# Flex-Configを使用したセキュアファイアウォー ル脅威対策でのBFDの設定

## 内容

<u>概要</u>	
<u>前提条件</u>	
<u>要件</u>	
<u>使用するコンポーネ</u>	ント
<u>背景説明</u>	
<u>設定</u>	
<u>確認</u>	
<u>トラブルシュート</u>	

#### 概要

このドキュメントでは、Flex-Configを使用して7.2以前を実行するSecure Firewall Management Center(SCM)でBFDプロトコルを設定する方法について説明します。

## 前提条件

Cisco Secure Firewall Management Center(FMC)を備えたCisco Secure Firewall Threat Defense(FTD)でBorder Gateway Protocol(BGP)が設定されていること。

#### 要件

次の項目に関する知識があることが推奨されます。

-BGPプロトコル -BFDの概念

#### 使用するコンポーネント

- 7.2以前のバージョンを実行しているCisco Secure Firewall Management Center。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

## 背景説明

双方向フォワーディング検出(BFD)は、すべてのメディアタイプ、カプセル化、トポロジ、およ びルーティングプロトコルに対して高速フォワーディングパス障害検出時間を提供するように設 計された検出プロトコルです。

#### 設定

バージョン7.2以前を実行しているFMCのBFD設定は、Flex-Configのポリシーとオブジェクトを 使用して設定する必要があります。

ステップ1:

FlexconfigオブジェクトからBFDテンプレートを作成します。

BFDテンプレートは、BFD間隔値のセットを指定します。BFDテンプレートに設定されている BFD間隔の値は、1つのインターフェイスに固有のものではありません。また、シングルホップお よびマルチホップセッションの認証も設定できます。

Flex-Configオブジェクトを作成するには、 Objects Tab 上部の FlexConfig オプションをクリックし、 FlexConfig Object オプションを選択し、 Add FlexConfig Object.

CISCO Firepower Manag Objects / Object Manage	ement Center Overview Analysis Policies Devices Objects 1 AMP Intelligence	Deploy Q 🌮 🕻	8 🕜 admin 🔻							
<ul> <li>&gt; AAA Server</li> <li>&gt; Access List</li> <li>&gt; Address Pools</li> <li>Application Filters</li> </ul>	FlexConfig Object FlexConfig Object include device configuration commands, variables, and scripting language instructions. It is used in FlexConfig polices.	4 Add FlexConfig Object Q Filter								
AS Path	Name Description									
Cipher Suite List	BFD-MULTIHOP	FD-MULTIHOP								
Distinguished Name	BFD-SINGLEHOP	D-SINGLEHOP								
DNS Server Group	BFD_Negate	D_Negate Fig								
> External Attributes	befault_DNS_Configure Default DNS with the help of TextObjects def 📭									
Flectist FlexConfig 2	Default_Inspection_Protocol_Disable	Default_Inspection_Protocol_Disable Disable Default Inspection.								
FlexConfig Object	Default_Inspection_Protocol_Enable	Enable Default Inspection.	<b>G</b> Q =							
Text Object	DHCPv6_Prefx_Delegation_Configure	Configure one outside (PD client) and one inside interfa	<b>₽</b> Q =							
Interface	DHCPv6_Prefix_Delegation_UnConfigure	Remove configuration of one outside (PD client) and on	<b>Β</b> Q ]]							
Key Chain	DNS_Configure	Configure DNS with the help of TextObjects dnsParame	¶a ⊒							
Network	DNS_UnConfigure	Remove the DNS configurations.	E q ≓							
Policy List	Eigrp_Configure	Configures eigrp. 1. Configures next hop, 2. configures	FL Q T							
Port	Elaro Interface Configures interface parameters for elaro. 1. Configure									
> Prefix List	Eigrp_UnConfigure	Clears eigrp configuration for an AS	Fig. Q							
> Security Intelligence	Elaro Unconfigure All	Clears elorp configuration.	E o =							
Sinkhole										
SLA Monitor		Displaying 1 - 20 of 51 rows 1 < < Page 1	of 3 > >  C							

