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

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 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 （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ければ、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限りルーティングテーブルから削除されます。

ルート トラッキングを実装すると、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. ゲートウェイや常時稼働サーバ（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かつ使用可能な状態の間にオフラインになる可能性のあるシステムの IP アドレスはモニタしません。SLA モニタ オブジェクトの設定 （12 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 とする必要があります。スタティック ルートの設定 （10 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 の場合は、バックアップルートは 10 などが考えられます。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 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。

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

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

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、ルートを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 （オプション、IPv4 ルートのみ）。このルートの有効性を追跡する**SLA モニタ**を選択します。

SLA モニタは、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、このルートにメトリック 1 がある場合は、メトリック 10 を使用してバックアップ 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 （8 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 できないためにモニタ対象のルートが削除された場合は、そのルートがスタティック ルート テーブルに示され、ルートが到達不能であることを示す警告が表示されます。問題が一時的なものなのか、またはルートを再設定する必要があるかを判断してください。ルートが有効であるが、モニタ対象のアドレスが十分に信頼できるものではない可能性があることを考慮してください。

ステップ 5 [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 （8 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。対象はホスト ネットワーク オブジェクトで定義されている任意の IP アドレスとすることができますが、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（ゲートウェイの使用可能状況に懸念がある場合）。
- システム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 IP アドレス。夜間にシャットダウンすることがあるワークステーションは適しません。

手順

ステップ 1 [オブジェクト（Objects）] を選択して、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 モニタに必要な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。

- [インターフェイス（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。

ICMP オプションにはすべてデフォルト値があり、ほとんどの場合それらは適切ですが、要件に合わせて調整することができます。

- [しきい値（Threshold）]：宣言する上昇しきい値（ミリ秒）（0 ～ 2147483647 の間）。デフォルトは 5000（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、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（Frequency）]：SLA プローブ間のミリ秒数（1000 ～ 604800000、1000の倍数）。タイムアウト値未満の頻度を設定することはできません。デフォルト値は 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。

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。