



ルーティングの概要

この章では、ASA 内でのルーティングの動作について説明します。

- [パスの決定 \(1 ページ\)](#)
- [サポートされるルート タイプ \(2 ページ\)](#)
- [ルーティングでサポートされるインターネット プロトコル \(4 ページ\)](#)
- [ルーティングテーブル \(5 ページ\)](#)
- [管理トラフィック用ルーティングテーブル \(12 ページ\)](#)
- [等コスト マルチパス \(ECMP\) ルーティング \(13 ページ\)](#)
- [プロキシ ARP 要求のディセーブル化 \(14 ページ\)](#)
- [ルーティング テーブルの表示 \(15 ページ\)](#)
- [ルート概要の履歴 \(15 ページ\)](#)

パスの決定

ルーティングプロトコルでは、メトリックを使用して、パケットの移動に最適なパスを評価します。メトリックは、宛先への最適なパスを決定するためにルーティングアルゴリズムが使用する、パスの帯域幅などの測定基準です。パスの決定プロセスを支援するために、ルーティングアルゴリズムは、ルート情報が格納されるルーティングテーブルを初期化して保持します。ルート情報は、使用するルーティングアルゴリズムによって異なります。

ルーティングアルゴリズムにより、さまざまな情報がルーティングテーブルに入力されます。宛先またはネクスト ホップの関連付けにより、最終的な宛先に達するまで、「ネクスト ホップ」を表す特定のルータにパケットを送信することによって特定の宛先に最適に到達できることがルータに示されます。ルータは、着信パケットを受信すると宛先アドレスを確認し、このアドレスとネクスト ホップとを関連付けようとします。

ルーティングテーブルには、パスの妥当性に関するデータなど、他の情報を格納することもできます。ルータは、メトリックを比較して最適なルートを決めます。これらのメトリックは、使用しているルーティングアルゴリズムの設計によって異なります。

ルータは互いに通信し、さまざまなメッセージの送信によりそのルーティングテーブルを保持しています。ルーティングアップデート メッセージはそのようなメッセージの 1 つで、通常はルーティング テーブル全体か、その一部で構成されています。ルーティングアップデート

を他のすべてのルータから分析することで、ルータはネットワークトポロジの詳細な全体像を構築できます。ルータ間で送信されるメッセージのもう1つの例であるリンクステートアドバタイズメントは、他のルータに送信元のリンクのステートを通知します。リンク情報も、ネットワークの宛先に対する最適なルートをルータが決定できるように、ネットワークトポロジの全体像の構築に使用できます。



(注) 非対称ルーティングがサポートされるのは、マルチコンテキストモードでのアクティブ/アクティブフェールオーバーに対してのみです。

サポートされるルートタイプ

ルータが使用できるルートタイプには、さまざまなものがあります。ASAでは、次のルートタイプが使用されます。

- スタティックとダイナミックの比較
- シングルパスとマルチパスの比較
- フラットと階層型の比較
- リンクステートと距離ベクトル型の比較

スタティックとダイナミックの比較

スタティックルーティングアルゴリズムは、実はネットワーク管理者が確立したテーブルマップです。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。

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ないため、一般に、変化を続ける大規模なネットワークには不向きであると考えられています。主なルーティングアルゴリズムのほとんどはダイナミックルーティングアルゴリズムであり、受信したルーティングアップデートメッセージを分析することで、変化するネットワーク環境に適合します。メッセージがネットワークが変化したことを示している場合は、ルーティングソフトウェアはルートを再計算し、新しいルーティングアップデートメッセージを送信します。これらのメッセージはネットワーク全体に送信されるため、ルータはそのアルゴリズムを再度実行し、それに従ってルーティングテーブルを変更します。

ダイナミックルーティングアルゴリズムは、必要に応じてスタティックルートで補足できます。たとえば、ラストリゾートルータ（ルーティングできないすべてのパケットが送信されるルータのデフォルトルート）を、ルーティングできないすべてのパケットのリポジトリとして機能するように指定し、すべてのメッセージを少なくとも何らかの方法で確実に処理することができます。

シングルパスとマルチパスの比較

一部の高度なルーティングプロトコルは、同じ宛先に対する複数のパスをサポートしています。シングルパスアルゴリズムとは異なり、これらのマルチパスアルゴリズムでは、複数の回線でトラフィックを多重化できます。マルチパスアルゴリズムの利点は、スループットと信頼性が大きく向上することであり、これは一般に「ロードシェアリング」と呼ばれています。

フラットと階層型の比較

ルーティングアルゴリズムには、フラットなスペースで動作するものと、ルーティング階層を使用するものがあります。フラットルーティングシステムでは、ルータは他のすべてのルータのピアになります。階層型ルーティングシステムでは、一部のルータが実質的なルーティングバックボーンを形成します。バックボーン以外のルータからのパケットはバックボーンルータに移動し、宛先の一般エリアに達するまでバックボーンを通じて送信されます。この時点で、パケットは、最後のバックボーンルータから、1つ以上のバックボーン以外のルータを通じて最終的な宛先に移動します。

