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Firewall 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。

About RIP

The Routing Information Protocol, or RIP, as it is more commonly called, is one of the most enduring of all routing protocols. RIP has four basic components: routing update process, RIP routing metrics, routing stability, and routing timers. Devices that support RIP send routing-update messages at regular intervals and when the network topology changes. These RIP packets include information about the networks that the devices can reach, as well as the number of routers or gateways that a packet must travel through to reach the destination address. RIP generates more traffic than OSPF, but is easier to configure.

RIP is a distance-vector routing protocol that uses hop count as the metric for path selection. When RIP is enabled on an interface, the interface exchanges RIP broadcasts with neighboring devices to dynamically learn about and advertise routes.

The Secure Firewall Threat Defense device supports both RIP Version 1 and RIP Version 2. RIP Version 1 does not send the subnet mask with the routing update. RIP Version 2 sends the subnet mask with the routing update and supports variable-length subnet masks. Additionally, RIP Version 2 supports neighbor authentication when routing updates are exchanged. This authentication ensures that the Secure Firewall Threat Defense device receives reliable routing information from a trusted source.

RIP has advantages over static routes because the initial configuration is simple, and you do not need to update the configuration when the topology changes. The disadvantage to RIP is that there is more network and processing overhead than in static routing.

Routing Update Process

RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by 1, and the sender is indicated as the next hop. RIP routers maintain only the best route (the route with the lowest metric value) to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change. These updates are sent independently of the regularly scheduled updates that RIP routers send.

RIP Routing Metric

RIP uses a single routing metric (hop count) to measure the distance between the source and a destination network. Each hop in a path from source to destination is assigned a hop count value, which is typically 1. When a router receives a routing update that contains a new or changed destination network entry, the router adds 1 to the metric value indicated in the update and enters the network in the routing table. The IP address of the sender is used as the next hop.

RIP Stability Features

RIP prevents routing loops from continuing indefinitely by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops in a path is 15. If a router receives a routing update that contains a new or changed entry, and if increasing the metric value by 1 causes the metric to be infinity (that is, 16), the network destination is considered unreachable. The downside of this stability feature is that it limits the maximum diameter of a RIP network to less than 16 hops.

RIP includes a number of other stability features that are common to many routing protocols. These features are designed to provide stability despite potentially rapid changes in network topology. For example, RIP implements the split horizon and hold-down mechanisms to prevent incorrect routing information from being propagated.

RIP Timers

RIP uses numerous timers to regulate its performance. Following are the timer stages for RIP:

- Update—The routing-update timer is the interval between periodic routing updates. This is how often the device sends routing updates. Generally, it is set to 30 seconds, with a small random amount of time added whenever the timer is reset. This is done to help prevent congestion, which could result from all routers simultaneously attempting to update their neighbors.
- Invalid—Each routing table entry has a route-timeout timer associated with it. This is the number of seconds since the device received the last valid update. When the route-timeout timer expires, the route is marked invalid but is retained in the table until the route-flush timer expires. Once this timer expires, the route goes into holddown. The default is 180 seconds (3 minutes).
- Holddown—The holddown period is the number of seconds the system waits before accepting any new updates for the route that is in holddown (that is, routes that have been marked invalid). The default is 180 seconds (3 minutes).

- Flush—The route-flush timer is the number of seconds since the system received the last valid update until the route is discarded and removed from the routing table. The default is 240 seconds (4 minutes).

As an example, when the interface on an adjacent router goes down, the system no longer receives routing updates from the adjacent router. At this time, the Invalid and Flush timers start increasing. In the first 180 seconds, nothing will happen. After 180 seconds, the invalid timer expires, making the route invalid, and the Holddown timer starts and holds the route for another 60 seconds. If there is still no update regarding the interface status on the adjacent router (that is, it is still down), then the route enters into the Flush state where in total the system has waited for 240 seconds from the last update (180 seconds for the Invalid timer and 60 seconds for Holddown timer), and the system flushes the route. Even if the adjacent routers interface comes up immediately, the system does not accept a routing update until the Holddown timer completes the remaining 120 seconds.

RIP の要件と前提条件

Model support

Firewall Threat Defense

Firewall Threat Defense Virtual

Supported domains

Any

User roles

Admin

Network Admin

Guidelines for RIP

IPv6 Guidelines

Does not support IPv6.

Additional Guidelines

The following information applies to RIP Version 2 only:

- If using neighbor authentication, the authentication key and key ID must be the same on all neighbor devices that provide RIP Version 2 updates to the interface.
- With RIP Version 2, the Secure Firewall Threat Defense device transmits and receives default route updates using the multicast address 224.0.0.9. In passive mode, it receives route updates at that address.
- When RIP Version 2 is configured on an interface, the multicast address 224.0.0.9 is registered on that interface. When a RIP Version 2 configuration is removed from an interface, that multicast address is unregistered.

Limitations

- The Secure Firewall Threat Defense device cannot pass RIP updates between interfaces.
- RIP Version 1 does not support variable-length subnet masks.
- RIP has a maximum hop count of 15. A route with a hop count greater than 15 is considered unreachable.
- RIP convergence is relatively slow compared to other routing protocols.
- You can only enable a single RIP process on the Secure Firewall Threat Defense device.

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 [**Devices** > **Device Management**] を選択し、Firewall 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、自動サマライズをディセーブルにします。自動サマライズをディセーブルにすると、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 を押しながらクリックします。

- [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す。

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。