# **Configuración de BFD en Secure Firewall Threat Defence con Flex-Config**

### Contenido

Introducción Prerequisites Requirements Componentes Utilizados Antecedentes Configurar Verificación Troubleshoot

# Introducción

Este documento describe cómo configurar el protocolo BFD en Secure Firewall Management Center que ejecuta 7.2 y versiones anteriores con Flex-Config.

## Prerequisites

Protocolo de gateway fronterizo (BGP) configurado en Cisco Secure Firewall Threat Defense (FTD) con Cisco Secure Firewall Management Center (FMC).

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

-Protocolo BGP -Conceptos BFD

### **Componentes Utilizados**

-Cisco Secure Firewall Management Center con versión 7.2 o anterior.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

### Antecedentes

La detección de reenvío bidireccional (BFD) es un protocolo de detección diseñado para proporcionar tiempos de detección de fallos de ruta de reenvío rápido para todos los tipos de medios, encapsulaciones, topologías y protocolos de routing.

# Configurar

Las configuraciones BFD en FMC que ejecutan versiones 7.2 y anteriores deben configurarse con objetos y políticas Flex-Config.

Paso 1.

Cree la plantilla BFD mediante el objeto Flexconfig.

La plantilla BFD especifica un conjunto de valores de intervalo BFD. Los valores del intervalo BFD configurados en la plantilla BFD no son específicos de una única interfaz. También puede configurar la autenticación para las sesiones de un solo salto y multisalto.

Para crear el objeto Flex-Config, seleccione la opción Objects Tab en la parte superior, haga clic en el botón FlexConfig en la columna izquierda y, a continuación, haga clic en el botón FlexConfig Object y, a continuación, en Add FlexConfig Object.

-ilialia cisco	Firepower Manage Objects / Object Manager	ement Center Overview Analysis Policies Devices Objects 1 AMP Intelligence	
> AAA S > Acces > Addre Applie	Server is List ss Pools iation Filters	FlexConfig Object include device configuration commands, variables, and scripting language instructions. It is used in FlexConfig polices.	4 🗖
AS Pa Ciphe	th r Suite List	Name BFD-MULTIHOP	Descr
> Comn > Distin	uunity List guished Name Server Group	BFD-SINGLEHOP	
> Extern	al Attributes st	BrD_Negate Default_DNS_Configure	Configu
Y FlexC Fl	onfig 2 exConfig Object 3	Default_Inspection_Protocol_Disable Default_Inspection_Protocol_Enable	Disable
Ti Geolo	ext Object cation	DHCPv6_Prefix_Delegation_Configure	Configu
Interfa Key C	ice hain	DHCPv6_Prefix_Delegation_UnConfigure DNS_Configure	Configu
> PKI Policy	urk List	DNS_UnConfigure	Remov
Port > Prefix	List	Eigrp_Interface_Configure	Configu
Route	Map ity Intelligence	Eigrp_UnConfigure Eigrp_Unconfigure_All	Clears
Sinkh SLA N	ble fonitor		

#### Paso 2.

Agregue los parámetros necesarios para el protocolo BFD:

La plantilla BFD especifica un conjunto de valores de intervalo BFD. Los valores del intervalo BFD configurados en la plantilla BFD no son específicos de una única interfaz. También puede configurar la autenticación para las sesiones de un solo salto y multisalto.

- single-hop Especifica una plantilla BFD de un solo salto.
- multi-hop: especifica una plantilla BFD de salto múltiple.
- template\_name: especifica el nombre de la plantilla. El nombre de la plantilla no puede contener espacios.
- (Opcional) Configure Echo en una plantilla BFD de un solo salto.

Nota: Sólo puede activar el modo Eco en una plantilla de un solo salto.

Configure los intervalos en la plantilla BFD:

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

- both: capacidad de intervalo mínimo de transmisión y recepción.
- El intervalo en milisegundos. El rango es 50 a 999.
- microseconds: especifica el intervalo BFD en microsegundos para bothandmin-tx.
- microsegundos: el intervalo es de 50 000 a 999 000.
- min-tx: la capacidad del intervalo de transmisión mínimo.

