AWS ホワイトペーパー

スケーラブルで安全なマルチ VPC の AWS ネットワークインフラストラクチャを構築する

スケーラブルで安全なマルチ VPC の AWS ネットワークインフラストラクチャを構築する: AWS ホワイトペーパー

Table of Contents

スケーラブルで安全なマルチ VPC の AWS ネットワークインフラストラクチャを構築する

発行日: 2020 年 6 月 10 日 (ドキュメント履歴)

要約

AWS のお客様は、多くの場合、ワークロードをセグメント化してフットプリントを拡大するために、数百のアカウントや VPC を利用します。このレベルの規模では、リソース共有、VPC 間接続、オンプレミスから VPC への接続に伴う課題が生じることがよくあります。

このホワイトペーパーでは、Amazon VPC、AWS Transit Gateway、AWS PrivateLink、AWS Direct Connect Gateway などの AWS のサービスを使用して、大規模なネットワークでスケーラブルかつ安全なネットワークアーキテクチャを作成するためのベストプラクティスについて説明します。スケーラビリティ、高可用性、セキュリティを確保し、同時にオーバーヘッドコストを低く抑えながら、増大するインフラストラクチャを管理するためのソリューションを示します。

はじめに

AWS のお客様は、許可、コスト、サービスの間の管理境界を表す単一の AWS アカウントでリソースを構築することから始めます。ただし、お客様の組織が成長するに従って、コストのモニタリング、アクセスの制御、および環境の容易な管理のために、サービスの細分化がさらに必要になります。マルチアカウントソリューションは、組織内の IT サービスやユーザーに特定のアカウントを提供することで、これらの問題を解決します。AWS には、AWS Landing Zone や AWS Control Tower など、このインフラストラクチャを管理および設定するためのツールがいくつか用意されています

図 1 - Landing Zone のアカウント構造

AWS Landing Zone と AWS Control Tower は、AWS の複数のサービスのセットアップと統合を自動化し、ID とアクセス管理 (IAM)、ガバナンス、データセキュリティ、ネットワーク設計、ログ記録を備えた、ベースラインの高度に制御されたマルチアカウント環境を提供します。

図 1 の AWS Landing Zone ソリューションには、4 つのアカウントが含まれています。AWS Organizations アカウント (AWS Landing Zone のマネージドアカウントの設定とアクセスの管理に使用)、共有サービスアカウント (ディレクトリサービスなどのインフラストラクチャ共有サービスの作成に使用)、ログアーカイブアカウント (S3 バケットへの一元化されたログ記録)、セキュリティアカウント (企業のセキュリティおよびコンプライアンスチームが、スポークアカウントでインシデントが発生した場合に緊急のセキュリティオペレーションを監査または実行するために使用) です。

このホワイトペーパーでは、AWS インフラストラクチャを管理するネットワークチームが所有するネットワークサービスアカウントを紹介します。アカウントのネットワークサービスとネットワークインフラストラクチャは、すべてのアカウントおよび VPC によって一元化された方法で共有されます (ハブスポーク設計に類似しています)。この設計により、ランディングゾーンの管理が容易になります。また、各スポーク VPC やアカウントでネットワークサービスを複製する必要がなくなるため、コストを削減できます。

> **Note**
>
> このホワイトペーパーにおいて、「ランディングゾーン」とは、ワークロードのデプロイ先であり、スケーラビリティ、安全性、パフォーマンスに優れたマルチアカウント/マルチ VPC セットアップを表す広義の用語です。このセットアップは、任意のツールを使用して構築できます。

ほとんどのお客様は、いくつかの VPC を使用してインフラストラクチャをデプロイすることから開始します。お客様が所有する VPC の数は、通常、アカウント、ユーザー、ステージングされた環境 (本番、開発、テストなど) の数に関係しています。クラウドの使用量が増えるに従って、お客様がやり取りするユーザー、ビジネスユニット、アプリケーション、リージョンの数が増え、新しい VPC を作成するようになります。

VPC の数が増えるに従って、お客様のクラウドネットワークの運用にはクロス VPC 管理が必要になります。このホワイトペーパーでは、クロス VPC 接続とハイブリッド接続における以下の 3 つの領域に関するベストプラクティスを取り上げます。

- ネットワーク接続 - VPC とオンプレミスネットワークを大規模に相互接続します。
- ネットワークセキュリティ - インターネットおよびエンドポイント (NAT ゲートウェイ、VPC エンドポイント、AWS PrivateLink など) にアクセスするための一元化されたエグレスポイントを構築します。
- DNS 管理 - ランディングゾーンおよびハイブリッド DNS 内で DNS を解決します。

VPC 間の接続

お客様は、マルチ VPC 環境をセットアップするための VPC フローパターンとして、多対多またはハブアンドスポークの 2 つの異なるパターンを使用できます。多対多のアプローチでは、各 VPC 間のトラフィックは各 VPC 間で個別に管理されます。ハブアンドスポークモデルでは、すべての VPC 間トラフィックが中央リソースを経由し、設定されたルールに従ってトラフィックがルーティングされます。

トピック

- VPC ピアリング
- トランジット VPC ソリューション
- トランジットゲートウェイ
- AWS PrivateLink
- Amazon VPC 共有

VPC ピアリング

2 つの VPC 間を接続する最も簡単な方法は、VPC ピアリングを使用することです。このセットアップでは、VPC 間の完全な双方向接続が可能になります。 このピアリング接続は、VPC 間でトラフィックをルーティングするために使用します。 複数のアカウントと AWS リージョンにまたがる VPC をピアリングすることもできます。VPC ピアリングでは、接続を介したトラフィックにのみ料金がかかります (時間単位のインフラストラクチャ料金はありません)。

VPC ピアリングは、ポイント間接続であり、推移的ルーティングをサポートしていません。例えば、VPC A と VPC B 間、および VPC A と VPC C 間に VPC ピアリング接続がある場合、VPC B 内のインスタンスが VPC A を通過して VPC C に到達することはできません。VPC B と VPC C の間でパケットをルーティングするには、直接 VPC ピアリング接続を作成する必要があります。

VPC の数が数十から数百に及ぶ大規模なセットアップでは、ピアリングで VPC 間を相互接続すると、数百から数千に及ぶピアリング接続のメッシュが作成され、管理とスケーリングが困難になります。VPC あたりのピアリング接続数は 125 が上限です。

図 2 - VPC ピアリングを使用したネットワークセットアップ

VPC ピアリングを使用する場合は、各 VPC に対してオンプレミス接続 (VPN または Direct Connect) を確立する必要があります。VPC 内のリソースは、ピアリングされた VPC のハイブリッド接続を使用してオンプレミスに到達することはできません (図 2)。

VPC ピアリングは、特定の VPC 内のリソースが別の VPC 内のリソースと通信する必要があり、両方の VPC の環境が制御および保護され、接続する VPC の数が 10 未満である (各接続の個別管理が可能である) 場合に最適です。VPC ピアリングは、VPC 間接続の他のオプションと比較して、全体的なコストが最も低くなります。

