AWS ホワイトペーパー

Amazon Virtual Private Cloud の接続オプション

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Virtual Private Cloud の接続オプション: AWS ホワイトペーパー

Copyright © 2025 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 が所有していない他のすべての商標は、それぞれの所有者の所有物であり、Amazon と提携、接続、または後援されている場合とされていない場合があります。

Table of Contents

要約 1
要約 1
序章 2
Network-to-Amazon VPC への接続オプション 4
AWS Site-to-Site VPN 7
追加リソース 9
AWS Transit Gateway + Site-to-Site VPN 10
追加リソース 12
AWS Direct Connect 13
追加リソース 16
AWS Direct Connect + AWS Transit Gateway 17
追加リソース 17
AWS Direct Connect + AWS Site-to-Site VPN 18
追加リソース 18
AWS Direct Connect + AWS Transit Gateway + AWS Site-to-Site VPN 19
追加リソース 20
AWS VPN CloudHub 20
追加リソース 21
AWS Transit Gateway + SD-WAN ソリューション 22
追加リソース 24
ソフトウェア VPN 24
追加リソース 25
Amazon VPC-to-Amazonオプション 27
VPC ピアリング 28
追加リソース 25
AWS Transit Gateway 30
追加リソース 32
AWS PrivateLink 32
へのアクセスコントロール AWS PrivateLink 33
追加リソース 33
ソフトウェア VPN 33
追加リソース 35
ソフトウェア VPN-to-AWS Site-to-Site VPN 35
追加リソース 36

Amazon VPC access-to-Amazonソフトウェアリモートアクセス接続オプション 37
AWS クライアント VPN 37
追加リソース 38
ソフトウェアクライアント VPN 38
追加リソース 40
トランジット VPC 41
追加リソース 42
AWS クラウド WAN 43
主要事項 44
追加リソース 44
結論 45
付録 A: ソフトウェア VPN インスタンスの高レベル HA アーキテクチャ 46
VPN モニタリング 46
寄稿者 48
ドキュメントの改訂 49
注意 50
..... li

Amazon Virtual Private Cloud の接続オプション

公開日: 2023 年 4 月 5 日 (ドキュメントの改訂)

要約

Amazon Virtual Private Cloud (Amazon VPC) を使用すると、Amazon Web Services (AWS) クラウドのプライベートで隔離されたセクションをプロビジョニングし、お客様が定義した IP アドレス範囲を使用して仮想ネットワークで AWS リソースを起動できます。Amazon VPC では、AWS 仮想ネットワークを他のリモートネットワークに接続するためのいくつかのオプションが用意されています。このドキュメントでは、お客様が利用できるいくつかの一般的なネットワーク接続オプションについて説明します。これには、リモートカスタマーネットワークを Amazon VPC と統合し、複数の Amazon VPCsを連続した仮想ネットワークに接続するための接続オプションが含まれます。

このホワイトペーパーは、利用可能な接続オプションを確認したい企業ネットワークアーキテクトやエンジニア、または Amazon VPC 管理者を対象としています。ネットワーク接続に関する議論を容易にするためのさまざまなオプションの概要と、より詳細な情報や例を含む追加のドキュメントやリソースへのポインタを提供します。

序章

Amazon VPC には、現在のネットワーク設計と要件に応じて、複数のネットワーク接続オプションが用意されています。これらの接続オプションには、インターネットまたは AWS Direct Connect 接続をネットワークバックボーンとして使用し、AWS またはユーザー管理のネットワークエンドポイントへの接続を終了することが含まれます。さらに、AWS では、AWS のサービスまたはユーザー管理のネットワーク機器とルートを活用して、Amazon VPC とネットワークの間でネットワークルーティングを配信する方法を選択できます。このホワイトペーパーでは、以下のオプションの概要と各オプションの概要の比較について説明します。

- Network-to-Amazon VPC への接続オプション
  - AWS Site-to-Site VPN – リモートネットワーク上のネットワーク機器から Amazon VPC へのマネージド IPsec VPN 接続の確立について説明します。
  - AWS Transit Gateway + AWS Site-to-Site VPN – を使用して、リモートネットワーク上のネットワーク機器から Amazon VPCs のリージョンネットワークハブへのマネージド IPsec VPN 接続を確立する方法について説明します AWS Transit Gateway。
  - AWS Direct Connect - を使用して、リモートネットワークから Amazon VPC へのプライベートで論理的な接続を確立する方法について説明します AWS Direct Connect。
  - AWS Direct Connect + AWS Transit Gateway – AWS Direct Connect および を使用して、リモートネットワークから Amazon VPCs のリージョンネットワークハブへのプライベート論理接続を確立する方法について説明します AWS Transit Gateway。
  - AWS Direct Connect + AWS Site-to-Site VPN – AWS Direct Connect と AWS Site-to-Site VPN を使用して、リモートネットワークから Amazon VPC への暗号化されたプライベート接続を確立する方法について説明します。
  - AWS Direct Connect + AWS Transit Gateway + AWS Site-to-Site VPN – AWS Direct Connect および を使用して、リモートネットワークから Amazon VPCs のリージョンネットワークハブへのプライベートで暗号化された接続を確立する方法について説明します AWS Transit Gateway。
  - AWS VPN CloudHub – リモートブランチオフィスを接続するためのhub-and-spokeモデルの確立について説明します。
  - ソフトウェア VPN – リモートネットワーク上の機器から Amazon VPC 内で実行されているユーザー管理のソフトウェア VPN アプライアンスへの VPN 接続の確立について説明します。
  - AWS Transit Gateway + SD-WAN ソリューション - バック AWS ボーンまたはインターネットをトランジットネットワークとして使用して、複数のリモートロケーションを Amazon VPCs

のリージョンネットワークハブに相互接続するソフトウェア定義のワイドエリアネットワーク (SD-WAN) ソリューションの統合について説明します。

- Amazon VPC-to-Amazonオプション
  - VPC ピアリング – Amazon VPCs ピアリング機能を使用して、リージョン内およびリージョン間で Amazon VPC を接続する方法について説明します。
  - AWS Transit Gateway – hub-and-spokeモデル AWS Transit Gateway で を使用して、リージョン内およびリージョン間で Amazon VPCs を接続する方法について説明します。
  - AWS PrivateLink – Amazon VPCs VPC インターフェイスエンドポイントおよび VPC エンドポイントサービスに接続する方法について説明します。
  - ソフトウェア VPN – 各 Amazon VPCs 内で実行されているユーザー管理のソフトウェア VPN アプライアンス間で確立された VPN 接続を使用して Amazon VPC を接続する方法について説明します。
  - ソフトウェア VPN-to-AWS Site-to-Site VPN – 1 つの Amazon VPCs 内のユーザー管理ソフトウェア VPN アプライアンスと、他の Amazon VPC にアタッチされた AWS Site-to-Site VPN の間に確立された VPN 接続を使用して Amazon VPC を接続する方法について説明します。
- Amazon VPC access-to-Amazonソフトウェアリモートアクセス接続オプション
  - AWS クライアント VPN – AWS クライアント VPN を活用して、ソフトウェアのリモートアクセスを Amazon VPC に接続する方法について説明します。
  - ソフトウェアクライアント VPN – ユーザー管理のソフトウェア VPN アプライアンスを活用して、ソフトウェアのリモートアクセスを Amazon VPC に接続する方法について説明します。
- トランジット VPC - ソフトウェア VPN と AWS マネージド VPN を組み合わせて AWS でグローバルトランジットネットワークを確立する方法について説明します。
- AWS クラウド WAN - Amazon VPCs、データセンター、リモートブランチ内のリソース間のグローバルな相互接続を簡単に構築、管理、モニタリングするためのマネージド型ワイドエリアネットワーク (WAN) の確立について説明します。

Network-to-Amazon VPC への接続オプション

このセクションでは、リモートネットワークを Amazon VPC 環境に接続するための設計パターンについて説明します。これらのオプションは、内部ネットワークを AWS クラウドに拡張することで、AWS リソースを既存のオンサイトサービス (モニタリング、認証、セキュリティ、データ、その他のシステムなど) と統合するのに役立ちます。このネットワーク拡張により、内部ユーザーは他の内部向けリソースと同様に、AWS でホストされているリソースにシームレスに接続できます。

リモートカスタマーネットワークへの VPC 接続は、接続するネットワークごとに重複しない IP 範囲を使用する場合に最適です。たとえば、1 つ以上の VPCs を企業ネットワークに接続する場合は、一意の Classless Inter-Domain Routing (CIDR) 範囲が設定されていることを確認してください。各 VPC で使用する 1 つの連続した重複しない CIDR ブロックを割り当てることをお勧めします。Amazon VPC のルーティングと制約の詳細については、「Amazon VPC に関するよくある質問」を参照してください。

オプション	ユースケース	利点	制限
AWS Site-to-Site VPN	インターネット経由で個々の VPC への AWS マネージド IPsec VPN 接続	既存の VPN 機器とプロセスの再利用 既存のインターネット接続を再利用する AWS マネージド高可用性 VPN サービス 静的ルートまたは動的ボーダーゲートウェイプロトコル (BGP) ピアリングおよびルーティングポリシーをサポート	ネットワークのレイテンシー、変動性、可用性はインターネットの状態によって異なります 冗長性とフェイルオーバーを実装する責任はお客様にあります (必要な場合)。 リモートデバイスはシングルホップ BGP をサポートする必要があります (動的ルーティングに BGP を活用する場合)

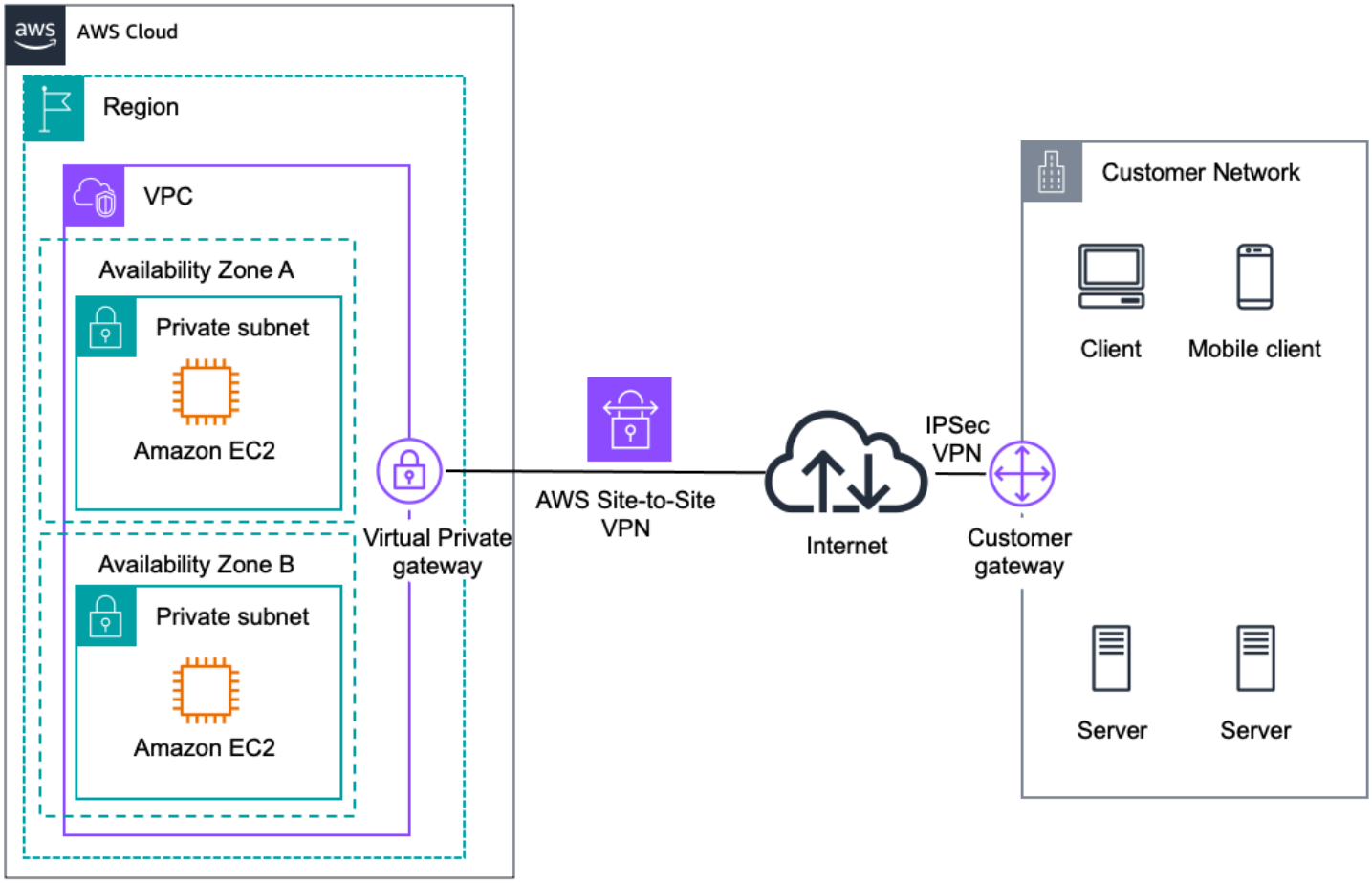
オプション	ユースケース	利点	制限
AWS Transit Gateway + AWS Site-to-Site VPN	複数の VPCs のリージョンルーターへのインターネット経由の AWS マネージド IPsec VPN 接続	前のオプションと同じ 最大 5,000 個のアタッチメント用の AWS マネージド高可用性とスケーラビリティのリージョンネットワークハブ	前のオプションと同じ
AWS Direct Connect	プライベートライン経由の専用ネットワーク接続	より予測可能なネットワークパフォーマンス 帯域幅コストの削減 BGP ピアリングポリシーとルーティングポリシーをサポート	追加の通信およびホスティングプロバイダー関係や新しいネットワーク回線のプロビジョニングが必要になる場合があります。
AWS Direct Connect + AWS Transit Gateway	複数の VPCs のリージョンルーターへのプライベートライン経由の専用ネットワーク接続	前のオプションと同じ 最大 5,000 個のアタッチメント用の AWS マネージド高可用性とスケーラビリティのリージョンネットワークハブ	前のオプションと同じ

オプション	ユースケース	利点	制限
AWS Direct Connect + AWS Site-to-Site VPN	プライベートライン経由の IPsec VPN 接続	より予測可能なネットワークパフォーマンス 帯域幅コストの削減 で BGP ピアリングポリシーとルーティングポリシーをサポート AWS Direct Connect 既存の VPN 機器とプロセスの再利用 AWS マネージド高可用性 VPN サービス VPN 接続で静的ルートまたは動的ボーダーゲートウェイプロトコル (BGP) ピアリングおよびルーティングポリシーをサポート	追加の通信およびホスティングプロバイダー関係や新しいネットワーク回線のプロビジョニングが必要になる場合があります。 冗長性とフェイルオーバーを実装する責任はお客様にあります (必要な場合) 。 リモートデバイスはシングルホップ BGP をサポートする必要があります (動的ルーティングに BGP を活用する場合)
AWS Direct Connect ＋ AWS Transit Gateway + AWS Site-to-Site VPN	複数の VPCs のリージョンルーターへのプライベートライン経由の IPsec VPN 接続	前のオプションと同じ 最大 5,000 個のアタッチメント用の AWS マネージド高可用性とスケーラビリティのリージョンネットワークハブ	前のオプションと同じ

オプション	ユースケース	利点	制限
AWS VPN CloudHub	プライマリ接続またはバックアップ接続用のhub-and-spokeモデルでリモートブランチオフィスを接続する	既存のインターネット接続と AWS VPN 接続を再利用する AWS マネージド高可用性 VPN サービス ルートとルーティングの優先順位を交換するための BGP をサポート	ネットワークのレイテンシー、変動性、可用性はインターネットに依存します ユーザーマネージドブランチオフィスエンドポイントは、冗長性とフェイルオーバーの実装を担当します (必要な場合)
AWS Transit Gateway + SD-WAN ソリューション	バック AWS ボーンまたはインターネットをトランジットネットワークとして使用して、リモートブランチとオフィスをソフトウェア定義の広域ネットワークに接続します。	幅広い SD-WAN ベンダー、製品、プロトコルをサポート 一部のベンダーソリューションは、AWS ネイティブサービスと統合されています。	Amazon VPC に配置された SD-WAN アプライアンスの HA (高可用性) を実装するのはお客様の責任です。
ソフトウェア VPN	インターネット経由のソフトウェアアプライアンスベースの VPN 接続	幅広い VPN ベンダー、製品、プロトコルをサポート 完全にカスタマー管理されたソリューション	すべての VPN エンドポイント (必要な場合) に HA (高可用性) ソリューションを実装する責任があります。

