Cisco ACI マルチサイト の使用例

Cisco ACI マルチサイト サービスの統合

リリース 2.0(1) 以降、 Cisco ACI マルチサイトは、以前からサポートされていたファイアウォールを伴う単一ノードグラフに加えて、ロードバランサを伴うサービスグラフと、ロードバランサとファイアウォールを伴う 2 ノードサービスグラフをサポートします。

以前のリリースでは、イーストウェストトラフィック向けのコンシューマサイトで PBR ポリシーを適用することにより、シングルノードサービス グラフがサポートされていました。イーストウェストシナリオで 2 ノードグラフをサポートするために、PBR ポリシーが、プロバイダーのサイトでも適用されるようになりました。これは、リターンデータパスのサイト間でトラフィックがバウンスするのを防ぎますが、そのためにはコンシューマ EPG でサブネットを構成する必要があります。ノースサウスシナリオでは、PBR ポリシーは、以前のリリースと同様に、非境界リーフに適用されます。

この章で説明する使用例をサポートするには、サービスノードに次のトポロジが必要です。

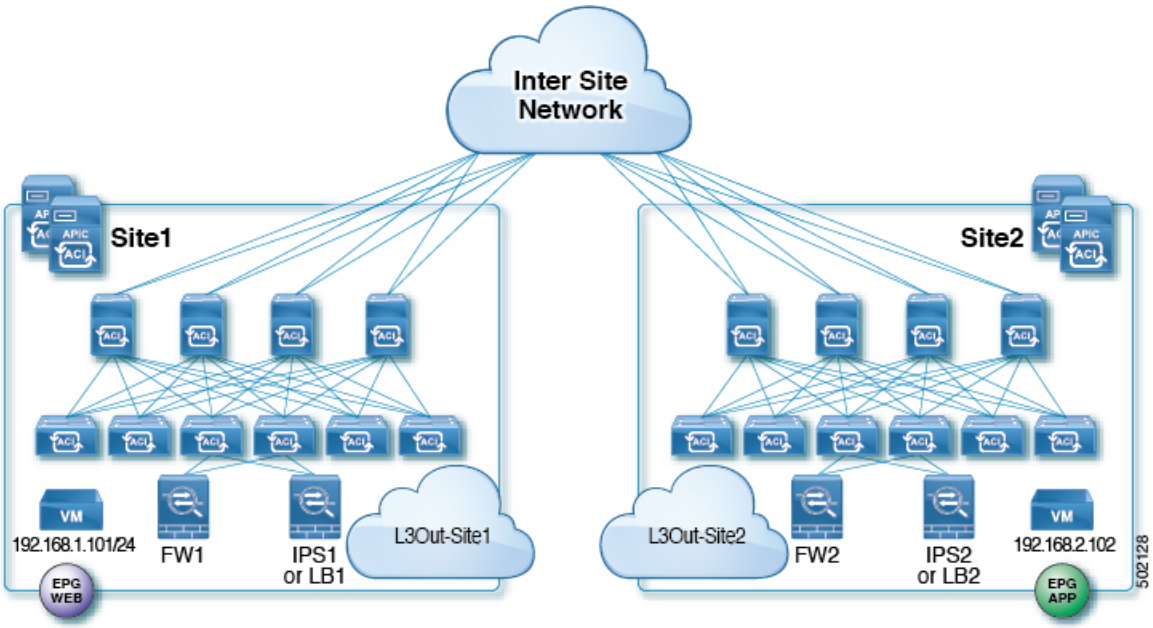
- 各サイトには、個別の現用系/スタンバイサービスノードペアがある
- レイヤ 4 ～ レイヤ 7 デバイスは管理対象外モード
- VRF はサイト全体にストレッチされる
- コンシューマ EPG とプロバイダーEPG にはクロスサイトコントラクトがある

上記のトポロジ要件に加えて、次の考慮事項に留意してください。

- ノードの外部コネクタと内部コネクタを同じ論理的なインターフェイスにすることができる
- イーストウェストトラフィックの場合は、コンシューマ EPG でサブネットを構成する必要がある
- イーストウェスト VRF 間トラフィックの場合は、コンシューマ EPG とプロバイダー EPG の両方でサブネットを構成する必要がある
- ノースサウストラフィックの場合、ポリシーは非境界リーフに適用される
- 共有サービスのシナリオは、イーストウェストトラフィックではサポートされるが、ノースサウストラフィックではサポートされない

この章の使用例全体で使用されるトポロジの例を次に示します。

図 *1 : Cisco ACI* マルチサイト サービス統合トポロジ



Single-Node Service Graphs

イーストウェスト FW サービスグラフ

これは、同じVRFまたはサイトをまたがる異なるVRF内のエンドポイント間のファイアウォール（FW）との、イーストウェスト通信のユースケースです。

サービスグラフには、次の 2 つのローカル PBR ポリシーが必要です。

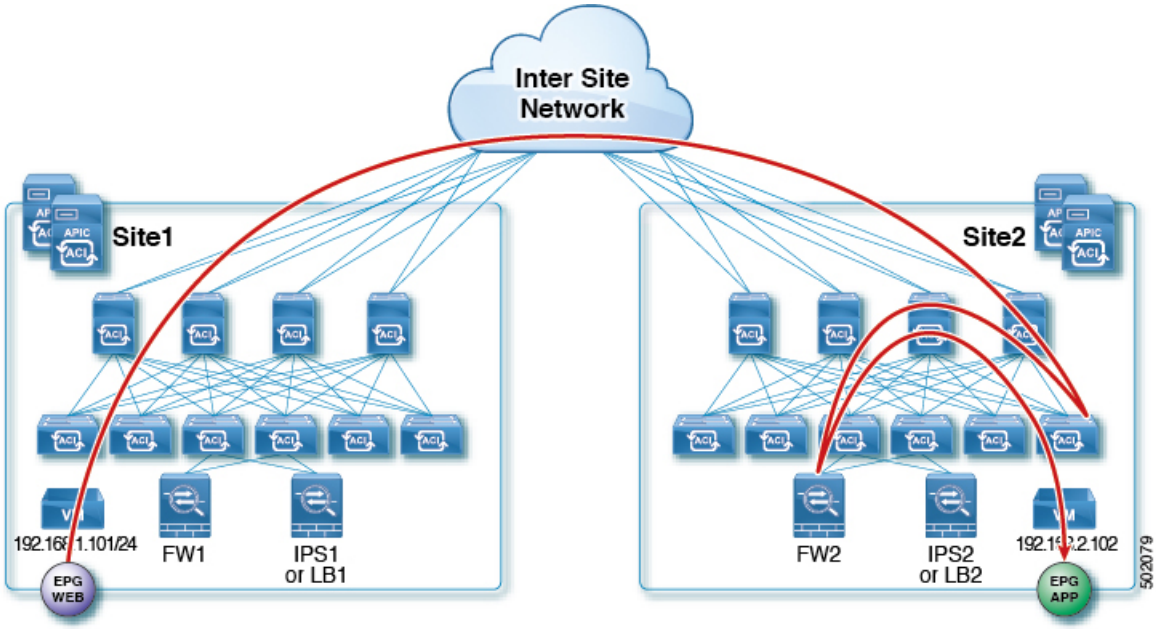
- コンシューマからプロバイダーへのトラフィックをFWの外部インターフェイスにリダイレクトするための FW の外部コネクタの PBRポリシー

- プロバイダーからコンシューマへのトラフィックを FW の内部インターフェイスにリダイレクトするための、FW の内部コネクタの PBRポリシー

次の図は、Site1 のコンシューマから Site2 のプロバイダーへの着信トラフィックパケットフローを示しています。

- コンシューマリーフはどんなルールも適用せず、トラフィックをプロバイダーに転送する
- プロバイダーリーフがポリシーを適用し、トラフィックを FW2 に送信する
- 最後に、トラフィックはプロバイダー EPG に送信される

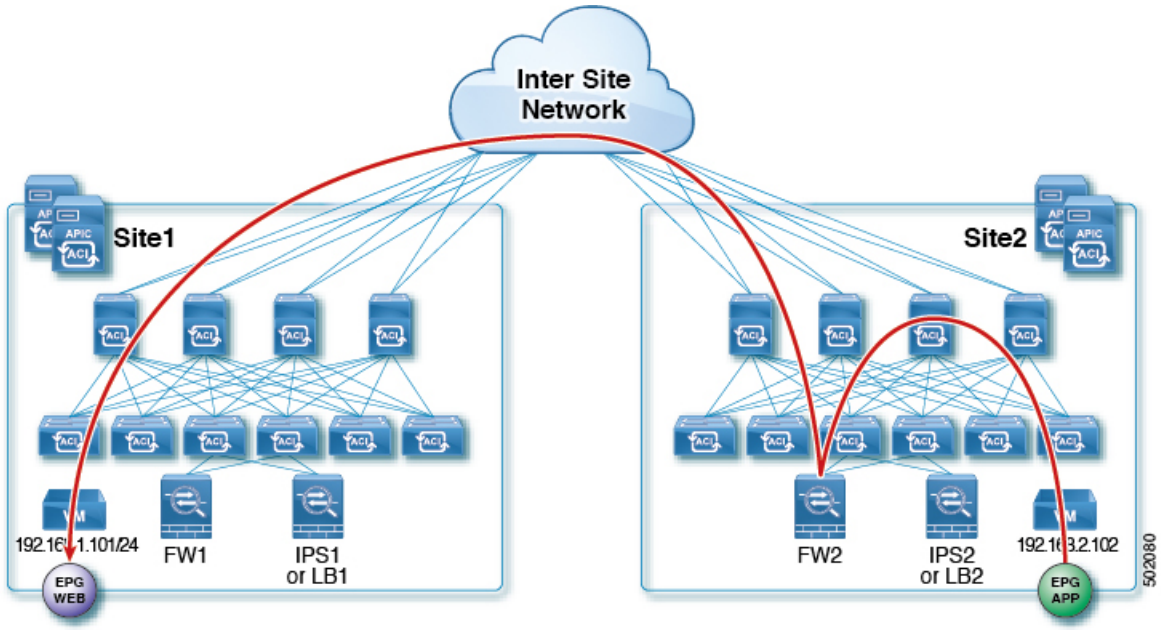
図 *2:* イーストウェスト *FW* 着信トラフィック



次の図は、Site2 のプロバイダーから Site1 のコンシューマへの戻りトラフィック パケット フローを示しています。

- プロバイダーリーフがポリシーを適用してトラフィックを FW2 にリダイレクトする
- それから、トラフィックは Site1 のコンシューマに送信される
- コンシューマリーフはどんなルールも適用せず、トラフィックをコンシューマ EPG に転送する

図 *3:* イーストウェスト *FW* リバーストラフィック



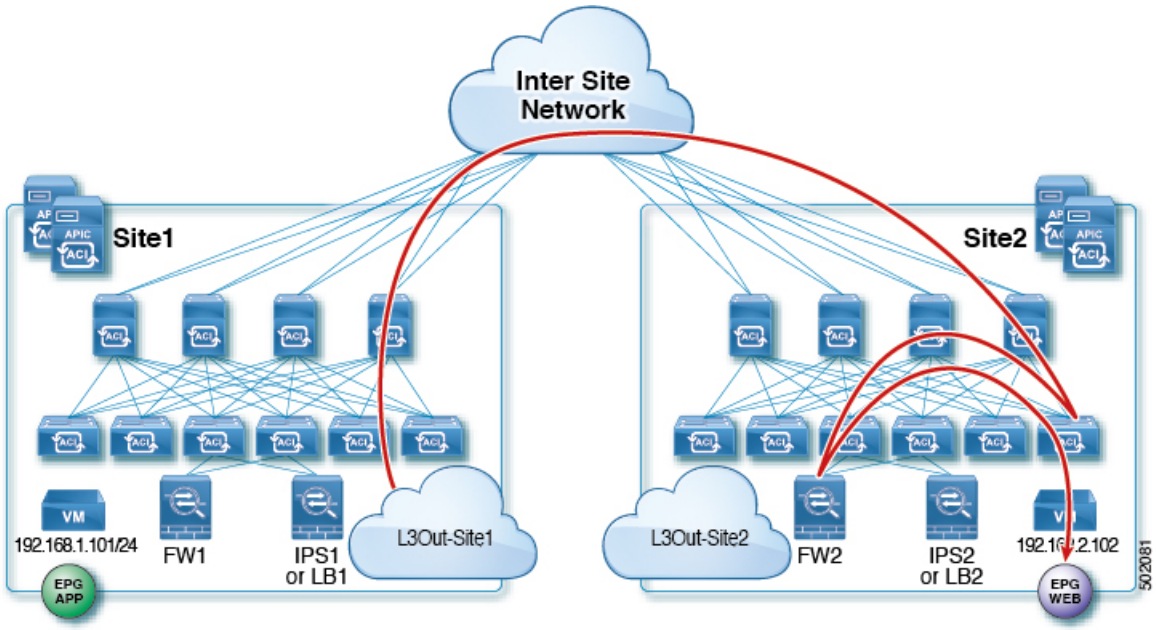
ノースサウス FW サービス グラフ

これは、サイト間の同じ VRF 内における、エンドポイント間ファイアウォール（FW）とのノースサウス通信の使用例です。

次の図は、Site1 のコンシューマから Site2 のプロバイダーへの着信トラフィック パケット フローを示しています。

- コンシューマボーダーリーフはどんなルールも適用せず、トラフィックをプロバイダーに転送する
- プロバイダーサイトの非境界リーフがポリシーを適用し、FW2 の外部インターフェイスにトラフィックを送信する
- 最後に、トラフィックは EPG に送信される

