PBR を搭載した Nexus Dashboard Orchestrator vzAny PBR リリース 4.4.1

目次

PBR を使用した vzAny の概要 1
使用例 1
PBR を使用して vzAny を構成するための一般的なワークフ ロー 1
トラフィック フロー：Intra-VRF vzAny-to-vzAny 2
Consumer-to-Provider への初期トラフィック フローと会話型学習 2
コンシューマからプロバイダへのトラフィック フロー（定常状態） 4
プロバイダからコンシューマへのトラフィック フロー（安定状態） 4
トラフィック フロー：Intra-VRF vzAny-to-EPG 5
コンシューマからプロバイダへのトラフィック フロー 5
Provider-to-Consumer トラフィック フロー（内部トラフィックおよび会話型学習） 5
Provider-to-Consumer トラフィック フロー（安定状態） 6
トラフィック フロー：Intra-VRF vzAny-to-External-EPG（L3Out EPG） 7
Consumer-to-Provider へのトラフィック フロー 7
Provider-to-Consumer トラフィック フロー（内部トラフィックおよび会話型学習） 7
Provider-to-Consumer トラフィック フロー（安定状態） 8
PBR 注意事項および制限事項を持つ vzAny 9
サービス デバイス テンプレートの作成 11
アプリケーション テンプレートの作成 20
コントラクトへのサービス チェーンの追加 25

PBR を使用した vzAny の概要

次のセクションでは、マルチファブリック e ドメインでポリシーベース リダイレクト（PBR）を使用して vzAny コントラクトを有効にするための概要、要件と注意事項、および構成手順について説明します。一般的な vzAny の概要と、PBR を含まない基本的な vzAny のユース ケースについては、「vzAny コントラクト 」の章を参照してください。

使用例

リリース 4.2(3) より前は、次の基本的な vzAny のユース ケース（PBR なし）がマルチファブリックでサポートされていました。これらはすべて、「vzAny コントラクト」の章で説明されています：

- 同じ VRF 内の EPG 間の自由な通信。
- 多対 1 通信により、同じ、または異なる VRF にある単一の EPG からの共有サービスを、同じ VRF 内のすべての EPG が消費できるようになります。

NDO リリース 4.2（3）以降、PBR を使用した vzAny の次の追加の使用例は、APIC リリース 6.0（4）以降を実行している ACI ファブリックでサポートされます。これにより、ワンアーム モードの各ファブリックに接続された論理ファイアウォール サービスにトラフィックをリダイレクトできます。

- 同じ VRF 内の 2 つの EPG または外部 EPG 間の VRF 内通信（vzAny から vzAny）。
- VRF（vzAny）内のすべての EPG と、同じ VRF の一部である特定の EPG 間の多数対 1 の通信。
- VRF（vzAny）内のすべての EPG と、同じ VRF の一部である特定の外部 EPG 間の多数対 1 の通信。

PBR を使用して vzAny を構成するための一般的なワークフロー

次のセクションでは、PBR を使用するすべての vzAny の使用例に必要な個々の構成要素（テンプレート、EPG、コントラクトなど）を作成および構成する方法について説明し、その後に、個々のビルディング ブロックを、構成する特定の使用例に合わせて使用します。

PBR のユース ケースで vzAny のいずれかを構成する場合は、リリース 4.2(3) で導入され、サービス グラフ構成の定義に使用される新しいサービス デバイス テンプレートを含む次のワークフローを実行します。

1. サービス デバイス テンプレートを作成し、構成が必要な特定のテナントとすべてのファブリックに関連付けます。これには次のものが含まれます。
    - （オプション）IP SLA ポリシーの参照。

      IP SLA ポリシーは、同じテナントに関連付けられたテナント ポリシー テンプレートですでに定義されている必要があります。

    - サービス デバイス テンプレートで 1 つ以上のサービス ノード デバイスの作成。

      サービス デバイス構成を作成する場合は、いずれかのアプリケーション テンプレートにすでに存在している必要があるブリッジ ドメインを指定する必要があります。正確な BD 要件は、「PBR を持つ vzAny の注意事項と制限事項」の項に記載されています。

- サービス デバイス テンプレートで定義されたサービス ノード デバイスのファブリックレベル構成を提供し、展開します。

> リリース 4.2（3）およびサービス デバイス テンプレートの導入以降、PBR の使用例について Nexus Dashboard Orchestrator で明示的に作成する必要があるサービス グラフ オブジェクトはありません。NDO は暗黙的にサービス グラフを作成し、ファブリックの APIC に展開します。

2. 作成したサービス デバイス テンプレートに関連付けられた特定のテナントの設定を完了します。これには、次のものが含まれます。
   - テナント アプリケーション テンプレートを作成し、構成が必要なすべてのファブリックへ割り当てる。
   - PBR とコントラクトを有効にするために必要な vzAny VRF 設定の構成。
   - コンシューマおよびプロバイダ EPG の構成。

     サービス BD はファブリック間で拡張する必要がありますが、EPG に使用する BD は拡張またはファブリックローカルにすることができます。
3. 手順 1 で作成したサービスデバイスを、ステップ 2 で作成した vzAny コントラクトに関連付けます。

> Cisco ACI コントラクトと PBR の用語を理解するには、『*ACI コントラクト ガイド*』と「*ACI PBR ホワイトペーパー*」を参照してください。

トラフィック フロー：Intra-VRF vzAny-to-vzAny

このセクションでは、異なるファブリックの特定の VRF の論理 vzAny 構造の一部である 2 つの EPG 間のトラフィック フローを要約します。このユース ケースでは、vzAny は PBR コントラクトのプロバイダとコンシューマの両方です。

> この場合、双方向のトラフィック フローは、2 つのファブリックに展開された独立した FW ノードによる非対称トラフィックフローを回避するため、両方のファイアウォールを通してリダイレクトされます。

Consumer-to-Provider への初期トラフィック フローと会話型学習

ローカル ファブリックとリモート ファブリックの両方の FW サービス ノードにトラフィックをリダイレクトするための設計原則は、トラフィック フローの両方向の入力リーフ スイッチに常に PBR ポリシーを適用することです。これを行うには、入力リーフ スイッチが宛先のエンドポイント ポリシー情報（クラス ID）を認識している必要があります。次の図は、通信がコンシューマ エンドポイントから開始され、入力（コンシューマ）リーフ スイッチに宛先（プロバイダ）エンドポイントのクラス ID 情報がまだない例を示しています。そのため、トラフィックはリモート ファブリックに接続されている宛先に転送されるだけです。このリリースでは、この使用例をサポートする新しいロジックが実装されているため、トラフィックを受信するプロバイダ リーフ スイッチは、フローがファブリック 1 で発生したが、そのファブリックに接続されたファイアウォール サービス ノードを介して送信されていないことを理解できます。その結果、コンシューマ エンドポイント情報（クラス ID）を学習した後、ファブリック 2 のプロバイダ リーフはファブリック 1 のファイアウォールに向けてトラフィックをバウンスバックします。

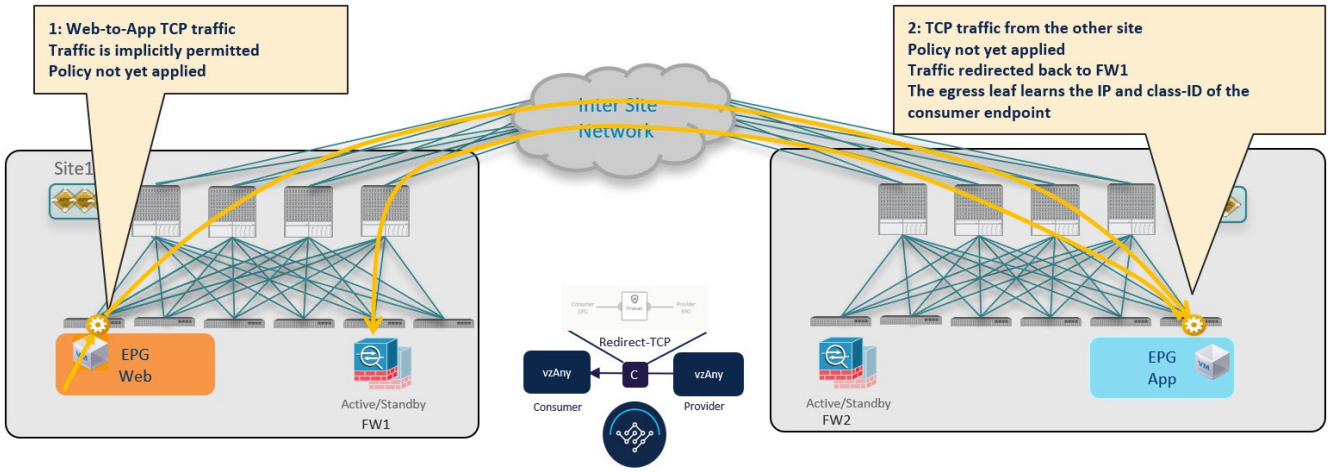

図 1. 会話型学習

ファブリック 1 のファイアウォールはセキュリティ ポリシーを適用し、トラフィックはファブリック 2 の宛先リーフ スイッチに再度転送されます。このリーフは、トラフィックがまだファブリック 1 から送信されている間に、そのファブリックに展開されたファイアウォールを介して送信されたことを認識できるようになりました。その結果、宛先リーフ スイッチはパケットを検査のためにローカル ファイアウォール デバイスに転送し、その後、次の図に示すように宛先エンドポイントに配信します。

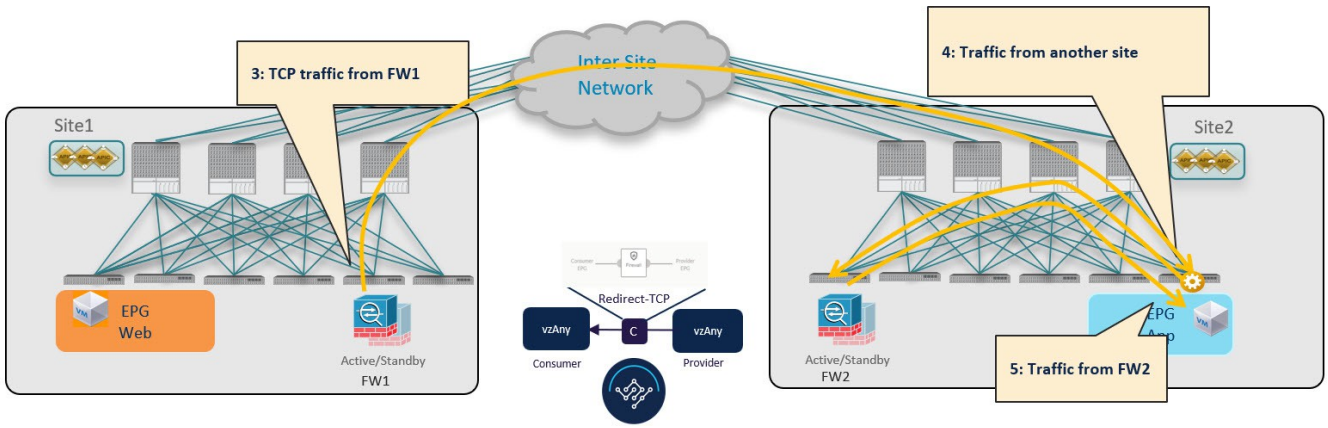

図 2 会話型学習

!!!Dita2Adoc_MissingReference:!!! のようなトラフィックの準最適なバウンスを回避するために、プロバイダ リーフ スイッチは特別な制御パケットを生成し、ファブリック 1 のコンシューマ リーフ スイッチに送信します。これにより、コンシューマ リーフはプロバイダ エンドポイントのクラス ID 情報を学習できます。

最初のフローがプロバイダからコンシューマへの方向で確立される場合、コンシューマからプロバイダへのトラフィックの方向について上記で説明したのと同じ動作が適用されます。

