



アーキテクチャ図

のトラフィックセグメンテーションオプション ン AWS Direct Connect



のトラフィックセグメンテーションオプション AWS Direct Connect: アーキテクチャ図

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

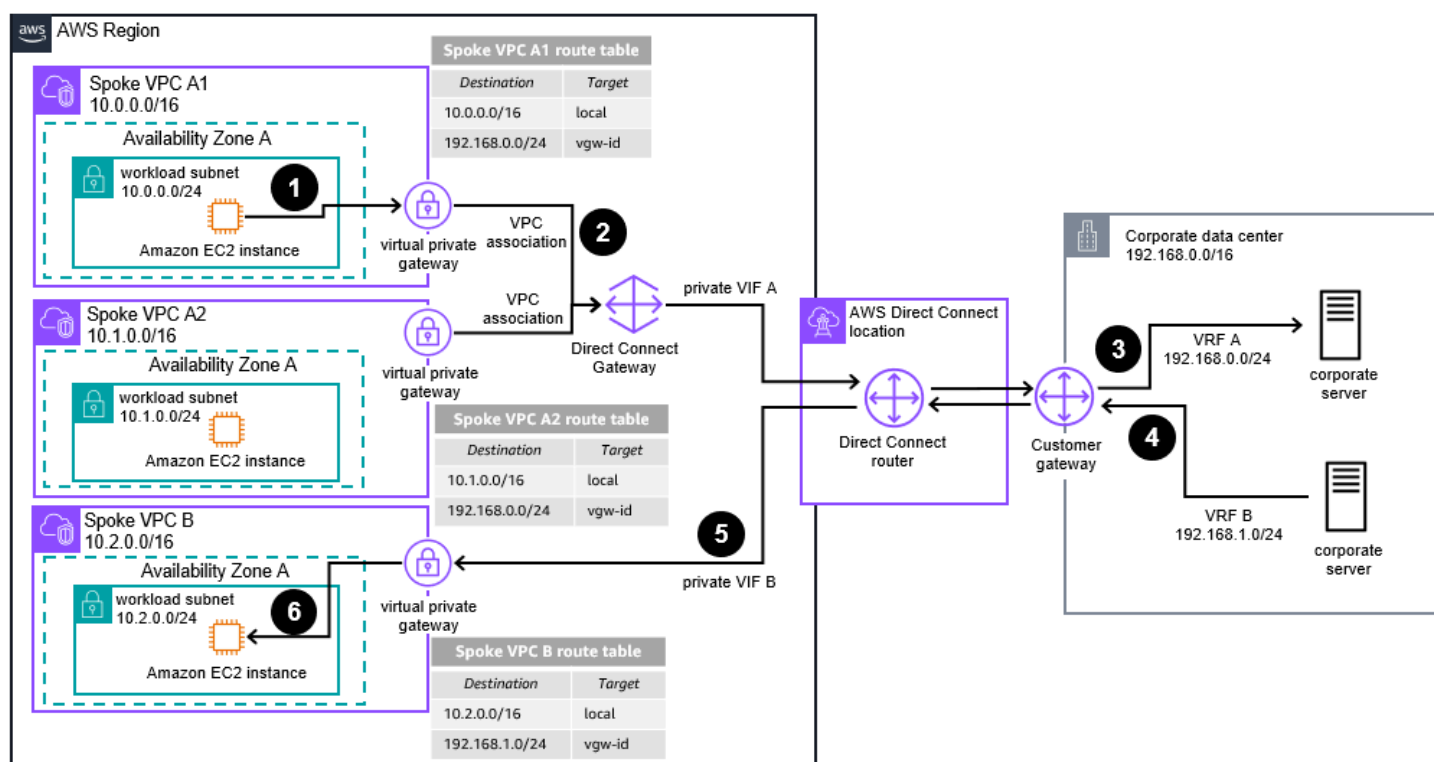
のトラフィックセグメンテーションオプション AWS Direct Connect	i
VPC または Direct Connect ゲートウェイ図で複数のプライベート VIFs AWS Direct Connect を使用してトラフィックをセグメント化する	1
複数のトランジット VIFsと Direct Connect ゲートウェイ AWS Direct Connect の図を使用して トラフィックをセグメント化する	3
AWS Transit Gateway Connect Attachments と AWS Direct Connect を使用して、オンプレミ ス VRFs をトランジット VIFs図	4
AWS Site-to-Site VPN アタッチメント (パブリック VIFs) と AWS Direct Connect を使用して オンプレミス VRFs図を拡張する	6
AWS Site-to-Site VPN プライベート IP VPN アタッチメントと を使用して、オンプレミス VRFs AWS Direct Connect を転送 VIFs図	7
詳細情報	8
寄稿者	8
図の履歴	8
.....	x

