使用Flex-Config在安全防火墙威胁防御中配置 BFD

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> <u>使用的组件</u> <u>背景信息</u> 配<u></u> 验 证 故障排除

简介

本文档介绍如何使用Flex-Config在运行7.2及更低版本的安全防火墙管理中心中配置BFD协议。

先决条件

在思科安全防火墙威胁防御(FTD)中配置的边界网关协议(BGP)与思科安全防火墙管理中心(FMC)。

要求

Cisco 建议您了解以下主题:

-BGP协议

-BFD概念

使用的组件

— 运行7.2或更低版本的思科安全防火墙管理中心。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

背景信息

双向转发检测(BFD)是一种检测协议,旨在为所有媒体类型、封装、拓扑和路由协议提供快速转发 路径故障检测时间。 运行7.2及更低版本的FMC中的BFD配置必须使用Flex-Config策略和对象进行配置。

步骤1:

通过Flexconfig对象创建BFD模板。

BFD模板指定一组BFD间隔值。在BFD模板中配置的BFD间隔值并非特定于单个接口。您还可以配置单跳和多跳会话的身份验证。

要创建Flex-Config对象,请选择 Objects Tab 在顶部,单击 FlexConfig 选项,然后单击 FlexConfig Object 选项,然后单击 Add FlexConfig Object.

CISCO Firepower Manage Objects / Object Manage	ement Center Overview Analysis Policies Devices Objects 1 AMP Intelligence	Deploy Q 🌮 🕻	ዩ 😗 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		6/0
> Distinguished Name	BFD-SINGLEHOP		9 / P
DNS Server Group	BFD_Nogate		6/ €
External Attributes File List	Default_DNS_Configure	Configure Default DNS with the help of TextObjects def	¶a 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 Geolocation	DHCPv6_Prefix_Delegation_Configure	Configure one outside (PD client) and one inside interfa	₽ _0 ⊂ ;;
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	E Q ≣
Network	DNS_UnConfigure	Remove the DNS configurations.	¶a q ≣
Policy List	Eigrp_Configure	Configures eigrp. 1. Configures next hop, 2. configures	¶a q ≣
Port	Eigrp_Interface_Configure	Configures interface parameters for eigrp. 1. Configure	¶a Q ≣
Prefix List Route Map	Eigrp_UnConfigure	Clears eigrp configuration for an AS	₽ Q =
> Security Intelligence	Eigrp_Unconfigure_All	Clears eigrp configuration.	E Q ⊒
Sinkhole SLA Monitor		Displaying 1 - 20 of 51 rows K 4 Page	of 3 > > C

第二步:

添加BFD协议所需的参数:

BFD模板指定一组BFD间隔值。在BFD模板中配置的BFD间隔值并非特定于单个接口。您还可以配置单跳和多跳会话的身份验证。

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

- single-hop 指定单跳BFD模板。
- multi-hop 指定多跳BFD模板。
- template_name 指定模板名称。模板名称不能包含空格。

• (可选)在单跳BFD模板上配置回声。

注意:您只能在单跳模板上启用回声模式。

在BFD模板中配置时间间隔:

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

- both 最小传输和接收间隔功能。
- 间隔(以毫秒为单位)。范围是 50 到 999。
- microseconds 指定min-tx的BFD间隔(单位为微秒)。
- microseconds 范围为50,000到999,000。
- min-tx 最小传输间隔功能。

在BFD模板中配置身份验证:

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

- authentication 指定身份验证类型。
- md5 -消息摘要5(MD5)身份验证。
- 小心谨慎的MD5 小心加密的MD5身份验证。
- 谨慎的SHA-1 谨慎的SHA-1密钥身份验证。
- sha-1 加密SHA-1身份验证。
- 0|8 0指定后面跟有未加密的密码。8指定后面跟有ENCRYPTED密码。
- word BFD密码(密钥),是一个最多包含29个字符的单位数密码/密钥。不支持以数字开头 、后跟空格的密码,例如0pass和1无效。
- key-id 身份验证密钥ID。
- id 与密钥字符串匹配的共享密钥ID。范围为0到255个字符。

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

第三步:

将BFD模板与接口关联。

Edit FlexConfig Object						
Name: BFD-SINGLEHOP Description:	roduce line break	s while generating CLI	. Please verify the	CLI before deployr	nent.	
Insert	Once		▼ Type:	Append	•	
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

注:将BFD多跳模板与目标映射关联。

第4步(可选):

创建包含可与多跳模板关联的目标的BFD映射。您必须已配置多跳BFD模板。

将BFD多跳模板与目标映射关联:

