AWS ホワイトペーパー

Amazon Virtual Private Cloud Connectivity Options

Amazon Virtual Private Cloud Connectivity Options: AWS ホワイトペーパー

Table of Contents

Amazon Virtual Private Cloud Connectivity Options

発行日: 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できます。このセクションでは、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オプションがいくつか用意されています。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、企業のネットワークアーキテクト、エンジニア、または利用可能な接続オプションを確認したい 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接続のいずれか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 サービスまたはユーザーが管理するネットワーク機器とルートを利用して、Amazon VPC とネットワーク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、概要とそれぞれの大まかな比較を含む以下のオプションについて説明します。

- ネットワークから 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 へのプライベートな論理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な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および 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 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 モデルの構築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 - AWSバック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広域ネットワーク (SD-WAN) ソリューションの統合について説明します。

- Amazon VPC から Amazon VPC への接続オプション
  - VPC ピアリング — Amazon VPCs ピア機能を使用して、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 — 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 hub-and-spoke。
  - 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の接続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 から AWS Site-to-Site VPN – 1 つの Amazon VPCs 内のユーザー管理のソフトウェア 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 接続で Amazon VPC を接続する方法について説明します。
- Amazon VPC への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 Client VPN を利用して、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、管理、監視するためのマネージド広域ネットワーク (WAN) の確立について説明します。

ネットワークから 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) と統合する場合に役立ちます。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することもできます。

リモートカスタマーネットワークへの VPC 接続は、接続されてい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。例えば、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ます。重複しない 1 つの連続した CIDR ブロックを各 VPC で使用するように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 のよくある質問」を参照してください。

オプション	ユースケース	利点	制限事項
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の再利用 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の実装はお客様の責任となります (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 を利用する場合)

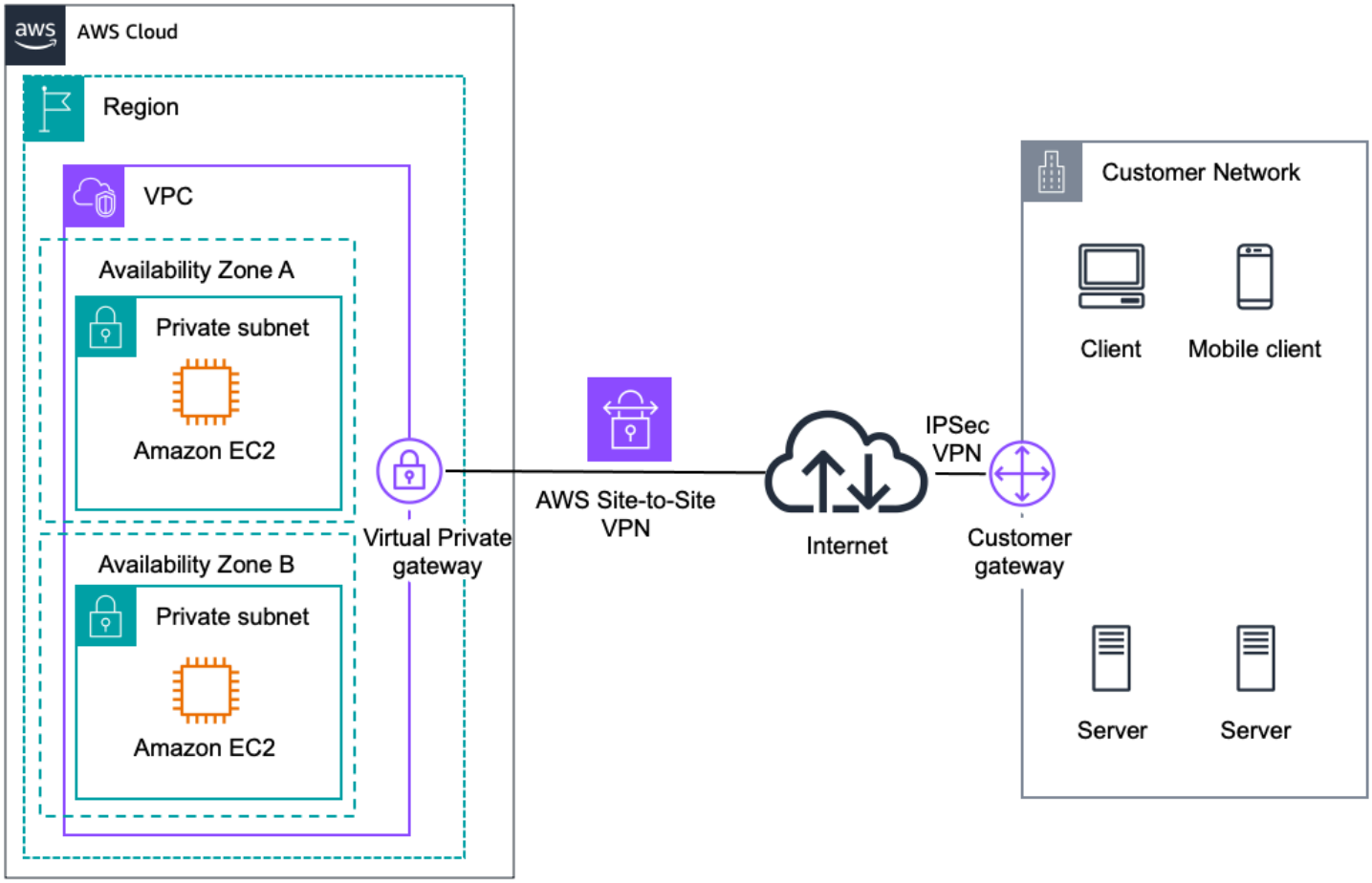
オプション	ユースケース	利点	制限事項
AWS Transit Gateway + AWS Site-to-Site VPN	複数の VPCs のリージョン別ルーターへのインターネット経由の AWS マネージド IPsec VPN 接続	前のオプションと同じ 最大 5,000 個のアタッチメント用の AWS マネージドの高可用性とスケーラビリティのリージョンネットワークハブ	前のオプションと同じ
AWS Direct Connect	プライベートライン経由の専用ネットワーク接続	より予測可能なネットワークパフォーマンス 帯域幅コストの削減 BGP ピアリングおよびルーティングポリシーをサポート	追加のテレコムとホスティングプロバイダーの関係や、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 マネージドの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	制限事項
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 での BGP ピアリングおよびルーティングポリシーのサポート 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	追加のテレコムとホスティングプロバイダーの関係、または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の実装はお客様の責任となります (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 を利用する場合)
AWS Direct Connect + AWS Transit Gateway + AWS Site-to-Site VPN	複数の VPCs のリージョン別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 マネージドの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	制限事項
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 接続の再利用 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の交換のために 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よって異なります ユーザーマネージドブランチオフィスのエンドポイントは、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	AWS バック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には、AWS ネイティブサービスとの統合があります。	Amazon VPC に配置される場合、SD-WAN アプライアンスの HA (高可用性) を実装する責任があります。
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 完全なカスタマーマネージドソリューション	すべての VPN エンドポイントに HA (高可用性) 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)

AWS Site-to-Site VPN

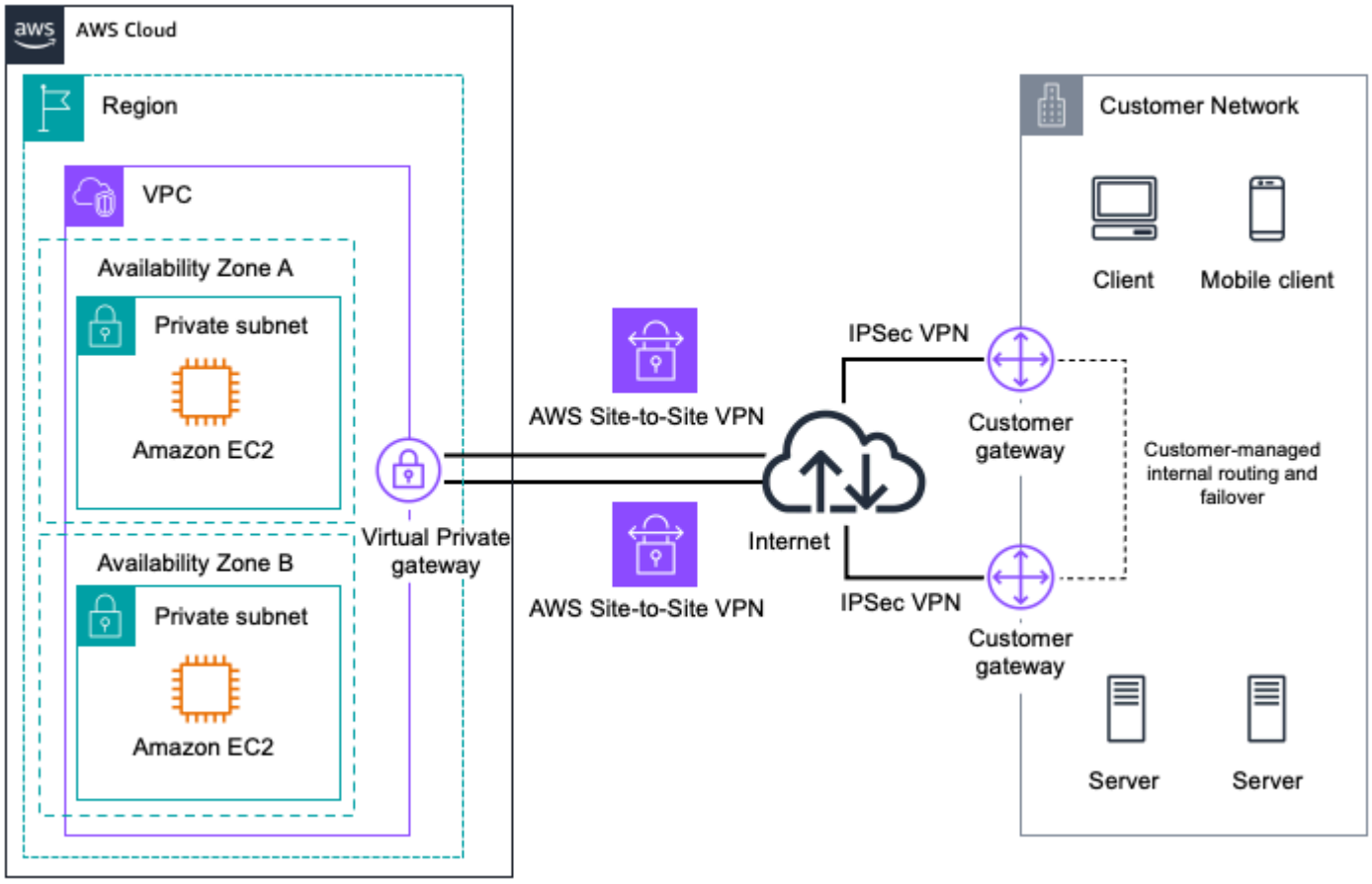
Amazon VPC には、次の図に示すように、インターネット経由でリモートネットワークと Amazon VPC の間に IPsec VPN 接続を作成するオプションがあります。



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

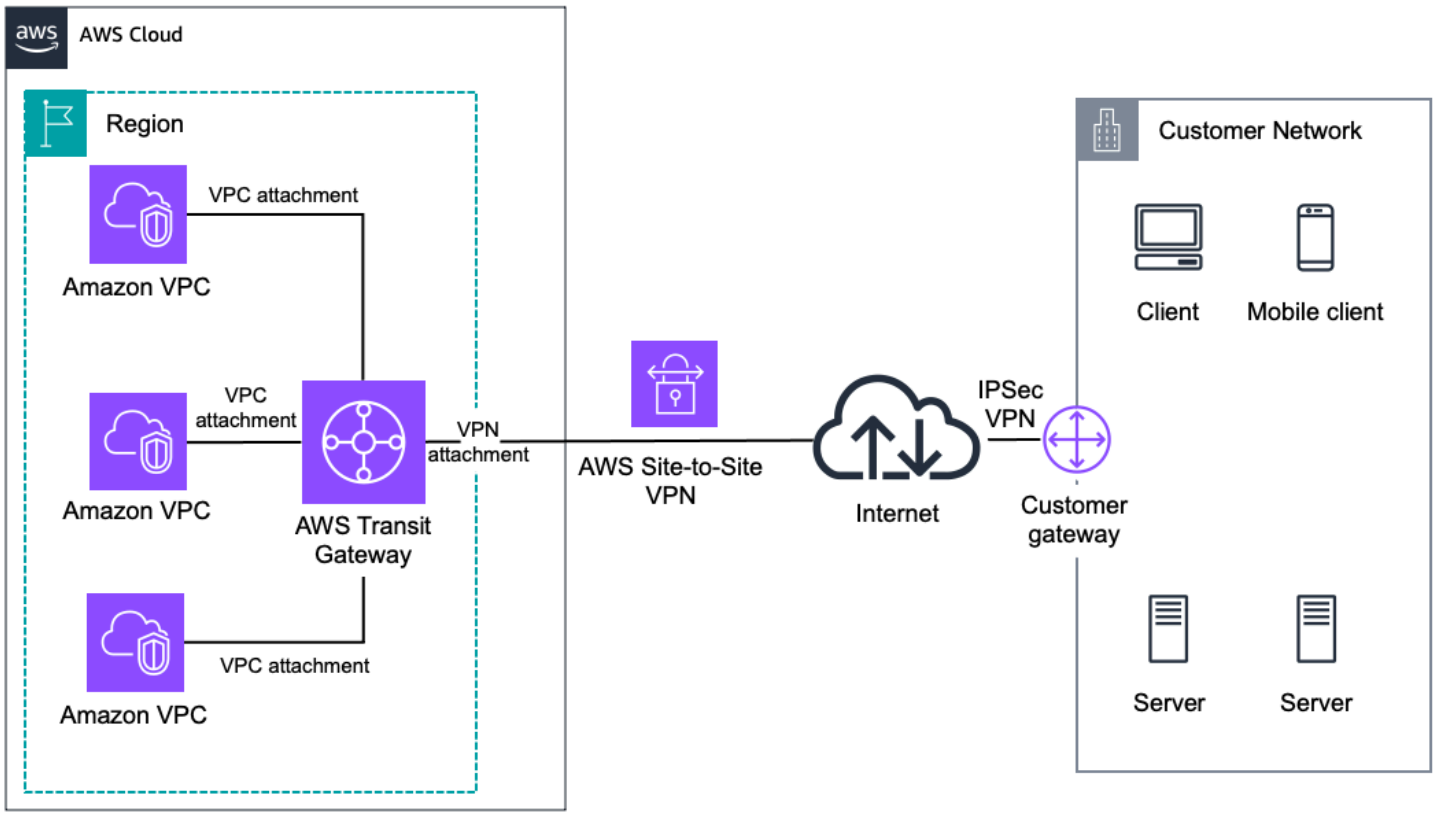
動的ルーティングオプションと静的ルーティングオプションの両方が用意されているため、ルーティング設定に柔軟性がもたらされます。動的ルーティングは BGP ピアリングを使用して、AWS とこれらのリモートエンドポイント間でルーティング情報を交換します。動的ルーティングでは、BGP アドバタイズでルーティングの優先順位、ポリシー、重み (メトリクス) を指定し、ネットワークと AWS 間のネットワークパスに影響を与えることもできます。BGP を使用する場合、IPsec セッションと BGP セッションの両方を同じユーザーゲートウェイデバイスで終了する必要があるため、IPsec セッションと BGP 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