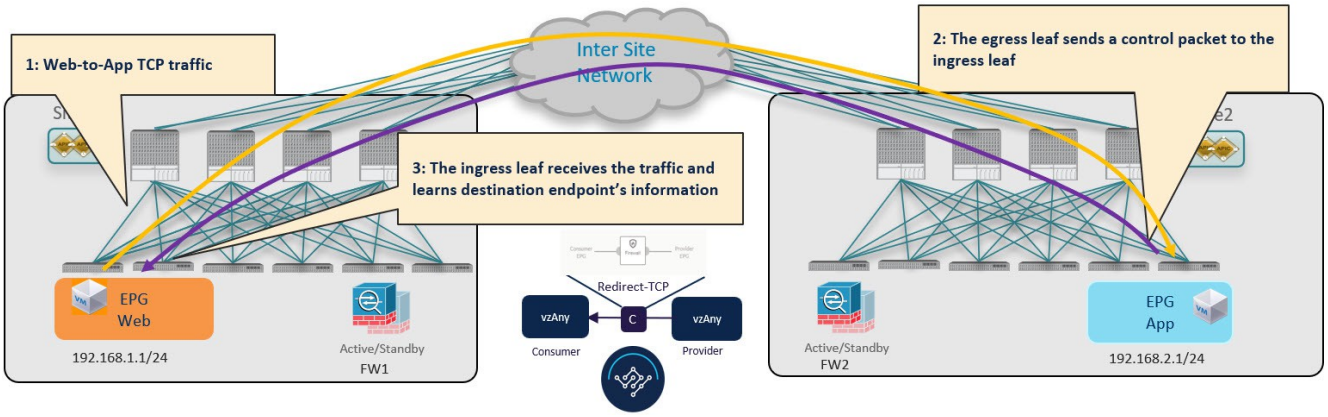

図 3. 会話型学習

コンシューマからプロバイダへのトラフィック フロー（定常状態）

コンシューマ リーフ スイッチは、前述の会話型学習ステージからプロバイダ エンドポイント情報を学習した後、ポリシーを適用し、以降のすべてのトラフィックに対してトラフィックをローカル ファイアウォールにリダイレクトできます。

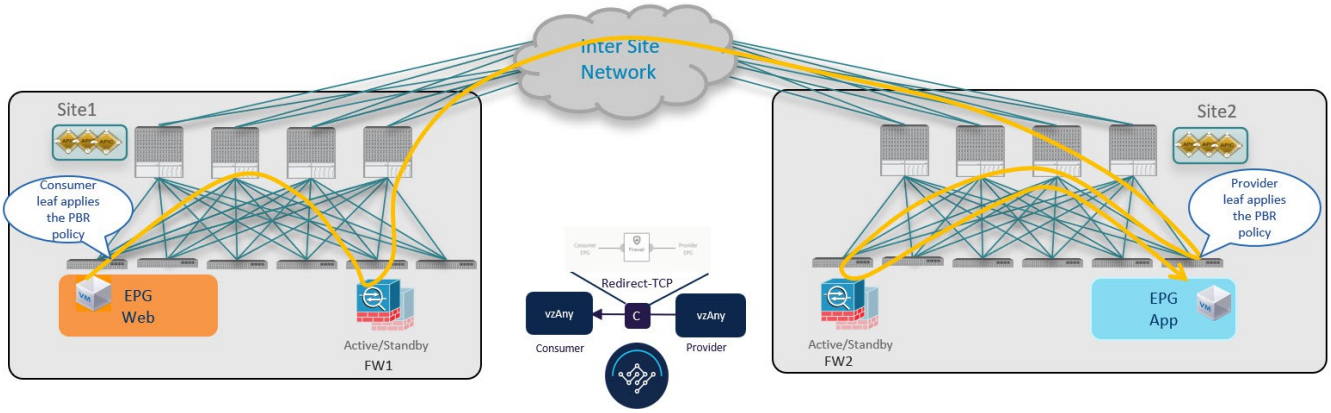

図 4 コンシューマからプロバイダへのトラフィック フロー

プロバイダからコンシューマへのトラフィック フロー（安定状態）

プロバイダ リーフ スイッチは、!!!Dita2Adoc_MissingReference:!!! に示す直接パケットから、または会話型学習に基づいてコンシューマ エンドポイント情報を学習した後、ポリシーを適用し、今後のすべてのトラフィックに対してトラフィックをローカル ファイアウォールにリダイレクトできます。

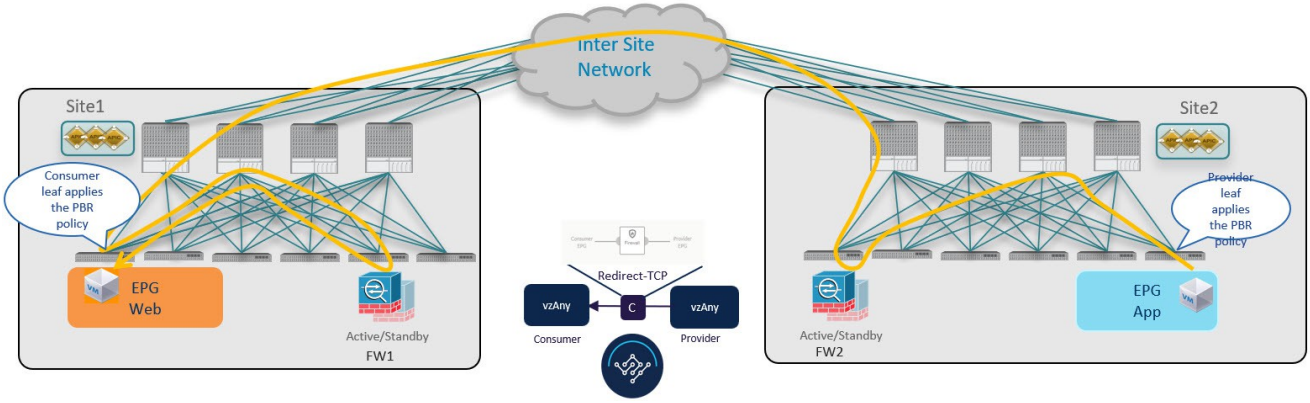

図 5 プロバイダからコンシューマへのトラフィック フロー

トラフィック フロー：Intra-VRF vzAny-to-EPG

このセクションでは、特定の VRF の論理 vzAny 構造の一部であるコンシューマ EPG と同じ VRF の一部であるプロバイダ EPG 間のトラフィック フローを要約します。このユース ケースでは、vzAny は PBR コントラクトのコンシューマですが、特定の EPG はプロバイダです。

トラフィックが常に両方のファブリックのファイアウォール デバイスを通過するvzAny-to-vzAny および vzAny-to-L3Out の使用例とは異なり、vzAny-to-EPG は常にプロバイダのファブリックのデバイスのみを使用します。

コンシューマからプロバイダへのトラフィック フロー

vzAny-to-EPG の使用例では、ポリシーはトラフィックの方向に関係なく、プロバイダ リーフ スイッチにのみ適用されます。したがって、コンシューマからプロバイダへのトラフィックの場合、コンシューマ EPG はトラフィックをプロバイダ EPG のリーフ スイッチに直接送信します。リーフ スイッチはコンシューマのエンドポイント 情報（クラス ID）を学習し、検査のためにトラフィックをローカルのファイアウォールにリダイレクトします。

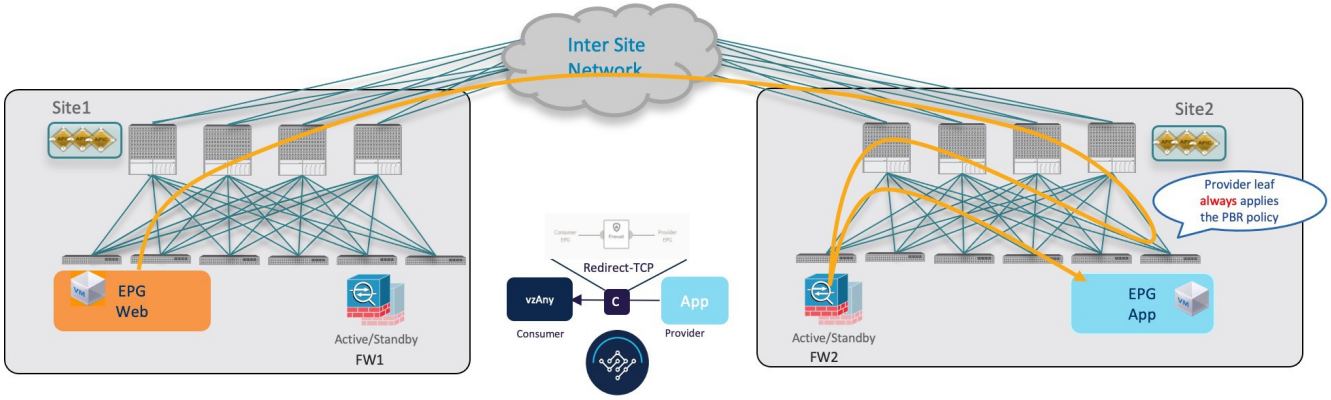

図 6 : vzAny-to-EPG のコンシューマからプロバイダへのトラフィック フロー

Provider-to-Consumer トラフィック フロー（内部トラフィックおよび会話型学習）

プロバイダ リーフ スイッチがコンシューマ エンドポイント情報（クラス ID）を学習できる前に、プロバイダ エンドポイントによって通信が開始された場合、トラフィックをローカル ファイアウォールにリダイレクトするポリシーを適用できないため、トラフィックはファブリック間でコンシューマ リーフ スイッチに送信されます。ポリシーが適用されなかったため（パケット内の制御ビットによって示される）、コンシューマ リーフ スイッチはインスペクションのためにトラフィックをプロバイダ ファブリックのファイアウォールにリダイレクトし、最終的にトラフィックをコンシューマ エンドポイントにバウンスします。

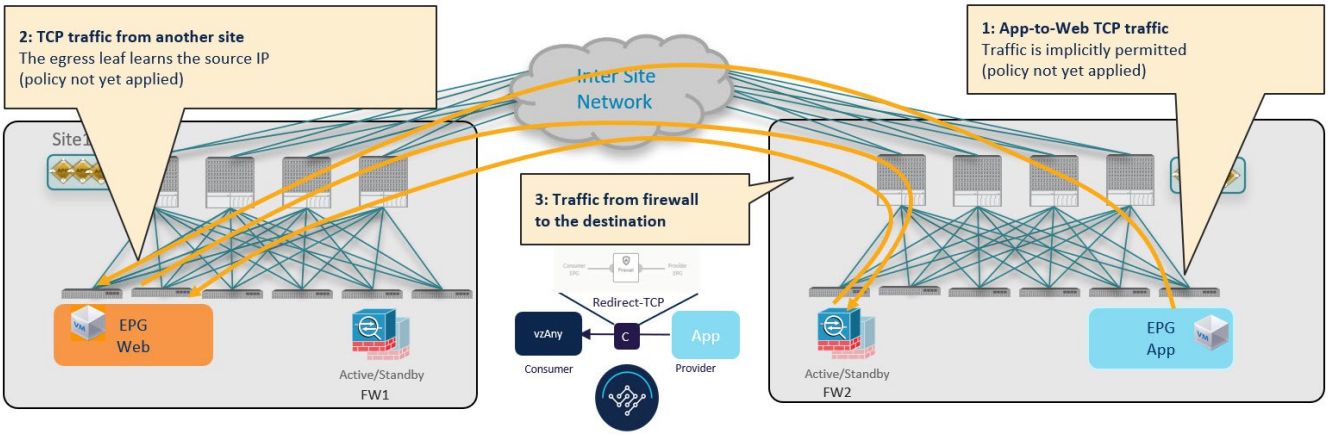

図 7 : vzAny-to-EPG プロバイダからコンシューマへのトラフィック フロー（初期トラフィックおよび会話型学習）

この準最適トラフィック フローは無期限に継続できますが、コンシューマ EPG のリーフ スイッチは、今後のトラフィックを最適化し、両方のファブリック間でバウンスしないようにするために、コンシューマ エンドポイント情報を含む別の制御パケットをプロバイダ リーフ スイッチにも送信します。