多くの場合、ルーティングシステムは、ドメイン、自律システム、またはエリアと呼ばれるノードの論理グループを指定します。階層型のシステムでは、ドメイン内の一部のルータは他のドメインのルータと通信できますが、他のルータはそのドメイン内のルータ以外とは通信できません。非常に大規模なネットワークでは、他の階層レベルが存在することがあり、最も高い階層レベルのルータがルーティングバックボーンを形成します。

階層型ルーティングの第一の利点は、ほとんどの企業の組織を模倣しているため、そのトラフィックパターンを適切にサポートするという点です。ほとんどのネットワーク通信は、小さい企業グループ（ドメイン）内で発生します。ドメイン内ルータは、そのドメイン内の他のルータだけを認識していれば済むため、そのルーティングアルゴリズムを簡素化できます。また、使用しているルーティングアルゴリズムに応じて、ルーティングアップデートトラフィックを減少させることができます。

リンクステートと距離ベクトル型の比較

リンクステートアルゴリズム（最短パス優先アルゴリズムとも呼ばれる）は、インターネットワークのすべてのノードにルーティング情報をフラッドします。ただし、各ルータは、それ自体のリンクのステートを記述するルーティングテーブルの一部だけを送信します。リンクステートアルゴリズムでは、各ルータはネットワークの全体像をそのルーティングテーブルに構築します。距離ベクトル型アルゴリズム（Bellman-Fordアルゴリズムとも呼ばれる）では、各ルータが、そのネイバーだけに対してそのルーティングテーブル全体または一部を送信するように要求されます。つまり、リンクステートアルゴリズムは小規模なアップデートを全体に送信しますが、距離ベクトル型アルゴリズムは、大規模なアップデートを隣接ルータだけに送信します。距離ベクトル型アルゴリズムは、そのネイバーだけを認識します。通常、リンクステートアルゴリズムはOSPFルーティングプロトコルとともに使用されます。

ルーティングでサポートされるインターネットプロトコル

ASAは、ルーティングに対してさまざまなインターネットプロトコルをサポートしています。この項では、各プロトコルについて簡単に説明します。

- Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRPは、IGRPルータとの互換性とシームレスな相互運用性を提供するシスコ独自のプロトコルです。自動再配布メカニズムにより、IGRPルートをEnhanced IGRPに、またはEnhanced IGRPからインポートできるため、Enhanced IGRPを既存のIGRPネットワークに徐々に追加できます。

- Open Shortest Path First (OSPF)

OSPFは、インターネットプロトコル (IP) ネットワーク向けに、インターネット技術特別調査委員会 (IETF) のInterior Gateway Protocol (IGP) 作業部会によって開発されたルーティングプロトコルです。OSPFは、リンクステートアルゴリズムを使用して、すべての既知の宛先までの最短パスを構築および計算します。OSPFエリア内の各ルータには、ルータが使用可能なインターフェイスと到達可能なネイバーそれぞれのリストである同一のリンクステートデータベースが置かれています。

- Routing Information Protocol (RIP)

RIPは、ホップカウントをメトリックとして使用するディスタンスベクトルプロトコルです。RIPは、グローバルなインターネットでトラフィックのルーティングに広く使用されているInterior Gateway Protocol (IGP) です。つまり、1つの自律システム内部でルーティングを実行します。

- ボーダー ゲートウェイ プロトコル (BGP)

BGPは自律システム間のルーティングプロトコルです。BGPは、インターネットのルーティング情報を交換するために、インターネットサービスプロバイダー (ISP) 間で使用されるプロトコルです。顧客はISPに接続し、ISPはBGPを使用して顧客のルートとISPのルートを交換します。自律システム (AS) 間でBGPを使用する場合、このプロトコルは外部BGP (EBGP) と呼ばれます。サービスプロバイダーがBGPを使用してAS内のルートを交換する場合、このプロトコルは内部BGP (IBGP) と呼ばれます。

- Intermediate System to Intermediate System (IS-IS)

IS-ISはリンクステート内部ゲートウェイプロトコル (IGP) です。リンクステートプロトコルは、各参加ルータで完全なネットワーク接続マップを構築するために必要な情報の伝播によって特徴付けられます。このマップは、その後、宛先への最短パスを計算するために使用されます。

ルーティングテーブル

ASA はデータトラフィック（デバイスを介して）および管理トラフィック（デバイスから）に別々のルーティングテーブルを使用します。ここでは、ルーティングテーブルの仕組みについて説明します。管理ルーティングテーブルの詳細については、[管理トラフィック用ルーティングテーブル（12 ページ）](#) も参照してください。

