ポリシーベースルーティング

この章では、ポリシーベースルーティング（PBR）をサポートするように ASA を設定する方法について説明します。この項では、ポリシーベースルーティング、PBR のガイドライン PBR の設定について説明します。

ポリシーベース ルーティングについて

従来のルーティングは宛先ベースであり、パケットは宛先 IP アドレスに基づいてルーティングされます。ただし、宛先ベースのルーティング システムでは特定トラフィックのルーティングを変更することが困難です。ポリシーベースルーティング（PBR）では、宛先ネットワークではなく条件に基づいてルーティングを定義できます。PBR では、送信元アドレス、送信元ポート、宛先アドレス、宛先ポート、プロトコル、またはこれらの組み合わせに基づいてトラフィックをルーティングできます。

ポリシーベース ルーティング：

- 区別したトラフィックに Quality of Service（QoS）を提供できます。
- 低帯域幅、低コストの永続パスと、高帯域幅、高コストのスイッチドパスに、インタラクティブ トラフィックとバッチ トラフィックを分散できます。
- インターネット サービス プロバイダーやその他の組織が、さまざまなユーザー セットから発信されるトラフィックを、適切に定義されたインターネット接続を経由してルーティングできます。

ポリシーベース ルーティングには、ネットワーク エッジでトラフィックを分類およびマークし、ネットワーク全体で PBR を使用してマークしたトラフィックを特定のパスに沿ってルーティングすることで、QoS を実装する機能があります。これにより、宛先が同じ場合でも、異

なる送信元から送信されるパケットを別のネットワークにルーティングすることができます。これは、複数のプライベート ネットワークを相互接続する場合に役立ちます。

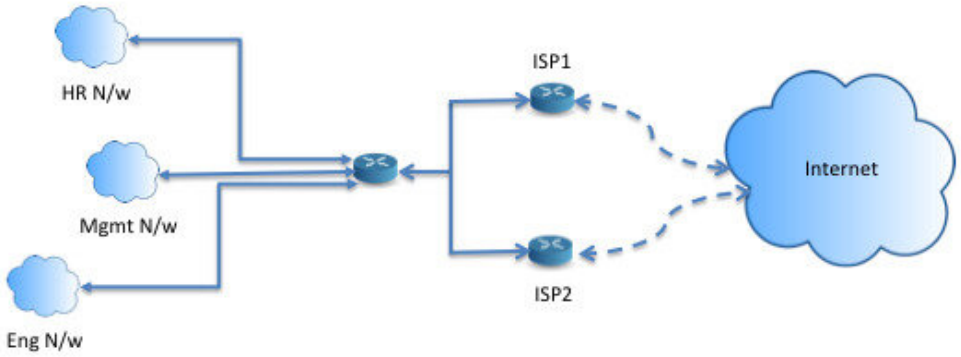
ポリシーベース ルーティングを使用する理由

ロケーション間に 2 つのリンクが導入されている企業を例に説明します。1 つのリンクは高帯域幅、低遅延、高コストのリンクであり、もう 1 つのリンクは低帯域幅、高遅延、低コストのリンクです。従来のルーティング プロトコルを使用する場合、高帯域幅リンクで、リンクの（EIGRP または OSPF を使用した）帯域幅/遅延の特性により実現するメトリックの節約に基づいて、ほぼすべてのトラフィックが送信されます。PBR では、優先度の高いトラフィックを高帯域幅/低遅延リンク経由でルーティングし、その他のすべてのトラフィックを低帯域幅/高遅延リンクで送信します。

