



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 \(1 ページ\)](#)
- [ePBR L3 の注意事項および制約事項 \(4 ページ\)](#)
- [ePBR L3 の構成 \(6 ページ\)](#)
- [ePBR L3 の構成例 \(13 ページ\)](#)
- [その他の参考資料 \(21 ページ\)](#)

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 ライセンス方式の推奨の詳細と、ライセンスの取得および適用の方法については、『[Cisco NX-OS ライセンス ガイド](#)』および『[Cisco NX-OS ライセンス 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

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。

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。

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、ヘルスマonitoring、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。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。

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。

- 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。
- 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。
- 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 トラフィ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。
- 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。
- VXLAN 上の ePBRv4 およびスタンドアロン ePBR は、Cisco Nexus 9500 シリーズ スイッチでサポートされています。
- 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。
- 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。

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。

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。

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. **vrf** *vrf-name*
4. **service-endpoint** {**ip** *ipv4 address* | **ipv6** *ipv6 address*} [**interface** *interface-name interface-number*]
5. **probe track** *track ID*

6. **reverse ip** *ip address interface interface-name interface-number*
7. **exit**
8. **epbr policy** *policy-name*
9. **match** { [**ip address** *ipv4 acl-name*] | [**ipv6 address** *ipv6 acl-name*] } [**redirect** | **drop** | **exclude**]
10. [**no**] **load-balance** [**method** { **src-ip** | **dst-ip** }] [**buckets** *sequence-number*]
11. *sequence-number* **set service** *service-name* [**fail-action** { **bypass** | **drop** | **forward** }]
12. **interface** *interface-name interface-number*
13. **epbr** { **ip** | **ipv6** } **policy** *policy-name* [**reverse**]
14. **exit**

手順の詳細

	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 <i>service-name</i> 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	vrf <i>vrf-name</i> 例： switch(config)# vrf tenant_A	ePBR サービスの VRF を指定します。
ステップ 4	service-endpoint { ip <i>ipv4 address</i> ipv6 <i>ipv6 address</i> } [interface <i>interface-name interface-number</i>] 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 5	probe track <i>track ID</i> 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 6	reverse ip <i>ip address interface interface-name interface-number</i> 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。

	コマンドまたはアクション	目的
ステップ 7	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 8	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 9	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 10	[no] load-balance [method { src-ip dst-ip }] [buckets sequence-number] 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。
ステップ 11	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 12	interface interface-name interface-number 例： switch(config)# interface vlan 2010	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。
ステップ 13	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。 <ul style="list-style-type: none"> • 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

	コマンドまたはアクション	目的
ステップ 14	exit 例 : <pre>switch(config-if)# end</pre>	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

	コマンドまたはアクション	目的
ステップ 1	epbr session 例 : <pre>switch(config)# epbr session</pre>	ePBR セッション モードに入ります。
ステップ 2	epbr service service-name 例 : <pre>switch(config-epbr-sess)# epbr service TCP_OPTIMIZER</pre>	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 {ip ipv4 address ipv6 ipv6 address} [interface interface-name interface-number] 例 : <pre>switch(config-epbr-sess-svc)# no service-end-point ip 172.16.20.200 interface VLAN200</pre>	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 : <pre>switch(config-epbr-sess-svc)#service-end-point ip 172.16.25.200 interface VLAN200</pre>	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。

	コマンドまたはアクション	目的
ステップ 5	reverse ip <i>ip address interface interface-name interface-number</i> 例 : <pre>switch(config-epbr-sess-svc-ep)# reverse ip 172.16.30.200 interface VLAN201</pre>	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 : <pre>switch(config-epbr-sess)# commit</pre>	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 : <pre>switch(config-epbr-sess)# abort</pre>	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*]
7. **commit**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	epbr session 例 : <pre>switch(config)# epbr session</pre>	ePBR セッ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 policy <i>policy-name</i> 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 <i>ipv4 acl-name</i>] [ipv6 address <i>ipv6 acl-name</i>] [l2 address <i>ipv6 acl-name</i>]} 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 <i>ipv4 acl-name</i>] [ipv6 address <i>ipv6 acl-name</i>] [l2 address <i>ipv6 acl-name</i>]} 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 <i>service-name</i> [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 <i>sequence-number</i>] 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、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。
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

	コマンドまたはアクション	目的
ステップ 1	epbr session access-list <i>acl-name</i> 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 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

	コマンドまたはアクション	目的
ステップ 1	show epbr policy <i>policy-name</i> [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 <i>policy-name</i> [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。