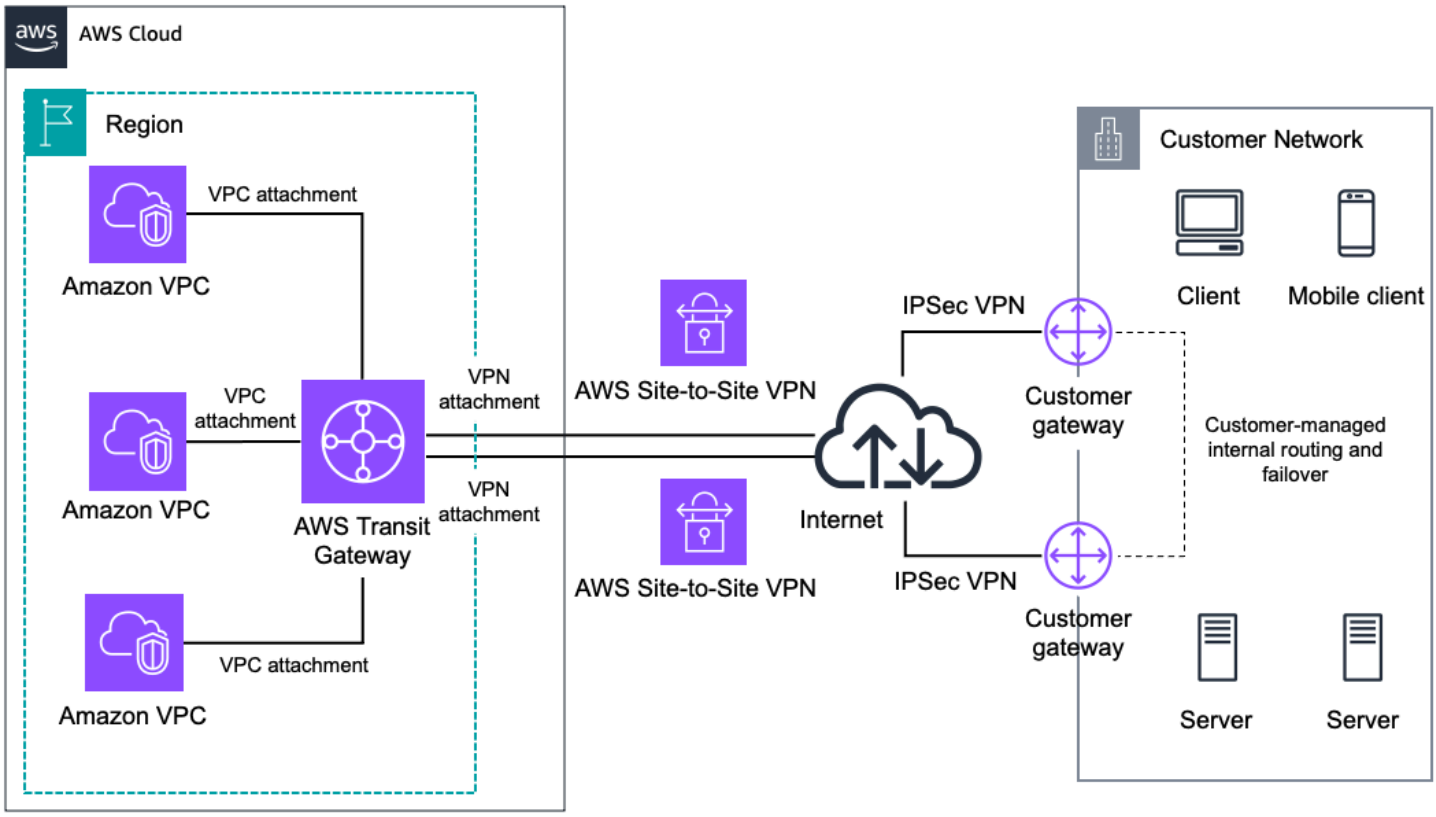
AWS Transit Gateway は、VPC とカスタマーネットワークを相互接続するために使用される AWS マネージドの高可用性とスケーラビリティを備えたリージョンネットワークの中継ハブVPCs。AWS Transit Gateway + VPN は、Transit Gateway VPN アタッチメント を使用して、次の図に示すように、インターネット経由でリモートネットワークと Transit Gateway の間に IPsec VPN 接続を作成するオプションを提供します。



AWS Transit Gateway and AWS Site-to-Site VPN

このアプローチは、複数の Amazon VPCs への複数の IPsec VPN 接続の追加コストや管理を必要とせずに、同じリージョン内の複数の 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。



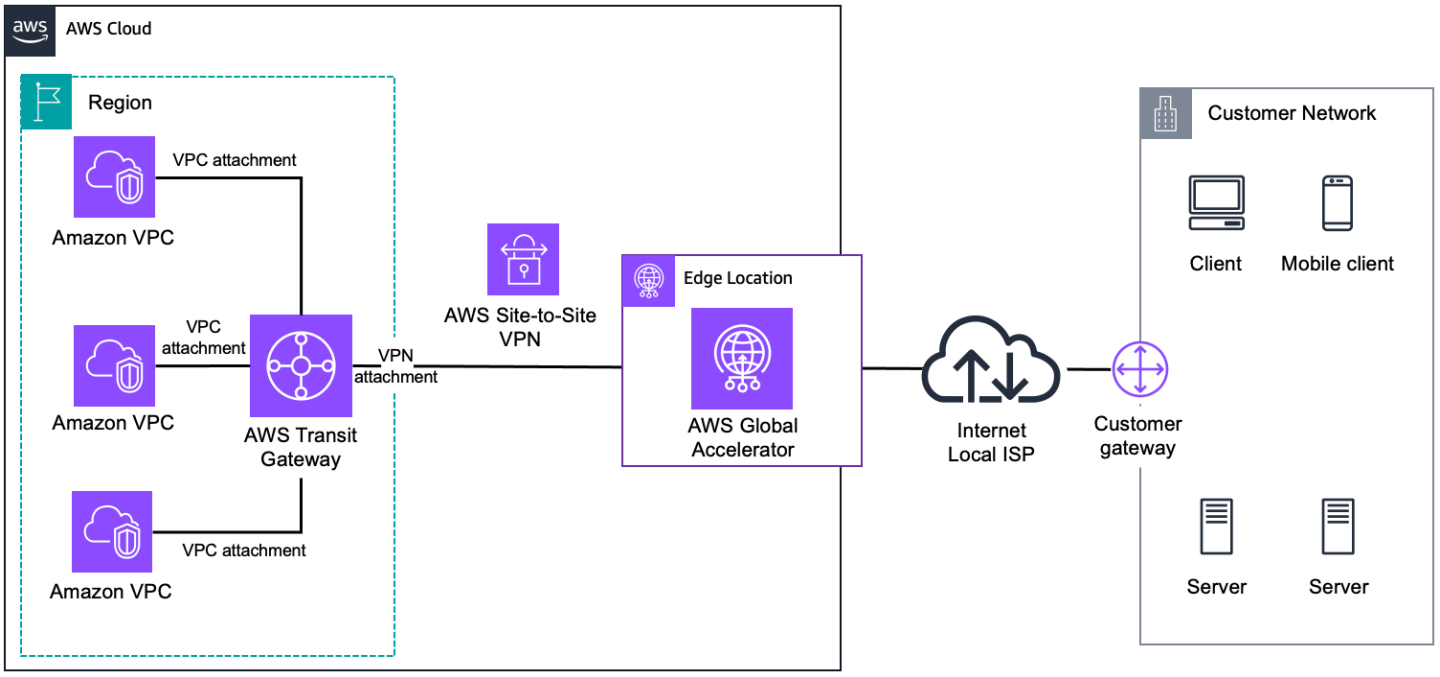
AWS Transit Gateway and Redundant VPN

Transit Gateway VPN IPsec アタッチメントのルーティング設定を柔軟に行えるように、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 1 秒あたり 140,000 パケットを実現できます。Transit Gateway で VPN 接続を終了する場合、等価コストマルチパス (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 VPN 帯域幅を高めることができます。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 接続でアクセラレーション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。アクセラレーションは、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 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 トラフィック用に異なる VPN トンネルを作成する必要があります。

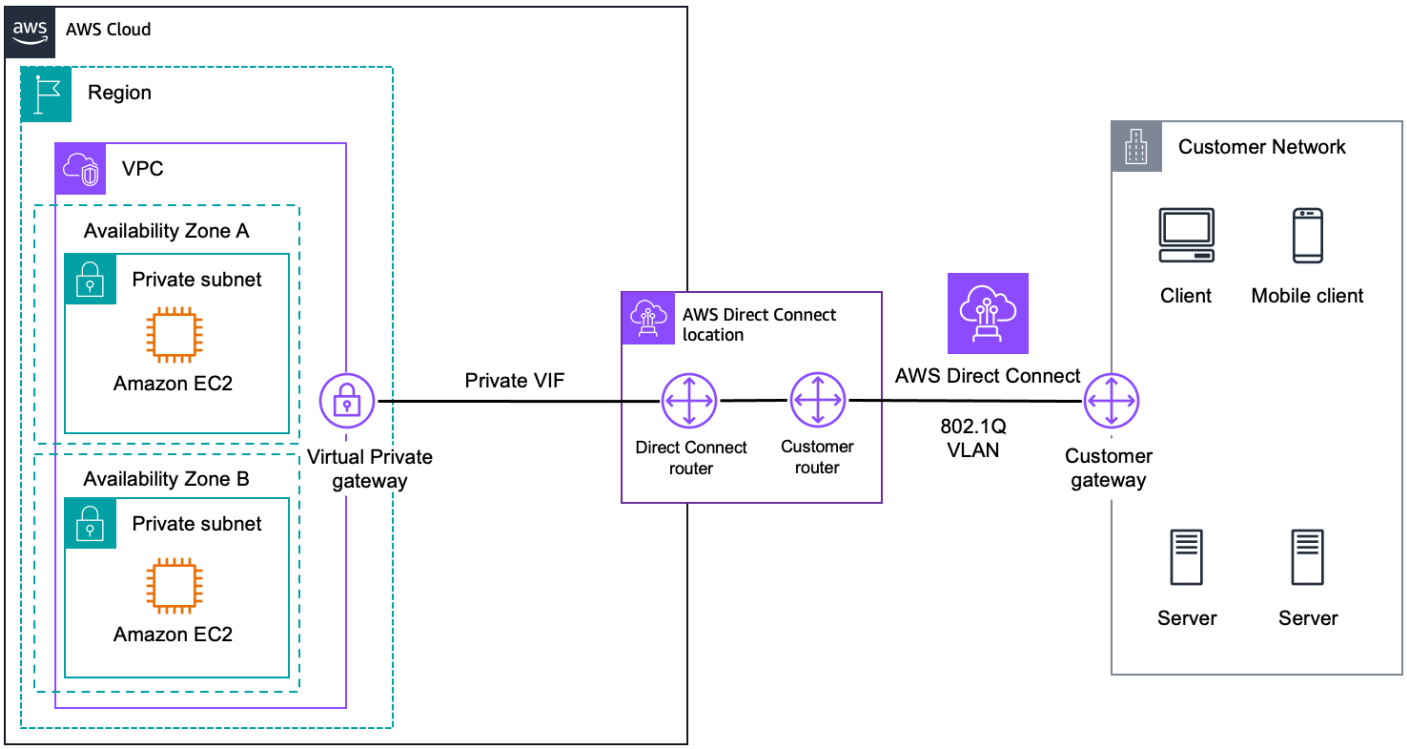
追加リソース

- 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 VPCs への専用接続を簡単に確立 AWS Direct Connect できます。 は、インターネットベースの接続よりも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、より一貫したネットワークエクスペリエンスを提供します。業界標準の 802.1Q VLANs、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、次の 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、または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との間に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

