ホワイトペーパー

Cisco public

The bridge to possible

Cisco Application Centric Infrastructure におけるポリシーベース リダイレクト サービス グラフの設計

目次

はじめに

Cisco Application Centric Infrastructure（Cisco ACI）テクノロジーでは、サービスグラフと呼ばれるアプローチを使用してレイヤ 4 ~ レイヤ 7（L4-L7）機能を挿入することができます。サービスグラフの主な機能の 1 つは、ポリシーベースリダイレクト（PBR）です。

Cisco ACI ファブリックでは、PBR を使用することでセキュリティゾーン間のトラフィックをファイアウォール、侵入防御システム（IPS）、ロードバランサなどの L4-L7 デバイスにリダイレクトできます。その際、これらの L4-L7 デバイスをサーバーのデフォルトゲートウェイにする必要も、VRF（Virtual Routing and Forwarding）サンドイッチ、VLAN スティッチングなどの従来のネットワーク構成を実行する必要もありません。Cisco ACI は、プロトコルやレイヤ 4 ポートなどに基づいて、L4-L7 デバイスにトラフィックを選択的に送信できます。ファイアウォールによる検査は、ルーティングやスイッチングの既存の設定をほとんど変更することなく、レイヤ 2 ドメインに透過的に挿入できます。

このドキュメントの目的

このドキュメントは、さまざまなユースケースとオプションを使用して、PBR サービスグラフの設計や設定の方法について説明します。

前提条件

このドキュメントは、読者が Cisco ACI およびサービスグラフとその仕組みに関する基本的な知識を持っていることを前提としています。詳細は、Cisco.com にある Cisco ACI のホワイトペーパー（https://www.cisco.com/c/ja_jp/solutions/data-center-virtualization/application-centric-infrastructure/white-paper-listing.html）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。

- BD：ブリッジドメイン
- EPG：エンドポイントグループ
- クラス ID：EPG を識別するタグ
- ポリシー：Cisco ACI では、「ポリシー」が設定一般を意味する場合がありますが、このドキュメントの文脈では、特にアクセス制御リスト（ACL）を指します。あるセキュリティゾーン（EPG）から別のセキュリティゾーン（EPG）に向けて送信されたパケットに対し許可、リダイレクト、ドロップのどれを実行するかを決定するために使用される三値連想メモリ（TCAM）ルックアップがその一例です。
- PBR ノード：PBR の接続先として使用される L4-L7 デバイス
- コンシューマーコネクタ：コンシューマー側に接続された PBR ノードインターフェイス
- プロバイダーコネクタ：プロバイダー側に接続された PBR ノードインターフェイス

概要

Cisco ACI ファブリックでは、接続先の IP アドレスと MAC アドレスに基づいてトラフィックのルーティングとブリッジングが行われます。これは従来のネットワークと変わりません。デフォルトでは、サービスグラフを使用する場合もこのプロセスは変わりません。したがって、サービスデバイスを挿入しようとすると、依然としてルーティングとブリッジングの設計を検討する必要があります。ただし、Cisco Application Policy Infrastructure Controller（APIC）リリース 2.0(1m) 以降では、サービスグラフが PBR の機能を提供するため、セキュリティゾーン間のトラフィックのリダイレクトが可能になります。PBR を使用すると、サービスデバイスの挿入と取り外しが簡単になります。

図 1 に、Cisco ACI におけるルーティングベースの設計（従来の VRF サンドイッチ）と PBR の違いの一例を示します。ルーティングベースの設計では、内部および外部のそれぞれのファイアウォール インターフェイスとファブリックとの間にレイヤ 3 外部（L3Out）接続が確立されます。したがって、従来の VRF サンドイッチ構成では、トラフィックがルーテッドファイアウォールを通過するようにする必要があります。ファイアウォールの内部インターフェイスの Web サブネットと IP サブネットは、VRF2 インスタンスの内部にあるファイアウォールに関連付けられています。ファイアウォールの WAN エッジルータ側の外部インターフェイスとレイヤ 3 インターフェイスは、VRF1 インスタンスの外部にある別のファイアウォールの一部です。この構成がない場合、VRF インスタンス内で接続先エンドポイントの IP アドレスを解決できるため、トラフィックは 2 つのエンドポイント間で直接伝送されます。

PBR を使用すると設定が簡素化されます。セキュリティゾーン間にレイヤ 3 ファイアウォールを挿入するために、上述の VRF サンドイッチ構成を行う必要がないためです。代わりに、トラフィックは PBR ポリシーに基づいてノードにリダイレクトされます。

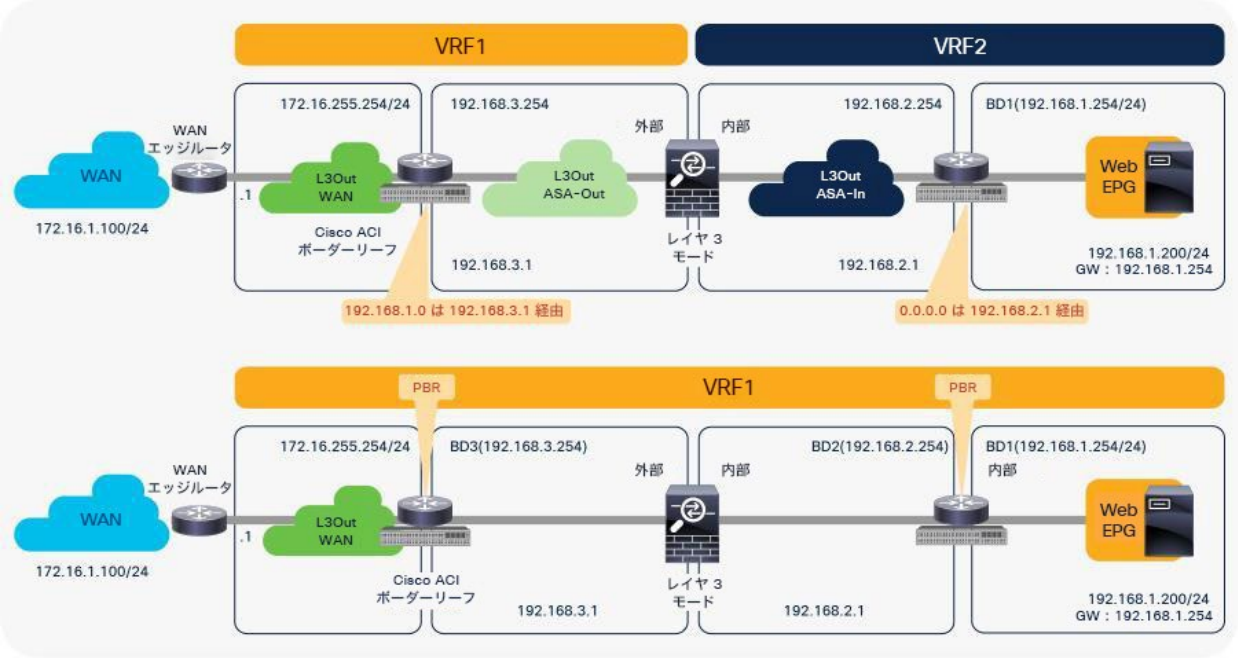


図 1.
比較：VRF サンドイッチ設計と PBR 設計

PBR では、エンドポイントグループ（EPG）間のコントラクトにサービスグラフがアタッチされている必要があります。トラフィックのリダイレクトは、コントラクトにある送信元 EPG、接続先 EPG、フィルタ（プロトコル、送信元レイヤ 4 ポート、接続先レイヤ 4 ポート）の設定に基づいて行われます。

たとえば、PBR サービスグラフを使用するコントラクト A が L3Out EPG と EPG-A の間にある場合、L3Out EPG サブネットと EPG-A にあるエンドポイントの間のトラフィックのみがサービスノード FW1 にリダイレクトされます。別の EPG である EPG-B が別のコントラクト B を使用して同じ L3Out インターフェイスと通信する場合は、別のアクションを設定して、別のサービスノードである FW2 へリダイレクトすることも、L3Out インターフェイスに直接トラフィックを転送することもできます（図 2）。

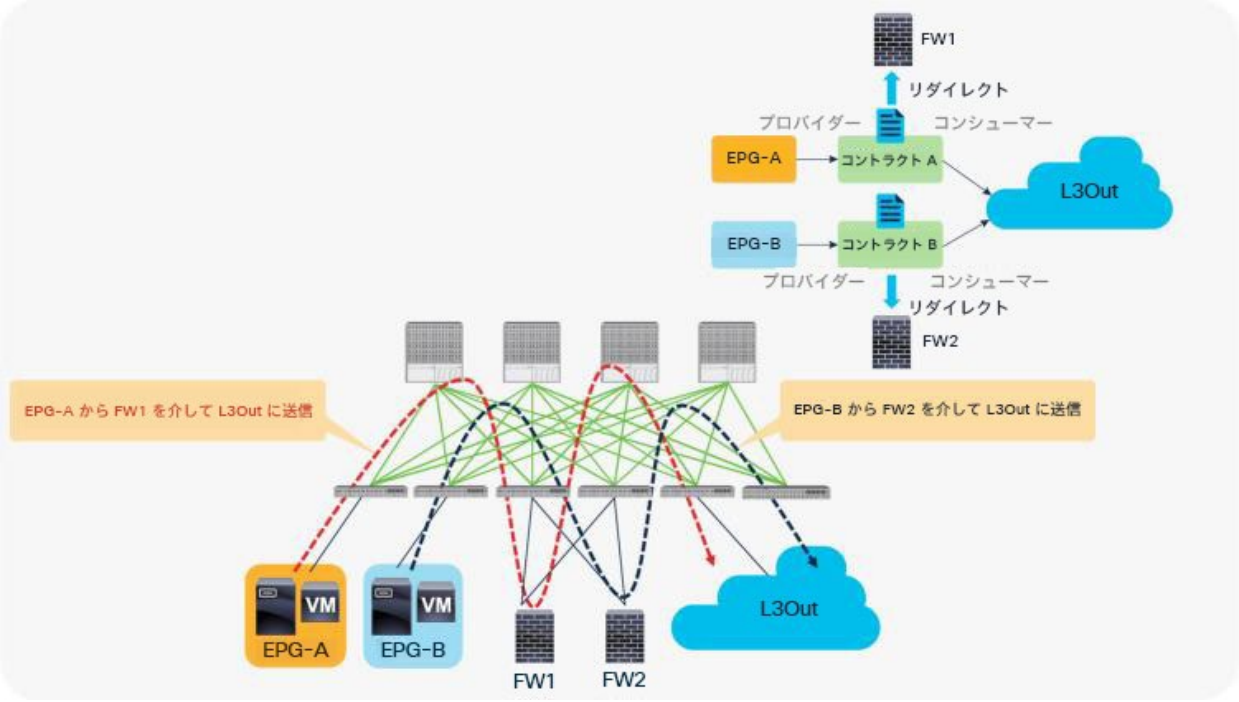


図 2.
例：送信元と接続先の EPG の組み合わせに基づいて異なる PBR ポリシーを使用

さらに、コントラクトでさまざまなフィルタを使用することで、異なる L4-L7 デバイスにトラフィックを送信できます。Cisco ACI では、フィルタはサブジェクトに分類されます。サブジェクトを組み合わせたものがコントラクトです。サービスグラフは、常に、コントラクトの配下にあるサブジェクトに適用する形で展開されます。コントラクト 1 で、HTTP を許可するサブジェクト 1 に PBR サービスグラフがあり、すべてを許可するサブジェクト 2 に PBR サービスグラフがない場合、HTTP トラフィックのみがリダイレクトされます。典型的なユースケースとしては、パケット内のデータを検査する必要がある IPS デバイスやディープ パケット インスペクション（DPI）デバイスの挿入があります。データが暗号化されている場合、そのトラフィックを IPS にリダイレクトしても、サービスデバイスのリソースが消費されるだけでメリットはありません。サービスグラフを使用してリダイレクトする場合、暗号化されていないトラフィックのみをリダイレクトするようにコントラクトを設定できます（図 3）。

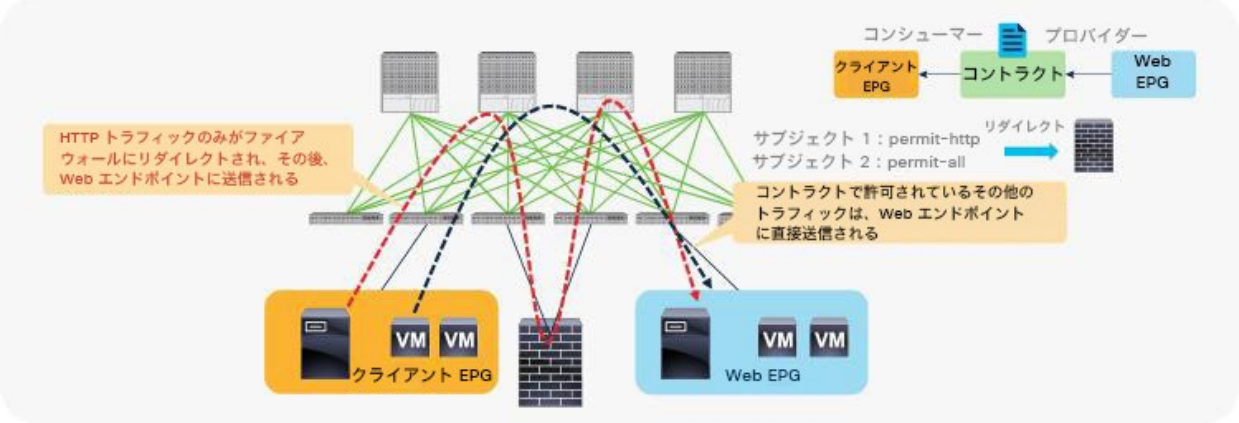


図 3.
例：コントラクトフィルタに基づいて異なる PBR ポリシーを使用

要件と設計上の考慮事項

このセクションでは、Cisco ACI PBR の要件と設計上の考慮事項について説明します。このドキュメントでは、PBR 機能を備えたサービスグラフのデバイスを PBR ノードと呼び、PBR ノードインターフェイスを含むブリッジドメインを PBR ノードブリッジドメインと呼びます。

Cisco ACI PBR の主な機能は次のとおりです。

- PBR は、物理サービスアプライアンスと仮想サービスアプライアンスの両方に対応しています。
- PBR は、管理対象モード（サービスポリシーモード）と非管理対象モード（ネットワークポリシーモード）の両方のサービスグラフに対応しています。
- PBR は、双方向コントラクトと単方向コントラクトの両方に対応しています。
- PBR は、L3Out EPG と EPG との間、EPG 間、L3Out EPG 間で使用できます。L2Out EPG がコントラクトに含まれている場合、PBR はサポートされません。
- PBR は、Cisco ACI のマルチポッド、マルチサイト、リモートリーフの各環境でサポートされています。
- 複数の L4-L7 デバイスに負荷を分散できます（対称 PBR）。

Cisco ACI PBR の主なユースケースは次のとおりです。

- PBR を使用して、ファイアウォールまたはロードバランサをエンドポイント間のパスに挿入します。一方で、分散ルーティングを使用するために Cisco ACI ファブリックにデフォルトゲートウェイを残します。
- PBR を使用して、同じサブネット内にあるエンドポイント間のパスに L4-L7 デバイスを挿入します。
- PBR を使用して、プロトコルとポートによるフィルタリングに基づいてトラフィックを L4-L7 デバイスに選択的に送信します。
- 対称 PBR を使用して、L4-L7 デバイスのパフォーマンスを水平方向に拡張します。

ルーテッドモードデバイス（L3 PBR）を使用する場合の Cisco ACI PBR の主な要件は次のとおりです。

- Cisco APIC リリース 2.0(1m) 以降を使用する必要があります。
- Cisco ACI ファブリックは、サーバーと PBR ノードのゲートウェイである必要があります。
- L4-L7 デバイスは、Go-To モード（ルーテッドモード）で展開する必要があります。
- PBR ノードインターフェイスは、FEX ホストインターフェイスの下ではなく、リーフ ダウンリンク インターフェイスの下に接続する必要があります。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は、FEX ホストインターフェイスの下に接続できます。
- PBR ノードインターフェイスは、L3Out ではなく、ブリッジドメインにある必要があります。APIC リリース 5.2 より新しいリリースの場合、この要件は L3 PBR に必須ではありません。L3 PBR ノードインターフェイスが L3Out にあっても問題ありません。
- コンシューマーまたはプロバイダーのブリッジドメインを PBR ノードブリッジドメインにすることはできません。そのため、専用のサービスブリッジドメインが必要です。APIC リリース 3.1 以降のリリースでは、この要件は必須ではありません。コンシューマーまたはプロバイダーのブリッジドメインを PBR ノードブリッジドメインにすることができます。
- APIC リリース 3.1 より前のリリースでは、PBR ノードがアタッチされているブリッジドメインのデータプレーン学習を管理者が無効化する必要があります。APIC リリース 3.1 以降のリリースで Cisco Nexus 9300-EX および -FX プラットフォーム リーフ スイッチ以降を使用する場合、PBR ノードインターフェイスがアタッチされている BD のデータプレーン IP 学習を管理者が無効化する必要はありません。
- 管理者は、APIC 設定で PBR ノードの IP アドレスと MAC アドレスを入力する必要があります。APIC リリース 5.2 以降のリリースでは、IP-SLA トラッキングが有効になっていれば、L3 PBR の MAC アドレスを設定する必要はありません。
- 対称 PBR（PBR ポリシーごとに複数の PBR 接続先がある）では、Cisco Nexus 9300-EX および -FX プラットフォーム リーフ スイッチ以降が必要です。
- PBR ノードブリッジドメインと PBR ノードの L3Out は、コンシューマーのブリッジドメイン（EPG）またはプロバイダーのブリッジドメイン（EPG）と同一の VRF インスタンスに属している必要があります。

ルーテッドモードデバイス（L3 PBR）を使用する場合の Cisco ACI PBR における設計上の考慮事項は次のとおりです。

- ファブリックが、Cisco Nexus 93128TX、93120TX、9396TX、9396PX、9372PX、9372PX-E、9372TX、9372TX-E などの第 1 世代の Cisco Nexus 9300 プラットフォームスイッチで構成されている場合、PBR ノードをコンシューマー EPG またはプロバイダー EPG と同じリーフノードの下に置くことはできません。
- APIC リリース 5.2 より前のリリースでは、PBR 接続先の動的 MAC アドレス検出がサポートされていません。したがって、アクティブ/スタンバイの高可用性を展開する場合、L4-L7 デバイスに仮想 IP アドレスと仮想 MAC アドレスを設定する必要があります。仮想 IP アドレスおよび仮想 MAC アドレスは、それぞれフローティングアドレスとして定義されるため、L4-L7 のアクティブノードがダウンすると、スタンバイノードに引き継がれます。
- 一般的に、L4-L7 デバイスのフェールオーバーには GARP が使用されるため、PBR ノードブリッジドメインで GARP ベースの検出を有効にすることをお勧めします。

- PBR ノードが HSRP、VRRP、IPv6 NS などのリンクローカル マルチキャスト パケットを交換する場合、リンクローカル マルチキャスト パケットの交換を想定している各 PBR ノードペアは、異なるリーフの下にある必要があります。これは、CSCvq57414 および CSCvq76504 の問題があるためです。
- APIC リリース 3.2 より前のリリースでは、サービスグラフの 1 つのノードでのみ PBR を使用できます。APIC リリース 3.2 以降のリリースでは、サービスグラフの複数のノードで PBR を使用できます。
- APIC リリース 3.2 より前のリリースでは、Cisco ACI マルチサイト環境で PBR がサポートされていません（異なるサイトにある EPG の間のコントラクトで PBR がサポートされていません）。APIC リリース 3.2 では、Cisco ACI マルチサイト環境で 1 ノードのファイアウォール PBR がサポートされます。 2 ノード PBR サービスグラフ（たとえばファイアウォールとロードバランサ）は、APIC リリース 4.0 でサポートされています。
- APIC リリース 3.2 より前のリリースでは、vzAny をプロバイダーとするコントラクトに PBR が設定されたサービスグラフを関連付けることはできません。APIC リリース 3.2 以降のリリースでは、vzAny をプロバイダーとするコントラクトで PBR がサポートされます。
- APIC リリース 4.0 より前のリリースでは、サービスグラフを EPG 内コントラクトに関連付けることはできません。APIC リリース 4.0 以降のリリースでは、EPG 内コントラクトを使用した PBR がサポートされます。APIC リリース 5.2 以降では、外部 EPG 内コントラクトを使用した PBR がサポートされます。

APIC リリース 4.1 以降では、インライン IPS、トランスペアレント ファイアウォール（FW）といった L1 デバイスまたは L2 デバイスで PBR を使用できます。L1/L2 モードデバイス（L1/L2 PBR）を使用する場合の Cisco ACI の主な要件は次のとおりです。

- APIC リリース 4.1 以降を使用する必要があります。
- L1/L2 PBR では、Cisco Nexus 9300-EX および -FX プラットフォーム リーフ スイッチ以降が必要です。
- Cisco ACI ファブリックは、サーバーと PBR ノードのゲートウェイである必要があります。
- L4-L7 デバイスは、物理ドメインに L1 モードまたは L2 モードで展開する必要があります。
- L1/L2 PBR ノードインターフェイスは、L3Out ではなく、ブリッジドメインにある必要があります。PBR ノードブリッジドメインは、専用の BD である必要があります。他のエンドポイントや他の L4-L7 デバイスのインターフェイスと共有できません。
- PBR ノードブリッジドメインは、コンシューマーのブリッジドメイン（EPG）またはプロバイダーのブリッジドメイン（EPG）と同一の VRF インスタンスに属している必要があります。
- L1/L2 デバイスはツーアームモードにする必要があります。L1/L2 デバイスのコンシューマーコネクタとプロバイダーコネクタは、異なる BD に存在する必要があります。
- L1 デバイスのコンシューマーコネクタとプロバイダーコネクタは、異なるリーフノードに接続する必要があります。ポート単位の VLAN はサポートされていません。L2 デバイスではこの点を考慮する必要はありません。

L1/L2 モードデバイス（L1/L2 PBR）を使用する場合の Cisco ACI における設計上の考慮事項は次のとおりです。

- L1/L2 PBR は、非管理対象モードのサービスグラフでのみサポートされます。

- APIC リリース 5.0 より前のリリースでは、L1/L2 PBR はアクティブ/スタンバイモードのみをサポートします。ACI リリース 5.0 より前のバージョンの ACI を使用する場合、L1/L2 PBR のアクティブ/アクティブ展開はサポートされません。これは L3 PBR と異なる点です。つまり、設定できる L1/L2 接続先の数は、PBR 接続先グループごとに最大 2 つです（つまり L4-L7 デバイスが最大 2 つ）。APIC リリース 4.1 および 4.2 では、同じ PBR 接続先グループ内に 3 つ以上の L4-L7 デバイスを設定することはできません。アクティブ/スタンバイモードでは PBR トラッキングが必要です。アクティブ/アクティブモードがサポートされないため、しきい値は適用されません。トラッキングが有効化されている場合、ダウンアクションは拒否されます。ダウンアクション「許可」は、APIC リリース 4.1 では設定できません。
- APIC リリース 5.0 以降では、L1/L2 PBR は対称 PBR のアクティブ/アクティブ展開もサポートします。APIC リリース 5.0 では、対称 PBR 関連機能として、しきい値、ダウンアクション、バックアップ PBR ポリシー（N+M 高可用性）などがサポートされます。L1 PBR アクティブ/アクティブモードの場合、各 L4-L7 デバイスのコンシューマーとプロバイダーのインターフェイス（コンシューマーコネクタとプロバイダーコネクタ）は、異なる物理ドメインにある必要があります。
- L2 Ping（Ethertype 0x0721）がトラッキングに使用されます。L2 Ping は、リーフノード間で交換され、サービスデバイスを通過します。したがって、L1/L2 モードで動作する L4-L7 デバイスは、Ethertype 0x0721 を許可する必要があります。
- リーフポートと L1/L2 PBR 接続先の間に中間スイッチが接続されている場合、中間スイッチは PBR 接続先 MAC を持つトラフィックを伝送できる必要があります。 L2 Ping のために Ethertype 0x0721 を許可することに加えて、中間スイッチで静的 MAC 設定または無差別モード設定が必要になる場合があります。
- L1/L2 PBR は、マルチポッド、マルチサイト、リモートリーフの展開で使用できます。L1/L2 PBR アクティブ/アクティブ設計の場合、「Flood in Encap」がリモートリーフでサポートされていないため、PBR 接続先をリモートリーフに接続できません。この場合でも、プロバイダーとコンシューマーはリモートリーフに接続できます。
- マルチノード PBR がサポートされます。L1/L2 モードで動作する L4-L7 デバイスと L3 モードで動作する L4-L7 デバイスを 1 つのサービスグラフで混在させることができます。
- ワンアームモードが必要なため、vzAny コントラクトまたは EPG 内コントラクトで PBR はサポートされません。

L1/L2 PBR と L3 PBR の両方に適用される Cisco ACI PBR に関する設計上の考慮事項は次のとおりです。

- コントラクトはユニキャストトラフィックにのみ適用されるため、マルチキャストトラフィックとブロードキャスト トラフィックのリダイレクトはサポートされません。
- リダイレクト、コピー、拒否などのユーザー定義のコントラクトアクションは、特定のタイプのパケットには適用できません。詳細については、ACI コントラクトガイドのよくある質問（FAQ）を参照してください。
- ARP、ND-Sol ICMPv6、ND-Advt ICMPv6 トラフィックなどの非 IP トラフィックとコントロール プレーン トラフィックに PBR を適用することは想定されていません。したがって、ARP、イーサネットトラフィックなどの非 IP トラフィックを含む共通デフォルトフィルタを PBR に使用しないでください。その一例をこのドキュメントで後ほど説明します。IPv6 トラフィックの場合は、デフォルト以外のフィルタを使用する場合でも、ND-Sol ICMPv6 および ND-Advt ICMPv6 トラフィックを PBR を使用するコントラクトサブジェクトから除外する必要があります。IP と IPv6 のイーサタイプには ICMPv6 が含まれているためです。

- サービスデバイスのモデルによって 高可用性（HA）/クラスタリングメカニズムは異なりますが、一般的に、PBR が適用される HA/クラスタリングの通信とデータトラフィックに個別のセグメント（BD）を使用することをお勧めします。
- 一般的に、多くの EPG を同じコントラクトのコンシューマーやプロバイダーにするのではなく、vzAny コントラクトを使用して、多数の EPG から多数の EPG へのトラフィックに PBR を適用することをお勧めします*。
- PBR はブリッジングされたトラフィックにも適用できます。送信元エンドポイントと接続先エンドポイントが 1 つの L3 ブリッジドメインにある場合、両者は同じサブネットに属します。送信元と接続先が同じサブネットにある場合でも、元の送信元 MAC が保持されず、TTL が減算されます。これは、PBR ポリシーが適用されると ACI ファブリックがトラフィックをルーティングするためです（ルーティングなので、ACI ファブリックが接続先 MAC アドレスを PBR 接続先 MAC アドレスに書き換えます）。
- PBR は、アウトオブバンド（oob）管理 EPG またはインバンド（inb）管理 EPG を含むトラフィックではサポートされません。管理 EPG が事前定義された oob VRF、inb VRF、ユーザー定義 VRF のいずれにあっても同様です。これは、管理 EPG では「許可」と「拒否」のコントラクトアクションのみがサポートされるためです。
- 同じサービスグラフで使用される L4-L7 デバイス（PBR 接続先または PBR ノードとも呼ばれる）は、リモートリーフノードとメインロケーションに分散して配置することはできません。
- 複数の PBR ポリシーが同じ VRF にある同じ PBR 接続先 IP を共有する場合、その PBR 接続先に対して同じ IP-SLA ポリシー、ヘルスグループ、ポッド ID 認識リダイレクト設定を使用する必要があります。これは、PBR 接続先が（VRF、IP）をトラッキングステータスと設定のキーとして使用するためです。例については、このドキュメントで後ほど説明します。
- TCAM 圧縮（以前はコントラクトフィルタの「no stats」オプションと呼ばれていた「ポリシー圧縮の有効化」）は、リダイレクトルールが設定されたゾーン分割ルールには適用されません。つまり、コントラクト/フィルタがある場合の TCAM 使用率を最適化する機能は、サービスグラフリダイレクト（PBR）の目的に使用されるコントラクト/フィルタルールには適用されません。
- APIC リリース 4.2(6) および 5.0(1) 以降では、コントラクトと EPG が同じテナントにある場合、サービスグラフとコントラクトの継承がサポートされます。

*注：この推奨事項は、多くのプロバイダー EPG とコンシューマー EPG が関わるコントラクトの設定変更に与える影響の大きさを考慮して設けられています。APIC における 1 つの設定変更が同時に複数のゾーン分割ルールの変更に関連する場合、特定のリーフノードのハードウェアに対するプログラミングを完了するのに時間を要する場合があります。ACI コントラクトガイドの「Scalability Considerations」セクションを参照してください。

APIC リリース 5.2 以降では、L3 PBR 接続先を L3 ブリッジドメインではなく L3Out に置くことができます。L3Out にある PBR 接続先に関する主な要件は次のとおりです。

- APIC リリース 5.2 以降を使用する必要があります。
- PBR 接続先がある L3Out は、コンシューマーのブリッジドメイン（EPG）またはプロバイダーのブリッジドメイン（EPG）と同一の VRF インスタンスに属している必要があります。
- IP-SLA トラッキングは必須です。
- 0.0.0.0/0 または 0::0 の L3Out EPG は、PBR 接続先の L3Out EPG としては使用できません。

L3Out にある PBR 接続先に関する設計上の考慮事項は次のとおりです。

- SVI、ルーテッド サブインターフェイス、またはルーテッドインターフェイスを使用する L3Out がサポートされます（インフラ L3Out、GOLF L3Out、SDA L3Out、または PBR 接続先にフローティング SVI を使用する L3Out はサポートされません）。
- シングルポッド、マルチポッド、リモートリーフがサポートされます。APIC リリース 5.2 では、マルチサイトはサポートされません。
- マルチノード PBR がサポートされます。
- コンシューマー EPG またはプロバイダー EPG が L3Out EPG である場合、これを PBR 接続先と同じ L3Out の下に置くことはできません。
- コンシューマー EPG またはプロバイダー EPG が L3Out EPG である場合、これを PBR 接続先の L3Out があるサービスリーフノードの下に置くことはできません。コンシューマー EPG またはプロバイダー EPG が L3Out EPG ではなく通常の EPG である場合、コンシューマー、プロバイダー、PBR 接続先の L3Out を同じリーフの下に置くことができます。この考慮事項は、コンシューマー EPG またはプロバイダー EPG が、L3Out にある PBR 接続先が有効化されている別のサービスデバイスを介して、目的のサービスデバイスの L3Out EPG と通信する場合に適用されます。以下にその例を示します。
- コンシューマー EPG と L3Out の背後にあるロードバランサの VIP との間のトラフィックをリダイレクトするために、L3Out にある PBR 接続先がファイアウォールで有効化されています。
  - サービスグラフは 2 ノードで、最初のノードとしてファイアウォールが、2 番目のノードとしてロードバランサがあります。
  - ファイアウォールとロードバランサは、L3Out（L3Out-FW および L3Out-LB）を介して接続されています。
  - コンシューマー EPG とロードバランサの VIP の間のトラフィックは、この考慮事項に該当します。これは、L3Out にある PBR 接続先が、コンシューマー EPG と VIP（L3Out-LB EPG）間のトラフィックに対して有効化されているためです。L3Out-FW と L3Out-LB を同じリーフノードの下に置くことはできません。
- サービスデバイスが ツーアームモードで、PBR 接続先の L3Out の 1 つが 0.0.0.0/0 または 0::0 ルートを学習する場合、サービスデバイスの両方のアームを同じリーフノードまたは同じ vPC ペアに接続する必要があります。
- サービスグラフの同じ機能ノード内で、L3 ブリッジドメインにある PBR 接続先と L3Out にある PBR 接続先を混在させることはできません。以下にその例を示します。
  - 次の構成はサポートされて**いません**。
  - 機能ノード 1 のコンシューマーコネクタは BD1 にある（PBR が有効）
  - 機能ノード 1 のプロバイダーコネクタは L3Out1 にある（PBR が有効）
  - 次の構成はサポートされて**います**。
  - 機能ノード 1 のコンシューマーコネクタは BD1 にある（PBR は有効化されていない）
  - 機能ノード 1 のプロバイダーコネクタは L3Out1 にある（PBR が有効）

- VRF 間コントラクトには次の考慮事項があります。
  - EPG コントラクト：PBR 接続先の L3Out が VRF 間コントラクトのプロバイダー VRF にある場合、L3Out EPG サブネットをコンシューマー VRF にリークする必要があります。そうしないと、コンシューマー VRF には PBR 接続先へのルートがなく、プロバイダー VRF にはプロバイダー VRF にある PBR 接続先からコンシューマー EPG へのトラフィックに対する許可ルールがありません（PBR 接続先が BD にある場合、PBR 接続先のサービスブリッジドメイン（BD）をコンシューマー VRF にリークする必要はありません）。
  - ESG コントラクト：L3Out EPG がコンシューマー VRF にあるかプロバイダー VRF にあるかに関係なく、L3Out EPG サブネットを他方の VRF にリークする必要があります。
- バイパス機能には既知の警告（CSCvy31805）があります。
- L3Out にある PBR 接続先を含む vzAny 対 vzAny のコントラクトがサポートされます。PBR 接続先の L3Out EPG は VRF の vzAny の一部でもあるため、vzAny 対 vzAny のコントラクトよりも優先度が高い別のコントラクトを用意して、送信元 IP が PBR 接続先の L3Out EPG と一致するトラフィックがリダイレクトされないようにする必要があります。

特に断りのない限り、このドキュメントに記載されているトポロジと設計の例は、L3 PBR に関する例です。

このドキュメントでは、単一ポッドに関する設計上の考慮事項について主に説明します。マルチポッド環境とマルチサイト環境の詳細については、マルチポッドサービス統合に関する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-c11-739571.html.

トポロジの例

このセクションでは、PBR のトポロジの例を示します。詳細については、このドキュメントで後ほど説明します。

図 4 の最初の例は、1 ノードファイアウォールを挿入する典型的なユースケースを示しています。PBR ノードはレイヤ 3 ノードです。APIC リリース 3.1 より前のリリースでは、コンシューマー EPG またはプロバイダー EPG を含むコンシューマーのブリッジドメインまたはプロバイダーのブリッジドメインを PBR ノードブリッジドメインにすることはできません。そのため、下の図 4 に示すように、PBR ノード用に別のブリッジドメインとサブネット範囲を用意する必要があります。APIC リリース 3.1 以降のリリースでは、この要件は必須ではありません。詳細については、「PBR ノード、コンシューマー EPG、プロバイダー EPG を同じサブネットに配置する設計」セクションを参照してください。

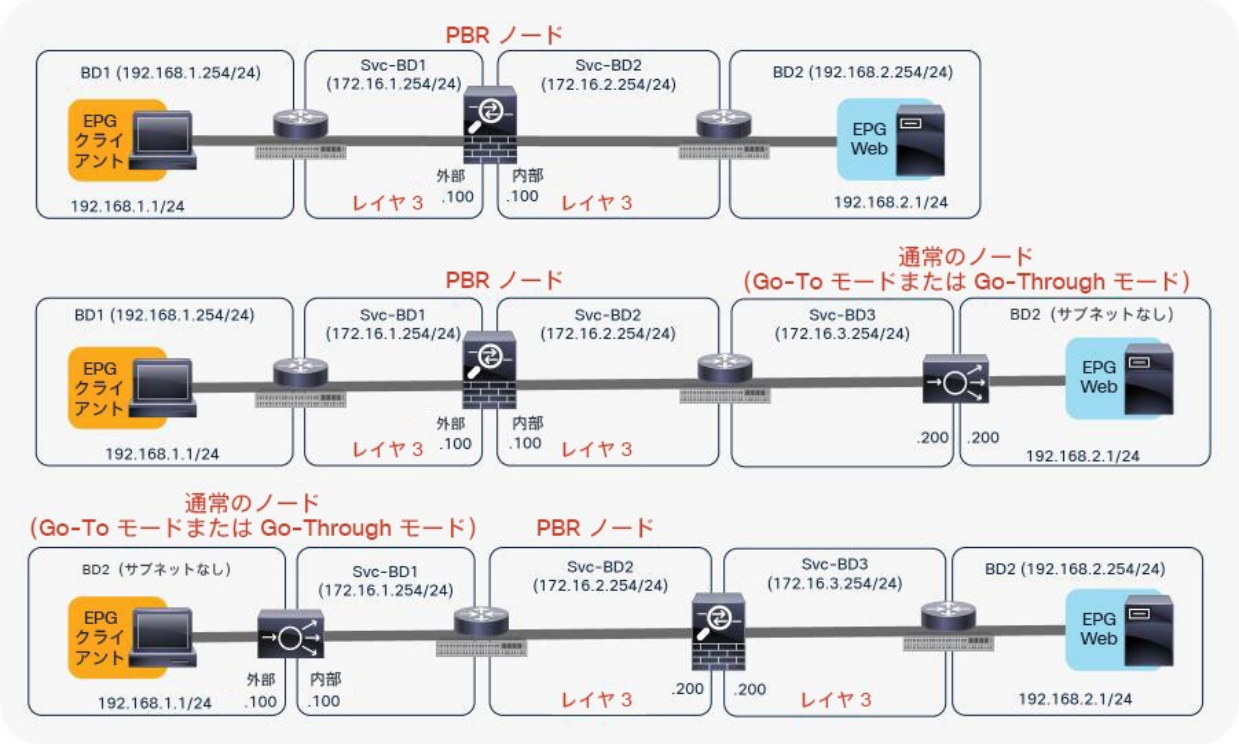
2 つ目と 3 つ目の例は、2 ノードのサービスグラフの例です。APIC リリース 3.2 より前のリリースでは、2 ノードのサービスグラフがある場合、2 つのノードうちいずれかのみを PBR ノードにできます。非 PBR ノードは、コンシューマー EPG またはプロバイダー EPG と同じブリッジドメインに置くことができます。APIC リリース 3.1 より前のリリースでは、PBR ノードは、専用のサービスブリッジドメインに置く必要があります。4 つ目の例は、共用のサービスブリッジドメインに置かれた PBR ノードの例です。APIC リリース 3.2 以降では、マルチモード PBR が導入されています。これにより、1 つのサービスグラフで PBR を複数回使用できます。詳細については、「PBR が設定されたマルチノードのサービスグラフ」セクションを参照してください。

5 つ目の例は L1/L2 PBR の例です。APIC リリース 4.1 より前のリリースでは、PBR ノードは L3 デバイスである必要があります。APIC リリース 4.1 以降では、L1/L2 デバイスへ PBR が導入されています。詳細については、「L1/L2 PBR」セクションを参照してください。

6 つ目の例は、もう一方のコネクタが L3Out にある単方向 PBR の例です。APIC リリース 4.1.2 より前のリリースでは、PBR ノードのコンシューマーコネクタとプロバイダーコネクタのどちらか一方のみで PBR が有効化されている場合でも、両方のコネクタを L3Out ではなくブリッジドメインに置く必要があります。APIC リリース 4.1.2 以降では、この要件は必須ではありません。PBR が有効化されていないコネクタに L3Out を使用できます。詳細については、「もう一方のコネクタが L3Out にある単方向 PBR」セクションを参照してください。

7 つ目の例は、PBR 接続先が L3Out にある例です。APIC リリース 5.2 より前のリリースでは、コネクタで PBR が有効化されている場合、PBR 接続先は L3Out ではなくブリッジドメインにある必要があります。APIC 5.2 以降では、この要件は必須ではありません。L3 PBR 接続先を L3Out に置くことができます。詳細については、「L3Out にある PBR 接続先」セクションを参照してください。

これらはツーアームモードの PBR ノードの例ですが、L1/L2 PBR を除き、ワンアームモードの PBR ノードを展開することもできます。サービスグラフの設計の詳細については、このドキュメントで後ほど説明します。



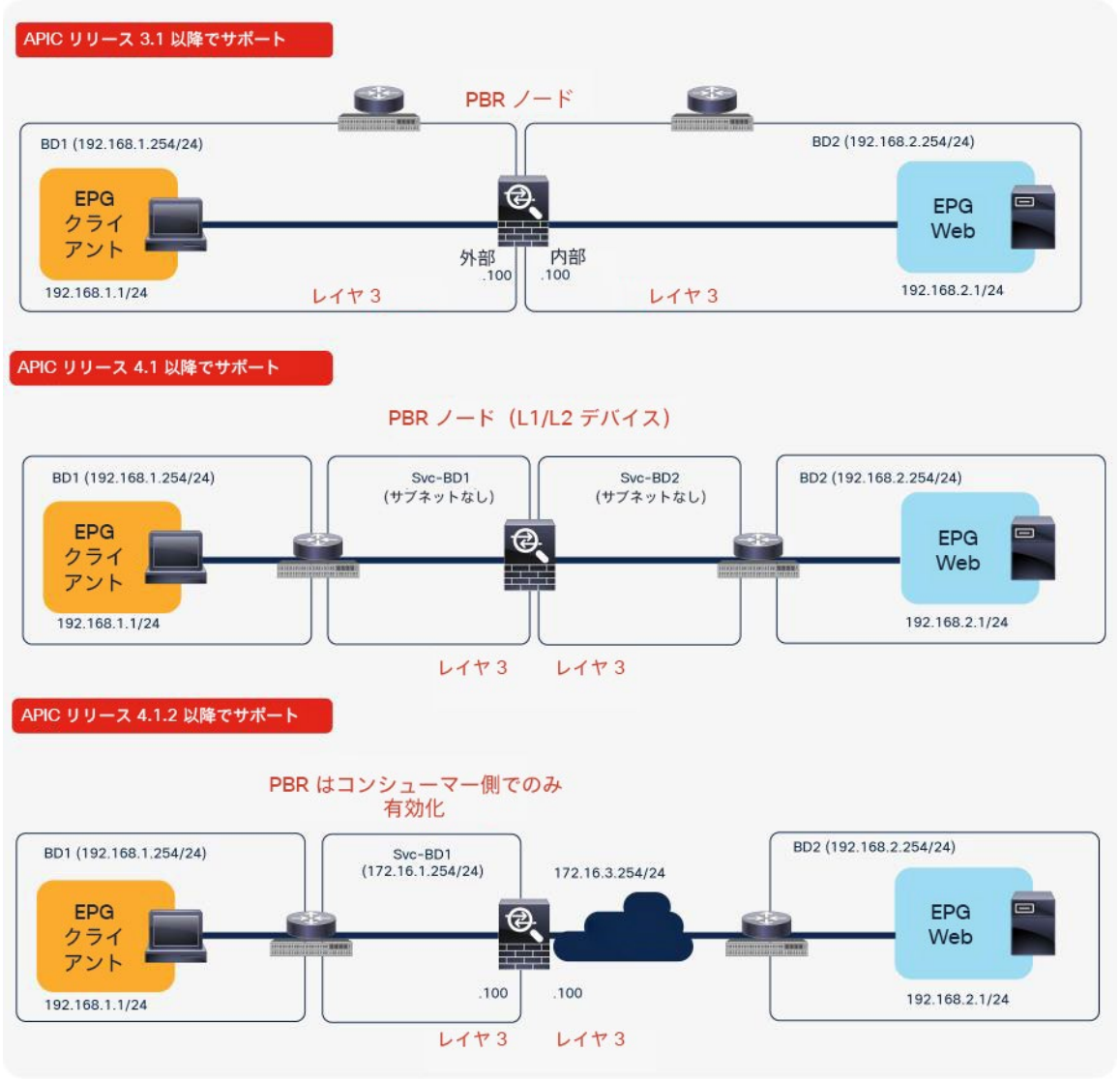


図 4.
サポートされるトポロジの例

PBR ノードは、VRF インスタンスの間に置くことも、いずれかの VRF インスタンスの内部に置くこともできます。PBR ノードは、コンシューマー VRF インスタンスまたはプロバイダー VRF インスタンスに置く必要があります（図 5）。たとえば、PBR ノードを、コンシューマー VRF インスタンスでもプロバイダー VRF インスタンスでもない VRF3 に置くことはできません。

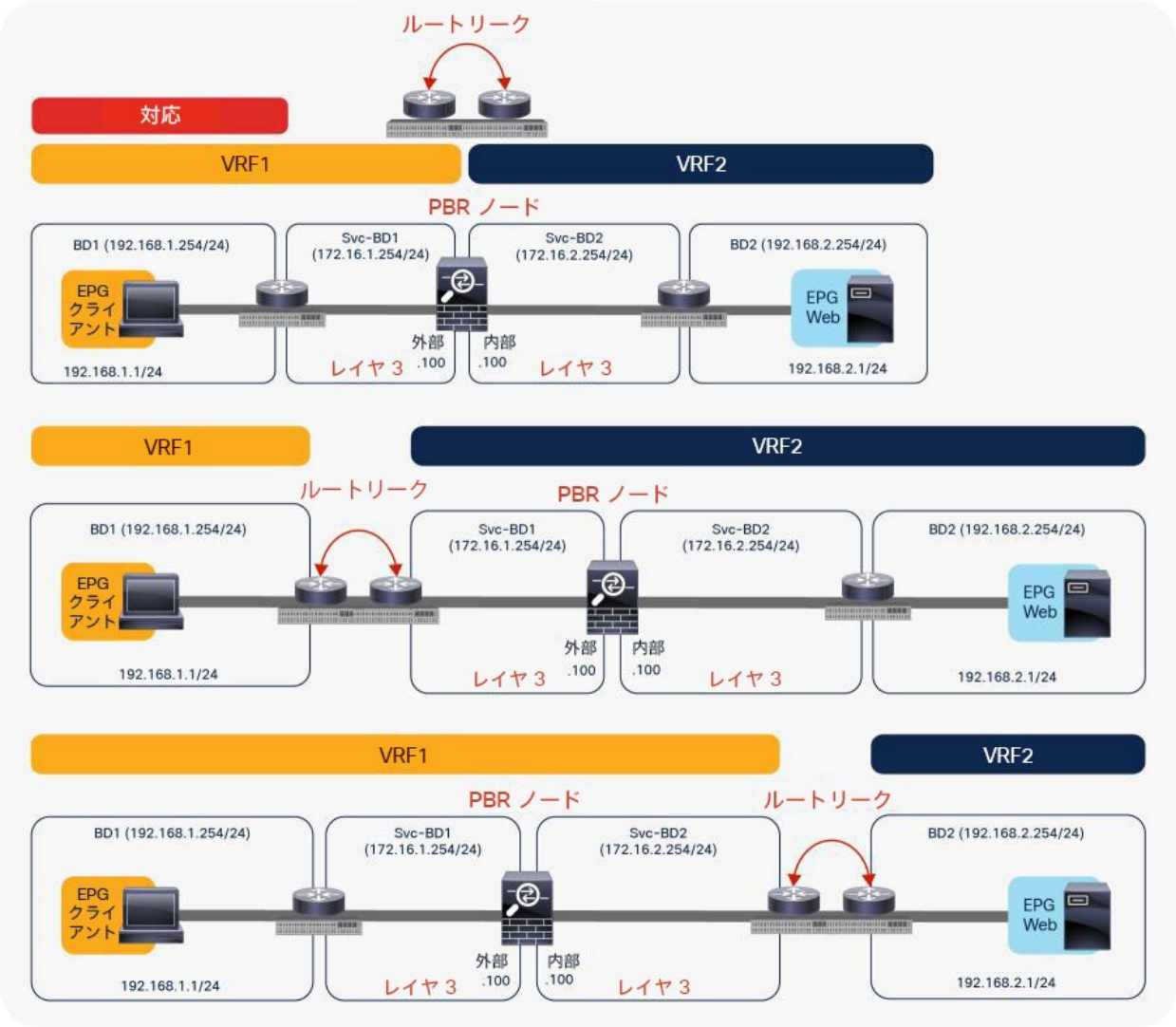


図 5.
サポートされるトポロジの例（VRF サンドイッチ設計）

図 6 に、サポートされないトポロジの例を示します。PBR ノードは、L2 ブリッジドメインではなく、L3 ブリッジドメインにあることが必要です。

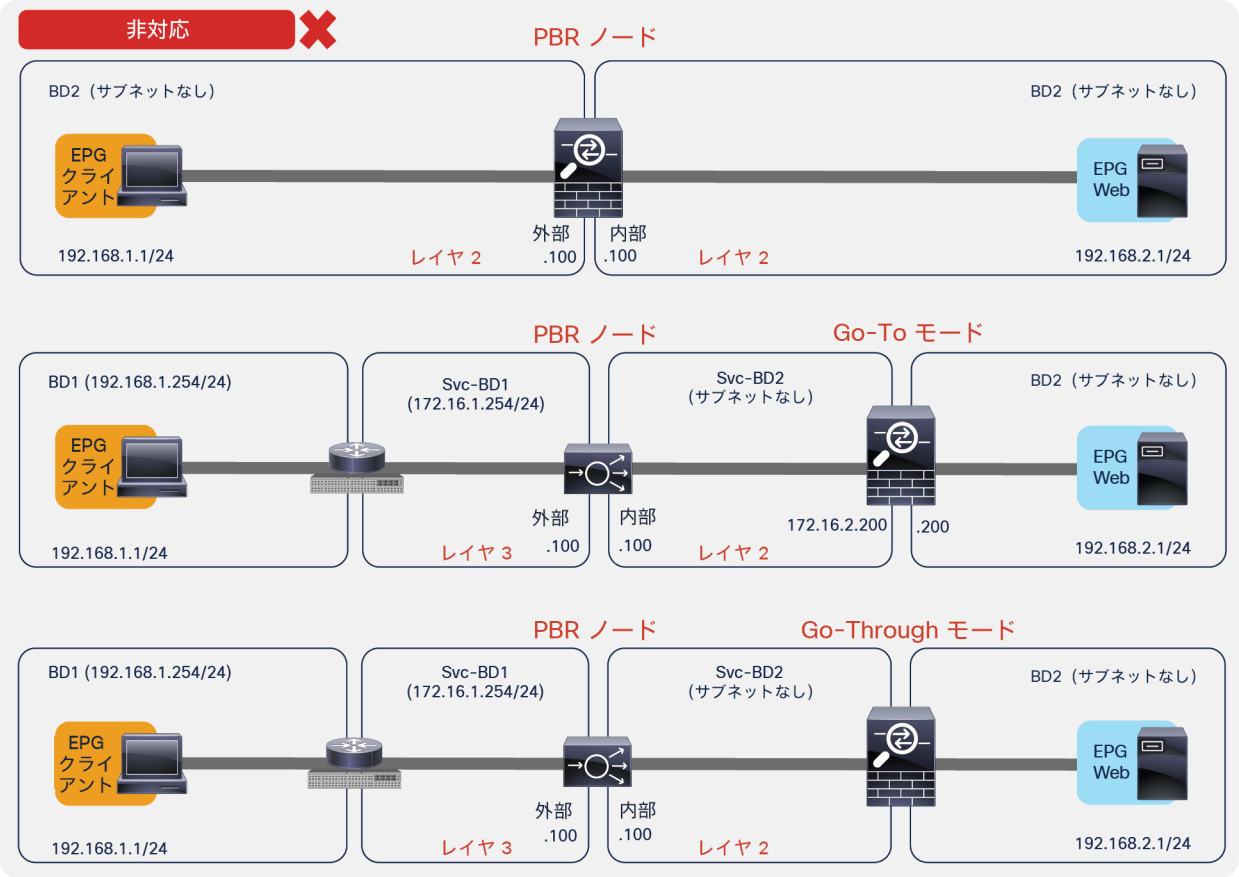


図 6.
サポートされないトポロジの例（PBR ノードは L3 ブリッジドメインにあることが必要です）

PBR ノードのエンドポイント データプレーン学習の設定

PBR が設定されたサービスグラフを展開する場合は、L4-L7 デバイスを L3 ブリッジドメインまたは L3Out に接続する必要があります。このブリッジドメインでは、エンドポイント データプレーン IP 学習を無効化する必要があります。図 8 でこの内容を説明しています。この図は、クライアント EPG と Web EPG の間に PBR ノード（ファイアウォール）が挿入された双方向 PBR を示しています。

このセクションでは、PBR ノードブリッジドメインのエンドポイント データプレーン IP 学習を無効化する必要性について説明します。L3Out にある PBR 接続先には適用されません。L3Out ドメインのデータプレーンからは IP アドレスを学習しないためです。

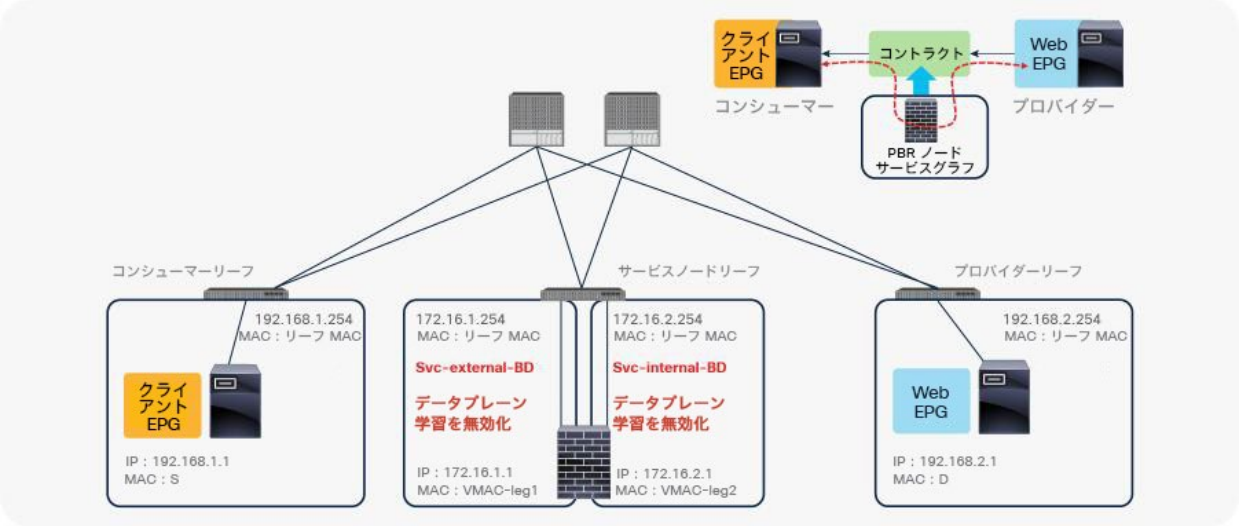


図 7.
PBR の設計例

エンドポイント データプレーン学習のオプションは、[テナント（Tenant）] > [ネットワーク（Networking）] > [ブリッジドメイン（Bridge Domains）] にあります（図 8）。デフォルト設定では有効化されています。このオプションでエンドポイント データプレーン IP 学習の有効または無効を設定できます。APIC リリース 5.0(1) 以降、このオプションは、ブリッジドメインの [ポリシー（Policy）] タブにある [詳細/トラブルシューティング（Advanced/Troubleshooting）] タブに移動しました。

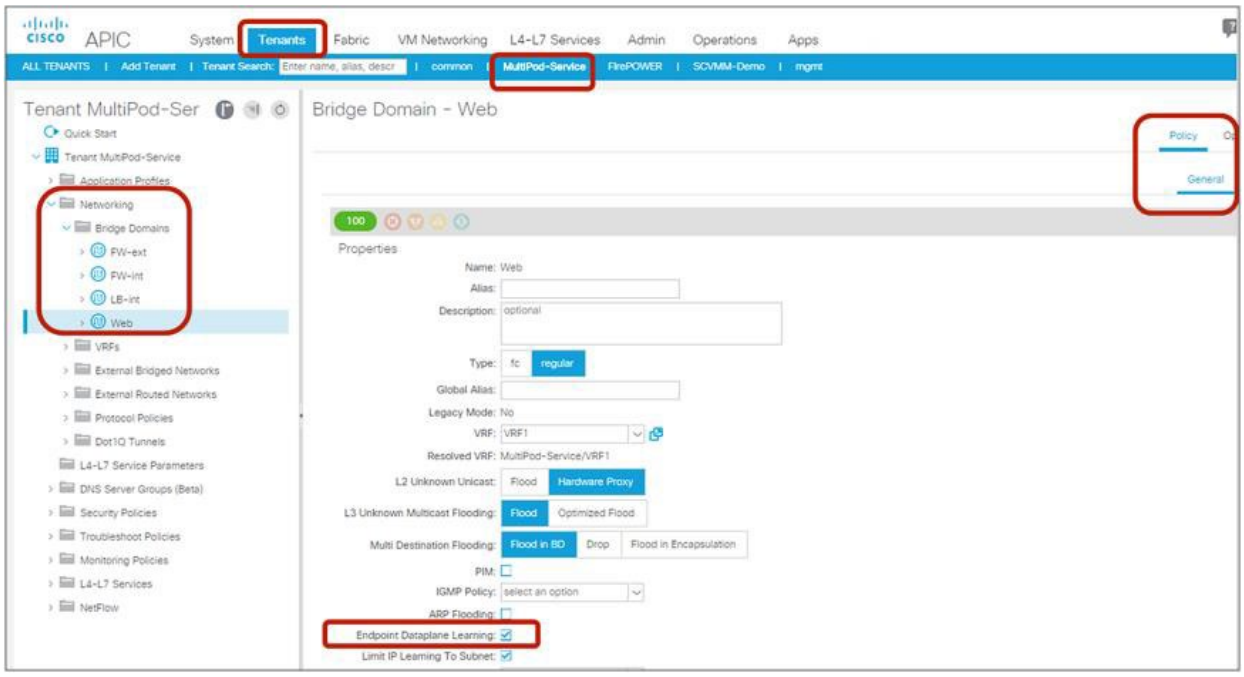


図 8.
ブリッジドメインのエンドポイント データプレーン学習の有効化と無効化

注： APIC リリース 3.1 より前のリリースでは、PBR ノードブリッジドメインのエンドポイント データプレーン学習の設定を無効化する必要があります。APIC リリース 3.1 以降では、PBR ノードブリッジドメインの設定は必須ではありません。PBR ノード EPG のエンドポイント データプレーン学習の設定は、サービスグラフのインスタンス化の段階で自動的に無効化されます。

PBR が設定されたサービスグラフを使用する場合にエンドポイント データプレーン IP 学習を無効化する必要があるのは、PBR ノードブリッジドメインでエンドポイント データプレーン学習を有効化しておくと、PBR トラフィックフローに関わるリーフノードで望ましくないエンドポイント学習動作が発生する可能性があるためです。

たとえば図 9 に示すように、PBR ノードから返されたトラフィックの送信元 IP アドレスは、PBR が適用された後も 192.168.1.1 のままです。したがって、プロバイダーリーフノードは、内部送信元 IP アドレスとして 192.168.1.1 を使用し、外部送信元 IP アドレスとしてサービスノードリーフの Virtual Extensible LAN（VXLAN）トンネルエンドポイント（VTEP）を使用したパケットを受信します。そのため、プロバイダーリーフノードは、実際には別のリーフノードの下に 192.168.1.1 が存在するにも関わらず、サービスノードリーフの VTEP IP アドレスを介して 192.168.1.1 を学習します。

PBR ノードのプロバイダー側のブリッジドメインである Svc-internal-BD でエンドポイント データプレーン学習を無効化すれば、プロバイダーリーフノードが PBR ノードからのトラフィックを介して 192.168.1.1 を学習することはありません。

この例では、トラフィックの対称性を維持するために、リターントラフィックに対する PBR も必要です。PBR が適用された後にコンシューマーリーフノードがサービスリーフノードを介して 192.168.2.1 を学習しないように、Svc-external-BD のエンドポイント データプレーン学習を無効化する必要があります。

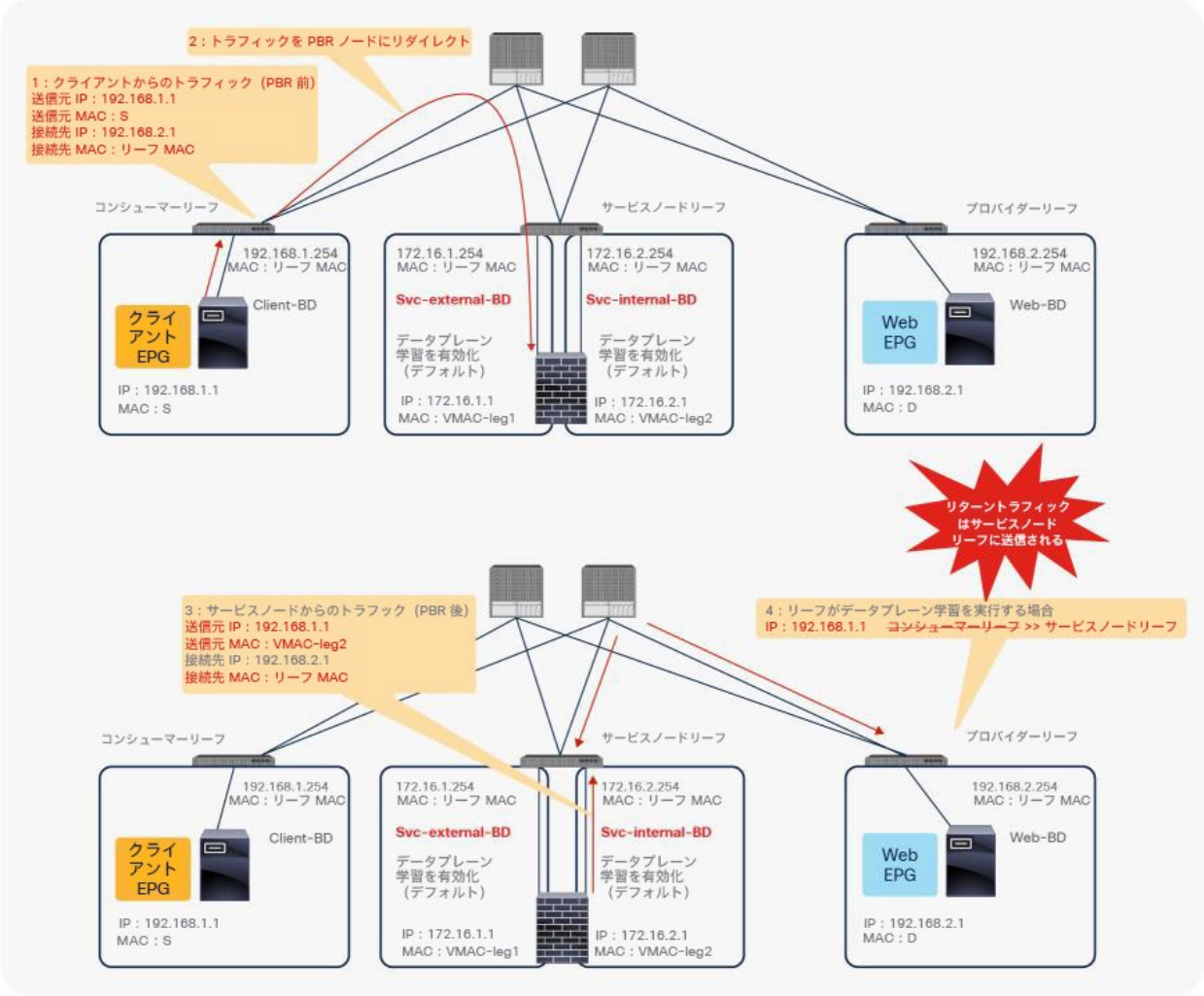


図 9.
PBR ノードブリッジドメインでデータプレーン学習を無効化する必要性

注：　プロバイダーリーフノードはコンシューマーエンドポイントを学習しませんが、スパインプロキシノードを使用してトラフィックを転送できます。

データプレーンのプログラミング

このセクションでは、PBR が設定されたサービスグラフが展開されると Cisco ACI ファブリックでポリシーがどのように更新されるかについて説明します。

概要

PBR ポリシーは、コンシューマーリーフノードとプロバイダーリーフノードでプログラムされます。たとえば、図 10 に示すように、コンシューマー、プロバイダー、サービスの各リーフノードがある場合、PBR ポリシーはリーフ 1 とリーフ 3 に設定され、リーフ 2 には設定されません。

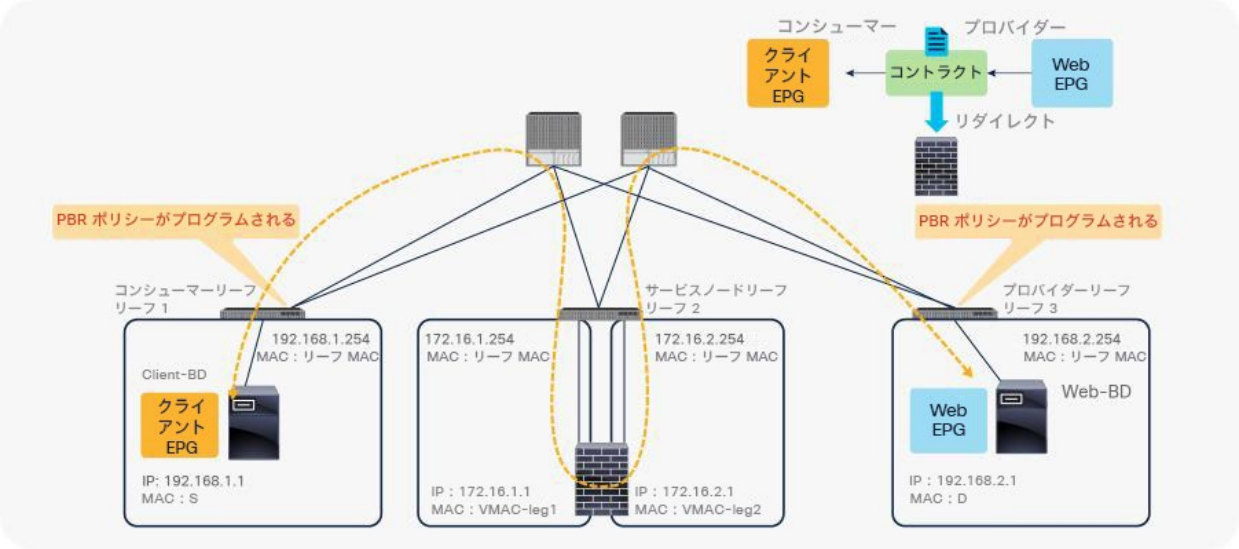


図 10.
トポロジの例

クライアント EPG（クラス ID 32774）と Web EPG（クラス ID 32771）の間のコントラクトにサービスグラフが適用される前の状態では、図 11 と表 1 に示すように、それらの間の許可エントリがリーフノードにプログラムされています（スコープ ID 2621442 は VRF ID）。

図 11.
サービスグラフが展開される前の状態

表 1. サービスグラフがない状態での許可ルール

送信元クラス ID	接続先クラス ID	フィルタ ID	アクション
32771（Web EPG）	32774（クライアント EPG）	38（コントラクトサブジェクトで使用されるフィルタ）	許可
32274（クライアント EPG）	32771（Web EPG）	39（コントラクトサブジェクトで使用されるフィルタの逆フィルタ）	許可

サービスグラフが展開されると、コンシューマーとプロバイダーのサービスノードコネクタの EPG が内部に作成されます。サービスノードのクラス ID は、展開されたグラフインスタンスの下の機能ノードに表示されます。[テナント（Tenant）] > [L4-L7サービス（L4-L7 Services）] > [展開済みグラフインスタンス（Deployed Graph Instances）] > [機能ノード（Function Nodes）] で確認できます（図 12）。

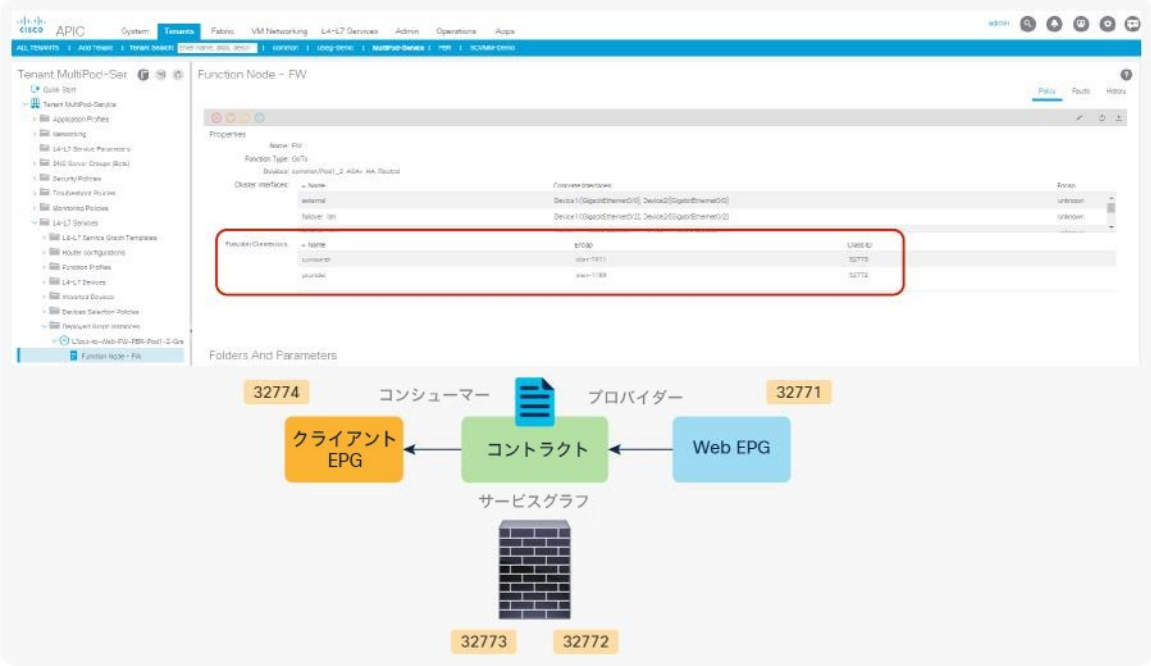


図 12.
サービスノードのクラス ID

サービスグラフを追加すると、表 2 に示すように許可ルールが更新されます。サービスグラフの目的は、コンシューマー EPG とプロバイダー EPG の間にサービスデバイスを挿入することです。そのため、サービスノードのコンシューマーコネクタとプロバイダーコネクタは、それぞれサービスノードとコンシューマー EPG の間、サービスノードとプロバイダー EPG の間に挿入されます。

表 2. サービスグラフがある場合の許可ルール（PBR なし）

送信元クラス ID	接続先クラス ID	フィルタ ID	アクション
32774（クライアント EPG）	32773（サービスノードのコンシューマーコネクタ）	コントラクトサブジェクトで使用されるフィルタ	許可
32772（サービスノードのプロバイダーコネクタ）	32771（Web EPG）	デフォルト	許可
32771（Web EPG）	32772（サービスノードのプロバイダーコネクタ）	コントラクトサブジェクトで使用されるフィルタの逆フィルタ	許可
32773（サービスノードのコンシューマーコネクタ）	32774（クライアント EPG）	コントラクトサブジェクトで使用されるフィルタの逆フィルタ	許可

PBR が設定されたサービスグラフを追加すると、コンシューマー EPG またはプロバイダー EPG が配置されているスイッチにリダイレクトポリシーがプログラムされます。この例では、PBR 接続先 172.16.1.1 はファイアウォールノードのコンシューマーコネクタで、172.16.2.1 はファイアウォールノードのプロバイダーコネクタです。送信元クラスが 32774（クライアント EPG）で、接続先クラスが 32771（Web EPG）の場合、トラフィックは PBR ノードのコンシューマーコネクタにリダイレクトされます。その後、トラフィックは PBR ノードによってルーティングされ、Cisco ACI ファブリックに戻ります。このときの送信元クラスは 32772（PBR ノードのプロバイダーコネクタ）で、接続先クラスは 32771 です。このトラフィックは許可されています。リターントラフィックは、送信元クラスが 32771、接続先クラスが 32774 であるため、同様に PBR ノードのプロバイダーコネクタにリダイレクトされます。リターントラフィックに対して PBR が実行された後、トラフィックは PBR ノードから Cisco ACI ファブリックに戻ります。このときの送信元クラスは 32773（PBR ノードのコンシューマーコネクタ）、接続先クラスは 32774 です。このトラフィックは許可されています（図 13 および表 3）。

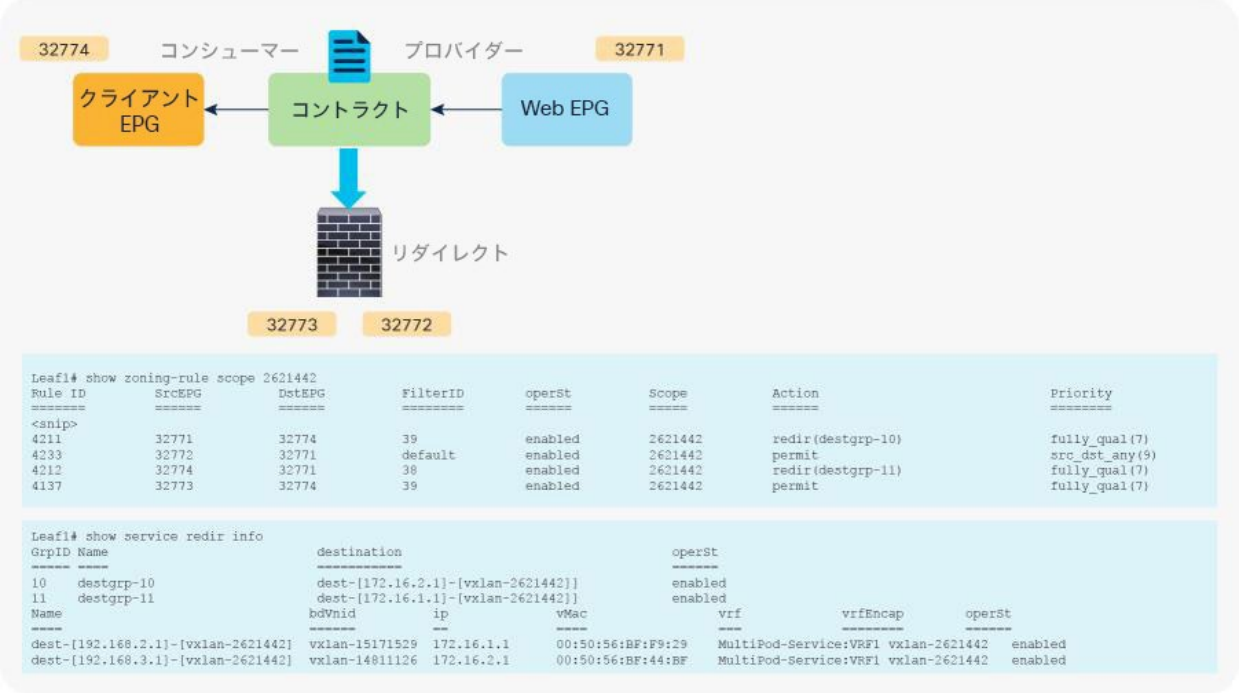


図 13.
PBR が設定されたサービスグラフが展開された後の状態

表 3. サービスグラフがある場合の許可ルールとリダイレクトルール（PBR あり）

送信元 EPG	接続先 EPG	フィルタ ID	アクション
32774（クライアント EPG）	32771（Web EPG）	38（コントラクトサブジェクトで使用されるフィルタ）	リダイレクト
32772（サービスノードのプロバイダーコネクタ）	32771（Web EPG）	デフォルト	許可
32771（Web EPG）	32774（クライアント EPG）	39（コントラクトサブジェクトで使用されるフィルタの逆フィルタ）	リダイレクト
32773（サービスノードのコンシューマーコネクタ）	32774（クライアント EPG）	39（コントラクトサブジェクトで使用されるフィルタの逆フィルタ）	許可

注： 図 13 の **show zoning-rule** コマンド出力に表示されたフィルタ ID は、PBR ノードのプロバイダーコネクタからプロバイダー EPG へ向かうトラフィックに対するルールにデフォルトフィルタ（Permit All）が適用されていることを示しています（表 3）。これと同じ動作が、PBR が設定されていない通常のサービスグラフにも適用されます（表 2）。Cisco ACI は、コンシューマー EPG のクラス ID が送信元または接続先として含まれていないゾーン分割ルールでデフォルトのフィルタを使用します。サービスグラフが適用されたコントラクトサブジェクトで特定のフィルタが使用されている場合でも同様です。外部（コンシューマー）側ですでにセキュリティが適用されていることが前提となっています。APIC リリース 4.2(3) 以降では、コントラクトからのフィルタ（filters-from-contract）オプションがサービスグラフテンプレートのレベルで用意されています。これを選択するとコントラクトサブジェクトで指定されたフィルタがデフォルトフィルタの代わりに使用されます（表 4）。詳細については、「コントラクトからのフィルタ（filters-from-contract）オプション」セクションを参照してください。

表 4. サービスグラフがある場合の許可ルールとリダイレクトルール（PBR あり、コントラクトからのフィルタ（filters-from-contract）オプションを選択）

送信元 EPG	接続先 EPG	フィルタ ID	アクション
32774（クライアント EPG）	32771（Web EPG）	38（コントラクトサブジェクトで使用されるフィルタ）	リダイレクト
32772（サービスノードのプロバイダーコネクタ）	**32771（Web EPG）**	**38（コントラクトサブジェクトで使用されるフィルタ）**	**許可**
32771（Web EPG）	32774（クライアント EPG）	39（コントラクトサブジェクトで使用されるフィルタの逆フィルタ）	リダイレクト
32773（サービスノードのコンシューマーコネクタ）	32774（クライアント EPG）	39（コントラクトサブジェクトで使用されるフィルタの逆フィルタ）	許可

直接接続オプション

PBR が設定されたサービスグラフをデフォルト設定で展開すると、L4-L7 デバイスの可用性をモニタリングするキープライブメッセージの L4-L7 デバイスからサーバーへの送信が失敗します。これは、プロバイダー EPG から PBR ノードのプロバイダーコネクタへのトラフィックに対する許可エントリがないためです。上の例では、コンシューマー EPG（32774）から PBR ノードのコンシューマーコネクタ（32773）へのトラフィックと、プロバイダー EPG（32771）から PBR ノードのプロバイダーコネクタ（32772）へのトラフィックは許可されません。このトラフィックの許可エントリが必要な場合は、[直接接続（Direct Connect）] オプションを [True] に設定します。

この設定は、[テナント（Tenant）] > [L4-L7サービス（L4-L7 Services）] > [L4-L7サービスグラフテンプレート（L4-L7 Service Graph Templates）] > [ポリシー（Policy）] にあります（図 14）。デフォルト設定は [False] です。

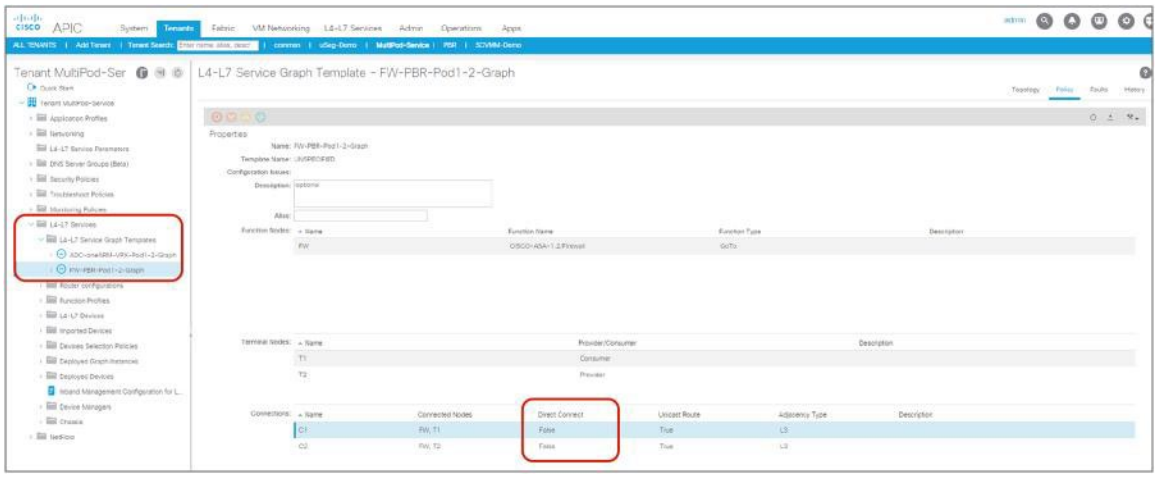


図 14.
L4-L7 サービスグラフテンプレートの直接接続オプション

図 15 は、両方の接続で [直接接続（Direct Connect）] が [True] に設定されている例を示しています。この場合、コンシューマー EPG（32774）から PBR ノードのコンシューマー側（32773）へのトラフィックと、プロバイダー EPG（32771）から PBR ノードのプロバイダー側（32772）へのトラフィックが許可されます（表 5）。

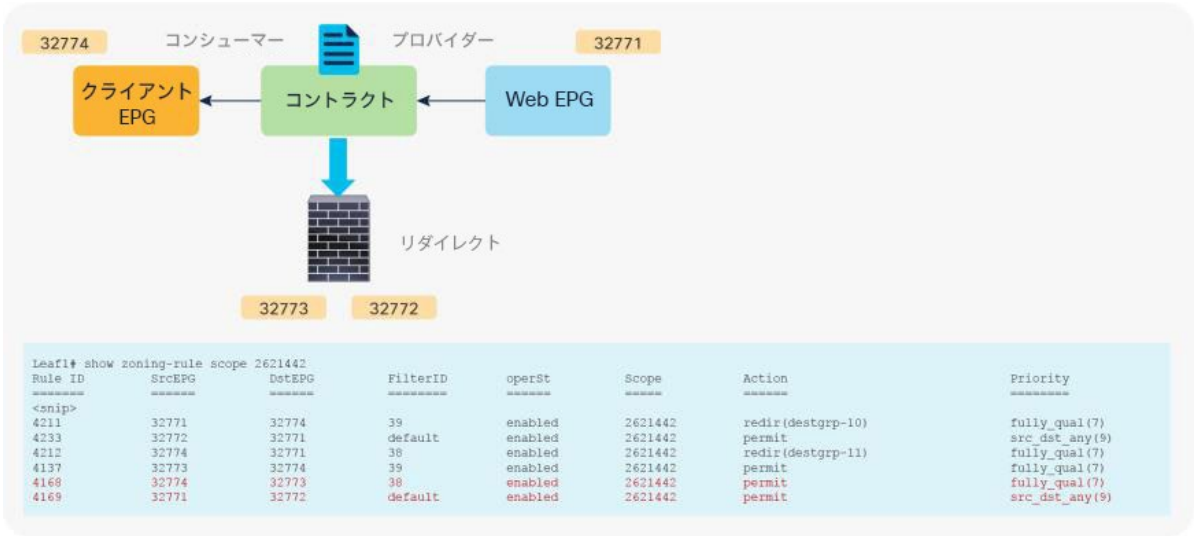


図 15.
PBR が設定されたサービスグラフを展開した後の状態（直接接続を True に設定）

表 5. サービスグラフがある場合の許可ルールとリダイレクトルール（PBR あり、直接接続を True に設定）

送信元クラス ID	接続先クラス ID	フィルタ ID	アクション
32774（クライアント EPG）	32771（Web EPG）	38（コントラクトサブジェクトで使用されるフィルタ）	リダイレクト
32772（サービスノードのプロバイダーコネクタ）	32771（Web EPG）	デフォルト	許可
32771（Web EPG）	32774（クライアント EPG）	39（コントラクトサブジェクトで使用されるフィルタの逆フィルタ）	リダイレクト
32773（サービスノードのコンシューマーコネクタ）	32774（クライアント EPG）	39（コントラクトサブジェクトで使用されるフィルタの逆フィルタ）	許可
32774（クライアント EPG）	32773（サービスノードのコンシューマーコネクタ）	38（コントラクトサブジェクトで使用されるフィルタ）	許可
32771（Web EPG）	32772（サービスノードのプロバイダーコネクタ）	デフォルト	許可

エンドポイント セキュリティ グループ（ESG）のサービス EPG セレクタ

5.2(4) リリースより前のリリースでは、サービスグラフを介して作成されたサービス EPG とのコントラクトを手動で作成することができず、これが課題となっていました。以下にその例を示します。

- 直接接続を使用すれば、サービス EPG からコンシューマー EPG とプロバイダー EPG へのトラフィックの許可ルールを追加できます。ただし、コンシューマー EPG でもプロバイダー EPG でもない EPG は、vzAny コントラクトまたは優先グループを設定しない限りサービス EPG と通信できません。
- vzAny にはサービス EPG が含まれているため、vzAny 対 vzAny のコントラクトは、サービス EPG とその VRF にある他の EPG との間のトラフィックを許可できます。ただし、その VRF にある他のすべての EPG がサービス EPG と通信できるようになり、特定の EPG に限定してサービス EPG との通信を許可することはできません。

以下の図に、2 番目の場合の例を示します。

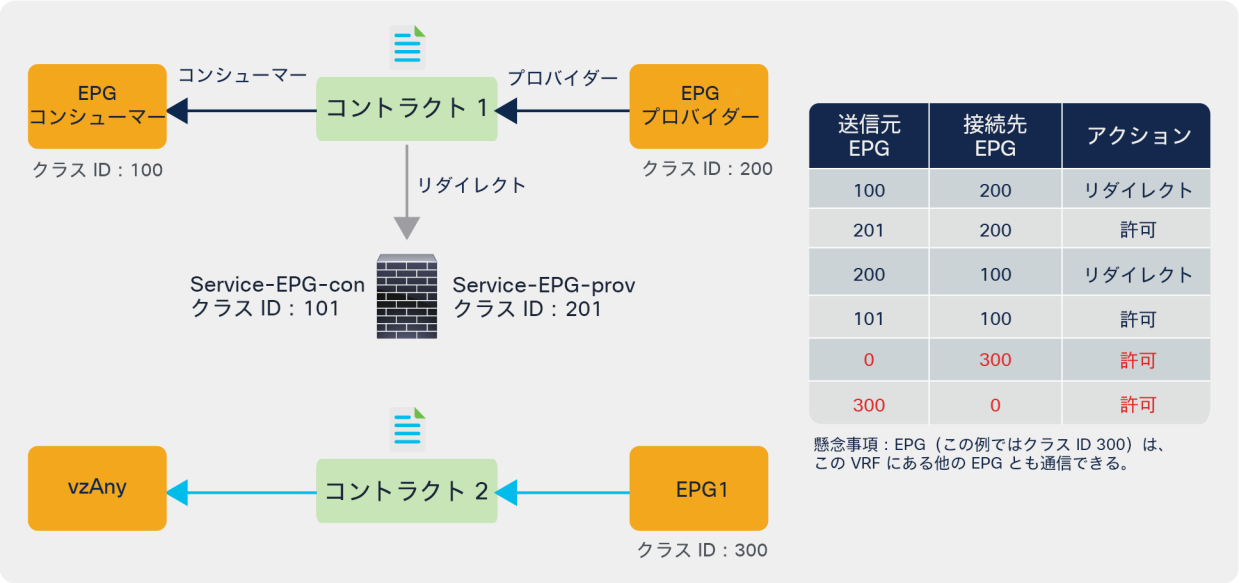


図 16.
ESG のサービス EPG セレクタを使用しないユースケースの例

APIC リリース 5.2(4) 以降では、ESG のサービス EPG セレクタを使用してサービス EPG を ESG にマッピングし、ESG とのコントラクトを作成できます。次の図にユースケースを示します。vzAny 対 vzAny の許可コントラクトに加えて、サービス ESG と他の ESG の間に拒否コントラクトを作成することで、特定の ESG に限定してサービス ESG との通信を許可できます。

以下の図に例を示します。サービス EPG「Service-EPG-con」は、ファイアウォールのコンシューマーコネクタの EPG で、ESG「Service-ESG-con」にマッピングされています。この ESG と、ESG1 や L3Out EPG との間にはコントラクトが作成されています。サービス EPG を含むゾーン分割ルールは、サービス EPG のクラス ID が ESG のクラス ID に変更されても継承されます。EPG と ESG の間のコントラクトはサポートされていないため、コントラクトは、サービスデバイス インターフェイスの ESG（この例では Service-ESG-con）と EPG との間ではなく、ESG または L3Out EPG との間で作成できることに注意してください。

