



ダイレクトインターネットアクセス (DIA) を使用したブランチからインター ネットへのアプリケーショントラフィッ クのルーティング

この章では、2つの使用例を使用して、ダイレクトインターネットアクセス (DIA) の実践的な応用について詳しく説明します。各使用例では、シナリオ、ネットワークトポロジ、ベストプラクティス、および前提条件について詳しく説明します。また、シームレスな導入のための包括的なエンドツーエンドの手順も提供します。

- [ダイレクトインターネットアクセス \(2 ページ\)](#)
- [利点 \(4 ページ\)](#)
- [この使用例の対象者 \(4 ページ\)](#)
- [ダイレクトインターネットアクセスのコンポーネント \(4 ページ\)](#)
- [ベストプラクティス \(5 ページ\)](#)
- [前提条件 \(5 ページ\)](#)
- [シナリオ 1: パスモニタリングを使用しないダイレクトインターネットアクセス \(6 ページ\)](#)
- [シナリオ 2: パスモニタリングを使用したダイレクトインターネットアクセス \(9 ページ\)](#)
- [信頼された DNS サーバーの設定 \(12 ページ\)](#)
- [インターフェイスの優先順位の設定 \(13 ページ\)](#)
- [ECMP ゾーンの作成 \(14 ページ\)](#)
- [等コストスタティックルートの設定 \(14 ページ\)](#)
- [パスモニタリングの設定 \(15 ページ\)](#)
- [YouTube の拡張 ACL オブジェクトの設定 \(15 ページ\)](#)
- [Webex の拡張 ACL オブジェクトの設定 \(16 ページ\)](#)
- [YouTube のポリシー ベース ルーティング ポリシーの設定 \(17 ページ\)](#)
- [Webex のポリシー ベース ルーティング ポリシーの設定 \(18 ページ\)](#)

- [Webex のパスマニタリングを使用したポリシー ベース ルーティング ポリシーの設定 \(19 ページ\)](#)
- [設定の展開 \(20 ページ\)](#)
- [アプリケーション トラフィック フローの確認 \(21 ページ\)](#)
- [ポリシーベースルーティングのモニターとトラブルシューティング \(23 ページ\)](#)
- [関連リソース \(26 ページ\)](#)

ダイレクト インターネット アクセス

デジタルイノベーションにより、ビジネスの運営、コミュニケーション、お客様とのやり取りの方法が変革されています。コラボレーションとカスタマーエクスペリエンスを向上させるための新しいアプリケーションとテクノロジーが作成され、高帯域幅の低遅延な接続が必要になっています。

従来のネットワークの課題

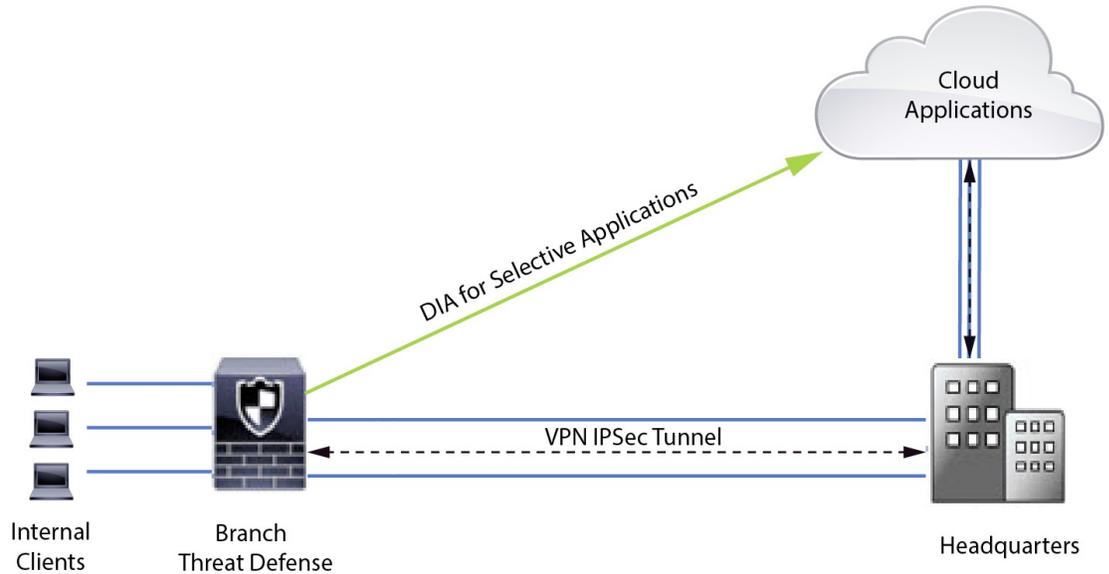
従来のネットワーク展開では、中央サイトの境界ファイアウォールを利用して、ローカルユーザーとブランチユーザーにセキュアなアクセスを提供しています。このアーキテクチャでは必要な接続が提供されますが、すべてのインターネットトラフィックが暗号化されたトラフィックとして VPN トンネル経由で中央サイトに転送されるため、パケットの遅延、ドロップ、およびジッターが発生します。さらに、このネットワークは、展開と複雑なネットワーク管理に関連する高いコストと帯域幅の使用率という課題に常に直面しています。

解決方法

これらの課題を克服する方法の 1 つは、ダイレクトインターネットアクセス (DIA) を使用することです。DIA は、Cisco Secure Firewall のブランチの簡素化機能のコンポーネントです。DIA では、ポリシーベースルーティング (PBR) が使用されます。DIA は、アプリケーション認識型ルーティングとも呼ばれます。

DIA トポロジでは、分散拠点からのアプリケーショントラフィックがインターネットに直接ルーティングされるため、本社へのインターネット宛トラフィックのトンネリングの遅延を回避できます。ブランチの Cisco Secure 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。入力インターフェイスで PBR ポリシーが適用され、拡張アクセスコントロールリストで定義されたアプリケーションに基づいてトラフィックが識別されます。それに応じて、トラフィックは出力インターフェイスを介して直接インターネットに転送されます。

図 1: 特定の出カインターフェイスを介したダイレクトインターネットアクセス



ポリシーベースルーティングを使用する理由

PBRを使用して、指定したアプリケーションのトラフィックを分類し、安全にブレイクアウトすることができます。また、特定のトラフィックのパスを指定することもできます。Cisco 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。

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。Cisco Secure Firewall Management Center 7.2 以降のバージョンでは、PBR 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 はこれらの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場合にモニタリング対象インターフェイスを 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、出力インターフェイスのモニタリングタイプを設定し、メトリック値を使用するパスモニタリングを活用するようにアプリケーショントラフィックを設定する必要があります。