のトラフィックセグメンテーションオプション AWS Direct Connect

公開日: 2023 年 11 月 9 日 ([図の履歴](#))

このアーキテクチャは AWS Direct Connect、でのトラフィックセグメンテーションオプションを示し、VPC VIFs の使用、Transit VIF 経由 AWS Transit Gateway の接続アタッチメントの使用、Transit VIF 経由 AWS Site-to-Site VPN の接続の使用が含まれます。Direct Connect

VPC または Direct Connect ゲートウェイ図で複数のプライベート VIFs AWS Direct Connect を使用してトラフィックをセグメント化する

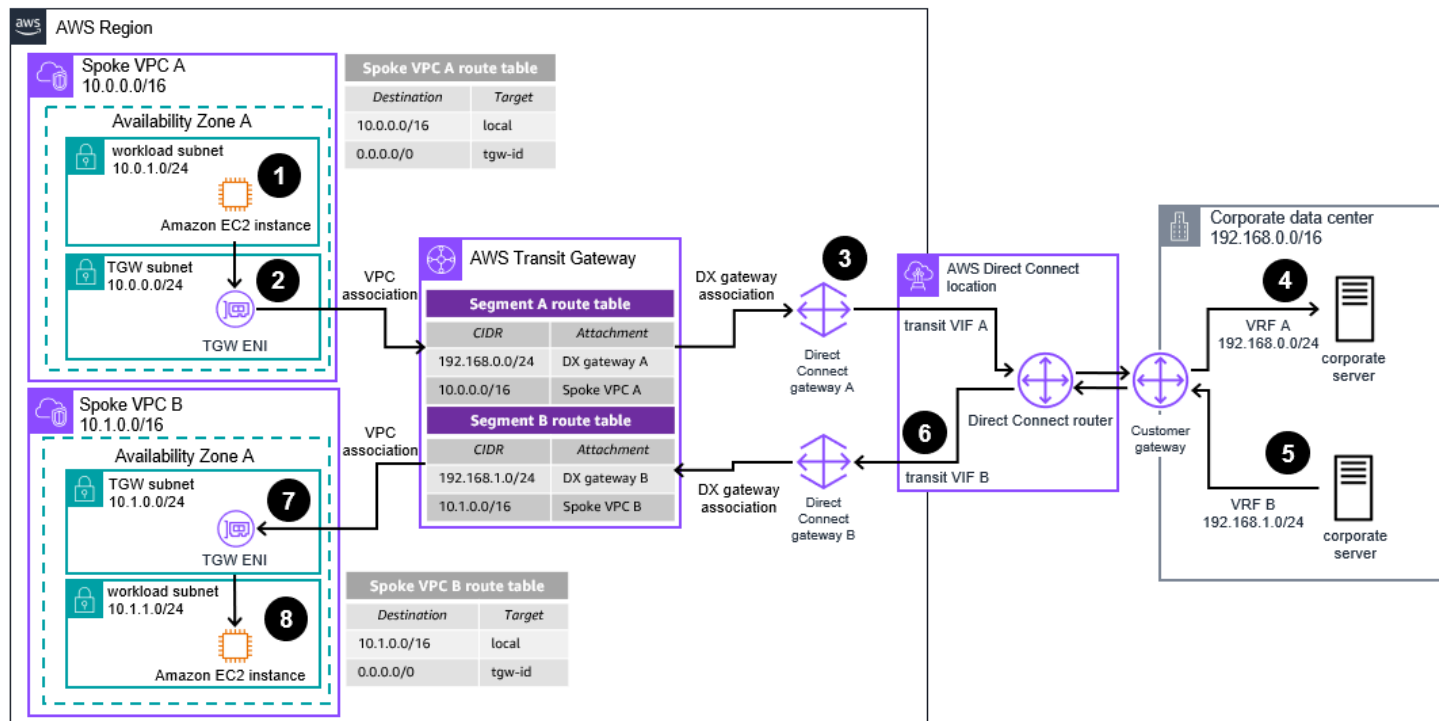


プライベート仮想インターフェイス (VIFs) は、プライベート IP アドレスを使用して Amazon Virtual Private Cloud (Amazon VPC) にアクセスするために使用されます。各 VIF には一意の仮想ローカルエリアネットワーク (VLAN) タグが設定されています。つまり、データセンターにある仮想ルーティングおよび転送 (VRF) ごとに 1 つの VIF を使用してトラフィックをセグメント化できます。Direct Connect 接続のタイプに応じて、VIFs の数の制限を考慮してください。専用接続を持つプライバー