ステップ 2:

BFDプロトコルに必要なパラメータを追加します。

BFDテンプレートは、BFD間隔値のセットを指定します。BFDテンプレートに設定されている BFD間隔の値は、1つのインターフェイスに固有のものではありません。また、シングルホップお よびマルチホップセッションの認証も設定できます。

- single-hop:シングルホップBFDテンプレートを指定します。
- multi-hop:マルチホップBFDテンプレートを指定します。
- template\_name:テンプレート名を指定します。テンプレート名にスペースを含めることはできません。
- (オプション)シングルホップBFDテンプレートでエコーを設定します。

注:エコーモードはシングルホップテンプレートでのみ有効にできます。

BFDテンプレートで間隔を設定します。

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

- both:最小送信間隔機能および最小受信間隔機能。
- ミリ秒単位の間隔。範囲は 50~999 です。
- microseconds:bothandmin-txのBFD間隔をマイクロ秒単位で指定します。
- マイクロ秒:範囲は50,000~999,000です。
- min-tx:最小送信間隔機能。

BFDテンプレートで認証を設定します。

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

- authentication:認証タイプを指定します。
- md5:Message Digest 5(MD5)認証。
- finiculous-md5:キー設定されたMD5認証を入念に行います。
- finiculous-sha-1:キー設定されたSHA-1認証を使用します。
- sha-1:キー設定されたSHA-1認証。
- 0|8:0は、暗号化されていないパスワードが後に続くことを指定します。8は、 ENCRYPTEDパスワードが後に続くことを指定します。
- ・ word:BFDパスワード(キー)。最大29文字の1桁のパスワード/キーです。数字で始まり、

その後に空白が続くパスワードはサポートされません。たとえば、0パスと1は無効です。

- ・ key-id:認証キーID。
- id:キー文字列と一致する共有キーID。範囲は0~255文字です。

Edit FlexConfig Object							
Name: BFD-SINGLEHOP							
Description:							
Copy-pasting any rich text might int	roduce line break	s while generating C	LI. Please	verify the Type:	CLI before deployr	nent.	
bfd-template single-hop TEMPLATE1 echo interval both 50 authentication sha-1 0 cisco key	-id 10						
▼ Variables							
Name	Dimension	Default Value	Prop (Type	erty e:Name)	Override	Description	
		No records to	display				
							Save

ステップ 3:

BFDテンプレートをインターフェイスに関連付けます。

Edit FlexConfig Object						
Name: BFD-SINGLEHOP Description:						
Copy-pasting any rich text might int	roduce line break	ks while generating C	LI. Please verify the	e CLI before deplo	yment.	
bfd-template single-hop TEMPLATE1 echo interval both 50 authentication sha-1 0 cisco key interface Ethernet1/7 bfd template TEMPLATE1	-id 10					
▼ Variables						
Name	Dimension	Default Value	Property (Type:Name)	Override	Description	
		No records to	display			
					Cancel	Save

注:BFDマルチホップテンプレートを宛先のマップに関連付けます。

ステップ 4(任意):

マルチホップテンプレートに関連付けることができる宛先を含むBFDマップを作成します。マル チホップBFDテンプレートがすでに設定されている必要があります。

BFDマルチホップテンプレートを宛先のマップに関連付けます。

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

- ・ ipv4:IPv4アドレスを設定します。
- ・ ipv6:IPv6アドレスを設定します。
- destination/cdir: 宛先のプレフィクス/長さを指定します。形式はA.B.C.D/<0-32>です。

- source/cdir: 宛先のプレフィクス/長さを指定します。形式はX:X:X;X::X/<0-128>です。
- template-name:このBFDマップに関連付けられているマルチホップテンプレートの名前を 指定します。