パスモニタリングについては、[シナリオ2：パスモニタリングを使用したダイレクトインターネットアクセス（9 ページ）](#)を参照してください。

利点

DIA を使用する利点は次のとおりです

- インターネットの速度と分散拠点のユーザー体験が向上します。
- 複雑さが軽減され、ネットワーク管理が簡単かつ低コストになります。
- 帯域幅の使用量が削減され、高価なハードウェアが不要になるため、コスト効率が高くなります。
- リアルタイムメトリックを使用した動的なパス選択。
- 手動介入なしで保証される最適な出力パス。
- リンクの正常性とネットワーク状態の継続的なモニタリング。
- 俊敏性の向上により、組織は変化するビジネスニーズに迅速に適応できます。

この使用例の対象者

この使用例の対象者は、ブランチからの直接のインターネット宛トラフィックのローカルブレイクアウトを許可するために、各リモートサイト内にダイレクトインターネットアクセスを導入することを希望するネットワーク設計エンジニア、ネットワーク運用担当者、およびセキュリティ運用担当者です。

ダイレクトインターネットアクセスのコンポーネント

ブランチファイアウォールが DIA に使用する重要なコンポーネントの一部を次に示します。

- **信頼された DNS サーバー** : DIA 機能のアプリケーション検出は、DNS スヌーピングを使用してアプリケーションまたはアプリケーションのグループを解決します。DNS リクエストが不正な DNS サーバーによって解決されず、実際に目的の DNS サーバーにロックされていることを確認するために、Management Center では、Threat Defense の信頼された DNS サーバーを設定できます。
- **インターフェイスの優先順位** : Cisco Secure Firewall は、インターフェイスの優先順位を使用して最適なインターネットパスを決定します。優先順位は小さいほど高く、インターネットにトラフィックを送信するときの特定の ISP の優先順位を決定します。Management Center では、Threat Defense のインターフェイスの優先順位を設定できます。
- **ネットワークサービス** : ポリシーベースルーティング内で使用される、特定のアプリケーションに関連付けられたオブジェクト。このオブジェクトは自動的に作成されます。
- **ネットワークサービスグループ (NSG)** : ネットワークサービスグループは、ファイアウォールが設定に基づいてパスを決定するために使用するアプリケーションのグループで

す。複数のネットワーク サービス オブジェクトを単一の NSG に含めることができます。Management Center は、ポリシーベースルーティング用に設定された拡張アクセスリストに基づいて NSG を自動生成します。

ベストプラクティス

- Cisco Secure Firewall Threat Defense はバージョン 7.1 以降を実行する必要があります。
- アプリケーショントラフィックフローをサポートするために、信頼された DNS サーバーを介して DNS スヌーピングが実行されるように、信頼された DNS サーバーを設定する必要があります。
- Threat Defense を通過する DNS リクエストはクリアテキスト形式である必要があります、DNS スヌーピングが PBR フローを支援できるように、暗号化されていない必要があります。
- アプリケーショントラフィックのアクティブ/アクティブロードバランシング用に、ECMP ゾーンを設定する必要があります。
- ECMP 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、デバイスは最大で 256 の ECMP ゾーンを持つことができます。
- ルーテッドインターフェイスのみを使用する必要があります。各インターフェイスは、単一の ECMP ゾーンにのみ属する必要があります。
- インターフェイスが、ECMP が設定されている仮想ルータに属していることを確認してください。
- ECMP ゾーン設定で使用されるインターフェイスには、インターフェイス設定内で論理名が定義されている必要があります。
- Cisco Secure Firewall Threat Defense で PBR に設定されているインターフェイスが、ECMP ゾーンごとに 8 つ以下であることを確認します。
- PBR はこのモードではサポートされていないため、Cisco Secure Firewall Threat Defense はクラスタに展開しないでください。
- PBR は、ユーザー定義の仮想ルータではサポートされていないため、グローバル仮想ルータ用に設定する必要があります。
- PBR 内の入力および出力インターフェイスで使用されるインターフェイスが、ルーテッドインターフェイスまたは管理専用以外のインターフェイスのいずれかであり、グローバル仮想ルータに属していることを確認します。

前提条件

- [Device Manager](#) を使用した Threat Defense の初期設定の完了

- デバイスへのライセンスの割り当て
- インターネットアクセスのルートの追加。「スタティックルートの追加」を参照してください
- 脅威に対する防御のための NAT の設定
- 基本的なアクセス コントロール ポリシーの作成

シナリオ 1: パスモニタリングを使用しないダイレクトインターネットアクセス

Bob はアカウントマネージャで、Ann はヘルプデスクスペシャリストです。どちらも大企業の分散拠点で働いています。最近、Webex などの Web 会議ツールや YouTube などのストリーミングプラットフォームを使用しているときに、遅延の問題が発生しています。

リスクがあるもの

ネットワーク遅延とネットワーク輻輳により、Web 会議およびストリーミングセッションのパフォーマンスとユーザー体験が低下します。これは、分散拠点の従業員の生産性と効率に影響を与え、事業運営全体に悪影響を及ぼす可能性があります。

PBR を使用した DIA による問題の解決方法

IT 管理者の Alice は、ポリシーベースのルーティングを DIA と組み合わせて使用し、ネットワークの遅延を低減します。

ダイレクトインターネットアクセスにより、分散拠点はセントラルサイトまたはデータセンターを介してトラフィックをルーティングすることなく、インターネットに直接アクセスできるようになりました。これにより、より直接的で最適化されたインターネット接続がブランチユーザーに提供されるため、遅延が低減されました。

ポリシーベースのルーティングにより、Webex と YouTube のトラフィックが異なる出力インターフェイスに分離されました。これにより、トラフィックが異なるパスを介して送信されるようになり、単一インターフェイスでの負荷が軽減され、アプリケーションのパフォーマンスが向上しました。

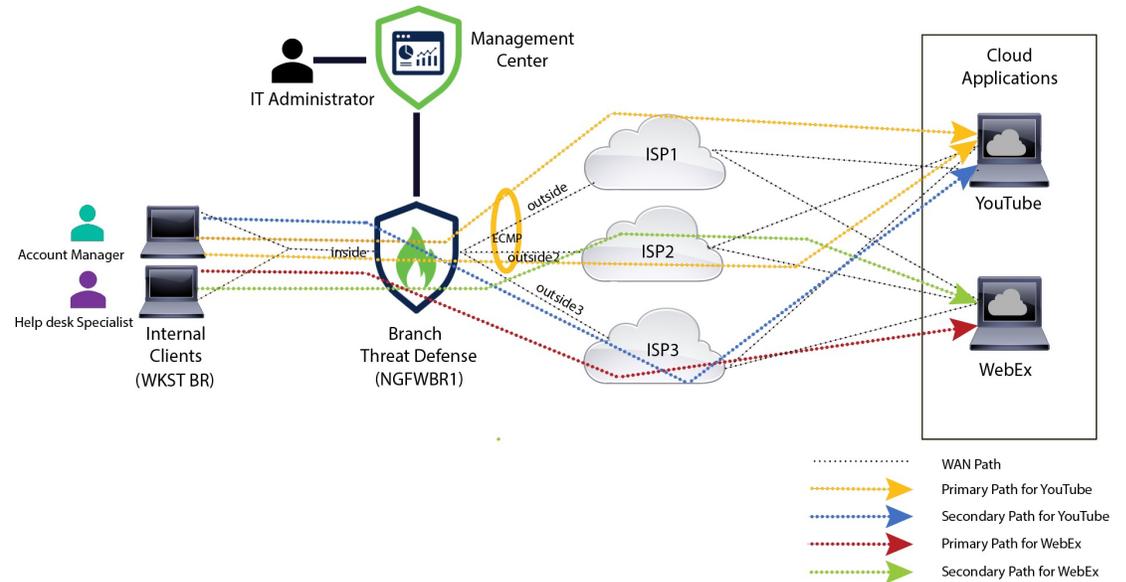
ネットワークトポロジ: パスモニタリングを使用しない DIA

このトポロジでは、Threat Defense デバイスが 3 つの出力インターフェイスを持つブランチロケーションに展開されます。デバイスは、PBR を使用した DIA 用に設定されています。

