レイヤ 4 ~ レイヤ 7 サービスの使用例
リリース 12.2.2

目次

新規情報および変更情報 1
NDFC サービスの命名法と冗長性モデル 2
ユースケース 1：デフォルト ゲートウェイとしてのサービス機能 5
1. サービス挿入のユースケース（デフォルトゲートウェイとしてのサービス機能）の選択 6
2a. サービス機能の追加 8
3. サービス クラスタの論理接続の追加 8
4a. サービス クラスタの追加 8
5. サービスノードを追加 9
4b. サービス ネットワークの作成 12
4c. スタティックピアリング 13
4c. eBGP ピアリング 14
2b. 内部ネットワークの作成/選択 17
ユースケースのアタッチと展開 19
ユースケース 2：境界デバイスとしてのサービス機能 20
1. サービス挿入のユースケース（境界サービス）の選択 21
2. サービス機能の追加 23
3. サービス クラスタの論理接続の追加 23
4a. サービス クラスタの追加 24
5. サービスノードを追加 24
4b. 内部/外部ネットワークの作成 27
4c. ローカル eBGP ピアリング 29
ユースケースのアタッチと展開 33
ユースケース 3：サービス チェーンへのリダイレクト 34
ユースケース 3a：ファイアウォール サービスへのリダイレクト 34
1a. サービス挿入のユースケースの選択（サービス チェーンにリダイレクト） 36
2a. ACL 照合トラフィックの作成 38
2b. サービス チェーンの作成（ファイアウォールのみ） 39
3. サービス機能の追加 40
4a. サービス クラスタの論理接続の追加 42
5a. サービス クラスタの追加 42
6. サービスノードを追加 43
4b. サービス クラスタの論理接続の追加 45
5b. プローブ設定の追加 46
4c. サービス クラスタの論理接続の追加 47
2c. プローブ失敗時のアクションの選択 48
2d. 送信元および接続先ネットワークの作成/選択 48
ユースケースのアタッチと展開 49
ユースケース 3b：ファイアウォール ロード バランサ サービス チェーンへのリダイレクト 50
1. サービス挿入のユースケースの選択（サービス チェーンにリダイレクト） 52
2a. ACL 照合トラフィックの作成 53
2b. サービス チェーンの作成（ファイアウォールとロード バランサ） 55

3a. サービス機能の追加（ファイアウォール） 56
4a. サービス クラスタの論理接続（ファイアウォール）の追加 58
5a. サービス クラスタの追加（ファイアウォール） 58
6. サービス ノードの追加（ファイアウォール） 59
4b. サービス クラスタの論理接続（ファイアウォール）の追加 61
5b. プローブ構成（ファイアウォール）の追加 62
4c. サービス クラスタの論理接続（ファイアウォール）の追加 64
2c. プローブ失敗アクションの選択（ファイアウォール） 64
3b. サービス機能の追加（ロード バランサ） 64
4a. サービス クラスタの論理接続の追加（ロード バランサ） 66
5a. サービスクラスタの追加（ロード バランサ） 66
6. サービスノードの追加（ロード バランサ） 67
4b. サービス クラスタの論理接続の追加（ロード バランサ） 68
5b. プローブ構成（ロード バランサ）の追加 70
4c. サービス クラスタの論理接続の追加（ロード バランサ） 71
2c. プローブ失敗アクション（ロード バランサ）の選択 72
2d. 送信元および接続先ネットワークの作成/選択 72
ユースケースのアタッチと展開 73
一般的な 1 アームサービス機能のユースケース 73
送信元 NAT を使用したロード バランサ（SNAT） 74
1 アーム境界ファイアウォール 75
著作権 78

新規情報および変更情報

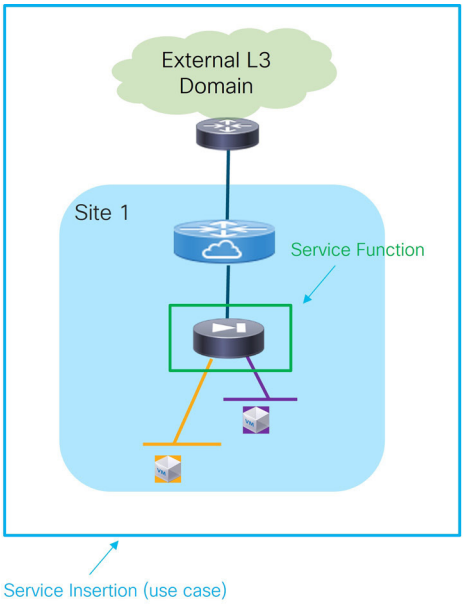
次の表は、この最新リリースまでの主な変更点の概要を示したものです。ただし、今リリースまでの変更点や新機能の一部は表に記載されていません。

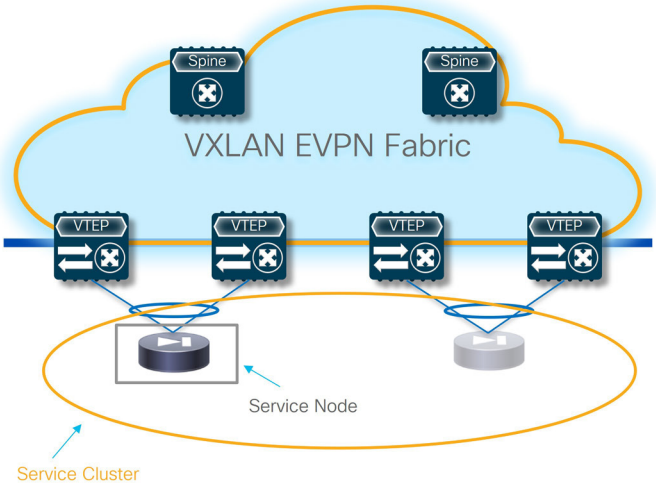
リリース バージョン	特長	説明
NDFC 12.2.2	レイヤ 4 からレイヤ 7 のユースケースを更新	レイヤ 4 ~ レイヤ 7 サービスを設定するための拡張ワークフローの一部として（レイヤ 4 ~ レイヤ 7 サービス の構成記載）、この記事では、いくつかの新しいレイヤ 4 ~ レイヤ 7 のユースケースを示します。

NDFC サービスの命名法と冗長性モデル

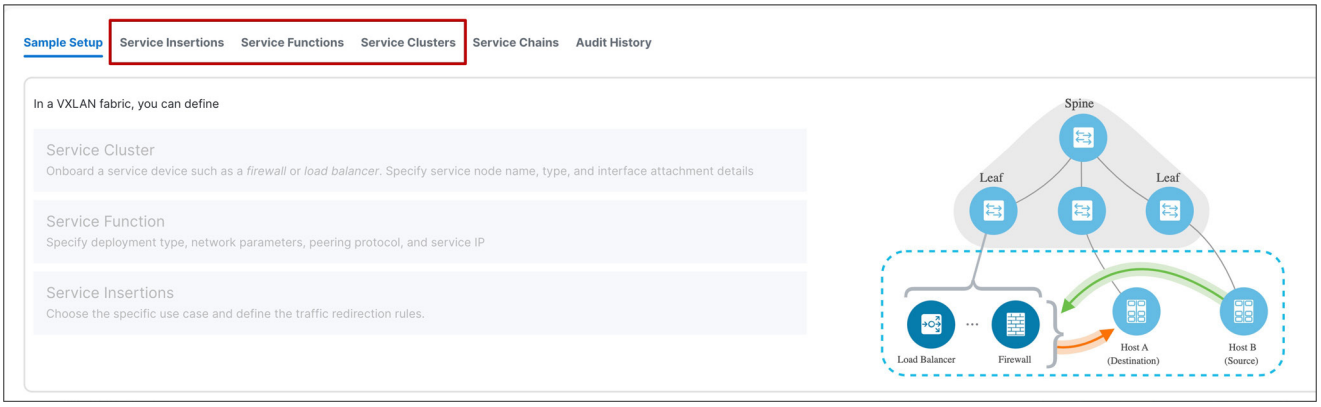
NDFC 12.2.2 を使用してプロビジョニングできるさまざまなユースケースを説明する前に、重要な点として、そのようなユースケースのプロビジョニングに使用される新しい NDFC の命名法と、サポートされるサービス冗長性モデルを明確にしておきます。

次の図は、NDFC 12.2.2 で L4/L7 サービスのユースケースをプロビジョニングするために必要なさまざまな構成要素を示しています。





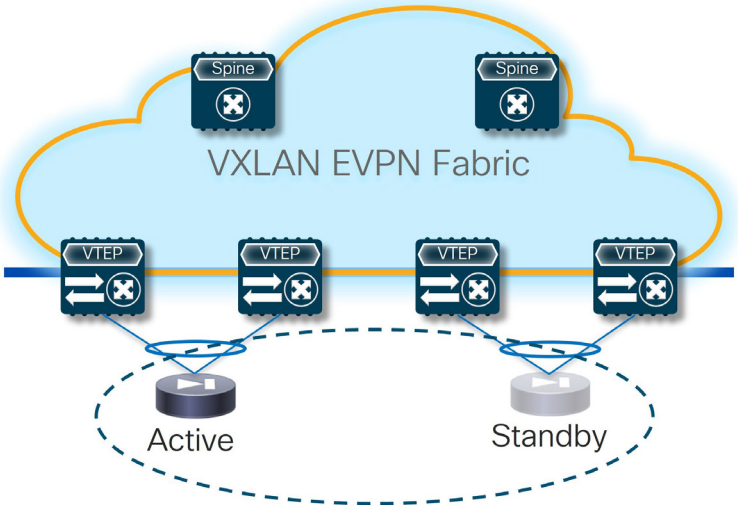
NDFC 12.2.2 の命名法



NDFC サービス UI

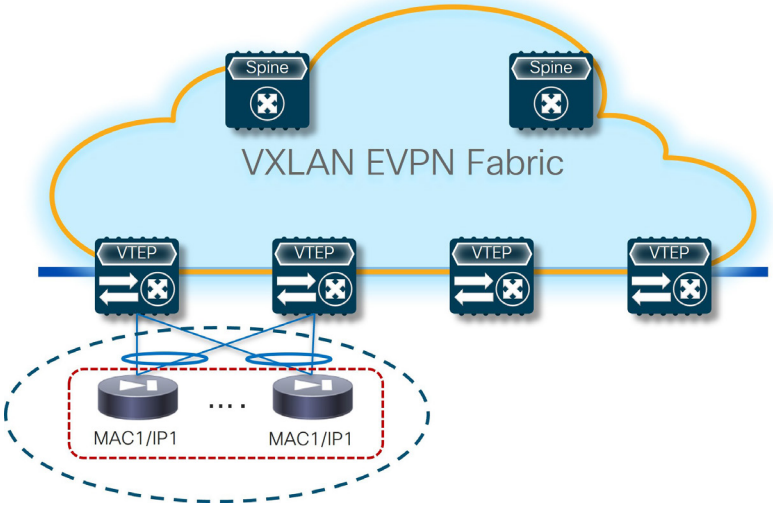
- **サービス挿入**：サポートされている一連のユースケースを表します。サービス挿入のユースケースの選択では、NDFC 12.2.2 で L4/L7 サービス挿入をプロビジョニングするために必要なワークフローの最初のステップが常に示されているはずです。これは、ファブリックノードでの構成のプロビジョニング（または削除）が、特定の各サービス挿入のユースケースの接続（または切断）を促すものとなるためです。
- **サービス機能**：ネットワークに統合する必要がある特定の L4/L7 サービス（ファイアウォール、ロード バランサなど）を識別します。選択したサービス挿入のユースケースに応じて、単一のサービス機能または一連のサービス機能をワークフローの一部としてプロビジョニングする必要があります。
- **サービスクラスタ**：選択したサービス機能の展開方法を表します。より具体的には、その冗長性モデルです。次のオプションがサポートされています。

- アクティブ/スタンバイ クラスタ：単一の MAC アドレスと IP アドレスをインフラストラクチャの残りの部分に公開するサービス機能を実装するための、デバイスのペア。特定の MAC/IP は常にアクティブ デバイスによって所有されますが、フェールオーバー イベントの結果としてスタンバイがアクティブになると、それによって継承されます。



アクティブ/スタンバイクラスタ

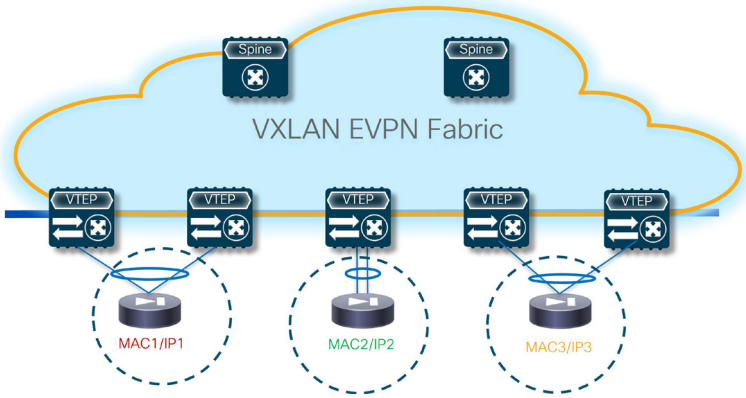
- アクティブ/アクティブ クラスタ：複数のデバイス（最大数は特定のクラスタの実装によって異なります）がクラスタ化され、アクティブ/アクティブ モードで動作する一方で、ネットワーク インフラストラクチャからは単一の MAC/IP の組み合わせとみなされます（つまり、すべてのアクティブなクラスタ内のノードは同じ MAC/IP アドレスのペアを所有します）。



アクティブ/アクティブクラスタ

- スタンドアロン ノード：一連のスタンドアロン サービス ノードで構築された特定タイプの「クラスタ」です。それぞれが専用の MAC/IP アドレス ペアを所有しています。MAC/IP アドレスのペアのセットを使用したサービス機能の展開は、トラフィック パスで非対称性を生じさせることなくトラフィックをロード バランシングできるメカニズムが必要であることを意味します（通常、スタンドアロン ノード間では、接続状態が同期されないからです）。

> 「スタンドアロン」ノードは単一の MAC/IP ペアによって識別されるため、アクティブ/スタンバイまたはアクティブ/アクティブ クラスタのどちらでも実装できます。



スタンドアロン サービス ノード

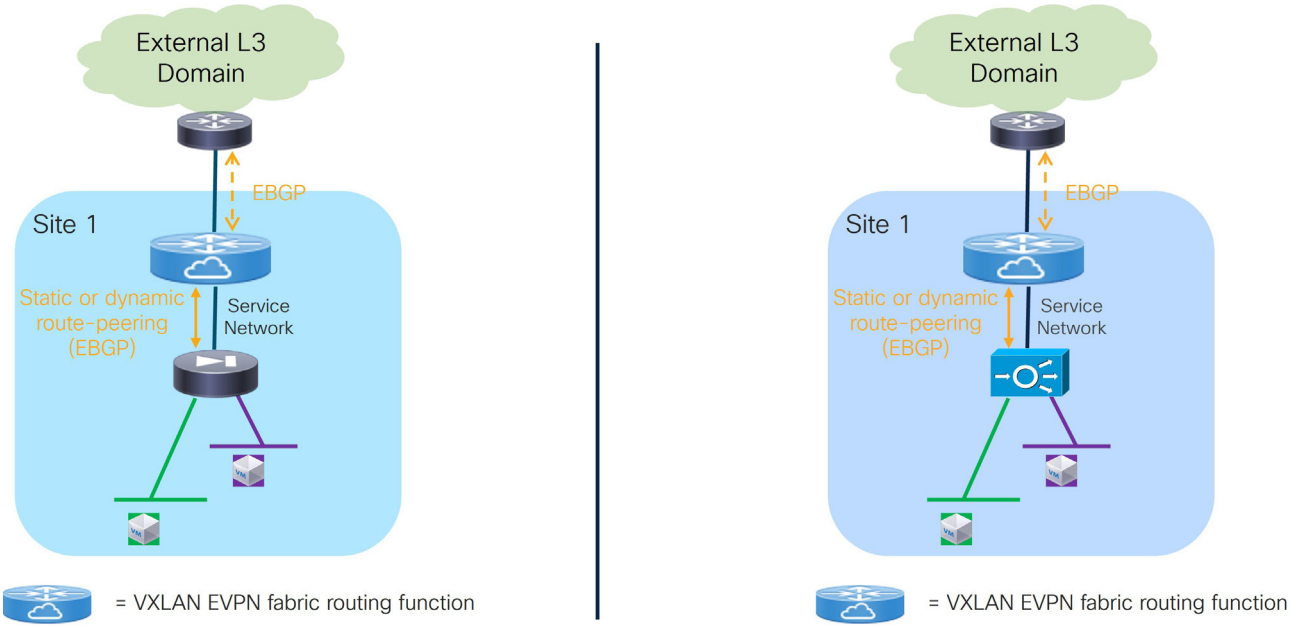
- **サービス ノード**：サービス機能の役割を提供する特定のデバイスを表します。これらのデバイスは、さまざまなフォーム ファクタで提供されます（物理または仮想）。

次のセクションでは、VXLAN EVPN ファブリックでのさまざまな L4/L7 サービス挿入のユースケースについて詳しく説明し、必要なさまざまな構成手順を強調します。NDFC には、これらのユースケースをプロビジョニングする方法に柔軟性がありますが、この設定ガイドで説明されているワークフローに従うことを強く推奨します。

> 以前の NDFC リリースでは、接続/切断オプションもサービス機能に直接関連付けられており、「サービス挿入」のユースケースの概念はありませんでした。古いリリースから NDFC 12.2.2（ND 3.2.1 統合イメージの一部）にアップグレードする場合、古い設定が受け入れられます。（トラフィックおよびファブリックにすでにプロビジョニングされている構成については、中断は発生しません）。
>
> ただし、12.2.2 より前の構成は特定のサービス挿入のユースケースに変換されません。つまり、その構成を削除または変更することは基本的にできません。

ユースケース 1：デフォルト ゲートウェイとしてのサービス機能

デフォルト ゲートウェイとしてのサービス機能ユースケースの論理ビューについては、次の図を参照してください。図にはファイアウォールとロード バランサの機能が示されていますが、このユースケースは一般のサービス機能に適用できます。



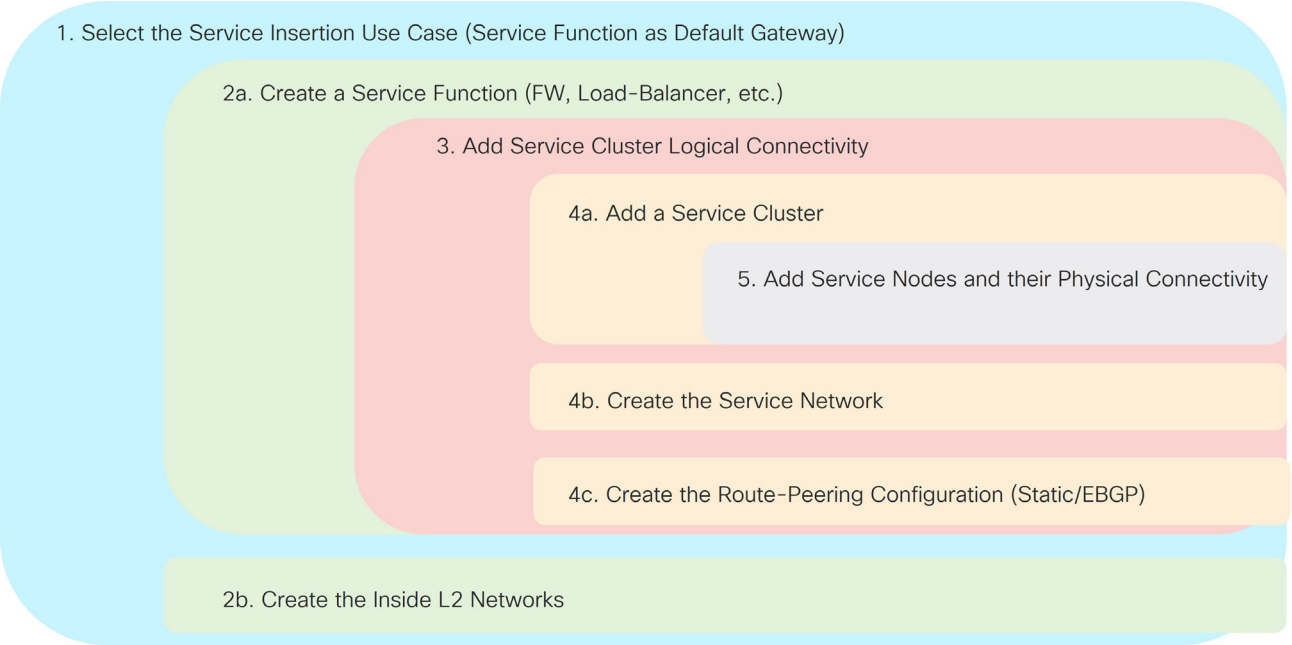
デフォルト ゲートウェイとしてのサービス機能：論理ビュー

サービス機能は **N アーム** モードで展開されます：

- 最初のアームでは、ファブリックに展開された専用 VRF とのピアリングが可能です。このピアリングでは、静的ルーティングを活用すること、または eBGP をコントロール プレーンとして使用することができます。ファブリックは通常、その VRF でサービス機能および外部ネットワーク ドメインとピアリングして、サービス機能の背後に接続されているデータセンター リソースへのアクセスを提供します。
- 他のアームは、ファブリックに展開され、デフォルト ゲートウェイとしてサービス機能を使用するエンドポイントをホストするレイヤ 2 専用ネットワークに接続されます。

サービス機能をデフォルト ゲートウェイとして構成する場合の NDFC ワークフローのグラフィカル表現については、次の図を参照してください。

> 次の図に示すプロビジョニング手順については、以降のセクションで詳しく説明します。各セクションに関連付けられた番号は、図の対応するステップにマッチしています。ワークフローはステップ間を前後に移動するため、セクションの番号付けは必ずしも、順番通りではありません。



デフォルトゲートウェイとしてのサービス機能：NDFC ワークフロー

1. サービス挿入のユースケース（デフォルトゲートウェイとしてのサービス機能）の選択

1. **[サービス インスタンス（Service Instance）]** タブに移動します。
   a. 次の順に選択：

      [管理（Manage）] > [ファブリック（Fabrics）]

   b. 適切な Data Center VXLAN EVPN ファブリックをダブルクリックします。

      ファブリックの**[概要（Overview）]** ウィンドウが表示されます。

   c. **[サービス（Services）]** タブをクリックします。
   d. **[サービス挿入（Service Insertions）]** サブタブをクリックします。

      構成されているサービス挿入のユースケースのリストが表示されます。

2. **[アクション（Actions）] > [サービス挿入の追加（Add Service Insertion）]** をクリックします。

   [サービス挿入の追加（Add Service Insertion）] ウィンドウが表示されます。

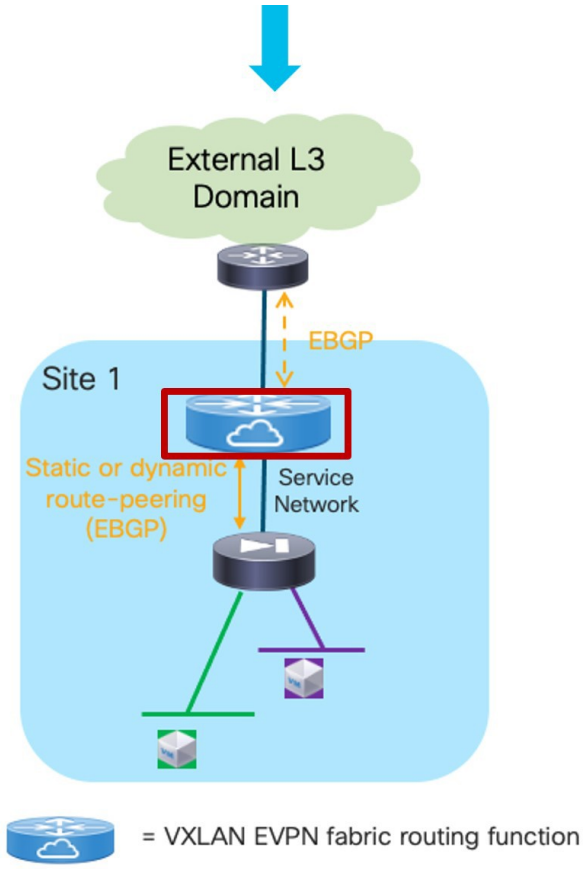
3. **[サービス挿入の名前（Service Insertion Name）]** フィールドに、サービスの名前を入力します。

   名前にはアルファベット、数字、アンダースコア、または文字を含めることができます。たとえば、この特定のユースケースでは、サービス挿入名として FW-as-Default-Gwy を使用できます。

4. **[ユースケース（Use Case）]** フィールドで、適切なユースケースを選択します。

   このユースケースでは、**[サービス（Service as Default Gateway）]** をユースケースとして選択します。

5. **[外部 VRF 名（Outside VRF Name）]** フィールドで、サービス機能がピアリングするファブリック内の VRF を選択します。



デフォルトゲートウェイとしてのサービス機能：外部 VRF

このサービス挿入のユースケースに関連付ける既存の外部 VRF を選択するか、**[+VRF の作成（+Create VRF）]** をクリックして新しい VRF を作成します。詳細については、LAN 動作モード セットアップのためのファブリックの概要 の「VRF」セクションを参照してください。

6. **[デタッチ/アタッチ（Detach/Attach）]** フィールドで、切り離す、または接続するようにスイッチを切り替えます。

   特定のサービス挿入ワークフローの最後にスイッチに構成をプロビジョニングできるようにするには、**[アタッチ（Attach）]**オプションを選択する必要があります。**[アタッチ（Attach）]** オプションは、この時点で、または構成設定ワークフローのすべての手順を完了した後の手順の最後に選択できます。

7. **[サービス機能（Service Function）]** フィールドで、このサービス挿入使用例に関連付ける既存のサービス機能を選択するか、**[+サービス機能の作成（+Create Service Function）]** をクリックして新しいサービス機能を作成します。

   - 推奨されるアプローチは、**[+サービス機能の作成 （+Create Service Function）]** をクリックして新しいサービス機能を作成することです。サービス機能のオプション（1 アーム、2 アームなど）が、プロビジョニングされる特定のサービス挿入のユースケースに基づいて自動的に提案され、適切であることが保証されるからです。**[+サービス機能の作成（+Create Service Function）]**をクリックした場合は、2a に進みます。サービス機能を追加します。
   - このユースケースで既存の構成済みサービス機能を選択した場合、**[ユースケース （Use Case）]** フィールドで **[デフォルト ゲートウェイとしてのサービス（Service as Default Gateway）]** を選択したはずなので、サービス機能のプルダウン リストには、**N アーム**接続モードやステップ 5 で指定する外部 VRF など、特定の設定オプションを持つサービス機能が事前に入力されます。2b に進みます。内部 ネットワークを作成/選択します。

2a. サービス機能の追加

1. **[タイプ（Type）]**フィールドで、展開するサービス機能のタイプを選択します。

   この特定の例では、展開するサービス機能のタイプとして **[ファイアウォール（Firewall）]** を選択します。

2. **[サービス機能名（Service Function Name）]** フィールドに、サービス機能の名前を入力します。

   名前にはアルファベット、数字、アンダースコア、または文字を含めることができます。

3. 次の 2 つのフィールドの情報を確認します。

   次の 2 つのフィールドは、すでに入力した情報に基づいて自動的に入力されます。

   - **[接続モード（Connectivity Mode）]**： ステップ 1 で選択した、サービス挿入の「デフォルト ゲートウェイとしてのサービス」のユースケースに基づいて、N アームが自動的に選択されます。
   - **[外部 VRF（Outside VRF）]**：1 の **[外部 VRF 名（Outside VRF Name）]** フィールド に指定したエントリに基づいて自動的に入力されます 1. [サービス挿入のユースケース (デフォルト ゲートウェイとしてのサービス機能) (Select the Service Insertion Use Case (Service Function as Default Gateway))] を選択します。