AWS Site-to-Site VPN

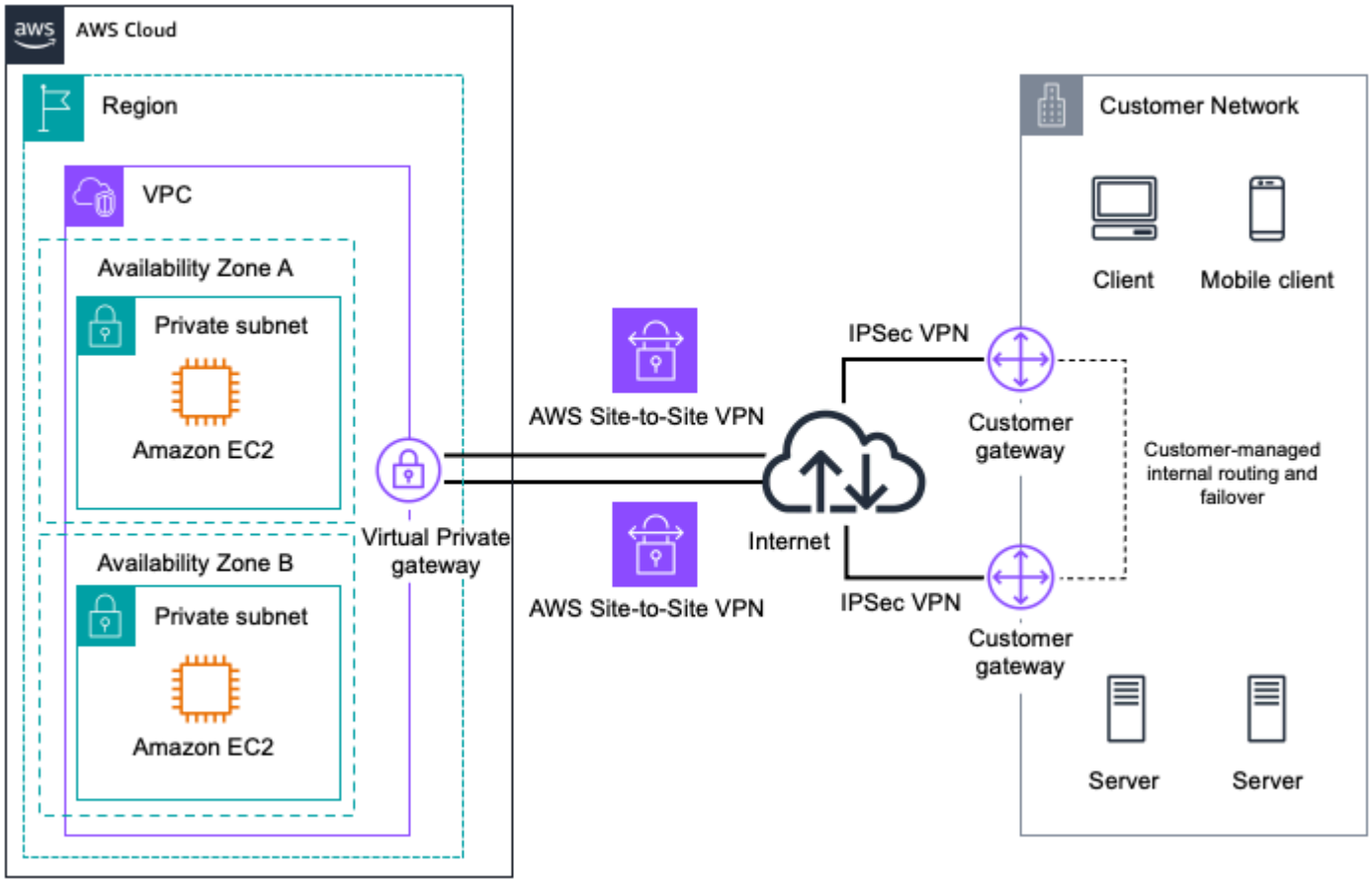
Amazon VPC には、次の図に示すように、インターネット経由でリモートネットワークと Amazon VPC の間に IPsec VPN 接続を作成するオプションがあります。



AWS Managed VPN

VPN 接続の AWS 側に組み込まれた自動冗長性とフェイルオーバーを含む AWS マネージド VPN エンドポイントを利用する場合は、このアプローチを検討してください。

仮想プライベートゲートウェイは、次の図に示すように、VPN 接続のユーザー側で冗長性とフェイルオーバーを実装できるように、複数のユーザーゲートウェイ接続もサポートおよび推奨します。



Redundant AWS Site-to-Site VPN Connections

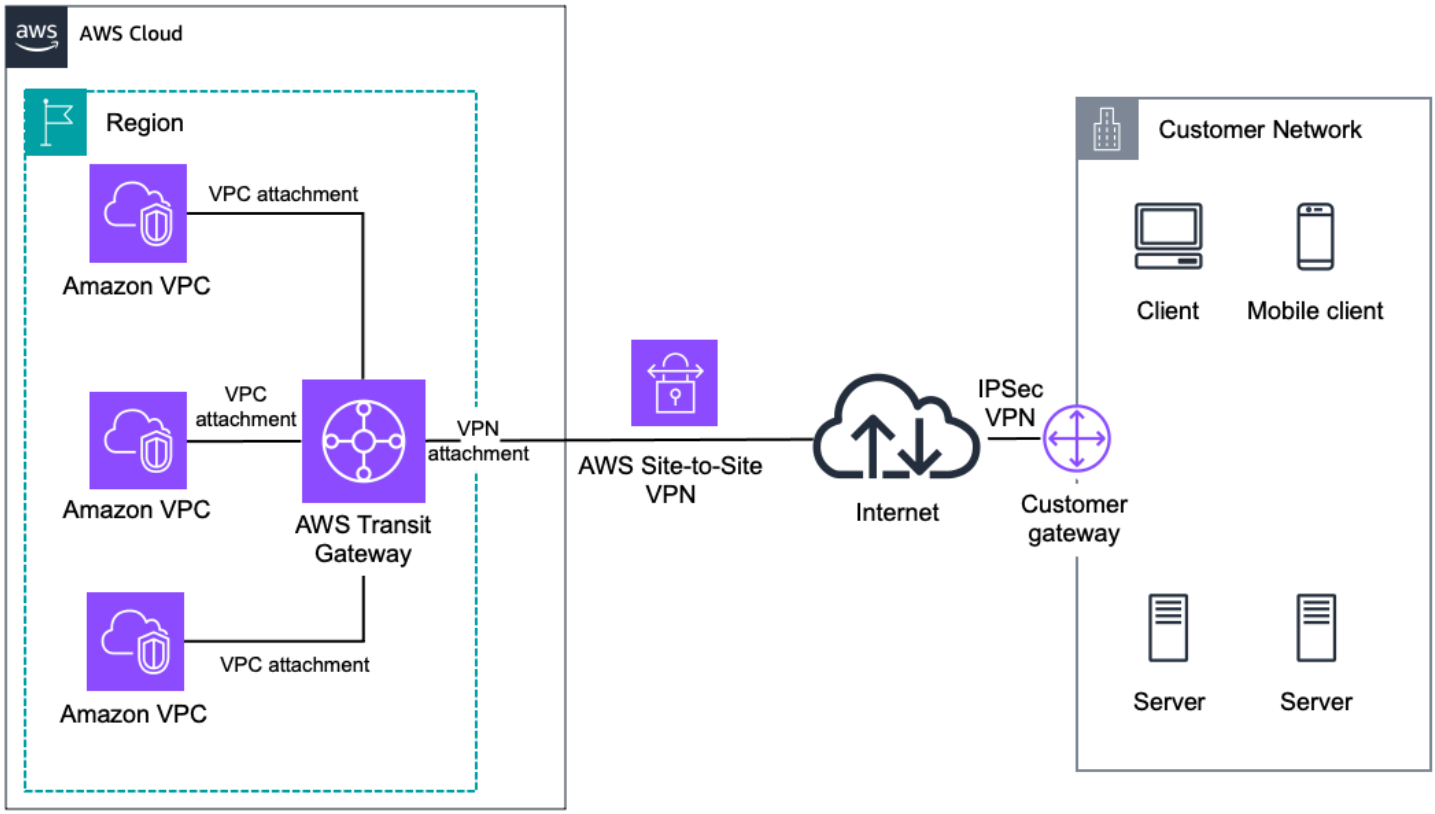
動的ルーティングオプションと静的ルーティングオプションの両方が用意されているため、ルーティング設定を柔軟に行うことができます。動的ルーティングは、BGP ピアリングを使用して AWS とこれらのリモートエンドポイント間でルーティング情報を交換します。動的ルーティングでは、BGP アドバタイズでルーティングの優先順位、ポリシー、重み (メトリクス) を指定し、ネットワークと AWS 間のネットワークパスに影響を与えることもできます。BGP を使用する場合、IPsec セッションと BGP セッションの両方を同じユーザーゲートウェイデバイスで終了する必要があるため、IPsec セッションと BGP セッションの両方を終了できる必要があることに注意してください。

追加リソース

- AWS Site-to-Site VPN ユーザーガイド
- カスタマーゲートウェイデバイスの要件
- Amazon VPC でテストされたカスタマーゲートウェイデバイス

AWS Transit Gateway + AWS Site-to-Site VPN

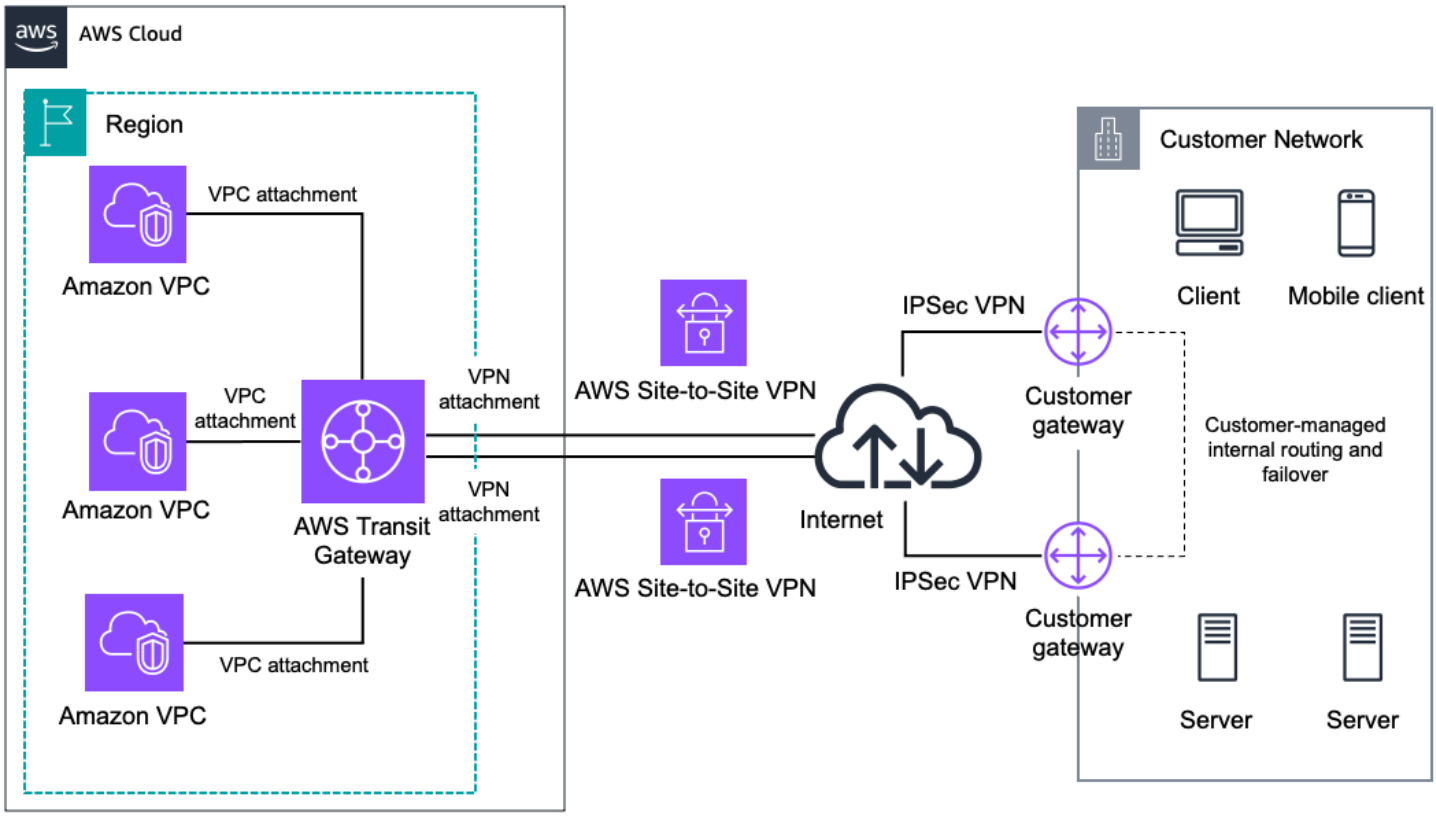
AWS Transit Gateway は、VPC とカスタマーネットワークの相互接続VPCs。AWS Transit Gateway + VPN では、Transit Gateway VPN アタッチメントを使用して、インターネット経由でリモートネットワークと Transit Gateway の間に IPsec VPN 接続を作成するオプションが用意されています。



AWS Transit Gateway and AWS Site-to-Site VPN

AWS が管理する VPN エンドポイントを利用して、同じリージョン内の複数の VPCs に接続する際に、複数の Amazon VPC への複数の IPsec VPN 接続の追加コストと管理を必要とせずに、このアプローチを使用することを検討VPCs。

AWS Transit Gateway は、次の図に示すように、VPN 接続のユーザー側で冗長性とフェイルオーバーを実装できるように、複数のユーザーゲートウェイ接続もサポートおよび推奨します。



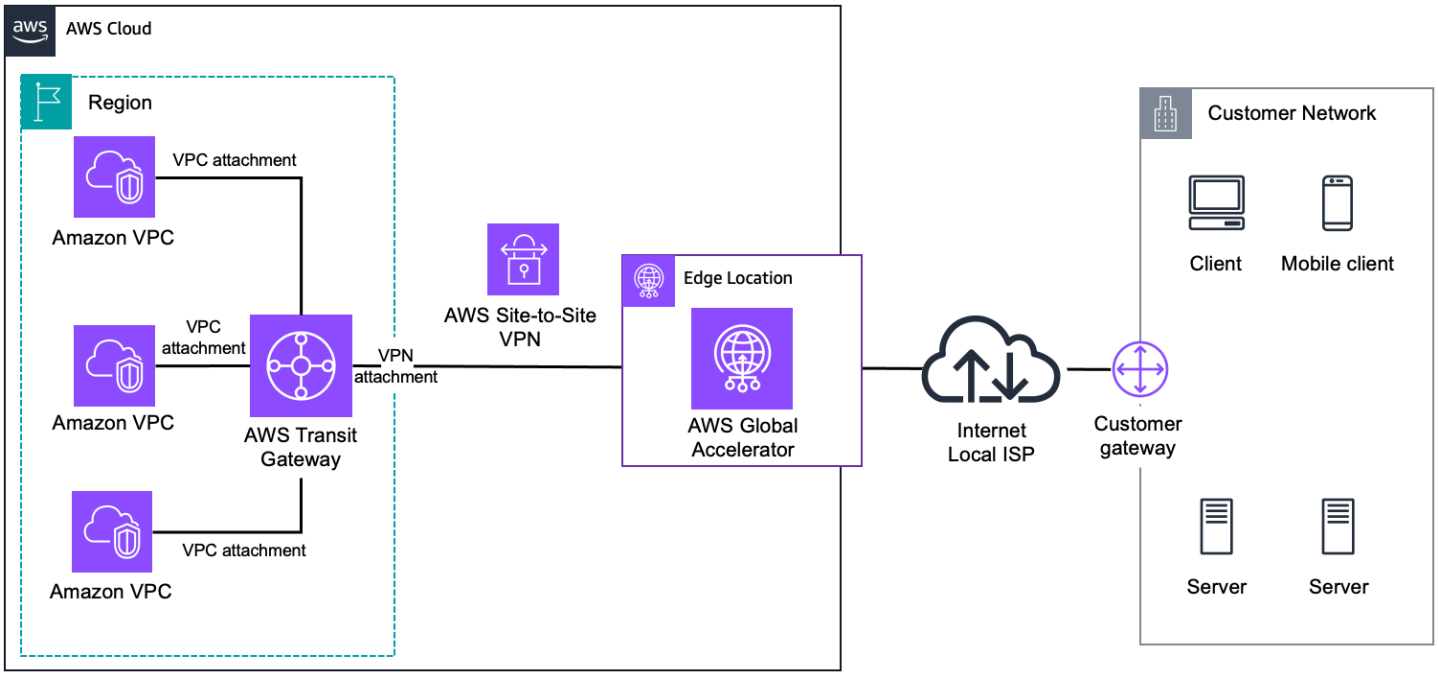
AWS Transit Gateway and Redundant VPN

Transit Gateway VPN IPsec アタッチメントのルーティング設定に柔軟性を持たせるために、動的ルーティングオプションと静的ルーティングオプションの両方が用意されています。動的ルーティングは、BGP ピアリングを使用して AWS とこれらのリモートエンドポイント間でルーティング情報を交換します。動的ルーティングでは、BGP アドバタイズでルーティングの優先順位、ポリシー、重み (メトリクス) を指定し、ネットワークと AWS 間のネットワークパスに影響を与えることもできます。BGP を使用する場合、IPsec セッションと BGP セッションの両方を同じユーザーゲートウェイデバイスで終了する必要があるため、IPsec セッションと BGP セッションの両方を終了できる必要があることに注意してください。

VPN 接続ごとに、1.25 Gbps のスループットと 140,000 パケット/秒を実現できます。Transit Gateway で VPN 接続を終了する場合、等コストマルチパス (ECMP) ルーティングを使用して、複数の VPN トンネルを集約することで、より高い VPN 帯域幅を取得できます。ECMP を使用するには、VPN 接続で動的ルーティングを設定する必要があります。ECMP は静的ルーティングではサポートされていません。

さらに、AWS Site-to-Site VPN 接続で高速化を有効にすることもできます。高速 VPN 接続では、AWS Global Accelerator を使用して、ネットワークからカスタマーゲートウェイデバイスに最も近い AWS エッジロケーションにトラフィックをルーティングします。このオプションを使用する

と、トラフィックがパブリックインターネット経由でルーティングされるときに発生する可能性のあるネットワークの中断を回避できます。高速化は、次の図に示すように、Transit Gateway にアタッチされた VPN 接続でのみサポートされています。



Accelerated AWS Site-to-Site VPN

最後に、IP アドレス指定に関して、 の Site-to-Site VPN 接続は AWS Transit Gateway IPv4 トラフィックと IPv6 トラフィックの両方をサポートします。以下のルールが適用されます。

- IPv6 は、VPN トンネルの内部 IP アドレスでのみサポートされています。 AWS エンドポイントの外部 IP アドレスはパブリック IPv4 アドレスです。カスタマーゲートウェイの IP アドレスはパブリック IPv4 アドレスである必要があります。
- Site-to-Site VPN 接続は、IPv4 トラフィックと IPv6 トラフィックの両方はサポートできません。ハイブリッド接続でデュアルスタック通信が必要な場合は、IPv4 トラフィックと IPv6 トラフィックに対して異なる VPN トンネルを作成する必要があります。

