AWS ホワイトペーパー

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

スケーラブルで安全なマルチ VPC AWS ネットワークインフラストラクチャの構築: 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 AWS ネットワークインフラストラクチャの構築

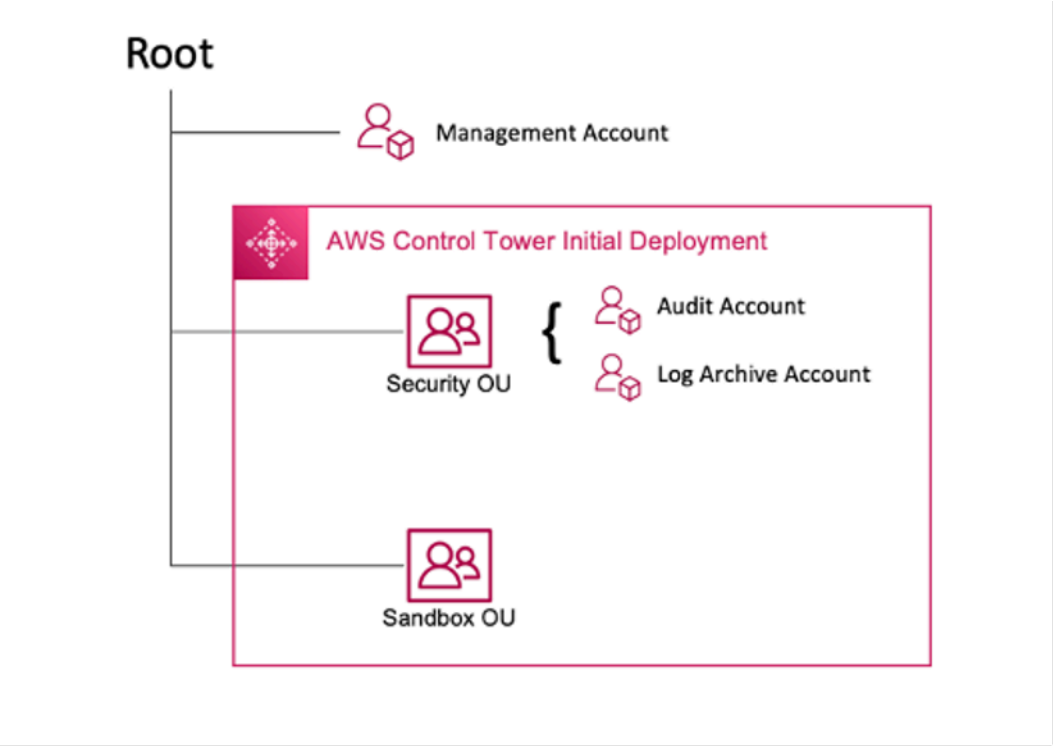
公開日: 2024 年 4 月 17 日 (ドキュメント履歴)

アマゾン ウェブ サービス (AWS) のお客様は、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、何百ものアカウントと仮想プライベートクラウド (VPCs) に頼ることがよくあります。このレベルのスケールでは、リソース共有、VPC 間接続、VPC 接続へのオンプレミス施設に関する課題が頻繁に生じます。

このホワイトペーパーでは、Amazon Virtual Private Cloud (Amazon VPC)、AWS Transit Gateway、、AWS PrivateLink、Direct ConnectGateway Load Balancer、、Amazon Route 53 などの AWS サービスを使用してAWS Network Firewall、大規模なネットワークにスケーラブルで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。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、オーバーヘッドコストを抑えながら、スケーラビリティ、高可用性、セキュリティを確保します。

序章

AWS のお客様は、アクセス許可、コスト、サービスをセグメント化する管理境界を表す 1 つの 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つれて、コストのモニタリング、アクセスの制御、環境管理の簡素化のために、サービスのセグメント化を強化する必要があります。マルチアカウントソリューションは、組織内の IT サービスと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。 には、 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 AWS 用意されていますAWS Control Tower。



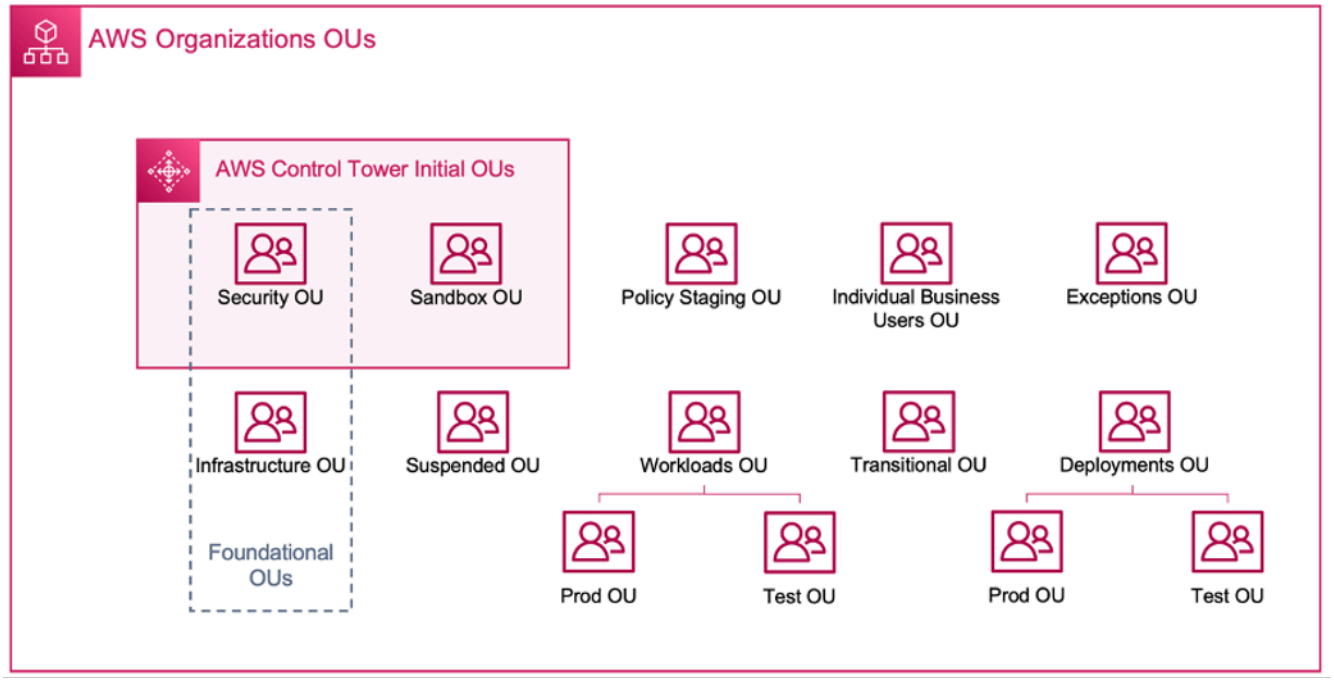
AWS Control Tower の初期デプロイ

を使用してマルチアカウント環境を設定すると AWS Control Tower、2 つの組織単位 (OUsが作成されます。

- セキュリティ OU – この OU 内で、 は 2 つのアカウント AWS Control Tower を作成します。
- ログアーカイブ
- 監査 (このアカウントは、ガイダンスで前述したセキュリティツールアカウントに対応します) 。
- サンドボックス OU – この OU は、 内に作成されたアカウントのデフォルトの送信先です AWS Control Tower。これには、チームの許容可能な使用ポリシーに従って、ビルダーが AWS サービス、およびその他のツールやサービスを試すことができるアカウントが含まれています。

AWS Control Tower では、追加の OUs を作成、登録、管理して初期環境を拡張し、ガイダンスを実装できます。

次の図は、 AWS Control Towerによって最初にデプロイされた OU を示しています。 AWS 環境を拡張して、図に含まれている推奨 OU のいずれかを実装し、要件を満たすことができます。



AWS 組織 OUs

を使用したマルチアカウント環境の詳細については AWS Control Tower、「複数アカウントを使用した環境の整理」ホワイトペーパーの「付録 E」を参照してください。 AWS

ほとんどのお客様は、インフラストラクチャをデプロイするためにいくつかの VPCs から始めます。顧客が作成する VPCs の数は通常、アカウント、ユーザー、ステージング環境 (本番稼働、開発、テストなど) の数に関連しています。クラウドの使用が増えるにつれて、顧客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、リージョンの数も増加し、新しい VPCsが作成されます。

VPCs の数が増えるにつれて、クロス VPC 管理はお客様のクラウドネットワークの運用に不可欠です。このホワイトペーパーでは、VPC 間およびハイブリッド接続における 3 つの特定の分野のベストプラクティスについて説明します。

- ネットワーク接続 — VPCs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 – ネットワークアドレス変換 (NAT) ゲートウェイ、VPC エンドポイント 、、、Gateway Load Balancer などのインターネットとエンドポイントにアクセスするための一元的な出力ポイントを構築します。 AWS PrivateLink AWS Network Firewall https://aws.amazon.com/elasticloadbalancing/gateway-load-balancer/
- DNS 管理 – Control Tower およびハイブリッド DNS 内の DNS を解決します。

IP アドレスの計画と管理

スケーラブルなマルチアカウントマルチ VPC ネットワーク設計を構築するには、IP アドレスの計画と管理が不可欠です。適切な IP アドレス指定スキームでは、現在および将来のネットワークニーズを考慮する必要があります。IP アドレススキーム IP は、オンプレミスワークロード、クラウドワークロードをカバーし、将来の拡張 (新規、ビジネスユニット AWS リージョン、合併や買収の追加など) も可能にする必要があります。また、チームが誤って重複CIDRs を作成しないようにする必要があります。分離されたワークロードや切断されたワークロードなど、重複する IP CIDR が必要な場合は、この決定を意識し、ルーティング、セキュリティ、コストへの影響を考慮する必要があります。また、このような例外に必要な承認プロセスの作成を検討する必要がある場合もあります。優れた IP アドレス指定スキームは、ネットワーク設計とルーティング設定の簡素化にも役立ちます。

主な考慮事項:

- IP アドレススキーム (パブリック IP とプライベート IPs) を事前に計画し、IP アドレス管理ツールを選択して、すべてのワークロードで IP アドレスの使用状況を割り当て、管理、追跡します。
- 階層型および要約された IP アドレス指定スキームを使用します。
- 環境、組織、またはビジネスユニットに基づいて AWS リージョン、一貫した IP 割り当てを計画します。
- オンプレミスネットワークとクラウドネットワーク用に個別の IP CIDRs (IPv4 と IPv6 の両方) を指定します。
- 重複する IP CIDRs。
- IP CIDRs のサイズを適切に設定して、スケーリングと将来の成長を可能にします。
- IPv6 またはデュアルスタックの互換性のためにワークロードを有効にして、IP 競合を減らし、IPv4 スペースの枯渇に対処します。

Amazon VPC IP Address Manager (IPAM) を使用すると、 AWS ワークロードのパブリック IP アドレスとプライベート IP アドレスの両方の計画、追跡、モニタリングを簡素化できます。IPAM を使用すると、複数の および 間で IP アドレス空間を整理、割り当て、モニタリング、共有できます AWS リージョン AWS アカウント。また、特定のビジネスルールを使用して CIDRs を VPCs に自動的に割り当てるのにも役立ちます。

「Amazon VPC IP Address Manager Best Practices」、「Managing IP pools across VPCs and Regions using Amazon VPC IP Address Manager」、「IP Address Management for AWS Control Tower blog posts」を参照して、IP Addressing best practices and how to use IPAM to manage IP pools across VPCs AWS リージョン」、および「」を参照してください AWS Control Tower。

Well-Architected の実現状況の確認

AWS Well-Architected フレームワークは、クラウド内でのシステム構築に伴う意思決定の長所と短所を理解するのに役立ちます。このフレームワークの 6 つの柱により、信頼性、安全性、効率、費用対効果、持続可能性の高いシステムを設計および運用するための、アーキテクチャのベストプラクティスを確認できます。AWS マネジメントコンソール で無料で提供されている AWS Well-Architected Tool を使用すると、柱ごとに一連の質問に答えることで、これらのベストプラクティスに照らしてワークロードを評価できます。

クラウドアーキテクチャに関する専門的なガイダンスやベストプラクティス (リファレンスアーキテクチャのデプロイ、図、ホワイトペーパー) については、AWS アーキテクチャセンターを参照してください。

VPC から VPC への接続

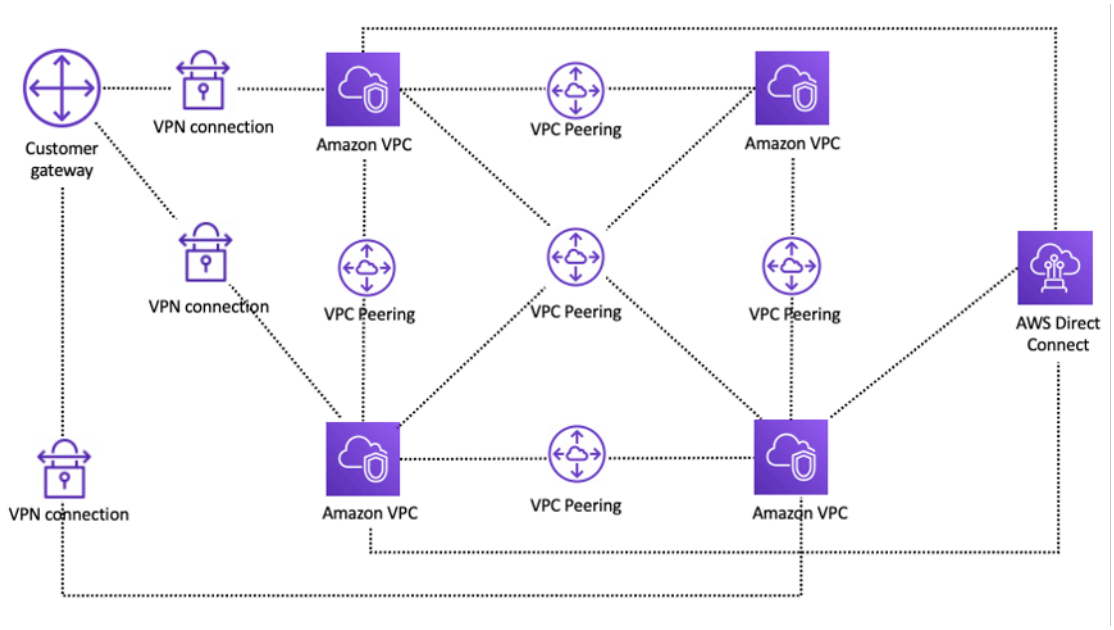
お客様は、2 つの異なる VPC 接続パターンを使用してマルチ VPC 環境をセットアップできます。多対多、またはハブアンドスポークです。many-to-manyアプローチでは、各 VPC 間のトラフィックは各 VPC 間で個別に管理されます。hub-and-spokeモデルでは、すべての VPC 間トラフィックは中央リソースを経由し、確立されたルールに基づいてトラフィックをルーティングします。

VPC ピアリング

2 つの VPCs を接続する最初の方法は、VPC ピアリングを使用することです。この設定では、接続により VPCs 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VPCs。VPCs は、ピアリング接続することもできます。アベイラビリティーゾーン内に留まる VPC ピアリング接続を介したデータ転送はすべて無料です。アベイラビリティーゾーンをまたぐ VPC ピアリング接続を介したすべてのデータ転送には、標準のリージョン内データ転送料金が課金されます。VPCs がリージョン間でピアリング接続されている場合、リージョン間の標準データ転送料金が適用されます。

VPC ピアリングはpoint-to-point接続であり、推移的な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 の間、および VPC A と VPC C の間に VPC ピアリング接続がある場合、VPC B のインスタンスは VPC A を経由して 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。

大規模な場合、数十または数百の VPCs がある場合、それらをピアリングと相互接続すると、数百または数千のピアリング接続のメッシュが発生する可能性があります。多数の接続は、管理とスケーリングが困難な場合があります。例えば、VPC が 100 個あり VPCs 、それらの間でフルメッシュピアリングを設定する場合、4,950 個のピアリング接続 [n(n-1)/2] が必要です。ここで、 n は VPCs。VPC あたり 125 のアクティブなピアリング接続の最大数があります。



VPC ピアリングを使用したネットワーク設定

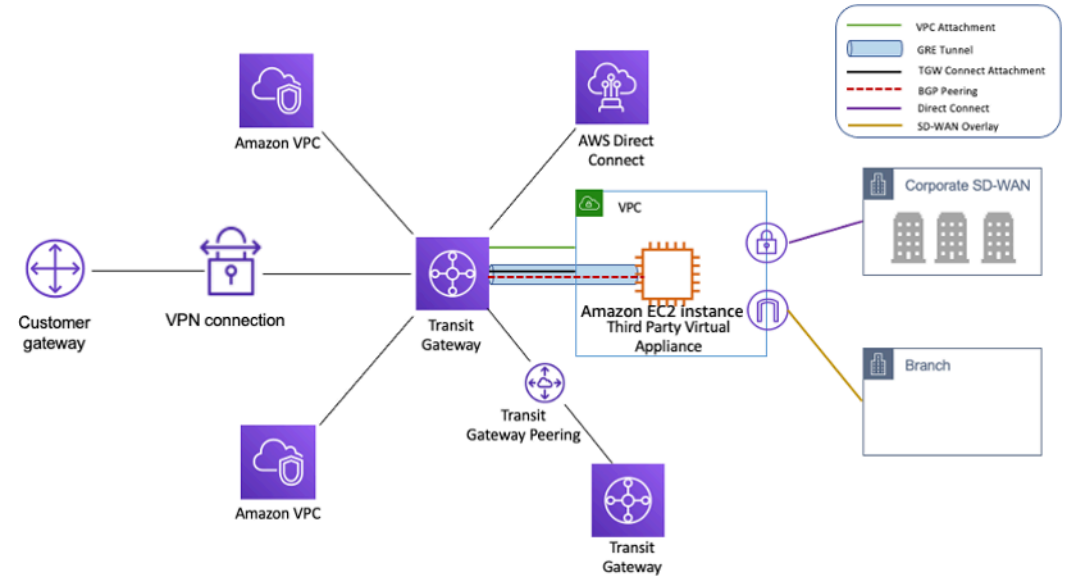
VPC ピアリングを使用している場合は、各 VPC にオンプレミス接続 (VPN または Direct Connect) を作成する必要があります。上の図に示すように、VPC 内のリソースは、ピア接続された VPC のハイブリッド接続を使用してオンプレミスに到達することはできません。

VPC ピアリングは、ある 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 VPCs の環境が制御および保護され、接続する VPCs の数が 10 未満である場合に最適です (各接続の個別の管理を可能にするため)。VPC ピアリングは、VPC 間接続の他のオプションと比較して、全体的なコストと総パフォーマンスが最も低くなります。

AWS Transit Gateway

AWS Transit Gateway は、サードパーティーVPCs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をフルマネージドサービスとして接続するためのハブアンドスポーク設計を提供します。VPN オーバーレイは不要で、高可用性とスケーラビリティ AWS を管理します。

Transit Gateway を使用すると、数千の VPCs。すべてのハイブリッド接続 (VPN および Direct Connect 接続) を単一のゲートウェイにアタッチし、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 (次の図を参照)。Transit Gateway は、ルートテーブルを使用して、接続されているすべてのスポークネットワーク間でトラフィックをルーティングする方法を制御します。このhub-and-spokeモデルは、VPCs が Transit Gateway インスタンスにのみ接続して接続されたネットワークにアクセスするため、管理を簡素化し、運用コストを削減します。



を使用したハブアンドスポーク設計 AWS Transit Gateway

Transit Gateway はリージョンリソースであり、同じ 内の数千の VPCs を接続できます AWS リージョン。ハイブリッド接続のために、1 つの Direct Connect 接続を介して複数のゲートウェイに接続できます。通常、特定のリージョン内のすべての VPC インスタンスを接続する Transit Gateway インスタンスを 1 つだけ使用し、必要に応じて Transit Gateway ルーティングテーブルを使用してそれらを分離できます。Transit Gateway は設計上高可用性であるため、高可用性のために追加の Transit Gateway は必要ありません。冗長性のために、各リージョンで 1 つのゲートウェイを使用します。ただし、複数のゲートウェイを作成して、設定ミスによる影響範囲を制限したり、コントロールプレーンオペレーションを分離したり、管理のease-of-useしたりすることは有効なケースです。

Transit Gateway ピアリングを使用すると、お客様は同じリージョンまたは複数のリージョン内で Transit Gateway インスタンスをピアリングし、それらの間でトラフィックをルーティングできます。VPC ピアリングと同じ基盤となるインフラストラクチャを使用するため、暗号化されます。詳細については、AWS Transit Gateway リージョン間ピアリングを使用したグローバルネットワークの構築」とAWS Transit Gateway がリージョン内ピアリングをサポートするようになりました」を参照してください。

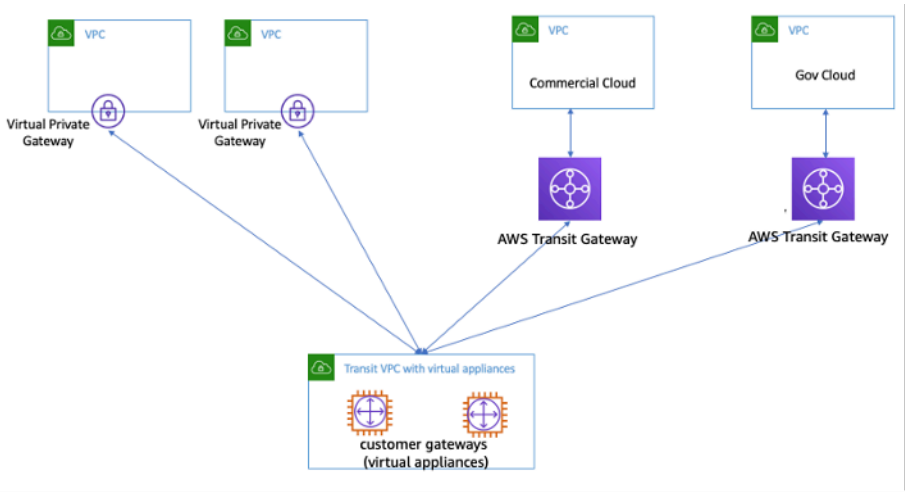
組織の Transit Gateway インスタンスを Network Services アカウントに配置します。これにより、ネットワークサービスアカウントを管理するネットワークエンジニアによる一元管理が可能になります。Resource Access Manager (RAM) AWS を使用して Transit Gateway インスタンスを共有し、同じリージョン内の AWS Organization 内の複数のアカウント間で VPCs を接続します。AWS RAM を使用すると AWS アカウント、 AWS リソースを AWS Organization 内または との間で簡単かつ安全に共有できます。詳細については、中央アカウントのブログ記事の「Transit Gateway への AWS Transit Gateway アタッチメントの自動化」を参照してください。

Transit Gateway では、Transit Gateway Connect を使用して SD-WAN インフラストラクチャと AWS 間の接続を確立することもできます。動的ルーティングにはボーダーゲートウェイプロトコル (BGP) で Transit Gateway Connect アタッチメントを使用し、高パフォーマンスには汎用ルーティングカプセル化 (GRE) トンネルプロトコルを使用して、Connect アタッチメントごとに最大 20 Gbps の合計帯域幅を提供します (Connect アタッチメントごとに最大 4 つの Transit Gateway Connect ピア) 。Transit Gateway Connect を使用すると、基盤となるトランスポートレイヤーとして VPC アタッチメントまたは アタッチメントを介して、オンプレミスの SD-WAN インフラストラクチャまたは Direct Connect クラウドで実行されている SD-WAN アプライアンスの両方を統合できます。リファレンスアーキテクチャと詳細な設定については、「Connect との SD-WAN AWS Transit Gateway 接続の簡素化」を参照してください。

トランジット VPC ソリューション

トランジット VPCs はVPCs 間接続用のハブアンドスポーク設計を導入することで、VPC ピアリングとは異なる方法で VPC 間の接続を作成できます。トランジット VPC ネットワークでは、1 つの中央 VPC (ハブ VPC) は、通常は IPsec 経由で BGP を利用する VPN 接続を介して他のすべての VPC (スポーク VPC) に接続します。中央 VPC には、VPN オーバーレイを使用して受信トラフィックを送信先にルーティングするソフトウェアアプライアンスを実行する Amazon Elastic Compute Cloud (Amazon EC2) インスタンスが含まれています。トランジット VPC ピアリングには次の利点があります。

- 推移的ルーティングはオーバーレイ VPN ネットワークを使用して有効になり、ハブアンドスポーク設計が可能になります。
- ハブトランジット VPC の EC2 インスタンスでサードパーティーベンダーソフトウェアを使用する場合、高度なセキュリティ (レイヤー 7 ファイアウォール/侵入防止システム (IPS)/侵入検知システム (IDS)) に関するベンダー機能を使用できます。オンプレミスで同じソフトウェアを使用している場合は、統一された運用/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。
- Transit VPC アーキテクチャは、一部のユースケースで必要な接続を可能にします。例えば、AWS GovCloud インスタンスと商用リージョン VPC または Transit Gateway インスタンスを Transit VPC に接続し、2 つのリージョン間の VPC 間接続を有効にすることができます。このオプションを検討するときは、セキュリティとコンプライアンスの要件を評価します。セキュリティを強化するために、このホワイトペーパーで後述する設計パターンを使用して一元的な検査モデルをデプロイできます。



仮想アプライアンスを備えたトランジット VPC

トランジット VPC には、インスタンスサイズ/ファミリーに基づいて EC2 でサードパーティーベンダーの仮想アプライアンスを実行する場合のコストの増加、VPN 接続あたりのスループットの制限 (VPN トンネルあたり最大 1.25 Gbps)、追加の設定、管理、および障害耐性のオーバーヘッド (お客様は、サードパーティーベンダーの仮想アプライアンスを実行している EC2 インスタンスの HA と冗長性を管理する責任があります) など、独自の課題があります。

VPC ピアリングと Transit VPC と Transit Gateway

表 1 — 接続の比較

条件	VPC ピアリング	トランジット VPC	Transit Gateway	PrivateLink	Cloud WAN	VPC Lattice
スコープ	リージョン/グローバル	リージョン別	リージョン別	リージョン別	グローバル	リージョン別
アーキテクチャ	フルメッシュ	VPN hub-and-spoke	アタッチメントベースのhub-and-spoke	プロバイダーまたはコンシューマーモデル	添付ファイルベース、マルチリージョン	アプリ間の接続
スケール	125 のアクティブなピア/VPC	仮想ルーター/EC2	リージョンあたり 5,000 個の	制限なし	コアネットワークあたり 5000 個	サービスあたり 500

