ポリシーベースルーティング

この章では、Firewall Management Centerの [ポリシーベースルーティング（Policy Based Routing）] ページを使用して、ポリシーベースルーティング（PBR）をサポートするようにFirewall Threat Defenseを設定する方法について説明します。次の項では、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 （1 ページ）
- ポリシーベース ルーティングの履歴 （3 ページ）
- ポリシーベース ルーティングの注意事項 （3 ページ）
- パスモニタリング （5 ページ）
- ポリシーベース ルーティング ポリシーの設定 （10 ページ）
- ポリシーベースルーティングの設定例 （21 ページ）
- パスモニタリングを使用した PBR の設定例 （27 ページ）
- PBR のモニタリングに役立つ CLI （29 ページ）
- PBRのトラブルシューティング （32 ページ）
- ポリシーベース ルーティングの履歴 （35 ページ）

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では、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。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）は、ルーティング プロトコルによって提供されるメカニズムを拡張および補完し、ルーティングをより細かく制御できるようにします。

PBR では、 IP precedence を設定できます。高コスト リンク上のプライオリティ トラフィックなど、特定のトラフィックのパスを指定することもできます。PBR では、宛先ネットワークではなく条件（送信元ポート、宛先アドレス、宛先ポート、プロトコル、アプリケーション、またはこれらのオブジェクトの組み合わせなど）に基づいてルーティングを定義できます。

PBRを使用すると、アプリケーション、ユーザー名、グループメンバーシップ、およびセキュリティグループの関連付けに基づいてネットワークトラフィックを分類できます。このルーティング方法は、大規模なネットワーク展開で多数のデバイスがアプリケーションやデータにアクセスするシナリオに適用されます。大規模な展開では、通常、ネットワーク トラフィック

はルートベースの VPN で暗号化されたトラフィックとしてハブにバックホールされます。これらのトポロジでは、パケットの遅延、帯域幅の減少、パケットのドロップなどの問題が発生することがよくあります。これらの問題を解決するには、コストがかかる複雑な展開と管理が必要です。

PBR ポリシーを使用すると、指定したアプリケーションのトラフィックを安全にブレークアウトできます。Secure Firewall Management Center ユーザーインターフェイスで PBR ポリシーを設定して、アプリケーションに直接アクセスできるようにすることができます。

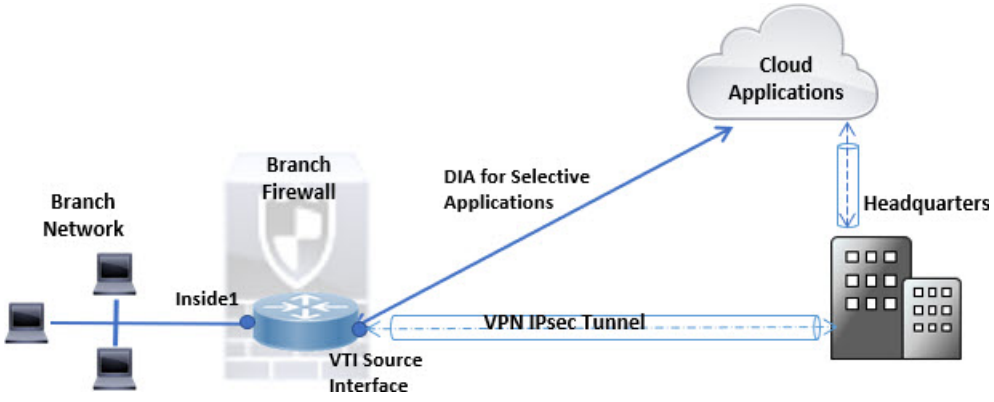
ポリシーベースルーティングを使用する理由

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、または両方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 ルーティングを使用できるシナリオをいくつか示します：

- **ダイレクト インターネット アクセス**

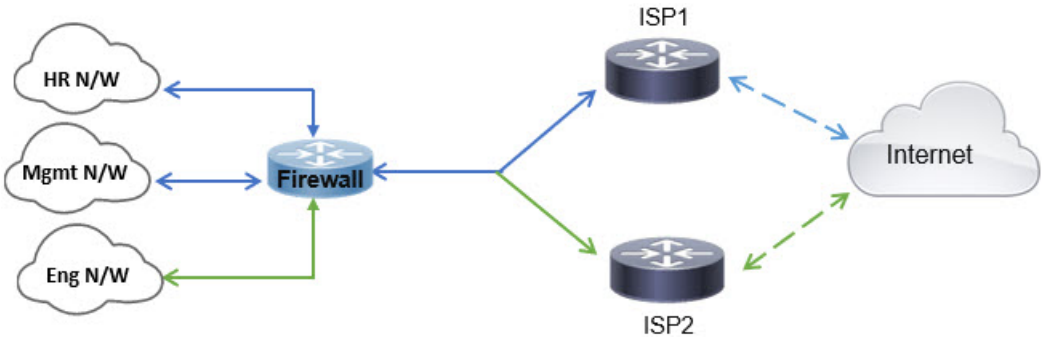
  このトポロジでは、ブランチオフィスからのアプリケーショントラフィックを、本社に接続する VPN トンネルを経由する代わりに、インターネットに直接ルーティングできます。ブランチFirewall Threat Defense は、インターネット イグジット ポイントを使用して設定されます。PBR ポリシーは入力インターフェイス（*Inside 1*）に適用されて、ACL で定義されたアプリケーション、ユーザー ID（ユーザー名とグループメンバーシップ）、およびセキュリティグループタグ（セキュリティグループの関連付け）に基づいてトラフィックを識別します。それに応じて、トラフィックは出力インターフェースを介して直接インターネットまたは IPsec VPN トンネルに転送されます。



- **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、この例では、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。



- **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 ネットワーク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ルーティングして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。

ポリシーベース ルーティングの履歴

- すべての PBR ポリシー機能は、 EssentialsFirewall Threat Defense スマート ライセンスでサポートされます。
- Secure Client ライセンスは、 RA VPNトンネル インターフェイスを介してトラフィックをルーティングするために PBR を設定する場合に必要です。
- PBR ポリシーで ISE を使用するには、Cisco ISE ライセンスが必要です。

ポリシーベース ルーティングの注意事項

デバイスの注意事項

- PBR ～ Firewall Management Center の [ポリシーベースのルーティング（Policy Based Routing）] ページは、 バージョン 7.1 または、それ以降を搭載する Firewall Management Center およびデバイスでのみサポートされます。
- Firewall Management Center または Firewall Threat Defense をバージョン 7.1 または、それ以降にアップグレードすると、デバイスの PBR 設定が削除されます。[ポリシーベースのルーティング（Policy Based Routing）] ページを使用して PBR を再度設定する必要があります。

管理対象デバイスがバージョン 7.1 以前の場合は、展開オプションを [毎回（every time）] に設定した FlexConfig を使用して PBR を再度設定する必要があります。

- クラスタデバイスでのアプリケーションベースのポリシーの設定は、サポートされていません。Secure Firewall 200PBR

インターフェイス ガイドライン

- グローバル仮想ルータに属するルーテッド インターフェイスおよび非管理専用インターフェイスのみ、PBR ポリシーに対して、入力インターフェイスまたは出力インターフェイスとして構成できます。ポリシーに対して、ユーザー定義の仮想ルータ インターフェイスを構成できません。
- ポリシー内で定義するインターフェイスには、論理的な名が必要です。
- スタティック VTI は、出力インターフェイスとしてのみ設定できます。
- PBR 出力インターフェイスの設定にはダイナミック VTI を選択しないでください。

IP アドレス（IP Address）

IPv4 と IPv6 の両方のトラフィックを管理するために、PBR を適用できます。

アプリケーションベースの PBR と DNS の設定

- アプリケーションベースの PBR は、アプリケーション検出に DNS スヌーピングを使用します。アプリケーションの検出は、DNS 要求がクリアテキスト形式で Firewall Threat Defense を通過する場合にのみ成功します。DNS トラフィックは暗号化されません。
- アプリケーション検出を成功させるには、信頼された DNS サーバーを設定する必要があります。

DNS サーバーの構成の詳細については、DNS を参照してください。

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、PBR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

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。応答がドロップされないように、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 ルートを構成する必要があります。

HTTP ベースのパスモニタリングのガイドライン

- HTTPベースのパス モニタリングは、物理、ポートチャネル、サブインターフェイス、およびスタティック トンネル インターフェイスでのみサポートされます。クラスター デバイスでは構成しないでください。
- HTTP は、IPv4 のみを使用してアプリケーションの ping を実行します。IPv4 メトリックは、IPv4 トラフィックと IPv6 トラフィックの両方のルーティングおよび転送に適用されます。
- Secure Firewall Management Center バージョン 7.4 以降の HTTP ベースのアプリケーション モニタリングは、デフォルトで有効になっています。ただし、以前のバージョンからアップグレードする場合、このオプションはデフォルトでは有効になりません。手動で有効にする必要があります。

その他のガイドライン

- 構成に関する既存のすべての制限事項とルートマップの制限が、引き続き適用されます。
- ポリシー一致基準のACLを定義するときに、リストから事前定義された複数のアプリケーションを選択して、アクセスコントロールエントリ（ACE）を形成することができます。Firewall Threat Defense では、事前定義されたアプリケーションはネットワーク サービス オブジェクトとして保存され、アプリケーションのグループはネットワーク サービス グループ（NSG）として保存されます。最大 1024 のそのような NSG を作成できます。アプリケーションまたはネットワーク サービス グループは、先頭パケット分類によって検出されます。現在、定義済みのアプリケーションリストへの追加やリストの変更はできません。ただし、カスタムのアプリケーション ディテクタを作成することはできます。PBR向けのカスタムアプリケーション検出器を作成する （14 ページ）を参照してください。
- 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 を必ず無効にしてください。

パスモニタリング

PBR は、スタティック コストまたはパス モニタリング（ダイナミックメトリック）を使用してトラフィックをルーティングします。

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。

ICMP ベースのパスモニタリング

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。

HTTP ベースのパスモニタリング

パス モニタリングでは、インターフェイスに関連付けられた各リモート ピアのダイナミックメトリックが計算されます。ブランチファイアウォールでポリシーを介して複数のアプリケーションをモニタリングし、ベストパスを決定するには、次の理由により、ICMP よりも HTTP が推奨されます。

- HTTP-ping は、アプリケーションがホストされているサーバーのアプリケーションレイヤまでのパスのパフォーマンスメトリックを取得できます。
- アプリケーションサーバーの IP アドレスが変更されるたびにファイアウォール設定を変更する必要がなくなります。これは、IP アドレスではなくアプリケーション ドメインが追跡されるためです。

（注） 同じインターフェイスで ICMP と HTTP の両方を設定できます。ポリシーの宛先がいずれかのドメイン IP に一致する場合、対応するメトリックが使用されます。宛先がどの設定済みドメインにも一致しない場合、PBR は、ICMP からのメトリックを使用して発信インターフェイスを選択します。

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。

PBR とパスモニタリング

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 ポリシーの設定 （10 ページ） を参照してください。

