

# Configurazione delle interfacce FDM in modalità coppia inline

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Linee guida e limitazioni](#)

[Operazioni preliminari](#)

[Dettagli modalità in linea](#)

[Diagramma reticolare set inline](#)

[Configura set inline](#)

[Modifica o eliminazione di un set in linea](#)

---

## Introduzione

Questo documento descrive i set in linea per FDM aggiunti in Cisco Secure Firewall 7.4.1.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Concetti e configurazione di FDM
- Si applica agli FTD sulle piattaforme serie 1000, 2100 e 3100 gestite da FDM

### Componenti usati

Le informazioni di questo documento si basano su FDM 7.4.2.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

Un set inline fornisce un'interfaccia solo IPS. È possibile implementare interfacce solo IPS se si

dispone di un firewall separato che protegge queste interfacce e non si desidera sovraccaricare le funzioni del firewall.

Un set inline agisce come un urto in cavo, collegando due interfacce in modo da inserirle in una rete esistente. Questa funzione consente di installare il dispositivo in qualsiasi ambiente di rete senza configurare i dispositivi di rete adiacenti. Le interfacce inline ricevono tutto il traffico incondizionatamente, ma tutto il traffico ricevuto su queste interfacce viene ritrasmesso da un set inline a meno che non venga esplicitamente scartato.

## Linee guida e limitazioni

- È possibile configurare i set inline solo su questi modelli di dispositivi: Firepower serie 1000, Firepower 2100, Secure Firewall 3100.
- Tipi di interfaccia consentiti in un set inline: fisica, EtherChannel.
- Non è possibile includere l'interfaccia di gestione in un set inline.
- Non è possibile modificare gli attributi delle interfacce utilizzate in un insieme inline: nome, modalità, ID interfaccia, MTU, indirizzo IP.
- Se si attiva la modalità maschiatura, l'opzione Snort Fail Open è disattivata.
- I pacchetti echo BFD (Bidirectional Forwarding Detection) non sono consentiti tramite il dispositivo quando si utilizzano set inline. Se ci sono due dispositivi adiacenti su entrambi i lati del dispositivo che esegue BFD, il dispositivo scarta i pacchetti echo BFD perché hanno lo stesso indirizzo IP di origine e destinazione e sembrano essere parte di un attacco LAND.
- Per i set inline e le interfacce passive, il dispositivo supporta fino a due intestazioni 802.1Q in un pacchetto (noto anche come supporto Q-in-Q).



Nota: Le interfacce di tipo firewall non supportano Q-in-Q e supportano solo un'intestazione 802.1Q.

---

- Le interfacce in un set inline non supportano routing, NAT, DHCP (server, client o relay), VPN, TCP Intercept, ispezione delle applicazioni o Netflow.

## Operazioni preliminari

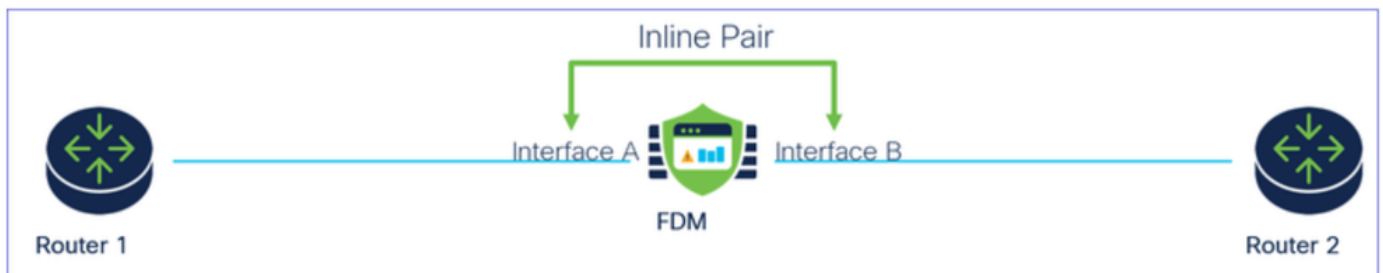
- Si consiglia di impostare STP PortFast per gli switch con abilitazione STP che si connettono alle interfacce in linea per la difesa dalle minacce.
- Configurare le interfacce fisiche o EtherChannel che possono essere membri del set inline. È possibile configurare solo questi valori: Nome, duplex, velocità e modalità di routing (non selezionare passiva). Non configurare alcun tipo di indirizzamento, ovvero indirizzi IP manuali, DHCP o PoE.

## Dettagli modalità in linea

- Questa funzione consente di utilizzare i set in linea. Ciò consente l'ispezione del traffico senza allocazione IP.
- La modalità inline è disponibile per le interfacce fisiche, EtherChannel e le aree di sicurezza.
- La modalità in linea viene impostata automaticamente per le interfacce e EtherChannel quando vengono utilizzate in una coppia in linea.
- La modalità in linea impedisce che vengano apportate modifiche alle interfacce e agli EtherChannel interessati finché non vengono rimossi dalla coppia in linea.
- Le interfacce in modalità in linea possono essere associate alle aree di protezione impostate sulla modalità in linea.

## Diagramma reticolare set inline

Il traffico passa da Router1 a Router2 attraverso le interfacce A e B usando solo una connessione fisica.