ト VIFs またはパブリック VIF を 50 個、ホスト接続を持つプライベート VIF またはパブリック VIF を 1 個持つことができます。さらに、同じ Direct Connect ゲートウェイに 30 個のプライベート VIFs を関連付けることができます。クォータは [Direct Connect ユーザーガイド](#)で確認できます。

1. スポーク VPC A のインスタンスから開始され、企業データセンターサーバー (VRF A 内) 宛てのトラフィックは、スポーク VPC A ルートテーブルに従って仮想プライベートゲートウェイにルーティングされます。
2. 仮想プライベートゲートウェイは、プライベート VIF (VLAN) を使用して企業データセンターに接続する Direct Connect ゲートウェイに関連付けられています。セグメンテーションを実現するには、複数のプライベート VIFs を使用します。オンプレミスルーターは、設定された VRF ごとに異なる VIF (VLAN) 接続を使用するように設定する必要があります。
3. オンプレミスルーターは、プライベート VIF A から VRF A および送信先サーバーにトラフィックを転送します。
4. スポーク VPC B 宛ての企業データセンターの VRF B からのトラフィックは、まずデータセンターにあるカスタマーゲートウェイに送信されます。
5. カスタマーゲートウェイは Direct Connect、リンク経由でプライベート VIF B を使用して、VPC B の仮想プライベートゲートウェイにトラフィックを送信します。
6. トラフィックは、スポーク VPC B ルートテーブルに従って送信先に転送されます。

