Cisco Cloud ACI

ハイブリッド マルチクラウド設計ガイド

目次

このドキュメントの目的

このドキュメントでは、AWS および Microsoft Azure を使用した Cisco® Cloud Application Centric Infrastructure（Cisco Cloud ACI®）の設計オプションおよび導入に関する考慮事項について説明します。次のユースケースを取り上げます。

- 複数のサイトにまたがるアプリケーション（テナント内）
- ハイブリッドマルチクラウド環境での共有サービス
- クラウド ネイティブ ルーティング機能を使用したクラウドからインターネットへの接続
- オンプレミスの L3 外部（L3Outs）を介したクラウドから外部ネットワークへの接続
- クラウド ネイティブ ルーティング サービスを使用した外部サイトへの接続
- WAN、ブランチ、または非 ACI サイトへの外部接続
- SD-WAN ソリューションとの相互運用
- ロードバランサの挿入
- ファイアウォールの挿入
- マルチノードサービスの挿入
- Microsoft Azure でのクラウド ネイティブ サービスの統合
- Microsoft Azure および AWS でのブラウンフィールド インポート

前提条件

このドキュメントは、読者が Cisco ACI および Cisco Cloud ACI テクノロジーの基本的な知識を持っていることを前提としています。

Cisco Cloud ACI は、複数のオンプレミス Cisco ACI データセンターおよびパブリッククラウドプラットフォーム全体でポリシーとネットワーク接続を管理する機能を提供します。詳細については、『Cisco Cloud ACI on AWS ホワイトペーパー』および『Cisco Cloud ACI on Microsoft Azure ホワイトペーパー』を参照してください。

Cisco ACI サービスグラフは、ファイアウォール、ロードバランサ、侵入防御システム（IPS）などのレイヤ 4 からレイヤ 7 のサービスを挿入する機能を提供します。詳細については、『Cisco ACI サービスグラフの設計ホワイトペーパー』を参照してください。

用語

このドキュメントで使用されている以下の用語を理解しておいてください。

- Cisco ACI および Cisco Cloud ACI の用語：
    - Cisco Cloud Application Policy Infrastructure Controller（Cisco Cloud APIC）
    - Nexus Dashboard Orchestrator（NDO）
    - Virtual Routing and Forwarding（VRF）
    - ブリッジドメイン（BD）
    - エンドポイント グループ（EPG）

- レイヤ 3 外部（L3Out）または外部ルーティングネットワーク（L3Out）
- レイヤ 3 外部のサブネットベースの EPG（L3Out 外部 EPG）
- サービス グラフ

- AWS の用語：
  - 仮想プライベート クラウド（VPC）
  - Security Group（SG）
  - Application Load Balancer（ALB）
  - Network Load Balancer（NLB）
- Azure の用語：
  - 仮想ネットワーク（VNet）
  - ネットワーク セキュリティ グループ（NSG）
  - アプリケーション セキュリティ グループ（ASG）
  - Azure Application Gateway
  - Basic Load Balancer
  - Standard Load Balancer
  - Microsoft Enterprise エッジルータ（MSEE）

はじめに

このドキュメントの主な目的は、Cisco Cloud ACI ハイブリッドマルチクラウドのユースケースに関する設計ガイドラインを提供することです。ACI マルチクラウドは、オンプレミスの Cisco ACI、サイト、Amazon パブリック クラウド（AWS）、Microsoft Azure（Azure）などの複数のクラウド環境を相互接続するために使用するソリューションです。

次の図は、オンプレミスの ACI ファブリック、AWS 環境、および Microsoft Azure 環境を接続する Cloud ACI の簡単なトポロジの例を示しています。

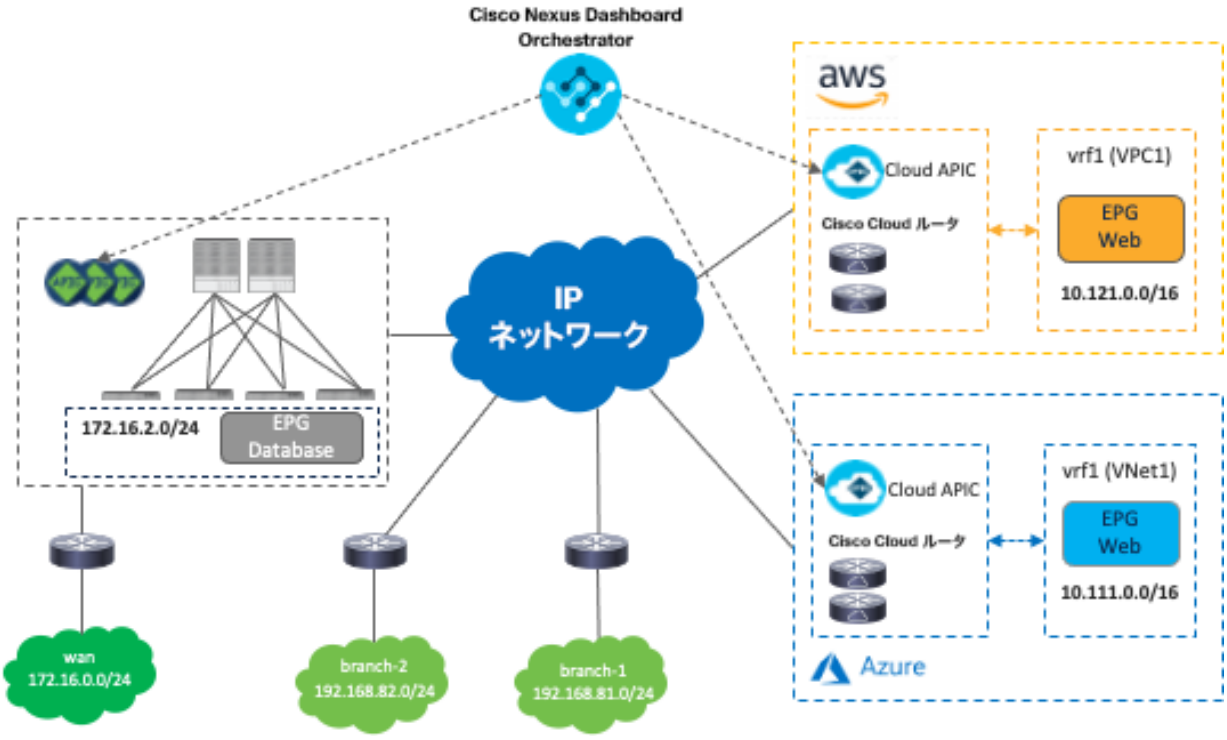

図 1. Cloud ACI ハイブリッドマルチクラウドの概要ソリューション

図 1 に示すように、Cisco Cloud ACI は次のコンポーネントで構成されています。

- Cisco Nexus Dashboard Orchestrator（NDO）：NDO は中央ポリシーコントローラとして機能し、各クラウドサイトを独自の Cloud APIC によって抽象化して、複数のオンプレミスの Cisco ACI データセンターおよびパブリッククラウドプラットフォームに全体でポリシーを管理します。NDO は Nexus ダッシュボード上のサービスとして実行されます。Nexus ダッシュボードは、VMware ESXi、Linux KVM、Amazon Web Services、または Microsoft Azure で実行される物理アプライアンスまたは仮想マシンのクラスタとして展開できます。以前にバージョン間サポートが導入されているため、NDO は、異なるソフトウェアバージョンを実行しているオンプレミス APIC とクラウド APIC を管理できます。

- Cisco Cloud APIC：Cisco Cloud APIC は、サポートされているパブリッククラウド上で仮想インスタンスとして実行され、パブリッククラウド内の自動接続、ポリシー変換、およびワークロードのさらなる可視性を提供します。Cisco Cloud APIC は、NDO から受け取ったすべてのポリシーを変換し、それらをクラウドネイティブの構造（AWS の VPC やセキュリティグループ、Microsoft Azure の VNet、アプリケーション セキュリティ グループ、ネットワーク セキュリティ グループなど）にプログラムします。Cloud APIC は、AWS Marketplace や Azure Marketplace などのパブリッククラウド マーケットプレイスを通じて展開されます。

- Cisco Cloud ルータ(CCR)：Cisco Cloud ルータは、パブリッククラウドプラットフォームの重要なコンポーネントです。CCR は、オンプレミスサイトおよびパブリッククラウドプラットフォームへのサイト間通信に使用されます。さらに、CCR は Microsoft Azure 内の VNet 間通信にも使用されます。このドキュメントでは CCR という用語を使用していますが、Cisco Cloud APIC のリリース 25.0(3) より前は、Cisco Services Router 1000V（CSR1000V または CSR）が CCR として使用され、Cisco Cloud APIC のリリース 25.0(3) からは、Cisco Catalyst 8000V（C8000V）が、新しい Cloud ACI の展開でデフォルトの CCR とし

て使用されていることに注意してください。C8000V は、より優れたパフォーマンスを提供する新しいクラウド仮想ルータプラットフォームです。CSR を使用するリリース 25.0(3) より前の既存の Cloud ACI の展開の場合、Cloud APIC がリリース 25.0(3) 以降にアップグレードされた場合は、古い CSR1000V から新しい C8000V に移行する必要があります。移行中、CSR は一度に 1 つずつ停止するため、キャパシティは減少しますが、トラフィックの中断は最小限に抑えられます。リリース 25.0(3) 以降、Cloud APIC ユーザーインターフェイスでは、C8000V を CCR（Cisco Cloud ルータ）呼んでいます。

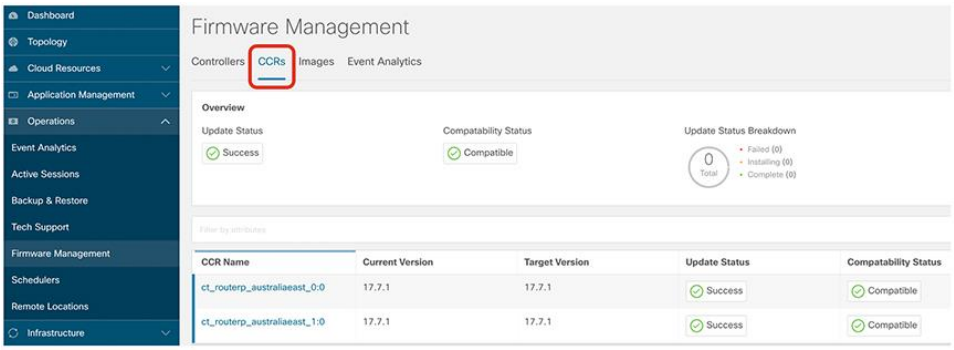

図 2. Cisco Cloud ルータ- CCR

- オンプレミス ACI ファブリック（オプション）：オンプレミス ACI ファブリックは Cisco APIC によって管理されます。Cisco Cloud ACI では、オンプレミス ACI ファブリックの存在は必須ではありませんが、オンプレミスのデータセンターとパブリッククラウドプラットフォームの両方があるのが一般的です。

Cloud ACI ポリシーモデル

このセクションでは、Cisco ACI、AWS、および Microsoft Azure のネットワークとセキュリティモデルについて簡単に説明します。これは、クラウドプロバイダーごとに構造と用語がわずかに異なるためです。たとえば、オンプレミスの ACI ファブリックの VRF は、AWS の VPC および Microsoft Azure の VNet として解釈できますが、同一ではありません（VPC や VNet は複数のルーティングテーブルを持つことができますが、VRF で持つことができるルーティングテーブルは 1 つです）。さらに、オンプレミスの ACI ファブリックの VRF は、AWS の複数の VPC（リージョン 1 の VPC1 およびリージョン 2 の VPC2）、および Microsoft Azure の複数の VNet（リージョン 1 の VNet1 およびリージョン 2 の VNet2）として解釈できます。

その他の例を次に示します。

- Cisco ACI ネットワークポリシーモデルは、テナント、ブリッジドメイン（BD）、ブリッジドメインサブネット、エンドポイントグループ（EPG）、およびコントラクトを使用します。
- AWS は、ユーザーアカウント、Virtual Private Cloud（VPC）、セキュリティグループ、セキュリティグループ ルール、およびネットワーク アクセス リストを使用します。
- Microsoft Azure は、リソースグループ、仮想ネットワーク（VNet）、アプリケーション セキュリティグループ（ASG）、ネットワーク セキュリティ グループ（NSG）、アウトバウンドルール、およびインバウンドルールを使用します。

次の図は、Cisco ACI、AWS、および Microsoft Azure のネットワークおよびセキュリティモデルを示しています。

図 3. Cisco ACI の EPG ベースのネットワークモデル

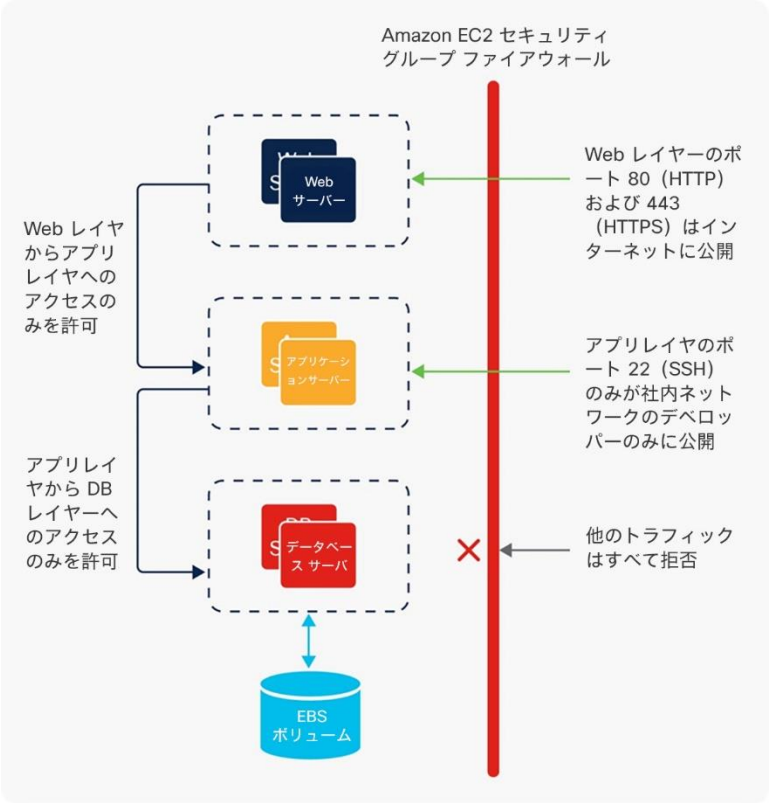

図 4. AWS の SG ベースのネットワークモデル

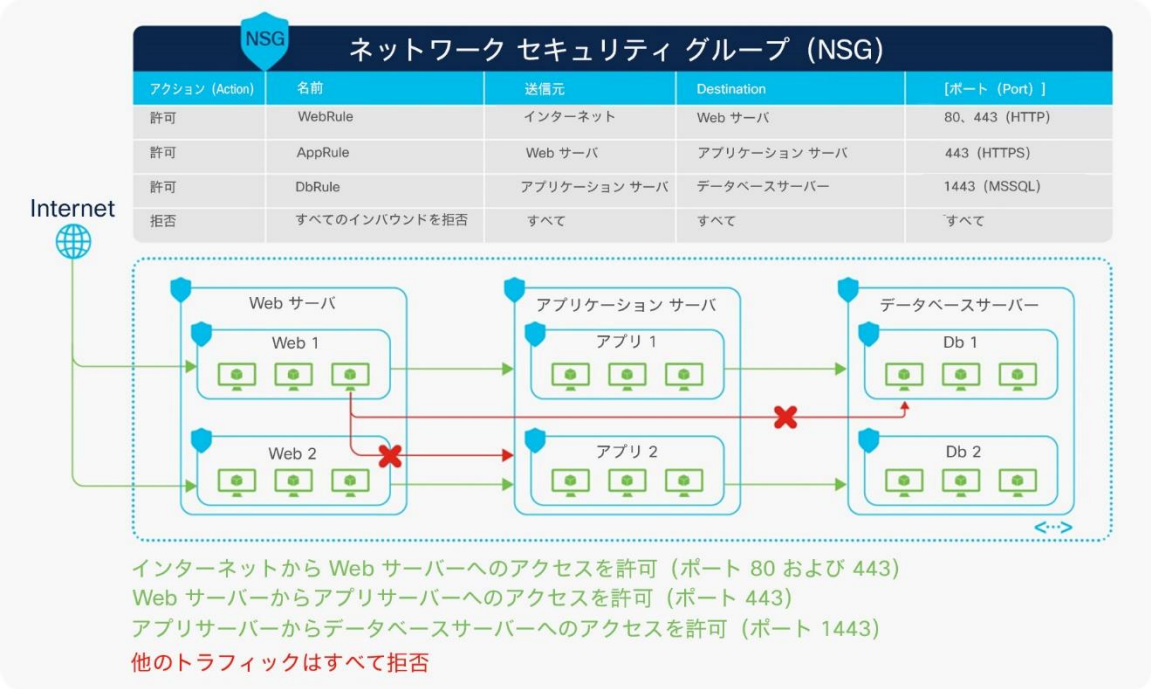

図 5. Microsoft Azure のセキュリティグループベースのネットワークモデル

運用とセキュリティを容易にする一貫したポリシーモデルを実現するには、オンプレミスの ACI サイトとパブリッククラウドプラットフォームの異なるオブジェクト間で、同じパースペクティブを維持するためのマッピングモデルが必要です。たとえば、管理者はポリシー規則を定義して、Web サーバーが特定のポートでデータベースサーバーと通信するようにできます。ポリシー規則は、場所に関係なくすべてのエンドポイントに適用されます。

Nexus Dashboard Orchestrator がモデルを作成し、オブジェクトとポリシーが、オンプレミスの ACI サイトの APIC コントローラと AWS または Azure の Cloud APIC によって、物理ファブリックとクラウド インフラストラクチャ上の具体的なオブジェクトにレンダリングされます。

図 6 と 7 は、Cisco ACI ポリシーモデルのオブジェクトと、AWS や Microsoft Azure で利用可能なクラウド ネイティブ コンストラクト間のマッピングを示しています。次に例を示します。

- ACI のコントラクトは、AWS のセキュリティグループ（SG）ルールや Microsoft Azure のネットワーク セキュリティ グループ（NSG）ルールにマップされます。
- コントラクトルールは、AWS の SG ルールや Microsoft Azure の NSG ルールにマッピングされます。

セキュリティルールが適用される場所は、クラウド環境によって異なります。AWS の場合、SG ルールは AWS インスタンス（クラウドエンドポイント）のネットワークインターフェイスに直接適用されます。Microsoft Azure の場合、Cloud ACI バージョン 5.1(2) から、NSG ルールは、仮想マシンが存在する Azure 上のサブネットに適用されます。仮想マシンは、NSG の送信元または接続先を参照するアプリケーション セキュリティ グループ（ASG）にグループ化されます。これらのマッピングはすべて、Cloud ACI ソリューションの重要なコンポーネントの 1 つである Cloud APIC によって、動的にレンダリングされます。

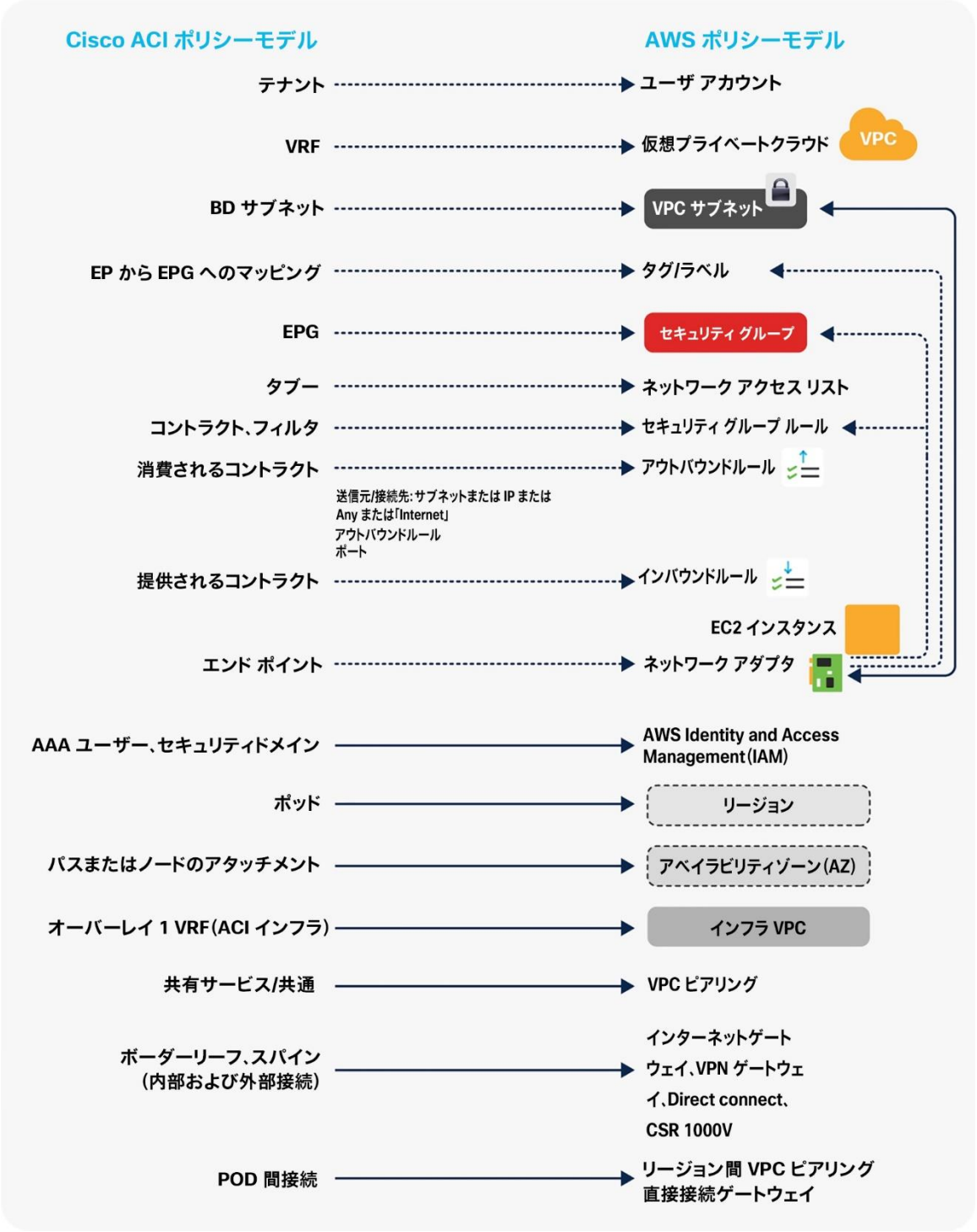

図 6. Cisco ACI ポリシーモデルから AWS へのマッピング

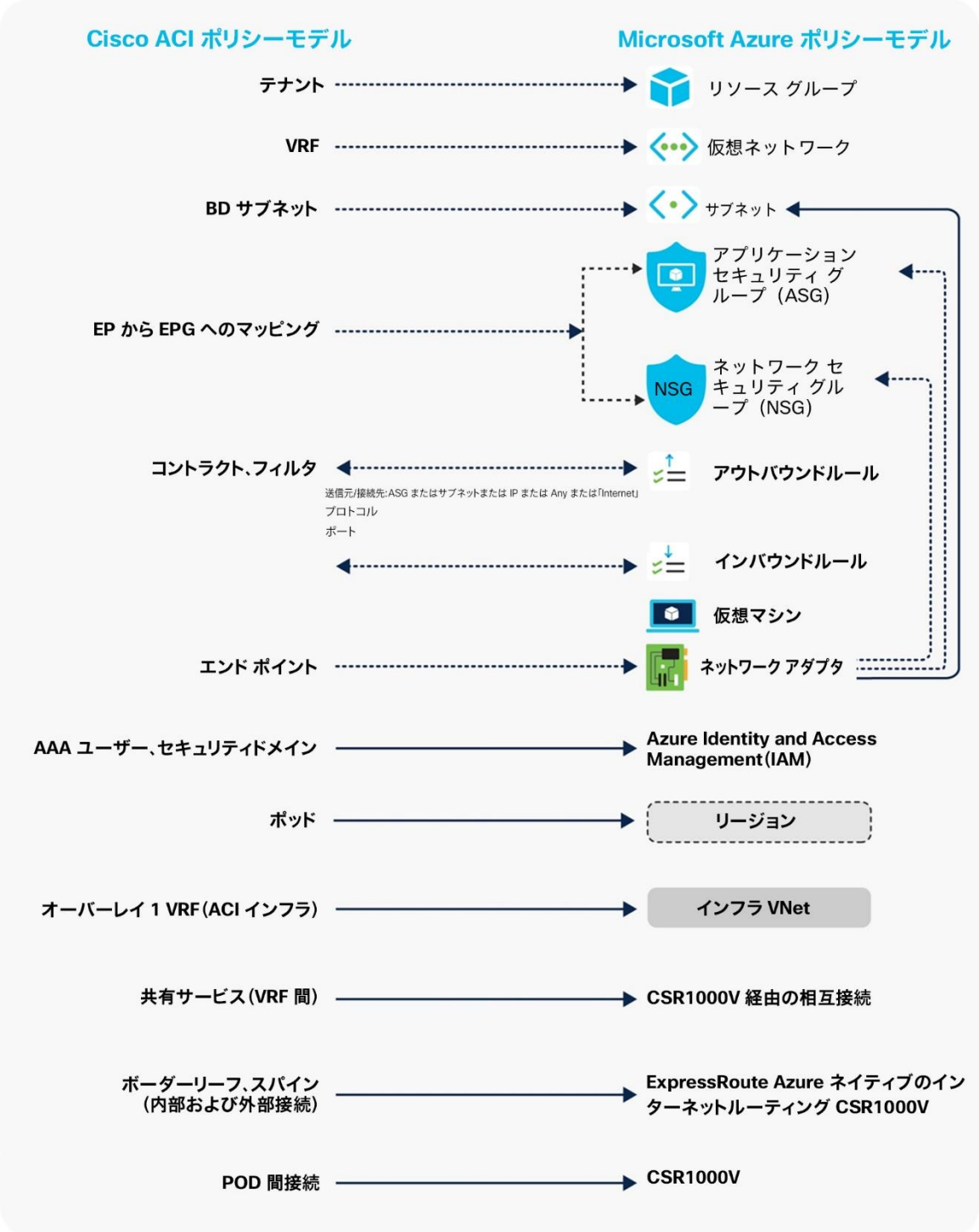

図 7. Cisco ACI ポリシーモデルから Microsoft Azure ポリシーモデルへのマッピング（サブネットごとの NSG）

詳細については、次のホワイトペーパーを参照してください。

- https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-741998.html
- https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-742844.html

マルチリージョン ハイブリッド クラウドプラットフォームの設計

このセクションでは、マルチリージョン ハイブリッド クラウドプラットフォーム トポロジのトラフィックフローについて説明します。

次の図は、このセクションで使用するトポロジの例を示したものです。次のネットワークで構成されています。

- オンプレミスの Cisco ACI ファブリック：
  - ブリッジドメインサブネット（172.16.2.0/24 はブリッジドメインサブネットです）
  - 外部ネットワーク（172.16.0.0/24 は、オンプレミスの L3Out 経由で到達可能な外部の接続先です）
- Cloud ACI サイト：
  - Microsoft Azure：リージョン 1 および 2（10.111.0.0/16、10.112.0.0/16、10.113.0.0/16 および 10.114.0.0/16 は VNet CIDR です）
  - AWS: リージョン 1 およびリージョン 2（10.121.0.0/16、10.122.0.0/16、10.123.0.0/16 および 10.124.0.0/16 は VPC CIDR です）
- ブランチネットワーク：
  - branch-1（192.168.81.0/24 は第 1 ブランチネットワークです）
  - branch-2（192.168.82.0/24 は第 2 ブランチネットワークです）

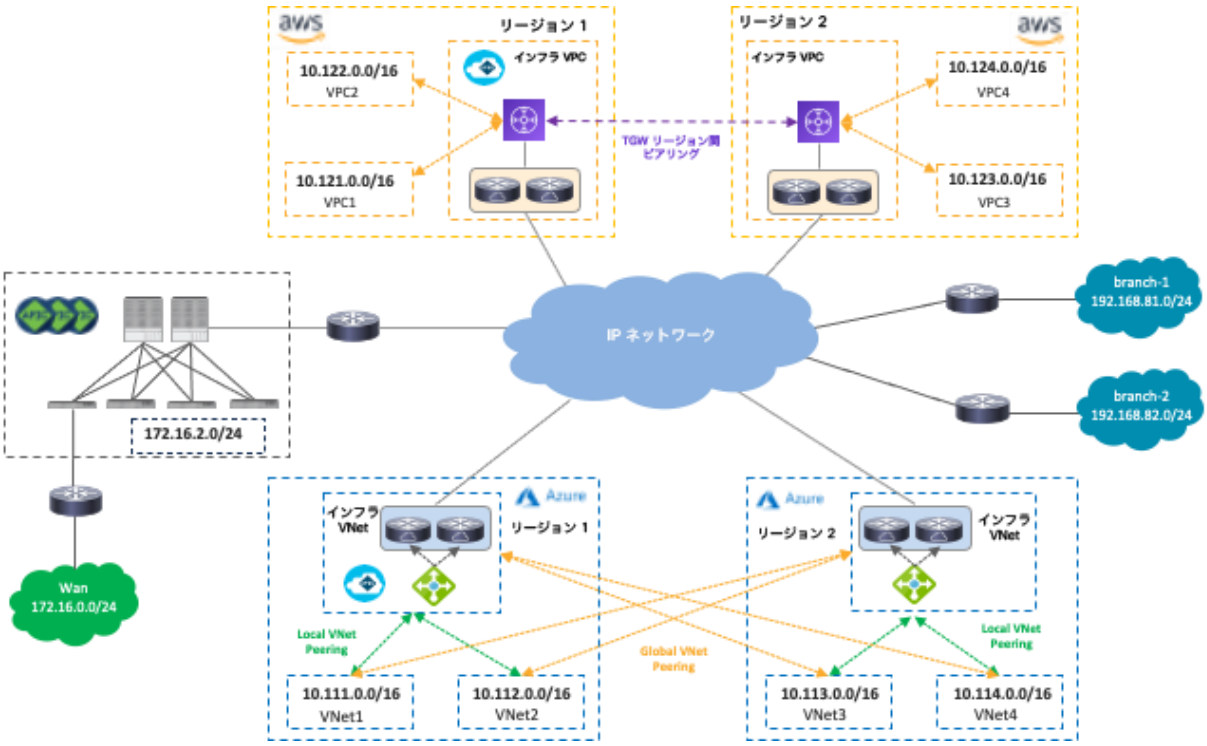

図 8. 複数のリージョンを持つ Cisco Cloud ACI

NDO と Cisco Cloud APIC は、異なるリージョンにあるクラウドプラットフォーム間でさまざまなネットワーク関連構成を調整して、マルチリージョンのハイブリッドクラウド環境でのトラフィックフローを実現します。ネットワーク関連の構成には次のようなものがあります。

- AWS：VPC、CIDR、サブネット、ルートテーブル、TGW、TGW ピアリング、セキュリティグループ、セキュリティグループルール、Application Load Balancer。
- Microsoft Azure：VNet、CIDR、サブネット、ルートテーブル、VNet ピアリング、ネットワーク セキュリティ グループ、アプリケーション セキュリティ グループ、Azure アプリケーション ゲートウェイ、ネットワークロードバランサ。
- Cisco Cloud ルータのライフサイクル管理と構成。

次の図は、NDO および Cisco Cloud APIC によって自動化される内容を示しています。

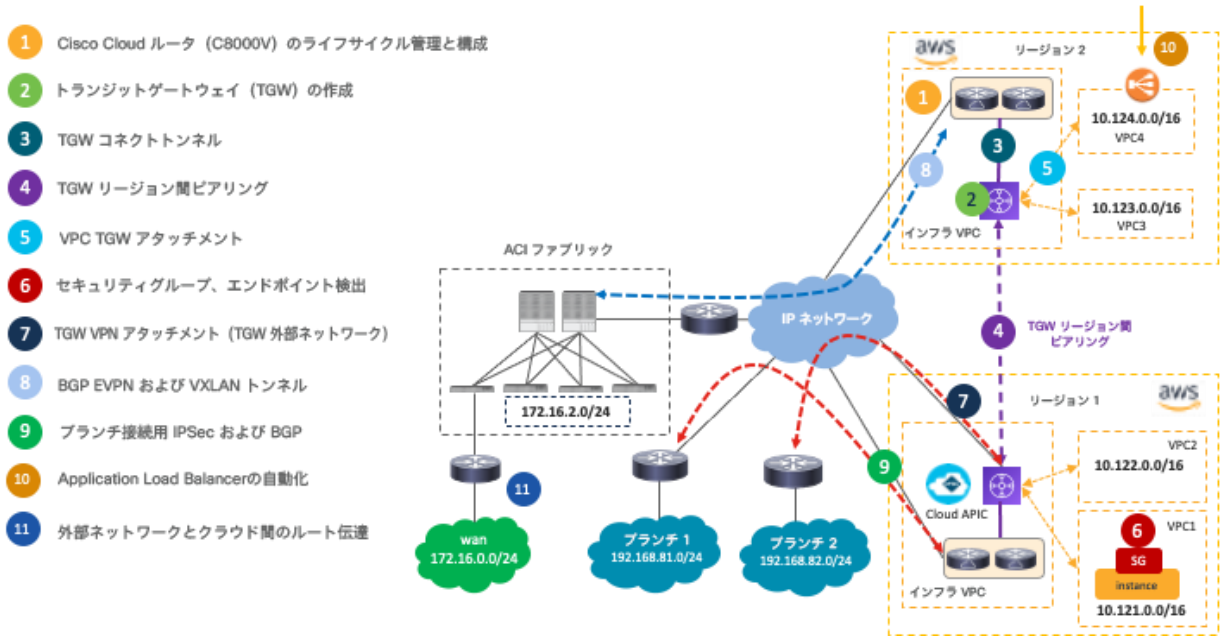

図 9. Cloud ACI によって自動化されるネットワークコンポーネント（AWS）

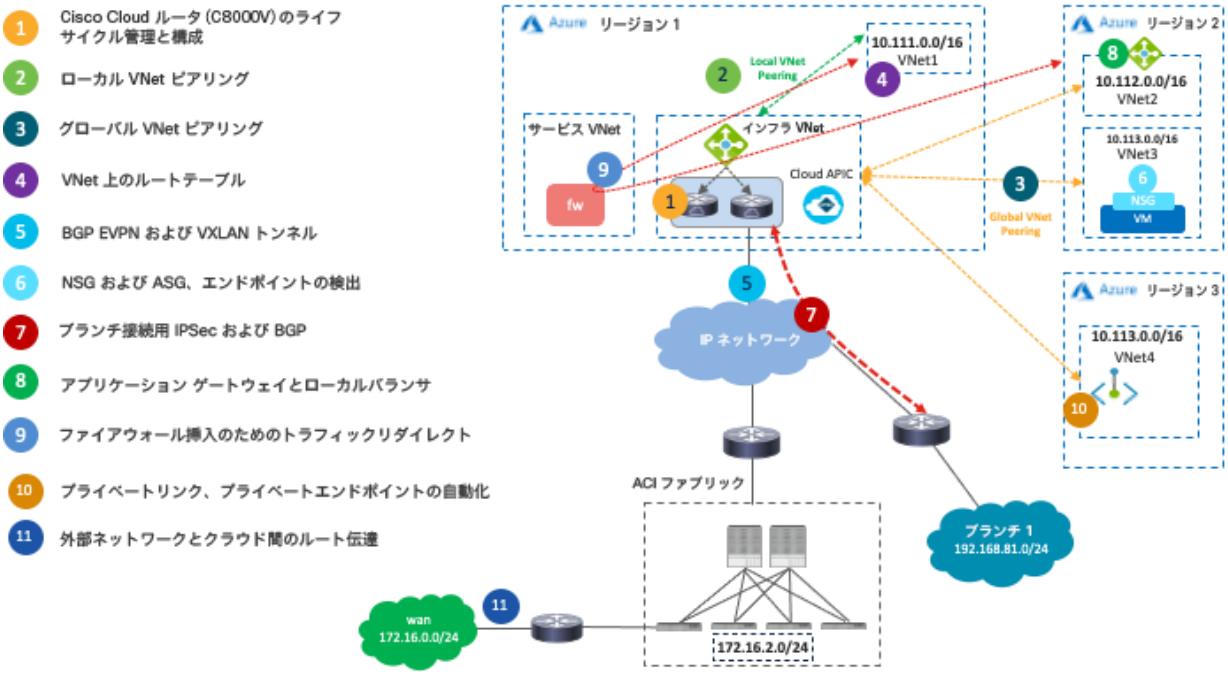

図 10. Cloud ACI によって自動化されるネットワークコンポーネント（Microsoft Azure）

Cisco Cloud ACI を導入する主な利点の 1 つは、ネットワーク接続のオーケストレーションと、複数のクラウド環境での運用の簡素化です。

次の表は、このセクションで説明するトラフィックフローをまとめたものです。次のサブセクションで、各シナリオについて詳しく説明します。

表 1. トラフィックフローパターン

トラフィックパターン	Traffic flow
パブリッククラウドプラットフォーム内のトラフィックフロー（プライベートサブネットからプライベートサブネットへ）	トラフィックは、AWS TGW や Microsoft Azure VNet ピアリングなどクラウドネイティブのルーティング機能を介して転送されます。
パブリッククラウドプラットフォーム間のトラフィックフロー Error! Bookmark not defined.（プライベートサブネットからプライベートサブネットへ）	トラフィックは、クラウドプラットフォーム内の Cisco Cloud ルータ間の VXLAN トンネルを介して転送されます。
オンプレミスの ACI ファブリックとパブリッククラウドプラットフォーム間のトラフィックフロー（プライベートサブネットからプライベートサブネットへ）	トラフィックは、クラウドプラットフォーム内の Cisco Cloud ルータと Cisco ACI スパインスイッチ間の VXLAN トンネルを介して転送されます。
インターネットとクラウドプラットフォーム間のトラフィックフロー Error! Bookmark not defined.（パブリックサブネットからプライベートサブネットへ）	トラフィックは、AWS IGW（インターネットゲートウェイ）や Microsoft Azure のデフォルトシステムルートなどのクラウド ネイティブ ルーティング機能を介して転送されます。
外部ネットワークとクラウドプラットフォーム間のトラフィックフロー（プライベートサブネットからプライベートサブネットへ）	トラフィックは、クラウドプラットフォームの Cisco Cloud ルータとブランチルータの間の IPsec トンネルを介して転送されます。

パブリッククラウドプラットフォーム内のリージョン内およびリージョン間トラフィックフロー

次の図は、同じパブリッククラウド プロバイダーの 2 つのリージョン間で確立されたトラフィックフローを示しています。

AWS を使用した Cloud ACI の場合、同じリージョン内の VPC 間トラフィックは、ローカルのトランジットゲートウェイ（TGW）を介して転送されます。リージョン間トラフィックは、複数のリージョンの TGW 間ピアリングを利用し、クラウドプロバイダーのプライベートバックボーンを介して転送されます。

