

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

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは、Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していない他のすべての商標は、それぞれの所有者の所有物であり、Amazon と提携、接続、または後援されている場合とされていない場合があります。

Table of Contents

要約と序章	1
序章	1
IP アドレスの計画と管理	4
Well-Architected の実現状況の確認	5
VPC から VPC への接続	6
VPC ピアリング	6
AWS Transit Gateway	7
トランジット VPC ソリューション	9
VPC ピアリングとトランジット VPC とトランジットゲートウェイ	10
AWS PrivateLink	12
VPC 共有	14
プライベート NAT ゲートウェイ	16
AWS クラウド WAN	18
Amazon VPC Lattice	20
ハイブリッド接続	23
VPN	23
AWS Direct Connect	26
Direct Connect 接続の MACsec セキュリティ	30
AWS Direct Connect 障害耐性に関する推奨事項	30
AWS Direct Connect SiteLink	30
インターネットへの一元的な出力	33
NAT ゲートウェイを使用した一元的なIPv4出力	33
高可用性	36
セキュリティ	36
スケーラビリティ	36
でNATゲートウェイを使用して - AWS Network Firewall 元的な出力IPv4を行う	37
スケーラビリティ	39
主な考慮事項	39
Amazon EC2インスタンスでのNATゲートウェイと Gateway Load Balancer IPv4 を使用した一元的な出力	40
高可用性	41
利点	42
主な考慮事項	42
の一元化された出力 IPv6	43

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	
ティ	48
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	48
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	50
AWS Network Firewall と AWS Gateway Load Balancer の主な考慮事項	51
一元化されたインバウンド検査	54
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	54
利点	56
主な考慮事項	56
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	56
利点	57
主な考慮事項	58
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	58
一元的な進入 AWS Network Firewall に を使用する	60
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	61
集中型進入アーキテクチャ AWS Network Firewall における の主な考慮事項	61
DNS	63
ハイブリッド DNS	63
Route 53 DNS ファイアウォール	66
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	67
インターフェイス VPC エンドポイント	67
クロスリージョンエンドポイントアクセス	69
AWS Verified Access	71
結論	74
寄稿者	75
ドキュメント履歴	76
注意	78
	lxxix

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

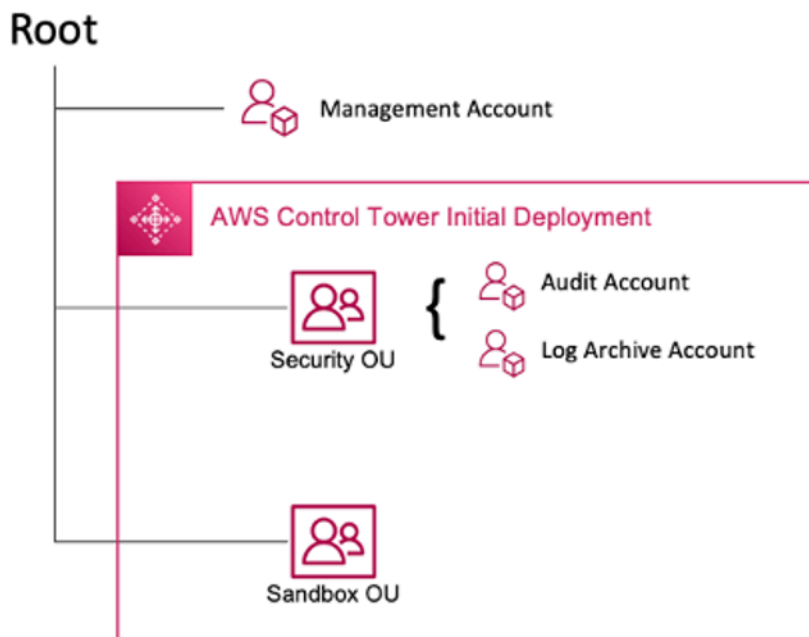
公開日: 2024 年 4 月 17 日 ([ドキュメント履歴](#))

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](#)、[Gateway Load Balancer](#)、[AWS Direct Connect](#)、[Amazon Route 53](#) などの AWS サービスを使用して [AWS Network Firewall](#)、大規模ネットワークで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、サービスを分割する管理境界を表すリソースを 1 つの AWS アカウントで構築することから始めます。ただし、顧客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では、IT サービスと組織内の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](#)。



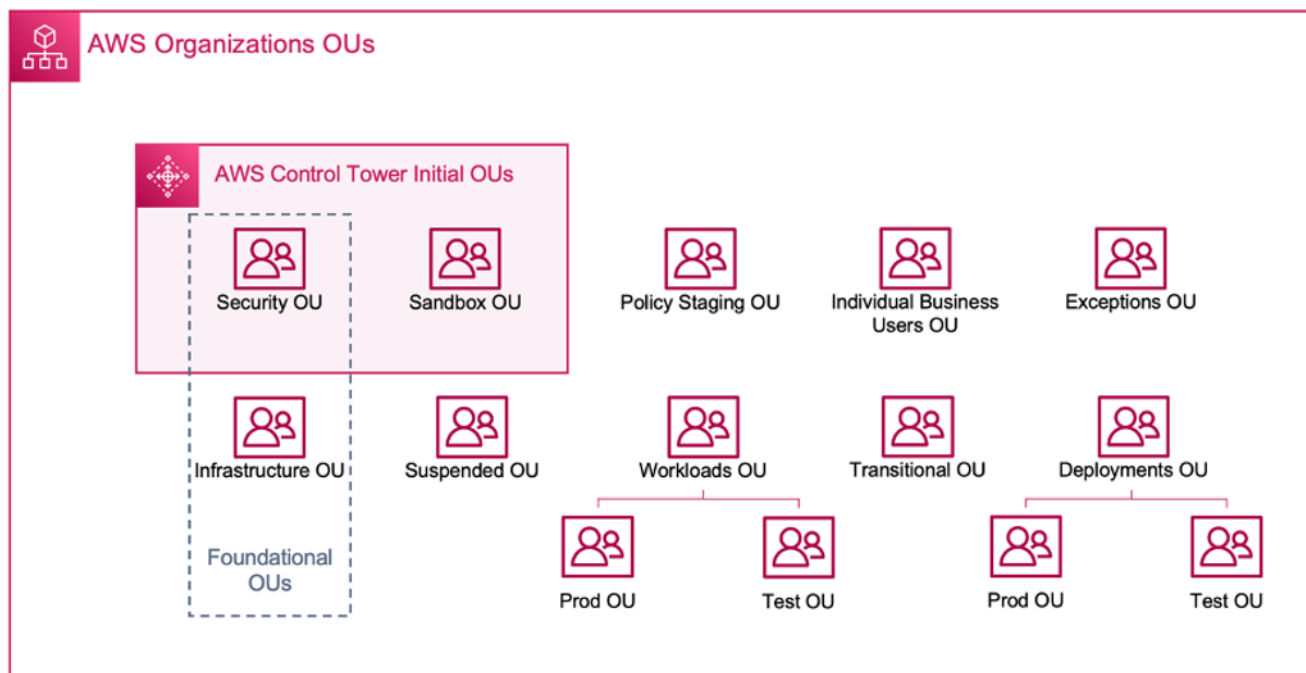
AWS Control Tower の初期デプロイ

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 内には、次の 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、内で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 のサービス、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、によって最初にデプロイされた OUs を示しています AWS Control Tower。AWS 環境を拡張して、図に含まれている推奨 OUs のいずれかを実装して、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 AWS 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。

Note

このホワイトペーパーでは、「Control Tower」は、ワークロードをデプロイするスケーラブルで安全でパフォーマンスの高いマルチアカウント/マルチ VPC セットアップの広義の用語です。この設定は、さまざまなツールを使用して構築できます。マルチアカウントクラウド基盤のベストプラクティス、設計原則、利点の詳細については、[「複数アカウントを使用した AWS 環境の整理」](#) ホワイトペーパーを参照してください。

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。お客様が作成する 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](https://aws.amazon.com/elasticloadbalancing/gateway-load-balancer/) <https://aws.amazon.com/elasticloadbalancing/gateway-load-balancer/>などのインターネット[AWS PrivateLink](#)[AWS Network Firewall](#)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。
- 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、オンプレミスのワークロード、クラウドワークロードをカバーする必要があり、将来の拡張 (新しい AWS リージョン、ビジネスユニット、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する IP CIDRs。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、このような例外に対して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。適切な 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 アドレス指定スキーム (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。
- 階層型および要約型の 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 の競合を減らし、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 AWS リージョン、共有できます 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。

ブログ投稿の「[Amazon VPC IP Address Manager のベストプラクティス](#)」、「Amazon VPC IP Address Manager を使用した VPC とリージョン間の IP プールの管理」、および「[IP アドレス管理 AWS Control Tower](#)」を参照して、IP アドレスのベストプラクティスと、IPAM を使用して VPCs 間の IP プールを管理する方法を確認してください AWS リージョン AWS Control Tower。 [VPCs](#)

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 Management Console](#) 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

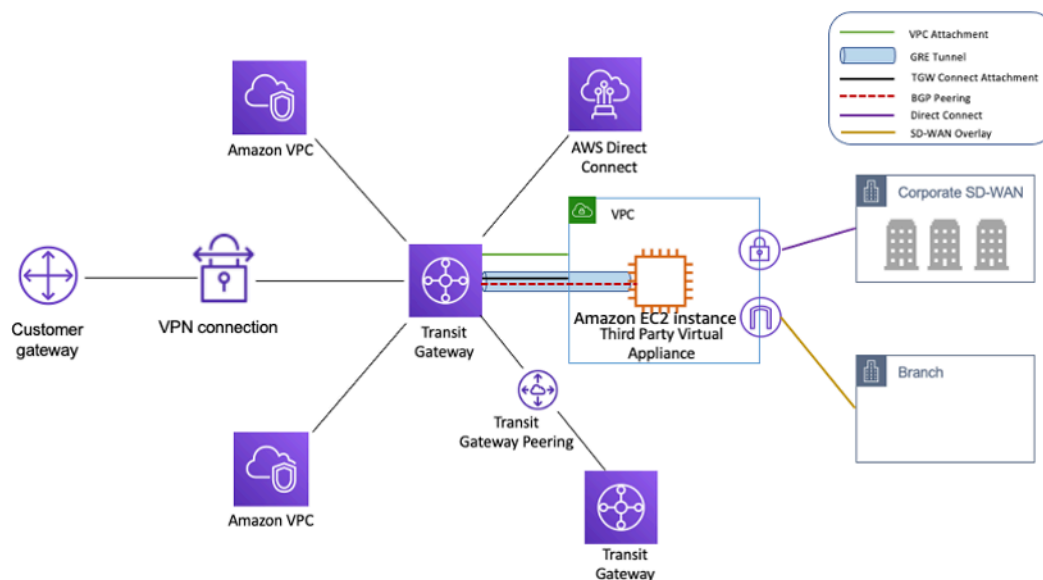
お客様は、2つの異なる VPC 接続パターンを使用して、マルチ VPC 環境をセットアップできます。多対多、またはハブアンドスポークです。この many-to-many アプローチでは、各 VPC 間のトラフィックは各 VPC 間で個別に管理されます。この hub-and-spoke モデルでは、VPC 間トラフィックはすべて中央リソースを経由し、確立されたルールに基づいてトラフィックをルーティングします。

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、異なるアカウントの VPCs、VPCs と AWS リージョン間のトラフィックをピアリングすることもできます。アベイラビリティゾーン内に留まる 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。

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にな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 VPCs あり、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。



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を接続できます。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、ブラスト半径の設定ミス、コントロールプレーンオペレーションの分離、管理を制限する有効なケースがあります ease-of-use。

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てグローバルネットワークを構築する](#)」を参照してください。[AWS Transit Gateway は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。](#)

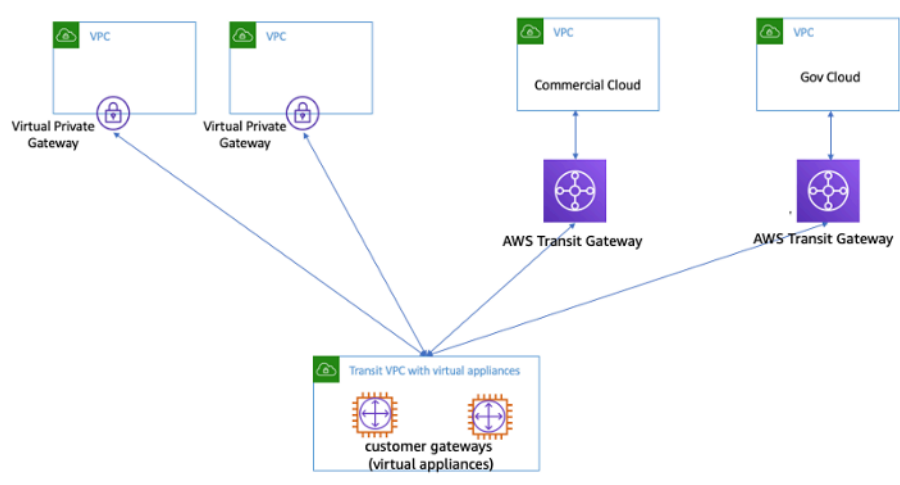
組織の Transit Gateway インスタンスを Network Services アカウントに配置します。これにより、ネットワークサービスアカウントを管理するネットワークエンジニアによる一元管理が可能になります。Resource Access Manager (RAM) AWS を使用して、同じリージョン内の AWS Organization 内の複数のアカウント間で VPCs を接続するための Transit Gateway インスタンスを共有します。AWS RAM を使用すると AWS アカウント、AWS リソースを任意のまたは AWS Organization 内で簡単かつ安全に共有できます。詳細については、[中央アカウントブログ記事の「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、SD-WAN インフラストラクチャと AWS Transit Gateway Connect 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、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 AWS 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、[「Simplify SD-WAN connectivity with AWS Transit Gateway Connect」](#) 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宛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の恩恵を受けます。
- 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、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 ピアリングとトランジット VPC とトランジットゲートウェイ

表 1 — 接続比較

条件	VPC ピアリング	トランジット VPC	トランジットゲートウェイ	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 ベース hub-and-spoke	添付ファイルベース 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

条件	VPC ピアリング	トランジット VPC	トランジットゲートウェイ	PrivateLink	Cloud WAN	VPC Lattice
スケール	125 個のアクティブなピア/VPC	仮想ルーター/EC2 によって異なります	リージョンあたり 5000 個のアタッチメント	制限なし	コアネットワークあたり 5000 個のアタッチメント	サービスあたり 500 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	カスタマー管理	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 と同じデータープレーンを使用する	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	アベイラビリティゾーンあたり 10 Gbps、最大 100 Gbps まで自動的にスケーリング	最大 100 Gbps (バースト)/アタッチメント	アベイラビリティゾーンあたり 10 Gbps

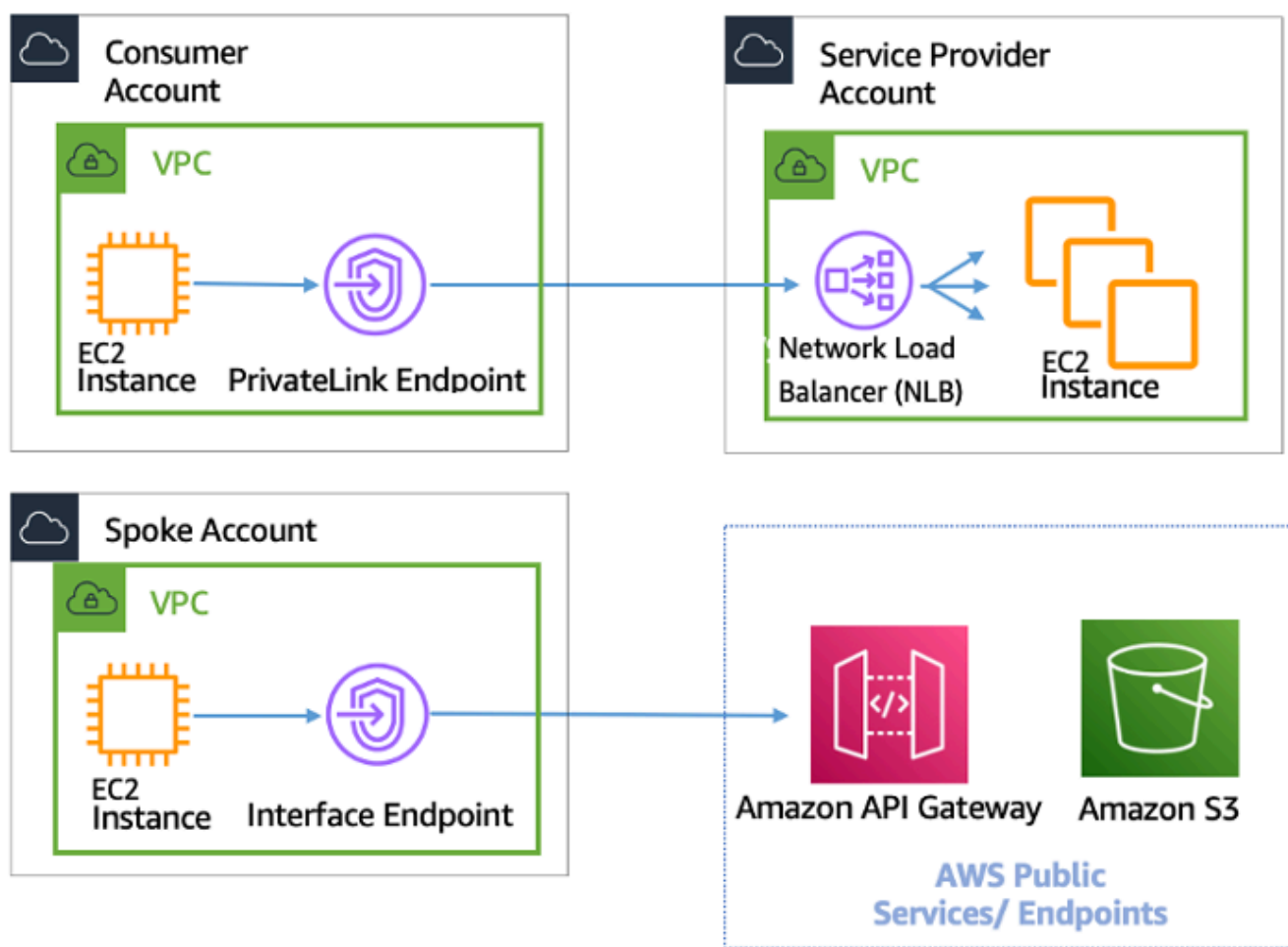
条件	VPC ピアリング	トランジット VPC	トランジットゲートウェイ	PrivateLink	Cloud WAN	VPC Lattice
可視性	VPC Flow Logs	VPC フローログと CloudWatch メトリクス	Transit Gateway Network Manager、VPC フローログ、CloudWatch メトリクス	CloudWatch メトリクス	Network Manager、VPC フローログ、CloudWatch メトリクス	CloudWatch アクセスログ
セキュリティグループ	サポート	サポートされません	サポートされません	サポートされません	サポートされません	該当しない
相互参照						
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、ある VPC (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、コンシューマー VPC のみがサービスプロバイダー VPCs への接続を開始する AWS リージョン 方法で、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。この例には、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の VPCs 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 内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 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 — クライアント/サーバーがセットアップされており、サービスプロバイダー VPCs または特定の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 1 つ以上のコンシューマー VPC の単方向アクセスを許可する AWS PrivateLink 場合に使用します AWS 。コンシューマー VPC にアクセスできる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 内のクライアントとサーバーで IP アドレスが重複している場合にも適しています。は、 がサービスプロバイダーと IP 競合しないように、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、 リージョン内またはリージョン間接続でプレースメントグループが引き続き必要になる可能性がある直接接続要件を処理する VPC ピアリング、大規模な VPCs の接続を簡素化する 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 VPC 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。VPCs 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 共有のメリット :

