Cisco Nexus 9000 シリーズ NX-OS ePBR 構成ガイド、リリース 10.6(x)

最終更新：2026 年 2 月 3 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

はじめに

この前書きは、次の項で構成されています。

対象読者

このマニュアルは、Cisco Nexus スイッチの設置、設定、および維持に携わるネットワーク管理者を対象としています。

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を指定する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
[x | y]	いずれか1つを選択できる省略可能なキーワードや引数は、角かっこで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。

表記法	説明
[x {y | z}]	角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
`variable`	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しないでください。引用符を使用すると、その引用符も含めて string と見なされます。

例では、次の表記法を使用しています。

表記法	説明
`screen フォント`	スイッチが表示する端末セッションおよび情報は、スクリーンフォントで示しています。
`太字の screen フォント`	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の *screen* フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコ（< >）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

Cisco Nexus 9000 シリーズ スイッチの関連資料

Cisco Nexus 9000 シリーズ スイッチ全体のマニュアル セットは、次の URL にあります。

https://www.cisco.com/en/US/products/ps13386/tsd_products_support_series_home.html

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバック フォームよりご連絡ください。ご協力をよろしくお願いいたします。

通信、サービス、およびその他の情報

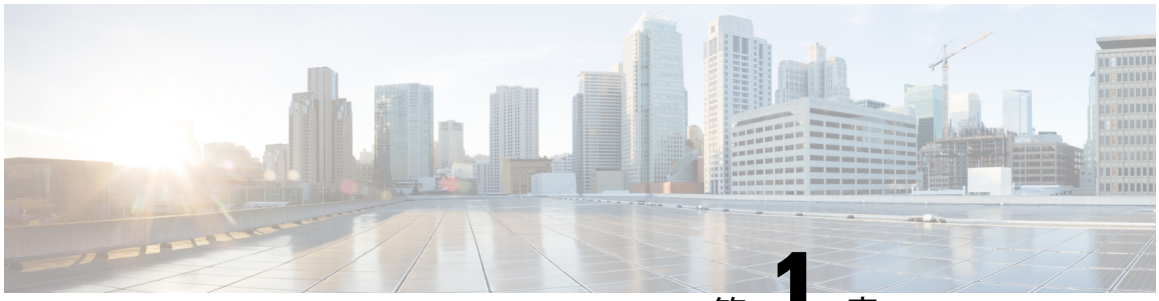
- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、Cisco Services にアクセスしてください。
- サービス リクエストを送信するには、Cisco Support にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco DevNet [英語] にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

Cisco バグ検索ツール

シスコバグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。



第 1 章

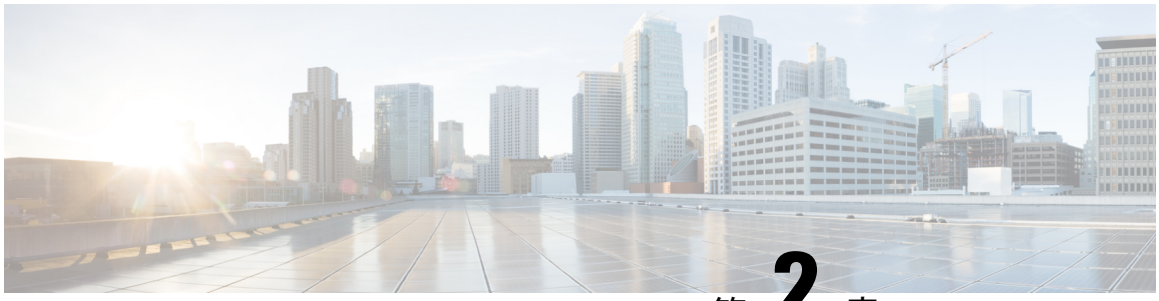
新機能と更新情報

新機能と更新情報

表 *1 : Cisco Nexus NX-OS* リリース *10.6(x)* の新機能および変更された機能

特長	説明	変更が行われたリリース	参照先
NA	このリリースで追加された新機能はありません。	10.6(1)F	該当なし

新機能と更新情報



第 2 章

概要

ライセンス要件

Cisco NX-OS を動作させるには、機能とプラットフォームの要件に従って適切なライセンスを取得し、インストールする必要があります。

- 基本（Essential）ライセンスとアドオンライセンスが、さまざまな機能セットに使用できます。
- ライセンスは、製品および購入オプションに応じて、永続的、一時的、または評価用のものがあります。
- 高度な機能を使用するには、基本ライセンス以外の追加の機能ライセンスが必要です。
- 高度な機能を使用するには、基本ライセンス以外の追加ライセンスが必要です。
- ライセンスの適用と管理は、デバイスのコマンドライン インターフェイス（CLI）を介して行われます。

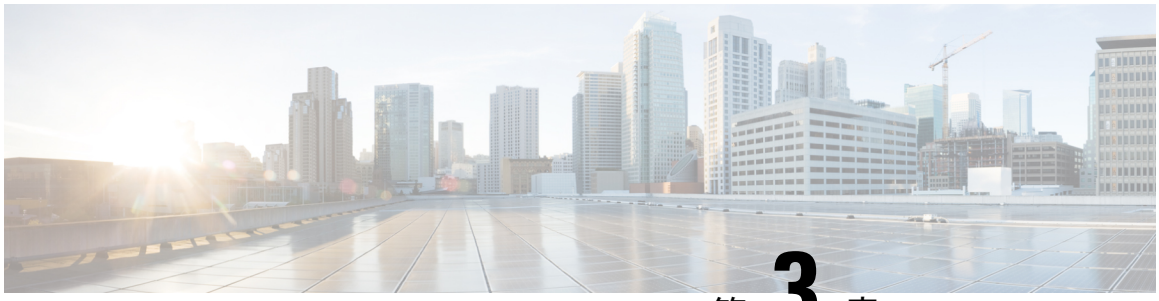
ライセンス タイプとインストールの手順の詳細については、『*Cisco NX-OS* ライセンシング ガイド』および『*Cisco NX-OS* ライセンシング オプション ガイド』を参照してください。

サポートされるプラットフォーム

Nexus スイッチプラットフォーム サポート マトリックスには、次のものがリストされています。

- サポートされている Cisco Nexus 9000 および 3000 スイッチ モデル
- NX- OS ソフトウェア リリース バージョン

プラットフォームと機能の完全なマッピングについては、『Nexus Switch Platform Support Matrix』を参照してください。



第 3 章

ePBR L3 の構成

この章では、Cisco NX-OS デバイスで 拡張済みポリシーベース リダイレクト（ePBR）を構成する方法について説明します。

ePBR L3 に関する情報

Elastic Services Re-direction（ESR）の Enhanced Policy-based Redirect（ePBR）は、ポリシーベースのリダイレクト ソリューションを活用することで、NX-OX およびファブリック トポロジ全体でトラフィック リダイレクトとサービスチェーンを可能にします。余分なヘッダーを追加せずにサービスチェーンを可能にし、余分なヘッダーを使用する際の遅延を回避します。

ePBR は、アプリケーション ベースのルーティングを可能にし、アプリケーションのパフォーマンスに影響を与えることなく、柔軟でデバイスに依存しないポリシーベースのリダイレクト ソリューションを提供します。ePBR サービス フローには、次のタスクが含まれます。

ライセンス要件

Cisco NX-OS を動作させるには、機能とプラットフォームの要件に従って適切なライセンスを取得し、インストールする必要があります。

- 基本（Essential）ライセンスとアドオンライセンスが、さまざまな機能セットに使用できます。
- ライセンスは、製品および購入オプションに応じて、永続的、一時的、または評価用のものがあります。
- 高度な機能を使用するには、基本ライセンス以外の追加の機能ライセンスが必要です。
- 高度な機能を使用するには、基本ライセンス以外の追加ライセンスが必要です。

- ライセンスの適用と管理は、デバイスのコマンドライン インターフェイス（CLI）を介して行われます。

ライセンス タイプとインストールの手順の詳細については、『*Cisco NX-OS* ライセンシング ガイド』および『*Cisco NX-OS* ライセンシング オプション ガイド』を参照してください。

ePBR サービスとポリシーの構成

まず、サービスエンドポイントの属性を定義するePBRサービスを作成する必要があります。サービスエンドポイントは、スイッチに関連付けることができるファイアウォール、IPSなどのサービス アプライアンスです。また、サービス エンド ポイントの状態を監視するプローブを定義したり、トラフィック ポリシーが適用されるフォワード インターフェイスと reverse インターフェイスを定義することもできます。また ePBR は、サービスチェーンとともにロードバランシングもサポートします。 ePBR を使用すると、サービス構成の一部として複数のサービス エンド ポイントを構成できます。

サービス端末の障害が発生した場合、障害が発生したサービスエンドポイントにリダイレクトされていたトラフィックは、ePBR サービスで構成された他の到達可能なサービス エンドポイントにリダイレクトされます。復元力のあるハッシュは、複数のサービスエンドポイントで展開されたePBRサービスのエンドポイント障害時にサポートされます。常に特定のサービス エンドポイントにリダイレクトされていたトラフィックは、同じサービスの他のサービスエンドポイントで障害が発生した場合でも、同じデバイスに引き続きリダイレクトされます。

Cisco NX-OS リリース 10.2(1)F 以降、チェーン内のすべてのサービスの VRF は、一意であるか、完全に同一である可能性があります。サービスに定義されたサービスエンドポイントとインターフェイスは、サービスに定義された VRF に関連する必要があります。

既存のIPv4 PBRポリシーを持つサービス エンドポイント インターフェイスは、IPv4 ePBR サービス内では使用できません。同様に、既存の ipv6 PBR ポリシーを持つサービス エンドポイント インターフェイスは、IPv6 ePBR サービス内では使用できません。

ePBR サービスを作成したら、ePBR ポリシーを作成する必要があります。ePBR ポリシーを使用すると、トラフィックの選択、サービスエンドポイントへのトラフィックのリダイレクト、およびエンド ポイントの正常性障害に関するさまざまな fail-action メカニズムを定義できます。許可アクセス コントロール エントリ（ACE）を備えた IP access-list エンド ポイントを使用して、一致する対象のトラフィックを定義し、適切なアクションを実行できます。

ePBRポリシーは、複数のACL一致定義をサポートします。一致には、シーケンス番号によって順序付けできるチェーンに複数のサービスを含めることができます。これにより、単一のサービス ポリシーでチェーン内の要素を柔軟に追加、挿入、および変更できます。すべてのサービス シーケンスで、ドロップ、転送、バイパスなどの失敗時のアクション メソッドを定義できます。ePBR ポリシーを使用すると、トラフィックの詳細なロード バランシングを行うために、送信元または接続先ベースのロード バランシングとバケット数を指定できます。

ePBR のインターフェイスへの適用

ePBR ポリシーを作成したら、インターフェイスにポリシーを適用する必要があります。これにより、トラフィックが NX-OS または Nexus ファブリックに入るインターフェイスを定義できます。順方向と逆方向の両方にポリシーを適用することもできます。インターフェイスに適用される IPv4/IPv6 ポリシーは、順方向と逆方向の 2 つだけです。

Cisco NX-OS リリース 10.2(1)F 以降、ePBR はレイヤ 3 ポートチャネル サブインターフェイスでのポリシー アプリケーションをサポートしています

Cisco NX-OS リリース 10.2(1)F 以降、ePBR ポリシーが適用されるインターフェイスは、チェーン内のサービスの VRF とは異なる VRF にある場合があります。

ePBR IPv4 ポリシーは、IPv4 PBR ポリシーがすでに適用されているインターフェイスには適用できません。 ePBR IPv6 ポリシーは、IPv6 PBR ポリシーがすでに適用されているインターフェイスには適用できません。

バケットの作成およびロード バランシング

ePBR は、チェーン内でサービスエンドポイントの最大数を持つサービスに基づいてトラフィック バケットの数を計算します。ロード バランス バケットを構成する場合は事前に行ってください。ePBR は送信元 IP および接続先 IP のロード バランシングをサポートしますが、L4 ベースの送信元または接続先のロード バランシング メソッドはサポートしていません。

ePBR サービス エンドポイント アウトオブサービス

ePBR サービス エンド ポイントのアウト オブ サービス機能には、エンドポ イントをサービスから一時的に削除するオプションがあります。次の 2 つの方法を使用して、エンドポイントをアウト オブサービスに移行できます。

1. **[管理アウトオブサービス（Administrative Out-of-Service）]**：この方法は、メンテナンス中またはアップグレード中に、サービス エンドポイントを一時的に運用ダウン状態に移行し、ノードへのトラフィックの送信を回避しながら、サービス中の有効なエンドポイント デバイスとしてサービス エンド ポイントを維持するために使用されます。

   また、メンテナンス手順の完了後に、Cisco NX-OS スイッチでサービス エンド ポイントをインサービスに戻す機能も必要です。これは、今日の業界のロードバランサで使用される標準規格です。

2. **[自動アウトオブサービス（Auto Out-of-Service）]**：この方法は、障害発生後のエンドポイントの回復中に使用され、ePBR は再確立されたエンドポイントの到達可能性を検出し、フローのサブセットをノードにリダイレクトしようとします。

   また、特定のネットワークがまれなエンドポイントの障害と回復に耐性がある場合でも、接続を失い、接続を再確立しているエンドポイントを検出する必要がある場合、各イベントはエンドツーエンド接続を 2 回中断します。このようなノードをアウトオブサービスにすることが望ましい場合があります。

ePBR オブジェクト トラッキング、ヘルスモニタリング、および Fail-Action

ePBR は、サービスで構成されたプローブ タイプに基づいて SLA およびトラック オブジェクトを作成し、ICMP、TCP、UDP、DNS、HTTP などのさまざまなプローブとタイマーをサポートします。 ePBR はユーザ定義のトラックもサポートしており、ePBR に関連するミリ秒プローブを含むさまざまなパラメータでトラックを作成できます。

ePBR プローブ構成を適用する場合、ePBR は IP SLA プローブをプロビジョニングすることによりエンドポイントの正常性をモニタし、オブジェクトをトラックして IP SLA の到達可能性をトラックします。

サービス向け、または転送または reverse の各エンドポイント向けに、ePBR プローブ オプションを構成することが可能です。また、IP SLA セッションの送信元 IP に使用できるように、頻度、タイムアウト、再試行のアップ カウントとダウン カウント、および送信元ループバック インターフェイスを構成できます。リトライアップとダウンのカウントは、 **遅延アップ** と **遅延ダウンの**間隔を決定する頻度の乗数として使用されます。サービスエンドポイントが最初に障害または回復として検出されると、システムはこれらの間隔の満了後にこれらのイベントに対処します。任意のタイプのトラックを定義し、順方向または逆方向エンドポイントに関連付けることができます。同じトラック オブジェクトが、同じ ePBR サービスを使用するすべてのポリシーに再利用されます。

トラックを個別に定義し、ePBR の各サービス エンド ポイントにトラック ID を割り当てることができます。ユーザ定義のトラックをエンドポイントに割り当てない場合、ePBR はエンドポイントのプローブ メソッドを使用してトラックを作成します。エンドポイント レベルで定義されているプローブ メソッドがない場合、サービスレベルで構成されるプローブ メソッドを使用できます。

ePBR は、自身のサービスチェーンのシーケンスで次の fail-action メカニズムをサポートします。

- バイパス
- ドロップオンフェイル
- 転送

サービス シーケンスのバイパスは、現在のシーケンスで障害が発生した場合に、トラフィックは次のサービス シーケンスにリダイレクトされる必要があることを示しています。

サービス シーケンスのドロップオンフェイルは、サービスのすべてのサービスエンドポイントが到達不能となる場合に、トラフィックはドロップされる必要があることを示しています。

転送はデフォルトのオプションであり、現在のサービスに障害が発生した場合、トラフィックは通常のルーティング テーブルを使用する必要があることを示します。これはデフォルトの fail-action メカニズムです。

（注） 対称性が維持されるのは、fail-action バイパスがサービスチェーン内のすべてのサービス向けに構成された場合です。その他の fail-action シナリオでは、1 つまたはそれ以上の機能不全サービスが存在する場合、転送または reverse フローでの対称性は維持されません。

ePBR セッションベースの構成

ePBR セッションにより、次のサービス内のアスペクトのサービスまたはポリシーの追加、削除、変更が可能になります。サービス内とは、アクティブインターフェイスまたはポリシーに適用されているポリシーに関連付けられたサービスを示し、アクティブインターフェイス上で変更される、現在構成済みのサービスを示します。

- インターフェイスおよびプローブを備えたサービスエンドポイント
- reverse エンドポイントおよびプローブ
- ポリシーで一致
- 一致させるための負荷分散メソッド
- 一致シーケンスおよび fail-action

（注） ePBR セッションで、同じセッション内で 1 つのサービスから別のサービスにインターフェイスを移動することはできません。1 つのサービスから別のサービスにインターフェイスを移動させるには、次の手順を行います。

1. まず初めに、既存のサービスからインターフェイスを削除するための 1 つ目のセッションを実行します。
2. 既存のサービスにインターフェイスを追加するための 2 つ目のセッションを実行します。

ePBR マルチサイト

Cisco NX-OS リリース 10.2(1)F 以降、VXLAN マルチサイト ファブリックでのサービスチェーンは、次の構成およびトポロジ ガイドラインを使用して実現できます。

- サービス内のエンドポイントまたはチェーン内のサービスは、同じサイトまたは異なるサイト内の異なるリーフスイッチに分散される場合があります。
- すべてのサービスは、ePBR ポリシーが適用されるテナント VRF コンテキストとは異なる一意の VRF にある必要があります。
- 異なるテナント VRF のトラフィックを分離するには、サービスに使用される VLAN を分離し、新しいサービスとポリシーを定義する必要があります。

- テナント VRF ルートは、サービスをホストするすべてのリーフスイッチの各サービス VRF にリークする必要があります。これにより、トラフィックがサービスチェーンの最後でテナント VRF 内の接続先にルーティングされるようになります。
- VNI は、さまざまなリーフスイッチおよびサイトに対称的に割り当てる必要があります。
- ePBR ポリシーは、使用されているサービス VRF のすべてのレイヤー 3 VNI、サービスをホストしているすべてのリーフスイッチ、およびマルチサイトのトランジットとして機能している場合はボーダー リーフまたはボーダーゲートウェイ スイッチで有効にする必要があります。
- サービスチェーンが 1 つのサイトに完全に分離され、トラフィックがさまざまなサイトから着信する場合があります。このシナリオにはサービスデバイスのマルチサイト配布は含まれませんが、ボーダーゲートウェイまたはボーダーリーフ上のサービス VRF のレイヤー 3 VNI は、マルチサイト トランジットとしてのみ扱う必要があり、ePBR ポリシーをそれらに適用する必要があります。ePBR ポリシーは、トラフィックが着信するリモートサイトのホストまたはテナントに面したインターフェイスにも適用する必要があります。

ACL リフレッシュ

ePBR セッション ACL リフレッシュにより、ユーザが入力した ACL がACE を使用して変更、追加、または削除される場合に、ACL を生成するポリシーを更新することができるようになります。リフレッシュ トリガーで、ePBR はこの変更によって影響を受けるポリシーを特定し、それらのポリシー向けに ACL を生成するバケットを作成、削除、または変更します。

ePBR のスケール数については、『Cisco Nexus 9000 Series NX-OS Verified Scalability Guide』を参照してください。

ePBR L3 の注意事項および制約事項

ePBR には、次の注意事項と制限事項 があります。

- L3 ePBR 機能が正しく機能するには、十分な ing-racl TCAMが必要です。現在の TCAM カービングを確認するには、**show hardware access-list tcam region** コマンドを使用します。適切な TCAM サイズが割り当てられていない場合は、 **hardware access-list tcam region ing-racl** *256* の倍数のサイズ コマンドを使用して、適切な TCAM サイズを割り当てます。
- Cisco Nexus NX-OS リリース 10.1(2) 以降、IPv4 および IPv6 を使用した ePBR は N9K-C93108TC-FX3P スイッチでサポートされます。
- Cisco NX-OS リリース 10.1(1) 以降、ePBR ポリシーの各一致ステートメントは、リダイレクト、ドロップ、および除外の 3 つのアクション タイプをサポートできます。ポリシーごとにドロップまたは除外の一致ステートメントを 1 つだけ指定できます。順方向および逆方向で除外またはドロップする必要があるトラフィックの ACE ルールは、除外またはドロップのアクションで使用される match アクセスリストに手動で追加する必要がありま

す。exclude および drop match アクセス リストの統計情報には、両方向のトラフィック ヒット カウンタが表示される場合があります。

- ePBR ポリシーには、リダイレクト アクションとの一致が少なくとも 1 つ必要です。
- Cisco NX-OS リリース 10.1（1）以降、IPv4、IPv6、および VXLAN 上の ePBR を使用した ePBR は、次のプラットフォーム スイッチでサポートされます：N9K-C9316D-GX、N9K-C93600CD-GX、N9K-C9364C-GX、N9K-C93180YC FX3S、N9K-C93360YC-FX3 と N9K-C93108TC-FX3P。
- fail-action がいずれかの一致ステートメントで指定されている場合、プローブは構成内に存在していることが必須です。
- OTM トラックの変更がある場合は常に、RPM の再プログラミングにより ePBR 統計がリセットされます。
- ePBR 構成内の複数の一致ステートメント全体で同じユーザ定義 ACL を共有しないでください。
- トラフィックの対称性が維持されるのは、fail-action バイパスが ePBR サービス向けに構成されたときのみです。サービスチェーン内の転送/ドロップなどのその他の fail-action の場合、トラフィックの順方向と逆方向のフローの対称性は維持されません。
- match access-list の定義に従ってトラフィックが任意の送信元 IP および s送信先 IP と一致する必要があり、VXLAN 環境に分散されたデバイスにリダイレクトする必要がある場合は、一意のレイヤ 4 送信元および宛先ポートパラメータを一致フィルタに指定する必要があります。順方向と逆方向の両方で、またはワンアームデバイスを介してサービスチェーンされます。
- 機能 ePBR および機能 ITD は同じ入力インターフェイスと共存できません。
- 拡張済み ePBR 構成では、**no feature epbr** コマンド を使用する前にポリシーを削除することが推奨されています。
- プローブ トラフィックを別の CoPP クラスに分類することが推奨されています。そうしないと、プローブ トラフィックはデフォルトの CoPP クラスになり、ドロップされる可能性があり、プローブ トラフィックの IP SLA バウンスが発生します。CoPP 構成について詳しくは、「IP SLA パケットの CoPP の構成」を参照してください。
- ePBR は、EX、FX、および FX2 ラインカードを備えた Cisco Nexus 9500 および Cisco Nexus 9300 プラットフォーム スイッチでサポートされています。
- Cisco NX-OS リリース 9.3(5) 以降、Catena 機能は廃止されました。
- システムから削除されたポートチャネルに構成された ePBR サービスエンドポイントを削除する場合、次の手順を実行してください。

1. 既存の ePBR ポリシーを削除します。
2. 既存の ePBR サービスを削除します。
3. ePBR サービス エンドポイントを必要なポートチャネルに再構成します。

- 「epbr_」という名前で始まる、動的に作成された ePBR の access-list エントリは変更しないでください。これらの access-lists は ePBR 内部使用向けに予約済みです。

（注） これらのプレフィックス文字列を変更すると ePBR が正しく機能せず、ISSU に影響を与える可能性があります。

- ルータ ACL は、サポートされているレイヤ 3 インターフェイスでレイヤ 3 ePBR ポリシーとともに有効にできます。この制限の詳細については、『**Cisco Nexus 9000 シリーズ NX-OS ユニキャスト ルーティング構成ガイド**』の「ポリシーベース ルーティング」の章にある「ポリシーベース ルーティングの注意事項と制限事項」を参照してください。
- Cisco Nexus N9K-C9316D-GX、N9K-C93600CD-GX、および N9K-C9364C-GX スイッチでは、Cisco NX-OS、リリース 10.2 以降のリリースからリリース 10.1 への ISSD を実行する前に、ePBR ポリシーを無効にして、ダウングレードを続行します。
- ePBR ポリシー定義は、順方向および逆方向でサポートされているインターフェイス タイプの最大 32 個のインターフェイスに適用できます。
- Cisco NX-OS リリース 10.4（1）F 以降、ePBR は、Cisco Nexus 9300-FX2/FX3/GX/GX2 プラットフォーム スイッチでのロードバランシングとリダイレクションのために、GRE および IP-IP トンネル インターフェイスで IPv4 および IPv6 ポリシーをサポートします：
- Cisco NX-OS リリース 10.4（1）F 以降、ePBR は、Cisco Nexus 9300-FX2/FX3/GX/GX2 プラットフォーム スイッチの IP-IP および GRE トンネル インターフェイスを介して到達可能なレイヤ3エンドポイントへのリダイレクションまたはロードバランシングをサポートします。

（注）
- ePBR IPv6 ポリシーは、IP-IP トンネル インターフェイスではサポートされません。
- 現在、ePBR は、IP-IP および GRE トンネルを介して到達可能なデバイスへのサービスチェーンをサポートしていません。

- 構成のロールバックと設定の置換は、ePBR ポリシーがインターフェイスに関連付けられておらず、ePBR サービス定義が送信元設定とターゲット設定の両方のアクティブな ePBR ポリシーで使用されていない場合にのみサポートされます。ただし、構成のロールバックと構成の置換では、ポリシーとインターフェイスの関連付けおよび関連付け解除はサポートされません。
- アトミック アップデートを無効にすると、より多くの TCAM リソースを ePBR ポリシーで使用できるようになりますが、ポリシーの構成変更中、またはサービス エンドポイントのフェイルオーバーとリカバリ中に、トラフィック中断の原因となる可能性があります。詳細については、*Cisco Nexus 9000* シリーズ *NX-OS* セキュリティ設定ガイドの**アトミック ACL 更新**を参照してください。