次の図では、内部クライアントまたはブランチワークステーションには **WKSTBR** というラベルが付けられ、ブランチの Threat Defense には **NGFWBR1** というラベルが付けられています。**NGFWBR1** の入力インターフェイスには **inside** という名前が付けられ、出力インターフェイスにはそれぞれ **outside**、**outside2**、および **outside3** という名前が付けられています。

outside と **outside2** のインターフェイス間のロードバランシングは、ECMP ゾーンとスタティックルートを設定することで実現されています。

図 2: ダイレクトインターネットアクセスのトポロジ (パスモニタリングなし)

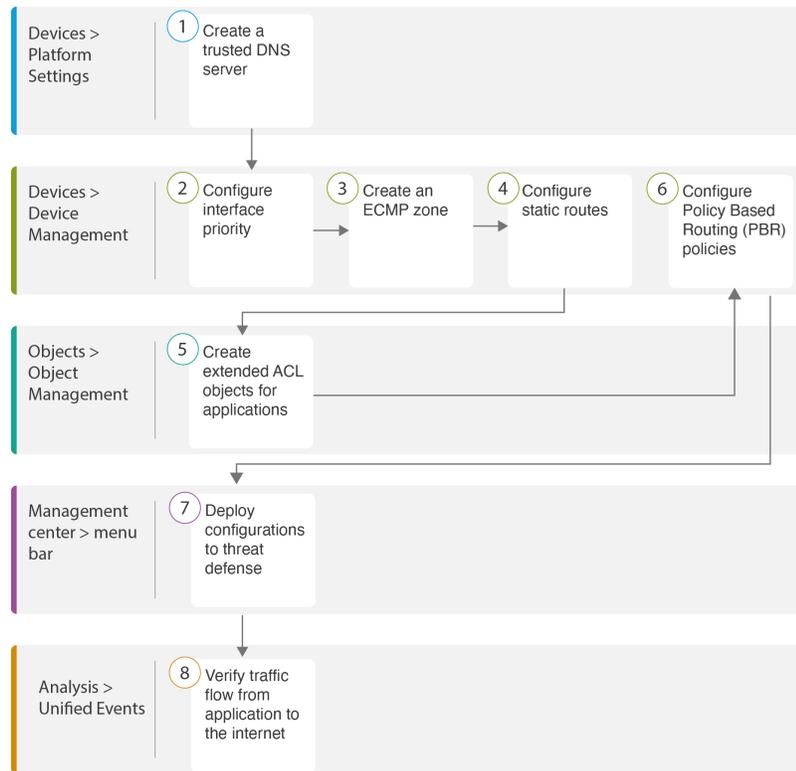


DIAを使用すると、ブランチファイアウォールの背後にあるユーザーは次へのアクセスが許可されます。

1. ソーシャルメディアアプリケーションのトラフィック (YouTube など)。2つの出カインターフェイス (**outside** と **outside2**) を使用してロードバランシングされます。両方のインターフェイスに障害が発生した場合、トラフィックは3番目の出カインターフェイス (**outside3**) にフォールバックします。
2. コラボレーションアプリケーションのトラフィック (Webex など)。**outside3** インターフェイスを介して転送され、このリンクに障害が発生した場合、トラフィックは **outside2** インターフェイスを介して転送されます。

パスモニタリングを使用しない DIA の設定のエンドツーエンドの手順

次のフローチャートは、Cisco Secure Firewall Management Center でパスモニタリングを使用せずに DIA を設定するためのワークフローを示しています。



ステップ	説明
①	(前提条件) 信頼された DNS サーバーを設定します。信頼された DNS サーバーの設定 (12 ページ) を参照してください。
②	(前提条件) インターフェ이스の優先順位を設定します。インターフェースの優先順位の設定 (13 ページ) を参照してください。
③	(前提条件) ECMP ゾーンを作成します。ECMP ゾーンを作成 (14 ページ) を参照してください。
④	(前提条件) スタティックルートを設定します。等コストスタティックルートの設定 (14 ページ) を参照してください。
⑤	アプリケーションの拡張 ACL オブジェクトを設定します。参照先 <ul style="list-style-type: none"> • YouTube の拡張 ACL オブジェクトの設定 (15 ページ) • Webex の拡張 ACL オブジェクトの設定 (16 ページ)
⑥	アプリケーションの PBR ポリシーを設定します。参照先 <ul style="list-style-type: none"> • YouTube の拡張 ACL オブジェクトの設定 (15 ページ) • YouTube のポリシー ベース ルーティング ポリシーの設定 (17 ページ)

ステップ	説明
7	設定を Threat Defense に展開します。設定の展開 (20 ページ) を参照してください。
8	YouTube および Webex のトラフィックフローを確認します。アプリケーショントラフィックフローの確認 (21 ページ) を参照してください。

シナリオ 2: パスモニタリングを使用したダイレクトインターネットアクセス

Ann はヘルプデスクスペシャリストであり、大企業の分散拠点で働いています。Ann は、Webex の使用中に接続の切断と遅延を経験しています。

リスクがあるもの

Webex Meetings は、会議のホストと参加者の間のリアルタイムのデータ伝送（音声とビデオのストリームを含む）に依存しています。このリアルタイムデータは、ネットワーク遅延とパケット損失の影響を受けます。ネットワークで大量のパケット損失が発生すると、フリーズ、遅れ、遅延などの音声とビデオの品質の問題が発生し、会議の体験に悪影響を与える可能性があります。

