EIGRP

This section describes how to configure the Firewall Threat Defense to route data, perform authentication, and redistribute routing information using the Enhanced Interior Gateway Routing Protocol (EIGRP).

About EIGRP Routing

Enhanced Interior Gateway Routing Protocol (EIGRP), developed by Cisco, is an enhanced version of IGRP. Unlike IGRP and RIP, EIGRP does not send out periodic route updates. EIGRP updates are sent out only when the network topology changes. Key capabilities that distinguish EIGRP from other routing protocols include fast convergence, support for variable-length subnet mask, support for partial updates, and support for multiple network layer protocols.

A router running EIGRP stores all the neighbor routing tables so that it can quickly adapt to alternate routes. If no appropriate route exists, EIGRP queries its neighbors to discover an alternate route. These queries are propagated until an alternate route is found. EIGRP support for the variable-length subnet masks allows routes to be automatically summarized on a network boundary. Additionally, EIGRP can be configured to summarize any bit boundary at any interface.

EIGRP does not make periodic updates. Instead, it sends partial updates when the metric for a route changes. Propagation of partial updates is automatically bounded such that only those routers that need the information are updated. As a result of these two capabilities, EIGRP consumes significantly less bandwidth than IGRP.

To dynamically learn of other routers on directly attached networks, threat defense uses neighbor discovery. EIGRP routers send out multicast hello packets to announce their presence on the network. When the EIGRP device receives a hello packet from a new neighbor, it sends its topology table to the neighbor with an initialization bit set. When the neighbor receives the topology update with the initialization bit set, the neighbor sends its topology table back to the device.

The hello packets are sent out as multicast messages. No response is expected for a hello message. Statically defined neighbors is an exception to this rule. If you manually configure a neighbor, hello messages, routing updates, and acknowledgments are sent as unicast messages.

Once this neighbor relationship is established, routing updates are not exchanged unless there is a change in the network topology. The neighbor relationship is maintained through the hello packets. Each hello packet

received from a neighbor includes a hold time. Hold time is the time within which threat defense can expect to receive a hello packet from that neighbor. If the device does not receive a hello packet from that neighbor within the hold time advertised by that neighbor, the device considers that neighbor to be unavailable.

EIGRP uses neighbor discovery/recovery, Reliable Transport Protocol (RTP), and Diffusing Update Algorithm (DUAL) for route computations. DUAL saves all routes to a destination in the topology table, and not just the least-cost route. The least-cost route is inserted into the routing table. The other routes remain in the topology table. If the main route fails, another route is chosen from the feasible successors. A successor is a neighboring router that is used for packet forwarding that has a least-cost path to a destination. A feasibility calculation ensures that the path is not part of a routing loop.

If a feasible successor is not found in the topology table, a route recomputation takes place. During route recomputation, DUAL queries the EIGRP neighbors for a route. The query is propagated to successive neighbors. If a feasible successor is not found, an unreachable message is returned.

During route recomputation, DUAL marks the route as active. By default, threat defense waits for three minutes to receive a response from its neighbors. If the device does not receive a response from a neighbor, the route is marked as stuck-in-active. All routes in the topology table that point to the unresponsive neighbor as a feasibility successor are removed.

Requirements and Prerequisites for EIGRP

Model Support

Threat Defense

Firewall Threat Defense Virtual

Supported Domains

Any

User Roles

Admin

Network Admin

Guidelines and Limitations of EIGRP Routing

Firewall Mode Guidelines

Supported on routed firewall mode only.

Device Guidelines

- Only one EIGRP process is allowed per device.
- EIGRP can be configured through management center UI on Firewall Threat Defense 6.6 and higher versions.

Interface Guidelines

- Only routed interfaces with logical names and with an IP address can be associated with an EIGRP routing process.
- Only interfaces belonging to the global virtual router can be part of EIGRP. EIGRP can learn, filter, and redistribute routes across routing protocols in global virtual router.
- Supports physical, EtherChannel, redundant, subinterfaces only. However, the members of EtherChannel interfaces are not supported.
- VTI, BVI, and VNI cannot be part of EIGRP.
- A passive interface cannot be configured as a neighbor interface.

IP Address and Network Objects Support

- Only IPv4 address is supported.
- Range, FQDN, and wildcard mask are not supported.
- Only Standard access list objects are supported.

Redistribution Guidelines

- BGP, OSPF, and RIP in the global virtual router can redistribute to EIGRP.
- EIGRP can redistribute to BGP, OSPF, RIP, Static, and Connected in the global virtual router.
- When EIGRP is configured on a device that is a part of OSPF network or vice versa, ensure that OSPF-router is configured to tag the route (EIGRP does not support route tag).