Esempio di rete

## Configura set inline

- Dal dashboard FDM, passare alla scheda Interfacce.

Firewall Device Manager

Monitoring Policies Objects **Device: firepower**

Model: Cisco Firepower 2120 Threat Defense | Software: 7.4.2-172 | VDB: 376.0 | Intrusion Rule Update: 20231011-1536 | Cloud Services: Not Registered | Register | High Availability: Not Configured

Interfaces  
Management: Merged  
Enabled 3 of 17  
[View All Interfaces](#)

Routing  
There are no static routes yet  
[View Configuration](#)

Updates  
Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds  
[View Configuration](#)

System Settings  
[Management Access](#)  
[Logging Settings](#)  
[DHCP Server / Relay](#)  
[DDNS Service](#)

scheda Interfacce

- Per abilitare le interfacce, fare clic su Icona Stato dell'interfaccia.

Device Summary  
Interfaces

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		Routed			Enabled	
>  Ethernet1/2	inside		Routed	192.168.95.1 <small>Static</small>		Enabled	
>  Ethernet1/3			Routed			Enabled	
>  Ethernet1/4			Routed			Enabled	

Icona di stato

Device Summary  
Interfaces

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		Routed			Enabled	
>  Ethernet1/2	inside		Routed	192.168.95.1 <small>Static</small>		Enabled	
>  Ethernet1/3			Routed			Enabled	

## Abilita interfaccia



- Per modificare le interfacce, fare clic sull'icona Modifica (matita) relativa all'interfaccia.

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

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

## Modifica interfaccia

- Immettere il nome dell'interfaccia e selezionare la modalità come Instradato. Non configurare alcun indirizzo IP.

# 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

 / 

Modifica interfaccia

- Per creare una serie in linea, passare alla scheda Serie in linea.

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	

Crea set inline

Per aggiungere un set in linea, fare clic su Aggiungi (icona +).

The screenshot shows the configuration page for a Cisco Firepower 2120 Threat Defense device. At the top, there is a 'Device Summary' section with 'Interfaces' selected. Below this, a grid of interface icons is displayed, including MGMT, CONSOLE, and various numbered ports (1/1 through 1/16). The 'Inline Sets' tab is active, showing a table with columns for 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 a plus sign icon in the top right corner of the interface.

Aggiungi set inline

- Impostare un nome per il set in linea.
- Impostare l'MTU desiderata (facoltativo). Il valore predefinito è 1500, che è l'MTU minima supportata.
- Nella sezione Coppie interfacce, selezionare le interfacce. Se sono necessarie più coppie, fare clic su Aggiungi un altro collegamento di coppia.

# Create New Inline Set



Name

inline

MTU

1500


General

Advanced

Interface Pairs

 inline (Ethernet1/3) ▼



 inside (Ethernet1/2) ▼



[Add another pair](#)

CANCEL

OK

Coppie di interfacce

- Per configurare le impostazioni avanzate per il set in linea, passare alla scheda Avanzate.



# Edit New Inline Set



Name

inline

MTU

1500

General

Advanced

Interface Pairs

inline (Ethernet1/3)



inside (Ethernet1/2)



[Add another pair](#)

CANCEL

OK

Impostazioni avanzate

- Selezionare la Modalità come Inline. Se la modalità mascheratura è attivata, l'opzione Snort Fail Open è disattivata.

## Edit New Inline Set



Name

inline

MTU

1500

General

**Advanced**

Mode 



Tap



Inline

Modalità in linea

- Snort Fail Open consente il passaggio di traffico nuovo ed esistente senza ispezione (abilitata) o perdita (disabilitata) quando il processo Snort è occupato o inattivo.
- Selezionare le impostazioni Snort Fail Open desiderate.
- È possibile impostare le opzioni Occupato e Giù su Nessuno, Uno o entrambi.

## 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

- L'opzione Propaga stato collegamento riduce automaticamente la seconda interfaccia nella coppia inline quando una delle interfacce diventa inattiva. Quando l'interfaccia di cui è stata eseguita la riattivazione è disponibile anche la seconda interfaccia.
- Una volta impostati tutti gli elementi, fare clic su OK per salvare la configurazione.

# 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

Propaga stato collegamento

- Per aggiungere questo set in linea a un'area di sicurezza, selezionare Oggetti > Aree di sicurezza.
- Fare clic su Add (Aggiungi) per creare una nuova area di sicurezza.

The screenshot shows the Firewall Device Manager interface for a firepower device. The 'Objects' tab is selected, and the 'Security Zones' section is active. A table lists two security zones: 'inside\_zone' and 'outside\_zone', both in 'Routed' mode. A red box highlights the 'Add' (+) button in the top right corner of the table.

#	NAME	MODE	INTERFACES	ACTIONS
1	inside_zone	Routed		
2	outside_zone	Routed		

- Impostare un Nome, selezionare la modalità come Inline e aggiungere le interfacce dell'Inline Set. Quindi fare clic su OK per salvare.

## Add Security Zone

Name  
inline

Description

Mode  
 Routed  Passive  Inline

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

CANCEL OK

- Passare alla scheda Distribuzione e distribuire le modifiche.

### Modifica o eliminazione di un set in linea

Le azioni Modifica ed Elimina sono disponibili per i Set in linea.



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	 

Azioni di Inline Set

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).