

Configure BFD in Secure Firewall Threat Defense with Flex-Config

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Background Information](#)
[Configure](#)
[Verify](#)
[Troubleshoot](#)

Introduction

This document describes how to configure the BFD Protocol in Secure Firewall Management Center running 7.2 and earlier with Flex-Config.

Prerequisites

Border Gateway Protocol (BGP) configured in Cisco Secure Firewall Threat Defense (FTD) with Cisco Secure Firewall Management Center (FMC).

Requirements

Cisco recommends that you have knowledge of these topics:

- BGP protocol
- BFD concepts

Components Used

-Cisco Secure Firewall Management Center running 7.2 or earlier versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Bidirectional Forwarding Detection (BFD) is a detection protocol designed to provide fast-forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols.

Configure

BFD configurations in FMC running versions 7.2 and earlier must be configured with Flex-Config policies and objects.

Step 1.

Create the BFD template through Flexconfig Object.

The BFD template specifies a set of BFD interval values. BFD interval values configured in the BFD template are not specific to a single interface. You can also configure authentication for single-hop and multi-hop sessions.

To Create the Flex-Config object, select the **Objects Tab** at the top, click the **FlexConfig** option on the left column, then click the **FlexConfig Object** option and then click on **Add FlexConfig Object**.

The screenshot shows the Firepower Management Center interface. The top navigation bar includes tabs for Overview, Analysis, Policies, Devices, Objects (which is highlighted with a red box and has a red number '1' next to it), AMP, and Intelligence. On the left, a sidebar lists various management objects, with 'FlexConfig' expanded, showing 'FlexConfig Object' selected (highlighted with a red box and has a red number '2' next to it). A sub-menu under 'FlexConfig Object' shows options like Text Object, Geolocation, Interface, Key Chain, Network, PKI, Policy List, Port, Prefix List, Route Map, Security Intelligence, Sinkhole, and SLA Monitor. The main content area is titled 'FlexConfig Object' and contains a table with 15 rows of configuration entries. The first row is highlighted with a red box and has a red number '3' next to it. The table columns include 'Name' (e.g., BFD-MULTIHOP, BFD-SINGLEHOP, BFD_Negate, Default_DNS_Configure, etc.) and 'Action' (e.g., Configure, Disable, Enable, Remove, Clear, ClearAll). The last column is labeled 'Descr' and contains short descriptions for each entry.

Name	Action	Descr
BFD-MULTIHOP	Configure	
BFD-SINGLEHOP	Configure	
BFD_Negate	Configure	
Default_DNS_Configure	Configure	
Default_Inspection_Protocol_Disable	Disable	
Default_Inspection_Protocol_Enable	Enable	
DHCPv6_Prefix_Delegation_Configure	Configure	
DHCPv6_Prefix_Delegation_UnConfigure	Remove	
DNS_Configure	Configure	
DNS_UnConfigure	Remove	
Eigrp_Configure	Configure	
Eigrp_Interface_Configure	Configure	
Eigrp_UnConfigure	Clears	
Eigrp_Unconfigure_All	Clears	

Step 2.

Add the parameters needed for the BFD Protocol:

The BFD template specifies a set of BFD interval values. BFD interval values configured in the BFD template are not specific to a single interface. You can also configure authentication for single-hop and multi-hop sessions.

```
bfd-template [single-hop | multi-hop] template_name
```

- single-hop - Specifies a single-hop BFD template.

- multi-hopâ€” Specifies a multi-hop BFD template.
- template_name â€” Specifies the template name. The template name cannot contain spaces.
- (Optional) Configure Echo on a single-hop BFD template.

Note: You can only enable Echo mode on a single-hop template.

Configure the intervals in the BFD template:

```
interval both milliseconds | microseconds {both | min-tx} microseconds | min-tx milliseconds echo
```

- bothâ€”Minimum transmit and receive interval capability.
- The interval in milliseconds. The range is 50 to 999.
- microsecondsâ€”Specifies the BFD interval in microseconds for both and min-tx.
- microseconds â€”The range is 50,000 to 999,000.
- min-txâ€”The minimum transmit interval capability.

Configure authentication in the BFD template:

```
authentication {md5 | meticulous-md5 | meticulous-sha-1 | sha-1}[0|8] wordkey-id id
```

- authenticationâ€” Specifies the authentication type.
- md5â€” Message Digest 5 (MD5) authentication.
- meticulous-md5â€” Meticulous keyed MD5 authentication.
- meticulous-sha-1â€” Meticulous keyed SHA-1 authentication.
- sha-1â€” Keyed SHA-1 authentication.
- 0|8â€”0 specifies that an UNENCRYPTED password follows. 8 specifies that an ENCRYPTED password follows.
- wordâ€”The BFD password (key), which is a single-digit password/key of up to 29 characters. Passwords starting with a digit followed by a whitespace are not supported, for example, 0 pass and 1 are not valid.
- key-idâ€”The authentication Key ID.
- idâ€”The shared key ID that matches the key string. The range is 0 to 255 characters.