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

- ipv4 配置IPv4地址。
- ipv6 配置IPv6地址。
- destination/cdir 指定目标前缀/长度。格式为A.B.C.D/<0-32>。
- source/cdir 指定目标前缀/长度。格式为X:X:X;X::X/<0-128>。

• template-name — 指定与此BFD映射关联的多跳模板的名称。

单击 Save 按钮以保存对象。

Edit FlexConfig Object								
Name: BFD-MULTIHOP Description:								
Copy-pasting any rich text might in	troduce line break	s while generating C	LI. Please verify the	CLI before deployr Append	nent. ▼			
bfd-template multi-hop MULTI-TEMPLATE1 interval both 50								
bfd map ipv4 10.11.11.0/24 10.36.	42.5/32 MULTI-1	EMPLATE1						
▼ Variables	Dimension	Dofault Value	Property	Override	Description			
	Dimension	No records to	(Type:Name)	Overnue	Description			
			uopray					
					Cancel	Save		

第五步:

单击 Devices 选项卡,然后选择 FlexConfig 选项.

CISCO Firepower 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 command	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	Name	FlexConfig 2	Site to Site Monitoring		on	
Community List	BFD-MULTIHOP	Certificates				9/i
> Distinguished Name	BFD-SINGLEHOP					6/9
DNS Server Group	BFD_Negate					6/7
> External Attributes	Default_DNS_Configure			Config	ure Default DNS with the help of TextObjects def.	. Baq
File List ✓ FlexConfig	Default_Inspection_Protocol_Disable			Disabl	e Default Inspection.	En Q ⊒
FlexConfig Object	Default_Inspection_Protocol_Enable			Enable	Default Inspection.	E o =
Text Object	DHCPv6 Prefix Delegation Configure			Config	ure one outside (PD client) and one inside interfa	B.O.E
Geolocation	DROBLE Brafer Delegation LisConfigure			Domo	and one densitie (o one ny dire one market metric	
Key Chain	Drice vo_Prenz_belegation_onconligure			Remov	e configuration of one outside (PD client) and on.	
Network	DNS_Configure			Config	ure DNS with the help of TextObjects dnsParame	. 1 3 Q ∰
> ркі	DNS_UnConfigure			Remov	ve the DNS configurations.	¶a Q ()
Policy List	Eigrp_Configure			Config	ures eigrp. 1. Configures next hop. 2. configures	P aq ⊒
Port	Eigrp_Interface_Configure			Config	ures interface parameters for eigrp. 1. Configure.	. P <u>a</u> q <u>⊒</u>
Route Map	Eigrp_UnConfigure			Clears	eigrp configuration for an AS	Pa Q ⊕
> Security Intelligence	Elgrp_Unconfigure_All			Clears	eigrp configuration.	R <u>a</u> Q ⊕
Sinkhole					Displaying 1 - 00 of 51 mms 1/ / Dans 1	
SLA Monitor					Displaying 1 = 20 or 51 rows 1 \ Page 1	0137710

第六步:

要创建新的FlexConfig策略,请点击 New Policy 按钮。

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

步骤 7.

Name 策略并选择分配给该策略的设备。单击 Add to Policy 然后单击 Save按钮。

New Policy				?
Name: BFD] 1			
Description:				
Targeted Devices	apply this policy			
Available Devices	apply the policy.	Selected Devices		
Q Search by name or value		SF3130-A		Ì
SF3130-A SF3130-B	Add to Policy	<mark>З</mark> SF3130-В		
			Cancel 4	Save

选择左列中的FlexConfig对象,然后单击 > 按钮将该对象添加到FlexConfig策略,然后单击 save 按 钮。

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	Cancel
								Policy A	ssignments (2)
	" Selected	Prepend Fle	xConfigs						
Available FlexConfig C FlexConfig Object									
×	# Name	8		U	escription				
V User Defined	2								
BFD-SINGLEHOP									
" BFD_Negate									
✓ System Defined									
¹³ Default_DNS_Configure									
Default_Inspection_Protocol_Disable									
Content Protocol_Enable									
The DHCPv6_Prefix_Delegation_Configure		Append Flee	«Configs						
DHCPv6_Prefix_Delegation_UnConfigure	# Name	b		D	escription				
" DNS_Configure	1 BFD-I	MULTIHOP							٩٦
DNS_UnConfigure									
Bigrp_Configure									
"i Eigrp_Interface_Configure									
Eigrp_UnConfigure									
Eigrp_Unconfigure_All									
inspect_IPv6_Configure									
-7 Inspect_IPv6_UnConfigure									

单击 Devices 选项卡,然后点击 Device Management 选项.