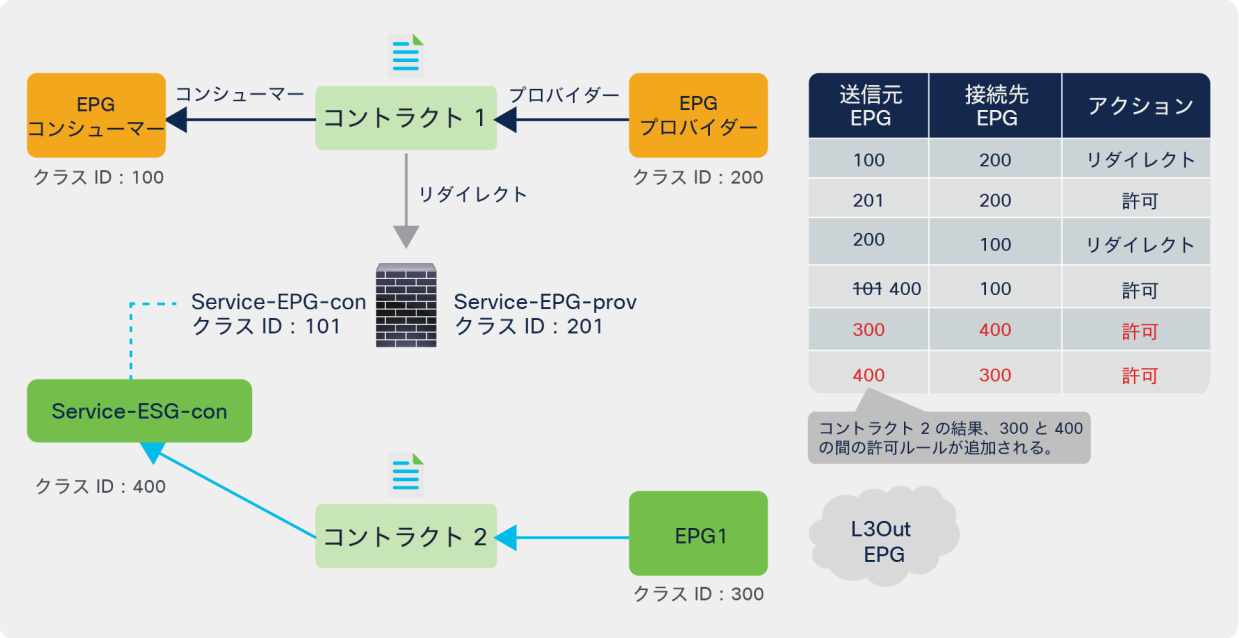


図 17.
ESG のサービス EPG セレクタを使用したユースケースの例 1

下の図に、別のユースケースを示します。 VRF 内のすべてのトラフィックを許可するために vzAny 対 vzAny のコントラクトが使用されています。vzAny からサービスデバイス インターフェイスの ESG（この例では Service-ESG-con）へのトラフィックに対する拒否コントラクトを追加することで、特定の EPG に限定してサービスデバイス インターフェイスとの通信を許可できます。

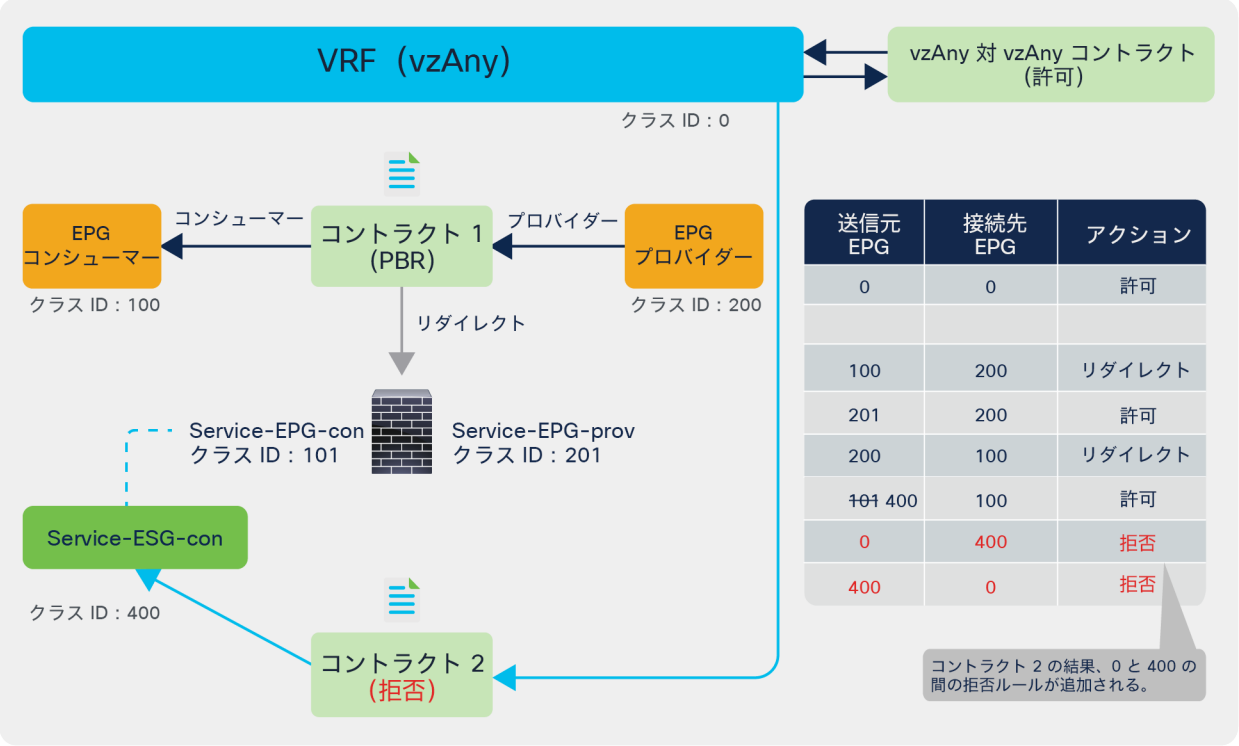


図 18.
ESG のサービス EPG セレクタを使用したユースケースの例 2

この設定は、[テナント（Tenant）] > [エンドポイントセキュリティグループ（Endpoint Security Groups）] > ESG 名 > [セレクタ（Selectors）] > [サービスEPGセレクタ（Service EPG Selectors）] にあります。テナントのデバイス選択ポリシーで定義されている LifCtx（サービス EPG を表すサービスデバイスコネクタ）の一覧がドロップダウンメニューに表示されます。LifCtx を選択すると、サービス EPG が ESG にマッピングされます。

図 19.
ESG のサービス EPG セレクタ

ESG のサービス EPG セレクタには、次の考慮事項があります。

- EPG と ESG の間のコントラクトはサポートされていません。
- サービス EPG を含むゾーン分割ルールは継承されますが、サービス EPG のクラス ID は、グローバルクラス ID に変更されます。サービス EPG がローバルクラス ID を使用する ESG にマッピングされるためです。クラス ID が変更されるため、トラフィック損失が発生します。
- 同じ BD を使用する同じデバイス内のすべての LifCtx を同じ ESG にマッピングする必要があります。以下にその例を示します。
  - ワンアームモード PBR （下の図 20 の例を参照してください）。
  - 複数のサービスグラフの展開にサービスデバイス インターフェイスを再利用する場合
- サービス EPG と ESG は同じ VRF にある必要があります。
  - サービス EPG と ESG が異なるテナントにある場合は、追加の考慮事項があります（下の図 21 と 22 の例を参照してください）。
- マルチサイトはサポートされません（この記事の執筆時点では、NDO は ESG をサポートしていません）。
- BD に PBR 接続先がある L3 PBR のみをサポートします。
  - L3Out にある PBR 接続先はサポートされません（L3Out EPG の場合、コントラクトは手動で設定できます）。
  - L1/L2 PBR はサポートされません（L1/L2 デバイスインターフェイスがサーバーと直接通信することは想定されていません）。

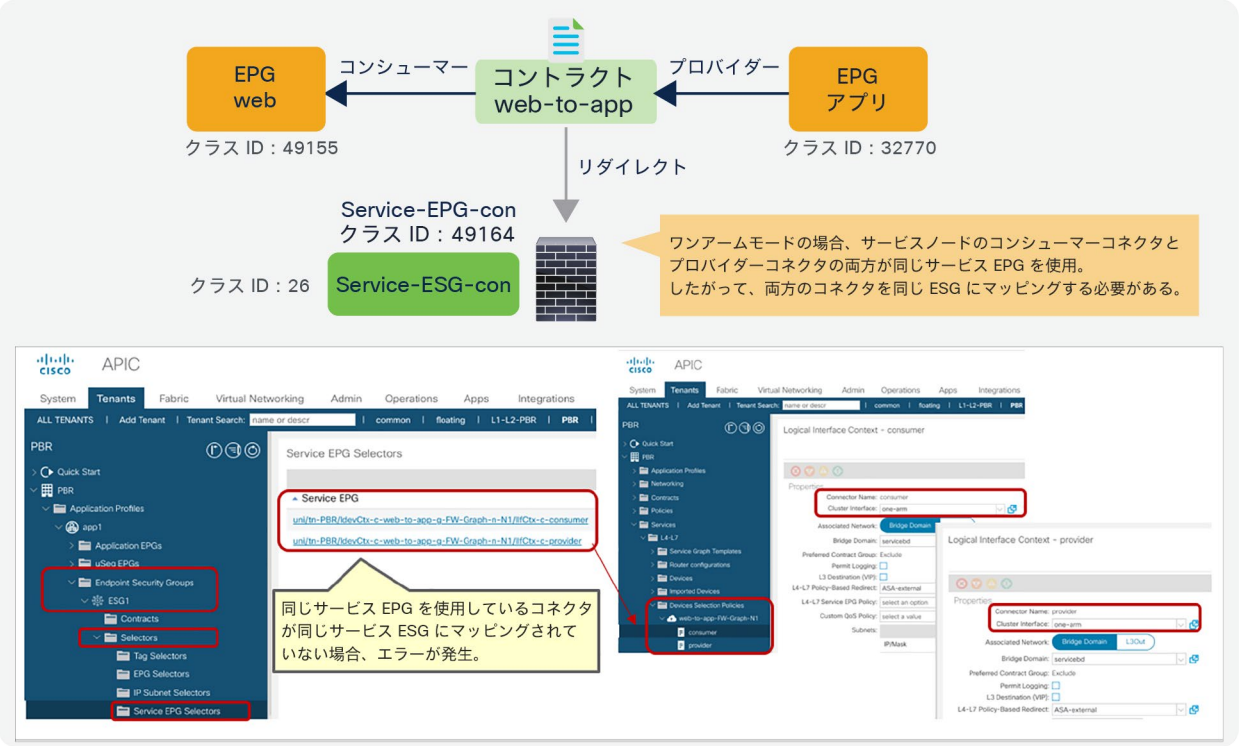


図 20.
同じ BD を使用する同じデバイス内のすべての LifCtx は、同じ ESG にマッピングする必要がある（ワンアームモード）

下の図 21 と図 22 は、サービス EPG と ESG が異なるテナントにある場合の考慮事項を示しています。サービス EPG オブジェクトは、L4-L7 デバイスが定義されているテナントに内部で作成されることに注意してください。L4-L7 デバイスが別のテナントで定義されている場合、サービス EPG オブジェクトは、L4-L7 デバイスが存在するテナントに内部で作成されます。図 21 に示すように、サービス EPG から ESG へのマッピングが単一のテナントでのみ定義されている場合、このマッピングがサポートされます。

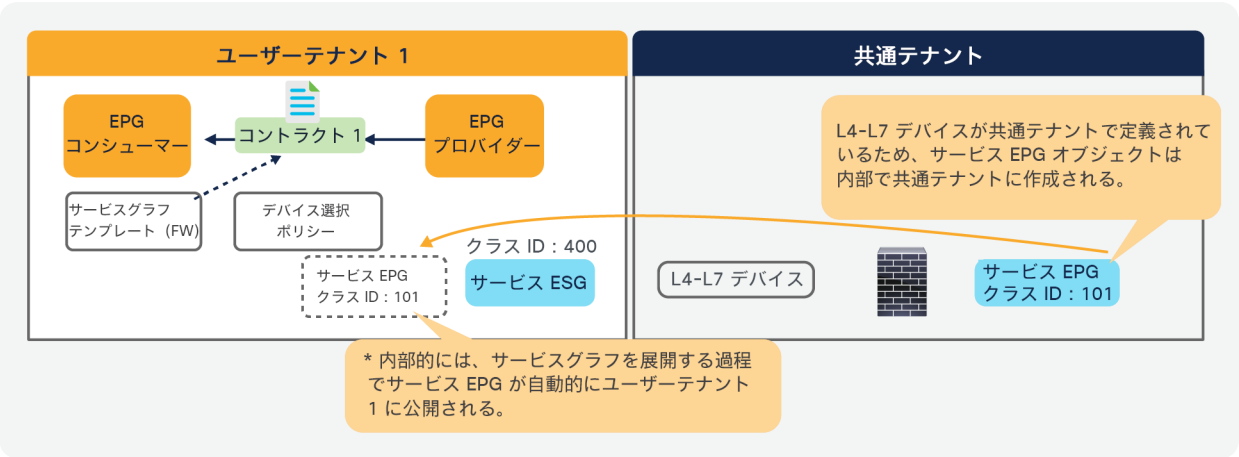


図 21.
複数テナントの場合の考慮事項（サポート対象）

ただし、図 22 に示すように、サービス EPG から ESG へのマッピングが複数のテナントで定義されている場合、競合が発生する可能性があるためサポートされません。

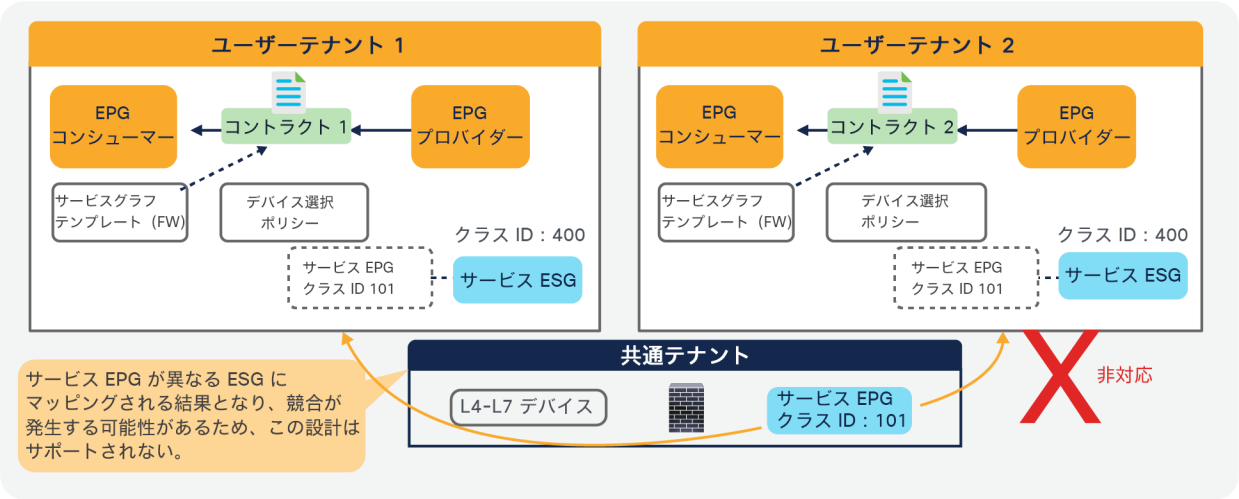
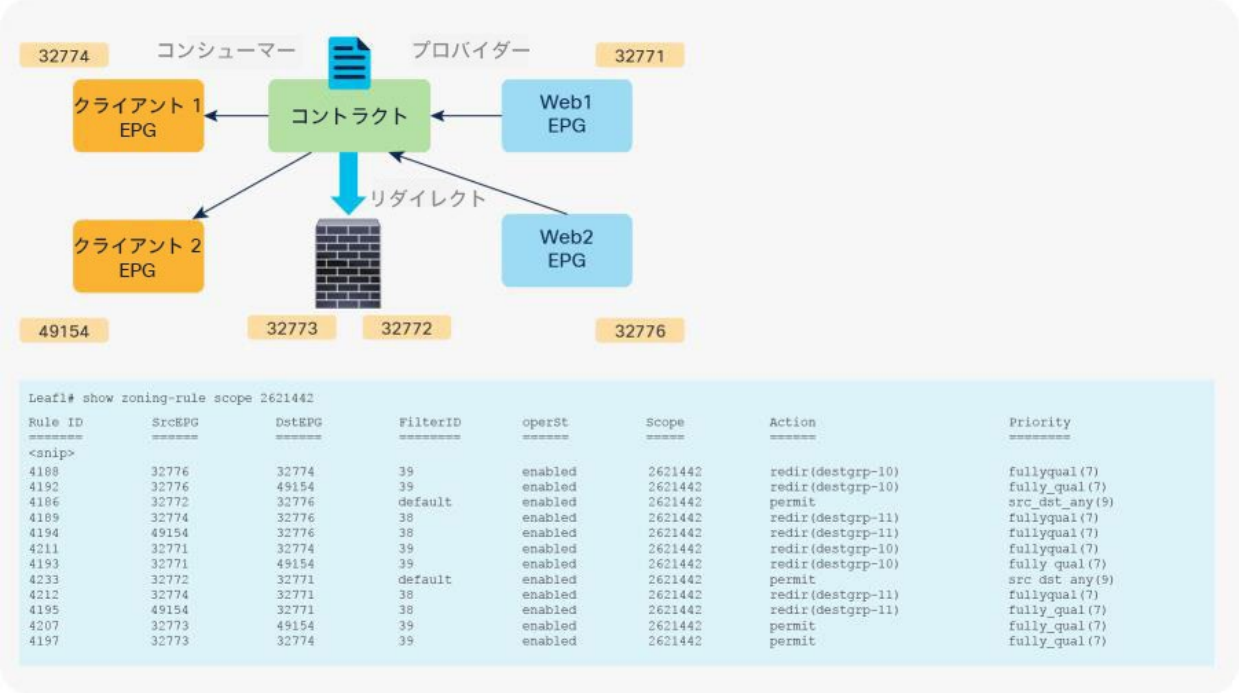


図 22.
複数テナントの場合の考慮事項（サポート対象外）

複数のコンシューマー EPG とプロバイダー EPG

サービスグラフはコントラクトに適用され、コントラクトは複数の EPG ペア間に設定できます。ルーテッド（Go-To）モードまたはブリッジ（Go-Through）モードの L4-L7 デバイスでサービスグラフを使用している場合、グラフを再利用する際に、L4-L7 デバイスがアタッチされているブリッジドメインを考慮する必要があります。PBR が設定されたサービスグラフを使用すると、柔軟性が向上し、複数のブリッジドメインにまたがる任意の 2 つの EPG ペア間にコントラクトをアタッチできるようになります。ただし、このアプローチが L4-L7 デバイスが属する VRF インスタンスと矛盾していない場合に限られます。

前の例のように、2 つのコンシューマー EPG と 2 つのプロバイダー EPG がある場合、ポリシーは図 23 のようにプログラムされます。コンシューマー EPG の 1 つとプロバイダー EPG の 1 つの間にトラフィックが発生した場合、そのトラフィックは PBR ノードにリダイレクトされます。




```
Leaf1# show zoning-rule scope 2621442
Rule ID      SrcEPG      DstEPG      FilterID    operSt      Scope       Action          Priority
=======      ======      ======      ========    ======      =====       ======          ========
<snip>
4188         32776       32774       39          enabled     2621442     redir(destgrp-10)   fullyqual(7)
4192         32776       49154       39          enabled     2621442     redir(destgrp-10)   fully_qual(7)
4186         32772       32776       default     enabled     2621442     permit          src_dst_any(9)
4189         32774       32776       38          enabled     2621442     redir(destgrp-11)   fullyqual(7)
4194         49154       32776       38          enabled     2621442     redir(destgrp-11)   fullyqual(7)
4211         32771       32774       39          enabled     2621442     redir(destgrp-10)   fullyqual(7)
4193         32771       49154       39          enabled     2621442     redir(destgrp-10)   fully_qual(7)
4233         32772       32771       default     enabled     2621442     permit          src_dst_any(9)
4212         32774       32771       38          enabled     2621442     redir(destgrp-11)   fullyqual(7)
4195         49154       32771       38          enabled     2621442     redir(destgrp-11)   fully_qual(7)
4207         32773       49154       39          enabled     2621442     permit          fully_qual(7)
4197         32773       32774       39          enabled     2621442     permit          fully_qual(7)
```

図 23.
PBR が設定されたサービスグラフが展開された後の状態（複数のコンシューマー EPG とプロバイダー EPG）

エンドツーエンドのパケットフロー

このセクションでは、L3 ブリッジドメインにある PBR 接続先を使用したエンドツーエンドの PBR パケットフローについて説明します。L3Out にある PBR 接続先については、「L3Out にある PBR 接続先」セクションを参照してください。いくつかの設計とトラフィックフローが考えられるため、この説明で使用されている例は実際の環境を正確に反映していない場合があります。

図 24 の例では、クライアント EPG がコンシューマー EPG、Web EPG がプロバイダー EPG で、両者間に PBR サービスグラフが設定されたコントラクトがあります。クライアントエンドポイントが Web エンドポイント宛てのトラフィックを生成しています。リーフ 1 が接続先エンドポイントを学習していない場合、リーフ 1 は接続先 EPG の クラス ID を解決できません。したがって、トラフィックはスパインプロキシに送信され、スパインノードは、接続先エンドポイントが接続されているリーフ 3 にトラフィックを転送します。リーフ 3 は、このトラフィックから送信元エンドポイントを学習します。次に、リーフ 3 が送信元と接続先の EPG のクラス ID を解決できるため、リーフ 3 で PBR が実行されます。ここで、接続先セグメント ID（VNID）が PBR ノードブリッジドメインのブリッジドメイン VNID に書き換えられ、接続先 MAC アドレスが APIC で設定されている PBR ノードの MAC アドレスに書き換えられます。接続先 MAC アドレスが接続されている場所をリーフ 3 が認識していないため、トラフィックはスパインプロキシに送信されます。スパインノードは、PBR ノードが接続されているリーフ 2 にトラフィックを転送します。リーフ 2 はこのトラフィックからクライアントの IP アドレスを学習しません。PBR ノードブリッジドメインのエンドポイント データプレーン 学習が無効化されているためです。

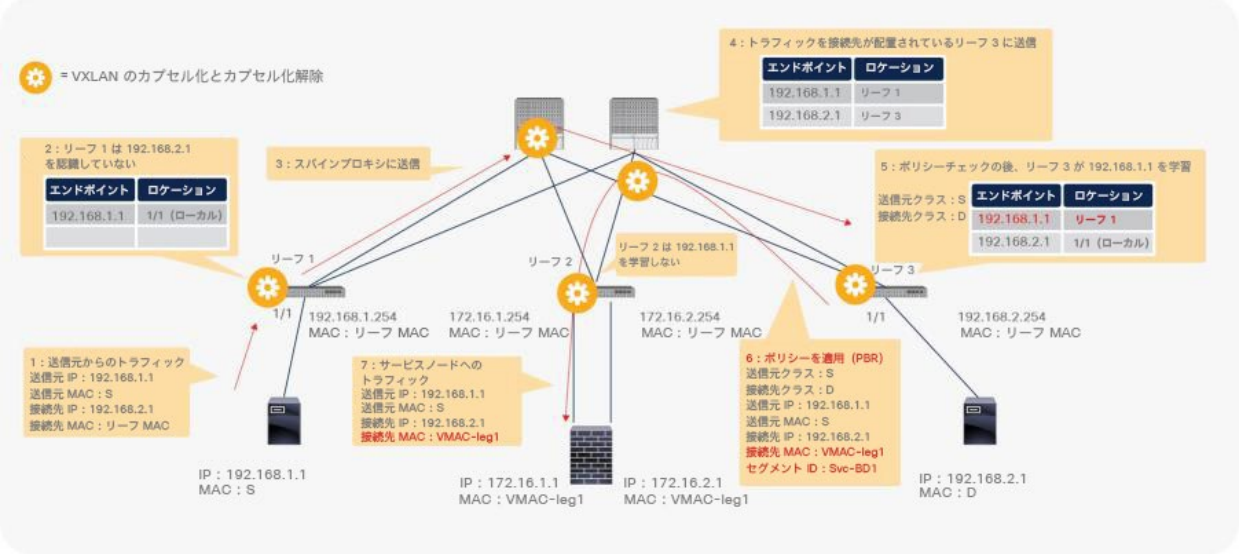


図 24.
エンドツーエンドのパケットフローの例（クライアントから PBR ノード）

トラフィックは、PBR ノードのルーティングテーブルに基づいて PBR ノードでルーティングされ、Cisco ACI ファブリックに戻ります。リーフ 2 は接続先エンドポイントを認識していないため、トラフィックは再度スパインプロキシに送信され、その後リーフ 3 に送信されます。ここで、送信元 EPG は PBR ノードのプロバイダーコネクタのクラス ID であり、接続先はプロバイダー EPG のクラス ID です。このトラフィックは許可されているため、Web エンドポイントに到達します。ここで重要な点は、リーフ 3 がこのトラフィックからクライアントの IP アドレスを学習しないことです。PBR ノードブリッジドメインのエンドポイント データプレーン学習が無効化されているためです（図 25）。

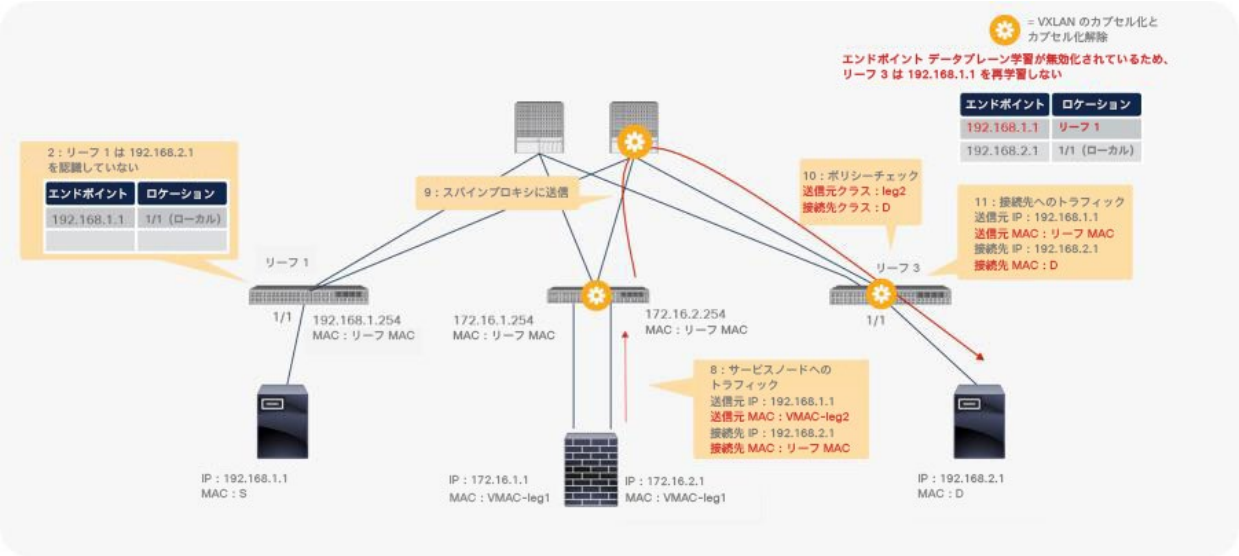


図 25.
エンドツーエンドのパケットフローの例（PBR ノードから Web）

リターントラフィックの場合、リーフ 3 が送信元と接続先の両方の EPG のクラス ID を解決できるため、PBR はリーフ 3 で実行されます。接続先 MAC アドレスが書き換えられ、トラフィックは PBR ノードのプロバイダー側に送信されます（図 26）。

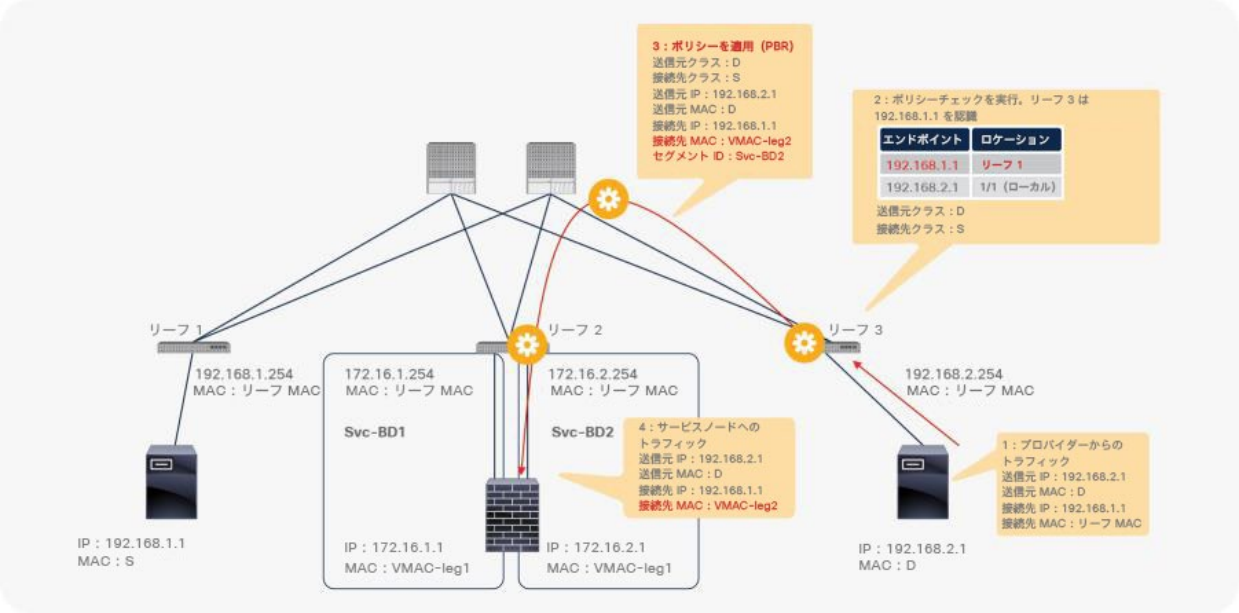


図 26.
エンドツーエンドのパケットフローの例（Web から PBR ノード）

トラフィックは、PBR ノードのコンシューマー側から Cisco ACI ファブリックに戻ります。リーフ 2 は接続先エンドポイントを認識していないため、トラフィックは再度スパインプロキシに送信され、その後リーフ 1 に送信されます。リーフ 1 がポリシーを適用します。送信元 EPG が PBR ノードのコンシューマーコネクタのクラス ID であり、接続先がコンシューマー EPG のクラス ID であるため、トラフィックが許可されます。リーフ 1 はこのトラフィックから Web エンドポイントの IP アドレスを学習しません。PBR ノードブリッジドメインのエンドポイントデータプレーン学習が無効化されているためです（図 27）。

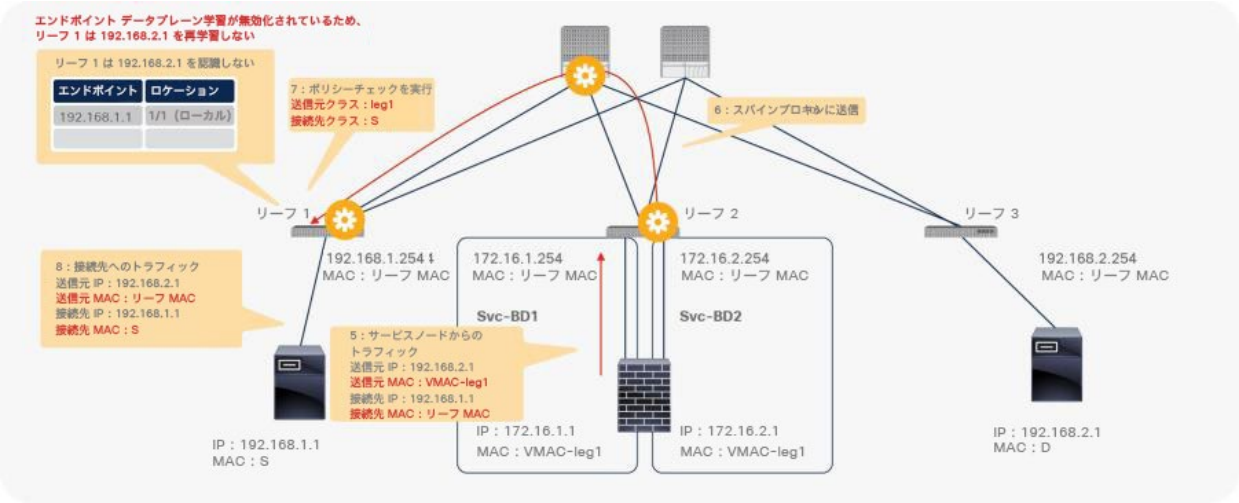


図 27.
エンドツーエンドのパケットフローの例（PBR ノードからクライアント）

この例では、リーフ 1 が Web エンドポイントの IP アドレスを学習しないため、残りのトラフィックもリーフ 3 でリダイレクトされます。Cisco ACI は、送信元と接続先のクラス ID を決定できるかどうかに応じてポリシーを適用します。これはトラフィックフローに依存します。トラフィックが最初に Web エンドポイントから生成される場合、または他のトラフィックによってリーフ 1 が Web エンドポイントの IP アドレスを学習できる場合は、リーフ 1 で PBR ポリシーを実行できます。

traceroute に関する考慮事項

リーフでルーティングされるため、TTL が減算されます。traceroute を実行すると、ACI のリーフ IP が traceroute 出力に表示されます。ネットワークデバイスは、最も近い IP を送信元 IP として使用して、ICMP の「Time Exceeded」メッセージを送信元に返信するため、ネットワーク設計によっては、同じサブネット範囲が 2 回表示される場合があります。

たとえば、ICMP トラフィックがリダイレクトされる場合、L3Out の背後にある外部クライアントから接続先エンドポイント 192.168.2.1 に対して traceroute を実行すると（図 28）、traceroute の出力に次のようなホップが表示されます。

1. リーフ 1 またはリーフ 2 の L3Out インターフェイスの IP（192.168.1.251 または 192.168.1.252）
2. PBR ノードの外部コネクタの IP（172.16.1.1）（PBR ノードが TTL を減算する場合）*
3. リーフ 2 の L3Out インターフェイスの IP（192.168.1.252）

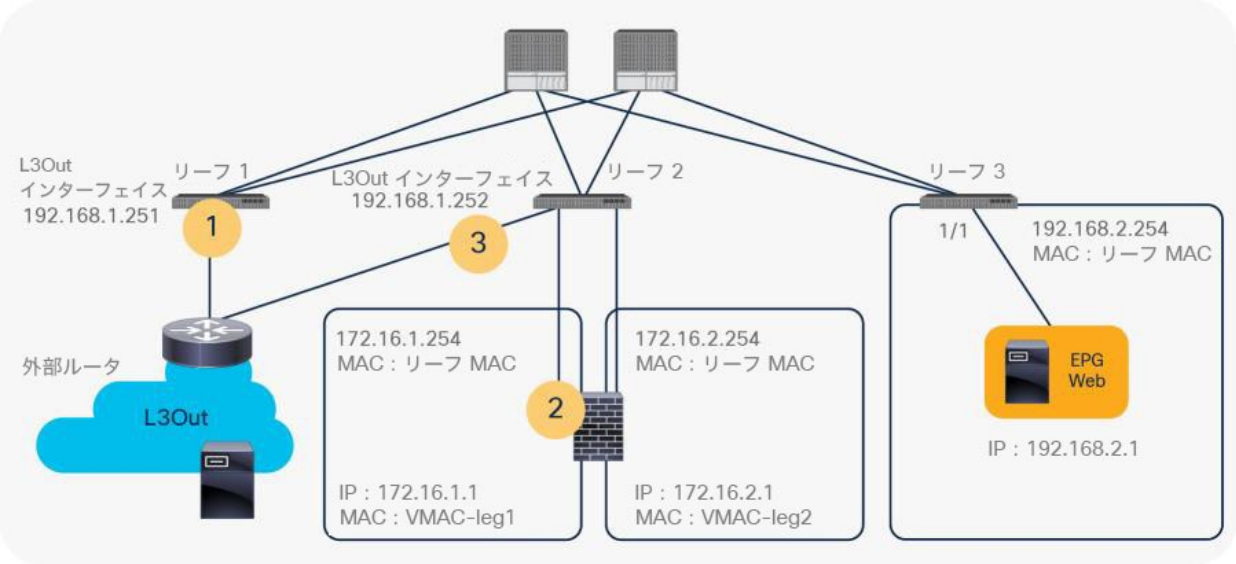


図 28.
traceroute に関する考慮事項（トポロジ）

*サービスデバイスが TTL を減算しない場合があります。たとえば、Cisco 適応型セキュリティアプライアンス（ASA）は、デフォルトでは TTL を減算しません。

これは、リーフ 2 が外部クライアントに返す ICMP の「Time Exceeded」メッセージの送信元 IP としてリーフ 2 の L3Out インターフェイス の IP を使用するためです。図 29 に、論理ネットワークトポロジを示します。

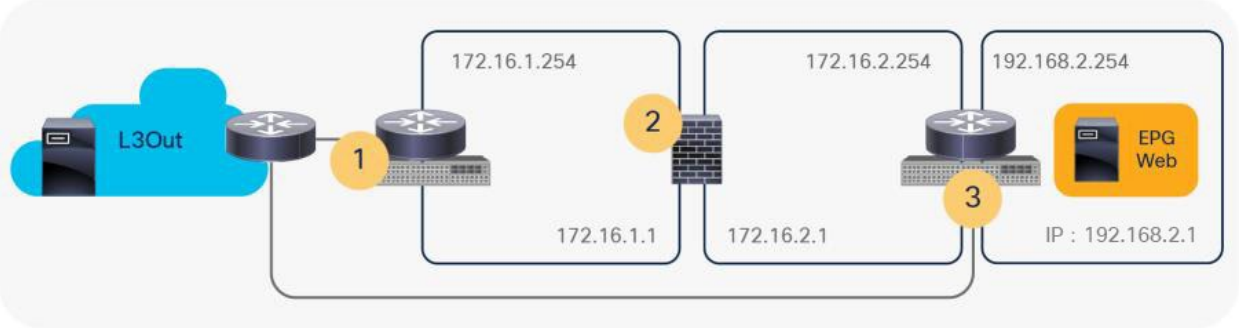


図 29.
traceroute に関する考慮事項（論理ネットワークトポロジ）

対称 PBR

これまでの PBR に関する説明では、PBR 接続先が単一の L4-L7 デバイスであることを前提にしていました。しかしながら、PBR は、個別のファイアウォールといった単一の接続先ではなく、複数の PBR 接続先にトラフィックの負荷を分散できます。たとえば、PBR 接続先が 3 つある場合、それぞれの IP アドレスと MAC アドレスのペアが PBR ポリシーで設定され、トラフィックはハッシュに基づいて 3 つの PBR ノードのいずれかにリダイレクトされます。ハッシュのタプルは、デフォルトでは、送信元 IP アドレス、宛先 IP アドレス、プロトコル番号です。L4-L7 デバイスが接続トラッキングを実行するため、L4-L7 デバイスから両方向のフローが見える必要があります。したがって、着信トラフィックとリターントラフィックが同じ PBR ノードにリダイレクトされるようにする必要があります。対称 PBR は、これを可能にする機能です（図 30）。

対称 PBR は、複数のサービスノードを挿入してシステムを拡張する場合に有用です。Cisco Nexus 9300-EX および -FX プラットフォーム リーフ スイッチ以降が必要です。

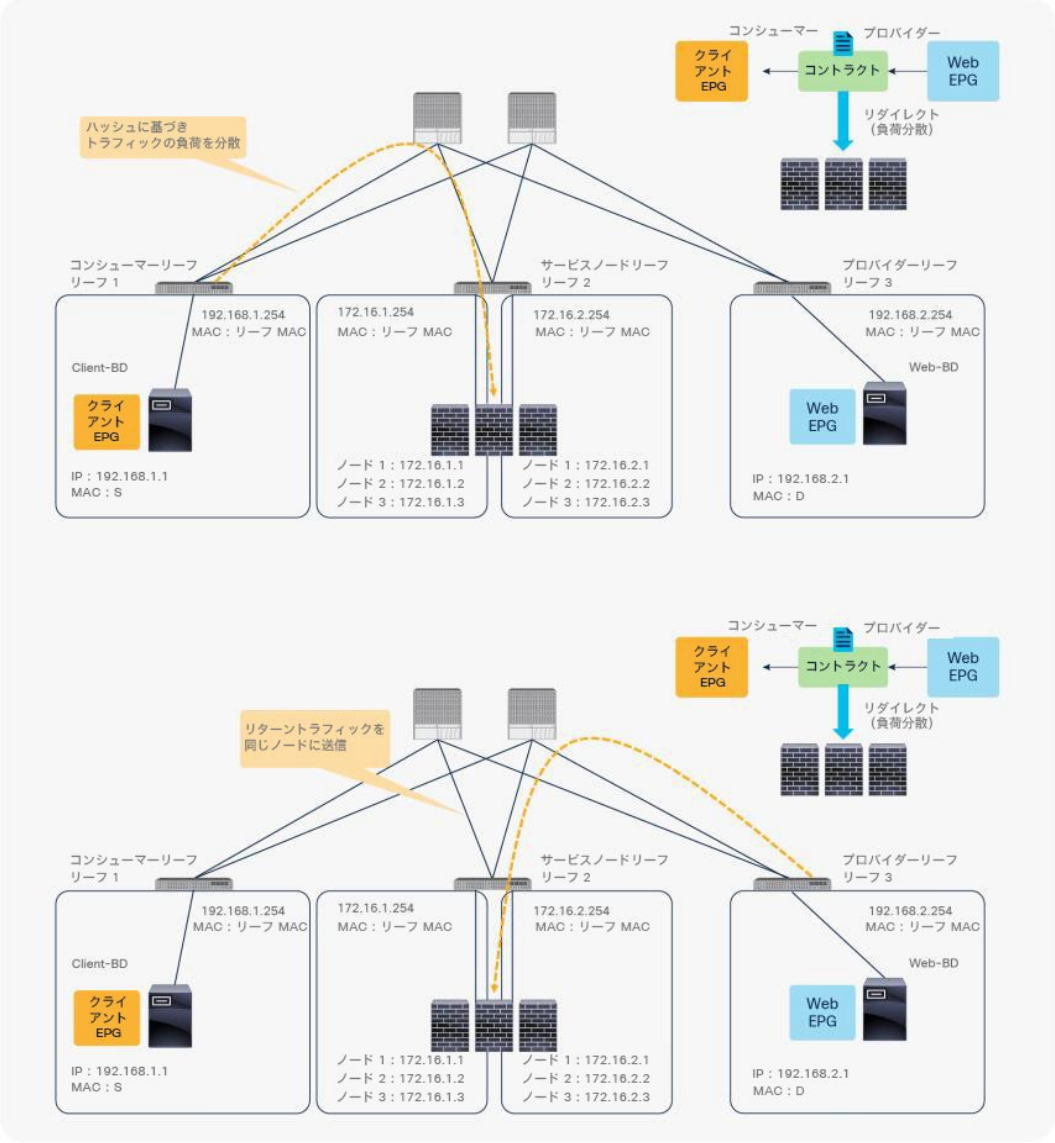


図 30.
対称 PBR

APIC リリース 2.2(3j) および 3.1 以降では、ハッシュタプルをユーザーが設定できます。送信元 IP アドレスのみ、宛先 IP アドレスのみ、送信元 IP アドレス、宛先 IP アドレス、プロトコル番号の組み合わせ（デフォルト）が可能です。送信元 IP アドレスのみ、または宛先 IP アドレスのみのオプションを使用する場合は、両方向でオプションを設定してトラフィックの対称性を維持する必要があります。たとえば、着信トラフィックに送信元 IP アドレスのみのオプションを使用する場合、リターントラフィックには宛先 IP アドレスのみのオプションを使用して、トラフィックの対称性を維持する必要があります（図 31 を参照）。

送信元 IP アドレスのみまたは宛先 IP アドレスのみのオプションを使用した対称 PBR のユースケースは、ある送信元 IP アドレス（ユーザー）からのトラフィックが常に同じサービスノードを通過する必要があるシナリオです。

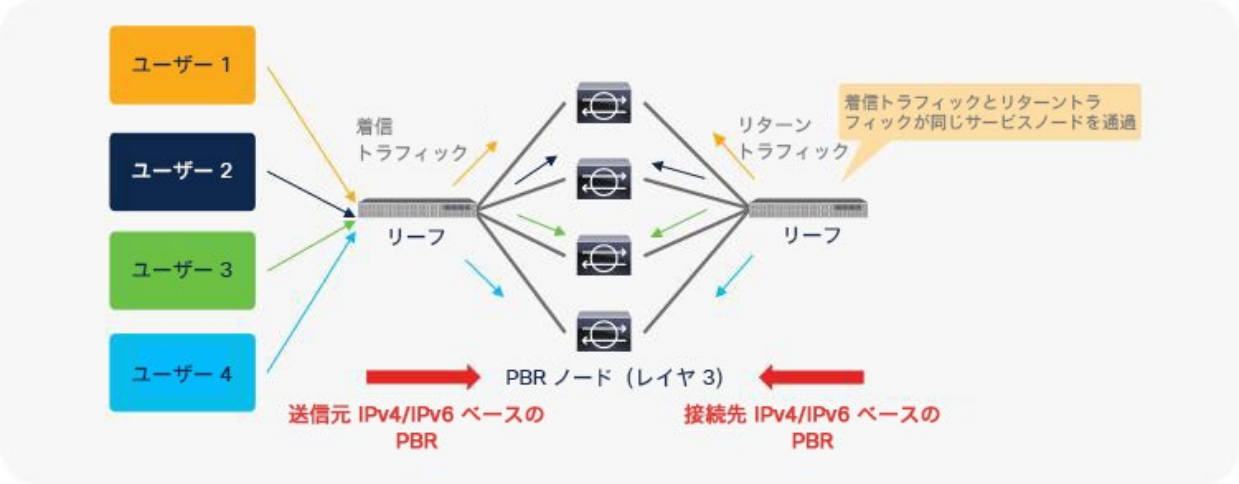


図 31.
送信元 IP アドレスのみと宛先 IP アドレスのみのオプションを使用した例

展開オプション

このセクションでは、PBR で使用できるさまざまな展開オプションについて説明します。

EPG が同じ VRF インスタンスの異なるサブネットにある場合

PBR の基本的かつ一般的な展開では、図 32 と図 33 に示すように、EPG ノードと PBR ノードが同じ VRF インスタンスに置かれ、各 EPG は異なるブリッジドメインに置かれます。エンドポイントのゲートウェイとなる Cisco ACI ファブリックは PBR に不可欠です。

図 32.
VRF 内設計（L3Out EPG から Web EPG）

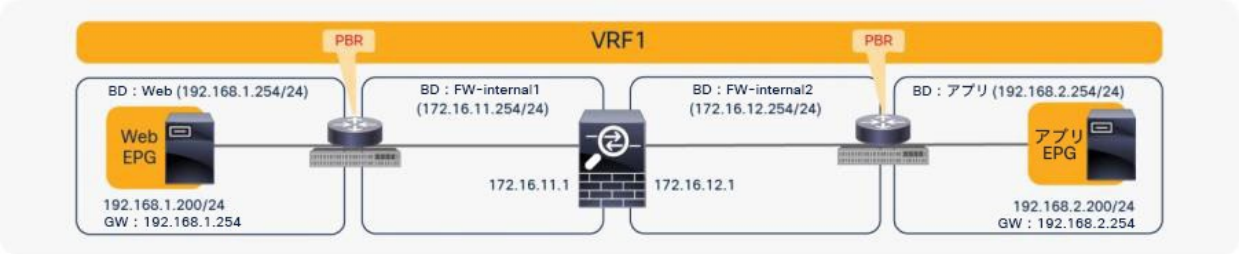


図 33.
VRF 内設計（Web EPG からアプリケーション EPG）

コンシューマー EPG とプロバイダー EPG が同じサブネットにある場合

PBR は、エンドポイントが同じブリッジドメインにある場合でも、トラフィックをリダイレクトできます。

たとえば、Web EPG とアプリケーション EPG が同じブリッジドメイン、同じサブネットにある場合でも、PBR を適用できます。この設計では、PBR ノードがより限定的なスタティックルートを持たない限り、PBR ノードで同じインターフェイスを使用する必要があります。このようなシナリオは、ワンアームモード展開と呼ばれます（図 34）。この例では PBR ノードに専用のブリッジドメインを使用しています。APIC リリース 3.1 以降では、Web EPG とアプリケーション EPG が置かれたブリッジドメイン、サブネットと同じブリッジドメイン、サブネットに L3 PBR 接続先を置くことができます。

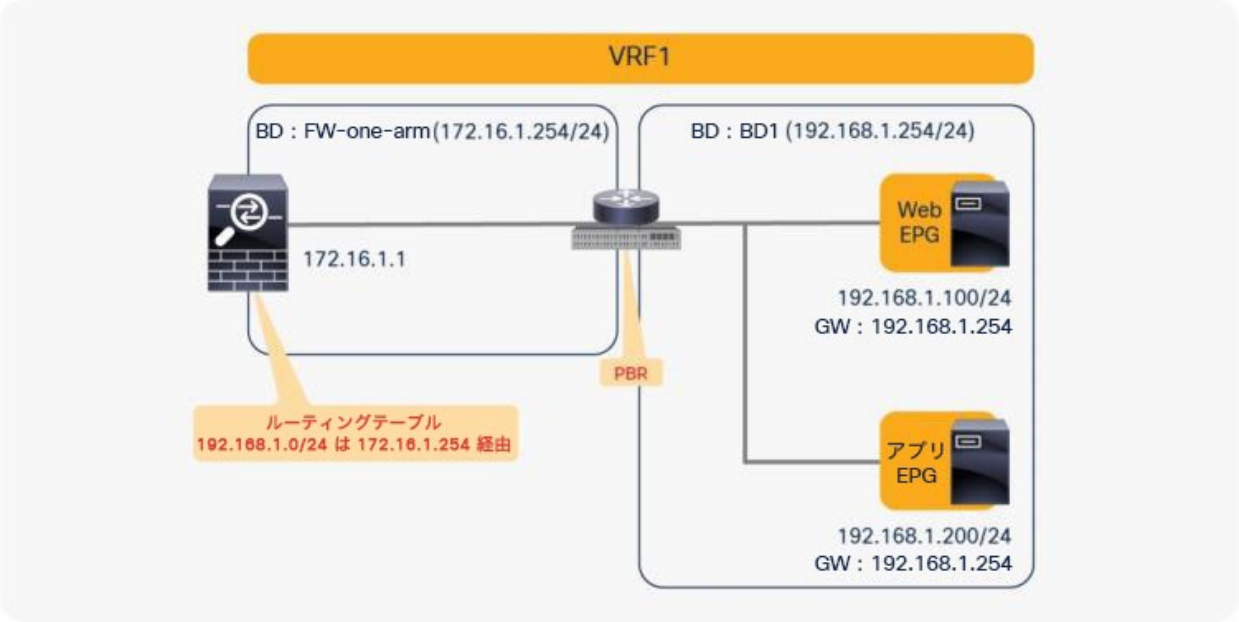


図 34.
コンシューマー EPG とプロバイダー EPG が同じサブネットにある場合

注： トラフィックの着信と発信が同じインターフェイスを経由することをファイアウォールが禁止している場合があります。したがって、このようなインターフェイス内トラフィックを許可するようにファイアウォールを適切に設定する必要があります。Cisco 適応型セキュリティアプライアンス（ASA）の設定例については、このドキュメントで後ほど説明します。

APIC リリース 4.0 より前のリリースでは、サービスグラフを EPG 内コントラクトに関連付けることはできません。APIC リリース 4.0 以降のリリースでは、EPG 内コントラクトを使用した PBR がサポートされます。APIC リリース 5.2 以降では、外部 EPG 内コントラクトを使用した PBR もサポートされます。

単方向 PBR

PBR は、双方向 PBR または単方向 PBR として展開できます。

ロードバランサが送信元 NAT を実行しない場合の単方向 PBR

単方向 PBR のユースケースの 1 つは、送信元ネットワークアドレス変換（NAT）を実行しないロードバランサの統合です。

たとえば図 35 に示すように、クライアントからのトラフィックの宛先 IP アドレスはロードバランサの仮想 IP アドレスになっているため、クライアントから Web へのトラフィックに PBR は必要ありません。ロードバランサが送信元 IP アドレスを変換しない場合、リターントラフィックには PBR が必要です。そうしないとリターントラフィックがロードバランサに戻りません。

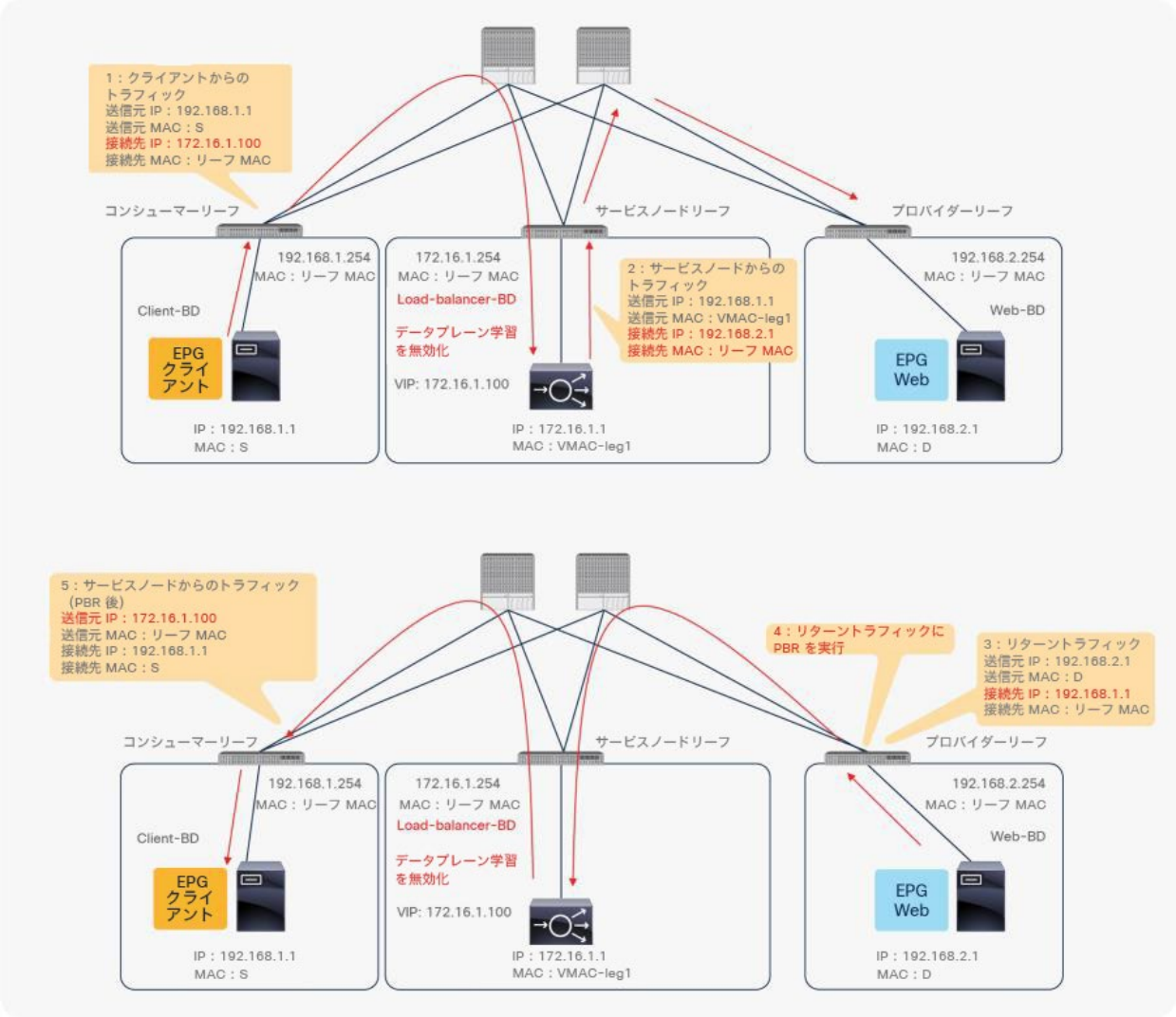


図 35.
単方向 PBR の例

注： 直接接続を True に設定して、ロードバランサ エンドポイントから Web エンドポイントへのキープアライブメッセージを許可する必要があります。

もう一方のコネクタが L3Out にある単方向 PBR

APIC リリース 4.1.2 より前のリリースでは、単方向 PBR の場合でも、両方のコネクタを L3Out ではなくブリッジドメインに置く必要があります。APIC リリース 4.1.2 以降では、その必要はありません。L3Out を使用して L4-L7 デバイスの一方のインターフェイスを接続すると同時に、もう一方のインターフェイスはブリッジドメインに接続して、PBR リダイレクトを介してトラフィックを受信できます。

もう一方のコネクタが L3Out にある単方向 PBR のユースケースとしては、NAT IP プールがローカルサブネットの外部にある場合が挙げられます。図 36 に例を示します。コンシューマーからプロバイダーへのトラフィックは、PBR ノードのいずれかにリダイレクトされます。PBR ノードが送信元 NAT を実行しますが、NAT IP アドレスはローカルサブネットの外部にあります。したがって、この NAT IP アドレスへのルートを追加するには、L3Out が必要です。このアドレスがプロバイダーからのリターントラフィックの宛先 IP アドレスになります。リターントラフィックの接続先は NAT IP アドレスであるため、PBR ノードのプロバイダーコネクタでの PBR は必要ありません。

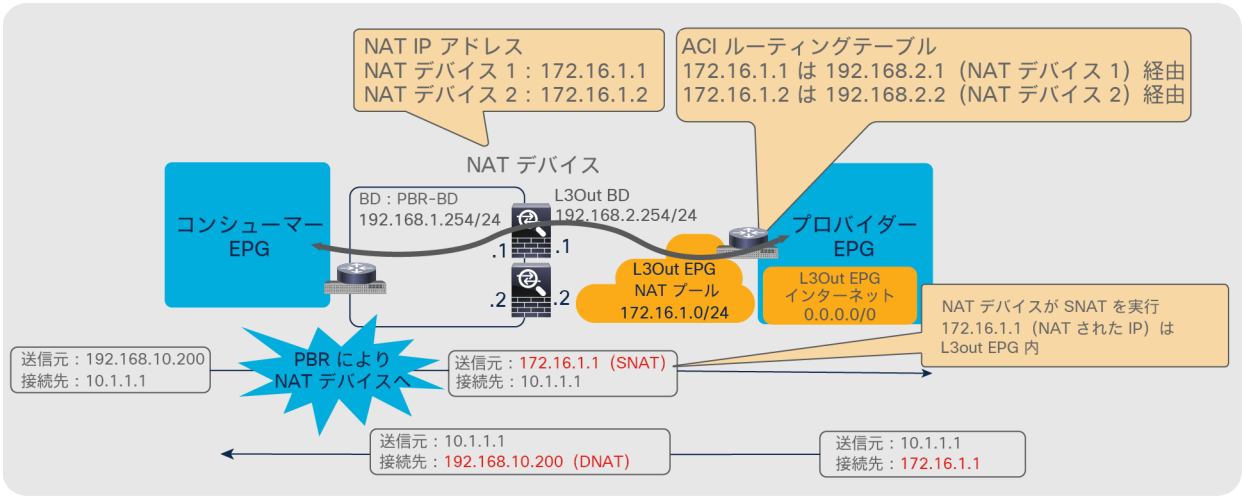


図 36.
L3Out にプロバイダーコネクタがある場合の単方向 PBR の設計例

APIC リリース 5.0 より前のリリースでは、L3Out はサービスグラフの最後のノードのプロバイダーコネクタ（L4-L7 デバイスのプロバイダー側インターフェイス）でのみサポートされています。図 36 の例がこれに該当します。

APIC リリース 5.0 以降では、この要件は必須ではありません。図 37 に、もう一方のコネクタが L3Out にある場合でプロバイダーからコンシューマーへのトラフィックに単方向 PBR が適用される例を示します。このユースケースでは、ローカルサブネットの外部にロードバランサの VIP があります。コンシューマーからプロバイダーへのトラフィックは、L3Out を介して VIP に送信されます。このトラフィックの接続先は VIP であるため、PBR は必要ありません。ロードバランサが NAT を実行しない場合は、リターントラフィックに PBR が必要です。この例では、L3Out がコンシューマーコネクタで使用されています。

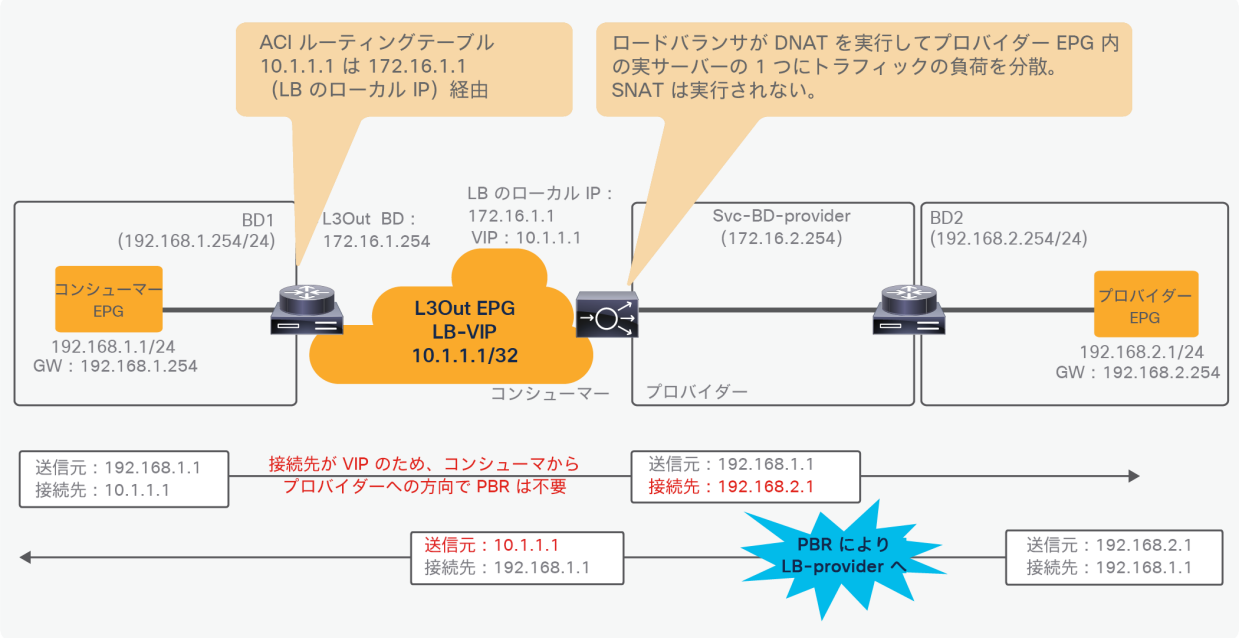


図 37.
L3Out にコンシューマーコネクタがありプロバイダーからコンシューマーへのトラフィックに単方向 PBR が適用される場合の設計例

注： PBR ノードで IP 変換が適切に実行されていることを確認する必要があります。さらに、同じ VRF に他の L3Out EPG がある場合は、個別の L3Out EPG サブネットが設定されていることを確認する必要があります。そうしないとループが発生する可能性があります。L3Out EPG の分類がインターフェイス単位ではなく VRF 単位で行われるためです。

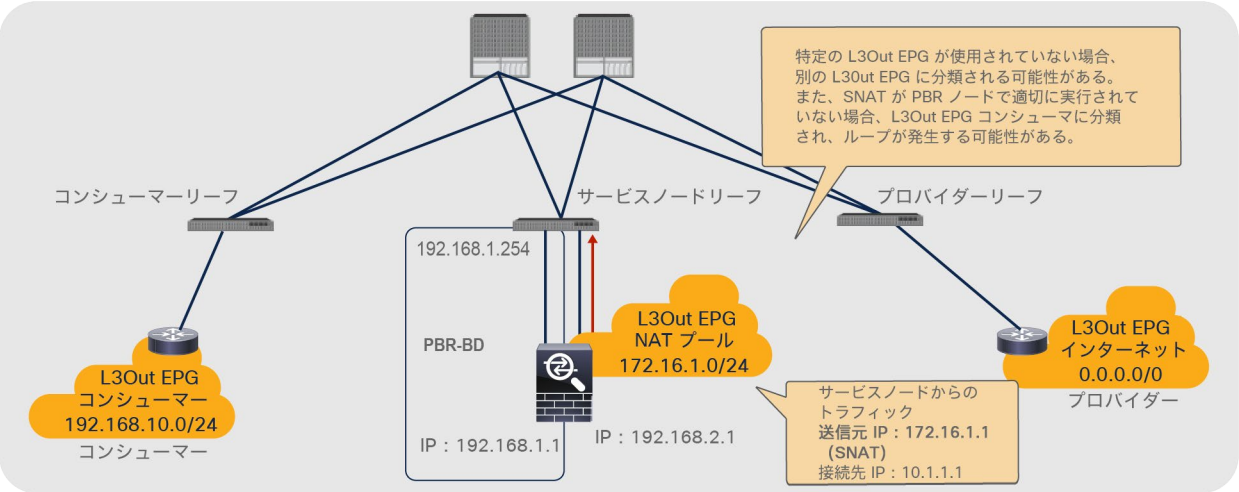


図 38.
もう一方のコネクタが L3Out にある単方向 PBR に関する設計上の考慮事項

APIC リリース 5.2 以降では、PBR 接続先を L3 ブリッジドメインではなく L3Out に置くことができます。詳細については、「L3Out にある PBR 接続先」のセクションを参照してください。

VRF インスタンスをまたぐ PBR

PBR は、異なる VRF インスタンスにある EPG の間に展開できます。この設計のユースケースとしては、ある VRF インスタンスにあるサービスを異なる VRF インスタンスにあるエンドポイントが共有する場合が挙げられます。

PBR デバイスは、図 39 に示すように、コンシューマーの VRF インスタンスとプロバイダーの VRF インスタンスの間、またはいずれかのインスタンスの中の置くことができます。PBR ノードブリッジドメインは、コンシューマー EPG の VRF インスタンスまたはプロバイダー EPG の VRF インスタンスに置く必要があります。他の VRF インスタンスに置くことはできません。

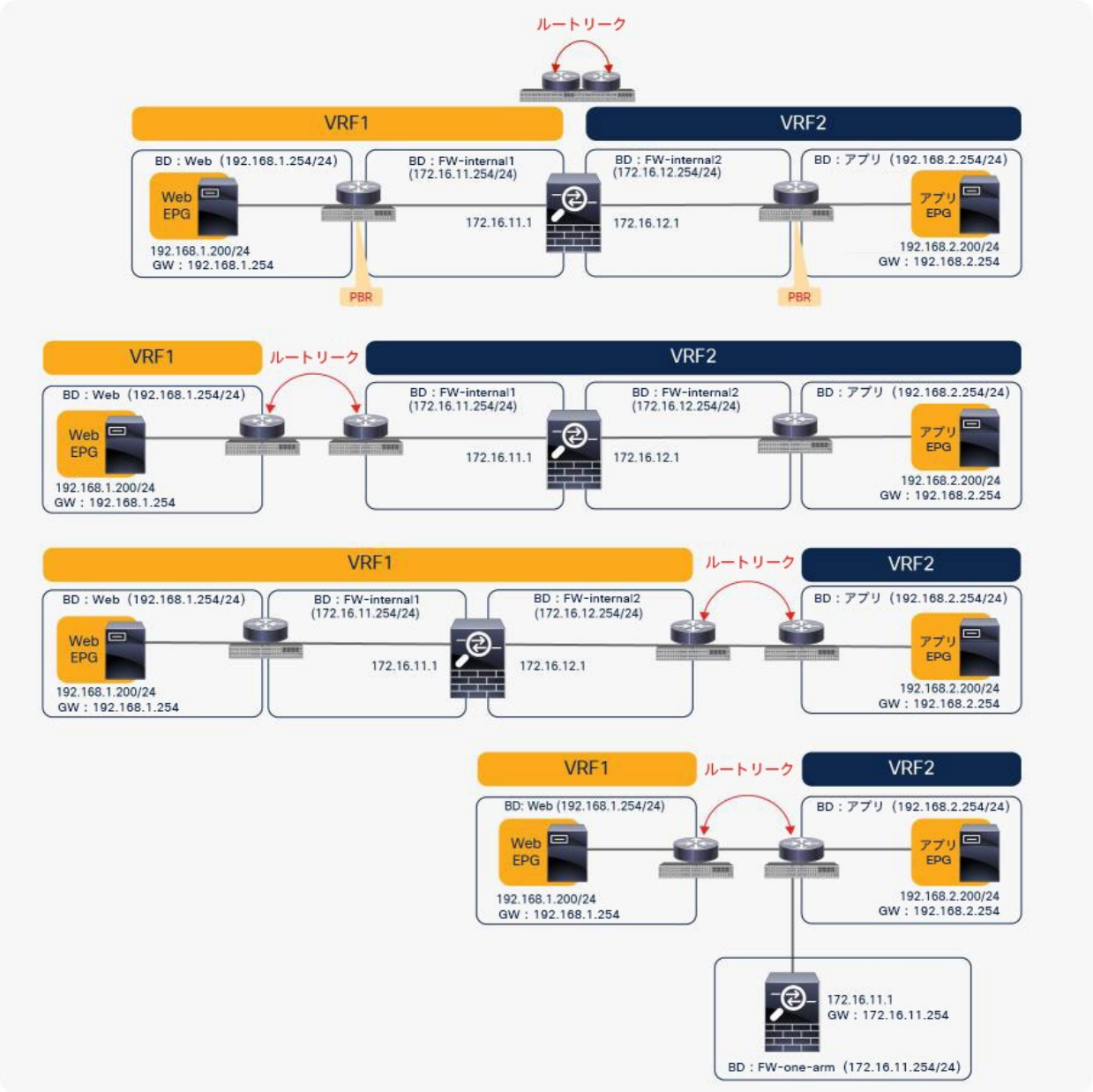


図 39.
VRF 間設計

注： コンシューマーの VRF インスタンスとプロバイダーの VRF インスタンスは、同じテナントに置くことも異なるテナントに置くこともできます。

VRF 間コントラクトの場合、プロバイダールートとコンシューマールートが VRF インスタンス間でリークされ、コンシューマーの VRF インスタンスで Cisco ACI コントラクトポリシーが適用されます。同様に、PBR を使用する場合でも、VRF インスタンスにまたがるルートリークが必要です（ルートリークの設定例については、このドキュメントで後ほど説明します）。たとえば、VRF1 には VRF2 からリークされたプロバイダー EPG のサブネット 192.168.2.0/24 が含まれている必要があり、VRF2 には VRF1 からリークされたコンシューマー EPG のサブネット 192.168.1.0/24 が含まれている必要があります。サービスグラフが展開されると、コンシューマーの VRF インスタンス（スコープ 2949121）には VRF 間トラフィックの許可ルールとリダイレクトルールが設定され、プロバイダーの VRF インスタンス（スコープ 2326532）には VRF 内トラフィックの許可ルールが設定されます（図 40 および表 6）。

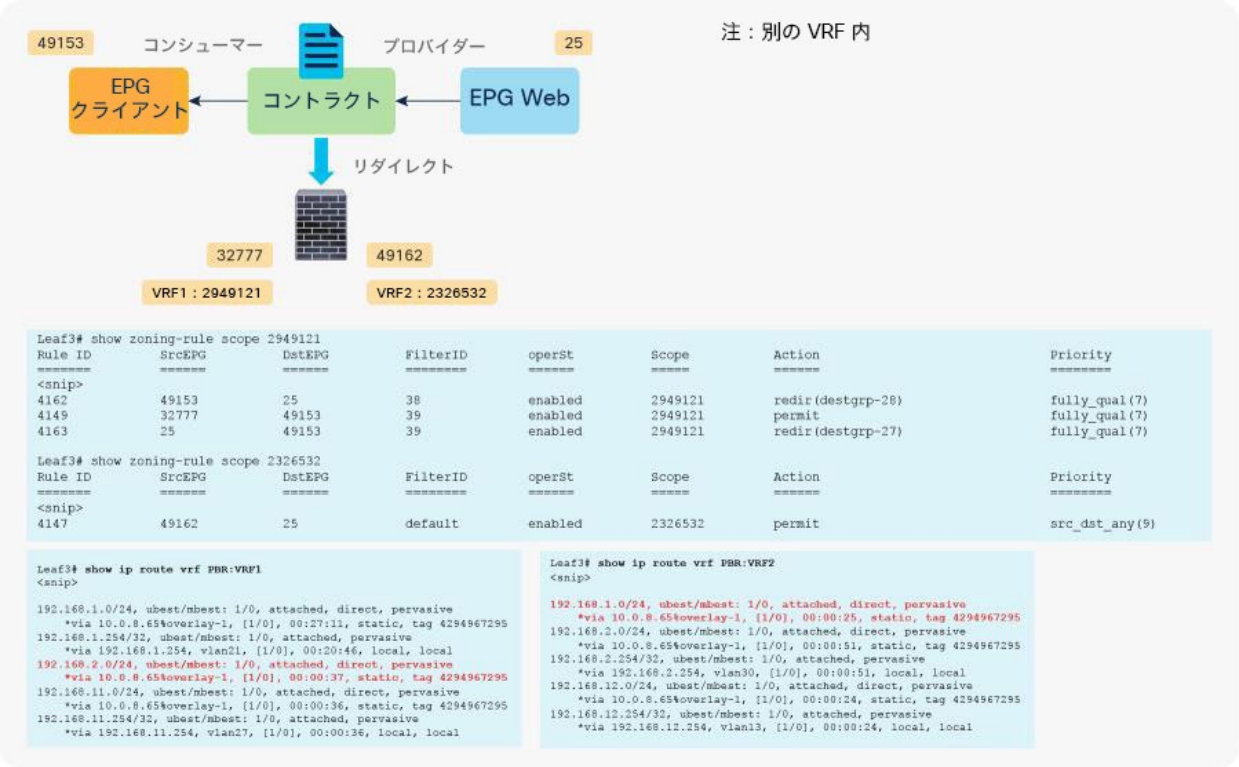


図 40.
許可ルールとリダイレクトルールが設定された VRF 間設計

表 6. 許可ルールとリダイレクトルール（VRF インスタンス間）

VRF インスタンス	送信元クラス ID	接続先クラス ID	フィルタ ID	アクション
VRF1	49153（クライアント EPG）	25（Web EPG）	38（コントラクトサブジェクトで使用されるフィルタ）	リダイレクト
VRF1	32777（サービスノードのコンシューマーコネクタ）	49153（クライアント EPG）	39（コントラクトサブジェクトで使用されるフィルタの逆フィルタ）	許可

VRF インスタンス	送信元クラス ID	接続先クラス ID	フィルタ ID	アクション
VRF1	25（Web EPG）	49153（クライアント EPG）	39（コントラクト サブジェクトで使用されるフィルタの逆フィルタ）	リダイレクト
VRF2	49162（サービスノードのプロバイダーコネクタ）	25（Web EPG）	デフォルト	許可

2 ノードサービスグラフ（PBR を伴うファイアウォール、NAT を伴うロードバランサ）

EPG 間に 2 つのサービスノード、たとえばファイアウォールに続いてロードバランサを挿入する場合は、ファイアウォールを挿入するために PBR が必要になる可能性があります。トラフィックの接続先がロードバランサの仮想 IP アドレスになっているため、ロードバランサへのリダイレクトは不要です。

たとえば、最初のノードを PBR ノードであるファイアウォール、2 番目のノードを PBR ノードではないロードバランサに設定したとします。コンシューマーのエンドポイントが、ロードバランサの仮想 IP アドレス宛てのトラフィックを生成します。このトラフィックはファイアウォールにリダイレクトされます。このとき Web EPG（プロバイダー EPG）からロードバランサ EPG（2 番目のノードのコンシューマーコネクタ）へのトラフィックに PBR ポリシーが適用されます。次に、このトラフィックはロードバランサに送信され、送信元 IP アドレスと宛先 IP アドレスがロードバランサによって変換されます。最後に、接続先に送信されます（図 41）。

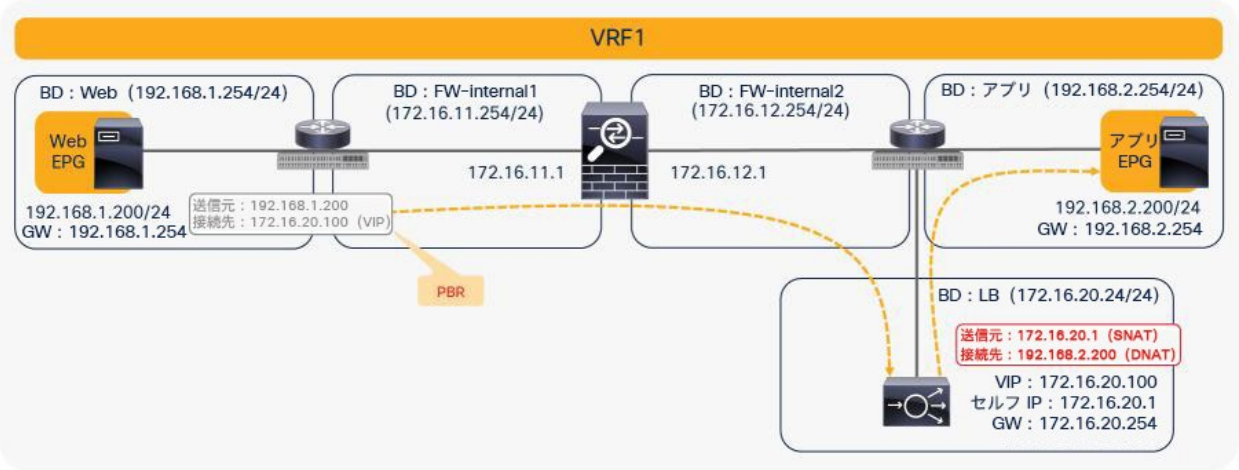


図 41.
2 ノードのサービスグラフ（着信トラフィック）

リターントラフィックの場合、ロードバランサによって送信元 NAT が実行されているため、宛先 IP アドレスはロードバランサの IP アドレスになります。トラフィックはロードバランサに戻り、IP アドレスが変換されます。次に、ロードバランサ EPG（2 番目のノードのコンシューマー側）と Web EPG の間のトラフィックに PBR ポリシーが再度適用されます（図 42）。

APIC リリース 3.2 より前のリリースでは、サービスグラフの最初のノードまたは 2 番目のノードのいずれかを PBR ノードにできます。したがって、この例では 2 番目のノードで NAT が必要です。

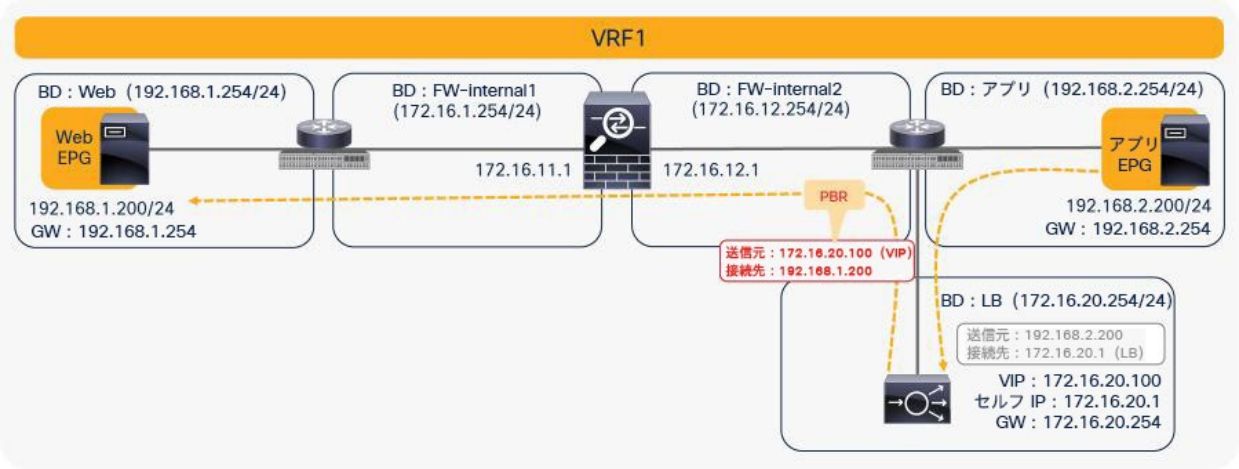


図 42.
2 ノードのサービスグラフ（リターントラフィック）

注： Cisco Nexus 9300 プラットフォームスイッチ（Cisco Nexus 9300-EX および -FX プラットフォームスイッチ以降を除く）を使用する場合、最初のノード（PBR ノード）は、コンシューマーエンドポイントと 2 番目のノードが接続されているリーフノードとは異なるリーフノードの下に置く必要があります。ただし、コンシューマーエンドポイント、プロバイダーエンドポイント、および 2 番目のノードは、同じリーフノードに下に置くことができます。2 番目のノードが PBR ノードの場合、PBR ノードは、最初のノードのプロバイダー側とプロバイダー EPG が接続されているリーフノードとは異なるリーフノードの下に置く必要がありますが、コンシューマーエンドポイントと PBR ノードは同じリーフノードの下に置くことができます。

Cisco Nexus 9300-EX および -FX プラットフォーム リーフ スイッチ以降では、この要件はありません（図 43）。

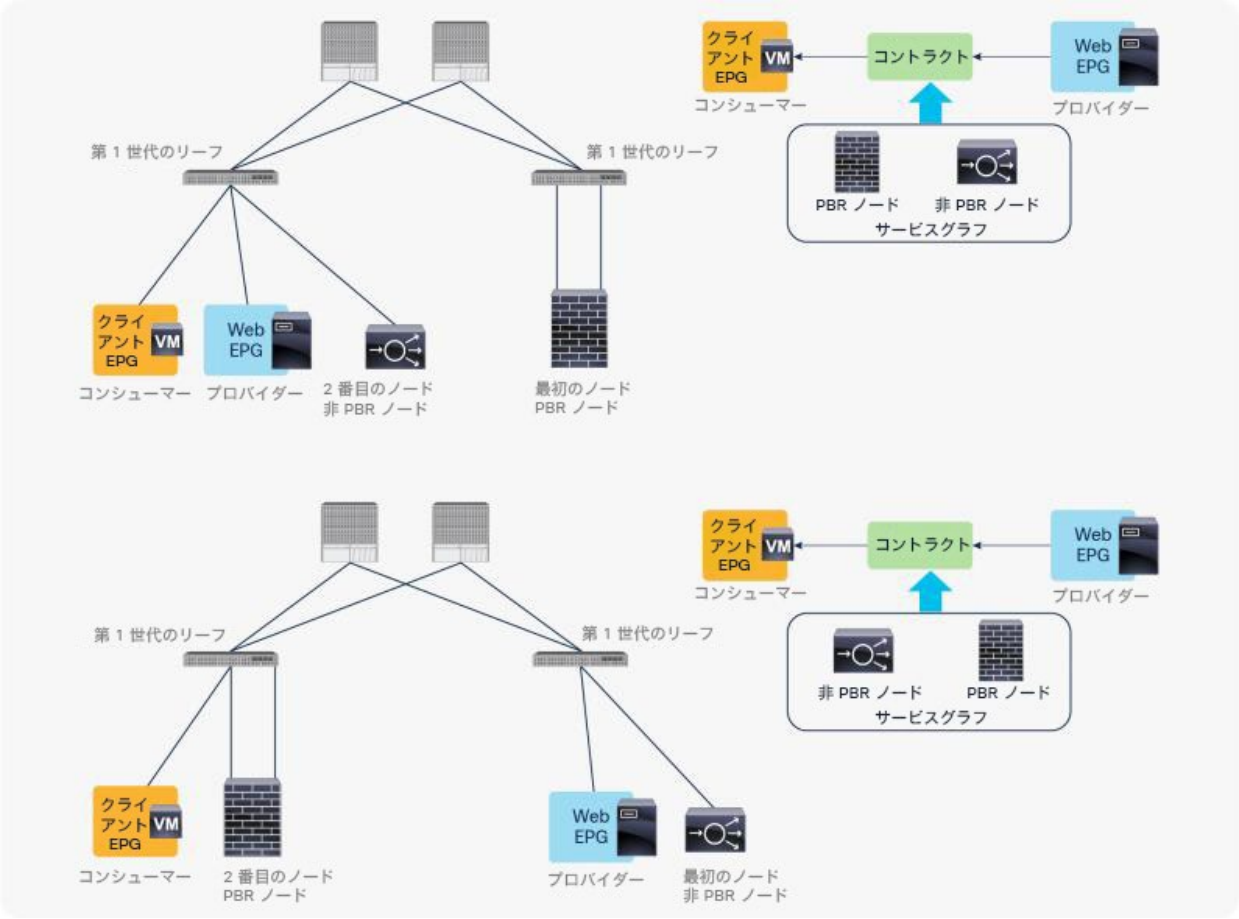


図 43.
Cisco Nexus 9300 プラットフォーム（Cisco Nexus 9300-EX および -FX プラットフォーム以降を除く）のリーフノードに関する考慮事項

PBR が設定されたマルチノードのサービスグラフ

マルチノード PBR は APIC リリース 3.2 で導入されました。PBR をサービスグラフで複数回使用できるため、VRF や BD のサンドイッチ構成を考慮することなく、複数のサービス機能を特定の順序で簡単に挿入できます。

同じサービスグラフ内に、PBR ノードと非 PBR ノードを混在させることができます。次に例を示します。

- FW（PBR）+ IPS（PBR）+ TCP オプティマイザ（PBR）
- FW（PBR）+ IPS（PBR）+ ロードバランサ（非 PBR）

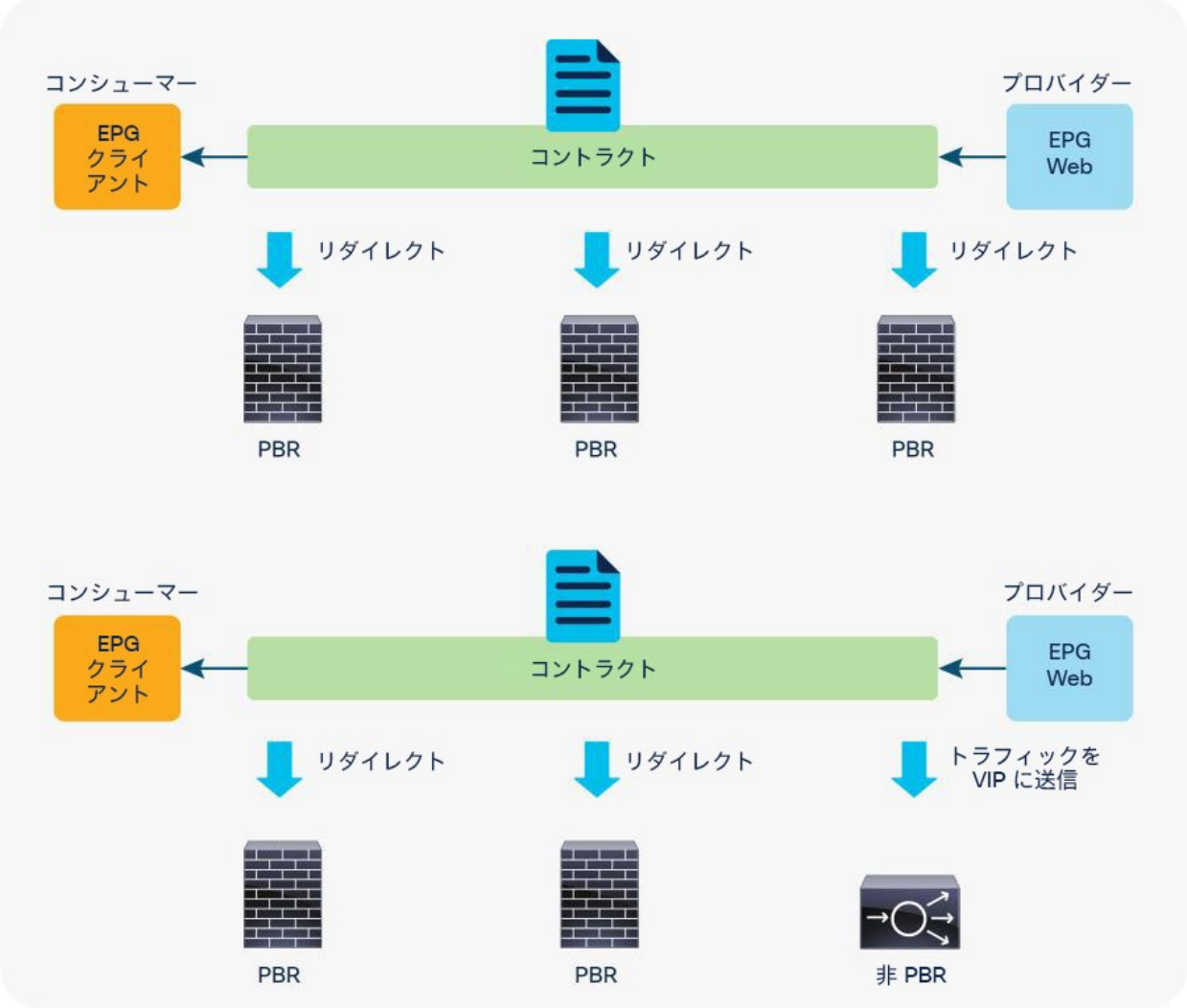


図 44.
マルチノード PBR の例

非 PBR ノードのないマルチノード PBR

図 45 と表 7 は、2 ノード PBR の場合にプログラムされるポリシーの例を示しています。すべてのサービスノードが PBR ノードであれば、単一ノード PBR と同様に動作します。接続先クラス ID は、常にコンシューマー EPG またはプロバイダー EPG のクラス ID です。