複数のトランジット VIFsと Direct Connect ゲートウェイ AWS Direct Connect の図を使用してトラフィックをセグメント化する

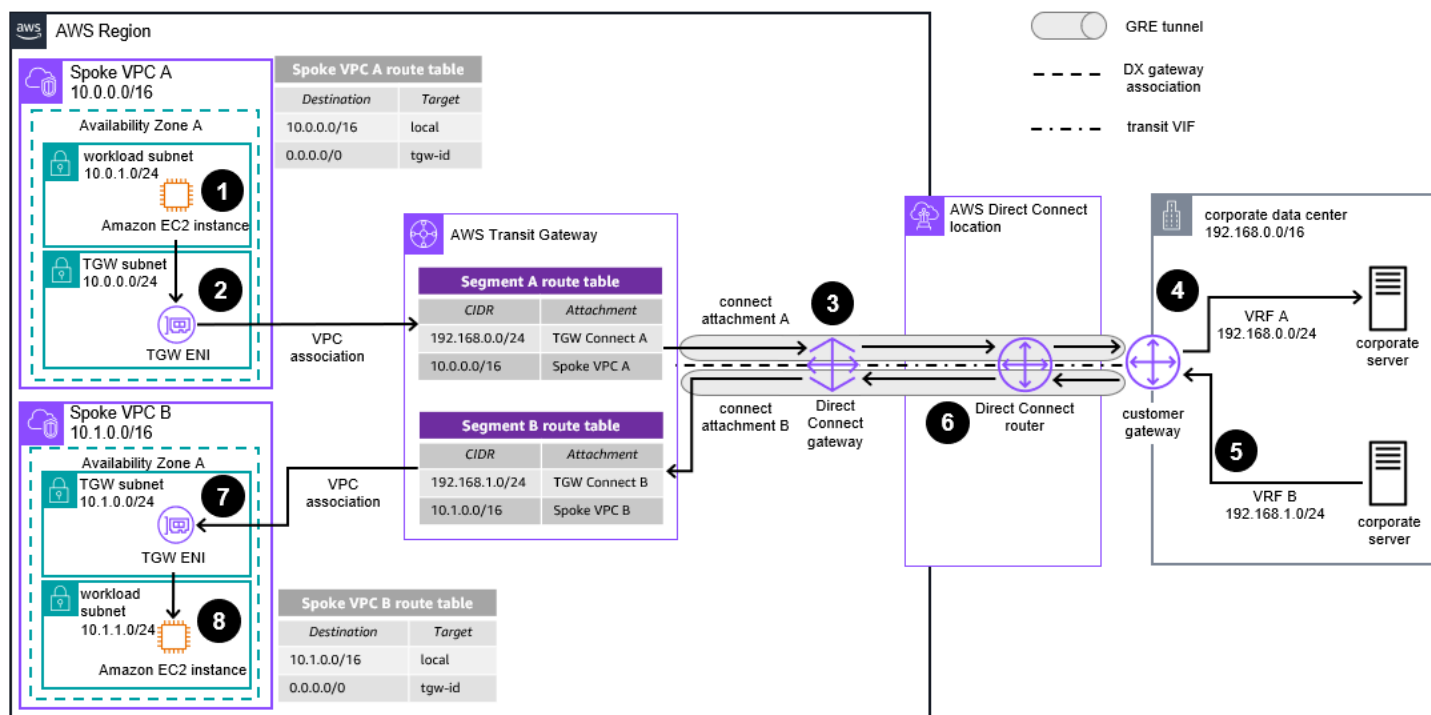


トランジット仮想インターフェイス (VIFsは、 Direct Connect ゲートウェイ AWS Transit Gateway を介して にアクセスするために使用されます。各 VIF には一意の仮想ローカルエリアネットワーク (VLAN) タグが設定されています。つまり、データセンターにある仮想ルーティングおよび転送 (VRF) ごとに 1 つの VIF を使用してトラフィックをセグメント化できます。Direct Connect 接続のタイプに応じて、VIFs の数の制限を考慮してください。専用接続ごとに最大 51 個のプライベート、パブリック、およびトランジット VIFs を組み合わせた 4 つのトランジット VIFs を持つことができます。ホスト接続の場合、トランジット VIF は 1 つだけ持つことができます。さらに、30 個のトランジット VIFs を同じ Direct Connect ゲートウェイに関連付けることができます。クォータは [Direct Connect ユーザーガイド](#)で確認できます。

1. スポーク VPC A のインスタンスから開始され、企業データセンターサーバー (VRF A 内) 宛てのトラフィックは、スポーク VPC A ルートテーブルAWS Transit Gatewayに従って にルーティングされます。
2. Transit Gateway は複数のゲートウェイ (DXGW) に関連付けられており、各 Direct Connect ゲートウェイは Transit VIF (VLAN) を使用して企業データセンターに接続し、トラフィックのセグメンテーションを実現します。オンプレミスルーターは、設定された VRF ごとに異なる VIF (VLAN) 接続を使用するように設定する必要があります。

3. トラフィックは、VPC A アタッチメントに関連付けられたセグメント A Transit Gateway ルートテーブルに従って DXGW A に転送されます。
4. オンプレミスルーターは、トランジット VIF A から VRF A および送信先サーバーにトラフィックを転送します。
5. スポーク VPC B 宛ての企業データセンターの VRF B からのトラフィックは、まずデータセンターにあるカスタマーゲートウェイに送信されます。
6. カスタマーゲートウェイは Direct Connect、リンク経由でトランジット VIF B を使用してトラフィックをトランジットゲートウェイセグメント B に送信します。
7. トラフィックは、セグメント B Transit Gateway ルートテーブルに従って VPC B に転送されます。
8. トラフィックは VPC B ルートテーブルに従って送信先に転送されます。

AWS Transit Gateway Connect Attachments と AWS Direct Connect を使用して、オンプレミス VRFs をトランジット VIFs

