PBR を使用した vzAny

PBR を使用した vzAny の概要

次のセクションでは、マルチサイト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、要件とガイドライン、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(1) より前は、次の基本的な vzAny のユース ケース（PBR なし）がマルチサイト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 VRF 内のすべての EPG が単一の EPG から共有サービスを利用できるようになります。

NDO リリース 4.2(1) 以降、PBR を使用した vzAny の次の追加のユース ケースは、APIC リリース 6.0(3) 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サイト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 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 のユース ケース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、構成する特定のユース ケース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(1) 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、設定が必要な特定のテナントとすべてのサイトに関連付けます。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、次の PBR 注意事項および制限事項を持つ vzAny （10 ページ） セクション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 デバイスのサイトレベル構成を提供し、展開します。

（注） リリース 4.2(1) およびサービス デバイス テンプレートの導入以降、PBR のユース ケースについて 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、サイトの 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サイトへの割り当て。
   - 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 はサイト間で拡張する必要がありますが、EPG に使用する BD は拡張またはサイト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 契約に関連付けます。

トラフィック フロー：Intra-VRF vzAny-to-vzAny

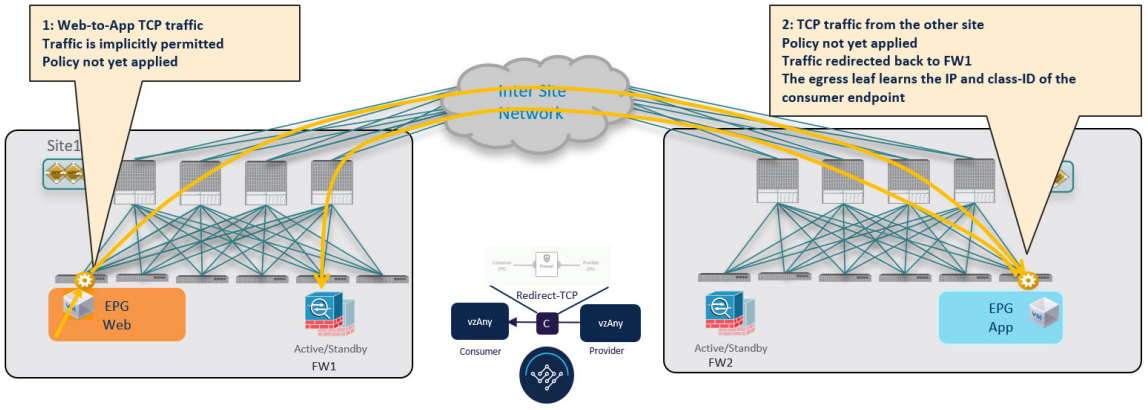
このセクションでは、異なるサイトの特定の VRF の論理 vzAny 構造の一部である 2 つの EPG 間のトラフィック フローを要約します。このユース ケースでは、vzAny は PBR コントラクトのプロバイダとコンシューマの両方です。

（注） この場合、2 つのサイト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に、両方向のトラフィック フローは両方のファイアウォールを介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 サイトとリモート サイトの両方の 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 サイト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、このユースケース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、フローがサイト 1 で発生したが、そのサイト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、サイト 2 のプロバイダー リーフはサイト 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



サイト 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、トラフィックはサイト 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サイト 1 から送信されている間に、そのサイト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されます。

図 *2*：会話型学習

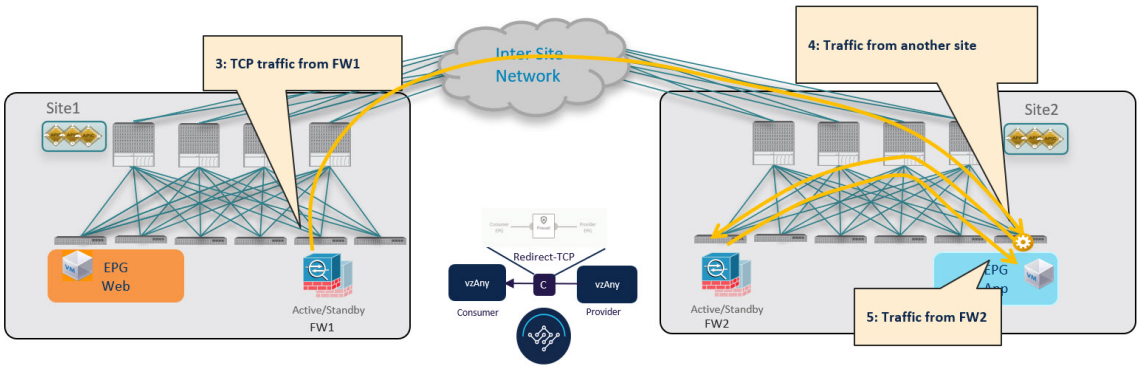
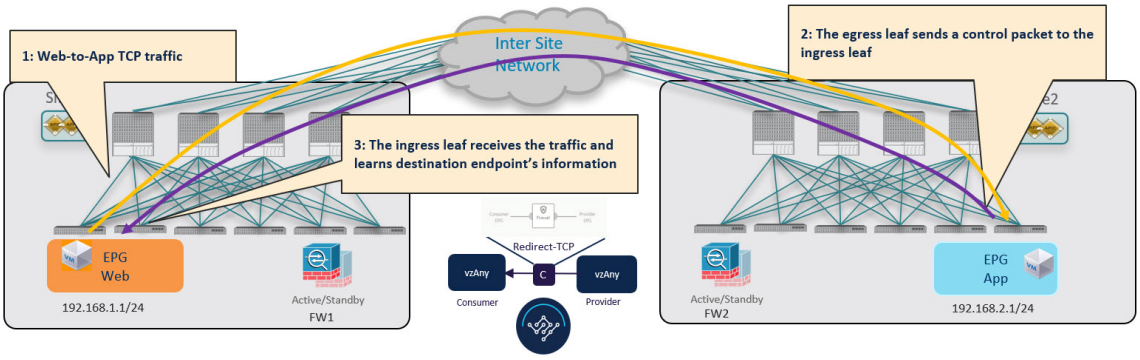