4. **[+ サービス クラスタ論理接続の追加（+ Add Service Cluster Logical Connectivity）]** をクリックします。

   これにより、サービス ノードをデフォルト ゲートウェイとして利用するファブリックの VRF およびエンドポイントのレイヤ 2 ネットワークとサービスノードをピアリングするために使用されるサービス ネットワークをプロビジョニングできます。

   [サービス クラスタ論理接続の追加（Add Service Cluster Logical Connectivity）] ウィンドウが表示されます。3 に進みます。サービス クラスタ の論理接続を追加します。

3. サービス クラスタの論理接続の追加

1. **[サービス クラスタ名（Service Cluster Name）]** フィールドで、構成済みのサービス クラスタを選択するか、**[+サービス クラスタの追加（+Add Service Cluster）]** をクリックして新しいクラスタを作成します。
   - **[+ サービス クラスタの追加（+Add Service Cluster）]**をクリックした場合は、4a に進みます。サービス クラスタを追加します。
   - このユースケースで既存の構成済みのサービス クラスタを選択した場合は、4b に進みます。サービス クラスタの論理接続を追加します。

4a. サービス クラスタの追加

1. **[タイプ（Type）]** フィールドの情報を確認します。

   2a のステップ 1 で選択したサービス挿入のユースケースに基づいて、**[タイプ（Type）]** フィールドが自動的に入力されます。サービス機能を追加します。

2. サービス クラスタを追加するために必要な情報を入力します。

フィールド	説明
サービスクラスタ名	サービス クラスタの名前を入力します。名前にはアルファベット、数字、アンダースコア、または文字を含めることができます。
ノードの冗長性	ノードの冗長性を選択します。 ・**[スタンドアロン（Standalone）]**：次の手順で単一のサービス ノードを追加する場合に適用されます。 ・**[アクティブ/スタンバイ クラスタ（Active/Standby Cluster）]**：次の手順で 2 つのサービス ノードを追加し、同じアクティブ/スタンバイ クラスタの一部にする場合に適用されます。 ・**[アクティブ/アクティブ クラスタ（Active/Standby Cluster）]**：次の手順で 2 つ以上のサービス ノードを追加し、単一のアクティブ/アクティブ クラスタの一部にする場合に適用されます。
フォーム ファクタ	**[物理（Physical）]** または **[仮想（Virtual）]** を選択します。

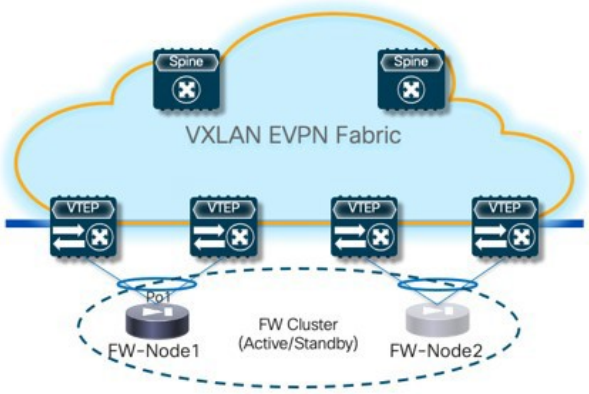
3. **[+ サービスノードの追加（+ Add Service Node）]** をクリックします。

   [サービス ノードの追加（Add Services Node）] ウィンドウが表示されます。「5. サービスノードを追加して、クラスタのサービス ノード部分とファブリックへの物理接続を定義します。

5. サービスノードを追加

ここで説明する特定の例では、次の図に示すように、2 つのサービスノード（同じアクティブ/スタンバイ クラスタの一部である FW-Node1 と FW-Node2）を設定します。

> 必要に応じ、デフォルト ゲートウェイとしてアクティブ/アクティブ クラスタを展開することもできます。



デフォルト ゲートウェイとしてのサービス機能：2 つのサービス ノードの構成

> 上の図に示すように、クラスタのサービス ノード部分を異なるリーフ ノードのセットに接続して、サービス機能の復元力を高めることを推奨します。ただし、NDFC 12.2.2 では、ファイアウォール サービス機能の展開に「アクティブ/スタンバイ」クラスタ オプションを選択した場合、アクティブなファイアウォール デバイスとスタンバイ ファイアウォール デバイスが接続されているリモート VTEP ノード間の eBGP ピアリングのプロビジョニングは許可されません。

ファイアウォール フェールオーバー シナリオでトラフィックの停止を最小限に抑えるために、通常はこれらの eBGP 隣接関係を確立することを推奨します。

NDFC 12.2.2 で使用可能な回避策は、図 9 に示すように、ファイアウォール サービス機能を 2 つの「スタンドアロン」クラスタとして展開し、クラスタの各ノードを異なる VTEP ノードに接続することです。この場合、各スタンドアロン ファイアウォールおよびそれが接続しているローカル VTEP ノード間で、eBGP 接続をプロビジョニングすることが可能です（各ファイア ウォールノードは、異なる VTEP ノードのペアを指定します）。その結果、アクティブ ファイアウォール ノード（eBGP プロトコルをアクティブに実行している唯一のノード）は、ローカル VTEP ノードとリモート VTEP ノード（スタンバイ ファイア ウォール ノードが接続されている）の両方と eBGP 隣接関係を確立します。

次に、ファイアウォール サービス機能を「アクティブ/スタンバイ」クラスタとして展開する場合に、NDFC 12.2.2 で完全にサポートされる追加の代替展開オプションを示します。

- ファイアウォール ノードを異なる VTEP ノードに接続し（図 9 を参照）、ファイアウォール機能とファブリック間で eBGP の代わりにスタティック ルーティングを使用します。
- アクティブとスタンバイの両方のファイアウォール デバイスを同じ VTEP ノードのペアに接続します。これにより、アクティブなファイアウォール ノード（eBGP プロトコルをアクティブに実行している唯一のノード）は、ローカルに接続されている VTEP ノードとピアリングするだけで済みます。

1. **[サービス ノード名（Service Node Name）]** フィールドにサービス ノードのノード名を入力します。

   たとえば、FW-Node1などです。

2. **[+ サービスノードの物理接続の追加（+ Add Service Node Physical Connectivity）]** をクリックして、ノードをファブリックに物理的に接続する方法を定義します。

   [サービス ノード論理接続の追加（Add Service Node Physical Connectivity）] ウィンドウが表示されます。

3. **[サービス ノード接続の追加（Add Service Node Connectivity ）]** ウィンドウで、必要な情報を入力します。

フィールド	説明
サービスノード名	前の手順で入力したサービス ノード名が自動的に入力されます。
サービス ノード インターフェイス	サービス ノード インターフェイスを入力します。サービスノード インターフェイスは表示目的のものなので、サービス ノードの特定のインターフェイスの名前と厳密に一致させる必要はありません（操作上便利な場合もあります）。

サービス ノード インターフェイスの使用状況	サービス ノード インターフェイスの使用状況を選択します。 図 9 に示す特定の例では、各サービス ノードは単一の vPC 接続を使用してサービス リーフ ノードのペアに接続されます（異なる VLAN がその vPC にトランキングされ、サービス ネットワークと内部ネットワークに接続を提供します）。このため、**[サービス ノード インターフェイスの使用状況（Service Node Interface Usage）]** の **[内部/外部（Inside-Outside）]**オプションを選択します。代わりに、サービス ネットワークと内部ネットワークにそれぞれ接続を提供するために個別の物理インターフェイスを使用する場合は、内部サービス ノード インターフェイスと外部サービス ノード インターフェイスを個別に選択する必要があります。
アタッチされたスイッチ	サービス ノードがシングル接続かデュアル接続かに応じて、リストからスイッチまたはスイッチ ペアを選択します。
スイッチ インターフェイス	リストからインターフェイスを選択します。 ・**[アタッチされるスイッチ（Attached Leaf Switch）]** リストから vPC ペアを選択すると、それらのスイッチで定義された vPC のポートチャネルのリストが **[スイッチ インターフェイス（Interface）]** リストに表示されます。 ・それ以外の場合、トランク モードで構成されたポートチャネルおよびインターフェイスは、**[スイッチ インターフェイス（Switch Interface）]** リストに表示されます。
リンク テンプレート	指定されたアタッチ済みスイッチ インターフェイス タイプに基づき、ドロップダウン リストから service_link_trunk、service_link_port_channel_trunk、または the service_link_vpc を選択します。テンプレートフィールドの詳細については、レイヤ 4 ～ レイヤ 7 サービスの構成の「テンプレート」の項を参照してください。

4. [サービス ノード物理接続の追加（Add Service Node Physical Connectivity）] ウィンドウに必要な情報を入力したら、[保存（Save）] をクリックします。

   [サービス ノードの追加（Add Service NoswCluster）] ウィンドウに戻ります。

5. 前の手順を繰り返して別のサービス ノード インターフェイスを追加か、**[サービス ノードの 追加（Add Service Node）]** ウィンドウで **[保存（Save）]** をクリックしてサービスノード情報を保存します。

   [サービス クラスタの追加（Add Service Cluster）] ウィンドウに戻ります。

6. **[+ サービスノードの追加（+ Add Service Node）]**をクリックし、このセクションの手順を繰り返して、このユースケースの 2 番目のサービスノード（FW-Node2）を追加します。

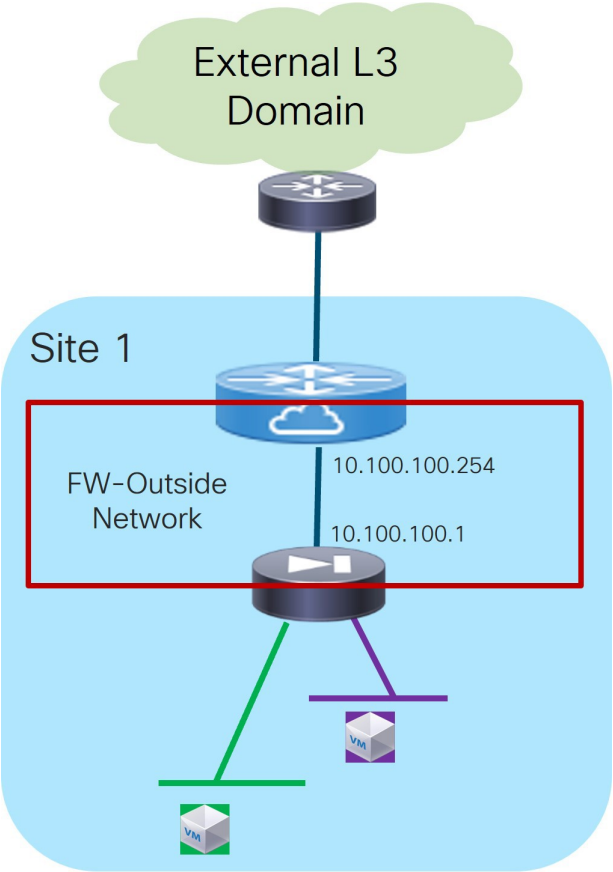
   FW-Node2 サービス ノードを追加する手順を完了すると、**[サービス クラスタの追加（Add Service Cluster）]** ウィンドウの **[サービス ノード（Service Nodes）]** エリアに FW-Node1 と FW-Node2 の情報が表示されます。

7. **[サービスクラスタの追加（Add Service Cluster）]** ウィンドウで [**保存（Save）**] をクリックして、サービス機能情報を保存します。

   [サービス クラスタの論理接続の追加（Add Service Cluster Logical Connectivity）] ウィンドウに戻ります。4b に進みます。サービスクラスタの論理接続を追加して、サービスクラスタの論理接続の構成を完了します。

4b. サービス ネットワークの作成

これらのユースケースの手順のこの時点までで、構成済みのサービス クラスタを選択するか、新しいサービス クラスタを構成しました。サービス クラスタの論理接続を追加するプロセスを続けるために必要な情報を入力します。そのために、ファブリックの VRF およびエンドポイントのレイヤ 2 ネットワークとサービス機能をピアリングするためのサービス ネットワークとして使用されるネットワークを選択または作成する必要があります。



デフォルト ゲートウェイとしてのサービス機能：サービス クラスタの論理接続の追加

1. **[IPv4/IPv6（IPv4/IPv6）]** フィールドで、次のオプションから選択します：
   - IPv4
   - IPv6
   - IPv4 および IPv6

   この例では、**IPv4 を**選択します。

2. サービス クラスタの論理接続を追加するプロセスを続けるために必要な情報を入力します。

   通常、このウィンドウの残りのフィールドは、選択した接続モードに応じて変わります。このユースケースでは、**N アーム**を接続モードとして選択したので、以下のフィールドが表示されます：

フィールド	説明
外部サービス IPv4	ファイアウォールの外部 IPv4 または IPv6（あるいはその両方）のサービス アドレスを入力します。これは、サービス リーフ ノードが（静的に、

外部サービス IPv6	または eBGP 経由で）L3 接続を確立する IP アドレスです。 たとえば、このセクションの最初に示したこのユースケースの構成例の図では、このフィールドに 10.100.100.1 と入力します。
サービス ネットワーク外	このサービス機能に関連付ける既存の外部サービス ネットワークを選択するか、**[+サービス ネットワークの追加（+Add Service ネットワーク）]** をクリックして新しい外部サービス ネットワークを作成します。詳細については、LAN 動作モードセットアップのファブリック概要 の「ネットワーク」セクションを参照してください。 新しいサービスネットワークを作成する場合、このセクションの最初に示したこのユースケースの構成例では、**[IPv4 エニーキャストゲートウェイ/ネットマスク（IPv4 Anycast Gateway/Netmask）]** フィールドに 10.100.100.254/24 と入力します。このケースでは、この値は、**[サービス クラスタ論理接続の追加（Add Service Cluster Logical Connectivity）]** ウィンドウの **[外部サービスネットワーク（Outside Service Network）]** エリアの **[ゲートウェイ IP（Gateway IP）]** フィールドに表示されます。
プローブ	デフォルト ゲートウェイとしてのサービスのユースケースでは、プローブを使用する必要はありません。
ピアリング オプション	適切なピアリング オプションを選択して、ファイアウォール ノードをサービス ネットワーク上のファブリックにピアリングする方法を定義します。以前に行った構成によっては、一部のピアリング オプションが使用できない場合があることに注意してください。 ・スタティック ・eBGP ・[接続済み（Connected）]：すでにルーティングが設定されている場合は、通常このピアリングオプションを選択します。ただし、このユースケースでは、スタティックまたは eBGP ピアリングのいずれかを構成することになります。
ピアリング設定	このサービス機能に関連付ける適切なピアリング構成を選択するか、**[+ピアリング構成の追加（+Add Peering Configuration）]** をクリックして新しいピアリング構成を作成します。 このユースケースでは、次のいずれかの項に進み、静的ピアリングまたは eBGP ピアリングを設定します。 ・4c. スタティックピアリング ・4c. eBGP ピアリング

4c. スタティックピアリング

1. **[ピアリング構成の追加（Add Peering Configuration）]** ウィンドウで、**[ピアリング名（Peering Name）]** フィールドに名前を入力します。
2. **[ピアリングテンプレート（Peering Template）]** フィールドで、service_static_route を選択します（このオプションは、前のセクションの **[ピアリング設定（Peering Configuration ）]** フィールドでの **[静的ピアリング（Static Peering ）]** の選択に基づいて事前に選択されています）。
3. 静的ピアリング ルートを設定するために必要な情報を入力します。

フィールド	説明
スタティック ルート	**[静的ルート（Static Routes）]** フィールドにスタティック ルートを入力します。回線ごとに1つのスタティックルートを入力できます。 たとえば、**[静的ルート（Static Routes）]** フィールドに次の値を入力するとします： `172.16.0.0/16, 10.100.100.1` ・172.16.0.0/16 は、ファイアウォールの背後にあるすべてのレイヤ 2 ネットワークを要約したものです（ファイアウォールをデフォルト ゲートウェイとして使用）。 ・10.100.100.1 は、ファイアウォールの外部 IPv4 サービス アドレスに対してこれらの手順で前に入力した値です。
エクスポート ゲートウェイ IP	ゲートウェイ IP（サービス ノード IP）アドレスをネクストホップ アドレスとしてエクスポートするには、クリックします。 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 ノードが異なるリーフ デバイスに接続されている場合、ファイアウォールの背後にあるネットワークに送られるトラフィックが、アクティブなファイアウォールが接続されているリーフ ノードに向かって常にカプセル化されるよう、このオプションを有効にする必要があります。VXLAN EVPN ファブリックにサービス機能を統合する場合のエクスポート ゲートウェイ IP の使用の詳細については、Cisco VXLAN マルチサイトおよび サービス ノード統合ホワイトペーパーを参照してください。

4. **[ピアリング構成の追加（Add Peering Configuration）]** ウィンドウに必要な情報をすべて入力したら、**[保存（Save）]** をクリックします。ウィンドウに追加してください。

   [サービス クラスタの論理接続の追加（Add Service Cluster Logical Connectivity）] ウィンドウに戻ります。

5. **[サービス クラスタ論理接続の追加（Add Service Cluster Logical Connectivity）]** ウィンドウに必要な情報を入力したら、**[保存（Save）]** をクリックします。

   [サービス挿入の追加（Add Service Insertion）] ウィンドウに戻ります。2b に進みます。内部 ネットワークを作成/選択します。

4c. eBGP ピアリング

1. **[ピアリング設定の追加（Add Peering Configuration）]** ウィンドウで、**[ピアリング名（Peering Name）]** フィールドに名前を入力します。
2. [ピアリングテンプレート（Peering Template）] フィールドで、service_ebgp_route を選択します（このオプションは、前のセクションの **[ピアリング構成（Peering Configuration ）]** フィールドでの **eBGP ピアリング** の選択に基づいて事前に選択されています）。

3. eBGP ピアリング ルートを構成するために必要な情報を入力します。

フィールド	説明
一般的なパラメータ	
サービス ノード ASN	サービス ノードの BGP ASN を指定します。
サービス ノード の IP アドレス	IPv4 アドレスまたはネットマスク付きアドレスを指定します（たとえば、1.2.3.4 または 1.2.3.1/24）。IPv4 または IPv6 アドレスは必須です。このフィールドには、ステップ 4b の一部として構成された IP アドレスが事前に入力されます。
VTEP ごとに VRF ごとに自動作成されたものを活用 ループバック	VTEP ループバック IP アドレスごとに VRF ごとに自動的に作成された を使用するには、このボックスをオンにします。**[Per VRF Per VTEP Loopback IPv4/IPv6 Auto-Provisioning]** オプションがファブリック構成で有効になっている場合にのみ適用されます。
ループバックIP	スイッチのループバックの IPv4アドレスを指定します。ループバック IPv4 または IPv6 アドレスは必須です。 特にこのユースケースでは、これはアクティブなファイアウォール ノードがピアリングしているサービスリーフ スイッチの IP アドレスです。
vPC ピアのループバック IP	ピア スイッチのループバックの IPv4アドレスを指定します。シリアル番号が小さいスイッチがこの値を使用します。これは、サービス ノードが同じ vPC ドメインの一部であるリーフ ノードのペアに物理的に接続されている場合にのみ必要です。 特にこのユースケースでは、これはアクティブなファイアウォールがピアリングしている 2 番目のサービスリーフ スイッチの IP アドレスです。
エクスポート ゲートウェイ IP	ゲートウェイ IP（サービス ノード IP）アドレスをネクストホップ アドレスとしてエクスポートするには、クリックします。 特にこのユースケースでは、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 ノードが異なるリーフ デバイスに接続されている場合、ファイアウォールの背後にあるネットワークに送られるトラフィックが、アクティブなファイアウォールが接続されているリーフ ノードに向かって常にカプセル化されるよう、このオプションを有効にする必要があります。 VXLAN EVPN ファブリックにサービス機能を統合する場合のエクスポート ゲートウェイ IP の使用の詳細については、Cisco VXLAN マルチサイトおよびサービス ノード統合 ホワイトペーパーを参照してください。
詳細	
サービス ノードの IPv6アドレス	IPv6 アドレスまたはネイバーのプレフィックスを持つアドレスを指定します。
ループバック IPv6	スイッチのループバックの IPv6 アドレスを指定します。
vPC ピアのループバック IPv6	ピア スイッチのループバックの IPv6アドレスを指定します。シリアル番号が小さいスイッチがこの値を使用します。これは、サービス ノードが同じ vPC ドメインの一部であるリーフ ノードのペアに物理的に接続されている場合にのみ必要です。
ルートマップ タグ	インターフェイスIDに関連付けられているルート マップ タグを指定します。

IPv 4インバウンド ルートマップ	IPv4インバウンド ルートマップを指定します。このフィールドを空白のままにすると、ルート マップは使用されません。
IPv4 アウトバウンド ルートマップ	IPv4 アウトバウンド ルートマップを指定します。このフィールドを空白のままにすると、システム は EXTCON-RMAP-FILTER、または EXTCON-RMAP-FILTER ALLOW-HOST を使用します（**[アドバタイズ ホスト ルート（Advertise Host Routes）]** オプションが有効になっている場合）。
IPv 6インバウンド ルートマップ	IPv6 インバウンド ルートマップを指定します。このフィールドを空白のままにすると、ルートマップは使用されません。
IPv6 アウトバウンド ルートマップ	IPv6 アウトバウンド ルートマップを指定します。このフィールドを空白のままにすると、システムは EXTCON-RMAP-FILTER-V6、または EXTCON-RMAP-FILTER-V6-ALLOW-HOST を使用します（**[ホスト ルートのアドバタイズ （Advertise Host Routes）]** オプションが有効になっている場合）。
インターフェイスの説明	インターフェイスの説明を入力します。
ローカルASN	システム ASN を上書きするローカル ASN を指定します。
アドバタイズ ホスト ルート	エッジルータへの/ 32および/ 128ルートのアドバタイズメントを有効にします。
eBGP パスワードの有効化	eBGP パスワードを有効にするには、このオプションを選択します。 このオプションを有効にすると、次の **[ファブリック構成から eBGP パスワードを継承（Inherit eBGP Password from Fabric Settings ）]** フィールドが自動的に有効になります。
ファブリック構成からの eBGP パスワードの継承	**[ファブリック設定（FabriSettings）]** から eBGPパスワードを継承するには、このオプションを選択します。 このオプションを有効にすると、次の [eBGP パスワード（eBGP Password）] および [eBGP 認証キー暗号化タイプ（eBGP Authentication Key Encryption Type）] フィールドは自動的に無効になります。
eBGP Password	**上記のファブリック構成から [eBGP パスワードを継承（Inherit eBGP Password from Fabric Settings ）]** フィールドを有効にしなかった場合に、有効になります。 有効になっている場合、暗号化された eBGP パスワードの 16 進文字列を指定します。
eBGP 認証キー暗号化タイプ	**上記のファブリック構成から [eBGP パスワードを継承（Inherit eBGP Password from Fabric Settings ）]** フィールドを有効にしなかった場合に、有効になります。 有効になっている場合は、BGP キー暗号化タイプを入力します。 ・**3**：3DES ・**7**: Cisco

[Enable Interface]	インターフェイスを無効にするには、このオプションをクリアします。デフォルトでは、インターフェイスは有効になっています。
vPC	
vPC ピア リンクビアのピアリング	vPC ピア リンクを介して per-VRF ピアリングを構成するには、このボックスをオンにします。 この特定のユースケースでは、サービスノードが vPC モードでリーフノードにデュアル接続されている場合（ファブリック レベルで vPC advertise-pip オプションを有効にした場合を除き）この**[vPC Peer-Link を介したピアリング （Peering via vPC Peer- Link）]** オプションを有効にする必要があります。 このタブの残りのフィールドは、**有効になる場合にのみ利用**可能になります。
送信元 IP アドレス/ネットマスク	送信元 IP アドレス と ネットマスクを指定 し ます。たとえば、192.168.10.1/30 です。
宛先 IP アドレス	接続先（BGP ネイバー）の IP アドレスを指定します。たとえば、192.168.10.2 などです。シリアル番号が小さいスイッチがこの値を使用します。
送信元 IPv6 アドレス/プレフィックス	送信 元 IPv6 アドレス と ネットマスクを指定します。たとえば、2001:db9::1/120です。
宛先 IPv6 アドレス	接続先 IPv6 アドレスを指定します。たとえば、2001:db9::10 です。シリアル番号が小さいスイッチがこの値を使用します。
vPC ピア間のピアリング用の VLAN	**vPC 間の VLAN ピアリングの値を入力します（最小：2、最大：4094）。このフィールドに値が指定されていない場合、VLAN ID は** 、ファブリック設定画面の [vPC] タブの [vPC ピア リンク VLAN 範囲（vPC Peer Link VLAN Range）] フィールドに**表示される VLAN プールから自動的に割り当てられます。**

4. **[ピアリング構成の追加（Add Peering Configuration）]** ウィンドウに必要な情報をすべて入力したら、**[保存（Save）]** をクリックします。
   ウィンドウに追加してください。

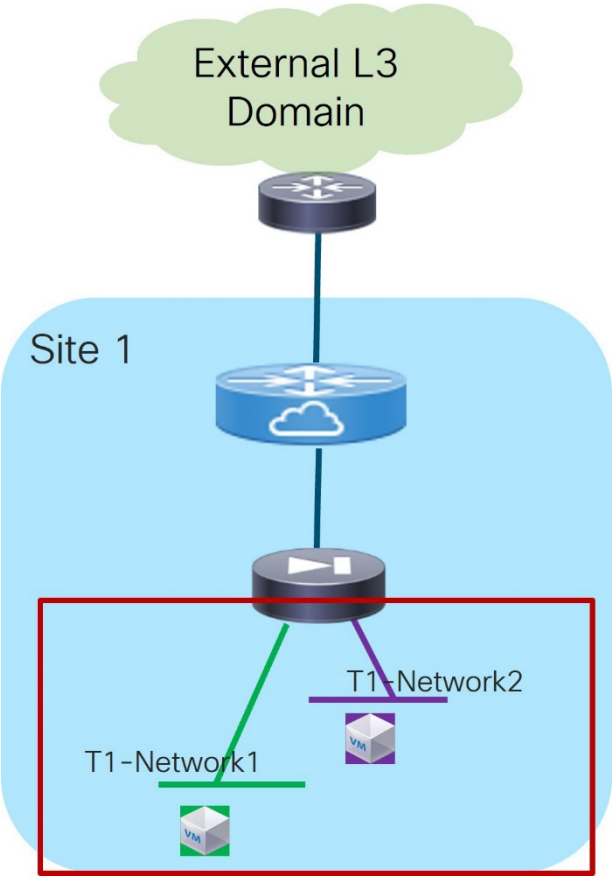
   [サービス クラスタの論理接続の追加（Add Service Cluster Logical Connectivity）] ウィンドウに戻ります。

5. **[サービス クラスタ論理接続の追加（Add Service Cluster Logical Connectivity）]** ウィンドウに必要な情報を入力したら、**[保存（Save）]** をクリックします。

   [サービス挿入の追加（Add Service Insertion）] ウィンドウに戻ります。2b に進みます。内部 ネットワークの作成/選択

2b. 内部ネットワークの作成/選択

次の手順を続行して、内部レイヤ 2 ネットワークを作成または選択します。これらのネットワークに接続されているエンドポイントは、デフォルト ゲートウェイとしてサービス機能を使用しています。



