ルーティングの基本ルートと静的ルート

システムでは、ルーティング テーブルを使用して、システムに入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静的ルーティングを設定する方法について説明します。

ルーティングのベストプラクティス

ネットワーク内のルーティングプロセスの設計は、複雑なプロセスになる可能性があります。この章では、脅威に対する防御 デバイスを、既存のネットワーク内で機能するように、およびネットワークですでに確立されているルーティングプロセスに参加するように設定していることを前提にしています。

そうではなく、新しいネットワークを作成している場合は、ルーティングプロトコルについて説明している箇所、およびネットワークに適した効果的なルーティング計画を設計する方法について説明している箇所を参照してください。この章では、プロトコルを選択するための推奨事項については説明しません。また、プロトコルの動作についても詳しく説明しません。

ネットワークが非常に小規模で、単に ISP にリンクするだけの場合は、少数のスタティックルートで十分であり、ルーティングプロトコルを実装する必要はまったくありません。

一方、多数のルータを含む大規模なネットワークを設定する場合は、内部ルーティング用に OSPF などのルーティングプロトコルを少なくとも 1 つ実装する必要があることが多く、場合によっては外部ルーティング用に BGP などのルーティングプロトコルを 1 つ実装する必要があります。サービスプロバイダーは、どのような外部ルーティングが必要になるかを理解する場合の助けになります。この状況に該当する場合は、まず 脅威に対する防御 を使用して設定可能なルーティングプロトコルを理解し、ネットワークを計画し、最後に計画に従って 脅威に対する防御 デバイスを設定します。

ルーティングの概要

ここでは、脅威に対する防御 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、発信元から宛先にネットワーク経由で情報を移動する動作のことです。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、ネットワーク経由で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。

サポートされるルーティング プロトコル

次の表では、Device Manager を使用して Threat Defense デバイスで設定できるルーティングプロトコルとテクノロジー、および設定を完了するために使用する必要があるメソッドについて説明します。

表 *1:* サポートされるルーティング プロトコル

ルーティング機能	設定方法	注記
BGP	スマート CLI	**[デバイス（Device）]** > **[ルーティング（Routing）]** ページから BGP スマート CLI オブジェクトを設定します。 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** ページで、スマート CLI オブジェクトを使用してルートマップなどの BGP で使用されるオブジェクトを設定します。
Bidirectional Forwarding Detection（BFD）	FlexConfig	**[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** ページで、FlexConfig オブジェクトを使用して BFD を設定します。BFD は BGP でのみサポートされています。
EIGRP	スマートCLI	**[デバイス（Device）]** > **[ルーティング（Routing）]** ページで、EIGRP スマート CLI オブジェクトを設定します。 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** ページで、スマート CLI オブジェクトを使用してルートマップなどの EIGRP で使用されるオブジェクトを設定します。
IS-IS	FlexConfig	**[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** ページで、FlexConfig オブジェクトを使用して IS-IS を設定します。
マルチキャスト ルーティング	FlexConfig	**[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** ページで、FlexConfig オブジェクトを使用してマルチキャストルーティングを設定します。

ルーティング機能	設定方法	注記
OSPFv2	スマートCLI	**[デバイス（Device）]** > **[ルーティング（Routing）]** ページから OSPFv2 スマート CLI オブジェクトを設定します。 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** ページで、スマート CLI オブジェクトを使用してルートマップなどの OSPFv2 で使用されるオブジェクトを設定します。
OSPFv3	—	OSPFv3設定はサポートされていません。
ポリシーベースルーティング（PBR）	FlexConfig	**[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** ページで、FlexConfig オブジェクトを使用してポリシーベースルーティング（PBR）を設定します。
RIP	FlexConfig	**[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** ページで、FlexConfig オブジェクトを使用して RIP を設定します。
スタティックルート	Device Manager	**[デバイス（Device）]** > **[ルーティング（Device Routing）]** ページからスタティックルートをグローバルに、または仮想ルータごとに設定します。
仮想ルータ、VRF	Device Manager	**[デバイス（Device）]** > **[ルーティング（Device Routing）]** ページから仮想ルータを設定します。

