

在內嵌配對模式下設定FDM介面

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[准則和限制](#)

[開始之前](#)

[內嵌模式詳細資訊](#)

[內嵌集網路圖表](#)

[配置內嵌集](#)

[修改或刪除內嵌集](#)

簡介

本檔案介紹新增到Cisco安全防火牆7.4.1中的FDM內嵌集。

必要條件

需求

思科建議您瞭解以下主題：

- FDM概念和配置
- 適用於FDM管理的1000、2100和3100系列平台上的FTD

採用元件

本文檔中的資訊基於FDM 7.4.2。

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

內嵌集提供僅IPS介面。如果您有單獨的防火牆保護這些介面並且不需要防火牆功能的開銷，則可以實施僅IPS介面。

內聯集就像電線上的凸點，將兩個介面繫結在一起，以插入現有網路。此功能允許將裝置安裝在任何網路環境中，而無需配置相鄰的網路裝置。內聯介面無條件接收所有流量，但是除非顯式丟棄

，否則這些介面上接收的所有流量都會從內聯集重新傳輸。

准則和限制

- 您只能在這些裝置型號上配置內聯集：Firepower 1000系列、Firepower 2100、安全防火牆 3100。
- 內聯集中允許的介面型別：物理，EtherChannel。
- 不能在內嵌集中包含管理介面。
- 不能更改內聯集中使用的介面的屬性：名稱、模式、介面ID、MTU、IP地址。
- 如果啟用Tap Mode，Snort Fail Open將被禁用。
- 使用內嵌集時，不允許雙向轉發檢測(BFD)回應資料包通過裝置。如果運行BFD的裝置兩側有兩個鄰居，則裝置會丟棄BFD回應資料包，因為這些資料包的源IP地址和目標IP地址相同，並且似乎是LAND攻擊的一部分。
- 對於內聯集和被動介面，裝置最多支援資料包中的兩個802.1Q報頭（也稱為Q-in-Q支援）。



附註：防火牆型別的介面不支援Q-in-Q，僅支援一個802.1Q報頭。

- 內嵌集中的介面不支援路由、NAT、DHCP（伺服器、使用者端或中繼）、VPN、TCP攔截、應用程式檢查或Netflow。

開始之前

- 建議為連線到威脅防禦內嵌配對介面的啟用STP的交換機設定STP PortFast。
- 設定可以是內嵌整合員的實體或EtherChannel介面。您只能配置以下值：名稱、雙工、速度和路由模式（請勿選擇被動）。請勿配置任何型別的定址，即手動IP地址、DHCP或PoE。

內嵌模式詳細資訊

- 此功能允許您使用內嵌集。這將啟用不分配IP的流量檢測。
- 內聯模式可用於物理介面、EtherChannel和安全區域。
- 在內嵌配對中使用介面和EtherChannel時，會自動為其設定內嵌模式。
- 內嵌模式可防止對相關的介面和EtherChannel進行變更，直到將它們從內嵌配對中移除。
- 處於內聯模式的介面可以與設定為內聯模式的安全區域關聯。

內嵌集網路圖表

流量僅使用物理連線通過介面A和B從Router1流到Router2。



網路圖表

配置內嵌集



- 從FDM儀表板導航到Interfaces卡。

The screenshot shows the Cisco Firepower Device Manager (FDM) interface. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device: firepower'. The main content area displays the configuration for a Cisco Firepower 2120 Threat Defense device. The 'Interfaces' card is highlighted with a red box, indicating it is the selected configuration page. The 'Interfaces' card shows 'Management: Merged' and 'Enabled 3 of 17'. Below the card are four tabs: 'Interfaces', 'Routing', 'Updates', and 'System Settings'. The 'Interfaces' tab is active, showing a list of 17 interfaces.

Interfaces頁籤

- 要啟用介面，請單擊接口的Status圖示。

The screenshot shows the 'Interfaces' page in the Cisco Firepower Device Manager (FDM). The page displays a list of 17 interfaces. The 'Ethernet1/3' interface is highlighted with a red box, indicating it is disabled. The 'Status' column for this interface shows a toggle switch that is currently turned off. The other interfaces listed are 'Ethernet1/1', 'Ethernet1/2', and 'Ethernet1/4', all of which are enabled.

