

Configurazione della bypass hardware di Secure Firewall 3100 FDM 7.7.0

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Nozioni di base: Piattaforme supportate, Licenze](#)

[Descrizione delle funzionalità e procedura dettagliata](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Bypass hardware](#)

[API REST dispositivo FDM](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Comandi](#)

[Set Inline -Convalide durante la creazione](#)

[Bypass hardware - Convalida durante la creazione](#)

[Limitazioni dell'implementazione per questa release](#)

[Funzionalità firewall non supportate sulle interfacce inline](#)

Introduzione

In questo documento viene descritto come configurare il bypass hardware per i set inline in Firepower Device Manager (FDM) gestito con Secure Firewall 7.7.0.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Set in linea
- Secure Firewall serie 3100
- Interfaccia grafica utente (GUI) di Firepower Device Manager

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure Firewall 3100 con v7.7.0.
- Cisco Secure Firewall Device Manager v7.7.0.

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

La funzionalità Set in linea è stata aggiunta a FDM nella versione 7.4.1. I set in linea consentono l'ispezione su una rete L2 senza la necessità di instradamento: [Configurazione delle interfacce FTD in modalità Inline-Pair](#)

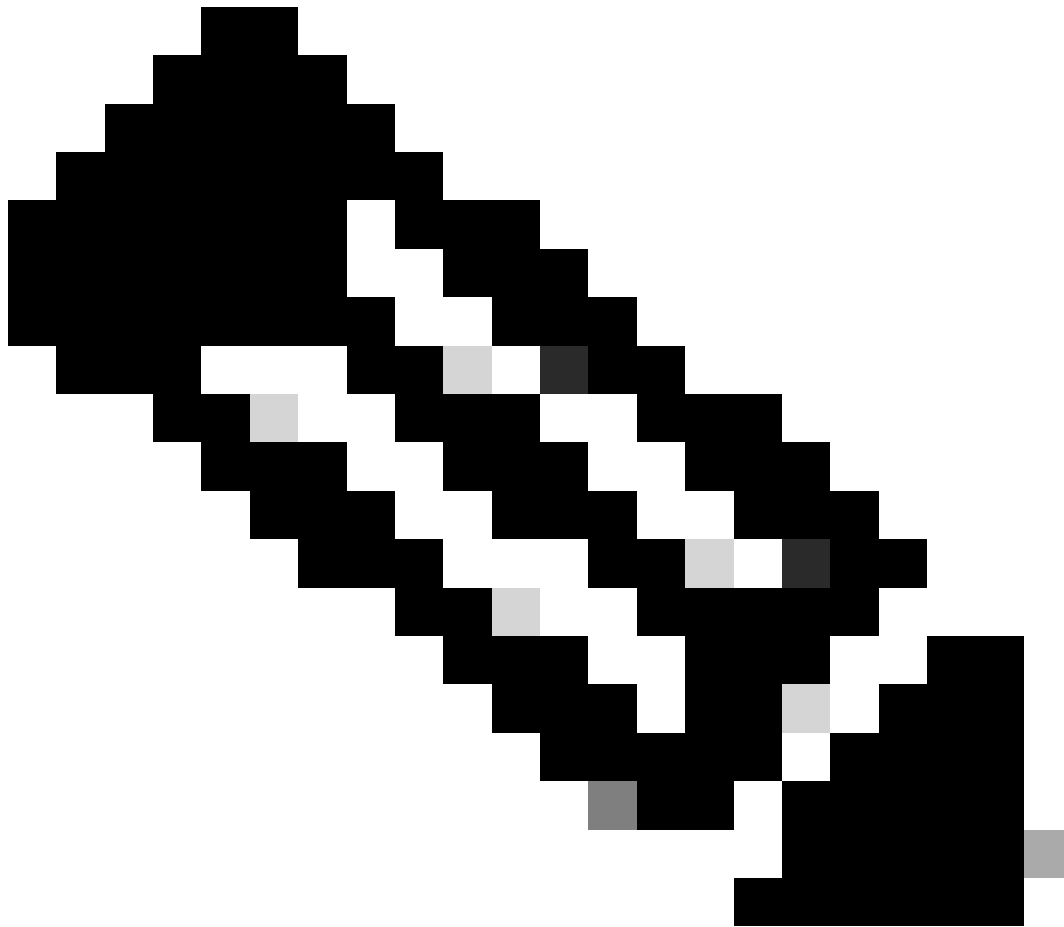
Contrasto rispetto a questa release

In Secure Firewall 7.6 and Below		New to Secure Firewall 7.7
• Inline Sets is available. • Hardware Bypass is not supported.		• Added support for Hardware Bypass.

Funzione Bypass Secure Firewall 7.0

Novità

- La funzione di bypass per l'ispezione dell'hardware assicura il flusso continuo del traffico tra una coppia di interfacce inline durante un'interruzione dell'alimentazione.
- Questa funzione viene utilizzata per mantenere la connettività di rete in caso di errori software o hardware.
- Bypass hardware è ora disponibile per i set inline per le piattaforme FDM serie 3100.



Nota: [Guida alla configurazione di Firepower Management Center](#)

Scenari di distribuzione

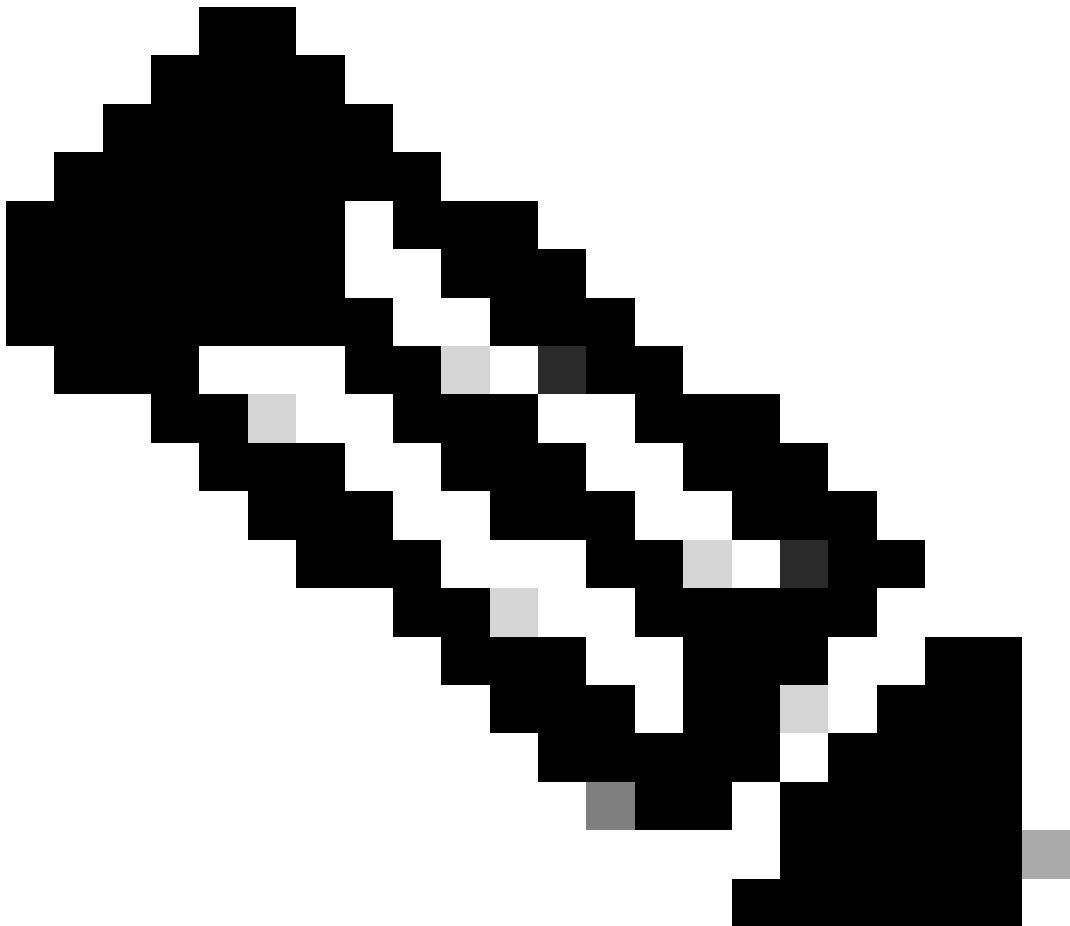
- Come si inserisce questa funzione in una configurazione di produzione?
 - I set inline vengono utilizzati per uno Use Case IPS (o IDS).
 - Consente l'ispezione del traffico senza dover configurare il routing. Consente il flusso del traffico se l'unità si guasta tramite bypass hardware.
- .Esempi pratici:
 - Configurare l'ispezione della rete di livello 2 in qualsiasi punto in modo semplice e veloce, senza la necessità di un livello 3.
 - Critico per reti completamente isolate, ovvero senza accesso a Internet.
 - Inserimento inline trasparente per l'ispezione approfondita dei pacchetti per un firewall standalone - architettura esistente di layer 2.