ポリシーベース ルーティングの用途のいくつかを以下に示します。

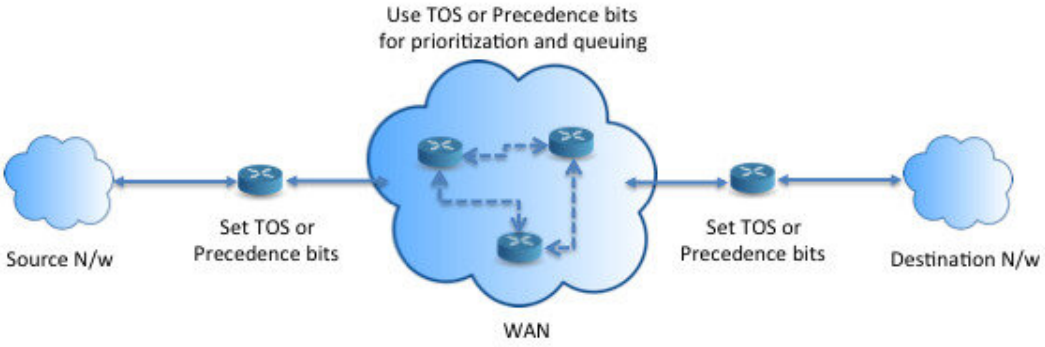
同等アクセスおよび送信元依存ルーティング

このトポロジでは、HR ネットワークと管理ネットワークからのトラフィックは ISP1 を経由するように設定し、エンジニアリング ネットワークからのトラフィックは ISP2 を経由するように設定できます。したがって、ここに示すように、ネットワーク管理者は、ポリシーベース ルーティングを使用して同等アクセスおよび送信元依存ルーティングを実現できます。



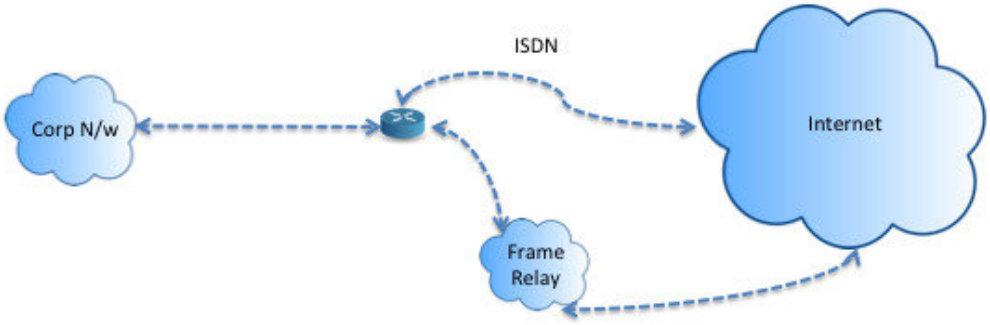
QoS

ネットワーク管理者は、ポリシーベース ルーティングでパケットにタグを付けることにより、ネットワーク トラフィックをネットワーク境界でさまざまなサービス クラスのために分類し、プライオリティ、カスタム、または重み付け均等化のキューイングを使用してそれらのサービス クラスをネットワークのコアに実装できます（下の図を参照）。この設定では、バックボーン ネットワークのコアの各 WAN インターフェイスでトラフィックを明示的に分類する必要がなくなるため、ネットワーク パフォーマンスが向上します。



コスト節約

組織は、特定のアクティビティに関連付けられている一括トラフィックを転送して、帯域幅が高い高コストリンクの使用を短時間にし、さらにここに示すようにトポロジを定義することで帯域幅が低い低コスト リンク上の基本的な接続を継続できます。



ロード シェアリング

ECMP ロード バランシングによって提供されるダイナミックなロード シェアリング機能に加え、ネットワーク管理者は、トラフィックの特性に基づいて複数のパス間にトラフィックを分散するためのポリシーを実装できます。

たとえば、同等アクセスおよび送信元依存ルーティングのシナリオに示すトポロジでは、管理者は、ISP1 を経由する HR netto からのトラフィックと ISP2 を経由するエンジニアリング ネットワークからのトラフィックをロード シェアするようにポリシーベース ルーティングを設定できます。

PBR の実装

ASA は、ACL を使用してトラフィックを照合してから、トラフィックのルーティングアクションを実行します。具体的には、照合のために ACL を指定するルート マップを設定し、次にそのトラフィックに対して1つ以上のアクションを指定します。最後に、すべての着信トラフィックに PBR を適用するインターフェイスにルートマップを関連付けます。