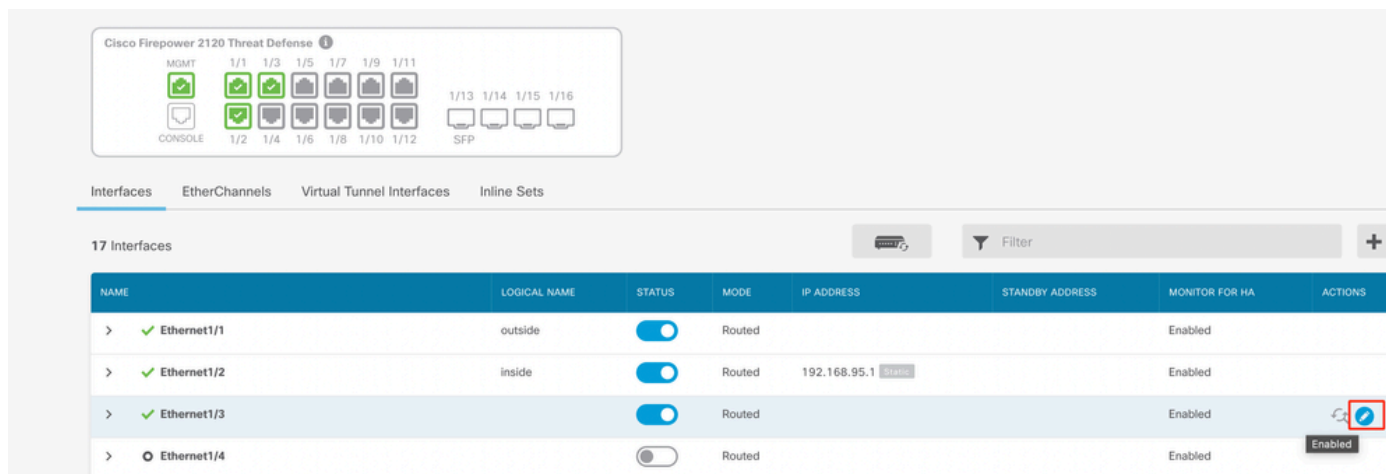
NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
> ✓ Ethernet1/1	outside	<input checked="" type="checkbox"/>	Routed			Enabled	
> ✓ Ethernet1/2	inside	<input checked="" type="checkbox"/>	Routed	192.168.95.1		Enabled	
> ○ Ethernet1/3		<input type="checkbox"/>	Routed			Enabled	 
> ○ Ethernet1/4		<input type="checkbox"/>	Routed			Enabled	

狀態圖示



啟用介面

- 要編輯介面，請點選介面的編輯（鉛筆）圖示。



編輯介面

- 輸入Interface Name並選擇模式作為Routed。請勿配置任何IP地址。

Ethernet1/3 Edit Physical Interface



Interface Name

Inline

Mode

Routed

Status



Most features work with named interfaces only, although some require unnamed interfaces.

Description

IPv4 Address IPv6 Address Advanced

Type

Static

IP Address and Subnet Mask

 /

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask

 /

編輯介面

- 要建立內嵌集，請導航到內嵌集選項卡。

Device Summary

Interfaces

Cisco Firepower 2120 Threat Defense

Interfaces EtherChannels Virtual Tunnel Interfaces **Inline Sets**

17 Interfaces

NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
> ✓ Ethernet1/1	outside	<input checked="" type="checkbox"/>	Routed			Enabled	
> ✓ Ethernet1/2	inside	<input checked="" type="checkbox"/>	Routed	192.168.95.1 <small>Static</small>		Enabled	
> ✓ Ethernet1/3	inline	<input checked="" type="checkbox"/>	Routed			Enabled	
> ○ Ethernet1/4		<input type="checkbox"/>	Routed			Enabled	

建立內嵌集

要新增內嵌集，請點選Add(+ icon)。

The screenshot shows the 'Device Summary' for a Cisco Firepower 2120 Threat Defense device. Under the 'Interfaces' section, there are tabs for 'Interfaces', 'EtherChannels', 'Virtual Tunnel Interfaces', and 'Inline Sets'. The 'Inline Sets' tab is active, showing a table with columns: NAME, MODE, MTU, INTERFACE PAIRS, and ACTIONS. The table is currently empty, with a message stating 'There are no Inline Sets yet. Start by creating the first Inline Set.' and a 'CREATE INLINE SET' button. A red box highlights the '+' icon in the top right corner of the table area.