Nozioni di base: Piattaforme supportate, Licenze

Versioni software e hardware

FDM		
	Inline Sets – before 7.7.0	Inline Sets with Hardware Bypass
FDM	7.4.1	7.7.0
REST API	7.4.1	7.7.0
Platforms	1000, 2100 (up to 7.4 only), and 3100 Series	3100 Series equipped with a network module: • 8 Ports: ◦ FPR-X-NM-6X1SXF • 6 Ports: ◦ FPR-X-NM-6X10SRF ◦ FPR-X-NM-6X10LRF ◦ FPR-X-NM-6X25SRF ◦ FPR-X-NM-6X25LRF

Software e hardware



Nota: [Informazioni sulla serie 3100 e sul bypass hardware](#)

Altri aspetti del supporto

FDM			
Inline Sets		Inline Sets with Hardware Bypass	
Licenses Required	Essentials	Licenses Required	Essentials
Works in Evaluation Mode	Yes	Works in Evaluation Mode	Yes
IP Addressing	Not required	IP Addressing	Not required
Supported with HA'd devices	Yes	Supported with HA'd devices	No
Other (only routed mode)	Yes	Other (only routed mode)	Yes
Multi-instances supported?	Not Supported on 3100 Series	Multi-instances supported?	Not Supported on 3100 Series
Supported with clustered devices?	Not Supported on 3100 Series	Supported with clustered devices?	Not Supported on 3100 Series

Licenze e compatibilità

Descrizione delle funzionalità e procedura dettagliata

Descrizione funzionalità funzionale

- Diagramma reticolare set inline



Diagramma reticolare set inline

- Il traffico passa dal router 1 al router 2 attraverso le interfacce A e B, utilizzando solo una connessione fisica.
- Diagramma di flusso dell'elaborazione dei pacchetti di FDM Inline Sets:

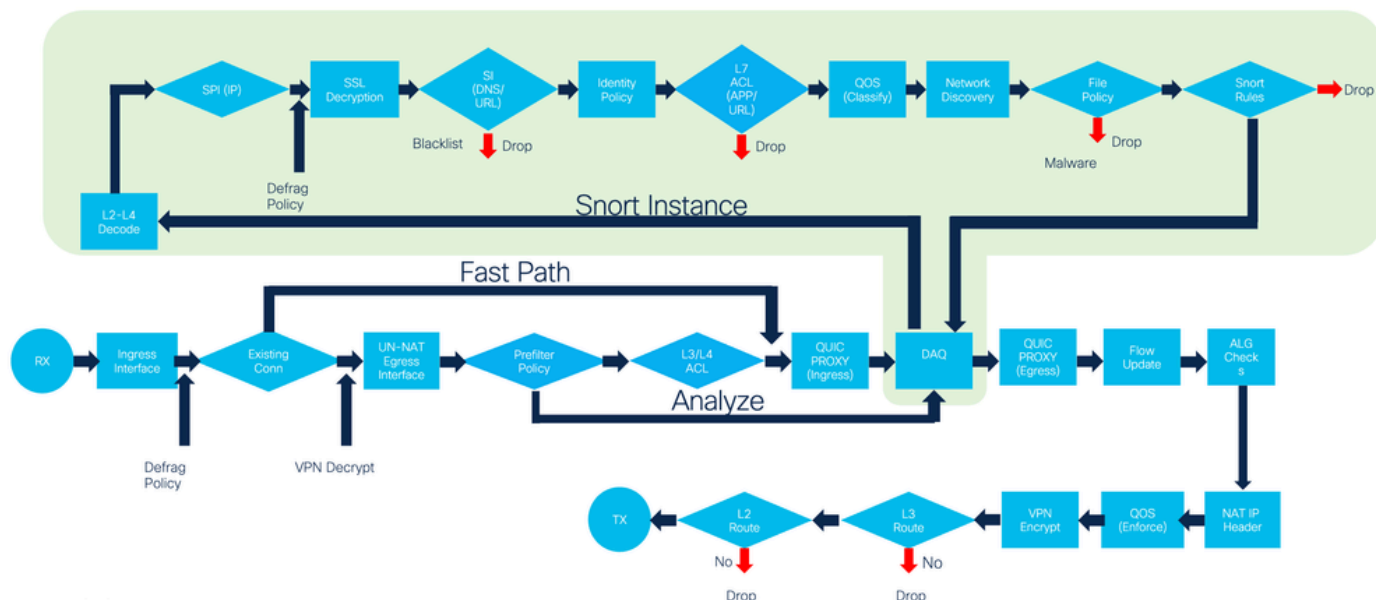


Diagramma di flusso

- Set in linea:
 - I set inline sono supportati sulle interfacce fisiche e su EtherChannel.
- Bypass hardware:
 - I set inline con bypass hardware sono supportati su coppie di interfacce fisiche predeterminate:
 - Ethernet 1 e 2
 - Ethernet 2 e 3
 - Ethernet 4 e 5
 - Ethernet 5 e 6
- Supporto interfaccia:
 - Interfacce che fanno parte di una coppia inline:
 - Deve essere denominato.
 - Essere liberi da qualsiasi IConfigurazioni P, DHCP o PPPoE.
 - Non deve essere in modalità passiva.
 - Non deve essere un'interfaccia di gestione.
 - Deve essere utilizzato solo in una coppia inline alla volta.
- Dettagli modalità in linea
 - La modalità in linea è disponibile per interfacce fisiche, EtherChannel e 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.

- GUI modalità inline
 - Nella finestra di dialogo Modifica interfaccia viene indicato che l'interfaccia o EtherChannel è in modalità in linea.
 - Le modifiche non sono consentite sulle interfacce in modalità inline. La finestra di dialogo Modifica interfaccia fisica (o Modifica EtherChannel) è di sola lettura.

Ethernet1/5
Edit Physical Interface

Interface Name: loekhozjo

Mode: Inline (highlighted with a red box)

Status: ☐

Description:

IPv4 Address | IPv6 Address | Advanced

This interface is a member of an inline set. You cannot configure IP addresses on inline set members.

Type:

Modifica interfaccia nella GUI

- Aggiornamento, importazione/esportazione, backup/ripristino, installazione
 - Implicazioni dell'aggiornamento
L'utente può aggiornare FDM senza alcuna restrizione.
Quando si esegue l'aggiornamento da una versione precedente, gli oggetti set in linea esistenti vengono configurati con il relativo campo bypass impostato su Disabilitato.
 - Implicazioni importazione/esportazione
Gli oggetti Set in linea vengono importati ed esportati.
 - Backup/Ripristino
Gli oggetti Inline Set vengono gestiti durante le operazioni di backup e ripristino.
 - Implementazione
Gli oggetti vengono distribuiti normalmente.
Sono stati implementati errori specifici.

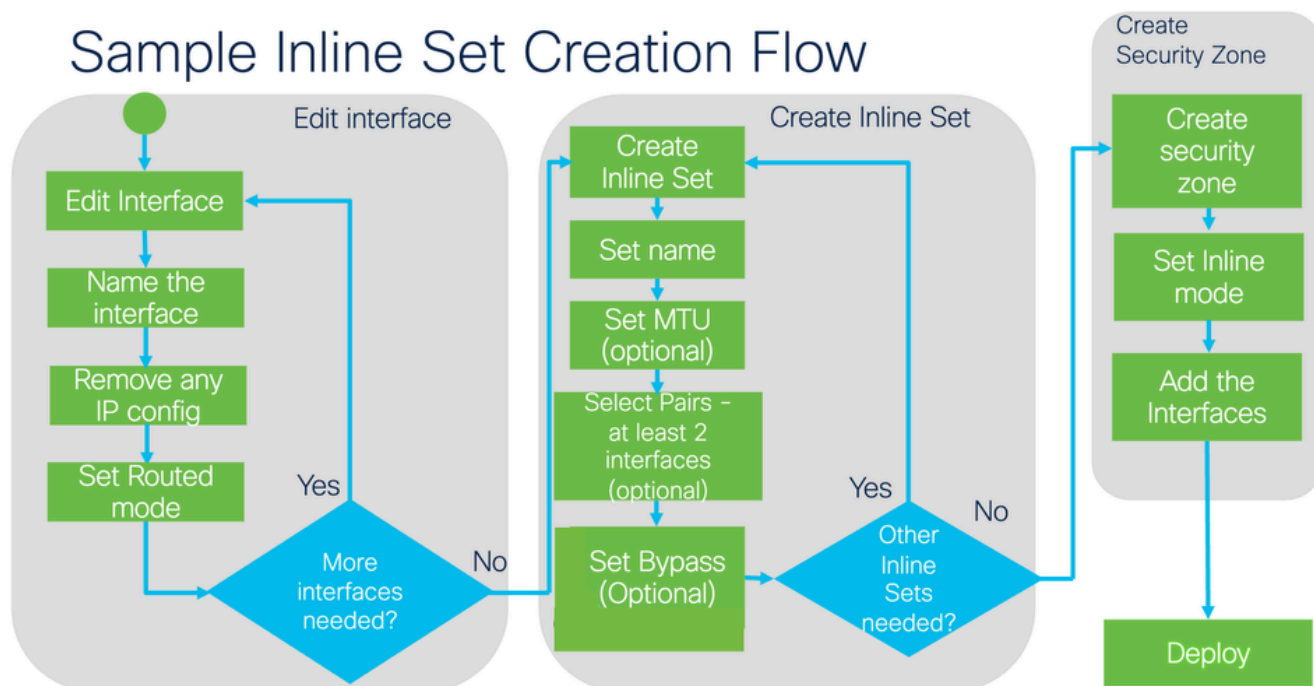
Configurazione

Esempio di rete



Esempio di rete

Sample Inline Set Creation Flow



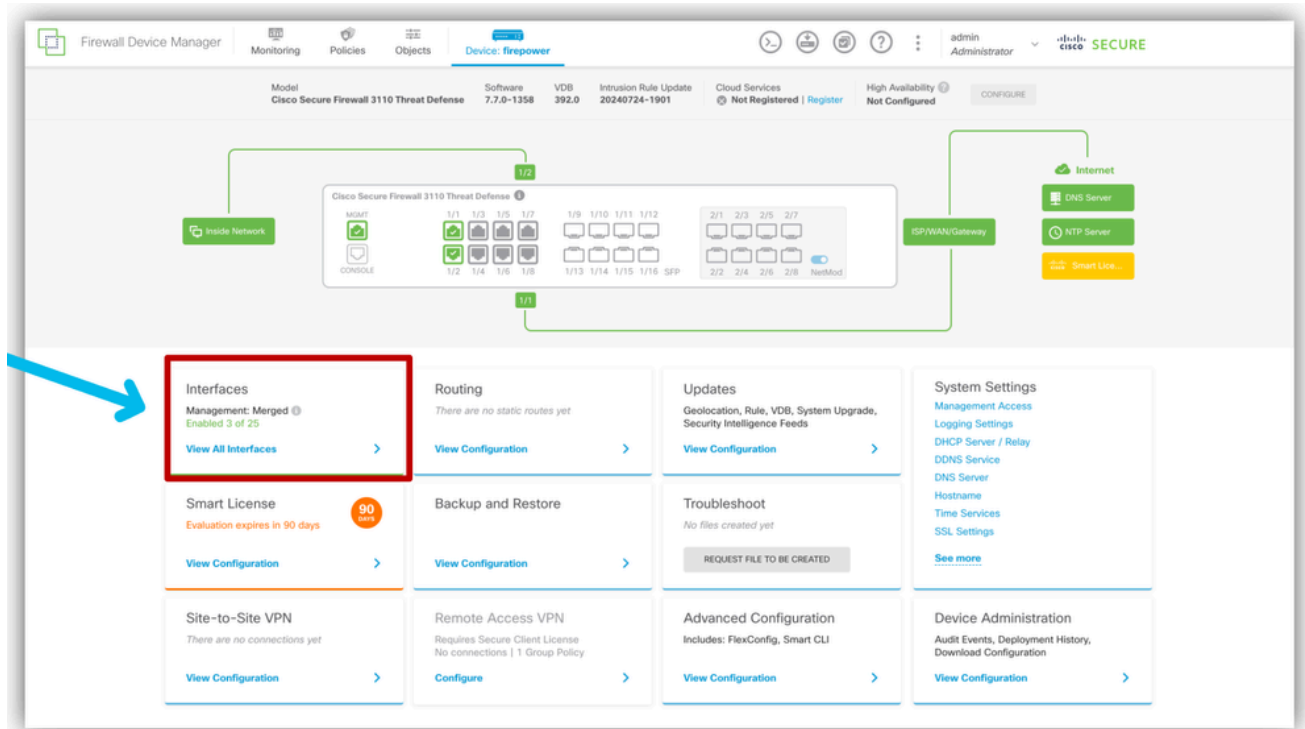
Flusso di creazione serie in linea

Configurazioni

In questa sezione vengono descritti i passaggi per configurare il bypass hardware in FDM

Passaggio 1: modificare le interfacce.