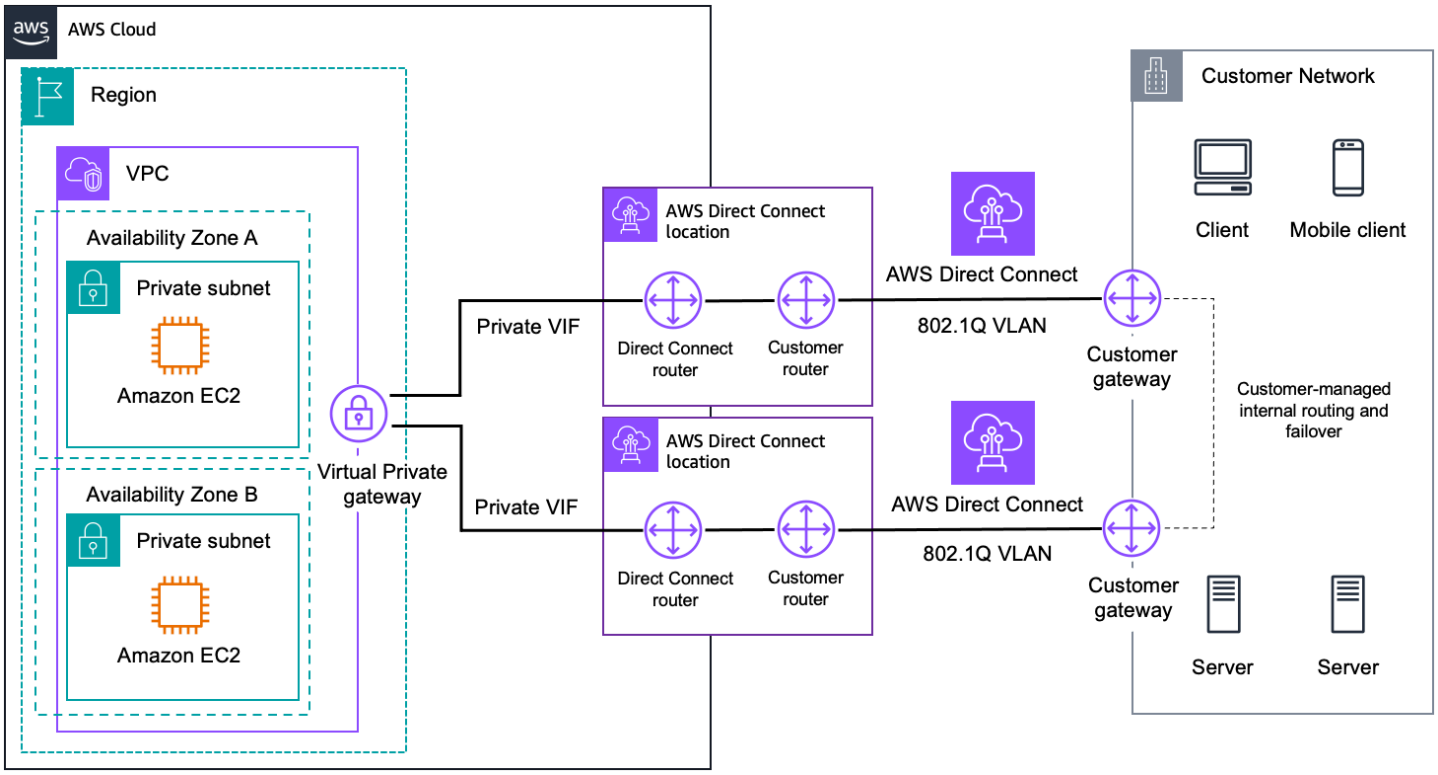
Direct Connect ロケーション 内の AWS デバイスへのクロス接続を確立 AWS Direct Connect することで、 を使用して AWS バックボーンへの接続を確立できます。Direct Connect ロケーション (中国を除く) から任意の AWS リージョンにアクセスできます。ロケーションに機器がない場合は、WAN サービスプロバイダーのエコシステムから選択して、 AWS Direct Connect ロケーションのエンドポイントを AWS Direct Connect リモートネットワークと統合できます。

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

- 専用接続 。物理的なイーサネット接続は 1 人の顧客に関連付けられます。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には、 AWS Direct Connect パートナープログラムのパートナーとの連携が必要になる場合があります。
- ホスト接続 。物理的な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、ユーザーと共有されます。50 Mbps ~ 10 Gbps のポート速度を注文できます。は、確立された AWS Direct Connect 接続と、 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間のネットワーク回線の両方で パートナーと連携します。

専用接続の場合、Link Aggregation Group (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。これらは単一のマネージド接続として扱います。1 または 10-Gbps の接続は最大 4 つ、100-Gbpsの接続は最大 2 つまで集約できます。

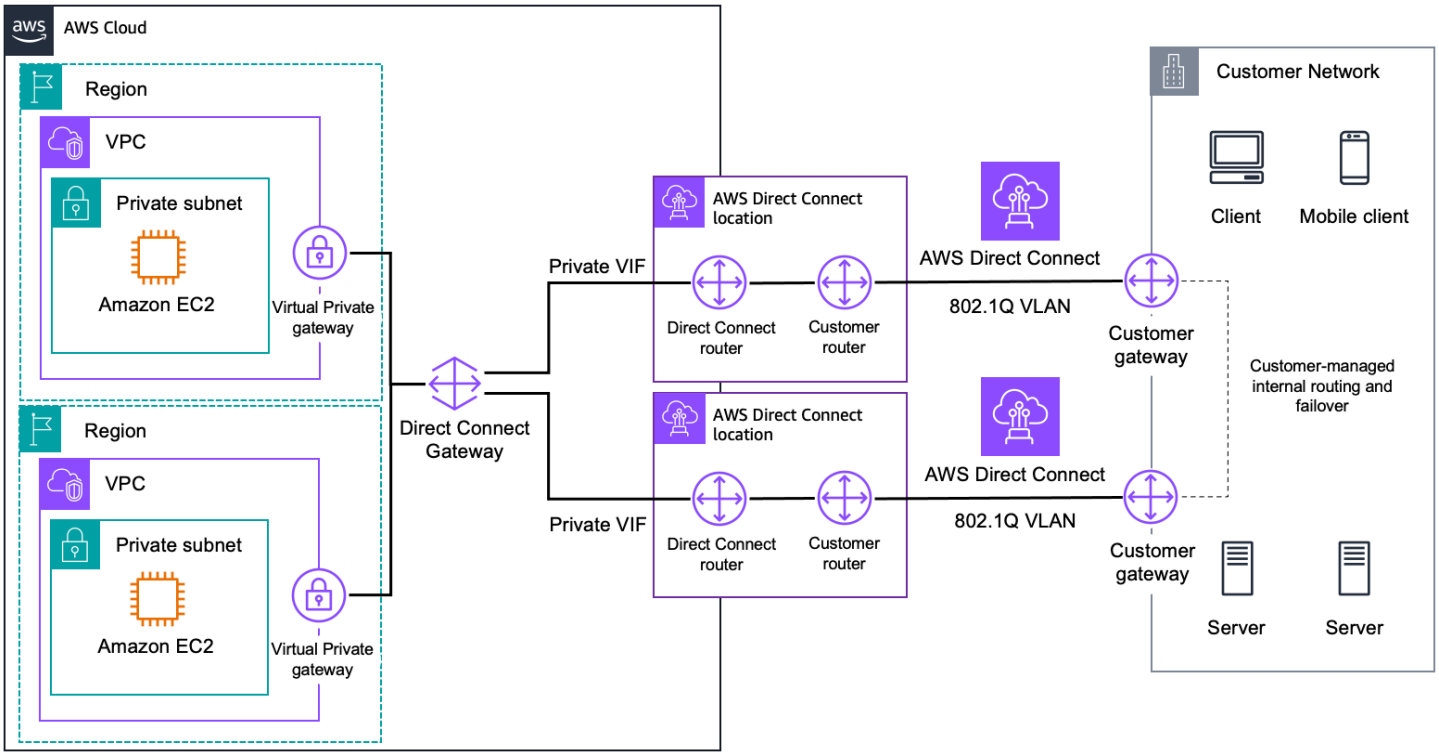
で高可用性について議論する場合は AWS Direct Connect、追加の AWS Direct Connect 接続を使用することをお勧めします。AWS Direct Connect Resiliency Toolkit は、 AWS とデータセンター、オフィス、またはコロケーション環境との間に回復性の高いネットワーク接続を構築する際のガイダンスを提供します。次の図は、2 つの異なる AWS Direct Connect 場所で 2 つの接続が終了する、耐障害性が高い AWS Direct Connect 接続オプションの例を示しています。



冗長 AWS Direct Connect

AWS Direct Connect デフォルトでは、 は暗号化されません。10 または 100 Gbps の専用接続の場合、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、グローバルに利用可能なリソースで、異なるリージョンまたは AWS アカウントで複数の Amazon VPCs または Transit Gateway への接続を可能にします。このリソースでは、次の図に示すように、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 Transit Gateway に接続することもできます。これにより、管理が減少します AWS Direct Connect 。



AWS Direct Connect Gateway

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で IPv4 セッションと IPv6 BGP セッションの両方をサポートします。

- 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、所有してい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) 。
- すべてのタイプの VIFs IPv6 BGP ピアリングでは、AWS は /125 CIDR を割り当てます。これは設定できません。

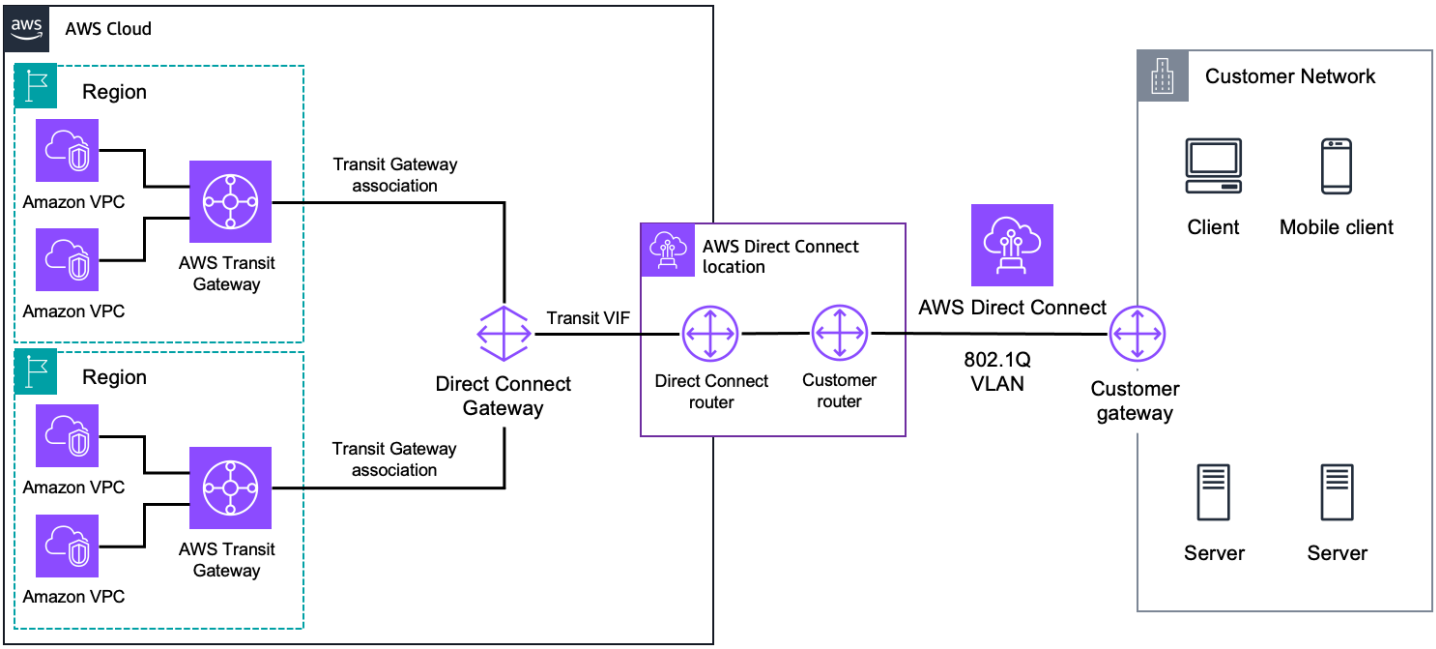
追加リソース

- 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 Resiliency Toolkit
- AWS Direct Connect MAC セキュリティ
- AWS Direct Connect ロケーション

- AWS Direct Connect デリバリーパートナー

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、ネットワークが複数のリージョン集中型ルーターをプライベート専用接続経由で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

