



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 \(9 ページ\)](#)
- [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 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 ルートは、宛先の IP アドレスとして 0.0.0.0/0 が指定された単なるスタティック ルートです。

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、Remotely Triggered Black Hole 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、[ECMP ルーティング](#)を参照してください。
- [Tunneled] オプションを使用してトンネルから出るトラフィックの場合、このルートは、その他の設定または学習されたデフォルト ルートをすべて上書きします。

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ルート

ASA から発信され、ブリッジ グループ メンバー インターフェイス経由で非直接接続ネットワークに向かうトラフィックについては、デフォルト ルートまたはスタティック ルートのい

いずれかを設定して、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のかを認識できるように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。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の、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。
- 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。

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 (**ip verify reverse-path** コマンド) 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

デフォルト ルート を追加します。

IPv4 :

route if_name0.0.0.0 0.0.0.0 gateway_ip [distance] [tunneled]

IPv6 :

ipv6 route if_name::/0 gateway_ip [distance] [tunneled]

例 :

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 192.168.2.4
ciscoasa(config)# route inside 0.0.0.0 0.0.0.0 10.1.2.3 tunneled
ciscoasa(config)# ipv6 route inside ::/0 3FFE:1100:0:CC00::1
```

if_name は、特定のトラフィックの送信を行うインターフェイスです。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。

distance 引数は、ルート のアドミニストレーティブ ディスタンス (1 ~ 254) です。値を指定しない場合、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。

(注) 異なるメトリックを持つ個別のインターフェイス上で2つのデフォルトルートが設定されている場合は、大きい方のメトリックを持つインターフェイスから ASA への接続の確立には失敗しますが、小さい方のメトリックを持つインターフェイスから ASA への接続は予期したとおりに成功します。

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、**tunneled** キーワードを使用して 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。

ヒント 宛先ネットワーク アドレスおよびマスクとして、**0.0.0.0 0.0.0.0** の代わりに **0 0** と入力することができます。たとえば、**route outside 0 0 192.168.2.4** のように入力します。

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

スタティック ルートを追加します。

IPv4 :

route if_name dest_ip mask gateway_ip [distance]

IPv6 :

ipv6 route if_name dest_ipv6_prefix/prefix_length gateway_ip [distance]

例 :

```
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1
ciscoasa(config)# ipv6 route outside 2001:DB8:1::0/32 2001:DB8:0:CC00::1
```

if_name は、特定のトラフィックの送信を行うインターフェイスです。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入力します。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。

dest_ip 引数と *mask* または *dest_ipv6_prefix/prefix_length* 引数は宛先ネットワークの IP アドレスであり、*gateway_ip* 引数はネクスト ホップ ルータのアドレスです。スタティック ルートに指定するアドレスは、ASA に到達して NAT を実行する前のパケットにあるアドレスです。

distance 引数は、ルートのアドミニストレーティブ ディスタンスです。値を指定しない場合、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进行比较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。

例

次に、同じゲートウェイに移動する 3 つのネットワークと、別のゲートウェイに移動するもう 1 つのネットワークの例を示します。

```
route outside 10.10.10.0 255.255.255.0 192.168.1.1
route outside 10.10.20.0 255.255.255.0 192.168.1.1
route outside 10.10.30.0 255.255.255.0 192.168.1.1
route inside 10.10.40.0 255.255.255.0 10.1.1.1
```

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 モニタリング プロセスを次のように定義します。

sla monitor sla_id

例 :

```
ciscoasa(config)# sla monitor 5
ciscoasa(config-sla-monitor)#
```

ステップ 2 モニタリング プロトコル、追跡対象ネットワークのターゲット ホスト、ネットワークに到達するときに経由するネットワークを指定します。

type echo protocol ipicmpecho target_ip interface if_name

例 :

```
ciscoasa(config-sla-monitor)# type echo protocol ipicmpecho 172.29.139.134
ciscoasa(config-sla-monitor-echo)#
```

target_ip 引数は、トラッキングプロセスによって使用可能かどうかをモニタされるネットワーク オブジェクトの IP アドレスです。このオブジェクトが使用可能な場合、トラッキングプロセス 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。このオブジェクトが使用できない場合、トラッキングプロセスがルートを削除し、代わりにバックアップ ルートが使用されます。

ステップ 3 (オプション) モニタリング オプションを設定します。**frequency**、**num-packets**、**request-data-size**、**threshold**、**timeout**、**tos** の各コマンドについては、コマンド リファレンスを参照してください。

ステップ 4 モニタリング プロセスのスケジュールを設定します。

sla monitor schedule *sla_id* [**life** {**forever** | **seconds**}] [**start-time** {hh:mm[:ss] [month day | day month] | **pending** | **now** | **after** hh:mm:ss}] [**ageout** seconds] [**recurring**]

例 :

```
ciscoasa(config)# sla monitor schedule 5 life forever start-time now
```

多くの場合、監視スケジュールのために **sla monitor schedule** **life forever start-time now** コマンドを使用し、監視設定でテストがどれほどの頻度で実行されるかを判断します。

ただし、このモニタリングプロセスを将来開始するようにしたり、指定した時刻だけに実行されるようにスケジュールを設定したりできます。

ステップ 5 追跡するスタティック ルートを SLA モニタリング プロセスに関連付けます。

track *track_id* **rtr** *sla_id* **reachability**

例 :

```
ciscoasa(config)# track 6 rtr 5 reachability
```

track_id 引数は、このコマンドで割り当てるトラッキング番号です。*sla_id* 引数は SLA プロセスの ID 番号です。

ステップ 6 次のルート タイプのいずれかを追跡します。

- スタティック ルート :

route *if_name* *dest_ip* *mask* *gateway_ip* [*distance*] **track** *track_id*

例 :

```
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1 track 6
```

tunneled オプションは使用できません。

- DHCP から取得したデフォルト ルート :

```
interface interface_id
  dhcp client route track track_id
  ip address dhcp setroute
```

- PPPoE から取得したデフォルト ルート :

```
interface interface_id
  pppoe client route track track_id
  ip address pppoe setroute
```

ステップ 7 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

- **show route**

ルーティング テーブルを表示します。

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。 clear configure sla、frequency、num-packets、request-data-size、show sla monitor、show running-config sla、sla monitor、sla monitor schedule、threshold、timeout、tos、track rtr の各コマンドが導入されました。
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)	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。 route コマンドが変更されました。