



# 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 (1 ページ)
- ePBR サービスとサービスチェーン (2 ページ)
- サービスのセキュリティ グループ (3 ページ)
- 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 (4 ページ)
- ePBR ヘルス モニタリング、および障害アクション (4 ページ)
- サービス機能のロードバランシング方式 (5 ページ)
- NAT デバイスへのリダイレクション (7 ページ)
- ePBR および GPO マルチサイト (8 ページ)
- 注意事項と制約事項 (14 ページ)
- マイクロセグメンテーションの ePBR 構成 (18 ページ)
- SGACL サービスチェーンの構成例 (23 ページ)

## 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なります。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。

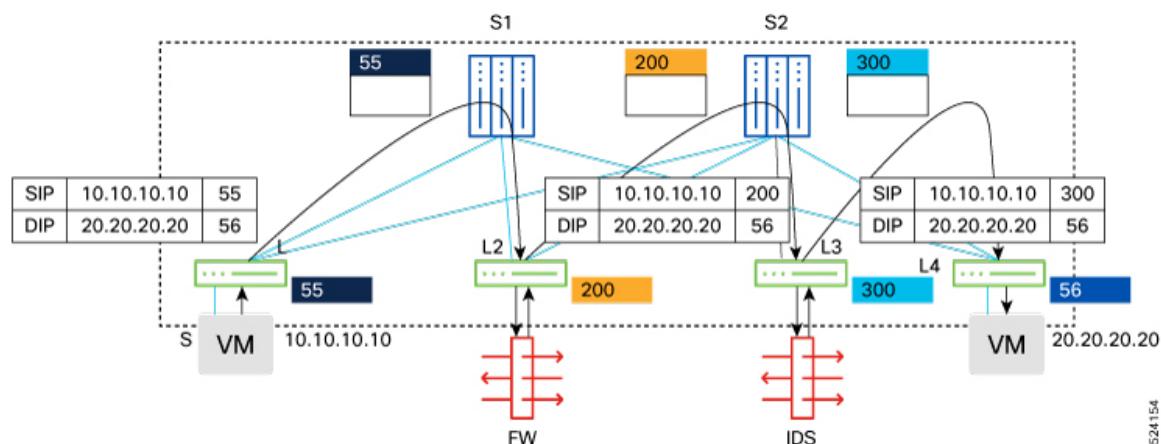
サービス エンドポイントのすべての転送アームに接続されたインターフェイスは、ePBR サービスの転送セキュリティ グループとして指定されているものと同じ識別子にマッピングする必要があります。

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 1: 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

# 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 ポイントに割り当たない場合、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た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

**N+M 変更性**

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 2: 重み付けロードバランシング

**N+M 変更性**

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。

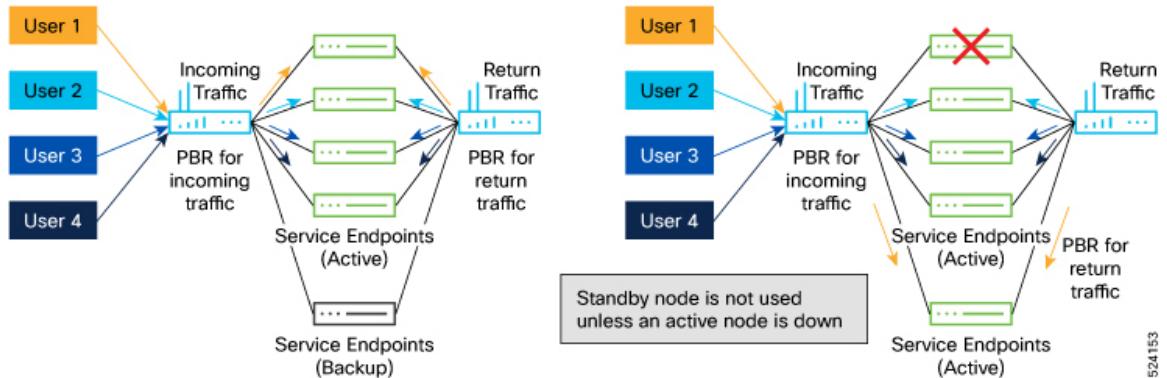
ホットスタンバイ エンドポイントを持つ ePBR サービス機能内のアクティブなサービス エンドポイントに障害が発生すると、障害が発生したサービス エンドポイントにロードバランシングされたトラフィックが、使用可能なホットスタンバイ サービス エンドポイントにリダイレクトされるようになりました。

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 変更構成については、図 3 を参照してください。

図 3: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 が有効になら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。