  When redistributing EIGRP into OSPF and OSPF into EIGRP, a routing loop occurs when there is an outage on one of the links, interfaces, or even when the route originator is down. To prevent the redistribution of routes from one domain back into the same domain, a router can tag a route that belongs to a domain while it is redistributing, and those routes can be filtered on the remote router based on the same tag. Because the routes will not be installed into the routing table, they will not be redistributed back into the same domain.

Deployment Process Guidelines

When you want to change the existing AS number of a deployed EIGRP configuration, you must disable the EIGRP and deploy it. This step will clear the deployed EIGRP configuration on the threat defense. Next, recreate the EIGRP configurations with a new AS number and then deploy it. Thus, this process prevents any deployment failures owing to the same EIGRP configuration being deployed on the threat defense.

Upgrade Guidelines

When you upgrade to version 7.2 and later when the previous version has any FlexConfig EIGRP policies, the management center displays a warning message during deployment. However, it does not stop the deployment process. However, after deployment, to manage the EIGRP policies from the UI (**Device (Edit)** > **Routing** > **EIGRP**), you must redo the configuration in the **Device (Edit)** > **Routing** > **EIGRP** page and remove the configuration from FlexConfig. To ease this manual process, a command-line migration tool is introduced to migrate EIGRP flex configuration to EIGRP routing policies. For more details, see Migrating FlexConfig Policies.

Configure EIGRP

You can enable and configure EIGRP on the firewall device in the **Routing** tab.

Procedure

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

Step 2 Click the **Routing** tab.

Step 3 Under Global, click **EIGRP**.

Step 4 Check the **Enable EIGRP** check box to enable the EIGRP routing process.

Step 5 In the **AS Number** field, enter the autonomous system (AS) number for the EIGRP process. The AS number includes multiple autonomous numbers. The AS number can be from 1 to 65535 and is a uniquely assigned value that identifies each network on the Internet.

Step 6 To configure other EIGRP properties, see the following topics:

a. Configure EIGRP Settings, on page 4.

b. Configure EIGRP Neighbors Settings, on page 5.

c. Configure EIGRP Filter Rules Settings, on page 5.

d. Configure EIGRP Redistribution Settings, on page 6.

e. Configure EIGRP Summary Address Settings, on page 7.

f. Configure EIGRP Interfaces Settings, on page 8.

g. Configure EIGRP Advanced Settings, on page 8.

Configure EIGRP Settings

Procedure

Step 1 On the **EIGRP** page, click the **Setup** tab.

Step 2 Check the **Auto Summary** check box to enable EIGRP to summarize network number boundaries.

Note
Enabling Auto Summary can cause routing problems if you have noncontiguous networks.

Step 3 In the **Available Networks/Hosts** box, click the networks or hosts that should participate in the EIGRP routing process, and then click **Add**. To add a new network object, click **Add** (+). See Network for the procedure for adding networks.

Step 4 To configure passive interfaces, check the **Passive Interface** check box. In EIGRP, a passive interface does not send or receive routing updates.

a) To specify selective interfaces as passive, click the **Selected Interface** radio button. In the **Available Interfaces** box, select the interfaces, and click **Add**.
b) To specify all interfaces as passive, click the **All Interfaces** radio button.

Step 5 Click **Ok** and **Save** the settings.

Configure EIGRP Neighbors Settings

You can define static neighbors for the EIGRP process. When you define an EIGRP neighbor, hello packets are unicast to that neighbor.

Procedure

Step 1 On the **EIGRP** page, click the **Neighbors** tab.
Step 2 Click **Add**.
Step 3 From the **Interface** drop-down, choose the interface through which the neighbor is available.
Step 4 From the **Neighbor** drop-down, choose the IP address of the static neighbor. To add the network object, click **Add** (+). See Network for the procedure for adding network objects.
Step 5 Click **Ok** and **Save** the settings.

Configure EIGRP Filter Rules Settings

You can configure route filtering rules for the EIGRP routing process. Filter rules allow you to control the routes that are accepted or advertised by the EIGRP routing process.

Procedure

Step 1 On the **EIGRP** page, click the **Filter Rules** tab.
Step 2 Click **Add** (+).
Step 3 In the **Add Filter Rules** dialog box, from the **Filter Direction** drop-down, choose the direction for the rule:

- Inbound—The rule filters default route information from incoming EIGRP routing updates.
- Outbound—The rule filters default route information from outgoing EIGRP routing updates.

Step 4 To select the interface to which the filtering rule applies, click the **Interface** radio button, and from the drop-down, select the interface.

Note
You cannot apply EIGRP filtering rules on VTI interfaces.

Step 5 To select the protocol to which the filtering rule applies, click the **Protocol** radio button and from the drop-down, select the protocol—BGP, RIP, Static, Connected, or OSPF. For BGP and OSPF protocols, you can specify the relevant Process ID.