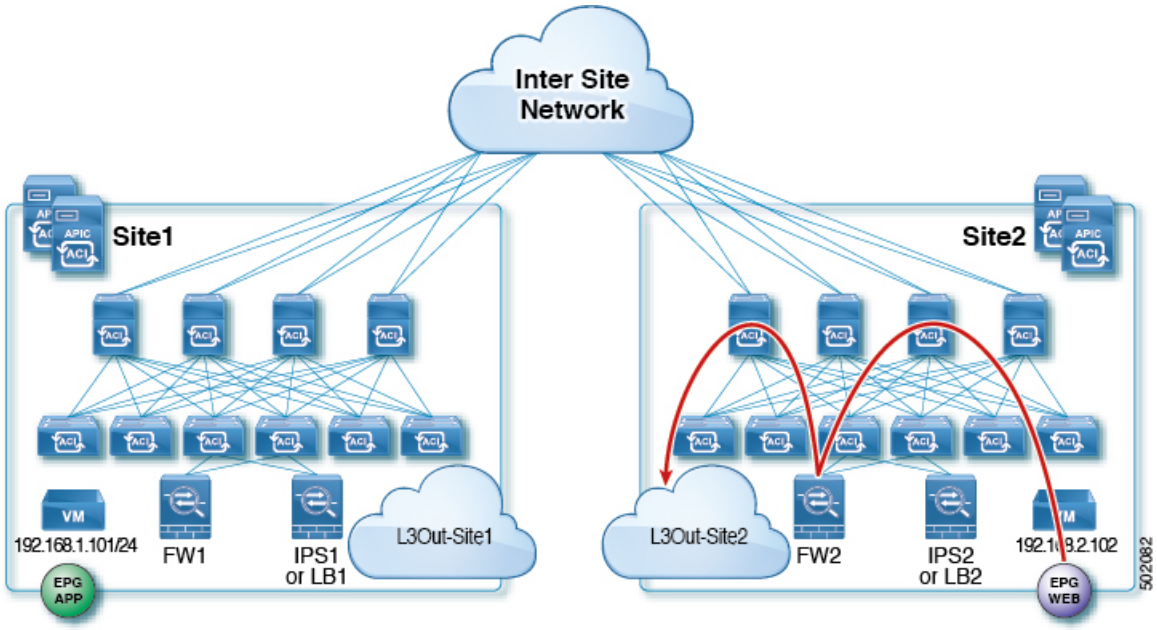
図 *4 : ノースサウス FW* 着信トラフィック



次の図は、Site2 のプロバイダーから Site1 のコンシューマへの戻りトラフィックパケットフローを示しています。

- プロバイダーサイトの非境界リーフは、ポリシーを適用し、FW2 の内部コネクタにトラフィックをリダイレクトする
- トラフィックは、Site2 の L3Out に送信される

図 *5:* ノースサウス *FW* リバーストラフィック



イーストウェスト LB サービス グラフ

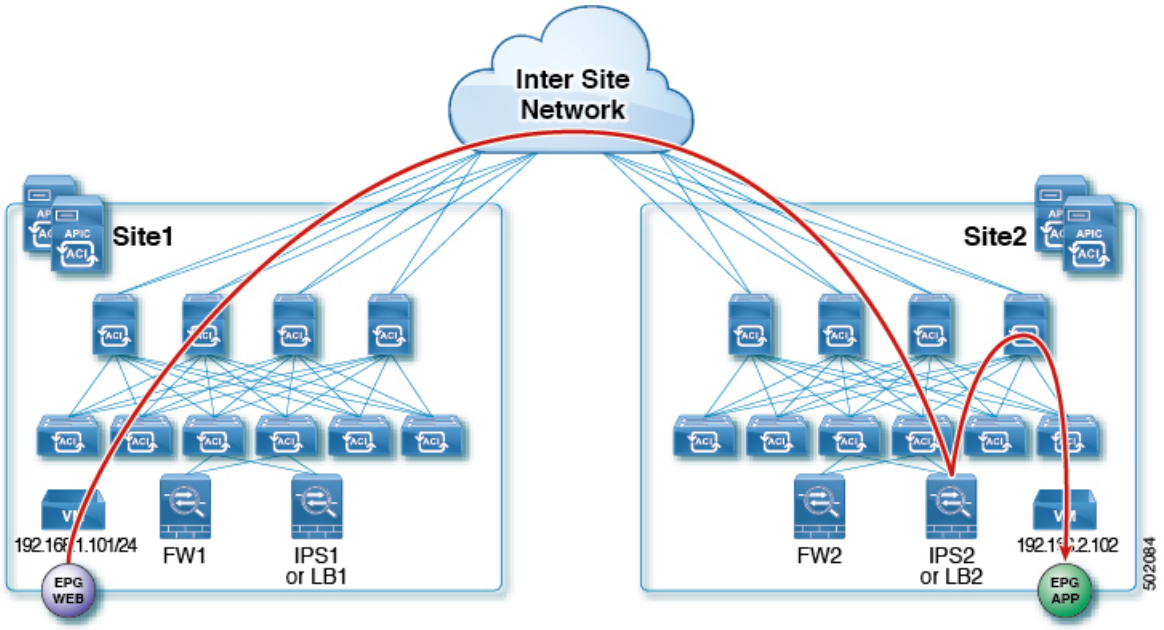
これは、サイト間の同じVRFまたは異なるVRF内のエンドポイント間のロードバランサ（LB）を使用したEast-West通信のユースケースです。LBを使用したサービスグラフは、ファイアウォール（FW）を使用したサービスグラフとは異なります。この場合、トラフィックはLBのVIP宛てに送信されるためです。このユースケースでは、LBがローカルプロバイダーEPGの存在する1つのサイトにあり、コンシューマが別のサイトにあるシナリオについて説明します。

次の図は、Site1のコンシューマからSite2のプロバイダー（EPGアプリケーション）への着信トラフィックパケットフローを示しています。

- コンシューマリーフはどんなルールも適用せず、トラフィックをプロバイダーに転送する
- トラフィックはLB2のVIPに転送される
- 最後に、トラフィックはプロバイダーEPGに送信される

（注） このセクションの例では、ロードバランサでSNATを使用しません。PBRはLBへのリターントラフィック用です。LBがSNAT処理を行う場合、PBRは必要ありません。また、SNATとPBRがない場合、LBのVIPとその実際のサーバーは同じサイトにある必要があることに注意してください。

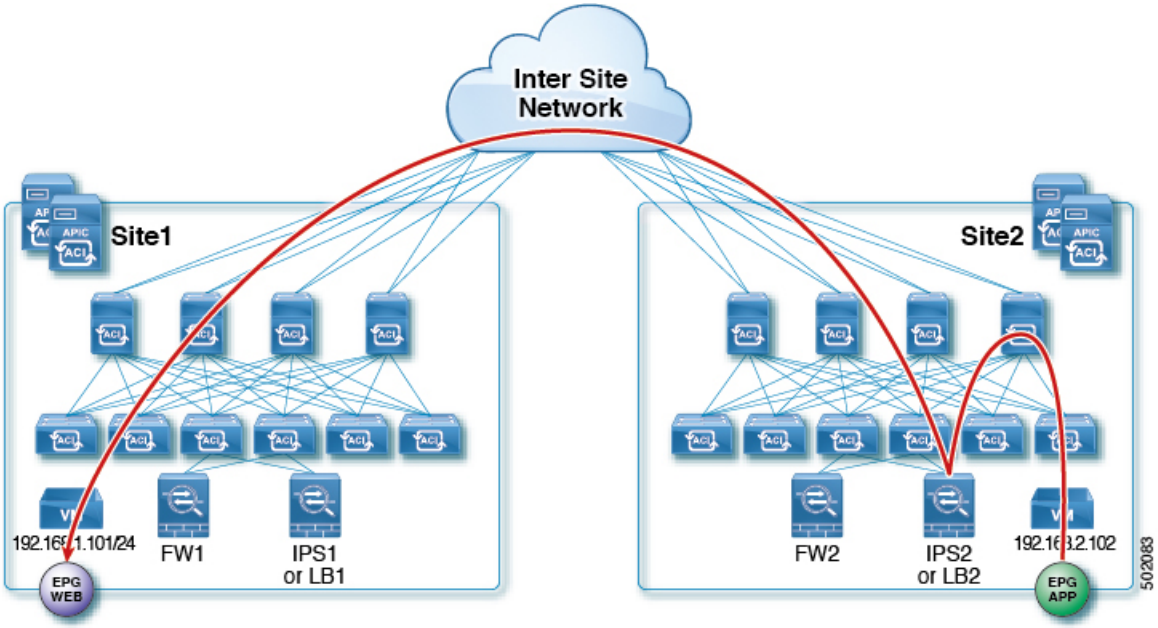
図 *6:* イーストウェスト *LB* 着信トラフィック



次の図は、Site2 のプロバイダーから Site1 のコンシューマへの戻りトラフィック パケット フローを示しています。

- プロバイダーリーフがポリシーを適用してトラフィックを LB2 にリダイレクトする
- それから、トラフィックは Site1 のコンシューマに送信される
- コンシューマリーフはどんなルールも適用せず、トラフィックをコンシューマ EPG に転送する

図 *7:* イーストウェスト *LB* リバーストラフィック



ノースサウス LB サービス グラフ

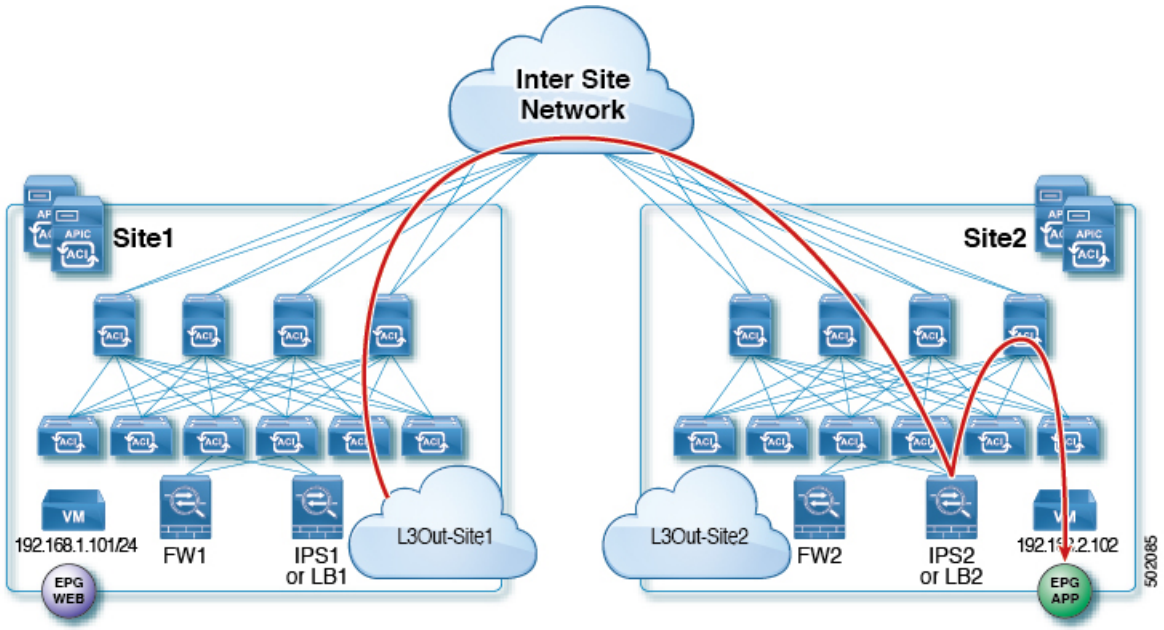
これは、データセンター内と外部のエンドポイント間のロードバランサ（LB）で使用される、ノースサウス通信のユースケースです。次の図は、L3Outトラフィックが、トラフィックが転送される LB をホストしていないサイトから入るシナリオでのパケットフローを示しています（VIP は別のサイトにあります）。この例では、コンシューマとして L3Out があり、プロバイダーとして通常の EPG があります。この場合、ポリシーは常にプロバイダーサイトの非境界リーフで適用されます。

次の図は、Site1 のコンシューマから Site2 のプロバイダーへの着信トラフィック パケット フローを示しています。

- コンシューマボーダーリーフはどんなルールも適用せず、トラフィックを Site2 の VIP に転送する
- プロバイダーサイトの非境界リーフがポリシーを適用し、トラフィックが LB に転送される
- 最後に、トラフィックは LB からプロバイダーEPG に送信される

（注） このセクションの例では、ロードバランサで SNAT を使用しません。PBR は LB へのリターントラフィック用です。LB が SNAT 処理を行う場合、PBR は必要ありません。また、SNAT と PBR がない場合、LB の VIP とその実際のサーバーは同じサイトにある必要があることに注意してください。