ルート タイプ

ルートには、スタティックとダイナミックという2つのタイプがあります。

スタティックルートは、明示的に定義するものです。これらは安定した、通常は優先順位の高いルートであり、ルートの宛先へのトラフィックが常に正しいインターフェイスから送信されるようにするために使用します。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。ルートは直接定義しません。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、ルーティングアップデートを順番に受信します。

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 アップデート 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、BGP。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。パケットに一致するルート エントリが複数ある場合、最も短い距離のルート エントリが使用されます。直接接続ネットワーク（インターフェイスで定義される）の距離は0のため、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

Threat Defense ルーティングテーブルには、静的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。メトリックス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、他のプロトコルと異なるアルゴリズムに基づいた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つのルートのいずれが最適パスであるかは、必ずしも判別できません。

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 *2:* サポートされ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

ルートの送信元	デフォルトの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

ルートの送信元	デフォル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	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、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/RRI）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 ルーロとフローティング 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しまい、インストールできなかった場合に、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順位の高い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た場合は、パケットが、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た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でインターフェイスに到着するとします。

- 192.168.32.0/24 ゲートウェイ 10.1.1.2
- 192.168.32.0/19 ゲートウェイ 10.1.1.3

この場合、192.168.32.1 は 192.168.32.0/24 ネットワーク内にあるため、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。もうひとつのルートにもあてはまりますが、192.168.32.0/24 の方が長いプレフィックスを持つためです（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る。

（注） 既存の接続は、新しい同様の接続がルートの変更により異なる動作になる場合でも、引き続き確立されたインターフェイスを使用します。

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：Device Manager 管理セッション、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 ルックアップと ICMP（ping およびトレースルート）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します。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。

Equal-Cost Multipath（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、および10.1.1.4間の外部インターフェイスでロードバランシングされます。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 つの等コストの静的または動的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、等コストルートを自動的に設定できます。Threat Defense デバイス 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のトラフィックのロードバランシングを行います。

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。

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。

- ネットワークでサポートされていないルータ検出プロトコルが使用されている。
- 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。
- デフォルトルートでは十分でない場合がある。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。

スタティック ルートのバックアップとスタティック ルートのトラッキング

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、関連付けられたインターフェイスがダウンした場合にのみルーティングテーブルから削除されます。

トラッキングルートを実装すると、サービス レベル契約（SLA）モニタを使用してスタティック ルートの可用性を追跡し、プライマリ ルートが失敗したら自動的にバックアップ ルートをインストールすることができます。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。

ルートトラッキングを使用する場合、トラッキング対象のルートに宛先ネットワークのターゲット IP アドレスを関連付けます。その後、システムは ICMP エコー要求を使用して、アドレスにアクセスできることを定期的に確認します。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。

したがって、デフォルトルートなどの特定の宛先にバックアップ スタティック ルートを使用するには、次を実行する必要があります。

1. ゲートウェイや always-up サーバ（Web サーバや syslog サーバなど）のような、宛先ネットワーク上の信頼できる IP アドレスをモニタする SLA モニタを作成します。宛先ネットワークが正常で使用可能な間は、オフラインになる可能性があるシステムのIPアドレスをモニタしないでください。「SLA モニタ オブジェクトの設定 （14 ページ）」を参照してください。
2. 宛先へのプライマリ ルートを作成し、ルートの SLA モニタを選択します。このルートのメトリックは通常1です。「スタティック ルートの設定 （12 ページ）」を参照してください。
3. プライマリルートが失敗した場合に使用されるバックアップ スタティック ルートを作成します。このルートには、プライマリルートより大きいメトリックが必要です。たとえば、プライマリルートが 1 の場合、バックアップルートは 10 にできます。また、通常はバックアップ ルートとは異なるインターフェイスを選択します。