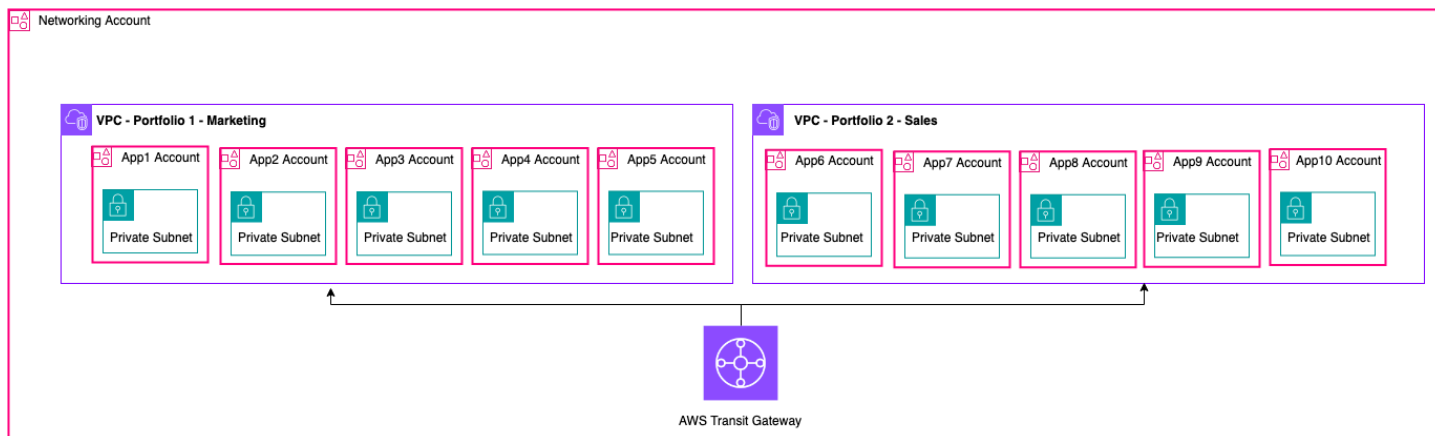
- シンプルな設計 — VPC 間の接続を複雑にしない
- 管理対象 VPCs の数を減らす
- ネットワークチームとアプリケーション所有者間の職務の分離
- IPv4 アドレス使用率の向上
- コスト削減 — 同じアベイラビリティゾーン内の異なるアカウントに属するインスタンス間でのデータ転送料金はかかりません。

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するように選択できます。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 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 に接続できます。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、NACLs)。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 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

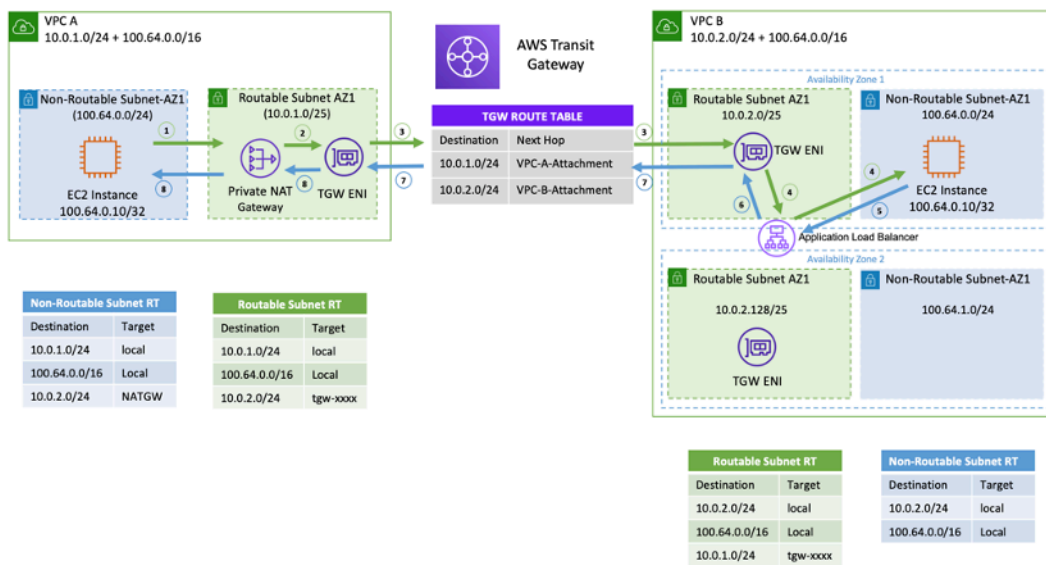
Note

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「[制限事項](#)」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: 主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

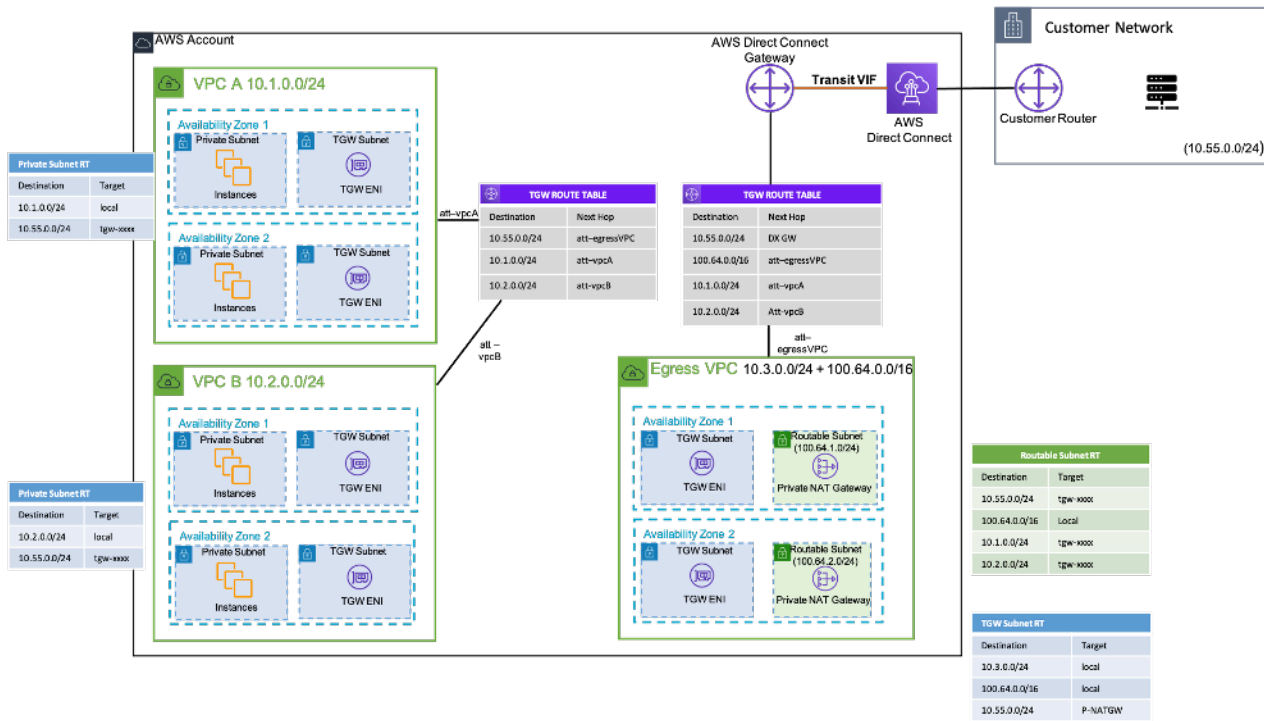
多くの場合、チームは独立して作業し、プロジェクト用に新しい VPC を作成することがあります。この VPC には、クラスレスドメイン間ルーティング (CIDR) ブロックが重複している可能性があります。統合のために、重複する CIDRs、VPC ピアリングや Transit Gateway などの機能では実現できません。プライベート NAT ゲートウェイはこのユースケースに役立ちます。プライベート NAT ゲートウェイは、一意のプライベート IP アドレスを使用して、重複する送信元 IP アドレスの送信元 NAT を実行し、ELB は重複する送信先 IP アドレスの送信先 NAT を実行します。Transit 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 (重複する 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、接続をリクエストしている元の Amazon EC2 インスタンスに処理されます。

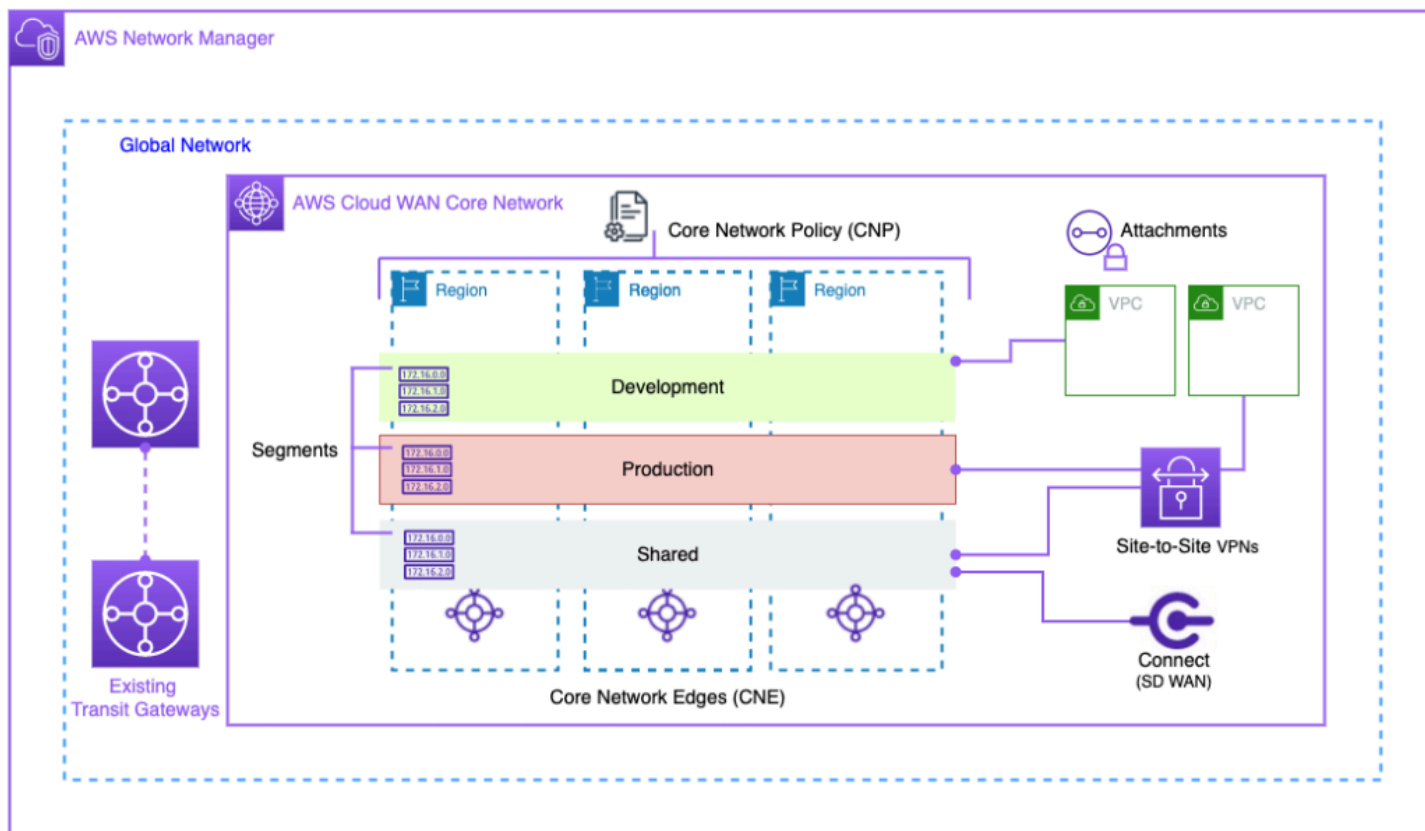
プライベート NAT ゲートウェイは、オンプレミスネットワークが承認された IPs へのアクセスを制限するときにも使用できます。少数のお客様のオンプレミスネットワークは、お客様が所有する承認済み IPs の連続した制限されたブロックを介してのみ、プライベートネットワーク (IGW なし) とのみ通信することをコンプライアンスで要求されます。各インスタンスにブロックから個別の IP を割り当てる代わりに、プライベート NAT ゲートウェイを使用して、許可リストに登録されている各 IP の背後にある AWS VPCs で大規模なワークロードを実行できます。詳細については、[「プライベート NAT 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 トンネルで実行できたネットワークを連結する新しい方法です。以前は、1 つ以上の VPCs を設定し、前述の方法のいずれかと接続して、IPSEC VPN または AWS Direct Connect 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をある場所で定義し、ネットワークを別の場所で定義します。Cloud 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本番トラフィックを分離できます。



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あり、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ニ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添付ファイル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、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. セグメントへのアタッチに使用するセグメント、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。

Cloud 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、社内の既存のインフラストラクチャを使用できます。Cloud WAN は、VPCsSD-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 を使用すると、クラウド環境とオンプレミス環境を統合ネットワークで接続できます。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 の移行および相互運用性パターン](#) 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「一元化された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、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して検出できます。

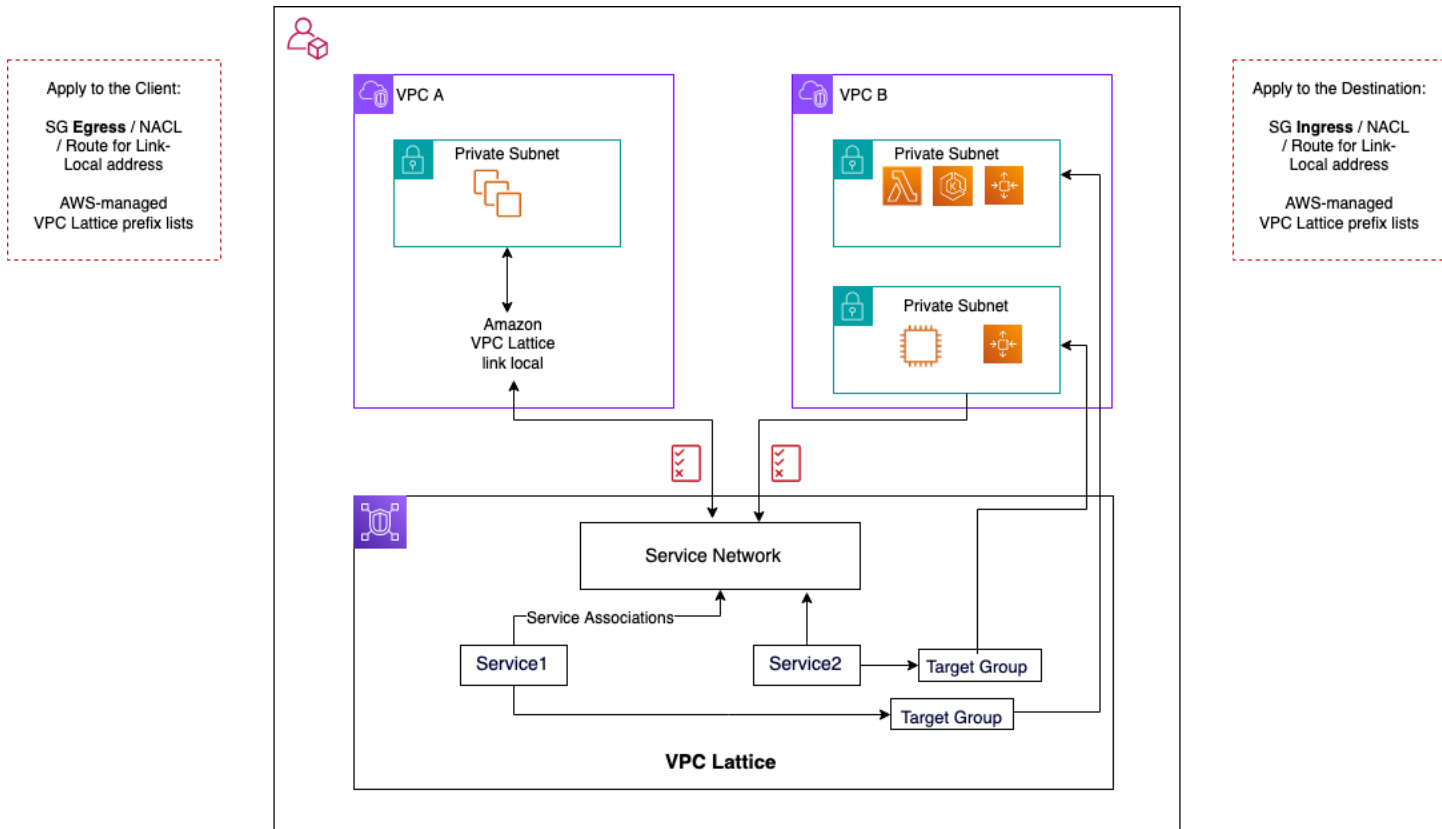
VPC Lattice コンポーネントは、以下で構成されます。

- サービス - インスタンス、コンテナ、または Lambda 関数で実行されてい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証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. サービスネットワークに VPCs をアタッチして、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内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使用されます。
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、認証および承認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。

