



スタティック ルートとデフォルト ルート

この章では、Threat Defense でスタティック ルートとデフォルト ルートを設定する方法について説明します。

- [スタティック ルートとデフォルト ルートについて \(1 ページ\)](#)
- [スタティック ルートの要件と前提条件 \(4 ページ\)](#)
- [スタティック ルートとデフォルト ルートのガイドライン \(5 ページ\)](#)
- [スタティック ルートの追加 \(5 ページ\)](#)
- [ルーティングのリファレンス \(7 ページ\)](#)

スタティック ルートとデフォルト ルートについて

接続されていないホストまたはネットワークにトラフィックをルーティングするには、スタティックルーティングとダイナミックルーティングのどちらかを使用して、ホストまたはネットワークへのルートを定義する必要があります。通常は、少なくとも1つのスタティックルート、つまり、他の方法でデフォルトのネットワーク ゲートウェイにルーティングされていない、すべてのトラフィック用のデフォルトルート（通常、ネクスト ホップ ルータ）を設定する必要があります。

デフォルトルート

最も単純なオプションは、すべてのトラフィックをアップストリームルータに送信するようにデフォルトスタティックルートを設定して、トラフィックのルーティングをルータに任せることです。デフォルトルートは、既知のルートもスタティック ルートも指定されていない IP パケットすべてを、Threat Defense デバイスが送信するゲートウェイの IP アドレスを特定するルートです。デフォルト スタティック ルートとは、つまり宛先の IP アドレスとして 0.0.0.0/0 (IPv4) または ::/0 (IPv6) が指定されたスタティック ルートのことです。

デフォルト ルートを常に定義する必要があります。

脅威に対する防御には、データインターフェイスと管理専用インターフェイス（特別な Linux 管理インターフェイスを含む）用の個別のルーティングテーブルがあります。データルーティングテーブルのデフォルトルートのみ追加できます。脅威に対する防御は、Linux 管理インターフェイスにトラフィックを送信する管理専用ルーティングテーブルにデフォルトルートを

自動的に追加します。このルートでは、Linux ルーティングテーブルで個別のルートルックアップが行われます。脅威に対する防御 CLI **configure network static-routes** コマンドを使用して、管理インターフェイスで使用可能な Linux ルーティングテーブルにスタティックルートを追加できます。



(注) デフォルトの Linux ルートは、**configure network ipv4** または **configure network ipv6** コマンドで設定します。

スタティック ルート

次の場合は、スタティック ルートを使用します。

- ネットワークがサポート対象外のルータ ディスカバリ プロトコルを使用している。
- ネットワークが小規模でスタティック ルートを容易に管理できる。
- ルーティング プロトコルが関係するトラフィックまたは CPU のオーバーヘッドをなくす必要がある。
- 場合によっては、デフォルトルートだけでは不十分である。デフォルトのゲートウェイでは宛先ネットワークに到達できない場合があるため、スタティックルートをさらに詳しく設定する必要があります。たとえば、デフォルトのゲートウェイが外部の場合、デフォルトルートは、Threat Defense デバイスに直接接続されていない内部ネットワークにはまったくトラフィックを転送できません。
- ダイナミック ルーティング プロトコルをサポートしていない機能を使用している。
- 仮想ルータはスタティックルートをを使用して、ルートリークを作成します。ルートリークは、仮想ルータのインターフェイスから別の仮想ルータ内の別のインターフェイスへのトラフィックフローを可能にします。詳細については、[仮想ルータの相互接続](#)を参照してください。

不要なトラフィックをドロップするための null0 インターフェイスへのルート

アクセスルールを使用すると、ヘッダーに含まれている情報に基づいてパケットをフィルタ処理することができます。null0 インターフェイスへのスタティック ルートは、アクセスルールを補完するソリューションです。null0 ルートを使用して不要なトラフィックや望ましくないトラフィックを転送することで、トラフィックをドロップできます。

スタティック null0 ルートには、推奨パフォーマンス プロファイルが割り当てられます。また、スタティック null0 ルートを使用して、ルーティンググループを回避することもできます。BGP では、リモート トリガ型ブラック ホールルーティングのためにスタティック null0 ルートを活用できます。

ルートのプライオリティ

- 特定の宛先が特定されたルートはデフォルトルートより優先されます。
- 宛先が同じルートが複数存在する場合（スタティックまたはダイナミック）、ルートのアドミニストレーティブディスタンスによってプライオリティが決まります。スタティックルートは1に設定されるため、通常、それらが最もプライオリティの高いルートです。
- 宛先かつアドミニストレーティブディスタンスが同じスタティックルートが複数存在する場合は、[等コストマルチパス \(ECMP\) ルーティング \(17 ページ\)](#) を参照してください。
- [トンネル化 (Tunneled)] オプションを使用してトンネルから出力されるトラフィックの場合、このルートが他の設定済みルートまたは学習されたデフォルトルートをすべてオーバーライドします。

トランスペアレント ファイアウォール モードおよびブリッジグループのルート

ブリッジグループメンバーインターフェイスを通じて直接には接続されていないネットワークに向かう Threat Defense デバイスで発信されるトラフィックの場合、Threat Defense デバイスがどのブリッジグループメンバーインターフェイスからトラフィックを送信するかを認識するように、デフォルトルートまたはスタティックルートを設定する必要があります。Threat Defense デバイスで発信されるトラフィックには、syslog サーバーまたは SNMP サーバーへの通信が含まれることもあります。1つのデフォルトルートで到達できないサーバーがある場合、スタティックルートを設定する必要があります。トランスペアレントモードの場合、ゲートウェイインターフェイスに BVI を指定できません。メンバーインターフェイスのみが使用できます。ルーテッドモードのブリッジグループの場合、スタティックルートに BVI を指定する必要があります。メンバーインターフェイスを指定することはできません。詳細については、[#unique_994](#)を参照してください。

スタティックルート トラッキング

スタティックルートの問題の1つは、ルートがアップ状態なのかダウン状態なのかを判定する固有のメカニズムがないことです。スタティックルートは、ネクストホップゲートウェイが使用できなくなった場合でも、ルーティングテーブルに保持されています。スタティックルートは、Threat Defense デバイス上の関連付けられたインターフェイスがダウンした場合に限りルーティングテーブルから削除されます。

