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

Amazon VPC の AWS Transit Gateway とは

AWS Transit Gateway は、仮想プライベートクラウド (VPCs) 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されるネットワークトランジットハブです。クラウドインフラストラクチャがグローバルに拡大するにつれて、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を使用してトランジットゲートウェイを接続します。 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 のウェブサイト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
  - 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
  - トランジットゲートウェイへの VPN コンセントレータ
  - トランジットゲートウェイへのクライアント VPN エンドポイント
  - ネットワーク関数アタッチメント。詳細については、「the section called “ネットワーク関数アタッチメント”」を参照してください。
- 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。トランジットゲートウェイは、VPCs、、Transit Gateway Connect Direct Connect、ピアリングアタッチメント (リージョン内、リージョン間、および Cloud WAN 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。
- 暗号化制御 — トランジットゲートウェイは、トランジットゲートウェイにアタッチされた VPCs 上のすべてのトラフィックに対してencryption-in-transitを適用する暗号化制御をサポートするように設定できます。暗号化コントロールを有効にすると、暗号化コントロールが適用された状態で

トランジットゲートウェイを VPCs にアタッチできます。この機能により、トランジットゲートウェイを通過するすべてのトラフィックが暗号化され、ネットワーク通信のセキュリティが強化されます。

- 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
- Transit Gateway を開始する
- 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 マネジメントコンソール — 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) — Amazon VPC を含む幅広い AWS サービスのコマンドを提供し、Windows、macOS、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。
- AWS SDKs — 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の処理、エラーの処理など、接続の詳細の多くを処理します。詳細については、AWS SDK 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、Amazon 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。デフォルトでは、データ処理料金はソースアタッチメントを所有するアカウントに割り当てられます。柔軟なコスト配分を使用して、組織のニーズに基づいてこれらの料金を割り当てる方法をカスタマイズできます。詳細については、AWS 「Transit Gateway の料金」および「」を参照してください柔軟なコスト配分。

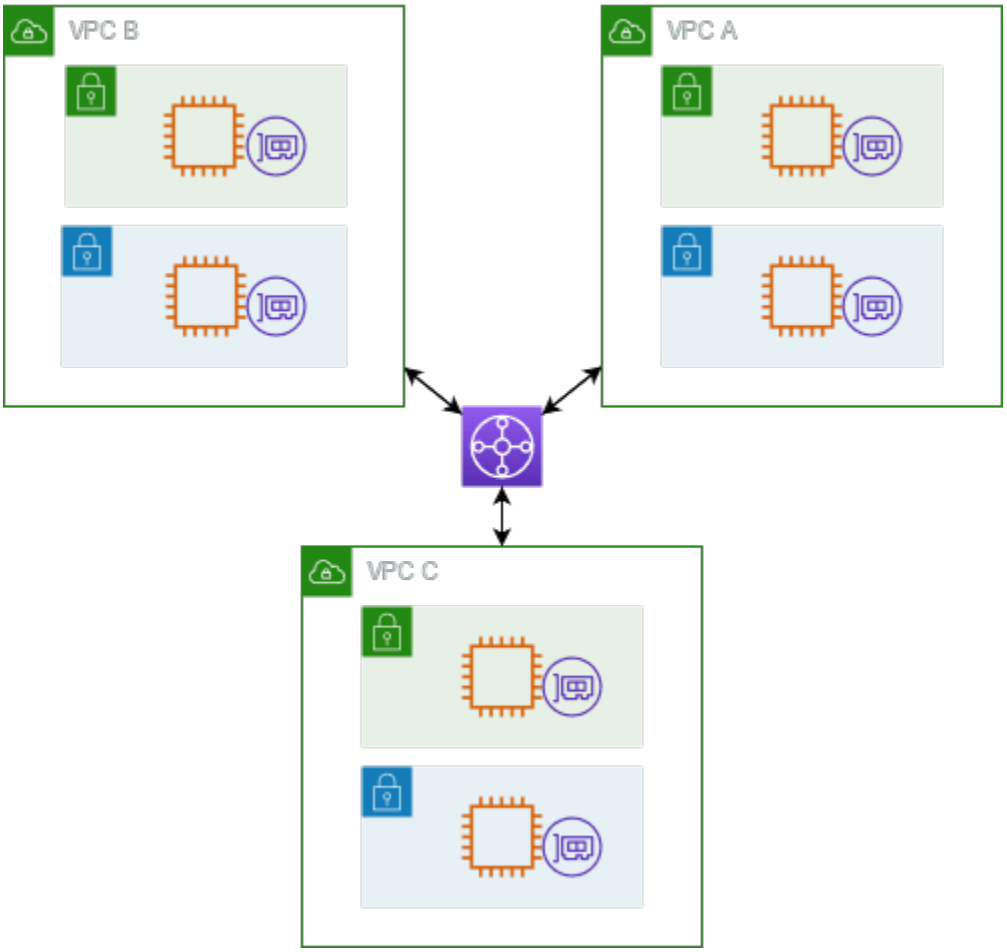
AWS Transit Gateway の仕組み

AWS Transit Gateway では、トランジットゲートウェイは、仮想プライベートクラウド (VPCs) とオンプレミスネットワーク間を流れるトラフィック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。

トピック

アーキテクチャ図の例

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。

ルーティング先	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 をデプロイします。これは、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 Transit Gateway によって使用されます。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 VPN コンセントレータ
- 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

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、プレフィックス長、AS_PATH が完全に同じ場合、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。
- VPN コンセントレータ - VPN コンセントレータは ECMP をサポートしていません。

> **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。サブネットを指定して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だけでなく、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。

ルーティングトピック

- ルートテーブル
- ルートテーブルの関連付け
- ルート伝達
- ピアリングアタッチメントのルート
- ルートの評価順序

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。ルート伝達とルートテーブルの関連付けの両方を無効にすると、 AWS は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を作成しません。ただし、ルート伝達またはルートテーブルの関連付けのいずれかが有効になっている場合、 AWS はデフォルトのルートテーブルを作成します。

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。

動的ルーティングを VPN アタッチメント、VPN コンセントレータアタッチメント、または Direct Connect ゲートウェイアタッチメントで使用すると、オンプレミスルーターから学習したルートを BGP 経由でトランジットゲートウェイルートテーブルに伝達できます。

VPN アタッチメントまたは VPN コンセントレータアタッチメントで動的ルーティングを使用する場合、VPN アタッチメントまたは VPN コンセントレータ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、許可されるプレフィックスインタラクションは、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 ゲートウェイが伝播したルート
  - Transit Gateway Connect が伝播したルート
  - プライベート Direct Connect 伝播ルート経由の Site-to-Site VPN
  - Site-to-Site VPN 伝播ルート
  - Site-to-Site VPN-Concentrator 伝達ルート
  - クライアント VPN 伝播ルート
  - 伝播ルートをピアリングする Transit Gateway (クラウド WAN)

一部のアタッチメントは、BGP 経由でルートアドバタイズをサポートしています。同じ CIDR を持つルートと、同じ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 BGP 属性によって制御されます。

- AS パスの長さがより短い
- MED 値がより低い
- アタッチメントがサポートしている場合は、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付け順序を保証できません。
> - MED を使用しない Transit Gateway にアドバタイズされたルートの場合、 AWS Transit Gateway は次のデフォルト値を割り当てます。
>   - Direct Connect アタッチメントでアドバタイズされるインバウンドルートの場合は 0。
>   - VPN および Connect アタッチメントでアドバタイズされるインバウンドルートの場合は 100。

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、以前にアクティブなルートがアドバタイズされなくなった場合にのみトランジットゲートウェイルートテーブルに表示されます。たとえば、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 Transit Gateway 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 Transit Gateway 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。

VPC のルートテーブルの例を次に示します。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

送信先	ターゲット	優先度
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

Transit Gateway のルートテーブルの例を次に示します。VPN アタッチメントよりも 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	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

ネットワーク関数アタッチメント

ネットワーク関数アタッチメントは、 AWS Network Firewall アタッチメントなどのネットワークセキュリティ関数をトランジットゲートウェイに直接接続するリソースです。これにより、検査 VPC を手動で作成および管理する必要がなくなります。

ネットワーク関数アタッチメントの場合:

- AWS は基盤となるインフラストラクチャを自動的に作成および管理します
- Transit Gateway を通過するトラフィックを検査できます
- セキュリティポリシーはネットワーク全体に一貫して適用されます

- シンプルルーティングルールを使用して、ファイアウォール経由でトラフィックをルーティングできます
- アタッチメントは複数のアベイラビリティーゾーンで動作し、高可用性を実現します

この統合により、複雑なルーティング設定を作成したり、別々の VPC を介して個別のエンドポイントを管理したりすることなく、ファイアウォールを Transit Gateway に直接接続できるようになり、ネットワークセキュリティが簡素化されます。

AWS Network Firewall 統合

AWS Network Firewall 統合により、サービスマネージドバッファ VPC 内のアベイラビリティーゾーンごとに 1 つずつ、Gateway Load Balancer Endpoints のグループの形式でファイアウォールを接続できます。Network Firewall アタッチメントは、アプライアンスモードが自動的に有効化された状態で作成されます。これにより、検査 VPC を明示的に管理する必要がなくなります。

Network Firewall 統合を使用すると、Network Firewall デプロイの検査 VPC を作成および管理する必要がなくなります。ファイアウォールの作成時に VPC とサブネットを選択する代わりに、Transit Gateway を直接選択すると、 AWS は背後で必要なすべてのリソースを自動的にプロビジョニングおよび管理します。個々のファイアウォールエンドポイントではなく、新しい Transit Gateway ネットワーク関数アタッチメントが表示されます。

クロスアカウントシナリオの場合、Transit Gateway は Transit Gateway 所有者から Network Firewall 所有者アカウントに RAM 共有でき、どちらのアカウントでもファイアウォールアタッチメントを管理できます。ファイアウォールとアタッチメントの準備が整い次第、Transit Gateway ルートテーブルを変更して、検査のためにトラフィックをアタッチメントに送信できます。

> **Note**
>
> - Transit Gateway は、Network Firewall アタッチメントの静的ルーティングのみをサポートします。
> - サードパーティーのファイアウォールはサポートされていません。

ファイアウォールとアタッチメントの詳細については、「Transit Gateway ネットワーク関数のアタッチメント」を参照してください。

トランジットゲートウェイシナリオの例

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。

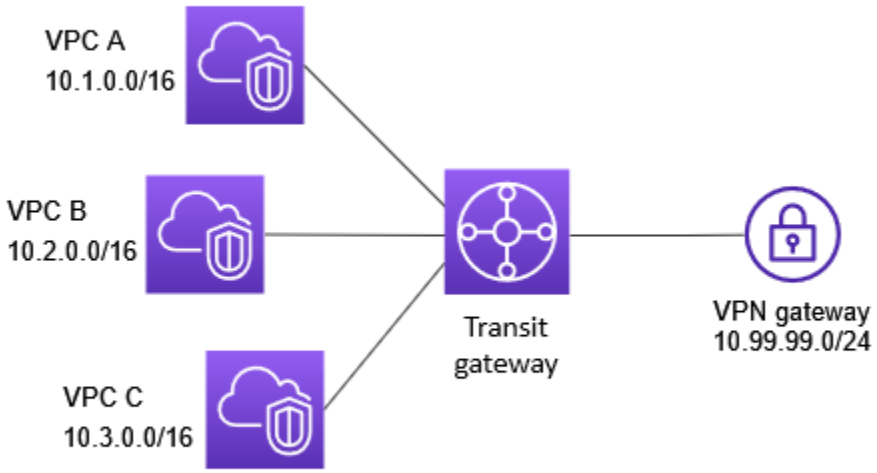
例: 集中型ルーター

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。

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。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。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。
- Transit Gateway。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 アタッチメントを作成する”」を参照してください。
- トランジットゲートウェイ上の 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。

  「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

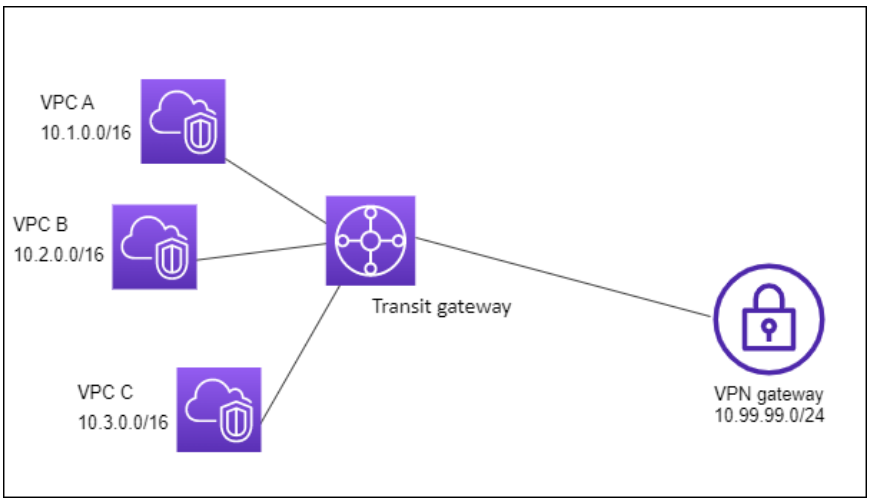
例: 隔離された VPC

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。

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。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。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。
- Transit Gateway。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 アタッチメントを作成する”」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。「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
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、「AWS Transit Gateway で Transit Gateway ルートテーブルへのルート伝達を有効にする」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

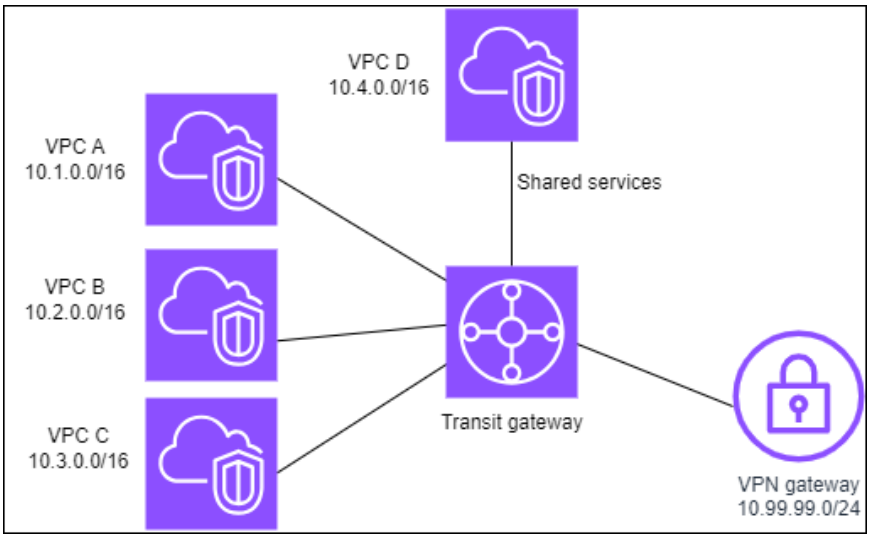
共有サービスを使用する複数の分離されたルーターとしてトランジットゲートウェイを設定できます。これは複数のトランジットゲートウェイを使用するのと似ていますが、ルートとアタッチメントが変わる可能性がある場合に、より高い柔軟性を提供します。このシナリオでは、独立した各ルーターに単一のルートテーブルがあります。独立したルーターに関連付けられているすべてのアタッチメントは、伝播されてそのルートテーブルに関連付けられます。1 つの独立したルーターに関連付けられているアタッチメントは、相互にパケットをルーティングできますが、別の独立したルーターのアタッチメントにパケットをルーティングしたり、アタッチメントか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

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。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。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。
- 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 アタッチメントを作成する”」(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。

  「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、「AWS Transit Gateway で Transit Gateway ルートテーブルへのルート伝達を有効にする」(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

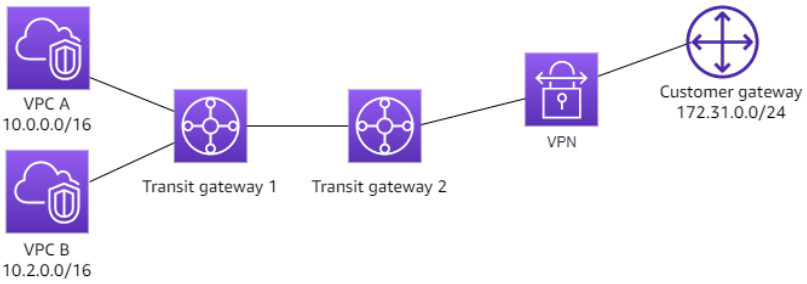
異なるリージョンで Transit Gateway 間に Transit Gateway ピアリング接続を作成できます。その後、各 Transit Gateway のアタッチメント間でトラフィックをルーティングできます。このシナリオでは、VPC および VPN アタッチメントは、Transit Gateway のデフォルトルートテーブルに関連付けられ、Transit Gateway のデフォルトルートテーブルに伝播されます。各 Transit Gateway のルートテーブルには、ゲートウェイのピアリングアタッチメントを指す静的ルートがあります。

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。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。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 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 アタッチメントを作成する”」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。「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、「AWS Transit Gateway の 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

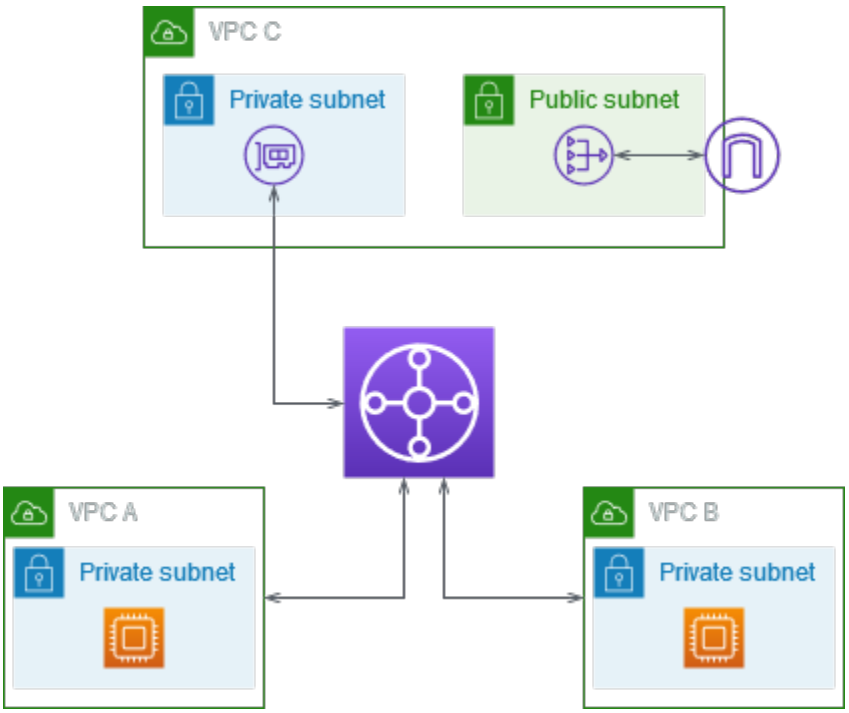
例: インターネットへの一元的な発信ルーティング

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。

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。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。

- 同一でもなく重複もしていない IP アドレス範囲を持つ 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 アタッチメントを作成する”」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	添付ファイル	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
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。

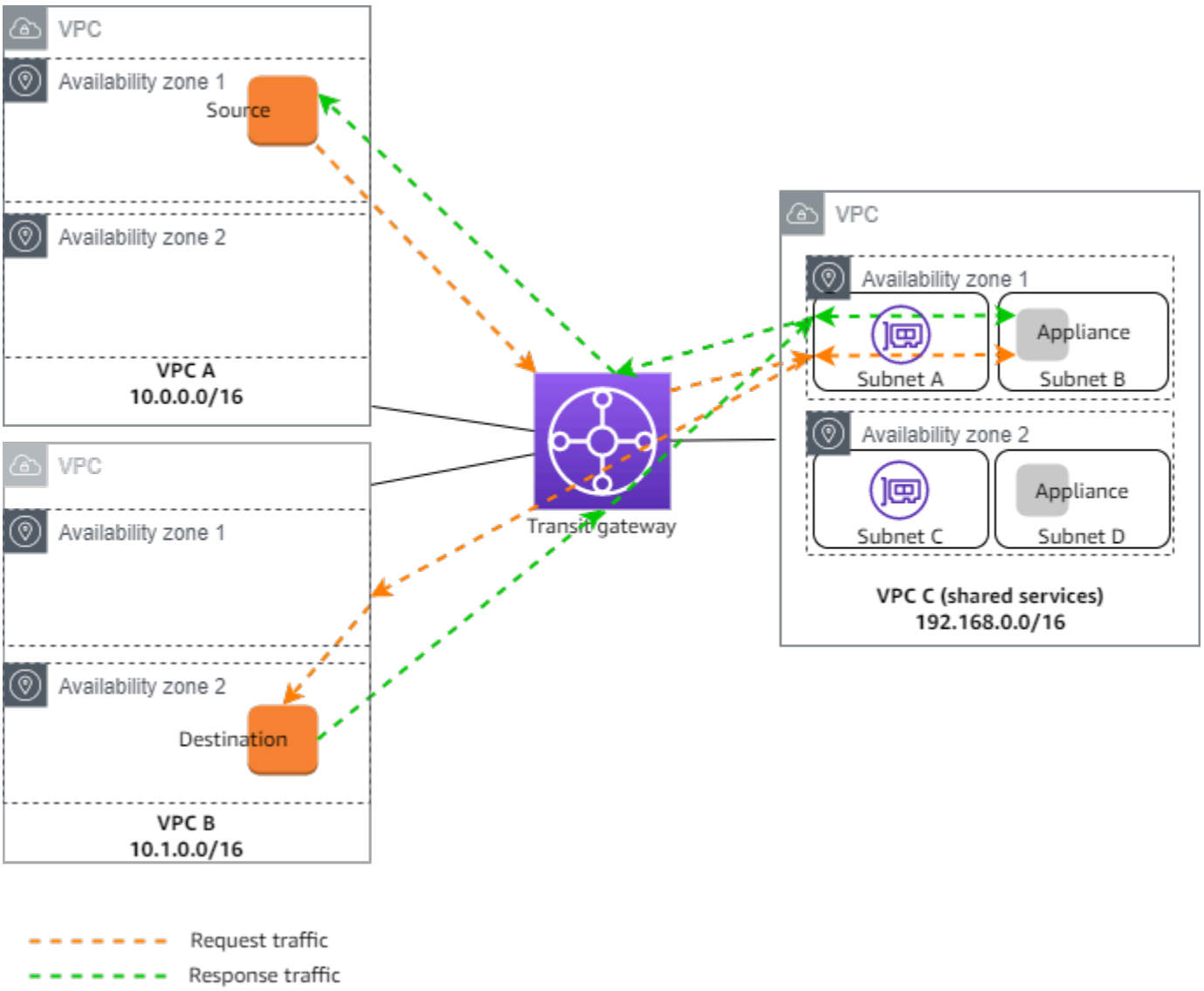
Important

- 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 アタッチメントにある場合、トラフィックが低下する可能性があります。中央 VPC がインターネットゲートウェイなどの別のゲートウェイからトラフィックを受信し、検査後にそのトラフィックを Transit Gateway アタッチメントに送信すると、トラフィックが低下する可能性があります。
- 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、アタッチメントがアベイラビリティーゾーンを通過す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。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。
- Transit Gateway。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 アタッチメントを作成する”」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、アプライアンスモードを有効にする AWS CLI 、または を使用することもできます CloudFormation。例えば、create-transit-gateway-vpc-attachment または modify-transit-gateway-vpc-attachment コマンドに `--options ApplianceModeSupport=enable` 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