PBR と HTTP ベースのパスモニタリング

Management Center バージョン 7.4 以降、PBR は、HTTP ベースのパスモニタリングを使用して、1 つの宛先 IP アドレスだけでなく、アプリケーションドメインのパフォーマンスメトリックを収集するように設定できます。パスモニタリングは、ドメインの DNS エントリが検出された後にのみ開始されます。HTTP ベースのアプリケーションモニタリングが設定されている場合、このサービスはすぐには開始されません。ドメインの解決された IP アドレスを取得した後、パスモニタリングは HTTP 要求を送信し、応答を受信します。DNS が単一ドメインの複数の IP アドレスを解決する場合、パス モニタリングは最初に解決された IP アドレスを用いて、アプリケーションのプローブとモニタリングを行います。IP アドレスが変更されるか、HTTP ベースのパス モニタリングが無効になるまで、モニタリングが継続されます。

HTTP 要求および応答の期間に基づいて、パスモニタリングはアプリケーションのパフォーマンスメトリックを計算します。パス モニタリングは、収集されたメトリックを定期的に PBR に送信するため、PBR は設定済みの入力インターフェイスからのトラフィックのルーティングと転送を決定できます。パスモニタリングがそのメトリックを PBR に送信する前にトラフィックが到着した場合、ルーティング テーブルがトラフィック フローを決定します。メトリックが使用可能になると、PBR はそれらを使用して後続のトラフィックのルーティングを決定します。

（注） ポリシーの一致 ACL のネットワーク サービス グループに基づいて、複数の IP アドレスを持つ複数のドメインに PBR を適用できます。

Management Center は、PBR 設定が次の基準を満たしている場合にのみ、アプリケーションと NSG を出力インターフェイスに関連付けます。

- 一致 ACL には、モニタリング対象のアプリケーションが含まれています。
- PBR ポリシーは、次のいずれかのインターフェイス順序値（メトリックタイプ）で設定されます。
  - 最小ジッター
  - 最大平均オピニオン評点
  - 最小ラウンドトリップ時間
  - 最小パケット損失

パスモニタリングの設定

PBR ポリシーは、往復時間（RTT）、ジッター、平均オピニオン スコア（MOS）、インターフェイスのパケット損失などのメトリックを柔軟に使用して、そのトラフィックに最適なルーティング パスを識別します。パスモニタリングは、指定されたインターフェイスでこれらのメトリックを収集します。**[インターフェイス（Interfaces）]** ページで、パス モニタリングの設定を使用してインターフェイスを設定し、メトリック収集のために ICMP プローブまたは HTTP ping を送信できます。

手順

ステップ 1 [**Devices** > **Device Management**] を選択して、Firewall Threat Defense デバイスに対して [**Edit** (✎)] をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス **Edit** (✎) をクリックします。

ステップ 3 [パスモニタリング（Path Monitoring）] タブをクリックします。

ステップ 4 インターフェイスの ICMP ベースのモニタリングを設定するには、[IPベースのモニタリングの有効化（Enable IP based Monitoring）] チェックボックスをオンにします。

ステップ 5 [モニタリングタイプ（Monitoring Type）] ドロップダウンリストから、該当するオプションを選択します。

- [自動（Auto）] : 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。IPv4 ゲートウェイが存在しない場合、パスモニタリングはプローブを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。

- [ピアIPv4（Peer 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した場合は、[モニターするピアIP（Peer IP To Monitor）] フィールドに IPv4 アドレスを入力します。
- [ピアIPv6（Peer IPv6）]：モニタリングのために、指定されたピア IPv6 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した場合は、[モニターするピアIP（Peer IP To Monitor）] フィールドに IPv6 アドレスを入力します。
- [自動IPv4（Auto IPv4）]：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。
- [自動IPv6（Auto IPv6）]：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。

（注）
- 自動オプションは、VTIインターフェイスでは使用できません。ピアアドレスを指定する必要があります。
- 宛先へ向かう 1 つのネクストホップのみがモニターされます。つまり、複数のピアアドレスを指定してインターフェイスをモニターすることはできません。

ステップ 6 デフォルトでは、[HTTPベースのアプリケーションモニタリングの有効化（Enable HTTP based Application Monitoring）] チェックボックスがオンになっています。このインターフェイスがポリシーで出力インターフェイスとして設定されている場合、PBR ポリシーの一致 ACL でパスモニタリング用に選択されたすべてのアプリケーションがリストされます。インターフェイスの HTTP ベースのモニタリングを無効にするには、チェックボックスをオフにします。

ステップ 7 **[OK]**をクリックします。

ステップ 8 設定を保存するには、[Save] をクリックします。

パス監視ダッシュボードの追加

パスモニタリングメトリックを表示するには、パス監視ダッシュボードをデバイスの [ヘルスモニタリング（Health Monitoring）] ページに追加する必要があります。

手順

ステップ 1 **System** (⚙) > **Health** > **Monitor**を選択します。

ステップ 2 デバイスを選択し、[新規ダッシュボードの追加（Add New Dashboard）] をクリックします。

ステップ 3 カスタムダッシュボードの名前を入力します。

ステップ 4 [メトリック（Metrics）] 領域で、[事前定義された相関関係から追加（Add from Predefined Correlations）] ボタンをクリックします。

ステップ 5 リストから、[インターフェイス - パスメトリック（Interface - Path Metrics）] をクリックします。

デフォルトでは、4つのメトリックすべてと追加のメトリック フィールドがダッシュボードのウィジェットとして表示されるように選択されています。いずれかを除外するには、**Delete**（）をクリックします。

ステップ 6 [ダッシュボードの追加（Add Dashboard）] をクリックします。

ポリシーベース ルーティング ポリシーの設定

PBR ポリシーを構成するには、ポリシー ベース ルーティング ページで、入力インターフェイス、一致基準（拡張アクセス制御リスト）および出力インターフェイスを指定します。

始める前に

出力インターフェイスでパスモニタリングメトリックを使用してトラフィック転送の優先順位を設定するには、インターフェイスのパスモニタリング設定を行う必要があります。パスモニタリングの設定 （8 ページ）を参照してください。

手順

ステップ 1 **Devices** > **Device Management** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）] をクリックします。

ステップ 3 [ポリシーベースルーティング（Policy Based Routing）] をクリックします。

[ポリシーベースルーティング（Policy Based Routing）] ページに、設定されたポリシーが表示されます。グリッドには、入力インターフェイスと、ポリシーベースのルート アクセス リストと出力インターフェイスの組み合わせが表示されます。

ステップ 4 ポリシーを設定するには、[追加（Add）] をクリックします。

ステップ 5 [ポリシーベースルートの追加（Add Policy Based Route）] ダイアログボックスで、ドロップダウンリストから [入力インターフェイス（Ingress Interface）] を選択します。

（注）
ドロップダウンから、論理名を持ち、グローバル仮想ルータに属するインターフェイスのみを選択できます。論理名を持つ VLAN インターフェイスを送信元（入力）インターフェイスとして設定することはできません。

ステップ 6 ポリシーで一致基準と転送アクションを指定するには、[追加（Add）] をクリックします。

ステップ 7 [転送アクションの追加（Add Forwarding Actions）] ダイアログボックスで、次の操作を実行します。

a) [Match ACL] ドロップダウンから、拡張アクセス コントロール リスト オブジェクトを選択します。ACL オブジェクトを事前に定義するか（拡張 ACL オブジェクトの設定を参照）、**Add**(＋)アイコンをクリックしてオブジェクトを作成することができます。[新しい拡張アクセスリストオブジェクト（New Extended Access List Object）] ボックスに名前を入力し、[追加（Add）] をクリックして [拡張アクセスリストエントリの追加（Add Extended Access List Entry）] ダイアログボックスを開きます。ここで、PBR ポリシーのネットワーク、ポート、ユーザーアイデンティティ、SGT、またはアプリケーションの一致基準を定義できます。PBR と同期されるカスタムドメインを作成する場合は、「PBR 向けのカスタムアプリケーション検出器を作成する （14 ページ）」を参照してください。

（注）
ACE に定義できるのは宛先アドレスまたはアプリケーション/ユーザーアイデンティティ/SGT のいずれかです。

着信インターフェイスに PBR を選択的に適用するには、ACE でブロック基準を定義します。トラフィックが ACE のブロックルールに一致すると、トラフィックはルーティングテーブルに基づいて出力インターフェイスに転送されます。

b) [送信先（Send To）] ドロップダウンリストから：

- 構成されたインターフェイスを選択するには、[出力インターフェイス（Egress Interfaces）] を選択します。
- IPv4/IPv6 ネクストホップアドレスを指定するには、[IPアドレス（IP Address）] を選択します。手順 7.e （12 ページ） に進みます

c) [出力インターフェイス（Egress Interfaces）] を選択した場合は、[インターフェイスの順位付け（Interface Ordering）] ドロップダウンから、関連するオプションを選択します。

- [インターフェイスの優先度（By Interface Priority）]：トラフィックはインターフェイスの優先度に基づいて転送されます。トラフィックは、優先度が最も低いインターフェイスに最初にルーティングされます。そのインターフェイスが使用できない場合、トラフィックは次に優先順位値が低いインターフェイスに転送されます。たとえば、*Gig0/1*、*Gig0/2*、および *Gig0/3* にそれぞれ優先順位値 *0*、*1*、および *2* が設定されているとします。トラフィックは *Gig0/1* に転送されます。*Gig0/1* が使用できなくなった場合、トラフィックは *Gig0/2* に転送されます。

  （注）
  インターフェイスの優先度を構成するには、[ポリシーベースルーティング（Policy Based Routing）] ページで [インターフェイスの優先度の設定（Configure Interface Priority）] をクリックします。ダイアログボックスで、インターフェイスに対する優先度番号を指定し、[保存（Save）] をクリックします。インターフェイス設定でインターフェイスの優先度を設定することもできます。

  すべてのインターフェイスで優先度値が同じである場合、トラフィックはインターフェイス間で分散されます。デフォルトでは、PBR のインターフェイス優先順位は 0 に設定されています。優先順位値が最も低いインターフェイスが、トラフィック転送で優先されます。

- [順序（By Order）]：トラフィックは、ここで指定されたインターフェイスの順序に基づいて転送されます。たとえば、*Gig0/1*、*Gig0/2*、*Gig0/3* が、*Gig0/2*、*Gig0/3*、*Gig0/1* の順に選択されたとします。トラフィックは、優先度の値に関係なく、最初に *Gig0/2* に転送され、次に *Gig0/3* に転送されます。
- [最小ジッター（By Minimal Jitter）]：トラフィックは、ジッター値が最小のインターフェイスに転送されます。ジッター値を取得するには、PBR のインターフェイスでパスモニタリングを有効にする必要があります。
- [最大平均オピニオン評点（By Maximum Mean Opinion Score）]：トラフィックは、平均オピニオン評点（MOS）が最大のインターフェイスに転送されます。MOS 値を取得するには、PBR のインターフェイスでパスモニタリングを有効にする必要があります。
- [最短ラウンドトリップ時間（By Minimal Round Trip Time）]：トラフィックは、ラウンドトリップ時間（RTT）が最短のインターフェイスに転送されます。RTT 値を取得するには、PBR のインターフェイスでパスモニタリングを有効にする必要があります。
- [最小パケット損失（By Minimal Packet Loss）]：トラフィックは、パケット損失が最小のインターフェイスに転送されます。パケット損失値を取得するには、PBR のインターフェイスでパスモニタリングを有効にする必要があります。

d) [使用可能なインターフェイス（Available Interfaces）]ボックスに、すべてのインターフェイスとその優先度の値が一覧表示されます。インターフェイスのリストから、**Add** (+) ボタンをクリックして、選択した出力インターフェイスに追加します。手順 7.k （13 ページ） に進みます