条件	VPC ピアリング	トランジット VPC	Transit Gateway	PrivateLink	Cloud WAN	VPC Lattice
		によって異なります	添付ファイル		のアタッチメント	VPC の関連付け
セグメンテーション	セキュリティグループ	カスタマーマネージド	Transit Gateway ルートテーブル	セグメンテーションなし	セグメント	サービスおよびサービスネットワークポリシー
レイテンシー	低	VPN 暗号化のオーバーヘッドによる追加	追加の Transit Gateway ホップ	トラフィックは AWS バックボーンにとどまるため、お客様はテストする必要があります	Transit Gateway と同じデータプレーンを使用します	トラフィックは AWS バックボーンにとどまるため、お客様はテストする必要があります
帯域幅制限	インスタンスあたりの制限、集計制限なし	サイズ/ファミリーに基づく EC2 インスタンスの帯域幅制限の対象	最大 100 Gbps (バースト)/アタッチメント	アベイラビリティーゾーンあたり 10 Gbps、自動的に 100 Gbps までスケールアップ	最大 100 Gbps (バースト)/アタッチメント	アベイラビリティーゾーンあたり 10 Gbps

条件	VPC ピアリング	トランジット VPC	Transit Gateway	PrivateLink	Cloud WAN	VPC Lattice
[可視性]	VPC フローログ	VPC フローログと CloudWatch メトリクス	Transit Gateway Network Manager、VPC フローログ、CloudWatch メトリクス	CloudWatch メトリクス	Network Manager、VPC フローログ、CloudWatch メトリクス	CloudWatch アクセスログ
セキュリティグループ 相互参照	サポート	サポートされません	サポートされません	サポートされません	サポートされません	該当しない
IPv6 サポート	サポート	仮想アプライアンスによって異なります	サポート	サポート対象	サポート対象	サポート

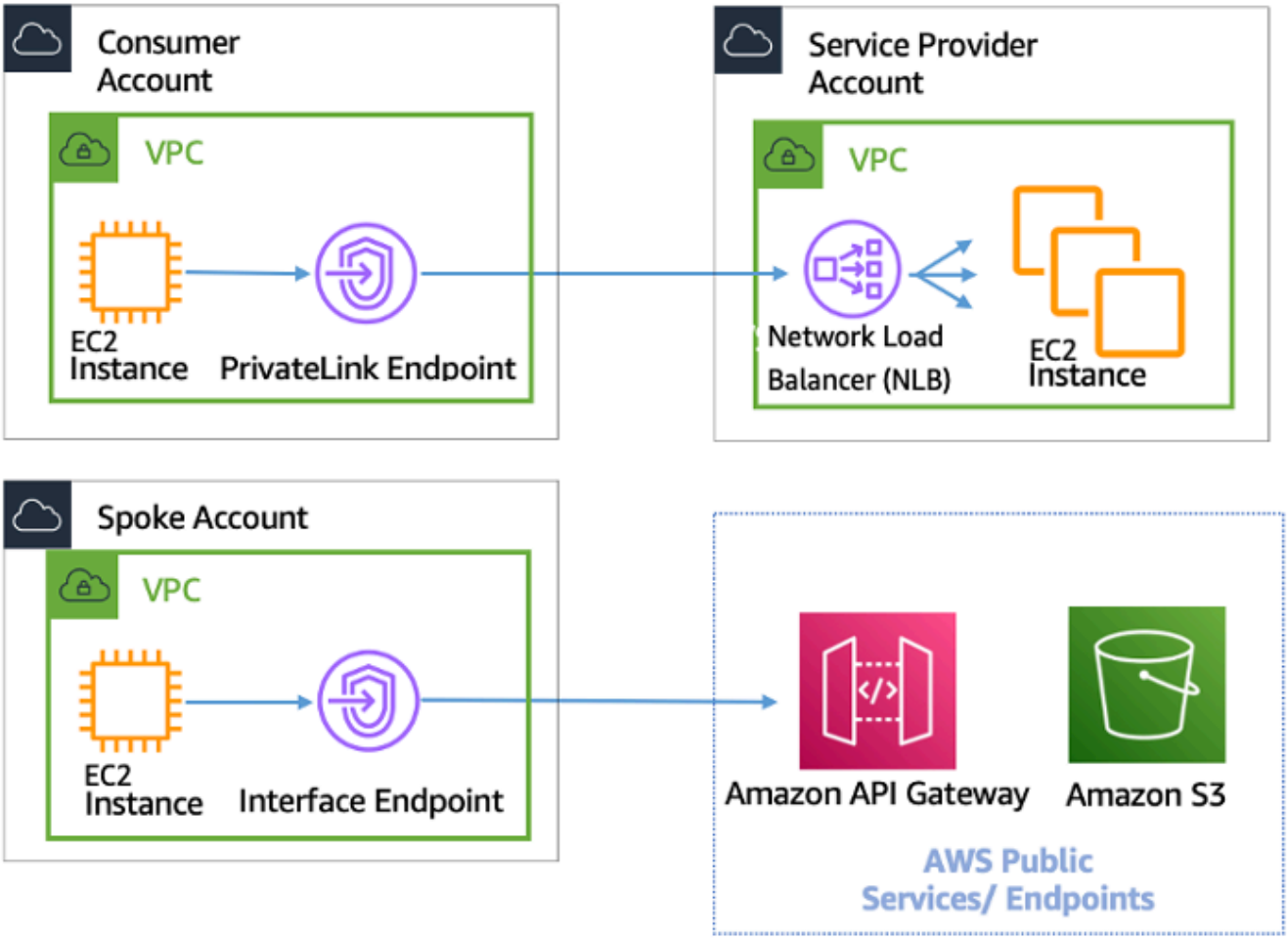
AWS PrivateLink

AWS PrivateLink は、トラフィックをパブリックインターネットに公開することなく、VPCs、AWS サービス、オンプレミスネットワーク間のプライベート接続を提供します。を利用したインターフェイス VPC エンドポイントを使用すると AWS PrivateLink、さまざまなアカウント AWS や VPCs 間で や他の サービスに簡単に接続できるため、ネットワークアーキテクチャが大幅に簡素化されます。これにより、コンシューマー VPC のみがサービスプロバイダー VPC への接続を開始する AWS リージョン 方法で、ある VPCs (サービスプロバイダー) に存在するサービス/アプリケーションを内の他の VPCs (コンシューマー) にプライベートに公開することができます。例としては、プライベートアプリケーションがサービスプロバイダー APIs。

を使用するには AWS PrivateLink、VPC でアプリケーションの Network Load Balancer を作成し、そ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は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、コンシュー

マーサブネットに Elastic Network Interface (ENI) が作成され、サービス宛てのトラフィックのエントリポイントとして機能するプライベート IP アドレスが割り当てられます。コンシューマーとサービスは、同じ VPC に存在する必要はありません。VPC が異なる場合、コンシューマーとサービスプロバイダーVPCs は重複する IP アドレス範囲を持つことができます。次の図に示すように、インターフェイス VPC エンドポイントを作成して他の VPCs のサービスにアクセスすることに加えて、インターフェイス VPC エンドポイントを作成して 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できます。

Application Load Balancer (ALB) を NLB のターゲットとして、ALB の高度なルーティング機能を と組み合わせることができるようになりました AWS PrivateLink。リファレンスアーキテクチャと詳細な設定については、Network Application Load Balancer の Application Load Balancer タイプのターゲットグループを参照してください。



AWS PrivateLink 他の VPCsおよび AWS サービスへの接続用

Transit Gateway、VPC ピアリング、 のいずれかの選択 AWS PrivateLink は、接続によって異なります。

- AWS PrivateLink — 1 つ以上のコンシューマー VPCs に、サービスプロバイダー VPC または特定の AWS サービス内の特定のサービスまたはインスタンスセットへの単方向アクセスを許可する AWS PrivateLink クライアント/サーバーが設定されている場合に使用します。コンシューマー VPC でアクセス権を持つクライアントのみが、サービスプロバイダー VPC またはサービス内の AWS サービスへの接続を開始できます。これは、2 つの VPCsを持つ場合にも適しています。 は、 がサービスプロバイダーとの IP 競合がないことを保証する方法でクライアント VPC 内の ENIs AWS PrivateLink を使用するためです。VPC ピアリング、VPN、Transit Gateway、Cloud WAN、および を介して AWS PrivateLink エンドポイントにアクセスできます AWS Direct Connect。
- VPC ピアリングと Transit Gateway — VPC 間のレイヤー 3 IP 接続を有効にする場合はVPCs。

  アーキテクチャには、さまざまなユースケースに対応するために、これらのテクノロジーが混在しています。これらのサービスはすべて、相互に組み合わせて運用できます。例えば、API スタイルのクライアント/サーバー接続 AWS PrivateLink の処理、 リージョン内でプレイスメントグループがまだ望ましい直接接続要件を処理するための VPC ピアリング、大規模な VPCs の接続を簡素化するための Transit Gateway、ハイブリッド接続のエッジ統合などです。

VPC 共有

VPCs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く、アカウントレベルのユーザーとアクセス許可が である必要がある場合に役立ちます。共有 VPC では、複数の AWS アカウントが、共有され一元管理された Amazon VPCs 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 VPCs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、ネットワークアクセスコントロールリスト (NACLs)、またはサブネット間のファイアウォールを使用して管理されます。

VPC 共有の利点：

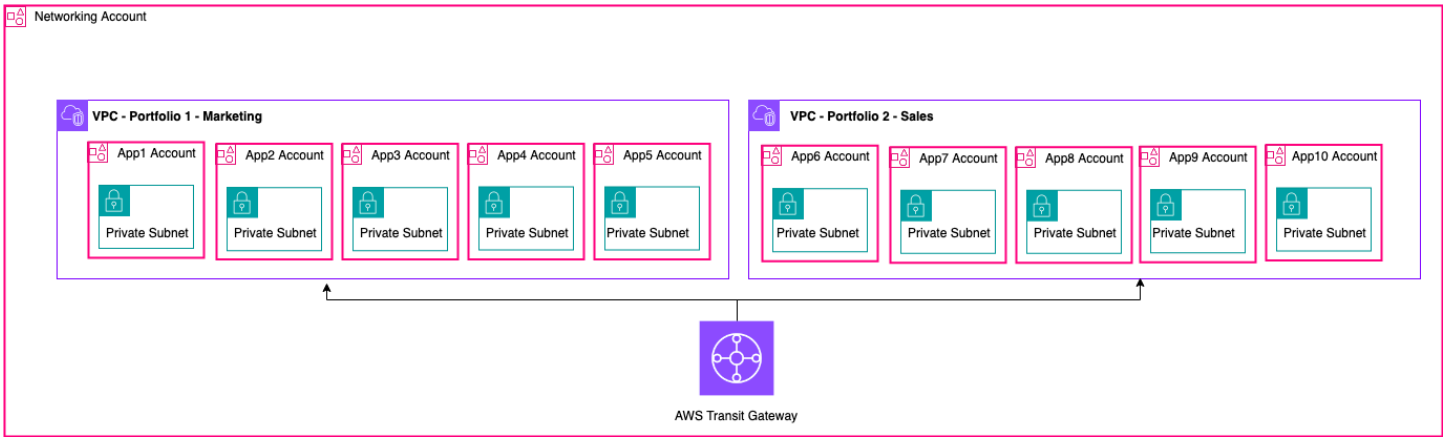
- 設計の簡素化 — VPC 間の接続を複雑にしない
- 管理対象 VPCsの削減

- ネットワークチームとアプリケーション所有者間の職務の分離
- IPv4 アドレス使用率の向上
- コストの削減 — 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のデータ転送料金は発生しません

> **Note**
>
> サブネットを複数のアカウントと共有する場合、参加者は IP スペースとネットワークリソースを共有しているため、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できます。参加者ごとに 1 つのサブネットにより、ネットワーク ACL はセキュリティグループに加えてネットワーク分離を提供できます。

ほとんどのカスタマーアーキテクチャには複数の VPCsが含まれ、その多くは 2 つ以上のアカウントと共有されます。Transit Gateway と VPC ピアリングを使用して、共有 VPCsを接続できます。例えば、10 個のアプリケーションがあるとします。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には、「マーケティング」のアプリケーション 1～5 と「セールス」のアプリケーション 6～10 という同様のネットワーク要件があります) 。

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 VPCs) を持つことができ、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。アプリ所有者は、それぞれの共有 VPC にアプリをデプロイします (この場合は、NACLs を使用したネットワークルートのセグメント化と分離のための異なるサブネット) 。2 つの共有 VPCs は Transit Gateway を介して接続されます。この設定では、次の図に示すように、10 個の VPCs を 2 つの VPC に接続する必要がなくなります。

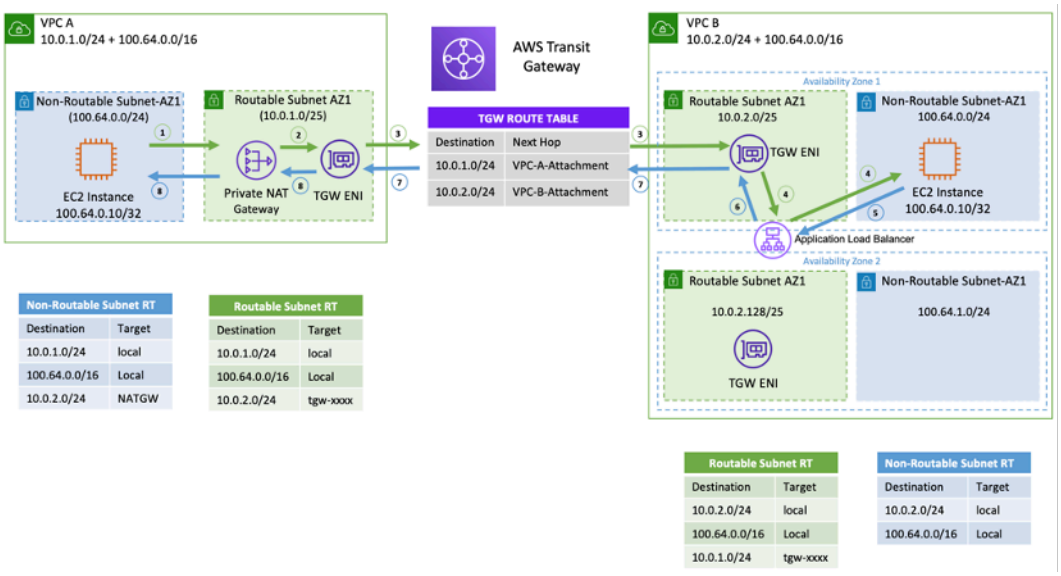


セットアップの例 – 共有 VPC

> **Note**
>
> VPC 共有参加者は、共有サブネットにすべての AWS リソースを作成することはできません。詳細については、VPC 共有ドキュメントの「制限」セクションを参照してください。VPC 共有の主な考慮事項とベストプラクティスの詳細については、ブログ記事「VPC 共有: 重要な考慮事項とベストプラクティス」を参照してください。

プライベート NAT ゲートウェイ

チームは多くの場合、独立して作業し、プロジェクト用に新しい VPC を作成することがあります。この VPC には、クラスレスドメイン間ルーティング (CIDR) ブロックが重複している可能性があります。統合のために、重複する CIDRs、VPC ピアリングや Transit Gateway などの機能では実現できません。プライベート NAT ゲートウェイはこのユースケースに役立ちます。プライベート NAT ゲートウェイは、一意のプライベート IP アドレスを使用して、重複する送信元 IP アドレスの送信元 NAT を実行し、ELB は重複する送信先 IP アドレスの送信先 NAT を実行します。Transit Gateway または仮想プライベートゲートウェイを使用して、プライベート NAT ゲートウェイから他の VPCs またはオンプレミスネットワークにトラフィックをルーティングできます。

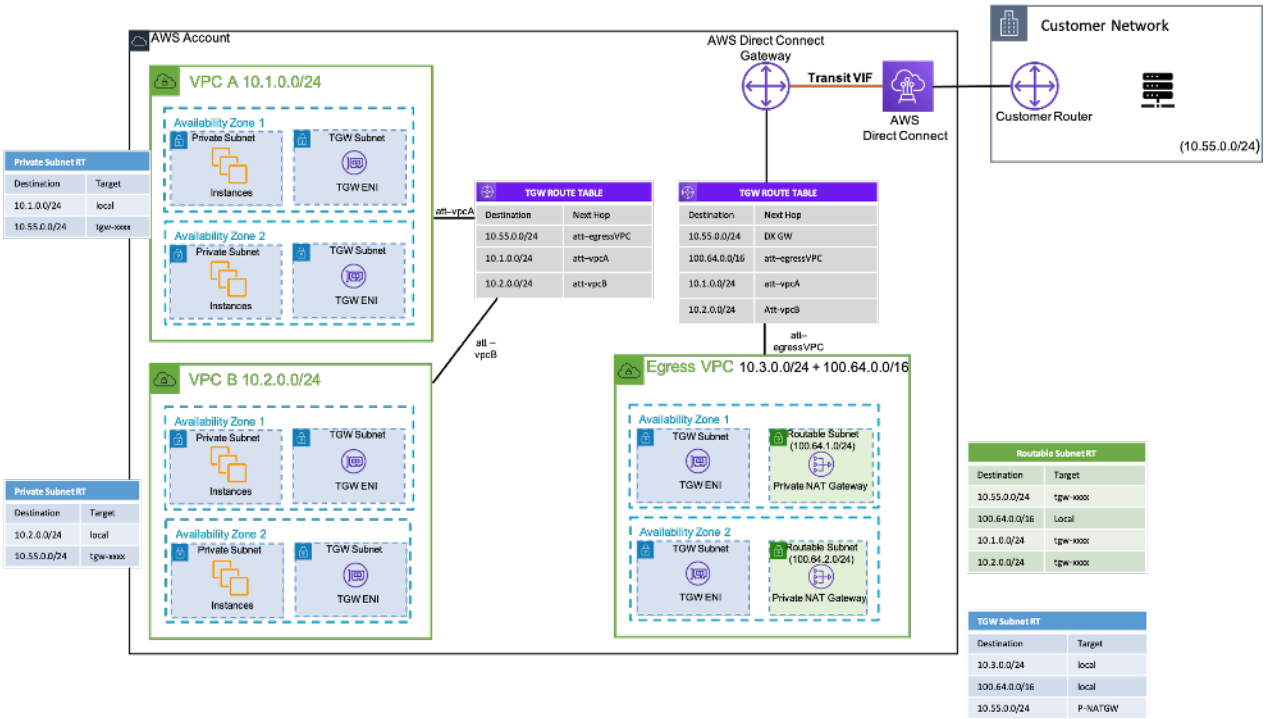


セットアップ例 – プライベート NAT ゲートウェイ

上の図は、VPC A と B の 2 つのルーティング不可能な (重複CIDRs、100.64.0.0/16) サブネットを示しています。それらの間の接続を確立するには、VPC A 10.0.1.0/24と B にそれぞれ、重複

しない/ルーティング可能なセカンダリ CIDRs (ルーティング可能なサブネット、10.0.2.0/24) を追加できます。ルーティング可能な CIDRs は、IP 割り当てを担当するネットワーク管理チームによって割り当てられる必要があります。プライベート NAT ゲートウェイは、IP アドレスが の VPC A のルーティング可能なサブネットに追加されます10.0.1.125。プライベート NAT ゲートウェイは、VPC A (100.64.0.10) のルーティング不可能なサブネットのインスタンスからのリクエストに対して10.0.1.125、プライベート NAT ゲートウェイの ENI である としてソースネットワークアドレス変換を実行します。これで、トラフィックは、 のターゲットを持つ VPC B () の Application Load Balancer (ALB10.0.2.10) に割り当てられたルーティング可能な IP アドレスを指すことができます100.64.0.10。トラフィックは Transit Gateway を介してルーティングされます。リターントラフィックは、プライベート NAT ゲートウェイによって元の Amazon EC2 インスタンスに接続をリクエストして処理されます。

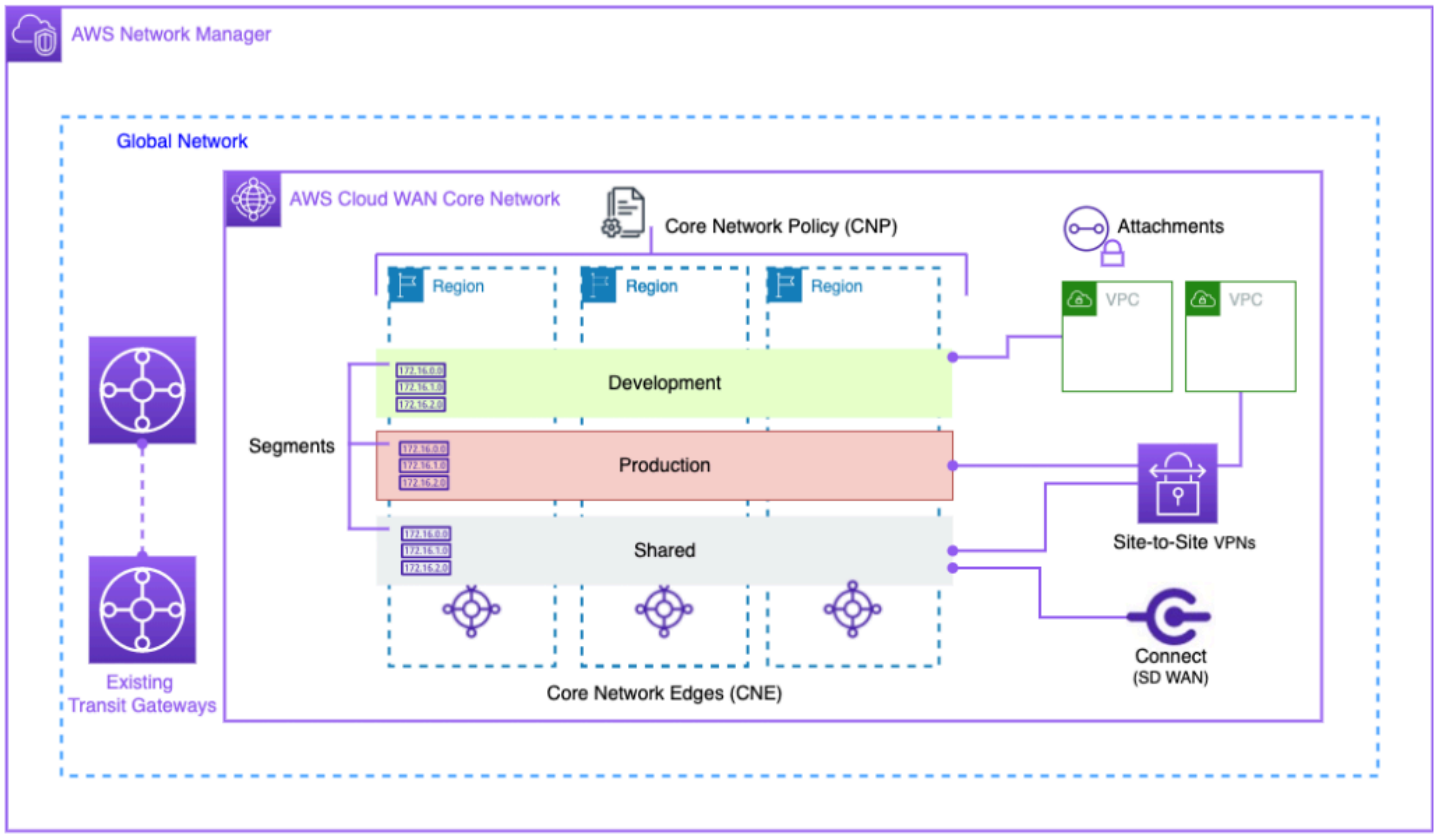
プライベート NAT ゲートウェイは、オンプレミスネットワークが承認された IPs へのアクセスを制限するときにも使用できます。少数のお客様のオンプレミスネットワークは、お客様が所有する承認された IPs の限られた連続したブロックを介してのみ、プライベートネットワーク (IGW なし) とのみ通信することをコンプライアンスで要求されます。各インスタンスに ブロックから個別の IP を割り当てる代わりに、プライベート NAT ゲートウェイを使用して、許可リストに登録された各 IP の背後にある AWS VPCs で大規模なワークロードを実行できます。詳細については、「プライベート NAT ソリューションによるプライベート IP の枯渇を解決する方法」ブログ記事を参照してください。



セットアップ例 – プライベート NAT ゲートウェイを使用してオンプレミスネットワークに承認された IPs を提供する方法

AWS クラウド WAN

AWS Cloud WAN は、以前はトランジットゲートウェイ、VPC ピアリング、IPSEC VPN トンネルでできたネットワークを接続する新しい方法です。以前は、1 つ以上の VPCs を設定し、前の方法のいずれかと併せて接続し、IPSEC VPN Direct Connect または を使用してオンプレミスネットワークに接続していました。ネットワークとセキュリティ体制のコンストラクトは 1 つの場所で定義し、ネットワークは別の場所で定義します。クラウド WAN を使用すると、これらのコンストラクトをすべて 1 か所に一元化できます。ポリシーにより、ネットワークをセグメント化して誰が誰と話せるかを判断し、これらのセグメントを介して本稼働トラフィックを開発ワークロードやテストワークロード、またはオンプレミスネットワークから分離できます。



クラウド WAN ブロック図

Network Manager のユーザーインターフェイスと APIs を使用してグローバル AWS ネットワークを管理します。グローバルネットワークは、すべてのネットワークオブジェクトのルートレベルのコンテナです。コアネットワークは、AWS によって管理されるグローバルネットワークの一部です。コアネットワークポリシー (CNP) は、コアネットワークのあらゆる側面を定義する単一のバージョン

ングポリシードキュメントです。アタッチメントは、コアネットワークに追加する接続またはリソースです。コアネットワークエッジ (CNE) は、 ポリシーに準拠するアタッチメントのローカル接続ポイントです。ネットワークセグメントはルーティングドメインであり、デフォルトではセグメント内での通信のみを許可します。

CloudWAN を使用するには：

1. AWS Network Manager で、グローバルネットワークと関連するコアネットワークを作成します。
2. セグメントにアタッチするセグメント、ASN 範囲、 AWS リージョン タグを定義する CNP を作成します。
3. ネットワークポリシーを適用します。
4. リソースアクセスマネージャーを使用して、コアネットワークをユーザー、アカウント、または組織と共有します。
5. 添付ファイルを作成してタグ付けします。
6. アタッチされた VPCsのルートを更新して、コアネットワークを含めます。

クラウド WAN は、AWS インフラストラクチャをグローバルに接続するプロセスを簡素化するように設計されています。これにより、一元的なアクセス許可ポリシーでトラフィックをセグメント化し、会社の場所で既存のインフラストラクチャを使用できます。Cloud WAN は、VPCs、SD-WANs、クライアント VPNs、ファイアウォール、VPNs、データセンターリソースも接続して Cloud WAN に接続します。詳細については、AWS Cloud WAN ブログ記事を参照してください。