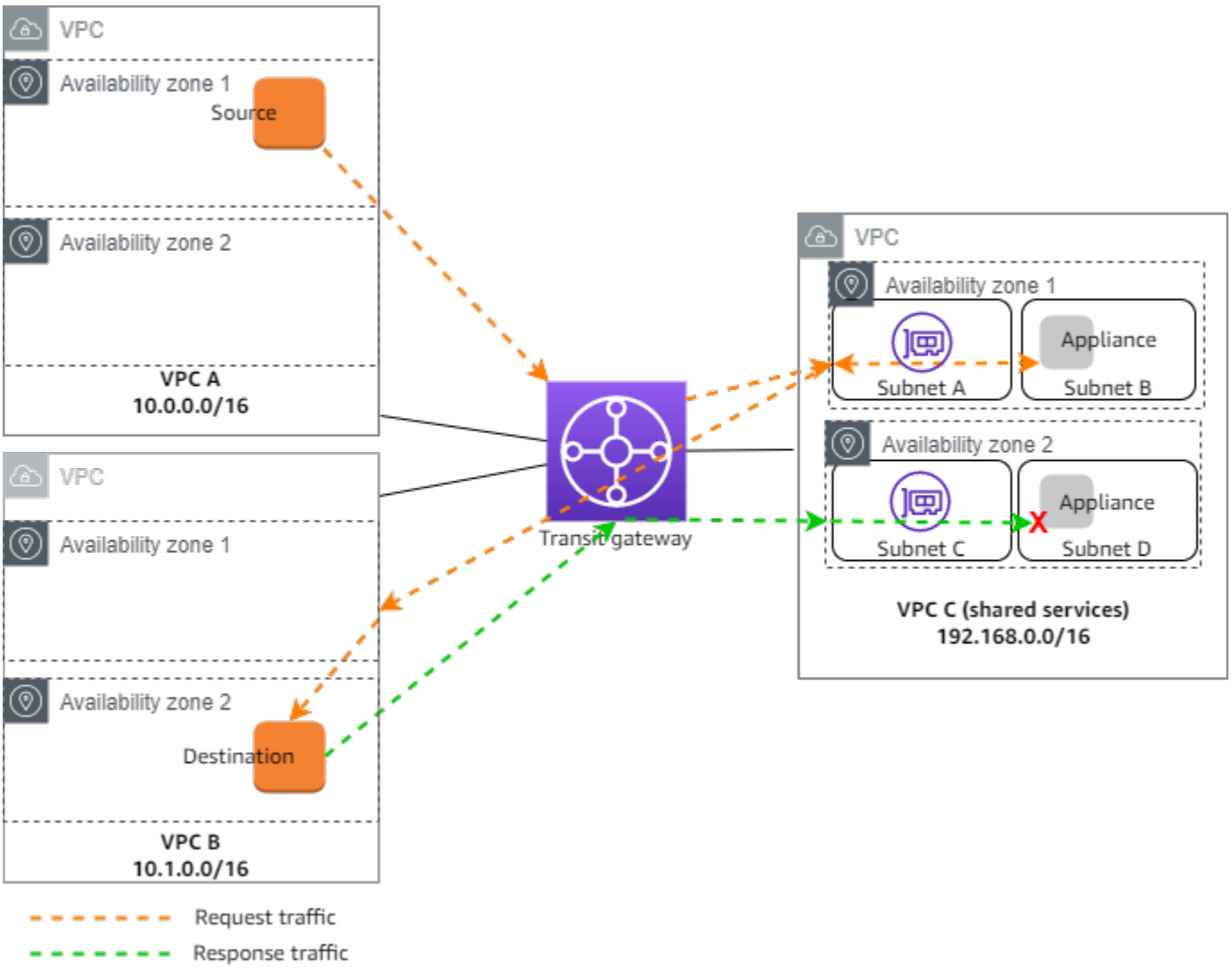
VPC アタッチメントが複数のアベイラビリティーゾーンにまたがっており、ステートフルな検査のために送信元ホストと送信先ホスト間のトラフィックを同じアプライアンスを介してルーティングする必要がある場合は、アプライアンスが配置されている VPC アタッチメントのアプライアンスモードサポートを有効にします。

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

チュートリアル: AWS Transit Gateway を開始する

次のチュートリアルは、AWS Transit Gateway の Transit Gateway を理解するのに役立ちます。次のチュートリアルのタスクでは、Transit Gateway を作成し、Transit Gateway を使用して 2 つの VPC を接続する手順を説明します。Amazon VPC コンソールまたは AWS CLI を使用して、Transit Gateway を作成できます。

タスク

- チュートリアル: Amazon VPC コンソールを使用して AWS Transit Gateway を作成する
- チュートリアル: AWS コマンドラインを使用して AWS Transit Gateway を作成する

チュートリアル: Amazon VPC コンソールを使用して AWS Transit Gateway を作成する

このチュートリアルでは、Amazon VPC コンソールを使用して Transit Gateway を作成し、2 つの VPC を接続する方法について説明します。Transit Gateway を作成し、両方の VPC をアタッチしてから、Transit Gateway と VPC 間の通信を有効化するために必要なルートを設定します。

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、同一のまたは重複する 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、「Amazon VPC ユーザーガイド」の「VPC の作成」および「Amazon EC2 ユーザーガイド」の「インスタンスの起動」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、「AWS Transit Gateway での Identity and Access Management」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ルールの設定」を参照してください。

ステップ

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. Amazon 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. [Transit Gateway の設定] セクションで、以下を実行します。

    1. [Amazon 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、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。
    2. (オプション) 次のいずれかを有効にするかどうかを選択します。
        - この Transit Gateway にアタッチされた VPC の [DNS サポート]。

- Transit Gateway にアタッチされた VPN 接続の [VPN ECMP] サポート。
- [デフォルトのルートテーブルの関連付け] により、Transit Gateway アタッチメントがこの Transit Gateway のデフォルトのルートテーブルに自動的に関連付けられます。
- [デフォルトのルートテーブル伝播] により、ルートテーブルアタッチメントがこの Transit Gateway のデフォルトのルートテーブルに自動的に伝播されます。
- [マルチキャストサポート] では、この Transit Gateway でマルチキャストドメインを作成できます。

8. (オプション) [クロスアカウント共有オプションの設定] セクションで、[共有アタッチメントを自動承認] にするかどうかを選択します。有効にすると、アタッチメントは自動的に受け入れられます。それ以外の場合は、アタッチメントリクエストを受け入れる、または拒否する必要があります。
9. (オプション) [Transit Gateway CIDR ブロックセクション] で、IPv4 アドレスの場合はサイズ /24 CIDR ブロック以上、IPv6 アドレスの場合はサイズ /64 ブロック以上を追加します。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。

> **Note**
>
> Transit Gateway CIDR ブロックは、Connect (GRE) アタッチメントまたは PrivateIP VPN を設定する場合に使用されます。Transit Gateway は、この範囲のトンネルエンドポイント (GRE/PrivateIP VPN) に IP を割り当てます。

10. (オプション) この Transit Gateway にキーと値のタグを追加して、識別しやすくします。
    1. [新しいタグを追加] をクリックします。
    2. [キー] の名前と関連する [値] を入力します。
    3. [新しいタグを追加] を選択してタグを追加するか、次のステップに進みます。
11. [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. 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] 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、「the section called “トランジットゲートウェイシナリオの例”」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、「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。

ルートを VPC ルートテーブルに追加するには

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、[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、「Amazon EC2 ユーザーガイド」の「EC2 インスタンスに接続する」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。

チュートリアル: AWS コマンドラインを使用して AWS Transit Gateway を作成する

このチュートリアルでは、 を使用してトランジットゲートウェイ AWS CLI を作成し、2 つの VPCs を接続する方法について説明します。Transit Gateway を作成し、両方の VPC をアタッチしてから、Transit Gateway と VPC 間の通信を有効化するために必要なルートを設定します。

前提条件

開始する前に、以下の準備が整っていることを確認します。

- AWS CLI 適切なアクセス許可でインストールおよび設定されている。 AWS CLI がインストールされていない場合は、「AWS コマンドラインインターフェイスドキュメント」を参照してください。
- VPC は、同一のまたは重複する CIDR を持つことはできません。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。
- 各 VPC で 1 つの EC2 インスタンス。VPC で EC2 インスタンスを起動する手順については、「Amazon EC2 ユーザーガイド」の「インスタンスの起動」を参照してください。
- インスタンス間の ICMP トラフィックを許可するように設定されたセキュリティグループ。セキュリティグループ使用の詳細については、「Amazon VPC ユーザーガイド」の「セキュリティグループを使用して AWS リソースへのトラフィックを制御する」を参照してください。
- Transit Gateway を操作するための適切な IAM アクセス許可。Transit Gateway IAM アクセス許可を確認するには、「 AWS Transit Gateway ガイド」のAWS 「Transit Gateway での Identity and Access Management」を参照してください。

Steps

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、 は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 AWS を作成し、それをデフォルトの関連付けルートテーブルとデフォルトの伝播ルートテーブルとして使用します。us-west-2 リージョンで create-transit-gateway リクエストの例を次に示します。リクエストで追加の options が渡されました。リクエストで渡すことができるオプションのリストなど、create-transit-gateway コマンドの詳細については、create-transit-gateway を参照してください。

```
aws ec2 create-transit-gateway \
  --description "My Transit Gateway" \
  --region us-west-2
```

次に、Transit Gateway が作成されたことがレスポンスに表示されます。レスポンスでは、返される Options はすべてデフォルト値です。

```
{
    "TransitGateway": {
        "TransitGatewayId": "tgw-1234567890abcdef0",
        "TransitGatewayArn": "arn:aws:ec2:us-west-2:123456789012:transit-gateway/
tgw-1234567890abcdef0",
        "State": "pending",
        "OwnerId": "123456789012",
        "Description": "My Transit Gateway",
        "CreationTime": "2025-06-23T17:39:33+00:00",
        "Options": {
            "AmazonSideAsn": 64512,
            "AutoAcceptSharedAttachments": "disable",
            "DefaultRouteTableAssociation": "enable",
            "AssociationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
            "DefaultRouteTablePropagation": "enable",
            "PropagationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
            "VpnEcmpSupport": "enable",
            "DnsSupport": "enable",
            "SecurityGroupReferencingSupport": "disable",
            "MulticastSupport": "disable"
        }
    }
}
```

> **Note**
>
> このコマンドは、ID を含む新しい Transit Gateway に関する情報を返します。後続のステップで必要になるため、Transit Gateway ID (tgw-1234567890abcdef0) を書き留めます。

ステップ 2: Transit Gateway の可用性状態を確認する

Transit Gateway を作成すると、pending 状態になります。状態は自動的に保留中から使用可能に変わりますが、状態が変わるまで VPC をアタッチすることはできません。状態を確認するには、新しく作成された Transit Gateway ID とフィルターオプションを使用して describe-transit-gatweways コマンドを実行します。filters オプションでは、Name=state と Values=available のペアを使用します。その後、コマンドは検索して、Transit Gateway の状態が使用可能な状態かどうかを確認します。その場合は、レスポンスに "State": "available" が表示されます。他の状態にある場合は、まだ使用できません。コマンドを実行する前に数分待ちます。

describe-transit-gateways コマンドの詳細については、describe-transit-gateways を参照してください。

```
aws ec2 describe-transit-gateways \
  --transit-gateway-ids tgw-1234567890abcdef0 \
  --filters Name=state,Values=available
```

Transit Gateway の状態が pending から available に変わるまで待ってから続行します。次のレスポンスでは、State が available に変更されました。

```
{
    "TransitGateways": [
        {
            "TransitGatewayId": "tgw-1234567890abcdef0",
            "TransitGatewayArn": "arn:aws:ec2:us-west-2:123456789012:transit-gateway/
tgw-1234567890abcdef0",
            "State": "available",
            "OwnerId": "123456789012",
            "Description": "My Transit Gateway",
            "CreationTime": "2022-04-20T19:58:25+00:00",
            "Options": {
                "AmazonSideAsn": 64512,
```

```
                "AutoAcceptSharedAttachments": "disable",
                "DefaultRouteTableAssociation": "enable",
                "AssociationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
                "DefaultRouteTablePropagation": "enable",
                "PropagationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
                "VpnEcmpSupport": "enable",
                "DnsSupport": "enable",
                "SecurityGroupReferencingSupport": "disable",
                "MulticastSupport": "disable"
            },
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "example-transit-gateway"
                }
            ]
        }
    ]
}
```

ステップ 3: VPCsをトランジットゲートウェイにアタッチする

Transit Gateway が使用可能になったら、`create-transit-gateway-vpc-attachment` を使用して各 VPC のアタッチメントを作成します。`transit-gateway-id`、`vpc-id`、`subnet-ids` を含める必要があります。

`create-transit-vpc attachment` コマンドの詳細については、create-transit-gateway-vpc-attachment を参照してください。

次の例では、各 VPC ごとに 1 回ずつ、計 2 回コマンドを実行します。

最初の VPC では、最初の `vpc_id` と`subnet-ids` を使用して次を実行します。

```
aws ec2 create-transit-gateway-vpc-attachment \
  --transit-gateway-id tgw-1234567890abcdef0 \
  --vpc-id vpc-1234567890abcdef0 \
  --subnet-ids subnet-1234567890abcdef0
```

レスポンスには、成功したアタッチメントが表示されます。アタッチメントは `pending` 状態で作成されます。この状態は自動的に `available` 状態に変更されるため、この状態を変更する必要はありません。この処理には数分かかることがあります。

```
{
    "TransitGatewayVpcAttachment": {
        "TransitGatewayAttachmentId": "tgw-attach-1234567890abcdef0",
        "TransitGatewayId": "tgw-1234567890abcdef0",
        "VpcId": "vpc-1234567890abcdef0",
        "VpcOwnerId": "123456789012",
        "State": "pending",
        "SubnetIds": [
            "subnet-1234567890abcdef0",
            "subnet-abcdef1234567890"
        ],
        "CreationTime": "2025-06-23T18:35:11+00:00",
        "Options": {
            "DnsSupport": "enable",
            "SecurityGroupReferencingSupport": "enable",
            "Ipv6Support": "disable",
            "ApplianceModeSupport": "disable"
        }
    }
}
```

2 番目の VPC では、2 番目の vpc_id と subnet-ids を使用して上記と同じコマンドを実行します。

```
aws ec2 create-transit-gateway-vpc-attachment \
  --transit-gateway-id tgw-1234567890abcdef0 \
  --vpc-id vpc-abcdef1234567890 \
  --subnet-ids subnet-abcdef01234567890
```

このコマンドのレスポンスには、現在 pending 状態にあるアタッチメントが成功したことも表示されます。

```
{
    {
    "TransitGatewayVpcAttachment": {
        "TransitGatewayAttachmentId": "tgw-attach-abcdef1234567890",
        "TransitGatewayId": "tgw-1234567890abcdef0",
        "VpcId": "vpc-abcdef1234567890",
        "VpcOwnerId": "123456789012",
        "State": "pending",
        "SubnetIds": [
            "subnet-fedcba0987654321",
```

```
            "subnet-0987654321fedcba"
        ],
        "CreationTime": "2025-06-23T18:42:56+00:00",
        "Options": {
            "DnsSupport": "enable",
            "SecurityGroupReferencingSupport": "enable",
            "Ipv6Support": "disable",
            "ApplianceModeSupport": "disable"
        }
    }
}
```

ステップ 4: Transit Gateway アタッチメントが使用可能であることを確認する

Transit Gateway アタッチメントは初期の pending 状態で作成されます。状態が available に変わるまで、これらのアタッチメントをルートで使用することはできません。これは自動的に行われます。describe-transit-gateways コマンドと transit-gateway-id を使用して、State を確認します。describe-transit-gateways コマンドの詳細については、describe-transit-gateways を参照してください。

次のコマンドを実行して、ステータスを確認します。この例では、オプションの Name フィールドと Values フィルターフィールドがリクエストに渡されます。

```
aws ec2 describe-transit-gateway-vpc-attachments \
  --filters Name=transit-gateway-id,Values=tgw-1234567890abcdef0
```

次のレスポンスは、両方のアタッチメントが available 状態にあることを示しています。

```
{
    "TransitGatewayVpcAttachments": [
        {
            "TransitGatewayAttachmentId": "tgw-attach-1234567890abcdef0",
            "TransitGatewayId": "tgw-1234567890abcdef0",
            "VpcId": "vpc-1234567890abcdef0",
            "VpcOwnerId": "123456789012",
            "State": "available",
            "SubnetIds": [
                "subnet-1234567890abcdef0",
                "subnet-abcdef1234567890"
```

```
            ],
            "CreationTime": "2025-06-23T18:35:11+00:00",
            "Options": {
                "DnsSupport": "enable",
                "SecurityGroupReferencingSupport": "enable",
                "Ipv6Support": "disable",
                "ApplianceModeSupport": "disable"
            },
            "Tags": []
        },
        {
            "TransitGatewayAttachmentId": "tgw-attach-abcdef1234567890",
            "TransitGatewayId": "tgw-1234567890abcdef0",
            "VpcId": "vpc-abcdef1234567890",
            "VpcOwnerId": "123456789012",
            "State": "available",
            "SubnetIds": [
                "subnet-fedcba0987654321",
                "subnet-0987654321fedcba"
            ],
            "CreationTime": "2025-06-23T18:42:56+00:00",
            "Options": {
                "DnsSupport": "enable",
                "SecurityGroupReferencingSupport": "enable",
                "Ipv6Support": "disable",
                "ApplianceModeSupport": "disable"
            },
            "Tags": []
        }
    ]
}
```


ステップ 5: Transit Gateway と VPC の間にルートを追加する

コマンド `create-route` と各 VPC ルートテーブルの `transit-gateway-id` を使用して、Transit Gateway 経由でトラフィックを他の VPC に転送するように各 VPC のルートテーブルにルートを設定します。次の例では、各ルートテーブルごとに 1 回ずつ、計 2 回コマンドを実行します。リクエストには、作成する各 VPC ルートの `route-table-id`、`destination-cidr-block`、`transit-gateway-id` が含まれます。

`create-route` コマンドの詳細については、create-route を参照してください。

最初の VPC のルートテーブルで、次のコマンドを実行します。

```
aws ec2 create-route \
  --route-table-id rtb-1234567890abcdef0 \
  --destination-cidr-block 10.2.0.0/16 \
  --transit-gateway-id tgw-1234567890abcdef0
```

2 番目の VPC のルートテーブルで、次のコマンドを実行します。このルートは、最初の VPC とは異なる `route-table-id` と `destination-cidr-block` を使用します。ただし、単一の Transit Gateway のみを使用しているため、同じ `transit-gateway-id` が使用されます。

```
aws ec2 create-route \
  --route-table-id rtb-abcdef1234567890 \
  --destination-cidr-block 10.1.0.0/16 \
  --transit-gateway-id tgw-1234567890abcdef0
```

レスポンスは、ルートごとに `true` を返し、ルートが作成されたことを示します。

```
{
    "Return": true
}
```

> **Note**
>
> 送信先 CIDR ブロックを VPC の実際の CIDR ブロックに置き換えます。

ステップ 6: トランジットゲートウェイをテストする

Transit Gateway が正常に作成されたことを確認するには、ある VPC の EC2 インスタンスに接続し、その他の VPC のインスタンスに ping を送信してから、 `ping` コマンドを実行します。

1. SSH または EC2 Instance Connect を使用して最初の VPC の EC2 インスタンスに接続する
2. 2 番目の VPC の EC2 インスタンスのプライベート IP アドレスに対する ping を実行します。

   ```
   ping 10.2.0.50
   ```

> **Note**
>
> `10.2.0.50` を 2 番目の VPC の EC2 インスタンスの実際のプライベート IP アドレスに置き換えます。

ping が成功すると、Transit Gateway が正しく設定され、VPC 間のトラフィックをルーティングします。

ステップ 7: Transit Gateway アタッチメントと Transit Gateway を削除する

不要になった Transit Gateway は削除できます。まず、すべてのアタッチメントを削除する必要があります。各アタッチメントの `transit-gateway-attachment-id` を使用して、`delete-transit-gateway-vpc-attachment` コマンドを実行します。コマンドを実行したら、`delete-transit-gateway` を使用して Transit Gateway を削除します。以下では、前のステップで作成した 2 つの VPC アタッチメントと 1 つの Transit Gateway を削除します。

> **Important**
>
> Transit Gateway アタッチメントをすべて削除すると、料金の発生が停止します。

1. `delete-transit-gateway-vpc-attachment` コマンドを使用して VPC アタッチメントを削除します。`delete-transit-gateway-vpc-attachment` コマンドの詳細については、delete-transit-gateway-vpc-attachment を参照してください。

   最初のアタッチメントで、次のコマンドを実行します。

   ```
   aws ec2 delete-transit-gateway-vpc-attachment \
     --transit-gateway-attachment-id tgw-attach-1234567890abcdef0
   ```

   最初の VPC アタッチメント削除時のレスポンスは、次を返します。

   ```
   {
       "TransitGatewayVpcAttachment": {
           "TransitGatewayAttachmentId": "tgw-attach-1234567890abcdef0",
           "TransitGatewayId": "tgw-1234567890abcdef0",
   ```

```
        "VpcId": "vpc-abcdef1234567890",
        "VpcOwnerId": "123456789012",
        "State": "deleting",
        "CreationTime": "2025-06-23T18:42:56+00:00"
    }
}
```

2 番目のアタッチメントの delete-transit-gateway-vpc-attachment コマンドを実行します。

```
aws ec2 delete-transit-gateway-vpc-attachment \
  --transit-gateway-attachment-id tgw-attach-abcdef1234567890
```

2 番目の VPC アタッチメント削除時のレスポンスは、次を返します。

```
The response returns:
{
    "TransitGatewayVpcAttachment": {
        "TransitGatewayAttachmentId": "tgw-attach-abcdef1234567890",
        "TransitGatewayId": "tgw-1234567890abcdef0",
        "VpcId": "vpc-abcdef1234567890",
        "VpcOwnerId": "123456789012",
        "State": "deleting",
        "CreationTime": "2025-06-23T18:42:56+00:00"
    }
}
```

2. アタッチメントは、削除されるまで deleting 状態になります。削除すると、Transit Gateway を削除できます。transit-gateway-id と一緒に delete-transit-gateway コマンドを使用します。delete-transit-gateway コマンドの詳細については、delete-transit-gateway を参照してください。

   次の例では、上記の最初のステップで作成した My Transit Gateway を削除します。

```
aws ec2 delete-transit-gateway \
  --transit-gateway-id tgw-1234567890abcdef0
```

   リクエストに対するレスポンスを次に示します。これには、削除された Transit Gateway ID と名前、および作成時に Transit Gateway に設定された元のオプションが含まれます。

```
{
    "TransitGateway": {
        "TransitGatewayId": "tgw-1234567890abcdef0",
        "TransitGatewayArn": "arn:aws:ec2:us-west-2:123456789012:transit-gateway/
tgw-1234567890abcdef0",
        "State": "deleting",
        "OwnerId": "123456789012",
        "Description": "My Transit Gateway",
        "CreationTime": "2025-06-23T17:39:33+00:00",
        "Options": {
            "AmazonSideAsn": 64512,
            "AutoAcceptSharedAttachments": "disable",
            "DefaultRouteTableAssociation": "enable",
            "AssociationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
            "DefaultRouteTablePropagation": "enable",
            "PropagationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
            "VpnEcmpSupport": "enable",
            "DnsSupport": "enable",
            "SecurityGroupReferencingSupport": "disable",
            "MulticastSupport": "disable"
        },
        "Tags": [
            {
                "Key": "Name",
                "Value": "example-transit-gateway"
            }
        ]
    }
}
```


結論

Transit Gateway を正常に作成し、2 つの VPC がアタッチされると、それらの間のルーティングを設定し、接続を確認できます。この簡単な例は、 AWS トランジットゲートウェイの基本機能を示しています。オンプレミスネットワークへの接続や高度なルーティング設定の実装など、より複雑なシナリオについては、「AWS Transit Gateway ガイド」を参照してください。