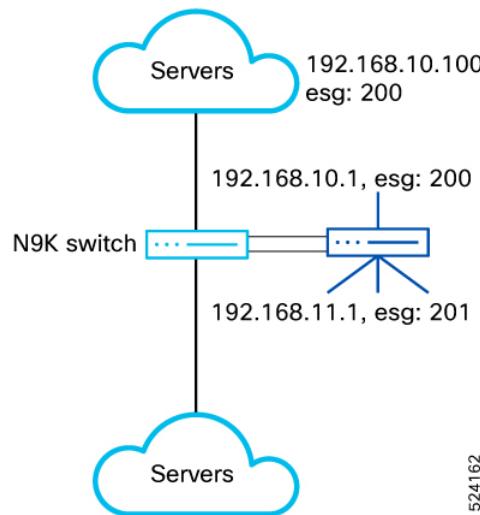
## ■ ePBR および GPO マルチサイト

- トライ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、トライ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。
- トライフィックに対して送信元 NAT のみを実行するサービスは、トライフィックの逆方向に對してのみ 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 4:2 アーム ロードバランサ（SNATなし）サービス デバイスの挿入

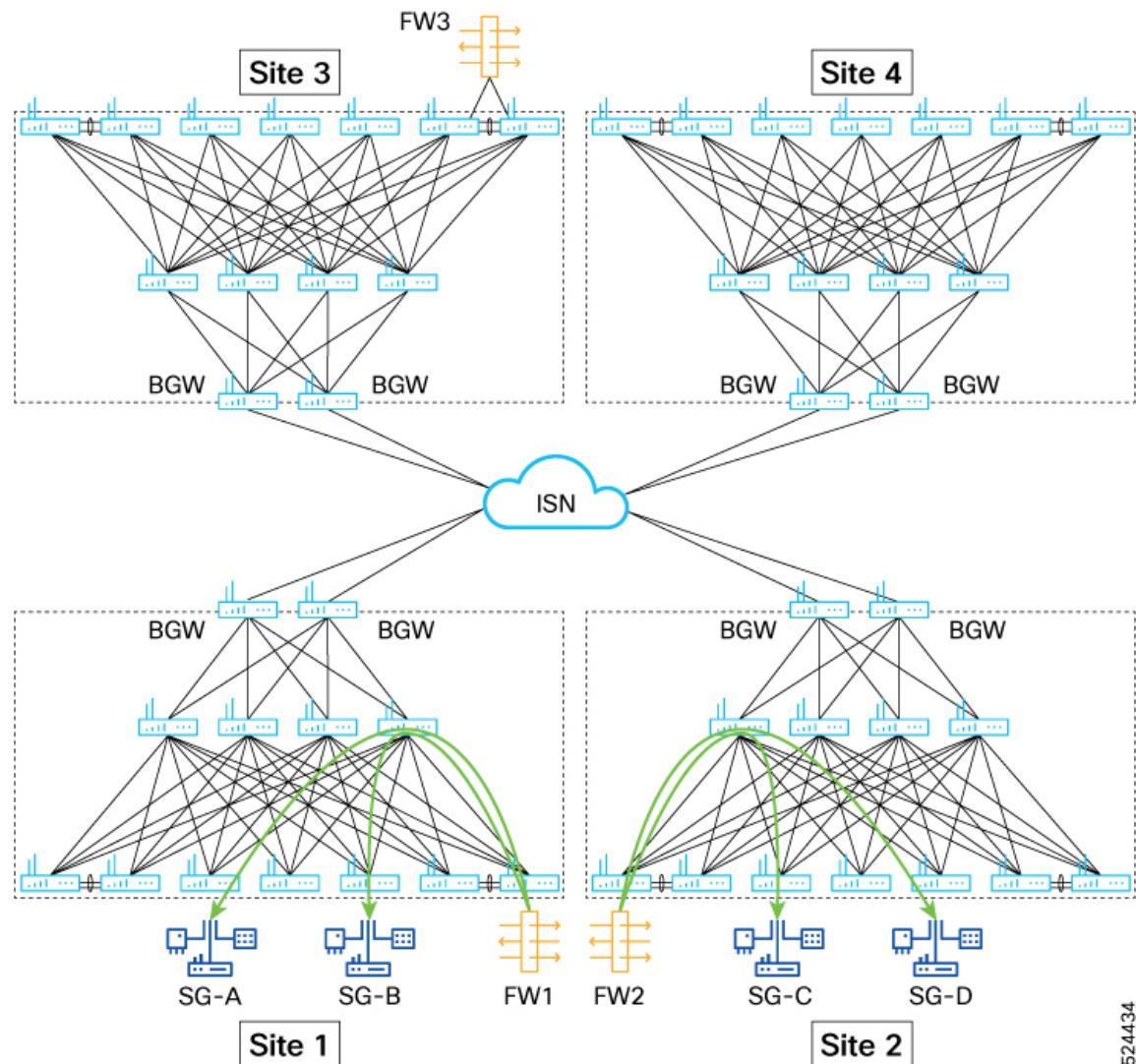


524162

## 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イフィック 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關係なく、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。

