Configuration de BFD dans Secure Firewall Threat Defense avec Flex-Config

Table des matières

Introduction Conditions préalables Exigences Composants utilisés Informations générales Configurer Vérifier Dépannage

Introduction

Ce document décrit comment configurer le protocole BFD dans Secure Firewall Management Center exécutant 7.2 et les versions antérieures avec Flex-Config.

Conditions préalables

Protocole BGP (Border Gateway Protocol) configuré dans Cisco Secure Firewall Threat Defense (FTD) avec Cisco Secure Firewall Management Center (FMC).

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

-Protocole BGP -Concepts BFD

Composants utilisés

-Cisco Secure Firewall Management Center exécutant la version 7.2 ou les versions antérieures.

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

Le protocole BFD (Bidirectional Forwarding Detection) est un protocole de détection conçu pour

fournir des temps de détection de défaillance de chemin de transfert rapide pour tous les types de supports, encapsulations, topologies et protocoles de routage.

Configurer

Les configurations BFD dans FMC exécutant les versions 7.2 et antérieures doivent être configurées avec des politiques et des objets Flex-Config.

Étape 1.

Créez le modèle BFD via l'objet Flexconfig.

Le modèle BFD spécifie un ensemble de valeurs d'intervalle BFD. Les valeurs d'intervalle BFD configurées dans le modèle BFD ne sont pas spécifiques à une seule interface. Vous pouvez également configurer l'authentification pour les sessions à saut unique et à saut multiple.

Pour créer l'objet Flex-Config, sélectionnez Objects Tab en haut de la page, cliquez sur FlexConfig dans la colonne de gauche, puis cliquez sur l'option FlexConfig Object, puis cliquez sur Add FlexConfig Object.

CISCO Objects / Object Manager	ement Center Overview Analysis Policies Devices Objects AMP Intelligence	Deploy Q 🧬	🔅 🕜 admin
AAA Server Access List Address Pools Application Filters	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		6/2
Distinguished Name	BFD-SINGLEHOP		6/9
DNS Server Group	BFD_Negate		6/ €
External Attributes	Default_DNS_Configure	Configure Default DNS with the help of TextObjects def	¶∎ Q
✓ FlexConfig 2	Default_Inspection_Protocol_Disable	Disable Default Inspection.	¶a Q
FlexConfig Object	Default_Inspection_Protocol_Enable	Enable Default Inspection.	¶a Q ≣
Text Object	DHCPv6_Prefix_Delegation_Configure	Configure one outside (PD client) and one inside interfa	F a Q
Interface	DHCPv6_Prefix_Delegation_UnConfigure	Remove configuration of one outside (PD client) and on	₽ a Q
Key Chain	DNS_Configure	Configure DNS with the help of TextObjects dnsParame	¶a q ≣
Network	DNS_UnConfigure	Remove the DNS configurations.	Ra Q ≡
Policy List	Elaro. Configure	Configures elarp. 1. Configures next hop. 2. configures	E o E
Port	Fioro Interface. Configure	Configures interface parameters for elloro. 1. Configure	B o E
> Prefix List	Elora LloCastoure	Classe along configuration for an AS	
Route Map Security Intelligence	Enging_circcatages All	Clears clear configuration for an AS	
Sinkhole	Ligrp_Unconfigure_All	Clears eigrp configuration.	B Q
SLA Monitor		Displaying 1 - 20 of 51 rows	of 3 > > C

Étape 2.

Ajoutez les paramètres requis pour le protocole BFD :

Le modèle BFD spécifie un ensemble de valeurs d'intervalle BFD. Les valeurs d'intervalle BFD configurées dans le modèle BFD ne sont pas spécifiques à une seule interface. Vous pouvez également configurer l'authentification pour les sessions à saut unique et à saut multiple.

- single-hop Spécifie un modèle BFD à saut unique.
- multi-hop : spécifie un modèle BFD à sauts multiples.
- template_name Spécifie le nom du modèle. Le nom du modèle ne peut pas contenir d'espaces.
- (Facultatif) Configurez Echo sur un modèle BFD à saut unique.

Remarque : vous ne pouvez activer le mode Écho que sur un modèle à saut unique.

Configurez les intervalles dans le modèle BFD :

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

- both : intervalle minimal de transmission et de réception.
- Intervalle en millisecondes. La vitesse est comprise entre 50 et 999.
- microsecondes : spécifie l'intervalle BFD en microsecondes pour la commande andmin-tx.
- microsecondes : la plage est comprise entre 50 000 et 999 000.
- min-tx : capacité d'intervalle de transmission minimum.