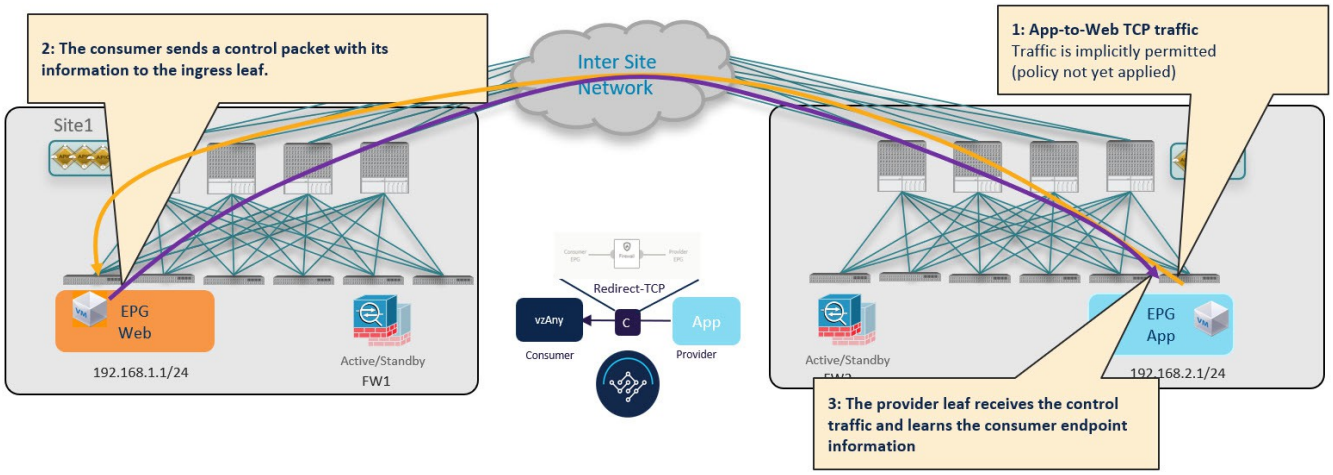

図 8 会話型学習

Provider-to-Consumer トラフィック フロー（安定状態）

プロバイダ リーフ スイッチは、!!!Dita2Adoc_MissingReference:!!! に示すコンシューマ エンドポイントから発信された直接パケットから、または会話型学習に基づいてコンシューマ エンドポイント情報を学習した後、ポリシーを適用し、今後のすべてのトラフィックに対してトラフィックをローカル ファイアウォールにリダイレクトできます。

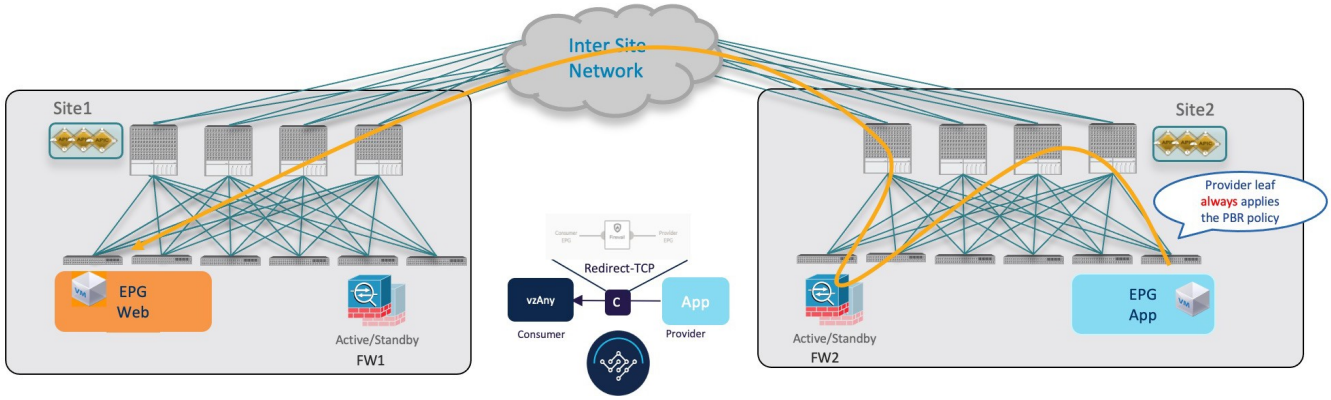

図 9 : vzAny-to-EPG Provider-to-Consumer トラフィック フロー

トラフィック フロー：Intra-VRF vzAny-to-External-EPG（L3Out EPG）

このセクションでは、特定の VRF の論理 vzAny 構造の一部である EPG と、別のファブリックの同じ VRF の一部である外部 EPG（L3Out EPG）間のトラフィック フローを要約します。このユース ケースでは、vzAny は vzAny コントラクトのコンシューマであり、L3Out に関連付けられた外部 EPG はプロバイダーです。

このユース ケースでは、トラフィックは常に両方のファブリックのファイアウォール デバイスを介してリダイレクトされます。

Consumer-to-Provider へのトラフィック フロー

入力リーフ スイッチは、宛先外部 EPG のクラス ID を常に解決でき、トラフィックをローカル FW にリダイレクトする PBR ポリシーを適用するため、この方向のトラフィックには会話型学習は必要ありません。トラフィックはファブリック 1 のファイアウォール ノードを通過した後にプロバイダ リーフ スイッチによって受信されるため、プロバイダ リーフ スイッチがこのデータプレーン通信からコンシューマ エンドポイント情報（クラス ID）を学習することはできません。

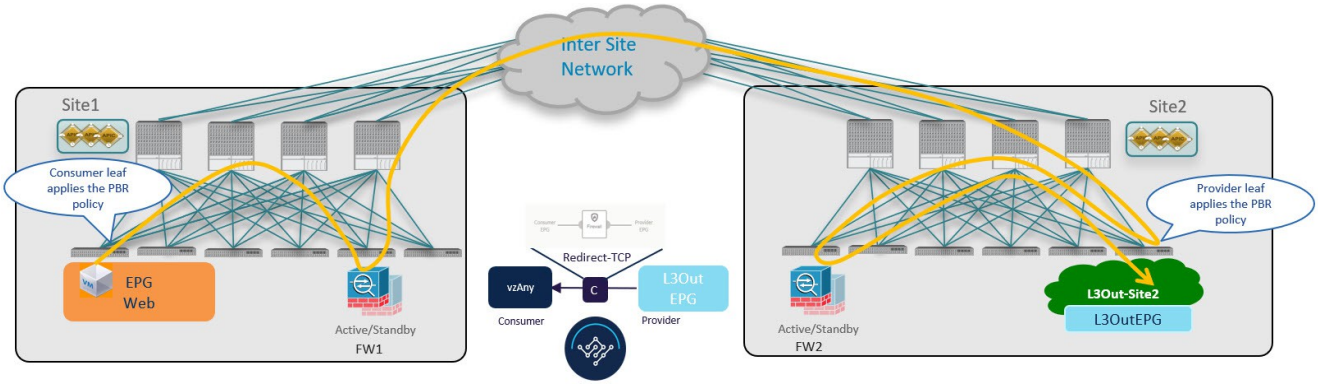

図 10：vzAny-to-External EPG のコンシューマからプロバイダへのトラフィック フロー

Provider-to-Consumer トラフィック フロー（内部トラフィックおよび会話型学習）

プロバイダ リーフ スイッチがコンシューマ エンドポイント情報を学習する前に、トラフィックをローカル ファイアウォールにリダイレクトするポリシーを適用できないため、トラフィックはファブリック間でコンシューマ リーフ スイッチに送信されます。ポリシーが適用されなかったため（パケット内の制御ビットによって示される）、コンシューマ リーフ スイッチはトラフィックをインスペクションのためにプロバイダ ファブリックのファイアウォールにリダイレクトし、最終的にトラフィックをコンシューマ エンドポイントに転送します。

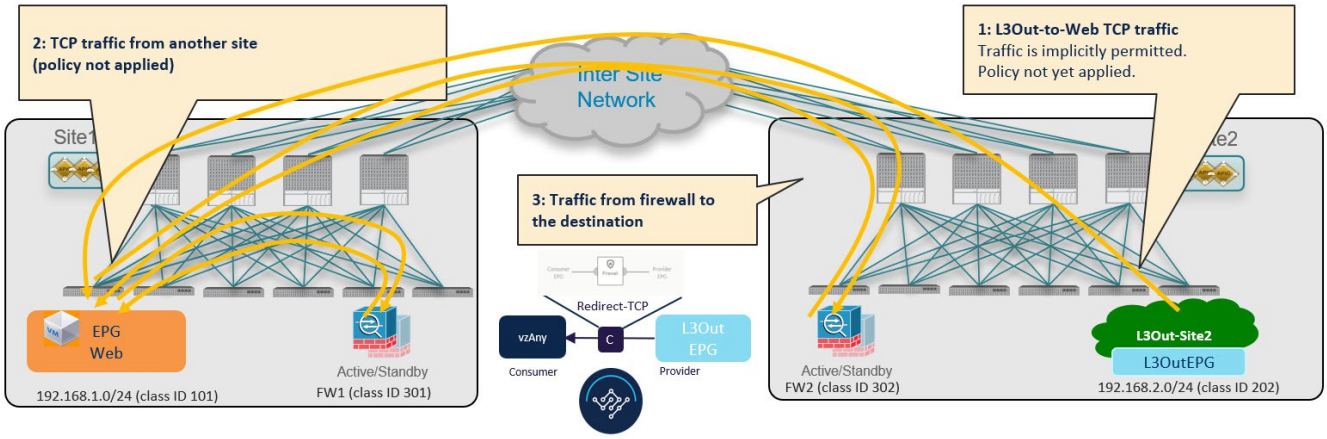

図 11 : vzAny-to-L3Out プロバイダからコンシューマへのトラフィックフロー（初期トラフィックおよび会話型学習）

このトラフィック フローは無期限に継続できますが、コンシューマ リーフ スイッチは、将来のトラフィックを最適化し、両方のファブリック間でバウンスしないようにするために、コンシューマ エンドポイント情報を含む別の制御パケットをプロバイダー リーフ スイッチにも送信します。

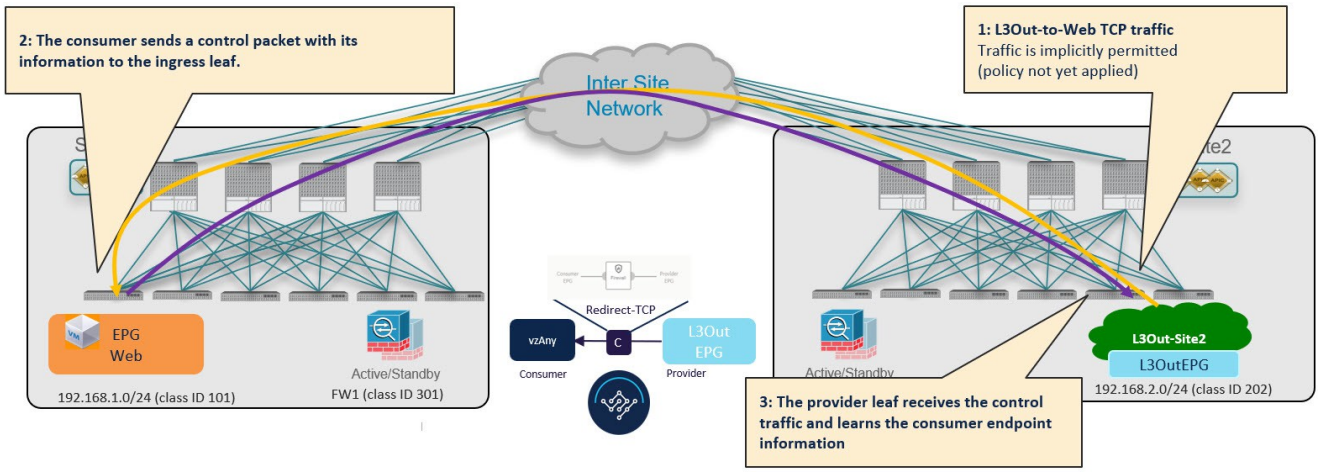

図 12 : vzAny-to-L3Out プロバイダからコンシューマへのトラフィックフロー（初期トラフィックおよび会話型学習）

Provider-to-Consumer トラフィック フロー（安定状態）

プロバイダ リーフ スイッチは、コンシューマ エンドポイント情報を学習した後、PBR ポリシーを適用して、最初にローカル ファイアウォール デバイスにトラフィックをリダイレクトします。次に、ファブリック間でトラフィックをコンシューマ リーフ スイッチに送信します。最後にコンシューマ エンドポイントに送信されます。

