ポリシーベースルーティング

この章では、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 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

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。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）は、ルーティングプロトコルで提供される既存のメカニズムを拡張および補完することにより、ルーティングの制御を強化します。

PBR を使用すると、IP プレジデンスを設定できます。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とデータにアクセスするシナリオに適用できます。従来、大規模な展開では、ルートベースの VPN の暗号化されたトラフィックとして、すべてのネットワークトラフィックをハブにバックホールするトポロジが設定されます。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。これらの問題を克服するには、コストの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。

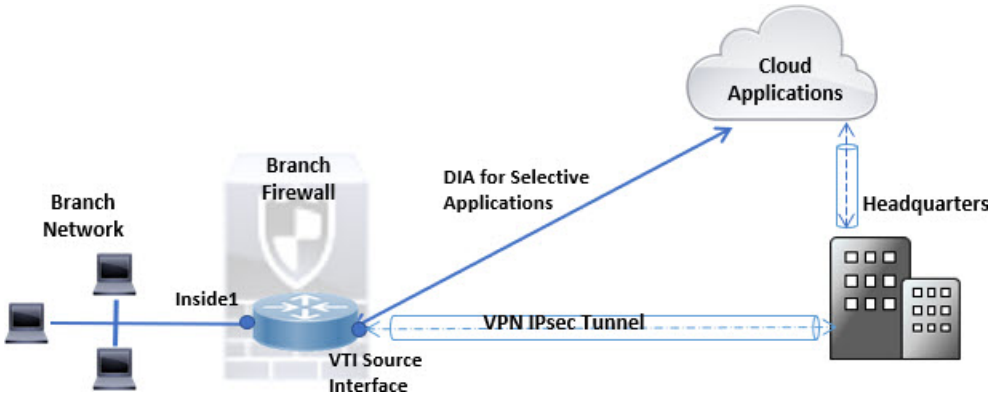
ポリシーベースルーティングを使用する理由

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いくつかのシナリオを次に示します。

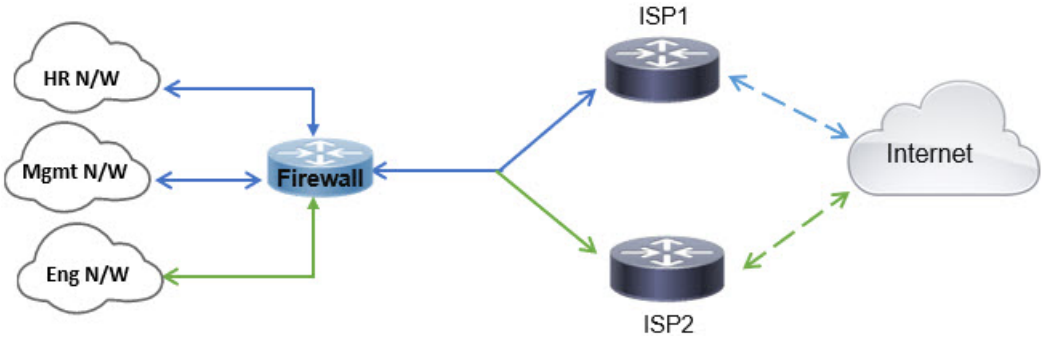
ダイレクト インターネット アクセス

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 Threat Defense はインターネットの出口ポイントで構成され、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。



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に関する注意事項と制約事項

ファイアウォール モードのガイドライン

PBR は、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。

デバイスのガイドライン

- PBR ～ 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 以降を搭載する Management Center およびデバイスでのみサポートされます。
- Management Center または 脅威に対する防御 をバージョン 7.1 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。
- アイデンティティと SGT を使用した ACL を設定した PBR がサポートされています。
- クラスタデバイスでのアプリケーション、ユーザーアイデンティティ、およびセキュリティグループタグ（SGT）ベースの PBR ポリシーの設定は、サポートされていません。

インターフェイスのガイドライン

- 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、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設定できます。
- ユーザー定義の仮想ルータでは PBR はサポートされません。
- ポリシーで定義できるのは、論理名を持つインターフェイスだけです。
- 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。
- 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。