- クライアント EPG（クラス ID：100）から Web EPG（クラス ID：300）へのトラフィックは、N1 のコンシューマーコネクタにリダイレクトされます。
- N1 のプロバイダーコネクタ（クラス ID：201）から Web EPG（クラス ID：300）へのトラフィックは、N2 のコンシューマーコネクタにリダイレクトされます。
- N2 のプロバイダーコネクタ（クラス ID：302）から Web EPG（クラス ID：300）へのトラフィックが許可されます。
- Web EPG（クラス ID：300）からクライアント EPG（クラス ID：100）へのトラフィックは、N2 のプロバイダーコネクタにリダイレクトされます。

- N2 のコンシューマーコネクタ（クラス ID：202）から EPG クライアント（クラス ID：100）へのトラフィックは、N1 のプロバイダーコネクタにリダイレクトされます。
- N1 のコンシューマーコネクタ（クラス ID：101）から EPG クライアント（クラス ID：100）へのトラフィックが許可されます。

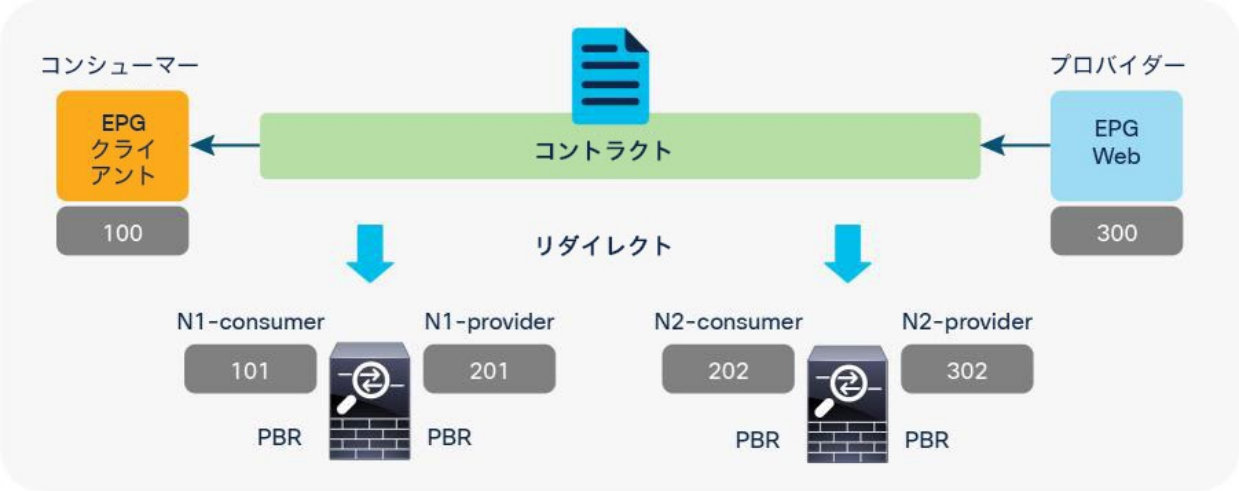


図 45.
2 ノード PBR

表 7. 許可ルールとリダイレクトルール（2 ノード PBR）

送信元クラス ID	接続先クラス ID	フィルタ ID	アクション
100（クライアント EPG）	300（Web EPG）	コントラクトサブジェクトで使用されるフィルタ	N1-consumer にリダイレクト
201（N1 のプロバイダーコネクタ）	300（Web EPG）	デフォルト	N2-consumer にリダイレクト
302（N2 のプロバイダーコネクタ）	300（Web EPG）	デフォルト	許可
300（Web EPG）	100（クライアント EPG）	コントラクトサブジェクトで使用されるフィルタの逆フィルタ	N2-provider にリダイレクト
202（N2 のコンシューマーコネクタ）	100（クライアント EPG）	コントラクトサブジェクトで使用されるフィルタの逆フィルタ	N1-provider にリダイレクト
101（N1 のコンシューマーコネクタ）	100（クライアント EPG）	コントラクトサブジェクトで使用されるフィルタの逆フィルタ	許可

図 46 と表 8 は、3 ノード PBR の場合にプログラムされるポリシーの例を示しています。2 ノード PBR の場合と同様に、送信元と接続先のクラス ID は常にコンシューマー EPG のクラス ID またはプロバイダー EPG のクラス ID です。

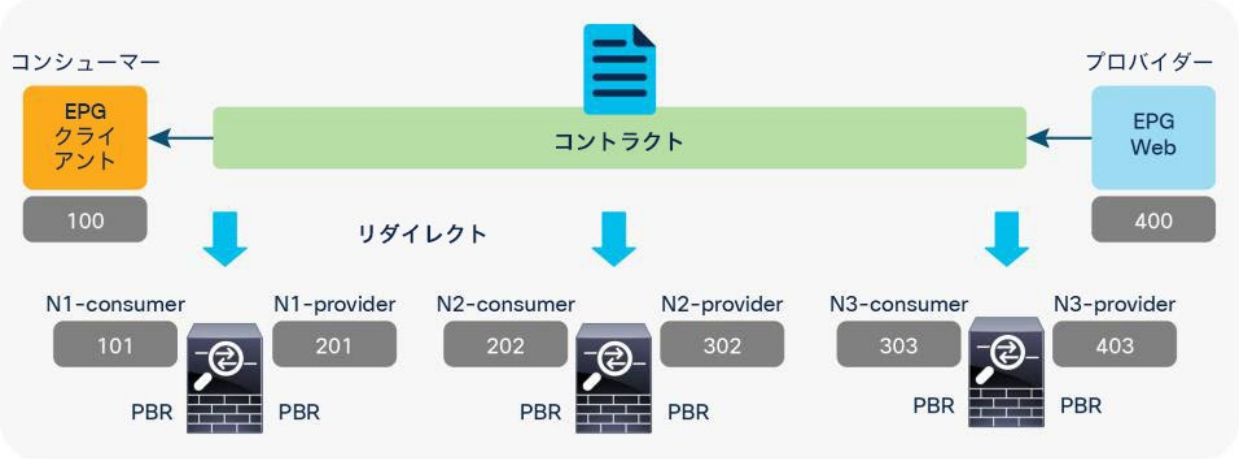


図 46.
3 ノード PBR

表 8. 許可ルールとリダイレクトルール（3 ノード PBR）

送信元クラス ID	接続先クラス ID	フィルタ ID	アクション
100（クライアント EPG）	400（Web EPG）	コントラクトサブジェクトで使用されるフィルタ	N1-consumer にリダイレクト
201（N1 のプロバイダーコネクタ）	400（Web EPG）	デフォルト	N2-consumer にリダイレクト
302（N2 のプロバイダーコネクタ）	400（Web EPG）	デフォルト	N3-consumer にリダイレクト
403（N3 のプロバイダーコネクタ）	400（Web EPG）	デフォルト	許可
400（Web EPG）	100（クライアント EPG）	コントラクトサブジェクトで使用されるフィルタの逆フィルタ	N3-provider にリダイレクト
303（N3 のコンシューマーコネクタ）	100（クライアント EPG）	コントラクトサブジェクトで使用されるフィルタの逆フィルタ	N2-provider にリダイレクト
202（N2 のコンシューマーコネクタ）	100（クライアント EPG）	コントラクトサブジェクトで使用されるフィルタの逆フィルタ	N1-provider にリダイレクト
101（N1 のコンシューマーコネクタ）	100（クライアント EPG）	コントラクトサブジェクトで使用されるフィルタの逆フィルタ	許可

PBR ノードと非 PBR ノードが混在するマルチノード PBR

サービスグラフに PBR ノードと非 PBR ノードの両方がある場合、プログラムされるポリシーは表 7 または表 8 とは異なります。非 PBR ノード（ロードバランサの VIP、NAT を伴うファイアウォールなど）に対してのリダイレクトは不要です。これらのノードがトラフィックの接続先になるためです。PBR が必要な場合は、サービスノードのコネクタがトラフィックの接続先であるかどうかを識別することが重要です。PBR ノードと非 PBR ノードの混在に対処するため、デバイス選択ポリシーに「L3 接続先（VIP）」と呼ばれる新しいフラグが導入されました。これを使用するとサービスチェーン内のトラフィックの接続先を識別できます。

図 47 と表 9 は、N1 と N2 が PBR ノードである 3 ノードのサービスグラフでプログラムされるポリシーの例を示しています。この例では、ファイアウォールと IPS ではアドレス変換が実行されず、N3 のロードバランサ（LB）では送信元 NAT が実行されます。

クライアント EPG からのトラフィックはロードバランサの VIP に送信されるため、トラフィックが N3 を通過するまで、接続先クラス ID はこの VIP がある N3 のコンシューマーコネクタになります。

- クライアント EPG（クラス ID：100）から N3（クラス ID：303）のコンシューマーコネクタへのトラフィックは、N1 のコンシューマーコネクタにリダイレクトされます。
- N1（クラス ID：201）のプロバイダーコネクタから N3（クラス ID：303）のコンシューマーコネクタへのトラフィックは、N2 のコンシューマーコネクタにリダイレクトされます。
- N2（クラス ID：302）のプロバイダーコネクタから N3（クラス ID：303）のコンシューマーコネクタへのトラフィックが許可されます。
- N3（クラス ID：403）のプロバイダーコネクタから Web EPG（クラス ID：400）へのトラフィックが許可されます。

リターントラフィックの場合、接続先クラス ID は N3 のプロバイダーコネクタです。トラフィックが N3 を通過するまでは、ここには送信元 NAT が変換されたアドレスが設定されています。Web EPG（クラス ID：400）から N3 のプロバイダーコネクタへのトラフィックは許可され、次に、トラフィックは N2 のプロバイダーコネクタにリダイレクトされ、さらに N1 のプロバイダーコネクタにリダイレクトされます。この動作はクライアントから Web へのトラフィックフローと同様です。

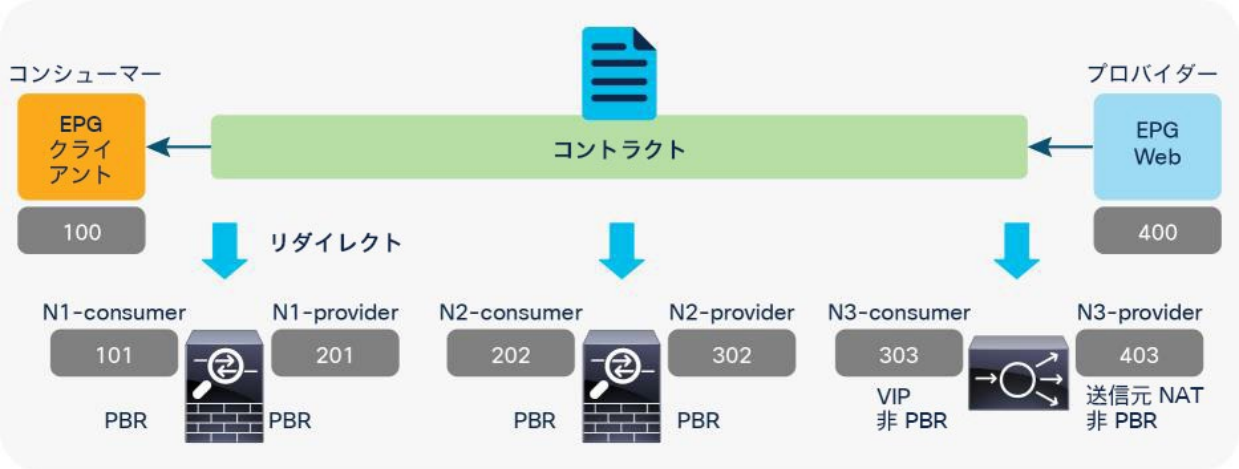


図 47.
PBR ノードと非 PBR ノードの混在（ノード 3 は送信元 NAT を伴うロードバランサ）

表 9. 許可ルールとリダイレクトルール（PBR ノードと非 PBR ノードの混在）

送信元クラス ID	接続先クラス ID	フィルタ ID	アクション
100（クライアント EPG）	**303（N3 のコンシューマーコネクタ。LB の VIP）**	コントラクトサブジェクトで使用されるフィルタ	N1-consumer にリダイレクト
201（N1 のプロバイダーコネクタ）	**303（N3 のコンシューマーコネクタ。LB の VIP）**	デフォルト	N2-consumer にリダイレクト
302（N2 のプロバイダーコネクタ）	**303（N3 のコンシューマーコネクタ。LB の VIP）**	デフォルト	許可
403（N3 のプロバイダーコネクタ）	400（Web EPG）	デフォルト	許可
400（Web EPG）	**403（N3 のプロバイダーコネクタ。SNAT アドレス）**	デフォルト	許可
303（N3 のコンシューマーコネクタ）	100（クライアント EPG）	コントラクトサブジェクトで使用されるフィルタの逆フィルタ	N2-provider にリダイレクト
202（N2 のコンシューマーコネクタ）	100（クライアント EPG）	コントラクトサブジェクトで使用されるフィルタの逆フィルタ	N1-provider にリダイレクト
101（N1 のコンシューマーコネクタ）	100（クライアント EPG）	コントラクトサブジェクトで使用されるフィルタの逆フィルタ	許可

この例では、デバイス選択ポリシーで N3 のコンシューマーコネクタとプロバイダーコネクタに新しいフラグ「L3 接続先（VIP）」を設定し、PBR ポリシーがそれに応じてプログラムされるようにする必要があります。

コントラクトからのフィルタ（filters-from-contract）オプション

サービスグラフテンプレートのコントラクトからのフィルタ（filters-from-contract）オプションは、APIC リリース 4.2(3) で導入されました。これにより、コンシューマー EPG のクラス ID を送信元または接続先として含まないゾーン分割ルールで、デフォルトフィルタの代わりに、サービスグラフがアタッチされたコントラクトサブジェクトで指定されたフィルタを使用できます（デフォルトでは、このオプションは無効化されています。デフォルトの動作については、「データプレーンのプログラミング」セクションを参照してください）。

図 48、表 10、表 11 にユースケースの一例を示します。異なるフィルタを持つコントラクトが同じコンシューマー EPG とプロバイダー EPG のペア間にあり、それぞれのコントラクトに 1 ノードサービスグラフと 2 ノードサービスグラフがアタッチされています。1 ノードサービスグラフがアタッチされたコントラクト 1 は、permit-https フィルタを使用し、2 ノードサービスグラフがアタッチされたコントラクト 2 は、permit-http フィルタを使用します。両方のサービスグラフで使用される最初のサービスノードのインターフェイスは同じです。デフォルトの動作では、コンシューマー EPG のクラス ID を送信元または接続先として含まないゾーン分割ルールでデフォルトフィルタが使用されるため、ゾーン分割ルールが重複して生成されることになります。これら 2 つのサービスグラフによって生成されたゾーン分割ルールには、まったく同じ送信元クラス、接続先クラス、フィルタ（デフォルトフィルタ）でありながら異なるリダイレクト接続先を持つルールが含まれます。コントラクトのフィルタが異なっていても反映しません。したがって、このユースケースでは、異なるポリシーを適用するために、コントラクトからのフィルタ（filters-from-contract）オプションを使用する必要があります。

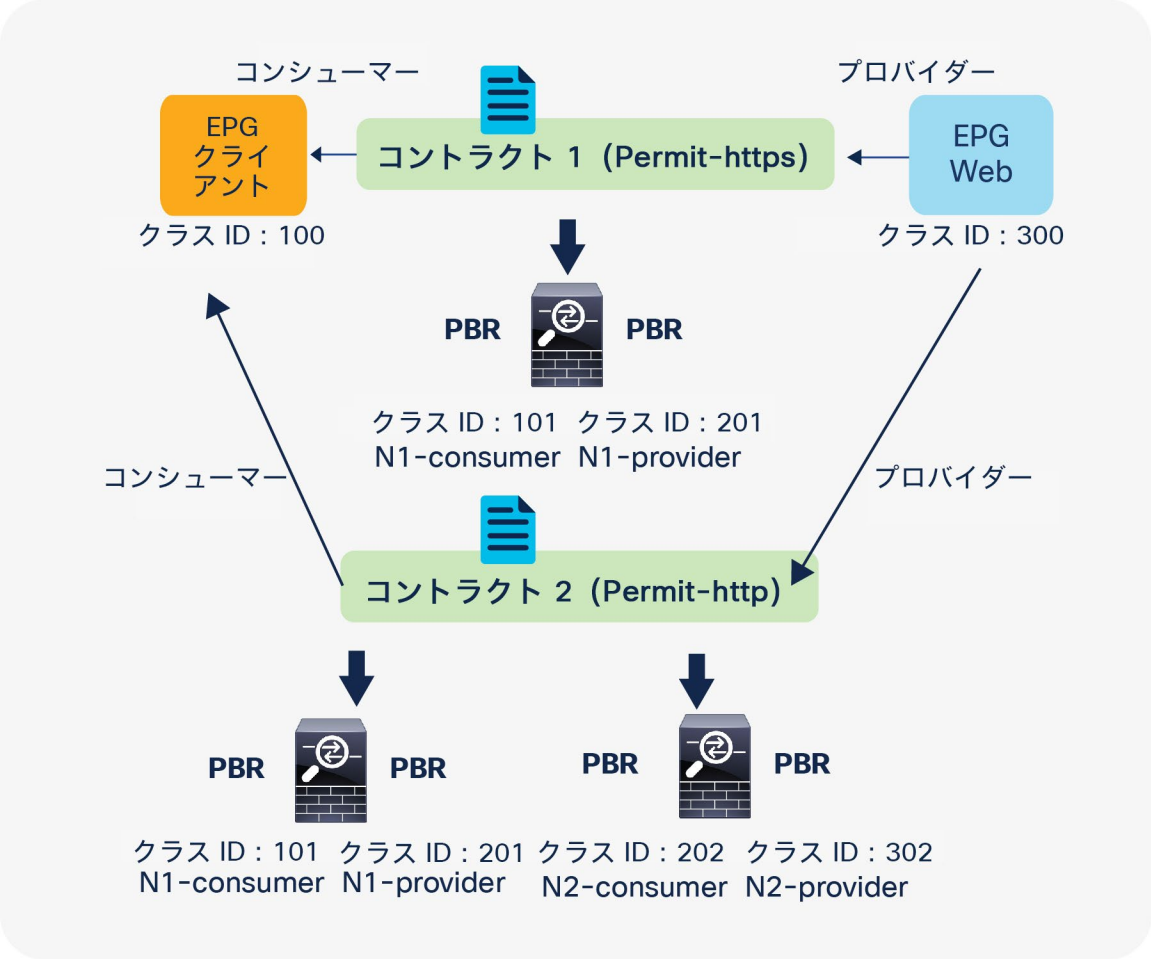


図 48.
同じサービスノードを使用する 1 ノード PBR と 2 ノード PBR

注： 送信元または接続先のクラス ID が一意の場合、コントラクトからのフィルタ（filters-from-contract）オプションは必須ではありません。たとえば、コントラクト 1 とコントラクト 2 のプロバイダー EPG が異なる場合や、最初のサービスノードのプロバイダーコネクタが異なる場合などです。

表 10. 1 ノード PBR の許可ルールとリダイレクトルール（コントラクトからのフィルタ（filters-from-contract）オプションなし）

送信元クラス ID	接続先クラス ID	フィルタ ID	アクション
100（クライアント EPG）	300（Web EPG）	コントラクトサブジェクトで使用されるフィルタ （送信元ポート：任意、接続先ポート：443）	N1-consumer にリダイレクト
201（N1 のプロバイダーコネクタ）	**300（Web EPG）**	**デフォルト**	**許可**
300（Web EPG）	100（クライアント EPG）	コントラクトサブジェクトで使用されるフィルタの逆フィルタ （送信元ポート：443、接続先ポート：任意）	N1-provider にリダイレクト
101（N1 のコンシューマーコネクタ）	100（クライアント EPG）	コントラクトサブジェクトで使用されるフィルタの逆フィルタ （送信元ポート：443、接続先ポート：任意）	許可

表 11. 2 ノード PBR の許可ルールとリダイレクトルール（コントラクトからのフィルタ（filters-from-contract）オプションなし）

送信元クラス ID	接続先クラス ID	フィルタ ID	アクション
100（クライアント EPG）	300（Web EPG）	コントラクトサブジェクトで使用されるフィルタ （送信元ポート：任意、接続先ポート：80）	N1-consumer にリダイレクト
201（N1 のプロバイダーコネクタ）	**300（Web EPG）**	**デフォルト**	**N2-consumer にリダイレクト**
302（N2 のプロバイダーコネクタ）	300（Web EPG）	デフォルト	許可
300（Web EPG）	100（クライアント EPG）	コントラクトサブジェクトで使用されるフィルタの逆フィルタ （送信元ポート：80、接続先ポート：任意）	N2-provider にリダイレクト
202（N2 のコンシューマーコネクタ）	100（クライアント EPG）	コントラクトサブジェクトで使用されるフィルタの逆フィルタ （送信元ポート：80、接続先ポート：任意）	N1-provider にリダイレクト
101（N1 のコンシューマーコネクタ）	100（クライアント EPG）	コントラクトサブジェクトで使用されるフィルタの逆フィルタ （送信元ポート：80、接続先ポート：任意）	許可

いずれかまたは両方のサービスグラフテンプレートでコントラクトからのフィルタ（filters-from-contract）オプションを有効化すると、ゾーン分割ルールが一意になり、異なるポリシーを適用できます。表 12 と表 13 に、両方のサービスグラフテンプレートでコントラクトからのフィルタ（filters-from-Contract）オプションを有効化した場合のゾーン分割ルールの例を示します。

表 12. 1 ノード PBR の許可ルールとダイレクトルール（コントラクトからのフィルタ（filters-from-contract）オプションを使用）

送信元クラス ID	接続先クラス ID	フィルタ ID	アクション
100（クライアント EPG）	300（Web EPG）	コントラクトサブジェクトで使用されるフィルタ（送信元ポート：任意、接続先ポート：443）	N1-consumer にリダイレクト
201（N1 のプロバイダーコネクタ）	**300（Web EPG）**	**コントラクトサブジェクトで使用されるフィルタ（送信元ポート：任意、接続先ポート：443）**	**許可**
300（Web EPG）	100（クライアント EPG）	コントラクトサブジェクトで使用されるフィルタの逆フィルタ（送信元ポート：443、接続先ポート：任意）	N1-provider にリダイレクト
101（N1 のコンシューマーコネクタ）	100（クライアント EPG）	コントラクトサブジェクトで使用されるフィルタの逆フィルタ（送信元ポート：443、接続先ポート：任意）	許可

表 13. 2 ノード PBR の許可ルールとリダイレクトルール（コントラクトからのフィルタ（filters-from-contract）オプションを使用）

送信元クラス ID	接続先クラス ID	フィルタ ID	アクション
100（クライアント EPG）	300（Web EPG）	コントラクトサブジェクトで使用されるフィルタ（送信元ポート：任意、接続先ポート：80）	N1-consumer にリダイレクト
201（N1 のプロバイダーコネクタ）	**300（Web EPG）**	**コントラクトサブジェクトで使用されるフィルタ（送信元ポート：任意、接続先ポート：80）**	**N2-consumer にリダイレクト**
302（N2 のプロバイダーコネクタ）	**300（Web EPG）**	**コントラクトサブジェクトで使用されるフィルタ（送信元ポート：任意、接続先ポート：80）**	**許可**
300（Web EPG）	100（クライアント EPG）	コントラクトサブジェクトで使用されるフィルタの逆フィルタ（送信元ポート：80、接続先ポート：任意）	N2-provider にリダイレクト
202（N2 のコンシューマーコネクタ）	100（クライアント EPG）	コントラクトサブジェクトで使用されるフィルタの逆フィルタ（送信元ポート：80、接続先ポート：任意）	N1-provider にリダイレクト
101（N1 のコンシューマーコネクタ）	100（クライアント EPG）	コントラクトサブジェクトで使用されるフィルタの逆フィルタ（送信元ポート：80、接続先ポート：任意）	許可

PBR が設定されたサービスグラフの再利用

サービスグラフテンプレートと L4-L7 デバイスは、複数のコントラクトで再利用できます。たとえば、1 つのテナント内の複数の EPG 間トラフィックフローにファイアウォールを挿入する場合、同じファイアウォールを同じインターフェイスまたは異なるインターフェイスで使用することが考えられます。どちらの設計も可能です。

異なるインターフェイスで同じ PBR ノードを再利用

同じ PBR ノードを階層ごとに異なるインターフェイスで再利用できます。L3Out EPG から Web EPG へのトラフィックは FW-external にリダイレクトされ、リターントラフィックは FW-internal1 にリダイレクトされます。Web EPG からアプリケーション EPG へのトラフィックは FW-internal1 にリダイレクトされ、リターントラフィックは FW-internal2 にリダイレクトされます（図 49）。

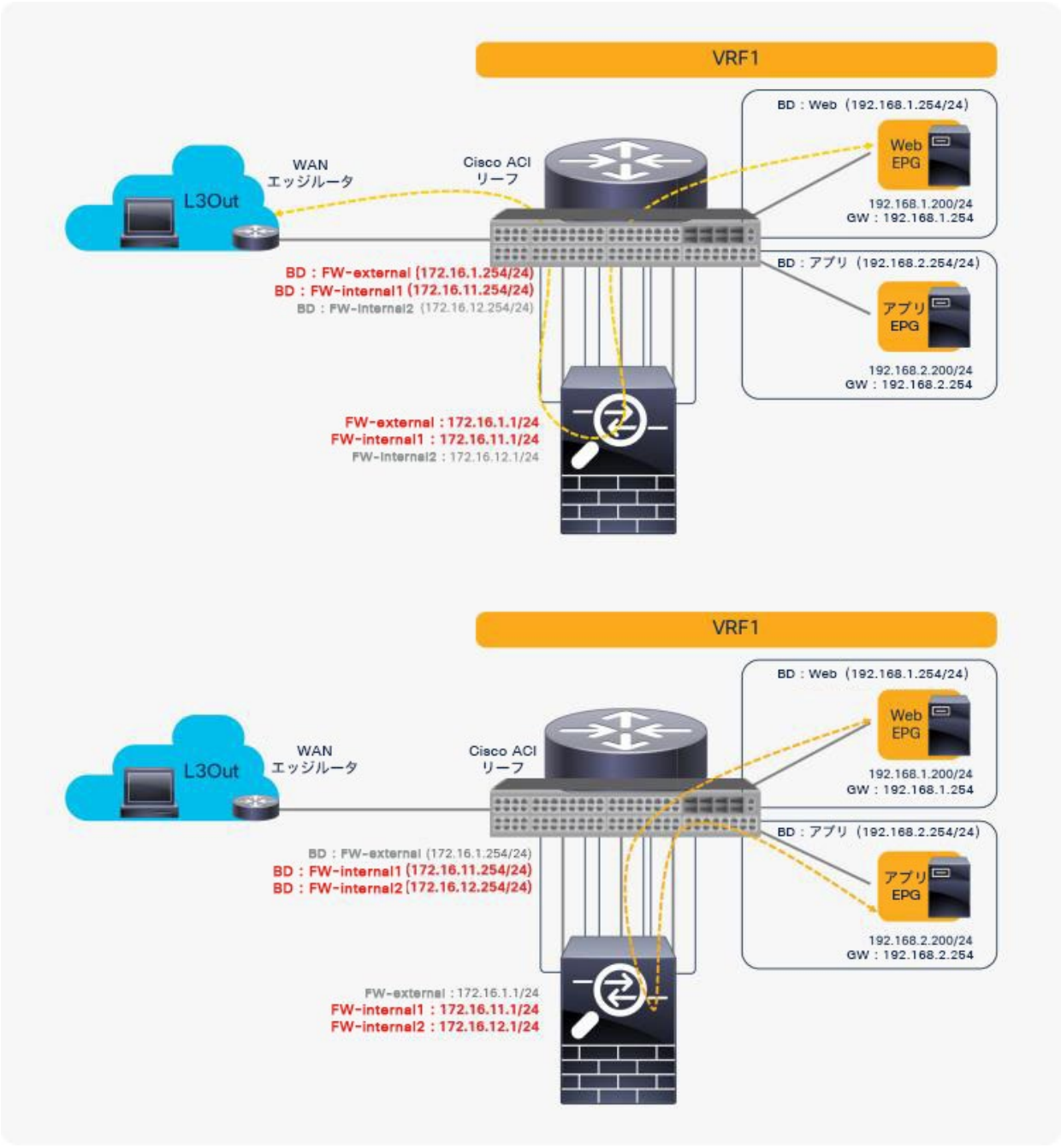


図 49.
同じ PBR ノードを再利用（異なるインターフェイスを使用）

この場合、サービスグラフテンプレートと L4-L7 デバイスを再利用できます。送信元 EPG と接続先 EPG のペアに基づいて別のインターフェイスにトラフィックをリダイレクトするには、別の PBR ポリシーとデバイス選択ポリシーが必要です（PBR を使用するサービスグラフの設定に関する基本情報については、このドキュメントで後ほど説明します）。

設定例を次に示します（図 50）。

- コントラクト：[テナント（Tenant）] > [セキュリティポリシー（Security Policies）] > [コントラクト（Contracts）]
  - コントラクト 1：L3Out EPG と Web EPG の間
  - コントラクト 2：Web EPG とアプリケーション EPG の間
- L4-L7 デバイス：[テナント（Tenant）] > [L4-L7サービス（L4-L7 Services）] > [L4-L7デバイス（L4-L7 Devices）]
  - PBRnode1 には 3 つのクラスタインターフェイスがあります。
  - FW-external：L3Out 接続のセキュリティゾーン
  - FW-internal1：Web EPG のセキュリティゾーン
  - FW-internal2：アプリケーション EPG のセキュリティゾーン
- サービスグラフテンプレート：[テナント（Tenant）] > [L4-L7サービス（L4-L7 Services）] > [L4-L7サービスグラフテンプレート（L4-L7 Service Graph Templates）]
  - FWGraph1：ノード 1 は、PBR が有効化されたファイアウォール機能ノードです。
- PBR ポリシー：[テナント（Tenant）] > [ネットワーク（Networking）] > [プロトコルポリシー（Protocol Policies）] > [L4-L7ポリシーベースリダイレクト（L4-L7 Policy Based Redirect）]
  - PBR-policy1（172.16.1.1、MAC A）
  - PBR-policy2（172.16.11.1、MAC B）
  - PBR-policy3（172.16.12.1、MAC C）
- デバイス選択ポリシー：[テナント（Tenant）] > [L4-L7サービス（L4-L7 Services）] > [デバイス選択ポリシー（Device Selection Policies）]
  - Contract1-FWGraph1-FW（FWGraph1 がコントラクト 1 に適用されている場合、このノードがファイアウォール機能ノードになります）
  - ノード：PBRnode1
  - コンシューマー：PBR-policy1 が適用される FW-external
  - プロバイダー：PBR-policy2 が適用される FW-internal1
  - Contract2-FWGraph1-FW（FWGraph1 がコントラクト 2 に適用されている場合、このノードがファイアウォール機能ノードになります）
  - ノード：PBRnode1

- コンシューマー：PBR-policy2 が適用される FW-internal1
- プロバイダー：PBR-policy3 が適用される FW-internal2

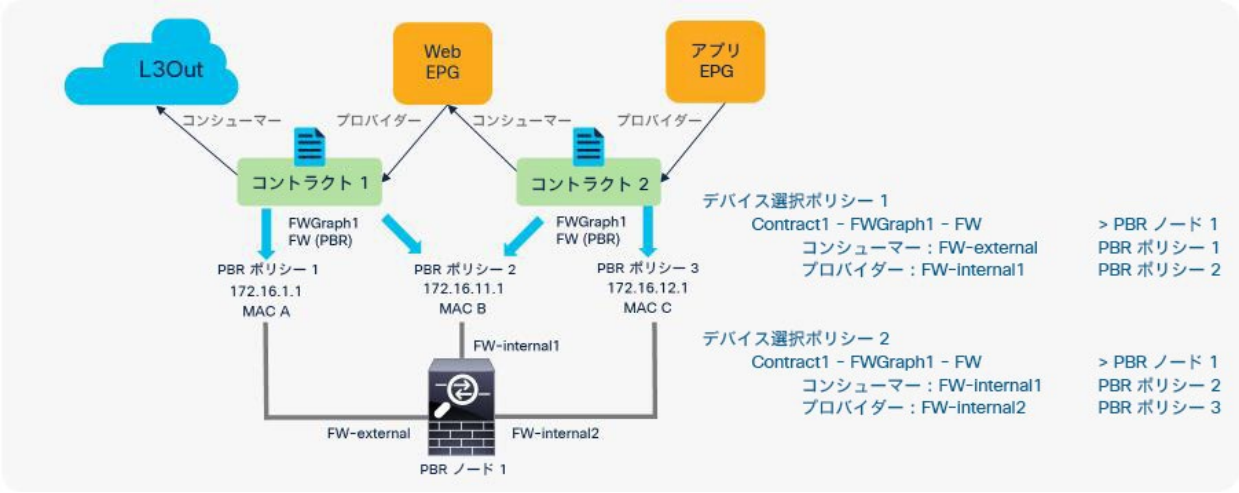


図 50.
設定例：同じ PBR ノードを再利用（異なるインターフェイスを使用）

同じ PBR ノードと同じインターフェイスを再利用

同じ PBR ノードとそのインターフェイスを使用する場合、サービスグラフテンプレート、L4-L7 デバイス、PBR ポリシー、デバイス選択ポリシーを再利用できます。この例では、L3Out EPG と Web EPG の間にあるトラフィック、Web EPG とアプリケーション EPG の間にあるトラフィックが FW-one-arm にリダイレクトされます（図 51）。

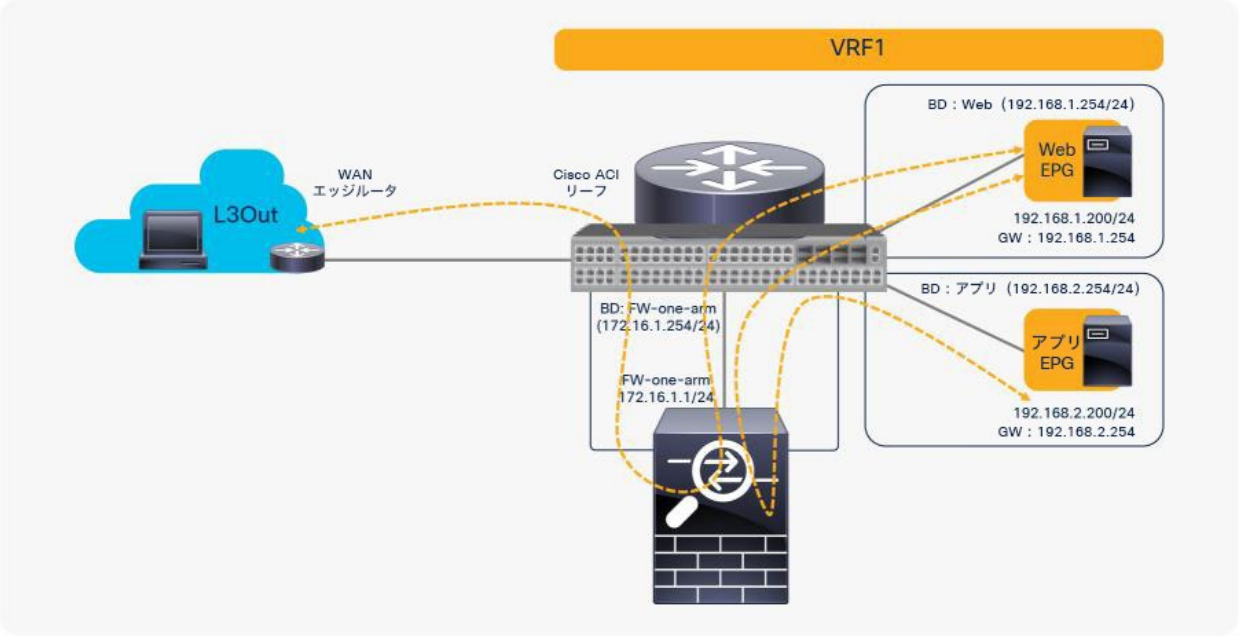


図 51.
同じ PBR ノードを再利用（ワンアームモードで同じインターフェイスを使用）

設定例を次に示します（図 52）。

- コントラクト：[テナント（Tenant）] > [セキュリティポリシー（Security Policies）] > [コントラクト（Contracts）]
  - コントラクト 1：L3Out EPG と Web EPG の間
  - コントラクト 2：Web EPG とアプリケーション EPG の間
- L4-L7 デバイス：[テナント（Tenant）] > [L4-L7サービス（L4-L7 Services）] > [L4-L7デバイス（L4-L7 Devices）]
  - PBRnode1 にはクラスタインターフェイスが 1 つあります。
  - これが FW-one-arm です。
- サービスグラフテンプレート：[テナント（Tenant）] > [L4-L7サービス（L4-L7 Services）] > [L4-L7サービスグラフテンプレート（L4-L7 Service Graph Templates）]
  - FWGraph1：ノード 1 は、PBR が有効化されたファイアウォール機能ノードです。
- PBR ポリシー：[テナント（Tenant）] > [ネットワーク（Networking）] > [プロトコルポリシー（Protocol Policies）] > [L4-L7ポリシーベースリダイレクト（L4-L7 Policy Based Redirect）]
  - PBR-policy1（172.16.1.1、MAC A）
- デバイス選択ポリシー：[テナント（Tenant）] > [L4-L7サービス（L4-L7 Services）] > [デバイス選択ポリシー（Device Selection Policies）]
  - any-FWGraph1-FW（FWGraph1 がいずれかのコントラクトに適用されている場合、このノードがファイアウォール機能ノードになります）
  - ノード：PBRnode1
  - コンシューマー：PBR-policy1 が適用される FW-one-arm
  - プロバイダー：PBR-policy1 が適用される FW-one-arm

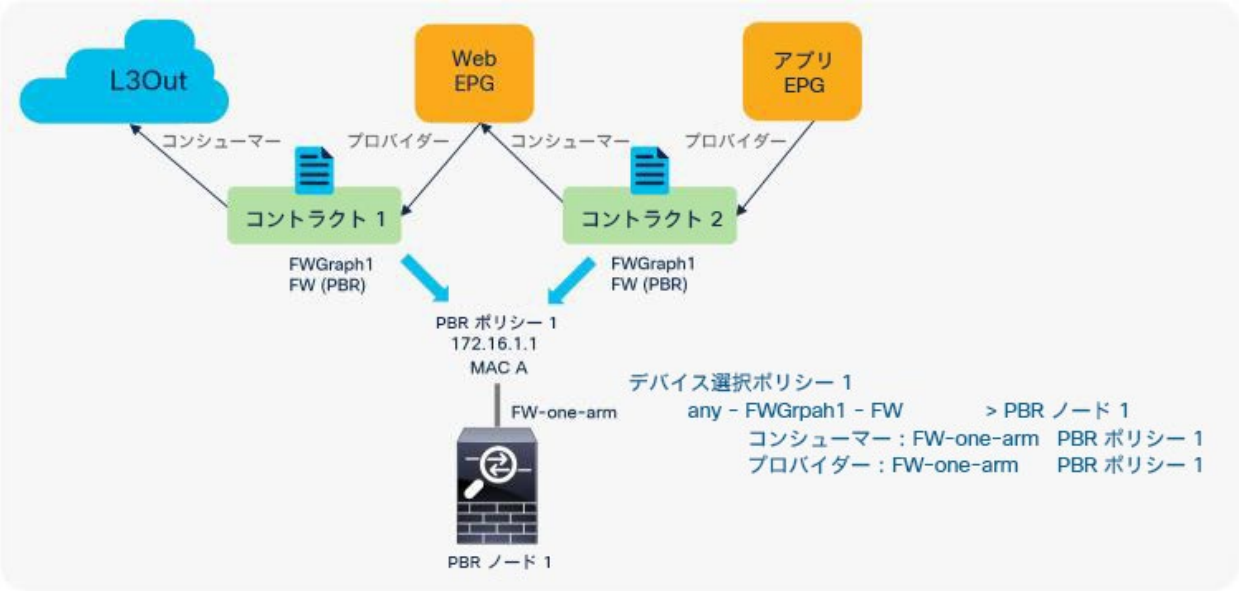


図 52.
設定例：同じ PBR ノードを再利用（同じインターフェイスを使用）

ワンアームモードを使用したり、EPG ごとに異なるインターフェイスを使用したりするのではなく、2 つのインターフェイスを備えたファイアウォールを使用できるのではないかと思われるかもしれません。たとえば、コンシューマーまたはプロバイダーになっている EPG を識別することなく、コンシューマーからプロバイダーへのトラフィックであれば常に FW-external インターフェイスにリダイレクトし、プロバイダーからコンシューマーへのトラフィックであれば常に FW-internal インターフェイスにリダイレクトする方法が考えられるかもしれません（図 53）。

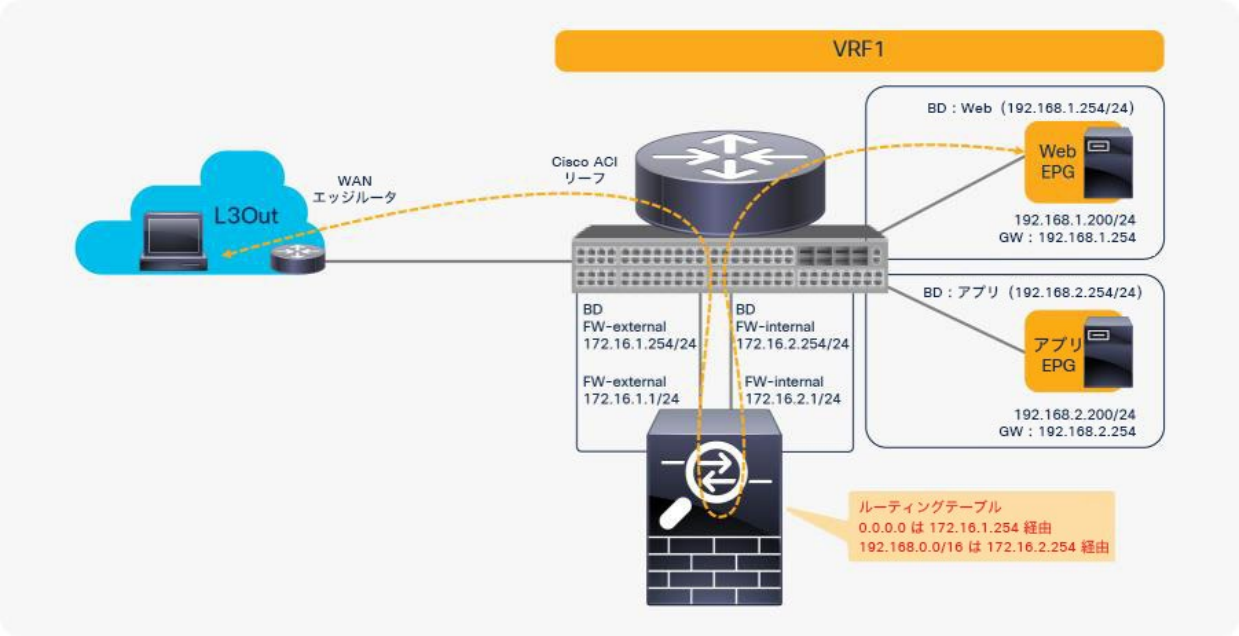


図 53.
同じ PBR ノードを再利用（垂直方向トラフィックにツーアームモードを使用）

このような設計の問題は、ファイアウォールにおけるルーティング設定にあります。おそらくファイアウォールでは、FW-external ブリッジドメインに 172.16.1.254 を介した 0.0.0.0/0 へのルートが、FW-internal ブリッジドメインに 172.16.2.254 を介した 192.168.1.0/24 へのルートが設定されています。これは、L3Out EPG と Web EPG の間のトラフィックにとっては問題ありません。ただし、Web EPG とアプリケーション EPG 間のトラフィックについては、FW-internal ブリッジドメインに 172.16.2.254 を介した 192.168.2.0/24 へのルートが設定されています。アプリケーション EPG から Web EPG に送信されるトラフィックが FW-internal にリダイレクトされる場合、ファイアウォールは、172.16.2.254 をネクストホップとして使用してトラフィックを返信します。192.168.1.0/24 と 192.168.2.0/24 の両方が 172.16.2.254 をネクストホップとして使用しているためです。その結果、インターフェイス内でのトラフィックの転送を伴うワンアーム設計のようなトラフィックパスが生成されます。したがって、垂直方向トラフィックにはツーアーム設計を使用できますが、水平方向トラフィックにはワンアーム設計を使用する必要があります。これは、PBR ノードのルーティングテーブルに起因します（図 54）。

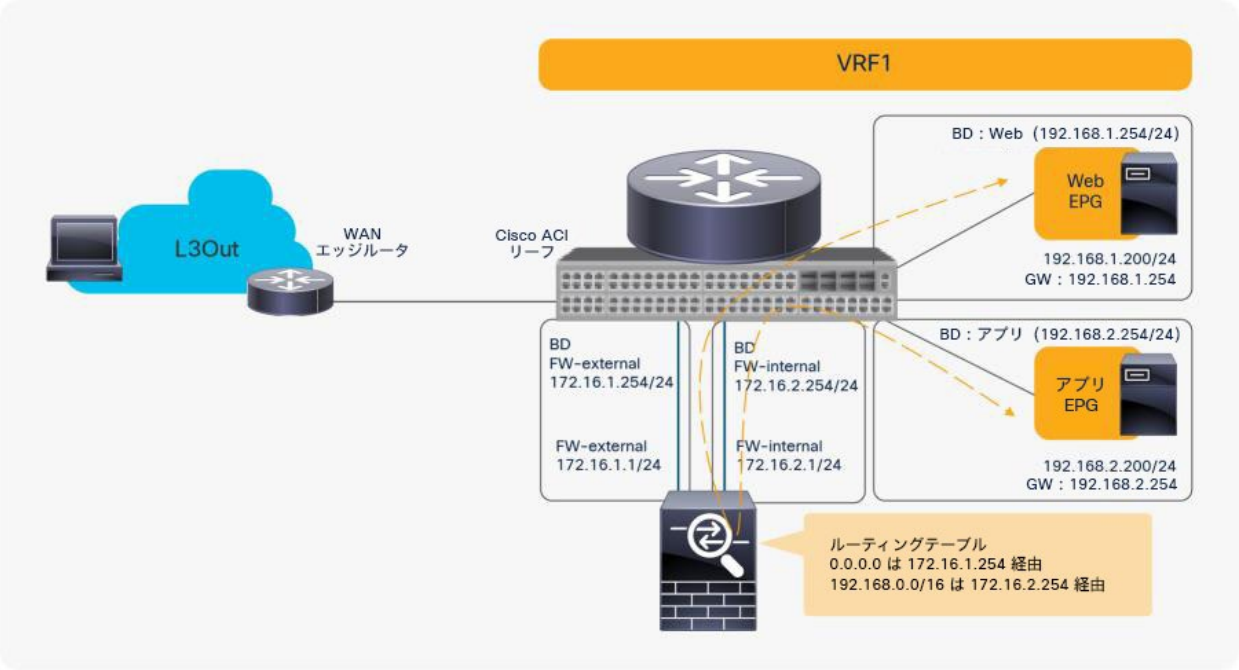


図 54.
同じ PBR ノードを再利用（水平方向トラフィックにワンアームモードを使用）

vzAny を使用する場合の PBR

vzAny 管理対象オブジェクトとは、1 つの VRF インスタンスにあるすべての EPG 集合のことです。このオブジェクトは VRF 内のすべての EPG に適用されるセキュリティ要件がある場合に役立ちます。ポリシー TCAM の使用量も削減できます。

APIC リリース 3.2 より前のバージョンで、PBR が設定されたサービスグラフを vzAny をプロバイダーとするコントラクトに関連付けることはできませんが、vzAny をコンシューマーとする場合は可能です。これを利用すると、コンシューマーである 1 つの VRF にあるすべての EPG と共有サービスのプロバイダーとの間のトラフィックを処理するサービスノードを挿入できます。図 55 にその例を示します。vzAny をコンシューマーとし、NFS（ネットワーク ファイル システム）EPG をプロバイダーとするコントラクトが VRF1 にあり、PBR が設定されていれば、VRF1 のすべてのエンドポイントからの NFS アクセスをファイアウォールで検査でき、複数のコンシューマー EPG のためにポリシー TCAM を消費することはありません。

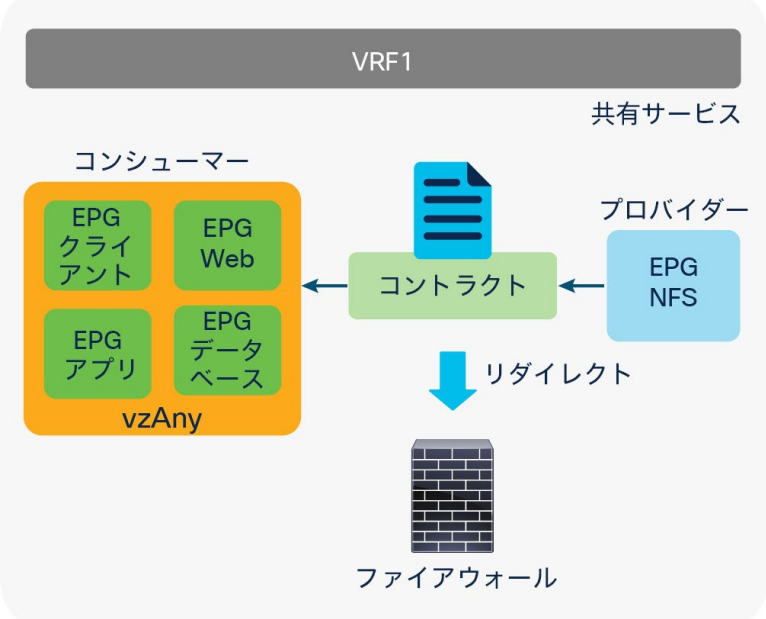


図 55.
コンシューマーとしての vzAny（共有サービスプロバイダーのユースケース）

APIC リリース 3.2 以降のリリースでは、vzAny をプロバイダーとするコントラクトでの PBR もサポートされます。これを利用すると、1 つの VRF にあるすべての EPG 間にサービスノードを挿入できます。図 56 にその例を示します。PBR が設定されたコントラクトで、コンシューマーとプロバイダーの両方を vzAny にすると、その VRF 内のエンドポイント間のすべてのトラフィックをファイアウォールで検査できます。

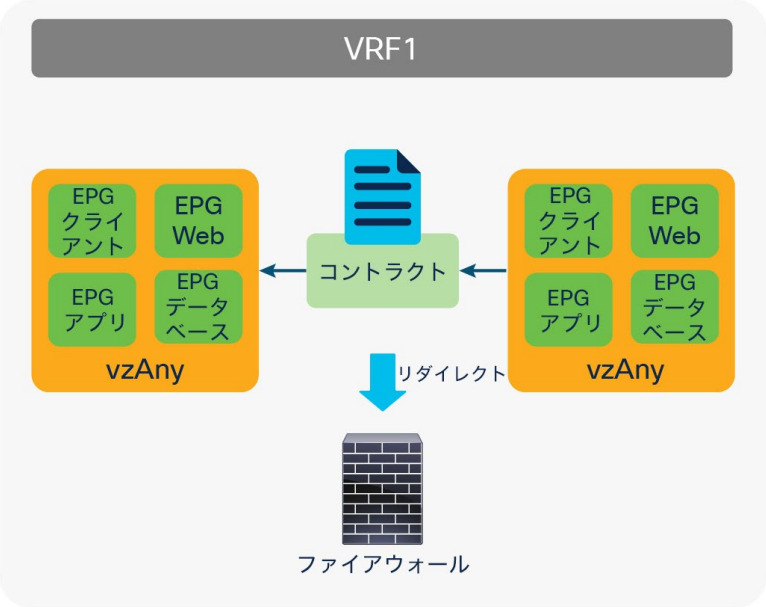


図 56.
コンシューマーとプロバイダーの両方が vzAny（「すべての EPG からすべての EPG」 のユースケース）

注： 「すべての EPG からすべての EPG」のユースケースでは、コンシューマーからプロバイダーへのトラフィックに適用されるルールとプロバイダーからコンシューマーへのトラフィックに適用されるルールが同じであるため、ワンアーム設計を使用する必要があります。どちらも vzAny から vzAny であるため、異なるアクションを使用することはできません（図 57 を参照）。

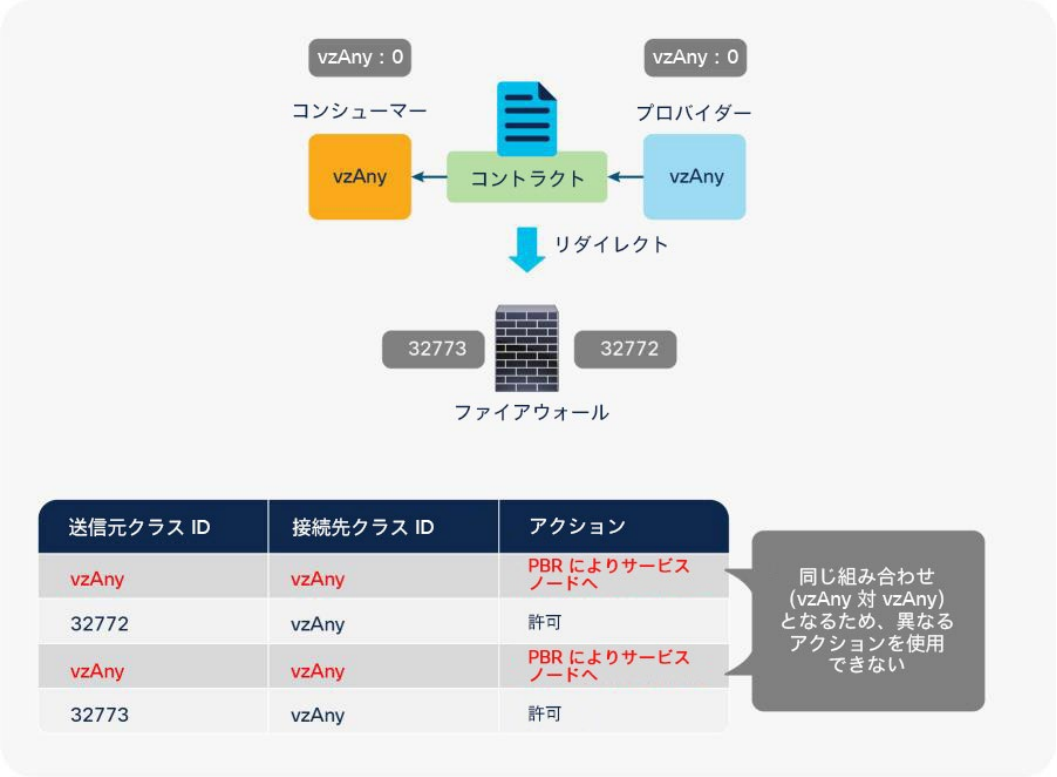


図 57.
「すべての EPG からすべての EPG」のユースケースでワンアームモードのみが機能する理由

サービスノードから ACI ファブリックに戻るトラフィックは、「すべての EPG からすべての EPG」 の PBR ルールがあってもリダイレクトされません。これは、より制約の強いフィルタルールが優先されるためです。たとえば、vzAny から vzAny へのトラフィックがサービスノードにリダイレクトされた後、そのトラフィックが ACI ファブリックに戻るとします。ここで、送信元クラス ID は 32773（PBR ノード）、接続先クラス ID は 0（vzAny）です。これは、「vzAny から vzAny」よりも制約の強いルールです。そのため、トラフィックはリダイレクトされずに許可されます（表 14）。

表 14. 許可ルールとリダイレクトルール（ワンアームを使用した「すべての EPG からすべての EPG」のユースケース）

送信元クラス ID	接続先クラス ID	フィルタ ID	アクション
0（vzAny）	0（vzAny）	コントラクトサブジェクトで使用されるフィルタ	サービスノードにリダイレクト
32773（サービスノードのインターフェイス）	0（vzAny）	デフォルト	許可
0（vzAny）	0（vzAny）	コントラクトサブジェクトで使用されるフィルタの逆フィルタ	サービスノードにリダイレクト
32773（サービスノードのインターフェイス）	0（vzAny）	コントラクトサブジェクトで使用されるフィルタの逆フィルタ	許可

注： vzAny がコンシューマーとしてもプロバイダーとしても使用されている場合は、共通デフォルトフィルタを使用しないでください。これは、ARP、イーサネットトラフィック、その他の非 IP トラフィックが含まれていて、これらがリダイレクトの対象となるためです。ARP Glean などの一部のインフラサービスは、リダイレクトされないポリシーを採用しています。PBR を使用する場合は、IP トラフィックのみがサポートされます。

EPG 内コントラクトを使用した PBR

EPG 内コントラクトとは、同じ EPG にあるエンドポイントに適用されるコントラクトのことです。これは、同じ EPG にあってもセキュリティを適用する必要がある場合に役立ちます。

APIC リリース 4.0 より前のリリースでは、サービスグラフを EPG 内コントラクトに関連付けることはできません。APIC リリース 4.0 以降のリリースでは、EPG 内コントラクトを使用した PBR がサポートされます。これを利用すると、同じ EPG にあるエンドポイント間のトラフィックを処理するサービスノードを挿入できます。図 58 にその例を示します。

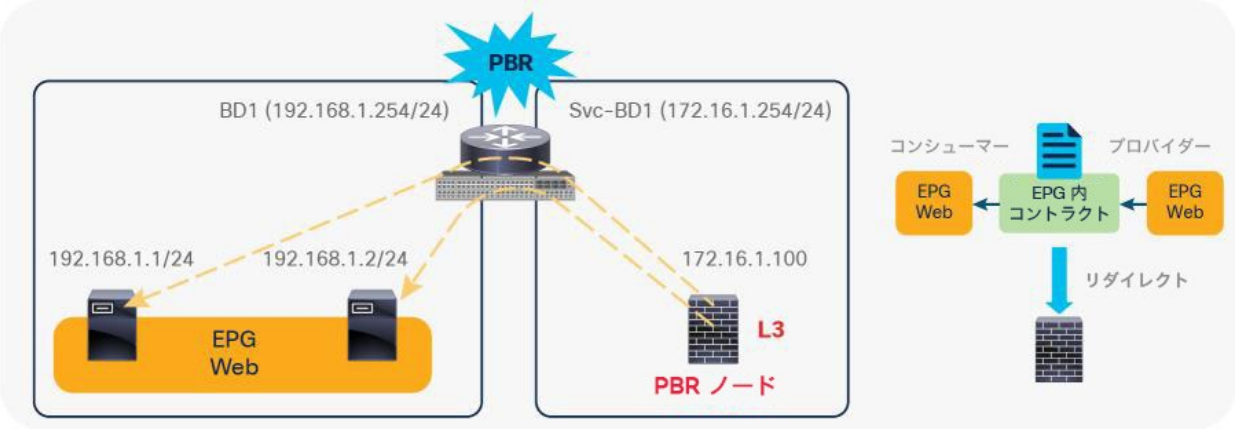


図 58.
EPG 内コントラクトを使用した PBR の例

EPG 内コントラクトを使用する場合の Cisco ACI PBR に関する主な考慮事項は次のとおりです。

- ワンアーム設計を使用する必要があります。
- PBR もコピーも設定されていないサービスグラフがアタッチされた EPG 内コントラクトは無意味です。PBR を使用せずに同じ BD にあるエンドポイント間にサービスノードを挿入する方法がないためです。
- 主なユースケースは、セキュリティデバイスの挿入です。ファイアウォールや IPS などが挿入できます。ロードバランサのユースケースはこのドキュメントの対象外です。

APIC リリース 5.2 以降では、L3Out EPG（外部 EPG）の外部 EPG 内コントラクトに PBR を設定できます。外部 EPG 内コントラクトで PBR を使用する際の注意点は次のとおりです。

- 0.0.0.0/0 または 0::0 の L3Out EPG で外部 EPG 内コントラクトを使用することはできません。このような L3Out EPG で外部 EPG 内コントラクトが設定されている場合、APIC のエラーが発生します。この問題を回避するには、L3Out EPG に 0.0.0.0/1 と 128.0.0.0/1 を使用してすべてのサブネットをキャッチします。これは、サブネットが 0.0.0.0/0 または 0::0 である L3Out EPG は pcTag が 2 つある動作をするためです。サブネットが 0.0.0.0/0 である L3Out EPG の詳細については、ACI コントラクトガイドを参照してください。
- EPG の EPG 内コントラクトとは異なり、L3Out EPG の外部 EPG 内コントラクトの場合、暗黙の拒否ルールは自動的には**追加されません**。他のトラフィックを拒否するには、Intra Ext-EPG isolation（外部 EPG 内での分離）を有効化する必要があります。

PBR が設定されたサービスグラフがクライアント EPG（クラス ID 49155）間の EPG 内コントラクトに適用される前に、それらの間の許可エントリと暗黙の拒否エントリがリーフノードでプログラムされます（図 59 および表 15）。クライアント EPG のエンドポイント間のトラフィックがコントラクトのフィルタとマッチした場合、EPG 内の許可ルールは暗黙の拒否ルールよりも優先度が高いため、トラフィックは許可されます。

```
Podi-Leaf1# show zoning-rule scope 2490368 | grep 49155
<sip>
| 4220 | 49155 | 49155 |    9    | uni-dir-ignore | enabled | 2490368 | intra-EPG | permit      | class-eq-filter(1) |
| 4214 | 49155 | 49155 |    8    |     bi-dir     | enabled | 2490368 | intra-EPG | permit      | class-eq-filter(1) |
| 4231 | 49155 | 49155 | implict |    uni-dir     | enabled | 2490368 |           | deny, log   | class-eq-deny(2)   |
```

図 59.
EPG 内コントラクトのゾーン分割ルールの例（PBR なし）

表 15. PBR が設定されていない場合の許可ルールと拒否ルール

送信元クラス ID	接続先クラス ID	フィルタ ID	アクション
49155（クライアント EPG）	49155（クライアント EPG）	9（コントラクトサブジェクトで使用されるフィルタ）	許可
49155（クライアント EPG）	49155（クライアント EPG）	8（コントラクトサブジェクトで使用されるフィルタの逆フィルタ）	許可
49155（クライアント EPG）	49155（クライアント EPG）	デフォルト（暗黙）	拒否

注： L3Out EPG の外部 EPG 内コントラクトの場合、暗黙の拒否ルールは自動的には**追加されません**。他の EPG 内トラフィックを拒否するには、Intra Ext-EPG isolation（外部 EPG 内での分離）を有効化する必要があります。

サービスグラフが展開されると、サービスノードのクラス ID が作成され、許可ルールが更新されます（図 60 および表 16 を参照）。

```
Pod1-Leaf1# show zoning-rule scope 2490368 | grep 49155
<snip>
| 4214 | 16386 | 49155 |     8     |    uni-dir     | enabled | 2490368 |     |     permit      |    fully_qual(7)    |
| 4220 | 49155 | 49155 |     8     |     bi-dir     | enabled | 2490368 |     |redir(destgrp-4)|  class-eq-filter(1) |
| 4183 | 49155 | 49155 |     9     |uni-dir-ignore  | enabled | 2490368 |     |redir(destgrp-4)|  class-eq-filter(1) |
| 4207 | 16386 | 49155 |  default  |    uni-dir     | enabled | 2490368 |     |     permit      |    arc_dst_any(9)   |
| 4231 | 49155 | 49155 | implicit  |    uni-dir     | enabled | 2490368 |     |    deny,log     |   class-eq-deny(2)  |
```

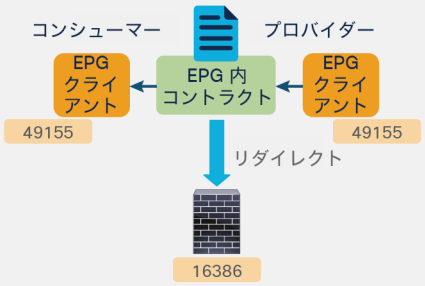


図 60.
EPG 内コントラクトのゾーン分割ルールの例（PBR あり）

表 16. PBR が設定された場合の許可ルール

送信元クラス ID	接続先クラス ID	フィルタ ID	アクション
49155（クライアント EPG）	49155（クライアント EPG）	9（コントラクトサブジェクトで使用されるフィルタ）	サービスノードにリダイレクト
16386（サービスノードのコネクタ）	49155（クライアント EPG）	デフォルト	許可
49155（クライアント EPG）	49155（クライアント EPG）	8（コントラクトサブジェクトで使用されるフィルタの逆フィルタ）	サービスノードにリダイレクト
16386（サービスノードのコネクタ）	49155（クライアント EPG）	8（コントラクトサブジェクトで使用されるフィルタの逆フィルタ）	許可
49155（クライアント EPG）	49155（クライアント EPG）	デフォルト（暗黙）	拒否

注： EPG 内コントラクトと外部 EPG 内コントラクトを使用する場合、PBR にワンアーム設計を使用する必要があります。前のセクションの「vzAny から vzAny」ユースケースと同様、コンシューマーからプロバイダーへのトラフィックに適用されるルールがプロバイダーからコンシューマーへのトラフィックに適用されるルールと同じになるためです。

オプション機能

このセクションでは、いくつかのオプション機能について説明します。PBR ノードトラッキング、Cisco ACI マルチポッド設計におけるロケーションベースの PBR、同じサブネット内に PBR ノード、コンシューマー EPG、プロバイダー EPG がある場合の設計を取り上げます。

PBR ノードトラッキング

PBR ノードトラッキングは、APIC リリース 2.2(3j) およびリリース 3.1 で導入されました。トラッキングにより、ダウンしている PBR ノードへのトラフィックのリダイレクトを防ぐことができます。サービスノード（PBR 接続先）がダウンした場合、PBR ハッシュ機能によりポリシーで使用可能な PBR ノードの選択を開始できます。この機能には、Cisco Nexus 9300-EX および -FX プラットフォーム リーフ スイッチ以降が必要です。

概要

図 61 に、PBR ノードトラッキングの動作を示します。PBR ノードが接続されているサービスリーフノードが、Internet Control Message Protocol（ICMP）、Transmission Control Protocol（TCP）、L2Ping、HTTP を使用してローカル PBR ノードに定期的にキープアライブを送信し、次に、システム全体に向けたブロードキャストメッセージによって他のすべてのリーフスイッチに可用性情報を定期的にアナウンスします。この情報により、ローカルで PBR ポリシーを適用する際に、すべてのリーフノードが、対象の PBR ノードが引き続き使用できるかどうかを確認できます。APIC リリース 5.2(1) 以降では、この定期的なアナウンスを使用して PBR 接続先 MAC をアナウンスすることにより、MAC 設定のない L3 PBR（PBR 接続先の 動的 MAC 検出）を実現しています。

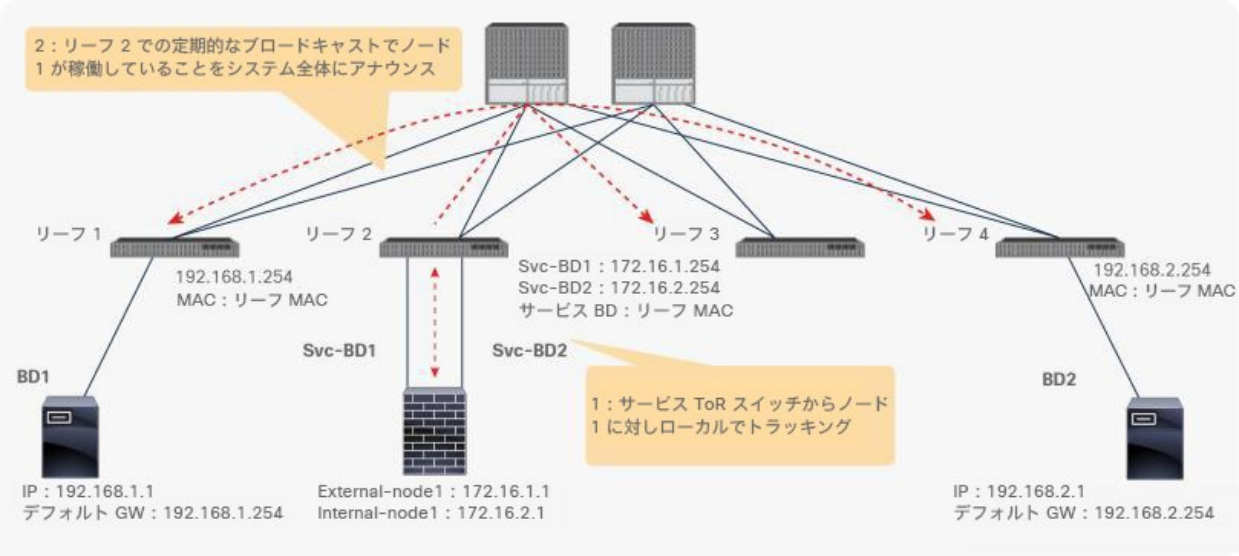


図 61.
トラッキング動作

次のトラッキングタイプがサポートされています。

- L3 PBR に対する TCP（APIC リリース 2.2(3j) 以降）
- L3 PBR に対する ICMP（APIC リリース 3.1 以降）
- L1/L2 PBR に対する L2Ping（APIC リリース 4.1 以降）
- L3 PBR に対する HTTP（APIC リリース 5.2 以降）

ヘルスグループ

PBR ノードのコンシューマーコネクタまたはプロバイダーコネクタのみがダウンしている場合はどうなるでしょうか。トラフィックがブラックホールに入らないようにするために、Cisco ACI は、両方向のトラフィックで PBR ノードの使用を避ける必要があります。一部の L4-L7 デバイスには、1 つのインターフェイスがダウンしている場合に他のインターフェイスをダウンさせる機能が備わっています。L4-L7 デバイスでこの機能を使用すると、ブラックホールに入るのを回避できます。PBR ノードにこの機能がない場合、コンシューマーコネクタまたはプロバイダーコネクタのいずれかがダウンした際に、ヘルスグループ機能を使用してこのノードへの PBR を無効化する必要があります。

それぞれの PBR 接続先の IP と MAC アドレスをヘルスグループに含めることができます。たとえば、PBR ノードの接続先が 2 つあるとします。1 つは、コンシューマーコネクタとして 172.16.1.1 を持ち、プロバイダーコネクタとして 172.16.2.1 を持っています。これらは Health-group1 に属しています。もう 1 つは、コンシューマーコネクタとして 172.16.1.2 を持ち、プロバイダーコネクタとして 172.16.2.2 を持っています。これらは Health-group2 に属しています。同じヘルスグループ内の PBR 接続先のいずれかがダウンしている場合、そのノードは PBR に使用されません（図 62）。

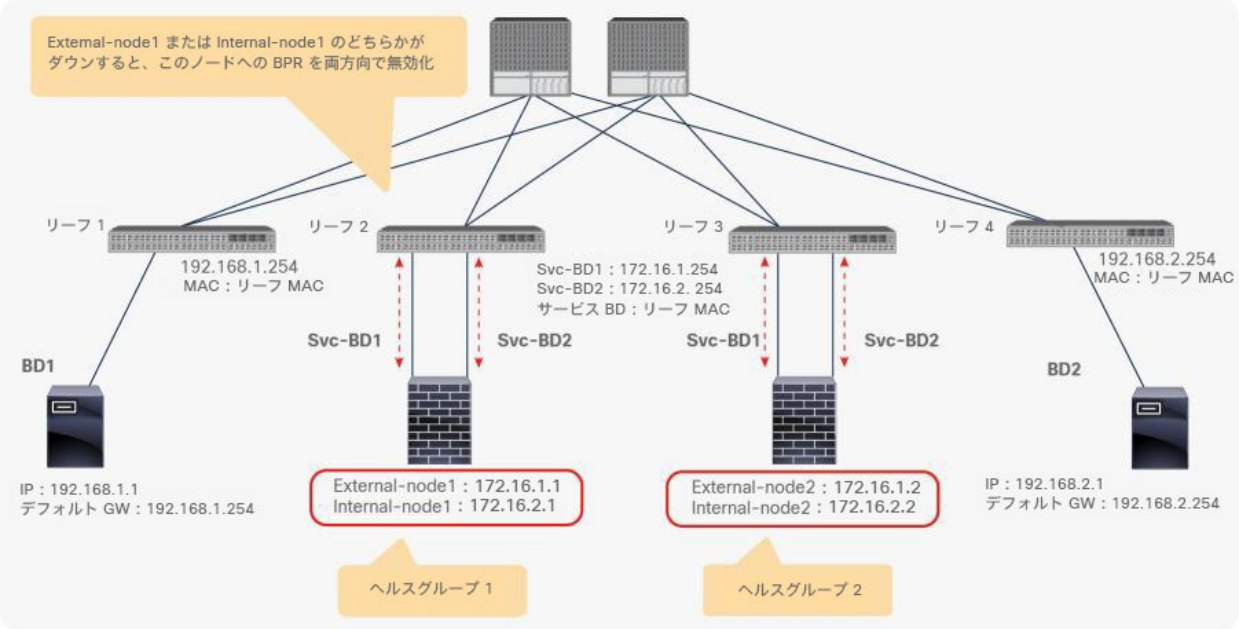


図 62.
ヘルスグループ機能

しきい値

L4-L7 デバイスがボトルネックになっていないこと、およびトラフィックを処理するのに十分な数の L4-L7 デバイスが利用できることを確認する必要があります。PBR の有効化の可否を判断するために、PBR トラッキングでは、PBR ポリシーで使用可能な PBR 接続先の割合をベースとする最小しきい値と最大しきい値を設定できます。使用可能な PBR 接続先の数が最小割合を下回ると、トラフィックがリダイレクトされずに許可またはドロップされます。これはダウンアクションの許可、拒否、バイパスの各設定に基づいて実行されます。これについては、次のセクションで説明します。トラフィックが再度リダイレクトされるには、使用可能な PBR 接続先の数が最大割合に達している必要があります。

たとえば、しきい値機能が有効化された PBR 接続先が 5 つあり、最小割合として 20%、最大割合として 80% が設定されているとします。最初はすべての PBR 接続先が稼働していて、トラフィックが PBR ノード 1 ~ 5 に負荷分散されているとします。ノード 1 ~ 4 がダウンすると、稼働しているノードの割合が 20% 以下であるため、PBR は無効化されます。ノード 4 が再度稼働した場合（つまり、ノード 4 と 5 が稼働している）でも、割合がまだ 80% 未満であるため、PBR は無効化されたままです。ノード 2 ~ 5 が稼働した場合、割合が 80% になるため、PBR は再度有効化されます（図 63）。

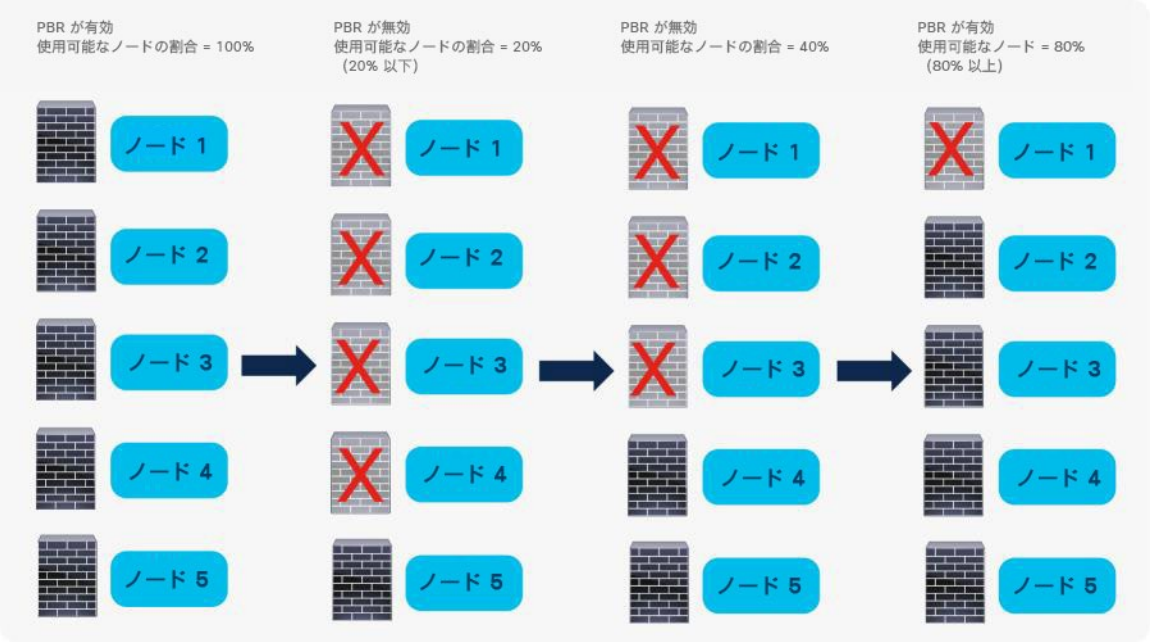


図 63.
しきい値機能

ダウンアクション

前のセクションで説明したように、PBR ノードトラッキングでは、PBR ポリシーで使用可能な PBR 接続先の数がしきい値として設定された最小割合を下回った場合の動作を設定できます。この設定可能な動作は、ダウンアクションと呼ばれます。ダウンアクションの使用可能なオプションを表 17 に示します。

表 17. ダウンアクションのオプション

ダウンアクション	最初に導入されたときの Cisco ACI リリース	動作	ユースケース
許可（デフォルト）	2.2(3j)	トラフィックは PBR なしで接続先に直接送信されます。	1 ノードサービスグラフの必須でないサービスノードをスキップする場合。
拒否	3.1	トラフィックはドロップされます。	必須のサービスを挿入する場合。
バイパス	4.1.2	トラフィックは、サービスグラフ内の次の PBR ノードにリダイレクトされます。	マルチノードサービスグラフの必須でないサービスノードをスキップする場合。

ダウンアクションに関する設計上の考慮事項は次のとおりです。

- ダウンアクションを使用するには、トラッキングとしきい値を有効化する必要があります。
- PBR ノードのプロバイダーコネクタとコンシューマーコネクタの両方で同じダウンアクションを使用します。ダウンアクションをこのように設定しないと、サービスグラフを展開するときにテナントで APIC のエラーが発生します。

デフォルトのダウンアクションは「許可」です。つまり、エンドポイント間のトラフィックが許可されます。ダウンアクション「許可」のユースケースとしては、トラフィックオプティマイザなどのオプションのサービスノードに PBR を使用するシナリオがあります。このようなサービスノードは、トラフィックをドロップせずにスキップさせることができます（図 64）。

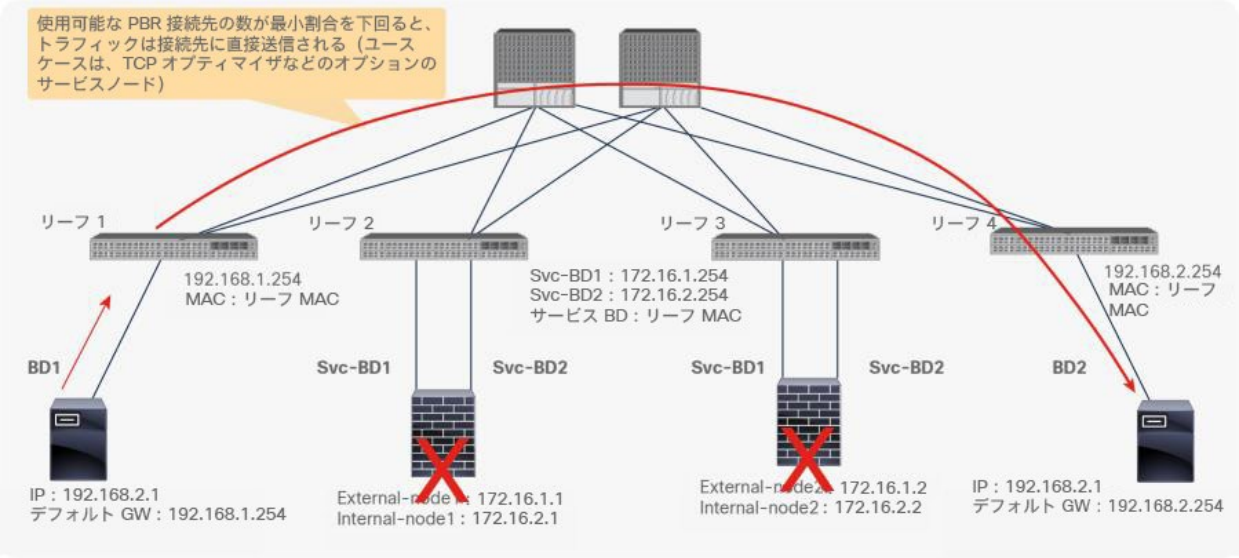


図 64.
ダウンアクション「許可」

ダウンアクションを「拒否」に設定すると、エンドポイント間でトラフィックがドロップされます。ダウンアクション「拒否」のユースケースとしては、挿入が必須のファイアウォール、IPS、またはセキュリティサービスノードへの PBR があります（図 65）。

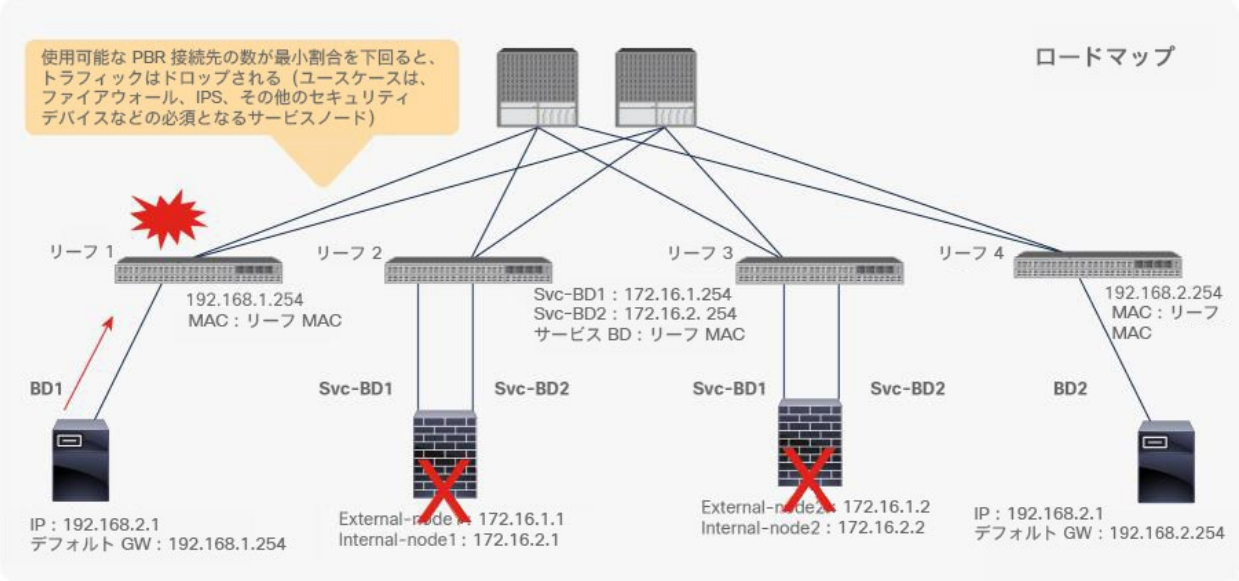


図 65.
ダウンアクション「拒否」

APIC リリース 4.1.2 以降では、「バイパス」アクションが導入されています。これを使用すると、マルチノード PBR サービスグラフにバイパス可能なオプションのサービスノードを追加できます。図 66 に、最初の機能ノードと 2 番目の機能ノードがある 2 ノードのサービスグラフを使用した例を示します。各機能ノードには、1 つの PBR ポリシーに属する 1 つ以上の PBR 接続先を設定できます。最初の機能ノードの PBR ポリシーで使用可能な PBR 接続先の数が最小割合を下回ると、トラフィックは、バックアップパスとなる 2 番目の機能ノードの PBR ポリシーで使用可能な PBR 接続先の 1 つにリダイレクトされます。トラフィックがドロップされたり、許可されて接続先に直接送信されたりすることはありません。

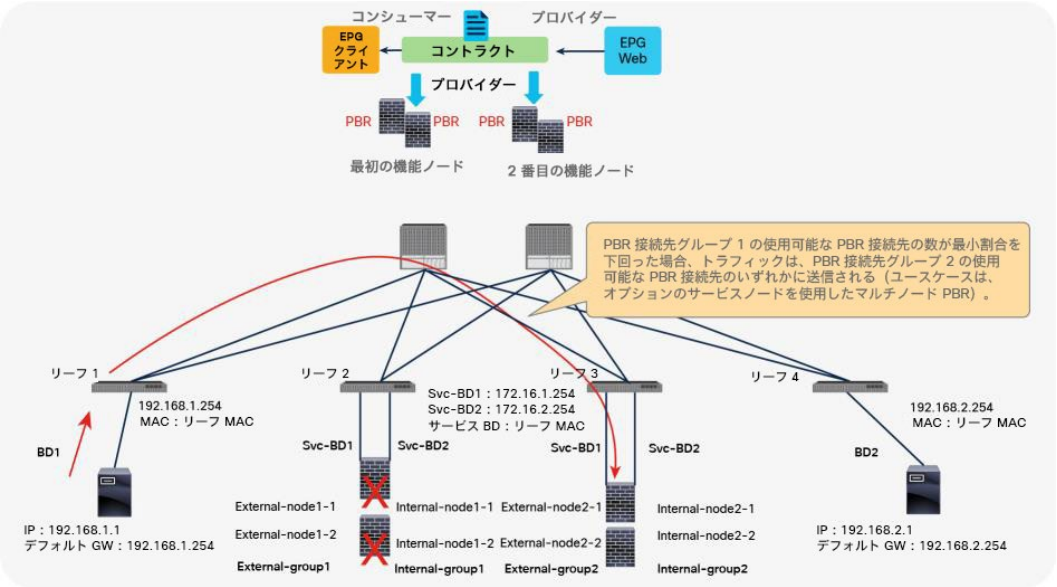


図 66.
ダウンアクション「バイパス」

2 番目の機能ノードの PBR ポリシーでも使用可能な PBR 接続先の数が最小割合を下回った場合、トラフィックは 2 番目の機能ノードもバイパスします。つまり、許可されて接続先に直接送信されます。

バイパスアクションに関する設計上の考慮事項は次のとおりです。

- バイパス機能は、1 ノードサービスグラフでは必要ありません。
- APIC リリース 5.0 より前のリリースでは、L1/L2 PBR が設定されたバイパス機能はサポートされません。
- NAT を実行するサービスノードは、トラフィックフローが中断されるためバイパスできません。
- APIC リリース 5.0 では、バイパスと次の機能との併用はサポートされません。
  - リモートリーフ
  - ワンアームモードの L4-L7 デバイス（バイパスは、ツーアームモードの L4-L7 デバイスでのみ機能します）
  - 複数のサービスグラフで同じ PBR ポリシーを使用し、バイパスアクションが有効化されている場合、同じ PBR 接続先の IP アドレスと MAC アドレスを持つ一意の「PBR ポリシー名」を使用する必要があります。PBR ポリシーが複数のサービスグラフで使用されている場合、バイパスを有効化して同じその PBR ポリシーを使用すると APIC で設定が拒否されます（CSCvp29837）。これは、バイパスアクションのバックアップが PBR ポリシーごとに設定されるためです。バイパスが有効化されている場合、同じ PBR ポリシーを異なるサービスグラフで使用しても、バイパスのバックアップはサービスグラフごとに異なっている可能性があります（図 67 と図 68）。この回避策は L3 PBR にのみ適用できます。APIC リリース 5.0 では、L1/L2 PBR の場合、異なる PBR ポリシーで PBR 接続先の IP、MAC、具象インターフェイスをまったく同じにすることはできません。