- Accedere a FDM e passa a Gestione interfaccia.
- Dal dashboard FDM, fare clic sulla scheda Interfacce.



Seleziona interfaccia

- Modificare le interfacce utilizzate nell'insieme inline.
- Per modificare le interfacce, fare clic sull'icona Modifica (matita) relativa all'interfaccia.

NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
> ☐ Ethernet1/6		☐	Routed			Enabled	
> ☐ Ethernet1/7		☐	Routed			Enabled	
> ☐ Ethernet1/8		☐	Routed			Enabled	
> ☐ Ethernet1/9		☐	Routed			Enabled	
> ☐ Ethernet1/10		☐	Routed			Enabled	
> ☐ Ethernet1/11		☐	Routed			Enabled	
> ☐ Ethernet1/12		☐	Routed			Enabled	
> ☐ Ethernet1/13		☐	Routed			Enabled	
> ☐ Ethernet1/14		☐	Routed			Enabled	
> ☐ Ethernet1/15		☐	Routed			Enabled	
> ☐ Ethernet1/16		☐	Routed			Enabled	
> ☐ Ethernet2/1	firstinterface	☐	Routed			Enabled	
> ☐ Ethernet2/2	secondinterface	☐	Routed			Enabled	
> ☐ Ethernet2/3	thirdinterface	☐	Routed			Enabled	
> ☐ Ethernet2/4	fourthinterface	☐	Routed			Enabled	
> ☐ Ethernet2/5		☐	Routed			Enabled	

Modifica interfaccia

- Modifica interfaccia fisica:
 1. Assegnare un nome all'interfaccia.

2. Selezionare Modalità instradamento.
3. Rimuovere eventuali configurazioni IP.

Ethernet2/1

Edit Physical Interface

Interface Name

firstinterface

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

Mode

Routed

Status

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

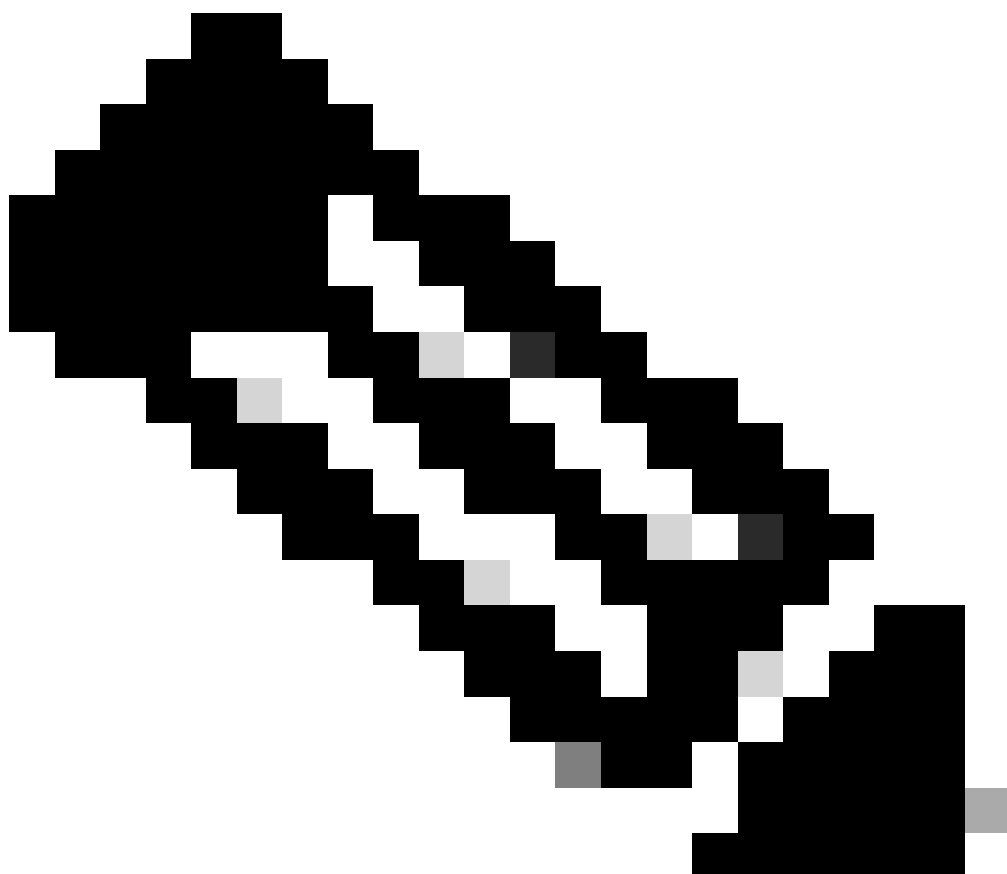
/

e.g. 192.168.5.16

CANCEL

OK

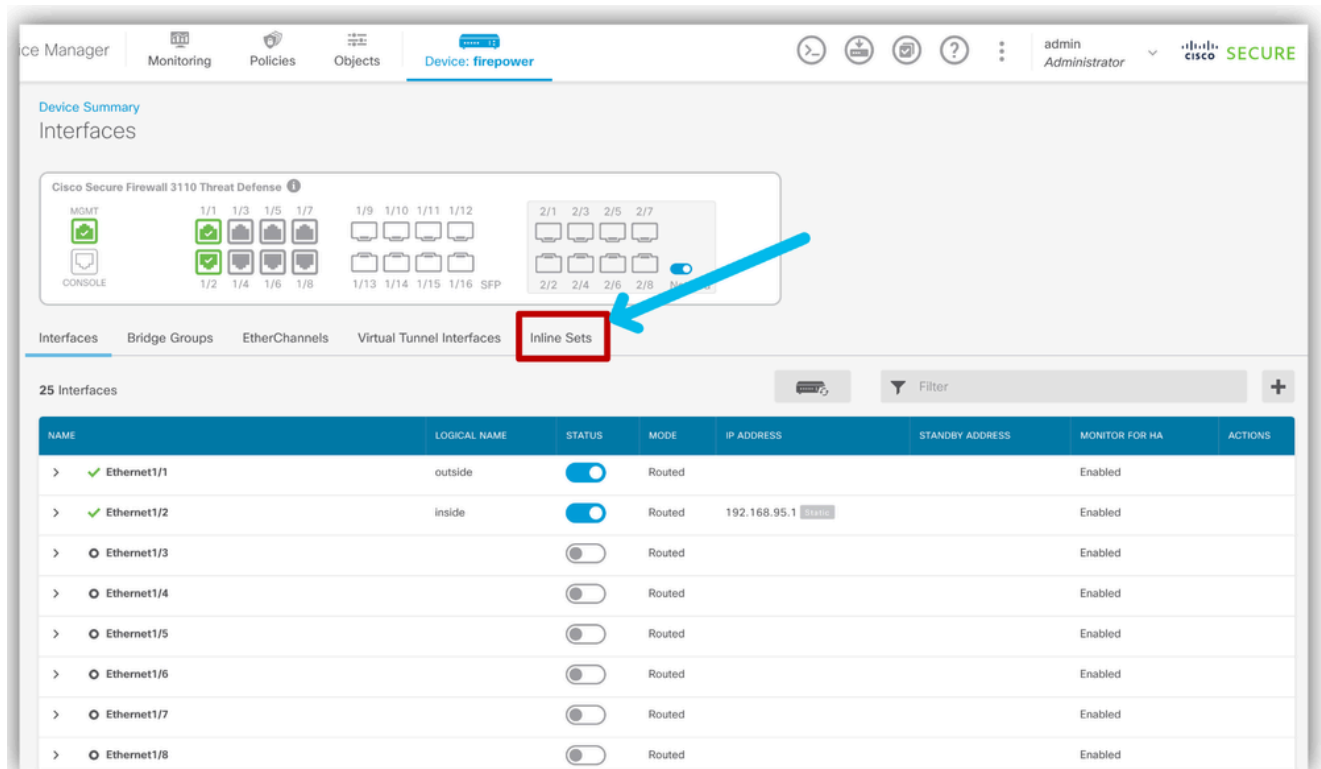
Configura parametri



Nota: La modalità viene automaticamente modificata in Inline dopo l'aggiunta dell'interfaccia in una coppia inline.

