使用FDM設定FTD高可用性

目錄

 簡介

 必要條件

 憲求

 援用元件

 網路拓撲

 設定

 配置主裝置以實現高可用性

 配置輔助裝置以實現高可用性

 驗證

簡介

本檔案介紹如何設定在本機管理的「安全防火牆威脅防禦(FTD)」的作用中/待命高可用性(HA)配對。

必要條件

需求

建議您瞭解以下主題:

• 透過GUI和/或外殼進行思科安全防火牆威脅防禦初始配置。

採用元件

本文中的資訊係根據以下軟體和硬體版本:

• FPR2110 7.2.5版由Firepower裝置管理器(FDM)本地管理

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。

網路拓撲



注意:本文檔中介紹的示例是推薦的多種網路設計之一。有關更多選項,請參閱<u>避免中斷</u> <u>的故障切換和資料鏈路</u>配置指南。



設定

配置主裝置以實現高可用性

步驟 1.按一下Device,並按位於右上角的Configure按鈕,旁邊是High Availability狀態。



步驟 2.在「高可用性」頁上,按一下主要裝置框。

Firewall De	vice Manager	Monitoring	Ø Policies	iiii Objects	Device: ftd-primar	<u>v</u>	(Σ)		۲	?	:	admin Administrator	Ÿ	cisco SECURE
	Device Summary High Availa	bility												
	How High Ava	ilability Works											~	
		The prima	ary device is th The sec	e unit that you condary device	Select the role intend should be active remains in standby mo	e for this de re under normal circ ode until the primar or Seconda	VİCƏ umstance y unit beco ry Device	s. Config omes un	gure the available	primary (init first.			

步驟 3.配置故障切換鏈路屬性。

選擇您已直接連線到輔助防火牆的介面,並設定主IP地址和輔助IP地址以及子網網路掩碼。

對於有狀態故障切換鏈路,請選中使用與故障切換鏈路相同的介面覈取方塊。

清除「IPSec加密金鑰」框並按一下Activate HA以儲存更改。

I have configuration of peer device in clipboard PASTE FROM CLIPBOARD	
FAILOVER LINK	STATEFUL FAILOVER LINK Use the same interface as the Failover Link
Interface	Interface
unnamed (Ethernet1/7) V	unnamed (Ethernet1/7) ~
Type IPv4 IPv6 Primary IP 10.1.1.1	Type IPv4 IPv6 Primary IP 10.1.1.1
e.g. 192.168.10.1	e.g. 192.168.11.1
Secondary IP 10.1.1.2 e.g. 192.168.10.2	Secondary IP 10.1.1.2 e.g. 192.168.11.2
Netmask	Netmask
255.255.255.252	255.255.255.252
e.g. 255.255.255.0 or 24	e.g. 255.255.255.0 or 24
IPSec Encryption Key (optional) For security purposes, the encryption key will not be included in the configuration copied to the clipboard when you activate HA. You will need to manually enter the key when you configure HA on the peer device.	IMPORTANT If you configure an IPsec encryption key with inconsistent settings for export controlled features, both devices will become active after you activate HA. Learn More
Before you activate HA, make sure both devices have the same Smart License and Cloud Regi	on. Otherwise HA will not work.
When you click Activate HA, these settings are automatically deployed to the dev momentary traffic loss. It might take a few minutes for deployment to finish.	ice. The deployment might restart inspection engines, which can result in the
Information is copied to the clipboard when deployment is done. You must allow the clipboard when deployment is done.	the browser to access your clipboard for the copy to be successful.





提示:使用專門用於故障切換流量的小型掩碼子網,以儘可能避免安全漏洞和/或網路問題 。



警告:系統立即將配置部署到裝置。您不需要啟動部署工作。如果您沒有看到說明您的配 置已儲存並且部署正在進行中的消息,請滾動到頁面頂部以檢視錯誤消息。組態也會複製 到剪貼簿。您可以使用副本快速配置輔助裝置。為了增加安全性,剪貼簿副本中不會包含 加密金鑰(如果您設定了加密金鑰)。

步驟 4.配置完成後,您將收到一條消息,說明後續步驟。閱讀資訊後,按一下Got It。

You have successfully deployed the HA configuration on the primary device. What's next?	×
 Copy the HA configuration to the clipboard. Copied Click here to copy again Paste it on the secondary device. Log into the secondary device and open the HA configuration page. 	
You are done! The devices should communicate and establish a high availability pair automatically.	
GOT IT	

配置輔助裝置以實現高可用性

步驟 1.按一下Device,並按位於右上角的Configure按鈕,旁邊是High Availability狀態。

Firewall Device Manager Monitoring	Policies Object	Bevice: ftd-secondary	۵.	: ?	admin Administrator	cisco SECURE
Model Cisco Firepower 2110 Th	Software eat Defense 7.2.5-208	VDB Intrusion Rule Update 370.0 20230925-1455	Cloud Services	High Availability Not Configured 2	CONFIGURE	
CT totick Metwork	Cisco Firepower 2110 Thr MGMT 1/1	1/3 1/5 1/7 1/9 1/11		ISP AMAN //Gateware	Internet DNS Server	
	CONSOLE 1/2	1/13 1/4 1/6 1/8 1/10 1/12 SFP			dente Smart License	

步驟 2.在「高可用性」頁上,按一下輔助裝置框。

Firewall De	vice Manager Monitoring Policies Objects Device: ftd-secondary	(b) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c							
	Device Summary High Availability								
	How High Availability Works	×							
Select the role for this device The primary device is the unit that you intend should be active under normal circumstances. Configure the primary unit first. The secondary device remains in standby mode until the primary unit becomes unavailable.									
	Primary Device or Seco	ndary Device							