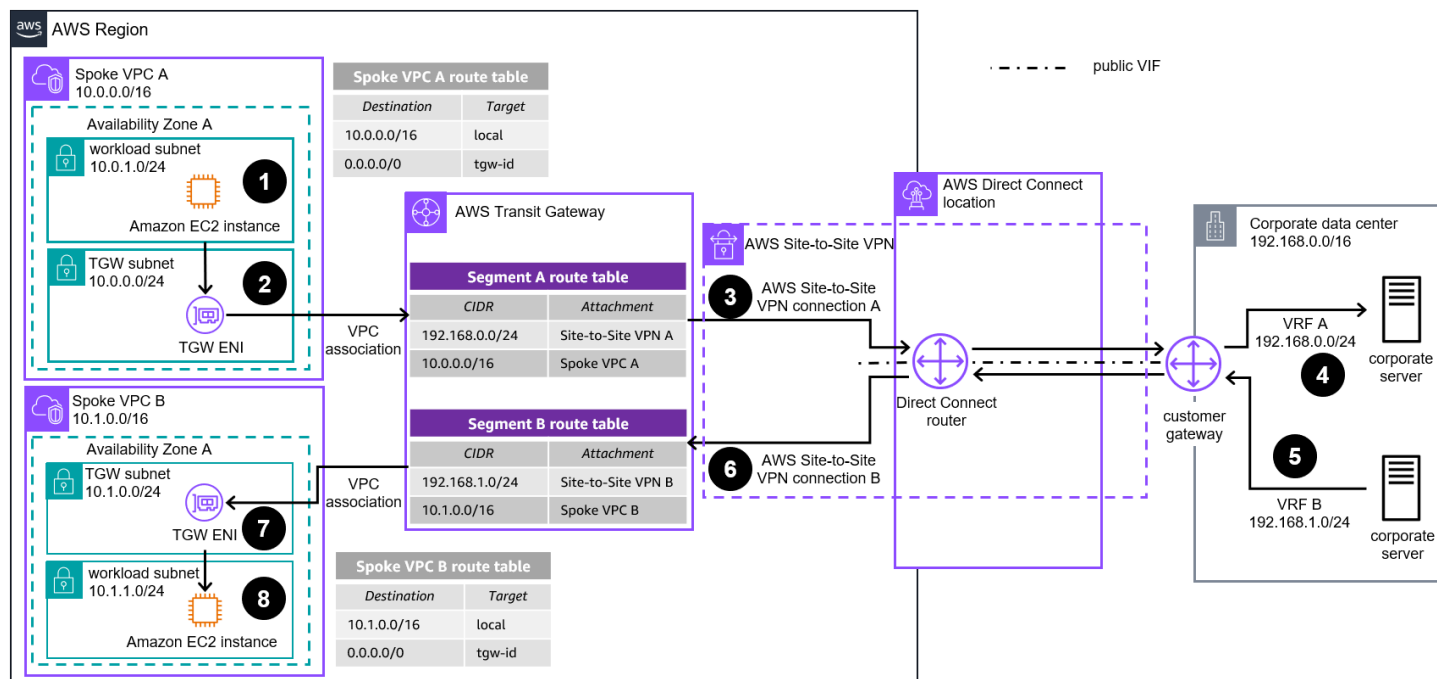


ホスト接続では 1 つのトランジット VIF を取得し、専用接続では 4 つを取得します。トランジット VIFs VRFs よりも多くの VRF がある場合、トランジット VIF で複数の Transit Gateway Connect アタッチメント (GRE トンネル) を使用してトラフィックをセグメント化し、データセンターに

ある VRF ごとに 1 つの接続アタッチメントを作成できます。このユースケースの詳細については、[「Connect AWS Transit Gateway を使用して VRFs」](#)を参照してください。

1. スポーク VPC A のインスタンスから開始され、企業データセンターサーバー (VRF A) 宛てのトラフィックは、スポーク VPC A ルートテーブルに従って Transit Gateway Elastic Network Interface (TGW ENI) にルーティングされます。
2. トラフィックは Transit Gateway に転送されます。その後、トラフィックはセグメント A ルートテーブルに従って Transit Gateway Connect アタッチメント A を介して企業データセンターにルーティングされます。
3. Transit Gateway Connect アタッチメントは、Direct Connect接続をトランスポートとして使用し、汎用ルーティングカプセル化 (GRE) トンネリングとボーダーゲートウェイプロトコル (BGP) を使用して Transit Gateway を企業のデータセンタールーターに接続します。オンプレミスルーターは、設定された VRF ごとに異なる接続アタッチメントを使用するように設定する必要があります。
4. オンプレミスルーターは、Connect アタッチメント A から VRF A および送信先サーバーにトラフィックを転送します。
5. スポーク VPC B 宛ての企業データセンターの VRF B からのトラフィックは、まずデータセンターにあるカスタマーゲートウェイに送信されます。
6. カスタマーゲートウェイは、Direct Connectリンク経由で Transit Gateway Connect アタッチメント B の GRE トンネルを使用して、トラフィックを Transit Gateway に送信します。
7. トラフィックは、Transit Gateway セグメント B ルートテーブルに従ってスポーク VPC B アタッチメントに転送されます。
8. スポーク VPC B の TGW ENI は、トラフィックを送信先に転送します。

