Firepower Threat Defense 用の RIP

この章では、ルーティング情報プロトコル（RIP）を使用してデータをルーティングし、認証を実行し、ルーティング情報を再配布するように Firepower Threat Defense を設定する方法について説明します。

RIP について

RIP と呼ばれることが多い Routing Information Protocol は、すべてのルーティング プロトコルの中で最も堅牢なものの 1 つです。RIP には、ルーティング アップデート プロセス、RIP ルーティング メトリック、ルーティング安定性、ルーティング タイマーの 4 つの基本的なコンポーネントがあります。RIP をサポートしているデバイスは、ルーティング アップデート メッセージを定期的に、またネットワーク トポロジが変更されたときに送信します。これらの RIP パケットには、デバイスが到達可能なネットワークに関する情報、さらに宛先アドレスに到達するためにパケットが通過しなければならないルータやゲートウェイの数が含まれています。RIP では、生成されるトラフィックは OSPF より多くなりますが、設定は OSPF より容易です。

RIP は、ホップ カウントをパス選択のメトリックとして使用するディスタンス ベクター ルーティング プロトコルです。インターフェイス上で RIP が有効になっている場合、インターフェイスは、ネイバー デバイスと RIP ブロードキャストを交換して、ルートの動的な学習およびアドバタイズを行います。

Firepower Threat Defense デバイス は、RIP バージョン 1 と RIP バージョン 2 の両方をサポートしています。RIP バージョン 1 では、ルーティング アップデートでサブネットマスクは送信されません。RIP バージョン 2 では、ルーティング アップデートでサブネットマスクが送信され、可変長サブネット マスクがサポートされています。さらに、RIP バージョン 2 では、ルーティング アップデートを交換するときのネイバー認証がサポートされています。この認証により、信頼性の高い送信元から信頼できるルーティング情報が Firepower Threat Defense デバイスで受信できるようになります。

RIP は、初期設定が簡単で、トポロジが変更されても設定を更新する必要がないため、スタティック ルーティングより有利です。RIP の欠点は、スタティック ルーティングよりネットワークや処理オーバーヘッドが大きいことです。

ルーティング アップデート プロセス

RIPは、ルーティングアップデートメッセージを定期的に送信するだけでなく、ネットワークトポロジが変更された場合にも送信します。ルータは、エントリの変更が含まれるルーティング アップデートを受け取ると、新しいルートを反映するようにそのルーティング テーブルを更新します。パスのメトリック値は1ずつ大きくなり、送信者はネクスト ホップとして示されます。RIP ルータは、宛先に対する最適なルート（メトリック値が最も小さいルート）だけを保持します。ルータは、そのルーティング テーブルを更新した後、他のネットワーク ルータに変更を通知するために、ルーティングアップデートの送信をただちに開始します。これらのアップデートは、RIP ルータが送信する定期的にスケジュールされたアップデートとは独立して送信されます。

RIP のルーティング メトリック

RIP は、1 つのルーティング メトリック（ホップ カウント）を使用して発信元と宛先ネットワークとの距離を測定します。発信元から宛先までのパスの各ホップにはホップ カウント値（通常は1）が割り当てられます。ルータが、新しいまたは変更された宛先ネットワーク エントリが含まれるルーティングアップデートを受け取ると、アップデートで示されたメトリック値に 1 を加算し、そのネットワークをルーティング テーブルに入れます。送信者の IP アドレスがネクスト ホップとして使用されます。

RIP 安定性機能

RIP は、送信元から宛先へのパスで許可されるホップ数に制限を導入することにより、ルーティング ループが無限に続くことを防止しています。パス内のホップの最大数は 15 です。新しいまたは変更されたエントリが含まれるルーティングアップデートをルータが受信し、メトリック値に1を加えた結果、メトリックが無限（つまり16）になる場合は、ネットワークの宛先は到達不能と見なされます。この安定性機能の欠点は、この機能によってRIPネットワークの直径の最大値が 16 ホップ未満に制限されることです。