ルーティングテーブルへの入力方法

ASA のルーティングテーブルには、スタティックに定義されたルート、直接接続されているルート、およびダイナミックルーティングプロトコルで検出されたルートを入力できます。ASA デバイスは、ルーティングテーブルに含まれるスタティックルートと接続されているルートに加えて、複数のルーティングプロトコルを実行できるため、同じルートが複数の方法で検出または入力される可能性があります。同じ宛先への2つのルートがルーティングテーブルに追加されると、ルーティングテーブルに残るルートは次のように決定されます。

- 2つのルートのネットワークプレフィックス長（ネットワークマスク）が異なる場合は、どちらのルートも固有と見なされ、ルーティングテーブルに入力されます。入力された後は、パケット転送ロジックが2つのうちどちらを使用するかを決定します。

たとえば、RIP プロセスと OSPF プロセスが次のルートを検出したとします。

- RIP : 192.168.32.0/24
- OSPF : 192.168.32.0/19

OSPF ルートのアドミニストレーティブディスタンスの方が適切であるにもかかわらず、これらのルートのプレフィックス長（サブネットマスク）はそれぞれ異なるため、両方の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。これらは異なる宛先と見なされ、パケット転送ロジックが使用するルートを決めます。

- ASA デバイスが、（RIP などの）1つのルーティングプロトコルから同じ宛先に複数のパスがあることを検知すると、（ルーティングプロトコルが判定した）メトリックがよい方のルートがルーティングテーブルに入力されます。

メトリックは特定のルートに関連付けられた値で、ルートを最も優先されるものから順にランク付けします。メトリックの判定に使用されるパラメータは、ルーティングプロトコルによって異なります。メトリックが最も小さいパスは最適パスとして選択され、ルーティングテーブルにインストールされます。同じ宛先への複数のパスのメトリックが等しい場合は、これらの等コストパスに対してロードバランシングが行われます。

- ASA デバイスが、ある宛先へのルーティングプロトコルが複数あることを検知すると、ルートのアドミニストレーティブディスタンスが比較され、アドミニストレーティブディスタンスが最も小さいルートがルーティングテーブルに入力されます。

ルートのアドミニストレーティブディスタンス

ルーティングプロトコルによって検出されるルート、またはルーティングプロトコルに再配布されるルートのアドミニストレーティブディスタンスは変更できます。2つの異なるルーティングプロトコルからの2つの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、デフォルトのアドミニストレーティブディスタンスが小さい方のルートがルーティングテーブルに入力されます。EIGRP ルートと OSPF ルートの場合、EIGRP ルートと OSPF ルートのアドミニストレーティブディスタンスが同じであれば、デフォルトで EIGRP ルートが選択されます。

アドミニストレーティブディスタンスは、2つの異なるルーティングプロトコルから同じ宛先に複数の異なるルートがある場合に、ASAが最適なパスの選択に使用するルートパラメータです。ルーティングプロトコルには、他のプロトコルとは異なるアルゴリズムに基づくメトリックがあるため、異なるルーティングプロトコルによって生成された、同じ宛先への2つのルートについて常にベストパスを判定できるわけではありません。

各ルーティングプロトコルには、アドミニストレーティブディスタンス値を使用して優先順位が付けられています。次の表に、ASAでサポートされているルーティングプロトコルのデフォルトのアドミニストレーティブディスタンス値を示します。

表 1: サポートされるルーティングプロトコルのデフォルトアドミニストレーティブディスタンス

ルートの送信元	デフォルトアドミニストレーティブディスタンス
接続されているインターフェイス	[0]
VPN ルート	1
スタティック ルート	1
EIGRP 集約ルート	5
外部 BGP	20
内部 EIGRP	90
OSPF	110
IS-IS	115
RIP	120
EIGRP 外部ルート	170
内部およびローカル BGP	200
不明 (Unknown)	255

アドミニストレーティブディスタンス値が小さいほど、プロトコルの優先順位が高くなります。たとえば、ASAが OSPF ルーティングプロセス（デフォルトのアドミニストレーティブ

ディスタンスが 110) と RIP ルーティング プロセス (デフォルトのアドミニストレーティブディスタンスが 120) の両方から特定のネットワークへのルートを受信すると、OSPF ルーティングプロセスの方が優先度が高いため、ASA は OSPF ルートを選択します。この場合、ルータは OSPF バージョンのルートをルーティングテーブルに追加します。

VPN アドバタイズされたルート (V-Route/RRR) は、デフォルトのアドミニストレーティブディスタンス 1 のスタティックルートと同等です。ただし、ネットワークマスク 255.255.255.255 の場合と同じように優先度が高くなります。

この例では、OSPF 導出ルートの送信元が (電源遮断などで) 失われると、ASA は、OSPF 導出ルートが再度現れるまで、RIP 導出ルートを使用します。

アドミニストレーティブディスタンスはローカルの設定値です。たとえば、OSPF を通じて取得したルートのアドミニストレーティブディスタンスを変更する場合、その変更は、コマンドが入力された ASA のルーティングテーブルにだけ影響します。アドミニストレーティブディスタンスがルーティングアップデートでアドバタイズされることはありません。