（注） 設定に進む前に、特に NAT と VPN が使用されている場合に、非対称ルーティングによって引き起こされる予期しない動作を回避するために、各セッションの入力トラフィックと出力トラフィックが同じ ISP 側のインターフェイスを通過することを確認してください。

ポリシーベース ルーティングのガイドライン

ファイアウォール モード

ルーテッド ファイアウォール モードでのみサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

フロー別のルーティング

ASA はフロー別にルーティングを実行するため、ポリシー ルーティングは最初のパケットに適用され、その結果決定したルーティングが、そのパケットに対して作成されたフローに格納されます。同一接続に属する後続のパケットはすべてこのフローと照合され、適切にルーティングされます。

出力ルート ルックアップに適用されない PBR ポリシー

ポリシーベース ルーティングは入力専用機能です。つまり、この機能は新しい着信接続の最初のパケットだけに適用され、この時点で接続のフォワード レグの出力インターフェイスが選択されます。着信パケットが既存の接続に属している場合、または NAT が適用され、NAT が出力インターフェイスを選択している場合には PBR がトリガーされないことに注意してください。

初期トラフィックに適用されない PBR ポリシー

（注） 初期接続とは、送信元と宛先の間で必要になるハンドシェイクが完了していない状態を指します。

新しい内部インターフェイスが追加され、一意のアドレスプールを使用して新しい VPN ポリシーが作成されると、新しいクライアントプールの送信元に一致する外部インターフェイスに PBR が適用されます。そのため、PBR はクライアントからのトラフィックを新しいインターフェイスの次のホップに送信します。ただし、PBR は、クライアントへの新しい内部インターフェイスルートとの接続をまだ確立していないホストからのリターントラフィックには関与しません。したがって、有効なルートがないため、ホストから VPN クライアントへのリターントラフィック、具体的には VPN クライアントの応答はドロップされます。内部インターフェイスにおいて、よりメトリックの高い重み付けされたスタティックルートを設定する必要があります。

クラスタ

- クラスタリングがサポートされています。
- クラスタのシナリオでは、スタティック ルートまたはダイナミック ルートがない場合、ip-verify-reverse パスを有効にした非対称トラフィックはドロップされる可能性があります。したがって、ip-verify-reverse パスを無効にすることが推奨されます。

IPv6 のサポート

IPv6 はサポートされます。

パスモニタリングのガイドライン

インターフェイスでパスモニタリングを設定するうえでのガイドラインは、次のとおりです。

- インターフェイスにはインターフェイス名が必要です。
- 管理専用インターフェイスには、パスモニタリングを設定できません。パスモニタリングを設定するには、[このインターフェイスを管理専用にする（Dedicate this interface to management only）] チェックボックスをオフにする必要があります。
- パスモニタリングは、トランスペアレントまたはマルチコンテキスト システム モードのデバイスではサポートされません。
- 自動モニタリングタイプ（auto、auto4、および auto6）は、トンネルインターフェイスではサポートされません。
- パスモニタリングは、次のインターフェイスには設定できません。
  - BVI
  - ループバック
  - DVTI

その他のガイドライン

- ルート マップ関連の既存のすべての設定の制限事項が引き続き適用されます。
- ポリシーベースルーティングには、一致ポリシーリストを含むルートマップを使用しないでください。一致ポリシーリストは BGP にのみ使用されます。
- Unicast Reverse Path Forwarding（uRPF）は、インターフェイスで受信したパケットの送信元 IP アドレスを、PBR ルートマップではなく、ルーティングテーブルと照合して検証します。uRPF が有効になっている場合、PBR を介してインターフェイスで受信されたパケットは、特定のルートエントリがない場合と同じようにドロップされます。したがって、PBR を使用する場合は、uRPF を無効にしてください。

パスモニタリング

パスモニタリングをインターフェイスに設定すると、ラウンドトリップ時間（RTT）、ジッター、平均オピニオン評点（MOS）、インターフェイスごとのパケット損失などのメトリックが得られます。これらのメトリックは、PBR トラフィックをルーティングするための最適なパスを決定するために使用されます。