パスモニタリングを使用した PBR による問題の解決方法

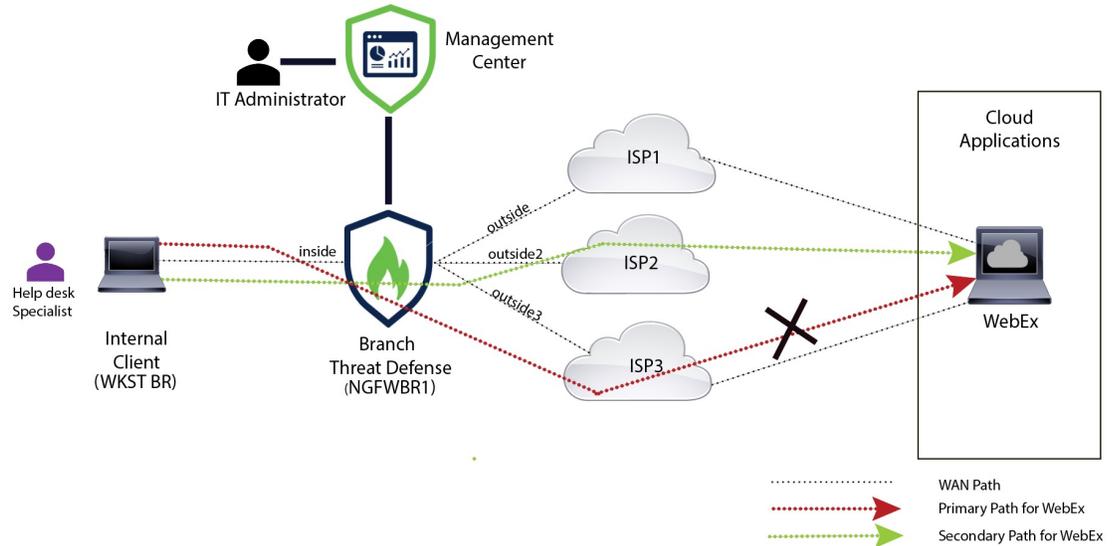
IT 管理者の Alice は、パスモニタリングを使用したポリシーベースルーティングを使用して、パケット損失を最小限に抑えながら Webex のアプリケーショントラフィックを出力インターフェイスを介してインターネットに誘導し、参加者に可能な限り優れた会議の体験を提供しました。

ネットワークトポロジ: パスモニタリングを使用した DIA

このトポロジでは、Threat Defense デバイスが 3 つの出力インターフェイスを持つブランチロケーションに展開されます。デバイスは、ポリシーベースルーティングを使用したダイレクトインターネットアクセス用に設定されています。

次の図では、内部クライアントまたはブランチワークステーションには **WKSTBR** というラベルが付けられ、ブランチの Threat Defense には **NGFWBR1** というラベルが付けられています。**NGFWBR1** の入力インターフェイスには **inside** という名前が付けられ、出力インターフェイスにはそれぞれ **outside**、**outside2**、および **outside3** という名前が付けられています。

図 3:ダイレクトインターネットアクセスのトポロジ (パスモニタリングあり)



outside2 および **outside3** 出力インターフェイスが、パスモニタリングで有効になっています。Webex の PBR ポリシーは、パケット損失を最小限に抑えてトラフィックが出力インターフェイスにルーティングされるように設定されています。

このシナリオでは、パスモニタリングを検証するために、アップストリームデバイスのアクセス制御リストを通じて、または、Firewall Management Center から Cisco Secure Firewall Threat Defense の **outside3** インターフェイスをシャットダウンして、**outside3** インターフェイスから送信されてインターネットに向かうアウトバウンドトラフィックを制限することで、パケット損失を引き起こすことができます。

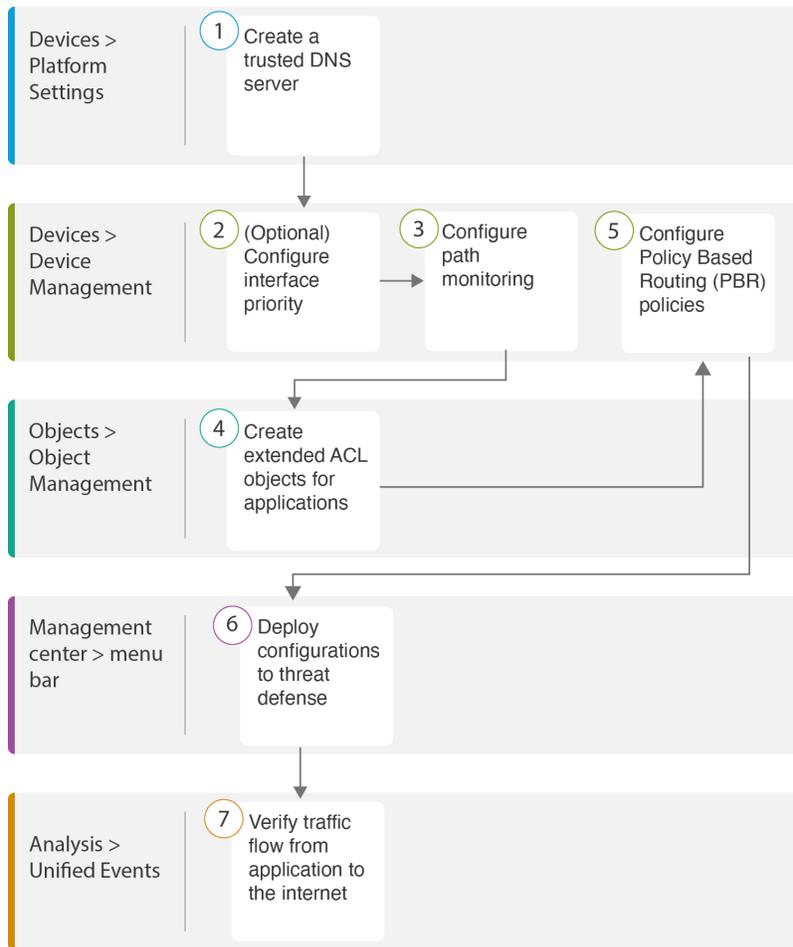


(注) インターフェイスをシャットダウンするとネットワークに影響が出る可能性があるため、実稼働ネットワークで試してはなりません。

パケット損失の結果として、**outside3** インターフェイスに関連付けられているリンクがダウンします。コラボレーションアプリケーションのトラフィックは、**outside3** インターフェイスの代わりに、**outside2** インターフェイスを介して転送されます。

パスモニタリングを使用した DIA の設定のエンドツーエンドの手順

次のフローチャートは、Cisco Secure Firewall Management Center でパスモニタリングを使用して DIA を設定するためのワークフローを示しています。



ステップ	説明
①	(前提条件) 信頼された DNS サーバーを設定します。信頼された DNS サーバーの設定 (12 ページ) を参照してください。
②	[前提条件 (オプション)] インターフェ이스の優先順位を設定します。インターフェ이스の優先順位の設定 (13 ページ) を参照してください。
③	パスモニタリングを設定します。パスモニタリングの設定 (15 ページ) を参照してください。
④	アプリケーションの拡張 ACL オブジェクトを設定します。Webex の拡張 ACL オブジェクトの設定 (16 ページ) を参照してください。
⑤	アプリケーションの PBR ポリシーを設定します。Webex のパスモニタリングを使用したポリシー ベース ルーティング ポリシーの設定 (19 ページ) を参照してください。
⑥	設定を Threat Defense に展開します。設定の展開 (20 ページ) を参照してください。