RIPには、その他にも、多くのルーティングプロトコルに共通の安定性機能がいくつか含まれます。ネットワークトポロジは急激に変化する可能性がありますが、これらの機能は、安定性を提供するように設計されています。たとえば、RIPでは、スプリットホライズンとホールドダウン メカニズムを実装して、間違ったルーティング情報が伝搬されることを防止しています。

RIP タイマー

RIP では、多数のタイマーを使用してそのパフォーマンスを調整しています。これらのタイマーには、ルーティングアップデートタイマー、ルートタイムアウトタイマー、ルートフラッ

シュタイマーがあります。ルーティングアップデートタイマーは、定期的なルーティングアップデートの間隔を測ります。通常は 30 秒に設定されており、タイマーがリセットされたときにはランダムな時間がわずかに追加されます。これは、すべてのルータがそのネイバーを同時にアップデートしようとした結果発生する輻輳を防ぐためです。ルーティング テーブルの各エントリには、ルートタイムアウト タイマーが関連付けられています。ルートタイムアウト タイマーが期限切れになると、ルートには無効のマークが付きますが、ルートフラッシュ タイマーが期限切れになるまではテーブル内に保持されます。

RIP のガイドライン

IPv6 のガイドライン

IPv6 はサポートされません。

その他のガイドライン

次の情報は、RIP バージョン 2 だけに適用されます。

- ネイバー認証を使用する場合、認証キーとキー ID は、RIP バージョン 2 アップデートをそのインターフェイスに提供するすべてのネイバーデバイス上で同じにする必要があります。
- RIP バージョン 2 の場合、Firepower Threat Defense デバイス は、マルチキャスト アドレス 224.0.0.9 を使用してデフォルト ルート アップデートを送受信します。パッシブ モードでは、そのアドレスでルート アップデートが受信されます。
- RIP バージョン 2 がインターフェイス上で設定されると、マルチキャスト アドレス 224.0.0.9 がそのインターフェイス上で登録されます。RIP バージョン 2 設定がインターフェイスから削除されると、そのマルチキャスト アドレスの登録は解除されます。

制限事項

- RIP アップデートは、Firepower Threat Defense デバイス のインターフェイス間を通過できません。
- RIP バージョン 1 では、可変長サブネット マスクがサポートされていません。
- RIP の最大ホップ カウントは 15 です。ホップ カウントが 15 を超えるルートは、到達不能と見なされます。
- RIP の収束は、他のルーティング プロトコルと比べて時間がかかります。
- Firepower Threat Defense デバイス では、RIP プロセスを 1 つだけイネーブルにできます。

RIP の設定

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 ルーティング プロトコルです。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、Firepower Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）] タブを選択します。

ステップ 3 コンテンツ テーブルから [RIP] を選択します。

ステップ 4 [RIP を有効にする（Enable RIP）] チェックボックスをオンにして、RIP を設定します。

ステップ 5 [RIP バージョン（RIP Version）] ドロップダウン リストから、RIP の更新を送受信するための RIP バージョンを選択します。

ステップ 6 （オプション）[デフォルト ルートの生成（Generate Default Route）] チェックボックスをオンにして、指定したルート マップに基づく配布用のデフォルト ルートを生成します。

a) [ルート マップ（Route map）] フィールドで、デフォルト ルートの生成に使用するルート マップ名を指定します。
[ルート マップ（Route map）] フィールドで指定したルート マップが存在する場合、特定のインターフェイスで配布されるデフォルト ルート 0.0.0.0/0 が生成されます。

ステップ 7 [RIP バージョン（RIP Version）] として [バージョン 2 の送受信（Send and Receive Version 2）] を選択した場合、[自動集約の有効化（Enable Auto Summary）] オプションが使用可能になります。[自動集約の有効化（Enable Auto Summary）] チェックボックスをオンにすると、自動ルート集約が有効になります。切断されているサブネット間のルーティングを実行する必要がある場合は、自動サマライズを無効にします。自動サマライズを無効にすると、サブネットがアドバタイズされます。