ポリシーの横の [レポート(Report)] save ボタンをクリックします。

Edit FlexConfig Object							9
Name: BFD-MULTIHOP Description:	troduce line break	s while generating Cl	LI. Please	verify the	e CLI before deploy	yment.	
Insert 🔻 🔣 Deployment	Once		•	Туре:	Append	•	
bfd map ipv4 10.11.11.0/24 10.36.	42.5/32 MULTI-1	'EMPLATE1					
▼ Variables			Prop	ortu			
Name	Dimension	Default Value	(Туре	e:Name)	Override	Description	
		No records to	display				
						Cancel	Save

#### ステップ 5:

ポリシーの横の [レポート (Report)] Devices タブをクリックし、 FlexConfig オプション.

CISCO Firepower Manage Objects / Object Manager	ement Center Overview Analysis Policies	Devices 1 Objects	AMP Intelligence		Deploy Q 🤞	😕 🌣 🕜 admin 🕶		
<ul> <li>&gt; AAA Server</li> <li>&gt; Access List</li> <li>&gt; Address Pools</li> <li>Application Filters</li> </ul>	FlexConfig Object FlexConfig Object include device configuration commands	Device Management Device Upgrade NAT QoS Platform Settings	VPN Site To Site Remote Access Dynamic Access Policy Troubleshooting	Troubleshoot File Download Threat Defense CLI Packet Tracer Packet Capture	FlexConfig Object Q. Filter			
AS Path Ciober Suite List	Name	FlexConfig 2	Site to Site Monitoring		on			
Community List	BFD-MULTIHOP	Certificates				G/₹		
> Distinguished Name	BFD-SINGLEHOP					<b>6/</b> €		
DNS Server Group	BFD_Negate					<b>6/</b> €		
> External Attributes	Default_DNS_Configure			Config	gure Default DNS with the help of TextObjects def	Faq		
File List	Dataili Iseanalise Dataili Iseanalise							
FlexConfig Object	Default Inspection, Portage Section							
Text Object	Denaut_Inspection_Protocol_Enable			Enau	e Deraut inspection.			
Geolocation	DHCPv6_Prefix_Delegation_Configure			Config	gure one outside (PD client) and one inside interfa			
Interface	DHCPv6_Prefix_Delegation_UnConfigure			Remo	ve configuration of one outside (PD client) and on	<b>P</b> aq ≣		
Key Chain	DNS_Configure			Configure DNS with the help of TextObjects dnsParam				
> PKI	DNS_UnConfigure			Remo	ve the DNS configurations.	Pa Q		
Policy List	Eigrp_Configure			Config	gures eigrp. 1. Configures next hop. 2. configures	Faq		
Port	Eigrp_Interface_Configure			Config	gures interface parameters for eigrp. 1. Configure	Fac, ⊒		
> Prefix List	Fiam LinConfigure			Ciear	s elorn configuration for an AS	B O D		
Security Intelligence	entre moderne te			01	reigep vormgunation für vier			
Sinkhole	Eigrp_Unconfigure_All			Clean	s eigrp configuration.	<b>B</b> ⊂ U		
SLA Monitor					Displaying 1 - 20 of 51 rows 1 < < Page	l of 3 > >l C		

#### 手順 6:

新しいFlexConfigポリシーを作成するには、 New Policy をクリックして、クエリーを実行します。

alaala cisco	Firepower Management Center Devices / FlexConfig	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	¢ 🌮	🕜 admin 🔻
										[	New Policy

手順 7:

Name ポリシーに割り当てられたデバイスを選択します。ポリシーの横の [レポート(Report)] Add to Policy 次に、 Saveをクリックして、クエリーを実行します。

New Policy				?
Name: BFD	] 1			
Description:				
Select devices to which you want to Available Devices Q Search by name or value SF3130-A SF3130-B 2	Add to Policy	Selected Devices SF3130-A SF3130-B		
			Cancel	Save

ステップ 8:

左側の列でFlexConfigオブジェクトを選択し、 > ボタンをクリックしてオブジェクトを FlexConfigポリシーに追加し、 save をクリックして、クエリーを実行します。

Firepower Management Center Devices / Flexconfig Policy Editor	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deptoy Q 🧨🏕	🕜 admin 🔻
BFD Enter Description								You have unsaved changes Preview Config	Cancel
								Policy A:	ssignments (2)
	Selected	Prepend Flex	xConfigs						
Available FlexConfig C FlexConfig Object	II Name			De	escription				
V User Defined	2								
BFD-MULTHOP									
BFD-SINGLEHOP									
"BFD_Negate									
V System Defined									
Default_DNS_Configure									
" Default_Inspection_Protocol_Disable									
Default_Inspection_Protocol_Enable	. Selected	Append Flex	Configs						
DHCPv6_Prefix_Delegation_Configure		-append ties	teoninge						
DHCPv6_Prefix_Delegation_UnConfigure	# Name			De	scription				
The DNS_Configure	1 BFD-N	ULTIHOP							۹
DNS_UnConfigure									
i Eigrp_Configure									
Eigrp_Interface_Configure									
- Eigrp_UnConfigure									
- Eigrp_Unconfigure_All									
inspect_IPv6_Configure									

## ステップ 9:

ポリシーの横の [レポート(Report)] Devices タブをクリックし、 Device Management オプション.

Firepower Management Center Devices / Flexconfig Policy Editor	Overview Analysis Policies	Devices 1 Objects AM	P Intelligence		Deploy Q 🌮 🌣	🕑 admin 🕇
BFD Enter Description Available FlexConfig C FlexConfig Object Viser Defined BFD-MULTEROP BFD-SINGLEHOP BFD-SINGLEHOP BFD_Negate System Defined Default_DNS_Configure	Selected Prepend FlexConfigs  Name	Device Management 2 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	unsaved changes Preview Config Save Policy As	Cancel sssignments (2)
Default_Inspection_Protocol_Disable     Default_Inspection_Protocol_Enable						
** DHCPv6_Prefix_Delegation_Configure	Selected Append FlexConfigs					
DHCPv6_Prefix_Delegation_UnConfigure	# Name	Description				
T DNS_Configure	1 BFD-MULTIHOP					٩
*1: Eigrp_Configure *1: Eigrp_Unterface_Configure # Eigrp_Unconfigure # Eigrp_Unconfigure_All *1: Inspect_IPv6_Configure # Inspect_IPv6_UnConfigure						

ステップ 10:

BFD設定を割り当てるデバイスを選択します。

cisco	Firepower Management Center Overview Analysi Devices / Device Management	is Policies Devices	Objects A	MP Intelligence		Deploy Q 🌄 🕫	🕜 admin
View By	Group					Deployme	ent History
All (2	Error (2)      Warning (0)     Offline (0)     Normal (0)	<ul> <li>Deployment Pending (2)</li> </ul>	<ul> <li>Upgrade (0)</li> </ul>	<ul> <li>Snort 3 (2)</li> </ul>		Q Search Device	Add 🔻
Collapse							
	Name	Model	Version	Chassis	Licenses	Access Control Policy	
	<ul> <li>Ungrouped (2)</li> </ul>						
	SF3130-A Short 3 10.88.146.203 - Routed	Firewall 3130 Threat Defense	7.1.0	Manage	Base, Threat (2 more)	Default	1
	() SF3130-B Snort 3 10.88.146.205 - Routed	Firewall 3130 Threat Defense	7.1.0	Manage	Base, Threat (2 more)	Default	1

ステップ 11

ポリシーの横の [レポート(Report)] Routing タブをクリックし、IPv4 または IPv6, 左側の列の BGPセクションの設定に応じて、 Neighbor タブをクリックし、[鉛筆を編集]ボタンをクリックして 編集します。

