

Beveiligde firewall 3100 configureren FDM 7.7.0

Hardware Bypass

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Basisprincipes: ondersteunde platforms, licenties](#)

[Kenmerken Beschrijving en Walkthrough](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Hardware-bypass](#)

[FDM Device REST API's](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Opdrachten](#)

[Inline set -validaties bij het maken](#)

[Hardware bypass - validatie bij het maken](#)

[Beperkingen van de implementatie voor deze release](#)

[Niet-ondersteunde firewallfuncties op inline interfaces](#)

Inleiding

In dit document wordt beschreven hoe u Hardware Bypass configureert voor inline sets in Firepower Device Manager (FDM) Managed Secure Firewall 7.7.0.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Inline-sets
- Secure Firewall 3100-reeks
- Firepower Device Manager Graphical User Interface (GUI)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De functie Inline Sets is toegevoegd aan FDM in 7.4.1. Inline-sets maken inspectie op een L2-netwerk mogelijk zonder routing: [FTD-interfaces configureren in inline-pairmodus](#)

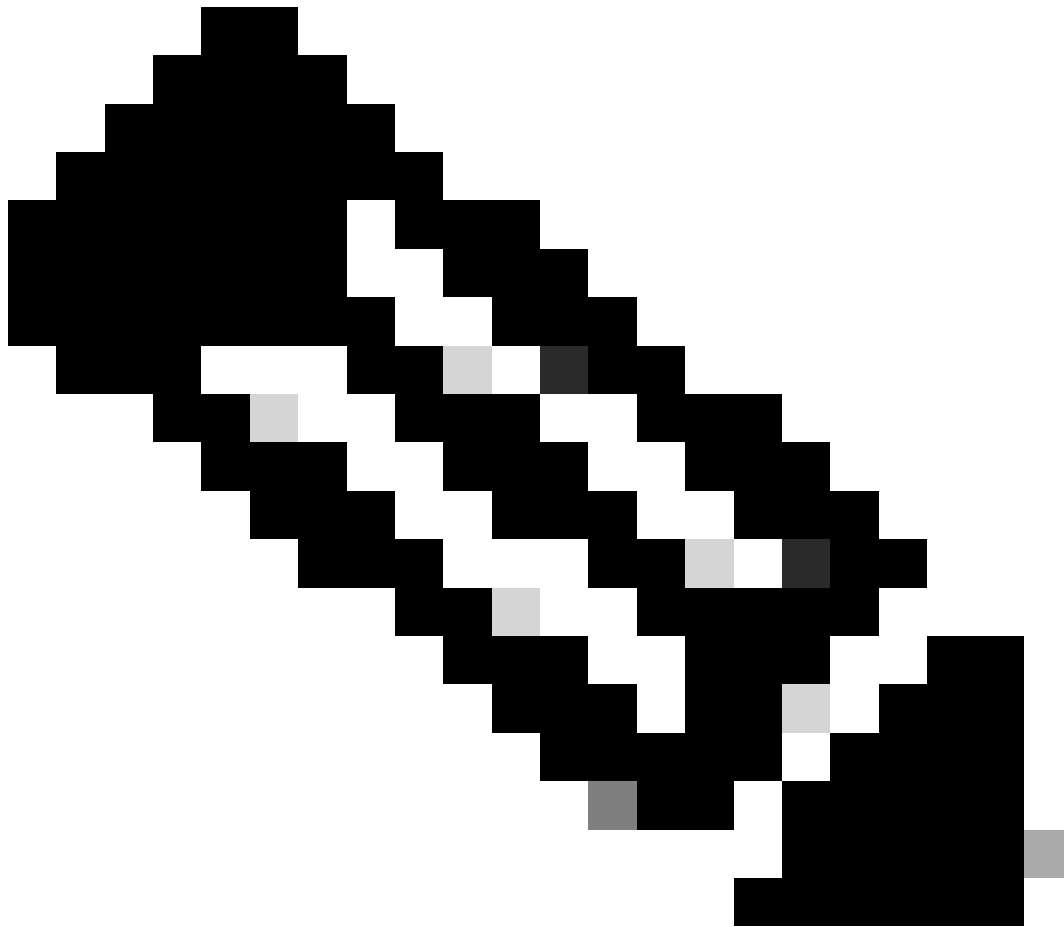
In tegenstelling tot de vorige release

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.

Beveiligde firewall 7.0-bypassfunctie

Wat is nieuw

- Hardware Inspection Bypass zorgt ervoor dat het verkeer blijft stromen tussen een Inline Interface Pair tijdens een stroomstoring.
- Deze functie wordt gebruikt om de netwerkconnectiviteit te behouden in het geval van software- of hardwarestoringen.
- Hardware Bypass is nu beschikbaar voor Inline Sets voor FDM 3100 Series-platforms.



Opmerking: [Configuratiehandleiding Firepower Management Center](#)

Implementatiescenario's

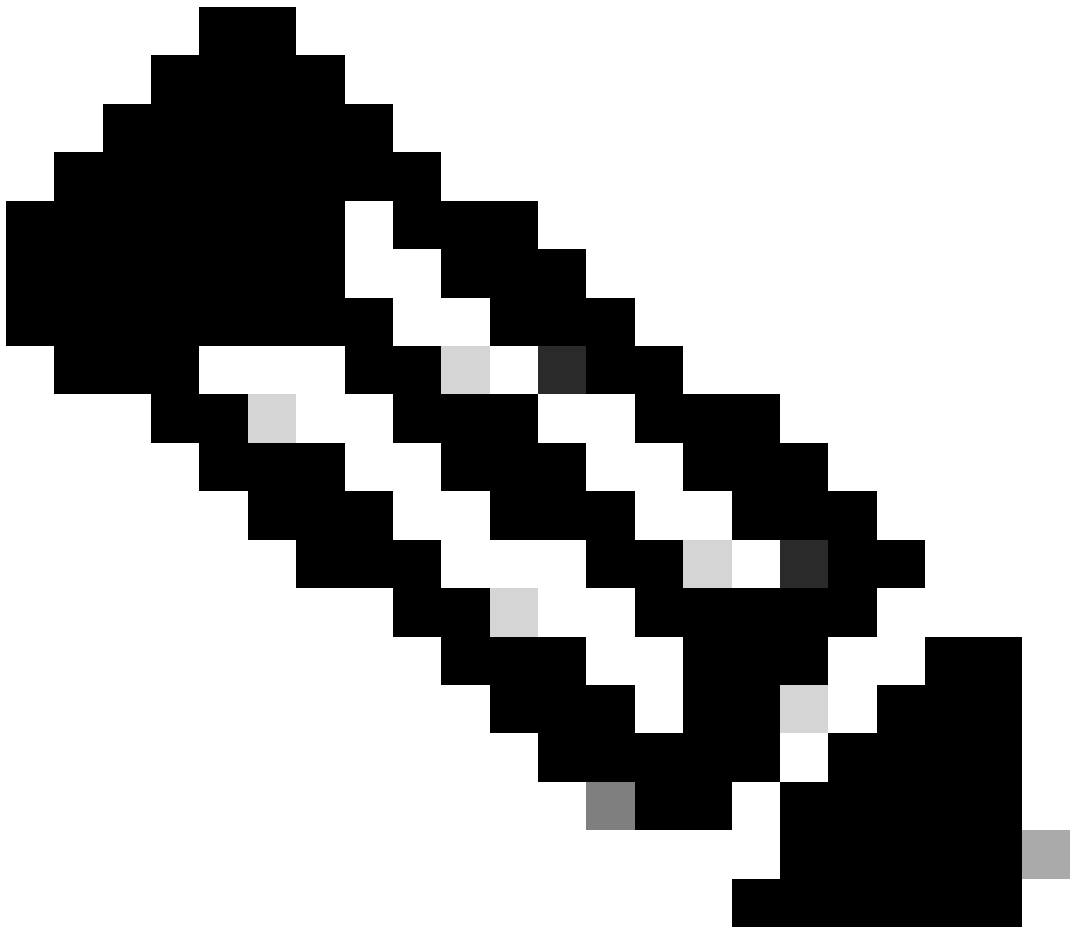
- Hoe zou deze functie passen in een productie-installatie?
 - Inline sets worden gebruikt voor een IPS (of IDS) use case.
 - Maakt verkeersinspectie mogelijk zonder dat routeringsconfiguraties nodig zijn. Stelt verkeersstromen toe als de eenheid uitvalt via Hardware Bypass.
- . Praktische voorbeelden:
 - Stel laag 2-netwerkinspectie overal op een snelle en eenvoudige manier in - zonder de noodzaak van laag 3.
 - Kritiek voor netwerken die volledig geïsoleerd zijn - geen toegang tot internet.
 - Transparante inline insertie voor diepe pakketinspectie voor standalone firewall - bestaande productielaag 2 architectuur.