AWS Cloud WAN は、クラウド環境とオンプレミス環境を接続する統合ネットワークを可能にします。組織は、次世代ファイアウォール (NGFWsと侵入防止システム (IPSs) をセキュリティに使用します。AWS Cloud WAN と Transit Gateway の移行と相互運用性のパターンに関するブログ記事では、単一リージョンネットワークとマルチリージョンネットワークを含む Cloud WAN ネットワーク内のアウトバウンドネットワークトラフィックを一元的に管理および検査するためのアーキテクチャパターンについて説明し、ルートテーブルを設定します。これらのアーキテクチャにより、安全なクラウド環境を維持しながら、データとアプリケーションを安全に維持できます。

Cloud WAN の詳細については、AWS Cloud WAN ブログ記事の「集中型アウトバウンド検査アーキテクチャ」を参照してください。

Amazon VPC Lattice

Amazon VPC Lattice は、フルマネージド型のアプリケーションネットワークサービスであり、さまざまなアカウントや仮想プライベートクラウドで サービスを接続、モニタリング、保護するために

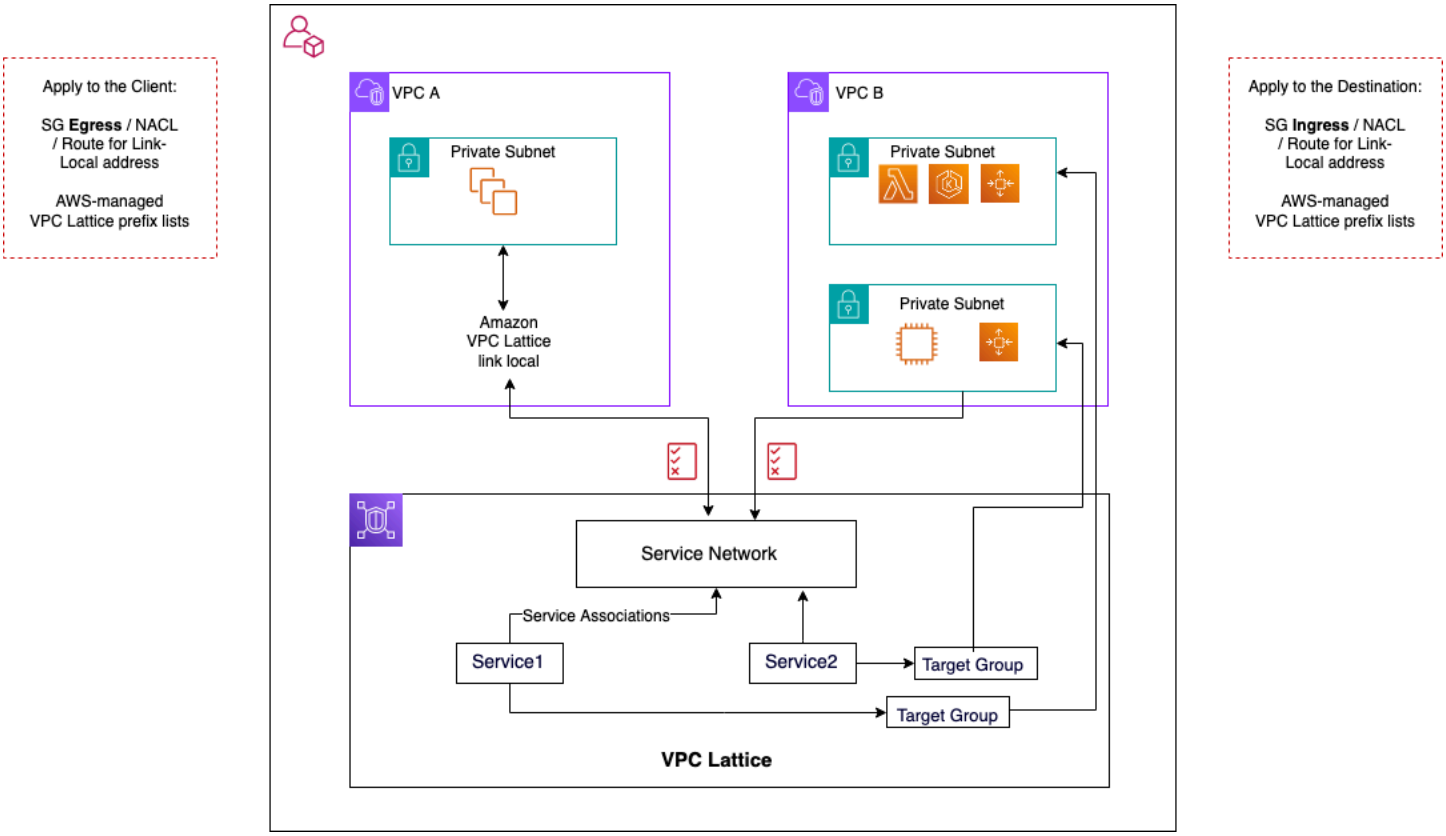
使用されます。VPC Lattice は、サービスを論理的な境界内で相互接続するのに役立つため、サービスを効率的に管理および検出できます。

VPC Lattice コンポーネントは以下で構成されます。

- サービス - インスタンス、コンテナ、または Lambda 関数で実行されるアプリケーションの単位であり、リスナー、ルール、ターゲットグループで構成されます。
- サービスネットワーク - これは、サービスの検出と接続を自動的に実装し、サービスのコレクションに共通のアクセスポリシーとオブザーバビリティポリシーを適用するために使用される論理的な境界です。
- 認証ポリシー - リクエストレベルの認証とコンテキスト固有の認可をサポートするために、サービスネットワークまたは個々のサービスに関連付けることができる IAM リソースポリシー。
- サービスディレクトリ - 所有しているサービス、または AWS Resource Access Manager を通じて共有されているサービスを一元的に表示します。

VPC Lattice の使用手順：

1. サービスネットワークを作成します。サービスネットワークは通常、ネットワーク管理者がフルアクセスを持つネットワークアカウントにあります。サービスネットワークは、組織内の複数のアカウント間で共有できます。共有は、個々のサービスまたはサービスアカウント全体で実行できます。
2. VPCs をサービスネットワークにアタッチして、各 VPC のアプリケーションネットワークを有効にし、異なるサービスがネットワークに登録されている他のサービスの消費を開始できるようにします。セキュリティグループは、トラフィックを制御するために適用されます。
3. デベロッパーは、サービスディレクトリに入力され、サービスネットワークに登録されるサービスを定義します。VPC Lattice には、設定されたすべてのサービスのアドレス帳が含まれています。デベロッパーは、ブルー/グリーンデプロイを使用するようにルーティングポリシーを定義することもできます。セキュリティは、認証および認可ポリシーが定義されているサービスネットワークレベルと、IAM によるアクセスポリシーが実装されているサービスレベルで管理されます。



VPC Lattice 通信フロー

詳細については、VPC Lattice ユーザーガイドを参照してください。

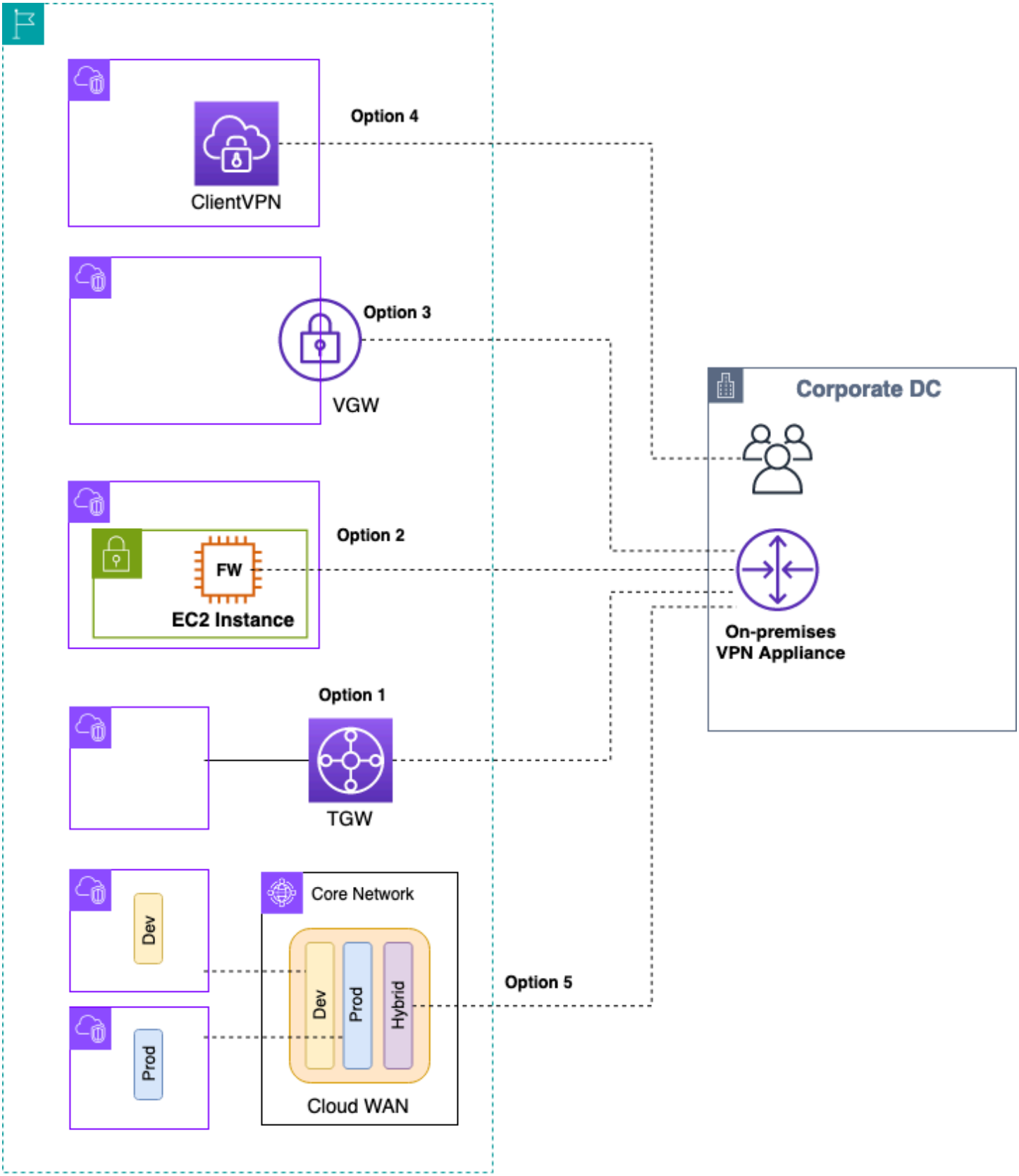
ハイブリッド接続

このセクションでは、クラウドリソースをオンプレミスデータセンターに安全に接続する方法について説明します。ハイブリッド接続を有効にするには、次の 3 つの方法があります。

- One-to-one の接続 — この設定では、VPC ごとに VPN 接続や Direct Connect プライベート VIF が作成されます。これは、Virtual Private Gateway (VGW) を使用して実現されます。このオプションは少数の VPCs に最適ですが、お客様が VPCs をスケールすると、VPC ごとのハイブリッド接続の管理が難しくなる可能性があります。
- エッジ統合 — この設定では、お客様は複数の VPCs。すべての VPCsこれらのハイブリッド接続を共有します。これは、 AWS Transit Gateway と Direct Connect ゲートウェイを使用して実現されます。
- フルメッシュハイブリッド統合 — この設定では、お客様は CloudWAN を使用して複数の VPCsを 1 つのエンドポイントに統合します AWS Transit Gateway。これは、コードで表される 1 つ以上の AWS アカウントでのネットワーキングに対するポリシーベースの完全なアプローチです。現時点では、エッジ接続 Direct Connect に を使用するには、Transit Gateway を CloudWAN にピアリングする必要があります。

VPN

AWS への VPN をセットアップするには、さまざまな方法があります。



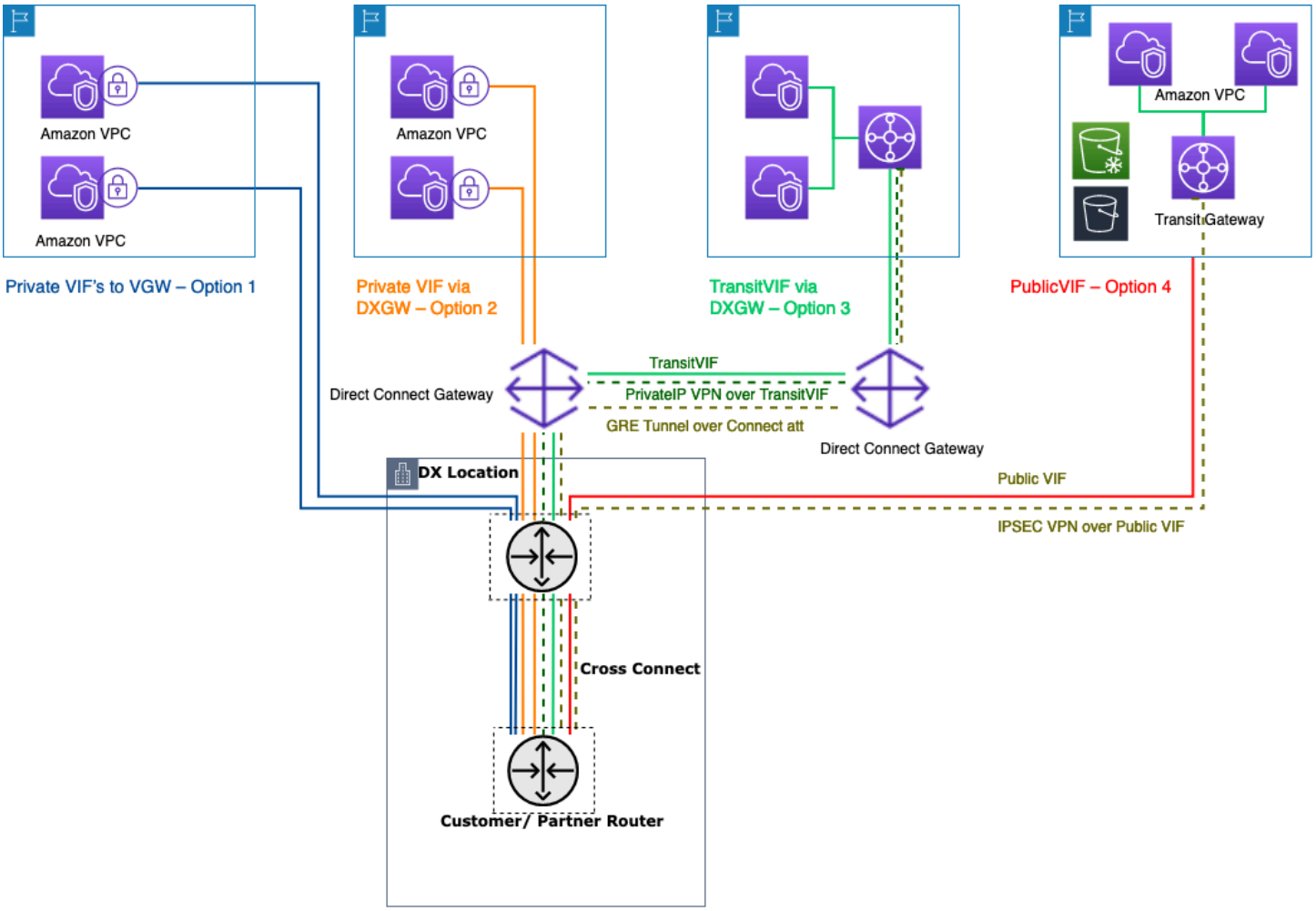
Site-to-Site VPN オプション

- オプション 1: Transit Gateway で VPN 接続を統合する — このオプションは、Transit Gateway の Transit Gateway VPN アタッチメントを活用します。Transit Gateway は、site-to-siteの IPsec ターミネーション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た VPCs 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ます。Transit Gateway は、VPN アタッチメントで等コストマルチパス (ECMP) もサポートしています。各 VPN 接続のスループットは、トンネルあたり最大 1.25 Gbps です。ECMP を有効にすると、VPN 接続全体でスループットを集約できるため、 はデフォルトの最大制限である 1.25 Gbps を超えてスケールできます。このオプションでは、Transit Gateway の料金とSite-to-Site VPN 料金に対して料金が発生します。AWS では、このオプションを 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 Transit Gateway を使用した VPN スループットのスケーリングに関するブログ記事を参照してください。
- オプション 2: Amazon EC2 インスタンスで VPN を終了する — このオプションは、エッジケースで特定のベンダーソフトウェア機能セット (Cisco DMVPN や汎用ルーティングカプセル化 (GRE) など) が必要な場合や、さまざまな VPN デプロイ間で運用の一貫性が必要な場合に、お客様が活用します。エッジ統合にはトランジット VPC 設計を使用できますが、トランジット VPC に関する VPC から VPC への接続セクションの重要な考慮事項はすべてハイブリッド VPN 接続に適用できることに注意してください。高可用性の管理はお客様の責任であり、EC2 インスタンスとベンダーソフトウェアのライセンスおよびサポート費用のお支払いとなります。
- オプション 3: 仮想プライベートゲートウェイ (VGW) で VPN を終了する — この AWS Site-to-Site VPN サービスオプションを使用すると、VPC ごとに 1 つの VPN 接続 (冗長 VPN トンネルのペアで構成される) を作成する 1 one-to-one の接続設計が可能になります。 これは AWS への VPN 接続を開始するのに最適な方法ですが、VPCs の数をスケールすると、VPN 接続の数の増加を管理することが難しくなる可能性があります。したがって、Transit Gateway を活用したエッジ統合設計は、最終的にはより良い選択肢になります。VGW への VPN スループットはトンネルあたり 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。料金の観点から見ると、AWS VPN 料金に対してのみお支払いいただきます。VGW の実行には料金はかかりません。詳細については、Site-to-Site VPN 仮想プライベートゲートウェイのSite-to-Site VPN「料金表」および「」を参照してください。
- オプション 4: クライアント VPN エンドポイントで VPN 接続を終了する — AWS Client VPN は、オンプレミスネットワーク内の AWS リソースとリソースに安全にアクセスできるマネージドクライアントベースの VPN サービスです。クライアント VPN では、OpenVPN または AWS が提供する VPN クライアントを使用して、任意の場所からリソースにアクセスできます。クライアント VPN エンドポイントを設定することで、クライアントとユーザーは接続して Transport Layer Security (TLS) VPN 接続を確立できます。詳細については、AWS Client VPN のドキュメントを参照してください。

- オプション 5: AWS クラウド WAN で VPN 接続を統合する — このオプションはこのリストの最初のオプションに似ていますが、CloudWAN ファブリックを使用して、ネットワークポリシードキュメントを介してプログラムで VPN 接続を設定します。

Direct Connect

インターネット経由の VPN は開始するための優れたオプションですが、本番環境のトラフィックではインターネット接続の信頼性が損なわれる可能性があります。この信頼性が低いため、多くのお客様は を選択しますDirect Connect。 Direct Connect は、インターネットを使用して AWS に接続する代わりに使用できるネットワークサービスです。を使用すると Direct Connect、以前はインターネット経由で転送されていたはずのデータが、施設と AWS 間のプライベートネットワーク接続を介して配信されます。多くの場合、プライベートネットワーク接続は、インターネットベースの接続よりもコストを削減し、帯域幅を増やし、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。Direct Connect を使用して VPCs に接続する方法はいくつかあります。



を使用してオンプレミスのデータセンターを接続する方法 Direct Connect

- オプション 1: 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 VIFs を作成し、最大 50 VPCs に接続できます (1 つの VIF は 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。この設定での接続は、Direct Connect ロケーションが所在する AWS リージョンに制限されます。VIF と VPC の one-to-one のマッピング (グローバルアクセスの欠如) により、これはランディングゾーンの VPCs にアクセスする最も望ましくない方法になります。
- オプション 2: 複数の VGWs 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 にアタッチされます) — 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す。Direct Connect ゲートウェイは、任意の リージョンに作成し、GovCloud (中国を除く) を含む他のすべての リージョンからアクセスできます。Direct Connect Gateway は、1 つのプライベート VIF を介して、任意の AWS アカウントで最大 20 個の VPCs に (VGWs 経由で) グローバルに接続できます。これは、ランディングゾーンが少数の VPCs (10 個以下の VPCs) 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です。Direct Connect 接続ごとに、Direct Connect Gateway ごとに 1 つの BGP ピアリングセッションがあります。Direct Connect ゲートウェイは、北/南トラフィックフロー専用であり、VPC-to-VPCは許可されません。詳細については、 Direct Connect ドキュメントの「仮想プライベートゲートウェイの関連付け」を参照してください。このオプションでは、Direct Connect ロケーションが置かれている AWS リージョンへの接続は制限されません。 Direct Connect ゲートウェイは北/南トラフィックフロー専用であり、VPC-to-VPCは許可されません。このルールの例外は、アタッチされた VPCs 間でスーパーネットがアドバタイズされる場合です。 VGWs Direct Connect この場合、VPCs は Direct Connect エンドポイントを介して相互に通信できます。詳細については、Direct Connect ゲートウェイのドキュメントを参照してください。
- オプション 3: 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 — Transit VIF を使用して、Transit Gateway インスタンスを Direct Connect ゲートウェイに関連付けることができます。 は、すべてのポート速度で Transit Gateway への接続をサポートする Direct Connect ようになり、高速接続 (1Gbps 以上) が必要ない場合に、Transit Gateway ユーザーにコスト効率の高い選択肢を提供します。これにより、Transit Gateway に接続する速度が 50、100、200、300、400、500 Mbps で Direct Connect を使用できます。Transit VIF を使用すると、単一のトランジット VIF および BGP ピア接続を介して、異なる AWS リージョンと AWS アカウント間で、ゲートウェイごとに最大 6 つの Transit Gateway インスタンス Direct Connect (数千の VPCs に接続できます) にオンプレミスデータセンターを接続できます。これは、複数の VPCs を大規模に接続するためのオプションの中で最も簡単な設定ですが、Transit Gateway のクォータに注意する必要があります。注意すべき重要な制限の 1 つは、トランジット VIF 経由で Transit Gateway からオンプレミスルーターにアドバタイズできるプレフィックスは

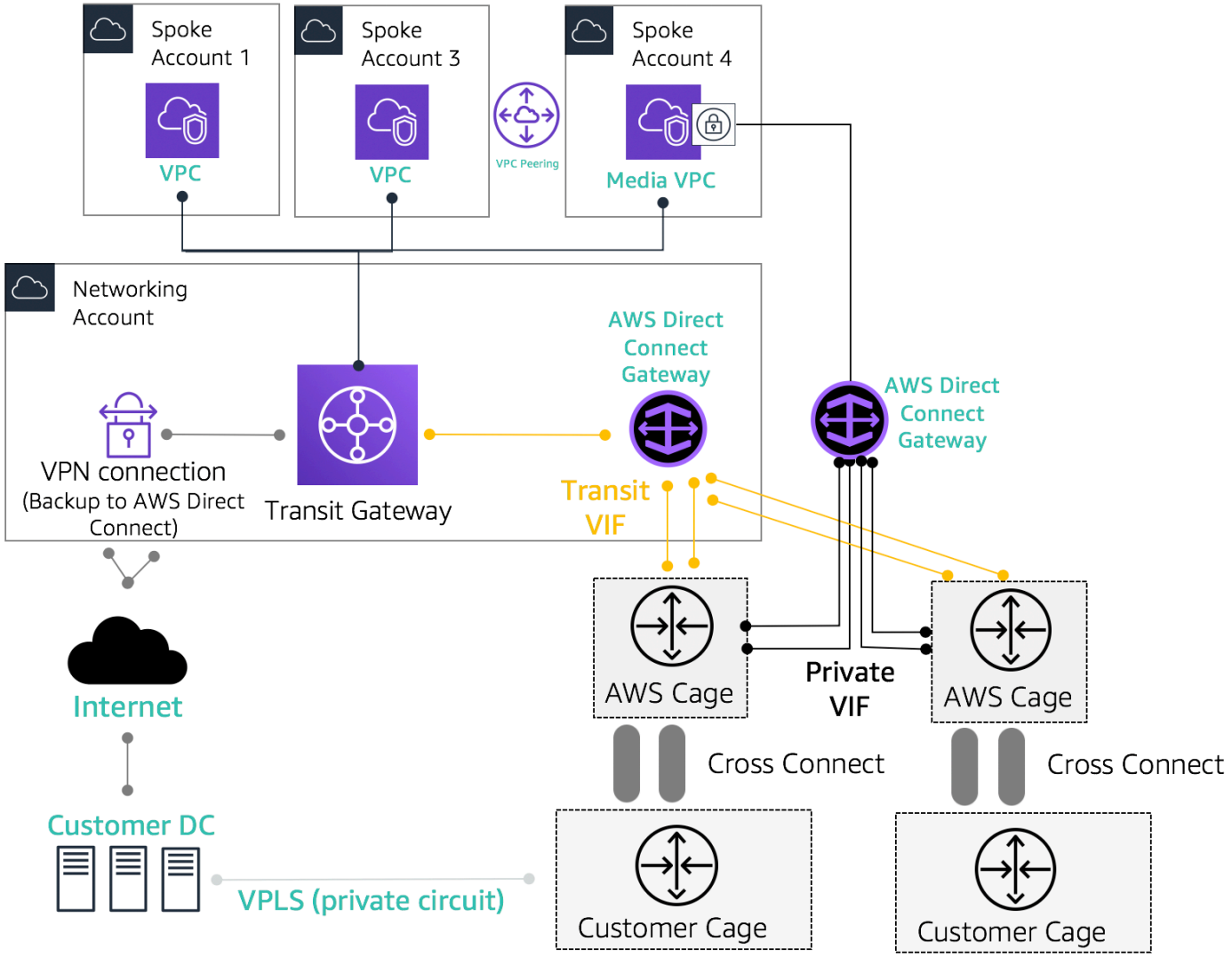
200 個のみです。上記のオプションでは、Direct Connect の料金がかかります。このオプションでは、Transit Gateway アタッチメントとデータ処理料金も支払います。詳細については、Direct Connect の Transit Gateway Associations ドキュメントを参照してください。