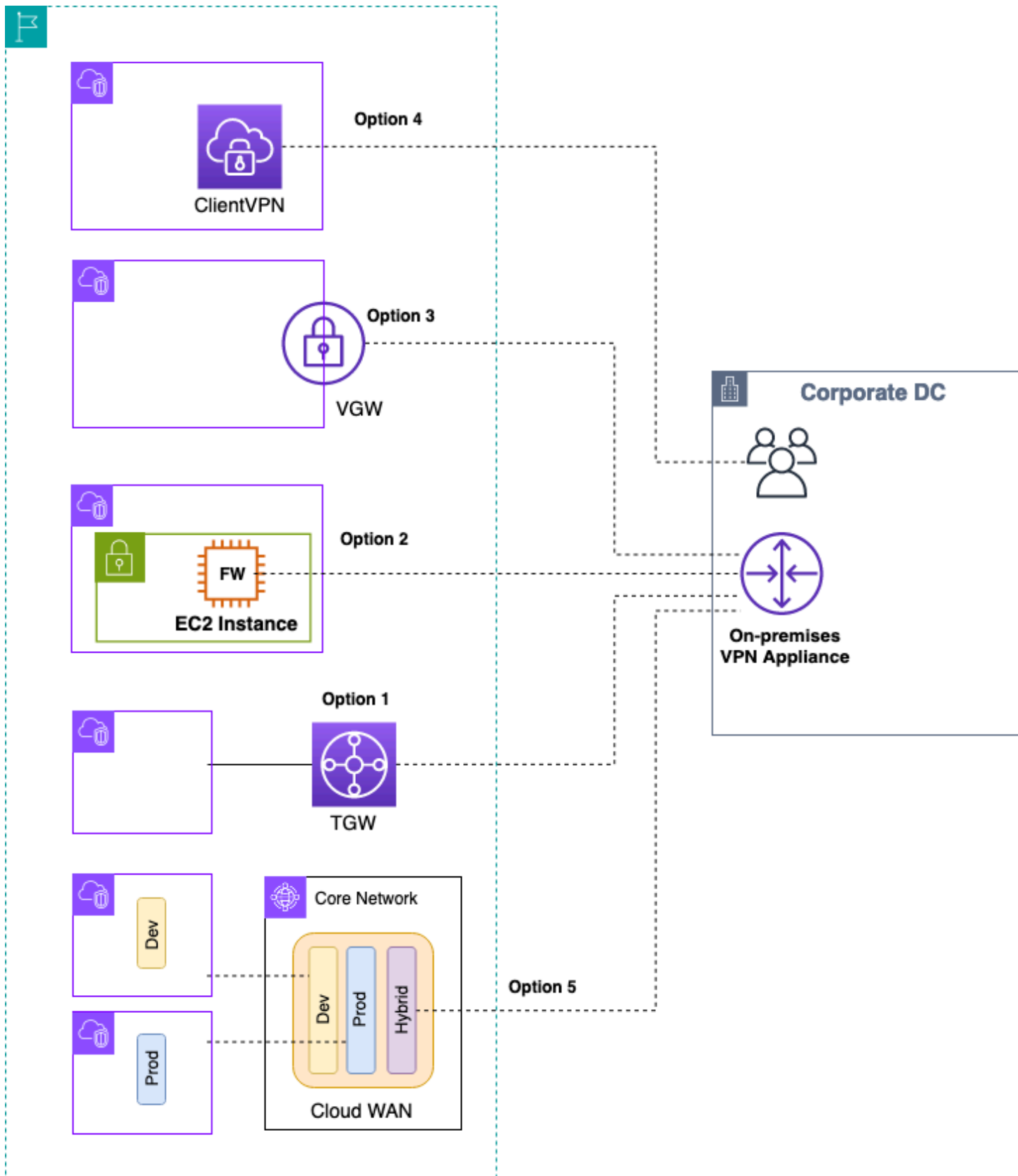
ハイブリッド接続

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ことに重点を置いています。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 接続** — この設定では、VPC ごとに VPN 接続または 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、VPC あたりのハイブリッド接続の管理が困難に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 に統合します。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 AWS 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、お客様は上に構築された CloudWAN を使用して、複数の VPCs の接続を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ク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 AWS 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

VPN を AWS にセットアップするには、さまざまな方法があります。



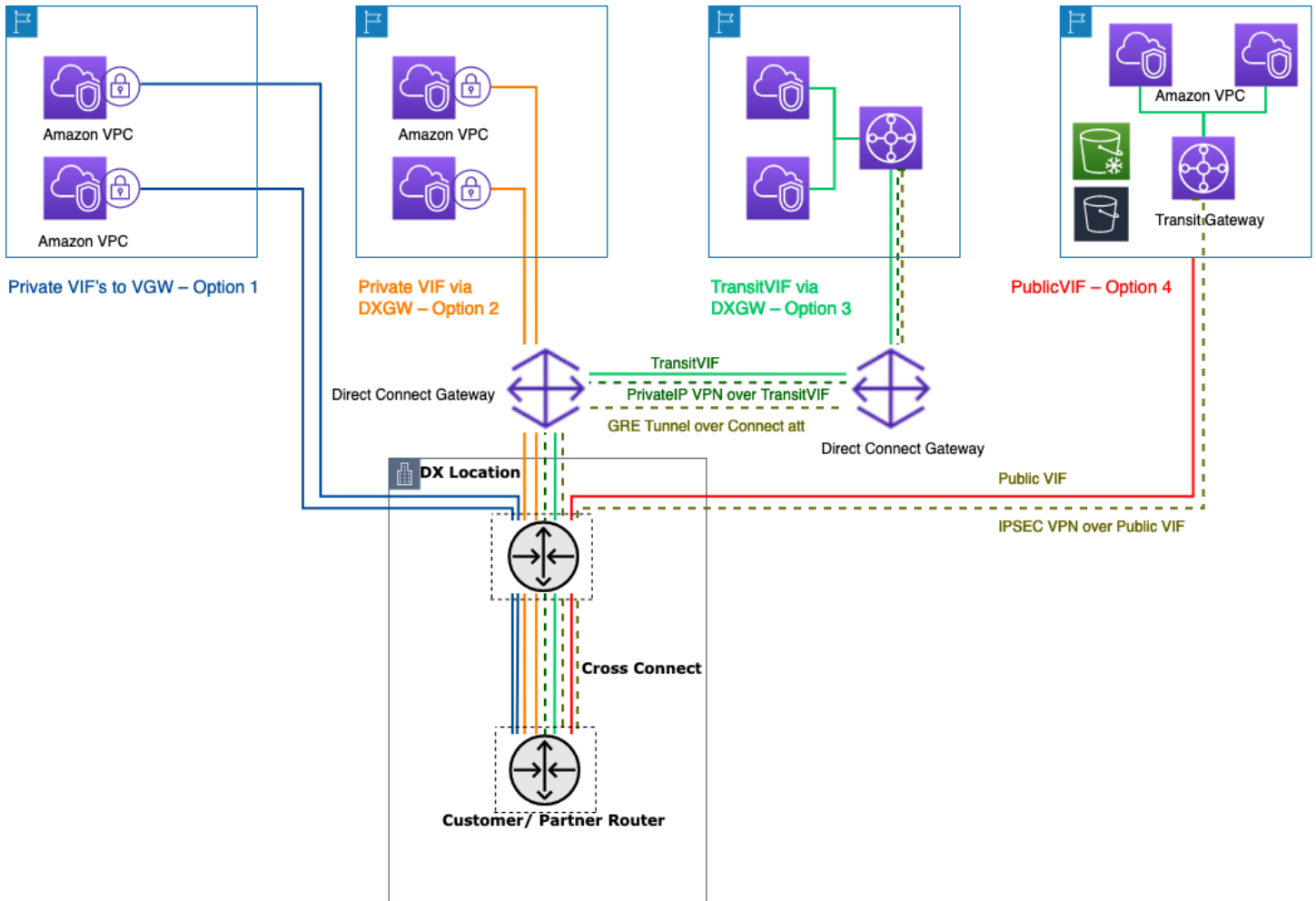
AWS VPN オプション

- オプション 1: Transit Gateway の 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、VPN の IPsec 終了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、そのゲートウェイにアタッチされた 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、はデフォルトの上限である 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 [AWS VPN の料金](#)が発生します。AWS では、VPN 接続にこのオプションを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ルリング](#)の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](#)セクションのすべての重要な考慮事項がハイブリッド VPN 接続に適用され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コストはお客様の負担となります。
- オプション 3: Virtual Private Gateway (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 one-to-one 接続設計が可能になります。これは AWS への VPN 接続を開始する優れた方法ですが、VPCs 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オプションになります。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 負荷分散はサポートされていません。料金の観点から見ると、AWS VPN の料金のみをお支払いいただけます。VGW の実行には料金はかかりません。詳細については、仮想プライベートゲートウェイの「[AWS VPN 料金](#)」および「」を参照してください。 [AWS VPN](#)
- 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 を使用すると、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 ドキュメント](#)を参照してください。

- オプション 5: AWS Cloud 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 VPN 接続をプログラムで設定します。

AWS 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。この信頼性がないため、多くのお客様はを選択します [AWS 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 AWS Direct Connect です。を使用すると AWS 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。AWS Direct Connect を使用して VPCs。



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 AWS 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 個の 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 ロケーションが置かれている AWS リージョンに制限されます。VIF から VPC への one-to-one マッピング (および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となります。
- オプション 2: 複数の VGWs (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 VGWs VPCs に (VPG を介して) 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なオプションです。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 から VPC への接続は許可されません。詳細については、AWS 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 ロケーションが格納されている AWS リージョンへの接続は制限されません。AWS Direct Connect ゲートウェイは北/南のトラフィックフロー専用であり、VPC から VPC への接続は許可されません。このルールの例外は、同じ AWS Direct Connect ゲートウェイと同じ仮想インターフェイスにアタッチされた VPCs VGWs にスーパーネットがアドバタイズされる場合です。この場合、VPCs は AWS 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、[AWS 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 ゲートウェイにトランジット 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 AWS Direct Connect ようになりました。高速接続 (1Gbps 以上) が不要ない場合、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 ピアリングを介して、異なる AWS リージョンと AWS アカウント間で AWS Direct Connect、ゲートウェイごとに最大 6 つの Transit Gateway インスタンス (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セットアップですが、[Transit Gateway のクォータ](#) に注意してください。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

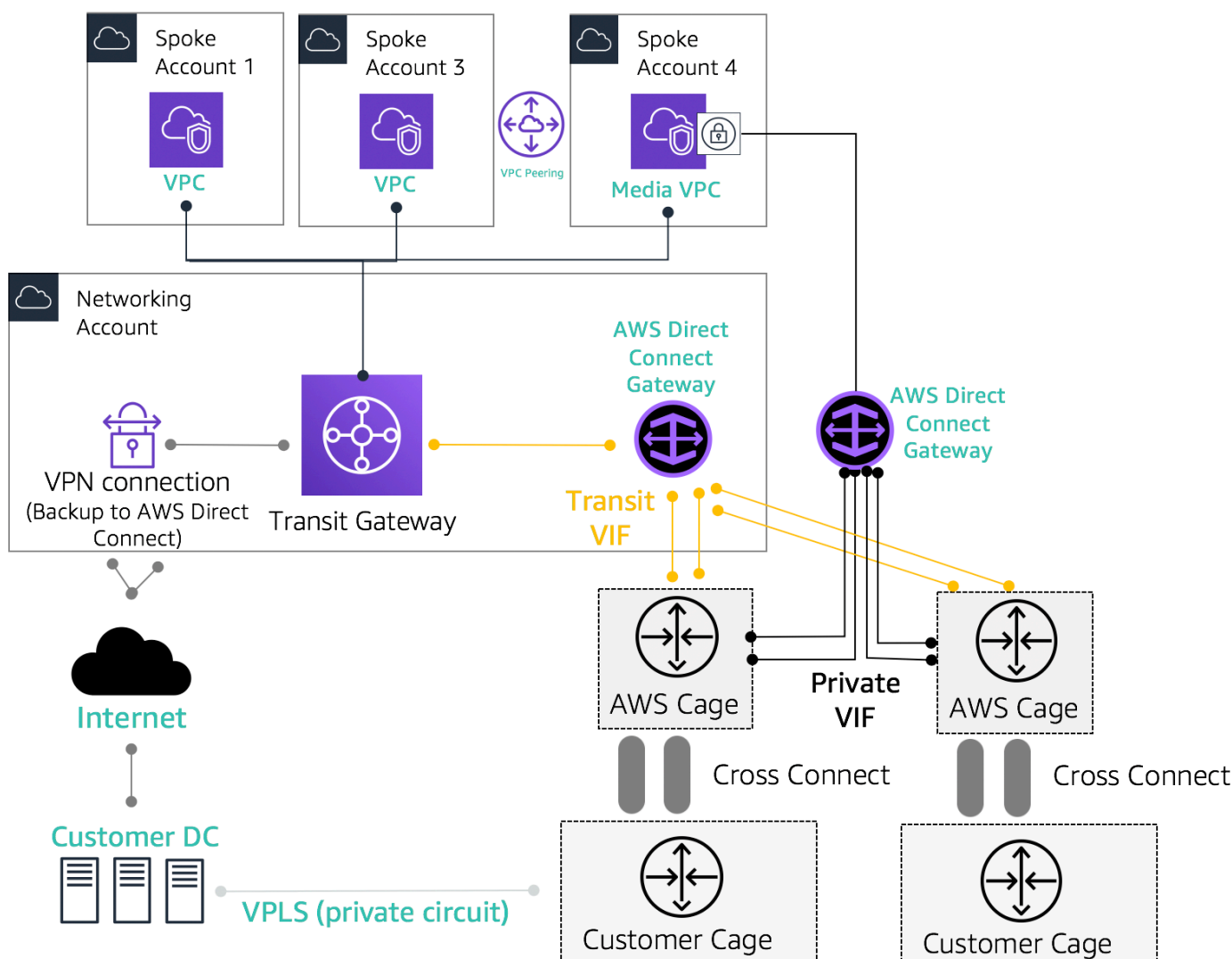
できるプレフィックスは 200 個のみです。上記のオプションでは、Direct Connect の料金が発生します。このオプションでは、Transit Gateway アタッチメントとデータ処理料金も発生します。詳細については、[Direct Connect ドキュメントの「Transit Gateway の関連付け」](#)を参照してください。

- 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 AWS 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が同時に強化されます。プライベート IP VPN は Transit VIFs、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: トランジット 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するトランジット VIF を介して確立でき、VPN 接続と比較してより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思えます。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、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 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 口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。VPN は、AWS Direct Connect 接続へのバックアップ接続として作成することもできます。

「トランジット VIF 経由で Transit Gateway への GRE トンネルを作成する」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 の間で 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 AWS Direct Connect には、 を介して Transit Gateway を AWS RAM 他アカウントと共有します。

Direct Connect 接続の MACsec セキュリティ

お客様は、[特定のロケーション](#) 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 hop-by-hop リンクをベースで保護するため、デバイスには Direct Connect デバイスとの直接レイヤー 2 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 と連携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。

AWS Direct Connect 障害耐性に関する推奨事項

を使用すると AWS Direct Connect、お客様は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。

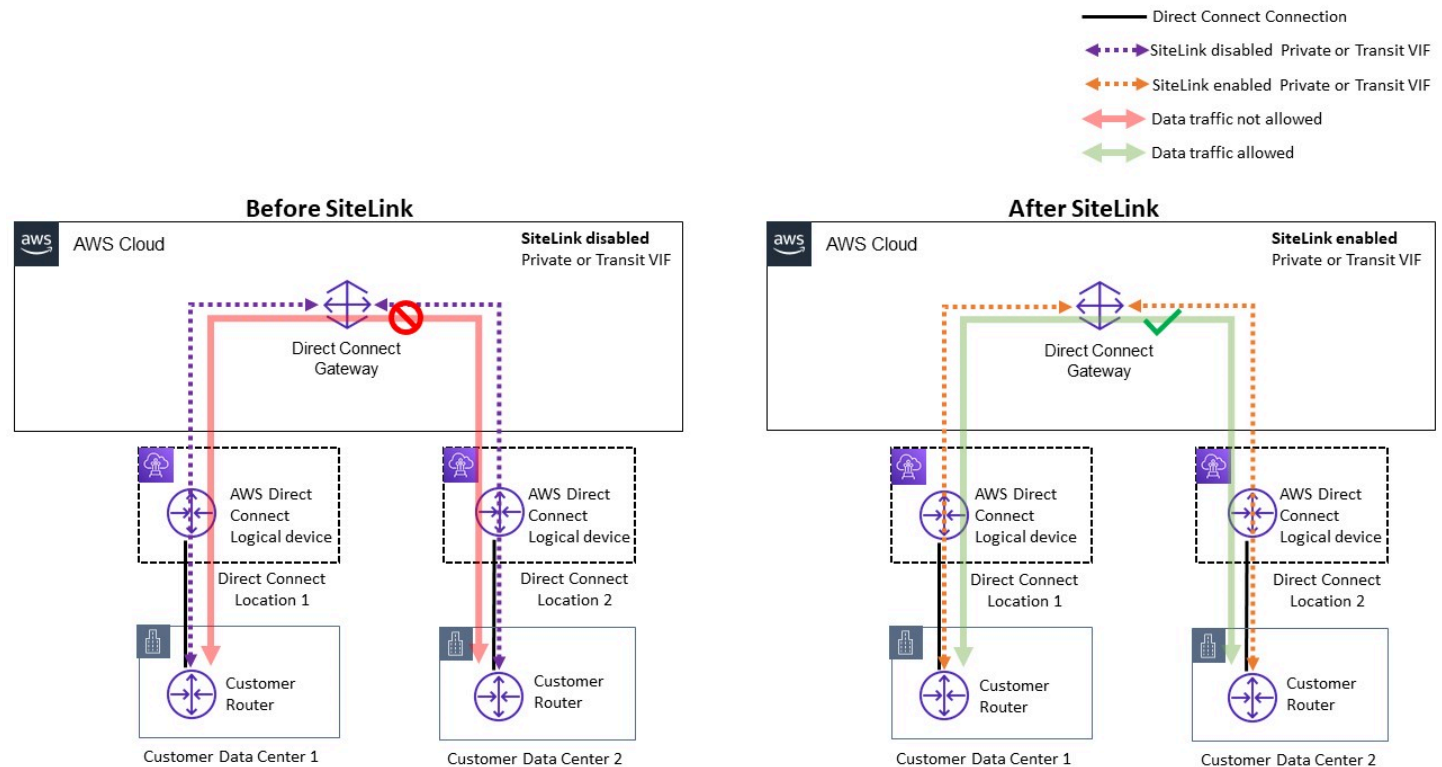
また、AWS は、サービスレベルアグリーメント (SLA) AWS Direct Connect の要件に最適なモデルを特定し、それに応じて Direct Connect 接続を使用してハイブリッド接続を設計するのに役立つ、接続ウィザードを提供する Resiliency Toolkit も提供しています。詳細については、[AWS Direct Connect 「障害耐性に関する推奨事項」](#)を参照してください。