Cisco Cloud APIC は、TGW の作成、各 VPC の TGW アタッチメント構成、TGW のリージョン間ピアリング、VPC ルートテーブルの作成、各 VPC の VPC ルートテーブル構成を処理します。

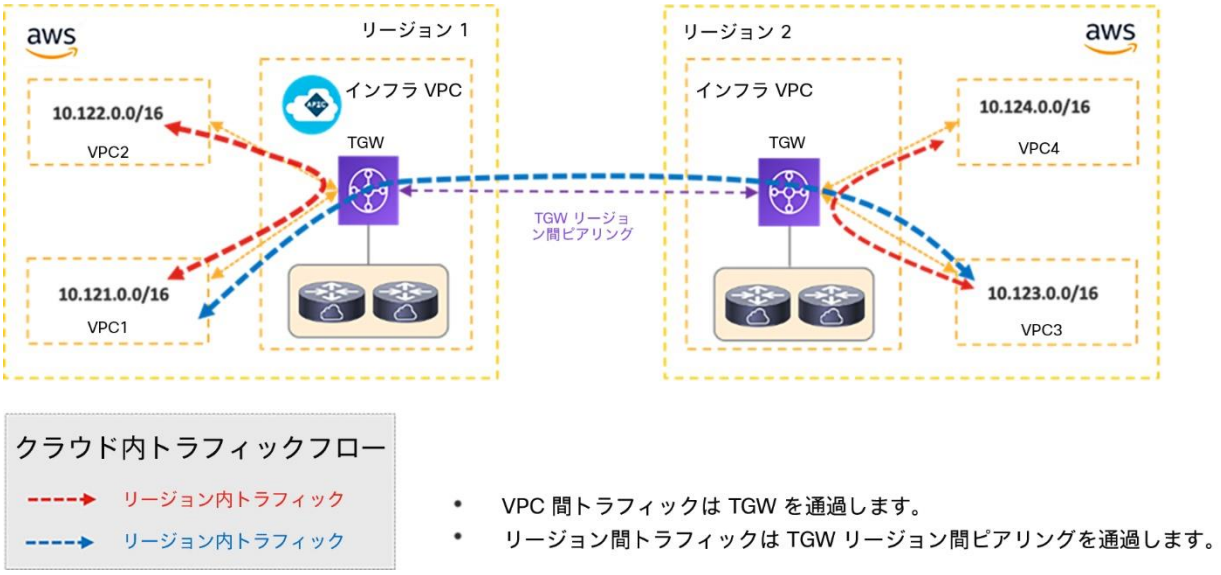

図 11. パブリッククラウドプラットフォーム（AWS）内のトラフィックフロー

Microsoft Azure を使用した Cloud ACI の場合、VNet 間トラフィックは VNet ピアリングを介してインフラ VNet 内の Azure Load Balancer に転送され、トラフィックはインフラ VNet 内の Cisco Cloud ルータの 1 つに負荷分散されます。次に、Cisco Cloud ルータは VNet ピアリングを介してトラフィックを接続先 VNet に転送します。リターントラフィックは、ロードバランシングに基づいて別の Cisco Cloud ルータに送信される可能性があります。

Cisco Cloud APIC は、VNet ピアリング、Azure Load Balancer、Cisco Cloud ルータ、および各 VNet のルートテーブルの構成を処理します。

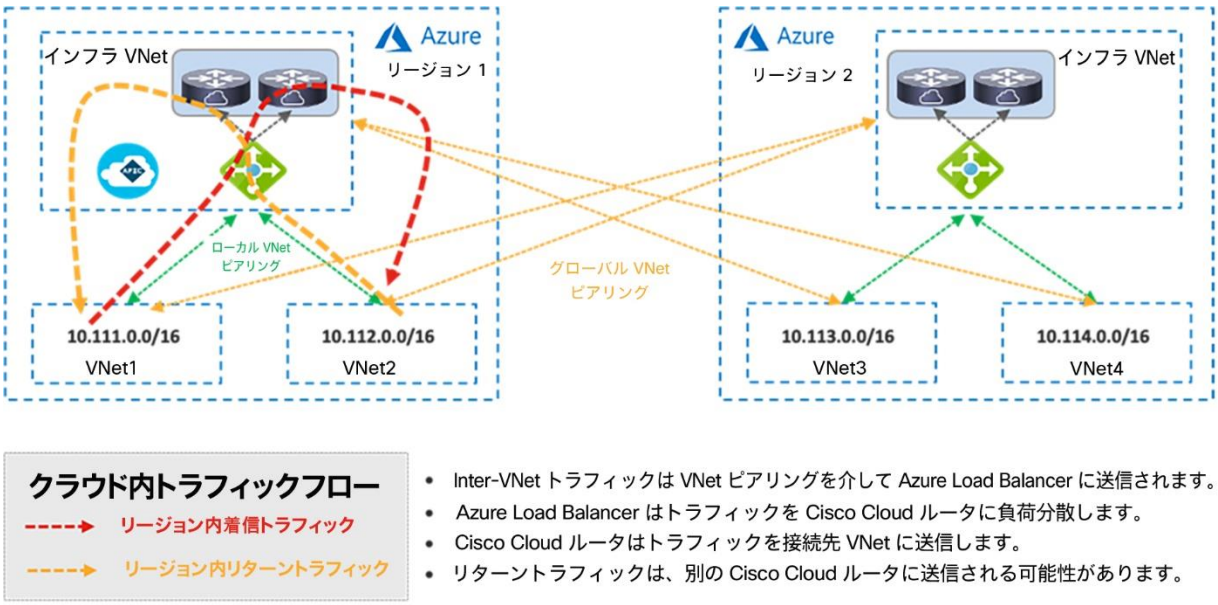

図 12. パブリッククラウドプラットフォーム（Microsoft Azure）内のリージョン内トラフィックフロー

ローカル VNet 外部のプライベートサブネット宛てのトラフィックは、同じリージョン内のローカル Azure Load Balancer に転送されるため、リージョン間トラフィックは、着信トラフィックとリターントラフィックで異なる Azure Load Balancer に転送されます。トラフィックは、Cisco Cloud ルータに負荷分散された後、グローバル VNet ピアリングを介して接続先 VNet に転送されます。

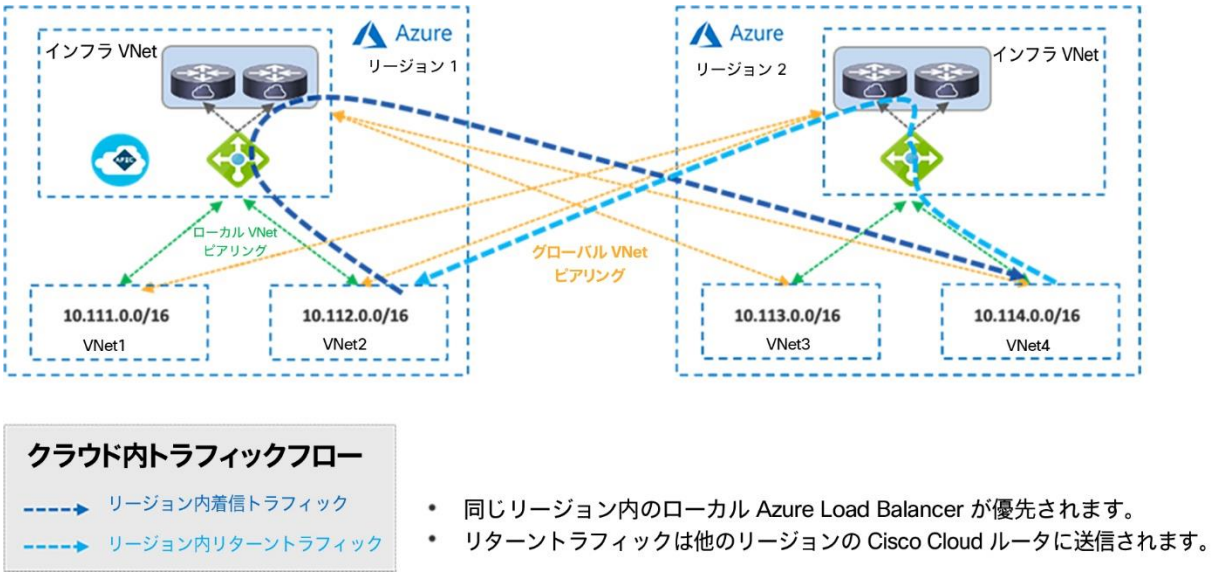

図 13. パブリッククラウドプラットフォーム（Microsoft Azure）内のリージョン間トラフィックフロー

同じリージョンにローカルの Azure Load Balancer がない場合、トラフィックはグローバル VNet ピアリングを介して接続先リージョンの Azure Load Balancer に転送されます。

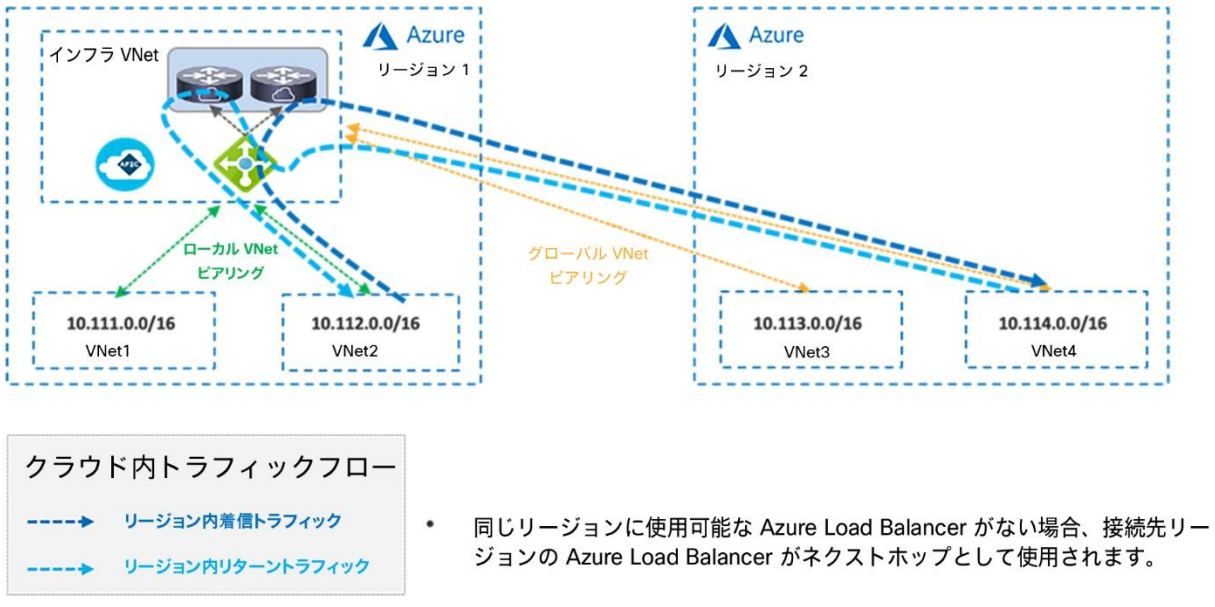

図 14. ローカル Azure Load Balancer がないパブリッククラウドプラットフォーム（Microsoft Azure）内のリージョン間トラフィックフロー

さまざまなリージョンで複数の Azure Load Balancer を使用できる場合、Cisco Cloud APIC は、VNet のルートテーブルを更新することで、ネクストホップとして使用する Azure Load Balancer を決定します。この判断は、

Cisco Cloud ルータの構成や可用性など、複数の要因に基づいています。次の図の例では、双方向に同じ Azure Load Balancer を使用していますが、トラフィックは、着信トラフィックとリターントラフィックで異なる Azure Load Balancer に転送される可能性があります。

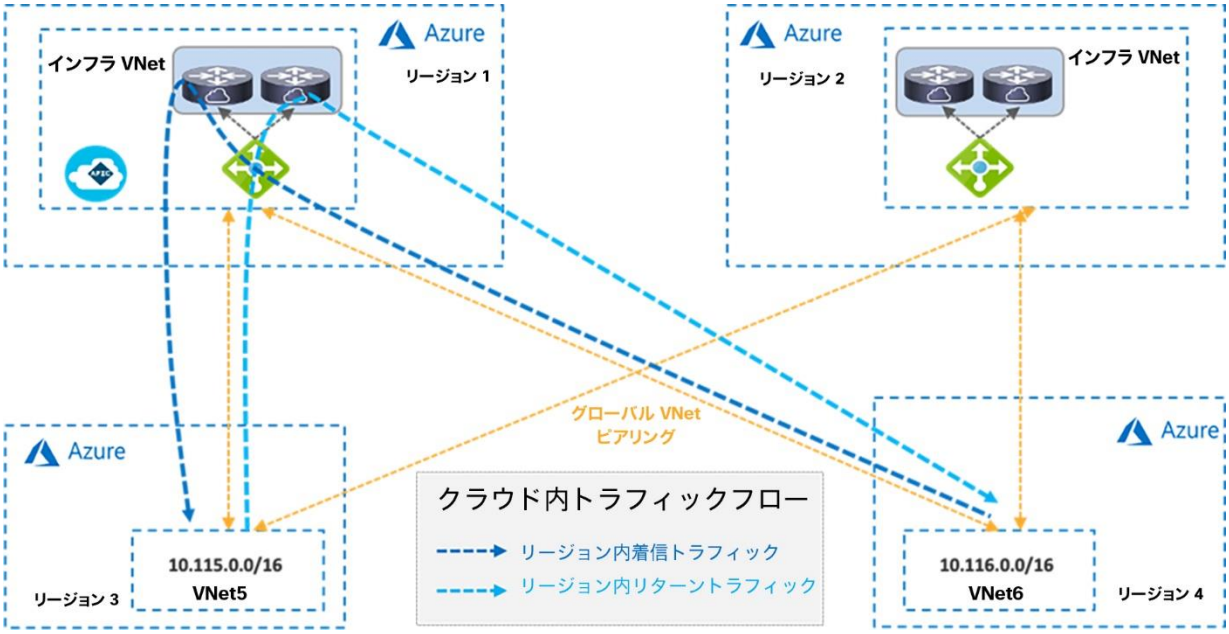

図 15. ローカル Azure Load Balancer を使用しないパブリッククラウド（Microsoft Azure）内のリージョン間トラフィックフロー

テナントの設計とガイドラインについては、次のセクションを参照してください。

- ユースケース #1：複数のサイトにまたがるアプリケーション（テナント内）
- ユースケース #2：複数のサイトにまたがるアプリケーション（テナント間共有サービス）

パブリッククラウドプラットフォーム間のトラフィックフロー

次の図は、異なるパブリッククラウドプラットフォームのプライベートサブネット間のトラフィックフローを示しています。

パブリッククラウド外部のプライベートサブネット宛てのトラフィックは、ローカルの TGW またはローカルの Azure Load Balancer に転送されます。その後、トラフィックは同じクラウド内の Cisco Cloud ルータに転送され、Cisco Cloud ルータのルーティングテーブルに基づいて、VXLAN トンネルの反対側の Cisco Cloud ルータに送信されます。

- 接続先 IP サブネットがオンプレミスの ACI ファブリックにある場合、Cisco Cloud ルータはオンプレミスの ACI のルータにトラフィックを送信します。「オンプレミスの ACI ファブリックとパブリッククラウドプラットフォーム間のトラフィックフロー」を参照してください。
- 接続先 IP サブネットがブランチネットワークなど別の外部ネットワークにある場合、Cisco Cloud ルータはトラフィックを接続先ロケーションのルータに送信します。「外部ネットワークとクラウドプラットフォーム間のトラフィックフロー」を参照してください。

次の図の例では、双方向に同じ Cisco Cloud ルータを使用していますが、トラフィックは、着信トラフィックとリターントラフィックで異なる Cisco Cloud ルータを通過する可能性があります。次の図に示すように、別のクラウドから Microsoft Azure へのトラフィックは、Azure Load Balancer を通過しません。

Cisco Cloud APIC は、ルートテーブル、TGW、VNet ピアリング、Azure Load Balancer などのパブリッククラウド ネットワーク構成に加えて、VXLAN トンネルを含む Cisco Cloud ルータの構成も処理します。

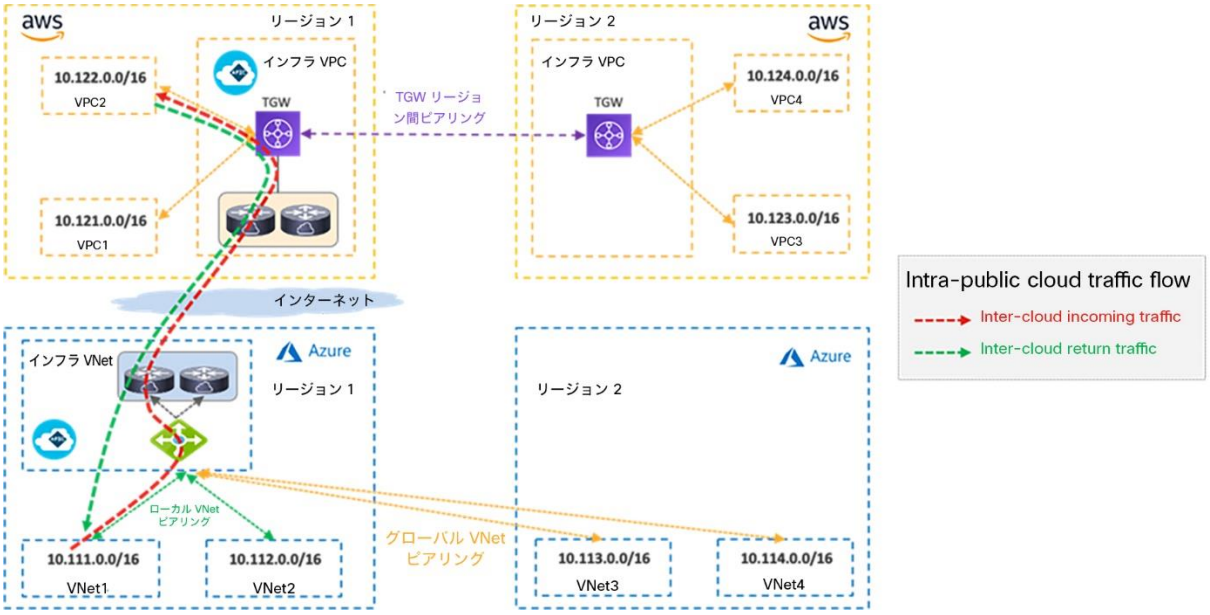

図 16. パブリッククラウドプラットフォーム間のトラフィックフロー

同じリージョンに Cisco Cloud ルータがない場合、トラフィックは Cisco Cloud ルータが存在するリージョンに転送され、Cisco Cloud ルータ間の VXLAN を介して接続先パブリッククラウドに転送されます。

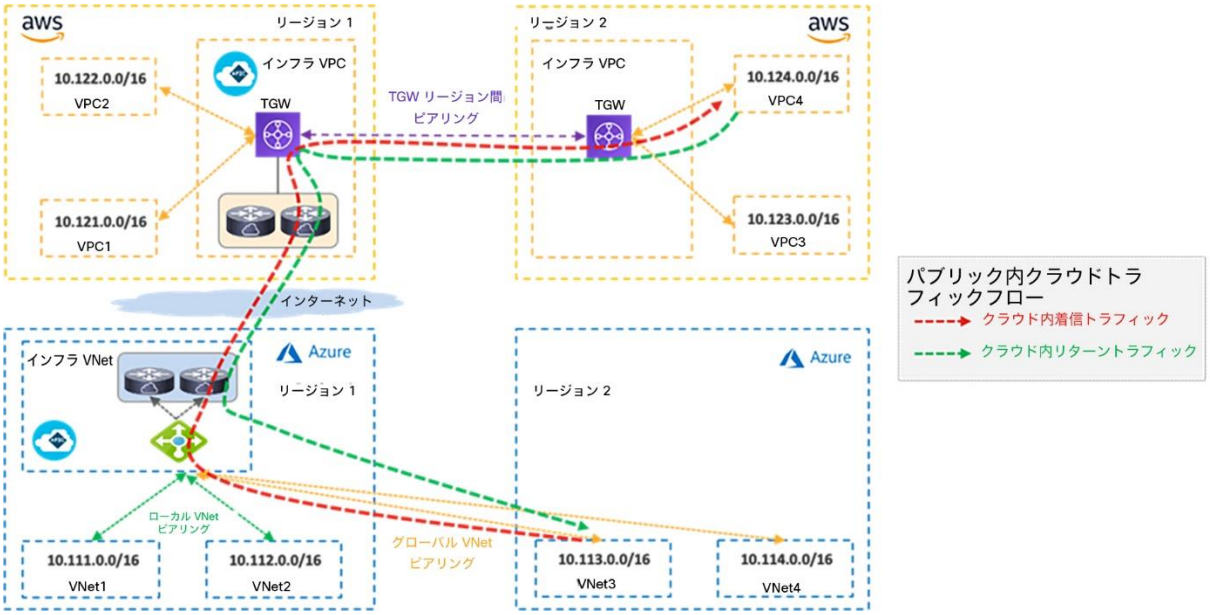

図 17. ローカル Cisco Cloud ルータがないパブリッククラウドプラットフォーム間のトラフィックフロー

テナントの設計とガイドラインについては、次のセクションを参照してください。

- ユースケース #1：複数のサイトにまたがるアプリケーション（テナント内）
- ユースケース #2：複数のサイトにまたがるアプリケーション（テナント間共有サービス）

オンプレミスの ACI ファブリックとパブリッククラウドプラットフォーム間のトラフィックフロー

次の図は、オンプレミスの ACI ファブリックとパブリッククラウドプラットフォーム間のトラフィックフローを示しています。

送信元 VPC または VNet 外部のプライベートサブネット宛てのトラフィックは、ローカルの TGW またはローカルの Azure Load Balancer に転送されます。その後、トラフィックは同じクラウド内の Cisco Cloud ルータに転送され、Cisco Cloud ルータのルーティングテーブルに基づいて、VXLAN トンネルの向こうのオンプレミスの ACI ファブリックのルータに送信されます。

- 接続先 IP サブネットが別のパブリッククラウドにある場合、Cisco Cloud ルータはトラフィックを接続先パブリッククラウドの Cisco Cloud ルータに送信します。「パブリッククラウドプラットフォーム間のトラフィックフロー」を参照してください。

- 接続先 IP サブネットがブランチネットワークなど別の外部ネットワークにある場合、Cisco Cloud ルータはトラフィックを接続先ロケーションのルータに送信します。「外部ネットワークとクラウドプラットフォーム間のトラフィックフロー」を参照してください。

トラフィックがオンプレミスの ACI ファブリックに着信すると、接続先 IP サブネットに応じて、オンプレミスの ACI ファブリックまたは外部ネットワークの接続先エンドポイントに L3Out 経由で転送されます。NDO とオンプレミス APIC は、オンプレミス ACI ファブリックでのネットワーク展開を処理します。

次の図の例では、双方向に同じ Cisco Cloud ルータを使用していますが、トラフィックは、着信トラフィックとリターントラフィックで異なる Cisco Cloud ルータを通過する可能性があります。次の図に示すように、オンプレミスの ACI ファブリックから Microsoft Azure へのトラフィックは、Azure Load Balancer を経由しません。

Cisco Cloud APIC は、ルートテーブル、TGW、VNet ピアリング、Azure Load Balancer などのパブリッククラウド ネットワーク構成に加えて、VXLAN トンネルを含む Cisco Cloud ルータの構成も処理します。NDO は、オンプレミスの ACI ファブリックのルータの構成テンプレートを生成します。構成テンプレートは Cisco IOS-XE CLI シンタックスに基づいているため、クラウド管理者がルータに合わせて編集する必要がある場合があります。

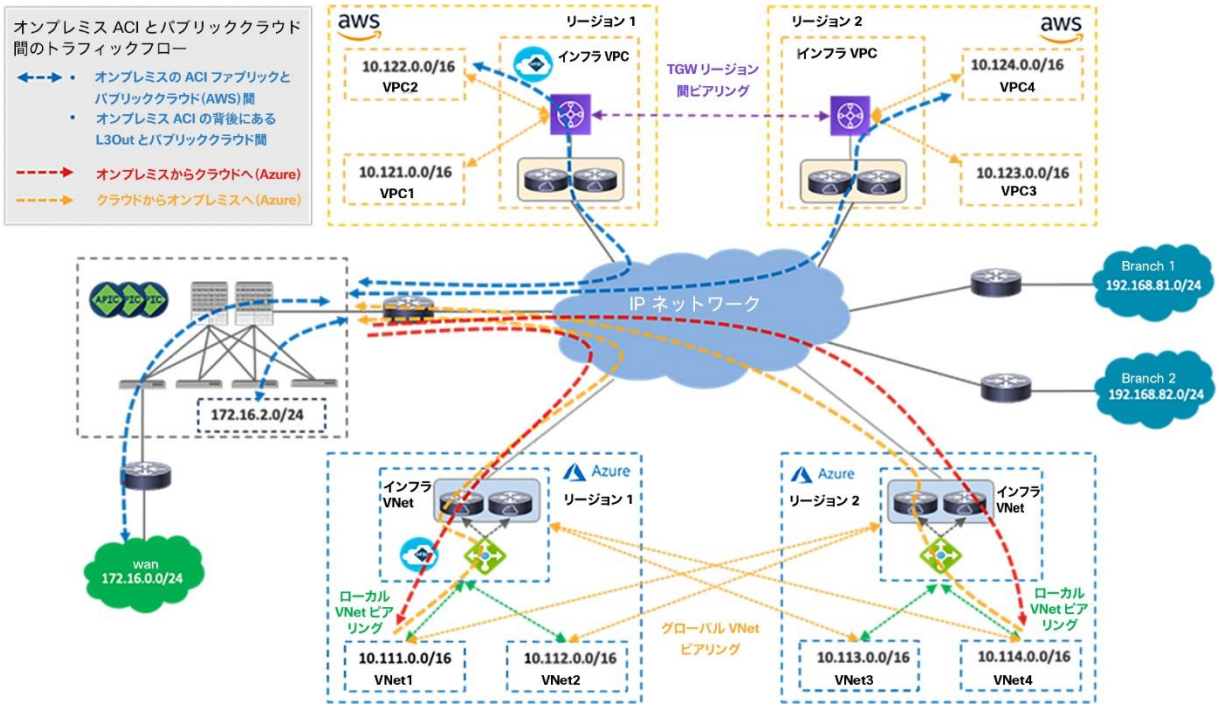

図 18. オンプレミスの ACI ファブリックとパブリッククラウドプラットフォーム間のトラフィックフロー

同じリージョンに Cisco Cloud ルータがない場合、トラフィックは Cisco Cloud ルータが存在するリージョンに転送され、オンプレミスの ACI ファブリックの Cisco Cloud ルータとスパインスイッチ間の VXLAN を介して接続先に転送されます。次の図では、リージョン 3 のエンドポイントとオンプレミスの ACI ファブリック間のトラフィックは、両方向にリージョン 2 の Cisco Cloud ルータを使用していますが、トラフィックは着信トラフィックとリターントラフィックで異なるリージョンの異なる Cisco Cloud ルータを通過する可能性があります。

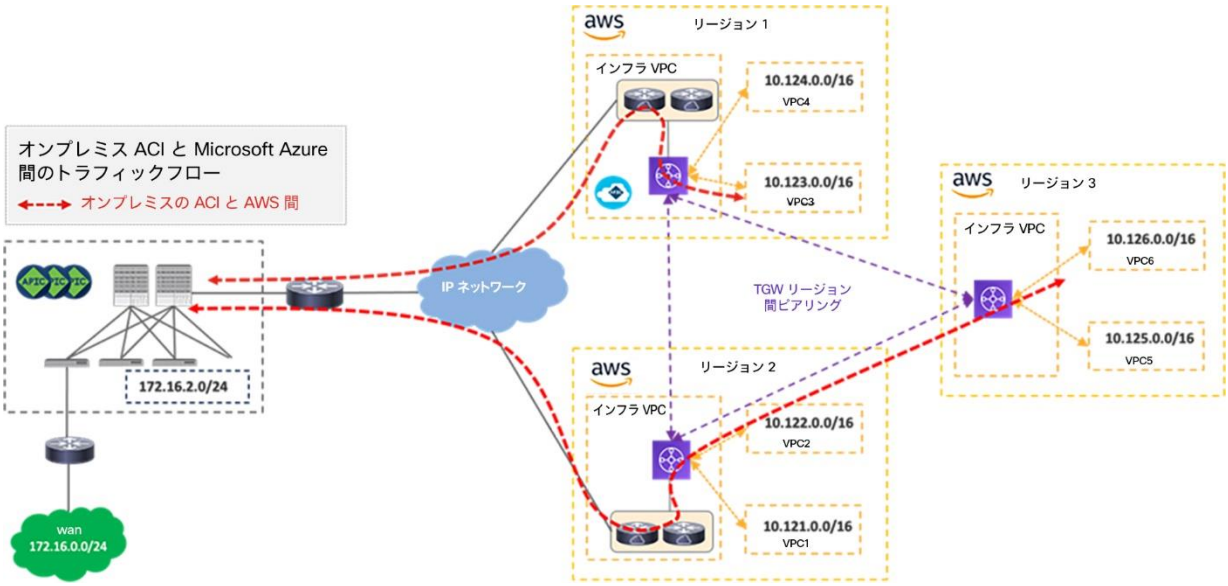

図 19. オンプレミスの ACI ファブリックとローカル Cisco Cloud ルータを使用しないパブリッククラウドプラットフォーム（AWS）間のトラフィックフロー

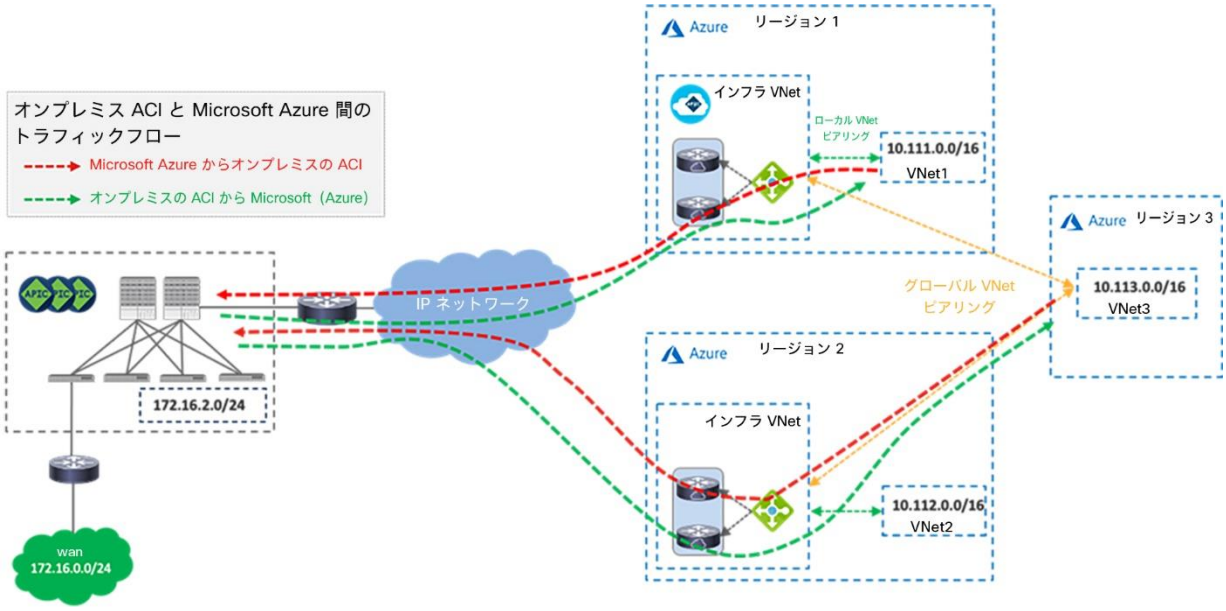

図 20. オンプレミスの ACI ファブリックとローカル Cisco Cloud ルータを使用しないパブリッククラウドプラットフォーム（Microsoft Azure）間のトラフィックフロー

テナントの設計とガイドラインについては、次のセクションを参照してください。

- ユースケース #1：複数のサイトにまたがるアプリケーション（テナント内）
- ユースケース #2：ハイブリッドマルチクラウド環境での共有サービス
- ユースケース #3：オンプレミスの L3 外部（L3Outs）を介したクラウドから外部ネットワークへの接続

インターネットとクラウドプラットフォーム間のトラフィックフロー

次の図は、インターネットとクラウドプラットフォーム間のトラフィックフローを示しています。

緑の矢印で示されているように、インターネット宛のトラフィックは、AWS Internet Gateway（IGW）や Microsoft Azure のデフォルトシステムルートなどのクラウド ネイティブ ルーティング機能を介して転送されますが、TGW、VNet ピアリング、Cisco Cloud ルータは経由しません。 Cisco Cloud APIC は、次のホップとしてインターネットゲートウェイを指定するデフォルトルートを、AWS ルートテーブルに追加します。

もう 1 つの例は、オンプレミスの ACI ファブリックでの L3Out の使用です。この場合、オンプレミスの ACI ファブリックとパブリッククラウドプラットフォーム間のトラフィックフローのシナリオと同様に、インターネット宛のトラフィックはオンプレミスの ACI ファブリックに転送され、L3Out を介して外部ネットワークに転送されます。 NDO、Cisco Cloud APIC、およびオンプレミス APIC は、オンプレミスの ACI ファブリックおよびパブリッククラウドプラットフォーム全体のネットワーク展開を処理します。

次の図の例では、双方向に同じ Cisco Cloud ルータを使用していますが、トラフィックは着信トラフィックとリターントラフィックで異なる Cisco Cloud ルータを通過する可能性があります。オンプレミスの ACI ファブリックから Microsoft Azure へのトラフィックは、Azure Load Balancer を経由しません。

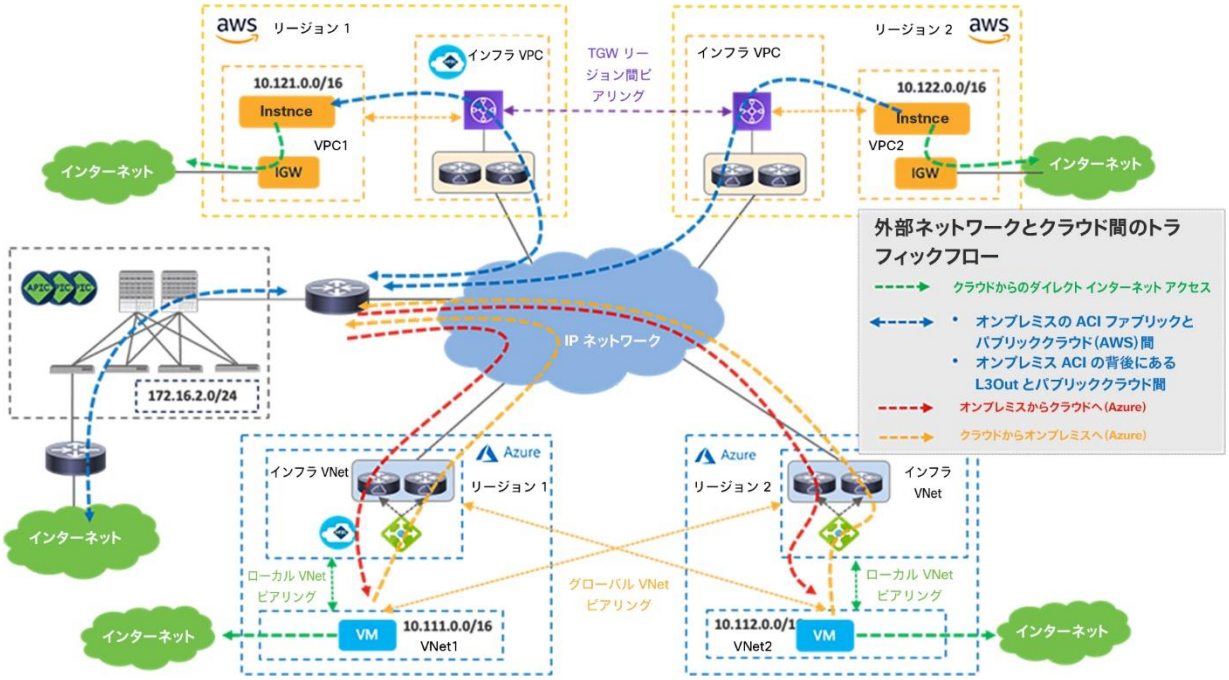

図 21. インターネットとクラウドプラットフォーム間のトラフィックフロー

テナントの設計とガイドラインについては、次のセクションを参照してください。

- ユースケース #3-1：クラウド ネイティブ ルーティング機能を使用したクラウドからインターネットへの接続
- ユースケース #3-2：オンプレミスの L3 外部（L3Outs）を介したクラウドから外部ネットワークへの接続

外部ネットワークとクラウドプラットフォーム間のトラフィックフロー

次の図は、外部ネットワークとクラウドプラットフォーム間のトラフィックフローを示しています。この例では、ブランチネットワークが外部ネットワークの代表として使用されています。

この場合、オンプレミスの ACI ファブリックとパブリッククラウドプラットフォーム間のトラフィックフローのシナリオと同様に、送信元 VPC/VNet の外部にあるプライベートサブネット宛のトラフィックは、ローカルの TGW またはローカルの Azure Load Balancer に転送されます。その後、トラフィックは同じクラウド内の Cisco Cloud ルータに転送され、Cisco Cloud ルータのルーティングテーブルに基づいて、IPsec トンネルの向こうの接続先ロケーション（この例ではブランチネットワーク）のルータに送信されます。

- 接続先 IP サブネットが別のパブリッククラウドにある場合、Cisco Cloud ルータはトラフィックを他のパブリッククラウドの Cisco Cloud ルータに送信します。「パブリッククラウドプラットフォーム間のトラフィックフロー」を参照してください。
- 接続先 IP サブネットがオンプレミスの ACI ファブリックにある場合、Cisco Cloud ルータはオンプレミスの ACI のルータにトラフィックを送信します。「オンプレミスの ACI ファブリックとパブリッククラウドプラットフォーム間のトラフィックフロー」を参照してください。

次の図の例では、双方向に同じ Cisco Cloud ルータを使用していますが、トラフィックは、着信トラフィックとリターントラフィックで異なる Cisco Cloud ルータを通過する可能性があります。Microsoft Azure の場合、次の図に示すように、外部ネットワークから Microsoft Azure へのトラフィックは Azure Load Balancer を通過しません。