Basisprincipes: ondersteunde platforms, licenties

Software- en hardwareversies

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 en hardware



Opmerking: [informatie over de 3100-reeks en de hardware-bypass](#)

Andere aspecten van ondersteuning

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

Licenties en compatibiliteit

Kenmerken Beschrijving en Walkthrough

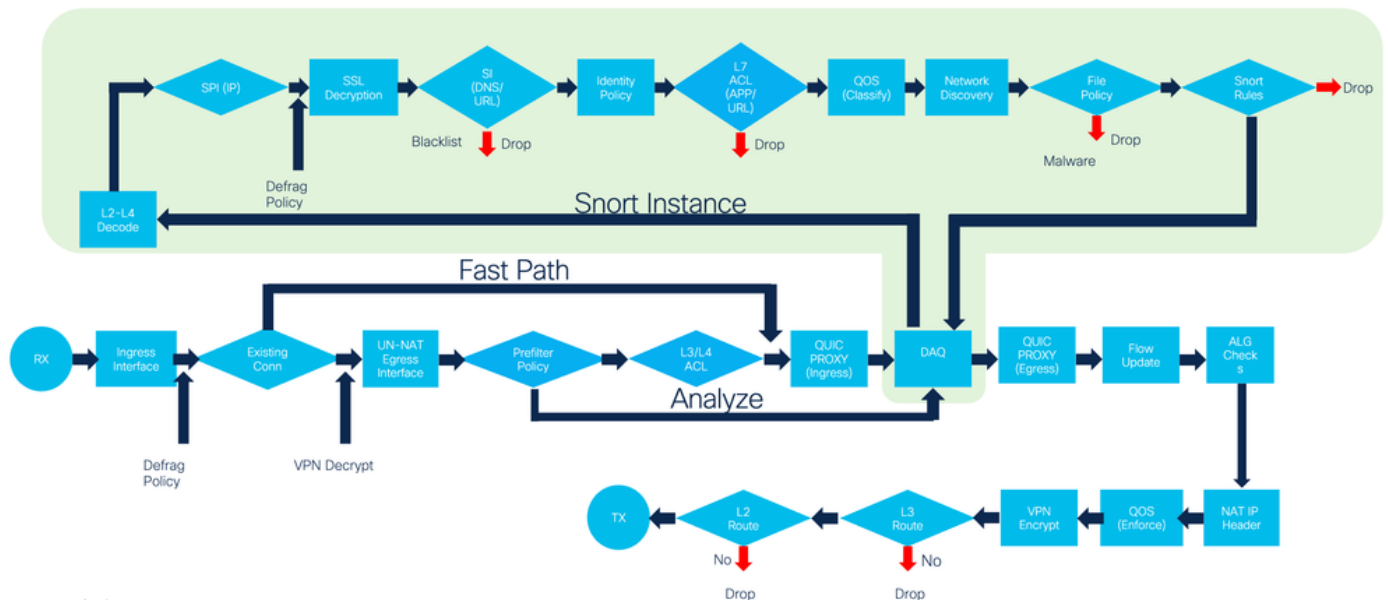
Functionele functiebeschrijving

- inline set netwerkdiagram



inline set netwerkdiagram

- Het verkeer stroomt van router 1 naar router 2, via interfaces A en B, waarbij alleen een fysieke verbinding wordt gebruikt.
- FDM Inline Sets Packet Processing Flow Diagram:



stroomschema

- Inline sets:
 - Inline Sets worden ondersteund op fysieke interfaces en EtherChannels.
- Hardware-bypass:
 - Inline sets met hardware bypass worden ondersteund op vooraf bepaalde fysieke interfaceparen:
 - Ethernet 1 en 2
 - Ethernet 2 en 3
 - Ethernet 4 en 5
 - Ethernet 5 en 6
- Interfaceondersteuning:
 - Interfaces die deel uitmaken van een inline-paar:
 - Moet benoemd worden.
 - Wees vrij van elke IConfiguraties van P, DHCP of PPPoE.
 - Niet in de passieve modus.
 - Het mag geen beheerinterface zijn.
 - Moet in slechts één inline paar tegelijk worden gebruikt.
- Details van de inline modus
 - De inline-modus is beschikbaar voor fysieke interfaces, etherkanalen en beveiligingszones.
 - De inline-modus wordt automatisch ingesteld voor interfaces en etherkanalen wanneer deze in een inline-paar worden gebruikt.
 - De inline modus voorkomt dat wijzigingen worden aangebracht op de betrokken interfaces en etherkanalen totdat deze uit het inline paar worden verwijderd.
 - Interfaces die zich in de inline-modus bevinden, kunnen worden gekoppeld aan beveiligingszones die zijn ingesteld op de inline-modus.

- Inline-modus GUI
 - Het dialoogvenster Interface bewerken geeft aan dat de interface of EtherChannel zich in de inline-modus bevindt.
 - Wijzigingen zijn niet toegestaan op interfaces wanneer deze zich in de inline-modus bevinden. Het dialoogvenster Fysieke interface bewerken (of EtherChannel bewerken) is alleen-lezen.

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:

Interface bewerken in GUI

- Upgrade, importeren/exporteren, back-up/herstel, implementeren
 - Implicaties van upgrade
De gebruiker kan zonder beperkingen FDM upgraden.
Bij het upgraden van een eerdere versie worden bestaande Inline Set-objecten geconfigureerd met het bypass-veld ingesteld op Uitgeschakeld.
 - Gevolgen van import/export
Inline Set-objecten worden geïmporteerd en geëxporteerd.
 - Back-up/herstel
Inline Set-objecten worden behandeld tijdens back-up/herstel.
 - Implementeren
Objecten worden normaal geïmplementeerd.
Er werden specifieke fouten gemaakt.