インターフェイスのメトリックは、インターフェイスのデフォルトゲートウェイまたは指定されたリモートピアへの ICMP プローブメッセージを使用して動的に収集されます。

デフォルトのモニタリングタイマー

メトリックの収集とモニタリングには、次のタイマーが使用されます。

- インターフェイスモニタの平均間隔は 30 秒です。この間隔は、プローブで平均する頻度を示します。
- インターフェイスモニタの更新間隔は 30 秒です。この間隔は、収集された値の平均が計算され、PBR が最適なルーティングパスを決定するために使用できるようになる頻度を示します。
- ICMP によるインターフェースモニタのプローブ間隔は 1 秒です。この間隔は、ICMP ping が送信される頻度を示します。
- HTTP によるアプリケーションモニタのプローブ間隔は 10 秒です。この間隔は、HTTP ping が送信される頻度を示します。パスモニタリングは、平均メトリックを計算するために HTTP ping の最新の 30 サンプルを使用します。

（注） これらのタイマーの間隔は設定または変更できません。

通常、PBR では、トラフィックは、出力インターフェイスに設定された優先順位値（インターフェイスコスト）に基づいて、出力インターフェイスを介して転送されます。Management Center のバージョン 7.2 以降では、PBR は IP ベースのパスモニタリングを使用して、出力インターフェイスのパフォーマンスメトリック（RTT、ジッター、パケット損失、MOS）を収集します。PBR はメトリックを使用して、トラフィックを転送するための最適なパス（出力インターフェイス）を決定します。パスモニタリングは、メトリックが変更されたモニタリング対象インターフェースを PBR に定期的に通知します。PBR は、モニタリング対象インターフェイスの最新のメトリック値をパス モニタリング データベースから取得し、データパスを更新します。

パスモニタリングは、ダイナミックメトリックを使用した場合のみ、RTT、ジッター、packet-lost、または MOS 変更がインターフェイスに設定されている場合にのみ機能します。パスモニタリングは、静的メトリック、つまりインターフェイスコスト（インターフェイスで設定されたコスト）では機能しません。

インターフェイスのパスモニタリングを有効にし、モニタリングタイプを設定する必要があります。[PBRポリシー（PBR policy）] ページでは、パスの決定に必要なメトリックを指定できます。ポリシーベース ルーティングの設定 （7 ページ） を参照してください。

パスモニタリングの設定

ネットワーク サービス グループに基づいてポリシーベースルーティングを実行するようにパスモニタリングを設定できます。NSGなしでパスモニタリングを使用するには、**[インターフェイス（Interface）]**>**[編集（Edit）]**ページに移動して、パスモニタリングのタイプを指定できます。「ポリシーベースルーティングの設定」を参照してください。

手順

ステップ 1 ASDM で、**[設定（Configuration）]** > **[デバイスの設定（Device Setup）]** > **[インターフェイスの設定（Interface Settings）]** > **[パスモニタリング（Path Monitoring）]**の順に選択します。

ステップ 2 [インターフェイス（Interface）] ドロップダウンからインターフェイスを選択します。

ステップ 3 [利用可能なネットワークサービスグループ（Available Network Service Groups）] ボックスでネットワーク サービス グループ（NSG）を選択します。複数の NSG を選択するには、制御キーを使用して必要な NSG をクリックします。

ステップ 4 [追加（Add）] をクリックして、ネットワーク サービス グループを追加します。

ステップ 5 [適用（Apply）] をクリックします。

ステップ 6 設定を削除するには、[追加されたネットワークサービスグループ（Added Network Service Groups）] ボックスから NSG を選択し、[削除（Remove）]、[適用（Apply）] の順にクリックします。

ポリシーベース ルーティングの設定

ルート マップは、1 つ以上のルート マップ文で構成されます。文ごとに、シーケンス番号と permit 句または deny 句が付加されます。各ルート マップ文には、match コマンドと set コマンドが含まれています。match コマンドは、パケット データに適用される一致基準を示します。set コマンドは、パケットに対して実行されるアクションを示します。