Configure la autenticación en la plantilla BFD:

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

- authentication: especifica el tipo de autenticación.
- md5: autenticación Message Digest 5 (MD5).
- meticulous-md5: meticulosa autenticación MD5 con clave.
- meticulous-sha-1: meticulosa autenticación de claves SHA-1.
- sha-1: autenticación de claves SHA-1.
- 0|8â€"0 especifica que le sigue una contraseña NO CIFRADA. 8 especifica que a continuación aparece una contraseña CIFRADA.
- palabra: la contraseña (clave) de BFD, que es una contraseña/clave de un solo dígito de hasta 29 caracteres. Las contraseñas que comienzan con un dígito seguido de un espacio en blanco no son compatibles; por ejemplo, 0 pass y 1 no son válidas.
- key-id: el ID de clave de autenticación.
- id: la ID de clave compartida que coincide con la cadena de clave. El intervalo es de 0 a 255

caracteres.

Name: BFD-SINGLEHOP Description: Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deplet and the 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	Edit FlexConfig Object				
Description: Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before depling the 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	Name: BFD-SINGLEHOP				
Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before depl  Insert Deployment: Once Type: Append  Did_template single-hop TEMPLATE1 echo authentication sha-1 0 cisco key-id 10  Variables  Variables  Dimension Default Value Property (Type:Name) Override  No records to display	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         Image: Second state       ● Variables       ● Property       Override         Name       ● Dimension       Default Value       Property       Override         No records to display       ● No records to display       ● No records to display       ● No records to display					
Insert •       E       Deployment:       Once       •       Type:       Append         bfd-template single-hop TEMPLATE1       echo       interval both 50       authentication sha-1 0 cisco key-id 10       Image: Single-hop TEMPLATE1       Image: Single-ho	Copy-pasting any rich text might interview of the second secon	troduce line break	s while generating CLI.	Please verify the	CLI before dep
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	Insert 🔻 🔣 Deployment	: Once		• Туре:	Append
Variables       Dimension       Default Value       Property (Type:Name)       Override         No records to display       No records to display	bfd-template single-hop TEMPLATE1 echo interval both 50 authentication sha-1 0 cisco key	-id 10			
No records to display	▼ Variables	Dimension	Default Value	Property	Override
No records to display		Dimension		(Type:Name)	Overnide
			No records to di	splay	

Paso 3.

Asocie la plantilla BFD a la interfaz.

Edit FlexConfig Object				
Name: BFD-SINGLEHOP				
Description:				
Copy-pasting any rich text might int	troduce line break	s while generating CLI.	Please verify the	CLI before depl
Insert 🔻 🔣 Deployment	Once		▼ Туре:	Append
bfd-template single-hop TEMPLATE1 echo interval both 50 authentication sha-1 0 cisco key interface Ethernet1/7 bfd template TEMPLATE1	-id 10			
▼ Variables	Dimension	Default Value	Property	Override
	Dimension	No records to di	(Type:Name)	Overnue
			spiay	

Nota: Asocie la plantilla multisalto BFD con un mapa de destinos.

Paso 4 (opcional).

Cree un mapa BFD que contenga destinos que pueda asociar a una plantilla de salto múltiple. Debe tener una plantilla BFD de salto múltiple ya configurada.

Asocie la plantilla multisalto BFD con un mapa de destinos:

- ipv4: configura una dirección IPv4.
- ipv6: configura una dirección IPv6.
- destination/cdir: especifica el prefijo/longitud de destino. El formato es A.B.C.D/<0-32>.
- source/cdir: especifica el prefijo/longitud de destino. El formato es X:X:X;X::X/<0-128>.
- template-name: especifica el nombre de la plantilla de salto múltiple asociada a este mapa BFD.

Haga clic en el Save para guardar el objeto.

Edit FlexConfig Object				
Name: BFD-MULTIHOP Description:	roduce line break	s while generating CLI.	Please verify the	CLI before deple
Insert 🔻 🔛 Deployment:	Once		• Туре:	Append
bfd-template multi-hop MULTI-TEMP interval both 50 bfd map ipv4 10.11.11.0/24 10.36.	LATE1 42.5/32 MULTI-T	'EMPLATE1		
▼ Variables			Property	
Name	Dimension	Default Value	(Type:Name)	Override
		No records to dis	splay	

Paso 5.