トランジット VPC ソリューション

トランジット VPC では、VPC 間の接続にハブアンドスポーク設計を導入することで、VPC ピアリングの欠点の一部を解決できます。トランジット VPC ネットワークでは、1 つの中央 VPC (ハブ VPC) が VPN 接続 (通常はIPsec 経由の BGP を利用) を介して他のすべての VPC (スポーク VPC) と接続します。中央 VPC には、ソフトウェアアプライアンスを実行する EC2 インスタンスが含まれており、VPN オーバーレイを使用して着信トラフィックを宛先にルーティングします (図 3)。トランジット VPC ピアリングには、以下の利点があります。

- オーバーレイ VPN ネットワークを使用した推移的ルーティングが可能になり、ハブアンドスポーク設計がシンプルになります。
- ハブのトランジット VPC 内の EC2 インスタンスでサードパーティーのベンダーソフトウェアを使用すると、ベンダーの高度なセキュリティ (レイヤー 7 ファイアウォール/IPS/IDS) に関する機能を活用できます。お客様がオンプレミスで同じソフトウェアを使用している場合、統合された運用/モニタリングエクスペリエンスからメリットを得られます。

図 3 - Cisco CSR を使用した Transit VPC

トランジット VPC には独自の課題があります。例えば、仮想アプライアンスの実行コストが高くなる、VPC あたりのスループットが制限される (VPN トンネルあたり最大 1.25 Gbps)、設定と管理のオーバーヘッドが増える (お客様が EC2 インスタンスの可用性と冗長性を管理する必要がある) などが挙げられます。

トランジットゲートウェイ

AWS Transit Gateway は、Cisco CSR などの仮想アプライアンスをプロビジョニングすることなく、VPC とオンプレミスネットワークとを接続するハブアンドスポーク設計をフルマネージドサー

ビスとして提供します。VPN オーバーレイは不要であり、AWS が高可用性と高スケーラビリティを管理します。

Transit Gateway を使用すると、お客様は数千の VPC に接続できます。すべてのハイブリッド接続 (VPN 接続と Direct Connect 接続) を 1 つの Transit Gateway にアタッチして、組織の AWS ルーティング設定全体を 1 か所に統合して制御できます (図 4)。Transit Gateway は、接続されているすべてのスポークネットワーク間で、ルートテーブルを使用してどのようにトラフィックをルーティングするかを制御します。このハブアンドスポークモデルでは、VPC は Transit Gateway に接続するだけで接続されているネットワークにアクセスできるため、管理が簡素化され、運用コストが削減されます。

図 4 - AWS Transit Gateway を使用したハブアンドスポーク設計

Transit Gateway はリージョンリソースで、同じ AWS リージョン内で何千もの VPC に接続できます。リージョンごとに複数の Transit Gateway を作成できますが、AWS リージョン内のトランジットゲートウェイはピアリングできません。ハイブリッド接続の場合、1 つの Direct Connect 接続を介して最大 3 つの Transit Gateway に接続できます。このような理由から、アーキテクチャを 1 つの Transit Gateway だけに制限して特定のリージョン内のすべての VPC を接続し、必要な場合はいつでも Transit Gateway のルーティングテーブルを使用して VPC 間を分離します。有効なケースとして、設定ミスの影響範囲を制限するためだけに複数の Transit Gateway を作成する場合があります。

組織の Transit Gateway は、ネットワークサービスアカウントに配置します。これにより、ネットワークサービスアカウントを管理するネットワークエンジニアによる一元管理が可能になります。AWS Resource Access Manager (RAM) を使用して、同じリージョン内で AWS Organization 内の複数のアカウントにわたって、VPC を接続する Transit Gateway を共有できます。 AWS RAM を使用すると、AWS リソースをあらゆる AWS アカウントと、または AWS Organization 内で簡単かつ安全に共有できます。詳細については、ブログ記事「セントラルアカウントでトランジットゲートウェイへの AWS Transit Gateway アタッチメントを自動化する」を参照してください。

トピック

Transit Gateway と Transt VPC の比較

Transit Gateway には、Transit VPC と比べていくつかの利点があります。

- Transit Gateway は、数百の VPC との VPN 接続を維持する複雑さを抽象化します。
- Transit Gateway を使用すると、EC2 ベースのソフトウェアアプライアンスを管理およびスケーリングする必要がなくなります。トラフィックのルーティングに必要なすべてのリソースを管理する責任は、AWS が引き受けます。
- Transit Gateway は、高可用性と冗長性を備えたマルチ AZ インフラストラクチャを提供することで、高可用性を管理する必要性をなくします。
- Transit Gateway は、VPC 間通信の帯域幅を AZ あたり 50 Gbps のバースト速度に向上させます。
- Transit Gateway は、ユーザーコストを GB 単位および時間単位のシンプルな転送モデルに合理化します。
- Transit Gateway は、EC2 プロキシと VPN カプセル化の必要性をなくすことで、レイテンシーを短縮します。

Transit Gateway と VPC ピアリング

Transit Gateway は、複数の VPC ピアリング接続を大規模に作成および管理する複雑さを解決します。これにより、TGW はほとんどのネットワークアーキテクチャにとって適切なデフォルトになります。ただし、VPC ピアリングは TGW と比べて以下の利点があるため、依然として有効な選択肢です。

- 低コスト - VPC ピアリングでは、データ転送料金のみ支払います。Transit Gateway は、データ転送料金に加えて、アタッチメントごとに時間単位の料金がかかります。
- 帯域幅制限なし - Transit Gateway では、VPC 接続あたりの最大帯域幅 (バースト) は 50 Gbps です。VPC ピアリングには集約帯域幅がありません。個々のインスタンスのネットワークパフォーマンス制限とフロー制限 (プレイスメントグループ内では 10 Gbps、それ以外では 5 Gbps) が両方のオプションに適用されます。VPC ピアリングのみがプレイスメントグループをサポートしています。
- レイテンシー - VPC ピアリングとは異なり、Transit Gateway は VPC 間の追加ホップです。
- セキュリティグループの互換性 - リージョン内 VPC ピアリングではセキュリティグループを参照できます。現在、Transit Gateway では参照できません。

ランディングゾーンのセットアップでは、Transit Gateway によって有効化されたハブアンドスポークモデルと組み合わせて VPC ピアリングを使用できます。

AWS PrivateLink

特定の VPC (サービスプロバイダー) にあるサービス/アプリケーションを、AWS リージョン内の他のコンシューマー VPC にプライベートに公開し、コンシューマー VPC だけがサービスプロバイダー VPC への接続を開始できるようにしたい場合があります。例えば、プライベートアプリケーションからサービスプロバイダー API にアクセスできるようにします。

