

EIGRP

EIGRP is a routing protocol that

- enables routers to efficiently exchange information,
- maintain network topology tables, and
- ensures secure data path selection and communication across networks.

EIGRP Operational Overview

This section covers the configuration of the Firewall Threat Defense to perform these routing tasks:

- Route data traffic
- Perform authentication
- Redistribute routing information

- EIGRP routing, on page 1
- Requirements and prerequisites for EIGRP, on page 2
- Guidelines and limitations for EIGRP routing, on page 2
- Configure EIGRP routing on firewall devices, on page 4

EIGRP routing

An Enhanced Interior Gateway Routing Protocol (EIGRP) is a routing protocol that

- sends updates only when network topology changes, not at regular intervals,
- offers rapid convergence and supports variable-length subnet masks, and
- supports partial updates and multiple network layer protocols.

EIGRP capabilities and operations

EIGRP stores all neighbor routing tables for quick adaptation to alternate routes. If a suitable route does not exist, EIGRP queries its neighbors to discover an alternate route. It propagates these queries through the network to locate a route. EIGRP's support for 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 sends partial updates when route metrics change, limiting propagation to necessary routers, which minimizes bandwidth use compared to protocols that send periodic full updates.

To learn about routers on attached networks, EIGRP uses neighbor discovery through multicast hello packets to announce their presence on the network. When a new neighbor is detected through hello packets, a topology table exchange occurs.

EIGRP hello packets are normally sent as multicast messages and do not require explicit replies. For manually configured static neighbors, hello packets are sent as unicast messages to the specified neighbor.

Once this neighbor relationship is established, routing updates are exchanged only on topology changes. The relationship persists through regular multicast hello packets, with devices expected to respond within advertised hold times. 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 within the advertised hold time, it considers the neighbor unavailable.

EIGRP employs mechanisms like neighbor discovery/recovery, Reliable Transport Protocol (RTP), and Diffusing Update Algorithm (DUAL) for route computations. DUAL retains all routes to a destination, selecting the least-cost route for packet forwarding while retaining others in case of network changes. 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. DUAL utilizes a feasibility condition to ensure 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 feasible successor are removed.

Requirements and prerequisites for EIGRP

This topic provides the necessary prerequisites and requirements for deploying EIGRP within a Cisco network environment.

Model support

Firewall Threat Defense

Firewall Threat Defense Virtual

Guidelines and limitations for EIGRP routing

Firewall mode guidelines

Use routed firewall mode only for EIGRP routing.

Device guidelines

Configure only one EIGRP process per device.

- EIGRP can be configured through management center UI on Firewall Threat Defense version 6.6 and later.

Interface guidelines

Use only routed interfaces with logical names and IP addresses for EIGRP routing processes.

- EIGRP can only incorporate interfaces from the global virtual router. EIGRP can learn, filter, and redistribute routes across routing protocols in the global virtual router.
- Supports physical, EtherChannel, redundant, and subinterfaces only. However, the members of EtherChannel interfaces are not supported.
-
- Passive interfaces cannot be configured as neighbor interfaces.

IP address and network objects support

Use only IPv4 addresses and standard access list objects for EIGRP configuration.

- Ranges, FQDNs, and wildcard masks are not supported.

Redistribution guidelines

Configure route tagging to prevent routing loops when redistributing between EIGRP and OSPF.

- BGP, OSPF, and RIP in the global virtual router can redistribute routes toward 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 an OSPF network or vice versa, ensure that the 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 can occur 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

Disable and redeploy EIGRP when changing the AS number to prevent deployment failures.

To effectively change the AS number of an existing EIGRP setup, you should disable and redeploy EIGRP configurations to avoid repeated deployments and ensure error-free deployment processes.

Upgrade guidelines

Migrate FlexConfig EIGRP policies to UI management after upgrading to version 7.2 and later.