AWS 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。
- Direct Connectゲートウェイアタッチメントおよび BGP Site-to-Site VPN アタッチメントのルート伝達を有効にします。
- 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 の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。

AWS 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。トランジットゲートウェイの暗号化サポートの有効化と管理については、「」を参照してくださいthe section called “暗号化のサポート”。

トピック

共有された Transit Gateway

AWS Resource Access Manager (RAM) を使用して、VPC アタッチメントのトランジットゲートウェイをアカウント間または組織全体で共有できます AWS Organizations。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。

考慮事項

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 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のと同じ 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、トランジットゲートウェイの関連付けを使用し、Direct Connect ゲートウェイと同じ AWS アカウントにあることも、Direct Connect ゲートウェイとは異なるアカウントにあることもできます。

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 であり、すべての AWS アカウントの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 アカウントと共有解除された場合、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 の AWS 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連携し AWS アカウント、 AWS RAM を使用してトランジットゲートウェイを他のアカウントと共有できます。トランジットゲートウェイを別のと共有すると AWS アカウント、アカウント所有者は VPCsをトランジットゲートウェイにアタッチできます。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。VPN コンセントレータアタッチメントは、BGP (動的) ルーティングのみをサポートします。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。Transit Gateway ルートテーブル内のルートをピアリングアタッチメントにポイントして、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できます。

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「IP アドレス指定」を参照してください。

タスク

- Transit Gateway で AWS Transit Gateway を作成する
- AWS Transit Gateway で Transit Gateway 情報を表示する
- AWS Transit Gateway で Transit Gateway タグを管理する
- Transit Gateway で Transit Gateway AWS を変更する
- AWS Resource Access Manager コンソールを使用して AWS Transit Gateway リソース共有を受け入れる
- AWS Transit Gateway で共有アタッチメントを承諾する
- Transit Gateway で Transit Gateway AWS を削除する
- AWS Transit Gateway の暗号化サポート

Transit Gateway で AWS 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。

> **Note**
>
> トランジットゲートウェイで暗号化サポートを有効にする場合は、ゲートウェイの作成中に有効に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、使用可能な状態になったら、それを変更して Encryption サポートを有効にすることができます。詳細については、「the section called “暗号化のサポート”」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. 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 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) セッションの AWS 側の ASN である必要があります。

   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、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. [セキュリティグループの参照のサポート] では、この機能を有効にして、Transit Gateway にアタッチされた VPC 間のセキュリティグループを参照します。セキュリティグループの参照の詳細については、「the section called “セキュリティグループの参照”」を参照してください。

9. [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。

10. [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。

11. [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。

12. (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。

13. (オプション) [クロスアカウント共有オプションの設定] セクションで、[共有アタッチメントを自動承認] にするかどうかを選択します。有効にすると、アタッチメントは自動的に受け入れら

れます。それ以外の場合は、アタッチメントリクエストを受け入れる、または拒否する必要があります。

[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。

14. (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。

    > **Note**
    >
    > トランジットゲートウェイ CIDR ブロックは、Connect (GRE) アタッチメント、PrivateIP VPNs、またはクライアント VPN アタッチメントを設定する場合に使用されます。Transit Gateway は、この範囲のトンネルエンドポイント (GRE/PrivateIP VPN) とクライアント VPN アタッチメントに IPs を割り当てます。

15. [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] コマンドを使用します。

AWS Transit Gateway で Transit Gateway 情報を表示する

任意の Transit Gateway を表示する

コンソールを使用して Transit Gateway 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] 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。

AWS CLI を使用して Transit Gateway を表示するには

[describe-transit-gateways] コマンドを使用します。

AWS Transit Gateway で Transit Gateway タグを管理する

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. 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. 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. [保存] を選択します。

Transit Gateway で Transit Gateway AWS を変更する

Transit Gateway の設定オプションを変更できます。Transit Gateway を変更しても、既存の Transit Gateway アタッチメントでサービスが中断されることはありません。

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。

> **Note**
>
> 暗号化サポートが有効になっているトランジットゲートウェイは、モニタリングモードまたは強制モードの暗号化コントロールを持つ VPCs、または暗号化コントロールが有効になっていない VPCs にアタッチできます。Enforce モードの暗号化コントロールを持つ VPCs は、暗号化サポートが有効になっている Transit Gateway にのみアタッチできます。
> 詳細については、「the section called “暗号化のサポート”」を参照してください。

Transit Gateway 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] 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 コマンドを使用します。

AWS Resource Access Manager コンソールを使用して AWS Transit Gateway 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、 AWS Resource Access Manager (AWS RAM) コンソールを通じてリソース共有を承諾する必要があります。

リソース共有を受け入れるには

1. https://console.aws.amazon.com/ram/ で AWS RAM コンソールを開きます。
2. ナビゲーションペインで [Shared with me] (自分と共有)、[Resource shares] (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。

AWS Transit Gateway で共有アタッチメントを承諾する

Transit Gateway の作成時に [共有アタッチメントを自動承諾] 機能を有効にしなかった場合は、Amazon VPC コンソールまたは AWS CLI を使用して、クロスアカウント (共有) アタッチメントを手動で承認する必要があります。

共有アタッチメントを手動で受け入れるには

1. 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 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。

AWS CLI を使用して、共有アタッチメントを受け入れるには

[accept-transit-gateway-vpc-attachment] コマンドを使用します。

Transit Gateway で Transit Gateway AWS を削除する

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. Amazon 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] コマンドを使用します。

AWS Transit Gateway の暗号化サポート

暗号化コントロールを使用すると、VPC 内のトラフィックフローの暗号化ステータスを監査し、VPC 内のすべてのトラフィックに対してencryption-in-transitを適用できます。VPC 暗号化コントロールが強制モードの場合、その VPC 内のすべての Elastic Network Interface (ENI) は AWS Nitro 暗号化対応インスタンスにのみアタッチするように制限され、転送中のデータを暗号化する AWS サービスのみが暗号化コントロール強制 VPC にアタッチできます。VPC 暗号化コントロールの詳細については、このドキュメントを参照してください。

Transit Gateway 暗号化のサポートと VPC 暗号化コントロール

Transit Gateway での暗号化サポートを使用すると、Transit Gateway にアタッチされた VPCs 間のトラフィックに対してencryption-in-transitを適用できます。VPCs 間のトラフィックを暗号化するには、modify-transit-gateway コマンドを使用して Transit Gateway で暗号化サポートを手動でアクティブ化する必要があります。有効にすると、すべてのトラフィックは、Transit Gateway を介して強制モード (除外なし) の VPCs 間の 100% 暗号化されたリンクを通過します。暗号化コントロールが有効になっていない VPCs を接続することもできます。このシナリオでは、Transit Gateway は、強制モードで実行されていない VPC の Transit Gateway アタッチメントまでのトラフィックを暗号化することが保証されます。さらに、トラフィックが強制モードで実行されていない VPC の に送信されるインスタンスによって異なります。

暗号化サポートは既存のトランジットゲートウェイにのみ追加でき、作成中は追加できません。Transit Gateway が Encryption Support Enabled 状態に移行すると、Transit Gateway またはアタッチメントにダウンタイムはありません。移行はシームレスで透過的であり、トラフィックはドロップされません。トランジットゲートウェイを変更して暗号化サポートを追加する手順については、「」を参照してくださいTransit Gateway の変更。

要件

トランジットゲートウェイで暗号化サポートを有効にする前に、以下を確認してください。

- トランジットゲートウェイに Connect アタッチメントがない
- トランジットゲートウェイにピアリングアタッチメントがない
- トランジットゲートウェイに Network Firewall アタッチメントがない
- トランジットゲートウェイに VPN コンセントレータアタッチメントがない
- トランジットゲートウェイにクライアント VPN アタッチメントがない
- Transit Gateway でセキュリティグループ参照が有効になっていない
- トランジットゲートウェイでマルチキャスト機能が有効になっていない

暗号化サポートの状態

トランジットゲートウェイは、次のいずれかの暗号化状態を持つことができます。

- enabling - トランジットゲートウェイは暗号化サポートを有効に中です。このプロセスが完了するまでに最大 14 日かかる場合があります。
- enabled - トランジットゲートウェイで暗号化サポートが有効になっています。暗号化コントロールが適用された VPC アタッチメントを作成できます。

- disabling - Transit Gateway は Encryption サポートを無効化中です。
- 無効 - トランジットゲートウェイで暗号化のサポートは無効になっています。

Transit Gateway アタッチメントルール

Transit Gateway で Encryption サポートが有効になっている場合、次のアタッチメントルールが適用されます。

- トランジットゲートウェイの暗号化状態が有効化または無効化されている場合、暗号化コントロール強制モードまたは強制モードではない Direct Connect アタッチメント、VPN アタッチメント、VPC アタッチメントを作成できます。
- トランジットゲートウェイの暗号化状態を有効にすると、任意の暗号化制御モードで VPC、Direct Connect アタッチメント、VPN アタッチメント、VPC アタッチメントを作成できます。
- トランジットゲートウェイの暗号化状態が無効になっている場合、暗号化コントロールが適用された新しい VPC アタッチメントを作成することはできません。
- 接続アタッチメント、ピアリングアタッチメント、Network Firewall アタッチメント、VPN コンセントレータアタッチメント、クライアント VPN アタッチメント、セキュリティグループリファレンス、およびマルチキャスト機能は、暗号化サポートではサポートされていません。

互換性のない添付ファイルを作成しようとすると、API エラーで失敗します。

AWS Transit Gateway の Amazon VPC アタッチメント

トランジットゲートウェイへの Amazon Virtual Private Cloud (VPC) アタッチメントを使用すると、1 つ以上の VPC サブネットとの間でトラフィックをルーティングできます。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。指定されたサブネットが、Transit Gateway トラフィックの送受信に使用されます。トラフィックは、Transit Gateway アタッチメントサブネットに、ターゲットサブネットを指すルートテーブルに適切なルートが設定されている場合にのみ、同じアベイラビリティーゾーン内の他のサブネットのリソースに到達できます。

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。

> **Note**
>
> Transit Gateway アタッチメントがあるアベイラビリティーゾーン内では、トラフィックはアタッチメントに関連付けられている特定のサブネットからのみ Transit Gateway に転送されます。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。ゾーンおよびアタッチメントサブネットのルートテーブルには、VPC 内のトラフィックの送信先に適切に到達できるルートが含まれています。

- 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アタッチされたすべての VPCs「Amazon Route 53 と AWS Transit Gateway を使用したハイブリッドクラウドの集中 DNS 管理」を参照してください。
- Transit Gateway は、同一の CIDR を持つ VPC 間のルーティングをサポートしていません。また、範囲内の CIDR がアタッチされた VPC 内の CIDR と重複している場合もサポートされません。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 と同一である、または重複する場合、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。

VPC アタッチメントのルートテーブル要件

Transit Gateway VPC アタッチメントを適切に機能させるには、特定のルートテーブル設定が必要です。

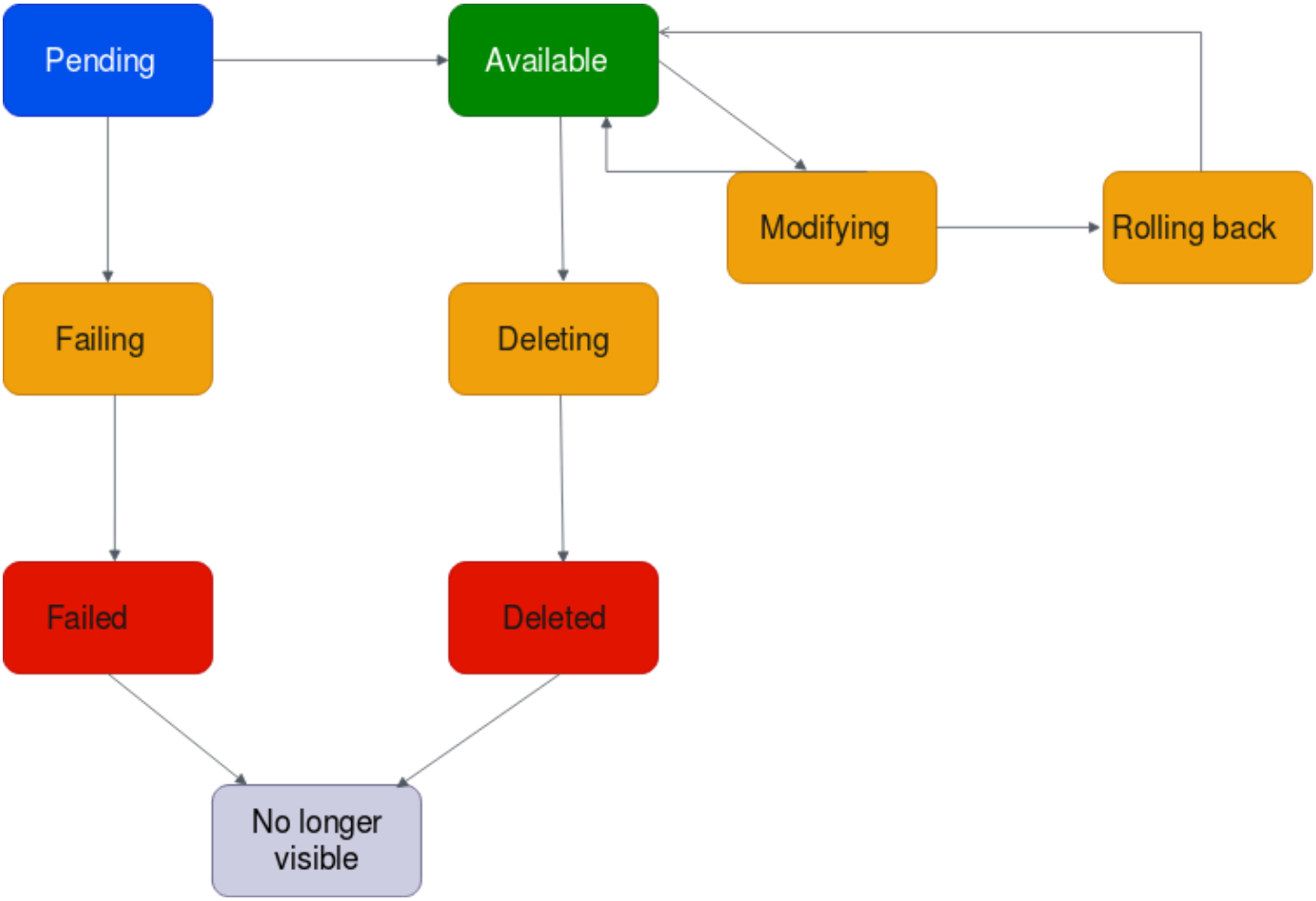
- アタッチメントサブネットルートテーブル: Transit Gateway アタッチメントに関連付けられたサブネットには、Transit Gateway 経由で到達する必要がある VPC 内の送信先のルートテーブルエントリが必要です。これには、他のサブネット、インターネットゲートウェイ、NAT ゲートウェイ、VPC エンドポイントへのルートが含まれます。
- ターゲットサブネットルートテーブル: Transit Gateway を介して通信する必要があるリソースを含むサブネットには、外部送信先へのトラフィックを返すために Transit Gateway を指すルートが必要です。
- ローカル VPC トラフィック: Transit Gateway アタッチメントは、同じ VPC 内のサブネット間の通信を自動的に有効化しません。標準 VPC ルーティングルールが適用され、VPC 内通信のルートテーブルにローカルルート (VPC CIDR) が存在する必要があります。

> **Note**
>
> 同じアベイラビリティーゾーン内のアタッチされていないサブネットにルートを設定しても、トラフィックフローを有効化しません。Transit Gateway アタッチメントに関連付けられた特定のサブネットのみが、Transit Gateway トラフィックの送受信に使用されます。

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。

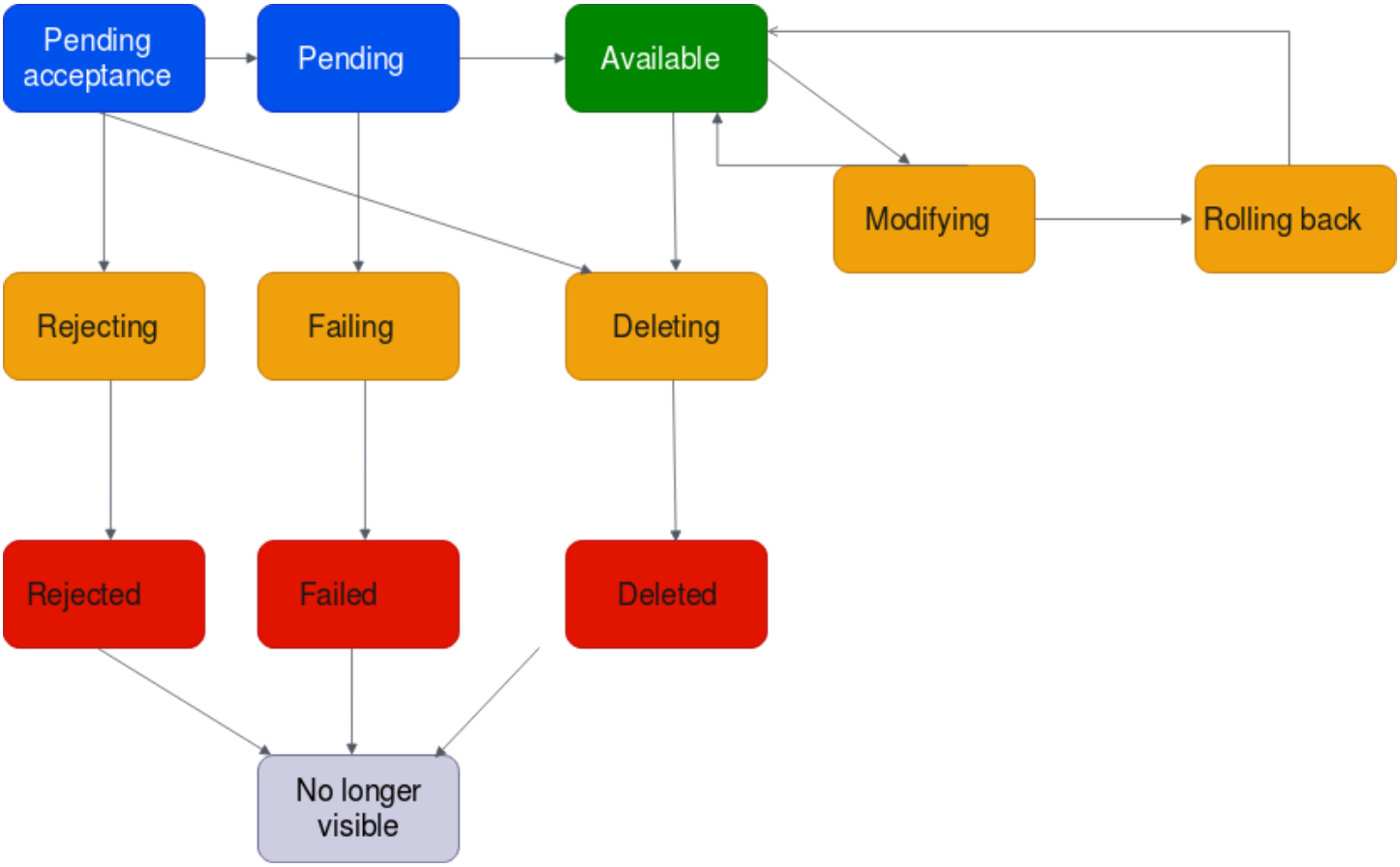
次の図は、単一のアカウント設定、または [共有アタッチメントを自動承諾] がオンになっているクロスアカウント設定で、アタッチメントが経る可能性のある状態を示しています。



- 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。

アプライアンスモード

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、アタッチメントを作成する際に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、送信元と送信先間のトラフィックフローの存続期間中、 AWS Transit Gateway は 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。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。アプライアンスモードは VPC アタッチメントでのみサポートされていますが、ネットワークフローは VPC、VPN、Connect アタッチメントなど、他の Transit Gateway アタッチメントタイプから取得で

きます。アプライアンスモードは、さまざまな AWS リージョンに送信元と送信先があるネットワークフローでも機能します。最初にアプライアンスモードを有効にせず、後でアタッチメント設定を編集して有効にすると、ネットワークフローは異なるアベイラビリティーゾーン間で再調整される可能性があります。コンソール、コマンドラインあるいは API を使用して、アプライアンスモードを有効化または無効化できます。

AWS Transit Gateway のアプライアンスモードは、アプライアンスモード VPC を通過するパスを決定するときに、送信元と送信先のアベイラビリティーゾーンを考慮してトラフィックルーティングを最適化します。このアプローチにより、効率が向上し、レイテンシーが短縮されます。動作は、特定の設定とトラフィックパターンによって異なります。サンプルシナリオを以下に示します。

シナリオ 1: アプライアンス VPC を介したアベイラビリティーゾーン内のトラフィックルーティング

us-east-1a と us-east-1b の両方でアプライアンスモード VPC アタッチメントを使用して、送信元アベイラビリティーゾーン us-east-1a から送信先アベイラビリティーゾーン us-east-1a にトラフィックが流れると、Transit Gateway はアプライアンス VPC 内の us-east-1a からネットワークインターフェイスを選択します。このアベイラビリティーゾーンは、送信元と送信先の間のトラフィックフローの全期間にわたって維持されます。

シナリオ 2: アプライアンス VPC を介したアベイラビリティーゾーン間のトラフィックルーティング

送信元アベイラビリティーゾーン us-east-1a から送信先アベイラビリティーゾーン us-east-1b に流れるトラフィックで、us-east-1a と us-east-1b の両方にアプライアンスモード VPC アタッチメントがある場合、Transit Gateway 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 で us-east-1a または us-east-1b を選択します。選択したアベイラビリティーゾーンは、フローの存続期間中一貫して使用されます。

シナリオ 3: アベイラビリティーゾーンデータなしでアプライアンス VPC 経由でトラフィックをルーティングする

トラフィックが送信元アベイラビリティーゾーン us-east-1a からアベイラビリティーゾーン情報のない送信先 (インターネットバインドトラフィックなど) に発信された場合、アプライアンスモード VPC アタッチメントは us-east-1a と us-east-1b の両方で、Transit Gateway はアプライアンス VPC 内の us-east-1a からネットワークインターフェイスを選択します。

シナリオ 4: 送信元または送信先とは異なるアベイラビリティーゾーンのアプライアンス VPC 経由でトラフィックをルーティングする

トラフィックが送信元アベイラビリティーゾーン us-east-1a から送信先アベイラビリティーゾーン us-east-1b に流れると、異なるアベイラビリティーゾーン us-east-1c と us-east-1d にアプライアンスモード VPC アタッチメントがある場合、Transit Gateway 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 で us-east-1c または us-east-1d を選択します。選択したアベイラビリティーゾーンは、フローの存続期間中一貫して使用されます。

> **Note**
>
> アプライアンスモードは VPC アタッチメントでのみサポートされています。アプライアンス VPC アタッチメントに関連付けられたルートテーブルに対してルート伝達が有効になっていることを確認します。

セキュリティグループの参照

この機能を使用すると、同じ Transit Gateway にアタッチされている VPC 間のインスタンス間トラフィックのセキュリティグループの管理と制御を簡素化できます。セキュリティグループは、インバウンドルールでのみ相互参照できます。アウトバウンドセキュリティルールは、セキュリティグループの参照をサポートしていません。セキュリティグループ参照の有効化、または使用に関連する追加コストはありません。

セキュリティグループ参照のサポートは、Transit Gateway と Transit Gateway VPC アタッチメントの両方で設定でき、Transit Gateway とその VPC アタッチメントの両方で有効になっている場合にのみ機能します。

