ePBR L2 の構成

ePBR L2 に関する情報

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

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

ePBR サービスとポリシーの構成

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

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

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

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

ePBR の L2 インターフェイスへの適用

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

アクセス ポートとしてのプロダクション インターフェイスの有効化

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

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

トランク ポートとしてのプロダクション インターフェイスの有効化

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

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

バケットの作成およびロード バランシング

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

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

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

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

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

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

- バイパス
- ドロップオンフェイル
- 転送

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

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

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

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

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

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

fail-action の最適化は、Cisco Nexus 9300-EX/FX/FX2/FX3/GX/GX2、C9364C、C9332C、および 9700-EX/FX/GX ライン カードを搭載した Cisco Nexus 9500 スイッチでサポートされます。

ePBR セッションベースの構成

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

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

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

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

ACL リフレッシュ

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

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

ePBR L2 の注意事項および制約事項

ePBR には、次の注意事項と制限事項 があります。

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

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

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

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

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

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

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

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

- Cisco NX-OS リリース 10.4(1)F 以降、ePBR L2 は、ePBR ポリシーに一致するすべての制御トラフィックのリダイレクションをサポートします。詳細については、「制御トラフィックのリダイレクションとドロップの適用 （15 ページ）」の項を参照してください。
- 意図しない動作を防ぐために、使用中の ePBR 実稼働インターフェイスおよび/またはサービス インターフェイスのデフォルト設定は避ける必要があります。
- Cisco NX-OS リリース 10.3(1)F 以降、ePBR L2 は、Cisco Nexus 9300-GX プラットフォーム スイッチの L2 制御パケットのリダイレクションのみをサポートします。サービスチェーンは Cisco Nexus 9300-GX プラットフォーム スイッチではサポートされません。
- Cisco NX-OS リリース 10.4(1)F 以降、ePBR には、Cisco Nexus 9300-EX/FX/FX2/FX3/GX/GX2、および Nexus 9700-EX/FX/GX ライン カードを搭載した Cisco Nexus 9500 プラットフォーム スイッチ で、IPv4 または IPv6 一致のユーザー定義 ACL においてロードバランシングに使用されるビットを選択する、**mask-position** オプションが用意されています。
- 構成のロールバックと設定の置換は、ePBR ポリシーがインターフェイスに関連付けられておらず、ePBR サービス定義が送信元設定とターゲット設定の両方のアクティブな ePBR ポリシーで使用されていない場合にのみサポートされます。ただし、構成のロールバックと構成の置換では、ポリシーとインターフェイスの関連付けおよび関連付け解除はサポートされません。

次の注意事項および制約事項を一致 ACL 機能に適用します。

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

次のガイドラインと制限事項が VRF 間のサービスチェーンに適用されます。

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

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

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

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

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

ePBRサービス、ポリシーの構成およびインターフェイスへの関連付け

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的

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

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

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

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

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

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

ePBR セッションを使用したサービスの変更

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

手順の概要

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

手順の詳細

手順

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

ePBR セッションを使用したポリシーの変更

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

手順の概要

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

手順の詳細

手順

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

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

ePBR ポリシーによる使用される Access-list の更新

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

手順の概要

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

手順の詳細

手順

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

制御トラフィックのリダイレクションとドロップの適用

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

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

all オプションを使用すると、次の動作が観察されます。

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

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

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

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的

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

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

ePBR Show コマンド

次のリストに、ePBR に関連する show コマンドを示します。

手順の概要

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

手順の詳細

手順

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

ePBR 構成の確認

ePBR 構成を確認するためには、次のコマンドを使用します。

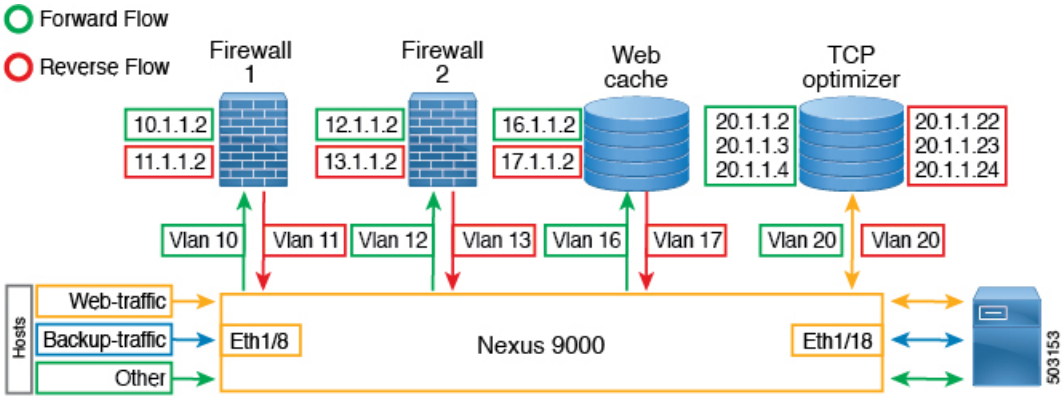
コマンド	目的
show ip access-list <access-list name> dynamic	バケットアクセスリストのトラフィック一致基準を表示します。
show ip sla configuration dynamic	プローブが有効になっている場合に、チェーン内のサービスエンドポイントに対してePBRによって生成されたIP SLA構成を表示します。
show track dynamic	プローブが有効になっている場合に、チェーン内のサービスエンドポイントに対してePBRによって生成されたトラックを表示します。
show ip access-list summary	バケット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

ePBR の構成例

例：ePBR NX-OS 構成

次のトポロジは、ePBR NX-OS 構成を示しています。

図 *1 : ePBR NX-OS* の構成



例：アクセス ポートおよびトランク ポートのサービス構成

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

```
epbr infra vlans 100-200

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

```
    reverse  interface Ethernet1/4

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

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

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

例：アクセス ポートの構成

次の例では、アクセス ポートを構成する方法を示します。

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

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

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

例：トランク ポートの構成

次の構成例は、トランク ポートを構成する方法を示します。

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

```
    10 set service app_1
    20 set service app_2

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

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

Collecting statistics
```

統計の収集：

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

Policy-map p1, match flow2

    Bucket count: 2

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

Policy-map p1, match flow3

    Bucket count: 1

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

Policy-map p1, match flow1

    Bucket count: 1

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

例：ePBR ポリシーの表示

次の例では、ePBR ポリシーを表示する方法を示します。

```
show epbr policy p3

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

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

例：mask-position の使用方法の表示

次に、mask-position の使用例を示します。

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

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

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。