# Konfigurieren von BFD in Secure Firewall Threat Defense mit Flex-Config

### Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konfigurieren Überprüfung Fehlerbehebung

### Einleitung

In diesem Dokument wird die Konfiguration des BFD-Protokolls in Secure Firewall Management Center mit Version 7.2 und früheren Versionen mit Flex-Config beschrieben.

### Voraussetzungen

Border Gateway Protocol (BGP) wird in Cisco Secure Firewall Threat Defense (FTD) mit Cisco Secure Firewall Management Center (FMC) konfiguriert.

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

-BGP-Protokoll - BFD-Konzepte

### Verwendete Komponenten

- Cisco Secure Firewall Management Center mit Version 7.2 oder früheren Versionen

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

### Hintergrundinformationen

BFD (Bidirectional Forwarding Detection) ist ein Erkennungsprotokoll, das entwickelt wurde, um eine schnelle Erkennung von Pfadausfällen für alle Medientypen, Kapselungen, Topologien und Routing-Protokolle zu ermöglichen.

## Konfigurieren

BFD-Konfigurationen in FMC mit Version 7.2 und früheren Versionen müssen mit Flex-Config-Richtlinien und -Objekten konfiguriert werden.

Schritt 1:

Erstellen Sie die BFD-Vorlage über Flexconfig-Objekt.

Die BFD-Vorlage legt eine Reihe von BFD-Intervallwerten fest. Die in der BFD-Vorlage konfigurierten BFD-Intervallwerte sind nicht spezifisch für eine einzelne Schnittstelle. Sie können auch die Authentifizierung für Single-Hop- und Multi-Hop-Sitzungen konfigurieren.

Um das Flex-Config-Objekt zu erstellen, wählen Sie Objects Tab Klicken Sie oben auf das FlexConfig in der linken Spalte ein, und klicken Sie dann auf FlexConfig Object und klicke anschließend auf Add FlexConfig Object.

Cisco Firepow Objects / Objects / Ob	er Manageme	ent Center	Overview	Analysis	Policies	Devices	Objects	1 амр	Intelligence		
<ul> <li>AAA Server</li> <li>Access List</li> <li>Address Pools</li> <li>Application Filters</li> </ul>		FlexConfig FlexConfig Object	g Object	e configuratio	on commands,	variables, and	l scripting lang	guage instru	ctions. It is used i	n FlexConfig polices	4 🗖
AS Path		Name									Descr
Cipher Suite List		BFD-MULTIHOP									
<ul> <li>Distinguished Name</li> </ul>	. //	BFD-SINGLEHO	P								
DNS Server Group		BFD_Negate									
External Attributes File List		Default_DNS_Co	onfigure								Configu
✓ FlexConfig 2		Default_Inspecti	on_Protocol_Dis	able							Disable
FlexConfig Obje	ect 3	Default_Inspecti	on_Protocol_En	able							Enable
Text Object Geolocation		DHCPv6_Prefix_	Delegation_Con	figure							Configu
Interface		DHCPv6_Prefix_	Delegation_Un0	onfigure							Remov
Key Chain		DNS_Configure									Configu
		DNS_UnConfigu	re								Remov
Policy List		Eigrp_Configure									Configu
Port		Eigrp_Interface_	Configure								Configu
> Prefix List		Eigro UnConfig	ure.								Clears
Security Intelligence		Eine Hansford									010010
Sinkhole		Eigrp_Unconfigu	ire_All								Clears
SLA Monitor											

#### Schritt 2:

Fügen Sie die für das BFD-Protokoll erforderlichen Parameter hinzu:

Die BFD-Vorlage legt eine Reihe von BFD-Intervallwerten fest. Die in der BFD-Vorlage konfigurierten BFD-Intervallwerte sind nicht spezifisch für eine einzelne Schnittstelle. Sie können auch die Authentifizierung für Single-Hop- und Multi-Hop-Sitzungen konfigurieren.

bfd-template [single-hop | multi-hop] template\_name

- single-hop Gibt eine single-hop BFD-Vorlage an.
- multi-hop Gibt eine Multi-Hop-BFD-Vorlage an.
- template\_name Gibt den Vorlagennamen an. Der Vorlagenname darf keine Leerzeichen enthalten.
- (Optional) Konfigurieren Sie Echo auf einer Single-Hop-BFD-Vorlage.

Hinweis: Sie können den Echo-Modus nur für eine Single-Hop-Vorlage aktivieren.