図 1 : 会話型学習 （3 ページ）上記のようにトラフィックの準最適なバウンスを回避するために、プロバイダ リーフ スイッチは特別な制御パケットを生成し、サイト 1 のコンシューマ リーフ スイッチに送信します。これにより、コンシューマ リーフはプロバイダ エンドポイントのクラス ID 情報を学習できます。

（注） 最初のフローが provider-to-consumer への方向で確立される場合、consumer-to-provider へのトラフィック方向について前述したのと同じ動作が適用されます。

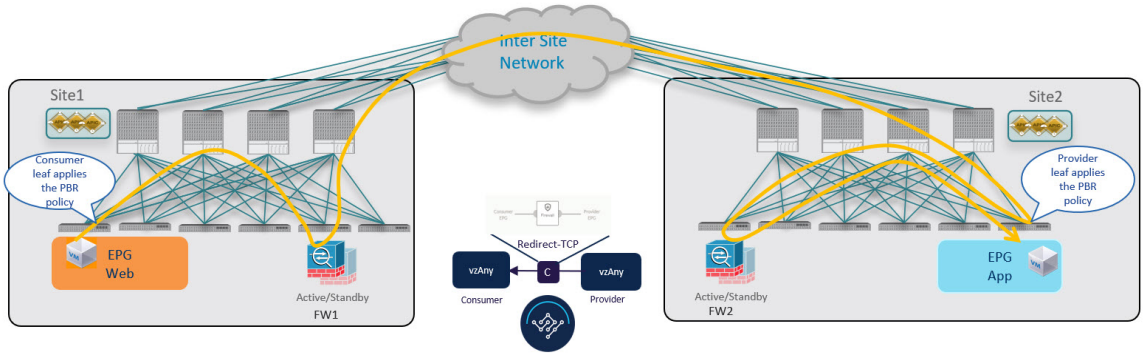
図 *3*：会話型学習



Consumer-to-Provider 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。

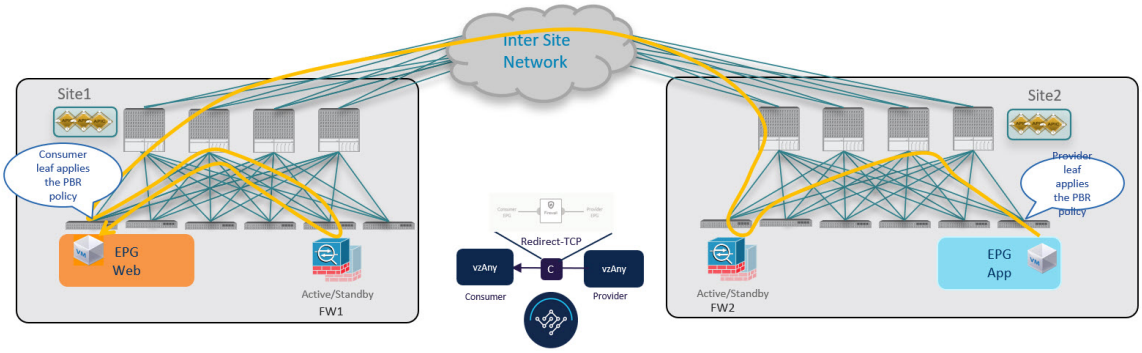
図 *4 : Consumer-to-Provider* へのトラフィック フロー



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、図 1 : 会話型学習 （3 ページ） に示されているダイレクト 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 *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

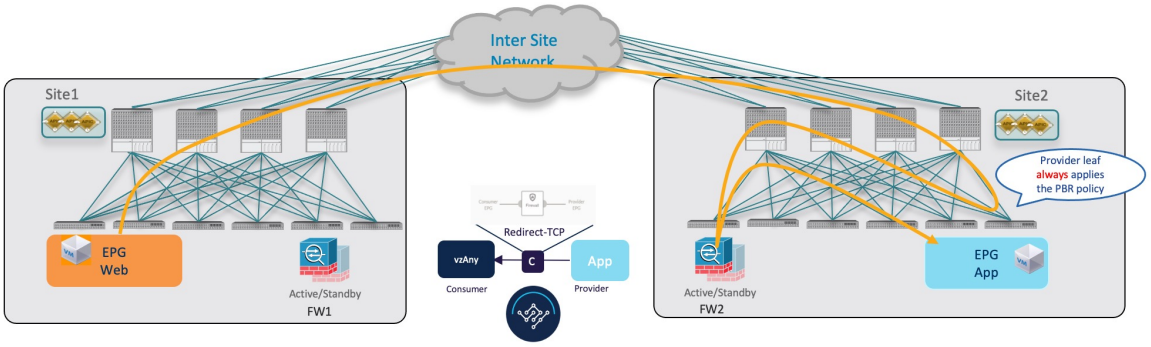
このセクションでは、特定の VRF の論理 vzAny 構造の一部であるコンシューマ EPG と同じ VRF の一部であるプロバイダ EPG 間のトラフィック フローを要約します。このユース ケースでは、vzAny は PBR コントラクトのコンシューマですが、特定の EPG はプロバイダです。

