

RIP

The Routing Information Protocol (RIP) is a distance-vector routing protocol that

- enables devices to exchange routing information,
- supports authentication mechanisms, and
- facilitates redistribution of routing information.

RIP Configuration Constraints

There are constraints when deploying RIP on the Firewall Threat Defense:

- RIP configuration is restricted to the global virtual router and is not supported for user-defined virtual routers.

- RIP, on page 1
- Requirements and prerequisites for RIP, on page 2
- Guidelines for RIP, on page 2
- Configure RIP, on page 3
- How RIP routing updates work, on page 6
- RIP stability features, on page 7
- RIP timers, on page 7

RIP

Routing Information Protocol (RIP) is a distance-vector routing protocol that

- uses hop count as the metric for path selection,
- exchanges RIP broadcasts with neighboring devices to dynamically learn and advertise routes, and
- includes four basic components: routing update process, RIP routing metrics, routing stability, and routing timers.

RIP characteristics and versions

RIP is a widely used routing protocol. It sends routing updates at regular intervals and when the network topology changes. These updates provide information about network reachability and the number of hops to each destination.

You can configure RIP with less effort than OSPF, but it generates more network traffic. RIP supports both Version 1 and Version 2.

Secure Firewall Threat Defense device supports both RIP Version 1 and Version 2. RIP Version 1 does not send subnet masks with its updates; Version 2 supports variable-length subnet masks and neighbor authentication to ensure trusted routing information exchanges.

RIP offers simple configuration and adapts to topology changes. In contrast, static routes require manual updates for each change. RIP, however, incurs higher network and processing overhead compared to static routing.

RIP routing metric

A RIP routing metric is a network measurement that

- calculates the distance between a source and a destination network,
- assigns a hop count value, typically 1, to each hop in a network path from the source to the destination, and
- updates the routing table when new routing data is received, using the sender's IP address as the next hop.

Requirements and prerequisites for RIP

These requirements and prerequisites must be met for configuring RIP on supported firewall models.

Model support

Firewall Threat Defense

Firewall Threat Defense Virtual

Supported domains

Any

User roles

Administrator

Network Admin

Guidelines for RIP

IPv6 guidelines

RIP does not support IPv6.

RIP version 2 guidelines

Consider these guidelines for RIP Version 2 configuration:

- 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.

RIP limitations

These are the limitations of RIP:

- 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.

Configure RIP

RIP is a distance-vector routing protocol that uses hop count as the metric for path selection.

Use this procedure to define networks, manage redistribution, and apply interface-specific filtering or broadcast parameters.

Procedure

Step 1 Choose **Devices** > **Device Management**, and edit the Firewall Threat Defense device.

Step 2 Select the **Routing** tab, and select **RIP** from the table of contents.

Check the **Enable RIP** check box to configure the RIP settings.

Choose the RIP versions for sending and receiving RIP updates from the **RIP Version** drop-down list:

- **Receive Version 1 & 2, Send Version 1**
- **Send & Receive Version 1**
- **Send & Receive Version 2**

Step 3 (Optional) Check the **Generate Default Route** check box to generate a default route for distribution, based on the route map that you specify.

a) Specify a route map name to use for generating default routes, in the **Route Map** field.

Generate the default route 0.0.0.0/0 for distribution when a route map is specified in the **Route Map** field.

Step 4 When you choose Send and Receive Version 2, the **Enable Auto Summary** option is available. When the **Enable Auto Summary** check box is checked, automatic route summarization is enabled. Disable automatic summarization if you must perform routing between disconnected subnets. When automatic summarization is disabled, subnets are advertised.



Note RIP Version 1 always uses automatic summarization—you cannot disable it.

Step 5 Click **Networks**. Define one or more networks for RIP routing. Enter IP address(es), or enter or select the desired Network/Hosts objects. There is no limit to the number of networks you can add to the security appliance configuration. Interfaces belonging to the defined network will participate in the RIP routing. The RIP routing updates will be sent and received only through interfaces on the specified networks. Also, if the network of an interface is not specified, the interface will not be advertised in any RIP updates.



Note RIP only supports IPv4 objects.

(Optional) Click **Passive Interface**. Use this option to specify passive interfaces on the appliance, and by extension the active interfaces. The device receives RIP routing broadcasts on passive interfaces, using that information to populate its routing tables, but does not broadcast routing updates on passive interfaces. Interfaces that are not designated as passive receive and send updates.

Step 6 Click **Redistribution** to manage redistribution routes. These are the routes that are being redistributed from other routing processes into the RIP routing process.

a) Click **Add** to specify redistribution routes.

b) Choose the routing protocol to redistribute into the RIP routing process, in the **Protocol** drop-down list. Available options are **Static**, **Connected**, **OSPF**, **BGP**, and **EIGRP**.



Note For OSPF, specify the process ID in the **Process ID** field. For BGP, specify the AS number in the **AS Number** field. When you choose the Connected option in the **Protocol** drop-down list, you can redistribute directly connected networks into the RIP routing process.

c) (Optional) If you are redistributing OSPF routes into the RIP routing process, you can select specific types of OSPF routes to redistribute in the **Match** drop-down list. Ctrl-click to select multiple types:

- **Internal**: Routes internal to the autonomous system (AS) are redistributed.
- **External 1**: Type 1 routes external to the AS are redistributed.
- **External 2**: Type 2 routes external to the AS are redistributed.
- **NSSA External 1**: Type 1 routes external to a not-so-stubby area (NSSA) are redistributed.
- **NSSA External 2**: Type 2 routes external to an NSSA are redistributed.