Haga clic en el Devices en la parte superior y seleccione la ficha FlexConfig opción.

ahah cisco	Firepower Manag Objects / Object Manage	ement Center Overview Analysis Policies	Devices Objects AMP	Intelligence	
<ul> <li>&gt; AAA</li> <li>&gt; Acce</li> <li>&gt; Address</li> <li>&gt; Address</li> <li>Appli</li> <li>AS Participate</li> <li>&gt; Ciphe</li> <li>&gt; Comm</li> </ul>	Server ss List ess Pools cation Filters ath er Suite List munity List	FlexConfig Object FlexConfig Object include device configuration commands, Name BFD-MULTIHOP	Device Management Device Upgrade NAT QoS Platform Settings FlexConfig 2 Certificates	VPN Site To Site Remote Access Dynamic Access Policy Troubleshooting Site to Site Monitoring	Troubleshoot File Download Threat Defense CLI Packet Tracer Packet Capture
> Distin DNS > Exten File L	guished Name Server Group nal Attributes ist	BFD_SINGLEHOP BFD_Negate Default_DNS_Configure			Config
✓ FlexC F T	config lexConfig Object ext Object	Default_Inspection_Protocol_Disable Default_Inspection_Protocol_Enable			Disable
Geok	ace	DHCPv6_Prefix_Delegation_Configure DHCPv6_Prefix_Delegation_UnConfigure			Config Remov
Netw > PKI	ihain ork	DNS_Configure DNS_UnConfigure			Config Remov
Policy Port	/ List	Eigrp_Configure Eigrp_Interface_Configure			Config
Route	Map rity Intelligence	Elgrp_UnConfigure Elgrp_Unconfigure_All			Clears
Sinkh	Manitar				

#### Paso 6.

Para crear una nueva política FlexConfig, haga clic en el botón New Policy botón.

altalta cisco	Firepower Management Center Devices / FlexConfig	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence

#### Paso 7.

Name seleccione la política y los dispositivos asignados a la política. Haga clic en el Add to Policy a continuación, haga clic en Savebotón.

New Policy		
Name: BFD	] 1	
Description:		
Targeted Devices Select devices to which you want to Available Devices	apply this policy.	Selected Devices
Q Search by name or value		SF3130-A
SF3130-A SF3130-в 2	Add to Policy	<mark>З</mark> SF3130-В

Paso 8.

Seleccione el objeto FlexConfig en la columna de la izquierda y haga clic en el botón > para agregar el objeto a la directiva FlexConfig y haga clic en el botón Save botón.

Firepower Management Center Devices / Flexconfig Policy Editor	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	
BFD Enter Description								
Available FlexConfig C FlexConfig Object	Selected	Prepend Fle	exConfigs	De	scription			
Vuser Defined	2							
DHCPv6_Prefix_Delegation_Configure DHCPv6_Prefix_Delegation_UnConfigure DNS_Configure DNS_LinConfigure	J Selected	Append Fle:	xConfigs	De	scription			
Eigrp_Configure     Eigrp_Interface_Configure     Eigrp_UnConfigure     Eigrp_UnConfigure     Eigrp_Unconfigure_All     Inspect_IPv6_Configure     Inspect_IPv6_UnConfigure								

### Paso 9.

Haga clic en el Devices en la parte superior y haga clic en el botón Device Management opción.

Firepower Management Center Devices / Flexconfig Policy Editor	Overview Analysis Policies	Devices 1 Objects AMP	Intelligence	
BFD		Device Management	VPN	Troubleshoot
Enter Description		Device Upgrade	Site To Site	File Download
		NAT	Remote Access	Threat Defense CLI
	Selected Prepend FlexConfigs	QoS	Dynamic Access Policy	Packet Tracer
Available FlexConfig C FlexConfig Object	# Name	Platform Settings	Troubleshooting	Packet Capture
×		Certificates	Site to Site Monitoring	
V User Defined				
BFD-MULTIHOP				
BFD-SINGLEHOP				
BFD_Negate				
✓ System Defined				
" Default_DNS_Configure				
Default_Inspection_Protocol_Disable				
" Default_Inspection_Protocol_Enable				
" DHCPv6_Prefix_Delegation_Configure	Selected Append FlexConfigs			
DHCPv6_Prefix_Delegation_UnConfigure	# Name	Description		
" DNS_Configure	1 BFD-MULTIHOP			
.9 DNS_UnConfigure				
ាំ Eigrp_Configure				
"i Eigrp_Interface_Configure				
-9 Eigrp_UnConfigure				
Eigrp_Unconfigure_All				
1 Inspect_IPv6_Configure				
Inspect_IPv6_UnConfigure				

#### Paso 10.

Seleccione el dispositivo al que se va a asignar la configuración BFD.

altalta cisco	Firepower Management C Devices / Device Management	Center <sub>Overview</sub>	Analysis	Policies	Devices	Objects /	AMP Intelligence	
View B	y: Group 2) • Error (2) • Warning (0)	▼ ● Offline (0)	Normal (0)	Deploymen	t Pending (2)	• Upgrade (0	) 🔹 Snort 3 (2)	
Collapse	<u>All</u>							
	Name			Model		Version	Chassis	Licenses
	<ul> <li>Ungrouped (2)</li> </ul>							
	SF3130-A Snort 3 10.88.146.203 - Routed		F	Firewall 3130 Thre	eat Defense	7.1.0	Manage	Base, Threat (2 mor
	SF3130-B Snort 3 10.88.146.205 - Routed		F	Firewall 3130 Thre	eat Defense	7.1.0	Manage	Base, Threat (2 mor

Paso 11.