デフォルト ゲートウェイとしてのサービス機能：レイヤ 2 ネットワーク内

1. **[L2 ネットワーク内（Inside L2 Network）]** エリアで、**[+L2 ネットワークの追加（+Add L2 Network）]** をクリックし、このサービス挿入のユースケースに関連付ける既存のレイヤ 2 ネットワークを選択するか、**[ネットワークの作成（Create Network）]** をクリックして新しいレイヤ 2 ネットワークを作成します。詳細については、LAN 動作モード 構成のファブリックの概要の「ネットワーク」セクションを参照してください。

   このユースケースでは、サービスデバイスがデフォルトゲートウェイであるため、**[レイヤ 2 のみ（Layer 2 Only）]** オプションが事前に選択されています。

2. 内部 レイヤ 2 ネットワークの構成が完了したら、行の末尾にあるチェックマークをクリックして、入力した値を受け入れます。

   必要に応じて、これらの手順を繰り返して、追加の内部 L2 ネットワークを構成します。

3. この使用例でサービス挿入を追加するために必要な情報を入力したら、**[保存（Save）]** をクリックします。

   [ファブリックの概要（Fabric Overview）] ページに戻ります。**[サービス（Services）] > [サービス挿入（Service Insertions）]** が選択されています。

ユースケースのアタッチと展開

1. 新しいサービスの挿入の横にあるボックスをオンにし（まだ行っていない場合）、下部（白色）の **[アクション（Actions ）]** ドロップダウンをクリックし、**[アタッチ（Attach）]**を選択します。

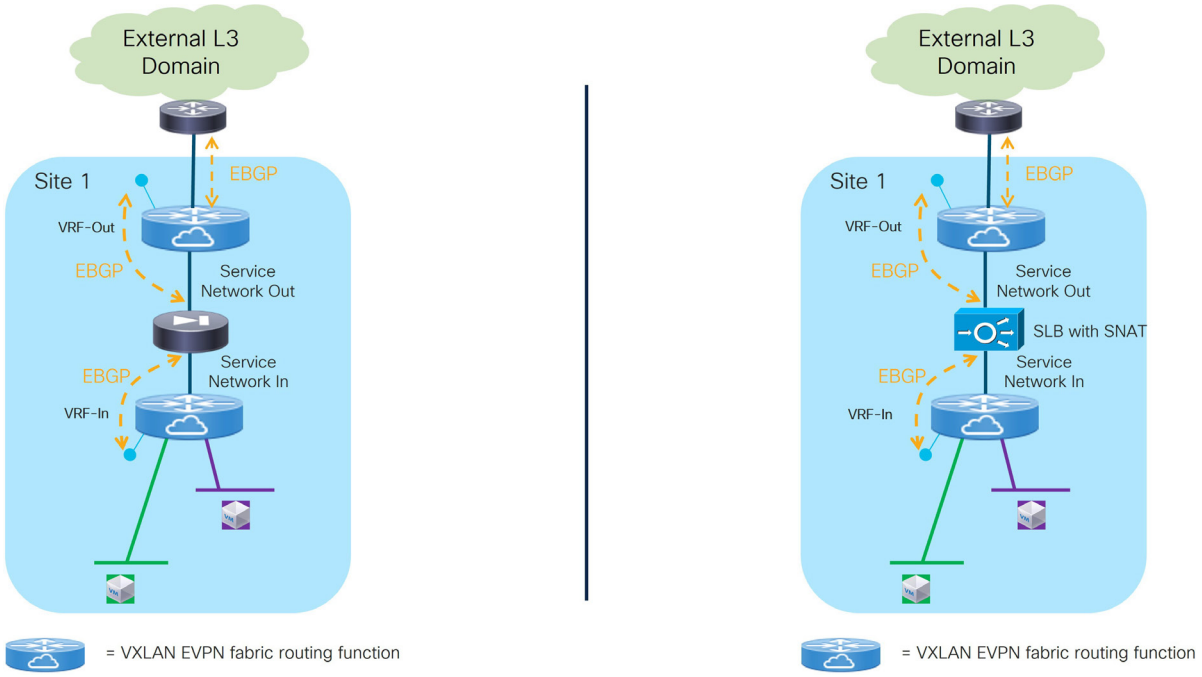
   数秒後に、**[アタッチ（Attached）]** 列に表示されている値が **[True]**に変わります。

2. 上部（青色）の **[アクション（Actions ）]** ドロップダウンをクリックし、**[再計算して展開（Recalculate and Deploy）]** を選択します。

   これで、新しい構成がサービス リーフ ノードに展開されました。

ユースケース 2：境界デバイスとしてのサービス機能

境界デバイスとしてのサービス機能のユースケースの論理ビューについては、次の図を参照してください。図にはファイアウォールとロード バランサの機能が示されていますが、このユースケースは一般的なサービス機能に適用できます。



境界デバイスとしてのサービス機能：論理ビュー

このユースケースでは、サービス機能がファブリックに展開された特定の「内部 VRF」に対するフロントエンドとなります。このようにして、この VRF のエンドポイント部分から開始され、他の VRF のエンドポイントまたは外部レイヤ 3 ネットワーク ドメインに向かうすべてのトラフィック フローは、サービス機能を介して誘導され、特定の役割を実行できます。

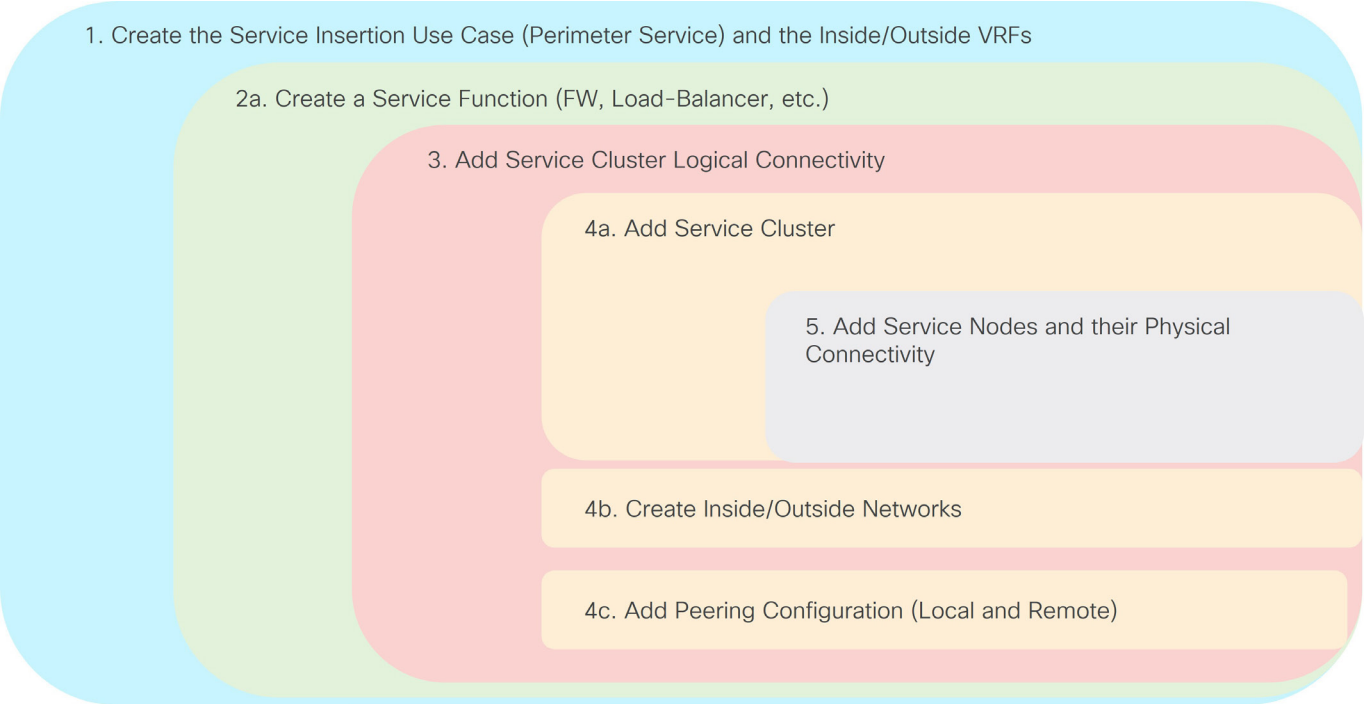
サービス機能は「2 アームモード」で展開されます。

- 最初のアームは、ファブリックに展開された「内部 VRF」とのピアリングを可能にします。このピアリングでは、静的ルーティングを活用すること、または EBGP をコントロール プレーンとして使用することができます。
- 一方、2 番目のアームは、ファブリックに展開されている「外部 VRF」とのピアリングに使用されます。またこの場合、静的ルーティングを利用すること、または EBGP をコントロール プレーンとして使用することができます。

> このセクションで説明する特定のサービス挿入のユースケースでは、サービス機能がファブリックで定義された 2 つの VRF を使用してサウスバウンドとノースバウンドをピアリングするように強制します。ただし、サービス機能が外部ルータでノースバウンドに直接的または間接的にピアリングできるシナリオ があります。1 アーム境界で説明されているとおりです。このドキュメントの最後にあるファイアウォールのセクションを参照してください。

サービス機能を境界デバイスのユースケースとして構成するためのワークフローのグラフィカル表現については、次の図を参照してください。

次の図に示すプロビジョニング手順については、以降のセクションで詳しく説明します。各セクションに関連付けられた番号は、図の対応するステップとマッチしています。ワークフローはこれらのステップ間を前後に移動するため、セクションの番号付けは必ずしも順序どおりにはなっていません。



境界デバイスとしてのサービス機能：ワークフロー

1. サービス挿入のユースケース（境界サービス）の選択

1. **[サービス インスタンス（Service Instance）]** タブに移動します。
   a. 次の順に選択：

      [管理（Manage）] > [ファブリック（Fabrics）]

   b. 適切な Data Center VXLAN EVPN ファブリックをダブルクリックします。

      ファブリックの**[概要（Overview）]** ウィンドウが表示されます。

   c. **[サービス（Services）]** タブをクリックします。
   d. **[サービス挿入（Service Insertions）]** サブタブをクリックします。

      構成されているサービス挿入のユースケースのリストが表示されます。

2. **[アクション（Actions）] > [サービス挿入の追加（Add Service Insertion）]** をクリックします。

   [サービス挿入の追加（Add Service Insertion）] ウィンドウが表示されます。

3. **[サービス挿入の名前（Service Insertion Name）]** フィールドに、サービスの名前を入力します。

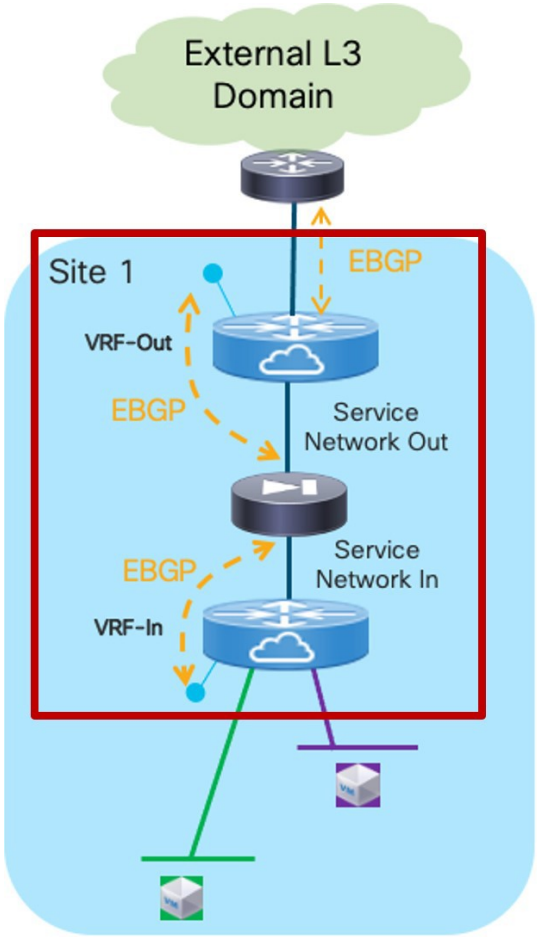
   名前にはアルファベット、数字、アンダースコア、または文字を含めることができます。たとえば、この特定のユースケースでは、サービス挿入名として FW-as-Perimeter を使用できます。

4. **[ユースケース（Use Case）]** フィールドで、適切なユースケースを選択します。

   このユースケースでは、ユースケースとして**境界サービス**を選択します。

5. 外部 VRF と内部 VRF を選択または作成します。

   これらは、サービス機能がピアリングするファブリック内の VRF です。



境界デバイスとしてのサービス機能：外部および内部 VRF

   a. **[外部 VRF 名（Outside VRF Name）]** フィールドで、このサービス挿入のユースケースに関連付ける既存の外部 VRF を選択するか、**[+VRF の作成（+Create VRF）]** をクリックして新しい VRF を作成します。

   b. **[内部 VRF 名（Outside VRF Name）]** フィールドで、このサービス挿入のユースケースに関連付ける既存の内部 VRF を選択するか、**[+VRF の作成（+Create VRF）]** をクリックして新しい VRF を作成します。

   詳細については、LAN 動作モード セットアップのためのファブリックの概要の「VRF」セクションを参照してください。

6. **[デタッチ/アタッチ（Detach/Attach）]** フィールドで、スイッチを切り替えて切り離しまたは接続します。

   特定のサービス挿入ワークフローの最後にスイッチに構成をプロビジョニングできるようにするには、**[アタッチ（Attach）]**オプションを選択する必要があります。**[アタッチ（Attach）]** オプションは、この時点で、または構成設定ワークフローのすべての手順を完了した後の手順の最後に選択できます。

7. **[サービス機能（Service Function）]** フィールドで、このサービス挿入使用例に関連付ける既存のサービス機能を選択するか、**[+サービス機能の作成（+Create Service Function）]** をクリックして新しいサービス機能を作成します。
   - 推奨されるアプローチは、**[+サービス機能の作成 （+Create Service Function）]** をクリックして新しいサービス機能を作成することです。サービス機能のオプション（1 アーム、2 アームなど）が、プロビジョニングされる特定のサービス挿入ワークフローに基づいて自動的に提案され、適切であることが保証されるからです。**[+サービス機能の作成（+Create Service Function）]**をクリックした場合は、2 に進みます。サービス機能を追加します。
   - このユースケースで既存の構成済みサービス機能を選択した場合、**[ユースケース （Use Case）]** フィールドで **[境界サービス（Perimeter Service）]** を選択したはずなので、サービス機能のプルダウン リストには、ステップ 5 で指定する外部と内部の VRF など、特定の設定オプションを持つサービス機能が事前に入力されます。次の項に進みます。「3. サービス クラスタの論理接続を追加します」。

2. サービス機能の追加

1. **[タイプ（Type）]**フィールドで、展開するサービス機能のタイプを選択します。

   このユースケースでは、展開するサービス機能のタイプとして **ファイアウォールを**選択します。

2. **[サービス機能名（Service Function Name）]** フィールドに、サービス機能の名前を入力します。

   名前にはアルファベット、数字、アンダースコア、または文字を含めることができます。

3. 次の 2 つのフィールドの情報を確認します。

   次の 3 つのフィールドは、すでに入力した情報に基づいて自動的に入力されます。

   - **[接続モード（Connectivity Mode）]**： ステップ 1 で選択した、サービス挿入のユースケースに基づいて、**2 アーム**が自動的に選択されます。
   - **[外部 VRF（Outside VRF）]**：1 の **[外部 VRF 名（Outside VRF Name）]** フィールド に指定したエントリに基づいて自動的に入力されます。[サービス挿入ユースケース (境界サービス) (Service Insertion Use Case (Perimeter Service))] を選択します。
   - **[内部 VRF（Inside VRF）]**：1 の **[内部 VRF 名（Inside VRF Name）]** フィールド に指定したエントリに基づいて自動的に入力されます。[サービス挿入ユースケース (境界サービス) (Service Insertion Use Case (Perimeter Service))] を選択します。

4. **[+ サービス クラスタ論理接続の追加（+ Add Service Cluster Logical Connectivity）]** をクリックします。

   [サービス クラスタ論理接続の追加（Add Service Cluster Logical Connectivity）] ウィンドウが表示されます。3 に進みます。サービス クラスタの 論理接続を追加します。

3. サービス クラスタの論理接続の追加

1. **[サービス クラスタ名（Service Cluster Name）]** フィールドで、構成済みのサービス クラスタを選択するか、**[+サービス クラスタの追加（+Add Service Cluster）]** をクリックして新しいクラスタを作成します。

- **[+ サービス クラスタの追加（+Add Service Cluster）]**をクリックした場合は、4a に進みます。サービス クラスタを追加します。
- このユースケースで既存の構成済みサービス クラスタを選択する場合は、4b に進みます。内部/外部ネットワークを作成します。

4a. サービス クラスタの追加

1. **[タイプ（Type）]** フィールドの情報を確認します。

   2a のステップ 1 で選択したサービス挿入のユースケースに基づいて、**[タイプ（Type）]** フィールドが自動的に入力されます。サービス機能を追加します。

2. サービス クラスタを追加するために必要な情報を入力します。

フィールド	説明
サービスクラスタ名	サービス クラスタの名前を入力します。名前にはアルファベット、数字、アンダースコア、または文字を含めることができます。
ノードの冗長性	ノードの冗長性を選択します。 ・**[スタンドアロン（Standalone）]**：次の手順で単一のサービス ノードを追加する場合に適用されます。 ・**[アクティブ/スタンバイ クラスタ（Active/Standby Cluster）]**：次の手順で 2 つのサービス ノードを追加し、同じアクティブ/スタンバイ クラスタの一部にする場合に適用されます。 ・**[アクティブ/アクティブ クラスタ（Active/Standby Cluster）]**：次の手順で 2 つ以上のサービス ノードを追加し、単一のアクティブ/アクティブ クラスタの一部にする場合に適用されます。
フォーム ファクタ	**[物理（Physical）]** または **[仮想（Virtual）]** を選択します。

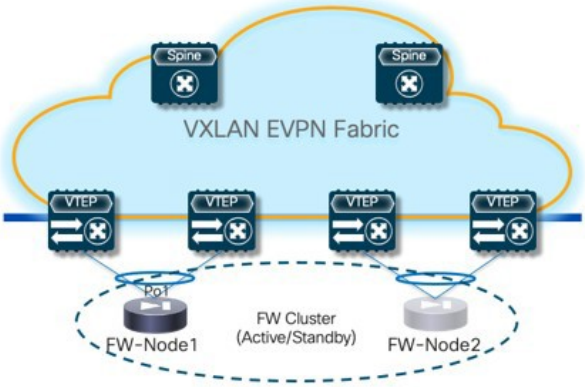
3. **[+ サービスノードの追加（+ Add Service Node）]** をクリックします。

   [サービス ノードの追加（Add Services Node）] ウィンドウが表示されます。「5. サービスノードを追加して、クラスタのサービス ノード部分とファブリックへの物理接続を定義します。

5. サービスノードを追加

ここで説明する特定の例では、次の図に示すように、2 つのサービスノード（同じアクティブ/スタンバイ クラスタの一部である FW-Node1 と FW-Node2）を設定します。

> 必要に応じ、境界ファイアウォールとしてアクティブ/アクティブ クラスタを展開することもできます。



境界デバイスとしてのサービス機能：2 つのサービスノードの構成

上の図に示すように、クラスタのサービス ノード部分を異なるリーフ ノードのセットに接続して、サービス機能の復元力を高めることを推奨します。ただし、NDFC 12.2.2 では、ファイアウォール サービス機能の展開に「アクティブ/スタンバイ」クラスタ オプションを選択した場合、アクティブなファイアウォール デバイスとスタンバイ ファイアウォール デバイスが接続されているリモート VTEP ノード間の eBGP ピアリングのプロビジョニングは許可されません。

ファイアウォール フェールオーバー シナリオでトラフィックの停止を最小限に抑えるために、通常はこれらの eBGP 隣接関係を確立することを推奨します。

NDFC 12.2.2 で使用可能な回避策は、図 12 に示すように、ファイアウォール サービス機能を 2 つの「スタンドアロン」クラスタとして展開し、クラスタの各ノードを異なる VTEP ノードに接続することです。この場合、各スタンドアロン ファイアウォールおよびそれが接続しているローカル VTEP ノード間で、eBGP 接続をプロビジョニングすることが可能です（各ファイア ウォールノードは、異なる VTEP ノードのペアを指定します）。その結果、アクティブ ファイアウォール ノード（eBGP プロトコルをアクティブに実行している唯一のノード）は、ローカル VTEP ノードとリモート VTEP ノード（スタンバイ ファイア ウォール ノードが接続されている）の両方と eBGP 隣接関係を確立します。

次に、ファイアウォール サービス機能を「アクティブ/スタンバイ」クラスタとして展開する場合に、NDFC 12.2.2 で完全にサポートされる追加の代替展開オプションを示します。

- ファイアウォール ノードを異なる VTEP ノードに接続し（図 12 を参照）、ファイアウォール機能とファブリック間で eBGP の代わりにスタティック ルーティングを使用します。
- アクティブとスタンバイの両方のファイアウォール デバイスを同じ VTEP ノードのペアに接続します。これにより、アクティブなファイアウォール ノード（eBGP プロトコルをアクティブに実行している唯一のノード）は、ローカルに接続されている VTEP ノードとピアリングするだけで済みます。

1. **[サービス ノード名（Service Node Name）]** フィールドにサービス ノードのノード名を入力します。

   たとえば、FW-Node1などです。

2. **[+ サービスノードの物理接続の追加（+ Add Service Node Physical Connectivity）]** をクリックして、ノードをファブリックに物理的に接続する方法を定義します。

[サービス ノード論理接続の追加（Add Service Node Physical Connectivity）] ウィンドウが表示されます。

3. **[サービス ノード接続の追加（Add Service Node Connectivity ）]** ウィンドウで、必要な情報を入力します。

フィールド	説明
サービスノード名	前の手順で入力したサービス ノード名が自動的に入力されます。
サービス ノード インターフェイス	サービス ノード インターフェイスを入力します。サービスノード インターフェイスは表示目的のものなので、サービス ノードの特定のインターフェイスの名前と厳密に一致させる必要はありません（操作上便利な場合もあります）。
サービス ノード インターフェイスの使用状況	サービス ノード インターフェイスの使用状況を選択します。 図 15 に示す特定の例では、各サービス ノードは単一の vPC 接続を使用してサービス リーフ ノードのペアに接続されます（異なる VLAN がその vPC にトランキングされ、外部サービス ネットワークと内部サービス ネットワークに接続を提供します）。このため、**[サービス ノード インターフェイスの使用状況（Service Node Interface Usage）]** の **[内部/外部（Inside-Outside）]**オプションを選択します。代わりに、外部サービス ネットワークと内部サービス ネットワークにそれぞれ接続を提供するために個別の物理インターフェイスを使用する場合は、内部サービス ノード インターフェイスと外部サービス ノード インターフェイスを個別に選択する必要があります。
アタッチされたスイッチ	サービス ノードがシングル接続かデュアル接続かに応じて、リストからスイッチまたはスイッチ ペアを選択します。
スイッチ インターフェイス	リストからインターフェイスを選択します。 ・**[アタッチされるスイッチ（Attached Leaf Switch）]** リストから vPC ペアを選択すると、それらのスイッチで定義された vPC のポートチャネルのリストが **[スイッチ インターフェイス（Interface）]** リストに表示されます。 ・それ以外の場合、トランク モードで構成されたポートチャネルおよびインターフェイスは、**[スイッチ インターフェイス（Switch Interface）]** リストに表示されます。
リンク テンプレート	指定されたアタッチ済みスイッチ インターフェイス タイプに基づき、ドロップダウン リストから service_link_trunk、service_link_port_channel_trunk、または the service_link_vpc を選択します。テンプレートフィールドの詳細については、レイヤ 4 ～ レイヤ 7 サービスの構成の「テンプレート」の項を参照してください。

4. [サービス ノード物理接続の追加（Add Service Node Physical Connectivity）] ウィンドウに必要な情報を入力したら、[保存（Save）] をクリックします。

   [サービス ノードの追加（Add Service NoswCluster）] ウィンドウに戻ります。

5. 前の手順を繰り返して別のサービス ノード インターフェイスを追加か、**[サービス ノードの 追加（Add Service Node）]** ウィンドウで **[保存（Save）]** をクリックしてサービスノード情報を保存します。

[サービス クラスタの追加（Add Service Cluster）] ウィンドウに戻ります。

6. **[+ サービスノードの追加（+ Add Service Node）]**をクリックし、このセクションの手順を繰り返して、このユースケースの 2 番目のサービスノード（FW-Node2）を追加します。

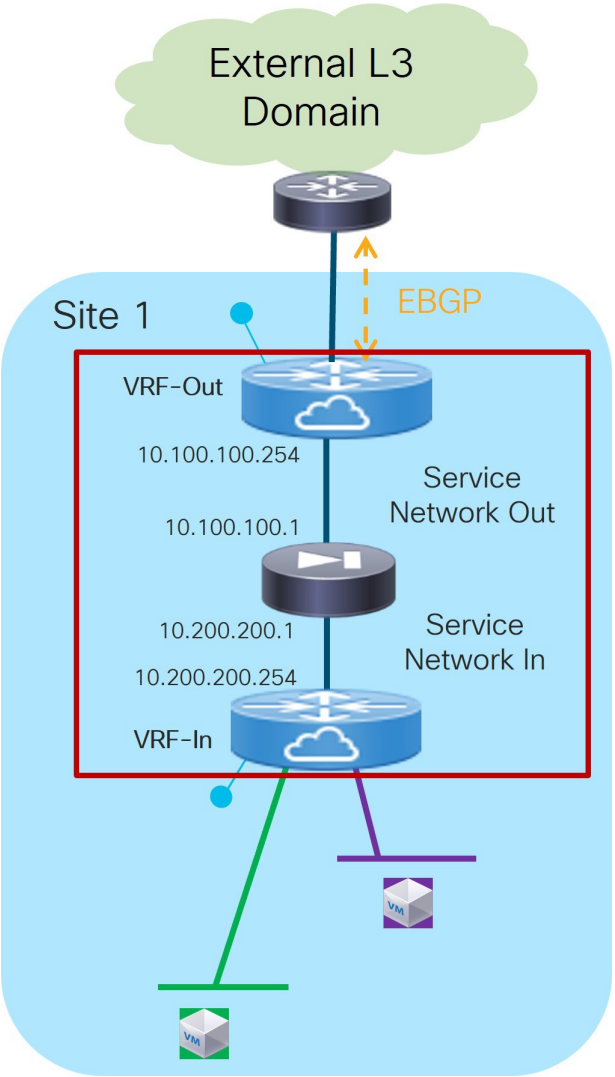
   FW-Node2 サービス ノードを追加する手順を完了すると、**[サービス クラスタの追加（Add Service Cluster）]** ウィンドウの **[サービス ノード（Service Nodes）]** エリアに FW-Node1 と FW-Node2 の情報が表示されます。

7. **[サービスクラスタの追加（Add Service Cluster）]** ウィンドウで **[保存（Save）]** をクリックして、サービス機能情報を保存します。

   [サービス クラスタの論理接続の追加（Add Service Cluster Logical Connectivity）] ウィンドウに戻ります。4b に進みます。内部/外部ネットワーク を作成して、サービスクラスタの論理接続構成を完了します。