AWS Site-to-Site VPN アタッチメント (パブリック VIFs) と AWS Direct Connect を使用してオンプレミス VRFs図を拡張する

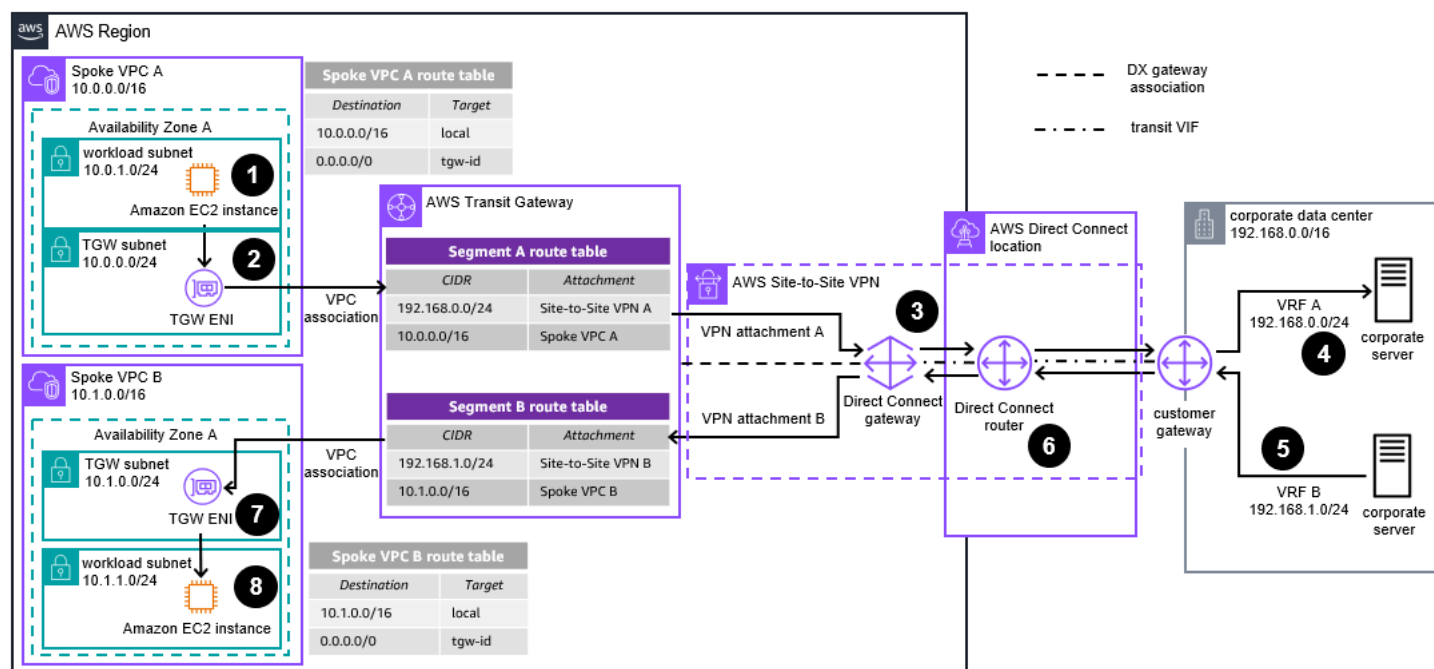


カスタマーゲートウェイが汎用ルーティングカプセル化 (GRE) をサポートしていない場合でも、データセンターにある VRF ごとに 1 AWS Site-to-Site VPN つの接続を作成してトラフィックをセグメント化できます。パブリック VIF をアンダーレイイングトランスポートとして使用できます。