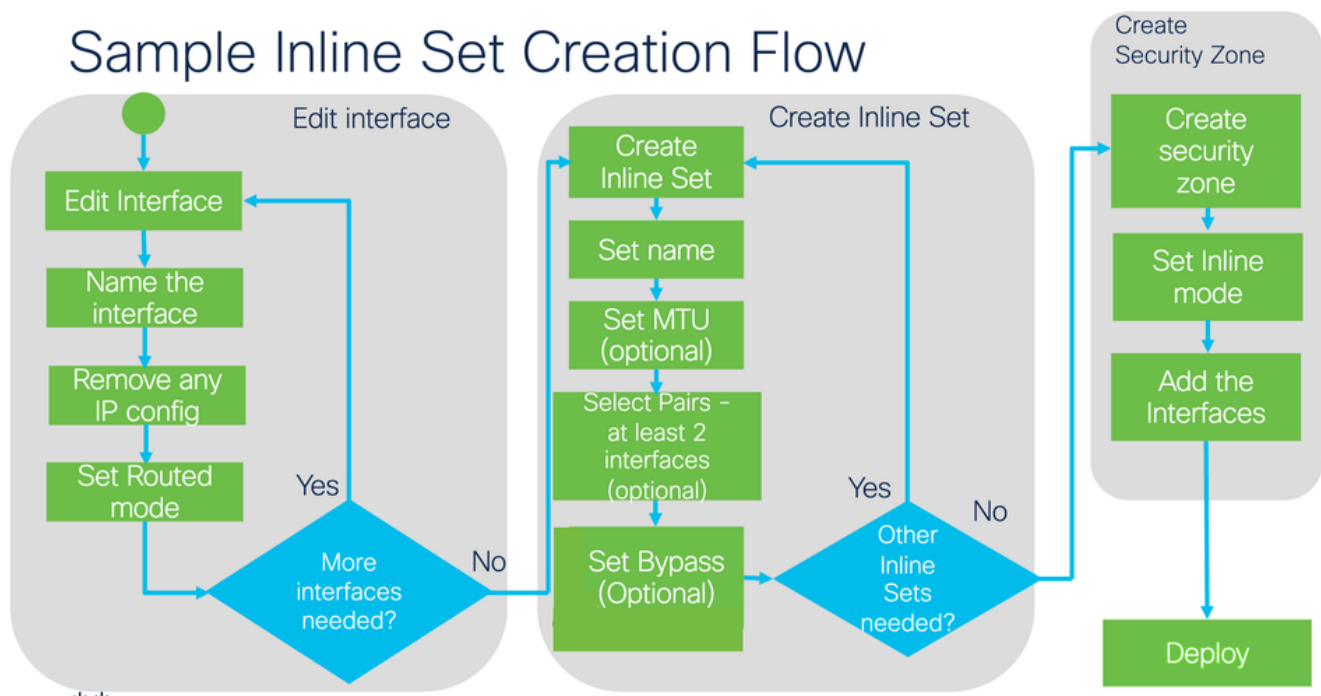
Configureren

Netwerkdigram



Netwerkdigram

Sample Inline Set Creation Flow



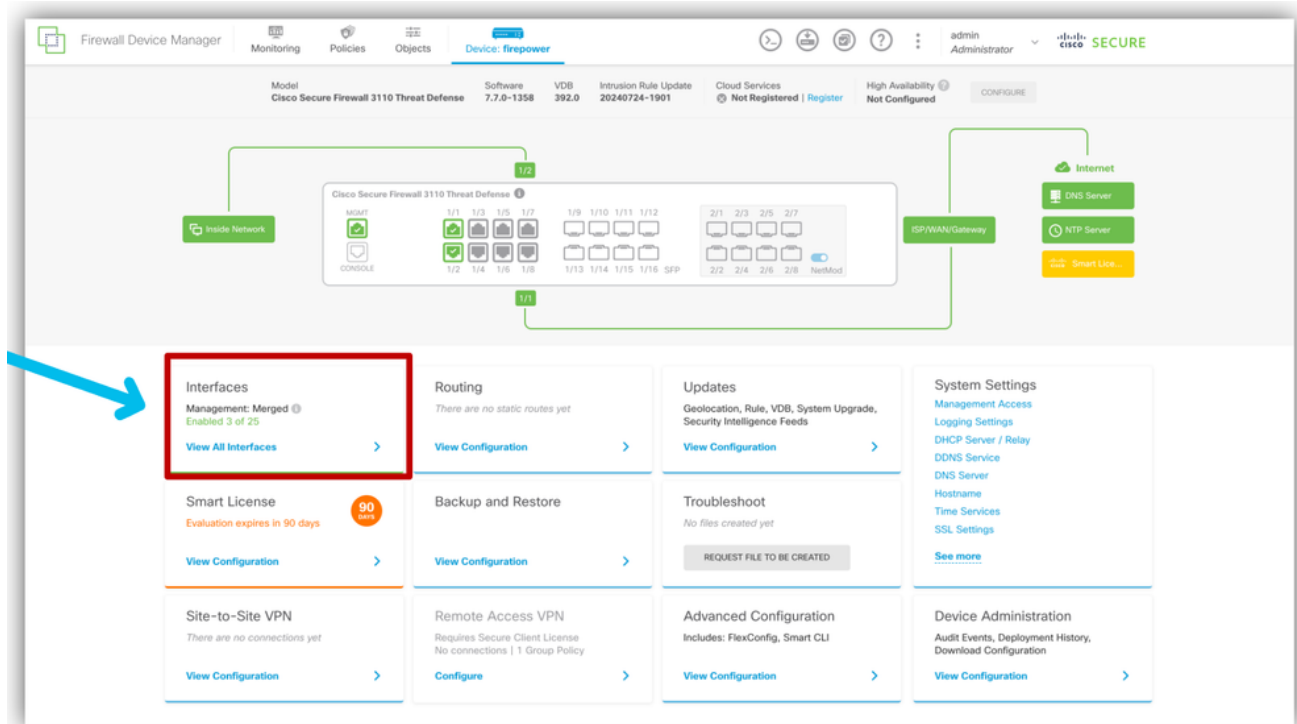
Inline set aanmaakstroom

Configuraties

In dit gedeelte worden de stappen beschreven voor het configureren van Hardware Bypass op FDM

Stap 1: Interfaces bewerken.

- Log in bij FDM en n navigeren naar Interfacebeheer.
- Klik in het FDM-dashboard op de kaart Interfaces.



Interface selecteren

- Bewerk de interfaces die worden gebruikt in de inline set.
- Om interfaces te bewerken, klikt u op het pictogram Bewerken (potlood) voor de interface.

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	

Interface bewerken

- Fysieke interface bewerken:
 1. Noem de interface.

2. Selecteer gerouteerde modus.
3. Verwijder elke IP-configuratie.

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

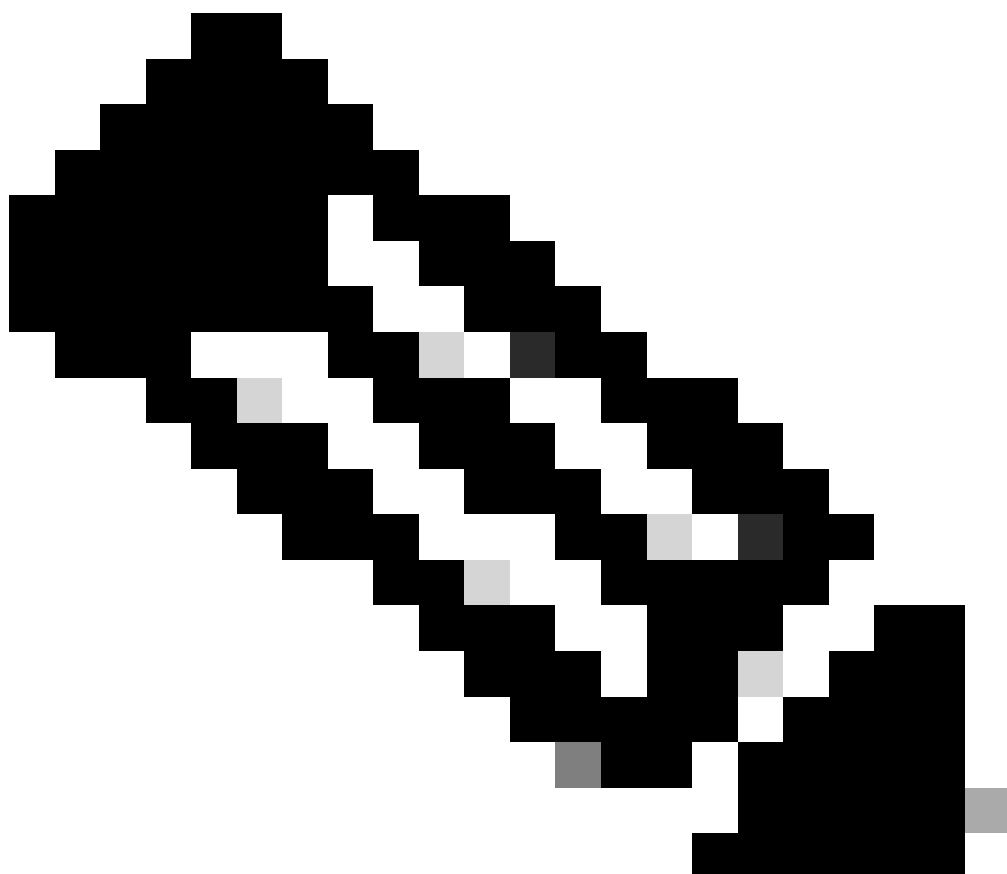
/

e.g. 192.168.5.16

CANCEL

OK

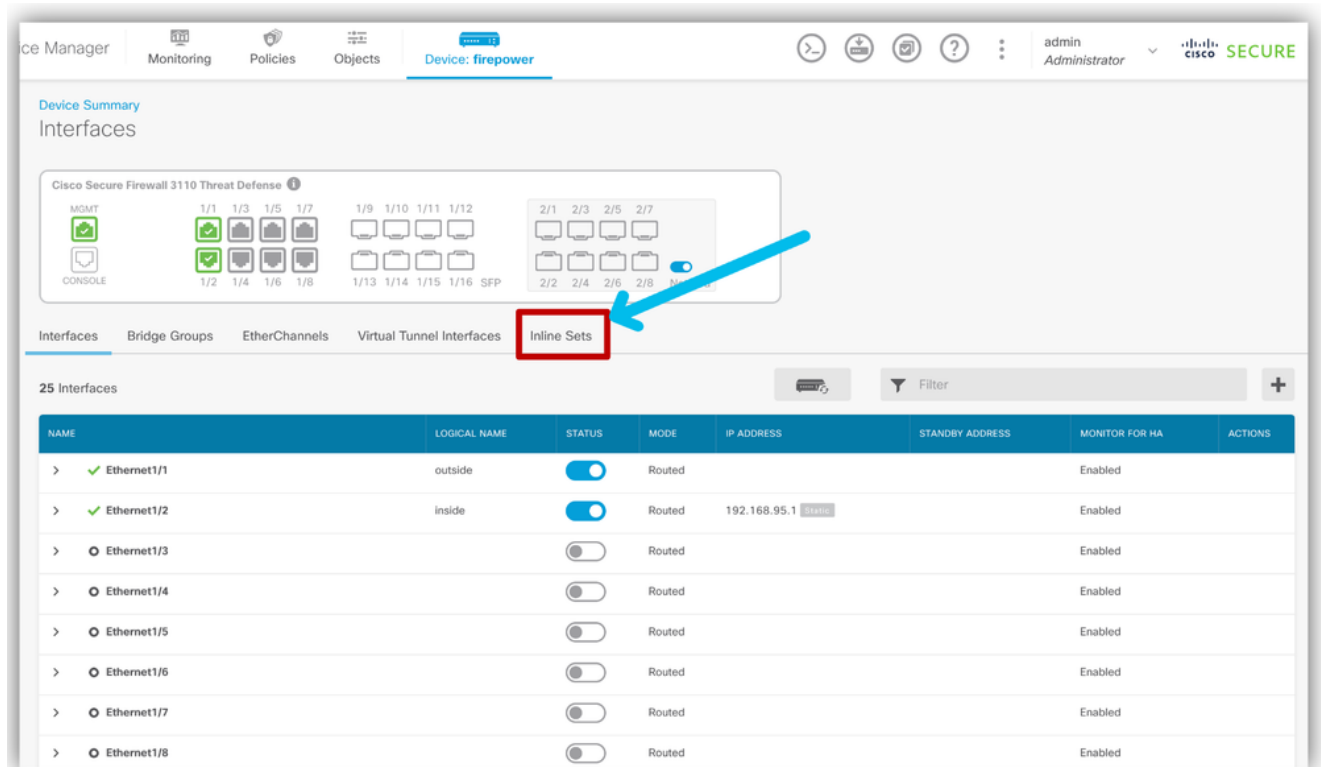
Parameters configureren



Opmerking: De modus wordt automatisch gewijzigd in Inline nadat de interface is toegevoegd in een Inline Pair.