アドミニストレーティブディスタンスは、ルーティングプロセスに影響を与えません。ルーティングプロセスは、ルーティングプロセスで検出されたか、またはルーティングプロセスに再配布されたルートだけをアドバタイズします。たとえば、RIP ルーティングプロセスは、のルーティングテーブルで OSPF ルーティングプロセスによって検出されたルートが使用されていても、RIP ルートをアドバタイズします。

ダイナミックルートとフローティングスタティックルートのバックアップ

ルートを最初にルーティングテーブルにインストールしようとしたとき、他のルートがインストールされているためにインストールできなかった場合、そのルートはバックアップルートとして登録されます。ルーティングテーブルにインストールされたルートに障害が発生すると、ルーティングテーブルメンテナンスプロセスが、登録されたバックアップルートを持つ各ルーティングプロトコルプロセスを呼び出し、ルーティングテーブルにルートを再インストールするように要求します。障害が発生したルートに対して、登録されたバックアップルートを持つプロトコルが複数ある場合、アドミニストレーティブディスタンスに基づいて優先ルートが選択されます。

このプロセスのため、ダイナミックルーティングプロトコルによって検出されたルートに障害が発生したときにルーティングテーブルにインストールされるフローティングスタティックルートを作成できます。フローティングスタティックルートとは、単に、ASA で動作しているダイナミックルーティングプロトコルよりも大きなアドミニストレーティブディスタンスが設定されているスタティックルートです。ダイナミックルーティングプロセスで検出された対応するルートに障害が発生すると、このスタティック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。

転送の決定方法

転送は次のように決定されます。

- 宛先が、ルーティング テーブル内のエントリと一致しない場合、パケットはデフォルト ルートに指定されているインターフェイスを通して転送されます。デフォルトルートが設定されていない場合、パケットは破棄されます。
- 宛先が、ルーティング テーブル内の1つのエントリと一致した場合、パケットはそのルートに関連付けられているインターフェイスを通して転送されます。
- 宛先が、ルーティング テーブル内の複数のエントリと一致し、パケットはネットワーク プレフィックス長がより長いルートに関連付けられているインターフェイスから転送されます。

たとえば、192.168.32.1宛てのパケットが、ルーティング テーブルの次のルートを使用してインターフェイスに到着したとします。

- 192.168.32.0/24 gateway 10.1.1.2
- 192.168.32.0/19 gateway 10.1.1.3

この場合、192.168.32.1は192.168.32.0/24 ネットワークに含まれるため、192.168.32.1宛てのパケットは10.1.1.2宛てに送信されます。このアドレスはまた、ルーティング テーブルの他のルートにも含まれますが、ルーティング テーブル内では192.168.32.0/24の方が長いプレフィックスを持ちます(24ビットと19ビット)。パケットを転送する場合、プレフィックスが長い方が常に短いものより優先されます。



(注) ルートの変更が原因で新しい同様の接続が異なる動作を引き起こしたとしても、既存の接続は設定済みのインターフェイスを使用し続けます。

ダイナミック ルーティングおよび フェールオーバー

アクティブなユニットでルーティング テーブルが変更されると、スタンバイ ユニットでダイナミック ルートが同期されます。これは、アクティブ ユニットのすべての追加、削除、または変更がただちにスタンバイ ユニットに伝播されることを意味します。スタンバイ ユニットがアクティブ/スタンバイの待受中 フェールオーバー ペアでアクティブになると、ルートはフェールオーバー バルク同期および連続複製プロセスの一部として同期されるため、そのユニットには以前のアクティブ ユニットと同じルーティング テーブルがすでに作成されています。