IPv6 のサポート

PBR は IPv6 をサポートしています。

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 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。
- 信頼できる DNS サーバーを設定する必要があります。

DNS サーバーの設定の詳細については、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、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。

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、および静的トンネルインターフェイスでサポートされます。クラスタデバイスではサポートされません。
- 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 トラフィックのルーティングおよび転送に適用されます。
- バージョン 7.4 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 Secure Firewall Management Center 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

- ルートマップの設定に関する既存のすべての制限事項が、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、事前定義されたアプリケーションのリストから複数のアプリケーションを選択してアクセス制御エントリ（ACE）を形成することができます。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。
- 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。

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、インターフェイスごとに複数のリモートピアの柔軟な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のベストパスをモニタリングおよび決定するには、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。

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 （9 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。パスモニタリングでは、HTTP ベースのアプリケーションモニタリングの設定直後にモニタリングが開始されません。ドメインの DNS エントリがスヌーピングされた場合にのみモニタリングが開始されます。ドメインの解決された IP に関する情報を使用して、HTTP 要求および応答をそれぞれ送受信します。DNS が単一ドメインの複数の IP アドレスを解決する場合、最初に解決された IP アドレスが、アプリケーションのプローブとモニタリングに使用されます。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。収集されたメトリックは定期的に PBR に転送され、それにより、設定された入力インターフェイスから発生するトラフィックのルーティングおよび転送が決定されます。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、トラフィックフローは、ルーティングテーブルによって選択されたパスに従います。パスモニタリングのメトリックが利用可能になった後に到着する後続のトラフィックフローについては、PBR は、メトリックに基づいてルーティング決定を適用し、トラフィックを転送します。

（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。

アプリケーションの HTTP ベースのパスモニタリングでは、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/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、平均オピニオン評点（MOS）、インターフェイスのパケット損失などの柔軟なメトリックを使用して、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 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Threat Defense デバイス**[編集（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 **[編集（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、[Save（保存）] をクリックして設定を保存します。

ポリシーベース ルーティング ポリシーの設定

[ポリシーベースルーティング（Policy Based Routing）] ページで、入力インターフェイス、一致基準（拡張アクセスコントロールリスト）および出力インターフェイスを指定することにより、PBR ポリシーを設定できます。

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 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、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のリストと、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） ドロップダウンには、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が表示されます。

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。

（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 （11 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。

- [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 （12 ページ） に進みます

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。

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。

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 **[システム（System）] > [正常性（Health）] > [モニター（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、ダッシュボードにポートレットとして表示される 4 つのメトリックがすべて選択され、追加のメトリックフィールドも表示されます。[削除（Delete）]（） をクリックすると、いずれかのポートレットを除外できます。