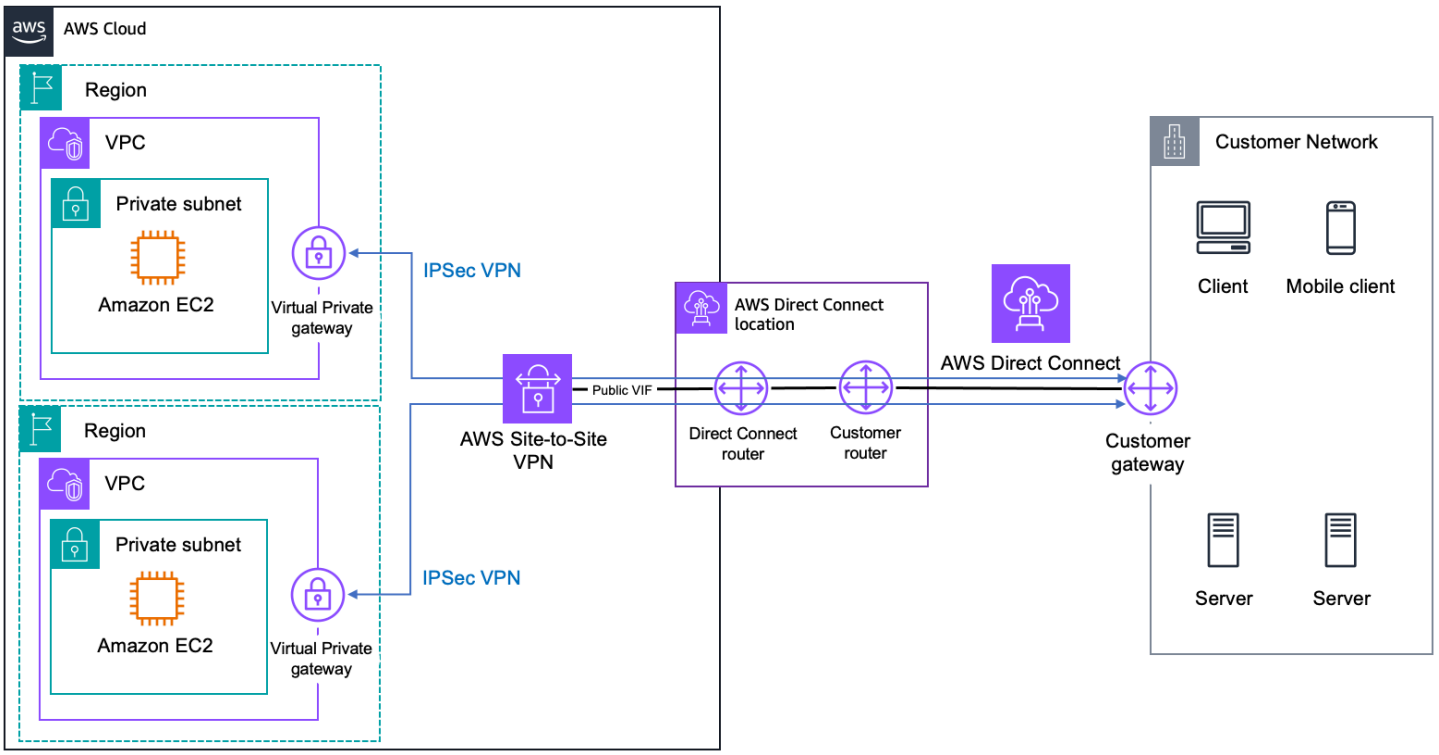
各 AWS Transit Gateway は、同じリージョン内の VPCs に相互接続するネットワーク中継ハブで、Amazon VPC ルーティング設定を 1 か所に統合します。このソリューションにより、プライベート接続を介した Amazon VPC とネットワーク間の接続の管理が簡素化され、インターネットベースの接続よりも一貫したネットワークエクスペリエンスを実現できます。

追加リソース

- AWS Direct Connect ユーザーガイド
- の集約グループをリンクする AWS Direct Connect
- ブログ記事: 1 Gbps 未満のホスト接続と 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 マネージド VPN ソリューションと AWS Direct Connect 接続を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 リソースとの間に専用の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 安全な IPsec 接続の利点を低レイテンシーで帯域幅を増や AWS Direct Connect し、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実現します。BGP 接続セッションは、パブリック VIF 上の 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、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で確立されます。

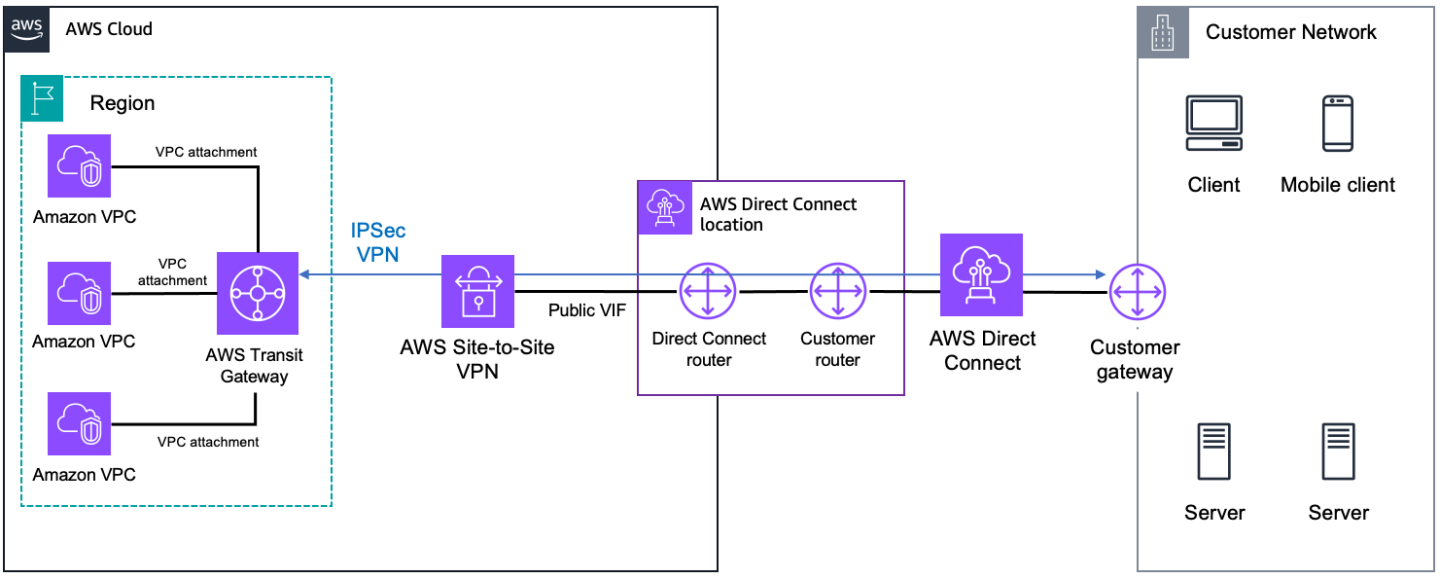
追加リソース

- 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

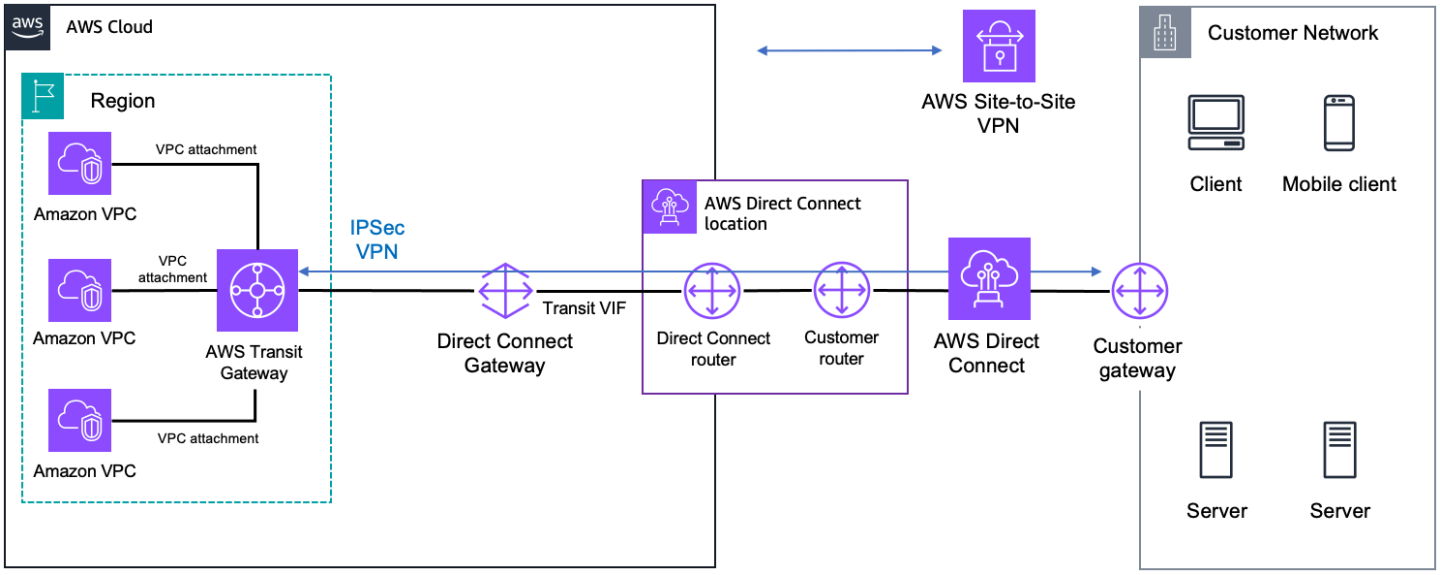
AWS Direct Connect + AWS Transit Gateway + AWS Site-to-Site VPN

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 のリージョン集中型ルーター間の end-to-end 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、同じリージョン内の複数の Amazon VPCs への IPsec VPN 接続の管理を簡素化してコストを最小限に抑える場合に検討することを検討してください。これにより、インターネットベースの VPN を介したプライベート専用接続のレイテンシーが低く、一貫したネットワークエクスペリエンスを実現できます。BGP セッションは、パブリック VIF 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との間で確立されます。

追加リソース

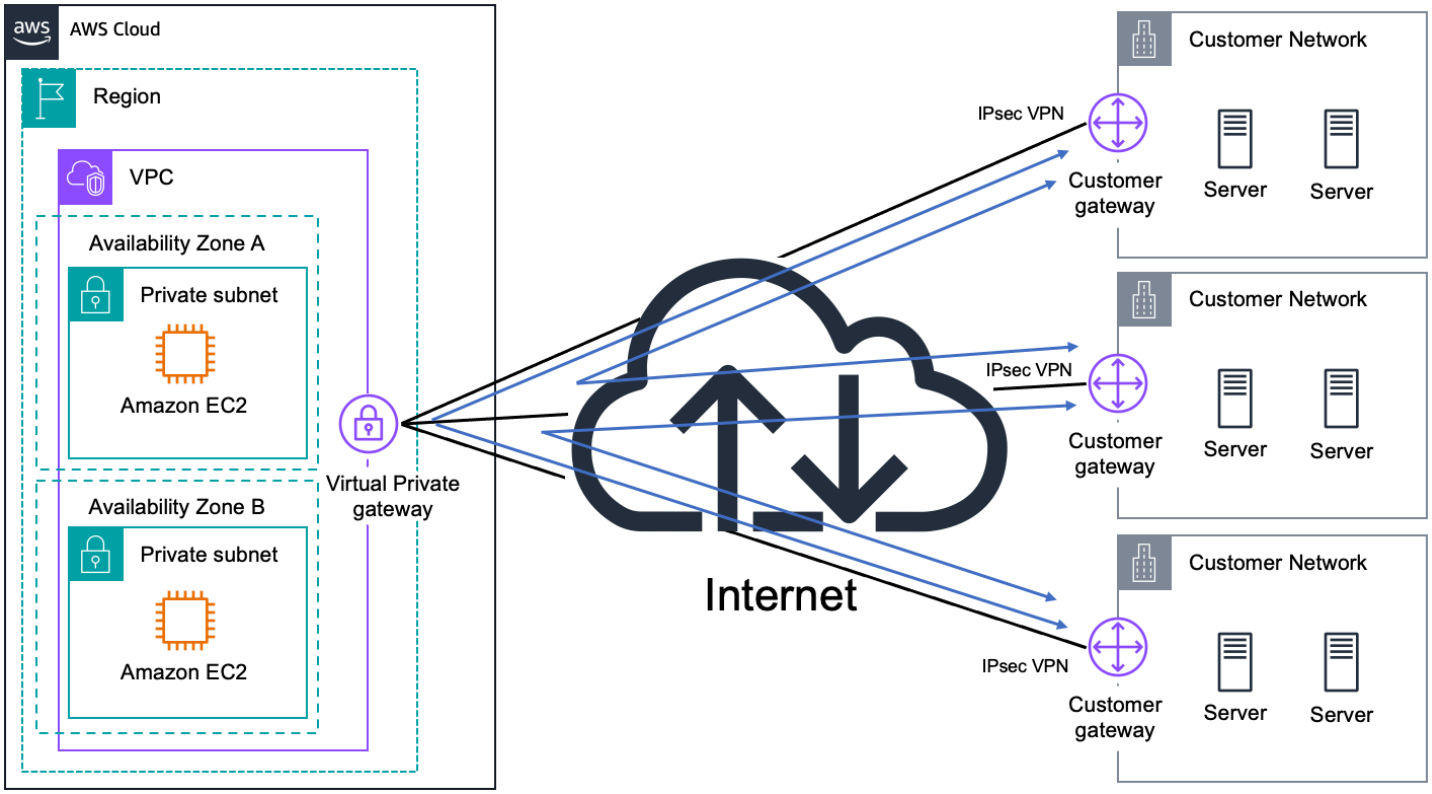
- AWS Direct Connect 仮想インターフェイス
- トランジットゲートウェイ VPN アタッチメント
- カスタマーゲートウェイデバイスの要件
- Amazon VPC でテストされたカスタマーゲートウェイデバイス
- AWS Site-to-Site VPN — とのプライベート IP VPN AWS Direct Connect

AWS VPN CloudHub

前述の AWS マネージド VPN オプションに基づいて構築すると、 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単純な hub-and-spoke モデルで AWS VPN CloudHub 動作します。このアプローチは、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コストが低い可能性のある hub-and-spoke モデルを実装する場合に使用します。

次の図は、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を含む AWS VPN CloudHub アーキテクチャを示しています。



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、それぞれが一意の BGP 自律システム番号 (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広告は、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、各 BGP ピアに対して受信および再アドバタイズされます。

追加リソース

- VPN を使用して安全なサイト間通信を提供する CloudHub
- 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

