



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 Threat Defense を設定する方法について説明します。仮想ルーティングを使用しているデバイスの場合、ユーザ定義の仮想ルータではなく、グローバル仮想ルータに対してのみ RIP を設定できます。

- [RIP について \(1 ページ\)](#)
- [RIP の要件と前提条件 \(3 ページ\)](#)
- [RIP のガイドライン \(4 ページ\)](#)
- [RIP の設定 \(4 ページ\)](#)

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。

Secure Firewall 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 Secure Firewall 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、エントリー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ー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ー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。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、間違っただけの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。RIPのタイマーステージは次のとおりです。

- 更新：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。これは、デバイスがルーティングアップデートを送信する頻度です。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。
- 無効：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。これは、デバイスが最後の有効な更新を受信してからの秒数です。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。このタイマーが期限切れになると、ルートはホールドダウン状態になります。デフォルト値は 180 秒 (3 分) です。
- ホールドダウン：ホールドダウン期間は、ホールドダウン状態のルート (つまり、無効とマークされたルート) の新しい更新を受け入れる前にシステムが待機する秒数です。デフォルト値は 180 秒 (3 分) です。
- フラッシュ：ルートフラッシュタイマーは、システムが最後の有効な更新を受信してから、ルートが破棄されてルーティングテーブルから削除されるまでの秒数です。デフォルトは 240 秒 (4 分) です。

たとえば、隣接ルータのインターフェイスがダウンすると、システムは隣接ルータからルーティングアップデートを受信しなくなります。この時点で、無効タイマーとフラッシュタイマーが増加し始めます。最初の 180 秒間は何も起こりません。180 秒後、無効タイマーが期限切れになり、ルートが無効になりますが、ホールドダウンタイマーが開始され、ルートはさらに 60 秒間保持されます。隣接ルータのインターフェイスステータスに関する更新がまだない場合 (つまり、まだダウンしている場合)、ルートはフラッシュ状態になり、システムは最後の更新から合計 240 秒 (無効タイマーの 180 秒とホールドダウンタイマーの 60 秒) 待機してから、ルートをフラッシュします。隣接ルータインターフェイスがすぐに起動しても、ホールドダウンタイマーが残りの 120 秒を完了するまで、システムはルーティングアップデートを受け入れません。

RIP の要件と前提条件

モデルのサポート

Threat Defense

Threat Defense Virtual

サポートされるドメイン

任意

ユーザの役割

管理者

ネットワーク管理者

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、Secure Firewall 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、Secure Firewall 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。
- Secure Firewall 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せん。

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、Threat Defense デバイスを編集します。
- ステップ 2** [ルーティング (Routing)] 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作成します。
- 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** [Networks] 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)] 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)] 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 を押しながらかlickします。
- [内部 (Internal)] : 自律システム (AS) に対して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 の外部のタイプ 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。
- (注) [なし (None)] オプションは、静的プロトコルと接続済みプロトコルにのみ適用されます。
- 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。新しいルートマップオブジェクトを作成するには、Add(+) をクリックします。新しいルートマップを追加する手順については、「[ルートマップエントリの設定](#)」を参照してください。
- 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)] 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せん。

- c) [フィルタオン (Filter On)] フィールドで適切な項目を選択して、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)] をクリックした場合、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)] をクリックした場合、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。新しい標準アクセスリストオブジェクトを追加するには、**Add (+)** をクリックし、[標準 ACL オブジェクトの設定](#)を参照してください。
- 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)] 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)] 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。
-

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。