

Configuration du contournement matériel de Secure Firewall 3100 FDM 7.7.0

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Notions de base Plates-formes prises en charge, licences](#)

[Description des fonctionnalités et procédure pas à pas](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations](#)

[Contournement matériel](#)

[API REST du périphérique FDM](#)

[Vérifier](#)

[Dépannage](#)

[Commandes](#)

[Jeu en ligne - Validations lors de la création](#)

[Contournement matériel - ValidationLors de la création](#)

[Limites de l'implémentation de cette version](#)

[Fonctions de pare-feu non prises en charge sur les interfaces en ligne](#)

Introduction

Ce document décrit comment configurer le contournement matériel pour les ensembles en ligne dans le pare-feu sécurisé 7.0 géré par le Gestionnaire de périphériques Firepower (FDM).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Jeux en ligne
- Pare-feu sécurisé série 3100
- Interface graphique utilisateur (GUI) du Gestionnaire de périphériques Firepower

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Secure Firewall 3100 version 7.7.0.
- Cisco Secure Firewall Device Manager v7.7.0.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

La fonction Ensembles en ligne a été ajoutée à FDM dans la version 7.4.1. Les ensembles en ligne permettent l'inspection sur un réseau L2 sans avoir besoin de routage : [Configuration des interfaces FTD en mode Inline-Pair](#)

Comparaison antérieure à cette version

In Secure Firewall 7.6 and Below		New to Secure Firewall 7.7
<ul style="list-style-type: none">• Inline Sets is available.• Hardware Bypass is not supported.		<ul style="list-style-type: none">• Added support for Hardware Bypass.

Fonction de contournement de Secure Firewall 7.0

Nouveautés de Cisco

- Le contournement de l'inspection matérielle garantit que le trafic continue à circuler entre une paire d'interfaces en ligne pendant une panne de courant.
- Cette fonction est utilisée pour maintenir la connectivité réseau en cas de panne logicielle ou matérielle.
- Le contournement matériel est désormais disponible pour les ensembles en ligne pour les plates-formes de la gamme FDM 3100.



Remarque : [Guide de configuration de Firepower Management Center](#)

Scénarios de déploiement

- Comment cette fonctionnalité s'intégrerait-elle dans une configuration de production ?
 - Les jeux en ligne sont utilisés dans un cas d'utilisation IPS (ou IDS).
 - Permet l'inspection du trafic sans configuration de routage. Autorise le flux de trafic si l'unité tombe en panne via le contournement matériel.
- . Exemples pratiques :
 - Configurez l'inspection du réseau de couche 2 n'importe où de manière simple et rapide, sans avoir besoin de la couche 3.
 - Critique pour les réseaux complètement isolés : pas d'accès à Internet.
 - Insertion en ligne transparente pour une inspection approfondie des paquets pour un pare-feu autonome - architecture de couche 2 de production existante.

Notions de base Plates-formes prises en charge, licences

Versions logicielles et matérielles

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: <ul style="list-style-type: none">• 8 Ports:<ul style="list-style-type: none">○ FPR-X-NM-6X1SXF• 6 Ports:<ul style="list-style-type: none">○ FPR-X-NM-6X10SRF○ FPR-X-NM-6X10LRF○ FPR-X-NM-6X25SRF○ FPR-X-NM-6X25LRF

Logiciels et matériel

Remarque : [Informations sur la gamme 3100 et contournement matériel](#)

Autres aspects du soutien

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

Licences et compatibilité

Description des fonctionnalités et procédure pas à pas

Description des fonctionnalités

- Diagramme de réseau à définition en ligne



Diagramme de réseau à définition en ligne

- Le trafic circule du routeur 1 au routeur 2, via les interfaces A et B, en utilisant uniquement une connexion physique.
- Organigramme du traitement des paquets des ensembles en ligne FDM :