- オプション 4: 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 VIF 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 VPN エンドポイントの 2 つのパブリック IP アドレスを取得します。これらのパブリック IPsには、パブリック VIF 経由でアクセスできます。パブリック VIF では、必要な数の Transit Gateway インスタンスへの 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には (VPN 終了エンドポイントへのトラフィックのみを許可するなど)、ファイアウォールのオンプレミス施設を使用することをお勧めします。このオプションは、ネットワークレイヤーで Direct Connect を暗号化するために使用できます。
- オプション 5: プライベート IP VPN Direct Connect を使用して 経由で Transit Gateway への VPN 接続を作成する — プライベート IP VPN は、お客様がプライベート IP アドレスを使用して Direct Connect 経由で AWS Site-to-Site VPN 接続をデプロイできるようにする機能です。この機能を使用すると、パブリック IP アドレスを必要とせずに Direct Connect 接続を介してオンプレミスネットワークと AWS 間のトラフィックを暗号化できるため、セキュリティとネットワークプライバシーを同時に強化できます。プライベート IP VPN は Transit VIFs 上にデプロイされるため、Transit Gateway を使用して、顧客の VPCs とオンプレミスネットワークへの接続をより安全でプライベート、スケーラブルな方法で一元管理できます。
- オプション 6: Transit VIF 経由で Transit Gateway への GRE トンネルを作成する – Transit Gateway Connect アタッチメントタイプは GRE をサポートします。Transit Gateway Connect を使用すると、SD-WAN ネットワーク仮想アプライアンスと Transit Gateway の間に IPsec VPNs を設定することなく、SD-WAN インフラストラクチャを AWS にネイティブに接続できます。GRE トンネルは、Transit Gateway Connect をアタッチメントタイプとして、Transit VIF 経由で確立でき、VPN 接続よりも高い帯域幅パフォーマンスを提供します。詳細については、ブログ記事「Simplify SD-WAN connectivity with AWS Transit Gateway Connect」を参照してください。

「Transit VIF to Direct Connect Gateway」オプションは、Direct Connect 接続ごとに AWS リージョン 1 つの BGP セッションを使用して、特定のポイント (Transit Gateway) のすべてのオンプレミス接続を統合することができるため、最適なオプションであるように見えるかもしれません。ただし、このオプションに関する制限と考慮事項によっては、ランディングゾーンの接続要件に合わせてプライベート VIF とトランジット VIFs の両方を使用する場合があります。

次の図は、VPCs、非常に大量のデータをオンプレミスのデータセンターからメディア VPC に転送する必要があるエッジユースケースにプライベート VIF を使用するサンプル設定を示しています。プライベート VIF は、Transit Gateway のデータ処理料金を回避するために使用されます。ベストプラクティスとして、冗長性を最大化するには、2 つの異なる Direct Connect ロケーションに少なくとも 2 つの接続が必要です。合計 4 つの接続が必要です。接続ごとに 1 つの VIF を作成し、合計で 4 つのプライベート VIFs と 4 つのトランジット VIFs。 Direct Connect 接続へのバックアップ接続として VPN を作成することもできます。

「Create GRE tunnels to Transit Gateway over a Transit VIF」オプションを使用すると、SD-WAN インフラストラクチャを AWS にネイティブに接続できます。これにより、SD-WAN ネットワーク仮想アプライアンスと Transit Gateway の間に IPsec VPNs を設定する必要がなくなります。



ハイブリッド接続のサンプルリファレンスアーキテクチャ

ネットワーク管理境界の境界を有効にする Direct Connect リソースを作成するには、 ネットワークサービスアカウントを使用します。Direct Connect 接続、Direct Connect ゲートウェイ、および Transit Gateway はすべて、ネットワークサービスアカウントに存在することができます。ランディングゾーンと接続を共有する Direct Connect には、 を介して Transit Gateway を他の アカウント AWS RAM と共有します。

Direct Connect 接続の MACsec セキュリティ

お客様は、特定の場所で 10 Gbps および 100 Gbps の専用接続の Direct Connect 接続で MAC Security Standard (MACsec) 暗号化 (IEEE 802.1AE) を使用できます。この機能を使用すると、お客様はレイヤー 2 レベルでデータを保護でき、Direct Connect はpoint-to-point暗号化を提供します。Direct Connect MACsec 機能を有効にするには、MACsec の前提条件が満たされていることを確認します。MACsec はリンクをhop-by-hop保護するため、デバイスには Direct Connect デバイスとの直接レイヤー 2 の隣接関係が必要です。ラストマイルプロバイダーは、接続が MACsec で動作することを確認するのに役立ちます。詳細については、「AWS Direct Connect 接続への MACsec セキュリティの追加」を参照してください。

Direct Connect 障害耐性に関する推奨事項

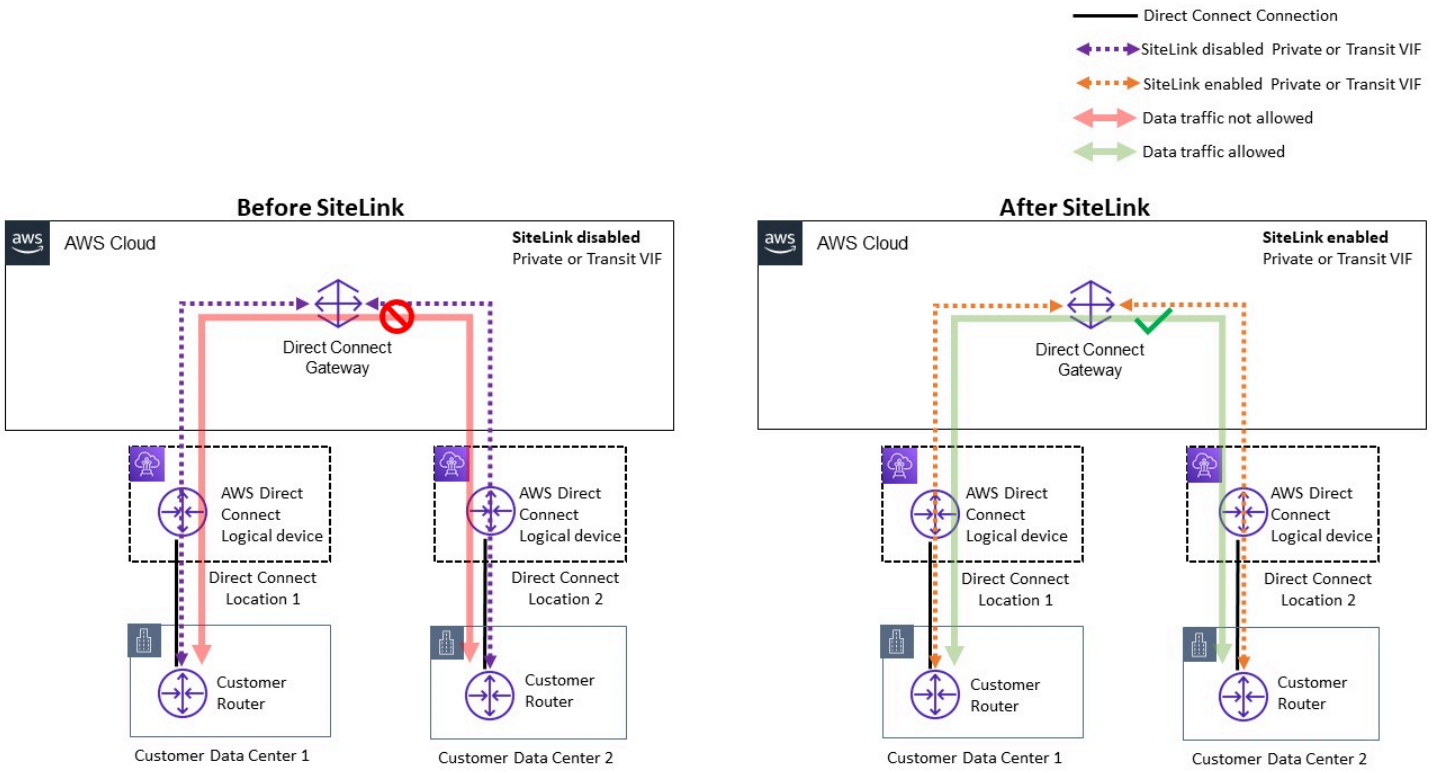
を使用すると Direct Connect、オンプレミスネットワークから Amazon VPCs と AWS リソースへの回復力の高い接続を実現できます。お客様が複数のデータセンターから接続して、単一ポイントの物理的な位置の障害を排除することがベストプラクティスです。また、ワークロードのタイプに応じて、冗長性のために複数の Direct Connect 接続を使用することをお勧めします。

AWS では、 Direct Connect Resiliency Toolkit も提供しています。これにより、接続ウィザードに複数の冗長モデルが提供されます。これにより、サービスレベルアグリーメント (SLA) の要件に最適なモデルを決定し、それに応じて Direct Connect 接続を使用してハイブリッド接続を設計できます。詳細については、Direct Connect 「障害耐性に関する推奨事項」を参照してください。

Direct Connect SiteLink

以前は、オンプレミスネットワークのsite-to-siteリンクの設定は、ダークファイバーやその他のテクノロジー、IPSEC VPNs を介した直接回路ビルドアウトを使用するか、""、MetroEthernet、レガシー T1 回路などのテクノロジーを備えたサードパーティーの回路プロバイダーを使用することによってのみ可能でした。SiteLink の導入により、お客様は Direct Connect ロケーションで終了するオンプレミスロケーションに対してsite-to-site直接接続を有効にできるようになりました。Direct Connect 回路を使用すると、VPC 経由でトラフィックをルーティングすることなくsite-to-site接続を提供でき VPCs 、AWS リージョンを完全にバイパスできます。

これで、 Direct Connect ロケーション間の最速パスでデータを送信することで、グローバルネットワーク内のオフィスとデータセンター間に、グローバルで信頼性が高く、pay-as-you-go接続を作成できるようになりました。

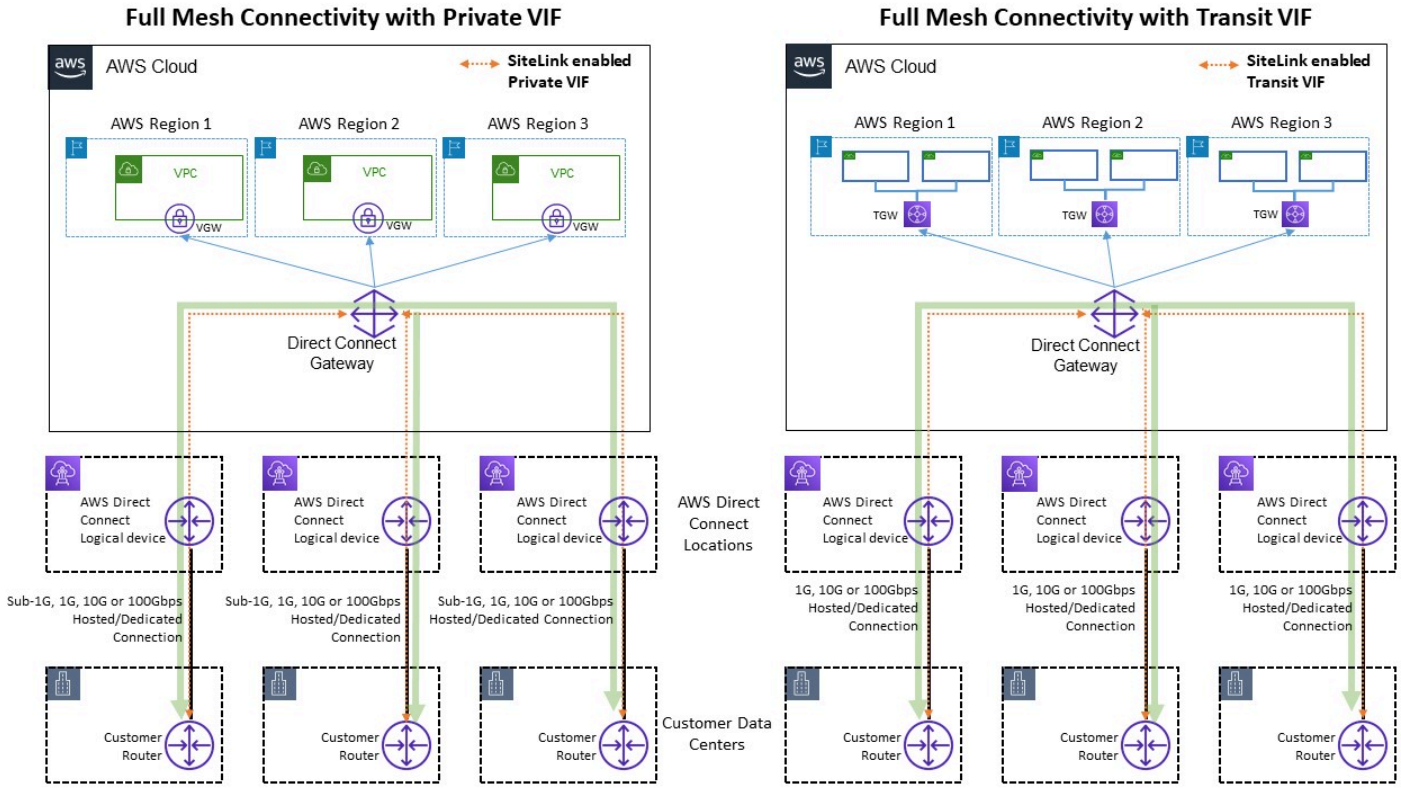


Direct Connect SiteLink のサンプルリファレンスアーキテクチャ

SiteLink を使用する場合は、まず、世界中の 100 を超える Direct Connect ロケーションのいずれかでオンプレミスネットワークを AWS に接続します。次に、それらの接続に仮想インターフェイス (VIFs) を作成し、SiteLink を有効にします。すべての VIFsされると、それらの間でデータの送信を開始できます。 Direct Connect データは、高速で安全で信頼性の高い AWS グローバルネットワークを使用して、 Direct Connect 送信先までの最短パスをたどります。SiteLink AWS リージョン を使用するには、 にリソースは必要ありません。

SiteLink を使用すると、DXGW は SiteLink が有効な VIFs を介してルーターから IPv4/IPv6 プレフィックスを学習し、BGP のベストパスアルゴリズムを実行し、NextHop や AS_Path などの属性を更新して、これらの BGP プレフィックスをその DXGW に関連付けられた SiteLink が有効な残りの VIFs に再アドバタイズします。VIF で SiteLink を無効にすると、DXGW はこの VIF を介して学習したオンプレミスプレフィックスを他の SiteLink 対応 VIFs にアドバタイズしません。SiteLink 無効 VIF からのオンプレミスプレフィックスは、DXGW に関連付けられた AWS Virtual Private Gateway

(VGWs) または Transit Gateway (TGW) インスタンスなどの DXGW Gateway 関連付けにのみアドバタイズされます。



Sitelink がトラフィックフローを許可する例

SiteLink を使用すると、お客様は AWS グローバルネットワークを使用して、高帯域幅と低レイテンシーでリモートロケーション間のプライマリまたはセカンダリ/バックアップ接続として機能し、動的ルーティングを使用して、相互に、および AWS リージョンリソースと通信できるロケーションを制御できます。

詳細については、「Introducing Direct Connect SiteLink」を参照してください。

インターネットへの一元的なエグレス

マルチアカウント環境にアプリケーションをデプロイする場合、多くのアプリではアウトバウンドのみのインターネットアクセス (ライブラリ、パッチ、OS 更新のダウンロードなど) が必要になります。これは、IPv4 トラフィックと IPv6 トラフィックの両方で実現できます。IPv4 の場合、これは、NAT ゲートウェイ (推奨) の形式のネットワークアドレス変換 (NAT)、またはすべての出力インターネットアクセスの手段として Amazon EC2 インスタンスで実行されているセルフマネージド NAT インスタンスを通じて実現できます。内部アプリケーションはプライベートサブネットにあり、NAT ゲートウェイと Amazon EC2 NAT インスタンスはパブリックサブネットにあります。

AWS では、NAT ゲートウェイの使用を推奨しています。NAT ゲートウェイは、可用性と帯域幅が向上し、管理にかかる労力が少なくて済むためです。詳細については、「NAT ゲートウェイと NAT インスタンスの比較」を参照してください。

IPv6 トラフィックの場合、Egress トラフィックは、分散された方法で Egress Only インターネットゲートウェイを介して各 VPC を離れるように設定することも、NAT インスタンスまたはプロキシインスタンスを使用して一元化された VPC に送信するように設定することもできます。IPv6 パターンについては、「」を参照してくださいIPv6 の一元化された出力。

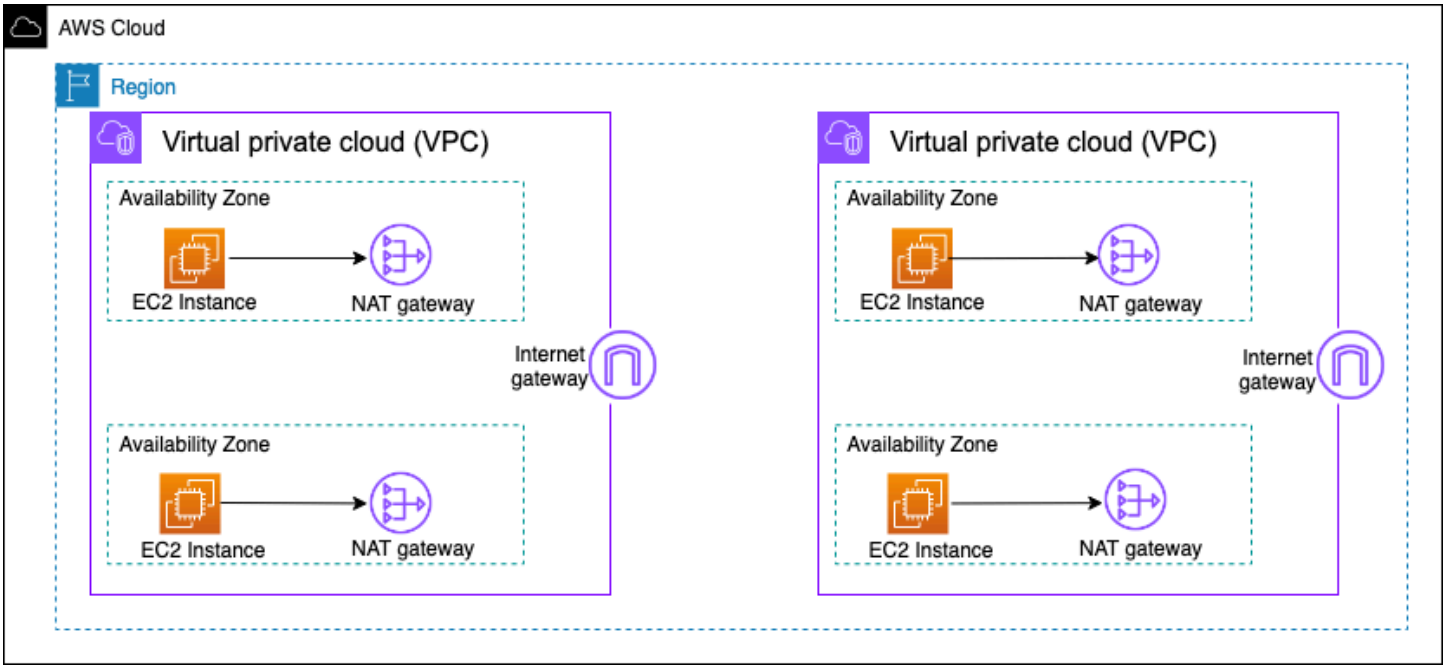
トピック

- 集中 IPv4 出力に NAT ゲートウェイを使用する
- で NAT ゲートウェイを使用して IPv4 を AWS Network Firewall 一元的に出力する
- Amazon EC2 インスタンスでの NAT ゲートウェイと Gateway Load Balancer を使用した一元的な IPv4 出力
- IPv6 の一元化された出力

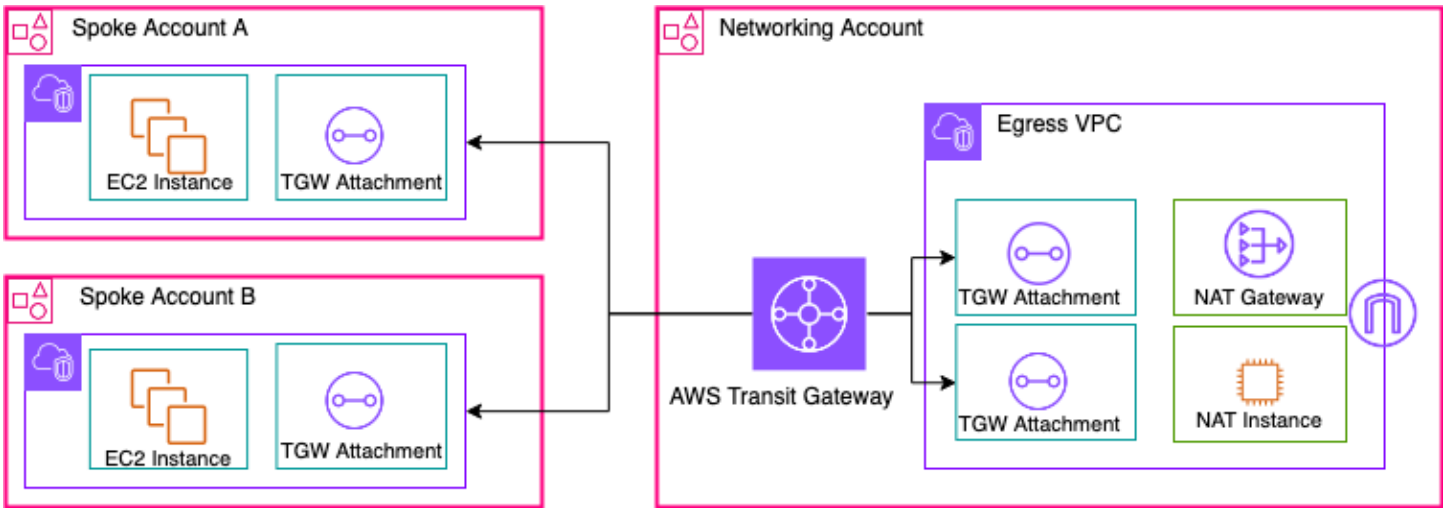
集中 IPv4 出力に NAT ゲートウェイを使用する

NAT ゲートウェイは、マネージドネットワークアドレス変換サービスです。すべてのスポーク VPC に NAT ゲートウェイをデプロイすると、デプロイするすべての NAT ゲートウェイに対して時間単位の料金が発生するため (Amazon VPC の料金を参照)、コストがかかる可能性があります。NAT ゲートウェイを一元化することは、コストを削減するための実行可能なオプションです。一元化するには、次の図に示すように、ネットワークサービスアカウントに個別の Egress VPC を作成し、Egress VPC に NAT ゲートウェイをデプロイし、スポーク VPCs からのすべての Egress トラフィックを Transit Gateway または CloudWAN を使用して Egress VPC に存在する NAT ゲートウェイにルーティングします。

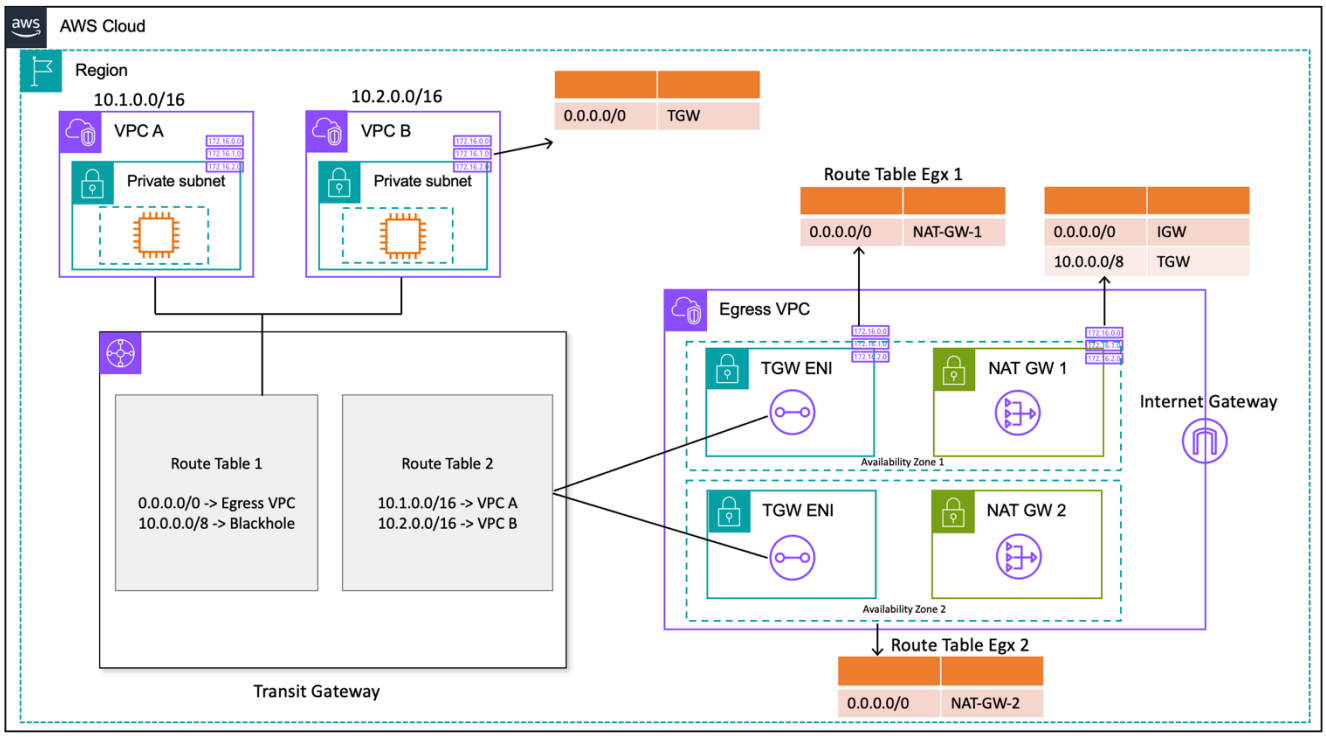
> **Note**
>
> Transit Gateway を使用して NAT ゲートウェイを一元化する場合、すべての VPC で NAT ゲートウェイを実行する分散アプローチと比較して、追加の Transit Gateway データ処理料金が発生します。エッジケースによっては、VPC から NAT ゲートウェイを介して大量のデータを送信する場合、Transit Gateway データ処理料金を回避するために、VPC で NAT をローカルにしておく方がコスト効率の高いオプションになる場合があります。



分散型高可用性 NAT ゲートウェイアーキテクチャ



Transit Gateway を使用した集中型 NAT ゲートウェイ (概要)



Transit Gateway を使用した一元化された NAT ゲートウェイ (ルートテーブル設計)

この設定では、スポーク VPC アタッチメントはルートテーブル 1 (RT1) に関連付けられ、ルートテーブル 2 (RT2) に伝達されます。2 つの VPCs 間の通信を禁止するブラックホールルートがあります。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、トランジット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 に伝達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関連付け/伝達することもできます) 。これにより、Transit Gateway を使用して VPCs 間の直接トラフィックフローが可能になります。

RT1 にすべてのトラフィックを Egress VPC にポイントする静的ルートを追加します。この静的ルートのため、Transit Gateway は、送信 VPC の ENIs を介してすべてのインターネットトラフィックを送信します。エグレス VPC に入ると、トラフィックはこれらの Transit Gateway ENIs が存在するサブネットルートテーブルで定義されたルートに従います。サブネットルートテーブルに、同じアベイラビリティーゾーン内のそれぞれの NAT ゲートウェイを指すルートを追加して、クロスアベイラビリティーゾーン (AZ) トラフィックを最小限に抑えます。NAT ゲートウェイサブネットルートテーブルには、ネクスト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フローバックするには、すべてのスポーク VPC バインドトラフィックをネクストホップとして Transit Gateway にポイントする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する必要があります。