Step 6 From the **Access List** drop-down, choose the access list. The list defines the networks that are to be received and that are to be suppressed in routing updates. To add a new standard access list object, click **Add** (+) and see Configure Standard ACL Objects for the detailed procedure.

Step 7 Click **Ok** and **Save** the settings.

Configure EIGRP Redistribution Settings

You can define the rules for redistributing routes from other routing protocols to the EIGRP routing process.

Procedure

Step 1 On the **EIGRP** page, click the **Redistribution** tab.

Step 2 Click **Add** (+).

Step 3 In the **Add Redistribution** dialog box, from the **Protocol** drop-down, choose the source protocol from which the routes are being redistributed:

- BGP—Redistributes routes discovered by the BGP routing process to EIGRP.
- RIP—Redistributes routes discovered by the RIP routing process to EIGRP.
- Static—Redistributes static routes to the EIGRP routing process. Static routes that fall within the scope of a network statement are automatically redistributed to EIGRP; you do not need to define a redistribution rule for them. However, when redistributing static routes that point to VTI interfaces in EIGRP, you must specify the metric. For static routes pointing to other types of interfaces, specifying the metric is not required.
- Connected—Redistributes connected routes (routes established automatically by virtue of having IP address enabled on the interface) to the EIGRP routing process. Connected routes that fall within the scope of a network statement are automatically redistributed to EIGRP; you do not need to define a redistribution rule for them.
- OSPF—Redistributes routes discovered by the OSPF routing process to EIGRP. If you choose this protocol, the Match options on this dialog box become available under **Optional OSPF Redistribution**:
  - Internal—Routes that are internal to a specific AS.
  - External1—Routes that are external to the AS and imported into OSPF as a Type 1 external route.
  - External2—Routes that are external to the AS and imported into the selected process as a Type 2 external route.
  - Nsaa-External1—Not-So-Stubby Area (NSSA) routes that are external to the AS and imported into the selected process as Type 1 external routes.
  - Nsaa-External2—(NSSA) routes that are external to the AS and imported into the selected process as Type 2 external routes.

Note
These options are not available when redistributing static, connected, RIP, or BGP routes.

Step 4 Under **Optional Metrics** enter the relevant values:

- **Bandwidth**—The minimum bandwidth of the route in kilobits per second. Valid values range from 1 to 4294967295.
- **Delay Time**—The routing delay in tens of microseconds. Valid values range from 0 to 4294967295.
- **Reliability** —The likelihood of successful packet transmission is expressed as a number 0 through 255. The value 255 indicates 100 percent reliability; 0 means no reliability.
- **Loading**— The effective bandwidth of the route. Valid values range from 1 to 255. 255 indicates 100 percent loading.
- **MTU**—The smallest permissible value for the maximum transmission unit of the path. Valid values range from 1 to 65535.

Step 5 From the **Route Map** drop-down, choose the route map object to apply to the redistribution entry. To create a new route map object, click **Add** (+). See Configure Route Map Entry for the procedure to add a new route map.

Step 6 Click **Ok** and **Save** the settings.

Configure EIGRP Summary Address Settings

You can configure summary addresses for each interface. You need to manually define summary addresses if you want to create summary addresses that do not occur at a network boundary, or if you want to use summary addresses on threat defense with automatic route summarization disabled. If more specific routes are available in the routing table, EIGRP advertises the summary address with a metric equal to the minimum of all the more specific routes.

Procedure

Step 1 On the **EIGRP** page, click the **Summary Address** tab.

Step 2 Click **Add**.

Step 3 From the **Interface** drop-down, choose the interface from which the summary address is advertised.

Step 4 From the **Network** drop-down, choose the network object with specific IP address and network mask to be summarized. To add a new network, click **Add** (+). See Network for the procedure for adding networks.

Step 5 In the **Administrative Distance** field, enter the administrative distance of the summary route. Valid values range from 1 to 255.

Step 6 Click **Ok** and **Save** the settings.

Configure EIGRP Interfaces Settings

You can configure interface-specific EIGRP routing properties in the Interfaces tab.

Procedure

Step 1 On the **EIGRP** page, click the **Interfaces** tab.

Step 2 Click **Add** (+).

Step 3 From the **Interface** drop-down, choose the name of the interface to which the configuration applies.

Step 4 In the **Hello Interval** field, enter the interval, in seconds, between EIGRP hello packets that are sent on an interface. Valid values range from 1 to 65535. The default value is 5 seconds.

Step 5 In the **Hold Time** field, enter the hold time that is advertised by the device in EIGRP hello packets. Valid values range from 3 to 65535. The default value is 15 seconds.

Step 6 To enable EIGRP split-horizon on the interface, click the **Split Horizon** check box.

Step 7 In the **Delay Time** field, enter the delay time in tens of microseconds. Valid values are from 1 to 16777215. This option is not supported for devices in multi-context mode.