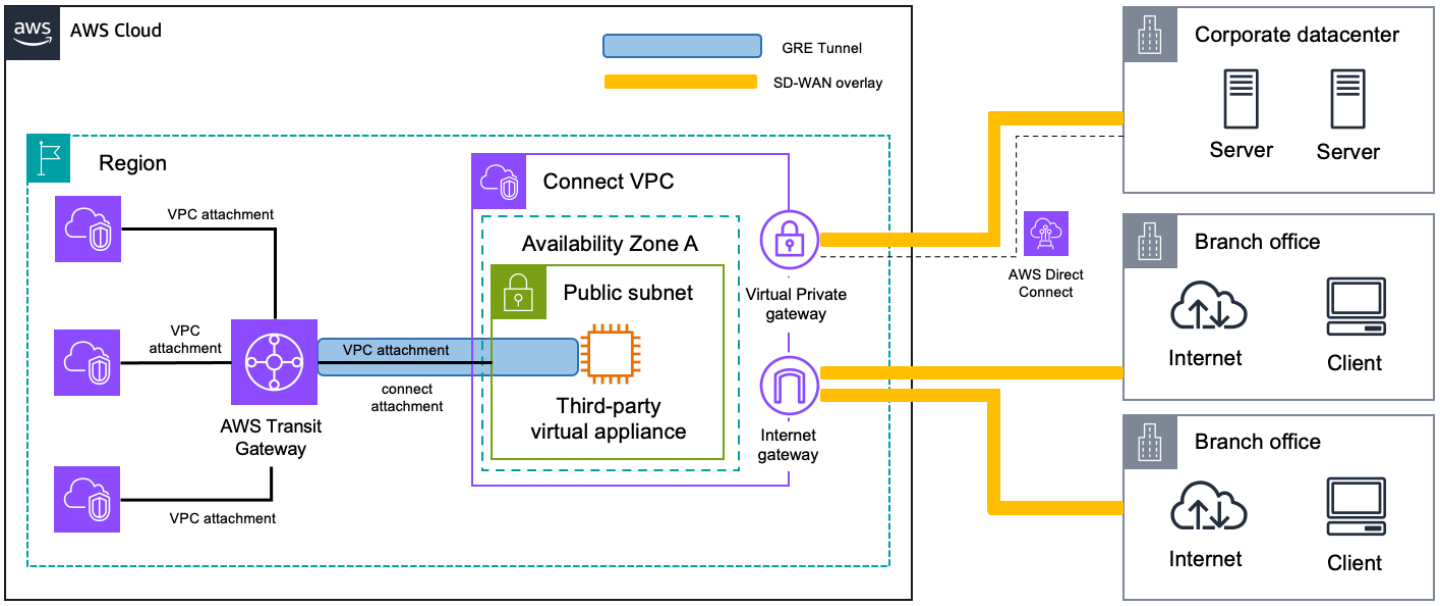
Software Defined Wide Area Networks (SD-WANsは、データセンター、オフィス、またはコロケーション環境をさまざまなトランジットネットワーク (を使用するパブリックインターネット、TAKネットワーク、AWS バックボーンなど AWS Direct Connect) に接続し、ネットワーク条件、アプリケーションタイプ、サービス品質 (QoS) 要件に基づいて、最も適切で効率的なパス全体でトラフィックを自動的かつ動的に管理するために使用します。

このアプローチは、自分と AWS の間で通信する必要がある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ある複雑なネットワークトポロジー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 ネットワークから AWS への接続について言及する場合、 は、VPC と SD-WAN ネットワークを相互接続するための、可用性が高くスケーラブルVPCsマネージドリージョンネットワーク中継ハブ 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 をセットアップしなくても、SD-WAN を AWS に簡単に拡張できます。

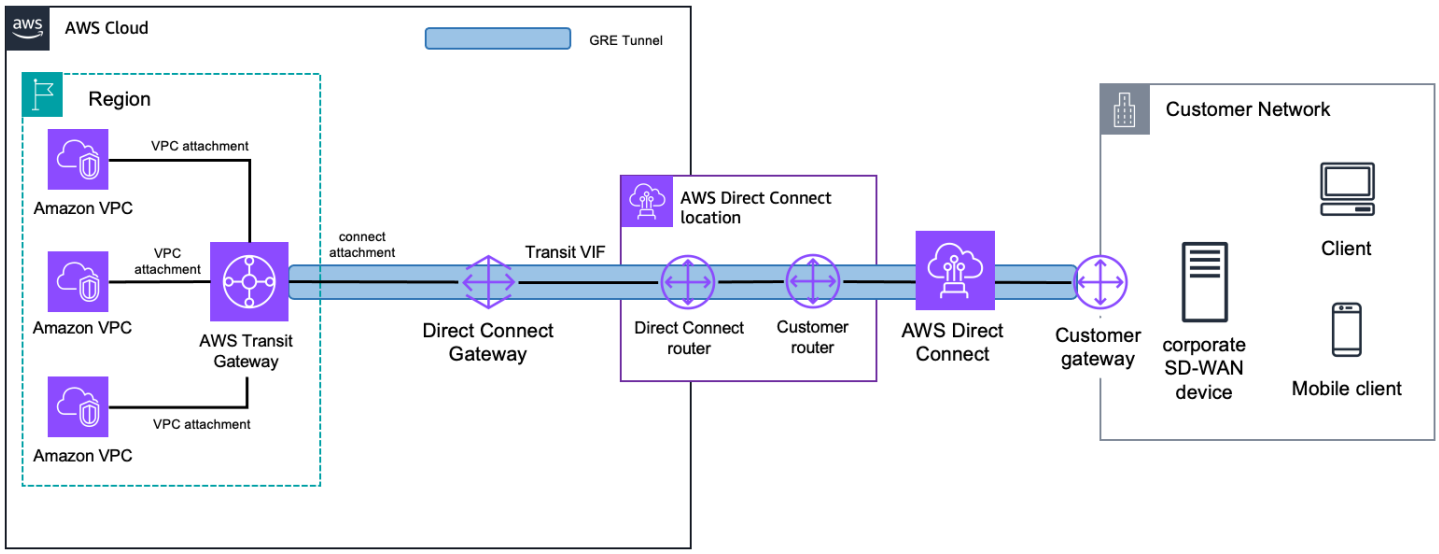
Transit Gateway 接続アタッチメントは、VPN 接続よりも高い帯域幅パフォーマンスを実現する汎用ルーティングカプセル化 (GRE) をサポートしています。動的ルーティングのボーダーゲートウェイプロトコル (BGP) をサポートし、静的ルートを設定する必要がなくなります。これにより、ネットワーク設計が簡素化され、関連する運用コストが削減されます。さらに、Transit Gateway Network Manager との統合により、グローバルネットワークトポロジ、アタッチメントレベルのパフォーマンスメトリクス、テレメトリデータを通じて高度な可視性が得られます。

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、インフラストラクチャを追加せずに SD-WAN トラフィックを AWS に拡張および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 Connect 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 Connect アタッチメントを使用する際には、注意すべき点がいくつかあります。

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

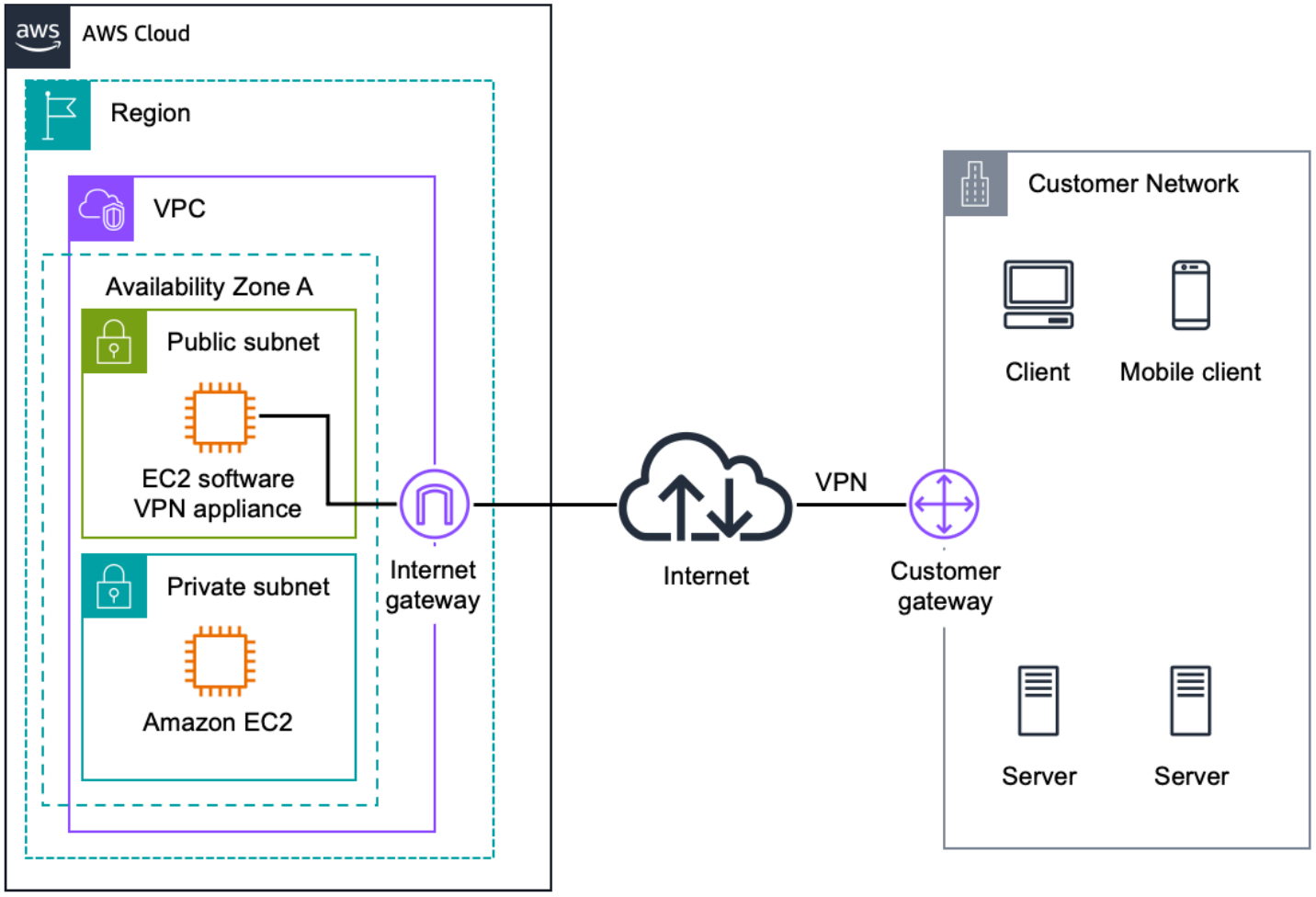
- 接続アタッチメントを使用して Transit Gateway からトラフィックを送受信するには、サードパーティーアプライアンスを GRE トンネルで設定する必要があります。動的ルート更新とヘルスチェックのために、アプライアンスを BGP で設定する必要があります。
- Connect アタッチメントは静的ルートをサポートしていません。
- Transit Gateway 接続アタッチメントは、GRE トンネルあたり 5 Gbps の最大帯域幅をサポートします。5 Gbps を超える帯域幅は、同じ Connect アタッチメントに対して複数の Connect ピア (GRE トンネル) に同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ます。
- Transit Gateway 接続アタッチメントは、マルチプロトコル拡張による BGP (MBGP または MP-BGP) 経由の 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: Simplify SD-WAN connection with AWS Transit Gateway Connect

ソフトウェア VPN

Amazon VPC 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を提供します。このオプションは、コンプライアンス上の目的、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 アプライアンスを生成した複数のパートナーや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。

ソフトウェア VPN アプライアンスは単一の Amazon EC2 インスタンスで実行されるため、この設計ではネットワーク設計に単一障害点が生じ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

- で使用可能な VPN アプライアンス AWS Marketplace
- テクニカルブリッジ - Cisco ASA を VPC EC2 インスタンスに接続する (IPsec)
- テクニカルブリッジ - 複数の VPCs EC2 インスタンスに接続する (IPsec)

- テクニカルブリッジ - 複数の VPCsを EC2 インスタンス (SSL) に接続する

Amazon VPC から Amazon VPC への接続オプション

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、セキュリティ、請求、複数のリージョンでのプレゼンス、または内部のチャージバック要件のために複数の VPCs を必要とする場合に便利です。これにより、Amazon VPCs。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および複数の 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 VPCs 接続は、接続されている各 VPC で重複しない IP 範囲を使用する場合に最適です。例えば、複数の VPCsを接続する場合は、各 VPC が一意のクラスレスドメイン間ルーティング (CIDR) 範囲で構成されていることを確認してください。そのため、重複しない 1 つの CIDR ブロックを、連続して割り当て、各 VPC で使用す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。