高可用性

高可用性を実現するには、複数の NAT ゲートウェイ (各アベイラビリティーゾーンに 1 つずつ) を使用する必要があります。NAT ゲートウェイが使用できない場合、影響を受けた NAT ゲートウェイを通過するそのアベイラビリティーゾーンでトラフィックがドロップされる可能性があります。1 つのアベイラビリティーゾーンが使用できない場合、そのアベイラビリティーゾーンの Transit Gateway エンドポイントと NAT ゲートウェイは失敗し、すべてのトラフィックは他のアベイラビリティーゾーンの Transit Gateway エンドポイントと 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

セキュリティグループは、ソースインスタンス、Transit Gateway ルートテーブルのブラックホールルート、および NAT ゲートウェイが配置されているサブネットのネットワーク ACL に依存します。たとえば、お客様は NAT Gateway パブリックサブネット (複数可) の ACLs を使用して、送信元または送信先の IP アドレスを許可またはブロックできます。または、NAT Gateway を と共に使用 AWS Network Firewall して、次のセクションで説明する一元的な出力を行い、この要件を満たすこともできます。

スケーラビリティ

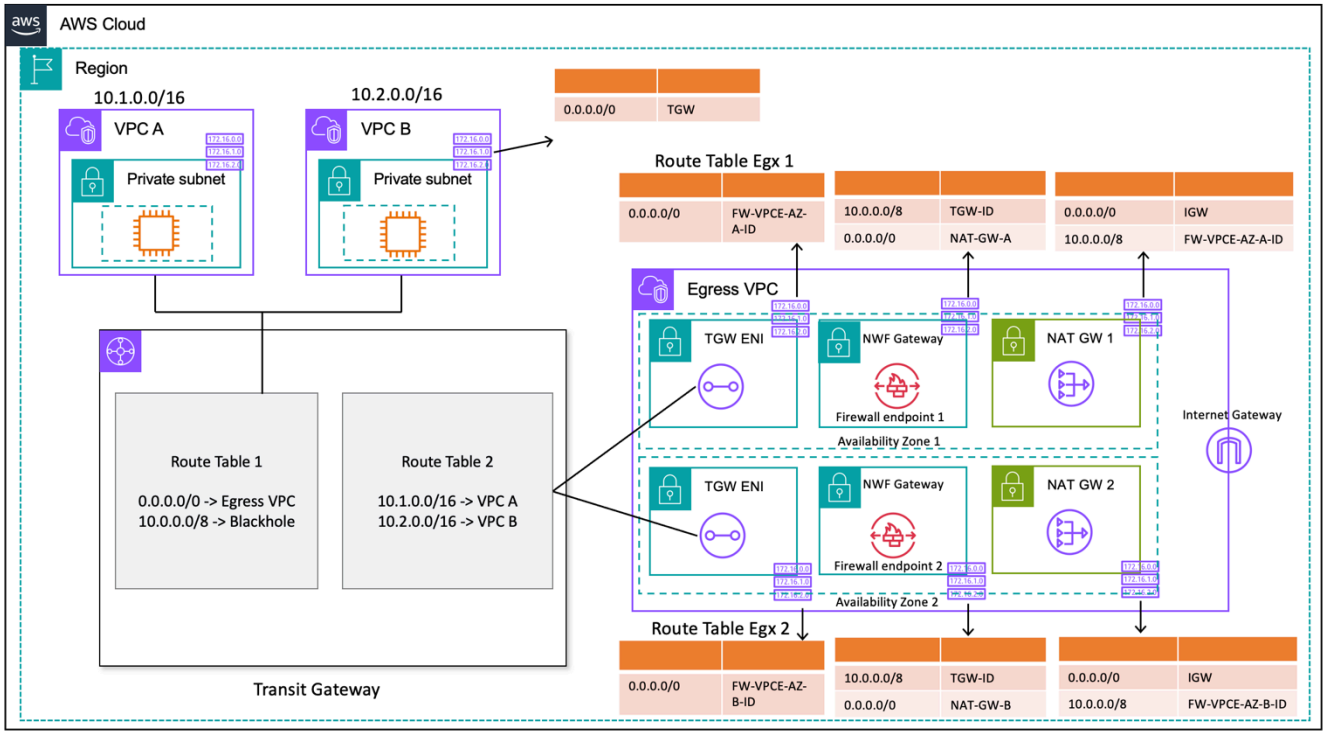
単一の NAT ゲートウェイは、割り当てられた IP アドレスごとに一意の送信先ごとに最大 55,000 の同時接続をサポートできます。クォータ調整をリクエストして、最大 8 つの割り当てられた IP アドレスを許可し、1 つの送信先 IP とポートへの同時接続を 440,000 回許可できます。NAT ゲートウェイは 5 Gbps の帯域幅を提供し、自動的に 100 Gbps にスケールします。トランジットゲートウェイは通常、ロードバランサーとして機能しず、複数のアベイラビリティーゾーンの NAT ゲートウェイ間でトラフィックを均等に分散しません。トランジットゲートウェイ全体のトラフィックは、可能であればアベイラビリティーゾーン内に留まります。トラフィックを開始する Amazon EC2 インスタンスがアベイラビリティーゾーン 1 にある場合、トラフィックはエグレス VPC の同じアベイラビリティーゾーン 1 の Transit Gateway Elastic Network Interface から流れ出し、Elastic Network Interface が存在するサブネットルートテーブルに基づいてネクストホップに流れます。ルールの完全なリストについては、Amazon Virtual Private Cloud ドキュメントの NAT ゲートウェイを参照してください。

詳細については、AWS Transit Gateway を使用して複数の VPCs から単一のインターネット出口ポイントを作成するブログ記事を参照してください。

で NAT ゲートウェイを使用して IPv4 を AWS Network Firewall 一元的に出力する

アウトバウンドトラフィックを検査およびフィルタリングする場合は、一元化された Egress アーキテクチャに AWS Network Firewall と NAT ゲートウェイを組み込むことができます。 AWS Network Firewall は、すべての VPCs。VPC 全体の Layer 3-7 ネットワークトラフィックを制御および可視化します。URL/ドメイン名、IP アドレス、コンテンツベースのアウトバウンドトラフィックフィルタリングを実行して、データ損失の可能性を防ぎ、コンプライアンス要件を満たし、既知のマルウェア通信をブロックできます。 は、既知の不正な IP アドレスまたは不正なドメイン名を宛先とするネットワークトラフィックを除外できる数千のルール AWS Network Firewall をサポートしています。また、オープンソースのルールセットをインポートするか、Suricata ルール構文を使用して独自の侵入防止システム (IPS) ルールを作成することで、 AWS Network Firewall サービスの一部として Suricata IPS ルールを使用することもできます。 では、AWS パートナーから取得した互換性のあるルールをインポート AWS Network Firewall することもできます。

検査を使用した一元化された Egress アーキテクチャでは、 AWS Network Firewall エンドポイントは、Egress VPC の Transit Gateway アタッチメントサブネットルートテーブルのデフォルトのルートテーブルターゲットです。スポーク VPCsとインターネット間のトラフィックは、次の図 AWS Network Firewall に示すように を使用して検査されます。



AWS Network Firewall と NAT ゲートウェイを使用した一元的な出力 (ルートテーブル設計)

Transit Gateway を使用した一元化されたデプロイモデルの場合、AWS では複数のアベイラビリティーゾーンにエンドポイントをデプロイ AWS Network Firewall することをお勧めします。前の図に示すように、お客様がワークロードを実行しているアベイラビリティーゾーンごとにファイアウォールエンドポイントが 1 つある必要があります。ベストプラクティスとして、 はファイアウォールサブネット内の送信元または送信先からのトラフィックを検査 AWS Network Firewall できないため、ファイアウォールサブネットには他のトラフィックを含めないでください。

前のセットアップと同様に、スポーク VPC アタッチメントはルートテーブル 1 (RT1) に関連付けられ、ルートテーブル 2 (RT2) に伝達されます。ブラックホールルートが明示的に追加され、2 つの VPCs 間の通信が禁止されます。

RT1 では、すべてのトラフィックを Egress VPC にポイントするデフォルトルートを引き続き使用します。Transit Gateway は、すべてのトラフィックフローを Egress VPC の 2 つのアベイラビリティーゾーンのいずれかに転送します。トラフィックが Egress VPC 内の Transit Gateway ENIs の 1 つに到達すると、トラフィックをそれぞれのアベイラビリティーゾーンの AWS Network Firewall エンドポイントの 1 つに転送するデフォルトルートに到達します。 AWS Network Firewall は、デフォルトルートを使用してトラフィックを NAT ゲートウェイに転送する前に設定したルールに基づいてトラフィックを検査します。

この場合、アタッチメント間でトラフィックを送信しないため、Transit Gateway アプライアンスモードは必要ありません。

> **Note**
>
> AWS Network Firewall はネットワークアドレス変換を実行しません。この関数は、 を介したトラフィック検査後に NAT ゲートウェイによって処理されます AWS Network Firewall。この場合、リターントラフィックはデフォルトで NATGW IPs に転送されるため、受信ルーティングは必要ありません。

Transit Gateway を使用しているため、ここでは NAT ゲートウェイの前にファイアウォールを配置できます。このモデルでは、ファイアウォールは Transit Gateway の背後にあるソース IP を確認できます。

これを単一の VPC で実行している場合、同じ VPC 内のサブネット間のトラフィックを検査できる VPC ルーティングの機能強化を使用できます。詳細については、「VPC ルーティング機能強化 AWS Network Firewall による のデプロイモデル」ブログ記事を参照してください。

スケーラビリティ

AWS Network Firewall は、トラフィック負荷に基づいてファイアウォール容量を自動的にスケールアップまたはスケールダウンして、安定した予測可能なパフォーマンスを維持し、コストを最小限に抑えることができます。 AWS Network Firewall は、何万ものファイアウォールルールをサポートするように設計されており、アベイラビリティーゾーンあたり最大 100 Gbps のスループットまでスケールできます。

主な考慮事項

- 各ファイアウォールエンドポイントは、約 100 Gbps のトラフィックを処理できます。より高いバーストまたは持続的なスループットが必要な場合は、AWS サポートにお問い合わせください。
- Network Firewall とともに AWS アカウントに NAT ゲートウェイを作成する場合、標準の NAT ゲートウェイ処理と 1 時間あたりの使用料金は、GB あたりの処理とファイアウォールの使用時間に基づいて one-to-one で免除されます。
- Transit Gateway AWS Firewall Manager を使用せずに、 を介して分散ファイアウォールエンドポイントを検討することもできます。
- ネットワークアクセスコントロールリストと同様に、ファイアウォールルールを本番環境に移行する前に、順序が重要かどうかをテストします。
- 詳細な検査には、高度な Suricata ルールが必要です。ネットワークファイアウォールは、イングレストラフィックとエグレストラフィックの暗号化されたトラフィック検査をサポートしています。
- `HOME_NET` ルールグループ変数は、ステートフルエンジンでの処理の対象となるソース IP 範囲を定義しました。一元化されたアプローチを使用して、Transit Gateway にアタッチされたすべての VPC CIDRs を追加して、処理の対象にする必要があります。`HOME_NET` ルールグループ変数の詳細については、Network Firewall のドキュメントを参照してください。
- Transit Gateway と Egress VPC を別の Network Services アカウントにデプロイして、職務の委任に基づいてアクセスを分離することを検討してください。たとえば、ネットワーク管理者のみが Network Services アカウントにアクセスできます。
- このモデル AWS Network Firewall での のデプロイと管理を簡素化するために、 AWS Firewall Manager を使用できます。Firewall Manager では、一元化された場所で作成した保護を複数のアカウントに自動的に適用することで、さまざまなファイアウォールを一元管理できます。Firewall Manager は、Network Firewall の分散デプロイモデルと集中デプロイモデルの両方をサポートします。詳細については、ブログ記事「 AWS Network Firewall を使用してデプロイする方法 AWS Firewall Manager」を参照してください。

Amazon EC2 インスタンスでの NAT ゲートウェイと Gateway Load Balancer を使用した一元的な IPv4 出力

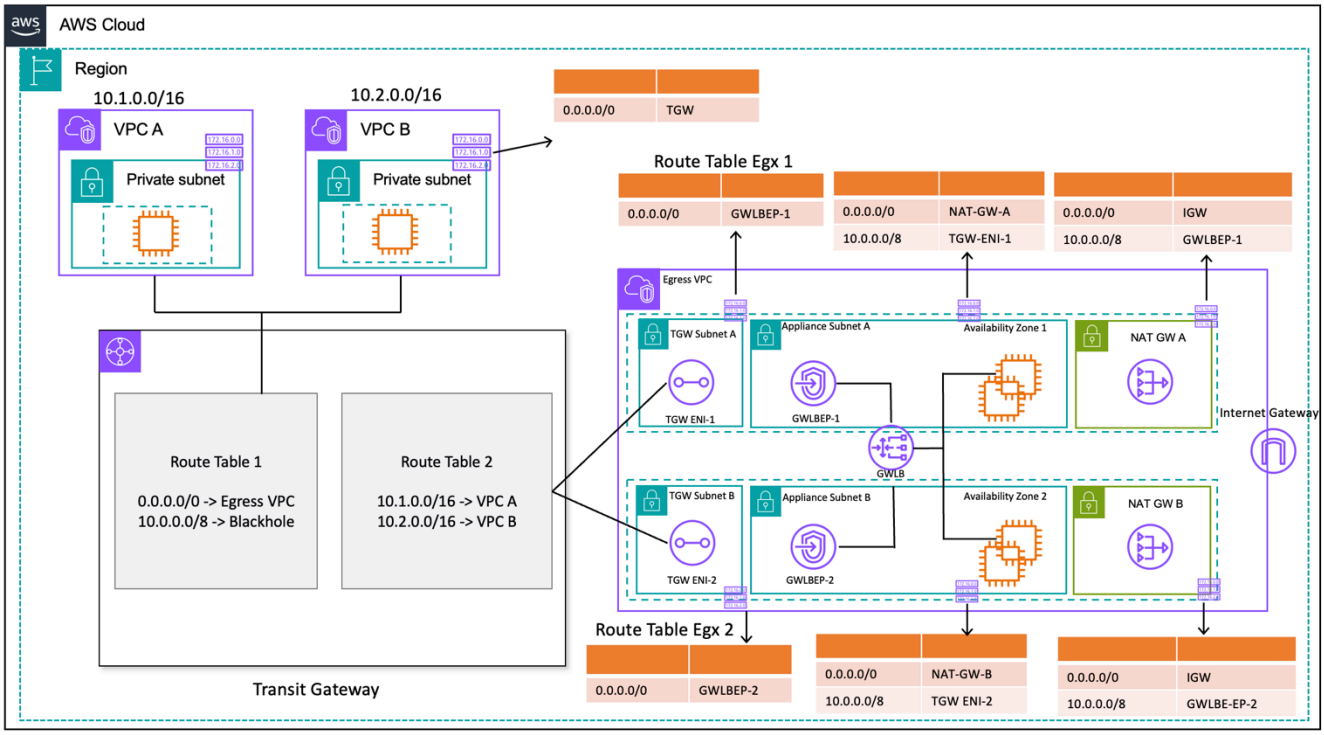
AWS Marketplace と からのソフトウェアベースの仮想アプライアンス (Amazon EC2 上) を出口ポイント AWS Partner Network として使用する方法は、NAT ゲートウェイのセットアップと似ています。このオプションは、さまざまなベンダーが提供する高度なレイヤー 7 ファイアウォール/侵入防止/検出システム (IPS/IDS) およびディープパケットインスペクション機能を使用する場合に使用できます。

次の図では、NAT ゲートウェイに加えて、Gateway Load Balancer (GWLB) の背後にある EC2 インスタンスを使用して仮想アプライアンスをデプロイします。この設定では、GWLB、Gateway Load Balancer Endpoint (GWLBE)、仮想アプライアンス、NAT ゲートウェイが、VPC アタッチメントを使用して Transit Gateway に接続されている一元化された VPC にデプロイされます。スポーク VPCsは、VPC アタッチメントを使用して Transit Gateway にも接続されます。GWLBEs はルーティング可能なターゲットであるため、Transit Gateway との間で送受信されるトラフィックを、GWLB の背後にあるターゲットとして設定された仮想アプライアンスのフリートにルーティングできます。GWLB bump-in-the-wireとして機能し、すべての Layer 3 トラフィックをサードパーティーの仮想アプライアンスに透過的に渡すため、トラフィックの送信元と送信先には表示されません。したがって、このアーキテクチャにより、Transit Gateway を通過するすべての出力トラフィックを一元的に検査できます。

VPCs「AWS Gateway Load Balancer を使用した一元化された検査アーキテクチャ AWS Transit Gateway」および「」を参照してください。

Transit Gateway でアプライアンスモードを有効にして、仮想アプライアンスを介してフロー対称性を維持できます。つまり、双方向トラフィックは、フローの存続期間中、同じアプライアンスとアベイラビリティーゾーンを介してルーティングされます。この設定は、ディープパケットインスペクションを実行するステートフルファイアウォールにとって特に重要です。アプライアンスモードを有効にすると、ソースネットワークアドレス変換 (SNAT) などの複雑な回避策が不要になり、トラフィックを適切なアプライアンスに強制的に戻して対称性を維持します。詳細については、「Gateway Load Balancer をデプロイするためのベストプラクティス」を参照してください。

Transit Gateway を使用せずに GWLB エンドポイントを分散的にデプロイして、出力検査を有効にすることもできます。このアーキテクチャパターンの詳細については、ブログ記事「AWS Gateway Load Balancer の紹介: サポートされているアーキテクチャパターン」を参照してください。



Gateway Load Balancer と EC2 インスタンスによる一元的な出力 (ルートテーブル設計)

高可用性

AWS では、可用性を高めるために、Gateway Load Balancer と仮想アプライアンスを複数のアベイラビリティーゾーンにデプロイすることをお勧めします。

Gateway Load Balancer は、ヘルスチェックを実行して仮想アプライアンスの障害を検出できます。アプライアンスに異常がある場合、GWLB は新しいフローを正常なアプライアンスに再ルーティングします。既存のフローは、ターゲットのヘルスステータスに関係なく、常に同じターゲットに送信されます。これにより、接続ドレインが可能になり、アプライアンスの CPU スパイクによるヘルスチェックの失敗に対応できます。詳細については、ブログ記事「Gateway Load Balancer をデプロイするためのベストプラクティス」の「セクション 4: アプライアンスとアベイラビリティーゾーンの障害シナリオを理解する」を参照してください。Gateway Load Balancer は、Auto Scaling グループをターゲットとして使用できます。この利点により、アプライアンスフリートの可用性とスケーラビリティの管理に手間がかかります。

利点

Gateway Load Balancer と Gateway Load Balancer エンドポイントは を利用しているため AWS PrivateLink、パブリックインターネットを経由することなく、VPC 境界間でトラフィックを安全に交換できます。

Gateway Load Balancer は、仮想セキュリティアプライアンスの管理、デプロイ、スケーリングの差別化されていない負担を軽減し、重要なことに集中できるようにするマネージドサービスです。Gateway Load Balancer は、お客様が を使用してサブスクライブできるように、ファイアウォールのスタックをエンドポイントサービスとして公開できますAWS Marketplace。これは Firewall as a Service (FWaaS) と呼ばれます。シンプルなデプロイを導入し、BGP と ECMP に依存して複数の Amazon EC2 インスタンスにトラフィックを分散する必要がなくなります。

主な考慮事項

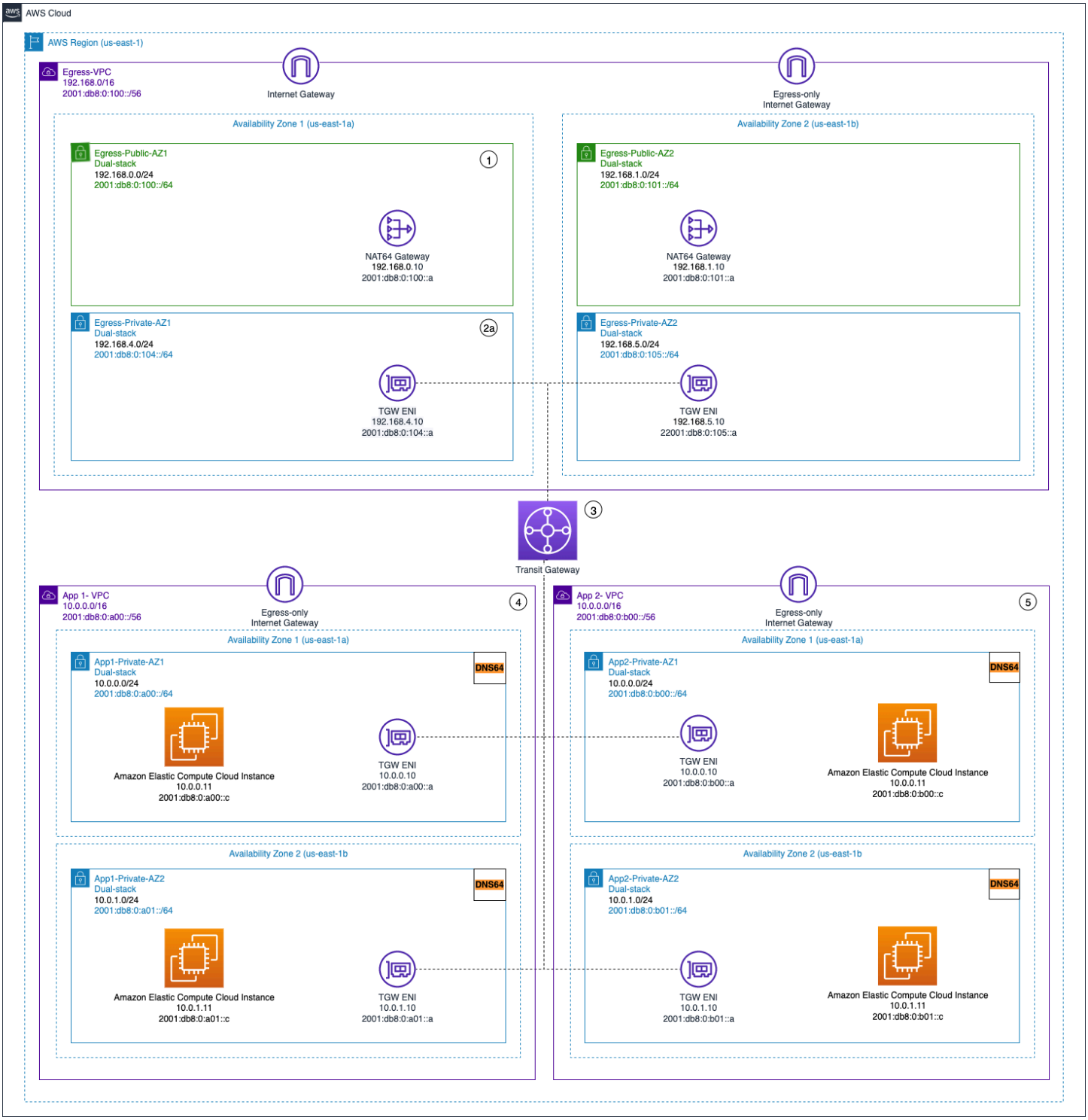
- アプライアンスは、GWLB と統合するために Geneve カプセル化プロトコルをサポートする必要があります。
- 一部のサードパーティーアプライアンスは SNAT およびオーバーレイルーティング (2 アームモード) をサポートできるため、コストを削減するために NAT ゲートウェイを作成する必要がなくなります。ただし、このモードを使用する前に、任意の AWS パートナーに相談してください。これはベンダーのサポートと実装に依存します。
- GWLB アイドルタイムアウトを書き留めます。これにより、クライアントで接続がタイムアウトする可能性があります。クライアント、サーバー、ファイアウォール、OS レベルでタイムアウトを調整して、これを回避できます。詳細については、「Gateway Load Balancer をデプロイするためのベストプラクティス」ブログ記事の「セクション 1: TCP キープアライブ値またはタイムアウト値をチューニングして、存続期間の長い TCP フローをサポートする」を参照してください。
- GWLBE は を利用しているため AWS PrivateLink、 AWS PrivateLink 料金が適用されます。詳細については、 のAWS PrivateLink 料金表ページを参照してください。Transit Gateway で一元化されたモデルを使用している場合は、TGW データ処理料金が適用されます。
- Transit Gateway と Egress VPC を別の Network Services アカウントにデプロイして、ネットワーク管理者のみが Network Services アカウントにアクセスできるなど、職務の委任に基づいてアクセスを分離することを検討してください。

IPv6 の一元化された出力

一元化された IPv4 出力を持つデュアルスタックデプロイで IPv6 出力をサポートするには、次の 2 つのパターンのいずれかを選択する必要があります。 IPv4

