# GUIを使用したセキュアファイアウォール脅威防 御でのBFDの設定

# 内容

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

# 概要

このドキュメントでは、7.3以降を実行するSecure Firewall Management Center(FMC)でBFDプロ トコルを設定する方法について説明します。

#### 要件

次の項目に関する知識があることが推奨されます。

- ・ボーダーゲートウェイプロトコル(BGP)プロトコル
- 双方向フォワーディング検出(BFD)の概念

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ・ セキュアFMC仮想バージョン7.3.1
- バージョン7.3以降を実行するCisco Secure FMCを使用するCisco Secure Firewall Threat Defense(FTD)で設定されたBGP

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

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な転送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。

バージョン7.3以降を実行するFMCのBFD設定については、次の手順を参照してください。

ステップ1:次に移動します。 Devicesボタンをクリックし、 Device Managementをクリックして、クエリーを実行します。

Firewall Management Center Overview / Dashboards / Dashboard	Overview Analysis Policies	Devices Objects Integration	Deploy Q 🤩 🏷 🕢 admin 🕇 🕬 SECURE
Summary Dashboard (setuin databased) Provides a summary of activity on the appliance Network Threats Intrusion Events St	atus × Geolocation QoS	Device Management         VPN         Teudieshoot           Device Upgrade         Site To Site         File Download           NAT         Remote Access         Threat Defense CLI           QoS         Dynamic Access Policy         Packet Tracer           Platform Settings         Troubleshooting         Packet Capture	Reporting Show the Last 1 hour • II
► Appliance Status		Hexcomig Certificates I - Арриалов изотласол - А	Add Widgets  Current Sessions - X
Normal (D)		Name PNC-Hack72 IPv4 Address 10.88.243.103 IPv6 Address Disabled Model Secure Firewall Management Center for VMware	Username         Address         Accessed           ▲ admin         10.152.200.94         12:16:23
		Versions         7.3.1           Software         7.3.1           Rule Update         2023-07-12-001-vrt           Geolocation Update         2023-07-10-101           VOB         X6	
	-Critical (3)	► RSS Feed - Unable to download feed - ×	Boot Time 2023-07-19 18:57:42
Product Updates		Unable to download feed	► System Load -×
Type Current	Latest		Last 1 hour Now
Geolocation Update Local Geolocation Update 2023-07-10-101 Rule Update			CPU 0 6% CPU 1 8%
Local Rule Update 2023-07-12-001-wt Software			CPU 2 9%
1 Management Center 7.3.1 2 Devices 7.3.1			CPU 3 6%
VDB 1 Management Center 368			Memory 23% Load Avg
► Disk Usage			
By Category:			
https://10.88.243.103/ddd/#SensorList			

画像 1.FMCダッシュボード。

### ステップ2:BFDプロトコルを設定するデバイスを選択します。

Firewall Management Center Overview Analysis	Policies Devices Obje	icts Integra	tion		Deploy Q 🧬 🖁	🌣 😨 admin 🕶 🔤	SECURE
View By:	Deployment Pending (0)	Upgrade (2)	<ul> <li>Snort 3 (2)</li> </ul>		٥	Deployment	History Add 🔻
Collaose All							
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (2)							
SF3130-A Snort 3 10.88.146.203 - Routed	Firewall 3130 Threat Defense		Manage	Essentials, IPS (2 more)	Default		1:
SF3130-B Snort 3 10.88.146.205 - Routed	Firewall 3130 Threat Defense		Manage	Essentials, IPS (2 more)	Default		1:

ステップ 3:ポリシーの横の [レポート(Report)] Routingタブをクリックし、 BFD オプションを選択します。設定するオプションを選択します(Single-Hop または Multi-Hop)を選択し、 Addを参照。