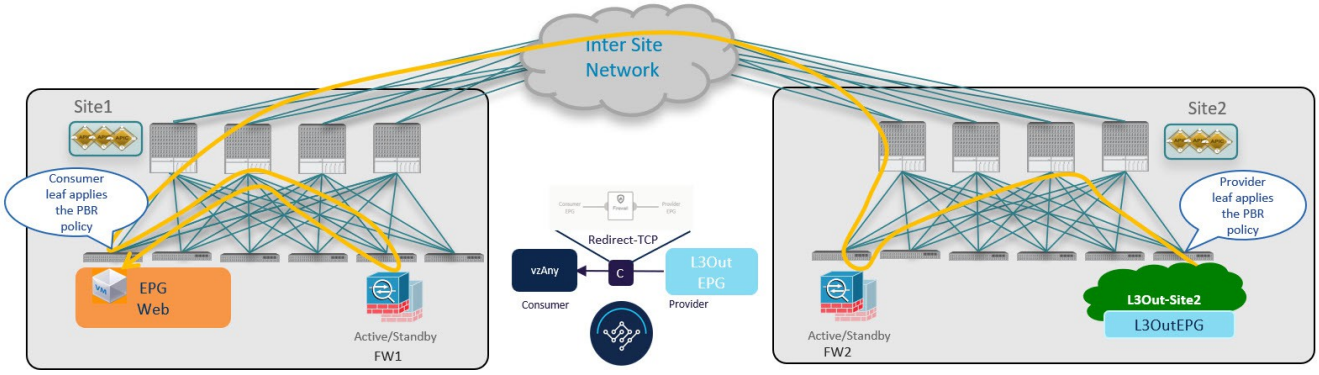

図 13 : vzAny-to-L3Out プロバイダからコンシューマへのトラフィック フロー

PBR 注意事項および制限事項を持つ vzAny

マルチファブリック展開の PBR を持つ vzAny を使用するときに、次の注意事項および制限事項が適用されます。

次のセクションは、PBR を使用する vzAny の使用例にのみ適用されます。基本的な vzAny の概念と使用例の詳細については、「vzAny コントラクト」の章を参照してください。

- エンドポイント グループ（EPG）間で MultiSite ポリシーベース リダイレクト（PBR）を設定する場合、次の機能は特定の IP エンドポイントまたはホスト プレフィックス（IPv4 の場合は /32、IPv6 の場合は /128）では
  サポートされません。
  - ブリッジ ドメインのスタティック ルート（NH 到達可能性）
  - Microsoft ネットワーク ロード バランシング
  - エニーキャストMAC
- ACI ファブリックは、Cisco APIC リリース 6.0(4) 以降を実行している必要があります。
- このリリースでは、サービス ブリッジ ドメインに接続されている単一のインターフェイスで、vzAny トラフィックの単一ノード ファイアウォールまたは単一ノード ロードバランサへのリダイレクトがサポートされています。シングルノード ファイアウォールは、vzAny-to-vzAny および vzAny-to-L3Out、vzAny-to-EPG、および L3Out-to-L3Out の使用例でサポートされています。シングルノード ロードバランサは、vzAny-to-EPG の使用例でサポートされています。

  これには、ワンアーム モード ファイアウォール サービス グラフの次の 3 つの使用例が含まれます。

  - ファブリック間の VRF 内通信（vzAny から vzAny）。
  - VRF（vzAny）内のすべての EPG と、同じ VRF の一部である特定の EPG 間の多数対 1 の通信。
  - VRF（vzAny）内のすべての EPG と、同じ VRF の一部である特定の外部 EPG 間の多数対 1 の通信。

  上記のすべてのケースで、対話型エンドポイント学習は PBR を持つ vzAny が構成されている場合にのみ有効になり、EPG 下の IP プレフィックスが構成されていない場合に使用されます。IP プレフィックスを持つ EPG と IP プレフィックスのない EPG の組み合わせもサポートされます。
- これらのユース ケースのアプリケーション テンプレートで定義されている既存のサービス グラフ オブジェクトを使用するとき、リリース 4.2（3）で導入された新しいサービス チェーン ワークフローを使用し、サービス デバイス テンプレートでポリシーを定義してコントラクトに関連付けることで、新しいサービス グラフを暗黙的に作成することを推奨します。

  次のセクションで説明する手順では、新しいサービス デバイス テンプレートを使用して、サポートされているユース ケースを有効にしますが、該当する場合は特定の違いについて説明します。

  アプリケーション テンプレートのサービス グラフ オブジェクトの構成は、今後のリリースで廃止されます。
- vzAny VRF は、ファブリック全体に拡張する必要があります。

この章で説明する vzAny PBR の使用例を有効にするには、vzAny VRF に対して [ファブリック対応ポリシーの適用（Fabric-aware Policy Enforcement）] オプションと [L3 マルチキャスト（L3 Multicast）] オプションを有効にする必要があることに注意してください。

次のセクションでは、vzAny を有効にしているか、または有効にする VRF がすでにあり、これらの使用例に使用することを前提としています。

VRF がまだない場合は、通常どおりにアプリケーション テンプレートで VRF を作成できます。VRF 構成の詳細については、「VRF の構成」を参照してください。

- サービス デバイス インターフェイスにアタッチするサービス BD は、L2 ストレッチする必要があります（BUM 転送は代わりのオプションで、無効にしておくべきです）。

  サービス BD がまだない場合は、通常どおりにアプリケーション テンプレートで作成できます。BD 構成の詳細については、「ブリッジ ドメインの構成」を参照してください。

- コンシューマ、プロバイダー、およびサービス BD は、ハードウェア プロキシ モードで構成する必要があります。
- vzAny PBR は、L3Out ではなく、ストレッチされたサービス BD に接続する必要があります。
- しきい値ダウン拒否アクションと sip-dip-protocol ハッシュのみがサポートされます。
- PBR 宛先ノードは、コンシューマ VRF またはプロバイダ VRF のいずれかにある必要があります。例えば、「*Cisco ACI におけるポリシーベース リダイレクト サービス グラフの設計に関するホワイト ペーパー*」を参照します。

以下は、PBR を使用する vzAny の使用例ではサポートされていません。

- 特定のリモート リーフ構成。
  - リモート リーフ ノードを利用するマルチファブリック展開には、特定の考慮事項が適用されます。異なるファブリックに属するリモート リーフ ノードに展開されているエンドポイント（コンシューマまたはプロバイダー）間の通信を目的とした、PBR を使用したファブリック間中継ルーティングは、vzAny PBR および L3Out-to L3Out ではサポートされません。
- 各 VRF は、vzAny-to-vzAny、L3OutEPG-to-L3OutEPG、および vzAny-To-L3OutEPG ポリシーベース ルーティング（PBR）のワンアーム構成で 1 つのデバイスのみを使用するように制限されます。この制限は、 APICの特別な ACL により適用されます。
- vzAny-to-vzAny/L3OutEPG-to- L3OutEPG のリダイレクト、および vzAny-to-EPG、EPG-to-EPG、EPG-to-L3OutEPG などの他の使用例では、それらが同じ VRF にある場合、異なるファイアウォール VLAN インターフェイスを使用する必要があります。
- PBR を使用した vzAny が、新しくサポートされたユースケース（vzAny-to-vzAny、vzAny-to-L3OutEPG、L3OutEPG-to-L3OutEPG）のノースサウス通信に適用される場合、ストレッチ サブネットに対して入力トラフィックの最適化を有効にする必要があります。
- L3 PBR 接続先を持つ 1 つのノード サービス チェーンのみがサポートされます。
- コントラクト許可ロギングは、ファブリック認識ポリシー適用モードが有効になっている VRF ではサポートされません。このモードは vzAny PBR および L3OutEPG-to-L3OutEPG PBR では必要です。
- PBR を使用したポッド対応 vzAny はサポートされていません。

サービス デバイス テンプレートの作成

始める前に：

- 「PBR を搭載した vzAny の 注意事項および制限事項」で説明されているように、要件を読んで満たしていることを確認します。
- このセクションで定義するサービス ノードで使用する拡張サービス ブリッジ ドメイン（BD）を作成しておく必要があります。

  BD がまだない場合は、通常どおりにアプリケーション テンプレートで BD を作成できます。BD 構成の詳細については、「ブリッジ ドメインの構成」を参照してください。

次の手順では、PBR ユース ケースを使用した vzAny の使用例に使用するサービス ノードとその設定を使用してサービス デバイス テンプレートを作成する方法について説明します。

1. Nexus Dashboard Orchestrator の GUI にログインします。
2. 左のナビゲーション ペインから、**[構成（Configure）] > [テナント テンプレート（Tenant Template）]** を選択します。
3. （オプション）テナント ポリシー テンプレートと IP-SLA モニタリング ポリシーを作成します。

   トラフィック リダイレクションの IP-SLA ポリシーを構成することを推奨します。これにより、以下の手順 7 で説明する PBR ポリシーの構成が簡素化されます。IP-SLA ポリシーがすでに定義されている場合は、この手順をスキップできます。それ以外の場合は、次の手順を実行します。

   a. **[テナント ポリシー（Tenant Policies）]** タブを選択します。
   b. **[テナント ポリシー（Tenant Policy）]**ページ内で**[テナント ポリシー テンプレートの作成（Create Tenant Policy Template）]**をクリックします。
   c. **[テナント ポリシー（Tenant Policies）]** ページの右のプロパティ サイトバーにテンプレートの **[名前（Name）]** を入力し、**[テナントの選択（Select a Tenant）] を選択します。**
   d. **[テンプレート プロパティ（Template Properties）]** ページで、**[アクション（Actions）] > [ファブリックの追加/削除（Add/Remove Fabrics）]** を選択し、両方のファブリックにテンプレートを関連付けます。
   e. メインペインで、**[オブジェクトの作成（Create Object）] > [IP SLA モニタリング ポリシー（IP SLA Monitoring Policy）]** を選択します。
   f. ポリシーの **[名前（Name）]** を指定し、その設定を定義します。
   g. **[保存（Save）]** をクリックして、テンプレートを保存します。
   h. **[テンプレートの展開（Deploy）]** をクリックして、展開します。
4. サービス デバイス テンプレートを作成し、テナントおよびファブリックに関連付けます。
   a. **[構成（Configure ）] > [テナント テンプレート（Tenant Templates）]** から、**[サービス デバイス（Service Device）]** タブを選択します。
   b. **[サービス デバイス テンプレートの作成（Create Service Device Template）]** をクリックします。

c. 開くテンプレート　プロパティ サイドバーで、テンプレートの **[名前（Name）]** を入力し、**[テナントの選択（Select a Tenant）]** を選択します。

d. **[テンプレート プロパティ（Template Properties）]** ページで、**[アクション（Actions）] > [ファブリックの追加/削除（Add/Remove Fabrics）]** を選択し、両方のファブリックにテンプレートを関連付けます。

e. **[保存（Save）]** をクリックして、テンプレートを保存します。

5. デバイス クラスタを作成して構成します。

a. **[テンプレート プロパティ（Template Properties）]** ページ（テンプレートレベルの構成）で、**[オブジェクトの作成（Create Object）] > [サービス デバイス クラスタ（Service Device Cluster）]** を選択します。