Configurez l'authentification dans le modèle BFD :

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

- authentication : spécifie le type d'authentification.
- md5 : authentification MD5 (Message Digest 5).
- meticulous-md5 Authentification MD5 à clés méticuleuses.
- meticulous-sha-1 Authentification SHA-1 à clés méticuleuses.
- sha-1 : authentification SHA-1 par clé.
- 0|8: 0 indique qu'un mot de passe NON CHIFFRÉ suit. La figure 8 indique qu'un mot de passe ENCRYPTED suit.
- word : mot de passe BFD (clé), qui est un mot de passe/clé à un chiffre comprenant jusqu'à 29 caractères. Les mots de passe commençant par un chiffre suivi d'un espace ne sont pas

pris en charge. Par exemple, 0 passe et 1 ne sont pas valides.

- key-id : ID de la clé d'authentification.
- id : ID de clé partagée correspondant à la chaîne de clé. La plage est comprise entre 0 et 255 caractères.

Edit FlexConfig Object							9
Name: BFD-SINGLEHOP Description:				de de la			
Insert Deployment	: Once	s while generating C	LI. Please	Type:	Append	ment. ▼	
bfd-template single-hop TEMPLATE1 echo interval both 50 authentication sha-1 0 cisco key	-id 10						
Name	Dimension	Default Value	Prop (Type	erty e:Name)	Override	Description	
		No records to	display				
							Save

Étape 3.

Associez le modèle BFD à l'interface.

Edit FlexConfig Object						
Name: BFD-SINGLEHOP Description:						
Copy-pasting any rich text might int Insert Deployment	troduce line break:	s while generating CLI	 Please verify the Type: 	CLI before deploy	ment. ▼	
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 d	isplay			
					Cancel	Save

Remarque : associez le modèle BFD à sauts multiples à une carte de destinations.

Étape 4 (facultatif).

Créez un mappage BFD contenant des destinations que vous pouvez associer à un modèle à sauts multiples. Vous devez avoir déjà configuré un modèle BFD à sauts multiples.

Associez le modèle à sauts multiples BFD à une carte des destinations :

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

- ipv4 : configure une adresse IPv4.
- ipv6 : configure une adresse IPv6.
- destination/cdir Spécifie le préfixe/la longueur de destination. Le format est A.B.C.D/<0-32>.

- source/cdir : spécifie le préfixe/la longueur de destination. Le format est X:X:X;X::X/<0-128>.
- template-name Spécifie le nom du modèle à sauts multiples associé à ce mappage BFD.

Cliquez sur le bouton save pour enregistrer l'objet.

Edit FlexConfig Object									
Name: BFD-MULTIHOP Description:	troduce line break	s while generating CL	I. Please v	verify the	CLI before deployr	nent.			
Insert 🔻 🔣 Deployment	Once		•	Type:	Append	•			
brd-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							
Name	Dimension	Default Value	Prope	rty	Override	Description			
		No recorde to	(Type:	:Name)					
	No records to display								
						Cancel	Save		

Étape 5.

Cliquez sur le bouton Devices en haut de la page, puis sélectionnez FlexConfig de l'assistant.

CISCO Firepower Manage Objects / Object Manager	ement Center Overview Analysis Policies	Devices Objects	AMP Intelligence		Deploy	۹ 🤗	🗘 🕜 admin -
AAA Server Access List Address Pools Application Filters AS Path	FlexConfig Object FlexConfig Object include device configuration commands, Name	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. Filt	ter	
Cipher Suite List Community List	BFD-MULTIHOP	FlexConfig 2 Certificates	Site to Site Monitoring				6/i
> Distinguished Name DNS Server Group	BFD-SINGLEHOP BFD_Negate						6/¥ 6/¥
 External Attributes File List 	Default_DNS_Configure			Configu	re Default DNS with the help of Te	extObjects def	F <u>a</u> Q]]
FlexConfig FlexConfig Object Text Object	Default_Inspection_Protocol_Disable Default_Inspection_Protocol_Enable			Disable Enable I	Default Inspection.		₽∎ Q ₽∎ Q
Geolocation	DHCPv6_Prefix_Delegation_Configure			Configu	re one outside (PD client) and one	e inside interfa	Fa Q ()
Key Chain Network	DNS_Configure			Configu	re DNS with the help of TextObjec	cts dnsParame	¶∎ α ≣
> PKI Policy List	DNS_UnConfigure			Remove	the DNS configurations.	2. configures	PaQ≣ PaQ≣
Port > Prefix List	Eigrp_Interface_Configure			Configu	res interface parameters for eigrp	. 1. Configure	F <u>a</u> Q ⊕
Route Map Security Intelligence	Eigrp_UnConfigure Eigrp_Unconfigure_All			Clears of Clears	elgrp configuration for an AS		EBQ EBQ
Sinkhole SLA Monitor					Displaying 1 - 20 of 51 rows	I< < Page 1	of 3 > > C