（注） トラフィックが常に両方のサイト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 のユース ケースとは異なり、vzAny-to-EPG は常にプロバイダのサイト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 はプロバイダ EPG のリーフ スイッチにトラフィックを直接送信します。

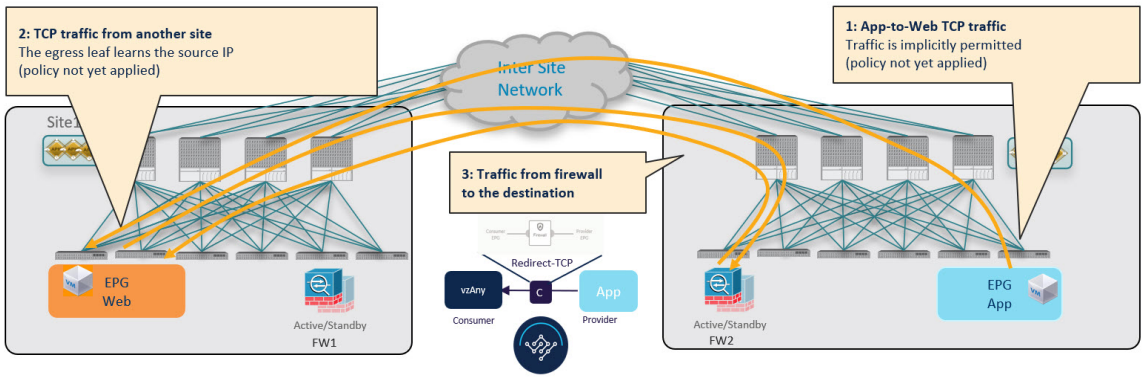
図 *6 : vzAny-to-EPG* のコンシューマからプロバイダへのトラフィック フロー



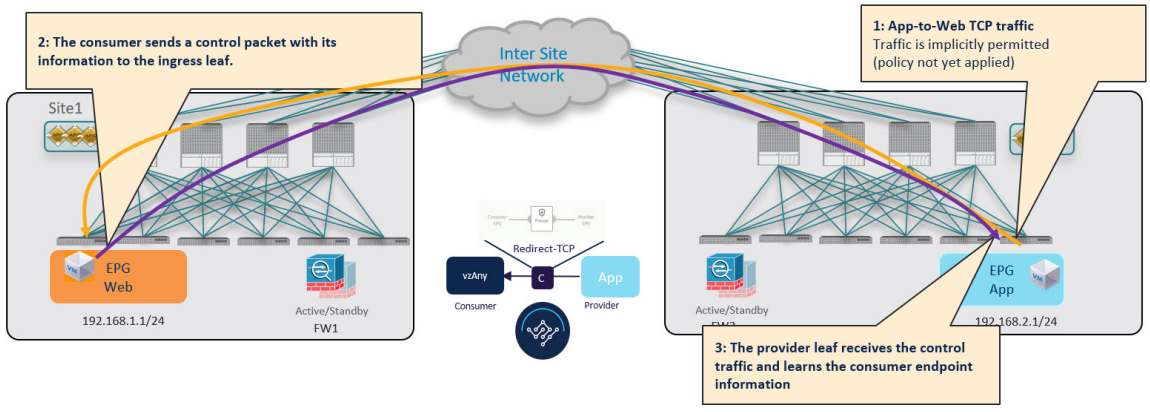
Provider-to-Consumer トラフィック フロー（内部トラフィックおよび会話型学習）

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、トラフィックはサイト間でコンシューマ 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 サイト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）



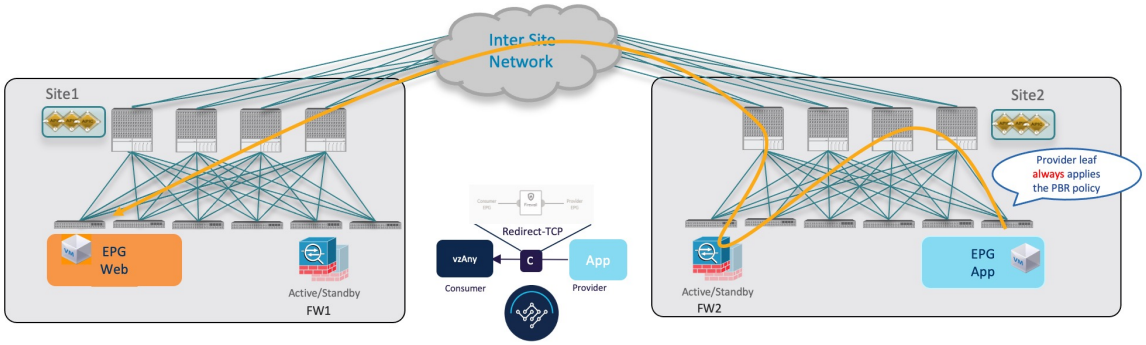
この準最適トラフィック フローは無期限に継続できますが、コンシューマ EPG のリーフ スイッチは、今後のトラフィックを最適化し、両方のサイト間でバウンスしないようにするために、コンシューマ エンドポイント情報を含む別の制御パケットをプロバイダ リーフ スイッチにも送信します。