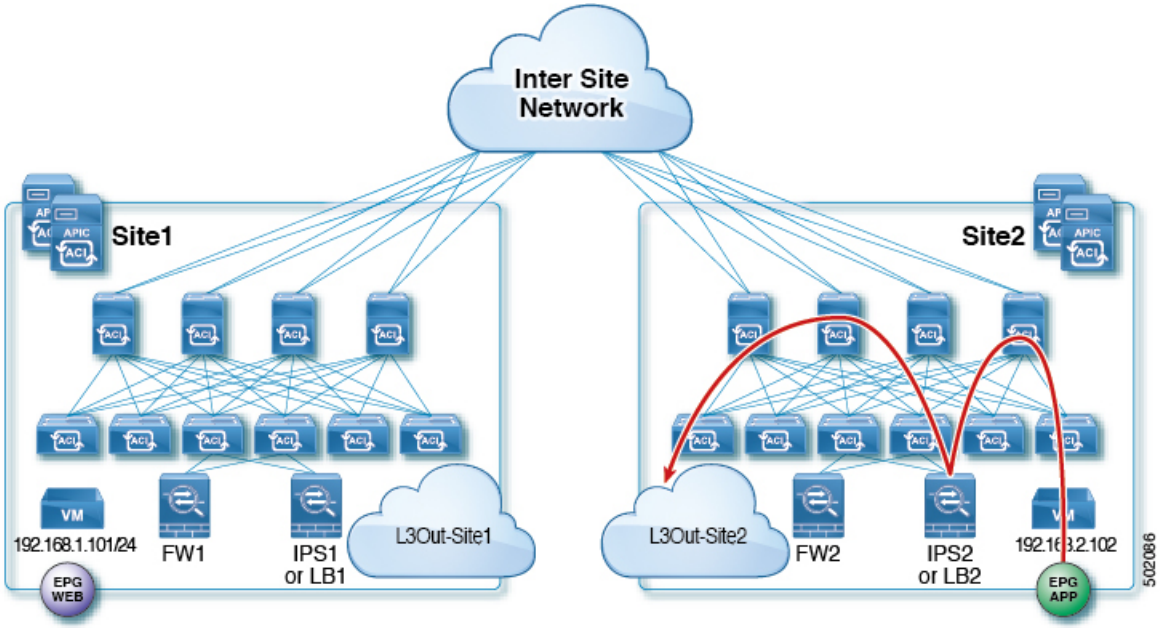
図 *8 :* ノースサウス *LB* 着信トラフィック



次の図は、Site2 のプロバイダーから Site1 のコンシューマへの戻りトラフィック パケット フローを示しています。

- プロバイダーサイトの非境界リーフがポリシーを適用してトラフィックを LB にリダイレクトする
- トラフィックは、Site2 の L3Out に送信される

図 *9:* ノースサウス *LB* リバーストラフィック



Two-Node Service Graphs

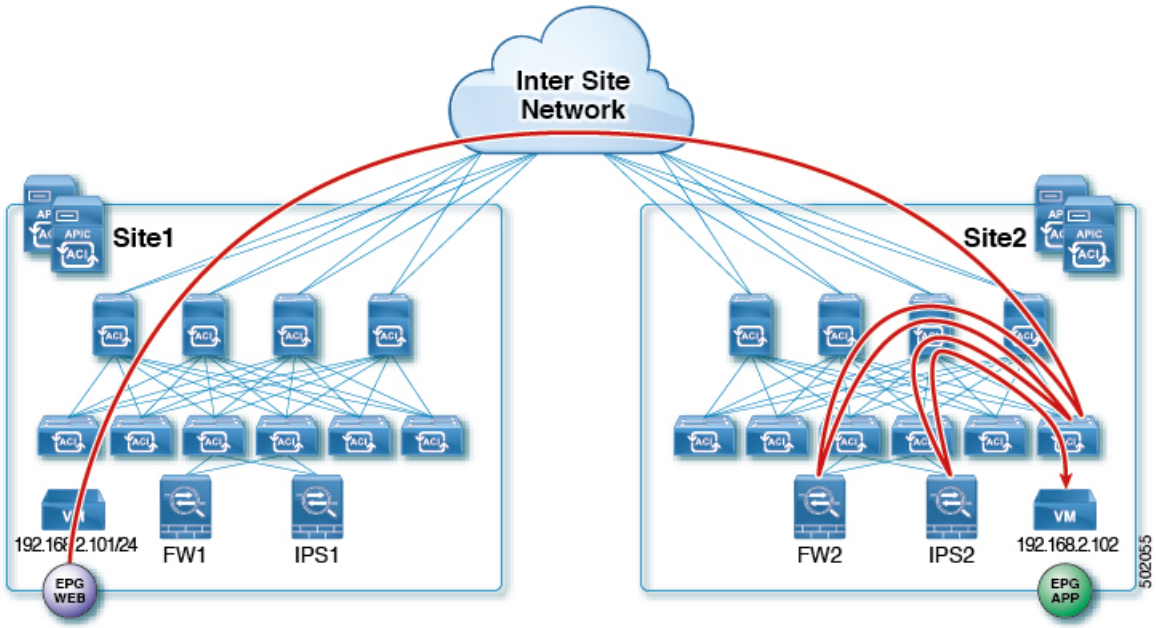
East-West FW および IPS サービスグラフ

これは、サイト間の同じ VRF または異なる VRF 内のエンドポイント間でファイアウォール（FW）およびIPSを使用した East-West通信のユースケースです。

次の図は、Site1 のコンシューマから Site2 のプロバイダーへの着信トラフィックパケットフローを示しています。

- コンシューマ リーフはどんなルールも適用せず、トラフィックをプロバイダーに転送する
- プロバイダーリーフがポリシーを適用し、トラフィックを FW2 の外部インターフェイスに送信する
- その後、トラフィックはプロバイダーリーフにリダイレクトされて戻り、さらに IPS2 の外部インターフェイスに送られる
- 最後に、トラフィックはプロバイダー EPG に送信される

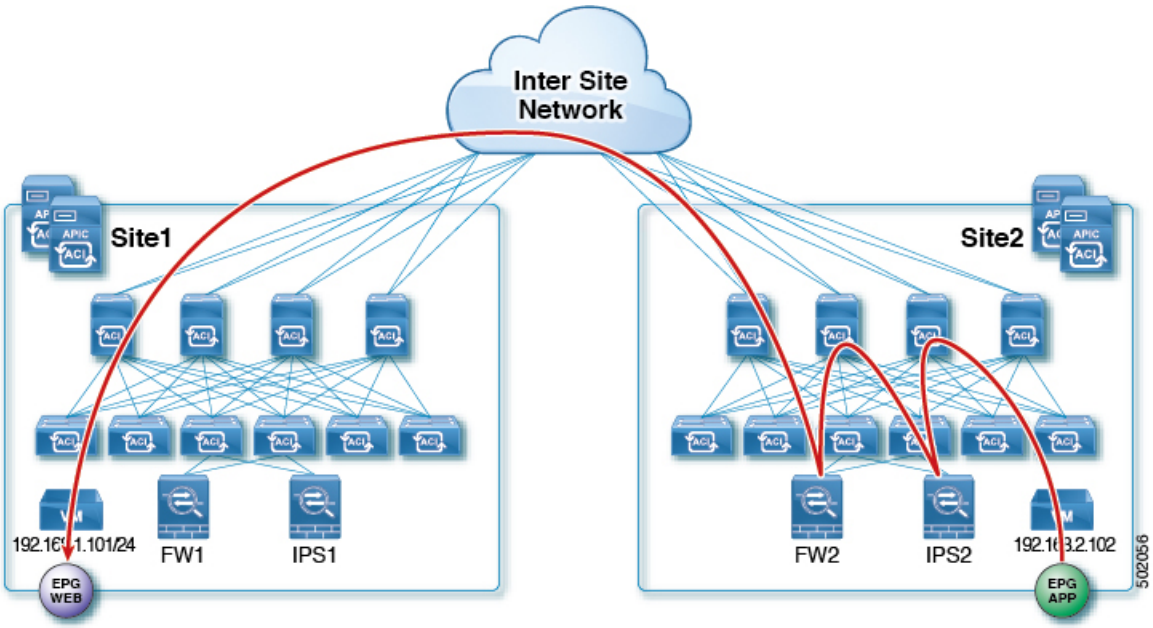
図 *10* : イーストウェスト *FW/IPS* 着信トラフィック



次の図は、Site2 のプロバイダーから Site1 のコンシューマへの戻りトラフィック パケット フローを示しています。

- プロバイダーリーフがポリシーを適用してトラフィックを IPS2 の内部コネクタにリダイレクトする
- それから、トラフィックは FW2 の内部コネクタにリダイレクトされる
- それから、トラフィックは Site1 のコンシューマに送信される
- コンシューマリーフはどんなルールも適用せず、トラフィックをコンシューマ EPG に転送する

図 *11* : イーストウェスト *FW/IPS* リバーストラフィック



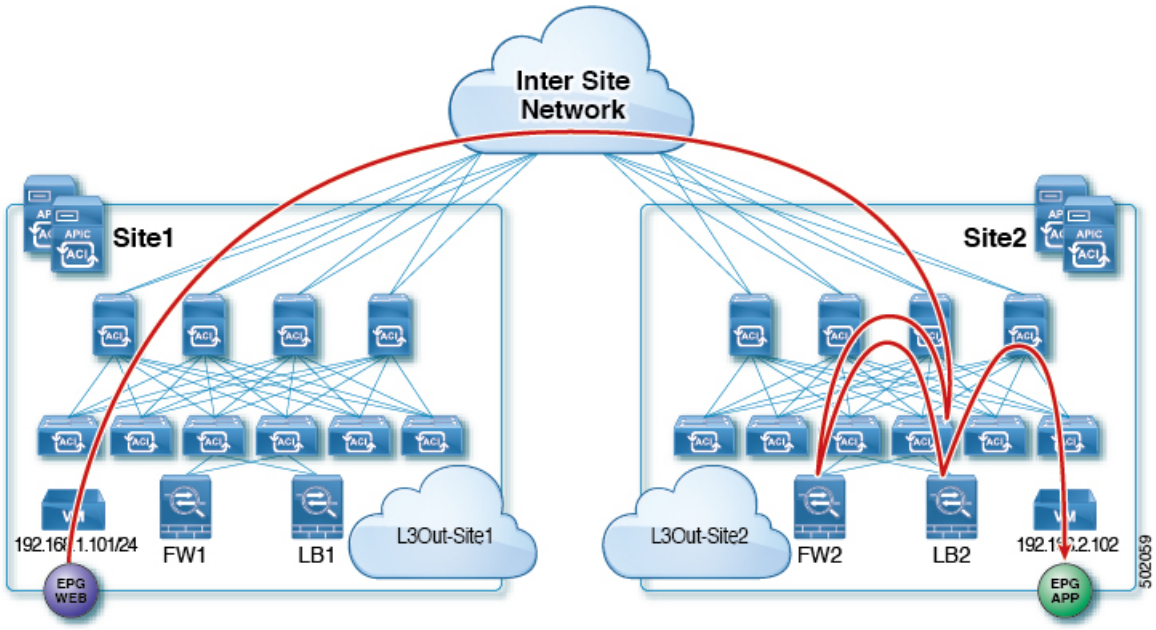
イーストウェスト FW および LB サービスグラフ

これは、サイト間の同じ VRF または異なる VRF 内のエンドポイント間のファイアウォール（FW）およびロードバランサ（LB）とのイーストウェスト通信のユースケースです。これは、高可用性と拡張性のためにサーバでのロードバランシングを必要とするアプリケーション内のトラフィックの一般的な設計です。

次の図は、Site1 のコンシューマから Site2 のプロバイダーへの着信トラフィックパケットフローを示しています。

- コンシューマ リーフはどんなルールも適用せず、トラフィックをプロバイダーに転送する
- LB2 の VIP が接続されているプロバイダーリーフがポリシーを適用し、トラフィックを FW2 の外部インターフェイスに送信する
- それからトラフィックは LB2 にリダイレクトされる
- 最後に、トラフィックはプロバイダー EPG に送信される

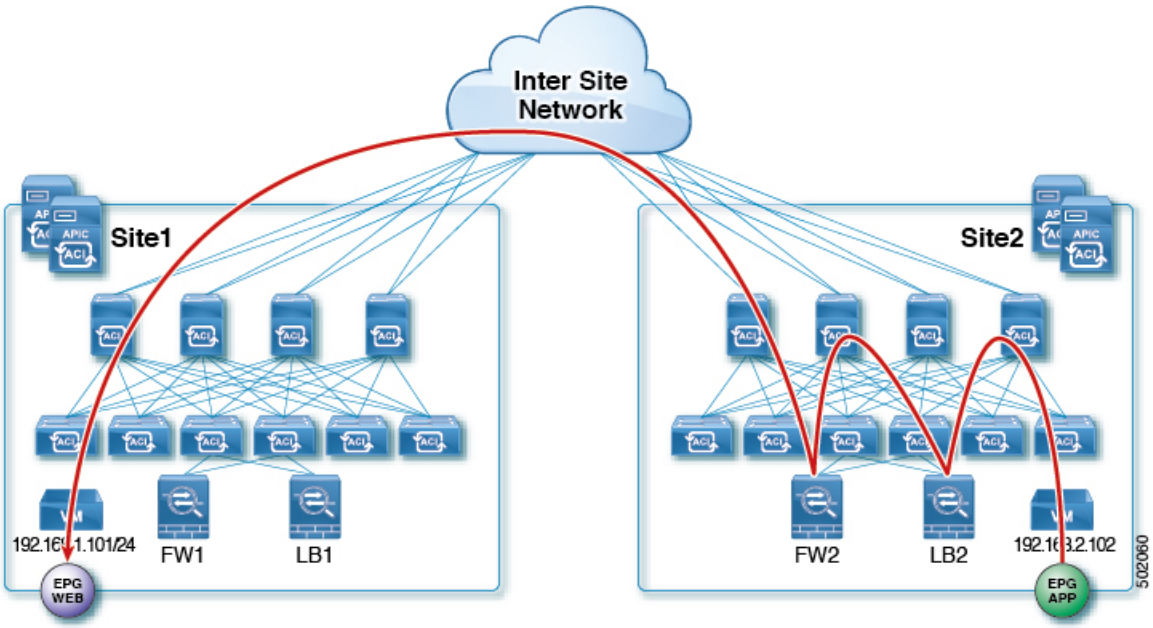
図 *12* : イーストウェスト *FW/LB* 着信トラフィック



次の図は、Site2 のプロバイダーから Site1 のコンシューマへの戻りトラフィック パケット フローを示しています。

- プロバイダーリーフがポリシーを適用してトラフィックを LB2 にリダイレクトする
- それから、トラフィックは FW2 の内部コネクタにリダイレクトされる
- それから、トラフィックは Site1 のコンシューマに送信される
- コンシューマリーフはどんなルールも適用せず、トラフィックをコンシューマ EPG に転送する