- 分散 IPv4 出力を使用した集中 IPv6 出力
- 一元化された IPv4 出力と一元化された IPv6 出力

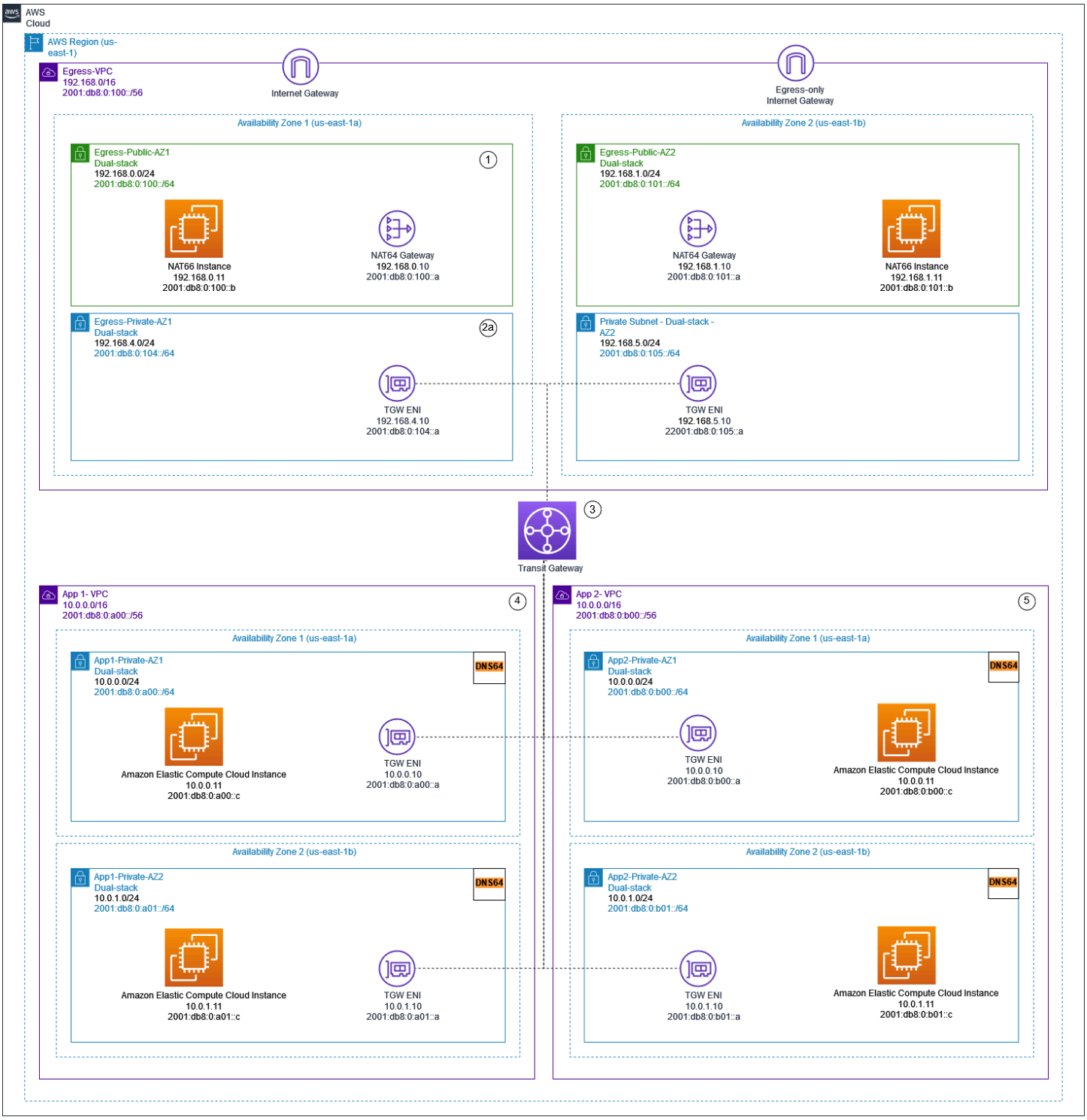
次の図に示す最初のパターンでは、エグレス専用インターネットゲートウェイが各スポーク VPC にデプロイされます。Egress-Only インターネットゲートウェイは、VPC 内のインスタンスからの IPv6 経由のアウトバウンド通信を可能にする、水平スケーリング、冗長化、高可用性のゲートウェイです。これにより、インターネットがインスタンスとの IPv6 接続を開始できなくなります。Egress-Only インターネットゲートウェイには料金はかかりません。このデプロイモデルでは、IPv6 トラフィックは各 VPC の Egress-Only インターネットゲートウェイから流れ出し、IPv4 トラフィックはデプロイされた一元化された NAT ゲートウェイを経由して流れます。



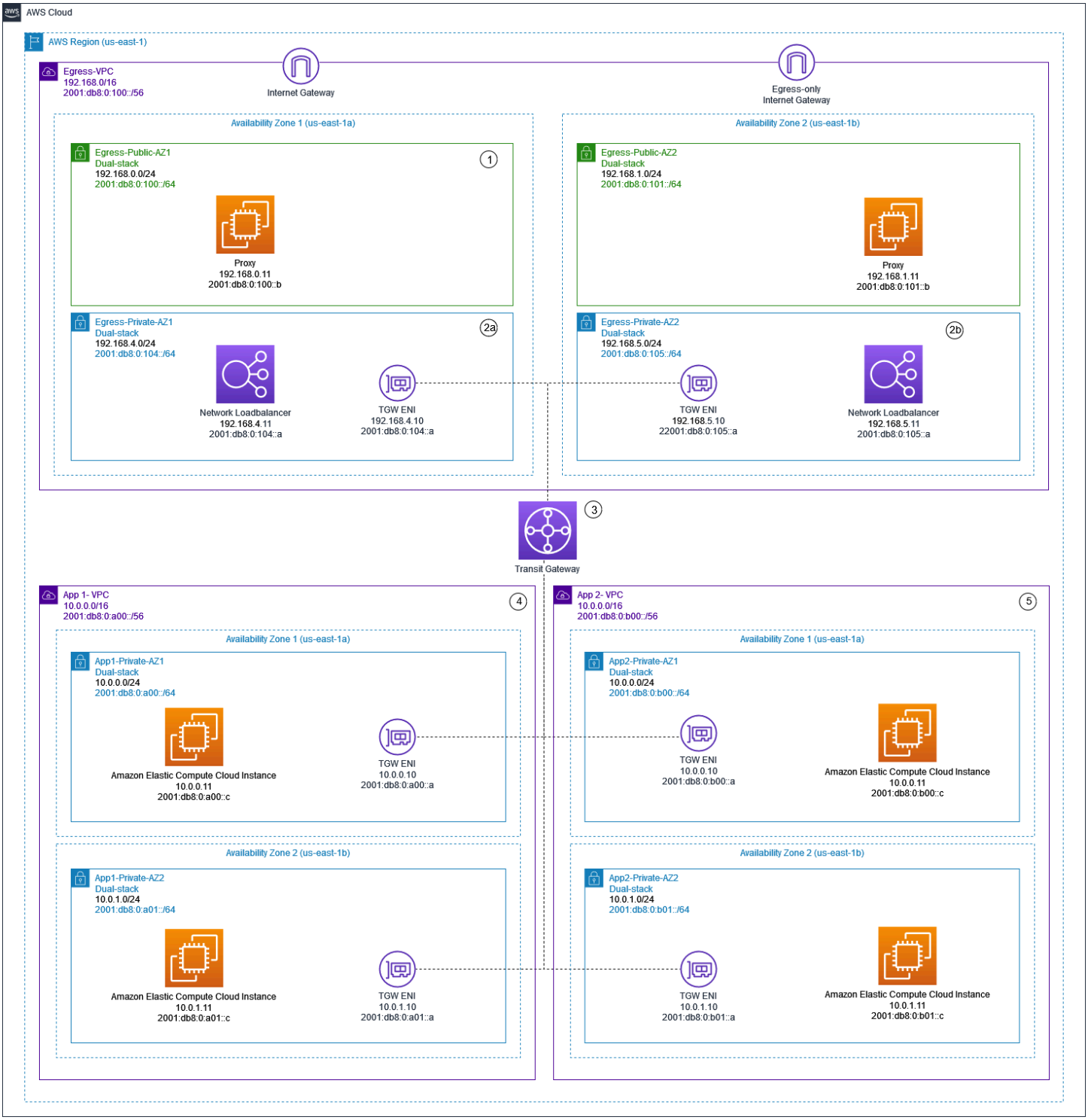
一元化された IPV4 出力と分散されたアウトバウンドのみの IPv6 出力

次の図に示す 2 番目のパターンでは、インスタンスからの出力 IPv6 トラフィックが集中型 VPC に送信されます。これは、NAT66 インスタンスと NAT ゲートウェイで IPv6-to-IPv6 Network Prefix Translation (NPTv6) を使用するか、プロキシインスタンスと Network Load Balancer を使用するこ

とで実現できます。 NAT66 このパターンは、アウトバウンドトラフィックの集中型トラフィック検査が必要であり、各スポーク VPC で実行できない場合に適用されます。



NAT ゲートウェイと NATIPv6NAT66 出力



プロキシインスタンスと Network Load Balancer を使用した一元的な IPv4 および IPv6 出力

AWS での IPv6 ホワイトペーパーでは、一元化された IPv6 出力パターンについて説明します。IPv6 出力パターンについては、ブログ記事「デュアルスタック IPv4 および IPv6 VPCs」で、特別な考慮事項、サンプルソリューション、図表とともに詳しく説明されています。

VPC 間およびオンプレミスから VPC トラフィックへの一元化されたネットワークセキュリティ

お客様がマルチアカウント環境内にレイヤー 3-7 ファイアウォール/IPS/IDS を実装してVPCs (東西のトラフィック) 間、またはオンプレミスデータセンターと VPC (北南のトラフィック) 間のトラフィックフローを検査するシナリオがあるかもしれません。これは、ユースケースと要件に応じてさまざまな方法で実現できます。例えば、Gateway Load Balancer 、Network Firewall、Transit VPC を組み込むか、Transit Gateway で集中型アーキテクチャを使用できます。これらのシナリオについては、次のセクションで説明します。

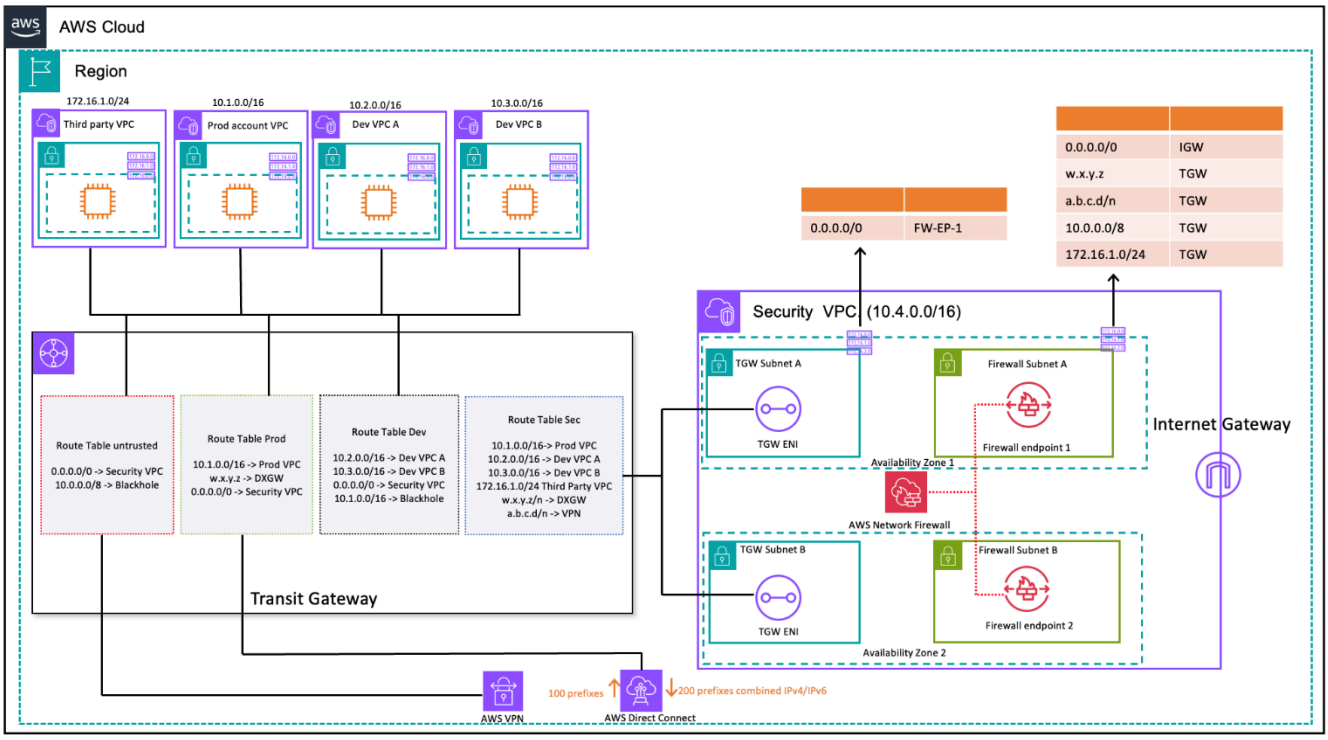
一元化されたネットワークセキュリティ検査モデルの使用に関する考慮事項

コストを削減するには、 AWS Network Firewall または Gateway Load Balancer を介して渡すトラフィックを選択する必要があります。続行する 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には、サードパーティーが管理するリモートサイト、制御/信頼しないベンダー VPC、サンドボックス/開発 VPC があり、他の環境と比較してセキュリティルールが緩い場合があります。この例では、次の 4 つのゾーンがあります。

- 信頼されていないゾーン — これは、「VPN からリモート信頼されていないサイト」またはサードパーティーベンダー VPC へのトラフィック用です。
- 本番稼働 (Prod) ゾーン — 本番稼働用 VPC とオンプレミスのカスタマー DC からのトラフィックが含まれます。
- 開発 (開発) ゾーン — これには、2 つの開発 VPCsからのトラフィックが含まれます。
- セキュリティ (Sec) ゾーン — ファイアウォールコンポーネント Network Firewall または Gateway Load Balancer が含まれます。

この設定には 4 つのセキュリティゾーンがありますが、他にもセキュリティゾーンがある場合があります。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。適切なゾーンセットの選択は、ランディングゾーンの設計戦略 (アカウント構造、VPC 設計) 全体によって異なります。ゾーンを設定して、ビジネスユニット (BUs)、アプリケーション、環境などの分離を有効にすることができます。

VPC から VPC へのトラフィック、ゾーン間トラフィック、および VPC オンプレミストラフィックを検査およびフィルタリングする場合は、一元化されたアーキテクチャに Transit Gateway AWS Network Firewall を組み込むことができます。の hub-and-spoke モデルを使用することで AWS Transit Gateway、一元化されたデプロイモデルを実現できます。 AWS Network Firewall は別のセキュリティ VPC にデプロイされます。別のセキュリティ VPC は、検査を管理するためのシンプルで一元的なアプローチを提供します。このような VPC アーキテクチャは、送信 AWS Network Firewall 元と送信先の IP を可視化します。送信元 IP と送信先 IPsの両方が保持されます。このセキュリティ VPC は、各アベイラビリティーゾーンの 2 つのサブネットで構成されます。1 つのサブネットは AWS Transit Gateway アタッチメント専用で、もう 1 つのサブネットはファイアウォールエンドポイント専用です。Network Firewall は AWS Network Firewall エンドポイントと同じサブネット内のトラフィックを検査できないため、この VPC 内のサブネットにはエンドポイントのみを含める必要があります。Network Firewall を使用してトラフィックを一元的に検査すると、イングレストラフィックに対してディープパケットインスペクション (DPI) を実行できます。DPI パターンは、このホワイトペーパーの「集中インバウンド検査」セクションで に展開されています。



Transit Gateway と AWS Network Firewall （ ルートテーブル設計) を使用した VPC 間およびオンプレミスから VPC へのトラフィック検査

検査機能を備えた集中型アーキテクチャでは、トラフィックが同じアベイラビリティーゾーン内のファイアウォールエンドポイントに転送されるように、Transit Gateway サブネットに別の VPC ルートテーブルが必要です。リターントラフィックには、Transit Gateway へのデフォルトルートを含む単一の VPC ルートテーブルが設定されます。トラフィックは、 によって検査された後、同

じアベイラビリティーゾーン AWS Transit Gateway の に返されます AWS Network Firewall。これは、Transit Gateway のアプライアンスモード機能が原因である可能性があります。Transit Gateway のアプライアンスモード機能は、 AWS Network Firewall がセキュリティ VPC 内にステートフルなトラフィック検査機能を持つのにも役立ちます。

トランジットゲートウェイでアプライアンスモードを有効にすると、接続の存続期間中、フローハッシュアルゴリズムを使用して単一のネットワークインターフェイスが選択されます。トランジットゲートウェイは、リターントラフィックに同じネットワークインターフェイスを使用します。これにより、双方向トラフィックは対称的にルーティングされます。つまり、フローの有効期間中、VPC アタッチメント内の同じアベイラビリティーゾーンを経由してルーティングされます。アプライアンスモードの詳細については、Amazon VPC ドキュメントの「ステートフルアプライアンスとアプライアンスモード」を参照してください。

AWS Network Firewall および Transit Gateway を使用したセキュリティ VPC のさまざまなデプロイオプションについては、AWS Network Firewall のデプロイモデルに関するブログ記事を参照してください。

一元化されたネットワークセキュリティのための Transit Gateway での Gateway Load Balancer の使用

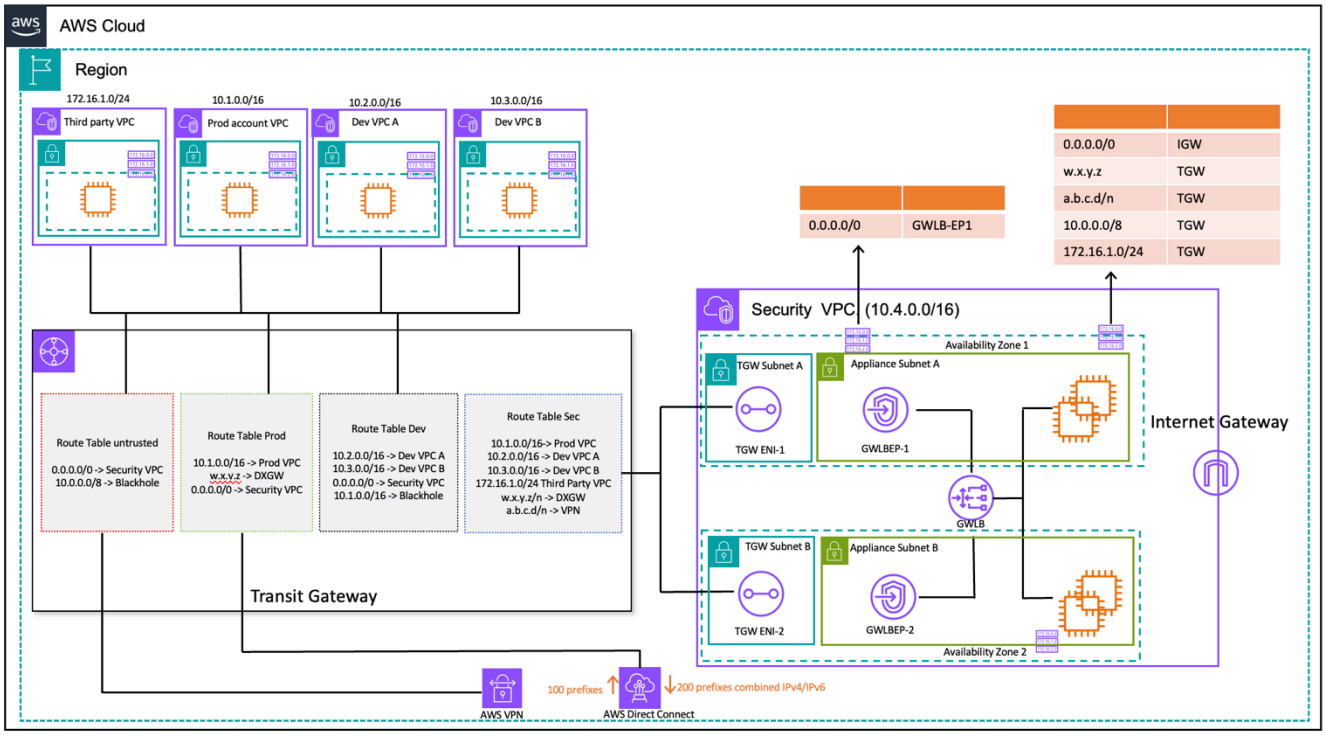
多くの場合、お客様はトラフィックフィルタリングを処理し、セキュリティ検査機能を提供するために仮想アプライアンスを組み込む必要があります。このようなユースケースでは、Gateway Load Balancer 、仮想アプライアンス、および Transit Gateway を統合して、VPC から VPC へのトラフィックと VPC to-on-premises トラフィックを検査するための一元化されたアーキテクチャをデプロイできます。

Gateway Load Balancer は、仮想アプライアンスとともに別のセキュリティ VPC にデプロイされます。トラフィックを検査する仮想アプライアンスは、Gateway Load Balancer の背後にあるターゲットとして設定されます。Gateway Load Balancer エンドポイントはルーティング可能なターゲットであるため、お客様は Transit Gateway との間で送受信されるトラフィックを仮想アプライアンスのフリートにルーティングできます。フローの対称性を確保するために、Transit Gateway でアプライアンスモードが有効になっています。

各スポーク VPC には、Transit Gateway に関連付けられたルートテーブルがあります。このルートテーブルには、ネクストホップとして Security VPC アタッチメントへのデフォルトルートがあります。

一元化されたセキュリティ VPC は、各アベイラビリティーゾーンのアプライアンスサブネットで構成されます。これには、Gateway Load Balancer エンドポイントと仮想アプライアンスがあります。次の図に示すように、各アベイラビリティーゾーンに Transit Gateway アタッチメントのサブネットもあります。

Gateway Load Balancer と Transit Gateway による一元化されたセキュリティ検査の詳細については、AWS Gateway Load Balancer による一元化された検査アーキテクチャと AWS Transit Gatewayブログ記事を参照してください。



Transit Gateway と AWS Gateway Load Balancer を使用した VPC 間および on-premises-to-VPC トラフィック検査 (ルートテーブル設計)

AWS Network Firewall と AWS Gateway Load Balancer の主な考慮事項

- 東西検査を行うときは、Transit Gateway でアプライアンスモードを有効にする必要があります。
- AWS Transit Gateway リージョン間ピアリング を使用して、同じモデルをデプロイして他の AWS リージョン へのトラフィックを検査できます。
- デフォルトでは、アベイラビリティーゾーンにデプロイされた各 Gateway Load Balancer は、同じアベイラビリティーゾーン内の登録済みターゲットにのみトラフィックを分散します。これはアベイラビリティーゾーンのアフィニティと呼ばれます。クロスゾーン負荷分散 を有効にすると、Gateway Load Balancer は、有効なすべてのアベイラビリティーゾーンのすべての登録済みターゲットと正常なターゲットにトラフィックを分散します。すべてのアベイラビリティーゾーン

のすべてのターゲットが異常である場合、Gateway Load Balancer はオープンに失敗します。詳細については、Gateway Load Balancer をデプロイするためのベストプラクティスのブログ記事のセクション 4: アプライアンスとアベイラビリティーゾーンの障害シナリオを理解するを参照してください。

- マルチリージョンデプロイの場合、リージョン間の依存関係を回避し、関連するデータ転送コストを削減するために、各ローカルリージョンに個別の検査 VPCs を設定する AWS ことをお勧めします。検査を別のリージョンに一元化するのではなく、ローカルリージョンのトラフィックを検査する必要があります。
- マルチリージョンデプロイで追加の EC2-based高可用性 (HA) ペアを実行すると、コストが増大する可能性があります。詳細については、Gateway Load Balancer をデプロイするためのベストプラクティスのブログ記事を参照してください。

AWS Network Firewall 対 Gateway Load Balancer

表 2 — AWS Network Firewall vs Gateway Load Balancer

条件	AWS Network Firewall	Gateway Load Balancer
ユースケース	Suricata と互換性のある侵入検知および防止サービス機能を備えたステートフルでマネージド型のネットワークファイアウォール。	サードパーティーの仮想アプライアンスのデプロイ、スケーリング、管理を容易にするマネージドサービス
複雑さ	AWS managed service.は、サービスのスケーラビリティと可用性 AWS を処理します。	AWS マネージドサービス。は Gateway Load Balancer サービスのスケーラビリティと可用性 AWS を処理します。お客様は、Gateway Load Balancer の背後にある仮想アプライアンスのスケーリングと可用性を管理する責任があります。
スケール	AWS Network Firewall エンドポイントは を利用しています AWS PrivateLink。Networ	Gateway Load Balancer エンドポイントは、エンドポイン

条件	AWS Network Firewall	Gateway Load Balancer
	k Firewall は、ファイアウォールエンドポイントごとに最大 100 Gbps のネットワークトラフィックをサポートします。	トあたり最大 100 Gbps の最大帯域幅をサポートします
コスト	AWS Network Firewall エンドポイントコスト + データ処理料金	Gateway Load Balancer + Gateway Load Balancer エンドポイント + 仮想アプライアンス + データ処理料金

集中インバウンド検査

インターネット向けアプリケーションは、その性質上、攻撃対象領域が大きく、他のほとんどのタイプのアプリケーションが直面する必要がない脅威のカテゴリにさらされます。これらのタイプのアプリケーションに対する攻撃から必要な保護を行い、影響領域を最小限に抑えることは、セキュリティ戦略の中核です。

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が、パブリックインターネット (コンテンツ配信ネットワーク (CDN) 経由、パブリック向けウェブアプリケーション経由など) 経由で、パブリック向けロードバランサー、API ゲートウェイ経由で、またはインターネットゲートウェイ経由で直接アクセスされます。この場合、インバウンドアプリケーション検査に AWS Web Application Firewall (AWS WAF) を使用するか、Gateway Load Balancer または を使用して IDS/IPS インバウンド検査を使用して、ワークロードとアプリケーションを保護できます AWS Network Firewall。

ランディングゾーンにアプリケーションをデプロイし続けると、インバウンドインターネットトラフィックを検査する必要がある場合があります。これを実現するには、サードパーティーのファイアウォールアプライアンスを実行する Gateway Load Balancer を使用する分散型、集中型、または複合型の検査アーキテクチャを使用するか、オープンソースの Suricata ルールを使用して AWS Network Firewall 高度な DPI および IDS/IPS 機能を使用します。このセクションでは、トラフィックをルーティングするための中央ハブ AWS Transit Gateway として機能する を使用した、一元化されたデプロイ AWS Network Firewall における Gateway Load Balancer と の両方について説明します。

AWS WAF インターネットからのインバウンドトラフィックを検査 AWS Firewall Manager するための および

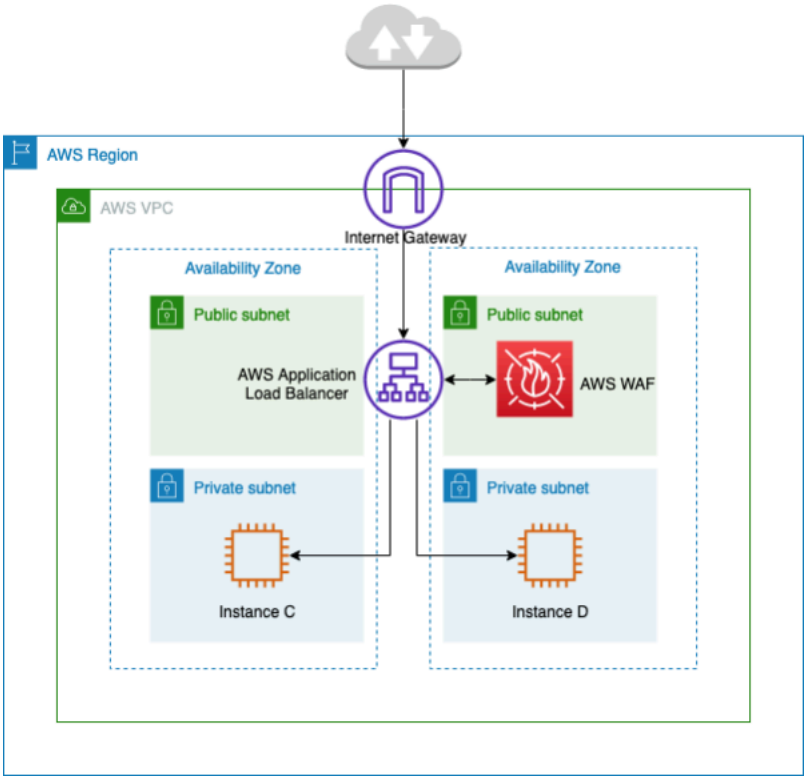
AWS WAF は、可用性に影響を与えたり、セキュリティを侵害したり、過剰なリソースを消費したりする可能性のある一般的なウェブエクスプロイトやボットからウェブアプリケーションまたは APIs を保護するウェブアプリケーションファイアウォールです。 AWS WAF は、ボットトラフィックを制御し、SQL インジェクションやクロスサイトスクリプティング (XSS) などの一般的な攻撃パターンをブロックするセキュリティルールを作成できるようにすることで、トラフィックがアプリケーションに到達する方法を制御できるようにします。特定のトラフィックパターンを除外するルールをカスタマイズすることもできます。

