Configuration de BFD dans Secure Firewall Threat Defense avec GUI

Table des matières

Introduction Exigences Composants utilisés Informations générales Configurer Vérifier Dépannage

Introduction

Ce document décrit comment configurer le protocole BFD dans Secure Firewall Management Center (FMC) exécutant 7.3 et versions ultérieures.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Protocole BGP (Border Gateway Protocol)
- · Concepts de détection de transfert bidirectionnel (BFD)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Secure FMC Virtual version 7.3.1
- BGP configuré dans Cisco Secure Firewall Threat Defense (FTD) avec Cisco Secure FMC version 7.3 et ultérieure

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

BFD est un protocole de détection conçu pour fournir des temps de détection de défaillance de chemin de transmission rapide pour tous les types de supports, les encapsulations, les topologies et les protocoles de routage.

Configurer

Reportez-vous à ces étapes pour les configurations BFD dans FMC exécutant les versions 7.3 et ultérieures.

Étape 1. Accédez à la page Devices dans la partie supérieure et cliquez sur le bouton Device Managements'affiche.

Firewall Management Center Overview / Dashboards / Dashboard	Verview Analysis	Policies	Devices 1 Objects	Integration			Deploy Q 🧬 🌣 () admin ▼ their SECURE
Summary Dashboard (setto: distributed) Provides a summary of activity on the appliance Network Threats Intrusion Events Sta	itus × Geolocation	QoS	Device Management Device Upgrade NAT QoS Platform Settings	Site To Site Remote Access Dynamic Access Policy Troubleshooting	Troubleshoot File Download Threat Defense CLI Packet Tracer Packet Capture		Show the Last 1 hOut	Reporting
			FlexConfig Certificates					
Appliance Status			 Appliance information 		- *	 Current Sessions 		
Normal (0)			Name Word Address	FMC-HackTZ		Username	Address	Accessed
			IPv6 Address Model	Disabled Secure Firewall Management Center for V				
			Versions Software Rule Update Geolocation Update VDB	7.3.1 2023-07-12-001-wrt 2023-07-10-101 365		System Time System Time Uptime Boot Time		- × 2023-07-20 12:19:42 17:22:00 2023-07-19 18:57:42
			 RSS Feed - Unable to d 	ownload feed				
Product Updates			U	nable to download feed		 System Load 		- ×
Type Current	Latest						Last 1 hour	Now
Geolocation Update Local Geolocation Update 2023-07-10-101						CPU 0		6%
Rule Update Local Rule Update 2023-07-12-001-vrt						CPU 1		
Software 1 Management Center 7.3.1						CPU 2		
2 Devices 7.3.1						Nemory		23%
1 Management Center 368						Load Avg		0.36
1. Philipping								
By Category:								

Image 1. Tableau de bord FMC.

Étape 2. Sélectionnez le périphérique que vous souhaitez configurer le protocole BFD.

Firewall Management Center Overview Analysis	Policies Devices Object	ts Integrat	ion		Deploy Q 🇳	🔅 🕜 admin 🕶 🏻 🖏	SECURE
View By: Group		learned a (0)	8 Court 8 (8)			Deploymen	t History
All (2) Fror (0) Warning (0) Children (0) Normal (2) Collapse All	 Deployment Pending (U) 	upgrade (2)	Short 3 (2)		C	or search perice	Add
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Unprouped (2)							
SF3130-A Short 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	7.3.1	Manage	Essentials, IPS (2 more)	Default	4D	1:



Étape 3. Cliquez sur le bouton Routing, puis cliquez sur l'onglet BFD dans la colonne de gauche. Sélectionnez l'option que vous souhaitez configurer (Single-Hop OU Multi-Hop), puis cliquez sur Add.

Firewall Management Devices / Secure Firewall Ro	nt Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🤩 🌣 🕜 admin 🕶 🖓 thether SECURE
SF3130-A Cisco Secure Firewall 3130 Threat Device Routing 1 Interfac	Defense es Inline Sets DHCP	Cancel
Manage Virtual Routers Global • Virtual Router Properties	Bidirectional Forwarding Detection Routing (BFD)	
ECMP		
BFD 2	1000 (1000-20000)	
OSPF		
OSPFv3		4 Add
EIGRP		
RIP		
Policy Based Routing		
Y BGP		
IPv4		
IPv6		
Static Route		
Y Multicast Routing		
IGMP	There are no BFD records Add	
PIM		
Multicast Boundary Filter		
General Settings		

Image 3. Section Device Routing.