スタティックルートトラッキング機能には、スタティックルートの使用可能状況を追跡し、プライマリルートがダウンした場合のバックアップルートをインストールするための方式が用意されています。たとえば、ISPゲートウェイへのデフォルトルートを定義し、かつ、プライマリISPが使用できなくなった場合に備えて、セカンダリISPへのバックアップデフォルトルートを定義できます。

Threat Defense デバイスでは、Threat Defense デバイスが ICMP エコー要求を使用してモニタする宛先ネットワーク上でモニタリング対象スタティックルートを関連付けることでスタティックルート トラッキングを実装します。指定された時間内にエコー応答がない場合は、そのホストはダウンしていると見なされ、関連付けられたルートはルーティングテーブルから削除されます。削除されたルートに代わって、メトリックが高い追跡対象外のバックアップルートが使用されます。

モニタリング対象の選択時には、その対象が ICMP エコー要求に応答できることを確認してください。対象には任意のネットワークオブジェクトを選択できますが、次のものを使用することを検討する必要があります。

- ISP ゲートウェイ アドレス (デュアル ISP サポート用)
- ネクストホップゲートウェイアドレス (ゲートウェイの使用可能状況に懸念がある場合)
- Threat Defense デバイスが通信を行う必要のある対象ネットワーク上のサーバー (syslog サーバーなど)
- 宛先ネットワーク上の永続的なネットワーク オブジェクト



(注) 夜間にシャットダウンする PC は適しません。

スタティックルート トラッキングは、スタティックに定義されたルートや、DHCP または PPPoE を通じて取得したデフォルトルートに対して設定することができます。設定済みのルート トラッキングでは、複数のインターフェイス上の PPPoE クライアントだけを有効化することができます。

スタティックルートの要件と前提条件

モデルのサポート

Threat Defense

サポートされるドメイン

任意

ユーザの役割

管理者

ネットワーク管理者

スタティックルートとデフォルトルートのガイドライン

ファイアウォールモードとブリッジグループ

- トランスペアレントモードでは、スタティックルートはブリッジグループメンバーインターフェイスをゲートウェイとして使用する必要があります。BVIを指定することはできません。
- ルーテッドモードでは、BVIをゲートウェイとして指定する必要があります。メンバーインターフェイスを指定することはできません。
- スタティックルートトラッキングは、ブリッジグループメンバーインターフェイスまたはBVIではサポートされません。

サポートされるネットワークアドレス

- IPv6では、スタティックルートトラッキングはサポートされません。
- ASAはクラスEルーティングをサポートしていません。したがって、クラスEネットワークはスタティックルートとしてルーティングできません。

クラスタリングとマルチコンテキストモード

- クラスタリングでは、スタティックルートトラッキングはプライマリユニットでのみサポートされます。
- スタティックルートトラッキングはマルチコンテキストモードではサポートされません。

ネットワークオブジェクトグループ

スタティックルートの設定時は、ネットワークオブジェクトの範囲やIPアドレス範囲を持つネットワークオブジェクトグループは使用できません。

ASPおよびRIBルートエントリ

デバイスにインストールされているすべてのルートとその距離は、ASPルーティングテーブルにキャプチャされます。これは、すべての静的および動的ルーティングプロトコルに共通です。最適な距離のルートのみがRIBテーブルにキャプチャされます。

スタティックルートの追加

スタティックルートは、特定の宛先ネットワークのトラフィックの送信先を定義します。少なくともデフォルトルートを定義する必要があります。デフォルトルートは、宛先IPアドレスが0.0.0.0/0のスタティックルートです。

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** (仮想ルータ対応デバイスの場合) [仮想ルータ (Virtual Routers)]ドロップダウンリストから、スタティックルートを設定する仮想ルータを選択します。
- ステップ 4** [スタティックルート (Static Route)]を選択します。
- ステップ 5** [ルートを追加 (Add Routes)]をクリックします。
- ステップ 6** 追加するスタティックルートのタイプに応じて、[IPv4]または[IPv6]をクリックします。
- ステップ 7** このスタティックルートを適用する[インターフェイス (Interface)]を選択します。

トランスペアレントモードの場合は、ブリッジグループのメンバーインターフェイスの名前を選択します。ブリッジグループによるルーティングモードの場合、BVI名として、いずれかのブリッジグループメンバーインターフェイスを選択できます。不要なトラフィックを「ブラックホール化」するには、Null0 インターフェイスを選択します。

仮想ルーティングを使用するデバイスの場合は、別の仮想ルータに属するインターフェイスを選択できます。このようなスタティックルートは、この仮想ルータから他の仮想ルータにトラフィックをリークする場合に作成できます。詳細については、「[仮想ルータの相互接続](#)」を参照してください。

- ステップ 8** [利用可能なネットワーク (Available Network)]リストで、宛先ネットワークを選択します。
- デフォルトルートを定義するには、アドレス 0.0.0.0/0 のオブジェクトを作成し、ここでそれを選択します。
- (注) IP アドレス範囲を持つネットワーク オブジェクト グループを作成および選択できますが、Management Center ではスタティックルートの設定時に、ネットワークオブジェクトの範囲の使用はサポートされません。
- ステップ 9** [ゲートウェイ (Gateway)]または[IPv6 ゲートウェイ (IPv6 Gateway)]フィールドで、このルートのネクストホップであるゲートウェイルータを入力または選択します。IP アドレスまたはネットワーク/ホストオブジェクトを指定できます。仮想ルータのスタティックルート構成を使用してルートをリークする場合は、ネクストホップのゲートウェイを指定しないでください。
- ステップ 10** [メトリック (Metric)]フィールドに、宛先ネットワークへのホップの数を入力します。有効値の範囲は1～255で、デフォルト値は1です。メトリックは、特定のホストが存在するネットワークへのホップ数 (ホップカウント) に基づくルートの「コスト」を示す測定値です。ホップカウントは、ネットワークパケットが最終的な宛先に到達するまでに通過する必要があるネットワークの数であり、宛先ネットワークも含まれます。メトリックは、複数のルーティングプロトコル間でルートを比較するために使用されます。スタティックルートのデフォルトのアドミニストレーティブディスタンスは1で、ダイナミックルーティングプロトコルで検出されるルートより優先されますが、直接には接続されていないルートです。OSPFで検出されるルートのデフォルトのアドミニストレーティブディスタンスは110です。スタティ