Konfigurieren Sie die Intervalle in der BFD-Vorlage:

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

- both Mindestkapazität für Übertragungs- und Empfangsintervall.
- Das Intervall in Millisekunden. Der Bereich liegt zwischen 50 und 999.
- microseconds (Mikrosekunden): Gibt das BFD-Intervall in Mikrosekunden für "forbothandmin-tx" an.
- Mikrosekunden Der Bereich liegt zwischen 50.000 und 999.000.
- min-tx: Die Funktion für das minimale Übertragungsintervall.

Konfigurieren Sie die Authentifizierung in der BFD-Vorlage:

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

- authentication Gibt den Authentifizierungstyp an.
- md5 MD5-Authentifizierung (Message Digest 5).
- meticulous-md5 Präzise verschlüsselte MD5-Authentifizierung.
- akribisch-sha-1 Akribisch verschlüsselte SHA-1-Authentifizierung.
- sha-1 Schlüsselbasierte SHA-1-Authentifizierung.
- 0|8-0 gibt an, dass ein UNVERSCHLÜSSELTES Kennwort folgt. 8 gibt an, dass ein VERSCHLÜSSELTES Kennwort folgt.
- word Das BFD-Kennwort (Schlüssel), d. h. ein einstelliges Kennwort bzw. ein Schlüssel mit bis zu 29 Zeichen. Kennwörter, die mit einer Ziffer gefolgt von einem Leerzeichen beginnen, werden nicht unterstützt, z. B. 0 pass und 1 sind ungültig.
- key-id: Die Authentifizierungsschlüssel-ID.
- id: Die ID des freigegebenen Schlüssels, die der Schlüsselzeichenfolge entspricht. Der Bereich umfasst 0 bis 255 Zeichen.

Edit FlexConfig Object				
Name: BFD-SINGLEHOP Description:	roduce line break	s while generating CLI.	. Please verify the	CLI before depl
Insert <b>T</b> Deployment:	Once		▼ Type:	Append
bfd-template single-hop TEMPLATE1 echo interval both 50 authentication sha-1 0 cisco key	-id 10			
▼ Variables			Description	
Name	Dimension	Default Value	Property (Type:Name)	Override
		No records to di	isplay	

Schritt 3:

Ordnen Sie die BFD-Vorlage der Schnittstelle zu.

Edit FlexConfig Object				
Name: BFD-SINGLEHOP				
Description:				
Copy-pasting any rich text might int	troduce line break	s while generating CLI.	Please verify the	e CLI before depl
Insert 🔻 🔢 Deployment	: Once		▼ Type:	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			Property	
Name	Dimension	Default Value	(Type:Name)	Override
		No records to dis	splay	
-				

Hinweis: Ordnen Sie die BFD-Multi-Hop-Vorlage einer Zielzuordnung zu.

Schritt 4 (optional).

Erstellen Sie eine BFD-Zuordnung mit Zielen, die Sie einer Multi-Hop-Vorlage zuordnen können. Es muss bereits eine Multi-Hop-BFD-Vorlage konfiguriert sein.

Ordnen Sie die BFD-Multi-Hop-Vorlage einer Zielzuordnung zu:

- ipv4 Konfiguriert eine IPv4-Adresse.
- ipv6 Konfiguriert eine IPv6-Adresse.
- destination/cdir Gibt das/die Zielpräfix/Länge an. Das Format ist A.B.C.D/<0-32>.
- source/cdir Gibt das/die Zielpräfix/Länge an. Das Format ist X:X:X;X::X/<0-128>.
- template-name Gibt den Namen der Multi-Hop-Vorlage an, die dieser BFD-Zuordnung zugeordnet ist.

Klicken Sie auf Save um das Objekt zu speichern.

Edit FlexConfig Object				
Name: BFD-MULTIHOP Description:	troduce line break	s while generating CLI.	Please verify the	CLI before deple
Insert 🔻 🔛 Deployment:	Once		Type:	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			Burnanta	
Name	Dimension	Default Value	Property (Type:Name)	Override
		No records to di	splay	

Schritt 5:

Klicken Sie auf Devices und wählen Sie die FlexConfig Option.