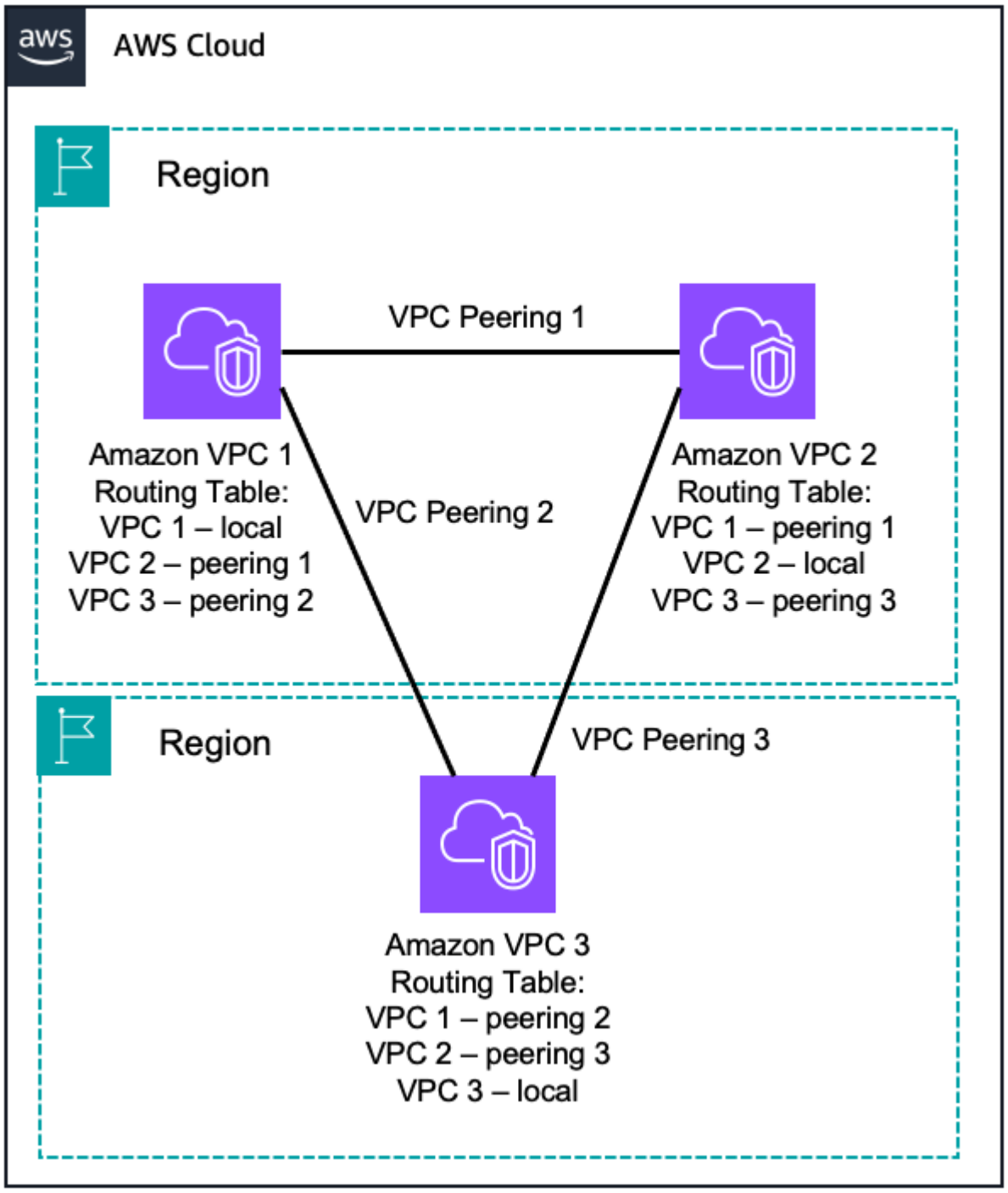
オプション	ユースケース	利点	制限事項
VPC ピアリング	2 つの VPCs 間の AWS が提供するネットワーク接続。	AWS マネージドスケーラブルネットワークインフラストラクチャを活用	VPC ピアリングは推移的なピアリング関係をサポートしていません 大規模な管理が困難
AWS Transit Gateway	VPCs 用の AWS 提供のリージョンルーター接続	AWS マネージド高可用性およびスケーラビリティサービス 最大 5,000 個のアタッチメント用のリージョンネットワークハブ	Transit Gateway ピアリングは静的ルートのみをサポートします
AWS PrivateLink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

オプション	ユースケース	利点	制限事項
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
ソフトウェア VPN から AWS Site-to-Site VPN	VPCs 間のソフトウェアアプライアンスから VPN 接続	AWS マネージド高可用性 VPC VPN 接続 さまざまな VPN ベンダーとお客様が管理する製品をサポート 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しないため、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、VPC 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 VPCs 。さらに、VPC ルーティングテーブル、セキュリティグループ、および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推移的なピアリング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リングされていない 2 つの VPC と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 の 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することもできます。

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 ピアリングを使用する場合は、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 ピア機能とは

AWS Transit Gateway

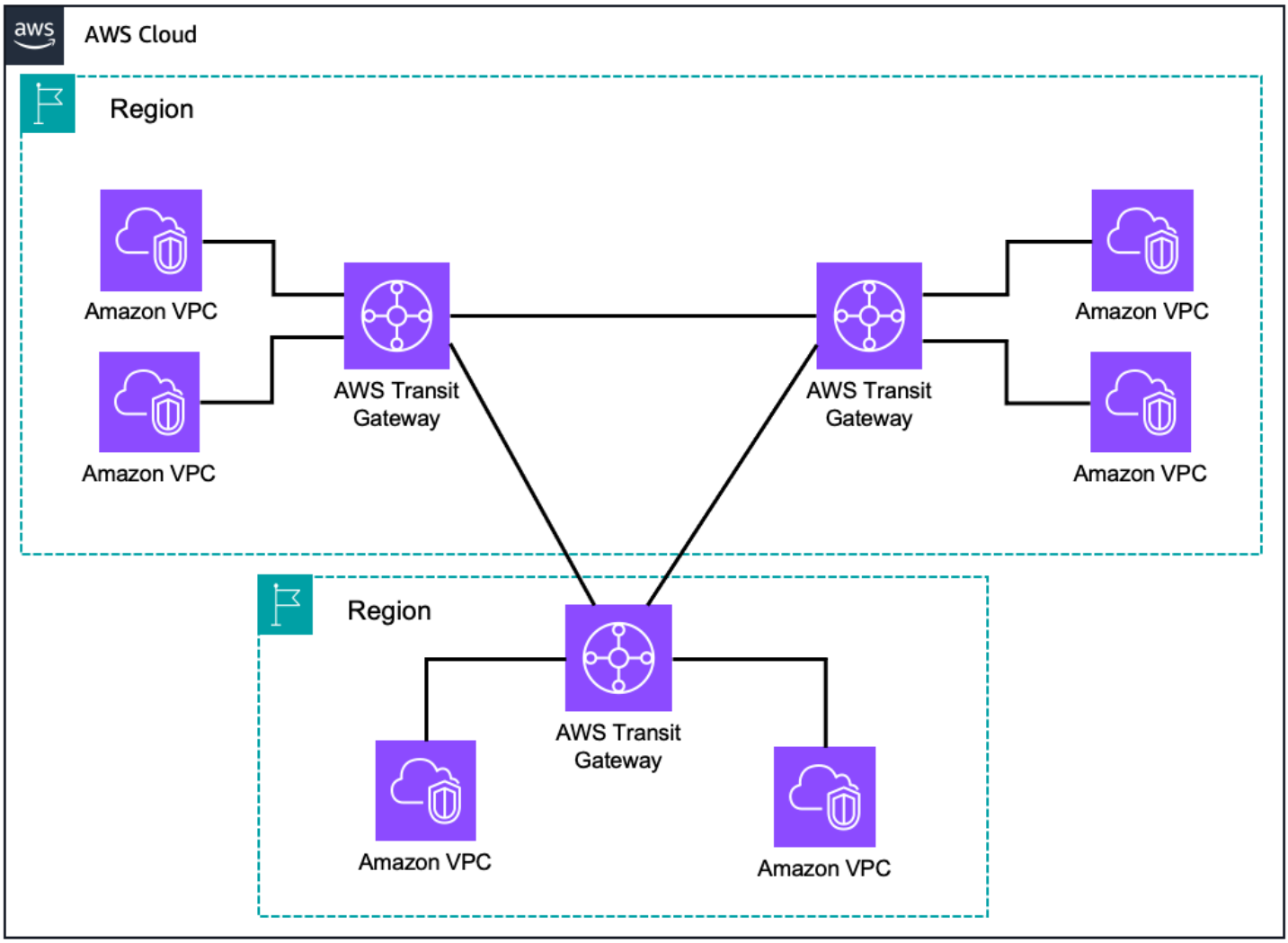
AWS Transit Gateway は、 hub-and-spoke アーキテクチャを備えたリージョンの AWS VPC ルーティング設定を統合するための、可用性が高くスケーラブルなサービスです。各スポーク VPC は、接続されている他の VPCs。では、IPv4 トラフィックと IPv6 トラフィックの両方がサポートされていますAWS Transit Gateway。

複数の Transit Gateway ルートテーブル、関連付け、伝達を利用して、同じ Transit Gateway 内でトラフィックをセグメント化できます。異なるルーティングドメイン (本番稼働用トラフィックと非本番稼働用トラフィックなど) を 1 つの管理ポイントから管理できるため、これらのルーティングドメインは相互に通信できません。

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でのこれらのリソースの管理の複雑さが軽減され、AWS のフットプリントを拡張する際の制御が向上します。

Transit Gateway 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リング接続できます。 AWS Transit Gatewayトラフィックは常にグローバル AWS バックボーンに留まり、パブリックインターネットを経由することがないため、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。

多数の VPCs、Transit Gateway は、次の図に示すように、VPC ピアリングを介した VPC 間の通信管理をよりシンプルにします。



AWS Transit Gateway

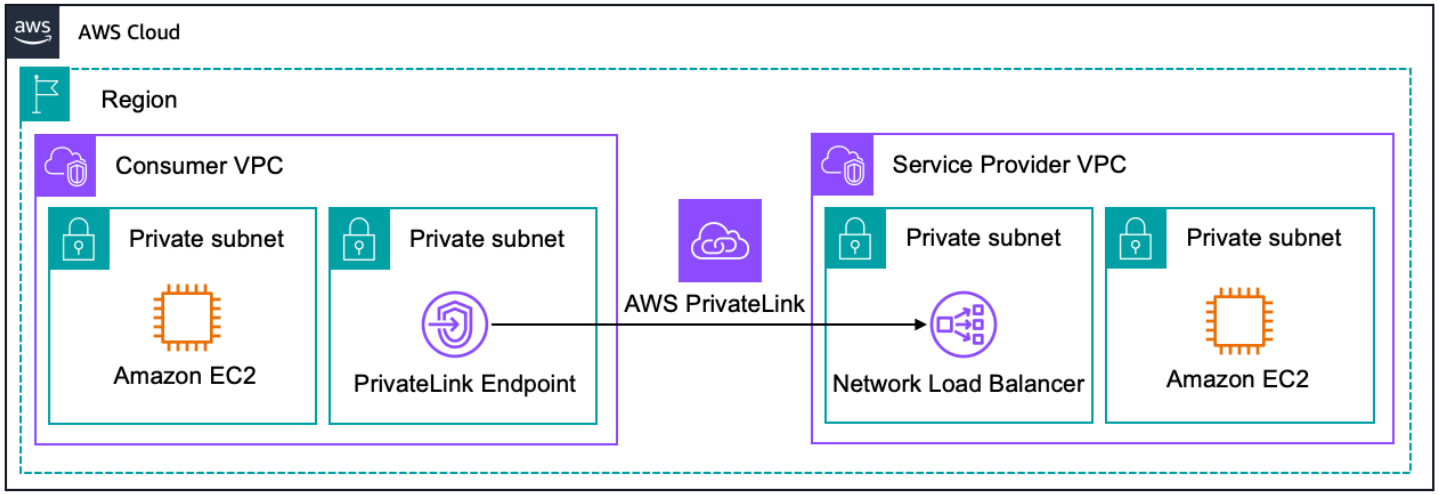
Transit Gateway との間で送受信される IP トラフィックを一元的に可視化するには、Transit Gateway Flow Logs を Amazon CloudWatch Logs と Amazon S3 に発行できます。フローログデータはネットワークトラフィックのパスの外で収集されるため、ネットワークのスループットやレイテンシーには影響しません。

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 Flow Logs 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、一部の AWS のサービス、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ます)、およびサポートされているAWS Marketplaceパートナーサービスに、VPC 内のプライベート IP アドレス経由で接続できます。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は VPCs の IP アドレスが重複している場合に適しています。

AWS PrivateLink は IPv6 を完全にサポートしますが、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、および DNS 名の両方を有効または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。

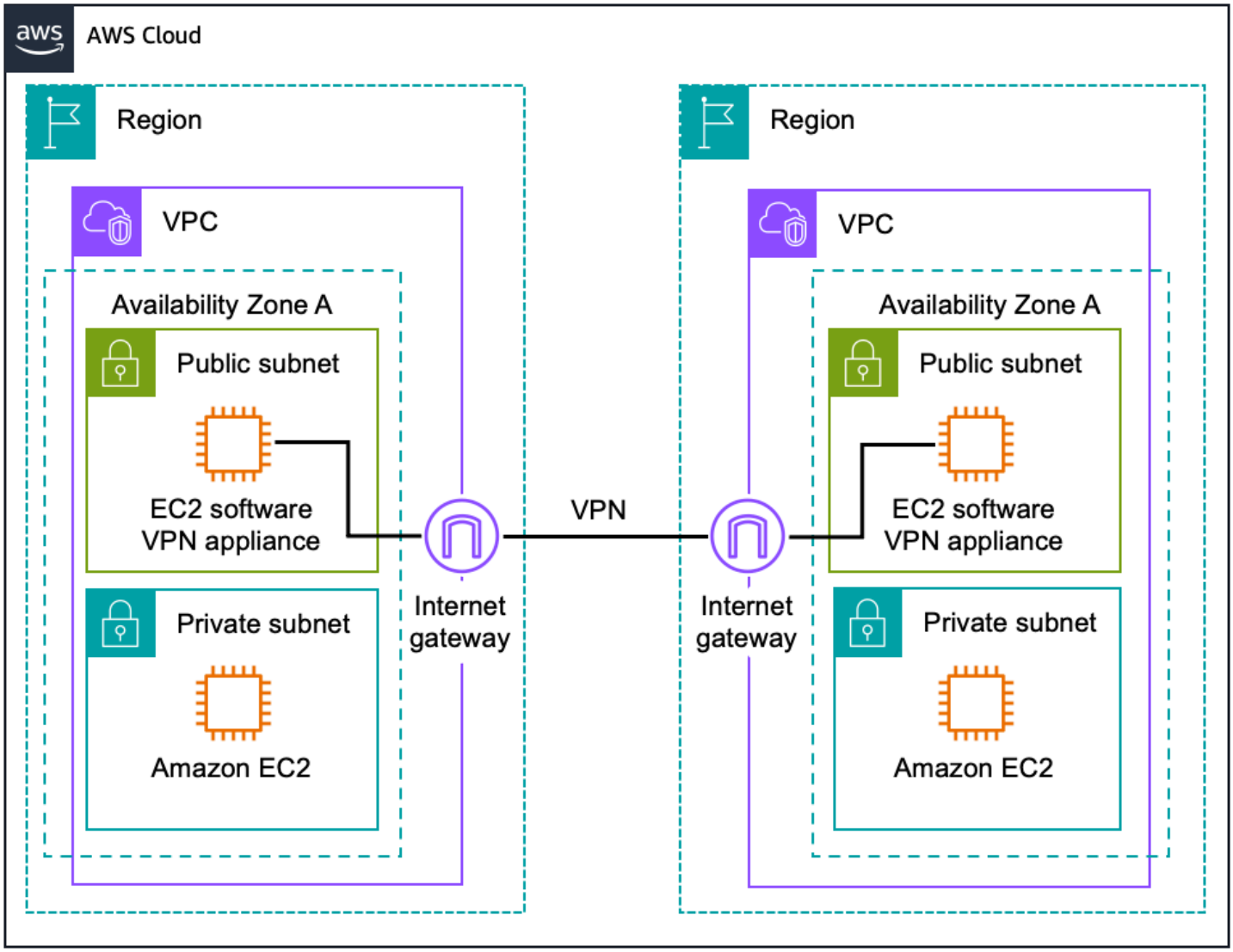
エンドポイントポリシーは、IAM ユーザーポリシーやサービス固有のポリシー (Amazon S3 バケットポリシーなど) を上書きまたは置き換えません。Amazon S3 に接続するためにインターフェイスエンドポイントを使用する場合、Amazon S3 バケットポリシーを使用して、特定のエンドポイントまたは特定の VPC からのバケットへのアクセスを制御できます。