クルートとダイナミックルートのアドミンスレーティブディスタンスが同じ場合、スタティックルートが優先されます。接続されているルートは常に、スタティックルートおよびダイナミックに検出されたルートのどちらよりも優先されます。

(注) デュアルISP/WAN インターフェイス構成の場合、プライマリ データ インターフェイスとセカンダリ データ インターフェイスに同じメトリック値を割り当てる必要があります。デフォルトでは、2つのインターフェイスに同じメトリック値を設定することは許可されていません。検証エラーを無効にするには、2つのインターフェイスが単一のECMPゾーンに属していることを確認してください。

ステップ 11 (任意) デフォルトルートの場合、[トンネル型 (Tunneled)] チェックボックスをオンにして、VPN トラフィック用に別個のデフォルトルートを定義します。

VPN トラフィックに非 VPN トラフィックとは別のデフォルトルートを使用する必要がある場合は、VPN トラフィック用の別個のデフォルトルートを定義できます。その場合、たとえば VPN 接続からの着信トラフィックは内部ネットワークに転送する一方、内部ネットワークからのトラフィックは外部に転送するといった設定を簡単に行うことができます。[トンネル型 (tunneled)] オプションを使用してデフォルトルートを作成すると、デバイスに着信するトンネルからのすべてのトラフィックは、学習したルートまたはスタティックルートを使用してルーティングできない場合、このルートに送信されます。設定できるデフォルトのトンネルゲートウェイは、デバイスごとに1つのみです。トンネルトラフィックの ECMP はサポートされません。

ステップ 12 (IPv4 スタティックルートのみ) ルートの可用性をモニタするには、モニタリングポリシーを定義する SLA (サービスレベル契約) モニタ オブジェクトの名前を [ルートトラッキング (Route Tracking)] フィールドで入力または選択します。

[SLA モニタ](#)を参照してください。

(注) プライマリデータインターフェイスとセカンダリデータインターフェイスのスタティックルートに SLA を割り当てるようにします (デュアルISP/WAN インターフェイス構成)。

ステップ 13 [OK] をクリックします。

ルーティングのリファレンス

ここでは、Threat Defense 内でのルーティング動作の基本概念について説明します。

パスの決定

ルーティングプロトコルでは、メトリックを使用して、パケットの移動に最適なパスを評価します。メトリックは、宛先への最適なパスを決定するためにルーティングアルゴリズムが使用する、パスの帯域幅などの測定基準です。パスの決定プロセスを支援するために、ルーティン

グアルゴリズムは、ルート情報が格納されるルーティングテーブルを初期化して保持します。ルート情報は、使用するルーティング アルゴリズムによって異なります。

ルーティング アルゴリズムにより、さまざまな情報がルーティング テーブルに入力されます。宛先またはネクスト ホップの関連付けにより、最終的な宛先に達するまで、「ネクスト ホップ」を表す特定のルータにパケットを送信することによって特定の宛先に最適に到達できることがルータに示されます。ルータは、着信パケットを受信すると宛先アドレスを確認し、このアドレスとネクスト ホップとを関連付けようとします。

ルーティング テーブルには、パスの妥当性に関するデータなど、他の情報を格納することもできます。ルータは、メトリックを比較して最適なルートを決定します。これらのメトリックは、使用しているルーティング アルゴリズムの設計によって異なります。

ルータは互いに通信し、さまざまなメッセージの送信によりそのルーティング テーブルを保持しています。ルーティング アップデート メッセージはそのようなメッセージの1つで、通常はルーティング テーブル全体か、その一部で構成されています。ルーティング アップデートを他のすべてのルータから分析することで、ルータはネットワーク トポロジの詳細な全体像を構築できます。ルータ間で送信されるメッセージのもう1つの例であるリンクステートアドバタイズメントは、他のルータに送信元のリンクのステートを通知します。リンク情報も、ネットワークの宛先に対する最適なルートをルータが決定できるように、ネットワーク トポロジの全体像の構築に使用できます。

サポートされるルート タイプ

ルータが使用できるルート タイプには、さまざまなものがあります。Threat Defense デバイスでは、次のルート タイプが使用されます。

- スタティックとダイナミックの比較
- シングルパスとマルチパスの比較
- フラットと階層型の比較
- リンクステートと距離ベクトル型の比較

スタティックとダイナミックの比較

スタティックルーティングアルゴリズムは、実はネットワーク管理者が確立したテーブルマップです。このようなマッピングは、ネットワーク管理者が変更するまでは変化しません。スタティック ルートを使用するアルゴリズムは設計が容易であり、ネットワーク トラフィックが比較的予想可能で、ネットワーク設計が比較的単純な環境で正しく動作します。

スタティック ルーティング システムはネットワークの変更に対応できないため、一般に、変化を続ける大規模なネットワークには不向きであると考えられています。主なルーティングアルゴリズムのほとんどはダイナミック ルーティング アルゴリズムであり、受信したルーティングアップデートメッセージを分析することで、変化するネットワーク環境に適合します。メッセージがネットワークが変化したことを示している場合は、ルーティングソフトウェアはルートを再計算し、新しいルーティングアップデートメッセージを送信します。これらのメッ

セージはネットワーク全体に送信されるため、ルータはそのアルゴリズムを再度実行し、それに従ってルーティングテーブルを変更します。

ダイナミックルーティングアルゴリズムは、必要に応じてスタティックルートで補足できます。たとえば、ラストリゾートルータ（ルーティングできないすべてのパケットが送信されるルータのデフォルトルート）を、ルーティングできないすべてのパケットのリポジトリとして機能するように指定し、すべてのメッセージを少なくとも何らかの方法で確実に処理することができます。

