



Cisco Nexus 9000 シリーズ NX-OS ePBR 構成ガイド、リリース 10.2(x)

初版：2021 年 12 月 16 日

最終更新：2022 年 4 月 26 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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: <http://www.cisco.com/go/softwareterms>. Cisco product warranty information is available at <http://www.cisco.com/go/warranty>. US Federal Communications Commission Notices are found here <http://www.cisco.com/c/en/us/products/us-fcc-notice.html>.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and-if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021–2022 Cisco Systems, Inc. All rights reserved.



目次

Trademarks ?

はじめに :

はじめに **vii**

対象読者 **vii**

表記法 **vii**

Cisco Nexus 9000 シリーズ スイッチの関連資料 **viii**

マニュアルに関するフィードバック **viii**

通信、サービス、およびその他の情報 **ix**

第 1 章

新機能と更新情報 **1**

新規および変更情報 **1**

第 2 章

拡張済みポリシーベース リダイレクトのプラットフォーム サポート **3**

拡張済みポリシーベース リダイレクトのプラットフォーム サポート **3**

第 3 章

ePBR L3 の構成 **7**

ePBR L3 に関する情報 **7**

ライセンス要件 **7**

ePBR サービスとポリシーの構成 **7**

ePBR のインターフェイスへの適用 **8**

バケットの作成およびロード バランシング **8**

ePBR オブジェクト トラッキング、ヘルスマonitoring、および Fail-Action **9**

ePBR セッションベースの構成 **10**

ePBR マルチサイト **10**

ACL リフレッシュ	11
ePBR L3 の注意事項および制約事項	11
ePBR L3 の構成	14
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	14
ePBR セッションを使用したサービスの変更	16
ePBR セッションを使用したポリシーの変更	17
ePBR ポリシーによる使用される Access-list の更新	19
ePBR Show コマンド	19
ePBR 構成の確認	20
ePBR L3 の構成例	21
その他の参考資料	29
関連資料	29
標準	30

第 4 章

ePBR L2 の構成	31
ePBR L2 に関する情報	31
ePBR サービスとポリシーの構成	31
ePBR の L2 インターフェイスへの適用	32
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	32
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	32
バケットの作成およびロードバランシング	32
ePBR オブジェクトトラッキング、ヘルスマonitoring、および Fail-Action	33
ePBR セッションベースの構成	33
ACL リフレッシュ	34
ePBR L2 の注意事項および制約事項	34
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	37
ePBR セッションを使用したサービスの変更	39
ePBR セッションを使用したポリシーの変更	40
ePBR ポリシーによる使用される Access-list の更新	42
ePBR Show コマンド	42
ePBR 構成の確認	43

ePBR の構成例 44



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](#) (vii ページ)
- [表記法](#) (vii ページ)
- [Cisco Nexus 9000 シリーズ スイッチの関連資料](#) (viii ページ)
- [マニュアルに関するフィードバック](#) (viii ページ)
- [通信、サービス、およびその他の情報](#) (ix ページ)

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。
<i>italic</i>	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。

http://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 Marketplace](#) 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

[Cisco Bug Search Tool](#) (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 Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。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。



第 1 章

新機能と更新情報

- [新規および変更情報 \(1 ページ\)](#)

新規および変更情報

表 1: NX-OS リリース 10.2(x) の新機能および変更された機能

機能	説明	変更が行われたリリース	参照先
ESR: ePBR L2	L2 サービス タイプの拡張ポリシーベースルーティング (ePBR) サポートが追加され、スタンドアロンおよびファブリックポロジ全体でトラフィックのリダイレクトとサービスチェーンが提供されます。	10.2(3)F	ePBR L2 の構成 (31 ページ)
ESR: ePBR L3	L3 サービス タイプの拡張ポリシーベースルーティング (ePBR) サポートが追加され、スタンドアロンおよびファブリックポロジ全体でトラフィックのリダイレクトとサービスチェーンが提供されます。	10.2(3)F	ePBR L3 の構成 (7 ページ)
アクセス ポートでの ePBR L2 のサポート	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に追加されるサポート	10.2(3)F	