AWS 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 を介した直接回路構築、または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 MetroEthernet、またはレガシー T1 回路を使用することによってのみ可能でした。の導入により SiteLink、お客様はロケーションで終了するオンプレミス AWS Direct Connect ロケーションの直接 site-to-site 接続を有効にできるようになりました。Direct Connect

回路を使用して、トラフィックを VPCs 経由でルーティングすることなく site-to-site 接続を提供し、AWS リージョンを完全にバイパスします。

これで、AWS Direct Connect 口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の間に、グローバルで信頼性の高い pay-as-you-go 接続を確立できます。



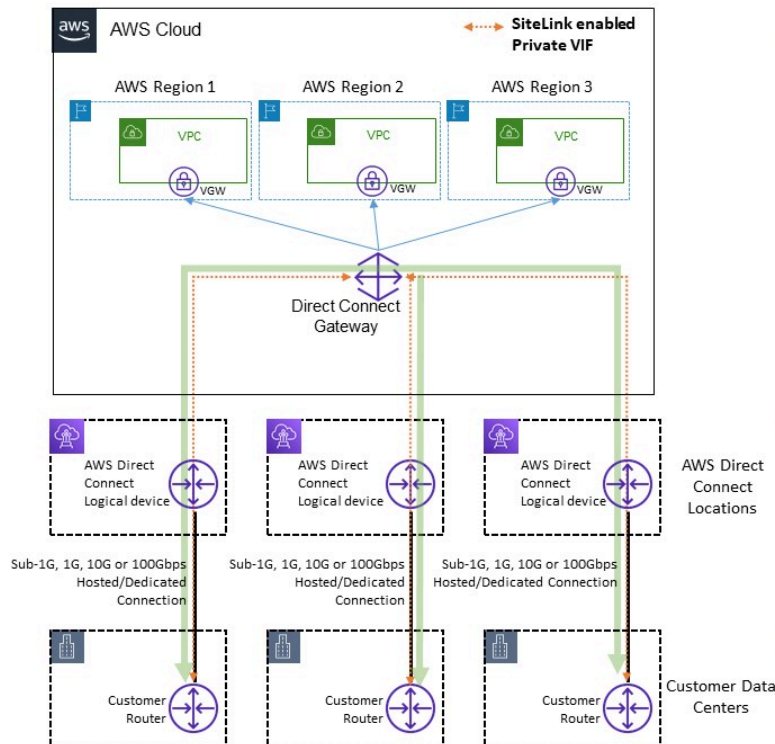
のサンプルリファレンスアーキテクチャ AWS Direct Connect SiteLink

を使用する場合 SiteLink、まずオンプレミスネットワークを世界中の 100 を超える AWS Direct Connect 口ケーションのいずれかの 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、を有効にします SiteLink。すべての VIFs が同じ AWS Direct Connect ゲートウェイ (DXGW) にアタッチされると、それらの間でデータの送信を開始できます。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、データは送信先への AWS Direct Connect 口ケーション間の最短パスをたどります。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。

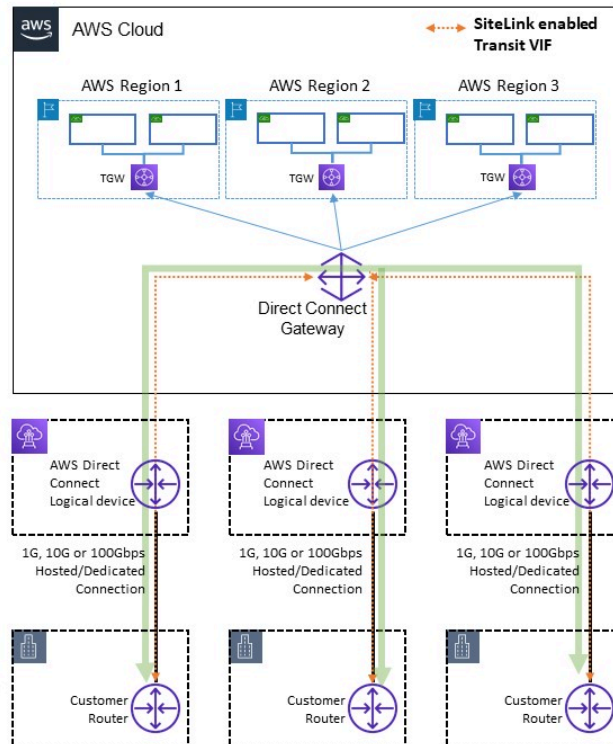
では SiteLink、DXGW は SiteLink 有効な VIFs を介してルーターから IPv4/IPv6 プレフィックスを学習し、BGP のベストパスアルゴリズムを実行し、NextHop や AS_Path などの属性を更新し、これらの BGP プレフィックスをその DXGW に関連付けられた SiteLink 対応 VIFs の残りの部分に再アドバタイズします。VIF SiteLink で を無効にすると、DXGW はこの VIF を介して学習したオンプレ

ミスプレフィックスを他の SiteLink が有効な VIFs にアドバタイズしません。SiteLink 無効化された 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) インスタンスや Transit Gateway (TGW) インスタンスなどの DXGW Gateway 関連付けのみアドバタイズされます。

Full Mesh Connectivity with Private VIF



Full Mesh Connectivity with Transit VIF



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、どのロケーションが相互に、および AWS リージョンリソースと通信できるかを制御できます。

詳細については、「[の紹介 AWS 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出力

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、多くのアプリケーションで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 更新のダウンロードなど) が必要になります。これは、トラフィックIPv4と IPv6トラフィックの両方で実現できます。の場合IPv4、これはNATゲートウェイの形式のネットワークアドレス変換 (NAT) によって実現できます (推奨)。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 NATインスタンスで実行されるセルフマネージドEC2インスタンスによって実現できます。内部アプリケーションはプライベートサブネットに、NATゲートウェイと Amazon EC2NATインスタンスはパブリックサブネットに存在します。

AWS では、可用性と帯域幅が向上し、管理にかかる労力が減るため、NATゲートウェイを使用することをお勧めします。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、Egress Only インターネットゲートウェイVPC を介してそれぞれを分散的に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VPCを使用して一元化された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、「」で説明します[の一元化された出力 IPv6](#)。

トピック

- [NAT ゲートウェイを使用した一元的なIPv4出力](#)
- [でNATゲートウェイを使用して - AWS Network Firewall 元的な出力IPv4を行う](#)
- [Amazon EC2インスタンスでのNATゲートウェイと Gateway Load Balancer IPv4 を使用した一元的な出力](#)
- [の一元化された出力 IPv6](#)

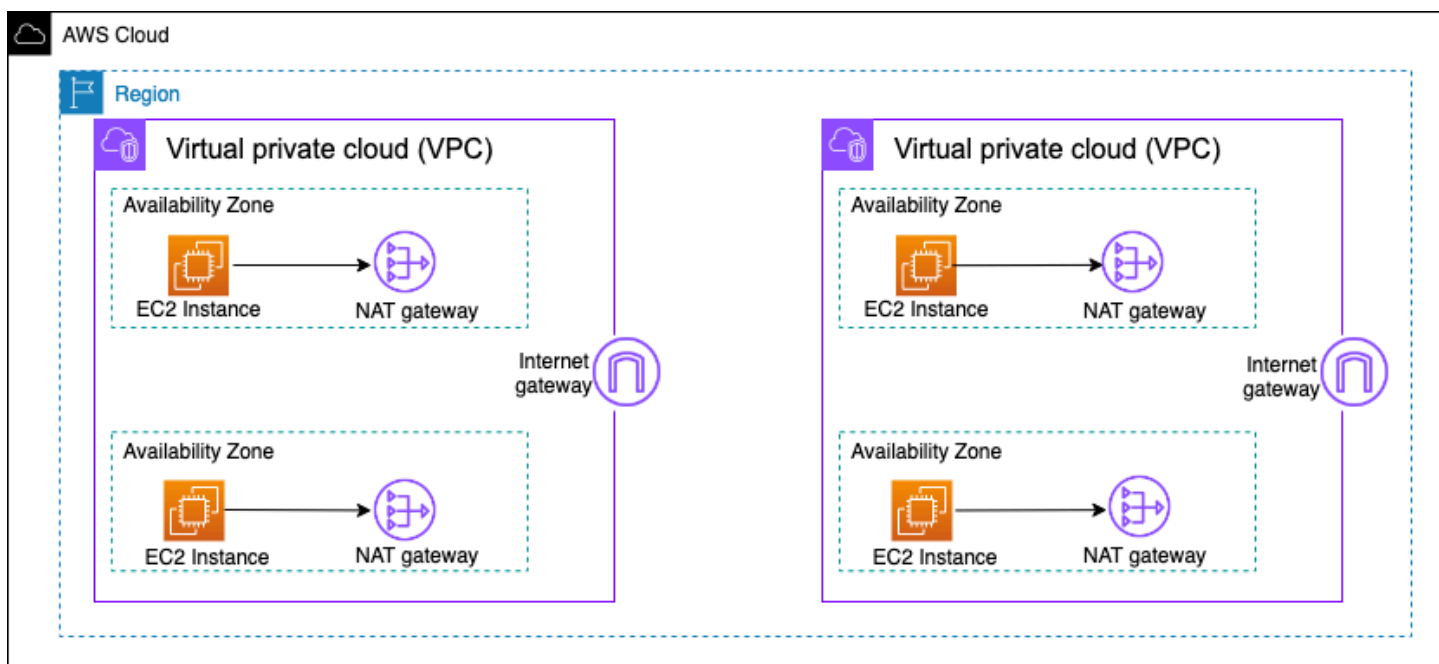
NAT ゲートウェイを使用した一元的なIPv4出力

NAT Gateway は、マネージド型のネットワークアドレス変換サービスです。すべてのスポークに NATゲートウェイをデプロイすると、NATデプロイするゲートウェイごとに時間単位の料金が発生するため、コストがかかりすぎるVPC可能性があります ([「Amazon VPCの料金」](#)を参照)。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、VPCネットワークサービスアカウントに個別の出力を作成し、出力にNATゲートウェイをデプロイしVPC、スポークからのすべての出力トラフィックVPCsを

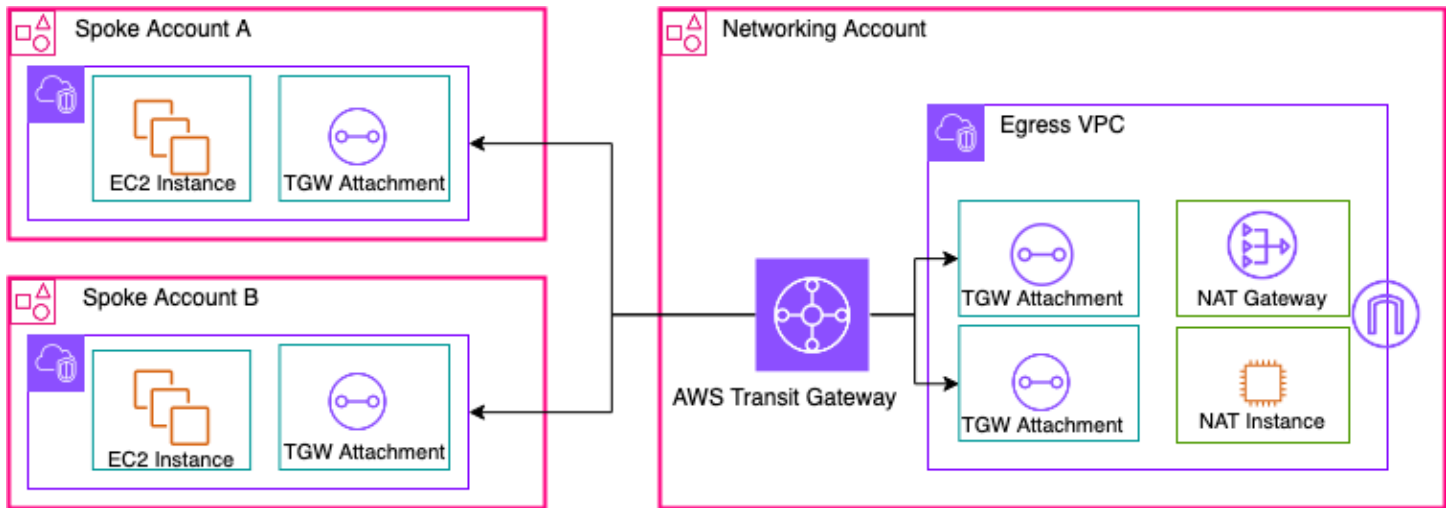
WAN、Transit Gateway または クラウド VPCを使用して出力に存在するNATゲートウェイにルーティングします。

Note

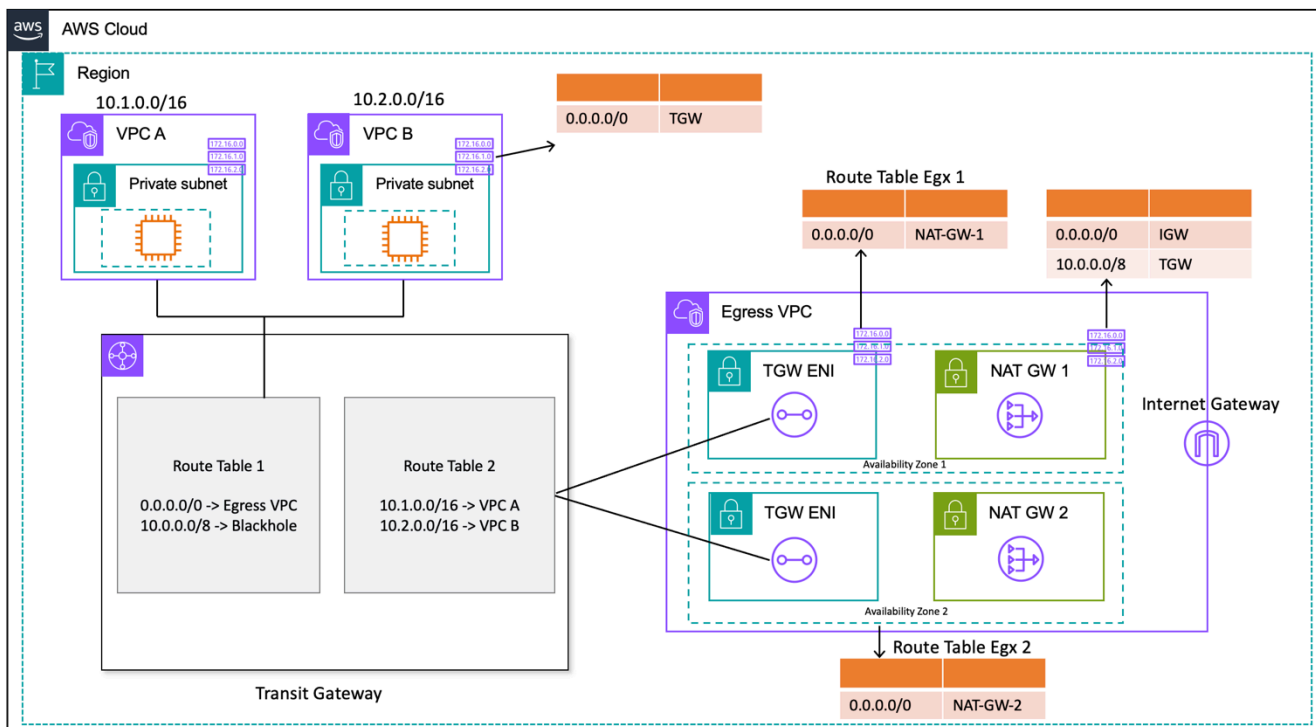
Transit Gateway を使用してNATゲートウェイを一元化する場合、すべての NATゲートウェイを実行する分散型アプローチと比較して、追加の Transit Gateway データ処理料金が発生しますVPC。エッジケースによっては、 からNATゲートウェイ経由で大量のデータを送信する場合VPC、Transit Gateway のデータ処理料金を回避VPCするためにNATローカルを残しておく方が、費用対効果の高いオプションになる場合があります。



分散型高可用性NATゲートウェイアーキテクチャ



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



Transit NAT Gateway を使用した集中型ゲートウェイ (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 () に伝達されますRT2。2 つのVPCs通信を禁止する ブラックホール ルートがあります。相互VPC通信を許可する場合は、 から10.0.0.0/8 -> Blackholeルートエントリを削除できます RT1。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 に伝達することもできます RT1(または、1 つのルートテーブルを使用して、そのす

べてに関連付け/伝達することもできます)。Transit Gateway VPCsを使用して 間の直接トラフィックフローを有効にすることもできます。

すべてのトラフィックを出力する RT1 に静的ルートを追加しますVPC。この静的ルートのため、Transit Gateway は出力 ENIsの 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VPC。エグレスに入るとVPC、トラフィックENIsはこれらの Transit Gateway 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ゾーン内の各NATゲートウェイを指すルートを追加して、アベイラビリティゾーン間 (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、すべてのスポークバインドトラフィックをネクストホップとして Transit Gateway VPC に向け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ゾーンに 1 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ゲートウェイを経由するそのアベイラビリティ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ゾーンが使用できない場合、そのアベイラビリティゾーンのNATゲートウェイとともに Transit Gateway エンドポイントは失敗し、すべてのトラフィックは Transit Gateway と他のアベイラビリティゾーンのNATゲートウェイエンドポイントを経由します。

セキュリティ

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ACLのネットワークは、セキュリティグループに依存します。例えば、お客様は NAT Gateway パブリックサブネットACLsで 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、この要件を満たすために、次のセクションで説明する一元的な出力 AWS Network Firewall のために で NAT Gateway を使用することもできます。

スケーラビリティ

1 つのNATゲートウェイで、一意の送信先ごとに割り当てられた IP アドレスごとに最大 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 アドレスを許可できます。これにより、1 つの送信先 IP とポートへの同時接続数が 440,000 件になります。NAT ゲートウェイは 5 Gbps の帯域幅を提供し、自動的に 100 Gbps に拡張します。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せず、複数のアベイラビリティゾーンのNAT

