

在内联对模式下配置FDM接口

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[准则和限制](#)

[开始使用前](#)

[内联模式详细信息](#)

[内联集网络图](#)

[配置内联集](#)

[修改或删除内联集](#)

简介

本文档介绍在Cisco安全防火墙7.4.1中添加的FDM内联集。

先决条件

要求

Cisco 建议您了解以下主题：

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

使用的组件

本文档中的信息基于FDM 7.4.2。

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

内联集提供仅IPS接口。如果您有单独的防火墙保护这些接口，并且不需要防火墙功能的开销，则可以实施仅IPS接口。

内联集的作用类似于线缆上的凸点，将两个接口绑定在一起，以插入现有网络。此功能允许将设备安装在任何网络环境中，而无需配置相邻网络设备。内联接口无条件地接收所有流量，但是除非明

确丢弃，否则在这些接口上接收的所有流量都会在内联集外重新传输。

准则和限制

- 您只能在这些设备型号上配置内联集：Firepower 1000系列、Firepower 2100、安全防火墙 3100。
- 内联集中允许的接口类型：物理、EtherChannel。
- 不能在内联集中包含管理接口。
- 不能更改内联集中使用的接口的属性：名称、模式、接口ID、MTU、IP地址。
- 如果启用分路模式，Snort失效开放将被禁用。
- 使用内联集时，不允许双向转发检测(BFD)回应数据包通过设备。如果设备两侧有两个邻居运行BFD，则设备会丢弃BFD回应数据包，因为它们具有相同的源IP地址和目标IP地址，并且似乎是LAND攻击的一部分。
- 对于内联集和被动接口，设备在一个数据包中最多支持两个802.1Q报头（也称为Q-in-Q支持）。



注意：防火墙类型接口不支持Q-in-Q，且仅支持一个802.1Q报头。

- 内联集中的接口不支持路由、NAT、DHCP（服务器、客户端或中继）、VPN、TCP拦截、应用检测或Netflow。

开始使用前

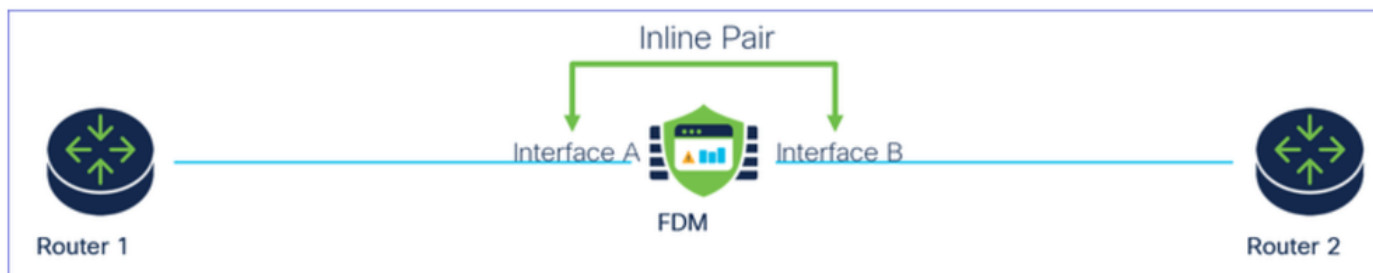
- 建议您为连接到威胁防御内联对接口的启用STP的交换机设置STP PortFast。
- 配置可成为内联集成员的物理或EtherChannel接口。您只能配置以下值：名称、双工、速度和路由模式（请勿选择被动）。请勿配置任何编址类型，即手动IP地址、DHCP或PPoE。

内联模式详细信息

- 此功能允许您使用内联集。这将启用流量检查，而不进行IP分配。
- 内联模式可用于物理接口、EtherChannel和安全区域。
- 当接口和EtherChannel用于内联对时，它们会自动设置内联模式。
- 内联模式可防止对相关接口和EtherChannel进行更改，直到将它们从内联对中删除。
- 处于内联模式的接口可以与设置为内联模式的安全区域相关联。

