

Configuration of Routing Information Protocol (RIP) Dynamic Routing on ISA500 Series Integrated Security Appliances

Objective

The Routing Information Protocol (RIP) is an interior gateway protocol (IGP) which is used to route traffic within a single autonomous system. RIP uses a single routing metric (hop count) to measure the distance between the source and destination networks. The RIP enabled network device dynamically learns network destinations and how to get to them and also advertises those destinations to its RIP enabled neighbors.

The objective of this document is to explain how to configure RIP on ISA500 series integrated security appliances.

Applicable Devices

- ISA500 Series Integrated Security Appliances

Software Version

- v1.1.14

Configuration of RIP

Step 1. Log in to the integrated security appliance configuration utility, and choose **Networking > Routing > Dynamic - RIP**. The *Dynamic - RIP* page opens:

Dynamic - RIP

RIP Enable: On Off

RIP Version: Version 1 Version 2 Default

Available Interface	RIP Enable	Authentication	Port Passive
WAN1	<input type="checkbox"/>	None	<input checked="" type="checkbox"/>
DEFAULT	<input type="checkbox"/>	None	<input type="checkbox"/>
GUEST	<input type="checkbox"/>	None	<input type="checkbox"/>
WAN2	<input type="checkbox"/>	None	<input checked="" type="checkbox"/>

Save Cancel

Step 2. By default, RIP is disabled. If RIP is to be enabled, click the **On** radio button.

Step 3. If RIP is enabled, click one of the following RIP version radio buttons.

- Version 1 — A class-based routing version. It does not include subnet information and therefore does not support variable length subnet masks (VLSM). RIPv1 also lacks support for authentication, making it vulnerable to attacks.
- Version 2 — Includes all the features of RIPv1 and also supports subnetting and authentication.
- Default — Uses RIPv1 to send data and RIPv2 for receiving data.

Step 4. Check the check box(es) corresponding to the WAN ports (WAN1, WAN2) or VLAN (DEFAULT, GUEST) under the RIP Enable column to enable rip on the port(s) and VLAN(s).

Dynamic - RIP

RIP Enable: On Off

RIP Version: Version 1 Version 2 Default

Available Interface	RIP Enable	Authentication	Port Passive
WAN1	<input checked="" type="checkbox"/>	None	<input checked="" type="checkbox"/>
DEFAULT	<input checked="" type="checkbox"/>	None	<input type="checkbox"/>
GUEST	<input checked="" type="checkbox"/>	None	<input type="checkbox"/>
WAN2	<input checked="" type="checkbox"/>	None	<input checked="" type="checkbox"/>

Save Cancel

Step 5. If RIP version 2 is chosen in step 3, click the **Edit (pencil)** icon corresponding to the port or VLAN to configure the authentication on it. The Authentication window opens:

Dynamic - RIP

RIP Enable: On Off

RIP Version: Version 1 Version 2 Default

Available Interface	RIP Enable	Authentication	Port Passive
WAN1	<input type="checkbox"/>	None	<input checked="" type="checkbox"/>
DEFAULT	<input type="checkbox"/>	None	<input type="checkbox"/>
GUEST	<input type="checkbox"/>	None	<input type="checkbox"/>
WAN2	<input type="checkbox"/>	None	<input checked="" type="checkbox"/>

Save Cancel

Step 6. Click one of the following radio buttons to describe the authentication method.

Authentication [Help](#)

None
 Simple Password Authentication (Length: 1 to 16 characters)
 MD5 Authentication

* MD5 Key ID : (Range: 1-255, Default: 1)
 * MD5 Auth Key: (Length: 1 to 64 characters)

OK Cancel

- None — Invalidates authentication.
- Simple Password Authentication — Authentication is validated through a simple password that is unencrypted.
- MD5 Authentication — Message-Digest Algorithm is used to check data integrity.

Step 7. If **Simple Password Authentication** is chosen in step 6, enter the password in the *Simple Password Authentication* field and click **OK**.

Authentication [Help](#)

None
 Simple Password Authentication (Length: 1 to 16 characters)
 MD5 Authentication

* MD5 Key ID : (Range: 1-255, Default: 1)
 * MD5 Auth Key: (Length: 1 to 64 characters)

OK Cancel

Step 8. If **MD5 Authentication** is chosen in step 6, enter the unique key ID in the *MD5 Key ID* field and the key in the *MD5 Auth Key* field and click **OK**.

Authentication [Help](#)

None
 Simple Password Authentication (Length: 1 to 16 characters)
 MD5 Authentication

* MD5 Key ID : (Range: 1-255, Default: 1)
 * MD5 Auth Key: (Length: 1 to 64 characters)





OK Cancel

Step 9. Check the check box (es) corresponding to the available interfaces under Port Passive column to enable the security appliance to receive RIP routing updates but not to advertise via that particular interface.

Dynamic - RIP

RIP Enable: On Off

RIP Version: Version 1 Version 2 Default

RIP Interfaces			
Available Interface	RIP Enable	Authentication	Port Passive
WAN1	<input type="checkbox"/>	 MD5	<input checked="" type="checkbox"/>
DEFAULT	<input type="checkbox"/>	 None	<input type="checkbox"/>
GUEST	<input type="checkbox"/>	 None	<input type="checkbox"/>
WAN2	<input type="checkbox"/>	 None	<input checked="" type="checkbox"/>

Step 10. Click **Save** to save the settings.

To view the current routing table refer to this article, [View the Routing Table on ISA500 Series Integrated Security Appliances.](#)