AWS PrivateLink を使用するには、VPC でアプリケーション用の Network Load Balancer を作成し、このロードバランサーを指す VPC エンドポイントサービス設定を作成します。次に、サービスコンシューマーがサービスへのインターフェイスエンドポイントを作成します。これにより、Elastic Network Interface がプライベート IP アドレスとともにサブネットに作成されます。このアドレスは、サービスへのトラフィックのエントリポイントとなります。コンシューマーとサービスは同じ VPC 内に存在する必要はありません。VPC が異なる場合、コンシューマー VPC とサービスプロバイダー VPC の IP アドレス範囲は重複しても構いません。他の VPC 内のサービスにアクセスするためのインターフェイス VPC エンドポイントを作成するほかに、AWS PrivateLink を介してサポートされている AWS のサービスにプライベートにアクセスするためのインターフェイス VPC エンドポイントを作成こともできます (図 5)。

図 5 – AWS PrivateLink

Transit Gateway、VPC ピアリング、AWS PrivateLink のどれを選択するかは、接続によって異なります。

AWS PrivateLink - クライアント/サーバーセットアップで、サービスプロバイダー VPC 内の特定のサービスや一連のインスタンスへの単方向アクセスを 1 つ以上のコンシューマー VPC に許可する場合は、AWS PrivateLink を使用します。コンシューマー VPC 内のクライアントだけが、サービスプロバイダー VPC 内のサービスへの接続を開始できます。これは、2 つの VPC 内のクライアントとサーバーの IP アドレスが重複している場合にも適しています。AWS PrivateLink は、クライアント VPC 内の ENI を活用してサービスプロバイダーとの IP 競合を回避します。AWS PrivateLink のエンドポイントには、VPC ピアリング、VPN、および AWS Direct Connect 経由でアクセスできます。

VPC ピアリングと Transit Gateway - VPC 間でレイヤー 3 の IP 接続を有効にする場合は、VPC ピアリングと Transit Gateway を使用します。

アーキテクチャでは、以上のテクノロジーを組み合わせてさまざまなユースケースに対応できます。これらすべてのサービスは、相互に組み合わせて運用できます。例えば、AWS PrivateLink では、API スタイルのクライアント/サーバー接続を処理します。VPC ピアリングでは、リージョン内

でプレイスメントグループが引き続き必要な場合やリージョン間接続が必要な場合に、直接接続要件を処理します。Transit Gateway では、大規模な VPC 間の接続やハイブリッド接続のエッジ統合を簡素化します。

Amazon VPC 共有

VPC を共有することは、チーム間のネットワーク分離を VPC 所有者が厳密に管理する必要はないが、アカウントレベルのユーザーおよび許可を厳密に管理する必要がある場合に便利です。共有 VPC では、複数の AWS アカウントが、一元化された共有の Amazon VPC 内にアプリケーションリソース (Amazon EC2 インスタンスなど) を作成します。このモデルでは、VPC を所有するアカウント (所有者) は、他のアカウント (参加者) と 1 つ以上のサブネットを共有します。サブネットが共有されると、参加者は共有しているサブネット内にある自分のアプリケーションリソースを表示、作成、変更、および削除できます。参加者は、他の参加者または VPC 所有者に属するリソースを表示、変更、または削除することはできません。共有 VPC 内のリソース間のセキュリティは、セキュリティグループとサブネットネットワーク ACL を使用して管理します。

VPC 共有の利点:

- 設計の簡素化 - VPC 間接続に関する複雑性がない
- マネージド VPC の減少
- ネットワークチームとアプリケーション所有者との職務分離
- IPv4 アドレスの使用率向上
- コスト低減 - 同じアベイラビリティーゾーン内の異なるアカウントに属するインスタンス間ではデータ転送料金が不要

注意: 複数のアカウント間でサブネットを共有する場合、IP 領域とネットワークリソースを共有することになるため、参加者間である程度の協力が必要です。必要に応じて、参加者アカウントごとに異なるサブネットを共有することを選択できます。参加者ごとに 1 つのサブネットを使用すると、セキュリティグループに加えて、ネットワーク ACL でネットワーク分離を達成できます。

ほとんどのお客様のアーキテクチャには複数の VPC が含まれ、その多くは 2 つ以上のアカウントで共有されます。Transit Gateway と VPC ピアリングを使用して、共有 VPC 間を接続できます。例えば、アプリケーションが 10 個あるとします。各アプリケーションには独自の AWS アカウントが必要です。アプリケーションは 2 つのアプリケーションポートフォリオに分類できます (同じポートフォリオ内のアプリケーション間ではネットワーク要件が類似しており、アプリケーション 1～5 は「マーケティング」、アプリケーション 6～10 は「セールス」です)。

アプリケーションポートフォリオごとに 1 つの VPC (合計 2 つの VPC) を持つことができます。VPC は、そのポートフォリオ内の異なるアプリケーション所有者アカウントと共有されます。アプリケーション所有者は、それぞれの共有 VPC 内にアプリケーションをデプロイします (この例では、異なるサブネット内にデプロイし、NACL を使用してネットワークルートの区分と分離を行います)。2 つの共有 VPC は Transit Gateway 経由で接続します。このセットアップにより、10 個の VPC を接続する代わりに 2 個の VPC を接続するだけで済みます (図 6)。

図 6 - セットアップ例 - 共有 VPC

> **Note**
>
> VPC を共有する参加者は、すべての AWS リソースを共有サブネット内で作成することはできません。詳細については、「Amazon VPC 制限」を参照してください。

ハイブリッド接続

このセクションでは、クラウドリソースとオンプレミスのデータセンターとの安全な接続に注目します。ハイブリッド接続を実現するには、次の 2 つのアプローチがあります。

1. 1 対 1 接続 - このセットアップでは、VPC ごとに VPN 接続または Direct Connect プライベート VIF を作成します。これを行うには、仮想プライベートゲートウェイ (VGW) を活用します。このオプションは少数の VPC には適していますが、VPC 数が増えるに従って VPC ごとにハイブリッド接続を管理することが難しくなる場合があります。
2. エッジ統合 - このセットアップでは、複数の VPC のハイブリッド IT 接続を 1 つのエンドポイントに統合します。すべての VPC が、これらのハイブリッド接続を共有します。これを行うには、AWS Transit Gateway と Direct Connect Gateway を使用します。