ステップ	説明
7	Webex トラフィックフローを確認します。 アプリケーショントラフィックフローの確認 (21 ページ) を参照してください。

信頼された DNS サーバーの設定

ダイレクトインターネットアクセス機能でのアプリケーション検出は、アプリケーションまたはアプリケーションのグループを検出するために、DNS スヌーピングを使用してアプリケーションドメインを IP にマッピングします。DNS リクエストが不正な DNS サーバーによって解決されず、実際に目的の DNS サーバーにロックされていることを確認するために、Cisco Secure Firewall Management Center では、Cisco Secure Firewall Threat Defense の信頼された DNS サーバーを設定できます。そのため、ファイアウォールは、信頼された DNS サーバーに向かうトラフィックのみをスヌーピングします。信頼された DNS サーバーの設定とは別に、設定済みのサーバーを、DNS サーバークラス、DHCP プール、DHCP リレー、および DHCP クライアントに、信頼された DNS サーバーとして含めることができます。

[信頼されたDNSサーバー (Trusted DNS Servers)] タブを使用して、DNS スヌーピング用の信頼された DNS サービスを構成できます。



- (注) アプリケーションベースの PBR の場合、信頼された DNS サーバーを構成する必要があります。また、ドメインを解決してアプリケーションを検出できるように、DNS トラフィックがクリアテキスト形式で Threat Defense を通過するようする必要があります (暗号化された DNS はサポートされていません)。

始める前に

- 1 つ以上の DNS サーバークラスを作成していることを確認します。詳細については、[DNS サーバークラスオブジェクトの作成](#) を参照してください。
- DNS サーバーに接続するためのインターフェイス オブジェクトが作成されていることを確認します。
- 管理対象デバイスに、DNS サーバーにアクセスするための適切なスタティックルートまたはダイナミックルートがあることを確認します。

ステップ 1 [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、Threat Defense ポリシーを編集します。

ステップ 2 [編集 (Edit)] (✎) アイコンをクリックします。

ステップ 3 [DNS] をクリックします。

ステップ 4 信頼された DNS サーバーを構成するには、[信頼されたDNSサーバー (Trusted DNS Servers)] タブをクリックします。

ステップ5 既存のホストオブジェクトから **DNS_Server** を選択するには、[使用可能なホストオブジェクト (Available Host Objects)] で検索フィールドを使用してそのサーバーを検索し、[追加 (Add)] をクリックして [選択済みDNSサーバー (Selected DNS Servers)] リストに追加します。

(注) **DNS_Server** は、この例で設定された DNS サーバーです。

ステップ6 [保存 (Save)] をクリックします。追加された DNS サーバーは、[信頼されたDNSサーバー (Trusted DNS Servers)] ページに表示されます。

ステップ7 [ポリシー割り当て (Policy Assignments)] をクリックして、**NGFWBR1** が [選択されたデバイス (Selected Devices)] リストにすでにあることを確認します。

ステップ8 [OK] をクリックして、変更内容を確定します。

ステップ9 [保存 (Save)] をクリックして、プラットフォーム設定の変更を書き込みます。

インターフェイスの優先順位の設定

Cisco Secure Firewall Threat Defense は、インターフェイスの優先順位を使用して最適なインターネットパスを決定します。優先順位の範囲は 0 ~ 65535 で、インターネットにトラフィックを送信するときの特定の ISP の優先順位を決定します。トラフィックは、インターフェイスの優先順位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。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、**outside2** と **outside3** の優先順位値がそれぞれ 10 と 20 に設定されているとします。トラフィックは **outside2** に転送されます。**outside2** が使用できなくなった場合、トラフィックは **outside3** に転送されます。

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 (**NGFWBR1**) を編集します。

ステップ2 NGFWBR1 のインターフェイスビューで [ルーティング (Routing)] タブをクリックします。

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。

ステップ4 [インターフェイスの優先順位の設定 (Configure Interface Priority)] をクリックします。

ステップ5 ダイアログボックスで、インターフェイスに対して優先順位番号を指定します。

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。

ステップ6 [保存 (Save)] をクリックします。

ECMP ゾーンの作成

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 (NGFWBR1) を編集します。

ステップ 2 NGFWBR1 のインターフェイスビューで [ルーティング (Routing)] タブをクリックします。

ステップ 3 [ECMP] をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 [ECMPの追加 (Add ECMP)] ボックスで、ECMP ゾーンの名前に **ECMP-WAN** と入力します。

ステップ 6 インターフェイスを関連付けるには、[使用可能なインターフェイス (Available Interfaces)] ボックスでインターフェイスを選択し、[追加 (Add)] をクリックします。

ステップ 7 [OK] をクリック

[ECMP] ページに、新しく作成された ECMP ゾーンが表示されます。

ステップ 8 [保存 (Save)] をクリックします。

等コストスタティックルートの設定

グローバル仮想ルータとユーザー定義仮想ルータのどちらも、そのインターフェイスをデバイスの ECMP ゾーンに割り当てることができます。

始める前に

- インターフェイスの等コストスタティックルートを設定する場合は、必ず、それを ECMP ゾーンに関連付けてください。[ECMP ゾーン の作成 \(14 ページ\)](#) を参照してください。
- インターフェイスを ECMP ゾーンに関連付けずに、同じ宛先とメトリックでインターフェイスのスタティックルートを定義することはできません。

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] ページから、Threat Defense デバイス (NGFWBR1) を編集します。

ステップ 2 [ルーティング (Routing)] タブをクリックします。

ステップ 3 ドロップダウンリストから、インターフェイスが ECMP ゾーンに関連付けられている仮想ルータを選択します。

ステップ 4 インターフェイスの等コストスタティックルートを設定するには、[スタティックルート (Static Route)] をクリックします。

ステップ 5 [ルートを追加 (Add Route)] をクリックして新しいルートを追加するか、既存のルートの場合は [編集 (Edit)] (✎) をクリックします。

- ステップ 6** [インターフェイス (Interface)] ドロップダウンから、仮想ルータと ECMP ゾーンに属するインターフェイスを選択します。
- ステップ 7** [使用可能なネットワーク (Available Networks)] ボックスから宛先ネットワークを選択し、[追加 (Add)] をクリックします。
- ステップ 8** ネットワークのゲートウェイを入力します。
- ステップ 9** メトリック値を入力します。1 ~ 254 の数値を指定できます。
- ステップ 10** 設定を保存するには、[Save] をクリックします。
- ステップ 11** 等コストスタティックルーティングを設定するには、手順を繰り返して、同じ ECMP ゾーンに含まれる別のインターフェイスのスタティックルートを、同じ宛先ネットワークとメトリック値で設定します。必ず、別のゲートウェイを指定してください。

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 (Interface)] 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プローブを送信できます。