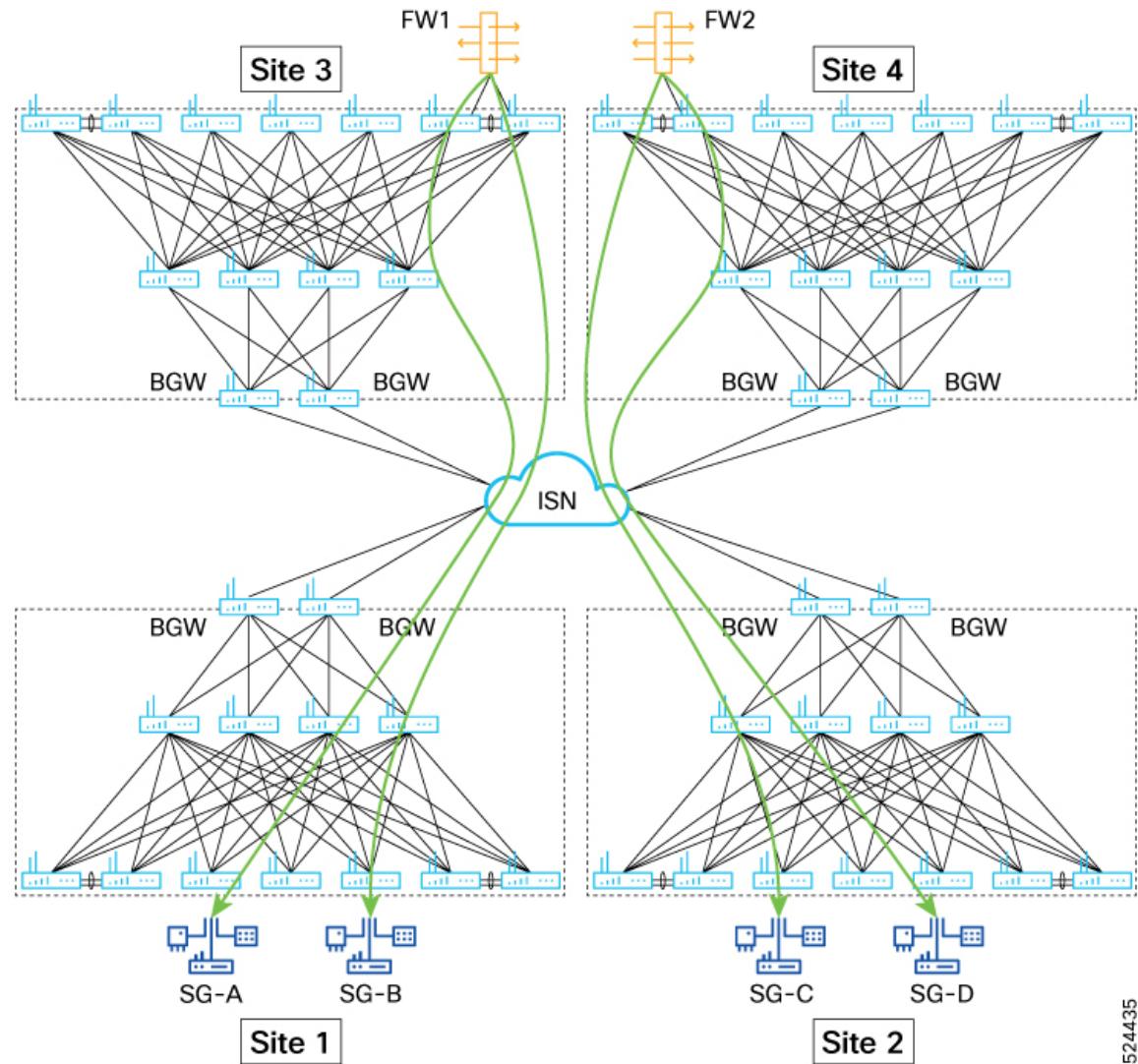
図 5: ローカルサービス チェーンを使用するローカルサイト ローカルサイトセキュリティ グループ



