CHAPTER 26

スタティック ルートおよびデフォルト ルートの設定

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。次の項目を取り上げます。

スタティック ルートとデフォルト ルートに関する情報

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、そのホストまたはネットワークへのスタティック ルートを定義するか、または少なくとも、ネットワークと ASA の間にルータがある場合など、ASA が直接接続されていない任意のネットワークのデフォルト ルートを定義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 ルートが定義されていない場合は、接続されていないホストやネットワークへのトラフィックによって次の syslog メッセージが生成されます。

```
%ASA-6-110001: No route to dest_address from source_address
```

マルチ コンテキスト モードではダイナミック ルーティングはサポートされていません。

次の場合は、シングル コンテキスト モードでスタティック ルートを使用します。

- ネットワークで EIGRP、RIP または OSPF とは異なるルータ検出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。

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。しかし、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。

トランスペアレント ファイアウォール モードでは、ASA から直接接続されていないネットワークに宛てたトラフィック用にデフォルト ルートまたはスタティック ルートを設定して、ASA がトラフィックの送信先インターフェイスを認識できるようにする必要があります。ASA から発信されるトラフィックには、syslog サーバ、Websense サーバまたは N2H2 サーバ、あるいは AAA サーバとの通信もあります。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。さらに、ASA では、ロード バランシングのために、1 つのインターフェイスあたり最大で 3 つの等コスト ルートをサポートします。

スタティック ルートおよびデフォルト ルートのライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
すべてのモデル	基本ライセンス

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。

フェールオーバーのガイドライン

ダイナミック ルーティング プロトコルのステートフル フェールオーバーをサポートします。

その他のガイドライン

- IPv6 スタティック ルートは、ASDM においてトランスペアレント モードでサポートされていません。
- 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、マスター ユニットでのみサポートされます。クラスタリングの詳細については、第 7 章「ASA のクラスタの設定」を参照してください。

スタティック ルートおよびデフォルト ルートの設定

この項では、スタティック ルートとスタティック デフォルト ルートを設定する方法について説明します。次の項目を取り上げます。

スタティック ルートの設定

スタティック ルーティング アルゴリズムは、基本的にはルーティングの開始前にネットワーク管理者によって確立されるテーブル マッピングのことです。このようなマッピングは、ネットワーク管理者が変更するまでは変化しません。スタティック ルートを使用するアルゴリズムは設計が容易であり、ネットワーク トラフィックが比較的予想可能で、ネットワーク設計が比較的単純な環境で正しく動作します。したがって、スタティック ルーティング システムはネットワークの変更に対応できません。

スタティック ルートは、指定されたゲートウェイが利用できなくなってもルーティング テーブルに保持されています。指定されたゲートウェイが利用できなくなった場合は、スタティック ルートをルーティング テーブルから手動で削除する必要があります。ただし、スタティック ルートは、指定されたインターフェイスが停止するとルーティング テーブルから削除され、インターフェイスが復旧すると最適用されます。

（注）　ASA で動作中のルーティング プロトコルのアドミニストレーティブ ディスタンスよりも長いアドミニストレーティブ ディスタンスを指定してスタティック ルートを作成すると、ルーティング プロトコルで検出される指定の宛先へのルートがスタティック ルートより優先されます。スタティック ルートは、ダイナミックに検出されたルートがルーティング テーブルから削除された場合に限り使用されます。

インターフェイスごとに同じ宛先でコストの等しいルートを 3 つまで定義できます。複数のインターフェイス間を通る等コスト マルチパス（ECMP）はサポートされていません。ECMP では、トラフィックは必ずしもルート間で均等に分割されるわけではありません。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。

スタティック ルートを設定するには、次の項を参照してください。

スタティック ルートの追加または編集

スタティック ルートを追加または編集するには、次のコマンドを入力します。

コマンド	目的
route *if_name dest_ip mask gateway_ip* [*distance*] **例：** hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1 [1]	スタティック ルートを追加できます。 *dest_ip* および *mask* 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。