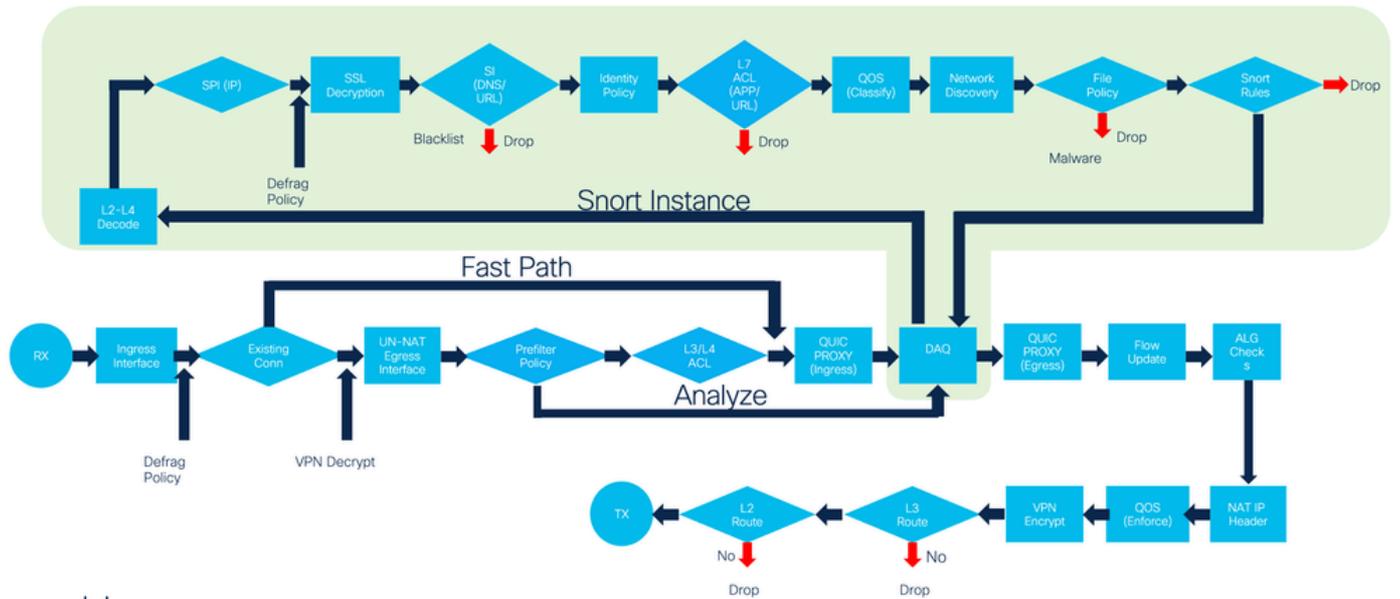
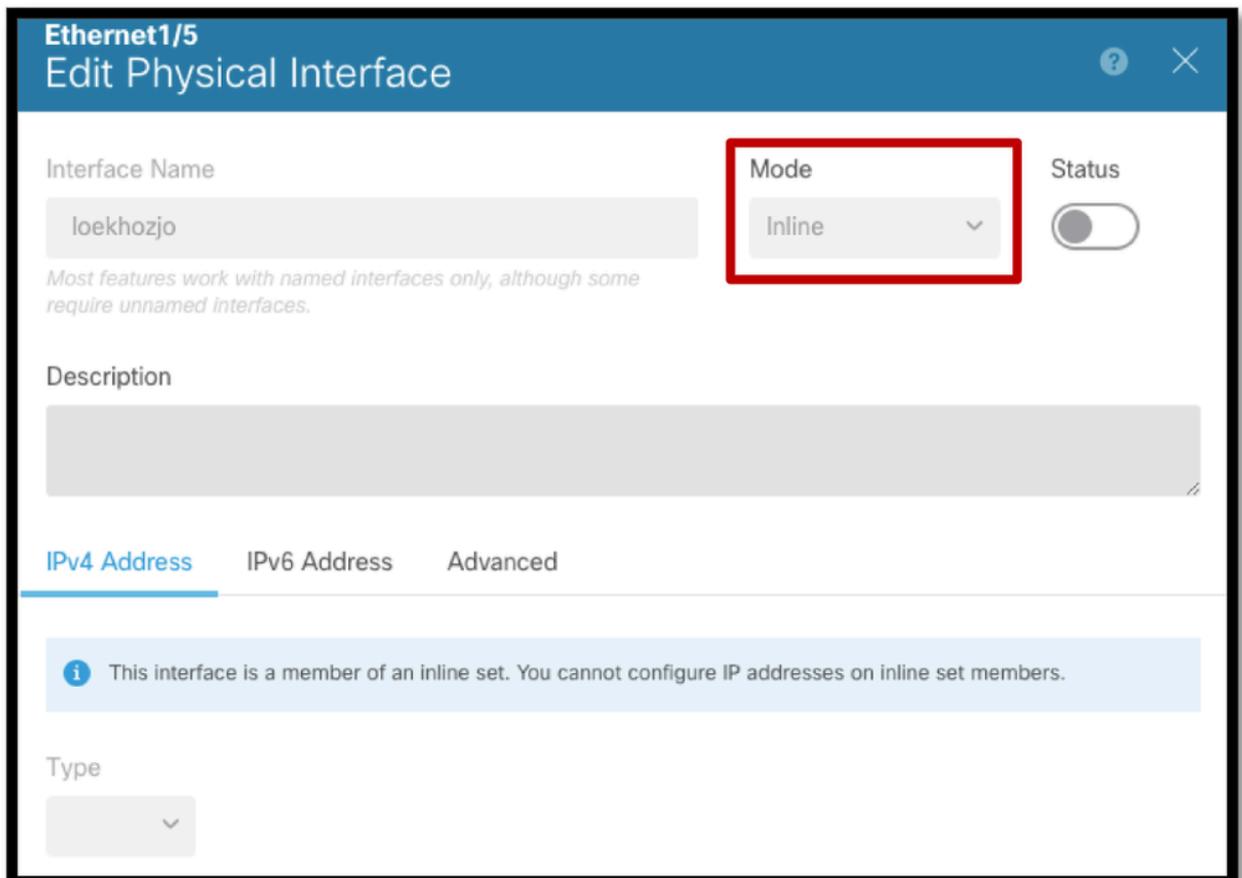


