使用Flex-Config在安全防火牆威脅防禦中配置 BFD

目錄

簡介

本文說明如何使用Flex-Config在運行7.2及更低版本的安全防火牆管理中心中配置BFD協定。

必要條件

在思科安全防火牆威脅防禦(FTD)中設定與思科安全防火牆管理中心(FMC)的邊界閘道通訊協定 (BGP)。

需求

思科建議您瞭解以下主題:

-BGP協定

-BFD概念

採用元件

— 運行7.2或更低版本的思科安全防火牆管理中心。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

雙向轉發檢測(BFD)是一種檢測協議,旨在為所有媒體型別、封裝、拓撲和路由協定提供快速轉發 路徑故障檢測時間。

設定

運行7.2及更低版本的FMC中的BFD配置必須使用Flex-Config策略和對象進行配置。

步驟 1.

通過Flexconfig對象建立BFD模板。

BFD模板指定一組BFD間隔值。在BFD模板中配置的BFD間隔值並非特定於單個介面。您還可以為 單跳和多跳會話配置身份驗證。

要建立Flex-Config對象,請選擇 Objects Tab 在頂部,按一下 FlexConfig 選項,然後按一下 FlexConfig Object 選項,然後按一下 Add FlexConfig Object.

Firepower Manag Objects / Object Manage	ement Center Overview Analysis Policies Devices Objects 1 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 Cipher Suite List > Community List > Distinguished Name	Name BFD-MULTIHOP BFD-SINGLEHOP	Description	9/7 9/7
DNS Server Group > External Attributes File List	BFD_Negate Default_DNS_Configure Default_Instanction_Protocol_Disable	Configure Default DNS with the help of TextObjects def	Ra ≠ 1 Ra Q 11 Ra Q 11
FlexConfig Object	Default_Inspection_Protocol_Contouro DHCPv6_Prefix_Delegation_Configure	Enable Default Inspection. Configure one outside (PD client) and one inside interfa	∎ < ∎ < ₽∎ <
Interface Key Chain Network	DHCPv6_Prefix_Delegation_UnConfigure DNS_Configure ONS_UnConfigure	Remove configuration of one outside (PD client) and on Configure DNS with the help of TextObjects dnsParame Remove the DNS configurations.	¶∎ Q = ¶∎ Q = ¶∎ Q =
Policy List Port > Prefix List	Eigrp_Configure Eigrp_Interface_Configure	Configures eigrp. 1. Configures next hop. 2. configures Configures interface parameters for eigrp. 1. Configure	¶_Q]] ¶_Q]]
Route Map > Security Intelligence Sinkhole SLA Monitor	Eigrp_Unconfigure_All	Clears eigrp configuration for an AS Clears eigrp configuration. Displaying 1 - 20 of 51 rows I< < Page 1	ng Q ■ Q ■ or 3 > > C

步驟 2.

新增BFD協定所需的引數:

BFD模板指定一組BFD間隔值。在BFD模板中配置的BFD間隔值並非特定於單個介面。您還可以為 單跳和多跳會話配置身份驗證。

bfd-template [single-hop | multi-hop] template_name

- single-hop 指定單跳BFD模板。
- multi-hop 指定多跳BFD模板。
- template_name 指定模板名稱。模板名稱不能包含空格。

• (可選)在單跳BFD模板上配置Echo。

注意:您只能在單跳模板上啟用回聲模式。

配置BFD模板中的時間間隔:

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

- both 最小傳輸和接收間隔功能。
- 間隔(以毫秒為單位)。範圍為50到999。
- microseconds 指定min-tx的BFD間隔(微秒)。
- 微秒 範圍為50,000到999,000。
- min-tx 最小傳輸間隔功能。

在BFD模板中配置身份驗證:

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

- authentication 指定身份驗證型別。
- md5 消息摘要5(MD5)身份驗證。
- 小心翼翼 md5 小心翼翼的MD5身份驗證。
- 小心謹慎的sha-1 小心謹慎的SHA-1身份驗證。
- sha-1 加密SHA-1身份驗證。
- 0|8-0指定後跟未加密密碼。8指定ENCRYPTED密碼後跟隨。
- word BFD密碼(金鑰),最多包含29個字元的單位密碼/金鑰。不支援以數字開頭、後跟空白的密碼,例如0pass和1無效。
- key-id 身份驗證金鑰ID。
- id 與金鑰字串匹配的共用金鑰ID。範圍為0到255個字元。

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

步驟 3.