（注）
選択したインターフェイスへのルートがルーティングテーブルに存在している必要があります。

e) [IPアドレス（IP Address）] を選択した場合は、[IPv4アドレス（IPv4 Addresses）] または [IPv6アドレス（IPv6 Addresses）] フィールドに IP アドレスをカンマで区切って入力します。トラフィックは、指定された IP アドレスの順序で転送されます。

（注）
複数のネクストホップ IP アドレスが指定されている場合、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、トラフィックは指定された IP アドレスの順序に従って転送されます。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。

f) [フラグメント化しない（Don't Fragment）] ドロップダウンリストから、[はい（Yes）]、[いいえ（No）]、または [なし（None）] を選択します。DF（フラグメント化しない（Don't Fragment））フラグが [はい（Yes）] に設定されている場合、中間ルータはパケットのフラグメント化を実行しません。

g) 現在のインターフェイスを転送のデフォルトとして指定するには、[デフォルトインターフェイス（Default Interface）] チェックボックスをオンにします。

h) **[IPv4設定（IPv4 Settings）]** および **[IPv6設定（IPv6 Settings）]** タブでは、再帰設定とデフォルト設定を指定できます。

（注）
ルートマップの場合、IPv4 または IPv6 ネクストホップ設定のいずれかのみを指定できます。

- [再帰（Recursive）]：ルートマップ設定は、指定された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が直接接続されたサブネット上で見つかった場合にのみ適用されます。ただし、再帰オプションを使用できます。この場合、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。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、ルータの現在の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。
- [デフォルト（Default）]：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すると、ここで指定されたネクストホップ IP アドレスにトラフィックが転送されます。

i) ネクストホップアドレスをピアアドレスとして使用するには、[ピアアドレス（Peer Address）] チェックボックスをオンにします。

（注）
デフォルトのネクストホップアドレスとピアアドレスの両方を使用してルートマップを設定することはできません。

j) IPv4 設定の場合、[可用性の検証（Verify Availability）] で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できます。**Add** (＋) ボタンをクリックし、ネクストホップ IP アドレスエントリを追加します。

- [IP Address]：ネクスト ホップ IP アドレスを入力します。
- [シーケンス（Sequence）]：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。重複するシーケンス番号が入力されていないことを確認してください。有効な範囲は 1 ～ 65535 です。
- [トラック（Track）]：有効な ID を入力します。有効範囲は 1 ～ 255 です。

k) [保存（Save）] をクリックします。

ステップ 8 ポリシーを保存するには、[保存（Save）] および [展開（Deploy）] をクリックします。

Firewall Threat Defense は、ACL を使用してトラフィックを照合し、トラフィックのルーティングアクションを実行します。通常、トラフィックが照合される 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。パスモニタリングにより、PBR でトラフィックのルーティングに最適な出力インターフェイスを選択できるようになりました。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。

PBR 向けのカスタムアプリケーション検出器を作成する

この項では、カスタムアプリケーション検出器の作成とアプリケーションベースの PBR ポリシーの構成プロセスについて概説します。

1. ユーザー定義アプリケーションを作成する で説明されている通り、ユーザー定義アプリケーション向けのカスタム検出器を作成します。

（注） ユーザー定義アプリケーションを作成中は、**[タグ（Tag）]** ドロップダウンリストで [NSG] をかならず選択します。

2. 検出パターンを手動で定義するには、基本ディテクタでの検出パターンの指定で説明されているように、**[基本（Basic）]** 検出器の種類を選択して、定義します。または、.lua ファイルを使用して検出パターンを作成する場合は、**[高度（Advanced）]** 検出器の種類を選択して、高度なディテクタでの検出条件の指定 に記載されている手順を実行します。
3. カスタム検出器をアクティブにします。
4. カスタムアプリケーション ACE を使用して PBR 向けの ACL ポリシー（拡張済み）を構成します。ACL の作成手順については、「拡張 ACL オブジェクトの設定」を参照してください。
5. PBR ポリシーで、希望の転送アクションと一致する ACL を選択します。PBR ポリシーの作成手順については、「ポリシーベース ルーティング ポリシーの設定 （10 ページ）」を参照してください。

カスタム アプリケーション ディテクタ を使用した PBR の設定例

この例では、以下のドメイン向けにカスタムアプリケーション検出器を使用した PBR ポリシーの構成を詳細に説明します：

- amazon123.com
- flipkart.com
- hamleysonline.com

始める前に

- この例では、PBR ポリシーおよびカスタムアプリケーション検出器を設定するための基本的な手順を理解していることを前提としています。
- 論理名による入力インターフェイスと出力インターフェイスの構成が完了している必要があります。この例では、入力インターフェイスの名前は *Inside1*、出力インターフェイスの名前は *eBuy* です。

手順

ステップ 1 カスタム ディテクタ *PBRePurchase*を作成します。

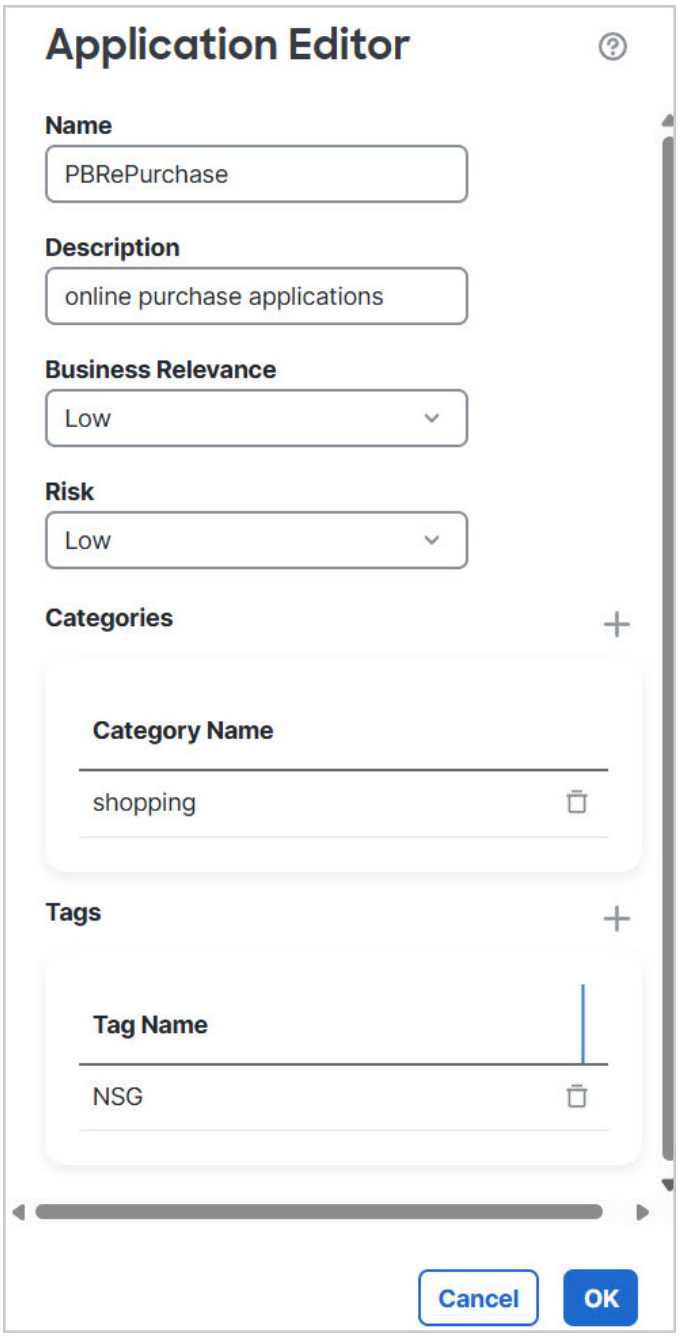
a) **Policies** > **Application Detectors** を選択し、**[カスタム ディテクタの作成（Create Custom Detector）]** をクリックします。

b) **[カスタム アプリケーション ディテクタを作成する（Create A Custom Application Detector）]** に、名前（この例では *PBRePurchase*）と説明を入力します。

c) カスタム アプリケーションを作成するには、(+) をクリックします。

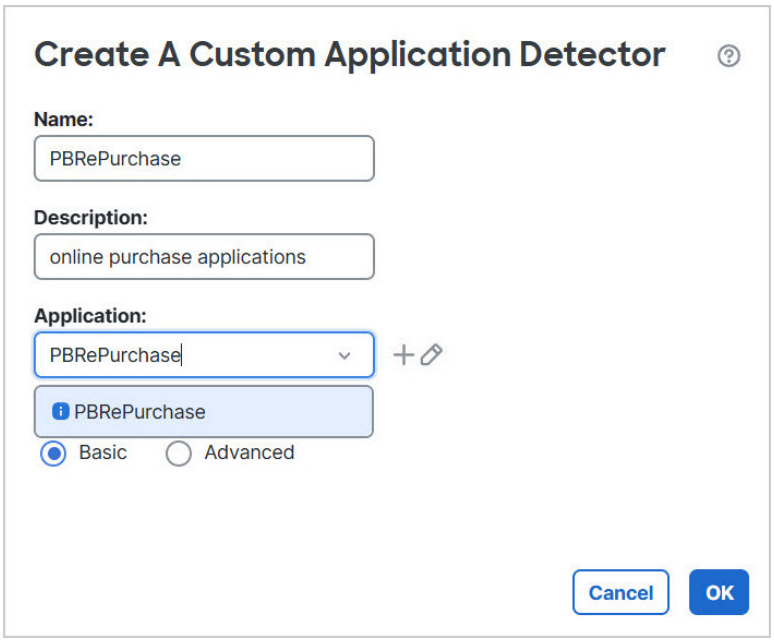
d) **[アプリケーション エディタ（Application Editor）]** ダイアログ ボックスで、フィールドに関連する値を入力します。各フィールドの詳細については、ユーザー定義アプリケーションを作成する を参照してください。

（注）
カスタム アプリケーションが PBRで検出可能になるようにするには、**[Tag]** ドロップダウン リストから **[NSG]** を選択していることを確認します。



e) **[OK]**をクリックします。

f) **[アプリケーション（Application）]** ドロップダウン リストから、*[PBRePurchase]*を選択します。

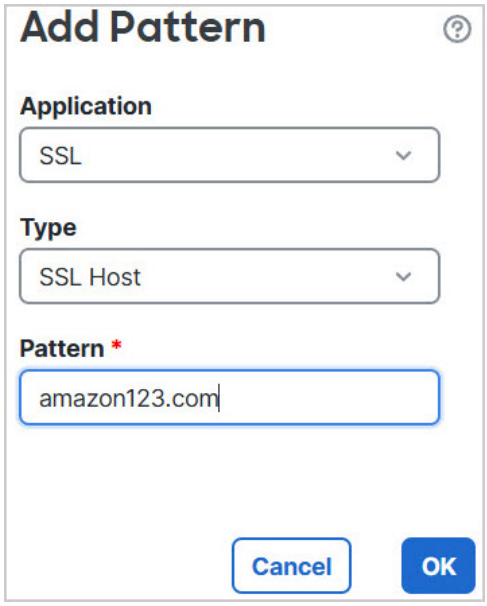


a) **[基本（Basic）]** オプションボタンをクリックし、**[OK]**をクリックします。

（注）
PBR ポリシーでは **[高度（Advanced）]** ディテクタ タイプはサポートされません。

b) **[アプリケーションディテクタ（Application Detector）]** ページで、**[検出パターン（Detection Patterns）]** 領域の **[追加（Add）]** ボタンをクリックしてパターンを追加します。

c) **[アプリケーション（Application）]** ドロップダウン リストから、プロトコル タイプとして **[SSL]** を選択し、適切なパターン タイプを選択します。選択したタイプ（この例では *amazon123.com*と入力）に一致するパターン文字列を入力して、**[OK]**をクリックします。