Étape 6.

Pour créer une nouvelle stratégie FlexConfig, cliquez sur le bouton New Policy s'affiche.

altalta cisco	Firepower Management Center Devices / FlexConfig	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Depk	, α	6	🕜 admin 🕶
												New Policy

Étape 7.

Name la stratégie et sélectionnez les périphériques affectés à la stratégie. Cliquez sur le bouton Add to Policy puis cliquez sur le bouton saves'affiche.

New Policy				?
Name: BFD] 1			
Description:				
Targeted Devices Select devices to which you want to	apply this policy.			
Available Devices \bigcirc Search by name or value		Selected Devices SF3130-A		Ì
SF3130-А SF3130-В 2	Add to Policy	З SF3130-В		T
			Cancel	Save

Étape 8.

Sélectionnez l'objet FlexConfig dans la colonne de gauche et cliquez sur le bouton > pour ajouter l'objet à la stratégie FlexConfig, puis cliquez sur le bouton s_{ave} s'affiche.

CISCO Devices / Flexconfig Policy Editor Devices / Flexconfig Policy Editor Devices / Plexconfig Policy Editor Devices / Plexconfig Policy Editor	🚰 🌣 🕜 admin •
BFD You have unsaved changes Preview Config Enter Description	Save Cancel
	Policy Assignments (2)
Selected Prepend FlexConfigs	
Available FlexConfig C FlexConfig Object II Name Description	
Viser Defined 2	
° ∎FD-SINGLEHOP	
"E BFD_Negate	
∑ System Defined	
ID Default_DNS_Configure 6	
Default_Inspection_Protocol_Enable Salected Annend ElexConfine Salected Annend ElexConfine	
DHCPv6_Prefx_Delegation_Configure Solutional Approximation and a second approximation and assecond approximation and assecond approximation and approximation	
- JDHCPv6_Prefx_Delegation_UnConfigure II Name Description	
¹² DNS_Configure 1 BFD-MULTIHOP	۹ 🖥
UNS_UnConfigure	
"E lign_Configure	
¹ Eigrp_Interface_Configure	
" Eigrp_UnConfigure	
." Eigrp_Unconfigure_All	
°i Inspect_IPv€_Configure	
- Inspect_IPv6_UnConfigure	

Étape 9.

Cliquez sur le bouton Devices dans la partie supérieure, puis cliquez sur l'onglet Device Management de l'assistant.

Firepower Management Center Devices / Flexconfig Policy Editor	Overv	/iew A	nalysis	Policies	Devices	Objects	AMP	Intelligence			Deploy	¢	🕑 admin -
BFD Enter Description Available FlexConfig C FlexConfig Object Vuser Defined	"i Sel	lected Prep Name	pend Flex(Configs	Device Device NAT QoS Platforr FlexCo Certific	Management Upgrade m Settings unfig cates	2	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		Save Policy As	Cancel signments (2)
IPED-MULTHEEP IPED-SINGLEHOP IPED-SINGLEHOP IPED-Negate System Defined IPED-Befault_INSS_Configure IPEdault_Inspection_Protocol_Disable IPED-Bable IPED-Bable IPED-Bable	_ Sel	ected App	end Flex0	Confias									
DHCPv6_Prefix_Delegation_UnConfigure		Name			D	escription							
") DNS_Configure DNS_UnConfigure ") Eigrp_Configure ") Eigrp_Interface_Configure Eigrp_Interface_Configure	1	BFD-MULTI	нор										۵∎
. Eigr_Unconfigure_All Inspect_IPv6_Configure Inspect_IPv6_UnConfigure													

Étape 10.