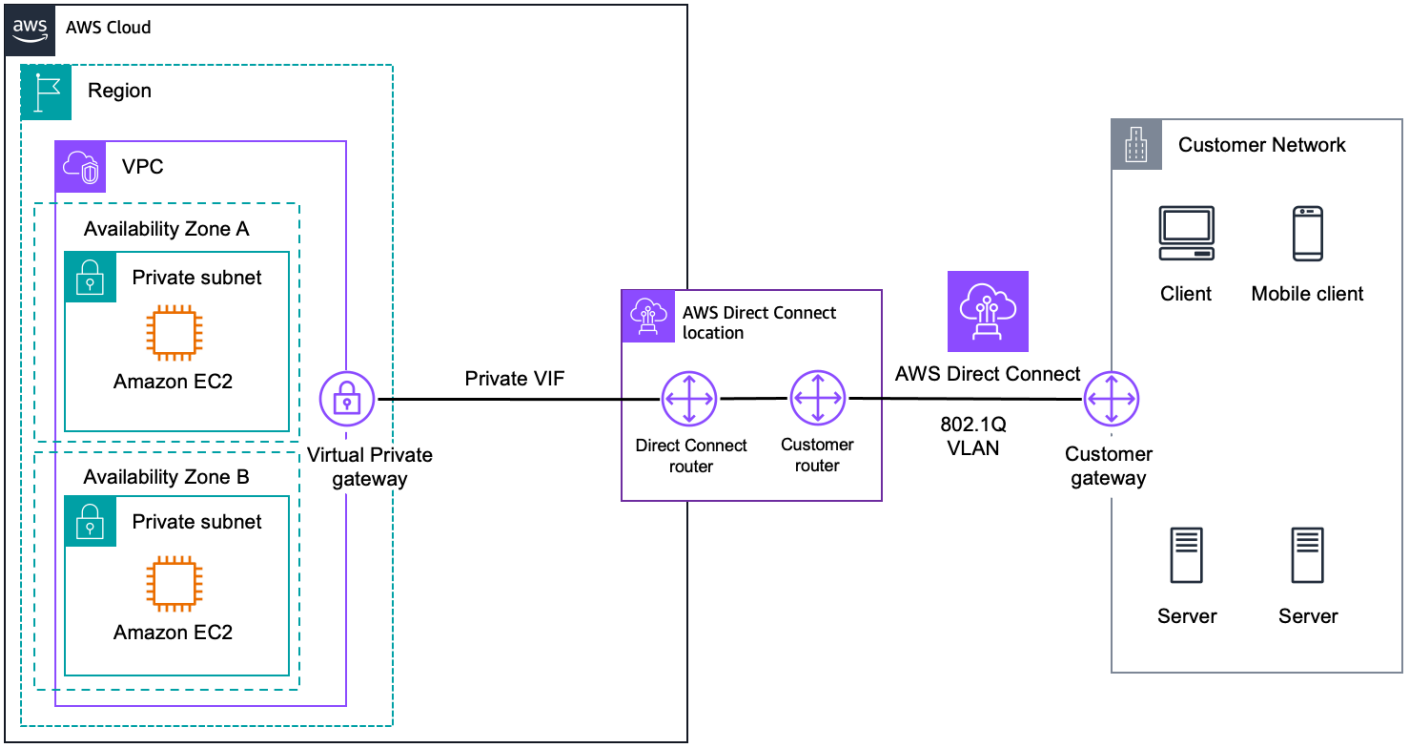
追加リソース

- トランジットゲートウェイ VPN アタッチメント
- カスタマーゲートウェイ
- Site-to-Site VPN の使用
- Site-to-Site VPN 接続の高速化

AWS Direct Connect

AWS Direct Connect を使用すると、オンプレミスネットワークから 1 つ以上の VPCs。 は、ネットワークコストを削減し、帯域幅スループットを向上させ、インターネットベースの接続よりも一貫したネットワークエクスペリエンスを提供 AWS Direct Connect できます。業界標準の 802.1Q VLANs を使用して、プライベート IP アドレスを使用して Amazon VPC に接続します。VLANs は仮想インターフェイス (VIFs) を使用して設定され、3 つの異なるタイプの VIFs を設定できます。

- パブリック仮想インターフェイス - AWS パブリックエンドポイントとデータセンター、オフィス、コロケーション環境間の接続を確立します。
- トランジット仮想インターフェイス - AWS Transit Gateway とデータセンター、オフィス、またはコロケーション環境との間にプライベート接続を確立します。この接続オプションについては、「」セクションで説明します???。
- プライベート仮想インターフェイス - Amazon VPC リソースとデータセンター、オフィス、またはコロケーション環境間のプライベート接続を確立します。プライベート VIFs の使用を次の図に示します。



AWS Direct Connect

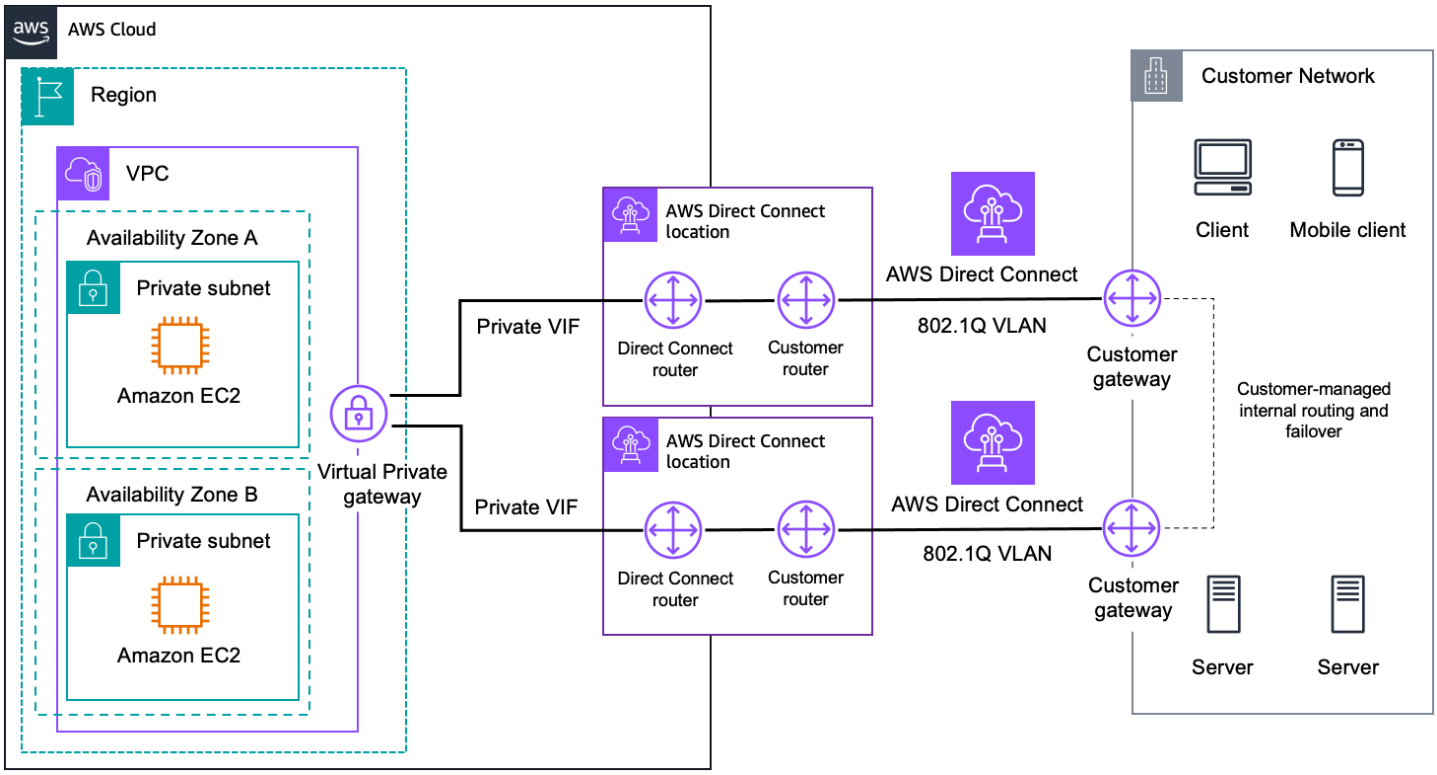
Direct Connect ロケーションの AWS デバイスへのクロスコネクトを確立 AWS Direct Connect することで、 を使用して AWS バックボーンへの接続を確立できます。Direct Connect ロケーション (中国を除く) から任意の AWS リージョンにアクセスできます。ロケーションに機器がない場合は、WAN サービスプロバイダーのエコシステムから選択して、 AWS Direct Connect ロケーションのエンドポイントを AWS Direct Connect リモートネットワークと統合できます。

では AWS Direct Connect、次の 2 種類の接続があります。

- 物理イーサネット接続が 1 人の顧客に関連付けられている専用接続。1、10、または 100 Gbps のポート速度を注文できます。 AWS Direct Connect 接続とデータセンター、オフィス、またはコロケーション環境との間にネットワーク回線を確立するために、 AWS Direct Connect パートナープログラムのパートナーと協力する必要がある場合があります。
- ホスト接続。物理イーサネット接続は AWS Direct Connect パートナーによってプロビジョニングされ、共有されます。ポート速度は 50 Mbps から 10 Gbps の間で注文できます。パートナーは、確立された AWS Direct Connect 接続と、 接続とデータセンター、オフィス、またはコロケーション環境間のネットワーク回路の両方で作業 AWS Direct Connect します。

専用接続の場合、リンク集約グループ (LAG) を使用して、単一の AWS Direct Connect エンドポイントで複数の接続を集約することもできます。これらを単一のマネージド接続として扱います。最大 4 つの 1 または 10-Gbps 接続と最大 2 つの 100-Gbps 接続を集約できます。

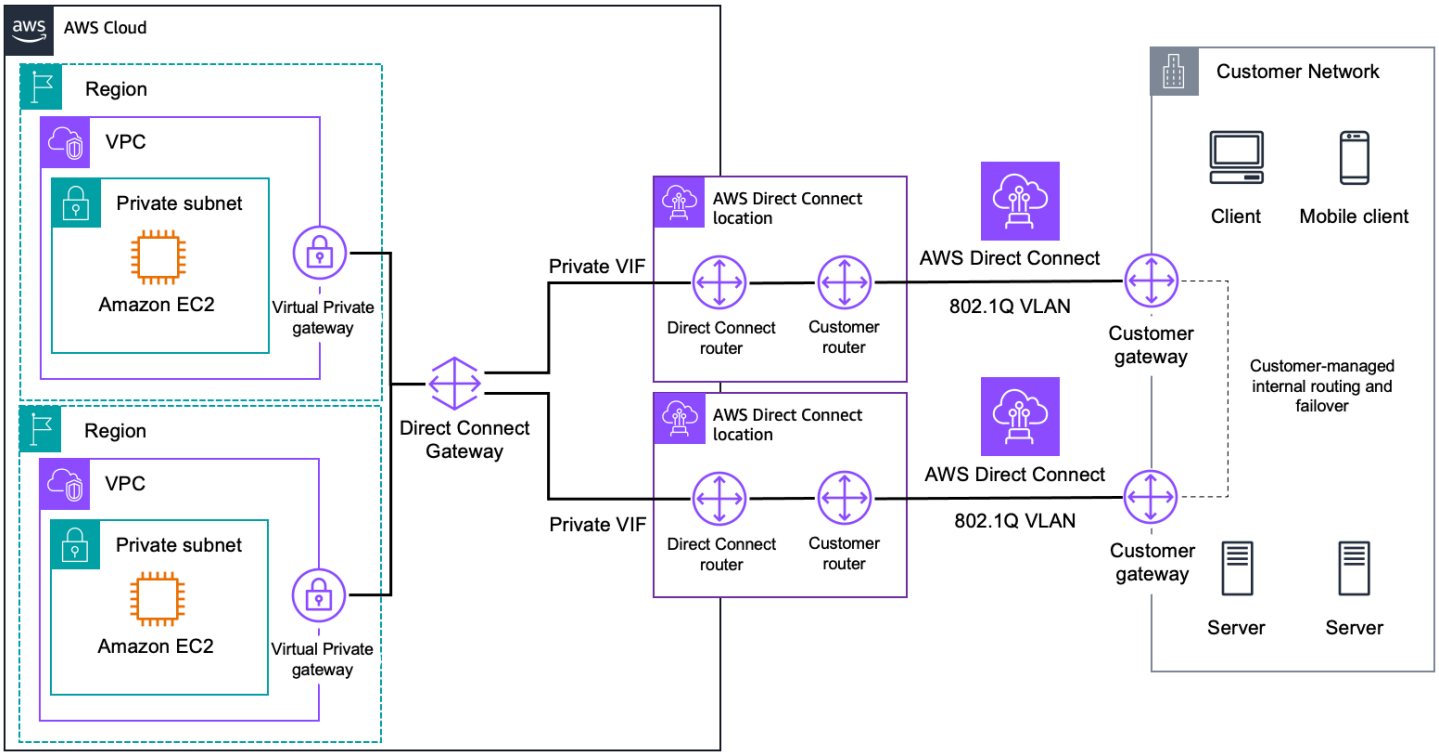
で高可用性について説明するときは AWS Direct Connect、追加の AWS Direct Connect 接続を使用することをお勧めします。AWS Direct Connect Resiliency Toolkit は、 AWS とデータセンター、オフィス、またはコロケーション環境との間に回復力の高いネットワーク接続を構築するためのガイダンスを提供します。次の図は、2 つの異なる AWS Direct Connect 場所で 2 つの接続が終了する、高回復性 AWS Direct Connect 接続オプションの例を示しています。



冗長 AWS Direct Connect

AWS Direct Connect はデフォルトでは暗号化されません。10 または 100 Gbps の専用接続では、暗号化オプションとして MAC セキュリティ (MACsec) を使用できます。1 Gbps 以下の接続の場合、接続の上に VPN トンネルを作成できます。このオプションについては、AWS Direct Connect + AWS Site-to-Site VPN「」およびAWS Direct Connect + AWS Transit Gateway + AWS Site-to-Site VPN「」セクションで説明します。

の重要なリソース AWS Direct Connect の 1 つは、Direct Connect ゲートウェイです。Direct Connect ゲートウェイは、異なるリージョンまたは AWS アカウント間で複数の Amazon VPCs または Transit Gateway への接続を可能にするグローバルに利用可能なリソースです。このリソースを使用すると、1 つのプライベート VIF またはトランジット VIF から参加している VPC またはトランジットゲートウェイに接続でき、次の図に示すように管理が軽減 AWS Direct Connect されます。



AWS Direct Connect Gateway

IP アドレス指定に関して、 AWS Direct Connect 仮想インターフェイスはデュアルスタックオペレーションの IPv4 と IPv6 の両方の BGP セッションをサポートします。

- プライベートおよびトランジット VIFs IPv4 設定では、AWS が生成した IPv4 アドレスまたはユーザーが設定したアドレスが使用されます。パブリック VIFs IPv4 BGP ピアリングでは、所有する一意のパブリック /31 IPv4 CIDR を指定する必要があります (または CIDR ブロックを割り当てるリクエストを送信する必要があります) 。
- すべてのタイプの VIFs IPv6 BGP ピアリングに対して、AWS は /125 CIDR を割り当てます。これは設定できません。

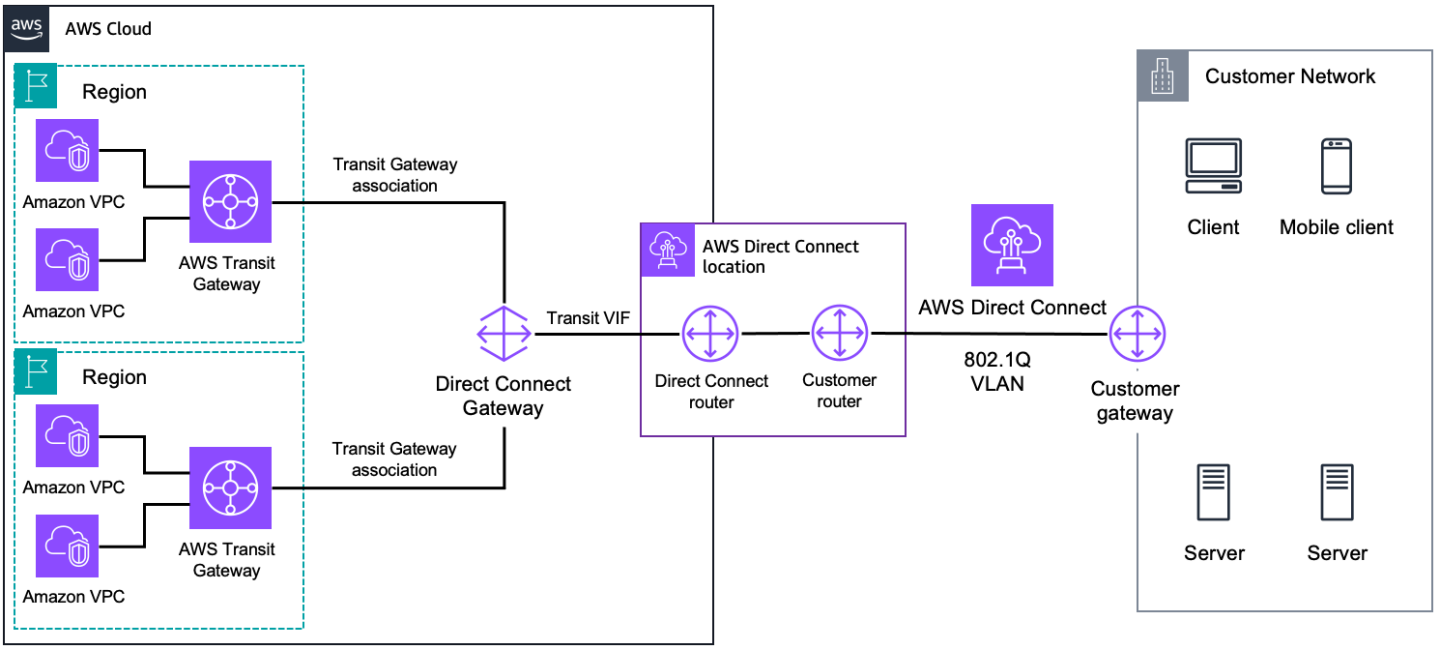
追加リソース

- AWS Direct Connect ユーザーガイド
- AWS Direct Connect 仮想インターフェイス
- AWS Direct Connect ゲートウェイ
- AWS Direct Connect レジリエンシーツールキット
- AWS Direct Connect MAC セキュリティ
- AWS Direct Connect ロケーション

- AWS Direct Connect 配信パートナー

AWS Direct Connect + AWS Transit Gateway

AWS Direct Connect + はAWS Transit Gateway、Direct Connect ゲートウェイへのトランジット VIF アタッチメントを使用して、ネットワークがプライベート専用接続を介して複数のリージョン集中型ルーターに接続できるようにします。次の図は、2 つのルーターへの接続を示しています。