altah cisco	Firepower Manage Objects / Object Manager	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>&gt; Address</li> <li>&gt; Address</li> <li>&gt; Ciphe</li> <li>&gt; Come</li> </ul>	Server ss List ess Pools cation Filters ath er Suite List munity List	FlexConfig Object FlexConfig Object include device configura Name BFD-MULTIHOP	ation commands,	Device Management Device Upgrade NAT QoS Platform Settings FlexConfig 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	guished Name Server Group	BFD-SINGLEHOP BFD_Negate				
> Exter File L	nal Attributes ist Config	Default_DNS_Configure				Config Disable
F	lexConfig Object	Default_Inspection_Protocol_Enable				Enable
Geok Interf	ace	DHCPv6_Prefix_Delegation_Configure DHCPv6_Prefix_Delegation_UnConfigure				Config Remov
Key C Netw	Chain ork	DNS_Configure				Config
> PKI Polic	y List	Eigrp_Configure				Config
> Prefix	(List	Eigrp_Interface_Configure				Config
> Secu	rity Intelligence	Eigrp_Unconfigure_All				Clears
SLAT	Monitor					

#### Schritt 6:

Um eine neue FlexConfig-Richtlinie zu erstellen, klicken Sie auf New Policy - Taste.

diada cisco	Firepower Management Center Devices / FlexConfig	Overview	Analysis	Policies	Devices	Objects	АМР	Intelligence

Schritt 7.

Name die Richtlinie und wählen Sie die der Richtlinie zugewiesenen Geräte aus. Klicken Sie auf Add to Policy klicken Sie dann auf Save-Taste.

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

Schritt 8:

Wählen Sie in der linken Spalte das FlexConfig-Objekt aus, und klicken Sie auf > um das Objekt der FlexConfig-Richtlinie hinzuzufügen, und klicken Sie auf Save -Taste.

Firepower Management Center Devices / Flexconfig Policy Editor	Overview	/ Analysis	Policies	Devices	Objects	AMP	Intelligence	
BFD Enter Description								
Available FlexConfig C	") Select	ed Prepend Fl	exConfigs					
X Hear Defined		ime		De	escription			
	2							
BFD_SINGLEHOP								
✓ System Defined								
" Default_DNS_Configure								
Default_Inspection_Protocol_Disable								
" Default_Inspection_Protocol_Enable								
" DHCPv6_Prefix_Delegation_Configure		ed Append Fie	exConfigs					
DHCPv6_Prefix_Delegation_UnConfigure	# Na	ime		De	scription			
DNS_Configure	1 BF	D-MULTIHOP						
DNS_UnConfigure								
" Eigrp_Configure								
" i Eigrp_Interface_Configure								
? Eigrp_UnConfigure								
? Eigrp_Unconfigure_All								
"i Inspect_IPv6_Configure								
Inspect_IPv6_UnConfigure								

#### Schritt 9.

Klicken Sie auf Devices und klicke auf die Schaltfläche Device Management Option.

Firepower Management Center Devices / Flexconfig Policy Editor	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	
BFD				Device	Management		VPN	Troubleshoot
Enter Description				Device	Upgrade		Site To Site	File Download
				NAT			Remote Access	Threat Defense CLI
	Calected I	Prepend Fle	xConfigs	QoS Platform	n Settinas		Dynamic Access Policy Troubleshooting	Packet Tracer Packet Capture
Available FlexConfig C FlexConfig Object	# Name			FlexCor	nfig		Site to Site Monitoring	
<u> </u>				Certifica	ates			
V User Defined								
BFD-MULTIHOP								
BFD-SINGLEHOP								
"BFD_Negate								
✓ System Defined								
"? Default_DNS_Configure								
.9 Default_Inspection_Protocol_Disable								
" Default_Inspection_Protocol_Enable								
The DHCPv6_Prefix_Delegation_Configure	. Selected /	Append Flex	Configs					
J DHCPv6_Prefix_Delegation_UnConfigure	# Name			D	escription			
" DNS_Configure	1 BED-M							
.9 DNS_UnConfigure	I DED-IN	OLIHOP						
"il Eigrp_Configure								
ി Eigrp_Interface_Configure								
Eigrp_UnConfigure								
Eigrp_Unconfigure_All								
"i Inspect_IPv6_Configure								
"Inspect_IPv6_UnConfigure								

#### Schritt 10.

Wählen Sie das Gerät aus, dem die BFD-Konfiguration zugewiesen werden soll.

ciso	lı. F	Firepower Ma revices / Device M	anagement Ce Aanagement	enter o	Overview	Analysis	Policies	Devices	Objects	AMP Intelligence	
View	By: I (2)	Group Error (2)	• Warning (0)	▼ ● Offline	(0) • No	rmal (0)	Deployment	nt Pending (2)	<ul> <li>Upgrade (0</li> </ul>	)) 🔹 Snort 3 (2)	
Colla	ose Al										
	Na	me					Model		Version	Chassis	Licenses
	×	Ungrouped (2)									
	4	SF3130-A Sno 10.88.146.203	ort 3 - Routed				Firewall 3130 Thr	eat Defense	7.1.0	Manage	Base, Threat (2 mor
	•	SF3130-B Sno 10.88.146.205	ert 3 - Routed				Firewall 3130 Thr	eat Defense	7.1.0	Manage	Base, Threat (2 mor

Schritt 11.