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。

## ePBR および GPO マルチサイト

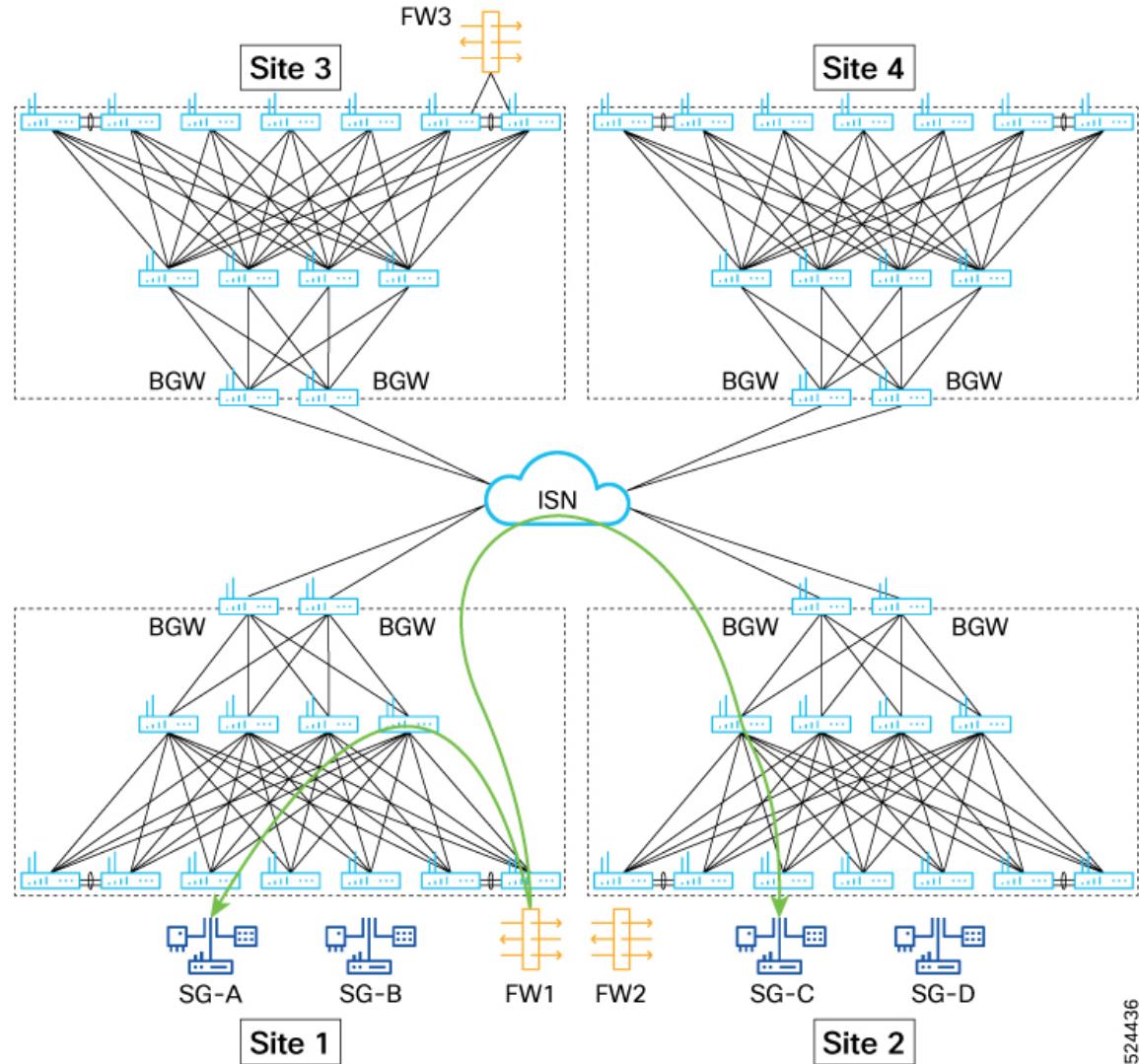
図 6: ローカルサービス チェーンのないローカルサイトセキュリティ グループ



524435

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。

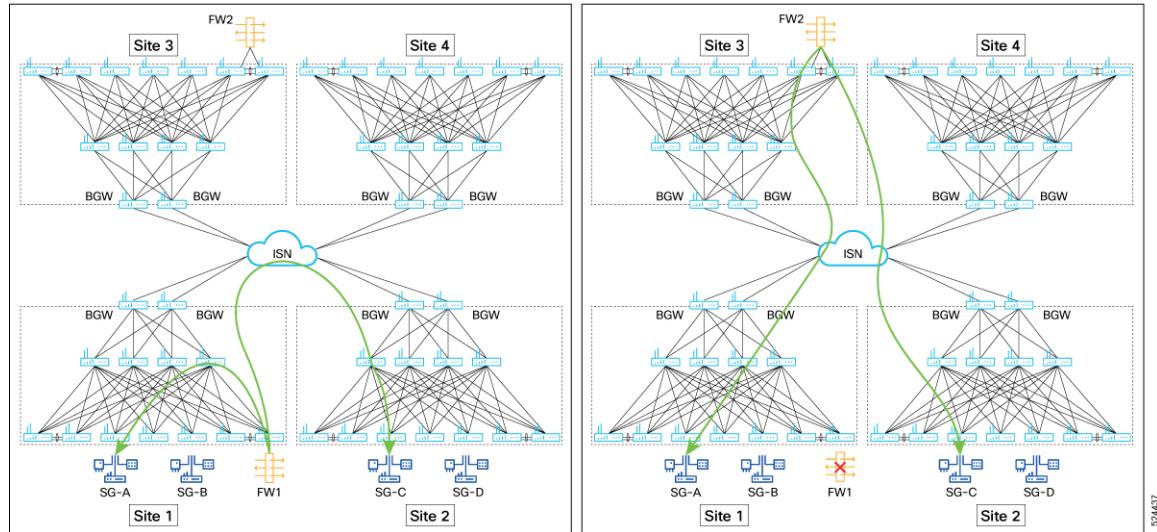
図 7:異なるサイトでの送信元ワークロードと接続先ワークロードのサービスチェーンインスペクション