Note The default is match Internal, External 1, and External 2.

d) Select the RIP metric type to apply to the redistributed routes in the **Metric** drop-down list. The three choices are:

- **Transparent**: Use the current route metric.
- **Specified Value**: Assign a specific metric value from 0 to 16 in the **Metric Value** field.
- **None**: No metric is specified. Do not use any metric value, to apply to redistributed routes.

Note **None** option is applicable only for **Static** and **Connected** protocols.

e) (Optional) Enter the name of a route map that must be satisfied, in the **Route Map** field before the route can be redistributed into the RIP routing process. Routes are redistributed only if IP address matches an allow statement in the route map address list. To create a new route map object, click **Add** (+). See Configure Route Map Entry for the procedure to add a new route map.

f) Click **OK**.

Step 7 (Optional) Click **Filtering** to manage filters for the RIP policy. In this section, filters are used to prevent routing updates through an interface, control the advertising of routes in routing updates, control the processing of routing updates and filtering sources of routing updates.

a) Click **Add** to add RIP filters.

b) Select the type of traffic to be filtered - Inbound or Outbound in the **Traffic Direction** field.

Note If traffic direction is inbound, you can only define an Interface filter.

c) Specify whether the filter is based on an Interface or a Route, by selecting appropriate option in the **Filter On** field. If you click **Interface**, you can enter or choose the name of the interface on which routing updates are to be filtered. If you click **Route**, you can choose the route type:

- **Static**: Only static routes are filtered.
- **Connected**: Only connected routes are filtered.
- **OSPF**: Only OSPFv2 routes discovered by the specified OSPF process are filtered. Enter the Process ID of the OSPF process to be filtered.
- **BGP**: Only BGPv4 routes discovered by the specified BGP process are filtered. Enter the value in the **Process ID** field.
- **EIGRP**: Only EIGRP routes are filtered.

d) In the **Access List** field, enter or choose the name of one or more access control lists (ACLs) that define the networks to be allowed or removed from RIP route advertisements. To add a new standard access list object, click **Add** (+) and see Configure a standard ACL object.

e) Click **OK**.

Step 8 (Optional) Click **Broadcast** to add or edit interface configurations. Using Broadcast, you can override the global RIP versions to send or receive per interface. You can also define the authentication parameters per interface if you want to implement authentication to ensure valid RIP updates.

a) Click **Add** to add interface configurations.
b) Enter or choose an interface defined on this appliance in the **Interface** field.
c) In the Send option, select the appropriate boxes to specify sending updates using the RIP **Version 1**, **Version 2**, or both. These options let you override, for the specified interface, the global Send versions specified.
d) In the Receive option, select the appropriate boxes to specify accepting updates using the RIP **Version 1**, **Version 2**, or both. These options let you override, for the specified interface, the global Receive versions specified.
e) Select the **Authentication** used on this interface for RIP broadcasts.

- **None**: No authentication
- **MD5**: Employ MD5
- **Clear Text**: Employ clear-text authentication

If you choose MD5 or Clear Text, you must also provide the following authentication parameters.

- **Key ID**: The ID of the authentication key; valid values are from 0 to 255.
- **Key**: The key used by the chosen authentication method; can contain up to 16 characters.
- **Confirm**: Enter the authentication key again to confirm.

f) Click **OK**.

How RIP routing updates work

Summary

Key components in the RIP routing update process include:

- RIP routers: Send and receive routing update messages to maintain network topology information
- Routing tables: Store the best routes to destinations with associated metric values
- Routing update messages: Contain network topology changes and route information
- Metric values: Determine the best path, with routers maintaining only the lowest metric route

Workflow

The process involves these stages:

1. RIP routers send routing-update messages at regular intervals and when the network topology changes.

2. 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.
3. RIP routers maintain only the best route to a destination, which is the route with the lowest metric value.
4. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change. These updates occur independently from regularly scheduled RIP router updates.

RIP stability features

RIP stability features are routing mechanisms that

- prevent routing loops by setting a limit on the number of hops in a path from source to destination,
- provide stability despite potentially rapid changes in network topology, and
- include split horizon and hold-down mechanisms to prevent incorrect routing information propagation.

Additional stability mechanisms

The maximum number of hops allowed in a path is 15. If a routing update shows a new or changed entry, the system increases the metric value to infinity (16), which makes the network destination unreachable. This stability mechanism limits the maximum diameter of a RIP network to fewer than 16 hops.

RIP timers

RIP timers are network protocol mechanisms that

- regulate RIP performance through timed intervals for routing updates and route management,
- control when routes are marked invalid, placed in holddown, or flushed from the routing table, and
- help prevent network congestion by managing the timing of routing updates across devices.

RIP timer stages

RIP uses numerous timers to regulate its performance. These 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, set to 30 seconds, a small random delay added to prevent simultaneous route updates.
- Invalid: Each routing table entry has a route-timeout timer for the last valid update. The route is marked invalid and moves to holddown once the timer expires. The default is 180 seconds (3 minutes).
- Holddown: The period the system waits before accepting any new updates for invalid routes. The default is 180 seconds (3 minutes).
- Flush: The route-flush timer marks the period from when the system receives the last valid update until the route is discarded and removed from the routing table. The default is 240 seconds (4 minutes).

RIP timer sequence when adjacent router interface goes down

When an adjacent router goes down, routing updates stop, and the Invalid and Flush timers start increasing. In the first 180 seconds, nothing will happen. After 180 seconds, the Invalid timer expires, marks the route invalid, and the Holddown timer begins, holding the route for 60 seconds.

If there is no routing update for the adjacent router's status (that is, it is still down), the route enters into the Flush state. 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 then the system flushes the route. Even if the adjacent router's interface comes up immediately, the system waits for the Holddown timer to complete the 120-second period before accepting updates.