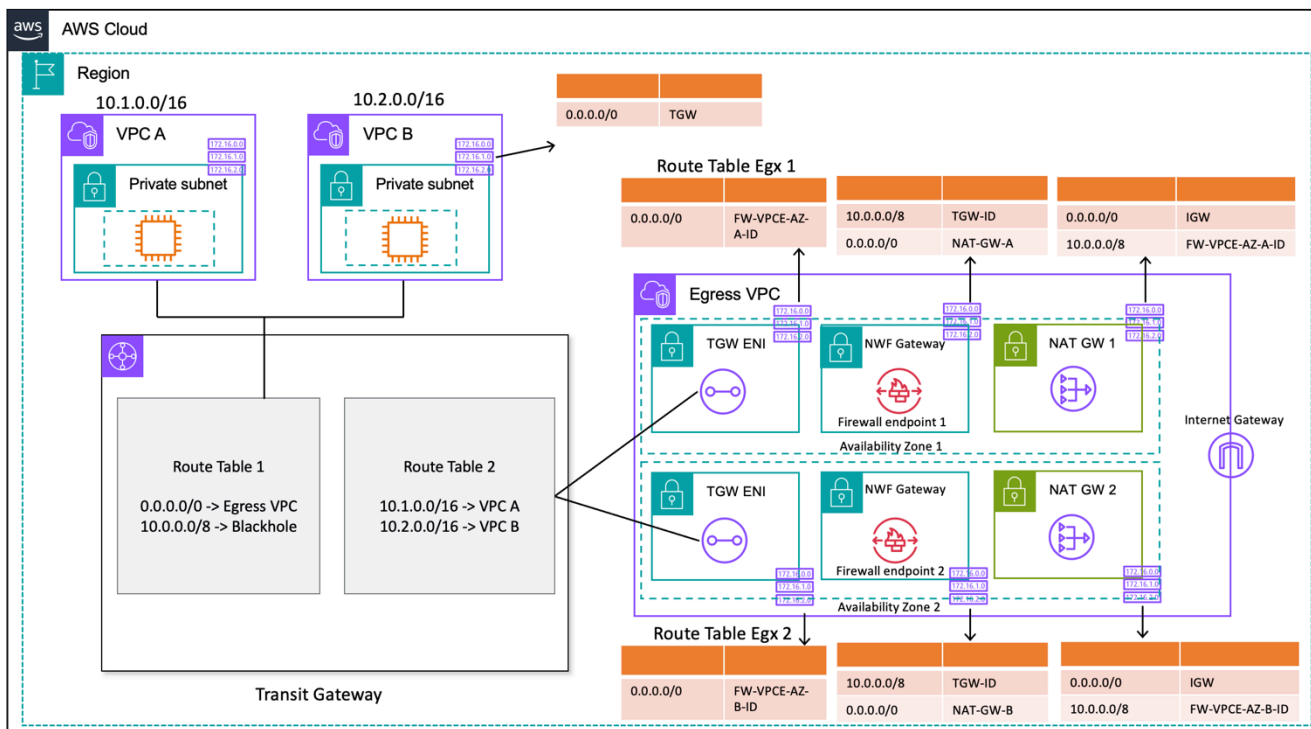
ゲートウェイ間でトラフィックを均等に分散しません。トランジットゲートウェイ全体のトラフィックは、可能であればアベイラビリティゾーン内に留まります。トラフィックを開始する Amazon EC2 インスタンスがアベイラビリティゾーン 1 にある場合、トラフィックはエグレスの同じアベイラビリティゾーン 1 の Transit Gateway Elastic Network Interface から流れ VPC 出し、Elastic Network Interface が存在するサブネットルートテーブルに基づいてネクストホップに流れます。ルールの完全なリストについては、Amazon Virtual Private 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、「[Creating a single internet exit point from multiple VPCs Using AWS Transit Gateway](#)」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 - AWS Network Firewall 元的な出力 IPv4 を行う

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、AWS Network Firewall と NAT ゲートウェイを一元化された出力アーキテクチャに組み込むことができます。AWS Network Firewall は、すべての VPC に不可欠なネットワーク保護を簡単にデプロイできるマネージドサービスです。これにより、全体のレイヤー 3-7 ネットワークトラフィックを制御および可視化できます。URL/ドメイン名、IP アドレス、および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フィルタリングできる何千ものルール AWS Network Firewall をサポートしています。オープンソースの IPS 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 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。

インスペクションを使用した集中型出力アーキテクチャでは、AWS Network Firewall エンドポイントは、出力のトランジットゲートウェイ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 VPC。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 ゲートウェイによる一元的な出力 (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、は複数のアベイラビリティゾーンにエンドポイントをデプロイ AWS Network Firewall することをAWS推奨しています。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ゾーンごとに1つのファイアウォールエンドポイントが必要です。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。

前の設定と同様に、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 () に伝達されますRT2。ブラックホールルートが明示的に追加され、両者が相互にVPCs 通信できなくなります。

引き続きデフォルトルートを使用して、すべてのトラフィックを出力にRT1向けますVPC。Transit Gateway は、すべてのトラフィックフローを出力の2つのアベイラビリティゾーンのいずれかに転送しますVPC。トラフィックがエグレスの Transit Gateway のいずれかに到達するENIsとVPC、デフォルトのルートに到達し、それぞれのアベイラビリティゾーンの AWS Network Firewall エンドポイントの1つにトラフィックが転送されます。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NATGWIPsデフォルトでに転送されるため、インGRESS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、NATここで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 を確認できません。

これを1つので実行していた場合はVPC、VPCルーティングの機能強化を使用して、同じ内のサブネット間のトラフィックを検査できますVPC。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、数万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、アベイラビリティゾーンごとに最大 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ことを選択した場合、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量時間 one-to-one に基づいて免除されます。
- 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。
- 注文が重要なため、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GRESSトラフィックとEGRESS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AVPCCIDRsタッチされたすべての追加を追加して、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を別のネットワークサービス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。例えば、ネットワーク管理者のみがネットワークサービス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 の分散型デプロイモデルと集中型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「を使用してデプロイする方法 AWS Network FirewallAWS 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 IPv4 を使用した一元的な出力

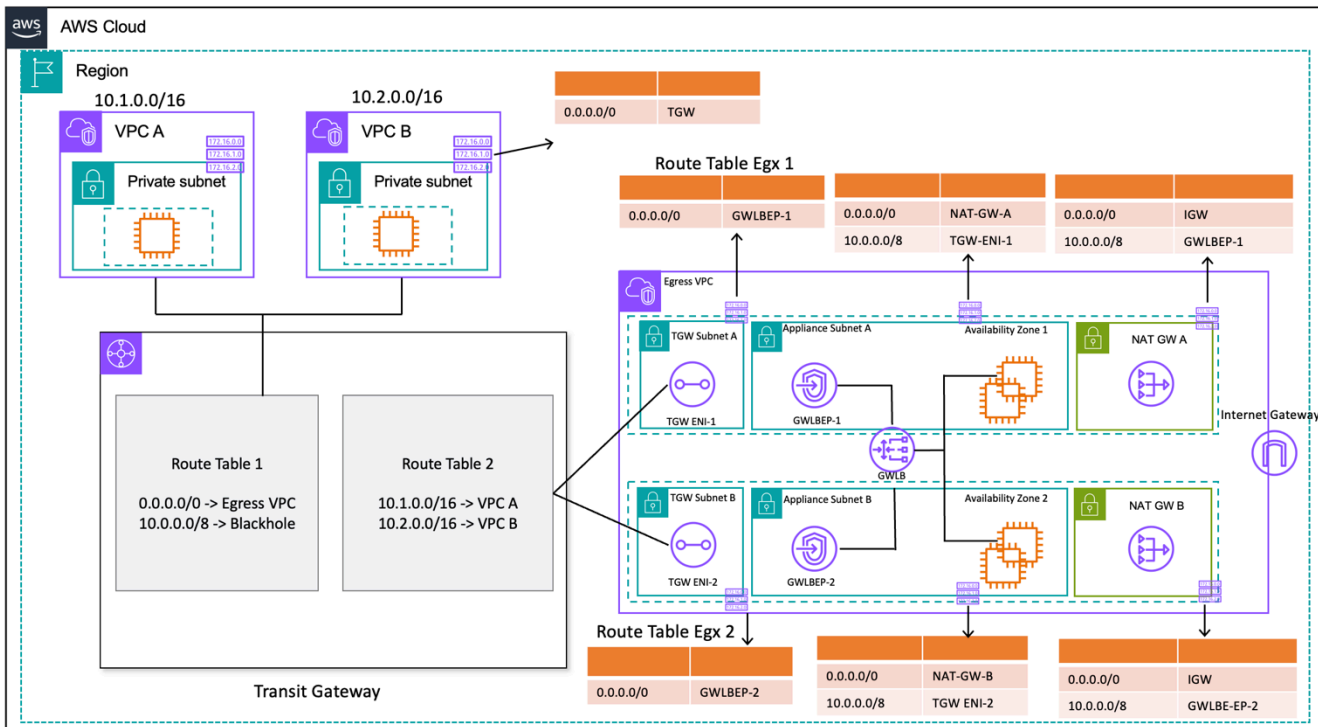
AWS Marketplace および からのソフトウェアベースの仮想アプライアンス (Amazon 上EC2) AWS Partner Network を出口として使用する方法は、NATゲートウェイのセットアップと似ています。このオプションは、さまざまなベンダーが提供する高度なレイヤー 7 ファイアウォール/侵入防止/検出システム (IPS/IDS) およびディープパケットインスペクション機能を使用する場合に使用できます。

次の図では、NATゲートウェイに加えて、Gateway Load Balancer () 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GWLBE。この設定では、Gateway Load Balancer Endpoint (GWLBE) GWLB、仮想アプライアンス、NATゲートウェイVPCは、VPCアタッチメントを使用して Transit Gateway に接続された一元化された にデプロイされます。スポークVPCsはアタッチメントを使用して Transit Gateway にも接続されますVPC。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、 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GWLBE。GWLBE はとして機能し bump-in-the-wire 、すべてのレイヤー 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見えません。したがって、このアーキテクチャでは、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。

トラフィックが 内のアプリケーションからインターネットVPCsに流れ、この設定を逆行する方法の詳細については、[AWS 「Gateway Load Balancer と による集中型検査アーキテクチャ AWS Transit Gateway」](#) 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、トラフィックを正しい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 「Introducing AWS Gateway Load Balancer: Supported architecture patterns」](#) 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、新しいフローを正常なアプライアンスにGWLB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、Connection Draining が可能になり、アプライアンスのCPU急増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、オートスケーリンググループをターゲットとして使用できます。この利点は、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の手間を省くことです。

利点

Gateway Load Balancer と Gateway Load Balancer エンドポイントは、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、境界を越えて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、スケーリングという差別化されていない重労働を排除し、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するためのエンドポイントサービスとしてファイアウォールのスタックを公開できます[AWS Marketplace](#)。これは、Firewall as a Service (FWaaS) と呼ばれ、デプロイを簡素化し、トラフィックを複数の Amazon EC2インスタンスBGPECMPに分散する必要性を排除します。

主な考慮事項

- アプライアンスは、 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GWLB。
- 一部のサードパーティアプライアンスはルーティング ([2 アームモード](#)) をサポートSNATおよびオーバーレイできるため、コストを削減するための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するためです。
- [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](#)のブログ記事の「[セクション 1: TCPキープアライブ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。

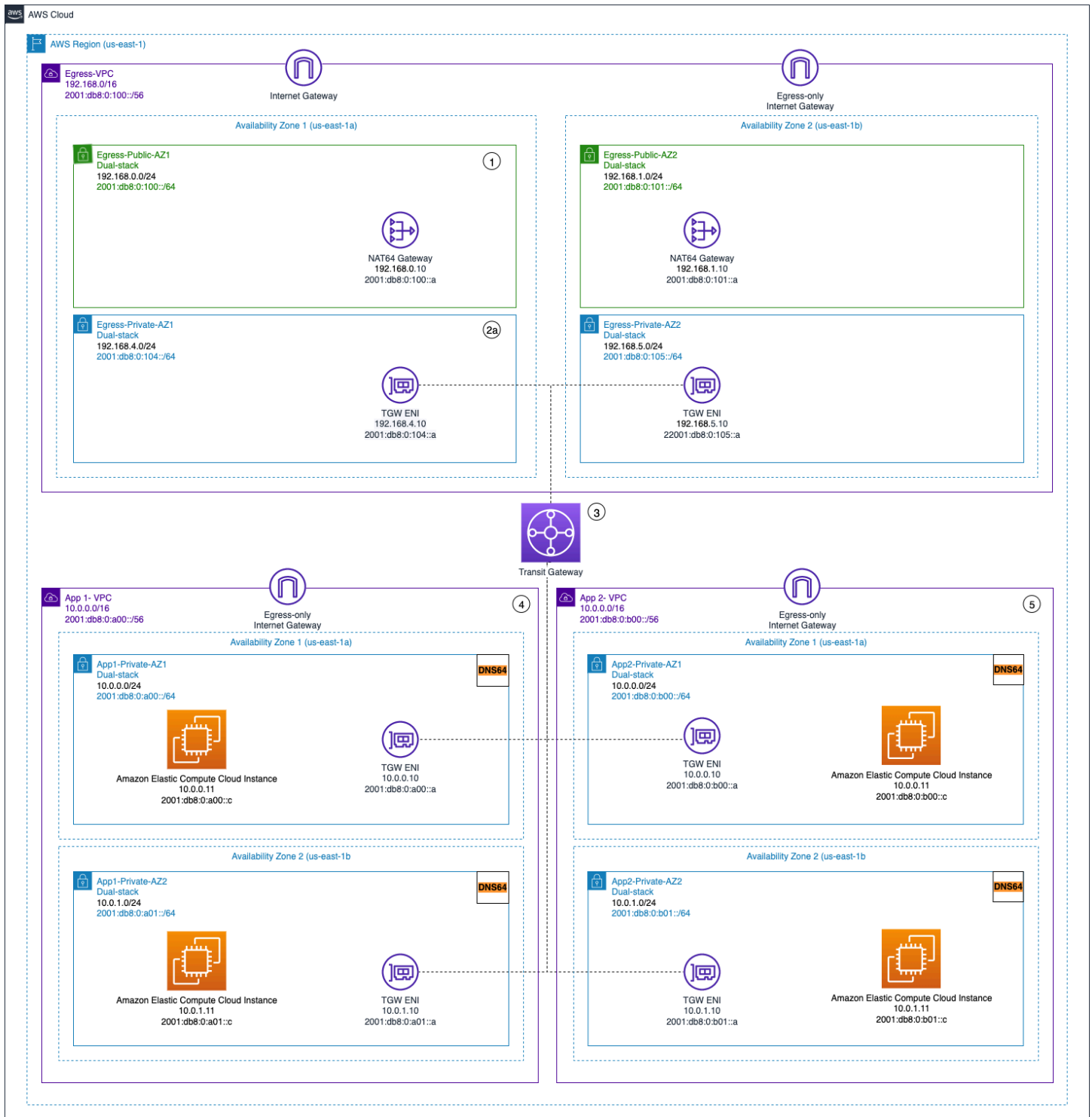
- GWLBE を利用しているため AWS PrivateLink、AWS PrivateLink 料金が適用されます。詳細については、「[のAWS PrivateLink 料金](#)」ページを参照してください。Transit Gateway で集中型モデルを使用している場合は、TGWデータ処理料金が適用されます。
- Transit Gateway と Egress VPCを別のネットワークサービスアカウントにデプロイして、ネットワーク管理者のみがネットワークサービスアカウントにアクセスできるなど、職務の委任に基づいてアクセスを分離することを検討してください。

の一元化された出力 IPv6

一元的なIPv6エグレスを持つデュアルスタックデプロイでエグレスをサポートするには、次の2 IPv4 つのパターンのいずれかを選択する必要があります。

- 分散IPv4出力による集中IPv6出力
- 一元的なIPv4出力と一元的なIPv6出力

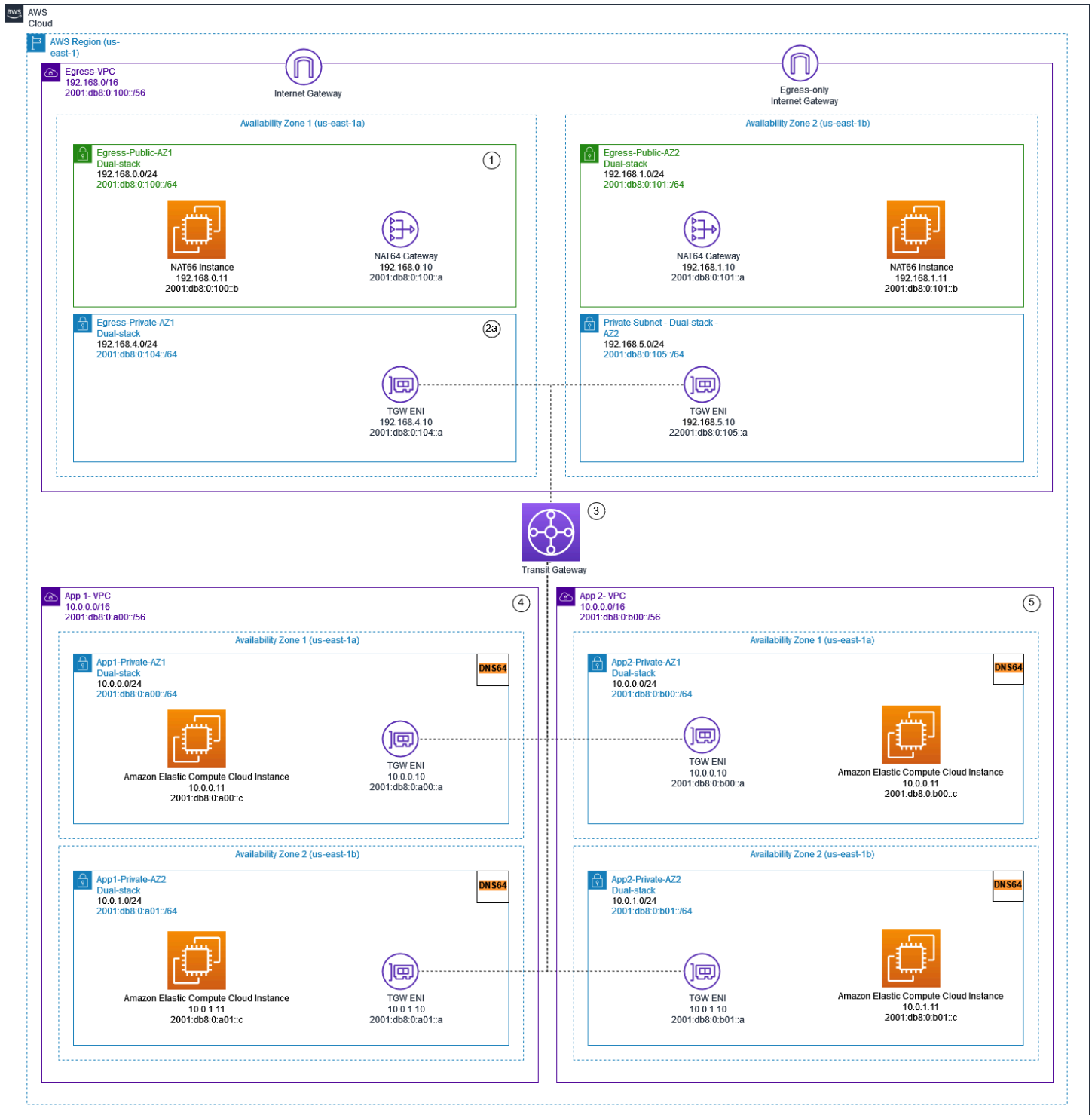
次の図に示す最初のパターンでは、エグレス専用インターネットゲートウェイが各スポークにデプロイされますVPC。Egress-Only インターネットゲートウェイは、内のインスタンスIPv6からのアウトバウンド通信を可能にする、水平スケーリング、冗長化、高可用性のゲートウェイですVPC。これにより、インターネットがインスタンスとIPv6の接続を開始できなくなります。Egress-Only インターネットゲートウェイには料金はかかりません。このデプロイモデルでは、IPv6トラフィックは各の Egress-Only インターネットゲートウェイから流出VPCし、IPv4トラフィックはデプロイされた一元化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