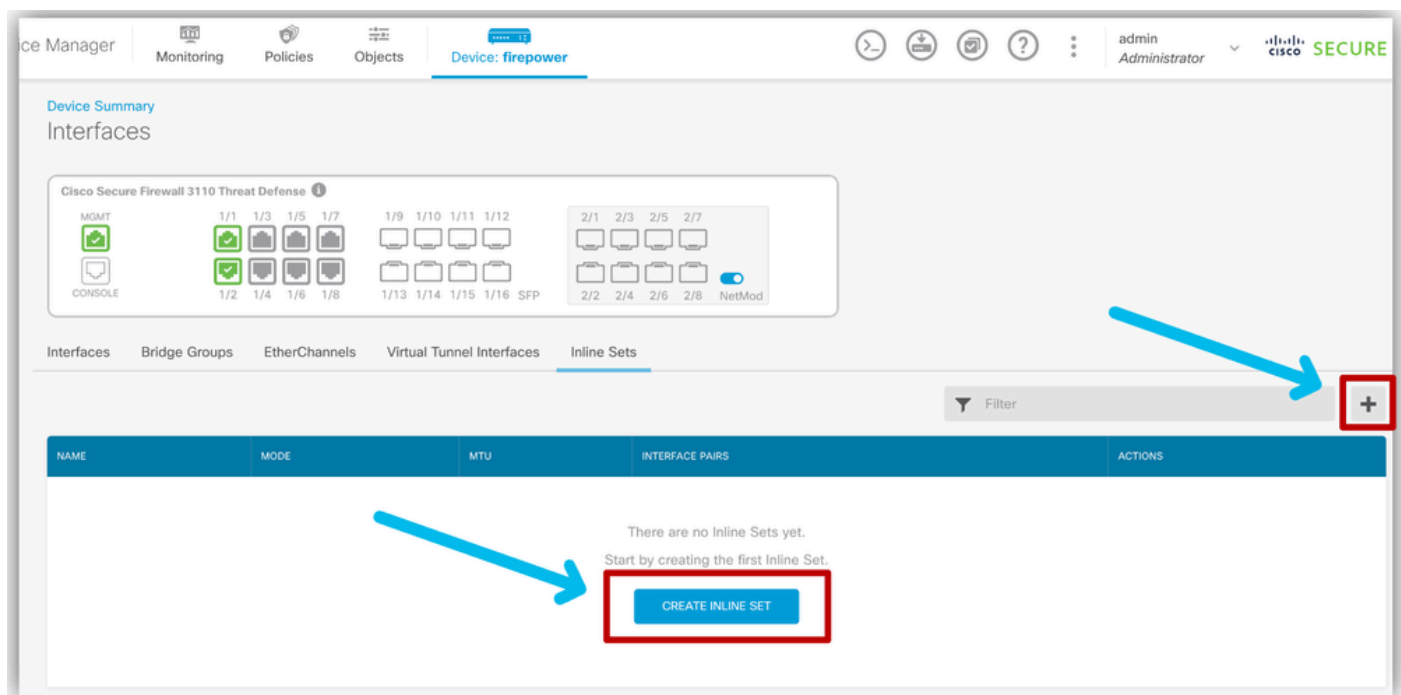
Passaggio 2: Creare un gruppo inline.

- Selezionare Dispositivo > Interfacce > scheda Insieme in linea.



Passa Alla Scheda Serie In Linea

- Aggiunge un nuovo set in linea.
- Fare clic sull'icona + o sul pulsante Crea set in linea.



Crea set inline

- Configurare le impostazioni di base.
 1. Impostare un nome.
 2. Impostare l'MTU desiderata (facoltativo). Il valore predefinito è 1500, ossia l'MTU minima supportata.
 3. Selezionare Ignora hardware (i dettagli sono disponibili nella sezione successiva). È stato aggiunto un nuovo menu a discesa per Ignora.
 4. Nella sezione Coppie di interfacce selezionare interfacce.
 5. Sono disponibili interfacce denominate da selezionare. Se sono necessarie più coppie, fare clic sul collegamento Aggiungi un'altra coppia.

Create New Inline Set

Name: inline_example

MTU: 1500

General | Advanced

Bypass: Standby

Interface Pairs

firstinterface (Ethernet2/1) ↔ fourthinterfa... (Ethernet2/4)

[Add another pair](#)

CANCEL OK

Configura impostazioni

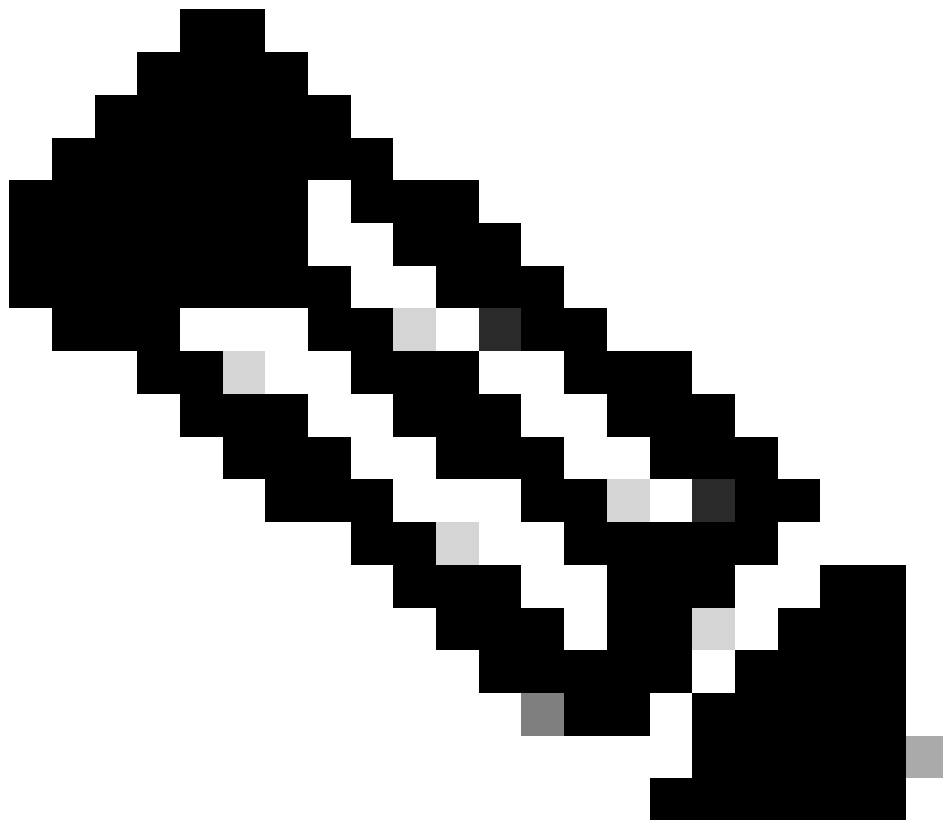
Bypass hardware

Funzionalità e limitazioni

- La funzione di bypass hardware assicura il flusso continuo del traffico tra una coppia di

interfacce in linea durante un'interruzione dell'alimentazione. Questa funzione può essere utilizzata per mantenere la connettività di rete in caso di errori software o hardware.

- Le porte di bypass hardware sono supportate solo per i set inline.
 - Bypass hardware NON supportato in modalità Alta disponibilità.
 - Modalità bypass hardware:
 - DISABLED - Disabilita il bypass sulle interfacce supportate. Modalità predefinita per interfacce non supportate.
 - STANDBY: nello stato di standby, le interfacce rimangono in funzionamento normale fino a quando non si verifica un evento trigger.
 - BYPASS FORCE - Impone manualmente alla coppia di interfacce di ignorare l'ispezione.
-



Nota: [Informazioni sui tipi di interfaccia FTD e sulla bypass hardware](#)

Snort Fail Open e bypass hardware

- La funzionalità di bypass dell'hardware consente il flusso del traffico durante un guasto hardware, inclusa un'interruzione completa dell'alimentazione e alcuni errori software limitati.
- Un errore software che attiva Snort Fail Open non attiva un bypass hardware.

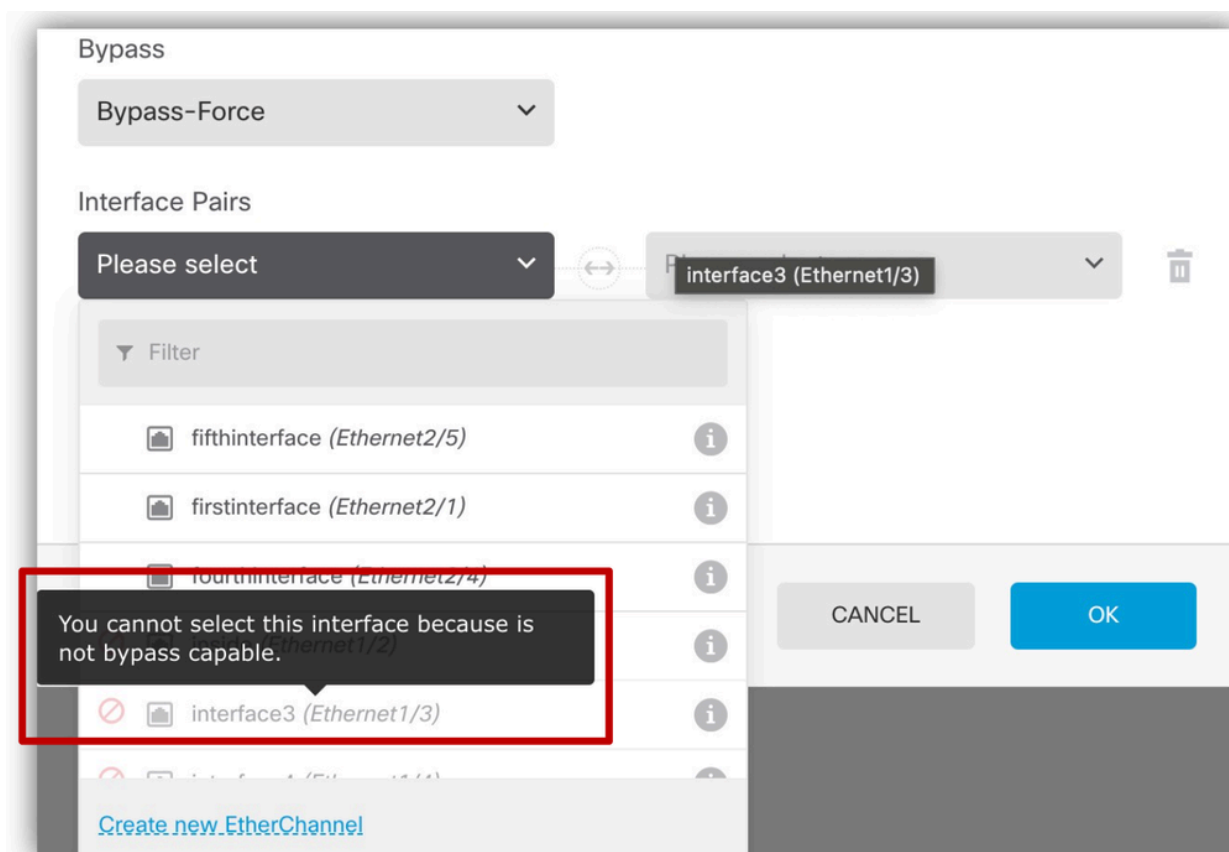
Trigger bypass hardware

Il bypass hardware può essere attivato nei seguenti scenari:

- Arresto anomalo dell'applicazione
- Riavvio applicazione
- Arresto anomalo dispositivo
- Riavvio o aggiornamento del dispositivo
- Interruzione dell'alimentazione del dispositivo
- Attivazione manuale

Per visualizzare le interfacce che supportano la funzione di bypass hardware:

- Dall'interfaccia utente di FDM, se è selezionato Bypass:
 - Le interfacce che la supportano sono selezionabili.
 - Le interfacce non supportate sono disattivate.
 - Per questo esempio, Ethernet1/3 è disattivato nella figura seguente:



Verifica supporto bypass hardware

Passaggio 3: Configurare le impostazioni in linea Impostazioni avanzate.