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は指定できません。
- 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 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）、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 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

- スタティックルートトラッキング(SLAモニタ)は、IPv6ではサポートされていません。

等コストマルチパス（ECMP）トラフィックゾーン

- ECMP トラフィックゾーンのメンバーインターフェイスを同じセキュリティゾーンに保持して、これらのインターフェイスに異なるアクセスルール、SSL ルール、または ID ルールが適用されないようにします。
- 特定の ECMP トラフィックゾーンのネットワークには最大 8 つの等コストルートを設定できます。
- 最大256のECMPトラフィックゾーンを作成でき、ゾーンごとに最大8つのインターフェイスを使用できます。
- ECMPゾーンには、物理インターフェイス、サブインターフェイス、およびEtherChannelを含めることができます。次のものを含めることはできません。
  - ブリッジグループ（BVI）またはそのメンバー
  - EtherChannel メンバーインターフェイス
  - HA インターフェイス（フェールオーバーまたはステートリンク）
  - 管理専用インターフェイス
  - サイト間 VPN 接続またはリモートアクセス VPN 接続に使用されるインターフェイス。
  - 仮想トンネルインターフェイス（VTI）またはその送信元インターフェイス。
  - VPN 管理アクセス用に設定されたインターフェイス。
- ゾーン内のインターフェイスで DHCP リレー を有効にできません。

スタティック ルートの設定

システム上のインターフェイスに直接接続されたネットワークに向かわないパケットをどこに送信すべきかをシステムに指示するには、スタティック ルートを定義します。

ネットワーク 0.0.0.0/0 用の少なくとも 1 つのスタティック ルート（デフォルト ルート）が必要です。このルートは、既存の NAT xlates（変換）、スタティック NAT ルール、その他のスタティック ルートによって出力インターフェイスを判定できないパケットをどこに送信するかを定義します。

すべてのネットワークに到達するためにデフォルト ゲートウェイを使用できない場合は、他のスタティック ルートが必要になることがあります。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アップストリーム（上流）ルータです。デバイスに直接接続されない内部ネットワークが別に存在し、デフォルト ゲートウェイ経由でそれらにアクセスできない場合、このような内部ネットワークそれぞれにスタティック ルートが必要になります。

システム インターフェイスに直接接続されるネットワークにスタティック ルートを定義することはできません。これらのルートは、システムによって自動的に作成されます。

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 仮想ルータを有効にした場合は、スタティック ルートを設定しているルータの表示アイコン（）をクリックします。

ステップ 3 [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場合は、ルートのごみ箱アイコンをクリックして削除します。

ステップ 4 ルート プロパティの設定

- [名前]: ルートの表示名。
- [説明]: ルートの目的の任意の説明。
- [インターフェイス]: トラフィックの送信経路となるインターフェイスを選択します。このインターフェイス経由でゲートウェイ アドレスにアクセスできる必要があります。

  ブリッジグループの場合は、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。

  仮想ルーティングとフォワーディングを有効にしている場合は、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。別の仮想ルータ内のインターフェイスの仮想ルータでスタティックルートを作成すると、そのルートは仮想ルータの境界を越え、この仮想ルータからのトラフィックが別の仮想ルータにリークするリスクがあります。望ましい結果である可能性もありますが、このルートリークが必要かどうかを慎重に判断してください。インターフェイスを選択すると、インターフェイスが属する仮想ルータの名前がインターフェイスの右側に表示されます。
- [プロトコル]: ルートがIPv4アドレス用かIPv6アドレス用かを選択します。
- [ネットワーク]: このルートでゲートウェイを使用する必要のある宛先ネットワークまたは宛先ホストを識別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-ipv6 ネットワーク オブジェクトを使用するか、0.0.0.0/0（IPv4）または ::/0（IPv6）ネットワーク用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アドレスを識別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。