CDN ソリューション、ウェブサーバーをフロントする Application Load Balancer、REST API 用の Amazon API Gateway、または GraphQL APIs AWS AppSync の一部として Amazon AWS WAF Amazon CloudFront にデプロイできます。 APIs

デプロイしたら AWS WAF、ビジュアルルールビルダー、JSON のコード、 が管理するマネージドルールを使用して独自のトラフィックフィルタールールを作成したり AWS、 からサードパーティールールをサブスクライブしたりできます AWS Marketplace。これらのルールは、指定されたパターンに対してトラフィックを評価することで、不要なトラフィックを除外できます。Amazon CloudWatch をさらに使用して、受信トラフィックメトリクスとログ記録をモニタリングできます。

のすべてのアカウントとアプリケーションを一元管理するために AWS Organizations、 を使用できます AWS Firewall Manager。 AWS Firewall Manager は、ファイアウォールルールを一元的に設定および管理できるセキュリティ管理サービスです。新しいアプリケーションが作成されると、 は、一般的な一連のセキュリティルールを適用することで、新しいアプリケーションとリソースを簡単にコンプライアンスに取り込む AWS Firewall Manager ことができます。

を使用すると AWS Firewall Manager、Application Load Balancer、API Gateway インスタンス、Amazon CloudFront distributions. AWS Firewall Manager integrates AWS マネージドルール for の AWS WAF ルールを簡単にロールアウトできます。これにより AWS WAF、事前設定済みの厳選された AWS WAF ルールをアプリケーションに簡単にデプロイできます。 AWS WAF による一元管理の詳細については AWS Firewall Manager、「Centrally manage AWS WAF (API v2) and AWS マネージドルール at scale with AWS Firewall Manager」を参照してください。



を使用した一元的なインバウンドトラフィック検査 AWS WAF

前述のアーキテクチャでは、アプリケーションはプライベートサブネットの複数のアベイラビリティーゾーンの Amazon EC2 インスタンスで実行されています。Amazon EC2 インスタンスの前に公開されている Application Load Balancer (ALB) がデプロイされ、異なるターゲット間でリクエストをロードバランシングします。は AWS WAF ALB に関連付けられています。

利点

- AWS WAF Bot Control を使用すると、アプリケーションへの一般的および広範なボットトラフィックを可視化して制御できます。
- の マネージドルール AWS WAFを使用すると、ウェブアプリケーションまたは APIs をすばやく開始し、一般的な脅威から保護できます。Open Web Application Security Project (OWASP) Top 10 セキュリティリスク、WordPress や Joomla などのコンテンツ管理システム (CMS) に固有の脅威、新しい共通脆弱性識別子 (CVE) などの問題に対処するルールタイプから選択できます。マネージドルールは、新しい問題が発生すると自動的に更新されるため、アプリケーションの構築により多くの時間を費やすことができます。
- AWS WAF はマネージドサービスであり、このアーキテクチャの検査にアプライアンスは必要ありません。さらに、Amazon Data Firehose を介してほぼリアルタイムのログを提供します。AWS WAF はウェブトラフィックをほぼリアルタイムで可視化し、Amazon CloudWatch で新しいルールやアラートを作成するために使用できます。

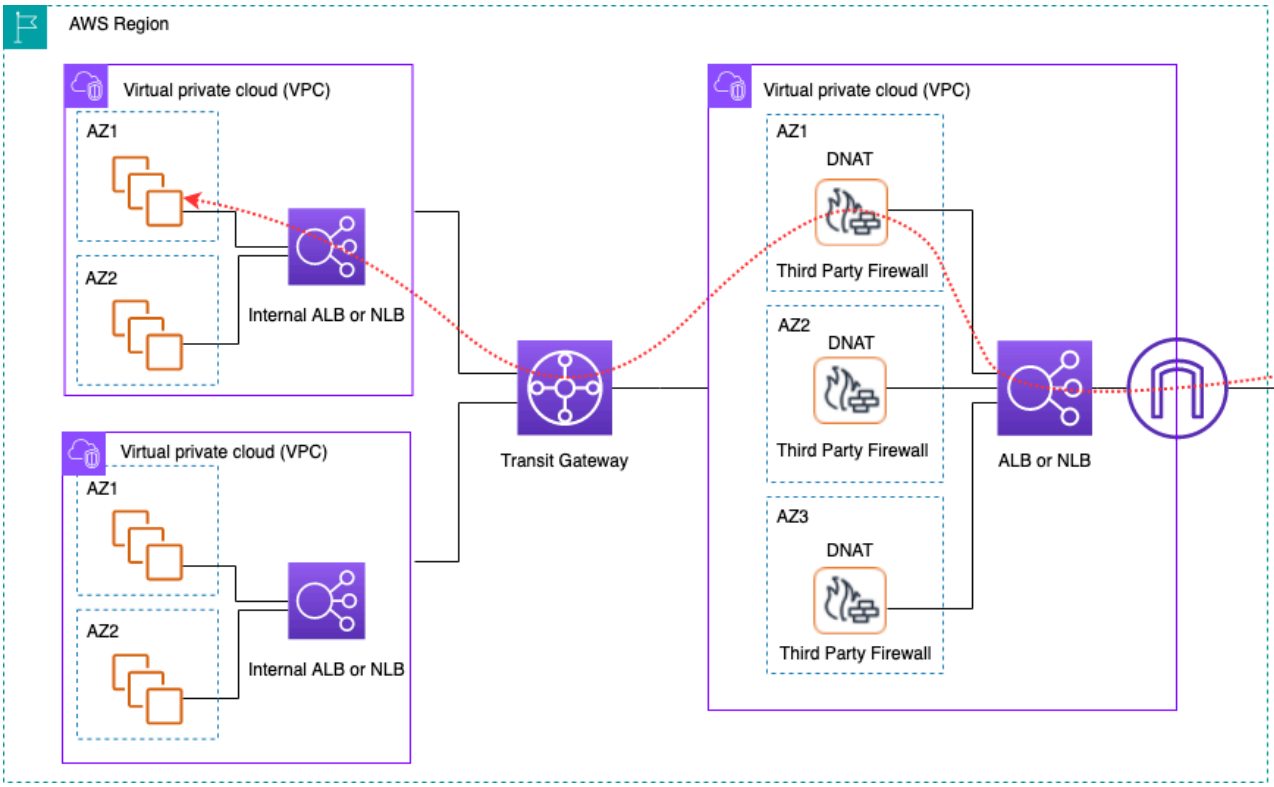
主な考慮事項

- このアーキテクチャは、ALB、CloudFront ディストリビューション、API Gateway ごとに AWS WAF が統合されているため、HTTP ヘッダー検査と分散検査に最適です。 AWS WAF はリクエスト本文を口グに記録しません。
- ALB の 2 番目のセット (存在する場合) に向かうトラフィックは、ALB の 2 番目のセットに新しいリクエストが行われるため、同じ AWS WAF インスタンスによって検査されない場合があります。

サードパーティーアプライアンスによる一元的なインバウンド検査

このアーキテクチャ設計パターンでは、別の検査 VPC の Application/Network Load Balancer など、Elastic Load Balancer (ELB) の背後にある複数のアベイラビリティーゾーンに、サードパーティーのファイアウォールアプライアンスを Amazon EC2 Load Balancer にデプロイします。

検査 VPC と他のスポーク VPCsは、VPC アタッチメントとして Transit Gateway を介して接続されます。スポーク VPCs のアプリケーションは、内部 ELB によるフロントエンドであり、アプリケーションタイプに応じて ALB または NLB のいずれかになります。インターネット経由のクライアントは、Firewall アプライアンスの 1 つにトラフィックをルーティングする検査 VPC 内の外部 ELB の DNS に接続します。Firewall はトラフィックを検査し、次の図に示すように内部 ELB の DNS を使用して Transit Gateway を介してスポーク VPC にトラフィックをルーティングします。サードパーティーアプライアンスを使用したインバウンドセキュリティ検査の詳細については、AWS 環境ブログ記事の「サードパーティーファイアウォールアプライアンスを AWS 環境に統合する方法」を参照してください。



サードパーティーのアプライアンスと ELB を使用した一元的な進入トラフィック検査

利点

- このアーキテクチャは、サードパーティーのファイアウォールアプライアンスを通じて提供される検査および高度な検査機能の任意のアプリケーションタイプをサポートできます。
- このパターンでは、ファイアウォールアプライアンスからスポーク VPCs への DNS ベースのルーティングがサポートされているため、スポーク VPCs 内のアプリケーションは ELB の背後で個別にスケーリングできます。

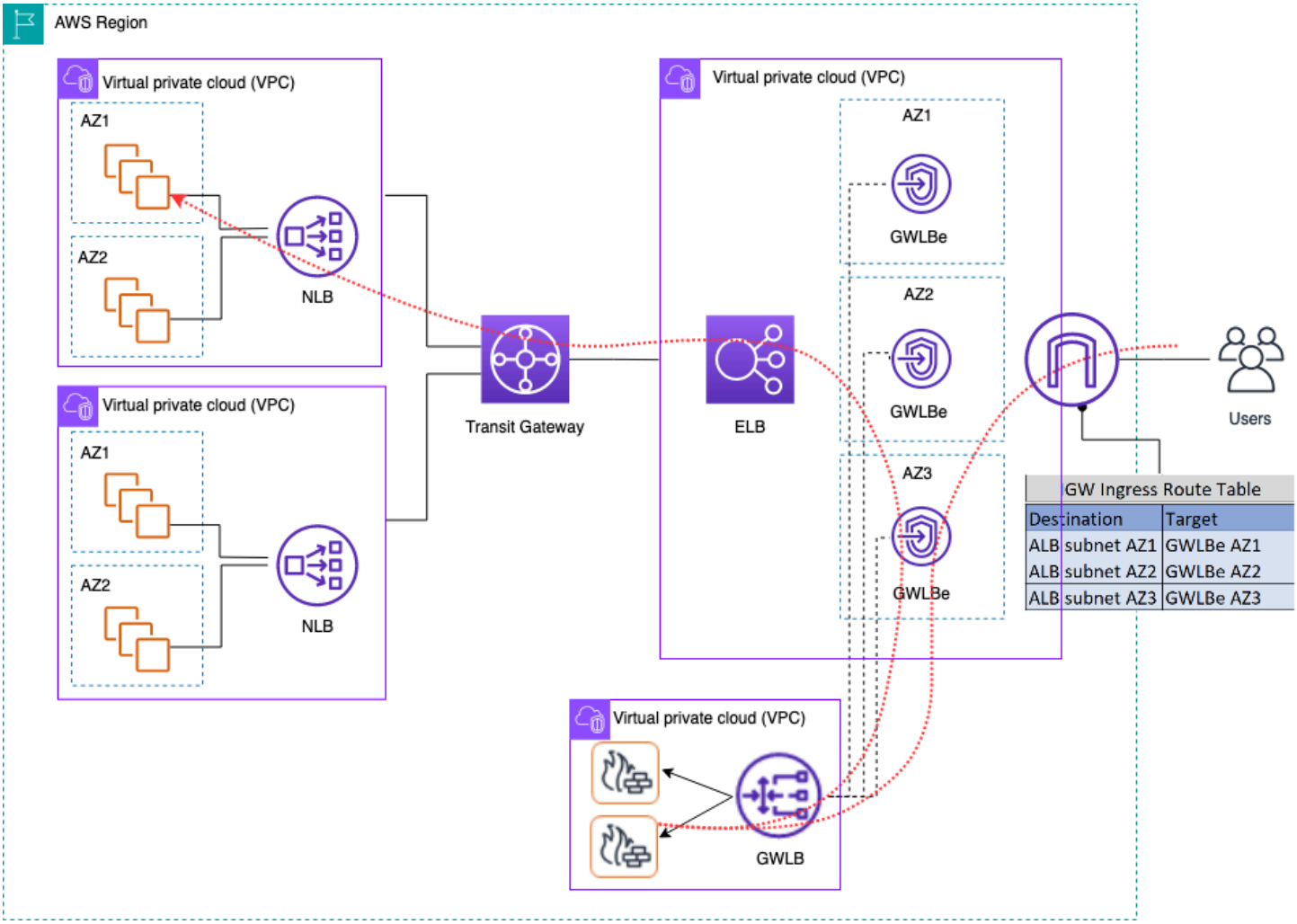
- ELB で Auto Scaling を使用して、検査 VPC 内のファイアウォールアプライアンスをスケーリングできます。

主な考慮事項

- 高可用性を実現するには、複数のファイアウォールアプライアンスをアベイラビリティーゾーンにデプロイする必要があります。
- フロー対称性を維持するために、ファイアウォールを で設定し、ソース NAT を実行する必要があります。つまり、クライアント IP アドレスはアプリケーションに表示されません。
- ネットワークサービスアカウントに Transit Gateway とインスペクション VPC をデプロイすることを検討してください。
- サードパーティーベンダーのファイアウォールのライセンス/サポートの追加コスト。Amazon EC2 の料金はインスタンスタイプによって異なります。

Gateway Load Balancer でファイアウォールアプライアンスを使用してインターネットからのインバウンドトラフィックを検査する

お客様は、多層防御戦略の一環として、サードパーティーの次世代ファイアウォール (NGFW) と侵入防止システム (IPS) を使用します。 通常、これらはハードウェアまたはソフトウェア/仮想アプライアンス専用です。Gateway Load Balancer を使用すると、次の図に示すように、これらの仮想アプライアンスを水平方向にスケーリングして、VPC との間で送受信されるトラフィックを検査できます。



Gateway Load Balancer でファイアウォールアプライアンスを使用した一元的な進入トラフィック検査

前述のアーキテクチャでは、Gateway Load Balancer エンドポイントは個別のエッジ VPC 内の各アベイラビリティーゾーンにデプロイされます。次世代ファイアウォール、侵入防止システムなどは、一元化されたアプライアンス VPC の Gateway Load Balancer の背後にデプロイされます。このアプライアンス VPC は、スポーク VPCs と同じ AWS アカウントまたは異なる AWS アカウント内に配置できます。仮想アプライアンスは Auto Scaling グループを使用するように設定でき、Gateway Load Balancer に自動的に登録されるため、セキュリティレイヤーの自動スケーリングが可能になります。

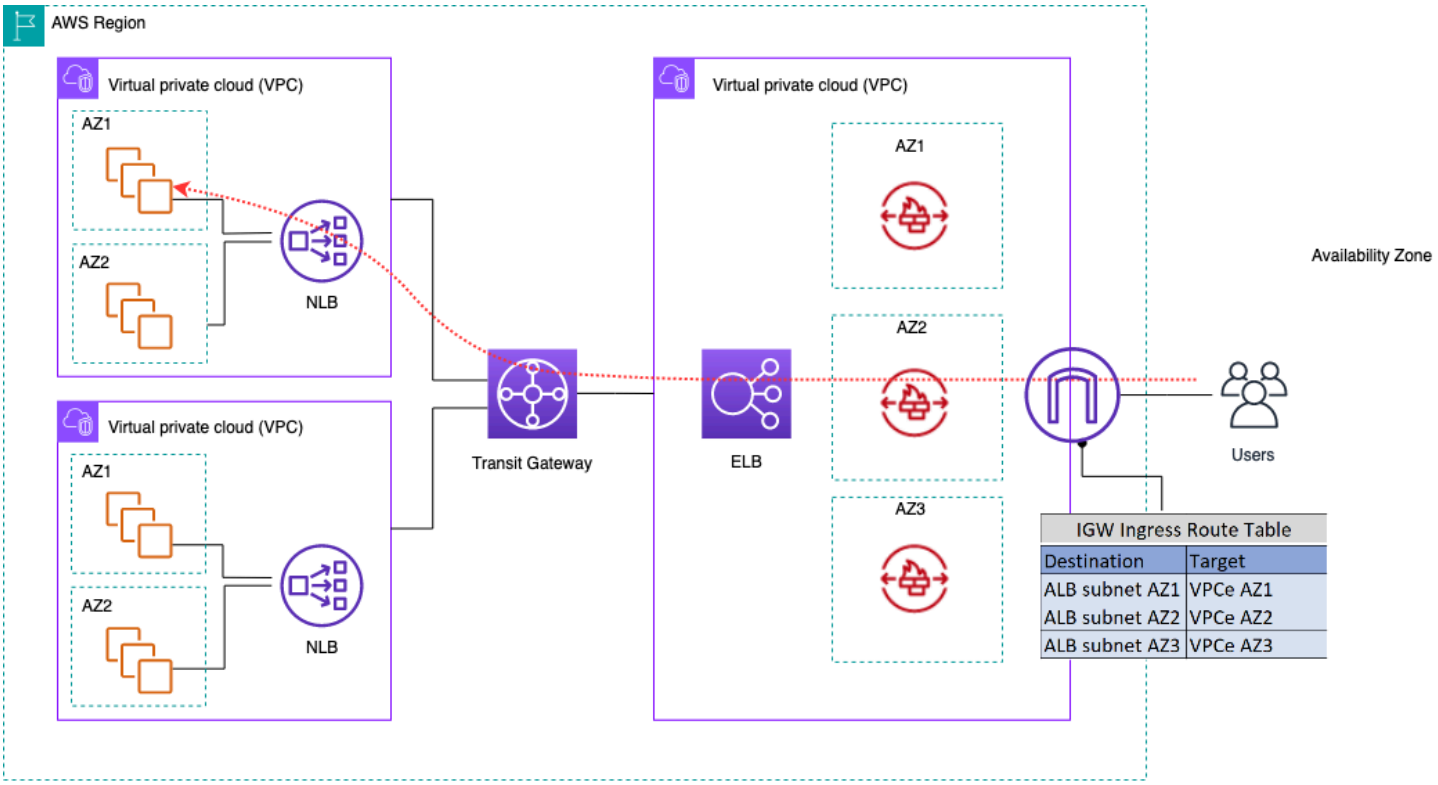
これらの仮想アプライアンスは、インターネットゲートウェイ (IGW) を介して管理インターフェイスにアクセスするか、アプライアンス VPC の踏み台ホスト設定を使用して管理できます。

VPC イングレスルーティング機能を使用して、エッジルートテーブルが更新され、インバウンドトラフィックがインターネットから Gateway Load Balancer の背後にあるファイアウォールアプライ

アンスにルーティングされます。検査されたトラフィックは、Gateway Load Balancer エンドポイントを介してターゲット VPC インスタンスにルーティングされます。Gateway Load Balancer を使用するさまざまな方法の詳細については、「AWS Gateway Load Balancer の紹介: サポートされているアーキテクチャパターン」ブログ記事を参照してください。 Load Balancer

集中進入 AWS Network Firewall に を使用する

このアーキテクチャでは、残りの VPC に到達する AWS Network Firewall 前に、イングレストラフィックが によって検査されます。 VPCs この設定では、トラフィックは Edge VPC にデプロイされたすべてのファイアウォールエンドポイントに分割されます。ファイアウォールエンドポイントと Transit Gateway サブネットの間にパブリックサブネットをデプロイします。ALB または NLB を使用できます。これには、スポーク VPCsながら、スポーク VPC に IP ターゲットが含まれます。 Auto Scaling



AWS Network Firewall を使用したイングレストラフィック検査

このモデル AWS Network Firewall での のデプロイと管理を簡素化するために、 AWS Firewall Manager を使用できます。Firewall Manager を使用すると、一元化された場所で作成した保護を複数のアカウントに自動的に適用することで、さまざまなファイアウォールを一元管理できます。Firewall Manager は、Network Firewall の分散デプロイモデルと集中デプロイモデルの両方をサ

ポートしています。ブログ記事「AWS Network Firewall を使用してデプロイする方法 AWS Firewall Manager」には、モデルの詳細が記載されています。

を使用したディープパケットインスペクション (DPI) AWS Network Firewall

Network Firewall は、イングレストラフィックに対してディープパケットインスペクション (DPI) を実行できます。Network Firewall は、 AWS Certificate Manager (ACM) に保存されている Transport Layer Security (TLS) 証明書を使用して、パケットの復号、DPI の実行、パケットの再暗号化を行うことができます。Network Firewall で DPI を設定する際の考慮事項がいくつかあります。まず、信頼できる TLS 証明書を ACM に保存する必要があります。次に、復号化と再暗号化のためにパケットを正しく送信するように Network Firewall ルールを設定する必要があります。詳細については、ブログ記事「暗号化されたトラフィックの TLS 検査設定」および AWS Network Firewall「」を参照してください。

一元化された進入アーキテクチャ AWS Network Firewall における の主な考慮事項

- Edge VPC の Elastic Load Balancing は、IP アドレスをホスト名ではなくターゲットタイプとしてのみ持つことができます。前の図では、ターゲットはスポーク VPC の Network Load Balancer のプライベート IPs です。 VPCs エッジ VPC で ELB の背後にある IP ターゲットを使用すると、Auto Scaling が失われます。
- ファイアウォールエンドポイントに を 1 つの時間枠 AWS Firewall Manager として使用することを検討してください。
- このデプロイモデルは、エッジ VPC に入ると同時にトラフィック検査を使用するため、検査アーキテクチャの全体的なコストを削減できる可能性があります。

DNS

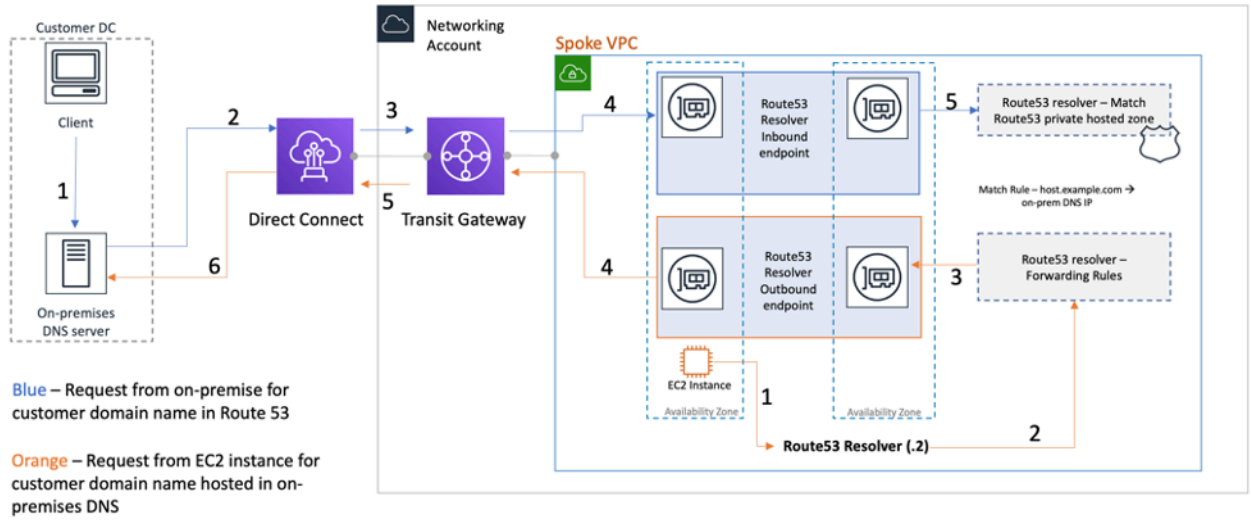
デフォルトの VPC を除く VPC でインスタンスを起動すると、 は、VPC に指定した DNS 属性 とインスタンスにパブリック IPv4 アドレスがあるかどうかに応じて、プライベート DNS ホスト名 (場合によってはパブリック DNS ホスト名) をインスタンス AWS に提供します。 `enableDnsSupport` 属性が に設定されている場合`true`、Route 53 Resolver (+2 IP オフセットから VPC CIDR) から VPC 内の DNS 解決を取得します。デフォルトでは、Route 53 Resolver は EC2 インスタンスまたは Elastic Load Balancing ロードバランサーのドメイン名などの VPC ドメイン名の DNS クエリに応答します。VPC ピアリングを使用すると、1 つの VPC のホストは、パブリック DNS ホスト名をピア接続された VPCs 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。ただし、そのオプションが有効になっている場合です。経由で接続VPCs にも同じことが当てはまります AWS Transit Gateway。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 DNS-to-IP-mapping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の DNS クエリにどのように応答するかに関する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経由で解決可能な DNS 情報が含まれていますが、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 VPCs にのみ情報を表示する特定の実装です。複数の VPCs または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、単一のプライベートホストゾーンを AWS アカウント間およびリージョン間で複数の VPCs に関連付けることができます (SDK/CLI/API でのみ可能) 。VPCs のエンドホストは、DNS クエリのネームサーバーとしてそれぞれの Route 53 Resolver IP (+2 offset the VPC CIDR) を使用します。VPC 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

DNS は、ハイブリッドなどのインフラストラクチャの重要なコンポーネントであり、アプリケーションが依存するhostname-to-IP-address解決を提供します。ハイブリッド環境を実装しているお客様は、通常、DNS 解決システムがすでに導入されており、現在のシステムと連携する DNS ソリューションが必要です。ネイティブ Route 53 リゾルバー (ベース VPC CIDR の +2 オフセット) は、VPN または を使用してオンプレミスネットワークから到達できません Direct Connect。したがって、AWS リージョンの VPCs の DNS をネットワークの DNS と統合する場合は、Route 53 Resolver インバウンドエンドポイント (VPCs に転送する DNS クエリの場合) と Route 53 Resolver アウトバウンドエンドポイント (VPCs からネットワークに転送するクエリの場合) が必要です。

次の図に示すように、VPC の Amazon EC2 インスタンスから受信したクエリをネットワーク上の DNS サーバーに転送 VPCs 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 からオンプレミスネットワークに転送するには、転送する DNS クエリのドメイン名 (example.com など) と、クエリを転送するネットワーク上の DNS リゾルバーの IP アドレスを指定する Route 53 Resolver ルールを作成します。オンプレミスネットワークから 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、指定された VPC 内のインバウンドリゾルバーエンドポイントにクエリを転送できます。