Diagramme De Flux

- Jeux en ligne :
 - Les jeux en ligne sont pris en charge sur les interfaces physiques et les EtherChannels.
- Contournement matériel :
 - Les ensembles en ligne avec contournement matériel sont pris en charge sur des paires d'interfaces physiques prédéterminées :
 - Ethernet 1 et 2
 - Ethernet 2 et 3
 - Ethernet 4 et 5
 - Ethernet 5 et 6
- Prise en charge des interfaces :
 - Interfaces faisant partie d'une paire en ligne :
 - Doit être nommé.
 - Soyez libre de tout IConfigurations P, DHCP ou PPPoE.
 - Ne doit pas être en mode passif.
 - Ne doit pas être une interface de gestion.
 - Doit être utilisé dans une seule paire en ligne à la fois.
- Détails du mode en ligne
 - Le mode en ligne est disponible pour les interfaces physiques, les EtherChannels et les zones de sécurité.
 - Le mode en ligne est automatiquement défini pour les interfaces et les EtherChannels lorsqu'ils sont utilisés dans une paire en ligne.
 - Le mode en ligne empêche les modifications apportées aux interfaces et aux EtherChannels concernés jusqu'à ce qu'ils soient supprimés de la paire en ligne.
 - Les interfaces qui sont en mode Inline peuvent être associées à des zones de sécurité définies en mode Inline.

- Interface utilisateur graphique en mode en ligne
 - La boîte de dialogue Edit Interface indique que l'interface ou EtherChannel est en mode Inline.
 - Les modifications ne sont pas autorisées sur les interfaces lorsqu'elles sont en mode Inline. La boîte de dialogue Modifier l'interface physique (ou Modifier EtherChannel) est en lecture seule.



Modifier l'interface dans GUI

- Mise à niveau, importation/exportation, sauvegarde/restauration, déploiement
 - Implications de mise à niveau
 - L'utilisateur peut mettre à niveau FDM sans aucune restriction.
 - Lors d'une mise à niveau à partir d'une version antérieure, les objets de définition en ligne existants sont configurés avec leur champ de contournement défini sur Désactivé.
 - Implications d'importation/exportation
 - Les objets Inline Set sont importés et exportés.
 - Sauvegarde/restauration
 - Les objets Inline Set sont traités pendant la sauvegarde/restauration.
 - Déploiement
 - Les objets se déploient normalement.
 - Des erreurs spécifiques ont été implémentées.