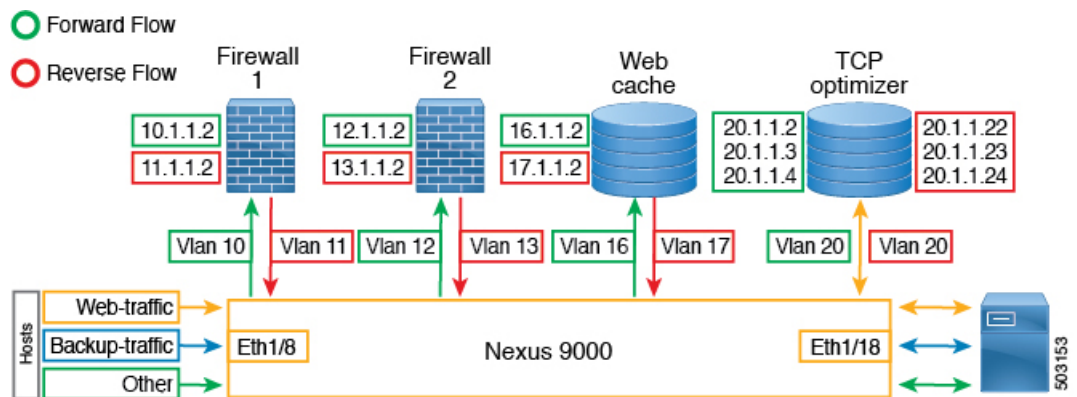
	コマンドまたはアクション	目的
ステップ 4	show running-config epbr 例： switch# show running-config epbr	ePBR の実行構成を表示します。
ステップ 5	show startup-config epbr 例： switch# show startup-config epbr	ePBR のスタートアップ構成を表示します。

ePBR 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

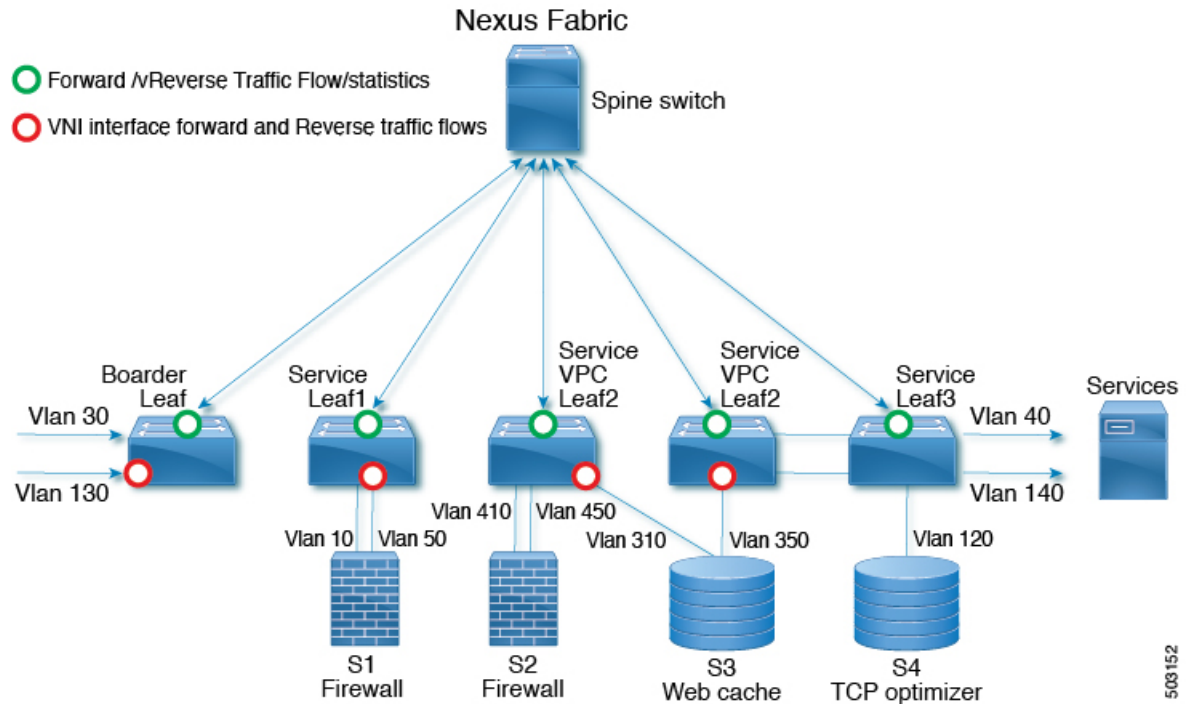
switch# show ePBR policy tenant_1 reverse

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 vrfl
  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 vrfl
  service-end-point ip 41.1.1.2 interface Vlan410
  probe icmp source-interface loopback9
  reverse ip 45.1.1.2 interface Vlan450

  probe icmp source-interface loopback10

epbr service s3
  vrf vrfl
  service-end-point ip 31.1.1.2 interface Vlan310
  probe http get index.html source-interface loopback9
  reverse ip 35.1.1.2 interface Vlan350

  probe http get index.html source-interface loopback10

```

```

epbr service s4
  service-interface Vlan120
  vrf vrf1
  probe udp 6900 control enable source-interface loopback9
  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
interface Vlan100 - Vxlan L3vni interface to which the policy is applied on all service
leafs
  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 Vlan30 - 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 130 - 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 eubr 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。

```

epubr 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)#epubr session
switch(config-epubr-sess)#epubr 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
```

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	<i>Cisco Nexus 9000 シリーズ NX-OS IP SLA 構成ガイド 9.3(x)</i>
ePBR ライセンス	『 <i>Cisco NX-OS Licensing Guide</i> 』
ePBR スケール値	『 <i>Cisco Nexus 9000 Series NX-OS Verified Scalability</i> 』

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されていません。

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。