Firewall Manageme Devices / Secure Firewall Ro	nt Center Overview Analysis Policies Devices Objects Integration	Deploy	<b>6</b> ¢	3 admin ▼   <sup>attrativ</sup> secure
SF3130-A Cisco Secure Firewall 3130 Threat Device Routing 1 Interfac	Defense es Inline Sets DHCP			Sive Cancel
Manage Virtual Routers Global	Bidirectional Forwarding Detection Routing (BFD)			
COMP COMP CSPFv3 EIGRP RIP Policy Based Routing V BGP IPv4 IPv6 Static Route V Multicast Routing IGMP PIM Multicast Routes Multicast Routes Multicast Boundary Filter	Slow Timer 1000 (1000-30000) There are no BFD records Add			4 🚮
General Settings				

画像 3.Device Routingセクション

ステップ 4:次のいずれかを選択します。 Interface BFDプロトコルを設定する場所を指定し、 + を クリックして、クエリーを実行します。

	nt Center Overview				Deploy Q 🥩 🗱 👩 admin 🔻 🔤				
SF3130-A Cisco Secure Firewall 3130 Threat I									
Device Routing Interfac									
	Bidirectional Forwa	arding Detection	Routing (BFD)						
Global •									
			Add BFD Single-Hop	0					
			Interface	1					
			BGP	` '	Add				
			Template Name						
			Select  Template Name is mandatory	<u>+</u> 2					
				Cancel OK					
					,				
				There are no BED records Ar	14				

図 4.インターフェイスの選択

ステップ 5:テンプレートに名前を付け、BFDに必要なパラメータを設定してから、Saveボタンをクリックします。

Errewall Management Center Overview Analysis Policies Devices Objects Integration Deploy Q. 🧬 🌣 🕢 admin 🔻 🛱 SECURE							
		uting (BFD)					
		Add BFD Template Object					
		Name*					
		Type: Single-Hop O Multi-Hop		Add			
		Echo: disabled					
		Interval Authentication		/1			
		Interval Type: None •					
		Minimum Transmit:					
		Minimum Receive:					
			Cancel Save				

図 5.テンプレートの設定。

#### 注:エコー機能は、シングルホップモードでのみ使用できます。

#### 手順6:前の手順ですでに作成したテンプレートを選択し、 oxを参照。

Firewall Managemen Devices / Secure Firewall Re	nt Center Overview Analysis Policies Devices	Objects Integration	Deploy 🔍 🧬 🌣 😨 admin 🔻 🔤 SECURE
SF3130-A Cisco Secure Firewall 3130 Threat Device Routing Interfac			
Manage Virtual Routers Global • Virtual Router Properties	Bidirectional Forwarding Detection Routing	(BFD)	
BFD OSPF OSPFv3		Edit BFD Single-Hop	Add
EIGRP RIP Policy Based Routing		Template Name Template 1 v +	/ î
IPv4 IPv6 Static Route		Cancel OK	
✓ Multicast Routing IGMP PIM			
Multicast Routes Multicast Boundary Filter General Settings			
BGP			

図 6.テンプレートの選択。

ステップ 7(オプション):BFDのフォールオーバーについては、 IPv4 または IPv6ボタンをクリックします。次のいずれかを選択しますNeighbor タブをクリックし、右側の編集鉛筆をクリックして 目的のネイバーアドレスを選択します。

Firewall Managemen	nt Center Overview A	malysis Policies Devices	Objects Integration		Deploy Q 🧬 🌣 🕜 admin 🗸 🔤 secure
SF3130-A Cisco Secure Firewall 3130 Threat D	Defense				You have unsaved changes Save Cancel
Device Routing Interfac	es Inline Sets DHCP				
Manage Virtual Routers	Enable IPv4: 🗹 AS Number 65000				
Global •					
Virtual Router Properties	General Neighbor 2 Add	Aggregate Address Filtering	Networks Redistribution Rout	e Injection	
ECMP					+ Add
BFD					
OSPF	Address	Remote AS Number	Address Family	Remote Private AS Number	Description
OSPFv3	172.16.10.2	65001	Enabled		3 ∠i
EIGRP					
RIP					
Policy Based Routing					
Y BGP					
IPv4					
IPv6					
Static Route					
<ul> <li>Multicast Routing</li> </ul>					
IGMP					
PIM Multi-set Deutee					
Multicast Routes					
Multicast boundary Pilter					
General Settings					