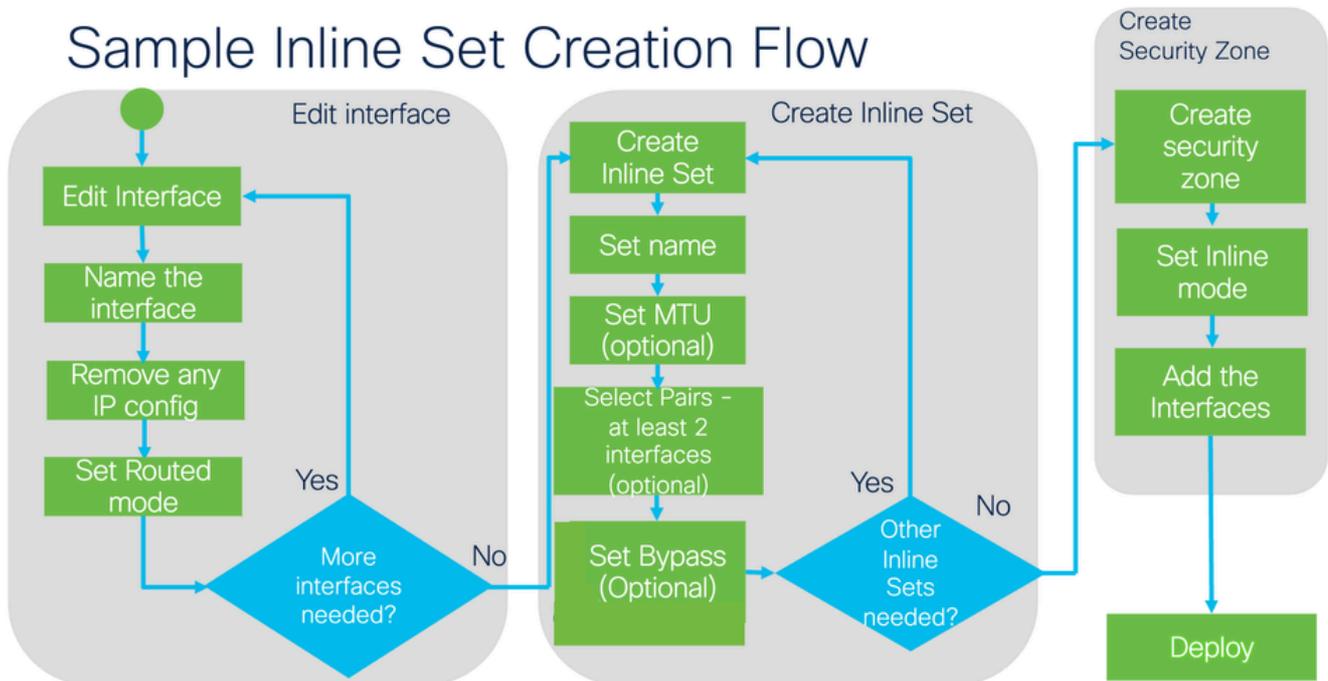
Configurer

Diagramme du réseau



Diagramme du réseau

Sample Inline Set Creation Flow



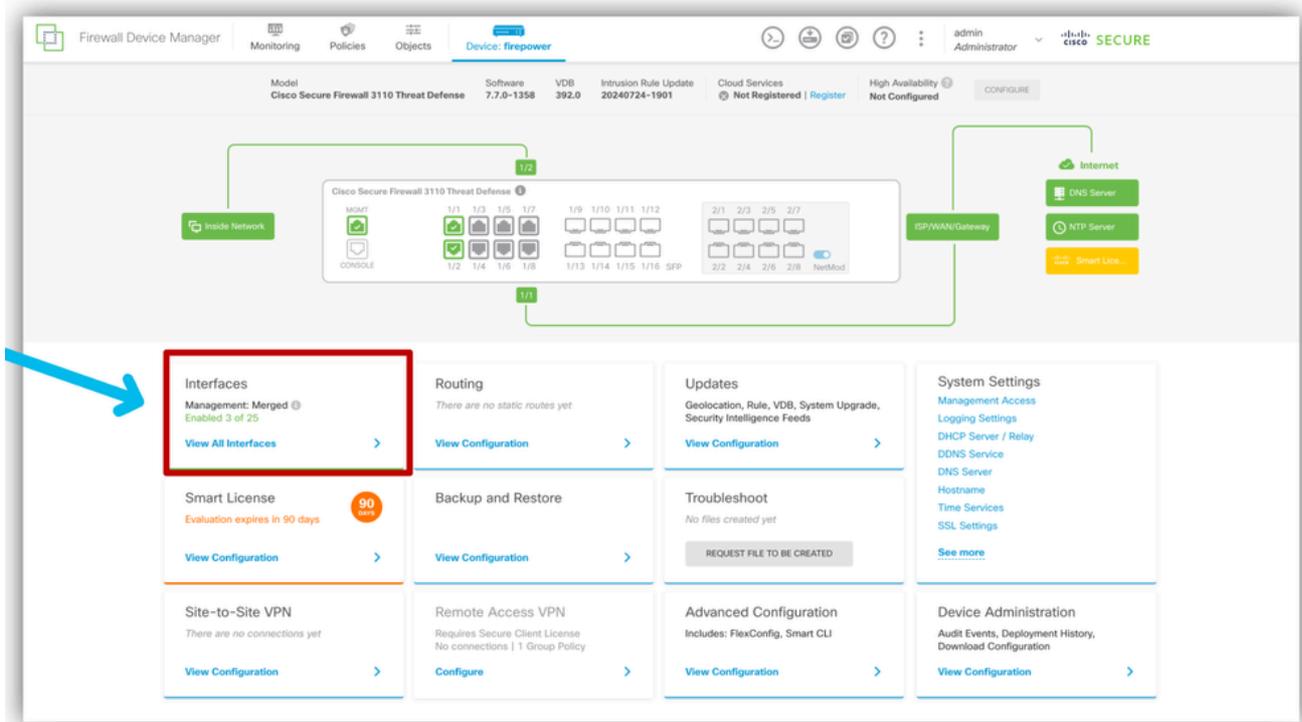
Flux de création de jeu en ligne

Configurations

Cette section décrit les étapes de configuration du contournement matériel sur FDM

Étape 1 : Modifier les interfaces

- Connectez-vous à FDM et nnaviguer jusqu'à Gestion des interfaces.
- Dans le tableau de bord FDM, cliquez sur la carte Interfaces.



Sélectionner une interface

- Modifiez les interfaces utilisées dans l'ensemble en ligne.
- Pour modifier des interfaces, cliquez sur l'icône Modifier (crayon) de l'interface.

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

Modifier l'interface

- Modifier l'interface physique :
 1. Nommez l'interface.