シングルパスとマルチパスの比較

一部の高度なルーティングプロトコルは、同じ宛先に対する複数のパスをサポートしています。シングルパスアルゴリズムとは異なり、これらのマルチパスアルゴリズムでは、複数の回線でトラフィックを多重化できます。マルチパスアルゴリズムの利点は、スループットと信頼性が大きく向上することであり、これは一般に「ロードシェアリング」と呼ばれています。

フラットと階層型の比較

ルーティングアルゴリズムには、フラットなスペースで動作するものと、ルーティング階層を使用するものがあります。フラットルーティングシステムでは、ルータは他のすべてのルータのピアになります。階層型ルーティングシステムでは、一部のルータが実質的なルーティングバックボーンを形成します。バックボーン以外のルータからのパケットはバックボーンルータに移動し、宛先の一般エリアに達するまでバックボーンを通じて送信されます。この時点で、パケットは、最後のバックボーンルータから、1つ以上のバックボーン以外のルータを通じて最終的な宛先に移動します。

多くの場合、ルーティングシステムは、ドメイン、自律システム、またはエリアと呼ばれるノードの論理グループを指定します。階層型のシステムでは、ドメイン内の一部のルータは他のドメインのルータと通信できますが、他のルータはそのドメイン内のルータ以外とは通信できません。非常に大規模なネットワークでは、他の階層レベルが存在することがあり、最も高い階層レベルのルータがルーティングバックボーンを形成します。

階層型ルーティングの第一の利点は、ほとんどの企業の組織を模倣しているため、そのトラフィックパターンを適切にサポートするという点です。ほとんどのネットワーク通信は、小さい企業グループ（ドメイン）内で発生します。ドメイン内ルータは、そのドメイン内の他のルータだけを認識していれば済むため、そのルーティングアルゴリズムを簡素化できます。また、使用しているルーティングアルゴリズムに応じて、ルーティングアップデートトラフィックを減少させることができます。

リンクステートと距離ベクトル型の比較

リンクステートアルゴリズム（最短パス優先アルゴリズムとも呼ばれる）は、インターネットワークのすべてのノードにルーティング情報をフラッドします。ただし、各ルータは、それ自体のリンクのステートを記述するルーティングテーブルの一部だけを送信します。リンクステートアルゴリズムでは、各ルータはネットワークの全体像をそのルーティングテーブルに構築します。距離ベクトル型アルゴリズム（Bellman-Fordアルゴリズムとも呼ばれる）では、各ルータが、そのネイバーだけに対してそのルーティングテーブル全体または一部を送信するように要求されます。つまり、リンクステートアルゴリズムは小規模なアップデートを全体に

送信しますが、距離ベクトル型アルゴリズムは、大規模なアップデートを隣接ルータだけに送信します。距離ベクトル型アルゴリズムは、そのネイバーだけを認識します。通常、リンクステート アルゴリズムは OSPF ルーティング プロトコルとともに使用されます。

ルーティングでサポートされるインターネット プロトコル

Threat Defense デバイスは、ルーティングに対してさまざまなインターネット プロトコルをサポートしています。この項では、各プロトコルについて簡単に説明します。

- Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP は、IGRP ルータとの互換性とシームレスな相互運用性を提供するシスコ独自のプロトコルです。自動再配布メカニズムにより、IGRP ルートを Enhanced IGRP に、または Enhanced IGRP からインポートできるため、Enhanced IGRP を既存の IGRP ネットワークに徐々に追加できます。

- Open Shortest Path First (OSPF)

OSPF は、インターネット プロトコル (IP) ネットワーク向けに、インターネット技術特別調査委員会 (IETF) の Interior Gateway Protocol (IGP) 作業部会によって開発されたルーティングプロトコルです。OSPF は、リンクステートアルゴリズムを使用して、すべての既知の宛先までの最短パスを構築および計算します。OSPF エリア内の各ルータには、ルータが使用可能なインターフェイスと到達可能なネイバーそれぞれのリストである同一のリンクステート データベースが置かれています。

- Routing Information Protocol (RIP)

RIP は、ホップ カウントをメトリックとして使用するディスタンスベクトルプロトコルです。RIP は、グローバルなインターネットでトラフィックのルーティングに広く使用されている Interior Gateway Protocol (IGP) です。つまり、1 つの自律システム内部でルーティングを実行します。

- ボーダー ゲートウェイ プロトコル (BGP)

BGP は自律システム間のルーティングプロトコルです。BGP は、インターネットのルーティング情報を交換するために、インターネットサービスプロバイダー (ISP) 間で使用されるプロトコルです。顧客は ISP に接続し、ISP は BGP を使用して顧客のルートと ISP のルートを交換します。自律システム (AS) 間で BGP を使用する場合、このプロトコルは外部 BGP (EBGP) と呼ばれます。サービスプロバイダーが BGP を使用して AS 内のルートを交換する場合、このプロトコルは内部 BGP (IBGP) と呼ばれます。

ルーティングテーブル

Threat Defense はデータ トラフィック (デバイスを介して) および管理トラフィック (デバイスから) に別々のルーティングテーブルを使用します。ここでは、ルーティングテーブルの仕組みについて説明します。管理ルーティングテーブルの詳細については、[管理トラフィック用ルーティングテーブル \(17 ページ\)](#) も参照してください。

ルーティングテーブルへの入力方法

Threat Defense のルーティングテーブルには、スタティックに定義されたルート、直接接続されているルート、およびダイナミックルーティングプロトコルで検出されたルートを入力できます。Threat Defense デバイスは、ルーティングテーブルに含まれるスタティックルートと接続されているルートに加えて、複数のルーティングプロトコルを実行できるため、同じルートが複数の方法で検出または入力される可能性があります。同じ宛先への2つのルートがルーティングテーブルに追加されると、ルーティングテーブルに残るルートは次のように決定されます。

- 2つのルートのネットワークプレフィックス長（ネットワークマスク）が異なる場合は、どちらのルートも固有と見なされ、ルーティングテーブルに入力されます。入力された後は、パケット転送ロジックが2つのうちどちらを使用するかを決定します。