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。

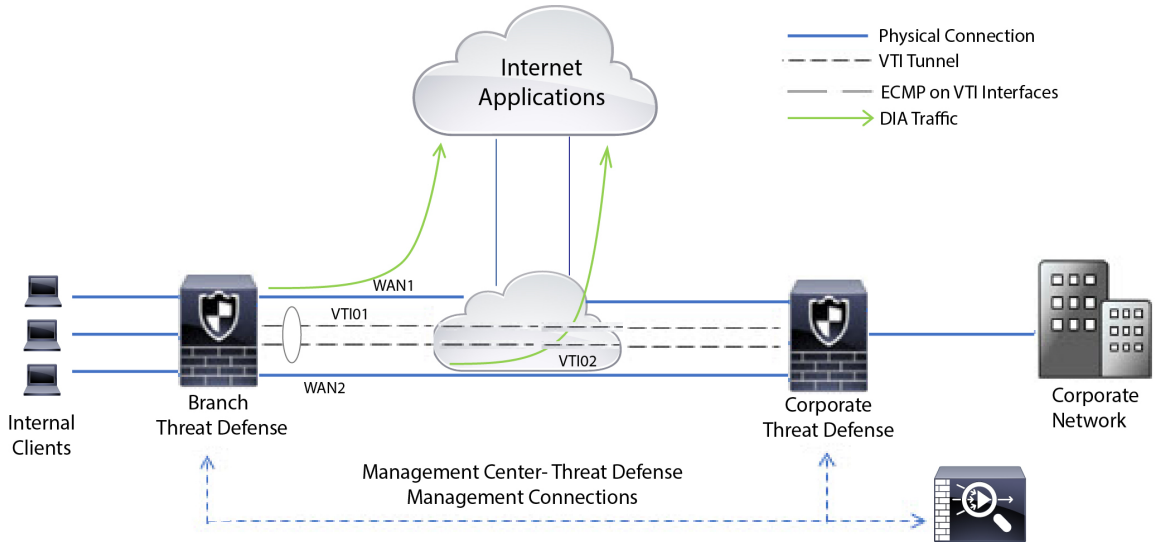
ポリシーベースルーティングの設定例

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に対処する Web ベースのアプリケーションにアクセスする場合、膨大なネットワーク拡張とメンテナンスコストが発生します。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 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 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。

この例では、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も示しています。

図 *1 : Management Center* のブランチ *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、Management Center のブランチ 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 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) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、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。

