでは、送信先 IP アドレスを使用して、Transit Gateway からインスタンスへのトラフィックを評価します。
- アウトバウンドルールは、インスタンスから Transit Gateway へのトラフィックの評価には使用されません。
- インバウンドルールでは、送信元 IP アドレスを使用して、インスタンスから Transit Gateway へのトラフィックを評価します。
- インバウンドルールは、Transit Gateway からインスタンスへのトラフィックの評価には使用されません。

ベストプラクティス

各 Transit Gateway VPC アタッチメントに個別のサブネットを使用します。各サブネットに対して、小さな CIDR (/28 など) を使用して、EC2 リソースのアドレスが増えるようにします。別のサブネットを使用する場合は、次の項目を設定できます。

- Transit Gateway サブネットに関連付けられているインバウンドおよびアウトバウンド NACL を開いたままにします。
- トラフィックフローに応じて、ワークロードサブネットに NACL を適用できます。

VPC アタッチメントの仕組みについての詳細は、「the section called “リソースアタッチメント”」を参照してください。

Transit Gateway のクォータ

AWS アカウント トランジットゲートウェイに関連する次のクォータ (以前は制限と呼ばれていました) があります。特に明記されていない限り、クォータは地域固有です。

Service Quotas コンソールには、アカウントのクォータに関する情報が表示されます。Service Quotas コンソールを使用して、デフォルトのサービスクォータを表示したり、調整可能なクォータのクォータの引き上げをリクエストしたりすることができます。詳細については、「Service Quotas ユーザーガイド」の「クォータ引き上げのリクエスト」を参照してください。

調整可能なクォータが Service Quotas でまだ使用できる状態になっていない場合は、サポートケースを開くことができます。

全般

名前	デフォルト	引き上げ可能
アカウントあたりの Transit Gateway	5	はい
Transit Gateway あたりの CIDR ブロック	5	いいえ

the section called “Connect アタッチメントおよび Connect ピア” 機能では、CIDR ブロックが使用されます。

ルーティング

名前	デフォルト	引き上げ可能
Transit Gateway あたりの Transit Gateway ルートテーブル	20	はい
1 つの Transit Gateway のすべてのルートテーブルにわたるすべてのルート (動的ルートと静的ルート) の合計数	10,000	はい

名前	デフォルト	引き上げ可能
仮想ルーターアプライアンスから Connect ピアにアドバタイズされるダイナミックルート	1,000	はい
Transit Gateway 上の Connect ピアから仮想ルーターアプライアンスへのアドバタイズされたルート	5,000	いいえ
単一のアタッチメントへのプレフィックスの静的ルートの数	1	いいえ

アドバタイズされたルートは、接続 アタッチメントに関連付けられているルートテーブルから取得されます。

Transit Gateway アタッチメント

Transit Gateway は、同じ VPC に対して複数のアタッチメントを持つことはできません。

名前	デフォルト	引き上げ可能
Transit Gateway あたりのアタッチメント	5,000	[いいえ]
VPC あたりの Transit Gateway	5	いいえ
Transit Gateway あたりのピアアタッチメント	50	はい
Transit Gateway あたりの保留中のピアリングアタッチメント	10	はい
2 つのトランジットゲートウェイ間、または 1 つのトランジットゲートウェイと Cloud WAN コアネットワークエッジ (CNE) 間のピアリングアタッチメント	1	[いいえ]
Connect アタッチメントあたりの Connect ピア (GRE トンネル)	4	[いいえ]

[帯域幅]

Site-to-Site VPN 接続を通じて実現される帯域幅に影響を与える要因には、パケットサイズ、トラフィックミックス (TCP/UDP)、中間ネットワークのシェーピングまたはスロットリングポリシー、インターネットの状況、特定のアプリケーション要件を始めとして多くのものがあります。VPC アタッチメントの場合、 AWS Direct Connect ゲートウェイ、またはピアリングされた Transit Gateway アタッチメントは、デフォルト値を超える帯域幅を提供するよう試みます。