（注） RIP バージョン 1 では、常に自動サマライズが使用されます。無効にすることはできません。

ステップ 8 [ネットワーク（Networks）] タブをクリックします。RIP ルーティングに対して 1 つ以上のネットワークを定義します。IP アドレスを入力するか、目的のネットワーク/ホスト オブジェクトを入力または選択します。セキュリティ アプライアンスの設定に追加できるネットワーク数に制限はありません。このコマンドで定義されるネットワークに属しているインターフェイスは、RIP ルーティング プロセスに参加します。RIP ルーティング更新は、指定したネットワークのインターフェイスだけを介して送受信されます。また、インターフェイスのネットワークを指定しない場合、インターフェイスは RIP 更新でアドバタイズされません。

（注） RIP では、IPv4 オブジェクトのみがサポートされます。

ステップ 9 （オプション）[パッシブ インターフェイス（Passive Interfaces）] タブをクリックします。このオプションを使用して、アプライアンスでパッシブ インターフェイスを指定してから、アク

ティブ インターフェイスを指定します。デバイスは、そのルーティング テーブルを入力するための情報を使用して、パッシブ インターフェイスでの RIP ルートのブロードキャストをリッスンしますが、パッシブ インターフェイスでのルーティング更新はブロードキャストしません。パッシブとして指定されていないインターフェイスは、更新を送受信します。

ステップ 10 [再配布（Redistribution）] タブをクリックして、再配布ルートを管理します。これらは、他のルーティング プロセスから RIP ルーティング プロセスに再配布されているルートです。

a) [追加（Add）] をクリックして、再配布ルートを指定します。

b) [プロトコル（Protocol）] ドロップダウン リストから、RIP ルーティング プロセスに再配布するルーティング プロトコルを選択します。

（注） OSPF プロトコルの場合は、プロセス ID を指定します。同様に、BGP の場合は AS パスとして指定します。[プロトコル（Protocol）] ドロップダウン リストで [接続済み（Connected）] オプションを選択すると、直接接続されたネットワークを RIP ルーティング プロセスに再配布できます。

c) （オプション）OSPF ルートを RIP ルーティング プロセスに再配布する場合、[一致（Match）] ドロップダウン リストで、再配布する特定のタイプの OSPF ルートを選択できます。複数のタイプを選択するには、Ctrl を押しながらクリックします。

- [内部（Internal）]：自律システム（AS）の内部のルートが再配布されます。
- [外部 1（External 1）]：AS に対して外部のタイプ 1 ルートが再配布されます。
- [外部 2（External 2）]：AS に対して外部のタイプ 2 ルートが再配布されます。
- [NSSA 外部 1（NSSA External 1）]：Not-So-Stubby Area（NSSA）の外部のタイプ 1 ルートが再配布されます。
- [NSSA 外部 2（NSSA External 2）]：NSSA に対して外部のタイプ 2 ルートが再配布されます。

（注） デフォルトの一致は、[内部（Internal）]、[外部 1（External 1）]、および [外部 2（External 2）] です。

d) [メトリック（Metric）] ドロップダウン リストから、再配布されたルートに適用する RIP メトリック タイプを選択します。選択肢は次の 2 つです。