2. Sélectionnez Routed Mode.
3. Supprimez toute configuration 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

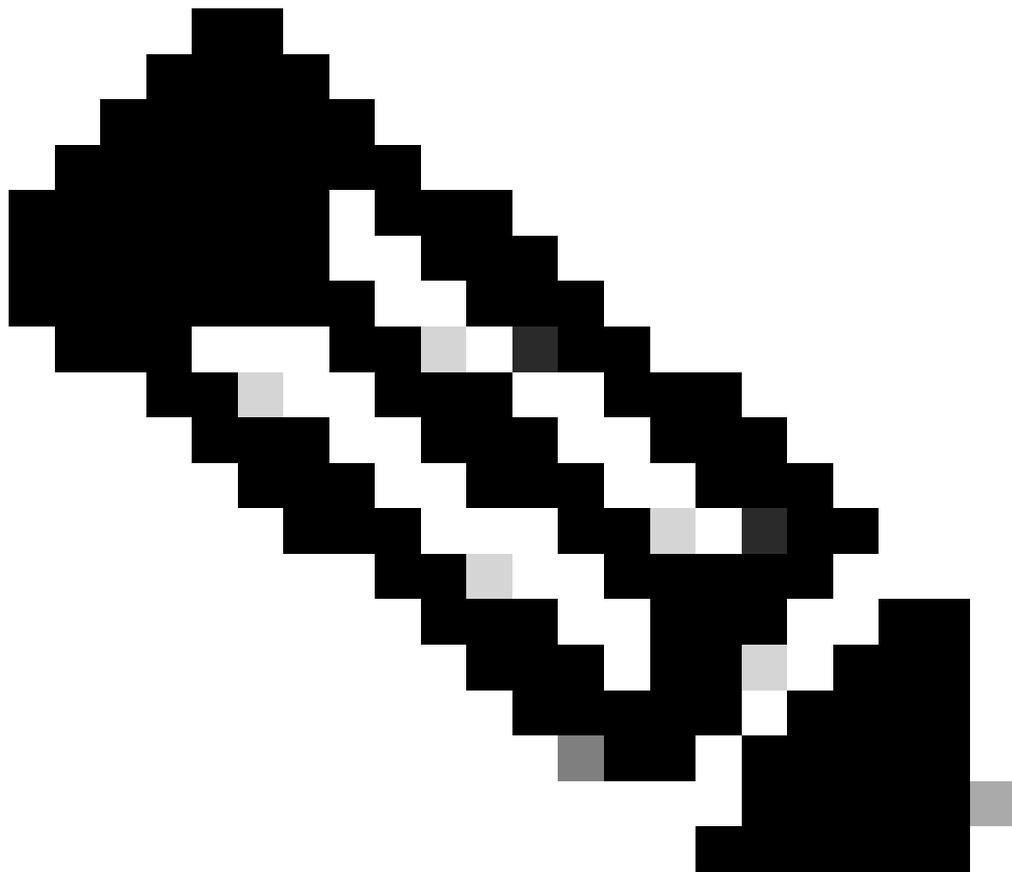
Type
Static

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

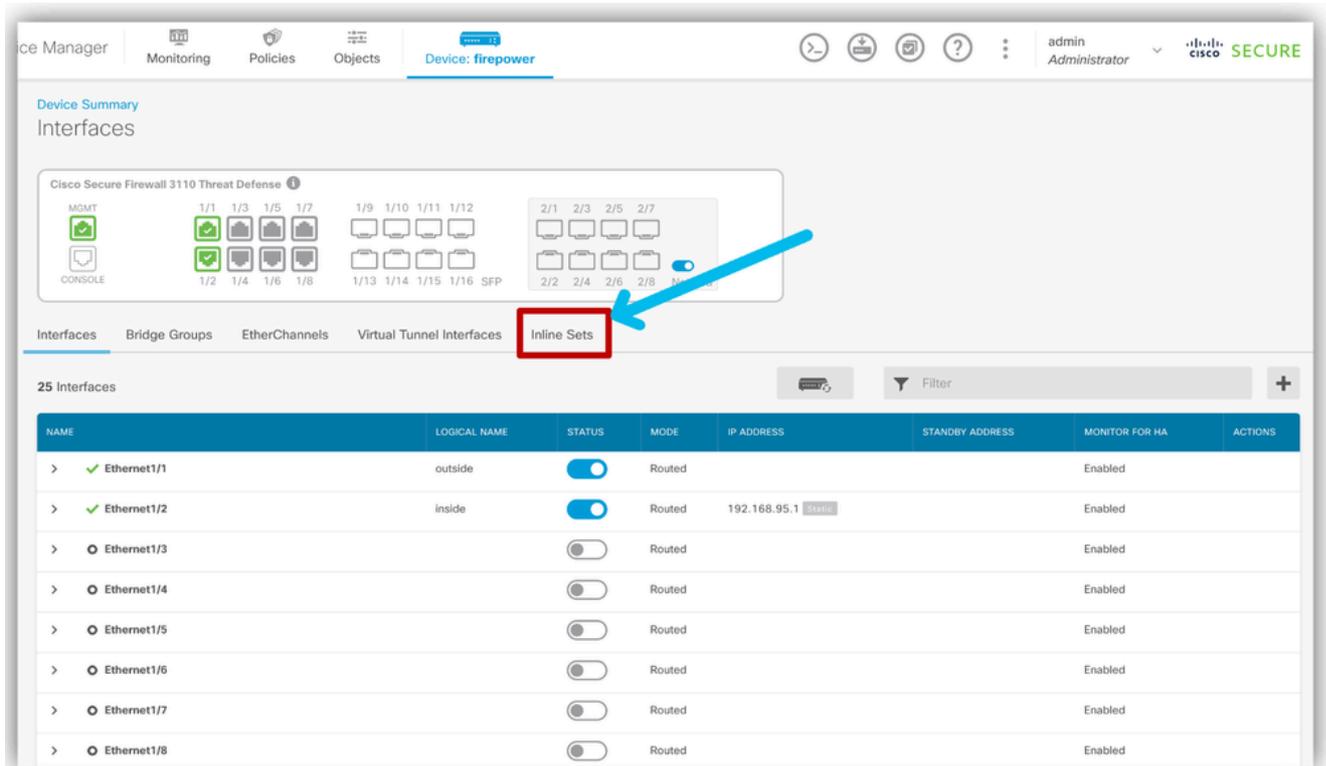
Configurer les paramètres