名前	デフォルト	引き上げ可能
アベイラビリティーゾーンごとの VPC アタッチメントあたりの帯域幅	最大 100 Gbps	詳細については、ソリューションアーキテクト (SA) またはテクニカルアカウントマネージャー (TAM) にお問い合わせください。
アベイラビリティーゾーンごとの Transit Gateway VPC アタッチメントあたりのパケット/秒	最大 7,500,000	詳細については、ソリューションアーキテクト (SA) またはテクニカルアカウントマネージャー (TAM) にお問い合わせください。
リージョン内の利用可能なアベイラビリティーゾーンごとのゲートウェイ接続またはピアリングされたトランジットゲートウェイ接続の帯域幅 AWS Direct Connect	最大 100 Gbps	詳細については、ソリューションアーキテクト (SA) またはテクニカルアカウントマネージャー (TAM) にお問い合わせください。
リージョン内の利用可能なアベイラビリティーゾーンごとのトランジットゲートウェイアタッチメント (AWS Direct Connect およびピアリ	最大 7,500,000	詳細については、ソリューションアーキテクト (SA) またはテクニカルアカウント

名前	デフォルト	引き上げ可能
ングアタッチメント) あたりの 1 秒あたりのパケット数		マネージャー (TAM) にお問い合わせください。
VPN トンネルごとの最大帯域幅	最大 1.25 Gbps	いいえ
VPN トンネルあたりの最大パケット/秒	最大 140,000	[いいえ]
Connect アタッチメントごとの Connect ピア (GRE トンネル) あたりの最大帯域幅	最大 5 Gbps	いいえ
Connect ピアあたりの 1 秒あたりの最大パケット数	最大 300,000	いいえ

ECMP を使用すると、複数の VPN トンネルを集約して、より高い VPN 帯域幅を確保できます。ECMP を使用するには、VPN 接続を動的ルーティング用に設定する必要があります。ECMP は、静的ルーティングを使用する VPN 接続ではサポートされません。

基盤となるトランスポート (VPC または) アタッチメントが必要な帯域幅をサポートしている限り、Connect アタッチメントごとに最大 4 つの Connect ピアを作成できます (Connect アタッチメントあたりの合計帯域幅は最大 20 Gbps AWS Direct Connect)。同じ転送ゲートウェイで同じ Connect アタッチメントの複数の Connect ピア全体、または複数の Connect アタッチメント全体で水平にスケーリングすることによって、より大きな帯域幅を得るために ECMP を使用することができます。Transit Gateway は、同じ Connect Peer の BGP ピア接続間で ECMP を使用することはできません。

AWS Direct Connect ゲートウェイ

名前	デフォルト	引き上げ可能
AWS Direct Connect トランジットゲートウェイあたりのゲートウェイ	20	[いいえ]
ゲートウェイあたりのトランジットゲートウェイ AWS Direct Connect	6	[いいえ]

最大送信単位 (MTU)

- ネットワーク接続の MTU は、その接続を通過できる最大許容パケットのサイズ (バイト単位) です。接続の MTU が大きいほど、より多くのデータを単一のパケットで渡すことができます。Transit Gateway は、VPC、トランジットゲートウェイConnect AWS Direct Connect、およびピアリングアタッチメント間のトラフィックで 8500 バイトの MTU をサポートします。VPN 接続を介したトラフィックは、1500 バイトの MTU を持つことができます。
- VPC ピアリングから Transit Gateway の使用に移行する場合、VPC ピアリングと Transit Gateway 間の MTU サイズの不一致により、非対称トラフィックのパケットがドロップされる可能性があります。サイズの不一致によりジャンボパケットがドロップされないように、両方の VPC を同時に更新します。
- Transit Gateway に到達したサイズが 8500 バイトを超えるパケットはドロップされます。
- Transit Gateway は、ICMPv4 パケットの場合は FRAG_NEEDED、ICMPv6 パケットの場合は Packet Too Big (PTB) を生成しません。したがって、パス MTU 検出 (PMTUD) はサポートされていません。
- Transit Gateway は、すべてのパケットに対して最大セグメントサイズ (MSS) クランプを適用します。詳細については、「RFC879」を参照してください。
- MTU のSite-to-Site VPN クォータの詳細については、AWS Site-to-Site VPN ユーザガイドの「最大送信単位 (MTU)」を参照してください。

マルチキャスト

名前	デフォルト	引き上げ可能
Transit Gateway あたりのマルチキャストドメイン	20	はい
Transit Gateway あたりのマルチキャストネットワークインターフェイス	10,000	はい
VPC あたりのマルチキャストドメインの関連付け	20	はい
Transit Gateway マルチキャストグループあたりの送信元	1	はい