Haga clic en el Routing y, a continuación, haga clic en el botón**IPv4** or **IPv6**, en función de su configuración en la sección BGP de la columna izquierda, haga clic en el botón **Neighbor** y haga clic en el botón editar lápiz para editarlo.

Firepower Manager Devices / NGFW Routing	ment Center	Overview	Analysis	Policies	Devices	Objects	АМР	Intelligence	
SF3130-A Cisco Secure Firewall 3130 Threat Device Routing 1 Interface	Defense es Inline Sets	DHCP							
Manage Virtual Routers Global Virtual Router Properties	Enable IPv4: 🗹 AS Number 650 General Ne	00 Highbor 3 Add	d Aggregate /	Address	Filtering N	etworks F	Redistribution	Route Injection	
ECMP OSRE									
OSPFv3	Address		Re	mote AS Num	iber	Ad	dress Family		Remote Private AS Number
RIP	172.16.10.2		65	001		Ene	abled		
Policy Based Routing									
Y BGP									
IPv4 2									
IPv6									
Static Route									
<ul> <li>Multicast Routing</li> </ul>									
DIM									
Multicast Routes									
Multicast Boundary Filter									

#### Paso 12.

Seleccione el checkbox para BFD fallover y haga clic en el botón OK botón.

### Edit Neighbor

IP Address*		<b>V</b>	Enabled addre	SS					
172.16.10.2			Shutdown adm	Shutdown administratively					
Remote AS*			Configure grad	ceful restart					
65001			Graceful restar	rt(failover/spanned mode)					
(1-4294967295 or 1.0-6	5535.65535)		BED Fallover						
Description				Configuring BFD support for BGP for multi-hop, ensure that the BFD map is already created for the source destination pair through flex-config.					
Filtering Routes	Routes	Timers	Advanced	Migration					
Incoming			Outgoing						
Access List			Access List						
		• +		• +					
Route Map			Route Map						
		• +		• +					
Prefix List			Prefix List						
		• +		• +					
AS path filter			AS path filter						
		• +		• +					
Limit the number Maximum Prefixes* (1-2147483647)	of prefixes a	llowed from	m the neighbor						

Paso 13.

Haga clic en el Deploy y haga clic en el botón Deployment botón.

cisco Devi	epower Management ( ices / Device Management	Center o	Verview Analy:	sis Policies	Devices	Objects	AMP	Intelligence	
View By:	Group	•							
All (2)	Error (2) Ø Warning (0)	• Offline (	0) • Normal (0)	Deploymer	nt Pending (2)	Upgrade	(0) 🔹	Snort 3 (2)	

Seleccione el dispositivo al que se van a asignar los cambios haciendo clic en el botón checkboxy, a continuación, haga clic en elDeploy botón.

ciso ciso	()); CO	Firepower Management Center Deploy / Deployment	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	
	Q Search using device name, user name, type, group or status									
		Device		Modified by		Inspect I	Interruption	Туре	Group	Last Deploy Time
>		SF3130-B		admin				FTD		Jul 18, 2023 4:55 P
>		SF3130-A		admin				FTD		Jul 18, 2023 4:55 P

Paso 15.

Haga clic en el Deploy botón.



Paso 16.

Haga clic en el Deploy botón.



Nota: se espera la advertencia y es sólo informativa.

### Verificación

Verifique la configuración BFD y el estado directamente en la sesión CLI con los siguientes comandos.

<#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.

#### enable

Password: SF3130-A#						
show running-co	nfig   inc bfd					
bfd-template si bfd template T neighbor 172.	ngle-hop Template emplate 16.10.2 fall-over	bfd single	-hop			
SF3130-A#						
show bfd summar	У					
Total	Session 1	Up 1	Down 0			
SF3130-A#						
show bfd neighb	ors					
IPv4 Sessions NeighAddr 172.16.10.2			LD/RD 1/1	RH/RS Up	State	Int

### Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

#### Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).