図 *13 :* イーストウェスト *FW/LB* リバーストラフィック



共有 L3Out を使用する 外部 EPG

リリース 2.0(1) 以降、Cisco ACI マルチサイトは、異なる VRF 内のコンシューマ EPG とプロバイダー EPG による共有サービスと、プロバイダーまたはコンシューマとしての L3Out 外部 EPG による共有サービスをサポートしています。以前のバージョンのマルチサイトは、L3Out とコンシューマ EPG が同じ VRF 内に存在する場合にのみ、このユースケースをサポートしていました。

これの最も一般的なユースケースは、インターネット サービスを提供する共通テナントに展開された外部 EPG であり、他のテナント（またはコンシューマ EPG）はそれを使用してインターネットにアクセスします。ただし、この機能により、さらに次のユースケースも可能になります。

（注） 次の例の外部 EPG はプロバイダーとして示されていますが、外部 EPG が代わりにコンシューマである場合にも同じことが当てはまります。

図 *14* : ユーザーテナント下の *EPG*、*VRF*、ブリッジドメイン、および外部 *EPG*

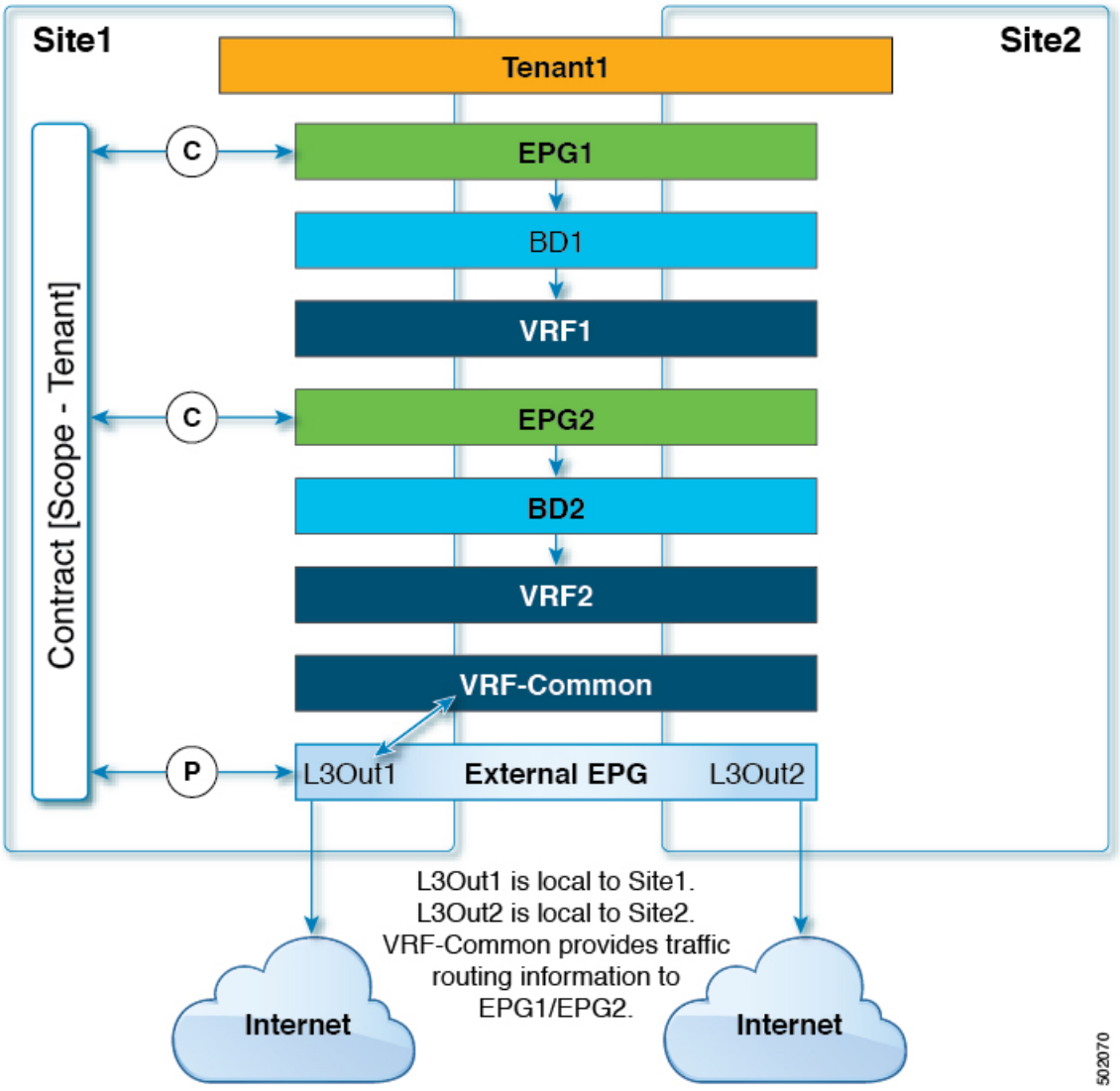


図 *15 :* ユーザーテナント下の *EPG*、*VRF*、およびブリッジドメイン。共通テナントの外部 *EPG*

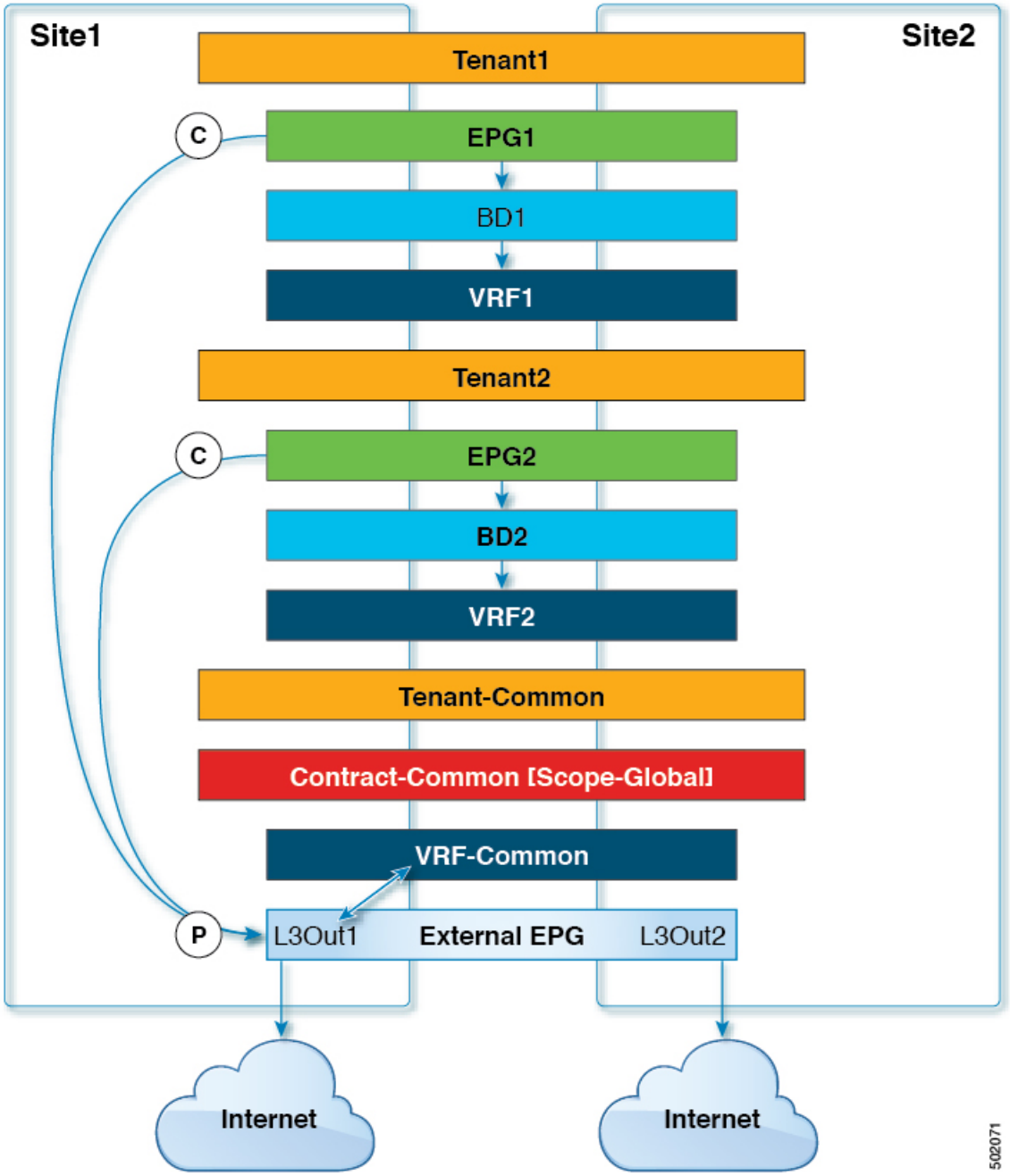
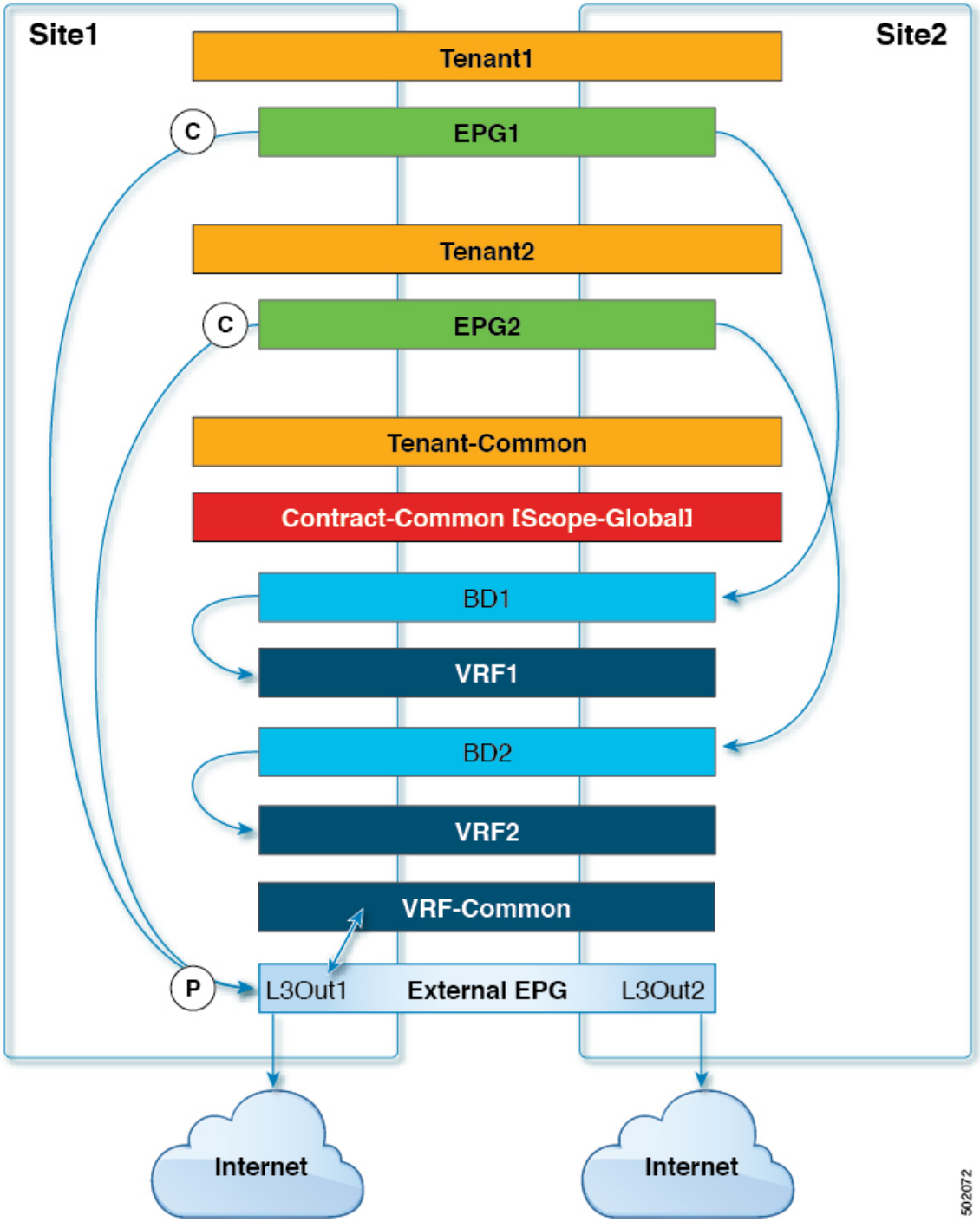


