

# 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の概要 （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 （9 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 （10 ページ）


# スタティックルートとデフォルトルートの概要

接続されていないホストまたはネットワークに通信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します。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、すべての通信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。

### デフォルトルートの設定要件

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。

### スタティックルートのユースケース

- 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。

# 不要な通信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。

### パフォーマンスおよびルーティング機能の利点

スタティック null0 ルートを使用すると、良好なパフォーマンス特性が得られます。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。

（注） null0インターフェイスへの通信をブラックホールにルーティングすると、不要な通信のドロップに役立ちますが、この方法では no-route ASP ドロップが増加します。

## ルートの優先順位

- 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 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 モードとブリッジグループのルート

ASA で発信され、ブリッジ グループ メンバー インターフェイス経由で直接接続されていないネットワークに向かう通信の場合、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通信を送信するかを認識できるように、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 で発信される通信には、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。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、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 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 ルートを設定できます。

### スタティック ルート トラッキングの導入

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。

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。ターゲットとして任意のネットワークオブジェクトを選択できますが、次のいずれかのオプションを使用することを検討してください。

- ISP ゲートウェイのアドレス（デュアル ISP サポート用）
- ネクストホップゲートウェイのアドレス（ゲートウェイの可用性に懸念がある場合）
- ASAが通信する必要のあるターゲット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

ファイアウォールモードおよびインターフェイスの要件に従ってスタティックルートを設定します。

- 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

ネットワークアドレスがスタティックルートの要件を満たしていることを確認します。

- 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ないため、クラス E ネットワークはスタティックルートで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

クラスタリングおよびマルチコンテキストモードの設定に関する制限事項を考慮してください。

- クラスタリングでは、スタティック ルート トラッキングはコントロールノード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。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 （8 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 （8 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 （7 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に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) | 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。<br>次の画面が導入または変更されました。<br>**[Configuration] > [Device Setup] > [Routing] > [Static Routes] > [Add Static Route] [Configuration] > [Device Setup] > [Routing] > [Static Routes] > [Add Static Route] > [Route Monitoring Options]** |
| 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) | 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。<br>次の画面が変更されました。<br>**[Configuration] > [Device Setup] > [Routing] > [Static Routes] > [Add Static Route]** |

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。

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。

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。