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で 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 内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する機能が含まれます。このオプションは、優先 VPN ソフトウェアプロバイダーを使用して VPN 接続の両方の終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お客様にあります。

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生じ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。

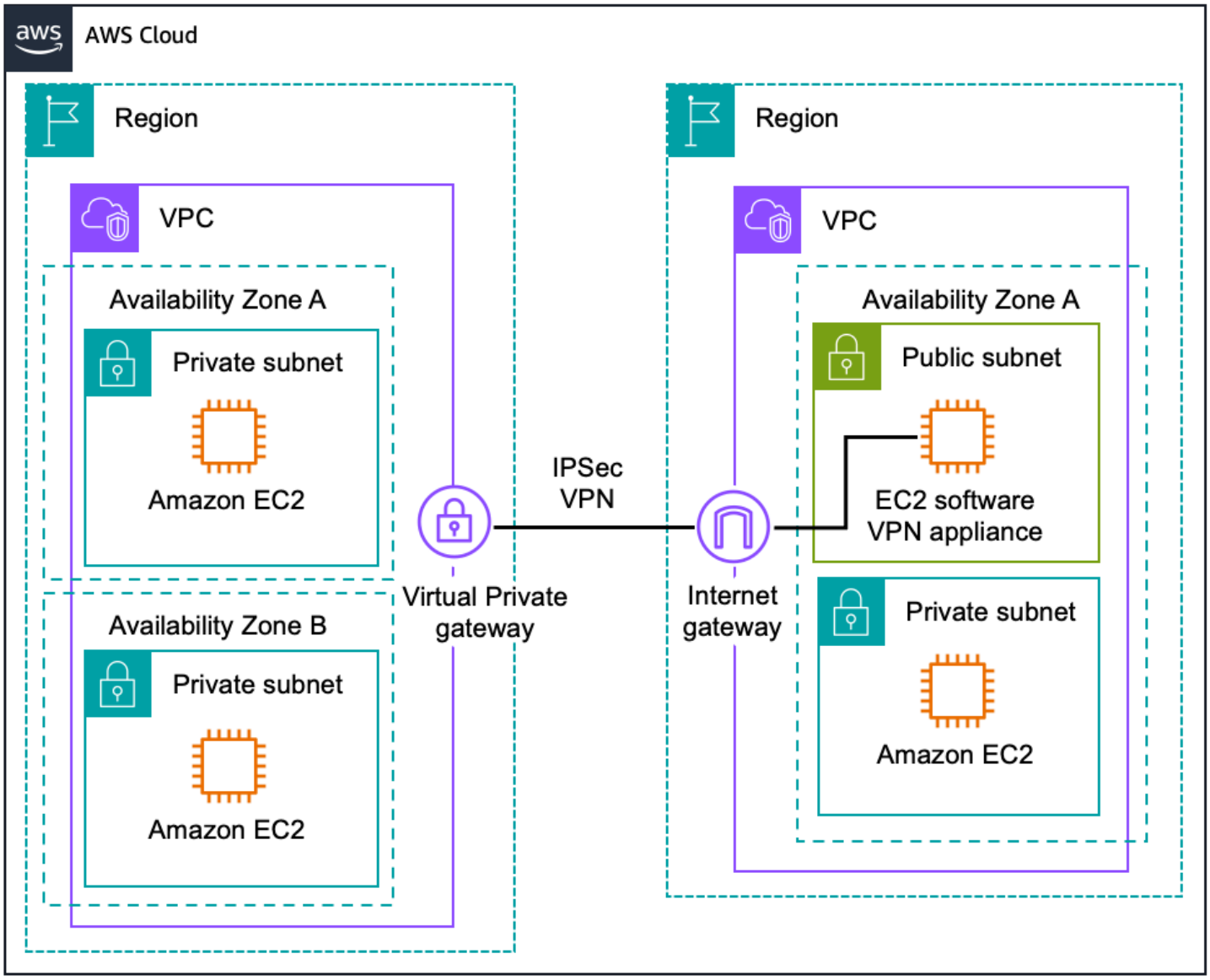
追加リソース

- から利用可能な VPN アプライアンス AWS Marketplace

- テクニカルブリッジ - 複数の VPCs EC2 インスタンスに接続する (IPsec)
- テクニカルブリッジ - 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 から AWS Site-to-Site VPN

Amazon VPC は、AWS マネージド VPN オプションとソフトウェア 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 で仮想プライベートゲートウェイを使用し、別の Amazon VPC でインターネットゲートウェイとソフトウェア VPN アプライアンスを組み合わせて使用します。



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生じ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 への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、低コストで伸縮自在な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できると同時に、AWS でホストされるリソースへの接続をシームレスに体験できます。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囲ではない小規模な企業や、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な企業に推奨されます。

これらのパターンとネットワークから Amazon VPC への接続オプション接続オプション および を組み合わせてAmazon VPC から Amazon VPC への接続オプション、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。

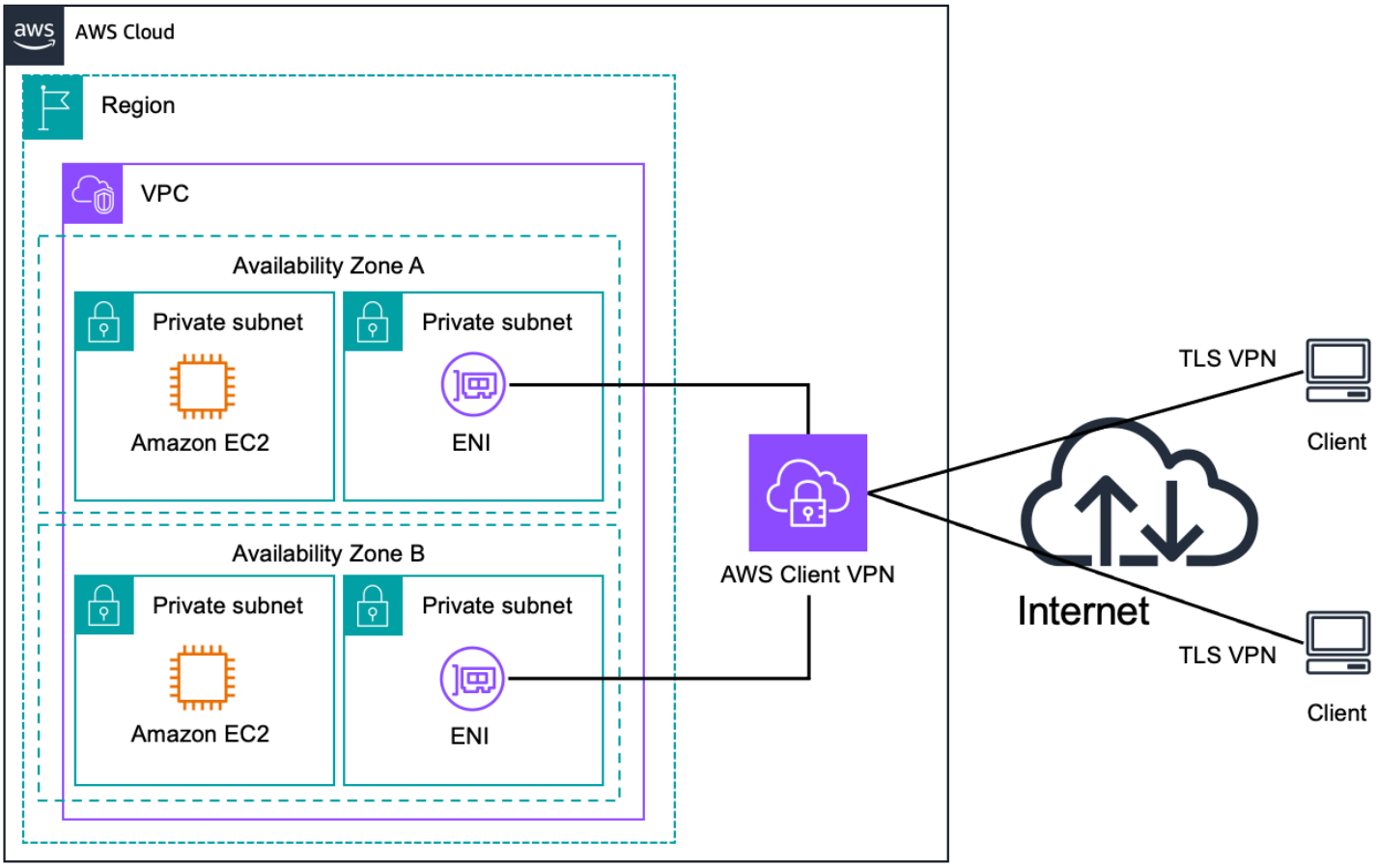
次の表に、これらのオプションの利点と制限事項の概要を示します。

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 マネージド高可用性および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 フルカスタマーマネージドソリューション	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 が管理する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

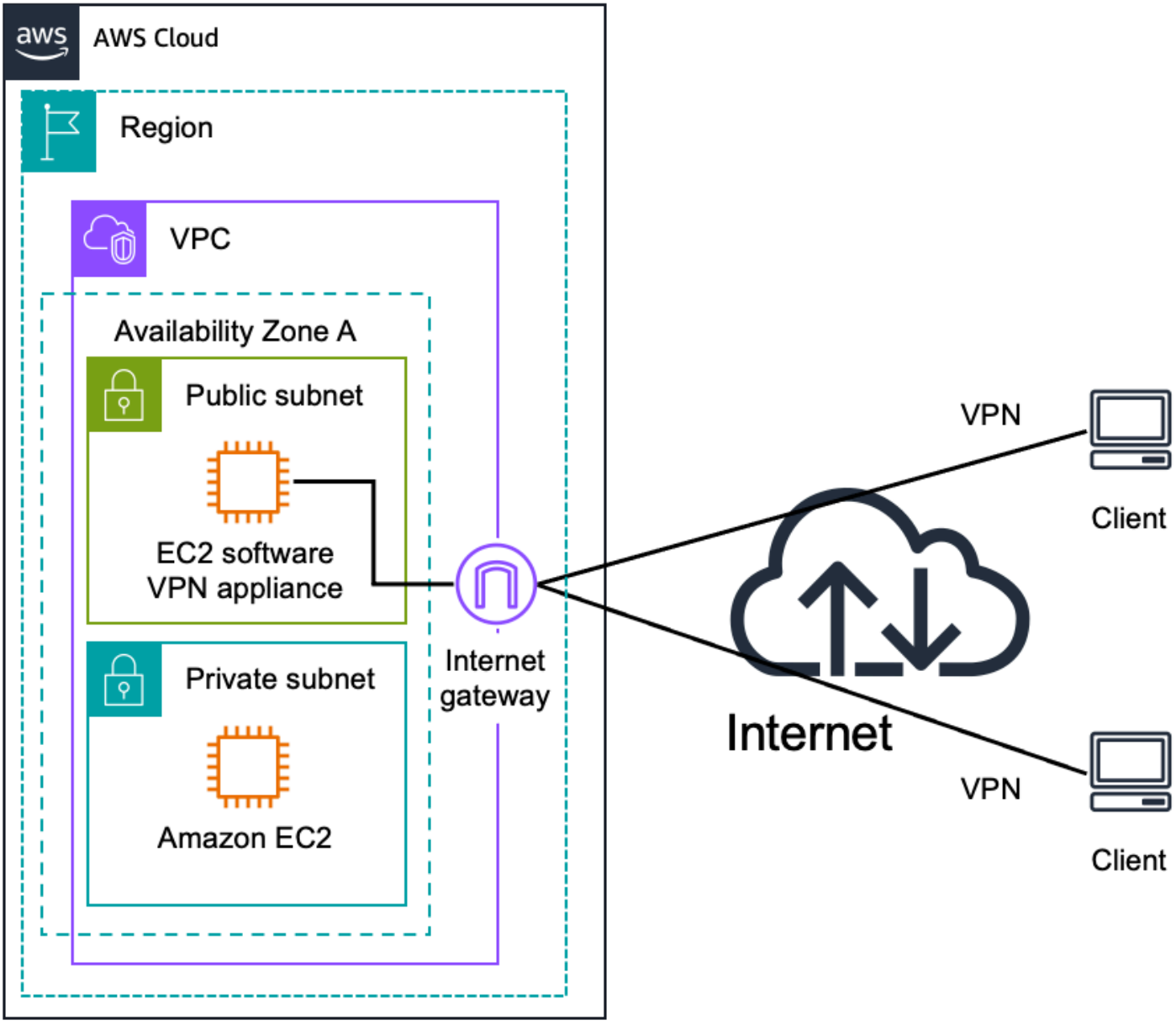
リモートクライアントは、デスクトップ用 AWS クライアント VPN でも、Active Directory による認証または相互証明書認証によるサードパーティーの OpenVPN VPN クライアントでもかまいません。

