



ルーティング

システムはルーティングテーブルを使用して、システムに入力されるパケットの出力インターフェイスを決定します。ここでは、ルーティングの基本とデバイスでのルーティングの設定方法について説明します。

- [ルーティングの概要 \(1 ページ\)](#)
- [スタティック ルート \(7 ページ\)](#)
- [ルーティングのモニタリング \(10 ページ\)](#)

ルーティングの概要

ここでは、FTDデバイス内でルーティングがどのように動作するのかを説明します。ルーティングは、送信元から宛先にネットワーク経由で情報を移動する行為のことです。その間に、通常は少なくとも1つの中間ノードがあります。ルーティングには、最適なルーティングパスの決定と、ネットワーク経由のパケットの転送という2つの基本的なアクティビティが含まれます。

ルート タイプ

ルートには、スタティックまたはダイナミックの2つの主要な種類があります。

スタティックルートは、明示的に定義するものです。これらは通常は優先度の高い安定したルートで、ルートの宛先へのトラフィックを常に正しいインターフェイスに送信するために使用されます。たとえば、その他のルートでカバーされていないすべてのトラフィックをカバーする、デフォルトのスタティックルート（つまり IPv4 では 0.0.0.0/0、IPv6 では ::/0）を作成する場合などです。別の例では、常に使用する内部syslogサーバへのスタティックルートがあります。

ダイナミックルートは、OSPF、BGP、EIGRP、IS-IS、またはRIPなどのルーティングプロトコルの動作を通じて学習されるものです。ルートを直接定義することはありません。その代わりにルーティングプロトコルを設定すると、システムはネイバールータと通信してルーティングアップデートを送信し、次にルーティングアップデートを受信します。

ダイナミック ルーティング プロトコルはルーティングテーブルを調整し、着信ルーティング更新メッセージを分析することで、ネットワーク状況の変化に対応します。ネットワークが変化したことをメッセージが示している場合は、システム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。

スタティックルーティングは単純であり、基本的なルーティングの目的を果たします。ネットワークトラフィックが比較的予想しやすい環境や、ネットワーク設計が比較的単純な環境での使用に適しています。ただし、編集しない限りスタティックルートは変更できないため、ネットワークの変化に対応することはできません。

小規模ネットワークがある場合を除き、通常はスタティックルートを1つまたは複数のダイナミック ルーティング プロトコルと組み合わせます。明示ルートに一致しないトラフィックのデフォルトルートとして、少なくとも1つのスタティックルートを定義します。



(注) スマート CLI を使用して次のルーティングプロトコルを設定することができます : OSPF。FlexConfig を使用して、ASA ソフトウェアでサポートされるその他のルーティングプロトコルを設定します。

ルーティング テーブルとルート選択

NAT 変換 (xlates) およびルールで出力インターフェイスを決定しない場合、システムはルーティングテーブルを使用してパケットのパスを決定します。

ルーティングテーブルのルートには、指定ルートに相対的な優先順位を定める「アドミニストレーティブディスタンス」というメトリックが含まれています。パケットが複数のルートエントリと一致する場合、最短距離のルートエントリが使用されます。直接接続されたネットワーク (インターフェイス上で定義されたネットワーク) の距離は0のため、これが常に優先されます。スタティックルートのデフォルトの距離は1ですが、1～254の距離で作成できます。

特定の宛先が指定されたルートは、デフォルトルート (宛先が0.0.0.0/0または::/0のルート) よりも優先されます。

ルーティング テーブルへの入力方法

FTD 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。FTD 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。

- FTD が、1つのルーティング プロトコル（RIP など）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。

- FTD 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、Firepower 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、Firepower Threat Defense デバイスがサポートす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
接続中のインターフェイス	0
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	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、Firepower 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、Firepower 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。

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、Firepower 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 Firepower 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、Firepower 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トリと一致しない場合、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つのエントリと一致した場合、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トリと一致し、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。