デバイス クラスタは、トラフィックをリダイレクトするサービスを定義します。このリリースでは、active/standby、active/active、または複数の独立したノードのクラスタの 3 つの異なる冗長モデルで展開できるファイアウォール サービス ノードへのリダイレクションがサポートされています。これらのさまざまなオプションのプロビジョニングについては、以下の手順 7 で説明します。ファブリックレベルでファイアウォール展開モデルを選択でき、同じマルチファブリック ドメインの一部であるさまざまなファブリックにさまざまなオプションを展開できることに注意してください。

b. **[<cluster-name>]** サイドバーで、クラスタの **[名前（Name）]**を入力します。

[デバイスの場所（Device Location）] と **[デバイス モード（Device Mode）]** は、現在サポートされている使用例に基づいて事前に入力されています。**デバイスの場所** は ACI として、 デバイス **モード** は L3として事前に構成する必要があります。

c. **[デバイス タイプ（Device Type）]** で、[ファイアウォール（Firewall）] を選択します。

このリリースでは、PBR を使用した vzAny の使用例のファイアウォールデバイスのみがサポートされます。

d. **[デバイス モード（Device Mode）]** では、[L3] を選択します。

e. **[接続モード（Connectivity Mode）]** の場合、[One Arm] を選択します。

このリリースでは、PBR を使用した vzAny のユース ケースのワンアーム デバイスのみがサポートされます。

デバイス接続モードを ワン アーム、ツー アーム、および詳細モードの間で変更すると、プロセスでデバイス インターフェイスの名前が変更される場合があります。警告メッセージはユーザーに警告し、インターフェイスを変更しようとすることは、そのインターフェイスが現在コントラクトによって使用されている場合、制限されます。以前に使用していたインターフェイス名を保持し、展開された構成の中断を回避することを望む場合は、変更プロセス中に名前の変更を上書きすることを選択できます。

検証は、ワン アーム モードとツー アーム モードでのみ実行されます。[詳細（Advanced）] モードでは、検証は実行されません。このモードを選択すると、ユーザーはエキスパートであると見なされます。

f. **[インターフェイス名（Interface Name）]** を入力します。

g. **[インターフェイス タイプ（Interface Type）]** で、[BD] を選択します。

PBR を使用した vzAny のユース ケースの場合、このリリースでは、ブリッジ ドメインへのサービス デバイスの接続のみがサポートされます。

h. **[BD の選択（Select BD）] をクリックして**、このデバイスを接続するサービス ブリッジ ドメインを選択します。

これは、「PBR を搭載した vzAny の 注意事項と制限事項」の一部として作成した拡張サービス BD です。

i. **[リダイレクト（Redirect）]** オプションで、[はい（Yes）] を選択します。

PBR の使用例では、リダイレクトの有効化を選択する必要があります。[はい（Yes）] を選択すると、**[IP SLA モニタリング ポリシー（IP SLA Monitoring Policy）]** オプションが使用可能になります。

j. （オプション）**[IP SLA モニタリング ポリシーの選択（Select IP SLA Monitoring Policy）]** をクリックし、前の手順で作成した IP SLA ポリシーを選択します。

k. （オプション）サービス クラスタの追加設定を指定する場合は、**[詳細設定（Advanced Settings）]** エリアで **[有効（Enable）]** を選択します。

次の詳細設定を構成できます。

- **[QoS ポリシー（QoS Policy）]**：リダイレクトされたトラフィックに ACI ファブリック内で特定の QoS レベルを割り当てることができます。
- **[優先グループ（Preferred Group）]**：このサービス デバイス インターフェイスクラスタが優先グループの一部であるかどうかを指定します。

  vzAny ユースケースを構成する場合は、このオプションを無効のままにします。

- **[ロード バランシング ハッシュ（Load Balancing Hashing）]**：PBR ロード バランシングのハッシュ アルゴリズムを指定できます。

> vzAny-to-vzAny、vzAny-to- ExtEPG、および ExtEPG-to-ExtEPG 使用例ではデフォルト構成のみをサポートしているため、デフォルト値のままにする必要があります。他の使用例（EPG から EPG、ExtEPG から EPG、および vzAny から EPG）の負荷バランシングハッシュを変更できます。

  詳細については、*「ACI ポリシーベースのリダイレクト サービス グラフの設計」* を参照してください。

- **[ポッド対応リダイレクション（Pod Aware Redirection）]**：優先 PBR ノードを指定する場合は、マルチポッド構成で構成できます。ポッド対応リダイレクションを有効にすると、ポッド ID を指定でき、リダイレクトは指定されたポッドにあるリーフ スイッチでのみプログラムされます。

- **[送信元 MACの書き換え（Rewrite Source MAC）]**：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に、送信元 MAC アドレスを更新します。

  詳細については、*「ACI ポリシーベースのリダイレクト サービス グラフの設計」*を参照してください。

- **[高度なトラッキング オプション（Advanced Tracking Options）]**：サービス ノード トラッキングのさまざまな詳細設定を構成できます。詳細については、**「***サービスノードをトラッキングするための ポリシーベースリダイレクトとしきい値の設定***」を参照してください。**

l. **[OK]** をクリックして保存します。

サービス デバイス クラスタを作成すると、**[テンプレート プロパティ（Template Properties）]**（テンプレート レベルの構成）ページで赤色で強調表示されることに注意してください。この時点で、ファイアウォール サービスへのリダイレクトを定義しましたが、やはりファブリックローカルレベルで使用するファイアウォール情報とリダイレクト ポリシーを指定する必要があります。

6. 前の手順で作成したサービス デバイス クラスタのファブリックローカル構成を指定します。
   a. **[サービス デバイス テンプレート（Service Device Template）]** 画面で、**[<fabric-name>]** タブをクリックします。
   b. ファブリック レベルで、作成したサービス デバイス クラスタを選択します。
   c. プロパティのサイドバーで、**[ドメイン タイプ（Domain Type）]** を選択します。

   このファブリックのファイアウォールデバイスが物理または VMM（仮想であり、VMM ドメインの一部であるハイパーバイザによってホストされる）のいずれであるかを選択できます。

   d. **[ドメインの選択（Select Domain）]** をクリックして、このファイアウォール デバイスが属するドメインを選択します。物理ドメインまたは仮想ドメインのいずれかを選択できます。

   - 物理ドメインを選択した場合は、次の情報を入力します。
     - **[VLAN]**：ファブリックとファイアウォール デバイス間のトラフィックに使用される VLAN ID を指定する必要があります。
     - **[ファブリックからデバイスへの接続（Fabric to Device Connectivity）]**：ファイアウォール デバイスへのファブリックの接続に関するスイッチ ノードとインターフェイス情報を提供します。
   - VMM ドメインを選択した場合は、追加のオプションを指定します。
     - **[トランキング ポート（Trunking Port）]**：L4-L7 VM のタグ付きトラフィックを有効にするために使用されます。

       デフォルトで、ACI サービス グラフ構成では、アクセスモード ポート グループが作成され、L4-L7 VM の vNIC に自動的に接続されます。

     - **[無差別モード（Promiscuous Mode）]**：L4-L7 仮想アプライアンスが、VM が所有する vNIC MAC 以外の MAC アドレス宛のトラフィックを受信する必要がある場合に必要です。

- **[VLAN]**：VMM ドメインのオプション構成であり、指定されていない場合は、ドメインに関連付けられたダイナミック VLAN プールから割り当てられます。
- **[拡張 LAG オプション（Enhanced LAG Option）]**：ハイパーバイザとファブリック間のポートチャネルに拡張 LACP を使用している場合。
- **[VM 名（VM Name）]**：この VMM ドメインと、ファイアウォール トラフィックで使用されるインターフェイス（**VNIC**）で使用可能なすべての VM のリストから、ファイアウォールの VM を選択します。

  展開するデバイス クラスタの種類に応じて、**[+ VM 情報の追加（+Add VM information）]** をクリックして追加のクラスタ ノードを指定します。

7. FW デバイス情報と PBR 宛先 IP アドレスを指定します。

   前述のように、このリリースでは、高可用性 FW クラスタの 3 つの展開オプション（active/standby クラスタ、active/active クラスタ、独立アクティブ ノード）がサポートされています。3 つのすべての展開オプションで、IP SLA ポリシー（手順 3 で説明）を使用すると、ファイアウォール ノードの IP アドレスのみを指定でき、対応する MAC アドレスが自動的に検出されます。

   異なるファブリックに異なる設計を展開できます。

   - Active/standby クラスタは、単一の MAC/IP ペアによって識別されます。

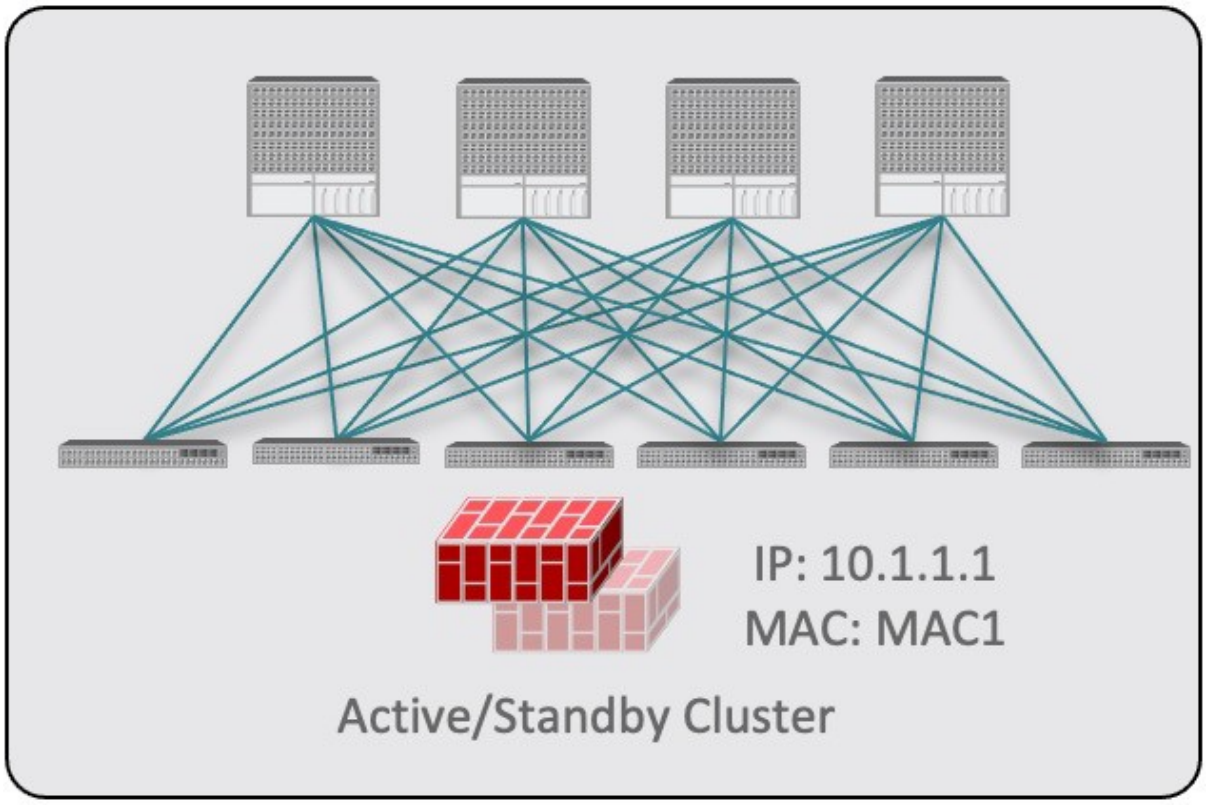

図 14.