機能	説明	変更が行われたリリース	参照先
複数のバックアップホップ	VRF間のサービスチェーンに追加されるガイドラインと制限事項	10.2(2)F	ePBR L3の注意事項および制約事項 (11 ページ)
CTPプローブ	EPBR レイヤ 2 サービスに追加されるガイドラインと制限事項	10.2(2)F	ePBR L3の注意事項および制約事項 (11 ページ)
ePBR マルチサイト	VXLAN マルチサイトファブリックでのサービスチェーン	10.2 (1) F	ePBR マルチサイト (10 ページ)
VRF 間のサービスチェーン	VRF間のサービスチェーンに追加されるガイドラインと制限事項	10.2 (1) F	ePBR L3の注意事項および制約事項 (11 ページ)
ePBR サービスとポリシーの構成	ePBR サービスとポリシー	10.2 (1) F	ePBR サービスとポリシーの構成 (7 ページ)



第 2 章

拡張済みポリシーベース リダイレクトのプラットフォーム サポート

この章では、Cisco Nexus プラットフォームスイート全体でサポートされていない機能のプラットフォーム サポートについて定義します。

- [拡張済みポリシーベース リダイレクトのプラットフォーム サポート \(3 ページ\)](#)

拡張済みポリシーベース リダイレクトのプラットフォーム サポート

次の表で、Cisco プラットフォームスイート全体でサポートされていない機能のプラットフォーム サポートについて定義します。初期製品のリリースでサポートされるプラットフォームについて詳細について、各リリースのインストールガイドおよびリリース ノートを参照する必要があります。

機能	サポートされるプラットフォームまたはラインカード	サポートされるようになった最初のリリース	プラットフォームの例外
ePBR 除外 ACL	N9K-C9336C-FX2-E、 N9K-C93108TC-EX、 N9K-C93108TC-FX、 N9K-C93180YC-EX、 N9K-C93180YC-FX、 N9K-C93216TC-FX2、 N9K-C93240YC-FX2、 N9K-C93360YC-FX2、 N9K-C9336C-FX2、 N9K-C9316D-GX、 N9K-C93600CD-GX、 N9K-C9364C-GX、	Cisco NX-OS リリース 10.1(1)	

機能	サポートされるプラットフォームまたはライセンスカード	サポートされるようになった最初のリリース	プラットフォームの例外
	N9K-C93180YC-FX3S および N9K-C93360YC-FX3。 N9K-C9504、 N9K-C9508、および N9K-C9516 と次のライセンスカード： N9K-X97160YC-EX、 N9K-X9732C-EX、 N9K-X9732C-FX、 N9K-X9736C-EX、 N9K-X9736C-FX、 N9K-X9736Q-FX およ び N9K-X9788TC-FX。		
IPv4 の ePBR、IPv6、および VXLAN を介した ePBR	N9K-C9316D-GX、 N9K-C93600CD-GX、 N9K-C9364C-GX、 N9K-C93180YC-FX3S および N9K-C93360YC-FX3。	Cisco NX-OS リリース 10.1(1)	
VXLAN を介した IPv4、IPv6、および ePBR を使用した ePBR	N9K-C93180YC-FX3S、 N9K-C93360YC-FX3、 N9K-C9336C-FX2-E、 N9K-C93108TC-EX、 N9K-C93108TC-FX、 N9K-C93180YC-EX、 N9K-C93180YC-FX、 N9K-C93216TC-FX2、 N9K-C93240YC-FX2、 N9K-C93360YC-FX2 お よび N9K-C9336C-FX2。 N9K-C9504、 N9K-C9508、および N9K-C9516 と次のライセンスカード： N9K-X97160YC-EX、 N9K-X9732C-EX、 N9K-X9732C-FX、	Cisco NX-OS リリース 9.3(5)	

機能	サポートされるプラットフォームまたはライセンスカード	サポートされるようになった最初のリリース	プラットフォームの例外
	N9K-X9736C-EX、 N9K-X9736C-FX、 N9K-X9736Q-FX および N9K-X9788TC-FX。		
ePBR L2	N9K-C9336C-FX2-E、 N9K-C93108TC-EX、 N9K-C93108TC-FX、 N9K-C93180YC-EX、 N9K-C93180YC-FX、 N9K-C93216TC-FX2、 N9K-C93240YC-FX2、 N9K-C93360YC-FX2、 N9K-C9336C-FX2、 N9K-C9316D-GX、 N9K-C93600CD-GX、 N9K-C9364C-GX、 N9K-C93180YC-FX3S および N9K-C93360YC-FX3。	Cisco NX-OS リリース 10.2(3)F	



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 \(7 ページ\)](#)
- [ePBR L3 の注意事項および制約事項 \(11 ページ\)](#)
- [ePBR L3 の構成 \(14 ページ\)](#)
- [ePBR L3 の構成例 \(21 ページ\)](#)
- [その他の参考資料 \(29 ページ\)](#)