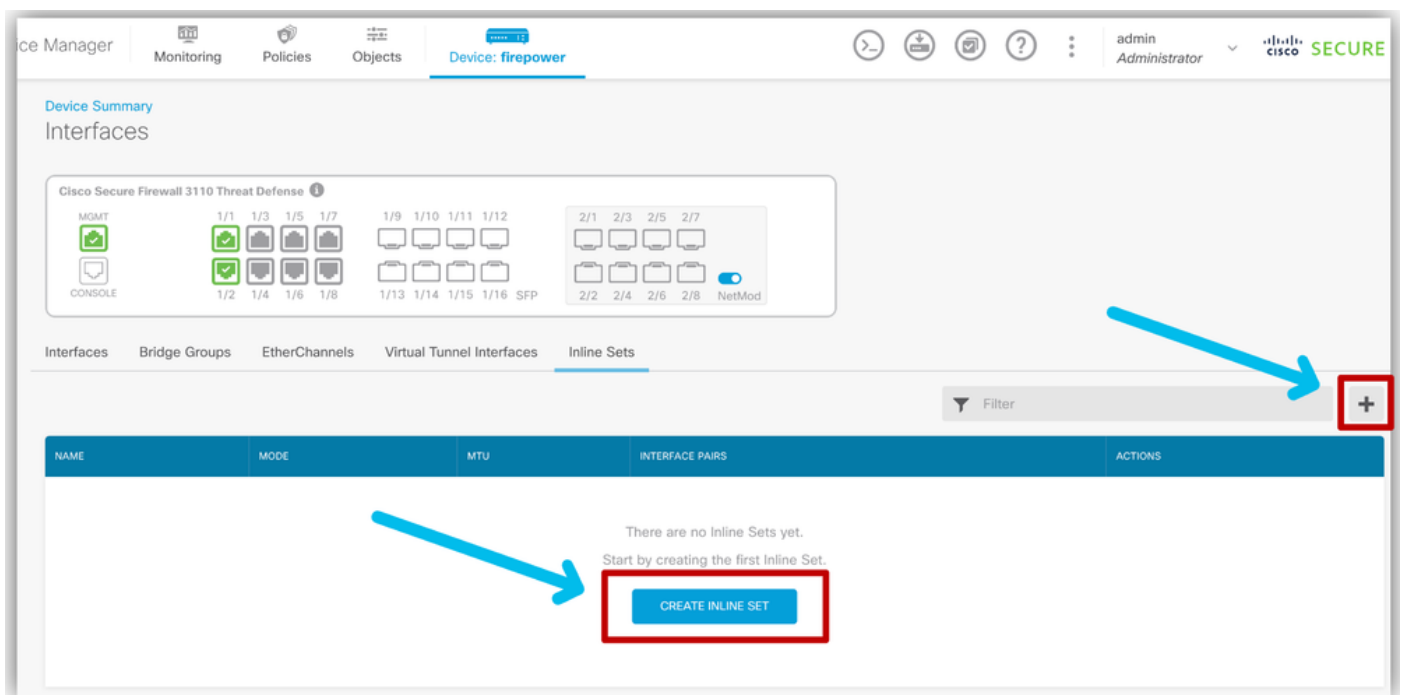
Stap 2: Maak een inline set aan.

- Navigeer naar Apparaat > Interfaces > Inline sets tabblad.



Navigeer naar het tabblad Inline sets

- Voeg een nieuwe inline set toe.
- Klik op + pictogram of Inline set maken knop.



Inline set maken

- Basisinstellingen configureren.
 1. Stel een naam in.
 2. Stel de gewenste MTU in (optioneel). De standaard is 1500, wat de minimaal ondersteunde MTU is.
 3. Selecteer Hardware Bypass (Details beschikbaar in de volgende sectie). Er is een nieuw dropdown menu toegevoegd voor Bypass.
 4. In de sectie Interfaceparen selecteert u interfaces.
 5. Genoemde interfaces zijn beschikbaar voor selectie. Als er meer paren nodig zijn, klikt u op de link Een ander paar toevoegen.

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

Instellingen configureren

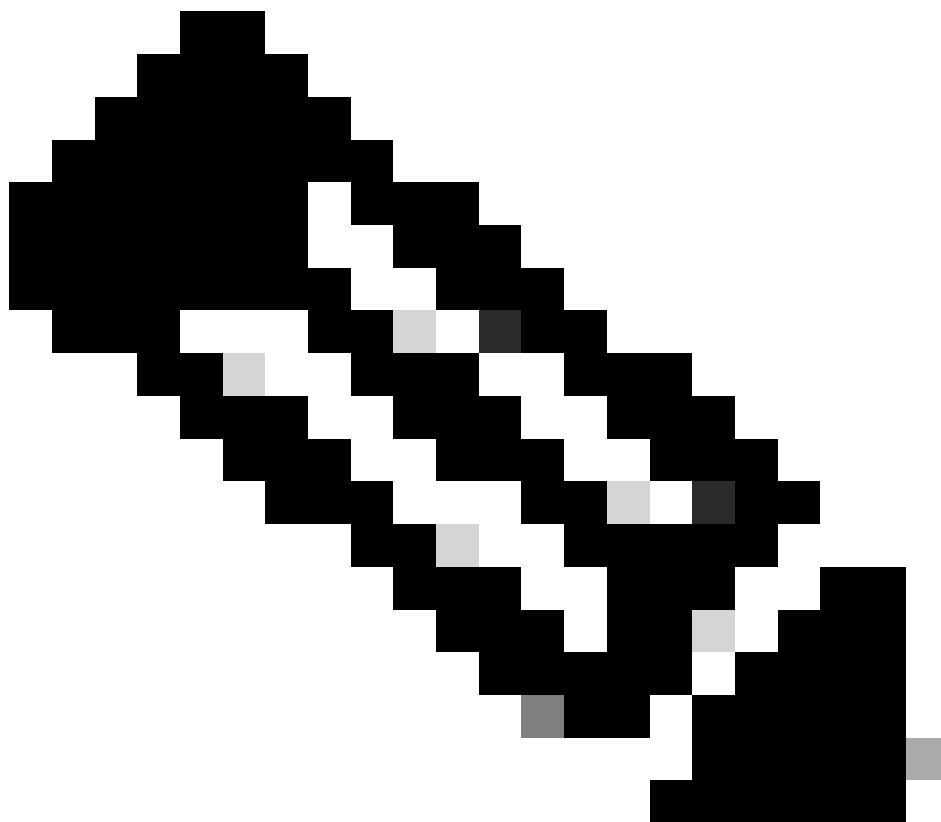
Hardware-bypass

Mogelijkheden en beperkingen

- Hardware Bypass zorgt ervoor dat het verkeer blijft stromen tussen een inline interfacepaar

tijdens een stroomstoring. Deze functie kan worden gebruikt om de netwerkconnectiviteit te behouden in het geval van software- of hardwarestoringen.

- Hardware Bypass-poorten worden alleen ondersteund voor inline sets.
 - Hardware Bypass wordt NIET ondersteund in de modus voor hoge beschikbaarheid.
 - Modi voor omzeilen van hardware:
 - UITGESCHAKELD - Hiermee schakelt u bypass uit op ondersteunde interfaces. Standaardmodus voor niet-ondersteunde interfaces.
 - STANDBY - In de stand-by-toestand blijven de interfaces normaal werken totdat er een trigger-gebeurtenis is.
 - BYPASS FORCE - dwingt het interfacepaar handmatig om inspectie te omzeilen.
-



Opmerking: [Informatie over typen FTD-interfaces en omzeiling van hardware](#)

Snort Fail Open vs Hardware Bypass

- Hardware Bypass-functionaliteit zorgt ervoor dat verkeer kan stromen tijdens een hardwarestoring, inclusief een volledige stroomuitval en bepaalde beperkte softwarefouten.
- Een softwarefout die Snort Fail Open activeert, leidt niet tot een Hardware Bypass.