CISCO Firepower Management Center Devices / Flexconfig Policy Editor	Overview Analysis Policies	Devices Objects AM	P Intelligence		Deploy Q 🌮 🌣	🕐 admin v
BFD Enter Description Available FlexConfig C FlexConfig Object Viser Defined BFD-SINGLEHOP BFD_SINGLEHOP BFD_Negate System Defined Defaut_DNS_Configure	*≧ Selected Prepend FlexConfigs	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 A) Cancel
Default_Inspection_Protocol_Disable Default_Inspection_Protocol_Enable Default_Inspection_Protocol_Enable DHCPv6_Prefix_Delegation_Configure						
.9 DHCPv6_Prefix_Delegation_UnConfigure TDNS_Configure	# Name 1 BFD-MULTIHOP	Description				٩.
"I NNS_LinConfigure "I Eigrp_Configure "I Eigrp_Interface_Configure "Eigrp_Unconfigure "Eigrp_Unconfigure_All "I Inspect_IPv6_Configure "Inspect_IPv6_Configure						

步骤 10

选择要分配BFD配置的设备。

-ihoho cisco	Firepower Management Center Overview Analys	is Policies Devices	Objects A	MP Intelligence		Deploy Q 🤗 🥵	admin 🔻
View By	: Group 🔻					Deploymen	t History
All (e Error (2) • Warning (0) • Offline (0) • Normal (0)	Deployment Pending (2)	 Upgrade (0) 	Snort 3 (2)		Q Search Device	Add 🔻
Collapse							
	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
	SF3130-B Snort 3 10.88.146.205 - Routed	Firewall 3130 Threat Defense	7.1.0	Manage	Base, Threat (2 more)	Default	1

单击 Routing 选项卡,然后单击IPv4 或 IPv6, 根据您在左列的BGP部分中的配置,然后单击 Neighbor 选 项卡,然后单击"编辑铅笔"按钮进行编辑。

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 Defense Device Routing 1 Interfaces Inline Sets DHCP										
Manage Virtual Routers	Enable IPv4: 🗹 AS Number 65000 General Neighbor 3 Add Aggreg	jate Address Filtering Networks	Redistribution Route Injection							
ECMP OSPE						+ Add				
OSPFv3	Address	Remote AS Number	Address Family	Remote Private AS Number	Description					
RIP	172.16.10.2	65001	Enabled			4 Z i				
Policy Based Routing										
∼ BGP										
IPv4 2										
IPv6										
Static Route										
✓ Multicast Routing										
IGMP										
PIM										
Multicast Routes										
Multicast Boundary Filter										

步骤 12

选择 checkbox 对于BFD故障,请单击 OK 按钮。

Edit Neighbor		0
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) BFD Fallover Configuring BFD support for BGP for multi-hop, ensure that the BFD map is already created for the BFD map is already created for Configuring BFD support for BGP for multi-hop, ensure that the BFD map is already created for 	
Filtering Routes Routes Timer	s Advanced Migration	_
Incoming Access List	Outgoing Access List	
Route Map	Route Map	
Prefix List	Prefix List	
AS path filter	AS path filter	
Limit the number of prefixes allowed Maximum Prefixes*	from the neighbor	
(1-2147483647)		K

单击 Deploy 按钮,然后单击 Deployment 按钮。

alialia cisco	Firepower Ma Devices / Device M	inagement Ce anagement	nter _{Overv}	iew Analysis	Policies	Devices	Objects	AMP	Intelligence		🗧 🕜 admin 🕶
View By: All (2	Group Group	• Warning (0)	▼ ● Offline (0)	Normal (0)	Deployment	t Pending (2)	Upgrade		 Snort 3 (2) 	2 Deployment Deployment History	hent History

步骤 14

通过点击 checkbox,然后单击Deploy 按钮。

cise	•	Firepower Management Center Deploy / Deployment	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence			Deploy Q 鎁🌣	🕐 admin 🕶
	٩	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	

步骤 15

单击 Deploy 按钮。

Deployment Confirmation

You have selected 1 device to deploy

Deployment Notes:

You can optionally add notes about the configuration changes

步骤 16

单击 Deploy 按钮。

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

注意:警告是预期的,只是提供信息。

验证

使用下一命令直接在CLI会话中验证BFD配置和状态。

<#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		

故障排除

目前没有针对此配置的故障排除信息。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。