新增內嵌集

- 為內嵌集設定名稱。
- 設定所需的MTU (可選)。預設值為1500，這是支援的最小MTU。
- 在Interface Pairs部分中，選擇介面。如果需要更多配對，請按一下「添加另一個配對」連結。

Create New Inline Set



Name

inline

MTU

1500



General

Advanced

Interface Pairs

 inline (Ethernet1/3) 



 inside (Ethernet1/2) 



[Add another pair](#)

CANCEL

OK

介面對

- 要配置內聯集的高級設定，請導航到Advanced頁籤。

Edit New Inline Set



Name

inline

MTU

1500

General

Advanced

Interface Pairs

inline (Ethernet1/3)



inside (Ethernet1/2)



[Add another pair](#)

CANCEL

OK

高級設定

- 選擇Mode作為Inline。如果分流器模式已啟用，則Snort失效開放功能會停用。

Edit New Inline Set



Name

inline

MTU

1500

General

Advanced

Mode 



Tap



Inline

內嵌模式

- Snort失效開放允許在Snort進程繁忙或關閉時新流量和現有流量未經檢查就通過（啟用）或丟棄（禁用）。
- 選擇所需的Snort失效開放設定。
- 無法設定Busy和Down選項中的任一、一個或兩個選項。

Edit New Inline Set



Name

inline

MTU

1500

General

Advanced

Mode

Tap

Inline

Enabling "Snort Fail Open" might allow traffic unrestricted.

Snort Fail Open Busy Down

Propagate Link State

CANCEL

OK

Snort失效開放

- 當其中一個介面關閉時，Propagate Link State選項會自動關閉內嵌配對中的第二個介面。當被關閉的介面恢復運行時，第二個介面也會自動恢復。
- 設定好所有內容後，按一下Ok以儲存組態。

Edit New Inline Set



Name

inline

MTU

1500

General

Advanced

Mode

Tap Inline

Enabling "Snort Fail Open" might allow traffic unrestricted.

Snort Fail Open Busy Down

Propagate Link State

CANCEL

OK

傳播連結狀態

- 要將此內聯集新增到安全區域，請導航到對象>安全區域。
- 按一下Add以建立新的安全區域。

Firewall Device Manager | Monitoring | Policies | **Objects** | Device: firepower | admin Administrator | CISCO SECURE

Object Types

- Networks
- Ports
- Security Zones**
- Application Filters
- URLs
- Geolocations
- Syslog Servers
- IKE Policies

Security Zones

2 objects

Filter

#	NAME	MODE	INTERFACES	ACTIONS
1	inside_zone	Routed		
2	outside_zone	Routed		

新增安全區域

- 設定Name，將模式選擇為Inline，然後新增Inline Set的介面。然後按一下OK進行儲存。

Add Security Zone

Name
inline

Description

Mode
 Routed Passive Inline

Interfaces
+
inline (Ethernet1/3)
inside (Ethernet1/2)

CANCEL OK

新增介面

- 導覽至Deployment索引標籤並Deploy變更內容。

修改或刪除內嵌集

「編輯」和「刪除」操作可用於內嵌集。

Device Summary Interfaces



Cisco Firepower 2120 Threat Defense

MGMT 1/1 1/3 1/5 1/7 1/9 1/11
CONSOLE 1/2 1/4 1/6 1/8 1/10 1/12
SFP 1/13 1/14 1/15 1/16

Interfaces | EtherChannels | Virtual Tunnel Interfaces | **Inline Sets**

1 inline set

Filter +

NAME	MODE	MTU	INTERFACE PAIRS	ACTIONS
inline	Inline	1500	inline ↔ inside	 

內嵌集的操作

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）。