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。

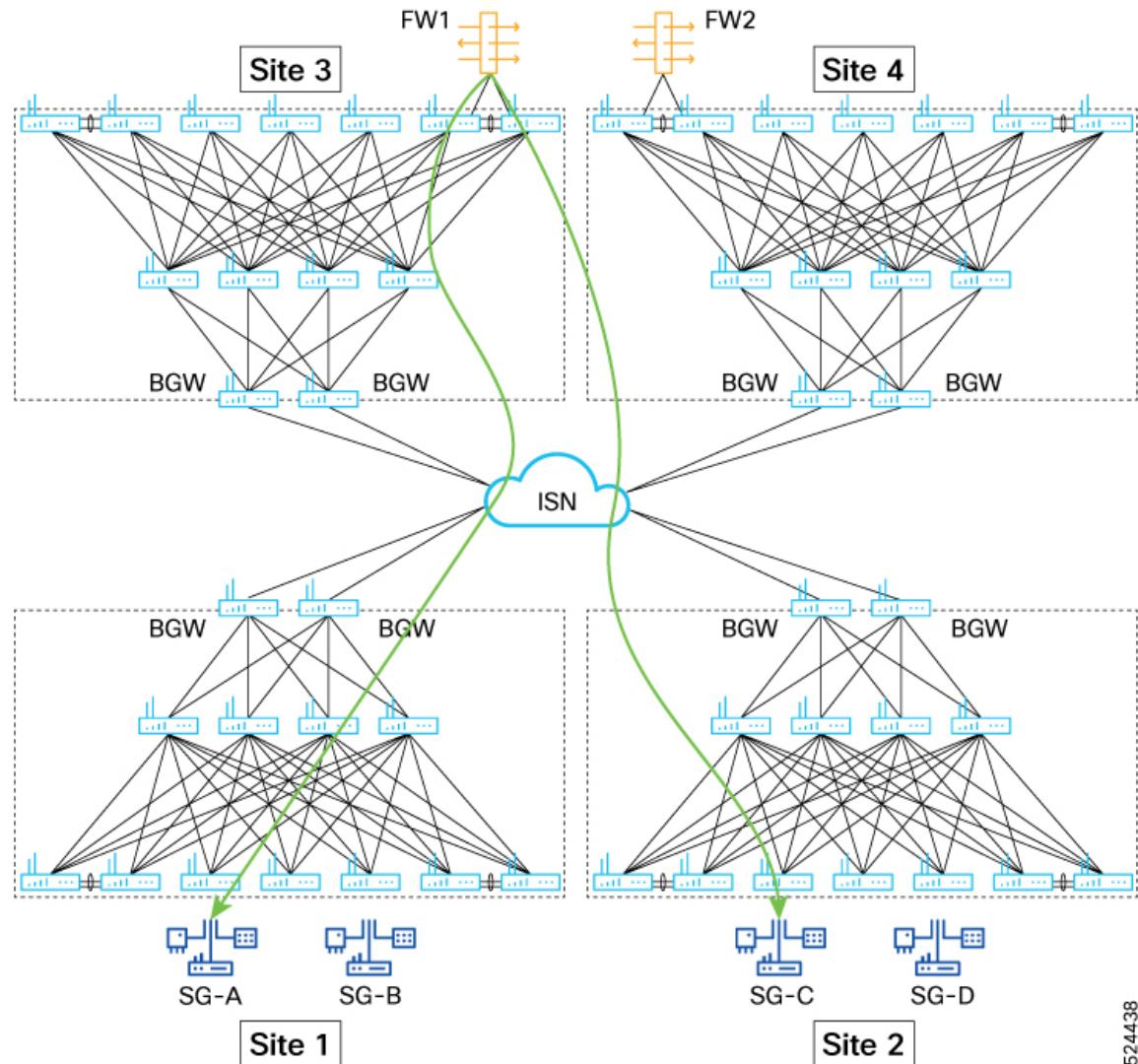
## ePBR および GPO マルチサイト

図 8:2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フロー。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 9: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LOAD。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。

## ■ 注意事項と制約事項

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ます、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ます、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ります、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。

## ■ 注意事項と制約事項

- ・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 トラフィックのスペイク時に、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 トラッカ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 トラッカは、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 トラッカは、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、单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。

## マイクロセグメンテーションの ePBR 構成

- 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 トライ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

- configure terminal**
- epbr service *service-name***
- [no]threshold *threshold-value***
- vrf *vrf-name***
- [no] security-group <fwdGrp> [reverse<revGrp>]**
- [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> ]+}**
- service-endpoint {ip *ipv4-address* | ipv6 *ipv6-address*}**
- probe track *track-ID***
- reverse {ip *ipv4-address* | ipv6 *ipv6-address*}**
- mode hot-standby**
- weight <weight>**
- 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	<b>configure terminal</b> 例： <pre>switch# configure terminal switch(config) #</pre>	コンフィギュレーション モードになります。