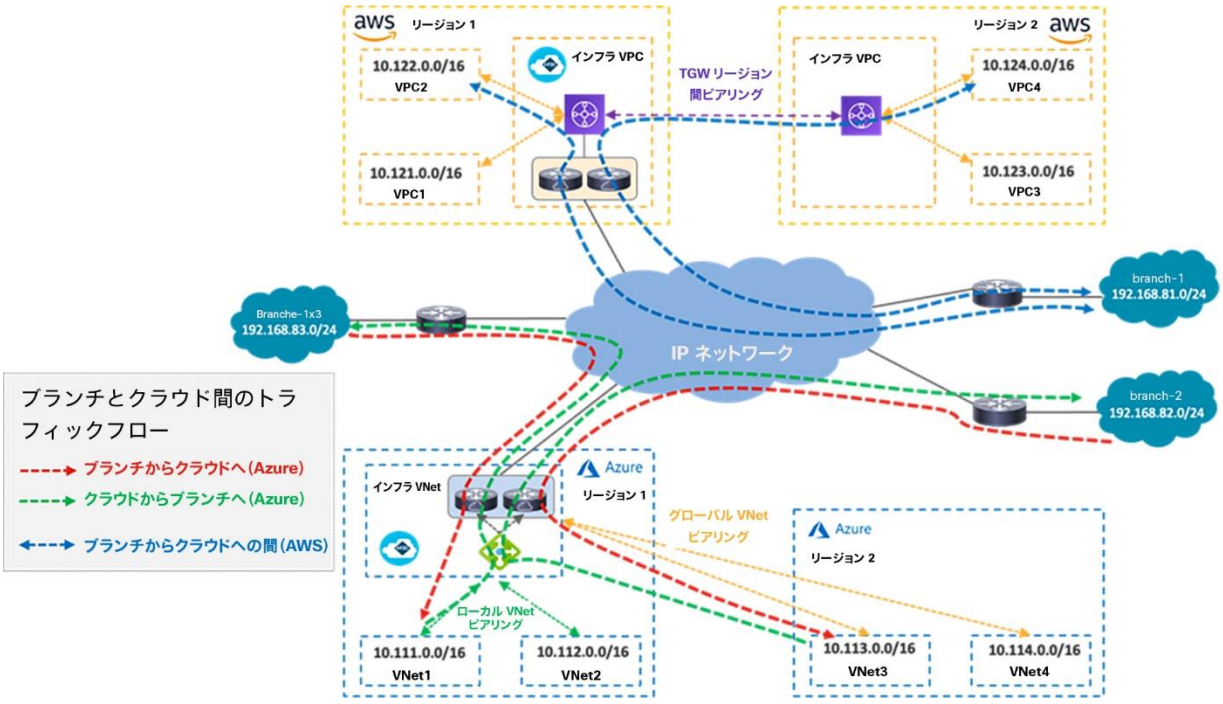

図 22. 外部ネットワークとクラウドプラットフォーム間のトラフィックフロー

テナントの設計とガイドラインについては、次のセクションを参照してください。

- ユースケース #4：クラウド ネイティブ ルーティング サービスを使用した外部サイトへの接続
- ユースケース #5：WAN、ブランチ、または非 ACI サイトへの外部接続
- ユースケース #6：SD-WAN ソリューションとの相互運用

サイト間接続

このサブセクションでは、オンプレミス ACI サイトとクラウドサイト間のサイト間接続について説明します。

オンプレミスの ACI サイトとクラウドサイトは、Cisco Cloud ルータとオンプレミスルータ間のアンダーレイネットワークの到達可能性のためのダイナミック ルーティング プロトコルとして OSPF を使用し、IPsec トンネルを介して接続されます。IPsec トンネルと OSPF はオプションです。

- NDO でのサイト接続の一部として IPsec が有効になっていない場合、NDO は OSPF を構成する代わりに、Cisco Cloud ルータで静的ルートを構成します。
- IPsec が有効になっている場合、NDO はインフラ VPC/VNet の Cisco Cloud ルータで IPsec と OSPF を構成します。

NDO は、オンプレミスルータの構成テンプレートも生成します。構成テンプレートは Cisco IOS-XE CLI シンタックスに基づいているため、クラウド管理者がルータに合わせて編集する必要がある場合があります。

アンダーレイ IP ネットワークは、インターネットを介して、AWS の場合は AWS Direct Connect で構成されるプライベートパスを介して、Microsoft Azure の場合は Azure ExpressRoute（ER）を介して通過できます。このアンダーレイネットワークは、2 つのサイト間のオーバーレイ コントロールプレーンとデータプレーンの IP 到達可能性を提供します。AWS Direct Connect または Azure ExpressRoute の場合、プライベート接続であるため、IPsec は必要ない場合があります。

次の図は、AWS Direct Connect および Azure ExpressRoute を使用した例を示しています。オンプレミスの Cisco ACI スパインスイッチは、サイト間ネットワークに接続します。オンプレミスルータは、AWS Direct Connect Gateway（DX GW）および Microsoft Enterprise Edge（MSEE）ルータとの eBGP ピアリングを確立します。オンプレミスルータとクラウドプラットフォームの Cisco Cloud ルータの間に、IPsec トンネルと OSPF ネイバーシップが確立されます。MP-BGP EVPN セッションが、オンプレミスの ACI ファブリック内の ACI スパインスイッチと、Cisco Cloud ルータの間で、IPsec トンネルを介して確立されます。

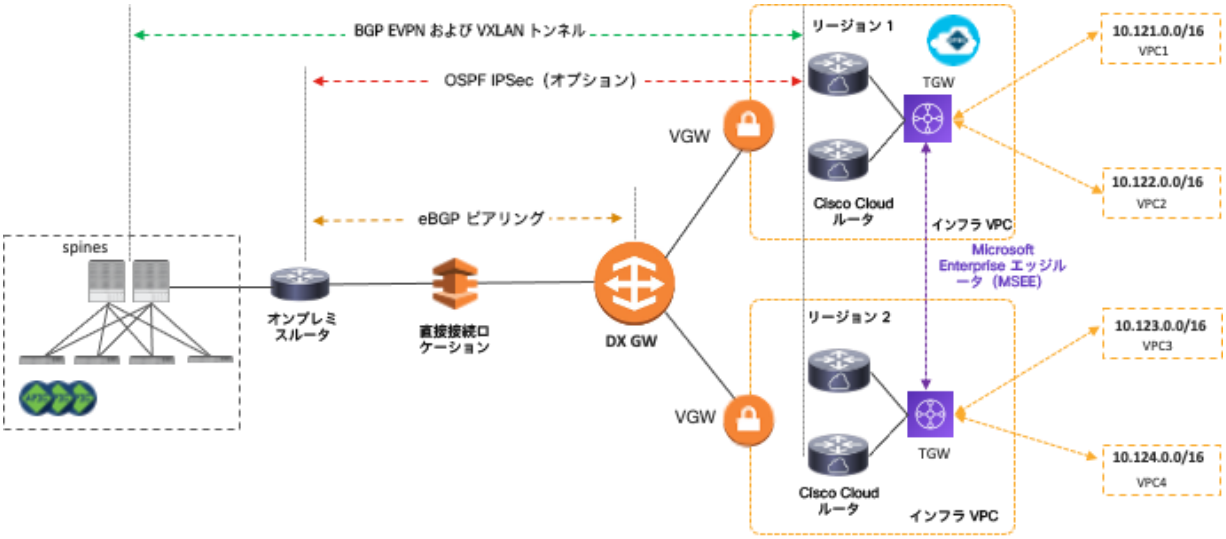

図 23. Direct Connect Gateway（DX GW）を使用したオンプレミスルータと AWS 間の接続

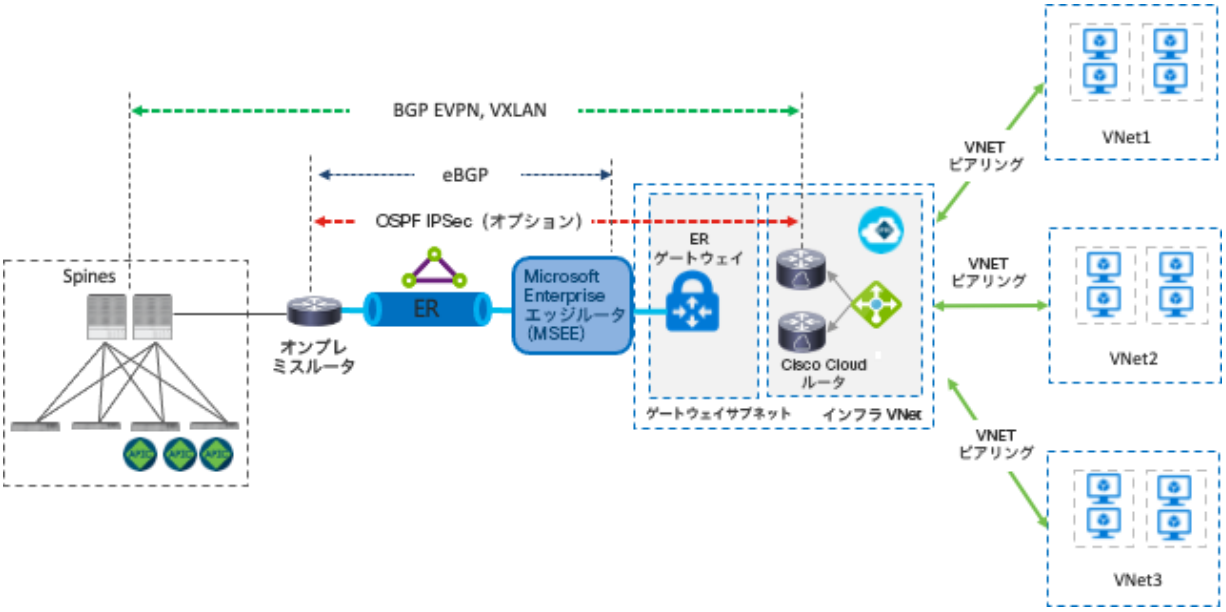

図 24. オンプレミスルータと Azure ExpressRoute ゲートウェイ（ER ゲートウェイ）間の接続

オンプレミスの ACI サイトとクラウドサイト間のオーバーレイネットワークは、コントロールプレーンとして BGP EVPN を実行し、データプレーンとして VXLAN カプセル化とトンネリングを使用します。VXLAN は、オンプレミスの Cisco ACI ファブリックとクラウドプラットフォーム全体に VRF をストレッチするときに、適切なルーティングドメインを識別するために使用されます。テナントホストルートとプレフィックスルートは、2 つのサ

イト間で BGP EVPN ルートタイプ 2（ホスト）およびタイプ 5（プレフィックス）として交換されます。このオーバーレイネットワーク接続のプロビジョニングは、NDO によって自動化されます。

IPsec トンネルと VXLAN カプセル化のオーバーヘッドによるフラグメンテーションを回避するために、BGP EVPN コントロールプレーンの ACI コントロールプレーン MTU ポリシーとデータプレーンのエンドポイントで、最大伝送ユニット（MTU）サイズを調整する必要がある場合があります。調整を行わないと、ネットワーク内のデバイスによるフラグメンテーションが全体のパフォーマンスを低下させる可能性があります。たとえば、関連するエンドポイントの MTU が 1,300 バイトに調整されている場合、これは、MTU の一般的な値が 1,500 バイトであるインターネットを通過するために、VXLAN からの追加の 50 バイトと、 IPsec オーバーヘッドの約 100 バイトを考慮しています。エンドポイントの MTU サイズの調整が許可されていないか、望ましくない場合は、Cisco Cloud APIC から、Cisco Cloud ルータの TCP 最大セグメントサイズ（MSS）を調整します。

Cisco Cloud APIC から Cisco Cloud ルータの TCP MSS 値を変更する構成手順については、https://www.cisco.com/c/en/us/td/docs/dcn/aci/cloud-apic/25x/installation/azure/cisco-cloud-apic-for-azure-installation-guide-250x/configuring-using-setup-wizard-250x.html を参照してください。

Cloud ACI 設計オプション

概説

このセクションでは、一般的な Cloud ACI 設計のユースケースと設計上の考慮事項について説明します。

表 2 は、このセクションで説明する設計オプションの比較をまとめたものです。次のサブセクションでは、各設計オプションとその考慮事項について説明します。

表 2. 一般的な Cloud ACI 設計オプション

使用例	検討
複数のサイトにまたがるアプリケーション（テナント内）	アプリケーションは、エンドポイントのグループとして導入できます。サブネットは、クラウドサイトとオンプレミスサイトで異なる必要があります。
ハイブリッドマルチクラウド環境での共有サービス	テナントはサイト（オンプレミスとクラウド）にまたがる必要があります。 VRF 間でサブネットをオーバーラップさせないでください。
オンプレミスの L3 外部（L3Outs）を介したクラウドから外部ネットワークへの接続 （共有オンプレミス L3 外部（L3Outs））	L3Out は、オンプレミス ACI の専用テンプレートで定義する必要があります。 オンプレミスの L3Out は、共通のテナントに配置することはできません。
クラウド ネイティブ ルーティング サービスを使用した外部サイトへの接続	Azure は Azure VPN ゲートウェイまたは Express Route ゲートウェイを使用します。 AWS は Transit Gateway を使用します。 外部サイトでブランチデバイスを手動で構成するのは、エンドユーザーの責任です。
WAN、ブランチ、または非 ACI サイトへの外部接続	外部デバイスで BGP と IPsec を有効にする必要があります。外部デバイスの BGP ASN は、クラウドプラットフォームの Cisco Cloud ルータの BGP ASN とは異なる必要があります。
SD-WAN ソリューションとの相互運用	SD-WAN 側での自動化構成はありません。SD-WAN 管理者は、 Cloud ACI に合わせてルーティングとポリシーを適宜手動で構成する必要があります。
ロードバランサの挿入	Cisco Cloud APIC リリース 25.0(3) の時点で、サードパーティのロードバランサ統合は Azure でのみ使用できます。
ファイアウォールの挿入	Cisco Cloud APIC リリース 25.0(3) の時点で、サードパーティのファイアウォールの挿入は Azure でのみ使用できます。
マルチノードサービスの挿入	Cisco Cloud APIC リリース 25.0(3) の時点で、マルチノードサービスの挿入は Azure でのみ使用できます。
Azure でのクラウドネイティブサービスの統合	Cisco Cloud APIC リリース 25.0(3) の時点で、クラウドネイティブサービスの統合は Azure でのみ使用できます。
Microsoft Azure および AWS でのブラウンフィールドインポート	Cisco Cloud APIC は、VPC/VNet などのネットワークオブジェクトのみをインポートします。クラウド管理者は、SG/NSG やルートテーブルの作成や更新な

	ど、特定の手動構成手順を実行する必要があります。

重要な注意事項：NDO 駆動のサイト間通信の場合、Cloud APIC リリース 25.0(3) の時点で、ルーティングとセキュリティポリシーは両方ともコントラクト主導であり、Cloud APIC リリース 25.0(2) の時点でサイト内のルーティングとセキュリティポリシーを分離する「コントラクトベースのルーティング」オプションが使用可能であっても、分離することはできません。したがって、サイト間通信の要件がある場合は、サイト間通信のルーティングとセキュリティポリシーを分離する機能が導入されるまで、「コントラクトベースのルーティング」オプションを有効にする必要があります。（「コントラクトベースのルーティング」はデフォルトでは有効になっていません。）

このドキュメントは、AWS と Microsoft Azure の両方の Cisco Cloud APIC で「コントラクトベースのルーティング」が有効になっているという前提に基づいて作成されています。「コントラクトベースのルーティング」オプションは、次の手順で見つけることができます。

1. ［インテント（Intent）］ボタンをクリックします。
2. ［Cloud APIC 設定（Cloud APIC Setup）］をクリックします。
3. ［コントラクトベースのルーティング（Contract Based Routing）］をオンにします。

図 25. ステップ 1：［インテント（Intent）］ボタンをクリックする

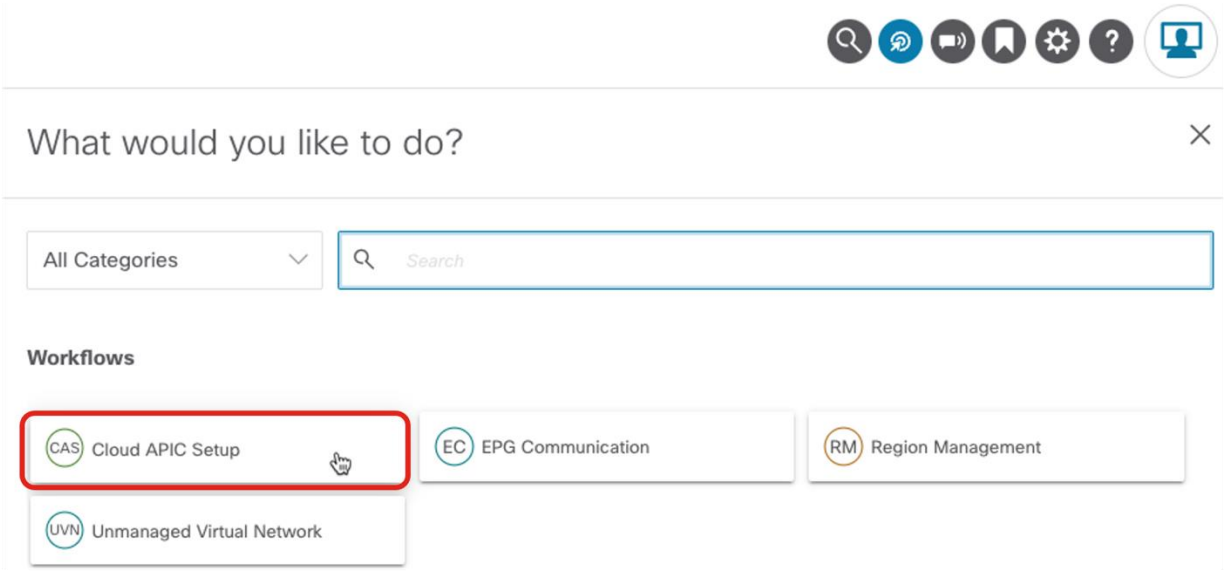

図 26. ステップ 2：[Cloud APIC 設定（Cloud APIC Setup）] をクリックする

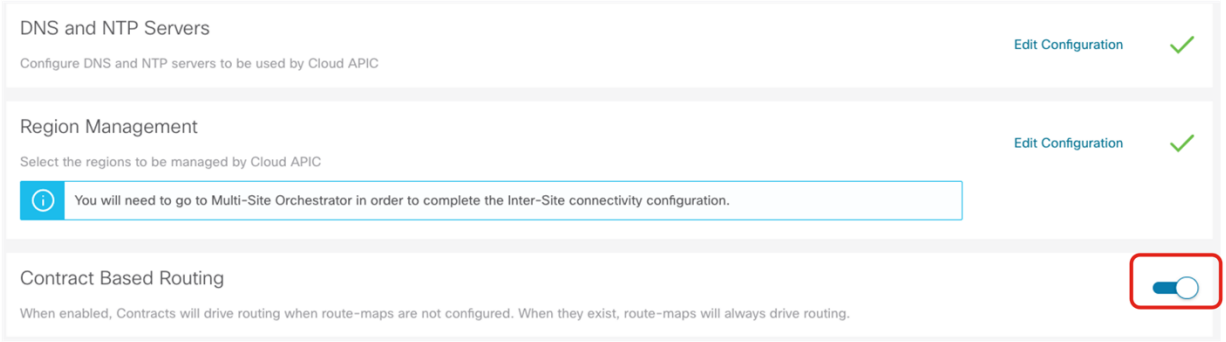

図 27. ステップ 3：[コントラクトベースのルーティング（Contract Based Routing）] を有効にする

ユースケース #1：複数のサイトにまたがるアプリケーション（テナント内）

このユースケースは、アプリケーションがオンプレミスのファブリックとパブリッククラウドプラットフォームにまたがる、最も一般的なユースケースの 1 つです。このユースケースの主な利点は、ワークロードの柔軟性と一元化されたポリシー制御です。Web 層などのアプリケーション層を、オンプレミスのファブリックとパブリッククラウドプラットフォーム全体に展開して、より優れたレジリエンスを提供できます。一方、Web 層とデータベース層など他の層との間のセキュリティポリシーは、ワークロードの場所に関係なく一貫して維持されます。

次の図は、このユースケースの例を示しています。この例では、サンプルアプリケーション「Ecom」はデータベース層と Web 層で構成されています。

- データベース層は、オンプレミスの ACI ファブリックでプロビジョニングされた EPG「Database」によって表されています。
- Web 層は、AWS と Microsoft Azure の両方に存在する EPG 「Web」によって表されています。

このユースケースでは、VRF が 3 つの環境（オンプレミスの ACI、AWS、および Microsoft Azure）にまたがって、それらの間のレイヤー 3 接続を有効にしています。次の例では、VRF は AWS の VPC と Microsoft Azure の VNet にマッピングされていますが、技術的には ACI の 1 つの VRF を複数の VPC/VNet にマッピングできます。たとえば、次の図に示すように、VPC が異なるリージョンにある場合、ACI で 1 つの VRF を作成し、その VRF を AWS の 2 つの VPC にマッピングできます。

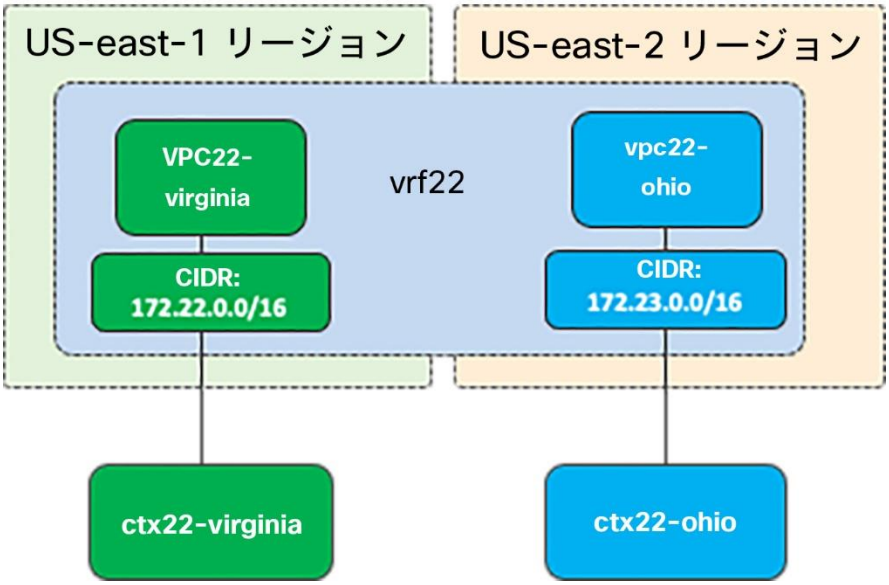

図 28. 1 つの VRF を複数の VPC にマッピングする

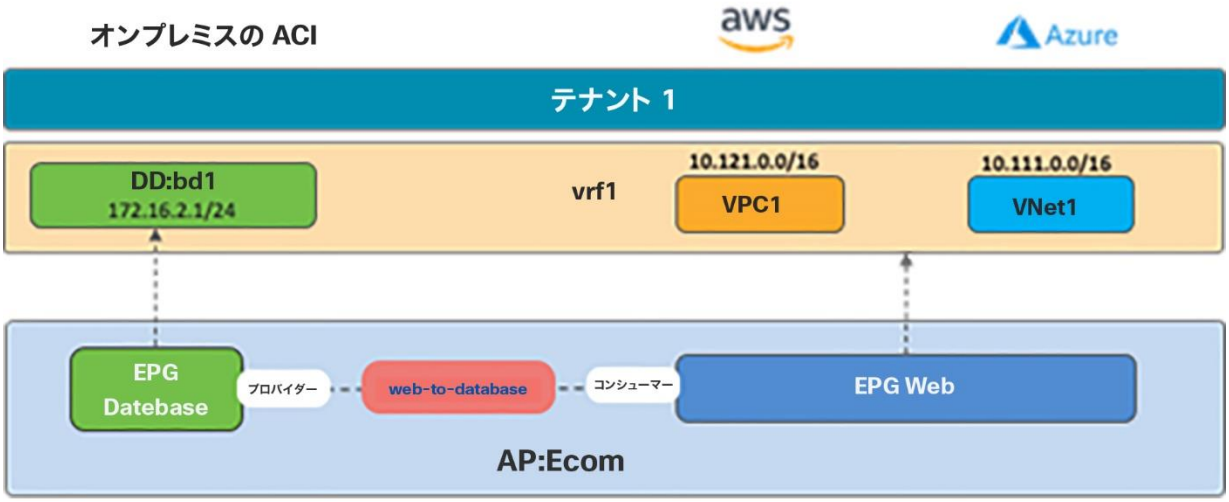

図 29. 複数のサイトにまたがるアプリケーション（テナント内）

エンドポイントが異なる環境にある場合でも、EPG 内の通信にはコントラクトは必要ありません。たとえば、EPG「Web」の AWS インスタンスは、コントラクトなしで EPG「Web」の Azure VM と通信できます。EPG がストレッチされている場合、通信に必要なルーティングとセキュリティポリシーの構成は、NDO を介して各環境に自動的に展開されます。

AWS と Microsoft Azure では、内部ルーティングと外部ルーティングの導入方法が異なりますが、Cloud ACI は、さまざまな環境に一貫したネットワークとセキュリティポリシーモデルを提供し、ハイブリッドマルチクラウド環境での運用を簡素化することで、この複雑さを標準化します。管理者は VRF、EPG、および NDO 上の EPG 間のコントラクトを作成します。これらは、Cisco APIC および Cloud APIC コントローラとの対話を通じて、これらの環境全体で展開を処理します。

考慮事項：このユースケースでは、アプリケーション層（Web EPG など）がパブリッククラウドプラットフォーム全体に広がっています。これを実現するには、AWS と Azure 両方のクラウドサイトに関連付けられているテンプレート（たとえば、「ストレッチテンプレート」）で、Web EPG 構成をプロビジョニングする必要があります。NDO では、テンプレートは構成プロビジョニングの最小単位を表します（構成の変更は一度に 1 つのテンプレートを展開できます）。したがって、ストレッチテンプレートを変更すると、ストレッチテンプレートが適用されるすべてのサイトに同時に変更がプッシュされます。結果として、このタイプのストレッチテンプレートでは、両方のパブリッククラウドサイトでサポートされている機能のみを使用できます。たとえば、クラウドサービス EPG は、現時点では Microsoft Azure を使用する Cloud ACI でのみサポートされている機能であるため、ストレッチテンプレートでは構成できません。

ユースケース #2：ハイブリッドマルチクラウド環境での共有サービス

このセクションでは、共有サービスと呼ばれる、共通のプロバイダーリソースが異なるコンシューマーで共有されるユースケースについて説明します。共有サービスの例には、ユーザーとアプリケーションで共有される共通データベース、DNS、AD サービスなどがあります。

ネットワーク設計の観点から言えば、共有サービスは、以下の特定の条件下では VRF 間接続を介して導入できます。

- VRF 間でリークできるのは、重複しない IP アドレスだけです。
- 複数のコンシューマ VRF からプロバイダー VRF にリークされるサブネットは一意にする必要があり、重複できません。

コントラクト設計の観点から言えば、VRF 間およびテナント間コントラクトには、次のガイドラインがあります。

- VRF 間テナント内コントラクトの場合、コントラクト範囲を [テナント（tenant）] に設定する必要があります。
- テナント間コントラクトの場合、コントラクト範囲を [グローバル（global）] に設定する必要があります。
- コンシューマーとプロバイダーの VRF は、サイト全体にストレッチする必要はありません（サイトローカルにできます）。
- サイト間のテナント間コントラクトの場合、NDO がクラウド環境を管理するための適切な資格情報を持つように、両方のサイトを NDO 「テナント」構成の両方のテナントに関連付ける必要がありますが、テナントを 「スキーマ」構成を介して両方のサイトに展開する必要はありません。次に例を示します。
    - オンプレミス ACI サイトの VRF1 の EPG1 の tenant1。
    - クラウドサイトの VRF2 の EPG2 の tenant2。
    - オンプレミスの ACI サイトとクラウドサイトの両方が、NDO「テナント」構成の tenant1 と tenant2 に関連付けられています。
    - tenant1 のスキーマ template1 はオンプレミスの ACI サイトにのみ展開され、tenant2 の template2 はクラウドサイトにのみ展開されます。

上記の考慮事項があるため、Cloud ACI のサイト間でサブネットリークとルート伝達がどのように機能するか、およびサポートされているコントラクト構成を理解することが重要です。次のサブセクションでは、VRF 内ルート伝達、VRF 間ルートリーク、および VRF 間コントラクトとテナント間コントラクトの構成例について説明します。

VRF 内のルート伝達

このサブセクションでは、サイト間の VRF 内ルート伝達について説明します。

次の図は、VRF が AWS、Microsoft Azure、オンプレミスの ACI サイトを含む複数のサイトにまたがっている場合の VRF 内ルート伝達の例を示しています。この例では、vrf1 もオンプレミスの ACI サイトに展開されています

が、オンプレミスの ACI サイトにはまだブリッジドメインが展開されていません。その結果、AWS と Microsoft Azure の両方の Cisco Cloud ルータには、vrf1 ルーティングテーブルに 2 つのルートがあります（この例では、10.111.0.0/16 と 10.121.0.0/16）。

図 30. オンプレミスの ACI サイトにブリッジドメインがなく VRF が複数のサイトにまたがっている

次に、BD サブネットが 172.16.2.1/24 であるブリッジドメイン（bd1）があり、そのブリッジドメインがオンプレミスの ACI サイトに展開されているとします。bd1 の EPG がオンプレミスの ACI サイトとクラウドサイトにまたがっている場合、または bd1 の EPG がクラウドサイトの別の EPG とコントラクトしている場合、172.16.2.0/24 サブネットは Cisco Cloud ルータにアドバタイズされます。

次の図は、ストレッチ EPG の存在により、オンプレミスの ACI サイトからクラウドサイトへのルートが伝達される第 1 の例です。

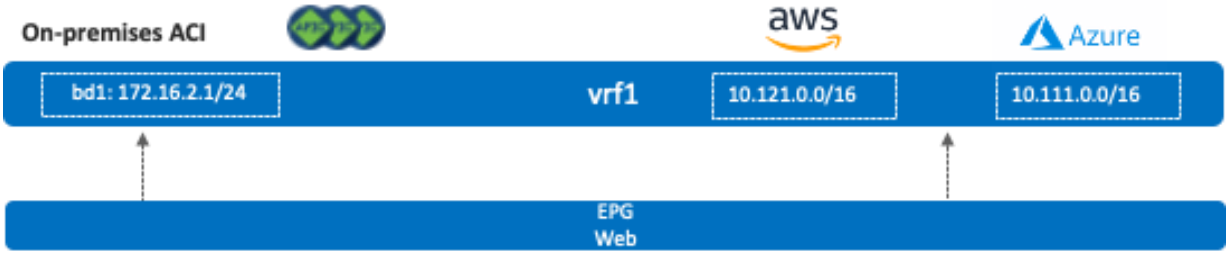

図 31. すべてのサイトにストレッチされた EPG

次の図は、ストレッチされていないオンプレミス EPG（EPG「Database」）と別のストレッチされていないクラウド EPG（EPG 「Web」）間のコントラクトを使用する第 2 の例です。

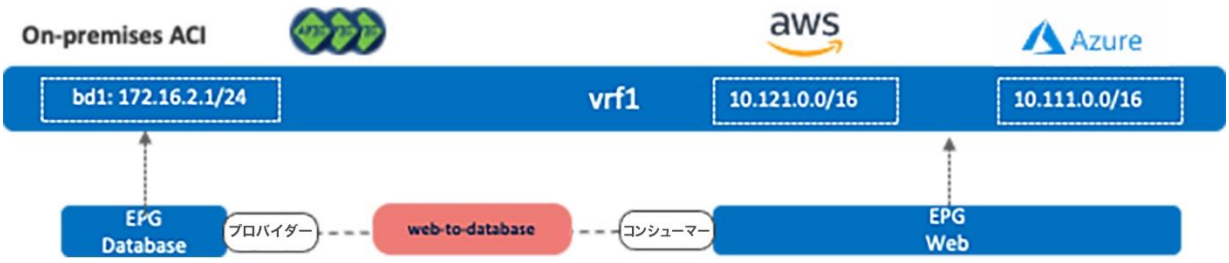

図 32. オンプレミス EPG とクラウド EPG 間のコントラクト

VRF 間およびテナント間コントラクトの構成例

このサブセクションでは、VRF 間ルートリークの動作、および VRF 間コントラクトとテナント間コントラクトの構成例について説明します。

次の図は、VRF がサイト全体にストレッチされるシナリオ 2a を示しています。テナント間コントラクトの場合、両方のテナントがサイト全体にストレッチされます（両方のテナントがすべてのサイトに展開されます）。この例では、EPG「Web」および「Web2」はクラウドサイトのみに展開され、EPG「Database」および

「Database2」はオンプレミスの ACI サイトのみに展開されます。このシナリオでは、これらの間のコントラクトにより、次の通信が許可されます。

- EPG Web のエンドポイントと EPG Database のエンドポイント
- EPG Web2 のエンドポイントと EPG Database2 のエンドポイント
- EPG Web のエンドポイントと EPG Web2 のエンドポイント

他の EPG 間通信は、ルートが存在する場合でも許可されません。たとえば、EPG Web のエンドポイントと EPG Database2 のエンドポイントは相互に通信できません。

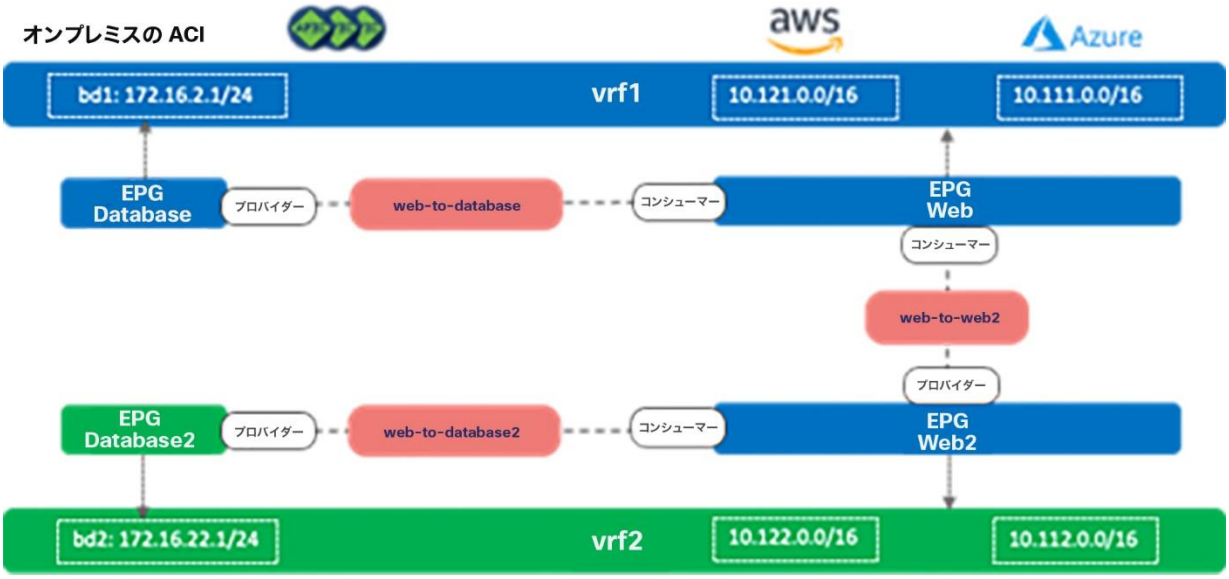

図 33. シナリオ 2a：コンシューマーとプロバイダーの VRF がサイト全体にストレッチされている

Cloud ACI での VRF 間ルートリークの動作は、特定のサブネットを他の VRF にのみリークするオンプレミス ACI ファブリック内の VRF 間ルート リークとは少し異なることに注意してください。Cloud ACI の場合、VRF 間コントラクトがある場合、すべての CIDR とルートが他の VRF にリークされます。たとえば、vrf1 と vrf2 の間の VRF 間コントラクトが EPG Web と Web2 の間だけである場合でも、vrf1 と vrf2 には、他の VRF からリークされた次のルートがあります。

- vrf1：10.122.0.0/16（AWS での vrf2 CIDR）、10.112.0.0/16（Azure での vrf2 CIDR）、および 172.16.22.0/24（bd2）
- vrf2：10.121.0.0/16（AWS での vrf1 CIDR）、10.111.0.0/16（Azure での vrf2 CIDR）、および 172.16.2.0/24（bd1）

次の図は、シナリオ 2a と比較してコントラクト数が多いシナリオ 2b を示しています。この場合、サイト間のすべての EPG 間通信が許可されます（たとえば、EPG Web のエンドポイントと EPG Database2 のエンドポイントは相互に通信できます）。

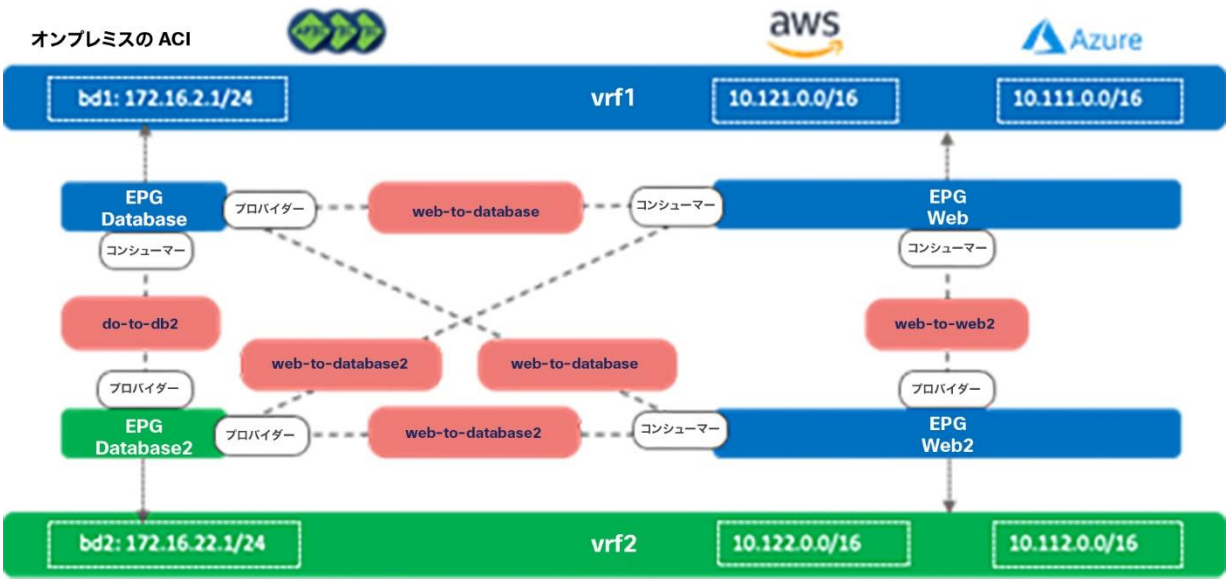

図 34. シナリオ 2b：サイト全体のフルメッシュコントラクト

次の図は、コンシューマーまたはプロバイダーの VRF がオンプレミスの ACI サイトとクラウドサイトにストレッチされていないシナリオ 2c を示しています。コンシューマー VRF 「vrf1」は AWS と Microsoft Azure にのみ展開され、プロバイダー VRF 「vrf2」はオンプレミスの ACI サイトにのみ展開されます。テナント間コントラクトの場合、テナントをすべてのサイトに展開する必要はありませんが、オンプレミスの ACI サイトとクラウドサイトの両方を NDO「Tenants」構成の両方のテナントに関連付ける必要があります。