Klicken Sie auf Routing auf, und klicken Sie dann auf IPv4 Oder IPv6, je nach Konfiguration im Abschnitt "BGP" in der linken Spalte. Klicken Sie dann auf Neighbor und klicke auf die Bleistiftschaltfläche, um sie zu bearbeiten.

Firepower Manager Devices / NGFW Routing	ment Center	Overview	Analysis	Policies	Devices	Objects	AMP	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	00 Highbor 3 Ad	ld Aggregate /	Address	Filtering N	etworks R	edistribution	Route Injection	
ECMP									
OSPF OSPFv3	Address		Re	mote AS Nun	nber	Add	dress Family		Remote Private AS Number
RIP	172.16.10.2		65	001		Ena	ibled		
Policy Based Routing									
✓ BGP									
IPv4 2									
IPv6									
Static Route									
V Multicast Routing									
IGMP									
PIM									
Multicast Routes									
Multicast Boundary Filter									

#### Schritt 12:

Wählen Sie checkbox für den BFD-Failover, und klicken Sie auf OK -Taste.

### Edit Neighbor

35.65535) Routes T	imers	Shutdown adr Configure grad Graceful resta BFD Fallover Advanced Outgoing Access List	ministratively ceful restart art(failover/spanned mode) Configuring BFD support for BGP for multi-hop, ensure that the BFD map is already created for the source destination pair through flex-config. Migration
35.65535) Routes T	Fimers	Configure grad Graceful resta BFD Fallover Advanced Outgoing Access List	ceful restart art(failover/spanned mode) Configuring BFD support for BGP for multi-hop, ensure that the BFD map is already created for the source destination pair through flex-config. Migration
35.65535) Routes T	Fimers	Graceful resta BFD Fallover Advanced Outgoing Access List	The source destination pair through flex-config.
35.65535) Routes T	Fimers	BFD Fallover Advanced Outgoing Access List	Configuring BFD support for BGP for multi-hop, ensure that the BFD map is already created for the source destination pair through flex-config. Migration
Routes T	Timers	Advanced Outgoing Access List	Configuring BFD support for BGP for multi-hop, ensure that the BFD map is already created for the source destination pair through flex-config. Migration
Routes T	Fimers	Advanced Outgoing Access List	Migration • +
•	+	Outgoing Access List	• +
	- +	Access List	+
•	+		• +
		Route Map	
•	+		• +
		Prefix List	
•	+		• +
	_	AS path filter	
•	+		• +
prefixes allo	wed from	m the neighbor	
	v prefixes allo	+ prefixes allowed from	<ul> <li>+</li> <li>AS path filter</li> <li>+</li> <li>prefixes allowed from the neighbor</li> </ul>

Schritt 13:

Klicken Sie auf Deploy klicken Sie auf die Schaltfläche Deployment - Taste.

altalta cisco	, Firepower Management Center Devices / Device Management			view Analysis	Policies	Devices	Objects	AMP	Intelligence	
View By:	Group		•							
All (2)	Error (2)	Warning (0)	• Offline (0)	Normal (0)	<ul> <li>Deployment</li> </ul>	Pending (2)	Upgrade	(0) 😐	Snort 3 (2)	

Wählen Sie das Gerät aus, dem die Änderungen zugewiesen werden sollen, indem Sie auf das checkbox, und klicken Sie dann aufDeploy -Taste.

ciso	() () :0	Firepower Management Center Deploy / Deployment	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	
T	٩	Q Search using device name, user name, type, group or status								
		Device		Modified by		Inspect I	nterruption	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

Schritt 15:

Klicken Sie auf Deploy - Taste.



Schritt 16:

Klicken Sie auf Deploy - Taste.



Hinweis: Die Warnung wird erwartet und ist nur informativ.

## Überprüfung

Überprüfen Sie mit den nächsten Befehlen die BFD-Konfiguration und den Status direkt in der CLI-Sitzung.

<#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											
Total	Session 1	Up 1	Down Ø								
SF3130-A#											
show bfd neighbors											
IPv4 Sessions				RH/RS	State	Int					
172.16.10.2			1/1	Up	JLALE	THE					

## Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

#### Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.