



スタティックルートとデフォルトルート

この章では、ASA 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 \(4 ページ\)](#)
- [デフォルトルートおよびスタティックルートの設定 \(5 ページ\)](#)
- [スタティックルートまたはデフォルトルートのモニタリング \(8 ページ\)](#)
- [スタティックルートまたはデフォルトルートの例 \(9 ページ\)](#)
- [スタティックルートおよびデフォルトルートの履歴 \(9 ページ\)](#)

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、ASA 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。

ASA デバイスはデータトラフィックと管理トラフィックに個別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専用またはデータルーティングテーブルが使用されます。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せん。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、ASA 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ドロップするための 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転送することで、トラフィックをドロップできます。

スタティック null0 ルートには、推奨パフォーマンス プロファイルが割り当てられます。また、スタティック null0 ルートを使用して、ルーティング ループを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。

- 宛先かつアドミンス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。

トランスパアレントファイアウォールモードおよびブリッジグループのルート

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ASAで発信されるトラフィックの場合、ASA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。ASAで発信されるトラフィックには、syslogサーバーまたはSNMPサーバーへの通信が含まれることもあります。1つのデフォルトルートで到達できないサーバーがある場合、スタティックルートを設定する必要があります。トランスパ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、[#unique_1107](#)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、ASA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。

ASAでは、ASA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）
- ASA が通信を行う必要のある対象ネットワーク上のサーバー（syslog サーバーなど）
- 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有効化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は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。

サポートされるネットワークアドレス

- 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。
- ASA はクラス E ルーティングをサポートしていません。したがって、クラス E ネットワークはスタティックルートとしてルーティングできません。

クラスタリングとマルチコンテキストモード

- クラスタリングでは、スタティックルートトラッキ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トラッキングはマルチコンテキストモードではサポートされません。

ASP および RIB ルートエントリ

デバイスにインストールされているすべてのルートとその距離は、ASPルーティングテーブルにキャプチャされます。これは、すべての静的および動的ルーティングプロトコルに共通です。最適な距離のルートのみが RIB テーブルにキャプチャされます。

デフォルトルートおよびスタティックルートの設定

少なくとも1つのデフォルトルートを設定する必要があります。また、スタティックルートの設定が必要になる場合があります。このセクションでは、デフォルトルートの設定、スタティックルートの設定、スタティックルートの追跡を行います。

デフォルトルートの設定

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。この手順に従って手動で設定するか、DHCP サーバーや他のルーティングプロトコルから取得するかに関わらず、デフォルトルートは必ず設定する必要があります。

始める前に

[Tunneled] オプションについては、次のガイドラインを参照してください。

- トンネルルートの出力インターフェイスで、ユニキャスト RPF を有効にしないでください。この設定を行うと、セッションでエラーが発生します。
- トンネルルートの出力インターフェイスで、TCP 代行受信をイネーブルにしないでください。この設定を行うと、セッションでエラーが発生します。
- これらのインスペクションエンジンはトンネルルートを無視するため、トンネルルートで VoIP インスペクションエンジン (CTIQBE、H.323、GTP、MGCP、RTSP、SIP、SKINNY)、DNS インスペクションエンジン、または DCE RPC インスペクションエンジンを使用しないでください。
- tunneled オプションで複数のデフォルトルートを定義することはできません。
- トンネルトラフィックの ECMP はサポートされません。
- トンネルルートは、通過トラフィックの VPN 終端をサポートしないブリッジグループではサポートされません。

手順

- ステップ 1** [Configuration] > [Device Setup] > [Routing] > [Static Routes] を選択し、[Add] をクリックします。
- ステップ 2** [IP Address Type]、[IPv4]、または [IPv6] を選択します。
- ステップ 3** 特定の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。

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指定します。ブリッジグループでルーテッドモードを使用する場合は、BVI名を指定します。

ステップ4 ネットワークの場合は、そのタイプに応じて **any4** または **any6** を入力します。

ステップ5 トラフィックを送信する **ゲートウェイ IP** を入力します。

ステップ6 **メトリック**を設定して、ルートのアドミニストレティブディスタンスを設定します。

デフォルトは **1** です。アドミニストレティブディスタンスは、複数のルーティングプロトコル間でルートと比較するのに使用されるパラメータです。スタティックルートのデフォルトのアドミニストレ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7 (オプション) [Options] 領域で、以下を設定します。

- [Tunneled] : 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。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、ASA 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。このオプションは、ブリッジグループではサポートされません。
- [Tracked] : (IPv4 のみ) ルートのトラッキングについては、[スタティックルートトラッキングの設定 \(7 ページ\)](#) を参照してください。

ステップ8 [OK] をクリックします。

スタティックルートの設定

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。

手順

ステップ1 [Configuration] > [Device Setup] > [Routing] > [Static Routes] を選択し、[Add] をクリックします。

ステップ2 [IP Address Type]、[IPv4]、または [IPv6] を選択します。

ステップ3 特定の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。

不要なトラフィックをドロップするには、[Null0]インターフェイスを選択します。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指定します。ブリッジグループでルーテッドモードを使用する場合は、BVI名を指定します。

ステップ4 ネットワークの場合は、トラフィックをルーティングする宛先ネットワークを入力します。

ステップ5 トラフィックを送信するゲートウェイ IP を入力します。

ステップ6 メトリックを設定して、ルートのアドミニストレーティブディスタンスを設定します。

デフォルトは1です。アドミニストレーティブディスタンスは、複数のルーティングプロトコル間でルートと比較するのに使用されるパラメータです。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7 (オプション) [Options] 領域で、以下を設定します。