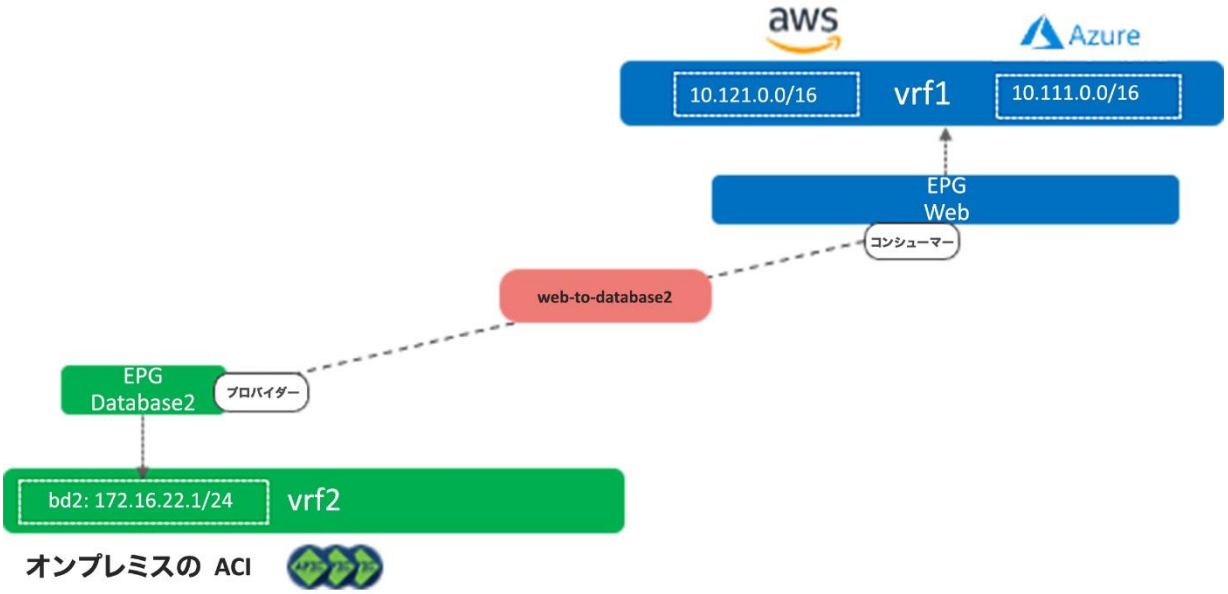

図 35. シナリオ 2c：オンプレミス ACI とクラウドサイト間の非ストレッチ VRF

次の図は、3 つの VRF がサイトローカルであるシナリオ 2d を示しています。シナリオ 2c の考慮事項と同様に、テナント間コントラクトの場合、テナントをすべてのサイトに展開する必要はありませんが、すべてのサイトを NDO「Tenants」構成のすべてのテナントに関連付ける必要があります。

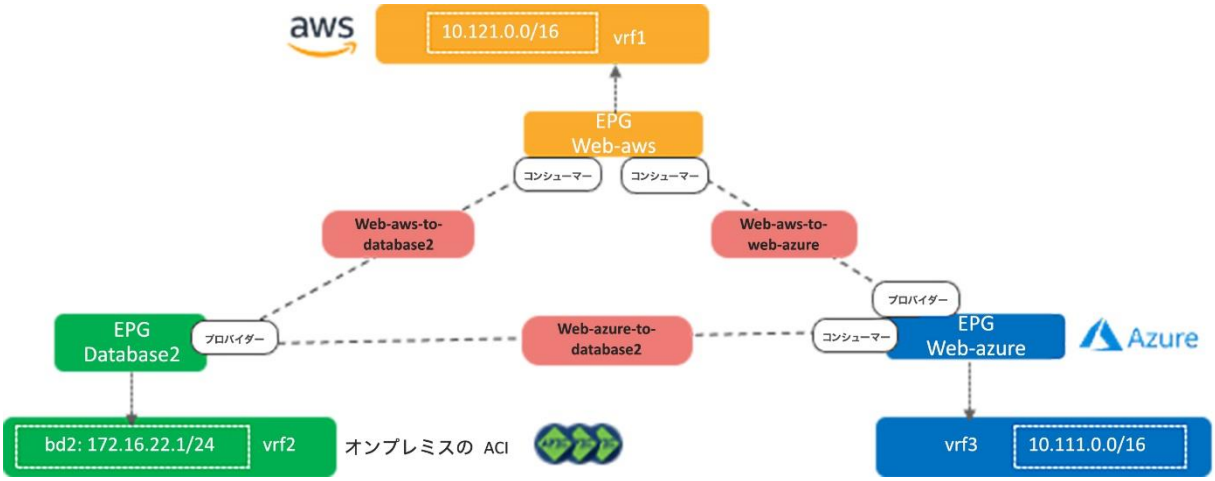

図 36. シナリオ 2d：3 つの非ストレッチ VRF

次の図は、シナリオ 2e を示しています。このシナリオは、オンプレミスの ACI ファブリックで外部 EPG として表される外部ネットワークに共有サービスが存在する一般的な共有サービスのユースケースの 1 つです。レイヤ 3 アウト（L3Out）は、VRF の 1 つ（図 37 の vrf1）または別の VRF（図 38 の vrf3）で構成する必要があります。vrf1 と vrf2 の両方で定義することはできません。

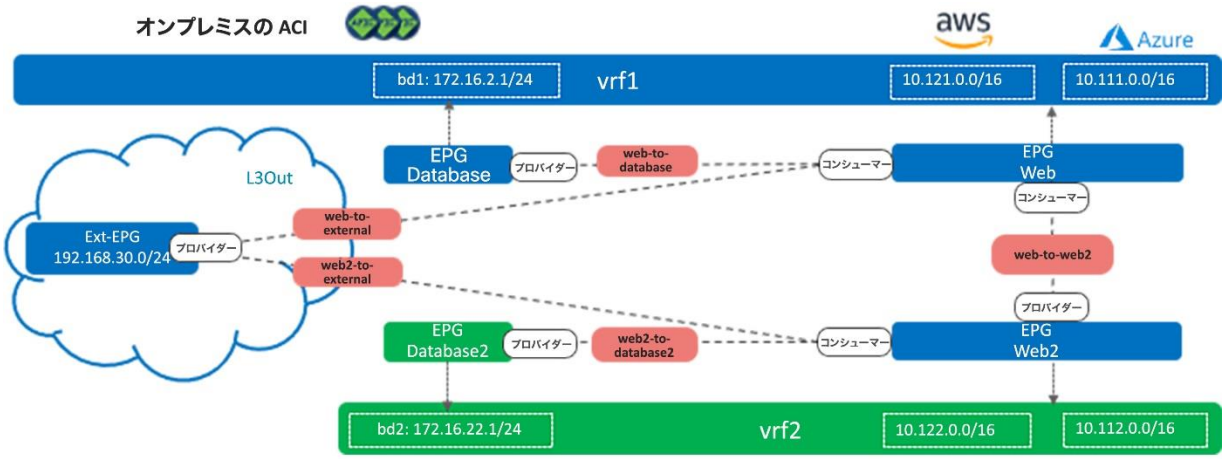

図 37. シナリオ 2e：オンプレミス ACI サイトの外部ネットワークを介した共有サービス

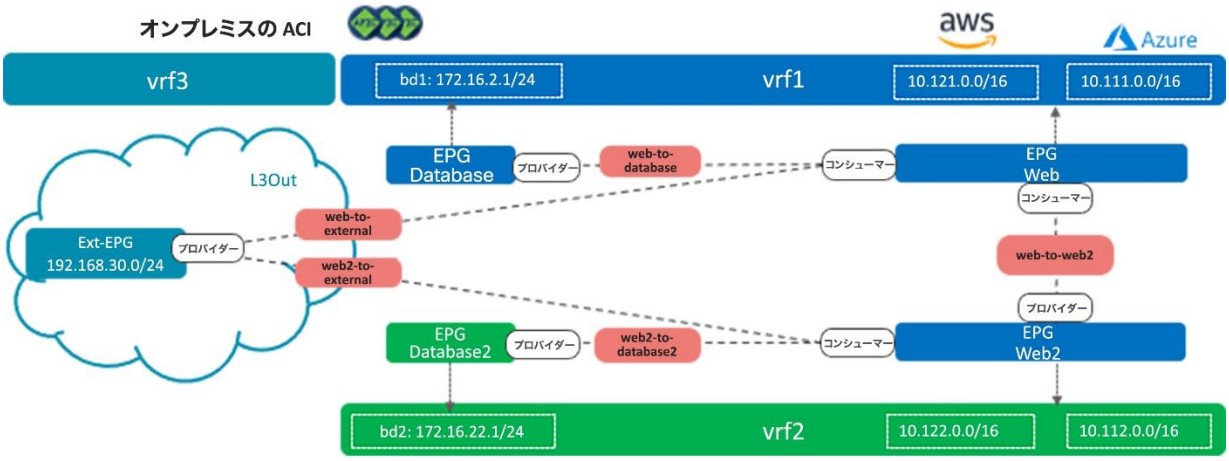

図 38. シナリオ 2e：オンプレミス ACI サイトの外部ネットワークを介した共有サービス（個別の VRF の使用）

vrf1 と vrf2 の両方に存在できない理由は、ルートが重複する可能性があるためです。シナリオ 2a で説明したように、Cloud ACI の場合、VRF 間コントラクトがあれば、すべての CIDR とルートが他の VRF にリークされます。以下の図にサポートされない例を示します。vrf1 と vrf2 の間の VRF 間コントラクトが EPG Web と Web2 の間だけである場合でも、vrf1 と vrf2 には、他の VRF からリークされた次のルートがあります。

- vrf1：10.122.0.0/16（AWS での vrf2 CIDR）、10.112.0.0/16（Azure での vrf2 CIDR）、172.16.22.0/24（bd2）、および **192.168.30.0/24**
- vrf2：10.121.0.0/16（AWS での vrf1 CIDR）、10.111.0.0/16（Azure での vrf2 CIDR）、172.16.2.0/24（bd1）、および **192.168.30.0/24**

問題は、両方の VRF で、192.168.30.0/24 ルートが VRF 内でリークされ、また他の VRF からもリークされるため、サブネットが重複することです。

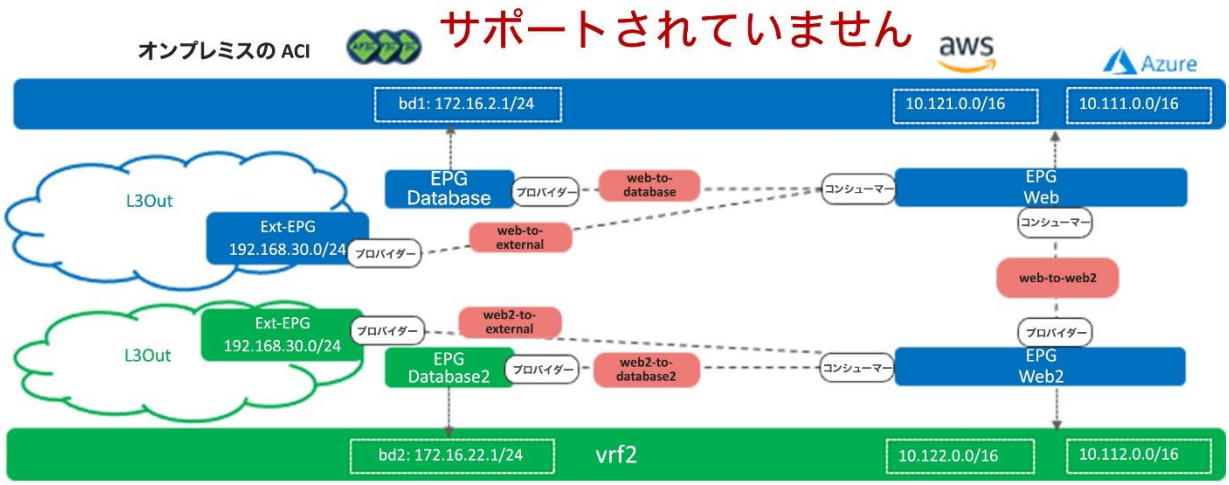

図 39. シナリオ 2e：サポートされない例

上級者向けの注意事項：このタイプの重複ルートがある場合、オンプレミスの ACI でトラフィックがドロップされる可能性があります。たとえば、vrf1 のクラウドエンドポイントから外部ネットワーク（192.168.30.0/24）へのトラフィックは、Cisco Cloud ルータの 1 つに転送され、vrf1 ではなく vrf2 経由のルートを使用してオンプレミスの ACI ファブリックにトラフィックを送信する可能性があります。つまり、トラフィックが vrf2 VNID を使用してオンプレミスの ACI ファブリックに到着します。その結果、ACI リーフスイッチは、vrf1 の EPG の許可ルールを持たない vrf2 のゾーン分割ルールを参照します。

外部 EPG とクラウド EPG の構成に関する考慮事項については、ユースケース #3-2 で説明します。

ユースケース #3：クラウドからインターネット/外部ネットワークへの接続

ユースケース #3-1：クラウド ネイティブ ルーティング機能を使用したクラウドからインターネットへの接続
これは、クラウドワークロードがクラウド ネイティブ ルーティング機能（AWS のインターネットゲートウェイや Microsoft Azure のデフォルト システム ルートなど）を使用してインターネットに直接アクセスする一般的なユースケースです。このユースケースの主な利点は、簡素化と拡張性です。構成が簡単であり、パブリッククラウドプラットフォームによって、その VPC（AWS 上）および VNet（Microsoft Azure 上）から直接、大規模なインターネットアクセスが提供されます。

次の図は、EPG「Web」と外部 EPG「Internet-EPG」（0.0.0.0/0 IP セレクタを使用）が、アプリケーションプロファイル「Ecom」のテナントで定義されている例を示しています。クラウドワークロードから開始されるインターネットアクセスを許可するには、コンシューマーとしての EPG「Web」とプロバイダーとしての「Internet EPG」の間にコントラクトを適用する必要があります。

この場合、Cloud ACI コントラクトがコンシューマーからプロバイダーへのトラフィックのみの許可ルールを作成するため、インターネット上のエンドポイントによって発信され、EPG Web（コンシューマー）のクラウドエンドポイントに向かうトラフィックは許可されません。プロバイダーからコンシューマーへのリターントラフィックは、（明示的な許可ルールがない場合でも）自動的に許可されます。これは、コンシューマーからプロバイダーへのトラフィックが以前に監視されているためです。したがって、インターネット上のエンドポイントが EPG Web 内のクラウドエンドポイントとの通信を開始する可能性がある場合、インターネット-EPG はコントラクトのコンシューマー、EPG Web はコントラクトのプロバイダーである必要があります。

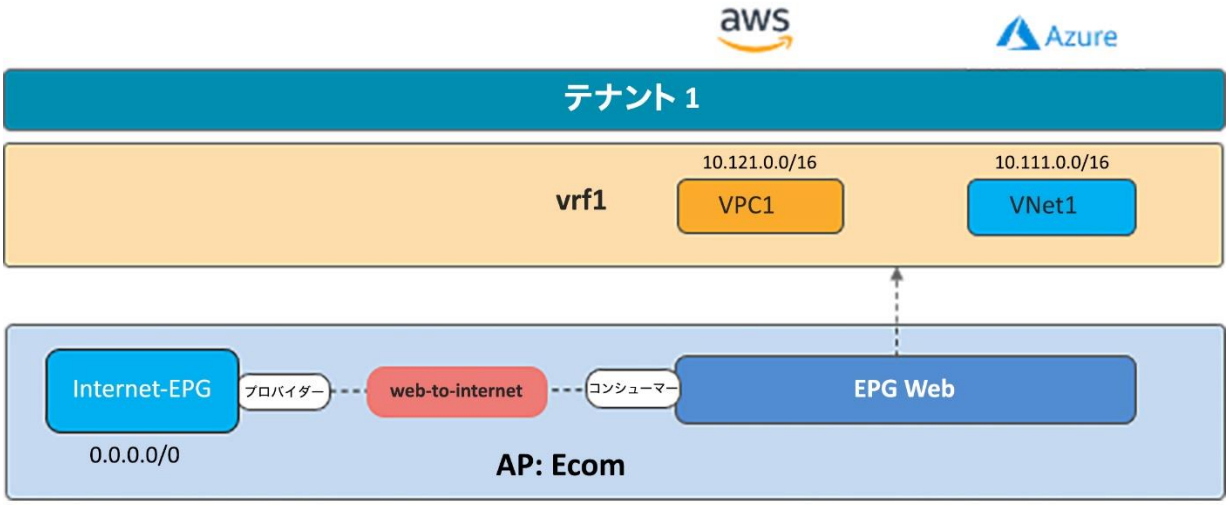

図 40. クラウドワークロードからインターネットへのアクセス

ユースケース #3-2：オンプレミスの L3 外部（L3Outs）を介したクラウドから外部ネットワークへの接続
このユースケースは、オンプレミスの ACI ファブリックを介して外部ネットワークとパブリッククラウド リソース間の接続を提供する必要がある場合に使用されます。外部ネットワークには、WAN、単純なブランチ、またはインターネット接続を使用できます。

このユースケースの利点は、一貫したセキュリティポリシーモデルと安全な接続です。通常のエンドポイントとして接続されているかのようにオンプレミスの ACI サイトへの接続をルーティングしたポリシーを、外部ネットワークに適用できます。オンプレミスのファイアウォールを使用して、クラウドサイトに出入りするトラフィックに特定のセキュリティポリシーを適用できます。

次の図は、アプリケーションプロファイル「Ecom」のテナントに、レイヤ 3 外部「L3Out」と外部 EPG 「Ext-EPG」が定義されている例を示しています。このユースケースの目的は、クラウドサイトでプロビジョニングされた EPG 「Web」と、オンプレミスの L3Out を介してアクセス可能な外部ネットワークリソースとの間の接続を提供することです。したがって、EPG「Ext-EPG」（オンプレミスの L3Out に関連付けられている）とクラウド内の EPG「Web」 の間にコントラクトを適用する必要があります。EPG「Database」と外部 EPG 「Ext-EPG」間のコントラクトは任意です。

。

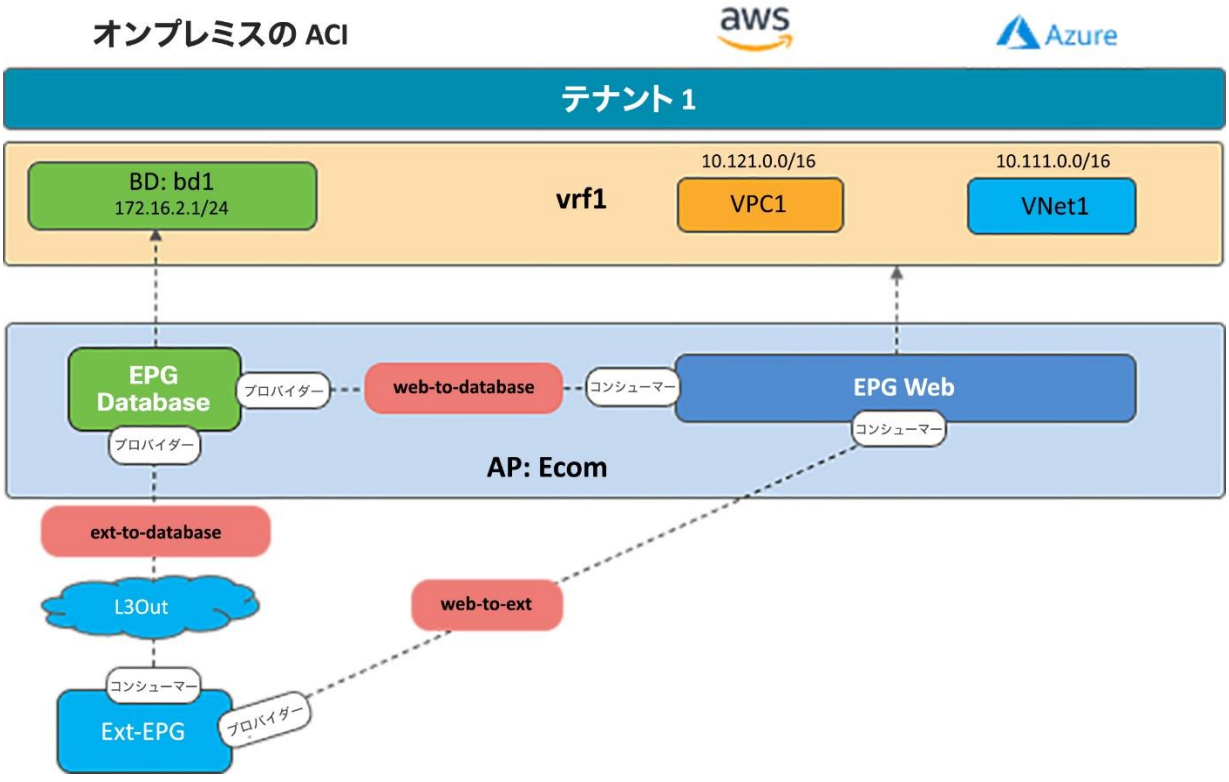

図 41. 共有オンプレミス L3Out

このユースケースには、次のガイドラインがあります。

- オンプレミスの ACI サイトにマッピングされた専用テンプレートで、関連付けられた外部 EPG とともに L3Out を構成する必要があります。
- オンプレミスの L3Out からクラウド EPG サブネット（この特定の例では Web EPG が存在するサブネット）をアドバタイズするには、Ext-EPG の下でクラウド CIDR プレフィックスを構成し、[ルート制御をエクスポート（Export Route Control）] をオンに設定する必要があります。（図 42）
- オンプレミスの L3Out 接続を介して学習した外部プレフィックスをクラウドサイトにアドバタイズするには、外部 EPG で [共有ルート制御（Shared Route Control）] と [外部 EPG の外部サブネット（External Subnets for External EPG）] を設定する必要があります（図 43）。

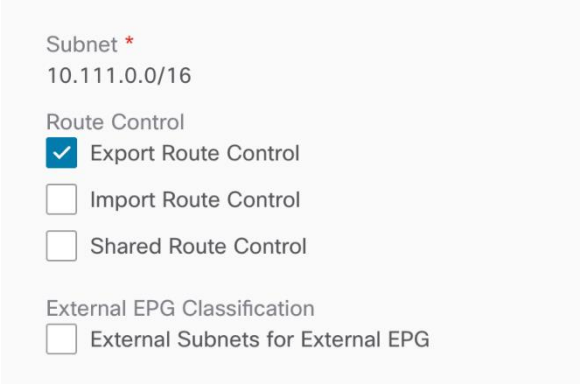

図 42. クラウド EPG サブネットの [ルート制御をエクスポート（Export Route Control）]

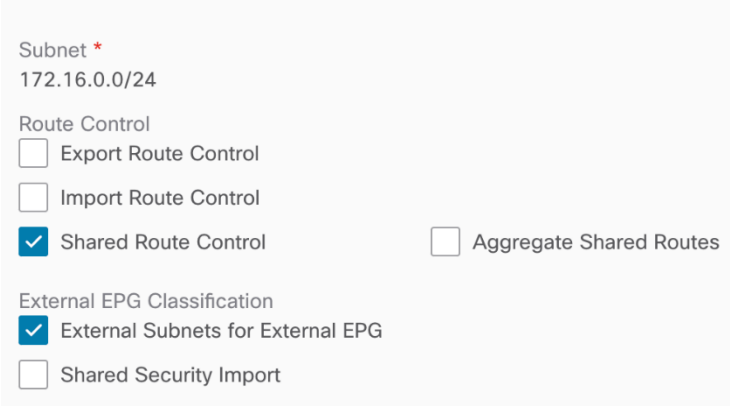

図 43. オンプレミス ACI ファブリック上の [共有ルート制御（Shared Route Control）] と [外部 EPG の外部サブネット（External Subnets for External EPG）]

ユースケース #4：クラウド ネイティブ ルーティング サービスを使用した外部サイトへの接続

概要

このユースケースの目的は、Azure VPN や ExpressRoute Gateway、AWS Transit Gateway などのクラウド ネイティブ ルーティング サービスを使用して、外部サイトに接続することです。

- Azure の場合、クラウド管理者が Microsoft Azure ポータルから直接 Azure VPN/ExpressRoute Gateway を作成する必要があります。
- AWS の場合、Cisco Cloud APIC は、Cisco Cloud APIC の初回設定プロセスの一部として Transit Gateway を自動的に作成します。

BGP は、ブランチの外部デバイスからクラウド ネイティブ ルーティング サービスへの動的プロトコルとして使用され、IPsec はアンダーレイトンネルとして使用されます。セキュリティルールは、AWS の SG ルールと Microsoft Azure の NSG ルールを使用して、各クラウドサイトで適用されます。

以下の表は、Cloud APIC の権限下でのクラウドプラットフォームから外部サイトへの外部接続の提供に関する Microsoft Azure と AWS の違いをまとめたものです。

表 3. 外部接続に関する Microsoft Azure VPN/ExpressRoute Gateway と AWS Transit Gateway の比較

	Microsoft Azure VPN/ExpressRoute Gateway	AWS Transit Gateway
サービスのプロビジョニングの自動化	クラウド管理者は、Microsoft Azure ポータルから VPN/ExpressRoute Gateway を手動で作成します。	Transit Gateway のプロビジョニングは、Cisco Cloud APIC の初回設定プロセスの一部として Cisco Cloud APIC によって自動化されています。
設定の自動化	Microsoft Azure は、ゲートウェイ構成を自動化し、外部デバイスの構成テンプレート（デバイス構成スクリプトとも呼ばれます）をエクスポートします。クラウド管理者は、Cisco ISR、ASA などのさまざまな製品の構成テンプレートを選択できます。クラウド管理者は、外部デバイスに合わせて構成テンプレートを編集する必要がある場合があります。	Cisco Cloud APIC は、Transit Gateway の設定を自動化し、外部デバイスの構成テンプレートをエクスポートします。構成テンプレートは Cisco IOS-XE CLI シンタックスに基づいているため、クラウド管理者が外部デバイスに合わせて編集する必要がある場合があります。
クラウドネイティブサービスと外部デバイス間のルーティングプロトコルとセキュリティ	IPsec 上の外部 BGP。	IPsec 上の外部 BGP。
スループットはサイズ変更可能か	はい、クラウド管理者はゲートウェイ SKU を指定したり、スループット要件に応じて別の SKU に変更したりできます。	いいえ、Transit Gateway は固定サービスであるためです。

ユースケース #4-1：Microsoft Azure VPN Gateway と ExpressRoute Gateway を使用した外部サイトへの接続

このユースケースは、外部サイト（ブランチネットワークなど）を Microsoft Azure に直接接続するオプションの 1 つです。Microsoft Azure がゲートウェイの展開に必要とするゲートウェイサブネットは、初回設定時に Cisco Cloud APIC によって自動的に展開されます。Azure ExpressRoute Gateway と Azure VPN Gateway はどちらも、ブランチネットワークから Microsoft Azure への接続に使用できます。

- Azure ExpressRoute Gateway は、Microsoft のグローバルネットワークを介して Microsoft Azure への直接接続を提供します。転送されるデータはすべて暗号化されず、インターネットを経由しません。
- Azure VPN Gateway は、インターネットを介した Microsoft Azure への安全な接続を提供します。転送されるすべてのデータはプライベートトンネルで暗号化され、インターネットを経由します。

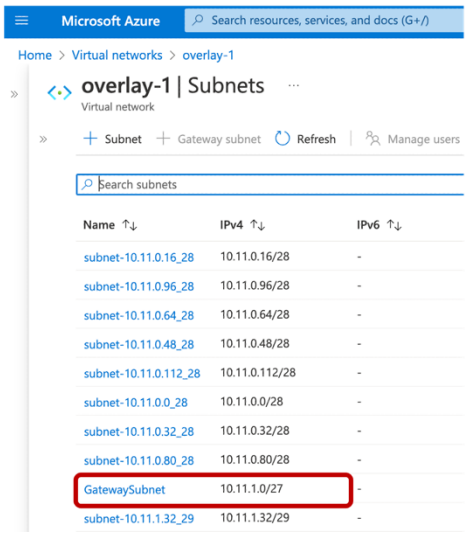

図 44. Cisco Cloud APIC によって作成されたゲートウェイサブネット

このユースケースでは、クラウド管理者が Microsoft Azure ポータルから直接 Microsoft Azure VPN Gateway（または ExpressRoute Gateway）を作成します。クラウド管理者は、ローカル ネットワーク ゲートウェイ（外部デバイスを表す Microsoft Azure の用語）も作成します。VPN Gateway の BGP ASN、外部デバイス、IPsec オプションなどの必須情報を入力すると、Microsoft Azure は外部デバイスタイプに基づいて構成テンプレートをエクスポートします（Microsoft Azure は、Cisco ASA、 ISR などさまざまなデバイスタイプをサポートします）。構成テンプレートには、IPsec トンネルや BGP の構成など、必要な情報が含まれています。構成テンプレートに基づいて外部デバイスを構成し、外部デバイスと Azure VPN Gateway の間に IPsec および BGP セッションを確立するのは、ネットワーク管理者の責任です。

外部デバイスの背後にあるブランチサブネットルートは、外部サイトからクラウドサイトへ、BGP を介して Azure VPN Gateway にアドバタイズされます。次に、Azure VPN Gateway は、ゲートウェイトランジットを使用した VNet ピアリング（トランジットピアリングとも呼ばれます）を使用して、ブランチサブネットルートをユーザー VNet（スポーク VNet とも呼ばれます）に伝達します。ゲートウェイトランジットを使用した VNet ピアリングは、Cisco Cloud APIC によって自動的に有効になります。

クラウドサイトから外部サイトへの逆方向では、ユーザーの VNet CIDR が Azure VPN Gateway に伝達され、Azure VPN Gateway が BGP を介して外部デバイスにアドバタイズします。

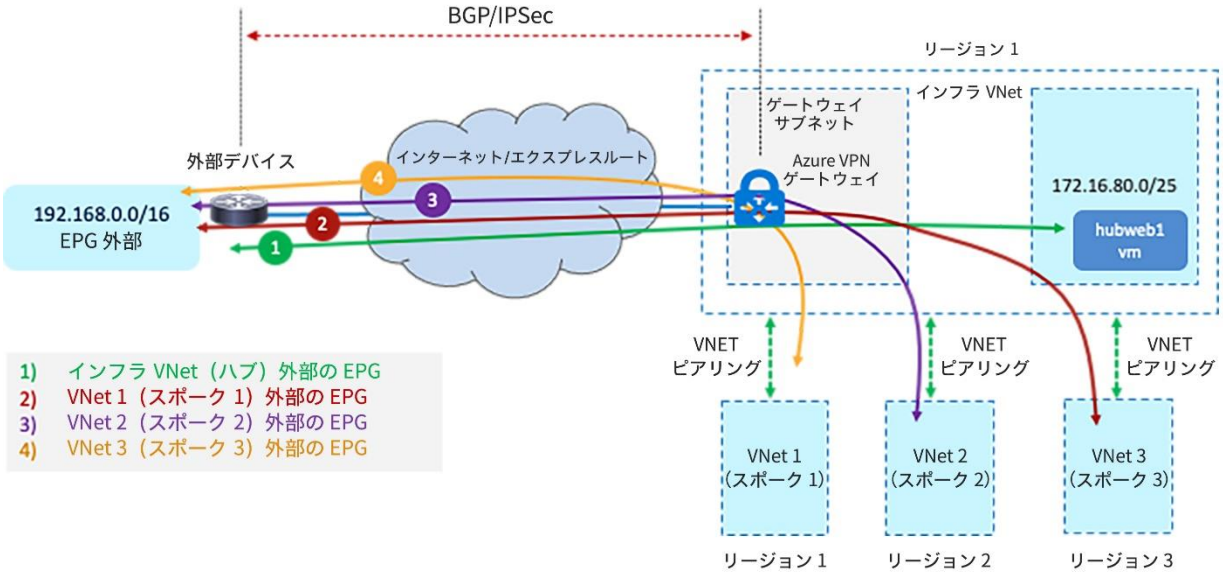

図 45. Azure VPN Gateway と外部デバイス間の接続

このユースケースの主な利点は、導入の柔軟性です。一部の設計シナリオでは、ブランチサイトが異なる物理リージョンに分散しており、すべてのブランチサイトがオンプレミスの ACI ファブリックを介してクラウドプラットフォームに接続するのは効率的ではありません。そのようなシナリオでは、このユースケースで、Azure ExpressRoute Gateway または VPN Gateway を終端ポイントとして利用し、ブランチサイトに展開された外部デバイスからクラウドプラットフォームに直接接続できます。Cloud ACI は一貫したポリシーモデルを引き続き提供します。

次の図はこのシナリオの例を示しています。この例では、外部 EPG 論理オブジェクト（Ext-EPG）を使用して、Microsoft Azure 外部のサブネットに属しており、クラウドでプロビジョニングされた EPG Web と通信する必要がある、すべてのエンドポイント（たとえば、外部サイト）を分類します。Ext-EPG と EPG Web の間で使用されるコントラクトの範囲は、[グローバル（global）] に設定する必要があります。これは、外部 EPG がインフラテナントに展開され、EPG「Web」がユーザーテナントに展開されるためです。

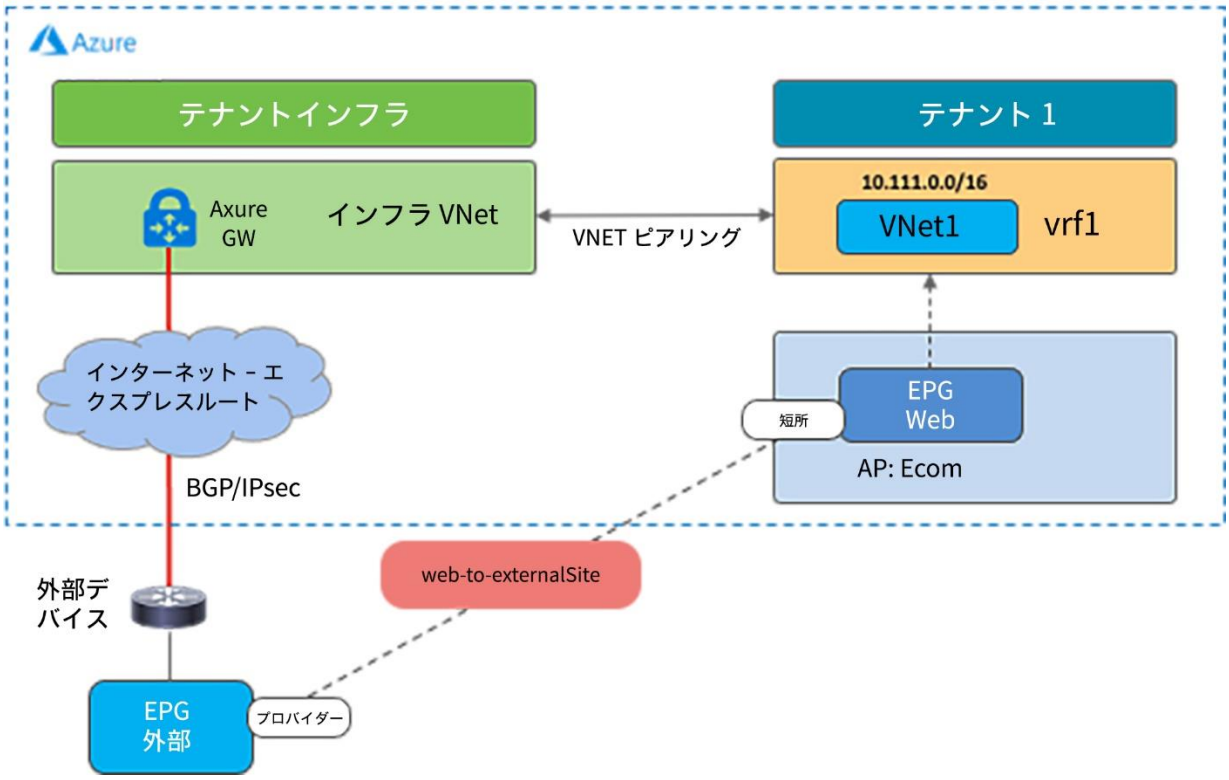

図 46. Azure Gateway を使用した外部サイトへの Microsoft Azure のアクセス

ブランチデバイスは IPsec と BGP を有効にする必要があることに注意してください。Microsoft Azure ExpressRoute Gateway と VPN Gateway がサポートするルートの数は限られているため、Microsoft Azure のドキュメントで最新のスケール数を確認してください。

ユースケース #4-2：AWS Transit Gateway を使用した外部サイトへの接続

このユースケースは、AWS のネイティブ ネットワーキング サービスである Transit Gateway を介して、ブランチネットワークなどの外部サイトを AWS に直接接続するオプションの 1 つです。Transit Gateway は、初回設定プロセス中に Cisco Cloud APIC によってインフラ VPC に自動的に展開されます。Cloud APIC 25.0(2) リリース以降、Cisco Cloud APIC は AWS Transit Gateway から外部サイトへの IPsec トンネルと BGP セッションを開始できます。Cisco Cloud APIC 管理者は、外部サイトのブランチデバイスのパブリック IP アドレスと BGP ASN、および AWS Transit Gateway とブランチデバイスの IKE や事前共有キーなどの一般的な IPsec パラメータを含む、適切な構成で外部接続を作成するだけです。構成ファイルをダウンロードし、Cisco Cloud APIC を介した接続を有効にして、外部デバイスを手動で構成するのはネットワーク管理者の責任です。

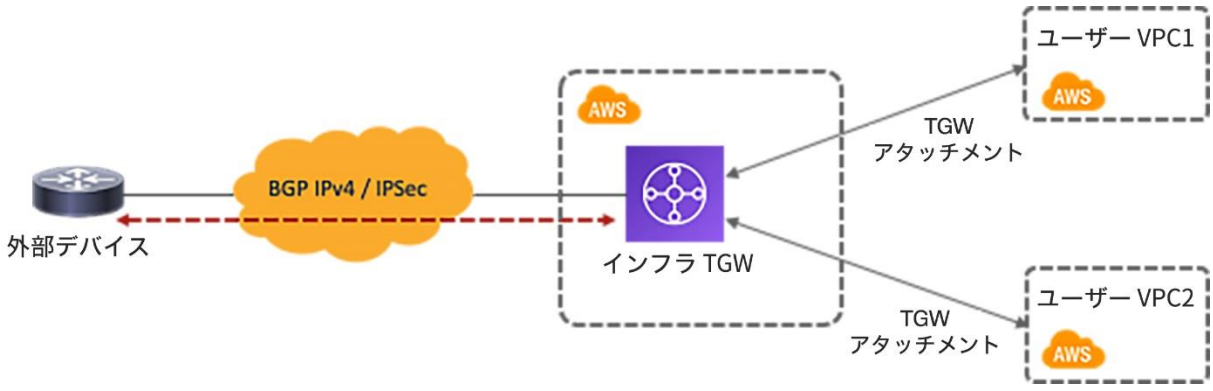

図 47. 外部デバイスの Transit Gateway への接続

このユースケースの主な利点は、ネットワークの自動展開における柔軟性です。このユースケースでは、Cisco Cloud APIC が TGW トンネルの構成と TGW ルートテーブルの作成を自動化します。さらに、Cisco Cloud APIC は、外部ネットワーク TGW ルートテーブルとユーザー VPC ルートテーブル間のルート伝達を自動化します。すべてのリージョンに Cisco Cloud ルータを導入する必要はありません。代わりに、AWS Transit Gateway VPN アタッチメントを活用することで、物理的な場所にあるブランチから異なる AWS リージョンにあるクラウドワークロードに接続できます。外部サイトの外部ネットワークはサブネットベースのセレクタを使用して外部 EPG として扱われ、外部 EPG とクラウド EPG の間でコントラクトを適用できるため、一貫したポリシーモデルも維持されます。