ダイナミック ルーティングおよび クラスタリング

ここでは、クラスタリングでダイナミック ルーティングを使用する方法について説明します。

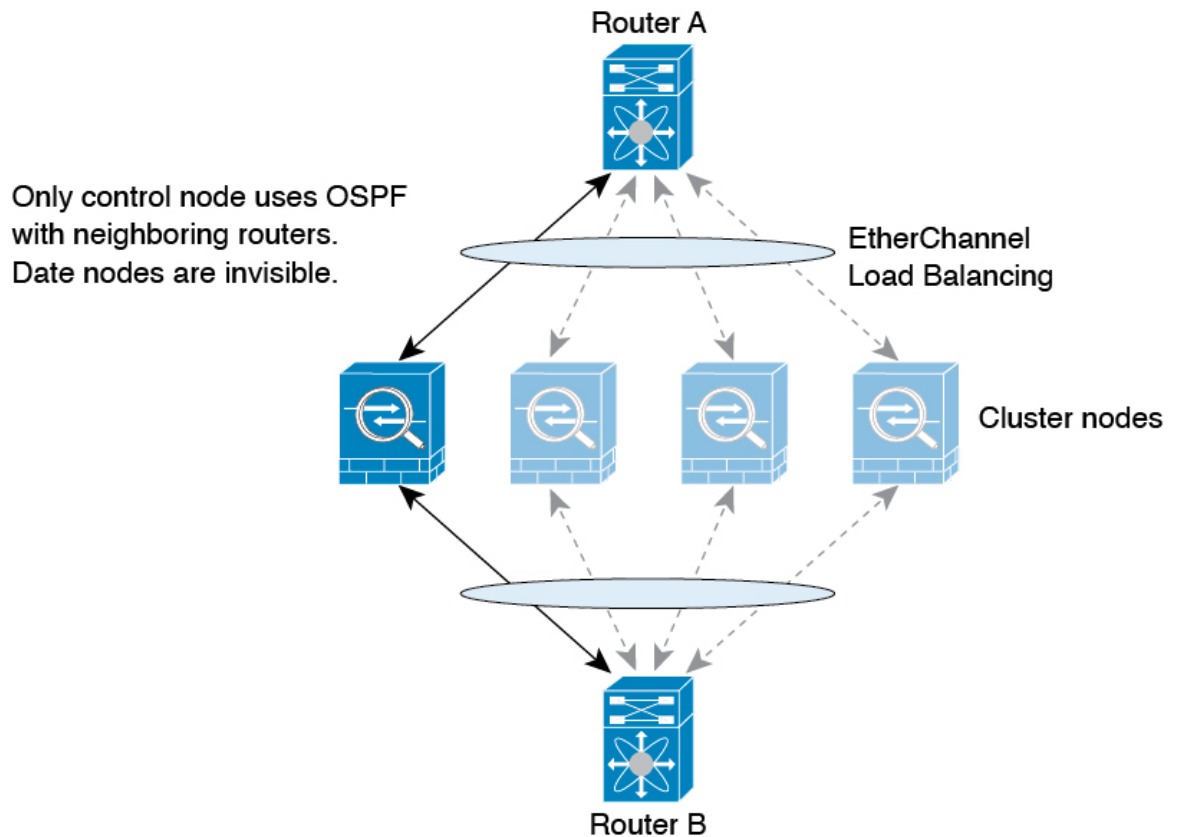
スパンド EtherChannel モードでのダイナミック ルーティング



(注) IS-IS は、スパンド EtherChannel モードではサポートされていません。

スパンド EtherChannel モード：ルーティングプロセスは制御ノードでのみ実行されます。ルートは制御ノードを介して学習され、データノードに複製されます。ルーティングパケットは、データノードに到着すると制御ノードにリダイレクトされます。

図 1: スパンド EtherChannel モードでのダイナミック ルーティング



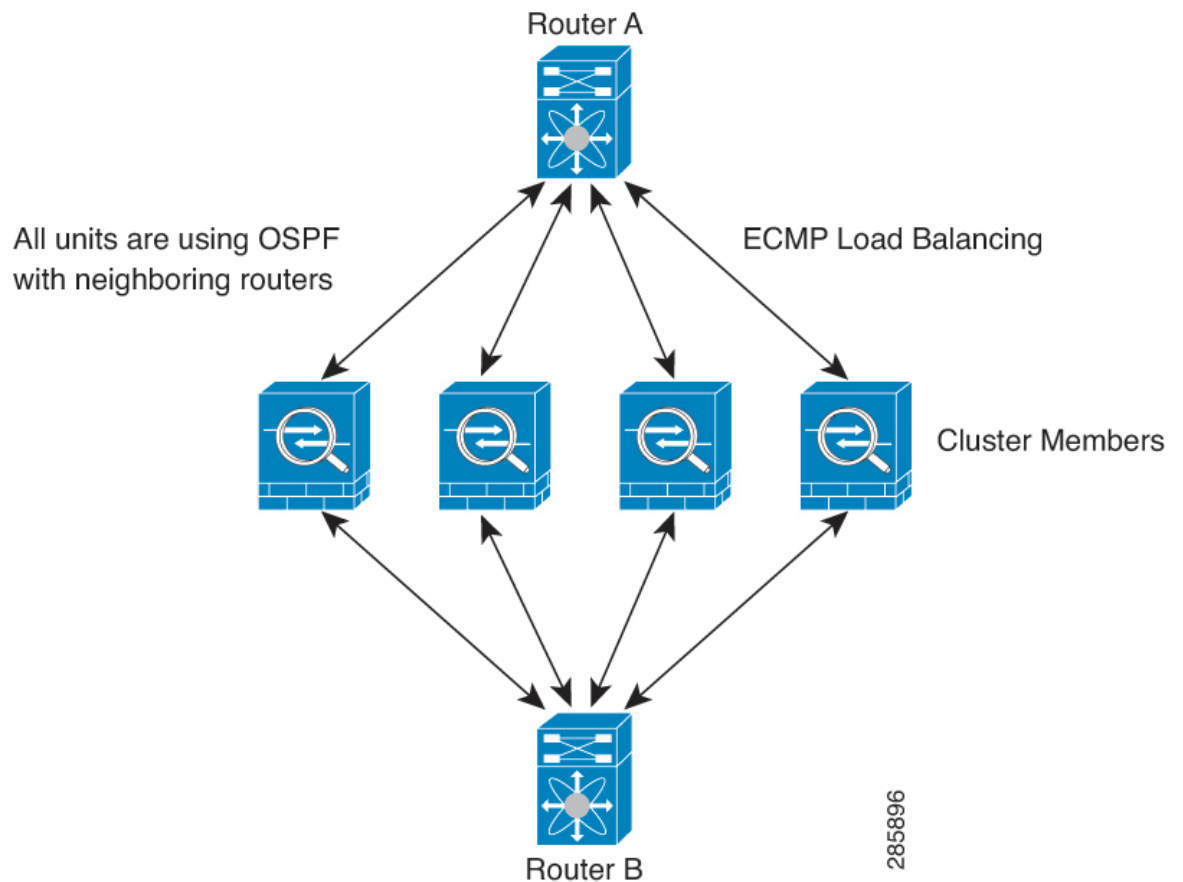
データノードが制御ノードからルートを学習すると、各ノードが個別に転送の判断を行います。