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、スタンドアロン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 Licensing Guide](#)』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、トラフィックがスタンドアロンまたは 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ポリシーアプリケーションをサポートします。

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。ロードバランシング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。

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ます、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。

- 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ます。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_」という名前が始まる、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。

- 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 ISSU 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。

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。

- 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。

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。

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的 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的 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。

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 : <pre>switch# configure terminal switch(config)#</pre>	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 <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。
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 <i>policy-name</i> 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 <i>ipv4 acl-name</i>] [ipv6 address <i>ipv6 acl-name</i>] } [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。

	コマンドまたはアクション	目的
ステップ 10	<code>[no] load-balance [method { src-ip dst-ip }] [buckets sequence-number</code> 例： <code>switch(config)# load-balance method src-ip</code>	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	<code>sequence-number set service service-name [fail-action { bypass drop forward }</code> 例： <code>switch(config)# set service firewall fail-action drop</code>	fail-action メカニズムを計算します。
ステップ 12	<code>interface interface-name interface-number</code> 例： <code>switch(config)# interface vlan 2010</code>	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	<code>epbr { ip ipv6 } policy policy-name [reverse]</code> 例： <code>switch(config-if)# epbr ip policy Tenant_A-Redirect</code>	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
ステップ 14	<code>exit</code> 例： <code>switch(config-if)# end</code>	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`

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： 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。
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。

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 policy policy-name**
2. **[no] match { [ip address ipv4 acl-name] | [ipv6 address ipv6 acl-name] [12 address ipv6 acl-name] } vlan {vlan | vlan range | all} [redirect | drop | exclude] }**
3. **match { [ip address ipv4 acl-name] | [ipv6 address ipv6 acl-name] [12 address ipv6 acl-name] } vlan {vlan | vlan range | all} [redirect | drop | exclude] }**

4. `sequence-number set service service-name [fail-action { bypass | drop | forward }] [load-balance [method { src-ip | dst-ip }] [buckets sequence-number]`
5. `load-balance set service service-name [fail-action { bypass | drop | forward }] [load-balance [method { src-ip | dst-ip }] [buckets sequence-number]`
6. `commit`
7. `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	<code>epbr policy policy-name</code> 例： <pre>switch(config-epbr-sess)# epbr policy Tenant_A-Redirect</pre>	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 2	<code>[no] match { [ip address ipv4 acl-name] [ipv6 address ipv6 acl-name] [I2 address ipv6 acl-name] } vlan {vlan vlan range all} [redirect drop exclude] }</code> 例： <pre>switch(config-epbr-sess-pol)# no match ip address WEB</pre>	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 3	<code>match { [ip address ipv4 acl-name] [ipv6 address ipv6 acl-name] [I2 address ipv6 acl-name] } vlan {vlan vlan range all} [redirect drop exclude] }</code> 例： <pre>switch(config-epbr-sess-pol)# match ip address HR</pre>	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 4	<code>sequence-number set service service-name [fail-action { bypass drop forward }] [load-balance [method { src-ip dst-ip }] [buckets sequence-number]</code> 例： <pre>switch(config-epbr-sess-pol-match)# 10 set service Web-FW</pre>	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 5	<code>load-balance set service service-name [fail-action { bypass drop forward }] [load-balance [method { src-ip dst-ip }] [buckets sequence-number]</code> 例： <pre>switch(config-epbr-sess-pol-match)# 10 set service Web-FW</pre>	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れを省略すると、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 6	<code>commit</code> 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。

	コマンドまたはアクション	目的
ステップ 7	end 例 : <code>switch(config-epbr-sess)#end</code>	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 : <code>switch(config)# epbr session access-list WEB refresh</code>	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 : <code>switch(config)# end</code>	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 :	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
	switch# show eubr policy Tenant_A-Redirect	
ステップ 2	show eubr statistics policy-name [reverse] 例： switch# show eubr statistics policy pol2	ePBR ポリシー統計を表示します。
ステップ 3	show tech-support eubr 例： switch# show tech-support eubr	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 eubr 例： switch# show running-config eubr	ePBR の実行構成を表示します。
ステップ 5	show startup-config eubr 例： switch# show startup-config eubr	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 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。