- Selezionare Dispositivo > Interfacce > scheda Insieme in linea o modificare un insieme in linea già creato.
- Passare alla scheda Avanzate.
 - La scheda Avanzate consente di configurare l'impostazione delle opzioni per i set in linea.

- Fare clic sulla scheda Avanzate.

Create New Inline Set

Name: inline_example MTU: 1500

General Advanced

Bypass: Standby

Interface Pairs:

firstinterface (Ethernet2/1) ↔ secondinterf... (Ethernet2/4)

[Add another pair](#)

CANCEL OK

Configura set inline

- Modalità
 - Tocca: Imposta la modalità tocco in linea. Se la modalità tocco è attivata, la funzione Snort Fail Open è disattivata.
 - In linea

Create New Inline Set

Name: inline_example MTU: 1500

General Advanced

Mode *i*

☐ Tap ☒ Inline

i Enabling " Snort Fail Open" might allow traffic unrestricted.

☒ Snort Fail Open ☐ Busy ☐ Down

☐ Propagate Link State

CANCEL OK

Modalità Select

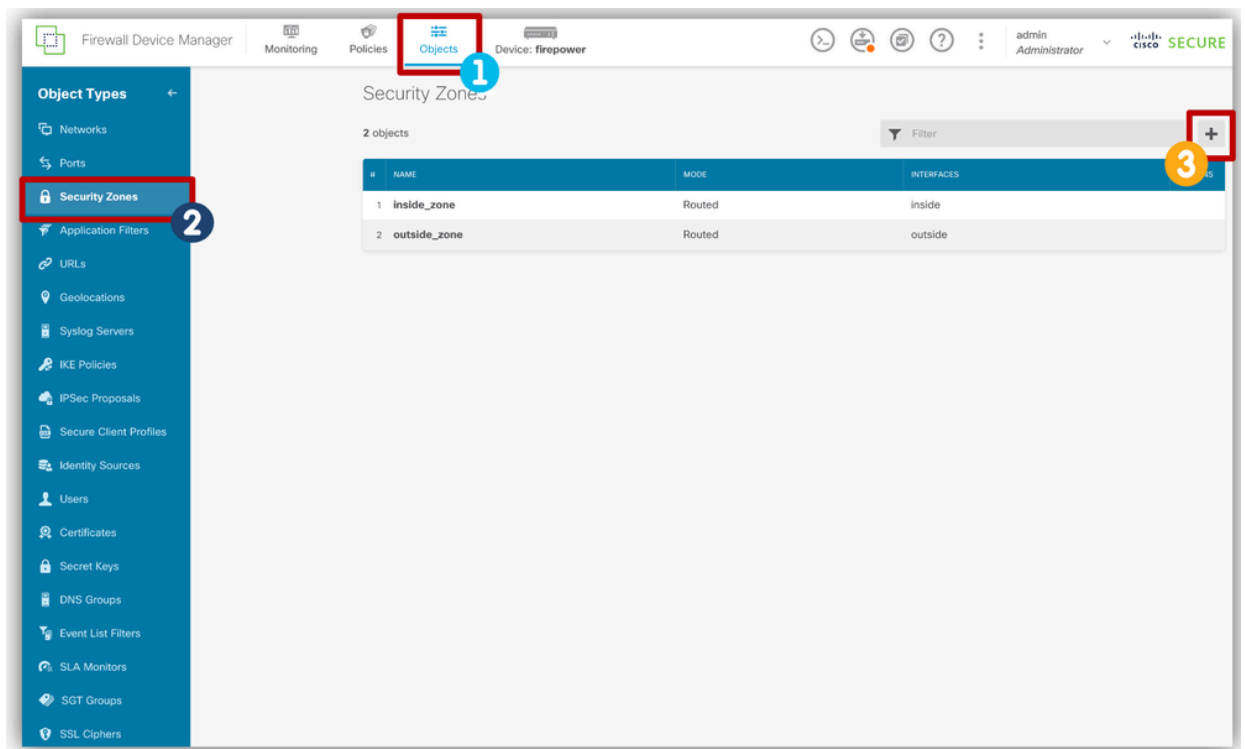
- Impostazioni di apertura Snort Fail.
 - Selezionare le impostazioni Snort Fail Open desiderate.
 - Nessuno, uno o entrambi. È possibile impostare le opzioni Occupato e Giù.
 - Snort Fail Open consente il passaggio di traffico nuovo ed esistente senza ispezione (abilitata) o perdita (disabilitata) quando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

Avvia apertura e propaga stato collegamento non riuscito

- Propaga stato collegamento.
 - Propaga stato collegamento riduce automaticamente la seconda interfaccia nella coppia in linea quando una delle interfacce diventa inattiva. Quando l'interfaccia di cui è stata eseguita la riattivazione è disponibile anche la seconda interfaccia.
- Fate clic su OK per creare l'insieme inline.

Passaggio 4: Applicare a un'area di sicurezza (facoltativo).

1. Dalla barra di navigazione in alto, passare a Oggetti.
2. Selezionare Aree di protezione dalla barra di navigazione a sinistra:
 - Fare clic su + per aggiungere l'area di protezione.



Aggiungi area di sicurezza

Configurare l'area di protezione (facoltativo)

1. Assegnare un nome all'area di protezione.
2. Selezionare Inline Mode.

Le aree di sicurezza e le interfacce devono avere la stessa modalità.