OSPF LSA データベースは、制御ノードからデータノードに同期されません。制御ノードのスイッチオーバーが発生した場合、ネイバールータが再起動を検出します。スイッチオーバーは透過的ではありません。OSPF プロセスが IP アドレスの 1 つをルータ ID として選択します。必須ではありませんが、スタティック ルータ ID を割り当てることができます。これで、同じルータ ID がクラスタ全体で使用されるようになります。割り込みを解決するには、OSPF ノンストップ フォワーディング機能を参照してください。

個別インターフェイスモードでのダイナミックルーティング

個別インターフェイスモードでは、各ノードがスタンドアロンルータとしてルーティングプロトコルを実行します。ルートの学習は、各ノードが個別に行います。

図 2: 個別インターフェイスモードでのダイナミックルーティング



上の図では、ルータ A はルータ B への等コストパスが 4 本あることを学習します。パスはそれぞれ 1 つの ASA を通過します。ECMP を使用して、4 パス間でトラフィックのロードバランシングを行います。各 ASA は、外部ルータと通信するときに、それぞれ異なるルータ ID を選択します。

管理者は、各ノードに異なるルータ ID が設定されるように、ルータ ID のクラスタプールを設定する必要があります。

EIGRP は、個別のインターフェイスモードのクラスタピアとのネイバー関係を形成しません。



- (注) 冗長性確保のためにクラスタが同一ルータに対して複数の隣接関係を持つ場合、非対称ルーティングが原因で許容できないトラフィック損失が発生する場合があります。非対称ルーティングを避けるためには、同じトラフィックゾーンにこれらすべての ASA インターフェイスをまとめます。[トラフィックゾーンの設定](#)を参照してください。

マルチ コンテキスト モードのダイナミック ルーティング

マルチ コンテキスト モードでは、各コンテキストで個別のルーティング テーブルおよびルーティング プロトコル データベースが維持されます。これにより、各コンテキストの OSPFv2 および EIGRP を個別に設定することができます。EIGRP をあるコンテキストで設定し、OSPFv2 を同じまたは異なるコンテキストで設定できます。混合コンテキストモードでは、ルーテッドモードのコンテキストの任意のダイナミック ルーティング プロトコルをイネーブルにできます。RIP および OSPFv3 は、マルチ コンテキスト モードではサポートされていません。

次の表に、EIGRP、OSPFv2、OSPFv2 および EIGRP プロセスへのルートの配布に使用されるルート マップ、およびマルチ コンテキスト モードで使用されている場合にエリアを出入りするルーティングアップデートをフィルタリングするために OSPFv2 で使用されるプレフィックス リストの属性を示します。

EIGRP	OSPFv2	ルートマップとプレフィックスのリスト
コンテキストごとに1つのインスタンスがサポートされます。	コンテキストごとに2つのインスタンスがサポートされます。	該当なし
システム コンテキストでディセーブルになっています。		該当なし
2つのコンテキストが同じまたは異なる自律システム番号を使用できます。	2つのコンテキストが同じまたは異なるエリア ID を使用できます。	該当なし
2つのコンテキストの共有インターフェイスでは、複数の EIGRP のインスタンスを実行できます。	2つのコンテキストの共有インターフェイスでは、複数の OSPF のインスタンスを実行できます。	該当なし
共有インターフェイス間の EIGRP インスタンスの相互作用がサポートされます。	共有インターフェイス間の OSPFv2 インスタンスの相互作用がサポートされます。	該当なし
シングル モードで使用可能なすべての CLI はマルチ コンテキスト モードでも使用できます。		
各 CLI は使用されているコンテキストでだけ機能します。		