- ePBR ポリシーが設定されているすべてのインターフェイスに対して、一意のポリシーが生成されます。さらに、ePBR ポリシー内で一致するように構成されたサービスチェーン内の次のサービス機能にトラフィックを誘導する必要があるすべてのサービス インターフェイスに対して、一意のポリシーも生成されます。サポートされる EPBR ポリシーの規模は、PBR ポリシーのシステムで使用可能な ACL ラベルによって異なる場合があります。ACL ラベル サイズの詳細については、 *Cisco Nexus 9000* シリーズ *NX-OS* セキュリティ構成ガイドの **ACL タイプでサポートされる最大ラベルサイズ**の項を参照してください。
- 使用される ePBR サービスまたはエンドポイント保留タイマーは、使用中のプローブ（トラックおよび IP SLA）の頻度およびタイムアウトと互換性がある必要があります。これにより、障害を時間内に検出できます。
- デュアルアーム デバイスのフォワード アームとリバース アームのエンドポイントの状態は、自動的に同期されません。これが必要な場合は、フォワード アームとリバース アームで同じプローブ トラック構成を使用する必要があります。エンドポイント用に設定されたプローブ トラックは、同じエンドポイントのフォワード アームとリバース アームの間で共有できますが、同じサービスまたは異なるサービスのエンドポイント間では共有できません。
- Cisco NX-OS リリース 10.5(1)F 以降では、ワンアーム サービス デバイスのリバース IP アドレスを明示的に構成する必要はなくなりました。サービス エンドポイントにリバース IP アドレスが割り当てられていない場合、ワンアームデバイスとして扱われ、トラフィックは順方向と逆方向の両方で同じ IP アドレスにリダイレクトされます。
- サービス プローブに関連付けられているループバック インターフェイスの IP アドレスが変更された場合は、サービスを参照するポリシーとコントラクトを削除して再適用する必要があります。
- Cisco NX-OS リリース 10.5(2)F 以降、ePBR は、Cisco Nexus 9300-FX2、FX3、GX、GX2、H2R、および H1 シリーズ スイッチの指定された VRF インスタンスを介してパケットをリダイレクトする **set-vrf** コマンドをサポートしますが、次の制限があります：
  - **source-vrf** および **destination-vrf** は、ePBR セッションを介して変更または削除することはできません。
  - **set-vrf** はVXLAN 上の ePBR ではサポートされていません。
  - **set-vrf** は、ドロップおよび除外トラフィックの VRF を切り替えません。

次の注意事項および制約事項を VXLAN 上での ePBR 機能に適用します。

- VXLAN ファブリックでは、同じ VLAN 内のデバイスに対してサービスチェーンを実行できません。すべてのデバイスは、個別の VLAN に存在する必要があります。
- チェーン内のすべてのサービスが同じ VRF にある場合、ePBR は VXLAN マルチサイト ファブリックの単一サイトでのみサポートされます。
- チェーン内のすべてのサービスが同じ VRF にある場合：

- アクティブ/スタンバイ チェーンは、制限のない 2 つのサービス ノードでサポートされます。
- チェーン内に3つ以上のサービス ノードがあるアクティブ/スタンバイ チェーンでは、同じサービス リーフの背後にあるタイプの異なる 2 つのノードは必要ありません。
- VXLAN ファブリックでは、リーフ内の 1 つのサービスからのトラフィックをステッチして、後で同じリーフに戻ってくることはできません。

（注） チェーン内のすべてのサービスが異なる VRF コンテキストにある場合、これらの制限は適用されません。

- サービス エンドポイントが VXLAN 環境または VPC ピアに分散されている場合、サービス エンドポイントはすべてのスイッチで同じ順序で構成する必要があります。
- VXLAN環境に分散されたサービスエンドポイントの場合、一意の送信元IPをIP SLAセッションに使用できるように、プローブの送信元ループバック インターフェイスを設定する必要があります。
- ePBR ポリシーは、最初は常にホストまたはテナントに面したインターフェイスに適用する必要があります。ePBR ポリシーは、トランジット インターフェイスとしてのみ、テナントまたはサービス VRF に関連するレイヤ 3 VNI インターフェイスに適用する必要があります。

  特定の VRF のエンドポイントに着信するトラフィックのみが、その VRF に関連するレイヤ 3 VNI インターフェイスに適用されるポリシーによってリダイレクトされます。レイヤ 3 VNI インターフェイスのポリシーに一致するトラフィックの統計情報は、ePBR statistics コマンドでは表示されません。
- Cisco NX-OS リリース 10.3（3）F 以降では、Cisco Nexus 9300-FX、9300-FX2、9300-FX3、9300-GX、および9300-GX2 プラットフォーム スイッチ、の新しい L3VNI インターフェイスに ePBR レイヤ 3 ポリシーを適用できます。

次の注意事項および制約事項を一致 ACL 機能に適用します。

- permit メソッドを持つ ACE のみが ACL でサポートされます。他の方法（deny または remark など）の ACE は無視されます。
- 1 つの ACL で最大 256 の許可 ACE がサポートされます。
- 送信元パラメータまたは宛先パラメータのいずれかでアドレス グループまたはポート グループとして指定されたオブジェクト グループを持つ ACE はサポートされません。
- Cisco NX-OS リリース 10.4（1）F 以降では、match access-list ルールのレイヤ 4 ポート範囲およびその他のポート操作（「等しくない」、「より大きい」、「より小さい」など）は、バケットアクセスリスト内のトラフィックのフィルタリングに使用されます。

- アクセスリストでレイヤ 4 ポートオペレータを使用しながら、TCAM ACE の使用率を最適化するには、この構成 **hardware access-list lou resource threshold**を使用する必要があります。このコマンドの詳細については、『*Cisco Nexus 9000* シリーズ *NX-OS* セキュリティ構成ガイド』の「**IP ACL の構成**」のセクションを参照してください。

次のガイドラインと制限事項が VRF 間のサービスチェーンに適用されます。

- Cisco NX-OS 10.2(1)F リリース以降、チェーン内のすべてのサービスは、同じ VRF または完全に一意の VRF に存在する必要があります。
- バージョン 10.2(1)F では、チェーン内のすべてのサービスが一意の VRF に存在する場合、fail-action アクション バイパス メカニズムはサポートされません。
- Cisco NX-OS 10.2(2)F リリースから、チェーン内のサービスが一意の VRF にある場合に fail-action アクション バイパスがサポートされます。
- サービスが、ePBR ポリシーが適用されるインターフェイスの VRF コンテキストとは異なる VRF にある場合、ユーザは、テナント ルートがすべてのサービス VRF にリークされていることを確認して、トラフィックがサービスチェーンの最後にあるテナント VRF にルート バックできるようにする必要があります。
- Cisco NX-OS リリース 10.2(2)F 以降、PBR では、異なる VRF に関連する複数のバックアップ ネクストホップをルート マップ シーケンスに構成できます。これにより、ePBR は、ある VRF に関連するサービスから別の VRF への fail-action バイパスを効果的に有効にすることができます。
- Cisco NX-OS リリース 10.2(3)F 以降、エンドポイントの追加、サービス シーケンスの追加、削除および変更のセッション操作中のトラフィックの中断を最小限にするために、事前にロードバランス バケットの構成を行い、ロードバランス構成への変更を回避することが推奨されています。ロードバランス向けに構成されたバケットの数が、チェーン内の各シーケンス向けのサービスで構成されたエンドポイントの数より多くなるようにしてください。

送信元 IP ベースのロード バランシングを使用して ePBR を構成した場合は、次の注意事項と制限事項が適用されます。

- ACE の送信元 IPv4 のプレフィックス長を /32 にすることはできません
- ACE の送信元 IPv6 アドレスのプレフィックス長を /128 にすることはできません
- 送信元アドレスのサブネットは、構成されたバケットと互換性がある必要があります。

送信先 IP ベースのロード バランシングを使用して ePBR を構成した場合は、次の注意事項と制限事項が適用されます：

- ACE の送信先 IPv4 のプレフィックス長を /32 にすることはできません
- ACE の送信先 IPv6 アドレスのプレフィックス長を /128 にすることはできません
- 送信先アドレスのサブネットは、構成されたバケットと互換性がある必要があります。

ePBR サービス エンドポイントのアウトオブサービス機能を構成している場合は、次の注意事項と制限事項が適用されます。

- ePBR サービスエンドポイントのアウトオブサービス機能は、Cisco Nexus 9300-FX/FX2/FX3/GX/GX2および X97160YC-EX、9700-FX/GX ライン カードを搭載した isco Nexus 9500 スイッチのレイヤ 3 サービスでサポートされます。
- ePBR アウトオブサービス（シャットダウンまたはホールドダウン）では、エンドポイントレベルまたはサービスレベルのいずれかで、エンドポイントにプローブを構成する必要があります。
- サービスがアクティブなポリシーによって使用されている場合、ePBR アウトオブサービス（シャットダウンまたはホールドダウン）は、 **epbr sessions**のみを使用して設定する必要があります。

送信元 IP ベースのロード バランシングおよび複数のエンドポイントへのロード バランシング トラフィックを使用する場合は、次のガイドラインと制限事項が適用されます。

- match access-list 内の ACE の送信元 IPv4 サブネット マスクを /32、または match access-list 内の送信元 IPv6 アドレスのサブネット マスクを /128 にすることはできません。
- match access-list 内の ACE の接続先 IPv4 サブネット マスクを /32、または match access-list 内の送信元 IPv6 アドレスのサブネット マスクを /128 にすることはできません。
- ロードバランシング メソッドに基づく、一致アクセスリスト内の送信元アドレスまたは接続先アドレスのサブネットマスクは、一致に使用されるサービスのエンドポイント数に基づき、一致するように構成されたバケットと互換性を持つか、必要なバケット数と互換性を持つか必要があります。

ePBR L3 の構成

はじめる前に

ePBR 機能を構成する前に、IP SLA および PBR 機能が構成されていることを確認してください。

ePBR サービス、ポリシーの構成およびインターフェイスへの関連付け

次のセクションでは、ePBR サービス、ePBR ポリシーの構成、およびインターフェイスへのポリシーの関連付けについて説明します。

手順の概要

1. **configure terminal**
2. **epbr service** *service-name*

3. [**no**] **probe** {**icmp** | *l4-proto port-number* [**control** *status*] | **http get** [*url-name* [**version** *ver*] | **dns host***host-name* **ctp**} [**frequency** *freq-num* | **timeout** *seconds* | **retry-down-count** *down-count* | **retry-up-count** *up-count* | **source-interface** *src-intf* | **reverse** *rev-src-intf*]
4. **vrf** *vrf-name*
5. **service-endpoint** {**ip** *ipv4 address* | **ipv6** *ipv6 address*} [**interface** *interface-name interface-number*]
6. **probe track** *track ID*
7. **reverse ip** *ip address* **interface** *interface-name interface-number*
8. **exit**
9. **epbr policy** *policy-name*
10. **match** { [**ip address** *ipv4 acl-name*] | [**ipv6 address** *ipv6 acl-name*] } [**redirect** | **drop** | **exclude**]
11. [**no**] **load-balance** [**method** { **src-ip** | **dst-ip**}] [**buckets** *sequence-number*] [**mask-position** *position-value*]
12. *sequence-number* **set service** *service-name* [**fail-action** { **bypass** | **drop** | **forward**}]
13. **interface** *interface-name interface-number*
14. **epbr** { **ip** | **ipv6**} **policy** *policy-name* [**reverse**]
15. **exit**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**epbr service** *service-name* 例： `switch(config)# epbr service firewall`	新しい ePBR サービスを作成します。
ステップ 3	[**no**] **probe** {**icmp**	*l4-proto port-number* [**control** *status*]	**http get** [*url-name* [**version** *ver*]	**dns host***host-name* **ctp**} [**frequency** *freq-num*	**timeout** *seconds*	**retry-down-count** *down-count*	**retry-up-count** *up-count*	**source-interface** *src-intf*	**reverse** *rev-src-intf*] 例： `switch(config)# probe icmp`	ePBR サービスのプローブを構成します。サポートされるプローブ タイプは、ICMP、TCP、UDP、DNS、および HTTP、CTP です。 オプションは次のとおりです。 • 頻度：プローブの頻度を秒単位で指定します。値の範囲は 1 ～ 604800 です。 • 再試行ダウン カウント：ノードがダウンしたときにプローブによって実行される再カウントの数を指定します。指定できる範囲は1～5です。

	コマンドまたはアクション	目的
		• 再試行アップ カウント：ノードが復帰したときにプローブが実行する再カウントの数を指定します。指定できる範囲は 1 ～ 5 です。 • タイムアウト：タイムアウト期間を秒単位で指定します。値の範囲は 1 ～ 604800 です。
ステップ 4	**vrf** *vrf-name* 例： `switch(config)# vrf tenant_A`	ePBR サービスの VRF を指定します。
ステップ 5	**service-endpoint** {**ip** *ipv4 address* | **ipv6** *ipv6 address*} [**interface** *interface-name interface-number*] 例： `switch(config-vrf)# service-endpoint ip 172.16.1.200 interface VLAN100`	ePBR サービスのサービスエンドポイントを構成します。 手順 2 ～ 5 を繰り返して、別の ePBR サービスを構成できます。
ステップ 6	**probe track** *track ID* 例： `switch(config-vrf)# probe track 30`	トラックを個別に定義し、ePBR の各サービス エンドポイントに既存のトラック ID を割り当てます。 各エンドポイントにトラック ID を割り当てることができます。
ステップ 7	**reverse ip** *ip address* **interface** *interface-name interface-number* 例： `switch(config-vrf)# reverse ip 172.16.30.200 interface VLAN201`	トラフィック ポリシーが適用される reverse IP とインターフェイスを定義します。 （注） Cisco NX-OS リリース 10.5(1)F 以降では、ワンアーム サービス デバイスのリバース IP アドレスを明示的に構成する必要はなくなりました。サービス エンドポイントにリバース IP アドレスが割り当てられていない場合、ワンアーム デバイスとして扱われ、トラフィックは順方向と逆方向の両方で同じ IP アドレスにリダイレクトされます。
ステップ 8	**exit** 例： `switch(config-vrf)# exit`	VRF コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 9	**epbr policy** *policy-name* 例： `switch(config)# epbr policy Tenant_A-Redirect`	ePBR ポリシーを構成します。

	コマンドまたはアクション	目的
ステップ 10	**match** { [**ip address** *ipv4 acl-name*] | [**ipv6 address** *ipv6 acl-name*] } [**redirect** | **drop** | **exclude**] 例： `switch(config)# match ip address WEB`	IPv4 または IPv6 アドレスを IP、または IPv6 ACL と照合します。リダイレクトは、一致トラフィックのデフォルト アクションです。ドロップは、着信インターフェイスでトラフィックをドロップする必要がある場合に使用されます。除外オプションは、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するために使用されます。 この手順を繰り返して、要件に基づいて複数の ACL を一致させることができます。
ステップ 11	[**no**] **load-balance** [**method** { **src-ip** | **dst-ip**}] [**buckets** *sequence-number*] [**mask-position** *position-value*] 例： `switch(config)# load-balance method src-ip mask-position 3`	ePBR サービスで使用されるロードバランス メソッドとバケット数を計算します。 Cisco NX-OS リリース 10.3（3）F 以降では、ユーザー定義 ACL でロードバランシングに使用されるビットを選択する**mask-position** オプションが提供されています。デフォルト値は 0 です。 mask-position が構成されている場合、ロードバランス ビットは構成された mask-position から始まります。必要なバケットの数に基づいて、最上位ビットに向かって、より多くのビットがロード バランシング バケットを生成するために使用されます。 （注） ユーザー定義の ACL 内の ACE では、ロード バランシング バケットの生成に使用されるビットがユーザー定義のサブネットと重複している場合、ACE のマスク位置は内部的に 0 にリセットされます。
ステップ 12	*sequence-number* **set service** *service-name* [**fail-action** { **bypass** | **drop** | **forward**}] 例： `switch(config)# set service firewall fail-action drop`	fail-action メカニズムを計算します。

ステップ 13	**interface** *interface-name interface-number*
	例：
	`switch(config)# interface vlan 2010`
	`switch(config)# interface vni500001`
		インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
		（注）
		Cisco NX-OS リリース 10.3（3）F 以降では、新しい L3VNI インターフェイスに ePBR L3 ポリシーを適用できます。

	コマンドまたはアクション	目的
ステップ 14	**epbr** { **ip** | **ipv6**} **policy** *policy-name* [**reverse**] 例： `switch(config-if)# epbr ip policy Tenant_A-Redirect`	インターフェイスは、いつでも次の1つ以上に関連付けることができます。 • 順方向の IPV4 ポリシー • 逆方向の IPv4 ポリシー • 順方向の IPv6 ポリシー • 逆方向の IPv6 ポリシー
ステップ 15	**exit** 例： `switch(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

ePBR セッションを使用したサービスの変更

次の手順では、ePBR セッションを使用してサービスを変更する方法を説明しています。

手順の概要

1. **epbr session**
2. **epbr service** *service-name*
3. [**no**] **service-endpoint** {**ip** *ipv4 address* | **ipv6** *ipv6 address*} [**interface** *interface-name interface-number*]
4. **service-endpoint** {**ip** *ipv4 address* | **ipv6** *ipv6 address*} [**interface** *interface-name interface-number*]
5. **reverse ip** *ip address* **interface** *interface-name interface-number*
6. **commit**
7. **abort**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**epbr session** 例： `switch(config)# epbr session`	ePBR セッション モードに入ります。
ステップ 2	**epbr service** *service-name* 例： `switch(config-epbr-sess)# epbr service TCP_OPTIMIZER`	ePBR セッション モードで構成する ePBR サービスを指定します。

	コマンドまたはアクション	目的
ステップ 3	[**no**] **service-endpoint** {**ip** *ipv4 address* | **ipv6** *ipv6 address*} [**interface** *interface-name interface-number*] 例： `switch(config-epbr-sess-svc)# no service-end-point ip 172.16.20.200 interface VLAN200`	ePBR サービス向けに構成されたサービスエンドポイントを無効にします。
ステップ 4	**service-endpoint** {**ip** *ipv4 address* | **ipv6** *ipv6 address*} [**interface** *interface-name interface-number*] 例： `switch(config-epbr-sess-svc)#service-end-point ip 172.16.25.200 interface VLAN200`	サービスエンドポイントを変更し、ePBR サービスの IP を置き換えます。
ステップ 5	**reverse ip** *ip address* **interface** *interface-name interface-number* 例： `switch(config-epbr-sess-svc-ep)# reverse ip 172.16.30.200 interface VLAN201`	トラフィック ポリシーが適用される reverse IP とインターフェイスを定義します。
ステップ 6	**commit** 例： `switch(config-epbr-sess)# commit`	ePBR セッションを使用した ePBR サービスの変更を完了します。 （注） このステップの完了後に ePBR セッションを再起動します。
ステップ 7	**abort** 例： `switch(config-epbr-sess)# abort`	セッションを中止し、セッションの現在の構成をクリアまたはリセットします。コミット中にエラーまたはサポートされていない構成が識別された場合に、現在のセッション構成を破棄するには、このコマンドを使用します。 （注） その後、修正した構成を使用して新しい ePBR セッションを再開します。

ePBR セッションを使用したポリシーの変更

次の手順では、ePBR セッションを使用してポリシーを変更する方法について説明します。

手順の概要

1. **epbr session**
2. **epbr policy** *policy-name*
3. [**no**] **match** { [**ip address** *ipv4 acl-name*] | [**ipv6 address** *ipv6 acl-name*] [**l2 address** *ipv6 acl-name*]} **vlan** {**vlan** | **vlan range** | **all**} [**redirect** | **drop** | **exclude**] }

4. **match** { [**ip address** *ipv4 acl-name*] | [**ipv6 address** *ipv6 acl-name*] [**l2 address** *ipv6 acl-name*]} **vlan** {**vlan** | **vlan range** | **all**} [**redirect** | **drop** | **exclude**] }
5. *sequence-number* **set service** *service-name* [**fail-action** { **bypass** | **drop** | **forward**}]
6. [**no**] **load-balance** [**method** { **src-ip** | **dst-ip**}] [**buckets** *sequence-number*] [**mask-position** *position-value*]
7. **commit**
8. **end**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**epbr session** 例： `switch(config)# epbr session`	ePBR セッション モードに入ります。
ステップ 2	**epbr policy** *policy-name* 例： `switch(config-epbr-sess)# epbr policy Tenant_A-Redirect`	ePBR セッション モードで構成する ePBR ポリシーを指定します。
ステップ 3	[**no**] **match** { [**ip address** *ipv4 acl-name*]	[**ipv6 address** *ipv6 acl-name*] [**l2 address** *ipv6 acl-name*]} **vlan** {**vlan**	**vlan range**	**all**} [**redirect**	**drop**	**exclude**] } 例： `switch(config-epbr-sess-pol)# no match ip address WEB`	IP または IPv6 ACL に対する IP アドレスの照合を無効にします。
ステップ 4	**match** { [**ip address** *ipv4 acl-name*]	[**ipv6 address** *ipv6 acl-name*] [**l2 address** *ipv6 acl-name*]} **vlan** {**vlan**	**vlan range**	**all**} [**redirect**	**drop**	**exclude**] } 例： `switch(config-epbr-sess-pol)# match ip address HR`	IP または IPv6 ACL に対する IP アドレスの照合を変更します。
ステップ 5	*sequence-number* **set service** *service-name* [**fail-action** { **bypass**	**drop**	**forward**}] 例： `switch(config-epbr-sess-pol-match)# set service firewall fail-action drop`	一致するシーケンスを追加、変更、または削除するか、既存のシーケンスの fail-action アクションを変更します。
ステップ 6	[**no**] **load-balance** [**method** { **src-ip**	**dst-ip**}] [**buckets** *sequence-number*] [**mask-position** *position-value*] 例： `switch(config-epbr-sess-pol-match)# load-balance method src-ip mask-position 3`	ePBR サービスで使用されるロードバランス メソッドとバケット数を計算します。 （注） 既存の一致のサービスチェーンを変更するときに、セッションコンテキストでこの構成を省略すると、

	コマンドまたはアクション	目的
		一致のロードバランス構成がデフォルトにリセットされます。 Cisco NX-OS リリース 10.3（3）F 以降では、ユーザー定義 ACL でロードバランシングに使用されるビットを選択する**mask-position** オプションが提供されています。デフォルト値は 0 です。 mask-position が構成されている場合、ロードバランス ビットは構成された mask-position から始まります。必要なバケットの数に基づいて、最上位ビットに向かって、より多くのビットがロードバランシング バケットを生成するために使用されます。 （注） ユーザー定義の ACL 内の ACE では、ロード バランシング バケットの生成に使用されるビットがユーザー定義のサブネットと重複している場合、ACE のマスク位置は内部的に 0 にリセットされます。
ステップ 7	**commit** 例： `switch(config-epbr-sess)#commit`	ePBR セッションを使用した ePBR サービスの変更を完了します。
ステップ 8	**end** 例： `switch(config-epbr-sess)#end`	ePBR セッション モードを終了します。

ePBR ポリシーによる使用される Access-list の更新

次の手順では、ePBR ポリシーで使用される access-list を更新する方法について説明します。

手順の概要

1. **epbr session access-list** *acl-name* **refresh**
2. **end**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**epbr session access-list** *acl-name* **refresh** 例： `switch(config)# epbr session access-list WEB refresh`	ポリシーによって生成された ACL を更新またはリフレッシュします。
ステップ 2	**end** 例： `switch(config)# end`	グローバル コンフィギュレーション モードを終了します。

ePBR サービス エンドポイント アウトオブサービスを構成

ここでは、ePBR サービス エンドポイント アウトオブサービスの設定について説明します。

手順の概要

1. **configure terminal**
2. **epbr service** *service-name*
3. [**no**] **shut**
4. **service-endpoint** [**interface** *interface-name interface-number*]
5. [**no**] **hold-down threshold count** *threshold count* **time** *threshold time*

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**epbr service** *service-name* 例： `switch(config)# epbr service s1`	構成されたサービスを開始します。
ステップ 3	[**no**] **shut** 例：	エンドポイントをシャットダウンしてアウトオブサービスにする

	コマンドまたはアクション	目的
	`switch(config)# shut`	このコマンドの **no** 形式は、ノードをシャットダウンしてエンドポイントをサービスに戻します。
ステップ 4	**service-endpoint** [**interface** *interface-name interface-number*] 例： `switch(config-epbr-svc)# service-end-point ip 1.1.1.1`	ePBR サービスのサービスエンドポイントを構成します。 手順 2 ～ 5 を繰り返して、別の ePBR サービスを構成できます。
ステップ 5	[**no**] **hold-down threshold count** *threshold count* **time** *threshold time* 例： `switch(config)# hold-down threshold count 2 time 5`	は、エンドポイント レベルまたはサービス レベルのしきい値タイマーと障害カウントを構成します。それと共にエンドポイント レベルのパラメータは、サービス レベルのパラメータを上書きします。 しきい値カウントが 1 より大きい場合、タイマーは必須です。しきい値カウントが 1 の場合、タイマーは無視または拒否されます。

ePBR ポリシーの ePBR Set-VRF の構成

Cisco NX-OS リリース 10.5(2)F 以降、ePBR は ePBR L3 ポリシーの **set-vrf** コマンドをサポートします。この機能拡張により、ePBR VRF 間の展開でホスト VRF からサービス VRF へのルートリークが不要になります。

set-vrf 機能は、ルートリークなしで、ホスト VRF コンテキストでルーティングされる最後のホップからのトラフィックを許可します。

set-vrf コマンドは、ePBR ポリシー レベルまたは一致レベルで設定できます。両方が構成されている場合、一致レベルが優先されます。

set-vrf を構成するには、次のステップを実行します:

始める前に

- インターフェイスに ePBR ポリシーを適用する前に、ホスト VRF コンテキストごとに 1 つの専用ポートチャネル インターフェイスと 1 つのポート チャネル サブインターフェイスを構成する必要があります。

  次に、source-vrf（vrf551）と destination-vrf（vrf555）の両方のポートチャネルおよびポートチャネル サブインターフェイスを作成する例を示します。

```
int port-channel 1
   no shut
 int e1/1
   channel-group 1
   link loopback
   no shut
int port-channel 1.1
   encapsulation dot1q 10
   vrf member vrf551
```

```
    ip forward
    ipv6 address use-link-local-only
    ipv6 nd dad attempts 0
    ipv6 nd prefix default no-advertise
    ipv6 nd suppress-ra
    mtu 9216
    no shut
 int port-channel 1.2
    encapsulation dot1q 11
    vrf member vrf555
    ip forward
    ipv6 address use-link-local-only
    ipv6 nd dad attempts 0
    ipv6 nd prefix default no-advertise
    ipv6 nd suppress-ra
    mtu 9216
    no shut
```

- また、ePBR ポリシーを適用する前に、VRF コンテキストで同等の RPM 構成を関連付ける必要があります。

  次に、VRF コンテキスト構成を作成する例を示します。

```
vrf context vrf551
    pbr set-vrf recirc interface port-channel1.1
vrf context vrf555
    pbr set-vrf recirc interface port-channel1.2
```

手順の概要

1. **configure terminal**
2. **epbr policy** ポリシー名*-IPv4* |ポリシー名*-IPv6*
3. （任意） **source-vrf** *source-vrf-name* **destination-vrf** *destination-vrf-name*
4. （任意） **match** { [**ip address** *ipv4 acl-name*] | [**ipv6 address** *ipv6 acl-name*] } **source-vrf** *source-vrf-name* **destination-vrf** *destination-vrf-name*

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**epbr policy** ポリシー名*-IPv4* |ポリシー名*-IPv6*
	例：
	IPV4 の場合：
	`switch(config)# epbr policy p_v4`
	`switch(config-epbr-policy)#`
		ePBR ポリシーを構成し、ePBR ポリシー構成モードを開始します。

	コマンドまたはアクション	目的
	IPV6 の場合： `switch(config-epbr-policy)# epbr policy p_v6`	
ステップ 3	（任意） **source-vrf** *source-vrf-name* **destination-vrf** *destination-vrf-name* 例： `switch(config-epbr-policy)# source-vrf vrf551 destination-vrf vrf555`	順方向の場合は `destination-vrf`、逆方向の場合は `source-vrf` を設定します。

ステップ 4	（任意） **match** { [**ip address** *ipv4 acl-name*] | [**ipv6 address** *ipv6 acl-name*] } **source-vrf** *source-vrf-name* **destination-vrf** *destination-vrf-name*
	例：
	IPv4 の場合：
	`switch(config-epbr-policy)# match ip address acl1 source-vrf vrf551 destination-vrf vrf555`
	IPV6 の場合：
	`switch(config-epbr-policy)# match ipv6 address acl1 source-vrf vrf551 destination-vrf vrf555`
		指定した送信元および接続先 VRF の IPv4 または IPv6 ACL を照合します。

ePBR Show コマンド

次のリストに、ePBR に関連する show コマンドを示します。

手順の概要

1. **show epbr policy** *policy-name* [**reverse**]
2. **show epbr statistics** *policy-name* [**reverse**]
3. **show tech-support epbr**
4. **show running-config epbr**
5. **show startup-config epbr**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**show epbr policy** *policy-name* [**reverse**] 例： `switch# show epbr policy Tenant_A-Redirect`	順方向または逆方向に適用される ePBR ポリシーに関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 2	**show epbr statistics** *policy-name* [**reverse**] 例： `switch# show ePBR statistics policy pol2`	ePBR ポリシー統計を表示します。
ステップ 3	**show tech-support epbr** 例： `switch# show tech-support epbr`	ePBR のテクニカル サポート情報を表示します。
ステップ 4	**show running-config epbr** 例： `switch# show running-config epbr`	ePBR の実行構成を表示します。
ステップ 5	**show startup-config epbr** 例： `switch# show startup-config epbr`	ePBR のスタートアップ構成を表示します。

ePBR 構成の確認

ePBR 構成を確認するためには、次のコマンドを使用します。

コマンド	目的
show ip/ipv6 policy vrf <context>	サービスチェーンが適用されるインターフェイスおよびサービスチェーンの関連するエンドポイント インターフェイスで、レイヤ 3 ePBR ポリシー用に作成された IPv4/IPv6 ルート マップ ポリシーを表示します。
show route-map dynamic <route-map name>	サービスチェーンのすべてのポイントでトラフィックを転送するために使用される、特定のバケットアクセスリストのトラフィック リダイレクション用に構成されたネクスト ホップを表示します。
show ip/ipv6 access-list <access-list name> dynamic	バケットアクセス リストのトラフィック一致基準を表示します。
show ip sla configuration dynamic	プローブが有効になっている場合に、チェーン内のサービスエンドポイントに対してePBRによって生成された IP SLA 構成を表示します。

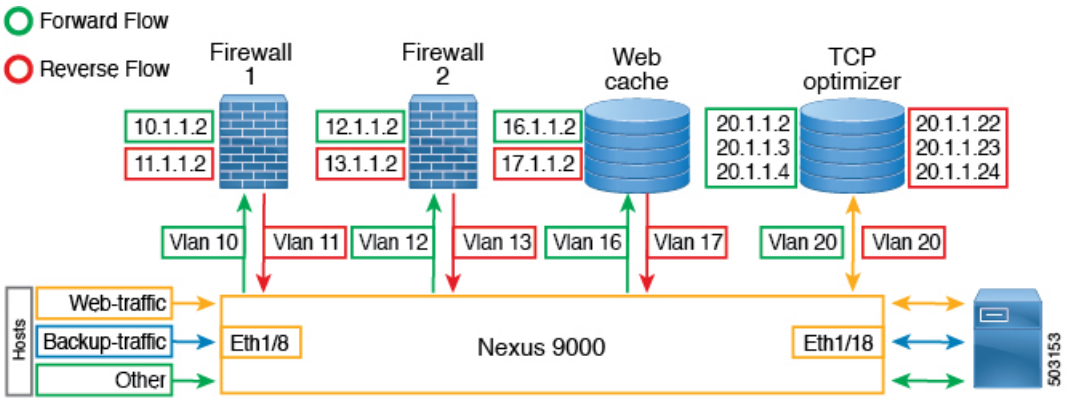
コマンド	目的
show track dynamic	プローブが有効になっている場合に、チェーン内のサービスエンドポイントに対してePBRによって生成されたトラックを表示します。

ePBR L3 の構成例

例：ePBR NX-OS 構成

次のトポロジは、ePBR NX-OS 構成を示しています。

図 *1 : ePBR NX-OS* の構成



例：ユースケース：順方向のみの Web トラフィックのサービスチェーンを作成する

次の構成例は、順方向のみの Web トラフィックのサービスチェーンを作成する方法を示しています。

```
IP access list web_traffic
        10 permit tcp any any eq www

ePBR service FW1
  service-end-point ip 10.1.1.2 interface Vlan10
    reverse interface Vlan11

ePBR service FW2
  service-end-point ip 12.1.1.2 interface Vlan12
    reverse interface Vlan13

ePBR service Web_cache
  service-end-point ip 16.1.1.2 interface Vlan16
    reverse interface Vlan17

ePBR policy tenant_1
  match ip address web-traffic
    10 set service FW1
    20 set service FW2
    30 set service Web_cache
```

```
interface Eth1/8
  ePBR ip policy tenant_1
```

次の例は、順方向の Web トラフィックのサービスチェーン作成の構成を確認する方法を示しています。

```
switch# show ePBR policy tenant_1

Policy-map : tenant_1
  Match clause:
    ip address (access-lists): web-traffic
  Service chain:
    service FW1, sequence 10, fail-action No fail-action
      IP 10.1.1.2
    service FW2, sequence 20, fail-action No fail-action
      IP 12.1.1.2
    service Web_cache, sequence 30, fail-action No fail-action
      IP 16.1.1.2
  Policy Interfaces:
    Eth1/8
```

例：ユースケース：順方向のみで ePBR を使用して TCP トラフィックを負荷分散する

次の構成例は、順方向のみでePBRを使用してTCPトラフィックを負荷分散する方法を示しています。

```
IP access list tcp_traffic
        10 permit tcp any any

ePBR service TCP_Optimizer
  service-interface Vlan20
  service-end-point ip 20.1.1.2
  service-end-point ip 20.1.1.3
  service-end-point ip 20.1.1.4

ePBR policy tenant_1
  match ip address tcp_traffic
    10 set service TCP_Optimizer

interface Eth1/8
  ePBR ip policy tenant_1
```

次の例は、順方向で EPBR を使用して負荷分散 TCP トラフィックの構成を確認する方法を示しています。

```
switch# show ePBR policy tenant_1

Policy-map : tenant_1
  Match clause:
    ip address (access-lists): tcp_traffic
  Service chain:
    service TCP_Optimizer, sequence 10, fail-action No fail-action
      IP 20.1.1.2
      IP 20.1.1.3
      IP 20.1.1.4
  Policy Interfaces:
    Eth1/8
```

例：ユースケース：双方向の Web トラフィックのサービスチェーンを作成する

次の構成例は、順方向と逆方向の両方で Web トラフィックのサービスチェーンを作成する方法を示しています。

```
IP access list web_traffic
        10 permit tcp any any eq www


ePBR service FW1
  service-end-point ip 10.1.1.2 interface Vlan10
    reverse ip 11.1.1.2 interface Vlan11

ePBR service FW2
  service-end-point ip 12.1.1.2 interface Vlan12
    reverse ip 13.1.1.2 interface Vlan13

ePBR service Web_cache
  service-end-point ip 16.1.1.2 interface Vlan16
    reverse ip 17.1.1.2 interface Vlan17

ePBR policy tenant_1
  match ip address web-traffic
    10 set service FW1
    20 set service FW2
    30 set service Web_cache

interface Eth1/8
  ePBR ip policy tenant_1

interface Eth1/18
  ePBR ip policy tenant_1 reverse
```

次の例は、順方向と逆方向の両方の Web トラフィックのサービスチェーン作成の構成を確認する方法を示しています。

```
switch# show ePBR policy tenant_1

Policy-map : tenant_1
  Match clause:
    ip address (access-lists): web-traffic
  Service chain:
    service FW1, sequence 10, fail-action No fail-action
      IP 10.1.1.2
    service FW2, sequence 20, fail-action No fail-action
      IP 12.1.1.2
    service Web_cache, sequence 30, fail-action No fail-action
      IP 16.1.1.2
  Policy Interfaces:
    Eth1/8

switch# show ePBR policy tenant_1 reverse

Policy-map : tenant_1
  Match clause:
    ip address (access-lists): web-traffic
  Service chain:
    service Web_cache, sequence 30, fail-action No fail-action
      IP 17.1.1.2
    service FW2, sequence 20, fail-action No fail-action
      IP 13.1.1.2
    service FW1, sequence 10, fail-action No fail-action
      IP 11.1.1.2
  Policy Interfaces:
    Eth1/18
```

例：ユースケース：ePBR を使用して両方向で TCP トラフィックを負荷分散する

次の構成例は、ePBR を使用して順方向と逆方向の両方で TCP トラフィックを負荷分散する方法を示しています。

```
ePBR service TCP_Optimizer
  service-interface Vlan20
  service-end-point ip 20.1.1.2
    reverse ip 20.1.1.22
  service-end-point ip 20.1.1.3
    reverse ip 20.1.1.23
  service-end-point ip 20.1.1.4
    reverse ip 20.1.1.24

ePBR policy tenant_1
  match ip address tcp_traffic
    10 set service TCP_Optimizer

interface Eth1/8
  ePBR ip policy tenant_1

interface Eth1/18
  ePBR ip policy tenant_1 reverse
```

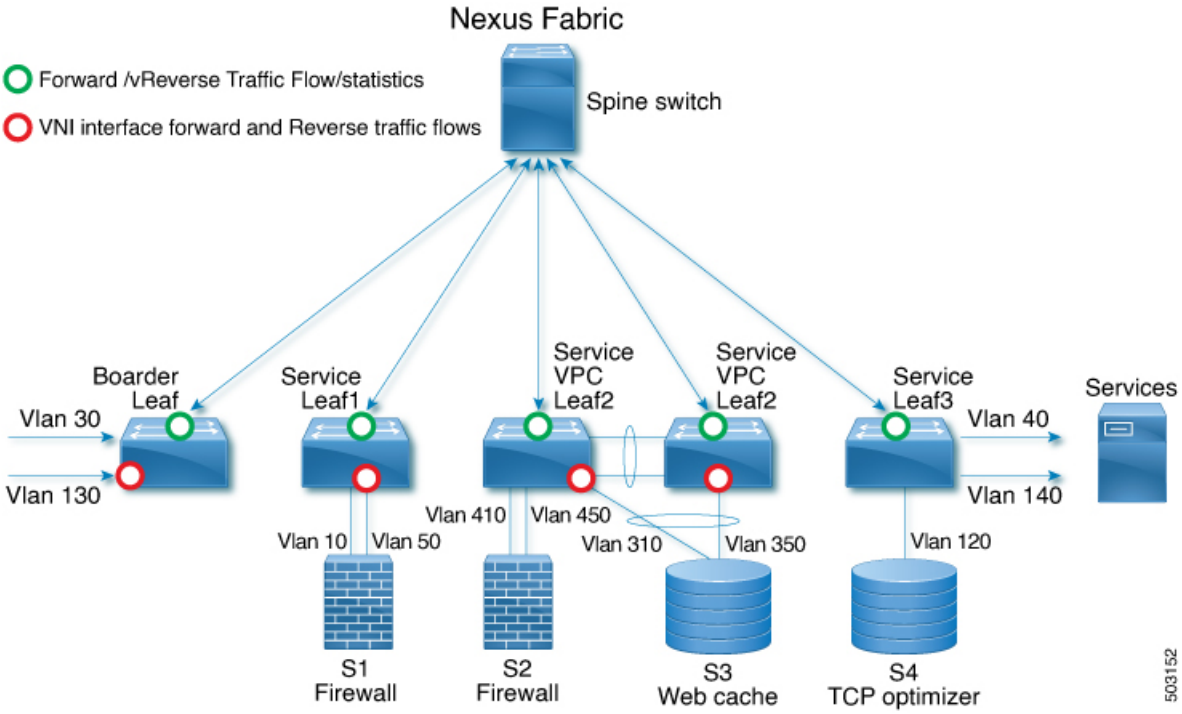
次の例は、ePBR を使用して双方向の負荷分散 TCP トラフィックの構成を確認する方法を示しています。

```
switch# show ePBR policy tenant_1

Policy-map : tenant_1
  Match clause:
    ip address (access-lists): tcp_traffic
  Service chain:
    service TCP_Optimizer, sequence 10, fail-action No fail-action
      IP 20.1.1.2
      IP 20.1.1.3
      IP 20.1.1.4
  Policy Interfaces:
    Eth1/8

switch# show ePBR policy tenant_1 reverse

Policy-map : tenant_1
  Match clause:
    ip address (access-lists): tcp_traffic
  Service chain:
    service TCP_Optimizer, sequence 10, fail-action No fail-action
      IP 20.1.1.22
      IP 20.1.1.23
      IP 20.1.1.24
  Policy Interfaces:
    Eth1/18
```

例：VXLAN ファブリックを使用した ePBR ポリシーの作成

次の例/トポロジは、VXLAN ファブリック上で ePBR を構成する方法を示しています。

図 *2 : VXLAN* ファブリック上の *ePBR* の構成




```
ip access-list acl1
        10 permit ip 30.1.1.0/25 40.1.1.0/25
        20 permit ip 30.1.1.128/25 40.1.1.128/25
ip access-list acl2
        10 permit ip 130.1.1.0/25 140.1.1.0/25
        20 permit ip 130.1.1.128/25 140.1.1.128/25

epbr service s1
  vrf vrf_s1
  service-end-point ip 10.1.1.2 interface Vlan10
     probe icmp frequency 4 retry-down-count 1 retry-up-count 1 timeout 2 source-interface
 loopback9
    reverse ip 50.1.1.2 interface Vlan50

       probe icmp frequency 4 retry-down-count 1 retry-up-count 1 timeout 2
source-interface loopback10

epbr service s2
  vrf vrf_s2
  service-end-point ip 41.1.1.2 interface Vlan410
     probe icmp source-interface loopback11
    reverse ip 45.1.1.2 interface Vlan450

       probe icmp source-interface loopback12

 epbr service s3
  vrf vrf_s3
  service-end-point ip 31.1.1.2 interface Vlan310
     probe http get index.html source-interface loopback13
    reverse ip 35.1.1.2 interface Vlan350

     probe http get index.html source-interface loopback14
```

```
epbr service s4
  service-interface Vlan120
  vrf vrf_s4
   probe udp 6900 control enable source-interface loopback15
  service-end-point ip 120.1.1.2

    reverse ip 120.1.1.2

epbr policy p1
 statistics
  match ip address acl1
    load-balance buckets 16 method src-ip
    10 set service s1 fail-action drop
    20 set service s2 fail-action drop
    30 set service s4 fail-action bypass
  match ip address acl2
    load-balance buckets 8 method dst-ip
    10 set service s1 fail-action drop
    20 set service s3 fail-action forward
    30 set service s4 fail-action bypass

! VXLAN L3 VNI interface for vrf_s1, vrf_s2, vrf_s3, vrf_s4 to which the policy is applied
 on all service leafs
interface vlan 100
epbr ip policy p1
epbr ip policy p1 reverse

interface vlan 101
epbr ip policy p1
epbr ip policy p1 reverse

interface vlan 102
epbr ip policy p1
epbr ip policy p1 reverse

interface vlan 103
epbr ip policy p1
epbr ip policy p1 reverse

Apply forward policy on ingress interface in border leaf where traffic coming in needs
to be service-chained:

interface Vlan 30 - Traffic matching acl1
  epbr ip policy p1
  int vlan 130  -  Traffic matching acl2
  epbr ip policy p1

Apply the reverse policy On leaf connected to server if reverse traffic flow needs to
be enabled:

int vlan 40 - Traffic matching reverse flow for acl1
epbr ip policy p1 rev
int vlan 140 - Traffic matching reverse flow for acl1
epbr ip policy p1 rev
```

例：ePBR サービスの構成

次の例は、ePBR サービスを構成する方法を示します。

```
epbr service FIREWALL
  probe icmp
  vrf TENANT_A
  service-endpoint ip 172.16.1.200 interface VLAN100
        reverse ip 172.16.2.200 interface VLAN101
```

```
service-endpoint ip 172.16.1.201 interface VLAN100
        reverse ip 172.16.2.201 interface VLAN101

epbr service TCP_Optimizer
   probe icmp
   vrf TENANT_A
service-endpoint ip 172.16.20.200 interface VLAN200
       reverse ip 172.16.30.200 interface VLAN201
```

例：ePBR ポリシーの構成

次の例は、ePBR ポリシーを構成する方法を示します。

```
epbr service FIREWALL
  probe icmp
  service-end-point ip 1.1.1.1 interface Ethernet1/1
     reverse ip 1.1.1.2 interface Ethernet1/2
epbr service TCP_Optimizer
 probe icmp
 service-end-point ip 1.1.1.1 interface Ethernet1/3
     reverse ip 1.1.1.4 interface Ethernet1/4
epbr policy Tenant_A-Redirect
 match ip address WEB
  load-balance method src-ip
  10 set service FIREWALL fail-action drop
  20 set service TCP_Optimizer fail-action bypass
match ip address APP
  10 set service FIREWALL fail-action drop
match ip address exclude_acl exclude
match ip address drop_acl drop
```

次の例は、fail-action drop 情報を含む show ePBR Policy コマンドの出力を示しています。

```
switch(config-if)# show epbr policy Tenant_A-Redirect

Policy-map : Tenant_A-Redirect
  Match clause:
    ip address (access-lists): WEB
action:Redirect
   service FIREWALL, sequence 10, fail-action Drop
     IP 1.1.1.1 track 1 [INACTIVE]
   service TCP_Optimizer, sequence 20, fail-action Bypass
     IP 1.1.1.1 track 2 [INACTIVE]
Match clause:
     ip address (access-lists): APP
action:Redirect
   service FIREWALL, sequence 10, fail-action Drop
     IP 1.1.1.1 track 1 [INACTIVE]
Match clause:
    ip address (access-lists): exclude_acl
action:Deny
Match clause:
   ip address (access-lists): drop_acl
action:Drop
 Policy Interfaces:
  Eth1/4
```

例：インターフェイスと ePBR ポリシーの関連付け

次の例は、ePBR ポリシーを構成する方法を示します。

```
interface vlan 2010
  epbr ip policy Tenant_A-Redirect
```

```
interface vlan 2011
  epbr ip policy Tenant_A-Redirect reverse
```

例：順方向に適用される ePBR ポリシー

次の例は、順方向に適用されるポリシーのサンプル出力を示しています。

```
show epbr policy Tenant_A-Redirect
policy-map Tenant_A-Redirect
 Match clause:
  ip address (access-lists): WEB
 Service chain:
  service FIREWALL  , sequence 10 , fail-action drop
   ip 172.16.1.200 track 10  [ UP ]
   ip 172.16.1.201 track 11 [ DOWN ]
                    service TCP_Optimizer, sequence 20 , fail-action bypass
   ip 172.16.20.200 track 12  [ UP] ]

 Match clause:
  ip address (access-lists): APP
 Service chain:
  service FIREWALL  , sequence 10 , fail-action drop
   ip 172.16.1.200 track 10  [ UP ]
   ip 172.16.1.201 track 11 [ DOWN ]

 Policy Interfaces:
     Vlan 2010
```

例：reverse 方向に適用される ePBR ポリシー

次の例は、reverse 方向に適用されるポリシーのサンプル出力を示しています。

```
show epbr policy Tenant_A-Redirect reverse
policy-map Tenant_A-Redirect
 Match clause:
  ip address (access-lists): WEB

 Service chain:
  service TCP_Optimizer, sequence 20 , fail-action bypass
   ip 172.16.30.200 track 15  [ UP] ]

  service FIREWALL  , sequence 10 , fail-action drop
   ip 172.16.2.200 track 13  [ UP ]
   ip 172.16.2.201 track 14 [ DOWN ]

 Match clause:
  ip address (access-lists): APP

 Service chain:

  service FIREWALL  , sequence 10 , fail-action drop
   ip 172.16.2.200 track 13  [ UP ]
   ip 172.16.2.201 track 14 [ DOWN ]

 Policy Interfaces:
     Vlan 2011
```

例：ユーザ定義トラック

次の例は、各エンド ポイントにトラック ID を割り当てる方法を示しています。

```
epbr service FIREWALL
  probe icmp
  service-end-point ip 1.1.1.2 interface Ethernet1/21
```

```
probe track 30
reverse ip 1.1.1.3 interface Ethernet1/22
  probe track 40
 service-end-point ip 1.1.1.4 interface Ethernet1/23
    reverse ip 1.1.1.5 interface Ethernet1/24
```

例：ePBR セッションを使用した ePBR サービスの変更

次の例は、ePBR サービスの IP を置き換え、別のサービス エンド ポイントを追加する方法を示しています。

```
switch(config)#epbr session
switch(config-epbr-sess)#epbr service TCP_OPTIMIZER
switch(config-epbr-sess-svc)# no service-end-point ip 172.16.20.200 interface VLAN200

switch(config-epbr-sess-svc)#service-end-point ip 172.16.25.200 interface VLAN200
switch(config-epbr-sess-svc-ep)# reverse ip 172.16.30.200 interface VLAN201
switch(config-epbr-sess)#commit
```

例：EPBR セッションを使用した ePBR ポリシーの変更

次の例は、ePBR ポリシーの IP を置き換え、変更されたポリシー トラフィックのサービスチェーンを追加する方法を示しています。

```
switch(config)#epbr session
switch(config-epbr-sess)#epbr policy Tenant_A-Redirect
switch(config-epbr-sess-pol)# no match ip address WEB
switch(config-epbr-sess-pol)#match ip address WEB
switch(config-epbr-sess-pol-match)# 10  set service Web-FW fail-action drop load-balance
 method src-ip
switch(config-epbr-sess-pol-match)# 20 set service TCP_Optimizer fail-action bypass
switch(config-epbr-sess-pol)#match ip address HR
switch(config-epbr-sess-pol-match)# 10  set service Web-FW
switch(config-epbr-sess-pol-match)# 20 set service TCP_Optimizer
switch(config-epbr-sess)#commit
```

例：ePBR 統計ポリシーの表示

次の例は、ePBR 統計ポリシーを表示する方法を示しています。

```
switch# show epbr statistics policy pol2

Policy-map pol2, match testv6acl

    Bucket count: 2

      traffic match : epbr_pol2_1_fwd_bucket_1
        two : 0
      traffic match : epbr_pol2_1_fwd_bucket_2
        two : 0
```