たとえば、RIP プロセスと OSPF プロセスが次のルートを検出したとします。

- RIP : 192.168.32.0/24
- OSPF : 192.168.32.0/19

OSPF ルートのアドミニストレーティブディスタンスの方が適切であるにもかかわらず、これらのルートのプレフィックス長（サブネットマスク）はそれぞれ異なるため、両方のルートがルーティングテーブルにインストールされます。これらは異なる宛先と見なされ、パケット転送ロジックが使用するルートを決定します。

- Threat Defense デバイスが、（RIP などの）1つのルーティングプロトコルから同じ宛先に複数のパスがあることを検知すると、（ルーティングプロトコルが判定した）メトリックがよい方のルートがルーティングテーブルに入力されます。

メトリックは特定のルートに関連付けられた値で、ルートを最も優先されるものから順にランク付けします。メトリックの判定に使用されるパラメータは、ルーティングプロトコルによって異なります。メトリックが最も小さいパスは最適パスとして選択され、ルーティングテーブルにインストールされます。同じ宛先への複数のパスのメトリックが等しい場合は、これらの等コストパスに対してロードバランシングが行われます。

- Threat Defense デバイスが、ある宛先へのルーティングプロトコルが複数あることを検知すると、ルートのアドミニストレーティブディスタンスが比較され、アドミニストレーティブディスタンスが最も小さいルートがルーティングテーブルに入力されます。

ルートのアドミニストレーティブディスタンス

ルーティングプロトコルによって検出されるルート、またはルーティングプロトコルに再配布されるルートのアドミニストレーティブディスタンスは変更できます。2つの異なるルーティングプロトコルからの2つのルートのアドミニストレーティブディスタンスが同じ場合、デフォルトのアドミニストレーティブディスタンスが小さい方のルートがルーティングテーブルに入力されます。EIGRP ルートと OSPF ルートの場合、EIGRP ルートと OSPF ルートのアドミニストレーティブディスタンスが同じであれば、デフォルトで EIGRP ルートが選択されます。

アドミニストレーティブディスタンスは、2つの異なるルーティングプロトコルから同じ宛先に複数の異なるルートがある場合に、Threat Defense デバイスが最適なパスの選択に使用するルートパラメータです。ルーティングプロトコルには、他のプロトコルとは異なるアルゴリズムに基づくメトリックがあるため、異なるルーティングプロトコルによって生成された、同じ宛先への2つのルートについて常にベストパスを判定できるわけではありません。

各ルーティングプロトコルには、アドミニストレーティブディスタンス値を使用して優先順位が付けられています。次の表に、Threat Defense デバイスでサポートされているルーティングプロトコルのデフォルトのアドミニストレーティブディスタンス値を示します。

表 1: サポートされるルーティングプロトコルのデフォルトアドミニストレーティブディスタンス

ルートの送信元	デフォルト アドミニストレーティブ ディスタンス
接続されているインターフェイス	[0]
VPN ルート	1
スタティック ルート	1
EIGRP 集約ルート	5
外部 BGP	20
内部 EIGRP	90
OSPF	110
IS-IS	115
RIP	120
EIGRP 外部ルート	170
内部およびローカル BGP	200
不明 (Unknown)	255

アドミニストレーティブディスタンス値が小さいほど、プロトコルの優先順位が高くなります。たとえば、Threat Defense デバイスが OSPF ルーティングプロセス（デフォルトのアドミニストレーティブディスタンスが 110）と RIP ルーティングプロセス（デフォルトのアドミニストレーティブディスタンスが 120）の両方から特定のネットワークへのルートを受信すると、OSPF ルーティングプロセスの方が優先度が高いため、Threat Defense デバイスは OSPF ルートを選択します。この場合、ルータは OSPF バージョンのルートをルーティングテーブルに追加します。

VPN アドバタイズされたルート（V-Route/RR1）は、デフォルトのアドミニストレーティブディスタンス1のスタティックルートと同等です。ただし、ネットワークマスク 255.255.255.255 の場合と同じように優先度が高くなります。

この例では、OSPF 導出ルートの送信元が（電源遮断などで）失われると、Threat Defense デバイスは、OSPF 導出ルートが再度現れるまで、RIP 導出ルートを使用します。

アドミニストレーティブディスタンスはローカルの設定値です。たとえば、OSPF を通じて取得したルートのアドミニストレーティブディスタンスを変更する場合、その変更は、コマンドが入力された Threat Defense デバイスのルーティングテーブルにだけ影響します。アドミニストレーティブディスタンスがルーティングアップデートでアドバタイズされることはありません。

アドミニストレーティブディスタンスは、ルーティングプロセスに影響を与えません。ルーティングプロセスは、ルーティングプロセスで検出されたか、またはルーティングプロセスに再配布されたルートだけをアドバタイズします。たとえば、RIP ルーティングプロセスは、のルーティングテーブルで OSPF ルーティングプロセスによって検出されたルートが使用されていても、RIP ルートをアドバタイズします。

ダイナミックルートとフローティングスタティックルートのバックアップ

ルートを最初にルーティングテーブルにインストールしようとしたとき、他のルートがインストールされているためにインストールできなかった場合、そのルートはバックアップルートとして登録されます。ルーティングテーブルにインストールされたルートに障害が発生すると、ルーティングテーブルメンテナンスプロセスが、登録されたバックアップルートを持つ各ルーティングプロトコルプロセスを呼び出し、ルーティングテーブルにルートを再インストールするように要求します。障害が発生したルートに対して、登録されたバックアップルートを持つプロトコルが複数ある場合、アドミニストレーティブディスタンスに基づいて優先ルートが選択されます。

このプロセスのため、ダイナミックルーティングプロトコルによって検出されたルートに障害が発生したときにルーティングテーブルにインストールされるフローティングスタティックルートを作成できます。フローティングスタティックルートとは、単に、Threat Defense デバイスで動作しているダイナミックルーティングプロトコルよりも大きなアドミニストレーティブディスタンスが設定されているスタティックルートです。ダイナミックルーティングプロセスで検出された対応するルートに障害が発生すると、このスタティックルートがルーティングテーブルにインストールされます。