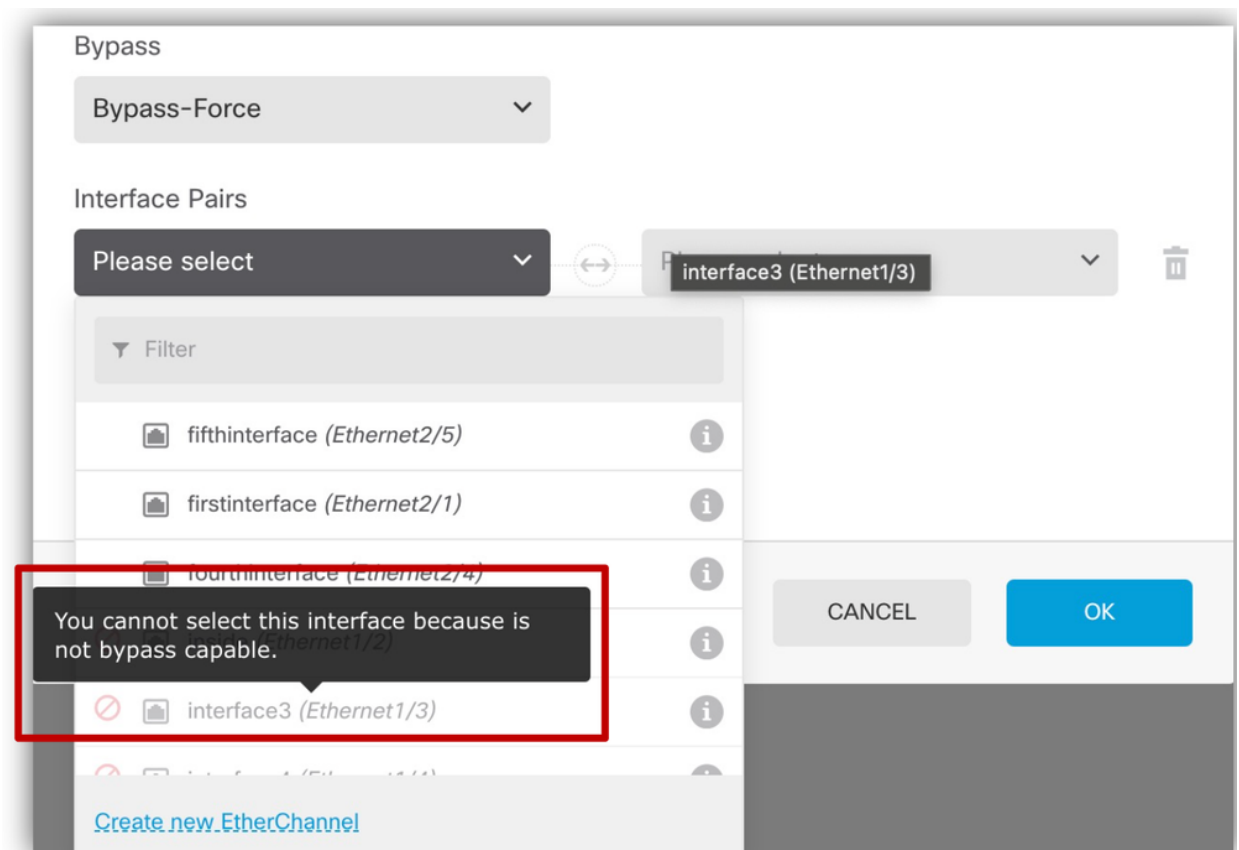
Hardware Bypass-triggers

Hardware Bypass kan worden geactiveerd in de volgende scenario's:

- Toepassingscrash
- Toepassing opnieuw opstarten
- Hulpmiddelcrash
- Opnieuw opstarten of upgraden van apparaat
- Stroomverlies van medisch hulpmiddel
- Handmatige trigger

Om te zien welke interfaces hardware bypass ondersteunen:

- Vanuit de FDM GUI, als Bypass is geselecteerd:
 - Interfaces die het ondersteunen zijn selecteerbaar.
 - Interfaces die geen ondersteuning bieden, worden grijs weergegeven.
 - In dit voorbeeld is Ethernet1/3 grijs weergegeven in deze afbeelding:



Support voor hardwarebypass controleren

Stap 3: Inline sets configureren Geavanceerde instellingen.

- Navigeer naar Apparaat > Interfaces > Inline sets tabblad of bewerk een reeds gemaakte inline set.
- Navigeer naar het tabblad Geavanceerd.
 - Op het tabblad Geavanceerd kunt u de instellingen voor inline sets configureren.
 - Klik op het tabblad Geavanceerd.

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

Inline set configureren

- modus
 - Tik: Instelt in de inline-tapmodus. Als de tapmodus is ingeschakeld, is Snijden en openen mislukt uitgeschakeld.
 - inline

Create New Inline Set

Name: inline_example 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

Selectiemodus

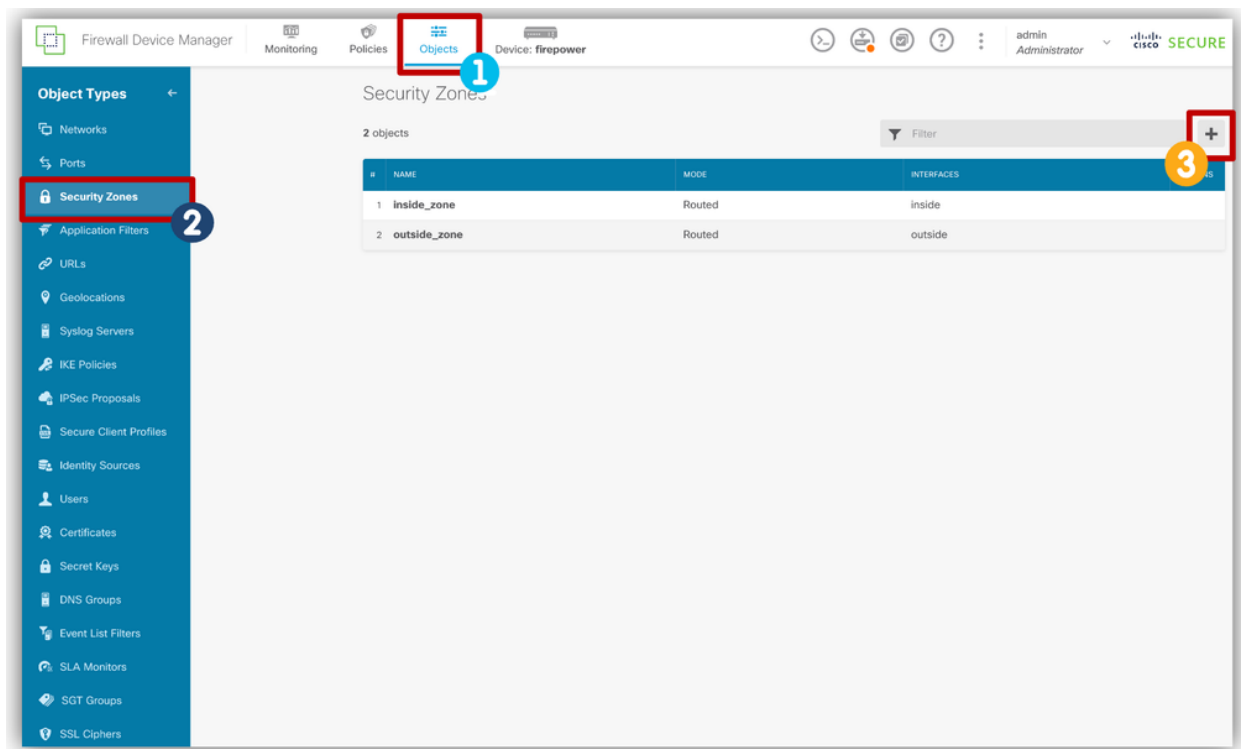
- Instellingen voor openen afbreken mislukt.
 - Kies de gewenste instellingen voor Snort Fail Open.
 - Geen, één of beide. De opties Bezig en Omlaag kunnen worden ingesteld.
 - Snort Fail Open maakt het mogelijk dat nieuw en bestaand verkeer zonder inspectie (ingeschakeld) of drop (uitgeschakeld) kan passeren wanneer het Snort-proces bezig of uitgeschakeld is.

Snort Fail Open en Verbindingsstatus propageren

- Koppelingsstatus propageren.
 - Propagate Link State verlaagt automatisch de tweede interface in het Inline-paar wanneer een van de interfaces uitvalt. Wanneer de neergehaalde interface weer omhoog komt, komt de tweede interface ook automatisch weer omhoog.
- Klik op OK om de inline set aan te maken.

Stap 4: Toepassen op een beveiligingszone (optioneel).

1. Navigeer vanuit de bovenste navigatiebalk naar Objecten.
2. Kies Beveiligingszones in de linkernavigatie:
 - Klik + om een beveiligingszone toe te voegen.



Een beveiligingszone toevoegen

De beveiligingszone configureren (optioneel)

1. Noem de veiligheidszone.
2. Selecteer Inline-modus.
Beveiligingszones en interfaces moeten dezelfde modus hebben.
3. Selecteer Interfaces die deel uitmaken van de inline set.
4. Klik op OK.