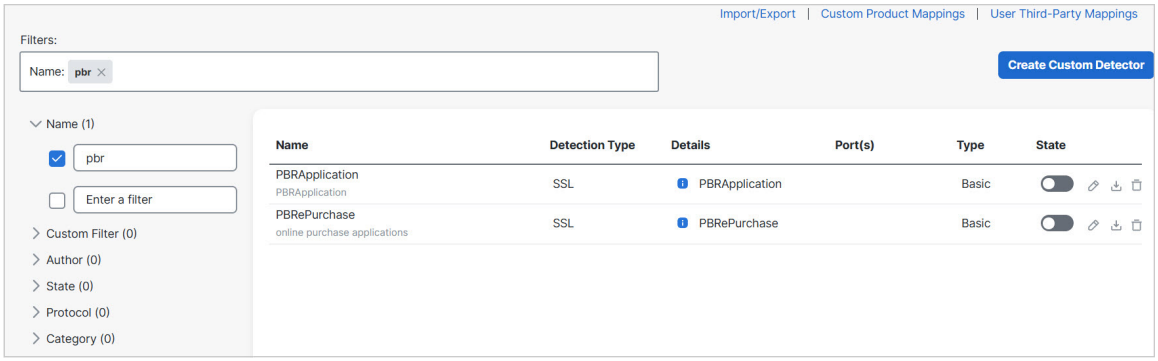


d) 手順を繰り返して、カスタム ドメインのほかの 2 つのパターンを作成します。*flipkart.com* と *hamleysonline.com* です。

e) **[保存（Save）]** をクリックします。

ステップ 2 アプリケーション ディテクタ ダッシュボードで、フィルタを使用して、作成したカスタム アプリケーション ディテクタを検索します。

ステップ 3 カスタムディテクタを有効にするには、対応するアプリケーションディテクタの横にある **[状態（State）]** トグルボタン () （）をクリックします。



ステップ 4 表示されるダイアログ ボックスで、 **[はい（Yes）]** をクリックします。

アプリケーション ディテクタがアクティブになると、成功メッセージが表示されます。

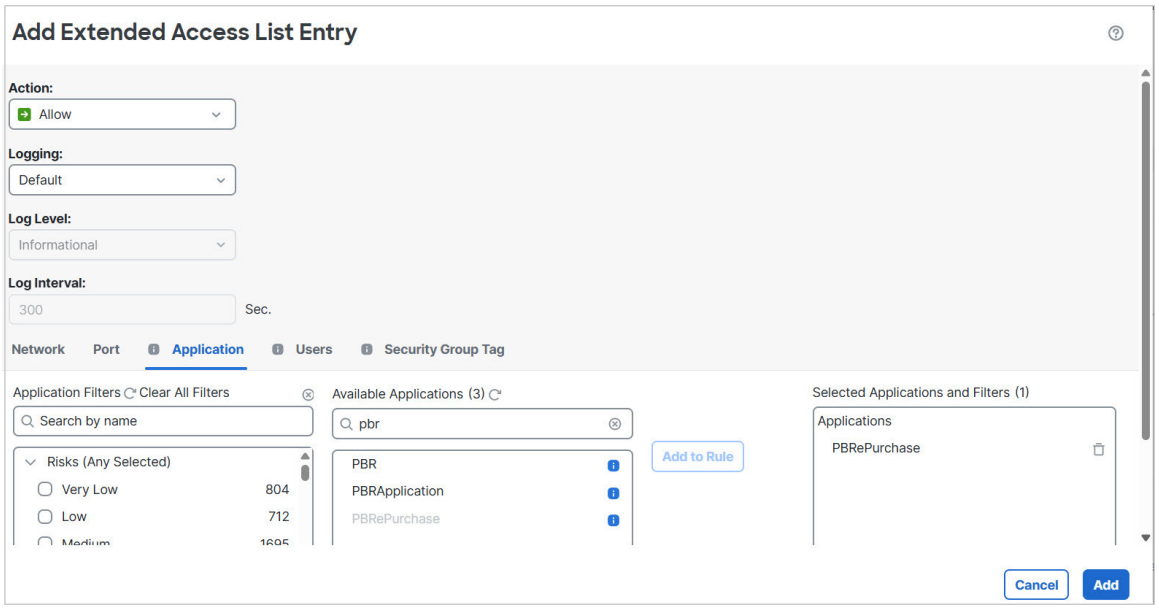
ステップ 5 PBR ポリシーと同期するためのカスタム アプリケーション ディテクタを使用して ACL を作成するには、次の手順を実行します。

a) **Objects** > **Object Management** > **Access List** > **Extended** を選択します。

b) [拡張アクセスリストを追加（Add Extended Access List）] をクリックします。

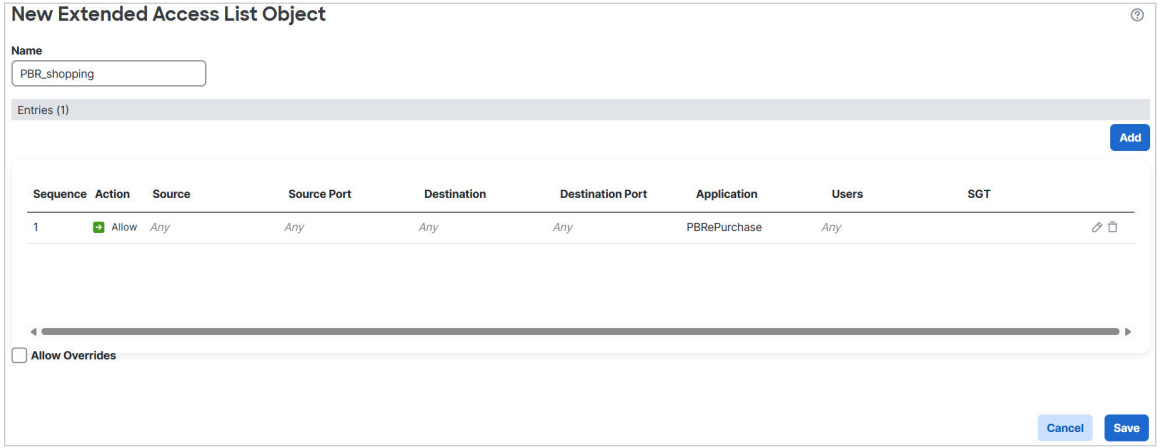
c) リストの名前（*PBR_customing* など）を入力し、**[追加（Add）]** をクリックしてリストの ACE を作成します。

d) **[拡張アクセス リスト エントリの追加（Add Extended Access List Entry）]** ダイアログ ボックスで、**[アプリケーション（Application）]** タブをクリックし、アプリケーション名として *[PBRePurchase]* を選択し、**[ルールに追加（Add to Rule）]** をクリックします。



e) [追加（Add）] をクリックします。

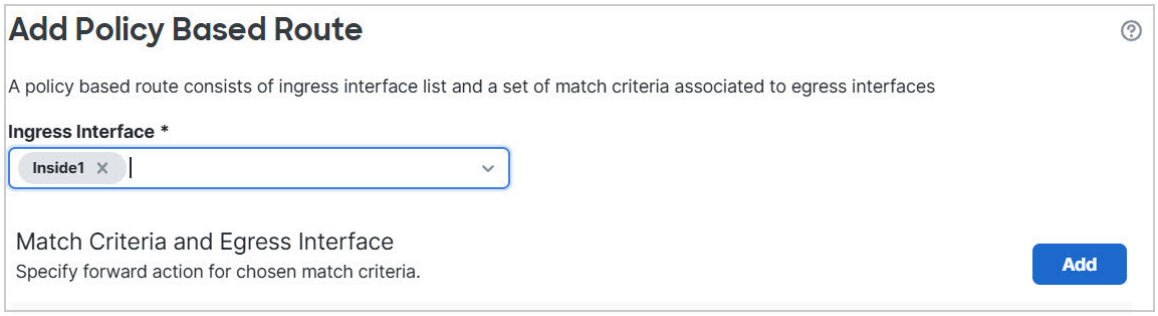
f) **[保存（Save）]** をクリックします。



ステップ 6 **[ルーティング（Routing）]** > **[ポリシー ベース ルーティング）]**を選択します。

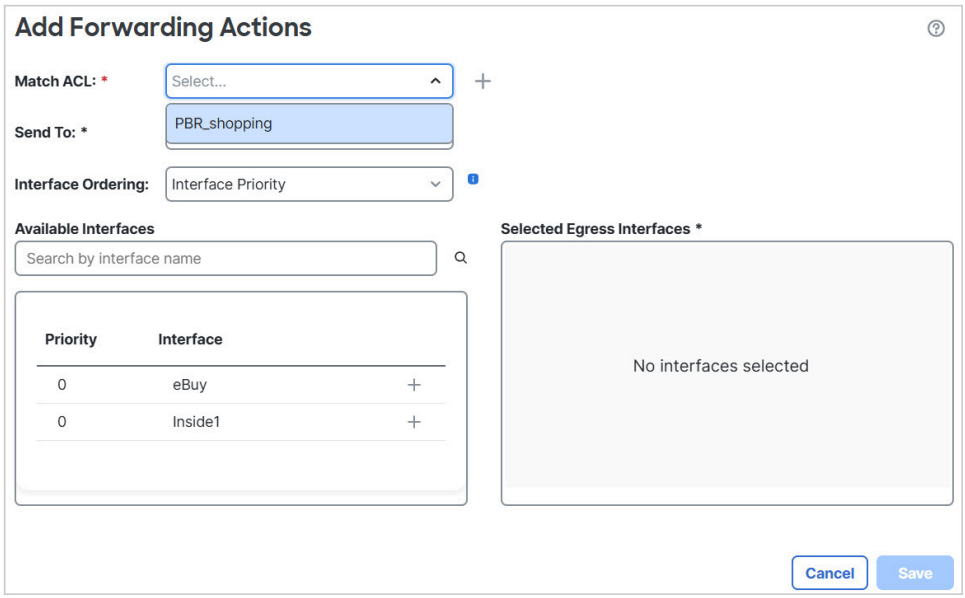
ステップ 7 表示される **[ポリシー ベース ルーティング）]** ページで、**[追加（Add）]**をクリックします。

ステップ 8 [ポリシー ベース ルートの追加（Add Policy Based Route）] ダイアログ ボックスで、[入力インターフェイス（Ingress Interface）] ドロップダウンリストから [内部 1（Inside 1）] を選択します。



ステップ 9 **[ACLの照合（Match ACL）]** ドロップダウン リストから、作成した ACL を選択します。この例では、 *PBR_customing* です。

（注）
Firewall Threat Defenseでは、 ACLのアプリケーション グループがネットワーク サービス グループとして構成されます。このため、カスタム アプリケーションに **NSG**をタグ付けします。

