



スタティックルートとデフォルトルート

この章では、Cisco 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 \(4 ページ\)](#)
- [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 \(8 ページ\)](#)
- [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

トラフィックを接続されていないホストやネットワークに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、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 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、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「ブラックホール化」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「ブラックホール」に転送できるため、トラフィックがドロップされます。

スタティック null0 ルートには、望ましいパフォーマンス プロファイルがあります。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。

- 宛先かつアドミニストレ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。

トランスペアレントファイアウォールモードルート

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は、syslog サーバまたはSNMPサーバへの通信も含むことがあります。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。トランスペ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。詳細については、「[MAC アドレスとルートルックアップ](#)」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。

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 (syslog サーバなど)
- 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イネーブルに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 ルートをブリッジグループ 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。
- 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

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。

クラスタ

クラスタリングでは、スタティック ルート モニタリングはプライマリ ユニットでのみサポートされます。

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。

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。

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を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「ブラックホール化」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。

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>
トラフィックを「ブラックホール化」するためのスタティック null0 ルート	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 packets 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>