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、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 （6 ページ） 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 *8 : 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）

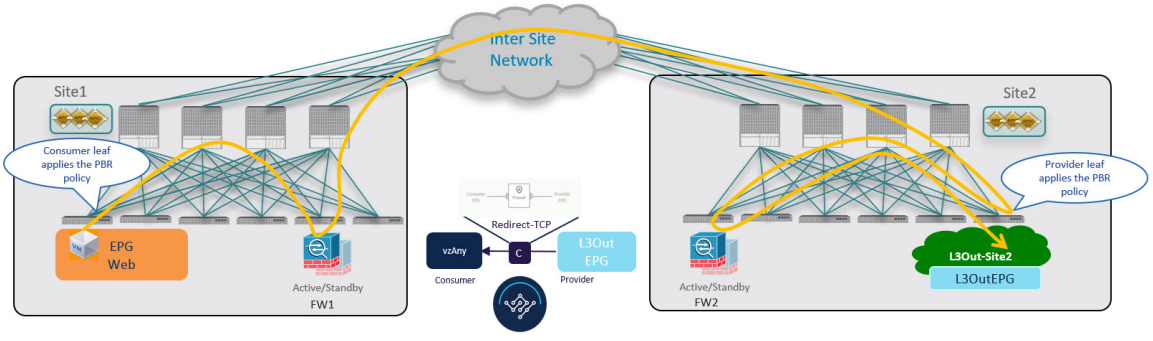
このセクションでは、特定の VRF の論理 vzAny 構造の一部である EPG と、別のサイトの同じ VRF の一部である外部 EPG（L3Out）間のトラフィック フローを要約します。このユース ケースでは、vzAny は vzAny コントラクトのコンシューマであり、L3Out に関連付けられた外部 EPG はプロバイダです。

（注） このユース ケースでは、トラフィックは常に両方のサイト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。トラフィックはサイト 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。

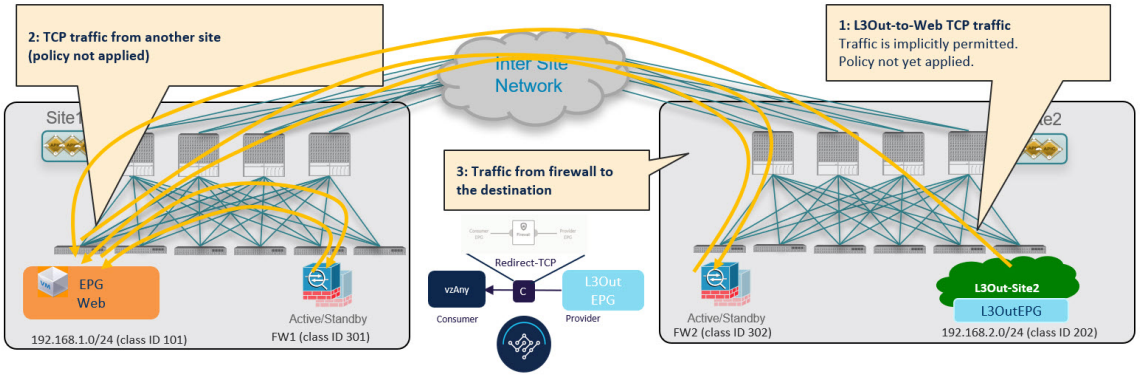
図 *9 : vzAny-to-L3Out* コンシューマからプロバイダへのトラフィック フロー



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）

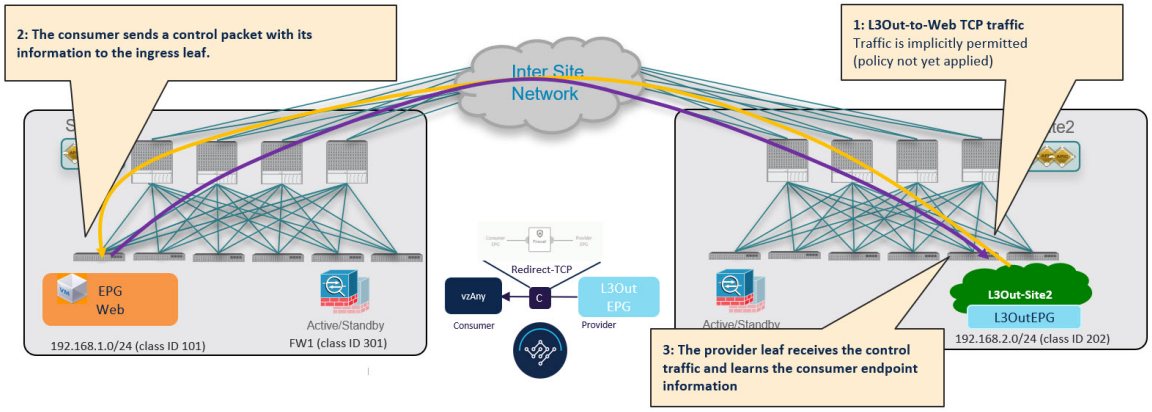
プロバイダ リーフ スイッチがコンシューマ エンドポイント情報を学習する前に、トラフィックをローカル ファイアウォールにリダイレクトするポリシーを適用できないため、トラフィックはサイト間でコンシューマ リーフ スイッチに送信されます。ポリシーが適用されなかったため（パケット内の制御ビットによって示される）、コンシューマ リーフ スイッチはトラフィックをインスペクションのためにプロバイダ サイトのファイアウォールにリダイレクトし、最終的にトラフィックをコンシューマ エンドポイントに転送します。