4b. 内部/外部ネットワークの作成

これらのユースケースの手順のこの時点までで、構成済みのサービス クラスタを選択するか、新しいサービス クラスタを構成しました。サービス クラスタの論理接続を追加するプロセスを続けるために必要な情報を入力します。そのために、ファブリックの 内部および外部 VRF のサービス機能をピアリングするために使用されるネットワークを選択または作成する必要があります。



境界デバイスとしてのサービス機能：サービス クラスタの論理接続

1. **[IPv4/IPv6（IPv4/IPv6）]** フィールドで、次のオプションから選択します：
   - IPv4
   - IPv6
   - IPv4 および IPv6

   この例では、**IPv4** を選択します。

2. サービス クラスタの論理接続を追加するプロセスを続けるために必要な情報を入力します。

   通常、このウィンドウの残りのフィールドは、選択した接続モードに応じて変わります。ただし、このユースケースで選択したサービス挿入のユースケースに基づいて **[2 アーム（Two Arms）]** が自動的に選択されたため、次のフィールドが表示されます。

フィールド	説明
外部サービス IPv4	ファイアウォールの外部 IPv4 または IPv6（あるいはその両方）のサービス アドレスを入力します。これは、サービス リーフ ノードが（静的に、または eBGP 経由で）L3 接続を確立する IP アドレスです。 たとえば、このセクションの最初に示したこのユースケースの構成例の図では、このフィールドに 10.100.100.1 と入力します。
外部サービス IPv6	
サービス ネットワーク外	このサービス機能に関連付ける既存の外部サービス ネットワークを選択するか、**[+サービス ネットワークの追加（+Add Service ネットワーク）]** をクリックして新しい外部サービス ネットワークを作成します。詳細については、LAN 動作モードセットアップのファブリック概要 の「ネットワーク」セクションを参照してください。 新しいサービスネットワークを作成する場合、このセクションの最初に示したこのユースケースの構成例では、**[IPv4 エニーキャストゲートウェイ/ネットマスク（IPv4 Anycast Gateway/Netmask）]** フィールドに 10.100.100.254/24 と入力します。このケースでは、この値は 、**[サービス クラスタ論理接続の追加（Add Service Cluster Logical Connectivity）]** ウィンドウの **[外部サービスネットワーク（Outside Service Network）]** エリアの **[ゲートウェイ IP（Gateway IP）]** フィールドに表示されます。
ピアリング オプション	このサービス機能に関連付ける適切なピアリング オプションを選択します。以前に行った構成によっては、一部のピアリング オプションが使用できない場合があることに注意してください。 ・スタティック ・eBGP ・[接続済み（Connected）]：すでにルーティングが設定されている場合は、通常このピアリングオプションを選択します。ただし、このユースケースでは、ローカルまたはリモート eBGP ピアリングのいずれかを構成することになります。
ピアリング設定	このサービス機能に関連付ける適切なピアリング構成を選択するか、**[+ピアリング構成の追加（+Add Peering Configuration）]** をクリックして新しいピアリング構成を作成します。詳細については、LAN 動作モード セットアップのファブリックの概要についての「サービス機能テンプレート」セクションを参照してください。

	このユースケースでは、ピアリング設定オプションに **[eBGP]** を選択します。4c を参照してください。詳細については、ローカル eBGP ピアリングを参照してください。
内部サービス IPv4 内部サービス IPv6	ファイアウォールの内部 IPv4 または IPv6（あるいはその両方）のサービス アドレスを入力します。 たとえば、このセクションの最初に示したこのユースケースの構成例の図では、このフィールドに 10.200.200.1 と入力します。
内部サービスネットワーク	このサービス機能に関連付ける既存の内部サービス ネットワークを選択するか、**[+サービス ネットワークの追加（+Add Service Network）]** をクリックして新しいサービス ネットワークを作成します。詳細については、LAN 動作モード セットアップのファブリックの概要について の「ネットワーク」セクションを参照してください。 新しいサービスネットワークを作成する場合、このセクションの最初に示したこのユースケースの構成例では、**[IPv4 エニーキャストゲートウェイ/ネットマスク（IPv4 Anycast Gateway/Netmask）]** フィールドに 10.200.200.254/24 と入力します。このケースでは、この値は 、**[サービス クラスタ論理接続の追加（Add Service Cluster Logical Connectivity）]** ウィンドウの **[内部サービスネットワーク（Inside Service Network）]** エリアの **[ゲートウェイ IP（Gateway IP）]** フィールドに表示されます。
ピアリング オプション	このサービス機能に関連付ける適切なピアリング オプションを選択します。以前に行った構成によっては、一部のピアリング オプションが使用できない場合があることに注意してください。 ・スタティック ・eBGP ・[接続済み（Connected）]：すでに回送が構成されている場合は、このピアリング オプションを選択します。テナント内ファイアウォールには、ピアリング オプションとして **[接続済み（Connected）]** のみが表示されます。
ピアリング設定	このサービス機能に関連付ける適切なピアリング構成を選択するか、**[+ピアリング構成の追加（+Add Peering Configuration）]** をクリックして新しいピアリング構成を作成します。詳細については、LAN 動作モード セットアップのファブリックの概要についての「サービス機能テンプレート」セクションを参照してください。 このユースケースでは、ピアリング設定オプションに **[eBGP]** を選択します。4c に移動します。ローカル eBGP ピアリング。

4c. ローカル eBGP ピアリング

このユースケースでは、このセクションの情報を使用して、外部ネットワークと内部ネットワークの両方にローカル eBGP ピアリングを構成します。

1. **[ピアリング構成の追加（Add Peering Configuration）]** ウィンドウで、**[ピアリング名（Peering Name）]** フィールドに名前を入力します。
2. [ピアリングテンプレート（Peering Template）] フィールドで、service_ebgp_routeを選択します。

3. eBGP ピアリング ルートを構成するために必要な情報を入力します。

> 内部 VRF と外部 VRF の両方が同じファブリックで定義されているため、デフォルトではファブリックの BGP ASN を継承します。したがって、それらの間で（ファイアウォールを介して）プレフィックスを交換する場合 は、各 VRF で「local-AS」構成を使用して、すべてが一意の BGP ASNを公開するようにします。この設定には、**[詳細（Advanced）]** エリアでアクセスできます。

フィールド	説明
一般的なパラメータ	
サービス ノード ASN	サービス ノードの BGP ASN を指定します。
サービス　ノードの IP アドレス	IPv4 アドレスまたはネットマスク付きアドレスを指定します（たとえば、1.2.3.4 または 1.2.3.1/24）。IPv4 または IPv6 アドレスは必須です。このフィールドには、ステップ 4b の一部として構成された IP アドレスが事前に入力されます。
VTEP ごとに VRF ごとに自動作成されたものを活用 ループバック	VTEP ループバック IP アドレスごとに VRF ごとに自動的に作成された を使用するには、このボックスをオンにします。**[Per VRF Per VTEP Loopback IPv4/IPv6 Auto-Provisioning]** オプションがファブリック構成で有効になっている場合にのみ適用されます。
ループバックIP	スイッチのループバックの IPv4アドレスを指定します。ループバック IPv4 または IPv6 アドレスは必須です。 特にこのユースケースでは、これはアクティブなファイアウォール ノードがピアリングしているサービスリーフ スイッチの IP アドレスです。
vPC ピアのループバック IP	ピア スイッチのループバックの IPv4アドレスを指定します。シリアル番号が小さいスイッチがこの値を使用します。これは、サービス ノードが同じ vPC ドメインの一部であるリーフ ノードのペアに物理的に接続されている場合にのみ必要です。 特にこのユースケースでは、これはアクティブなファイアウォールがピアリングしている 2 番目のサービスリーフ スイッチの IP アドレスです。
エクスポート ゲートウェイ IP	ゲートウェイ IP（サービス ノード IP）アドレスをネクストホップ アドレスとしてエクスポートするには、クリックします。 特にこのユースケースでは、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 ノードが異なるリーフ デバイスに接続されている場合、ファイアウォールの背後にあるネットワークに送られるトラフィックが、アクティブなファイアウォールが接続されているリーフ ノードに向かって常にカプセル化されるよう、このオプションを有効にする必要があります。 VXLAN EVPN ファブリックにサービス機能を統合する場合のエクスポート ゲートウェイ IP の使用の詳細については、Cisco VXLAN マルチサイトおよびサービス ノード統合 ホワイトペーパーを参照してください。
詳細	
サービス　ノードの IPv6アドレス	IPv6 アドレスまたはネイバーのプレフィックスを持つアドレスを指定します。

ループバック IPv6	スイッチのループバックの IPv6 アドレスを指定します。
vPC ピアのループバック IPv6	ピア スイッチのループバックの IPv6アドレスを指定します。シリアル番号が小さいスイッチがこの値を使用します。これは、サービス ノードが同じ vPC ドメインの一部であるリーフ ノードのペアに物理的に接続されている場合にのみ必要です。
ルートマップ タグ	インターフェイスIDに関連付けられているルート マップ タグを指定します。
IPv 4インバウンド ルートマップ	IPv4インバウンド ルートマップを指定します。このフィールドを空白のままにすると、ルート マップは使用されません。
IPv4 アウトバウンド ルートマップ	IPv4 アウトバウンド ルートマップを指定します。このフィールドを空白のままにすると、システム は EXTCON-RMAP-FILTER、または EXTCON-RMAP-FILTER ALLOW-HOST を使用します（**[アドバタイズ ホスト ルート（Advertise Host Routes）]** オプションが有効になっている場合）。
IPv 6インバウンド ルートマップ	IPv6 インバウンド ルートマップを指定します。このフィールドを空白のままにすると、ルートマップは使用されません。
IPv6 アウトバウンド ルートマップ	IPv6 アウトバウンド ルートマップを指定します。このフィールドを空白のままにすると、システムは EXTCON-RMAP-FILTER-V6、または EXTCON-RMAP-FILTER-V6-ALLOW-HOST を使用します（**[ホスト ルートのアドバタイズ （Advertise Host Routes）]** オプションが有効になっている場合）。
インターフェイスの説明	インターフェイスの説明を入力します。
ローカルASN	システム ASN を上書きするローカル ASN を指定します。
アドバタイズ ホスト ルート	エッジルータへの/ 32および/ 128ルートのアドバタイズメントを有効にします。
eBGP パスワードの有効化	eBGP パスワードを有効にするには、このオプションを選択します。 このオプションを有効にすると、次の **[ファブリック構成から eBGP パスワードを継承（Inherit eBGP Password from Fabric Settings ）]** フィールドが自動的に有効になります。
ファブリック構成からの eBGP パスワードの継承	**[ファブリック設定（FabriSettings）]** から eBGPパスワードを継承するには、このオプションを選択します。 このオプションを有効にすると、次の [eBGP パスワード（eBGP Password）] および [eBGP 認証キー暗号化タイプ（eBGP Authentication Key Encryption Type）] フィールドは自動的に無効になります。
eBGP Password	**上記のファブリック構成から [eBGP パスワードを継承（Inherit eBGP Password from Fabric Settings ）]** フィールドを有効にしなかった場合に、有効になります。 有効になっている場合、暗号化された eBGP パスワードの 16 進文字列を指定します。

eBGP 認証キー暗号化タイプ	**上記のファブリック構成から [eBGP パスワードを継承（Inherit eBGP Password from Fabric Settings ）]** フィールドを有効にしなかった場合に、有効になります。 有効になっている場合は、BGP キー暗号化タイプを入力します。 ・**3**：3DES ・**7**: Cisco
[Enable Interface]	インターフェイスを無効にするには、このオプションをクリアします。デフォルトでは、インターフェイスは有効になっています。
vPC	
vPC ピア リンクビアのピアリング	vPC ピア リンクを介して per-VRF ピアリングを構成するには、このボックスをオンにします。 この特定のユースケースでは、サービスノードが vPC モードでリーフノードにデュアル接続されている場合（ファブリック レベルで vPC advertise-pip オプションを有効にした場合を除き）この**[vPC Peer-Link を介したピアリング （Peering via vPC Peer- Link）]** オプションを有効にする必要があります。 このタブの残りのフィールドは 、 **有効になる場合にのみ利用**可能になります。
送信元 IP アドレス/ネットマスク	送信元 IP アドレス と ネットマスクを指定 し ます。たとえば、192.168.10.1/30 です。
宛先 IP アドレス	接続先（BGP ネイバー）の IP アドレスを指定します。たとえば、192.168.10.2 などです。シリアル番号が小さいスイッチがこの値を使用します。
送信元 IPv6 アドレス/プレフィックス	送信 元 IPv6 アドレス と ネットマスクを指定します。たとえば、2001:db9::1/120です。
宛先 IPv6 アドレス	接続先 IPv6 アドレスを指定します。たとえば、2001:db9::10 です。シリアル番号が小さいスイッチがこの値を使用します。
vPC ピア間のピアリング用の VLAN	**vPC 間の VLAN ピアリングの値を入力します（最小：2、最大：4094）。このフィールドに値が指定されていない場合、VLAN ID は** 、ファブリック設定画面の [vPC] タブの [vPC ピア リンク VLAN 範囲（vPC Peer Link VLAN Range）] フィールドに**表示される VLAN プールから自動的に割り当てられます。**

4. **[ピアリング構成の追加（Add Peering Configuration）]** ウィンドウに必要な情報をすべて入力したら、**[保存（Save）]** をクリックします。
   ウィンドウに追加してください。

   [サービス クラスタの論理接続の追加（Add Service Cluster Logical Connectivity）] ウィンドウに戻ります。この時点で、リモート サービス リーフ ノードとも eBGP 隣接関係を確立する必要がある場合は、[4c リモート eBGP ピアリング] に進みます。それ以外の場合は、以下のステップ 5 に進みます。

5. **[サービス クラスタ論理接続の追加（Add Service Cluster Logical Connectivity）]** ウィンドウに必要な情報を入力したら、**[保存（Save）]** をクリックします。

   [サービス挿入の追加（Add Service Insertion）] ウィンドウに戻ります。2b に進みます。[内部 ネットワーク（Inside Networks）]を作成または選択します。

ユースケースのアタッチと展開

1. 新しいサービスの挿入の横にあるボックスをオンにし（まだ行っていない場合）、下部（白色）の **[アクション（Actions ）]** ドロップダウンをクリックし、**[アタッチ（Attach）]**を選択します。

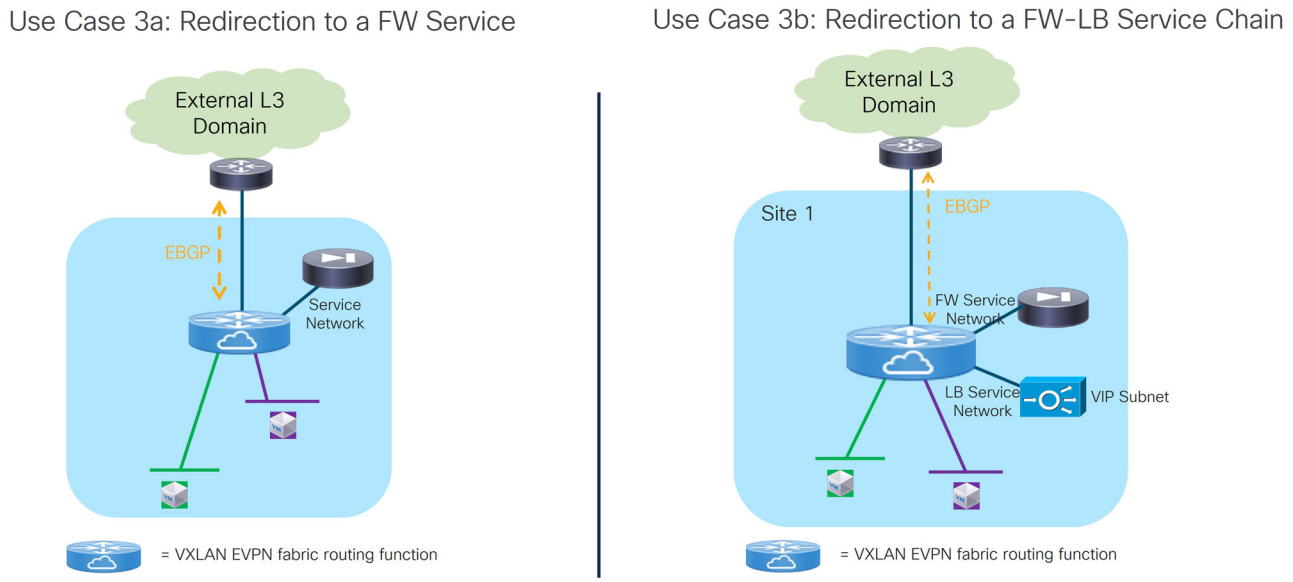
   数秒後に、**[アタッチ（Attached）]** 列に表示されている値が **[True]**に変わります。

2. 上部（青色）の **[アクション（Actions ）]** ドロップダウンをクリックし、[再 **計算して展開（Recalculate and Deploy）]**を選択します。

   これで、新しい構成がサービス リーフ ノードに展開されました。

ユースケース 3：サービス チェーンへのリダイレクト

サービス チェーンへのリダイレクトのユースケースの論理ビューについては、次の図を参照してください。図にはファイアウォールとロード バランサの機能が示されていますが、このユースケースは一般的なサービス機能に適用できます。



サービス チェーンへのリダイレクト：論理ビュー

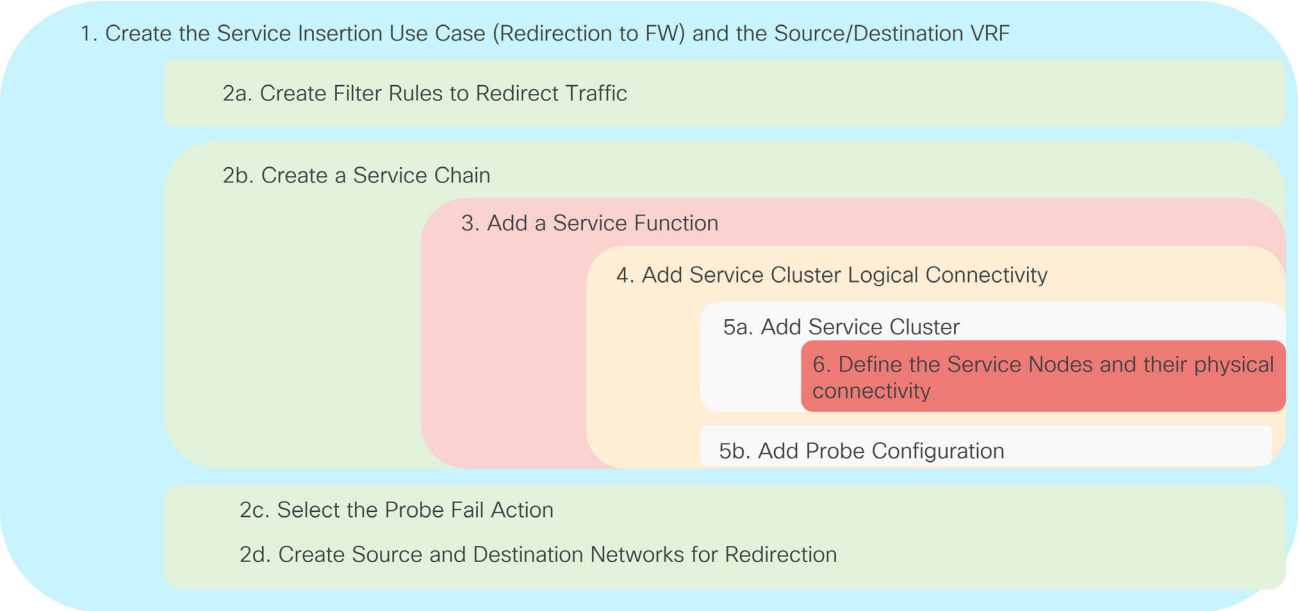
上の図で強調表示されているサービス機能は、「1 アームモード」で接続されています。これは、サービス ネットワークの IP アドレスを指すシンプルなデフォルトルートだけで十分であり、サービス機能のルーティング構成が簡素化されるため、ベストプラクティスの展開モデルです。

次のセクションでは、2 種類のサービス チェーンへのリダイレクトのユースケースについて詳しく説明します。

ユースケース 3a：ファイアウォール サービスへのリダイレクト

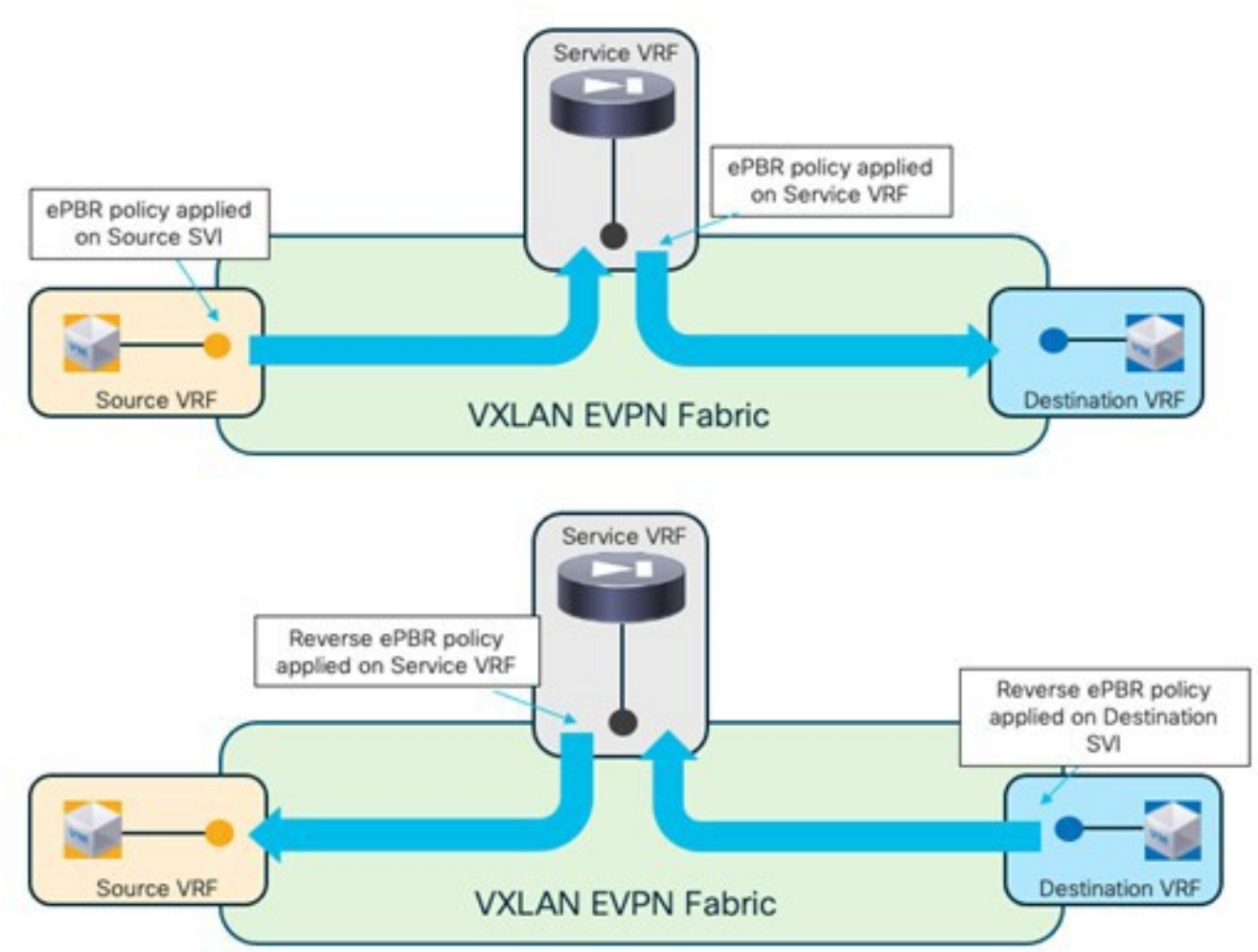
ファイアウォール サービスのユースケース（より一般的にはサービス機能）への双方向リダイレクトを構成するためのワークフローのグラフィカル表現については、次の図を参照してください。

> 次の図に示すプロビジョニング手順については、以降のセクションで詳しく説明します。各セクションに関連付けられた番号は、図の対応するステップにマッチしています。ワークフローはステップ間を前後に移動するため、セクションの番号付けは必ずしも、順番通りではありません。



ファイアウォール サービスへのリダイレクト：ワークフロー

次の図 19 に、送信元ネットワークと接続先ネットワーク間のフローに必要な、トラフィック リダイレクト機能の論理ビューを示します。以下の手順で説明するように、これらのネットワークは、イーストウェストまたは ノースサウスのトラフィック フローにサービス リダイレクトが必要かどうかに応じて、ファブリックの内部または外部になります。



ファイアウォール サービスへのリダイレクト：トラフィック フロー ステアリング

送信元ネットワークと接続先ネットワークは、同じ VRF の、または異なる VRF に属していることがあり得ます。ファイアウォール サービス機能は、専用のサービス VRF に展開する必要があります。

上の図に示すように、送信元ネットワークと接続先ネットワークのインターフェイスにサービス リダイレクト ポリシーを適用すると、トラフィックを正しいサービス VRF のサービス機能にリダイレクトできます（つまり、「set-VRF」機能が送信元/接続先 VRF で自動的に実行され、トラフィックフローをサービス VRF のファイアウォールに適切にリダイレクトします）。送信元/接続先 VRF で「set-VRF」を使用すると、ファイアウォール IP アドレスのルックアップが対応するサービス VRF で適切に実行され、必要な VRF 間接続が適切に確立されます。

代わりに、NDFC 12.2.2 で送信元/接続先ネットワーク ルートをサービス VRF にリークする場合には、明示的なユーザー主導の構成が必要です。これが必要なのは、「set-VRF」機能がサービス VRF レベルで適用される ePBR ポリシーに適用されないためです（この構成については、以下の特定の設定手順で説明します）。そのため、必要な VRF 間接続を確立するには、必要なテナントのルートをサービス VRF にリークしなければなりません。

1a. サービス挿入のユースケースの選択（サービス チェーンにリダイレクト）

1. **[サービス インスタンス（Service Instance）]** タブに移動します。
   a. 次の順に選択：

      [管理（Manage）] > [ファブリック（Fabrics）]

   b. 適切な Data Center VXLAN EVPN ファブリックをダブルクリックします。

      ファブリックの**[概要（Overview）]** ウィンドウが表示されます。

   c. **[サービス（Services）]** タブをクリックします。
   d. **[サービス挿入（Service Insertions）]** サブタブをクリックします。

      構成されているサービス挿入のユースケースのリストが表示されます。

2. **[アクション（Actions）] > [サービス挿入の追加（Add Service Insertion）]** をクリックします。

   [サービス挿入の追加（Add Service Insertion）] ウィンドウが表示されます。

3. **[サービス挿入の名前（Service Insertion Name）]** フィールドに、サービスの名前を入力します。

   名前にはアルファベット、数字、アンダースコア、または文字を含めることができます。たとえば、この特定のユースケースでは、Redirect-to-FW をサービス挿入名として使用できます。

4. **[ユースケース（Use Case）]** フィールドで、適切なユースケースを選択します。

   このユースケースでは、ユースケースとして **[サービス チェーンへのリダイレクト（Redirect to Service Chain）]** を選択します。

5. エンドポイントのサブネットを使用して VRF を選択するか、作成します。
   a. **[トラフィック送信元 VRF]** フィールドで、このサービス挿入のユースケースに関連付ける既存のトラフィック送信元VRF を選択するか、**[+VRF の作成（+Create VRF）]** をクリックして新しい VRF を作成します。

b. **[トラフィック接続先 VRF（Traffic Destination VRF）]** フィールドで、このサービス挿入のユースケースに関連付ける既存のトラフィック接続先 VRF を選択するか、**[+VRF の作成（+Create VRF）]** をクリックして新しい VRF を作成します。