制限事項

VPC アタッチメントでセキュリティグループ参照を使用する場合、次の制限が適用されます。

- セキュリティグループの参照は、Transit Gateway ピアリング接続全体ではサポートされていません。両方の VPC を同じ Transit Gateway にアタッチする必要があります。
- セキュリティグループの参照は、アベイラビリティーゾーン use1-az3 の VPC アタッチメントではサポートされていません。
- セキュリティグループの参照は PrivateLink エンドポイントではサポートされていません。代わりに IP CIDR ベースのセキュリティルールを使用することをお勧めします。

- セキュリティグループ参照は、すべての出力セキュリティグループルールが VPC の EFS インターフェイスに対して設定されている場合、Elastic File System (EFS) で機能します。
- トランジットゲートウェイ経由のローカルゾーン接続では、us-east-1-atl-2a、us-east-1-dfw-2a、us-east-1-iah-2a、us-west-2-lax-1a、us-west-2-lax-1b、us-east-1-mia-2a、us-east-1-chi-2a、us-west-2-phx-2a のみサポートされています。
- サポートされていないローカルゾーン、 AWS Outposts、および Wavelength Zones のサブネットを持つ VPC では、サービスの中断を引き起こす可能性があるため、この機能を VPCs AWS アタッチメントレベルで無効にすることをお勧めします。
- 検査 VPC がある場合、トランジットゲートウェイを介して参照するセキュリティグループは、AWS Gateway Load Balancer または AWS Network Firewall 全体で機能しません。

タスク

- AWS Transit Gateway で VPC アタッチメントの作成
- AWS Transit Gateway で VPC アタッチメントを変更する
- AWS Transit Gateway で VPC アタッチメントタグを変更する
- AWS Transit Gateway で VPC アタッチメントを表示する
- AWS Transit Gateway で VPC アタッチメントを削除する
- AWS Transit Gateway セキュリティグループのインバウンドルールを更新する
- AWS Transit Gateway の参照されるセキュリティグループを特定する
- 古い AWS Transit Gateway セキュリティグループルールを削除する
- AWS Transit Gateway VPC アタッチメントの作成のトラブルシューティング

AWS Transit Gateway で VPC 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. [アタッチメントタイプ] で、[VPC] を選択します。
7. [DNS サポート]、[IPv6 サポート] および [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を選択した場合、送信元と送信先間のトラフィックフローは、そのフローの有効期間中、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. [セキュリティグループの参照のサポート] を有効にするかどうかを選択します。この機能を有効にして、Transit Gateway にアタッチされた VPC 間のセキュリティグループを参照します。セキュリティグループの参照の詳細については、「the section called “セキュリティグループの参照”」を参照してください。
9. [IPv6 サポート] を有効にするかどうかを選択します。
10. [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。
11. [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 Transit Gateway 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。
12. [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 VPC アタッチメントを作成するには

[create-transit-gateway-vpc-attachment] コマンドを使用します。

AWS Transit Gateway で 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. 次のいずれかを有効または無効にします。

   - [DNS サポート]
   - IPv6 サポート
   - [アプライアンスモードサポート]

5. アタッチメントからサブネットを追加または削除するには、追加または削除したい [サブネット ID] でチェックボックスをオンまたはオフにします。

> **Note**
>
> 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 にアタッチされた VPC 間でセキュリティグループを参照できるようにするには、[セキュリティグループの参照のサポート] を選択します。セキュリティグループの参照の詳細については、「the section called “セキュリティグループの参照”」を参照してください。

> **Note**
>
> 既存の Transit Gateway のセキュリティグループの参照を無効にすると、すべての VPC アタッチメントで無効になります。

7. 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-attachment] コマンドを使用します。

AWS Transit Gateway で 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. [保存] 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。

AWS Transit Gateway で VPC アタッチメントを表示する

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。

AWS CLI を使用して VPC アタッチメントを表示するには

[describe-transit-gateway-vpc-attachments] コマンドを使用します。

AWS Transit Gateway で VPC アタッチメントを削除する

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。

AWS CLI を使用して VPC アタッチメントを削除するには

[delete-transit-gateway-vpc-attachment] コマンドを使用します。

AWS Transit Gateway セキュリティグループのインバウンドルールを更新する

トランジットゲートウェイに関連付けられているインバウンドセキュリティグループルールは、どれでも更新できます。セキュリティグループルールは、Amazon VPC コンソールのコンソールもしくはコマンドラインまたは API を使用して更新できます。セキュリティグループの参照の詳細については、「the section called “セキュリティグループの参照”」を参照してください。

コンソールを使用してセキュリティグループルールを更新するには

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、[Security Groups] (セキュリティグループ) を選択します。
3. セキュリティグループを選択し、インバウンドルールを変更するには、[アクション]、[インバウンドのルールの編集] の順にクリックします。
4. ルールを追加するには、[ルールの追加] を選択し、タイプ、プロトコル、ポート範囲を指定します。[ソース] (インバウンドルール) には、Transit Gateway に接続された VPC のセキュリティグループの ID を入力します。

   > **Note**
   >
   > Transit Gateway に接続された VPC のセキュリティグループは、自動的には表示されません。

5. 既存のルールを編集するには、値 (ソースや説明など) を変更します。
6. ルールを削除するには、ルールの隣にある [削除] を選択します。
7. [Save Rules] (ルールの保存) を選択してください。

コマンドラインを使用してインバウンドルールを更新するには

- authorize-security-group-ingress (AWS CLI)
- Grant-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)
- Revoke-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)
- revoke-security-group-ingress (AWS CLI)

AWS Transit Gateway の参照されるセキュリティグループを特定する

同じ Transit Gateway にアタッチされた VPC 内のセキュリティグループのルールでセキュリティグループが参照されているかどうかを確認するには、次のいずれかのコマンドを使用します。

- describe-security-group-references (AWS CLI)
- Get-EC2SecurityGroupReference (AWS Tools for Windows PowerShell)

古い AWS Transit Gateway セキュリティグループルールを削除する

古いセキュリティグループルールは、同じ VPC または同じ Transit Gateway にアタッチされた VPC 内の削除されたセキュリティグループを参照するルールです。セキュリティグループルールは古くなっても、セキュリティグループから自動的に削除されません。手動で削除する必要があります。

Amazon VPC コンソールを使用して、VPC の古くなったセキュリティグループルールを表示および削除できます。

古くなったセキュリティグループルールを表示および削除するには

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、[Security Groups] (セキュリティグループ) を選択します。
3. [Action] (アクション)、[Manage stale rules] (古いルールの管理) の順に選択します。
4. VPC で古いルールを持つ VPC を選択します。
5. [Edit] を選択します。
6. 削除するルールの横にある [Delete] (削除) ボタンを選択します。[変更のプレビュー]、[ルールの保存] を選択します。

コマンドラインを使用して古いセキュリティグループルールを記述するには

- describe-stale-security-groups (AWS CLI)
- Get-EC2StaleSecurityGroup (AWS Tools for Windows PowerShell)

古くなったセキュリティグループルールを特定した後、revoke-security-group-ingress コマンドまたは revoke-security-group-egress コマンドを使用してそれらのルールを削除できます。

AWS Transit Gateway 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、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. Transit Gateway 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。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. 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 アタッチメントを作成する”」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. Transit Gateway 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 を表示する”」を参照してください。

AWS Transit Gateway ネットワーク関数アタッチメント

ネットワーク関数アタッチメントを作成して、Transit Gateway を AWS Network Firewall に直接接続できます。これにより、検査 VPC を作成および管理する必要がなくなります。

ファイアウォールアタッチメントを使用すると、AWS は背後で必要なすべてのリソースを自動的にプロビジョニングおよび管理します。個々のファイアウォールエンドポイントではなく、新しい Transit Gateway アタッチメントを表示します。これにより、一元化されたネットワークトラフィック検査を実装するプロセスが簡素化されます。

ファイアウォールアタッチメントを使用する前に、まず AWS Network Firewall でアタッチメントを作成する必要があります。アタッチメントを作成する手順については、「AWS Network Firewall デベロッパーガイド」の「AWS Network Firewall 管理の開始方法」を参照してください。ファイアウォールの作成後、[アタッチメント] セクションの Transit Gateway コンソールでアタッチメントを表示できます。アタッチメントは、[ネットワーク関数] のタイプとともに表示されます。

トピック

- AWS Transit Gateway ネットワーク関数アタッチメントを承諾または拒否する
- AWS Transit Gateway ネットワーク関数のアタッチメントを表示する
- AWS Transit Gateway ネットワーク関数アタッチメントを介してトラフィックをルーティングする

AWS Transit Gateway ネットワーク関数アタッチメントを承諾または拒否する

Amazon VPC コンソール、CLI、または API AWS Network Firewall のいずれかを使用して、Network Firewall アタッチメントを含むトランジットゲートウェイネットワーク関数アタッチメントを承諾または拒否できます。Transit Gateway の所有者で、別のアカウントから Transit Gateway にファイアウォールアタッチメントを作成している場合は、アタッチメントリクエストを承諾または拒否する必要があります。

Network Firewall CLI を使用してネットワーク関数アタッチメントを承諾または拒否するには、「AWS Network Firewall APIリファレンス」の `AcceptNetworkFirewallTransitGatewayAttachment` または `RejectNetworkFirewallTransitGatewayAttachment` API を参照してください。

コンソールを使用してネットワーク関数アタッチメントを承諾または拒否する

Amazon VPC コンソールを使用して、Transit Gateway ネットワーク関数アタッチメントを承諾または拒否します。

コンソールを使用してネットワーク関数アタッチメントを承諾または拒否するには

1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
2. ナビゲーションペインで、[Transit Gateway] を選択します。
3. [Transit Gateway アタッチメント] を選択します。
4. [承諾保留中] の状態と [ネットワーク関数] のタイプを持つアタッチメントを選択します。

5. [アクション] を選択し、[アタッチメントを承諾] または [アタッチメントを拒否] を選択します。
6. 確認のダイアログボックスで、[承諾] または [拒否]を選択します。

アタッチメントを承諾すると、アタッチメントはアクティブになり、ファイアウォールはトラフィックを検査できます。アタッチメントを拒否すると、拒否状態になり、最終的に削除されます。

AWS Transit Gateway ネットワーク関数のアタッチメントを表示する

Amazon VPC コンソールまたは Network Manager コンソールを使用して、アタッチメントを含むネットワーク関数の AWS Network Firewall アタッチメントを表示し、ネットワークトポロジを視覚的に表現できます。

Network Manager コンソールを使用してネットワーク関数アタッチメントを表示する

Network Manager コンソールを使用して、ネットワーク関数のアタッチメントを表示できます。

Network Manager でファイアウォールアタッチメントを表示するには

1. https://console.aws.amazon.com/networkmanager/home/ で Network Manager コンソールを開きます。
2. まだ作成していない場合は、Network Manager でグローバルネットワークを作成します。
3. Transit Gateway を Network Manager に登録します。
4. [グローバルネットワーク] で、アタッチメントが配置されているグローバルネットワークを選択します。
5. ナビゲーションペインで、[Transit Gateway] を選択します。
6. アタッチメントを表示する Transit Gateway を選択します。
7. [トポロジーツリー] ビューを選択します。Network Firewall アタッチメントには、ネットワーク関数アイコンが表示されます。
8. 特定のファイアウォールアタッチメントの詳細を表示するには、トポロジービューで Transit Gateway を選択し、[ネットワーク関数] タブを選択します。

Network Manager コンソールには、ステータス、関連する Transit Gateway、アベイラビリティーゾーンなど、ファイアウォールアタッチメントに関する詳細情報が表示されます。

Amazon VPC コンソールを使用してネットワーク関数アタッチメントを表示する

VPC コンソールを使用して、Transit Gateway アタッチメントタイプのリストを表示します。

VPC コンソールを使用して Transit Gateway アタッチメントタイプを表示するには

- 「VPC アタッチメントを表示する」を参照してください。

AWS Transit Gateway ネットワーク関数アタッチメントを介してトラフィックをルーティングする

ネットワーク関数アタッチメントを作成したら、Transit Gateway ルートテーブルを更新して、Amazon VPC コンソールまたは CLI を使用して検査のためにファイアウォール経由でトラフィックを送信する必要があります。Transit Gateway ルートテーブルの関連付けを更新する手順については、「Transit Gateway ルートテーブルの関連付け」を参照してください。

コンソールを使用してファイアウォールアタッチメントを介してトラフィックをルーティングする

Amazon VPC コンソールのコンソールを使用して、Transit Gateway ネットワーク関数アタッチメントを介してトラフィックをルーティングします。

コンソールを使用してネットワーク関数アタッチメントを介してトラフィックをルーティングするには

1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
2. ナビゲーションペインで、[Transit Gateway] を選択します。
3. [Transit Gateway ルートテーブル] を選択します。
4. 変更するルートテーブルを選択します。
5. [アクション]、[静的ルートの作成] の順に選択します。
6. [CIDR] の場合は、ルートの送信先 CIDR ブロックを入力します。
7. [アタッチメント] で、ネットワーク関数のアタッチメントを選択します。たとえば、これは AWS Network Firewall 添付ファイルである場合があります。
8. [静的ルートの作成] を選択します。

> **Note**
>
> 静的ルートのみがサポートされています。

ルートテーブルの CIDR ブロックに一致するトラフィックは、検査のためにファイアウォールアタッチメントに送信されてから、最終送信先に転送されます。

CLI または API を使用してネットワーク関数アタッチメントを介してトラフィックをルーティングする

コマンドラインまたは API を使用して、Transit Gateway ネットワーク関数アタッチメントをルーティングします。

コマンドラインまたは API を使用してネットワーク関数アタッチメントを介してトラフィックをルーティングするには

- create-transit-gateway-route を使用します。

  例えば、リクエストはネットワークファイアウォールアタッチメントをルーティングすることです。

```
aws ec2 create-transit-gateway-route \
  --transit-gateway-route-table-id tgw-rtb-0123456789abcdef0 \
  --destination-cidr-block 0.0.0.0/0 \
  --transit-gateway-attachment-id tgw-attach-0123456789abcdef0
```

  その後、出力が次を返します。

```
{
  "Route": {
    "DestinationCidrBlock": "0.0.0.0/0",
    "TransitGatewayAttachments": [
      {
        "ResourceId": "network-firewall",
        "TransitGatewayAttachmentId": "tgw-attach-0123456789abcdef0",
        "ResourceType": "network-function"
      }
    ],
    "Type": "static",
    "State": "active"
  }
}
```

ルートテーブルの CIDR ブロックに一致するトラフィックは、検査のためにファイアウォールアタッチメントに送信されてから、最終送信先に転送されます。

AWS Site-to-Site VPN AWS Transit Gateway のアタッチメント

Site-to-Site VPN アタッチメントを AWS Transit Gateway のトランジットゲートウェイに接続して、VPCs とオンプレミスネットワークに接続できます。動的ルートと静的ルートの両方がサポートされ、IPv4 と IPv6 もサポートされています。

要件

- VPN 接続を Transit Gateway に接続するには、特定のデバイス要件を持つ VPN カスタマーゲートウェイを指定する必要があります。Site-to-Site VPN アタッチメントを作成する前に、カスタマーゲートウェイの要件を確認して、ゲートウェイが正しく設定されていることを確認します。ゲートウェイ構成ファイルの例を含むこれらの要件の詳細については、[AWS Site-to-Site VPN ユーザーガイド」の「Site-to-Site VPN 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、まずTransit Gateway のルート テーブルに静的ルートを追加する必要があります。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 によってフィルタリングされません。これにより、BGP ベースの VPN を使用するときに意図しないアウトバウンドトラフィックフローが許可される可能性があるためです。Transit Gateway ルートテーブルに静的ルートを追加する手順については、「静的ルートを作成する」を参照してください。

Amazon VPC コンソールまたは CLI を使用して、トランジットゲートウェイの Site-to-Site VPN AWS アタッチメントを作成、表示、または削除できます。

タスク

- Transit Gateway で VPN への AWS Transit Gateway アタッチメントを作成する
- AWS Transit Gateway で VPN アタッチメントを表示する
- AWS Transit Gateway で VPN アタッチメントを削除する

Transit Gateway で VPN への AWS Transit Gateway アタッチメントを作成する

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 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] コマンドを使用します。

AWS Transit Gateway で VPN アタッチメントを表示する

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 アタッチメントを表示するには AWS CLI

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

AWS Transit Gateway で VPN アタッチメントを削除する

コンソールを使用して VPN 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. VPN アタッチメントを選択します。
4. VPN 接続のリソース ID を選択して、[VPN 接続] ページに移動します。
5. [Actions] で、[Delete] 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、[削除] を選択します。

を使用して VPN アタッチメントを削除するには AWS CLI

[delete-vpn-connection] コマンドを使用します。

AWS Transit Gateway の VPN コンセントレータアタッチメント

AWS Site-to-Site VPN Concentrator は、分散企業のマルチサイト接続を簡素化する新機能です。VPN コンセントレータは、25 以上のリモートサイトを に接続し AWS、各サイトに低帯域幅 (100 Mbps 未満) が必要なお客様に適しています。

VPN コンセントレータの仕組み

VPN コンセントレータはトランジットゲートウェイに単一のアタッチメントとして表示されますが、複数の Site-to-Site VPN 接続をホストできます。

Concentrator 上のすべての VPN 接続からのトラフィックは、同じ Transit Gateway アタッチメントを介してルーティングされるため、接続されているすべてのサイトに一貫したルーティングポリシーとセキュリティルールを適用できます。Concentrator はトランジットゲートウェイルートテーブルとシームレスに統合されるため、リモートサイトと VPCs、他の VPN 接続、ピアリング接続などの他のアタッチメント間のトラフィックフローを制御できます。

VPN コンセントレータの利点

- コストの最適化: 複数の低帯域幅 VPN 接続を単一のトランジットゲートウェイアタッチメントに統合することでコストを削減します。特に、個々のサイトが完全な VPN アタッチメント容量を必要としない場合に便利です。
- 管理の簡素化: 個々の VPN 接続の制御とモニタリングを維持しながら、統合されたアタッチメントを通じて複数のリモートサイト接続を管理します。
- 一貫したルーティング: 単一の Transit Gateway ルートテーブルの関連付けを通じて、接続されているすべてのサイトに統一されたルーティングポリシーを適用します。
- スケーラブルなアーキテクチャ: 1 つのコンセントレータを使用して最大 100 のリモートサイトに接続し、トランジットゲートウェイあたり最大 5 つのコンセントレータをサポートします。
- 標準 VPN 機能: 各 VPN 接続は、標準の Site-to-Site VPN 接続と同じセキュリティ、モニタリング、ルーティング機能をサポートしています。

要件と制限事項

- BGP ルーティングのみ: VPN コンセントレータは BGP (動的) ルーティングのみをサポートします。静的ルーティングは起動時にサポートされていません。
- カスタマーゲートウェイの要件: 各リモートサイトには、BGP ルーティングをサポートするカスタマーゲートウェイが必要です。Concentrator で VPN 接続を作成する前に、AWS Site-to-Site VPN 「ユーザーガイド」のSite-to-Site VPN カスタマーゲートウェイデバイスの要件」でカスタマーゲートウェイの要件を確認してください。
- パフォーマンスに関する考慮事項: コンセントレータの各 VPN 接続は、最大 100 Mbps の帯域幅用に設計されています。より高い帯域幅要件については、標準の Transit Gateway VPN アタッチメントの使用を検討してください。

AWS VPC コンソールまたは AWS CLI を使用して、VPN コンセントレータアタッチメントを作成、表示、または削除できます。Concentrator の個々の VPN 接続は、標準の VPN 接続 APIsとコンソールインターフェイスを介して管理されます。

タスク

- AWS Transit Gateway で VPN コンセントレータアタッチメントを作成する
- AWS Transit Gateway で VPN コンセントレータアタッチメントを表示する
- AWS Transit Gateway で VPN コンセントレータアタッチメントを削除する

AWS Transit Gateway で VPN コンセントレータアタッチメントを作成する

前提条件

- アカウントに既存の Transit Gateway が必要です。

コンソールを使用して VPN コンセントレータアタッチメントを作成するには

1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
2. ナビゲーションペインで、Site-to-Site VPN コンセントレータを選択します。
3. Site-to-Site VPN コンセントレータの作成を選択します。
4. (オプション) Name タグに、Site-to-Site VPN Concentrator の名前を入力します。
5. Transit Gateway で、既存の Transit Gateway を選択します。
6. (オプション) 追加のタグを追加するには、新しいタグを追加を選択し、各タグのキーと値を指定します。
7. Site-to-Site VPN コンセントレータの作成を選択します。

VPN Concentrator アタッチメントを作成すると、リソースタイプが VPN Concentrator、初期状態が Pending のアタッチメントのリストに表示されます。アタッチメントの準備が完了すると、状態は Available に変わります。その後、このコンセントレータで Site-to-Site VPN 接続を作成できます。

を使用して VPN コンセントレータアタッチメントを作成するには AWS CLI

create-vpn-concentrator コマンドを使用します。

コンソールを使用して VPN コンセントレータで VPN 接続を作成するには

1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
2. ナビゲーションペインで、Site-to-Site VPN 接続を選択します。
3. [Create VPN connection] (VPN 接続の作成) を選択します。
4. ターゲットゲートウェイタイプで、Site-to-Site VPN コンセントレータを選択します。
5. Site-to-Site VPN Concentrator で、VPN 接続を作成する VPN Concentrator 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 BGP ルーティングをサポートしていることを確認します。
   - カスタマーゲートウェイを作成するには、[New (新規)] を選択します。IP アドレスには、カスタマーゲートウェイデバイスの静的パブリック IP アドレスを入力します。BGP ASN の場合は、カスタマーゲートウェイ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) を入力します。

     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。
7. ルーティングオプションでは、動的 (BGP が必要) が自動的に選択されます。VPN コンセントレータは、BGP を使用した動的ルーティングのみをサポートします。
8. 事前共有キーストレージの場合は、スタンダードまたは Secrets Manager を選択します。
9. トンネル帯域幅の場合、標準 が自動的に選択されます。VPN コンセントレータは、標準トンネル帯域幅のみをサポートします。
10. IP バージョン内のトンネルの場合は、IPv4 または IPv6 を選択します。
11. (オプション) アクセラレーションを有効にするを選択して、VPN トンネルのパフォーマンスを向上させます。
12. (オプション) ローカル IPv4 ネットワーク CIDR の場合は、IPv4 CIDR 範囲を指定します。
13. (オプション) リモート IPv4 ネットワーク CIDR の場合は、IPv4 CIDR 範囲を指定します。
14. 外部 IP アドレスタイプでは、パブリック IPv4 アドレスまたは IPv6 アドレスのいずれかを選択できます。
15. (オプション) トンネルオプションでは、トンネル IP アドレス内や事前共有キーなどのトンネル設定を構成できます。詳細については、「 AWS Site-to-Site VPN ユーザーガイド」のSite-to-Site VPN アーキテクチャ」を参照してください。

16. (オプション) 追加のタグを追加するには、新しいタグを追加を選択し、各タグのキーと値を指定します。
17. [Create VPN connection] (VPN 接続の作成) を選択します。

VPN 接続は、Transit Gateway ID 列の VPN Concentrator ID と初期状態が Pending の VPN 接続のリストに表示されます。VPN 接続の準備が完了すると、状態は Available に変わります。

を使用して VPN コンセントレータで VPN 接続を作成するには AWS CLI

create-vpn-connection コマンドを使用して、 `--vpn-concentrator-id`パラメータを使用して VPN コンセントレータ ID を指定します。

AWS Transit Gateway で VPN コンセントレータアタッチメントを表示する

コンソールを使用して VPN コンセントレータアタッチメントを表示するには

1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
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、VPN コンセントレータを探します。これらは VPN Concentrator 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。

コンソールを使用して VPN コンセントレータの VPN 接続を表示するには

1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
2. ナビゲーションペインで、Site-to-Site VPN 接続を選択します。
3. VPN 接続のリストで、Transit Gateway ID 列に VPN コンセントレータ ID を示す接続を識別します。これらは、VPN コンセントレータでホストされている VPN 接続です。
4. VPN 接続を選択して詳細を表示します。