Add Security Zone

Name

test_sz

Description

Mode

☐ Routed

☐ Passive

☒ Inline

Interfaces

+

CANCEL

OK

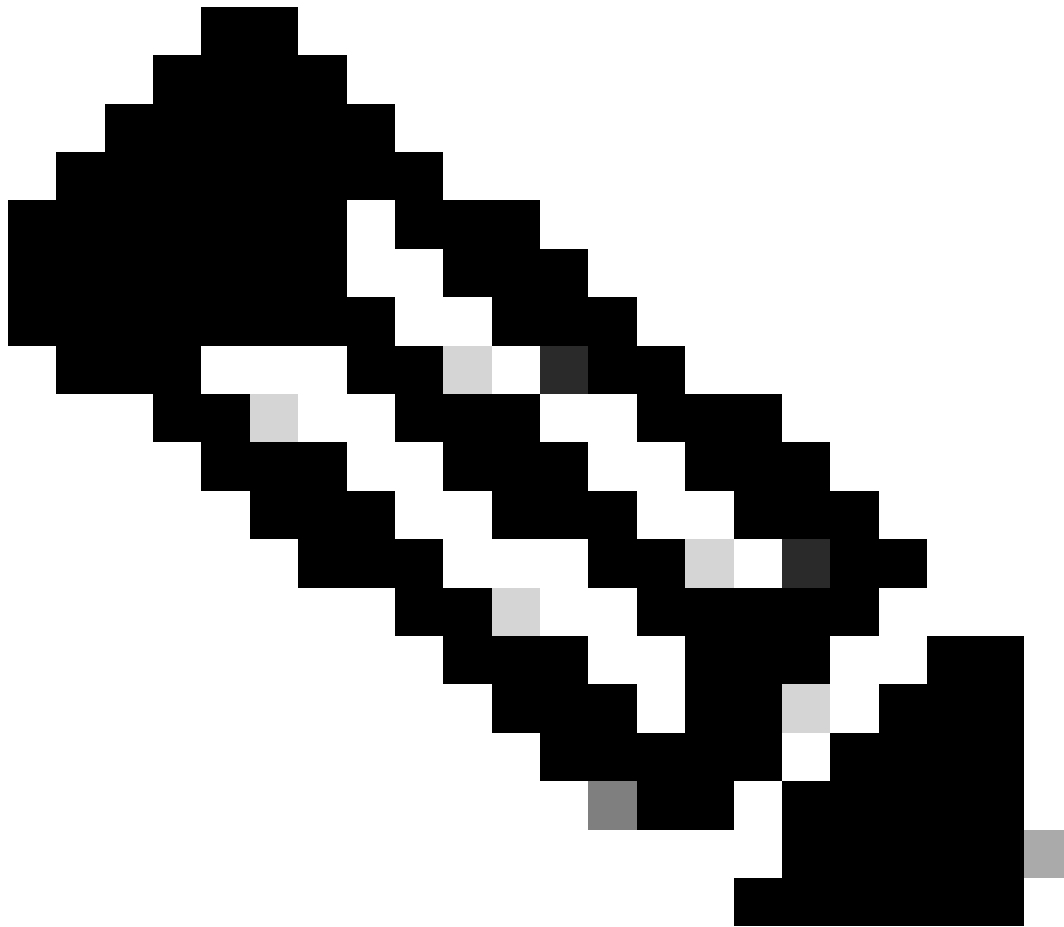
1

2

3

4

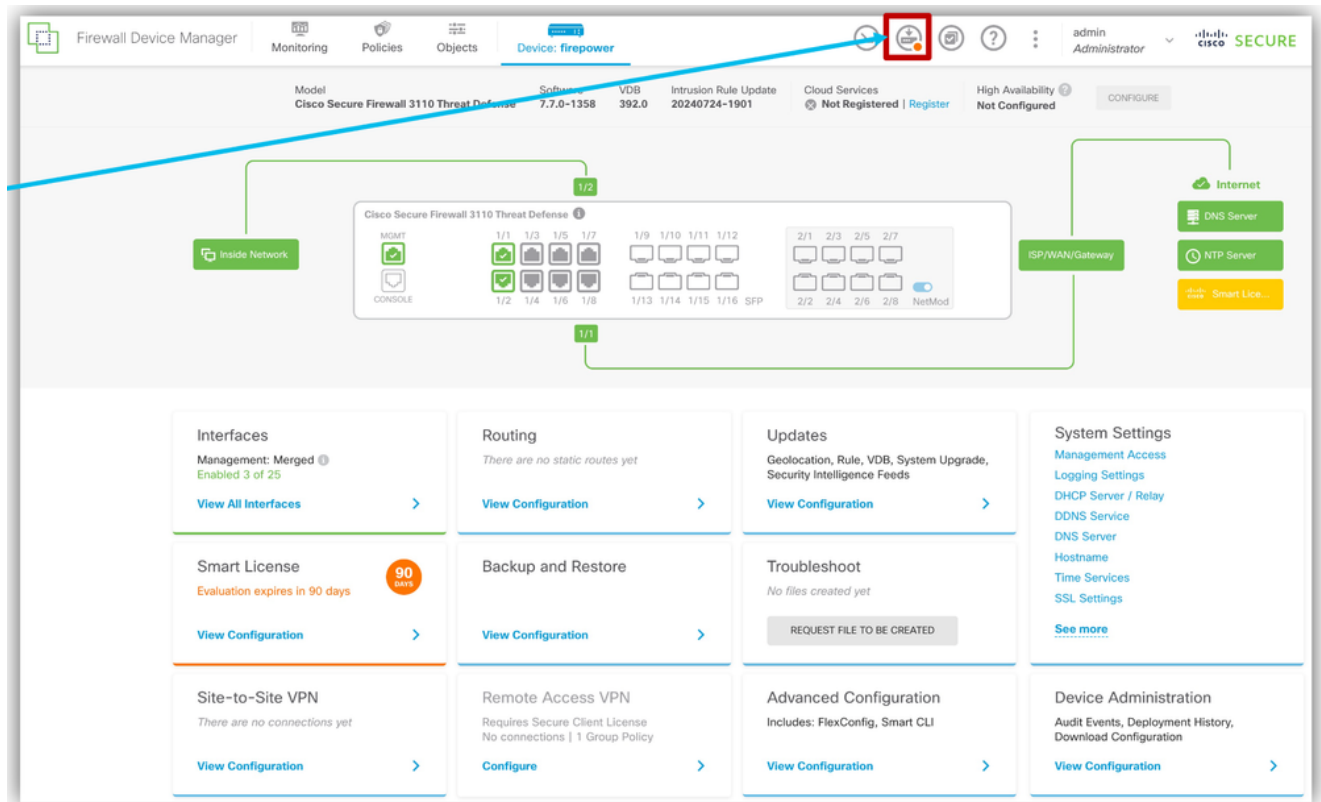
Beveiligingszone configureren



Opmerking: voor interfaces wordt de modus automatisch gewijzigd in Inline nadat de interface is toegevoegd in een Inline Pair.

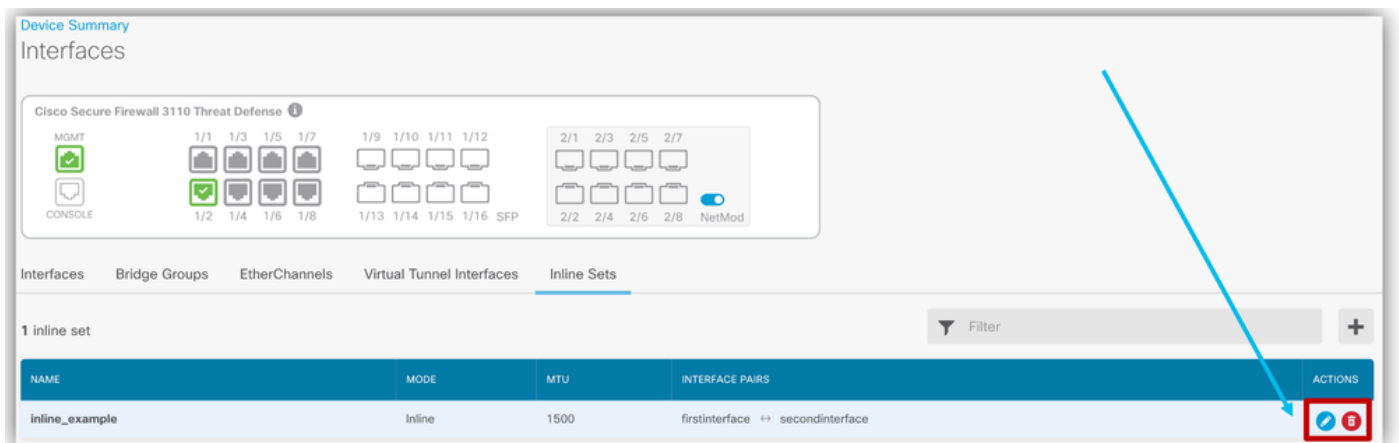
Stap 4: implementeren

- Navigeer naar het tabblad Implementatie en implementeer.



Wijzigingen implementeren

- Inline sets bewerken en verwijderen.
 - Navigeer naar Apparaat > Interfaces > Inline sets tabblad.
 - De knoppen Bewerken en Verwijderen zijn beschikbaar voor inline sets.