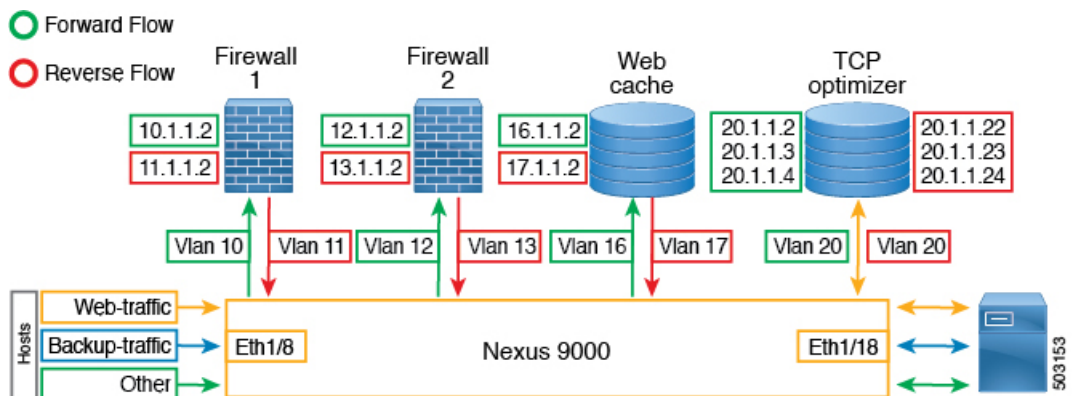
コマンド	目的
<code>show track dynamic</code>	プローブが有効になっている場合に、チェーン内のサービスエンドポイントに対して ePBR によって生成されたトラックを表示します。

ePBR L3 の構成例

例：ePBR のスタンドアロン構成

次のトポロジは、ePBR スタンドアロン構成を示しています。

図 1: ePBR のスタンドアロン構成



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

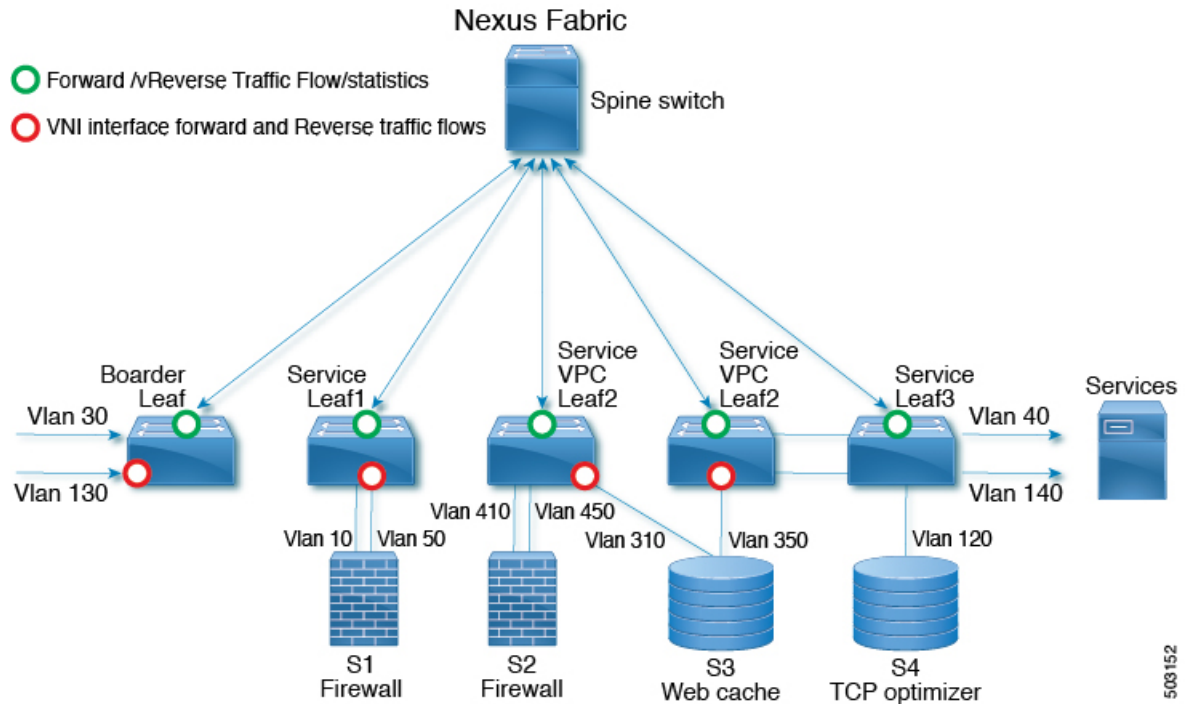
switch# show ePBR policy tenant_1 reverse