転送の決定方法

転送は次のように決定されます。

- 宛先が、ルーティングテーブル内のエン트리と一致しない場合、パケットはデフォルトルートに指定されているインターフェイスを通して転送されます。デフォルトルートが設定されていない場合、パケットは破棄されます。
- 宛先が、ルーティングテーブル内の1つのエン트리と一致した場合、パケットはそのルートに関連付けられているインターフェイスを通して転送されます。
- 宛先が、ルーティングテーブル内の複数のエン트리と一致し、パケットはネットワークプレフィックス長がより長いルートに関連付けられているインターフェイスから転送されます。

たとえば、192.168.32.1 宛てのパケットが、ルーティング テーブルの次のルートを使用してインターフェイスに到着したとします。

- 192.168.32.0/24 gateway 10.1.1.2
- 192.168.32.0/19 gateway 10.1.1.3

この場合、192.168.32.1 は 192.168.32.0/24 ネットワークに含まれるため、192.168.32.1 宛てのパケットは 10.1.1.2 宛てに送信されます。このアドレスはまた、ルーティング テーブルの他のルートにも含まれますが、ルーティング テーブル内では 192.168.32.0/24 の方が長いプレフィックスを持ちます (24 ビットと 19 ビット)。パケットを転送する場合、プレフィックスが長い方が常に短いものより優先されます。



(注) ルートの変更が原因で新しい同様の接続が異なる動作を引き起こしたとしても、既存の接続は設定済みのインターフェイスを使用し続けます。

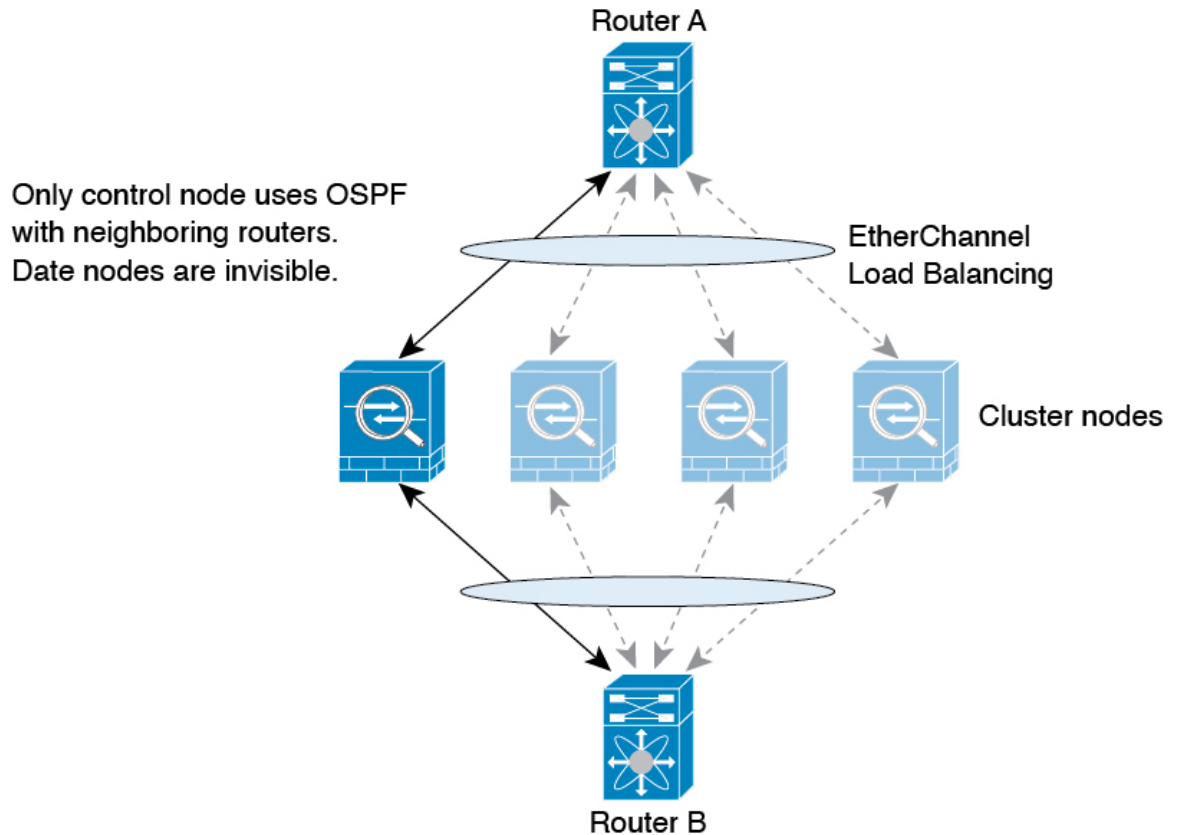
ダイナミック ルーティングおよび 高可用性

アクティブなユニットでルーティング テーブルが変更されると、スタンバイ ユニットでダイナミック ルートが同期されます。これは、アクティブ ユニットのすべての追加、削除、または変更がただちにスタンバイ ユニットに伝播されることを意味します。スタンバイ ユニットがアクティブ/スタンバイの待受中 高可用性 ペアでアクティブになると、ルートは 高可用性 バルク同期および連続複製プロセスの一部として同期されるため、そのユニットには以前のアクティブ ユニットと同じルーティング テーブルがすでに作成されています。

クラスタリングでのダイナミック ルーティング

ルーティングプロセスは制御ノード上だけで実行されます。ルートは制御ノードを介して学習され、データノードに複製されます。ルーティングパケットは、データノードに到着すると制御ノードにリダイレクトされます。