When you upgrade to version 7.2 and later, and if the previous version includes any FlexConfig EIGRP policies, the management center displays a warning message during deployment. It does not stop the deployment process; a warning message is displayed. After deployment, to manage the EIGRP policies from the UI (**Devices** > **Device Management**, click the **Edit** (✎) icon. Then, click **Routing**>**EIGRP**), you must redo the

configuration in the **EIGRP** page and remove the configuration from FlexConfig. To automate policy creation in the UI, Cloud-Delivered Firewall Management Center provides an option to migrate the policies from FlexConfig to the UI. For more information, refer to Migrate FlexConfig policies.

Configure EIGRP routing on firewall devices

Enable EIGRP on a firewall device for efficient routing within an autonomous system.

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.

Valid values are from 1 to 65535. The AS number identifies the local EIGRP routing domain and must match on EIGRP neighbors.

Step 6 To configure other EIGRP properties, refer to these topics for detailed steps:

a. Configure EIGRP settings, on page 4.

b. Configure EIGRP neighbors settings, on page 5.

c. Configure EIGRP filter rules, on page 6.

d. Configure EIGRP redistribution settings, on page 6.

e. Configure EIGRP summary address settings, on page 8.

f. Configure EIGRP interfaces settings, on page 9.

g. Configure EIGRP advanced settings, on page 10.

The firewall device is now configured with the base EIGRP process and the designated AS number. It can participate in EIGRP routing after the required interfaces, networks, and related settings are configured.

Configure EIGRP settings

Use this procedure when you need to set up EIGRP routing protocol parameters on your device. EIGRP configuration includes enabling automatic network summarization, selecting networks that participate in the routing process, and configuring passive interfaces that do not exchange routing updates.

Procedure

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

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

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

Step 3 In the **Available Networks/Hosts** box, select the networks or hosts that should participate in the EIGRP routing process, and then click **Add**. To add a new network object, click **Add** (+). For detailed instructions on adding networks, refer to 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 **Save**.

The EIGRP settings are configured and saved. The routing protocol will operate according to the specified configuration, including automatic summarization behavior, network participation, and passive interface settings.

Configure EIGRP neighbors settings

Define static neighbors for the EIGRP process. This results in unicast hello packets being sent to that neighbor.

Procedure

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

Step 2 Click +**Add**.

Step 3 Select the interface through which the neighbor is available from the **Interface** drop-down list.

Step 4 Select the IP address of the static neighbor from the **Neighbor** drop-down list.

Step 5 To add a new network object, click +. For instructions on adding network objects, refer to Networks.

Step 6 Click **OK**.

Step 7 Click **Save**.

The EIGRP static neighbor is configured, and hello packets are sent as unicast to the specified neighbor through the designated interface.

Configure EIGRP filter rules

Filter rules provide granular control over EIGRP route advertisements and acceptances, allowing you to manage network traffic flow and routing table contents based on specific criteria such as interface or protocol type.

To configure EIGRP filter rules, perform these steps:

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, select the direction for the rule from the **Filter Direction** drop-down list:

- **Inbound**: The rule filters routes received in incoming EIGRP updates.
- **Outbound**: The rule filters routes advertised in outgoing EIGRP updates.

Step 4 Under **Type**, choose one of these options:

- To select the interface to which the filtering rule applies, click **Interface**, and then select the interface from the **Select Interface** drop-down list. Select the access list from the **Access List** drop-down list. The list defines the networks that are to be received and suppressed in routing updates. To add a new standard access list object, click +. For more information, refer to Configure a standard ACL object. Click **OK**.

Note You cannot apply EIGRP filtering rules on VTI interfaces.

- (This option is enabled only if you choose **Outbound** filter direction.) To select the protocol to which the filtering rule applies, click **Protocol** and then select BGP, RIP, Static, Connected, or OSPF from the **Select Protocol** drop-down list. You can specify the relevant **Process ID** for BGP and OSPF protocols. Select the access list from the **Access List** drop-down list. The list defines the networks that are to be received and suppressed in routing updates. To add a new standard access list object, click +. For more information, refer to Configure a standard ACL object. Click **OK**.

Step 5 Click **Save**.