Edit FlexConfig Object

Name:

BFD-SINGLEHOP

Description:

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert ▾



Deployment:

Once



Type:

Append

```
bfd-template single-hop TEMPLATE1
echo
interval both 50
authentication sha-1 0 cisco key-id 10
```

▼ Variables

Name	Dimension	Default Value	Property (Type:Name)	Override
No records to display				

Step 3.

Associate the BFD Template with the interface.

Edit FlexConfig Object

Name:

BFD-SINGLEHOP

Description:

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert ▾



Deployment:

Once



Type:

Append

```
bfd-template single-hop TEMPLATE1
echo
interval both 50
authentication sha-1 0 cisco key-id 10

interface Ethernet1/7
    bfd template TEMPLATE1
```

▼ Variables

Name	Dimension	Default Value	Property (Type:Name)	Override
No records to display				

Note: Associate the BFD multi-hop template with a map of destinations.

Step 4 (Optional).

Create a BFD map containing destinations that you can associate with a multi-hop template. You must have a multi-hop BFD template already configured.

Associate the BFD multi-hop template with a map of destinations:

```
bfd map {ipv4 | ipv6} destination/cdir source/cdire template-name
```

- **ipv4**” Configures an IPv4 address.
- **ipv6**” Configures an IPv6 address.
- **destination/cdir** ” Specifies the destination prefix/length. The format is A.B.C.D/<0-32>.
- **source/cdir**” Specifies the destination prefix/length. The format is X:X:X;X::X/<0-128>.
- **template-name** ” Specifies the name of the multi-hop template associated with this BFD map.

Click the **Save** button to save the object.

Edit FlexConfig Object

Name:

BFD-MULTIHOP

Description:

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert ▾



Deployment:

Once



Type:

Append

```
bfd-template multi-hop MULTI-TEMPLATE1
interval both 50

bfd map ipv4 10.11.11.0/24 10.36.42.5/32 MULTI-TEMPLATE1
```

▼ Variables

Name	Dimension	Default Value	Property (Type:Name)	Override
No records to display				

Step 5.

Click the Devices tab at the top, and select the FlexConfig option.

Firepower Management Center Overview Analysis Policies Devices **1** Objects AMP Intelligence

> AAA Server
> Access List
> Address Pools
Application Filters
AS Path
Cipher Suite List
> Community List
> Distinguished Name
DNS Server Group
> External Attributes
File List
FlexConfig
FlexConfig Object
Text Object
Geolocation
Interface
Key Chain
Network
> PKI
Policy List
Port
> Prefix List
Route Map
> Security Intelligence
Sinkhole
SLA Monitor

FlexConfig Object

FlexConfig Object include device configuration commands, such as BFD, DNS, DHCPv6, EIGRP, and NAT.

Name	Action
BFD-MULTIHOP	Configure
BFD-SINGLEHOP	Configure
BFD_Negate	Remove
Default_DNS_Configure	Configure
Default_Inspection_Protocol_Disable	Disable
Default_Inspection_Protocol_Enable	Enable
DHCPv6_Prefix_Delegation_Configure	Configure
DHCPv6_Prefix_Delegation_UnConfigure	Remove
DNS_Configure	Configure
DNS_UnConfigure	Remove
Eigrp_Configure	Configure
Eigrp_Interface_Configure	Configure
Eigrp_UnConfigure	Clears
Eigrp_Unconfigure_All	Clears

Step 6.

To create a new FlexConfig Policy, click the New Policy button.

Firepower Management Center Overview Analysis Policies Devices Objects AMP Intelligence

Devices / FlexConfig

Step 7.

Name the policy and select the devices assigned to the policy. Click the Add to Policy then click the Savebutton.

New Policy

Name:

BFD

1

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

Search by name or value

SF3130-A

SF3130-B

2

Add to Policy

Selected Devices

SF3130-A

3 SF3130-B

Step 8.

Select the FlexConfig Object on the left column and click the > button to add the object to the FlexConfig Policy, and click the Save button.

BFD

Enter Description

The screenshot shows the 'Selected Prepend FlexConfigs' section with one item listed:

#	Name	Description
1	BFD-MULTIHOP	

The 'Available FlexConfig' sidebar on the left has the 'FlexConfig Object' tab selected. Under 'User Defined', the 'BFD-MULTIHOP' item is highlighted with a red box labeled '1'. A red box labeled '2' highlights the 'Selected Prepend FlexConfigs' table header.

Step 9.

Click the **Devices** tab at the top and click the **Device Management** option.