  仮想ルータでルートを定義し、そのインターフェイスが別の仮想ルータに属している場合は、ゲートウェイを空のままにしておく必要があります。これらのネットワークへのトラ

フィックは他の仮想ルータにルーティングされ、ターゲット仮想ルータのルーティングテーブルを使用してゲートウェイが決定されます。

- [メトリック]: ルートのアドミニストレーティブディスタンス。1～254の範囲で指定します。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のルータが存在する場合は、ホップの数をアドミニストレーティブディスタンスとして入力します。

  アドミニストレーティブディスタンスは、ルートを比較するのに使用されるパラメータです。値が小さいほど、そのルートの優先順位は高くなります。接続済みのルート（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、必ずスタティックルートより優先順位が高くなります。

ステップ 5 （任意、IPv4 ルートのみ）このルートの有効性を追跡する [SLAモニタ（SLA Monitor）] を選択します。

SLAモニタでは、ターゲットネットワーク上の常時利用可能なホストが到達可能であることを確認できます。到達不能になった場合、システムはバックアップルートをインストールできます。したがって、SLA モニタを設定する場合は、このネットワークに対してより大きなメトリックを持つ別のスタティックルートも設定する必要があります。たとえば、このルートのメトリックが 1 である場合は、メトリック 10 のバックアップルートを作成します。詳細については、「スタティック ルートのバックアップとスタティック ルートのトラッキング（10 ページ）」を参照してください。

SLA モニタ オブジェクトがまだ存在しない場合は、リストの下部にある [SLA モニタの作成（Create SLA Monitor）] リンクをクリックしてここで作成します。

（注）
モニタ対象のアドレスが ping できないことが原因でモニタ対象のルートが削除された場合、このルートは、ルートが到達不能であることを示す警告とともにスタティックルートテーブルに示されます。問題が一時的なものであるか、またはルートを再設定する必要があるかどうかを確認します。ルートが有効でも、監視対象のアドレスが十分に信頼できない可能性もあります。

ステップ 6 **[OK]** をクリックします。

SLA モニタ オブジェクトの設定

スタティックルートとともに使用するためのサービスレベル契約（SLA）モニタオブジェクトを設定します。SLAモニタを使用すると、スタティックルートの状態を追跡し、失敗したルートを自動的に新しいものに交換できます。ルートトラッキングの詳細については、スタティック ルートのバックアップとスタティック ルートのトラッキング（10 ページ）を参照してください。

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。ターゲットには、ホストネットワークオブジェクトで定義された任意のIPアドレスを指定できますが、次の使用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(ゲートウェイの可用性に懸念がある場合)。
- システムが通信する必要があるターゲット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IPアドレス。夜間にシャットダウンされる可能性のあるワークステーションは、適切な選択肢ではありません。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [SLAモニタ（SLA Monitors）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ 3 オブジェクトの名前、さらにオプションで説明を入力します。

ステップ 4 SLAモニタの必須オプションを定義します。

- [モニタアドレス（Monitor Address）]：宛先ネットワークでモニタするアドレスを定義するホスト ネットワーク オブジェクトを選択します。必要なオブジェクトが存在しない場合は、[新しいネットワークの作成（Create New Network）] をクリックします。

  このアドレスは、SLAモニタをスタティックルートに接続している場合にのみモニタされます。

- [ターゲットインターフェイス（Target Interface）]：エコー要求パケットを送信する際に通過するインターフェイスを選択します。これは通常、スタティックルートを定義するインターフェイスになります。インターフェイス送信元アドレスが、エコー要求パケットの送信元アドレスとして使用されます。

ステップ 5 （オプション）。[IP ICMPエコーオプション（IP ICMP Echo Options）] を調整します。

すべてのICMPオプションには、ほとんどの場合に適合するデフォルトがありますが、要件に合わせて調整できます。

- [しきい値（Threshold）]：宣言する上昇しきい値（ミリ秒）（0 ～ 2147483647 の間）。デフォルト値は5,000（5秒）です。この値は、タイムアウトに設定された値以下にする必要があります。しきい値は、しきい値超過イベントを示すためにだけ使用されます。到達可能性には影響しません。しきい値イベントの頻度を使用すると、タイムアウトの設定を評価できます。

