



Firepower Threat Defense のルーティングの概要

この章では、Cisco Firepower Threat Defense 内でのルーティング動作の基本概念と、サポートされているルーティングプロトコルについて説明します。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。

- [パスの決定 \(1 ページ\)](#)
- [サポートされるルート タイプ \(2 ページ\)](#)
- [Firepower Threat Defense 内でのルーティングの仕組み \(4 ページ\)](#)
- [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 \(6 ページ\)](#)
- [着信サービス一覧 \(Routing Table\) \(7 ページ\)](#)
- [管理トラフィック用ルーティングテーブル \(12 ページ\)](#)
- [ルート マップについて \(12 ページ\)](#)

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めます。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状態を通知します。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。Firepower 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。

Firepower Threat Defense 内でのルーティングの仕組み

Firepower Threat Defense デバイスは NAT の設定に応じて、ルーティングの判断のために、ルーティング テーブルまたは NAT (xlate) テーブルを使用します。

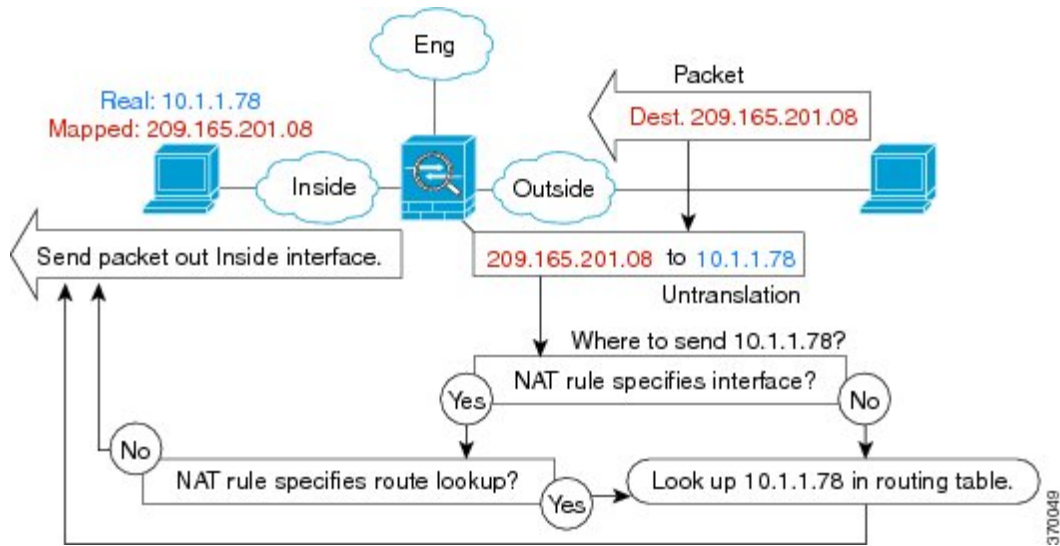
出インターフェイスの決定

NAT を使用していて、Firepower Threat Defense デバイスがマッピングアドレスのトラフィックを受信する場合、Firepower Threat Defense デバイスは NAT ルールに従って宛先アドレスを逆変換し、実際のアドレスにパケットを送信します。Firepower Threat Defense デバイスは、次の方法でパケットの出インターフェイスを決定します。

- トランスペアレント モードまたはルーテッドモードのブリッジグループ インターフェイス : Firepower Threat Defense デバイスは NAT ルールを使用して実際のアドレスの出インターフェイスを決定します。NAT ルールの一部として送信元、宛先のブリッジグループ メンバ インターフェイスを指定する必要があります。
- ルーテッドモードの通常インターフェイス : Firepower Threat Defense デバイスは、次のいずれかの方法で出インターフェイスを決定します。
 - NAT ルールでインターフェイスを設定する : Firepower Threat Defense デバイスは NAT ルールを使用して出インターフェイスを決定します。ただし、代わりにオプションとして常にルート ルックアップを使用することもできます。一部のシナリオでは、ルート ルックアップの上書きが必要になる場合があります。
 - NAT ルールでインターフェイスを設定しない : Firepower Threat Defense デバイスはルート ルックアップを使用して出インターフェイスを決定します。