例：mask-position の使用方法の表示

次に、mask-position の使用例を示します。

```
IP access list acl1
        10 permit tcp 10.0.0.0/24 any
epbr policy l3_Pol
  statistics match ip address acl1
  load-balance buckets 4 mask-position 5
10 set service s1_l3
switch# show ip access-list dynamic
IP access list epbr_l3_Pol_1_fwd_bucket_1
 10 permit tcp 10.0.0.0 0.0.0.159 any
IP access list epbr_l3_Pol_1_fwd_bucket_2
```

```
 10 permit tcp 10.0.0.32 0.0.0.159 any
IP access list epbr_l3_Pol_1_fwd_bucket_3
 10 permit tcp 10.0.0.64 0.0.0.159 any
IP access list epbr_l3_Pol_1_fwd_bucket_4
 10 permit tcp 10.0.0.96 0.0.0.159 any
```

その他の参考資料

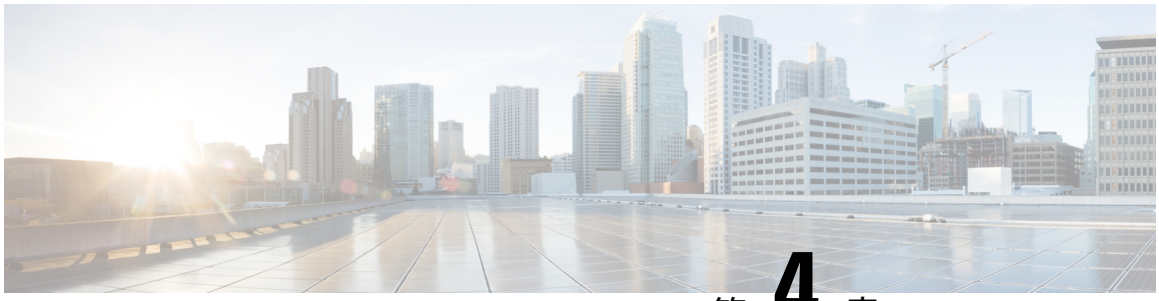
ePBR の構成の詳細については、次の各セクションを参照してください。

関連資料

関連項目	マニュアル タイトル
IP SLA パケットの CoPP の構成	*Cisco Nexus 9000* シリーズ *NX-OS IP SLA* 構成ガイド *9.3(x)*
ePBR ライセンス	『*Cisco NX-OS Licensing Guide*』
ePBR スケール値	『*Cisco Nexus 9000 Series NX-OS Verified Scalability Gu*

標準

標準
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポート れていません。



第 4 章

ePBR L2 の構成

ePBR L2 に関する情報

Elastic Services Re-direction（ESR）の強化されたポリシーベースのリダイレクト レイヤ2（ePBR）は、ポート ACL と VLAN 変換を利用して、レイヤ 1/レイヤ 2 サービス アプライアンスの透過的なサービス リダイレクトとサービスチェーンを提供します。このアクションは、余分なヘッダーを追加することなくサービスチェーンと負荷分散機能を実現し、余分なヘッダーを使用する際の遅延を回避するのに役立ちます。

ePBR は、アプリケーション ベースのルーティングを可能にし、アプリケーションのパフォーマンスに影響を与えることなく、柔軟でデバイスに依存しないポリシーベースのリダイレクト ソリューションを提供します。ePBR サービス フローには、次のタスクが含まれます。

ePBR サービスとポリシーの構成

まず、サービスエンドポイントの属性を定義する ePBR サービスを作成する必要があります。サービスエンドポイントは、スイッチに関連付けることができるファイアウォール、IPS などのサービス アプライアンスです。また、サービス エンド ポイントの状態を監視するプローブを定義したり、トラフィック ポリシーが適用されるフォワード インターフェイスと reverse インターフェイスを定義したりすることもできます。 ePBR は、サービスチェーンとともにロー

ドバランシングもサポートします。 ePBR を使用すると、サービス構成の一部として複数のサービス エンド ポイントを構成できます。

ePBR サービスを作成したら、ePBR ポリシーを作成する必要があります。ePBR ポリシーを使用すると、トラフィックの選択、サービスエンドポイントへのトラフィックのリダイレクト、およびエンド ポイントの正常性障害に関するさまざまな fail-action メカニズムを定義できます。許可アクセス コントロール エントリ（ACE）を備えた IP access-list エンド ポイントを使用して、一致する対象のトラフィックを定義し、適切なアクションを実行できます。

ePBR ポリシーは、複数の ACL 一致定義をサポートします。一致には、シーケンス番号によって順序付けできるチェーンに複数のサービスを含めることができます。これにより、単一のサービス ポリシーでチェーン内の要素を柔軟に追加、挿入、および変更できます。すべてのサービス シーケンスで、ドロップ、転送、バイパスなどの失敗時のアクション メソッドを定義できます。ePBR ポリシーを使用すると、トラフィックの詳細なロード バランシングを行うために、送信元または接続先ベースのロード バランシングとバケット数を指定できます。

ePBR の L2 インターフェイスへの適用

ePBR ポリシーを作成したら、インターフェイスにポリシーを適用する必要があります。これにより、トラフィックが NX-OS スイッチに入力するインターフェイスと、トラフィックがリダイレクションまたはサービスチェーンの後にスイッチから出力される必要があるインターフェイスを定義できます。NX-OS スイッチに順方向と逆方向の両方でポリシーを適用することもできます。

アクセス ポートとしてのプロダクション インターフェイスの有効化

サービスチェーンするスイッチがトラフィックのリダイレクト向けの 2 つの L3 ルータ間に挿入されている場合、実稼働インターフェイスがアクセス ポートとして有効になります。以下の制限があります。

- 一致構成の一部としてポートの VLAN を使用する必要があります。
- これは、mac-learn 無効モードに制限されます。

トランク ポートとしてのプロダクション インターフェイスの有効化

プロダクション インターフェイスはトランク ポートとして構成できます。インターフェイスによってトランクされるサービスチェーンする必要がある着信トラフィックの VLAN は、一致構成の一部として構成する必要があります。

または、一致構成で「vlan all」を使用すると、インターフェイス上の着信 VLAN に関連するすべてのトラフィックが一致し、サービスチェーンされます。

バケットの作成およびロード バランシング

ePBRは、チェーン内でサービスエンドポイントの最大数を持つサービスに基づいてトラフィック バケットの数を計算します。ロード バランス バケットを構成する場合は事前に行ってください。ePBR は送信元 IP および接続先 IP のロード バランシングをサポートしますが、L4 ベースの送信元または接続先のロード バランシング メソッドはサポートしていません。

ePBR オブジェクト トラッキング、ヘルスモニタリング、および Fail-Action

レイヤ 2 ePBR は、デフォルトでサービス エンドポイントのリンク ステート モニタリングを実行します。サービスでサポートされている場合、ユーザはさらにCTP（構成テスト支援プロトコル）を有効にすることができます。

サービス向け、または転送またはreverseの各エンドポイント向けに、ePBR プローブ オプションを構成することが可能です。頻度、タイムアウト、および再試行のアップカウントとダウンカウントを構成することもできます。同じトラック オブジェクトが、同じ ePBR サービスを使用するすべてのポリシーに再利用されます。

エンドポイント レベルで定義されているプローブ メソッドがない場合、サービスレベルで構成されるプローブ メソッドを使用できます。

ePBR は、自身のサービスチェーンのシーケンスで次の fail-action メカニズムをサポートします。

- バイパス
- ドロップオンフェイル
- 転送

サービス シーケンスのバイパスは、現在のシーケンスで障害が発生した場合に、トラフィックは次のサービス シーケンスにリダイレクトされる必要があることを示しています。

サービス シーケンスのドロップオンフェイルは、サービスのすべてのサービスエンドポイントが到達不能となる場合に、トラフィックはドロップされる必要があることを示しています。

転送はデフォルトのオプションであり、現在のサービスに障害が発生した場合、トラフィックは出力インターフェイスに転送する必要があることを示します。これはデフォルトの fail-action メカニズムです。

（注） 対称性が維持されるのは、fail-action バイパスがサービスチェーン内のすべてのサービス向けに構成された場合です。その他の fail-action シナリオでは、1 つまたはそれ以上の機能不全サービスが存在する場合、転送または reverse フローでの対称性は維持されません。

Cisco NX-OS リリース 10.4(1)F 以降、ePBR L2 fail-action 機能は、ノードの障害によって現在影響を受けている ACE のみを変更するように最適化されています。ただし、fail-action 最適化

は、ユーザーが ePBR match ステートメントで **load-balance buckets** を構成したサービスチェーンに対してのみ有効になります。

fail-action の最適化は、Cisco Nexus 9300-FX/FX2/FX3/GX/GX2および X97160YC-EX、9700-FX/GX ライン カードを搭載した Cisco Nexus 9500 スイッチでサポートされます。

ePBR セッションベースの構成

ePBR セッションにより、次のサービス内のアスペクトのサービスまたはポリシーの追加、削除、変更が可能になります。サービス内とは、アクティブインターフェイスまたはポリシーに適用されているポリシーに関連付けられたサービスを示し、アクティブインターフェイス上で変更される、現在構成済みのサービスを示します。

- インターフェイスおよびプローブを備えたサービスエンドポイント
- reverse エンドポイントおよびプローブ
- ポリシーで一致
- 一致させるための負荷分散メソッド
- 一致シーケンスおよび fail-action

（注） ePBR セッションで、同じセッション内で 1 つのサービスから別のサービスにインターフェイスを移動することはできません。1 つのサービスから別のサービスにインターフェイスを移動させるには、次の手順を行います。

1. まず初めに、既存のサービスからインターフェイスを削除するための 1 つ目のセッションを実行します。
2. 既存のサービスにインターフェイスを追加するための 2 つ目のセッションを実行します。

ACL リフレッシュ

ePBR セッション ACL リフレッシュにより、ユーザが入力した ACL がACE を使用して変更、追加、または削除される場合に、ACL を生成するポリシーを更新することができるようになります。リフレッシュ トリガーで、ePBR はこの変更によって影響を受けるポリシーを特定し、それらのポリシー向けに ACL を生成するバケットを作成、削除、または変更します。

ePBR のスケール数については、『Cisco Nexus 9000 Series NX-OS Verified Scalability Guide』を参照してください。

ePBR L2 の注意事項および制約事項

ePBR には、次の注意事項と制限事項 があります。

- fail-action がいずれかの一致ステートメントで指定されている場合、プローブは構成内に存在していることが必須です。
- スイッチでMACラーニングを無効化するには、**mac-learn disable**コマンドを使用します。
- ePBR構成内の複数の一致ステートメント全体で同じユーザ定義ACLを共有しないでください。
- トラフィックの対称性が維持されるのは、fail-actionバイパスがePBRサービス向けに構成されたときのみです。サービスチェーン内の転送/ドロップなどのその他のfail-actionの場合、トラフィックの順方向と逆方向のフローの対称性は維持されません。
- 機能 ePBR および機能 ITD は同じ入力インターフェイスと共存できません。
- 拡張済み ePBR 構成では、**no feature epbr**コマンド を使用する前にポリシーを削除することが推奨されています。
- VXLAN上のePBRv6は、Cisco Nexus 9500シリーズ スイッチでサポートされていません。
- システムから削除されたポートチャネルに構成された ePBR サービスエンドポイントを削除する場合、次の手順を実行してください。
  1. 既存の ePBR ポリシーを削除します。
  2. 既存の ePBR サービスを削除します。
  3. ePBR サービス エンドポイントを必要なポートチャネルに再構成します。
- 「epbr_」という名前で始まる、動的に作成された ePBR の access-list エントリは変更しないでください。これらの access-lists は ePBR 内部使用向けに予約済みです。

（注） これらのプレフィックス文字列を変更すると ePBR が正しく機能せず、ISSU に影響を与える可能性があります。

- すべてのリダイレクション ルールは、ing-ifacl リージョンを使用して ACL TCAM でプログラムされます。このリージョンは、ePBR L2 ポリシーを適用する前に分割して割り当てる必要があります。

（注） TCAM リージョンの分割方法の手順については、「*Cisco Nexus 9000* シリーズ *NX-OS* セキュリティ構成ガイド」の **[IP ACL の構成（Configuring IP ACLs）]** セクションを参照してください。

- ePBR ポリシーには、リダイレクト アクションとの一致が少なくとも 1 つ必要です。
- ePBR L2 では、VLAN 変換と Q-in-Q 用に VLAN 範囲を予約する必要があります。この範囲は、トラフィックの一致構成に使用される VLAN と重複しないようにすることが推奨されています。

- ePBR の「インフラ」VLAN は、ePBR レイヤ 2 ポリシーを適用する前に予約済みにする必要があります。
- トランク ポートとして構成された本番インターフェイスの場合、ePBR「infra vlan」範囲で指定された VLAN に対してのみ VLAN トランキングを有効にします。
- トランク許可 VLAN のリストにネイティブ VLAN を追加する必要があります。これは、選択的 QinQ や選択的 Q-in-VNI などの使用可能なアクセス機能と一致しています。
- ePBR L2 は、VLAN ヘッダーを変更または削除せずに、パケットをそのまま転送するようにサービス アプライアンスが構成されていることを想定しています。
- ePBR L2 ポリシーの各一致には、トランク インターフェイスに適用される場合、一意の一致 VLAN または一意の VLAN 範囲が必要です。トランク インターフェイスに適用されるポリシーには、「vlan all」との一致が 1 つだけ存在できます。
- ePBR L2 ポリシー定義は、順方向および逆方向でサポートされているインターフェイス タイプの最大 32 個のインターフェイスに適用できます。
- Cisco NX-OS リリース 10.3(1)F 以降、同じ EPBR L2 ポリシー内の複数の一致は、同じ VLAN または VLAN 範囲を共有するか、トランク インターフェイスに適用されるポリシーで「vlan all」で構成される場合があります。

（注） 同じアドレス ファミリ（IPv4、ipv6、または L2）の複数の一致 ACL がポリシー内の同じ VLAN を共有する場合、構成された一致 ACL 全体の ACL フィルタが一意であり、重複していないことを確認してください。

- 実稼働ポート ペアの場合、順方向のインターフェイスとその逆方向の reverse インターフェイスに適用されるポリシーは、一致するもので構成され、同一の match-vlan または VLAN 範囲に個別にマッピングされます。
- 複数のサービス デバイス間の負荷分散を行い、CTP ヘルスチェックを介してこれらのデバイスの障害を一意に検出するには、各サービス デバイスを ePBR サービスの一意のエンドポイントとして定義する必要があります。
- バケットベースの負荷分散は、ePBR ポリシーのレイヤ 2 一致ではサポートされていません。
- ネイバー探索など、IPv6 トラフィックをサービスチェーンに送る、またはリダイレクトするには、プロトコル タイプが ND-NA および ND-NS である ICMPv6 ACE を、ユーザー定義の一致アクセス リストで明示的に定義する必要があります。
- ARP（0x806）、VN タグ（0x8926）、FCOE（0x8906）、MPLS ユニキャスト（0x8847）、MPLS マルチキャスト（0x8848）などのプロトコルで、レイヤ 2 トラフィックをサービス チェーンに送る、またはリダイレクトするには、プロトコル情報をユーザー定義の一致アクセス リスト内の ACE に明示的に追加する必要があります。

- Cisco NX-OS リリース 10.4(1)F 以降、ePBR L2 は、ePBR ポリシーに一致するすべての制御トラフィックのリダイレクションをサポートします。詳細については、「制御トラフィックのリダイレクションとドロップの適用 （53 ページ）」の項を参照してください。
- 意図しない動作を防ぐために、使用中の ePBR 実稼働インターフェイスおよび/またはサービス インターフェイスのデフォルト設定は避ける必要があります。
- Cisco NX-OS リリース 10.3(1)F 以降、ePBR L2 は、Cisco Nexus 9300-GX プラットフォーム スイッチの L2 制御パケットのリダイレクションのみをサポートします。サービスチェーンは Cisco Nexus 9300-GX プラットフォーム スイッチではサポートされません。
- Cisco NX-OS リリース 10.4(1)F 以降、ePBR には、Cisco Nexus 9300-FX/FX2/FX3/GX/GX2、および Nexus X97160YC-EX、9700-FX/GX ライン カードを搭載した Cisco Nexus 9500 プラットフォーム スイッチ で、IPv4 または IPv6 一致のユーザー定義 ACL においてロードバランシングに使用されるビットを選択する、**mask-position** オプションが用意されています。
- 構成のロールバックと設定の置換は、ePBR ポリシーがインターフェイスに関連付けられておらず、ePBR サービス定義が送信元設定とターゲット設定の両方のアクティブな ePBR ポリシーで使用されていない場合にのみサポートされます。ただし、構成のロールバックと構成の置換では、ポリシーとインターフェイスの関連付けおよび関連付け解除はサポートされません。

次の注意事項および制約事項を一致 ACL 機能に適用します。

- permit メソッドを持つ ACE のみが ACL でサポートされます。他の方法（deny または remark など）の ACE は無視されます。
- 1 つの ACL で最大 256 の許可 ACE がサポートされます。
- Cisco NX-OS リリース 10.4（1）F 以降では、match access-list ルールのレイヤ 4 ポート範囲およびその他のポート操作（「等しくない」、「より大きい」、「より小さい」など）は、バケットアクセスリスト内のトラフィックのフィルタリングに使用されます。
- アクセスリストでレイヤ 4 ポートオペレータを使用しながら、TCAM ACE の使用率を最適化するには、この構成 **hardware access-list lou resource threshold**を使用する必要があります。このコマンドの詳細については、『*Cisco Nexus 9000* シリーズ *NX-OS* セキュリティ構成ガイド』の「**IP ACL の構成**」のセクションを参照してください。

次のガイドラインと制限事項が VRF 間のサービスチェーンに適用されます。

- Cisco NX-OS リリース 10.2(3)F 以降、エンドポイントの追加、サービス シーケンスの追加、削除および変更のセッション操作中のトラフィックの中断を最小限にするために、事前にロードバランスバケットの構成を行い、ロードバランス構成への変更を回避することが推奨されています。ロードバランス向けに構成されたバケットの数が、チェーン内の各シーケンス向けのサービスで構成されたエンドポイントの数より多くなるようにしてください。

送信元 IP ベースのロード バランシングを使用して ePBR を構成した場合は、次の注意事項と制限事項が適用されます。

- ACE の送信元 IPv4 のプレフィックス長を /32 にすることはできません
- ACE の送信元 IPv6 アドレスのプレフィックス長を /128 にすることはできません
- 送信元アドレスのサブネットは、構成されたバケットと互換性がある必要があります。

送信先 IP ベースのロード バランシングを使用して ePBR を構成した場合は、次の注意事項と制限事項が適用されます：

- ACE の送信先 IPv4 のプレフィックス長を /32 にすることはできません
- ACE の送信先 IPv6 アドレスのプレフィックス長を /128 にすることはできません
- 送信先アドレスのサブネットは、構成されたバケットと互換性がある必要があります。

ePBRサービス、ポリシーの構成およびインターフェイスへの関連付け

次のセクションでは、ePBR サービス、ePBR ポリシーの構成、およびインターフェイスへのポリシーの関連付けについて説明します。

手順の概要

1. **configure terminal**
2. **[no] epbr infra vlans** *[vlan range]*
3. **epbr service** *service-name* **type** *l2*
4. **mode** [**full duplex** | **half duplex**]
5. **probe** {**ctp**} [**frequency** *seconds*] [**timeout** *seconds*] [**retry-down-count** *count*] **retry-up-count** *count*]
6. **service-endpoint** [**interface** *interface-name interface-number*]
7. **reverse interface** *interface-name interface-number*
8. **exit**
9. **epbr policy** *policy-name*
10. **match** { [**ip address** *ipv4 acl-name*] | [**ipv6 address** *ipv6 acl-name*] | [**l2 address** *l2 acl-name*]} {**drop** | **exclude** | **redirect** | **vlan**{**vlan** | **vlan range** | **all**}}
11. [**no**] **load-balance** [**method** { **src-ip** | **dst-ip**}] [**buckets** *count*] [**mask-position** *position-value*]
12. *sequence-number* **set service** *service-name* [**fail-action** { **bypass** | **drop** | **forward**}]
13. **interface** *interface-name interface-number*
14. **epbr** {**l2**} **policy** *policy-name egress-interface interface-name* [**reverse**]
15. **exit**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**[no] epbr infra vlans** *[vlan range]*	VLAN 範囲は、サービス デバイスへのリダイレクト中に選択的な dot1q 変換用に予約された VLAN を示すために使用されています。
ステップ 3	**epbr service** *service-name* **type** *l2* 例： `switch(config)# epbr service firewall type l2`	新しい ePBR L2 サービスを作成します。
ステップ 4	**mode** [**full duplex** | **half duplex**]	サービスを半二重または全二重モードに構成します。
ステップ 5	**probe** {**ctp**} [**frequency** *seconds*] [**timeout** *seconds*] [**retry-down-count** *count*] **retry-up-count** *count*] 例： `switch(config)# probe icmp`	ePBR サービスのプローブを構成します。 オプションは次のとおりです。 • 頻度：プローブの頻度を秒単位で指定します。値の範囲は 1 ～ 604800 です。 • 再試行ダウン カウント：ノードがダウンしたときにプローブによって実行される再カウントの数を指定します。指定できる範囲は1 ～ 5 です。 • 再試行アップ カウント：ノードが復帰したときにプローブが実行する再カウントの数を指定します。指定できる範囲は 1 ～ 5 です。 • タイムアウト：タイムアウト期間を秒単位で指定します。値の範囲は 1 ～ 604800 です。
ステップ 6	**service-endpoint** [**interface** *interface-name interface-number*] 例： `switch(config-epbr-svc)# service-end-point interface Ethernet1/3`	ePBR サービスのサービスエンドポイントを構成します。 手順 2 ～ 5 を繰り返して、別の ePBR サービスを構成できます。
ステップ 7	**reverse interface** *interface-name interface-number* 例：	トラフィック ポリシーが適用される reverse インターフェイスを定義します。

	コマンドまたはアクション	目的
	`switch(config-epbr-fwd-svc)# reverse interface Ethernet1/4`	

ステップ 8	**exit**
	例：
	`switch(config-epbr-reverse-svc)# exit`
	`switch(config-epbr-fwd-svc)# exit`
	`switch(config-epbr-svc)# exit`
	`switch(config)#`
		ePBR サービス構成モードを終了し、グローバル コンフィギュレーション モードを開始します。

ステップ 9	**epbr policy** *policy-name* 例： `switch(config)# epbr policy Tenant_A-Redirect`	ePBR ポリシーを構成します。
ステップ 10	**match** { [**ip address** *ipv4 acl-name*] | [**ipv6 address** *ipv6 acl-name*] | [**l2 address** *l2 acl-name*]} {**drop** | **exclude** | **redirect** | **vlan**{**vlan** | **vlan range** | **all**}} 例： `switch (config) # match ip address WEB vlan 10`	IPv4 または IPv6 アドレス、または MAC アドレスを IP、IPv6、または MAC ACL と照合します。リダイレクトは、一致トラフィックのデフォルト アクションです。ドロップは、着信インターフェイスでトラフィックをドロップする必要がある場合に使用されます。除外オプションは、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するために使用されます。 この手順を繰り返して、要件に基づいて複数の ACL を一致させることができます。
ステップ 11	[**no**] **load-balance** [**method** { **src-ip** | **dst-ip**}] [**buckets** *count*] [**mask-position** *position-value*] 例： `switch(config)# load-balance method src-ip mask-position 3`	ePBR サービスで使用されるロードバランス メソッドとバケット数を計算します。 Cisco NX-OS リリース 10.4(1)F 以降では、IPv4 または IPv6 マッチでのユーザー定義 ACL でロード バランシングに使用されるビットを選択する、**mask-position** オプションが提供されています。デフォルト値は 0 です。 mask-position が構成されている場合、ロードバランス ビットは構成された mask-position から始まります。必要なバケットの数に基づいて、最上位ビットまたは最下位ビットのどちらが選択されたかに応じ、より多くのビットがロードバランシング バケットを生成するために使用されます。 （注） ユーザー定義の ACL 内の ACE では、ロード バランシング バケットの生成に使用されるビットがユーザー定義のサブネットと重複している場合、ACE のマスク位置は内部的に 0 にリセットされます。