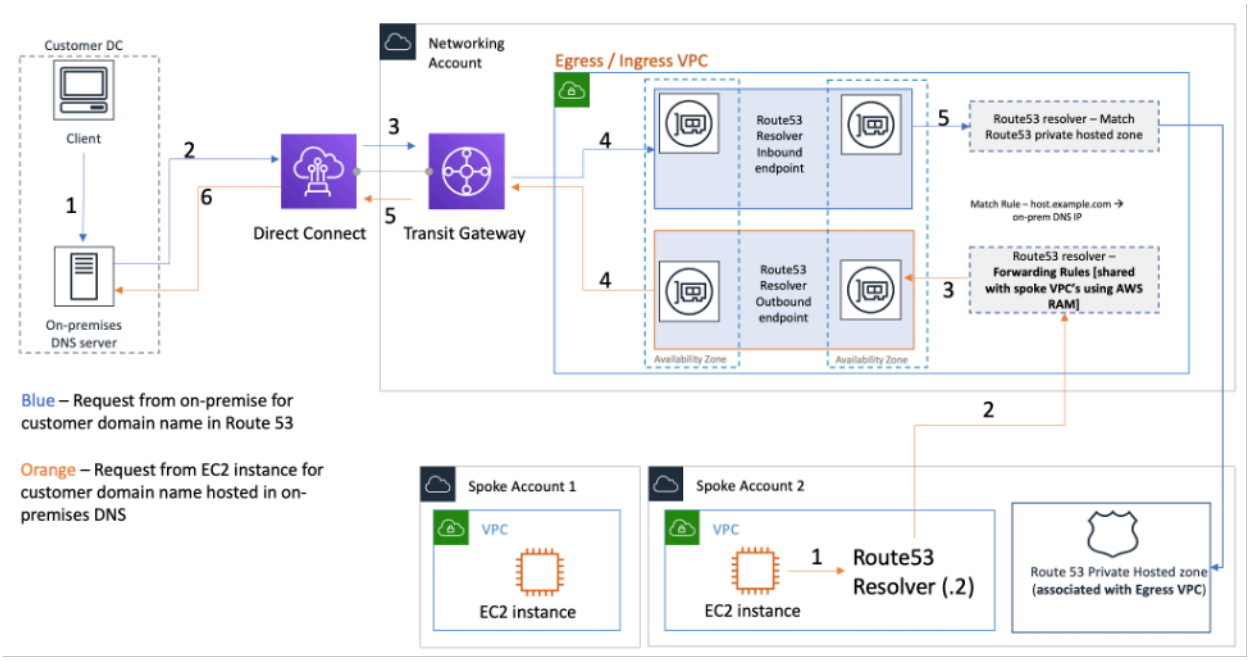
Route 53 Resolver を使用したハイブリッド DNS 解決

これにより、オンプレミスの DNS リゾルバーは、その VPC に関連付けられた Route 53 プライベートホストゾーンの Amazon EC2 インスタンスやレコードなど、AWS リソースのドメイン名を簡単に解決できます。さらに、Route 53 Resolver エンドポイントは ENI あたり 1 秒あたり最大約 10,000 件のクエリを処理できるため、 ははるかに大きな DNS クエリボリュームに簡単にスケールできます。詳細については、Amazon Route 53 ドキュメントの「リゾルバーのベストプラクティス」を参照してください。

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。中央出力 VPC (ネットワークサービスアカウント) に一元化します。このアプローチにより、コストを抑えながら管理しやすくなります (作成したインバウンド/アウトバウンドリゾルバーエンドポイントごとに時間単位の料金が課金されます)。一元化されたインバウンドエンドポイントと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の部分と共有します。

- アウトバウンド解決 — Network Services アカウントを使用して、リゾルバールールを書き込みます (DNS クエリがオンプレミスの DNS サーバーに転送される基準に基づく)。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と共有します (アカウント内の VPCsと関連付けます)。スポーク VPCs 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 Egress VPC のアウトバウンド Route 53 Resolver エンドポイントを介してオンプレミス DNS サーバーに転送します。 スポーク VPCs を出力 VPC にピア接続したり、Transit Gateway 経由で接続したりする必要はありません。スポーク VPCs のプライマリ DNS としてアウトバウンドリゾルバーエンドポイントの IP を使用しないでください。スポーク VPCs、VPC で Route 53 Resolver (VPC CIDR のオフセット) を使用する必要があります。



Route 53 Resolver エンドポイントを Ingress/Egress VPC に一元化する

- 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、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この一元化された VPC に関連付けます。詳細については、「より多くの VPCs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。前の図に示すように、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、任意のプライベートホストゾーン (中央 VPC に関連) のエントリの DNS を解決できます。ハイブリッド DNS 設定の詳細については、「Amazon Route 53 と AWS Transit Gateway によるハイブリッドクラウドの一元化された DNS 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。

Route 53 DNS ファイアウォール

Amazon Route 53 Resolver DNS Firewall はVPCs のアウトバウンド DNS トラフィックをフィルタリングおよび規制するのに役立ちます。DNS Firewall の主な用途は、VPC 内のリソースが、組織が信頼するサイトに対してのみアウトバウンド DNS リクエストを実行できるようにするドメイン名の許可リストを定義することで、データの流出を防ぐことです。また、VPC 内のリソースが DNS 経由で通信したくないドメインのブロックリストを作成することもできます。 Amazon Route 53 Resolver DNS ファイアウォールには次の機能があります。

お客様は、DNS クエリの応答方法を定義するルールを作成できます。ドメイン名に定義できるアクションには、NODATA、、 OVERRIDE などがありますNXDOMAIN。

お客様は、許可リストと拒否リストの両方のアラートを作成して、ルールアクティビティをモニタリングできます。これは、顧客がルールを本番環境に移行する前にテストする場合に便利です。

詳細については、「Amazon VPC Amazon Route 53 Resolver 用 DNS ファイアウォールの開始方法」ブログ記事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一元化されたアクセス

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、NAT デバイス、VPN 接続、または 接続を必要とせずに、サポートされている AWS のサービスに VPC をプライベート Direct Connect に接続できます。したがって、VPC はパブリックインターネットに公開されません。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と AWS サービスエンドポイントと通信できます。VPC と他の サービス間のトラフィックは、AWS ネットワークバックボーンを離れません。VPC エンドポイントは仮想デバイスです。これらは水平にスケールされ、冗長で、可用性の高い VPC コンポーネントです。現在、インターフェイスエンドポイント (を使用AWS PrivateLink) とゲートウェイエンドポイントの 2 種類の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を使用して、Amazon S3 および Amazon DynamoDB サービスにプライベートにアクセスできます。ゲートウェイエンドポイントは追加料金なしで使用できます。データ転送とリソースの使用量に対する標準料金が適用されます。

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、サポートされている AWS サービス宛てのトラフィックのエントリポイントとして機能するプライベート IP アドレスを持つ 1 つ以上の Elastic Network Interface で構成されます。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、エンドポイントが実行されている 1 時間ごとに、データ処理料金とともにコストが発生します。デフォルトでは、 AWS サービスにアクセスするすべての VPC にインターフェイスエンドポイントを作成します。これは、お客様が複数の VPCs で特定の AWS サービスとやり取りしたいという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、管理が難しい場合があります。これを回避するには、一元化された 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 VPCsは、Transit Gateway を介してこれらの一元化されたエンドポイントを使用します。

AWS 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 を有効にできます。有効にすると、AWS マネージド Route 53 プライベートホストゾーン (PHZ) が作成されます。これにより、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。この設定では、スポーク VPCs が集中型 VPC でホストされている VPC エンドポイント DNS を解決できるようにすると、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。次に、サービスエンドポイント名と一致する Route 53 プライベートホストゾーンを手動で

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 エンドポイント名を持つエイリアスレコードを追加します。

1. にログイン AWS マネジメントコンソール し、Route 53 に移動します。
2. プライベートホストゾーンを選択し、レコードの作成に移動します。
3. レコード名フィールドに値を入力し、レコードタイプを A として選択し、エイリアスを有効にします。

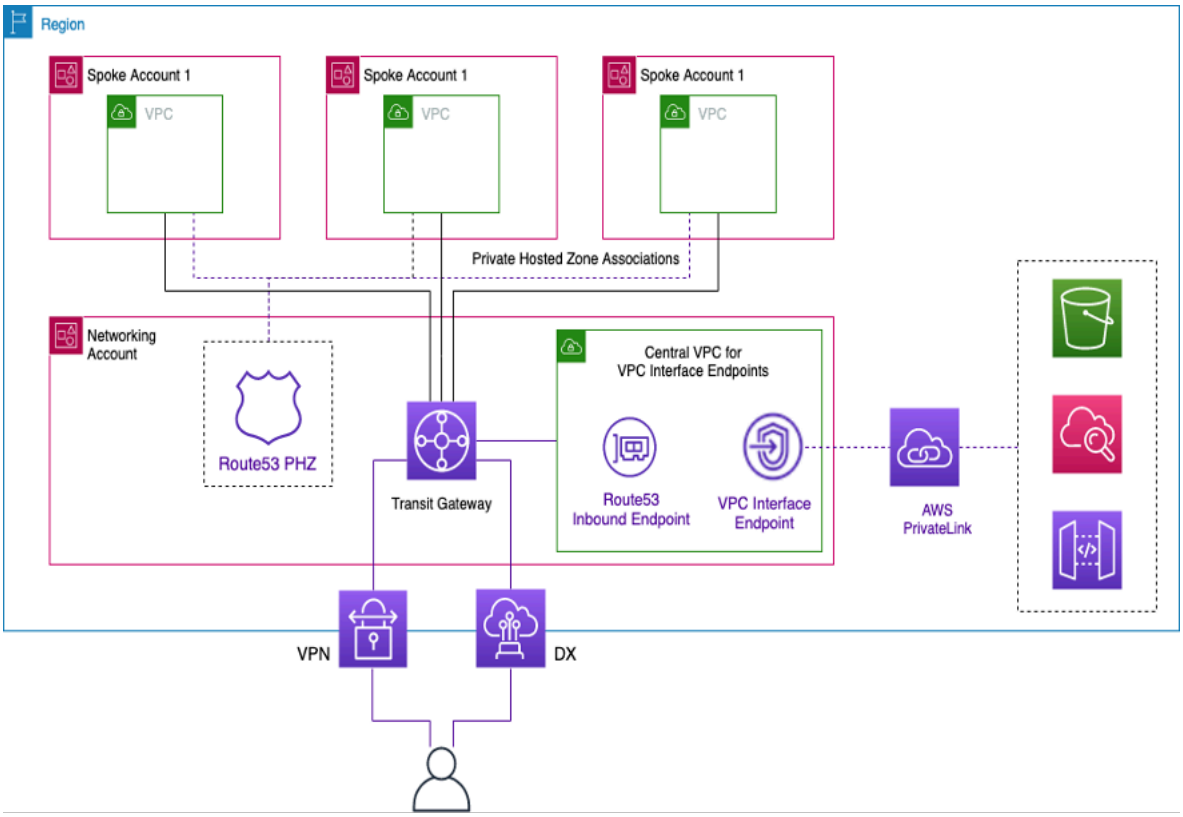
   Docker や OCI クライアントエンドポイント (`dkr.ecr`) などの一部のサービスでは、レコード名にワイルドカードエイリアス (*) を使用する必要があります。
4. 「Route Traffic to」セクションで、トラフィックの送信先のサービスを選択し、ドロップダウンリストからリージョンを選択します。
5. 適切なルーティングポリシーを選択し、ターゲットの状態を評価するオプションを有効にします。

このプライベートホストゾーンをランディングゾーン内の他の VPCs に関連付けます。この設定により、スポーク VPCs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 VPCs のホストが VPC の Route 53 Resolver 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 Resolver インバウンドエンドポイントに送信します。これにより、プライベートホストゾーンに従って DNS リクエストが解決されます。

次の図では、Transit Gateway はスポーク VPCs 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のスポーク VPCs と共有します。エンドポイント情報を他の VPCs「Integrating AWS Transit Gateway with AWS PrivateLink and Amazon Route 53 Resolver」を参照してください。

> **Note**
>
> 分散 VPC エンドポイントアプローチ、つまり VPC あたりのエンドポイントでは、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上のすべてのスポーク VPC アクセスにポリシーを適用および管理します。VPCs の数が増えるにつれて、1 つのポリシードキュメントで最小特権を維持する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、ブラスト半径も大きくなります。また、ポリシードキュメントのサイズ (20,480 文字) も制限されます。



インターフェイス VPC エンドポイントの一元化

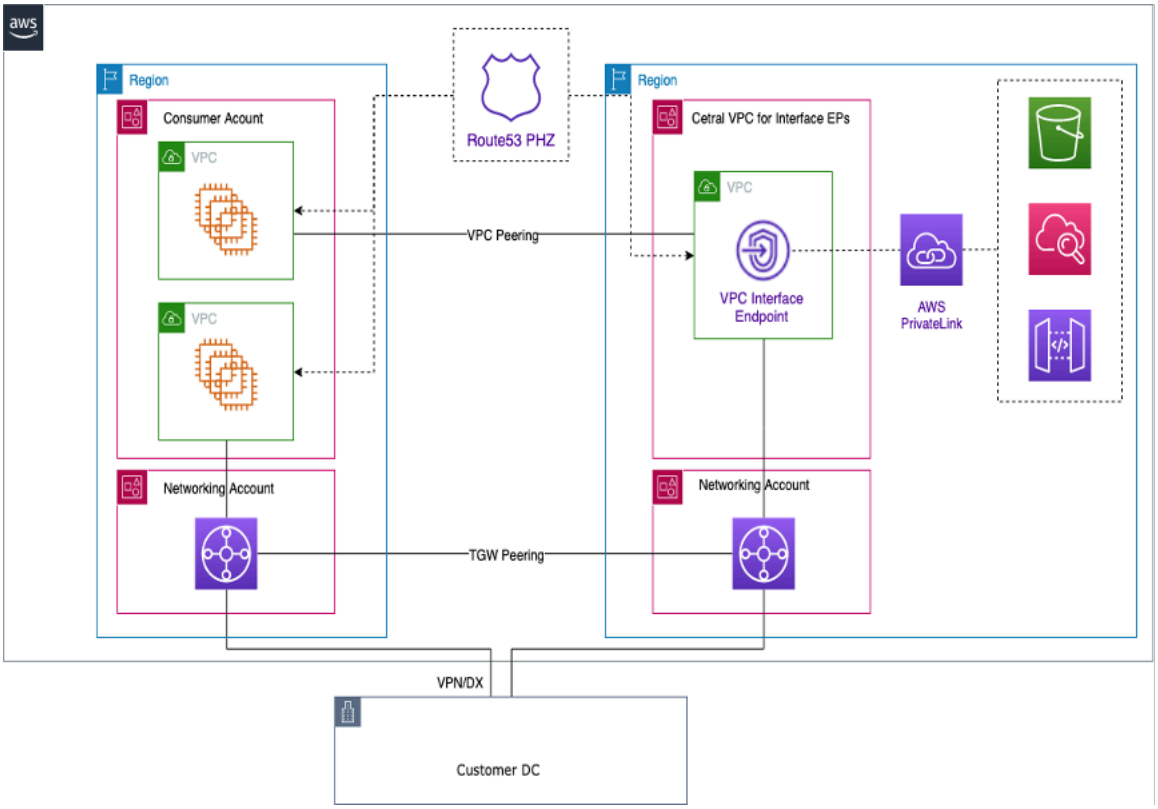
クロスリージョンエンドポイントアクセス

共通の VPCs エンドポイントを共有する異なるリージョンに複数の VPC を設定する場合は、前述のように PHZ を使用します。各リージョンの両方VPCs は、エンドポイントのエイリアスを持つ PHZ に関連付けられます。マルチリージョンアーキテクチャの VPCs 間でトラフィックをルーティングするには、各リージョンの Transit Gateway をピアリング接続する必要があります。詳細について

は、ブログ「クロスアカウントマルチリージョンアーキテクチャに Route 53 プライベートホストゾーンを使用する」を参照してください。

異なるリージョンVPCs は、Transit Gateway または VPC ピアリングを使用して相互にルーティングできます。Transit Gateway のピアリングには、次のドキュメントを使用します。Transit Gateway ピアリングアタッチメント。

この例では、VPC us-west-1リージョンの Amazon EC2 インスタンスは PHZ を使用してus-west-2リージョン内のエンドポイントのプライベート IP アドレスを取得し、Transit Gateway ピアリングまたは VPC ピアリングを介してus-west-2リージョン VPC にトラフィックをルーティングします。このアーキテクチャを使用すると、トラフィックは AWS ネットワーク内にとどまり、 の EC2 インスタンスがインターネットを経由us-west-2せずに の VPC サービスus-west-1に安全にアクセスできます。



マルチリージョン VPC エンドポイント

> **Note**
>
> リージョン間のデータ転送料金は、リージョン間でエンドポイントにアクセスする場合に適用されます。

前の図を参照すると、エンドポイントサービスは us-west-2リージョンの VPC に作成されます。このエンドポイントサービスは、そのリージョンの AWS サービスへのアクセスを提供します。別のリージョン (などus-east-1) のインスタンスがus-west-2リージョンのエンドポイントにアクセスするには、目的の VPC エンドポイントへのエイリアスを使用して PHZ にアドレスレコードを作成する必要があります。

まず、各リージョンの VPCs が、作成した PHZ に関連付けられていることを確認します。

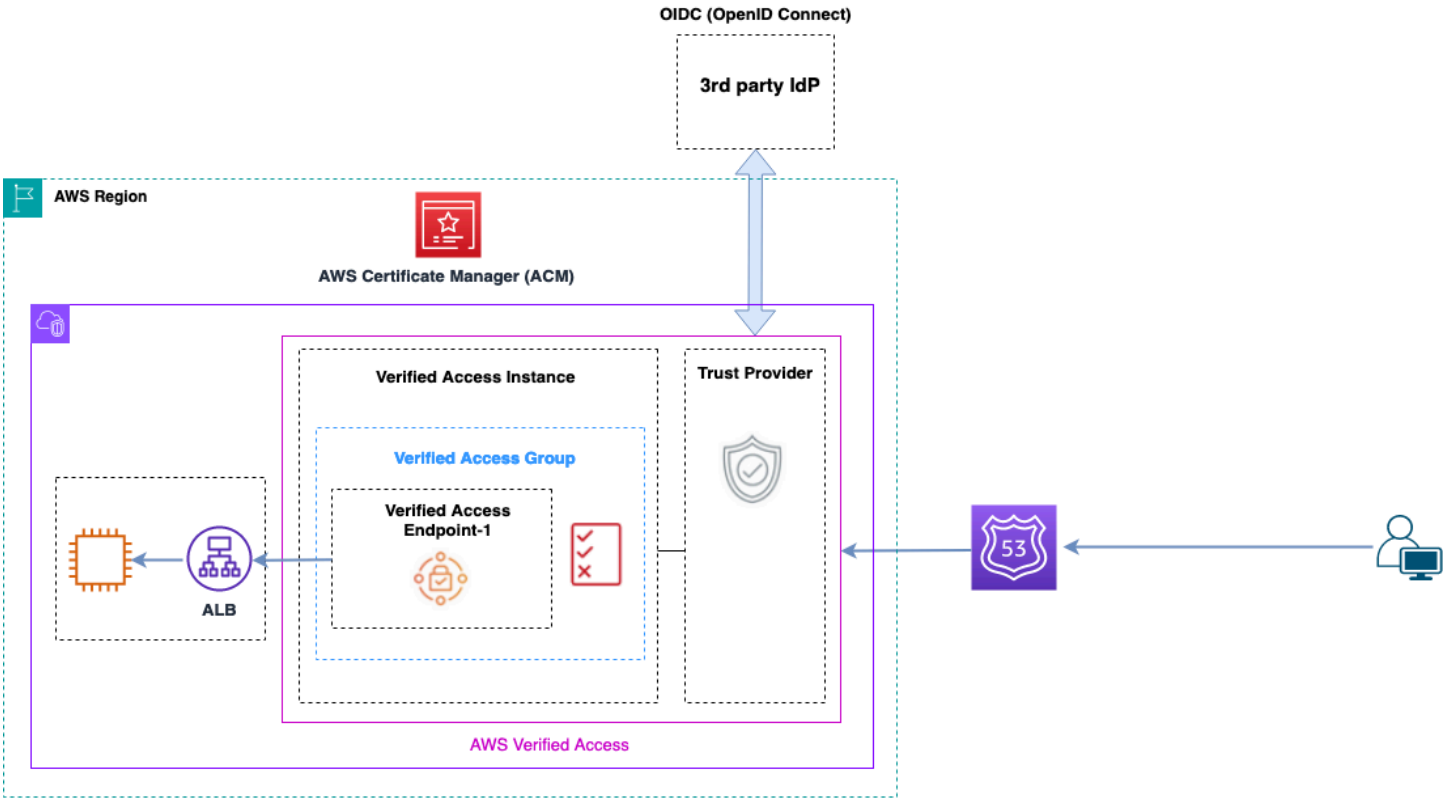
エンドポイントを複数のアベイラビリティーゾーンにデプロイする場合、DNS から返されるエンドポイントの IP アドレスは、割り当てられたアベイラビリティーゾーン内のサブネットのいずれかからのものです。

エンドポイントを呼び出すときは、PHZ にある完全修飾ドメイン名 (FQDN) を使用します。

AWS Verified Access

AWS Verified Access は、VPN なしでプライベートネットワーク内のアプリケーションへの安全なアクセスを提供します。ID、デバイス、場所などのリクエストをリアルタイムで評価します。このサービスは、アプリケーションのポリシーに基づいてアクセスを許可し、組織のセキュリティを強化することでユーザーを接続します。Verified Access は、アイデンティティ対応リバースプロキシとして機能することで、プライベートアプリケーションへのアクセスを提供します。ユーザー ID とデバイスの状態は、該当する場合、トラフィックをアプリケーションにルーティングする前に実行されます。

次の図は、Verified Access の仕組みの大まかな概要を示しています。ユーザーはアプリケーションへのアクセス要求を送信します。Verified Access は、グループのアクセスポリシーおよびアプリケーション固有のエンドポイントポリシーと照らし合わせてリクエストを評価します。Access が許可されている場合、リクエストはエンドポイントを介してアプリケーションに送信されます。



Verified Access の概要

AWS Verified Access アーキテクチャの主なコンポーネントは次のとおりです。

- Verified Access インスタンス — インスタンスはアプリケーションリクエストを評価し、セキュリティ要件が満たされた場合にのみアクセス権を付与します。
- Verified Access エンドポイント — 各エンドポイントはアプリケーションを表します。エンドポイントは、NLB、ALB、またはネットワークインターフェイスです。
- Verified Access グループ — Verified Access エンドポイントのコレクション。同様のセキュリティ要件を持つアプリケーションのエンドポイントをグループ化し、ポリシー管理を簡素化することをお勧めします。
- アクセスポリシー — アプリケーションへのアクセスを許可するか拒否するかを決定するユーザー定義のルール。
- 信頼プロバイダー – Verified Access は、ユーザー ID とデバイスのセキュリティ状態の管理を容易にするサービスです。これは、 とサードパーティーの信頼プロバイダーの両方 AWS と互換性があり、各 Verified Access インスタンスに少なくとも 1 つの信頼プロバイダーをアタッチする必要があります。これらの各インスタンスには、単一の ID 信頼プロバイダーと複数のデバイス信頼プロバイダーを含めることができます。

- 信頼データ – ユーザーの E メールアドレスや属するグループなど、信頼プロバイダーが Verified Access に送信するセキュリティデータは、アプリケーションリクエストを受信するたびにアクセスポリシーに対して評価されます。

詳細については、Verified Access ブログ記事を参照してください。

結論

AWS Landing Zone でアプリケーションの使用をスケール AWS してデプロイすると、VPCsとネットワークコンポーネントの数が増加します。このホワイトペーパーでは、この成長するインフラストラクチャを管理し、コストを抑えながらスケーラビリティ、高可用性、セキュリティを確保する方法について説明します。Transit Gateway、共有 VPC、、VPC エンドポイント Direct Connect、Gateway Load Balancer、Amazon Route 53 AWS Network Firewall、サードパーティー製ソフトウェアアプライアンスなどのサービスを使用する際に、適切な設計上の意思決定を行うことが重要になります。各アプローチの主な考慮事項を理解し、要件から逆算して、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寄稿者は次のとおりです。

- Amazon Web Services、ソリューションアーキテクト、Sohaib Tahir
- Shirin Bhambhani、Amazon Web Services、ソリューションアーキテクト
- Amazon Web Services、ソリューションアーキテクト、Kunal Pansari
- Amazon Web Services、ソリューションアーキテクト、Eric Vasquez
- Amazon Web Services、ソリューションアーキテクト、Tushar Jagdale
- Amazon Web Services、ソリューションアーキテクト、Ameer Shariff
- Amazon Web Services、ソリューションアーキテクト、Glenn Davis
- Amazon Web Services、ソリューションアーキテクト、Nick Kniveton
- Amazon Web Services、Principal Solutions Architect、Sidhartha Chauhan

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 フィードにサブスクライブしてください。

変更	説明	日付
メジャーな更新	CloudWAN、Amazon VPC Lattice、ENA Express、ハイブリッド接続、 Direct Connect Sitelink、ディープパケットインスペクション、および の変更に関するホワイトペーパー全体の更新 AWS Verified Access。	2024 年 4 月 17 日
マイナーな更新	図を更新して、より一貫性を高め、DX 接続オプションを更新してプライベート IP VPN を含め、全体で多数の軽微な変更を行いました。	2023 年 7 月 6 日
マイナーな更新	AWS Control Tower 情報の更新、さまざまなサービスの新しいスループット制限の反映、NAT ゲートウェイ図の更新、出力を一元化するためのセキュリティセクションの更新。	2023 年 4 月 4 日
マイナーな更新	セクションを追加: クロスリージョンエンドポイントアクセス。	2022 年 7 月 19 日
メジャーな更新	Transit Gateway Connect で Transit Gateway セクションを更新、Transit VPC セク	2022 年 2 月 22 日

	ションを更新、MACsec と障害耐性に関する推奨事項で Direct Connect セクションを更新、セクションを更新 AWS PrivateLink しました。VPC ピアリングと Transit VPC と Transit Gateway の比較テーブルを追加しました。一元的なインバウンド検査セクションを追加しました。VPC-to-VPC および VPC-on-premisesの集中型ネットワークセキュリティを VPC に更新し、 AWS Network Firewall と Gateway Load Balancer の設計パターンを使用してインターネットに一元的に送信しました。プライベート NAT ゲートウェイと Amazon Route 53 DNS Firewall セクションを追加しました。	
マイナーな更新	Transit Gateway と VPC ピアリングセクションを更新	2021 年 4 月 2 日
ホワイトペーパーの更新	図 7 に示されているオプションと一致するようにテキストを修正しました。	2020 年 6 月 10 日
初版発行	ホワイトペーパーの発行。	2019 年 11 月 15 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ており、(b) 現在の AWS 製品の提供とプラクティスを表し、予告なしに変更される可能性があり、(c) AWS およびその関連会社、サプライヤー、または許諾者からのコミットメントや保証は生じません。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。

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。