詳細については、LAN 動作モード設定のファブリックの概要の「VRF」セクションを参照してください。

> この特定の例では、トラフィック送信元 VRF とトラフィック接続先 VRF の両方に同じテナント VRF（T1-VRF）を使用する必要があります。ただし 異なるテナント VRF の一部であるエンドポイント間（またはエンドポイントと外部ネットワーク間）のトラフィックのリダイレクト実行も サポートされています。サポートされていません。

6. **[デタッチ/アタッチ（Detach/Attach）]** フィールドで、スイッチを切り替えて切り離しまたは接続します。

   特定のサービス挿入ワークフローの最後にスイッチに構成をプロビジョニングできるようにするには、**[アタッチ（Attach）]**オプションを選択する必要があります。**[アタッチ（Attach）]** オプションは、この時点で、または構成設定ワークフローのすべての手順を完了した後の手順の最後に選択できますが、すべての手順の完了後に選択することを推奨します。

7. **[方向（Direction）]** フィールドで、このサービス挿入ユースケースの方向を選択します。

   オプションは、次のとおりです。
   - 双方向
   - 転送
   - 反転

   この特定の例では、選択した各トラフィック フローの両方のレッグをファイアウォールにリダイレクトすることを目的としているため、**[双方向（Bidirectional）]** を選択します。

8. このサービス挿入の **[統計の有効化（Enable Statistics）]** フィールドで、チェックボックスをオンにして、このサービス挿入ユースケースの統計を有効にします。

   統計情報を有効にすると、特定の ePBR ポリシーにマッチし、サービス機能にリダイレクトまたはサービス チェーン処理されたパケットの数が追跡されます。これらの統計情報は、後で時系列グラフの形式で視覚化して、トラフィック リダイレクト パターンを理解することもできます。

9. **[トラフィック フロー リダイレクト（Traffic Flow Redirects）]** エリアで、**[+トラフィックフローリダイレクトの追加（+Add Traffic Flow Redirect ）]** をクリックし、必要な情報を入力して、トラフィック フロー リダイレクトの作成をトリガーします。
10. **[ACL 名の照合（Match ACL Name）]**フィールドで、ドロップダウン リストから構成済みのアクセス制御リスト（ACL）を選択するか、**[+ACL の作成（+Create ACL）]** をクリックして新しいACLを作成します。

    このユースケースでは、**[+ACL の作成（+Create ACL）]** をクリックして新しいアクセス制御リストを作成します。2a に移動します。ACL 照合トラフィックを作成します。

2a. ACL 照合トラフィックの作成

ACL を作成して、後のセクションで定義するサービス機能にリダイレクトするべき特定のプロトコルを定義する必要があります。送信元ネットワークと接続先ネットワーク間のすべてのトラフィックをサービス機能にリダイレクトする必要がある最も単純なシナリオでは、ACL エントリについて、送信元ポートまたは接続先ポートを設定せずに、**[プロトコル（Protocol）]** フィールドに ip を指定するだけで済みます。

1. **[アクセス制御リスト名（Access Control List Name）]** フィールドに新しい ACL の名前を入力します。
2. **[アクセス リスト エントリ（Access List Entries）]** エリアで、**[+ アクセス リスト エントリの追加（+ Add Access List Entries）]**をクリックします。
3. 新しいアクセス制御リストを作成するために必要な情報を入力します。

フィールド	説明
シーケンス番号（Sequence Number)	ACL のシーケンス番号を入力します。有効な範囲は 1 ~ 4294967295 です。
プロトコル	ACL に使用するプロトコルを指定します。オプションは、次のとおりです。 ・icmp ・ip ・tcp ・udp
送信元 IP	ACL の送信元 IP アドレスを入力します。このエントリには、IPv4アドレス、IPv6アドレス、または any を指定できます。ファブリックの外部にあり、ボーダー リーフ ノードで設定されたレイヤ 3 ピアリングを介してファブリックに接続する送信元としてサブネットを指定する場合は、any を使用します。
宛先 IP	ACL の宛先 IP アドレスを入力します。このエントリには、IPv4アドレス、IPv6アドレス、または any を指定できます。ファブリックの外部にあり、ボーダー リーフ ノードで設定されたレイヤ 3 ピアリングを介してファブリックに接続する送信元としてサブネットを指定する場合は、any を使用します。
送信元ポート	送信元ポート番号を入力します（たとえば、*any* または *443*）。**[プロトコル（Protocol）]** フィールドで **ip** または **icmp** を選択した場合、このフィールドの値は無視されます。
宛先ポート	宛先ポート番号を入力します（たとえば、*any* または *443*）。**[プロトコル（Protocol）]** フィールドで **ip** または **icmp** を選択した場合、このフィールドの値は無視されます。

ファイアウォール機能へのリダイレクトの特定のシナリオでは、送信元ネットワークから接続先ネットワークに向かう（およびその逆の）トラフィックは、常にファイアウォールに誘導される必要があります。したがって、必要な ACL には、特定の送信元/接続先ネットワークとマッチするエントリが必要です（上記の表で説明したように、送信元ネットワークまたは接続ネットワークの各エントリで any を使用できます）。

4. アクセス制御コントロール リストのエントリを受け入れるには、チェックマークをクリックします。

   [サービス挿入を追加（Add Service Insertion）] ウィンドウに戻り、新しく作成したアクセス制御リストが **[ACL 名の照合（Match ACL Name）]** フィールドに表示されます。

5. **[照合アクション（Macth Action）]** フィールドで、適切な ACL 照合アクションを選択します。

   オプションは、次のとおりです。

   - [リダイレクト（Redirect）]：トラフィックを照合し、サービス チェーンにリダイレクトするためのデフォルト アクション。
   - [ドロップ（Drop）]：着信インターフェイスで特定のトラフィックを照合し、トラフィックをドロップします。
   - [除外（Exclude）]：着信インターフェイスのサービス チェーンから特定のトラフィックを除外します。

   サービス チェーンのサービス挿入 には 、1 つのドロップ と 1 つの 除外のみを含めること ができ ます。

6. **[サービス チェーン名（Service Chain Name）]** フィールドで、構成設定済みのサービス チェーンをドロップダウン リストから選択するか、**[+サービス チェーンの 作成（+Create Service Chain）]** をクリックして新しいサービス チェーンを作成します。

   このユースケースでは、**[+サービス チェーンの作成（+Create Service Chain）]** をクリックして、新しいサービス チェーンを作成します。2b に進みます。サービス チェーンを作成します（ファイアウォールのみ）。

2b. サービス チェーンの作成（ファイアウォールのみ）

このセクションで説明する特定の例では、単一のサービス機能（ファイアウォール）を含むシンプルなサービス チェーンを検討します。この記事の冒頭で説明した冗長性モデル（アクティブ/スタンバイ クラスタ、アクティブ/アクティブ クラスタ、一連のスタンドアロン ノードなど）は、ファイアウォール サービス機能の展開に使用できます。この例では、アクティブ/スタンバイ クラスタを検討します。

1. **[サービス チェーンの追加（Add Service Chain）]** ウィンドウで、**[サービス チェーン名（Service Chain Name）]** にサービス チェーンの名前を入力します。
   field.
2. **[+サービス チェーン エントリの追加（+Add Service Chain Entries）]** をクリックします。
3. サービス チェーン エントリに必要な情報を入力します。

フィールド	説明
シーケンス番号（Sequence Number）	シーケンス番号を入力します。シーケンス番号が小さいほど、プライオリティが高くなります。 ファイアウォール専用サービス チェーンの具体例では、ファイアウォール サービス機能に任意のシーケンス番号を選択できます。
サービスクラスタタイプ	サービス クラスタを選択します。このユースケースでは、**ファイアウォール VRF を選択します。**

VRF	このサービス チェーンに関連付ける既存の VRF を選択するか、**[+ VRF の作成（+ Create VRF）]** をクリックして新しい VRF を作成します。サービス チェーンの各サービス機能部分は、送信元および接続先ネットワークに使用される VRF とは異なる専用 VRF を使用する必要があります。チェーン内の単一のファイアウォール サービスの例では、単一のファイアウォール サービス VRF を使用できます。 単一のサービス機能へのファブリック内リダイレクトの特定のユースケースでは、送信元/接続先ネットワークの同じ VRF にサービス機能を展開することは技術的に実現可能であり、サポートされています。ただし異なる VRF を使用する必要がある場合複数のサービス機能がサービス チェーンの一部である場合またはマルチサイト展開でサービスリダイレクトをサポートする場合は、各サービス機能を常に独自の専用 VRF に展開することを推奨します。
サービス機能	このサービス チェーンに関連付ける既存のサービス機能を選択するか、**[+サービス機能の追加（+Add Service Function）]** をクリックして新しいサービス機能を追加します。 推奨されるアプローチは、**[+サービス機能の追加（+Add Service Function）]** をクリックして新しいサービス機能を作成することです。サービス機能のオプション（1 アーム、2 アームなど）が、プロビジョニングされる特定のサービス挿入のワークフローに基づいて自動的に提案され、適切であることが保証されるからです。 このユースケースでは、**[+サービス機能の追加（+Add Service Function）]** をクリックして新しいサービス機能を作成します。次の項に進みます。「3. サービス機能を追加します」。

3. サービス機能の追加

この例では、サービス チェーンにはファイアウォール サービス機能のみが含まれているため、以下の手順は 1 回だけ実行します。より複雑なサービス チェーンのシナリオでは、チェーンに含まれるサービス機能ごとに、以下で説明するのと同じワークフローを繰り返します。

1. **[タイプ（Type）]**フィールドで、展開するサービス機能のタイプを選択します。

   このユースケースでは、展開するサービス機能のタイプとして **ファイアウォールを**選択します。

2. **[サービス機能名（Service Function Name）]** フィールドに、サービス機能の名前を入力します。名

   前にはアルファベット、数字、アンダースコア、または文字を含めることができます。

3. **[接続モード（Connectivity Mode）]** フィールドで、**[1 アーム（One Arm）]** または **[2 アーム（Two Arms）]** を選択します。

   通常は **[1 アーム （One Arm）]** オプションを推奨します。サービス機能のルーティング構成を簡素化するためです（サービス ネットワークの IP アドレスを指すデフォルト ルートのみが必要です）。

4. **[サービス VRF（Service VRF]** フィールドで、サービス VRF を選択します。

- 作成するすべてのサービス機能に専用のサービス VRF が必要です。
- テナント VRF からサービス VRF へのルート リークを設定します。このルートリーク設定は、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 ノードが接続されているサービス リーフ ノードにのみ適用する必要があります。これは、サービス機能を通過し、ファブリックに送り返されるトラフィック フローが、特定のテナント VRF の接続先に向けられるようにするためです。

> 推奨されるアプローチは、ルートリーク構成を使用してフリーフォーム テンプレートを定義し、サービス リーフ ノードにのみテンプレートを適用することです。

次に、テナント VRF とサービス VRF 間のリーク ルートを許可する構成のシンプルな例を示します（この例で使用されるファブリックの BGP ASN は 65002 です）。

テナント VRF の構成：「route-target auto」は、route-target を BGP-ASN:L3VNI（65002:50001）として使用することを意味します。

```
vrf context t1-vrf1
  vni 50001
  rd auto
address-family ipv4 unicast
  route-target both auto route-
  target both auto evpn
address-family ipv6 unicast
  route-target both auto route-
  target both auto evpn
```

サービス（ファイアウォール）VRF の構成：特定の「import」ステートメントは、自動生成された RT 値によって識別されるテナント プレフィックスがサービス VRF ルーティング テーブルにインポートされるようにするためのものであることに注意してください。

```
vrf context t1-fw1-vrf1
 vni 50002
 rd auto
 address-family ipv4 unicast
   route-target both auto route-
   target both auto evpn
   route-target import 65002:50001
 route-target import 65002:50001 evpn
 address-family ipv6 unicast
   route-target both auto
   route-target both auto evpn
   route-target import 65002:50001 route-
   target import 65002:50001 evpn
```

5. **[+ サービス クラスタ論理接続の追加（+ Add Service Cluster Logical Connectivity）]** をクリックします。

[サービス クラスタ論理接続の追加（Add Service Cluster Logical Connectivity）] ウィンドウが表

示されます。4a に移動します。サービスクラスタの 論理接続を追加して、サービス機能の論理接続を構成します。

4a. サービス クラスタの論理接続の追加

1. **[サービス クラスタ名（Service Cluster Name）]** フィールドで、構成済みのサービス クラスタを選択するか、**[+サービス クラスタの追加（+Add Service Cluster）]** をクリックして新しいクラスタを作成します。

   サービス機能の論理接続を構成する前に、そのようなサービス機能を実装するサービス クラスタを定義する必要があります。

   - **[+ サービスクラスタの追加（+Add Service Cluster）]**をクリックした場合は、5a に進みます。サービス クラスタを追加します。
   - このユースケースで既存の構成済みのサービスクラスタを選択する場合は、4b に進みます。サービス クラスタの論理接続を追加します。

5a. サービス クラスタの追加

1. **[タイプ（Type）]** フィールドの情報を確認します。

   「サービス機能の追加」のステップ 1 で選択したサービス挿入のユースケースに基づいて、**[タイプ（Type）]** フィールドが自動的に入力されます。

2. サービス クラスタを追加するために必要な情報を入力します。

フィールド	説明
サービスクラスタ名	サービス クラスタの名前を入力します。名前にはアルファベット、数字、アンダースコア、または文字を含めることができます。
ノードの冗長性	ノードの冗長性を選択します。 ・**[スタンドアロン（Standalone）]**：次の手順で単一のサービス ノードを追加する場合に適用されます。 ・**[アクティブ/スタンバイ クラスタ（Active/Standby Cluster）]**：次の手順で 2 つのサービス ノードを追加し、同じアクティブ/スタンバイ クラスタの一部にする場合に適用されます。 ・**[アクティブ/アクティブ クラスタ（Active/Standby Cluster）]**：次の手順で 2 つ以上のサービス ノードを追加し、単一のアクティブ/アクティブ クラスタの一部にする場合に適用されます。
フォーム ファクタ	**[物理（Physical）]** または **[仮想（Virtual）]** を選択します。

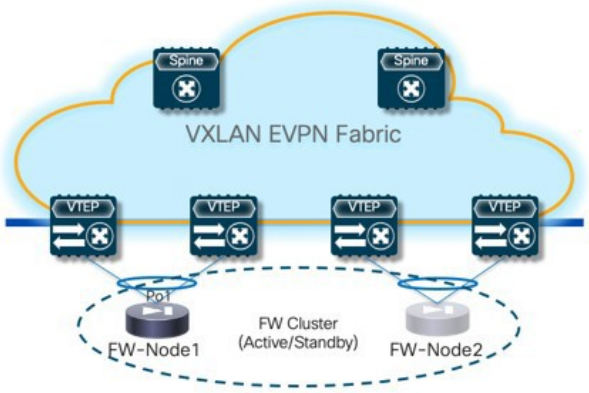
3. **[+ サービスノードの追加（+ Add Service Node）]** をクリックします。

   [サービス ノードの追加（Add Services Node）] ウィンドウが表示されます。6 に移動します。サービスノードを追加して、クラスタのサービス ノード部分とファブリックへの物理接続を定義します。

6. サービスノードを追加

ここで説明する特定の例では、次の図に示すように、2 つのサービスノード（同じアクティブ/スタンバイクラスタの一部である FW-Node1 と FW-Node2）を設定します。

> 前述のように、サービス機能の展開には、アクティブ/アクティブ クラスタまたはスタンドアロン ノードのセットを使用することもできます。



サービス チェーンへのリダイレクト：2 つのサービス ノードの構成

1. **[サービス ノード名（Service Node Name）]** フィールドにサービス ノードのノード名を入力します。

   たとえば、FW-Node1などです。

2. **[+ サービスノードの物理接続の追加（+ Add Service Node Physical Connectivity）]** をクリックして、ノードをファブリックに物理的に接続する方法を定義します。

   [サービス ノード論理接続の追加（Add Service Node Physical Connectivity）] ウィンドウが表示されます。

3. **[サービス ノード接続の追加（Add Service Node Connectivity ）]** ウィンドウで、必要な情報を入力します。

フィールド	説明
サービスノード名	前の手順で入力したサービス ノード名が自動的に入力されます。
サービス ノード インターフェイス	サービス ノード インターフェイスを入力します。サービスノード インターフェイスは表示目的のものなので、サービス ノードの特定のインターフェイスの名前と厳密に一致させる必要はありません（操作上便利な場合もあります）。

サービス ノード インターフェイスの使用状況	サービス ノード インターフェイスの使用状況を選択します。 図 20 に示す特定の例では、各サービス ノードは単一の vPC 接続を使用してサービス リーフ ノードのペアに接続されます（異なる VLAN がその vPC にトランキングされ、サービス ネットワークと内部ネットワークに接続を提供します）。このため、**[サービス ノード インターフェイスの使用状況（Service Node Interface Usage）]** の **[内部/外部（Inside-Outside）]**オプションを選択します。代わりに、サービス ネットワークと内部ネットワークにそれぞれ接続を提供するために個別の物理インターフェイスを使用する場合は、内部サービス ノード インターフェイスと外部サービス ノード インターフェイスを個別に選択する必要があります。
アタッチされたスイッチ	サービス ノードがシングル接続かデュアル接続かに応じて、リストからスイッチまたはスイッチ ペアを選択します。
スイッチ インターフェイス	リストからインターフェイスを選択します。 ・**[アタッチされるスイッチ（Attached Leaf Switch）]** リストから vPC ペアを選択すると、それらのスイッチで定義された vPC のポートチャネルのリストが **[スイッチ インターフェイス（Interface）]** リストに表示されます。 ・それ以外の場合、トランク モードで構成されたポートチャネルおよびインターフェイスは、**[スイッチ インターフェイス（Switch Interface）]** リストに表示されます。
リンク テンプレート	指定されたアタッチ済みスイッチ インターフェイス タイプに基づき、ドロップダウン リストから service_link_trunk 、service_link_port_channel_trunk、または the service_link_vpc を選択します。テンプレートフィールドの詳細については、レイヤ 4 ~ レイヤ 7 サービスの構成の「テンプレート」の項を参照してください。

4. [サービス ノード物理接続の追加（Add Service Node Physical Connectivity）] ウィンドウに必要な情報を入力したら、[保存（Save）] をクリックします。

   [サービス ノードの追加（Add Service NoswCluster）] ウィンドウに戻ります。

5. 前の手順を繰り返して別のサービス ノード インターフェイスを追加か、**[サービス ノードの 追加（Add Service Node）]** ウィンドウで **[保存（Save）]** をクリックしてサービスノード情報を保存します。

   [サービス クラスタの追加（Add Service Cluster）] ウィンドウに戻ります。

6. **[+ サービスノードの追加（+ Add Service Node）]**をクリックし、このセクションの手順を繰り返して、このユースケースの 2 番目のサービスノード（FW-Node2）を追加します。

   FW-Node2 サービス ノードを追加する手順を完了すると、**[サービス クラスタの追加（Add Service Cluster）]** ウィンドウの **[サービス ノード（Service Nodes）]** エリアに FW-Node1 と FW-Node2 の情報が表示されます。

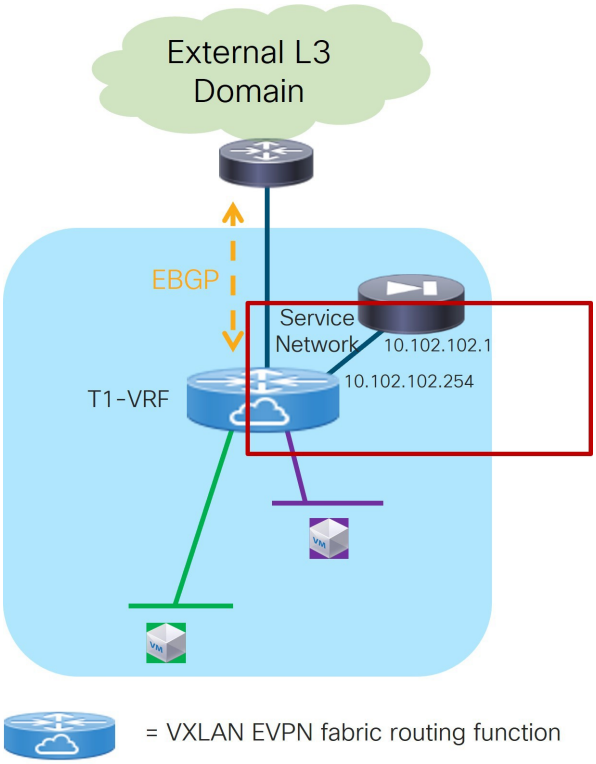
7. **[サービスクラスタの追加（Add Service Cluster）]** ウィンドウで [**保存（Save）**] をクリックして、サービス機能情報を保存します。

   [サービス クラスタの論理接続の追加（Add Service Cluster Logical Connectivity）] ウィンドウに戻ります。4b に進みます。サービスクラスタの論理接続を追加して、サービスクラスタの論理接続の構成を完了します。

4b. サービス クラスタの論理接続の追加

これらのユースケースの手順のこの時点までで、構成済みのサービス クラスタを選択するか、新しいサービス クラスタを構成しました。サービス クラスタの論理接続を追加するプロセスを続けるために必要な情報を入力します。

図 21 に示すように、ファイアウォール サービス機能は、サービス ネットワークを使用して 1 アーム モードでファブリックに接続されます。これはエニーキャスト ゲートウェイ アドレスが構成された L2VNI セグメントで表されます。ファブリックとファイアウォールの間にルーティング ピアリング（静的または eBGP）を確立する必要はありません。トラフィックのリダイレクトは、サービス ネットワークの一部である（ファブリックに直接接続され、EVPN ファブリックのコントロールプレーンに再配布される）ファイアウォールの IP アドレスに適用されるからです。



サービス チェーンへのリダイレクト：サービスクラスタの論理接続

1. **[IPv4/IPv6（IPv4/IPv6）]** フィールドで、次のオプションから選択します：
   - IPv4
   - IPv6
   - IPv4 および IPv6

   この例では、**IPv4** を選択します。
2. サービス クラスタの論理接続を追加するプロセスを続けるために必要な情報を入力します。

   このウィンドウの残りのフィールドは、選択した接続モードに応じて変わります。この例では、このユースケースで選択したサービス挿入のユースケースに基づいて **[2 アーム（Two Arms）]** が自動的に選択された場合、次のフィールドが表示されます。

フィールド	説明
Service IPv4	ファイアウォールの IPv4 または IPv6（あるいはその両方）のサービス ア

Service IPv6	ドレスを入力します。 たとえば、このセクションの最初に示したこのユースケースの構成例の図では、このフィールドに 10.102.102.1 と入力します。
サービスネットワーク	このサービス機能に関連付ける既存のサービス ネットワークを選択するか、**[+サービス ネットワークの 追加（+Add Service ネットワーク ）]** をクリックして新しいサービス ネットワークを作成します。詳細については、LAN 動作モード セットアップのファブリックの概要について の「ネットワーク」セクションを参照してください。 新しいサービス ネットワークを作成する場合、このセクションの最初に示したこのユースケースの構成例では、**[IPv4 エニーキャストゲートウェイ/ネットマスク（IPv4 Anycast Gateway/Netmask）]** フィールドに 10.102.102.254/24 と入力します。この場合、この値は 、**[サービスクラスタ論理接続の追加（Add Service Cluster Logical Connectivity）]** ウィンドウの **[サービス ネットワーク（Service Network）]** エリアの **[ゲートウェイIP（Gateway IP）]**フィールドに表示されます。
プローブ	このサービス機能に関連付ける既存のプローブをクリックするか、または **[+プローブの追加（+Add Probe）] をクリックして** 、新しいプローブを作成します。 このユースケースでは、**[+プローブの追加（+Add Probe）]** をクリックしてプローブ構成を追加します。5b に移動します。プローブ構成を追加します。

5b. プローブ設定の追加

1. **[プローブ構成の追加（Add Probe Configuration）]** ウィンドウで、**[プローブ名（Probe Name）]** フィールドに名前を入力します。
2. **[プローブ テンプレート（Probe Template）]** フィールドで、**service_endpoint** を選択します。
3. プローブを構成するために必要な情報を入力します：

フィールド	**説明**
一般的なパラメータ	
プローブの有効化	ネクスト ホップ アドレスのプローブを有効にするには、このボックスをオンにします。 プローブは、ファブリック内のすべてのリーフ ノードから実行されます。プローブに使用される送信元インターフェイスは、サービス VRF の各リーフ ノードで定義されたループバック インターフェイスです。これらのループバックのプロビジョニングは、そのファブリックの **[リソース（Resources）]** にある **[VRF ごと、VTEP ごとの IPv4ループバック オートプロビジョニング（Per VRF Per VTEP Loopback IPv4 Auto-Provisioning）]** および **[VRF ごと、VTEP ごとの IPv6 ループバック オートプロビジョニング（Per VRF Per VTEP Loopback IPv6 Auto-Provisioning）]** フィールドを設定するために必須です。詳細については、データセンター VXLAN EVPN を参照してください。

		上記の **[VRF ごと、VTEP ごとのループバック（Per VRF Per VTEP Loopback）]** オプションを有効にすると、ローカルに定義されているすべての VRF の各 VTEP にループバック アドレスが割り当てられます。これらのループバック アドレスに割り当てられる IP アドレスは、ファブリック レベルで指定されたグローバル プールから取得されます。NDFC 12.2.2 リリースでは、重複する IP アドレスを、異なる VRF の異なる VTE に割り当てられたループバックアドレスに割り当てることが許可されています。そのため、VRF リークがテナント VRF と Service-FW および Service-LB VRF の間で構成された場合、問題が生じることがあります。したがって、これらのループバック アドレスを手動で割り当て（ファブリック内の各 VTEP の VRF レベルで実行できます）、定義された VRF 内および定義された VRF 全体で一意であることを確認することを強く推奨します。
プロトコル	プローブに使用するプロトコルを指定します。オプションは、次のとおりです。 ・icmp ・tcp ・udp ・http	
ポート番号	プロトコルが tcp または udp の場合にのみ、入力に対して表示されます。プローブのポート番号を入力します。有効な範囲：1 ~ 65535（推奨範囲：1025 ~ 65534）。	
HTTP プローブのユーザー入力	プロトコルが http の場合にのみ、入力用に表示されます。HTTPプローブのユーザー入力テキスト/ファイル名を入力します（例：http://192.168.50.254/index.html）。最大サイズ：99	
詳細		
しきい値	しきい値（秒）を入力します。有効な範囲：1 ~ 60	
周波数	周波数の値を秒単位で入力します。有効な範囲：1 ~ 604800。	
遅延ダウン変更履歴	遅延ダウン変更通告値を秒単位で入力します。有効な範囲は1 ~ 180	
遅延アップ変更履歴	遅延アップ変更通告値を秒単位で入力します。有効な範囲：1 ~ 180。	
タイムアウト（Timeout）	タイムアウト値を秒単位で入力します。有効な範囲：1 ~ 604800。	