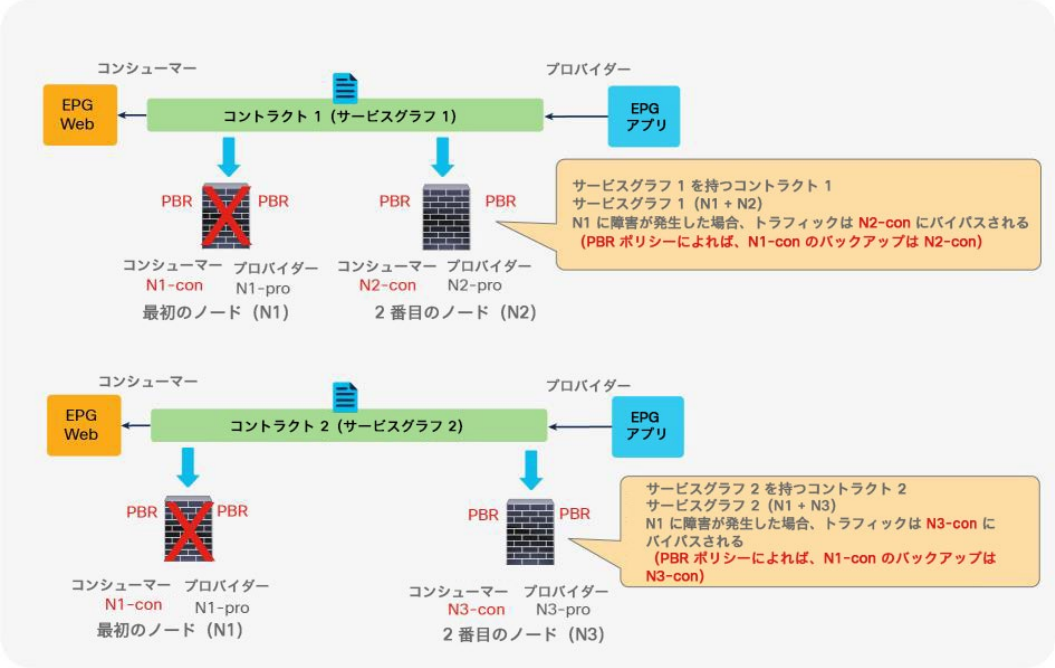


図 67.
設計上の考慮事項：PBR 接続先が複数のサービスグラフで使用されていて、バイパスアクションが有効化されている

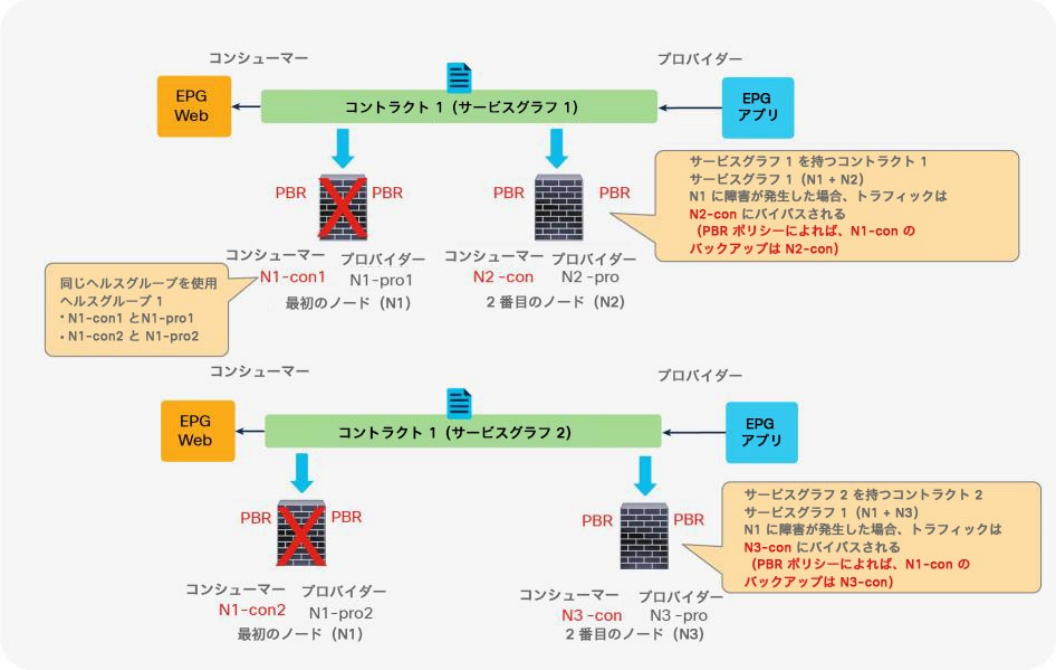


図 68.
回避策：同じ PBR 接続先の IP と MAC を使用した一意の PBR ポリシー名を使用

注： PBR 接続先の IP アドレスと MAC アドレスが同じであるため、これらの PBR ポリシーには同じヘルスグループを使用してください。

復元力のあるハッシュ

PBR ポリシー内のいずれかの PBR ノードがダウンしたにも関わらず PBR が依然として有効化されている場合、デフォルトでは、PBR ポリシー内の使用可能な PBR ノードを使用してトラフィックが再ハッシュされます。その使用可能な PBR ノードを通過していた一部のトラフィックは、別の PBR ノードに負荷分散され、障害が発生した PBR ノードを通過していなかったにも関らず、影響を受ける可能性があります。そのトラフィックを受信した新しい PBR ノードがそれまでの接続情報を持っていないためです（図 69）。

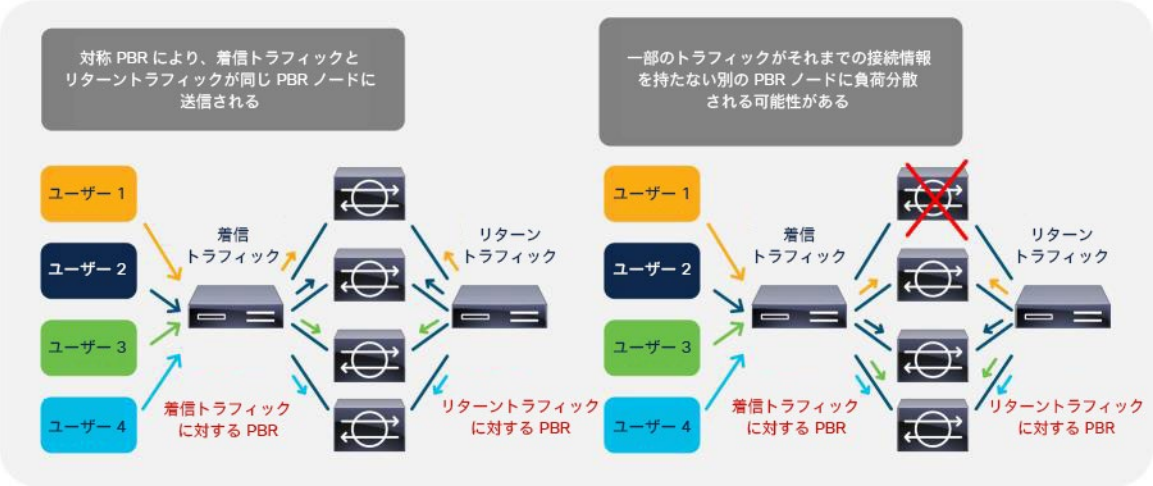


図 69.
PBR ノード障害時の動作（デフォルト：復元力のあるハッシュが無効）

復元力のあるハッシュ PBR（APIC リリース 3.2 で導入）を使用すると、障害が発生したノードを通過していたトラフィックのみが別の使用可能な PBR ノードにリダイレクトされます。他のトラフィックは引き続き同じノードにリダイレクトされるため、他の PBR ノードを通過するトラフィックは影響を受けません（図 70 を参照）。

復元力のあるハッシュは、L4-L7 の PBR ポリシーで設定できます。

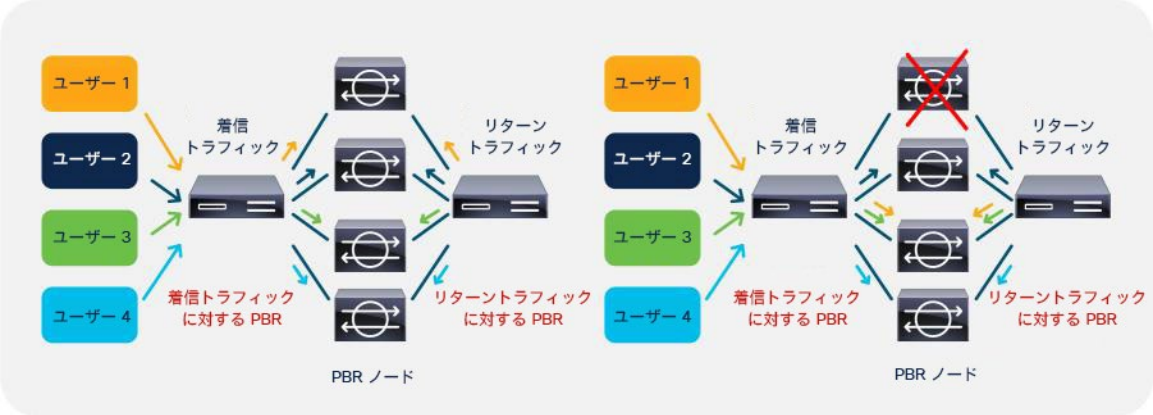


図 70.
PBR ノード障害時の動作（復元力のあるハッシュが有効）

注：　障害が発生したノードを通過していたトラフィックは、使用可能な複数の PBR ノードに再分散されず、**使用可能な PBR ノードの 1 つ**にリダイレクトされます。これは、復元力と負荷分散の間のトレードオフです。PBR ノード障害時の PBR ノードのキャパシティが懸念される場合は、バックアップ PBR ノードを使用して、障害が発生したノードを通過していたトラフィックを処理できます。詳細については、「バックアップ PBR ポリシー（N+M 高可用性）」セクションを参照してください。

注： 複数の障害が発生している場合、状況によっては、使用可能なノードを通過するトラフィックが再ハッシュされている可能性があります。たとえば、ノード A が停止し、その後ノード B が停止し、その後ノード D が停止した場合（図 71 を参照）、ノード C、E、F にハッシュされたトラフィック 3、5、6 は影響を受けていません。

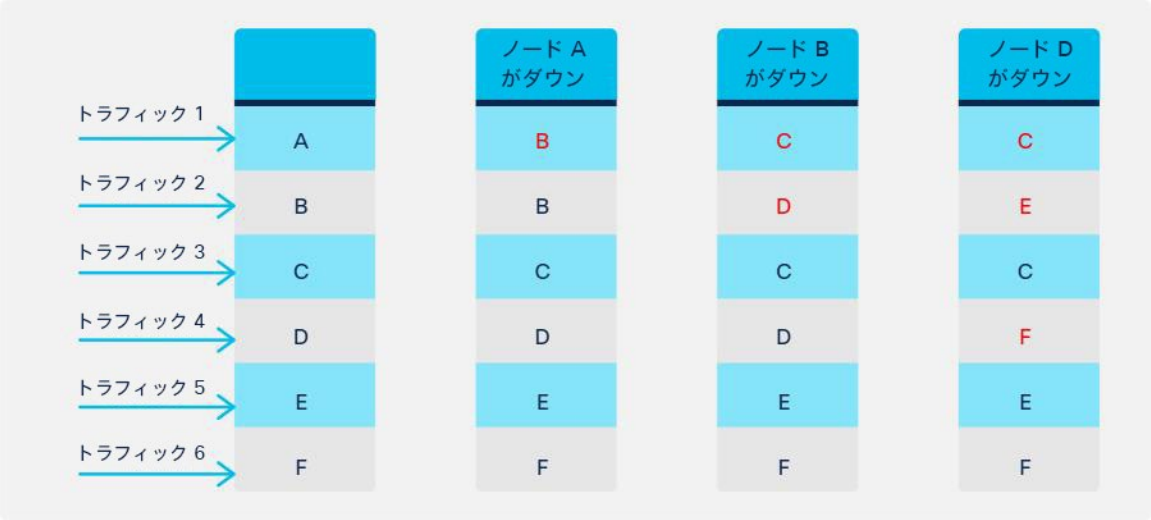


図 71.
複数の障害のシナリオ（ノード A がダウン、ノード B がダウン、ノード D がダウン）

ノード F がダウンし、その後ノード E がダウンし、その後ノード A がダウンした場合（図 72 を参照）、使用可能なノードを通過しているトラフィックが影響を受ける可能性があります。

図 72.
複数の障害のシナリオ（ノード F がダウン、ノード E がダウン、ノード A がダウン）

バックアップ PBR ポリシー（N+M 高可用性）

復元力のあるハッシュでは、障害が発生したノードを通過するすべてのトラフィックが使用可能なノードのいずれか 1 つにリダイレクトされるため、そのノードのキャパシティが問題になる可能性があります。すべての PBR ノードが使用可能な場合と比較して、そのノードのトラフィック量が 2 倍になる可能性があります。Cisco ACI リリース 4.2 以降では、バックアップ PBR ポリシーが導入されています。このポリシーでは、バックアップ PBR 接続先を設定できます。障害が発生したノードを通過していたトラフィックは、使用可能なプライマリ PBR ノードの 1 つを使用する代わりに、バックアップ PBR ノードにリダイレクトされます。他のトラフィックは引き続き同じ PBR ノードにリダイレクトされます（図 73 を参照）。これにより、キャパシティ超過の懸念を回避できます。

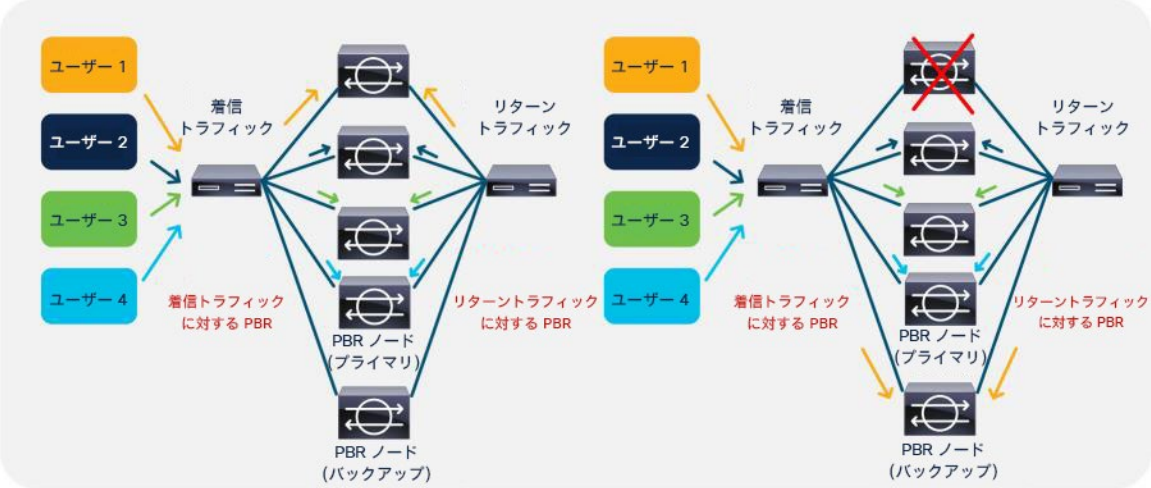


図 73.
PBR ノード障害時の動作（バックアップ PBR 接続先）

バックアップ PBR ポリシーに関する設計上の考慮事項は次のとおりです。

- 復元力のあるハッシュを有効化しておく必要があります。
- APIC リリース 4.2 より前のリリースでは、L1/L2 PBR ではなく L3 PBR を対象とするバックアップ PBR ポリシーのみがサポートされます。APIC リリース 4.2 の L1/L2 PBR の場合、1 つの PBR ポリシーに複数のアクティブな PBR 接続先を設定できないためです。APIC リリース 5.0 以降では、L1/L2 PBR でバックアップ PBR ポリシーがサポートされます。
- プライマリ PBR 接続先とそのバックアップ PBR 接続先は、同じ非表示サービス EPG に分類する必要があります。つまり、プライマリ PBR 接続先とバックアップ PBR 接続先の両方の具象インターフェイスが、同じクラスタインターフェイスに属している必要があります。さらに、そのプライマリ PBR 接続先とバックアップ PBR 接続先は、同じ L4-L7 デバイスの下に定義する必要があります。
- PBR 接続先は、PBR ポリシーでプライマリ PBR 接続先として使用するか、その PBR ポリシーのバックアップ PBR ポリシーでバックアップ PBR 接続先として使用することができますが、両方で使用することはできません。つまり、プライマリ PBR 接続先をバックアップ PBR ポリシーでバックアップ PBR 接続先として使用することはできません（プライマリ接続先とバックアップ接続先が同じブリッジドメインにある場合、プライマリ PBR 接続先を異なる PBR ポリシーでバックアップ PBR 接続先として使用できます）。
- 1 つのバックアップ PBR ポリシーは、1 つの PBR ポリシーでのみ使用できます。そうでない場合は、設定が拒否されます。複数の PBR ポリシーで同じバックアップ PBR 接続先を使用する場合は、同じバックアップ PBR 接続先と同じヘルスグループを使用して 2 つの異なるバックアップ PBR ポリシーを作成します（図 74）。

図 74.
複数の PBR ポリシーに同じバックアップ PBR 接続先を使用

- 1 つのバックアップ PBR ポリシーに複数のバックアップ PBR 接続先を設定できます。したがって、N+1 高可用性だけでなく、N+M 高可用性の設計が可能です。使用可能なバックアップ PBR 接続先が複数ある場合、デフォルトでは、使用可能なバックアップ PBR 接続先の 1 つが IP アドレスの順序（昇順）で選択されます（図 75）。すべてのバックアップ PBR 接続先が使用されている場合、トラフィックは、プライマリ IP アドレスの順序（昇順）で、使用可能なプライマリ PBR 接続先またはバックアップ PBR 接続先のいずれかにリダイレクトされます（図 76）。APIC リリース 4.2(5) および 5.0 以降では、IP アドレスベースのソートの代わりに、接続先名ベースのソートを使用できます。接続先名オプションの詳細については、「接続先名ベースのソート」セクションを参照してください。

図 75.
バックアップ PBR ノードが複数あるシナリオ

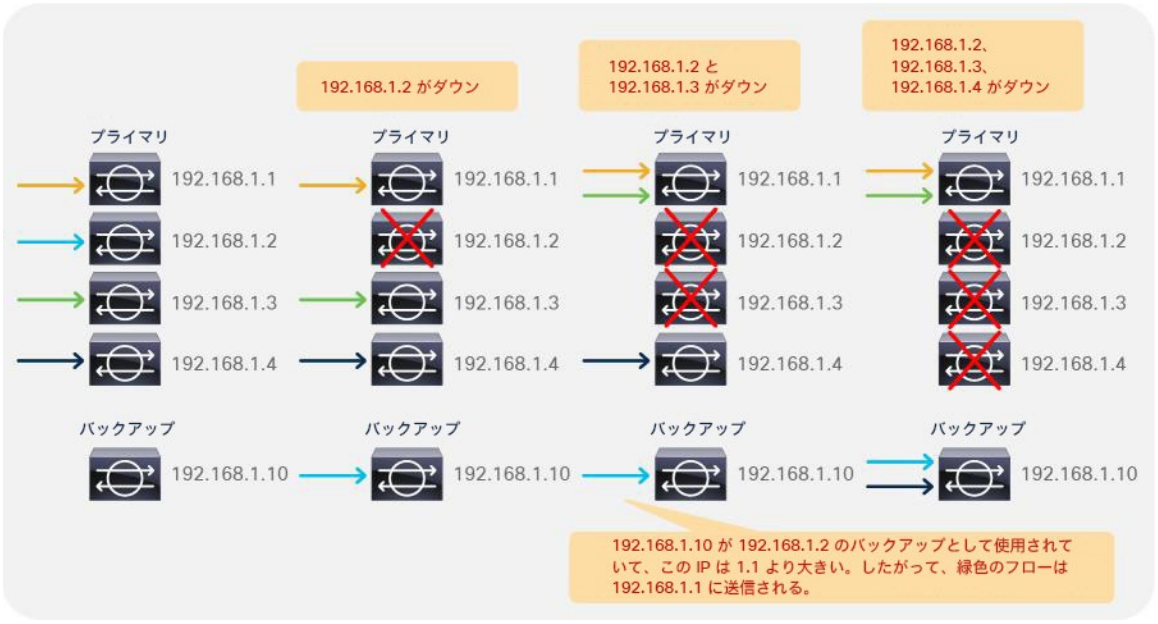


図 76.
障害ノードの数がバックアップ PBR ノードの数よりも多い複数障害のシナリオ

- バックアップ PBR 接続先がある場合、しきい値は、使用中のプライマリ PBR 接続先とバックアップ PBR 接続先の合計数を設定されているプライマリ PBR 接続先の数で割った値に基づいて計算されます（図 77）。

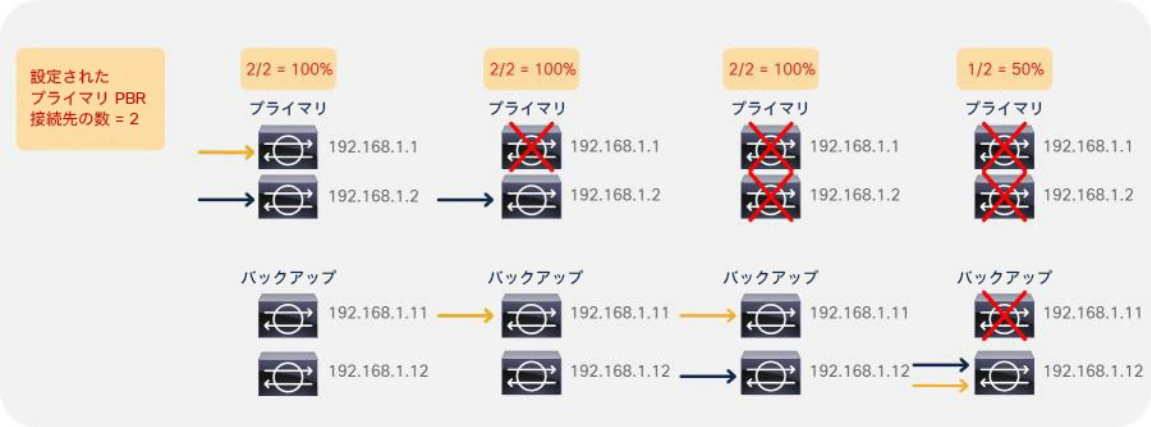
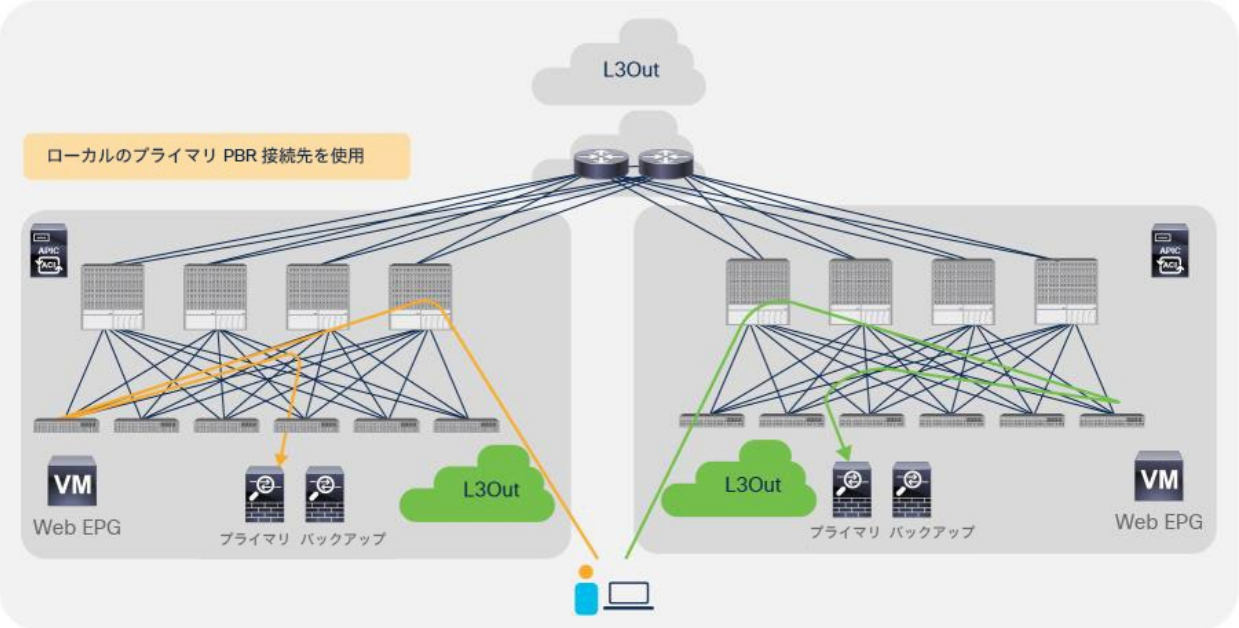
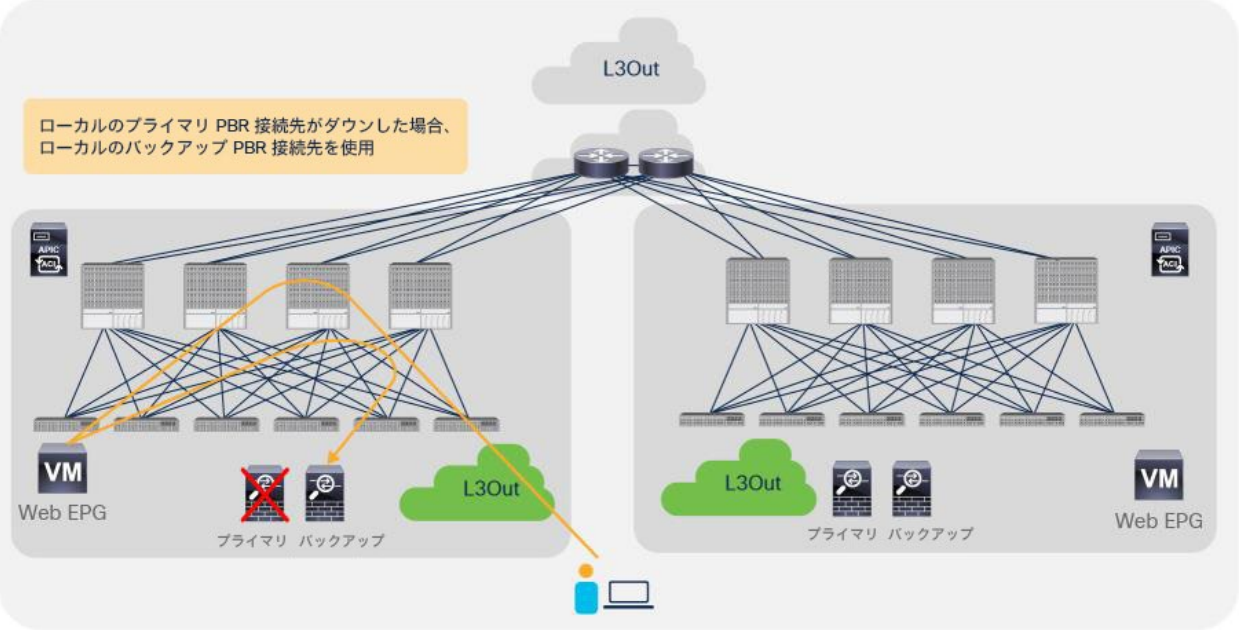
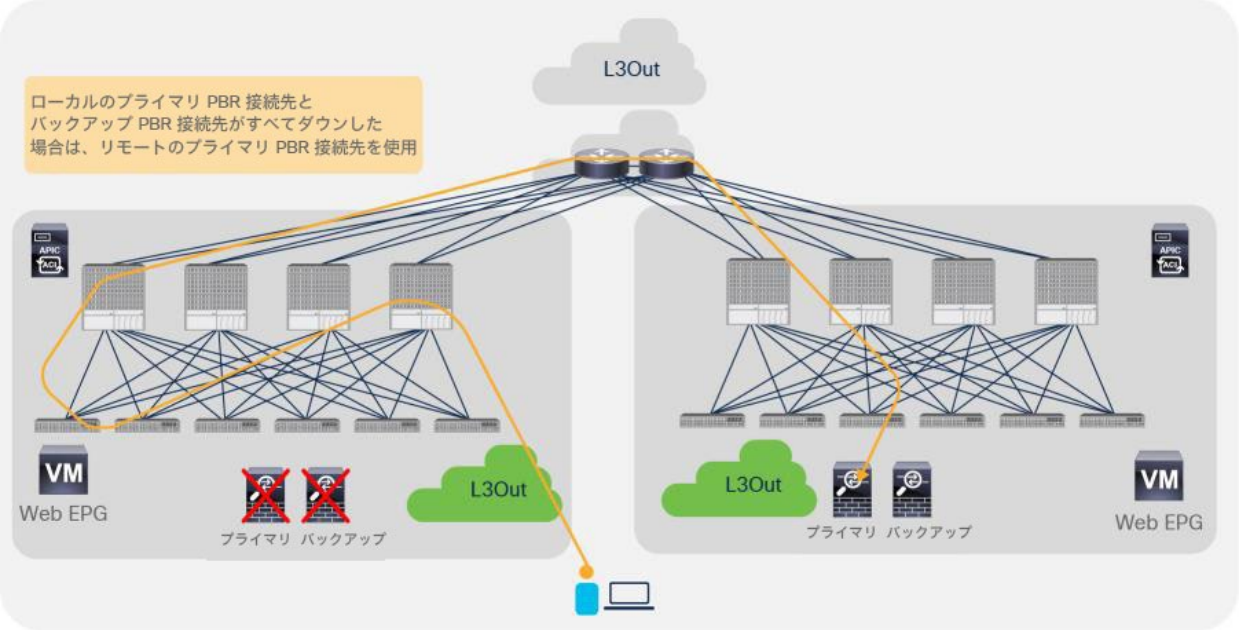


図 77.
しきい値の計算例

- マルチポッドでバックアップ PBR ポリシーがサポートされます。ロケーション認識型 PBR では、ローカルのプライマリ PBR 接続先がダウンすると、ローカルのバックアップ PBR 接続先が使用されます。ローカルのプライマリ PBR 接続先とバックアップ PBR 接続先がすべてダウンした場合は、リモートのプライマリ PBR 接続先が使用されます。リモートのプライマリ PBR 接続先もダウンした場合は、リモートのバックアップ PBR 接続先が使用されます（図 78）。
- バックアップ PBR ポリシーはサイトローカルの設定であるため、サイト内で使用する必要があります。プライマリ PBR 接続先またはバックアップ PBR 接続先を異なるサイトで使用することはできません。







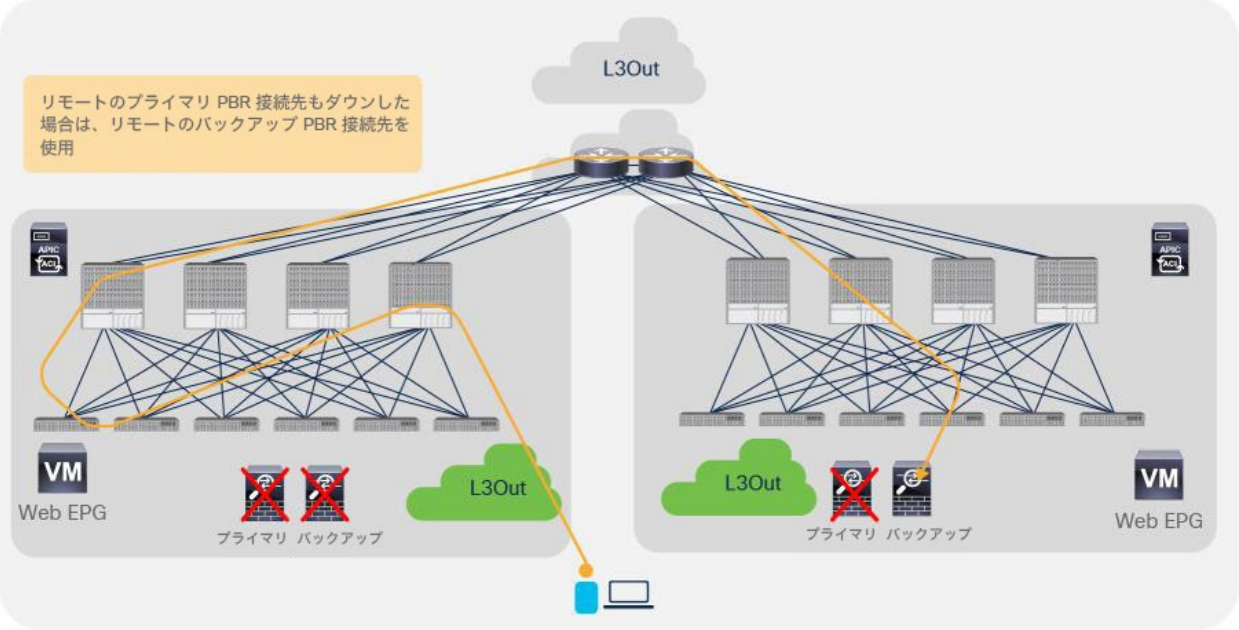
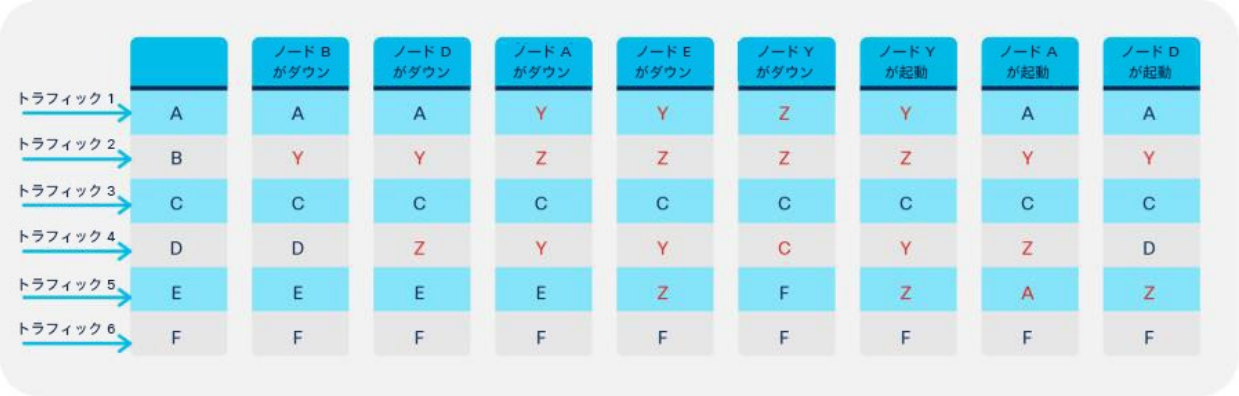


図 78.
マルチポッドにおけるバックアップ PBR ポリシーの例

注： バックアップ PBR ポリシーを使用していない図 64 と図 65 の例と同様、複数の障害が発生している場合、状況によっては、使用可能なノードを通過するトラフィックが再ハッシュされている可能性があります。図 79 に、ノード A ~ F がプライマリで、ノード Y ~ Z がバックアップである場合の例を示します。



		ノード B がダウン	ノード D がダウン	ノード A がダウン	ノード E がダウン	ノード Y がダウン	ノード Y が起動	ノード A が起動	ノード D が起動
トラフィック 1	A	A	A	Y	Y	Z	Y	A	A
トラフィック 2	B	Y	Y	Z	Z	Z	Z	Y	Y
トラフィック 3	C	C	C	C	C	C	C	C	C
トラフィック 4	D	D	Z	Y	Y	C	Y	Z	D
トラフィック 5	E	E	E	E	Z	F	Z	A	Z
トラフィック 6	F	F	F	F	F	F	F	F	F

図 79.
複数障害のシナリオの例

Cisco ACI マルチポッド設計におけるロケーションベースの PBR

Cisco ACI リリース 2.0 以降では、Cisco ACI が提供する Cisco ACI マルチポッドと呼ばれるソリューションが利用できます。これにより、異なる Cisco ACI リーフ/スパインファブリックを同じ APIC クラスタの管理下で相互接続できます。Cisco ACI ファブリックは、物理的に同じ場所に配置されている場合も地理的に分散している場合もあります。この設計により、これらを相互接続する運用上シンプルな方法が提供されます。

このセクションでは、Cisco ACI マルチポッド設計の PBR 展開オプションを中心に説明します。ただし、L4-L7 ネットワークサービスを Cisco ACI マルチポッドファブリックに統合するための展開モデルにはいくつかの選択肢があります。Cisco ACI マルチポッドファブリックの詳細については、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-c11-737855.html?cachemode=refresh

前のセクションで説明したように、PBR によるリダイレクトはハッシュに基づいています。位置認識機能は使用しません。たとえば、送信元エンドポイント、接続先エンドポイント、使用可能な PBR ノードが同じポッドにあっても、別のポッドにある使用可能な PBR ノードにトラフィックがリダイレクトされることがあります。この場合、トラフィックは別のポッドに送信されてから戻ってくるため、遅延が増加し、ポッド間のネットワークリソースが消費されます。

図 80 に、エンドポイントと PBR ノードが異なるポッドにある例を示します。接続先はポッド 2 の 192.168.1.202 です。外部ネットワークからのトラフィックはポッド 1 のボーダーリーフノードで受信され、スパインを介して接続先エンドポイントがある接続先リーフに送信されます。その後、PBR ポリシーが接続先リーフで適用され、ハッシュに基づいてポッド 1 の PBR ノードが選択されます。トラフィックがポッド 2 の接続先エンドポイントに到達するには、最終的にポッド 1 の PBR ノードから戻ってくる必要があります。最終的に、この入力フローの場合、IPN をまたいでトラフィックが 3 回ヘアピンする必要があります。

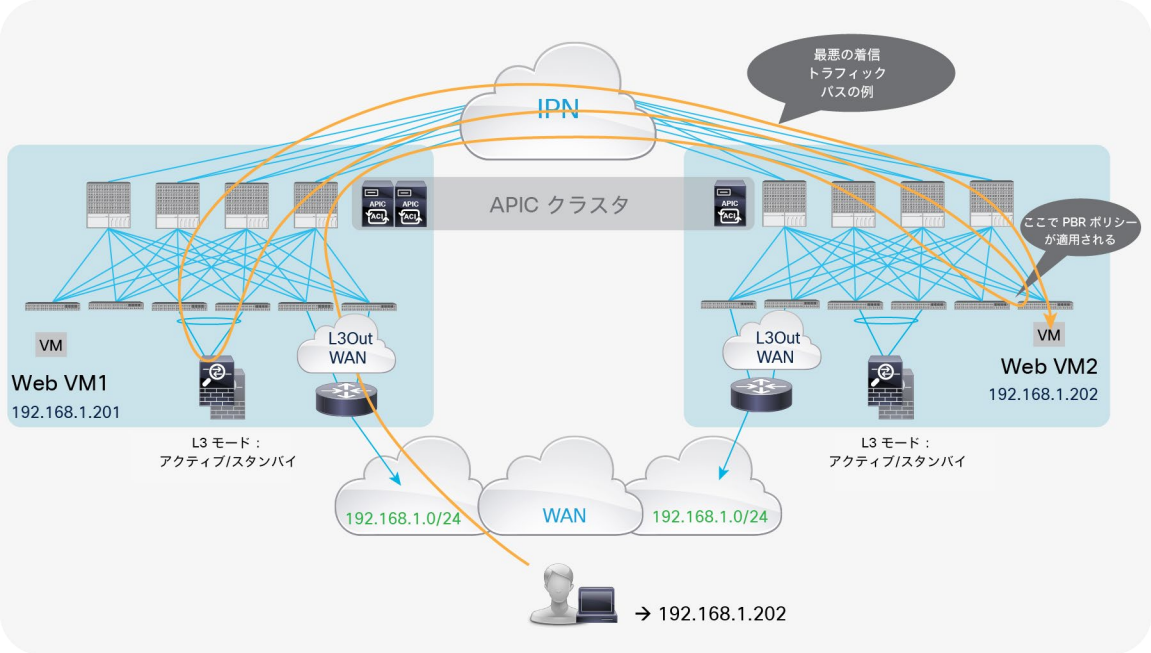


図 80.
最悪のトラフィックパスの例

前の図に示した最適ではないトラフィックの動作は、Cisco ACI ボーダーリーフノードからのホストルートアドバタイズ（Cisco ACI リリース 4.0 以降で利用可能）と「ロケーションベースの PBR」と呼ばれる機能（Cisco ACI リリース 3.1 以降で利用可能）を組み合わせることで回避できます。ロケーションベースの PBR では、エンドポイントが配置されている接続先リーフノードがローカルのサービスノードを優先的に選択するため、トラフィックのポッドをまたぐヘアピン動作を回避できます。ロケーションベースの PBR には、Cisco Nexus 9300-EX および -FX プラットフォーム リーフ スイッチ以降が必要です。

図 81 に、接続先がポッド 1 の 192.168.1.201 である例を示します。ACI ボーダーリーフノードが提供するホストルートアドバタイズ機能により、外部クライアントから発信されたトラフィックは、選択的にポッド 1 に誘導され、エンドポイント 192.168.1.201 が配置されている接続先リーフノードに到達できます。次に、ポッド 1 の接続先リーフノードがローカルの PBR ノードを選択し、その PBR ノードがトラフィックを接続先に送り返します。ポッド 2 のエンドポイント 192.168.1.202 を接続先とするトラフィックでも同様の動作が行われます。

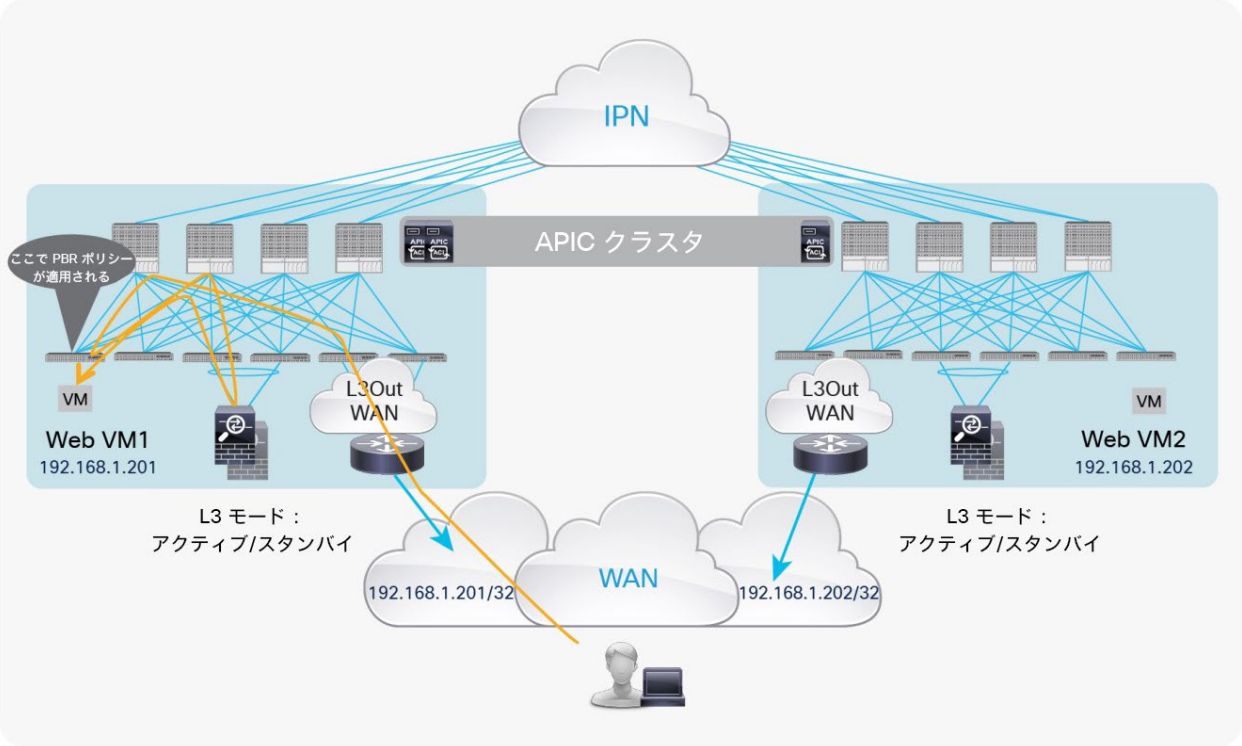


図 81.
ホストルートアドバタイズを伴うロケーションベースの PBR（インバウンド）

リターントラフィックの場合、接続先リーフノードが PBR ポリシーを適用し、同じローカルの PBR ノードを選択します。その後、トラフィックはローカルのボーダーリーフノードで定義された L3Out 接続を介して外部ネットワークドメインに戻ります。これは Cisco ACI マルチポッドのデフォルト動作です（図 82）。

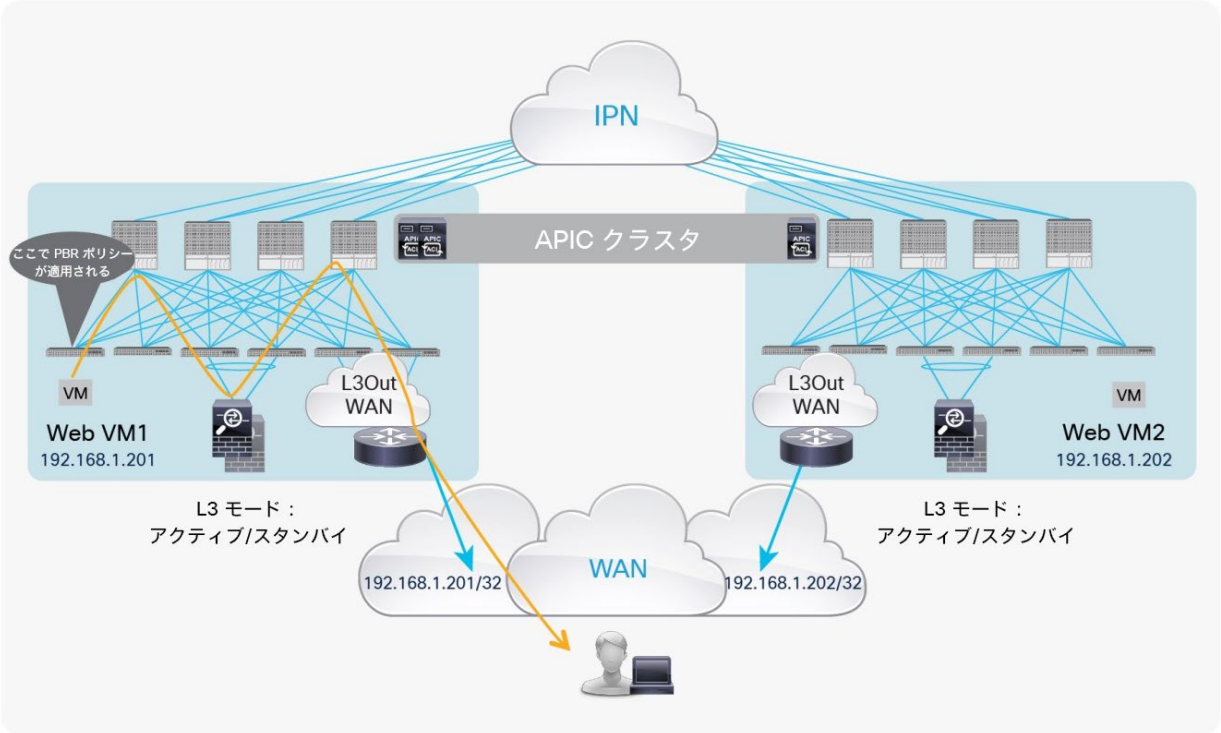


図 82.
ホストルートアドバタイズを伴うロケーションベースの PBR（アウトバウンド）

ポッド 1 の Cisco ACI リーフノードがローカルのサービスノードの障害を検出すると、ハッシュ機能がリモートポッドにあるサービスノードの選択を開始します。このプロセスの結果、トラフィックの IPN をまたぐヘアピン動作が発生しますが、トラフィックがブラックホールに入るのを回避できます。

注： ポッドにまたがって展開された独立したファイアウォールペア間では接続状態が同期されないため、ポッド 1 の障害が発生したファイアウォールを通過していた長期のトラフィックフローは、リモートポッドのファイアウォールを介して再確立する必要があります。

PBR ノード、コンシューマー EPG、プロバイダー EPG を同じサブネットに配置する設計

APIC リリース 3.1 より前のリリースでは、PBR ノードブリッジドメインは、コンシューマーのブリッジドメインおよびプロバイダーのブリッジドメインと異なっている必要があります。そのため、PBR ノードには別のブリッジドメインとサブネット範囲が必要です。APIC リリース 3.1 以降では、この要件は必須ではありません。PBR ブリッジドメインは、コンシューマーのブリッジドメインまたはプロバイダーのブリッジドメインと同じにすることができます（図 83）。この機能には、Cisco Nexus 9300-EX および -FX プラットフォーム リーフ スイッチ以降が必要です。

注： APIC リリース 3.1 では、PBR ノードのブリッジドメイン設定でデータプレーン学習を無効化する必要はありません。サービスグラフが展開されると、PBR ノード EPG のデータプレーン学習が自動的に無効化されます。

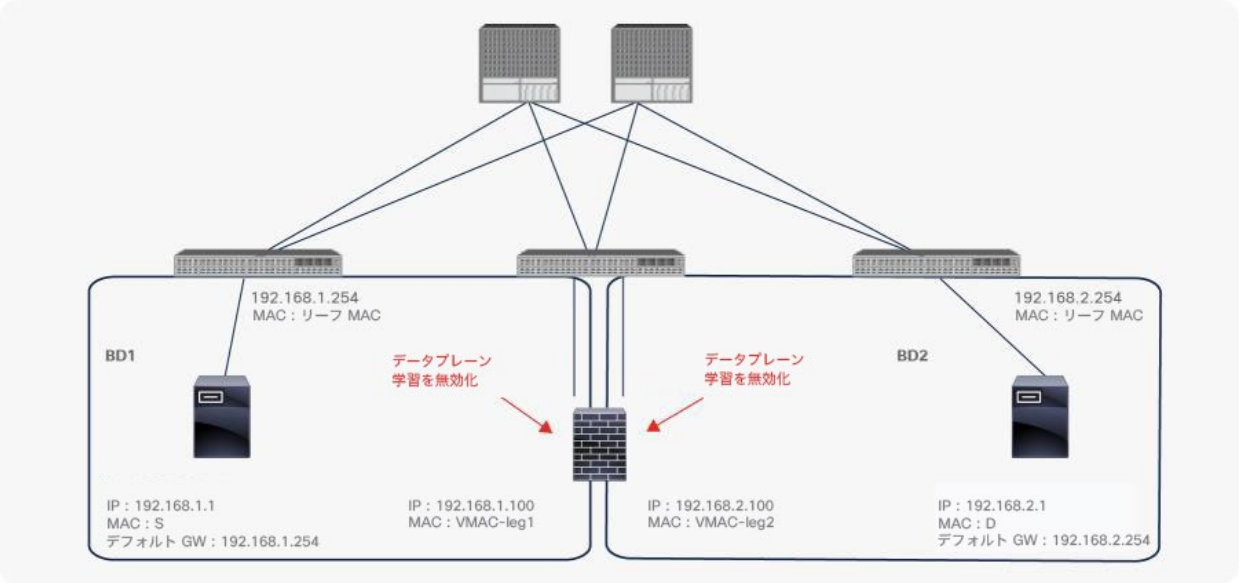


図 83.
コンシューマーのブリッジドメインとプロバイダーのブリッジドメインにある PBR ノード

「送信元 MAC ベースの転送」が設定された L4-L7 デバイスに対応した送信元 MAC の書き換え

APIC リリース 5.0 より前のバージョンでは、トラフィックが PBR ノードに送信されるように ACI PBR が接続先 MAC を書き換えますが、送信元 MAC は変更しません。そのため、PBR ノードは、ACI ファブリックが所有するサービス BD の MAC ではなく送信元エンドポイントの送信元 MAC アドレスを持つトラフィックを受信します。PBR ノードが IP ベースの転送ではなく「送信元 MAC ベースの転送」を使用している場合、問題が発生する可能性があります。

APIC リリース 5.0 以降では、「送信元 MAC の書き換え」オプションが導入され、送信 MAC を書き換えることが可能です。デフォルトでは、「送信元 MAC の書き換え」は無効化されています。この機能には、Cisco Nexus 9300-EX および -FX プラットフォーム リーフ スイッチ以降が必要です。

注： サービスノードのベンダーによって、「送信元 MAC ベースの転送」を意味する用語が異なる場合があります。たとえば、F5 BIG-IP では「Auto Last Hop」、Citrix NetScaler では「MAC ベース転送（MBF）」です。

図 84 および図 85 に、「送信元 MAC の書き換え」オプションを使用した場合のトラフィック転送のパケットウォークを示します。図 84 に、コンシューマーからプロバイダーエンドポイントへの着信トラフィックを示します。コンシューマーである Web からプロバイダーであるアプリケーションへのトラフィックがリーフによってリダイレクトされると、接続先 MAC が PBR 接続先 MAC に、送信元 MAC がサービス BD の MAC（00:22:bd:f8:19:ff）に書き換えられ、トラフィックは PBR ノードに到達します。送信元 MAC ベースの転送が PBR ノードで有効化されている場合、PBR ノードはフローを記憶し、リターントラフィックの接続先 MAC として送信元 MAC（00:22:bd:f8:19:ff）を使用します。その後、トラフィックは接続先であるアプリケーション エンドポイントに到着します。

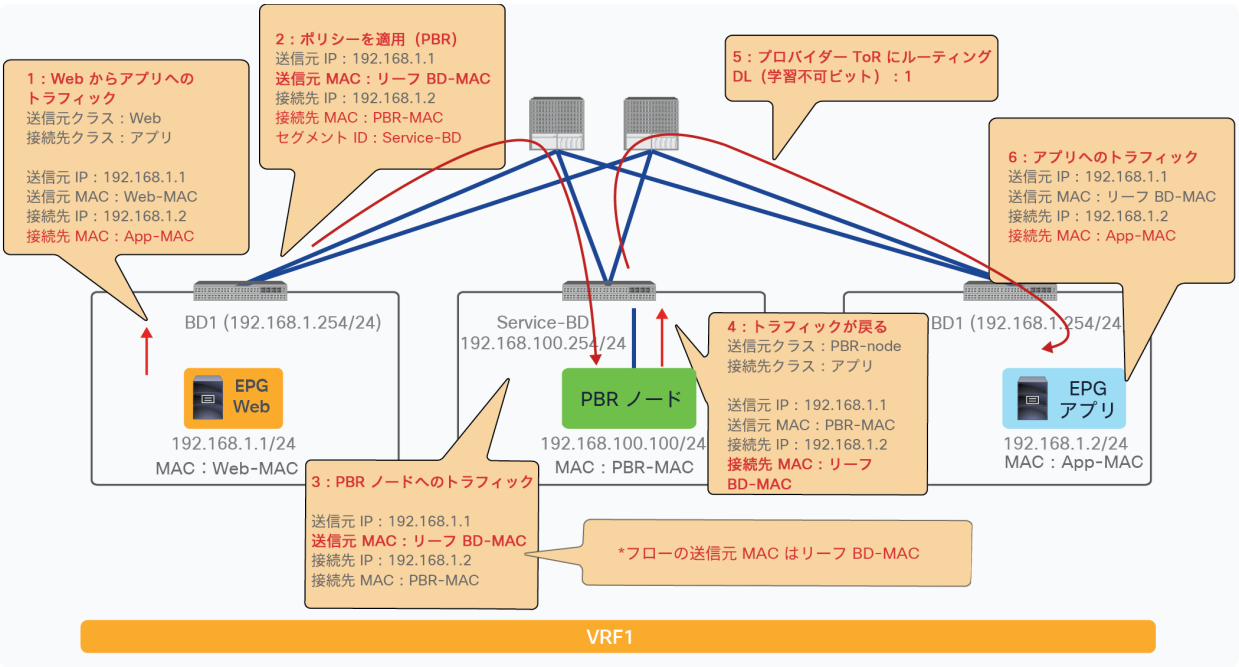


図 84.
送信元 MAC が書き換えられるパケットウォーク（コンシューマーからプロバイダーへの着信トラフィック）

図 85 に、プロバイダーからコンシューマーエンドポイントへのリターントラフィックを示します。プロバイダーとしてのアプリケーションからコンシューマーとしての Web へのトラフィックがリーフによってリダイレクトされると、接続先 MAC が PBR 接続先 MAC に書き換えられ、そのトラフィックが PBR ノードに到達します。PBR ノードが送信元 MAC ベースの転送を使用する場合、サービス BD MAC（00:22:bd:f8:19:ff）が接続先 MAC として使用されます。したがって、トラフィックは、サービスリーフを介して接続先である Web エンドポイントに到達できます。着信トラフィックフローで送信元 MAC が書き換えられていない場合、PBR ノードは Web-MAC を接続先 MAC として使用します。Web-MAC がサービス BD にないため、サービスリーフはトラフィックをドロップします。

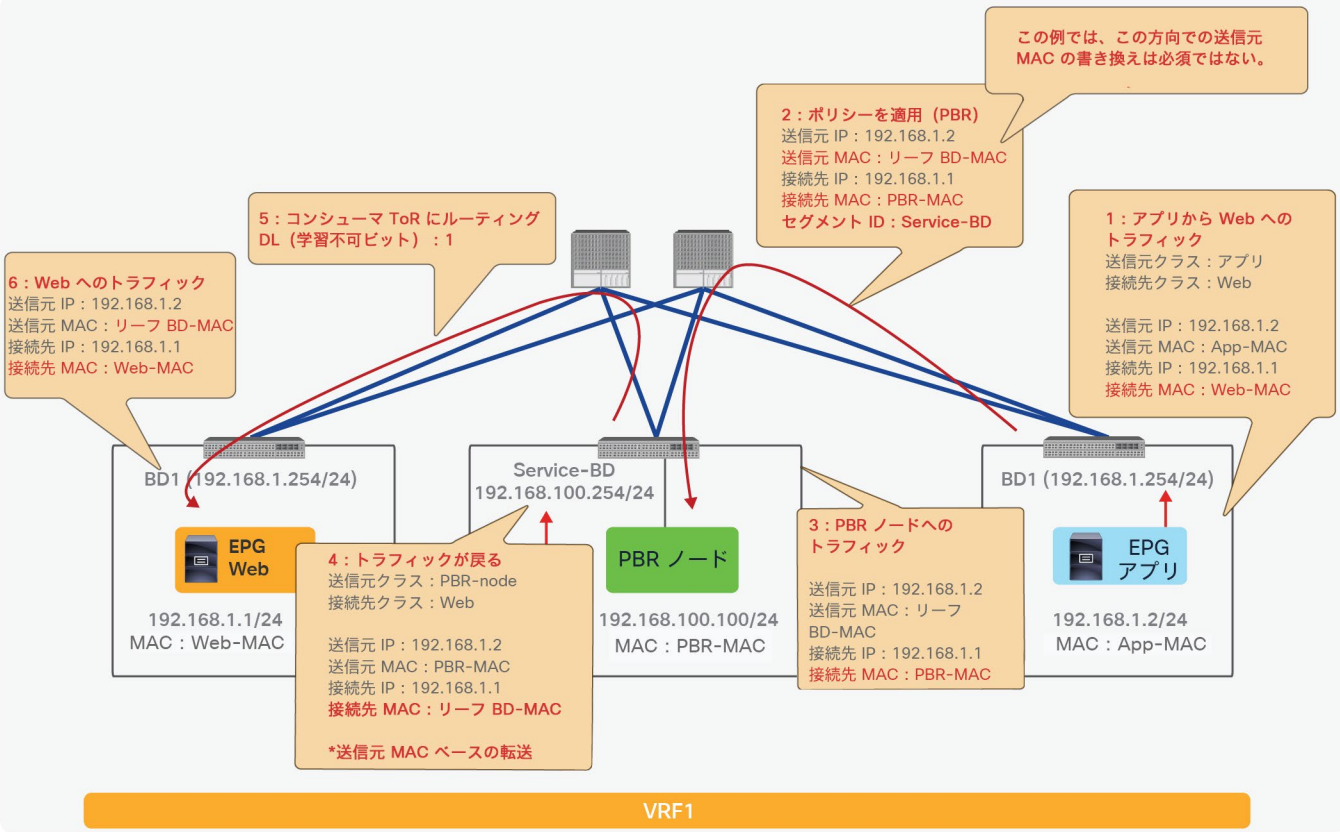
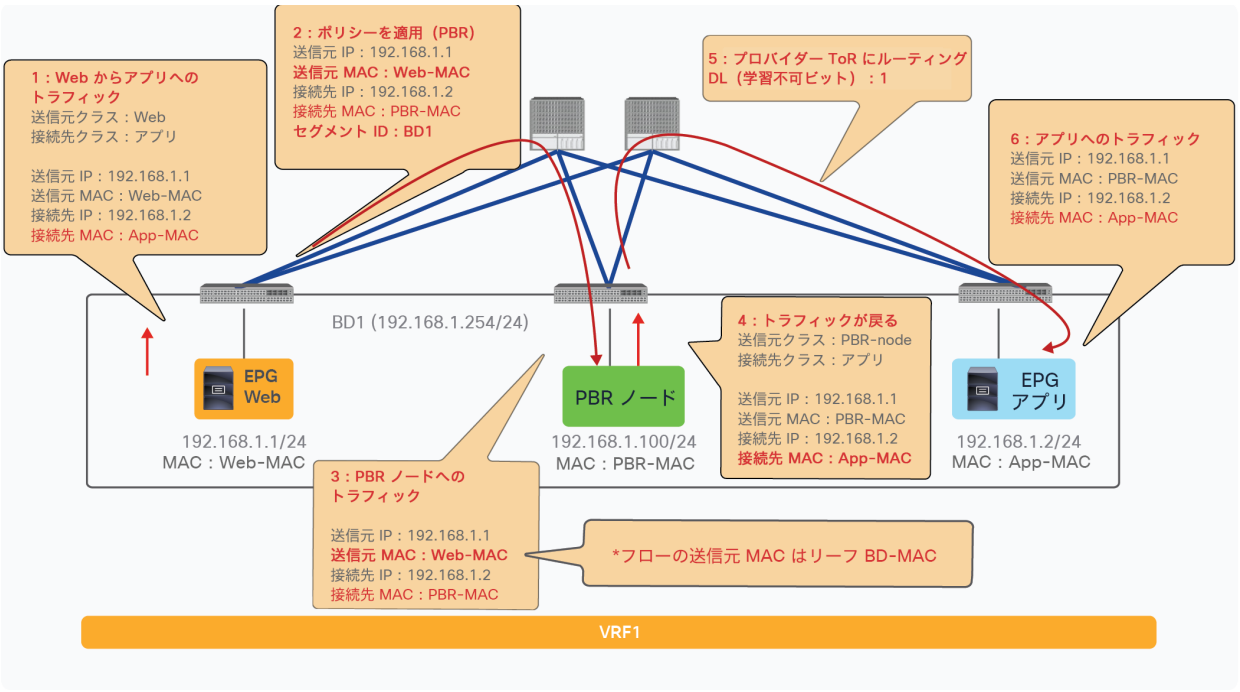


図 85.
送信元 MAC が書き換えられるパケットウォーク（プロバイダーからコンシューマーへのリターントラフィック）

注： このトラフィックフローの例では、トラフィックが常にコンシューマーからプロバイダーに向かって開始される場合、プロバイダーからコンシューマーへの方向で送信元 MAC の書き換えは必須ではありません。

展開された L4-L7 デバイス（PBR ノード）のインターフェイスが、接続先と同じブリッジドメインサブネットにある場合：

- L4-L7 デバイスは接続先と同じサブネットにあるため、PBR ノードから接続先に戻るトラフィックのルーティングは必要ありません。
- 接続先 MAC が正しく、ブリッジドメイン内で到達可能であるため、「送信元 MAC の書き換え」機能も必要ありません（「送信元 MAC ベースの転送」が PBR ノードで有効になっている場合でも）。図 86 に例を示します。



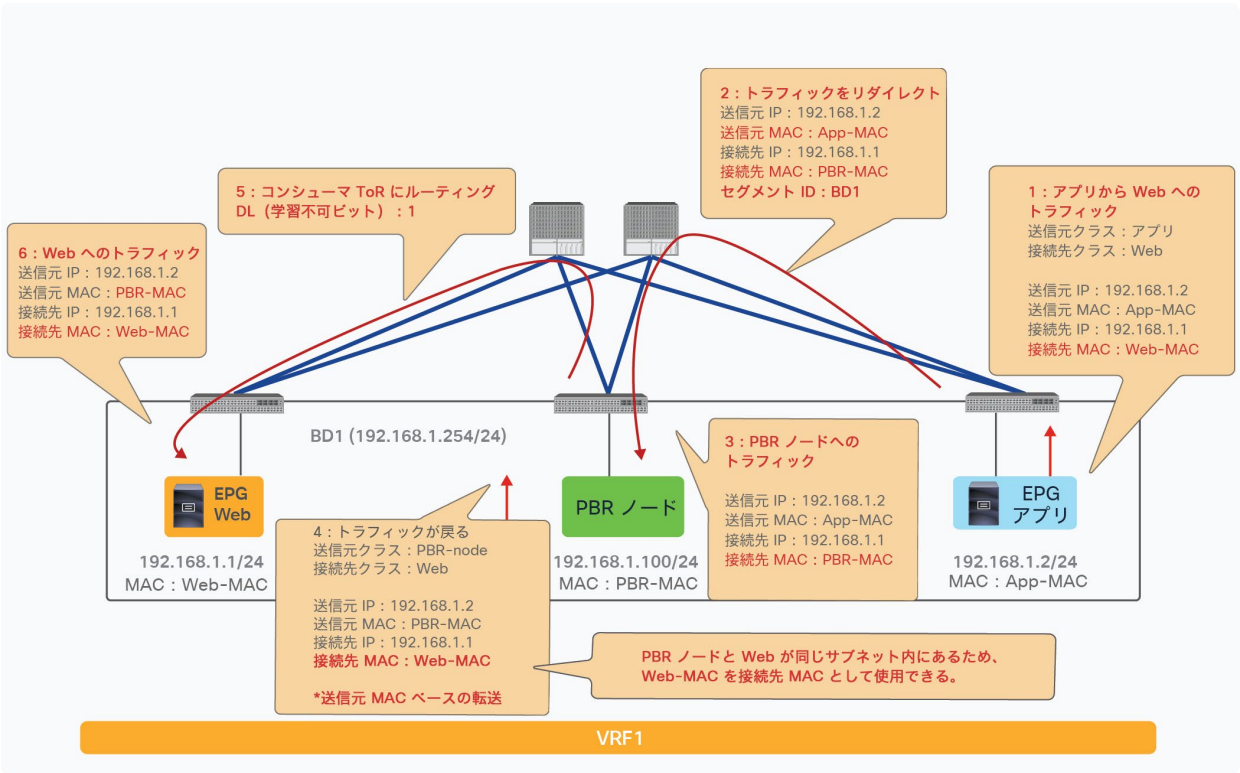


図 86.
接続先と PBR ノードが同じサブネットにある場合、送信元 MAC の書き換えは不要

接続先名ベースのソート

APIC リリース 4.2(5) または 5.0 より前のバージョンでは、対称 PBR は IP ベースのソートを使用します。PBR 接続先が複数ある場合は、ランダムな順序ではなく IP アドレスと同じ順序で設定する必要があります。PBR ノードに 2 つのインターフェイスがあり、一方の IP アドレスが接続先グループ内で最小の場合、もう一方のインターフェイスの IP アドレスはもう一方の PBR ポリシーで最小にする必要があります。これは、着信トラフィックとリターントラフィックが同じデバイスに送信されるようにするためです。着信トラフィックとリターントラフィックの両方でトラフィックの対称性を維持するために、たとえば、図 87 の 10.1.1.1 のデバイスは 10.1.2.1 を使用し、10.1.1.2 のデバイスは 10.1.2.2 を使用するように設定する必要があります。

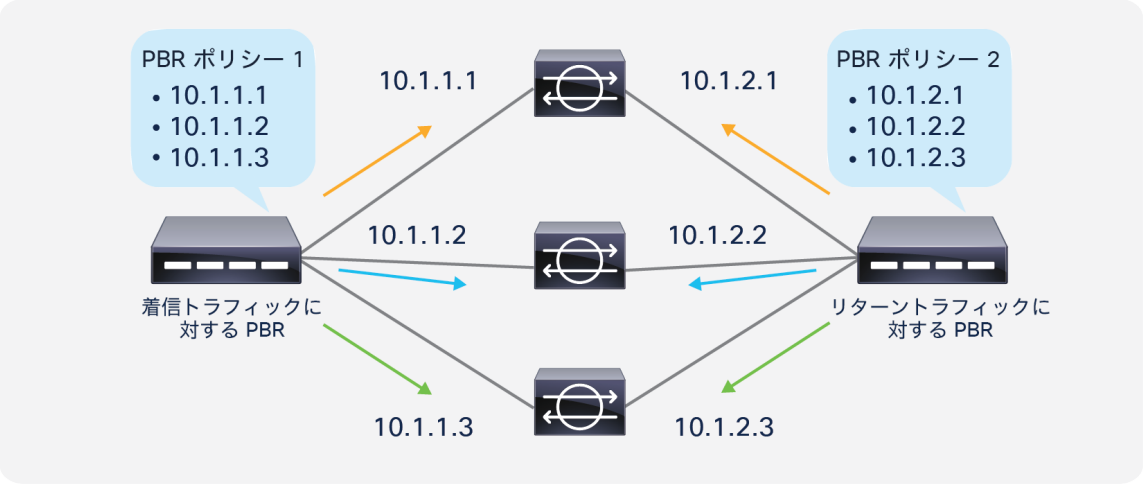


図 87.
対称 PBR における IP ベースのソート（デフォルトの動作）

APIC リリース 4.2(5) および 5.0 以降では、PBR 接続先の IP アドレスの順序が正しくない場合に、接続先名ベースのソートを使用できます。たとえば、図 88 の 10.1.1.1 のデバイスは、もう一方の側で最小 IP ではない 10.1.2.3 を使用しているため、接続先名ベースのソートが必要です。接続先名ベースのソートを使用する場合は、トラフィックの対称性を維持するために、それに応じた接続先名を設定する必要があります。着信トラフィックとリターントラフィックの PBR ポリシーに設定される各 PBR 接続先名は完全に同じである必要はありませんが、トラフィックの対称性を維持するために名前ベースの順序が同じであることが必要です。

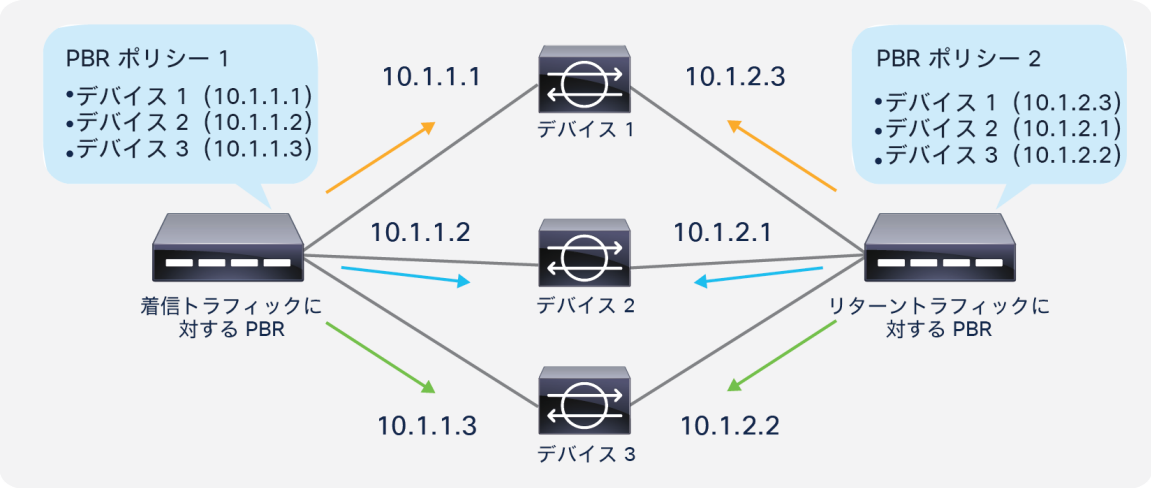


図 88.
対称 PBR における接続先名ベースのソート

APIC リリース 5.0 以降では、L1/L2 対称 PBR がサポートされます。L1/L2 対称 PBR の場合は、常に接続先名ベースのソートになります。

PBR 接続先ごとの重み

APIC リリース 6.0 より前のリリースでは、PBR 接続先ごとの重みを指定するオプションはありません。したがって、同じ PBR ポリシーに設定された PBR 接続先（サービスデバイス）は、トラフィックを処理するキャパシティが同じかほぼ同じであることが前提となっています。

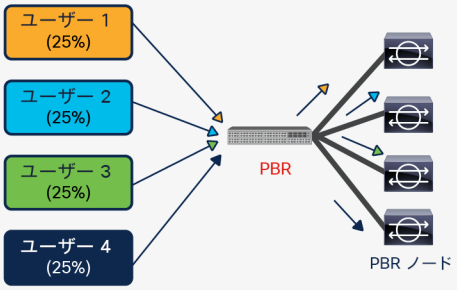
APIC リリース 6.0 以降では、PBR 接続先ごとに重みを設定できます。異なるキャパシティのサービスデバイスが PBR ポリシーに混在している状況にも対応できます。

デフォルトでは、すべての PBR 接続先の重みが 1 に設定されます。設定可能な重みの範囲は 1 ~ 10 です。PBR ポリシーごとの重みの合計数は、PBR 接続先が BD にある場合は最大 128、PBR 接続先が L3Out にある場合は 64 です。これは、プライマリ PBR 接続先とバックアップ PBR 接続先の重みの合計数です。

すべての PBR 接続先でデフォルトの重み（= 1）を使用

接続先	IP	重み（オプション）	%
接続先 1	10.1.1.1	未設定（1）	25%
接続先 2	10.1.1.2	未設定（1）	25%
接続先 3	10.1.1.3	未設定（1）	25%
接続先 4	10.1.1.4	未設定（1）	25%

バケット合計：4



重みを設定

接続先	IP	重み（オプション）	%
接続先 1	10.1.1.1	4	40%
接続先 2	10.1.1.2	3	30%
接続先 3	10.1.1.3	2	20%
接続先 4	10.1.1.4	1	10%

バケット合計：10（1+2+3+4）

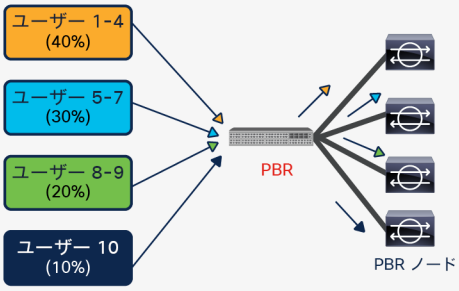


図 89.
PBR 接続先ごとの重み

トラフィックの対称性を維持するために、コンシューマーからプロバイダーへの トラフィックに対する PBR ポリシーとプロバイダーからコンシューマーへのトラフィックに対する PBR ポリシーで同じ重みを使用する必要があります。以下の図に例を示します。

接続先	IP	重み（オプション）
接続先 1	10.1.1.1	4
接続先 2	10.1.1.2	3
接続先 3	10.1.1.3	2
接続先 4	10.1.1.4	1

コンシューマーからプロバイダーへのトラフィックに適用される PBR ポリシー 1

接続先	IP	重み（オプション）
接続先 1	10.1.2.1	4
接続先 2	10.1.2.2	3
接続先 3	10.1.2.3	2
接続先 4	10.1.2.4	1

プロバイダーからコンシューマーへのトラフィックに適用される PBR ポリシー 2

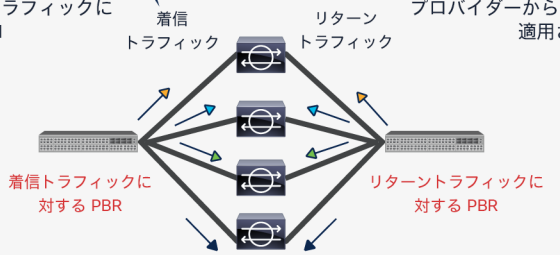
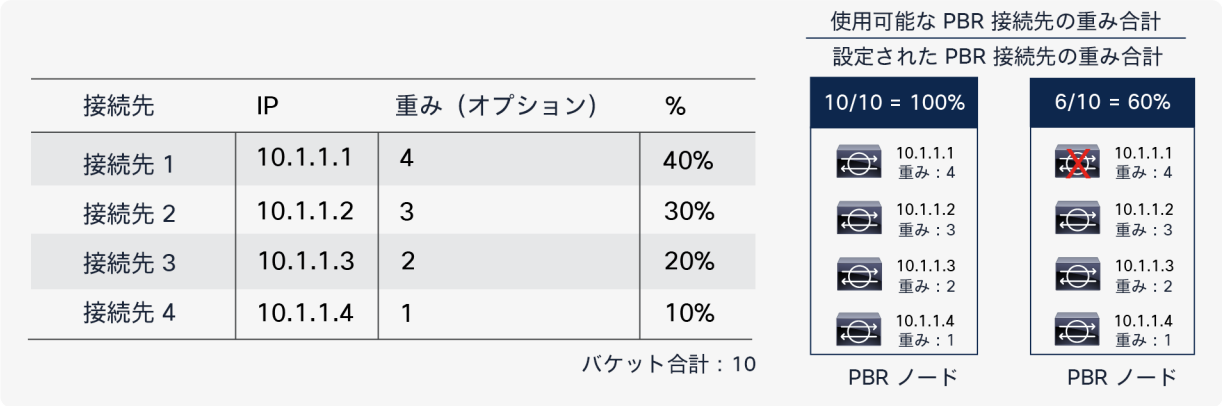


図 90.
重みオプションに関する考慮事項：同じ重みを使用

しきい値は、使用可能な PBR 接続先の重みの合計値と設定された PBR 接続先の重みの合計値に基づいて計算されます。以下の図に例を示します。この例では、設定された PBR 接続先の重みの合計値は 10 です。10.1.1.1 がダウンしている場合、使用可能な PBR 接続先の重みの合計値は 6 です。したがって、しきい値は 60% です。



接続先	IP	重み（オプション）	%
接続先 1	10.1.1.1	4	40%
接続先 2	10.1.1.2	3	30%
接続先 3	10.1.1.3	2	20%
接続先 4	10.1.1.4	1	10%

バケット合計：10

図 91.
重みオプションに関する考慮事項：しきい値

設定

ここでは、Cisco PBR の設定について説明します。基本設定に続いて、ワンアームモード、VRF 間、対称 PBR の各設定の例と、いくつかのオプション設定を示します。

基本設定

このセクションでは、図 92 を例として用いて、PBR を使用する非管理モードサービスグラフの基本的な設定手順について説明します。Cisco ACI の基本設定は、このドキュメントの範囲外です（たとえば、ファブリック検出、インターフェイスポリシー、物理ドメインおよび仮想ドメイン、VRF、EPG、コントラクトの設定については説明しません）。

注： このドキュメントでは、いくつかの APIC リリースを使用して GUI の操作手順を示します。どのリリースを使用するかは機能が導入されたときのリリースに依存します。そのため、このドキュメントに示された GUI の操作手順が APIC の実際の GUI と多少異なる場合があります。たとえば APIC リリース 3.1 以降では、表 18 に示すように、[プロトコルポリシー（Protocol Policies）] と [L4 -L7サービス（L4-L7 Services）] が異なる場所に配置されています。

表 18. GUI での設定場所

Cisco APIC リリース 3.1 より前	Cisco APIC リリース 3.1 以降
[テナント（Tenant）] > [ネットワーク（Networking）] > [プロトコルポリシー（Protocol Policies）]	[テナント（Tenant）] > [ポリシー（Policies）] > [プロトコル（Protocol）]
[テナント（Tenant）] > [L4-L7サービス（L4-L7 Service）]	[テナント（Tenant）] > [サービス（Services）] > [L4-L7]

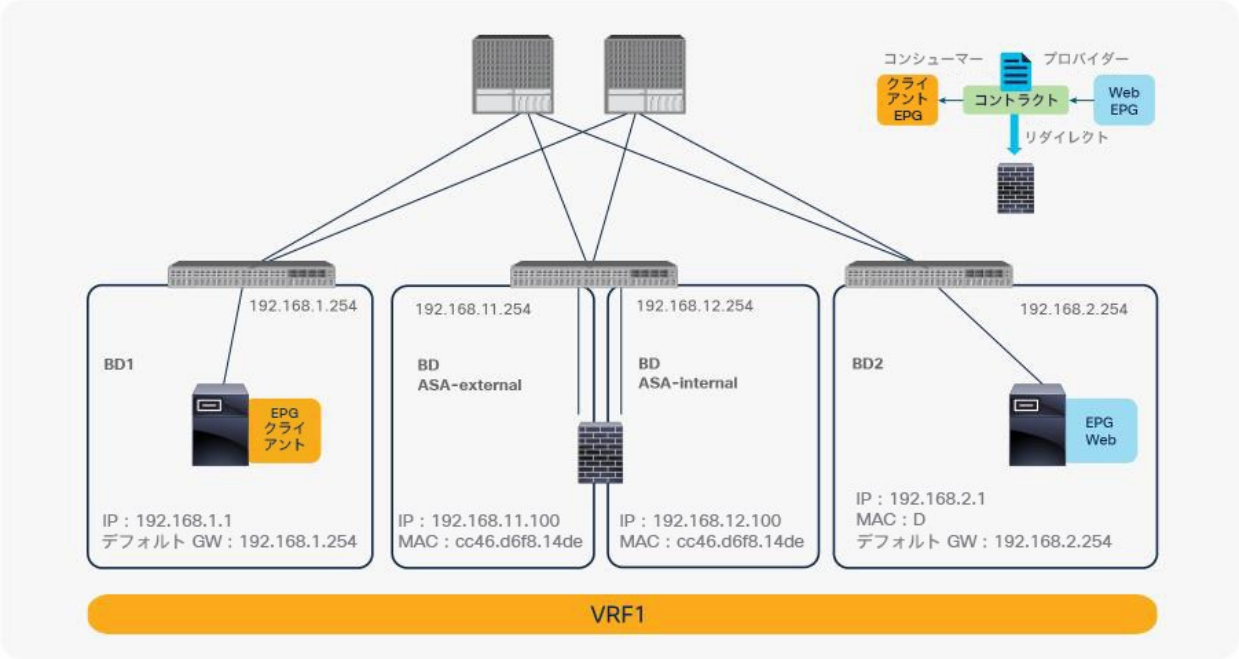


図 92.
1 ノード PBR の設計例（ツーアームモード）

PBR ノードブリッジドメインの作成

PBR ノードのブリッジドメインを作成します。APIC リリース 3.1 より前のバージョンの APIC または第 1 世代の Cisco Nexus 9300 プラットフォームスイッチを使用している場合は、PBR ノードブリッジドメインのエンドポイント データプレーン学習を無効化する必要があります。APIC リリース 5.0(1) 以降、このオプションは、ブリッジドメインの [ポリシー（Policy）] タブにある [詳細/トラブルシューティング（Advanced/Troubleshooting）] タブに移動しています。図 93 の例では、ASA-ext ブリッジドメインと ASA-int ブリッジドメインで [エンドポイントデータプレーン学習（Endpoint Dataplane Learning）] が無効化されています。

場所は、[テナント（Tenant）] > [ネットワーク（Networking）] > [ブリッジドメイン（Bridge Domains）] です。

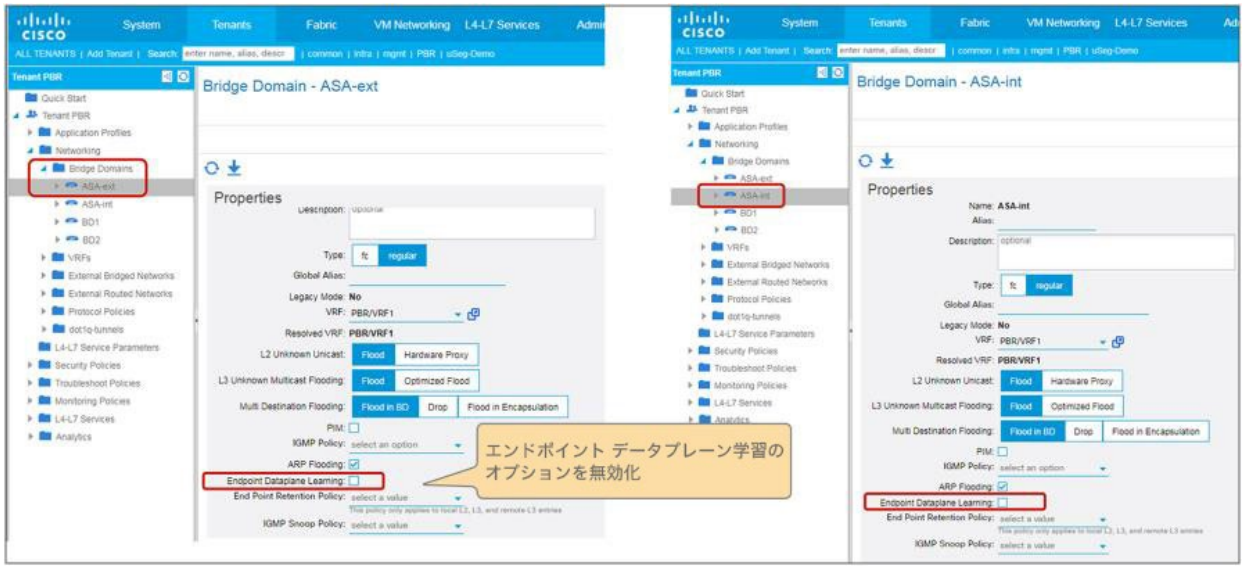


図 93.
PBR ブリッジドメインのデータプレーン IP 学習を無効化

PBR ポリシーの作成

PBR ポリシーを作成します。PBR ノードの IP アドレスと MAC アドレスを設定する必要があります。この例では、192.168.11.100 と MAC アドレス CC:46:D6:F8:14:DE を外部側に使用し、192.168.12.100 と MAC アドレス CC:46:D6:F8:14:DE を内部側に使用しています（図 94）。

場所は、[テナント（Tenant）] > [ポリシー（Policies）] > [プロトコル（Protocol）] > [L4-L7ポリシーベースリダイレクト（L4-L7 Policy Based Redirect）] です。

APIC リリース 5.2 以降では、IP-SLA トラッキングが有効化されている場合、L3 PBR の MAC 設定は必須ではありません。MAC 設定は空白のままにするか、00:00:00:00:00:00 に設定できます。

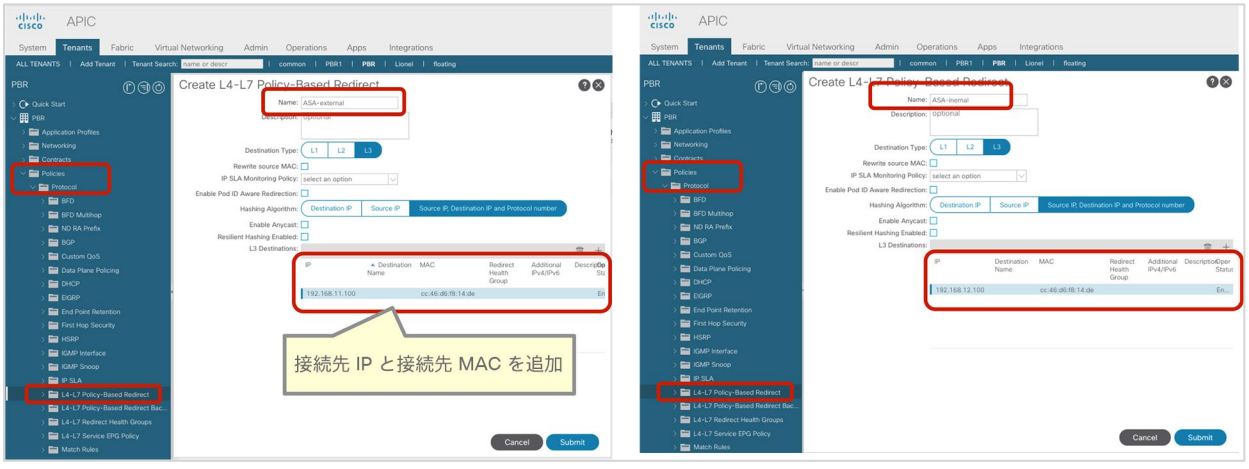


図 94.
PBR ポリシーの作成

L4-L7 デバイスの作成

L4-L7 デバイスを作成します。L4-L7 デバイスの設定には、PBR 固有の設定はありません。1 つ以上の L4-L7 デバイスを設定できます。この例では、デバイス 1 とデバイス 2 という 2 つのデバイスがアクティブ/スタンバイ高可用性クラスタペアとして構成されています。[L4-L7ポリシーベースリダイレクト（L4-L7 Policy Based Redirect）] で定義された PBR ノードの IP アドレスと MAC アドレスが、アクティブ/スタンバイ高可用性クラスタペアの仮想 IP アドレスと仮想 MAC アドレスになります（図 95）。