次の図で、構成例について説明します。この例では、外部 EPG は AWS 外部のサブネット用です。コントラクトの範囲は、[グローバル（global）] に設定する必要があります。これは、外部 EPG がインフラテナントに展開され、EPG「Web」がユーザーテナントに展開されるためです。

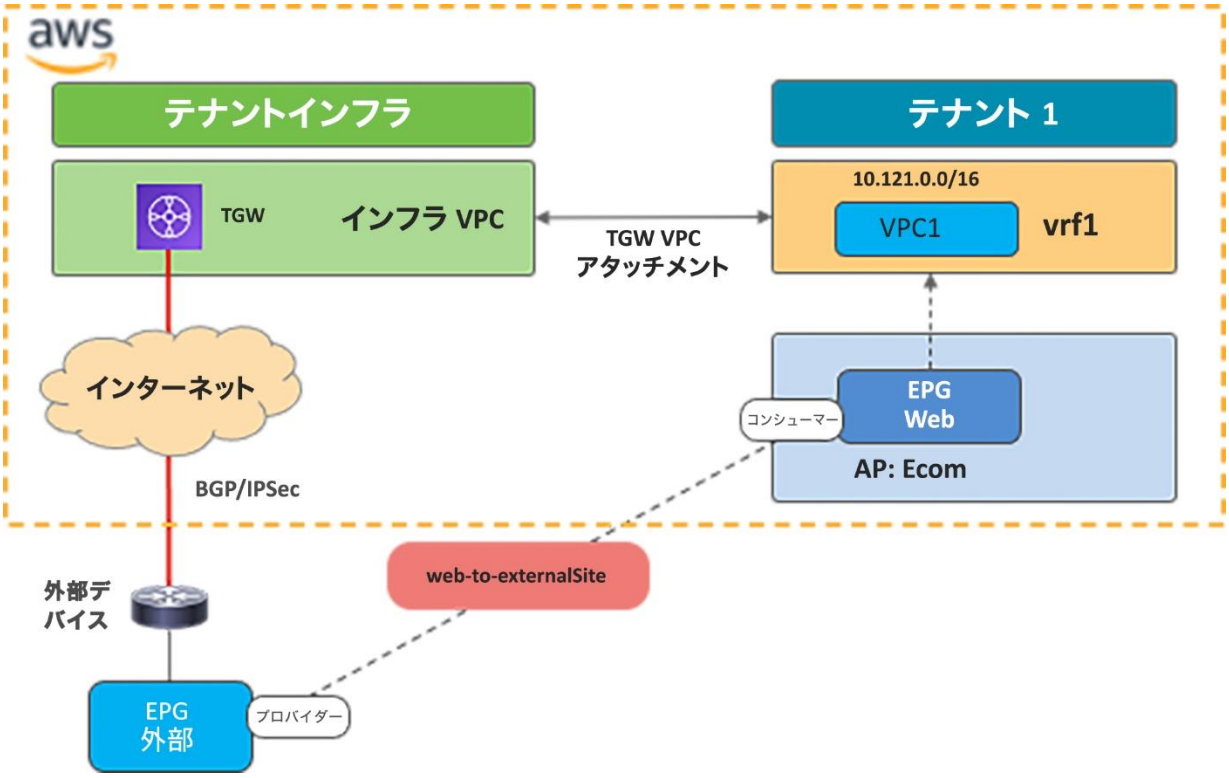

図 48. Transit Gateway を使用した外部サイトへの AWS のアクセス

ユースケース #5：WAN、ブランチ、または非 ACI サイトへの外部接続

このユースケースは、AWS と Microsoft Azure の両方で、Cloud ACI リリース 25.0(1) からサポートされている Cisco Cloud ルータの外部接続機能に基づいています。このユースケースは、オンプレミスの ACI ファブリックを経由せずに、外部 IP ネットワークをクラウドプラットフォーム（AWS および Microsoft Azure）に直接接続する必要がある場合に使用されます。

このユースケースとユースケース #4 の違いは、Cisco Cloud ルータまたはクラウド ネイティブ ルーティング サービスのどちらを終端地点として使用するかです。このユースケースの利点の 1 つは、ルーティングの規模です。Cisco Cloud ルータは、クラウドネイティブサービスと比較して、より多くのルートをサポートするためです。外部ネットワークのルーティングデバイスは、BGP と IPsec を使用して、インフラテナントの Cisco Cloud ルータへの IP 接続を確立する必要があります。集中型オーケストレーターとして、NDO は Cloud APIC と通信して Cisco Cloud ルータを構成し、外部デバイスの構成テンプレートを生成します。Cisco Cloud ルータは、外部デバイスが BGP と IPsec をサポートしている場合、クラウドプラットフォームの外部にある任意のネットワークに接続できます。

次の図で、構成例について説明します。この例では、外部ネットワークは Microsoft Azure 外部のサブネットとして分類されています。コントラクトの範囲は、[グローバル（Global）] に設定する必要があります。これは、外部 EPG がインフラテナントに展開され、EPG「Web」がユーザーテナントに展開されるためです。

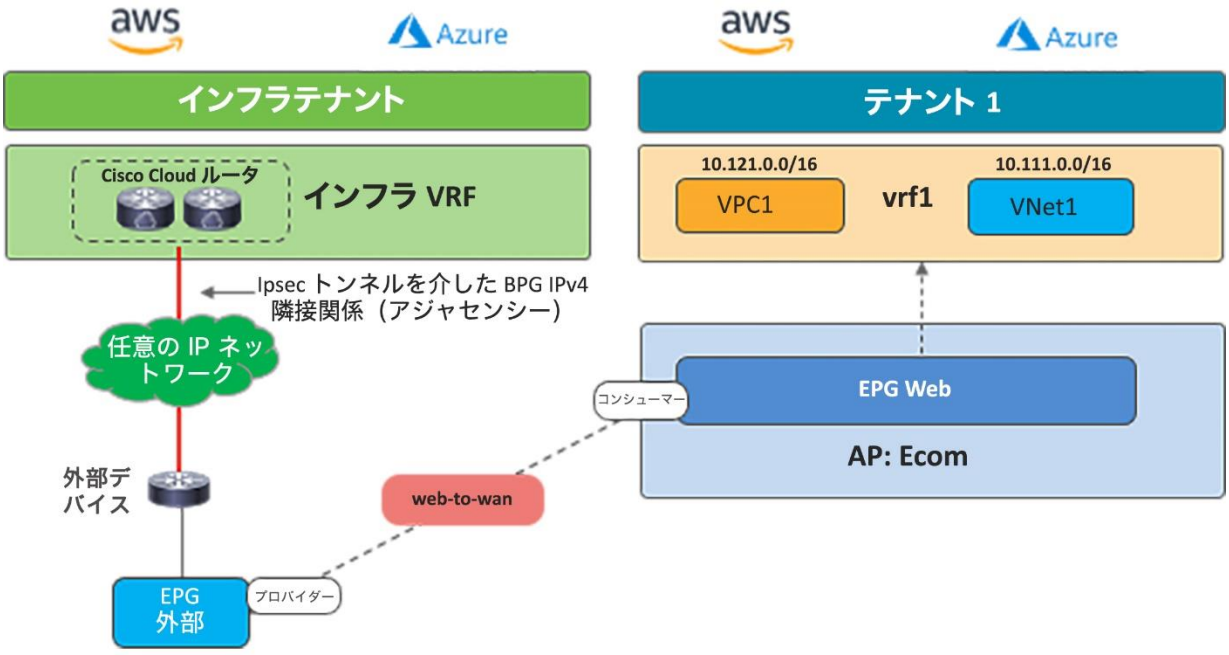

図 49. インフラ VRF の Cisco Cloud ルータを介した外部接続

このユースケースには、次のガイドラインがあります。

- 1 つのクラウドプラットフォームの Cloud ACI によって管理される Cisco Cloud ルータは、他のクラウドプラットフォームの Cisco Cloud ルータに接続するブランチのトランジットにはなりません。たとえば、ブランチのエンドポイントからのトラフィックは、Microsoft Azure サイトの Cisco Cloud ルータを介して AWS サイトのエンドポイントに到達できません。

- Cisco Cloud ルータはブランチのトランジットにはできません。つまり、ブランチ 1 からのトラフィックは Cisco Cloud ルータを介してブランチ 2 に到達できません。
- Cisco Cloud ルータはブランチおよびオンプレミスの ACI サイトのトランジットにはできません。つまり、1 つのブランチからのトラフィックは Cisco Cloud ルータを介してオンプレミスの ACI サイトに到達できません。

次の図は、サポートされているトラフィックフローとサポートされていないトラフィックフローを示しています。

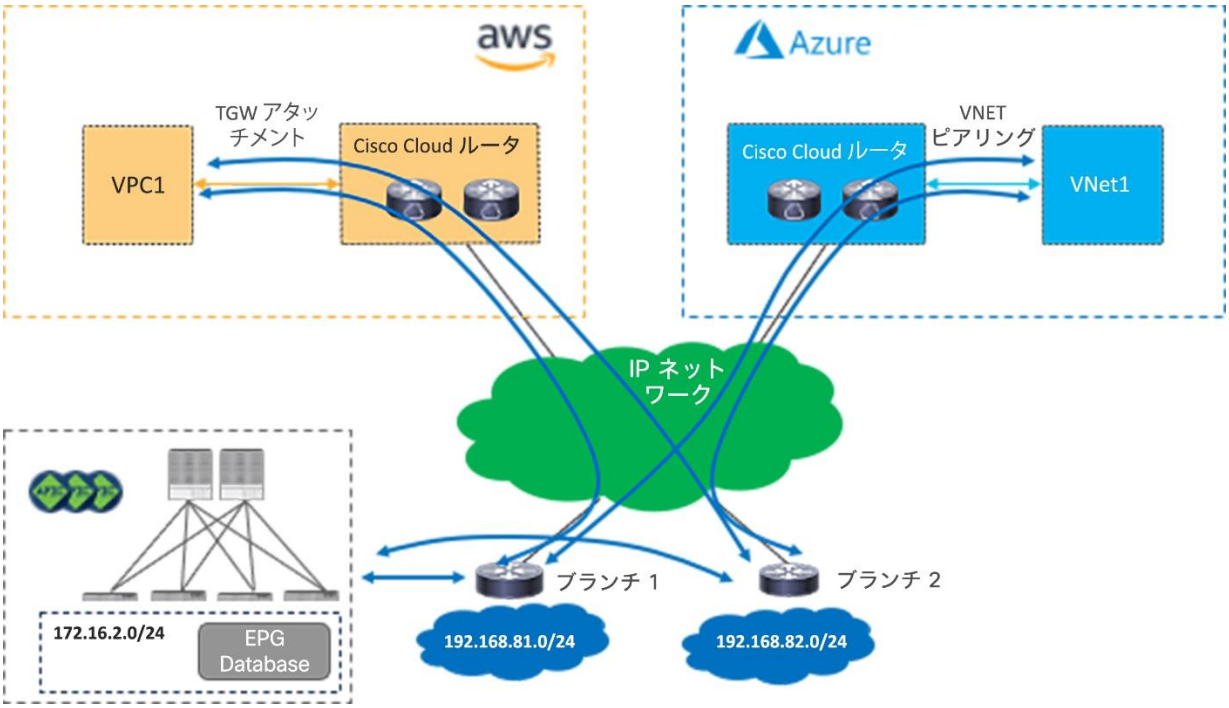

図 50. サポートされているトラフィックフロー

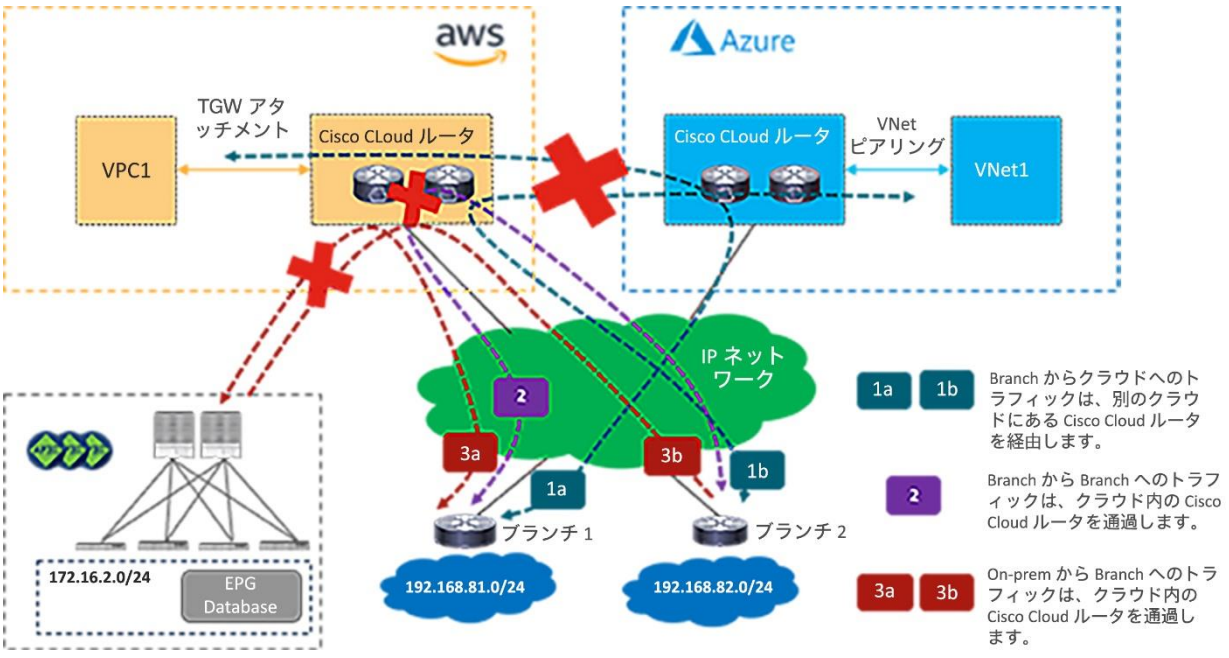

図 51. サポートされていないトラフィックフロー

ユースケース #6：SD-WAN ソリューションとの相互運用

Cloud ACI リリース 25.0(1) でサポートされている Cisco Cloud ルータの外部接続機能を活用することで、ユースケース #4 で説明されているように、Cisco SD-WAN または任意の SD-WAN ソリューションが Cloud ACI と相互作用して、ブランチネットワークからクラウドワークロードへの接続とセグメンテーションを提供できます。

次の図はこのシナリオの例を示しています。Cloud ACI から見ると、SD-WAN ブランチネットワークは外部 EPG です。SD-WAN エッジデバイスは、パブリッククラウドプラットフォームなど、どこにでも導入できます。SD-WAN エッジデバイスから Cisco Cloud ルータへの通信チャネルには、インターネット、Microsoft Azure Express Route、AWS Direct Connect などがあります。

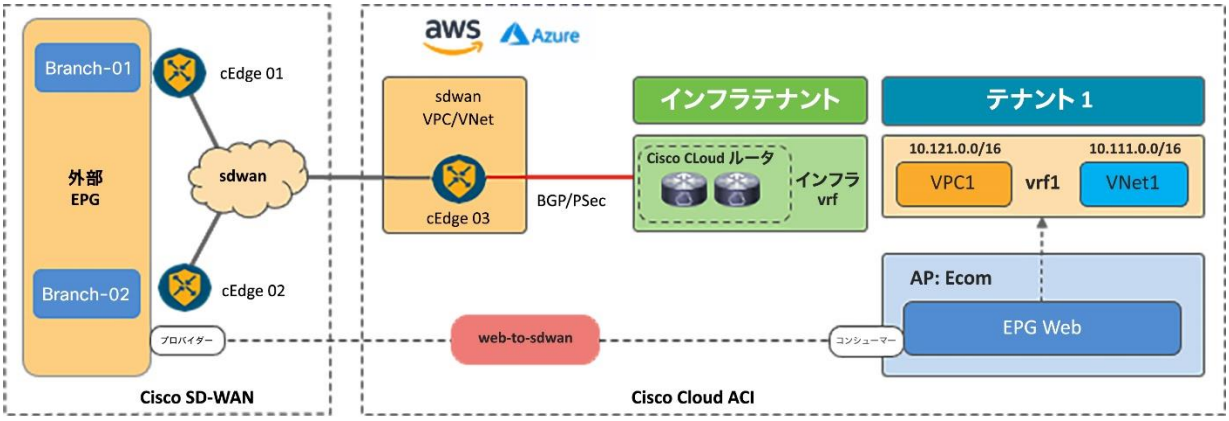

図 52. SD-WAN と Cloud ACI の相互作用

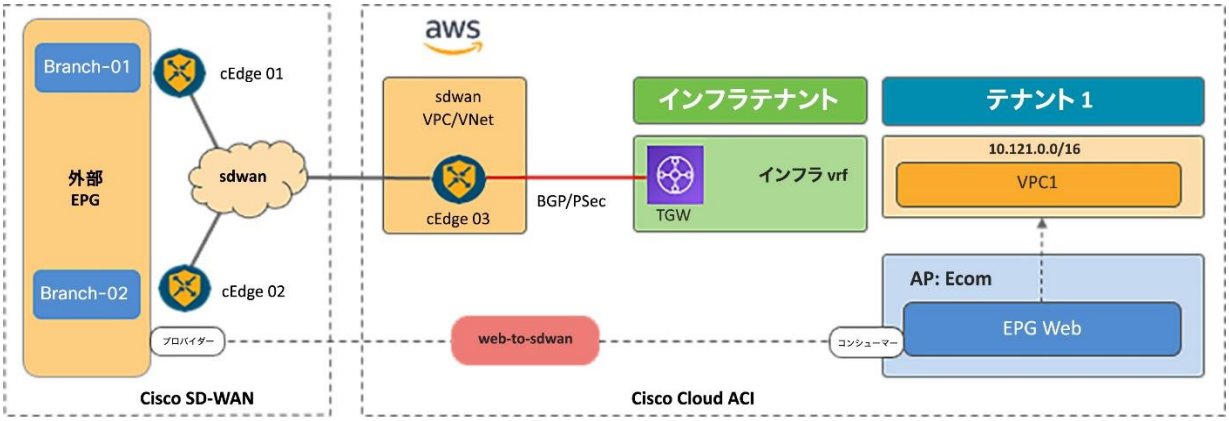

図 53. SD-WAN から AWS TGW への接続

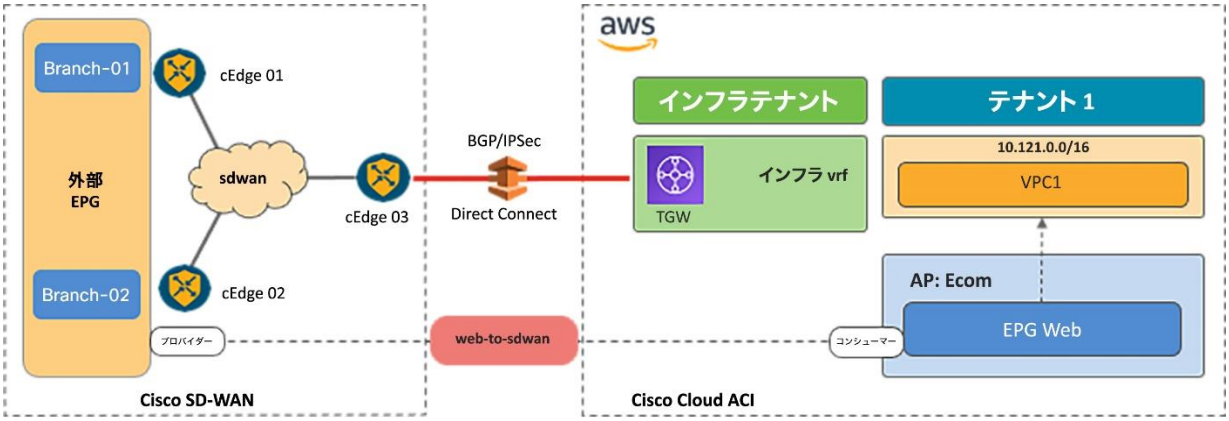

図 54. Direct Connect を介した SD-WAN から AWS TGW への接続

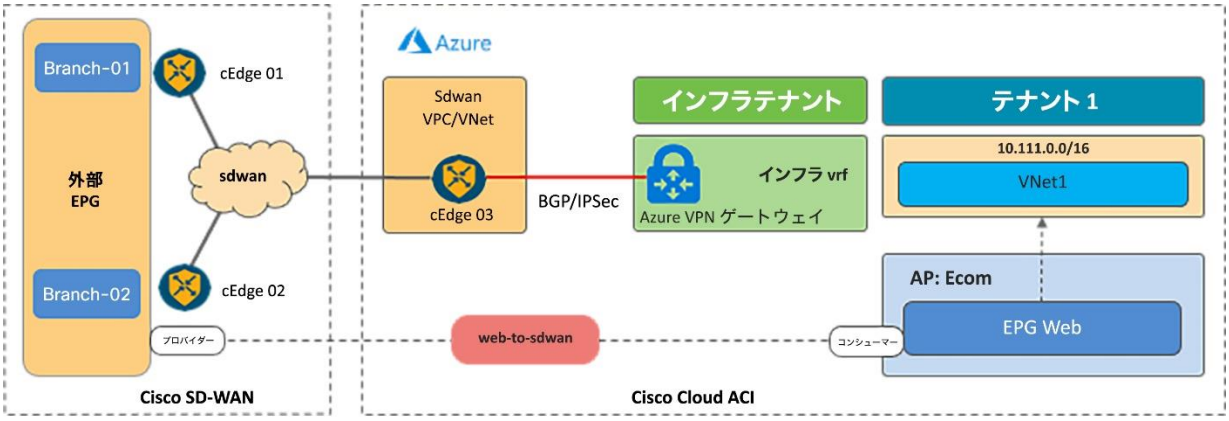

図 55. SD-WAN から Microsoft Azure VPN Gateway への接続

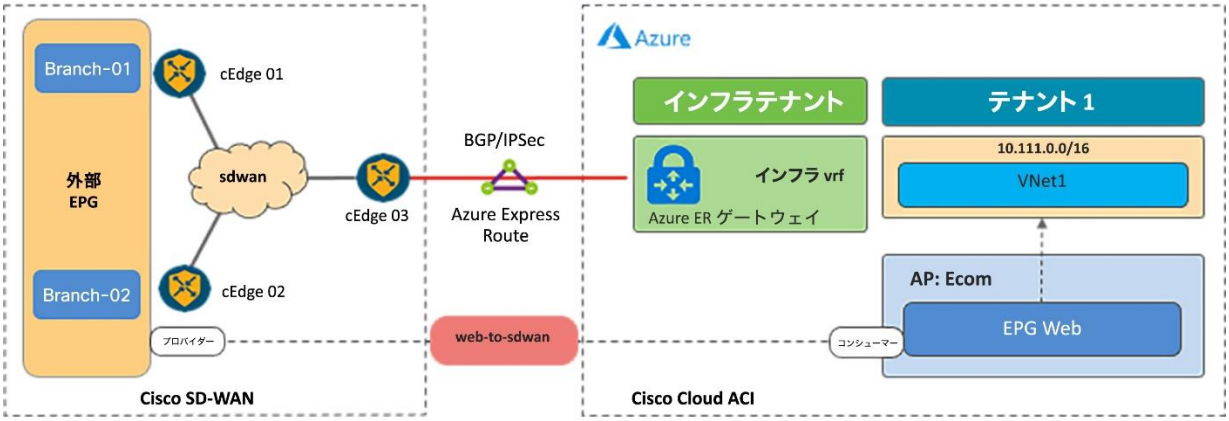

図 56. SD-WAN から Microsoft Azure ExpressRoute Gateway への接続

外部 EPG 分類を微調整して、SD-WAN ブランチネットワークからクラウドワークロードまでのエンドツーエンドのセグメンテーションを行うことができます。このシナリオ例では、branch-01 ネットワークサブネットは外部 EPG1 として分類され、branch-02 ネットワークサブネットは外部 EPG2 として分類されます。個別の外部 EPG を使用することで、ブランチ ネットワーク サブネットに基づいて異なるセキュリティポリシーを適用できます。たとえば、外部 EPG1 とクラウドの EPG1 の間にコントラクトを適用し、外部 EPG2 とクラウドの EPG2 の間に別のコントラクトを適用できます。この構成では、branch-01 はクラウドの EPG1 のワークロードと通信できますが、クラウドの

EPG2 とは通信できません。一方、branch-02 はクラウドの EPG2 のワークロードとは通信できますが、クラウドの EPG1 とは通信できません。コントラクトが適用されている場合、セキュリティポリシーは Cloud APIC によって、AWS では SG ルール、Microsoft Azure では NSG ルールとして、それぞれプログラムされます。

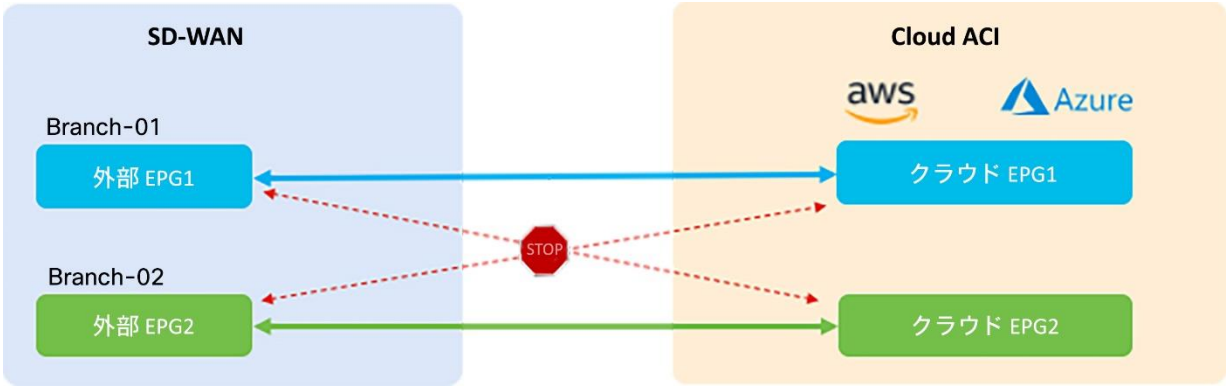

図 57. SD-WAN を介してブランチと Cloud ACI にまたがるエンドツーエンドのセグメンテーション。

このユースケースには、次のガイドラインがあります。

- 現時点では、Cisco SD-WAN コントローラと NDO は独立して動作します。NDO は、Cisco Cloud ルータの構成を自動化し、BGP および IPsec パラメータを含む外部デバイスの構成テンプレートを生成します。Cisco SD-WAN 管理者は、構成テンプレートに基づいて、cEdge デバイスを設定し、Cisco Cloud ルータへの IPsec および BGP セッションを確立できます。
- SD-WAN エッジデバイスと Cisco Cloud ルータの BGP ASN は異なっている必要があります。

ユースケース #7：ロードバランサの挿入

概要

このユースケースでは、ロードバランサが、サービスグラフに伴うコントラクトを使用して EPG 間に挿入されます。Cloud ACI は、AWS および Microsoft Azure が提供するクラウド ネイティブ ロードバランサと、F5 BIG-IP Virtual Edition、Citrix ADC VPX などのサードパーティのロードバランサをサポートします。

次の表は、クラウド ネイティブ ロードバランサとサードパーティ ロードバランサで Cloud ACI がサポートするものの違いをまとめたものです。

表 4. クラウド ネイティブ ロードバランサとサードパーティのロードバランサの比較

	クラウド ネイティブ ロードバランサ	サードパーティのロードバランサ
ロードバランサの作成と構成	Cisco Cloud APIC は、サービスグラフ展開の一部として、ロードバランサを作成および構成します。	サードパーティのロードバランサの作成と構成は、Cisco Cloud APIC の外部で行います。
VIP のターゲットとしてプロバイダーエンドポイントを動的に追加/削除します	はい	いいえ

サポートされているロードバランサ	Cloud ACI では、クラウド ネイティブ ロードバランサは ALB または NLB と呼ばれます。
	• ALB（Application Load Balancer）
	  ○ AWS Application Load Balancer
	  ○ Azure Application Gateway（Standard および Standard_v2 SKUs）
	• NLB（Network Load Balancer）
	  ○ Azure Load Balancer（Standard SKU）
		ロードバランサの種類に制限はありません。
		以下は、ロードバランサインスタンスの例です。
		• F5 BIG-IP Virtual Edition
		• Citrix ADC VPX
		• Radware Alteon VA- ADC
		• A10 vThunder

考慮事項	Cisco Cloud APIC リリース 25.0(2) の時点で、VM Scale セットは Azure を使用した Cloud ACI でのみサポートされています。	サードパーティのロードバランサの挿入は、この記事の執筆時点で、Microsoft Azure を使用した Cloud ACI でのみサポートされています。

2 つの主な違いは、Cisco Cloud APIC はクラウドネットワーキングのルーティングとセキュリティポリシーに加えてクラウド ネイティブ ロードバランサの作成と構成も管理しますが、サードパーティのロードバランサは管理しないことです。Cisco Cloud APIC はサードパーティのロードバランサを構成しないため、ロードバランサの VIP のターゲットとしてプロバイダーエンドポイントを動的に追加または削除する機能は、クラウド ネイティブ ロードバランサでのみ使用できます。

このドキュメントでは、以下で説明するロードバランサ挿入のユースケースについて説明し、各オプションのトラフィックフローと関連する展開の考慮事項について説明します。

- パブリック（外部）ロードバランサ：インターネットなどの外部ネットワークと、同じ VRF の一部であるプロバイダーエンドポイントとの間の垂直方向トラフィックフロー。パブリックロードバランサは、外部向けのパブリック IP アドレスを所有し、クラウドプラットフォームのプロバイダーエンドポイントへのトラフィックを負荷分散します。
- プライベート（内部）ロードバランサ：同じ VRF にあるコンシューマーエンドポイントとプロバイダーエンドポイントの間の水平方向トラフィックフロー。プライベートロードバランサはプライベート IP アドレスを所有し、クラウドプラットフォームのプロバイダーエンドポイントへのトラフィックを負荷分散するために使用されます。ハイブリッドシナリオでは、オンプレミスネットワークからロードバランサのフロントエンドにアクセスできます。

次の図は、パブリックおよびプライベート（内部）ロードバランサを使用した Cloud ACI 設計の例を示しています。

- パブリックロードバランサは、同じテナント内の外部 EPG「internet」と EPG「web」間のコントラクト「external-to-web」に挿入されます。
- プライベートロードバランサは、同じテナント内の EPG「web」と EPG「app」間のコントラクト「web-to-app」に挿入されます。

この図では、プライベートロードバランサに 1 つの VRF（VPC または VNet）を使用していますが、Azure では VNet 間設計もサポートされています。オンプレミスの ACI ファブリックとは異なり、Cloud ACI はロードバランサの設計にトラフィックリダイレクトを使用しないため、前提として、リターントラフィックが接続を開始したクライアントに到達する前にロードバランサに誘導されるように、SNAT を常に有効にする必要があります。

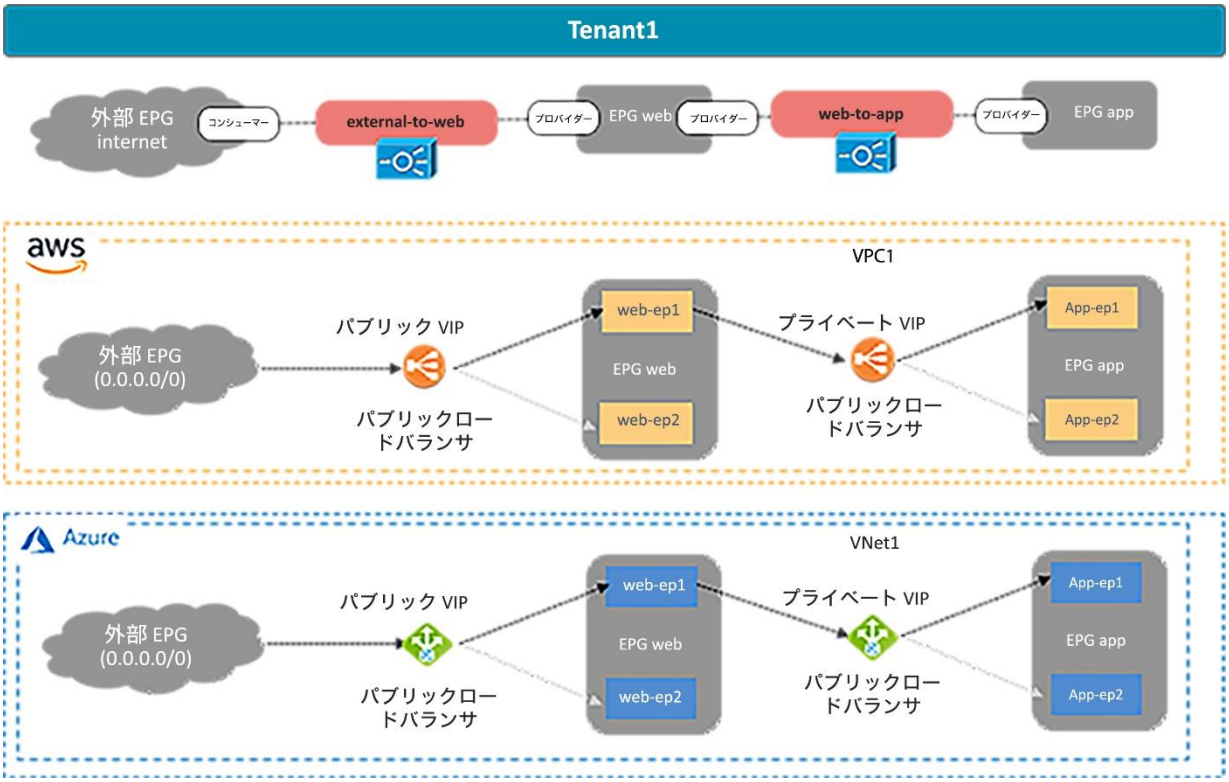

図 58. パブリック（外部）およびプライベート（内部）ロードバランサを備えた Cloud ACI

クラウド ネイティブ ロードバランサのユースケースには、次のガイドラインがあります。

- SNAT は ALB では有効化されていますが、NLB では有効化されていません。
- Cisco Cloud APIC は、Azure Load Balancer（NLB）および Application Gateway（ALB）のバックエンドターゲットとして VM インスタンスと VM スケールセットをサポートしています。VM スケールセットをバックエンドターゲットとして使用するには、Cisco Cloud APIC リリース 25.0(2) 以降が必要です。
- Cisco Cloud APIC は、AWS Application Load Balancer（ALB）のバックエンドターゲットとして Amazon EC2 インスタンスをサポートしています。現時点では、Auto Scaling グループはサポートされていません。
- AWS ALB：コンシューマーとプロバイダーの EPG は、同じ VPC にある必要があります。ALB は、ターゲット EC2 インスタンスが存在する同じ VPC の 2 つのアベイラビリティゾーンに関連付けられています。アベイラビリティゾーンごとに、ALB のアベイラビリティゾーンで 1 つのサブネットを選択する必要があり、そのサブネットは、TGW VPC のアタッチメントに使用されるサブネットであってはなりません。（Transit Gateway の設計プラクティスの推奨事項に基づいて、Cloud ACI では、VPC を Transit Gateway にアタッチするために、アベイラビリティゾーンごとに 1 つの専用ゲートウェイサブネットが必要です。）下の図 46 は、シナリオの例を示しています。
- Azure NLB：NLB とそのターゲット（プロバイダー EPG）は、同じ VNet 内にある必要があります。NLB は専用サブネットにある必要があります。
- Azure ALB：ALB は、コンシューマーとプロバイダーから到達可能なハブ VNet またはプロバイダー VNet のいずれかにある必要があります。ALB は専用サブネットにある必要があります。

- 動的 IP または静的 IP の割り当て
    - パブリックおよびプライベート/内部 AWS ロードバランサ（Azure ALB）：
        - 動的 IP が使用されます。
    - パブリック Azure Application Gateway（Azure ALB）：
        - Standard V1 の場合、動的パブリック IP が使用されます。
        - Standard V2 の場合、静的パブリック IP が使用されます。
    - プライベート/内部 Azure Application Gateway（Azure ALB）：
        - Standard V1 の場合、Azure が静的および動的プライベート IP の両方をサポートしているため、両方がサポートされます。
        - Standard V2 の場合、Azure が Standard V2 の動的プライベート IP をサポートしていないため、静的プライベート IP のみがサポートされます。
- 現時点では、サイト間トラフィックはサポートされていません。次に例を示します。
    - コンシューマーが AWS サイトにあり、プロバイダーが Microsoft Azure サイトにある場合。
    - コンシューマーが ACI オンプレミスサイトにあり、プロバイダーが Microsoft Azure サイトにある場合。

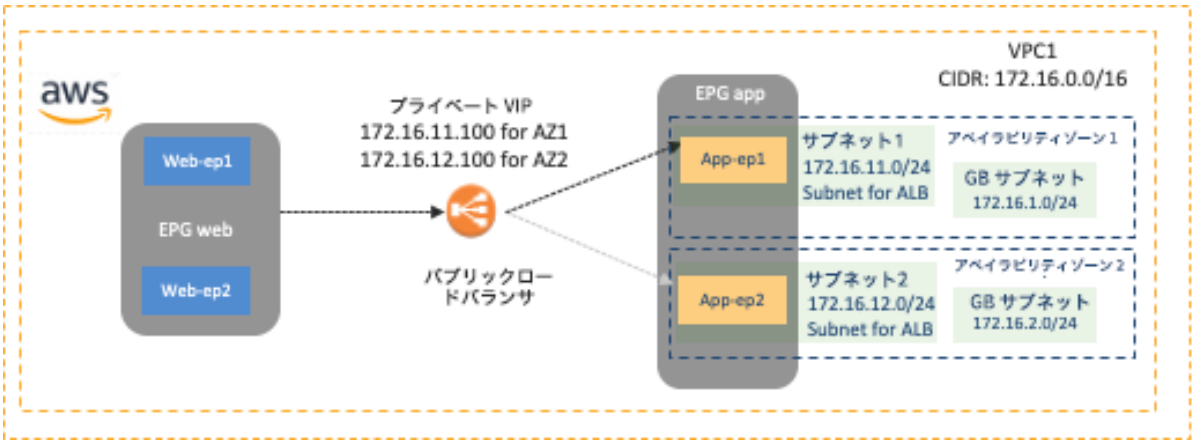

図 59. AWS ALB のアベイラビリティゾーンとサブネット

サードパーティのロードバランサのユースケースには、次のガイドラインがあります。

- 現時点では、Cloud ACI は Microsoft Azure でのサードパーティのロードバランサの挿入のみをサポートしています。
- サードパーティのロードバランサは、コンシューマーとプロバイダーから到達可能なハブ VNet またはプロバイダー VNet にある必要があります。
- サードパーティのロードバランサで SNAT を有効にする必要があります（現時点では、リターントラフィックのトラフィックリダイレクトはサポートされていません）。
- サードパーティのロードバランサは、次の設計オプションをサポートしていません。