図 *16* : ユーザーテナント下の *EPG*、ただし共通テナント下の *VRF*、*BD*、および外部 *EPG*を除く



共有 L3Out 向けの外部 EPG の構成

次の手順では、テンプレートレベルで外部EPGのルート制御プロパティとルート制御プロファイル名を構成する方法について説明します。

手順

ステップ 1 マルチサイト GUI にログインします。

ステップ 2 左側のサイドバーから、**[スキーマ (schema)]** ビューを選択します。

ステップ 3 スキーマを選択します。

ステップ 4 構成する外部 EPG を選択します。

ステップ 5 右側のペインで、**[+SUBNET]** をクリックしてサブネットを追加します。

次のフィールドを入力します。

- **[分類サブネット（Classification Subnet ）]**：このサブネットとマッチする L3Out からのルートと、定義されたプレフィックス内の外部トラフィックは、この外部 EPG の一部として分類されます。
- **[共有ルート制御サブネット（Shared Route Control Subnet）]**：定義されたルートが、共有されている VRF にリークされるかどうかを決定します。
- **[共有セキュリティインポートサブネット（Shared Security Import Subnet）]**：ルーティングおよびポリシープレーンのより詳細な制御を行えます。この設定の特定の例の詳細については、共有セキュリティインポートサブネットの例 （18 ページ）を参照してください。
- **[集約共有ルート（Aggregate Shared Routes）]**：定義されたルートに入るすべてのプレフィックスが、共有されている VRF にリークされるかどうかを決定します。集約共有ルートは、**[共有ルート制御サブネット（Shared Route Control Subnet）]** が有効になっている場合にのみ有効にできます

ルートは他のプライベート ネットワークにリークされる可能性がありますが、他のネットワークのルートに対する ACL はインストールされません。このようなシナリオは、共有ルートがより大きなサブネットにあり、セキュリティが別の小さなサブネットに適用されている場合に発生します。

共有セキュリティインポートサブネットの例

このセクションでは、**共有セキュリティインポートサブネット** 設定を使用して、ルーティングおよびポリシープレーンのより詳細な制御を設定する例を示します。

次の 3 つの使用例では、L3Out が `10.0.1.0/24`、`10.0.2.0`/24 、および `10.0.3.0/24` の 3 つのルートを受信したことを前提としています。

使用例 1

2 つの外部 EPG が次の設定で構成されています。

- 10.0.1.0/24 サブネット、**共有ルート制御サブネット**と**共有セキュリティインポートサブネット**の設定が有効になっている外部 EPG1、および TCP トラフィックのみを許可するコントラクト
- 10.0.2.0/24 サブネット、**共有ルート制御サブネット** と **共有セキュリティインポートサブネット**の設定が有効になっている外部 EPG2、および UDP トラフィックのみを許可するコントラクト

この場合、 10.0.1.0/24 および 10.0.2.0/24 プレフィックスのみが他の VRF にリークされます。そして異なるコントラクトを指定して、10.0.1.0/24 サブネットには TCP ベースのトラフィックのみ、10.0.2.0/24 サブネットには UDP トラフィックのみを許可することができます。

使用例 2

3 つの外部 EPG が次の設定で構成されています。

- 10.0.0.0/16 サブネット、 **共有ルート制御サブネット** 、および**集約共有ルート**設定が有効になっている外部 EPG1
- 10.0.1.0/24 サブネットを持ち、**共有セキュリティインポートサブネット**設定のみが有効で、TCP トラフィックのみを許可するコントラクトを持つ外部 EPG2
- 10.0.2.0/24 サブネットを持ち、**共有セキュリティインポートサブネット**設定のみが有効で、UDP トラフィックのみを許可するコントラクトを持つ外部 EPG3

この場合、EPG1 で定義された集約 10.0.0.0/16 により、サブセット 10.0.1.0/24、10.0.2.0/24、および 10.0.3.0/24 が他の VRF にリークされますが、ACL は 10.0.1.0/24 および 10.0.2.0/24 に対してのみインストールされます。

10.0.1.0/24 および 10.0.2.0/24 については、異なるコントラクトを指定して、10.0.1.0/24 サブネットのTCPトラフィックのみと、10.0.2.0/24 サブネットの UDPトラフィックのみを許可することができます。10.0.3.0/24 には ACL が存在しないため、ルートが他の VRF にリークされても、ポリシーでドロップされます。

使用例 3

3 つの外部 EPG が次の設定で構成されています。

- •外部 EPG1（10.0.0.0/16 サブネット、**共有セキュリティインポートサブネット**設定が有効、すべてのトラフィックを許可するコントラクト）
- •外部 EPG2（10.0.1.0/24 サブネット、**共有ルート制御サブネット**設定が有効）
- •外部 EPG3（10.0.2.0/24 サブネット、**共有ルート制御サブネット**設定が有効）

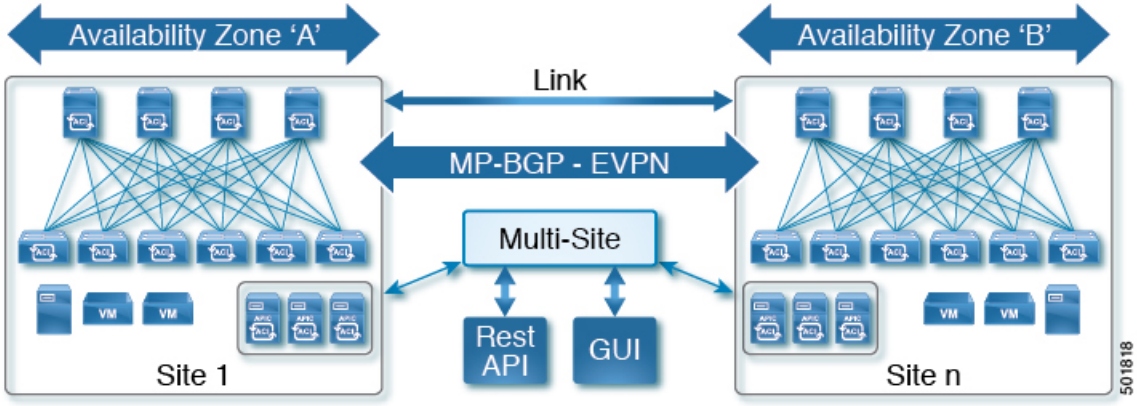
この場合、10.0.1.0/24 と 10.0.2.0/24 のみが共有ルートとしてマークされるため、他の VRF にリークされますが、10.0.3.0/24 はリークされません。サブネット 10.0.0.0/16 内の L3Out へのすべてのトラフィックを許可する単一の ACL があります。

Cisco ACI マルチサイト IPN を使用しないサイト間のバックツーバックスパイン接続

この Cisco ACI マルチサイト のユースケースは、サイト間で IPN を使用しない、異なる 2 つのサイトのスパイン間直接接続をサポートします。このユースケースにより、次のことが可能になります。

- サイト間で IPN を使用しない、異なる 2 つのサイトのスパイン間直接接続のサポート
- サイト展開ごとに単一のポッドのみをサポート
- サイト間で一意のファブリック名が必要

図 *17:* マルチサイト バックツーバックスパイン：基本セットアップ



設計

- LLDP はスパイン間の接続を検出し、そのポートでの配線の問題を作成します。
- DHCP リレーはリンク上で設定されません
- LLDP が一意のファブリック名を検出し、両側のスパインが検出されると、ポートは次の場合を除いてインサービスに戻ります。
  - ISIS はリンクで有効にならない
  - インフラ VLAN はリンクから学習されない
  - LLDP TLV はサイト間であり、無視される
- スパイン間リンクは外部サブインターフェイスとして扱われる
- 構成とデータパスは、通常の マルチサイト セットアップと同じになる

制限事項

- バックツーバック接続では、各サイトに複数のスパインを展開して、サイト間接続を提供することを推奨します。これらの各スパインから、他の各サイトの各スパインへの複数のリンクを提供します。
- バックツーバックスパインでは 2 つのサイトのみがサポートされます。
- このユースケースでは、 APIC での新しい構成は必要ありません。

トラブルシューティング

- APIC において、両方のサイトでこのインターフェイスに l3extOut が構成されているかどうかを確認します。
- 2 つのサイトスパイン間が到達可能でない場合は、次の手順を実行します。
  - 配線の問題がなく、ポートが稼働していて、スイッチングが有効になっていることを確認します。

```
dev-infra1-spine1# cat /mit/sys/lldp/inst/if-[eth1--1]/summary | grep wiringIssues
wiringIssues :
dev-infra1-spine1#
```

  - IPアドレスが l3extOut 構成から割り当てられ、OSPF セッションが起動していることを確認します。

```
IP Interface Status for VRF "overlay-1"
eth1/53.7, Interface status: protocol-up/link-up/admin-up, iod: 63, mode: external
```

- 他のサイトに接続されているスパインの `svc_ifc_policyelem.log*` ファイルを確認します。

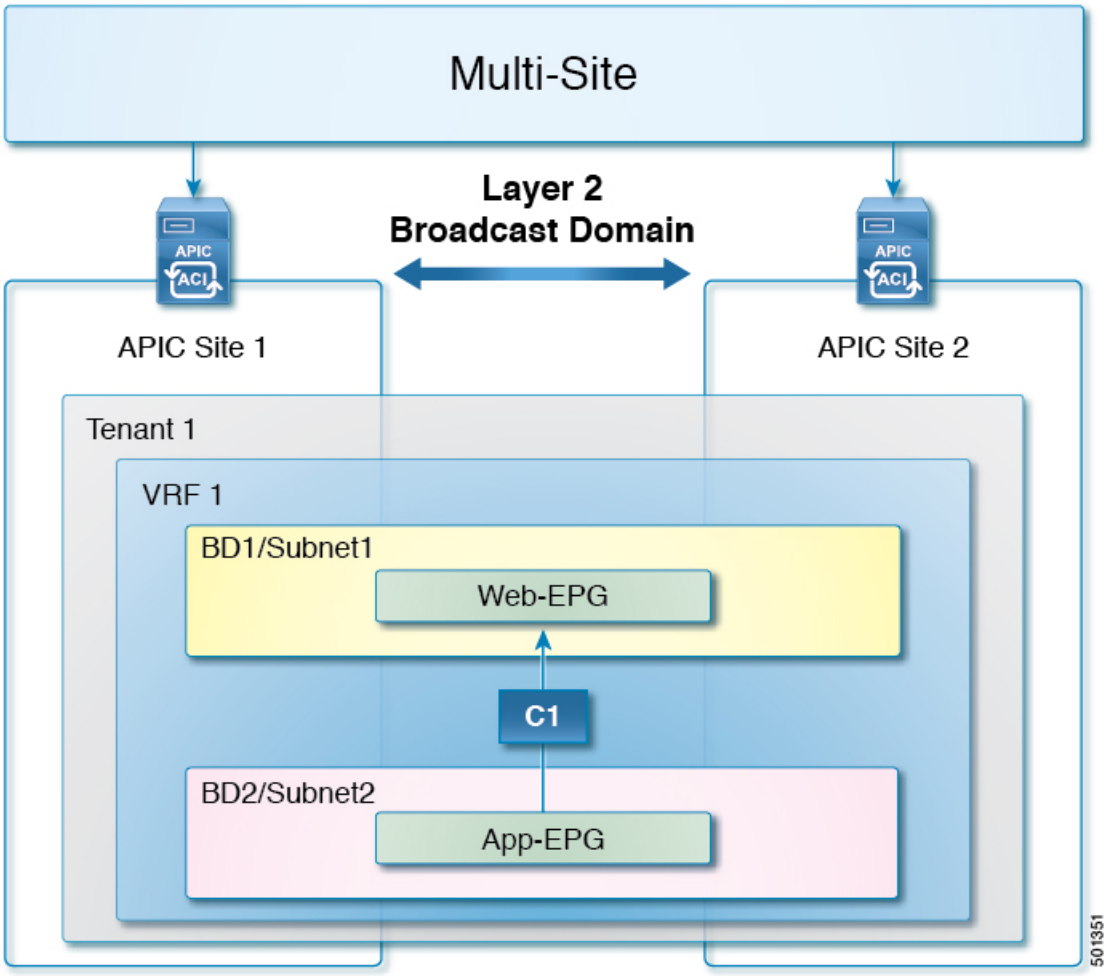
```
$ zgrep "back to back spine ignore wiring check." \
/var/sysmgr/tmp_logs/dme_logs/svc_ifc_policyelem.log*
```

レイヤ 2 ブロードキャスト拡張を使用したストレッチブリッジドメイン

これは最も基本的な Cisco ACI マルチサイト のユースケースで、サイト間でテナントと VRF が拡大されます。VRF 内の EPG（およびそのブリッジドメイン（BD）とサブネット）と、それらのプロバイダーとコンシューマのコントラクトもサイト間で拡大されます。

このユースケースでは、レイヤ2ブロードキャストフラッディングがファブリック全体で有効になっています。不明なユニキャストトラフィックは、レイヤ 2 BD がストレッチされている各リモートファブリックにフレームを複製して送信するスパインノードの、ヘッドエンドレプリケーション（HER）機能を利用して、サイト間で転送されます。

図 *18 :* レイヤ *2* ブロードキャスト拡張を使用したストレッチブリッジドメイン



このユースケースにより、次のことが可能になります。

- 共通のポリシーを使用してすべてのサイトに同じアプリケーション階層を展開すること。これにより、さまざまなファブリック間で、さまざまなEPGに属するワークロードをシームレスに展開し、共通の一貫したポリシーで通信を管理することができます。
- レイヤ 2 クラスタリング
- ライブ VM 移行
- サイト間のアクティブ/アクティブの高可用性
- サービスグラフを使用したサイト間での共有アプリケーションのプッシュはサポートされていません。