場所は、[テナント（Tenant）] > [サービス（Services）] > [L4-L7] > [デバイス（Devices）] です。

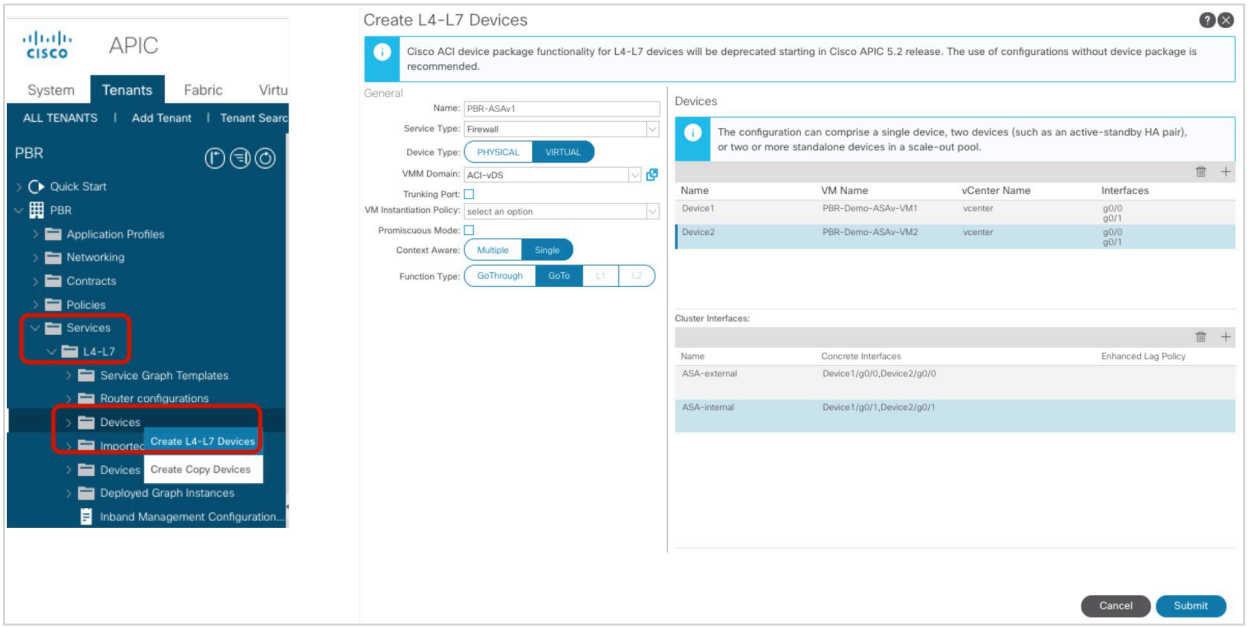
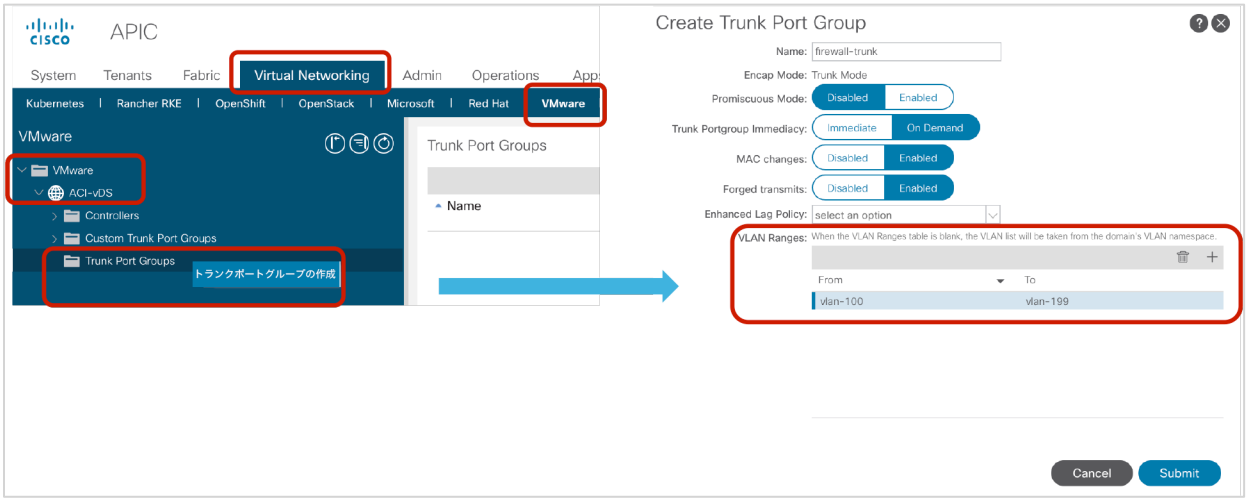


図 95.
L4-L7 デバイスの作成

設計によっては、次のポートグループ関連の設定オプションを有効化する必要があります。

- 無差別モード：L4-L7 仮想アプライアンスが、VM が所有する vNIC MAC ではない MAC を接続先とするトラフィックを受信する必要がある場合は、無差別モードのポートグループが必要です。デフォルトでは、go-to モード L4-L7 デバイスを使用したサービスグラフの展開によって作成されたポートグループの無差別モードは無効化されています。[L4-L7デバイスの作成（Create L4-L7 Device）] 設定でこのオプションをオンにすると、ポートグループの無差別モードが有効化されます。

- トランクポートグループ：デフォルトでは、ACI サービスグラフを設定することでアクセスモードのポートグループが作成され、L4-L7 VM の vNIC が自動的にそれにアタッチされます。したがって、L4-L7 VM はタグなしトラフィックを受信します。L4-L7 VM でタグ付きトラフィックを送受信する必要がある場合は、トランクポートグループを使用できます。[L4-L7デバイスの作成（Create L4-L7 Device）] 設定でこのオプションをオンにすると、vNIC の自動配置は行われません。このオプションは、Cisco ACI リリース 2.1 以降で使用できます。このオプションを使用したサービスグラフでは、VM のトランクポートグループの作成や自動 vNIC の配置は行われません。そのため、サービスグラフの設定に加えて、必要な VLAN を許可するトランクポートグループを作成し、そのトランクポートグループを VM の vNIC にアタッチする必要があります。トランクポートグループは、[仮想ネットワーク（Virtual Networking）] > [VMware] > [ドメイン名（Domain name）] > [トランクポートグループ（Trunk Port Groups）] で作成できます（図 96）。トランクポートグループを使用する場合、サービスグラフの展開によってクラスタインターフェイスの VLAN が自動的に生成されることも、vNIC が自動的に配置されることもありません。したがって、物理ドメインでの展開と同様に、L4-L7 デバイスのクラスタインターフェイスを L4-L7 デバイスに構成されている正しい VLAN に管理者が関連付ける必要があります。正しい VLAN ID を使用して L4-L7 VM インターフェイスを設定するには、動的 VLAN 割り当てではなく静的 VLAN 割り当てを使用する必要があります。デフォルトでは、VMM ドメインにある L4-L7 デバイスの場合、L4-L7 デバイスインターフェイスの VLAN ID は動的に割り当てられますが、静的 VLAN 範囲を動的 VLAN プールに追加できます。VLAN カプセル化は、クラスタインターフェイス設定で [カプセル化（Encap）] ボックスをオンにすることで、クラスタインターフェイスに静的に割り当てることができます（図 96）。
- 拡張 LAG ポリシー：VMM ドメインに使用される VMware vDS に VMware Link Aggregation Group（LAG）がある場合は、クラスタインターフェイスごとに LAG ポリシーを指定する必要があります。これがサービスグラフの展開によって作成されるポートグループの LAG ポリシーになります。このオプションは、Cisco ACI リリース 5.2 以降で使用できます。



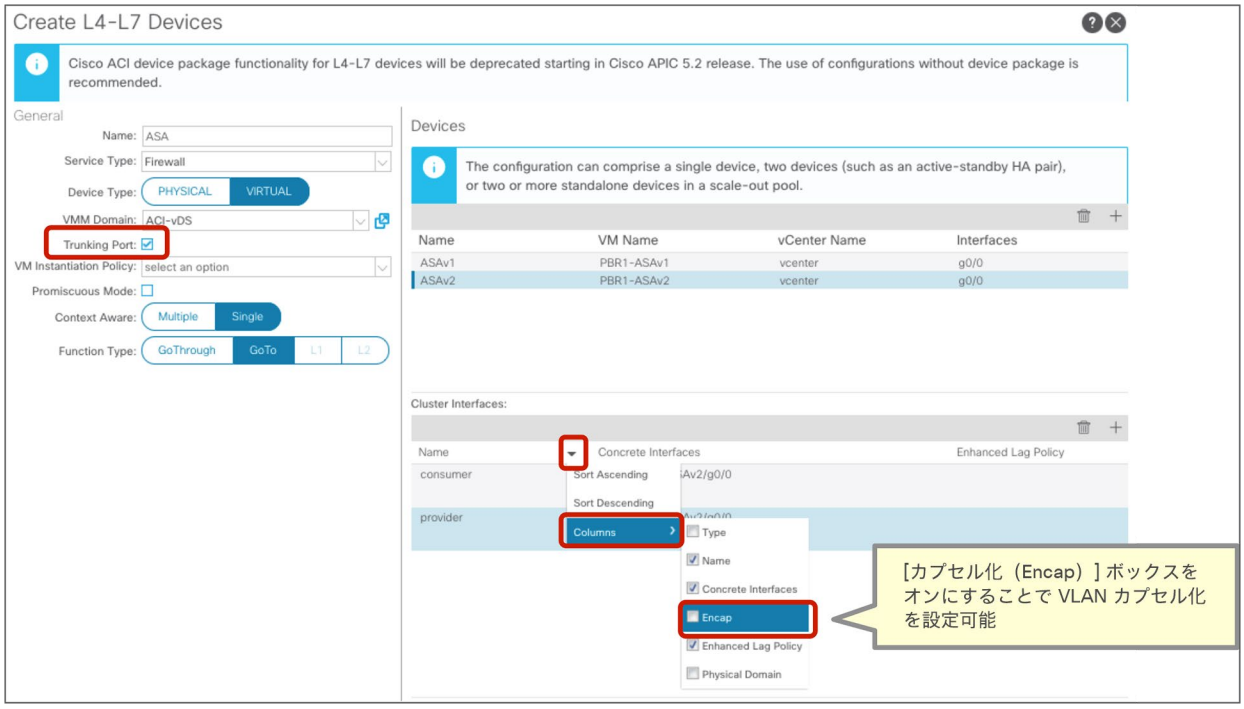


図 96.
トランクポートグループが設定された仮想アプライアンス

サービスグラフテンプレートの作成

作成した L4-L7 デバイスを使用してサービスグラフテンプレートを作成します。ノードで PBR を使用するには、ルートリダイレクトを有効化する必要があります（図 97）。

場所は、[テナント（Tenant）] > [サービス（Services）] > [L4-L7] > [サービスグラフテンプレート（Service Graph Templates）] です。

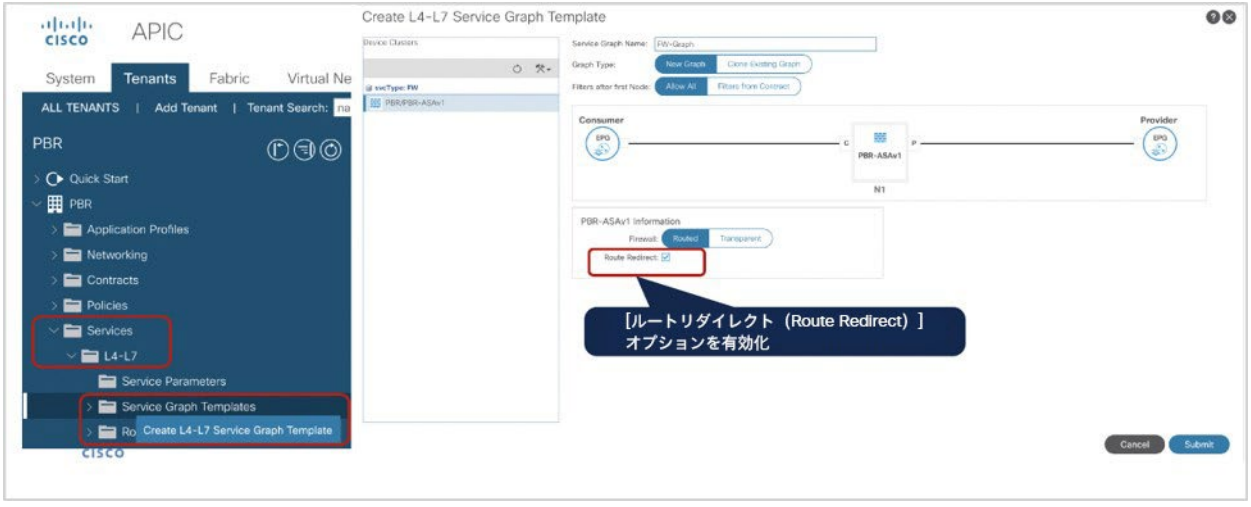


図 97.
サービスグラフテンプレートの作成

APIC リリース 4.2(3) 以降では、コントラクトからのフィルタ（filters-from-contract）オプションが導入されています。詳細については、「コントラクトからのフィルタ（filters-from-contract）オプション」セクションを参照してください。

デバイス選択ポリシーの作成

デバイス選択ポリシーを作成して、サービスノードのコンシューマーコネクタとプロバイダーコネクタのブリッジドメインと PBR ポリシーを指定します。図 98 の例では、サービスノードのコンシューマー側は「ASA-ext」ブリッジドメインにあり、以前に作成した PBR ポリシー ASA-external を使用しています。サービスノードのプロバイダー側は「ASA-int」ブリッジドメインにあり、PBR ポリシー ASA-internal を使用しています。その結果、コンシューマーからプロバイダーへの EPG トラフィックは ASA-external（192.168.11.100、CC:46:D6:F8:14:DE）にリダイレクトされ、プロバイダーからコンシューマーへの EPG トラフィックは ASA-internal（192.168.12.100、CC:46:D6:F8:14:DE）にリダイレクトされます。

場所は、[テナント（Tenant）] > [サービス（Services）] > [L4-L7] > [デバイス選択ポリシー（Device Selection Policies）] です。

[サービスグラフテンプレートの適用（Apply Service Graph Template）] ウィザードを使用する場合、デバイス選択ポリシーはウィザードを通じて作成されます。

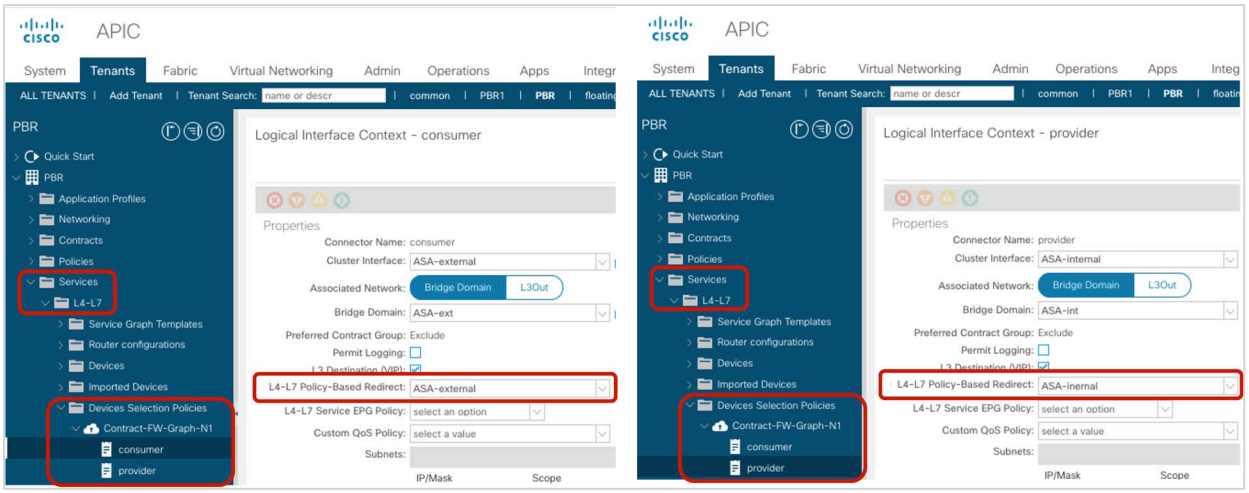


図 98.
デバイス選択ポリシーの作成（ツーアームモード）

コントラクトへのサービスグラフの適用

コントラクトサブジェクトにサービスグラフテンプレートを適用します。この例では、サービスグラフテンプレート FW-Graph がクライアント EPG と Web EPG の間のコントラクトに適用されます（図 99）。

場所は、[テナント（Tenant）] > [コントラクト（Contracts）] > [標準（Standard）] > [コントラクト（Contract）] です。

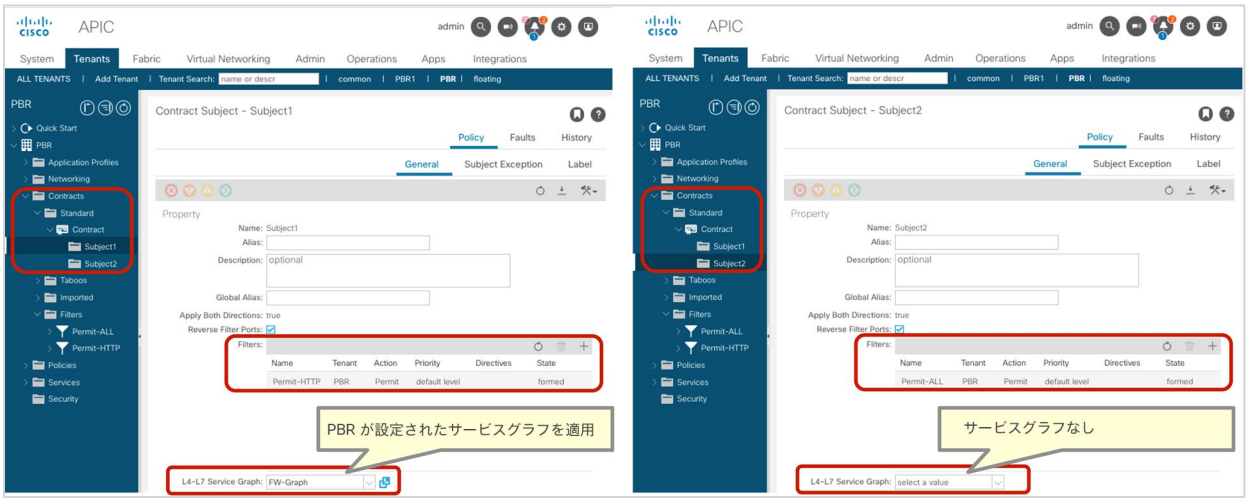


図 99.
コントラクトへのサービスグラフの適用

PBR は、コントラクトサブジェクトに設定されたフィルタに基づいて適用されます。そのため、コントラクトに Permit-HTTP フィルタが設定されたサブジェクトと Permit-ALL フィルタが設定されたサブジェクトがあり、前者にサービスグラフテンプレートを適用した場合、HTTP トラフィックのみがリダイレクトされます（図 100）。

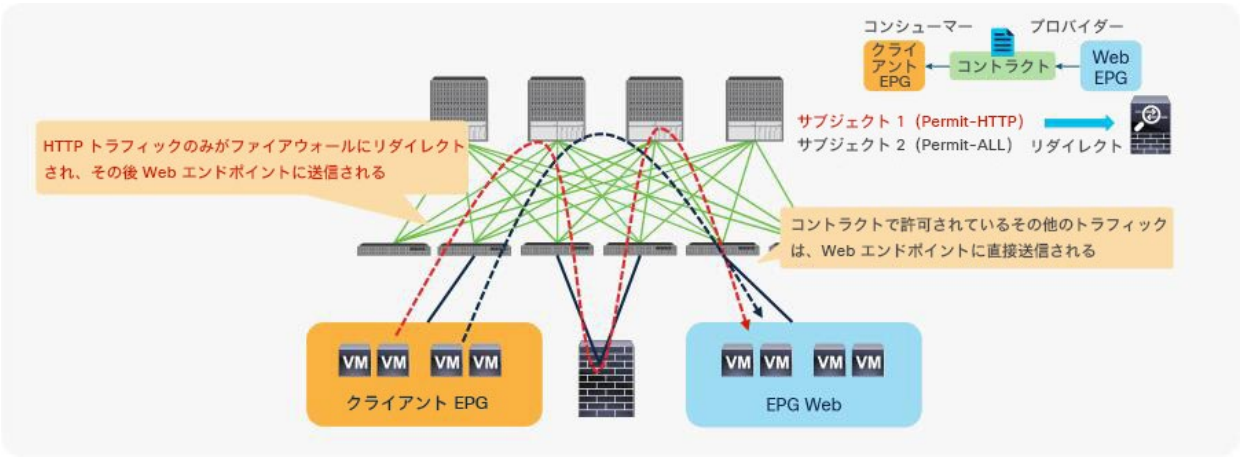


図 100.
コントラクトへのサービスグラフの適用

サブジェクトの順序は関係ありません。より制約の強いフィルタが優先されます。そのため、コントラクトに Permit-ALL フィルタが設定されたサブジェクトと Permit-HTTP フィルタが設定されたサブジェクトがあり、前者に PBR が有効化されたサービスグラフテンプレートが適用され、後者にサービスグラフがない場合、HTTP トラフィックを除くすべてのトラフィックがリダイレクトされます。

確認用の GUI と CLI の出力例

サービスグラフテンプレートが正常に適用されると、展開されたグラフインスタンスを確認できます。管理対象モードを使用している場合は、展開されたデバイスも表示されます（図 101）。

サービスグラフのインスタンス化に失敗すると、展開されたグラフインスタンスにエラーが表示されます。たとえば、デバイス選択ポリシーが設定されていない場合、「管理モードの L4-L7 パラメータが正しく設定されていません」といったエラーが表示されます。

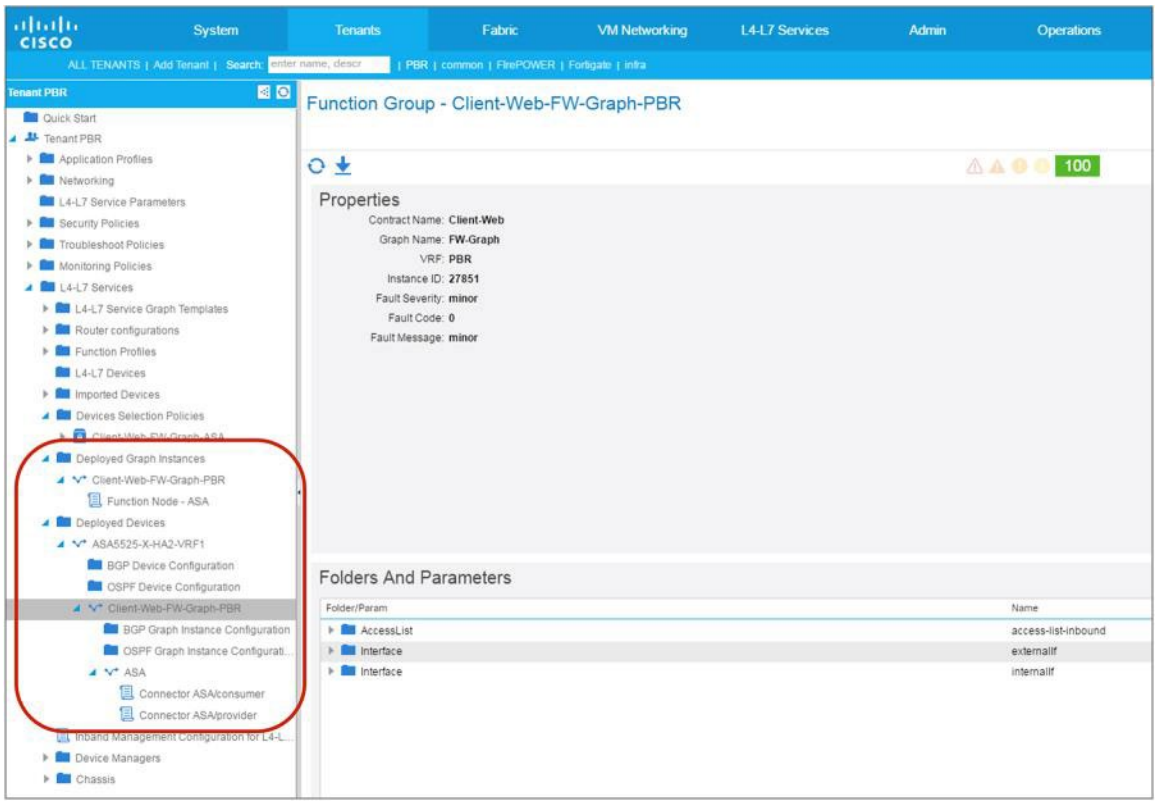


図 101.
展開されたグラフインスタンスと展開されたデバイス

前のセクションで説明したように、PBR ポリシーはコンシューマーのリーフノードとプロバイダーのリーフノードでプログラムされます。図 102 と 103 に、サービスグラフの展開前後の例を示します。これらの例では、コンシューマー EPG のクラス ID は 32771、プロバイダー EPG のクラス ID は 49154 です。

```
Leaf1# show service redir info
GrpID Name                          destination                                operSt
===== ====                          ===========                                ======

Leaf1# show zoning-rule | grep redir
```

図 102.
接続先グループとリダイレクトポリシー（サービスグラフ展開前）

```
Leaf1# show service redir info
GrpID Name                          destination                                   operSt
===== ====                          ===========                                   ======
5     destgrp-5                     dest-[192.168.11.100]-[vxlan-2555906]]        enabled
6     destgrp-6                     dest-[192.168.12.100]-[vxlan-2555906]]        enabled

Leaf1# show zoning-rule | grep redir
4288    32771           49154           default         enabled         2555906         redir(destgrp-5)        src_dst_any(8)
4290    49154           32771           default         enabled         2555906         redir(destgrp-6)        src_dst_any(8)
```

図 103.
接続先グループとリダイレクトポリシー（サービスグラフ展開後）

トラフィックが実際に PBR ノードにリダイレクトされているかどうかを確認したい場合は、PBR ノードでその情報をキャプチャできます。図 104 に、Cisco ASA を使用した場合の例を示します。ASA では、コマンドライン インターフェイス（CLI）または GUI からリアルタイムのキャプチャが可能です。この例では、192.168.1.1 が 192.168.2.1 への ping と 192.168.2.1:80 へのアクセスを試みています。PBR が設定されたサービスグラフが Permit-HTTP フィルタとともに適用されるため、HTTP トラフィックのみがリダイレクトされます。したがって、ASA で HTTP トラフィックは確認できますが、ICMP トラフィックは確認できません。

```
ASA5525X-1/6-ASA-HA-routed2# capture externalIf interface externalIf real-time

Warning: using this option with a slow console connection may
         result in an excessive amount of non-displayed packets
         due to performance limitations.

Use ctrl-c to terminate real-time capture


   1: 17:25:35.829546       802.1Q vlan#672 P0 192.168.1.1.49183 > 192.168.2.1.80: S 1736820795:1736820795(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
   2: 17:25:35.830019       802.1Q vlan#672 P0 192.168.2.1.80 > 192.168.1.1.49183: S 2928727526:2928727526(0) ack 1736820796 win 8192 <mss 1380,nop,wscale 8,nop,nop,sackOK>
   3: 17:25:35.830676       802.1Q vlan#672 P0 192.168.1.1.49183 > 192.168.2.1.80: . ack 2928727527 win 16560
   4: 17:25:35.834582       802.1Q vlan#672 P0 192.168.1.1.49183 > 192.168.2.1.80: P 1736820796:1736821209(413) ack 2928727527 win 16560
   5: 17:25:35.887481       802.1Q vlan#672 P0 192.168.2.1.80 > 192.168.1.1.49183: . ack 1736821209 win 258
   6: 17:25:35.920881       802.1Q vlan#672 P0 192.168.2.1.80 > 192.168.1.1.49183: P 2928727527:2928728296(769) ack 1736821209 win 258
   7: 17:25:36.068767       802.1Q vlan#672 P0 192.168.1.1.49184 > 192.168.2.1.80: S 1781356319:1781356319(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
   8: 17:25:36.069103       802.1Q vlan#672 P0 192.168.2.1.80 > 192.168.1.1.49184: S 2150204720:2150204720(0) ack 1781356320 win 8192 <mss 1380,nop,wscale 8,nop,nop,sackOK>
   9: 17:25:36.069317       802.1Q vlan#672 P0 192.168.1.1.49184 > 192.168.2.1.80: . ack 2150204721 win 16560
  10: 17:25:36.069469       802.1Q vlan#672 P0 192.168.1.1.49184 > 192.168.2.1.80: P 1781356320:1781356609(289) ack 2150204721 win 16560
  11: 17:25:36.070949       802.1Q vlan#672 P0 192.168.2.1.80 > 192.168.1.1.49184: . 2150204721:2150206101(1380) ack 1781356609 win 258
  12: 17:25:36.070949       802.1Q vlan#672 P0 192.168.2.1.80 > 192.168.1.1.49184: P 2150206101:2150206103(2) ack 1781356609 win 258
  13: 17:25:36.071544       802.1Q vlan#672 P0 192.168.1.1.49184 > 192.168.2.1.80: . ack 2150206103 win 16560
  14: 17:25:36.073619       802.1Q vlan#672 P0 192.168.1.1.49184 > 192.168.2.1.80: R 1781356609:1781356609(0) ack 2150206103 win 0
  15: 17:25:36.191045       802.1Q vlan#672 P0 192.168.1.1.49183 > 192.168.2.1.80: . ack 2928728296 win 16367
15 packets shown.
0 packets not shown due to performance limitations.
```

図 104.
Cisco ASA のスクリーンキャプチャの例

ワンアームモード PBR の設定例

このセクションでは、図 105 を例として使用して、ワンアームモード PBR の設定に関する考慮事項について説明します。この例では、コンシューマー EPG とプロバイダー EPG が同じブリッジドメインサブネットにありますが、異なるブリッジドメインサブネットにあっても問題ありません。

この説明は、Cisco ACI の基本的な設定と PBR 関連の設定が完了していることを前提としています。たとえば、PBR ノードブリッジドメイン、PBR ポリシー、L4-L7 デバイス、サービスグラフテンプレートは設定済みであるとしています。

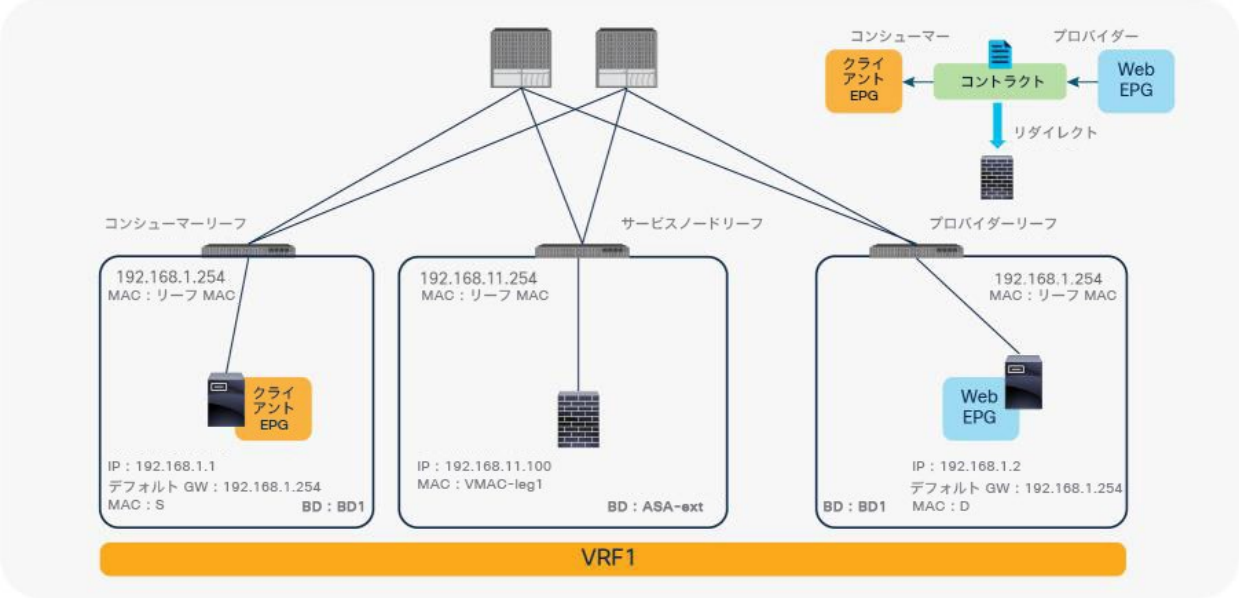


図 105.
1 ノード PBR の設計例（ワンアームモード）

デバイス選択ポリシーに関する考慮事項

PBR ノードのインターフェイスは 1 つですが、デバイス選択ポリシーには、コンシューマーコネクタとプロバイダーコネクタの両方の設定があります。ワンアームモードのサービスグラフの場合は、デバイス選択ポリシーにあるコンシューマーコネクタとプロバイダーコネクタの両方の設定で同じオプションを選択するだけです。これにより、サービスグラフのインスタンス化中に 1 つのインターフェイスに 1 つのセグメントのみが展開されます（図 106）。

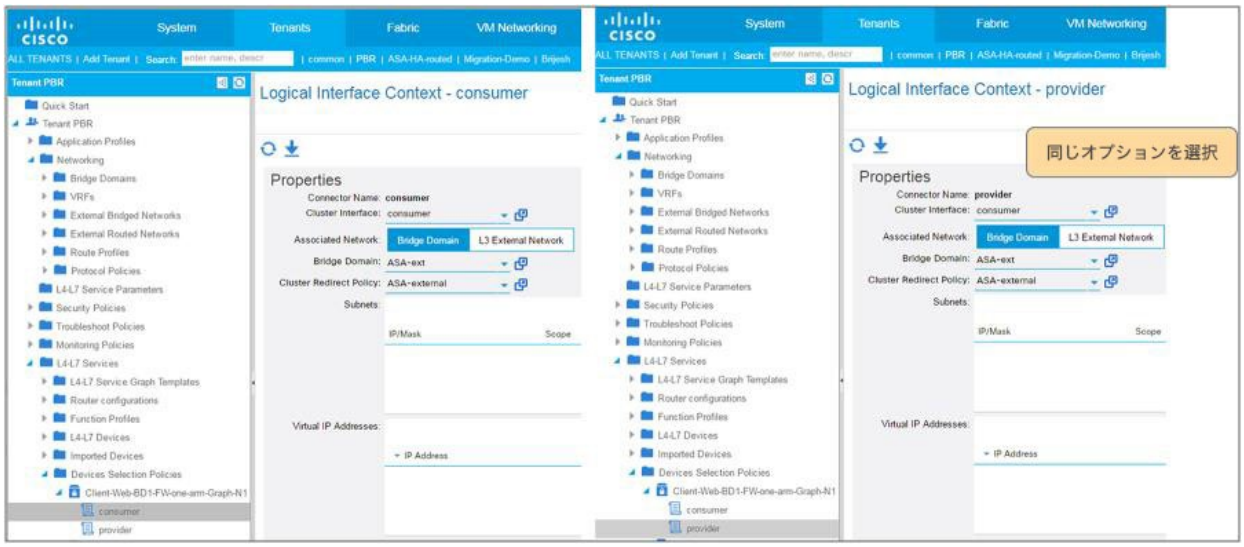


図 106.
デバイス選択ポリシー（ワンアームモード）

ファイアウォールの設定に関する考慮事項

同じインターフェイスを介して送受信されるトラフィックをファイアウォールが拒否する場合があります。インターフェイス内トラフィックを許可するようにファイアウォールを設定する必要があります。たとえば、Cisco ASA はデフォルトでインターフェイス内トラフィックを拒否します。インターフェイス内トラフィックを許可するには、ASA で **same-security-traffic permit intra-interface** を設定します。管理対象モードのサービスグラフを使用している場合、この設定は [L4-L7デバイス（L4-L7 Device）] にあります（図 107）。

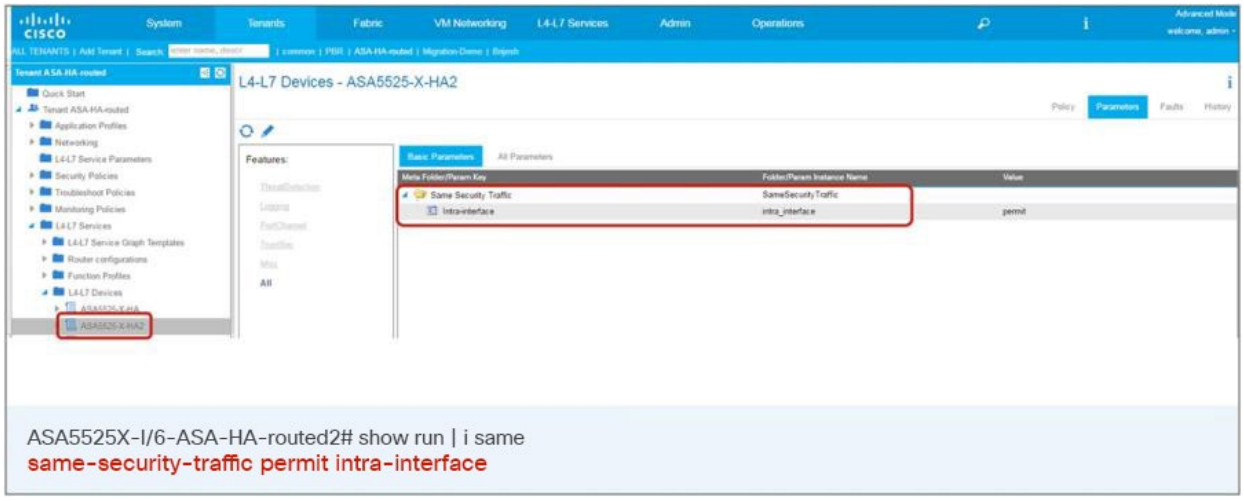


図 107.
same-security-traffic permit intra-interface の設定

Address Resolution Protocol（ARP）の動作に関する考慮事項

このセクションでは、ワンアームモード PBR 設計を例に、非 IP トラフィックを含む共通デフォルトフィルタ（Permit All）を PBR に使用すべきではない理由について説明します。同じブリッジドメイン内の EPG 間に PBR を設定する場合は、Permit All コントラクトフィルタを使用しないでください。このフィルタは、Address Resolution Protocol（ARP）トラフィックも L4-L7 デバイスにリダイレクトするためです（図 108）。この例では ARP が使用されていますが、IP フィルタや IPv6 フィルタから ICMPv6 トラフィックを除外する際にも同じ考慮事項が適用されます。

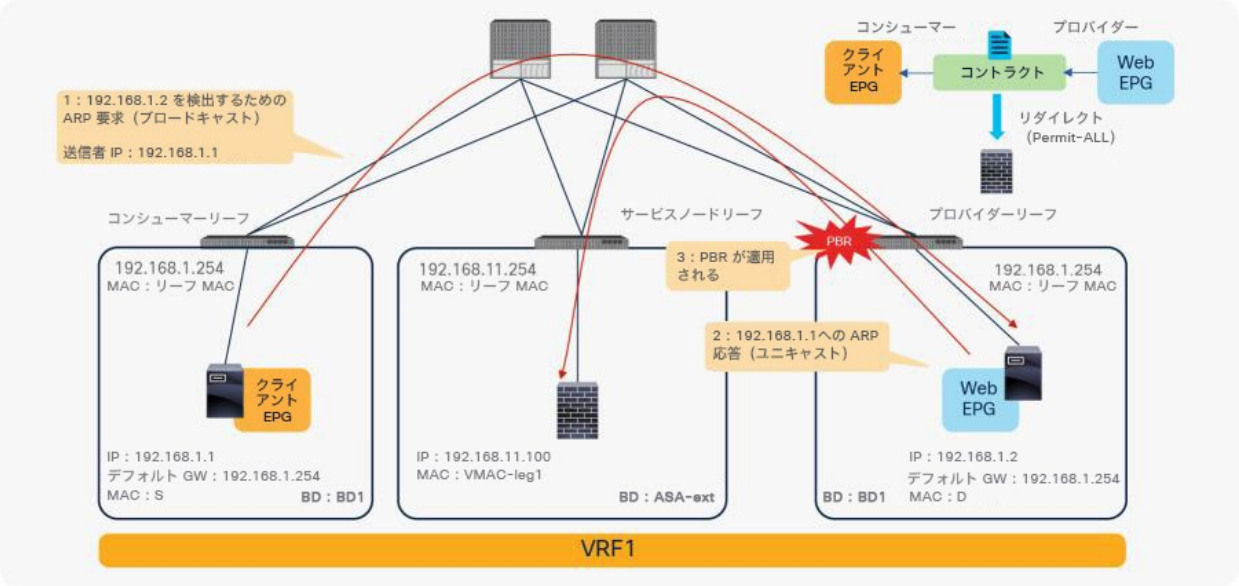


図 108.
ARP に関する考慮事項の例

コントラクトサブジェクトのフィルタが Permit All に設定されていない場合、たとえば Permit ICMP や Permit HTTP に設定されている場合や、ARP を含めない制約の強いフィルタの場合は、ARP トラフィックがリダイレクトされないため、正常に機能します。

図 109 と図 110 に、設定例とその動作を示します。サブジェクトの順序は関係ありません。最も制約の強いフィルタが優先されるため、クライアント EPG と Web EPG の間の HTTP トラフィックのみがリダイレクトされます。

図 109.
ARP 応答を除外するコントラクトサブジェクトの設定例

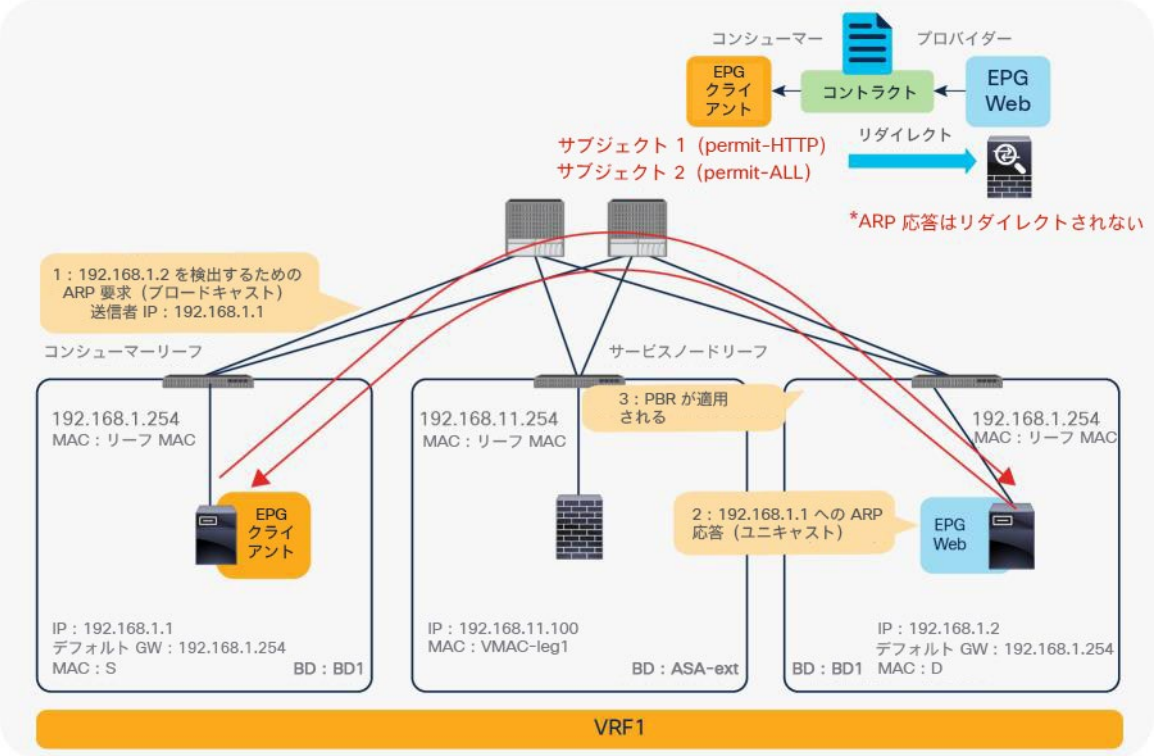


図 110.
ARP 応答トラフィックはリダイレクトされない

VRF 間の設定例

このセクションでは、図 111 を例として使用して、VRF 間 PBR 設定に関する考慮事項について説明します。この例では、コンシューマー EPG とプロバイダー EPG が異なる VRF インスタンスにあり、PBR ノードはこれらの VRF インスタンスの間にあります。

この説明は、Cisco ACI の基本的な設定と PBR 関連の設定が完了していることを前提としています。たとえば、PBR ノードブリッジドメイン、PBR ポリシー、L4-L7 デバイス、サービスグラフテンプレートは設定済みであるとしています。

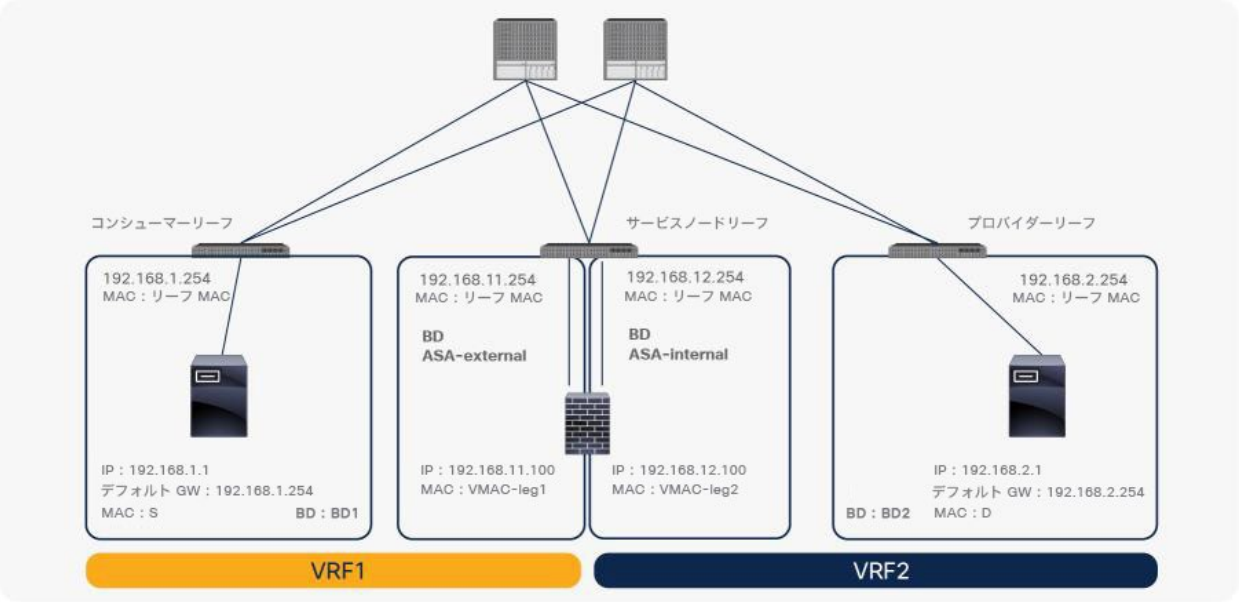


図 111.
VRF 間設計の例

コンシューマーのブリッジドメインとプロバイダーのブリッジドメインのルートリーク設定

「展開オプション」セクションでの説明にあるように、VRF 間設計では、EPG サブネットを他の VRF インスタンスにリークして、EPG のクラス ID を取得できるようにする必要があります。サブネットを別の VRF インスタンスにリークするには、サブネット範囲を VRF 間で共有する必要があります。コンシューマー EPG のブリッジドメイン配下のサブネットとプロバイダー EPG のブリッジドメイン配下のサブネットを、[VRF間で共有（Shared across VRFs）] に設定する必要があります。これは、VRF 間コントラクトの設定の場合と同じです。PBR ノードブリッジドメインのサブネットは、この例では宛先 IP アドレスになることはないため、リークする必要はありません（図 112）。

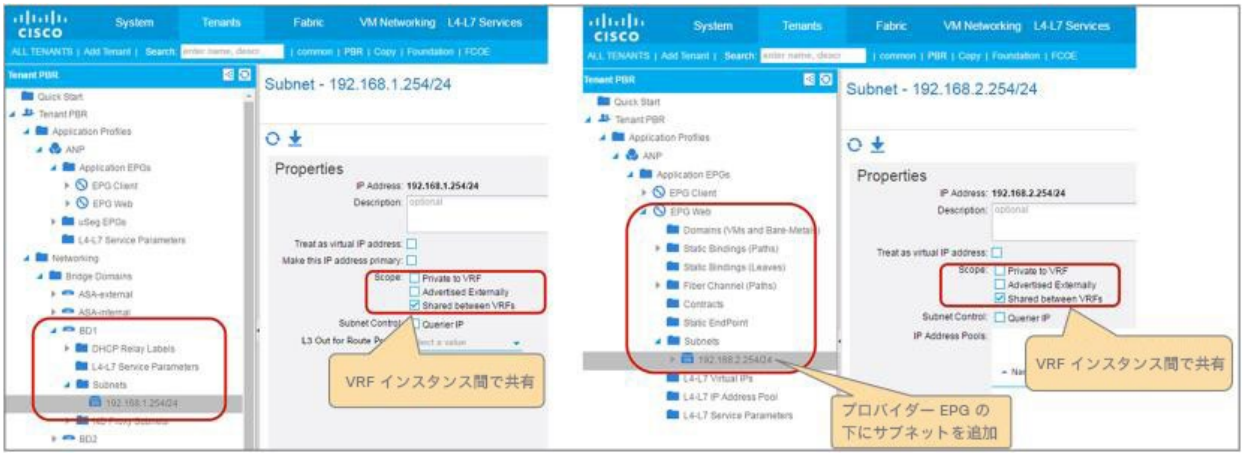


図 112.
ルートリークの設定例

PBR ノードブリッジドメインのルートリーク設定

コンシューマー EPG またはプロバイダー EPG と PBR ノードの間の直接通信を許可する必要がある場合、PBR ノードサブネットも他の VRF インスタンスにリークする必要があります。さらに、[直接接続（Direct Connect）] オプションを [True] に設定する必要があります。図 113 にトポロジの例を示します。PBR ノードのコンシューマー側が配置されている 192.168.11.0/24 サブネットを VRF1 にリークする必要があります。

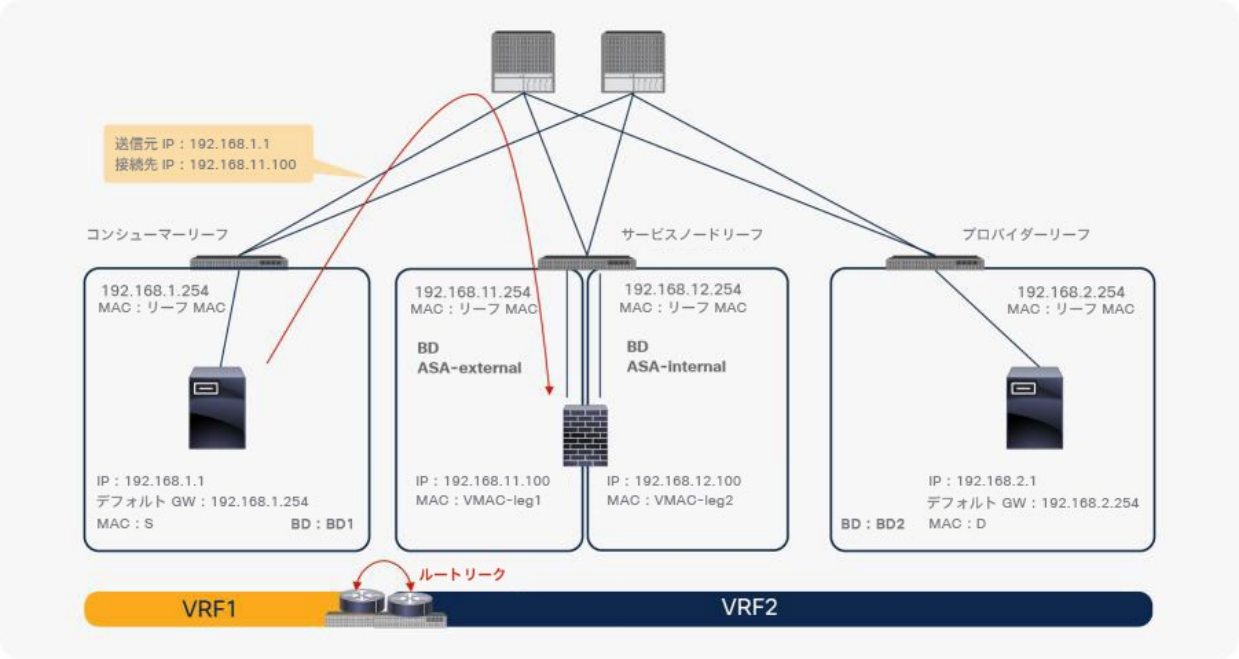


図 113.
ルートリークのトポロジ

図 113 に示すように、PBR ノードサブネットをコンシューマーの VRF インスタンスにリークする必要がある場合は、デバイス選択ポリシーにサブネットを追加する必要があります（図 114）。この設定はプロバイダー EPG 配下のサブネットの設定と似ていますが、設定を行う場所が異なります。サービスノード EPG が通常の EPG として表示されないためです。

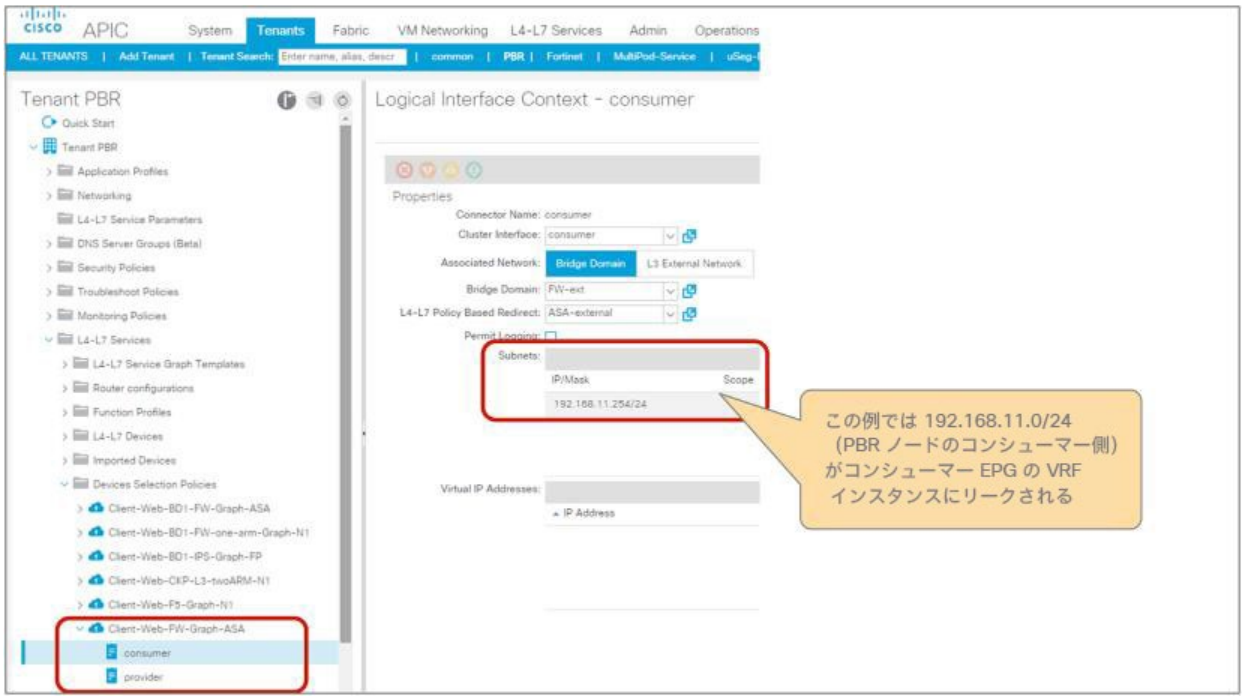


図 114.
デバイス選択ポリシーの設定例

PBR ノードサブネットをプロバイダーの VRF インスタンスにリークする必要がある場合は、図 115 のように、PBR ノードブリッジドメイン（この例では ASA -internal ブリッジドメイン）で [VRF間で共有（Shared between VRFs）] オプションを有効化する必要があります。ただし、コンシューマーのブリッジドメインのサブネットがプロバイダーの VRF インスタンスにリークされるため、デバイス選択ポリシーにサブネットを追加する必要はありません。

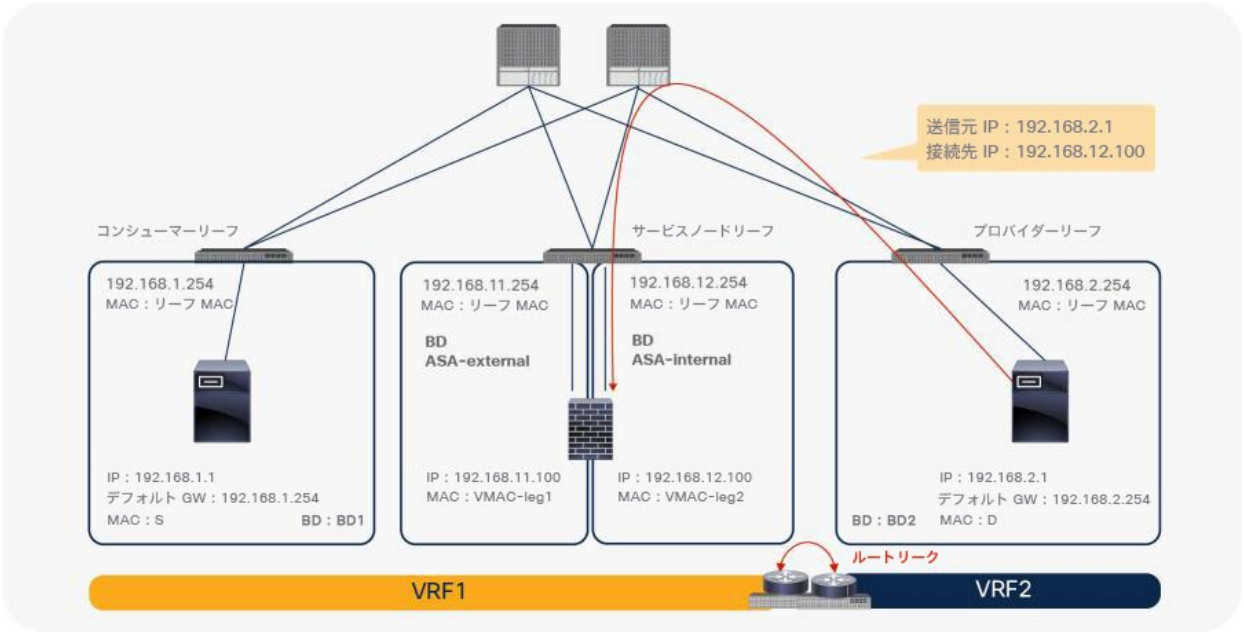


図 115.
PBR ノードサブネットをプロバイダーの VRF インスタンスにリークするトポロジ

VRF 内コントラクトと VRF 間コントラクトで同じ PBR ノードインターフェイスを再利用する場合

VRF 間コントラクトと VRF 内コントラクトに同じ PBR ノードとそのインターフェイスを使用する場合は、VRF 内コントラクトと VRF 間コントラクトの各デバイス選択ポリシーで同じコンテキスト名を設定する必要があります。これは、サービスノードへのクラス ID の割り当てが VRF ごと（「コンテキスト」とも呼ばれる）であるためです。両方のコントラクトで使用されるインターフェイスに同じクラス ID を使用する必要があるため、サービスグラフの両方の展開で同じコンテキスト名を使用する必要があります。

たとえば、コントラクト 1 は VRF1 内の VRF 内通信用で、コントラクト 2 は VRF1 と VRF2 の間の VRF 間通信用で、どちらも同じファイアウォール インターフェイスである ASA-external を使用するとします（図 116）。コントラクト 1 のデバイス選択ポリシーとコントラクト 2 のデバイス選択ポリシーには、同じコンテキスト名を設定する必要があります（図 117）。

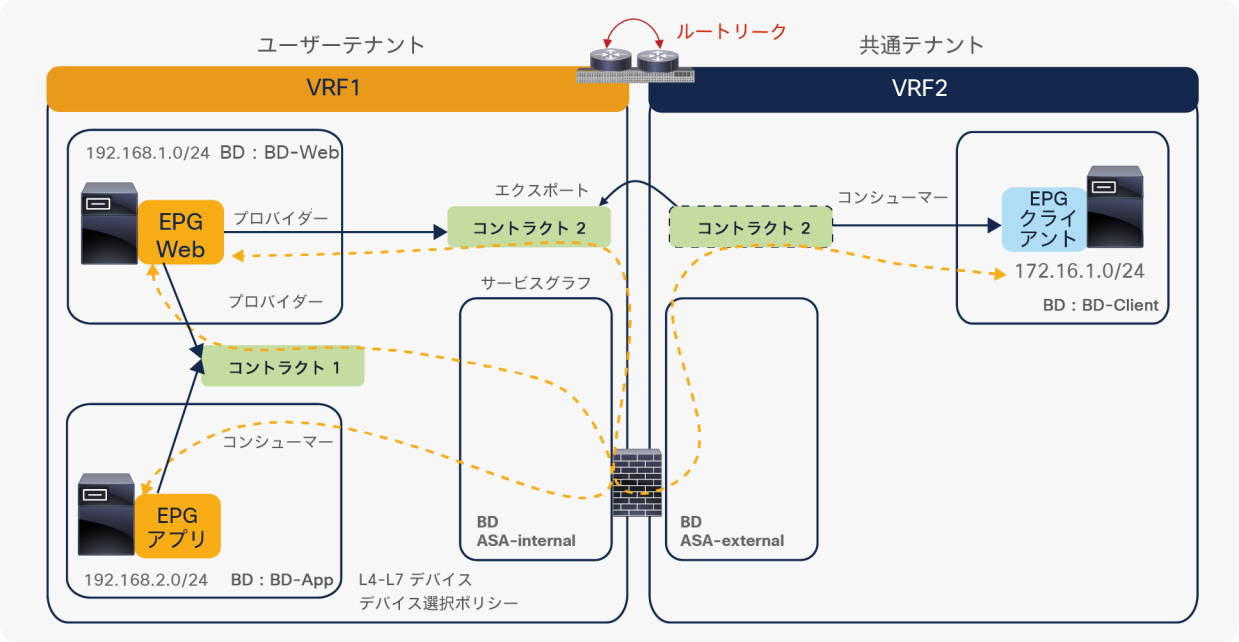


図 116.
VRF 内コントラクトと VRF 間コントラクトで同じ PBR ノードとそのインターフェイスを再利用

図 117.
デバイス選択ポリシーで同じコンテキスト名を使用

テナント間設定

コンシューマーの VRF インスタンスとプロバイダーの VRF インスタンスは、異なるテナントに置くことができます。VRF 間設定に加えて、テナント間サービスグラフを設定する場合には、追加で適用される重要な考慮事項がいくつかあります。

- 共通テナントで定義されたオブジェクトは他のテナントから参照できますが、ユーザーテナントで定義されたオブジェクトは同じテナントからしか参照できません。
- コントラクトは、プロバイダー EPG とコンシューマー EPG から参照できる必要があります。
- サービスグラフテンプレートは、コントラクトから参照できる必要があります。
- L4-L7 デバイスは、デバイス選択ポリシーから参照できる必要があります。
- デバイス選択ポリシーは、プロバイダー EPG のテナントで定義する必要があります。このオブジェクトは、L4-L7 デバイスのクラスタインターフェイスと PBR ブリッジドメインを参照できる必要があります。

図 118 に、プロバイダー EPG が共通テナントの VRF1 にあり、コンシューマー EPG がユーザーテナントの VRF2 にある構成例を示します。

- コントラクトは、コンシューマー EPG とプロバイダー EPG の両方から参照できるように、共通テナントで定義されます。
- プロバイダー EPG が共通テナントにあるため、デバイス選択ポリシーは共通テナントで定義されます。
- L4-L7 デバイスとサービスグラフテンプレートは、コントラクトがサービスグラフテンプレートを参照できるように、共通テナントで定義されます。
- VRF1 の PBR ブリッジドメインは、デバイス選択ポリシーが L4-L7 デバイスのクラスタインターフェイスと PBR ブリッジドメインを参照できるように、共通テナントで定義されます。

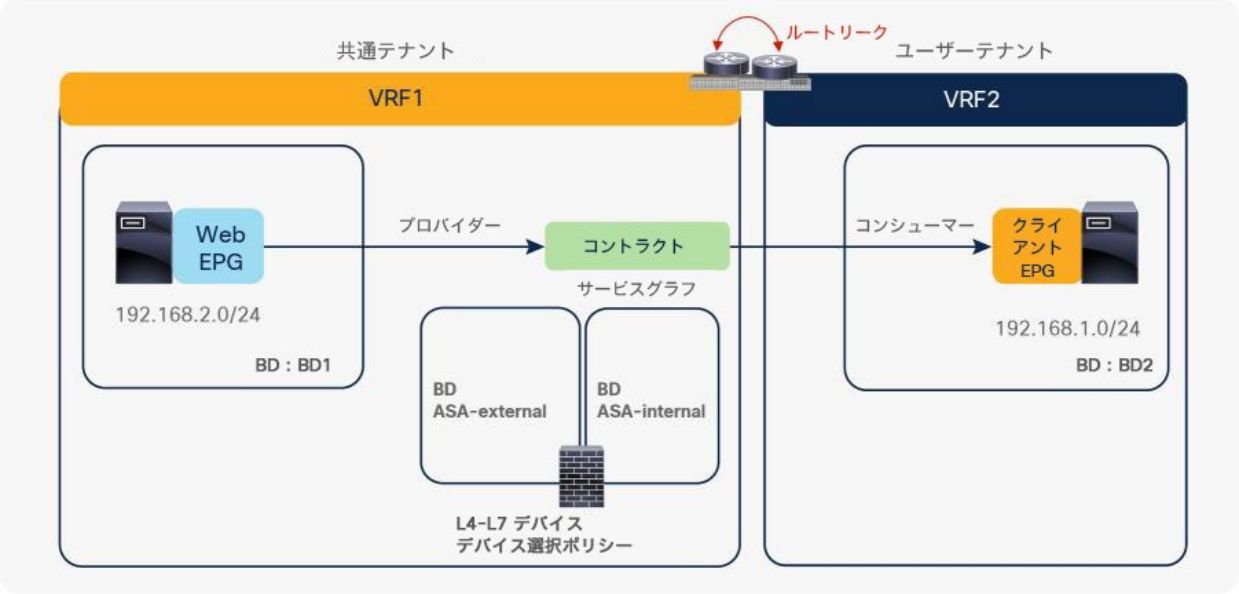


図 118.
PBR が設定されたテナント間サービスグラフの例（プロバイダー EPG が共通テナントにある場合）

図 119 に、コンシューマー EPG が共通テナントの VRF1 にあり、プロバイダー EPG がユーザーテナントの VRF2 にある構成例を示します。

- コントラクトはユーザーテナントで定義され、コンシューマー EPG とプロバイダー EPG の両方から参照できるように、共通テナントにエクスポートされます。
- プロバイダー EPG がユーザーテナントにあるため、デバイス選択ポリシーはユーザーテナントで定義されます。
- L4-L7 デバイスはユーザーテナントで定義されるか、または共通テナントで定義されてユーザーテナントにエクスポートされます。
- コントラクトがユーザーテナントで定義されているため、そのコントラクトがサービスグラフテンプレートを参照できるように、サービスグラフテンプレートはユーザーテナントで定義されます。
- PBR ブリッジドメインは、共通テナントの VRF1 またはユーザーテナントの VRF2 に置くことができます。これは、共通テナントまたはユーザーテナントで定義されたオブジェクトは、ユーザーテナントにあるデバイス選択ポリシーから参照できるためです。

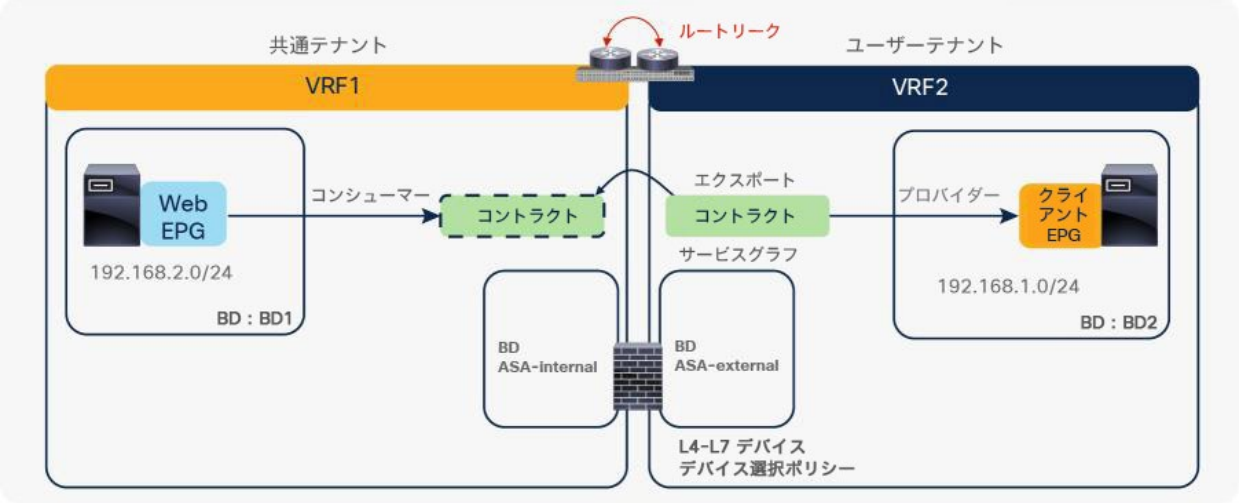


図 119.
PBR が設定されたテナント間サービスグラフの例（コンシューマー EPG が共通テナントにある場合）

上記の 2 つの例では、共通テナントとユーザーテナントの間のコントラクトを使用しています。ユーザーテナント間のコントラクトの場合は、2 番目の例と同様にコントラクトをエクスポートします。

図 120 に、プロバイダー EPG がユーザーテナントの VRF2 にあり、コンシューマー EPG が別のユーザーテナントの VRF1 にある構成例を示します。

- コントラクトはプロバイダーテナントで定義され、コンシューマー EPG とプロバイダー EPG の両方から参照できるように、コンシューマーテナントにエクスポートされます。
- プロバイダー EPG がプロバイダーテナントにあるため、デバイス選択ポリシーはプロバイダーテナントで定義されます。
- L4-L7 デバイスとサービスグラフテンプレートは、コントラクトがそのサービスグラフテンプレートを参照できるように、プロバイダーテナントで定義されます。
- VRF2 の PBR ブリッジドメインは、デバイス選択ポリシーが L4-L7 デバイスのクラスタインターフェイスと PBR ブリッジドメインを参照できるように、プロバイダーテナントで定義されます。

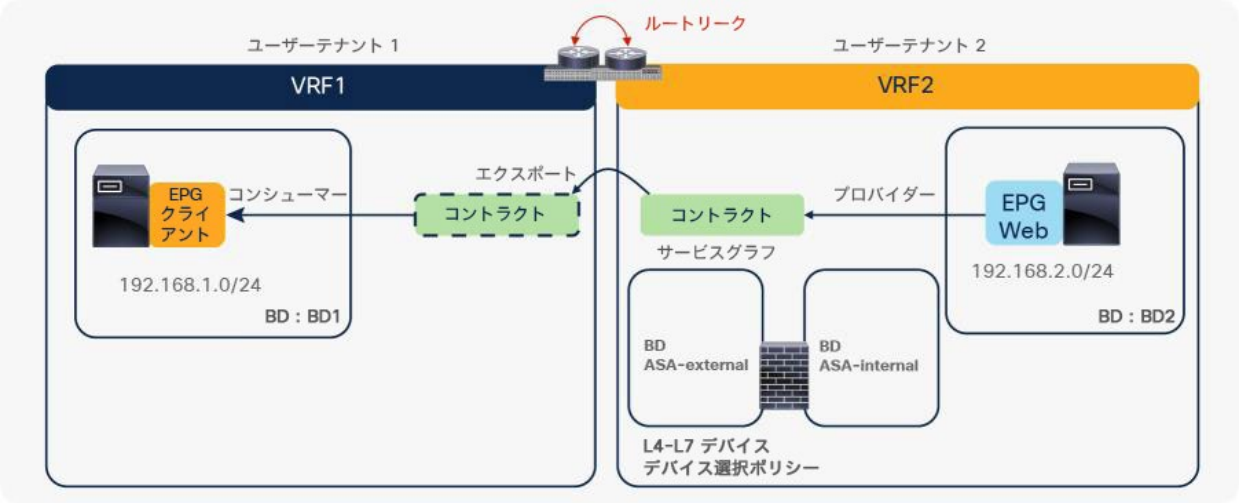


図 120.
PBR が設定されたテナント間サービスグラフの例（両方のテナントがユーザーテナントの場合）

単方向 PBR の設定例

このセクションでは、単方向 PBR の設定例を示します。デバイス選択ポリシーの設定を除き、単方向 PBR の設定は、このドキュメントで先に説明した基本的な PBR の設定と同じです。

PBR ポリシーの作成

場所は、[テナント（Tenant）] > [サービス（Services）] > [L4-L7] > [デバイス選択ポリシー（Device Selection Policies）] です。

送信元 NAT を実行しないロードバランサの単方向 PBR の場合（図 121）、両方のコネクタが 1 つの BD にあり、PBR はコンシューマーコネクタまたはプロバイダーコネクタのいずれかで有効化され、もう一方のコネクタでは有効化されません。

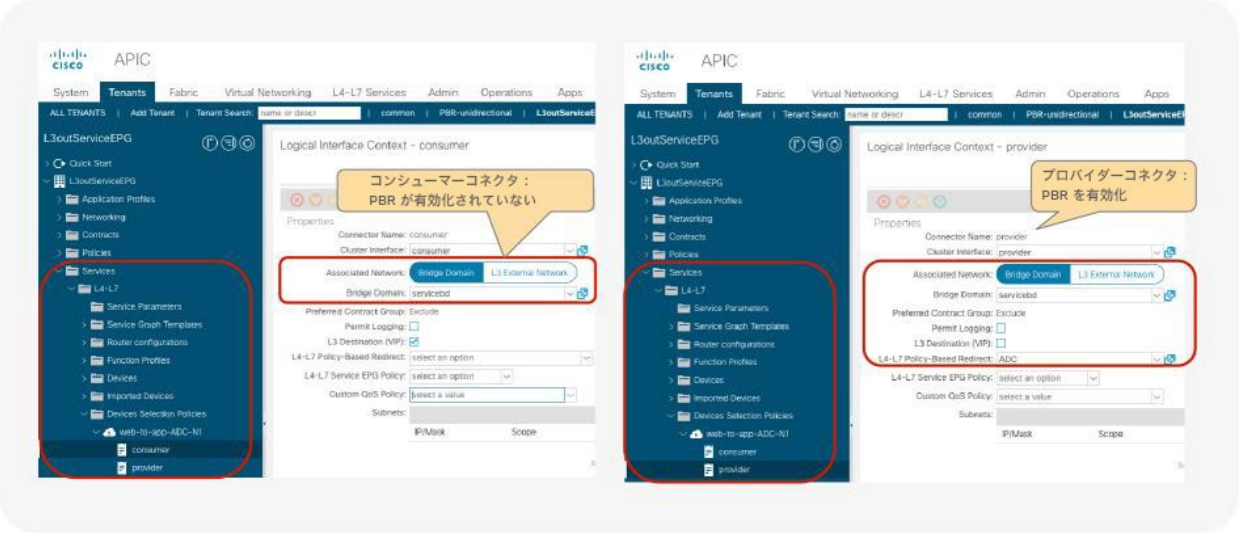


図 121.
単方向 PBR のデバイス選択ポリシーの作成

もう一方のコネクタが L3Out にある単方向 PBR の場合（図 122）、PBR は BD にあるコンシューマーコネクタで有効化され、L3Out にあるプロバイダーコネクタでは有効化されません。L3Out のプロバイダーコネクタで接続先 VIP を無効化する必要があります。有効化すると、このユースケースには不要なゾーン分割ルールが追加で作成されるためです。

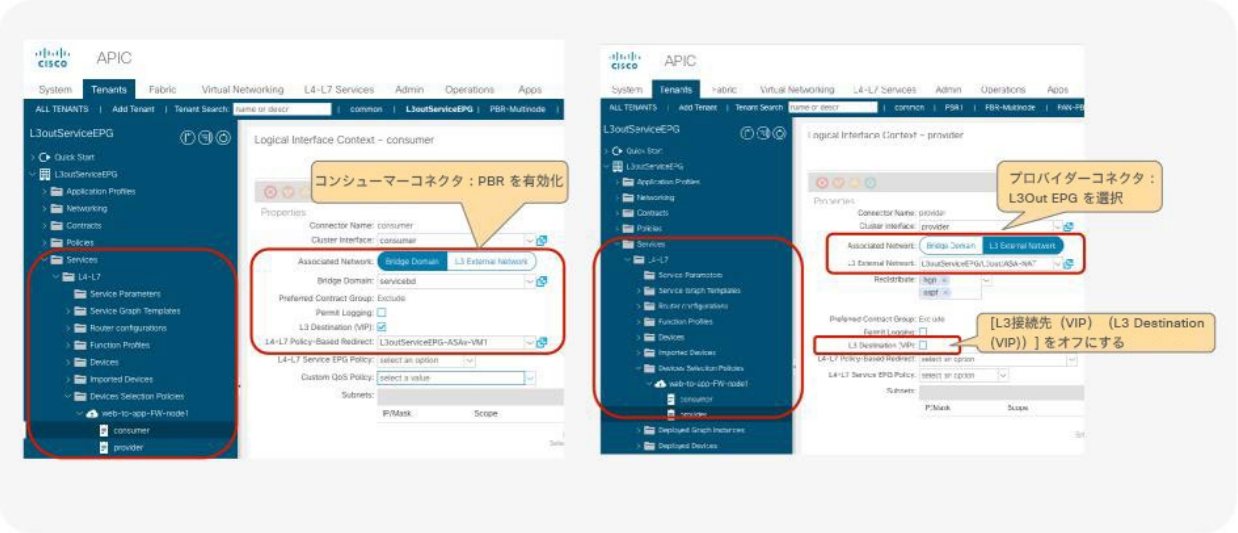


図 122.
もう一方のコネクタが L3Out にある単方向 PBR の PBR ポリシーの作成（PBR をコンシューマーコネクタで有効化する場合）

もう一方のコネクタが L3Out にある単方向 PBR の場合（図 123）、PBR は BD にあるプロバイダーコネクタで有効化され、L3Out にあるコンシューマーコネクタでは有効化されません。

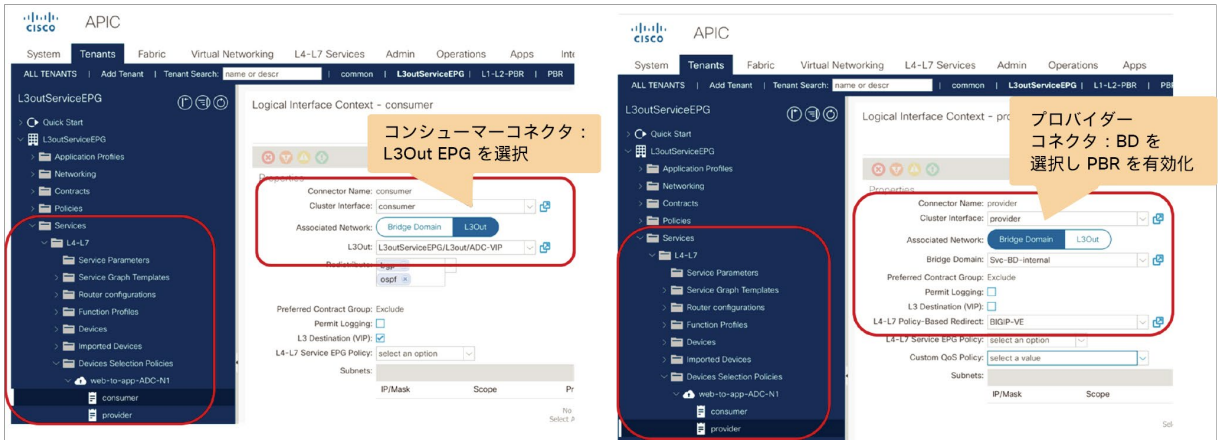


図 123.
もう一方のコネクタが L3Out にある単方向 PBR の PBR ポリシーの作成（PBR をプロバイダーコネクタで有効化する場合）

対称 PBR の設定例

このセクションでは、対称 PBR の設定例を示します。PBR ポリシーと L4-L7 デバイスの設定を除き、対称 PBR の設定は、このドキュメントで先に説明した基本的な PBR の設定と同じです。

PBR ポリシーの作成

複数の PBR 接続先を持つ PBR ポリシーを作成します（図 124）。APIC リリース 5.2 以降では、IP-SLA トラッキングが有効化されている場合、L3 PBR の MAC 設定は必須ではありません。MAC 設定は空白のままにするか、00:00:00:00:00:00 に設定できます。APIC リリース 6.0 以降では、PBR ポリシーごとに重みを設定できます。デフォルトでは、すべての PBR 接続先の重みが 1 に設定されます。

場所は、[テナント（Tenant）] > [ポリシー（Policies）] > [プロトコル（Protocol）] > [L4-L7ポリシーベースリダイレクト（L4-L7 Policy Based Redirect）] です。

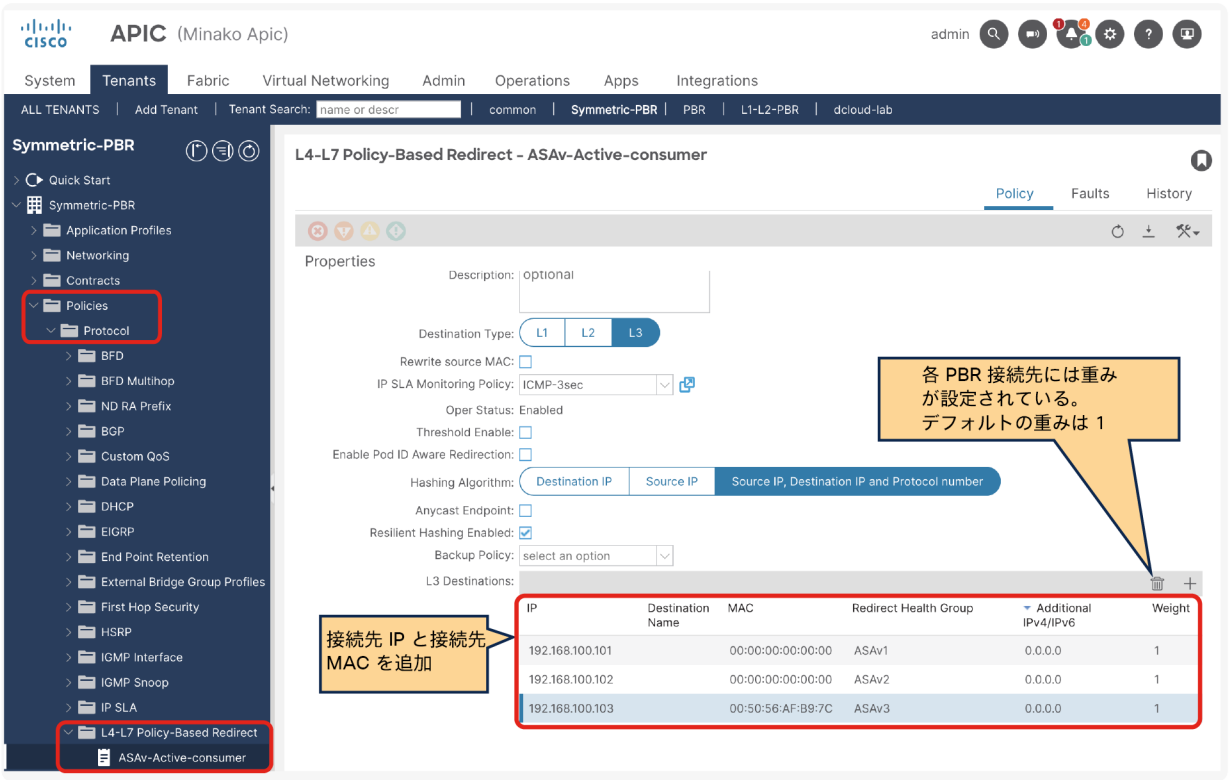


図 124.
PBR ポリシーの作成

注： デフォルトでは、接続先グループ内での IP アドレスの順序は重要です。PBR ノードが複数ある場合は、ランダムな順序ではなく IP アドレスと同じ順序で設定する必要があります。PBR ノードに インターフェイスが 2 つあり、一方の IP アドレスが接続先グループ内で最小の場合、もう一方のインターフェイスの IP アドレスはもう一方の 接続先グループで最小にする必要があります。これは、着信トラフィックとリターントラフィックが同じ PBR ノードに送信されるようにするためです。たとえば、図 124 の 192.168.11.101 のデバイスは 192.168.12.101 を使用し、192.168.11.102 のデバイスは 192.168.12.102 を使用する必要があります。APIC リリース 4.2(5) および 5.0 以降では、PBR 接続先の IP アドレスの順序が正しくない場合に、IP アドレスベースのソートではなく、接続先名ベースのソートを使用する接続先名オプションが追加されました。接続先名の設定方法については、「接続先名」セクションを参照してください。

L4-L7 デバイスの作成

複数の具象デバイスを使用して L4-L7 デバイスを作成します。対称 PBR は、各 PBR ノードの設定が一意であるため、非管理対象モードのサービスグラフでのみサポートされます（図 125）。

場所は、[テナント（Tenant）] > [サービス（Services）] > [L4-L7] > [デバイス（Devices）] です。

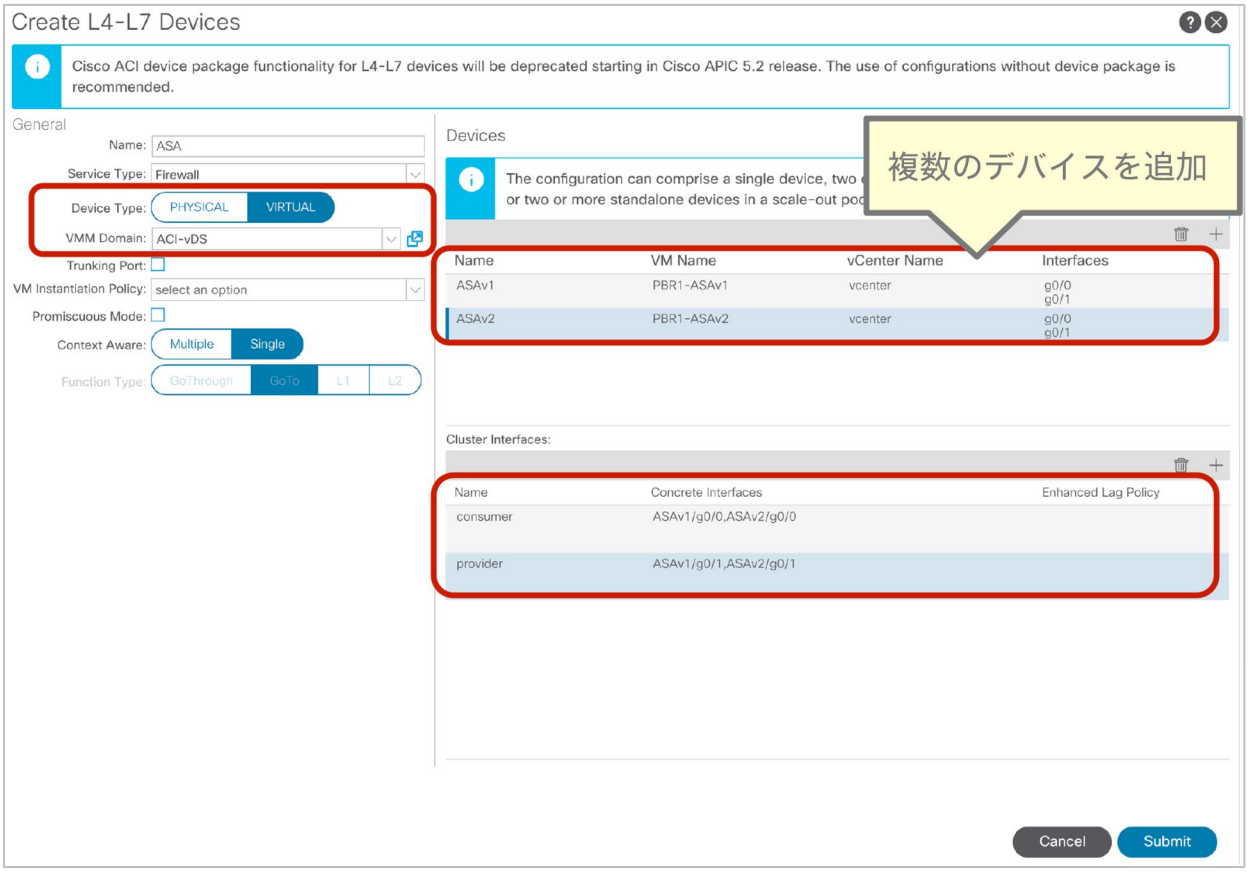


図 125.