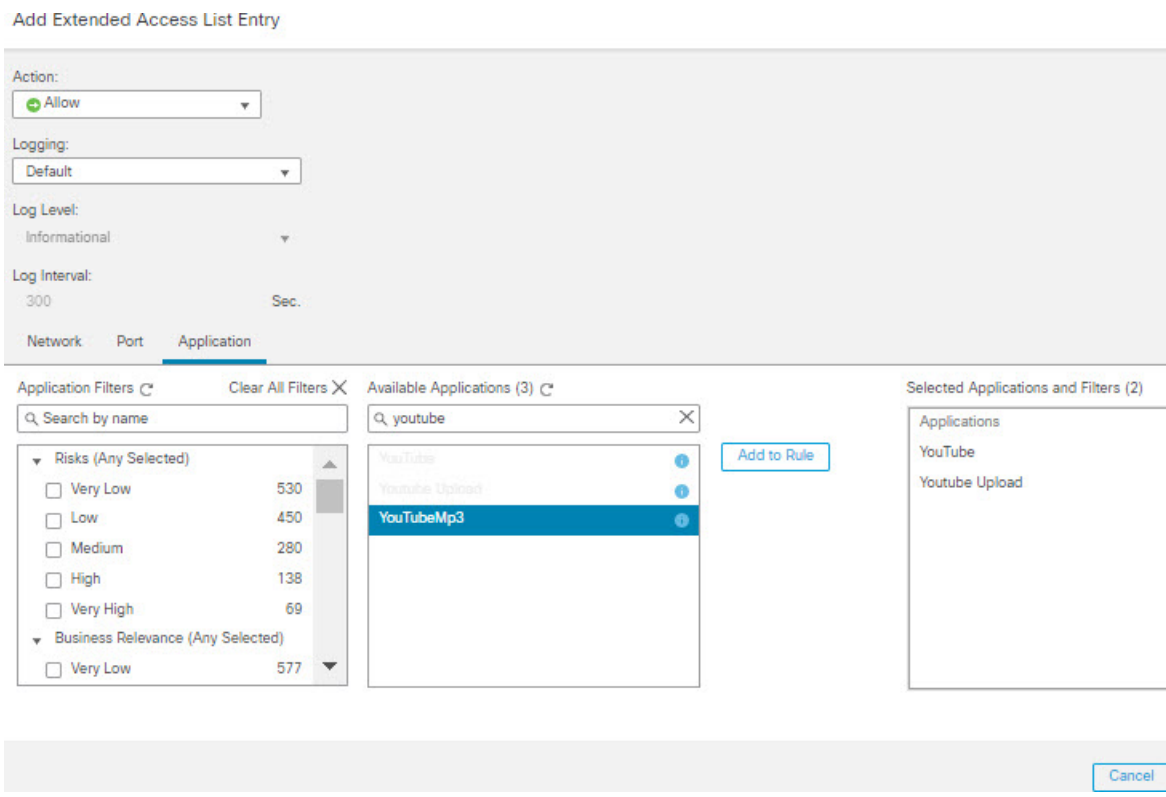
a) [追加（Add）] をクリックします。

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。

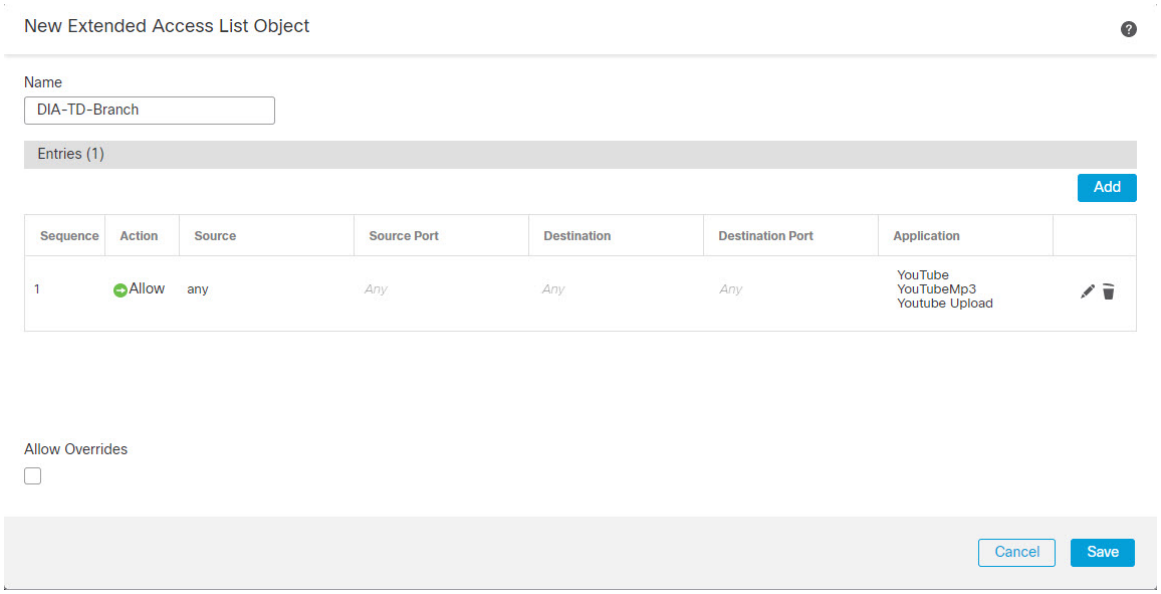
d) [拡張アクセスリストエントリの追加（Add Extended Access List Entry）] ダイアログボックスで、[アプリケーション（Application）] タブから必要な Web ベースのアプリケーションを選択します。

図 *2 : [Applications]* タブ



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*

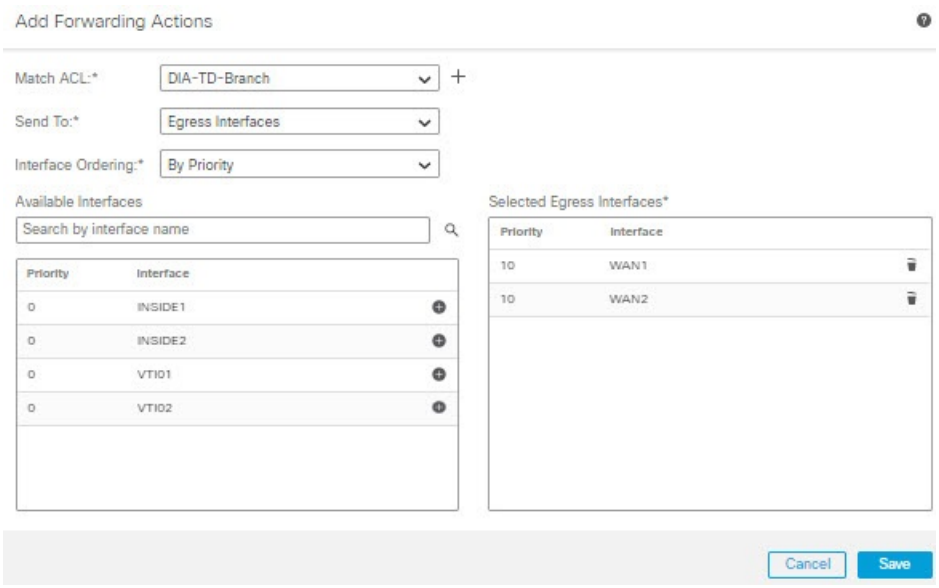


e) [保存（Save）] をクリックします。
f) [ACLの照合（Match ACL）] ドロップダウンリストから [DIA-FTD-Branch] を選択します。