この場合、アクティブなファイアウォール ノードを識別する単一の PBR 宛先 IP アドレスを指定し、クラスタ内のすべてのノードに関する情報も含める必要があります。
たとえば、2 ノードの active/standby クラスタの場合は、次のように指定します。

- 仮想ファイアウォール クラスタの場合、アクティブ ファイアウォール ノードとスタンバイ ファイアウォール ノードを表す VM と、PBR の宛先としてのアクティブ ファイアウォールの IP アドレスを表します。
- 物理ファイアウォール クラスタの場合、アクティブ ファイアウォール ノードおよびスタンバイ ファイアウォール ノードをファブリックのリーフ スイッチに接続するために使用されるインターフェイス（以下の具体例では vPC インターフェイス）と、PBR の宛先となるアクティブ ファイアウォールの IP アドレス。

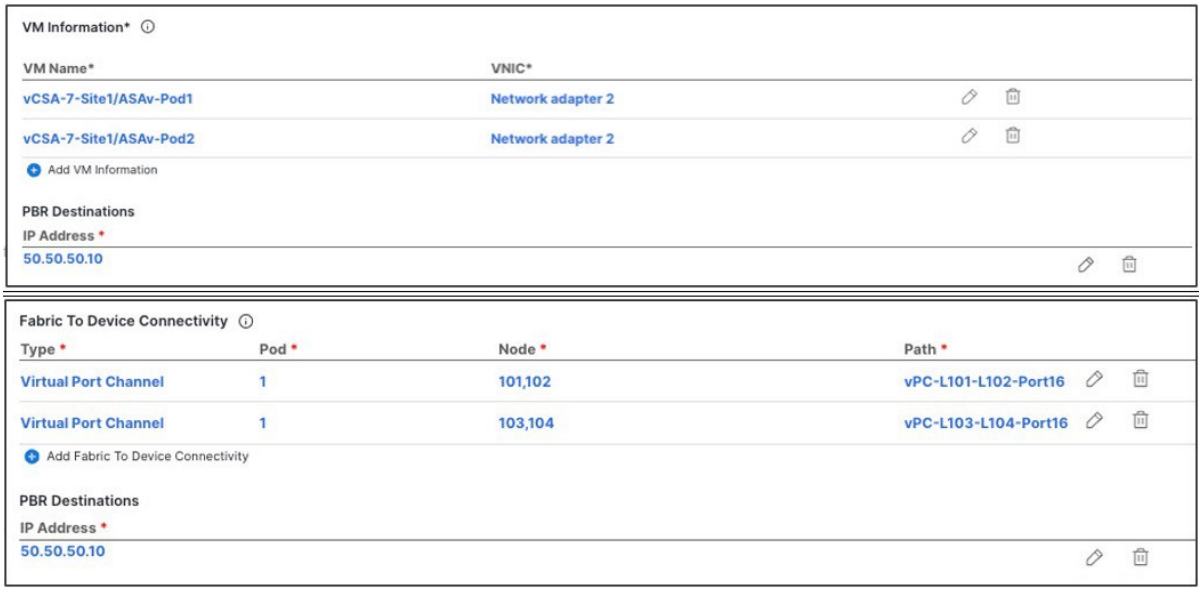

図 15.

- Active/active クラスタは、単一の MAC/IP ペアによっても識別されます。

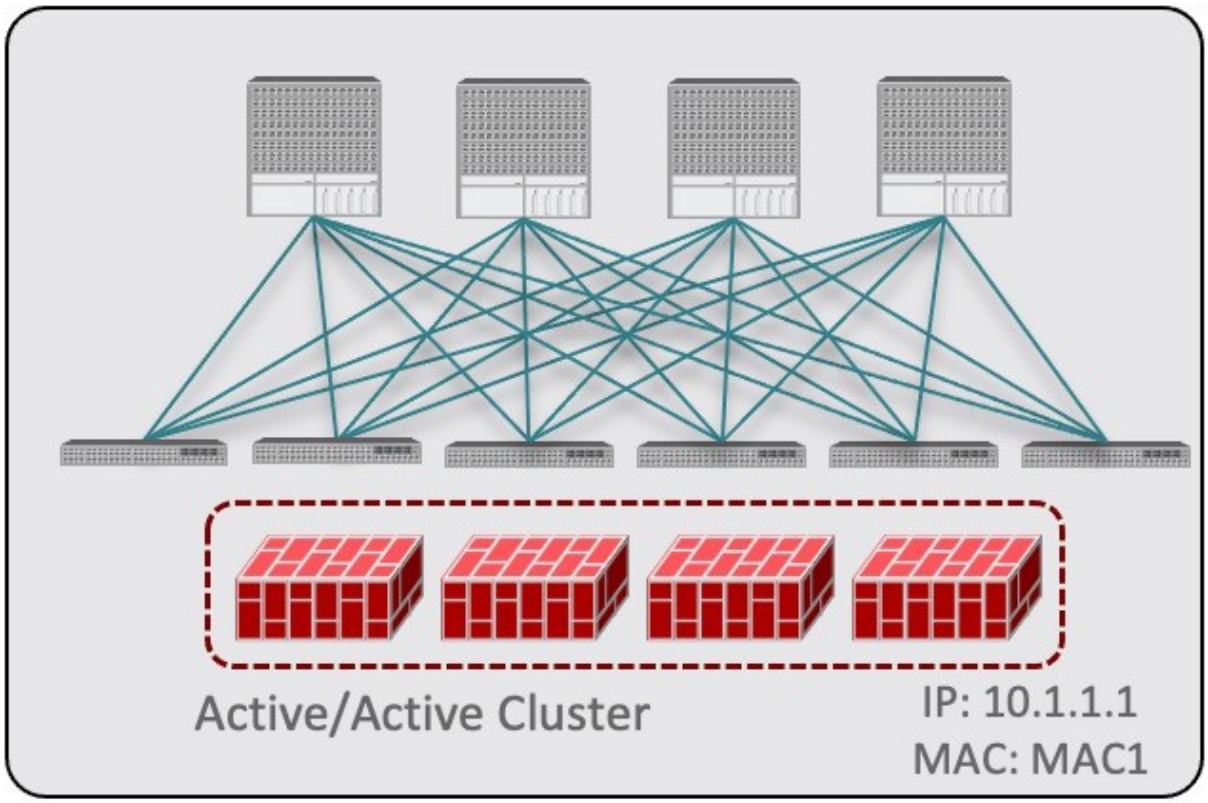

図 16.

Cisco ファイアウォール（ASA または FTD モデル）の場合、Active/Active クラスタは物理フォーム ファクタでのみサポートされ、すべてのクラスタ ノードは同じ MAC/IP アドレスを所有し、ACI リーフ スイッチのペアに展開された同じ vPC 論理接続に接続されている必要があります。次の図は、その結果として、単一の vPC インターフェイスと単一の IP アドレスを NDO で構成する方法を示しています。ここでは、前のユース ケースで説明した IP SLA ポリシーを使用すると、MAC アドレスが動的に検出されます。

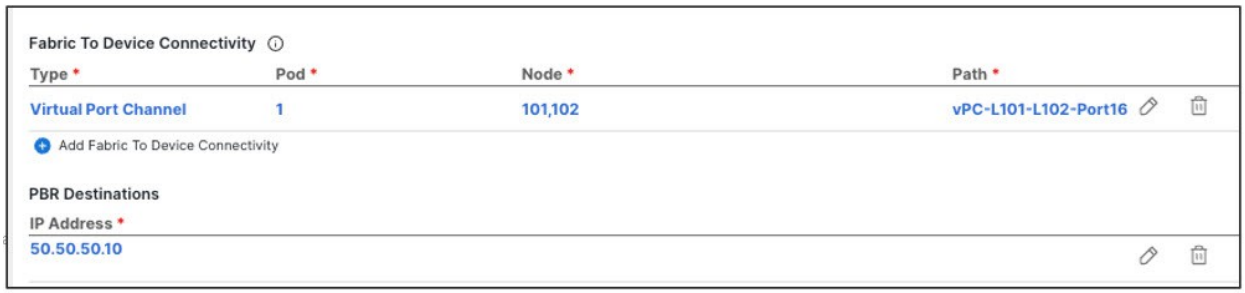

図 17.

- 独立したアクティブ ノード構成の場合、各アクティブ ノードは一意の MAC/IP アドレス ペアによって識別されます。

  対称 PBR により、トラフィックは両方向で同じアクティブ ノードによって処理されることに注意してください。

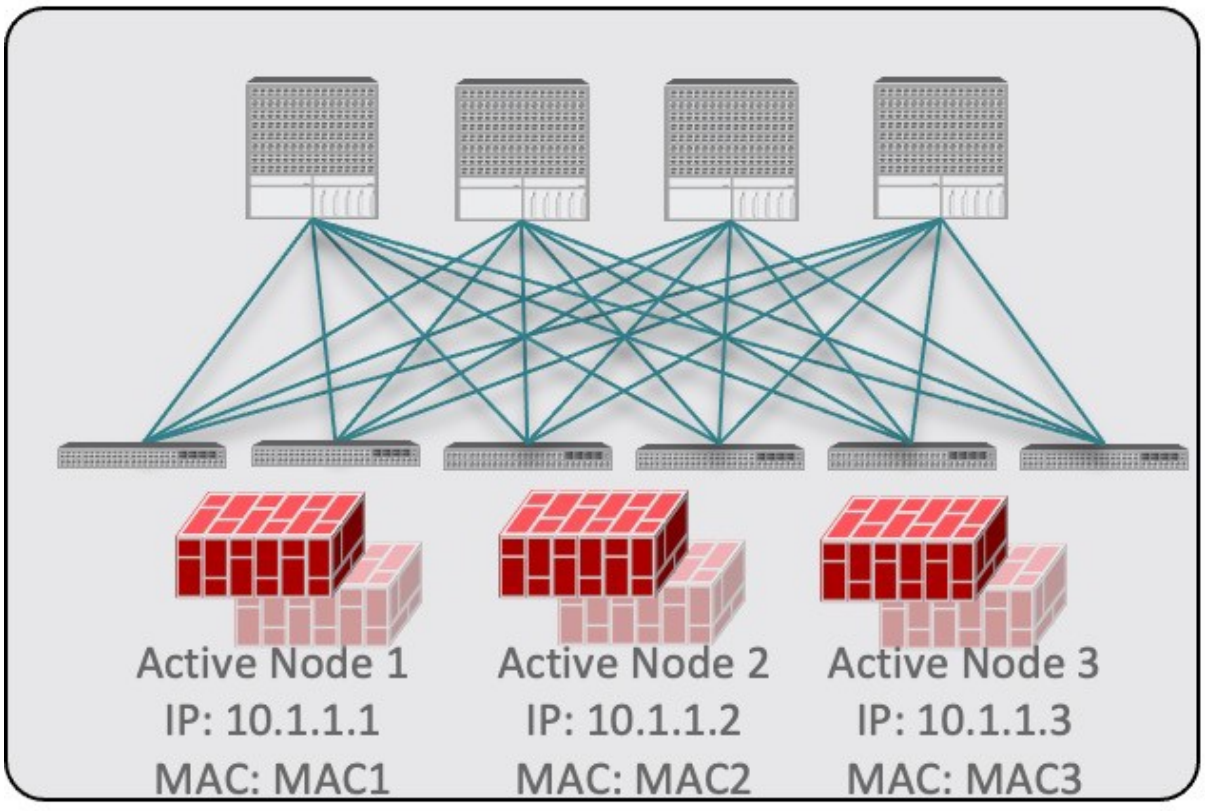

図 18

この場合、NDO 構成で各アクティブ ノードの個々の IP アドレスと各ノードの情報を指定する必要があります。
たとえば、3 つの独立したファイアウォール ノードを展開する場合は、次のように指定します。