L4-L7 デバイスの作成：確認用の CLI 出力例

前述の例のように、リダイレクトポリシーは、コンシューマーリーフノードとプロバイダーリーフノードでプログラムされ、コンシューマークラス ID とプロバイダークラス ID の間に設定されます。単一の PBR ノードの場合と比較すると、この例では「service redir info」に複数の接続先があります（図 126 および図 127）。

```
Leaf1# show service redir info
GrpID Name                            destination                                operSt
===== ====                            ===========                                ======

Leaf1# show zoning-rule | grep redir
```

図 126.
接続先グループとリダイレクトポリシー（サービスグラフ展開前）

```
Leaf1# show service redir info
GrpID Name                            destination                                 operSt
===== ====                            ===========                                 ======
5     destgrp-5                       dest-[192.168.11.100]-[vxlan-2555906]]      enabled
6     destgrp-6                       dest-[192.168.12.100]-[vxlan-2555906]]      enabled

Leaf1# show zoning-rule | grep redir
4288    32771           49154           default         enabled         2555906         redir(destgrp-5)        src_dst_any(8)
4290    49154           32771           default         enabled         2555906         redir(destgrp-6)        src_dst_any(8)
```

図 127.
接続先グループとリダイレクトポリシー（サービスグラフ展開後）

オプション設定

このセクションでは、PBR のオプション設定について説明します。

ハッシュアルゴリズムの設定

図 128 に、ハッシュアルゴリズムの設定を示します。

場所は、[テナント（Tenant）] > [ポリシー（Policies）] > [プロトコル（Protocol）] > [L4-L7ポリシーベースリダイレクト（L4-L7 Policy Based Redirect）] です。デフォルト設定は、[Source IP, Destination IP and Protocol number] です。

図 128.
ハッシュアルゴリズム

PBR ノードトラッキングの設定

各 L4-L7 PBR ノードでトラッキングを有効化できます（図 129）。場所は、[テナント（Tenant）] > [ポリシー（Policies）] > [プロトコルポリシー（Protocol Policies）] > [L4-L7ポリシーベースリダイレクト（L4-L7 Policy Based Redirect）] です。

トラッキング機能では、各 L4-L7 PBR ノードの接続先ごとに、しきい値、ダウンアクション、IP サービスレベル契約（SLA）モニタリングポリシー、復元力のあるハッシュ、バックアップ PBR ポリシー、ヘルスグループも設定できます。

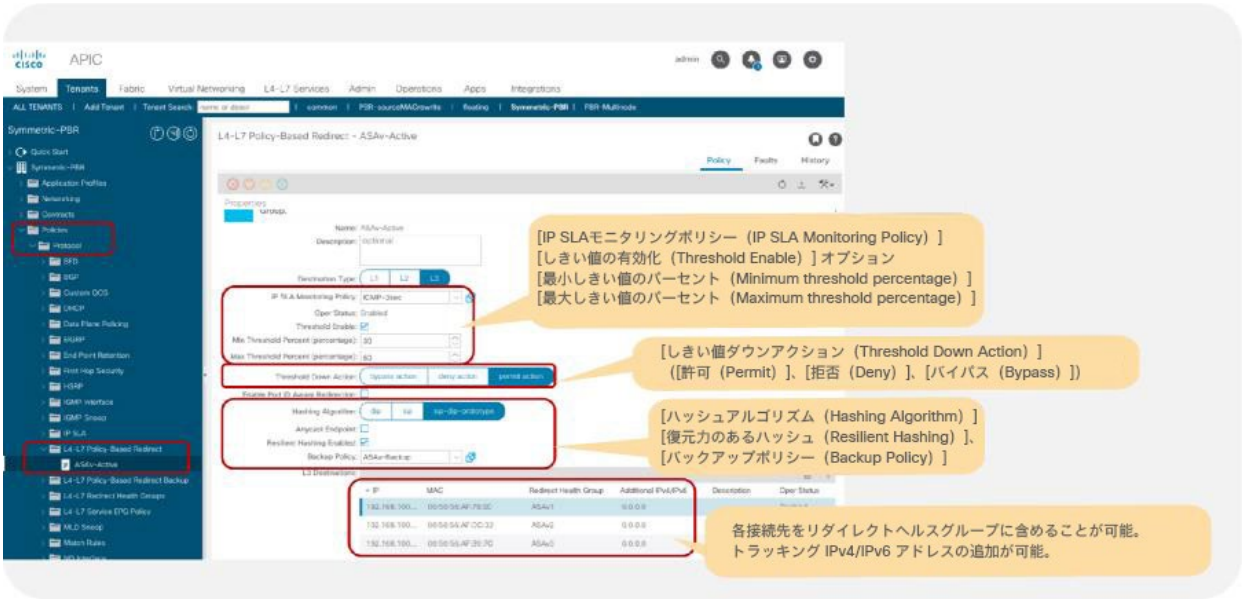


図 129.
L4-L7 PBR トラッキング、ヘルスグループ、ダウンアクション、しきい値の設定

設計上の考慮事項を次に示します。

- トラッキングを有効化するには、IP SLA モニタリングポリシーとヘルスグループを設定する必要があります。
- デフォルトでは、接続先で定義されている IP アドレス（プライマリ IP アドレス）が追跡されます。トラッキングする IPv4/IPv6 アドレスを追加することもできます。プライマリ IP アドレスと追加の IP アドレスの両方を設定すると、両方が稼働している場合に PBR ノードが稼働中としてマークされます。
- しきい値が有効化されておらず、PBR ポリシーにあるすべての PBR 接続先がダウンしている場合、トラフィックはドロップされます。
- しきい値が有効化されている場合は、ダウンアクションと、最小しきい値（割合）、最大しきい値（割合）を指定できます。サポートされているダウンアクションは、「許可」、「拒否」、「バイパス」です。デフォルトでは、ダウンアクションは 「許可」です。PBR ノードのコンシューマーコネクタとプロバイダーコネクタの両方で同じアクションを使用する必要があります。そうしないと、サービスグラフがレンダリングされてもテナントでエラーが発生します。
- トラッキングと復元力のあるハッシュが有効化されている場合は、バックアップポリシーを指定してバックアップ PBR 接続先を設定できます。

注： 同じ VRF に同じ PBR 接続先 IP を持つ複数の PBR ポリシーがあり、これらのポリシーのいずれかでトラッキングが有効化されいる場合は、同じ IP-SLA ポリシーを使用し、それらすべての IP に対して同じヘルスグループを使用する必要があります。これは、PBR 接続先が（VRF、IP）をトラッキングステータスのキーとして使用するためです。VRF 内の同じ PBR 接続先 IP を同時に稼働中とダウンの状態にすることはできません。たとえば、次の設定はサポートされていません。

- PBR ポリシー 1 では PBR 接続先 192.168.1.1 が VRF A にあり IP-SLA モニタリングポリシー 1（ICMP トラッキング）が設定されている。
- PBR ポリシー 2 では PBR 接続先 192.168.1.1 が VRF A にあり IP-SLA モニタリングポリシー 2（TCP トラッキング）が設定されている。

IP SLA モニタリングポリシー

IP SLA モニタリングポリシーを設定できます（図 130）。

場所は、[テナント（Tenant）] > [ネットワーク（Networking）] > [プロトコルポリシー（Protocol Policies）] > [IP SLAモニタリングポリシー（IP SLA Monitoring Policies）] です。デフォルトでは、この設定は L4-L7 PBR で使用されません。

SLA 頻度、SLA ポート、SLA タイプを指定できます。

次の SLA タイプがサポートされています。

- L3 PBR に対する TCP（APIC リリース 2.2(3j) 以降）
- L3 PBR に対する ICMP（APIC リリース 3.1 以降）
- L1/L2 PBR に対する L2Ping（APIC リリース 4.1 以降）
- L3 PBR に対する HTTP（APIC リリース 5.2 以降）

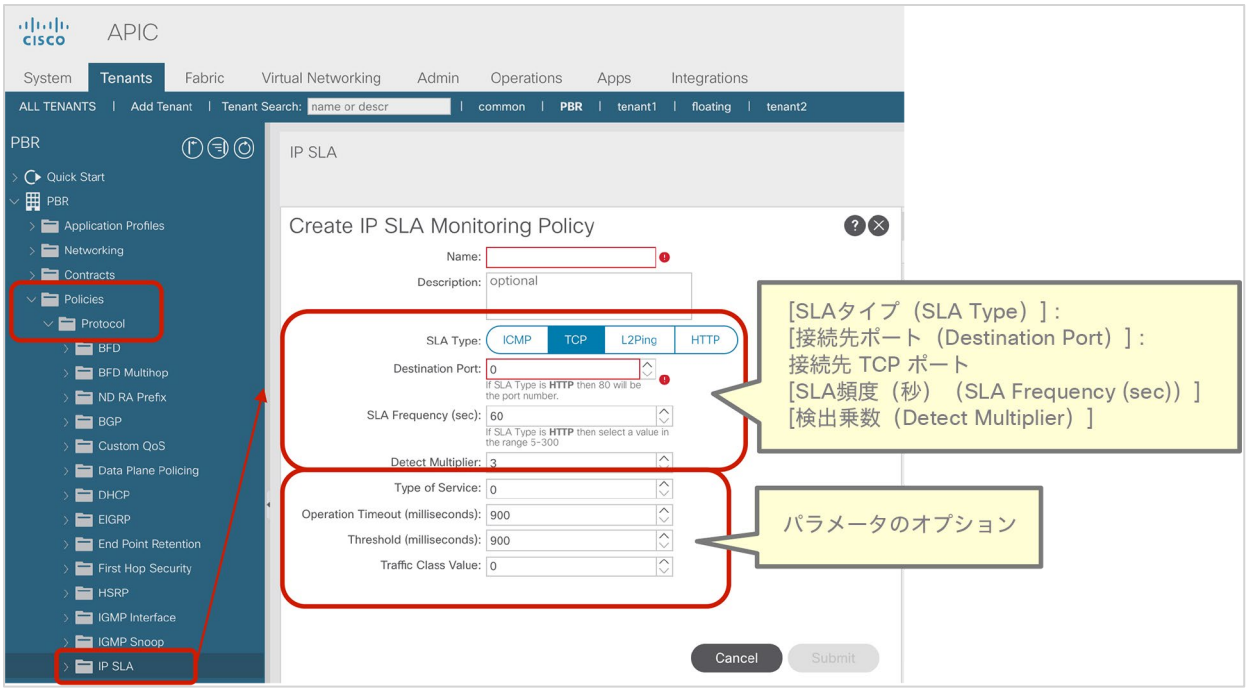


図 130.
IP SLA モニタリングポリシー

SLA 頻度の最小値は、HTTP トラッキングの場合は 5 秒、その他の SLA タイプの場合は 1 秒です。検出乗数はデフォルトで 3 ですが、APIC リリース 4.2 以降では GUI で設定できます。検出乗数の最小値は 1 です。たとえば、SLA 頻度が 1 秒で、検出乗数が 3 の場合、PBR ノードのプローブと障害検出は次のように動作します。

- 時刻 T0 の最初のプローブ：失敗
- 時刻 T0 + 1 秒の 2 回目のプローブ：失敗
- 時間 T0 + 2 秒の 3 回目のプローブ：失敗。このとき、接続先ダウンが報告されます。

APIC リリース 5.1(3) 以降では、次のパラメータオプションがサポートされています。

- ICMP、L2Ping、HTTP のリクエストデータサイズ（バイト）
- タイプオブサービス（ToS）
- 処理のタイムアウト（ミリ秒）
- しきい値（ミリ秒）
- トラフィッククラスの値

APIC リリース 5.2(1) 以降では、HTTP SLA タイプのサポートについて次の考慮事項があります。

- HTTP のみをサポート。HTTPS は未対応
- HTTP バージョン 1.0 および 1.1 のみをサポート
- 接続先ポートは 80 のみ

- SLA 頻度の最小値は 5 秒
- （URL ではなく）URI の設定が必要。ドメイン名解決は未対応。「/」で始まる URI を入力。空白は不可

図 131.
IP SLA モニタリングポリシー（HTTP）

ヘルスグループ

ヘルスグループを設定できます（図 132）。

場所は、[テナント（Tenant）] > [ポリシー（Policies）] > [プロトコル（Protocol）] > [L4-L7リダイレクトヘルスグループ（L4-L7 Redirect Health Groups）] です。デフォルトでは、この設定は L4-L7 PBR で使用されません。

ここでヘルスグループを作成します。L4-L7 PBR では、PBR 接続先の IP アドレスごとにヘルスグループを選択するため、コンシューマー側のアドレスとプロバイダー側のアドレスをグループ化できます。

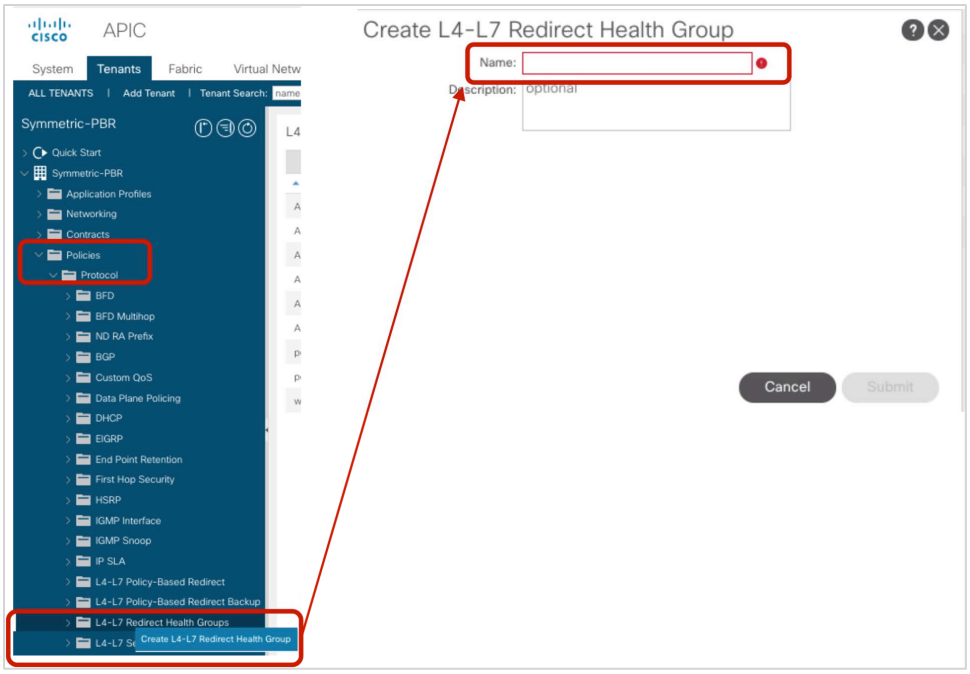
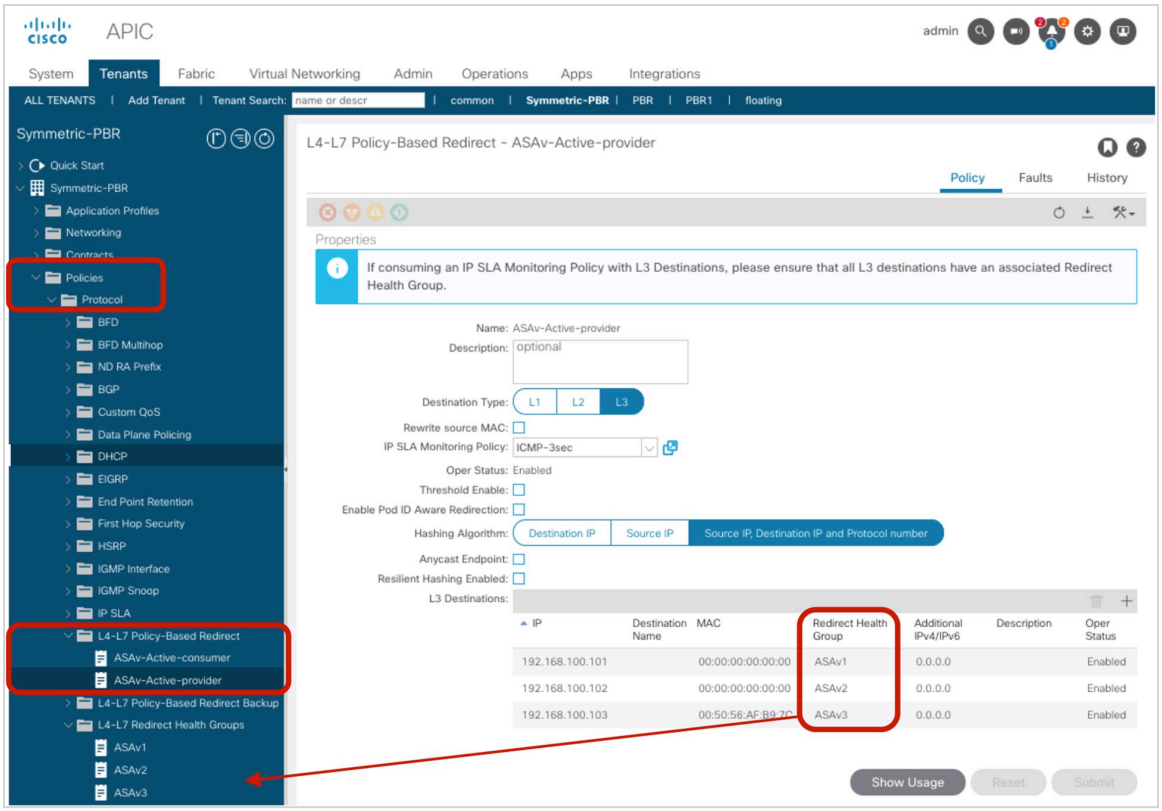


図 132.
リダイレクトヘルスグループ

この例では、3 つのヘルスグループが作成されています（表 19 および図 133）。

表 19. ヘルスグループ

プロバイダー側	コンシューマー側	ヘルスグループ
192.168.100.101	192.168.101.101	ASAv1
192.168.100.102	192.168.101.102	ASAv2
192.168.100.103	192.168.101.103	ASAv3



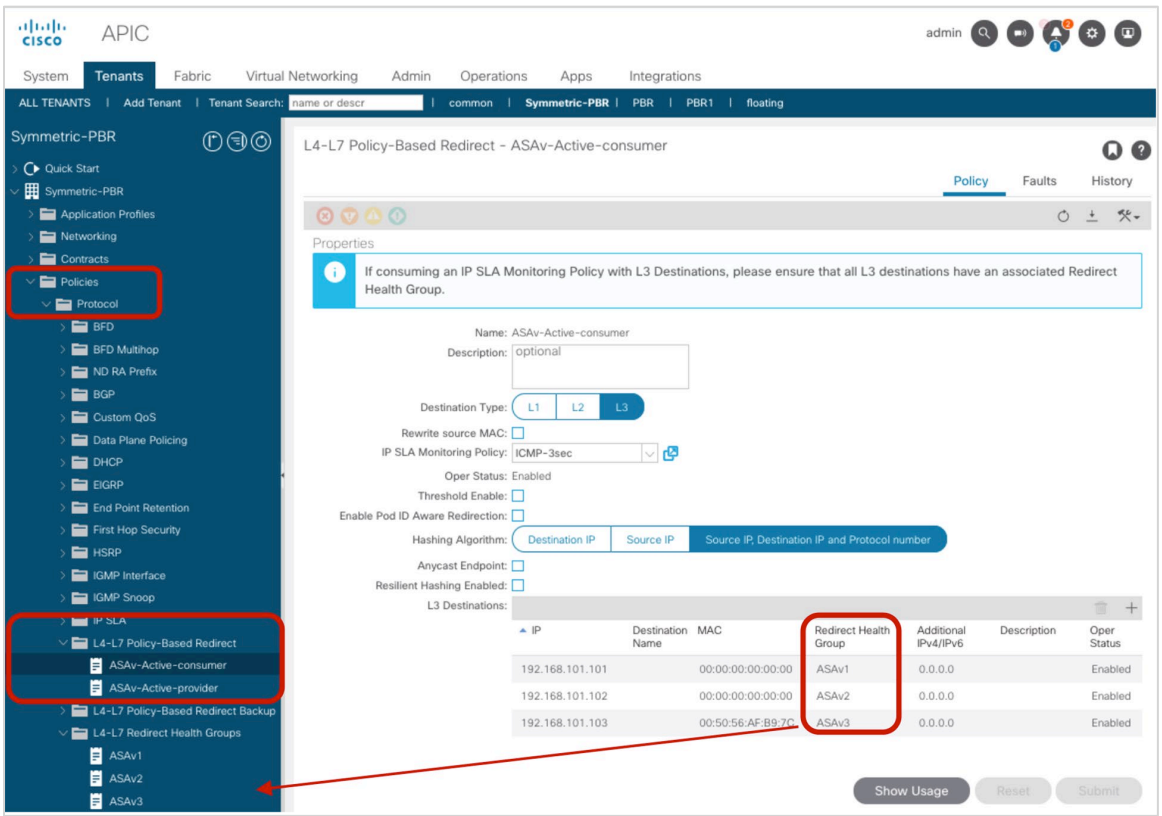


図 133.
リダイレクトヘルスグループに宛先 IP アドレスを追加

復元力のあるハッシュの設定

復元力のあるハッシュのオプションを有効化または無効化できます（図 134）。場所は、[テナント（Tenant）] > [ポリシー（Policies）] > [プロトコル（Protocol）] > [L4-L7ポリシーベースリダイレクト（L4-L7 Policy Based Redirect）] です。

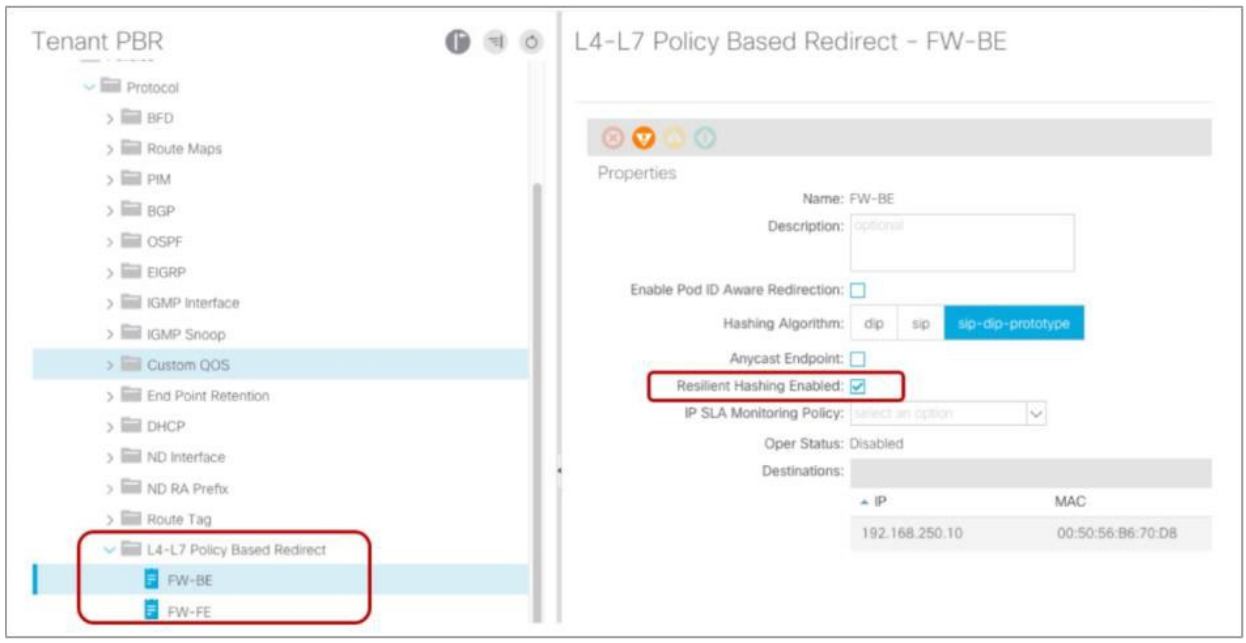


図 134.
L4-L7 PBR 復元力のあるハッシュのオプション

バックアップ PBR ポリシー

バックアップ PBR ポリシーを設定できます（図 135）。

場所は、[テナント（Tenant）] > [ポリシー（Policies）] > [プロトコル（Protocol）] > [L4-L7ポリシーベースリダイレクトのバックアップ（L4-L7 Policy Based Redirect Backup）] です。

ここでバックアップ PBR ポリシーを作成します。[L4-L7ポリシーベースリダイレクトのバックアップ（L4-L7 Policy Based Redirect Backup）] で、バックアップ PBR ポリシーを選択して、バックアップ PBR の接続先を設定します。デフォルトでは、この設定は L4-L7 PBR で使用されません。つまり、バックアップ PBR 接続先はありません。

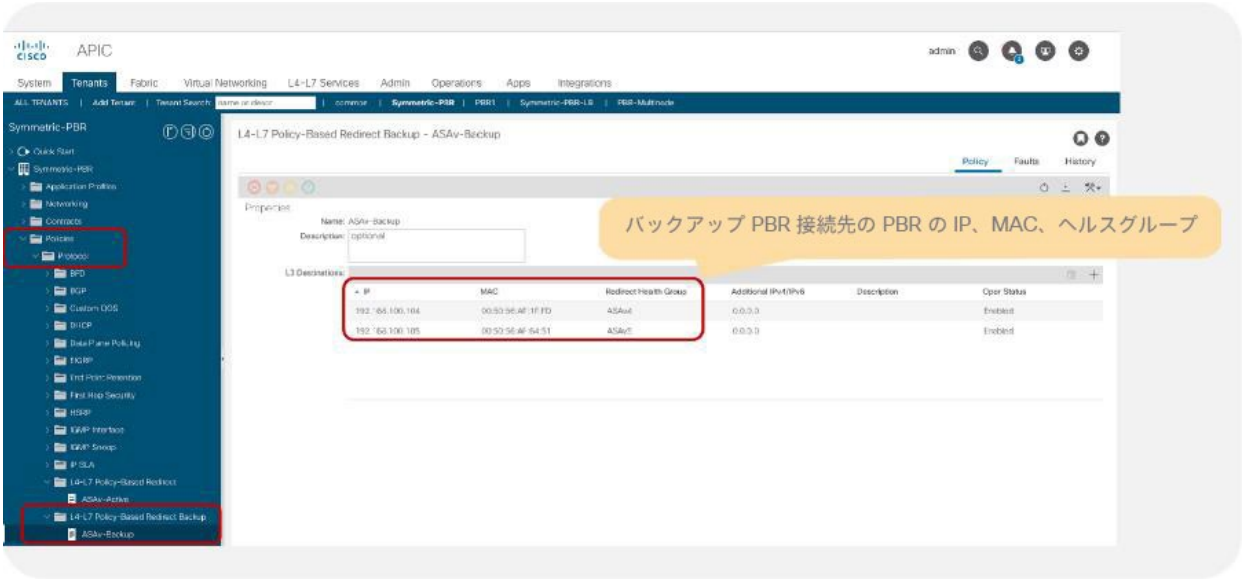


図 135.
バックアップ PBR ポリシー

PBR ポリシーと同様に、バックアップ PBR 接続先の IP、MAC、ヘルスグループ、トラッキング用の追加の IPv4 または IPv6 アドレスを指定できますが、IP SLA モニタリングポリシーやしきい値など、PBR ポリシーごとのその他の設定は指定できません。バックアップ PBR ポリシーは、PBR ポリシーのプライマリ PBR 接続先に関する設定と同じ設定を使用します。

図 136 に CLI 出力例を示します。192.168.100.101、192.168.100.102、192.168.100.103 は PBR ポリシーで設定されたプライマリ PBR 接続先であり、192.168.100.104、192.168.100.105 はバックアップ PBR ポリシーで設定されたバックアップ PBR 接続先です。

図 136.
コンシューマーリーフノードとプロバイダーリーフノードでのトラッキングとバックアップステータス（すべての PBR 接続先が稼働中）

プライマリ PBR 接続先の 1 つがダウンした場合、192.168.100.104 が使用されます。

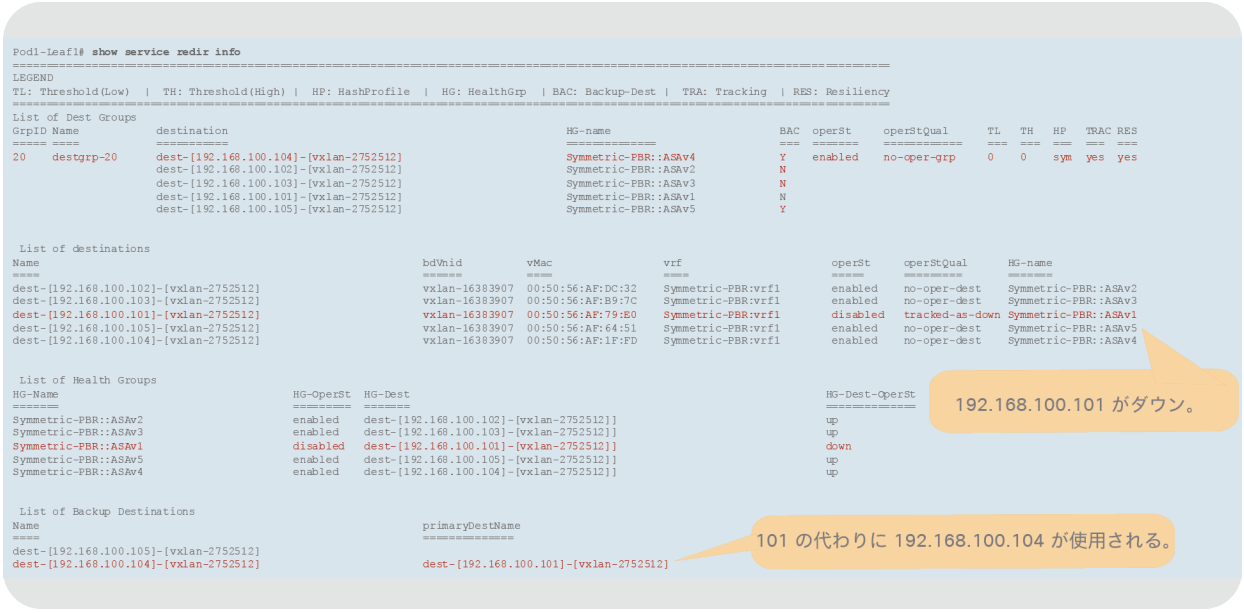


図 137.
コンシューマーリーフノードとプロバイダーリーフノードでのトラッキングとバックアップステータス（192.168.100.101 がダウン）

注： 使用可能なバックアップ PBR 接続先が複数ある場合は、そのうちの 1 つが、IP アドレスの小さいものから順に使用されます。したがって、この例では 192.168.100.105 ではなく 192.168.100.104 が使用されます。

さらにもう 1 つの PBR 接続先がダウンした場合は、192.168.100.105 が使用されます。

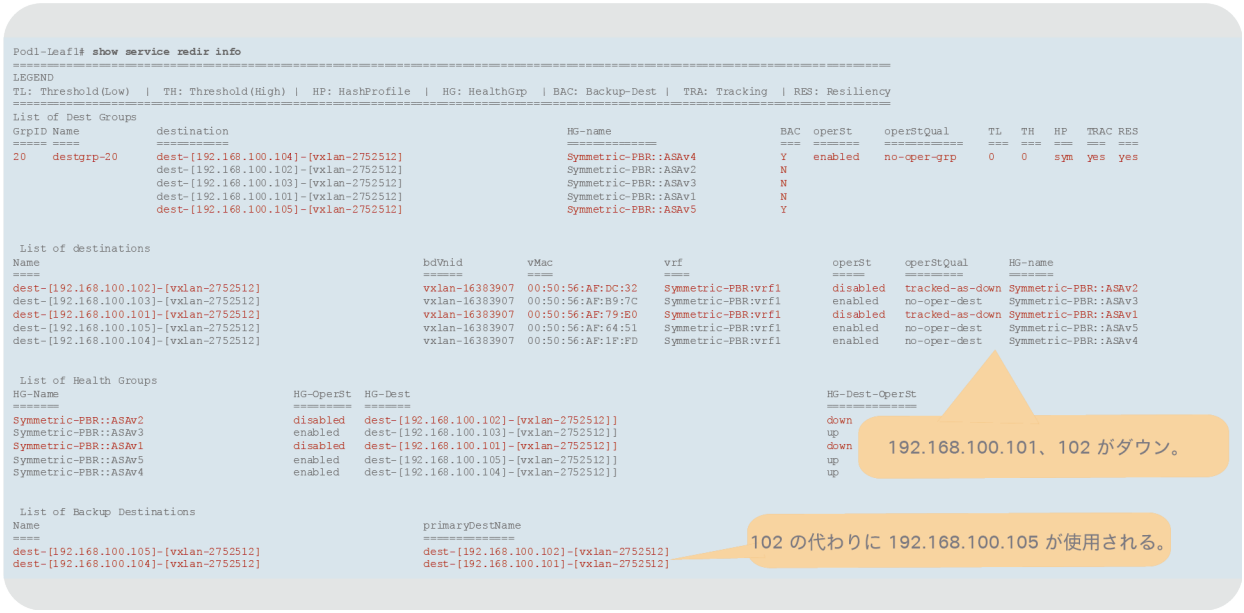


図 138.
コンシューマーリーフノードとプロバイダーリーフノードでのトラッキングとバックアップステータス（192.168.100.101 と 192.168.100.102 がダウン）

送信元 MAC の書き換え設定

図 139 に示すように、送信元 MAC の書き換え機能を有効化または無効化できます。場所は、[テナント（Tenant）] > [ポリシー（Policies）] > [プロトコル（Protocol）] > [L4-L7ポリシーベースリダイレクト（L4-L7 Policy Based Redirect）] です。デフォルトでは、[送信元MACの書き換え（Rewrite source MAC）] は無効化されています。

注： [送信元MACの書き換え（Rewrite source MAC）] が有効化されている場合、サービス BD の MAC アドレスはデフォルトの 00:22:bd:f8:19:ff にする必要があります。管理者がサービス BD に別の MAC を設定すると、サービスグラフのレンダリングが失敗し、展開されたグラフインスタンスにエラーが表示されます。

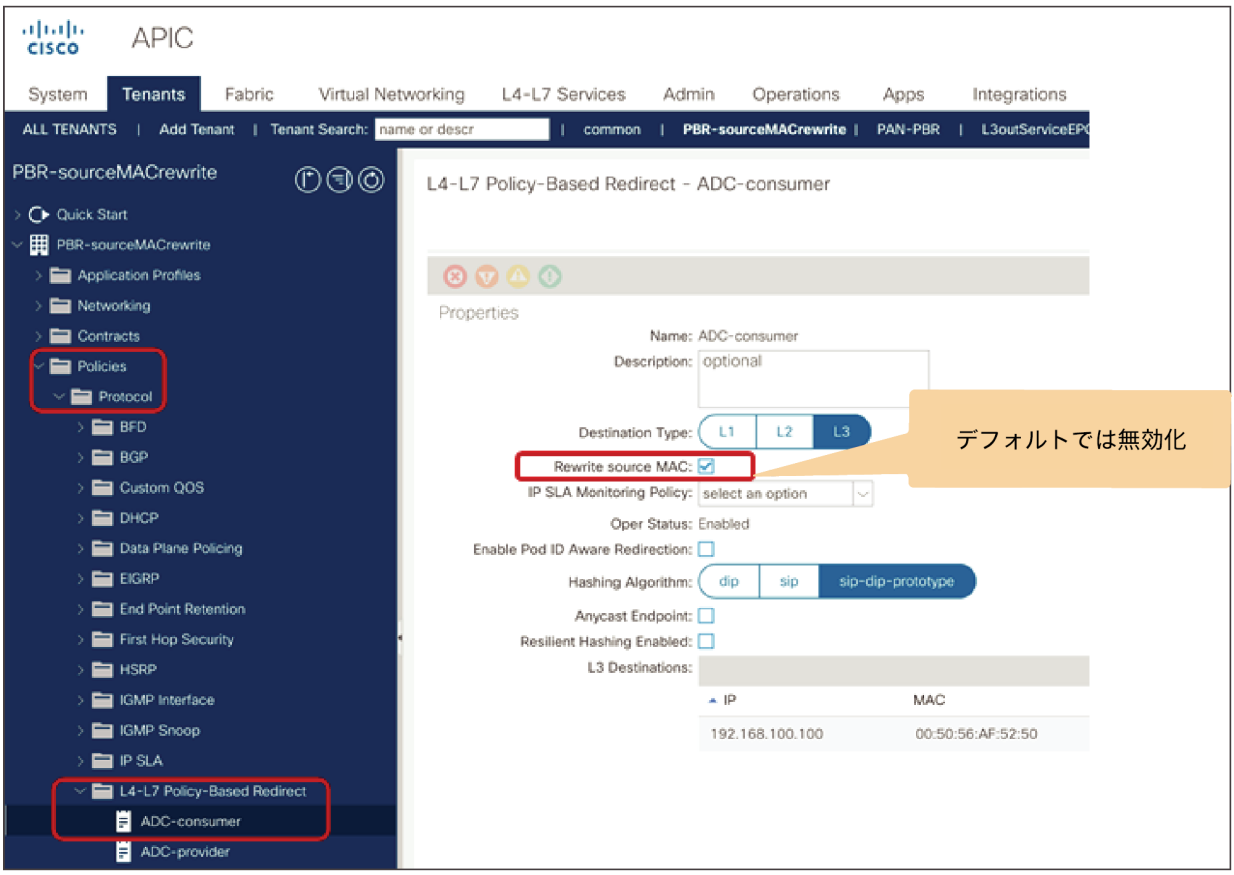


図 139.
L4-L7 PBR 送信元 MAC の書き換え設定

接続先名

図 140 に示すように [接続先名（Destination Name）] を設定することで、対称 PBR で IP ベースのソートの代わりに接続名ベースのソートを使用できます。場所は、[テナント（Tenant）] > [ポリシー（Policies）] > [プロトコル（Protocol）] > [L4-L7ポリシーベースリダイレクト（L4-L7 Policy Based Redirect）] です。デフォルトでは、接続先名ベースのソートは無効化されていて、IP ベースのソートが使用されます。L1/L2 対称 PBR の場合は、常に接続先名ベースのソートになります。

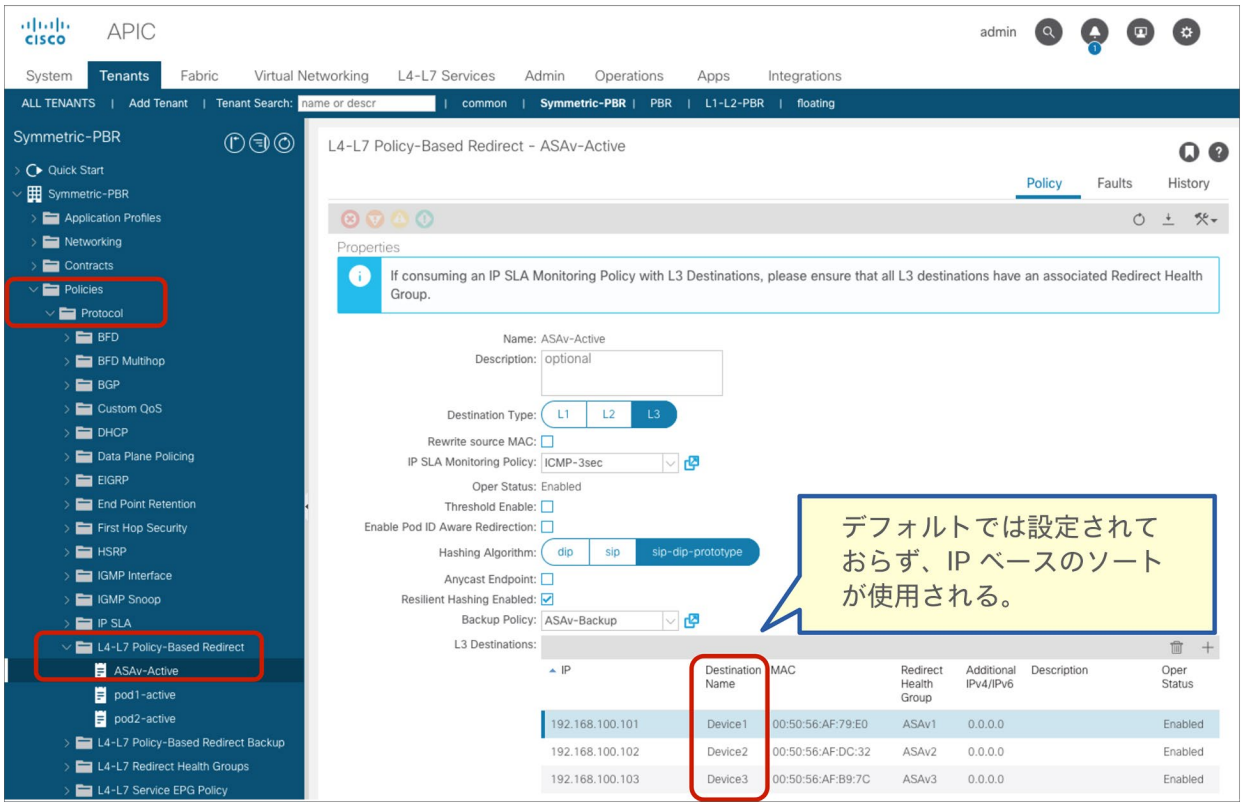


図 140.
接続先名の設定

注： 接続先名が設定されている場合、IP ベースのソートではなく、接続先名ベースのソートが使用されます。PBR ポリシーに、接続先名が設定されている PBR 接続先と接続先名がない PBR 接続先が混在している場合、サービスグラフのレンダリングが失敗します。バックアップ PBR ポリシーが設定されている場合は、バックアップ PBR ポリシーの PBR 接続先にも接続先名を設定する必要があります。

ロケーションベースの PBR

PBR ポリシーごとにロケーションベースの PBR を有効化できます（図 141）。場所は、[テナント（Tenant）] > [ポリシー（Policies）] > [プロトコル（Protocol）] > [L4-L7ポリシーベースリダイレクト（L4-L7 Policy Based Redirect）] です。この設定はデフォルトでは有効化されていません。

PBR 接続先ごとにポッド ID を設定する必要があります。[ポッドID認識リダイレクトを有効化（Enable Pod ID Aware Redirect）] をオンにすると設定できます。

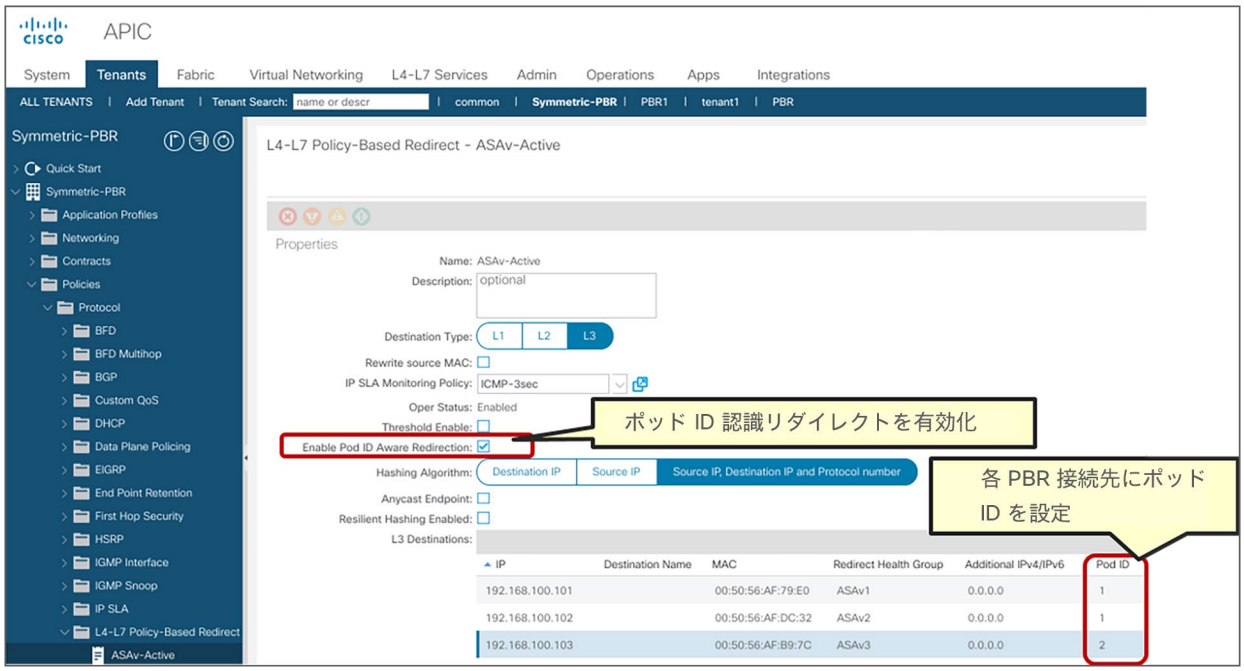


図 141.
ポッド ID 認識リダイレクトの有効化

注： 複数の PBR ポリシーが同じ VRF に同じ PBR 接続先 IP を持つ場合、すべてのポリシーでポッド ID 認識リダイレクトを有効化するか、ポッド ID 認識リダイレクトを無効化する必要があります。同じ（VRF、IP）ペアをポッド ID 認識リダイレクトが有効化されたポリシーとポッド ID 認識リダイレクトが無効化されたポリシーで同時に使用することはできません。たとえば、次の設定はサポートされていません。

- PBR ポリシー 1 では PBR 接続先 192.168.1.1 が VRF A にあり、ポッド ID 認識リダイレクトが有効化されている。
- PBR ポリシー 2 では PBR 接続先 192.168.1.1 が VRF A にあり、ポッド ID 認識リダイレクトが無効化されている。

L1/L2 PBR

APIC リリース 4.1 以降では、L1 または L2 モードで動作する L4-L7 サービスデバイスで PBR が使用できます。PBR は現在、インライン IPS、トランスペアレント ファイアウォール（FW）などに対応しています。このセクションでは、L1/L2 PBR の動作と L1/L2 PBR の設定について説明します。いくつかの設計とトラフィックフローが考えられるため、この説明で使用されている例は実際の環境を正確に反映していない場合があります。

概要

サービスデバイス展開モードに関する用語はベンダーによってさまざまですが、ここでは以下の用語と定義を使用します。

- L1 デバイス
  - サービスデバイスで VLAN 変換は行われません。
  - 両方のサービスデバイス インターフェイスが同じ VLAN を使用します。
  - 通常、インラインモードまたはワイヤモードと呼ばれます。
  - 通常、ファイアウォールおよび IPS に使用されます。ただし、サービスデバイスが L2 転送または L3 転送に関与しないセキュリティ機能を実行することを想定している場合に限ります。
- L2 デバイス
  - サービスデバイスでブリッジングが行われます（接続先 MAC のルックアップが発生する場合があります）。
  - サービスデバイスで VLAN 変換が行われます。
  - 両方のサービスデバイス インターフェイスが異なる VLAN を使用します。
  - 通常、トランスペアレントモードまたはブリッジモードと呼ばれます。
  - 通常、ファイアウォールと IPS に使用されます。
- L3 デバイス
  - サービスデバイスでルーティングが行われます（接続先 IP のルックアップが発生します）。
  - 両方のサービスデバイス インターフェイスが異なる VLAN を使用します。
  - 通常、ルーテッドモードと呼ばれます。
  - 通常、ファイアウォールとロードバランサに使用されます。

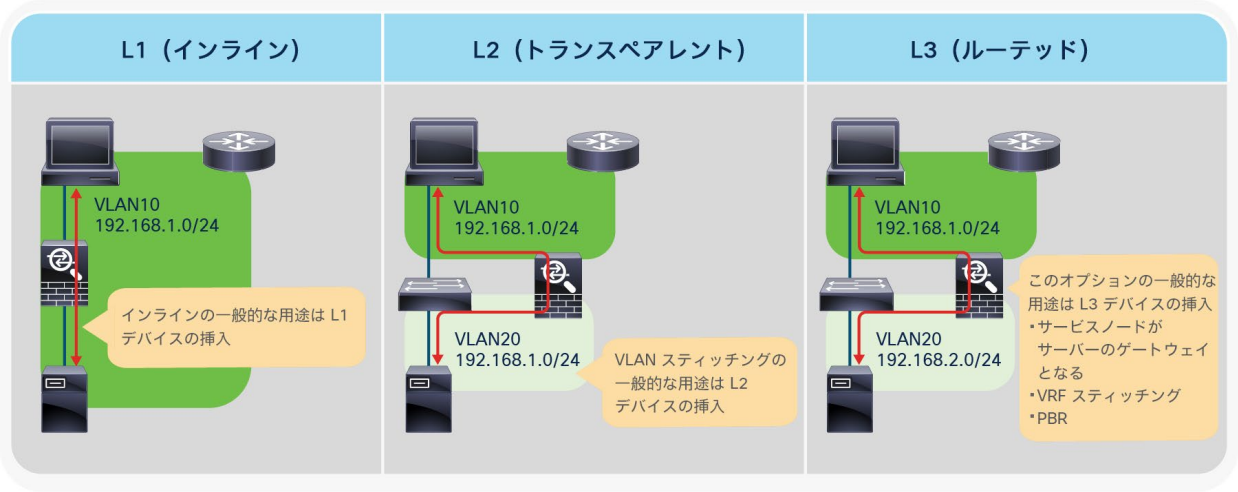


図 142.
サービスデバイス展開モードの比較

表 20. サポートされる展開モード

サービスデバイス	L3（ルーテッドモード）	L2（トランスペアレントモード）	L1（インラインモード）
Cisco 適応型セキュリティアプライアンス（ASA）	あり	あり	なし
Cisco Firepower NGFW	あり	あり	あり（インラインペア）
Fortinet 次世代ファイアウォール	あり	あり	あり（仮想ワイヤペア）
Palo Alto Networks 次世代ファイアウォール	あり	あり	あり（vWire モード）

L1/L2 デバイスを挿入する一般的な設計では、L1/L2 デバイスが常にトラフィックパスの一部になるため、VLAN を通過するすべてのトラフィックが L1/L2 デバイスを通過する必要があります。ACI で L1/L2 PBR を使用することで、コントラクトフィルタに基づいてトラフィックを選択的にリダイレクトできます。これは、L3 PBR を使用する場合と同じメリットです。

L1/L2 PBR の動作

Cisco ACI 転送の観点からは、L3 PBR と L1/L2 PBR の間に大きな違いはありません。トラフィックは、L1/L2 デバイスインターフェイスに接続されたリーフインターフェイスでプログラムされた静的 MAC エンドポイントである PBR 接続先 MAC にリダイレクトされます。したがって、L1/L2 デバイスに接続されたリーフインターフェイスにトラフィックをリダイレクトできます。

図 143 に、クライアント EPG がコンシューマー EPG、Web EPG がプロバイダー EPG で、両者間に L1/L2 PBR サービスグラフを持つコントラクトが設定されている例を示します。リーフ 2 の Eth1/1 に接続されているかのようにエンドポイント MAC-A がプログラムされます。また、リーフ 3 の Eth1/1 に接続されているかのようにエンドポイント MAC-B がプログラムされます。

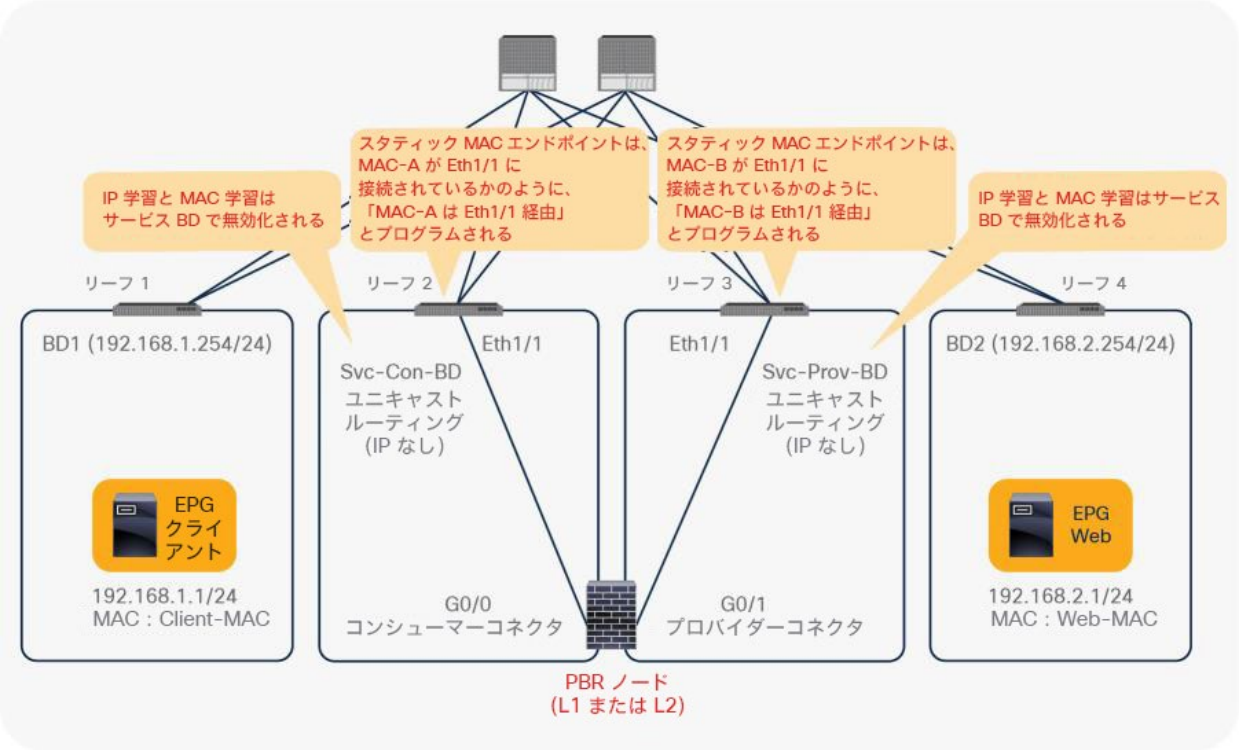


図 143.
L1/L2 PBR トポロジの例

注： デフォルトでは、L1/L2 PBR の MAC-A と MAC-B は、APIC によって自動的に生成されます（設定で変更可能）。L1/L2 PBR デバイスの BD は、サービスグラフによって自動的に作成されません。事前に作成する必要があります。設定に関する考慮事項は次のとおりです。

- IP ルーティングを有効化する必要があります（ただし、BD サブネットは必要ありません）。
- データプレーン IP 学習は自動的に無効化されます。これは L3 PBR の場合と同様です

クライアントエンドポイントが、Web エンドポイントを接続先とするトラフィックを生成します。リーフ 1 が接続先エンドポイントをすでに学習している場合、リーフ 1 が送信元と接続先の EPG のクラス ID を解決できるため、リーフ 1 で PBR が実行されます。ここで、接続先 MAC アドレスが静的 MAC であるエンドポイント MAC-A に書き換えられます。その結果、トラフィックが PBR デバイスのコンシューマーコネクタにリダイレクトされます。PBR 接続先へのリダイレクトトラフィックは、常に L2 スパインプロキシに送信された後、PBR デバイスに転送されます。L3 PBR と同様に、リーフ 2 はこのトラフィックからクライアントの IP アドレスを学習しません。これは、PBR ノードブリッジドメインのエンドポイント データプレーン学習が無効化されているためです。

注： 接続先 MAC アドレスは書き換えられますが、デフォルトでは送信元 MAC アドレスが保持されます。したがって、PBR ノードは、送信元エンドポイントの送信元 MAC アドレスを持つトラフィックを受信します。ただし、その送信元 MAC がリダイレクトされたトラフィックの接続先 MAC アドレスになることはありません。したがって、PBR ノードで MAC アドレス学習を無効化することをお勧めします。トラッキングが有効化されている場合は、無効化する必要があります。「トラッキングを使用したアクティブ/スタンバイ設計」セクションも参照してください。

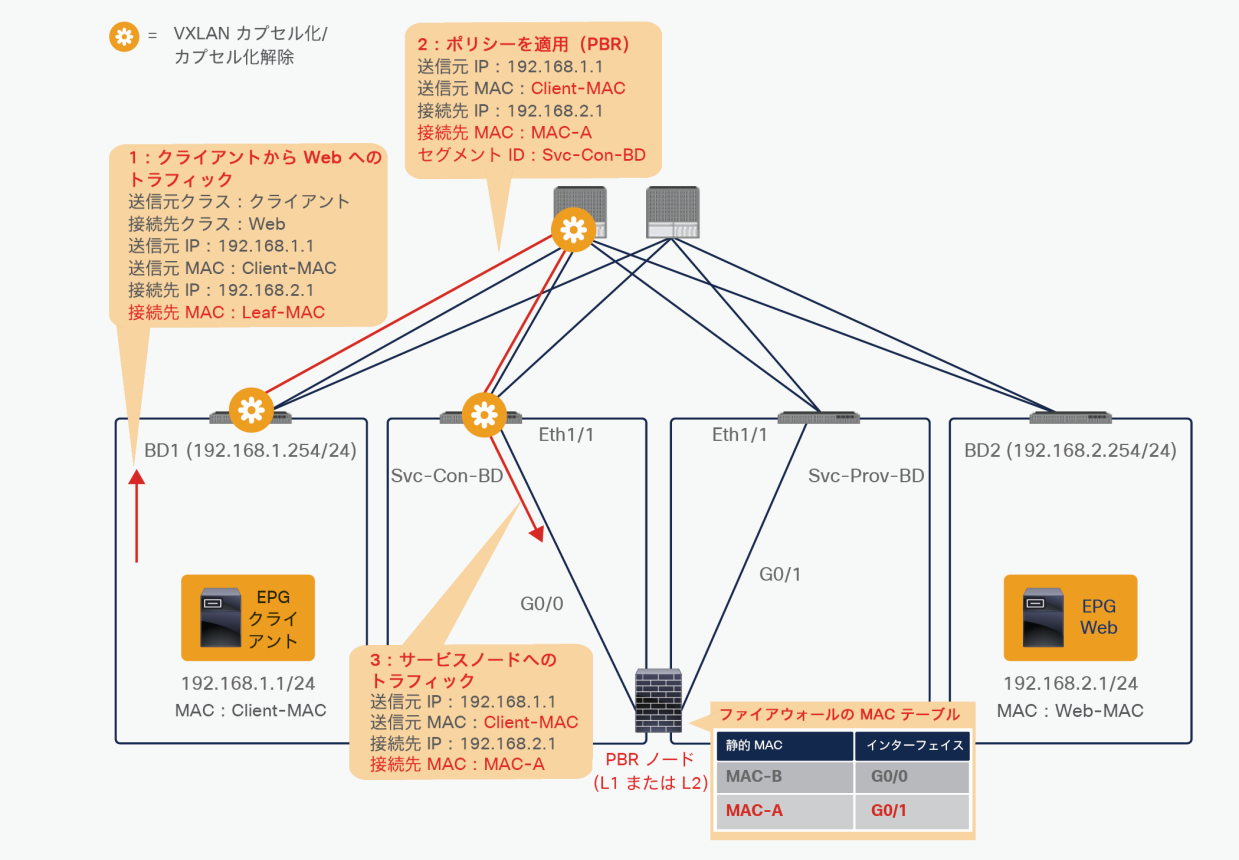


図 144.
パケットフローの例（クライアントから Web へのトラフィックを PBR ノードにリダイレクト）

その後、トラフィックは PBR ノードを通過し、Cisco ACI ファブリックに戻ります。

注： PBR デバイスが MAC アドレステーブルに基づいてトラフィックをブリッジングする場合、接続先 MAC のルックアップを実行するため、PBR デバイスに、Cisco ACI ファブリックにトラフィックを戻すための MAC アドレステーブルエントリが必要です。たとえば、Cisco ASA トランスペアレントモード ファイアウォール（L2 デバイス）は、接続先 MAC のルックアップを実行します。したがって、「MAC-A は G0/1 経由」という MAC アドレステーブルエントリが必要です。この例では G0/1 はリーフ 3 の Eth1/1 に接続されています。

PBR ノードブリッジドメインには BD サブネットがありませんが、トラフィックはリーフ 3 でルーティングできます。リーフ 3 は接続先エンドポイント（Web EPG の 192.168.2.1）を認識していないため、トラフィックは再度 L2 スパインプロキシに送信され、その後リーフ 4 に送信されます。ここで、送信元 EPG は PBR ノードのプロバイダーコネクタのクラス ID であり、接続先はプロバイダー EPG のクラス ID です。このトラフィックは許可されているため、Web エンドポイントに到達します。ここで重要な点は、リーフ 4 がこのトラフィックからクライアントの IP アドレスを学習しないことです。PBR ノードブリッジドメインのエンドポイント データプレーン学習が無効化されているためです（図 145）。

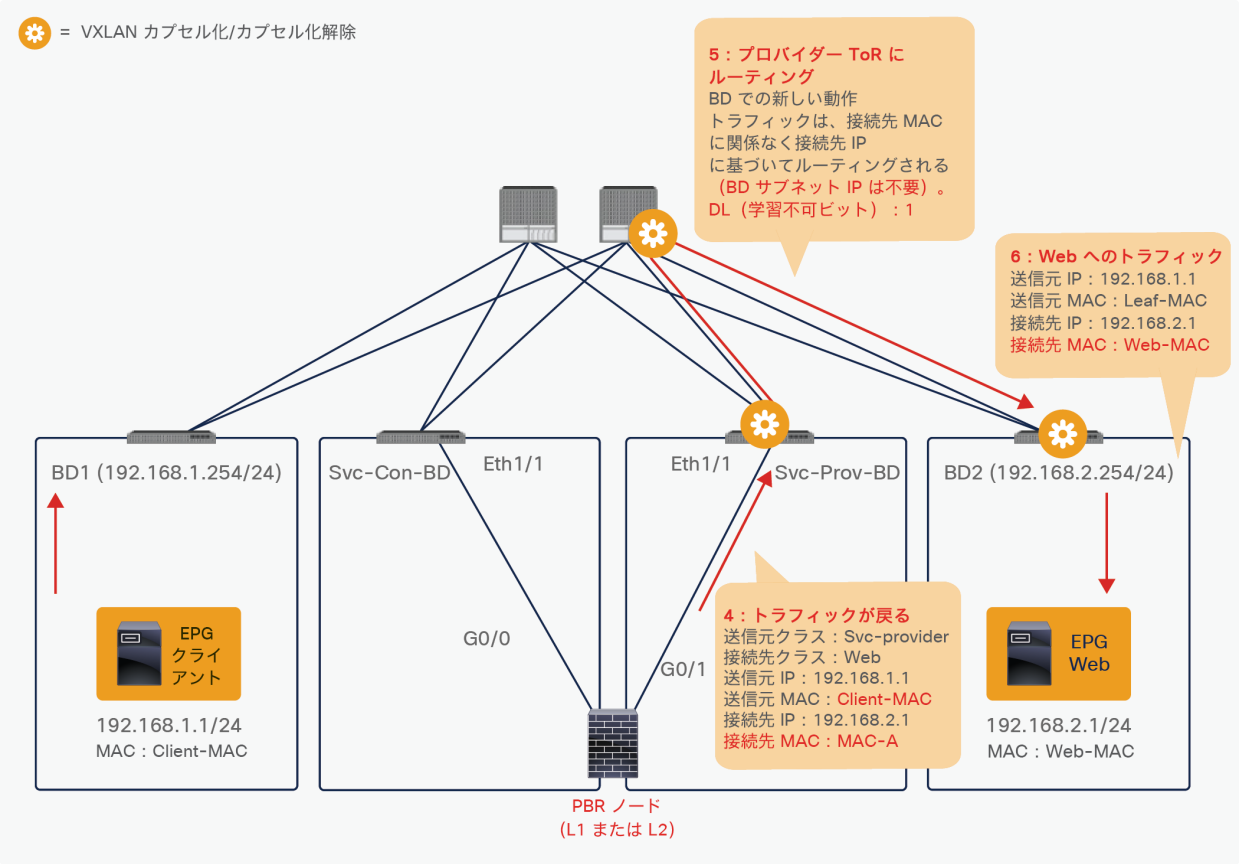


図 145.
パケットフローの例（PBR ノードから Web）

リターントラフィックの場合、PBR が実行されると、接続先 MAC アドレスが静的 MAC であるエンドポイント MAC-B に書き換えられ、トラフィックが PBR ノードのプロバイダー側に送信されます（図 146）。

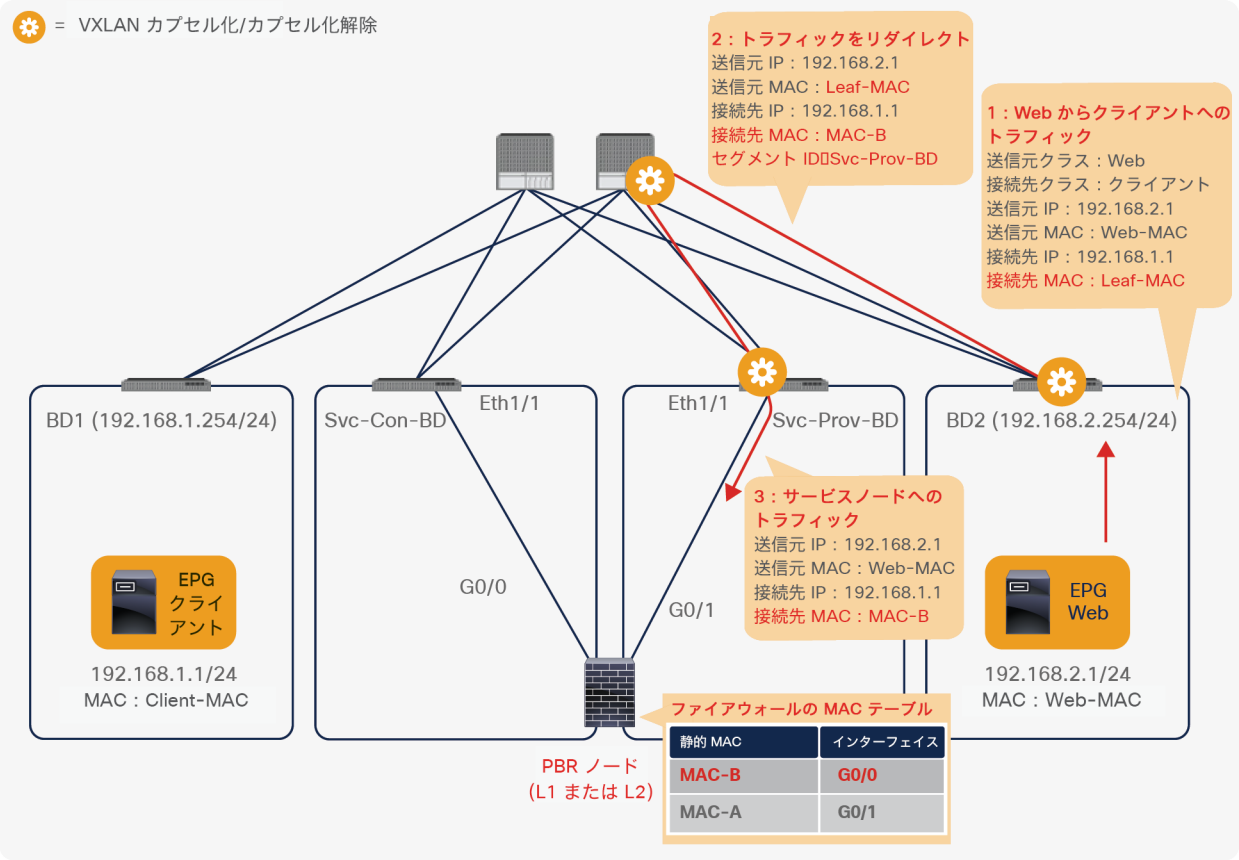


図 146.
エンドツーエンドのパケットフローの例（Web からクライアントへのトラフィックを PBR ノードにリダイレクト）

トラフィックは、PBR ノードのコンシューマー側から Cisco ACI ファブリックに戻ります。コンシューマーからプロバイダーへのトラフィックと同様に、リーフ 2 がルーティングを行います。リーフ 2 は接続先エンドポイントを認識していないため、トラフィックは再度 L2 スパインプロキシに送信され、その後リーフ 1 に送信されます。リーフ 1 はこのトラフィックから Web エンドポイントの IP アドレスを学習しません。PBR ノードブリッジドメインのエンドポイント データプレーン学習が無効化されているためです（図 147）。

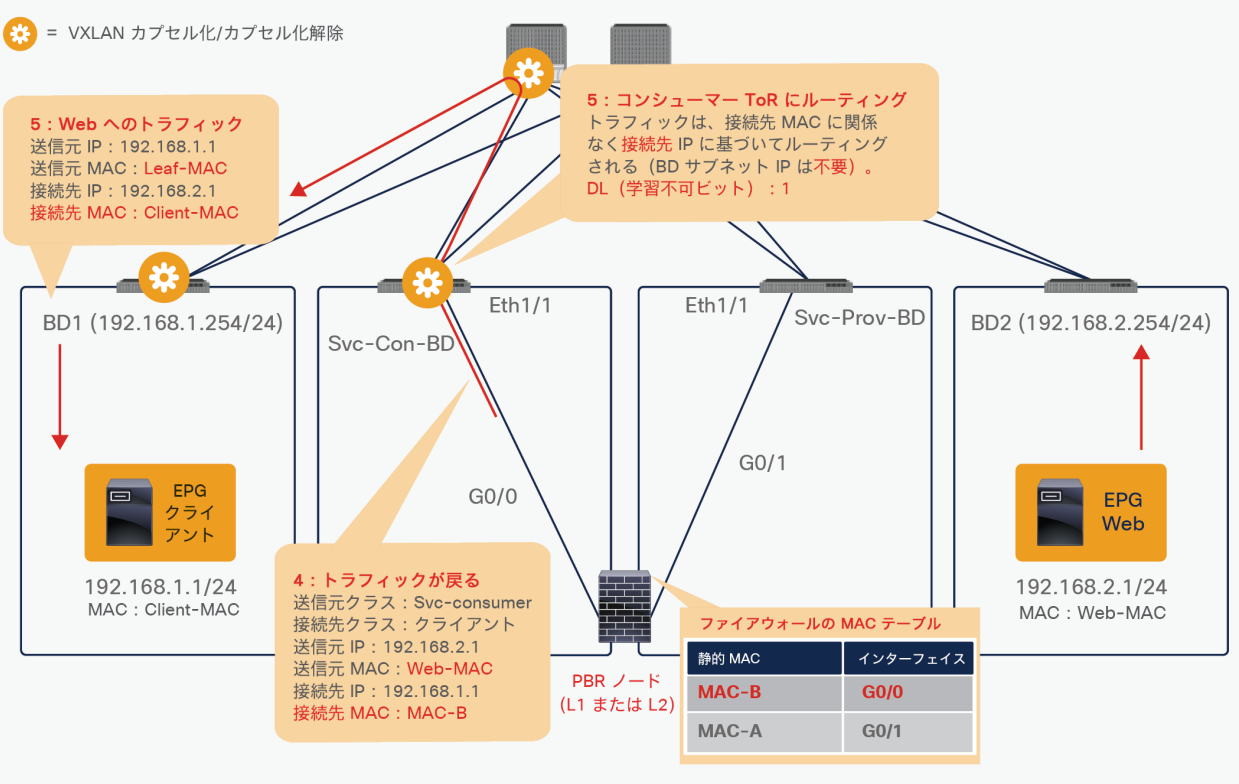


図 147.
エンドツーエンドのパケットフローの例（PBR ノードからクライアント）

注： リーフノードでルーティングされるため、TTL が減少します。

この例では、コンシューマー EPG とプロバイダー EPG が異なる BD に存在しますが、同じブリッジドメインや同じブリッジドメインサブネットに存在する場合もあります。コンシューマー EPG とプロバイダー EPG の BD 設計に関係なく、L1/L2 サービスデバイスを挿入できます。この柔軟性は、Cisco ACI の L1/L2 PBR が持つメリットの 1 つです。

トラッキングを使用したアクティブ/スタンバイ設計

APIC リリース 5.0 より前のリリースでは、対称 PBR のアクティブ/アクティブ設計を L1/L2 PBR に適用することはできません。APIC リリース 4.1 および 4.2 では、トラッキングを使用したアクティブ/スタンバイ設計がサポートされています。このセクションでは、トラッキングを使用した L1/L2 PBR のアクティブ/スタンバイ設計の動作について説明します。

L3 PBR ノードでのトラッキングと同様に、PBR ノードが接続されているサービスリーフノードがキープアライブメッセージを定期的に送信し、他のすべてのリーフスイッチに可用性情報をアナウンスします。L3 PBR トラッキングと L1/2 PBR トラッキングの違いは、L1/2 PBR トラッキングではリーフスイッチ間で L2 Ping が使用されることです。

図 148 に例を示します。L2 Ping の送信元 MAC アドレスと接続先 MAC アドレスは、PBR 接続先 MAC です。PBR ノードが稼働してトラフィックを伝送している場合、L2 Ping は正常に Cisco ACI ファブリックに戻ることになります。Cisco ACI ファブリックは、PBR 接続先が使用可能であると解釈します。

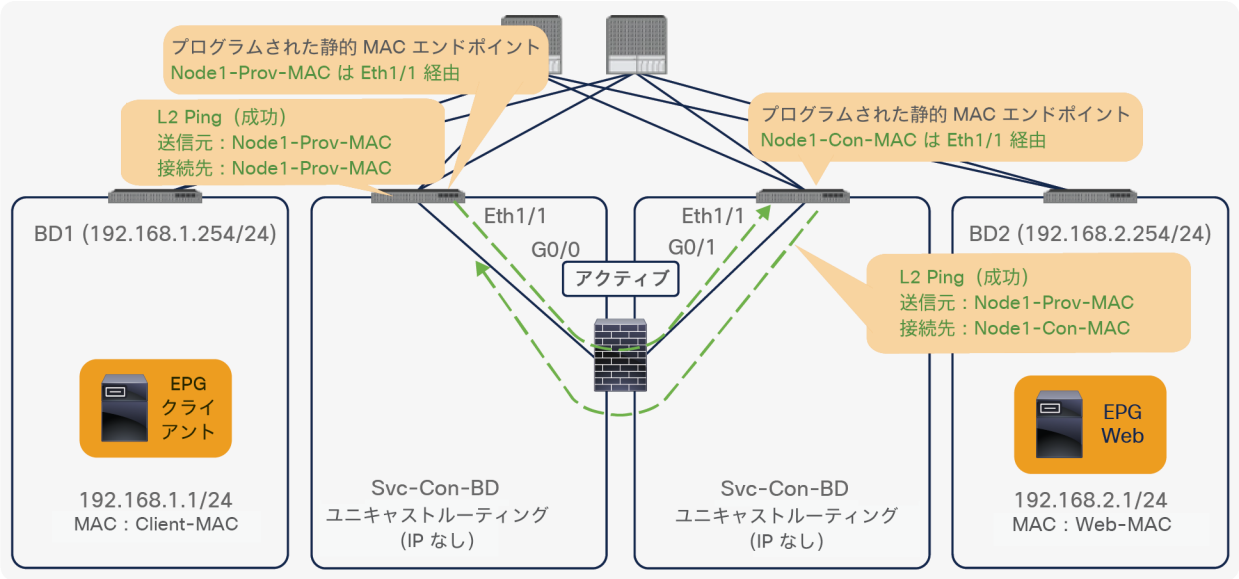


図 148.
リーフスイッチ間の L2 Ping

注： PBR ノードで MAC アドレス学習を無効化する必要があります。そうしないと、L2 Ping が PBR ノードで MAC アドレスフラッピングを引き起こす可能性があります。L2 Ping の送信元 MAC アドレスがコンシューマーコネクタとプロバイダーコネクタへ送られるキープアライブメッセージの送信元 MAC アドレスと同じであり、PBR ノードが異なるインターフェイスから同一の送信元 MAC を受け取るためです。

アクティブ/スタンバイ高可用性の L1/L2 サービスノードがあり、L1/2 PBR を使用してこれを挿入したいとします。2 つの PBR 接続先があり、トラッキングを有効化しています。スタンバイデバイスはトラフィックを転送しないため、パスのうちアクティブノードに接続されている 1 つのパスだけが稼働します。したがってトラフィックは、アクティブノードに接続されているインターフェイス（この例では Eth1/1）にリダイレクトされます。

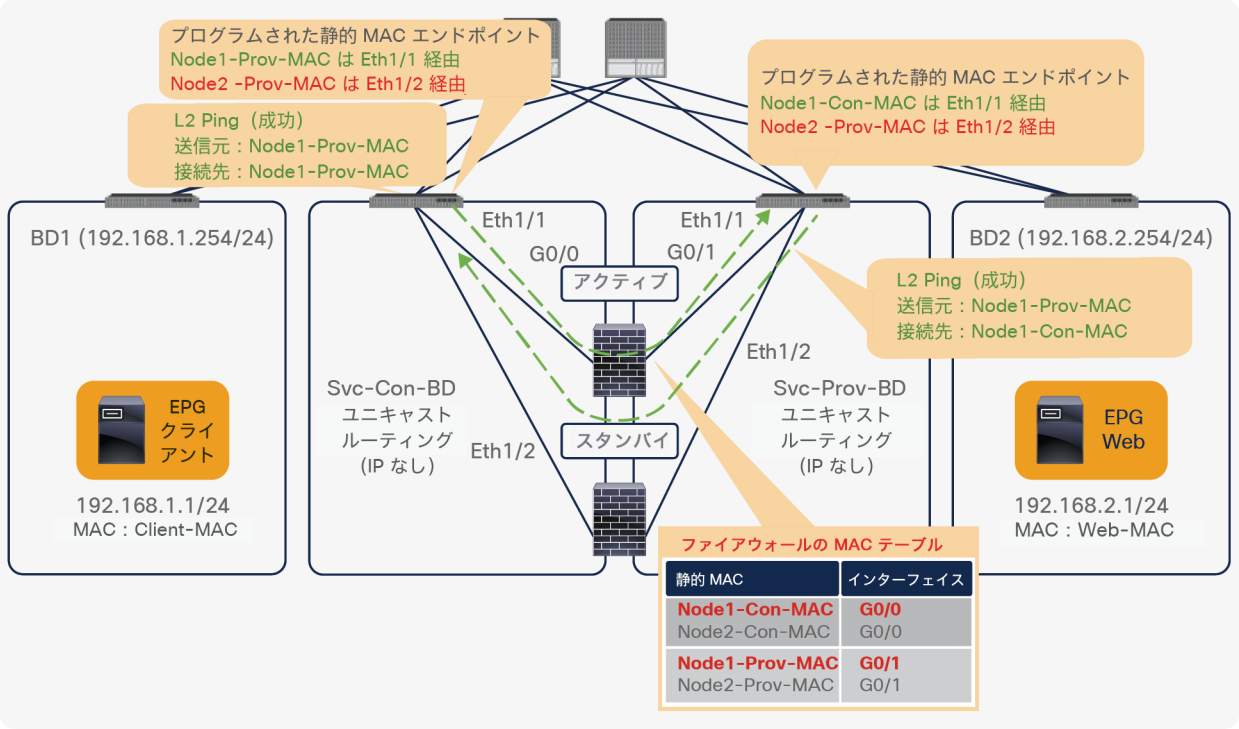


図 149.
アクティブデバイスを使用した L2 Ping パスが成功

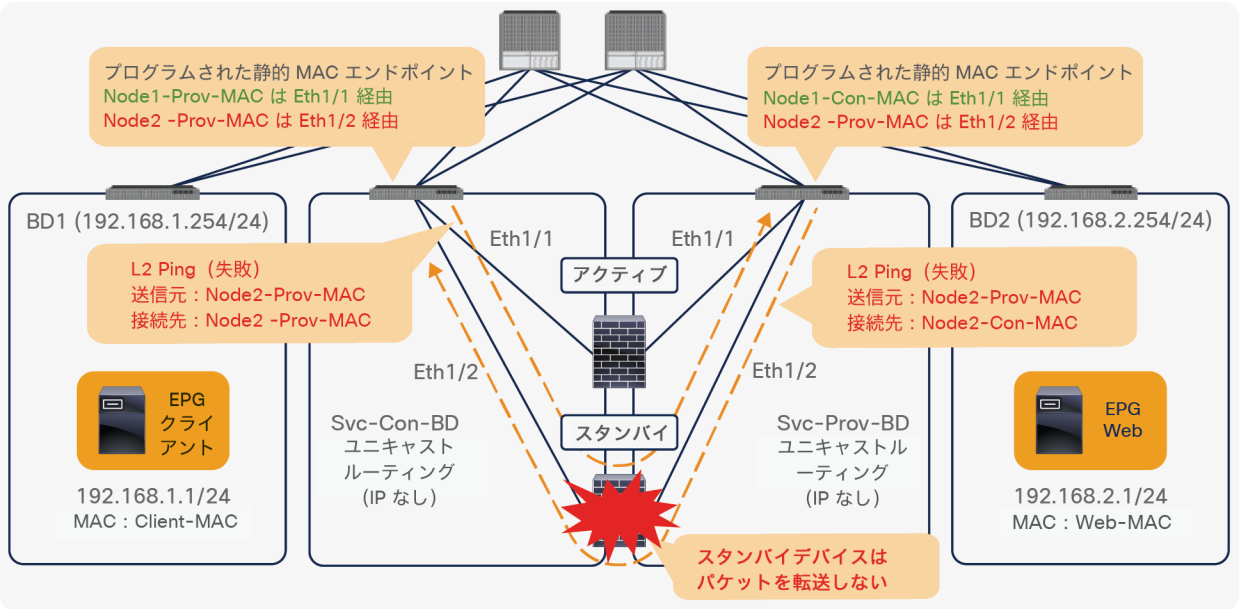


図 150.
スタンバイデバイスを使用した L2 Ping パスが失敗

フェールオーバーが発生し、スタンバイデバイスがアクティブロールを引き継ぐと、トラッキングステータスが変化し、トラフィックは、新しいアクティブノードに接続されているインターフェイス（この例では Eth1/2）にリダイレクトされます。

アクティブ/アクティブ設計

APIC リリース 5.0 以降では、対称 PBR のアクティブ/アクティブ設計も L1/L2 PBR に適用できます。APIC リリース 5.0 では、対称 PBR 関連機能として、しきい値、ダウンアクション、バックアップ PBR ポリシー（N+M 高可用性）なども利用できます。このセクションでは、L1/L2 PBR アクティブ/アクティブ機能と、L1/L2 PBR アクティブ/スタンバイ機能の動作の違いについて説明します。

ACI 5.0 より前のリリースでアクティブ/アクティブ設計がサポートされていないのは、同じサービスブリッジドメインのペアにアクティブな L1/L2 デバイスが複数ある場合、ループが発生する可能性があるためです。図 151 に例を示します。アクティブ/スタンバイ設計モードで動作している L4-L7 デバイスでは、ブリッジドメイン内でトラフィックがフラッディングされ、2 番目の L4-L7 デバイスに到達しても、このデバイスがスタンバイモードであるため、ループは発生しません。アクティブ/アクティブ設計では、2 番目の L4-L7 デバイスがトラフィックをもう一方のブリッジドメインにあるもう一方のインターフェイスに転送し、トラフィックが最初のデバイスに到達するため、ループが発生します。

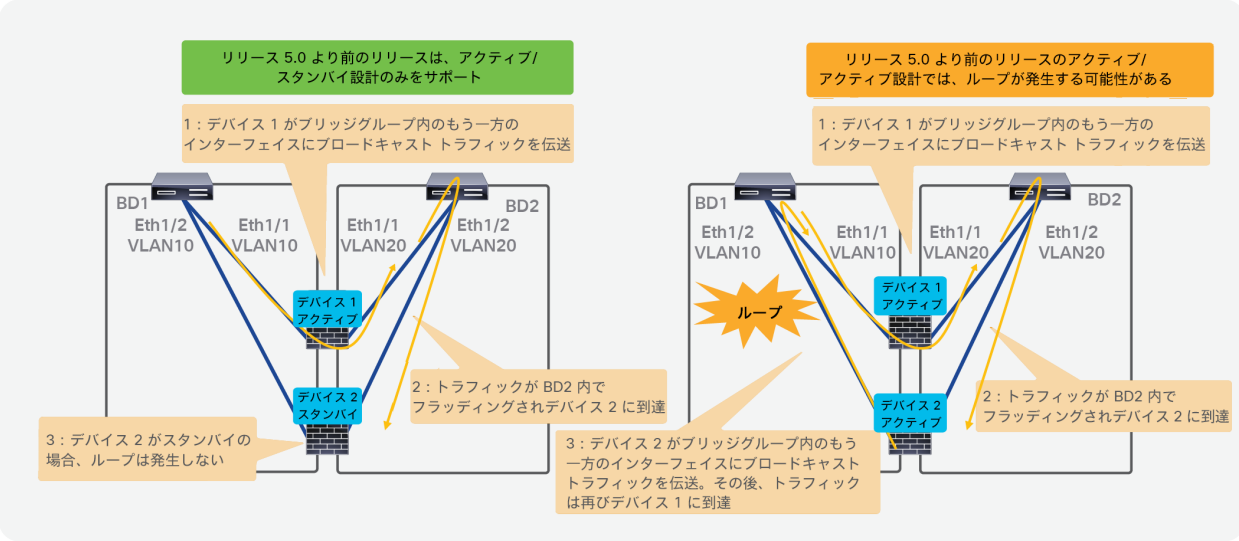


図 151.
APIC リリース 5.0 より前のリリースでは、ループが発生する可能性があるため、アクティブ/アクティブ設計がサポートされていない

APIC リリース 5.0 以降では、アクティブ/アクティブモードの L4-L7 デバイスが設定されたサービスグラフを展開できます。この設定により L4-L7 デバイスインターフェイス（具象インターフェイス）ごとに異なるカプセル化が割り当てられ、非表示サービス EPG で ACI が自動的に「Flood in Encap」を設定するためです（非表示サービス EPG は、サービスブリッジドメインにアタッチされた L4-L7 デバイスのインターフェイスを関連付けるために ACI が自動的に作成します）。

管理者が非表示サービス EPG を設定する必要はありません。サービスグラフのレンダリング中に ACI が自動的にサービス EPG で「Flood in Encap」を有効化します。

L1 PBR アクティブ/アクティブ設計を使用するには、ポートローカルスコープを設定する必要があります。つまり、L4-L7 デバイスのコンシューマーとプロバイダーのクラスタインターフェイス（コンシューマー「コネクタ」とプロバイダー「コネクタ」）は、同じ VLAN 範囲を使用する異なる VLAN プールを持つ異なる物理ドメインに属している必要があります。

図 152 に例を示します。L2 モードで動作するアクティブな各 L4-L7 デバイスは、コンシューマーとプロバイダーのインターフェイスに異なる VLAN カプセル化を使用します。「Flood in Encap」オプションは VLAN にまたがるフラッディングの伝播を回避するため、ループは発生しません。L4-L7 デバイスが L1 モードで動作している場合、アクティブな各デバイスのプロバイダーコネクタとコンシューマーコネクタは同じ VLAN カプセル化を使用します。コンシューマーコネクタとプロバイダーコネクタのペアが共用している VLAN カプセル化でフラッディングが伝播しないようにするために、異なる物理ドメインを使用し、ポートローカルスコープを設定する必要があります。

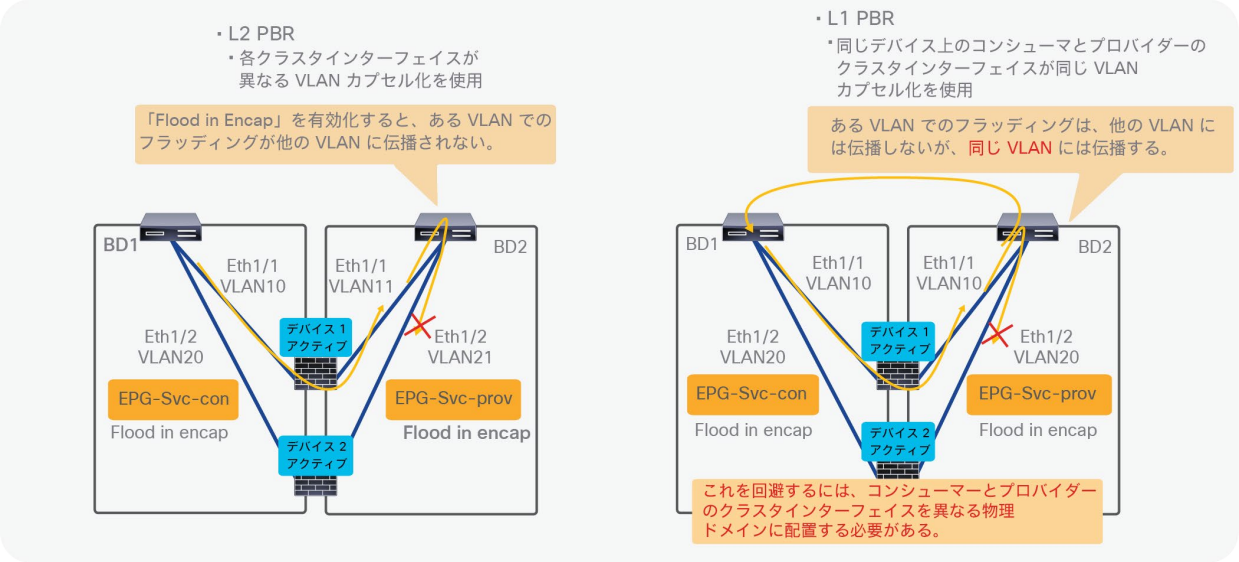


図 152.
アクティブ/アクティブ L1/L2 PBR でループを回避する方法

L1/L2 PBR のアクティブ/アクティブ設計で、複数のアクティブ/スタンバイペアを使用することもできます。図 153 に例を示します。L2 論理デバイスには 4 つの具象デバイスがあります。ファイアウォールペア 1 には、VLAN-711 と VLAN-712 を使用するアクティブ/スタンバイの 2 つのファイアウォールがあります。ファイアウォールペア 2 には、VLAN-721 と VLAN-722 を使用するアクティブ/スタンバイの 2 つのファイアウォールがあります。つまり、PBR 接続先が 4 つあり、そのうち 2 つだけがアクティブです。その結果「エラー」と判断されます。