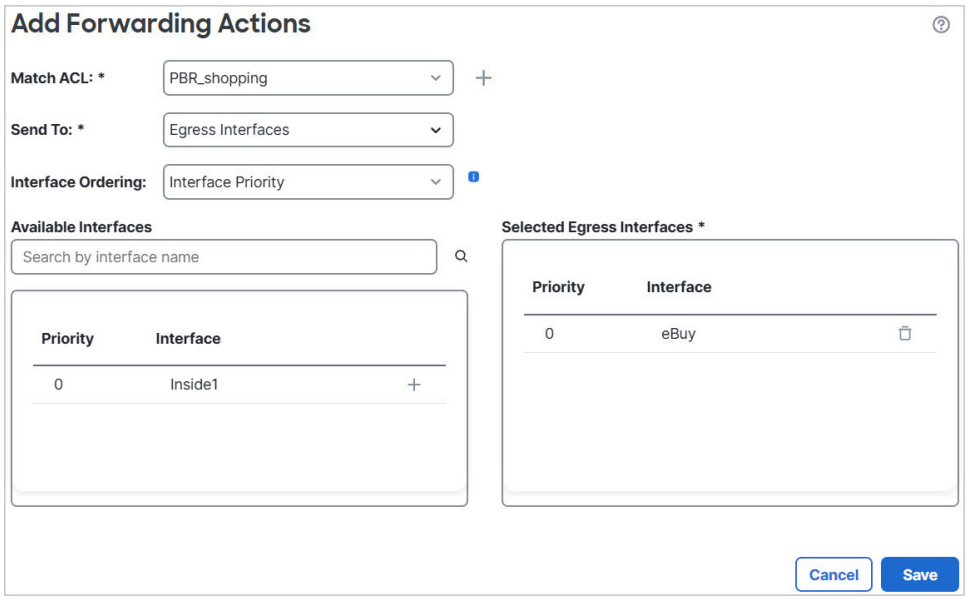


ステップ 10 出力インターフェイスを指定します。

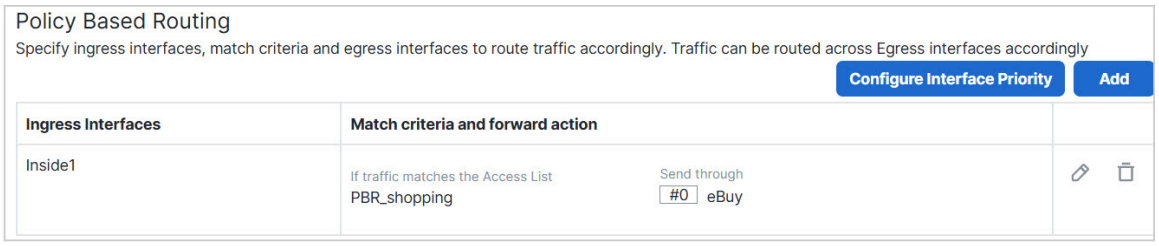
a) **[宛先（Send to）]** ドロップダウン リストから **[出力インターフェイス（Egress Interfaces）]** を選択します。

b) **[インターフェイスの順序付け（Interface Ordering）]** ドロップダウン リストから適切な順序を選択します。

c) **[利用可能なインターフェイス（Available Interfaces）]**で、対応するインターフェイスの横にある（＋）、つまり *eBuy* をクリックします。



d) **[保存（Save）]** をクリックします。



ステップ 11 [保存（Save）]、[展開（Deploy）] の順にクリックします。

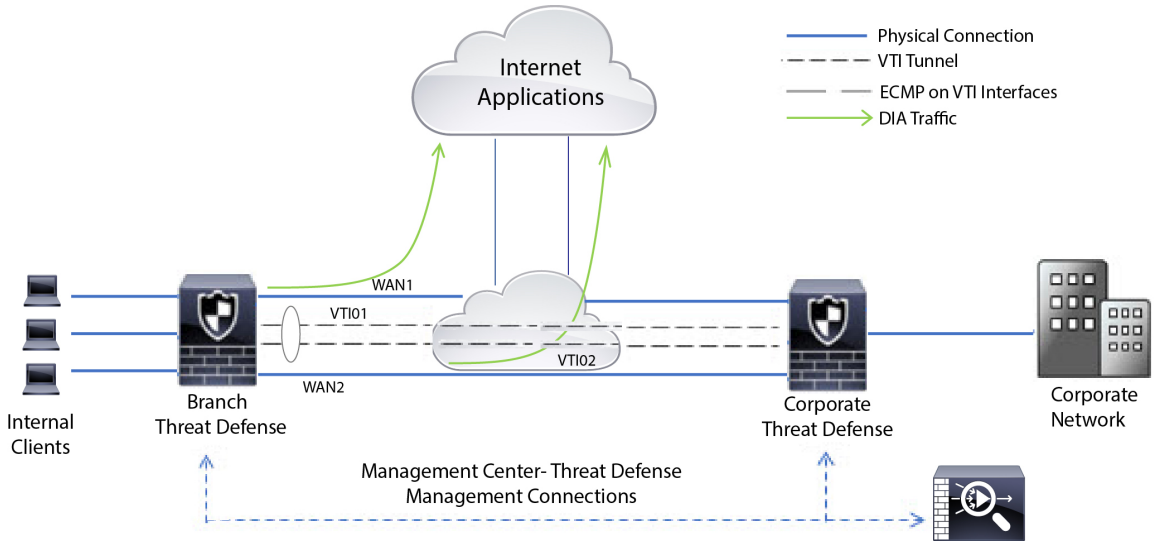
ポリシーベースルーティングの設定例

すべてのブランチ ネットワーク トラフィックが企業ネットワークのルートベースの VPN を通過し、必要に応じてエクストラネットに分岐する一般的な企業ネットワークシナリオを考えてください。企業ネットワークを介して日常業務向けの Web ベース アプリケーションにアクセスすると、ネットワークのサイズとメンテナンス コストが増大する場合があります。この例は、ダイレクト インターネット アクセスの PBR 設定手順を示しています。

次の図は、企業ネットワークのトポロジを示しています。ブランチネットワークは、ルートベースの VPN を介して企業ネットワークに接続されています。従来、企業 Firewall Threat Defense は、ブランチオフィスの内部トラフィックと外部トラフィックの両方を処理するように設定されていました。PBR ポリシーにより、ブランチ Firewall Threat Defense は、特定のトラフィックを仮想トンネルではなく WAN ネットワークにルーティングするポリシーで設定されます。残りのトラフィックは、通常どおり、ルートベースの VPN を通過します。

この例は、ロードバランシングを実現するための ECMP ゾーンを使用した WAN および VTI インターフェイスの設定方法も示しています。

図 *1 : Firewall Management Center* のブランチ *Firewall Threat Defense* でのポリシーベースルーティングの設定



始める前に

この例では、Firewall Management Center のブランチ Firewall Threat Defense の WAN および VTI インターフェイスがすでに設定されていることを前提としています。

手順

ステップ 1 ブランチ Firewall Threat Defense のポリシーベースルーティングを設定し、入力インターフェイスを選択します。

a) **Devices** > **Device Management** を選択し、Firewall Threat Defense デバイスを編集します。

b) **[ルーティング（Routing）]** > **[ポリシーベースルーティング（Policy Based Routing）]** を選択し、[ポリシーベースルーティング（Policy Based Routing）] ページで、[追加（Add）] をクリックします。

c) [ポリシーベースルートの追加（Add Policy Based Route）] ダイアログボックスで、[入力インターフェイス（Ingress Interface）] ドロップダウンリストからインターフェイス（*[内部1（Inside 1）]* と *[内部2（Inside 2）]* など）を選択します。

ステップ 2 一致基準を指定します。

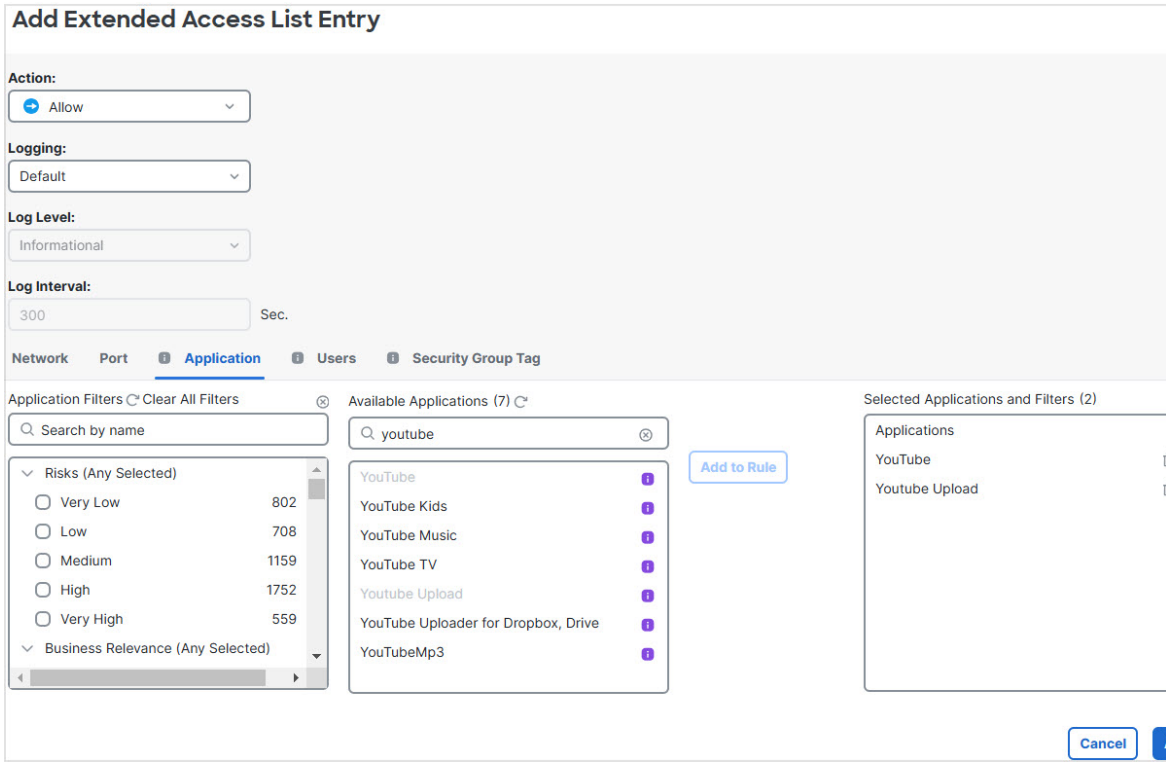
a) [追加（Add）] をクリックします。

b) 一致基準を定義するには、**Add** (＋) ボタンをクリックします。

c) [新しい拡張アクセスリストオブジェクト（New Extended Access List Object）] で、ACL の名前（たとえば、*DIA-FTD-Branch*）を入力し、[追加（Add）] をクリックします。