- 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 (NGFWBR1) の [編集 (Edit)] (✎) をクリックします。
- ステップ 2** 編集するインターフェイス (**outside**) の [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** [IPベースのパスモニタリングの有効化 (Enable IP based Path 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。この例では、デフォルト値の [インターフェイス外のデフォルトルートのネクストホップ (自動) (Next-hop of default route out of interface (Auto))] を使用します。
- ステップ 6** [OK] をクリックします。
- ステップ 7** **outside2** および **outside3** インターフェイスに対してステップ 2 ~ 8 を繰り返します。
- ステップ 8** [保存 (Save)] をクリックします。

YouTube の拡張 ACL オブジェクトの設定

ポリシーベースルーティングを利用して、YouTube トラフィックがさまざまな出力インターフェイスからインターネットに向けて誘導されるように、アクセスリストが設定されます。

-
- ステップ 1 [オブジェクト (Objects)]>[オブジェクト管理 (Object Management)] を選択し、コンテンツテーブルから [アクセスリスト (Access Lists)]>[拡張 (Extended)] を選択します。
- ステップ 2 ソーシャルメディアトラフィック用の拡張アクセスリストを作成するには、[拡張アクセスリストの追加 (Add Extended Access List)] をクリックします。
- ステップ 3 [拡張ACLオブジェクト (Extended ACL Object)] ダイアログボックスで、オブジェクトの名前 (**DIA_SocialMedia**) を入力します。
- ステップ 4 [追加 (Add)] をクリックして、新しい拡張アクセスリストを作成します。
- ステップ 5 次のアクセス制御のプロパティを設定します。
1. トラフィック基準を許可 (一致) するように [アクション (Action)] を選択します。
 2. [アプリケーション (Application)] タブをクリックし、[使用可能なアプリケーション (Available Applications)] リストで **YouTube** を検索します。
 3. [YouTube] を選択し、[ルールに追加 (Add to Rule)] をクリックします。
 4. [追加 (Add)] をクリックして、エントリをオブジェクトに追加します。
 5. [保存 (Save)] をクリックします。
-

Webex の拡張 ACL オブジェクトの設定

ポリシーベースルーティングを利用して、Webex トラフィックがさまざまな出力インターフェイスからインターネットに向けて誘導されるように、アクセスリストが設定されます。

- ステップ 1 [オブジェクト (Objects)]>[オブジェクト管理 (Object Management)] を選択し、コンテンツテーブルから [アクセスリスト (Access Lists)]>[拡張 (Extended)] を選択します。
- ステップ 2 コラボレーショントラフィック用の拡張アクセスリストを作成するには、[拡張アクセスリストの追加 (Add Extended Access List)] をクリックします。
- ステップ 3 [拡張ACLオブジェクト (Extended ACL Object)] ダイアログボックスで、オブジェクトの名前 (**DIA_Collaboration**) を入力します。
- ステップ 4 [追加 (Add)] をクリックして、新しい拡張アクセスリストを作成します。
- ステップ 5 次のアクセス制御のプロパティを設定します。
1. トラフィック基準を許可 (一致) するように [アクション (Action)] を選択します。
 2. [アプリケーション (Application)] タブをクリックし、[使用可能なアプリケーション (Available Applications)] リストで **Webex** を検索します。
 3. [Webex] を選択し、[ルールに追加 (Add to Rule)] をクリックします。
 4. [追加 (Add)] をクリックして、エントリをオブジェクトに追加します。

5. [保存 (Save)] をクリックします。

YouTube の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、YouTube トラフィックをルーティングするための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。

YouTube トラフィックは、**outside** および **outside2** のインターフェイス間でロードバランシングされ、両方のリンクに障害が発生した場合は **outside3** にフォールバックします。

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 (NGFWBR1) を編集します。

ステップ 2 NGFWBR1 のインターフェイスビューで [ルーティング (Routing)] タブをクリックします。

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、[入力インターフェイス (Ingress Interface)] ドロップダウンリストから [inside] 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) [ACLの照合 (Match ACL)] ドロップダウンから、[DIA_SocialMedia] を選択します。
- b) 設定されたインターフェイスを選択するには、[送信先 (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。
- c) [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 [優先順位による (By Priority)] を選択します。

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、**outside2** と **outside3** の優先順位値がそれぞれ 10 と 20 に設定されているとします。トラフィックは **outside2** に転送されます。**outside2** が使用できなくなった場合、トラフィックは **outside3** に転送されます。

- 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。Add (+) アイコンをクリックして、選択した出力インターフェイスを追加します。

このシナリオでは、次の手順を実行します。

1. [使用可能なインターフェイス (Available Interfaces)] から、**outside** および **outside2** インターフェイスの横にある Add (+) アイコンをクリックして、[選択した出力インターフェイス (Selected Egress Interfaces)] に移動します。
2. 次に、**outside3** インターフェイスの横にある Add (+) アイコンをクリックして、[選択した出力インターフェイス (Selected Egress Interfaces)] に移動します。

- e) [保存 (Save)] をクリックして、一致基準の変更を書き込みます。

- f) 設定を確認し、[保存 (Save)] をクリックして、ポリシーベースルーティングのすべての設定変更を書き込みます。

ステップ 8 [保存 (Save)] をクリックします。

Webex のポリシーベース 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、Webex アプリケーショントラフィックをルーティングするための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。

Webex アプリケーショントラフィックは **outside3** にルーティングされ、プライマリリンクに障害が発生した場合は **outside2** にフォールバックします。

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 (NGFWBR1) を編集します。

ステップ 2 NGFWBR1 のインターフェイスビューで [ルーティング (Routing)] タブをクリックします。

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 ポリシーを編集するには、[編集 (Edit)] () アイコンをクリックします。

ステップ 5 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 6 [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) [ACLの照合 (Match ACL)] ドロップダウンから、[DIA_Collaboration] を選択します。

- b) 設定されたインターフェイスを選択するには、[送信先 (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。
- c) [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 [順序 (Order)] を選択します。

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。

- 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。Add (+) アイコンをクリックして、選択した出力インターフェイスを追加します。

このシナリオでは、次の手順を実行します。

1. [使用可能なインターフェイス (Available Interfaces)] から、**outside3** インターフェイスの横にある Add (+) アイコンをクリックして、[選択した出力インターフェイス (Selected Egress Interfaces)] に移動します。
 2. 次に、**outside2** インターフェイスの横にある Add (+) アイコンをクリックして、[選択した出力インターフェイス (Selected Egress Interfaces)] に移動します。
- e) [保存 (Save)] をクリックして、一致基準の変更を書き込みます。
 - f) 設定を確認し、[保存 (Save)] をクリックして、ポリシーベースルーティングのすべての設定変更を書き込みます。

ステップ7 [保存 (Save)] をクリックします。

Webex のパスモニタリングを使用した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、パスモニタリングを使用した PBR ポリシーを設定できます。この例では、Webex のアプリケーショントラフィックが、トラフィック損失が最も少ないインターフェイスに転送されます。

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 (NGFWBR1) を編集します。

ステップ2 NGFWBR1 のインターフェイスビューで [ルーティング (Routing)] タブをクリックします。

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、[入力インターフェイス (Ingress Interface)] ドロップダウンリストから [inside] 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。