	コマンドまたはアクション	目的
ステップ 12	*sequence-number* **set service** *service-name* [**fail-action** { **bypass** | **drop** | **forward**}] 例： `switch(config)# set service firewall fail-action drop`	fail-action メカニズムを構成します。
ステップ 13	**interface** *interface-name interface-number* 例： `switch(config)# interface Ethernet1/1`	インターフェイス構成モードを開始します。
ステップ 14	**epbr** {**l2**} **policy** *policy-name egress-interface interface-name* [**reverse**] 例： `epbr l2 policy Tenant_A_Redirect egress-interface Ethernet1/2`	インターフェイスは、いつでも次の 1 つの順方向のポリシーと 1 つの逆方向のポリシーに関連付けることができます。 • 順方向の IPV4 ポリシー • 逆方向の IPv4 ポリシー • 順方向の IPv6 ポリシー • 逆方向の IPv6 ポリシー • 順方向の l2 ポリシー • 逆方向の l2 ポリシー
ステップ 15	**exit** 例： `switch(config-if)# end`	ポリシー構成モードを終了し、グローバル モードに戻ります。

ePBR セッションを使用したサービスの変更

次の手順では、ePBR セッションを使用してサービスを変更する方法を説明しています。

手順の概要

1. **epbr session**
2. **epbr service** *service-name type l2*
3. [**no**] **service-endpoint** [**interface** *interface-name*]
4. **service-endpoint** [**interface** *interface-name*]
5. **reverse** [**interface** *interface-name*]
6. **commit**
7. **abort**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**epbr session** 例： `switch(config)# epbr session`	ePBR セッション モードに入ります。
ステップ 2	**epbr service** *service-name type l2* 例： `switch(config-epbr-sess)# epbr service TCP_OPTIMIZER`	ePBR セッション モードで構成する ePBR サービスを指定します。
ステップ 3	[**no**] **service-endpoint** [**interface** *interface-name*] 例： `switch(config-epbr-sess-svc)# no service-end-point interface ethernet 1/3`	ePBR サービス向けに構成されたサービスエンドポイントを無効にします。
ステップ 4	**service-endpoint** [**interface** *interface-name*] 例： `switch(config-epbr-sess-svc)# service-end-point interface ethernet 1/15`	サービスにサービスエンドポイントを追加します。
ステップ 5	**reverse** [**interface** *interface-name*] 例： `switch(config-epbr-sess-fwd-svc)# reverse interface ethernet 1/4`	トラフィック ポリシーが適用される reverse インターフェイスを定義します。
ステップ 6	**commit** 例： `switch(config-epbr-sess)#commit`	ePBR セッションを使用した ePBR サービスの変更を完了します。 （注） このステップの完了後に ePBR セッションを再起動します。
ステップ 7	**abort** 例： `switch(config-epbr-sess)# abort`	セッションを中止し、セッションの現在の構成をクリアまたはリセットします。コミット中にエラーまたはサポートされていない構成が識別された場合に、現在のセッション構成を破棄するには、このコマンドを使用します。 （注） その後、修正した構成を使用して新しい ePBR セッションを再開します。

ePBR セッションを使用したポリシーの変更

次の手順では、ePBR セッションを使用してポリシーを変更する方法について説明します。

手順の概要

1. **epbr session**
2. **epbr policy** *policy-name*
3. [**no**] **match** { [**ip address** *ipv4 acl-name*] | [**ipv6 address** *ipv6 acl-name*] | **l2 address** *mac acl-name*]} **vlan** {**all** | **vlan-id** | **vlan-id-range**
4. **match** { [**ip address** *ipv4 acl-name*] | [**ipv6 address** *ipv6 acl-name*] | **l2 address** *mac acl-name*]} **vlan** {**all** | **vlan-id** | **vlan-id-range**]
5. *sequence-number* **set service** *service-name* [**fail-action** { **bypass** | **drop** | **forward**}]
6. [**no**] **load-balance** [**method** { **src-ip** | **dst-ip**}] [**buckets** *count*] [**mask-position** *position-value*]
7. **commit**
8. **end**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**epbr session**	
ステップ 2	**epbr policy** *policy-name* 例： `switch(config-epbr-sess)# epbr policy Tenant_A-Redirect`	ePBR セッション モードで構成する ePBR ポリシーを指定します。
ステップ 3	[**no**] **match** { [**ip address** *ipv4 acl-name*]	[**ipv6 address** *ipv6 acl-name*]	**l2 address** *mac acl-name*]} **vlan** {**all**	**vlan-id**	**vlan-id-range** 例： `switch(config-epbr-sess-pol)# no match ip address WEB`	IP、IPv6、または L2 ACL に対する一致を無効にします。
ステップ 4	**match** { [**ip address** *ipv4 acl-name*]	[**ipv6 address** *ipv6 acl-name*]	**l2 address** *mac acl-name*]} **vlan** {**all**	**vlan-id**	**vlan-id-range**] 例： `switch(config-epbr-sess-pol)# match ip address HR`	IP、IPv6、または L2 ACL に対する一致を変更します。
ステップ 5	*sequence-number* **set service** *service-name* [**fail-action** { **bypass**	**drop**	**forward**}] 例：	fail-action メカニズムを構成します。

	コマンドまたはアクション	目的
	`switch(config-epbr-sess-pol-match)# set service firewall fail-action drop`	
ステップ 6	[**no**] **load-balance** [**method** { **src-ip** | **dst-ip**}] [**buckets** *count*] [**mask-position** *position-value*] 例： `switch(config)# load-balance method src-ip mask-position 3`	一致のロードバランス メソッドとバケットを構成します。 （注） 既存の一致のサービスチェーンを変更するときに、セッション コンテキストでこの構成を省略すると、一致のロードバランス構成がデフォルトにリセットされます。 Cisco NX-OS リリース 10.4(1)F 以降では、IPv4 または IPv6 マッチでのユーザー定義 ACL でロード バランシングに使用されるビットを選択する、**mask-position** オプションが提供されています。デフォルト値は 0 です。 mask-position が構成されている場合、ロードバランス ビットは構成された mask-position から始まります。必要なバケットの数に基づいて、最上位ビットまたは最下位ビットのどちらが選択されたかに応じ、より多くのビットがロードバランシング バケットを生成するために使用されます。 （注） ユーザー定義の ACL 内の ACE では、ロード バランシング バケットの生成に使用されるビットがユーザー定義のサブネットと重複している場合、ACE のマスク位置は内部的に 0 にリセットされます。
ステップ 7	**commit** 例： `switch(config-epbr-sess)#commit`	ePBR セッションを使用した ePBR サービスの変更を完了します。
ステップ 8	**end** 例： `switch(config-epbr-sess)#end`	ePBR セッション モードを終了します。

ePBR ポリシーによる使用される Access-list の更新

次の手順では、ePBR ポリシーで使用される access-list を更新する方法について説明します。

手順の概要

1. **epbr session access-list** *acl-name* **refresh**
2. **end**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**epbr session access-list** *acl-name* **refresh** 例： `switch(config)# epbr session access-list WEB refresh`	ポリシーによって生成された ACL を更新またはリフレッシュします。
ステップ 2	**end** 例： `switch(config)# end`	グローバル コンフィギュレーション モードを終了します。

制御トラフィックのリダイレクションとドロップの適用

Cisco NX-OS リリース 10.4(1)F 以降では、次の構成オプションを使用して、ePBR L2 ポリシーを介して制御トラフィックのリダイレクションおよびドロップ動作を制御できます。

all構成オプションは、ACEに最も高いプライオリティが必要であることを示すため、ePBRのユーザー定義の match access-list の ACE 内で使用されます。この構成の詳細については、*Cisco Nexus 9000* シリーズ *NX-OS* セキュリティ構成ガイドの、**SUP ルールに対する IP ACL ルールの優先順位の適用**または**SUP ルールに対する MAC ACL ルールの優先順位の適用**のセクションを参照してください。

all オプションを使用すると、次の動作が観察されます。

- **redirection** または **exclude** アクションと一致した場合、ePBR は対応するリダイレクション ACE を生成して、それぞれ指定されたサービス デバイスまたは出力インターフェイスへの制御トラフィックを含む、一致するすべてのトラフィックのリダイレクションを適用します。
- **drop** アクションと一致した場合、ePBR は拒否 ACE を生成して、制御トラフィックを含むすべての一致トラフィックを強制的にドロップします。このオプションが構成どおりに検出されなった場合、通常は Cisco NX-OS 9000 シリーズ スイッチのスーパーバイザにコピーまたはリダイレクトされる制御トラフィックが、ePBR レイヤ 2 ポリシー定義に一致する場合でも、引き続きコピーされる可能性があります。

all オプションは、match アクセスリストが ePBR レイヤ 3 ポリシー内で使用されている場合は効果がありません。

default-traffic-action redirect-all 構成オプションは、ePBR レイヤ 2 ポリシー内で使用され、リダイレクト、除外、またはドロップ一致に一致しないトラフィック（制御トラフィックを含む）を、指定された出力インターフェイスにリダイレクトする必要があることを指定します。このオプションが構成されていない場合、ポリシー内のアクセスリストに一致せず、通常、Cisco NX-OS 9000 シリーズ スイッチのスーパーバイザにコピーまたはリダイレクトされる制御トラフィックは（出力インターフェイスにリダイレクトされのではなく）引き続き同様に処理されます。

次のコマンドを使用して、ポリシー レベルでデフォルトの catch-all トラフィック動作を構成できます。

手順の概要

1. **configure terminal**
2. **epbr policy** *policy-name*
3. **default-traffic-action** [**redirect** | **redirect-all**]

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**epbr policy** *policy-name* 例： `switch(config)# epbr policy p3`	ePBR ポリシーを構成します。
ステップ 3	**default-traffic-action** [**redirect** | **redirect-all**] 例： `switch(config-epbr-policy)# default-traffic-action redirect-all`	ePBR ポリシーのデフォルトの catch-all 動作を設定します。 • **redirect**：データトラフィックをリダイレクトします。 **redirect** はデフォルトのオプションです。 • **redirect-all**：すべてのトラフィックをリダイレクトします。 （注） • このオプションは、レイヤ 3 ePBR ポリシー内ではサポートされません。 • このオプションは ePBR セッション内では変更できないため、ポリシーを無効にして再構成し、再度適用する必要があります。

ePBR Show コマンド

次のリストに、ePBR に関連する show コマンドを示します。

手順の概要

1. **show epbr policy** *policy-name* [**reverse**]
2. **show epbr statistics** *policy-name* [**reverse**]
3. **show tech-support epbr**
4. **show running-config epbr**
5. **show startup-config epbr**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**show epbr policy** *policy-name* [**reverse**] 例： `switch# show epbr policy Tenant_A-Redirect`	順方向または逆方向に適用される ePBR ポリシーに関する情報を表示します。
ステップ 2	**show epbr statistics** *policy-name* [**reverse**] 例： `switch# show ePBR statistics policy pol2`	ePBR ポリシー統計を表示します。
ステップ 3	**show tech-support epbr** 例： `switch# show tech-support epbr`	ePBR のテクニカル サポート情報を表示します。
ステップ 4	**show running-config epbr** 例： `switch# show running-config epbr`	ePBR の実行構成を表示します。
ステップ 5	**show startup-config epbr** 例： `switch# show startup-config epbr`	ePBR のスタートアップ構成を表示します。

ePBR 構成の確認

ePBR 構成を確認するためには、次のコマンドを使用します。

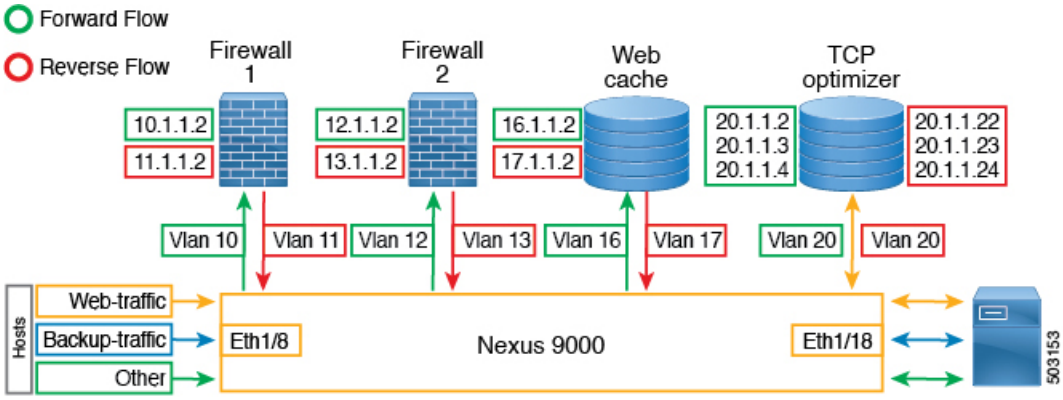
コマンド	目的
show ip access-list <access-list name> dynamic	バケットアクセスリストのトラフィック一致基準を表示します。
show ip sla configuration dynamic	プローブが有効になっている場合に、チェーン内のサービスエンドポイントに対して ePBR によって生成された IP SLA 構成を表示します。
show track dynamic	プローブが有効になっている場合に、チェーン内のサービスエンドポイントに対して ePBR によって生成されたトラックを表示します。
show ip access-list summary	バケットアクセスリストのトラフィック一致基準のサマリを表示します。
show [ip | ipv6 | mac] access-lists dynamic	一致基準のダイナミック エントリを表示します。

ePBR の構成例

例：ePBR NX-OS 構成

次のトポロジは、ePBR NX-OS 構成を示しています。

図 *3 : ePBR NX-OS* の構成



例：アクセス ポートおよびトランク ポートのサービス構成

次の構成例は、アクセス ポートとトランク ポートのサービス構成を実行する方法を示しています。

```
epbr infra vlans 100-200

epbr service app_1 type l2
   service-end-point interface Ethernet1/3
```

```
    reverse  interface Ethernet1/4

epbr service app_2 type l2
   probe ctp frequency 2 retry-down-count 1 retry-up-count 1 timeout 1
   service-end-point interface port-channel10
    reverse  interface port-channel11

epbr service app_3 type l2
   probe ctp frequency 2 retry-down-count 1 retry-up-count 1 timeout 1
   service-end-point interface Ethernet1/9
    reverse  interface Ethernet1/10

epbr service app_4 type l2
   probe ctp frequency 2 retry-down-count 1 retry-up-count 1 timeout 1
   service-end-point interface port-channel12
    reverse  interface port-channel13
```

例：アクセス ポートの構成

次の例では、アクセス ポートを構成する方法を示します。

```
epbr policy p1
  statistics
  match ipv6 address flow2 vlan 10
    load-balance buckets 2
    10 set service app_1
    20 set service app_3
    25 set service app_4
    30 set service app_2
  match l2 address flow3 vlan 10
    20 set service app_2
    25 set service app_4
    50 set service app_3
  match ip address flow1 vlan 10
    10 set service app_1
    15 set service app_3
    20 set service app_2

interface Ethernet1/1
  switchport
  switchport access vlan 10
  no shutdown
  epbr l2 policy p1 egress-interface Ethernet1/2

interface Ethernet1/2
  switchport
  switchport access vlan 10
  no shutdown
  epbr l2 policy p1 egress-interface Ethernet1/1 reverse
```

例：トランク ポートの構成

次の構成例は、トランク ポートを構成する方法を示します。

```
epbr policy p3
  statistics
  match ip address flow1 vlan 10
    load-balance buckets 2
    10 set service app_1
    20 set service app_2
  match ipv6 address flow2 vlan 20
    load-balance buckets 2
    10 set service app_3
    20 set service app_4
  match l2 address flow3 vlan 30
```

```
    10 set service app_1
    20 set service app_2

interface Ethernet1/27
  switchport
  switchport mode trunk
  no shutdown
  epbr l2 policy p3 egress-interface Ethernet1/28

interface Ethernet1/28
  switchport
  switchport mode trunk
  no shutdown
  epbr l2 policy p3 egress-interface Ethernet1/27 reverse

Collecting statistics
```

統計の収集：

```
itd-san-2# show epbr statistics policy p1

Policy-map p1, match flow2

    Bucket count: 2

      traffic match : bucket 1
        app_1 : 8986 (Redirect)
        app_3 : 8679 (Redirect)
        app_4 : 8710 (Redirect)
        app_2 : 8725 (Redirect)
      traffic match : bucket 2
        app_1 : 8696 (Redirect)
        app_3 : 8680 (Redirect)
        app_4 : 8711 (Redirect)
        app_2 : 8725 (Redirect)

Policy-map p1, match flow3

    Bucket count: 1

      traffic match : bucket 1
        app_2 : 17401 (Redirect)
        app_4 : 17489 (Redirect)
        app_3 : 17461 (Redirect)

Policy-map p1, match flow1

    Bucket count: 1

      traffic match : bucket 1
        app_1 : 17382 (Redirect)
        app_3 : 17348 (Redirect)
        app_2 : 17411 (Redirect)
```

例：ePBR ポリシーの表示

次の例では、ePBR ポリシーを表示する方法を示します。

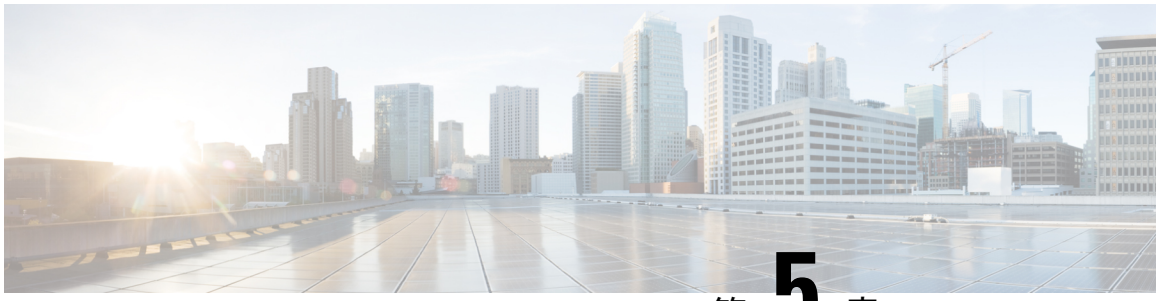
```
show epbr policy p3

Policy-map : p3
Match clause:
ip address (access-lists): flow1
```

```
action:Redirect
service app_1, sequence 10, fail-action No fail-action
Ethernet1/3 track 4 [UP]
service app_2, sequence 20, fail-action No fail-action
port-channel10 track 10 [UP]
Match clause:
ipv6 address (access-lists): flow2
action:Redirect
service app_3, sequence 10, fail-action No fail-action
Ethernet1/9 track 13 [UP]
service app_4, sequence 20, fail-action No fail-action
port-channel12 track 3 [UP]
Match clause:
layer-2 address (access-lists): flow3
action:Redirect
service app_1, sequence 10, fail-action No fail-action
Ethernet1/3 track 4 [UP]
service app_2, sequence 20, fail-action No fail-action
port-channel10 track 10 [UP]
Policy Interfaces:
egress-interface Eth1/28
```

例：mask-position の使用方法の表示

次に、mask-position の使用例を示します。

```
ip access-list acl1
   10 permit tcp 10.1.1.0/24 any
epbr service s1_l2 type l2
  service-end-point interface Ethernet1/2
    reverse interface Ethernet1/3
epbr policy l2_pol
   statistics
   match ip address acl1 vlan all
   load-balance buckets 4 mask-position 5
   10 set service s1_l2
interface Ethernet1/18
  epbr l2 policy l2_pol egress-interface Ethernet1/19
switch(config-if)# show access-lists epbr_Ethernet1_18_ip dyn

IP access list epbr_Ethernet1_18_ip
        statistics per-entry
        200001 permit tcp 10.1.1.0 0.0.0.159 any vlan 100 redirect Ethernet1/2 [
match=0]
        200002 permit tcp 10.1.1.32 0.0.0.159 any vlan 100 redirect Ethernet1/2
[match=0]
        200003 permit tcp 10.1.1.64 0.0.0.159 any vlan 100 redirect Ethernet1/2
[match=0]
        200004 permit tcp 10.1.1.96 0.0.0.159 any vlan 100 redirect Ethernet1/2
[match=0]
        4294967295 permit ip any any redirect Ethernet1/19 [match=0]
```



第 5 章

セキュリティ グループを使用したサービス チェーンの構成

ePBR およびグループ ポリシー オプションに関する情報

Cisco NX-OS リリース 10.5(1)F 以降、ユーザーは異なるセキュリティ グループのエンドポイント部分の間で、トラフィックフローをリダイレクトできます。リダイレクションは、単一のサービス機能（ファイアウォールまたはロードバランサとして）を介して、またはサービス機能のチェーンを介して発生する可能性があります。Cisco NX-OS リリース 10.5(2)F 以降、ユーザーはサービスチェーンに最大5つのサービス機能を含めることができます。特定のサービス機能は、そのような機能を実行するサービスデバイスを表す1つ以上のエンドポイントで構築されます。トラフィック フローは、これらのサービスエンドポイント間でロード バランシングでき、トラフィック フローの両方向が同じサービスエンドポイントを対称的に使用するようにします。これらのサービスデバイスのオンボーディング、ヘルスモニタリングメカニズム、およびこれらのサービスデバイスのプロパティに基づいたトラフィックのチェーン化とロードバランシングのユーザーの意図は、ePBR を介してキャプチャされ、適用されます。マイクロセグメンテーション構成の詳細については、 グループ ポリシー オプション（GPO）を使用した VXLAN ファブリックのマイクロセグメンテーションを参照してください。

ePBR サービスとサービスチェーン

最初に、特定の属性を持つ1つ以上のエンドポイントで定義されるサービス機能を作成する必要があります。サービスエンドポイントは、トラフィックをリダイレクトする必要があるネットワークで使用可能な、ファイアウォール、IPS などのサービス アプライアンスです。サービス エンドポイントの正常性をモニターするプローブを定義することもできます。 ePBR は、サービスチェーンとともにロードバランシングもサポートします。 ePBR を使用すると、特定のサービス機能の一部として複数のサービスエンドポイントを構成できます。これらのエンドポイント間でトラフィックのロード バランシングを行い、同じトラフィック フローの 2 つのレッグが同じサービスエンドポイントを使用するようにします。これは、特定のサービス機能に定義されたさまざまなサービスエンドポイントがクラスタ化されておらず、それらの間で接続状態を共有しない場合に必要です。

サービス エンドポイントが到達可能なコンテキストとして、サービスの VRF コンテキストを指定する必要があります。

1つ（または複数）の ePBR サービスを作成したら、ePBR サービスチェーンを作成する必要があります。ePBR サービスチェーンを使用すると、トラフィックをリダイレクトするサービス機能（またはサービス機能のチェーン）と、これを実行する順序を定義できます。

チェーンで使用されるサービスは、シーケンス番号によって識別されます。NXOS 10.5(1)F では、サービスチェーン内で単一のサービス機能のみを指定できるため、トラフィックが接続先に許可される前に、単一のサービス機能へのリダイレクションおよびロードバランシング機能のみがサポートされます。

すべてのサービス シーケンスで、サービス内のすべてのエンドポイントで障害が発生した場合に実行する必要があるアクションを示す、ドロップ、転送、バイパスなどの fail-action メソッドを定義できます。fail-action が設定されていない場合、デフォルトの動作では、サービスが失敗したと見なされるとトラフィックがドロップされます。

ePBR サービスチェーンでは、サービス内のエンドポイント間でトラフィックをロードバランシングする方法を指定することもできます。

Cisco NX-OS リリース 10.5(2)F 以降、ePBR マルチノード サービスチェーンはグループ ポリシー オプションでサポートされます。サービスチェーンには最大 5 つのサービス機能（ノード）を設定できます。マルチノード サービス チェーンには、ファイアウォール、ロード バランサ、NAT、IPS、およびその他のデバイスを含めることができます。

Cisco NX-OS リリース 10.5(2)F 以降では、ePBR シングル ノードまたはマルチ ノード サービス チェーンを使用するコントラクトの送信元と接続先を、VXLAN グループ ポリシー オプションを使用して複数のサイトに分散できます。

Cisco NX-OS リリース 10.5(2)F 以降では、ePBR マルチノード サービスチェーンおよびマルチサイト機能は、異なる VRF コンテキストの送信元と接続先でサポートされます。サービスデバイスは、送信元 VRF、接続先 VRF、またはその他の VRF に属することができます。

サービスのセキュリティ グループ

VxLAN GPO ベースのリダイレクションとチェーンにサービスを使用する場合、ePBR サービスのワンアームモードでサービスを展開することもできるため、セキュリティ グループ識別子を設定する必要があります。この設定は、トラフィックをサービスデバイスに正しく誘導し、チェーンを通過させるために必要です。

これらのセキュリティグループは、タイプ layer4-7 のセレクタとしてシステムで定義する必要があります。サービス内のサービスエンドポイントに接続された各インターフェイスは、match インターフェイス セレクタとして正しいセキュリティグループにマッピングする必要があります。詳細については、グループ ポリシー オプションを使用した VXLAN ファブリックのマイクロセグメンテーション（GPO）のセキュリティ グループの作成を参照してください。

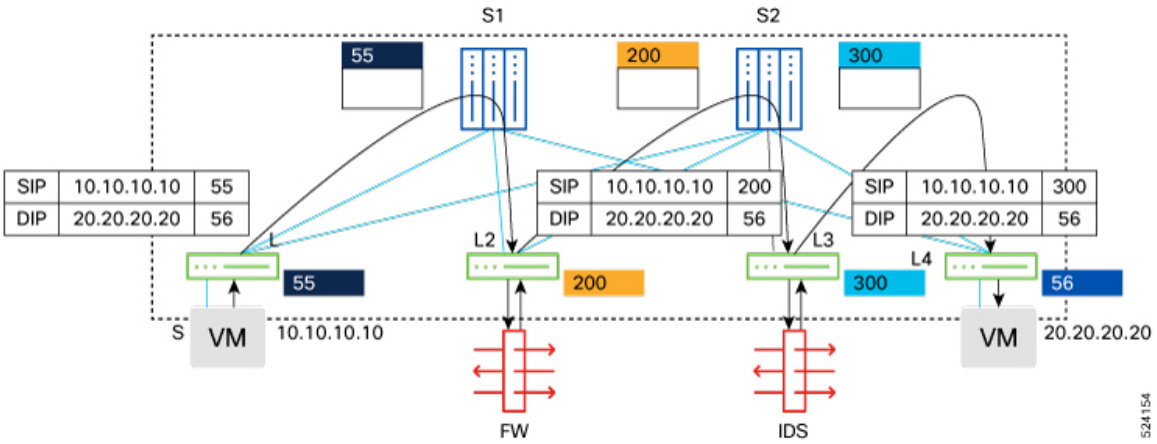
サービス エンドポイントのすべての転送アームに接続されたインターフェイスは、ePBR サービスの転送セキュリティ グループとして指定されているものと同じ識別子にマッピングする必要があります。

サービス エンドポイントのすべてのリバース アームに接続されたインターフェイスは、ePBR サービスのリバースセキュリティグループとして指定されているものと同じ識別子にマッピングする必要があります。

ワンアーム エンドポイントを使用する ePBR サービスには、セキュリティグループ識別子を 1 つだけ構成する必要があります。

デュアルアーム エンドポイントを使用する ePBR サービスには、2 つの一意の順引きおよび逆引きセキュリティ グループ識別子を構成する必要があります。マイクロセグメンテーション ベースのリダイレクションとチェーンの説明となるトポロジについては、図 1 を参照してください。