図 1: スパンド EtherChannel モードでのダイナミックルーティング



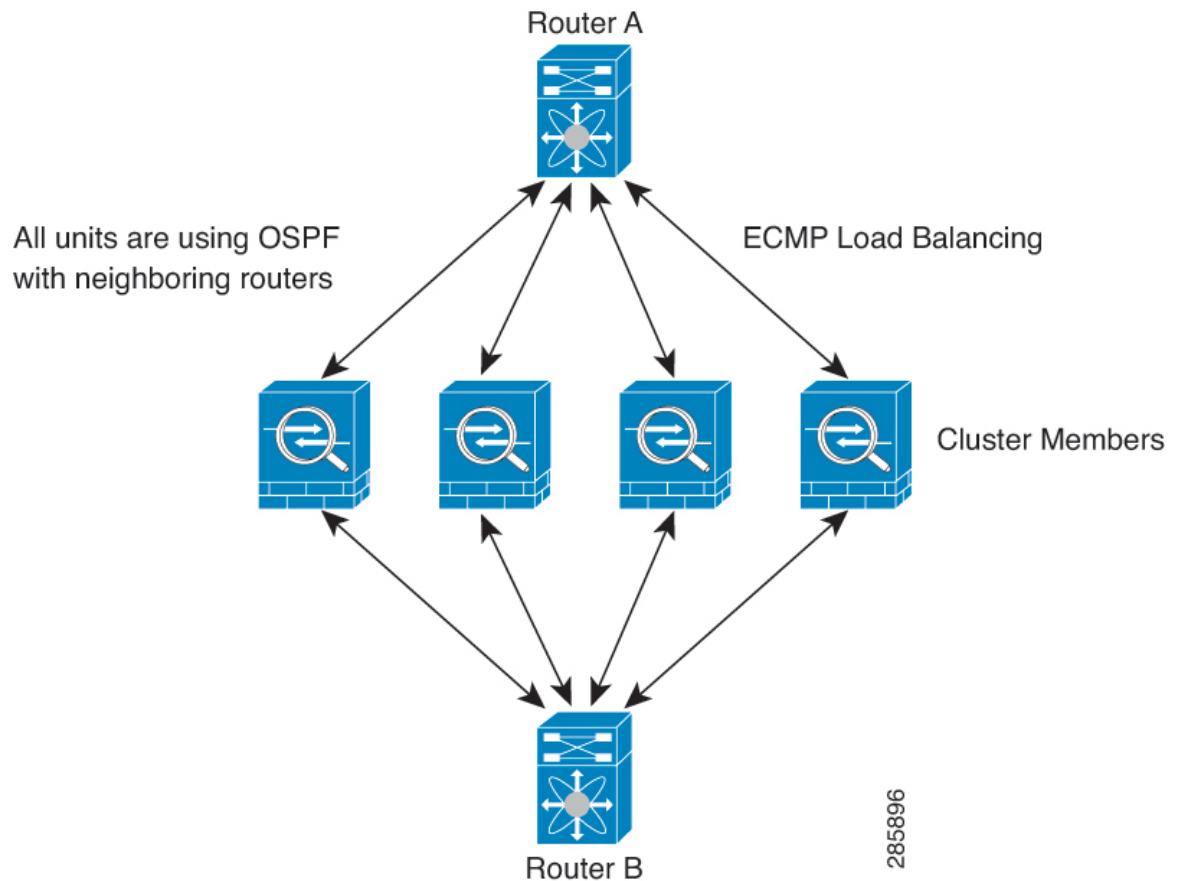
データノードが制御ノードからルートを学習すると、各ノードが個別に転送の判断を行います。

OSPF LSA データベースは、制御ノードからデータノードに同期されません。制御ノードのスイッチオーバーが発生した場合、ネイバルーターが再起動を検出します。スイッチオーバーは透過的ではありません。OSPF プロセスが IP アドレスの 1 つをルータ ID として選択します。必須ではありませんが、スタティック ルータ ID を割り当てることができます。これで、同じルータ ID がクラスタ全体で使用されるようになります。割り込みを解決するには、OSPF ノンストップ フォワーディング機能を参照してください。

個別インターフェイスモードでのダイナミックルーティング

個別インターフェイスモードでは、各ノードがスタンドアロンルータとしてルーティングプロトコルを実行します。ルートの学習は、各ノードが個別に行います。

図 2: 個別インターフェイスモードでのダイナミックルーティング



上の図では、ルータ A はルータ B への等コストパスが 4 本あることを学習します。パスはそれぞれ 1 つのノードを通過します。ECMP を使用して、4 パス間でトラフィックのロードバランシングを行います。各ノードは、外部ルータと通信するときに、それぞれ異なるルータ ID を選択します。

管理者は、各ノードに異なるルータ ID が設定されるように、ルータ ID のクラスタプールを設定する必要があります。

EIGRP は、個別のインターフェイスモードのクラスタピアとのネイバー関係を形成しません。



- (注) 冗長性確保のためにクラスタが同一ルータに対して複数の隣接関係を持つ場合、非対称ルーティングが原因で許容できないトラフィック損失が発生する場合があります。非対称ルーティングを避けるためには、同じトラフィックゾーンにこれらすべてのノードインターフェイスをまとめます。[ECMP ゾーンの作成](#)を参照してください。

管理トラフィック用ルーティングテーブル

Threat Defense デバイスには、デバイス発信管理トラフィック用の次のルーティングテーブルが含まれています。

- **Linux 管理ルーティングテーブル**：Management Center 通信、ライセンス通信、データベース更新などの管理インターフェイスから送信される特別な管理トラフィックは、常に Linux 管理ルーティングテーブルを使用します。
- **データルーティングテーブル**：すべてのデバイス発信トラフィック（およびすべての通過トラフィック）は、デフォルトでデータルーティングテーブルを使用します。通常のデータインターフェイスはすべて、このルーティングテーブルに含まれます。ほとんどのサービスでは、特定のインターフェイスを選択できるため、そのインターフェイスに関連付けられているルートのみが使用されます。
- **管理専用ルーティングテーブル**：管理専用インターフェイスに設定した管理インターフェイスとすべてのデータインターフェイスは、このルーティングテーブルに含まれます。これらのインターフェイスのいずれかからデバイス発信トラフィックを送信するには、サービスの設定時に特定の管理専用インターフェイスを選択する必要があります。DNS ルックアップの場合は例外です。ルートが見つからない場合、Threat Defense はデータを使用して自動的に管理にフォールバックすることもあります。管理専用インターフェイスにはスタティックルートを追加できますが、特殊な管理インターフェイスには追加できません。Threat Defense デバイスは、Linux にトラフィックを転送する管理用のデフォルトルートを自動的に追加します。この場合、Linux ルーティングテーブルで別のルートルックアップが行われます。Threat Defense CLI `configure network static-routes` コマンドを使用して、管理インターフェイスで使用可能な Linux ルーティングテーブルにスタティックルートを追加できます。