内联集网络图

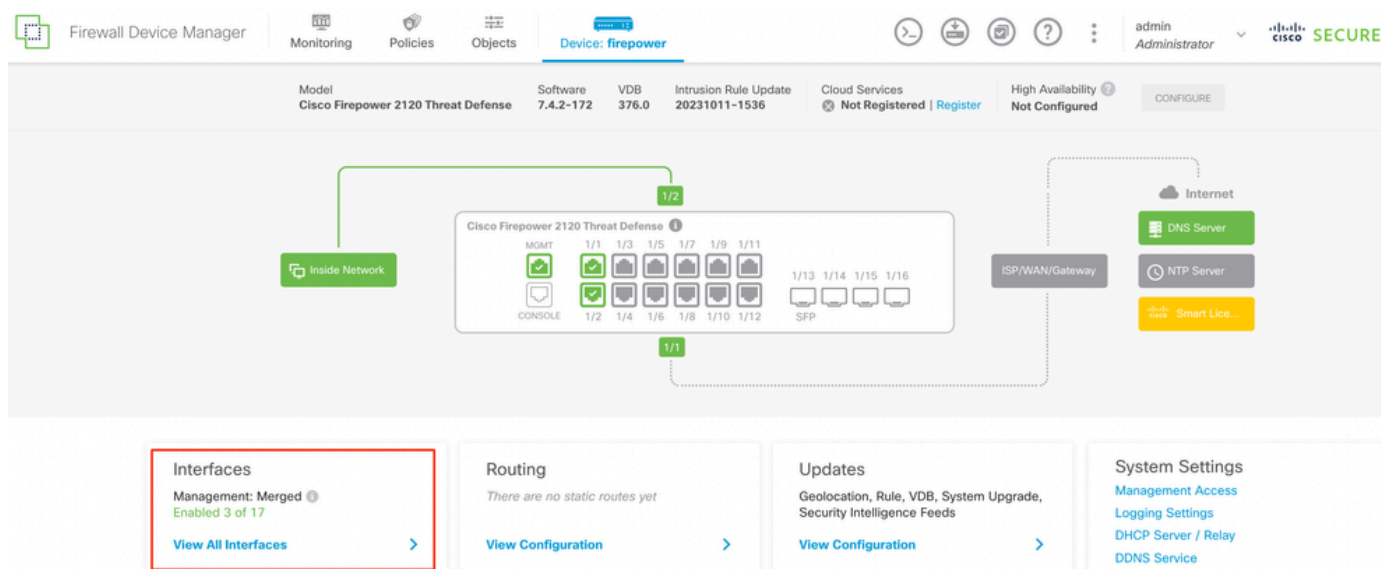
流量仅使用物理连接通过接口A和B从Router1流到Router2。



网络图

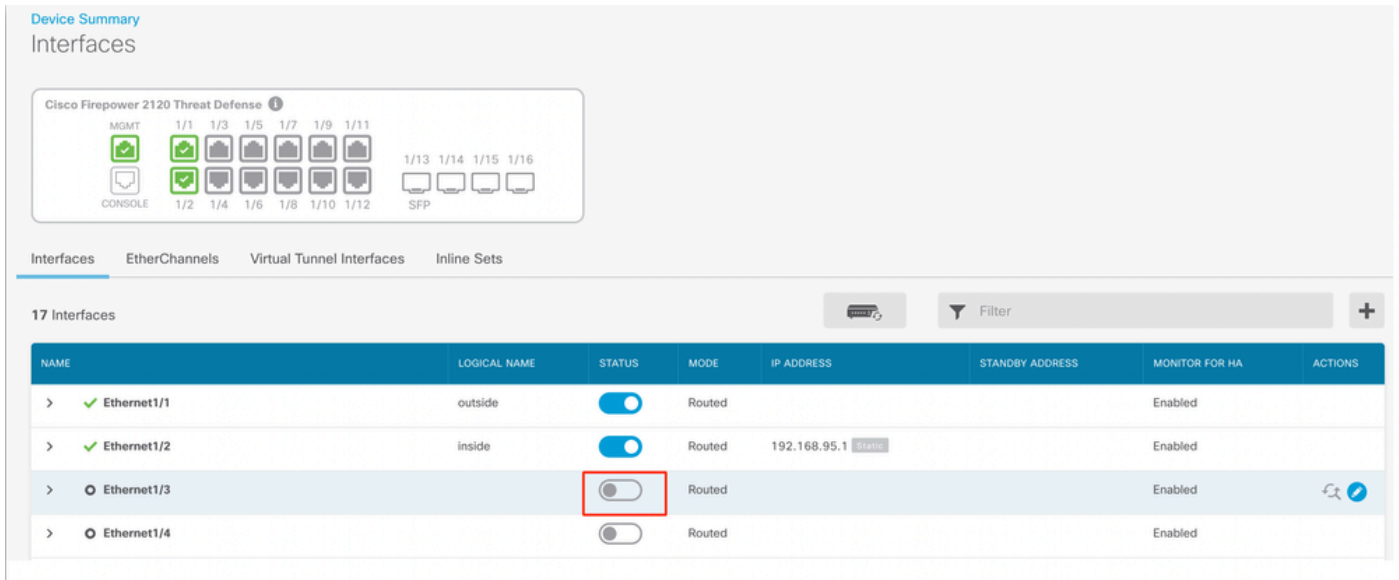
配置内联集

- 在FDM控制面板中，导航到接口卡。

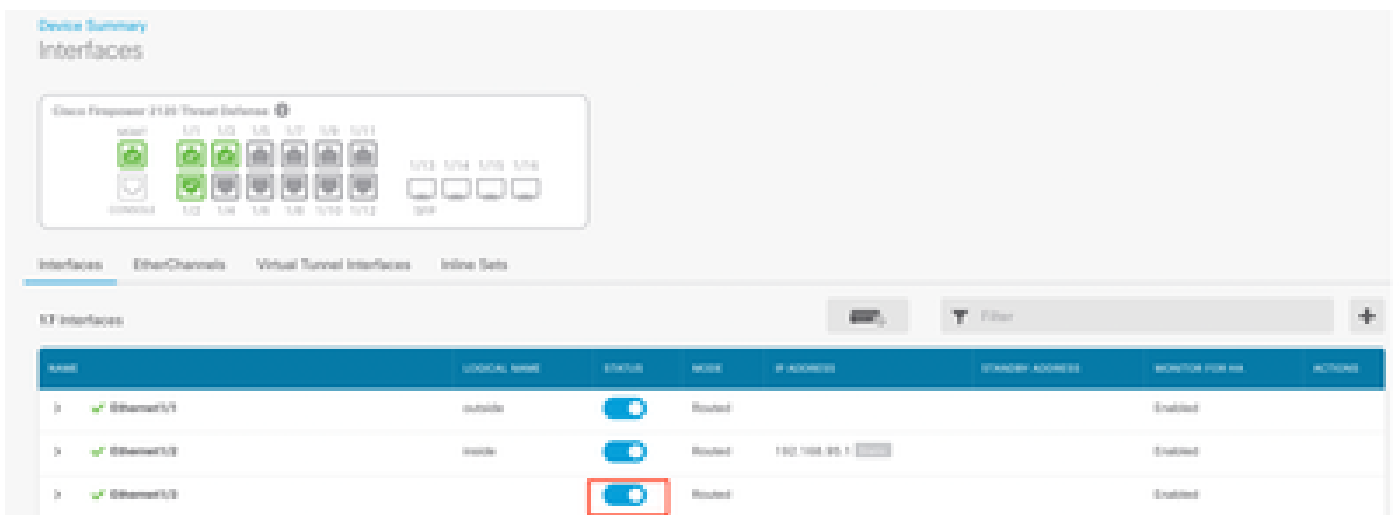


Interfaces选项卡

- 要启用接口，请点击接口的Status图标。

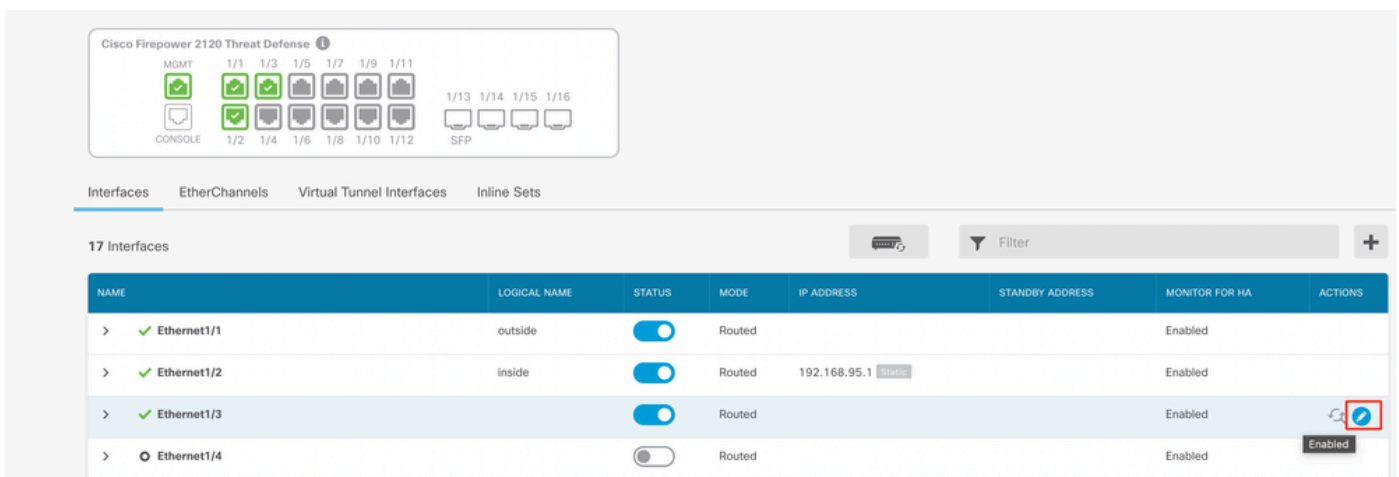


状态图标



启用接口

- 要编辑接口，请点击接口的Edit（铅笔）图标。



编辑接口

- 输入Interface Name并选择模式作为Routed(路由)。请勿配置任何IP地址。

Ethernet1/3

Edit Physical Interface

Interface Name:

Mode:

Status:

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

Description:

IPv4 Address | IPv6 Address | Advanced

Type:


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: /

编辑接口

- 要创建内联集，请导航到内联集选项卡。

Device Summary
Interfaces



Interfaces EtherChannels Virtual Tunnel Interfaces **Inline Sets**


17 Interfaces Filter +

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	

创建内联集

要添加内联集，请点击Add(+图标)。

Device Summary
Interfaces



Interfaces EtherChannels Virtual Tunnel Interfaces **Inline Sets**

Filter +

NAME	MODE	MTU	INTERFACE PAIRS	ACTIONS