図 *10 : 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、両方のサイト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。

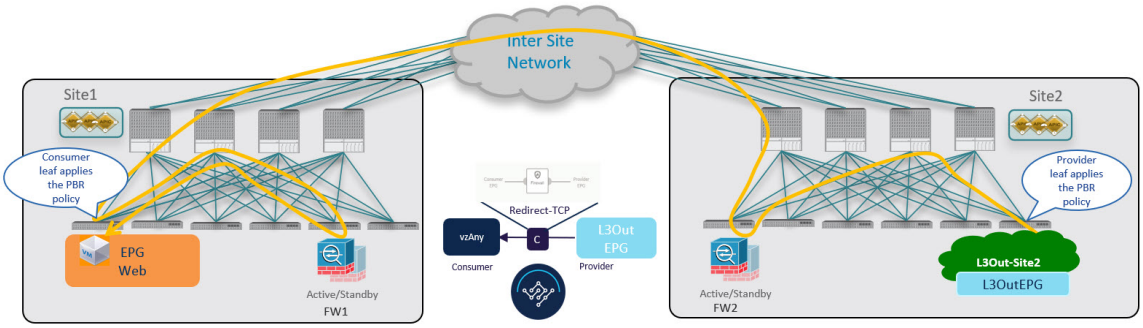
図 *11 : vzAny-to-L3Out* プロバイダーからコンシューマへのトラフィックフロー（初期トラフィックおよび会話型学習）



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、サイト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 *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



PBR 注意事項および制限事項を持つ vzAny

マルチサイト展開の 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。

（注） 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 の概念と使用例については、「vzAny コントラクト」の章を参照してください。

- 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のみ、vzAny トラフィックの単一ノード ファイアウォールへのリダイレクトが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。

  - サイト間の 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、コンシューマ EPG サブネットが構成されていない場合にのみ有効になります。サブネットを持つ EPG とサブネットのない 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(1) 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。

（注） 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、サイト全体に拡張する必要があります。

  この章で説明する PBR の使用例を有効にするには、vzAny VRF に対して [サイト対応ポリシーの適用（Site-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 設定の詳細については、VRF の設定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 を拡張する必要があります。

  次のセクションでは、これらのユース ケースに使用するサービス デバイスのブリッジ ドメイン（BD）がすでにあることを前提としています。

  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 BD を作成できます。BD 構成の詳細については、「ブリッジ ドメインの設定」を参照してください。

- コンシューマ、プロバイダ、およびサービス BD は、プロキシモードで構成する必要があります。

- 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。

  - 既存の構成を新しいサービス デバイス テンプレートにインポートします。

    このリリースでは、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する場合、PBR 構成を使用した vzAny のグリーンフィールド展開のみがサポートされます。以前にサポートされていたサービス グラフ オブジェクト構成を使用して、既存のサービス グラフ構成を APIC からアプリケーション テンプレートにインポートし、新しい vzAny PBR ユース ケースを展開できます。ただし、アプリケーション テンプレートのサービス グラフ オブジェクトは、今後のリリースで廃止される予定です。

  - L3Out の PBR 接続先。

  - [サービス グラフのコピー（Copy Service Graph）] 機能を使用したサービス グラフ デバイスのコピー。

  - 管理対象モード サービス グラフ。

    この機能は、APIC リリース 5.2(1) で廃止されました。

- リモート リーフ構成。
- ハイブリッド クラウド展開。

  この章で説明するすべての vzAny と PBR の使用例は、オンプレミスのマルチサイト展開にのみ適用され、オンプレミスのファブリックとクラウドリソースを相互接続するハイブリッド クラウド ソリューションには適用されません。

サービス デバイス テンプレートの作成

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。

始める前に

- PBR 注意事項および制限事項を持つ vzAny （10 ページ） 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 構成は ブリッジ ドメインの設定 で詳細が説明されています。

ステップ 1 Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 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。

ステップ 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）]** > **[サイトの追加/削除（Add/Remove Sites）]** を選択し、それらのサイト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（IPSLA Monitoring Policy）]** を選択します。
f) ポリシーの**名前**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。

ステップ 4 サービス デバイス テンプレートを作成し、テナントおよびサイトに関連付けます。

a) **テナント テンプレートの > 構成** （Configure 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）] > [サイトの追加/削除（Add/Remove Sites）]** を選択し、それらのサイト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。

ステップ 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設定）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。サイトレベルでファイアウォール展開モデルを選択でき、同じ Multi-Site 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ユースケースに基づいて事前に入力されています。