このユースケースの前提条件

- サイトが追加され、 APIC コントローラが現用系であり、通信が確立されていること。

- ストレッチされるテナントが作成されていること。
- マルチサイト のサイトおよびテナントマネージャーのアカウントが使用可能であること

次の表のオブジェクトを含む単一のプロファイル。複数のサイトにプッシュされます。

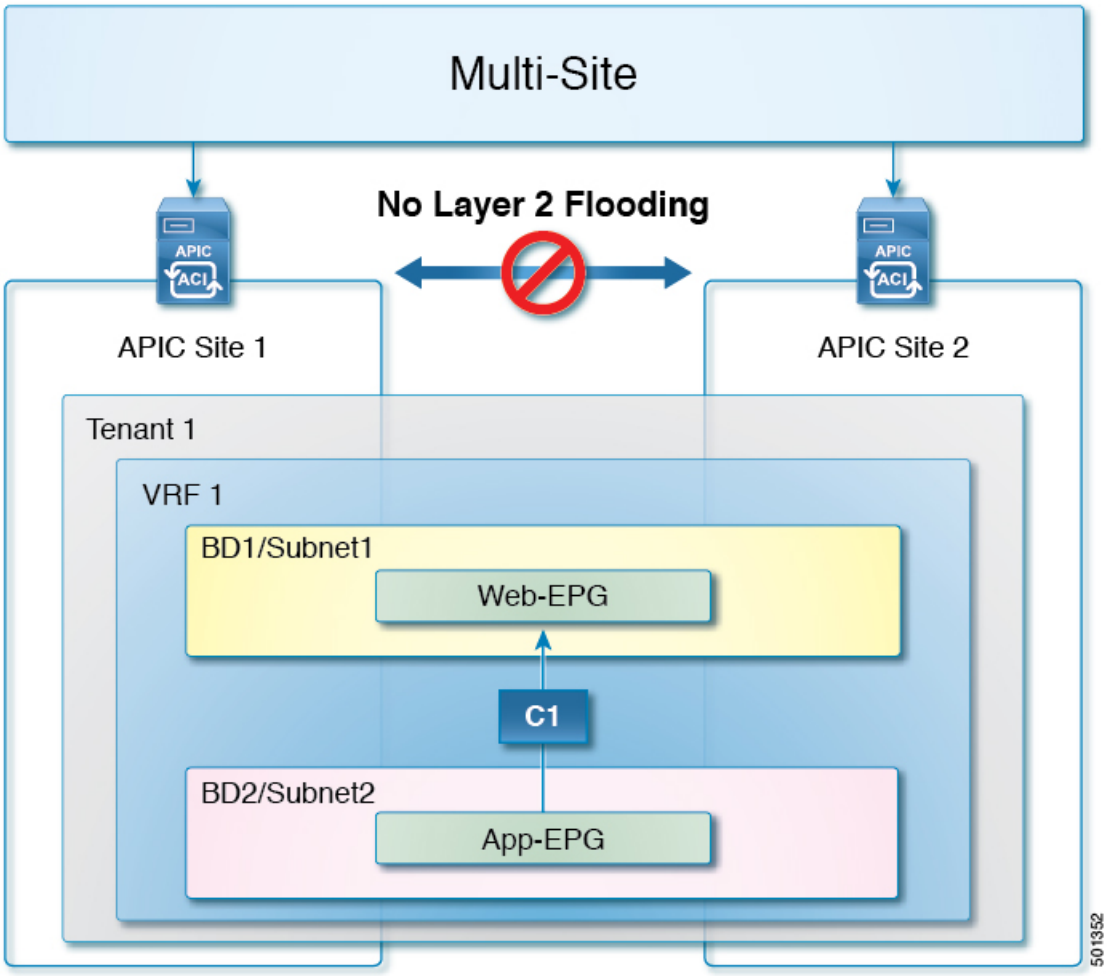
表 *1:* このユースケースで構成する機能

設定	説明	ストレッチまたはローカル
テナント	APIC からインポートされたか、 マルチサイトで作成された	ストレッチ
サイトのL3 Out(Site L3Outs)	APIC GUI で構成され、ストレッチされたテナントと VRF、サイト固有のテンプレートにリンクされている	ローカル
VRF	テナントの VRF	ストレッチ
ブリッジ ドメイン	レイヤ 2 ストレッチが有効 レイヤ 2 フラッディングが有効 共有するサブネットが追加されている	ストレッチ
EPG	BD 内の EPG	ストレッチ
コントラクト	EPG 通信を管理するために必要なフィルタを含める	ストレッチ
外部 EPG	サイト L3Out のネットワークマッピング（Cisco ACI マルチサイト、リリース 1.0(1)） 外部 EPG を介したサイト L3Out のサイト接続（マルチサイト、リリース 1.0(2)）	ローカル、ただし他のサイトにリンクされる

レイヤ 2 ブロードキャスト拡張を使用しないストレッチブリッジドメイン

この Cisco ACI マルチサイト のユースケースは、テナント、VRF、およびそれらの EPG（ブリッジドメインとサブネット）がサイト間で拡張される最初のユースケースに似ています。

図 *19 :* レイヤ *2* ブロードキャスト拡張を使用しないストレッチブリッジドメイン



ただし、このユースケースでは、レイヤ2ブロードキャストフラッディングは各サイトでローカライズされます。レイヤ2ブロードキャスト、マルチキャスト、および不明なユニキャストトラフィックは、複製された VXLAN トンネルを介してサイト間で転送されません。

このユースケースにより、次のことが可能になります。

- レイヤ2フラッディングをローカルに保つことで、コントロールプレーンのオーバーヘッドを削減
- ディザスタリカバリのためのサイト間 IP モビリティ
- VM の「コールド」移行
- サービスグラフを使用したサイト間での共有アプリケーションのプッシュはサポートされていません。

このユースケースの前提条件

- サイトが追加され、 APIC コントローラが現用系であり、通信が確立されていること。

- ストレッチされるテナントが作成されていること。
- マルチサイト のサイトおよびテナントマネージャーのアカウントが使用可能であること

次の表のオブジェクトを使用するプロファイルを、複数のサイトにプッシュします。

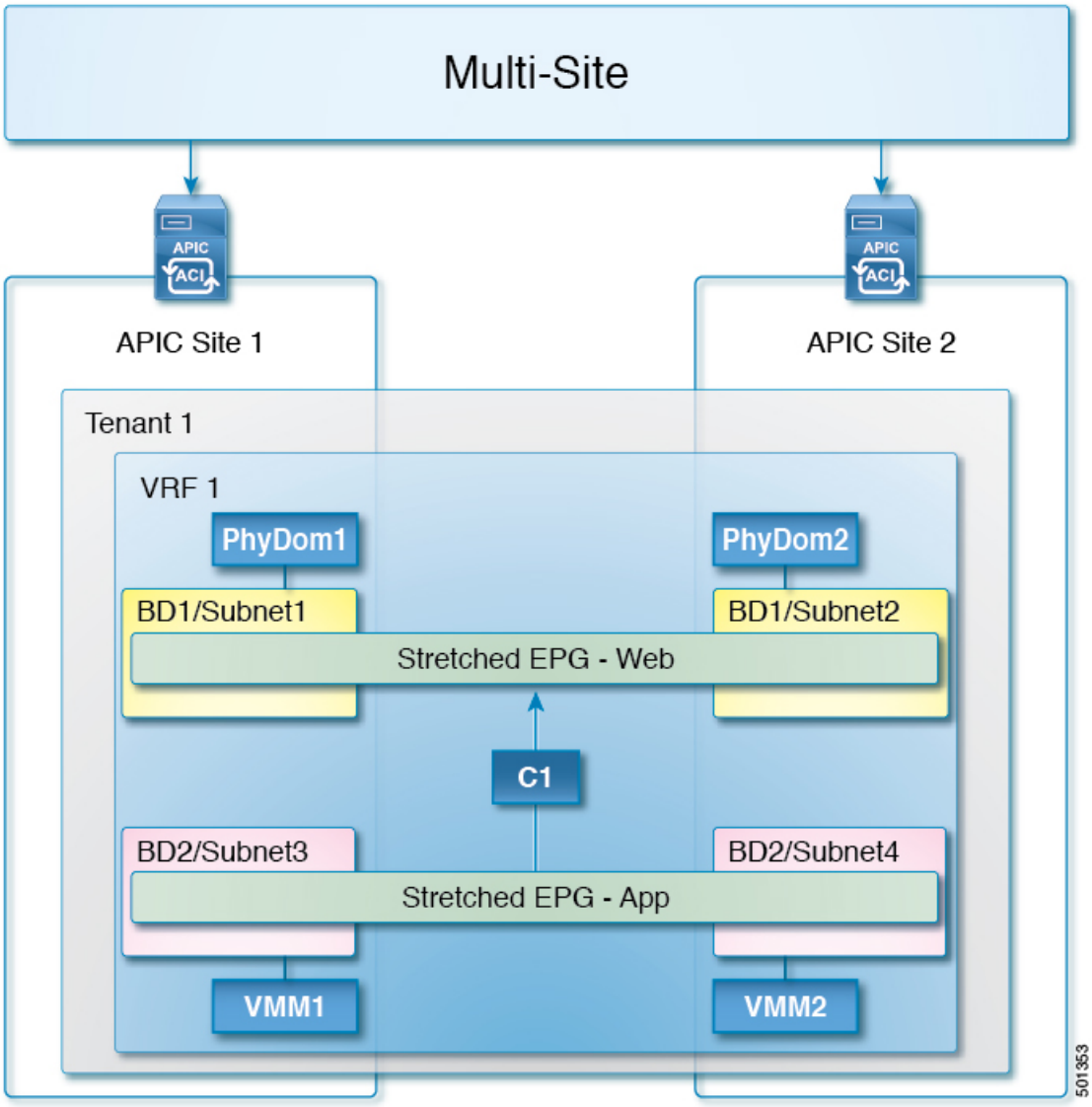
表 *2:* このユースケースで構成する機能

設定	説明	ストレッチまたはローカル
テナントおよび VRF	APIC からインポートされたか、 マルチサイトで作成された	ストレッチ
サイトのL3 Out(Site L3Outs)	APIC GUI で構成され、ストレッチされたテナントと VRF、サイト固有のテンプレートにリンクされている	ローカル
ブリッジ ドメイン	レイヤ 2 ストレッチが有効 レイヤ 2 フラッディングが無効 共有するサブネットが追加されている	ストレッチ
EPG	BD 内のすべての EPG	ストレッチ
コントラクト	EPG 通信を管理するために必要なフィルタとコントラクトをすべて含める	ストレッチ
外部 EPG	サイト L3Out のネットワークマッピング（Cisco ACI マルチサイト、リリース 1.0(1)） 外部 EPG を介したサイト L3Out のサイト接続（マルチサイト、リリース 1.0(2)）	ローカル、ただし他のサイトにリンクされる

サイト間ストレッチ EPG

この Cisco ACI マルチサイト のユースケースは、複数のサイトにまたがるエンドポイント グループ（EPG）を提供します。ストレッチEPGは、基盤となるネットワーキング、サイトローカル、およびブリッジドメインが異なる可能性がある複数のサイトに展開する、エンドポイントグループとして定義されます。

図 *20 :* サイト間ストレッチ *EPG*



このユースケースでは、すべてのサイトでレイヤ 3 転送を使用できます。

このユースケースの前提条件

- サイトが追加され、 APIC コントローラが現用系であり、通信が確立されていること。
- 関連するテナントが作成されていること。
- マルチサイト のサイトおよびテナントマネージャーのアカウントが使用可能であること
- 物理ドメインと VMM ドメインが APIC に存在する必要があります。

次の表のオブジェクトを含む、単一または複数のサイトにプッシュされるプロファイル：

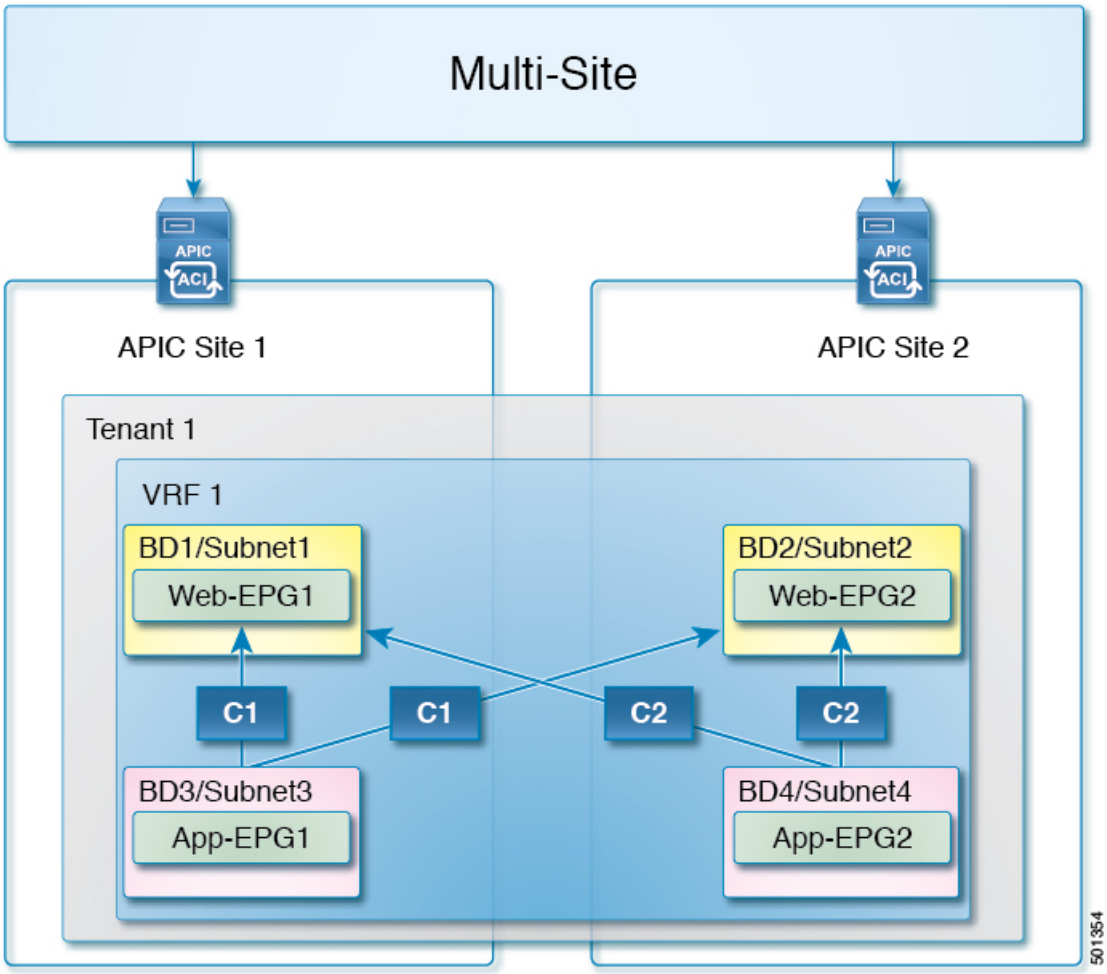
表 *3:* このユースケースで構成する機能

設定	説明	ストレッチまたはローカル
テナント、VRF、および EPG	APIC からインポートされたか、マルチサイト で作成されました。	ストレッチ
サイトのL3 Out(Site L3Outs)	APIC GUI で構成され、ストレッチされたテナントと VRF、サイト固有のテンプレートにリンクされている	ローカル
ブリッジドメイン（BD）	レイヤ 2 ストレッチが無効になっています。	ストレッチ
サブネット	ローカルサイトの各 BD に固有です。	ローカル
コントラクト	提供されたサイトで構成されたコントラクト	ローカル
外部 EPG	サイト L3Out のネットワークマッピング（Cisco ACI マルチサイト、リリース 1.0(1)） 外部 EPG を介したサイト L3Out のサイト接続（マルチサイト、リリース 1.0(2)）	ローカル、ただし他のサイトにリンクされる