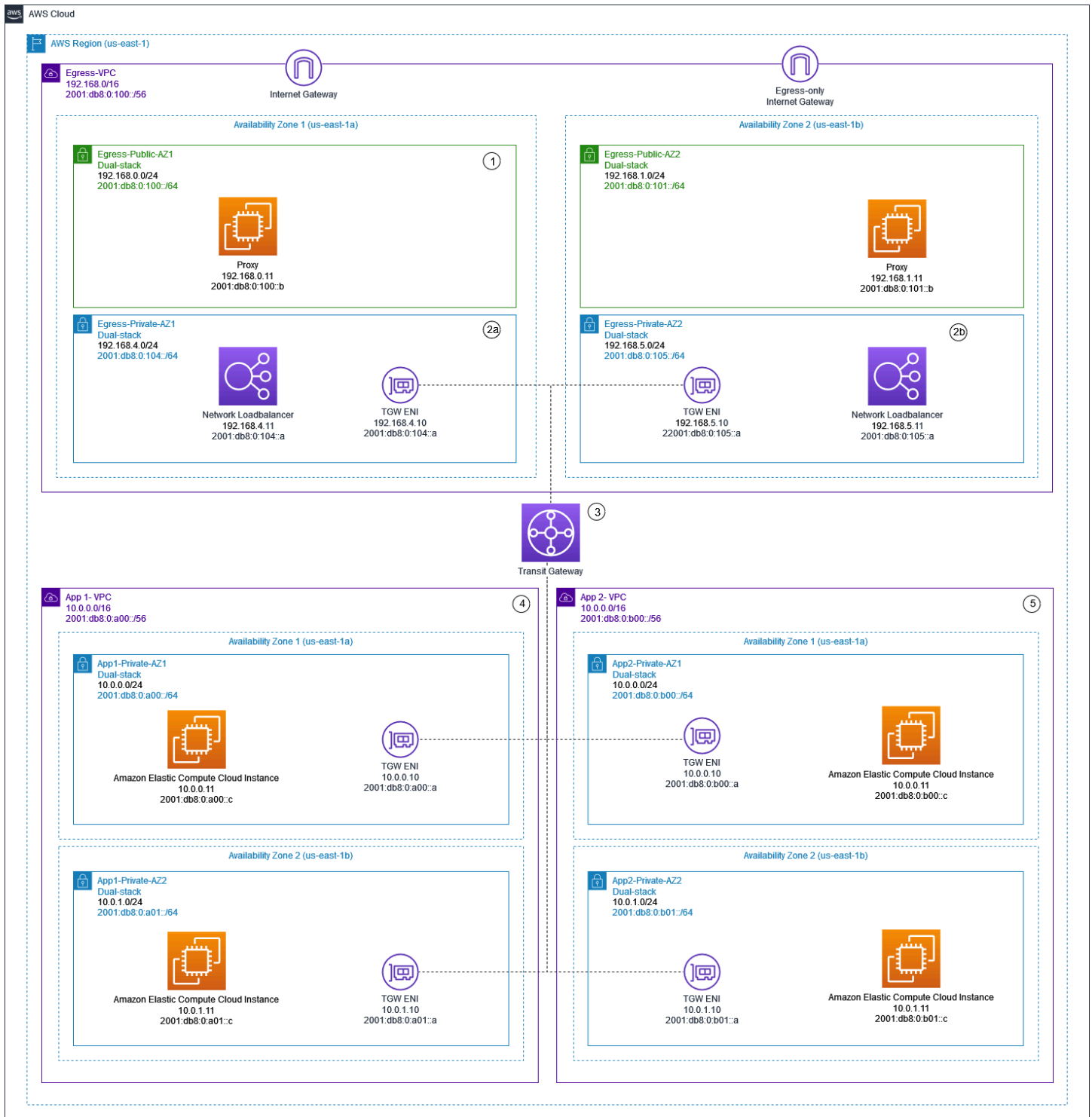
一元的なIPv4出力と分散されたアウトバウンドのみIPv6の出力

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に送信されますVPC。これは、NAT66インスタンスとNATゲートウェイで IPv6からIPv6ネットワークプレフィックスへの変換 (NPTv6) を使用するが、プロキシインスタンスと Network Load Balancer を使

用して実現できます。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、各スポークで実行できない場合に適用されますVPC。



NATゲートウェイとNAT64インスタンスを使用した一元的なIPv6出力



プロキシインスタンスIPv4と Network Load Balancer IPv6 を使用した一元化および出力

[IPv6 AWS ホワイトペーパーのIPv6「」](#)では、一元化された出力パターンについて説明しています。IPv6 Egress パターンについては、ブログ記事「[デュアルスタックIPv4と の一元化されたアウト](#)

[バウンドインターネットトラフィック](#)」で、特別な考慮事項IPv6VPCs、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。

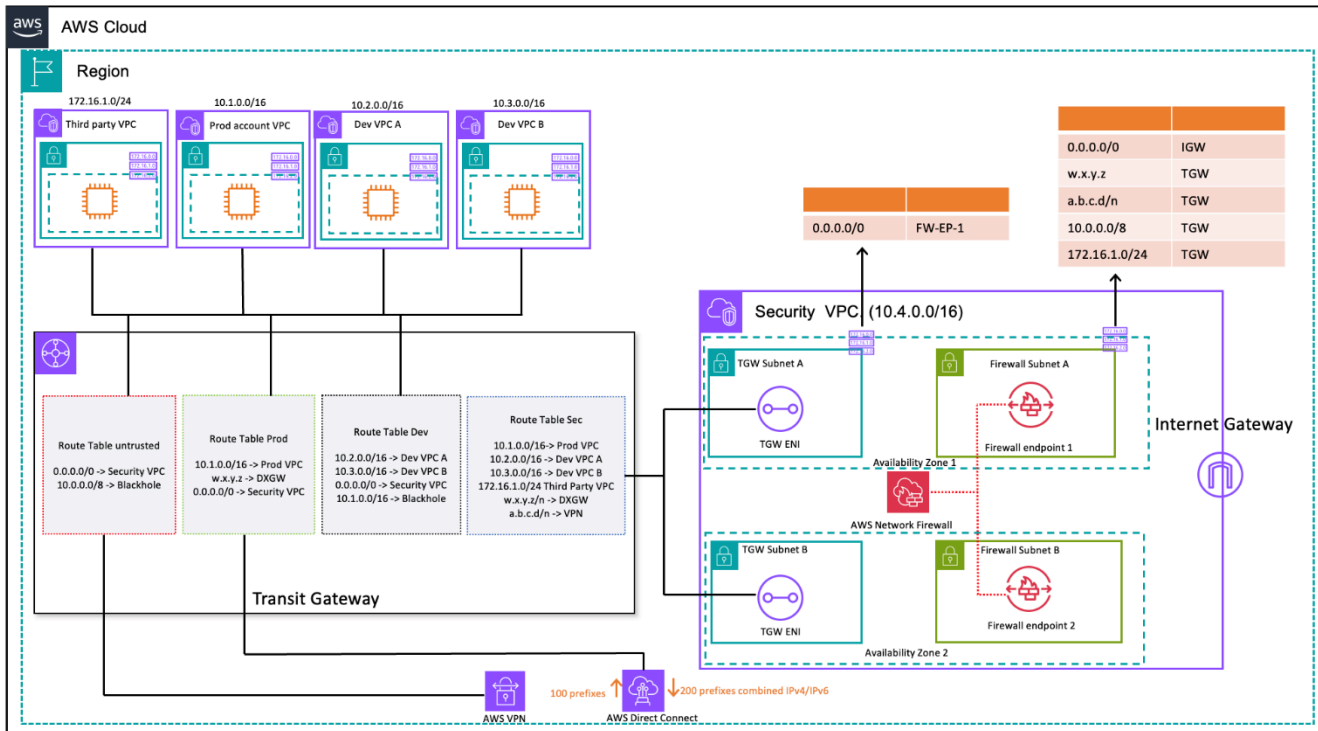
一元化されたネットワークセキュリティ検査モデルの使用に関する考慮事項

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。この 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ゾーン内の 2 つのサブネットに構成されます。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GRESS 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

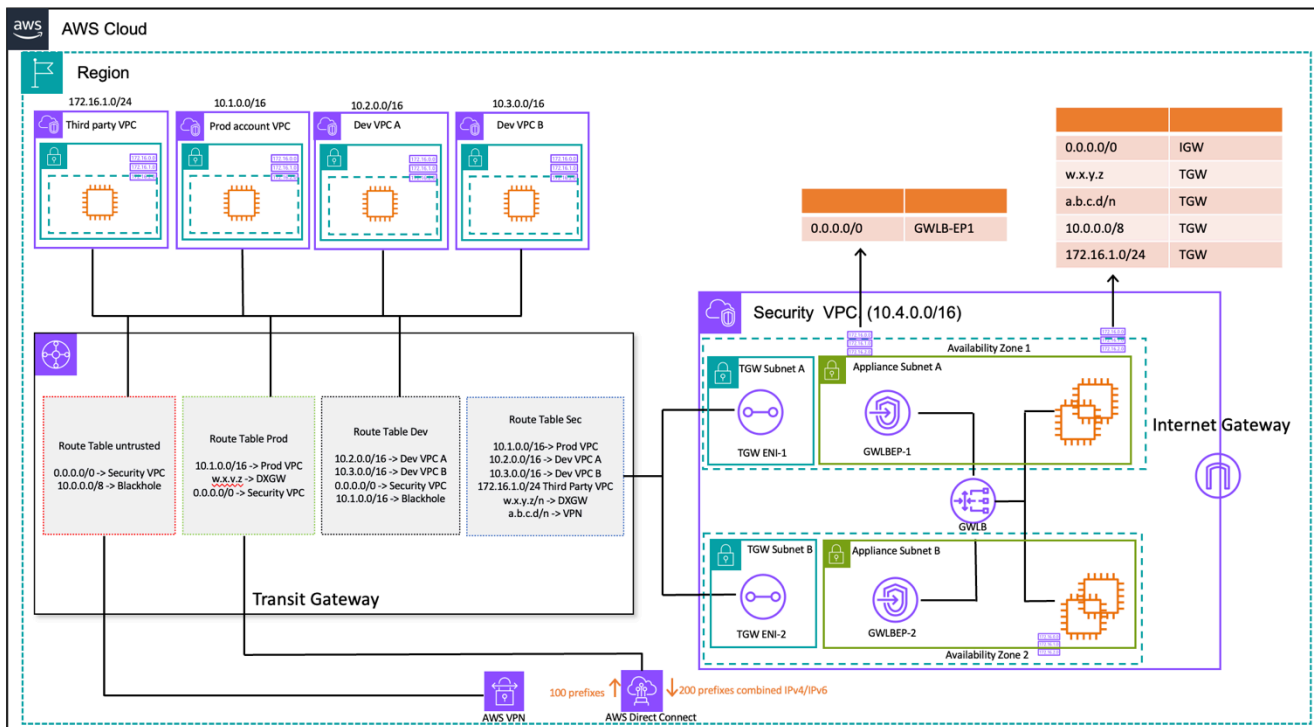
多くの場合、お客様はトラフィックフィルタリングを処理し、セキュリティ検査機能を提供するために仮想アプライアンスを組み込む必要があります。このようなユースケースでは、Gateway Load Balancer、仮想アプライアンス、および Transit Gateway を統合して、VPC から VPC へのトラフィックと VPC to-on-premises トラフィックを検査するための一元化されたアーキテクチャをデプロイできます。

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、 AWS PrivateLink を利用しています	Gateway Load Balancer エンドポイントは、 AWS PrivateLink を利用しています

条件	AWS Network Firewall	Gateway Load Balancer
	<p>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。</p>	<p>トあたり最大 100 Gbps の最大帯域幅をサポートします</p>
コスト	<p>AWS Network Firewall エンドポイントコスト + データ処理料金</p>	<p>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</p>

一元化されたインバウンド検査

インターネット向けアプリケーションの性質上、攻撃領域が大きく、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) やパブリック向けウェブアプリケーションなど) 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、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、Gateway Load Balancer と の両方について、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 を使用して、一元化されたデプロイ AWS Network Firewall で説明します。

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

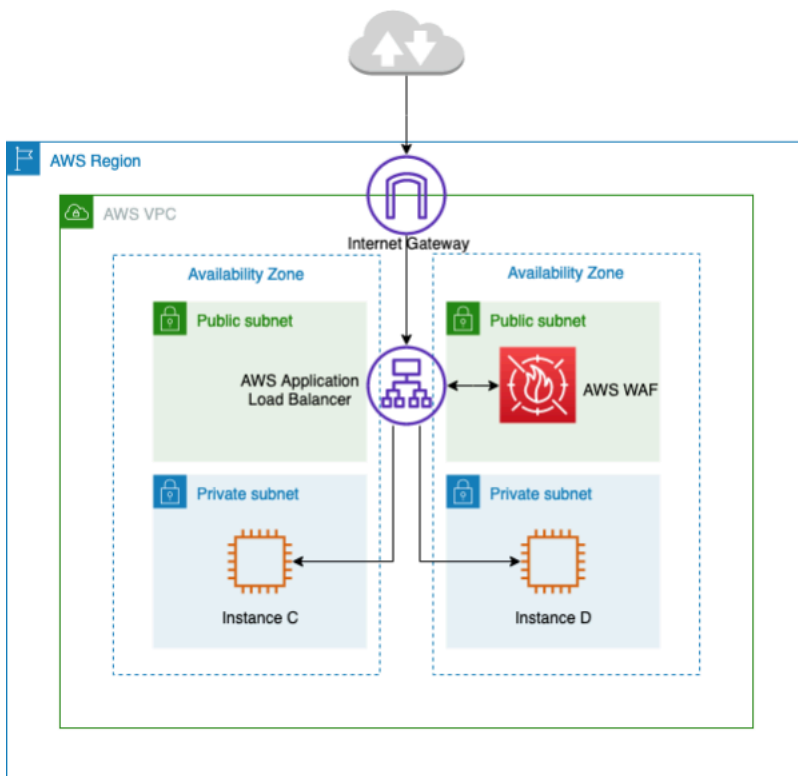
AWS WAF は、可用性に影響を与えたり、セキュリティを侵害したり、過剰なリソースを消費したりする可能性のある一般的なウェブエクスポジイトやボットからウェブアプリケーションまたは APIs を保護するウェブアプリケーションファイアウォールです。AWS WAF は、ボットトラフィックを制御し、SQL インジェクションやクロスサイトスクリプティング (XSS) などの一般的な攻撃パターンをブロックするセキュリティルールを作成できるようにすることで、トラフィックがアプリケーションに到達する方法を制御できるようにします。特定のトラフィックパターンを除外するルールをカスタマイズすることもできます。

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

をデプロイしたら AWS WAF、ビジュアルルールビルダー、JSON のコード、によって管理され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の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。さらに、Amazon を使用して CloudWatch、受信トラフィックのメトリクスとログをモニタリングできます。

内のすべてのアカウントとアプリケーションにわたって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 AWS Firewall Manager すると、共通のセキュリティルールのセットを適用することで、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導入できます。

を使用すると AWS Firewall Manager、Application Load Balancer、API Gateway インスタンス、および Amazon CloudFront distributions. AWS Firewall Manager integrates の AWS WAF ルールを for AWS マネージドルール に簡単にロールアウトできます。これにより AWS WAF、事前設定済みのキュレーションされた 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、[「一元管理 AWS WAF \(API v2\)」](#) および [「による大規模な AWS マネージドルール 管理 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内の複数のアベイラビリティゾーンの 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の負荷分散が行われます。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のおよび広範なボットトラフィックを可視化し、制御できます。
- [マネージドルールを使用すると AWS WAF](#)、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、さらには新たな共通脆弱性識別子 (CVE) などの問題に対処するルールタイプなど、多くの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](#) . AWS WAF gives を介してほぼリアルタイムのログを提供し、ウェブトラフィックをほぼリアルタイムで可視化します。これを使用して、Amazon で新しいルールまたはアラートを作成できます CloudWatch。