AWS Direct Connect and AWS Transit Gateway

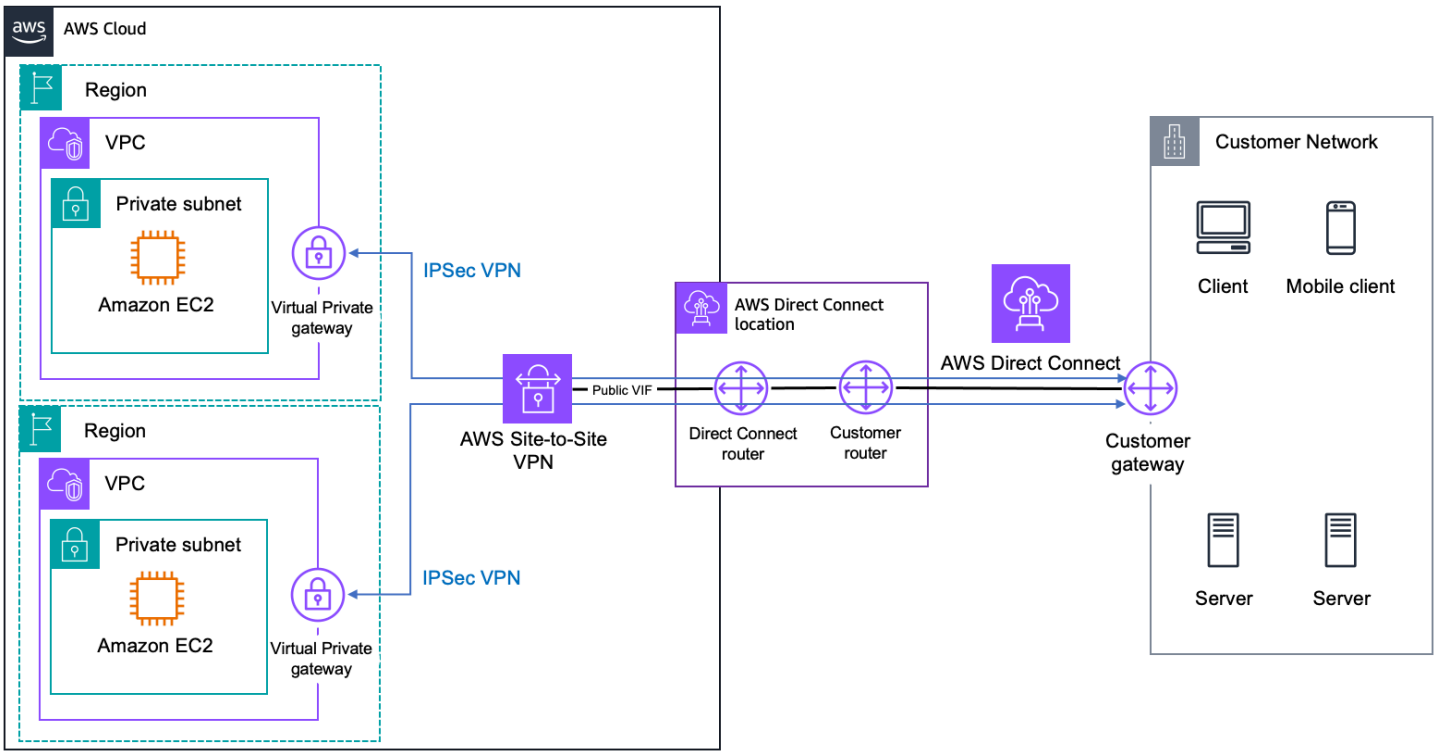
各 AWS Transit Gateway は、同じリージョンの VPCs を相互接続するネットワークトランジットハブであり、Amazon VPC ルーティング設定を 1 か所に統合します。このソリューションは、プライベート接続を介した Amazon VPC とネットワーク間の接続の管理を簡素化し、ネットワークコストを削減し、帯域幅スループットを向上させ、インターネットベースの接続よりも一貫したネットワークエクスペリエンスを提供します。

追加リソース

- AWS Direct Connect ユーザーガイド
- のリンク集約グループ AWS Direct Connect
- ブログ記事: Sub-1 Gbps ホスト接続と AWS Transit Gateway の統合

AWS Direct Connect + AWS Site-to-Site VPN

AWS Direct Connect + AWS Site-to-Site VPN を使用すると、 AWS Direct Connect 接続を AWS マネージド VPN ソリューションと組み合わせることができます。 AWS Direct Connect パブリック VIFs は、ネットワークと AWS Site-to-Site VPN エンドポイントなどのパブリック AWS リソース間の専用ネットワーク接続を確立します。サービスへの接続を確立したら、対応する Amazon VPC 仮想プライベートゲートウェイへの IPsec 接続を作成できます。次の図は、このオプションを示しています。



AWS Direct Connect and AWS Site-to-Site VPN

このソリューションは、end-to-endの安全な IPsec 接続の利点を低レイテンシーと の帯域幅の増加と組み合わせ AWS Direct Connect 、インターネットベースの VPN 接続よりも一貫したネットワークエクスペリエンスを提供します。BGP 接続セッションは、 AWS Direct Connect とパブリック VIF 上のルーターの間で確立されます。別の BGP セッションまたは静的ルートが、仮想プライベートゲートウェイと IPsec VPN トンネル上のルーターの間に確立されます。

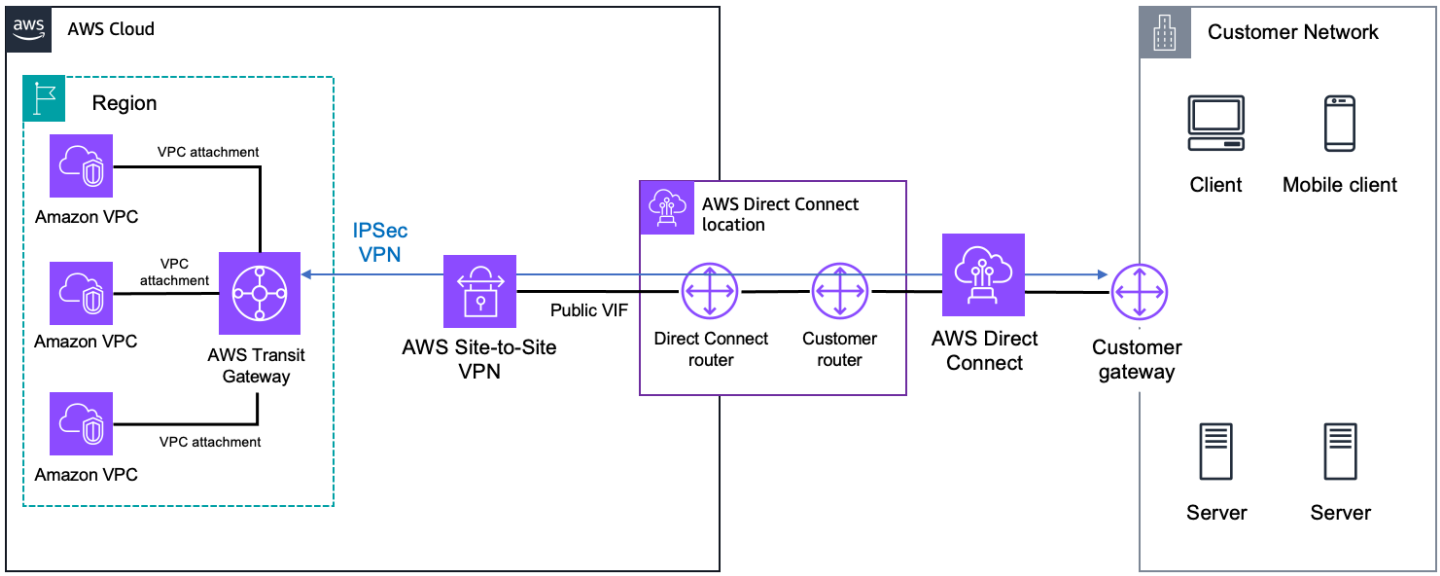
追加リソース

- AWS Direct Connect
- AWS Direct Connect 仮想インターフェイス
- AWS Site-to-Site VPN ユーザーガイド

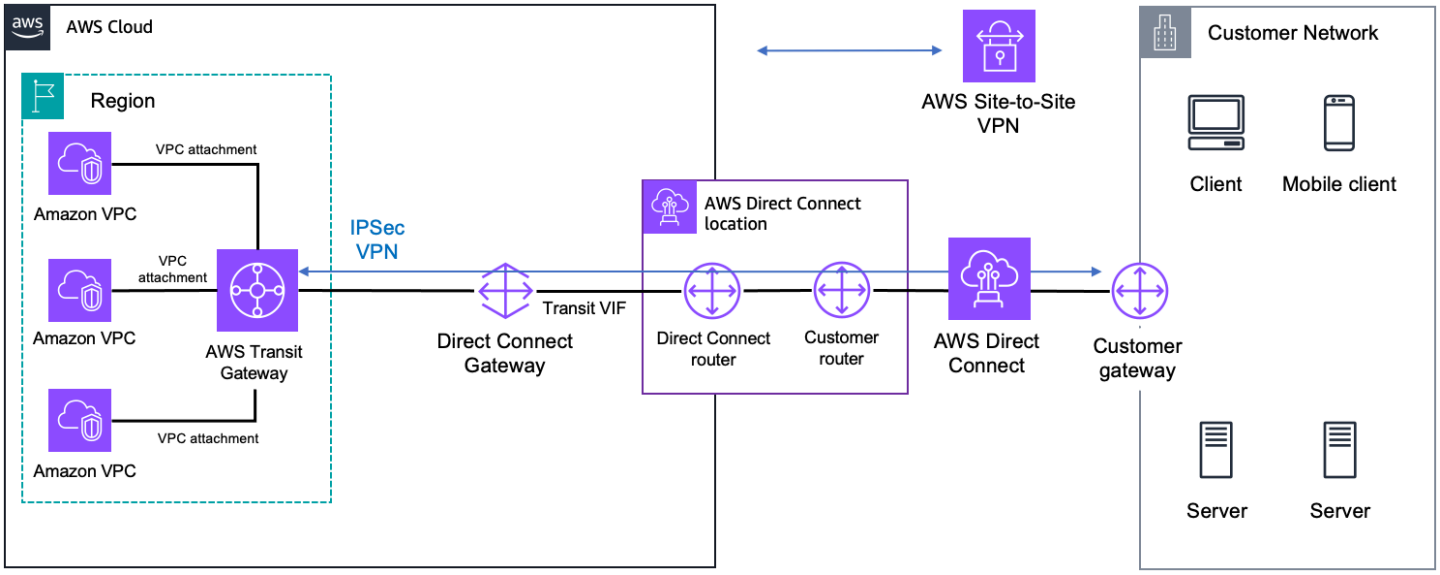
AWS Direct Connect + AWS Transit Gateway + AWS Site-to-Site VPN

AWS Direct Connect + AWS Transit Gateway + AWS Site-to-Site VPN を使用すると、プライベート専用接続を介して、ネットワークと Amazon VPCs 用のリージョン集中型ルーター間のend-to-endの IPsec 暗号化接続を有効にできます。

AWS Direct Connect パブリック VIFs を使用して、まずネットワークと AWS Site-to-Site VPN エンドポイントなどのパブリック AWS リソース間の専用ネットワーク接続を確立できます。この接続が確立されたら、 への IPsec 接続を作成できます AWS Transit Gateway。次の図は、このオプションを示しています。



AWS Direct Connect, AWS Transit Gateway, and AWS Site-to-Site VPN (public VIF)



AWS Direct Connect, AWS Transit Gateway, and AWS Site-to-Site VPN (transit VIF)

このアプローチは、管理を簡素化し、同じリージョン内の複数の Amazon VPCs への IPsec VPN 接続のコストを最小限に抑え、低レイテンシーで一貫したネットワークエクスペリエンスを実現する場合に、インターネットベースの VPN よりもプライベート専用接続を使用するというメリットをもたらします。BGP セッションは、パブリックまたはトランジット VIF を使用して、 AWS Direct Connect とルーターの間で確立されます。別の BGP セッションまたは静的ルートが、 AWS Transit Gateway と IPsec VPN トンネル上のルーターの間に確立されます。

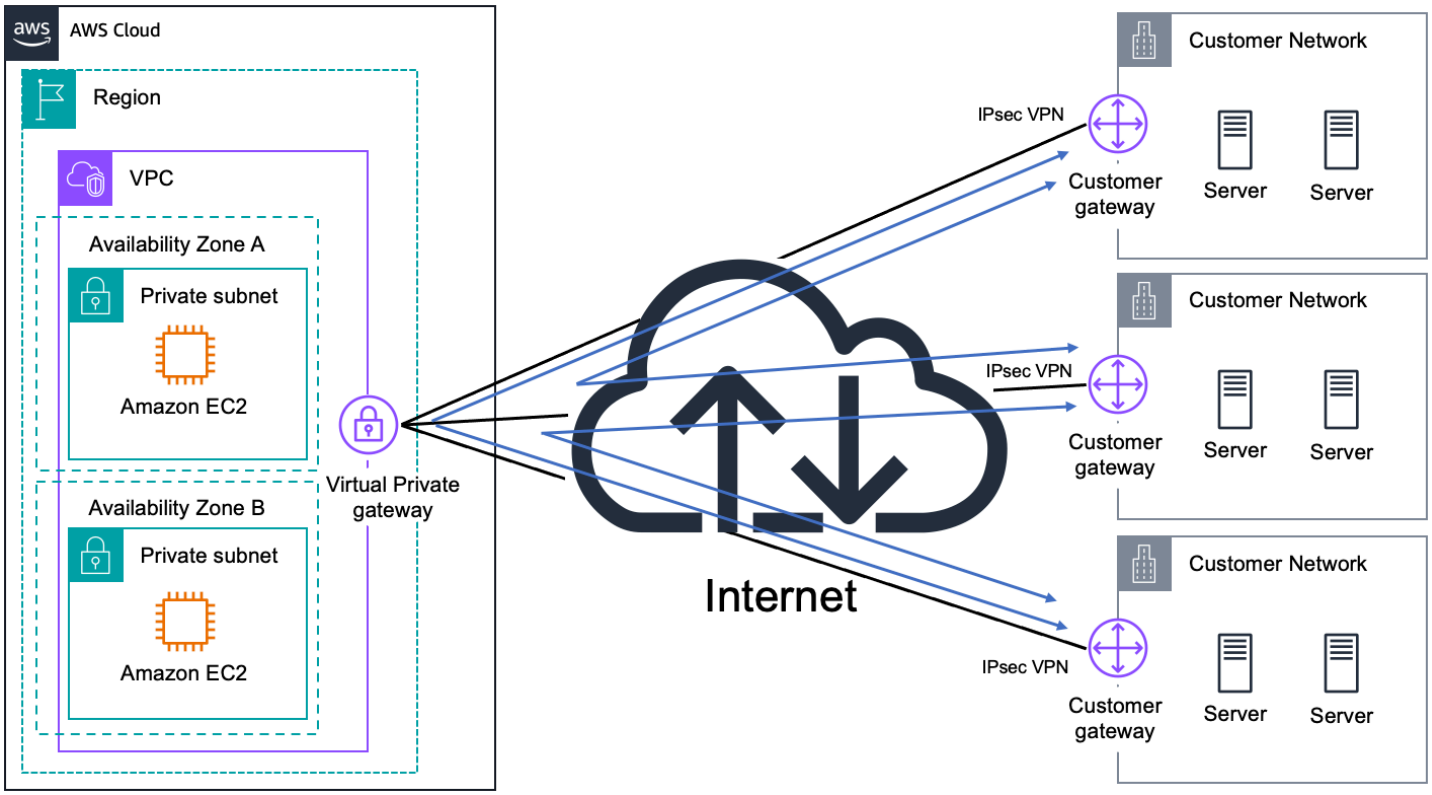
追加リソース

- AWS Direct Connect 仮想インターフェイス
- トランジットゲートウェイ VPN アタッチメント
- カスタマーゲートウェイデバイスの要件
- Amazon VPC でテストされたカスタマーゲートウェイデバイス
- AWS Site-to-Site VPN — を使用したプライベート IP VPN AWS Direct Connect

AWS VPN CloudHub

前述の AWS マネージド VPN オプションに基づいて、 AWS VPN CloudHub を使用して、あるサイトから別のサイトに安全に接続できます。 AWS VPN CloudHub は、VPC の有無にかかわらず使用できるシンプルなhub-and-spokeモデルで動作します。複数のブランチオフィスと既存のインターネット接続があり、これらのリモートオフィス間のプライマリ接続またはバックアップ接続に、便利で低コストのhub-and-spokeモデルを実装する場合は、このアプローチを使用します。

次の図は、 AWS VPN CloudHub アーキテクチャを示しています。このアーキテクチャでは、リモートサイト間のネットワークトラフィックが AWS VPN 接続経由でルーティングされていることを示す行が表示されています。



AWS VPN CloudHub

AWS VPN CloudHub は、複数のカスタマーゲートウェイを持つ Amazon VPC 仮想プライベートゲートウェイを使用し、それぞれに一意の BGP 自動システム番号 (ASNs) を使用します。リモートサイトに重複する IP 範囲があってはなりません。ゲートウェイは、VPN 接続を介して適切なルート (BGP プレフィックス) をアドバタイズします。これらのルーティングアドバタイズは、各 BGP ピアに対して受信および再アドバタイズされ、各サイトが他のサイトとの間でデータを送受信できるようになります。

追加リソース

- VPN CloudHub を使用してサイト間の安全な通信を提供する
- AWS Site-to-Site VPN ユーザーガイド
- カスタマーゲートウェイデバイスの要件
- Amazon VPC でテストされたカスタマーゲートウェイデバイス