ルートのリソース管理

routes というリソース クラスは、コンテキストに存在できるルーティング テーブル エントリの最大数を指定します。これは、別のコンテキストの使用可能なルーティング テーブル エントリに影響を与える1つのコンテキストの問題を解決し、コンテキストあたりの最大ルート エントリのより詳細な制御を提供します。

明確なシステム制限がないため、このリソース制限には絶対値のみを指定できます。割合制限は使用できません。また、コンテキストあたりの上限および下限がないため、デフォルトクラ

スは変更されません。コンテキストのスタティックまたはダイナミック ルーティング プロトコル（接続、スタティック、OSPF、EIGRP、および RIP）のいずれかに新しいルートを追加し、そのコンテキストのリソース制限を超えた場合、ルートの追加は失敗し、syslog メッセージが生成されます。

管理トラフィック用ルーティングテーブル

標準的なセキュリティ対策として、多くの場合、（デバイスからの）管理トラフィックをデータトラフィックから分離する必要があります。この分離を実現するために、ASA デバイスは管理専用トラフィックとデータトラフィックに個別のルーティングテーブルを使用します。個別のルーティングテーブルを使用することで、データと管理用に別のデフォルトルートを作成できます。

各ルーティングテーブルのトラフィックのタイプ

デバイス間トラフィックでは、常にデータルーティングテーブルが使用されます。

デバイス発信トラフィックでは、タイプに応じて、デフォルトで管理専用ルーティングテーブルまたはデータルーティングテーブルが使用されます。デフォルトのルーティングテーブルで一致が見つからなかった場合は、他のルーティングテーブルがチェックされます。

- 管理専用テーブルのデバイス発信トラフィックには、HTTP、SCP、TFTP、**copy** コマンド、スマートライセンス、Smart Call Home、**trustpoint**、**trustpool** などを使用してリモートファイルを開く機能が含まれています。
- データテーブルのデバイス発信トラフィックには、ping、DNS、DHCP などの他のすべての機能が含まれます。

管理専用ルーティングテーブルに含まれるインターフェイス

管理専用インターフェイスには、すべての **Management x/x** インターフェイス、および管理専用として設定したすべてのインターフェイスが含まれています。

他のルーティングテーブルへのフォールバック

デフォルトのルーティングテーブルで一致が見つからなかった場合は、他のルーティングテーブルがチェックされます。

デフォルト以外のルーティングテーブルの使用

デフォルトのルーティングテーブルにないインターフェイスに移動するために、ボックス内のトラフィックを必要とするとき、場合によっては、他のテーブルへのフォールバックに頼るのではなく、インターフェイスを設定するときにそのインターフェイスを指定する必要があります。ASA は、指定されたインターフェイスのルートのみをチェックします。たとえば、管理専用インターフェイスから ping を送信する必要がある場合は、ping 機能でインターフェイスを指定します。他方、データルーティングテーブルにデフォルトルートがある場合は、デフォルトルートに一致し、管理ルーティングテーブルにフォールバックすることは決してありません。

ダイナミック ルーティング

管理専用ルーティングテーブルは、データ インターフェイス ルーティング テーブルから分離したダイナミックルーティングをサポートします。ダイナミック ルーティング プロセスは管理専用インターフェイスまたはデータインターフェイスで実行されなければなりません。両方のタイプを混在させることはできません。分離した管理ルーティングテーブルが含まれていない以前のリリースからアップグレードする際、データインターフェイスと管理インターフェイスが混在し、同じダイナミックルーティングプロセスを使用している場合、管理インターフェイスは破棄されます。

VPN 要件の管理アクセス機能

VPN を使用している際に ASA で参加したインターフェイス以外のインターフェイスに管理アクセスを許可する管理アクセス機能を設定した場合、分離した管理およびデータルーティングテーブルに関するルーティングの配慮のために、VPN 終端インターフェイスと管理アクセスインターフェイスは同じタイプである必要があります。両方とも管理専用インターフェイスまたは通常のデータ インターフェイスである必要があります。

管理インターフェイスの識別

management-only で設定されたインターフェイスは、管理インターフェイスと見なされます。

次の設定では、GigabitEthernet0/0 と Management0/0 の両インターフェイスは、管理インターフェイスと見なされます。

```
a/admin(config-if)# show running-config int g0/0
!
interface GigabitEthernet0/0
  management-only
  nameif inside
  security-level 100
  ip address 10.10.10.123 255.255.255.0
  ipv6 address 123::123/64
a/admin(config-if)# show running-config int m0/0
!
interface Management0/0
  management-only
  nameif mgmt
  security-level 0
  ip address 10.106.167.118 255.255.255.0
a/admin(config-if)#
```