- IPv4 と IPv6 の両方の match/set 句でルート マップを設定した場合、または IPv4 および IPv6 トラフィックを照合する統合 ACL を使用した場合、宛先 IP のバージョンに基づいた set アクションが適用されます。
- 複数のネクストホップまたはインターフェイスを set アクションとして設定すると、使用できる有効なオプションが見つかるまですべてのオプションが順に評価されます。設定された複数のオプション間のロード バランシングは実行されません。
- verify-availability オプションは、マルチ コンテキスト モードではサポートされません。

手順

ステップ 1 ASDM で、ポリシーベース ルーティングを実行するトラフィックを特定する 1 つ以上の標準または拡張 ACL を設定します。**[Configuration]** > **[Firewall]** > **[Advanced]** > **[ACL Manager]** を表示します。

ステップ 2 **[設定（Configuration）]** > **[デバイスの設定（Device Setup）]** > **[ルーティング（Routing）]** > **[ルートマップ（Route Maps）]** の順に選択し、[Add] をクリックします。

[Add Route Map] ダイアログボックスが表示されます。

ステップ 3 ルート マップ名とシーケンス番号を入力します。オプションでルート マップ文を追加する場合は、このルート マップ名と同じ名前を使用します。シーケンス番号は、ASA がルートマップを評価する順序です。

ステップ 4 [Deny] または [Permit] をクリックします。

ACL には、固有の permit および deny 文も含まれます。ルート マップと ACL が permit/permit で一致する場合、ポリシーベース ルーティング処理が続行されます。permit/deny で一致する場合、このルート マップでの処理が終了し、別のルート マップがチェックされます。それでも結果が permit/deny であれば、通常のルーティング テーブルが使用されます。deny/deny で一致する場合、ポリシーベース ルーティング処理が続行されます。

ステップ 5 [Match Clause] タブをクリックし、作成した ACL を確認します。

[IPv4] セクションで、ドロップダウン メニューから [Access List] を選択し、ダイアログボックスで 1 つ以上の標準または拡張 ACL を選択します。

（注）
アクセスリストに非アクティブなルールが含まれていないことを確認します。非アクティブなルールを持つ一致 ACL を PBR に設定することはできません。

標準 ACL を使用する場合、照合は宛先アドレスに対してのみ行われます。拡張 ACL を使用する場合、送信元、宛先、またはその両方に対して照合を行えます。

IPv4 と IPv6 の両方に [IPv4] セクションを使用します。拡張 ACL では、IPv4、IPv6、アイデンティティ ファイアウォール、または Cisco TrustSec パラメータを指定できます。ネットワーク サービス オブジェクトを含めることもできます。完全な構文については、ASA コマンドリファレンスを参照してください。

ステップ 6 [ポリシーベースルーティング（Policy Based Routing）] タブをクリックし、トラフィック フローのポリシーを定義します。

一致するトラフィック フローに対して実行する set アクションを、次のうちから 1 つ以上選択します。

- [Set PBR next hop address]：IPv4 および IPv6 では、複数のネクストホップ IP アドレスを設定できます。その場合、ルーティングできる有効なネクスト ホップ IP アドレスが見つかるまで、それらのアドレスが指定された順で評価されます。設定済みのネクストホップは、直接接続する必要があります。そうでなければ、set アクションが適用されません。