AWS Transit Gateway + SD-WAN ソリューション

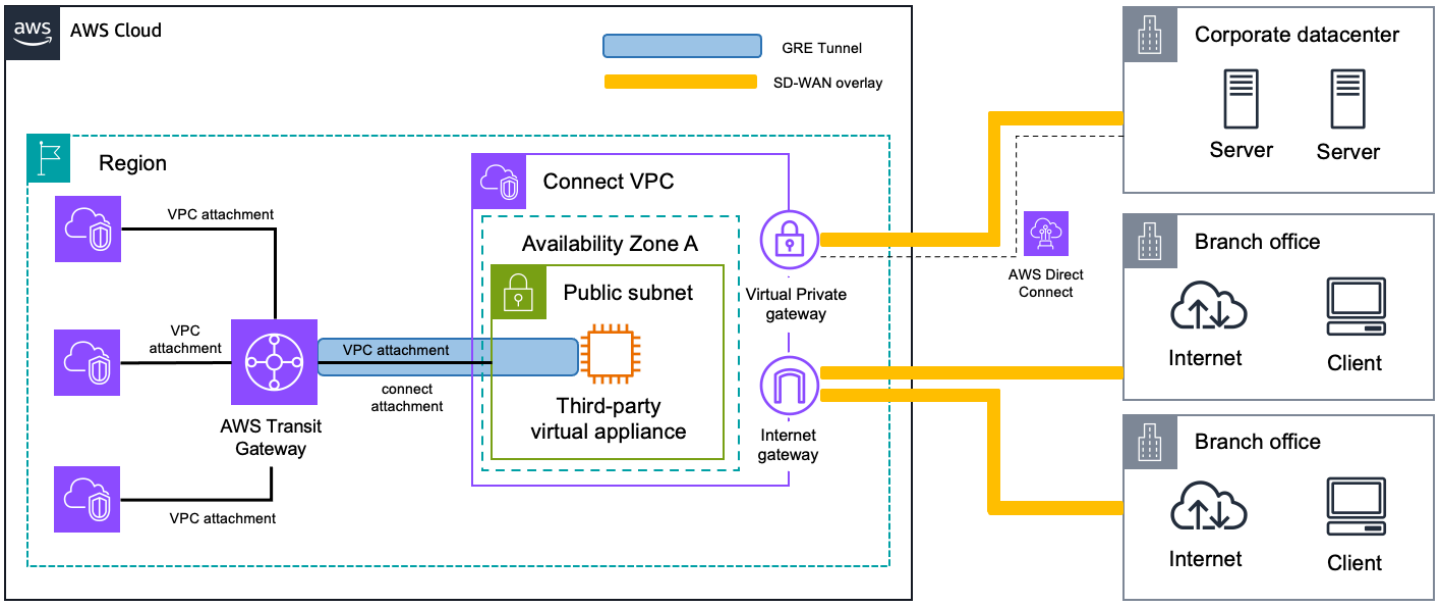
Software Defined Wide Area Networks (SD-WANs) は、データセンター、オフィス、またはコロケーション環境をさまざまなトランジットネットワーク (を使用するパブリックインターネット、Splunk ネットワーク、AWS バックボーンなど AWS Direct Connect) に接続し、ネットワーク条件、アプリケーションタイプ、またはサービス品質 (QoS) 要件に基づいて、最も適切で効率的なパス全体でトラフィックを自動的かつ動的に管理するために使用します。

このアプローチは、複雑なネットワークトポロジーがあり、複数のデータセンター、オフィス、またはコロケーション環境が自分自身と AWS の間で通信する必要がある場合に使用します。SD-WAN ソリューションは、このタイプのネットワークを効率的に管理するのに役立ちます。

SD-WAN ネットワークと AWS の接続について話す場合、 はVPCsでスケーラブルなマネージドリージョンネットワークトランジットハブ AWS Transit Gateway を提供します。Transit Gateway 接続アタッチメントは、SD-WAN インフラストラクチャとアプライアンスを AWS に接続するためのネイティブな方法を提供します。これにより、IPsec VPNs を設定することなく、SD-WAN を AWS に簡単に拡張できます。

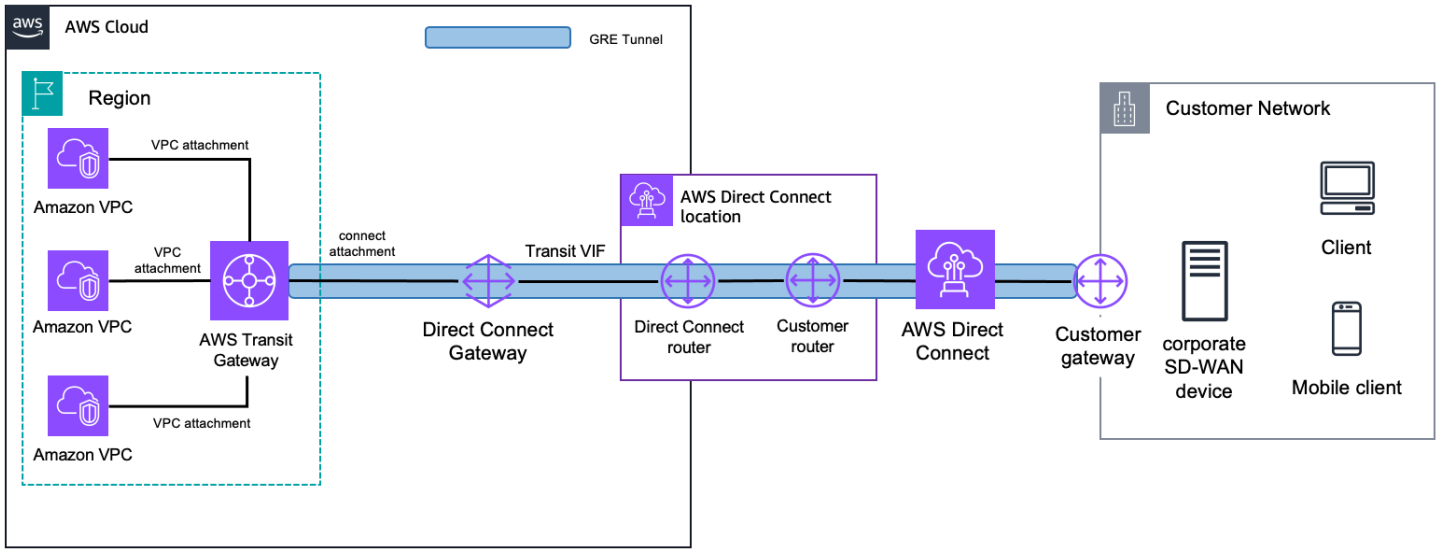
Transit Gateway 接続アタッチメントは、VPN 接続と比較して帯域幅パフォーマンスを向上させる汎用ルーティングカプセル化 (GRE) をサポートしています。動的ルーティングのボーダーゲートウェイプロトコル (BGP) をサポートし、静的ルートを設定する必要がなくなります。これにより、ネットワーク設計が簡素化され、関連する運用コストを削減できます。さらに、Transit Gateway Network Manager との統合により、グローバルネットワークトポロジ、アタッチメントレベルのパフォーマンスメトリクス、テレメトリデータを通じて高度な可視性を提供します。

接続アタッチメントを使用して SD-WAN ネットワークを Transit Gateway に統合する場合、2 つの一般的なパターンがあります。1 つ目は、SD-WAN ネットワークの仮想アプライアンスを AWS 内の VPC に配置することです。次に、次の図に示すように、仮想アプライアンスと Transit Gateway 間の Transit Gateway Connect アタッチメントの基盤となるトランスポートとして VPC アタッチメントを使用します。



SD-WAN connectivity with AWS Transit Gateway (virtual appliance in AWS)

または、追加のインフラストラクチャを追加することなく、SD-WAN トラフィックを AWS に拡張してセグメント化することもできます。次の図に示すように、基盤となるトランスポートとして AWS Direct Connect 接続を使用して Transit Gateway 接続アタッチメントを作成できます。



SD-WAN connectivity with AWS Transit Gateway (Direct Connect as transport)

Transit Gateway 接続アタッチメントを使用する際には、いくつかの考慮事項があります。

- 既存の Transit Gateway に接続アタッチメントを作成できます。

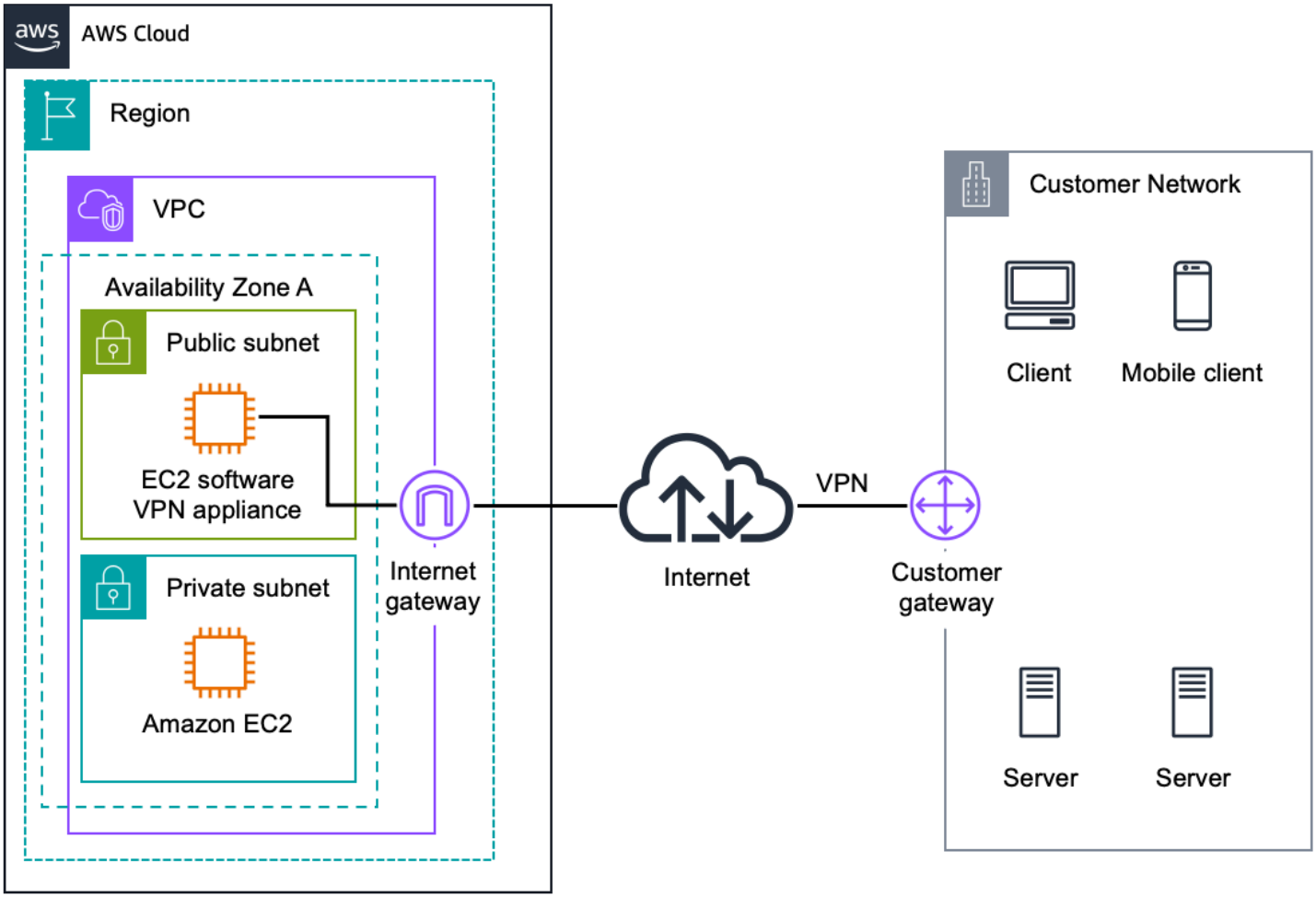
- 接続アタッチメントを使用して Transit Gateway からトラフィックを送受信するには、サードパーティーアプライアンスを GRE トンネルで設定する必要があります。アプライアンスは、動的ルート更新とヘルスチェックのために BGP で設定する必要があります。
- Connect アタッチメントは静的ルートをサポートしていません。
- Transit Gateway 接続アタッチメントは、GRE トンネルあたり 5 Gbps の最大帯域幅をサポートします。5 Gbps を超える帯域幅は、同じ Connect アタッチメントに対して複数の Connect ピア (GRE トンネル) に同じプレフィックスをアドバタイズすることで実現できます。
- 接続アタッチメントごとに最大 4 つの Connect ピアがサポートされています。
- Transit Gateway 接続アタッチメントは、BGP のマルチプロトコル拡張 (MBGP または MP-BGP) による IPv6 および動的ルートアドバタイズをサポートします。

追加リソース

- 「Transit Gateway ピアリングアタッチメント」
- 要件と考慮事項
- ブログ記事: AWS Transit Gateway Connect による SD-WAN 接続の簡素化

ソフトウェア VPN

Amazon VPC では、リモートネットワークと Amazon VPC ネットワークで実行されているソフトウェア VPN アプライアンスの間に VPN 接続を作成することで、Amazon VPC 接続の両側を完全に管理できる柔軟性が得られます。このオプションは、コンプライアンスの目的で、または Amazon VPC の VPN ソリューションで現在サポートされていないゲートウェイデバイスを活用するために、VPN 接続の両端を管理する必要がある場合に推奨されます。次の図は、このオプションを示しています。



ソフトウェア Site-to-Site VPN

Amazon EC2 で実行されるソフトウェア VPN アプライアンスを作成した複数のパートナーとオープンソースコミュニティのエコシステムから選択できます。この選択に加えて、設定、パッチ、アップグレードなど、ソフトウェアアプライアンスを管理する必要があります。

この設計では、ソフトウェア VPN アプライアンスが 1 つの Amazon EC2 インスタンスで実行されるため、ネットワーク設計に単一障害点が発生する可能性があることに注意してください。詳細については、「ソフトウェア VPN インスタンスの付録 A: ソフトウェア VPN インスタンスの高レベル HA アーキテクチャアーキテクチャ」を参照してください。

追加リソース

- で利用可能な VPN アプライアンス AWS Marketplace
- 技術概要 - Cisco ASA を VPC EC2 インスタンスに接続する (IPsec)
- 技術概要 - 複数の VPCs EC2 インスタンスに接続する (IPsec)

- 技術概要 - 複数の VPCsを EC2 インスタンス (SSL) に接続する

Amazon VPC-to-Amazonオプション

複数の Amazon VPCs をより大きな仮想ネットワークに統合する場合は、これらの設計パターンを使用します。これは、Amazon VPCs間で AWS リソースをより簡単に統合するために、セキュリティ、請求、複数のリージョンでのプレゼンス、または内部チャージバック要件のために複数の VPCs が必要な場合に便利です。これらのパターンを Network-to-Amazon VPC 接続オプションと組み合わせて、リモートネットワークと複数の VPCs にまたがる企業ネットワークを作成することもできます。

VPC 間の VPCsは、接続する VPC ごとに重複しない IP 範囲を使用する場合に最適です。たとえば、複数の VPCs を接続する場合は、各 VPC に一意の Classless Inter-Domain Routing (CIDR) 範囲が設定されていることを確認してください。したがって、各 VPC で使用する 1 つの連続した重複しない CIDR ブロックを割り当てることをお勧めします。Amazon VPC のルーティングと制約の詳細については、「Amazon VPC に関するよくある質問」を参照してください。

オプション	ユースケース	利点	制限
VPC ピアリング	2 つの VPCs 間の AWS 提供のネットワーク接続。	AWS マネージドスケーラブルネットワークインフラストラクチャを活用	VPC ピアリングは推移的なピアリング関係をサポートしていません 大規模な管理が困難
AWS Transit Gateway	VPCs 用の AWS 提供のリージョンルーター接続	AWS マネージド高可用性およびスケーラビリティサービス 最大 5,000 個のアタッチメント用のリージョンネットワークハブ	Transit Gateway ピアリングは静的ルートのみをサポートします
AWS PrivateLink	インターフェイスエンドポイントを使用した 2 つの VPCs 間	AWS マネージドスケーラブルネットワークインフラストラクチャを活用	VPC エンドポイントサービスは、それらが作成された AWS

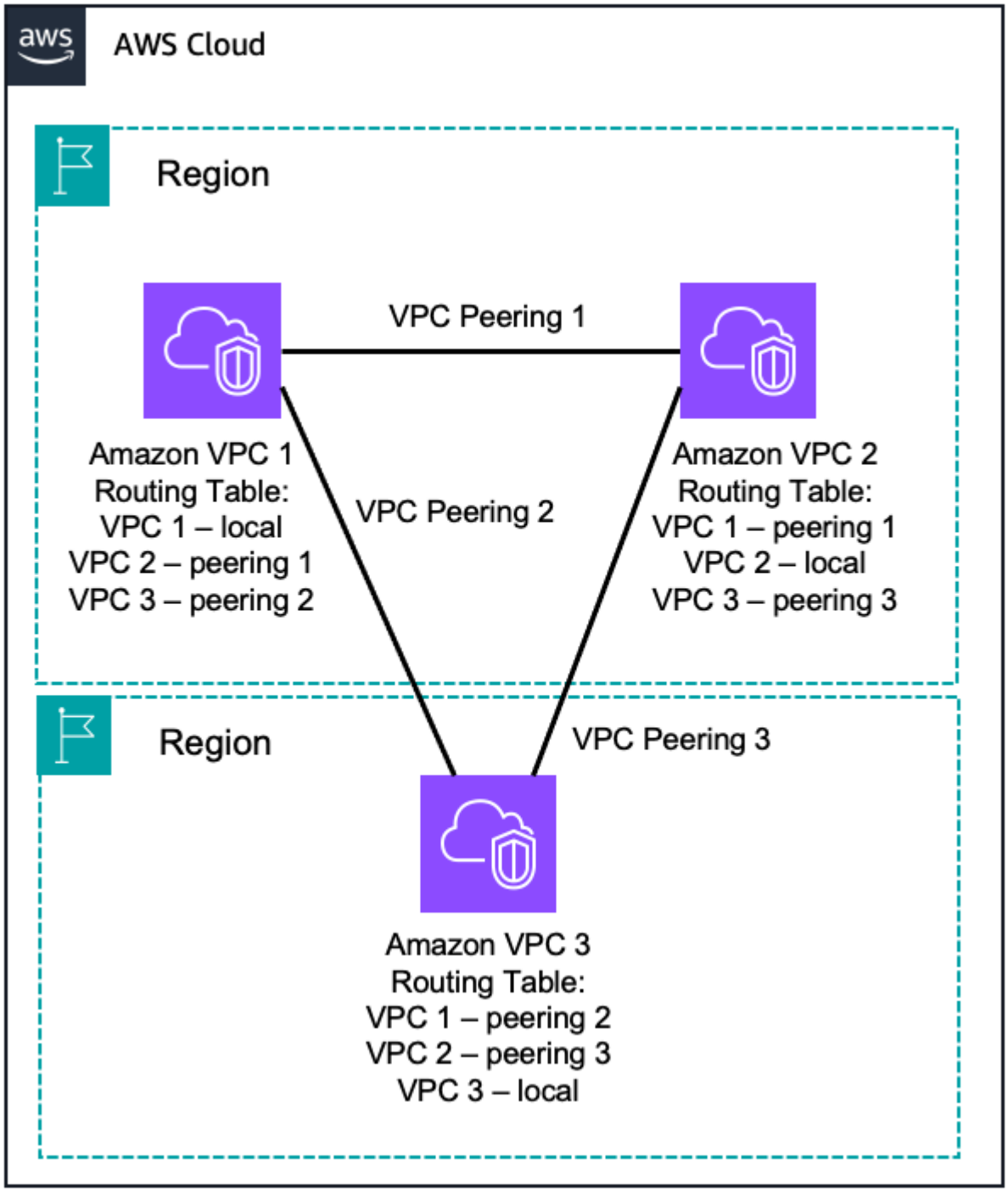
オプション	ユースケース	利点	制限
	の AWS 提供のネットワーク接続		リージョンでのみ使用できます
ソフトウェア VPN	VPCs 間のソフトウェアアプライアンスベースの VPN 接続	さまざまな VPN ベンダー、製品、プロトコルをサポート ユーザーが完全に管理する	すべての VPN エンドポイントに HA ソリューションを実装する責任があります (必要な場合) VPN インスタンスがネットワークのボトルネックになる可能性がある
ソフトウェア VPN-to-AWS Site-to-Site VPN	VPCs 間のソフトウェアアプライアンスから VPN への接続	AWS マネージド高可用性 VPC VPN 接続 お客様が管理するさまざまな VPN ベンダーと製品をサポート 静的ルートと動的 BGP ピアリングおよびルーティングポリシーをサポート	ソフトウェアアプライアンス VPN エンドポイントの HA ソリューションを実装する責任はお客様にあります (必要な場合)。 VPN インスタンスがネットワークのボトルネックになる可能性がある AWS Managed VPN への IPsec VPN プロトコルのみ