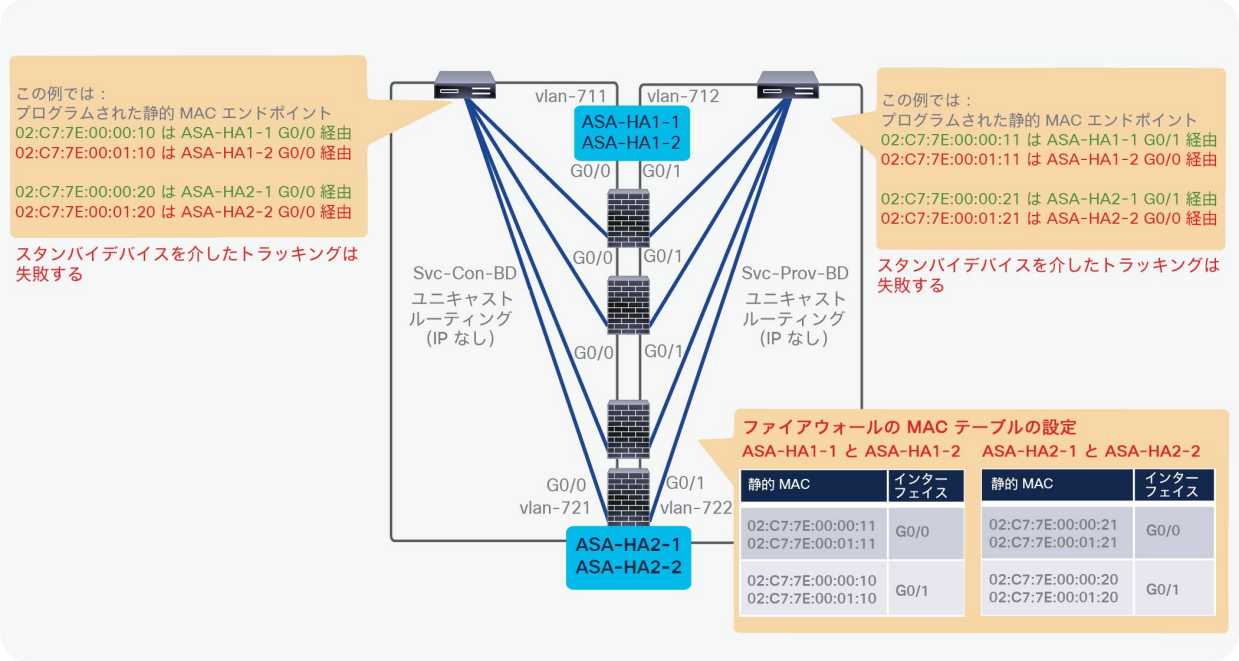


図 153.
複数のアクティブ/スタンバイペアの例

L1/L2 PBR の設定

L1/L2 PBR の設定フローは L3 PBR の場合と同様ですが、ブリッジドメイン、L4-L7 デバイス、PBR ポリシー、トラッキングの設定にはいくつかの要件があります。このセクションでは、L1/L2 PBR の設定に関する考慮事項と例について説明します。一般的な PBR の設定については、以前のセクションを参照してください。

このセクションでは、テナント、VRF、コンシューマーとプロバイダーの BD と EPG の作成方法については説明しません。コンシューマーとプロバイダーの EPG と BD がすでに設定されていることを前提としています。

このセクションで説明する L1/L2 PBR の設定は次のとおりです。

1. PBR ノードのブリッジドメインを作成します。
2. L4-L7 デバイスを作成します。
3. サービスグラフを作成します（L3 PBR の場合と同じ）。
4. IP SLA モニタリングポリシーを設定します（アクティブ/スタンバイのファイアウォールを使用する場合は必須）。
5. PBR ポリシーを作成します。
6. コントラクトにサービスグラフテンプレートを適用します。

このセクションで説明するオプション設定、CLI コマンド、設定に関する考慮事項は次のとおりです。

- PBR 接続先の MAC アドレスの変更
- トランスペアレントモード ASA 固有の設定
- 確認用の CLI 出力例
- L1 デバイスの接続に関する考慮事項

- アクティブ/スタンバイ高可用性ペアが複数ある場合の設計上の考慮事項

PBR ノードのブリッジドメインの作成

L1/L2 PBR ノードのコンシューマーコネクタとプロバイダーコネクタの BD を作成します。L1/L2 PBR ノードブリッジドメインには、次の要件と考慮事項があります。

- PBR ノードブリッジドメインは専用にする必要があり、他のエンドポイントとの共有はできません。
- PBR ノードブリッジドメインでは、[ユニキャストルーティング（Unicast Routing）] オプションを有効化する必要があります。
- PBR が設定されたサービスグラフが展開されると、データプレーン IP 学習が自動的に無効化されるため、IP データプレーン学習ノブを変更する必要はありません。

注： APIC は、サービスグラフのレンダリング中に、L1/L2 PBR のサービス BD が複数のデバイス選択ポリシーで設定されていないかどうか、EPG で使用されていないかどうかを確認します。使用されている場合エラーが発生します。別のサービスグラフがまだ展開されていなくてもサービスグラフのレンダリングが失敗します。

場所は、[テナント（Tenant）] > [ネットワーク（Networking）] > [ブリッジドメイン（Bridge Domains）] です。

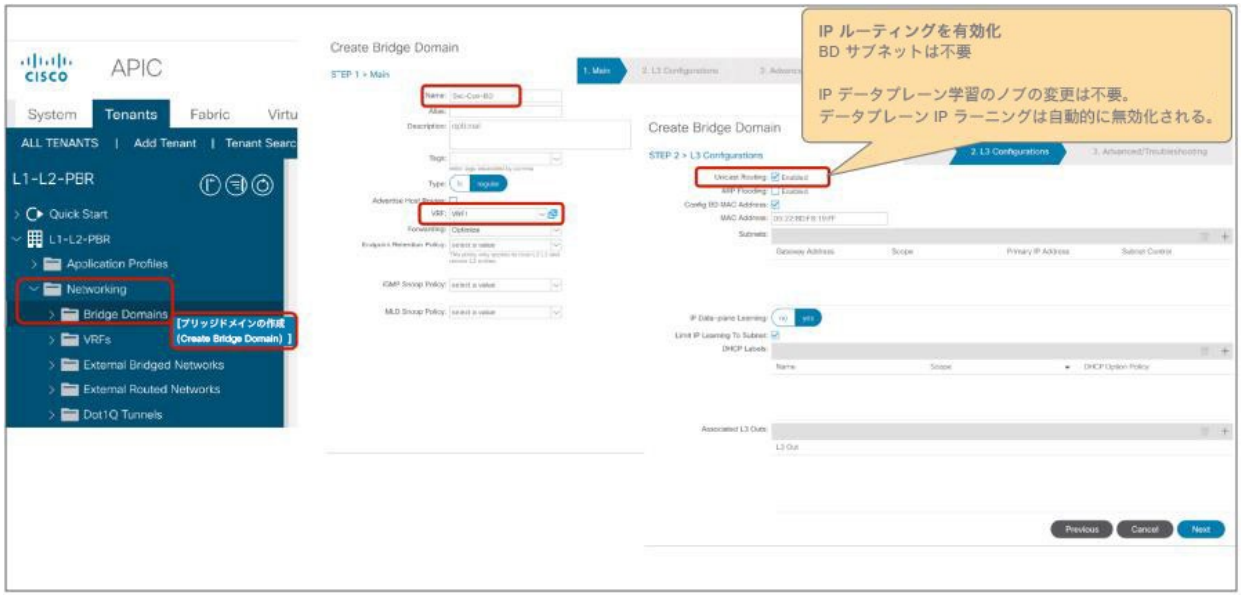


図 154.
ブリッジドメインの作成

図 155 に、ブリッジドメインの設定例を示します。[ユニキャストルーティング（Unicast Routing）] を有効化する必要がある場合でも、PBR ノードブリッジドメインに BD サブネットを設定する必要ありません。しかし、PBR では Cisco ACI ファブリックをレイヤ 3 として使用する必要があるため、コンシューマーとプロバイダーのブリッジドメインに BD サブネットが必要です。

図 155.
ブリッジドメインの設定例

L4-L7 デバイスの作成

L4-L7 デバイスを作成します。L1/L2 PBR に使用する L4-L7 デバイスには、次の要件と考慮事項があります。

- [管理対象（Managed）] オプションをオフにする必要があります（非管理対象モードのサービスグラフのみ）。
- [サービスタイプ（Service type）] : [その他（Other）]
- [デバイスタイプ（Device type）] : [物理（Physical）]
- [機能タイプ（Function type）] : [L1] または [L2]
- APIC リリース 5.0 より前のリリースでは、アクティブ/スタンバイ設計のみがサポートされているため、L4-L7 デバイスとして設定できるデバイスは最大 2 つです。
- L1 デバイスの場合、コンシューマーコネクタとプロバイダーコネクタを異なるリーフに接続する必要があります。

場所は、[テナント（Tenant）] > [L4-L7サービス（L4-L7 Services）] > [L4-L7デバイス（L4-L7 Devices）] です。

図 156 に、APIC リリース 4.1 を使用したアクティブ/スタンバイ L2 デバイスの設定例を示します。この論理デバイスは、次の設定例で使用されます。

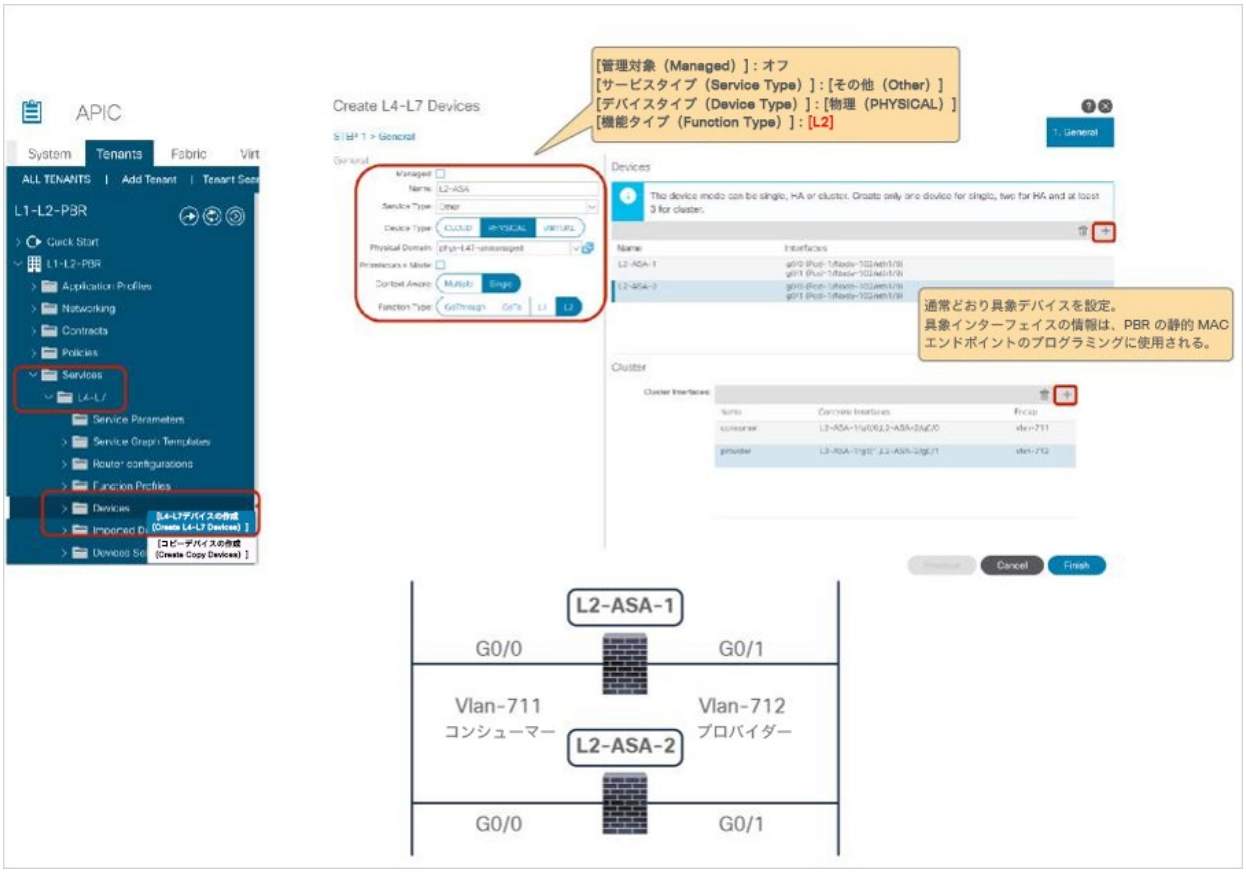


図 156.
L4-L7 デバイスの作成（APIC リリース 5.0 より前）

注： 具象インターフェイスの情報は、静的 MAC エンドポイントのプログラミングのために PBR ポリシー設定で参照されます。

L1/L2 PBR のアクティブ/アクティブモードでは、他にも次のような設定上の考慮事項があります。

- VLAN カプセル化の設定は、クラスタインターフェイスごとではなく、具象インターフェイスごとになります。
- L1 デバイスの場合、ポートローカルスコープを設定するために、各クラスタインターフェイスを異なる物理ドメインに置く必要があります。

図 157 に、APIC リリース 5.0 を使用したアクティブ/アクティブ L2 デバイスの設定例を示します。L4-L7 デバイスが L2 アクティブ/アクティブモードで動作する展開の場合、VLAN カプセル化の設定は、クラスタインターフェイスごとではなく、具象インターフェイスごとになります。各アクティブデバイスが異なる VLAN カプセル化を使用できるようにするためです。

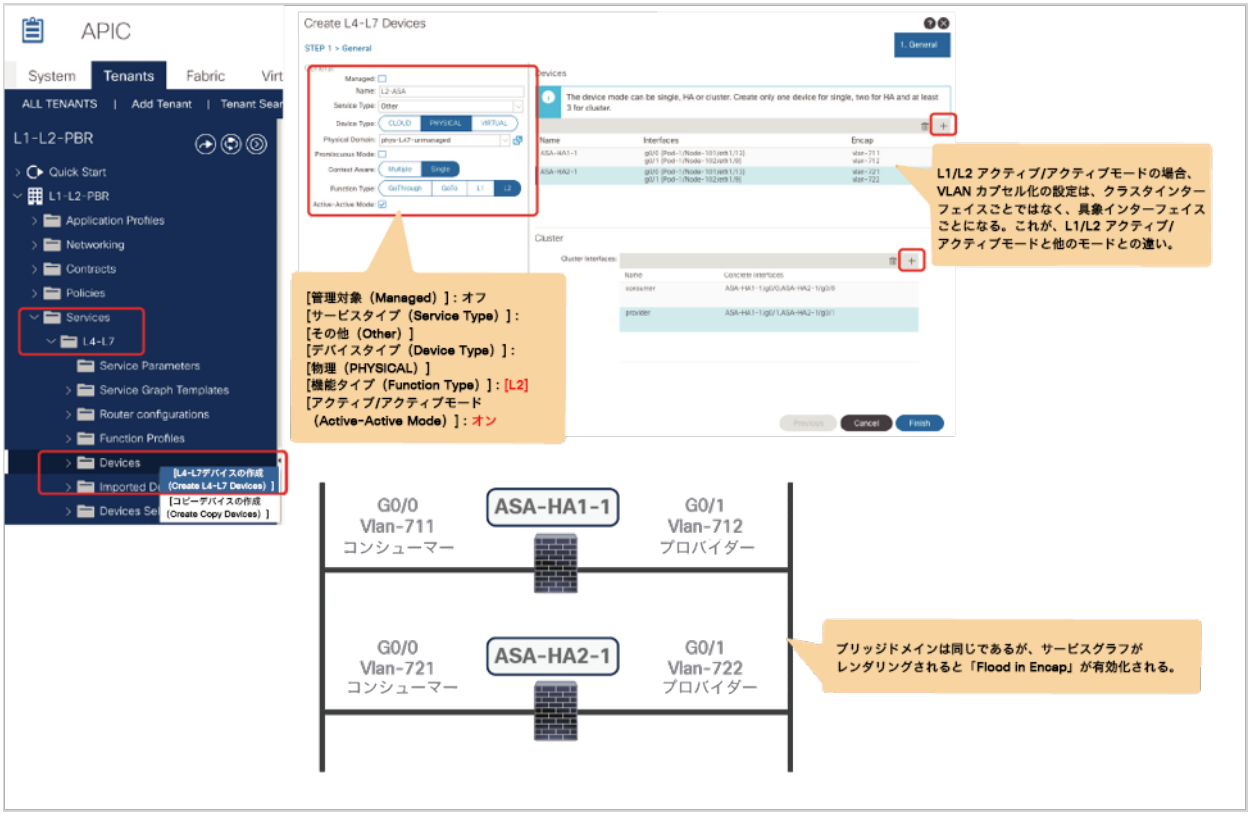


図 157.
L2 アクティブ/アクティブ展開に使用する L4-L7 デバイス（APIC リリース 5.0）の作成

図 158 に、APIC リリース 5.0 を使用してアクティブ/アクティブモードの L1 デバイスとして設定された L4-L7 デバイスの例を示します。このデバイスは L1 アクティブ/アクティブモードで動作しているため、VLAN カプセル化設定はクラスタインターフェイスごとではなく具象インターフェイスごとになります。物理ドメイン設定はポートローカルスコープの設定が必要なことからクラスタインターフェイスごとになります。ポートローカルスコープと物理ドメインの設定方法については、「L1 PBR アクティブ/アクティブモードでのポートローカルスコープの設定」を参照してください。

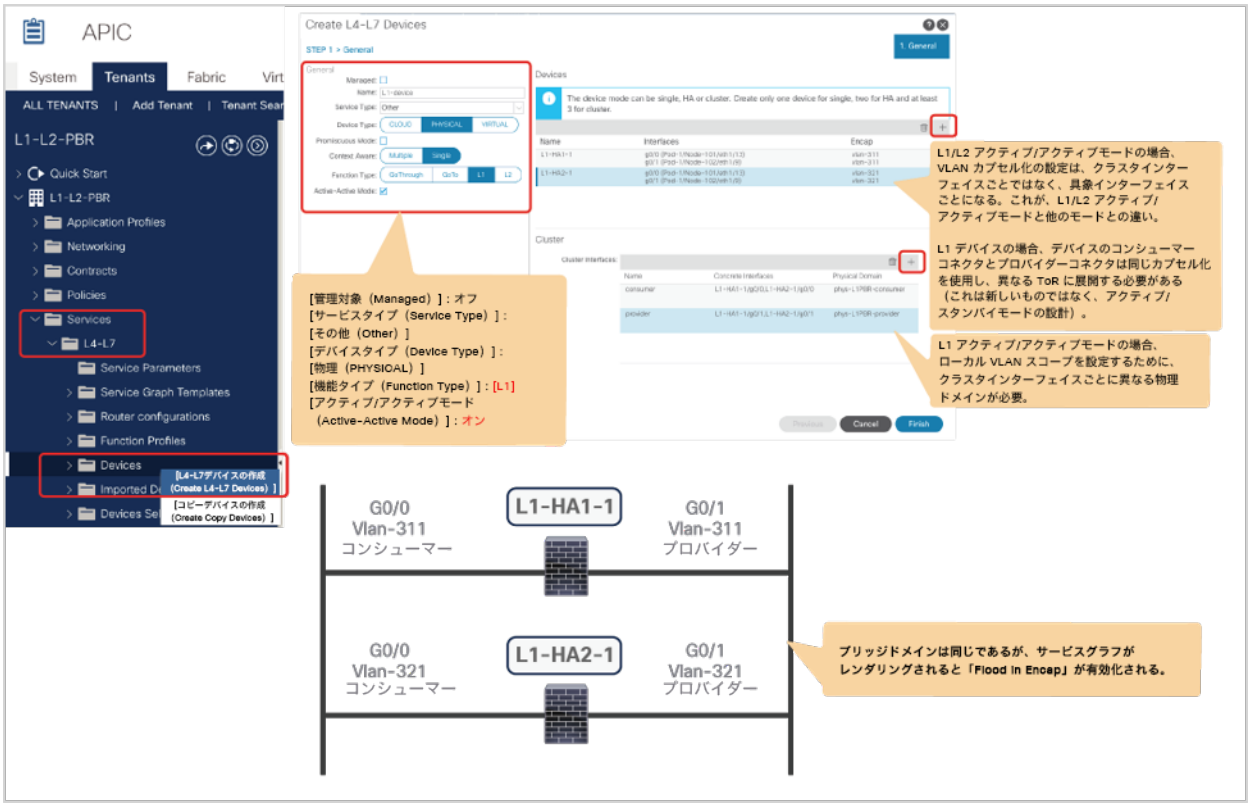


図 158.
L1 アクティブ/アクティブ展開に使用する L4-L7 デバイス（APIC リリース 5.0）の作成

サービスグラフテンプレートの作成（L3 PBR の場合と同じ）

この手順は、L1/L2 PBR に固有のものではありません。作成した L4-L7 デバイスを使用してサービスグラフテンプレートを作成します。ノードで PBR を使用するには、[ルートリダイレクト（Route Redirect）] を有効化する必要があります（図 159）。

場所は、[テナント（Tenant）] > [L4-L7サービス（L4-L7 Services）] > [L4-L7サービスグラフテンプレート（L4-L7 Service Graph Templates）] です。

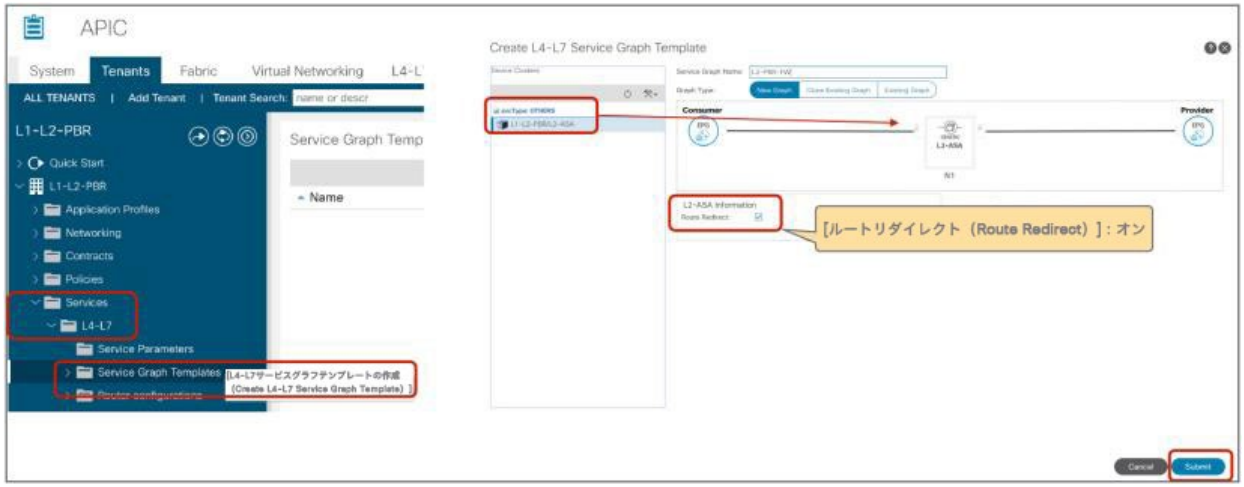


図 159.
サービスグラフテンプレートの作成

IP SLA モニタリングポリシーの作成

トラッキング用の IP SLA モニタリングポリシーを作成します。L1/L2 PBR では [L2Ping] を選択する必要があります。デフォルトの SLA 頻度は、60 秒です。IP SLA モニタリングポリシーは、次のステップの PBR ポリシーで参照されます。

場所は、[テナント（Tenant）] > [ポリシー（Policies）] > [プロトコル（Protocols）] > [IP SLA] です。

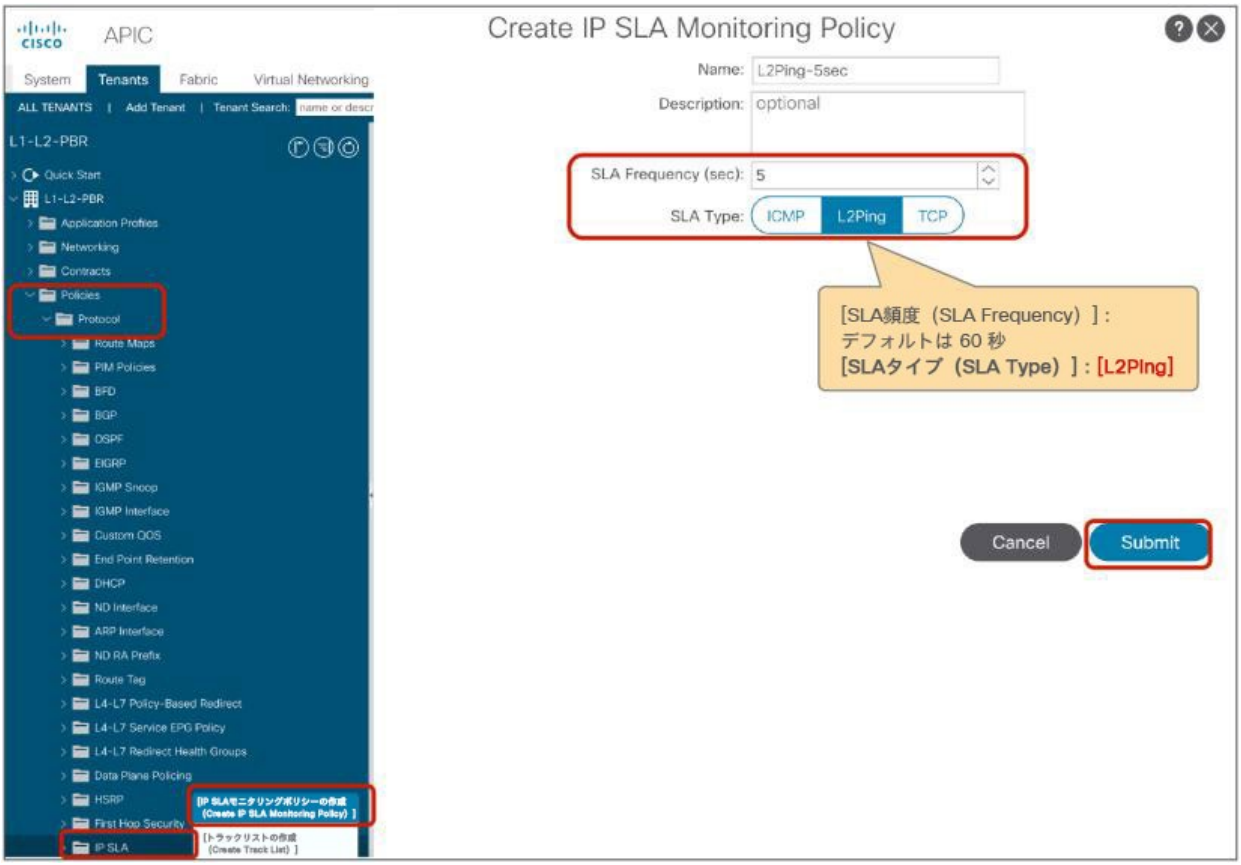


図 160.
IP SLA モニタリングポリシーの作成（L2Ping）

PBR ポリシーの作成

PBR ポリシーを作成します。[接続先タイプ（Destination Type）] として [L1] または [L2] を選択し、L1/L2 PBR デバイスに接続するインターフェイスを設定する必要があります。このインターフェイスは、PBR の静的 MAC エンドポイントをプログラムする際に使用されます。L3 PBR とは異なり、IP 情報は不要、MAC 情報はオプションです。この例では、G0/0 をコンシューマーコネクタとして、G0/1 をプロバイダーコネクタとして使用します。この 2 つは同じヘルスグループに属しています。

場所は、[テナント（Tenant）] > [ネットワーク（Networking）] > [プロトコルポリシー（Protocol Policies）] > [ポリシーベースリダイレクト（Policy Based Redirect）] です。

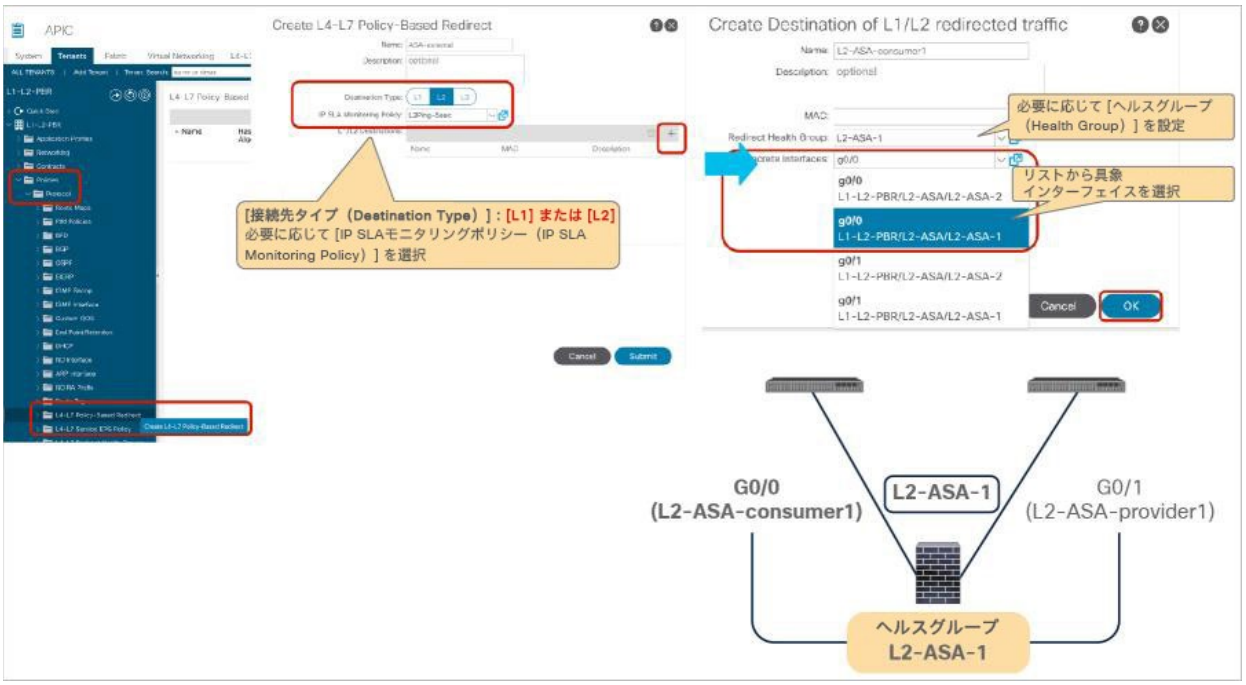


図 161.
コンシューマー側の PBR ポリシー

APIC リリース 5.0 より前のリリースでは、トラッキングを使用するアクティブ/スタンバイの場合、追加できる L1/L2 接続先は最大 2 つです。3 つ以上はサポートされていないため、エラーが発生します。APIC リリース 5.0 以降では、アクティブ/アクティブモードの場合、3 つ以上の L1/L2 接続先を追加できます。

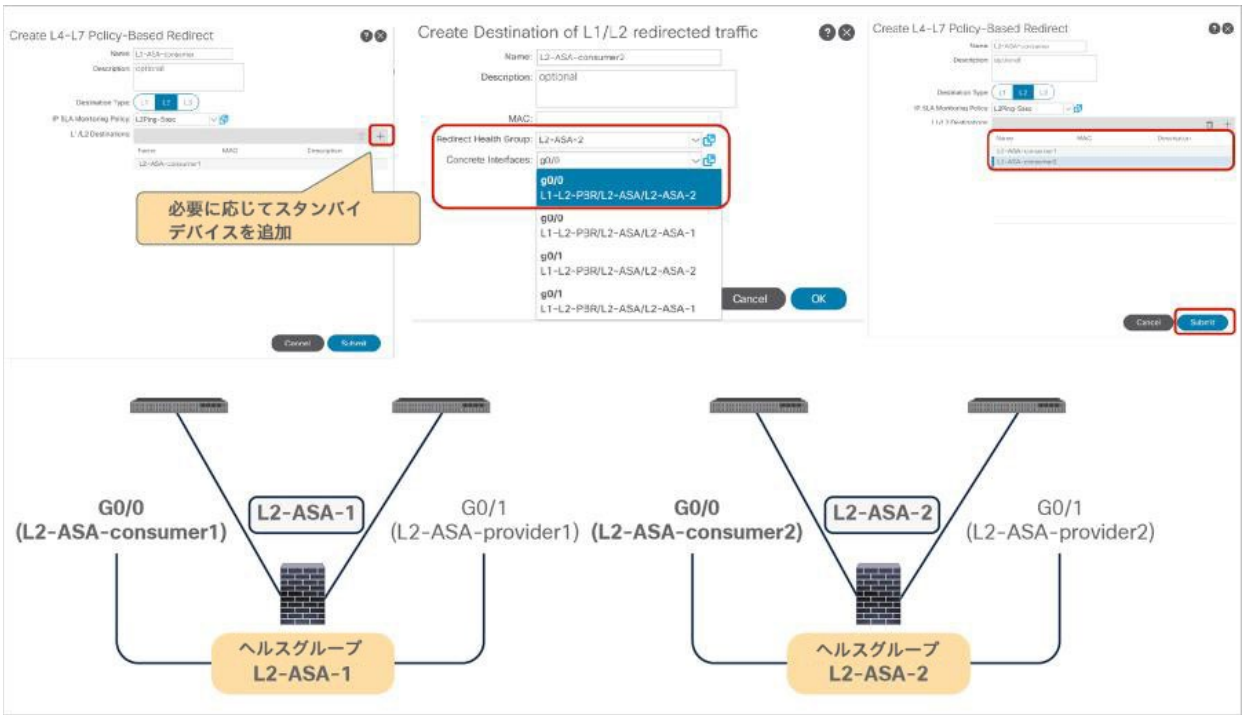


図 162.
コンシューマー側の PBR ポリシー（スタンバイデバイスの追加）

注： アクティブ/スタンバイモードではトラッキングが必要です。APIC リリース 5.0 より前のリリースでは、アクティブ/アクティブがサポートされていないため、しきい値は適用されません。トラッキングが有効化されている場合、ダウンアクションは 「拒否」 になります。ダウンアクション「許可」は、APIC リリース 4.1 および 4.2 では設定できません。ダウンアクションのオプションは、APIC リリース 5.0 以降でサポートされます。

IP と MAC は自動的に生成されます。MAC は設定で変更できますが、IP は変更できません。IP は L2 Ping ヘッダーには使用されませんが、すべての接続先のキーとなります。Cisco ACI ファブリックは、トラッキング情報を公開する際に IP を使用して接続先を識別します。

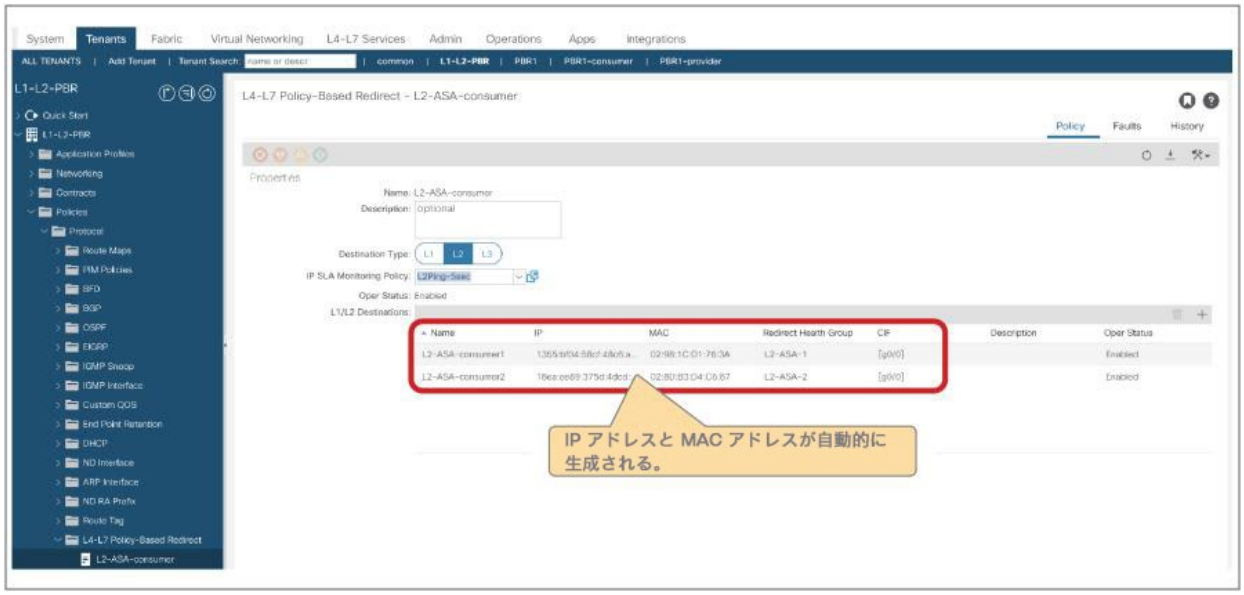
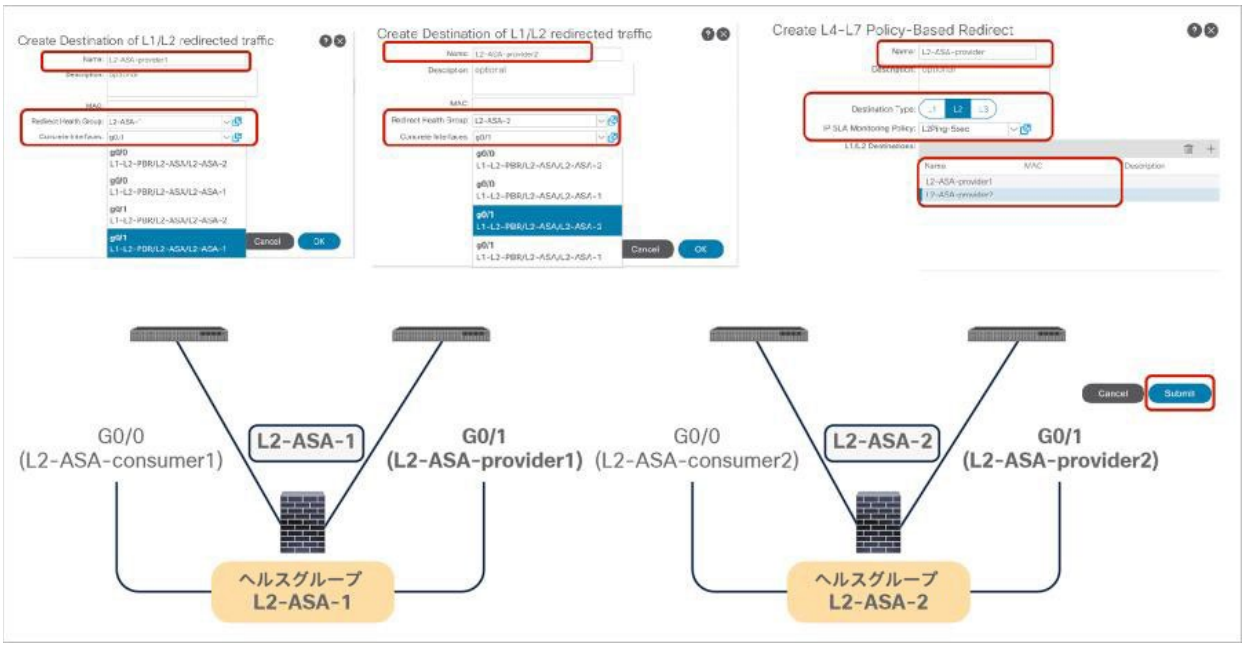


図 163.
コンシューマー側の PBR ポリシー

L1/L2 PBR ではツーアームモードが必須のため、もう一方の側の PBR ポリシーが必要です。図 164 に、プロバイダー側の PBR ポリシーの設定例を示します。



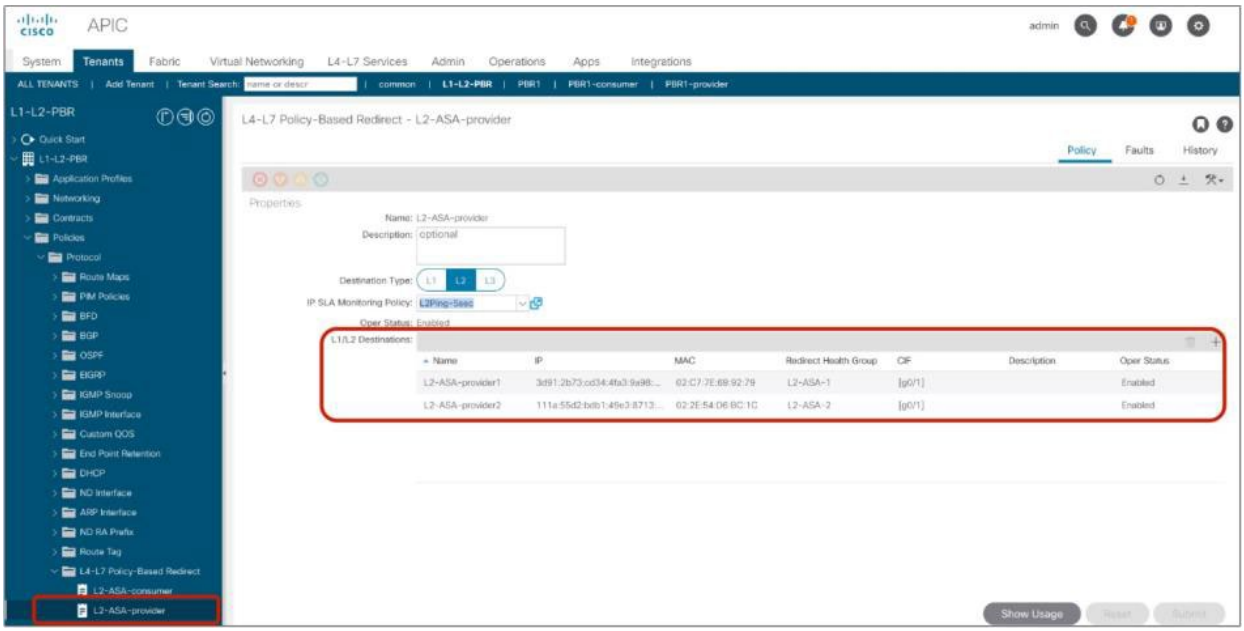


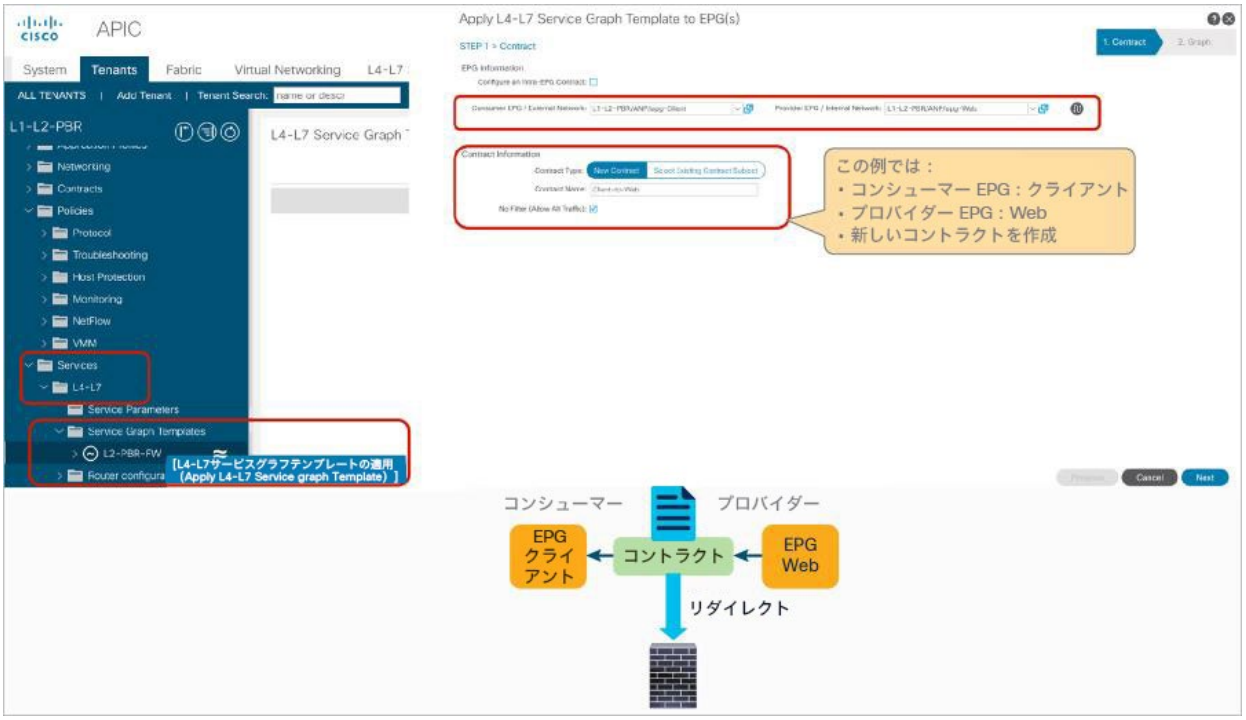
図 164.
プロバイダー側の PBR ポリシー

コントラクトへのサービスグラフテンプレートの適用

この手順は、L1/L2 PBR に固有のものではありません。[L4-L7サービスグラフテンプレートの適用（Apply L4-L7 Service Graph Templates）] ウィザードを使用するか、デバイス選択ポリシーを手動で作成します。この例では、ウィザードを使用しています。ウィザードでは、次の情報を選択するように求められます（図 165）。

- コンシューマー EPG、プロバイダー EPG、サービスグラフを適用するコントラクトサブジェクト
- BD、PBR ポリシー、PBR ノードのプロバイダーコネクタとコンシューマーコネクタの各クラスタインターフェイス

場所は、[サービス（Services）] > [L4-L7] > [サービスグラフテンプレート（Service Graph Templates）] です。



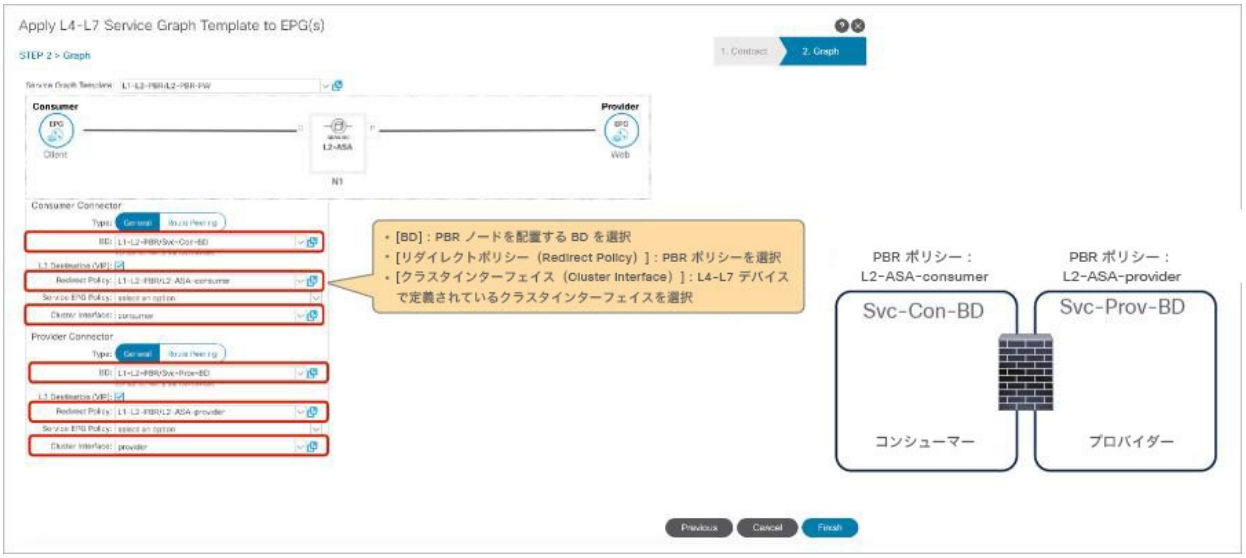


図 165.
サービスグラフテンプレートの適用

デバイス選択ポリシーを作成し、サービスグラフをコントラクトに関連付けます。場所は、[サービス（Services）] > [L4-L7] > [デバイス選択ポリシー（Device Selection Policy）] です。

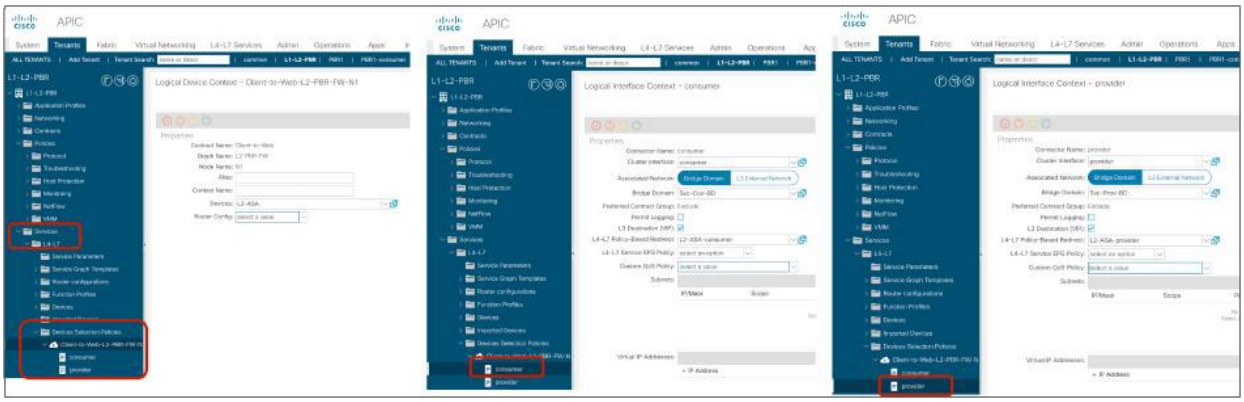


図 166.
デバイス選択ポリシー

すべてが適切に設定されていれば、[展開されたグラフインスタンス（Deployed Graph Instance）] にエラーが表示されないはずです。場所は、[サービス（Services）] > [L4-L7] > [展開されたグラフインスタンス（Deployed Graph Instance）] です。

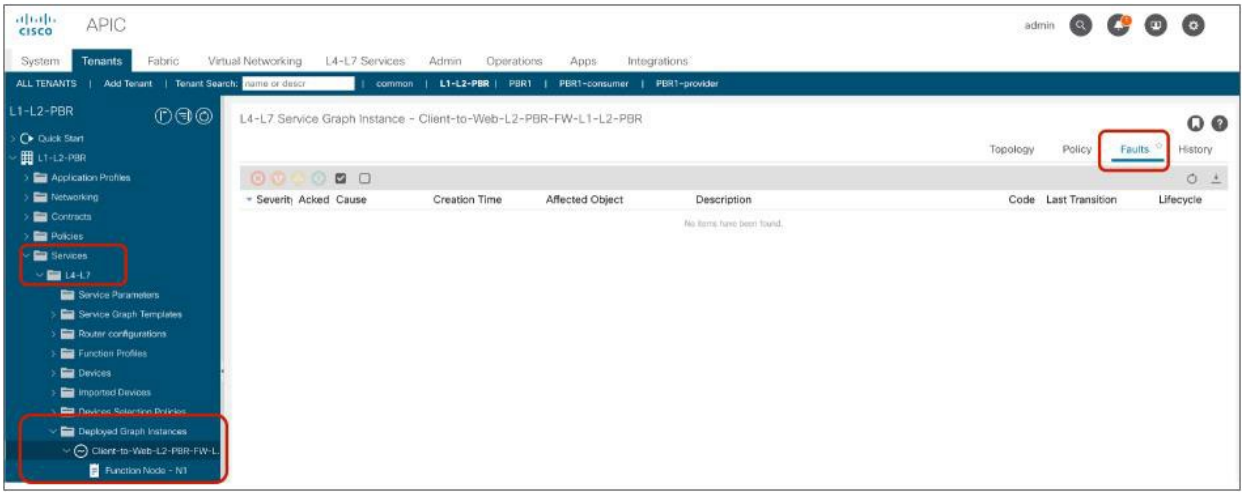


図 167.
展開されたグラフインスタンス

注： さらに、ゾーン分割ルールがプロバイダーリーフスイッチとコンシューマーリーフスイッチで更新されます。これについては、後のセクションで説明します。

Cisco 適応型セキュリティアプライアンス（ASA）の設定例

このセクションでは、Cisco ASA の設定例について説明します。Cisco ASA での L2 PBR に関する考慮事項は次のとおりです。

- アクセス制御リストを設定して、L2 Ping に Ethertype 0x0721 を許可します。デフォルトでは、Cisco ASA はこれを許可していないためです。
- MAC アドレステーブルに PBR 接続先 MAC アドレスを設定します。Cisco ASA トランスペアレントモードでは接続先 MAC のルックアップが実行されるためです。
- Cisco ASA で MAC アドレス学習を無効化します。L2 Ping の送信元 MAC アドレスがコンシューマーコネクタとプロバイダーコネクタへ送られるキープアライブメッセージの送信元 MAC アドレスと同じであり、Cisco ASA が異なるインターフェイスから同一の送信元 MAC を受け取ることによって、Cisco ASA で MAC アドレスフラッピングが発生するためです。

以下では、図 168 の例を使用します。

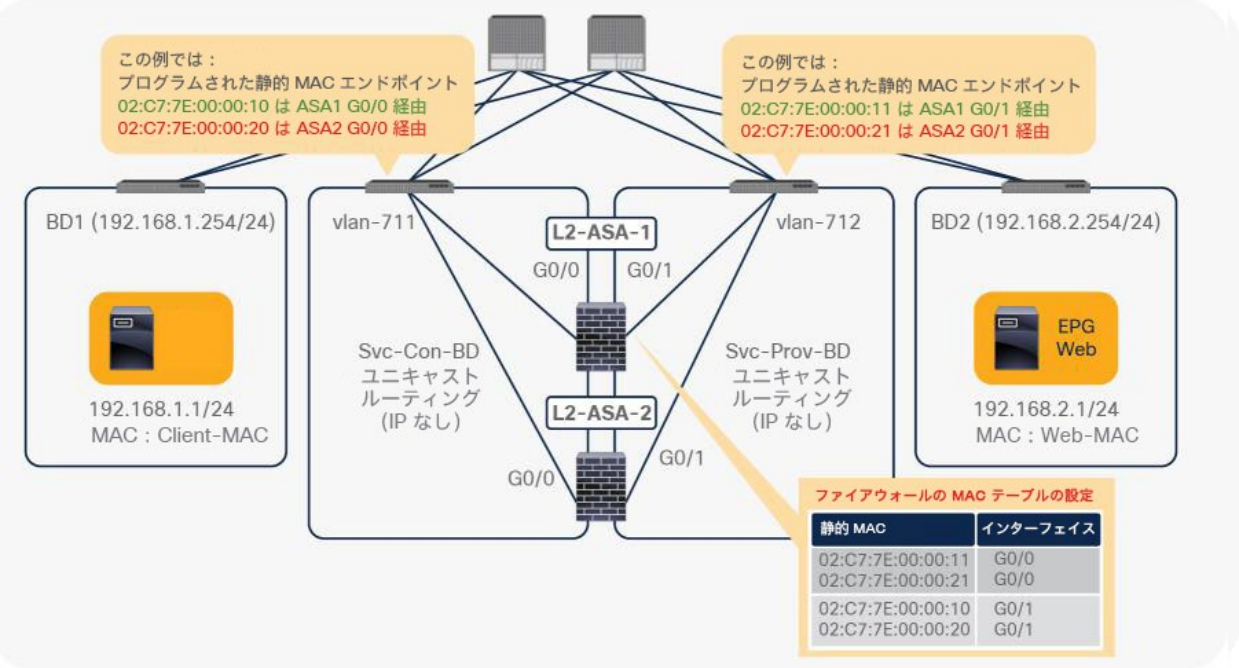


図 168.
トポロジの例

必要に応じて PBR 接続先 MAC を指定できます。デフォルトでは自動的に生成されます。場所は、[テナント（Tenant）] > [ネットワーク（Networking）] > [プロトコルポリシー（Protocol Policies）] > [ポリシーベースリダイレクト（Policy Based Redirect）] です。

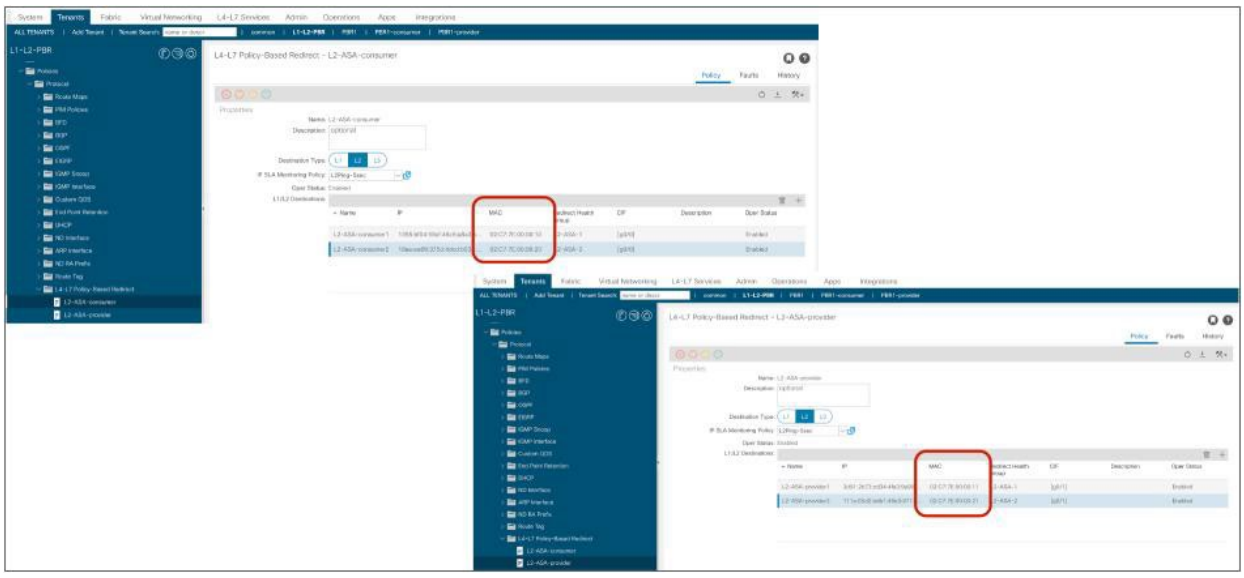


図 169.
PBR の接続先 MAC アドレスの指定（オプション）

図 170 に、Cisco ASA の設定例を示します。この例では、ASA 外部インターフェイス（コンシューマーコネクタ）の名前は「externalIf」、ASA 内部インターフェイス（プロバイダーコネクタ）の名前は「internalIf」です。

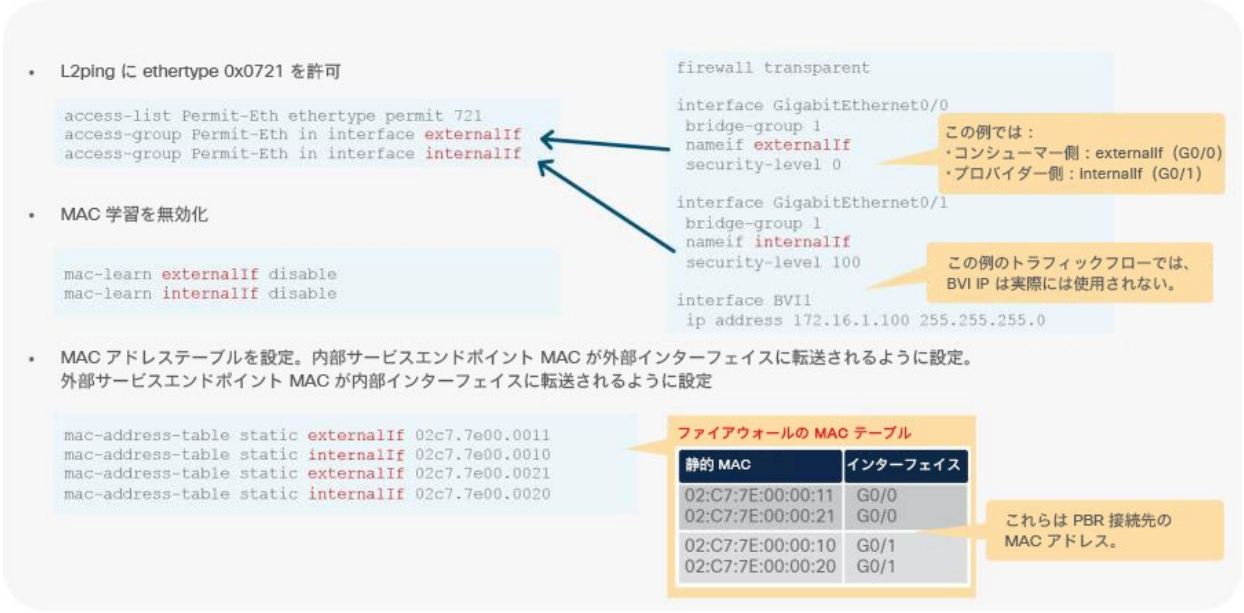


図 170.
Cisco ASA の設定例

確認用の CLI 出力例

このセクションでは、PBR とトラッキングを確認するためにリーフスイッチで実行する CLI コマンドについて説明します。

コンシューマーリーフノードとプロバイダーリーフノードで、コントラクトポリシーがプログラムされています。L3 PBR の場合と同じように、サービスグラフが展開されると VRF のゾーン分割ルールが更新されます。


```
Pod1-Leaf1# show zoning-rule scope 2195457
+---------+--------+--------+----------+----------------+---------+---------+------+------------------+-----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |      Action      |       Priority        |
+---------+--------+--------+----------+----------------+---------+---------+------+------------------+-----------------------+
|    4126 |      0 |  16389 | implicit |     uni-dir    | enabled | 2195457 |      |      permit      |    any_dest_any(16)   |
|    4127 |      0 |      0 | implicit |     uni-dir    | enabled | 2195457 |      |     deny,log     |    any_any_any(21)    |
|    4128 |      0 |      0 | implarp  |     uni-dir    | enabled | 2195457 |      |      permit      |  any_any_filter(17)   |
|    4129 |      0 |     15 | implicit |     uni-dir    | enabled | 2195457 |      |     deny,log     | any_vrf_any_deny(22)  |
|    4130 |  49156 |  16388 | default  |     uni-dir    | enabled | 2195457 |      |      permit      |     src_dst_any(9)    |
|    4131 |      0 |  49154 | implicit |     uni-dir    | enabled | 2195457 |      |      permit      |    any_dest_any(16)   |
|    4132 |  49155 |  32770 | default  |     uni-dir    | enabled | 2195457 |      |      permit      |     src_dst_any(9)    |
|    4133 |      0 |  16387 | implicit |     uni-dir    | enabled | 2195457 |      |      permit      |    any_dest_any(16)   |
|    4136 |      0 |  49153 | implicit |     uni-dir    | enabled | 2195457 |      |      permit      |    any_dest_any(16)   |
|    4134 |  16388 |  32770 | default  |     bi-dir     | enabled | 2195457 |      | redir(destgrp-5) |     src_dst_any(9)    |
|    4135 |  32770 |  16388 | default  | uni-dir-ignore | enabled | 2195457 |      | redir(destgrp-4) |     src_dst_any(9)    |
+---------+--------+--------+----------+----------------+---------+---------+------+------------------+-----------------------+
```

図 171.
コンシューマーリーフノードとプロバイダーリーフノードのゾーン分割ルール

アクティブなサービスノードを通過すればトラッキングは成功します。この例では、L2-ASA-1 がアクティブで、L2-ASA-2 がスタンバイです。Cisco ACI ファブリックは、PBR ポリシー内の自動的に生成された IP を使用して接続先を識別します。

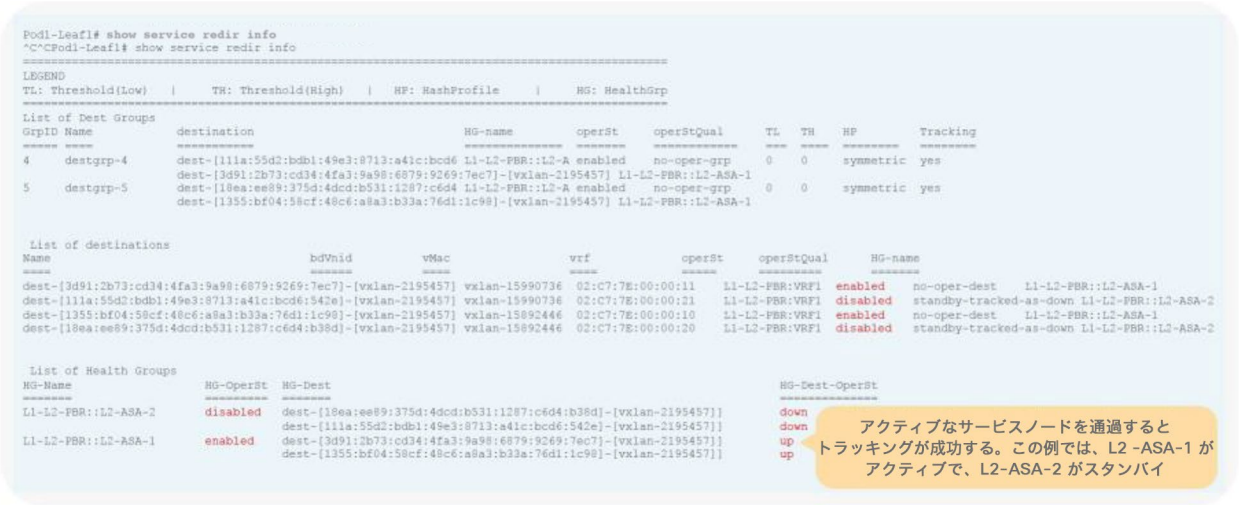


図 172.
コンシューマーリーフノードとプロバイダーリーフノードでのトラッキングステータス

トラブルシューティングのヒントを以下に挙げます。

- PBR ノードがトラフィックを受信しない：
  - コンシューマーリーフスイッチとプロバイダーリーフスイッチでゾーン分割ルールをチェックして、リダイレクトルールがあることを確認します。
  - コンシューマーリーフスイッチとプロバイダーリーフスイッチで PBR ポリシーが適用されているかどうかを確認します。
  - トラッキングステータスが稼働しているかどうかを確認します。
- トラッキングは有効化されているが、ステータスが「ダウン」になっている：
  - PBR 接続先 MAC が、PBR ノードが接続されているサービスリーフにあるかどうかを確認します。
  - PBR ノードの設定をチェックしてデバイスが L2 Ping を許可していることを確認するとともに、パケットのキャプチャを試みます。
- トラフィックが PBR ノードから戻らない：
  - PBR ノードの設定をチェックして、PBR ノードがそのトラフィックを許可していることを確認します。

L1 デバイスの接続に関する考慮事項

このセクションでは、L1 デバイスの接続に関する考慮事項について説明します。

ループ検出メカニズムの無効化

ACI ファブリックにはループ検出メカニズムがあります。リーフノード間の L1 デバイスが Mis-Cabling Protocol（MCP）パケットまたは CDP/LLDP パケットを伝送すると、ACI ファブリックがループを検出することがあります。検出されると、ポートが「サービス停止中」のステータスに変更されます。これを回避するには、L1 デバイスに接続されているポートで MCP や CDP/LLDP を無効化する必要があります。

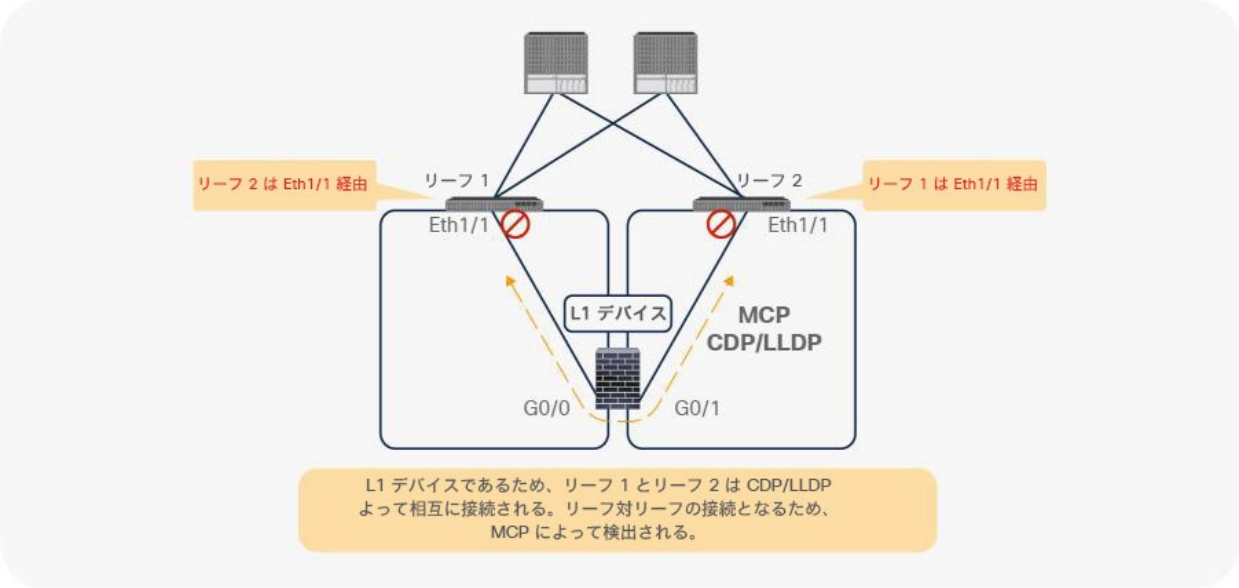


図 173.
ACI によるループ検出

MCP はデフォルトで無効化されています。MCP をグローバル設定で有効化している場合は、L1 デバイスに接続されているリーフインターフェイスのインターフェイス ポリシー グループで MCP を無効化する必要があります。グローバルな MCP の設定場所は、[ファブリック（Fabric）] > [アクセスポリシー（Access Policies）] > [ポリシー（Policies）] > [グローバル（Global）] です。

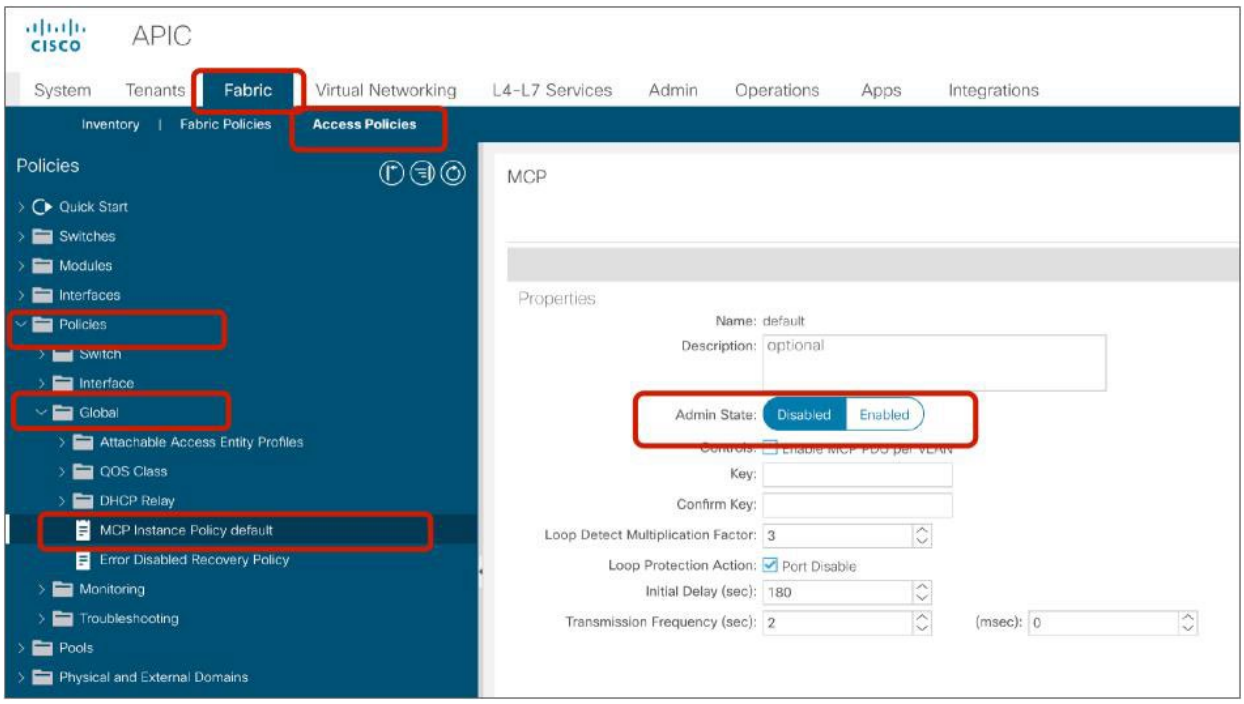


図 174.
MCP 設定（グローバル）

CDP はデフォルトで無効化されていて、LLDP はデフォルトで有効化されています。インターフェイス ポリシー グループの設定場所は、[ファブリック（Fabric）] > [アクセスポリシー（Access Policies）] > [インターフェイス（Interfaces）] > [リーフインターフェイス（Leaf Interfaces）] > [ポリシーグループ（Policy Groups）] です。

図 175.
CDP/LLDP 設定（インターフェイス ポリシー グループ）

L1 PBR アクティブ/アクティブモードでのポートローカルスコープの設定

L1 PBR アクティブ/アクティブモードの場合、ポートローカルスコープを設定するために、コンシューマーコネクタとプロバイダーコネクタを異なる物理ドメインに置く必要があります。L1 PBR デバイスに接続されているリーフインターフェイスのインターフェイス ポリシー グループで、前のセクションで説明したループ検出メカニズムを無効化するとともに、[ポートローカルスコープ（Port Local Scope）] を設定する必要があります。

インターフェイス ポリシー グループの設定場所は、[ファブリック（Fabric）] > [アクセスポリシー（Access Policies）] > [インターフェイス（Interfaces）] > [リーフインターフェイス（Leaf Interfaces）] > [ポリシーグループ（Policy Groups）] です。

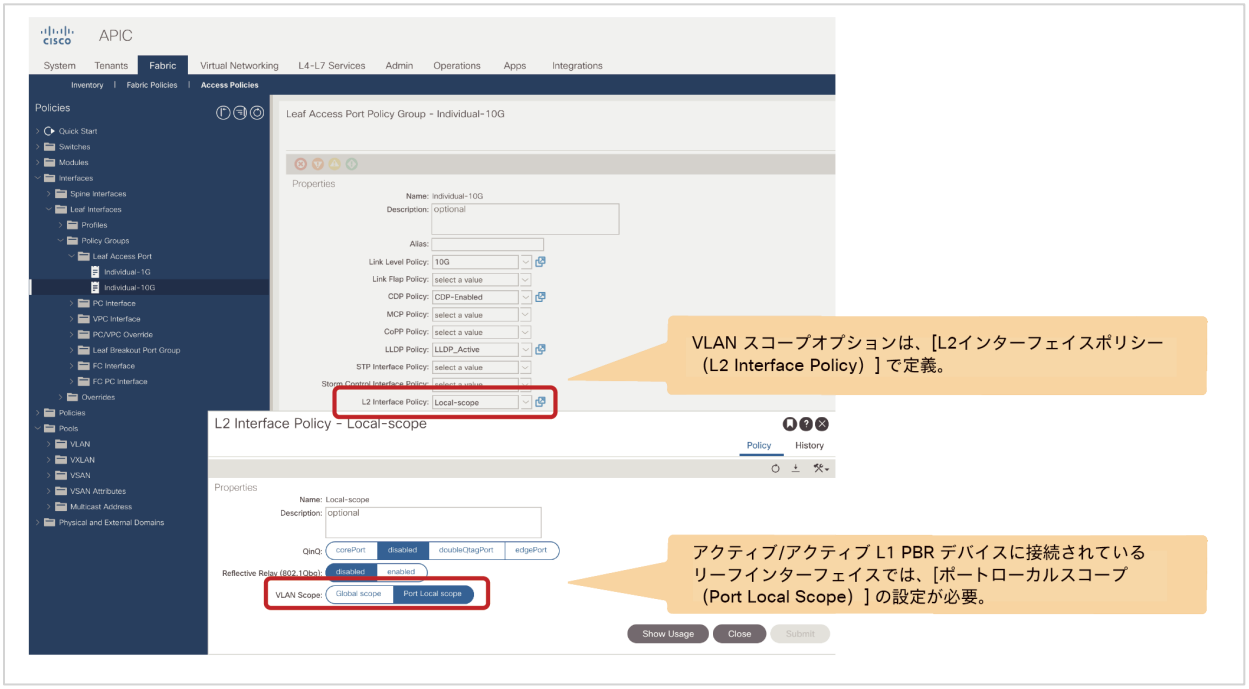


図 176.
ポートローカルスコープの設定（L2 インターフェイスポリシー）

ポートローカルスコープを使用するには、各クラスタインターフェイスが異なる物理ドメインに属している必要があります。そのため、同じ VLAN 範囲を使用する異なる VLAN プールを持つ 2 つの物理ドメインを設定する必要があります。物理ドメインは異なる必要がありますが、リーフインターフェイスの接続エンティティプロファイル（AEP）は、コンシューマーとプロバイダーのクラスタインターフェイスが異なるリーフに接続されている限り、両方で同じにすることができます。物理ドメインの設定場所は、[ファブリック（Fabric）] > [アクセスポリシー（Access Policies）] > [物理ドメインと外部ドメイン（Physical and External Domains）] です。

図 177.
異なる VLAN プールを持つ 2 つの物理ドメインの作成

アクティブ/スタンバイ高可用性ペアが複数ある場合の設計上の考慮事項

複数のアクティブ/スタンバイペアが使用されている場合、サービスノードのフェールオーバータイマーは IP-SLA のフェールオーバータイマーよりも常に小さくする必要があります。

図 178 に、サービスノードのフェールオーバータイマーが IP-SLA のフェールオーバータイマーよりも小さい例 1 を示します。高可用性ペア 1 にはアクティブ接続先 A とスタンバイ接続先 B があり、高可用性ペア 2 にはアクティブ接続先 C とスタンバイ接続先 D があります。A がダウンすると（t0）、最初にサービスノードのフェールオーバーが発生し、B がアクティブになります（t1）。その後、B のトラッキングは「稼働中」（t2）になり、A のトラッキングは「ダウン」（t3）になります。

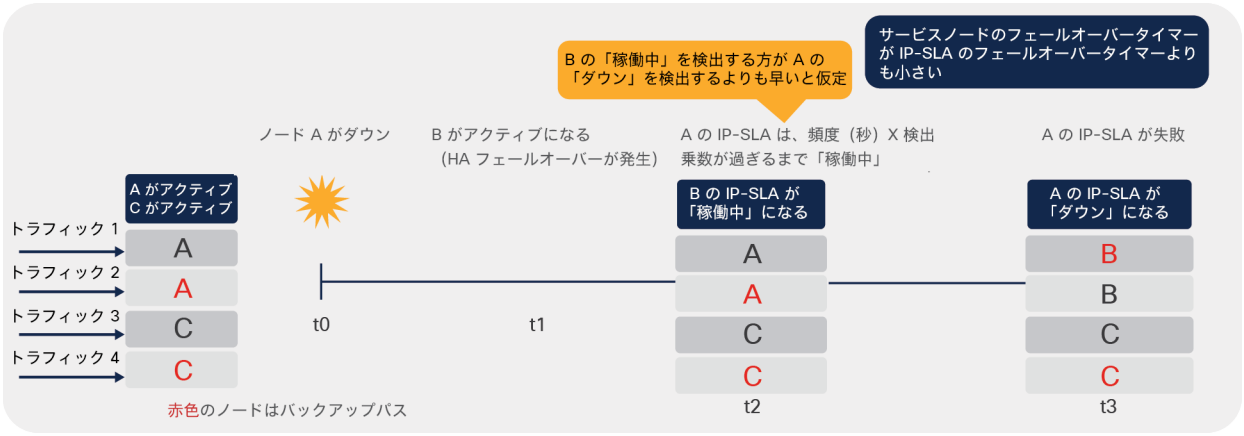


図 178.
例 1：サービスノードのフェールオーバータイマーが IP-SLA のフェールオーバータイマーよりも小さい（推奨）

図 179 に、サービスノードのフェールオーバータイマーが IP-SLA のフェールオーバータイマーより大きい例 2 を示します。A がダウン（t0）すると、サービスノードのフェールオーバータイマーが IP-SLA のフェールオーバータイマーより大きいため、A のトラッキングが最初に「ダウン」（t1）になります。その後、サービスノードのフェールオーバーが発生し、B がアクティブになります（t2）。その後、最終的に B のトラッキングは「稼働中」（t3）になります。例 1 は例 2 よりも明らかに優れています。例 2 の t1 のステータスがボトルネックを引き起こす可能性があるうえ、例 2 の方が例 1 よりも長い（t3-t0）時間を要するためです。

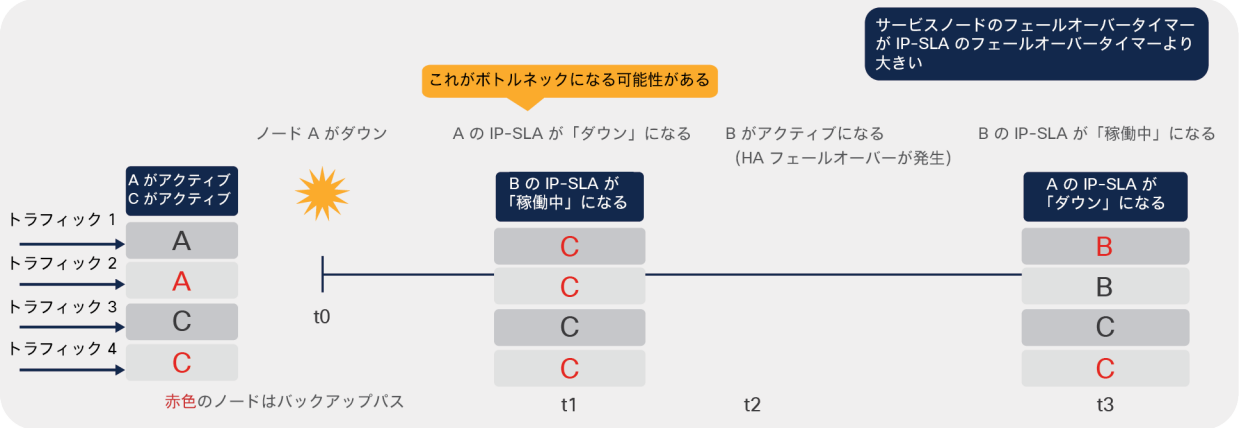


図 179.
例 2：サービスノードのフェールオーバータイマーが IP-SLA のフェールオーバータイマーより大きい（非推奨）

L3Out にある PBR 接続先

APIC リリース 5.2 以降では、L3 PBR 接続先を L3 ブリッジドメインではなく L3Out に置くことができるため、より柔軟な設計オプションが利用できます。このセクションでは、ユースケースの例、設定方法、転送動作、設計上の考慮事項について説明します。

ユースケースの例

図 180 に、最初の例として、垂直方向ファイアウォールと水平方向ファイアウォールを挿入するユースケースを示します。ファイアウォールは L3Out を介して接続されているとします。この L3Out は、垂直方向トラフィック（L3Out-EPG）の検査用です。次に、水平方向トラフィック（EPG-EPG）の検査に同じファイアウォールの内部インターフェイスを使用したいとします。APIC リリース 5.2 より前のリリースでは、ファイアウォールの内部インターフェイスが PBR を有効化できない L3Out を介して接続されていたため、これが不可能でした。

現在では、次の設定を実行することでこの要件を実現できます。

- 水平方向ファイアウォールを挿入するために、EPG 間のコントラクト（この例ではコントラクト 1）で PBR を有効化します。PBR 接続先は L3Out を介して接続されます。
- 垂直方向ファイアウォールを挿入するために、L3Out EPG と他の EPG との間に PBR がないコントラクト（この例ではコントラクト 2）を設定します。

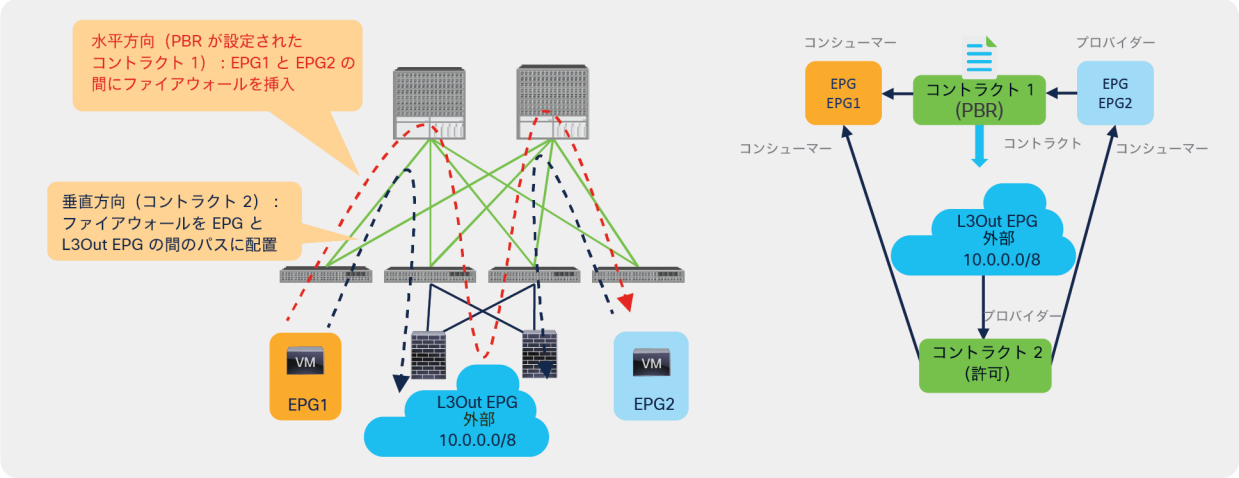


図 180.
ユースケースの例 1：垂直方向境界ファイアウォールの挿入

図 181 に、2 番目の例として、ロードバランサを挿入するユースケースを示します。ロードバランサは、L3Out を介して接続されているとします。ロードバランサのインターフェイスの IP アドレスが存在するブリッジドメインのサブネット範囲に VIP アドレスが含まれていないためです。同時に、ロードバランサで NAT を有効化するのを避けるために、ロードバランサの同じインターフェイスを使用し、リターントラフィック（この例では EPG2 から EPG1）の PBR を有効化したいとします。APIC リリース 5.2 より前は、ロードバランサの別の内部インターフェイスを L3 ドメインに置いて PBR を有効化しない限り、これは不可能でした。

以下のようにしてリターントラフィックの PBR を有効化することで、この要件を実現できます。

- コンシューマーからプロバイダーへのトラフィックには PBR を設定しません。トラフィックの接続先がロードバランサが所有する VIP になるため、PBR を有効化する必要はありません。ロードバランサへの L3Out を使用して VIP にルーティングするように ACI ファブリックを設定する必要があります。
- プロバイダーからコンシューマーへのトラフィックに PBR を設定します。PBR を有効化して、リターントラフィックをロードバランサに戻します。PBR 接続先は L3Out を介して接続されます。