- [Set default next-hop IP address]：IPv4 および IPv6 では、一致するトラフィックに対する通常のルート ルックアップが失敗した場合、ASA はここで指定されたネクストホップ IP アドレスを使用してトラフィックを転送します。
- [Recursively find and set next-hop IP address]：ネクストホップ アドレスとデフォルトのネクストホップアドレスのいずれでも、直接接続されたサブネット上でネクストホップが検出されることが要件となります。このオプションを指定した場合、ネクストホップアドレスが直接接続されている必要はありません。代わりにネクストホップアドレスで再帰ルックアップが実行され、一致するトラフィックは、ルータで使用されているルーティング パスに従って、そのルート エントリで使用されているネクストホップに転送されます。
- [Configure Next Hop Verifiability]：ルート マップの次の IPv4 ホップが使用できるかどうかを確認します。ネクストホップの到達可能性を確認するには、SLA モニター追跡オブジェクトを設定できます。[Add] をクリックして、ネクストホップ IP アドレス エントリを追加し、次の情報を指定します。
  - [Sequence Number]：エントリはシーケンス番号を使用して順に評価されます。
  - [IP Address]：ネクスト ホップ IP アドレスを入力します。
  - [Tracking Object ID]：有効な ID を入力します。
- [Set interfaces]:このオプションを使用して、一致するトラフィックを転送するために使用するインターフェイスを設定します。複数のインターフェイスを設定できます。その場合、有効なインターフェイスが見つかるまで、それらのインターフェイスが指定された順で評価されます。**null0** を指定すると、ルート マップと一致するすべてのトラフィックがドロップされます。指定されたインターフェイス（静的または動的のいずれか）経由でルーティングできる宛先のルートが存在している必要があります。
- **[条件を設定（Set Clause）]** > **[適応インターフェイスコスト（Adaptive Interface Cost）]**：このオプションは、[ポリシーベースルーティング（Policy Based Routing）] タブではなく、[条件を設定（Set Clause）] タブにあります。このオプションは、インターフェイスのコストに基づいて出力インターフェイスを設定します。[使用可能なインターフェイス（Available Interfaces）] フィールドをクリックし、考慮する必要があるインターフェイスを選択します。出力インターフェイスは、インターフェイスのリストから選択されます。インターフェイスのコストが同じである場合、アクティブ-アクティブ設定であり、出力インターフェイスでパケットがロードバランシング（ラウンドロビン）されます。コストが異なる場合、コストが最も低いインターフェイスが選択されます。インターフェイスは、アップしている場合にのみ考慮されます。
- [Set null0 interface as the default interface]：通常のルート ルックアップが失敗すると、ASA はトラフィックを null0 に転送し、トラフィックがドロップされます。
- [Set do-not-fragment bit to either 1or 0]：適切なオプション ボタンを選択します。
- [Set differential service code point (DSCP) value in QoS bits]：[IPv4] または [IPv6] ドロップダウン リストから値を選択します。

ステップ 7 [OK] をクリックし、さらに [Apply] をクリックします。

ステップ 8 **[構成（Configuration）]**>**[デバイス設定（Device Setup）]**>**[インターフェイス設定（Interface Settings）]**>**[インターフェイス（Interfaces）]**の順に選択し、このルートマップを適用して出力インターフェイスを決定する入力インターフェイスを設定します。

a) 入力インターフェイスを選択して、[編集（Edit）] をクリックします。

b) [ルートマップ（Route Map）] で、適用するポリシーベースのルートマップを選択します。

c) [適応インターフェイスコスト（Adaptive Interface Cost）] を使用してルートマップで出力インターフェイスを選択した場合は、インターフェイスの [コスト（Cost）] 値を設定します。

値は 1 ー 65535 です。デフォルトは 0 で、このフィールドから値を削除することでリセットできます。値が小さいほど、プライオリティが高くなります。たとえば、1 は 2 よりも優先されます。

d) PBR で柔軟なメトリックを使用してパケットのルーティングに最適なパスを特定するには、[パスモニタリング（Path Monitoring）] ドロップダウンリストから関連するモニタリングタイプを選択します。

- [自動（auto）]：自動 IPv4 と同じように、インターフェイスの IPv4 デフォルトゲートウェイ（存在する場合）に ICMP プローブを送信します。それ以外の場合は、自動 IPv6 と同じように、インターフェイスの IPv6 デフォルトゲートウェイに送信します。
- [ipv4]：モニタリングのために、指定されたピア IPv4 アドレス（ネクストホップ IP）に ICMP プローブを送信します。このオプションを選択すると、隣接するフィールドが有効になります。フィールドに IPv4 アドレスを入力します。
- [ipv6]：モニタリングのために、指定されたピア IPv4 アドレス（ネクストホップ IP）に ICMP プローブを送信します。このオプションを選択すると、隣接するフィールドが有効になります。フィールドに IPv4 アドレスを入力します。
- [auto4]：インターフェイスの IPv4 デフォルトゲートウェイに ICMP プローブを送信します。
- [auto6]：インターフェイスの IPv6 デフォルトゲートウェイに ICMP プローブを送信します。
- [なし（None）]：インターフェイスのパスモニタリングを無効にします。