Remarque : Le mode est automatiquement modifié en Inline après l'ajout de l'interface dans une paire Inline.

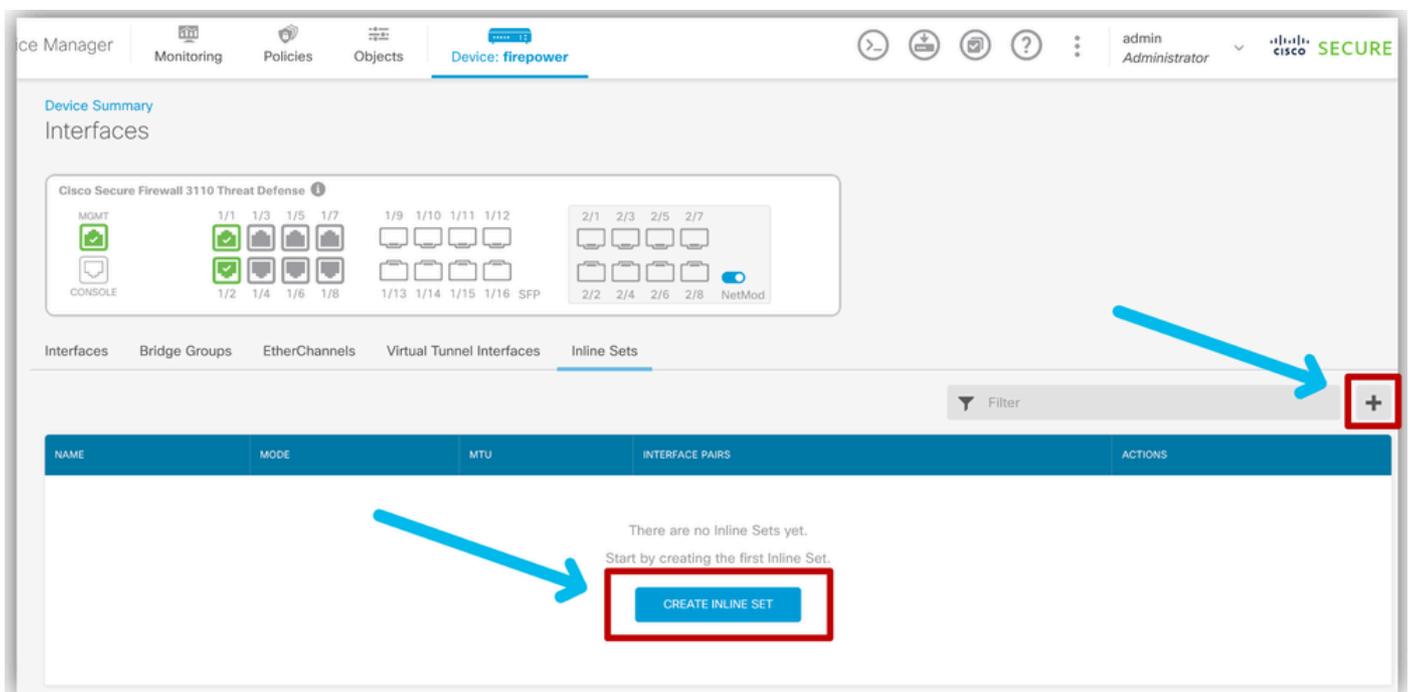
Étape 2 : Créer un jeu en ligne.

- Accédez à Device > Interfaces > Inline sets tab.



Accédez À L'Onglet Jeux Inline

- Ajouter un nouvel ensemble en ligne.
- Cliquez sur l'icône + ou sur le bouton Créer un ensemble en ligne.