<p>There are no Inline Sets yet. Start by creating the first Inline Set.</p> <p>CREATE INLINE SET</p>				

添加内联集

- 为内联集设置名称。
- 设置所需的MTU (可选)。默认值为1500，这是支持的最低MTU。
- 在Interface Pairs部分中，选择接口。如果需要更多线对，请单击Add another pair链接。

Create New Inline Set



Name

inline

MTU

1500

General

Advanced

Interface Pairs

 inline (Ethernet1/3) 



 inside (Ethernet1/2) 



[Add another pair](#)

CANCEL

OK

接口对

- 要配置内联集的高级设置，请导航到Advanced选项卡。

Edit New Inline Set



Name

inline

MTU

1500

General

Advanced

Interface Pairs

inline (Ethernet1/3)



inside (Ethernet1/2)



[Add another pair](#)

CANCEL

OK

高级设置

- 选择Mode作为Inline。如果启用分路模式，则禁用Snort失效开放。

Edit New Inline Set



Name

inline

MTU

1500

General

Advanced

Mode 



Tap



Inline

内联模式

- 当Snort进程繁忙或关闭时，Snort失效开放允许新的和现有的流量通过而不检查（启用）或丢弃（禁用）。
- 选择所需的Snort Fail Open设置。
- 不能设置Busy和Down选项中的一个或两个。

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失效开放

- 当其中一个接口关闭时，Propagate Link State选项会自动关闭内联对中的第二个接口。当被关闭的接口恢复正常时，第二个接口也会自动恢复正常。
- 设置完所有内容后，单击Ok保存配置。

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

传播链路状态

- 要将此内联集添加到安全区域，请导航到对象>安全区域。
- 单击Add以创建新的安全区域。

The screenshot shows the Firepower Security Zones configuration page. The 'Objects' tab is selected in the top navigation bar. The 'Security Zones' section displays a table with 2 objects:

#	NAME	MODE	INTERFACES	ACTIONS
1	inside_zone	Routed		
2	outside_zone	Routed		

A red box highlights the '+' icon in the top right corner of the table, indicating the 'Add' button for creating a new security zone.

添加安全区域

- 设置Name，将模式选择为Inline，然后添加Inline集接口。然后单击OK保存。

Add Security Zone

Name
inline

Description

Mode
 Routed Passive Inline

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

CANCEL OK

添加接口

- 导航到Deployment选项卡并Deploy更改。

修改或删除内联集

Edit和Delete操作可用于内联集。



Device Summary
Interfaces

Cisco Firepower 2120 Threat Defense

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

1 inline set

Filter +

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

内联集的操作

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）。