CISCO Firepower Manage Devices / NGFW Routing	ement Center <sub>Overview</sub> Analy	rsis Policies Devices Obje	cts AMP Intelligence		Deploy	Q 🎒 🖓 admin 🔻				
SF3130-A Cisco Secure Firewall 3130 Threat Defense Device Routing 1 Interfaces Inline Sets DHCP										
Manage Virtual Routers Global	Enable IPv4: AS Number 65000 General Neighbor 3 Add Aggre	gate Address Filtering Networks	Redistribution Route Injection							
ECMP OSPF						+ Add				
OSPFv3	Address	Remote AS Number	Address Family	Remote Private AS Number	Description					
RIP	172.16.10.2	65001	Enabled			4 🔼 i				
Policy Based Routing V BGP										
IPv4 2										
IPv6 Static Route										
Static Route ~ Multicast Routing IGMP PIM Multicast Routes Multicast Boundary Filter										

ステップ 12

次のいずれかを選択します。 checkbox BFDのfalloverを探し、 ок をクリックして、クエリーを実行 します。

Edit Neighbor		0
IP Address* 172.16.10.2 Remote AS* 65001 (1-4294967295 or 1.0-65535.65535) Description	<ul> <li>Enabled address</li> <li>Shutdown administratively</li> <li>Configure graceful restart</li> <li>Graceful restart(failover/spanned mode)</li> <li>BFD Fallover          <ul> <li>Configuring BFD support for BGP for multi-hop, ensure that the BFD map is already created for the source destination pairs through files-config</li> </ul> </li> </ul>	
Filtering Routes Routes Time	ers Advanced Migration	
Incoming Access List Route Map Prefix List AS path filter Limit the number of prefixes allowed Maximum Prefixes* (1-2147483647)	Outgoing Access List + + Route Map + + Prefix List + + AS path filter + + d from the neighbor	
		ОК

#### ステップ 13

ポリシーの横の [レポート(Report)] Deploy ボタンをクリックし、 Deployment をクリックして、ク エリーを実行します。

ahaha cisco	Firepower Ma Devices / Device M	anagement Centra lanagement	er <sub>Overview</sub>	Analysis	Policies	Devices	Objects	AMP	Intelligence	1 Deploy Q 🥮 3	🍹 🕜 admin 🕶
View By:	Group									2 Deployment	hent History
All (2)	Error (2)	Warning (0)	Offline (0)	Normal (0)	Deployment	Pending (2)	<ul> <li>Upgrade</li> </ul>	(0)	Snort 3 (2)	Deployment History	Add 🔻

#### ステップ 14:

変更を割り当てるデバイスを選択するには、 checkboxをクリックし、Deploy をクリックして、クエリーを実行します。

altal cisco	•	Firepower Management Center Deploy / Deployment	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence			Deploy Q 🧬🌣	🕑 admin 🕶
<b>T</b>	۹	Search using device name, user name, type, {	group or status									2	Deploy
		Device		Modified by		Inspect In	nterruption	Туре	Group	Last Deploy Time	Preview	Status	
>		SF3130-B		admin				FTD		Jul 18, 2023 4:55 PM	B.	Ready for Deployment	
>		SF3130-A		admin				FTD		Jul 18, 2023 4:55 PM		Ready for Deployment	

ポリシーの横の [レポート(Report)] Deploy をクリックして、クエリーを実行します。

Deployment Confirmation	$\times$
You have selected 1 device to deploy Deployment Notes:	
You can optionally add notes about the configuration changes	
Cancel	oy

ステップ 16:

ポリシーの横の [レポート (Report)] Deploy をクリックして、クエリーを実行します。



注:警告は予期されるものであり、単に情報を提供するためのものです。

## 確認

次のコマンドを使用して、CLIセッションのBFD設定とステータスを直接確認します。

<#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 0			
SF3130-A#						
show bfd neighbors						
IPv4 Sessions NeighAddr 172.16.10.2		I	_D/RD 1/1	RH/RS Up	State	Int

## トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。