Bidirectional Forwarding Detection Routing

This chapter describes how to configure Firewall Threat Defense to use the Bidirectional Forwarding Detection (BFD) routing protocol.

About BFD Routing

BFD is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. BFD operates in a unicast, point-to-point mode on top of any data protocol being forwarded between two systems. However, in Firewall Threat Defense, BFD is supported on BGP protocols only. Packets are carried in the payload of the encapsulating protocol appropriate for the media and the network.

BFD provides a consistent failure detection method for network administrators in addition to fast forwarding path failure detection. Because the network administrator can use BFD to detect forwarding path failures at a uniform rate, rather than the variable rates for different routing protocol hello mechanisms, network profiling and planning are easier and reconvergence time is consistent and predictable.

Guidelines for BFD Routing

Context Mode Guidelines

BFD is supported on all Firewall Threat Defense platforms. It is supported in multi-instance mode.

Firewall Mode Guidelines

Supported in routed firewall mode and not in transparent mode.

Failover and Cluster Guidelines

- BFD is not supported on failover interfaces.
- In clustering, BFD is supported only on the control node.

Routing and Protocol Guidelines

- OSPFv2, OSPFv3, BGP IPv4, and BGP IPv6 protocol are supported.

Note For optimal routing, do not configure BFD when BGP graceful restart for NSF is configured on the device.

IS-IS and EIGRP protocols are not supported.

- BFD for static routes is not supported. You can configure BFD on interfaces that belong only to virtual routers.
- Only named interfaces are supported.
- BFD on BVI, VTI, and loopback interfaces are not supported.

Single-hop Guidelines

- Echo mode is disabled by default. You can enable echo mode on single-hop only.
- Echo mode is not supported for IPv6.
- Use only a single-hop template to configure a single-hop policy.
- Authentication of the single-hop template is optional.
- You cannot configure multiple BFDs on the same interface.

Multi-hop Guidelines

- Do not configure the source IP address also as the destination IP address.
- Source and destination address should have same IP type—IPV4 or IPV6.
- Only network objects of host or network type are allowed.
- Use only a multi-hop template to configure a multi-hop policy.
- Authentication is mandatory for the multi-hop template.

Upgrade Guidelines

When you upgrade to version 7.3 and when the previous version has any FlexConfig BFD policies, the management center displays a warning message during deployment. However, it does not stop the deployment process. After post-upgrade deployment, to manage the BFD policies from the UI (**Device (Edit)** > **Routing** > **BFD**), you must configure BFD policies in the **Device (Edit)** > **Routing** > **BFD** page and remove the configuration from the FlexConfig policy for the device.

Configure BFD

This section describes how to enable and configure the BFD routing policy on your system.

Procedure

Step 1 Create BFD Template.

Step 2 Configure BFD Policies, on page 3.

Step 3 Configure BFD support in the BGP neighbor settings; see, 12

Configure BFD Policies

You can bind a BFD template to an interface belonging to a virtual router, or to a source and destination address pair.

Before you begin

- BFD policy is configurable only on interfaces that belong to virtual routers. See Configure interfaces to a virtual router.

Procedure

Step 1 From the **Devices** > **Device Management** page, edit the virtual-router supported device. Navigate to **Routing**.

Step 2 From the drop-down list, select the desired virtual router, and then click **BFD**.

Step 3 To configure a BFD on the interface, click the **Single-Hop** tab or **Multi-Hop** tab.

Note
For a single-hop policy, the BFD template is configured on an interface; for a multi-hop policy, the BFD template is configured on a source and destination address pair.

Step 4 Click **Add**. To modify the configured BFD policy, click **Edit** ( ).

Note
When you edit the interface mapping with BFD template to replace it with a new BFD template, the Firewall Management Center uses a **no** command to remove the template mapping from interface and applies the new template to the interface which causes a BFD flap which may also lead to an OSPFv2, OSPFv3, or BGP flap. However, if the BFD intervals are higher, the BFD flap might not occur. Alternatively, to avoid the flapping, you can delete the existing BFD template mapping; deploy the interface, and then add the new BFD template to the interface and deploy the configuration.

- See Configure Single-Hop BFD Policies, on page 4.
- See Configure Multi-Hop BFD Policies, on page 4.

Configure Single-Hop BFD Policies

You can configure a single-hop BFD policy only on an interface that is belonging to a virtual router.

Before you begin

- Create single-hop BFD templates. You cannot configure single-hop BFD policy on interfaces using a multi-hop template.

Procedure

Step 1 In the **Single-Hop** tab, click **Add** or **Edit**.

Step 2 In the **Add BFD Single-Hop** dialog box, configure the following:

a) In the **Interface** drop-down list, interfaces belonging to virtual routers are listed. Select the interface you want to configure with the BFD policy.

b) In the **Template Name** drop-down list, single-hop templates are listed. Select the template that you want to apply.

If you have not created a single-hop template, use **Add** (+) and create a single-hop BFD template.

Step 3 Click **OK** and **Save** the configuration.

Configure Multi-Hop BFD Policies

You can configure multi-hop BFD policy on a source and destination address pair.

Before you begin

- Create multi-hop BFD templates. You cannot configure multi-hop BFD policy using a single-hop template.

Procedure

Step 1 In the **Add BFD Multi-Hop** dialog box, configure the following:

a) Click the BFD source address type—**IPv4** or **IPv6** radio button.

b) In the **Source Address** drop-down list, network objects are listed. Select the source address that you want to configure for the BFD policy. You cannot choose *any-ipv4* or *any-ipv6*.

If you have not created the required network object, use **Add** (+) and create a host/network object.

Note
The created network object's IP type should match with the selected source IP type.

c) In the **Destination Address** drop-down list, network objects are listed. Select the destination address that you want to configure for the BFD. You cannot choose *any-ipv4* or *any-ipv6*.

If you have not created the required network object, use **Add** (+) and create a host/network object.

Note
The created network object's IP type should match with the selected source IP type.

Attention
Do not select the network object that has the same IP address as that of the source address.

d) In the **Template Name** drop-down list, multi-hop templates are listed. Select the template that you want to apply on the BFD policy.

If you have not created a multi-hop template, use **Add** (+) and create a multi-hop BFD template.

Step 2 Click **OK** and **Save** the configuration.

The multi-hop map (table view) is displayed on the **Multi-Hop** tab page.

History for BFD Routing

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
BFD support for OSPF	7.4	7.4	You can enable BFD on OSPFv2 and OSPFv3 interfaces. New/modified screens: • **Configuration** > **Device Setup** > **Routing** > **OSPFv2** • **Configuration** > **Device Setup** > **Routing** > **OSPFv3**
BFD configuration	7.4	7.4	In the previous releases, BFD was configurable on threat defense only through FlexConfig. FlexConfig no longer supports BFD configuration. You can now configure BFD policies for threat defense in the management center UI. In threat defense, BFD is supported only on the BGP protocol. New/modified screens: **Devices** > **Device Management** > **Routing** > **BFD**.