サービスリダイレクトのプローブ設定の詳細については、NX-OS 構成ガイドを参照してください。

4. 4c に進みます。サービス クラスタの論理接続を追加します。

4c. サービス クラスタの論理接続の追加

1. **[ピアリング オプション（Peering Option）]** フィールドで、このサービス機能に関連付ける適切なピアリング オプションを選択します。

このユースケースでは、ピアリング オプションとして **[接続済み （Connected）]** を選択します。先ほど定義した FW-Service-Network に接続されているファイアウォールの IP アドレスにリダイレクトされるからです。

2. 2c に進みます。適切なプローブ失敗時のアクションを選択します。

2c. プローブ失敗時のアクションの選択

1. **[サービス チェーンの追加（Add Service Chain）]** ウィンドウの **[プローブ失敗アクション（Probe Fail Action）]** フィールドで、適切なプローブ失敗アクションを選択します。

   オプションは、次のとおりです。

   - **[転送（Forward）]** : トラフィックが通常のルーティングテーブルを使用するデフォルトのオプションです。
   - **[ドロップ（Drop）]** : サービスが到達不能になると、トラフィックをドロップします。
   - **[バイパス（Bypass）]** : 現在のシーケンスで障害が発生した場合に、トラフィックを次のサービス シーケンスにリダイレクトします。
   - **なし**

2. チェックマークをクリックして、サービス チェーン エントリの値を受け入れます。

   [サービス挿入の追加（Add Service Insertion）] ウィンドウに戻ります。2d に進みます。送信元 および接続先ネットワークを作成/選択します。

2d. 送信元および接続先ネットワークの作成/選択

ステップ 2a で作成したアクセス制御リストの結果として、ステップ 1a で設定した送信元および接続先 VRF にマッチする送信元および接続先ネットワーク部分が、**[ネットワーク（Networks）]** エリアに事前入力されます。これらのエントリは、ePBR ポリシーを適用する必要があるインターフェイスを NDFC に示すために必要です。通常、これらのエントリを変更する必要はありません。ただし、送信元または接続先ネットワークが any キーワードを用いて構成されている場合は例外です（any を同じエントリの送信元および接続先ネットワークの両方で使用するのは不可能であることに注意してください）。

送信元または接続先ネットワークとして any を使用することは、ファブリックの外部にあるプレフィックスを指定する意図を表します。送信元として any を使用するルールは、フローの送信元が外部ネットワーク ドメインに接続されているクライアントであることを意味します。逆に、接続先として any を使用するルールは、フローの接続先がファブリックの外部にあるクライアントであることを意味します。外部ネットワーク ドメインは境界リーフ ノードを介して到達可能である必要があるため、UI では、送信元（または接続先）の any ネットワークで外部ドメインへの接続に使用される、境界リーフ ノードのインターフェイスを指定する必要があります。

1. [ネットワーク（Networks）] エリアで、[+行の追加（+Add Row）] をクリックし、必要な情報を入力します。

フィールド	説明
送信元ネットワーク	選択した ACL または新しく作成した ACL の ACL エントリに基づいて、送信送信元ネットワーク フィールドと接続先ネットワーク フィールドが自動的に入力されます。システムが自動入力した送信元ネットワークまたは接続先ネットワーク、あるいはその両方を上書きできます。
宛先ネットワーク（Destination Network)	システムが自動入力した送信元ネットワークまたは接続先ネットワーク、あるいはその両方を上書きする場合は、ドロップダウン リストから構成済みの送信元ネットワークまたは接続先ネットワークを選択するか、**[+ネットワークの作成（+Create Network）]** をクリックして新しいネットワークを作成します。詳細については、『About Fabric Overview for LAN Operational Mode Setups』の「Networks」セクションを参照してください。
送信元スイッチ（インターフェイス）	外部ネットワーク ドメインに接続する境界リーフ ノードのインターフェイスを選択します。この構成は、any が送信元ネットワークとして構成されている場合に必要です。
接続先スイッチ（インターフェイス）	外部ネットワーク ドメインに接続する境界リーフ ノードのインターフェイスを選択します。この構成は、any が接続先ネットワークとして構成されている場合に必要です。

2. このネットワークの構成が完了したら、行の末尾にあるチェックマークをクリックして、入力した値を受け入れます。

   追加のトラフィックを構成するには、これらの手順を繰り返します。

3. この使用例でサービス挿入を追加するために必要な情報を入力したら、**[保存（Save）]** をクリックします。

   [ファブリックの概要（Fabric Overview）] ページに戻ります。**[サービス（Services）] > [サービス挿入（Service Insertions）]** が選択されています。

ユースケースのアタッチと展開

サービス機能に関連付けられたサービス VRF がコンピューティング リーフ ノードに展開されていない場合、NDFC 12.2.2 はエラーを表示します。したがって、以下のステップ 1 に進む前に、コンピューティング リーフ ノードにサービス VRF を展開する必要があります。

1. 新しいサービスの挿入の横にあるボックスをオンにし、下部（白色）の **[アクション（Actions ）]** ドロップダウンをクリックして、**[アタッチ（Attach）]**を選択します。

   数秒後に、**[アタッチ（Attached）]** 列に表示されている値が **[True]**に変わります。

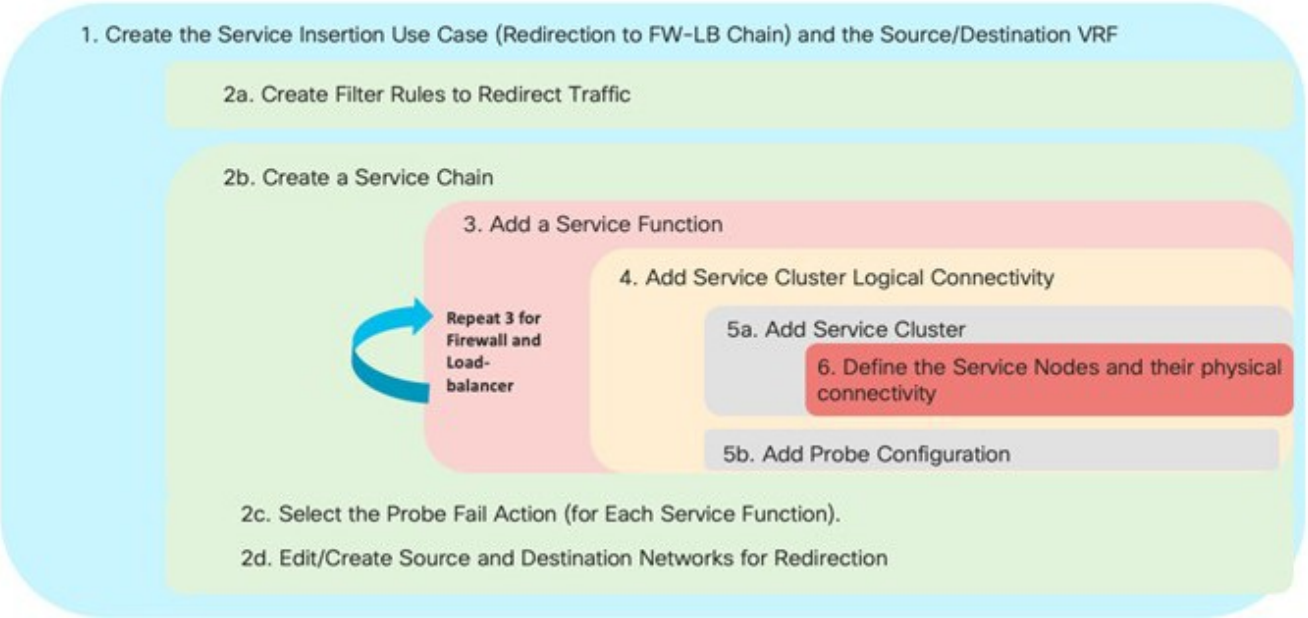
2. 上部（青色）の **[アクション（Actions ）]** ドロップダウンをクリックし、**[再計算して展開（Recalculate and Deploy）]** を選択します。

   これで、新しい構成がサービス リーフ ノードに展開されました。

ユースケース 3b：ファイアウォール ロード バランサ サービス チェーンへのリダイレクト

ファイアウォール ロード バランサ サービス チェーンへのリダイレクトのユースケースを設定するためのワークフローのグラフィカル表現については、次の図を参照してください。

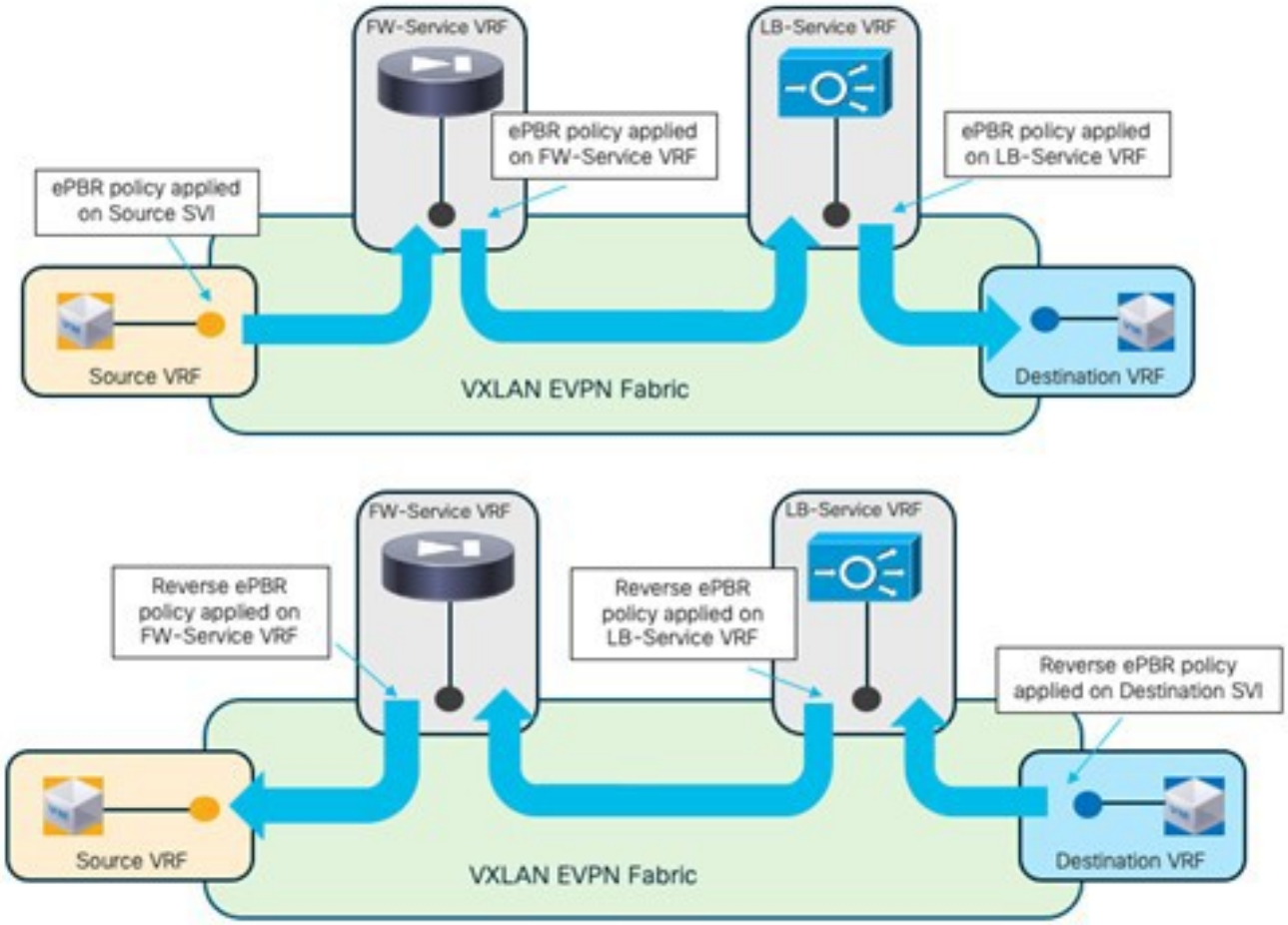
> 次の図に示すプロビジョニング手順については、以降のセクションで詳しく説明します。各セクションに関連付けられた番号は、図の対応するステップにマッチしています。ワークフローはステップ間を前後に移動するため、セクションの番号付けは必ずしも、順番通りではありません。



ファイアウォール ロード バランサ サービス チェーンへのリダイレクト：ワークフロー

基本的な前提は、ロード バランサが Source-NAT（SNAT）を実行していないことです。これは、サービス リダイレクトを活用して、サーバー ファームとクライアント間のトラフィック フローをロード バランサに戻す必要があることを意味します。

次の図 23 は、送信元ネットワーク（クライアント）と接続先ネットワーク（サーバー ファーム）の間のフローに必要なトラフィック リダイレクト機能の論理ビューを示しています。以下の手順で説明するように、これらのネットワークは、イーストウェストまたはノースサウストラフィックフローにサービスリダイレクトが必要かどうかに応じて、ファブリックの内部または外部になります。



ファイアウォール ロード バランサ サービス チェーンへのリダイレクト：トラフィック フロー ステアリング

送信元ネットワークと接続先ネットワークは、同じ VRF の一部であることも、異なる VRF の一部であることもあり得ます。ファイアウォールおよびロード バランサ サービス機能は、それぞれ専用のサービス VRF（FW-Service VRF および LB-Service VRF）に展開する必要があります。

上の図に示すように、フローの方向に応じて、サービス リダイレクト ポリシーが送信元（または接続先）SVI およびサービス VRF に適用されます。サービス VRF で、チェーンの一部である両方のサービス機能によって、フローの行き先が決まるようにするためです。「set-vrf」機能は、送信元/接続先 VRF で自動的に実行され、トラフィック フローを、サービス VRF のサービス機能に適切にリダイレクトします。送信元/接続先 VRF で「set-VRF」を使用すると、ファイアウォール（またはロード バランサ）の IP アドレスのルックアップが対応するサービス VRF で適切に実行され、必要な VRF 間接続が適切に確立されます。

> FW サービス VRF での ePBR ポリシーの適用は、VRF 間接続を有効にする場合にのみ必要です。これは、送信元ネットワーク（クライアント）から開始されたトラフィック フローの接続先は、常に、別の LB サービス VRF で到達可能なロード バランサ VIP アドレスであるためです。

送信元/接続先ネットワーク ルートをサービス VRF にリークする場合には、明示的なユーザー主導の構成が必要です。具体的には、接続先ネットワーク ルートはチェーンの最後のサービス機能（この例ではロード バランサ）の VRF にリークする必要がありますが、送信元ネットワーク ルートはチェーンの最初のサービス機能の VRF にリークする必要があります。（この例ではファイアウォール）。

特定のルートリーク構成は 、サービス機能が接続されているサービスリーフ ノードでのみプロビジョニングする必要があります。これについては、以下の特定の構成手順で説明します。

1. サービス挿入のユースケースの選択（サービス チェーンにリダイレクト）

1. **[サービス インスタンス（Service Instance）]** タブに移動します。
   a. 次の順に選択：

      [管理（Manage）] > [ファブリック（Fabrics）]

   b. 適切な Data Center VXLAN EVPN ファブリックをダブルクリックします。

      ファブリックの**[概要（Overview）]** ウィンドウが表示されます。

   c. **[サービス（Services）]** タブをクリックします。
   d. **[サービス挿入（Service Insertions）]** サブタブをクリックします。

      構成されているサービス挿入のユースケースのリストが表示されます。

2. **[アクション（Actions）] > [サービス挿入の追加（Add Service Insertion）]** をクリックします。

   [サービス挿入の追加（Add Service Insertion）] ウィンドウが表示されます。

3. **[サービス挿入の名前（Service Insertion Name）]** フィールドに、サービスの名前を入力します。

   名前にはアルファベット、数字、アンダースコア、または文字を含めることができます。たとえば、この特定のユースケースでは、Redirect-to-FW-LB-chain をサービス挿入名として使用できます。

4. **[ユースケース（Use Case）]** フィールドで、適切なユースケースを選択します。

   このユースケースでは、ユースケースとして **[サービス チェーンへのリダイレクト（Redirect to Service Chain）]** を選択します。

5. エンドポイントのサブネットを使用して VRF を選択または作成します。
   a. **[トラフィック送信元 VRF** フィールドで、このサービス挿入のユースケースに関連付ける既存のトラフィック送信元VRF を選択するか、**[+VRF の作成（+Create VRF）]** をクリックして新しい VRF を作成します。
   b. **[トラフィック接続先 VRF（Traffic Destination VRF）]** フィールドで、このサービス挿入のユースケースに関連付ける既存のトラフィック接続先 VRF を選択するか、**[+VRF の作成（+Create VRF）]** をクリックして新しい VRF を作成します。

      詳細については、LAN 動作モード設定のファブリックの概要の「VRF」セクションを参照してください。

      > この特定の例では、トラフィック送信元 VRF とトラフィック接続先 VRF の両方に同じテナント VRF（T1-VRF）を使用する必要があります。ただし異なるテナント VRF の一部であるエンドポイント間（またはエンドポイントと外部ネットワーク間）のトラフィックのリダイレクト実行もサポートされています。サポートされていません。

6. **[デタッチ/アタッチ（Detach/Attach）]** フィールドで、スイッチを切り替えて切り離しまたは接続します。

特定のサービス挿入ワークフローの最後にスイッチに構成をプロビジョニングできるようにするには、**[アタッチ（Attach）]**オプションを選択する必要があります。**[アタッチ（Attach）]** オプションは、この時点で、または構成設定ワークフローのすべての手順を完了した後の手順の最後に選択できますが、すべての手順の完了後に選択することを推奨します。

7. **[方向（Direction）]** フィールドで、このサービス挿入ユースケースの方向を選択します。

   オプションは、次のとおりです。

   - 双方向
   - 転送
   - 反転

   この特定の例では、**[双方向（Bidirectional ）]** を選択します。図 23 に示すように、選択した各トラフィック フローの両方のレッグをファイアウォールとロード バランサのサービス機能のチェーンにリダイレクトすることを目的としているからです。

8. このサービス挿入の **[統計の有効化（Enable Statistics）]** フィールドで、チェックボックスをオンにして、このサービス挿入ユースケースの統計を有効にします。

   統計情報を有効にすると、特定の ePBR ポリシーにマッチし、サービス機能にリダイレクトまたはサービス チェーン処理されたパケットの数が追跡されます。これらの統計情報は、後で時系列グラフの形式で視覚化して、トラフィック リダイレクト パターンを理解することもできます。

9. **[トラフィック フロー リダイレクト**（Traffic Flow Redirects）] エリアで、**[トラフィックフローリダイレクトの追加**（Add Traffic Flow Redirect ）] をクリックし、**必要な情報**を入力します。

10. **[ACL 名の照合（Match ACL Name）]**フィールドで、ドロップダウン リストから構成済みのアクセス制御リスト（ACL）を選択するか、**[+ACL の作成（+Create ACL）]** をクリックして新しいACLを作成します。

    このユースケースでは、**[+ACL の作成（+Create ACL）]** をクリックして新しいアクセス制御リストを作成します。2a に移動します。ACL 照合トラフィックを作成します。

2a. ACL 照合トラフィックの作成

ACL を作成して、後のセクションで定義するサービス機能にリダイレクトするべき特定のトラフィック フローを定義する必要があります。すべてのトラフィックをサービス機能（またはサービス機能のチェーン）にリダイレクトする最もシンプルなシナリオでは、送信元ポートまたは接続先ポートを構成せずに、**[プロトコル（Protocol）]** フィールドで ACL エントリを ip として指定するだけです。

ファイアウォール/ロード バランサ チェーンの特定のシナリオでは、送信元ネットワーク（クライアント）から発信されたトラフィックは常にロード バランサの VIP アドレスに送られますが、接続先ネットワーク（サーバー ファーム）から発信されたリターンフローは常に送信元ネットワーク（クライアント）に送られます。したがって、必要な ACL は（少なくとも）2 つのエントリで定義する必要があります。

- 1 つ目は、クライアント ネットワークを送信元として照合し（クライアントがファブリックの外部のネットワークに接続されている場合は any を 使用できます）、接続先としてロード バランサ VIPを照合します。これは、クライアントから VIP 宛てのトラフィックを最初にファイアウォールにリダイレクトするために使用されます。前述のように、クライアントから発信され LB VIP 宛てのトラフィックの場合でも、二重のサービス リダイレクトが技術的に実行され、「set ip next-hop + VRF」機能が有効になり、ファブリックがファイアウォール サービス機能を通過したトラフィックをロード バランサ VIP に送信できるようになります（図 23 の上部）。

- 2 つ目は、クライアント ネットワークを送信元として照合し（クライアントがファブリックの外部のネットワークに接続されている場合は any を 使用できます）、接続先としてサーバー ファーム ネットワークを照合します。このエントリは、サーバー ファームからクライアント宛てのリバース フローに対してのみ照合され、トラフィックを最初にロード バランサに、次にファイアウォールにリダイレクトするために使用されます（図 23 の下部）。

この場合の仮定は、送信元ネットワーク（クライアント）と接続先ネットワーク（サーバーファーム）の間に、直接通信が必要とされていないということです。その場合、これらのトラフィック フローは、上記で定義された 2 番目の ACL エントリの働きによりサービス チェーンにリダイレクトされます。

1. **[アクセス制御リスト名（Access Control List Name）]** フィールドに新しい ACL の名前を入力します。

   たとえば、ACL-Traffic-to-ServiceChain です。

2. **[アクセス リスト エントリ（Access List Entries）]** エリアで、**[+ アクセス リスト エントリの追加（+ Add Access List Entries）]**をクリックします。
3. 新しいアクセス制御リストを作成するために必要な情報を入力します。

フィールド	説明
シーケンス番号（Sequence Number）	ACL のシーケンス番号を入力します。有効な範囲は 1 ~ 4294967295 です。
プロトコル	ACL に使用するプロトコルを指定します。オプションは、次のとおりです。 ・icmp ・ip ・tcp ・udp
送信元 IP	ACL の送信元 IP アドレスを入力します。このエントリには、IPv4アドレス、IPv6アドレス、または any を指定できます。送信元として、ファブリックの外部にあり、境界リーフ ノードで構成されたレイヤ 3 ピアリングを介して内部エンドポイントに接続するサブネットを指定する場合は、any を使用します。それ以外の場合は、ファブリック内部のクライアントのサブネットの IP プレフィックスを構成します。
宛先 IP	ACL の宛先 IP アドレスを入力します。このエントリには、IPv4アドレス、IPv6アドレス、または any を指定できます。送信元として、ファブリックの外部にあり、境界リーフ ノードで構成されたレイヤ 3 ピアリングを介して内部エンドポイントに接続するサブネットを指定する場合は、any を使用します。それ以外の場合は、ファブリック内部のクライアントのサブネットの IP プレフィックスを構成します。
送信元ポート	送信元ポート番号を入力します（たとえば、*any* または *443*）。**[プロトコル（Protocol）]** フィールドで **ip** または **icmp** を選択した場合、このフィールドの値は無視されます。
宛先ポート	宛先ポート番号を入力します（たとえば、*any* または *443*）。**[プロトコル（Protocol）]** フィールドで **ip** または **icmp** を選択した場合、このフィールドの値は無視されます。

4. アクセス制御コントロール リストのエントリを受け入れるには、チェックマークをクリックします。

   [サービス挿入を追加（Add Service Insertion）] ウィンドウに戻り、新しく作成したアクセス制御リストが **[ACL 名の照合（Match ACL Name）]** フィールドに表示されます。

5. **[照合アクション（Macth Action）]** フィールドで、適切な ACL 照合アクションを選択します。

   オプションは、次のとおりです。

   - **[リダイレクト（Redirect）]**：トラフィックを照合し、サービス チェーンにリダイレクトするためのデフォルト アクション。
   - **[ドロップ（Drop）]**：着信インターフェイスで特定のトラフィックを照合し、トラフィックをドロップします。
   - **[除外（Exclude）]：**着信インターフェイスのサービス チェーンから特定のトラフィックを除外します。

     このユースケースでは、**リダイレクトを** 照合アクションとして選択します。

     > サービス チェーンのサービス挿入 には 、1 つのドロップと 1 つの 除外のみを含めることができ ます。

6. **[サービス チェーン名（Create Service Name）]** フィールドで、ドロップダウン リストから構成済みのサービス チェーンを選択するか、**[+サービス チェーンの作成（+Create Service Chain）]** をクリックして新しいサービス チェーンを作成します。

   このユースケースでは、**[+サービス チェーンの作成（+Create Service Chain）]** をクリックして、新しいサービス チェーンを作成します。2b に進みます。サービス チェーン（ファイアウォールとロード バランサ）を作成します。

2b. サービス チェーンの作成（ファイアウォールとロード バランサ）

このセクションで説明する特定の例では、ファイアウォールとロード バランサを含むサービス チェーンを検討します。この記事の冒頭で説明した冗長性モデル（アクティブ/スタンバイ クラスタ、アクティブ/アクティブ クラスタ、一連のスタンドアロン ノードなど）は、ファイアウォールおよびロード バランサ サービス機能の展開に使用できます。この例では、アクティブ/スタンバイ クラスタを検討します。

1. **[サービス チェーンの追加（Add Service Chain）]** ウィンドウで、**[サービス チェーン名（Service Chain Name）]** にサービス チェーンの名前を入力します。field.