を使用して VPN Concentrator アタッチメントを表示するには AWS CLI

describe-vpn-concentrator コマンドを使用して VPN Concentrator の詳細を表示するか、describe-transit-gateway-attachments コマンドをリソースタイプ のフィルターとともに使用しますvpn-concentrator。

を使用して VPN コンセントレータの VPN 接続を表示するには AWS CLI

のフィルターで describe-vpn-connections コマンドを使用して、特定の Concentrator に関連付けられた VPN 接続vpn-concentrator-idを表示します。

AWS Transit Gateway で VPN コンセントレータアタッチメントを削除する

前提条件

- VPN Concentrator アタッチメントを削除する前に、VPN Concentrator 上のすべての VPN 接続を削除する必要があります。
- VPN コンセントレータとそれに関連する VPN 接続の削除を考慮して、ルーティング設定を更新していることを確認します。

コンソールを使用して VPN コンセントレータの VPN 接続を削除するには

1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
2. ナビゲーションペインで、Site-to-Site VPN 接続を選択します。
3. トランジットゲートウェイ ID 列で VPN コンセントレータ ID を検索して、VPN コンセントレータに関連付けられた VPN 接続を特定します。
4. 削除する VPN 接続を選択します。
5. [Actions] で、[Delete] 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、[削除] を選択します。
7. VPN コンセントレータに関連付けられた VPN 接続ごとに、ステップ 4 ~ 6 を繰り返します。

コンソールを使用して VPN コンセントレータアタッチメントを削除するには

1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
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. 削除する VPN コンセントレータアタッチメントを選択します。このコンセントレータに関連付けられている VPN 接続がないことを確認します。
4. アクション、添付ファイル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、[削除] を選択してください。

VPN コンセントレータアタッチメントが削除状態になり、アカウントから削除されます。このプロセスが完了するまでに数分かかる場合があります。

を使用して VPN コンセントレータの VPN 接続を削除するには AWS CLI

VPN コンセントレータに関連付けられた VPN 接続ごとに delete-vpn-connection コマンドを使用します。

を使用して VPN コンセントレータアタッチメントを削除するには AWS CLI

すべての VPN 接続が削除されたら、delete-vpn-concentrator コマンドを使用します。

AWS Transit Gateway のクライアント VPN アタッチメント

クライアント VPN エンドポイントをトランジットゲートウェイに関連付けると、クライアント VPN アタッチメントが自動的に作成され、VPCs、オンプレミスネットワーク、クライアント VPN エンドポイント間でトラフィックをルーティングできます。 AWS Transit Gateway はクロスアカウントクライアント VPN アタッチメントをサポートし、トランジットゲートウェイが共有されているアカウントが独自のクライアント VPN アタッチメントを作成できるようにします。

クライアント VPN エンドポイントがトランジットゲートウェイに関連付けられていると、トランジットゲートウェイアタッチメントの Transit Gateway コンソールでアタッチメントを表示できます。アタッチメントは、クライアント VPN のタイプで一覧表示されます。

要件と制限事項

- クライアント VPN アタッチメントを作成する前に、トランジットゲートウェイに IPv4 または IPv6 CIDR ブロックを割り当てる必要があります。
- クライアント VPN エンドポイントとトランジットゲートウェイ間のトラフィックを許可するには、クライアント VPN アタッチメントでルートテーブルの伝播を有効にする必要があります。「ルート伝播を有効にする」を参照してください。

タスク

- AWS Transit Gateway でクライアント VPN アタッチメントを作成する
- AWS Transit Gateway でクライアント VPN アタッチメントを表示する
- AWS Transit Gateway でクライアント VPN アタッチメントを削除する
- AWS Transit Gateway でクライアント VPN アタッチメントを承諾または拒否する

AWS Transit Gateway でクライアント VPN アタッチメントを作成する

前提条件

- アカウントに既存の Transit Gateway が必要です。
- トランジットゲートウェイには、IPv4 または IPv6 CIDR ブロックが割り当てられている必要があります。

クライアント VPN エンドポイントをトランジットゲートウェイに関連付けると、クライアント VPN アタッチメントが自動的に作成されます。

コンソールを使用してクライアント VPN アタッチメントを作成するには

1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
2. ナビゲーションペインで、クライアント VPN エンドポイントを選択します。
3. [クライアント VPN エンドポイントの作成] を選択します。
4. 関連付けタイプとして Transit Gateway を選択し、使用する Transit Gateway ID を入力します。
5. [クライアント VPN エンドポイントの作成] を選択します。

クライアント VPN アタッチメントを作成すると、リソースタイプがクライアント VPN、初期状態が保留中のアタッチメントのリストに表示されます。アタッチメントの準備が完了すると、状態は Available に変わります。トランジットゲートウェイが別のアカウントにある場合、アタッチメントの状態は、トランジットゲートウェイの所有者がそれを受け入れるまで承認保留中です。

クライアント VPN エンドポイントの作成の詳細については、AWS 「クライアント VPN の開始方法」を参照してください。

を使用してクライアント VPN アタッチメントを作成するには AWS CLI

create-client-vpn-endpoint コマンドを使用します。

AWS Transit Gateway でクライアント VPN アタッチメントを表示する

コンソールを使用してクライアント VPN アタッチメントを表示するには

1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
2. ナビゲーションペインでTransit Gatewaysを選択します。
3. [Transit Gateway アタッチメント] を選択します。
4. リソースタイプ列で、クライアント VPN を探します。
5. 詳細を表示するには、アタッチメントを選択します。

を使用してクライアント VPN アタッチメントを表示するには AWS CLI

リソースタイプ のフィルタで describe-transit-gateway-attachments コマンドを使用しますclient-vpn。

AWS Transit Gateway でクライアント VPN アタッチメントを削除する

コンソールを使用してクライアント VPN アタッチメントを削除するには

1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
2. ナビゲーションペインでTransit Gatewaysを選択します。
3. [Transit Gateway アタッチメント] を選択します。
4. 削除するクライアント VPN アタッチメントを選択します。
5. アクション,Transit Gateway のアタッチメントの削除を選択します。
6. 確認を求められたら、「**delete**」を入力し、[削除] を選択します。

クライアント VPN アタッチメントが削除状態になり、アカウントから削除されます。このプロセスが完了するまでに時間がかかる場合があります。

を使用してクライアント VPN アタッチメントを削除するには AWS CLI

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

AWS Transit Gateway でクライアント VPN アタッチメントを承諾または拒否する

別のアカウントのクライアント VPN エンドポイントがトランジットゲートウェイにアタッチメントを作成する場合は、トラフィックが流れる前にアタッチメントリクエストを承認または拒否する必要があります。

コンソールを使用してクライアント VPN アタッチメントを承諾または拒否するには

1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
2. ナビゲーションペインでTransit Gatewaysを選択します。
3. [Transit Gateway アタッチメント] を選択します。
4. 承認保留中の状態とクライアント VPN のタイプを持つアタッチメントを選択します。
5. [アクション] を選択し、[アタッチメントを承諾] または [アタッチメントを拒否] を選択します。

6. 確認のダイアログボックスで、[承諾] または [拒否]を選択します。

アタッチメントを受け入れるとアクティブになり、 AWS Transit Gateway はクライアント VPN エンドポイントとの間のトラフィックの処理を開始します。アタッチメントを拒否すると、拒否状態になり、最終的に削除されます。

を使用してクライアント VPN アタッチメントを受け入れるには AWS CLI

accept-transit-gateway-client-vpn-attachment コマンドを使用します。

を使用してクライアント VPN アタッチメントを拒否するには AWS CLI

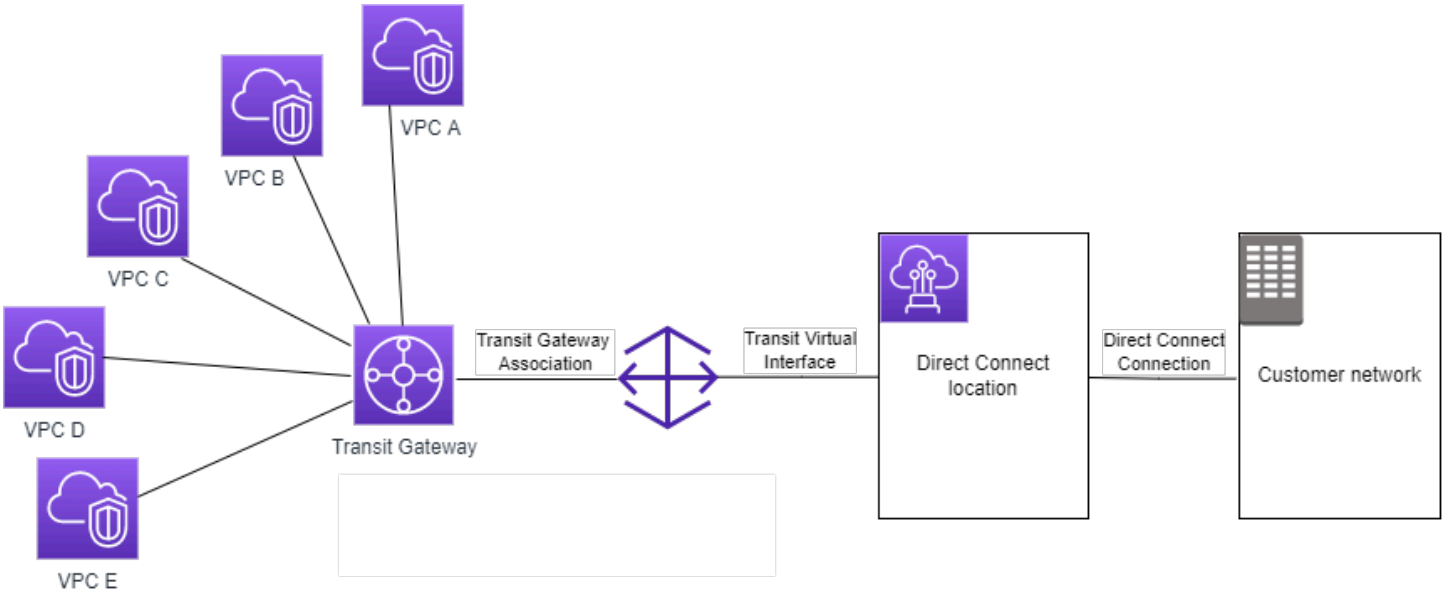
reject-transit-gateway-client-vpn-attachment コマンドを使用します。

AWS Transit Gateway の Direct Connect ゲートウェイへの Transit Gateway 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。

AWS Transit Gateway の 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 Transit Gateway は、アカウント内にあることも、別のアカウントからの場合もあります。自分のアカウントから別のアカウントの Transit Gateway にピアリングアタッチメントをリクエストすることもできます。

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。

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、「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。

タスク

- AWS Transit Gateway でピアリングアタッチメントを作成する

- AWS Transit Gateway のピアリングアタッチメントのリクエストを承諾または拒否します。
- Transit Gateway を使用して Transit Gateway AWS ルートテーブルにルートを追加する
- AWS Transit Gateway のピアリングアタッチメントを削除する

AWS Transit Gateway でピアリングアタッチメントを作成する

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承諾または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。共有されている Transit Gateway はピアリングに使用できません。
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。

AWS Transit Gateway のピアリングアタッチメントのリクエストを承諾または拒否します。

作成されると、Transit Gateway のピアリングアタッチメントは `pendingAcceptance` 状態で自動的に作成され、承諾または拒否されるまで永続的にこの状態を維持します。ピアリングアタッチメントをアクティブにするには、両方の Transit Gateway が同じアカウントにある場合でも、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承諾する必要があります。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、ピアリングアタッチメントを拒否する場合は、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 を使用して Transit Gateway AWS ルートテーブルにルートを追加する

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。

を使用して静的ルートを作成するには AWS CLI

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 ピアリングアタッチメントはTransit Gateway ルートテーブルにすでに関連付けられている必要があります。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。

AWS Transit Gateway のピアリングア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。

AWS Transit Gateway でアタッチメントとピアを接続する

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、オンマネージドインフラストラクチャを終了する 2 つの BGP AWS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推奨されるデュアル BGP ピアリングセッションを設定せずに動作している場合、 AWS インフラストラクチャオペレーション中に一時的に接続が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 アタッチメントをトランスポート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、「SD-WAN デバイスを AWS Transit Gateway と と統合 Direct Connectする」を参照してください。

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。

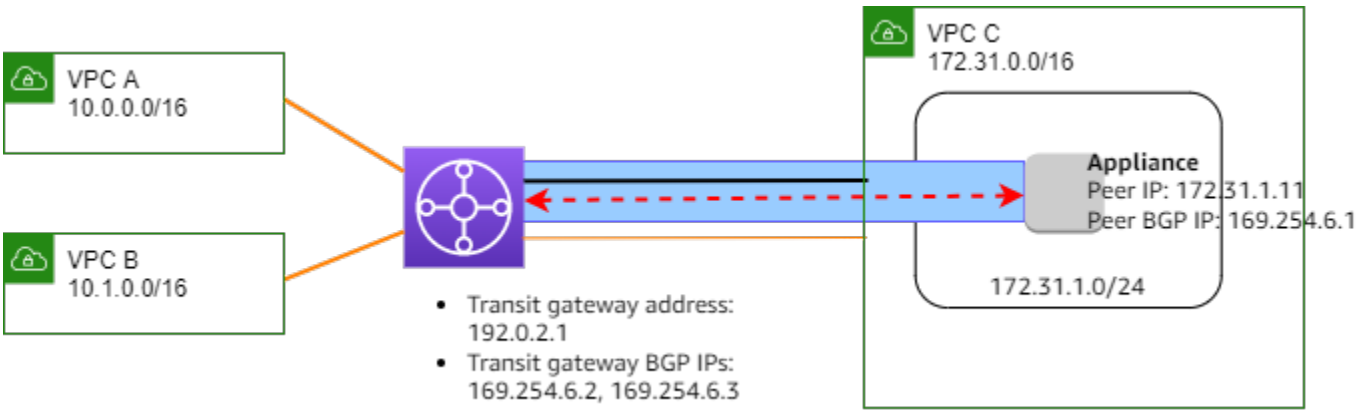
トランジットゲートウェイを作成または変更するときに、トランジットゲートウェイ CIDR ブロックを追加できます。

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。
- GRE ヘッダー (4 バイト) と外部 IP ヘッダー (20 バイト) のオーバーヘッドを引いて、外部インターフェイス MTU よりも小さくするように GRE トンネル MTU を設定します。例えば、外部インターフェイス MTU が 1500 バイトの場合、GRE トンネル MTU を 1476 バイト (1500 - 4 - 20 = 1476) に設定して、パケットの断片化を防止します。

タスク

- AWS Transit Gateway の Connect アタッチメントを作成する
- AWS Transit Gateway で Connect ピアを作成する
- AWS Transit Gateway で Connect アタッチメントと Connect ピアを表示する
- AWS Transit Gateway で Connect アタッチメントと Connect ピアタグを変更する
- AWS Transit Gateway で Connect ピアを削除する
- AWS Transit Gateway の Connect アタッチメントを削除する

AWS Transit Gateway の Connect アタッチメントを作成する

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。

AWS Transit Gateway で Connect ピアを作成する

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。

AWS Transit Gateway で 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 ピアを表示します。

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 コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
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。

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

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

AWS Transit Gateway で Connect アタッチメントと Connect ピアタグを変更する

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 コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
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. [保存] を選択します。

を使用して Connect アタッチメントと Connect ピアタグを変更するには AWS CLI

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

AWS Transit Gateway で 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。

AWS Transit Gateway の 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 の Transit Gateway AWS 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。ルートテーブルは、VPC と VPN 間でネットワークトラフィックがどのようにルーティングされるかを指示するルールを含むテーブルです。テーブル内の各ルートには、トラフィックを送信する送信先の IP アドレスの範囲が含まれます。

Transit Gateway ルートテーブルを使用すると、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。VPC、VPN、VPN Concentrator、クライアント VPN、Direct Connect ゲートウェイ、ピアリング、Connect アタッチメントはすべてサポートされています。関連付けると、これらのアタッチメントのルートはアタッチメントからターゲットの Transit Gateway ルートテーブルに伝播されます。アタッチメントは複数のルートテーブルに伝播できます。

さらに、ルートテーブルを使用して静的ルートを作成および管理できます。例えば、動的なルートに影響を与えるネットワーク中断が発生した場合に、バックアップルートとして使用される静的ルートがあるとします。

タスク

- AWS Transit Gateway で Transit Gateway ルートテーブルを作成する
- Transit Gateway を使用して Transit Gateway AWS ルートテーブルを表示する
- AWS Transit Gateway で Transit Gateway ルートテーブルを関連付ける
- Transit Gateway で Transit Gateway AWS ルートテーブルの関連付けを削除する
- AWS Transit Gateway で Transit Gateway ルートテーブルへのルート伝達を有効にする
- AWS Transit Gateway でルート伝播を無効にする
- AWS Transit Gateway で静的ルートを作成する
- AWS Transit Gateway で静的ルートを削除する
- AWS Transit Gateway で静的ルートを置き換える
- AWS Transit Gateway でルートテーブルを Amazon S3 にエクスポートする
- AWS Transit Gateway で Transit Gateway ルートテーブルを削除する
- AWS Transit Gateway でルートテーブルのプレフィックスリストリファレンスを作成する
- AWS Transit Gateway でプレフィックスリストリファレンスを変更する
- AWS Transit Gateway 内のプレフィックスリストリファレンスを削除する

AWS Transit Gateway で Transit Gateway ルートテーブルを作成する

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、Transit Gateway 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。

AWS CLI CLI を使用して Transit Gateway ルートテーブルを作成するには

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

Transit Gateway を使用して Transit Gateway AWS ルートテーブルを表示する

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 コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
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オンにするか、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 Transit Gateway 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のルートを表示するには AWS CLI

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

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 コマンドを使用します。

AWS Transit Gateway で Transit Gateway ルートテーブルを関連付ける

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、[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、[関連付けの作成 (関連付けの作成)] を選択します。

AWS CLI を使用して Transit Gateway ルートテーブルを関連付けるには

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

Transit Gateway で Transit Gateway AWS ルートテーブルの関連付けを削除する

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。

AWS Transit Gateway で Transit Gateway ルートテーブルへのルート伝達を有効にする

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達を有効にするには AWS CLI

[enable-transit-gateway-route-table-propagation] コマンドを使用します。

AWS Transit Gateway でルート伝播を無効にする

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、[伝播] タブを選択します。
5. アタッチメントを選択し、次に[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、[伝播の削除] を選択します。

AWS CLI を使用してルート伝達を無効にするには

[disable-transit-gateway-route-table-propagation] コマンドを使用します。

AWS Transit Gateway で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します。

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。

AWS CLI を使用して静的ルートまたはブラックホールルートを作成するには

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

AWS Transit Gateway で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します。

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。

AWS CLI を使用して静的ルートを削除するには

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

AWS Transit Gateway で静的ルートを置き換える

Transit Gateway ルートテーブル内の静的ルートを別の静的ルートに置き換えます。

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。

AWS CLI を使用してスタティックルートを置換します。

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

AWS Transit Gateway でルートテーブルを Amazon S3 にエクスポートする

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. [アクション]、[ルートのエクスポート] を選択します。

5. [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. [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"
      }
    ]
}
```

AWS Transit Gateway で Transit Gateway ルートテーブルを削除する

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。

AWS CLI を使用して Transit Gateway ルートテーブルを削除するには

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

AWS Transit Gateway でルートテーブルのプレフィックスリストリファレンスを作成する

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。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。

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リファレンスを作成] 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リファレンスを作成] 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。

AWS Transit Gateway でプレフィックスリストリファレンスを変更する

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リファレンスの変更] 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。

AWS Transit Gateway 内のプレフィックスリストリファレンスを削除する

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変更するには

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

AWS Transit Gateway の 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「ピアリング」を参照してください。

タスク

- Transit Gateway で Transit Gateway AWS ポリシーテーブルを作成する
- AWS Transit Gateway で Transit Gateway ポリシーテーブルを削除する

Transit Gateway で Transit Gateway AWS ポリシーテーブルを作成する

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 コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
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。

AWS Transit Gateway で Transit Gateway ポリシーテーブルを削除する

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 コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
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。

AWS Transit Gateway 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。

トピック

- マルチキャストの概念
- 考慮事項
- マルチキャストのルーティング
- AWS Transit Gateway のマルチキャストドメイン
- AWS Transit Gateway の共有マルチキャストドメイン
- AWS Transit Gateway でマルチキャストグループにソースを登録する
- AWS Transit Gateway でマルチキャストグループにメンバーを登録する
- AWS Transit Gateway でマルチキャストグループからソースを登録解除する

- AWS Transit Gateway でマルチキャストグループからメンバーを登録解除する
- AWS Transit Gateway でマルチキャストグループを表示する
- AWS Transit Gateway で Windows Server のマルチキャストを設定する
- 例: AWS Transit Gateway を使用して IGMP 設定を管理する
- 例: AWS Transit Gateway で静的ソース設定を管理する
- 例: AWS Transit Gateway で静的グループメンバー設定を管理する

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の参加、脱退、および送信を行うホストが含まれます。AWSは、IGMPv2 プロトコルと IGMP および静的 (API ベースの) グループメンバシップマルチキャストドメインの両方をサポートします。

- 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。AWS CLIを使用して、送信元および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

- Transit Gateway マルチキャストは、高頻度取引やパフォーマンス重視のアプリケーションには適していない場合があります。制限のマルチキャストクォータを確認することを強くお勧めします。パフォーマンス要件の詳細なレビューについては、アカウントまたはソリューションアーキテクトチームにお問い合わせください。
- サポートされるリージョンについては、 AWSTransit 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、Amazon Virtual Private Cloud Console、AWS CLI、または IGMP を使用して管理します。
- 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] チェックボックスを無効にする必要があります。詳細については、「Amazon EC2 ユーザーガイド」の「送信元または送信先チェックの変更」を参照してください。
- 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。
- マルチキャストのルーティングは、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Transit Gateway 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、クエリ対象リストからメンバーを完全に削除する前に、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、AWS Transit Gateway 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。

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
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のルール」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
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

AWS Transit Gateway のマルチキャストドメイン

マルチキャストドメインを使用すると、マルチキャストネットワークを異なるドメインに分割できます。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。

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。 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。

属性	説明
	• 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送信元を静的に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。

AWS Transit Gateway で 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 “マルチキャストドメイン”」を参照してください。

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 サポート] では、チェックボックスをオンにします。
7. [静的な送信元のサポート] では、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。

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
```

AWS Transit Gateway で静的ソース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 “マルチキャストドメイン”」を参照してください。

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. [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 サポート] では、チェックボックスをオフにします。
7. [静的な送信元のサポート] では、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、[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。