	コマンドまたはアクション	目的
ステップ 2	<b>epbr service</b> <i>service-name</i>  例： <pre>switch(config)# epbr service firewall</pre>	新しい ePBR サービス機能を作成します。
ステップ 3	<b>[no]threshold</b> <i>threshold-value</i>  例： <pre>switch(config)# threshold 26</pre>	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	<b>vrf</b> <i>vrf-name</i>  例： <pre>switch(config-epbr-svc)# vrf tenant_A</pre>	ePBR サービス機能の VRF を指定します。
ステップ 5	<b>[no] security-group</b> <fwdGrp> [ <b>reverse</b> <revGrp>]  例： <pre>switch(config-epbr-svc)# security-group 10 reverse 20 switch(config-epbr-svc)# security-group 30</pre>	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 <b>no</b> 形式を使用します。
ステップ 6	<b>[no] probe</b> { <b>icmp</b>   <l4proto> <port-num> } [ <b>control</b> <status> ]   <b>http get</b> [ <url-name> [version <ver> ]   <b>dns host</b> <host-name> <b>ctp</b> ] [ <b>frequency</b> <freq-num>] [ <b>timeout</b> <timeout>] [ <b>retry-down-count</b> <down-count>] [ <b>retry-up-count</b> <up-count>] [ <b>source-interface</b> <src-intf>] [ <b>reverse</b> <rev-src-intf> ]+  例： <pre>switch(config-epbr-svc)# probe icmp control status switch(config-epbr-svc)# probe http get switch(config-epbr-svc)# probe dns host switch(config-epbr-svc)# probe frequency switch(config-epbr-svc)# probe timeout switch(config-epbr-svc)# probe retry-down-count switch(config-epbr-svc)# probe retry-up-count switch(config-epbr-svc)# probe source-interface switch(config-epbr-svc)# probe reverse</pre>	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 <b>no</b> 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	<b>service-endpoint</b> { <b>ip</b> <i>ipv4-address</i>   <b>ipv6</b> <i>ipv6-address</i> }  例： <pre>switch(config-vrf)# service-endpoint ip 172.16.1.200</pre>	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	<b>probe track</b> <i>track-ID</i>  例： <pre>switch(config-epbr-fwd-svc)# probe track 30</pre>	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	<b>reverse</b> { <b>ip</b> <i>ipv4-address</i>   <b>ipv6</b> <i>ipv6-address</i> }  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

## ePBR サービスチェーンの構成

	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	エ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	<b>mode hot-standby</b>  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	<b>weight &lt;weight&gt;</b>  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	<b>exit</b>  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	<b>configure terminal</b>  例： switch# configure terminal switch(config) #	コンフィギュレーション モードになります。
ステップ 2	[no] <b>epbr service-chain &lt;chain-name&gt;</b>  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： <pre>mode multisite failover-group fallback-web-chain3</pre>	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： <pre>switch(config-epbr-svc-chain)# load-balance method src-ip</pre>	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 <b>src-dst-ipprotocol</b> です。
ステップ 5	sequence-number set service service-name[ fail-action { bypass   drop   forward}]  例： <pre>switch(config-epbr-svc-chain)# 10 set service fw2 fail-action drop 20 set service tcp_optim2 fail-action bypass</pre>	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： <pre>switch(config-epbr-svc-chain-seq)# action route reverse-action route</pre>	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 <b>redirect</b> 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>**

## ePBR サービスチェーン構成の確認

### 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	<b>configure terminal</b>  例： <pre>switch# configure terminal switch(config)#</pre>	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	<b>epbr service-chain <i>service-chain-name</i></b>  例： <pre>Switch(config-epbr-svc-chain)# epbr service-chain web</pre>	サービス チェーンを構成します。
ステップ 3	<b>epbr failover-group <i>failover-group-name</i></b>  例： <pre>switch(config-epbr-svc-chain)# epbr failover-group fallback-web-chain1</pre>	フェールオーバー グループを構成します。
ステップ 4	<b>[no] service-chain &lt;name&gt; preference &lt;preference&gt;</b>  例： <pre>switch(config-epbr-fail-group)# service-chain site1-web-chain preference 20</pre>	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