例

次に、外部インターフェイス上の 3 台のゲートウェイにトラフィックを転送する、コストの等しいスタティック ルートの例を示します。ASA は、指定された複数のゲートウェイ間にトラフィックを分散します。

```
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.2
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.3
```

デフォルト スタティック ルートの設定

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。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。

（注） バージョン 7.0(1) 以降で、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、それよりも大きいメトリックを持つインターフェイスから ASA への接続は失敗しますが、小さいメトリックを持つインターフェイスからの ASA への接続は予期したとおりに成功します。

デバイスあたり最大 3 つの等コスト デフォルト ルート エントリを定義することができます。複数の等コスト デフォルト ルート エントリを定義すると、デフォルト ルートに送信されるトラフィックは、指定されたゲートウェイの間に分散されます。複数のデフォルト ルートを定義する場合は、各エントリに同じインターフェイスを指定する必要があります。

4 つ以上の等コスト デフォルト ルート、またはすでに定義されているデフォルト ルートとは別のインターフェイスでデフォルト ルートを定義しようとすると、次のメッセージが表示されます。

```
"ERROR: Cannot add route entry, possible conflict with existing routes."
```

トンネル トラフィックには、標準のデフォルト ルートの他に別のデフォルト ルートを 1 つ定義することができます。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。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。

デフォルト スタティック ルートの設定の制限事項

tunneled オプションが指定されたデフォルト ルートには、次の制限事項が適用されます。

- セッションにエラーが発生する原因となるため、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）をイネーブルにしないでください。
- セッションにエラーが発生する原因となるため、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 オプションでは、複数のデフォルト ルートを定義できません。
- 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 デフォルト スタティック ルートを追加または編集するには、次のコマンドを入力します。

コマンド	目的
route *if_name* 0.0.0.0 0.0.0.0 *gateway_ip* [*distance* | *tunneled*] **例：** `hostname(config)# route outside 0 0 192.168.2.4 tunneled`	スタティック ルートを追加できます。 *dest_ip* および *mask* 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。

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、次のように入力します。

```
hostname(config)# route outside 0 0 192.168.1 1
```

IPv6 デフォルト ルートおよびスタティック ルートの設定

ホストが接続されているインターフェイスが IPv6 に対応し、IPv6 ACL でトラフィックが許可されていれば、ASA は、直接接続されているホスト間で IPv6 トラフィックを自動的にルーティングします。

IPv6 デフォルト ルートおよびスタティック ルートを設定するには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ 1	**ipv6 route** *if_name* **::/0** *next_hop_ipv6_addr* **例：** `hostname(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1`	デフォルトの IPv6 ルートを追加します。 この例では、ネットワーク 7fff::0/32 のパケットを、3FFE:1100:0:CC00::1 の内部インターフェイス上のネットワーキング デバイスにルーティングします。 アドレス ::/0 は任意の IPv6 に相当します。
ステップ 2	**ipv6 route** *if_name destination next_hop_ipv6_addr* [*admin_distance*] **例：** `hostname(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1 [110]`	IPv6 ルーティング テーブルに IPv6 スタティック ルートを追加します。 この例では、ネットワーク 7fff::0/32 のパケットを、3FFE:1100:0:CC00::1 の内部インターフェイス上にあり、アドミニストレーティブ ディスタンスが 110 のネットワーキング デバイスにルーティングします。