Inline sets bewerken en verwijderen

FDM Device REST API's

REST API-eindpunten

- GET: /devices/default/inlinesets
Een lijst met alle bestaande inline-sets ophalen.

- GET:/devices/default/inlinesets/{objID}
Een specifiek inline-setobject ophalen met de bijbehorende ID.
- POST: /devices/default/inlinesets
Maak een nieuwe inline-set aan.
- PUT: /devices/default/inlinesets/{objID}
Bestaande inline-objecten bijwerken met de bijbehorende ID.
- Verwijderen:/devices/default/inlinesets/{objID}
Bestaande inline-set objecten verwijderen met de bijbehorende ID.
- GET:/operational/interface/{objID}
Een lijst met alle InterfaceInfoEntiteiten ophalen.
- Ter ondersteuning van Hardware Bypass is een nieuw veld toegevoegd aan de InterfaceInfo API.

Interface Info REST API Modellen

- Een nieuwe field bypassInterfacePeerID werd toegevoegd om de hardware bypass integratie te ondersteunen.
- Dit veld vertegenwoordigt de ID van het Hardware Bypass Interface Pair voor de huidige interface.
- Waarden:
 - Null - interface ondersteunt geen bypass.
 - ID - interface ondersteunt 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"
  }
}

```

Interface Info REST API

Interface Info REST API voorbeeld

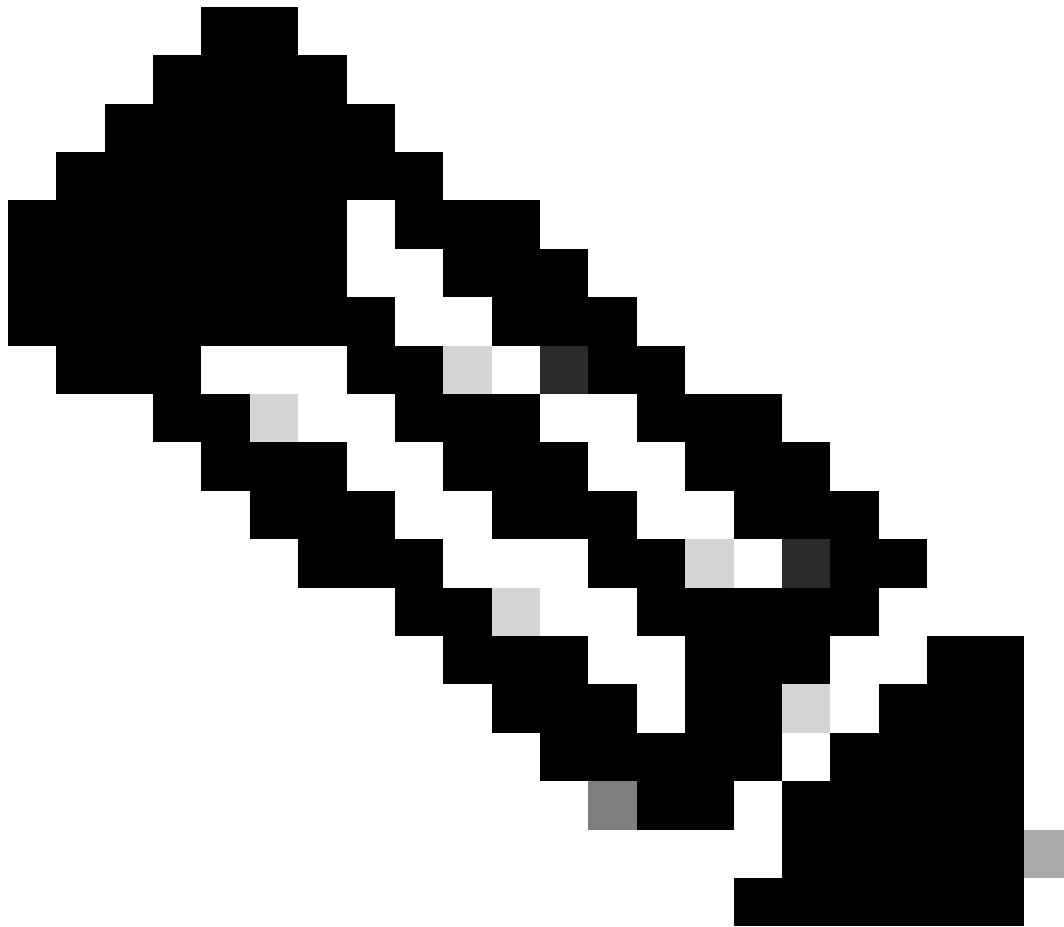
- Interface Info REST API voorbeeld.
 - Interface zonder ondersteuning voor hardware-bypass (Ethernet 1/4).
 - Interfacepaar met ondersteuning voor hardware-bypass (Ethernet2/1 en Ethernet 2/2).

```

{ "interfaceInfoList": [
  {
    "interfaceId": "da9edc2d-58ba-11ef-b764-ffca0b8d9fa2",
    "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"
}
}

```

Interface Info REST API voorbeeld



Opmerking: Dit is een fragment van de volledige oproep, vanwege de grootte.

Inline Set REST API's Model

- Het Inline Set model bestaat uit:
 - Type
 - Naam
 - Tikmodus
 - MTU
 - Verbindingsstatus propageren
 - Falen Open Snort bezig
 - Waarden omzeilen: UITGESCHAKELD, 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

Voorbeeld van Inline Set REST API

- Basis Inline Set voorbeelden met:

- Eén inline-paar
- Standby-bypass

```
{
  "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. Inline set maken (zie API Explorer voor voorbeelden van payload).

POST/apparaten/standaard/inlinesets

3. Maak Beveiligingszone (zie API Explorer voor voorbeelden van nuttige lading) (optioneel).

POST/object/beveiligingszones

4. Implementeren op apparaat (zie API Explorer voor voorbeelden van nuttige lading).

POST/operationeel/implementatie

Een inline set configureren en implementeren met Hardware Bypass

1. Ontvang interface-ID's en informatie over Hardware Bypass-interfaceparen (zie API Explorer voor voorbeelden van nuttige lading).