The EIGRP filter rule is configured and applied to control route filtering based on the specified direction, interface, protocol, and access list criteria.

Configure EIGRP redistribution settings

Define rules to redistribute routes from other routing protocols to the EIGRP routing process to enable route sharing across different routing protocols.

To configure EIGRP redistribution settings, perform these steps:

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 list, select the source protocol from which the routes are being redistributed:

- **BGP**: Redistributes routes discovered by the BGP routing process to EIGRP. Specify the relevant **Process ID**.
- **RIP**: Redistributes routes discovered by the RIP routing process to EIGRP.
- **Static**: Redistributes static routes to the EIGRP routing process. Static routes within a network statement scope automatically redistribute to EIGRP, without additional rules. Specify the metric when redistributing static routes to VTI interfaces in EIGRP. You do not need to specify the metric for static routes pointing to other types of interfaces.
- **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. Specify the relevant **Process ID**. If you select 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.
- **Route Map**: Select the route map object to apply to the redistribution entry from the **Route Map** drop-down list. To create a new route map object, click +. For instructions on adding a new route map, refer to Configure Route Map Entry.

Step 5 Click **OK**.

Step 6 Click **Save**.

The EIGRP redistribution settings have been configured and saved. Routes from the selected source protocol will be redistributed to EIGRP according to the specified rules and metrics.

Configure EIGRP summary address settings

You can configure summary addresses for each interface. If you want to create summary addresses that do not occur at a network boundary, you should manually define them. Alternatively, you can use summary addresses 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 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 list, select the interface from which the summary address is advertised.

Step 4 From the **Network** drop-down list, select the network object with a specific IP address and network mask to be summarized. To add a new network, click +. For detailed instructions for adding networks, refer to 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**.

Step 7 Click **Save**.

The EIGRP summary address settings are configured and saved. EIGRP will advertise the summary address from the specified interface with the configured administrative distance.

Configure EIGRP interfaces settings

Manage interface settings to optimize routing operations.

To configure EIGRP interface settings, perform these steps:

Procedure

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

Step 2 Click **Add**.

Step 3 Select the appropriate interface from the **Interface** drop-down list.

Step 4 In the **Hello Interval** field, enter the hello interval in seconds for EIGRP packets 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 1 to 65535. The default value is 15 seconds.

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

Step 6 In the **Delay Time** field, enter the delay time in tens of microseconds. Valid values are from 1 to 16777215.

Note This option is not supported in multi-context mode devices.

Step 7 Specify authentication properties:

- **Enable MD5 Authentication**: Check the check box to use the MD5 hash algorithm for authentication of EIGRP packets.
- **Key Type**: Select one key type from the drop-down list:
  - **None**: Indicates that no authentication is required.
  - **Unencrypted**: Indicates that the key string is a clear text password for authentication.
  - **Encrypted**: Indicates that the key string is an encrypted password for authentication.
  - **Auth Key**: Indicates that the key string 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 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 8 Click **OK**.

Step 9 Click **Save**.

The EIGRP interface settings that you configured are saved. The interface uses the specified hello interval, hold time, split-horizon setting, delay time, and authentication parameters for EIGRP routing operations.

Configure EIGRP advanced settings

Configure EIGRP advanced settings to optimize routing behavior and performance in your network.

To configure EIGRP advanced settings, perform these steps:

Procedure

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

Step 2 Under **Default Route Information**, 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. Specify a global address for the router ID to prevent this issue. Each EIGRP router requires a unique value.
- (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, refer to Configure address pools.
- **Accept Default Route Info**: Check the check box to configure EIGRP to accept default route information.
  - **Access List**: From the **Access List** drop-down list, 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 +. For more information, refer to Configure a standard ACL object.
- **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 list, 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 +. For more information, refer to Configure a standard ACL object.

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**: Check the check box to enable the logging of EIGRP neighbor adjacency changes.
- **Log Neighbor Warnings**: Check 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 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 from 0 to 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.

EIGRP advanced settings are configured according to your specifications, optimizing routing behavior and performance.