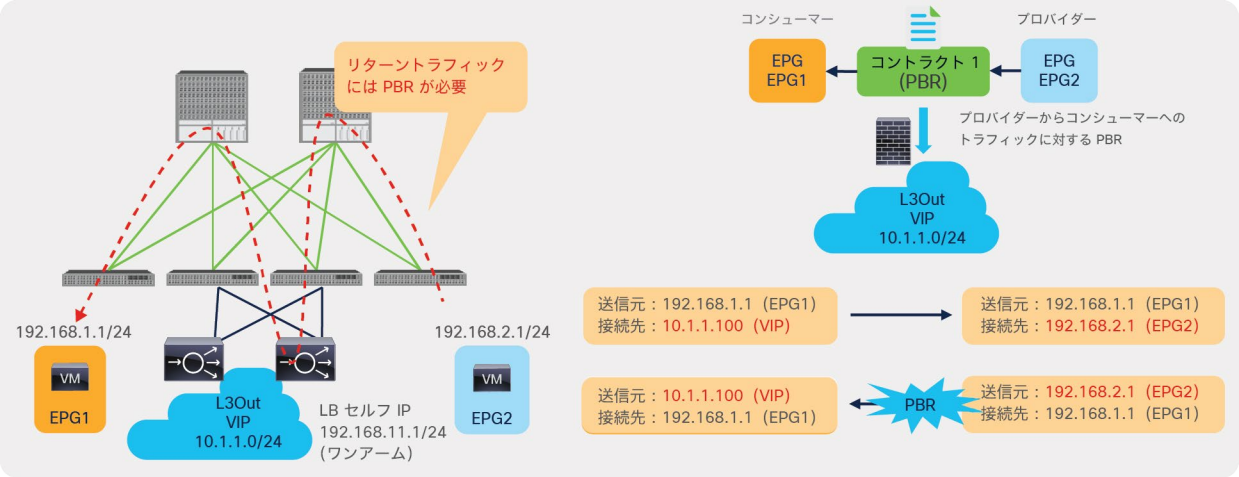


図 181.
ユースケースの例 2：ロードバランサの挿入

図 182 に、3 番目の例として、ACI ファブリックに直接接続されていないサービスデバイスのユースケースを示します。APIC リリース 5.2 以降では、L3Out を介して接続された外部ルータの背後に PBR 接続先を置くことができます。

設計上の考慮事項を次に示します。

- PBR リダイレクトポリシーを設定する際には、外部ルータの MAC アドレスとその外部ルータの背後にあるサービスノードの IP アドレスを使用する必要があります。ACI はトラフィックの接続先 MAC を書き換えますが、IP アドレスは書き換えません。PBR 接続先の IP アドレスを入力するのは、ACI がこの情報を IP-SLA トラッキングに使用するためです。
- 上記の設定をすることで、ACI がトラフィックを外部ルータにリダイレクトできるようになります。リダイレクトされたトラフィックの宛先 IP アドレスは、EPG2 にあるサーバーの IP であり、ポリシーベースリダイレクトではこの IP アドレスは書き換えられません。外部ルータは、本来、単に宛先 IP アドレスに基づいてこのトラフィックを転送するだけです。したがって、ルータにアタッチされたサービスデバイスをトラフィックが通過するようにするには、外部ルータでポリシーベースルーティングを設定する必要があります。

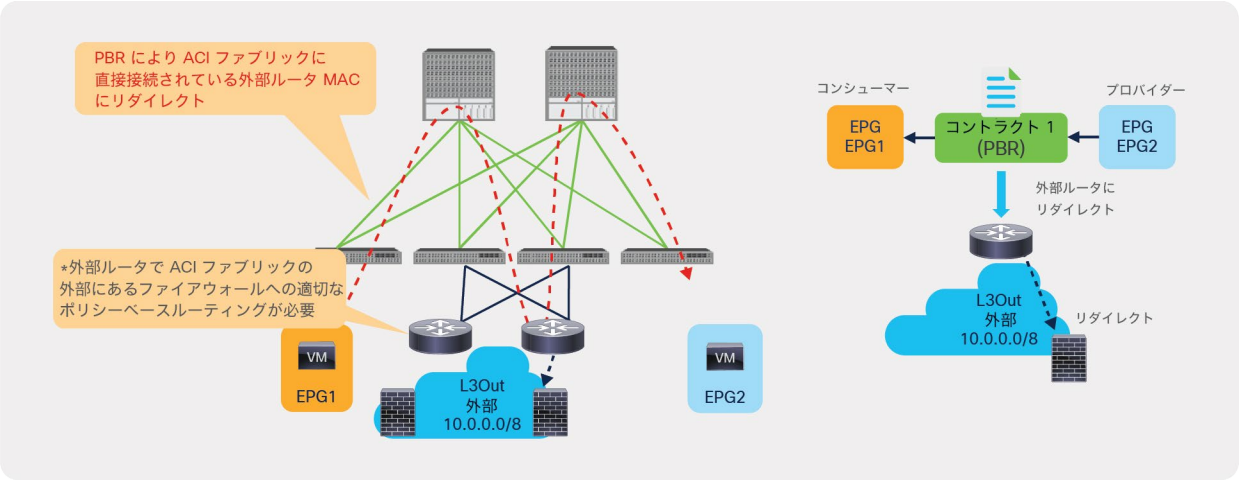


図 182.
ユースケースの例 3：ACI ファブリックに直接接続されていないサービスデバイス

設定

設定フローは、L3 ブリッジドメインにある PBR 接続先を使用する L3 PBR サービスグラフの場合と同じですが、L3Out、L4-L7 デバイス、トラッキングの設定に関する追加の設定要件がいくつかあります。このセクションでは、L3Out 固有の設定に関する考慮事項のなかでも特に PBR 接続先について説明します。一般的な PBR 設定については、以前のセクションを確認してください。

このセクションでは、テナント、VRF、コンシューマーとプロバイダーの BD と EPG の作成方法については説明しません。コンシューマーとプロバイダーの EPG と BD がすでに存在し設定されていることを前提としています。

設定手順は次のとおりです。

1. PBR 接続先の L3Out を作成します。
2. L4-L7 デバイスを作成します。
3. サービスグラフテンプレートを作成します（L3Out にある PBR 接続先を使用する L3 PBR と同じ）。

4. IP SLA モニタリングポリシーを設定します（L3Out にある PBR 接続先には IP-SLA トラッキングが必須です）。
5. PBR ポリシーを作成します。
6. コントラクトにサービスグラフテンプレートを適用します。

L3Out にある PBR 接続先には、次の設定要件があります。

- PBR 接続先がある L3Out は、コンシューマー VRF またはプロバイダー VRF のいずれかにある必要があります。
- SVI、ルーテッド サブインターフェイス、またはルーテッドインターフェイスを使用する L3Out がサポートされます（インフラ L3Out、GOLF L3Out、SDA L3Out、または PBR 接続先にフローティング SVI を使用する L3Out はサポートされません）。
- コンバージェンスを向上させるために、L3Out にある PBR 接続先にはトラッキングが必須です。
- サブネットが 0.0.0.0/0 または 0::0 である L3Out EPG は、PBR 接続先の L3Out EPG としては使用できません*。

詳細については、「要件と設計上の考慮事項」セクションも確認してください。

* これは、サブネットが 0.0.0.0/0 および 0::0 である L3Out EPG に固有の EPG 分類動作が原因です。この問題を回避するには、L3Out EPG に 0.0.0.0/1 と 128.0.0.0/1 を使用してすべてのサブネットをキャッチします。

PBR 接続先の L3Out の作成

PBR 接続先の L3Out を作成する場所は、任意の L3Out と同じです。場所は、[テナント（Tenant）] > [ネットワーク（Networking）] > [L3Outs] です。図 183 の例では SVI インターフェイスを使用していますが、ルーテッドインターフェイスを設定することもできます。フローティング SVI の統合は、PBR 接続先との併用にまだ対応していません。

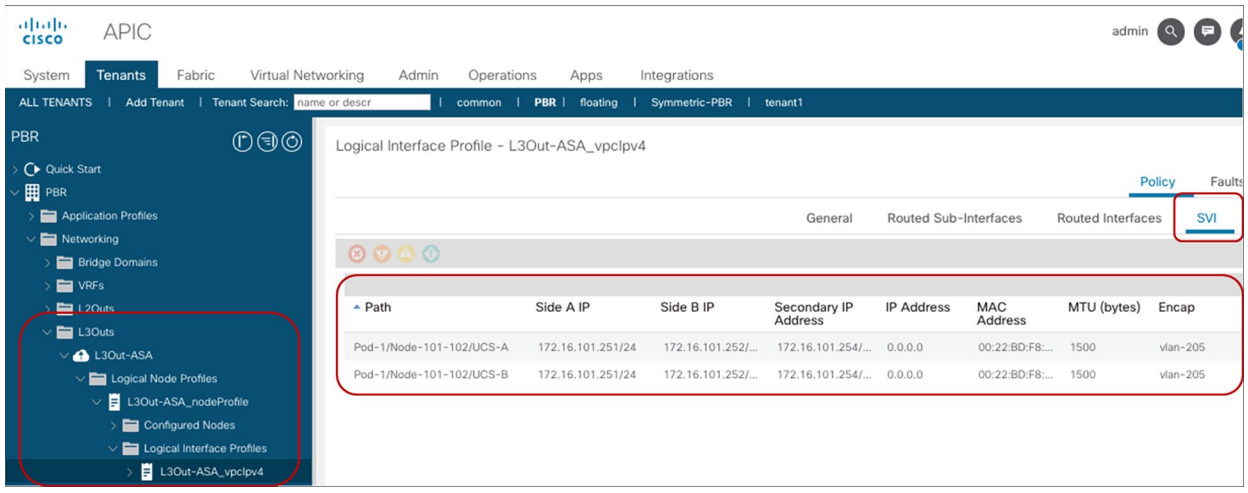


図 183.
L3Out の作成

L4-L7 デバイスの作成

L4-L7 デバイスを作成する場所は、[テナント（Tenant）] > [サービス（Services）] > [L4-L7] > [デバイス（Devices）] です。L4-L7 デバイスが VMM ドメインにある場合でも、L3Out にある PBR 接続先に対しては、具象デバイスインターフェイスでのパス設定が必須です。

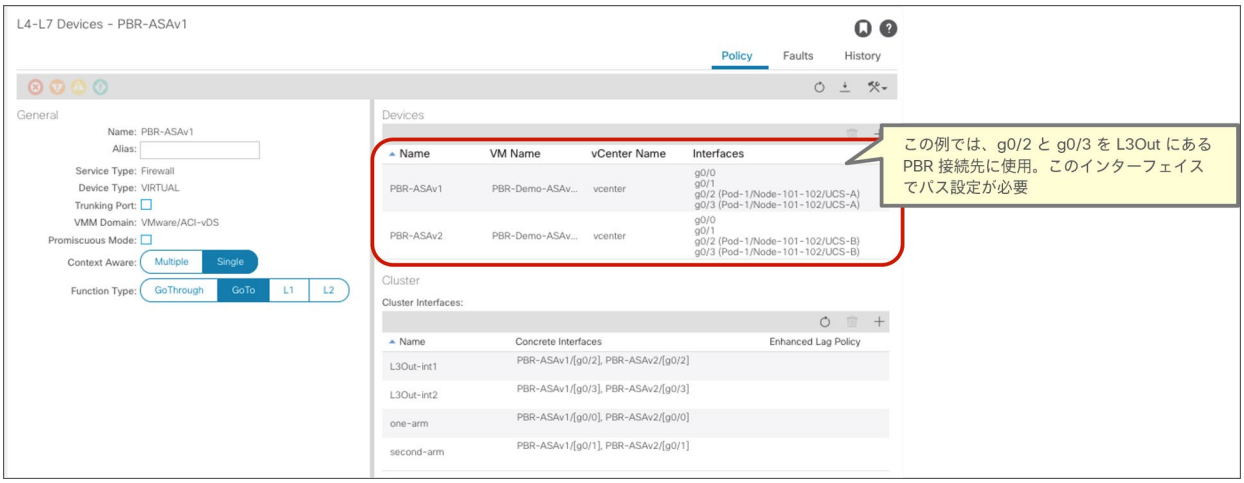


図 184.
L3Out にある PBR 接続先として使用する L4-L7 デバイスの作成

注： APIC は、サービスグラフのレンダリング中に、PBR の L3Out 論理インターフェイスが L4-L7 デバイスの具象インターフェイスと一致しているかどうかをチェックします（図 183 と図 184 のパス設定は一致している必要があります）。一致しない場合（インターフェイスのパス設定が異なる場合など）、APIC でエラーが発生し、サービスグラフのレンダリングが失敗します。

サービスグラフテンプレートの作成

この設定手順は、L3 ブリッジドメインにある PBR 接続先を使用するサービスグラフと同じです。場所は、[テナント（Tenant）] > [サービス（Services）] > [L4-L7] > [サービスグラフテンプレート（Service Graph Templates）] です。

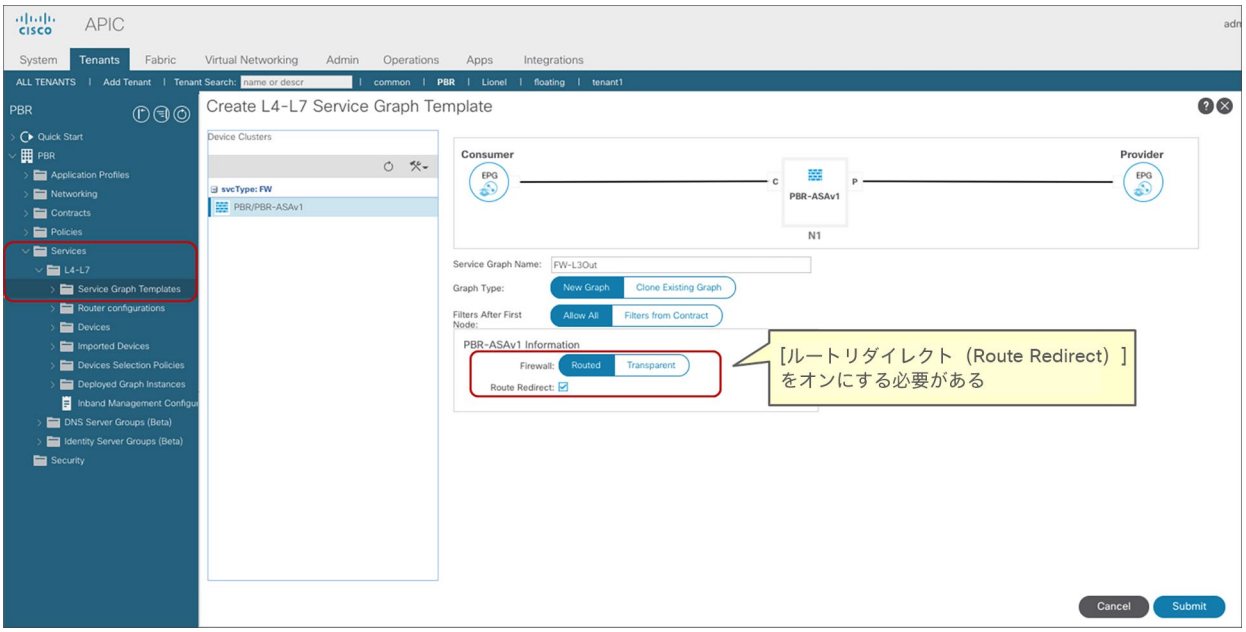


図 185.
サービスグラフテンプレートの作成

IP SLA モニタリングポリシーの設定

L3Out にある PBR 接続先には、IP SLA モニタリングの設定が必須です。設定手順は、L3 ブリッジドメインにある PBR 接続先を使用するサービスグラフと同じです。場所は、[テナント（Tenant）] > [ポリシー（Policies）] > [プロトコル（Protocol）] > [IP SLA] > [IP SLAモニタリングポリシー（IP SLA Monitoring Policies）] です。

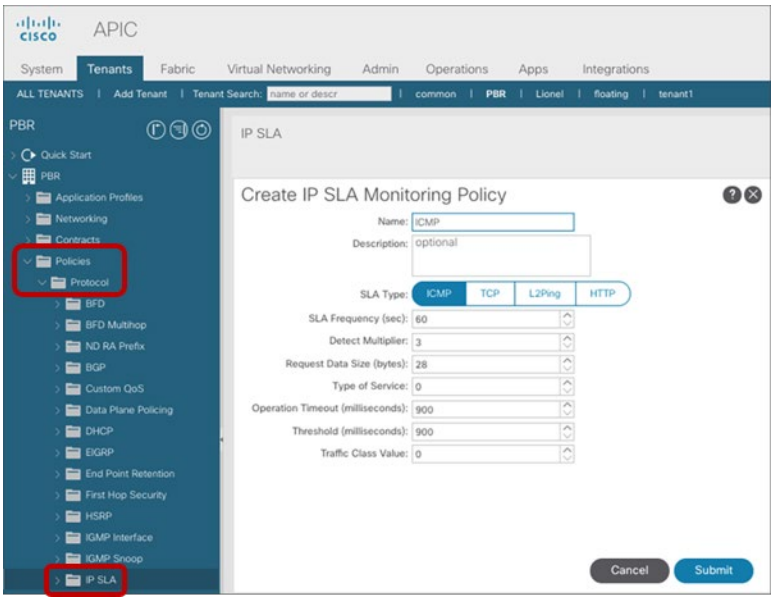


図 186.
IP SLA モニタリングポリシーの作成

PBR ポリシーの作成

PBR ポリシーを作成して、PBR 接続先の IP アドレスと MAC アドレスを APIC に提供します。L3Out にある PBR 接続先にはトラッキングが必須です。トラッキングを有効化するには、リダイレクトヘルスグループを設定する必要があります。設定の場所は、[テナント（Tenant）] > [ポリシー（Policies）] > [プロトコル（Protocol）] > [L4-L7 ポリシーベースリダイレクト（L4-L7 Policy-Based Redirect）] です。

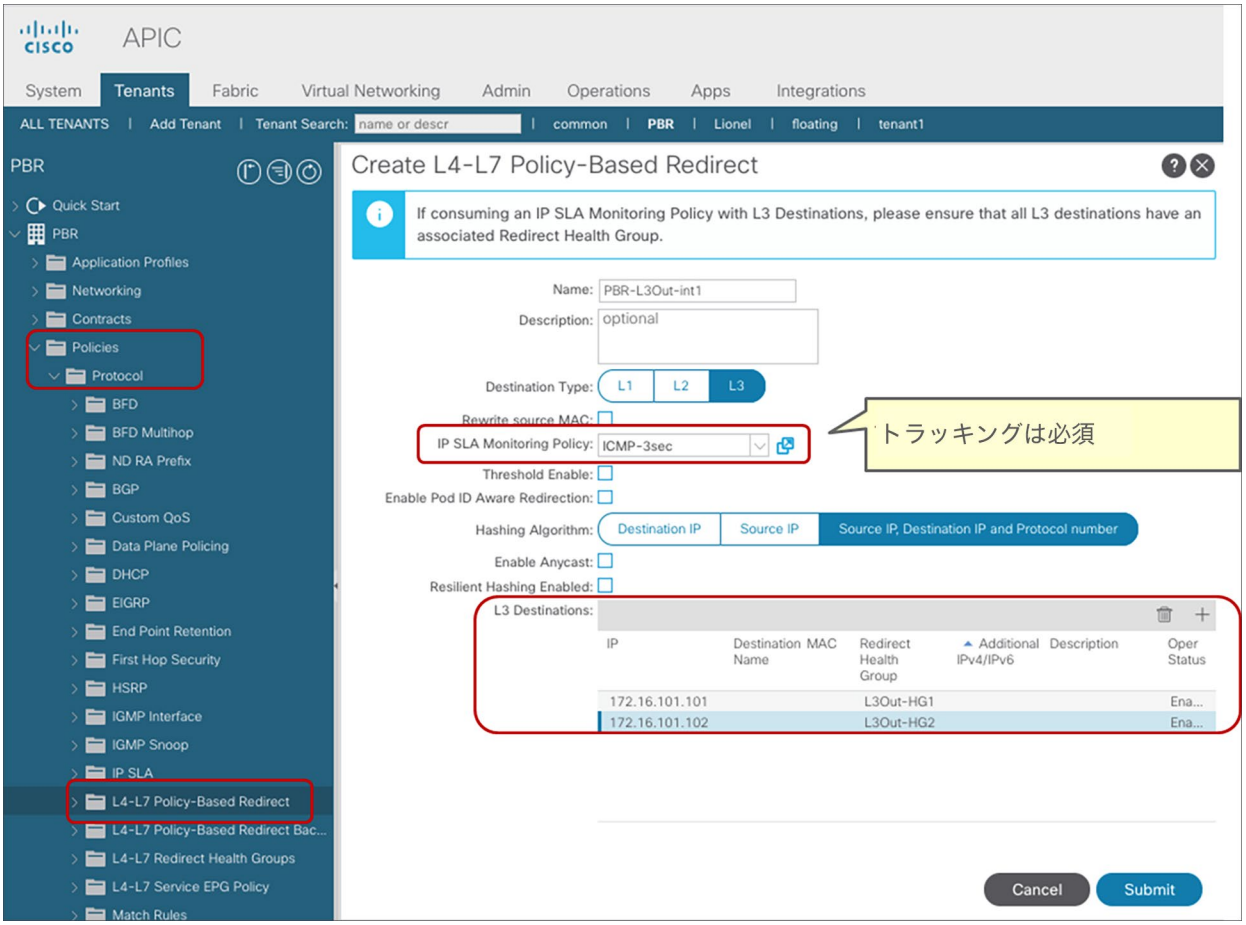


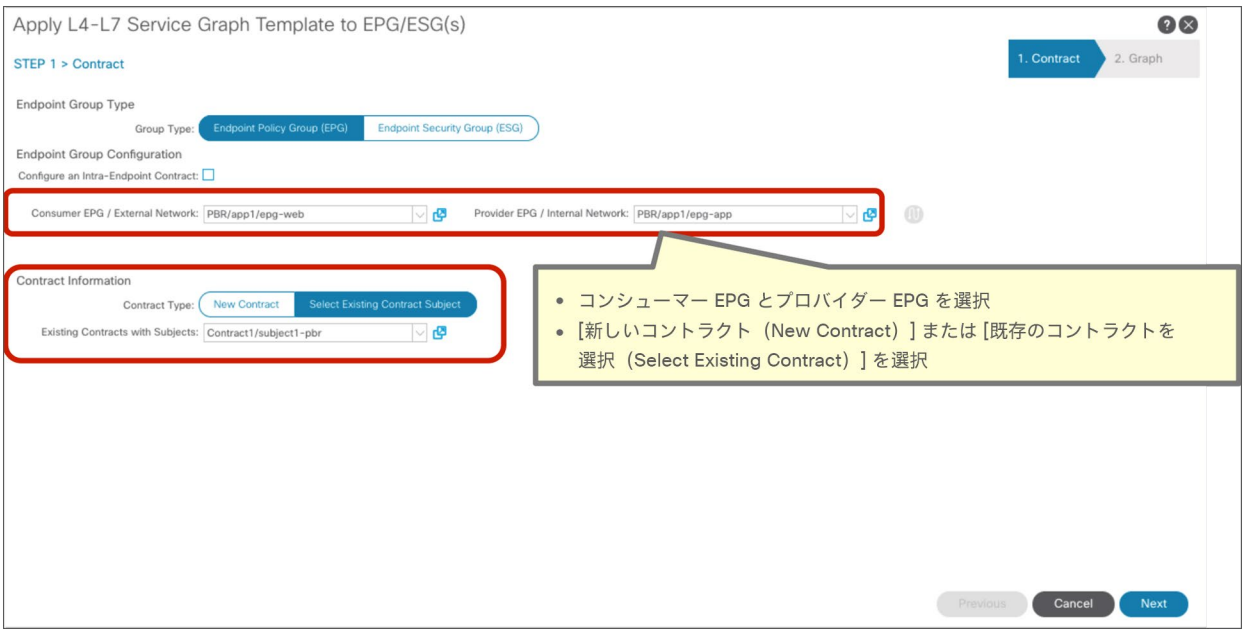
図 187.
PBR ポリシーの作成

コントラクトへのサービスグラフテンプレートの適用

[L4-L7サービスグラフテンプレートの適用（Apply L4-L7 Service Graph Templates）] ウィザードを使用するか、デバイス選択ポリシーを手動で作成して、サービスグラフテンプレートをコントラクトに適用します。この例では、ウィザードを使用しています。ウィザードでは、次の情報を選択するように求められます（図 188）。

- コンシューマー EPG、プロバイダー EPG、サービスグラフを適用するコントラクトサブジェクト
- BD または L3Out、PBR ポリシー、PBR ノードのプロバイダーコネクタとコンシューマーコネクタの各クラスタインターフェイス

場所は、[テナント（Tenant）] > [サービス（Services）] > [L4-L7] > [サービスグラフテンプレート（Service Graph Templates）] です。



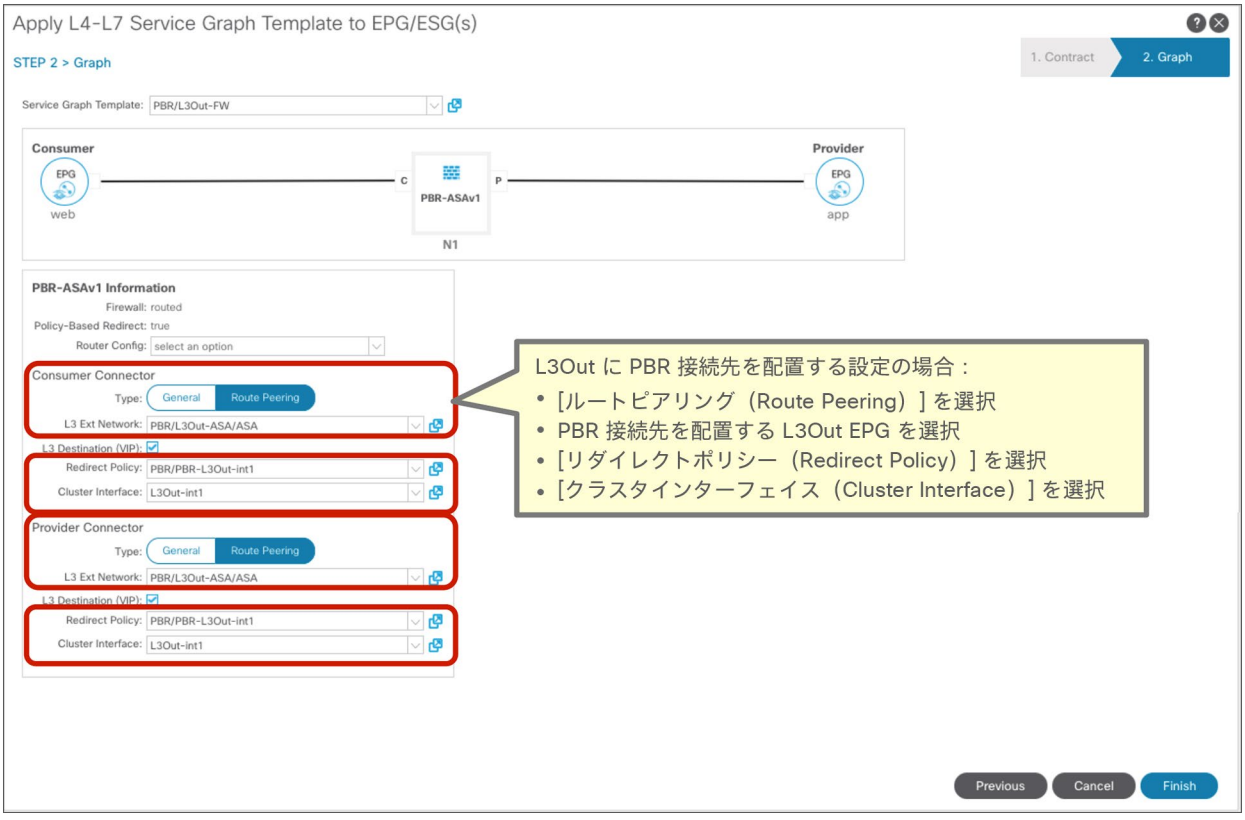


図 188.
サービスグラフテンプレートの適用

サービスグラフテンプレートのウィザードの適用で全手順が完了すると、デバイス選択ポリシーが作成され、サービスグラフがコントラクトサブジェクトに関連付けられます。デバイス選択ポリシーの場所は、[テナント（Tenant）] > [サービス（Services）] > [L4-L7] > [デバイス選択ポリシー（Device Selection Policy）] です。

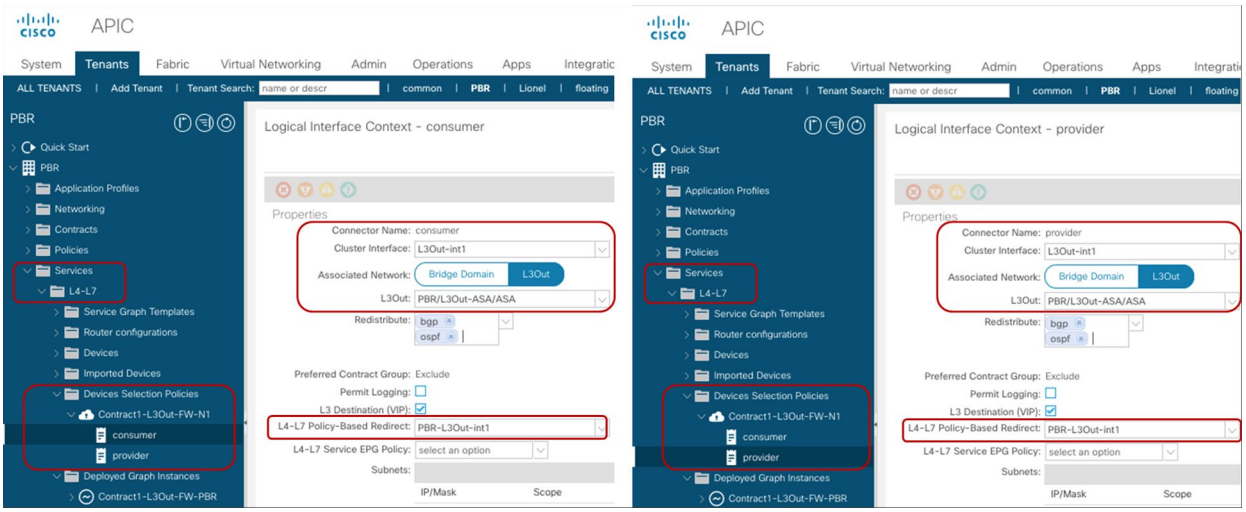


図 189.
デバイス選択ポリシー

すべてが適切に設定されていれば、[展開されたグラフインスタンス（Deployed Graph Instance）] にエラーが表示されないはずです。場所は、[テナント（Tenant）] > [サービス（Services）] > [L4-L7] > [展開されたグラフインスタンス（Deployed Graph Instance）] です。

検証

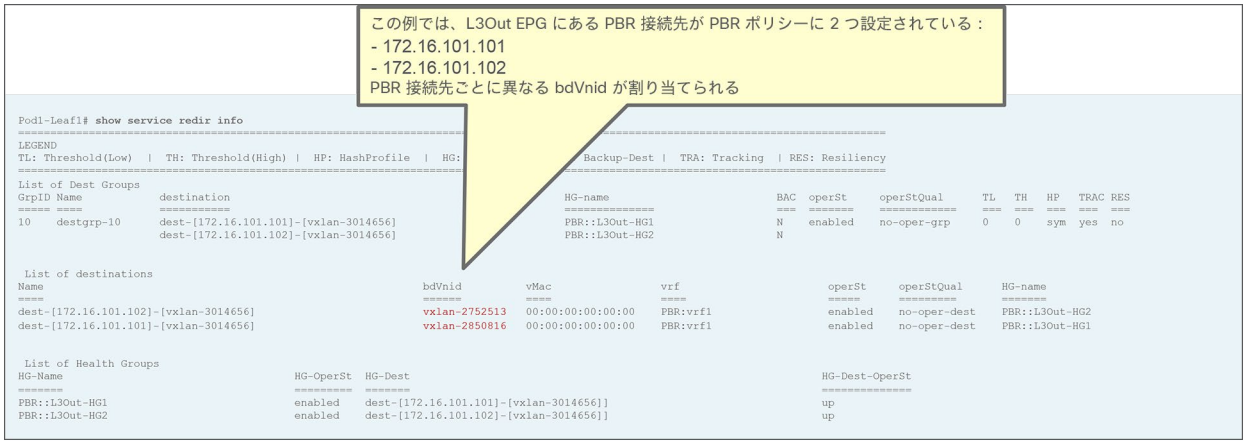
サービスグラフが展開されると、ゾーン分割ルールが更新されます。

ACI が PBR のゾーン分割ルールをプログラムする方法は、PBR 接続先が L3Out にある場合でも通常の PBR 展開の場合と非常によく似ていますが、次のような小さな違いがあります。

- 非表示サービス EPG は、VRF 内コントラクトがある場合でも、グローバル範囲（16 ~ 16384）のクラス ID を使用します（図 190）。
- 複数の L4-L7 デバイスが同じ L3Out を介して接続されている場合でも、一意の bdVnid（VNID：VXLAN インスタンス ID）が各 PBR 接続先（L4-L7 デバイス）に割り当てられます（図 191）。この VNID 情報を使用した転送の動作について次のセクションで説明します。


```
Pod1-Leaf1# show zoning-rule scope 3014656
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |       Action      |       Priority       |
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------+----------------------+
|   4109  |   10   |    0   | implicit |    uni-dir     | enabled | 3014656 |      |      deny,log     |   class-eq-deny(2)   |
|   4101  |    0   | 49153  | implicit |    uni-dir     | enabled | 3014656 |      |       permit      |   any_dest_any(16)   |
|   4102  |    0   |    0   | implicit |    uni-dir     | enabled | 3014656 |      |      deny,log     |   any_any_any(21)    |
|   4103  |    0   |    0   | implarp  |    uni-dir     | enabled | 3014656 |      |       permit      | any_any_filter(17)   |
|   4110  |    0   |   10   | implicit |    uni-dir     | enabled | 3014656 |      |      deny,log     |   class-eq-deny(2)   |
|   4104  |    0   |   15   | implicit |    uni-dir     | enabled | 3014656 |      |      deny,log     | any_vrf_any_deny(22) |
|   4112  |    0   | 32773  | implicit |    uni-dir     | enabled | 3014656 |      |       permit      |   any_dest_any(16)   |
|   4126  | 49155  | 32774  |    5     | uni-dir-ignore | enabled | 3014656 |      | redir(destgrp-10) |    fully_qual(7)     |
|   4135  | 32774  | 49155  |    5     |     bi-dir     | enabled | 3014656 |      | redir(destgrp-10) |    fully_qual(7)     |
|   4128  | 10934  | 32774  |    5     |    uni-dir     | enabled | 3014656 |      |       permit      |    fully_qual(7)     |
|   4127  | 10934  | 49155  | default  |    uni-dir     | enabled | 3014656 |      |       permit      |    src_dst_any(9)    |
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------+----------------------+
```

図 190.
コンシューマーリーフノードとプロバイダーリーフノードのゾーン分割ルール




```
Pod1-Leaf1# show service redir info
========================================================================================================================
LEGEND
TL: Threshold(Low)  |  TH: Threshold(High)  |  HP: HashProfile  |  HG:                    Backup-Dest  |  TRA: Tracking  | RES: Resiliency
========================================================================================================================
List of Dest Groups
GrpID Name            destination                                   HG-name                       BAC  operSt    operStQual      TL   TH   HP   TRAC RES
===== ====            ===========                                   =======                       ===  =======   ==========      ===  ===  ===  ===  ===
10    destgrp-10      dest-[172.16.101.101]-[vxlan-3014656]         PBR::L3Out-HG1                N    enabled   no-oper-grp     0    0    sym  yes  no
                      dest-[172.16.101.102]-[vxlan-3014656]         PBR::L3Out-HG2                N


 List of destinations
Name                                          bdVnid          vMac               vrf                operSt    operStQual      HG-name
====                                          ======          ====               ===                =====     ==========      =======
dest-[172.16.101.102]-[vxlan-3014656]         vxlan-2752513   00:00:00:00:00:00  PBR:vrf1           enabled   no-oper-dest    PBR::L3Out-HG2
dest-[172.16.101.101]-[vxlan-3014656]         vxlan-2850816   00:00:00:00:00:00  PBR:vrf1           enabled   no-oper-dest    PBR::L3Out-HG1


 List of Health Groups
HG-Name                          HG-OperSt  HG-Dest                                          HG-Dest-OperSt
=======                          =========  =======                                          ==============
PBR::L3Out-HG1                   enabled    dest-[172.16.101.101]-[vxlan-3014656]]           up
PBR::L3Out-HG2                   enabled    dest-[172.16.101.102]-[vxlan-3014656]]           up
```

図 191.
PBR 接続先のステータス

転送の動作

このセクションでは、前のセクションの設定例に基づいて、転送の動作について説明します。図 192 に、Web EPG がコンシューマー EPG、アプリケーション EPG がプロバイダー EPG で、両者間に L3Out にある PBR 接続先を使用するサービスグラフを持つコントラクトが設定されている例を示します。この例では、ワンアームファイアウォール設計と VRF 内コントラクトを使用していますが、ツーアームサービスノード設計と VRF 間コントラクトも可能です。この例では、PBR ポリシーは両方向の入力リーフに適用されますが、ポリシーが適用される場所は、コントラクトの設定とエンドポイント学習のステータスによって異なる場合があります。

前のセクションの図 190 と図 191 に示すように、非表示サービス EPG が内部で作成され、一意の bdVNid が各 PBR 接続先に割り当てられます。

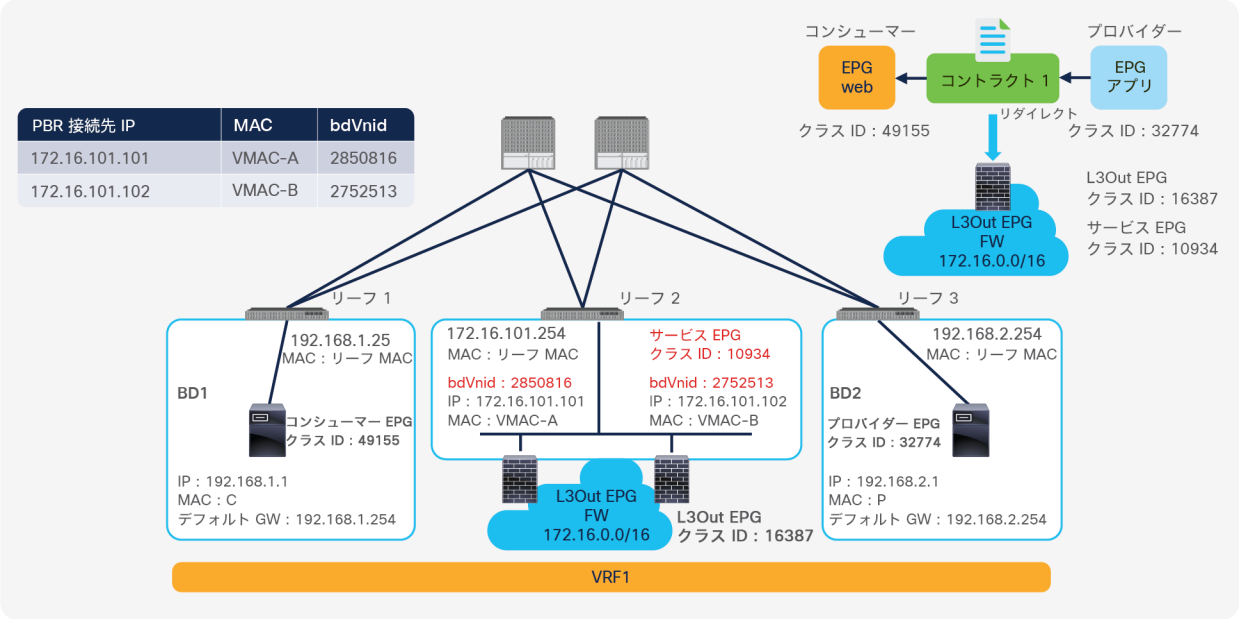


図 192.
トポロジの例：L3Out にある PBR 接続先

コンシューマーエンドポイントが、プロバイダーエンドポイントを接続先とするトラフィックを生成します。リーフ 1 が接続先エンドポイントをすでに学習している場合、リーフ 1 が送信元と接続先の EPG のクラス ID を解決できるため、リーフ 1 で PBR が実行されます。ここで、VXLAN ヘッダーの接続先 VNID が PBR 接続先に割り当てられた bdVNid に設定されます。これが選択された PBR 接続先を示します。接続先 TEP はサービスリーフノード TEP です。PBR 接続先が L3 ブリッジドメインにある場合と異なり、PBR 接続先へのリダイレクトトラフィックは L2 スパインプロキシに送信されません。これは、コンシューマーリーフとプロバイダーリーフがルーティングテーブルから PBR 接続先サブネット（この場合は 172.16.101.0/24、リーフ 2 から BGP によってアドバタイズされる L3Out 論理インターフェイスのサブネット）へのルートを取得し、パケットをサービスリーフノード TEP に直接送信できるためです。

bdVNid ごとにそれに対応する内部 VRF が、コンシューマー VRF またはプロバイダー VRF とは異なるものとしてサービスリーフに展開されます。この内部 VRF のルーティングテーブルには、PBR 接続先の MAC アドレスをネクストホップとするデフォルトルート（この例では VMAC-A 経由 0.0.0.0/0）が含まれています。VMAC-A は内部 VRF のエンドポイントではありませんが、サービスリーフの転送テーブルによってトラフィックを VRF1 の VMAC-A に転送することが可能になります。したがって、サービスリーフに到着したトラフィックは、接続先 VNID が PBR 接続先となっているため、対応する PBR 接続先に転送されます。

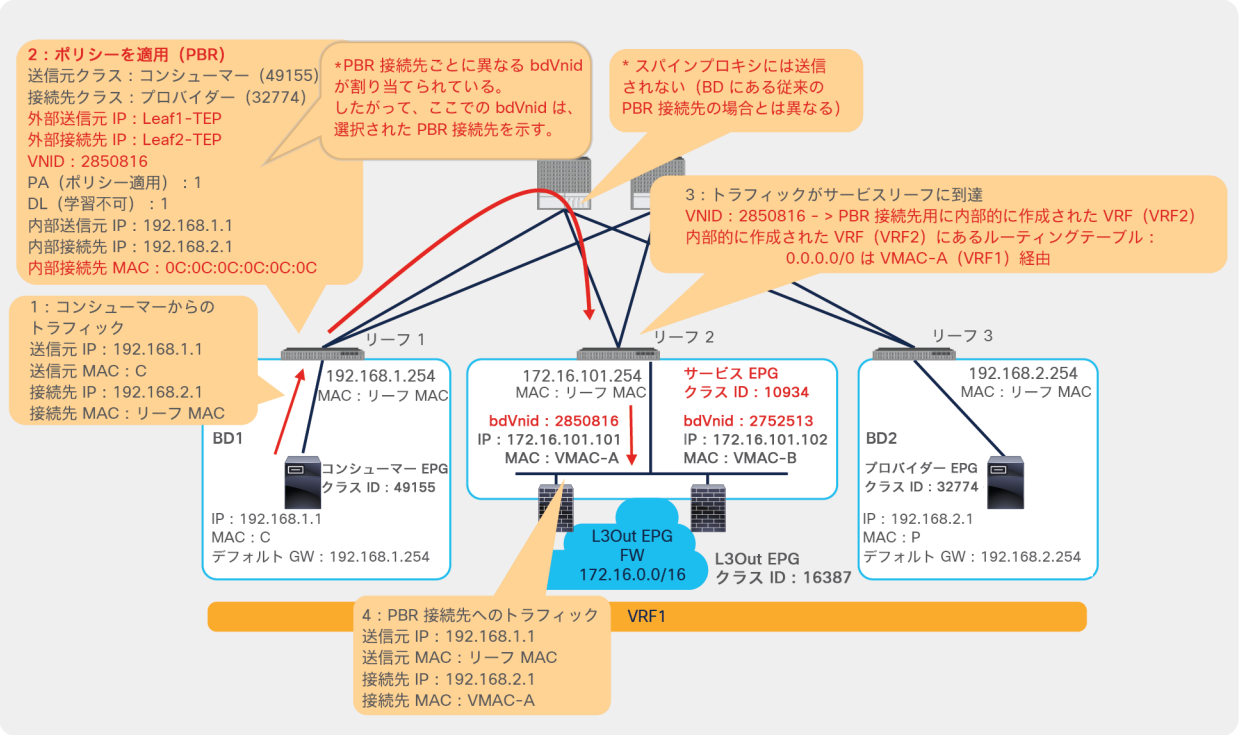


図 193.
トラフィックフローの例：コンシューマーからプロバイダーへのトラフィックは PBR ノードにリダイレクトされる

注： 内部 VRF は、サービスリーフノードにのみ展開されます。サービスリーフノードでの VRF の拡張性を考慮する必要があります。たとえば、PBR ポリシーに PBR 接続先が 10 個あり、すべてが同じサービスリーフノードに接続されている場合、サービスリーフノードに内部 VRF が 10 個展開されます（PBR 接続先ごとに 1 つの内部 VRF が作成されます）。

その後、トラフィックは PBR ノードを通過し、ACI ファブリックに戻ります。L3Out 論理インターフェイスに到着しても、PBR 接続先がある L3Out の下にある L3Out EPG サブネットと送信元 IP アドレスが一致しない場合、トラフィックは、PBR 接続先として使用された L3Out EPG（この例ではクラス ID 16387）ではなく非表示サービス EPG に分類されます（この例ではクラス ID 10934）。このように、ACI ファブリックは、PBR 後に戻ってくるトラフィックと、PBR を使用せずに L3Out 論理インターフェイスに到着するトラフィックを区別できます。この例では、サービスグラフの展開によって作成されたゾーン分割ルールにより、非表示サービス EPG からプロバイダー EPG（10934 から 32774）へのトラフィックが許可されます（図 190）。

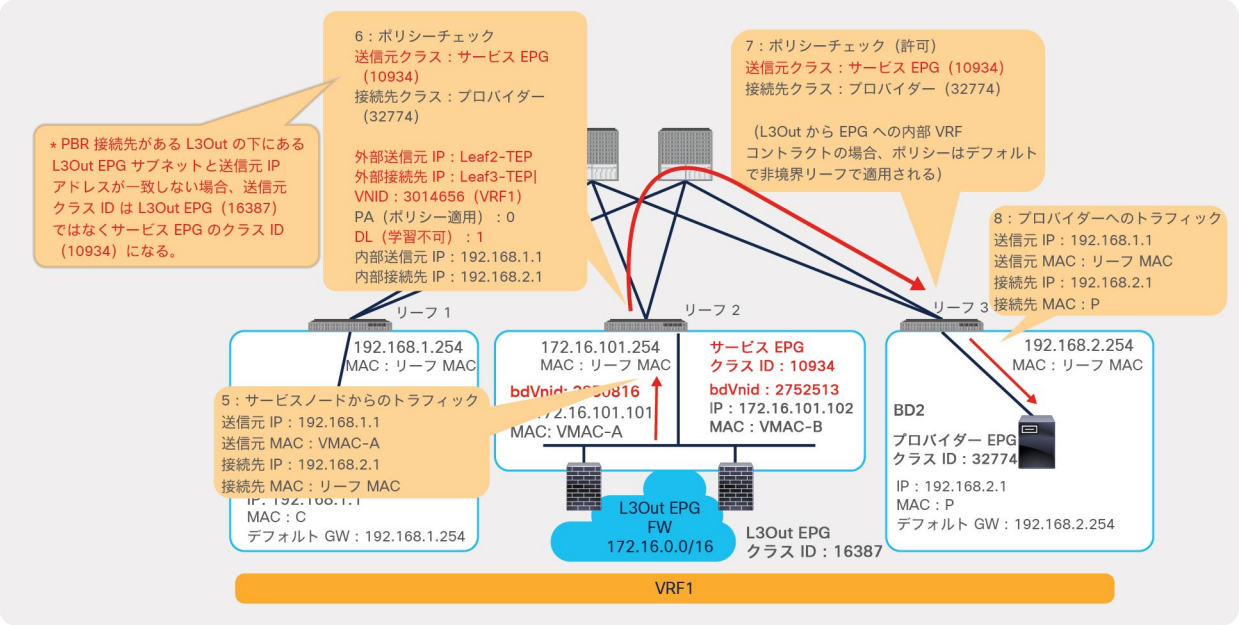


図 194.
トラフィックフローの例：PBR ノードからプロバイダー

トラフィックが PBR を使用せずに ACI L3Out 論理インターフェイスに到着した場合、図 195 に示すように、送信元 IP アドレスは L3Out EPG サブネットと一致します。非表示サービス EPG ではなく、L3Out EPG（この例ではクラス ID 16387）に分類されます。16387 から 32774 の許可ルールがない場合、トラフィックがドロップされます。このルールは、サービスグラフの展開によって作成されたゾーン分割ルールには含まれません（図 190）。

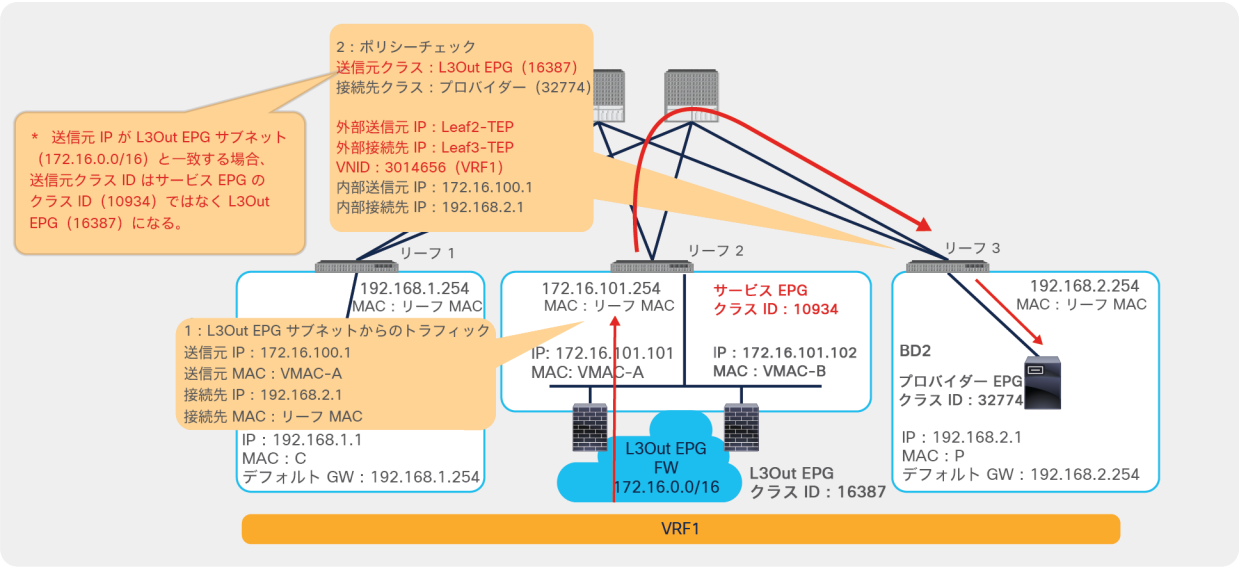


図 195.
トラフィックフローの例：PBR を使用しない L3Out からのトラフィック

以下は、L3Out にある PBR 接続先に固有の転送動作の概要です。

- サービスグラフが VRF 内コントラクトに適用される場合でも、グローバル範囲（16 ~ 16384）のクラス ID を使用する非表示サービス EPG が作成されます。
- 一意の bdVnid（VNID：VXLAN インスタンス ID）が各 PBR 接続先に割り当てられます。
- bdVNid ごとに 1 つの内部 VRF がサービスリーフに作成されます。
- リーフノードが PBR ポリシーを適用するとき、VRF 間コントラクトの場合であってもスパインプロキシは使用されません。

設計上の考慮事項

このセクションでは、次の設計上の考慮事項について例を用いて説明します。

- 外部ルータの背後にある PBR 接続先 IP
- ツーアーム設計
- ロードバランサのキープアライブ

L3Out にある PBR 接続先に関連する一般的な考慮事項については、「要件と設計上の考慮事項」を参照してください。

外部ルータの背後にある PBR 接続先 IP

PBR 接続先 IP が外部ルータの背後にある場合、ACI リーフノードとサービスノードの間にある外部ルータには、トラフィックを管理するための適切なポリシーベースルーティングの設定が必要です。これは、APIC が ACI ファブリックの外部にあるネットワークを構成しないためです。

図 196 に、1 つの外部ルータと 1 つの PBR 接続先 IP からなるトポロジの例を示します。この場合、サービスノード IP が PBR 接続先 IP となり、IP-SLA トラッキングに使用されます。ACI ファブリックに直接接続されている外部ルータの MAC が PBR 接続先 MAC となり、リダイレクトに使用されます。

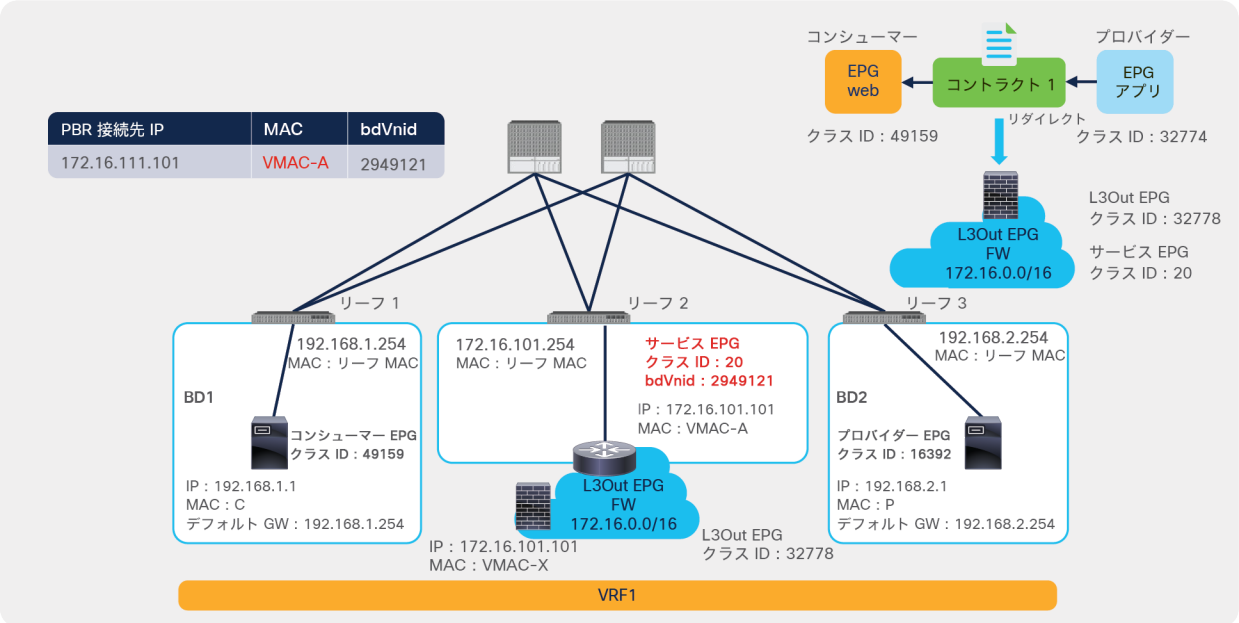


図 196.
トラフィックフローの例：PBR 接続先 IP が外部ルータの背後にある場合

図 197 に示すように、リダイレクトのメカニズムは図 193 に示した例と同じです。

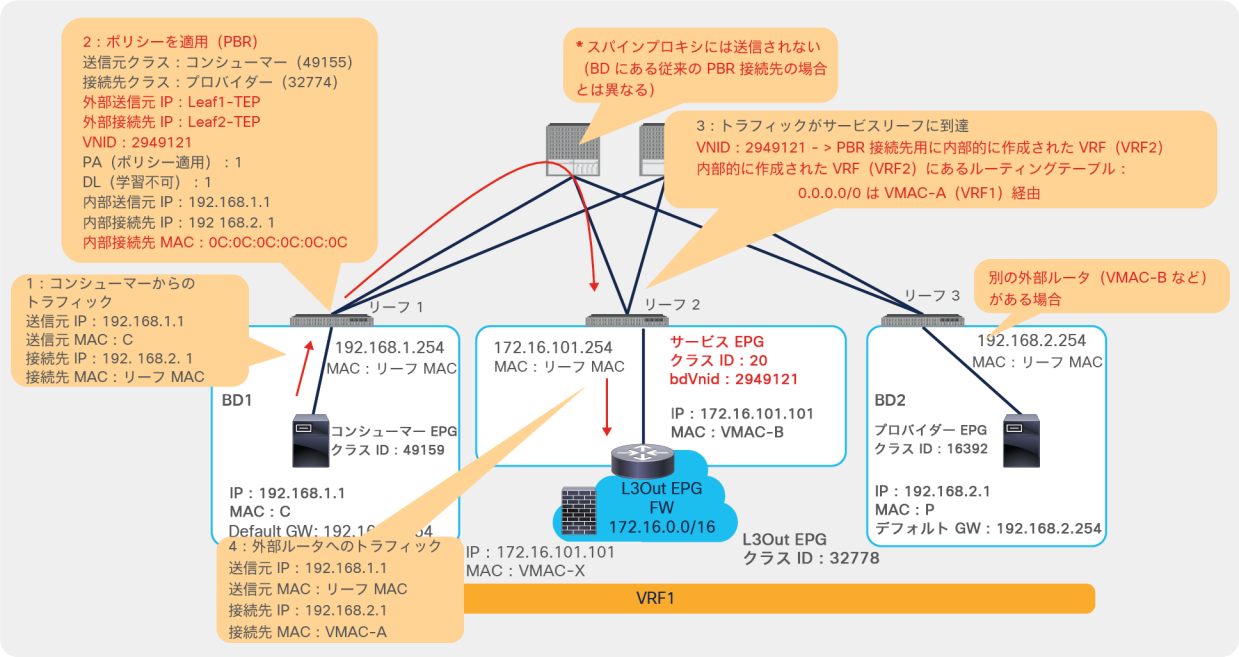


図 197.
トラフィックフローの例：コンシューマーからプロバイダーへのトラフィックが外部ルータにリダイレクトされる

リダイレクト後、外部ルータが ACI ファブリックの外部にあるサービスノードにトラフィックを適切に転送する必要があります（この例のステップ 5）。また、サービスノードが外部ルータにトラフィックを送り返した後、外部ルータがトラフィックを ACI ファブリックに送り返す必要があります（この例のステップ 6）。

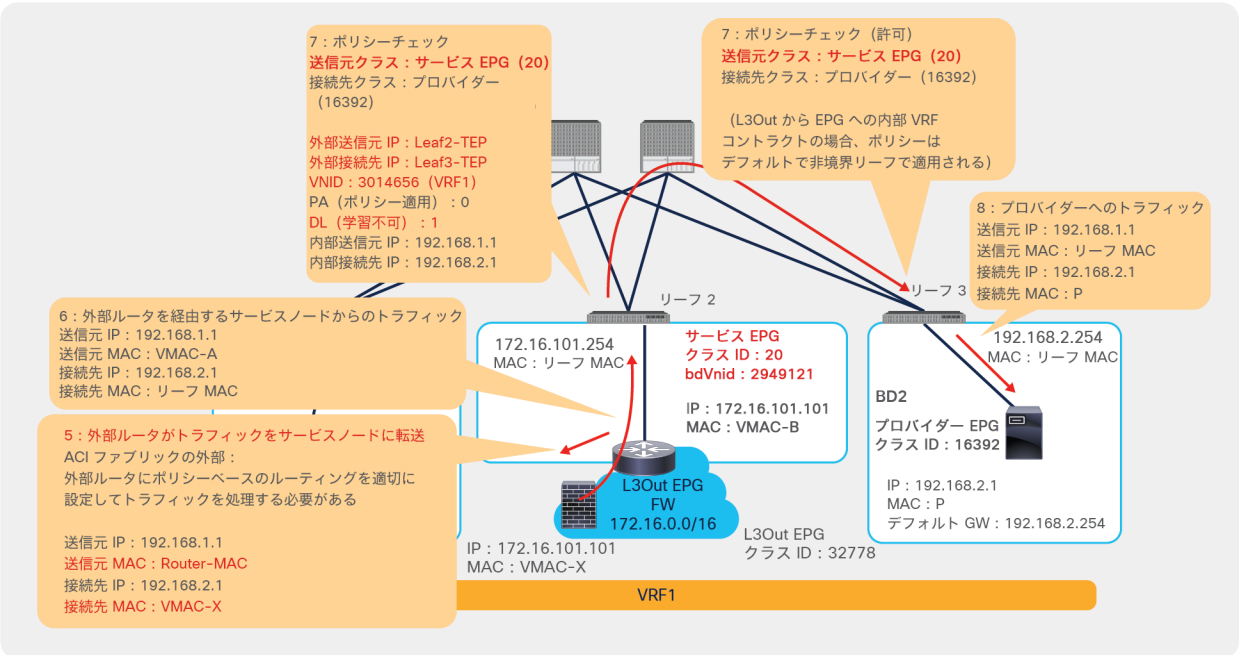


図 198.
トラフィックフローの例：PBR ノードからプロバイダー

図 199 に、2 つの外部ルータと 1 つの PBR 接続先 IP からなるトポロジの例を示します。この場合、サービスリーフノードの内部 VRF には 2 つの ECMP デフォルトルートがあります。トラフィックは、ハッシュに基づいて、いずれかの外部ルータ（この例では VMAC-A または VMAC-B）に転送されます。外部ルータが 3 つ以上ある場合でも、内部 VRF のデフォルトルートで使用されるネクストホップは最大 2 つです。

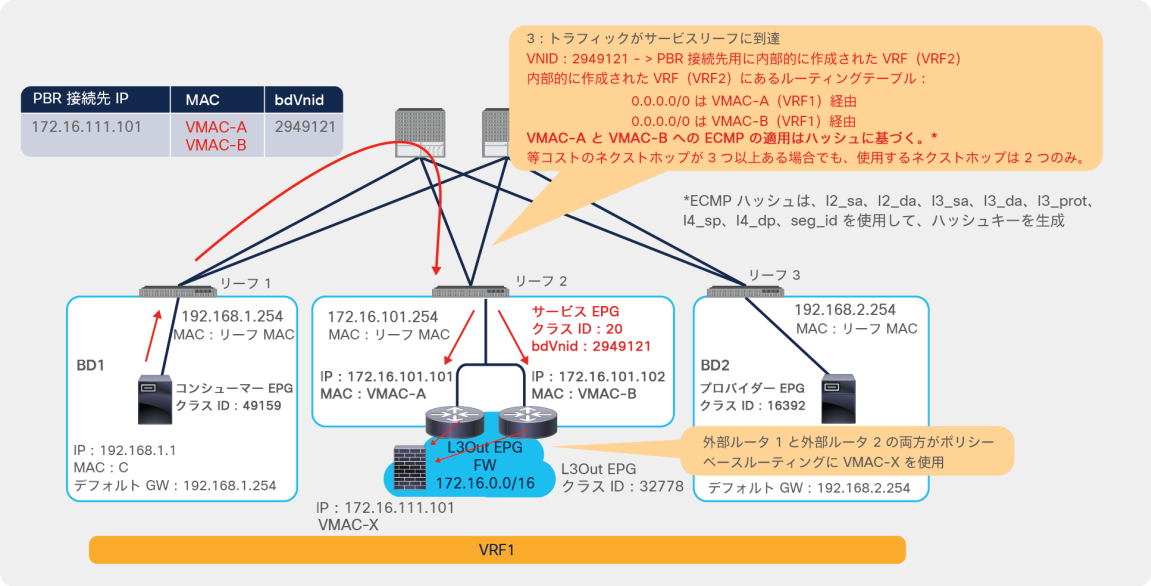


図 199.
トラフィックフローの例：外部ルータが複数ある場合

図 200 に、1 つの外部ルータと 2 つの PBR 接続先 IP からなるトポロジの例を示します。この場合、各 PBR 接続先 IP に一意の bdVNid が割り当てられますが、PBR 接続先 MAC は外部ルータ MAC と同じになります。したがって、負荷分散の動作は外部ルータの動作に依存します。トラフィックの対称性を維持するために、外部ルータが着信トラフィックとリターントラフィックを同じサービスノードに送信する必要があります。

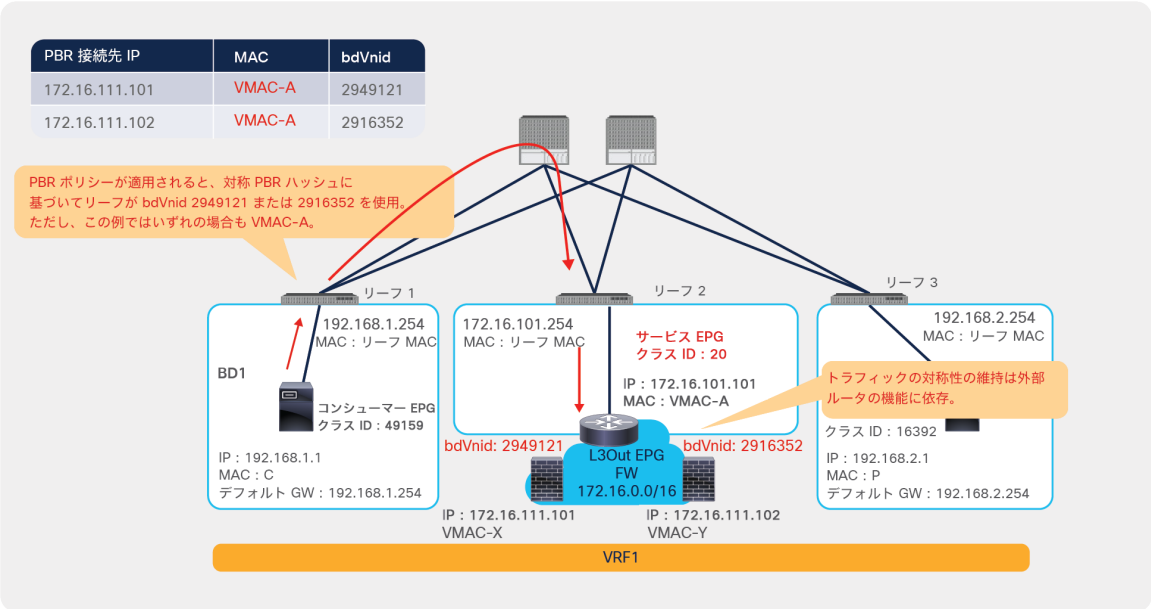


図 200.
トラフィックフローの例：1 つの外部ルータと 2 つの PBR 接続先がある場合

ツーアーム設計

サービスノードがツーアーム設計によって ACI ファブリックに接続されている場合、サービスノードに適切なルーティングテーブルが必要です。図 201 に機能する例を示し、図 202 に機能しない例を示します。

プロバイダーを接続先とするトラフィックは、サービスデバイスのプロバイダーコネクタを介して送信され、コンシューマーを接続先とするトラフィックは、サービスデバイスのコンシューマーコネクタを介して送信される必要があります。そうしないと、コンシューマーコネクタからプロバイダーへのトラフィックとプロバイダーコネクタからコンシューマーへのトラフィックを許可するゾーン分割ルールがないため、トラフィックがドロップする可能性があります。

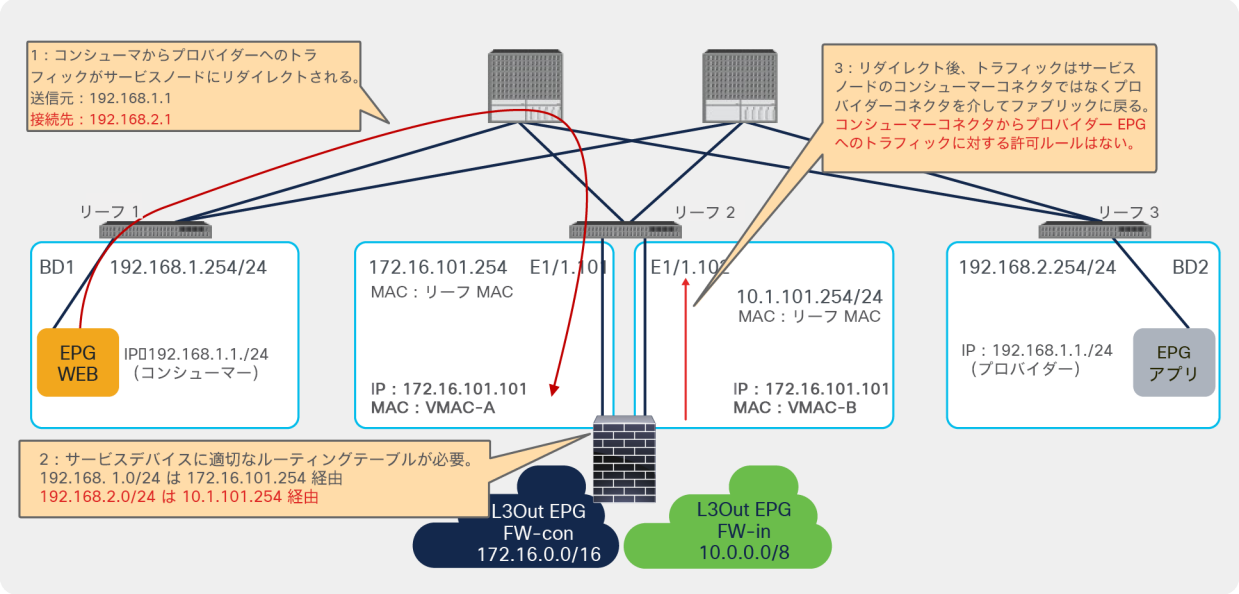


図 201.
有効なツーアーム設計の例

同じリーフ上の同じ VRF で OSPF または EIGRP を使用する 2 つの L3Out がサービスデバイスに接続されている場合、2 つの隣接関係を持つ単一の OSPF セッションまたは EIGRP セッションがサービスデバイスとの間で形成されます。ACI ファブリックが同じリーフ上の同じ VRF で 2 つのルータ ID を持てないためです。そのため、サービスリーフで等コストマルチパス（ECMP）ルーティングが発生し、トラフィックがドロップする可能性があります。可能な設計オプションは次のとおりです。

- OSPF または EIGRP の代わりに BGP またはスタティックルートを使用
- 個別の VRF を使用
- L3Out ごとに異なるサービスリーフノードを使用

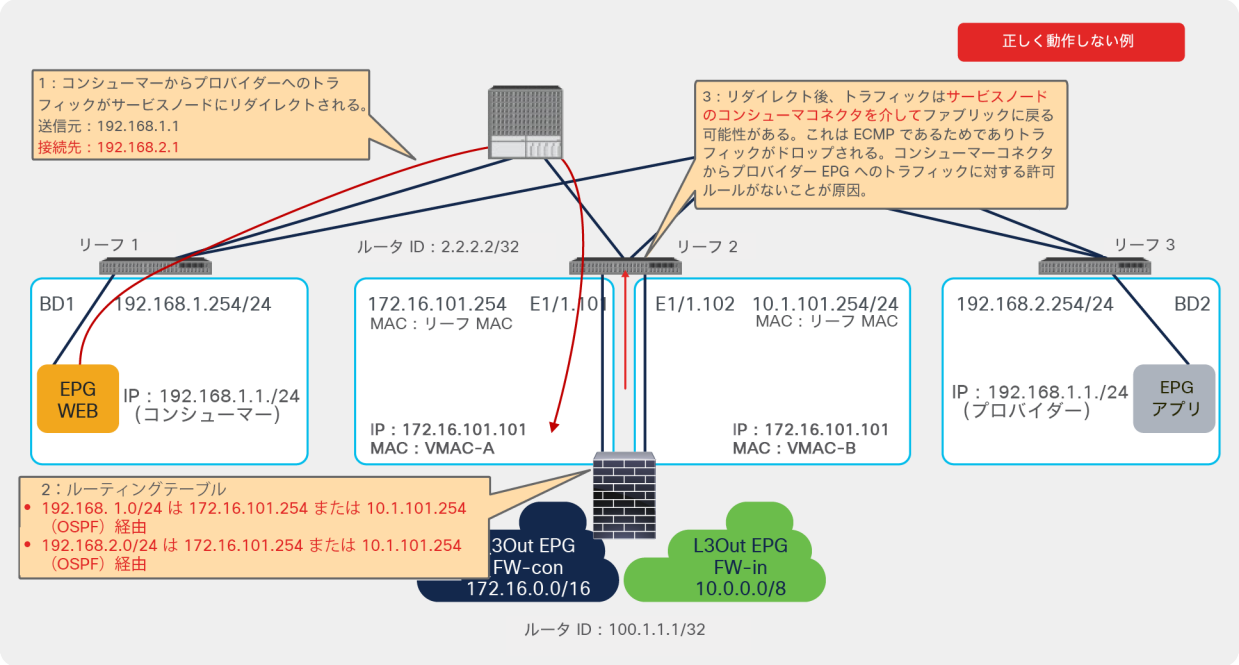


図 202.
正しく動作しないツーアーム設計の例

ロードバランサのキープアライブに関する考慮事項

設計によっては、L4-L7 デバイス（PBR 接続先でもある）がファブリック内のエンドポイントとの間で直接トラフィックを送受信する必要があります。その一例がロードバランサの展開です。ロードバランサはキープアライブを送信して、トラフィックを分散するサーバーの到達可能性と活性度を確認する必要があります。これらの設計では、L4-L7 デバイスと通常の EPG の間のトラフィックを許可する方法を理解する必要があります。さらに、L4-L7 デバイスが L3Out に接続されている場合は、L3Out EPG（L4-L7 デバイスが接続されている）と通常の EPG の間のトラフィックを許可する方法も理解する必要があります。

デフォルトでは、コンシューマー EPG またはプロバイダー EPG と非表示サービス EPG の間の双方向の許可ルールは作成されません。PBR 接続先との直接通信が必要な場合、双方向の許可ルールが必要になることがあります（ロードバランサのキープアライブトラフィックを許可する場合など）。L3 ブリッジドメインに PBR 接続先がある場合の例については、「直接接続オプション」セクションで説明します。このセクションでは、L3Out にある PBR 接続先を使用する例について説明します。

表 21 に、サービス EPG、L3Out EPG、通常の EPG の可能なさまざまな組み合わせを、PBR 接続先との通信を許可する方法に関連付けてまとめています。EPG1 と EPG2 の列は、プロバイダーとコンシューマーの EPG タイプの可能な組み合わせを表します。EPG1 と EPG2 はプロバイダーの場合もコンシューマーの場合もあります。EPG1 がプロバイダーの場合、EPG2 はコンシューマーです。同様に、EPG2 がプロバイダーの場合、EPG1 はコンシューマーです。この表の見方としては、L4-L7 デバイスが L3 ブリッジドメインに接続されている PBR 設計の場合は行 1 を、L4 -L7 デバイスが PBR 接続先として L3Out に接続されている PBR 設計の場合は行 2 を、1 つの L4-L7 デバイスが PBR 接続先として L3Out に接続され、別の L4-L7 デバイスが PBR 接続先として L3 ブリッジドメインに接続されているマルチノードのサービスグラフの場合は行 3 を参照してください。

表 21. PBR 接続先として使用される L4-L7 デバイスとの通信を許可するオプション

EPG1	EPG2	コメント
L3 ブリッジドメインにあるサービス EPG	コンシューマー/プロバイダー EPG、コンシューマー/プロバイダー L3Out EPG、または L3 ブリッジドメインにあるサービス EPG（マルチノードサービスグラフ）	対応 「直接接続」を有効にする必要があります。
L3Out にある PBR 接続先に使用される L3Out EPG（非表示サービス EPG ではない）	EPG または L3Out EPG	対応 L3Out にある PBR 接続先に使用される L3Out EPG と EPG または L3Out EPG との間でコントラクトを作成できます。
L3Out にある PBR 接続先に使用される L3Out EPG（非表示サービス EPG ではない）	L3 ブリッジドメインにあるサービス EPG	ACI リリース 5.2 では未対応

このセクションでは、表 21 の行 2 と行 3 のユースケースについて説明します。行 1 のユースケースについては、「直接接続オプション」セクションで説明しています。

図 203 に、表 21 の行 2 にあるユースケースの例としてファイアウォールを挿入する場合を示します。ファイアウォールを挿入するために PBR を使用するコントラクトが、EPG1 と EPG2 の間に設定されています。EPG2 のエンドポイントが L3Out EPG サブネットにあるファイアウォール IP と直接通信する必要がある場合、L3Out EPG（非表示サービス EPG ではない）から EPG2 へのコントラクトを手動で設定する必要があります。サービスグラフの展開の一環として非表示サービス EPG からプロバイダー EPG（この例では 400 から 200）へのトラフィックの許可ルールが作成されたとしても、L3Out EPG と EPG2 の間に双方向の許可ルールが作成されないためです。

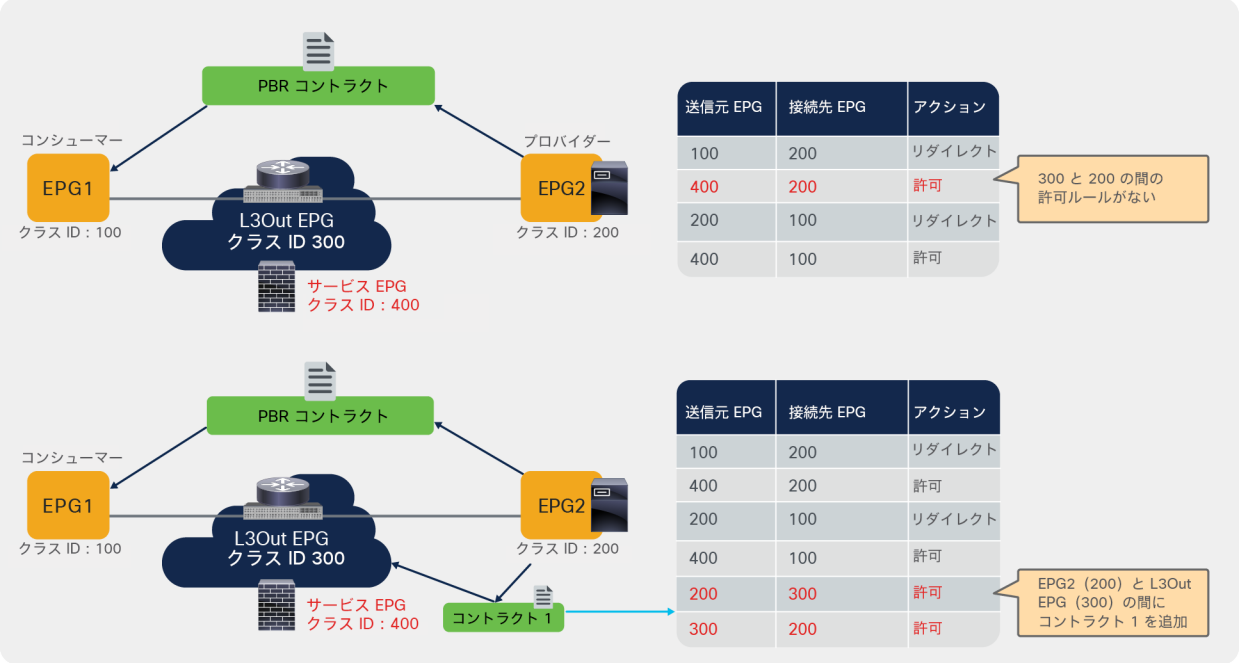


図 203.
プロバイダー EPG と PBR 接続先に使用される L3Out EPG の間のトラフィックを許可

図 204 に、表 21 の行 2 にあるユースケースの例としてロードバランサを挿入する場合を示します。ロードバランサを挿入するために単方向 PBR を使用するコントラクトが、EPG1 と EPG2 の間に設定されています。ロードバランサからプロバイダーエンドポイントへのキープアライブトラフィックに使用されるロードバランサ IP が L3Out EPG サブネットに属していることを前提としています。

非表示サービス EPG からプロバイダー EPG へのトラフィックに対する許可ルールがサービスグラフの展開の一環として作成されます。一方、L3Out EPG とプロバイダー EPG に双方向の許可ルールはありません（この例では 300 から 200 および 200 から 300）。ロードバランサとプロバイダーエンドポイントの間のキープアライブトラフィックを許可するには、L3Out EPG（非表示サービス EPG ではない）から EPG2 へのコントラクトを手動で設定する必要があります。

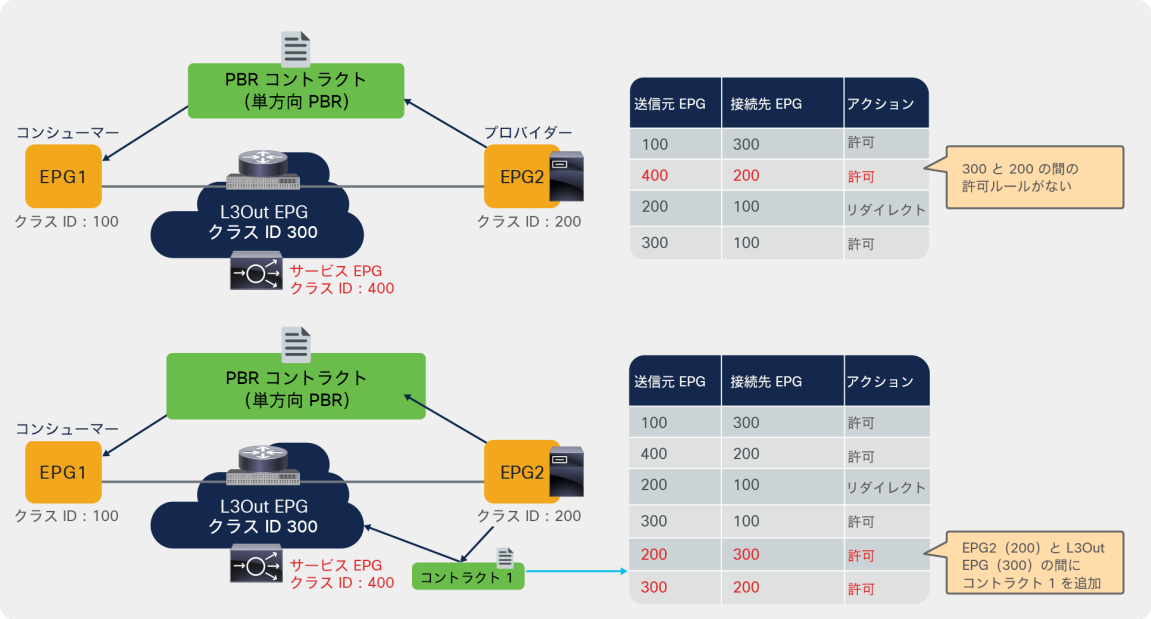


図 204.
プロバイダー EPG と PBR 接続先に使用される L3Out EPG の間のロードバランサによるキープアライブトラフィックを許可

図 205 に、表 21 の行 3 にあるユースケースの例を示します。マルチノード PBR を使用するコントラクトが、EPG1 と EPG2 の間に設定されています。APIC リリース 5.2(1g) では、L3Out EPG サブネットにある最初のノード IP と L3 ブリッジドメインにある 2 番目のノード IP の間に双方向の許可ルールを追加できません。これは、L3 ブリッジドメインにあるサービス EPG とのコントラクトを手動で追加するオプションがないためです。したがって、ノード間の直接通信が必要な場合、サービスグラフのノード間コネクタで L3Out にある PBR 接続先と L3 ブリッジドメインにある PBR 接続先を混在させることはできません。回避策は、サービス EPG も含む vzAny コントラクトを使用することです。

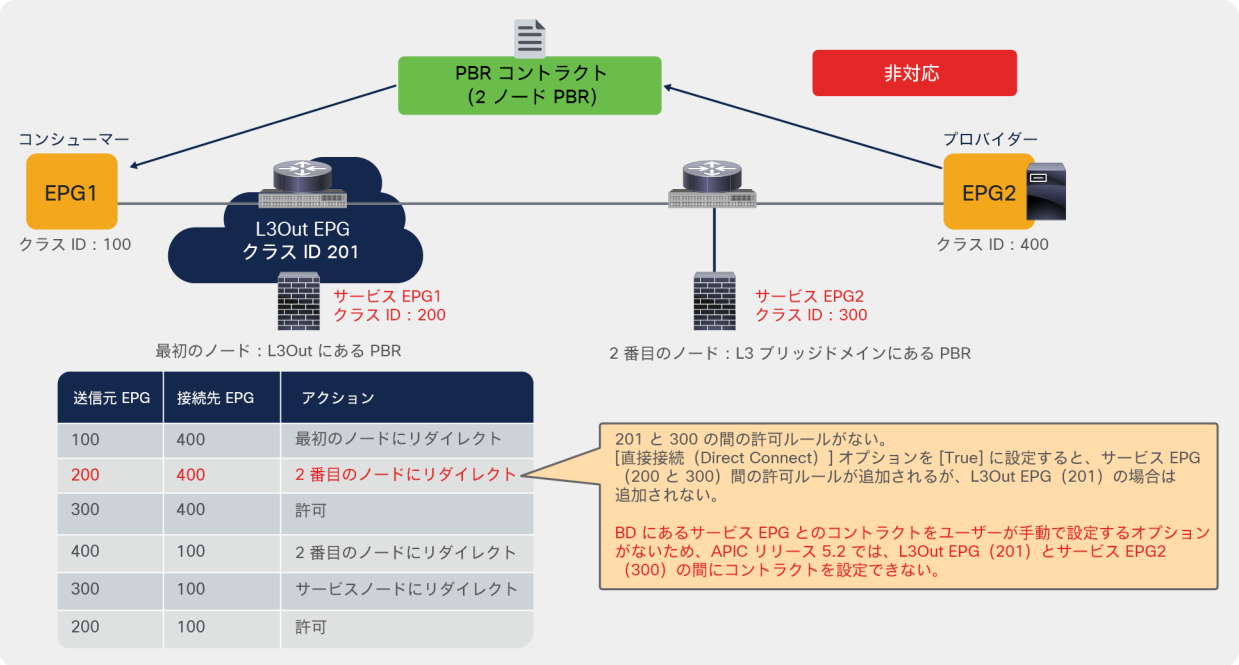


図 205.
マルチノードサービスグラフに関する考慮事項：ノード間の通信

付録：PBR 関連の機能強化履歴

表 22 に、PBR 関連の機能強化とその導入時期（リリース）の一覧を示します。

表 22. PBR 関連の機能

ACI リリース	機能
2.0	PBR 対称 PBR
2.1	トランクポートグループ
2.2(3j)	PBR ノードトラッキング（ICMP、ダウンアクションは「許可」のみ）
3.1	PBR ノードトラッキング（ICMP と TCP、ダウンアクションは「許可」と「拒否」） 同じサブネットにある PBR ノード、コンシューマー EPG、プロバイダー EPG Cisco ACI マルチポッド設計におけるロケーションベースの PBR PBR が vDS VMM ドメインにある uSeg EPG を除く uSeg EPG 間のコントラクトに対応
3.2	マルチノード PBR 復元力のあるハッシュ PBR を使用したエニーキャストサービス vzAny をプロバイダーとする PBR マルチサイト + PBR が設定されたサービスグラフ（1 ノードサービスグラフ） PBR が設定されたサービスグラフが vDS VMM ドメインにある uSeg EPG 間のコントラクトに対応

ACI リリース	機能
4.0	マルチサイト + PBR が設定されたサービスグラフ（2 ノードサービスグラフ） EPG 内コントラクトでの PBR、EPG 内コントラクトでのコピー サービス EPG の優先グループ
4.1	L1/L2 PBR
4.1.2	ダウンアクション「バイパス」 もう一方のコネクタが L3out にある単方向 PBR
4.2	バックアップ PBR ポリシー（N+M 高可用性）
4.2(3)	コントラクトからのフィルタ（filters-from-contract）オプション
4.2(5)	接続先名ベースのソート
5.0	アクティブ/アクティブ L1/L2 PBR 送信元 MAC の書き換え もう一方のコネクタが L3out にある単方向 PBR
5.1(3)	IP-SLA パラメータのオプション
5.2(1)	仮想 L4-L7 デバイスを対象とする VMware 拡張 LACP のサポート PBR ノードトラッキング（HTTP） L3Out EPG を対象とする EPG 内コントラクト（許可、拒否、PBR） MAC 設定のない L3 PBR（PBR 接続先の動的 MAC 検出） L3Out にある PBR 接続先
5.2(4)	エンドポイント セキュリティ グループ（ESG）のサービス EPG セレクタ
6.0	PBR 接続先ごとの重み

注： これらの機能を利用するには、Cisco Nexus 9300-EX および -FX プラットフォーム リーフ スイッチ以降が必要です（Cisco ACI リリース 2.0 の PBR を除く）。

詳細情報

詳細については、『ACI Multi-Pod White Paper』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-c11-737855.html

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-743107.html

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
cisco.com/jp

0915-2023-000-X