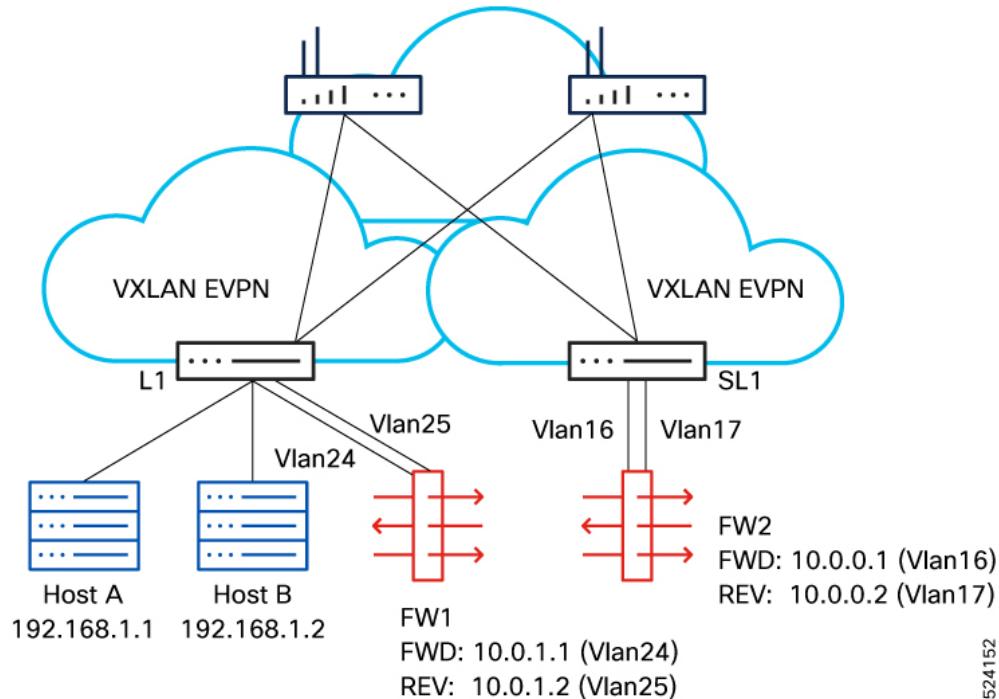
	コマンドまたはアクション	目的
ステップ 1	<b>show epbr service [ &lt;svc-name&gt; ]</b> 例： switch# show epbr service fw	ePBR サービス機能とエンドポイントに関する情報を表示します。
ステップ 2	<b>show epbr service-chain [ &lt;chain-name&gt; ] [ reverse ]</b> 例： switch# show epbr service-chain web	順方向または逆方向の ePBR サービス チェーン ポリシーに関する情報を表示します。
ステップ 3	<b>show tech-support epbr</b> 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	<b>show consistency-checker epbr service-chain { &lt;svcChainName&gt;   all }</b> 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	<b>show running-config epbr</b> 例： switch# show running-config epbr	ePBR の実行構成を表示します。
ステップ 6	<b>show startup-config epbr</b> 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。

## SGACL サービス チェーンの構成例

図 10: 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		

## SGACL サービス チェーンの構成例

Security-group	Reverse security-group	Threshold	
2010	2011		
Endpoint IP/Intf Role Weight	Track SLA	Op-ST	Probe
Reverse IP/Intf	Track SLA	Op-ST	Probe
10.0.1.1/ A 1	1 20001	UP	TCP/5/3/0/0
10.0.1.2/	3 20003	UP	TCP/5/3/0/0
10.0.0.1/ A 1	2 20002	UP	TCP/5/3/0/0
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]
```

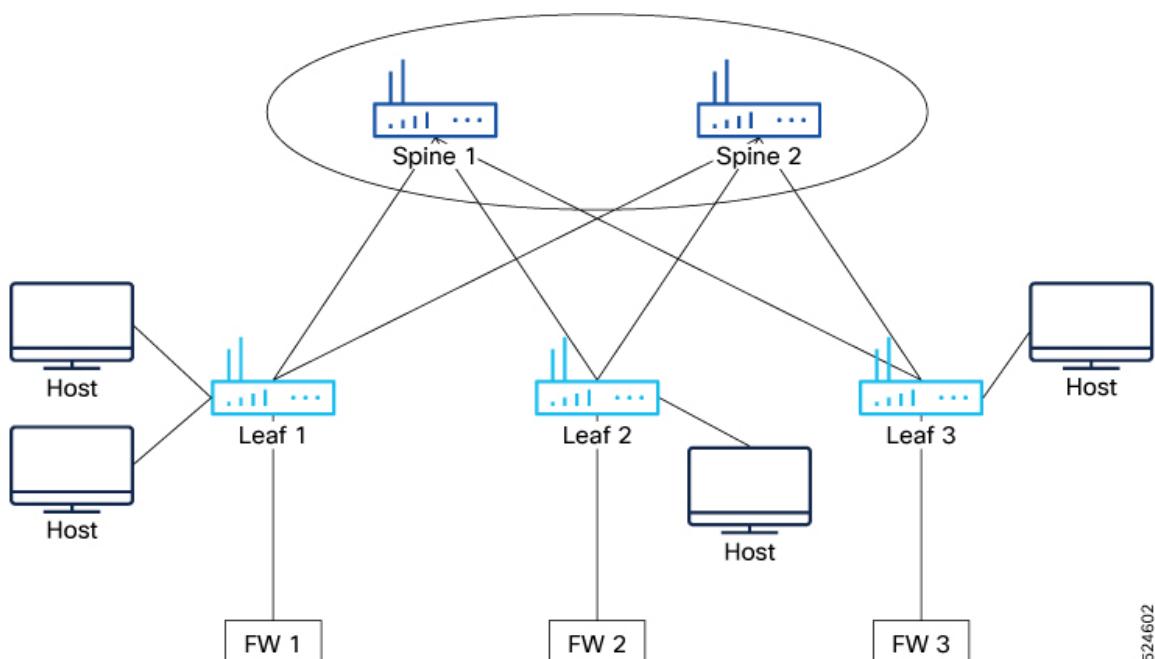
```
IP 10.0.0.2 track 4 [UP]
```

- 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 11: 設定例



524602

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
```