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 のユース ケース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、`[L3]` を選択します。

e) **[接続モード（Connectivity Mode）]** の場合、`[ワン アーム（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。

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 注意事項および制限事項を持つ vzAny （10 ページ） の一部として作成した拡張サービス BD です（例：`FW-external`）。

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）]** 領域で **[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**：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。

  （注） vzAny-to-EPG ユースケースのロードバランシング ハッシュは変更できますが、vzAny-to-vzAny、vzAny-to-ExtEPG、および ExtEPG-to-ExtEPG ユース ケース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。

  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設定できます。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 レベルの設定）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、やはりサイトローカル 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。

ステップ 6 前の手順で作成したサービス デバイス クラスタのサイト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、**<site-name>** タブをクリックします。
b) サイト 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。

このサイト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**：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**：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**：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**：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**：この VMM ドメイン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、ファイアウォール トラフィックに使用されるインターフェイス（**VNIC**）を選択します。

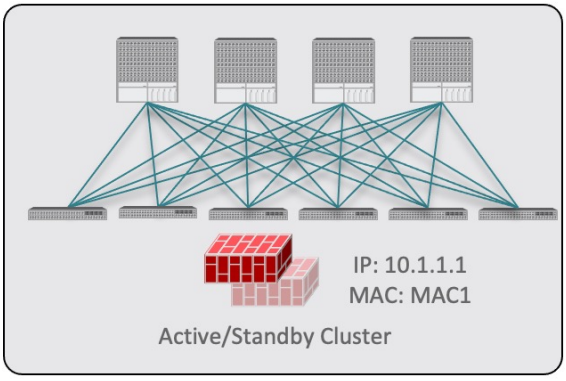
    展開するデバイス クラスタの種類に応じて、**[+ VM 情報の追加（+Add VM information）]** をクリックして追加のクラスタ ノードを指定します。

ステップ 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。

（注） 異なるサイトに異なる設計を展開できます。

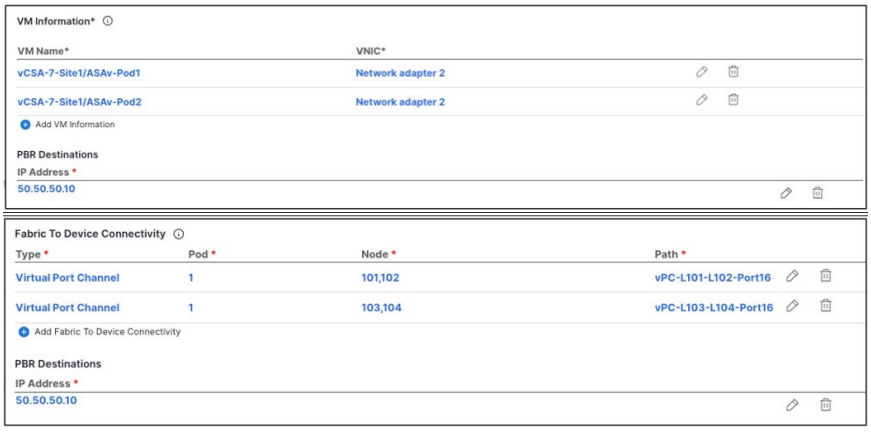
- Active/standby クラスタは、単一の MAC/IP ペアによって識別されます。



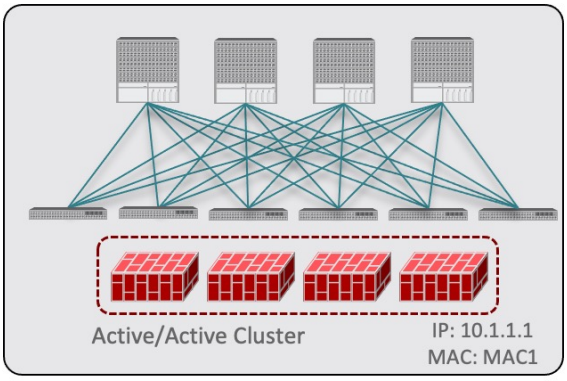
この場合、アクティブなファイアウォール ノードを識別する単一の PBR 宛先 IP アドレスを指定し、クラスタ内のすべてのノードに関する情報も含める必要があります。

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。

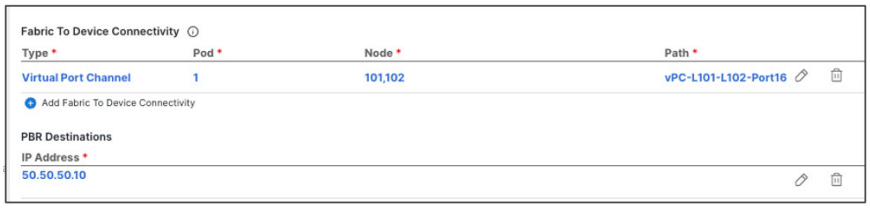
- 仮想ファイアウォール クラスタの場合、アクティブ ファイアウォール ノードとスタンバイ ファイアウォール ノードを表す VM と、PBR の宛先としてのアクティブ ファイアウォールの IP アドレスを表します。
- 物理ファイアウォール クラスタの場合、アクティブ ファイアウォール ノードおよびスタンバイ ファイアウォール ノードをファブリックのリーフ スイッチに接続するために使用されるインターフェイス（以下の具体例では vPC インターフェイス）と、PBR の宛先となるアクティブ ファイアウォールの IP アドレス。