管理トラフィック用ルーティングテーブル

標準的なセキュリティ実践として、データトラフィックを管理トラフィックから分離しなければならない場合があります。この分離を実現するために、FTDは管理専用トラフィックとデータトラフィックに個別のルーティングテーブルを使用します。個別のルーティングテーブルは、データと管理用に別のデフォルトルートを作成できることを意味します。

デバイス間トラフィックでは、常にデータルーティングテーブルが使用されます。

デバイス間トラフィックでは、そのタイプに応じて、デフォルトで管理ルーティングテーブルまたはデータルーティングテーブルのいずれかが使用されます。デフォルトのルーティングテーブルで一致が見つからなかった場合は、他のルーティングテーブルがチェックされます。

デバイス間トラフィックの管理テーブルには、HTTP、SCP、TFTP、などを使用してリモートファイルを開く機能が含まれています。

データテーブルのデバイス間トラフィックには、ping、DNS、DHCPなどの他のすべての機能が含まれています。

デフォルトのルーティングテーブルにないインターフェイスに移動するために、ボックス内のトラフィックを必要とするとき、場合によっては、他のテーブルへのフォールバックに頼るのではなく、インターフェイスを設定するときにそのインターフェイスを指定する必要があります。FTDは、正しいルーティングテーブルをチェックし、そのインターフェイスのルートがないか調べます。たとえば、管理専用インターフェイスにpingを送信する必要がある場合は、ping機能でそのインターフェイスを指定します。そうではなく、データルーティングテーブルにデフォルトルートがある場合は、デフォルトルートに一致し、管理ルーティングテーブルにフォールバックすることは決してありません。

管理ルーティングテーブルは、データインターフェイスルーティングテーブルとは分離したダイナミックルーティングをサポートします。ダイナミックルーティングプロセスは管理専用インターフェイスまたはデータインターフェイスで実行されなければなりません。両方のタイプを混在させることはできません。

管理専用インターフェイスには、すべてのManagement x/x（「diagnostic」と名付けられた）インターフェイス、および管理専用として設定したすべてのインターフェイスが含まれています。



- (注) このルーティングテーブルは、FMCとの通信に使用する特別なFTD管理論理インターフェイスには影響しません。そのインターフェイスには独自のルーティングテーブルが備わっています。一方、診断論理インターフェイスは、この項で説明している管理専用ルーティングテーブルを使用します。



- (注) このルーティングテーブルは、ライセンスサーバとの通信またはデータベースの更新に使用する特別な FTD 管理仮想インターフェイスには影響を及ぼしません。このインターフェイスには独自のルーティングテーブルが備わっています。一方、診断物理インターフェイスは、この項で説明している管理専用ルーティングテーブルを使用します。

等コスト マルチパス (ECMP) ルーティング

Firepower 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 3 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 アドレスおよび宛先 IP アドレス、着信トラフィック、プロトコル、送信元ポートおよび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。

ECMPは複数のインターフェイス間ではサポートされないため、異なるインターフェイスで同じ宛先へのルートを定義することはできません。上記のルートのいずれかを設定すると、次のルートは拒否されます。

```
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.1
```

スタティック ルート

スタティックルートを作成して、ネットワークの基本的なルーティングを提供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、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 \(6 ページ\)](#) 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。

スタティックルーティングのガイドライン

ブリッジグループ

- 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。
- 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（syslog

またはSNMPなど)、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。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。

スタティック ルートの設定

システムのインターフェイスに直接接続されているネットワークに向かわないパケットの送信先をシステムに伝えるため、スタティック ルートを定義します。

少なくとも1つのスタティック ルート、ネットワーク 0.0.0.0/0 のデフォルト ルートが必要になります。このルートは、既存の NAT xlates (変換) またはスタティック NAT ルール、またはその他のスタティックルートでは出力インターフェイスを判別できないパケットの送信先を定義します。