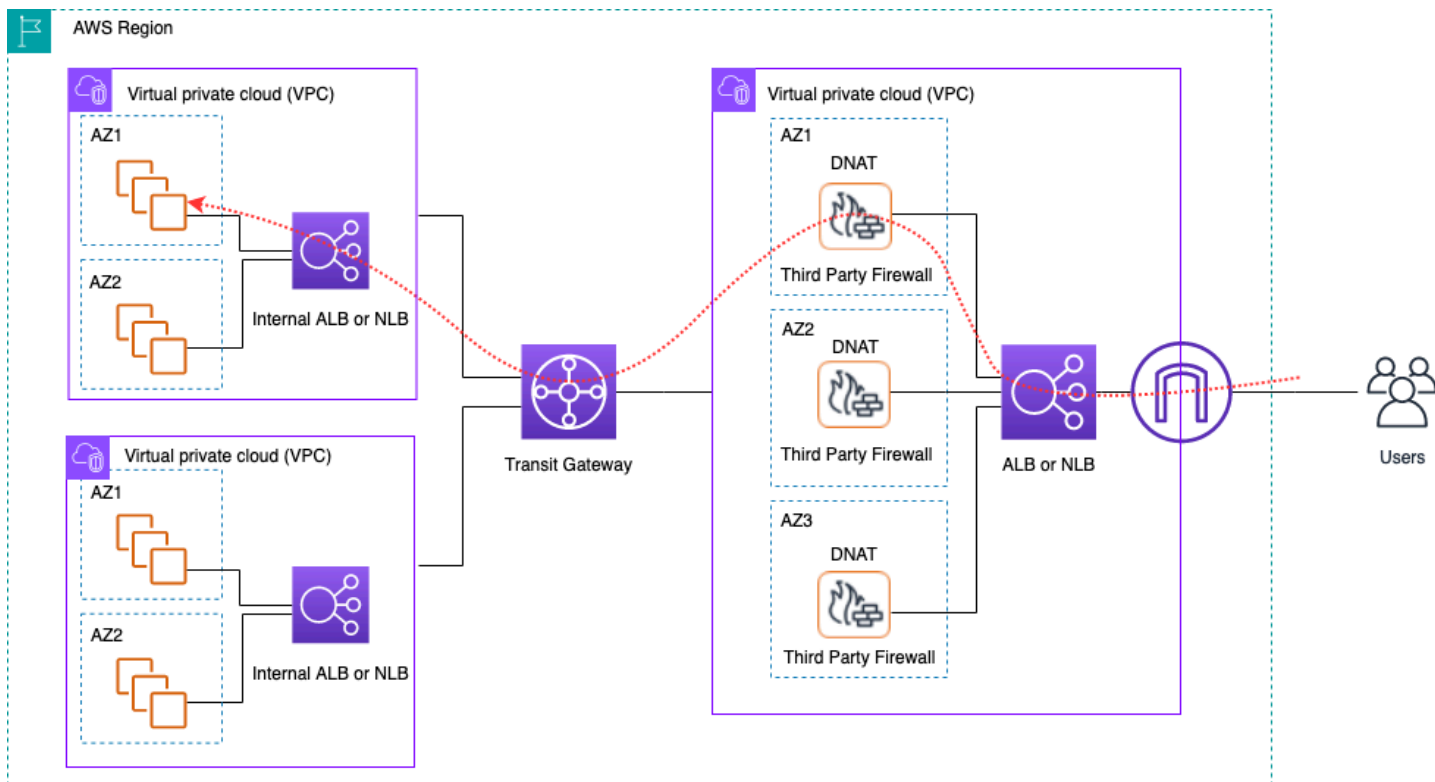
主な考慮事項

- は ALB、ディストリビューション、API Gateway ごとに統合されているため、このアーキテクチャ AWS WAF は HTTP ヘッダー検査と CloudFront 分散検査に最適です。リクエストボディはログに記録 AWS WAF されません。
- 2 番目の ALB セット (存在する場合) に向かうトラフィックは、2 番目の ALB 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、別のインスペクション 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ゾーンに Amazon EC2 Load Balancer 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、アプリケーションタイプに応じて ALB または NLB のいずれかになる内部 ELB によってフロントエンドになります。インターネット経由のクライアントは、トラフィックを Firewall アプライアンスの 1 つに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によるインバウンドセキュリティ検査の詳細については、AWS [環境のブログ記事「サードパーティーファイアウォールアプライアンスを統合する方法」](#)を参照してください。



サードパーティーアプライアンスと 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ため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 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ルアップできます。

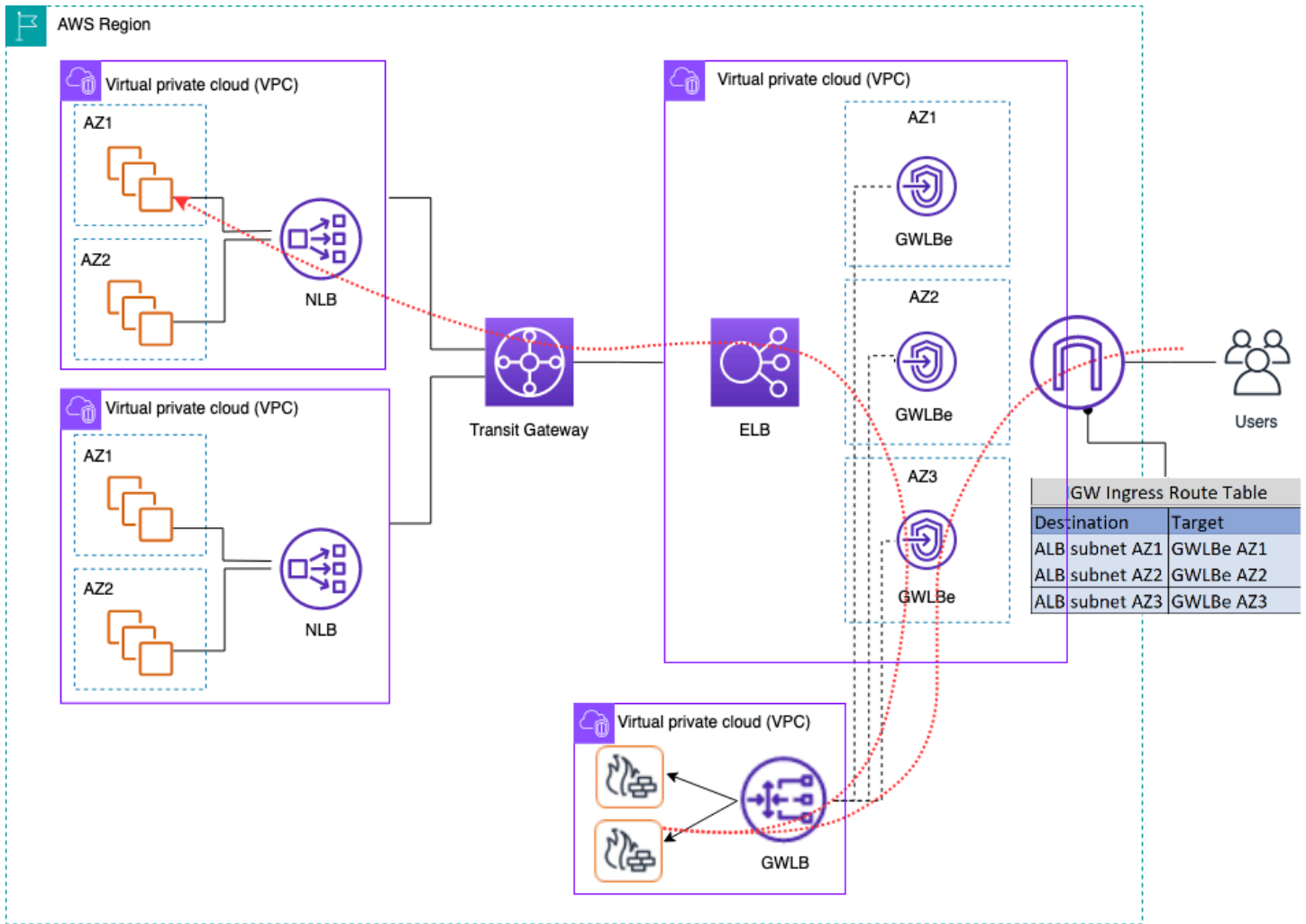
- ELB で Auto Scaling を使用して、インスペクション VPC 内のファイアウォールアプライアンスをスケーリングできます。

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。従来、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。次の図に示すように、Gateway Load Balancer を使用して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、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 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。

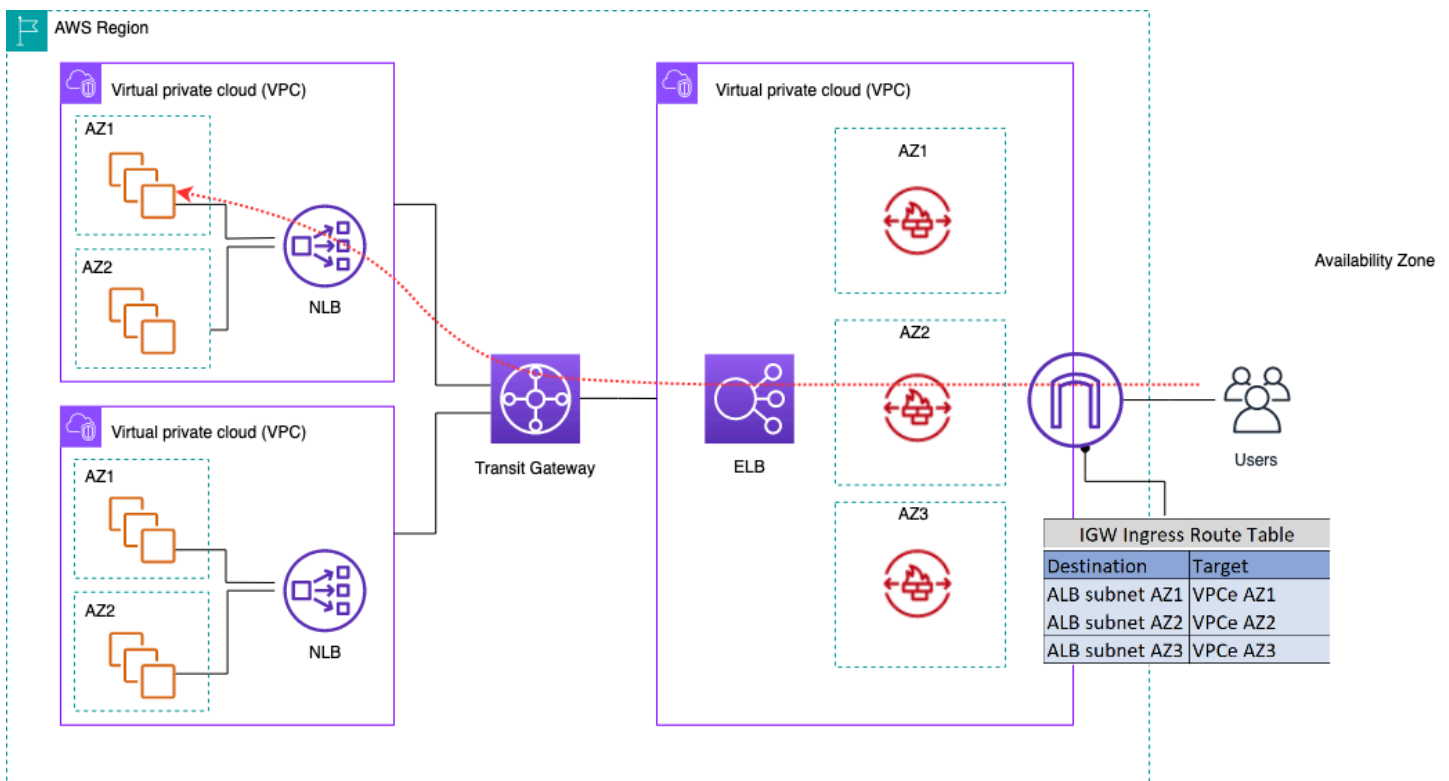
これらの仮想アプライアンスは、インターネットゲートウェイ (IGW) を介して管理インターフェイスにアクセスするか、アプライアンス VPC の踏み台ホスト設定を使用して管理できます。

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インバウンドトラフィックが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

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。[AWS Gateway Load Balancer](#) を使用するさまざまな方法の詳細については、「[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

一元的な進入 AWS Network Firewall に を使用する

このアーキテクチャでは、入カトラフィックは VPCs の残りの部分に到達する AWS Network Firewall 前に によって検査されます。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。スポーク VPC の背後にあるターゲットの Auto Scaling を処理しながら、スポーク VPCs に IP ターゲットを含む ALB または NLB を使用できます。

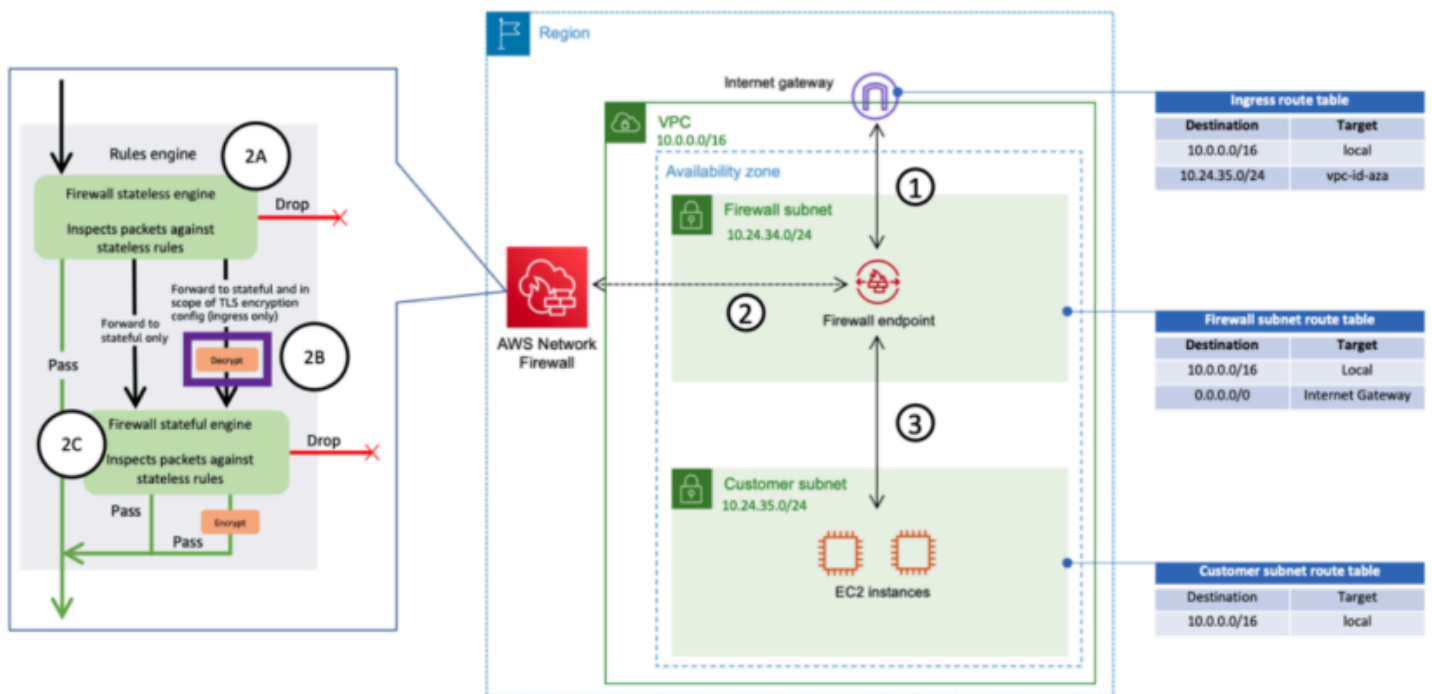


AWS Network Firewall を使用したイングレストラフィック検査

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 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 の分散型デプロイモデルと集中型デプロイモデルの両方をサポートします。ブログ記事「[を使用してデプロイする方法 AWS Network FirewallAWS 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。AWS Certificate Manager (ACM) に保存されている Transport Layer Security (TLS) 証明書を使用すると、Network Firewall はパケットの復号、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。[暗号化されたトラフィックと詳細については、ブログ記事「TLS 検査設定 AWS Network Firewall」](#)を参照してください。



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

集中型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 では、IP アドレスをターゲットタイプとしてのみ使用でき、ホスト名として使用することはできません。前の図では、ターゲットはスポーク VPC 内の 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。

- をファイアウォールエンドポイントの 1 つのペイン 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 に入るとき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 から VPC 内の DNS 解決が得られます (+2 IP オフセットから VPC CIDR へ)。IPv4 デフォルトでは、Route 53 Resolver は EC2 インスタンスのドメイン名や Elastic Load Balancing ロードバランサーなどの 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 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。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。

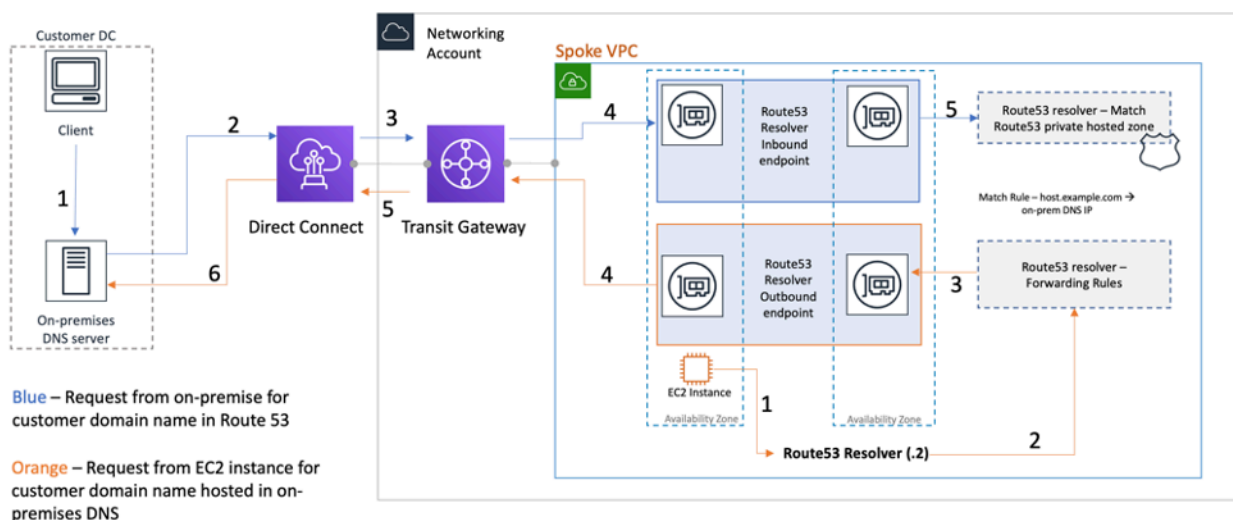
インスタンスをカスタムドメイン名にマッピングする場合は、[Amazon Route 53](#) を使用してカスタム DNS から IP へのマッピングレコードを作成できます。Amazon Route 53 ホストゾーンは、Amazon Route 53 がドメインとそのサブドメインの DNS クエリにどのように応答するかに関する情報を保持するコンテナです。パブリックホストゾーンには、パブリックインターネット経由で解決可能な DNS 情報が含まれていますが、プライベートホストゾーンは、特定のプライベートホストゾーンにアタッチされた VPCs へのみ情報を表示する特定の実装です。複数の VPCs 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、AWS アカウント間およびリージョン間で複数の VPCs に単一のプライベートホストゾーンを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 オフセット 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、アプリケーションが依存するホスト名から IP アドレスへの解決を提供するため、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用意されており、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 AWS 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、Route 53 Resolver の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 の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 内の 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 Resolver エンドポイントにクエリを転送できます。