步驟 3.配置故障切換鏈路屬性。設定主要FTD後,您可以貼上儲存在剪貼簿中的設定,或者手動繼 續。

步驟 3.1.要從剪貼簿貼上,只需按一下從剪貼簿貼上按鈕,然後貼上到配置中(同時按住Ctrl+v鍵),然後按一下確定。

Select the role for this device							
The primary device is the unit that you intend should be active under normal circumstances. Configure the primary unit first. The secondary device remains in standby mode until the primary unit becomes unavailable.							
Primary Device or Secondary Device							
I have configuration of peer device in clipboard PASTE FROM CLIPBOARD							

X

```
Paste here Peer Device Configuration
```

FAILOVER LINK CONFIGURATION Interface: Ethernet1/7 Primary IP: 10.1.1.1/255.255.255.252 Secondary IP: 10.1.1.2/255.255.255.252

STATEFUL FAILOVER LINK CONFIGURATION Interface: Ethernet1/7 Primary IP: 10.1.1.1/255.255.255.252 Secondary IP: 10.1.1.2/255.255.255.252

CANCEL	ок

步驟 3.2.要手動繼續,請選擇您已直接連線到輔助防火牆的介面,並設定主要和輔助IP地址以及子 網網路掩碼。對於有狀態故障切換鏈路,請選中使用與故障切換鏈路相同的介面覈取方塊。

I have configuration of peer device in clipboard	PASTE FROM CLIPBOARD		
FAILOVER LINK		STATEFUL FAILOVER LINK	Use the same interface as the Failover Link
Interface		Interface	
unnamed (Ethernet1/7)	~	unnamed (Ethernet1/7)	~
Type IPv4 IPv6 Primary IP 10.1.1.1		Type IPv4 IPv6 Primary IP 10.1.1.1	
e.g. 192.168.10.1		e.g. 192.168.11.1	
Secondary IP		Secondary IP	
10.1.1.2		10.1.1.2	
e.g. 192.168.10.2		e.g. 192.168.11.2	
Netmask		Netmask	
255.255.255.252		255.255.255.252	
e.g. 255.255.255.0 or 24		e.g. 255.255.255.0 or 24	
IPSec Encryption Key (optional) For security purposes, the encryption key will not be include clipboard when you activate HA. You will need to manually enter the key when you configure	ed in the configuration copied to the HA on the peer device.	IMPORTANT If you configure an IPsec encryption ke features, both devices will become ac	iy with inconsistent settings for export controlled live after you activate HA. Learn More (2
 Before you activate HA, make sure both devices have When you click Activate HA, these settings all momentary traffic loss. It might take a few million 	e the same Smart License and Cloud Reg re automatically deployed to the de nutes for deployment to finish.	pion. Otherwise HA will not work.	ection engines, which can result in the
Information is copied to the clipboard when a	leployment is done. You must allow	the browser to access your clipboard	for the copy to be successful.
	ACTI	VATE HA	

步驟 4.清除「IPSec加密金鑰」框並按一下Activate HA以儲存更改。



警告:系統立即將配置部署到裝置。您不需要啟動部署工作。如果您沒有看到說明您的配 置已儲存並且部署正在進行中的消息,請滾動到頁面頂部以檢視錯誤消息。

步驟 5.配置完成後,您將收到一條消息,說明您需要採取的後續步驟。閱讀資訊後,按一下Got It。

the H	You have successfully deployed HA configuration on the primary device. What's next?	×
1	Copy the HA configuration to the clipboard.	
2	Paste it on the secondary device. Log into the secondary device and open the HA configuration page.	
	You are done! The devices should communicate and establish a high availability pair automatically.	
	GOT IT	

驗證

此時,您的裝置狀態大部分表明這是「高可用性」頁面上的輔助裝置。如果與主裝置的連線成功,裝置將開始與主裝置同步,最終模式更改為「備用」,而對等裝置更改為「活動」。

	🚯 This device is part of a high availability (HA) pair and is currently in standby state. With few exceptions, you cannot edit the configuration for this device. To make any changes, please log into the active unit. Learn More C							
Firewall Device Manager	题 ⑦ 章	Device: ftd-primary	admin v thethe SECURE					
	Model Cisco Firepower 2110 Threat	Software VDB Intrusion Rule Update Cloud Services Defense 7.2.5-208 370.0 20230925-1455 Connected SEC TAC	High Availability Secondary Device: Standby 🛛 🧬 Peer: Active					
	F	122 Cisco Firepower 2110 Threat Defendence MCMT 1/1 1/3 1/5 1/7 1/9 1/11 Console 1/2 1/4 1/5 1/16 1/1 1/14 1/15 1/16 CONSOLE 1/2 1/4 1/6 1/8 1/10 1/12 5/FP 171	Internet DNS Server ISP/WAN/Gateway Control Server Smart License					

• 主要FTD也大部分顯示「高可用性」狀態,但顯示為「作用中」和「對等點:待命」。

Firewall Device Manager Monitorin	g Policies Objects Devi	ce: ftd-primary		admin Administrator	
	Model Cisco Firepower 2110 Threat Defense	Software VDB Intrusion Rule Update 7.2.5-208 370.0 20230925-1455	Cloud Services	h Availability mary Device: Active 👶 Peer: Standby	
	Cisco Fi	Image: Second	/13 1/14 1/15 1/16	SDYWAN/Cateway	

• 開啟與主要FTD的SSH作業階段,並發出命令show running-config failover以驗證設定。



• 使用命令show failover state驗證裝置的當前狀態。



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)。