- [ACLの照合 (Match ACL)] ドロップダウンから、[DIA_Collaboration] を選択します。
- 設定されたインターフェイスを選択するには、[送信先 (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。
- [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 [最小パケット損失 (Minimal Packet Loss)] を選択します。

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。

- [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が一覧表示されます。インターフェイスのリストから、**Add (+)** アイコンをクリックして、選択した出力インターフェイスを追加します。

このシナリオでは、次の手順を実行します。

- [使用可能なインターフェイス (Available Interfaces)] から、**outside3** インターフェイスの横にある **Add (+)** アイコンをクリックして、[選択した出力インターフェイス (Selected Egress Interfaces)] に移動します。
- 次に、**outside2** インターフェイスの横にある **Add (+)** アイコンをクリックして、[選択した出力インターフェイス (Selected Egress Interfaces)] に移動します。
- [保存 (Save)] をクリックして、一致基準の変更を書き込みます。
- 設定を確認し、[保存 (Save)] をクリックして、ポリシーベースルーティングのすべての設定変更を書き込みます。

ステップ 8 [保存 (Save)] をクリックします。

設定の展開

すべての設定が完了したら、管理対象デバイスに設定を展開します。

ステップ 1 Management Center メニューバーで、[展開 (Deploy)] をクリックします。

ステップ 2 設定の変更を展開する NGFWBR1 の横にあるチェックボックスをオンにします。

ステップ 3 [展開 (Deploy)] をクリックします。

ステップ4 展開する変更に関するエラーや警告がシステムによって識別された場合は、[検証エラー (Validation Errors)] または [検証の警告 (Validation Warnings)] ウィンドウにその内容が表示されます。完全な詳細を表示するには、[検証エラー (Validation Errors)] または [検証の警告 (Validation Warnings)] リンクをクリックします。

次の選択肢があります。

- [展開の続行 (Proceed with Deploy)] : 警告状態を解決せずに展開を続行します。システムがエラーを確認した場合は続行できません。
- [閉じる (Close)] : 展開せずに終了します。エラーおよび警告状態を解決し、設定の再展開を試行します。

アプリケーショントラフィックフローの確認

ステップ1 Management Center のインターフェイスで、[分析 (Analysis)] > [統合イベント (Unified Events)] を選択します。

ステップ2 [Webアプリケーション (Web Application)] と [出力インターフェイス (Egress Interface)] を選択し、[適用 (Apply)] をクリックすることで、列ピッカーを使用して列をカスタマイズします。

ステップ3 確認しやすいように列の順序を変更します。

ステップ4 [Webアプリケーション (Web Application)] フィルタ内で、**Webex** という名前を入力し、[適用 (Apply)] をクリックします。

ステップ5 [Webアプリケーション (Web Application)] フィルタ内で、**YouTube** という名前を入力し、[適用 (Apply)] をクリックします。

ステップ6 Cisco Secure Firewall の背後にあるホストで **YouTube** および **Webex** アプリケーションのトラフィックを開始します。このシナリオでは、ブランチワークステーション **WKST BR1** で Google Chrome ブラウザを起動し、異なるタブで <https://youtube.com> と <https://webex.com> に移動します。

ステップ7 Management Center で、両方のアプリケーションのトラフィックフローを確認します。

1. パスモニタリングを使用しない DIA の場合 :

- **Webex** アプリケーショントラフィックは、次の図に示すように、設定に従って **outside3** インターフェイスを介して送信されます。

Time	Event Type	Web Application	Ingress Interface	Egress Interface	Device
2023-03-29 12:54:18	Connection	WebEx	inside	outside3	NGFWBR1
2023-03-29 12:54:18	Connection	WebEx	inside	outside3	NGFWBR1
2023-03-29 12:54:18	Connection	WebEx	inside	outside3	NGFWBR1
2023-03-29 12:54:18	Connection	WebEx	inside	outside3	NGFWBR1
2023-03-29 12:54:18	Connection	WebEx	inside	outside3	NGFWBR1

- **YouTube** アプリケーショントラフィックは、次の図に示すように、設定に従って **outside** および **outside2** インターフェイスの間でロードバランシングされます。

Time	Event Type	Web Application	Ingress Interface	Egress Interface	Device
2023-03-29 03:43:50	Connection	YouTube	inside	outside2	NGFWBR1
2023-03-29 03:43:30	Connection	YouTube	inside	outside2	NGFWBR1
2023-03-29 03:43:10	Connection	YouTube	inside	outside	NGFWBR1
2023-03-29 03:42:50	Connection	YouTube	inside	outside	NGFWBR1
2023-03-29 03:42:50	Connection	YouTube	inside	outside2	NGFWBR1
2023-03-29 03:42:40	Connection	YouTube	inside	outside	NGFWBR1

2. パスモニタリングを使用する DIA の場合 :

Webex アプリケーショントラフィックは、次の図に示すように、**outside3** インターフェイスでパケット損失があるため、**outside2** インターフェイスを介して送信されます。

Time	Event Type	Web Application	Ingress Interface	Egress Interface	Device
2023-03-29 12:29:08	Connection	WebEx	inside	outside2	NGFWBR1
2023-03-29 12:28:30	Connection	WebEx	inside	outside2	NGFWBR1

ポリシーベースルーティングのモニターとトラブルシューティング

展開後に、次の CLI を使用して、Cisco Secure Firewall Threat Defense でのポリシーベースルーティングに関連する問題をモニターおよびトラブルシューティングします。

操作	CLI コマンド
Cisco Secure Firewall Threat Defense の Lina CLI にログインする	system support diagnostic-cli
展開中に Management Center から Threat Defense にプッシュされる事前定義されたネットワーク サービス オブジェクトを表示する	<ul style="list-style-type: none"> • show object network-service • show object network-service detail
設定されたアプリケーションに関連する特定のネットワーク サービス オブジェクト (NSG) を表示する	<ul style="list-style-type: none"> • show object id YouTube • show object id WebEx
Cisco Secure Firewall にプッシュされるネットワーク サービスグループ (NSG) を確認する	show run object-group network-service
ポリシーベースルーティングに関連付けられたルートマップを表示する	show run route-map
インターフェイス名やインターフェイスの優先順位などのインターフェイス設定の詳細を確認する	show run interface
信頼された DNS サーバーの設定を確認する	show dns
トラフィックが通過したパスを特定する	debug policy-route 重要 debug コマンドではトラフィックに基づいた詳細な出力が行われる可能性があるため、特に実稼働環境では注意して実行してください。
ルートのデバッグを停止する	undebug all