Étape 4. Sélectionnez le Interface dans lequel le protocole BFD va être configuré, et créez un nouveau modèle en cliquant sur le bouton + s'affiche.

	nt Center Overview Analysis Policies	Devices Objects Integration	Deploy Q 🥏 🌮 🧭 admin 🕶 🔤
SF3130-A Cisco Secure Firewall 3130 Threat Device Routing Interfac			
Manage Virtual Routers	Bidirectional Forwarding Detection	Routing (BFD)	
ECMP BFD	Slow Timer 1000 (1000-30000)	Add BFD Single-Hop	
		BGP 1 Template Name Select + 2	Add
Policy Based Routing V BGP IPv4		Template Name is mandatory. Cancel OK	

Image 4. Sélection d'interface.

Étape 5. Nommez le modèle et configurez les paramètres souhaités pour le BFD, puis cliquez sur le bouton Enregistrer.

Firewall Managemen	it Center Overview Analysis Policies D	evices Objects Integration		Deploy 🔍 🦑 🌣 🎯 admin 🛛 🖓 🕸 SECURE
		uting (BFD) Add BFD Template Object		
		Name* Template Type:		
		Echo: disabled • Interval Authentication		Add 🖉
		Interval Type: None • Multiplier:		
		Minimum Transmit:		
		Minimum Receive:		
BGP			Cancel	

Image 5. Configuration du modèle.

Remarque : la fonction d'écho est uniquement disponible en mode à saut unique.

Étape 6. Choisissez le modèle que vous avez déjà créé à l'étape précédente et cliquez sur ok.

Firewall Management			Deptoy Q 🥩 🗱 🚳 admin • 🔤
SF3130-A Cisco Secure Firewall 3130 Threat Device Routing Interfac			
Manage Virtual Routers Global • Virtual Router Properties	Bidirectional Forwarding Detection Routing (BFD)		
ECMP BFD OSPFv3 EIGRP RIP Policy Based Routing	Stow Timer Edit E 1000 (1000-30000) Interfar Interface BGP Templa	3FD Single-Hop	Add
Policy based routing >> BGP IPv4 IPv6 Static Route		Cancel OK	
 Multicast Routing IGMP PIM Multicast Routes Multicast Boundary Filter 			
General Settings BGP			

Image 6. Sélection du modèle.

Étape 7 (facultatif). Pour le basculement BFD, cliquez sur le bouton IPv4 ou IPv6en fonction de votre configuration de BGP dans la colonne de gauche. Sélectionnez laNeighbor , puis cliquez sur le crayon d'édition à droite pour l'adresse de voisinage souhaitée.

Firewall Managemen	nt Center Overview Analysis	Policies Devices Objects	Integration	De	ploy Q 🧬 🌣 🕜 admin 🕶 🔤 secure
SF3130-A Cisco Secure Firewall 3130 Threat	Defense				You have unsaved changes Save Cancel
Device Routing Interfac	ces Inline Sets DHCP				
Manage Virtual Routers	Enable IPv4: 🗹 AS Number 65000				
Global •					
Virtual Router Properties	General Neighbor 2 Add Aggres	ate Address Hiltering Networks	Redistribution Route Injection		
ECMP					+ Add
BFD					
OSPF	Address	Remote AS Number	Address Family	Remote Private AS Number	Description
OSPFv3	172.16.10.2	65001	Enabled		3 Z i
EIGRP					
RIP					
Policy Based Routing					
✓ BGP					
IPv4					
Static Doute					
V Multicast Pouting					
IGMP					
PIM					
Multicast Routes					
Multicast Boundary Filter					
General Settings					

Image 7. Configuration du voisin.

Étape 8 (facultatif). Sélectionnez l'option Basculement BFD pour single_hop ou multi_hop et cliquez sur ок.