サイト間コントラクトを使用したストレッチ VRF

この マルチサイト のユースケースは、同じストレッチ VRF の一部であるものの、異なるブリッジドメイン（BD）に接続されたエンドポイント間の、サイト間通信を可能にします。VRF ストレッチは、サイト間でEPG（およびサイト間のコントラクト）を管理するための便利な方法です。

図 *21* : サイト間コントラクトを使用した *VRF* ストレッチ



上の図では、App-EPG はサイト全体で C1 および C2 コントラクトを提供し、Web-EPG はサイト全体でそれらを消費します。

このユースケースには次の利点があります。

- テナントと VRF はサイト全体にストレッチされますが、EPG とそのポリシー（サブネットを含む）はローカルに定義されます。
- VRF はサイト間でストレッチされるため、コントラクトは EPG 間のサイト間通信を管理します。コントラクトは、サイト内またはサイト間で一貫して提供し、消費できます。
- トラフィックはサイト内およびサイト間（ローカルサブネットを使用）で回送され、サイト間の静的回送がサポートされます。
- 個別のプロファイルを使用して、ローカルオブジェクトとストレッチオブジェクトを定義し、プッシュします。
- レイヤ 2 ストレッチおよびローカル レイヤ 2 ブロードキャスト ドメインはありません。

- 「コールド」VM の移行では、移行されるエンドポイントの IP アドレスを保持する機能はありません。
- サービスグラフを使用したサイト間での共有アプリケーションのプッシュはサポートされていません。

このユースケースの前提条件

- サイトが追加され、 APIC コントローラが現用系であり、通信が確立されていること。
- ストレッチするテナントが作成されていること。
- マルチサイトのサイトおよびテナントマネージャーのアカウントが使用可能であること。

次の表のオブジェクトを含む、単一または複数のサイトにプッシュされるプロファイル：

表 *4*: このユースケースで構成する機能

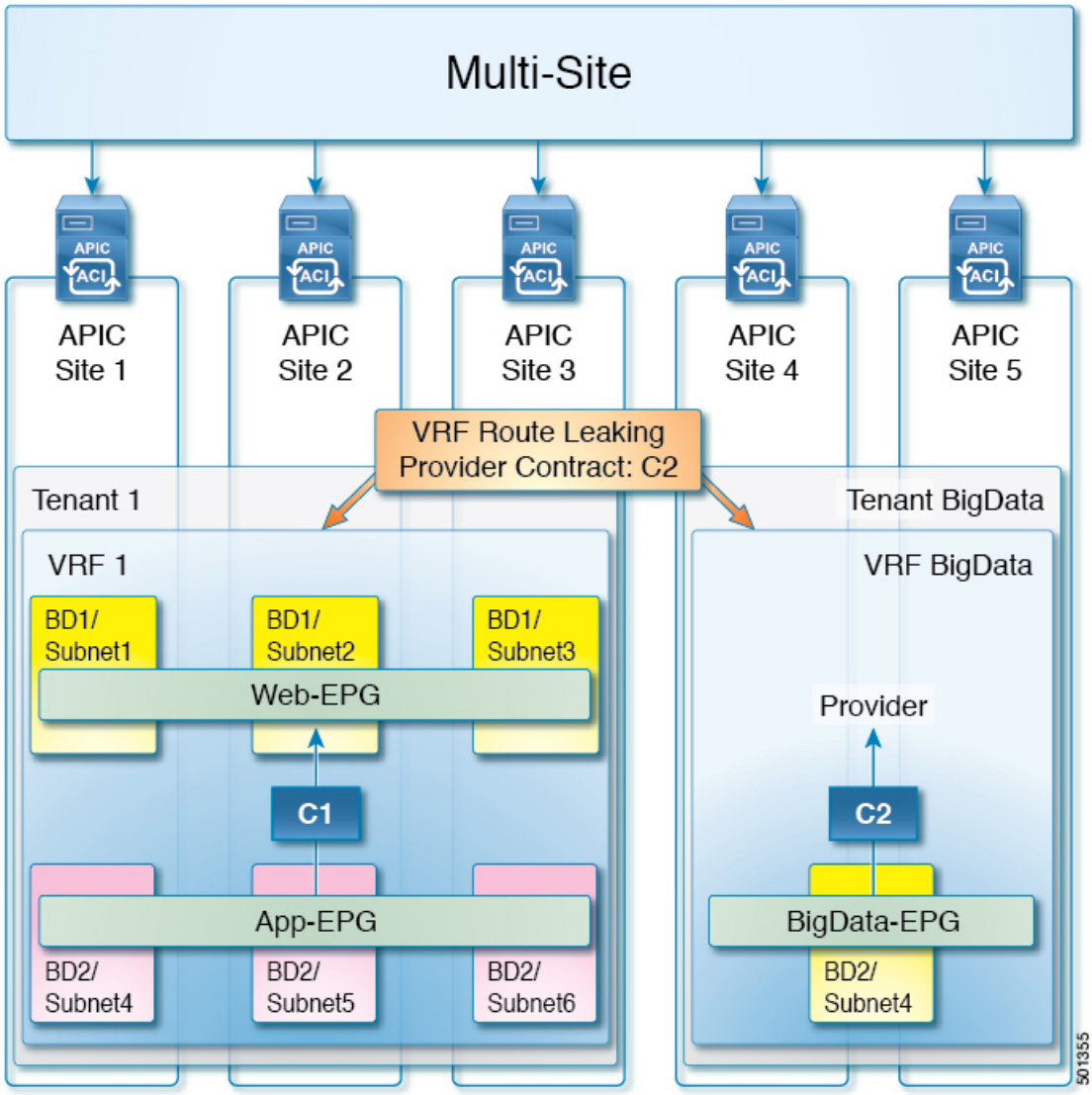
設定	説明	ストレッチまたはローカル
テナントおよび VRF	APIC からインポートされたか、 マルチサイトで作成された	ストレッチ
サイトのL3 Out(Site L3Outs)	APIC GUI で構成され、ストレッチされたテナントと VRF、サイト固有のテンプレートにリンクされている	ローカル
コントラクトを提供する EPG	サービスを提供する各サイトの EPG。	ローカル
コントラクトを消費する EPG	提供されたコントラクトを消費する EPG は、同じサイトにあることも、または複数のサイトに存在することもあり得る	ローカル
各 EPG のブリッジドメイン	レイヤ 2 ストレッチが無効 レイヤ 2 フラッディングが無効	ローカル
コントラクト	提供されたサイトで構成されたコントラクト	ローカル、ただし共有される

設定	説明	ストレッチまたはローカル
外部 EPG	サイト L3Out のネットワークマッピング（Cisco ACI マルチサイト、リリース 1.0(1)） 外部 EPG を介したサイト L3Out のサイト接続（マルチサイト、リリース 1.0(2)）	ローカル、ただし他のサイトにリンクされる

ストレッチプロバイダー EPG を使用した共有サービス

このユースケースでは、1つのサイトグループのプロバイダーEPGが共有サービスを提供し、別のサイトグループの EPG がサービスを消費します。すべてのサイトにローカル EPG とブリッジドメインがあります。

図 *22* : ストレッチプロバイダー *EPG* を使用した共有サービス



上の図では、サイト 4 とサイト 5（テナント BigData/VRF BigData 内の BigData-EPG を使用）が共有データサービスを提供し、テナント 1/VRF 1 内のサイト 1 ～サイト 3 の EPG がサービスを消費します。

マルチサイト の共有サービスのユースケースでは、ルーティング接続のために VRF 間で VRF 境界ルートがリークされます。これはサイト間でコントラクトをインポートすることによって行われます。

このユースケースには次の利点があります。

- 共有サービスにより、VRF とテナントの分離ポリシーとセキュリティポリシーを維持しながら、テナント間の通信が可能になります。
- 共有サービスは、重複しないサブネットのみでサポートされます。

- サイトの各グループには、異なるテナント、VRF、および 1 つ以上の EPG がストレッチされています。
- サイトグループは、レイヤ 2 ブロードキャスト拡張を使用するか、またはレイヤ 2 フラッディングをローカライズするように構成できます。
- ストレッチ EPG は同じブリッジドメインを共有しますが、EPG にはブリッジドメインではなく EPG で設定されたサブネットがあります。
- プロバイダーコントラクトはグローバル範囲に設定する必要があります。
- VRF ルートリークにより、VRF 間の通信が可能になります。
- サービスグラフを使用したサイト間での共有アプリケーションのプッシュはサポートされていません。

このユースケースの前提条件

- サイトが追加され、 APIC コントローラが現用系であり、通信が確立されていること。
- 関連するテナントが作成されていること。
- マルチサイト のサイトおよびテナントマネージャーのアカウントが使用可能であること

次の表のオブジェクトを含む、サイトのグループにスキーマがプッシュされていること（テンプレートによる）：

表 *5:* この活用ケースで構成する機能

設定	説明	ストレッチまたはローカル
複数のテンプレートを使用した共有サービスプロバイダースキーマ	共有テンプレートには、次のオブジェクトが含まれます。 • テナント • VRF • グローバル範囲のプロバイダーコントラクト。 • サブネットが**外部でアドバタイズ**および**VRF 間で共有**に設定された EPG。 ブリッジドメイン（オプションでレイヤ 2 拡張用に設定）および外部 EPG を含む、サイト固有のテンプレート	ストレッチ（プロバイダーグループ内のすべてのサイトにプッシュ）

設定	説明	ストレッチまたはローカル
複数のテンプレートを使用した共有サービスコンシューマスキーマ	共有テンプレートには、次のオブジェクトが含まれます。 • テナント • VRF • サブネットが**外部でアドバタイズ**および**VRF 間で共有**に設定された EPG。 （注） コンシューマ EPG の場合、代わりにサブネットを BD に追加できます。 • コンシューマコントラクト（提供されたコントラクトと同じ名前）。 ブリッジドメイン（オプションでレイヤ 2 拡張用に設定）および外部 EPG を含む、サイト固有のテンプレート	ストレッチまたはローカル
VRF ルート リーク	VRF ルートリークを有効にするようにコントラクトを構成する必要があります。	構成3済みのクロスサイト

Cisco ACI ファブリックから Cisco ACI マルチサイト への移行

これは Cisco ACI マルチサイト の一般的な使用例で、テナントを Cisco ACI ファブリックから Cisco ACI マルチサイト に移行またはインポートします。