3. Selezionare le interfacce che fanno parte dell'insieme inline.
4. Fare clic su OK.

Add Security Zone?×

Name

test_sz

Description

Mode

☐ Routed

☐ Passive

☒ Inline

Interfaces

+

CANCEL

OK

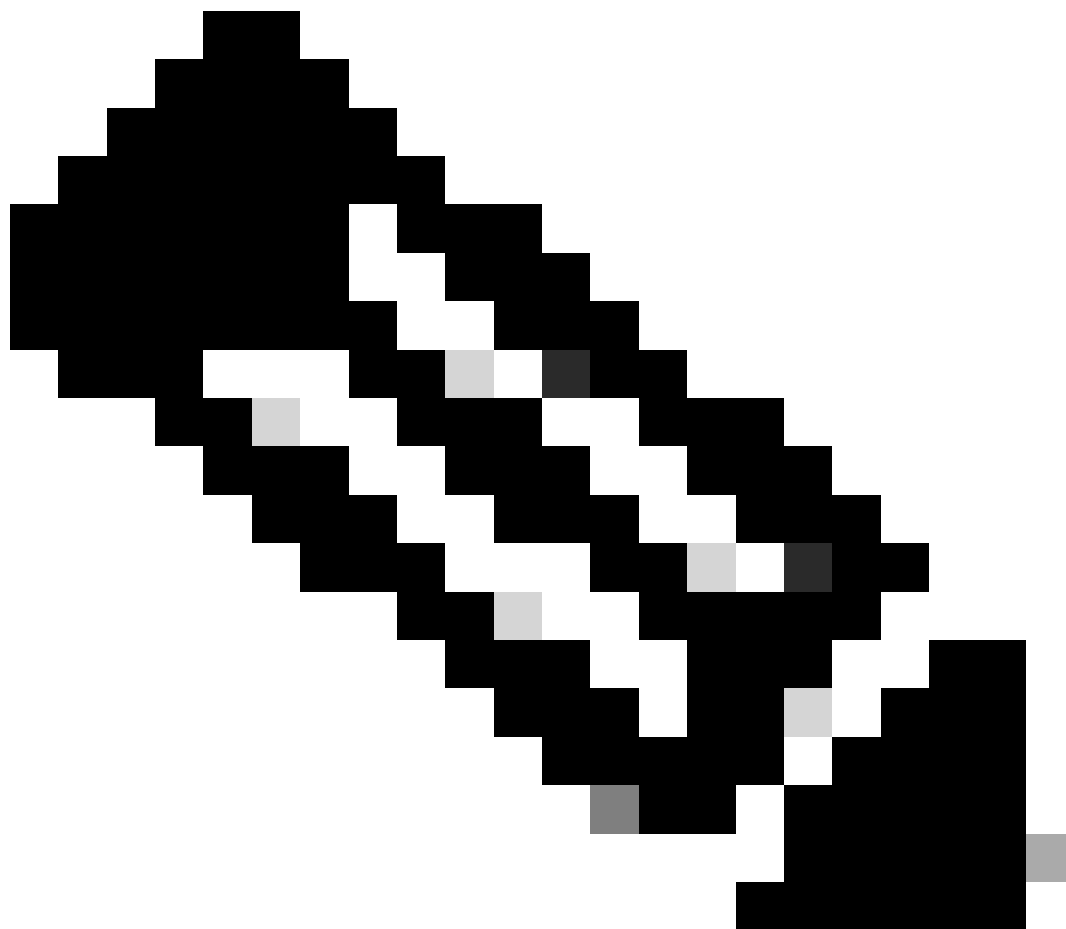
1

2

3

4

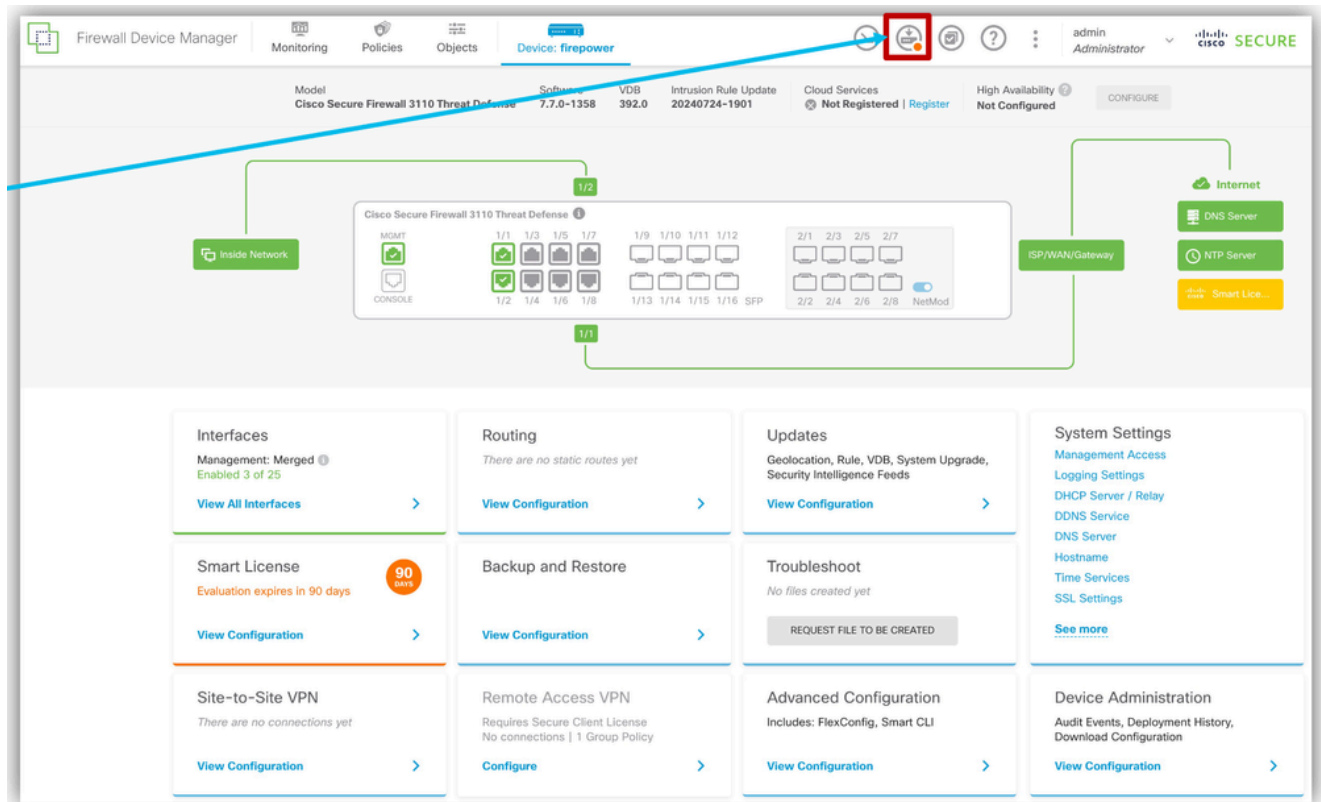
Configura area di protezione



Nota: Per le interfacce, la modalità passa automaticamente a Inline dopo l'aggiunta dell'interfaccia in una coppia inline.

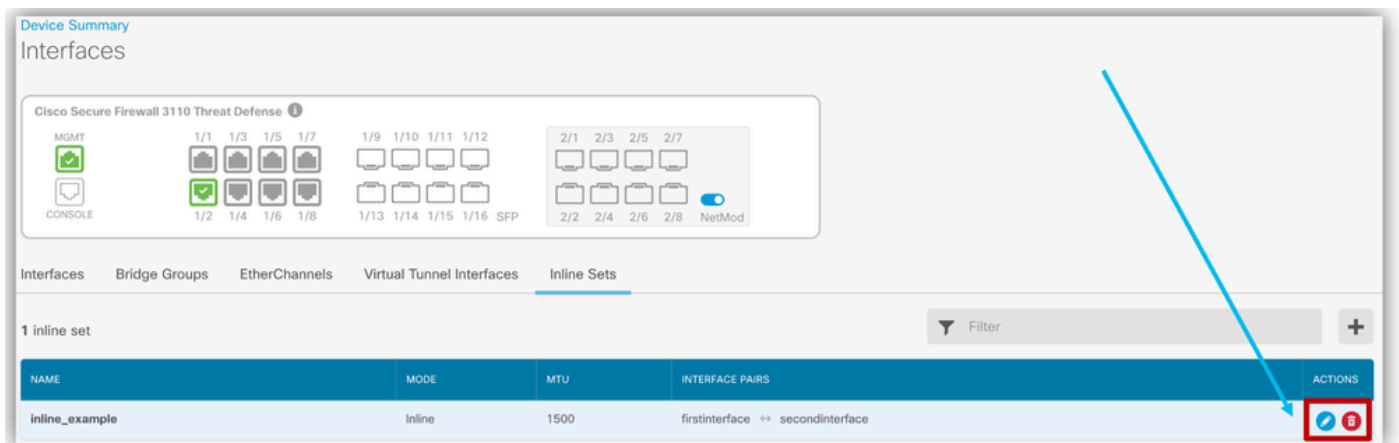
Passaggio 4: Implementazione

- Passare alla scheda Distribuzione e distribuire.



Distribuisce modifiche

- Modificare ed eliminare i set in linea.
 - Selezionare Dispositivo > Interfacce > scheda Insieme in linea.
 - I pulsanti Modifica ed Elimina sono disponibili per i set in linea.



Modifica ed elimina set inline

API REST dispositivo FDM

Endpoint API REST

- OTTIENI: /devices/default/inlinesets
Recupera un elenco di tutti i set in linea esistenti.

- GET: /devices/default/inlinesets/{objID}
Recupera un oggetto inline-set specifico in base al relativo ID.
- POST: /devices/default/inlinesets
Create un nuovo insieme inline.
- PUT: /devices/default/inlinesets/{idobj}
Aggiorna l'oggetto inline-set esistente in base al relativo ID.
- ELIMINA :/devices/default/inlinesets/{objID}
Elimina l'oggetto inline-set esistente in base al relativo ID.
- GET: /operating/interfaceinfo/{objID}
Recuperate un elenco di tutte le entità InterfaceInfo.
- Per supportare Hardware Bypass, è stato aggiunto un nuovo campo all'API InterfaceInfo.

Informazioni sull'interfaccia - Modelli API REST

- È stato aggiunto un nuovo campo bypassInterfacePeerId per facilitare l'integrazione di Bypass hardware.
- Questo campo rappresenta l'ID della coppia di interfacce di bypass hardware per l'interfaccia corrente.
- Valori:
 - Null - l'interfaccia non supporta il bypass.
 - ID: l'interfaccia supporta il bypass.

```
{ "interfaceInfoList":  
  [ {  
    "interfaceId": "string",  
    "hardwareName": "string",  
    "bypassInterfacePeerId": "string",  
    "speedCapability": [ "SFP_DETECT" ],  
    "duplexCapability": [ "AUTO" ],  
    "interfacePresent": true,  
    "splitInterface": true,  
    "autoNegCapable": true,  
    "id": "string",  
    "type": "InterfaceInfoEntry"  
  } ],  
  "id": "string",  
  "type": "InterfaceInfo",  
  "links":  
  {  
    "self": "string"  
  }  
}
```

API REST Informazioni interfaccia

Esempio di API REST di informazioni sull'interfaccia

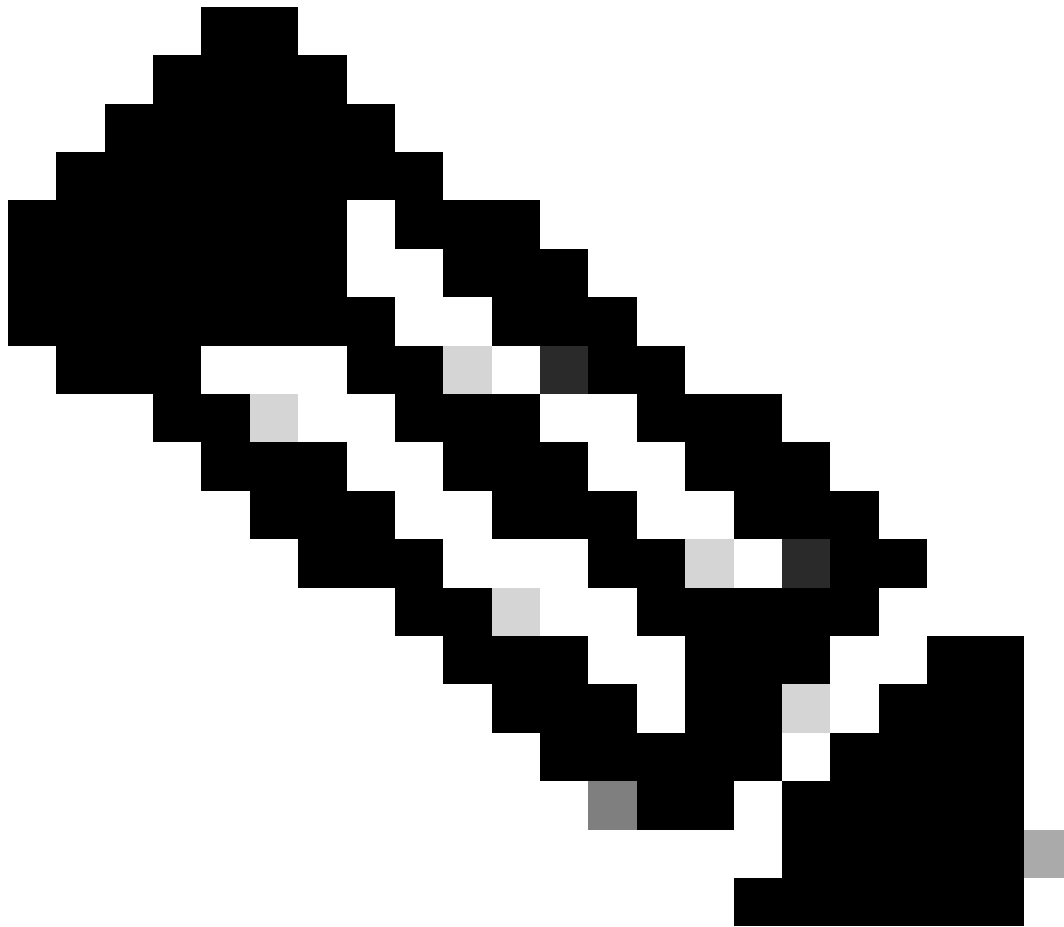
- Esempio di API REST di informazioni sull'interfaccia.
 - Interfaccia senza supporto bypass hardware (Ethernet 1/4).
 - Coppia di interfacce con supporto bypass hardware (Ethernet2/1 ed Ethernet 2/2).


```

{ "interfaceInfoList": [
  {
    "interfaceId": "da9edc2d-58ba-11ef-b764-ffea0b8d9fa2",
    "hardwareName": "Ethernet1/4",
    "bypassInterfacePeerId": null,
    ...
  },
  {
    "interfaceId": "dbe9d2c1-58ba-11ef-b764-396644d1c752",
    "hardwareName": "Ethernet2/1",
    "bypassInterfacePeerId": "dc74fbc3-58ba-11ef-b764-11d423dbcb7",
    ...
  },
  {
    "interfaceId": "dc74fbc3-58ba-11ef-b764-11d423dbcb7",
    "hardwareName": "Ethernet2/2",
    "bypassInterfacePeerId": "dbe9d2c1-58ba-11ef-b764-396644d1c752",
    ...
  }
],
"id": "default",
"type": "interfaceinfo",
"links": { "self": "https://u90c04p02-
vrouters.cisco.com:25455/api/fdm/v6/operational/interfaceinfo/1/default"
}
}