Créer un jeu en ligne

- Configurer les paramètres de base
 1. Définissez un nom.
 2. Définissez le MTU souhaité (facultatif). La valeur par défaut est 1500, qui est la valeur MTU minimale prise en charge.
 3. Sélectionnez Contournement matériel (Détails disponibles dans la section suivante). Un nouveau menu déroulant a été ajouté pour Contournement.
 4. Dans la section Paires d'interfaces, sélectionnez interfaces.
 5. Les interfaces nommées peuvent être sélectionnées. Si d'autres paires sont nécessaires, cliquez sur le lien Ajouter une autre paire.

The screenshot shows the 'Create New Inline Set' configuration window. It features a blue header with the title and a close button. The main area is divided into sections: 'Name' (input field with 'inline_example'), 'MTU' (input field with '1500'), 'Bypass' (dropdown menu with 'Standby'), and 'Interface Pairs' (two interface pairs: 'firstinterface (Ethernet2/1)' and 'fourthinterfa... (Ethernet2/4)'). A red box highlights the Name, MTU, Bypass, and Interface Pairs sections, with numbered callouts (1, 2, 3, 4) indicating the steps. The 'Add another pair' link is visible below the interface pairs. At the bottom right, there are 'CANCEL' and 'OK' buttons.

Configuration des paramètres

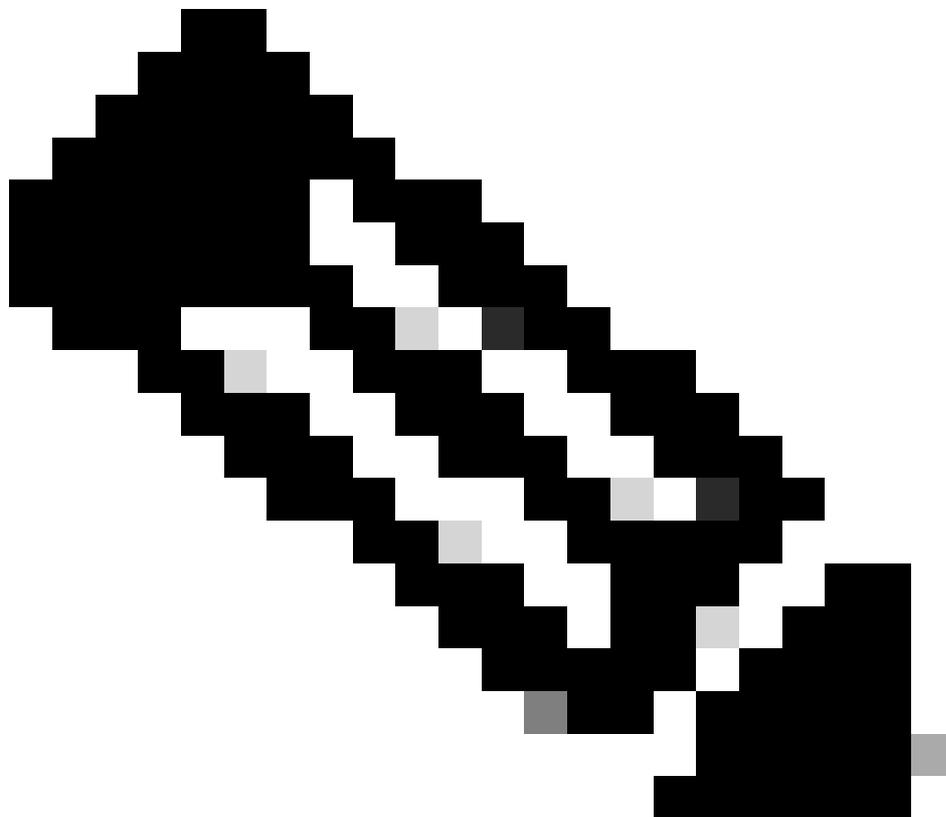
Contournement matériel

Capacités et limites

- Le contournement matériel garantit que le trafic continue à circuler entre une paire

d'interfaces en ligne lors d'une panne de courant. Cette fonction peut être utilisée pour maintenir la connectivité réseau en cas de panne logicielle ou matérielle.

- Les ports de contournement matériel sont pris en charge uniquement pour les jeux en ligne.
- Le contournement matériel n'est PAS pris en charge en mode haute disponibilité.
- Modes de contournement matériel :
 - DISABLED : désactive le contournement sur les interfaces prises en charge. Mode par défaut pour les interfaces non prises en charge.
 - STANDBY - En état de veille, les interfaces restent en fonctionnement normal jusqu'à ce qu'un événement déclencheur se produise.
 - FORCE DE CONTOURNEMENT : force manuellement la paire d'interfaces à contourner l'inspection.



Remarque : [Informations sur les types d'interface FTD et le contournement matériel](#)

Panne d'arrêt/contournement matériel

- La fonctionnalité de contournement matériel permet au trafic de circuler pendant une panne matérielle, y compris une coupure de courant complète et certaines pannes logicielles limitées.