- [Tunneled] : 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。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、ASA 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。
- [Tracked] : (IPv4 のみ) ルートのトラッキングについては、[スタティックルートトラッキングの設定 \(7 ページ\)](#) を参照してください。

ステップ8 [OK] をクリックします。

スタティックルートトラッキングの設定

スタティックルートトラッキングを設定するには、次の手順を実行します。

手順

ステップ1 [Configuration] > [Device Setup] > [Routing] > [Static Routes] の順に選択し、[スタティックルートの設定 \(6 ページ\)](#) に従ってスタティックルートを追加または編集します。

ステップ2 [Options] 領域で [Tracked] オプション ボタンをクリックします。

ステップ3 [Track ID] フィールドに、ルートトラッキングプロセスの固有識別子を入力します。

ステップ4 [Track IP Address/DNS Name] フィールドに、追跡対象のIPアドレスまたはホスト名を入力します。これは通常、このルートのネクストホップゲートウェイのIPアドレスになりますが、そのインターフェイスから利用できる任意のネットワークオブジェクトとすることもできます。

ステップ5 [SLA ID] フィールドに、SLA モニタリング プロセスの固有識別子を入力します。

ステップ6 (任意) [Monitoring Options] をクリックします。

[Route Monitoring Options] ダイアログボックスが表示されます。ここから、次のトラッキングオブジェクトのモニタリングプロパティを変更します。

- [Frequency] : 追跡対象の存在を ASA がテストする頻度を秒数で設定します。有効な値の範囲は、1 ~ 604800 秒です。デフォルト値は 60 秒です。
- [Threshold] : しきい値を超えたイベントを示す時間をミリ秒数で設定します。この値に、タイムアウト値より大きい値は指定できません。
- [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をミリ秒数で設定します。有効な値の範囲は、0 ~ 604800000 ミリ秒です。デフォルト値は 5000 ミリ秒です。
- [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を設定します。デフォルト値は 28 です。有効値の範囲は 0 ~ 16384 です。
(注) 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。
- [ToS] : エコー要求の IP ヘッダーにあるサービスバイトのタイプの値を設定します。有効な値は、0 ~ 255 です。デフォルト値は 0 です
- [Number of Packets] : 各テストに送信されるエコー要求の数を設定します。有効値の範囲は 1 ~ 100 です。デフォルト値は 1 です。

[OK] をクリックします。

ステップ7 [OK] をクリックしてルートを保存してから、[Apply] をクリックします。

追跡するルートを適用するとすぐに、モニタリングプロセスが開始されます。

ステップ8 追跡対象外のバックアップルートを作成します。

バックアップルートは、追跡されたルートと同じ宛先へのスタティックルートですが、異なるインターフェイスまたはゲートウェイを経由します。このルートは、追跡されたルートより長いアドミニストレーティブディスタンス (メトリック) に割り当てする必要があります。

スタティックルートまたはデフォルトルートのモニタリング

- [Monitoring] > [Routing] > [Routes]

[Routes] ペインでは、それぞれの行が1つのルートを表しています。IPv4 接続、IPv6 接続、またはその両方でフィルタリングできます。ルーティング情報には、プロトコル、ルートタイプ、宛先IPアドレス、ネットマスクまたはプレフィックスの長さ、ゲートウェイ IP アドレス、ルートに接続するときを経由するインターフェイス、およびアドミニストレーティブディスタンスが含まれています。

スタティックルートまたはデフォルトルートの例

次の例は、スタティックルートの作成方法を示します。スタティックルートは、宛先が 10.1.1.0/24 のトラフィックすべてを内部インターフェイスに接続されているルータ (10.1.2.45) に送信します。また、dmz インターフェイスで3つの異なるゲートウェイにトラフィックを誘導する3つの等コストスタティックルートを定義し、トンネルトラフィックのデフォルトルートと通常のトラフィックのデフォルトルートを追加します。

```
route inside 10.1.1.0 255.255.255.0 10.1.2.45
route dmz 10.10.10.0 255.255.255.0 192.168.2.1
route dmz 10.10.10.0 255.255.255.0 192.168.2.2
route dmz 10.10.10.0 255.255.255.0 192.168.2.3
route outside 0 0 209.165.201.1
route inside 0 0 10.1.2.45 tunneled
```

スタティックルートおよびデフォルトルートの履歴

表 1: スタティックルートおよびデフォルトルートの機能履歴

機能名	プラットフォームリリース	機能情報
スタティックルートトラッキング	7.2(1)	<p>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。</p> <p>次の画面が導入または変更されました。</p> <p>[Configuration] > [Device Setup] > [Routing] > [Static Routes] > [Add Static Route] [Configuration] > [Device Setup] > [Routing] > [Static Routes] > [Add Static Route] > [Route Monitoring Options]</p>

機能名	プラットフォームリリース	機能情報
スタティック null0 ルートによるトラフィックのドロップ	9.2(1)	<p>トラフィックを null0 インターフェイスへ送信すると、指定したネットワーク宛のパケットはドロップします。この機能は、BGP の Remotely Triggered Black Hole (RTBH) の設定に役立ちます。</p> <p>次の画面が変更されました。</p> <p>[Configuration] > [Device Setup] > [Routing] > [Static Routes] > [Add Static Route]</p>

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。