- ワンアーム モード
- リダイレクション
- DSR（Direct Server return）
- ロードバランサ インターフェイス サブネットの外部にあるエイリアン VIP 範囲。
- アクティブ-スタンバイ HA

- 現時点では、サイト間トラフィックはサポートされていません。次に例を示します。
  - コンシューマーが AWS サイトにあり、プロバイダーが Microsoft Azure サイトにある場合。
  - コンシューマーが ACI オンプレミスサイトにあり、プロバイダーが Microsoft Azure サイトにある場合。

特に明記されていない限り、次のサブセクションでは、SNAT を備えた Azure Application Gateway を使用した Azure での Cloud ACI を例として使用します。

ユースケース #7-1：パブリック（外部）ロードバランサ

次の図は、パブリックロードバランサを使用した Cloud ACI 設計の例を示しています。この設計の一般的なユースケースは、インターネットなどの外部ネットワークに公開されるパブリックサービスです。この例では、外部 EPG がコンシューマーであり、クラウド EPG 「Web」がコントラクトのプロバイダーです。ロードバランサのインターフェイスは 1 つです。コンシューマーから VIP へのトラフィックは、ロードバランサに着信します。ロードバランサが送信元と接続先の IP アドレスを変更した後、トラフィックはクラウド EPG 「Web」のエンドポイントの 1 つに転送されます。リターントラフィックは、NAT された IP アドレスを所有するロードバランサに戻ります。ロードバランサが送信元と接続先の IP アドレスを変更すると、トラフィックは外部エンドポイントに転送されます。

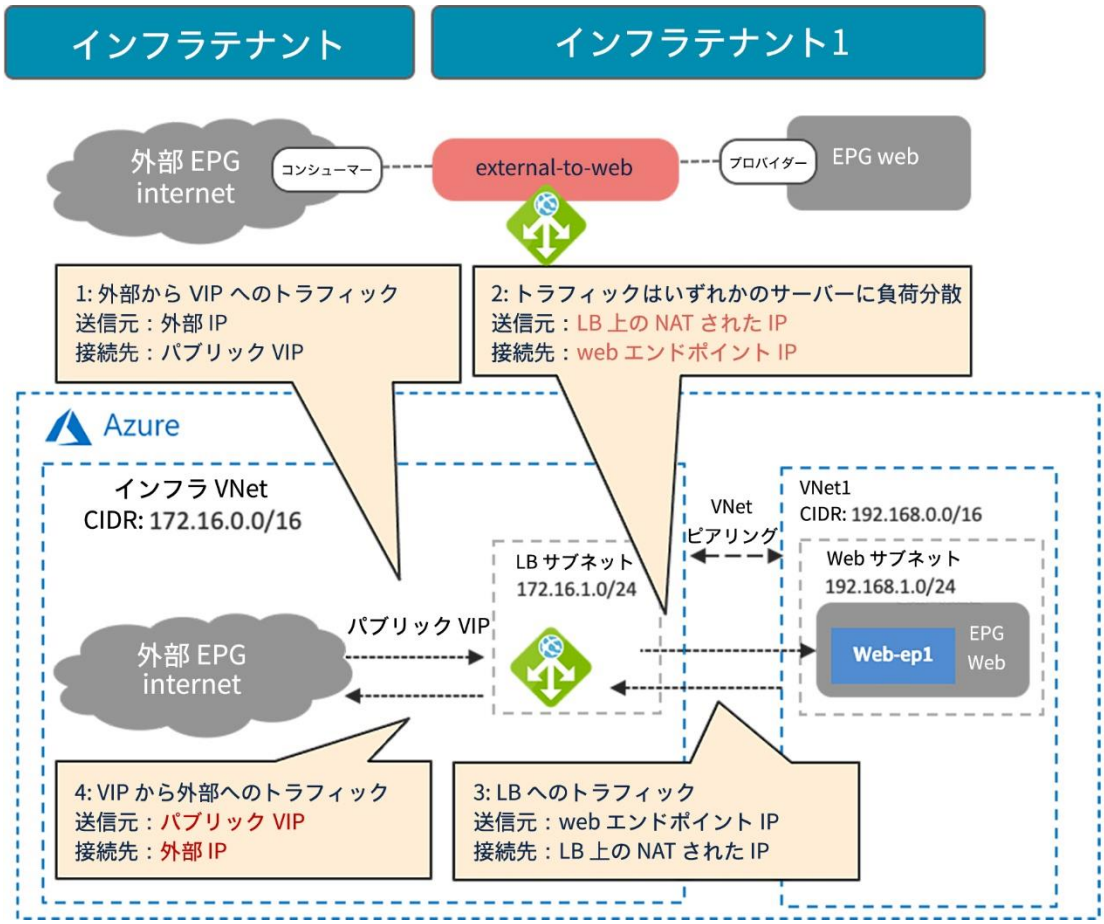

図 60. パブリック（外部）ロードバランサを使用した Cloud ACI

前のサブセクションのロードバランサの挿入に関する考慮事項で提供されたガイドラインに加えて、このユースケースには次のガイドラインがあります。

- この例ではインフラ VNet でロードバランサを使用していますが、Azure を使用した Cloud ACI では、次のような他の組み合わせもサポートされています。
    - インフラ VNet 内のコンシューマー外部 EPG、ロードバランサ、プロバイダークラウド EPG。
    - インフラ VNet 内のコンシューマー外部 EPG とロードバランサ、ユーザー VNet 内のプロバイダークラウド EPG。
    - インフラ VNet 内のコンシューマー外部 EPG、ユーザー VNet 内のロードバランサおよびプロバイダークラウド EPG。
- ALB を使用した AWS での Cloud ACI は、VPC 内設計のみをサポートします。つまり、コンシューマー、ロードバランサ（ALB）、プロバイダーは同じ VPC に存在する必要があります。

ユースケース #7-2：プライベート（内部）ロードバランサ

次の図は、プライベートロードバランサを使用した Cloud ACI 設計の例を示しています。この設計の一般的なユースケースは、他のプライベートネットワークに公開されるサービスです。この例では、クラウド EPG 「Web」がコンシューマーであり、クラウド EPG 「App」がコントラクトのプロバイダーです。ロードバランサのインターフェイスは 1 つです。コンシューマーから VIP へのトラフィックは、ロードバランサに着信します。ロードバランサが送信元と接続先の IP アドレスを変更した後、トラフィックはクラウド EPG 「App」のエンドポイントの 1 つに

転送されます。リターントラフィックは、NAT された IP アドレスを所有するロードバランサに戻ります。ロードバランサが送信元と接続先の IP アドレスを変更すると、トラフィックは外部エンドポイントに転送されます。

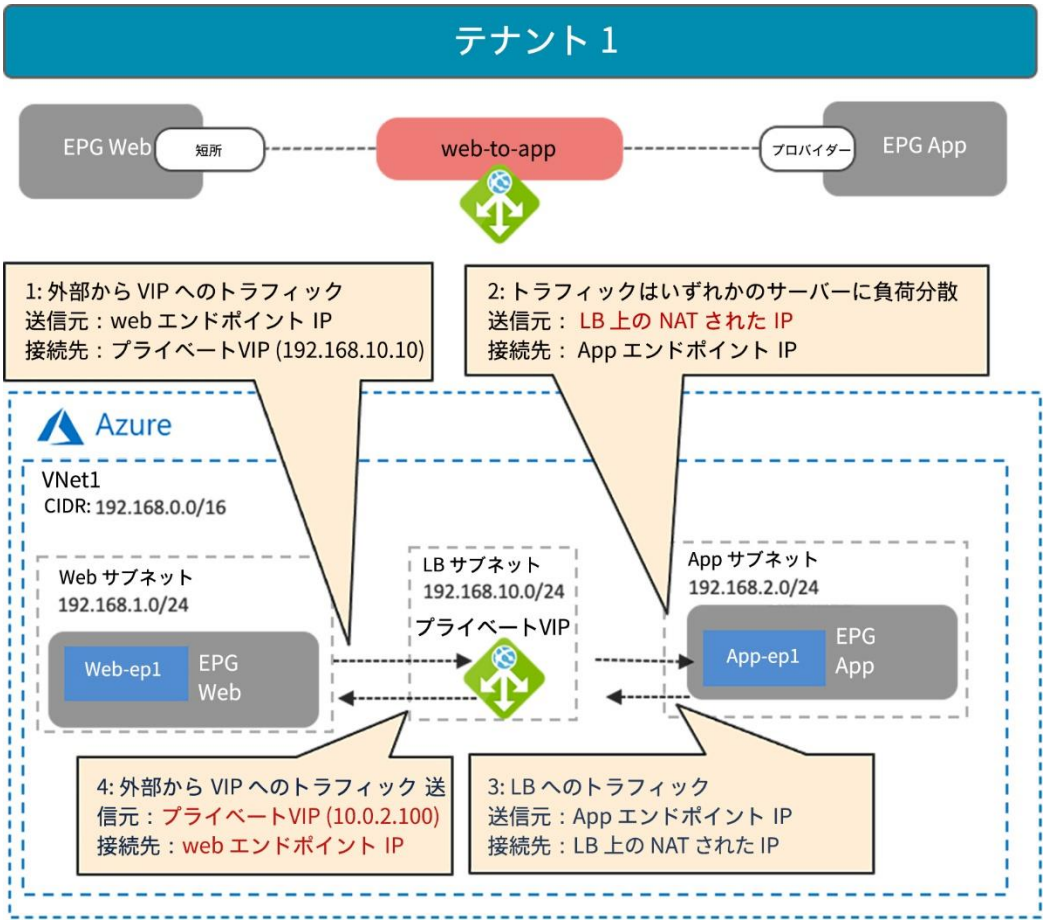

図 61. プライベート（内部）ロードバランサを備えた Cloud ACI

前のサブセクションのロードバランサの挿入に関する考慮事項で提供されたガイドラインに加えて、このユースケースには次のガイドラインがあります。

- この例では VNet 内設計を使用していますが、Azure を使用した Cloud ACI では、次のような他の組み合わせもサポートされています。
    - 同じ VNet 内のコンシューマークラウド EPG、ロードバランサ、プロバイダークラウド EPG。
    - コンシューマー VNet のコンシューマークラウド EPG、プロバイダー VNet のロードバランサおよびプロバイダークラウド EPG。
    - コンシューマー VNet のコンシューマークラウド EPG、インフラ VNet のロードバランサ、プロバイダー VNet のプロバイダークラウド EPG。
- ALB を使用した AWS での Cloud ACI は、VPC 内設計のみをサポートします。つまり、コンシューマー、ロードバランサ（ALB）、プロバイダーは同じ VPC に存在する必要があります。

ユースケース #8：ファイアウォールの挿入

概要

このユースケースでは、サービスグラフに伴うコントラクトを使用した EPG 間のファイアウォール挿入について説明します。現時点では、これは Microsoft Azure を使用した Cloud ACI でのみサポートされています。Cloud ACI は、Cisco Adaptive Security Virtual Appliance（ASAv）、Cisco Firepower NGFW Virtual（NGFWv）などのサードパーティ ファイアウォールをサポートしています。Azure Firewall や Azure Web Application Firewall（WAF）などのクラウド ネイティブ セキュリティ サービスは、現在サポートされていません。

Cisco Cloud APIC は、ルーティングとセキュリティポリシーを管理して、クラウドネットワーキングにファイアウォールを挿入します。ただし、Cisco Cloud APIC はサードパーティのファイアウォールを管理しません（Cisco Cloud APIC がサードパーティのロードバランサを管理しないのと同様です）。トラフィックをファイアウォールにリダイレクトするために、Cisco Cloud APIC は、サービスグラフを使用するコントラクトに基づいて UDR（ユーザー定義ルート）を構成します。

このセクションでは、以下で説明するファイアウォール挿入のユースケースについて説明し、各オプションのトラフィックフローと関連する展開の考慮事項について説明します。

- NAT を使用したファイアウォールの挿入：クラウドエンドポイントによって開始された外部ネットワークへの垂直方向トラフィックフロー。ファイアウォールは、クラウドエンドポイントのプライベート IP アドレスをパブリック IP アドレスに変換します。
- NAT を使用しないファイアウォール挿入：異なる VRF にあるコンシューマーエンドポイントとプロバイダーエンドポイントの間の水平方向トラフィックフロー。

次の図は、ファイアウォールを使用した Cloud ACI 設計の例を示しています。垂直方向ファイアウォールは、外部 EPG「internet」と EPG 「Web」間のコントラクト「external-to-web」に挿入されます。トラフィックリダイレクトは、外部サイトへのトラフィックに対してのみ有効になっています。水平方向ファイアウォールは、EPG「Web」と EPG 「App」間のコントラクト「web-to-app」に挿入されます。トラフィックのリダイレクトは両方向で有効になっています。

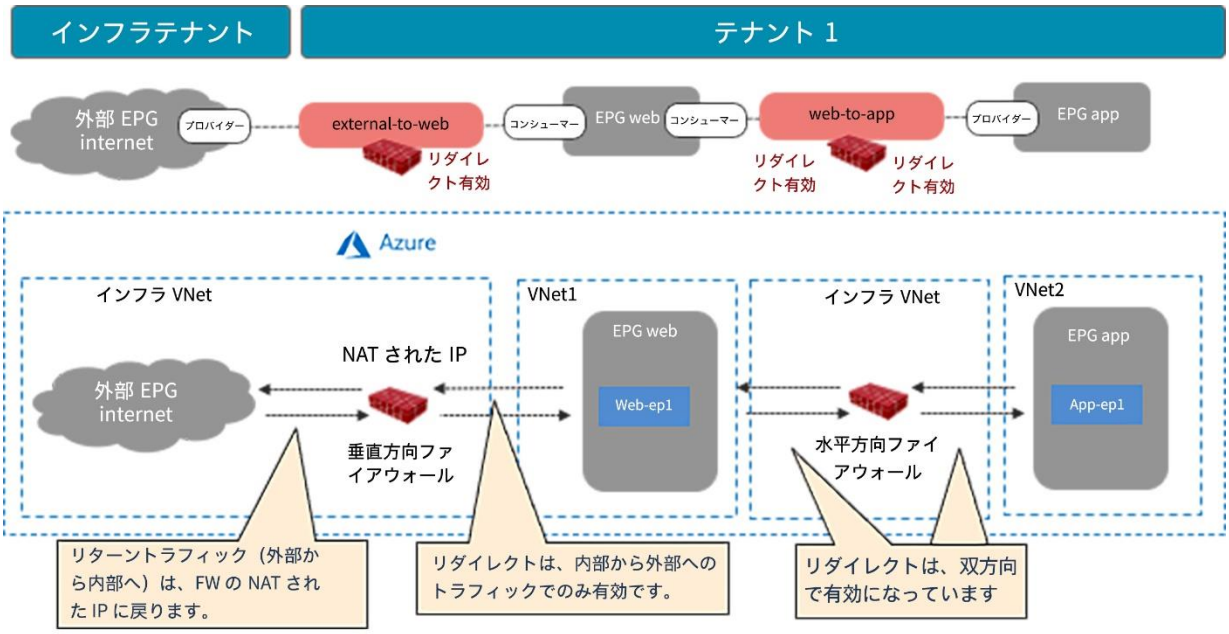

図 62. ファイアウォールを備えた Cloud ACI

ファイアウォールの挿入には、次のガイドラインがあります。

- VNet 間トラフィックの場合、VNet ピアリングが必要です。
- リダイレクトの接続先（この例ではファイアウォール インターフェイスの IP アドレス）は、ハブ VNet（インフラ VNet）内にある必要があります。
- ファイアウォール インターフェイスは、クラウド EPG が存在するサブネットとは異なる専用サブネットにある必要があります。
- 現時点では、サイト間トラフィックはサポートされていません。次に例を示します。
    - コンシューマーが AWS サイトにあり、プロバイダーが Microsoft Azure サイトにある場合。
    - コンシューマーが ACI オンプレミスサイトにあり、プロバイダーが Microsoft Azure サイトにある場合。

このセクションでは例として単一ノードのファイアウォールについて説明しますが、高可用性のために複数のファイアウォールを使用することをお勧めします。ロードバランサを使用してトラフィックを複数のファイアウォールに分散させる方法については、マルチノードサービスの挿入セクションで説明します。

ユースケース #8-1：垂直方向ファイアウォールの挿入：NAT を使用した内部から外部へのトラフィック
次の図は、NAT でファイアウォールを挿入した Cloud ACI 設計の例を示しています。この設計の一般的なユースケースは、クラウドエンドポイントがインターネットからソフトウェアアップデートをダウンロードするなど、クラウドエンドポイントによって外部ネットワークに対して開始される通信です。この例では、外部 EPG「Internet」がコントラクトのプロバイダーであり、クラウド EPG「Web」がコントラクトのコンシューマーです。ファイアウォールには、異なるサブネットに「FW-External」と「FW-Web」という 2 つのインターフェイスがあります。コンシューマー（Web）からプロバイダー（Internet）へのトラフィックは、ファイアウォールの「FW-Web」インターフェイスにリダイレクトされ、ファイアウォールは「FW-External」インターフェイスを介してトラフィックを外部ネットワークに送信します。ファイアウォール上の送信元 NAT（SNAT）のため、リターントラフィックは、NAT された IP アドレスを所有するファイアウォール信頼インターフェイスに戻ります。

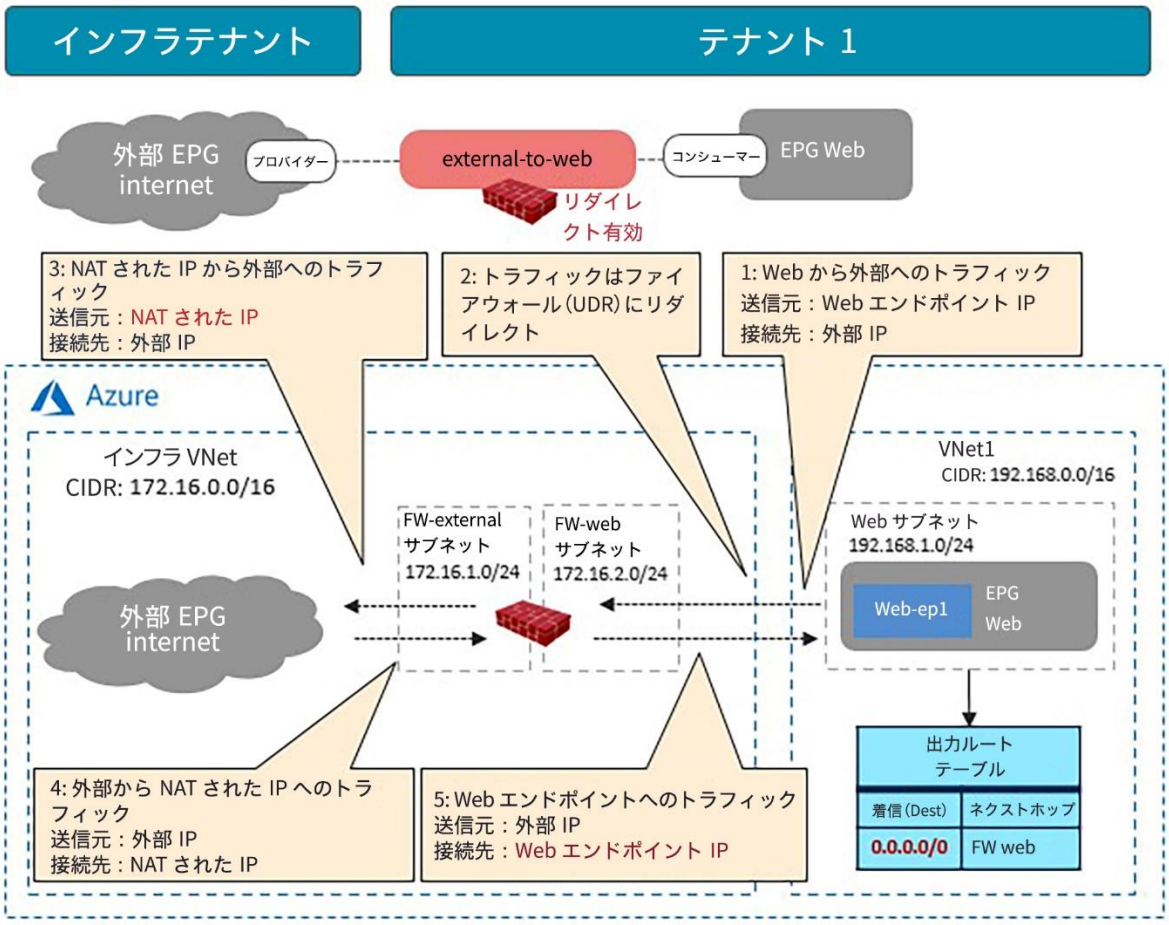

図 63. 垂直方向ファイアウォールの挿入：NAT を使用した内部から外部へのトラフィック

コントラクトを伴うサービスグラフ展開の一環として、Cisco Cloud APIC は、Web サブネットと外部 EPG サブネット間の通信でトラフィックをファイアウォールにリダイレクトする出力ルートテーブルを作成します。この例では、Web サブネット（192.168.1.0/24）は、FW-Web サブネット内のファイアウォールの IP アドレスを次のホップとして使用して、外部ネットワーク（0.0.0.0/0）に到達します。NSG もそれに応じて更新されます。

前のサブセクションのファイアウォールの挿入に関する考慮事項で提供されたガイドラインに加えて、このユースケースには次のガイドラインがあります。

- 外部 EPG とコンシューマー EPG は、同じ VNet または異なる VNet に配置できます。
- 外部から内部（垂直型）のトラフィック方向の場合、非 ACI ネットワーク（ExpressRoute 経由の外部 EPG）から Microsoft Azure サイトのクラウドエンドポイントへのトラフィックであれば、リダイレクトがサポートされます。詳細については、「垂直方向トラフィックフローの NLB-FW 挿入」を参照してください。
- 同じ外部ネットワークに接続しているがリダイレクトを必要としない別のクラウド EPG がある場合、そのサブネットは、リダイレクトを必要とするクラウド EPG のサブネットとは異なる CIDR にある必要がある場合があります。詳細については、サードパーティ ファイアウォールの管理ネットワークに関する考慮事項セクションを参照してください。

ユースケース #8-2：水平方向ファイアウォールの挿入：NAT を使用しないスポーク間トラフィック

次の図は、NAT なしでファイアウォールを挿入する Cloud ACI 設計の例を示しています。この例では、クラウド EPG 「Web」がコンシューマーであり、クラウド EPG 「App」がコントラクトのプロバイダーです。ファイアウォールには、異なるサブネットにある信頼と非信頼の 2 つのインターフェイスがあります。リダイレクトは両方で有効になっています。

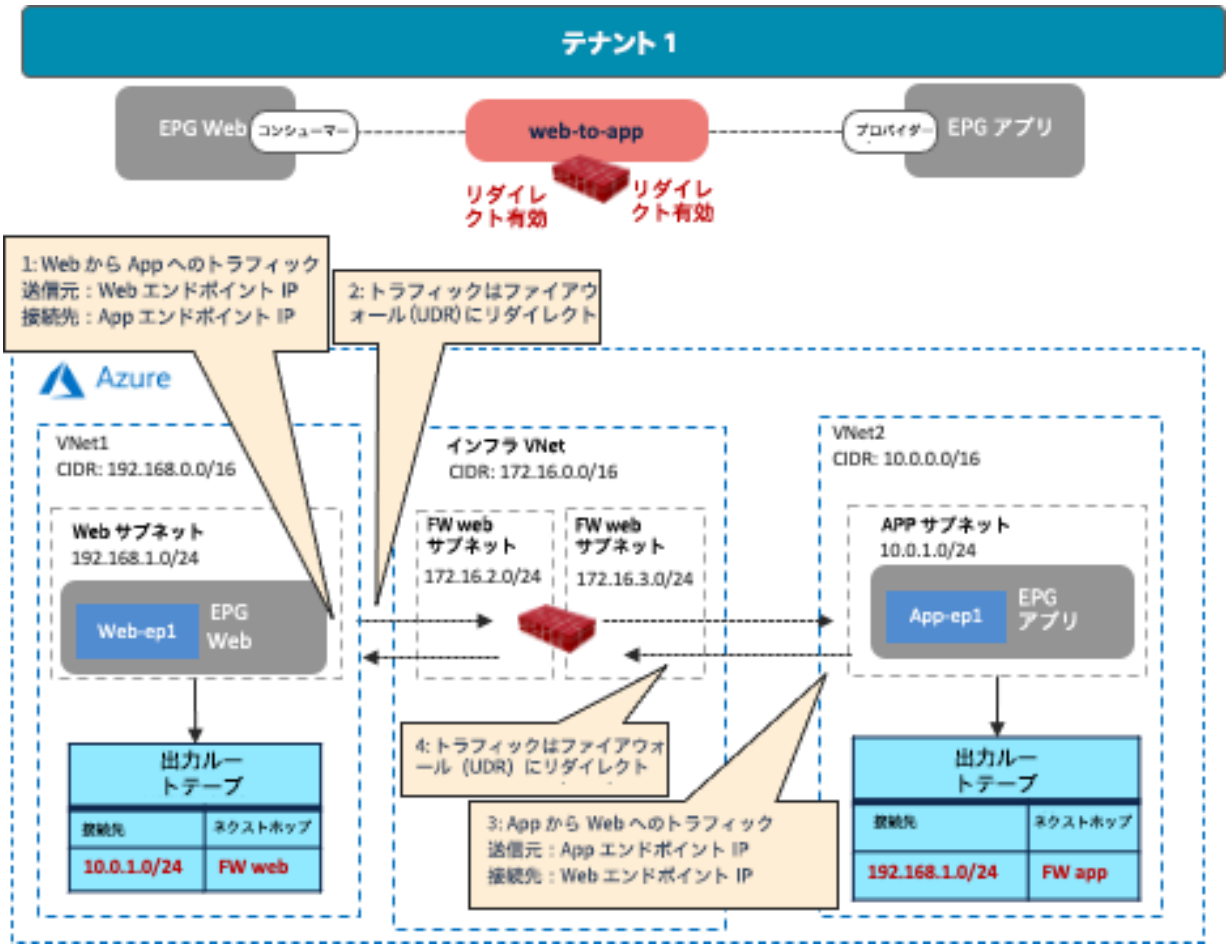

図 64. 水平方向ファイアウォールの挿入：NAT を使用しないスポーク間トラフィック

コントラクトを使用するサービスグラフ展開の一部として、Cisco Cloud APIC は両方向の出力ルートテーブルを作成します。

- 1 つは、トラフィックを Web サブネットから App サブネットにリダイレクトし、次に FW-Web サブネットのファイアウォール IP アドレスにリダイレクトします。
- もう 1 つは、トラフィックを App サブネットから Web サブネットにリダイレクトし、次に FW-App サブネットのファイアウォール IP アドレスにリダイレクトします。

NSG も更新され、コンシューマーサブネットからプロバイダーサブネットへのトラフィックを許可します。そのため、明示的な許可ルールがない場合でも、プロバイダーからコンシューマーへのリターントラフィックは自動的に許可されます。

前のサブセクションのファイアウォールの挿入に関する考慮事項で提供されたガイドラインに加えて、このユースケースには次のガイドラインがあります。

- 同じリージョンに展開されたコンシューマーとプロバイダーの EPG は、同じ VNet の一部にすることはできません。

サービスの挿入に関する一般的な考慮事項

このセクションでは、ファイアウォールとロードバランサの両方に適用される、サービス挿入に関する次の一般的な設計上の考慮事項について説明します。

- サードパーティ アプライアンスの管理ネットワークに関する考慮事項
- ハブ VNet（overlay-1）のサブネット内のサービスアプライアンス

サードパーティ アプライアンスの管理ネットワークに関する考慮事項

このサブセクションでは、例としてサードパーティ ファイアウォールを使用するサードパーティ アプライアンスの管理ネットワークの設計上の考慮事項について説明します。

これらの例では、ファイアウォールの管理インターフェイスは、コントラクトのプロバイダーであるクラウド EPG「FW-mgmt」の一部であり、EPG または外部 EPG がコンシューマーです。この場合、Cloud ACI コントラクトは、コンシューマーからプロバイダーへのトラフィックのみに対する許可ルールを作成するため、ファイアウォールによって発信されコンシューマーに向かうトラフィックは許可されません。プロバイダーからコンシューマーへのリターントラフィックは、（明示的な許可ルールがない場合でも）自動的に許可されます。これは、コンシューマーからプロバイダーへのトラフィックが以前に監視されているためです。したがって、サービスデバイスの管理インターフェイスが別の EPG との通信を開始する可能性がある場合、両方の EPG がコントラクトのコンシューマーであり、プロバイダーである必要があります。この考慮事項は、このセクションの両方の例に適用できますが、例ではプロバイダー EPG としてクラウド EPG 「FW-mgmt」を使用します。

オンプレミス ACI ファブリックから管理ネットワークへのアクセス

次の図は、設計例を示しています。オンプレミスの ACI ファブリックとクラウドのファイアウォールの管理インターフェイス間のトラフィックを許可するために、ファイアウォールの管理インターフェイス用に EPG「Client-mgmt」とクラウド EPG「FW-mgmt」の間でコントラクトが構成されます。論理設計は、「ユースケース #2：ユースケース #2：複数のサイトにまたがるアプリケーション（テナント間共有サービス）」に似ています。この例では EPG 間の VRF 間コントラクトを使用しますが、代わりに VRF 内コントラクトにすることもでき、またクライアントは通常の EPG ではなくオンプレミスの外部 EPG にすることもできます。

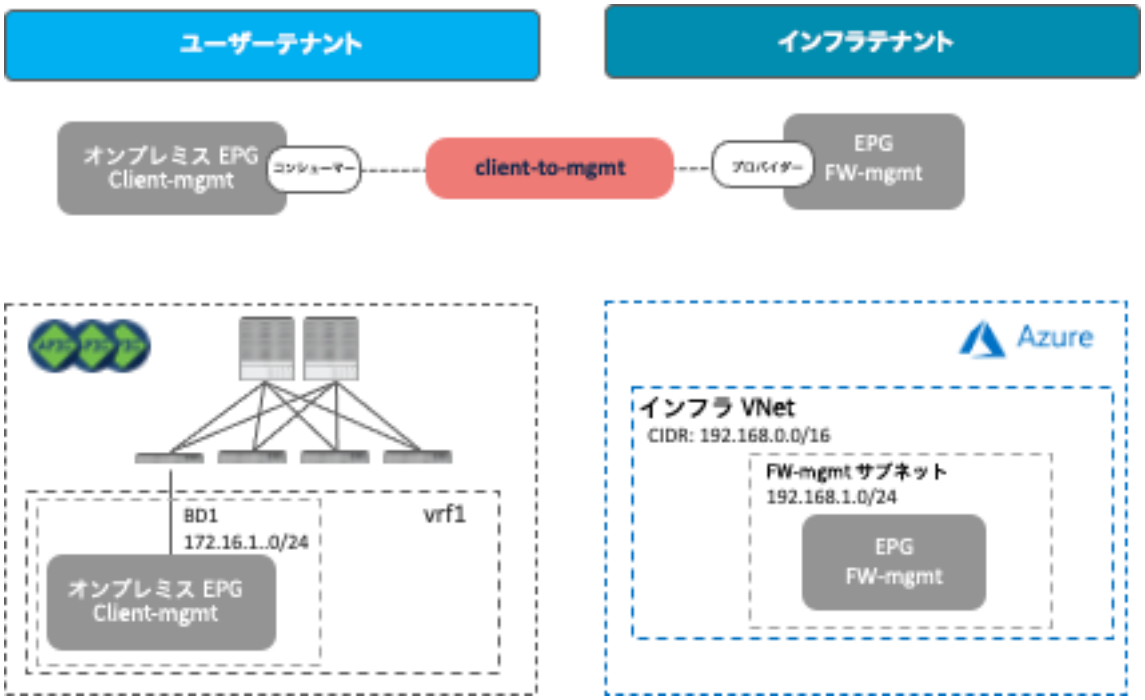

図 65. オンプレミス ACI のクライアントとサードパーティ アプライアンスの管理インターフェイス間のトラフィックを許可する

外部ネットワークから管理ネットワークへのアクセス

このシナリオは、Microsoft Azure を使用する Cloud ACI で利用可能なリダイレクト機能に適用できます。次の図は、設計例を示しています。外部ネットワークとファイアウォールの管理インターフェイス間のトラフィックを許可するために、ファイアウォールの管理インターフェイス用に外部 EPG とクラウド EPG「FW-mgmt」の間でコントラクトが構成されます。

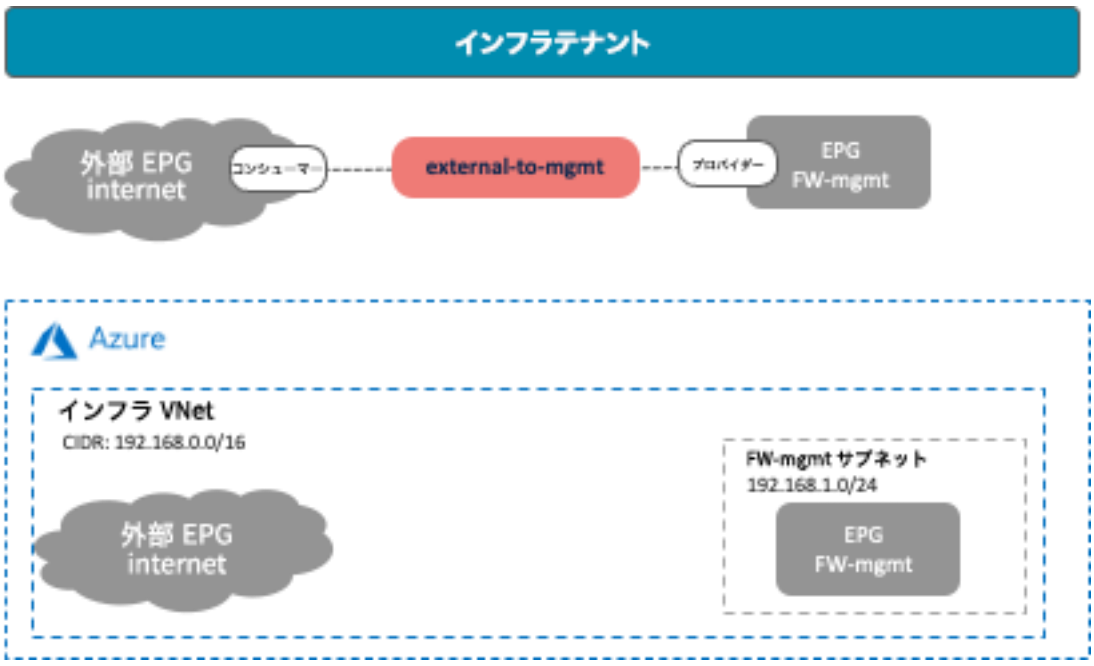

図 66. 外部ネットワークとサードパーティ アプライアンスの管理インターフェイス間のトラフィックを許可する

外部 EPG と、クラウド EPG FW-mgmt と同じ CIDR に展開されているクラウド EPG（以下の例では EPG「Web」）との間のトラフィックに対してリダイレクトが有効になっている場合、他のクラウド EPG コントラクト（以下の例では「external-to-web」コントラクト）用に Cisco Cloud APIC によって構成された出力ルートテーブルのために、FW-mgmt サブネットからのトラフィックもリダイレクトされます。リダイレクトを伴うサービスグラフ展開の一部として、Cisco Cloud APIC は、以下に示すように、サービス デバイス インターフェイスのサブネットを除き、CIDR 内のすべてのサブネットからファイアウォールにトラフィックをリダイレクトする出力ルートテーブルを作成します。この状況では、外部ネットワークからクラウド EPG FW-mgmt への接続が失われる可能性があります。

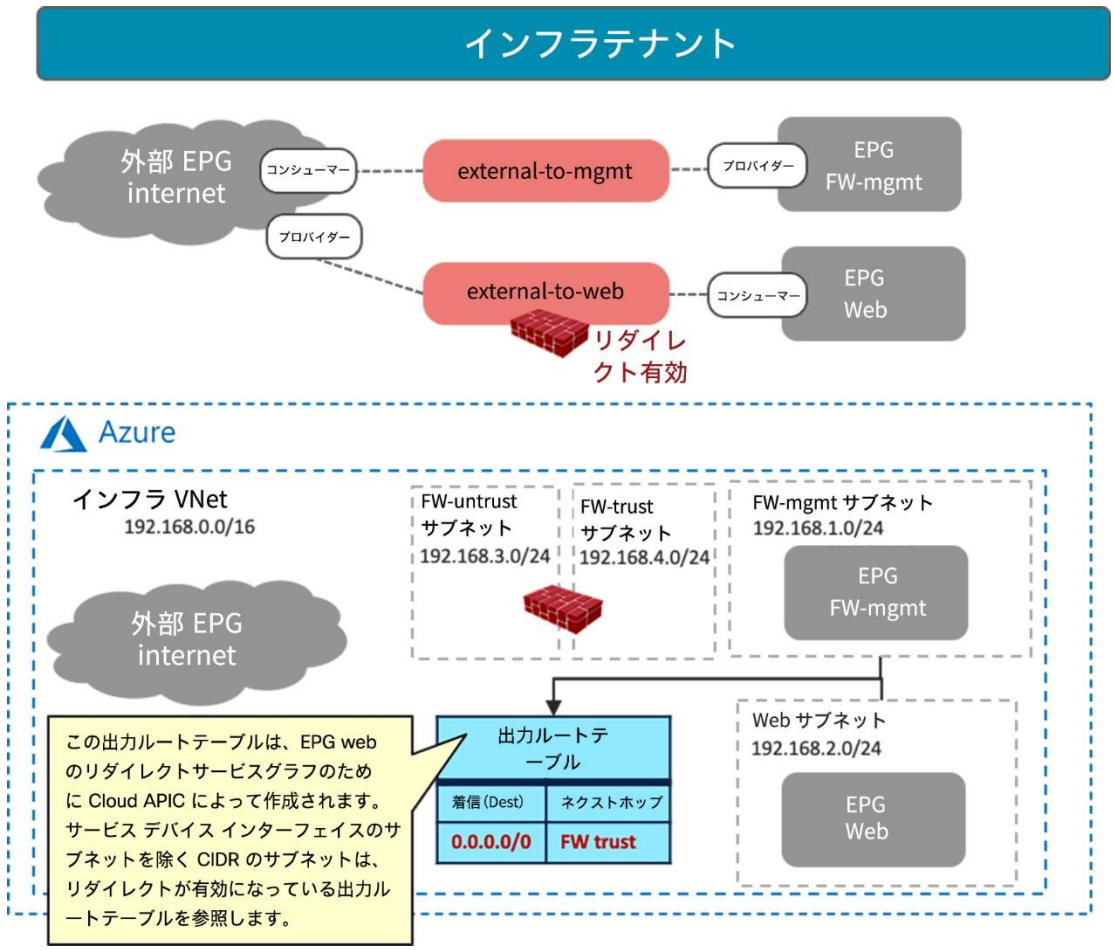

図 67. FW-mgmt サブネットと Web サブネットの両方がリダイレクトに出力ルートテーブルを参照

その場合、クラウド EPG「FW-mgmt」のファイアウォールの管理インターフェイスにアクセスするには、別の CIDR のジャンプホストを使用する必要があります。次の図で、構成例について説明します。クラウド EPG「Jump-host」は、クラウド EPG 「Web」とは異なる CIDR にある「Jump-subnet」にあります。CIDR が異なるため、「Jump-host」サブネットは、ファイアウォール挿入のリダイレクトを使用した出力ルートテーブルを参照しません。出力ルートテーブルと、それに応じた「FW-mgmt」と「Jump-host」間のコントラクトを追加することで、管理者はジャンプホスト VM にアクセスし、その後ジャンプホスト VM からファイアウォールの管理インターフェイスにアクセスできます。