デフォルト ゲートウェイを使用してもすべてのネットワークに到達できない場合、他のスタティック ルートが必要になる可能性があります。たとえば、デフォルト ルートは通常、外部インターフェイスの上流に位置するルータです。デバイスに直接接続されていない追加の内部ネットワークがあり、それらにデフォルトゲートウェイを介してアクセスできない場合、これらそれぞれの内部ネットワークに対してスタティック ルートが必要です。

システムのインターフェイスに直接接続されたネットワークのスタティックルートを定義することはできません。システムは自動でこれらのルートを作成します。

手順

ステップ 1 [デバイス (Device)] をクリックしてから、[ルーティング (Routing)] サマリーにあるリンクをクリックします。

ステップ 2 [ルーティングの選択 (Select Routing)] ページで、次のいずれかを実行します。

- 新しいルートを追加するには、[+] をクリックします。
- 編集するルートの編集アイコン (✎) をクリックします。

ルートが不要になったら、ルートの [ごみ箱 (trash can)] アイコンをクリックして削除します。

ステップ 3 ルート プロパティの設定

[名前 (Name)]

ルートの表示名。

説明

ルートの目的の説明 (オプション) 。

インターフェイス

トラフィックの送信を行うインターフェイスを選択します。ゲートウェイアドレスは、このインターフェイスを介してアクセス可能である必要があります。

ブリッジグループの場合、メンバー インターフェイスではなくブリッジグループ インターフェイス (BVI) のルートを設定します。

プロトコル

[IPv4] または [IPv6] アドレスのどちらのルートであるかを選択します。

ネットワーク

このルートのゲートウェイを使用する必要がある、宛先ネットワークまたはホストを特定するネットワーク オブジェクトを選択します。

デフォルト ルートを定義するには、事前定義された `any-ipv4` または `any-ipv6set` ネットワーク オブジェクトを使用するか、または `0.0.0.0/0` (IPv4) または `::/0` (IPv6) ネットワークのオブジェクトを作成します。

ゲートウェイ

ゲートウェイの IP アドレスを特定するホスト ネットワーク オブジェクトを選択します。トラフィックはこのアドレスに送信されます。複数のインターフェイス上のルートには同じゲートウェイを使用できません。

メトリック (Metric)

1~254 間のルートのアドミニストレーティブ ディスタンス。スタティック ルートのデフォルト値は1です。インターフェイスとゲートウェイの間に追加ルータがある場合、アドミニストレーティブ ディスタンスとしてホップ数を入力します。

アドミニストレーティブ ディスタンスは、ルートと比較するために使用されるパラメータです。番号が低いほど、ルートに高い優先順位が与えられます。接続されたルート (デバイスのインターフェイスに直接接続されているネットワーク) は、スタティックルートよりも常に優先されます。

ステップ 4 [OK] をクリックします。

ルーティングのモニタリング

ルーティングをモニタし、トラブルシューティングを行うには、CLI コンソールを開くか、またはデバイスの CLI にログインして、次のコマンドを使用します。

- **show route** はデータ インターフェイスのルーティング テーブルを表示します。直接接続されたネットワークのルートが含まれます。
- **show ipv6 route** はデータ インターフェイスの IPv6 ルーティング テーブルを表示します。直接接続されたネットワークのルートが含まれます。
- **show network** は仮想管理インターフェイスの設定を表示します。管理ゲートウェイが含まれます。仮想インターフェイスを介したルーティングは、データ インターフェイスを管理ゲートウェイに指定しなければ、データ インターフェイス ルーティング テーブルによって処理されません。

- **show network-static-routes** は、**configure network static-routes** コマンドを使用して仮想管理インターフェイスに対して設定されたスタティックルートを表示します。通常、ほとんどの場合、管理ゲートウェイは管理ルーティングに対して十分機能するため、スタティックルートは存在しません。これらのルートは、データ インターフェイス上のトラフィックには使用できません。このコマンドは、CLI コンソールでは使用できません。