1. スポーク VPC A のインスタンスから開始され、企業データセンターサーバー (VRF A) 宛てのトラフィックは、スポーク VPC A ルートテーブルに従って Transit Gateway Elastic Network Interface (TGW ENI) にルーティングされます。
2. トラフィックは Transit Gateway に転送されます。その後、トラフィックはセグメント A ルートテーブルに従って Site-to-Site VPN 接続 A を介して企業データセンターにルーティングされます。
3. Site-to-Site VPN 接続は、パブリック VIF as Transport (VLAN) を使用して作成されます。オンプレミスルーターは、設定された VRF ごとに異なる VPN 接続を使用するように設定する必要があります。
4. オンプレミスルーターは、Site-to-Site VPN 接続 A から VRF A と送信先サーバーにトラフィックを転送します。
5. スポーク VPC B 宛ての企業データセンターの VRF B からのトラフィックは、まずデータセンターにあるカスタマーゲートウェイに送信されます。

6. カスタマーゲートウェイは Site-to-Site VPN 接続 B を選択して、Direct Connectリンク経由でトラフィックを Transit Gateway に送信します。
7. トラフィックは、Transit Gateway セグメント B ルートテーブルに従ってスポーク VPC B アタッチメントに転送されます。
8. スポーク VPC B の TGW ENI は、トラフィックを送信先に転送します。

AWS Site-to-Site VPN プライベート IP VPN アタッチメントと を使用して、オンプレミス VRFs AWS Direct Connect を転送 VIFs図



カスタマーゲートウェイが GRE (汎用ルーティングカプセル化) をサポートしていない場合でも、データセンターにある VRF ごとに 1 つの AWS Site-to-Site VPN 接続 (2 つのトンネルを使用) を作成してトラフィックをセグメント化できます。Site-to-Site VPN プライベート IP VPN 機能を使用すると、AWS Direct Connect ゲートウェイとトランジット VIF を基盤となるトランスポートとして使用 IPs して VPNs を作成できます。

1. スポーク VPC A のインスタンスから開始され、企業データセンターサーバー (VRF A) 宛てのトラフィックは、スポーク VPC A ルートテーブルに従って AWS Transit Gateway Elastic Network Interface (TGW ENI) にルーティングされます。
2. トラフィックは Transit Gateway に転送されます。その後、トラフィックはセグメント A ルートテーブルに従って Transit Gateway VPN アタッチメント A を介して企業データセンターにルーティングされます。

3. Transit Gateway Site-to-Site VPN アタッチメントは、Direct Connect接続をトランスポートとして使用し、1 つの IPSec VPN 接続 (2 つのトンネルを使用) を使用して Transit Gateway を企業のデータセンタールーターに接続します。オンプレミスルーターは、設定された VRF ごとに異なる VPN アタッチメントを使用するように設定する必要があります。
4. オンプレミスルーターは、VPN アタッチメント A から VRF A および送信先サーバーにトラフィックを転送します。
5. スポーク VPC B 宛ての企業データセンターの VRF B からのトラフィックは、まずデータセンターにあるカスタマーゲートウェイに送信されます。
6. カスタマーゲートウェイはDirect Connect、リンク経由で Site-to-Site VPN 接続 B を使用してトラフィックを Transit Gateway に送信します。
7. トラフィックは、Transit Gateway セグメント B ルートテーブルに従ってスポーク VPC B アタッチメントに転送されます。
8. スポーク VPC B の TGW ENI は、トラフィックを送信先に転送します。

詳細情報

詳細については、「」を参照してください。

- [AWS アーキテクチャアイコン](#)
- [AWS アーキテクチャセンター](#)
- [AWS Well-Architected](#)
- [Direct Connect ユーザーガイド](#)

寄稿者

このリファレンスアーキテクチャ図の寄与要因は次のとおりです。

- Amazon Web Services、スペシャリストソリューションアーキテクト、Pablo Sánchez Carmona
- Amazon Web Services、シニアソリューションアーキテクト、Thaddeus Worsnop

図の履歴

このリファレンスアーキテクチャ図の更新について通知を受け取るには、RSS フィードにサブスクライブします。

変更	説明	日付
図が更新されました	複数のトランジット VIFsと Direct Connect ゲートウェイ AWS Direct Connect を使用してトラフィックをセグメント化	2023 年 11 月 9 日
初版発行	リファレンスアーキテクチャ図が最初に公開されました。	2022 年 6 月 30 日

 Note

RSS 更新をサブスクライブするには、使用しているブラウザで RSS プラグインが有効になっている必要があります。

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。