図 7.ネイバー設定。

ステップ 8(オプション):BFD Failover forオプションを選択します。 single\_hop または multi\_hop をクリックして окを参照。

Firewall Management Center Devices / Secure Firewall Routing	Overview Analysis Policies Devices	Objects Integration	Deploy Q 🧳 🏟 🕢 admin 🗸 📑
SF3130-A			You have unsaved changes Save Cancel
Cisco Secure Firewall 3130 Threat Defense			
Device Routing Interfaces Inline Sets	DHCP Edit Neighbor		
Manage Virtual Routers     Enable IPv4: €       Global     ✓       Virtual Router Properties     General       ECMP     Address       OSPF     Address       OSPFv3     172.16.10.2       EIGRP     RIP       RIP     Bed       EV4     Ev6       Static Route     Multicast Routing       YMP     PiM       Multicast Routes     Multicast Boundary Filter	00 IP Address* 172.16.10.2 Remote AS* 65001 (1-4294067295 or 1.0-65535.655 BFD Fallover Single_hop Indit_hop auto_detect_hop none Prefix List Limit the number of prefixes al Maximum Prefixes*	Enabled address Shuddown administratively Configure graceful restart( Graceful restart(fallower/spanned mode) Description Particular start(fallower/spanned mode) Advanced Migration Outgoing Access List Access List + Prefix List + Prefix List + + Aspath filter + - + - + - + - + + + + <	+ Add Description
General Settings	(1-2147483647)		
BGP	Threshold Level		
		Cance	OK

図 8.BFD Fallover設定。

ステップ 9:設定を保存するには、 save をクリックして、クエリーを実行します。

Firewall Management Devices / Secure Firewall Rout	t Center Overview Ani	alysis Policies Devices Objects	Integration		Deploy Q 🗳 🌣 🗿 admin 🕶 🔤
SF3130-A Cisco Secure Firewall 3130 Threat D	ofense				You have unsaved changer Save Cancel
Device Routing Interface Manage Virtual Routers Global	s Inline Sets DHCP VTEP Enable IPv4: 🗹 AS Number 65000 General <u>Neighbor</u> Add Ay	y gregate Address Filtering Networks R	distribution Route Injection		
ECMP					+ Add
OSPF	Address	Remote AS Number	Address Family	Remote Private AS Number	Description
OSPFv3			Enabled		/i
EIGRP RIP Policy Based Routing > BGP IPv6 Static Route VMulticast Routing IGMP PIM Multicast Routes Multicast Routes Multicast Routes General Settings					
BGP					

図 9.設定の保存

ステップ 10:ポリシーの横の [レポート(Report)] Deploy ボタンをクリックし、 checkbox 変更を適用したデバイスに対して、もう一度 Deploy をクリックして、クエリーを実行します。

Firewall Management	t Center Overview Analysis	Policies Devices Objects Integr	ation		🥐 🌣 🕜 admin 🔹 號 SECURE
SF3130-A					Advanced Deploy Deploy neel
Cisco Secure Firewall 3130 Threat D	efense			SF3130-A 2	Ready for Deployment
Device Routing Interface	s Inline Sets DHCP VTEP				
Manage Virtual Routers	Enable IPv4: 🗹				
Global	AS Number 65000				
	General Neighbor Add Aggregate A	ddress Filtering Networks Redistril	bution Route Injection		
Virtual Router Properties					
BED					bb
OSPF	Address	Remote AS Number	Address Family		
OSPFv3	172.16.10.2	65001	Enabled	1 selected 0 1 pending	₽ •9 ■
EIGRP					-
RIP					
Policy Based Routing					
✓ BGP					
IPv4					
IPv6					
Static Route					
Y Multicast Routing					
IGMP					
PIM					
Multicast Routes					
Multicast Boundary Filter					
General Settings					
BGP					

図 10.変更の展開。

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>

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#
SF3130-A#

show bfd summary

Total SF3130-A# SF3130-A# show bfd neighbors	Session 1	Up 1	Down O			
IPv4 Sessions NeighAddr 172.16.10.2		I	LD/RD 1/1	RH/RS Up	State Up	Int BGP

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。