（注）　**ipv6 route** コマンドは、**route** コマンド（IPv4 スタティック ルートの定義に使用）と同じように動作します。

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

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 は、定義したモニタリング対象にスタティック ルートを関連付けることによってこの機能を実装し、ICMP エコー要求を使用して対象をモニタリングします。指定された時間内にエコー応答がない場合は、そのオブジェク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、すでに定義されているバックアップ 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 ICPM 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（AAA 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デスクトップ PC やノートブック 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 トラッキングを設定するには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ 1	**sla monitor** *sla_id* **例：** `hostname(config)# sla monitor sla_id`	モニタリング プロセスを定義することにより、追跡されるオブジェクトのモニタリング パラメータを設定します。 新しいモニタリング プロセスを設定する場合は、SLA モニタ コンフィギュレーション モードに入ります。 タイプが定義済みでスケジュールが未設定のモニタリング プロセスのモニタリング パラメータを変更する場合は、自動的に SLA プロトコル コンフィギュレーション モードに入ります。
ステップ 2	**type echo protocol ipIcmpEcho** *target_ip* **interface** *if_name* **例：** `hostname(config-sla-monitor)# type echo protocol ipIcmpEcho target_ip interface if_name`	モニタリング プロトコルを指定します。 タイプが定義済みでスケジュールが未設定のモニタリング プロセスのモニタリング パラメータを変更する場合は、自動的に SLA プロトコル コンフィギュレーション モードに入り、この設定は変更できません。 *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。

	コマンド	目的
ステップ 3	**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：** `hostname(config)# 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]`	モニタリング プロセスのスケジュールを設定します。 一般に、モニタリング スケジュールには **sla monitor schedule** *sla_id* **life forever start-time now** コマンドを使用し、モニタリング コンフィギュレーションがテスト頻度を判別できるようにします。 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 4	**track** *track_id* **rtr** *sla_id* **reachability** **例：** `hostname(config)# track track_id rtr sla_id reachability`	追跡されるスタティック ルートを SLA モニタリング プロセスに関連付けます。 *track_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 5	追跡されるオブジェクトが到達可能なときに、ルーティング テーブルにインストールするスタティック ルートを定義するには、次のいずれかの手順を実行します。 これらのオプションによって、スタティック ルート、または DHCP または PPPoE を通じて取得されたデフォルト ルートを追跡できます。	
	route *if_name dest_ip mask gateway_ip* [*admin_distance*] **track** *track_id* **例：** `hostname(config)# route if_name dest_ip mask gateway_ip [admin_distance] track track_id`	スタティック ルートが追跡されます。 スタティック ルート トラッキングでは、**route** コマンドに **tunneled** オプションを使用できません。

	例：
	`hostname(config)# interface phy_if`
	`hostname(config-if)# dhcp client route track track_id`
	`hostname(config-if)# ip address dhcp setroute`
	`hostname(config-if)# exit`
		DHCP を使用して取得されたデフォルト ルートが追跡されます。
		DHCP を使用してデフォルト ルートを取得するには、**ip address dhcp** コマンドで **setroute** キーワードを使用する必要があることに注意してください。

	例：
	`hostname(config)# interface phy_if`
	`hostname(config-if)# pppoe client route track track_id`
	`hostname(config-if)# ip address pppoe setroute`
	`hostname(config-if)# exit`
		PPPoE を使用して取得されたデフォルト ルートが追跡されます。
		PPPoE を使用してデフォルト ルートを取得するには、**ip address pppoe** コマンドで **setroute** キーワードを使用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 ルートの設定例

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、外部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 ルートを追加します。ASA は、指定された複数のゲートウェイ間にトラフィックを分散します。

```
hostname(config)# route inside 10.1.1.0 255.255.255.0 10.1.2.45 1
```

```
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.2.1
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.2.2
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.2.3
hostname(config)# route outside 0 0 192.168.2.4 tunneled
```

ASA で受信した非暗号化トラフィックは、スタティック ルートも既知のルートも指定されていない場合、IP アドレスが 192.168.2.1、192.168.2.2、192.168.2.3 のゲートウェイの間に分散されます。ASA で受信した暗号化されたトラフィックは、スタティック ルートも既知のルートも指定されていない場合、IP アドレス 192.168.2.4 のゲートウェイに転送されます。

次に、10.1.1.0/24 宛てのすべてのトラフィックを、内部インターフェイスに接続されたルータ（10.1.2.45）に送信するスタティック ルートを作成する例を示します。

```
hostname(config)# route inside 10.1.1.0 255.255.255.0 10.1.2.45 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

表 26-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。

表 26-1　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
ルーティング	7.0(1)	スタティック ルートおよびデフォルト ルートが導入されました。 **route** コマンドが導入されました。
クラスタリング	9.0(1)	スタティック ルート モニタリングは、マスター ユニットでのみサポートされます。