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非常に柔軟を提供します。



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広く、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 (ネットワークから Amazon VPC オプションのいずれかを活用) 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責任はユーザーにあります。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

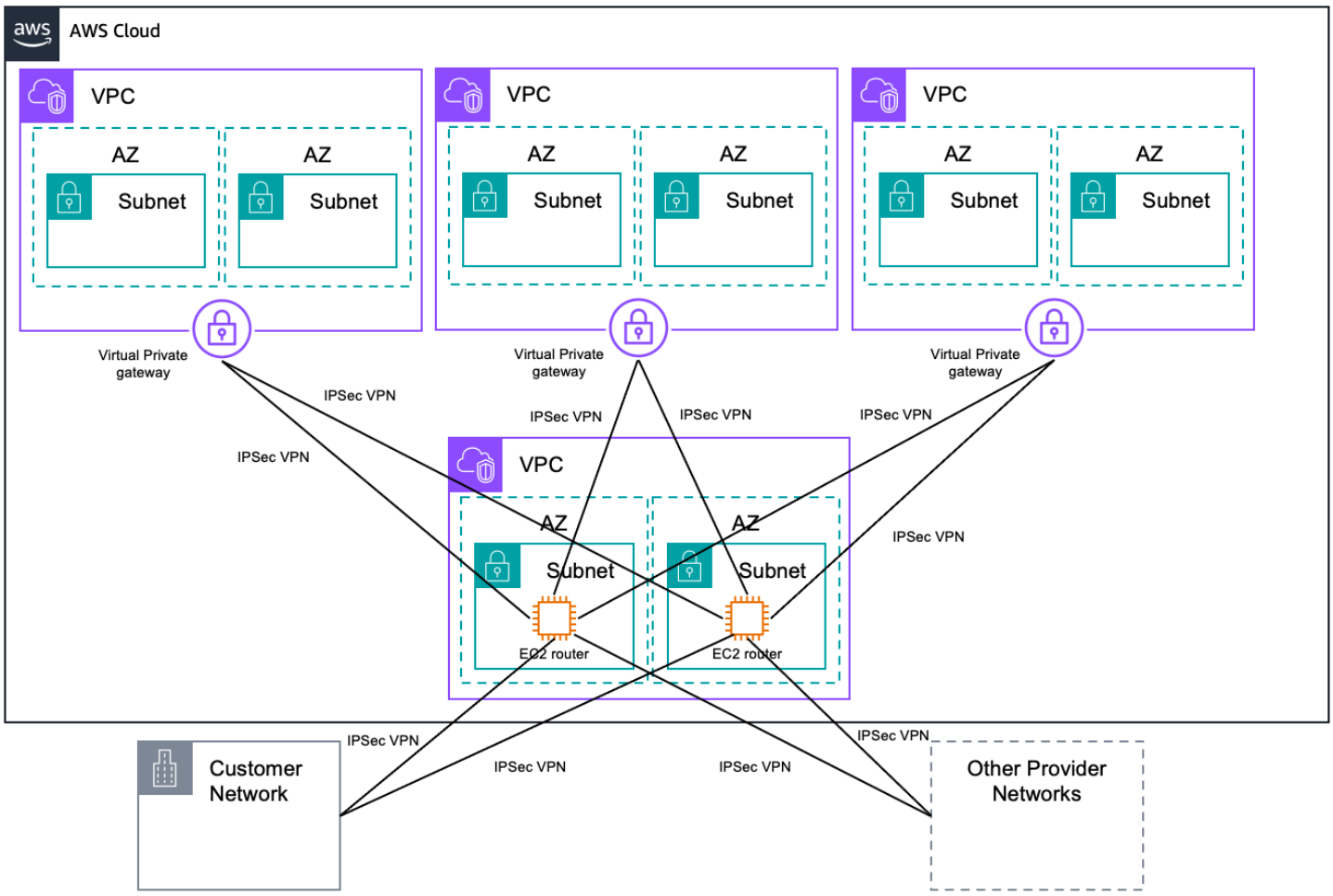
は、「付録 A: ソフトウェア VPN インスタンスの高レベル HA アーキテクチャ」を参照してください。

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

上記のソフトウェア 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、複数の地理的に離れた 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方法です。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

この設計では、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ことに加えて、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することもできます。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
- Cisco Catalyst 8000V for SD-WAN & Routing in AWS Marketplace

AWS クラウド WAN

AWS Cloud WAN は、インテント駆動型のマネージド広域ネットワーク (WAN) です。これは、データセンター、ブランチ、AWS ネットワークを統合するポリシーによって記述されます。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。Cloud WAN には、自動 VPC 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、および添付ファイルをセグメントにマッピングする方法を定義する宣言型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意図を記述できますが、AWS Cloud WAN はネットワーク設定の詳細を処理します。

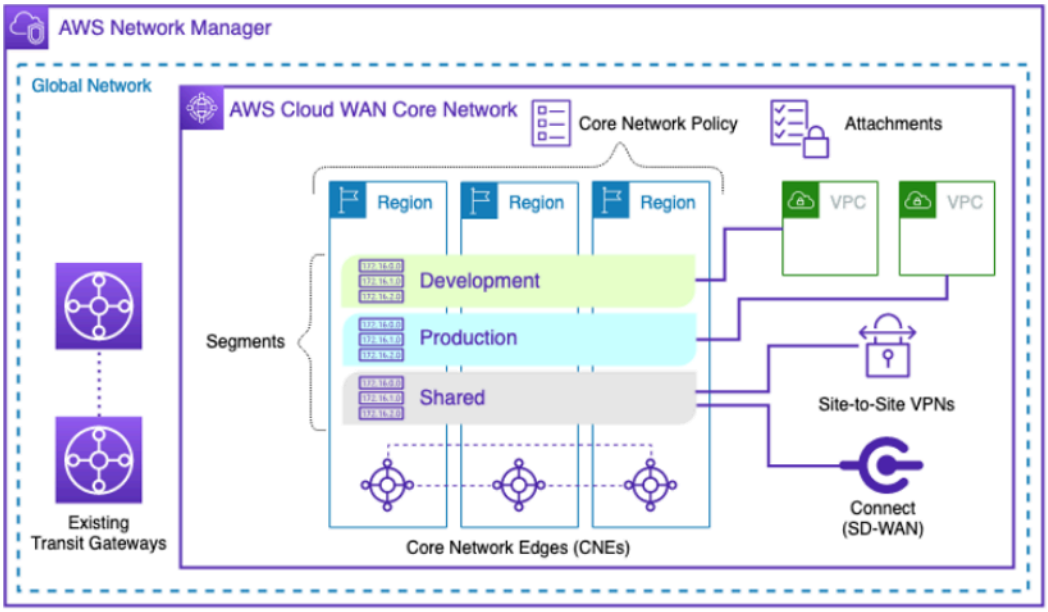
Cloud WAN は AWS Network Manager 内で管理されます。これにより、AWS アカウント、リージョン、オンプレミスロケーション全体で Cloud WAN コアネットワークと Transit Gateway ネットワークを一元管理および可視化できます。Network Manager には、グローバルネットワークのすべての側面を表示およびモニタリングするのに役立つダッシュボードの視覚化がいくつか用意されています。ダッシュボードには、次のようなものがあります。

- 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の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。
- Transit Gateway ネットワークと Transit Gateway のトポロジ図と論理図。

Transit Gateway と Cloud WAN の両方でVPCs とオンプレミスの場所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 リージョンで運用されているお客様、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。Cloud WAN は、ポリシーを使用してグローバルネットワークを定義し、サービスに基盤となるコンポーネントを自動的に実装させたいお客様に最適です。

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。
- Cloud WAN は IPv4 と IPv6 の両方をサポートします。
- 現在、Cloud WAN はAWS Direct Connect添付ファイルをネイティブにサポートしていません。Cloud WAN AWS Direct Connectで を使用するには、 ゲートウェイにアタッチされた Transit Gateway とAWS Direct Connect、 クラウド WAN にピアリング接続された Transit Gateway が必要です。
- 多くの変更がある大規模なネットワークでは、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を作成することを検討してください。



AWS Cloud WAN

追加リソース

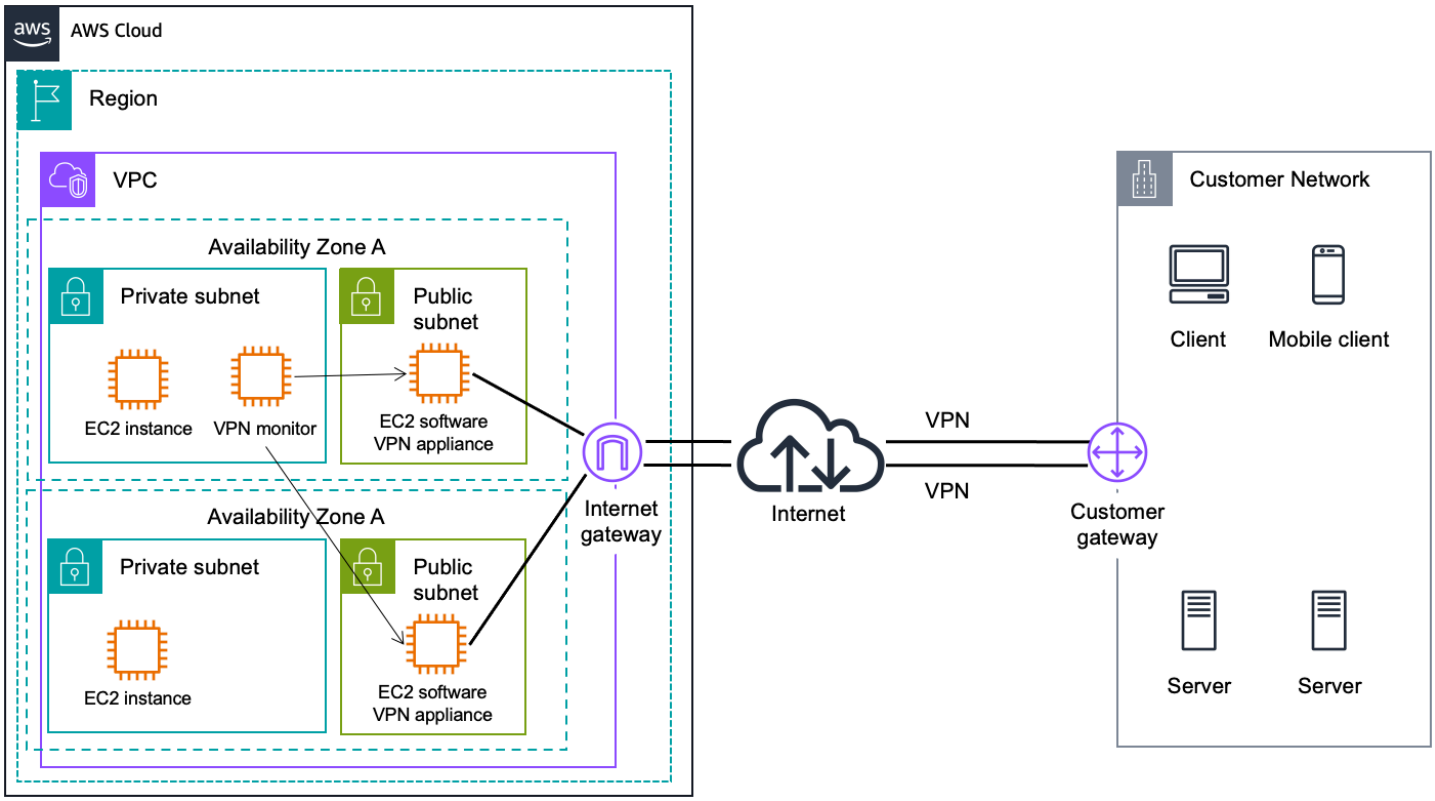
- AWS Cloud WAN ドキュメント
- ブログ記事: AWS Cloud WAN と AWS Transit Gateway の移行と相互運用性のパターン

まとめ

AWS には、リモートネットワークを Amazon VPC と統合する際に AWS を最大限に活用できるように、効率的で安全な接続オプションが数多く用意されています。このホワイトペーパーで示すオプションでは、お客様が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使用している接続オプションやパターンのいくつかに注目します。ここに記載している情報を使用して、物理的な配置場所やホスト場所を問わず、ビジネスの運営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判断できます。

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 インスタンスに対して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をセットアップして設定し、VPN 接続の状態を監視する必要があります。



高レベルのソフトウェア VPN HA

1 つのアベイラビリティーゾーン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 インスタンスを介して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利用するように VPC ルートテーブルを設定することをお勧めします。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対して 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 を作成します。VPN モニターは、VPN モニタリングスクリプトを実行する必要がある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、モニターは、両方の接続が再び機能するまで、影響を受けた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例は、ソフトウェア VPN インスタンスの 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ようとしたりするために必要なビジネスロジックを考慮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収集し、リアルタイムに近い読み取り可能なメトリクスに加工することができます。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 に発行します CloudWatch。これらのメトリクスにより、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 エンタープライズサポート、シニアテクニカルアカウントマネージャー、Daniel Yu
- 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
- スティーブ・モラード、シニアマネージャー、ソリューション・ビルダー、AWS ソリューション・アーキテクチャ
- Sohaib Tahir、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
- Fiona Armada、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
- Pablo Sánchez Carmona、AWS ソリューションアーキテクチャ、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
- Tony TAKe、AWS Enterprise Support、シニアネットワークスペシャリストテクニカルアカウントマネージャー

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、更新された図、および情報を全体で追加しました。	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を修正するための軽微な変更。	2020 年 5 月 20 日
ホワイトペーパーの更新	全体で情報を更新しました。トランジット VPC、Direct Connect ゲートウェイ、および 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 接続オプションが公開されました。	2014 年 7 月 1 日

注意

お客様は、この文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、明示または暗示を問わず、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 契約により規定されます。本書は、AWS とお客様の間で締結されるいかなる契約の一部でもなく、その内容を修正するものでもありません。

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。