- 仮想ファイアウォール フォーム ファクタの場合、3 つのファイアウォール ノードを表す VM と、PBR 宛先としての一意の IP アドレス。
- 物理ファイアウォールのフォーム ファクタの場合、各ファイアウォール ノードをファブリックのリーフ スイッチに接続するために使用されるインターフェイス（以下の具体例では vPC インターフェイス）と、PBR の宛先となる各ファイアウォール ノードの固有 IP アドレス。

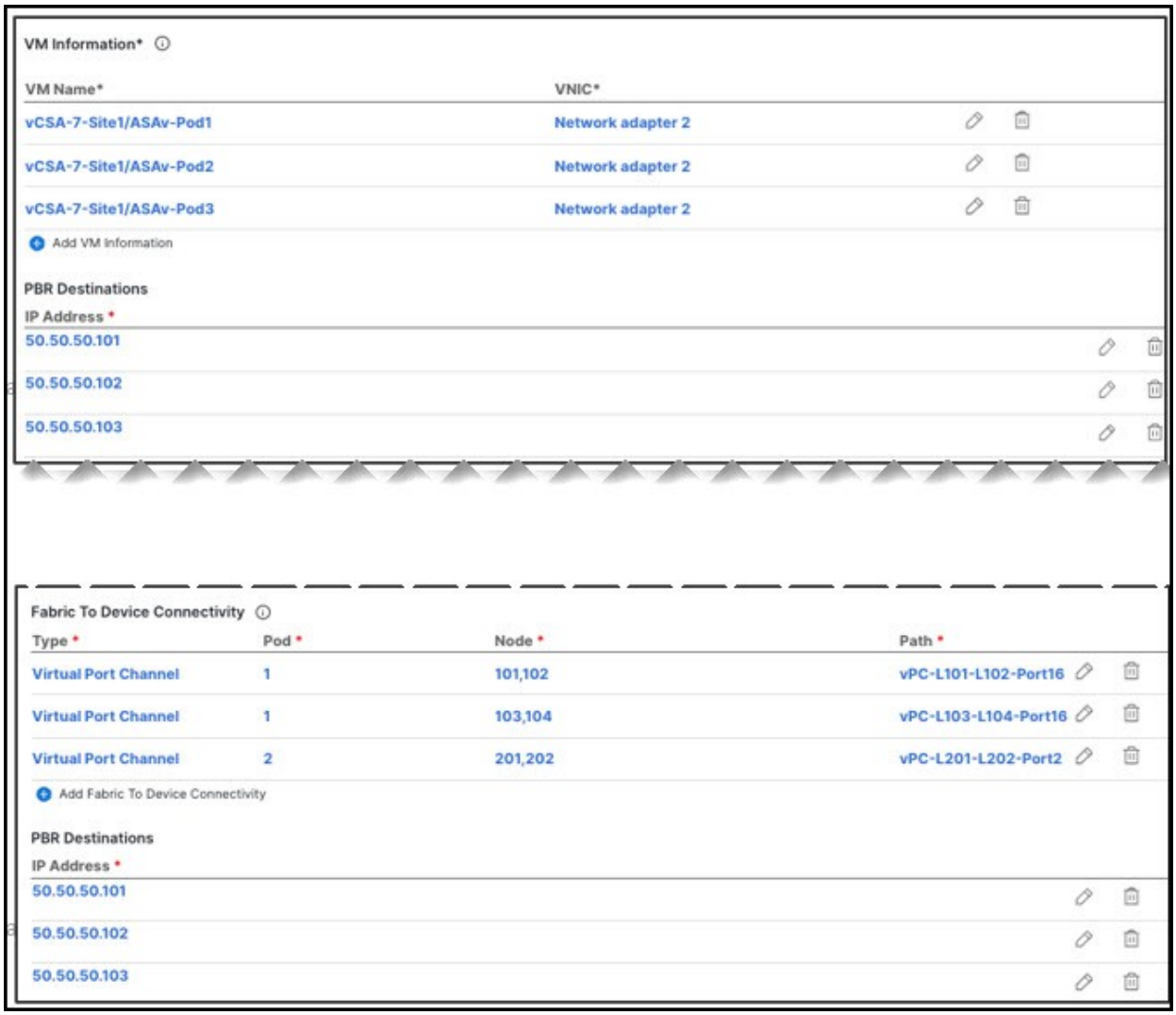

図 19.

a. **[デバイス接続にファブリックを追加（Add Fabric To Device Connectivity）]**（物理ドメイン）または **[VM 情報を追加（Add VM Information）]**（VMM ドメイン）をクリックします。

   前の手順で物理ドメインと VMM ドメインのどちらを選択したかに応じて、ファイアウォール VM またはファイアウォール デバイスへの物理ファブリック接続のいずれかの情報を指定します。

   物理ドメインの場合は、ポッド、スイッチノード、およびインターフェイス情報を指定します。

   VMM ドメインの場合は、VM 名と vNIC 情報を指定します。

b. **[PBR 宛先の追加（Add PBR Destination）]** をクリックして、サービス ブリッジ ドメインに接続されているファイアウォール上のインターフェイスの IP アドレスを指定します。

展開するデバイス クラスタの種類によっては、1 つ以上の PBR 宛先 IP アドレスを指定する必要があります。

これにより、ファイアウォールのインターフェイスに IP アドレスがプロビジョニングされるのではなく、その IP アドレスへのトラフィックのリダイレクトが構成されるだけです。特定のファイアウォール構成は NDO から展開されないため、個別にプロビジョニングする必要があります。

c. **[OK]** をクリックして、指定した構成を保存します。

d. テンプレートを関連付けた他のファブリックに対してこの手順を繰り返します。

8. テンプレートを保存して展開します。

a. **[サービス デバイス テンプレート（Service Device Template）]** レベルで、**[保存（Save）]** をクリックしてテンプレート構成を保存します。

b. **[テンプレート プロパティ（Template Properties）]** タブを選択し、**[テンプレートの展開（Deploy Template）]** をクリックして構成をファブリックにプッシュします。

c. （オプション）構成がファブリックレベルで作成されたことを確認します。

L4-L7 デバイスが APIC で構成されていることを確認するには、APIC GUI で **[<tenant-name>] > [サービス（Services）] > [L4-L7] > [デバイス（Devices）] > [<cluster-name>]** に移動します。これにより、デバイスクラスタが、前の手順で指定したすべての構成とともに表示されます。

PBR ポリシーが APIC で構成されたことを確認するには、**[<tenant-name>] > [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）]** に移動します。手順 *8i* で選択した IP SLA モニタリング ポリシーと手順 *7d* で提供した IP アドレスで定義された **<cluster-name>-one-arm** リダイレクトが表示されるはずです。

次に行う作業：

サービス デバイス構成を展開したら、「アプリケーション テンプレートの作成」の説明に従って、アプリケーション テンプレートおよびサービス チェーンを関連付けるコントラクトを作成します。

アプリケーション テンプレートの作成

始める前に：

- 「PBR を搭載した vzAny の 注意事項および制限事項」で説明されているように、要件を読んで満たしていることを確認します。
- vzAny を有効にするか、または有効にする VRF を作成し、これらの使用例に使用する必要があります。

  VRF がまだない場合は、通常どおりにアプリケーション テンプレートで VRF を作成できます。VRF 構成の詳細については、 「コントラクトとフィルタの作成」を参照してください。

次の手順では、PBR を使用した vzAny のユース ケースに使用するテナント テンプレートと構成オブジェクトを作成する方法について説明します。

1. Nexus Dashboard Orchestrator の GUI にログインします。
2. 左のナビゲーション ペインから、**[構成（Configure）] > [テナント テンプレート（Tenant Template）]** を選択します。
3. **[アプリケーション（Application）]** タブを選択します。
4. 構成を定義するスキーマを選択します。

   更新する既存のスキーマがある場合は、メイン ウィンドウ ペインでスキーマの名前をクリックするだけでかまいません。そうではない場合、新しいスキーマを作成する場合は、**[スキーマの追加（Add Schema）]** ボタンをクリックして、いつも通り、スキーマ情報を指定してください。

5. 構成を定義するテンプレートを選択します。

   更新する既存のテンプレートがある場合は、スキーマ ビューでテンプレートを選択します。

   

   これらの手順では、単一のアプリケーション テンプレートを作成し、両方のファブリックにすべてのオブジェクトを拡張する方法について説明しますが、拡張する必要があるのはサービス BD（BD FW-external）のみです。EPG BD は、ストレッチまたはファブリックローカルとして構成できます。 EPG のファブリックローカル BD を構成する場合は、それらのオブジェクト用に追加のアプリケーション テンプレートを作成し、特定のファブリックにのみ割り当てる必要があります。

   新しいテンプレートを作成するには:

   a. **[テンプレートの作成（Create Template）]** をクリックします。
   b. **[テンプレート タイプの選択（Select a Template type）]** 画面で、[ACI マルチクラウド（ACI Multi-Cloud）] を選択します。
   c. テンプレートの **[表示名（Display Name）]** を入力し、**[テナントの選択（Select a Tenant）]** を選択します。
   d. **[展開モード（Deployment Mode）]** では、[マルチファブリック（Multi-Fabric）] または [自律（Autonomous）] を選択できます。

この章で説明する PBR を使用した vzAny の使用例は、マルチファブリック テンプレートと自律テンプレートの両方に展開できます。自律テンプレートを作成することを選択した場合、リダイレクション ポリシーはファブリック内のトラフィック フローにのみ適用されます。

e. **[テンプレートに保存（Continue to Template）]** をクリックして情報を保存します。

f. **[アクション（Actions）]**、**[ファブリックの追加/削除（Add/Remove Fabrics）]** の順に選択し、テンプレートをサイトに関連付けます。

g. ストレッチされていないオブジェクト用に追加のテンプレートを作成する場合は、これらのサブステップを繰り返します。

6. コントラクトを作成します。

サービスデバイステンプレートで以前に定義したサービスデバイスをこのコントラクトに関連付けて、PBR 機能を有効にします。コントラクトは、プロビジョニングする特定のユースケースに応じて、vzAny および EPG/ExtEPG によって使用（消費/提供）されます。

a. **[テンプレート プロパティ（Template Properties）]** ビューで、**[オブジェクトの作成（Create Object）][コントラクト（Contract）]** を選択して新しいコントラクトを追加します。

b. コントラクトの名前を指定します。

たとえば、vzAny-to-vzAny です。

c. **[範囲（Scope）]** ドロップダウンから、[VRF] を選択します。

コントラクトの範囲を VRF に設定する必要があります。

d. **[+フィルタの作成（+Create Filter）]** をクリックして、1 つ以上のコントラクト フィルタを追加します。

たとえば、すべてのトラフィックをリダイレクトする Permit-IP コントラクト フィルタを作成できます。

e. ここでは、**[サービス チェーン/サービス グラフ（Service Chaining/Service Graph）]** の構成をスキップします。次のセクションで、サービス デバイス テンプレートをこのコントラクトに関連付けます。

f. 通常どおりに他のコントラクト オプションを定義し、**[OK]** をクリックして保存します。

7. VRF で必要な設定を有効にします。

a. vzAny with PBR のユース ケースに使用する VRF を選択します。

通常どおり、既存の VRF を使用することも新しい VRF を作成することもできます。

b. **[vzAny]** を有効にし、前の手順で作成した **[コントラクトの追加（Add Contract）]** を行います。

コントラクト **[タイプ（Type）]** は、構成する使用例によって異なります。

- VRF 内通信（vzAny-to-vzAny）の使用例では、コントラクトを VRF に 2 回割り当てます。1 回はコンシューマとして、もう 1 回はプロバイダとして割り当てます。