図 *4*:サービス チェーンによるマイクロセグメンテーション



SGACL ポリシーおよびコントラクトでの ePBR サービスチェーンの使用

GPO を使用した ePBR サービスチェーンは、GPO ポリシーとコントラクトを使用してトラフィックのリダイレクトを提供できます。サービスチェーンは、コントラクトで使用されるポリシー内のクラスマップと一致するようにアタッチすることで、セキュリティコントラクトに対して有効にできます。構成の詳細については、グループ ポリシー オプション（GPO）を使用した VXLAN ファブリックのマイクロセグメンテーションを参照してください。

ePBR ヘルス モニタリング、および障害アクション

プローブ構成を適用する場合、ePBR は IP SLA プローブをプロビジョニングすることによりエンドポイントの正常性をモニタし、オブジェクトをトラックして IP SLA の到達可能性をトラックします。

ePBR は、ICMP、TCP、UDP、DNS、HTTP などのさまざまなプローブとタイマーをサポートします。 ePBR はユーザー定義のトラックもサポートしており、ミリ秒プローブを含むさまざまなパラメータでトラックを作成し、ePBR に関連付けることができます。

サービスのすべてのエンドポイントで同様のプローブ方式とプロトコルが必要な場合は、サービスの ePBR プローブ オプションを設定できます。1 つ以上のエンドポイントで別のプローブメカニズムが必要な場合は、それらのフォワード エンドポイントとリバース エンドポイントに固有のプローブ オプションを設定できます。頻度、タイムアウト、および再試行のアップカウントとダウンカウントを構成することもできます。VXLAN 環境に分散されたサービスエンドポイントの場合、ユーザーはエンドポイントまたはサービスプローブの送信元ループバック インターフェイスを構成する必要があります。これらのループバック インターフェイスの IP アドレスは、これらのエンドポイントで確立された IP SLA セッションの一意の送信元 IP として使用されます。

サービスに対してプローブが設定されている場合、転送アームとリバース アームに一意のループバックは必要ありません。同じループバックを共有することも、別のループバックを提供することもできます。

トラック ID を個別に定義し、ePBR の各サービス エンド ポイントにそれを割り当てることができます。これらのトラック ID は、同じまたは異なる ePBR サービス内の異なるエンドポイント間で再利用することはできませんが、エンドポイントのフォワードアームとリバースアーム間で共有できます。ユーザー定義のトラックをエンドポイントに割り当てない場合、ePBR はエンドポイントのプローブ メソッドを使用してトラックを作成します。エンドポイント レベルで定義されているプローブ メソッドがない場合、サービス レベルで構成されるプローブ メソッドを使用できます。

デバイスに障害が発生すると、障害が発生したデバイスにリダイレクトされていたトラフィックは、サービスが障害として検出されるまで、他の到達可能なデバイスにリダイレクトされます。復元力のあるハッシュは、複数のサービスエンドポイントで展開されたサービス機能のデ

バイス障害時にサポートされます。常に特定のサービスエンドポイントにリダイレクトされていたトラフィックは、同じサービス機能の他のサービスエンドポイントで障害が発生した場合でも、同じデバイスに引き続きリダイレクトされます。

ePBR は、自身のサービスチェーンのシーケンスで次の fail-action メカニズムをサポートします。

- ドロップ
- 転送
- バイパス

[ドロップ（Drop）]は、現在のシーケンス内のサービスが失敗したと見なされた場合に、トラフィックをドロップする必要があることを示します。これは、fail-action が設定されていない場合のデフォルトの動作です。

[転送（Forward）] は、現在のシーケンスでサービスに障害が発生した場合、トラフィックが通常のルーティングを使用する必要があることを示します。この fail-action メカニズムは、チェーン内で単一のサービス機能が定義されている場合にのみサポートされます。

[バイパス（Bypass）] は、現在のシーケンス内のサービスが失敗したと見なされた場合に、チェーンの次のサービス機能にリダイレクトする必要があることを示します。単一シーケンスのサービスチェーンで、バイパス トラフィックを使用する場合、転送の fail-action オプションのような通常のルーティングが使用されます。

サービス機能のロードバランシング方式

Cisco NX-OS 10.5(1)F 以降、GPO を使用した ePBR は、同じサービス機能の一部であるサービス エンドポイント間のロードバランシング トラフィックをサポートします。チェーン内のすべてのサービス機能に同じ負荷分散メカニズムが必要な場合は、サービスチェーンに対して負荷分散方式を構成できます。チェーン内の 1 つ以上のサービス機能またはシーケンスで別のロードバランシング メカニズムが必要な場合は、チェーン内の特定のシーケンスに対してこれを構成できます。トラフィックは、IPヘッダーで使用可能なプロトコル指示とともに、送信元 IP パラメータ、接続先 IP パラメータ、または送信元 IP、接続先 IP を使用して負荷分散できます。マイクロセグメンテーションを備えた ePBR により、トラフィックは両方向で同じサービス デバイスに対称的にロードバランシングされます。

重み付けロードバランシング

Cisco NX-OS 10.5(1)F 以降、GPO を使用する ePBR は、エンドポイントの構成された重みに比例するサービス エンドポイントへのロード バランシング トラフィックをサポートします。

サービス関数内で設定された各サービスエンドポイントには、重み設定を構成できます。重みの範囲は、1 ～ 10 です。サービス機能ごとの重みの合計数は最大 128 です。サービスエンドポイントは、デバイスの帯域幅または容量に基づいてオプションで設定できます。サービス機能に重みが構成されていない場合、サービス機能内に設定されているすべてのサービスエンドポ

イントの重みは 1 と見なされ、トラフィックは等コスト マルチパス メカニズムによってロードバランシングされます。

エンドポイントで障害が発生した場合、障害が発生したエンドポイントのトラフィックの受信では、重みの高いエンドポイントが重みの低いエンドポイントよりも優先されます。

サービス デバイスへの重み付けされたトラフィック分散は、ロードバランシング アルゴリズムの選択と、Nexus 9000 スイッチによるサービスチェーンのために受信されるトラフィックフローの送信元または接続先 IP アドレスの分散に依存することに注意してください。重み付けロードバランシングの配置については、図 2 を参照してください。

図 *5:* 重み付けロードバランシング

Destination	IP	Weight (optional)	%
Destination 1	10.1.1.1	4	40%
Destination 2	10.1.1.2	3	30%
Destination 3	10.1.1.3	2	20%
Destination 4	10.1.1.4	1	10%

N+M 冗長性

Cisco NX-OS 10.5(1)F 以降、GPO を使用した ePBR は、ホット スタンバイモードでサービス エンドポイントを定義する機能をサポートしています。M 個のホット スタンバイ サービス エンドポイントをサービス機能用に定義でき、N 個のプライマリ（アクティブ）エンドポイントを使用できます。すべてのプライマリ サービス エンドポイントが使用可能な場合、トラフィックはホット スタンバイ サービス エンドポイントにリダイレクトされません。

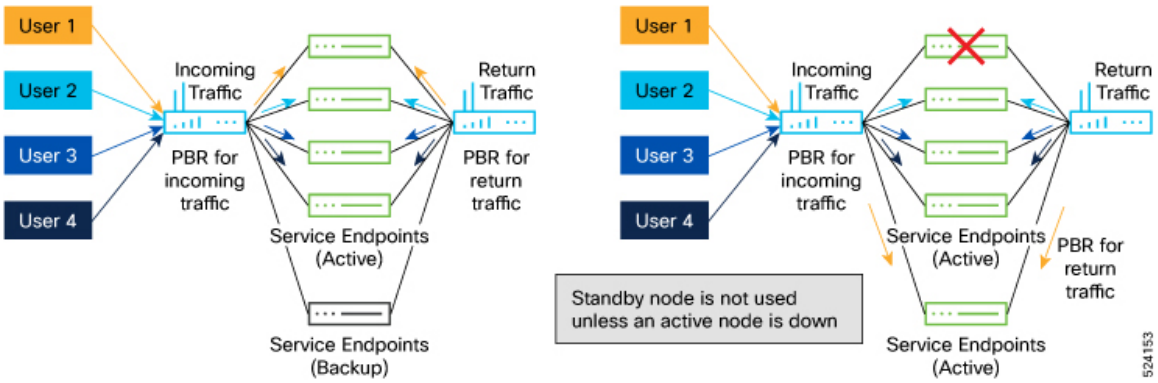
ホット スタンバイ エンドポイントを持つ ePBR サービス機能内のアクティブなサービス エンドポイントに障害が発生すると、障害が発生したサービス エンドポイントにロード バランシングされたトラフィックが、使用可能なホット スタンバイ サービス エンドポイントにリダイレクトされるようになりました。

より多くのアクティブなエンドポイントの後続の障害が発生し、すべてのホット スタンバイ エンドポイントがアクティブエンドポイントのバックアップとして使用された後、新しく障害が発生したアクティブエンドポイントによって処理されたトラフィックは、1 つ以上の使用可能なアクティブおよびホット スタンバイ エンドポイントにリダイレクトされ始める可能性があります。

アクティブなエンドポイントが回復すると、障害が発生する前にリダイレクトされていたトラフィックが復元されます。この動作は避けられず、復元されたステートフル サービス エンドポイントを介してトラフィック セッションを再確立する必要がある場合があります。

ホットスタンバイ エンドポイントには重みを設定できます。重み付けされたホットスタンバイ エンドポイントを持つ ePBR サービス機能内の重み付けされたアクティブ エンドポイントに障害が発生した場合、トラフィックは最初に、障害が発生したアクティブエンドポイントと同等またはそれ以上の重みを持つ重み付けされたホットスタンバイ エンドポイントにリダイレクトされます。 N+M 冗長構成については、図 3 を参照してください。

図 *6 : N+M* 冗長性



NAT デバイスへのリダイレクション

Cisco NX-OS 10.5(1)F 以降、GPO を使用した ePBR は、トラフィックの宛先または送信元 IP アドレスを変更するサービスデバイスへのトラフィックのリダイレクションをサポートします。これらのデバイスは、外部ロードバランサ、NATTing ファイアウォール、および CGNAT デバイスである場合があります。

サービスデバイスは、接続先 NAT（SNAT が無効になっているロードバランサ）、送信元 NAT（リターン トラフィック用の CGNAT デバイス）のみ、またはその両方（SNAT が有効になっているロードバランサ）を実行できます。

順方向で接続先 NAT を実行する外部ロードバランサなどのデバイスへのトラフィックは、ポリシーベースのリダイレクションを必要としませんが、ロードバランサによって公開された VIP アドレスに到達するために許可される必要があります。

同様に、順方向で送信元 NAT を実行した外部ロードバランサや CGNAT デバイスなどのデバイスに戻る逆方向のトラフィックには、ポリシーベースのリダイレクションは必要ありませんが、許可する必要があります。

送信元 NAT が有効になっていない外部ロードバランサなどのデバイスへのトラフィックは、逆方向のトラフィックに対してポリシーベースのリダイレクションが必要です。

前述のように、これらのサービスへのトラフィックは、NAT 機能に基づいてさまざまな方法で処理する必要があります。さらに、これらのアプライアンスによるトラフィックの IP アドレスの変更により、これらのサービスへのリダイレクションの前後で、接続先または送信元のセキュリティグループタグが異なる場合があります。これらの差異を処理するには、通常、複雑な非対称の単方向コントラクトが必要になる場合があります。

ePBR は、特定のシーケンスの ePBR サービスチェーン内のサービス機能が接続先や送信元 NAT 機能を持っていることをユーザーが示すことを可能にすることで、ユーザーのコントラクトの作成を簡素化します。これは、トラフィックの順方向および逆方向に対して、チェーン内のサービスのアクションを設定することによって実行されます。

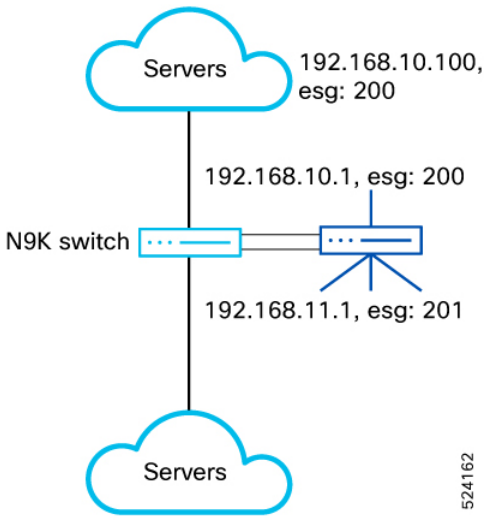
- トラフィックに対してのみ接続先 NAT を実行するサービスは、順方向の route アクションで構成されます。

- トラフィックに対して接続先 NAT と送信元 NAT の両方のみを実行するサービスは、トラフィックの両方向に対して route アクションを使用して設定されます。
- トラフィックに対して送信元 NAT のみを実行するサービスは、トラフィックの逆方向に対してのみ route のアクションが構成されます。

ルートの接続オプションを使用すると、ユーザーはコンシューマ ESG からプロバイダー ESG への単一のコントラクトを作成できます。この構成により、接続先 ESG の変更に伴い、コンシューマからロードバランサ、ロードバランサからプロバイダー ESG の間で個別のコントラクトを作成する負担が軽減されます。

どの方向に対してもアクションが設定されていない場合、チェーン内のサービス機能は両方向のリダイレクトを必要とするものとして扱われます。Fail-action およびしきい値機能は、順方向または逆方向に設定されたルートのアクションを持つサービスチェーン内のサービス機能ではサポートされません。

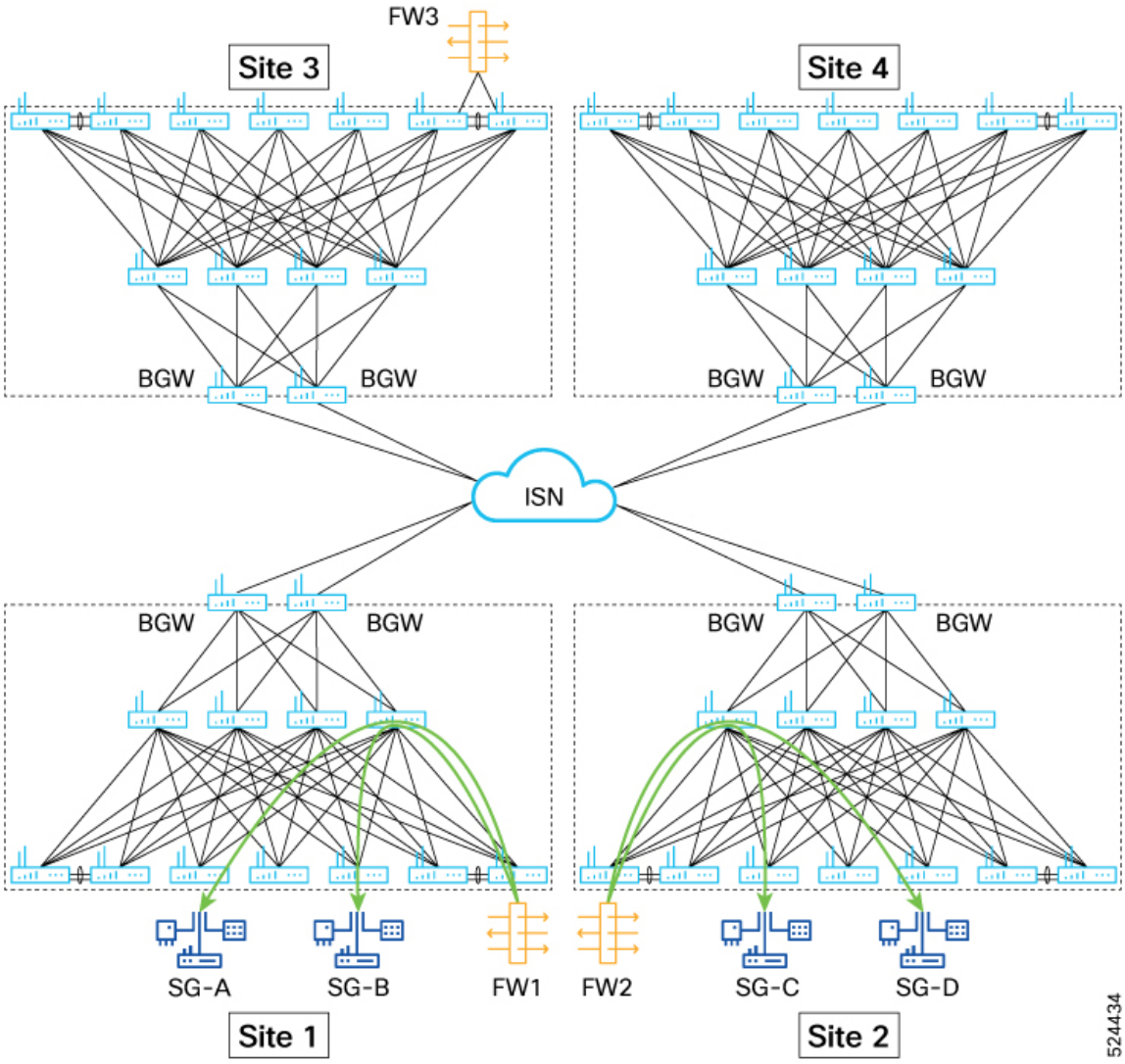
図 *7: 2* アーム ロードバランサ（*SNAT* なし）サービス デバイスの挿入



ePBR および GPO マルチサイト

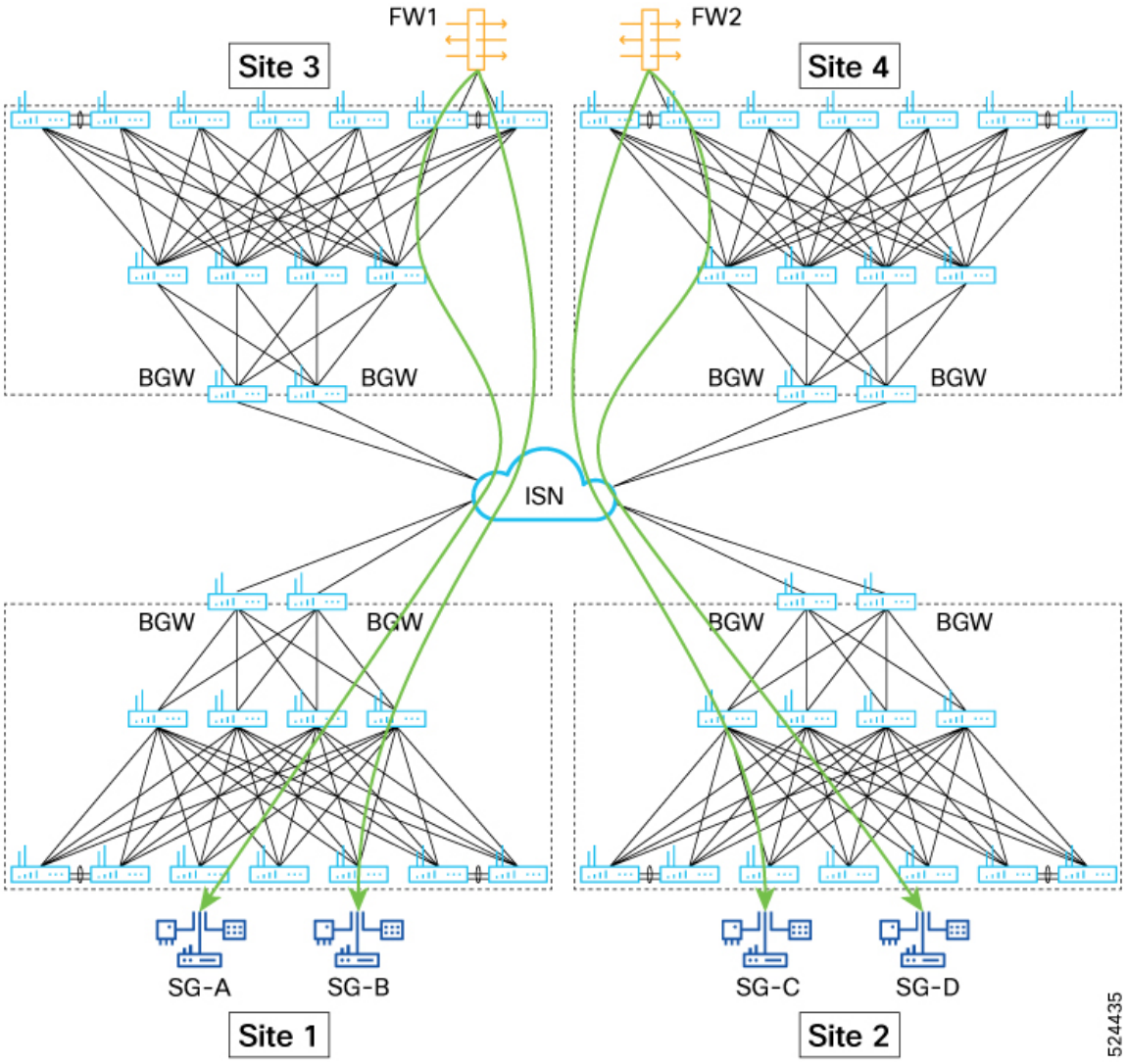
Cisco NX-OS リリース 10.5(2)F 以降では、複数のサイトに属する異なるセキュリティグループのエンドポイント間のトラフィック フローを、サービスチェーンのマルチサイト モードを有効にすることで、サービスチェーンにリダイレクトできます。これらのシングルノードまたはマルチノードのサービスチェーンは、ファイアウォール、ロード バランサ、NAT、IPS、TCP オプティマイザなどのサービス機能で構成できます。この機能を使用すると、ユーザーは、物理的に同じ場所に配置されているか地理的に分散されているかに関係なく、異なる NX-OS VXLAN EVPN ファブリック間でサービスチェーンを使用してセキュリティ グループを相互接続および管理できます。

図 *8:* ローカル サービス チェーンを使用するローカル サイト ローカル サイト セキュリティ グループ



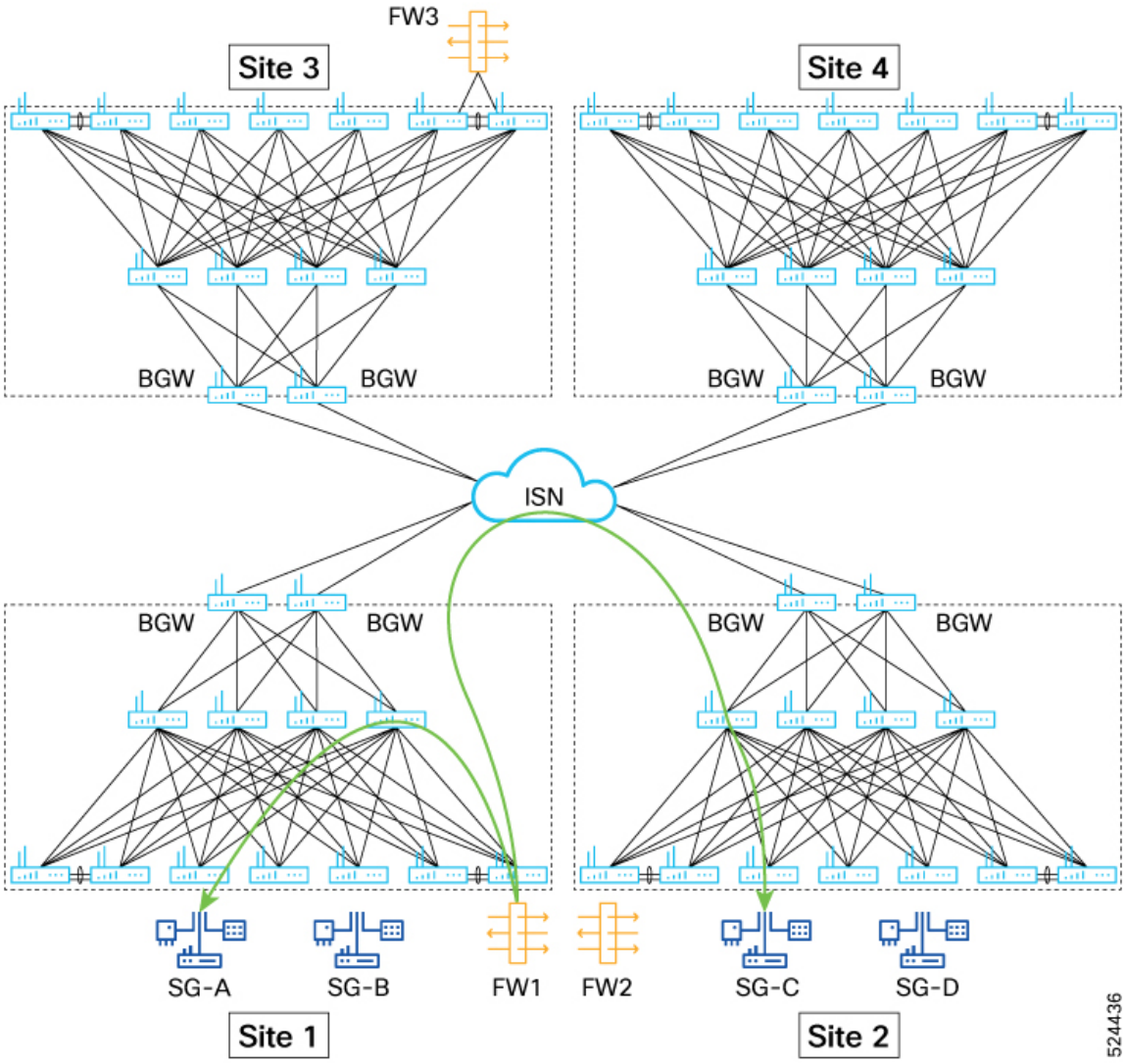
サイト 1 と 2 には独自のサービス機能があり、同じサイト内のサービス機能 FW 1 と FW 2 をそれぞれ使用することにより、SG-A と SG-B、および SG-C と SG-D の間にサービスチェーンが作成されます。サイト 1 のフェールオーバー サービス チェーンは、サイト 2 の FW2 を使用して作成し、サイト 2 のフェールオーバー サービス チェーンは、サイト 1 の FW1 を使用して作成できます。