GET/operational/interface/{objId}

2. Inline set maken (zie API Explorer voor voorbeelden van payload).

POST/apparaten/standaard/inlinesets

3. Maak Beveiligingszone (zie API Explorer voor voorbeelden van nuttige lading) (optioneel).

POST/object/beveiligingszones

4. Implementeren op apparaat (zie API Explorer voor voorbeelden van nuttige lading).

POST/operationeel/implementatie

Een inline set bewerken

1. Ontvang interface-ID's (zie API Explorer voor voorbeelden van nuttige lading).

GET/devices/default/interfaces

2. Inline sets ophalen.

GET/devices/default/inlinesets

3. Bewerk de inline set (zie API Explorer voor voorbeelden van payload).

PUT/devices/default/inlinesets/{objId}

4. Implementeren op apparaat (zie API Explorer voor voorbeelden van nuttige lading).

POST/operationeel/implementatie

Verifiëren

```
<#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

Problemen oplossen

Opdrachten

- Inline-set met actieve configuratie weergeven
- Inline-set weergeven
- show interface
- System Support Trace

Inline set - validaties bij het maken

- Fouten worden weergegeven op de GUI voor elk van de velden.
 - De naam moet worden ingevuld.
 - De MTU moet minimaal 1500 zijn.
 - Beide interfaces in een paar moeten worden gekozen.

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

MTU-grootte

Hardware Bypass - validatie bij het maken

- Nieuwe fouten worden weergegeven op de GUI voor elk van de velden, wanneer bypass is ingeschakeld:
 - Alle interfaces moeten Bypass ondersteunen.
 - Fout: niet-ondersteunde interfaces worden weergegeven.
 - Alle paren moeten het vooraf bepaalde interfacepaar gebruiken.
 - Foutbericht vermeldt beschikbare bypass-interfaceparen.

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)

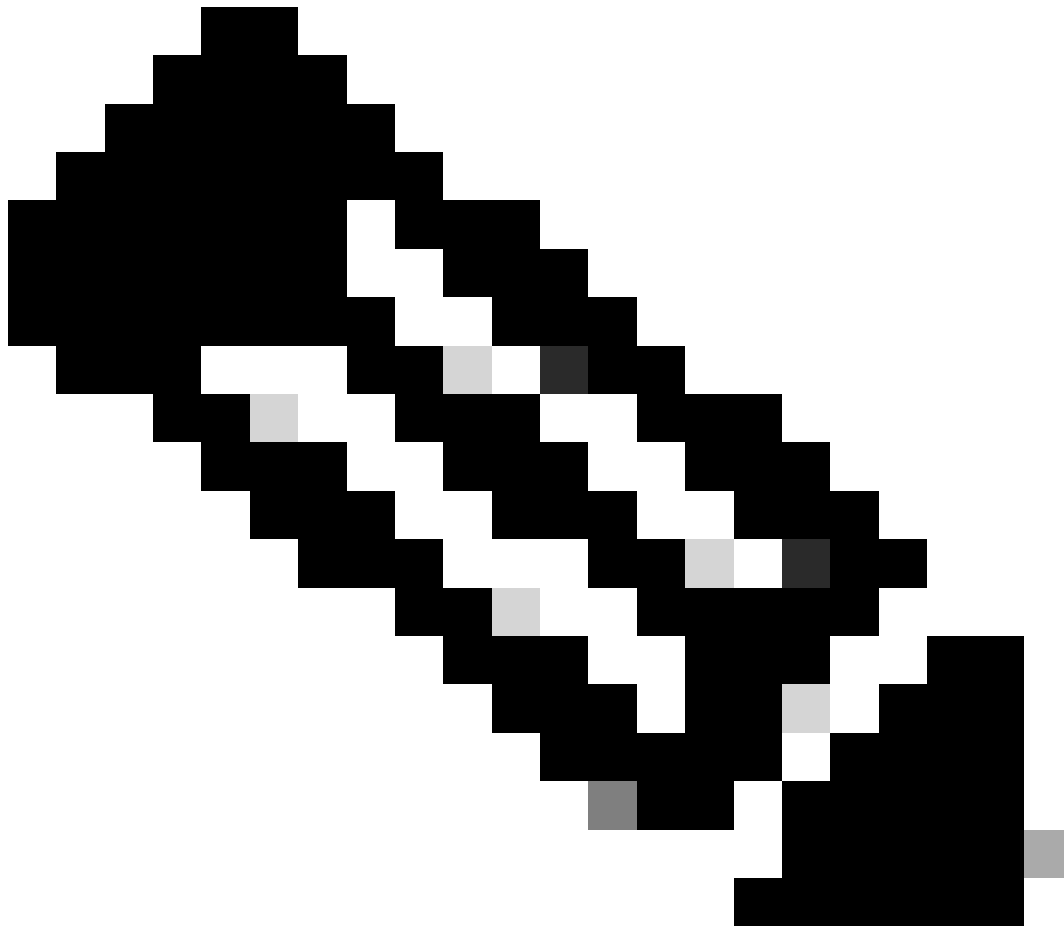


This pair of interfaces does not support the selected bypass mode.

[Add another pair](#)

CANCEL

OK



Opmerking: het eerste paar (Ethernet2/1-Ethernet2/2) is geldig.

REST API Response toont fouten

- Fouten worden weergegeven in de REST API-respons.
 - Hier is de MTU-waarde ongeldig.

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

REST API-validatie

Beperkingen van de implementatie voor deze release

- Inline Sets: werkt alleen met fysieke interfaces en EtherChannel.
- Inline sets met hardware bypass: werkt alleen met fysieke interfaces en vereist een netwerkmodule.

Niet-ondersteunde firewallfuncties op inline interfaces

- DHCP-server
- DHCP-relais
- DHCP-client
- TCP-onderschepping
- routing
- NAT
- VPN
- Toepassing
- inspectie
- QoS
- NetFlow

Logboeken van CLI verifiëren

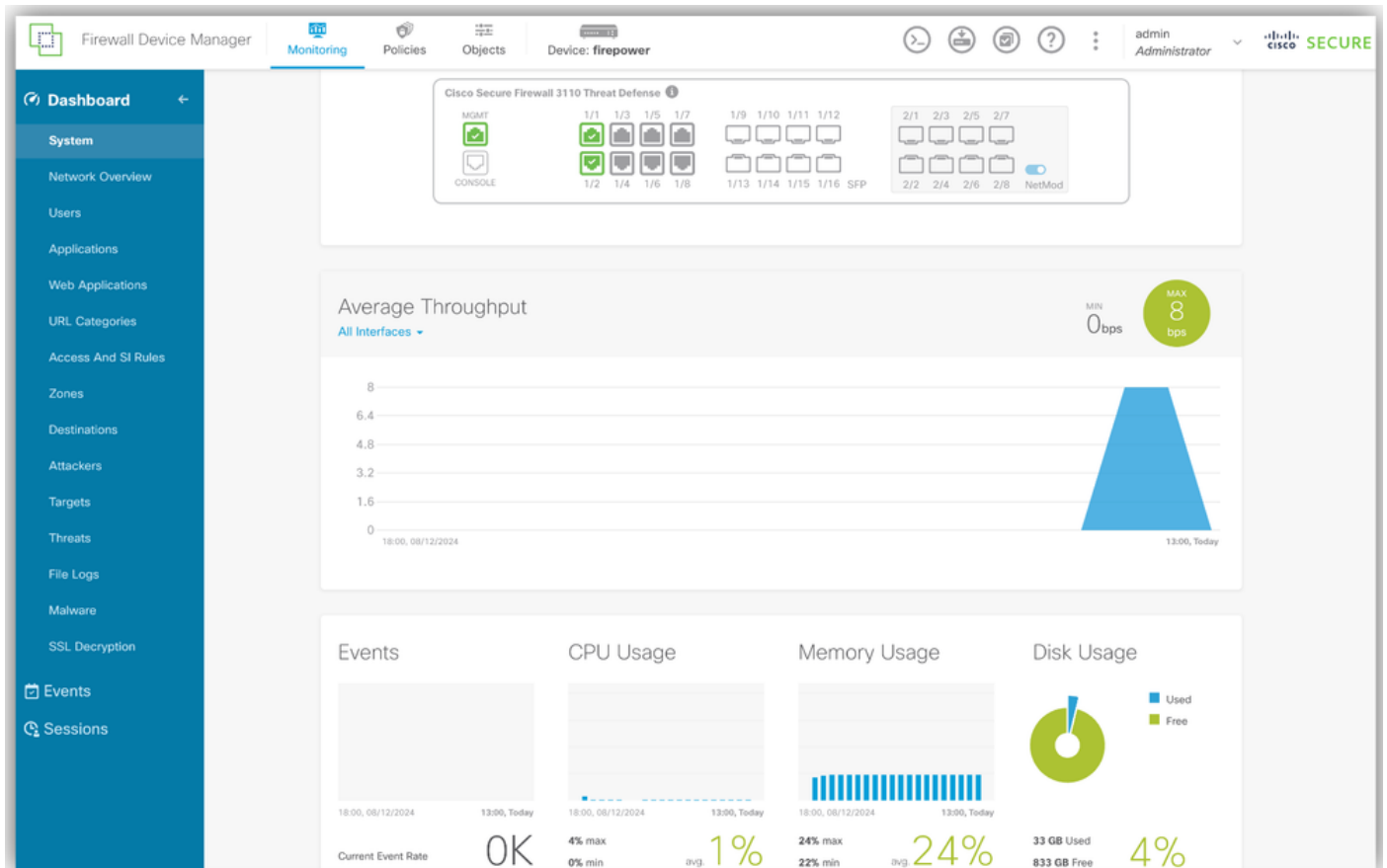
- Logboekregistratie.
 - Logs zijn te vinden op /ngfw/var/log/cisco/ngfw-onbox.log.
 - Zoeken naar inline set.
 - Voorbeeld van mogelijke fouten in logs:
 - Twee interfaces ondersteunen geen bypass.
 - Twee interfaces zijn geen geldig bypasspaar.

```

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

```

- Verifieer verkeer vanuit GUI.
 - Evenementen worden gepresenteerd op de GUI.
 - De juistheid van de verkeersstroom kan hier worden gecontroleerd.
 - Navigeer naar Controle > Systeem.



FDM-bewaking

- Controleer de verkeerscorrectie van 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]

Veelgestelde vragen

V: Wordt HA ondersteund met inline-sets op FDM?

A: Inline sets zonder bypass worden ondersteund.

Inline sets met bypass worden NIET ondersteund.

V: Zijn de spanning-tree BPDU's geblokkeerd op het inline-set paar?

A: Nee, ze zijn niet geblokkeerd.

V: Worden FTW-kaarten ondersteund in 3100?

A: Ja, FTW-netmods worden ondersteund sinds de 3100-serie werd geïntroduceerd met 7.1/9.17. Hardware Bypass is beschikbaar vanaf 7.7.0.

V: Voor 3100 FTW-kaarten worden de Bypass-modi Disabled, Standby, Bypass-Force zoals op FMC ondersteund of niet?

A: Hardware Bypass is beschikbaar vanaf 7.7.0 op 3100 apparaten met FTW-kaarten.

V: Worden inline-sets met poortkanalen ondersteund wanneer het verkeer ook asymmetrisch is over de poortkanalen?

A: Er wordt geen validatie uitgevoerd op de door PortChannel geconfigureerde snelheid, dus zolang de FTD deze ondersteunt, moet deze worden ondersteund.

V: Als Snort faalt voor inspectie, wordt failopen dan ondersteund?

A: Raadpleeg de documentatie bij deze instelling in de [configuratiehandleiding van het Firepower Management Center](#).

Gerelateerde informatie

- [FTD-interfaces configureren in Inline-Pair-modus](#)
- [Configuratiehandleiding van Firepower Management Center, versie 6.3](#)
- [Installatiehandleiding voor hardware uit de Cisco Secure Firewall 3100-reeks](#)
- [Cisco Secure Firewall 3100-reeks — Gegevensoverzicht](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.