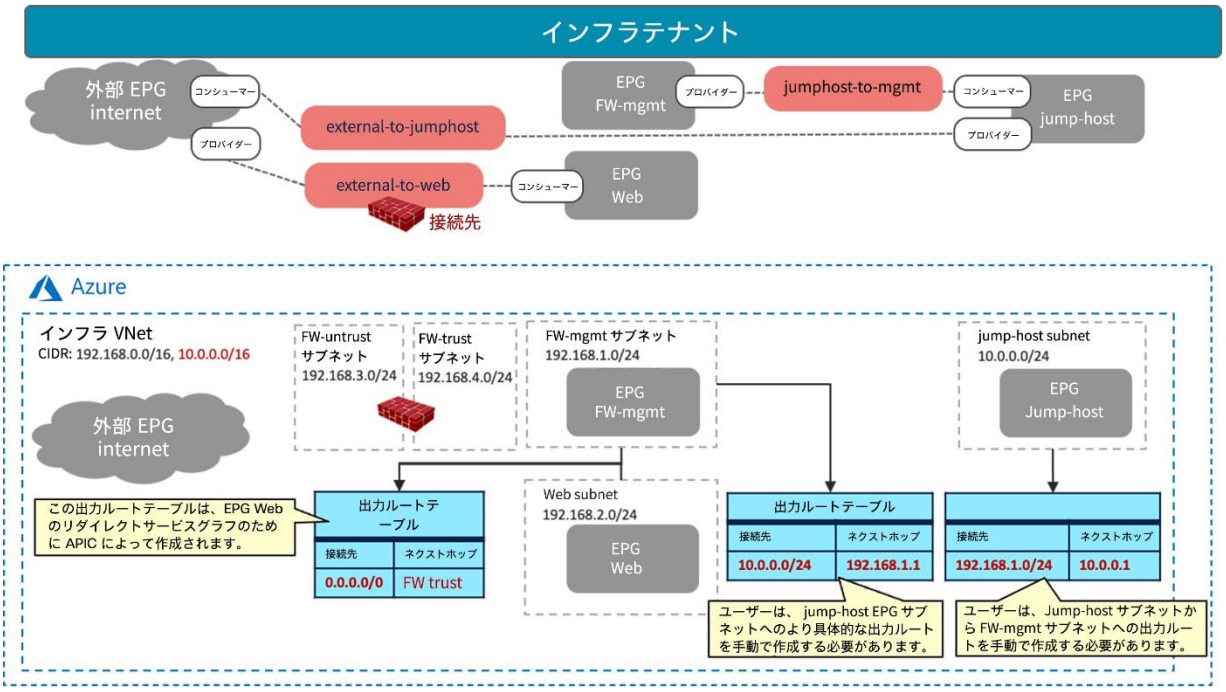

図 68. 異なる CIDR でのジャンプホストの使用

ハブ VNet（overlay-1）のサブネット内のサービスアプライアンス

このサブセクションでは、ハブ VNet に CIDR とサブネットを追加するシナリオについて説明します。これらの CIDR とサブネットは、サービスアプライアンスに使用できます。このシナリオは、Microsoft Azure を使用する Cloud ACI にのみ適用されます。

Azure ポータルの overlay-1 VNet（「インフラ VNet」または「ハブ VNet」とも呼ばれます）は、Cisco Cloud APIC によって作成され、Cisco Cloud ルータおよび Cisco Cloud ルータのロードバランシング用の NLB を展開します。

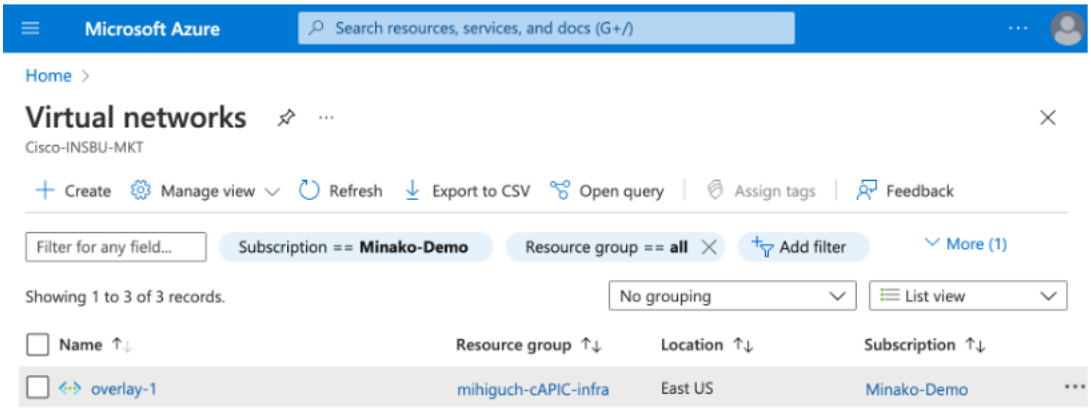

図 69. Azure ポータル上の overlay-1 VNet

ハブ VNet にサービスアプライアンスを追加する必要がある場合は、以下のいずれかのオプションを使用して、新しい CIDR とサブネットをハブ VNet に追加する必要があります。

Cisco Cloud APIC リリース 25.0(2) より前は、Cisco Cloud APIC は、インフラ VNet に 2 つのオブジェクト、overlay-1 と overlay-2 を内部的に作成していました。

- overlay-1 の CIDR は、Cisco Cloud ルータと、Cloud ACI の必須コンポーネントである Cisco Cloud ルータロードバランシングの NLB を展開するために使用されます。
- overlay-2 の CIDR は、ユーザー定義のサービスアプライアンスの展開に使用できます。overlay-2 に新しい CIDR とサブネットを追加できます。

次の図で、構成例について説明します。

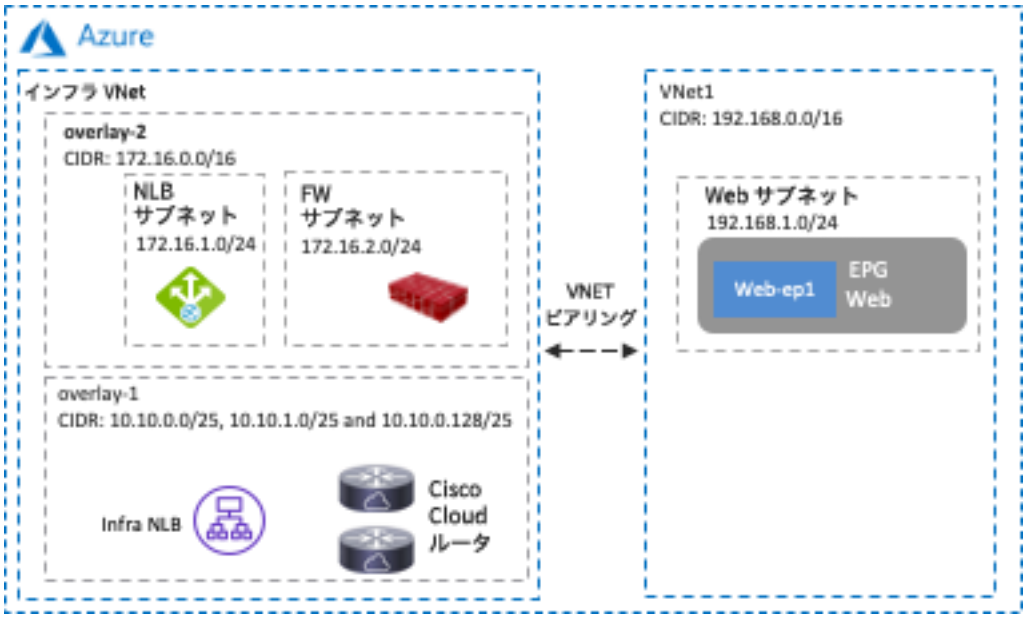

図 70. overlay-2 の新しい CIDR のサービスアプライアンス

Cisco Cloud APIC リリース 25.0(2) 以降、Cisco Cloud APIC が以前のリリースから 25.0(2) にアップグレードされない限り、overlay-2 は存在しません。overlay-2 を使用する代わりに、新しい VRF をハブ VNet に追加できます。新しい VRF は、ユーザー定義のサービスアプライアンスの新しい CIDR およびサブネットに使用できます。次の図で、構成例について説明します。

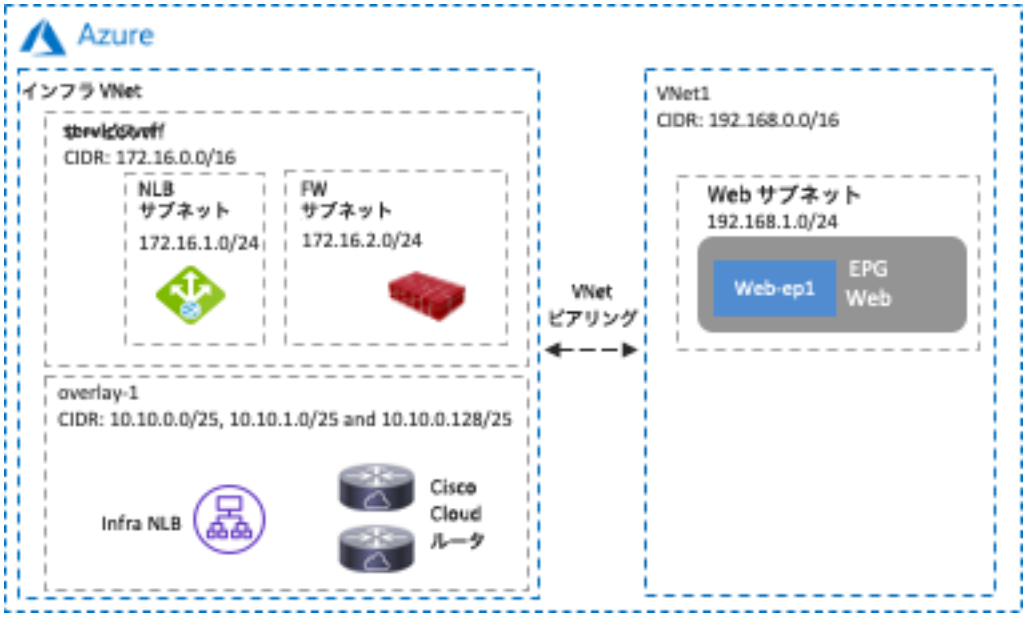

図 71. ユーザー定義 VRF の新しい CIDR のサービスアプライアンス

overlay-2 に新しい CIDR を追加するとき、または Cisco Cloud APIC を介してハブ VNet にユーザー定義の VRF を追加するときは、VNet ピアリングを無効にする必要があるため、最初にサービスデバイスの CIDR を作成することをお勧めします（既存の CIDR に新しいサブネットを追加するために VNet ピアリングを無効にする必要はありません）。

ユースケース #9：マルチノードサービスの挿入

概要

このユースケースは、サービスグラフを伴うコントラクトを使用した EPG 間のマルチノードサービス挿入です。Cloud ACI は、同じサービスグラフで、サードパーティ ファイアウォール、クラウド ネイティブ ロードバランサ、およびサードパーティ ロードバランサの組み合わせをサポートします。単一ノードサービスの挿入については、「ロードバランサの挿入」セクションおよび「ファイアウォールの挿入」セクションを参照してください。

このユースケースの主な利点は、トラフィックを複数のファイアウォールに分散させることで、高可用性とファイアウォール インスペクションのキャパシティが向上することです。

このセクションでは、さまざまなマルチノードサービス挿入のユースケースについて説明し、各オプションのトラフィックフローと関連する展開の考慮事項について説明します。

- 水平方向トラフィックフローの NLB-FW 挿入：サービスデバイスは、異なる VNet にあるコンシューマー エンドポイントとプロバイダーエンドポイントの間に挿入されます。ファイアウォールの前に展開された NLB 機能によって、トラフィックフローが複数のファイアウォールに分散されます。
- 垂直方向トラフィックフローの NLB-FW 挿入：サービスデバイスは、非 ACI オンプレミスサイトに向かう外部ネットワークと、プロバイダーエンドポイントの間に挿入されます。ファイアウォールの前にある NLB によって、トラフィックフローが複数のファイアウォールに分散されます。
- NLB-FW-LB 挿入：別のロードバランサ（NLB、ALB、またはサードパーティのロードバランサ）をファイアウォールの背後に追加して、クラウドプラットフォームのプロバイダーエンドポイントにトラフィックを分散させることができます。

他のユースケースのリストについては、『Cisco Cloud APIC for Azure User Guide』の「Deploying Layer 4 to Layer 7 Services section」セクションを参照してください。

次の図は、マルチノードサービスグラフを使用した Cloud ACI 設計の例を示しています。

- プライベートロードバランサは、EPG「Web」と EPG 「App」間のコントラクト「web-to-app」に挿入されます。
- パブリックロードバランサは、外部 EPG 「internet」と EPG 「web」間のコントラクト「external-to-web」に挿入されます。

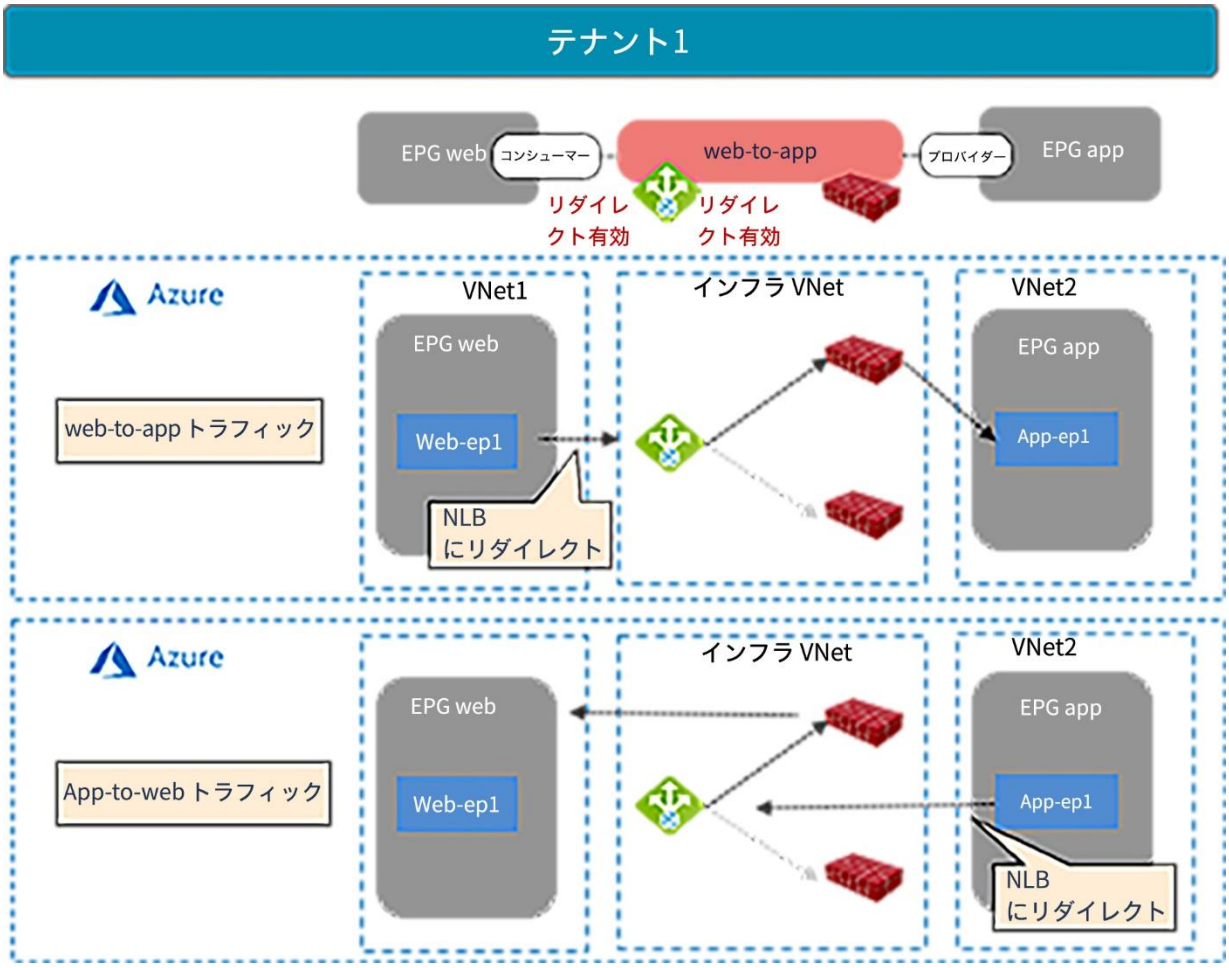

図 72. 水平方向トラフィックでの NLB-FW 挿入を使用した Cloud ACI：クラウドエンドポイントからクラウドエンドポイント

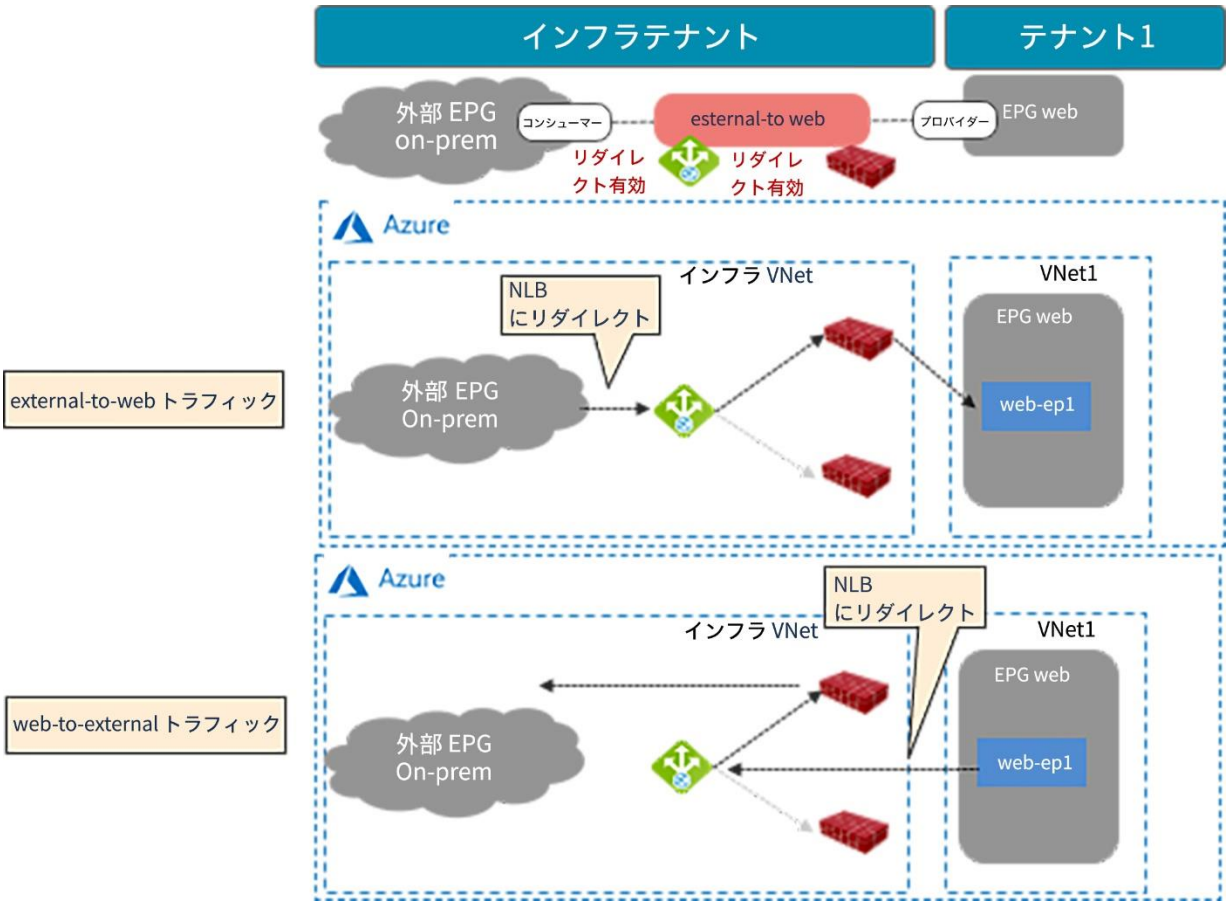

図 73. 垂直方向トラフィックでの NLB-FW 挿入を使用した Cloud ACI：非 ACI オンプレミスからクラウドエンドポイント

次の図は、ファイアウォールの背後に別のロードバランサ（NLB、ALB、またはサードパーティのロードバランサ）を持つ 3 ノードサービス挿入のユースケースを示しています。

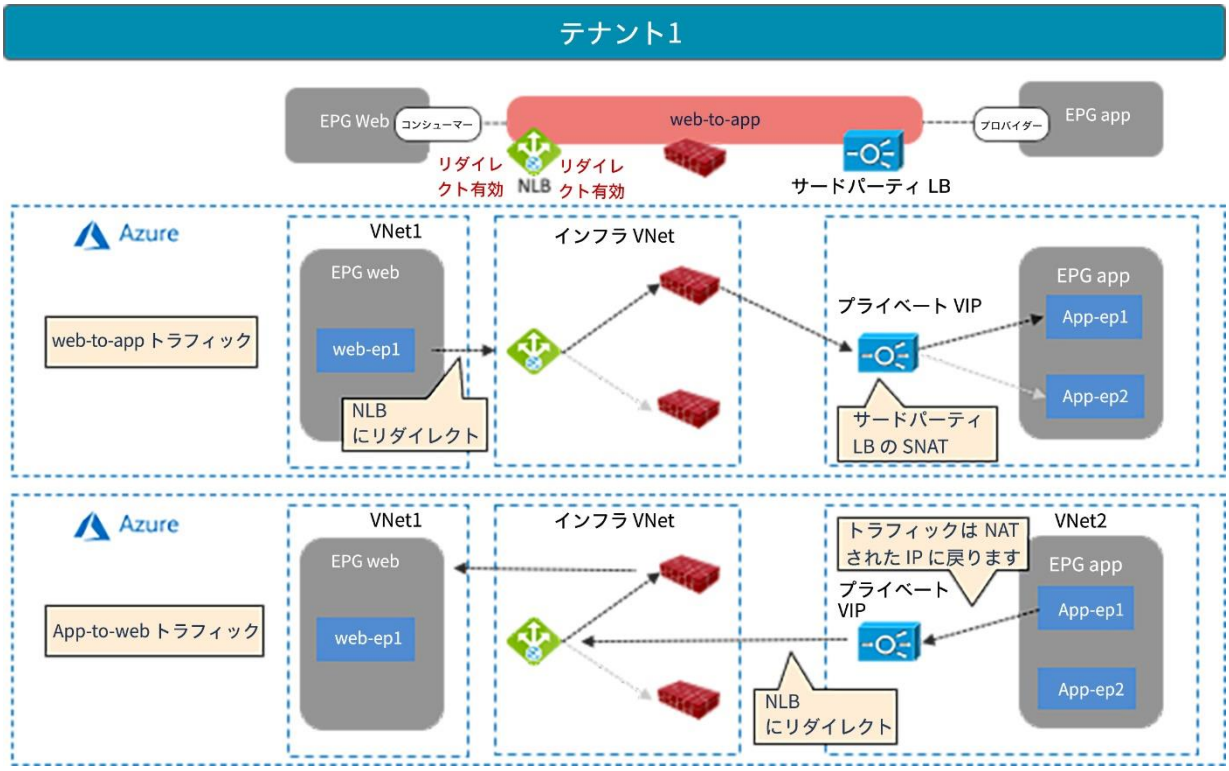

図 74. 水平方向トラフィックでの NLB-FW-LB 挿入を使用した Cloud ACI：クラウドエンドポイントからクラウドエンドポイント

マルチノードサービスの挿入には、次のガイドラインがあります。

- サービス デバイス インターフェイスは、クラウド EPG が存在するサブネットとは異なる専用サブネットにある必要があります。
- VNet 間トラフィックの場合、VNet ピアリングが必要です。
- リダイレクト先（この例では NLB IP アドレス）は、ハブ VNet（インフラ VNet）にある必要があります。
- ロードバランサ インターフェイスとそのターゲットは、同じ VNet 内にある必要があります。
- 現時点では、サイト間の水平方向通信はサポートされていません。次に例を示します。
    - コンシューマー エンドポイントが AWS サイトにあり、プロバイダーエンドポイントが Microsoft Azure サイトにある場合。
    - コンシューマー エンドポイントが ACI オンプレミスサイトにあり、プロバイダーエンドポイントが Microsoft Azure サイトにある場合。
- 外部から内部（垂直型）のトラフィック方向の場合、非 ACI ネットワーク（ExpressRoute 経由の外部 EPG）から Microsoft Azure サイトのクラウドエンドポイントへのトラフィックであれば、リダイレクトがサポートされます。
- マルチノードサービスグラフの場合、サードパーティのロードバランサ インターフェイスは「サブネットベース」のインターフェイスセレクタを使用する必要があります。

ユースケース #9-1：水平方向トラフィックフローの NLB-FW 挿入

次の図は、複数のファイアウォールへの水平方向トラフィックを NLB ロードバランシングする Cloud ACI 設計の例を示しています。この構成例では、クラウド EPG 「Web」がコントラクトのコンシューマーであり、クラウド EPG 「App」がコントラクトのプロバイダーです。ファイアウォールのインターフェイスは 1 つです。

NLB の双方向でリダイレクトが有効になっています。

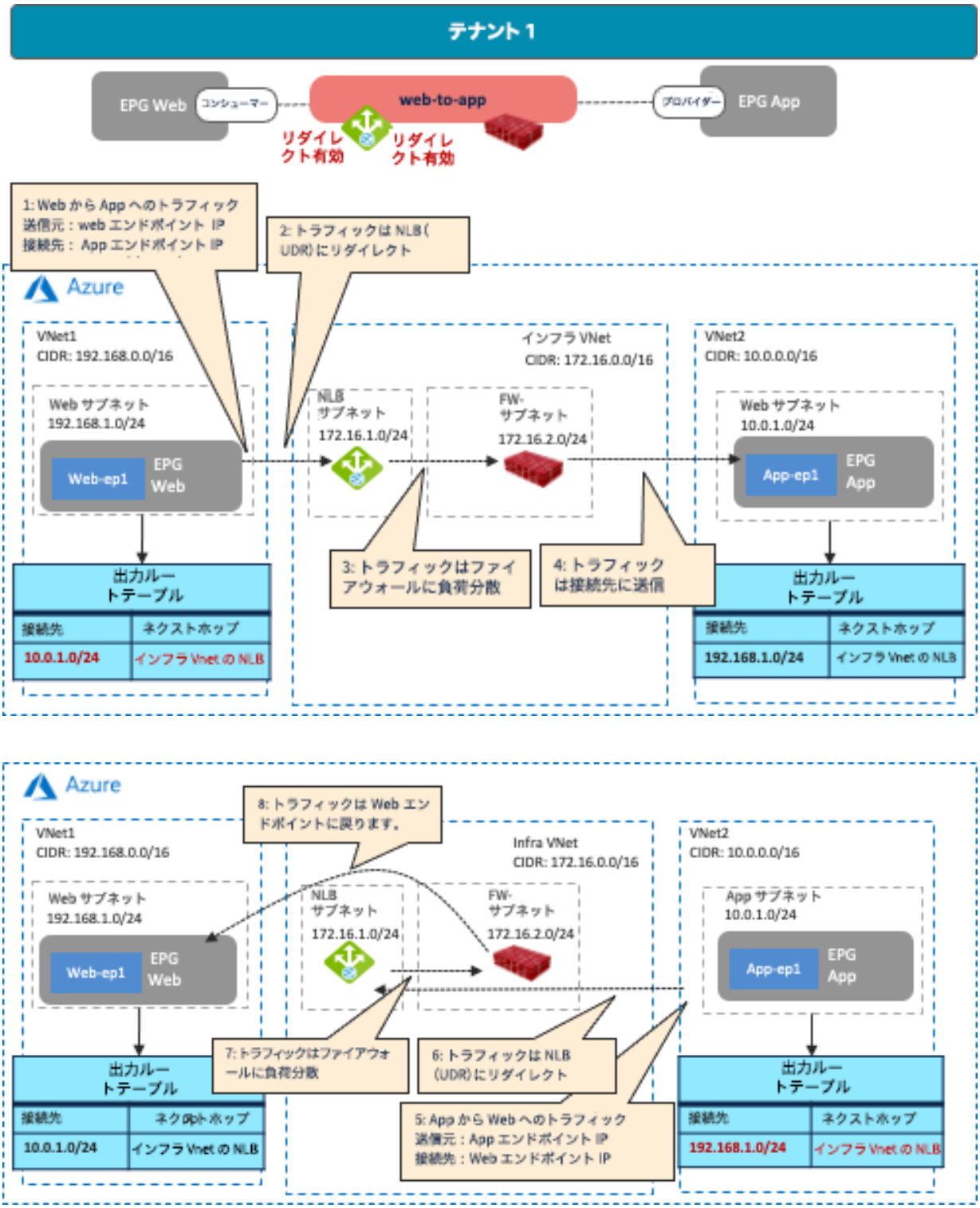

図 75. 水平方向 NLB-FW 挿入：スポーク間トラフィック

コントラクトを使用するサービスグラフ展開の一部として、Cisco Cloud APIC は両方向の出力ルートテーブルを作成します。

- 1 つは、Web サブネットから App サブネットへの通信で、NLB IP アドレスにトラフィックをリダイレクトするためのものです。
- もう 1 つは、App サブネットから Web サブネットへの通信で、NLB IP アドレスにトラフィックをリダイレクトするためのものです。

NLB により、着信トラフィックとリターントラフィックの両方が、同じファイアウォールに負荷分散されます。Cisco Cloud APIC も、それに応じて NSG および NLB 構成を更新します。たとえば、Cisco Cloud APIC は、ファイアウォールの NSG に入力セキュリティルールと出力セキュリティルールを追加し、コンシューマサブネットからプロバイダーサブネットへのトラフィックを許可します。そのため、明示的な許可ルールがない場合でも、プロバイダーからコンシューマーへのリターントラフィックは自動的に許可されます。

前のサブセクションのマルチノードサービスの挿入に関する考慮事項で提供されたガイドラインに加えて、このユースケースには次のガイドラインがあります。

- コンシューマーとプロバイダーの EPG は、同じリージョンに展開されている場合、同じ VNet の一部にすることはできません。

ユースケース #9-2：垂直方向トラフィックフローの NLB-FW 挿入

次の図は、複数のファイアウォールへの垂直方向トラフィックを NLB ロードバランシングする Cloud ACI 設計の例を示しています。この構成例では、非 ACI オンプレミスサイトに接続された外部 EPG「On-Prem」がコントラクトのコンシューマーであり、クラウド EPG「Web」がコントラクトのプロバイダーです。ファイアウォールのインターフェイスは 1 つです。NLB の双方向でリダイレクトが有効になっています。

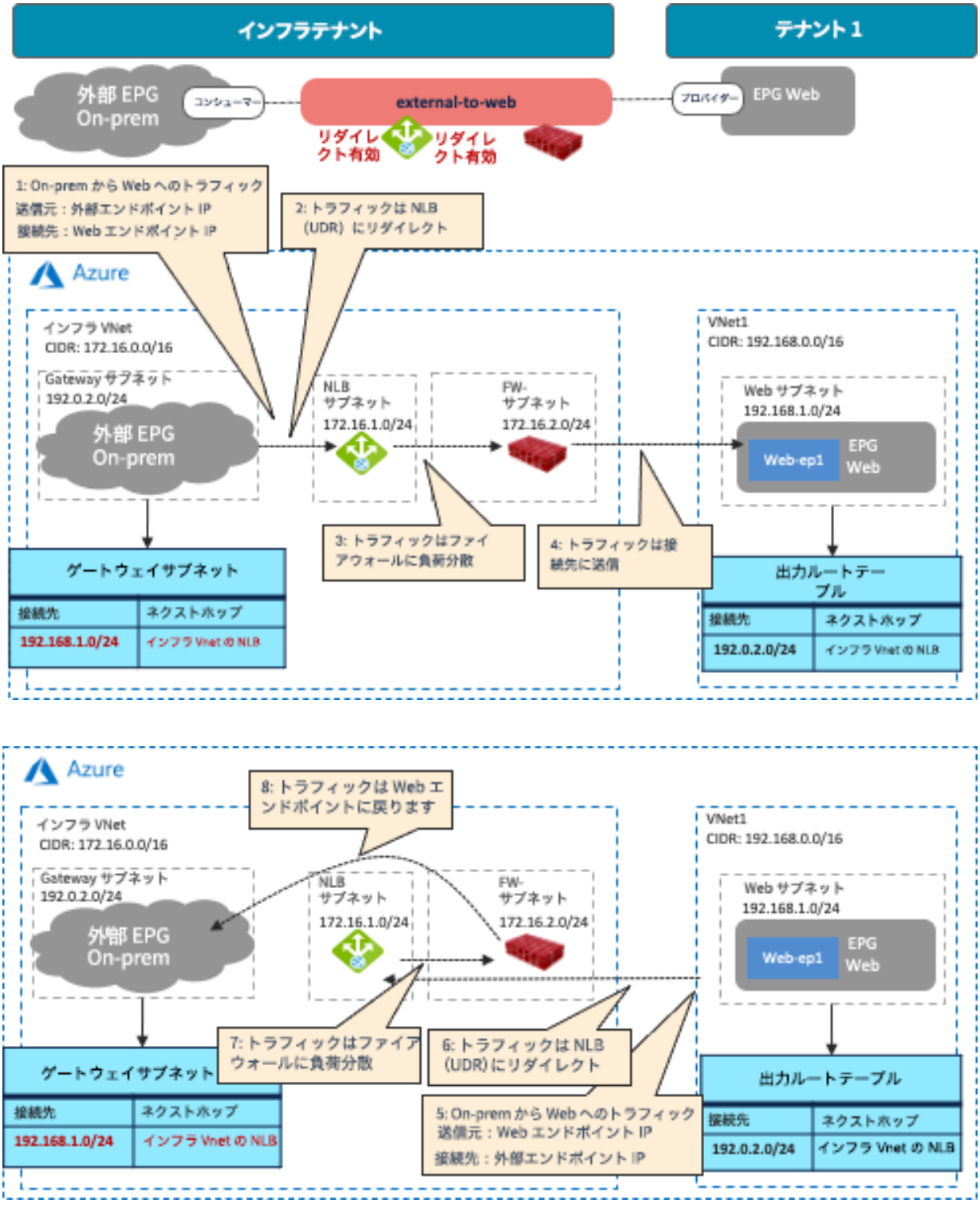

図 76. 垂直方向 NLB-FW の挿入：非 ACI オンプレミスからクラウドエンドポイント

コントラクトを使用するサービスグラフ展開の一部として、Cisco Cloud APIC は両方向の出力ルートテーブルを作成します。

- 1 つは、トラフィックを外部 EPG サブネットから Web サブネットにリダイレクトし、次に NLB IP アドレスにリダイレクトするためのものです。
- もう 1 つは、トラフィックを Web サブネットから外部 EPG サブネットにリダイレクトし、次に NLB IP アドレスにリダイレクトするためのものです。

NLB により、着信トラフィックとリターントラフィックの両方が、同じファイアウォールに負荷分散されます。Cisco Cloud APIC も、それに応じて NSG および NLB 構成を更新します。

前のサブセクションのマルチノードサービスの挿入に関する考慮事項で提供されたガイドラインに加えて、このユースケースには次のガイドラインがあります。

- 外部 EPG は Azure ExpressRoute を経由する必要があります。これは、外部 EPG が非 ACI オンプレミスネットワークを表すことを示しています。
- 非 ACI ネットワーク（ExpressRoute 経由の外部 EPG 内）からクラウドエンドポイント（クラウド EPG 内）へのトラフィックのリダイレクトを有効にするには、Cisco Cloud APIC 5.1(2) リリース以降が必要です。
- Azure ExpressRoute を経由しない外部 EPG は、リダイレクトをサポートしていません。
- このドキュメントでは主にリダイレクトのユースケースについて説明していますが、リダイレクトなしでハブ VNet に ExpressRoute ゲートウェイを展開することもできます。
- サイト内の異なる Cisco Cloud APIC 管理リージョンに複数のハブ VNet がある場合（リージョン間設計）、次の設計ガイドラインが適用されます。
    - 各リージョンには、ハブ VNet に ExpressRoute ゲートウェイが必要です。
    - 各 ExpressRoute ゲートウェイは同じルーティングドメインに接続され、お客様のネットワークから同じルートセットを受け取ります。
    - 特定のスポークの場合、ローカルリージョンのハブ VNet がトランジット VNet として最初に選択されます。ローカルリージョンの ExpressRoute ゲートウェイが障害のために使用できない場合、代替リージョンが自動的に選択されます。

ユースケース #9-3：NLB-FW-LB 挿入

このユースケースの目的は、次の図に示すように、「水平方向トラフィックフローの NLB-FW 挿入」で説明されているユースケースに別のロードバランサ（NLB、ALB、またはサードパーティのロードバランサ）を追加することです。このサブセクションでは、水平方向トラフィックフローに別のロードバランサを追加する例（ユースケース #9-1）を使用しますが、垂直方向トラフィックフローに別のロードバランサを追加するのも有効な設計です（ユースケース#9-2）。