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、リリース 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 Guide</i> 』

標準

標準	タイトル
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は変更されていません。	



第 4 章

ePBR L2 の構成

- ePBR L2 に関する情報 (31 ページ)
- ePBR L2 の注意事項および制約事項 (34 ページ)
- 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 (37 ページ)
- ePBR セッションを使用したサービスの変更 (39 ページ)
- ePBR セッションを使用したポリシーの変更 (40 ページ)
- ePBR ポリシーによる使用される Access-list の更新 (42 ページ)
- ePBR Show コマンド (42 ページ)
- ePBR 構成の確認 (43 ページ)
- ePBR の構成例 (44 ページ)

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、トラフィックがスタンドアロン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。スタンドアロン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

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

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。

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ンネルに構成された 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ンネルに再構成します。
- 「epbr_」という名前で作成される、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 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。
- 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 ポリシーは、順方向の単一のインターフェイスと逆方向の単一のインターフェイスにのみ適用できます。異なるインターフェイスペアで同様にサービスチェーンを作成するには、ポリシーを複製する必要があります。
- 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。
- 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。
- パ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。
- ネイバー探索パケットを含む「すべての」IPv6 トラフィックをサービスチェーン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 エースを、ユーザ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。
- 「すべての」レイヤ 2 トラフィックをサービスチェーンまたはリダイレクトするために、ARP (0x806)、VN-Tag (0x8926)、FCOE (0x8906)、MPLS ユニキャスト (0x8847)、MPLS マルチキャスト (0x8848) のプロトコルに一致する一意の ACES 必要に応じて、ユーザ定義の一致アクセス リストに明示的に追加する必要があります。
- レイヤ 2 ePBR は、レイヤ 2 制御パケットのサービスチェーンまたはリダイレクトをサポートしていません。
- 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。

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。

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。

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]**
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

	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。

	コマンドまたはアクション	目的
ステップ 5	<p>probe {<i>ctp</i>} [<i>frequency seconds</i>] [<i>timeout seconds</i>] [<i>retry-down-count count</i>] retry-up-count <i>count</i>]</p> <p>例 :</p> <pre>switch(config)# probe icmp</pre>	<p>ePBR サービスのプローブを構成します。</p> <p>オプションは次のとおりです。</p> <ul style="list-style-type: none"> • 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	<p>service-endpoint [<i>interface interface-name interface-number</i>]</p> <p>例 :</p> <pre>switch(config-epbr-svc)# service-end-point interface Ethernet1/3</pre>	<p>ePBR サービスのサービスエンドポイントを構成します。</p> <p>手順 2 ~ 5 を繰り返して、別の ePBR サービスを構成できます。</p>
ステップ 7	<p>reverse interface <i>interface-name interface-number</i></p> <p>例 :</p> <pre>switch(config-epbr-fwd-svc)# reverse interface Ethernet1/4</pre>	<p>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。</p>
ステップ 8	<p>exit</p> <p>例 :</p> <pre>switch(config-epbr-reverse-svc)# exit switch(config-epbr-fwd-svc)# exit switch(config-epbr-svc)# exit switch(config)#</pre>	<p>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。</p>
ステップ 9	<p>epbr policy <i>policy-name</i></p> <p>例 :</p> <pre>switch(config)# epbr policy Tenant_A-Redirect</pre>	<p>ePBR ポリシーを構成します。</p>
ステップ 10	<p>match { [<i>ip address ipv4 acl-name</i>] [<i>ipv6 address ipv6 acl-name</i>] [<i>l2 address l2 acl-name</i>]} {drop exclude redirect vlan{<i>vlan</i> <i>vlan range</i> all}}</p> <p>例 :</p> <pre>switch (config) # match ip address WEB vlan 10</pre>	<p>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</p>