```

Esempio di API REST di informazioni sull'interfaccia



Nota: Frammento della chiamata completa, a causa delle dimensioni.

Modello Inline Set REST API

- Il modello Inline Set è costituito da:
 - Tipo
 - Nome
 - Modalità tocco
 - MTU
 - Propaga stato collegamento
 - Errore apertura snort occupata
 - Ignora valori: DISABILITATO, STANDBY, BYPASS_FORCE

```

{
  "id": "string",
  "type": "string",
  "name": "string",
  "tapMode": "boolean", //(optional) false by default
  "mtu": "integer", //(optional) 1500 by default
  "propagateLinkState": "boolean", //(optional) false by default
  "failOpenSnortBusy": "boolean", //(optional) false by default
  "failOpenSnortDown": "boolean", //(optional) false by default
  "bypass": "string", //(optional) DISABLED by default
  "inlinePairs":
  [{
    "first": {
      "id": "string",
      "type": "physicalinterface",
      "name": "string"
    },
    "second": {
      "id": "string",
      "type": "physicalinterface",
      "name": "string"
    },
    "type": "inlinesetpair"
  }], // list can be empty
  "links": {
    "self": "string"
  }
}

```

Sec FW 7.7.0 IFT TOI: FDM HW Bypass with
Inline Sets Page 58

API REST set inline

Esempio di API REST Set inline

- Esempi di set in linea di base con:

- Una coppia inline
- Ignora standby

```
{
  "name": "inline_set_example",
  "type": "inlineset",
  "tapMode": false,
  "mtu": 1500,
  "propagateLinkState": false,
  "failOpenSnortBusy": false,
  "failOpenSnortDown": true,
  "bypass": "STANDBY",
  "inlinePairs": [
    {
      "first": {
        "id": "12345-6789-1234-56789",
        "type": "physicalinterface"
      },
      "second": {
        "id": "12345-6789-1234-56789",
        "type": "physicalinterface"
      },
      "type": "inlinesetpair"
    }
  ]
}
```

2.Create Inline Set (vedere API Explorer per esempi di payload).

POST/dispositivi/predefiniti/set inline

3.Create Security Zone (vedere API Explorer per gli esempi di payload) (facoltativo).

POST/oggetto/zone di sicurezza

4.Distribuire sul dispositivo (per gli esempi di payload, vedere API Explorer).

POST/operativo/installazione

Configurazione e distribuzione di un set inline con bypass hardware

1. Ottenere gli ID di interfaccia e le informazioni sulle coppie di interfacce di bypass hardware (vedere API Explorer per esempi di payload).

GET/operating/interfaceinfo/{objId}

2.Create Inline Set (vedere API Explorer per esempi di payload).

POST/dispositivi/predefiniti/set inline

3.Create Security Zone (vedere API Explorer per gli esempi di payload) (facoltativo).

POST/oggetto/zone di sicurezza

4.Distribuire sul dispositivo (per gli esempi di payload, vedere API Explorer).

POST/operativo/installazione

Modifica di un set in linea

1. Ottenere gli ID di interfaccia (vedere gli esempi di payload in Esplora API).

GET/devices/default/interfaces

2. Ottieni set inline.

GET/devices/default/inlinesets

3. Modificare il set inline (vedere API Explorer per esempi di payload).

PUT/devices/default/inlinesets/{objId}

4. Distribuire sul dispositivo (per esempi sul payload, vedere Esplora API).

POST/operativo/installazione

Verifica

```
<#root>
```

```
> show running-config inline-set
```

```
inline-set test_inline_0
  interface-pair test2 test1
inline-set test_inline_1
```

```
hardware-bypass standby
```

```
  interface-pair test27 test28
```

```
inline-set test_inline_2
  hardware-bypass bypass
  interface-pair test26 test25
```

> show inline-set

```
Inline-set test_inline_0
  Mtu is 1600 bytes
  Fail-open for snort down is off
  Fail-open for snort busy is off
  Tap mode is off
  Propagate-link-state option is off
```

hardware-bypass mode is disabled

```
Interface-Pair[1]:
  Interface: Ethernet1/3 "test1"
  Current-Status: DOWN
  Interface: Ethernet1/4 "test2"
  Current-Status: DOWN
  Bridge Group ID: 519
```

> show inline-set

```
Inline-set test_inline_1
  Mtu is 1500 bytes
  Fail-open for snort down is off
  Fail-open for snort busy is off
  Tap mode is off
  Propagate-link-state option is off
  hardware-bypass mode is standby
  Interface-Pair[1]:
  Interface: Ethernet2/7 "test27"
  Current-Status: DOWN
  Interface: Ethernet2/8 "test28"
  Current-Status: DOWN
  Bridge Group ID: 618
```

> show inline-set

```
Inline-set test_inline_1
  Mtu is 1500 bytes
  Fail-open for snort down is off
  Fail-open for snort busy is off
  Tap mode is off
  Propagate-link-state option is off
```

hardware-bypass mode is bypass

```
Interface-Pair[1]:
  Interface: Ethernet2/6 "test26"
  Current-Status: DOWN
  Interface: Ethernet2/5 "test25"
  Current-Status: DOWN
  Bridge Group ID: 610
```

```
> show interface
```

```
...
```

```
Interface Ethernet1/7 "", is admin down, line protocol is down  
Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec  
Available but not configured via nameif
```

```
...
```

```
Interface Ethernet2/7 "", is admin down, line protocol is down  
Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
```

Hardware bypass is supported with interface Ethernet2/8

Available but not configured via nameif

```
...
```

```
Interface Ethernet2/8 "", is admin down, line protocol is down  
Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
```

Hardware bypass is supported with interface Ethernet2/7

Available but not configured via nameif

Risoluzione dei problemi

Comandi

- show running-config inline-set
- show inline-set
- show interface
- traccia supporto di sistema

Set in linea - Convalide durante la creazione

- Gli errori vengono presentati sulla GUI per ciascun campo.
 - È necessario specificare il nome.
 - La dimensione MTU deve essere almeno 1500.
 - È necessario selezionare entrambe le interfacce di una coppia.

Edit New Inline Set

Name

MTU

Cannot be blank

The MTU must be between 1500 and 9198.

General Advanced

Bypass

Disabled

Interface Pairs

fifthinterface (Ethernet2/5) ↔ Please select

Interface Pair can't be partially empty.

[Add another pair](#)

CANCEL OK

Dimensioni MTU

Bypass hardware - Convalida durante la creazione

- Quando il bypass è abilitato, sulla GUI vengono visualizzati nuovi errori per ognuno dei campi:
 - Tutte le interfacce devono supportare Bypass.
 - Errore: le interfacce non sono supportate.
 - Tutte le coppie devono utilizzare la coppia di interfacce predeterminata.
 - Il messaggio di errore indica le coppie di interfacce di bypass disponibili.

Edit New Inline Set



- ✗ Invalid interface pair for Bypass. Interface Ethernet2/4 can be paired with Ethernet2/3.
- ✗ Invalid interface pair for Bypass. Interface Ethernet2/5 can be paired with Ethernet2/6.
- ✗ Bypass is not available for Interface Ethernet1/3.
- ✗ Bypass is not available for Interface Ethernet1/4.

Name

test

MTU

1500

General

Advanced

Bypass

Standby



Interface Pairs

firstinterface (Ethernet2/1)



secondinterf... (Ethernet2/2)



fourthinterfa... (Ethernet2/4)



fifthinterface (Ethernet2/5)



This pair of interfaces does not support the selected bypass mode.

interface3 (Ethernet1/3)



interface4 (Ethernet1/4)