- 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。

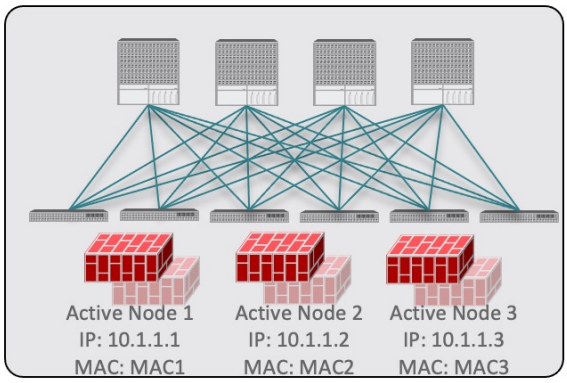


Cisco ファイアウォール（ASA または FTD モデル）の場合、Active/Active クラスタは物理フォームファクタでのみサポートされ、すべてのクラスタ ノードは同じ MAC/IP アドレスを所有し、ACI リーフ スイッチのペアに展開された同じ vPC 論理接続に接続されている必要があります。その結果、次の図は、単一の vPC インターフェイスと単一の IP アドレスを NDO でプロビジョニングする方法を示しています。ここでは、前のユース ケースで説明した IPSLA ポリシーを使用すると、MAC アドレスが動的に検出されます。



- 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。

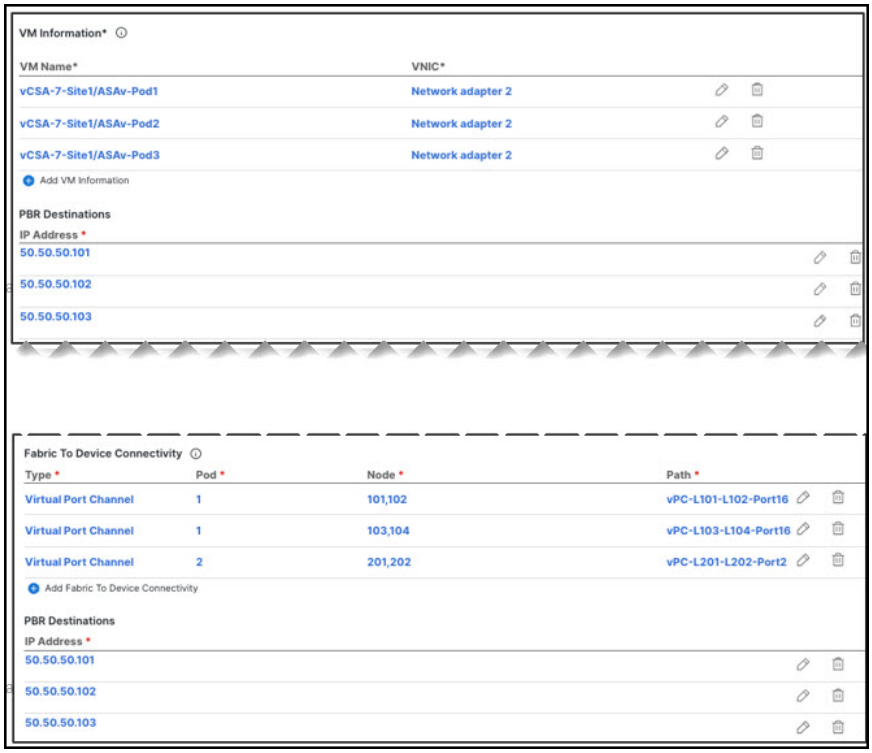
  対称 PBR により、トラフィックは両方向で同じアクティブ ノードによって処理されることに注意してください。



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。



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。

（注） 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、構成を保存します。
d) テンプレートを関連付けた他のサイトに対してこの手順を繰り返します。

ステップ 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サイトにプッシュします。
c) （オプション）構成がサイト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 で設定されていることを確認するには、APIC GUI で **<*tenant-name*>** > **Services** > **L4-L7** > **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>** > **Policies** > **Protocol** > **L4-L7 Policy-Based Redirect**に移動し、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。

次のタスク

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 （19 ページ）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

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。

始める前に

- PBR 注意事項および制限事項を持つ vzAny （10 ページ） 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 構成は、コントラクトとフィルタの作成 で詳細が説明されています。

ステップ 1 Nexus Dashboard Orchestrator の GUI にログインします。
ステップ 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。

ステップ 3 [アプリケーション（Application）] タブを選択します。

ステップ 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。

ステップ 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。

（注） 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、両方のサイト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、ストレッチまたはサイトローカルとして構成できます。 EPG のサイトローカル 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、特定のサイト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、`[マルチサイト（Multi-Site）]` 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 のユース ケースは、マルチサイト テンプレートと自律型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）]>、[サイトの追加/削除（Add/Remove Sites）]** 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。

ステップ 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) **[スコープ（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**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。