AWS CLI 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

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
```

AWS Transit Gateway での VPC アタッチメントとサブネットのマルチキャストドメインへの関連付け

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、「AWS Transit Gateway の Amazon VPC アタッチメント」を参照してください。

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. [アソシエーションを作成する] を選択してください。

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。

AWS Transit Gateway でマルチキャストドメインから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。

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. [関連付] 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。

AWS CLI を使用して、サブネットの関連付けを解除するには

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

AWS Transit Gateway で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します。

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。

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。

AWS Transit Gateway 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。

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. [Save] (保存) を選択します。

AWS CLI 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

create-tags コマンドを使用します。

AWS Transit Gateway で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。

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、[アクション] 、[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。

AWS CLI を使用してマルチキャストドメインを削除するには

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

AWS Transit Gateway の共有マルチキャストドメイン

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。

- AWS 組織内または の組織全体の 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
- AWS の外部にある アカウント AWS Organizations。

  マルチキャストドメインを Organization 外の AWS アカウントと共有するには、 を使用してリソース共有を作成し AWS Resource Access Manager、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任意のユーザーとの共有を許可するを選択する必要があります。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

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、 AWS アカウントでドメインを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。
- マルチキャストドメインを の組織または組織単位と共有するには AWS Organizations、 との共有を有効にする必要があります AWS Organizations。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。

関連サービス

マルチキャストドメイン共有は AWS Resource Access Manager () と統合されますAWS RAM。AWS RAM は、任意の AWS アカウントまたは を通じて AWS リソースを共有できるサービスです

AWS Organizations。 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、それらを共有するユーザーを指定します。コンシューマーは、個々の AWS アカウント、組織単位、または組織全体にすることができます AWS Organizations。

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

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で作成するリソースを表示、変更、削除できます。

コンシューマーのアクセス許可

共有マルチキャスト ドメインのユーザーは、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、所有者および共有ユーザ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。

AWS Transit Gateway のアベイラビリティーゾーン間でリソースを共有する

リソースがリージョンのアベイラビリティーゾーンに分散されるように、 AWS Transit Gateway はのアベイラビリティーゾーンを各アカウントの名前に個別にマッピングします。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 AWS アカウントのアベイラビリティーゾーンがus-east-1a別の AWS アカウントと同じ場所ではない場合があります。

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 アカウントにわたるアベイラビリティーゾーンの一意で一貫した識別子です。たとえば、 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です。

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. https://console.aws.amazon.com/ram/home で AWS RAM コンソールを開きます。
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。

AWS Transit Gateway でマルチキャストドメインを共有する

所有者がマルチキャストドメインを共有する場合、次の操作を実行できます。

- 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

> **Note**
>
> 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。リソース共有は、 AWS アカウント間で AWS RAM リソースを共有できる 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。を使用してマルチキャストドメインを共有する場合は Amazon Virtual Private Cloud Console、既存のリソース共有に追加します。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。
> の組織に属 AWS Organizations していて、組織内での共有が有効になっている場合、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権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 コンソール、 AWS RAM コンソール、または 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 AWS CLI。

*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。

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 CLI

create-resource-share コマンドを使用します。

AWS Transit Gateway で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。これを行うには、 AWS RAM コンソールまたは を使用します AWS CLI。

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、、 AWS RAM コンソール、または を使用します AWS CLI。

*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。

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 CLI

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

AWS Transit Gateway で共有マルチキャストドメインを特定する

所有者とコンシューマーは、 Amazon Virtual Private Cloud と を使用して共有マルチキャストドメインを識別できます。 AWS CLI

*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. トランジットマルチキャストドメインの詳細ページで、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。

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 AWS CLI

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

AWS Transit Gateway で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

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。

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。

AWS Transit Gateway で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

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。

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。

AWS Transit Gateway で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。

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、[ソースを削除] を選択します。

AWS CLI を使用して、ソースを削除するには

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

AWS Transit Gateway で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。

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。

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。

AWS Transit Gateway で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 (コンソール内) 、または `MemberType` (内 AWS CLI) は、プロトコルでメンバー AWS を検出したときに IGMP を表示します。

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。

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"
        }
    ]
}
```

AWS Transit Gateway で Windows Server のマルチキャストを設定する

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。これをセットアップするには、PowerShell を使用し、次のコマンドを実行する必要があります。

PowerShell を使用して Windows Server のマルチキャストを設定するには

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 Value は 3 である必要があります。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 に設定することができます。

```
    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。

例: AWS Transit Gateway を使用して IGMP 設定を管理する

この例では、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 つ表示されます。 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、IGMP 以外の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。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。詳細については、「Amazon VPC ユーザーガイド」の「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 アタッチメントを作成する”」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。

例: AWS Transit Gateway で静的ソース設定を管理する

この例では、マルチキャストソースをグループに静的に追加します。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。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。詳細については、「Amazon VPC ユーザーガイド」の「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 アタッチメントを作成する”」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。

例: AWS Transit Gateway で静的グループメンバー設定を管理する

この例では、グループにマルチキャストメンバーを静的に追加しています。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。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。詳細については、「Amazon VPC ユーザーガイド」の「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 アタッチメントを作成する”」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。

柔軟なコスト配分

デフォルトでは、Transit Gateway は送信者ベースのコスト配分モデルを使用して、ソースアタッチメントを所有するアカウントにデータ処理料金が割り当てられます。アタッチメントタイプ、特定のアタッチメント IDs、ネットワークアドレスなどのトラフィックフロープロパティに基づいて課金するアカウントを定義するカスタム計測ポリシーを作成できます。

計測ポリシーは、ルール番号の最小値から最大値まで評価される順序付けられたルールで構成されます。トラフィックがルールに一致すると、指定されたアカウントはルールの設定に従って課金されます。以下のオプションから、コストを割り当てるアカウント所有者を指定できます。

- ソースアタッチメント所有者 - 料金はソースアタッチメントを所有するアカウントに割り当てられます (デフォルトの動作)
- 送信先アタッチメント所有者 - 料金は送信先アタッチメントを所有するアカウントに割り当てられます
- トランジットゲートウェイ所有者 - 料金はトランジットゲートウェイを所有するアカウントに割り当てられます

Flexible Cost Allocation を使用すると、一元化されたネットワークアーキテクチャを使用する組織のコスト管理が改善され、ネットワークトポロジーに関係なく、適切なビジネスユニットまたはアプリケーション所有者にコストを割り当てることができます。

> **Note**
>
> Flexible Cost Allocation を使用すると、計測使用量とコストを任意のアカウント所有者に柔軟に割り当てることができます。ただし、 AWS アカウントの税への影響は、地理的な場所、使用パターン、その他の要因によって大きく異なる場合があります。この機能を有効にする前に、 AWS 組織内のアカウントの請求、税金、コスト管理への影響を確認してください。リファレンス: Billing AWS and Cost Management とは

計測ポリシー

計測ポリシーを使用すると、トランジットゲートウェイのコスト配分ルールを設定して、トラフィックフロープロパティに基づいてデータ処理と転送コストに課金されるアカウントを制御できます。この機能により、一元化されたネットワークアーキテクチャを使用する組織のコスト管理とチャージバック機能が向上します。

計測ポリシーは、以下で構成されます。

- 計測ポリシー - 計測ポリシールールを含む全体的な設定コンテナ。作成時に、ソースアタッチメント所有者へのすべてのトラフィックを課金するように設定されたデフォルトの計測ポリシーエントリが 1 つ含まれます。各トランジットゲートウェイには、1 つの計測ポリシーのみを含めることができます。
- 計測ポリシーエントリ - 特定の一致基準と使用量を計測するアカウントを定義する計測ポリシー内の個々のルール。各エントリには、評価順序のルール番号、トラフィック一致条件 (送信元と送信先のアタッチメントタイプ、アタッチメント IDs、CIDR ブロック、ポート、プロトコルなど) 、および一致するトラフィックに対して課金するアカウント所有者が含まれます。ポリシーには最大 50 個のエントリを含めることができ、ルール番号の順に評価されます。

  計測使用量は、次のいずれかに割り当てることができます。

  - ソースアタッチメント所有者: トラフィックが発生するアタッチメントを所有するアカウントに計測使用量を割り当てます (デフォルトの動作)
  - 送信先アタッチメント所有者: トラフィックが終了するアタッチメントを所有するアカウントに計測使用量を割り当てます。

- トランジットゲートウェイ所有者: トランジットゲートウェイを所有するアカウントに計測使用量を割り当てます。
- ミドルボックスアタッチメント - (オプション) セキュリティ検査、負荷分散、またはその他のネットワーク機能のためにネットワークアプライアンスを介してトラフィックをルーティングする指定のトランジットゲートウェイアタッチメント。ミドルボックスアタッチメントを通過するトラフィックのデータ使用量は、計測ポリシーで指定されたアカウント所有者に計測されます。最大 10 個のミドルボックスアタッチメントを指定できます。サポートされているミドルボックスアタッチメントタイプは、Network Function (AWS Network Firewall)、VPC、VPN アタッチメントです。

計測ポリシーの仕組み

デフォルトでは、Transit Gateway は送信者ベースのコスト配分モデルを使用し、データ処理料金はソースアタッチメントを所有するアカウントに対して計測されます。計測ポリシーを使用すると、次のトラフィックフロープロパティに基づいて使用量を柔軟に計測するカスタムルールを作成できます。

- 送信元と送信先のアタッチメントタイプ (VPC、VPN、クライアント VPN、Direct Connect Gateway、ピアリング、ネットワーク関数、VPN コンセントレータ)
- 送信元と送信先のアタッチメント IDs
- 送信元と送信先の IP アドレス、ポート範囲とプロトコル

計測ポリシーは、ルール番号の最小値から最大値まで評価される順序付けられたルールで構成されます。トラフィックがルールに一致すると、指定されたアカウントはルールの従量制アカウント設定に従って課金されます。計測ポリシーは、いくつかの一般的な組織シナリオに対処します。

- ハイブリッド環境のコスト配分: Direct Connect Gateway 経由でオンプレミス AWS から入力するデータのコストを、中央の IT 管理者アカウントの所有者ではなく、宛先 VPC アカウントの所有者に配分します。
- 一元化された検査アーキテクチャ: 検査 VPC を介したトラフィックトラバースについて、中央セキュリティチームではなく、個々のアプリケーションまたは VPCs。
- アプリケーションベースのチャージバック: トラフィックの方向に関係なく、ワークロードのすべてのデータ使用コストを VPC 所有者に割り当てます。
- クライアントコスト配分: クライアントアカウントが Transit Gateway へのアタッチメントを作成するときに、データコストをクライアントアカウントに割り当てます。

ミドルボックスアタッチメント

トランジットゲートウェイ計測ポリシーは、ミドルボックスアタッチメントをサポートしているため、ネットワークファイアウォールやロードバランサーなどのミドルボックスアプライアンスを介してルーティングされるネットワークトラフィックのデータ処理料金を柔軟に割り当てることができます。ミドルボックスアタッチメントの例としては、Network Firewall への AWS Network Function アタッチメントや、VPC 内のサードパーティーのセキュリティアプライアンスにトラフィックをルーティングする VPC アタッチメントなどがあります。送信元と送信先のトランジットゲートウェイアタッチメント間のトラフィックは、一般的なセキュリティ検査のユースケースのために、これらのミドルボックスアタッチメントを経由します。計測ポリシーを定義して、元のソースアタッチメント、最終送信先アタッチメント、または Transit Gateway アカウント所有者へのミドルボックスアタッチメントのデータ処理使用量を柔軟に割り当てることができます。Network Function アタッチメントの場合、 AWS Network Firewall データ処理料金も計測対象アカウントに割り当てられます。

Flexible Cost Allocation - Metering の使用タイプ

計測ポリシーによる柔軟なコスト配分は、次のデータ使用タイプに適用されます。

- VPC、VPN、クライアント VPN、VPN コンセントレータ、および Direct Connect アタッチメントでのトランジットゲートウェイデータ処理の使用
- クライアント VPN アタッチメントでのクライアント VPN データ転送出力の使用
- VPN アタッチメントでのSite-to-site VPN データ転送の使用
- Direct Connect アタッチメントでの Direct Connect Data Transfer Out の使用。
- TGW ピアリングアタッチメントでのデータ転送の使用
- トランジットゲートウェイ Network Function アタッチメントでのデータ処理の使用
- AWS Network Function アタッチメントでの Network Firewall (NFW) データ処理の使用。

柔軟なコスト配分は、アタッチメントの時間単位の使用とマルチキャストデータ処理の使用には適用されません。Transit Gateway Connect アタッチメントの場合、基盤となるトランスポート VPC または Direct Connect アタッチメントに計測ポリシーを定義できます。プライベート IP VPN アタッチメントの場合、基盤となるトランスポート Direct Connect アタッチメントに計測ポリシーを定義できます。

考慮事項と制限事項

トランジットゲートウェイに計測ポリシーを実装する場合は、次の点を考慮してください。

アクセス許可

- トランジットゲートウェイ所有者のみが計測ポリシーを作成、変更、または削除できます。
- コスト配分設定は、トランジットゲートウェイレベルに適用されます。
- アタッチメント所有者は、トランジットゲートウェイ所有者によって設定されたコスト配分設定を上書きすることはできません。

トランジットゲートウェイピアリング

トラフィックがトランジットゲートウェイピアリング接続を通過する場合:

- 各トランジットゲートウェイは、独自の計測ポリシーを個別に適用します。
- データ料金は、ローカルポリシーに基づいて各トランジットゲートウェイによって個別に割り当てられます。
- トラフィックは、ソースアタッチメントからピアリング、および宛先アタッチメントへのピアリングの 2 つの異なるフローと考えることができます。

クラウド WAN 統合

トランジットゲートウェイが Cloud WAN コアネットワークにアタッチされている場合:

- ピアリング接続のトランジットゲートウェイデータ転送料金は、トランジットゲートウェイの計測ポリシーに従って割り当てられます。
- 計測ポリシーは、クラウド WAN コアネットワークではサポートされていません。

パフォーマンスへの影響

- 計測ポリシーでは、追加のデータパスレイテンシーは発生しません。
- 計測ポリシーは、アタッチメントあたりの最大帯域幅には影響しません。
- Transit Gateway リソース共有機能に変更はありません。

請求の統合

- コスト配分タグは、ビジネスユニット別にコストを整理するための計測ポリシーと引き続き連携します。

- 計測ポリシーはコストが発生するアカウントを定義しますが、コスト配分タグはそれらのコストの分類に役立ちます。
- 計測ポリシーの変更は、次の請求時間の終了時に有効になります。

IPv6 サポート

計測ポリシーは、IPv4 トラフィックと IPv6 トラフィックの両方でサポートされています。ポリシーエントリの CIDR ブロックマッチングは、両方のアドレスファミリーで機能します。

ミドルボックスアタッチメントのサポート

- ミドルボックス計測ポリシーは、元の送信元アタッチメントと送信先アタッチメント間のトラフィックが、指定されたミドルボックスアタッチメント (VPC-to-VPCトラフィックの東西検査など) を介してヘアピン留めされていることを前提としています。したがって、ミドルボックスアタッチメントに出入りするフローのネットワーク 5 タプル (送信元/送信先 IPs、送信元/送信先ポート、プロトコル) は一致する必要があります。ミドルボックスアタッチメントに 5 タプルのミスマッチがあるフロー (検査 VPC での NAT 変換など) は、通常の送信元と送信先のアタッチメントフロー (ミドルボックスアタッチメントフローではなく) として扱われます。
- ミドルボックスアタッチメントのすべての出力専用フロー (検査 VPC の IGW 経由でインターネットへの南北トラフィックなど) は、通常の送信元/送信先フロー (ミドルボックスアタッチメントフローではなく) として扱われます。
- Network ファイアウォールがパケットを削除すると AWS 、Network Function アタッチメントの場合、計測ポリシーの設定に関係なく、すべてのデータ処理使用量が送信者アカウントに請求されます。

AWS Transit Gateway 計測ポリシーを作成する

計測ポリシーを有効にするには、トランジットゲートウェイの計測ポリシーを作成し、計測使用量の割り当て方法を定義するポリシーエントリを設定する必要があります。計測ポリシーはフレームワークとデフォルト設定を確立しますが、ポリシーエントリには、トラフィック特性に基づいて計測されるアカウントを決定する特定のルールが含まれています。

計測ポリシーエントリは、トランジットゲートウェイを通過するトラフィックのルール番号の最小値から最大値まで順番に適用される順序付けられたルールとして機能します。各エントリは、送信元と送信先のアタッチメントタイプ、CIDR ブロック、プロトコル、ポート範囲などの一致する条件と、一致するトラフィックを計測する必要があるアカウントを定義します。トラフィックフローが複数の

エントリと一致する場合、ルール番号が最も低いエントリが優先されます。特定のフローに一致するエントリがない場合、ポリシーで指定されたデフォルトの計測アカウントが課金されます。

ポリシーを作成したら、ポリシーエントリを追加してコスト配分ロジックを実装する必要があります。計測ポリシーエントリを作成する手順については、「」を参照してください計測ポリシーエントリを作成する。

コンソールを使用して計測ポリシーを作成する

Transit Gateway データ使用量の柔軟なコスト配分ルールを定義するポリシーを作成します。デフォルトでは、すべてのフローはソースアタッチメント所有者に計測されます。エントリを作成して、特定のネットワークフローを異なるアカウントに請求します。

計測ポリシーを作成するには

1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
2. ナビゲーションペインで、計測ポリシーを選択します。
3. 計測ポリシーの作成 を選択します。
4. トランジットゲートウェイ ID で、計測ポリシーを作成するトランジットゲートウェイを選択します。
5. (オプション) Middlebox アタッチメント IDs、1 つ以上のミドルボックスアタッチメントを選択します。デフォルトでは、データ使用量はミドルボックス所有者に計測されます。ミドルボックスアタッチメントのサポートにより、ミドルボックスアタッチメントを通過するトラフィックに計測ポリシーを適用できます。添付ファイルは後で追加できます。
6. (オプション) タグセクションで、計測ポリシーの識別と整理に役立つタグを追加します。
   a. [新しいタグを追加] をクリックします。
   b. タグキーと、オプションでタグ値を入力します。
   c. [新しいタグを追加] を選択してタグを追加するか、次のステップに進みます。最大 50 個のタグを追加できます。
7. Transit Gateway 計測ポリシーの作成を選択します。

> **Note**
>
> デフォルトの計測アカウントはソースアタッチメント所有者であり、計測ポリシーを作成した後、トラフィックフローのプロパティに基づいて課金されるアカウントを定義するエント

リを追加できます。デフォルトのポリシーエントリ (最後のエントリ) は、他のポリシーエントリと同様に変更または削除できないことに注意してください。

を使用して計測ポリシーを作成する AWS CLI

計測ポリシーは、トランジットゲートウェイのデフォルトのコスト配分動作とグローバル設定を定義します。create-transit-gateway-metering-policy を使用します。

必須パラメータ:

- `--transit-gateway-id` - ポリシーを作成するトランジットゲートウェイの ID

任意指定のパラメータ:

- `--middle-box-attachment-ids` - ミドルボックスとしてポリシーに追加する、サポートされている Transit Gateway アタッチメント ID
- `--tag-specifications` - 計測ポリシーのタグ

を使用して計測ポリシーを作成するには AWS CLI

1. create-transit-gateway-metering-policy コマンドを実行して、オプションのミドルボックスアタッチメントを使用して新しい計測ポリシーを作成します。

```
aws ec2 create-transit-gateway-metering-policy \
    --transit-gateway-id tgw-07a5946195a67dc47 \
    --middle-box-attachment-ids \
    tgw-attach-0123456789abcdef0 \
    tgw-attach-0abc123def456789a \
    --tag-specifications \
    '[{ "ResourceType": "transit-gateway-metering-policy", \
    "Tags": [ { "Key": "Env", "Value": "Prod" } ] }]'
```

   このコマンドは、指定されたトランジットゲートウェイの計測ポリシーを作成し、ミドルボックスのアタッチメントとタグを指定します。
2. コマンドは、ポリシーが正常に作成されると、次の出力を返します。

```
{
    "TransitGatewayMeteringPolicy": {
```

```
        "TransitGatewayMeteringPolicyId": "tgw-mp-042d444564d4b2da7",
        "TransitGatewayId": "tgw-07a5946195a67dc47",
        "MiddleboxAttachmentIds":  ["tgw-attach-0123456789abcdef0",
        "tgw-attach-0abc123def456789a"],
        "State": "pending",
        "UpdateEffectiveAt": "2025-11-05T21:00:00.000Z",
        "Tags": [{"Key": "Env","Value": "Prod"}]
    }
}
```

後続のコマンドで使用するためにレスポンスで返される計測ポリシー ID に注意してください。describe-transit-gateway-metering-policies コマンドを使用して、トランジットゲートウェイに関連付けられた計測ポリシーを取得できます。

AWS Transit Gateway 計測ポリシーの管理

計測ポリシーを作成したら、現在の設定の表示、設定オプションの変更、不要になったポリシーの削除によって管理できます。管理オペレーションでは、ネットワーク要件の変化に応じてミドルボックスアタッチメントを追加または削除できます。作成または削除できるのは、ポリシーエントリのみです。既存のルールを変更する必要がある場合は、エントリを削除し、変更された設定で新しいルールを作成できます。すべての管理オペレーションにはトランジットゲートウェイ所有者のアクセス許可が必要であり、2 請求時間後に有効になります。

ネットワークアーキテクチャの進化に合わせて正確なコスト配分を維持するには、効果的な計測ポリシー管理が不可欠です。多くの場合、組織は、ビジネスユニットの変更、新しいアプリケーションのデプロイ、またはネットワークトポロジの変更時にポリシーを調整する必要があります。たとえば、ミドルボックス計測のサポート設定では、ファイアウォールのセキュリティアーキテクチャが変更されたときや、新しい検査サービスがトラフィックパスに導入されたときに更新が必要になる場合があります。

ポリシーの変更は、季節的なトラフィックパターンの変更、合併と買収のアクティビティ、コンプライアンス要件の更新など、さまざまな運用シナリオをサポートします。ポリシーを管理するときは、既存の請求手配への影響を考慮し、実装前に影響を受ける利害関係者に変更を伝達します。

定期的なポリシーレビューは、コスト配分がビジネス目標と組織構造と一致していることを確認するのに役立ちます。ベストプラクティスには、ポリシーの変更の文書化、可能であれば非本番環境での変更のテスト、請求への影響を理解するための財務チームとの調整が含まれます。さらに、毎月の請求サイクルと財務報告プロセスの中断を最小限に抑えるために、ポリシー変更のタイミングを検討してください。

トピック

AWS Transit Gateway 計測ポリシーを編集する

既存の計測ポリシーを編集して、ミドルボックスアタッチメント設定を変更します。ポリシーの変更は次の請求時間に有効になり、トランジットゲートウェイを通過する今後のすべてのトラフィックフローに適用されます。

コンソールを使用して計測ポリシーを編集する

コンソールを使用して、トランジットゲートウェイの既存の計測ポリシー設定を変更します。

コンソールを使用して既存の計測ポリシーを編集するには

1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
2. ナビゲーションペインで、計測ポリシーを選択します。
3. ポリシー ID を選択して、変更する計測ポリシーを選択します。
4. アクションで使用可能なポリシー設定を変更します。コンソールでは、ミドルボックスアタッチメントの追加と削除のみが許可されます。
    - ミドルボックスアタッチメント - 特殊な請求用のミドルボックスとして扱う必要がある Transit Gateway アタッチメントを追加または削除します。

を使用して計測ポリシーを編集する AWS CLI

modify-transit-gateway-metering-policy コマンドを使用して、計測ポリシーを表示および変更します。

変更オペレーションに必要なパラメータ:

- `--transit-gateway-metering-policy-id` - 変更する計測ポリシーの ID
- `--add-middle-box-attachment-ids` または `--remove-middle-box-attachment-ids` - ミドルボックスとしてポリシーを追加または削除するためにサポートされている Transit Gateway アタッチメント ID

AWS CLI を使用して計測ポリシーを表示および編集するには

1. (オプション) describe-transit-gateway-metering-policies コマンドを使用して既存の計測ポリシーを表示し、現在の設定を確認します。

```
aws ec2 describe-transit-gateway-metering-policies
```

このコマンドは、アカウント内のすべての計測ポリシーを返し、現在の状態と、各計測ポリシーでミドルボックスとして有効になっている添付ファイルを表示します。

2. modify-transit-gateway-metering-policy コマンドを使用して計測ポリシーを変更し、設定オプションを更新します。

```
aws ec2 modify-transit-gateway-metering-policy \
    --transit-gateway-metering-policy-id tgw-mp-042d444564d4b2da7 \
    --add-middle-box-attachment-ids tgw-attach-0123456789abcdef1  \
    --remove-middle-box-attachment-ids tgw-attach-0abc123def456789a
```

このコマンドは、ミドルボックスアタッチメントを追加または削除することで、計測ポリシーを変更します。

3. このコマンドは、ポリシーが正常に変更されると、次の出力を返します。

