

Configure FDM Interfaces in Inline-Pair Mode

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Guidelines and Limitations](#)

[Before You Begin](#)

[Inline Mode Details](#)

[Inline Set Network Diagram](#)

[Configure Inline Set](#)

[Modify or Delete an Inline Set](#)

Introduction

This document describes the Inline Sets for FDM added in Cisco Secure Firewall 7.4.1.

Prerequisites

Requirements

Cisco recommends you have knowledge of these topics:

- FDM concepts and configuration
- Applies to FTDs on the 1000, 2100, and 3100 Series platforms managed by FDM

Components Used

The information in this document is based on FDM 7.4.2.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

An inline set provides an IPS-only interface. You can implement IPS-only interfaces if you have a separate firewall protecting these interfaces and do not want the overhead of firewall functions.

An inline set acts like a bump on the wire, binding two interfaces together to slot into an existing network. This function allows the device to be installed in any network environment without the configuration of adjacent network devices. Inline interfaces receive all traffic unconditionally, but all traffic received on these interfaces is retransmitted out of an inline set unless explicitly dropped.

Guidelines and Limitations

- You can configure inline sets on these device models only: Firepower 1000 series, Firepower 2100, Secure Firewall 3100.
- Interface types allowed in an inline set: physical, EtherChannel.
- You cannot include the Management interface in an inline set.
- You cannot change the attributes of the interfaces used in an inline set: name, mode, interface ID, MTU, IP address.
- If you enable Tap Mode, Snort Fail Open is disabled.
- Bidirectional Forwarding Detection (BFD) echo packets are not allowed through the device when using inline sets. If there are two neighbors on either side of the device running BFD, then the device drops BFD echo packets because they have the same source and destination IP address and appear to be part of a LAND attack.
- For inline sets and passive interfaces, the device supports up to two 802.1Q headers in a packet (also known as Q-in-Q support).



Note: Firewall-type interfaces do not support Q-in-Q, and only support one 802.1Q header.

- Interfaces in an inline set do not support routing, NAT, DHCP (server, client, or relay), VPN, TCP Intercept, application inspection, or Netflow.

Before You Begin

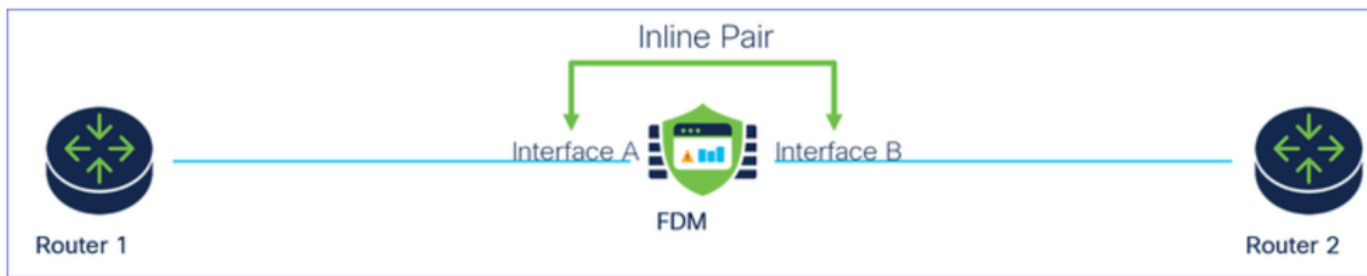
- It is recommended that you set STP PortFast for STP-enabled switches that connect to the threat defense inline pair interfaces.
- Configure the **physical** or **EtherChannel interfaces** that can be members of the inline set. You can configure these values only: Name, duplex, speed, and Routed mode (do not select passive). Do not configure any type of addressing, that is, manual IP addresses, DHCP, or PPOE.

Inline Mode Details

- This feature allows you to use Inline sets. This enables traffic inspection without IP allocation.
- Inline Mode is available for physical interfaces, EtherChannels, and Security Zones.
- Inline Mode is automatically set for Interfaces and EtherChannels when they are used in an Inline Pair.
- Inline Mode prevents changes from being made on the involved Interfaces and EtherChannels until they are removed from the Inline Pair.
- Interfaces that are in Inline Mode can be associated with Security Zones set to Inline Mode.

Inline Set Network Diagram

Traffic flows from Router1 to Router2 through Interfaces A and B using only a physical connection.



Network Diagram

Configure Inline Set

- From the FDM dashboard, navigate to **Interfaces** card.

Interfaces Tab

- To enable interfaces, click **Status** icon of the interface.