- [トランスペアレント（Transparent）]：現在のルート メトリックを使用します。
- [指定値（Specified Value）]：特定のメトリック値を割り当てます。[メトリック値（Metric Value）] フィールドに 0 ～ 16 の特定の値を入力します。
- [なし（None）]：メトリックが指定されません。再配布されたルートに適用するメトリック値を使用しないでください。

e) （オプション）[ルート マップ（Route Map）] フィールドに、ルートが RIP ルーティング プロセスに再配布される前に満たす必要のあるルート マップの名前を指定します。ルートは、IP アドレスがルートマップ アドレス リストの許可文と一致する場合にのみ再配布されます。

f) [OK] をクリックします。

ステップ 11 （オプション）[フィルタリング（Filtering）] タブをクリックして、RIP ポリシーのフィルタを管理します。このセクションでは、インターフェイスでのルーティング更新の回避、ルーティング更新でのルートのアドバタイズ制御、ルーティング更新の処理制御、およびルーティング更新の送信元フィルタリングに、フィルタを使用します。

a) [追加（Add）] をクリックして、RIP フィルタを追加します。

b) [トラフィックの方向（Traffic Direction）] フィールドでフィルタリングされるトラフィックのタイプ（[着信（Inbound）] または [発信（Outbound）]）を選択します。

（注） トラフィックの方向が着信の場合、インターフェイス フィルタだけを定義できます。

c) [フィルタ オン（Filter On）] フィールドで適切なラジオ ボタンを選択して、フィルタがインターフェイスまたはルートのいずれに基づくかを指定します。[インターフェイス（Interface）] を選択した場合、ルーティング更新がフィルタリングされるインターフェイスの名前を入力または選択します。[ルート（Route）] を選択した場合、ルート タイプを選択します。

- [スタティック（Static）]：スタティック ルートだけがフィルタリングされます。
- [接続済み（Connected）]：接続されたルートだけがフィルタリングされます。
- [OSPF]：指定した OSPF プロセスによって検出された OSPFv2 ルートだけがフィルタリングされます。フィルタリングされる OSPF プロセスの [プロセス ID（Process ID）] を入力します。
- [BGP]：指定した BGP プロセスによって検出された BGPv4 ルートだけがフィルタリングされます。フィルタリングされる BGP プロセスの AS パスを入力します。

d) [アクセス リスト（Access List）] フィールドで、許可されるネットワークまたは RIP ルート アドバタイズメントから削除されるネットワークを定義する 1 つ以上のアクセス コントロール リスト（ACL）の名前を入力または選択します。

e) [OK] をクリックします。

ステップ 12 （オプション）[ブロードキャスト（Broadcast）] タブをクリックして、インターフェイス設定を追加または編集します。[ブロードキャスト（Broadcast）] タブを使用して、インターフェイスごとに送受信するグローバル RIP バージョンをオーバーライドできます。また、有効な RIP アップデートを確認するための認証を実装する場合は、インターフェイスごとの認証パラメータを定義できます。

a) [追加（Add）] をクリックして、インターフェイス設定を追加します。

b) [インターフェイス（Interface）] フィールドで、このアプライアンスで定義されるインターフェイスを入力または選択します。

c) [送信（Send）] オプションで、該当するボックスを選択して、RIP **バージョン 1**、**バージョン 2**、または両方を使用して更新を送信するように指定します。これらのオプションを使用して、指定されたインターフェイスについて、指定したグローバルな送信バージョンをオーバーライドできます。

d) [受信（Receive）] オプションで、該当するボックスを選択して、RIP **バージョン 1**、**バージョン 2**、または両方を使用して更新を受け入れるように指定します。これらのオプションを使用して、指定されたインターフェイスについて、指定したグローバルな受信バージョンをオーバーライドできます。

e) RIP ブロードキャストに対してこのインターフェイスで使用される**認証**を選択します。

- [なし（None）]：認証はありません。
- [MD5]：MD5 を使用します。
- [クリア テキスト（Clear Text）]：クリア テキスト認証を使用します。

[MD5] または [クリア テキスト（Clear Text）] を選択した場合、次の認証パラメータも指定する必要があります。

- [キー ID（Key ID）]：認証キーの ID。有効な値は 0 ～ 255 です。
- [キー（Key）]：選択した認証方式で使用されるキー。最大 16 文字まで使用できます
- [確認（Confirm）]：確認のために、認証キーを再度入力します。

f) [OK] をクリックします。