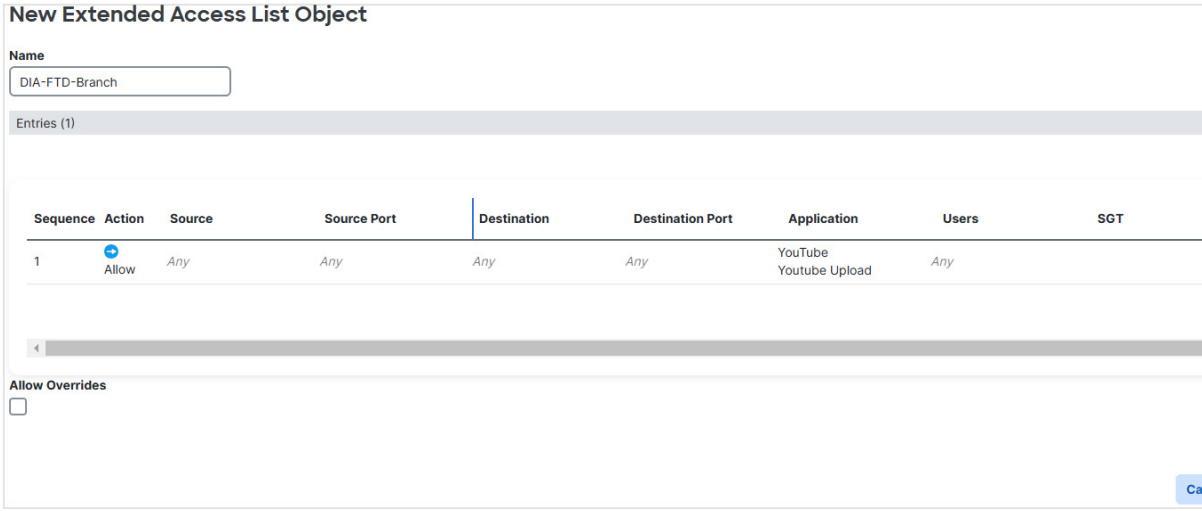
d) [拡張アクセスリストエントリの追加（Add Extended Access List Entry）] ダイアログボックスで、[アプリケーション（Application）] タブから必要な Web ベースのアプリケーションを選択します。

図 2 : [Applications] タブ



Firewall Threat Defense では、ACL のアプリケーショングループがネットワーク サービス グループとして設定され、各アプリケーションがネットワーク サービス オブジェクトとして設定されます。

図 *3*：拡張 *ACL*



e) [保存（Save）] をクリックします。

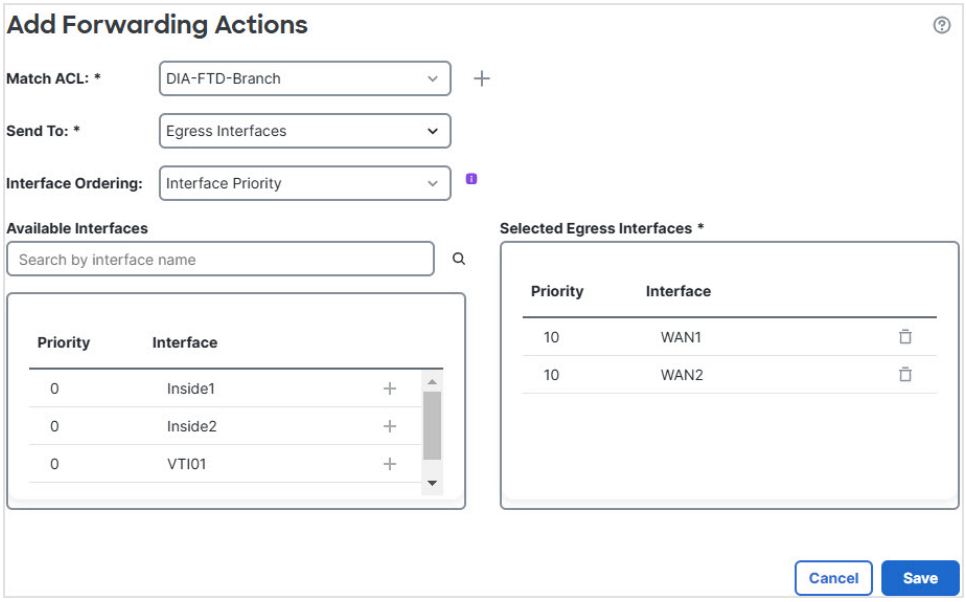
f) [ACLの照合（Match ACL）] ドロップダウンリストから [DIA-FTD-Branch] を選択します。

ステップ 3 出力インターフェイスを指定します。

a) **[宛先（Send To）]** および **[インターフェイスの順序付け（Interface Ordering）]** ドロップダウン リストから、[出力インターフェイス（Egress Interfaces）] と [インターフェイスの優先順位（Interface Priority）] をそれぞれ選択します。

b) [使用可能なインターフェイス（Available Interfaces）] で、それぞれのインターフェイス名の ⊕ ボタンをクリックして、[WAN1] と [WAN2] を追加します。

図 *4*：ポリシーベース ルーティングの設定



c) **[保存（Save）]** をクリックします。

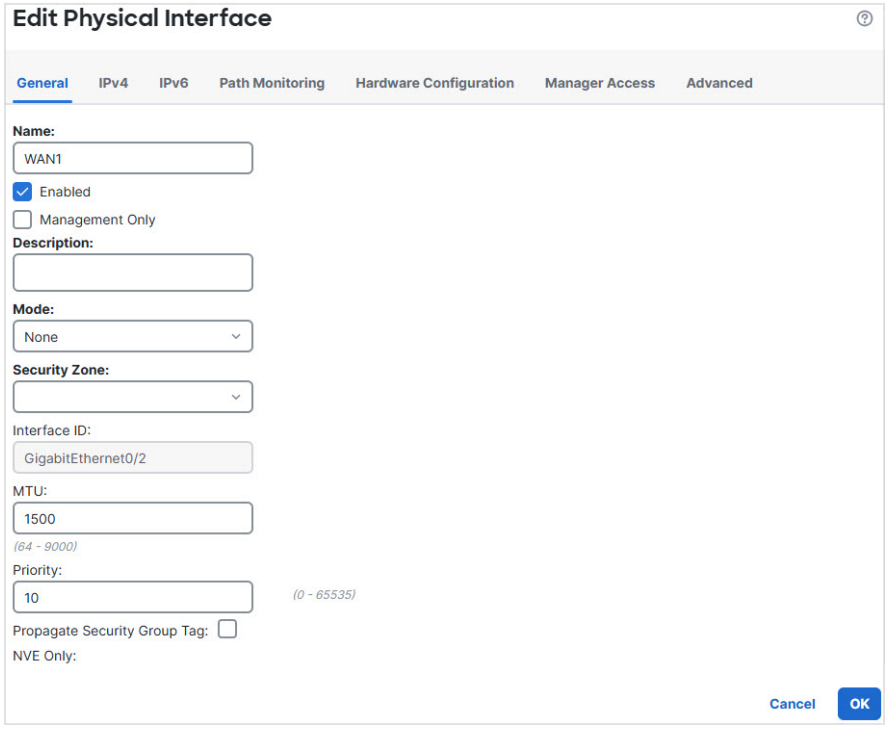
ステップ 4 インターフェイスの優先順位の設定：

[物理インターフェイスの編集（Edit Physical Interface）]ページまたは[ポリシーベースルーティング（Policy Based Routing）]ページ（[インターフェイスの優先順位の設定（Configure Interface Priority）]）で、インターフェイスの優先順位の値を設定できます。この例では、[物理インターフェイスの編集（Edit Physical Interface）] のメソッドが示されています。

a) **Devices** > **Device Management**を選択し、ブランチ Firewall Threat Defenseを編集します。

b) インターフェイスの優先順位を設定します。インターフェイスに対して [編集（Edit）] をクリックし、優先順位の値を入力します。

図 *5*：インターフェイスの優先順位の設定



c) [OK] をクリックし、[保存（Save）] をクリックして保存します。

ステップ 5 ロードバランシング用の ECMP ゾーンを作成します。

a) [ルーティング（Routing）] ページで、[ECMP] をクリックします。

b) インターフェイスを ECMP ゾーンに関連付けるには、[追加（Add）] をクリックします。

c) [WAN1] と [WAN 2] を選択し、ECMP ゾーン（*ECMP-WAN*）を作成します。同様に、[VTI01] と [VTI02] を追加し、ECMP ゾーン（*ECMP-VTI*）を作成します。

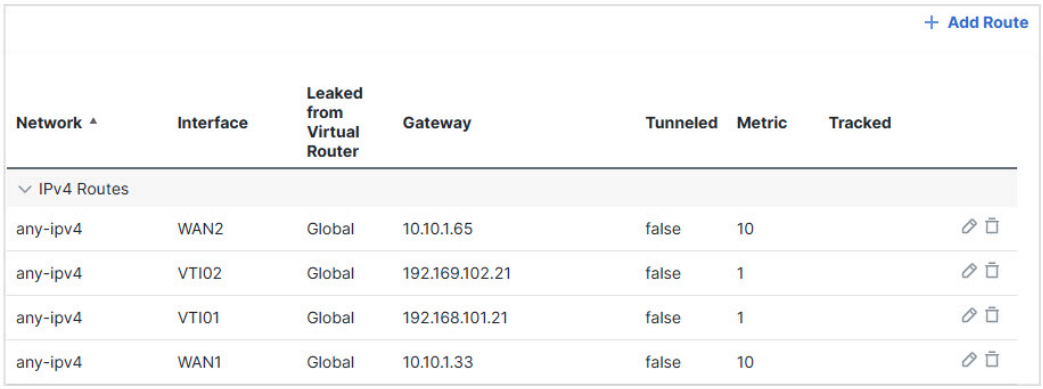
図 *6*: インターフェイスと *ECMP* ゾーンの関連付け

ステップ 6 ロードバランシング用のゾーンインターフェイスのスタティックルートを設定します。

a) [ルーティング（Routing）] ページで、[スタティックルート（Static Route）] をクリックします。

b) [追加（Add）] をクリックし、*WAN1*、*WAN2*、*VTI01*、および *VTI02* のスタティックルートを指定します。必ず、同じ ECMP ゾーンに属するインターフェイスには同じメトリック値を指定してください（手順 5）。

図 *7*: *ECMP* ゾーンインターフェイスのスタティックルートの設定



（注）
ゾーンインターフェイスの宛先アドレスとメトリックは同じであるが、ゲートウェイアドレスが異なることを確認してください。

ステップ 7 インターネットへのセキュアなトラフィック フローが確保されるように、ブランチ Firewall Threat Defense の WAN オブジェクトで信頼できる DNS を設定します。

a) **Devices** > **Platform Settings** を選択し、ブランチ Firewall Threat Defense で DNS ポリシーを作成します。

b) 信頼できる DNS を指定するには、[編集（Edit）] をクリックしてポリシーを編集し、[DNS] をクリックします。

c) WAN オブジェクトが使用する DNS 解決用の DNS サーバーを指定するには、[DNS 設定（DNS Settings）] タブで、DNS サーバーグループの詳細情報を指定し、インターフェイスオブジェクトから WAN を選択します。

d) [信頼できるDNSサーバー（Trusted DNS Servers）] タブを使用して、DNS 解決のために信頼できる特定の DNS サーバーを指定します。

ステップ 8 **[保存（Save）]** をクリックして、**[展開（Deploy）]** をクリックします。

ネットワーク *INSIDE1* または *INSIDE2* 内のブランチからの *YouTube* 関連のアクセス要求は、*DIA-FTD-Branch* ACL と一致するため、*WAN1* または *WAN2* にルーティングされます。*google.com* などの他のすべての要求は、サイト間 VPN 設定で指定されているように、*VTI01* または *VTI02* を介してルーティングされます。

ECMP が設定されていると、ネットワークトラフィックはシームレスに分散されます。

パスモニタリングを使用した PBR の設定例

この例では、柔軟なメトリックによる次のアプリケーションのパスモニタリングを備えた PBR の構成方法について説明します。

- ジッタのある、音声やビデオが不安定になる可能性があるアプリケーション（Webex Meetings など）。
- RTT のある、クラウドベースのアプリケーション（Office365 など）。
- パケット損失のある、ネットワーク ベースのアクセス制御（特定の送信元と接続先を使用）。