```
{
    "TransitGatewayMeteringPolicy": {
        "TransitGatewayMeteringPolicyId": "tgw-mp-042d444564d4b2da7",
        "TransitGatewayId": "tgw-07a5946195a67dc47",
        "MiddleboxAttachmentIds":  ["tgw-attach-0123456789abcdef0",
        "tgw-attach-0123456789abcdef1"],
        "State": "modifying",
        "UpdateEffectiveAt": "2025-11-05T21:00:00.000Z"
    }
}
```

変更が有効になるまでに最大 2 請求時間かかる場合があります。

AWS Transit Gateway 計測ポリシーを削除する

トランジットゲートウェイのコスト配分戦略に不要になった計測ポリシーを削除します。ポリシーを削除すると、コスト配分がデフォルトの送信者ベースのモデルに戻されます。このモデルでは、デー

タ処理料金とデータ転送料金がソースアタッチメントを所有するアカウントに割り当てられます。削除された計測ポリシーに関連付けられているすべてのポリシーエントリも削除されます。

コンソールを使用して計測ポリシーを削除する

コンソールを使用して、不要になった計測ポリシーを削除します。

コンソールを使用して計測ポリシーを削除するには

1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
2. ナビゲーションペインで、計測ポリシーを選択します。
3. ポリシー ID を選択して、削除するポリシーを選択します。
4. [Actions] (アクション)、[Delete] (削除) の順に選択します。
5. 削除を確認するには、確認ダイアログ**delete**に と入力します。
6. [削除] を選択します。

> **Important**
> 計測ポリシーの削除は元に戻せません。すべてのポリシーエントリと設定は完全に削除され、コスト配分はデフォルトの送信者ベースのモデルに戻ります。

を使用して計測ポリシーを削除する AWS CLI

delete-transit-gateway-metering-policy コマンドを使用して、計測ポリシーをプログラムで削除します。

要件:

- トランジットゲートウェイ所有者のアクセス許可

必須パラメータ:

- `--transit-gateway-metering-policy-id` - 削除する計測ポリシーの ID

AWS CLI を使用して計測ポリシーを表示および削除するには

1. (オプション) describe-transit-gateway-metering-policies コマンドを使用して既存の計測ポリシーを表示し、現在の設定を確認します。

```
aws ec2 describe-transit-gateway-metering-policies
```

このコマンドは、アカウントのすべての計測ポリシーを返し、現在の状態と設定を表示します。

2. delete-transit-gateway-metering-policy コマンドを使用して計測ポリシーを削除し、ポリシーを完全に削除します。

```
aws ec2 delete-transit-gateway-metering-policy \
    --transit-gateway-metering-policy-id tgw-mp-042d444564d4b2da7
```

このコマンドは、指定された計測ポリシーと関連するすべてのエントリを完全に削除します。コスト配分は、将来のすべてのトラフィックフローのデフォルトの送信者ベースのモデルに戻ります。また、この変更が有効になるまでに 2 請求時間かかります。

3. このコマンドは、ポリシーが正常に削除されると、次の出力を返します。

```
{
    "TransitGatewayMeteringPolicy": {
        "TransitGatewayMeteringPolicyId": "tgw-mp-042d444564d4b2da7",
        "TransitGatewayId": "tgw-07a5946195a67dc47",
        "MiddleboxAttachmentIds":  ["tgw-attach-0123456789abcdef0",
        "tgw-attach-0123456789abcdef1"],
        "State": "deleting",
        "UpdateEffectiveAt": "2025-11-05T21:00:00.000Z"
    }
}
```

レスポンスは、トランジットゲートウェイインフラストラクチャ全体で削除が処理されている間、ポリシーが deleting状態で削除されていることを確認します。

AWS Transit Gateway 計測ポリシーエントリを作成する

デフォルトでは、すべてのフローはソースアタッチメント所有者に計測されます。異なるアカウントへの特定のフローを計測するには、トラフィックフローのプロパティに基づいて課金されるアカウントを定義する個別のポリシーエントリを作成します。

計測ポリシーエントリは、トラフィックがトランジットゲートウェイを通過するときにルール番号に基づいて順番に評価される条件付きルールとして機能します。各エントリは「if-then」ステートメントとして機能します。トラフィックが指定された条件 (ソースアタッチメントタイプ、送信先 CIDR ブロック、プロトコルなど) に一致する場合は、指定されたアカウントに課金されます。システムは、最も低いルール番号から最も高いルール番号までのエントリを評価し、最初に一致するエントリによって、そのトラフィックフローの請求アカウントが決まります。

エントリは、アタッチメントタイプ (VPC、VPN、クライアント VPN、Direct Connect Gateway、ピアリング、ネットワーク関数、VPN コンセントレータ) 、特定のアタッチメント IDs、送信元と送信先の CIDR ブロック、プロトコルタイプ、ポート範囲など、幅広い一致基準をサポートします。1 つのエントリ内に複数の条件を組み合わせて、正確なターゲティングルールを作成できます。たとえば、VPC アタッチメントからのすべての HTTPS トラフィック (ポート 443) を特定の送信先 CIDR 範囲に一致させ、それらのフローをセキュリティチームのアカウントに請求するエントリを作成できます。特定のトラフィックフローに一致するエントリがない場合、親計測ポリシーで指定されたデフォルトの計測アカウントが課金され、すべてのトラフィックが適切に請求されます。エントリの作成が有効になるまでに 2 請求時間かかります。

> **Important**
>
> - ルール番号を慎重に計画する - 将来の挿入を可能にするためにギャップ (10、20、30 など) を残す
> - より制限の厳しいルールを追加する前に、まずより具体的な条件でエントリをテストする
> - 特定の一致条件を使用して、意図しない請求を回避する

コンソールを使用して計測ポリシーエントリを作成する

計測ポリシーは、トランジットゲートウェイのデフォルトのコスト配分動作とグローバル設定を定義します。

コンソールを使用して計測ポリシーエントリを作成するには

1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
2. ナビゲーションペインで、計測ポリシーを選択します。
3. 計測ポリシー ID リンクを選択して詳細を表示します。
4. 計測ポリシーエントリタブを選択します。
5. 計測ポリシーの作成エントリを選択します。

6. ポリシールール番号 - 評価順序を決定する一意の番号 (1 ~ 32,766) である必要があります。数値が低いほど優先度が高くなります。
7. 従量制アカウント - 一致するトラフィックフローに対して課金される次のいずれかのアカウントタイプを選択します。
   a. ソース添付ファイル所有者
   b. 送信先添付ファイル所有者
   c. トランジットゲートウェイアタッチメント所有者
8. (オプション) ルール条件を選択する - これらのオプション条件は、特定のトラフィックに一致する条件を定義します。
   - ソースアタッチメントタイプまたは ID - アタッチメントタイプ (VPC、VPN、クライアント VPN、Direct Connect Gateway、ピアリング、ネットワーク関数、VPN コンセントレータ) または ID でフィルタリングします。
   - 送信先アタッチメントタイプまたは ID - 送信先アタッチメントタイプまたは ID でフィルタリングする
   - ソース CIDR ブロック - 特定の IP 範囲からのトラフィックを照合する
   - 送信先 CIDR ブロック - トラフィックを特定の IP 範囲に一致させる
   - ソースポート範囲 - 特定のソースポートを一致
   - 送信先ポート範囲 - 特定の送信先ポートと一致
   - プロトコル - ルールのプロトコルでフィルタリングする (1、6、17 など)
9. 計測ポリシーエントリの作成を選択して設定を保存します。

を使用して計測ポリシーエントリを作成する AWS CLI

ポリシーエントリは、トラフィックの特性に基づいてコスト配分の特定のルールを定義します。ルールは、ルール番号の順に評価されます。

必須パラメータ:

- `--transit-gateway-metering-policy-id` - エントリを追加する計測ポリシーの ID
- `--policy-rule-number` - 評価順序を決定する一意の数値 (1 ~ 32,766)
- `--metered-account` - 支払者タイプ (source-attachment-owner/ destination-attachment-owner/ transit-gateway-owner)

任意指定のパラメータ:

特定のトラフィックに一致する基準を定義する以下のオプションパラメータ。

- `--source-transit-gateway-attachment-id` - ソーストランジットゲートウェイアタッチメントの ID。
- `--source-transit-gateway-attachment-type` - ソーストランジットゲートウェイアタッチメントのタイプ。
- `--source-cidr-block` - ルールのソース CIDR ブロック。
- `--source-port-range` - ルールのソースポート範囲。
- `--destination-transit-gateway-attachment-id` - 送信先トランジットゲートウェイアタッチメントの ID。
- `--destination-transit-gateway-attachment-type` - 送信先トランジットゲートウェイアタッチメントのタイプ。
- `--destination-cidr-block` - ルールの送信先 CIDR ブロック。
- `--destination-port-range` - ルールの送信先ポート範囲。
- `--protocol` - ルールのプロトコル番号

を使用して計測ポリシーエントリを作成するには AWS CLI

1. create-transit-gateway-metering-policy-entry コマンドを使用して、VPC トラフィックを特定の計測アカウントにルーティングする新しいポリシーエントリを作成します。

```
aws ec2 create-transit-gateway-metering-policy-entry \
    --transit-gateway-metering-policy-id tgw-mp-042d444564d4b2da7 \
    --policy-rule-number 100 \
    --destination-transit-gateway-attachment-type vpc \
    --metered-account destination-attachment-owner
```

   このコマンドは、VPC アタッチメント宛てのトラフィックと一致するルール番号 100 のポリシーエントリを作成し、それらのフローの送信先アタッチメント所有者に課金します。

2. このコマンドは、エントリが正常に作成されると、次の出力を返します。

```
{
    "TransitGatewayMeteringPolicyEntry": {
        "MeteredAccount": "destination-attachment-owner",
```

```
        "MeteringPolicyRule": {
            "DestinationTransitGatewayAttachmentType": "vpc"
        },
        "PolicyRuleNumber": 100,
        "State": "available",
        "UpdateEffectiveAt": "2025-11-06T02:00:00.000Z"
    }
}
```

レスポンスは、トランジットゲートウェイインフラストラクチャ全体でアクティブ化されている間に、エントリが「使用可能」状態で作成されたことを確認します。

AWS Transit Gateway 計測ポリシーエントリを削除する

ネットワークトラフィックフローに特定のコスト配分ルールが不要になった場合は、計測ポリシーエントリを削除します。エントリの削除は、ポリシー構造全体を維持しながら、古いルールや不要なルールを削除することで、ポリシー管理を簡素化するのに役立ちます。エントリを削除すると、以前に削除されたルールに一致したトラフィックは、ルール番号の順序で残りのエントリと評価されるか、他のエントリが一致しない場合はデフォルトのポリシー動作に戻ります。

エントリを削除する前に、現在の請求手配とトラフィックフローへの影響を考慮してください。削除されると、変更が有効になるまでに最大 2 請求時間かかり、元に戻すことができないため、影響を受けるアカウント所有者や財務チームと変更を調整します。残りのエントリを確認して、削除後の適切なトラフィックカバレッジと請求配分を確認します。残りのエントリのルール評価順序は変更されず、継続的なトラフィックフローに対する予測可能なコスト配分動作が維持されます。

Important

- 削除は元に戻せません
- 以前にこのエントリに一致するトラフィックは、残りのエントリに対して再評価されます。
- 残りのエントリを確認して、適切なトラフィックカバレッジを確保する

コンソールを使用して計測ポリシーエントリを削除する

コンソールを使用して、誤って削除されないように確認ダイアログを提供する直感的なインターフェイスを介してポリシーエントリを削除します。

コンソールを使用してポリシーエントリを削除するには

1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
2. ナビゲーションペインで、計測ポリシーを選択します。
3. 削除するエントリを含む計測ポリシーを選択します。
4. 削除するエントリを選択し、削除を選択します。
5. 確認ダイアログで、エントリの詳細を確認して と入力**delete**し、削除を確認します。
6. 削除を選択して、エントリを完全に削除します。

を使用して計測ポリシーエントリを削除する AWS CLI

delete-transit-gateway-metering-policy-entry コマンドを使用して、プログラムでポリシーエントリを削除します。

要件:

- トランジットゲートウェイ所有者のアクセス許可
- 有効な計測ポリシー ID とエントリルール番号

必須パラメータ:

- `--transit-gateway-metering-policy-id` - 計測ポリシーの ID
- `--policy-rule-number` - 削除するエントリのルール番号

AWS CLI を使用してポリシーエントリを表示および削除するには

1. (オプション) get-transit-gateway-metering-policy-entries コマンドを使用して既存のポリシーエントリを表示し、現在の設定を確認します。

   ```
   aws ec2 get-transit-gateway-metering-policy-entries \
       --transit-gateway-metering-policy-id tgw-mp-0123456789abcdefg
   ```

   このコマンドは、指定されたポリシーのすべてのエントリを返し、ルール番号、一致基準、計測されたアカウントを表示します。
2. delete-transit-gateway-metering-policy-entry コマンドを使用してポリシーエントリを削除し、エントリを完全に削除します。

```
aws ec2 delete-transit-gateway-metering-policy-entry \
    --transit-gateway-metering-policy-id tgw-mp-0123456789abcdefg \
    --policy-rule-number 100
```

このコマンドは、指定されたエントリをポリシーから完全に削除します。以前にこのエントリに一致したトラフィックは、残りのエントリとすぐに再評価されるか、デフォルトのポリシー動作に戻ります。

3. エントリが正常に削除されると、 コマンドは次の出力を返します。

```
{
    "TransitGatewayMeteringPolicyEntry": [
        {
            "PolicyRuleNumber": 100,
            "MeteredAccount": "destination-attachment-owner",
            "UpdateEffectiveAt": "2024-01-01T01:00:00+00:00",
            "state": "deleted",
            "MeteringPolicyRule": {
                "DestinationTransitGatewayAttachmentType": "vpc"
            }
        }
}
```

レスポンスは、トランジットゲートウェイインフラストラクチャ全体で削除が処理されている間、エントリが「削除」状態で削除されていることを確認します。

AWS Transit Gateway 計測ポリシーのミドルボックスアタッチメントを管理する

トランジットゲートウェイ計測ポリシーは、ミドルボックスアタッチメントをサポートしているため、ネットワークファイアウォールやロードバランサーなどのミドルボックスアプライアンスを介してルーティングされるネットワークトラフィックのデータ処理料金を柔軟に割り当てることができます。ミドルボックスアタッチメントの例としては、Network Firewall への AWS Network Function アタッチメントや、VPC 内のサードパーティーのセキュリティアプライアンスにトラフィックをルーティングする VPC アタッチメントなどがあります。送信元と送信先のトランジットゲートウェイアタッチメント間のトラフィックは、一般的なセキュリティ検査のユースケースのために、これらのミドルボックスアタッチメントを経由します。計測ポリシーを定義して、元のソースアタッチメント、最終送信先アタッチメント、またはトランジットゲートウェイアカウントの所有者にミドルボッ

クスアタッチメントのデータ処理使用量を柔軟に割り当てることができます。Network Function アタッチメントの場合、 AWS Network Firewall データ処理料金も計測対象アカウントに割り当てられます。

セキュリティ検査、負荷分散、またはその他のネットワーク機能のためにネットワークアプライアンスを介してトラフィックをルーティングする指定のトランジットゲートウェイアタッチメント。ミドルボックスアタッチメントを通過するトラフィックのデータ使用量は、計測ポリシーで指定されたアカウント所有者に計測されます。最大 10 個のミドルボックスアタッチメントを指定できます。サポートされているミドルボックスアタッチメントタイプは、Network Function (AWS Network Firewall)、VPC、VPN アタッチメントです。

トピック

- AWS Transit Gateway 計測ポリシーのミドルボックスアタッチメントを追加する
- AWS Transit Gateway 計測ポリシーのミドルボックスアタッチメントを削除する

AWS Transit Gateway 計測ポリシーのミドルボックスアタッチメントを追加する

ミドルボックスアタッチメントを追加して、ネットワークアプライアンスを Transit Gateway 計測ポリシーに統合できます。これにより、きめ細かなコスト配分制御を維持しながら、セキュリティアプライアンス、ロードバランサー、またはその他のネットワーク機能を介して特定のトラフィックをルーティングできます。

Important

- ミドルボックスアプライアンスが正しく設定され、アクセス可能であることを確認する
- 本稼働ワークロードに適用する前にトラフィックルーティングをテストする
- レイテンシーが発生しないようにミドルボックスのパフォーマンスをモニタリングする
- 高可用性のために適切なフェイルオーバー動作を設定する

コンソールを使用してミドルボックスアタッチメントを追加する

ミドルボックスアタッチメントエントリを追加するには

1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
2. ナビゲーションペインで、計測ポリシーを選択します。
3. 計測ポリシー ID リンクを選択して詳細を表示します。

4. ミドルボックスアタッチメントタブを選択します。
5. [Add] (追加) を選択します。
6. プロンプトが表示されたら、特殊請求用のミドルボックスとして扱うミドルボックスアタッチメント IDs を選択します。最大 10 個のミドルボックスアタッチメントを選択できます。
7. ミドルボックスアタッチメントの追加を選択して設定を保存します。

を使用してミドルボックスアタッチメントを追加する AWS CLI

modify-transit-gateway-metering-policy コマンドを使用して添付ファイルを追加します。

開始する前に、次の必須パラメータがあることを確認してください。

- `--transit-gateway-metering-policy-id` - 既存の計測ポリシーの ID
- `--add-middle-box-attachment-ids` - ポリシーに追加する 1 つ以上の添付ファイル IDs (添付ファイルを追加する場合)

AWS CLI を使用して既存のポリシーにミドルボックスアタッチメントを追加するには

1. 次の例では、 modify-transit-gateway-metering-policyを使用して、既存の計測ポリシーに 4 つのミドルボックスアタッチメントを追加します。コマンドは、現在の添付ファイルを削除せずに、指定された添付ファイル IDsを既存のリストに追加します。

```
aws ec2 modify-transit-gateway-metering-policy \
    --transit-gateway-metering-policy-id tgw-mp-0123456789abcdefg \
    --add-middle-box-attachment-ids tgw-attach-0bdc681c211bf71f3 tgw-
attach-0987654321fedcba0 tgw-attach-0456789012345abcd tgw-attach-0fedcba0987654321
```

2. 次のレスポンス例では、JSON 出力に更新されたポリシー設定が表示され、4 つのミドルボックスアタッチメントがすべて含まれています。

```
{
    "TransitGatewayMeteringPolicy": {
        "TransitGatewayMeteringPolicyId": "tgw-mp-0123456789abcdefg",
        "TransitGatewayId": "tgw-0ecec6433f4bfe55a",
        "MiddleBoxAttachmentIds": [
            "tgw-attach-0bdc681c211bf71f3",
            "tgw-attach-0987654321fedcba0",
            "tgw-attach-0456789012345abcd",
            "tgw-attach-0fedcba0987654321"
```

```
        ],
        "State": "available",
        "UpdateEffectiveAt": "2024-09-05T16:00:00.000Z"
    }
}
```

AWS Transit Gateway 計測ポリシーのミドルボックスアタッチメントを削除する

デフォルトでは、計測コストはミドルボックスアタッチメント所有者に帰属します。ただし、これらの割り当てを変更して、トラフィックの実際の送信元または送信先にコストが適切に配分されるようにすることができます。計測ポリシーには、最大 10 個のミドルボックスアタッチメントを追加または削除できます。

コンソールを使用してミドルボックスアタッチメントを削除する

Amazon VPC コンソールを使用して、計測ポリシー設定からミドルボックスアタッチメントを削除します。

ミドルボックスアタッチメントを削除するには

1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
2. ナビゲーションペインで、トランジットゲートウェイ、計測ポリシーを選択します。
3. 変更する計測ポリシーを選択します。
4. ミドルボックスアタッチメントタブを選択します。
5. 計測ポリシーから削除するミドルボックスアタッチメントを最大 10 個選択します。
6. [を削除] を選択します。
7. プロンプトが表示されたら、選択したミドルボックスアタッチメントを更新して削除できます。削除されたアタッチメントを通過するトラフィックは、ミドルボックスアタッチメント所有者に計測されます。
8. ミドルボックスアタッチメントの削除を選択します。

を使用してミドルボックスアタッチメントを削除する AWS CLI

modify-transit-gateway-metering-policy コマンドを使用して添付ファイルを削除します。

開始する前に、次の必須パラメータがあることを確認してください。

- `--transit-gateway-metering-policy-id` - 既存の計測ポリシーの ID

- `--remove-middle-box-attachment-ids` - ポリシーから削除する 1 つ以上の添付ファイル IDs (添付ファイルの削除用)

AWS CLI を使用して既存のポリシーからミドルボックスアタッチメントを削除するには

1. 次の例では、 modify-transit-gateway-metering-policyを使用して、既存の計測ポリシーから 2 つの特定のミドルボックスアタッチメントを削除します。コマンドは、残りの添付ファイルを保持しながら、指定された添付ファイル IDs のみを削除します。

```
aws ec2 modify-transit-gateway-metering-policy \
    --transit-gateway-metering-policy-id tgw-mp-0123456789abcdefg \
    --remove-middle-box-attachment-ids tgw-attach-0456789012345abcd tgw-
attach-0fedcba0987654321
```

2. 次のレスポンス例では、JSON 出力に、指定された添付ファイルが削除され、残りの添付ファイルがまだアクティブな状態で更新されたポリシー設定が表示されます。

```
{
    "TransitGatewayMeteringPolicy": {
        "TransitGatewayMeteringPolicyId": "tgw-mp-0123456789abcdefg",
        "TransitGatewayId": "tgw-0ecec6433f4bfe55a",
        "MiddleBoxAttachmentIds": [
            "tgw-attach-0bdc681c211bf71f3",
            "tgw-attach-0987654321fedcba0"
        ],
        "State": "available",
        "UpdateEffectiveAt": "2024-09-05T16:00:00.000Z"
    }
}
```

AWS トランジットゲートウェイフローログ

トランジットゲートウェイフローログは AWS 、トランジットゲートウェイ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できる Transit Gateway の機能です。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**
>
> Transit Gateway フローログを作成するには、Transit Gateway の所有者である必要があります。ユーザーが所有者でない場合は、Transit Gateway の所有者からアクセス許可を付与する必要があります。

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。

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 Logs または Amazon S3 にも発行されません。フローログを削除しても、Transit Gateway の既存のフローログレコードやログストリーム (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 Logs 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、「AWS Transit Gateway フローログレコードを削除する」を参照してください。

CloudWatch Logs、Amazon S3、または Amazon Data Firehose にデータを発行できる Transit Gateway 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:

- CloudWatch Logs に発行するフローログの作成
- 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の作成

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、Transit Gateway 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 フローログは、アカウントごとにリソースごとに最大 250 のサブスクリプションをサポートします。この制限に達したリソースで追加のサブスクリプションを作成するには、まず既存のサブスクリプションを削除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	バージョン
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 TransitGateway になります。 Parquet データ型: STRING	6
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。	6

フィールド	説明	バージョン
	Parquet データ型: STRING	
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
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

フィールド	説明	バージョン
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_32	2
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

フィールド	説明	バージョン
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。 Parquet データ型: STRING	3
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	存続可能期間の満了によりパケットが失われました。 Parquet データ型: INT_64	6

フィールド	説明	バージョン
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

フィールド	説明	バージョン
flow-direction	トランジットゲートウェイ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
pkt-src-aws-service	ソース 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

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。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteFlowLogs",
        "ec2:CreateFlowLogs",
        "ec2:DescribeFlowLogs"
      ],
      "Resource": "*"
    }
  ]
}
```

発行先が CloudWatch Logs であるか Amazon S3 であるかにより、追加の IAM ロールとアクセス許可の設定が必要になります。詳細については、「AWS Amazon CloudWatch Logs のトランジットゲートウェイフローログレコード」および「AWS Amazon S3 の Transit Gateway フローログレコード」を参照してください。