**SGACL サービス チェーンの構成例**

```
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]

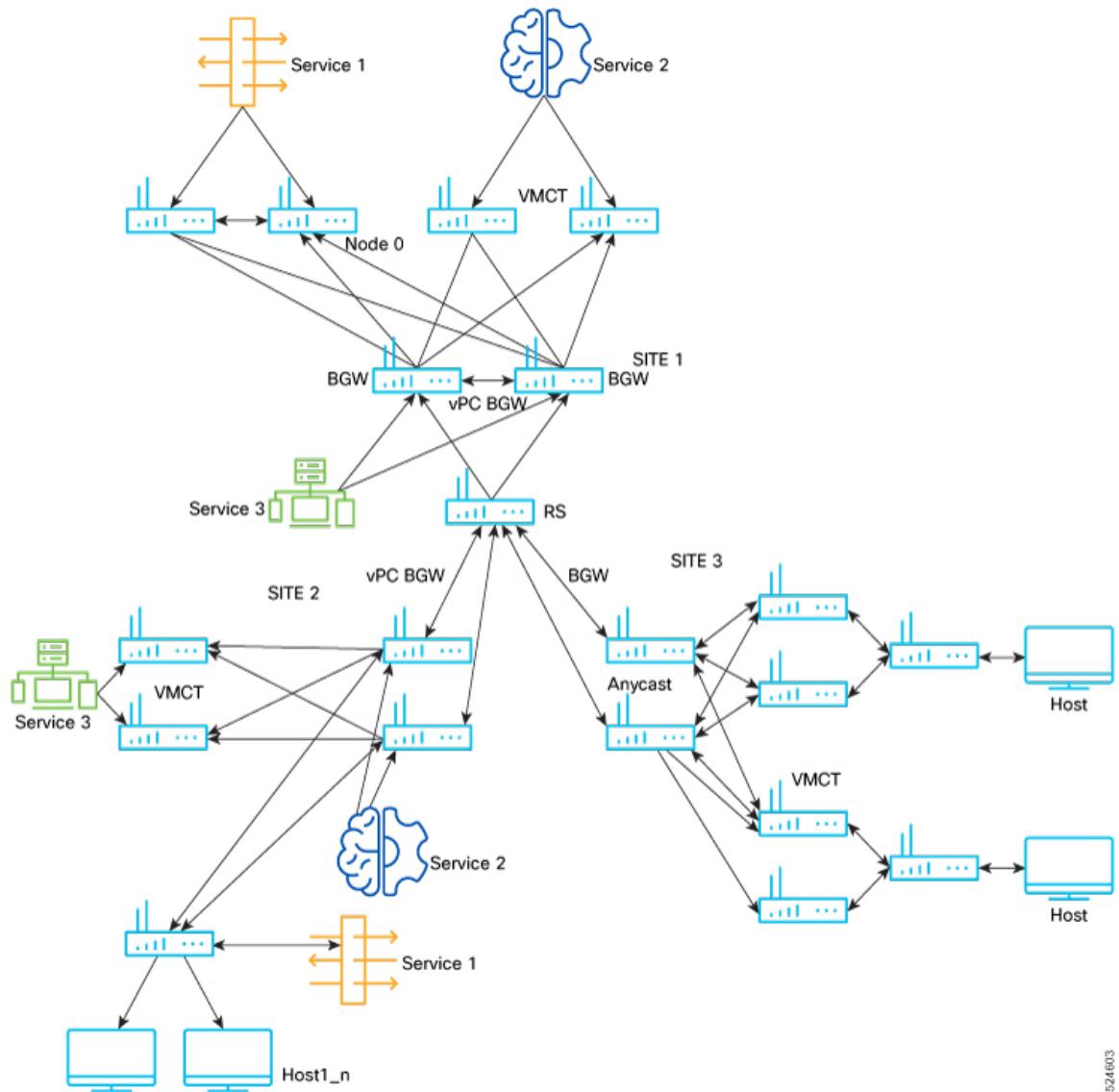
    service:fw2, sequence:20, fail-action:Drop
        load-balance:Source-Destination-ipprotocol, action:Redirect
        state:UP
            IP 50.1.1.2 track 7 [UP]
            IP 54.1.1.2 track 8 [UP]
            IP 58.1.1.2 track 9 [UP]
            IP 59.1.1.2 track 10 [UP] [HOT-STANDBY]
            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]
```

## SGACL サービス チェーンの構成例

## GPO を使用したマルチサイト ePBR の構成例

図 12: 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 sitel-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
```

## SGACL サービス チェーンの構成例

```
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. フエールオーバー 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]

```

**SGACL サービス チェーンの構成例**

```
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。