(注) デフォルトの Linux ルートは、`configure network ipv4` または `configure network ipv6` コマンドで設定します。



(注) 管理インターフェイスとレガシー診断インターフェイスをまだマージしていないデバイスについては、このガイドの 7.3 より前のバージョンを参照してください。

等コスト マルチパス (ECMP) ルーティング

Threat Defense デバイスは、等コスト マルチパス (ECMP) ルーティングをサポートしています。

インターフェイスごとに最大 8 つの等コストのスタティックルートまたはダイナミックルートを設定できます。たとえば、次のように異なるゲートウェイを指定する外部インターフェイスで複数のデフォルト ルートを設定できます。

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

この場合、トラフィックは、10.1.1.2、10.1.1.3 と 10.1.1.4 間の外部インターフェイスでロードバランスされます。トラフィックは、送信元 IP アドレスと宛先 IP アドレス、着信インターフェイス、プロトコル、送信元ポートと宛先ポートをハッシュするアルゴリズムに基づいて、指定したゲートウェイ間に分配されます。

トラフィックゾーンを使用した複数のインターフェイス間の ECMP

インターフェイスのグループを含むようにトラフィックゾーンを設定する場合、各ゾーン内の最大 8 つのインターフェイス間に最大 8 つの等コストのスタティックルートまたはダイナミックルートを設定できます。たとえば、次のようにゾーン内の 3 つのインターフェイス間に複数のデフォルトルートを設定できます。

```
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.2
route for 0.0.0.0 0.0.0.0 through outside3 to 10.3.1.2
```

同様に、ダイナミックルーティングプロトコルは、自動的に等コストルートを設定できます。Threat Defense デバイスでは、より堅牢なロードバランシングメカニズムを使用してインターフェイス間でトラフィックをロードバランスします。

ルートが紛失した場合、デバイスはフローをシームレスに別のルートに移動させます。

ルートマップについて

ルートマップは、ルートを OSPF、RIP、EIGRP、または BGP ルーティングプロセスに再配布するときに使用します。また、OSPF ルーティングプロセスにデフォルトルートを生成するときにも使用します。ルートマップは、指定されたルーティングプロトコルのどのルートを対象ルーティングプロセスに再配布できるのかを定義します。

ルートマップは、広く知られた ACL と共通の機能を数多く持っています。両方に共通する主な特性は次のとおりです。

- いずれも、それぞれが許可または拒否の結果を持つ個別のステートメントの順序シーケンスです。ACL またはルートマップの評価は、事前に定義された順序でのリストのスキャンと、一致する各ステートメントの基準の評価で構成されています。リストのスキャンは、ステートメントの一致が初めて見つかり、そのステートメントの一致に関連付けられたアクションが実行されると中断します。
- これらは汎用的なメカニズムです。基準照合と一致解釈は、適用方法とこれらを使用する機能によって決定します。同じルートマップであっても異なる機能に適用されると、解釈が異なる場合があります。

次のように、ルートマップと ACL には違いがいくつかあります。

- ルートマップは ACL よりも柔軟性が高く、ACL が確認できない基準に基づいてルートを確認できます。たとえば、ルートマップはルートタイプが内部であるかどうかを確認できます。
- 設計規則により、各 ACL は暗黙の deny ステートメントで終了します。照合中にルートマップの終わりに達した場合、そのルートマップの特定の適用によって結果が異なります。再配布に適用されるルートマップの動作は ACL と同じです。ルートがルートマップのどの句とも一致しない場合は、ルートマップの最後に deny ステートメントが含まれている場合と同様に、ルート再配布が拒否されます。

permit 句と deny 句

ルートマップでは permit 句と deny 句を使用できます。deny 句は、ルートの照合の再配布を拒否します。ルートマップでは、一致基準として ACL を使用できます。ACL には permit 句と deny 句もあるので、パケットが ACL と一致した場合に次のルールが適用されます。

- ACL の permit + ルートマップの permit : ルートは再配布されます。
- ACL の permit + ルートマップの deny : ルートは再配布されません。
- ACL の deny + ルートマップの permit または deny : ルートマップの句は一致せず、次のルートマップ句が評価されます。

match 句と set 句の値

各ルートマップ句には、次の 2 種類の値があります。

- match 値は、この句が適用されるルートを選択します。
- set 値は、ターゲットプロトコルに再配布される情報を変更します。

再配布される各ルートについて、ルータは最初にルートマップの句の一致基準を評価します。一致基準が満たされると、そのルートは、permit 句または deny 句に従って再配布または拒否され、そのルートの一部の属性が、set コマンドによって設定された値で変更されます。一致基準が満たされないと、この句はルートに適用されず、ソフトウェアはルートマップの次の句でルート进行评估します。ルートマップのスキャンは、ルートと一致する句が見つかるまで、もしくはルートマップの最後に到達するまで続行します。

次のいずれかの条件が満たされる場合は、各句の match 値または set 値を省略したり、何回か繰り返したりできます。

- 複数の match エントリが句に含まれる場合に、特定のルートが句に一致するためには、そのルートですべての照合に成功しなければなりません（つまり、複数の match コマンドでは論理 AND アルゴリズムが適用される）。
- match エントリが 1 つのエントリの複数のオブジェクトを指している場合は、そのいずれかが一致していなければなりません（論理 OR アルゴリズムが適用される）。
- match エントリがない場合は、すべてのルートが句に一致します。

- ルート マップの **permit** 句に **set** エントリが存在しない場合、ルートは、その現在の属性を変更されずに再配布されます。



-
- (注) ルート マップの **deny** 句では **set** エントリを設定しないでください。deny 句を指定するとルートの再配布が禁止され、情報が何も変更されないからです。
-

match エントリまたは **set** エントリがないルート マップ句はアクションを実行します。空の **permit** 句を使用すると、変更を加えずに残りのルートの再配布が可能になります。空の **deny** 句では、他のルートの再配布はできません。これは、ルートマップがすべてスキャンされたときに、明示的な一致が見つからなかったときのデフォルトアクションです。

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。