次の図に、ルーテッドモードでの出インターフェイスの選択方法を示します。ほとんどの場合、ルート ルックアップは NAT ルールのインターフェイスと同じです。ただし、一部の構成では、2つの方法が異なる場合があります。

図 1: NATによるルーテッドモードでの出カインターフェイスの選択



ネクスト ホップの選択プロセス

前述のいずれかの方法を使用して出カインターフェイスを選択した後、さらにルートルックアップが実行され、これまでに選択した出カインターフェイスに属する適切なネクストホップが検出されます。選択されたインターフェイスに明示的に属するルートがルーティングテーブルにない場合は、パケットがドロップされてレベル 6 の syslog メッセージ 110001（ホストへのルートなし）が生成されます（別の出カインターフェイスに属する、指定の宛先ネットワークへの別のルートがあるかどうかにかかわらず）。選択した出カインターフェイスに属するルートが見つかり、パケットは対応するネクストホップに転送されます。

Firepower Threat Defense デバイスでのロードシェアリングは、1つの出カインターフェイスを使用して複数のネクストホップが使用できる場合に限り可能です。ロードシェアリングでは、複数の出カインターフェイスの共有はできません。

ダイナミックルーティングが Firepower Threat Defense デバイスで使用されており、XLATE の作成後にルートテーブルが変更された場合も（ルートフラップなど）、宛先変換トラフィックは、XLATE がタイムアウトするまでは、ルートテーブルではなく古い XLATE を使用して転送されます。トラフィックが、正しくないインターフェイスに転送されたり、ドロップされてレベル 6 の syslog メッセージ 110001（ホストへのルートなし）が生成されたりすることもあります（ルーティングプロセスによって古いルートが古いインターフェイスから削除されて別のインターフェイスに接続された場合）。

Firepower Threat Defense デバイス自体でルートフラップが発生していないにもかかわらず、その周りで一部のルーティングプロセスがフラッピングし、発信元変換された、同じフローに属するパケットを、別のインターフェイスを使用して Firepower Threat Defense デバイス経由で送信する場合は、同様の問題が発生することがあります。宛先変換された返送パケットは、間違った出カインターフェイスを使用して戻されることがあります。

セキュリティトラフィック構成によっては、この問題が高い確率で発生します。具体的には、ほぼすべてのトラフィックが、フローの最初のパケットの方向に応じて、発信元変換されるか宛先変換されるような構成です。ルートフラップの後にこの問題が発生した場合は、XLATEのタイムアウトによって自動的に解決することもできます。XLATEのタイムアウトは、必要に応じて小さくできます。この問題がほとんど発生しないようにするには、Firepower Threat Defense デバイス やその周りでルートフラップが発生しないようにします。つまり、同じフローに属する宛先変換されたパケットが必ず同じ方法でFirepower Threat Defense デバイス を通して転送されることを確認します。