ステップ 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）]** を選択します。

コントラクト **タイプ**は、構成するユース ケースによって異なります。

- VRF 内通信（vzAny-to-vzAny）のユース ケースでは、コントラクトを VRF に 2 回割り当てます。1 回は `consumer` として、もう 1 回は `provider` 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、vzAny EPG が別の 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 `consumer` として割り当て、vzAny EPG がサービスを提供する場合は、`provider` としてコントラクトを割り当てます。
- 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 `consumer` として割り当て、vzAny EPG がサービスを提供する場合は、`provider` としてコントラクトを割り当てます。

c) **[サイト対応ポリシー適用モード（Site-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 **[サイト認識ポリシー適用モード（Site-Aware Policy Enforcement Mode）]** 設定を有効にする必要があります。

（注） **[サイト認識ポリシー適用モード（Site-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。

[サイト認識ポリシー適用モード（Site-Aware Policy Enforcement Mode）] を有効にすると、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、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**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。

ステップ 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。

ステップ 9 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 ドメインの作成（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 ドメインの設定 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。

ステップ 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) **[+オブジェクトの作成（+Create Object）]** > **[EPG]** 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**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 の設定 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 ドメインの設定 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、構成するユース ケースによって異なります。

- 任意の VRF 内通信（vzAny-to-vzAny）。

  これは上記の使用例であり、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、コントラクトを consumer（vzAny VRF コントラクトが provider として割り当てられている場合）または provider（vzAny VRF コントラクトが consumer として割り当てられている場合）として明示的に割り当てます。

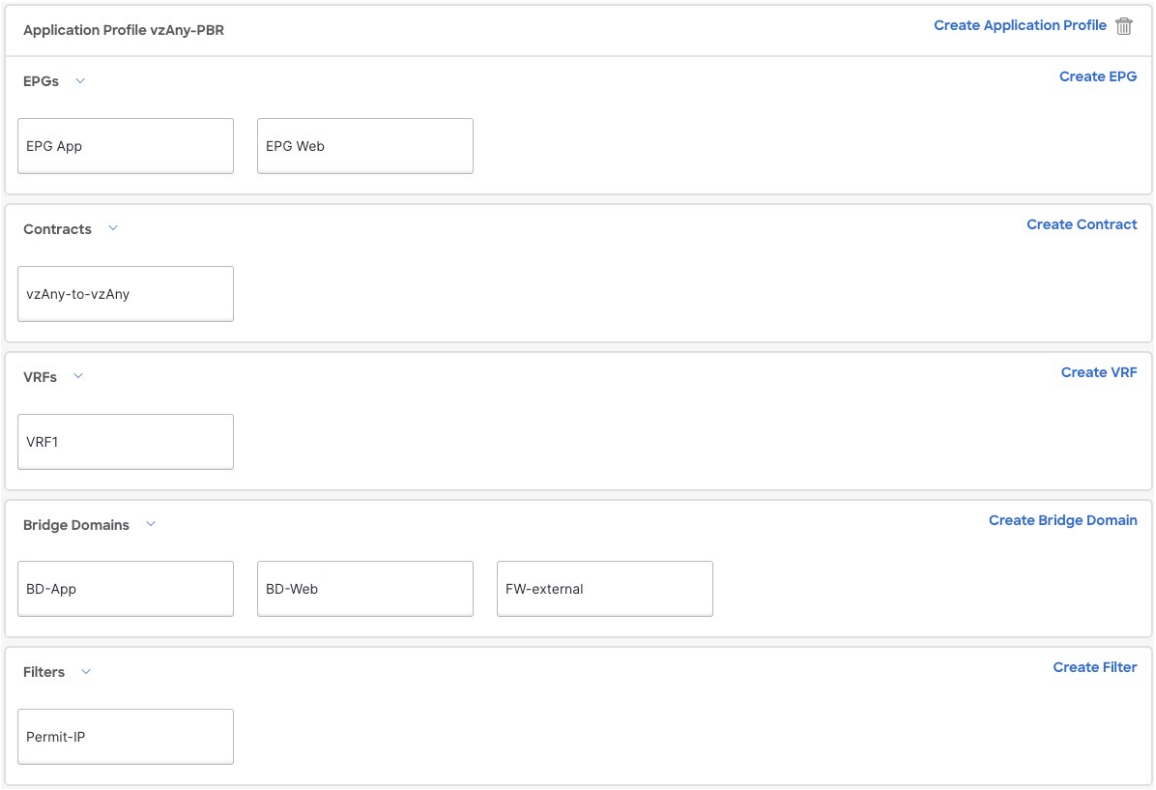
- VRF（vzAny）内のすべての EPG と、同じ VRF の一部である特定の外部 EPG 間の多数対 1 の通信。

  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 provider として外部 EPG に明示的に割り当てる必要があります。

ステップ 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。



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。

次のタスク

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 （24 ページ） 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

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。

始める前に

- サービス デバイス テンプレートの作成 （12 ページ） 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 （19 ページ） 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（まだ展開していません）。

ステップ 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。

ステップ 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。

ステップ 3 **[サービス チェーン（Service Chaining）]** 領域で、**[+ サービス チェーン（+Service Chaining）]** をクリックします。

（注） これらの手順は、サービス デバイス テンプレートの作成 （12 ページ） で説明されているように、リリース 4.2(1) 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 8 **[追加（Add）]** をクリックして続行します。

ステップ 9　**[保存（Save）]** をクリックして、テンプレートを保存します。

ステップ 10　**[テンプレートの展開（Deploy）]** をクリックして、展開します。

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