   たとえば、Redirect_to_FW-LB_Chainです。

2. **[+サービス チェーン エントリの追加（+Add Service Chain Entries）]** をクリックします。
3. サービス チェーン エントリに必要な情報を入力します。

フィールド	説明
シーケンス番号（Sequence Number）	シーケンス番号を入力します。シーケンス番号が小さいほど、プライオリティが高くなります。 この例では、サービス チェーンに 2 つのサービス機能が定義されているため、次のエントリを設定します：

	・ファイアウォール、シーケンス番号 10 ・ロード バランサ、シーケンス番号 20 その後、シーケンス番号 10 のファイアウォールが優先順位され、シーケンス番号が最初にトリガーされ、シーケンス番号 20 のロード バランサが続きます。
サービスクラスタタイプ	サービス クラスタを選択します。このユースケースでは、最初にファイアウォール、次に **ロード バランサ**を選択します。
VRF	このサービス チェーンに関連付ける既存の VRF を選択するか、**[+ VRF の作成（+ Create VRF）]** をクリックして新しい VRF を作成します。サービス チェーンの各サービス機能部分は、送信元および接続先ネットワークに使用される VRF とは異なる専用 VRF を使用する必要があります。この例では、チェーンのサービス機能部分ごとに一意のサービス VRF が展開されます。
サービス機能	このサービス チェーンに関連付ける既存のサービス機能を選択するか、**[+サービス機能の追加（+Add Service Function）]** をクリックして新しいサービス機能を追加します。 推奨されるアプローチは、**[+サービス機能の追加（+Add Service Function）]** をクリックして新しいサービス機能を作成することです。サービス機能のオプション（1 アーム、2 アームなど）が、プロビジョニングされる特定のサービス挿入のワークフローに基づいて自動的に提案され、適切であることが保証されるからです。 このユースケースでは、**[+サービス機能の追加（+Add Service Function）]** をクリックして新しいサービス機能を作成します。3a に移動します。サービス機能の追加（ファイアウォール）および [3b. サービス機能（ロード バランサ）]を追加します。

3a. サービス機能の追加（ファイアウォール）

1. **[タイプ（Type）]**フィールドで、展開するサービス機能のタイプを選択します。

   このユースケースでは、展開するサービス機能のタイプとして **ファイアウォールを**選択します。

2. **[サービス機能名（Service Function Name）]** フィールドに、サービス機能の名前を入力します。

   名前にはアルファベット、数字、アンダースコア、または文字を含めることができます。

3. **[接続モード（Connectivity Mode）]** フィールドで、**[1 アーム（One Arm）]** または **[2 アーム（Two Arms）]** を選択します。

   通常は **[1 アーム （One Arm）]** オプションを推奨します。サービス機能のルーティング構成を簡素化するためです（サービス ネットワークの IP アドレスを指すデフォルト ルートのみが必要です）。

4. **[サービス VRF（Service VRF]** フィールドで、サービス VRF を選択します。

   作成するすべてのサービス機能に専用のサービス VRF が必要です。このサービス チェーンのユースケースでは、ファイアウォール サービス機能に使用される Service-FW VRF と、ロード バランサ サービス機能に使用される Service-LB VRF を定義します。

サービス挿入ワークフローの最後に、発信元ネットワークのテナント VRF と Service-FW VRF からのルートリークも構成する必要があります。前述のように、これは、リターン フロー（サーバー ファームとクライアント間）がファイアウォール サービス機能からファブリックに送り返された後、正常にクライアントにルーティングされるために必要です。

送信元ネットワークと Service-FW VRF 間のルートリーク構成は、ファイアウォール ノードが 接続されているサービスリーフノードにのみ適用する必要があります。NDFC 12.2.2 リリース では、ルートリーク構成を使用してフリーフォーム テンプレートを定義し、テンプレートをそれらのサービス リーフ ノードに適用することを推奨します。

次に、送信元ネットワークのテナント VRF と Service-FW VRF に属するリーク ルートを許可する構成のシンプルな例を示します（この例で使用される BGP ASN は 65002 です）。

テナント VRF の構成：「route-target auto」を使用すると、route-target が BGP-ASN:L3VNI（65002:50001）として定義されます。

```
vrf context t1-vrf
 vni 50001
 rd auto
 address-family ipv4 unicast
   route-target both auto route-
   target both auto evpn
 address-family ipv6 unicast
   route-target both auto route-
   target both auto evpn
```

Service-FW VRF の構成：テナント VRF からのプレフィックスが Service-FW VRF ルーティング テーブルにインポートされるようにする、特定の「import」ステートメントに注意してください。

```
vrf context t1-fw-vrf
 vni 50002
 rd auto
 address-family ipv4 unicast
   route-target both auto route-
   target both auto evpn
   route-target import 65002:50001 route-
   target import 65002:50001 evpn

 address-family ipv6 unicast
   route-target both auto route-
   target both auto evpn
   route-target import 65002:50001 route-
   target import 65002:50001 evpn
```

5. **[+ サービス クラスタ論理接続の追加（+ Add Service Cluster Logical Connectivity）]** をクリックします。

   [サービス クラスタ論理接続の追加（Add Service Cluster Logical Connectivity）] ウィンドウが表示されます。4a に移動します。サービスクラスタの 論理接続（ファイアウォール）を追加して、サービス機能の論理接続を構成します。

4a. サービス クラスタの論理接続（ファイアウォール）の追加

1. **[サービス クラスタ名（Service Cluster Name）]** フィールドで、構成済みのサービス クラスタを選択するか、**[+サービス クラスタの追加（+Add Service Cluster）]** をクリックして新しいクラスタを作成します。

   サービス機能の論理接続を構成する前に、そのようなサービス機能を実装するサービス クラスタを定義する必要があります。

   - **[+ サービスクラスタの追加（+Add Service Cluster）]**をクリックした場合は、5a に進みます。サービス クラスタ（ファイアウォール）を追加します。
   - このユースケースで既存の構成済みのサービスクラスタを選択する場合は、4b に進みます。サービス クラスタの論理接続（ファイアウォール）を追加します。

5a. サービス クラスタの追加（ファイアウォール）

1. **[タイプ（Type）]** フィールドの情報を確認します。

   「サービス機能の追加」のステップ 1 で選択したサービス挿入のユースケースに基づいて、**[タイプ（Type）]** フィールドが自動的に入力されます。

2. サービス クラスタを追加するために必要な情報を入力します。

フィールド	説明
サービスクラスタ名	サービス クラスタの名前を入力します。名前にはアルファベット、数字、アンダースコア、または文字を含めることができます。
ノードの冗長性	ノードの冗長性を選択します。 ・**[スタンドアロン（Standalone）]**：次の手順で単一のサービス ノードを追加する場合に適用されます。 ・**[アクティブ/スタンバイ クラスタ（Active/Standby Cluster）]**：次の手順で 2 つのサービス ノードを追加し、同じアクティブ/スタンバイ クラスタの一部にする場合に適用されます。 ・**[アクティブ/アクティブ クラスタ（Active/Standby Cluster）]**：次の手順で 2 つ以上のサービス ノードを追加し、単一のアクティブ/アクティブ クラスタの一部にする場合に適用されます。
フォーム ファクタ	**[物理（Physical）]** または **[仮想（Virtual）]** を選択します。

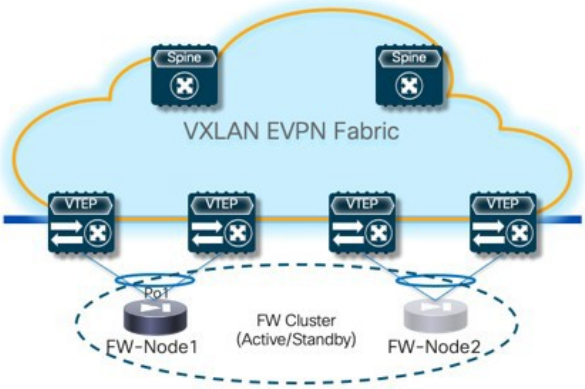
3. **[+ サービスノードの追加（+ Add Service Node）]** をクリックします。

[サービス ノードの追加（Add Services Node）] ウィンドウが表示されます。6 に移動します。サービスノード（ファイアウォール）を追加して、クラスタのサービス ノード部分とファブリックへの物理接続を定義します。

6. サービス ノードの追加（ファイアウォール）

ここで説明する特定の例では、次の図に示すように、2 つのサービスノード（同じアクティブ/スタンバイクラスタの一部である FW-Node1 と FW-Node2）を設定します。

> 前述のように、サービス機能の展開には、アクティブ/アクティブ クラスタまたはスタンドアロン ノードのセットを使用することもできます。



サービス チェーンへのリダイレクト：2 つのサービス ノードの構成

1. **[サービス ノード名（Service Node Name）] フィールドにサービス ノードのノード名を入力します。**

   たとえば、FW-Node1などです。

2. **[+ サービスノードの物理接続の追加（+ Add Service Node Physical Connectivity）]** をクリックして、ノードをファブリックに物理的に接続する方法を定義します。

   [サービス ノード論理接続の追加（Add Service Node Physical Connectivity）] ウィンドウが表示されます。

3. **[サービス ノード接続の追加（Add Service Node Connectivity ）]** ウィンドウで、必要な情報を入力します。

フィールド	説明
サービスノード名	前の手順で入力したサービス ノード名が自動的に入力されます。
サービス ノード インターフェイス	サービス ノード インターフェイスを入力します。サービスノード インターフェイスは表示目的のものなので、サービス ノードの特定のインターフェイスの名前と厳密に一致させる必要はありません（操作上便利な場合もあります）。

サービス ノード インターフェイスの使用状況	サービス ノード インターフェイスの使用状況を選択します。 前の図に示す特定の例では、各サービス ノードは単一の vPC 接続を使用してサービス リーフ ノードのペアに接続されます（異なる VLAN がその vPC にトランキングされ、サービス ネットワークと内部ネットワークに接続を提供します）。このため、**[サービス ノード インターフェイスの使用状況（Service Node Interface Usage）]** の **[内部/外部（Inside-Outside）]**オプションを選択します。代わりに、サービス ネットワークと内部ネットワークにそれぞれ接続を提供するために個別の物理インターフェイスを使用する場合は、内部サービス ノード インターフェイスと外部サービス ノード インターフェイスを個別に選択する必要があります。
アタッチされたスイッチ	サービス ノードがシングル接続かデュアル接続かに応じて、リストからスイッチまたはスイッチ ペアを選択します。
スイッチ インターフェイス	リストからインターフェイスを選択します。 ・**[アタッチされるスイッチ（Attached Leaf Switch）]** リストから vPC ペアを選択すると、それらのスイッチで定義された vPC のポートチャネルのリストが **[スイッチ インターフェイス（Interface）]** リストに表示されます。 ・それ以外の場合、トランク モードで構成されたポートチャネルおよびインターフェイスは、**[スイッチ インターフェイス（Switch Interface）]** リストに表示されます。
リンク テンプレート	指定されたアタッチ済みスイッチ インターフェイス タイプに基づき、ドロップダウン リストから service_link_trunk、service_link_port_channel_trunk、または the service_link_vpc を選択します。テンプレートフィールドの詳細については、レイヤ 4 ～ レイヤ 7 サービスの構成の「テンプレート」の項を参照してください。

4. [サービス ノード物理接続の追加（Add Service Node Physical Connectivity）] ウィンドウに必要な情報を入力したら、[保存（Save）] をクリックします。

   [サービス ノードの追加（Add Service NoswCluster）] ウィンドウに戻ります。

5. 前の手順を繰り返して別のサービス ノード インターフェイスを追加か、**[サービス ノードの 追加（Add Service Node）]** ウィンドウで **[保存（Save）]** をクリックしてサービスノード情報を保存します。

   [サービス クラスタの追加（Add Service Cluster）] ウィンドウに戻ります。

6. **[+ サービスノードの追加（+ Add Service Node）]**をクリックし、このセクションの手順を繰り返して、このユースケースの 2 番目のサービスノード（FW-Node2）を追加します。

   FW-Node2 サービス ノードを追加する手順を完了すると、**[サービス クラスタの追加（Add Service Cluster）]** ウィンドウの **[サービス ノード（Service Nodes）]** エリアに FW-Node1 と FW-Node2 の情報が表示されます。

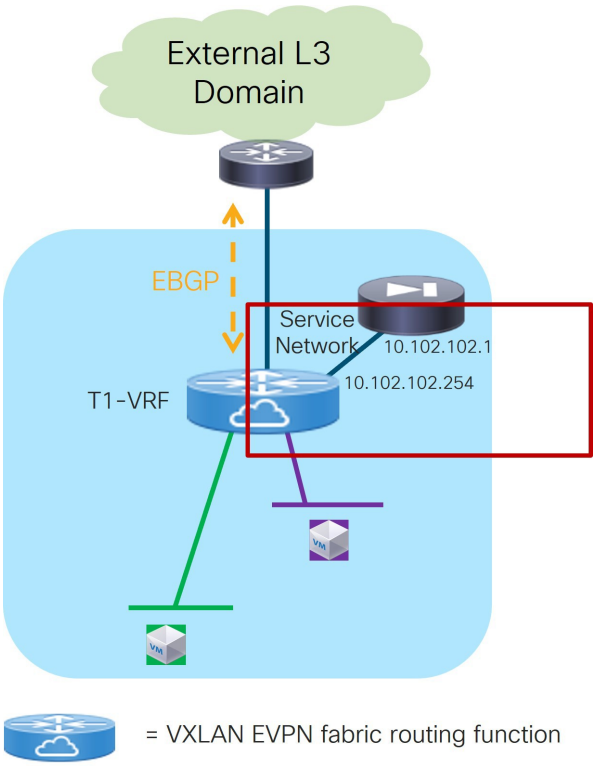
7. **[サービスクラスタの追加（Add Service Cluster）]** ウィンドウで **[保存（Save）]** をクリックして、サービス機能情報を保存します。

[サービス クラスタの論理接続の追加（Add Service Cluster Logical Connectivity）] ウィンドウに戻ります。4b に進みます。サービスクラスタの論理接続（ファイアウォール）を追加して、サービス クラスタの論理接続の構成を完了します。

4b. サービス クラスタの論理接続（ファイアウォール）の追加

これらのユースケースの手順のこの時点までで、構成済みのサービス クラスタを選択するか、新しいサービス クラスタを構成しました。サービス クラスタの論理接続を追加するプロセスを続けるために必要な情報を入力します。

図 25 に示すように、ファイアウォール サービス機能は、サービスネットワークを使用して 1 アームモードでファブリックに接続されます。これは、設定されたエニーキャストゲートウェイアドレスを持つ L2VNI セグメントによって表されます。ファブリックとファイアウォールの間にルーティング ピアリング（静的または EBGP）を確立する必要はありません。トラフィックのリダイレクトは、サービス ネットワークの一部である（ファブリックに直接接続され、そのため EVPN ファブリックのコントロールプレーンに再配布される）ファイアウォールの IP アドレスに対して実行されるからです。



サービス チェーンへのリダイレクト：サービスクラスタの論理接続

1. **[IPv4/IPv6（IPv4/IPv6）]** フィールドで、次のオプションから選択します：
   - IPv4
   - IPv6
   - IPv4 および IPv6

   この例では、**IPv4** を選択します。

2. サービス クラスタの論理接続を追加するプロセスを続けるために必要な情報を入力します。

   このウィンドウの残りのフィールドは、選択した接続モードに応じて変わります。この例では、推奨される **[2 アーム（Two Arms）]** オプションを選択した場合、次のフィールドが表示されます：

フィールド	説明
Service IPv4	ファイアウォールの IPv4 または IPv6（あるいはその両方）のサービス アドレスを入力します。 たとえば、このセクションの最初に示したこのユースケースの構成例の図では、このフィールドに 10.102.102.1 と入力します。
Service IPv6	
サービスネットワーク	このサービス機能に関連付ける既存のサービス ネットワークを選択するか、**[+サービス ネットワークの 追加（+Add Service ネットワーク ）]** をクリックして新しいサービス ネットワークを作成します。詳細については、LAN 動作モード セットアップのファブリックの概要について の「ネットワーク」セクションを参照してください。 新しいサービス ネットワークを作成する場合、このセクションの最初に示したこのユースケースの構成例では、**[IPv4 エニーキャストゲートウェイ/ネットマスク（IPv4 Anycast Gateway/Netmask）]** フィールドに 10.102.102.254/24 と入力します。この場合、この値は 、**[サービスクラスタ論理接続の追加（Add Service Cluster Logical Connectivity）]** ウィンドウの **[サービス ネットワーク（Service Network）]** エリアの **[ゲートウェイIP（Gateway IP）]**フィールドに表示されます。
プローブ	このサービス機能に関連付ける既存のプローブをクリックするか、または **[+プローブの追加（+Add Probe）] をクリックして** 、新しいプローブを作成します。 このユースケースでは、**[+プローブの追加（+Add Probe）]** をクリックしてプローブ構成を追加します。5b に移動します。プローブ構成（ファイアウォール）を追加します。

5b. プローブ構成（ファイアウォール）の追加

1. **[プローブ構成の追加（Add Probe Configuration）]** ウィンドウで、**[プローブ名（Probe Name）]** フィールドに名前を入力します。
2. **[プローブ テンプレート（Probe Template）]** フィールドで、**service_endpoint** を選択します。
3. プローブを構成するために必要な情報を入力します：

フィールド	説明
一般的なパラメータ	
プローブの有効化	（反転された）ネクスト ホップアドレスのプローブを有効にするには、このボックスをオンにします。 プローブは、ファブリック内のすべてのリーフ ノードから実行されます。プローブに使用される送信元インターフェイスは、サービス VRF の各リーフで定義されたループバック インターフェイスです。これらのループバックのプロビジョニングは、そのファブリックの **[リソース（Resources）]** にある **[VRF ごと、VTEP ごとの IPv4ループバック オートプロビジョニング（Per VRF Per VTEP Loopback IPv4 Auto-Provisioning）]** および **[VRF ごと、VTEP ごとの IPv6 ループバック オ**

	ートプロビジョニング（Per VRF Per VTEP Loopback IPv6 Auto-Provisioning）] フィールドを設定するために必須です。詳細については、「Data CenterVXLAN EVPN」 を参照してください。 上記の [VRF ごと、VTEP ごとのループバック（Per VRF Per VTEP Loopback）] オプションを有効にすると、ローカルに定義されているすべての VRF の各 VTEP にループバック アドレスが割り当てられます。これらのループバック アドレスに割り当てられる IP アドレスは、ファブリック レベルで指定されたグローバル プールから取得されます。NDFC 12.2.2 リリースでは、重複する IP アドレスを、異なる VRF の異なる VTE に割り当てられたループバックアドレスに割り当てることが許可されています。そのため、VRF リークがテナント VRF と Service-FW および Service-LB VRF の間で構成された場合、問題が生じることがあります。したがって、これらのループバック アドレスを手動で割り当て（ファブリック内の各 VTEP の VRF レベルで実行できます）、定義された VRF 内および定義された VRF 全体で一意であることを確認すること**を強く**推奨します。
プロトコル	プローブに使用するプロトコルを指定します。オプションは、次のとおりです。 ・icmp ・tcp ・udp ・http
ポート番号	プロトコルが tcp または udp の場合にのみ、入力に対して表示されます。プローブのポート番号を入力します。有効な範囲：1 ~ 65535（推奨範囲：1025 ~ 65534）。
HTTP プローブのユーザー入力	プロトコルが http の場合にのみ、入力用に表示されます。HTTPプローブのユーザー入力テキスト/ファイル名を入力します（例：http://192.168.50.254/ index.html）。最大サイズ：99
詳細	
しきい値	しきい値（秒）を入力します。有効な範囲：1 ~ 60
周波数	周波数の値を秒単位で入力します。有効な範囲：1 ~ 604800。
遅延 ダウン 変更履歴	遅延ダウン変更通告値を秒単位で入力します。有効な範囲は1 ~ 180
遅延 アップ 変更履歴	遅延アップ変更通告値を秒単位で入力します。有効な範囲：1 ~ 180。
タイムアウト（Timeout）	タイムアウト値を秒単位で入力します。有効な範囲：1 ~ 604800。

サービス リダイレクト用プローブの構成の詳細については、NX-OS 構成ガイドを参照してください。

4. 4c に進みます。サービス クラスタの論理接続（ファイアウォール）を追加します。

4c. サービス クラスタの論理接続（ファイアウォール）の追加

1. **[ピアリング オプション（Peering Option）]** フィールドで、このサービス機能に関連付ける適切なピアリング オプションを選択します。

   このユースケースでは、ピアリング オプションとして **[接続済み （Connected）]** を選択します。先ほど定義した FW-Service-Network に接続されているファイアウォールの IP アドレスにリダイレクトされるからです。

2. **[保存（Save）]** をクリックして、**[サービス チェーンの追加（Add Service Chain）]** ウィンドウに戻ります。
3. 2c に進みます。プローブ失敗時のアクションを選択します（ファイアウォール）。

2c. プローブ失敗アクションの選択（ファイアウォール）

1. **[サービス チェーンの追加（Add Service Chain）]** ウィンドウの **[プローブ失敗アクション（Probe Fail Action）]** フィールドで、適切なプローブ失敗アクションを選択します。

   オプションは、次のとおりです。

   - **[転送（Forward）]** : トラフィックが通常のルーティングテーブルを使用するデフォルトのオプションです。
   - **[ドロップ（Drop）]** : サービスが到達不能になると、トラフィックをドロップします。
   - **[バイパス（Bypass）]** : 現在のシーケンスで障害が発生した場合に、トラフィックを次のサービス シーケンスにリダイレクトします。
   - **なし**

2. チェックマークをクリックして、サービス チェーン ファイアウォール エントリの値を受け入れます。
3. 3b に進みます。サービス機能を追加します（ロード バランサ）。

3b. サービス機能の追加（ロード バランサ）

1. **[タイプ（Type）]**フィールドで、展開するサービス機能のタイプを選択します。

   このユースケースでは、展開するサービス機能のタイプとして **ロード バランサ**を選択します。

2. **[サービス機能名（Service Function Name）]** フィールドに、サービス機能の名前を入力します。

   名前にはアルファベット、数字、アンダースコア、または文字を含めることができます。

3. **[接続モード（Connectivity Mode）]** フィールドで、**[1 アーム（One Arm）]** または **[2 アーム（Two Arms）]** を選択します。

   通常は **[1 アーム （One Arm）]** オプションを推奨します。サービス機能のルーティング構成を簡素化するためです（サービス ネットワークの IP アドレスを指すデフォルト ルートのみが必要です）。

4. **[サービス VRF（Service VRF]** フィールドで、サービス VRF を選択します。

   作成するすべてのサービス機能に専用のサービス VRF が必要です。このサービス チェーンのユースケースでは、Service-FW VRF と Service-LB VRF を定義します。

サービス挿入ワークフローの最後に、接続先ネットワークのテナント VRF と Service-LB VRF からのルートリークも構成する必要があります前述のように、これはクライアントに発するフローが、ロード バランサ サービス機能からファブリックに送り返された後で、サービス ファームに正常に送られるようにするために必要です。

接続先ネットワークと Service-LB VRF 間のルートリーク構成は、ロード バランサ ノードが接続されているサービス リーフ ノードにのみ適用します。NDFC 12.2.2 リリース では、ルートリーク構成を使用してフリーフォーム テンプレートを定義し、そのテンプレートをそれらのサービス リーフ ノードに適用することを推奨します。

ルートリーク構成を使用して NDFC でフリーフォーム テンプレートを定義し、そのテンプレートをサービスリーフノードに適用することを推奨します。

次に、接続先ネットワークのテナント VRF と Service-LB VRF に属するリーク ルートを許可する構成のシンプルな例を示します（この例で使用される BGP ASN は 65002 です）。

テナント VRF の構成：「route-target auto」を使用すると、route-target が BGP-ASN:L3VNI（65002:50001）として定義されます。

```
vrf context t1-vrf
 vni 50001
 rd auto
 address-family ipv4 unicast
   route-target both auto route-
   target both auto evpn
 address-family ipv6 unicast
   route-target both auto route-
   target both auto evpn
```

Service-LB VRF の構成：テナント VRF からのプレフィックスが Service-LB VRF ルーティング テーブルにインポートされるようにする、特定の「import」ステートメントに注意してください。

```
vrf context t1-lb-vrf
 vni 50003
 rd auto
 address-family ipv4 unicast
   route-target both auto route-
   target both auto evpn
   route-target import 65002:50001 route-
   target import 65002:50001 evpn

 address-family ipv6 unicast
   route-target both auto
```

```
route-target both auto evpn
route-target import 65002:50001
route-target import 65002:50001 evpn
```

5. **[+ サービス クラスタ論理接続の追加（+ Add Service Cluster Logical Connectivity）]** をクリックします。

   [サービス クラスタ論理接続の追加（Add Service Cluster Logical Connectivity）] ウィンドウが表示されます。4a に移動します。サービスクラスタの 論理接続（ロード バランサ）を追加して、サービス機能の論理接続を構成します。

4a. サービス クラスタの論理接続の追加（ロード バランサ）

1. **[サービス クラスタ名（Service Cluster Name）]** フィールドで、構成済みのサービス クラスタを選択するか、**[+サービス クラスタの追加（+Add Service Cluster）]** をクリックして新しいクラスタを作成します。

   サービス機能の論理接続を構成する前に、そのようなサービス機能を実装するサービス クラスタを定義する必要があります。

   - **[+ サービスクラスタの追加（+Add Service Cluster）]**をクリックした場合は、5a に進みます。サービス クラスタを追加します（ロード バランサ）。
   - このユースケースで既存の構成済みのサービスクラスタを選択する場合は、4b に進みます。 サービス クラスタの論理接続を追加します（ロードバランサ）。

5a. サービスクラスタの追加（ロード バランサ）

1. **[タイプ（Type）]** フィールドの情報を確認します。

   「サービス機能の追加」のステップ 1 で選択したサービス挿入のユースケースに基づいて、**[タイプ（Type）]** フィールドが自動的に入力されます。

2. サービス クラスタを追加するために必要な情報を入力します。

フィールド	説明
サービスクラスタ名	サービス クラスタの名前を入力します。名前にはアルファベット、数字、アンダースコア、または文字を含めることができます。
ノードの冗長性	ノードの冗長性を選択します。 ・**[スタンドアロン（Standalone）]**：次の手順で単一のサービス ノードを追加する場合に適用されます。 ・**[アクティブ/スタンバイ クラスタ（Active/Standby Cluster）]**：次の手順で 2 つのサービス ノードを追加し、同じアクティブ/スタンバイ クラスタの一部にする場合に適用されます。 ・**[アクティブ/アクティブ クラスタ（Active/Standby Cluster）]**：次の手順で 2 つ以上のサービス ノードを追加し、単一のアクティブ/アクティブ クラスタの一部にする場合に適用されます。

	ここで説明する特定の例では、ノードの冗長性のために、**[スタンドアロン（Standalone）]** を選択します。
フォーム ファクタ	**[物理（Physical）]** または **[仮想（Virtual）]** を選択します。

3. **[+ サービスノードの追加（+ Add Service Node）]** をクリックします。

   [サービス ノードの追加（Add Services Node）] ウィンドウが表示されます。6 に移動します。サービスノード（ロード バランサ）を追加して、クラスタのサービス ノード部分とファブリックへの物理接続を定義します。

6. サービスノードの追加（ロード バランサ）

ここで説明する特定の例では、1 つのサービス ノード（LB-Node1）を設定します。

1. **[サービス ノード名（Service Node Name）]** フィールドにサービス ノードのノード名を入力します。

   たとえば、LB-Node1です。

2. **[+ サービスノードの物理接続の追加（+ Add Service Node Physical Connectivity）]** をクリックして、ノードをファブリックに物理的に接続する方法を定義します。

   [サービス ノード論理接続の追加（Add Service Node Physical Connectivity）] ウィンドウが表示されます。

3. **[サービス ノード接続の追加（Add Service Node Connectivity ）]** ウィンドウで、必要な情報を入力します。

フィールド	説明
サービスノード名	前の手順で入力したサービス ノード名が自動的に入力されます。
サービス ノード インターフェイス	サービス ノード インターフェイスを入力します。サービスノード インターフェイスは表示目的のものなので、サービス ノードの特定のインターフェイスの名前と厳密に一致させる必要はありません（操作上便利な場合もあります）。
サービス ノード インターフェイスの使用状況	サービス ノード インターフェイスの使用状況を選択します。 ここで説明する特定の例では、**[第一第二アーム（First-Second Arm）]**を選択します。
アタッチされたスイッチ	サービス ノードがシングル接続かデュアル接続かに応じて、リストからスイッチまたはスイッチ ペアを選択します。
スイッチ インターフェイス	リストからインターフェイスを選択します。 ・**[アタッチされるスイッチ（Attached Leaf Switch）]** リストから vPC ペアを選択すると、それらのスイッチで定義された vPC のポートチャネルのリストが **[スイッチ インターフェイス（Interface）]** リストに表示されます。 ・それ以外の場合、トランク モードで構成されたポートチャネルおよびインターフェイスは、**[スイッチ インターフェイス（Switch Interface）]** リストに表示されます。

リンク テンプレート	指定されたアタッチ済みスイッチ インターフェイス タイプに基づき、ドロップダウン リストから service_link_trunk 、service_link_port_channel_trunk、または the service_link_vpc を選択します。テンプレートフィールドの詳細については、レイヤ 4 ~ レイヤ 7 サービスの構成の「テンプレート」の項を参照してください。

4. [サービス ノード物理接続の追加（Add Service Node Physical Connectivity）] ウィンドウに必要な情報を入力したら、[保存（Save）] をクリックします。

   [サービス ノードの追加（Add Service NoswCluster）] ウィンドウに戻ります。

5. 前の手順を繰り返して別のサービス ノード インターフェイスを追加するか、**[サービス ノードの追加（Add Service Node ）]** ウィンドウで **[保存（Save）]** をクリックして、サービスノード情報を保存します。