トピック

VPN

図 7 - AWS VPN 終端オプション

VPN を AWS に設定するには、3 つの方法があります。

1. Transit Gateway で VPN 接続を統合する - このオプションでは、Transit Gateway で Transit Gateway VPN アタッチメントを活用します。Transit Gateway は、Site-to-Site VPN の IPsec 終端をサポートしています。お客様は Transit Gateway への VPN トンネルを作成し、それにアタッチされている VPC にアクセスできます。Transit Gateway は、静的 VPN 接続と BGP ベースの動的 VPN 接続の両方をサポートしていますTransit Gateway は、VPN アタッチメントでの等価コストマルチパス (ECMP) もサポートしています。各 VPN 接続のスループットは最大 1.25 Gbps で、ECMP を有効にすると、VPN 接続全体のスループットを集約できます。このオプションでは、Transit Gateway の料金と AWS VPN の料金を支払います。このオプションは、VPN 接続に使用することをお勧めします。詳細については、「AWS VPN の概要」を参照してください。
2. EC2 インスタンスで VPN を終端する - このオプションは、特定のベンダーのソフトウェア機能セット (Cisco DMVPN や GRE など) を必要とする場合、またはさまざまな VPN デプロイにわ

たって運用を一貫させる必要がある場合に、エッジケースで利用します。トランジット VPC 設計はエッジ統合に利用できますが、トランジット VPC の「VPC 間接続」セクションで説明したすべての主要な考慮事項がハイブリッド VPN 接続にも該当することを覚えておくことが重要です。お客様は、高可用性を管理する責任を負い、EC2 インスタンスとベンダーのソフトウェアライセンスのコストを負担します。

3. 仮想プライベートゲートウェイ (VGW) で VPN を終端する - このオプションを使用すると、1 対 1 の接続設計が可能になります。この設計では、VPC ごとに 1 つの VPN 接続 (冗長 VPN トンネルのペアで構成) を作成します。これは AWS への VPN 接続を開始するのに適した方法ですが、VPC 数を増やす場合は、Transit Gateway を利用するエッジ統合設計が最終的にはより適切なオプションとなります。VPC への VPN スループットは 1.25 Gbps に制限されており、ECMP ロードバランシングはサポートされていません。料金は、AWS VPN に対してのみ支払います。VGW の実行には料金がかかりません。詳細については、「AWS VPN の料金」と「仮想プライベートゲートウェイでの AWS VPN」を参照してください。

Direct Connect

インターネット経由の VPN は、使い始める際に便利なオプションですが、本番トラフィックではインターネット接続を信頼できない場合があります。この信頼性の低さから、多くのお客様が AWS Direct Connect を選択しています。AWS Direct Connect は、お客様のデータセンターと AWS との間で、一貫性のある低レイテンシーで高帯域幅の専用ファイバー接続を可能にします。AWS Direct Connect を利用して VPC に接続するには、4 つの方法があります。

図 8 - オンプレミスのデータセンターをランディングゾーンに接続する 4 つの方法

- VPC にアタッチされた VGW へのプライベート仮想インターフェイス (VIF) を作成する - Direct Connect 接続ごとに 50 個の VIF を作成し、最大 50 個の VPC に接続できます (1 つの VIF が 1 つの VPC への接続を提供します)。VPC ごとに 1 つの BGP ピアリングがあります。このセットアップにおける接続は、Direct Connect が存在する AWS リージョンに制限されます。VIF から VPC への 1 対 1 のマッピング (およびグローバルアクセスの欠如) は、ランディングゾーンの VPC にアクセスするための最も好ましくない方法となっています。
- 複数の VGW に関連付けられた Direct Connect ゲートウェイへのプライベート VIF を作成する (各 VGW は VPC にアタッチされる) - Direct Connect Gateway は、いずれの AWS アカウントでも最大 10 個の VGW にグローバルに (中国を除く) 接続できます。これは、ランディングゾーンが少数の VPC (10 個以下) で構成されている場合や、グローバルアクセスが必要な場合に最適なオプションです。Direct Connect 接続ごとの Direct Connect ゲートウェイごとに 1 つの BGP ピアリングが

あります。Direct Connect ゲートウェイは、南北トラフィックフロー専用で、VPC 間接続は許可しません。

- Transit Gateway に関連付けられた Direct Connect ゲートウェイへのトランジット VIF を作成する - 1 Gbps 以上で動作する専用接続または Direct Connect ホスト接続を介して、Transit Gateway を Direct Connect ゲートウェイに関連付けることができます。このオプションを使用すると、1 つの VIF および BGP ピアリングを介して、複数の異なる AWS リージョンや AWS アカウントにわたって最大 3 つの Transit Gateway (それぞれが数千の VPC に接続可能) にオンプレミスのデータセンターを接続できます。これは、複数の VPC を大規模に接続するための 4 つのオプションの中で最も単純なセットアップですが、Transit Gateway の制限に注意する必要があります。 1 つの重要な制限は、トランジット VIF を介して Transit Gateway からオンプレミスルーターにアドバタイズできる CIDR 範囲は 20 に限られることです。オプション 1 およびオプション 2 では、Direct Connect の料金を支払います。オプション 3 では、Transit Gateway のアタッチメント料金とデータ転送料金も支払います。詳細については、Direct Connect での Transit Gateway の関連付けに関するドキュメントを参照してください。
- Direct Connect パブリック VIF 経由で Transit Gateway への VPN 接続を作成する - パブリック仮想インターフェイスを使用すると、パブリック IP アドレスを使用してすべての AWS パブリックサービスとエンドポイントにアクセスできます。Transit Gateway で VPN アタッチメントを作成すると、AWS 側での VPN 終端用として 2 つのパブリック IP アドレスが取得されます。これらのパブリック IP には、パブリック VIF 経由で到達可能です。パブリック VIF を介して、必要なだけ多くの Transit Gateway への VPN 接続を作成できます。パブリック VIF 経由で BGP ピアリングを作成すると、AWS は AWS パブリック IP 範囲全体をルーターにアドバタイズします。特定のトラフィックのみを許可する (VPN 終端エンドポイントへのトラフィックのみを許可するなど) には、オンプレミスでファイアウォールを使用することをお勧めします。このオプションを使用すると、ネットワークレイヤーで Direct Connect を暗号化できます。

オプション 3 (Direct Connect ゲートウェイへのトランジット VIF) は、Direct Connect 接続ごとに 1 つの BGP セッションを使用して、特定の AWS リージョンのすべてのオンプレミス接続を 1 つのポイント (Transit Gateway) に統合できるという点で、最適なオプションのように思えます。ただし、オプション 3 にはいくつかの制限や考慮事項が伴うため、ランディングゾーンの接続要件に応じてオプション 2 とオプション 3 の両方を活用することをお勧めします。図 9 に示すセットアップ例では、VPC に接続するためのデフォルトの方法として Transit VIF を使用しています。また、オンプレミスの DC からメディア VPC に大量のデータを転送する必要があるエッジユースケースにはプライベート VIF を使用しています。プライベート VIF は、Transit Gateway のデータ転送料金を回避するために使用します。ベストプラクティスとしては、冗長性を最大限に高めるために、2 つの異なる Direct Connect ロケーションで少なくとも 2 つの接続 (合計 4 つの接続) を使用します。接続ごと

に 1 つの VIF を作成し、合計 4 つのプライベート VIF と 4 つのトランジット VIF を使用します。また、AWS Direct Connect 接続へのバックアップ接続としての VPN も作成します。