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 [優先順位による（By 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



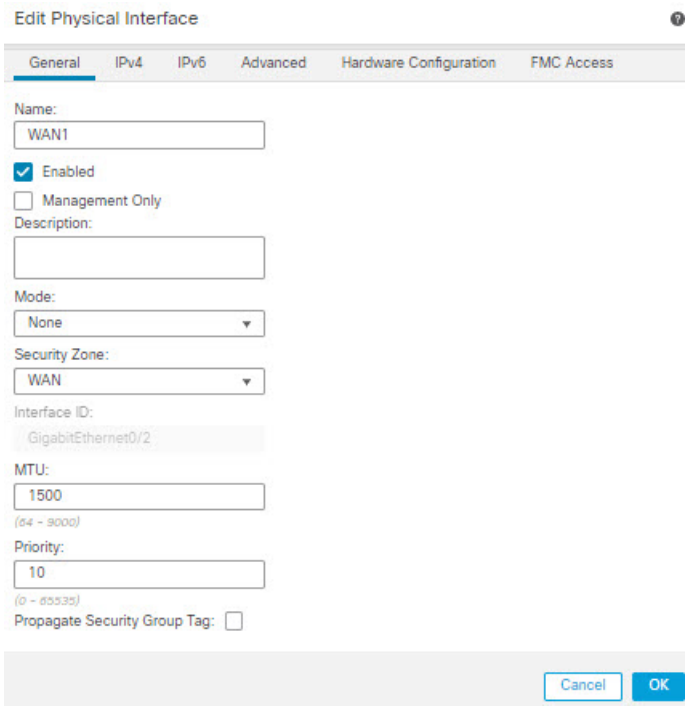
c) [保存（Save）] をクリックします。

ステップ 4 インターフェイスの優先順位を設定します。

[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) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、ブランチ 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。