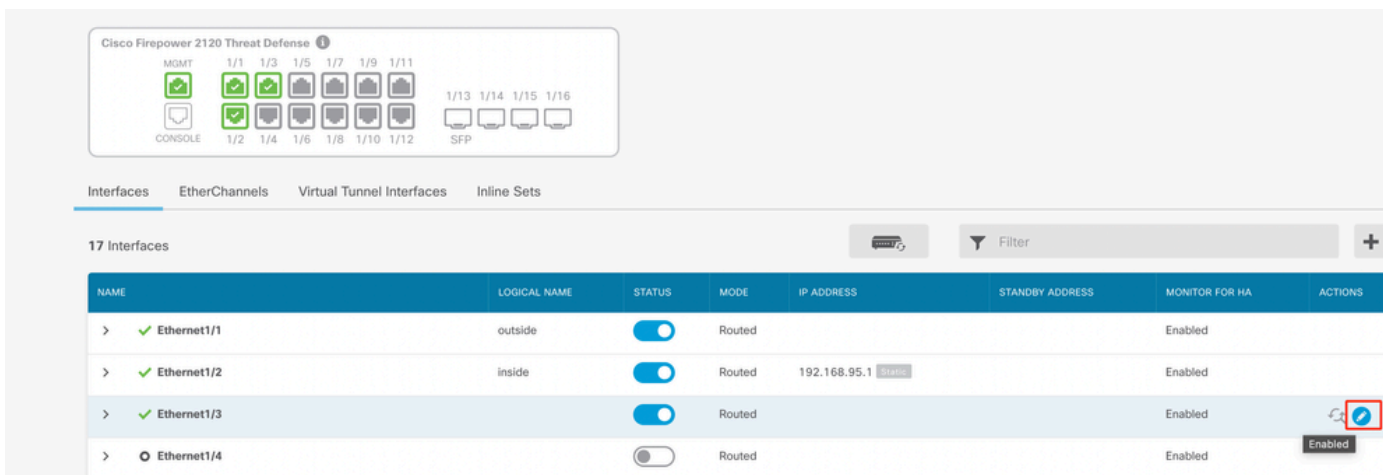
NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
> Ethernet1/1	outside		Routed			Enabled	
> Ethernet1/2	inside		Routed	192.168.95.1		Enabled	
> Ethernet1/3			Routed			Enabled	
> Ethernet1/4			Routed			Enabled	

Status Icon



Enable Interface

- To Edit interfaces, click **Edit** (pencil) icon for the interface.



Edit Interface

- Enter the **Interface Name** and select the mode as **Routed**. Do not configure any **IP Address**.

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

Edit Interface

- To create an Inline Set, navigate to **Inline Sets** Tab.

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		Enabled	
> ✓ Ethernet1/3	inline	<input checked="" type="checkbox"/>	Routed			Enabled	
> ○ Ethernet1/4		<input type="checkbox"/>	Routed			Enabled	

Create Inline Set

To add an Inline Set, click **Add** (+ icon).

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**

Filter +

NAME	MODE	MTU	INTERFACE PAIRS	ACTIONS
There are no Inline Sets yet. Start by creating the first Inline Set.				

CREATE INLINE SET

Add Inline Set

- Set a name for the inline set.
- Set desired MTU (optional) . The default is 1500, which is the minimum supported MTU.
- In the **Interface Pairs** section, select the **interfaces**. If more pairs are required, click **Add another pair** link.

Create New Inline Set



Name

inline

MTU

1500


General

Advanced

Interface Pairs

 inline (Ethernet1/3) ▼



 inside (Ethernet1/2) ▼



[Add another pair](#)

CANCEL

OK

Interface Pairs

- To configure the advanced settings for the Inline Set, navigate to the **Advanced** Tab.

Edit New Inline Set



Name

inline

MTU

1500

General

Advanced

Interface Pairs

inline (Ethernet1/3) ↔ inside (Ethernet1/2)

[Add another pair](#)

CANCEL

OK

Advanced Settings

- Select the **Mode** as **Inline**. If Tap Mode is enabled, Snort Fail Open is disabled.

Edit New Inline Set



Name

inline

MTU

1500

General

Advanced

Mode 



Tap



Inline

Mode Inline

- Snort Fail Open allows new and existing traffic to pass without inspection (enabled) or drop (disabled) when the Snort process is busy or down.
- Pick the desired **Snort Fail Open** settings.
- None, one, or both of the **Busy** and **Down** options can be set.

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 Fail Open

- The Propagate Link State option automatically brings down the second interface in the Inline Pair when one of the interfaces goes down. When the downed interface comes back up, the second interface also automatically comes back up.
- Once everything is set, click **Ok** to save the configuration.

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

Propagate Link State

- To add this inline set to a security zone, navigate to **Objects > Security Zones**.
- Click **Add** to create a new security zone.

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		

Add Security Zone

- Set a **Name**, select the mode as **Inline** and add the **interfaces** of the Inline Set. Then click **OK** to save.

Add Security Zone

Name
inline

Description

Mode
 Routed Passive Inline

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

CANCEL OK

Add Interfaces

- Navigate to **Deployment** tab and **Deploy** the changes.

Modify or Delete an Inline Set

Edit and Delete actions are available for the Inline Sets.



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	 

Actions of Inline Set