図 9 - ハイブリッド接続のリファレンスアーキテクチャの例

ネットワークサービスアカウントを使用して Direct Connect リソースを作成し、ネットワーク管理境界を定めます。 Direct Connect 接続、Direct Connect ゲートウェイ、Transit Gateway のすべては、ネットワークサービスアカウント内に存在できます。AWS Direct Connect 接続をランディングゾーンと共有するには、単に Transit Gateway を RAM 経由で他のアカウントと共有します。

インターネットへのエグレスの一元化

ランディングゾーンにアプリケーションをデプロイすると、多くのアプリケーションにはアウトバウンド専用のインターネットアクセス (ライブラリ/パッチ/OS アップデートのダウンロードなど) が必要になります。これを実現するには、ネットワークアドレス変換 (NAT) ゲートウェイまたは EC2 インスタンス (ソース NAT (SNAT) で設定) を、すべてのエグレスインターネットアクセスの次ホップとして使用します。内部アプリケーションはプライベートサブネット内に存在し、NAT ゲートウェイ/EC2 NAT インスタンスはパブリックサブネット内に存在します。

NAT ゲートウェイの使用

NAT ゲートウェイをスポーク VPC ごとにデプロイすると、デプロイする NAT ゲートウェイごとに時間単位の料金 (「Amazon VPC の料金」を参照) がかかるため、コストが高くなる可能性があります。したがって、NAT ゲートウェイを一元化することが望ましいオプションとなります。一元化するには、ネットワークサービスアカウントでエグレス VPC を作成し、Transit Gateway を利用して、この VPC 内にある NAT ゲートウェイ経由ですべてのエグレストラフィックをスポーク VPC からルーティングします (図 10 を参照)。

注意: Transit Gateway を使用して NAT ゲートウェイを一元化すると、VPC ごとに NAT ゲートウェイを実行する分散アプローチに比べて、Transit Gateway のデータ処理料金が余分にかかります。VPC から NAT ゲートウェイ経由で大量のデータを送信するエッジケースでは、Transit Gateway のデータ処理料金を回避するために NAT を VPC 内でローカルに維持する方が、費用対効果の高いオプションとなる場合があります。

図 10 - Transit Gateway を使用して一元化した NAT ゲートウェイ (概要)

図 11 - Transit Gateway を使用して一元化した NAT ゲートウェイ (ルートテーブル設計)

このセットアップでは、スポーク VPC アタッチメントがルートテーブル 1 (RT1) に関連付けられ、ルートテーブル 2 (RT2) に伝播されます。2 つの VPC が相互に通信できないように、ブラックホールルートを明示的に追加しています。VPC 間通信を許可する場合は、RT1 から「10.0.0.0/8-> BlackHole」ルートエントリを削除できます。これにより、VPC 間では NAT ゲートウェイ経由で通信できるようになります。スポーク VPC アタッチメントを RT1 に伝播することもできます (または、1 つのルートテーブルを使用して、すべてをそのテーブルに関連付ける/伝播することもできます)。これにより、Transit Gateway を使用した VPC 間の直接トラフィックフローが可能になります。

すべてのトラフィックをエグレス VPC に向ける静的ルートを RT1 に追加します。この静的ルートにより、Transit Gateway はすべてのインターネットトラフィックをエグレス VPC の ENI 経由で送信します。トラフィックは、エグレス VPC に入ると、これらの Transit Gateway ENI が存在するサブネットルートテーブルに定義されているルールに従います。このサブネットルートテーブルに、すべてのトラフィックを NAT ゲートウェイに向けるルートを追加します。NAT ゲートウェイのサブネットルートテーブルには、次ホップとしてインターネットゲートウェイ (IGW) があります。リターントラフィックを逆流させるには、静的ルートテーブルエントリを NAT ゲートウェイサブネットルートテーブルに追加し、スポーク VPC 向けのすべてのトラフィックを、次ホップとしての Transit Gateway に向ける必要があります。

高可用性

高可用性を実現するには、2 つの NAT ゲートウェイ (各 AZ に 1 つ) を使用する必要があります。AZ 内では、NAT ゲートウェイの可用性 SLA は 99.9% です。AZ 内のコンポーネント障害に対する冗長性は、SLA 契約に基づいて AWS が処理します。トラフィックは、AZ で NAT ゲートウェイが使用できない 0.1% の時間中にドロップされます。1 つの AZ が完全に失敗すると、その AZ 内の Transit Gateway エンドポイントと NAT ゲートウェイが失敗するため、すべてのトラフィックは他の AZ の Transit Gateway および NAT ゲートウェイエンドポイントを経由して流れます。

セキュリティ

セキュリティについては、ソースインスタンスのセキュリティグループ、Transit Gateway ルートテーブルのブラックホールルート、NAT ゲートウェイがあるサブネットのネットワーク ACL に依存します。

スケーラビリティ

NAT ゲートウェイは、送信先ごとに最大 55,000 の同時接続をサポートできます。スループットは、NAT ゲートウェイのパフォーマンス上限によって制限されます。Transit Gateway はロードバランサーではないため、複数の AZ の NAT ゲートウェイにトラフィックを均等に分散させることはありません。Transit Gateway を通過するトラフィックは、可能な限り、AZ 内にとどまります。トラフィックを開始する EC2 インスタンスが AZ 1 にある場合、トラフィックは同じ AZ 1 でエグレス VPC 内にある Transit Gateway の Elastic Network Interface から出て、Elastic Network Interface が存在するサブネットルートテーブルに基づく次ホップへ流れます。ルールの詳細なリストについては、「NAT ゲートウェイのルールと制限」を参照してください。

詳細については、ブログ記事「AWS Transit Gateway を使用して複数の VPC からの 1 つのインターネット出口ポイントを作成する」を参照してください。

EC2 インスタンスを使用したアウトバウンドの一元化

AWS Marketplace からソフトウェアベースのファイアウォールアプライアンス (EC2 上) をエグレスポイントとして使用することは、NAT ゲートウェイのセットアップと似ています。このオプションは、さまざまなベンダーが提供するレイヤー 7 ファイアウォール/侵入防御/検出システム (IPS/IDS) 機能を活用する場合に役立ちます。

図 12 では、NAT ゲートウェイを EC2 インスタンスに置き換えています (EC2 インスタンスで SNAT を有効化する)。このオプションには、以下の主な考慮事項があります。

高可用性

このセットアップでは、ユーザーが EC2 インスタンスのモニタリング、障害の検出、EC2 インスタンスからバックアップ/スタンバイインスタンスへの置換の責任を負います。ほとんどの AWS ベンダーは、このセットアップでデプロイされるソフトウェアに対して、オートメーションを事前に構築済みです。このオートメーションで、以下を制御できます。