	コマンドまたはアクション	目的
		<p>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。</p> <p>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。</p>
ステップ 11	<p>[no] load-balance [method { src-ip dst-ip }] [buckets count]</p> <p>例 :</p> <pre>switch(config)# load-balance method src-ip</pre>	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 12	<p>sequence-number set service service-name [fail-action { bypass drop forward }]</p> <p>例 :</p> <pre>switch(config)# set service firewall fail-action drop</pre>	fail-action メカニズムを構成します。
ステップ 13	<p>interface interface-name interface-number</p> <p>例 :</p> <pre>switch(config)# interface Ethernet1/1</pre>	インターフェイス構成モードを開始します。
ステップ 14	<p>epbr {l2} policy policy-name egress-interface interface-name [reverse]</p> <p>例 :</p> <pre>epbr l2 policy Tenant_A_Redirect egress-interface Ethernet1/2</pre>	<p>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。</p> <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 • 順方向の l2 ポリシー • 逆方向の l2 ポリシー
ステップ 15	<p>exit</p> <p>例 :</p> <pre>switch(config-if)# end</pre>	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**

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： <code>switch(config)# epbr session</code>	ePBR セッション モードに入ります。
ステップ 2	epbr service <i>service-name type l2</i> 例： <code>switch(config-epbr-sess)# epbr service TCP_OPTIMIZER</code>	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 <i>interface-name</i>] 例： <code>switch(config-epbr-sess-svc)# no service-end-point interface ethernet 1/3</code>	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 <i>interface-name</i>] 例： <code>switch(config-epbr-sess-svc)# service-end-point interface ethernet 1/15</code>	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 <i>interface-name</i>] 例： <code>switch(config-epbr-sess-fwd-svc)# reverse interface ethernet 1/4</code>	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： <code>switch(config-epbr-sess)#commit</code>	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。

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**}] [**load-balance** [**method** { **src-ip** | **dst-ip**}] [**buckets** *sequence-number*]
6. **load-balance set service** *service-name* [**fail-action** { **bypass** | **drop** | **forward**}] [**load-balance** [**method** { **src-ip** | **dst-ip**}] [**buckets** *no-of-buckets*]
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	
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>mac acl-name</i>]} 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 <i>ipv4 acl-name</i>] [ipv6 address <i>ipv6 acl-name</i>] l2 address <i>mac acl-name</i>]} 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 <i>service-name</i> [fail-action { bypass drop forward }] [load-balance [method { src-ip dst-ip }] [buckets <i>sequence-number</i>] 例： switch(config-epbr-sess-pol-match)# 10 set service Web-FW	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	load-balance set service <i>service-name</i> [fail-action { bypass drop forward }] [load-balance [method { src-ip dst-ip }] [buckets <i>no-of-buckets</i>]	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。

	コマンドまたはアクション	目的
	例： switch(config-epbr-sess-pol-match)# 10 set service Web-FW	(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。
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	パ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。

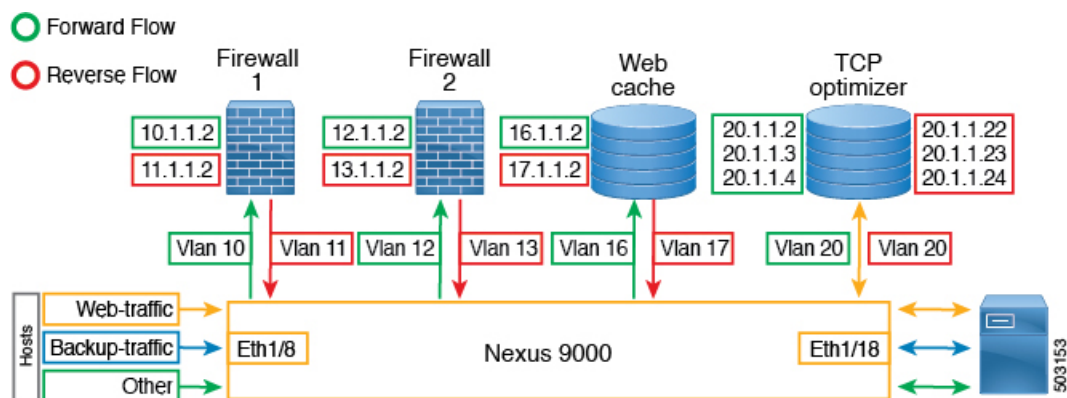
コマンド	目的
show track dynamic	プローブが有効になっている場合に、チェーン内のサービスエンドポイントに対して ePBR によって生成されたトラックを表示します。
show ip access-list summary	バケットアクセスリストのトラフィック一致基準のサマリを表示します。
show [ip ipv6 mac] access-lists dynamic	一致基準のダイナミック エントリを表示します。

ePBR の構成例

例：ePBR のスタンドアロン構成

次のトポロジは、ePBR スタンドアロン構成を示しています。

図 3: ePBR のスタンドアロン構成



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
```


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。