



# Firepower Threat Defense のスタティックルートとデフォルトルート

この章では、FTD 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とデフォルトルートのガイドライン](#) (4 ページ)
- [スタティックルートの追加](#) (4 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や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またはダイナミックルーティングを使用して、ホストや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。

### Default Route

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、FTD 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。

FTD はデータトラフィックと管理トラフィックに別々のルーティングテーブルを使用するため、必要に応じて、データトラフィック用のデフォルトルートと管理トラフィック用の別のデフォルトルートを設定できます。デバイス間トラフィックでは、タイプに応じてデフォルトで管理またはデータルーティングテーブルが使用されます（[管理トラフィック用ルーティングテーブル](#)を参照）。ただし、ルートが見つからない場合は、他のルーティングテーブルに

フォールバックします。デフォルトルートは常にトラフィックに一致するため、他のルーティングテーブルへのフォールバックが妨げられます。この場合、インターフェイスがデフォルトのルーティングテーブルになれば、出力トラフィックに使用するインターフェイスを指定する必要があります。

## 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、FTD 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。

## 不要なトラフィックを「ブラックホール化」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「ブラックホール」に転送できるため、トラフィックがドロップされます。

スタティック null0 ルートには、望ましいパフォーマンス プロファイルがあります。また、スタティック null0 ルートを使用して、ルーティング ループ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](#)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とブリッジグループルート

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 Firepower Threat Defense デバイス で発信されるトラフィックの場合、Firepower 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。Firepower Threat Defense デバイス で発信されるトラフィックは、syslog サーバまたはSNMPサーバへの通信も含むことがあります。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、「[MACアドレスとルートルックアップ](#)」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、Firepower 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。

Firepower Threat Defense デバイス では、Firepower 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思われ、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）
- Firepower 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（syslog サーバなど）
- 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イネーブルにすることができます。

## 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 ルートをブリッジグループ 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。

### IPv6

- 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。

### クラスタ

クラスタリングでは、スタティック ルート モニタリングはプライマリ 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。

- ステップ 1** [デバイス (Devices) ]>[デバイス管理 (Device Management) ]の順に選択し、FTD デバイスを編集します。
- 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** コンテンツのテーブルから [スタティック ルート (Static Route) ]を選択します。
- ステップ 4** [ルートを追加 (Add Routes) ]をクリックします。
- ステップ 5** 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] オプション ボタンをクリックします。
- ステップ 6** 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。
- ステップ 7** [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。
- ステップ 8** [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。
- ステップ 9** [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。スタティックルートと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。
- ステップ 10** (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 11** (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 オブジェクト](#) を参照してください。

**ステップ 12** [OK] をクリックします。

---