等コスト マルチパス (ECMP) ルーティング

ASA は、等コスト マルチパス (ECMP) ルーティングをサポートしています。

インターフェイスごとに最大8つの等コストのスタティックルートまたはダイナミックルートを設定できます。たとえば、次のように異なるゲートウェイを指定する外部インターフェイスで複数のデフォルト ルートを設定できます。

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

この場合、トラフィックは、10.1.1.2、10.1.1.3 と 10.1.1.4 間の外部インターフェイスでロードバランスされます。トラフィックは、送信元 IP アドレスと宛先 IP アドレス、着信インターフェイス、プロトコル、送信元ポートと宛先ポート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。

トラフィックゾーンを使用した複数のインターフェイス間の ECMP

インターフェイスのグループを含むようにトラフィックゾーンを設定する場合、各ゾーン内の最大 8 つのインターフェイス間に最大 8 つの等コストのスタティックルートまたはダイナミックルートを設定できます。たとえば、次のようにゾーン内の 3 つのインターフェイス間に複数のデフォルト ルートを設定できます。

```
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.2
route for 0.0.0.0 0.0.0.0 through outside3 to 10.3.1.2
```

同様に、ダイナミックルーティングプロトコルは、自動的に等コストルートを設定できます。ASA では、より堅牢なロード バランシング メカニズムを使用してインターフェイス間でトラフィックをロード バランスします。

ルートが紛失した場合、デバイスはフローをシームレスに別のルートに移動させます。

プロキシ ARP 要求のディセーブル化

あるホストから同じイーサネット ネットワーク上の別のデバイスに IP トラフィックを送信する場合、そのホストは送信先のデバイスの MAC アドレスを知る必要があります。ARP は、IP アドレスを MAC アドレスに解決するレイヤ 2 プロトコルです。ホストは IP アドレスの所有者を尋ねる ARP 要求を送信します。その IP アドレスを所有するデバイスは、自分が所有者であることを自分の MAC アドレスで返答します。

プロキシ ARP は、デバイスが ARP 要求に対してその IP アドレスを所有しているかどうかに関係なく自分の MAC アドレスで応答するときに使用されます。NAT を設定し、ASA インターフェイスと同じネットワーク上のマッピングアドレスを指定する場合、ASA でプロキシ ARP が使用されます。トラフィックがホストに到達できる唯一の方法は、ASA でプロキシ ARP が使用されている場合、MAC アドレスが宛先マッピングアドレスに割り当てられていると主張することです。

まれに、NAT アドレスに対してプロキシ ARP をディセーブルにすることが必要になります。

既存のネットワークと重なる VPN クライアントアドレスプールがある場合、ASA はデフォルトで、すべてのインターフェイス上でプロキシ ARP 要求を送信します。同じレイヤ 2 ドメイン上にもう 1 つインターフェイスがあると、そのインターフェイスは ARP 要求を検出し、自分の MAC アドレスで応答します。その結果、内部ホストへの VPN クライアントのリターントラフィックは、その誤ったインターフェイスに送信され、破棄されます。この場合、プロキシ ARP 要求をそれらが不要なインターフェイスでディセーブルにする必要があります。

手順

- ステップ 1 **[Configuration] > [Device Setup] > [Routing] > [Proxy ARP/Neighbor Discovery]** の順に選択します。
- [Interface] フィールドにインターフェイス名が一覧表示されます。[Enabled] フィールドには、NAT グローバルアドレスに対してプロキシ ARP/ネイバー探索がイネーブルか (Yes) ディセーブルか (No) が表示されます。
- ステップ 2 選択したインターフェイスに対してプロキシ ARP/ネイバー探索をイネーブルにするには、[Enable] をクリックします。デフォルトでは、プロキシ ARP/ネイバー探索はすべてのインターフェイスに対してイネーブルです。
- ステップ 3 選択したインターフェイスに対してプロキシ ARP/ネイバー探索をディセーブルにするには、[Disable] をクリックします。
- ステップ 4 **[Apply]** をクリックして設定を実行コンフィギュレーションに保存します。

ルーティング テーブルの表示

ルーティング テーブルにある ASDM のすべてのルートを表示するには、**[Monitoring] > [Routing] > [Routes]** の順に選択します。各行は 1 つのルートを表します。

ルート概要の履歴

表 2: ルート概要の履歴

機能名	プラットフォーム リリース	機能情報
管理インターフェイス用のルーティングテーブル	9.5(1)	データトラフィックから管理トラフィックを区別して分離トラフィック専用のルーティングテーブルが追加されました。それぞれの専用ルーティングテーブルは IPv4 と Ipv6 の ASA の各コンテキストごとに作成されます。さらに、ASA の各コンテキストに対して、RIB と FIB の両方に 2 つの予備のルーティングテーブルが追加されます。 次の画面が更新されました。

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。