將BFD模板與介面關聯。

Edit FlexConfig Object							
Name: BFD-SINGLEHOP Description:							
Copy-pasting any rich text might int	roduce 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	Prope (Type	erty e:Name)	Override	Description	
		No records to d	isplay				
						Cancel	Save

注意:將BFD多跳模板與目標對映關聯。

第4步(可選)。

建立一個BFD對映,該對映包含您可以與多跳模板關聯的目標。您必須已配置多跳BFD模板。

將BFD多跳模板與目標對映關聯:

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

- ipv4 配置IPv4地址。
- ipv6 配置IPv6地址。
- destination/cdir 指定目標字首/長度。格式為A.B.C.D/<0-32>。
- source/cdir 指定目標字首/長度。格式為X:X:X;X::X/<0-128>。

• template-name — 指定與此BFD對映關聯的多跳模板的名稱。

按一下 Save 按鈕儲存對象。

Edit FlexConfig Object						
Name: BFD-MULTIHOP Description:	troduce line break	s while generating CI	I Please verify the	CI I before deployr	nent	
Insert Deployment:	: Once		Type:	Append	▼	
bfd-template multi-hop MULTI-TEMP interval both 50	LATE1					
bfd map ipv4 10.11.11.0/24 10.36.	42.5/32 MULTI-1	EMPLATE1				
Name	Dimension	Default Value	Property (Type:Name)	Override	Description	
		No records to	display			
					Cancel	Save

步驟 5.

按一下 Devices 頁籤,然後選擇 FlexConfig 選項。

Cisco Firepower Manage	ement Center Overview Analysis Policies	Devices 1 Objects	AMP Intelligence		Deploy Q 🤞	😕 🌣 🚱 admin 🕶
AAA Server Access List Address Pools Application Filters	FlexConfig Object FlexConfig Object include device configuration command:	Device Management Device Upgrade 8, V NAT QoS Bistform Sattinger	VPN Site To Site Remote Access Dynamic Access Policy Towitechastics	Troubleshoot File Download Threat Defense CLI Packet Tracer	FlexConfig Object Q. Filter	
AS Path	Name	FlexConfig 2	Site to Site Monitoring	Packet Gapture	on	
Cipher Suite List	BFD-MULTIHOP	Certificates				6/T
Distinguished Name	BFD-SINGLEHOP					B/₹
DNS Server Group	BFD_Negate					6/9
External Attributes Eite List	Default_DNS_Configure			Confi	gure Default DNS with the help of TextObjects def	Baq≣
 ✓ FlexConfig 	Default_Inspection_Protocol_Disable			Disab	le Default Inspection.	₽ 4 Q =
FlexConfig Object	Default_Inspection_Protocol_Enable			Enabl	e Default Inspection.	Ea Q ;;;
Text Object	DHCPv6_Prefix_Delegation_Configure			Config	gure one outside (PD client) and one inside interfa	B iq ∰
Interface	DHCPv6_Prefix_Delegation_UnConfigure			Remo	ve configuration of one outside (PD client) and on	B Q
Key Chain	DNS_Configure			Config	gure DNS with the help of TextObjects dnsParame	16 q ≣
Network	DNS_UnConfigure			Remo	ve the DNS configurations.	En Q ⊒
Policy List	Eigrp_Configure			Config	gures eigrp. 1. Configures next hop. 2. configures	Paq
Port	Eigrp_Interface_Configure			Confi	gures interface parameters for eigrp. 1. Configure	Bac.⊒
> Prefix List	Elaro, UnConfigure			Clear	s eloro configuration for an AS	B o P
Security Intelligence	Einn Linconfigure All			Ciear	s elern configuration	B O D
Sinkhole	all p_oneomyone_ver			Clean	- and provided and the second s	
SLA Monitor					Displaying 1 - 20 of 51 rows 1 < Page	

步驟 6.

要建立新的FlexConfig策略,請按一下 New Policy 按鈕。

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

步驟 7.

Name 並選擇分配給策略的裝置。按一下 Add to Policy 然後按一下 Save按鈕。

New Policy				8	
Name: BFD] 1				
Description:					
Targeted Devices	apply this policy				
	apply this policy.	Selected Devices			
Q Search by name or value		SF3130-A			
SF3130-A SF3130-B	Add to Policy	З SF3130-В			
			Cancel	Save	

步驟 8.

選擇左列上的FlexConfig對象,然後按一下 > 按鈕將該對象新增到FlexConfig策略,然後按一下 save 按鈕。

Firepower Management Center Devices / Flexconfig Policy Editor	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy Q 🌮 🔅	🕜 admin 🕇
BFD Enter Description								You have unsaved changes Preview Config	e Cancel
									Assignments (2)
	" Selected	d Prepend Fle	exConfigs						
Available FlexConfig C FlexConfig Object	II Nam	•		De	escription				
V User Defined	2								
BFD-MULTIHOP									
BFD-SINGLEHOP									
BFD_Negate									
✓ System Defined									
" Default_DNS_Configure									
.9 Default_Inspection_Protocol_Disable									
Carter Content Protocol_Enable									
BHCPv6_Prefix_Delegation_Configure	! Selected	d Append Fle	xConfigs						
DHCPv6_Prefix_Delegation_UnConfigure	# Nam	e		De	escription				
"i DNS_Configure	1 BFD-	MULTIHOP							Q T
DNS_UnConfigure									
"i Eigrp_Configure									
" Eigrp_Interface_Configure									
Eigrp_UnConfigure									
Eigrp_Unconfigure_All									
"Inspect_IPv6_Configure									
.9 Inspect_IPv6_UnConfigure									

步驟 9.