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。提供されたログの発行に伴う料金の詳細については、「Amazon CloudWatch の料金」を開き、[有料利用枠] で [ログ] を選択して、[提供されたログ] を見つけます。

AWS Transit Gateway フローログの IAM ロールを作成または更新する

既存のロールを更新するか、次の手順を使用して、 AWS Identity and Access Management コンソール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. [信頼されたエンティティのタイプの選択] で、[AWS のサービス] 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] を選択します。
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] を選択してください。
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. 「CloudWatch Logs へのフローログ発行のための IAM 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。

AWS Amazon CloudWatch Logs のトランジットゲートウェイフローログレコード

フローログはフローログデータを直接 Amazon CloudWatch に発行できます。

フローログデータは、CloudWatch Logs に対して発行されるときはロググループに発行され、各 Transit Gateway 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、提供されたログに対するデータの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 では、[timestamp] フィールドはフローログレコードでキャプチャされた開始時刻に対応します。[ingestionTime] フィールドは、CloudWatch Logs によってフローログレコードが受

信された日時を示します。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です。

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

内容

CloudWatch Logs へのフローログ発行のための IAM ロール

フローログに関連付けられた IAM ロールには、CloudWatch Logs の指定されたロググループにフローログを発行するために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。

JSON

```
{
  "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。

JSON

```
{
  "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"
    }
}
```

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。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::111122223333:role/flow-log-role-name"
        }
    ]
}
```

が に発行する AWS Transit Gateway フローログレコードを作成する Amazon CloudWatch Logs

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。

Amazon CloudWatch AWS フローログを作成できます。

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 マネジメントコンソール 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、[CloudWatch ログへの送信] 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、ログを CloudWatch Logs に発行できるアクセス許可がある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-EC2FlowLog (AWS Tools for Windows PowerShell)

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 `my-flow-logs` を使用し、アカウント 123456789101 内で、`publishFlowLogs` と呼ばれる CloudWatch Logs 内のロググループに配信されます。

```
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
```

Amazon CloudWatch で AWS Transit Gateway 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 Logs 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. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) 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 CloudWatch Logs で AWS Transit Gateway フローログレコードを処理する

CloudWatch Logs で収集された他のログイベントのように、フローログレコードを操作できます。モニタリングログデータとメトリックフィルターの詳細については、「Amazon CloudWatch ユーザーガイド」の「フィルターを使用したログイベントからのメトリクスの作成」を参照してください。

例: フローログの CloudWatch メトリクスフィルターとアラームの作成

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. CloudWatch コンソールの https://console.aws.amazon.com/cloudwatch/ を開いてください。
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] を選択します。
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。

AWS Amazon S3 の Transit Gateway フローログレコード

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。

データ取り込みとアーカイブ Amazon CloudWatch の料金は、フローログを Amazon S3 に発行するときに、 によって提供されたログに適用されます。CloudWatch のVended Logs の料金情報の詳細については、「Amazon CloudWatch 料金表」を参照してください。[ログ]を選択すると、[Vended Logs] の下に価格が表示されます。

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 S3 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 Logs の詳細については、「Amazon CloudWatch Logs ユーザーガイド」の「Amazon S3 に送信されたログ」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。

JSON

```
{
  "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。この新しい自動生成されたポリシーは、元のポリシーに追加されます。

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」を参照してください。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::bucket_name/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
```

```
                    "aws:SourceArn": "arn:aws:logs:us-east-1:123456789012:*"
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": [
                "s3:GetBucketAcl"
            ],
            "Resource": "arn:aws:s3:::bucket_name",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:us-east-1:123456789012:*"
                }
            }
        }
    ]
}
```

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、これらのアクセス許可を 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。

> **Note**
>
> S3 バケットキーを使用すると、バケットレベルのキーを使用して Encrypt、GenerateDataKey、および Decrypt オペレーション AWS KMS の へのリクエストを減らすことで、 AWS Key Management Service (AWS KMS) リクエストのコストを節約できます。設計上、このバケットレベルのキーを利用する後続のリクエストでは、 AWS KMS API リクエストは発生せず、 AWS KMS キーポリシーに対するアクセスも検証されません。

```
{
    "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 の AWS Transit Gateway Flow Logs ソースアカウントロールを作成する

ソースアカウントから、 AWS Identity and Access Management コンソールでソース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 マネジメントコンソール 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 を選択してください。
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] を選択してください。
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] を選択します。

```
"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] を選択してください。

Amazon S3 に発行する AWS Transit Gateway フローログレコードを作成する

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。Amazon VPC コンソールまたは AWS CLI を使用して、Amazon S3 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 コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
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-EC2FlowLog (AWS Tools for Windows PowerShell)

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tgw-00112233344556677するフローログを作成し、フローログを という名前の 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 AWS Transit Gateway フローログレコードを表示する

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] では、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。

Amazon S3 で処理された AWS Transit Gateway フローログレコード

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。

AWS Amazon Data Firehose の Transit Gateway、Flow Logs レコード

トピック

- クロスアカウント配信のための IAM ロール
- Amazon Data Firehose の AWS Transit Gateway Flow Logs ソースアカウントロールを作成する
- Amazon Data Firehose の AWS Transit Gateway Flow Logs 送信先アカウントロールを作成する
- Amazon Data Firehose に発行する AWS Transit Gateway フローログレコードを作成する

フローログはフローログデータを直接 Firehose に発行できます。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 に発行すると、フローログデータは Firehose 配信ストリームにプレーンテキスト形式で発行されます。最初に、Firehose の配信ストリームを作成しておく必要があります。配信ストリーム作成の詳細については、「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

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] を参照してください。

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、ソースアカウントと送信先アカウントに IAM ロールをそれぞれ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。

JSON

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::111122223333:role/mySourceRole",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "delivery.logs.amazonaws.com"
                },
                "StringLike": {
                    "iam:AssociatedResourceARN": [
                        "arn:aws:ec2:us-east-1: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::111122223333: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。

JSON

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

送信先アカウントロール

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

JSON

```
{
  "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。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/mySourceRole"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Amazon Data Firehose の AWS Transit Gateway Flow Logs ソースアカウントロールを作成する

ソースアカウントから、 AWS Identity and Access Management コンソールでソース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 マネジメントコンソール 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 を選択してください。
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] を選択してください。

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] を選択します。

```
"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] を選択してください。

Amazon Data Firehose の AWS Transit Gateway Flow Logs 送信先アカウントロールを作成する

送信先アカウントから、 AWS Identity and Access Management コンソールで送信先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 マネジメントコンソール 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 を選択してください。
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. AWSLogDeliveryFirehoseCrossAccountRole で始まるポリシーの名前を入力し、[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 Roles (ロール) を選択してください。
6. [ロールの作成] を選択してください。

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] を選択します。

```
"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] を選択してください。

Amazon Data Firehose に発行する AWS Transit Gateway フローログレコードを作成する

Amazon Data Firehose に公開する Transit Gateway フローログを作成します。フローログを作成する前に、クロスアカウント配信のソース IAM アカウントロールと宛先 IAM アカウントロールを設定し、Firehose 配信ストリームを作成します。詳細については「Amazon Data Firehose のフローログ」を参照してください。Firehose フローログは、Amazon VPC コンソールまたは CLI AWS を使用して作成できます。

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

1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
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-EC2FlowLog (AWS Tools for Windows PowerShell)

次の CLI AWS 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、指定された Firehose 配信ストリームにフローログを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 CLI AWS 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
```

APIs または CLI を使用した AWS Transit Gateway フローログの作成と管理

このページで説明しているタスクは、コマンドラインを使用して実行できます。

create-flow-logs コマンドを使用する場合、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)

フローログの説明

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

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)

フローログの削除

- delete-flow-logs (AWS CLI)
- Remove-EC2FlowLog (AWS Tools for Windows PowerShell)

AWS Transit Gateway フローログレコードを表示する

Amazon VPC 経由で Transit Gateway フローログに関する情報を表示します。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 コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
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。

AWS Transit Gateway フローログタグの管理

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 コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
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。

AWS Transit Gateway フローログレコードの検索

CloudWatch Logs コンソールを使用して、CloudWatch Logs に発行されたフロー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。

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

1. CloudWatch コンソールの https://console.aws.amazon.com/cloudwatch/ を開いてください。
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]
```

AWS Transit Gateway フローログレコードを削除する

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、既存のログストリームは CloudWatch Logs から削除されず、ログファイルは Amazon S3 から削除されません。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 コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
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。

AWS Transit Gateway のメトリクスとイベント

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、「AWS Transit Gateway 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、「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。

CloudTrail ログ

を使用して AWS CloudTrail 、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、ログファイルとして Amazon S3 に保存できます。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、「CloudTrail ログ」を参照してください。

Network Manager を使用する CloudWatch イベント

を使用して CloudWatch にイベント AWS Network Manager を転送し、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。

AWS Transit Gateway の CloudWatch メトリクス

Amazon 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。

Amazon 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。

すべてのメトリクスは常に報告されます。これらの値は、Transit Gateway 経由のトラフィックによって異なります。サポートされているディメンションについては、「Transit Gateway のメトリクスディメンション」を参照してください。

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。 [Statistics] (統計): 唯一意味のある統計は `Sum` です。
`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。

メトリクス	説明
	[Statistics] (統計): 唯一意味のある統計は Sum です。
BytesIn	Transit Gateway あたりの受信バイト数。 [Statistics] (統計): 唯一意味のある統計は Sum です。
BytesOut	Transit Gateway からの送信バイト数。 [Statistics] (統計): 唯一意味のある統計は Sum です。
PacketsIn	Transit Gateway によって受信されたパケットの数。 [Statistics] (統計): 唯一意味のある統計は Sum です。
PacketsOut	Transit Gateway によって送信されたパケットの数。 [Statistics] (統計): 唯一意味のある統計は Sum です。
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。 [Statistics] (統計): 唯一意味のある統計は Sum です。
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。 [Statistics] (統計): 唯一意味のある統計は Sum です。
PacketDropCountTTLExpired	TTL の有効期限が切れたために削除されたパケットの数。 [Statistics] (統計): 唯一意味のある統計は Sum です。

アタッチメントレベルとアベイラビリティーゾーンのメトリクス

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。

アベイラビリティーゾーンメトリクスは、Transit Gateway アタッチメントのアベイラビリティーゾーン (AZ) に対して有効になっています。VPC アタッチメントのみが AZ ごとのメトリクスをサポートします。すべての AZ レベルメトリクスは、Transit Gateway 所有者のアカウントに発行されます。アタッチメントの各 AZ メトリクスも同様に、 アタッチメント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 AZ ごとのメトリクスのみを表示できます。

すべてのメトリクスは常に報告されます。これらの値は、Transit Gateway アタッチメントの内外のトラフィックによって異なります。サポートされているディメンションについては、「Transit Gateway のメトリクスディメンション」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。 [Statistics] (統計): 唯一意味のある統計は Sum です。
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。 [Statistics] (統計): 唯一意味のある統計は Sum です。
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。 [Statistics] (統計): 唯一意味のある統計は Sum です。
BytesOut	Transit Gateway からアタッチメントに送信されたバイト数。 [Statistics] (統計): 唯一意味のある統計は Sum です。
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。 [Statistics] (統計): 唯一意味のある統計は Sum です。
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。 [Statistics] (統計): 唯一意味のある統計は Sum です。

メトリクス	説明
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。 [Statistics] (統計): 唯一意味のある統計は Sum です。
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。 [Statistics] (統計): 唯一意味のある統計は Sum です。
PacketDropCountTTLExpired	TTL の有効期限が切れたために削除されたパケットの数。 [Statistics] (統計): 唯一意味のある統計は Sum です。

Transit Gateway のメトリクスディメンション

次のディメンションを使用して Transit Gateway メトリクスデータをフィルタリングします。

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。
TransitGateway , AvailabilityZone	Transit Gateway とアベイラビリティーゾーンの両方でメトリクスデータをフィルタリングします。
TransitGatewayAttachment , AvailabilityZone	Transit Gateway アタッチメントとアベイラビリティーゾーンの両方によってメトリクスデータをフィルタリングします。

を使用した AWS Transit Gateway API コールのログ記録 AWS CloudTrail

AWS Transit Gateway; は、ユーザーAWS CloudTrail、ロール、または によって実行されたアクションを記録するサービスである と統合されています AWS のサービス。CloudTrail は、Transit Gateway のすべての 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、Transit Gateway コンソールからの呼び出しと、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。CloudTrail で収集した情報を使用して、Transit Gateway へのリクエスト、リクエスト元の IP アドレス、リクエストの作成日時、その他の詳細を確認できます。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- ルートユーザーまたはユーザー認証情報のどちらを使用してリクエストが送信されたか。
- リクエストが IAM Identity Center ユーザーに代わって行われたかどうか。
- 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テンポラリ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。

CloudTrail は、アカウントを作成する AWS アカウント と でアクティブになり、CloudTrail イベント履歴に自動的にアクセスできます。CloudTrail の [イベント履歴] では、 AWS リージョンで過去 90 日間に記録された管理イベントの表示、検索、およびダウンロードが可能で、変更不可能な記録を確認できます。詳細については、「AWS CloudTrail ユーザーガイド」の「CloudTrail イベント履歴の使用」を参照してください。[イベント履歴] の閲覧には CloudTrail の料金はかかりません。

AWS アカウント 過去 90 日間のイベントの継続的な記録については、証跡または CloudTrail Lake イベントデータストアを作成します。

CloudTrail 証跡

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。を使用して作成されたすべての証跡 AWS マネジメントコンソール はマルチリージョンです。 AWS CLIを使用する際は、単一リージョンまたは複数リージョンの証跡を作成できます。アカウント AWS リージョン 内のすべての でアクティビティをキャプチャするため、マルチリージョン証跡を作成することをお勧めします。単一リージョンの証跡を作成する場合、証跡の AWS リージョンに記録されたイベントのみを表示できます。証跡の詳細については、「AWS CloudTrail ユーザーガイド」の「AWS アカウントの証跡の作成」および「組織の証跡の作成」を参照してください。

証跡を作成すると、進行中の管理イベントのコピーを 1 つ無料で CloudTrail から Amazon S3 バケットに配信できますが、Amazon S3 ストレージには料金がかかります。CloudTrail の料金の詳細については、「AWS CloudTrail の料金」を参照してください。Amazon S3 の料金に関する詳細については、「Amazon S3 の料金」を参照してください。

CloudTrail Lake イベントデータストア

[CloudTrail Lake] を使用すると、イベントに対して SQL ベースのクエリを実行できます。CloudTrail Lake は、行ベースの JSON 形式の既存のイベントを Apache ORC 形式に変換します。ORC は、データを高速に取得するために最適化された単票ストレージ形式です。イベントは、イベントデータストアに集約されます。イベントデータストアは、高度なイベントセレクタを適用することによって選択する条件に基づいた、イベントのイミュータブルなコレクションです。どのイベントが存続し、クエリに使用できるかは、イベントデータストアに適用するセレクタが制御します。CloudTrail Lake の詳細については、 AWS CloudTrail ユーザーガイドのAWS CloudTrail 「Lake の使用」を参照してください。

CloudTrail Lake のイベントデータストアとクエリにはコストがかかります。イベントデータストアを作成する際に、イベントデータストアに使用する料金オプションを選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、そのイベントデータストアのデフォルトと最長の保持期間が決まります。CloudTrail の料金の詳細については、「AWS CloudTrail の料金」を参照してください。

Transit Gateway 管理イベント

管理イベントは、 のリソースで実行される管理オペレーションに関する情報を提供します AWS アカウント。これらのイベントは、コントロールプレーンオペレーションとも呼ばれます。CloudTrail は、デフォルトで管理イベントをログ記録します。

AWS Transit Gateway は、すべての Transit Gateway コントロールプレーンオペレーションを管理イベントとしてログに記録します。 AWS Transit Gateway が CloudTrail に記録する Transit Gateway コントロールプレーンオペレーションのリストについては、「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。 Amazon EC2

Transit Gateway イベントの例

各イベントは任意の送信元からの単一のリクエストを表し、リクエストされた API オペレーション、オペレーションの日時、リクエストパラメータなどに関する情報を含みます。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、イベントは特定の順序で表示されません。

「トレイル」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 のログファイルは、単一か複数のログエントリを含みます。イベントは、任意の出典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、リクエストパラメータなどに関する情報が含まれます。CloudTrail ログファイルは、パブリック API 呼び出し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。

ログファイルには、トランジットゲートウェイ API コールだけでなく、 AWS アカウントのすべての API コールの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"
}
```

AWS Transit Gateway での Identity and Access Management

AWS 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許可します。 AWS Identity and Access Management (IAM) の機能を使用すると、セキュリティ認証情報を共有することなく、他のユーザー、サービス、アプリケーションが AWS リソースを完全にまたは制限付きで使用できるようになります。

デフォルトでは、IAM ユーザーには AWS リソースを作成、表示、または変更する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。

トランジットゲートウェイを使用するには、次のいずれかの AWS マネージドポリシー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。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCreateTaggedTGWs",
            "Effect": "Allow",
            "Action": "ec2:CreateTransitGateway",
            "Resource": "arn:aws:ec2:us-east-1:123456789012:transit-gateway/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/stack": "prod"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "stack"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:123456789012: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。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteTransitGatewayRouteTable",
                "ec2:CreateTransitGatewayRouteTable"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1:123456789012:transit-gateway/
tgw-11223344556677889",
                "arn:aws:ec2:*:*:transit-gateway-route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTransitGatewayRoute",
                "ec2:ReplaceTransitGatewayRoute"
            ],
            "Resource": "arn:aws:ec2:*:*:transit-gateway-attachment/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/network": "new-york-office"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTransitGatewayRoute",
                "ec2:ReplaceTransitGatewayRoute"
            ],
            "Resource": "arn:aws:ec2:*:*:transit-gateway-route-table/*"
        }
    ]
```

```
}
```

Transit Gateway で Transit Gateway AWS のサービスにリンクされたロールを使用する

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「Service-linked roles」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。

サービスリンクロールの作成、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) に許可するにはアクセス許可を設定する必要があります。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役割のアクセス許可」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。

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は、 AWS アカウント内のすべての Transit Gateway VPC アタッチメントを削除した後にのみ削除できます。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。

AWS AWS Transit Gateway での Transit Gateway の マネージドポリシー

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できるように、多くの一般的なユースケースにアクセス許可を付与するように設計されています。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、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注意してください。ユースケースに固有のカスタマー管理ポリシーを定義して、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されているアクセス許可は変更できません。が AWS マネージドポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) に影響します。 AWS は、新しい が起動されるか、新しい API オペレーション AWS のサービス が既存のサービスで使用できるようになったときに、 AWS マネージドポリシーを更新する可能性が高くなります。

詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」を参照してください。

トランジットゲートウェイを使用するには、次のいずれかの AWS マネージドポリシー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 管理ポリシーへのトランジットゲートウェイの更新

Amazon VPC が 2021 年 3 月にこれらの変更の追跡を開始した以降の、トランジットゲートウェイの AWS マネージドポリシーの更新に関する詳細を表示します。

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 は、 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

AWS Transit Gateway の Transit Gateway のネットワーク ACLs

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。

AWS トランジットゲートウェイのクォータ

AWS アカウント には、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。特に明記していない限り、クォータはリージョン固有です。

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「クォータの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。

General

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	あり
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	あり
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	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
		マネージャー (TAM) にお問い合わせください。
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	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。
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	あり
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	あり

名前	デフォルト	引き上げ可能
2 つの Transit Gateway 間、または 1 つの Transit Gateway 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	不可
Connect アタッチメントあたりの Connect ピア (GRE トンネル)	4	不可
トランジットゲートウェイあたりの VPN コンセントレータ	5	不可
VPN コンセントレータあたりの VPN 接続数	100	不可

[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、 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	各方向で最大 100 Gbps (100 Gbps の進入と 100 Gbps の進入)	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

名前	デフォルト	引き上げ可能
		マネージャー (TAM) にお問い合わせください。
リージョンで使用可能なアベイラビリティーゾーンあたりの Direct Connect ゲートウェイまたはピア接続の帯域幅	各方向で最大 100 Gbps (100 Gbps の進入と 100 Gbps の進入)	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。
リージョンで使用可能なアベイラビリティーゾーンあたりのトランジットゲートウェイアタッチメント (Direct Connect およびピアリングアタッチメント) あたりの 1 秒あたりのパケット数	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。
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 アタッチメントごとに合計帯域幅で最大 20 Gbps 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。

VPN トンネルの帯域幅とパケットの制限については、「VPN 帯域幅とスループット」を参照してください。

Direct Connect ゲートウェイ

名前	デフォルト	引き上げ可能
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	不可
ゲートウェイあたりのトランジット Direct Connect ゲートウェイ	6	不可

最大送信単位 (MTU)

- 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) 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。トランジットゲートウェイは、VPCs、、Transit Gateway Connect Direct Connect、ピアリングアタッチメント (リージョン内、リージョン間、および Cloud WAN 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。
- 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 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。
- Transit Gateway は、VPC および Connect アタッチメントへのトラフィック進入のパス MTU 検出 (PMTUD) をサポートします。Transit Gateway は、ICMPv4 パケットの場合は `FRAG_NEEDED` を生成し、ICMPv6 パケットの場合は `Packet Too Big (PTB)` を生成します。Transit Gateway は、Site-to-site VPN、Direct Connect、ピアリングアタッチメントの PMTUD をサポートしていません。パス MTU 検出の詳細については、「Amazon EC2 ユーザーガイド」の「パス MTU 検出」を参照してください。

マルチキャスト

> **Note**
>
> Transit Gateway マルチキャストは、高頻度取引やパフォーマンス重視のアプリケーションには適していない場合があります。次のマルチキャスト制限を確認することを強くお勧めします。パフォーマンス要件の詳細なレビューについては、アカウントまたはソリューションアーキテクトチームにお問い合わせください。

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	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。
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	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。
VPC あたりのマルチキャストドメインの関連付け	20	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。

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	不可
フローごとの 1 秒あたりの最大パケット数 (10 レシーバー未満)	75,000	不可
フローごとの 1 秒あたりの最大パケット数 (10 レシーバー以上)	15,000	不可
1 秒あたりの最大総パケット数 (10 レシーバー未満)	2,500,000	不可
1 秒あたりの最大総パケット数 (10 レシーバー以上)	500,000	不可

AWS Network Manager

名前	デフォルト	引き上げ可能
あたりのグローバルネットワーク 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

名前	デフォルト	引き上げ可能
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 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 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
クライアント VPN アタッチメント	クライアント VPN アタッチメントを作成して、トランジットゲートウェイをクライアント VPN エンドポイントに接続します。	2026 年 4 月 20 日
柔軟なコスト配分	柔軟なコスト配分ポリシーを設定して、組織全体でのデータ処理と転送コストの割り当て方法を制御します。	2025 年 11 月 20 日
トランジットゲートウェイの暗号化サポート	トランジットゲートウェイの暗号化サポートを管理し、すべてのトラフィックにencryption-in-transitを適用します。	2025 年 11 月 20 日
ネットワーク関数アタッチメント	Transit Gateway を AWS Network Firewallに直接接続するためのネットワーク関数アタッチメントを作成します。	2025 年 6 月 16 日
セキュリティグループの参照サポート	トランジットゲートウェイにアタッチされた VPC 間でセキュリティグループを参照できるようになりました。	2024 年 9 月 25 日
AWS トランジットゲートウェイのクォータ	帯域幅の制限が追加されました。	2023 年 8 月 14 日
AWS トランジットゲートウェイフローログ	Transit Gateway Flow Logs が Transit Gateway でサポー	2022 年 7 月 14 日

	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。	
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ティー仮想アプライアンスの間の接続を確立できます。	2020 年 12 月 10 日
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	Direct Connect ゲートウェイを使用して、トランジット仮想インターフェイス経由で Direct Connect トランジットゲートウェイにアタッチされた VPCs VPNs に接続できます。	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。