- プライマリ EC2-1 インスタンスの障害を検出する。
- プライマリインスタンスで障害が発生した場合、すべてのトラフィックをバックアップ EC2-2 インスタンスに向けるようにルートテーブル「Route Table Egx 1」を変更する。これは AZ 2 のサブネットに対しても行う必要があります。

図 12 - EC2 インスタンスと Transit Gateway を使用した集中型 NAT

スケーラビリティ

Transit Gateway はロードバランサーではないため、2 つの AZ のインスタンス間でトラフィックを均等に分散させることはありません。Transit Gateway を通過するトラフィックは、可能な限り、AZ 内にとどまります。1 つの EC2 インスタンスの帯域幅の能力によって制限を受けます。この EC2 インスタンスは、使用量の増加に従って垂直方向にスケーリングできます。

エグレストラフィックの検査のために選択したベンダーが障害検出のオートメーションをサポートしていない場合、または水平スケーリングが必要な場合は、別の設計を使用できます。この設計 (図 13) では、エグレス VPC の Transit Gateway に VPC アタッチメントを作成せず、代わりに IPsec VPN アタッチメントを作成します。また、Transit Gateway から EC2 インスタンスへの IPsec VPN を作成し、BGP を利用してルートを交換します。

利点

- トラフィックの障害検出と再ルーティングは BGP で処理されます。VPC サブネットルートテーブルのオートメーションは不要です。
- BGP ECMP を使用すると、複数の EC2 インスタンス間でトラフィックをロードバランスできます。水平スケーリングが可能です。

図 13 - EC2 インスタンスと Transit Gateway VPN を使用した集中型 NAT

主な考慮事項

- EC2 インスタンスの VPN 管理オーバーヘッド
- Transit Gateway の帯域幅は、VPN トンネルあたり 1.25 Gbps に制限されています。ECMP を使用すると、Transit Gateway は最大 50 Gbps の合計 VPN 帯域幅をサポートできます。ベンダーアプライアンスの VPN およびパケット処理機能が制限要因になる可能性があります。
- この設計では、FW EC2 インスタンスがインバウンドトラフィックとアウトバウンドトラフィックに同じ Elastic Network Interface を使用して動作していることを前提としています。
- 複数の EC2 インスタンスでトラフィックの ECMP ロードバランシングを有効にする場合は、リターンフローの対称性を保証するために、EC2 インスタンスでトラフィックを SNAT する必要があります。この場合、送信先には真の送信元がわかりません。

VPC 間のトラフィックおよびオンプレミスから VPC へのトラフィックのネットワークセキュリティの一元化

AWS は、ランディングゾーン内にネットワークセキュリティを実装するためのセキュリティグループとサブネット NACLS を提供しています。これらはレイヤー 4 のファイアウォールです。VPC 間またはオンプレミスのデータセンターと VPC との間を流れるトラフィックを検査するために、ランディングゾーン内にレイヤー 7 のファイアウォール/IPS/IDS を実装したい場合があります。これを実現するには、Transit Gateway とサードパーティーのソフトウェアアプライアンス (EC2 インスタンス上で実行) を使用します。図 14 のアーキテクチャを使用すると、VPC 間のトラフィックとオンプレミスから VPC へのトラフィックを EC2 インスタンス経由で流すことができます。この設定は図 12 で既に説明したものと似ています。ただし、ルートテーブル 1 のブラックホールルートを削除して、インターン VPC トラフィックフローを許可し、さらに VPN アタッチメントまたは Direct Connect GW アタッチメントをルートテーブル 1 にアタッチしてハイブリッドトラフィックフローを許可します。これにより、スポークから送信されるすべてのトラフィックは、宛先に送信される前に、エグレス VPC へ流れます。トラフィックの検査後に、スポーク VPC とオンプレミス CIDR へのトラフィックを Transit Gateway 経由で送信するには、エグレス VPC サブネットルートテーブル (ファイアウォール EC2 アプライアンスが存在) 内に静的ルートが必要です。

> **Note**
>
> ルート情報は、Transit Gateway からサブネットルートテーブルに動的に伝達されないため、静的に入力する必要があります。サブネットルートテーブルでは、50 個の静的ルートがソフト制限になっています。

図 14 - VPC 間および VPC からオンプレミスへのトラフィックの制御

インライン検査のために EC2 インスタンスにトラフィックを送信する際の主な考慮事項:

- Transit Gateway のデータ処理に伴う追加料金
- トラフィックはさらに 2 つのホップ (EC2 インスタンスと Transit Gateway) を通過する必要がある
- 帯域幅とパフォーマンスのボトルネックの可能性
- EC2 インスタンスの保守、管理、スケーリングの複雑化

- 障害の検出とスタンバイへのフェイルオーバー
- 使用状況の追跡と水平/垂直スケーリング
- ファイアウォール設定、パッチ管理
- ロードバランシングによって対称フローを保証する際のトラフィックの送信元ネットワークアドレス変換 (SNAT)

これらの EC2 インスタンスを経由してどのトラフィックを通過させるかを選択する必要があります。その 1 つの方法は、セキュリティゾーンを定義し、信頼できないゾーン間のトラフィックを検査することです。信頼できないゾーンとしては、サードパーティが管理するリモートサイト、自分が管理/信頼していないベンダー VPC、自分の環境と比較してセキュリティフレームワークが緩いサンドボックス/開発 VPC などがあります。図 15 では、信頼できるネットワーク間の直接的なトラフィックフローを実現するとともに、インライン EC2 インスタンスを使用して信頼できないネットワークとの間で送受信されるトラフィックフローを検査しています。この例では、以下の 3 つのゾーンを作成しています。

- 信頼できないゾーン - これは「信頼できないリモートサイト向けの VPN」またはサードパーティーのベンダー VPC へのトラフィック用です。
- 本番ゾーン - これには、本番 VPC とオンプレミスのお客様 DC からのトラフィックが含まれます。
- 開発ゾーン - これには 2 つの開発 VPC からのトラフィックが含まれます。

ゾーン間の通信用に定義するルール例を以下に示します。

1. 信頼できないゾーン/本番ゾーン間 - 通信を許可しない
2. 本番ゾーン/開発ゾーン間 - エグレス VPC の EC2 FW アプライアンスを経由した通信を許可する
3. 信頼できないゾーン/開発ゾーン間 - エグレス VPC の EC2 FW アプライアンスを経由した通信を許可する
4. 本番ゾーン/本番ゾーン間、開発ゾーン/開発ゾーン間 - Transit Gateway 経由の直接通信

このセットアップはセキュリティゾーンが 3 つある場合ですが、3 つ以上ある場合もあります。複数のルートテーブルとブラックホールルートを使用して、セキュリティの分離と最適なトラフィックフローを実現できます。適切なゾーンの選択は、全体的なランディングゾーンの設計戦略 (アカウント構造、VPC 設計) によって異なります。ゾーンを使用して、BU、アプリケーション、環境などの間を分離できます。