Step 8 Specify values for the Authentication properties:

- **Enable MD5 Authentication**—Check the check box to use MD5 hash algorithm for authentication of EIGRP packets.
- **Key Type**—From the drop-down, select any one of the following key type:
  - None—To indicate that no authentication is required.
  - Unencrypted—To indicate that the key string to be used is a clear text password for authentication.
  - Encrypted—To indicate that the key string to be used is an encrypted password for authentication.
  - Auth Key—To indicate that the key string to be used is an EIGRP authentication key.
- **Key ID**—The ID of the key that is used to authenticate EIGRP updates. Enter a numerical key identifier. Valid values range from 0 to 255.
- **Key**—An alphanumeric character string of up to 17 characters. For an encrypted authentication type, this field should have a minimum of 17 characters.
- **Confirm Key**—Re-enter the key.

Step 9 Click **Ok** and **Save** the settings.

Configure EIGRP Advanced Settings

You can configure EIGRP advanced settings such as the router ID, stub routing, and adjacency changes.

Procedure

Step 1 On the **EIGRP** page, click the **Advanced** tab.

Step 2 Under **Default Route Information**, you can specify the sending and receiving of default route information in EIGRP updates.

- (Appears for non-cluster and cluster in spanned etherchannel mode)**Router ID (IP Address)**—Enter the ID used to identify the originating router for external routes. If an external route is received with the local router ID, the route is discarded. To prevent this issue, specify a global address for the router ID. An unique value should be configured for each EIGRP router.
- (Appears only for a cluster in individual interface mode)**IPv4 Address Pool**—Select the relevant cluster pool value (IPv4 address pool object). To create the address pool, see Address Pools.
- **Accept Default Route Info**—Check the check box to configure EIGRP to accept exterior default routing information.
  - **Access List**—From the **Access List** drop-down, specify a standard access list that defines the networks that are allowed and the networks that are not when receiving default route information.

    To add a new standard access list object, click **Add** (+) and see Configure Standard ACL Objects for the detailed procedure.
- **Send Default Route Info**—Check the check box to configure EIGRP to advertise exterior default routing information.
  - **Access List**—From the **Access List** drop-down, specify a standard access list that defines the networks that are allowed and the networks that are not when sending default route information.

    To add a new standard access list object, click **Add** (+) and see Configure Standard ACL Objects for the detailed procedure.

Step 3 Under **Administrative Distance**, specify:

- **Internal Distance**—Administrative distance for EIGRP internal routes. Internal routes are those that are learned from another entity within the same autonomous system. Valid values range from 1 to 255. The default value is 90.
- **External Distance**—Administrative distance for EIGRP external routes. External routes are those for which the best path is learned from a neighbor external to the autonomous system. Valid values range from 1 to 255. The default value is 170.

Step 4 Under **Adjacency Changes**, specify:

- **Log Neighbor Changes**—Click the check box to enable the logging of EIGRP neighbor adjacency changes.
- **Log Neighbor Warnings**—Click the check box to enable the logging of EIGRP neighbor warning messages.
- (Optional) Enter the time interval (in seconds) between repeated neighbor warning messages. Valid values range from 1 to 65535. Repeated warnings are not logged if they occur during this interval.

Step 5 Under **Stub**, to enable the device as an EIGRP stub routing process, click one or more of the following EIGRP stub routing processes check boxes:

- **Receive only**—Configures the EIGRP stub routing process to receive route information from the neighbor routers but not send route information to the neighbors. If this option is selected, you cannot select any of the other stub routing options.
- **Connected**—Advertises connected routes.
- **Redistributed**—Advertises redistributed routes.
- **Static**—Advertises static routes.
- **Summary**—Advertises summary routes.

Step 6 Under **Default Metrics**, define the default metrics for routes redistributed to the EIGRP routing process:

- **Bandwidth**—the minimum bandwidth of the route in kilobits per second. Valid values range from 1 to 4294967295.
- **Delay Time**—the route delay in tens of microseconds. Valid values range from 0 to 4294967295.
- **Reliability**—the likelihood of successful packet transmission expressed as a number 0 through 255. The value 255 indicates 100 percent reliability; 0 means no reliability.
- **Loading**—the effective bandwidth of the route. Valid values range from 1 to 255; 255 indicates 100 percent loading.
- **MTU**—the smallest allowed value for the maximum transmission unit of the path. Valid values range from 1 to 65535.

History for EIGRP

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
EIGRP configuration	7.2	Any	In the previous releases, EIGRP was configurable on threat defense only through FlexConfig. FlexConfig no longer supports EIGRP configuration. You can now configure EIGRP settings for threat defense in the management center UI. New/modified screens: **Devices** > **Device Management** > **Routing** > **EIGRP**.