按一下 Devices 頁籤,然後按一下 Device Management 選項。

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 Vuser Defined C BFD-MULTIHOP C BFD-SINGLEHOP C BFD_Negate System Defined C Defaut, DNS_Configure	Selected Prepend FlexConfigs Name Name	Device Management 2 Device Uprade 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 Sav Policy A	e Cancel
? Default_Inspection_Protocol_Disable "ii Default_Inspection_Protocol_Enable	Colored Accord FlavOcafee					
* DHCPv6_Prefx_Delegation_Configure DHCPv6_Prefx_Delegation_UnConfigure DNS_Configure	Selected Append FlexConfigs # Name	Description				
ONS_Configure ONS_UnConfigure Eigrp_Configure Eigrp_Interface_Configure Eigrp_UnConfigure Eigrp_UnConfigure Ispect_IPv6_Configure Inspect_IPv6_UnConfigure	1 BFD-MULTIHOP					٩ 🖬

步驟 10.

選擇要分配BFD配置的裝置。

-ihoho cisco	Firepower Management Center Overview Analys	is Policies Devices	Objects A	MP Intelligence		Deploy Q 🌮🌣 🕻	🔋 admin 🔻
View By	r: Group 🔻					Deploymer	nt History
All (: Collapse	Error (2) Warning (0) Offline (0) Normal (0)	 Deployment Pending (2) 	Upgrade (0)	Snort 3 (2)		Q Search Device	Add 🔻
	Name	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
	\$F3130-B Snort 3 10.88.146.205 - Routed	Firewall 3130 Threat Defense	7.1.0	Manage	Base, Threat (2 more)	Default	1:

步驟 11.

按一下 Routing 頁籤,然後按一下IPv4 或 IPv6, 根據您在左列的BGP部分中的配置,然後按一下 Neighbor 頁籤,然後按一下「編輯鉛筆」按鈕進行編輯。

Firepower Manage Devices / NGFW Routing	ment Center _{Overview} Analy	sis Policies Devices Obje	cts AMP Intelligence		Deploy	오, 🇬 🌣 🕜 admin 🔻
SF3130-A Cisco Secure Firewall 3130 Threat I Device Routing 1 Interfac	Defense es Inline Sets DHCP					Save Cancel
Manage Virtual Routers	Enable IPv4: 🗹 AS Number 65000 General Neighbor 3 Add Aggreg	ate 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						
∼ BGP						
IPv4 2						
IPv6						
Static Route						
Multicast Routing						
IGMP						
PIM Multicast Poutes						
Multicast Boundary Filter						

步驟 12.

選擇 checkbox 對於BFD故障,按一下 OK 按鈕。

Edit Neighbor			6
IP Address* 172.16.10.2 Remote AS* 65001 (1-4294967295 or 1.0-65535.65535) Description		Enabled addre Shutdown adm Configure grac Graceful restar BFD Fallover	ress Iministratively aceful 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 flow config
Filtering Routes Routes T	imers	Advanced	Migration
Incoming Access List Route Map Prefix List AS path filter	- + - + - +	Outgoing Access List Route Map Prefix List AS path filter	• + • + • +
AS pair little	wed from	m the neighbor	• + r
			Сапсе

步驟 13.

按一下 Deploy 按鈕,然後按一下 Deployment 按鈕。

ahaha cisco	Firepower Ma Devices / Device M	anagement Ce lanagement	nter _{Over}	view Analysis	s Policies	Devices	Objects	AMP	Intelligence	1 Deploy Q 🧬	🔅 🕜 admin 🔻
View By:	Group		•							2 Deployment Deployment History	hent History
All (2	Error (2)	Warning (0)	• Offline (0)	Normal (0)	Deploymen	t Pending (2)	Upgrade	(0)	Snort 3 (2)	Copicyment matery	Add 🔻

步驟 14.

通過按一下 checkbox,然後按一下Deploy 按鈕。

cisco Deploy / De	ployment	Overview An	alysis Pol	licies Device	s Objects	AMP	Intelligence		_	Deploy Q 🍄 🌣	😗 admin 🕶
🝸 🍳 Search u	ing device name, user name, type, ;	group or status								2	Deploy
Device		Mod	dified by	Insp	ect Interruption	Type	Group	Last Deploy Time	Preview	Status	
> 🗌 SF3130	в	adn	nin			FTD		Jul 18, 2023 4:55 PM	B.	Ready for Deployment	
> _ SF3130	-A	adn	nin			FTD		Jul 18, 2023 4:55 PM		Ready for Deployment	

步驟 15.

按一下 Deploy 按鈕。

Deployment Confirmation

You have selected 1 device to deploy

Deployment Notes:

You can optionally add notes about the configuration changes

步驟 16.

按一下 Deploy 按鈕。

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	e Deploy

Х

Deploy

Cancel

驗證

使用下一命令直接在CLI會話中驗證BFD配置和狀態。

<#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						
NeighAddr			LD/RD	RH/RS	State	Int
172.16.10.2			1/1	Up		

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。