次の例では、Transit Gateway で信頼できないリモート VPN を終端し、すべてのトラフィックを EC2 上のソフトウェア FW アプライアンスに送信して検査します。または、Transit Gateway ではなく EC2 インスタンスでこれらの VPN を直接終端することもできます。このアプローチでは、信頼できない VPN トラフィックが Transit Gateway と直接やり取りすることはありません。トラフィックフローのホップ数が 1 つ減少し、AWS VPN のコストが削減されます。動的ルート交換を有効にする (Transit Gateway が BGP 経由でリモート VPN の CIDR を確認できるようにする) には、ファイアウォールインスタンスを VPN 経由で Transit Gateway に接続する必要があります。ネイティブの TGW アタッチメントモデルでは、次ホップをエグレス/セキュリティ VPC として VPN CIDE の TGW 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。このセットアップ (図 15) では、すべてのトラフィック用にエグレス VPC へのデフォルトルートがあるため、特定の静的ルートを明示的に追加する必要はありません。このアプローチでは、フルマネージドの Transit Gateway VPN 終端エンドポイントからセルフマネージドの EC2 インスタンスに移行するため、コンピューティングとメモリに関して VPN 管理のオーバーヘッドと負荷が EC2 インスタンスで増大します。

図 15 - トラフィックを分離するための Transit Gateway の使用とセキュリティゾーンの定義

DNS

デフォルト以外の VPC 内でインスタンスを起動すると、AWS はこのインスタンスにプライベート DNS ホスト名を割り当てます。さらに、このインスタンスにパブリック IPv4 アドレスがある場合は、VPC に指定した DNS 属性に応じて、パブリック DNS ホスト名が割り当てられる場合があります。「enabledNSSupport」属性を true に設定すると、VPC 内に Route 53 Resolver から DNS 解決 (および VPC CIDR に対する 2 つの IP オフセット) が取得されます。デフォルトでは、Route 53 Resolver は、EC2 インスタンスや Elastic Load Balancing ロードバランサーのドメイン名などの VPC ドメイン名に対する DNS クエリに応答します。VPC ピアリングでは、1 つの VPC 内のホストは、パブリック DNS ホスト名をピアリングされた VPC 内のインスタンスのプライベート IP アドレスに解決できます (このためのオプションを有効にしている場合)。AWS Transit Gateway 経由で接続された VPC についても同様です。詳細については、「VPC ピアリング接続の DNS 解決サポートの有効化」を参照してください。

インスタンスをカスタムドメイン名にマッピングする場合は、Amazon Route 53 を使用してカスタムの DNS から IP へのマッピングレコードを作成できます。Amazon Route 53 ホストゾーンは、Amazon Route 53 がドメインとそのサブドメインに対する DNS クエリにどのように応答するかについての情報を保持するコンテナです。パブリックホストゾーンにはパブリックインターネット上で解決可能な DNS 情報が含まれています。一方、プライベートホストゾーンは特定のプライベートホストゾーンにアタッチされた VPC にのみ情報を提供する特定の実装です。複数の VPC/アカウントがあるランディングゾーンのセットアップでは、複数の AWS アカウントやリージョンにまたがって 1 つのプライベートホストゾーンを複数の VPC に関連付けることができます。VPC 内のエンドホストは、それぞれの Route 53 Resolver の IP (および VPC CIDR に対する 2 つのオフセット) を DNS クエリのネームサーバーとして使用します。VPC 内の Route 53 Resolver は、VPC 内のリソースからの DNS クエリのみを受け入れます。

ハイブリッド DNS

AWS ランディングゾーンの設定とオンプレミスのリソースとの間で DNS 解決を調整することは、ハイブリッドネットワークで最も重要な要件の 1 つです。ハイブリッド環境を実装しているお客様は、通常、DNS 解決システムを導入済みであり、現在のシステムと連携する DNS ソリューションを必要としています。AWS リージョン内の VPC 用の DNS とネットワーク用の DNS を統合する場合は、1 つの Route 53 Resolver インバウンドエンドポイント (VPC に転送する DNS クエリ用) と 1 つの Route 53 Resolver アウトバウンドエンドポイント (VPC からネットワークに転送するクエリ用) が必要です。 図 16 に示すように、VPC 内の EC2 インスタンスから受け取ったクエリをネットワーク上の DNS サーバーに転送するように、アウトバウンド Resolver エンドポイントを設定で

きます。選択したクエリを VPC からオンプレミスに転送するには、Route 53 Resolver ルールを作成して、転送する DNS クエリのドメイン名 (example.com など) と、クエリの転送先であるネットワーク上の DNS リゾルバーの IP アドレスを指定します。オンプレミスから Route 53 ホストゾーンへのインバウンドクエリの場合、ネットワーク上の DNS サーバーは、指定した VPC 内のインバウンド Resolver エンドポイントにクエリを転送できます。

図 16 - Route 53 Resolver を使用したハイブリッド DNS 解決

これにより、オンプレミスの DNS リゾルバーは、その VPC と関連付けられている Route 53 プライベートホストゾーンの EC2 インスタンスやレコードなどの AWS リソースのドメイン名を簡単に解決できます。

ランディングゾーンのすべての VPC に Route 53 Resolver エンドポイントを作成することはお勧めしません。エンドポイントは、中央のエグレス VPC (ネットワークサービスアカウント内) に一元化します。このアプローチにより、管理が容易になるとともにコストを低く抑えることができます (作成したインバウンド/アウトバウンドエンドポイントごとに時間単位の料金が請求されます)。一元化したインバウンド/アウトバウンドエンドポイントを、ランディングゾーンの残りと共有します。

アウトバウンド解決 - ネットワークサービスアカウントを使用してリゾルバーを記述します (どの DNS クエリをオンプレミスの DNS サーバーに転送するかに基づきます)。Resource Access Manager (RAM) を使用して、これらの Route 53 Resolver ルールを複数のアカウントで共有します (また、アカウントの VPC と関連付けます)。スポーク VPC の EC2 インスタンスは DNS クエリを Route 53 Resolver に送信できます。Route 53 Resolver Service は、これらのクエリをエグレス VPC のアウトバウンド Route 53 Resolver エンドポイント経由でオンプレミス DNS サーバーに転送します。 スポーク VPC をエグレス VPC にピアリングしたり、Transit Gateway 経由で接続したりする必要はありません。アウトバウンドリゾルバーエンドポイントの IP をスポーク VPC のプライマリ DNS として使用しないでください。スポーク VPC は、VPC 内で (VPC CIDR のオフセットに) Route 53 Resolver を使用する必要があります。

図 17 - エグレス VPC での Route 53 Resolver エンドポイントの一元化

インバウンド DNS 解決 - 一元化された VPC に Route 53 Resolver インバウンドエンドポイントを作成し、この一元化された VPC にランディングゾーン内のすべてのプライベートホストゾーンを関連付けます。詳細については、「より多くの VPC をプライベートホストゾーンに関連付ける」を参照してください。VPC に関連付けられた複数のプライベートホストゾーン (PHZ) は重複できません。図 17 に示すように、この PHZ と一元化された VPC の関連付けにより、オンプレミスサーバーは、一元化された VPC のインバウンドエンドポイントを使用して (中央 VPC に関連付けられてい