- [タイムアウト（Timeout）]：ルート監視操作が要求パケットからの応答を待つ時間（ミリ秒）（0 ～ 604800000 ミリ秒（7 日間）の間）。デフォルト値は5000ミリ秒(5秒)です。モニタがこの期間中に少なくとも 1 つのエコー要求への応答を受信しなかった場合、プロセスはバックアップ ルートをインストールします。
- [頻度]: SLAプローブ間のミリ秒数(1000ー604800000、1000の倍数単位)。タイムアウト値未満の頻度は設定できません。デフォルトは60000ミリ秒(60秒)です。
- [サービスタイプ（Service Type）]：ICMP エコー要求パケットの IP ヘッダーの Type of Service（ToS）タイプを定義する整数（0 ～ 255 の間）。デフォルトは 0 です。
- [パケットの数（Number of Packets）]：各ポーリングを送信するパケットの数（1 ～ 100 の間）。デフォルトは 1 パケットです。
- [データサイズ（Data Size）]：エコー要求パケットで使用するデータ ペイロードのサイズ（0 ～ 16384 バイトの間）。デフォルト値は 28 です。この設定では、ペイロードのサイズだけが指定されます。パケット全体のサイズは指定されません。

ステップ 6 [OK]をクリックします。

これで、スタティック ルートで SLA モニタ オブジェクトを使用することができます。

ECMP トラフィックゾーンの設定

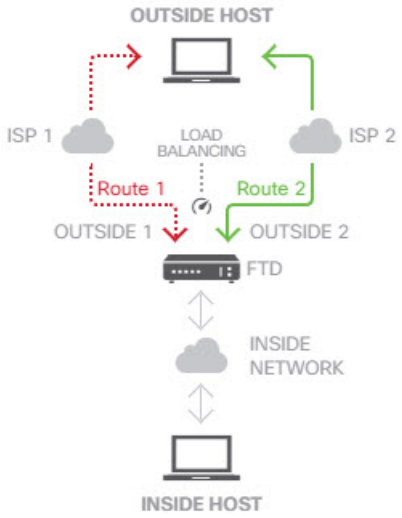
通常、同じルートメトリックを使用して特定のネットワークプレフィックスに複数のルートを設定するには、同じインターフェイスでルートを設定する必要があります。そのため、システムは、等コストマルチパス（ECMP）ルーティング計算を使用して、インターフェイス経由でゲートウェイに送信されるトラフィックのロードバランシングを実現します。

たとえば、次のように、異なるゲートウェイを指定する複数のデフォルトルートを外部インターフェイスに設定でき、この設定は追加の変更なしで許可されます。

```
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
```

また、ECMP を使用して、同じネットワークプレフィックスおよびルートメトリックの複数のインターフェイス（仮想ルータ内）間でトラフィックのバランシングを実現することもできます。この設定は、複数の個別インターフェイスを介してゲートウェイにアクセスできる場合に必要です。たとえば、ISP が 2 つあり、ISP 間でロードバランシングを行いたいものの、ISP ゲートウェイ間で内部アドレス空間を分割したくないとします。一方の ISP には outside1 インターフェイスを介してアクセスでき、もう一方の ISP には outside2 インターフェイスを介してアクセスできます。これを実現するには、outside1 インターフェイスと outside2 インターフェイスを含むルーティング トラフィック ゾーンを作成する必要があります。

```
isp-zone containing outside1 and outside2
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 10.1.1.3
```



（注） ECMP ルーティング トラフィック ゾーンはセキュリティゾーンに関連していません。outside1 インターフェイスと outside2 インターフェイスを含むセキュリティゾーンを作成しても、ECMP ルーティング用のトラフィックゾーンは実装されません。