VPC ピアリング

VPC ピア接続は、同じネットワーク内にあるかのように各 VPC のプライベート IP アドレスを使用してルーティングできるようにする、2 つの VPC 間のネットワーキング接続です。VPC ピアリング

接続は、独自の VPCs 間、または別の AWS アカウントの VPC との間で作成できます。VPC ピアリングは、リージョン間ピアリングもサポートしています。

リージョン間 VPC ピアリングを使用するトラフィックは、常にグローバル AWS バックボーンにとどまり、パブリックインターネットを経由することはありません。これにより、一般的なエクスプロイトや DDoS 攻撃などの脅威ベクトルが減少します。



VPC-to-VPC Peering

AWS は VPC の既存のインフラストラクチャを使用して VPC ピアリング接続を作成し、個別の物理ハードウェアに依存しません。したがって、VPCs 間で単一障害点やネットワーク帯域幅のボトルネックが発生する可能性はありません。さらに、VPC ルーティングテーブル、セキュリティグループ、ネットワークアクセスコントロールリストを活用して、VPC ピアリング接続を利用できるサブネットまたはインスタンスを制御できます。

Amazon VPCs推移的なピア接続をサポートしていません。つまり、3 番目の VPCs を転送として使用して直接ピア接続されていない 2 つの VPC を通信することはできません。すべての VPCs が VPC ピアリングを使用して相互に通信できるようにする場合は、各 VPC 間に 1:1 VPC ピアリング接続を作成する必要があります。または、 AWS Transit Gateway または AWS Cloud WAN を使用して、ネットワークトランジットハブとして機能します。

IPv4 トラフィックと IPv6 トラフィックはどちらも VPC ピアリング接続でサポートされています。ただし、使用されているセカンダリ IPv4 または IPv6 CIDR ブロックに関係なく、プライマリ IPv4 CIDR ブロックが重複している場合、2 つの VPCs をピアリングすることはできません。VPCs 間で VPC ピアリングを使用する予定がある場合は、プライマリ CIDR ブロックを VPC に割り当てるときにこの点を考慮してください。

追加リソース

- Amazon VPC ピアリング
- VPC ピアリングとは

AWS Transit Gateway

AWS Transit Gateway は、hub-and-spokeアーキテクチャを使用してリージョンの AWS VPC ルーティング設定を統合するための、可用性とスケーラビリティに優れたサービスです。各スポーク VPC は、他の接続された VPCs にアクセスするために、Transit Gateway にのみ接続する必要があります。IPv4 トラフィックと IPv6 トラフィックの両方が でサポートされています AWS Transit Gateway。

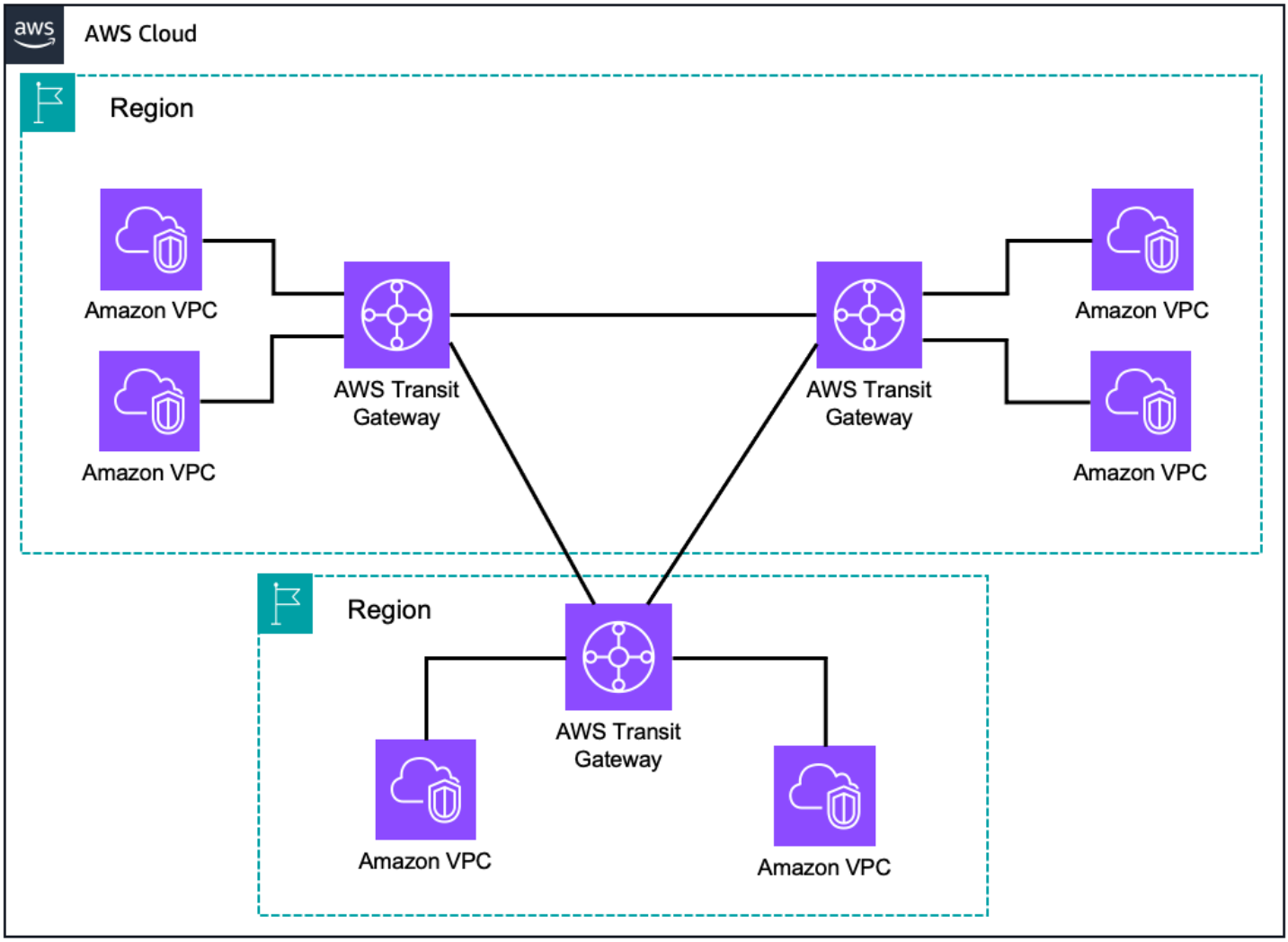
複数の Transit Gateway ルートテーブル、関連付け、伝達を活用して、同じ Transit Gateway 内でトラフィックをセグメント化できます。1 つの管理ポイントから異なるルーティングドメイン (本番トラフィックや非本番トラフィックなど) を管理できるため、これらのルーティングドメインは相互に通信できなくなります。

また、Transit Gateway によって作成されたhub-and-spokeアーキテクチャを活用して、トラフィック検査、インターフェイス VPC エンドポイントアクセス、NAT ゲートウェイまたは NAT インスタ

ンスを介したトラフィックの出力などの共有サービスへのアクセスを一元化することもできます。この一元化により、複数の VPCs でこれらのリソースを管理する複雑さが簡素化され、AWS でフットプリントを拡張する際の制御が向上します。

トランジットゲートウェイは、同じ AWS リージョン内または異なる AWS リージョン間で相互にピア接続できます。 AWS Transit Gateway トラフィックは常にグローバル AWS バックボーンにとどまり、パブリックインターネットを通過することはありません。これにより、一般的なエクスプロイトや DDoS 攻撃などの脅威ベクトルが軽減されます。

次の図に示すように、Transit Gateway は多数の VPCs で VPC-to-VPC通信管理を簡素化します。



AWS Transit Gateway

Transit Gateway との間で送受信される IP トラフィックを一元的に可視化するために、Transit Gateway フローログを Amazon CloudWatch Logs と Amazon S3 に発行できます。フローログデー

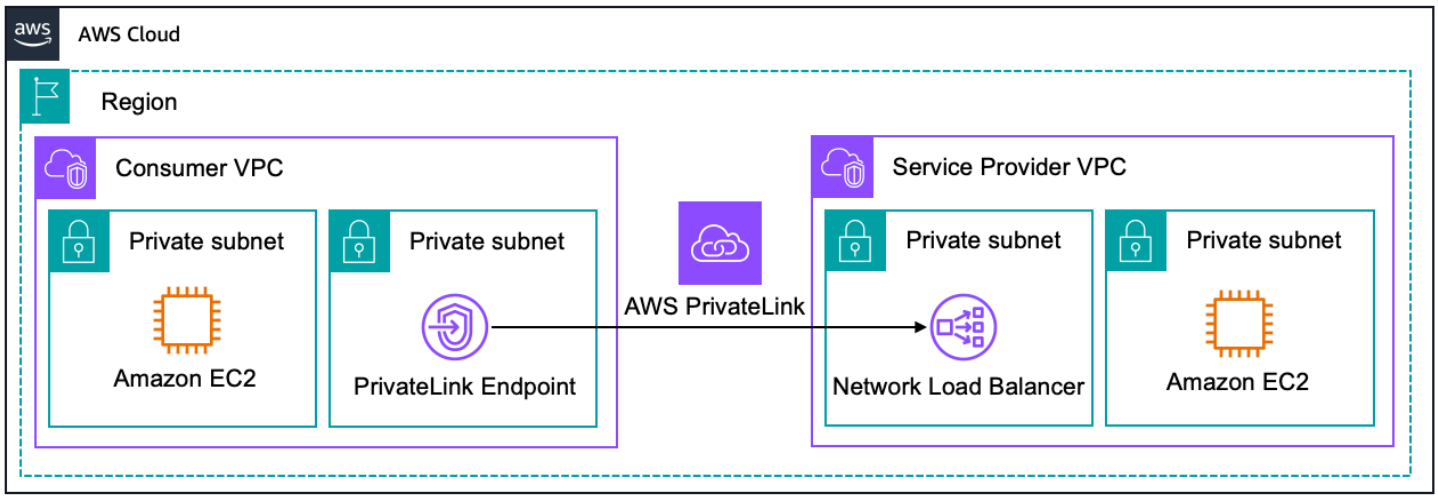
タはネットワークトラフィックのパスの外で収集されるため、ネットワークのスループットやレイテンシーには影響しません。

追加リソース

- Amazon VPC トランジットゲートウェイ
- 「Transit Gateway ピアリングアタッチメント」
- Transit Gateway の使用
- Transit Gateway フローログを使用したネットワークトラフィックのログ記録

AWS PrivateLink

AWS PrivateLink では、VPC 内のプライベート IP アドレスを介して、一部の AWS サービス、他の AWS アカウントによってホストされるサービス (エンドポイントサービスと呼ばれる) 、およびサポートされている AWS Marketplace パートナーサービスに接続できます。インターフェイスエンドポイントは、VPC のサブネット内の Elastic Network Interface と IP アドレスを使用して、VPC 内で直接作成されます。つまり、VPC セキュリティグループを使用してエンドポイントへのアクセスを管理できます。



AWS PrivateLink

プライベート IP アドレスを使用して、AWS ネットワーク内で別の VPC によって提供されるサービスを安全に使用する場合は、このアプローチをお勧めします。または、 AWS PrivateLink VPCs の IP アドレスが重複している場合に が適しています。

AWS PrivateLink は IPv6 を完全にサポートしていますが、デュアルスタックを使用するには、送信先 VPCs、VPC サブネット、Network Load Balancer、DNS 名の両方を有効にするか変更する必要が

あります。これらの前提条件が満たされると、エンドポイントのサービス設定で IPv6 を有効にできます。

へのアクセスコントロール AWS PrivateLink

インターフェイスエンドポイントは、VPC のサブネットで Elastic Network Interface と IP アドレスを使用して VPC 内に直接作成されます。つまり、VPC セキュリティグループを使用して、エンドポイントへのネットワークアクセスを管理できます。

インターフェイスエンドポイントまたはゲートウェイエンドポイントを作成するときに、エンドポイントポリシーをアタッチすることもできます。エンドポイントポリシーは、VPC エンドポイントを使用してエンドポイントサービスにアクセスできる AWS プリンシパル (AWS アカウント、IAM ユーザー、ロール) を制御します。

1 つのエンドポイントに複数のポリシーを関連付けることはできません。ただし、エンドポイントポリシーはいつでも変更できます。

エンドポイントポリシーは、IAM ユーザーポリシーまたはサービス固有のポリシー (Amazon S3 バケットポリシーなど) を上書きまたは置き換えません。Amazon S3 に接続するためにインターフェイスエンドポイントを使用する場合、Amazon S3 バケットポリシーを使用して、特定のエンドポイントまたは特定の VPC からのバケットへのアクセスを制御できます。

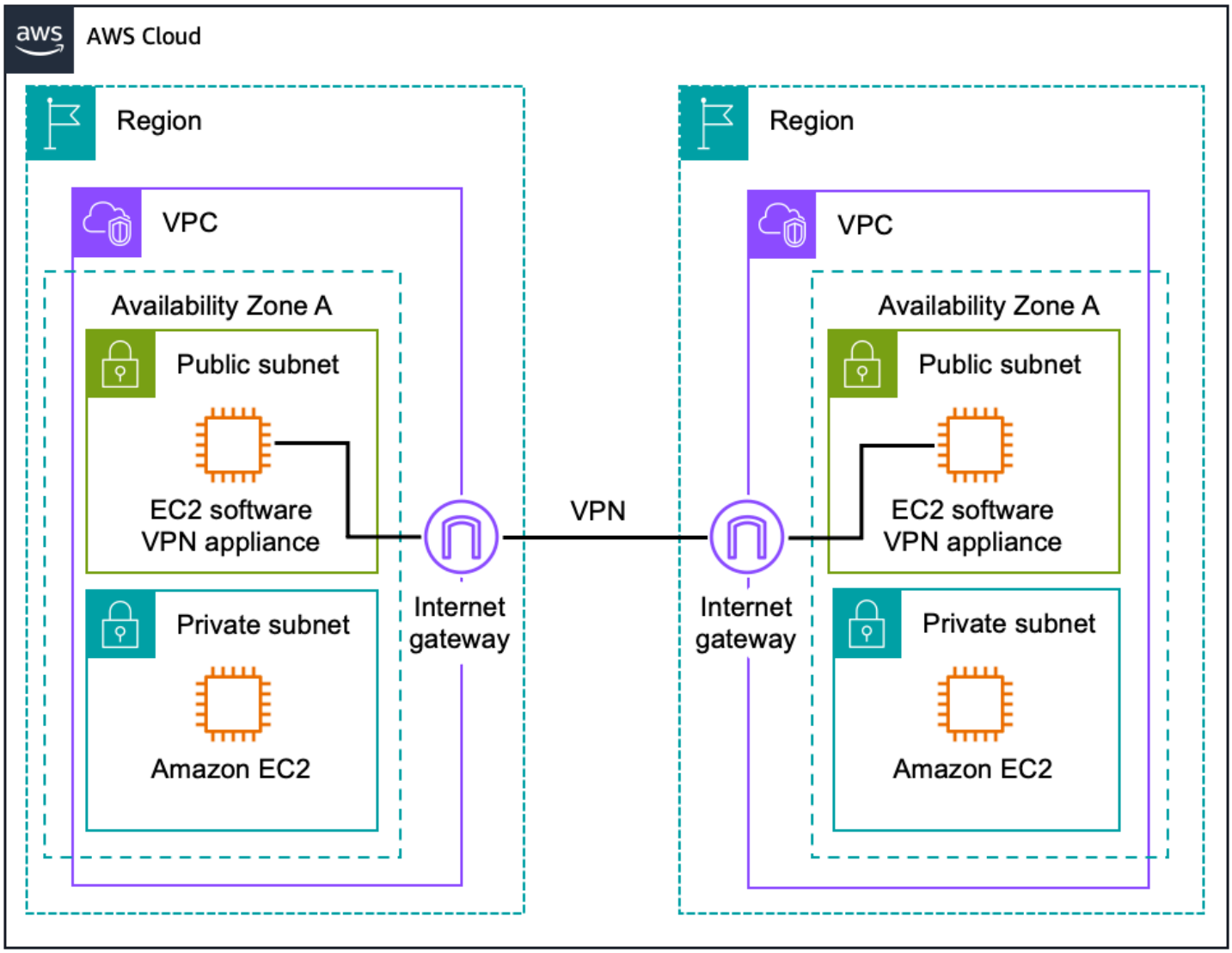
追加リソース

- インターフェイス VPC エンドポイント (AWS PrivateLink)
- VPC エンドポイントサービス (AWS PrivateLink)
- ブログ記事: PrivateLink サービスとエンドポイントを使用して IPv6 の導入を迅速化する
- ブログ記事: Connecting Networks with Overlaping IP Ranges
- AWS PrivateLink パートナー