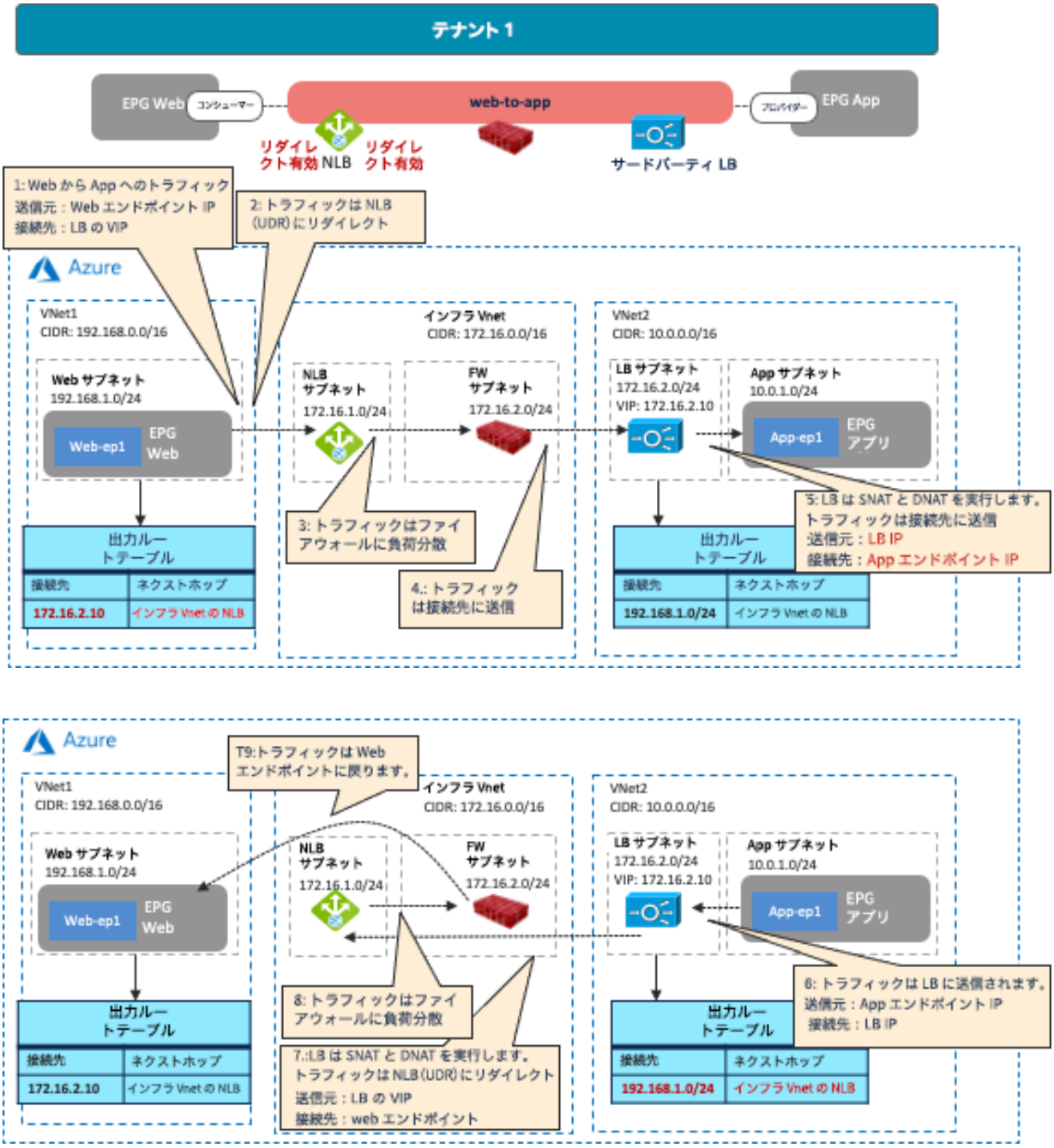

図 77. 水平方向 NLB-FW-LB 挿入：スポーク間トラフィック

コントラクトを使用するサービスグラフ展開の一部として、Cisco Cloud APIC は両方向の出力ルートテーブルを作成します。

- 1 つは、Web サブネットおよびサードパーティのロードバランサの VIP からのトラフィックを NLB IP アドレスにリダイレクトするためのものです。
- もう 1 つは、LB サブネットおよび Web サブネットから NLB IP アドレスへのトラフィックをリダイレクトするためのものです。

NLB により、着信トラフィックとリターントラフィックの両方が、同じファイアウォールに負荷分散されます。Cisco Cloud APIC も、それに応じて NSG および NLB 構成を更新します。Cisco Cloud APIC はサードパーティのロードバランサを構成しないため、お客様が適宜構成する必要があります。

前のサブセクションのマルチノードサービスの挿入に関する考慮事項で提供されたガイドラインに加えて、このユースケースには次のガイドラインがあります。

- コンシューマーとプロバイダーの EPG は、同じリージョンにある場合、同じ VNet に置くことはできません。

ユースケース #10：Microsoft Azure でのクラウドネイティブサービスの統合

現時点では、この機能は Microsoft Azure を使用する Cloud ACI でのみサポートされています。Cloud APIC では、クラウドサービス EPG と呼ばれる新しいタイプの EPG が導入されています。クラウドサービス EPG は、構成されたセレクタに基づくサービスユニットのコレクションです。たとえば、クラウドストレージサービス EPG は、特定のキーと値のペアでタグ付けされたすべてのストレージユニット（Microsoft Azure のコンテナまたは blob）で構成されている場合があります。クラウドサービス EPG は、サービスとしてのプラットフォームやサービスとしてのソフトウェアなどの導入モデルのタイプも示します。

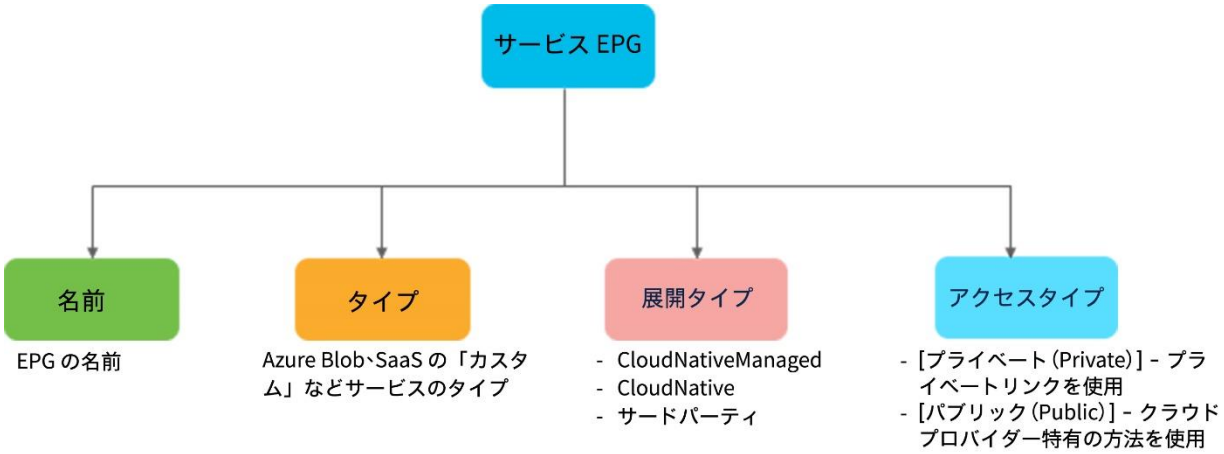

図 78. クラウドサービス EPG のプロパティ

クラウドサービス EPG のプロパティは次のとおりです。

- [名前（Name）]：EPG の名前
- [サービスタイプ（Service Type）]：この EPG が表すサービスのタイプ。例：Azure Storage、AKS、Databricks など。サードパーティのサービス（SaaS）の場合、サービスタイプは「custom」になります。
- [展開タイプ（Deployment Type）]：サービスは、導入モデルに基づいて区別されます。このフィールドは、これがクラウドネイティブか SaaS サービスか、およびホストしているのがお客様の VNet か Azure VNet かを示します。簡単に言えば、この属性は、サービスが展開されている方法と場所を示します。使用可能な展開タイプは次のとおりです。
    - [クラウドネイティブ（Cloud Native）]：Microsoft Azure 独自の VNet（Cisco Cloud APIC によって作成された VNet ではありません）でホストされるクラウドネイティブサービス。
    - [クラウドネイティブマネージド（Cloud Native Managed）]：お客様の VNet（Cisco Cloud APIC によって作成された VNet）でホストされるクラウドネイティブサービス。

- [サードパーティ（Third-Party）]：マーケットプレイスを通じてサービスを提供するサードパーティ（Microsoft Azure ではない）のサービス。このサービスへのアクセスは、プライベートリンク機能を通じて提供されます。

- [アクセスタイプ（Access Type）]：サービスへのアクセスの種類。
  - [パブリック（Public）]：サービスには、割り当てられたパブリック IP アドレスを使用してアクセスできます。特定のサービスのパブリック IP アドレス範囲へのアクセスは、NSG ルールの Azure「サービスタグ」を使用して行います。
  - [プライベート（Private）]：サービスには、割り当てられたプライベート IP アドレスを使用してアクセスできます。この割り当ては、展開が [クラウドネイティブ（Cloud Native）] に設定されている場合に、プライベートエンドポイントを作成することで行われます。[クラウドネイティブマネージド（Cloud Native Managed）] 展開の場合、プライベート IP はサービスによってサブネット IP スペースから割り当てられます。

Azure サービスタグの詳細については、https://docs.microsoft.com/en-us/azure/virtual-network/service-tags-overview を参照してください。

サポートされるクラウドサービス EPG セレクタは、展開タイプによって異なります。たとえば、クラウドサービスがお客様の VNet（Cloud APIC によって作成された VNet）に展開される [クラウドネイティブマネージド（Cloud Native Managed）] の場合、次のセレクタを使用できます。タグ、リージョン、サービス名、およびサービスが展開されているサブネット IP アドレス。クラウドサービス EPG が作成されると、Cloud APIC はプライベートエンドポイントとプライベートリンクを自動的に作成します。クライアントマシンからサービスへのアクセスの制御に、コントラクトを適用できます。

次の図は、サービスがクラウドサービス EPG にグループ化される例を示しています。Cloud APIC では、適切な NSG ルールをプログラミングすることで、EPG からクラウドサービス EPG への通信を制御できます。たとえば、Cisco Cloud APIC によって作成された VNet に AKS クラスタを展開し、インターネットからポート TCP 80 の AKS サービスに到達するトラフィックのみを許可できます。このポートは、インターネット外部 EPG と AKS クラウドサービス EPG「AzureEKS」の間に適用されるコントラクトのフィルタルールで構成されます。クラウド管理者は、異なるルールを使用して別のコントラクトを構成し、EPG（クライアント EPG など）から AKS クラウドサービス EPG「AzureEKS」への通信を制御することもできます。EPG は、クラウドサービス EPG と同じ VNet または別の VNet に配置できます。

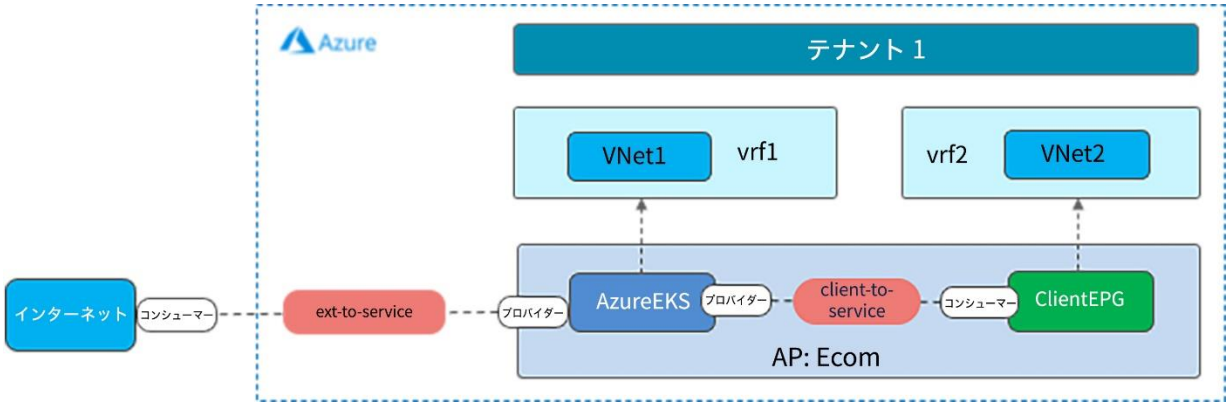

図 79. Azure クラウドネイティブサービスの統合

ユースケース #11：Microsoft Azure および AWS でのブラウンフィールド インポート

概要

このユースケースは、Cloud ACI インフラストラクチャに接続する必要がある既存のパブリッククラウドリソースがある場合に使用されます。Cisco Cloud APIC リリース 5.2(1) より前は、Cloud ACI は、Cisco Cloud APIC がリソースグループ、VPC/VNet、CIDR、サブネットなどをゼロから作成するグリーンフィールド環境のみをサポートします。つまり、既存のブラウンフィールド環境（リソースグループ、VPC/ VNET などは Cisco Cloud APIC を使用せずにユーザーが作成済み）は、Cisco Cloud APIC が管理するリソースでは共存できません。Microsoft Azure の場合は Cisco Cloud APIC リリース 5.2 以降、AWS の場合はリリース 25.0(2) 以降、ブラウンフィールド環境との共存機能がサポートされています。

Cisco Cloud APIC は、既存のブラウンフィールド VPC/VNet のインポートをサポートし、VPC/VNet および SG/NSG を含む Cisco Cloud APIC 管理のリソースグループからのネットワークおよびセキュリティポリシーの接続を自動化します。現時点では、Cisco Cloud APIC は、既存のブラウンフィールド リソースグループで構成やプロビジョニングを行いません。既存のブラウンフィールド リソースグループのセキュリティとルーティングは、引き続きユーザーが所有することが前提です。

現時点では、ブラウンフィールド インポート プロセスは Cisco Cloud APIC 自体で実行されます。 NDO ではまだブラウンフィールド インポートはサポートされていません。サポートされているリソースが Cisco Cloud APIC にインポートされると、NDO がそれらのリソースを Cisco Cloud APIC からインポートできます。NDO から見ると、リソースが NDO テンプレートにインポートされた後、ブラウンフィールドリソースとグリーンフィールドリソースに違いはありません。次のサブセクションでは、Microsoft Azure および AWS でブラウンフィールド インポートを実行するための高レベルの手順と固有の考慮事項について、それぞれ説明します。

Microsoft Azure でのブラウンフィールド インポート

ブラウンフィールドリソースは、グリーンフィールドリソースと同じ Azure サブスクリプションにある場合も、異なる Azure サブスクリプションにある場合もあります。ブラウンフィールドリソースが、グリーンフィールドサブスクリプションとは異なる Active Directory にある別の Azure サブスクリプションにある場合もあります。ブラウンフィールドリソースが別の Azure サブスクリプションにある場合、Cisco Cloud APIC は最初にブラウンフィールド Azure サブスクリプションを表す新しいテナントを作成する必要があります。ブラウンフィールド VNet は、管理対象外仮想ネットワークとも呼ばれます。Cisco Cloud APIC GUI のボタンタイトルに [管理対象外仮想ネットワーク（Unmanaged Virtual Network）] と表示されるのはそのためです。

たとえば、ブラウンフィールド VNet をインポートするには、[インテント（Intent）] ボタンから、[ワークフロー（Workflows）] セクションの [管理対象外仮想ネットワーク（Unmanaged Virtual Network）] オプションを選択できます。

図 80. Cisco Cloud APIC の [インテント（Intent）] ボタン

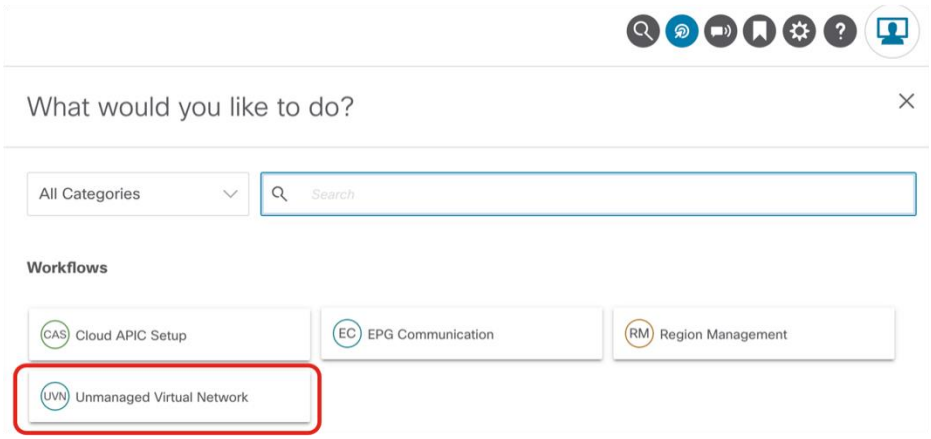

図 81. 管理対象外仮想ネットワークのインポート（ブラウンフィールド インポート）

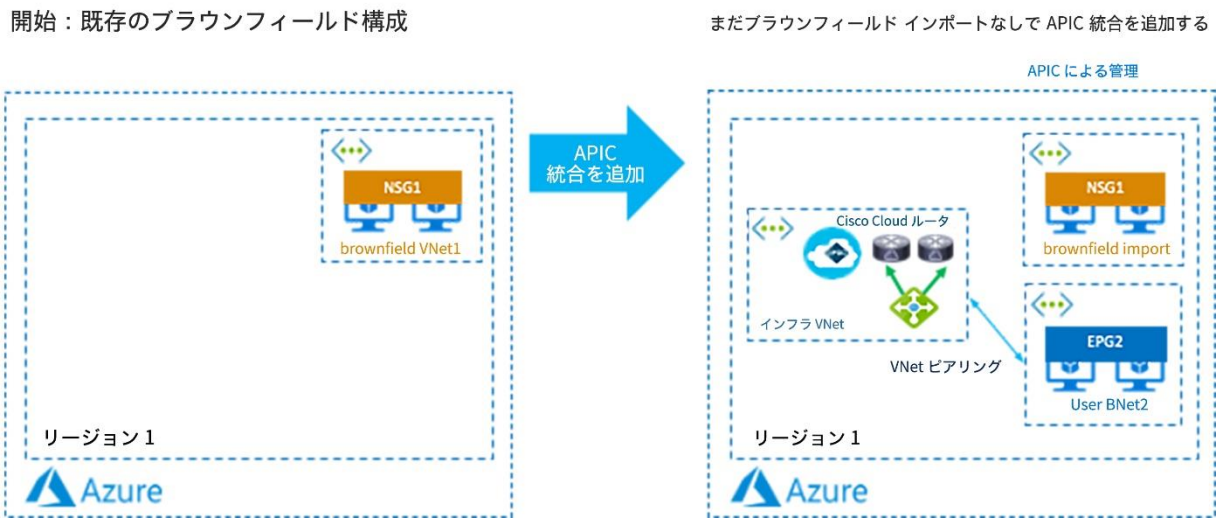

図 82. ブラウンフィールド VNet を Cisco Cloud APIC にインポートする

ブラウンフィールド インポートの後、Cisco Cloud APIC は、インフラ VNet（overlay-1 VNet）からブラウンフィールド（管理対象外）VNet への VNet ピアリング要求を自動的に開始します。ブラウンフィールド VNet からインフラ VNet へのピアリングセッションを開始して VNet ピアリングセッションを完了させるのは、エンドユーザーの責任です。

サブネットベースのセレクタ EPG のみがサポートされているため、Cisco Cloud APIC 管理者は、ブラウンフィールド VNet のエンドポイントを表すサブネットベースのセレクタ EPG を作成する必要があります。

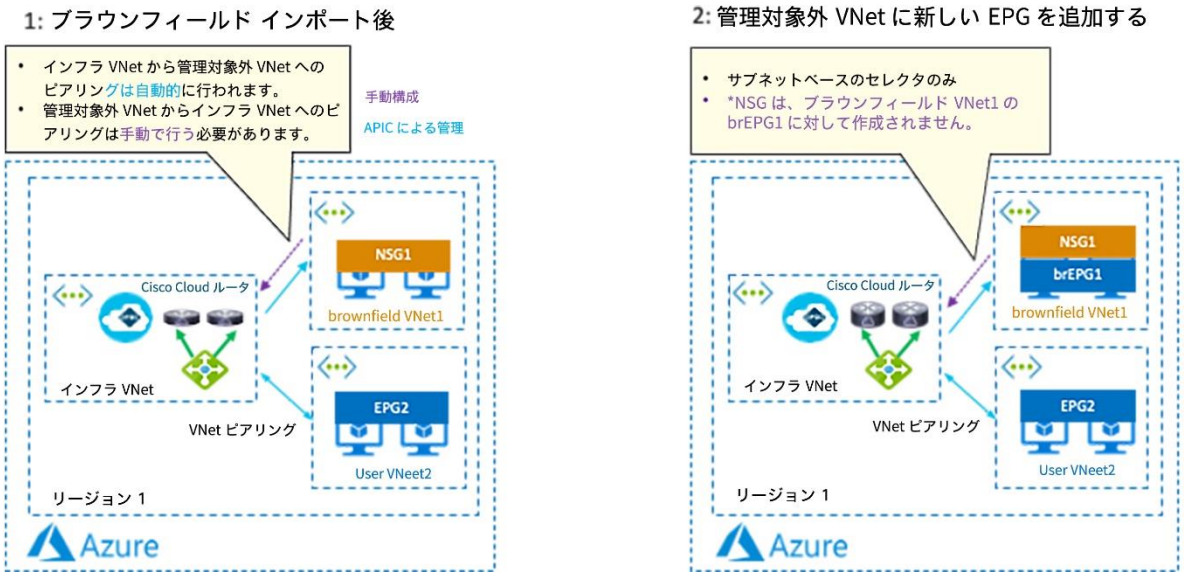

図 83. ブラウンフィールド VNet からの VNet ピアリングの作成およびブラウンフィールドサブネットのサブネットベースのセレクタ

Cisco Cloud APIC は、Cisco Cloud ルータのルーティング構成を自動化して、グリーンフィールド VNet とブラウンフィールド VNet の間でトラフィックをルーティングします。グリーンフィールド EPG とブラウンフィールド EPG の間にコントラクトが適用されると、Cisco Cloud APIC はグリーンフィールド側で NSG ルールを自動化し、グリーンフィールド VNet ルートテーブルに UDR ルートエントリを自動的に追加します。ブラウンフィールド VNet で UDR ルートテーブルエントリを構成または編集し、NSG ルールを構成または編集して、グリーンフィールド EPG とブラウンフィールド EPG 間の適切な通信を許可するのは、エンドユーザーの責任です。

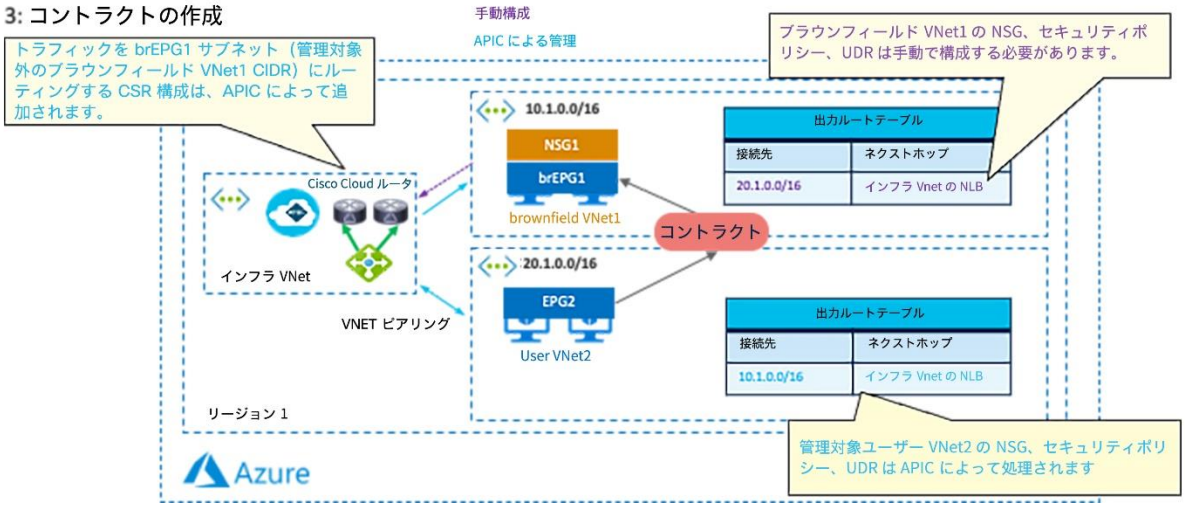

図 84. ブラウンフィールド VNet ルートテーブルと NSG ルールを作成または編集する

詳細な手順については、以下を参照してください。

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/cloud-apic/5-x/use-case/importing-existing-brownfield-cloud-configurations-into-cloud-apic.html

Microsoft Azure のブラウンフィールド インポートには、次のガイドラインがあります。

- ブラウンフィールド リソースグループでは、Cisco Cloud APIC によって実行されないものがいくつかあります。これらのポリシーをすべて作成して適用するのは、ブラウンフィールド VNet 所有者の責任です。Cisco Cloud APIC は、グリーンフィールド EPG とのコントラクトに基づいてインフラ NLB を指す UDR を含むルートテーブルを作成しません。Cisco Cloud APIC は、ブラウンフィールド リソースグループに NSG または ASG を作成しません。これらのブラウンフィールド リソースグループのエンドポイントに対して行われるエンドポイント検出はありません。ブラウンフィールド VNet に関連付けられているクラウド EPG には、サブネットベースのエンドポイントセレクタが必要です（タグベースの EPG はブラウンフィールド VNet には適用されません）。
- ブラウンフィールド VNet 内のすべての構成は、ユーザーが管理する必要があります。Cisco Cloud APIC は、グリーンフィールド VNet からブラウンフィールド VNet への接続のみを自動化します。ブラウンフィールド VNet は、どこにでも存在できます(たとえば、同じサブスクリプション、同じ Active Directory ドメイン内の異なるサブスクリプション、または異なる Active Directory ドメイン全体)。また、さまざまなリソースに対する読み取りアクセス許可を持つ、この管理対象外サブスクリプションに関連付けられたサービスプリンシパルも必要です。
- ブラウンフィールド VNet とグリーンフィールド VNet 間のサービスリダイレクトは、まだ正式にはサポートされていません。

AWS でのブラウンフィールド インポート

ブラウンフィールドリソースは、グリーンフィールドリソースと同じ AWS アカウントにある場合も、異なる AWS アカウントにある場合もあります。ブラウンフィールドリソースが別の AWS アカウントにある場合、Cisco Cloud APIC は最初に AWS アカウントを表す新しいテナントを作成する必要があります。ブラウンフィールド VPC は、管理対象外 VPC とも呼ばれます。Cisco Cloud APIC GUI のボタンタイトルに [管理対象外 VPC（Unmanaged VPC）] と表示されるのはそのためです。

たとえば、ブラウンフィールド VNet をインポートするには、[インテント（Intent）] ボタンから、[ワークフロー（Workflows）] セクションの [管理対象外 VPC（Unmanaged VPC）] オプションを選択します。

図 85. Cisco Cloud APIC の [インテント（Intent）] ボタン

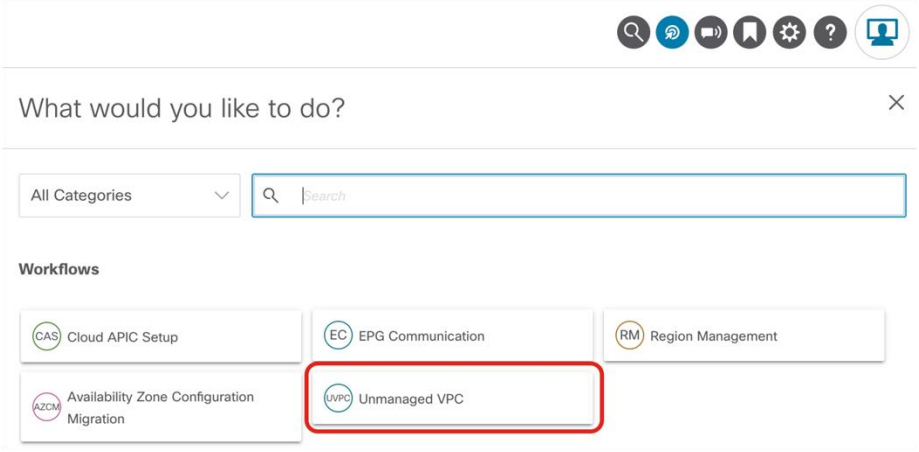

図 86. 管理対象外 VPC のインポート（ブラウンフィールド インポート）

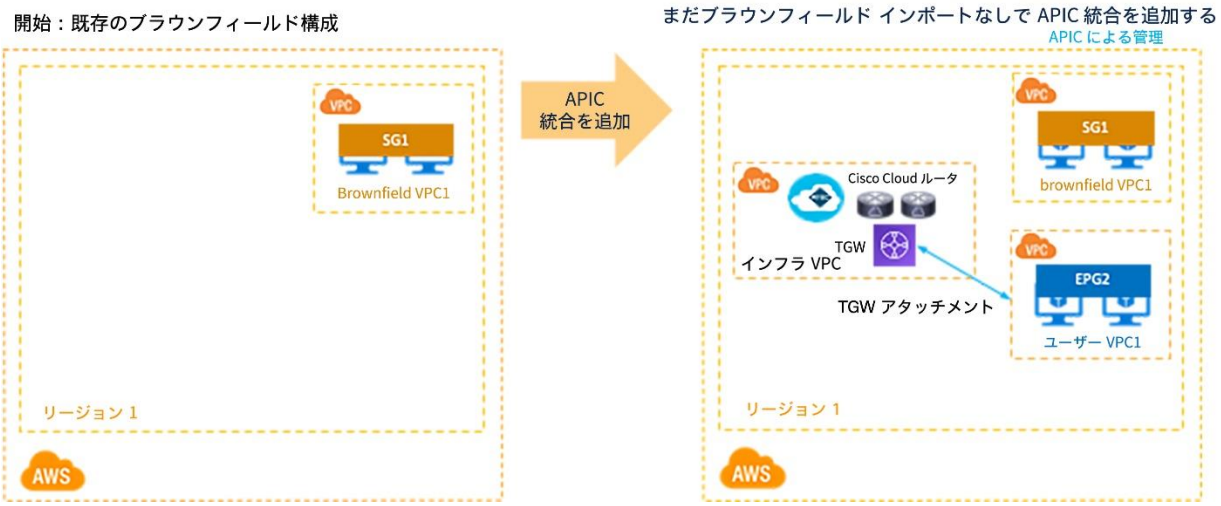

図 87. ブラウンフィールド VPC を Cisco Cloud APIC にインポートする

ブラウンフィールド インポートの後、グリーンフィールド TGW（Cisco Cloud APIC によって作成された TGW）へのブラウンフィールド VPC アタッチメントを手動で作成する必要があります。

サブネットベースのセレクタ EPG のみがサポートされているため、Cisco Cloud APIC 管理者は、ブラウンフィールド VPC のエンドポイントを表すサブネットベースのセレクタ EPG を作成する必要があります。

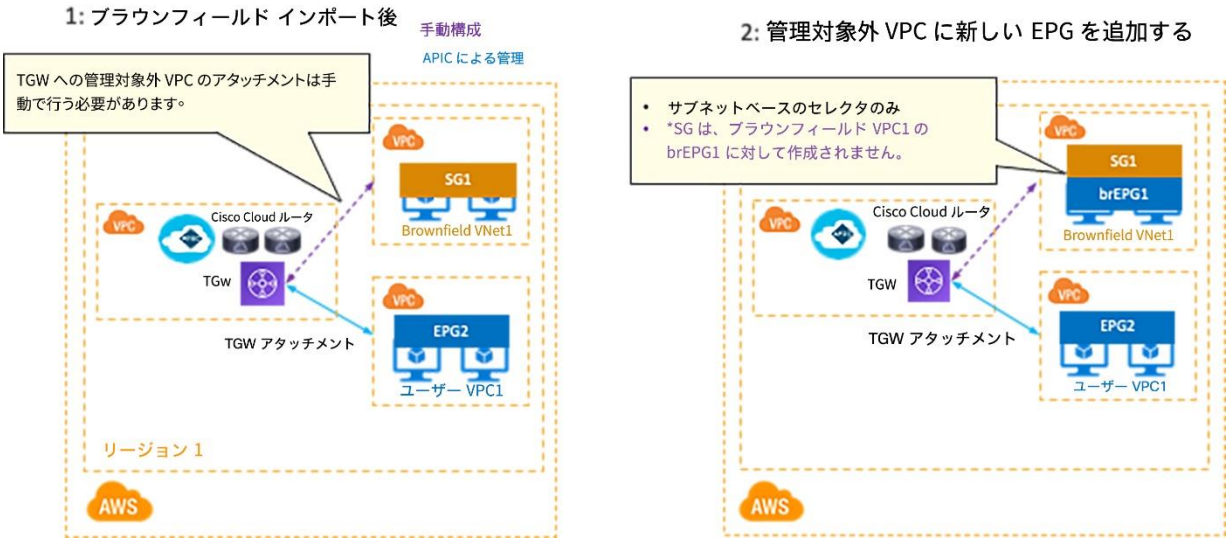

図 88. ブラウンフィールド VPC を Cisco Cloud APIC 管理の TGW にアタッチし、ブラウンフィールド サブネット用のサブネットベースのセレクタ EPG を作成する

グリーンフィールド EPG とブラウンフィールド EPG の間にコントラクトが適用されると、Cisco Cloud APIC はグリーンフィールド側で SG ルールを自動化します。Cisco Cloud APIC は、グリーンフィールド VPC ルートテーブルにルートエントリを自動的に追加します。ブラウンフィールド VPC で VPC ルートテーブルを構成または編集し、SG ルールを構成または編集して、グリーンフィールド EPG とブラウンフィールド EPG 間の適切な通信を許可するのは、エンドユーザーの責任です。

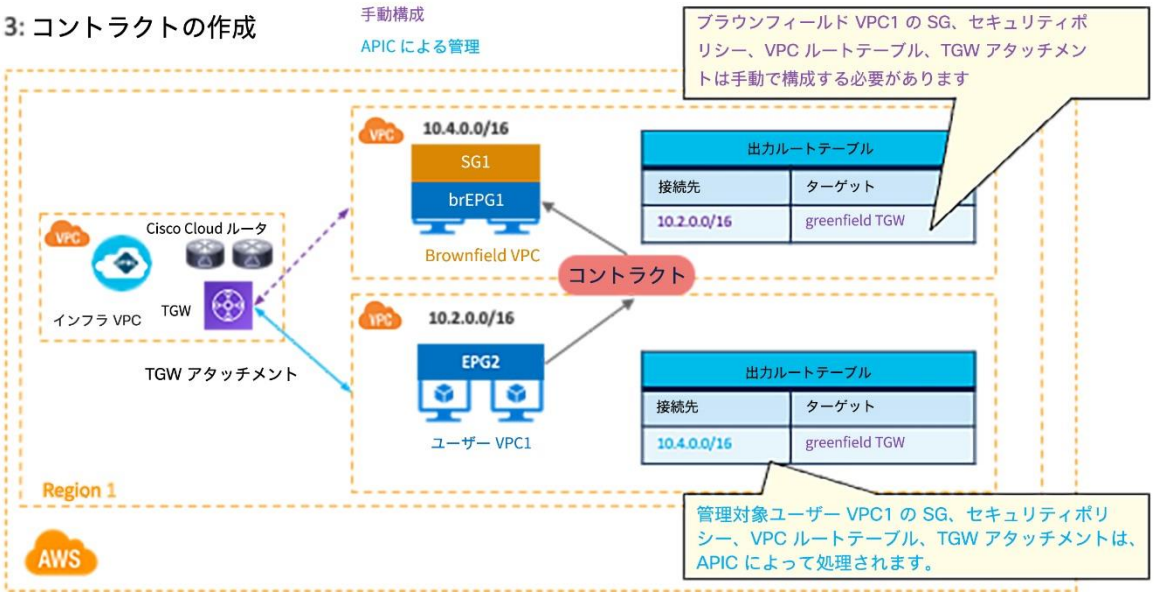

図 89. ブラウンフィールド SG および VPC ルートテーブルの作成または編集

詳細な手順については、以下を参照してください。

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/cloud-apic/5-x/use-case/importing-existing-brownfield-aws-cloud-vpcs-into-cloud-apic.html

AWS のブラウンフィールド インポートには、次のガイドラインがあります。

- ブラウンフィールド VPC では CIDR のすべてまたは特定のセットを選択的にインポートできますが、プライマリ CIDR がなければブラウンフィールド VPC をインポートすることはできません。ブラウンフィールド VPC をインポートする場合、プライマリ CIDR のインポートは必須です。
- グリーンフィールド展開の場合、Cisco Cloud APIC は TGW とグリーンフィールド VPC を作成し、グリーンフィールド VPC とグリーンフィールド TGW（Cisco Cloud APIC 管理の TGW）の間の TGW アタッチメントを自動構成します。Cisco Cloud APIC は、ブラウンフィールド VPC の TGW アタッチメントを構成しません。ブラウンフィールド VPC からグリーンフィールド TGW への TGW アタッチメントは手動で構成する必要があります。
- Cisco Cloud APIC は、グリーンフィールド VPC のセキュリティ グループ ルールをプログラムして、ブラウンフィールド VPC との間のインバウンドおよびアウトバウンドトラフィックを許可します。Cisco Cloud APIC は、ブラウンフィールド VPC のセキュリティ グループ ルールをプログラミングしません。
- Cisco Cloud APIC は、 ブラウンフィールド VPC のルートテーブルまたはルートをプログラミングしません。ブラウンフィールド VPC がグリーンフィールド VPC と通信するには、次の構成を手動で行う必要があります。
    - グリーンフィールドとブラウンフィールドの EPG 間のコントラクトを作成します。
    - インフラ VPC 内のグリーンフィールド TGW を使用して、トランジットゲートウェイ VPC アタッチメントを作成します。
    - ブラウンフィールド VPC とサブネットのルートテーブルを作成または編集します。
    - 接続先がグリーンフィールド CIDR であり、ネクストホップがグリーンフィールド TGW VPC アタッチメントであるルートを追加します。
- ブラウンフィールド VNPC に関連付けられているクラウド EPG には、サブネットベースのエンドポイントセレクタが必要です（タグベースの EPG はブラウンフィールド VNet には適用されません）。

詳細については、以下を参照してください。

https://www.cisco.com/c/ja_jp/solutions/data-center-virtualization/application-centric-infrastructure/white-paper-listing.html

シスコ コンタクトセンター

自社導入をご検討されているお客様へのお問い合わせ窓口です。
製品に関して ｜ サービスに関して ｜ 各種キャンペーンに関して ｜ お見積依頼 ｜ 一般的なご質問

お問い合わせ先

お電話での問い合わせ
平日 9:00 - 17:00
0120-092-255

お問い合わせウェブフォーム
cisco.com/jp/go/vdc_callback

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。