次の手順で、インターフェイス間で ECMP 処理を利用するように ECMP ゾーンを設定する方法について説明します。

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 仮想ルータを有効にした場合は、スタティック ルートを設定しているルータの表示アイコン（）をクリックします。

ステップ 3 [ECMP トラフィックゾーン（ECMP Traffic Zones）] タブをクリックします。

ステップ 4 [ECMP トラフィックゾーン（ECMP Traffic Zones）] ページで、次のいずれかを実行します。

- 新しいゾーンを追加するには、[+] または [ECMP トラフィックゾーンの追加（Add ECMP Traffic Zone）] をクリックします。
- 編集するゾーンの編集アイコン（）をクリックします。

ゾーンが不要になった場合は、ゾーンのごみ箱アイコンをクリックして削除します。ゾーンを削除する前に、そのゾーンに依存するすべての静的ルートを削除する必要があります。

ステップ 5 ゾーンの [名前（Name）] を入力し、必要に応じて説明を入力します。

ステップ 6 [インターフェイス（Interfaces）] で、ゾーンに含める最大 8 つのインターフェイス選択します。

- インターフェイスを追加する場合は、[+] をクリックします。
- 削除するには、インターフェイスの右横にある [x] をクリックします。

インターフェイスを選択する際は、次の制限事項に注意してください。

- 物理インターフェイス、サブインターフェイス、および EtherChannel を選択できます。
- ECMP トラフィックゾーンに含めることのできないインターフェイスのタイプは、ブリッジ グループ（BVI）やそのメンバー、Etherchannel メンバー インターフェイス、HA インターフェイス（フェールオーバー リンクまたはステート リンク）、管理専用インターフェイス、またはVPN 管理アクセス用に設定されたインターフェイスです。
- リモートアクセスまたはサイト間 VPN 接続で使用されるインターフェイスを含めることはできません。
- DHCP リレーが有効になっているインターフェイスは、サーバまたはエージェントとして選択できません。
- インターフェイスは同じ仮想ルータに割り当てる必要があります。
- 1 つのインターフェイスは 1 つのトラフィックゾーンにのみ含まれます。

ステップ 7 [OK] をクリックします。

次のタスク

これで、[静的ルート（Static Routes）] タブに移動し、これらのインターフェイスを介した同じ宛先への等コストルートを作成できます。または、動的ルーティングプロトコルがシステムを通じて配布される場合、等コストルートを自動的に設定できます。

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、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。また、[ルーティング（Routing）] ページの [コマンド（Commands）] メニューから、これらのコマンドの一部を選択することもできます。

- **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。管理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として指定しない限り、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、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、管理ルーティングでは、管理ゲートウェイで十分であるため、スタティック ルートはありません。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。
- **show ospf** は OSPF プロセスと学習ルートに関する情報を表示します。OSPF に関する特定の情報を表示するために含めることができるオプションのリストを取得するには、**show ospf ?** を使用します。
- **show bgp** は BGP プロセスと学習ルートに関する情報を表示します。BGP に関する特定の情報を表示するために含めることができるオプションのリストを取得するには、**show bgp ?** を使用します。
- **show eigrp** *option* は EIGRP プロセスと学習ルートに関する情報を表示します。含めることができるオプションのリストを取得するには、**show eigrp ?** を使用します。オプションを指定する必要があります。
- **show isis** *option* は IS-IS プロセスと学習ルートに関する情報を表示します。含めることができるオプションのリストを取得するには、**show isis ?** を使用します。オプションを指定する必要があります。
- **show rip database** は RIP プロセスと学習ルートに関する情報を表示します。
- **show vrf** システムで定義されている仮想ルータの情報を表示します。
- **show zone** は ECMP トラフィックゾーンに関する情報（各ゾーンに含まれるインターフェイスなど）を表示します。

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。