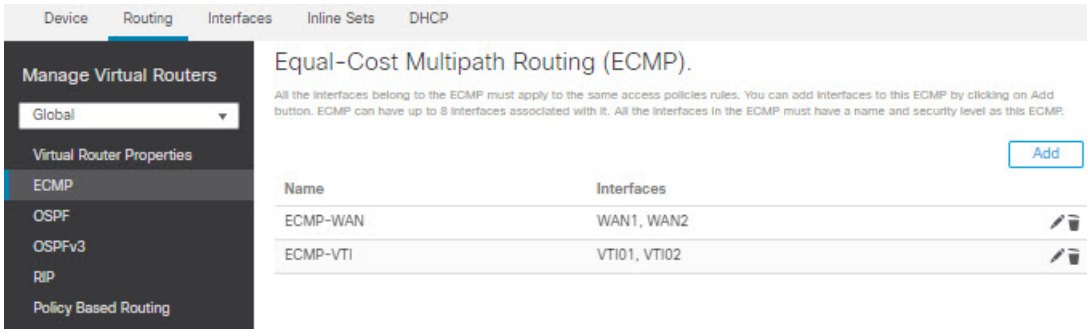
ステップ 5 ロードバランシング用の ECMP ゾーンを作成します。

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

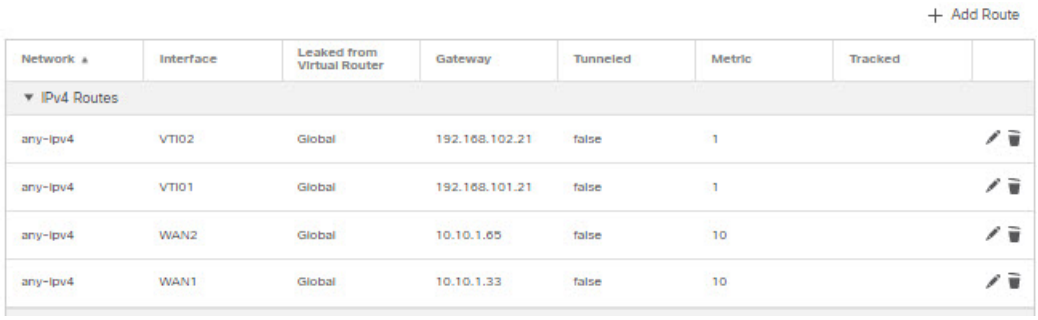


ステップ 6 ロードバランシング用のゾーンインターフェイスのスタティックルートを設定します。

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（ステップ 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安全なトラフィックフローが確保されるように、ブランチ Threat Defense の WAN オブジェクトで信頼できる DNS を設定します。

a) **[デバイス（Devices）]>[プラットフォーム設定（Platform Settings）]**を選択し、ブランチ 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。

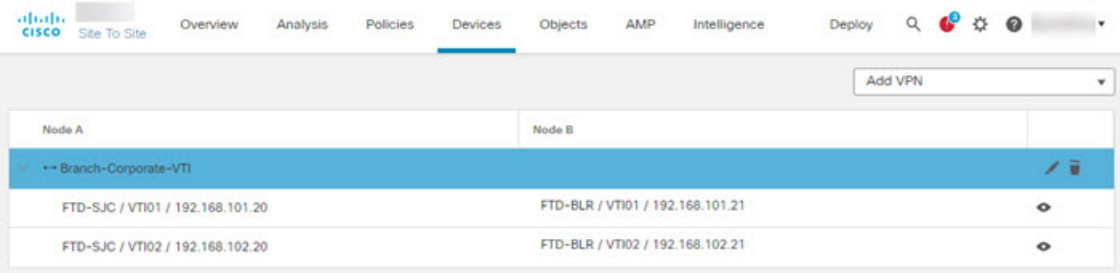
c) WAN オブジェクトが使用する DNS 解決用の DNS サーバーを指定するには、[DNS 設定（DNS Settings）]タブで、DNSサーバーグループの詳細情報を指定し、インターフェイスオブジェクトから WAN を選択します。

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）]、[展開（Deploy）] の順にクリックします。

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。

図 *8* : サイト間 *VPN* の設定



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 の設定について詳しく説明します。

- 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（特定の送信元と宛先を使用）。

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) **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、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) 同じ手順を繰り返し、ISP02 と ISP03 のパスモニタリングの設定を指定します。

ステップ 2 組織の 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、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 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 [右矢印（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、同じインターフェイス（*Inside1*）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）]、[展開（Deploy）] の順にクリックします。

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、**その他** 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 （13 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。

ポリシーベース ルーティングの履歴

表 *1*:

機能	最小 Management Center	最小 Threat Defense	詳細
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。

機能	最小 Management Center	最小 Threat Defense	詳細
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。
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。

機能	最小 Management Center	最小 Threat Defense	詳細
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。
FMC Web インターフェイスからポリシーベースルーティングを設定します。	7.1.0	7.1.0	**アップグレードの影響。アップグレード後に、FlexConfig をやり直します。** FMC Web インターフェイスからポリシーベースルーティング（PBR）を設定できるようになりました。これにより、アプリケーションに基づいてネットワークトラフィックを分類し、ダイレクトインターネットアクセス（DIA）を実装して、ブランチ展開からインターネットにトラフィックを送信することができます。PBR ポリシーを定義し、入力インターフェイスに設定して、一致基準と出力インターフェイスを指定できます。アクセスコントロールポリシーに一致するネットワークトラフィックは、ポリシーで設定されている優先順位または順序に基づいて、出力インターフェイスを介して転送されます。 この機能を使用するには、FMC とデバイスの両方にバージョン 7.1 以降が必要です。FMC をバージョン 7.1 以降にアップグレードすると、既存のポリシーベースルーティング FlexConfig が削除されます。デバイスをバージョン 7.1 以降にアップグレードした後、FMC Web インターフェイスでポリシーベースルーティング設定をやり直します。バージョン7.1+にアップグレードしないデバイスの場合は、FlexConfig を再実行し、「毎回」展開するように設定します。 新規/変更された画面：**[デバイス（Devices）]> [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）]**

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。