ソフトウェア VPN

Amazon VPC は、ネットワークルーティングの柔軟性を提供します。これには、2 つ以上のソフトウェア VPN アプライアンス間に安全な VPN トンネルを作成して、複数の VPCs をより大きな仮想プライベートネットワークに接続し、各 VPC のインスタンスがプライベート IP アドレスを使用してシームレスに相互に接続できるようにする機能が含まれます。このオプションは、任意の VPN ソ

フトウェアプロバイダーを使用して VPN 接続の両端を管理する場合に推奨されます。このオプションは、各 VPC にアタッチされたインターネットゲートウェイを使用して、ソフトウェア VPN アプライアンス間の通信を容易にします。



Software Site-to-Site VPN VPC-to-VPC Routing

Amazon EC2 で実行されるソフトウェア VPN アプライアンスを作成した複数のパートナーとオープンソースコミュニティのエコシステムから選択できます。この選択に加えて、設定、パッチ、アップグレードなどのソフトウェアアプライアンスを管理する責任も負います。

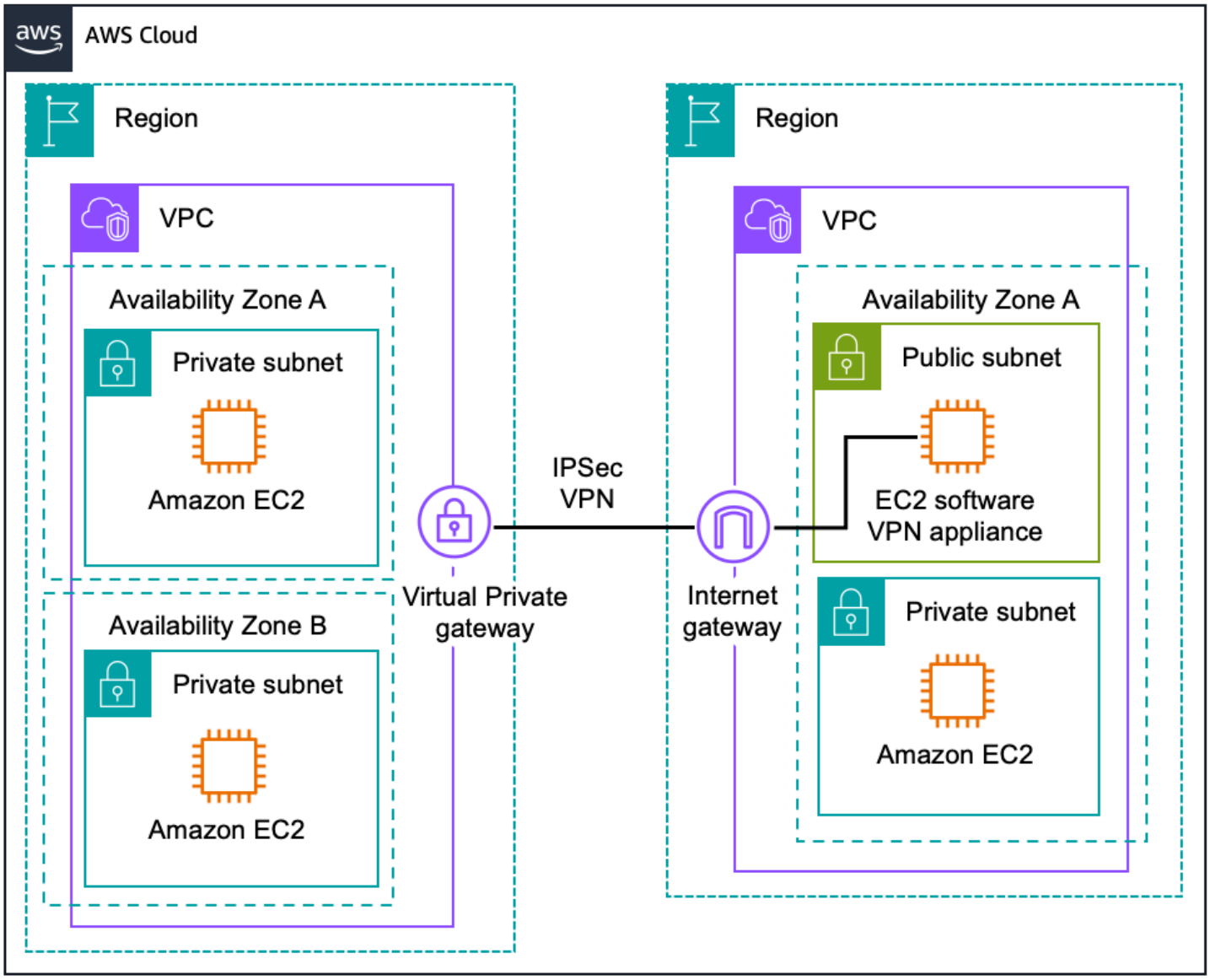
この設計では、ソフトウェア VPN アプライアンスが 1 つの Amazon EC2 インスタンスで実行されるため、ネットワーク設計に単一障害点が発生する可能性があることに注意してください。詳細については、「付録 A: ソフトウェア VPN インスタンスの高レベル HA アーキテクチャ」を参照してください。

追加リソース

- から利用可能な VPN アプライアンス AWS Marketplace
- 技術概要 - 複数の VPCs EC2 インスタンスに接続する (IPsec)
- 技術概要 - 複数の VPCsを EC2 インスタンス (SSL) に接続する

ソフトウェア VPN-to-AWS Site-to-Site VPN

Amazon VPC は、AWS マネージド VPN とソフトウェア VPN オプションを組み合わせて複数の VPCs を接続する柔軟性を提供します。この設計により、ソフトウェア VPN アプライアンスと仮想プライベートゲートウェイの間に安全な VPN トンネルを作成し、各 VPC のインスタンスがプライベート IP アドレスを使用してシームレスに相互に接続できるようになります。このオプションは、次の図に示すように、ある Amazon VPC に仮想プライベートゲートウェイを使用し、別の Amazon VPC にインターネットゲートウェイとソフトウェア VPN アプライアンスの組み合わせを使用します。



Software VPN to AWS Site-to-Site VPN VPC-to-VPC Routing

この設計では、ネットワーク設計に単一障害点が発生する可能性があることに注意してください。詳細については、「付録 A: ソフトウェア VPN インスタンスの高レベル HA アーキテクチャ」を参照してください。

追加リソース

- から利用可能な VPN アプライアンス AWS Marketplace
- AWS Site-to-Site VPN ユーザーガイド
- カスタマーゲートウェイデバイスの要件

Amazon VPC access-to-Amazonソフトウェアリモートアクセス接続オプション

ソフトウェアリモートアクセス VPN を使用すると、低コスト、伸縮自在、安全なサービスを活用してリモートアクセスソリューションを実装しながら、AWS ホストリソースへのシームレスな接続エクスペリエンスを提供できます。このオプションは、通常、リモートネットワークがそれほど広範ではない小規模企業や、従業員向けのリモートアクセスソリューションをまだ構築およびデプロイしていない小規模企業に推奨されます。

これらのパターンをNetwork-to-Amazon VPC への接続オプション接続オプション および と組み合わせてAmazon VPC-to-Amazonオプション、リモートネットワークと複数の VPCs にまたがるネットワークを作成できます。

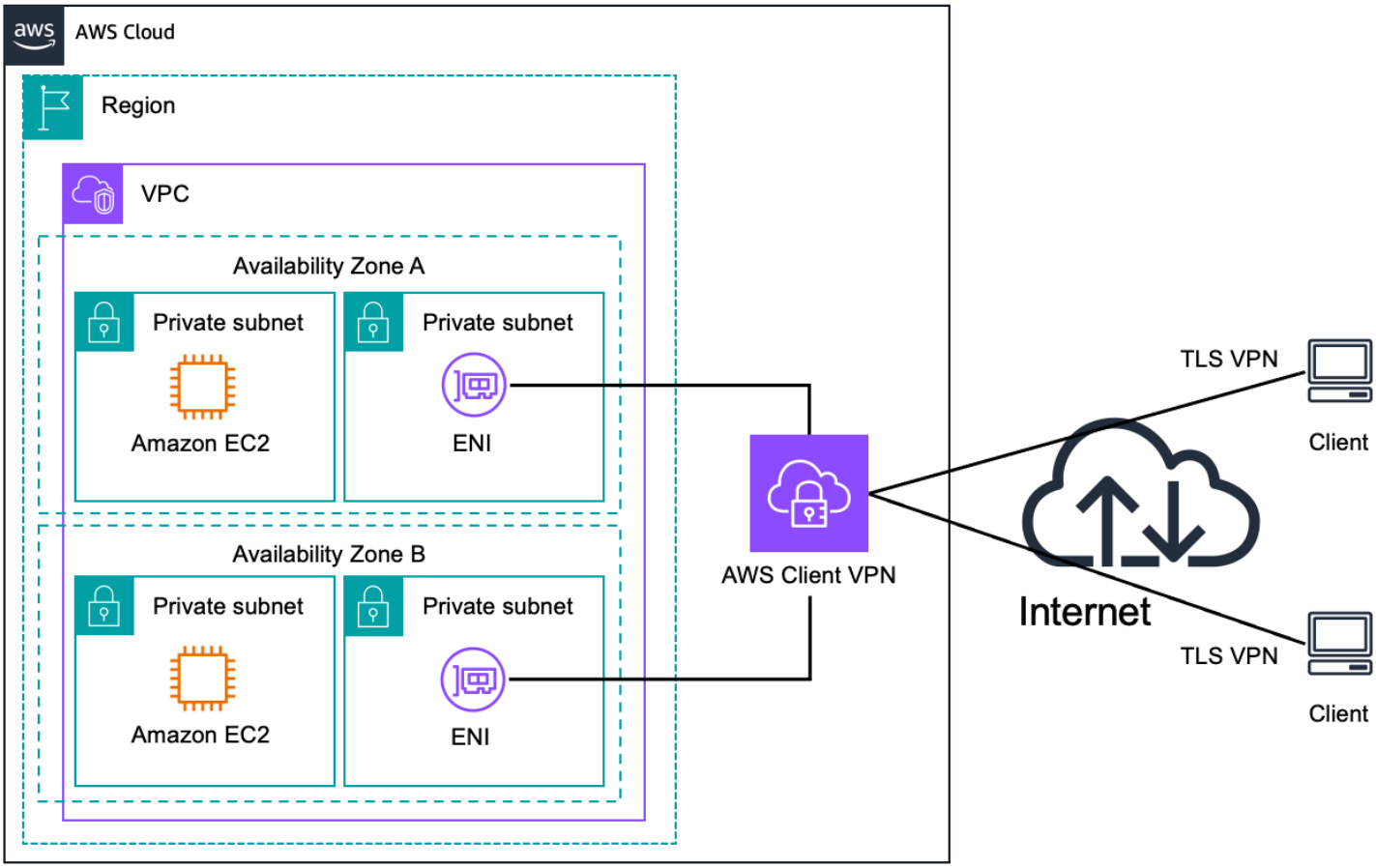
次の表は、これらのオプションの利点と制限の概要を示しています。

オプション	ユースケース	利点	制約事項
AWS クライアント VPN	Amazon VPC や内部ネットワークへの AWS マネージドリモートアクセスソリューション	AWS マネージドの高可用性とスケーラビリティサービス	OpenVPN クライアントのみ
ソフトウェアクライアント VPN	Amazon VPC や内部ネットワークへのソフトウェア VPN アプライアンスのリモートアクセスソリューション	幅広い VPN ベンダー、製品、プロトコルをサポート 完全にカスタマー管理されたソリューション	HA ソリューションの実装はお客様の責任となります。

AWS クライアント VPN

AWS Client VPN は、AWS マネージドの高可用性およびスケーラビリティサービスで、安全なソフトウェアのリモートアクセスを可能にします。次の図に示すように、リモートクライアントと

Amazon VPCs の間に安全な TLS 接続を作成して、インターネット経由で AWS リソースとオンプレミスに安全にアクセスするオプションを提供します。



AWS Client VPN Remote Access

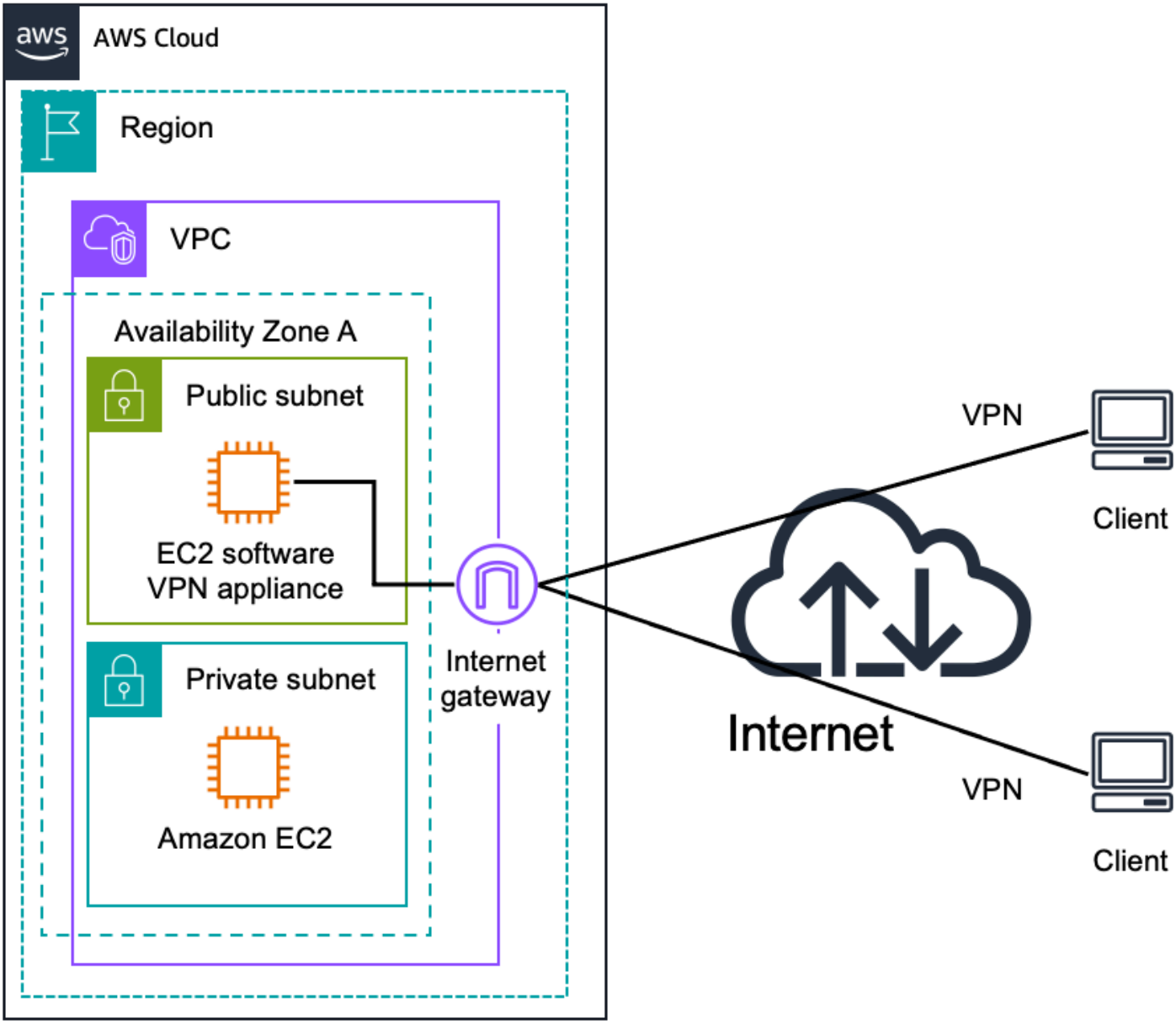
リモートクライアントは、AWS Client VPN for Desktop またはサードパーティーの OpenVPN VPN クライアントで、Active Directory による認証または相互証明書認証のいずれかを使用できます。

追加リソース

- AWS Client VPN 管理者ガイド

ソフトウェアクライアント VPN

Amazon EC2 で実行されるリモートアクセスソリューションを生成した複数のパートナーとオープンソースコミュニティのエコシステムから選択できます。これらのソリューションは、次の図に示すように、Amazon VPCs へのリモートアクセス、インターネット経由で AWS リソースとオンプレミスに安全にアクセスするためのセキュリティプロトコルの使用に高い柔軟性を提供します。



Software Client VPN Remote Access

リモートアクセスソリューションは、複雑性が高く、複数のクライアント認証オプション (多要素認証を含む) をサポートしており、Microsoft Active Directory やその他の LDAP/多要素認証ソリューションなど、Amazon VPC またはリモートでホストされる ID およびアクセス管理ソリューション (network-to-Amazon VPC へのオプションの 1 つを活用) と統合できます。