始める前に

1. この例は、PBR の基本的な設定手順を理解していることを前提としています。
2. 論理名による入力インターフェイスと出力インターフェイスの設定が完了しています。この例では、入力インターフェイスの名前は「Inside1」、出力インターフェイスの名前は「ISP01」、「ISP02」、および「ISP03」です。

手順

ステップ 1 インターフェイス ISP01、ISP02、および ISP03 でのパスモニタリングの設定：

出力インターフェイスでのメトリック収集については、それらのインターフェイスでパスモニタリングを有効にして設定する必要があります。

a) **Devices** > **Device Management**を選択し、Firewall Threat Defense を編集します。
b) [インターフェイス（Interfaces）] タブで、インターフェイス（この例では「ISP01」）を編集します。
c) [パスモニタリング（Path Monitoring）] タブをクリックし、[パスモニタリングの有効化（Enable Path Monitoring）] チェックボックスをオンにしてから、モニタリングタイプを指定します（パスモニタリングの設定 （8 ページ）を参照）。
d) [OK] をクリックし、[保存（Save）] をクリックして保存します。
e) これらの手順を繰り返し、*ISP02* と *ISP03* のパス モニタリングの設定を構成します。

ステップ 2 組織の Firewall Threat Defense に含まれるブランチのポリシーベースルーティングを設定し、入力インターフェイスを選択します。

a) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

b) **[ルーティング（Routing）]** > **[ポリシーベースルーティング（Policy Based Routing）]** を選択し、[ポリシーベースルーティング（Policy Based Routing）] ページで、[追加（Add）] をクリックします。

c) [ポリシーベースルートの追加（Add Policy Based Route）] ダイアログボックスで、[入力インターフェイス（Ingress Interface）] ドロップダウンリストから [内部 1（Inside 1）] を選択します。

ステップ 3 一致基準を指定します。

a) [追加（Add）] をクリックします。

b) 一致基準を定義するには、**Add** (＋) ボタンをクリックします。

c) [新しい拡張アクセスリストオブジェクト（New Extended Access List Object）] で、ACL の名前（たとえば、*PBR-WebEx*）を入力し、[追加（Add）] をクリックします。

d) **[拡張アクセス リスト エントリの追加（Add Extended Access List Entry）]** ダイアログ ボックスで、**[アプリケーション（Application）]** タブから必要な Web ベースのアプリケーション（WebEx Meetings など）を選択します。

メモ
Firewall Threat Defense では、ACL のアプリケーショングループがネットワーク サービス グループとして設定され、各アプリケーションがネットワーク サービス オブジェクトとして設定されます。

e) [保存（Save）] をクリックします。

f) [ACLの照合（Match ACL）] ドロップダウンリストから [PBR-WebEx] を選択します。

ステップ 4 出力インターフェイスを指定します。

a) [宛先（Send to）] ドロップダウンリストから [出力インターフェイス（Egress Interfaces）] を選択します。

b) [インターフェイスの順序付け（Interface Ordering）] ドロップダウンリストから [最小ジッターによる（By Minimal Jitter）] を選択します。

c) [使用可能なインターフェイス（Available Interfaces）] で、それぞれのインターフェイス名の **Right Arrow** (＞) ボタンをクリックして、[ISP01]、[ISP02]、および [ISP03] を追加します。

d) [保存（Save）] をクリックします。

ステップ 5 手順 2 と手順 3 を繰り返して、*Inside1* インターフェイスに、Office365 およびネットワークベースアクセス制御トラフィックをルーティングする PBR を作成します。

a) 一致基準オブジェクト（*PBR-Office365* など）を作成し、[アプリケーション（Application）] タブから Office365 アプリケーションを選択します。

b) [インターフェイスの順序付け（Interface Ordering）] ドロップダウンリストから、[最短ラウンドトリップ時間による（By Minimal Round Trip Time）] を選択します。

c) 出力インターフェイス「ISP01」、「ISP02」、および「ISP03」を指定し、[保存] をクリックします。
d) ここで、一致基準オブジェクト（*PBR-networks* など）を作成し、[ネットワーク（Network）] タブで送信元および宛先インターフェイスを指定します。
e) [インターフェイスの順序付け（Interface Ordering）] ドロップダウンリストから [最小ラウンドトリップ時間による（By Minimal Packet Loss）] を選択します。
f) 出力インターフェイス「ISP01」、「ISP02」、および「ISP03」を指定し、[保存] をクリックします。

ステップ 6 **[保存（Save）]** をクリックして、**[展開（Deploy）]** をクリックします。

ステップ 7 パスモニタリングメトリックを表示するには、**[デバイス（Devices）]**>**[デバイス管理（Device Management）]** を選択し、**More** (⋮) から [ヘルスモニター（Health Monitor）] をクリックします。デバイスのインターフェイスのメトリックに関する詳細情報を表示するには、パスメトリックダッシュボードを追加する必要があります。詳細については、パス監視ダッシュボードの追加 （9 ページ）を参照してください。

Webex、Office365、およびネットワークベース ACL トラフィックは、*ISP01*、*ISP02*、および *ISP03* で収集されたメトリック値から得られる最適ルートを介して転送されます。

PBR のモニタリングに役立つ CLI

Firewall Threat Defense デバイスの CLI から、このトピックで説明されているモニタリングコマンドを実行します。

インターフェイス構成

デバイスのインターフェイス構成を表示するには、`show run interface` コマンドを実行します。

```
> show run interface
!
interface Ethernet1/1
 description Outside ispl handoff
 nameif outside1
 security-level 0
 zone-member ECMP-WAN
 ip address dhcp setroute
 policy-route cost 10
 policy-route path-monitoring 8.8.8.8
 policy-route path-monitoring object-group network-service FMC_NSG_4295470581 policy-route
 path-monitoring object-group network-service FMC_NSG_4295470600
!
interface Ethernet1/2
 description Outside isp2 handoff
 nameif outside2
 security-level 0
 zone-member ECMP-WAN
 ip address 192.133.243.240 255.255.255.192
 policy-route cost 20
 policy-route path-monitoring 8.8.8.8
 policy-route path-monitoring object-group network-service FMC_NSG_4295470581 policy-route
```

```
 path-monitoring object-group network-service FMC_NSG_4295470600
!
```

DNS 構成

アプリケーションベースのルーティングでは、信頼できる DNS サーバーのみを使用してドメインを解決します。デバイスの DNS 設定を表示するには、`show run dns` コマンドを実行します。

```
> show run dns
DNS server-group DefaultDNS
dns trusted-source 10.100.0.5
dns trusted-source 10.200.0.5
```

ルート マップ設定を確認します。

デバイスに PBR を設定すると、Management Centerはルート マップを自動生成し、指定した入力インターフェイスに適用します。デバイスのルートマップを表示するには、`show run route-map` コマンドを実行します。

```
> show run route-map
!
route-map FMC_VPN_CONNECTED_DIST_RMAP_1000 permit 10
 match interface inside-employee
 set community 1000
!
route-map FMC GENERATED PBR 1729024850865 permit 5
 match ip address Cloud-storage-apps-acl
  set adaptive-intertace cost outside1 outside2

!
route-map FMC_GENERATED PBR 1729024850865 permit 10
match ip address Social-media-apps-acl
set adaptive-interface rtt outsidel outside2

!
route-map FMC GENERATED PBR 1729024850865 permit 15
match ip address Conferencing-apps-acl
set adaptive-interface jitter outside1 outside2

!
route-map FMC_GENERATED_PBR_1729024850865 permit 20
match ip address Corp-internal-apps-acl
set adaptive-interface cost outsidel_static_vti_1 outside2_static_vti_4
```

アクセス リストとネットワーク サービス グループの設定

入力インターフェイスに適用されるルート マップは、拡張アクセス コントロール リストを参照できます。PBR のアクセスリストの詳細を表示するには、`show run access list <access list_name>` コマンドを実行します。

```
> show run access-list Cloud-storage-apps-acl
access-list Cloud-storage-apps-acl extended permit ip any object-group-network-service
FMC_NSG_4295470562
```

ネットワークサービス オブジェクトとオブジェクト グループは、拡張アクセス コントロール リストで設定され、ポリシーベースのルーティング ルート マップとアクセス コントロール グループで参照されます。NSG 構成を表示するには、`show object-group network-service`

<network-service-groups-name> コマンドを実行します。*network-service-groups-name* は、アクセスリストに対する上記の show コマンドから派生したものです。

```
> show object-group network-service FMC_NSG_4295470562
 object-group network-servire FMC_NSG_4295470562 (id=@xfdff0000)
 network-service-member "Box" dynamic
 description File storage and transfer site.
 app-id 1326
 domain box.com (bid=436735707) ip (hitcnt=0)
 domain boxcloud.com (bid=436924171) ip (hitcnt=0)
 domain box.net (bid=437080553) ip (hitcnt=0)
 domain box.org (bid=437174273) ip (hitcnt=0)
 domain boxcdn.net (bid=437272231) ip (hitcnt=0)
 domain boxrelay.com (bid=437481703) ip (hitcnt=0)
 domain boxenterprise.net (bid=437626005) ip {hitcnt=0)
 domain boxinvestorrelations.com (bid=437672765) ip (hitcnt=0)
 domain segment-box.com (bid=437886771) ip (hitcnt=0)
 domain box-corp.com (bid=437924995) ip (hitcnt=0)
 domain boxcn.net (bid=438072833) ip (hitcnt=0)
network-service-member "Dropbox" dynamic
 description Cloud based tile storage.
 app-id 125
 domain dropbox.com (bid=24259639) ip (hitcnt=0)
 domain cfl.dropboxstatic.com (bid=24495525) ip (hitcnt=0)
 domain dl.dropboxusercontent.com (bid=24596237) ip (hitcnt=0)
 domain dropboxapi.com (bid=24694467) ip (hitcnt=0)
 domain dropboxbusiness.com (bid=24859859) ip (hitcnt=0)
 domain dropboxcaptcha.com (bid=25008145) ip {hitcnt=0)
 domain dropbox-dns.com (bid=25087753) ip (hitcnt=0)
 domain dropboxer.net (bid=25236751) ip (hitcnt=0)
 domain dropboxusercontent.com (bid=25324335) ip (hitcnt=0)
 domain getdropbox.com (bid=25437501) ip (hitcnt=0)
 domain cloudon.com (bid=25580229) ip (hitcnt=0)
```