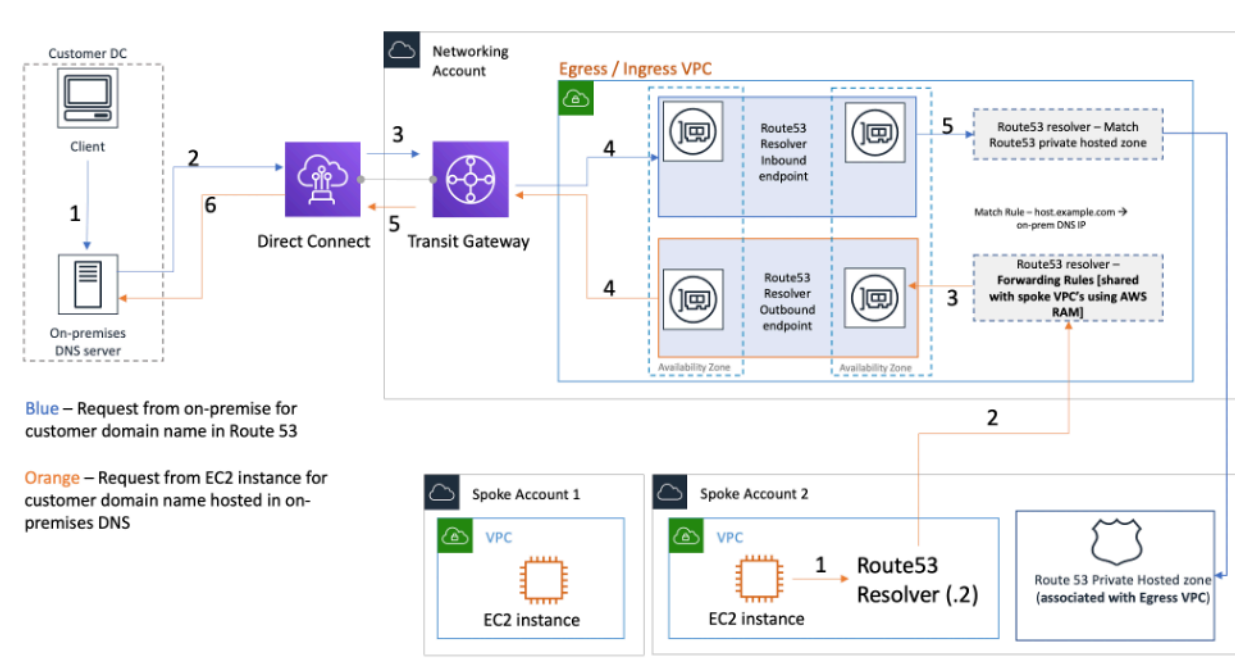


Route 53 Resolver を使用したハイブリッド DNS 解決

これにより、オンプレミスの DNS リゾルバーは、Amazon EC2 インスタンスや、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 ごとに 1 秒あたり最大約 10,000 件のクエリを処理できるため、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。それらを中央出力 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 (作成するインバウンド/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は、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** — ネットワークサービスアカウントを使用して、リゾルバールールを書き込みます (DNS クエリがオンプレミス DNS サーバーに転送される基準)。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 に関連付けます)。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。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トエンドポイントの IP を使用しないでください。スポーク VPCs は、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 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。前の図に示すように、PHZ と集中型 VPC の関連付けにより、オンプレミスサーバーは集中型 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 を解決できるようになります。ハイブリッド DNS 設定の詳細については、[「Amazon Route 53 と AWS Transit Gateway を使用したハイブリッドクラウドの集](#)

[中型 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、お客様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 用 Amazon Route 53 Resolver DNS Firewall 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、接続、または VPN 接続を必要とせずに、をVPCサポートされている AWS サービスにプライベート AWS 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は公開されません。のインスタンスは、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するためにパブリック IP アドレスを必要としVPCません。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。これらは水平方向にスケーリングされ、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VPCにアクセスするすべての 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、顧客が複数の 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VPCs。これを回避するには、一元化された でインターフェイスエンドポイントをホストできますVPC。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 を有効にできますDNS。有効にすると、設定はAWSマネージド Route 53 プライベートホストゾーン (PHZ) を作成します。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。マネージドは、インターフェイスエンドポイントVPCを持つ 内でPHZ のみ機能します。このセットアップでは、一元化された VPCs でDNSホストされているVPCエンドポイントをスポークで解決できるようにするとVPC、 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DNS時にプライベート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 Management Console 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 フィールドを入力し、レコードタイプを 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. 「トラフィックを にルーティングする」セクションで、トラフィックの送信先となるサービスを選択し、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、ターゲットのヘルス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VPCs内の他のホストゾーンに[関連付け](#)ます。この設定により、スポークはフルサービスエンドポイント名を一元管理された のインターフェイスエンドポイントに解決VPCsできますVPC。

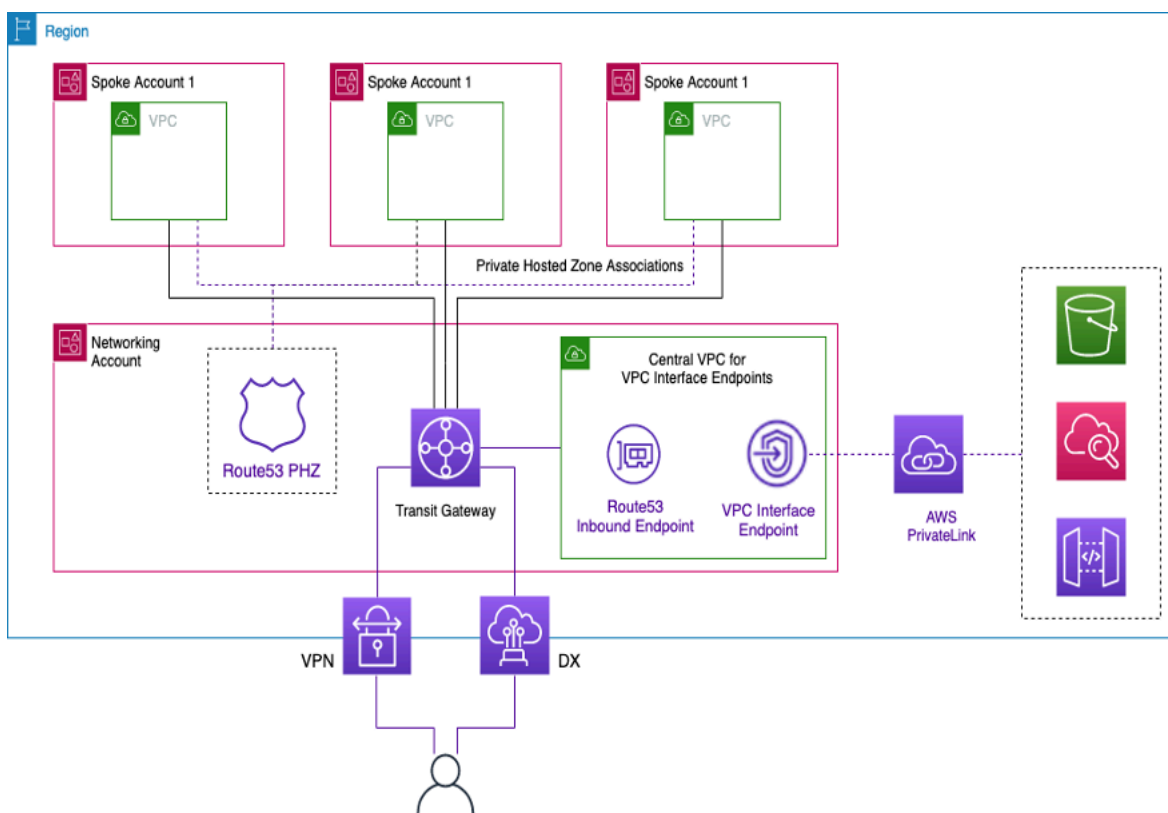
Note

共有プライベートホストゾーンにアクセスするには、スポークのホストVPCsが の Route 53 Resolver IP を使用する必要がありますVPC。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 はスポークから集中型インターフェイスエンドポイントVPCs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VPCsでスポークと共有します。エンドポイント情報を他の と共有する方法の詳細についてはVPCs、[「Integrating AWS Transit Gateway with AWS PrivateLink and Amazon Route 53 Resolver」](#) ブログ記事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 あたりのエンドポイントVPC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ですべてのスポークVPCアクセスのポリシーを適用および管理します。の数が増えるにつれてVPCs、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

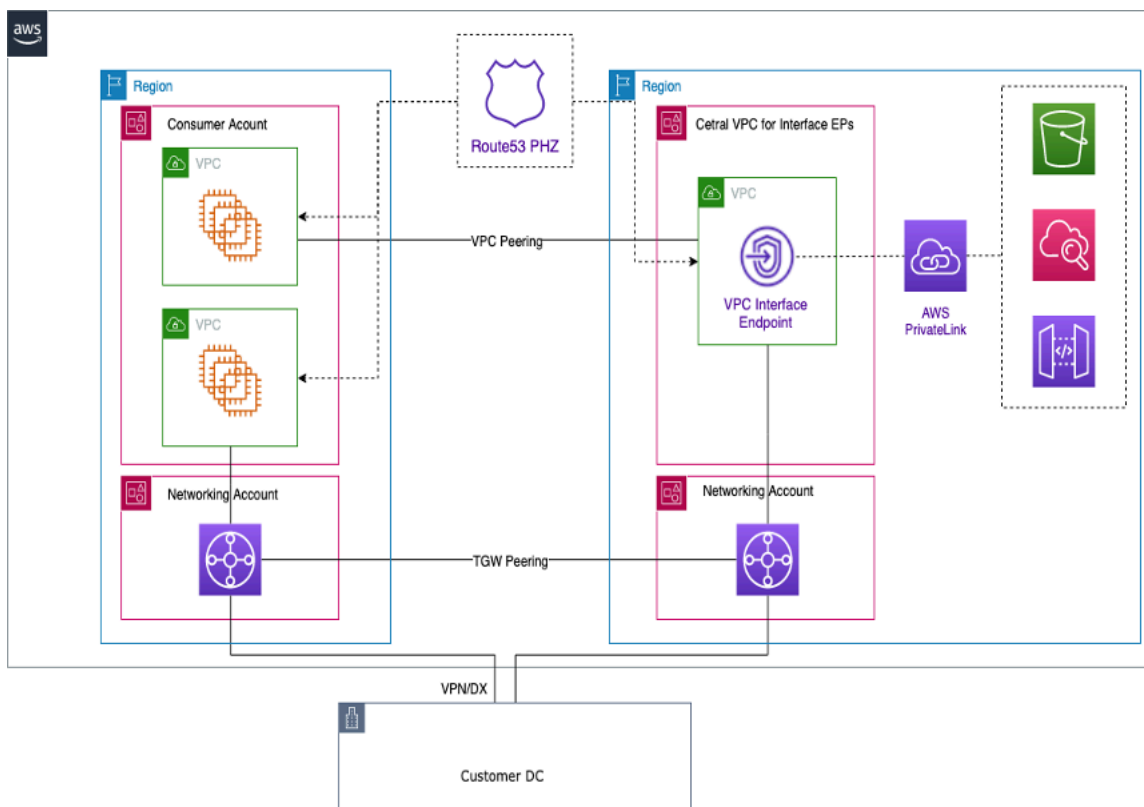
クロスリージョンエンドポイントアクセス

共通のVPCエンドポイントを共有する異なるリージョンで複数のVPCs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VPCsの両方が、エンドポイントのエイリアスPHZを持つに関連付けられます。マルチリージョンアーキテクチャVPCsで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、

このブログ「[クロスアカウントの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。

VPCs 異なるリージョンのは、Transit Gateway または Peering VPC 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、VPCus-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VPCを介してトラフィックをus-west-2リージョンに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 VPC のサービス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エンドポイントのエイリアスPHZを使用して 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VPCsの が、作成した PHZ に関連付けられていることを確認します。

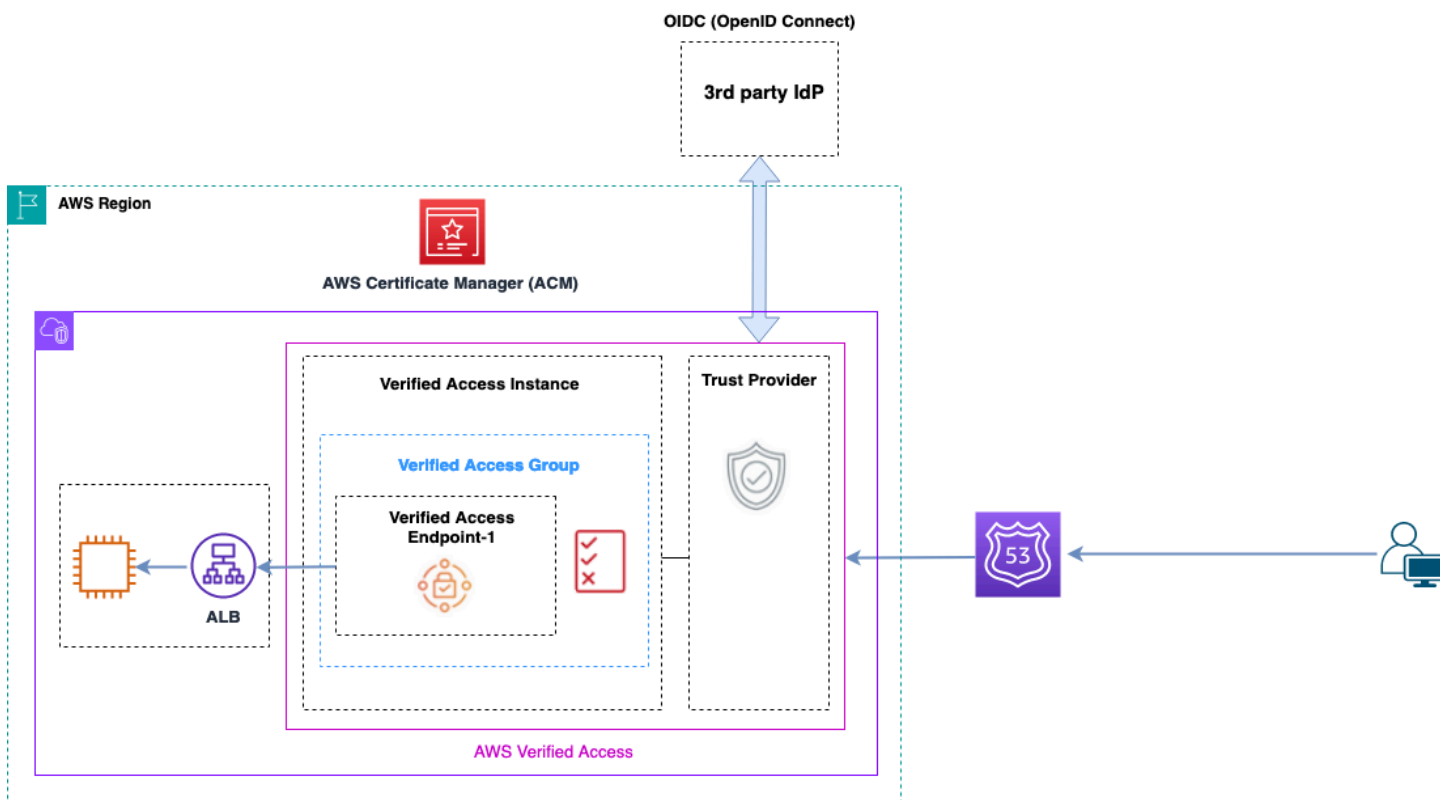
エンドポイントを複数のアベイラビリティーゾーンにデプロイする場合、 から返されるエンドポイントの IP アドレスは、割り当てられたアベイラビリティーゾーン内の任意のサブネットからDNS取得されます。

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

AWS Verified Access

AWS Verified Access は、 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VPN。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してユーザーを接続します。Verified Access は、アイデンティティ対応の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 とデバイスのヘルスは、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せん。

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 とデバイスセキュリティの状態の管理を容易にするサービスです。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 メールアドレスやそれらが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が受信され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 ランディングゾーンでアプリケーションの使用をスケーリング 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えます。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、スケーラビリティ、高可用性、セキュリティを確保しながら、コストを低く抑える方法について説明しました。Transit Gateway、共有 VPC、VPC エンドポイント AWS Direct Connect、Gateway Load Balancer、Amazon Route 53 AWS Network Firewall、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使用する際は、適切な設計上の決定を行うことが不可欠です。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

本書への貢献者:

- アマゾン ウェブ サービス、ソリューションアーキテクト、Sohaib Tahir
- Shirin Bhambhani、ソリューションアーキテクト、Amazon Web Services
- アマゾン ウェブ サービス、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
- Tushar Jagdale、ソリューションアーキテクト、Amazon Web Services
- 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
- Nick Kniveton、ソリューションアーキテクト、Amazon Web Services
- Sidhartha Chauhan、プリンシパルソリューションアーキテクト、Amazon Web Services

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、AWS Direct Connect Sitelink、データ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、より一貫性を持たせ、DX 接続オプションを更新してプライベート IP VPN を含め、全体で多数の小さな変更を加えました。	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 セクションを更新し、Transit VPC セクショ	2022 年 2 月 22 日

ンを更新しました。また、MA Csec と障害耐性に関する推奨事項で AWS Direct Connect セクションを更新しました AWS PrivateLink 。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 間および VPC オンプレミスの集中型ネットワークセキュリティを VPC に更新し、と AWS Network Firewall 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出力しました。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 ピアリングの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、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、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。

© 2019 Amazon Web Services, Inc. or its affiliates. All rights reserved.

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。