る) プライベートホストゾーンのエントリの DNS を解決できるようになります。 ハイブリッド DNS のセットアップの詳細については、「Amazon Route 53 と AWS Transit Gateway を使用したハイブリッドクラウドの DNS の一元管理」および「Amazon VPC のハイブリッドクラウド DNS オプション」を参照してください。

VPC プライベートエンドポイントへのアクセスの一元化

VPC エンドポイントを使用すると、インターネットゲートウェイや NAT デバイスを必要とせずに、サポートされている AWS のサービスに VPC をプライベートに接続できます。VPC 内のインスタンスは、パブリック IP アドレスがなくても、このインターフェイスエンドポイントを使用して AWS のサービスエンドポイントと通信できます。VPC と他のサービスとの間のトラフィックは、AWS ネットワークバックボーンから離れません。現在、2 種類のエンドポイントとして、インターフェイスエンドポイント (AWS PrivateLink を使用) とゲートウェイエンドポイントをプロビジョニングできます。ゲートウェイエンドポイントは自由にプロビジョニングできます。一元化のための強力なユースケースはありません。

インターフェイス VPC エンドポイント

インターフェイスエンドポイントは、1 つ以上の Elastic Network Interface で構成され、サポートされている AWS のサービスへのトラフィックのエントリポイントとなるプライベート IP アドレスが割り当てられます。インターフェイスエンドポイントをプロビジョニングすると、エンドポイントを実行した時間ごとにコストがかかります。デフォルトでは、AWS のサービスにアクセスする VPC ごとにインターフェイスエンドポイントを作成します。したがって、複数の VPC で AWS の特定のサービスとやり取りするランディングゾーンのセットアップでは、コストがかかり、管理しにくい場合があります。これを回避するには、一元化された 1 つの VPC でインターフェイスエンドポイントをホストできます。すべてのスポーク VPC は、これらの一元管理されたエンドポイントを使用します。

AWS のサービスへの VPC エンドポイントを作成するときに、プライベート DNS を有効にすることができます。この設定を有効にすると、AWS マネージドの Route 53 プライベートホストゾーン (PHZ) が作成され、パブリック AWS サービスエンドポイントをインターフェイスエンドポイントのプライベート IP に解決できるようになります。マネージド PHZ は、インターフェイスエンドポイントを持つ VPC 内でのみ機能します。このセットアップでは、一元化された VPC でホストされている VPC エンドポイント DNS をスポーク VPC で解決できるようにしたい場合、マネージド PHZ は機能しません。これを克服するには、インターフェイスエンドポイントの作成時にプライベート DNS を自動的に作成するオプションを無効にします。または、図 18 に示すように、Route 53 PHZ を手動で作成し、インターフェイスエンドポイントを指す完全な AWS のサービスエンドポイント名でエイリアスレコードを追加することもできます。

図 18 – 手動で作成した PHZ

このプライベートホストゾーンは、ランディングゾーン内の他の VPC と関連付けられます。この設定により、スポーク VPC はフルサービスエンドポイント名を、一元化された VPC のインターフェイスエンドポイントに解決できます。

> **Note**
>
> 共有プライベートホストゾーンにアクセスするには、スポーク VPC 内のホストが VPC の Route 53 リゾルバー IP を使用する必要があります。インターフェイスエンドポイントには、VPN および Direct Connect 経由でオンプレミスネットワークからもアクセスできます。条件付き転送ルールを使用して、フルサービスエンドポイント名のすべての DNS トラフィックを Route 53 リゾルバーのインバウンドエンドポイントに送信します。このインバウンドエンドポイントがプライベートホストゾーンに従って DNS リクエストを解決します。

図 19 では、Transit Gateway がスポーク VPC から一元化されたインターフェイスエンドポイントへのトラフィックフローを有効にしています。ネットワークサービスアカウントで VPC エンドポイントとそのプライベートホストゾーンを作成し、スポークアカウントでスポーク VPC と共有します。他の VPC とエンドポイント情報を共有する方法の詳細については、AWS Transit Gateway と AWS PrivateLinkAmazon Route 53 Resolver の統合に関するブログ記事を参照してください。

注意: VPC エンドポイントの分散アプローチ (つまり、VPC ごとのエンドポイント) を使用すると、VPC エンドポイントに最小特権ポリシーを適用できます。一元化されたアプローチでは、1 つのエンドポイントですべてのスポーク VPC アクセスにポリシーを適用して管理します。VPC の数が増えるに従って、単一のポリシードキュメントで最小特権を維持することの複雑さが増す可能性があります。単一のポリシードキュメントでは、影響範囲も拡大します。ポリシードキュメントのサイズも制限されます (20,480 文字)。

図 19 - インターフェイス VPC エンドポイントの一元化

まとめ

AWS の使用量をスケールし、アプリケーションを AWS ランディングゾーンにデプロイすると、VPC とネットワークコンポーネントの数が増えます。このホワイトペーパーでは、スケーラビリティ、高可用性、セキュリティを確保し、同時にコストを低く抑えながら、増大するインフラストラクチャをどのように管理できるかについて説明しました。Transit Gateway、共有 VPC、AWS Direct Connect、VPC エンドポイント、サードパーティーのソフトウェアアプライアンスなどのサービスを活用する場合、設計上の適切な意思決定を行うことが重要になります。各アプローチの主要な考慮事項を理解し、要件から逆向きに作業を進めて、どのオプションまたはオプションの組み合わせが最適かを分析することが重要です。

寄稿者

このドキュメントの執筆に当たり、以下の人物が寄稿しました。

- Sidhartha Chauhan、アマゾン ウェブ サービス、ソリューションアーキテクト
- Amir Abu-Akeel、アマゾン ウェブ サービス、クラウドインフラストラクチャアーキテクト
- Kevin Bell、アマゾン ウェブ サービス、ソリューションアーキテクト

ドキュメント履歴

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 フィードをサブスクライブしてください。

update-history-change	update-history-description	update-history-date
マイナーな更新	「Transit Gateway と VPC ピアリングの比較」セクションを更新しました。	2021 年 4 月 2 日
ホワイトペーパーの更新	図 7 に示しているオプションに合わせてテキストを修正しました。	2020 年 6 月 10 日
マイナーな更新	図 7 に示しているオプションに合わせてテキストを修正しました。	2020 年 6 月 10 日
初版発行	ホワイトペーパーを発行しました。	2019 年 11 月 15 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 の現行製品と慣行を表すものであって、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構成する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 とお客様の間で行われるいかなる契約の一部でもなく、そのような契約の内容を変更するものでもありません。