- VRF（vzAny）内のすべての EPG と同じ VRF の一部である特定の EPG 間の多対 1 の通信では、コンシューマとして vzAny EPG、プロバイダとして特定の EPG とする場合は、コントラクトをコンシューマとして割り当てます。
- 同様に VRF（vzAny）内のすべての EPG と同じ VRF の一部である特定の外部 EPG 間の多対 1 の通信では、vzAny EPG が L3Out 外部 EPG によって提供されるサービスを利用する場合は、コントラクトをコンシューマとして割り当てます。

c. **[ファブリック対応ポリシー適用モード（Fabrics-aware Policy Enforcement Mode）]** を有効にします

新しい vzAny PBR の使用例を有効にするには、VRF で [ファブリック認識ポリシー適用モード（Fabric-Aware Policy Enforcement Mode）] 設定を有効にする必要があります。

> **[ファブリック認識ポリシー適用モード（Fabric-Aware Policy Enforcement Mode）]** オプションを有効または無効にすると、リーフ スイッチでゾーン分割ルールを更新する必要があるため、短時間のトラフィックの中断（EPG 間の既存のコントラクトを含む）が発生します。この操作はメンテナンス期間中に実行することを推奨します。
> [ファブリック対応ポリシー適用モード（Enabling Fabric-aware Policy Enforcement Mode）] **を有効にすると、**TCAM の使用率が増加します。既存のコントラクトのリーフ スイッチでの TCAM 使用率が増加します。コントラクト許可ロギングをこのオプションと組み合わせて使用することはできません。

d. **[L3 マルチキャスト（L3 Multicast）]** を有効にします。

この章で前述した会話型学習機能を有効にするには、vzAny VRF の L3 マルチキャスト オプションを有効にする必要があります。

e. **[OK]** をクリックして、変更内容を保存します。

8. サービス BD が、前の手順で vzAny コントラクトに使用したものと同じ VRF に関連付けられていることを確認します。
9. ハードウェア プロキシ モードで構成されたアプリケーション ブリッジ ドメインを作成します。

次の手順で作成する各アプリケーション EPG には、BD を関連付ける必要があります。

a. **[テンプレート プロパティ（Template Properties）]** ビューで、**[オブジェクトの作成（Create Object）] > [ブリッジ ドメイン（Bridge Domain）]** を選択します。

b. BD の名前を入力します。

たとえば、BD-App などです。

c. **[仮想ルーティングと転送（Virtual Routing & Forwarding）]** ドロップダウンから、前の手順で作成された VRF を選択します。

d. 通常どおりに他の BD オプションを定義します。

使用可能なすべての BD 構成の詳細については、「ブリッジ ドメインの構成」を参照してください。

e. **[OK]** をクリックして、変更内容を保存します。

f. この手順を繰り返して、2 番目の BD を作成します。

上の図に従って、BD の名前に [BD-Web] を使用します。

10. EPG を作成します。

この手順では、特定のユース ケースに応じて、2 つのアプリケーション EPG またはアプリケーション EPG と外部 EPG のいずれかを設定します。

a. **[+オブジェクトの作成（+Create Object）] > [アプリケーション プロファイル（Application Profile）]** を選択して、アプリケーション プロファイルを作成します。

b. **[+オブジェクト EPG の作成（+Create ObjectEPG）]** を選択し、作成したアプリケーション プロファイルを選択します。

c. プロパティペインで、EPG の **[表示名（Display Name）]** を入力し、この EPG 用に作成した BD を選択します。

たとえば、EPG-App です。使用可能なすべての BD 構成の詳細については、「アプリケーション プロファイルと EPG の構成」を参照してください。

d. 通常どおりに他の EPG オプションを定義します。

使用可能なすべての BD 構成の詳細については、「ブリッジ ドメインの構成」を参照してください。

e. **[OK]** をクリックして、変更内容を保存します。

f. 2 番目の EPG を作成します。

EPG のタイプとそのコントラクト構成は、構成する使用例によって異なります。

- 任意の VRF 内通信（vzAny-to-vzAny）。

  これは「トラフィック フロー：VRF 内 vzAny-to-vzAny」に記されている使用例であり、同じ VRF で 2 番目の EPG を簡単に作成できます。たとえば、EPG-Web を作成し、BD-Web ブリッジドメインを割り当てます。

- VRF（vzAny）内のすべての EPG と同じ VRF の一部である特定の EPG 間の多数対 1 の通信。

  この場合、同じ VRF 内に 2 番目の EPG を作成しますが、プロバイダとしてコントラクトを明示的に割り当てます（特定の EPG の vzAny VRF コントラクトはコンシューマとして割り当てられます）。

- VRF（vzAny）内のすべての EPG と、同じ VRF の一部である特定の外部 EPG 間の多数対 1 の通信。

  この場合、代わりに外部 EPG を作成し（**[+オブジェクトの作成（+Create Object）] > [外部 EPG（External EPG）]**）、L3Out を外部 EPG に関連付けてから、コントラクトをプロバイダとして外部 EPG に明示的に割り当てる必要があります。

11. **[スキーマの保存（Save Schema）]** をクリックして、構成を保存します。

ファイアウォールのリダイレクトなしでエンドポイント間の望ましくない通信を回避するために、次のセクションで説明するようにサービス チェーンが構成されるまで、テンプレートを展開しないことをお勧めします。

この段階で、PBR を使用したサービス チェーンを追加せずに、2 つの EPG 間の vzAny 通信の基本的なユース ケースを効果的に構成しました。

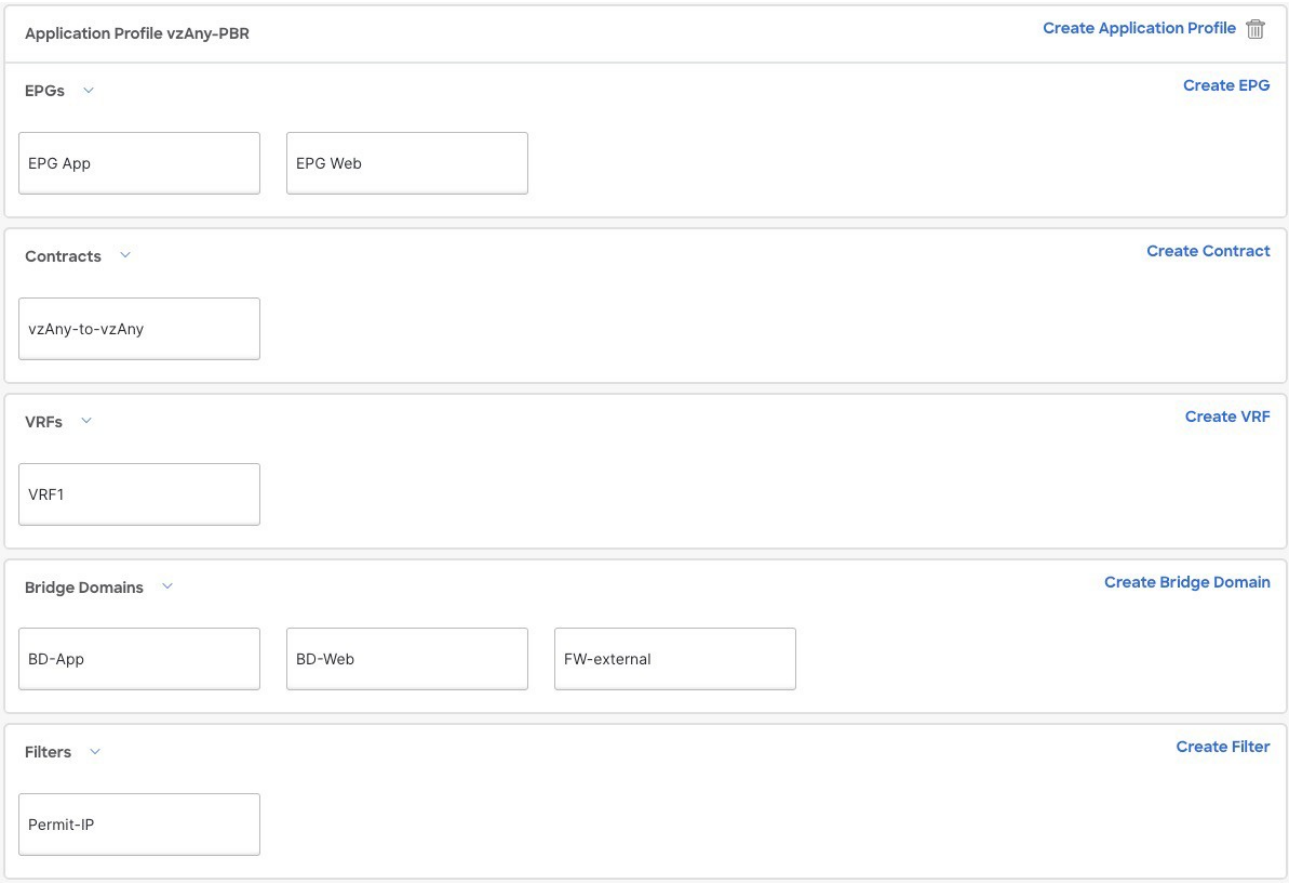

図 20.

次のセクションでは、前のセクションで作成したサービス デバイスを前の手順で作成したコントラクトに関連付ける方法について説明します。

次に行う作業：

アプリケーション テンプレートとコントラクトを作成したら、「コントラクトへのサービス チェーンの追加」の説明に従って、サービス デバイスとコントラクトの関連付けに進みます。

コントラクトへのサービス チェーンの追加

始める前に：

- 「サービス デバイス テンプレートの作成」の説明に従って、デバイス構成を含むサービス デバイス テンプレートを作成して展開しておく必要があります。
- 「アプリケーション テンプレートの作成」で説明されているように、アプリケーション ブリッジ ドメインと EPG を含むアプリケーション テンプレートを作成しておく必要があります（まだ展開はしません）。

アプリケーションとサービス デバイス テンプレートを作成した後、前のセクションで作成したサービス デバイスにコントラクトを関連付けることで、ポリシーベースのリダイレクションを追加できます。

1. 前のセクションで作成したアプリケーション テンプレートに戻ります。
2. 前のセクションで作成したコントラクトを選択します。
3. **[サービス チェーン（Service Chaining）]** エリアで、**[+ サービス チェーン（+Service Chaining）]** をクリックします。

これらの手順は、「サービス デバイス テンプレートの作成」で説明されているように、リリース 4.2(3) で導入された新しいサービス デバイス テンプレート ワークフローを使用して、この使用例の新しいサービス デバイスを構成していることを前提としています。アプリケーション テンプレートでサービス グラフがすでに定義されている場合は、代わりに [サービス グラフ（Service Graph）] を選択し、既存のサービス グラフを選択します。ただし、[サービス グラフ（Service Graph）] オプションは将来のリリースで廃止されることに注意してください。

4. **[デバイス タイプ（Device Type）]** で、[ファイアウォール（Firewall）] を選択します。

   このリリースでは、ワンアーム ファイアウォール サービス グラフのみがサポートされます。

5. **[デバイス（Device）]** ドロップダウンから、前の手順で作成した FW デバイス クラスタを選択します。
6. **[コンシューマ コネクタ タイプのリダイレクト（Consumer Connector Type Redirect）]** が有効になっていることを確認します。
7. **[プロバイダ コネクタ タイプのリダイレクト（Provider Connector Type Redirect）]** が有効になっていることを確認します。
8. **[追加（Add）]** をクリックして続行します。
9. **[保存（Save）]** をクリックして、テンプレートを保存します。
10. **[テンプレートの展開（Deploy）]** をクリックして、展開します。

最初の発行日：2024-03-11
最終更新日：2024 年 7 月 26 日

米国本社
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax：408 527-0883