名前	デフォルト	引き上げ可能
Transit Gateway あたりの静的マルチキャストグループおよび IGMPv2 マルチキャストグループのメンバーおよび送信元の数	10,000	いいえ
Transit Gateway マルチキャストグループあたりの静的マルチキャストグループおよび IGMPv2 マルチキャストグループのメンバーの数	100	いいえ
フローあたりの最大マルチキャストスループット	1 Gbps	いいえ
アベイラビリティーゾーンあたりの最大集約マルチキャストスループット	20 Gbps	[いいえ]

AWS ネットワークマネージャー

名前	デフォルト	引き上げ可能
グローバルネットワーク、ピア AWS アカウント	5	はい
グローバルネットワークあたりのデバイス数	200	はい
グローバルネットワークあたりのリンク数	200	はい
グローバルネットワークあたりのサイト数	200	はい
グローバルネットワークあたりの接続数	500	いいえ

その他のクォータリソース

詳細については、以下を参照してください。

- AWS Site-to-Site VPN ユーザーガイド の Site-to-Site VPN のクォータ

- Amazon VPC ユーザーガイドの Amazon VPC クォータ
- AWS Direct Connect ユーザーガイド の AWS Direct Connect クォータ

Transit Gateway のドキュメント履歴

次の表は、Transit Gateway の各リリースの説明です。

変更	説明	日付
AWS Transit Gateway のクォータ	帯域幅の制限が追加されました。	2023 年 8 月 14 日
AWS Transit Gateway Flow Logs	Transit Gateway Flow Logs が Transit Gateway でサポートされるようになり、Transit Gateway 間のネットワークトラフィックをモニタリングしログ記録できるようになりました。	2022 年 7 月 14 日
Transit Gateway ポリシーテーブル	ポリシーテーブルを使用して、Transit Gateway 用の動的ルーティングを設定し、ルーティングおよび到達可能性の情報をピアリングされた Transit Gateway と自動的に交換できるようにします。	2022 年 7 月 13 日
Network Manager ユーザーガイド	Network Manager のガイドは単体のものが作成されたため、「AWS Transit Gateway ユーザーガイド」には含まれなくなりました。	2021 年 12 月 2 日
添付のピアリング	同じリージョンの Transit Gateway と、ピアリング接続を構築することが可能です。	2021 年 12 月 1 日
Transit Gateway 接続	Transit Gateway と VPC で実行されているサードパー	2020 年 12 月 10 日

	ティー仮想アプライアンスの間の接続を確立できます。	
アプライアンスモード	VPC アタッチメントでアプライアンスモードを有効にして、双方向トラフィックがアタッチメントの同じアベイラビリティーゾーンを通過するようにできます。	2020 年 10 月 29 日
プレフィックスリスト参照	Transit Gateway ルートテーブルでプレフィックスリストを参照できます。	2020 年 8 月 24 日
Transit Gateway の変更	Transit Gateway の設定オプションを変更できます。	2020 年 8 月 24 日
Transit Gateway アタッチメント用の CloudWatch メトリクス	個々の Transit Gateway アタッチメントの CloudWatch メトリクスを表示できます。	2020 年 7 月 6 日
Network Manager ルートアナライザー	グローバルネットワーク内のトランジットゲートウェイルートテーブルのルートを分析できます。	2020 年 5 月 4 日
添付のピアリング	別のリージョンの Transit Gateway と、ピアリング接続を構築することが可能です。	2019 年 12 月 3 日
マルチキャストサポート	Transit Gateway は、接続された VPC のサブネット間のマルチキャストトラフィックのルーティングをサポートし、複数の受信インスタンス宛てのトラフィックを送信するインスタンスのマルチキャストルーターとして機能します。	2019 年 12 月 3 日

AWS Network Manager	Transit Gateway を中心に構築されたグローバルネットワークの視覚化およびモニタリングができます。	2019 年 12 月 3 日
AWS Direct Connect のサポート	トランジット仮想インターフェイス経由で Transit Gateway にアタッチした VPC または VPN に AWS Direct Connect 接続をつなげるには、AWS Direct Connect ゲートウェイを使用します。	2019 年 3 月 27 日
初回リリース	このリリースでは、Transit Gateway が導入されました。	2018 年 11 月 26 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。