図 *9:* ローカル サービス チェーンのないローカル サイト セキュリティ グループ



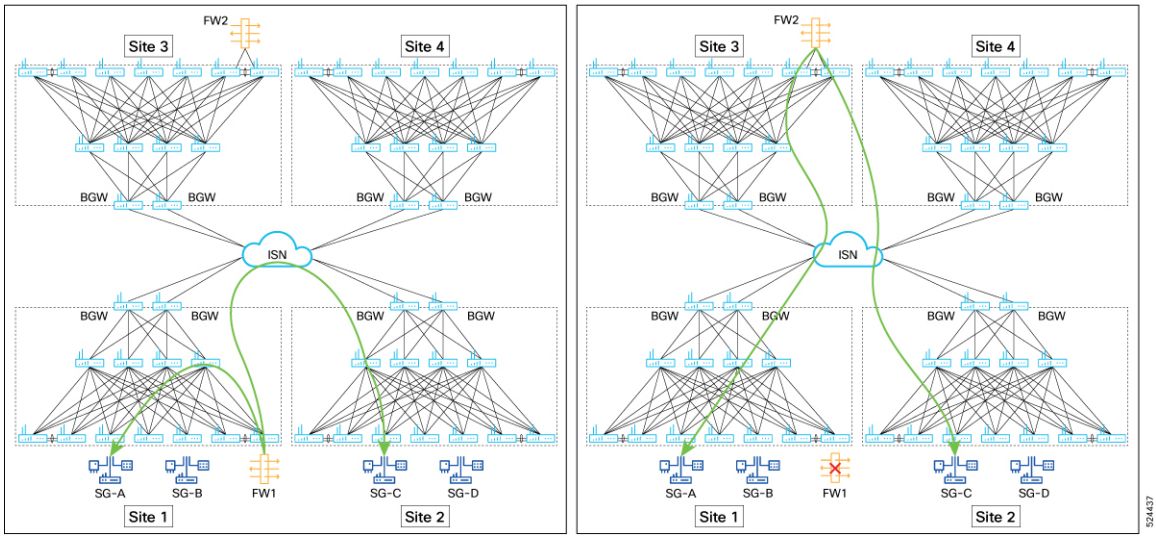
同じサイト内で使用可能なサービス機能がない場合、ユーザーはリモートサイトで使用可能なサービス機能を使用し、コントラクトを使用してサービス チェーンを作成できます。

図 *10* : 異なるサイトでの送信元ワークロードと接続先ワークロードのサービスチェーン インスペクション



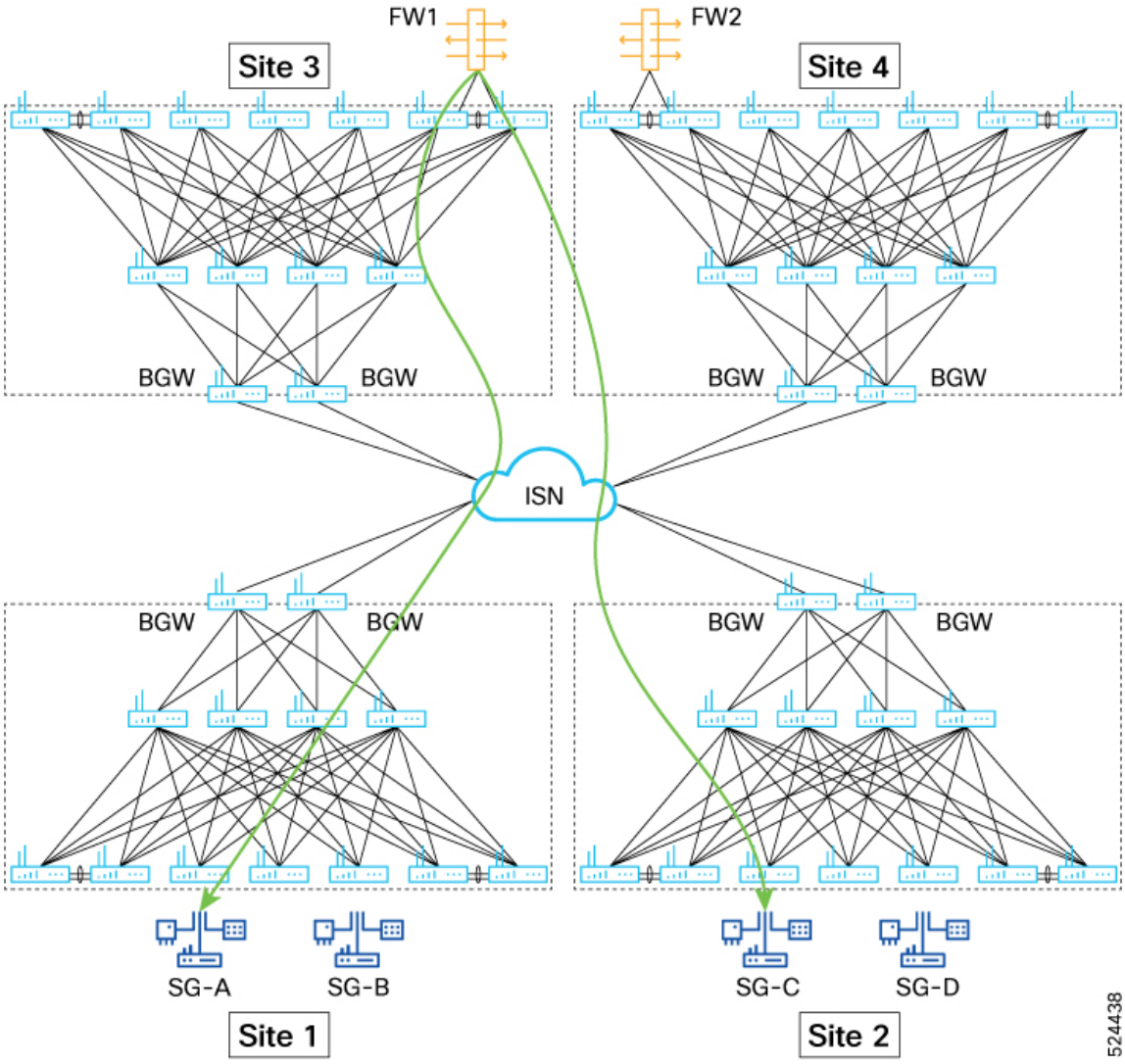
複数のサイトにまたがるワークロードのサービス チェーンを構成する場合は、送信元サイトまたは接続先サイトのいずれかにあるサービス チェーンを選択します。ePBR ポリシーは、セキュリティ グループが小さいサイトに適用されます。

図 *11 : 2* つのサイトのいずれかでのみのサービスチェーン（サイト間フロー）とフェールオーバー



サービス チェーンが 1 つのサイトにのみ存在するサービス チェーン インスペクションを使用したサイト間ワークロード。順方向フローと逆方向フローの両方が同じチェーンを通過する必要があります。サービスチェーンに障害が発生した場合は、順方向と逆方向の両方のフローに対して、サードサイトのサービス チェーンへの後続フェールオーバーが必要です。

図 *12* : 送信元サイトまたは接続先サイトにサービスチェーンがない



サービスチェーンが送信元サイトまたは接続先サイトに存在せず、第3のサイトにのみ存在する場合の、サービス チェーン インスペクションを使用するサイト間ワークロード。順方向フローと逆方向フローの両方が同じチェーンを通過する必要があります。

サービスチェーンの ePBR フェールオーバー グループ

Cisco NX-OS リリース 10.5(2)F 以降、ePBR はサービスチェーンのフェールオーバー グループをサポートし、ファブリックのリモートサイトにあるサービスチェーンにトラフィックをフェールオーバーできるようになりました。フェールオーバー グループは、プライマリ サービス チェーンに障害が発生したときに使用する必要がある、フォールバック サービスチェーンの集まりです。ユーザーはフォールバック サービスチェーンを設定し、サイト間の遅延、地理的近接性、またはキャパシティに基づいて設定を割り当てることができます。フォールバック サービスチェーンは、プライマリ チェーンと同じ数のサービス ノードからなるフェールオーバー グループ内のメンバーチェーンとして参照されるもので、前もってシステムで定義する必要が

あります。フェールオーバー グループ内には、最大5つのメンバーチェーンを構成できます。次に示すのは、一般的な展開シナリオのいくつかの例です。

注意事項と制約事項

マイクロセグメンテーションが構成されたePBRには、次のガイドラインと制限事項があります。

- Cisco NX-OS リリース 10.5（3）F 以降、ユーザーはサービス グループ内のアクティブ エンドポイントの数のしきい値をパーセンテージで設定できます。アクティブなエンドポイントの割合がしきい値を下回ると、サービスグループはダウンしていると見なされ、構成された fail アクションに基づいてトラフィックがドロップ、バイパス、または転送されます。
  - しきい値が構成されていない場合、または構成値が0の場合、この機能は無効のままになります。
  - サービスグループが無効になった後、サービスグループ内のアクティブなサービスエンドポイントの割合がしきい値以上になると、サービスグループは再び稼働していると見なされます。
- マイクロセグメンテーションを使用したePBRは、マイクロセグメンテーションがサポートされているすべてのプラットフォームでサポートされています。詳細については、「**注意事項と制限事項（Guidelines and Limitations）**」を参照してください。
- Cisco NX-OS リリース 10.5（3）F 以降、マルチノードおよびマルチサイト ファブリックの GPO ベースのサービス リダイレクション機能に対する ISSU のサポートが追加されています。
- NXOS 10.5(1)F では、SGACL ベースのサービス リダイレクションは、チェーン内の単一のサービス機能に対してのみサポートされます。サービス機能には、1 つ以上のレイヤ 3 ワンアームまたはデュアルアーム サービス エンドポイントを含めることができます。
- GPO ベースの ePBR サービスチェーン内のロードバランサ サービス機能は、単一のロードバランサ エンドポイントでのみ構成できます。
- ワンアームとデュアルアームのサービスエンドポイントが混在するサービス機能はサポートされていません。
- ePBR サービスのすべてのアクティブなエンドポイントの重みの合計が 128 を超えることはできません。
- 外部ロードバランサがサーバー クラスタの正常性をモニターするには、ロードバランササービスのレイヤ4～7セキュリティタグとサーバーの間で許可アクションを含むコントラクトを明示的に作成する必要があります。
- ワンアームデバイスを使用したサービスには、逆セキュリティグループ識別子を構成しないでください。

- デュアル アーム デバイスを使用するサービスは、順方向セキュリティ グループとは異なる逆方向セキュリティ グループ識別子を使用して構成する必要があります。
- デュアルアーム デバイスを使用するサービスでは、エンドポイントのフォワード アームとリバース アームに異なるサービス VLAN を使用する必要があります。サービス機能内の 1 つ以上のサービス エンドポイントのフォワード アームは 1 つのサービス VLAN を共有でき、1 つ以上のサービス エンドポイントのリバース アームは別のサービス VLAN を使用できます。
- ユーザーは、サービス VLAN がサービス エンドポイント専用に使用され、他のホスト トラフィックには使用されていないことを確認する必要があります。ホストをこのような VLAN に接続することはできません。これは、このようなトラフィックの誤った分類を回避するために必要です。
- ePBR サービス内で定義されたフォワードおよびリバース セキュリティ グループは、接続されたインターフェイス（インターフェイス VLAN）が構成されている VXLAN リーフ スイッチのレイヤ 4 ～ 7 セキュリティ グループ セレクタとして定義する必要があります。
- NXOS 10.5(1)F では、サービスで使用されるエンドポイント接続インターフェイスは、インターフェイス VLAN のみである必要があります。エンドポイント接続インターフェイスは、レイヤ 3 物理インターフェイス、サブインターフェイス、レイヤ 3 ポートチャネルまたはポートチャネル サブインターフェイス、または IPACL EPBR でサポートされているその他のインターフェイスにすることはできません。
- セキュリティグループとサービス VLAN は ePBR サービス間で共有できますが、ユーザーは、これらのサービスをチェーンで使用するコントラクトに競合する一致フィルタまたはアクションがないことを確認する必要があります。
- NXOS 10.5(1)F では、トラフィックがリダイレクトされるサービスは、コントラクトと同じ VRF コンテキストで構成する必要があります。
- IPv4 トラフィックの match クラスマップは、IPv4 サービスを含むサービスチェーンで構成する必要があり、IPv6 トラフィックの match class-map は、IPv6 トラフィックを含むサービスチェーンで構成する必要があります。
- コントラクトの any-any 送信元および宛先セキュリティグループと一致する必要があり、サービスデバイスへのリダイレクトが必要なトラフィックは、ワンアームサービスデバイスにのみリダイレクトできます。

  コントラクト内の any-any 送信元および宛先セキュリティグループに一致する必要があるトラフィックは、マルチノードサービスチェーンにリダイレクトするように構成できません。
- ユーザーは、同じ送信元と接続先のセキュリティグループを使用する複数のコントラクトが、同じトラフィック フローに対して異なるサービスリダイレクションの結果を生じさせるポリシーおよび一致クラスマップにより構成されていないことを確認する必要があります。

- サービスチェーン内のシーケンスに対して fail-action が構成されている場合は、サービスレベルまたはエンドポイントレベルのプローブを介して、サービスに対してプローブを一貫して有効にすることをお勧めします。
- プローブ トラフィックは別の CoPP クラスに分類することが推奨されています。そうしないと、プローブ トラフィックがデフォルトの CoPP クラスを使用し、スーパーバイザ トラフィックのスパイク時に、IP SLA 状態の変化が継続的して生じる可能性があります。CoPP 構成について詳しくは、「IP SLA パケットの CoPP の構成」を参照してください。
- ePBR の管理および運用のアウトオブサービス機能は、マイクロセグメンテーションを使用したサービス リダイレクションで使用されるサービスではサポートされません。詳細については、 ePBR L3 の構成を参照してください。
- デュアルアーム デバイスのフォワード アームとリバース アームのエンドポイントの状態は、自動的に同期されません。これが必要な場合は、フォワード アームとリバース アームで同じプローブ トラック構成を使用する必要があります。
- エンドポイント用に設定されたプローブ トラックは、同じエンドポイントのフォワード アームとリバース アームの間で共有できますが、同じサービスまたは異なるサービスのエンドポイント間では共有できません。
- プローブ トラックは、デュアルアーム デバイスのフォワードアームとリバースアーム間でエンドポイントの状態を自動同期するために使用する必要があります。
- サービス ノードは、送信元 VRF または接続先 VRF の一部にすることも、別の VRF にすることもできます。サービス ノードの一部が送信元 VRF の一部であり、一部が接続先 VRF の一部である場合、送信元に続くすべての連続する要素は、送信元 VRF に一様に関連する必要があります。チェーン内の要素の VRF が接続先 VRF に関連している場合、これに続くすべての連続する要素が、サービスチェーンの最後まで宛先 VRF に関連している必要があります。
- デュアルアーム サービス エンドポイントでは、各アームを異なる VRF に設定することはできません。

マルチノード サービスチェーンのガイドラインと制限事項：

- サービス チェーンでは最大 5 つのサービス機能（ノード）がサポートされます。
- マルチノード構成では、バイパスおよびドロップの fail-action オプションのみがサポートされます。転送の fail-action オプションはサポートされていません。
- マルチノード サービス チェーン内では、IP アドレス変換を実行する単一のサービス機能（ロード バランサまたは CGNAT デバイス）のみを構成できます。

マルチサイト サービスチェーンのガイドラインと制限事項：

- 特定のサービス チェーンのすべてのサービス機能は、単一のサイトに属する必要があります。
- フェールオーバー グループ内では、最大 5 つのフェールオーバー サービスチェーンがサポートされます。

- VXLAN グループ ポリシー オプションで EPBR サービスチェーンを使用しているマルチサイト ファブリックでは、最大 10 のサイトがサポートされます。
- マルチサイト フェールオーバーオプションは、ロードバランサデバイスで構成されるサービスチェーンではサポートされません。ロードバランサ デバイスには一意の VIP があり、異なるロードバランサにフェールオーバーされます。これは、VTEP の範囲外で変更された VIP により、フェールオーバーの決定が下されるからです。
- サービスチェーンで使用される、送信元 NAT が有効になっていないロードバランサ デバイスと、ロードバランシング先のサーバーは、同じサイトに共存している必要があります。
- サービスチェーンと、使用するように設定されたフェールオーバー サービスチェーンは、同じ数のサービスノードで構成する必要があります。ただし、各サービス ノードは、さまざまな数のサービスエンドポイントを持つことができます。
- サービスチェーン内のすべてのサービスノードと、使用するように構成されたフェールオーバーサービスチェーンは、同じサービス セキュリティグループで構成する必要があります。
- マルチサイトを構成する前に、TCAM プログラミング スケールが単一サイトの構成で指定された制限の 80% 未満に設定されていることを確認します。これは、モード マルチサイト ノブを有効にすると、ノブを使用しない同じ構成と比較して、TCAM プログラミングの要件が増加するためです。
- 外部接続先への GPO サービス リダイレクションが確実に機能するためには、マルチサイト ドメイン（MSD）内の各サイトが常に外部への直接接続を持つ必要があり、ローカルに接続されたエンドポイントの外部に対して /32 ホスト ルートとしてアドバタイズする必要があります（ホストベース ルーティング）。これにより、ノース サウス トラフィックが両方向で同じサービス端末にリダイレクトされるようになります。このシナリオは、一部のサイトにローカル サービス端末がない場合にもサポートされます。
- サイトが直接外部接続を欠き、他のサイトに依存している場合、またはホストベース ルーティング アドバタイズメントを実装できない場合、1 つのリモート サイトだけが、MSD 全体でVRF全体の出力/入力点として機能する必要があります。すべてのサイトからのトラフィックは、ルート プリファレンスの手法（BGP 属性操作など）を使用して、選択した出力サイトにルーティングする必要があります。

  同様に、そのファブリック VRF 宛てのリターン トラフィックは、トラフィックの対称性と一貫したポリシーの適用を維持するために、出力方向に選択されたのと同じサイトを介して MSD に入る必要があります。

（注） アクティブな出力/入力サイトを変更すると、一部のフローが別のサービス端末に再ハッシュされ、セッションのリセットまたはタイムアウトが発生する可能性があります。

- 複数のサイトが出力/入力に対応し、ルートプリファレンスが適用されていない場合、N/S トラフィックがサイト間でロードバランシング（ECMP）され、予測できないリダイレクトやサービスチェーンバイパスが発生する可能性があります。このシナリオはサポートされていません。

マイクロセグメンテーションの ePBR 構成

ePBR サービスの構成

始める前に

ここでは、ePBR サービスの構成について説明します。

手順の概要

1. **configure terminal**
2. **epbr service** *service-name*
3. **[no]threshold** *threshold-value*
4. **vrf** *vrf-name*
5. **[no] security-group <fwdGrp> [reverse**<*revGrp*>]
6. **[no] probe {icmp |** <*l4-proto*> **<port-num> [control**<*status*> **] | http get [** <*url-name*> **[version** <*ver*> **] | dns host** <*host-name*> **ctp} [frequency** <*freq-num*> **| timeout** <*timeout*> **| retry-down-count** <*down-count*> **| retry-up-count** <*up-count*> **| source-interface** <*src-intf*> **| reverse** <*rev-src-intf*> **]+**
7. **service-endpoint {ip** *ipv4-address* | **ipv6** *ipv6-address*}
8. **probe track** *track-ID*
9. **reverse {ip** *ipv4-address* | **ipv6** *ipv6-address*}
10. **mode hot-standby**
11. **weight** <*weight*>
12. **exit**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

	コマンドまたはアクション	目的
ステップ 2	**epbr service** *service-name* 例： `switch(config)# epbr service firewall`	新しい ePBR サービス機能を作成します。
ステップ 3	**[no]threshold** *threshold-value* 例： `switch(config)# threshold 26`	サービス グループのアクティブ エンドポイントの数のしきい値をパーセンテージで構成します。 デフォルト：0 範囲：0～100
ステップ 4	**vrf** *vrf-name* 例： `switch(config-epbr-svc)# vrf tenant_A`	ePBR サービス機能の VRF を指定します。

ステップ 5	**[no] security-group <fwdGrp> [reverse**<*revGrp*>]
	例：
	`switch(config-epbr-svc)# security-group 10 reverse 20`
	`switch(config-epbr-svc)# security-group 30`
		順方向および逆方向のサービスセキュリティ グループ タグを構成します。シングル アーム デバイスの場合、単一の順方向セキュリティ グループを指定する必要があります。デュアル アーム デバイスの場合、順方向セキュリティ グループと逆方向セキュリティ グループは一意である必要があります。
		構成を削除するには、このコマンドの **no** 形式を使用します。

ステップ 6	**[no] probe {icmp |** <*l4-proto*> **<port-num> [control**<*status*> **] | http get [** <*url-name*> **[version** <*ver*> **] | dns host** <*host-name*> **ctp} [frequency** <*freq-num*> **| timeout** <*timeout*> **| retry-down-count** <*down-count*> **| retry-up-count** <*up-count*> **| source-interface** <*src-intf*> **| reverse** <*rev-src-intf*> **]+**	サービス機能のプローブを構成します。同じ構成は、サービス エンドポイントの順方向アームと逆方向アームにも適用できます。このコマンドの no 形式を使用すると、構成が削除されます。 VXLAN環境に分散されたサービスエンドポイントの場合、一意の送信元 IP を IP SLA セッションに使用できるように、プローブの送信元ループバック インターフェイスを設定する必要があります。
ステップ 7	**service-endpoint {ip** *ipv4-address* | **ipv6** *ipv6-address*} 例： `switch(config-vrf)# service-endpoint ip 172.16.1.200`	ePBR サービスのサービス エンドポイントを構成します。ステップ 6 ～ 10 を繰り返して、別の ePBR サービス エンドポイントを構成できます。
ステップ 8	**probe track** *track-ID* 例： `switch(config-epbr-fwd-svc)# probe track 30`	サービスエンドポイントの順方向または逆方向アームのユーザー定義トラックを設定します。
ステップ 9	**reverse {ip** *ipv4-address* | **ipv6** *ipv6-address*} 例：	デュアルアーム サービス エンドポイントの逆方向 IP アドレスを定義します。これは、ワンアーム エ

	コマンドまたはアクション	目的
	`switch(config-epbr-fwd-svc)# reverse ip 172.16.30.200`	ンドポイントには必要ないことに注意してください。
ステップ 10	**mode hot-standby** 例： `switch(config-epbr-fwd-svc)# mode hot-standby`	サービスエンドポイントをホットスタンバイ エンドポイントとして構成します。
ステップ 11	**weight** <*weight*> 例： `switch(config-epbr-fwd-svc)# weight 6`	アクティブまたはホットスタンバイ エンドポイントの重みを構成します。 デフォルト値は 1 です。
ステップ 12	**exit** 例： `switch(config-vrf)# exit`	ePBR サービス構成モードを終了します。

ePBR サービスチェーンの構成

手順の概要

1. **configure terminal**
2. **[no] epbr service-chain** <*chain-name*>
3. **[no] mode multisite [failover-group <group-name>]**
4. **load-balance method** <*lb-method*> **{ src-ip | dst-ip | src-dst-ipprotocol}**
5. *sequence-number* **set service** *service-name***[fail-action { bypass | drop | forward}]**
6. **action {route | redirect} [reverse-action {route| redirect}]**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**[no] epbr service-chain** <*chain-name*> 例： `Switch(config-epbr-svc-chain)# epbr service-chain web`	ePBR サービスチェーンを構成します。設定を削除するには、このコマンドの no 形式を使用します。

	コマンドまたはアクション	目的
ステップ 3	**[no] mode multisite [failover-group <group-name>]** 例： `mode multisite failover-group fallback-web-chain3`	NX-OS 10.5(2)F 以降では、サービスチェーンのモード マルチサイトおよびフェールオーバー グループを構成できます。 • フェールオーバー グループは、モード マルチサイトがサービスチェーンに対して有効になっている場合にのみ構成できます。フェールオーバー グループを使用せずにモード multi-site を使用することができます。
ステップ 4	**load-balance method** <*lb-method*> **{ src-ip | dst-ip | src-dst-ipprotocol}** 例： `switch(config-epbr-svc-chain)# load-balance method src-ip`	ePBR サービスチェーンのロードバランシング方式を設定します。同じ構成を、サービスチェーン内の個々のサービス機能に適用することもできます。 デフォルト オプションは **src-dst-ipprotocol** です。

ステップ 5	*sequence-number* **set service** *service-name***[fail-action { bypass | drop | forward}]**
	例：
	`switch(config-epbr-svc-chain)#`
	`10 set service fw2 fail-action drop`
	`20 set service tcp_optim2 fail-action bypass`
		チェーン内の特定のシーケンスでサービス機能を指定し、そのシーケンスの失敗アクション メカニズムを指定します。
		NX-OS 10.5(2)F 以降では、マルチノード サービス チェーンを使用した GPO がサポートされています。