事前定義されたネットワーク サービス オブジェクトを表示するには、次のコマンドを使用します。

```
ngfwbr1# show object network-service
object network-service "ADrive" dynamic
description Online file storage and backup.
app-id 17
```

```
domain adrive.com (bid=0) ip (hitcnt=0)
object network-service "Amazon" dynamic
description Online retailer of books and most other goods.
app-id 24
domain amazon.com (bid=0) ip (hitcnt=0)
domain amazon.jobs (bid=0) ip (hitcnt=0)
domain amazon.in (bid=0) ip (hitcnt=0)
.
.
.
output snipped
.
.
.
object network-service "Logitech" dynamic
description Company develops Computer peripherals and accessories.
app-id 4671
domain logitech.com (bid=0) ip (hitcnt=0)
object network-service "Lenovo" dynamic
description Company manufactures/markets computers, software and related services.
app-id 4672
domain lenovo.com (bid=0) ip (hitcnt=0)
domain lenovo.com.cn (bid=0) ip (hitcnt=0)
domain lenovomm.com (bid=0) ip (hitcnt=0)
ngfwbr1#
```

YouTube や Webex などの特定のネットワーク サービス オブジェクトを表示するには、次のコマンドを使用します。

```
ngfwbr1# show object id YouTube
object network-service "YouTube" dynamic
description A video-sharing website on which users can upload, share, and view videos.
app-id 929
domain youtubei.googleapis.com (bid=592729) ip (hitcnt=0)
domain yt3.ggpht.com (bid=709809) ip (hitcnt=102)
domain youtube.com (bid=830871) ip (hitcnt=101)
domain ytimg.com (bid=1035543) ip (hitcnt=93)
domain googlevideo.com (bid=1148165) ip (hitcnt=466)
domainyoutu.be (bid=1247981) ip (hitcnt=0)
ngfwbr1# show object id WebEx
object network-service "WebEx" dynamic
description Cisco's online meeting and web conferencing application.
app-id 905
domain files-prod-us-east-2.webexcontent.com (bid=182837) ip (hitcnt=0)
domain webex.com (bid=290507) ip (hitcnt=30)
domain avatar-prod-us-east-2.webexcontent.com (bid=452667) ip (hitcnt=0)
ngfwbr1#
```

NSG が Threat Defense にプッシュされていることを確認するには、次のコマンドを使用します。

```
ngfwbr1# show run object-group network-service
object-group network-service FMC_NSG_292057776181
network-service-member "WebEx"
object-group network-service FMC_NSG_292057776200
network-service-member "YouTube"
ngfwbr1#
```

PBR に関連付けられたルートマップを確認するには、次のコマンドを使用します。

```
ngfwbr1# show run route-map
!
route-map FMC_GENERATED_PBR_1678091359817 permit 5
match ip address DIA_Collaboration
```

```
set interface outside3 outside2

!  
route-map FMC_GENERATED_PBR_1678091359817 permit 10  
match ip address DIA_SocialMedia  
set adaptive-interface cost outside outside2 outside3  
!  
ngfwbr1#
```

インターフェイス設定とインターフェイスの優先順位の詳細を確認するには、次のコマンドを使用します。

```
ngfwbr1# show run interface  
!  
interface GigabitEthernet0/0  
  nameif outside  
  cts manual  
  propagate sgt preserve-untag  
  policy static sgt disabled trusted  
  security-level 0  
  zone-member ECMP-WAN  
  ip address 198.18.128.81 255.255.192.0  
  policy-route cost 10  
!  
interface GigabitEthernet0/1  
  nameif inside  
  cts manual  
  propagate sgt preserve-untag  
  policy static sgt disabled trusted  
  security-level 0  
  ip address 198.19.11.4 255.255.255.0  
  policy-route route-map FMC_GENERATED_PBR_1678091359817  
!  
interface GigabitEthernet0/2  
  shutdown  
  no nameif  
  no security-level  
  no ip address  
!  
interface GigabitEthernet0/3  
  nameif outside2  
  cts manual  
  propagate sgt preserve-untag  
  policy static sgt disabled trusted  
  security-level 0  
  zone-member ECMP-WAN  
  ip address 198.19.40.4 255.255.255.0  
  policy-route cost 10  
!  
interface GigabitEthernet0/4  
  nameif outside3  
  cts manual  
  propagate sgt preserve-untag  
  policy static sgt disabled trusted  
  security-level 0  
  ip address 198.19.30.4 255.255.255.0  
  policy-route cost 20  
!  
interface Management0/0  
  management-only  
  nameif diagnostic  
  cts manual  
  propagate sgt preserve-untag  
  policy static sgt disabled trusted
```

```
security-level 0
no ip address
ngfwbr1#
```

信頼された DNS 設定を確認するには、次のコマンドを使用します。

```
ngfwbr1# show dns

DNS Trusted Source enabled for DHCP Server Configured
DNS Trusted Source enabled for DHCP Client Learned
DNS Trusted Source enabled for DHCP Relay Learned
DNS Trusted Source enabled for DNS Server Configured
DNS Trusted Source not enabled for Trust-any
DNS Trusted Source: Type: IPs : Interface : Idle/Timeout (sec)
  DNS Server Configured: 198.19.10.100: <ifc-not-specified> : N/A
Trusted Source Configured: 198.19.10.100: <ifc-not-specified> : N/A
DNS snooping IP cache: 0 in use, 37 most used
Address                               Idle(sec) Timeout(sec) Hit-count          Branch(es)
ngfwbr1#
```

ポリシールートを手元でデバッグするには、次のコマンドを使用します。

```
ngfwbr1# debug policy-route
debug policy-route  enabled at level 1
ngfwbr1# pbr: policy based route lookup called for 198.19.11.225/58119 to 198.19.10.100/53
  proto 17 sub_proto 0 received on interface inside, NSGs, nsg_id=none
pbr: no route policy found; skip to normal route lookup
.
output-snipped
.
pbr: policy based route lookup called for 198.19.11.225/61482 to 63.140.48.151/443 proto
  6 sub_proto 0 received on interface inside
                                     , NSGs, nsg_id=1
pbr: First matching rule from ACL(2)
pbr: route map FMC_GENERATED_PBR_1678091359817, sequence 5, permit; proceed with policy
  routing
pbr: evaluating interface outside3
pbr: policy based routing applied; egress_ifc = outside3 : next_hop = 198.19.30.63

ngfwbr1#
```

上記のデバッグ例は、Webex のトラフィック用です。PBR によりルートパスが outside2 インターフェイスに変更される前は、トラフィックが outside3 インターフェイスを介してルーティングされることに注意してください。

デバッグプロセスを停止するには、次のコマンドを使用します。

```
ngfwbr1# undebug all
```

関連リソース

リソース (Resource)	URL
Cisco Secure Firewall Threat Defense リリースノート	https://www.cisco.com/go/firewall-release-notes
すべての新機能と廃止された機能	http://www.cisco.com/go/whatsnew-fmc
Cisco.com の Cisco Secure Firewall	http://www.cisco.com/go/firewall

リソース (Resource)	URL
Cisco.com のマニュアル	http://www.cisco.com/go/firewall-docs
YouTube 上の Cisco Secure Firewall	https://www.youtube.com/cisco-netsec
Cisco Secure Firewall Essentials	https://secure.cisco.com/secure-firewall

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。