Firewall Management Center Devices / Secure Firewall Routing	verview Analysis Policies Devices	Objects Integration	Deploy Q 🥐 🌣 🎯 admin 🗸 📸 SECURE
SF3130-A			You have unsaved changes Save Cancel
Cisco Secure Firewall 3130 Threat Defense			
Device Routing Interfaces Inline Sets	Edit Neighbor		
Manage Virtual Routers Global AS Number Global Virtual Router Properties ECMP BED BED ECMP BED ECMP E	HP Address* 172.16.10.2 A Remote AS* 65001 (1-4294967295 or 1.0-65535.65533		+ Add
Address	BFD Fallover	Description	Description
OSPFv3 172.16.10.2	single_hop	Trs_ Advanced Migration	/1
EIGRP RiP Policy Based Routing ~ BGP IPv4 IPv6 Static Route ~ Multicast Routing IGMP PIM Multicast Routes Multicast Boundary Filter	multi_hop auto_detect_hop none Route Map Prefix List AS path filter Linit the number of prefixes allow Maximum Prefixes*	Outgoing Access List + Route Map + + • + • + • + • + • + • + • + • + • + • + • + • + • + • + • + • + • + • + •	
General Settings	(1-2147483647)		
BGP	Threshold Level		
		Cance Cance	

Image 8. Configuration du basculement BFD.

Étape 9. Pour enregistrer votre configuration, cliquez sur le bouton save s'affiche.

Firewall Managemen Devices / Secure Firewall Rou	t Center Overview Analysis	Policies Devices Objects Integ	ration		Deploy Q 🇬 🌣 🕢 admin 🕶 🖓 🚓 SEC	URE
SF3130-A Cisco Secure Firewall 3130 Threat D	lefense ve Juliee Sote DM/D V/TED				You have unsaved changes Save C	incel
Manage Virtual Routers	Enable IPv4: AS Number 65000 General Neighbor Add Aggreg	ate Address Filtering Networks Redist	ibution Route Injection			
ECMP BED					+ 2	dd
OSPF	Address	Remote AS Number	Address Family	Remote Private AS Number	Description	
OSPFv3			Enabled		,	1
ExterP RIP Policy Based Routing >> BGP IPv4 IPv6 Static Route >> Multicast Routing IGMP PIM Multicast Routes Multicast Routes Multicast Routes Multicast Boundary Filter General Settings						
BGP						

Image 9. Enregistrez les configurations.

Étape 10. Cliquez sur le bouton Deploy en haut à droite, cliquez sur le bouton checkbox pour le périphérique auquel vous avez appliqué les modifications, puis à nouveau Deploy s'affiche.

Firewall Management Center Overview And Devices / Secure Firewall Routing	alysis Policies Devices Objects Inte	gration	1 Deploy Q	🥏 🌣 🥝 admin 🔹 🖓 🖓
SF3130-A				Advanced Deploy Deploy ncel
Cisco Secure Firewall 3130 Threat Defense			SF3130-A 2	Ready for Deployment
Device Routing Interfaces Inline Sets DHCP VTER				
Manage Virtual Routers AS Number 65000				
General Neighbor Add A	ggregate Address Filtering Networks Redist	ribution Route Injection		
ECMP				
BFD				Da la
OSPF Address	Remote AS Number	Address Family		
OSPFv3 172.16.10.2	65001	Enabled	1 selected 1 pending	2 • 9
EIGRP				
RIP				
Policy Based Routing				
→ BGP				
IPv4				
IPv6				
Static Route				
IGMP				
PIM				
Multicast Routes				
Multicast Boundary Filter				
General Settings				
BGP				

Image 10. Déploiement des modifications.

Vérifier

Vérifiez la configuration BFD et l'état directement sur la session CLI à l'aide des commandes suivantes :

```
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#
SF3130-A#
show bfd summary
                    Session
                                     Up
                                                  Down
Total
                    1
                                      1
                                                  0
SF3130-A#
SF3130-A#
show bfd neighbors
IPv4 Sessions
                                                 LD/RD
                                                               RH/RS
NeighAddr
                                                                            State
                                                                                    Int
172.16.10.2
                                                  1/1
                                                                                    BGP
                                                               Up
                                                                            Up
```

Dépannage

>

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.