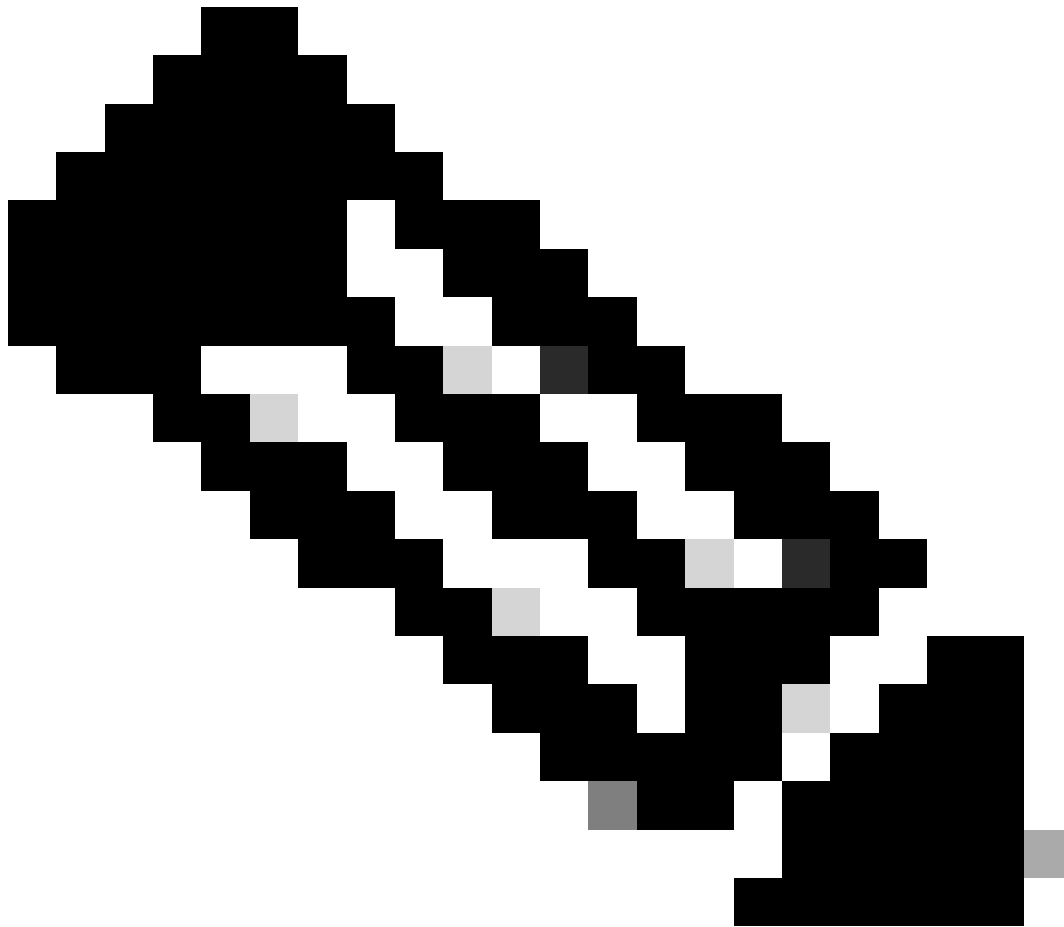


This pair of interfaces does not support the selected bypass mode.

[Add another pair](#)

CANCEL

OK



Nota: La prima coppia (Ethernet2/1-Ethernet2/2) è valida.

La risposta dell'API REST mostra gli errori

- Gli errori sono presentati nella risposta dell'API REST.
 - Il valore MTU non è valido.

Response Body

```
{
  "error": {
    "severity": "ERROR",
    "key": "Validation",
    "messages": [
      {
        "description": "Invalid MTU value. The MTU should be greater
than or equal to 1500.",
        "code": "invalidMtuValueInInlineSet",
        "location": "mtu"
      }
    ]
  }
}
```

Response Code

422

Convalida API REST

Limitazioni dell'implementazione per questa release

- Set in linea: Funziona solo con interfacce fisiche ed EtherChannel.
- Set inline con bypass hardware: Funziona solo con interfacce fisiche e richiede un modulo di rete.

Funzionalità firewall non supportate sulle interfacce inline

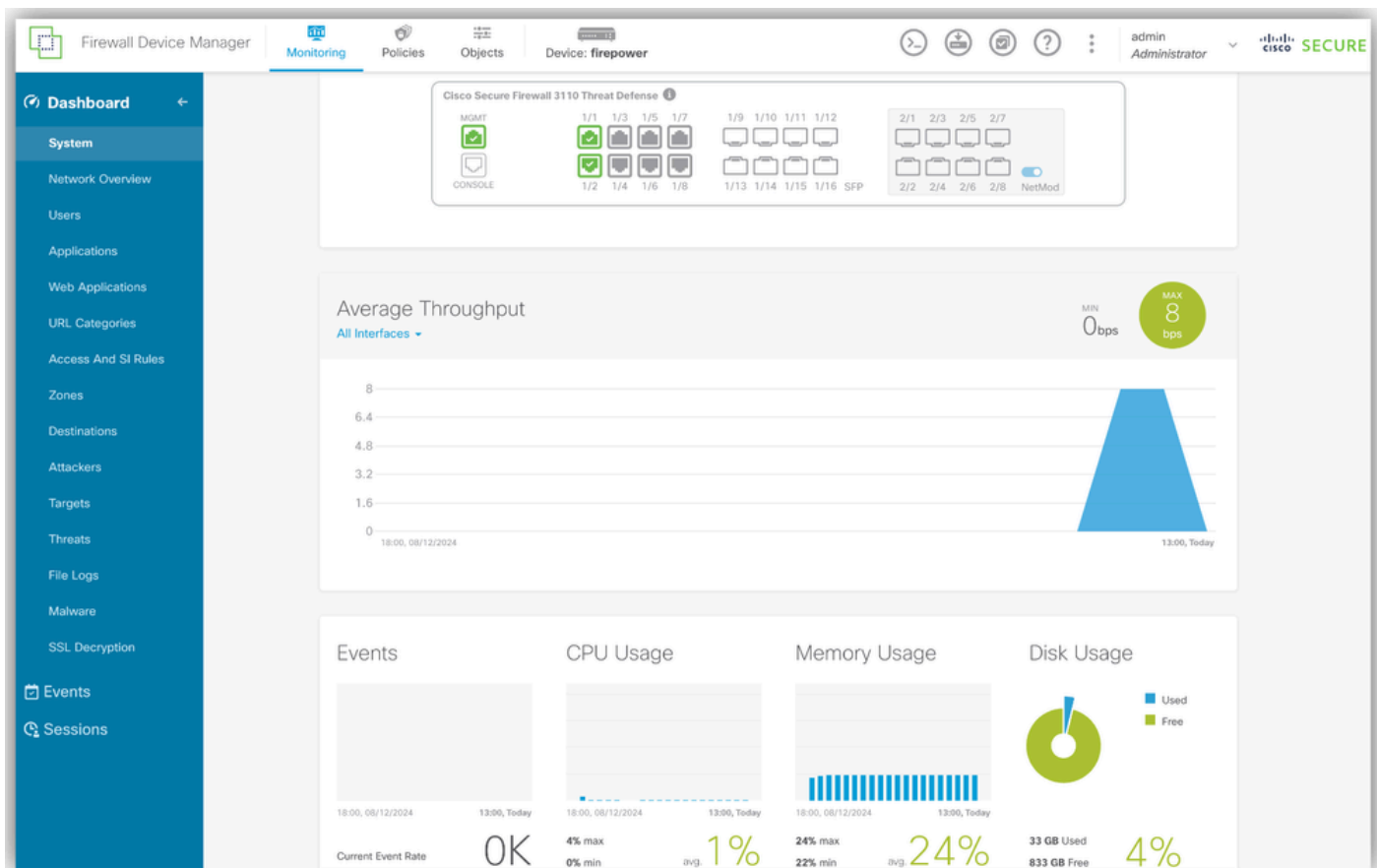
- Server DHCP
- inoltro DHCP
- client DHCP
- TCP Intercept
- Routing
- NAT
- VPN
- Applicazione
- ispezione
- QoS
- NetFlow

Verifica dei log dalla CLI

- Registrazione.
 - I registri sono disponibili in /ngfw/var/log/cisco/ngfw-onbox.log.
 - Cerca set inline.
 - Esempio di possibili errori rilevati nei registri:
 - Due interfacce non supportano il bypass.
 - Due interfacce non sono una coppia di bypass valida.

```
root@FPR-3110-Pair:/home/admin# cd /ngfw/var/log/cisco/
root@FPR-3110-Pair:/ngfw/var/log/cisco# cat ngfw-onbox.log | grep "InlineSet"
2024-08-28 12:35:00 ajp-nio-8009-exec-1: ERROR InlineSetValidator: 548 - Invalid
interface pair for Bypass. Interface Ethernet2/4 can be paired with Ethernet2/3.
2024-08-28 12:35:00 ajp-nio-8009-exec-1: ERROR InlineSetValidator:548 - Invalid
interface pair for Bypass. Interface Ethernet2/5 can be paired with Ethernet2/6.
2024-08-28 12:35:00 ajp-nio-8009-exec-1: ERROR InlineSetValidator:541 - Bypass
is not available for Interface Ethernet1/3.
2024-08-28 12:35:00 ajp-nio-8009-exec-1: ERROR InlineSetValidator:541 - Bypass
is not available for Interface
```

- Verificare il traffico dalla GUI.
 - Gli eventi vengono presentati sulla GUI.
 - Qui è possibile monitorare la correttezza del flusso del traffico.
 - Selezionare Monitoraggio > Sistema.



Monitoraggio FDM

- Verificare la correttezza del traffico dalla CLI.

<#root>

```
> system support trace
Enable firewall-engine-debug too? [n]:
Please specify an IP protocol: ICMP
Please specify a client IP address:
Please specify a server IP address:
Monitoring packet tracer debug messages
```

[packets show up here]

Wireless LAN Controller serie 9800

Q: Ha è supportato con i set inline su FDM?

R: Sono supportati i set inline senza bypass.

I set inline con bypass NON sono supportati.

Q: Le BPDU Spanning-Tree sono bloccate sulla coppia inline-set?

A: No, non sono bloccati.

Q: Le schede FTW sono supportate in 3100?

A: Sì, le netmod FTW sono supportate da quando la serie 3100 è stata introdotta con 7.1/9.17. La funzione di bypass hardware è disponibile a partire dalla versione 7.7.0.

Q: Per le schede 3100 FTW, le modalità Bypass di Disabled, Standby, Bypass-Force come su FMC sono supportate o meno?

A: Il bypass hardware è disponibile a partire dalla versione 7.7.0 sui dispositivi 3100 con schede FTW.

Q: Sono supportati gli Inline-Set con canali porte dove il traffico è asimmetrico anche attraverso i canali porte?

A: Non viene eseguita alcuna convalida sulla velocità configurata PortChannel, a condizione che sia supportata dall'FTD.

Q: Nel caso in cui lo snort non riesca a eseguire l'ispezione, failopen è supportato?

A: Consultare la documentazione relativa a questa impostazione nella [Guida alla configurazione di Firepower Management Center](#).

Informazioni correlate

- [Configurazione delle interfacce FTD in modalità Inline-Pair](#)
- [Guida alla configurazione di Firepower Management Center, versione 6.3](#)
- [Guida all'installazione dell'hardware di Cisco Secure Firewall serie 3100](#)
- [Scheda tecnica di Cisco Secure Firewall serie 3100](#)

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).