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
```

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

Firepower 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。カスタマーは ISP に接続し、ISP は BGP を使用してカスタマーおよび ISP 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。

着信サービス一覧 (Routing Table)

ここでは、ルーティングテーブルについて説明します。

ルーティング テーブルへの入力方法

Firepower Threat Defense デバイス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。Firepower 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。

- Firepower Threat Defense デバイスが、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。

- Firepower 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への異なるルートが複数存在する場合に、ASA がベスト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、ASA がサポートす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]

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
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
RIP	120
EIGRP 外部ルート	170
内部 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、ASA が OSPF ルーティングプロセス（デフォルト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、ASA 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、ASA 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 を通し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ために **distance-ospf** コマンドを使用する場合、その変更は、コマンドが入力された ASA 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。EIGRP、OSPF、RIP および BGP ルーティングプロセスは、そのルーティングプロセスによって検出されたルートまたはそのルーティングプロセスに再配布されたルートのみ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、ASA 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せん。

バックアップルート

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。

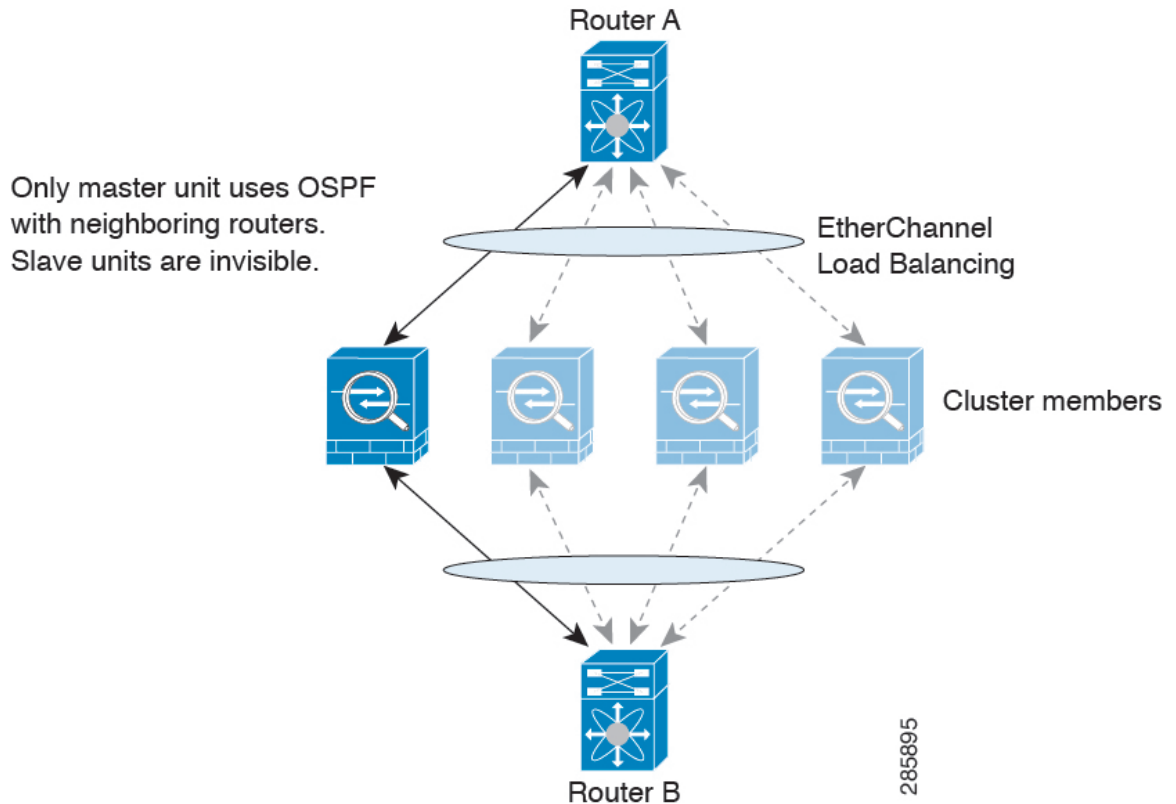
ダイナミック ルーティングおよび高可用性

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 プロセスはマスター ユニット上だけで実行されます。ルートはマスター ユニットの介して学習され、スレーブに複製されます。ルーティング パケットがスレーブに到着した場合は、マスター ユニットにリダイレクトされます。

図 2: クラスタリングでのダイナミック ルーティング



スレーブ メンバがマスター ユニットからルートを学習した後は、各ユニットが個別に転送に関する判断を行います。

OSPF LSA データベースは、マスター ユニットからスレーブ ユニットに同期されません。マスター ユニットのスイッチオーバーが発生した場合は、隣接ルータ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。

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、Firepower Threat Defense デバイス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。

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。

HTTP、SCP、TFTP などを使用してリモートファイルを開くすべての機能に関しては、インターフェイスを指定していない場合、Firepower Threat Defense デバイスは管理専用ルーティングテーブルを確認します。一致がない場合はデータルーティングテーブルを確認します。

その他のすべての機能に関しては、インターフェイスを指定しなかった場合、Firepower Threat Defense デバイスはデータルーティングテーブルを確認し、一致するものが見つからなければ、管理専用ルーティングテーブルを確認します。たとえば、ping、DNS、DHCP などがあります。

管理専用インターフェイスには、すべての診断 x/x 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。

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を使用します。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を評価します。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。