Sélectionnez le périphérique auquel la configuration BFD sera attribuée.

ahaha cisco	Firepower Management Center Overview Analy Devices / Device Management	sis Policies Devices	Objects A	MP Intelligence		Deploy Q 🌮 🌣 🍘	admin 🔻
View Ry:	Group 👻					Deployment	t History
All (2)	Error (2) Warning (0) Offline (0) Normal (0)	 Deployment Pending (2) 	 Upgrade (0) 	 Snort 3 (2) 		Q. Search Device	Add 🔻
Collapse /							
	ame	Model	Version	Chassis	Licenses	Access Control Policy	
• •	Ungrouped (2)						
	SF3130-A Snort 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:

Étape 11.

Cliquez sur le bouton Routing, puis cliquez sur l'ongletIPv4 ou IPv6, selon votre configuration dans la section BGP sur la colonne de gauche, puis cliquez sur le bouton Neighbor, puis cliquez sur le bouton modifier le crayon pour le modifier.

CISCO Firepower Manage Devices / NGFW Routing	ement Center _{Overview} Analy	sis Policies Devices Objec	cts AMP Intelligence		Deploy	역 🥐 🔅 🕜 admin 🕶
SF3130-A Cisco Secure Firewall 3130 Threat I Device Routing 1 Interfac	Defense res Inline Sets DHCP					Cancel
Manage Virtual Routers Global	Enable IPv4: 🗹 AS Number 65000 General Neighbor 3 Add Aggre	ate Address Filtering Networks	Redistribution Route Injection			
ECMP OSPF						+ Add
OSPFv3 RIP	Address 172.16.10.2	Remote AS Number	Address Family Enabled	Remote Private AS Number	Description	471
Policy Based Routing						
IPV4 2 IPv6 Static Doute						
Static Route ~ Multicast Routing IGMP PIM Multicast Routes Multicast Boundary Filter						

Étape 12.

Sélectionnez le checkbox pour le basculement BFD et cliquez sur le bouton ok s'affiche.

Edit Neighbor		
IP Address* 172.16.10.2 Remote AS* 65001 (1-4294967295 or 1.0-65535.65535) Description	 Enabled address Shutdown administratively Configure graceful restart Graceful restart(failover/spanned mode) ØFD Fallover 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 Time	rs Advanced Migration	
Incoming Access List Route Map	Outgoing Access List + + Route Map	
▼ Prefix List	+ + Prefix List + +	
AS path filter	AS path filter + + +	
(1-2147483647)		

Étape 13.

Cliquez sur le bouton Deploy, puis cliquez sur le bouton Deployment s'affiche.

ahaha cisco	Firepower Ma Devices / Device M	inagement Ce	nter _{Overvie}	w Analysis	Policies	Devices	Objects	AMP	Intelligence	1 Deploy Q 🥮 🕻	ŧ 🕜 admin ▼
View By: All (2)	Group Error (2)	• Warning (0)	 Offline (0) 	 Normal (0) 	Deployment	t Pending (2)	Upgrade	(0) •	Snort 3 (2)	2 Deployment Deployment History	hent History

Étape 14.

Sélectionnez le périphérique auquel les modifications vont être attribuées en cliquant sur le bouton checkbox, puis cliquez sur le boutonDeploy s'affiche.

oliol cisco	•	Firepower Management Center Deploy / Deployment	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence			Deploy Q 🌮🌣	😗 admin 🕶
T	۹	Search using device name, user name, type,	group or status									2	Deploy
		Device		Modified by		Inspect In	terruption	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	
> >		SF3130-B SF3130-A		admin admin				FTD FTD		Jul 18, 2023 4:55 PM Jul 18, 2023 4:55 PM	6.	Ready for Deployment Ready for Deployment	

Étape 15.

Cliquez sur le bouton Deploy s'affiche.

Deployment Confirmation

You have selected 1 device to deploy

Deployment Notes:

You can optionally add notes about the configuration changes

Étape 16.

Cliquez sur le bouton Deploy s'affiche.

Validation Messages: SF3130-B		×
1 total 0 errors 1 warning 0 info PG.TEMPLATE.TemplatePolicy: BFD		
> Warning: FlexConfig policies intentionally do not contain extensive input validation. Please ensure that the configurations in this FlexConfig	policy are	correct. In
	Close	Deploy

Deploy

Cancel

Remarque : l'avertissement est attendu et n'a qu'un caractère informatif.

Vérifier

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

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