ステップ 6	**action {route | redirect} [reverse-action {route| redirect}]** 例： `switch(config-epbr-svc-chain-seq)# action route reverse-action route`	サービスの接続先や送信元 NAT 機能を示すために、チェーン内のサービスの転送やリバースアクションを構成します。 デフォルト オプションは **redirect** です。

フェールオーバー グループの構成

フェールオーバー グループを構成するには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **epbr service-chain** *service-chain-name*
3. **epbr failover-group** *failover-group-name*
4. **[no] service-chain <name> preference <preference>**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**epbr service-chain** *service-chain-name* 例： `Switch(config-epbr-svc-chain)# epbr service-chain web`	サービスチェーンを構成します。
ステップ 3	**epbr failover-group** *failover-group-name* 例： `switch(config-epbr-svc-chain)# epbr failover-group fallback-web-chain1`	フェールオーバー グループを構成します。
ステップ 4	**[no] service-chain <name> preference <preference>** 例： `switch(config-epbr-fail-group)# service-chain site1-web-chain preference 20`	フェールオーバー グループ内でフォールバック サービスチェーンを構成し、フォールバック サービスチェーンにプリファレンスを割り当てます。

ePBR サービスチェーン構成の確認

ePBR サービスチェーン構成を確認するには、次のコマンドを使用します：

手順の概要

1. **show epbr service [<svc-name>]**
2. **show epbr service-chain [<chain-name>] [reverse]**
3. **show tech-support epbr**
4. **show consistency-checker epbr service-chain { <svcChainName> | all }**
5. **show running-config epbr**
6. **show startup-config epbr**

手順の詳細

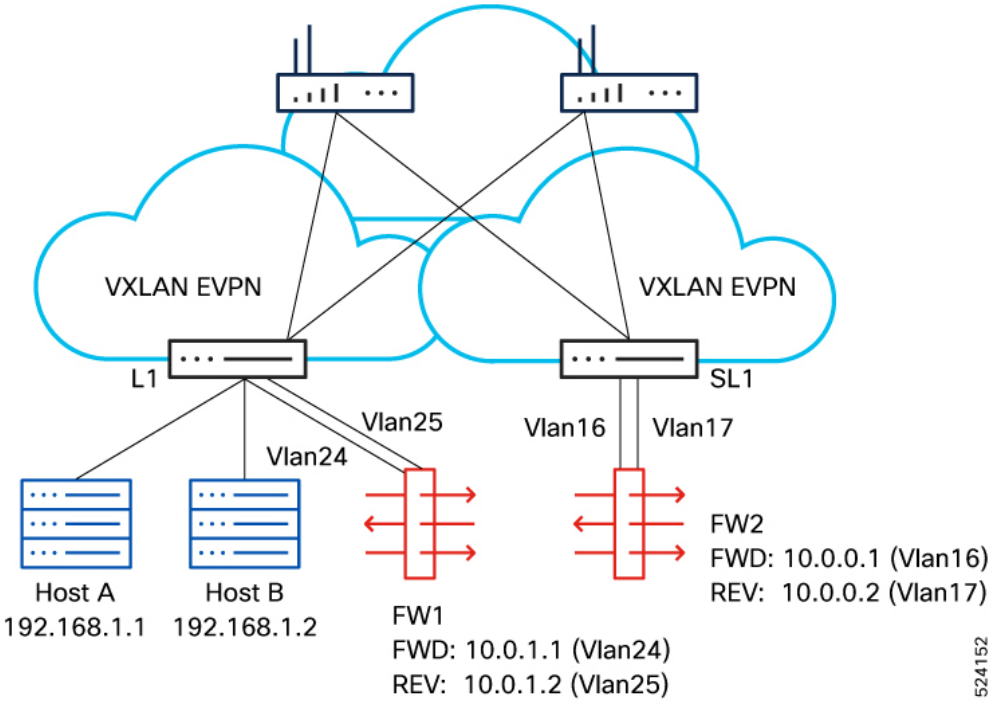
手順

	コマンドまたはアクション	目的
ステップ 1	**show epbr service [<svc-name>]** 例： `switch# show epbr service fw`	ePBR サービス機能とエンドポイントに関する情報を表示します。
ステップ 2	**show epbr service-chain [<chain-name>] [reverse]** 例： `switch# show epbr service-chain web`	順方向または逆方向の ePBR サービスチェーン ポリシーに関する情報を表示します。
ステップ 3	**show tech-support epbr** 例： `switch# show tech-support epbr`	ePBR のテクニカル サポート情報を表示します。
ステップ 4	**show consistency-checker epbr service-chain { <svcChainName> | all }** 例： `show consistency-checker epbr service-chain web`	ePBR 設定、コントロール プレーンでの ePBR のリダイレクション情報、および有効になっているヘルス モニタリング メカニズムの整合性チェックを実行します。
ステップ 5	**show running-config epbr** 例： `switch# show running-config epbr`	ePBR の実行構成を表示します。
ステップ 6	**show startup-config epbr** 例： `switch# show startup-config epbr`	ePBR のスタートアップ構成を表示します。

SGACL サービスチェーンの構成例

SGACL サービスチェーン構成を示す構成例については、図 5 を参照してください。

図 *13 :* 設定例



1. サービスのレイヤ 4 ～ 7 セレクタを作成します。

```
security-group 2010 name FWD
  type layer4-7
  match interface vlan 24
  match interface vlan 16
security-group 2011 name REV
  type layer4-7
  match interface vlan 25
  match interface vlan 17
```

2. ePBR サービスとエンドポイントの作成。

```
epbr service fw
  vrf tenant
  security-group 2010 reverse 2011
  probe tcp 80 frequency 5 timeout 3 source-interface
   loopback10 reverse loopback11
  service-end-point ip 10.0.1.1
    reverse ip 10.0.1.2
  service-end-point ip 10.0.0.1
    reverse ip 10.0.0.2
```

3. ホスト トラフィックのセキュリティグループ セレクタを作成します。

```
security-group 5051 name sec_5051
  match connected-endpoints vrf tenant ipv4 151.1.1.0/24

security-group 5050 name sec_5050
  match connected-endpoints vrf tenant ipv4 150.1.1.0/24
```

4. レイヤ 3、レイヤ 4 の一致基準を定義するセキュリティ クラスマップを作成します。

```
class-map type security match-any class_ipv4_tcp
  match ipv4 tcp dport 80
  match ipv4 tcp dport 443
```

5. ePBR サービスチェーンを構成します。vrf でのクラスマップ、ポリシーマップ、およびコントラクトの構成は、すべてのリーフで一貫している必要があります。

```
epbr service-chain web
  load-balance method src-dst-ipprotocol
  10 set service fw fail-action drop
```

6. セキュリティ ポリシーマップを設定し、サービスチェーンを必要な match クラスマップに付加します。

```
policy-map type security web_policy
  class type security class_ipv4_tcp
    service-chain web
```

7. コントラクトの設定

```
vrf context tenant
  security contract source 5050 destination 5051 policy web_policy
```

VRF コンテキストを強制モードに移行する方法の詳細については、セキュリティ グループ間のセキュリティ コントラクトの構成を参照してください。

設定の確認

- 次に、ePBR サービスとエンドポイントを構成する方法の例を示します。

```
show epbr service fw

Legend:

Operational State (Op-STS):  UP:Reachable, DOWN:Unreachable,

                             SVC-ADMIN-DOWN:Service shut

                             ADMIN-DOWN:Admin shut, OPER-DOWN:Out-of-service

Probe:
Protocol/Frequency(sec)/Timeout(sec)/Retry-Up-Count/Retry-Down-Count

Hold-down Threshold:         Count/Time(sec)

Service mode:                Full:Full-Duplex, Half:Half-Duplex

Type:                        L3:Layer-3, L2:Layer-2

Threshold:                   Threshold High/Low


Name                              Type      Service mode  VRF
================================================================================


fw                                L3        Full
tenant
```

```
Security-group    Reverse security-group   Threshold

=======================================================

2010              2011


Endpoint IP/Intf        Track SLA      Op-ST         Probe              Hold-down
 Role Weight

Reverse IP/Intf          Track SLA       Op-ST          Probe

=============================================================================================



10.0.1.1/               1  20001     UP          TCP/5/3/0/0
          A     1

10.0.1.2/               3   20003     UP          TCP/5/3/0/0


10.0.0.1/              2   20002     UP             TCP/5/3/0/0
            A     1

10.0.0.2/               4   20004     UP             TCP/5/3/0/0
```

- 次に、ePBR サービスチェーンを順方向または逆方向で確認する例を示します。

```
show epbr service-chain web

Service-chain : web

    service:fw, sequence:10, fail-action:Drop

      load-balance: Source-Destination-ipprotocol, action:Redirect

      state:UP

      IP 10.0.1.1 track 1 [UP]

      IP 10.0.0.1 track 2 [UP]


show epbr service-chain web reverse


Service-chain : web

    service:fw, sequence:10, fail-action:Drop

      load-balance: Source-Destination-ipprotocol, action:Redirect

      state:UP

      IP 10.0.1.2 track 3 [UP]
```

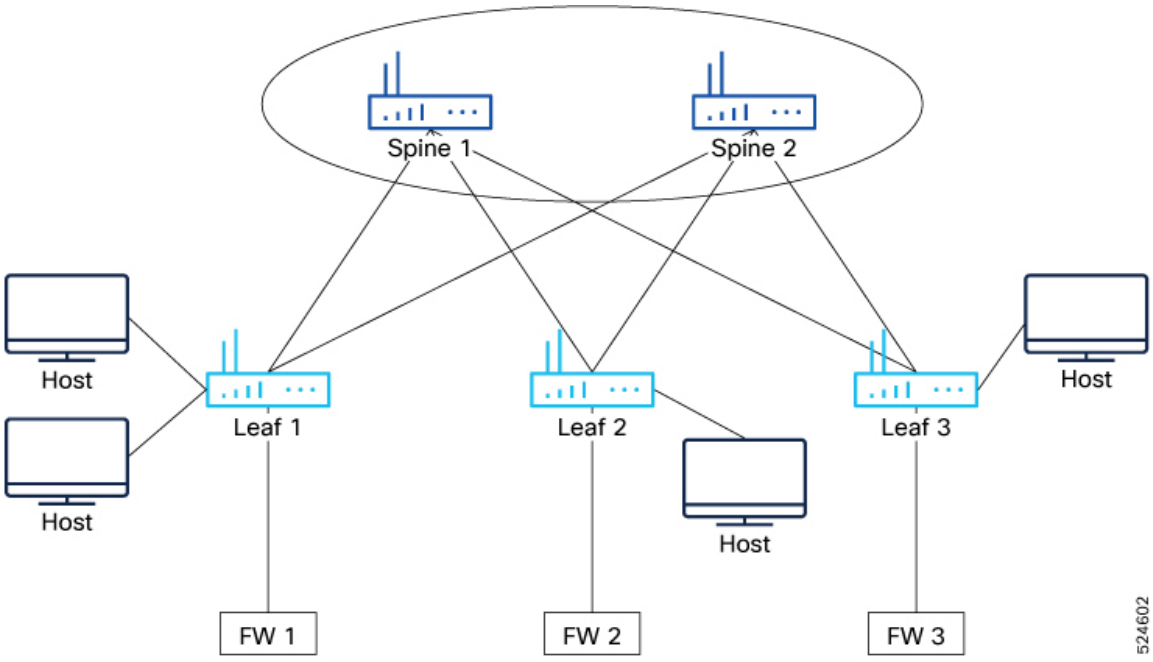
```
IP 10.0.0.2 track 4 [UP]
```

- 次に、サービスチェーンの整合性チェッカーを確認する例を示します。

```
show consistency-checker epbr service-chain chain1
EPBR CC: Service Chain validation passed
show consistency-checker epbr service-chain all
EPBR CC: Service Chain validation passed
```

マルチノード シングル サイト サービス チェーンの構成例

図 *14* : 設定例



次に、サービスチェーンの一部であるサービスとして3つのファイアウォールを持つ構成例を示します。各ファイアウォールは、複数のサービスエンドポイントで実装されます。

1. ePBR サービス fw1 の構成

```
epbr service fw1
  vrf tenant
  security-group 2010 reverse 2011
  probe icmp frequency 2 retry-down-count 2 retry-up-count 1 timeout 1 source-interface
 loopback3 reverse loopback4
  service-end-point ip 10.1.1.2
    weight 10
    reverse ip 11.1.1.2
  service-end-point ip 18.1.1.2
    reverse ip 19.1.1.2
  service-end-point ip 20.1.1.2
    mode hot-standby
    reverse ip 21.1.1.2
  service-end-point ip 253.1.1.2
    mode hot-standby
    weight 10
    reverse ip 254.1.1.2
```

```
  service-end-point ip 26.1.1.2
    weight 5
    reverse ip 27.1.1.2
  service-end-point ip 34.1.1.2
    mode hot-standby
    weight 6
    reverse ip 35.1.1.2
```

2. ePBR サービス fw2 の構成

```
epbr service fw2
  vrf tenant
  security-group 2013
  probe icmp frequency 2 retry-down-count 2 retry-up-count 1 timeout 1 source-interface
 loopback3 reverse loopback4
  service-end-point ip 255.1.1.2
    mode hot-standby
  service-end-point ip 50.1.1.2
    weight 10
  service-end-point ip 54.1.1.2
    weight 5
  service-end-point ip 58.1.1.2
  service-end-point ip 59.1.1.2
    mode hot-standby
    weight 10
  service-end-point ip 62.1.1.2
    mode hot-standby
    weight 6
```

3. ePBR サービス fw3 の構成

```
epbr service fw3
  vrf tenant
  security-group 2014 reverse 2015
  probe icmp frequency 2 retry-down-count 2 retry-up-count 1 timeout 1 source-interface
 loopback3 reverse loopback4
  service-end-point ip 12.1.1.2
    weight 10
    reverse ip 13.1.1.2
  service-end-point ip 22.1.1.2
    weight 10
    reverse ip 23.1.1.2
  service-end-point ip 32.1.1.2
    weight 5
    reverse ip 33.1.1.2
  service-end-point ip 40.1.1.2
    reverse ip 41.1.1.2
```

4. ePBR マルチノード サービスチェーンの構成

```
epbr service-chain FW-chain-v4
  load-balance method dst-ip
  10 set service service1-v4-2arm fail-action bypass
    load-balance method src-ip
  20 set service service3-v4-1arm fail-action drop
  30 set service service5-v4-2arm fail-action bypass
    load-balance method src-dst-ipprotocol
```

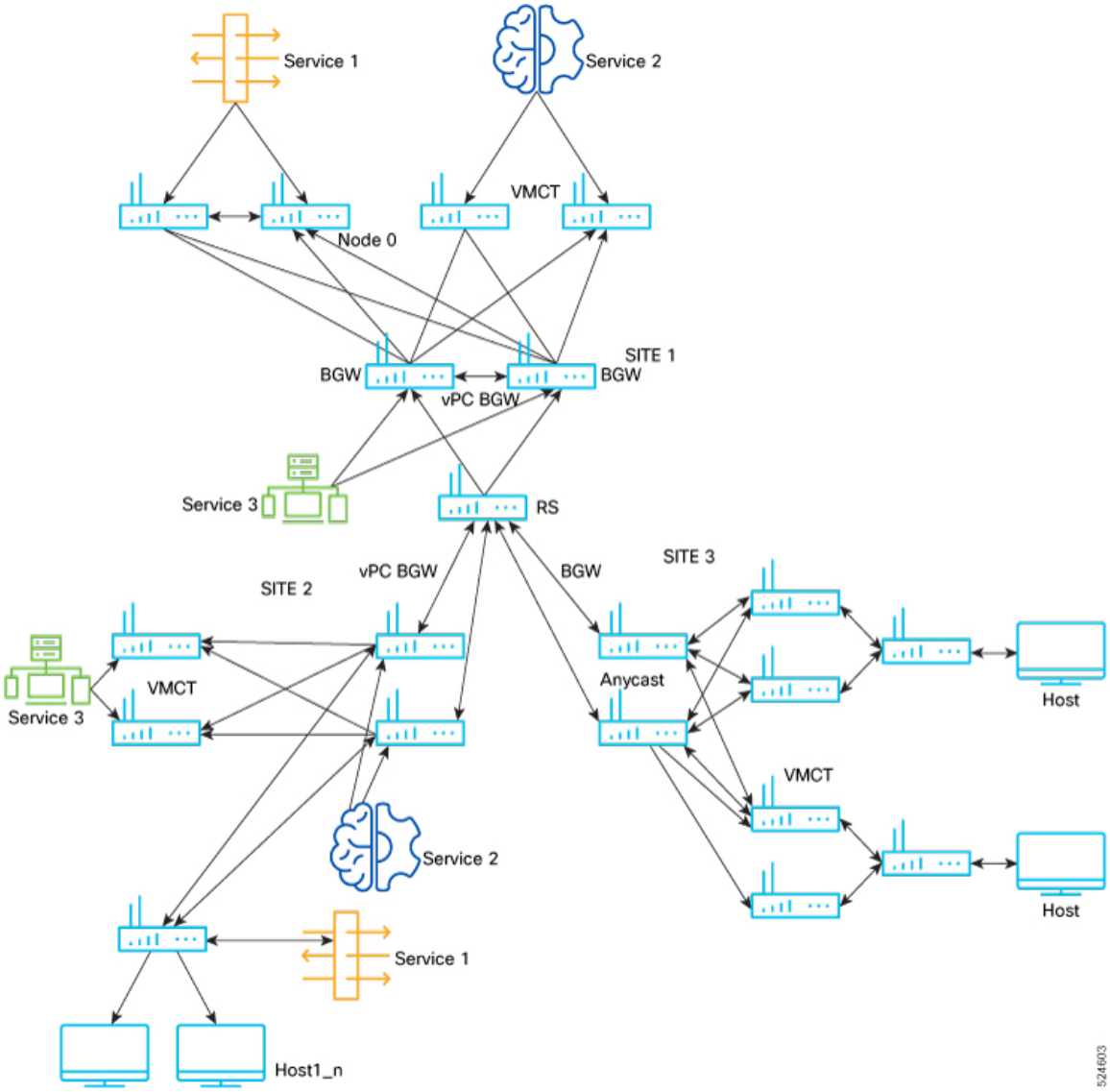
マルチノード サービス チェーンの確認

sh epbr service-chain FW-chain-v4

```
Service-chain : FW-chain-v4  state:UP
    service:fw1, sequence:10, fail-action:Bypass
      load-balance:Source-Destination-ipprotocol, action:Redirect
      state:UP
      IP 10.1.1.2 track 1 [UP]
      IP 18.1.1.2 track 2 [UP]
      IP 26.1.1.2 track 3 [UP]
      IP 20.1.1.2 track 4 [UP] [HOT-STANDBY]
      IP 34.1.1.2 track 5 [UP] [HOT-STANDBY]
      IP 253.1.1.2 track 6 [UP] [HOT-STANDBY]
    service:fw2, sequence:20, fail-action:Drop
      load-balance:Source-Destination-ipprotocol, action:Redirect
      state:UP
      IP 50.1.1.2 track 7 [UP]
      IP 54.1.1.2 track 8 [UP]
      IP 58.1.1.2 track 9 [UP]
      IP 59.1.1.2 track 10 [UP] [HOT-STANDBY]
      IP 62.1.1.2 track 11 [UP] [HOT-STANDBY]
      IP 255.1.1.2 track 12 [UP] [HOT-STANDBY]
    service:fw3, sequence:30, fail-action:Bypass
      load-balance:Source-Destination-ipprotocol, action:Redirect
      state:UP
      IP 12.1.1.2 track 13 [UP]
      IP 22.1.1.2 track 14 [UP]
      IP 32.1.1.2 track 15 [UP]
      IP 40.1.1.2 track 16 [UP]
```

GPO を使用したマルチサイト ePBR の構成例

図 *15* : 設定例



サイト 1

1. レイヤ 3、レイヤ 4 の一致基準を定義するセキュリティ クラス マップを作成します。

```
class-map type security match-any web_class
  match ipv4 tcp dport 80
```

2. セキュリティ ポリシーマップを構成し、サービスチェーンを必要な match クラスマップに付加します。

```
policy-map type security web
  class type security web_class
    service-chain site1-web-chain
```

3. ePBR サービスとエンドポイントの作成。

```
epbr service fw
  security-group 100
  probe icmp
  service-end-point ip 10.1.1.2
  service-end-point ip 20.1.1.2
   mode hot-standby

epbr service fw2
  security-group 100
  probe icmp
  service-end-point ip 11.1.1.2

epbr service fw3
  security-group 100
  probe icmp
  service-end-point ip 13.1.1.2
```

4. マルチサイトモードとフェール オーバー グループとチェーンの構成

```
epbr service-chain site1-web-chain
  mode multisite failover-group fallback-web-chain1
  load-balance method dst-ip
  10 set service fw fail-action drop

epbr service-chain site2-web-chain
  load-balance method dst-ip
  10 set service fw2 fail-action drop

epbr service-chain site3-web-chain
  load-balance method dst-ip
  10 set service fw3 fail-action drop

epbr failover-group fallback-web-chain1
  service-chain site2-web-chain preference 5
  service-chain site3-web-chain preference 20
```

サイト 2

1. レイヤ 3、レイヤ 4 の一致基準を定義するセキュリティ クラス マップを作成します。

```
 class-map type security match-any web_class
  match ipv4 tcp dport 80
```

2. セキュリティ ポリシーマップを設定し、サービスチェーンを必要な match クラスマップに付加します。

```
policy-map type security web
  class type security web_class
    service-chain site2-web-chain
```

3. ePBR サービスとエンドポイントの作成。

```
epbr service fw
  security-group 100
  probe icmp
  service-end-point ip 10.1.1.2
  service-end-point ip 20.1.1.2
   mode hot-standby

 epbr service fw2
  security-group 100
  probe icmp
```

```
  service-end-point ip 11.1.1.2

epbr service fw3
  security-group 100
  probe icmp
  service-end-point ip 13.1.1.2
```

4. マルチサイトモードとフェール オーバー グループとチェーンの構成

```
epbr service-chain site1-web-chain
  load-balance method dst-ip
  10 set service fw fail-action drop

epbr service-chain site2-web-chain
  mode multisite failover-group fallback-web-chain2
  load-balance method dst-ip
  10 set service fw2 fail-action drop

epbr service-chain site3-web-chain
  load-balance method dst-ip
  10 set service fw3 fail-action drop

epbr failover-group fallback-web-chain2
  service-chain site1-web-chain preference 5
  service-chain site3-web-chain preference 25
```

サイト 3

1. レイヤ 3、レイヤ 4 の一致基準を定義するセキュリティ クラス マップを作成します。

```
class-map type security match-any web_class
  match ipv4 tcp dport 80
```

2. セキュリティ ポリシーマップを構成し、サービスチェーンを必要な match クラスマップに付加します。

```
policy-map type security web
  class type security web_class
    service-chain site3-web-chain
```

3. ePBR サービスとエンドポイントの作成

```
epbr service fw
  security-group 100
  probe icmp
  service-end-point ip 10.1.1.2
  service-end-point ip 20.1.1.2
   mode hot-standby


epbr service fw2
  security-group 100
  probe icmp
  service-end-point ip 11.1.1.2

epbr service fw3
  security-group 100
  probe icmp
  service-end-point ip 13.1.1.2
```

4. サービスチェーンとマルチサイトの構成

```
epbr service-chain site1-web-chain
  load-balance method dst-ip
```

```
  10 set service fw fail-action drop


epbr service-chain site2-web-chain
  load-balance method dst-ip
  10 set service fw2 fail-action drop

 epbr service-chain site3-web-chain
  mode multisite failover-group fallback-web-chain3
  load-balance method dst-ip
  10 set service fw3 fail-action drop
```

5. フェールオーバー グループの構成

```
epbr failover-group fallback-web-chain3
  service-chain site1-web-chain preference 20
  service-chain site2-web-chain preference 25
```

マルチサイト構成の確認

次の show コマンドを使用して、マルチサイトの構成を確認できます。

- 次に、ePBR サービスチェーンの状態を確認する例を示します。

```
show epbr service-chain site1-web-chain
Service-chain : site1-web-chain  state:DOWN


  mode: multisite, failover-group:fallback-web-chain [AVAILABLE][IN USE]
failover-chain: site3-web-chain
    service:fw, sequence:10, fail-action:Drop
      load-balance:Destination-ip, action:Redirect
      state:DOWN
      IP 10.1.1.2 track 9 [DOWN]
      IP 20.1.1.2 track 10 [DOWN][HOT-STANDBY]
    service:tcp_optim, sequence:20, fail-action:Bypass
      load-balance:Destination-ip, action:Redirect
      state:UP
      IP 30.1.1.2 track 11 [UP]
```

- 次の例は、フェールオーバー グループ内のフェールオーバー チェーンの詳細を取得する方法を示しています。

```
show epbr failover-group fallback-web-chain

Failover group : fallback-web-chain
    Failover Service-chain : site2-web-chain  Preference: 1  state: DOWN
      service:fw2, sequence:10, fail-action:Drop
        load-balance:Destination-ip, action:Redirect
        state:DOWN
        IP 11.1.1.2 track 12 [DOWN]
      service:tcp_optim2, sequence:20, fail-action:Bypass
        state: UP
        load-balance:Destination-ip, action:Redirect
        state:UP

        IP 12.1.1.2 track 13 [UP]

    Failover Service-chain : site3-web-chain  Preference: 2  state: UP
      service:fw3, sequence:10, fail-action:Drop
        load-balance:Destination-ip, action:Redirect
        state:UP
        IP 13.1.1.2 track 14 [UP]
```

```
service:tcp_optim2, sequence:20, fail-action:Bypass
  load-balance:Destination-ip, action:Redirect
  state:UP

  IP 14.1.1.2 track 15 [UP]
```

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