パス モニタリングの設定

出力インターフェイスで収集されたパス モニタリング メトリックを表示するには、show path-monitor コマンドを実行します。

```
> show path-monitor
Interface: outside2 (Ethernetl/2)
Remote peer: 8.8.8.8
    Remote peer reachable: Yes
    RTT average: 9138 microsecondes) Jitter: 1093 microsecond(s)
    Packet loss: 0% MOS: 4.39
    Last updated: 12 second(s) ago
Interface: outside2 (Ethernetl/2)
Remote NSG: FMC_NSG_4295470581
    Network Service: Facebook Domain name: fbsbx.com Remote peer reachable: Yes
    RTT average: 17460 microsecond(s) Jitter: 911 microseconde)
    Packet loss: 0%
    MOS: 4.39
    Last updated: 12 second(s) ago

    Network Service: Facebook
    Domain name: facebook.net
    Remote peer reachable: Yes
    RTT average: 17444 microsecondes)
    Jitter: 836 microsecondes)
    Packet loss: 0%
    MOS: 4.39
    Last updated: 12 second(s) ago
```

```
    Network Service: Instagram
    Domain name: instagram.com Remote peer reachable: Yes
    RTT average: 17576 microsecondes)
    Jitter: 429 microsecondes)
    Packet loss: 0%
    MOS: 4.39
    Last updated: 12 secondes) ago

Interface: outside2 (Ethernetl/2)
Remote NSG: FMC_NSG_4295470600
    Network Service: WebEx
    Domain name: webex.com Remote peer reachable: Yes RTT average: 18537 microsecond(s)
 Jitter: 318 microseconde)
    Packet loss: 0%
    MOS: 4.39
    Last updated: 12 second(s) ago
    Network Service: Zoom Domain name: zoom.com Remote peer reachable: Yes
    RTT average: 98196 microsecond(s) Jitter: 4120 microseconde)
    Packet loss: 0%
    MOS: 4.34
    Last updated: 12 second(s) ago
```

PBRのトラブルシューティング

パケットがドロップされた場合に PBR 設定をデバッグするには、次の手順を実行します。

1. 該当するテーブルにおいて show route コマンドまたは show ipv6 route コマンドを使用して、再帰解決に不可欠なルートがすべて存在することを確認します。 PBR に参加しているインターフェイスのルート マップが正しいルートで更新されない限り、 PBR は意図したとおりに動作しません。

2. `show running-config interface` コマンドは、パス モニタリングが ICMP パケットを送信してメトリックをモニターするために使用するリモートアドレスを表示します。

```
interface GigabitEthernet0/0
nameif outside_0
security-level 0
zone-member ecmp-zone
ip address 20.0.0.3 255.255.255.0 -> This is egress interface ”show running-config”
 output, the monitored address and cost metric value is determined in this output.
policy-route cost 1
policy-route path-monitoring
20.0.0.4
!
int GigabitEthernet 0/3
!
interface GigabitEthernet0/3
nameif outside_3
security-level 0
ip address 11.1.1.2 255.255.255.0 -> This is ingress interface ”show running-config”
 output, the specific route-map will be used by PBR to determine the next route.
policy-route route-map rtt-tes
```

3. `show path-monitoring` および `show run route-map` の出力でパケット損失を調べます。

```
ciscoasa(config)# show path-monitoring
Interface: outside_0  -> The remote address used for ICMP monitoring
Remote peer: 20.0.0.4
Version: 6223
```

```
Remote peer reachable: Yes -> If this value turns ”No”, then the ICMPv4/v6 packet is
 not reaching the required remote address.
RTT average: 1920 microsecond(s)
Jitter: 394 microsecond(s)
Packet loss: 0%
MOS: 4.40
Last updated: 17 second(s) ago -> The data should be updated by path monitoring after
 every 30 seconds. The 'show route-map' would show the
updated metric values.
Interface: outside_2
Remote peer: 40.0.0.4
Version: 6223
Remote peer reachable: Yes
RTT average: 1935 microsecond(s)
Jitter: 433 microsecond(s)
Packet loss: 0%
MOS: 4.40
Last updated: 17 second(s) ago
```

```
ciscoasa(config)# show route-map
route-map rtt-test, permit, sequence 10
Match clauses:
Set clauses:
adaptive-interface rtt outside_0 (1920) outside_2 (1935) outside_1 (1971) -> Displays
 the metric type (rtt) that is used by the policy route to select the adequate
interface to send the packet. The interface list where cost of each interface is
given. As the metric type is “rtt” and considering the minimum rtt value, the
“outside_0” interface route will be selected by PBR.
route-map mos-test, permit, sequence 10
Match clauses:
Set clauses:
adaptive-interface mos outside_0 (378) outside_1 (390) outside_2 (440) - > As the
metric type is “mos”, considering the maximum value of mos, the “outside_2” interface
 will be selected by PBR.
```

メトリック タイプ（lost、rtt、ジッター、コスト）によって、ルーティングの最小メトリック値を持つインターフェイスを選択する必要があります。

メトリック タイプ「mos」は、ルーティングの最大メトリック値を持つインターフェイスを選択する必要があります。

4. packet-tracer コマンドを活用、 PBRで定義されたメトリックタイプに基づいてインターフェイス選択を検証します。

```
packet-tracer input <interface> icmp <src ip address> 8 0 <dst ip
address> detailed
Phase: 3
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Elapsed time: 60656 ns
Config:
route-map rtt-test permit 10
match ip address allow_101_1_1_2
set adaptive-interface rtt outside_0 outside_2
Additional Information:
Matched route-map rtt-test, sequence 10, permit
Found next-hop 40.0.0.4 using egress ifc outside_2 -> PBR selects the adequate
interface from adaptiveinterface list given in “rtt-test” route-map.
```

5. debug policy-route コマンドと同様に、 packet-tracer コマンドを使用することもできます。

- PBR が正常にルートを選択した場合、パケットトレーサの出力は次のようになります。

```
pbr: policy based route lookup called for 101.1.1.1/0 to 101.1.1.2/0 proto 1
sub_proto 8 received on
interface outside_3, NSGs, nsg_id=none
pbr: First matching rule from ACL(-1)
pbr: route map rtt-test, sequence 10, permit; proceed with policy routing
pbr: policy based routing applied; egress_ifc = outside_2 : next_hop = 20.0.0.4
```

- PBR が適切なルートを見つけることができない場合、通常のルート ルックアップにフォールバックします。パケットトレーサの出力は次のようになります。

```
pbr: policy based route lookup called for 100.1.1.1/0 to 100.1.1.2/0 proto 1
sub_proto 8
received on interface outside_3, NSGs, nsg_id=none
pbr: First matching rule from ACL(-1)
pbr: route map mos-test, sequence 10, permit; proceed with policy routing
pbr: no route to 100.1.1.2 on adaptive-interface outside_2
pbr: no route to 100.1.1.2 on adaptive-interface outside_1
pbr: no route to 100.1.1.2 on adaptive-interface outside_0
pbr: policy based routing could not be applied; proceeding with normal route
lookup
```

- モニター対象のリモートアドレスがダウンし、パスモニタリングによってそのアドレスの **リモートピア到達可能** が **No** とマークされると、 PBR は適応型インターフェイスリストからインターフェイスを除外するログを表示します。

```
pbr: policy based route lookup called for 100.1.1.1/0 to 101.1.1.2/0 proto 1
sub_proto 8 received on
interface outside_3, NSGs, nsg_id=none
pbr: First matching rule from ACL(-1)
pbr: route map rtt-test, sequence 10, permit; proceed with policy routing
pbr: Path Monitoring Ifc Down : adaptive-interface outside_1 Excluded from PBR
routing
pbr: policy based routing applied; egress_ifc = outside_2 : next_hop = 40.0.0.4
```

（注） インターフェイスは、パスモニタリングモジュールで到達可能であると報告されると、適応型 PBR ルーティングの対象になります。

ポリシーベース ルーティングの履歴

表 *1*: 履歴テーブル

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
PBR でサポートされるカスタム アプリケーション ディテクタ	7.7	7.7	カスタム アプリケーション ドメインを使用して PBR ポリシーを作成できるようになりました。ユーザー定義のドメインはカスタムディテクタ パターンとして作成され、アプリケーション ベースの PBR ポリシーの拡張 ACL で使用できます。 新規/変更された画面：新規または変更された画面は追加されませんでした。
ID および SGT ベースの PBR ポリシー	7.4.0	7.4.0	ユーザーとユーザーグループ、および PBR ポリシーの SGT に基づいてネットワークトラフィックを分類できるようになりました。PBR ポリシーの拡張 ACL を定義するときに、ID および SGT オブジェクトを選択できます。 新しい/変更された画面：ポリシーベースルーティングのポリシーを設定するための拡張アクセスリストオブジェクトに追加された新しいタブ：**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** > **[アクセス制御リスト（Access Control Lists）]** > **[拡張の追加（Add Extended）]**ページ、[ユーザー（Users）] および [セキュリティグループ（Security Group）] タグ。
HTTP ベースのパスモニタリング	7.4.0	7.2.0	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評価指標（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。インターフェイスの HTTP ベースのアプリケーション モニタリング オプションは、デフォルトで有効になっています。モニタリング対象アプリケーション、パスを決定するための目的のメトリックタイプを含む一致 ACL を使用して、PBR ポリシーを設定できます。 新規/変更された画面：パスモニタリングを有効にするための [インターフェイス（Interfaces）] ページの新しいオプション：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[インターフェイスの編集（Edit Interfaces）]** > **[パスモニタリング（Path Monitoring）]** > **[HTTPベースのアプリケーションモニタリングの有効化（Enable HTTP based Application Monitoring）]**チェックボックス。

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
デュアル WAN/ISP Threat Defense 管理のサポート	7.3.0	7.3.0	デュアル WAN 対応の脅威防御では、単一のデータインターフェイスが Management Center と通信するように構成されました。現在、プライマリ データ インターフェイスに障害が発生した場合に通信チャネルが維持されるように、セカンダリ データ インターフェイスを構成するサポートが提供されています。Management Center は、優先順位と SLA メトリックに基づいて、SF-Tunnel トラフィックを Tapnlp（内部）インターフェイスから使用可能なデータインターフェイスの 1 つにルーティングするように PBR を自動設定します。
PBR ルートマップのネクストホップの設定	7.3.0	7.1.0	パケット転送アクションを有効にしながら、PBR ルートマップのネクストホップを設定できます。 新規/変更された画面：出力インターフェイスを設定するための [転送アクションの追加/編集（Add/Edit Forwarding Actions）] ページの新しいフィールド：**[デバイス管理（Device Management）] > [ルーティング（Routing）] > [ポリシーベースルーティング（Policy Based Routing）] > [転送アクションの追加（Add Forwarding Actions）]**ページ。
PBR とパスモニタリング	7.2.0	7.2.0	PBR ではパスモニタリングを使用して、出力インターフェイスの評価指標（RTT、ジッター、パケット損失、MOS）が収集されます。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。パスの決定に必要なメトリックを使用して PBR ポリシーを設定できます。 新規/変更された画面：パスモニタリングを有効にするための [インターフェイス（Interfaces）] ページの新しいタブ：**[デバイス（Device）] > [デバイス管理（Device Management）] > [インターフェイスの編集（Edit Interfaces）] > [パスモニタリング（Path Monitoring）]**タブ。

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
Configure policy based routing from the FMC web interface.	7.1.0	7.1.0	**Upgrade impact. Redo FlexConfigs after upgrade.** You can now configure policy based routing (PBR) from the FMC web interface. This allows you to classify network traffic based on applications and to implement direct internet access (DIA) to send traffic to the internet from a branch deployment. You can define a PBR policy and configure it on ingress interfaces, specifying match criteria and egress interfaces. Network traffic that matches the access control policy is forwarded through the egress interface based on priority or the order as configured in the policy. This feature requires Version 7.1+ on both the FMC and the device. When you upgrade the FMC to Version 7.1+, existing policy based routing FlexConfigs are removed. After you upgrade your devices to Version 7.1+, redo your policy based routing configurations in the FMC web interface. For devices that you do not upgrade to Version 7.1+, redo the FlexConfigs and configure them to deploy "every time." New/modified screens: **Devices** > **Device Management** > **Routing** > **Policy Based Routing**

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。