The screenshot shows the Firepower Management Center interface. The top navigation bar includes tabs for Overview, Analysis, Policies, Devices (highlighted in red), Objects, AMP, and Intelligence. Below the navigation is a sidebar titled 'BFD' with sections for 'Available FlexConfig' and 'FlexConfig Object'. Under 'Available FlexConfig', 'User Defined' and 'System Defined' sections are listed, with 'BFD-MULTIHOP' selected. To the right, two tables are displayed: 'Selected Prepend FlexConfigs' and 'Selected Append FlexConfigs', both showing 'BFD-MULTIHOP'.

Step 10.

Select the device where the BFD configuration is going to be assigned.

The screenshot shows the Firepower Management Center interface with the 'Devices' tab selected. The main area displays a list of devices. One device, 'SF3130-A' (Snort 3, 10.88.146.203 - Routed), is selected and highlighted with a red border. Other devices listed include 'SF3130-B' (Snort 3, 10.88.146.204 - Routed).

Step 11.

Click the Routing tab, then click the IPv4 or IPv6, depending on your configuration in the BGP section on the left column, then click the Neighbor tab, and click the edit pencil button to edit it.

SF3130-A

Cisco Secure Firewall 3130 Threat Defense

Device Routing **1** Interfaces Inline Sets DHCP

Manage Virtual Routers

Global **2**

Virtual Router Properties

ECMP

OSPF

OSPFv3

RIP

Policy Based Routing

✓ BGP

IPv4 **3**

IPv6

Static Route

✓ Multicast Routing

IGMP

PIM

Multicast Routes

Multicast Boundary Filter

Enable IPv4:

AS Number: 65000

General Neighbor **3** Add Aggregate Address Filtering Networks Redistribution Route Injection

Address	Remote AS Number	Address Family	Remote Private AS Number
172.16.10.2	65001	Enabled	

Step 12.

Select the checkbox for BFD fallover and click the **OK** button.

Edit Neighbor

IP Address*
172.16.10.2

Remote AS*
65001
(1-4294967295 or 1.0-65535.65535)

Description

Filtering Routes Routes Timers Advanced Migration

Enabled address

Shutdown administratively

Configure graceful restart

Graceful restart(failover/spanned mode)

BFD Fallover i

Configuring BFD support for BGP for multi-hop, ensure that the BFD map is already created for the source destination pair through flex-config.

Incoming	Outgoing
Access List	Access List
Route Map	Route Map
Prefix List	Prefix List
AS path filter	AS path filter

Limit the number of prefixes allowed from the neighbor

Maximum Prefixes*
(1-2147483647)

Step 13.

Click the Deploy button, then click the Deployment button.

Firepower Management Center
Devices / Device Management

Overview Analysis Policies **Devices** Objects AMP Intelligence

View By: Group

All (2) Error (2) Warning (0) Offline (0) Normal (0) Deployment Pending (2) Upgrade (0) Snort 3 (2)

Step 14.

Select the device where the changes are going to be assigned by clicking the **checkbox**, and then click the **Deploy** button.

The screenshot shows the Firepower Management Center interface. At the top, there's a navigation bar with tabs for Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. Below the navigation bar is a search bar labeled "Search using device name, user name, type, group or status". Underneath the search bar is a table with two rows of data. The first row has a checkbox column, a "Device" column with "SF3130-B" and a count of "1", and columns for "Modified by" (admin), "Inspect Interruption" (disabled), "Type" (FTD), "Group" (empty), and "Last Deploy Time" (Jul 18, 2023 4:55 PM). The second row has a checkbox column, a "Device" column with "SF3130-A", and similar columns. A red box highlights the checkbox in the first row.

Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time
SF3130-B 1	admin	disabled	FTD		Jul 18, 2023 4:55 PM
SF3130-A	admin	disabled	FTD		Jul 18, 2023 4:55 PM

Step 15.

Click the **Deploy** button.

The screenshot shows a "Deployment Confirmation" page. It starts with the message "You have selected 1 device to deploy". Below that is a section titled "Deployment Notes:" containing the placeholder text "You can optionally add notes about the configuration changes...". At the bottom right, there is a large blue button with the text "Can't wait! Deploy now!".

Step 16.

Click the **Deploy** button.

Validation Messages: SF3130-B

1 total

0 errors

1 warning

0 info

PG.TEMPLATE.TemplatePolicy: BFD

- › | Warning: FlexConfig policies intentionally do not contain extensive input validation. Please ensure that the configurations are valid.

Note: The warning is expected and it is just informational.

Verify

Verify the BFD configuration and the status directly on the CLI session with the next commands.

```
<#root>
>
system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
SF3130-A>
```

```
enable
```

```
Password:  
SF3130-A#
```

```
show running-config | inc bfd  
  
bfd-template single-hop Template  
  bfd template Template  
    neighbor 172.16.10.2 fall-over bfd single-hop
```

```
SF3130-A#
```

```
show bfd summary
```

	Session	Up	Down
Total	1	1	0

```
SF3130-A#
```

```
show bfd neighbors
```

IPv4 Sessions	NeighAddr	LD/RD	RH/RS	State	Int
	172.16.10.2	1/1	Up		

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.