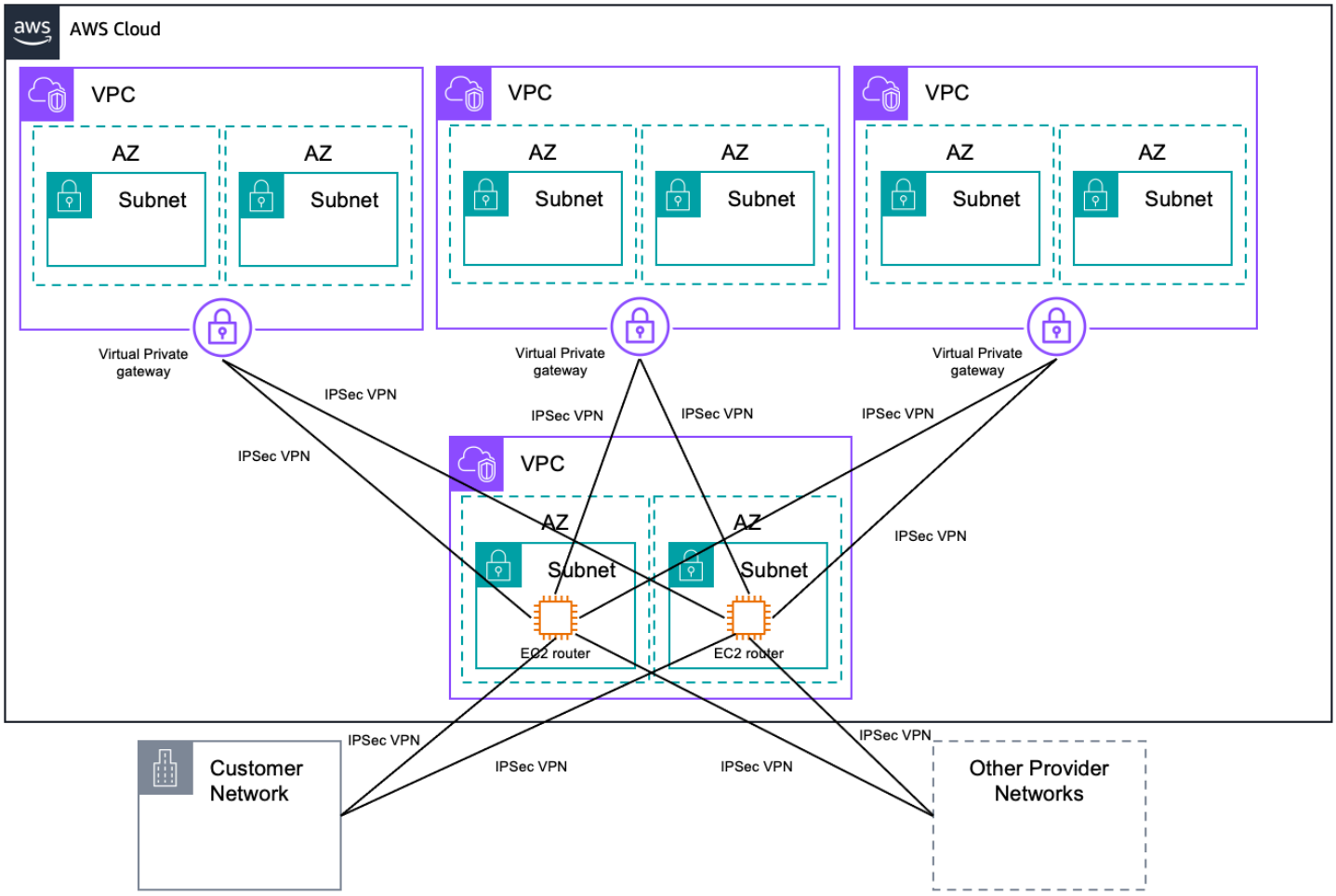
ユーザー管理、設定、パッチ、アップグレードなど、リモートアクセスソフトウェアを管理するのはお客様の責任です。この設計では、リモートアクセスサーバーが単一の Amazon EC2 インスタンスで実行されるため、ネットワーク設計に単一障害点が発生する可能性があります。詳細については、「付録 A: ソフトウェア VPN インスタンスの高レベル HA アーキテクチャ」を参照してください。

追加リソース

- から利用可能な VPN アプライアンス AWS Marketplace
- OpenVPN Access Server クイックスタートガイド

トランジット VPC

上記の Software VPN 設計に基づいて、AWS でグローバルトランジットネットワークを作成できます。トランジット VPC は、複数の地理的に分散した VPCsとリモートネットワークを接続してグローバルネットワークトランジットセンターを作成するための一般的な戦略です。中継 VPC はネットワーク管理を単純化して、複数の VPC とリモートのネットワークを接続するために必要な接続数を最小限に抑えます。次の図は、この設計を示しています。



Transit VPC

この設計により、VPCs とオンプレミスネットワーク間の直接ネットワークルーティングを提供するだけでなく、トランジット VPC は重複するネットワーク範囲間のネットワークアドレス変換などのより複雑なルーティングルールを実装したり、ネットワークレベルのパケットフィルタリングや検査を追加したりできます。トランジット VPC 設計は、プライベートネットワーク、共有接続、クロスアカウント AWS の使用などの重要なユースケースをサポートするために使用できます。

追加リソース

- AWS Transit Gateway
- での SD-WAN およびルーティング用の Cisco Catalyst 8000V AWS Marketplace

AWS クラウド WAN

AWS Cloud WAN は、データセンター、ブランチ、および AWS ネットワークを統合するポリシーによって定義された、インテント駆動型のマネージド型ワイドエリアネットワーク (WAN) です。リージョン間で複数の Transit Gateway を相互接続することで独自のグローバルネットワークを作成できますが、Cloud WAN には、コアネットワークポリシーに基づいてグローバルネットワークを構築および運用するために特別に設計された組み込みの自動化、セグメンテーション、および設定管理機能が用意されています。クラウド WAN には、VPC の自動アタッチメント、統合パフォーマンスモニタリング、一元化された設定などの機能が追加されました。

コアネットワークポリシーは、セグメント、AWS リージョンルーティング、およびアタッチメントがセグメントにどのようにマッピングされるかを定義する宣言言語で記述されます。コアネットワークポリシーを使用すると、アクセスコントロールとトラフィックルーティングのインテントを記述できますが、AWS Cloud WAN はネットワーク設定の詳細を処理できます。

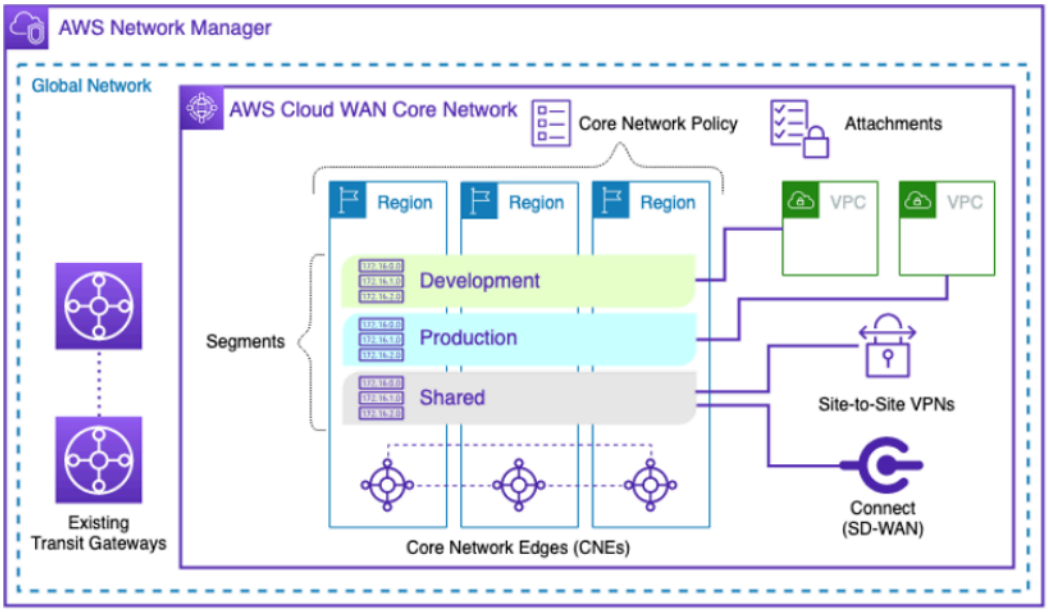
クラウド WAN は AWS Network Manager 内で管理されます。これにより、AWS アカウント、リージョン、オンプレミスロケーション間でクラウド WAN コアネットワークと Transit Gateway ネットワークを一元管理および視覚化できます。Network Manager には、グローバルネットワークのあらゆる側面を表示およびモニタリングするのに役立つダッシュボードの視覚化がいくつか用意されています。ダッシュボードには、次のようなものがあります。

- エッジロケーション、デバイス、アタッチメントなどのネットワークリソースが配置されている場所を特定するワールドマップ。
- CloudWatch Events を使用して 15 か月分の統計を追跡するモニタリングにより、ネットワークのパフォーマンスをより的確に把握できます。
- リアルタイムイベントをイベントダッシュボードにストリーミングするイベント追跡。
- トランジットゲートウェイネットワークとトランジットゲートウェイのトポロジ図と論理図。

Transit Gateway と Cloud WAN の両方により、VPCs とオンプレミスロケーション間の一元化された接続が可能になります。Transit Gateway は、リージョンのネットワーク接続ハブであり、いくつかの AWS リージョンで運用しているお客様、独自のピアリングとルーティングの設定を管理したいお客様、または独自のオートメーションを使用したいお客様に最適です。クラウド WAN は、ポリシーを通じてグローバルネットワークを定義し、基盤となるコンポーネントを自動的に実装するお客様に最適です。

主要事項

- CNE (コアネットワークエッジ) は、VPC アタッチメントあたりのスループットなど、多くの Transit Gateway 特性を継承します。
- クラウド WAN は、IPv4 と IPv6 の両方をサポートしています。
- 変更が多い大規模なネットワークの場合は、変更を検証できる個別の開発およびテストグローバルネットワークの作成を検討してください。



AWS Cloud WAN

追加リソース

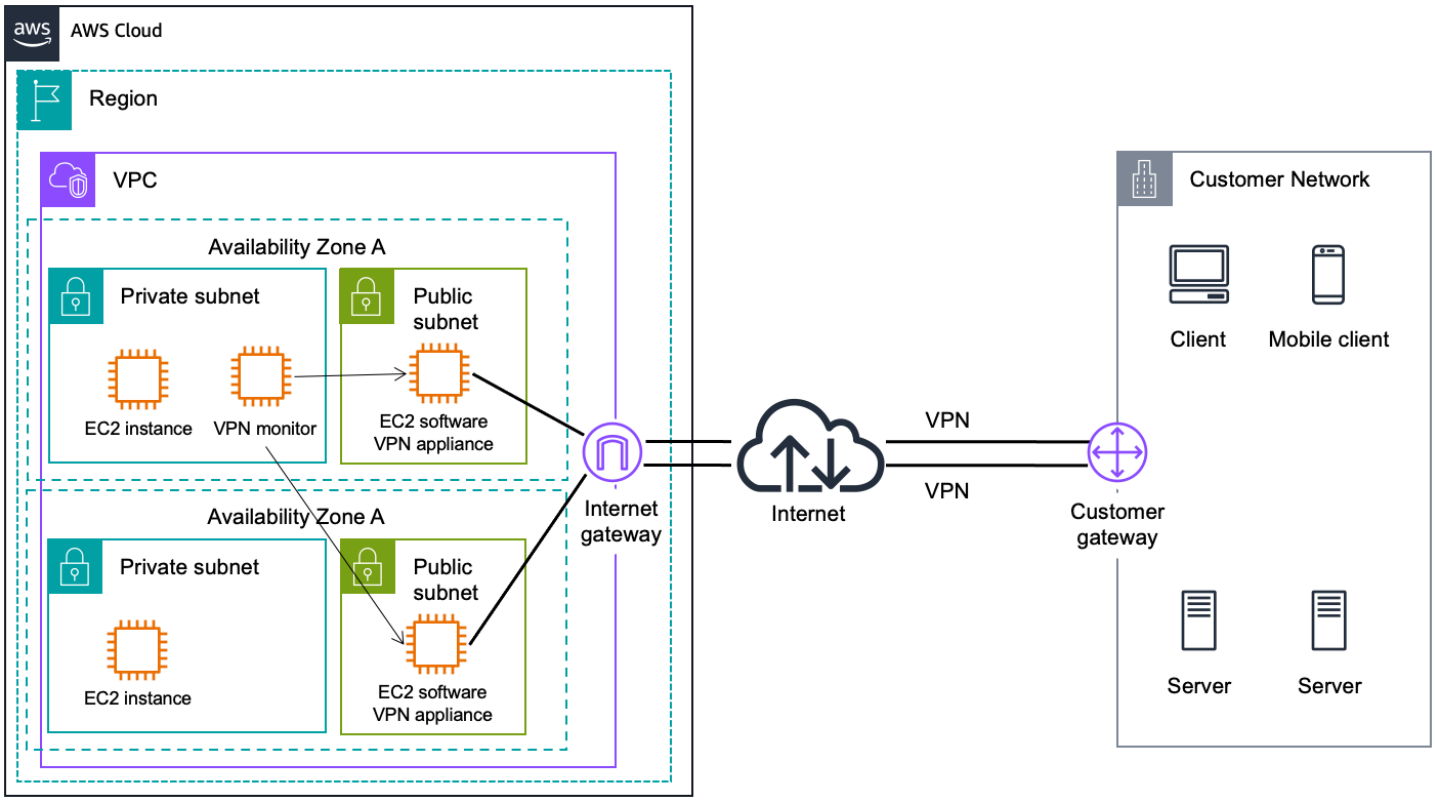
- AWS Cloud WAN ドキュメント
- ブログ記事: AWS Cloud WAN と AWS Transit Gateway の移行と相互運用性のパターン

結論

AWS には、リモートネットワークを Amazon VPC と統合する際に AWS を最大限に活用するための、効率的で安全な接続オプションが多数用意されています。このホワイトペーパーで提供されるオプションでは、リモートネットワークまたは複数の Amazon VPC ネットワークを正常に統合するためにお客様が使用した接続オプションとパターンをいくつか紹介します。ここに記載されている情報を使用して、ビジネスを運営するために必要なインフラストラクチャを接続するための最適なメカニズムを決定できます。物理的な場所やホスト場所は関係ありません。

付録 A: ソフトウェア VPN インスタンスの高レベル HA アーキテクチャ

ソフトウェア VPN インスタンス用に完全に回復力のある VPC 接続を作成するには、複数の VPN インスタンスとモニタリングインスタンスのセットアップと設定を行って、VPN 接続の状態を監視する必要があります。



高レベルソフトウェア VPN HA

1 つのアベイラビリティーゾーン内のすべてのサブネットからのトラフィックを同じアベイラビリティーゾーン内のそれぞれの VPN インスタンス経由でルーティングすることで、すべての VPN インスタンスを同時に活用するように VPC ルートテーブルを設定することをお勧めします。次に、各 VPN インスタンスは、同じアベイラビリティーゾーンを共有するインスタンスに VPN 接続を提供します。

VPN モニタリング

ソフトウェアベースの VPN アプライアンスをモニタリングするには、VPN Monitor を作成できます。VPN モニターは、VPN モニタリングスクリプトを実行するために必要なカスタムインスタンス

です。このインスタンスは、VPN 接続と VPN インスタンスの状態を実行およびモニタリングすることを目的としています。VPN インスタンスまたは接続がダウンした場合、モニタは両方の接続が再び機能するまで、影響を受けるサブネットから動作中の VPN インスタンスにトラフィックを再ルーティングしながら、VPN インスタンスを停止、終了、または再起動する必要があります。お客様の要件は異なるため、AWS は現在、このモニタリングインスタンスを設定するための規範的なガイダンスを提供していません。ただし、NAT インスタンス間で HA を有効にするスクリプトの例を、ソフトウェア VPN インスタンス用の HA ソリューションを作成するための出発点として使用できます。VPN 接続に障害が発生した場合に通知を提供したり、ネットワーク接続を自動的に修復したりするために必要なビジネスロジックを検討することをお勧めします。

さらに、Amazon CloudWatch メトリクスを使用して AWS Managed VPN トンネルをモニタリングできます。これにより、VPN サービスからデータポイントを読み取り可能なほぼリアルタイムのメトリクスに収集します。各 VPN 接続は、さまざまなトンネルメトリクスを収集して Amazon CloudWatch に発行します。これらのメトリクスを使用すると、トンネルの状態、アクティビティをモニタリングし、自動アクションを作成できます。

寄稿者

本ドキュメントの寄稿者は次のとおりです。

- AWS Enterprise Support、シニアテクニカルアカウントマネージャー、Daniel Yu
- AWS ソリューションアーキテクチャ、ソリューションビルダー、Garvit Singh
- AWS ソリューションアーキテクチャ、ソリューションビルダー、シニアマネージャー、Steve Morad
- AWS ソリューションアーキテクチャ、ソリューションアーキテクト、Sohaib Tahir
- AWS ソリューションアーキテクチャ、プリンシパルソリューションアーキテクト、Fiona Armada
- Pablo Sánchez Carmona、ネットワークスペシャリストソリューションアーキテクト、AWS ソリューションアーキテクチャ
- AWS Enterprise Support、シニアネットワーキングスペシャリストテクニカルアカウントマネージャー、Tony Hawke

ドキュメントの改訂

このホワイトペーパーの更新に関する通知を受け取るには、RSS フィードにサブスクライブしてください。

変更	説明	日付
ホワイトペーパーの更新	AWS Cloud WAN と Transit Gateway の接続アタッチメントオプションを追加し、図と情報を全体的に更新しました。	2023 年 4 月 5 日
ホワイトペーパーの更新	AWS Transit Gateway と AWS Client VPN オプションを追加し、図と情報を全体で更新しました。	2020 年 6 月 6 日
マイナーな更新	ソフトウェア VPN アプライアンスへの参照の修正に関する軽微な変更。	2020 年 5 月 20 日
ホワイトペーパーの更新	全体の情報を更新しました。トランジット VPC、Direct Connect ゲートウェイ、 の設計/機能に焦点を当てます AWS PrivateLink。	2018 年 1 月 1 日
初版発行	Amazon Virtual Private Cloud Connectivity Options が公開されました。	2014 年 7 月 1 日

注意

お客様は、本書に記載されている情報を独自に評価する責任を負うものとします。本書は、(a) 情報提供のみを目的とし、(b) AWS の現行製品と慣行について説明しており、これらは予告なしに変更されることがあり、(c) AWS およびその関連会社、サプライヤー、またはライセンサーからの契約上の義務や保証をもたらすものではありません。AWS の製品やサービスは、明示または黙示を問わず、一切の保証、表明、条件なしに「現状のまま」提供されます。お客様に対する AWS の責任は AWS 契約によって規定されています。また、本文書は、AWS とお客様との間の契約に属するものではなく、また、当該契約が本文書によって修正されることもありません。

© 2020 Amazon Web Services, Inc. またはその関連会社。All rights reserved.

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。