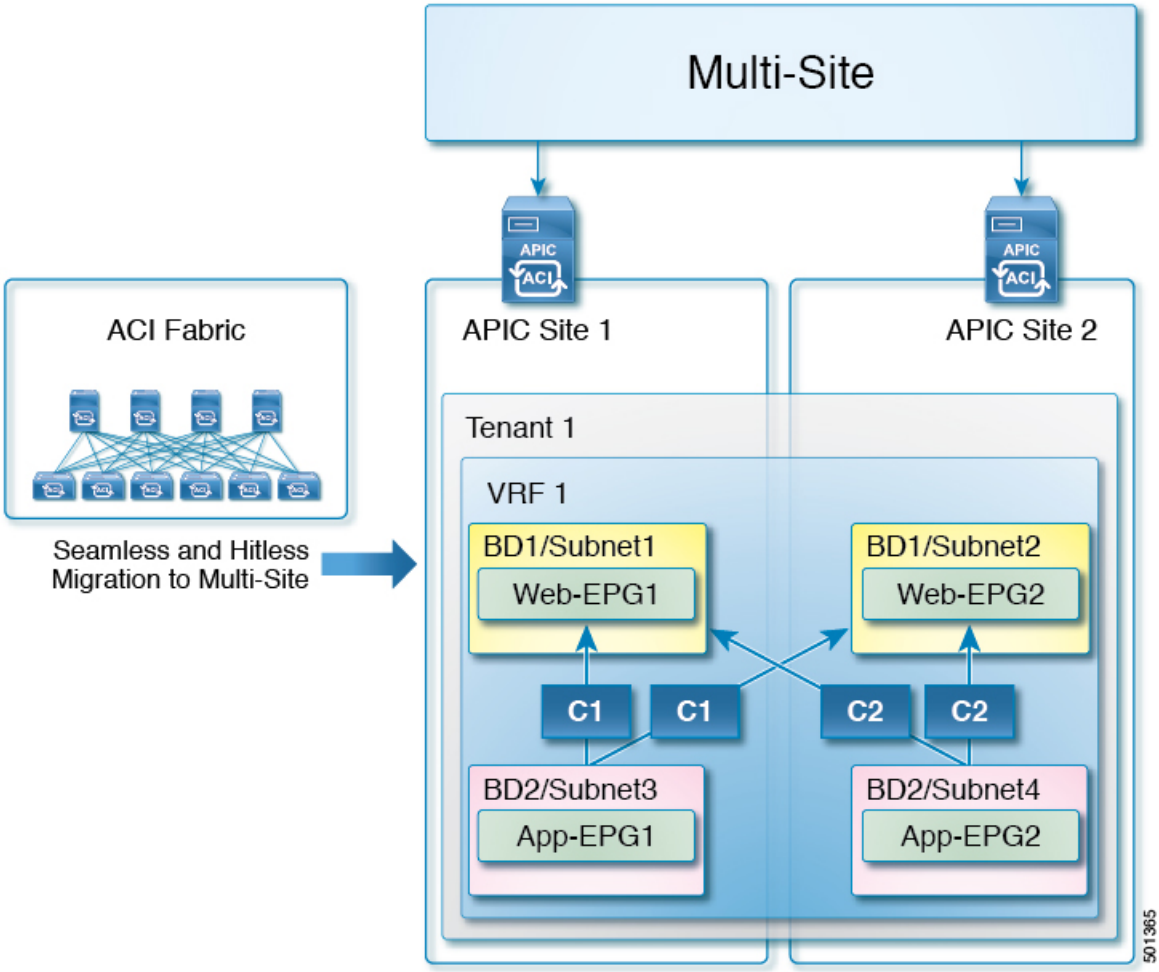
このユースケースは、ブラウンフィールドからグリーンフィールドおよびグリーンフィールドからグリーンフィールドへの展開タイプを対象としています。ブラウンフィールドからブラウンフィールドへの使用例は、両方の Cisco APICサイトが同じ構成で展開されている場合にのみ、このリリースでサポートされます。その他のブラウンフィールドからブラウンフィールドへの使用例は、今後の Cisco ACI マルチサイト リリースで展開される予定です。

ブラウンフィールド構成では、次の 2 つの展開シナリオが考慮されます。

- 単一または複数のポッド ACI ファブリックがすでに配置されている。マルチサイト 構成に別のサイトを追加できます。

- 2 つの ACI ファブリックがすでに配置されており、サイト間のオブジェクト（テナント、VRF、および EPG）は最初、同じ名前とポリシーで定義され、従来の L2/L3 DCI ソリューションを利用して接続されている。次の構成図で説明されているように、この構成をマルチサイト に変換することができます。

図 *23 : Cisco ACI* ファブリックから *Cisco ACI* マルチサイト への移行



マルチポッド対応ファブリックで Cisco ACI マルチサイト を設定する

リリース1.2(1) 以降、2 つの使用例で、マルチポッド対応ファブリックで Cisco ACI マルチサイト をセットアップするためのサポートが追加されています。

これら 2 つの使用例のガイドラインと制限事項は次のとおりです。

- 次のスイッチのみが IPN/ISN に接続されます。
  - Cisco Nexus 93180LC-EX、93180YC-EX、および 93108TC-EX スイッチ。
  - 以下のラインカードを搭載した Cisco Nexus 9504、9408、9516 スイッチ

- X9736C-EX
- X97160YC-EX
- X9732C-EX
- X9732C-EXM

- 旧世代のスパインスイッチから IPN リンクを削除します。

- マルチポッドと マルチサイトには同じ IPN/ISN が使用されます。
- Cisco ACI マルチサイト 展開では、単一の IPN/ISN を使用する 2 つのサイトで、重複するトンネルエンドポイント（TEP）プール範囲と GIPO プール範囲を使用することはできません。

テナントが Cisco APIC GUI からインポートされると、テナントに関連付けられているすべてのオブジェクトが Cisco ACI マルチサイト にインポートされます。

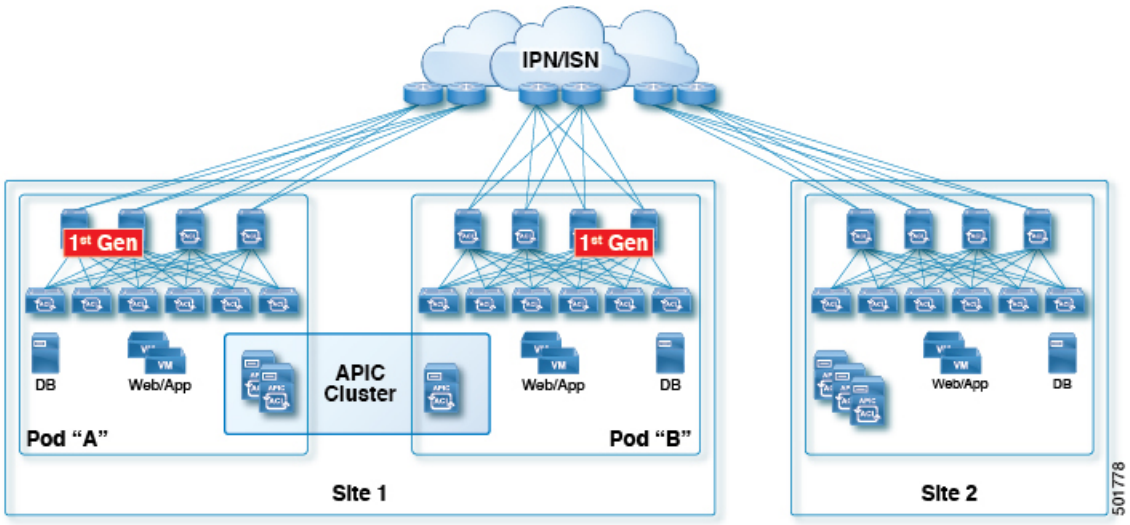
表 *6 :* これらの使用例で構成する機能

設定	説明	ストレッチまたはローカル
テナント	Cisco ACI マルチサイト でテナントを作成し、Cisco APIC からテナントポリシーをインポートします。	ストレッチ
VRF	テナントの VRF インスタンス	ストレッチ
ブリッジ ドメイン	レイヤ 2 ストレッチが有効 レイヤ 2 フラッディングが有効 共有するサブネットが追加されている	ストレッチ
EPG	BD 内の EPG	ストレッチ
コントラクト	EPG 通信を管理するために必要なフィルタを含める	ストレッチ
サイトのL3 Out(Site L3Outs)	Cisco APIC で構成され、外部 EPG とリンクされている	ローカル

マルチポッドファブリックを Cisco ACI マルチサイト のサイトとして追加する

このセクションでは、 Cisco ACI マルチサイト にマルチポッドファブリックをサイトとして追加する方法の概要について説明します。

図 *24 : Cisco ACI* マルチサイト に複数のポッドを持つ *Cisco ACI* ファブリック



次に、手順の概要を示します。

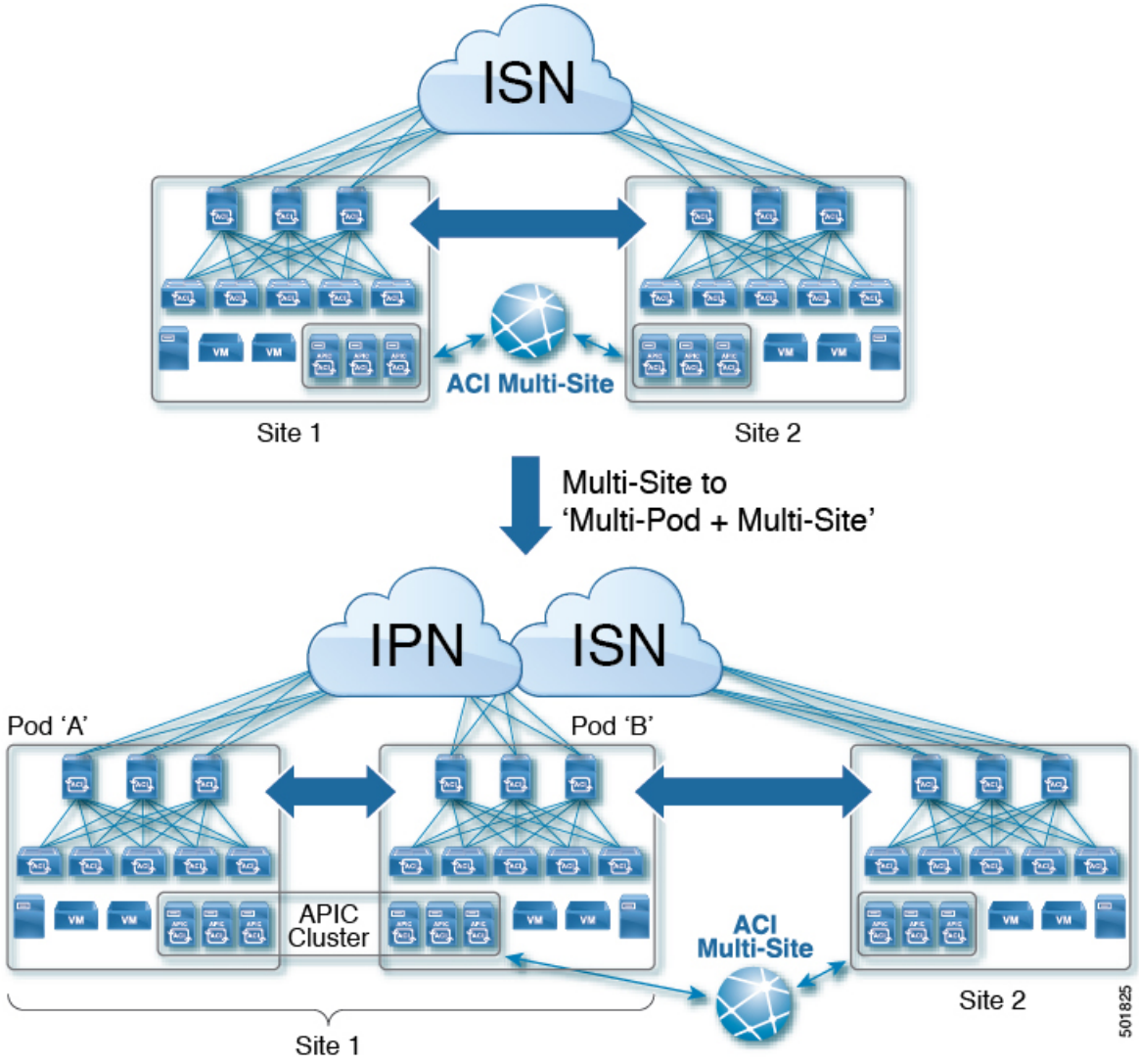
- Cisco ACI マルチサイト でマルチポッド対応ファブリックをサイトとして追加します。
  - Cisco ACI マルチサイト は、 マルチサイト とマルチポッドの一般的な構成（スパインから IPN へのリンクの構成、OSPF 情報、BGP 情報など）を検出し、 Cisco ACI マルチサイト のインフラ構成に自動入力します。
- マルチサイト 固有の構成（MCAST TEP、MSITE DP-TEP、MSITE CP-TEP など）を指定し、 Cisco ACI マルチサイト のインフラページでサイトの マルチサイト を有効にします。
  - マルチサイト にも、マルチポッド用に設定したものと同じ DP-TEP/CP-TEP を構成できます。
- Cisco ACI マルチサイト にインフラ構成を展開します。
  - Cisco ACI マルチサイト は、Cisco APIC を マルチサイト 固有の構成と、 マルチサイト とマルチポッドの一般的な構成（スパインから IPN リンク構成、OSPF 情報、BGP 情報など）で構成します。マルチポッド固有の構成は構成しません。
  - Cisco ACI マルチサイト は、マルチポッドに使用されるのと同じインフラ L3Out を使用して マルチサイト を構成します。 Cisco ACI マルチサイト は、インフラ L3Out の l3extInfraNodeP での fabricExtCtrlPeering=yes および fabricExtIntersiteCtrlPeering=yes に基づいて決定します。

- マルチサイト およびマルチポッドに使用するのと同じ L3Out で GOLF を構成できます。サポートされている構成は次のとおりです。
  - マルチサイト、マルチポッド、および GOLF 用の 1 つの L3Out、および GOLF 用の異なる（0 以上の）L3Out。
  - マルチサイト 用の 1 つの L3Out、マルチポッド、および GOLF 用の異なる（0 以上の）L3Out。

マルチサイトのシングルポッドサイトからマルチポッドサイトへの変換

このセクションでは、マルチサイトのシングルポッドサイトをマルチポッドサイトに変換する方法の概要について説明します。

図 *25 :* マルチサイトのシングルポッドサイトからマルチポッドサイトへの変換



次に、手順の概要を示します。

- 両方の通信に同じスパインノードとアップリンクを使用します。
- Cisco APIC を使用してマルチポッドを構成します。マルチサイト で使用したものと同じインフラ L3Out をマルチポッドにも使用します。
- マルチポッドと マルチサイト の両方に同じ BGP-EVPN ルータ ID とオーバーレイ TEP を使用することも、マルチポッドと マルチサイト に別個のルータ ID と TEP を定義することもできます。
- Cisco ACI マルチサイト を構成した後、Cisco ACI マルチサイト インフラページの [更新] アイコンをクリックして、新しいポッドを検出します。

- Cisco ACI マルチサイト で、 マルチサイト 固有の構成（オーバーレイ TEP や BGP-EVPN ルータ ID など）を指定します。
- インフラストラクチャを展開します。

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。