   [サービス クラスタの追加（Add Service Cluster）] ウィンドウに戻ります。

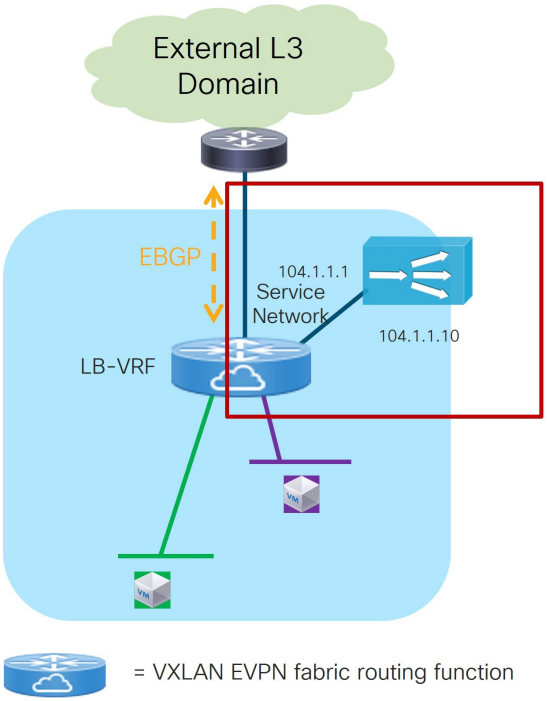
6. **[サービスクラスタの追加（Add Service Cluster）]** ウィンドウで **[保存（Save）]** をクリックして、サービス機能情報を保存します。

   [サービス クラスタの論理接続の追加（Add Service Cluster Logical Connectivity）] ウィンドウに戻ります。4b に進みます。サービス クラスタの論理接続（ロード バランサ）を追加して、サービス クラスタの論理接続の構成を完了します。

4b. サービス クラスタの論理接続の追加（ロード バランサ）

これらのユースケースの手順のこの時点までで、構成済みのサービス クラスタを選択するか、新しいサービス クラスタを構成しました。サービス クラスタの論理接続を追加するプロセスを続けるために必要な情報を入力します。

図 26 に示すように、ロード バランサ サービス機能は、サービスネットワークを使用して 1 アームモードでファブリックに接続されます。これは、設定されたエニーキャストゲートウェイアドレスを持つ L2VNI セグメントによって表されます。ロード バランサによって公開されるロード バランサ VIP がサービス ネットワークのサブネットの一部である場合、ファブリックとロード バランサの間にルーティング ピアリング（静的または EBGP）を確立する必要はありません。サービス ネットワークはファブリックに直接接続されているため、EVPN ファブリックのコントロール プレーンに再配布されるからです。ただし、VIP が別のサブネットの一部である場合は、スタティック ルーティングまたは EBGP を使用して、ファブリックが VIP サブネットを認識できるようにする必要があります。



サービス チェーンへのリダイレクト：サービスクラスタの論理接続

1. **[IPv4/IPv6（IPv4/IPv6）]** フィールドで、次のオプションから選択します：
   - IPv4
   - IPv6
   - IPv4 および IPv6

   この例では、**IPv4** を選択します。
2. サービス クラスタの論理接続を追加するプロセスを続けるために必要な情報を入力します。

   このウィンドウの残りのフィールドは、選択した接続モードに応じて変わります。この例では、このユースケースで選択したサービス挿入のユースケースに基づいて **[2 アーム（Two Arms）]** が自動的に選択された場合、次のフィールドが表示されます。

フィールド	説明
Service IPv4	ファイアウォールの IPv4 または IPv6（あるいはその両方）のサービス アドレスを入力します。 たとえば、このセクションの最初に示したこのユースケースの構成例の図では、このフィールドに 10.102.102.1 と入力します。
Service IPv6	
サービスネットワーク	このサービス機能に関連付ける既存のサービス ネットワークを選択するか、**[+サービス ネットワークの 追加（+Add Service ネットワーク ）]** をクリックして新しいサービス ネットワークを作成します。詳細については、LAN 動作モード セットアップのファブリックの概要について の「ネットワーク」セクションを参照してください。 新しいサービス ネットワークを作成する場合、このセクションの最初に示したこのユースケースの構成例では、**[IPv4 エニーキャストゲートウェイ/ネットマスク（IPv4 Anycast Gateway/Netmask）]** フィールドに 10.102.102.254/24 と入力します。この場合、この値は 、**[サービスクラ**

	スタ論理接続の追加（Add Service Cluster Logical Connectivity）] ウィンドウの **[サービス ネットワーク（Service Network）]** エリアの **[ゲートウェイIP（Gateway IP）]**フィールドに表示されます。
プローブ	このサービス機能に関連付ける既存のプローブをクリックするか、または **+ [プローブの追加（Add Probe）] をクリックして** 、新しいプローブを作成します。 このユースケースでは、**[+プローブの追加（+Add Probe）]** をクリックしてプローブ構成を追加します。5b に移動します。プローブ構成（ロード バランサ）を追加します。

5b. プローブ構成（ロード バランサ）の追加

1. **[プローブ構成の追加（Add Probe Configuration）]** ウィンドウで、**[プローブ名（Probe Name）]** フィールドに名前を入力します。
2. **[プローブ テンプレート（Probe Template）]** フィールドで、**service_endpoint** を選択します。
3. プローブを構成するために必要な情報を入力します：

フィールド	説明
一般的なパラメータ	
プローブの有効化	（反転された）ネクスト ホップアドレスのプローブを有効にするには、このボックスをオンにします。 プローブは、ファブリック内のすべてのリーフ ノードから実行されます。プローブに使用される送信元インターフェイスは、サービス VRF の各リーフ ノードで定義されたループバック インターフェイスです。これらのループバックのプロビジョニングは、そのファブリックの **[リソース（Resources）]** にある **[VRF ごと、VTEP ごとの IPv4ループバック オートプロビジョニング（Per VRF Per VTEP Loopback IPv4 Auto-Provisioning）]** および **[VRF ごと、VTEP ごとの IPv6 ループバック オートプロビジョニング（Per VRF Per VTEP Loopback IPv6 Auto-Provisioning）]** フィールドを設定するために必須です。詳細については、データセンター VXLAN EVPN を参照してください。 上記の [VRF ごと、VTEP ごとのループバック（Per VRF Per VTEP Loopback）] オプションを有効にすると、ローカルに定義されているすべての VRF の各 VTEP にループバック アドレスが割り当てられます。これらのループバック アドレスに割り当てられる IP アドレスは、ファブリック レベルで指定されたグローバル プールから取得されます。NDFC 12.2.2 リリースでは、重複する IP アドレスを、異なる VRF の異なる VTE に割り当てられたループバックアドレスに割り当てることが許可されています。そのため、VRF リークがテナント VRF と Service-FW および Service-LB VRF の間で構成された場合、問題が生じることがあります。したがって、これらのループバック アドレスを手動で割り当て（ファブリック内の各 VTEP の VRF レベルで実行できます）、定義された VRF 内および定義

		された VRF 全体で一意であることを確認すること**を強く**推奨します。
プロトコル	プローブに使用するプロトコルを指定します。オプションは、次のとおりです。 ・icmp ・tcp ・udp ・http	
ポート番号	プロトコルが tcp または udp の場合にのみ、入力に対して表示されます。プローブのポート番号を入力します。有効な範囲：1 ~ 65535（推奨範囲：1025 ~ 65534）。	
HTTP プローブのユーザー入力	プロトコルが http の場合にのみ、入力用に表示されます。HTTPプローブのユーザー入力テキスト/ファイル名を入力します（例：http://192.168.50.254/ index.html）。最大サイズ：99	
詳細		
しきい値	しきい値（秒）を入力します。有効な範囲：1 ~ 60	
周波数	周波数の値を秒単位で入力します。有効な範囲：1 ~ 604800。	
遅延ダウン変更履歴	遅延ダウン変更通告値を秒単位で入力します。有効な範囲は1 ~ 180	
遅延アップ変更履歴	遅延アップ変更通告値を秒単位で入力します。有効な範囲：1 ~ 180。	
タイムアウト（Timeout）	タイムアウト値を秒単位で入力します。有効な範囲：1 ~ 604800。	

サービスリダイレクトのプローブ設定の詳細については、NX-OS 構成ガイドを参照してください。

4. 4c に進みます。サービス クラスタの論理接続を追加します（ロードバランサ）。

4c. サービス クラスタの論理接続の追加（ロード バランサ）

1. **[ピアリング オプション（Peering Option）]** フィールドで、このサービス機能に関連付ける適切なピアリング オプションを選択します。

   選択するべき特定のオプションは、主にロード バランサの VIP 構成によって変わります。

   - VIP が、ロード バランサの 1 アームをファブリックに接続するために使用する以前に作成された LB-Service-Network の一部である場合は、ピアリングオプションとして **[接続済み（Connected）]**を選択します。
   - VIP が別のサブネットの一部である場合は、**[静的（Static）]** または **[eBGP]** オプションを選択して、ファブリックがその VIP 接続先に到達する方法を認識していることを確認できます。
2. 2c に進みます。プローブ失敗アクションを選択します（ロード バランサ）。

2c. プローブ失敗アクション（ロード バランサ）の選択

1. **[サービス チェーンの追加（Add Service Chain）]** ウィンドウの **[プローブ失敗アクション（Probe Fail Action）]** フィールドで、適切なプローブ失敗アクションを選択します。

   オプションは、次のとおりです。

   - **[転送（Forward）]**：トラフィックが通常のルーティングテーブルを使用するデフォルトのオプションです。
   - **[ドロップ（Drop）]**：サービスが到達不能になると、トラフィックをドロップします。
   - **[バイパス（Bypass）]**：現在のシーケンスで障害が発生した場合に、トラフィックを次のサービス シーケンスにリダイレクトします。
   - **なし**

2. チェックマークをクリックして、ロード バランサ サービス チェーン エントリの値を受け入れます。
3. **[保存（Save）]** をクリックします。

   [サービス挿入の追加（Add Service Insertion）] ウィンドウに戻ります。

4. 2d に進みます。送信元および接続先ネットワークを作成/選択します。

2d. 送信元および接続先ネットワークの作成/選択

ステップ 2a で作成したアクセス制御リストの結果として、ステップ 1a で構成した送信元および接続先 VRF にマッチする送信元および接続先ネットワーク部分が、**[ネットワーク（Networks）]** エリアに事前入力されます。これらのエントリは、ePBR ポリシーを適用する必要があるインターフェイスを NDFC に示すために必要です。通常、これらのエントリを変更する必要はありません。ただし、送信元または接続先ネットワークが any キーワードを用いて構成されている場合は例外です（any を同じエントリの送信元および接続先ネットワークの両方で使用するのは不可能であることに注意してください）。

送信元または接続先ネットワークとして any を使用することは、ファブリックの外部にあるプレフィックスを指定する意図を表します。送信元として any を 使用するルールは、フローの送信元が外部ネットワーク ドメインに接続されているクライアントであることを意味します。逆に、接続先として any を使用するルールは、フローの接続先がファブリックの外部にあるクライアントであることを意味します。外部ネットワーク ドメインは境界リーフ ノードを介して到達可能である必要があるため、UI では、送信元（または接続先）の any ネットワークで外部ドメインへの接続に使用される、境界リーフ ノードのインターフェイスを指定する必要があります。

ファイアウォール ロード バランサ サービス チェーンの特定のユースケースでは、構成する ACL には通常 2 つのエントリがあります：

- 最初のエントリは、クライアント ネットワーク（クライアントが外部接続されている場合は any の可能性があります）からロード バランサの VIP アドレス（この例では 172.16.100.100/32）を接続先とするトラフィックを照合するために使用されます。
- 2 番目のエントリは、サーバー ファームからクライアントへのリターン トラフィックを照合するために使用されます。

次の図に、ACL 構成のために自動的に作成されるネットワーク エントリを示します。

ACL 構成を基に作成されたネットワーク エントリ

続行する前に、接続先ネットワークとして VIP サブネットを持つ特定のエントリを手動で削除する必要があります。これは、VIP がテナント VRF ではなくサービス LB VRF の一部であるため、接続先が外部接続先として解釈されるためです。いずれの場合も、テナント VRF のインターフェイスにのみ ePBR ポリシーを適用する必要があるため、必要なエントリは送信元ネットワーク（クライアント）と接続先ネットワーク（サーバー ファーム）を含むエントリだけです。

[ファブリックの概要（Fabric Overview）] ページに戻ります。**[サービス（Services）] > [サービス挿入（Service Insertions）]** が選択されています。

ユースケースのアタッチと展開

各サービス機能に関連付けられたサービス VRF がコンピューティング リーフ ノードに展開されていない場合、NDFC 12.2.2 はエラーを表示します。したがって、以下のステップ 1 に進む前に、コンピューティング リーフ ノードにサービス VRF を展開する必要があります。

1. 新しいサービスの挿入の横にあるボックスをオンにし、下部（白色）の **[アクション（Actions ）]** ドロップダウンをクリックして、**[アタッチ（Attach）]**を選択します。

   数秒後に、**[アタッチ（Attached）]** 列に表示されている値が **[True]**に変わります。

2. 上部（青色）の **[アクション（Actions ）]** ドロップダウンをクリックし、**[再計算して展開（Recalculate and Deploy）]** を選択します。

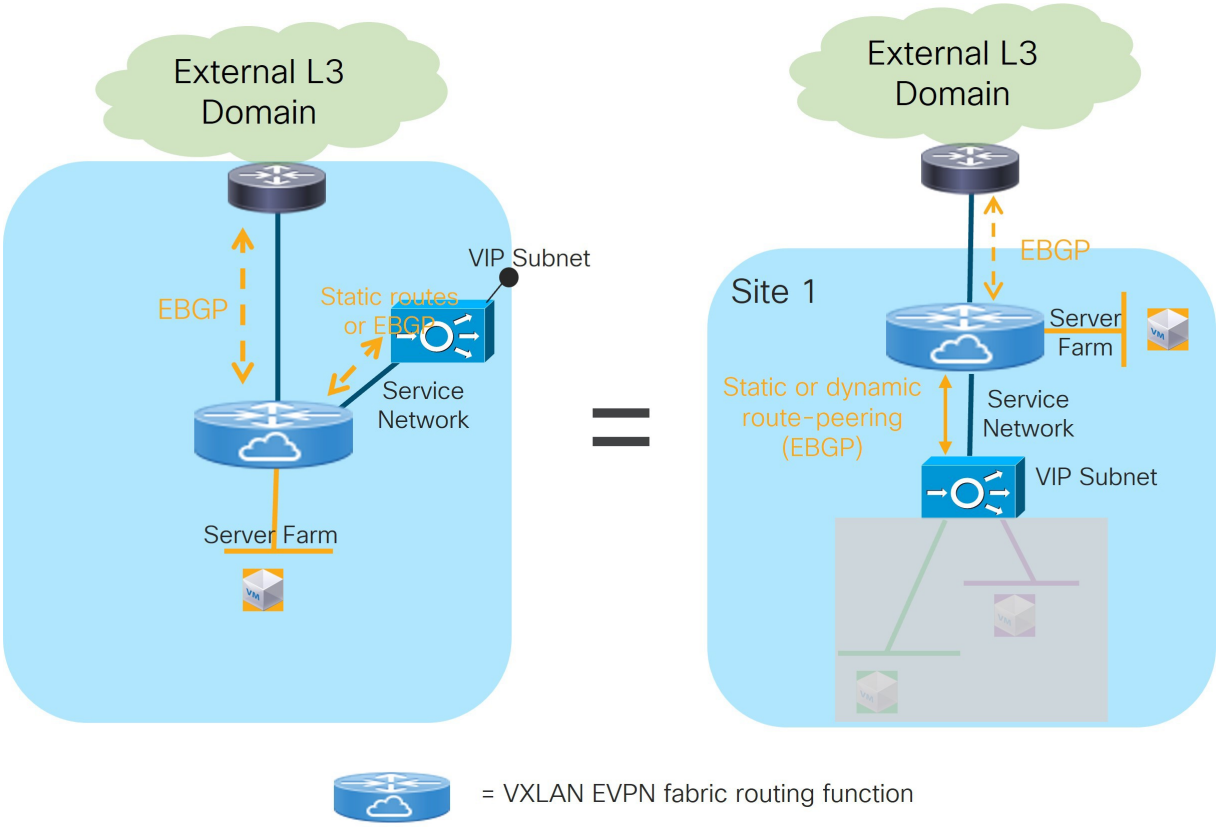
   これで、新しい構成がサービス リーフ ノードに展開されました。

一般的な 1 アームサービス機能のユースケース

前のセクションでは、NDFC 12.2.2 でプロビジョニングできる特定のユースケース（デフォルト ゲートウェイとしてのサービス機能、境界デバイスとしてのサービス機能、およびサービス チェーンへのリダイレクト）について説明しました。

以下のセクションでは、ファブリックで定義された VRF との静的ピアリングまたは eBGP ピアリングを確立する機能を備えた、1 アーム モードでのサービス機能の展開が必要となる、共通した特性を持つ他の特定のシナリオについて説明します。

この一般的な 1 アームユースケースのプロビジョニングは、NDFC 12.2.2 の GUI では明示的にサポートされていませんが、次の図 28 で示しているとおり、デフォルトのユースケースとしてのサービス機能を活用すれば、このような現時点での制限は簡単に解決できます。



1 アームサービス機能のデフォルト ゲートウェイとしてのサービスの使用

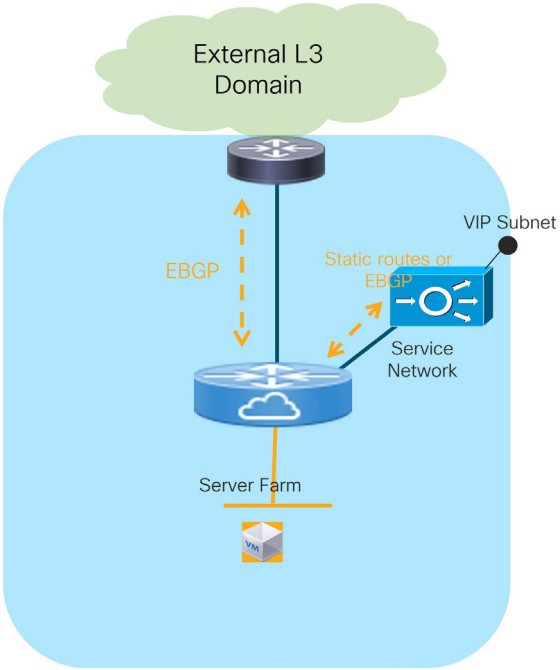
デフォルト ゲートウェイとしてのサービス機能のプロビジョニングと、ファブリックとピアに 1 アームで接続されたサービス機能の違いは、展開モードとレイヤ 2 のみの VNI だけです。前者は N アーム展開モードとして定義する必要がありますが、後者は 1 アーム展開モードです。

> NDFC 12.2.2 では、デフォルト ゲートウェイのユースケースとしてサービスをプロビジョニングするときに、少なくとも 1 つのレイヤ 2 専用 VNI を定義する必要があります。ファブリックとの 1 アーム モード ピアリングでサービス機能を展開することが目標の場合は、プロビジョニング ワークフローを満たすために、少なくとも 1 つの「ダミー」レイヤ 2 専用 VNI を展開する必要があります。

特定のプロビジョニング手順については、ユースケース 1：デフォルト ゲートウェイとしてのサービス機能のセクションを参照してください。以下のセクションでは、1 アームモードでのサービス機能の展開とファブリックとのピアリングを必要とするいくつかのユースケースについて説明します（ただし、情報はすべてを網羅しているわけではありません）。

送信元 NAT を使用したロード バランサ（SNAT）

送信元 NAT（SNAT）を使用したロード バランサのユースケースについては、次の図を参照してください。



送信元 NAT を使用したロード バランサ

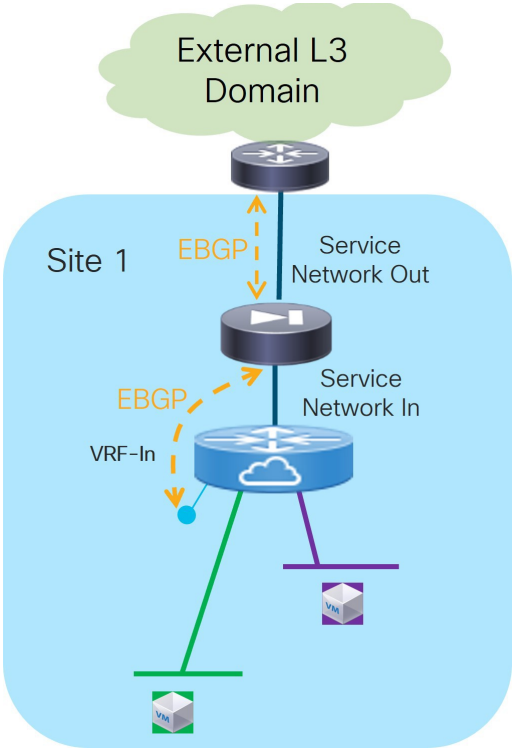
ロード バランサは 1 アームモードで接続され、「サービスネットワーク」のインターフェイス部分を介して（静的にまたは EBGP を使用して）ファブリックとピアリングします。これは、クライアントが接続できるように、ファブリックへの VIP アドレスへのアクセスを提供するために行われます。

> VIP アドレスが「サービスネットワーク」に関連付けられたサブネットの一部であるシナリオでは、ロード バランサとファブリック間に静的または動的ルーティングが必要ないため、設計が簡素化されます。通常のエンドポイントであるかのように「サービスネットワーク」にロード バランサを接続するだけで十分です。

ロード バランサは、クライアントから発信されたトラフィックを受信すると、SNAT と DNAT の両方を実行し、トラフィックをサーバー ファームに転送します。したがって、サーバー ファームから発信されたリターン トラフィックは、特定のロード バランサ IP アドレスを使用して、自動的にロード バランサに戻されます（ファブリックでのサービス リダイレクト機能は必要ありません）。ロード バランサは、SNAT と DNAT を実行し、トラフィックをクライアントに送り返します。

1 アーム境界ファイアウォール

このシナリオを図 30 に示します。これは、前述の ユースケース 2：境界デバイスとしてのサービス機能 セクションで説明したユースケースのバリエーションを表しています。

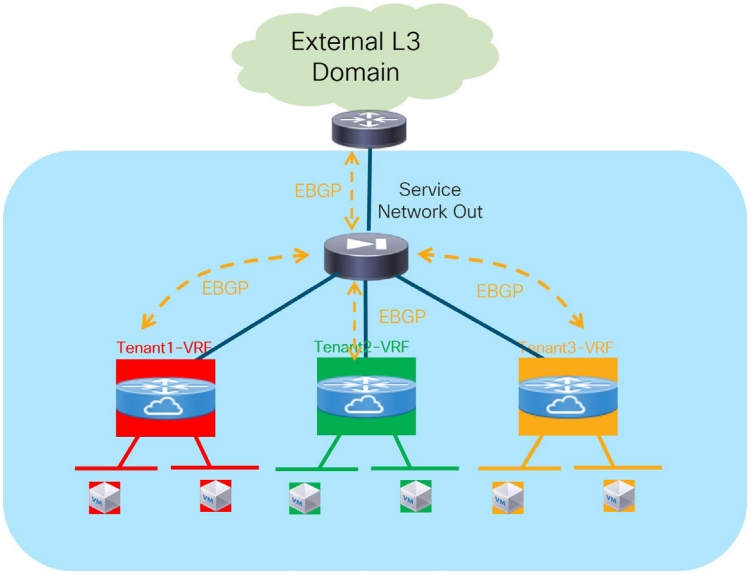


1 アーム境界ファイアウォール

唯一の違いは、この場合のファイアウォールは、（ファブリックで定義された VRF ではなく）外部ルータと直接ノースバウンドでピアリングすることです。したがって、ユースケース 2 で説明したワークフローはここでは適用できません。

> ファイアウォールは、2 つの異なる 方法で外部ルータにノースバウンド接続できます。1 番目は専用の物理インターフェイスを使用する方法で、2 番目はファブリックをレイヤ 2 トランスポートとしてを使用して、外部ルータとのルーティング ピアリングを確立する方法です。ルータに拡張されます。2 番目のシナリオでは、レイヤ 2 のみの VNII をファブリックで別個にプロビジョニングし、ファイアウォール ノードと外部ルータを接続する必要があります。

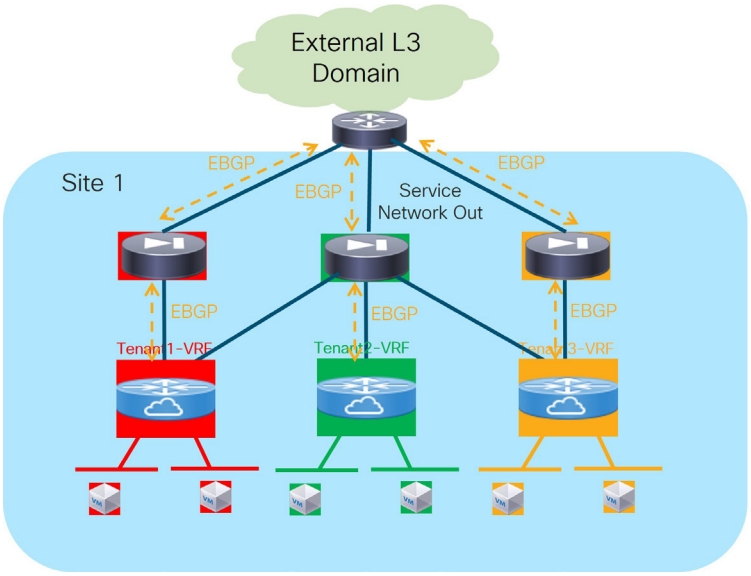
マルチテナント ファブリック展開では、同じ 1 アームの境界ファイアウォール シナリオを活用することもできます。このシナリオでは、ファイアウォール ノードが異なるテナントの VRF 間の「融合デバイス」として機能し、各テナントと外部ネットワーク ドメイン間でのトラフィック フローにおいて、異なるテナント間のトラフィック フローに対し、ポリシーを強制します（図 31）。



マルチテナント展開での 1 アーム境界ファイアウォール

すべての VRF は同じファブリックで定義されるため、デフォルトではファブリックの BGP ASN を継承します。したがって、テナント間で（ファイアウォールを介して）プレフィックスを正常に交換するため、各 VRF で「local-AS」構成を使用して、すべての VRF が一意の BGP ASN を公開することを推奨します。サービス機能とファブリックの間に eBGP ピアリングを設定するときに、**[詳細（Advanced）]** エリアでこの設定にアクセスできます。

> この特定のシナリオでは、各テナント VRF へのサービス機能の接続に必要なワークフローで同じファイアウォール クラスタが使用されます。これは、同じファイアウォール デバイスの異なるインターフェイスは、異なるテナントに割り当てられるからです。A 可能な代替シナリオとしては、図 32 に示すように、テナントごとに専用のファイアウォール クラスタを置くことです。



1 アーム境界ファイアウォール

著作権

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任となります。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『INFORMATION PACKET』に記載されており、この参照により本マニュアルに組み込まれるものとします。添付されていない場合には、代理店にご連絡ください。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアルの中の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

Cisco およびCisco のロゴは、Cisco またはその関連会社の米国およびその他の国における商標または登録商標です。商標または登録商標です。Cisco の商標の一覧は、https://www.cisco.com/go/trademarks でご確認いただけます。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」という言葉が使用されていても、シスコと他社の間にパートナー関係が存在することを意味するものではありません。（1110R）。

© 2017-2024 Cisco Systems, Inc. All rights reserved.