e) [OK] をクリックし、さらに [Apply] をクリックします。

ポリシーベース ルーティングの履歴

表 *1:* ルート マップの履歴

機能名	プラットフォーム リリース	機能情報
HTTP クライアントによるパスモニタリング	9.20(1)	PBR は、特定の宛先 IP のメトリックではなく、アプリケーションドメインの HTTP クライアントを介したパスモニタリングによって収集されたパフォーマンスメトリック（RTT、ジッター、パケット損失、およびMOS）を使用できるようになりました。HTTP ベースのパスモニタリングは、ネットワーク サービス グループのオブジェクトを使用してインターフェイスで設定できます。 新規/変更された画面：**[設定（Configuration）]**>**[デバイス設定（Device Setup）]** > **[インターフェイス設定（Interface Settings）]** > **[パスモニタリング（Path Monitoring）]**
PBR のパスモニタリングメトリック。	9.18(1)	PBR はメトリックを使用して、トラフィックを転送するための最適なパス（出力インターフェイス）を決定します。パスモニタリングは、メトリックが変更されたモニタリング対象インターフェースを PBR に定期的に通知します。PBR は、モニタリング対象インターフェイスの最新のメトリック値をパス モニタリング データベースから取得し、データパスを更新します。 新規/変更された画面：**[設定（Configuration）]**>**[デバイス設定（Device Setup）]** > **[インターフェイス設定（Interface Settings）]**>**[インターフェイス（Interfaces）]**

機能名	プラットフォーム リリース	機能情報
ポリシーベース ルーティング	9.4(1)	ポリシーベースルーティング（PBR）は、ACLを使用して指定されたQoSでトラフィックが特定のパスを経由するために使用するメカニズムです。ACLでは、パケットのレイヤ3およびレイヤ4ヘッダーの内容に基づいてトラフィックを分類できます。このソリューションにより、管理者は区別されたトラフィックにQoSを提供し、低帯域幅、低コストの永続パス、高帯域幅、高コストのスイッチドパスの間でインタラクティブ トラフィックとバッチ トラフィックを分散でき、インターネットサービスプロバイダーとその他の組織は明確に定義されたインターネット接続を介して一連のさまざまなユーザーから送信されるトラフィックをルーティングできます。 次の画面が更新されました。[Configuration] > [Device Setup] > [Routing] > [Route Maps] > [Policy Based Routing]、[Configuration] > [Device Setup] > [Routing] > [Interface Settings] > [Interfaces]
ポリシーベース ルーティングの IPv6 サポート	9.5(1)	ポリシーベース ルーティングで IPv6 アドレスがサポートされました。 次の画面が変更されました。 **[Configuration] > [Device Setup] > [Routing] > [Route Maps] > [Add Route Map] > [Policy Based Routing]** **[Configuration] > [Device Setup] > [Routing] > [Route Maps] > [Add Route Maps] > [Match Clause]**
ポリシーベース ルーティングの VXLAN サポート	9.5(1)	VNIインターフェイスでポリシーベースルーティングを有効にできるようになりました。 次の画面が変更されました。[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface] > [General]。
アイデンティティ ファイアウォールと Cisco TrustSec でのポリシーベース ルーティングのサポート	9.5(1)	アイデンティティ ファイアウォールと Cisco TrustSec を設定し、ポリシーベースルーティングのルートマップでアイデンティティ ファイアウォールとCisco TrustSec ACLを使用できるようになりました。 次の画面が変更されました。**[Configuration] > [Device Setup] > [Routing] > [Route Maps] > [Add Route Maps] > [Match Clause]**

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。