- Une défaillance logicielle qui déclenche l'échec de l'ouverture de Snort ne déclenche pas de contournement matériel.

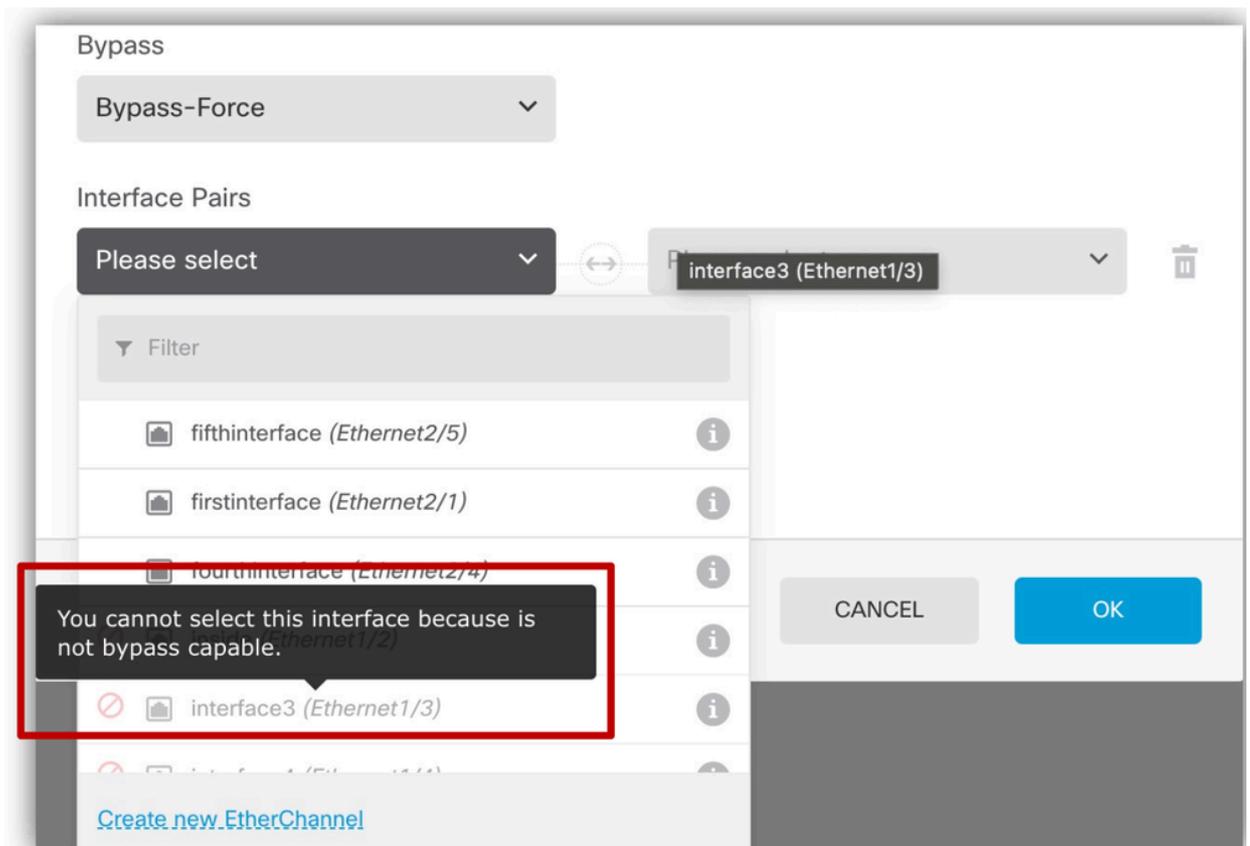
Déclencheurs de contournement matériel

Le contournement matériel peut être déclenché dans les scénarios suivants :

- Panne de l'application
- Redémarrage de l'application
- Panne du périphérique
- Redémarrage ou mise à niveau du périphérique
- Perte de puissance des périphériques
- Déclencheur manuel

Pour voir quelles interfaces prennent en charge le contournement matériel :

- Dans l'interface utilisateur graphique de FDM, si l'option Contourner est sélectionnée :
 - Les interfaces qui le prennent en charge peuvent être sélectionnées.
 - Les interfaces qui ne prennent pas en charge sont grisées.
 - Pour cet exemple, Ethernet1/3 est grisé dans cette figure :



Vérifier la prise en charge du contournement matériel

Étape 3 : Configurer les paramètres avancés des jeux en ligne.

- Accédez à Device > Interfaces > Inline sets ou modifiez un jeu en ligne déjà créé.
- Accédez à l'onglet Avancé.

- L'onglet Avancé vous permet de configurer les options des jeux en ligne.
- Cliquez sur l'onglet Advanced.

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

Configurer le jeu en ligne

- Mode
 - Effleurez : Définit le mode de pointage en ligne. Si le mode de pointage est activé, l'option Panne de renard ouvert est désactivée.
 - En Ligne

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

Sélectionner le mode

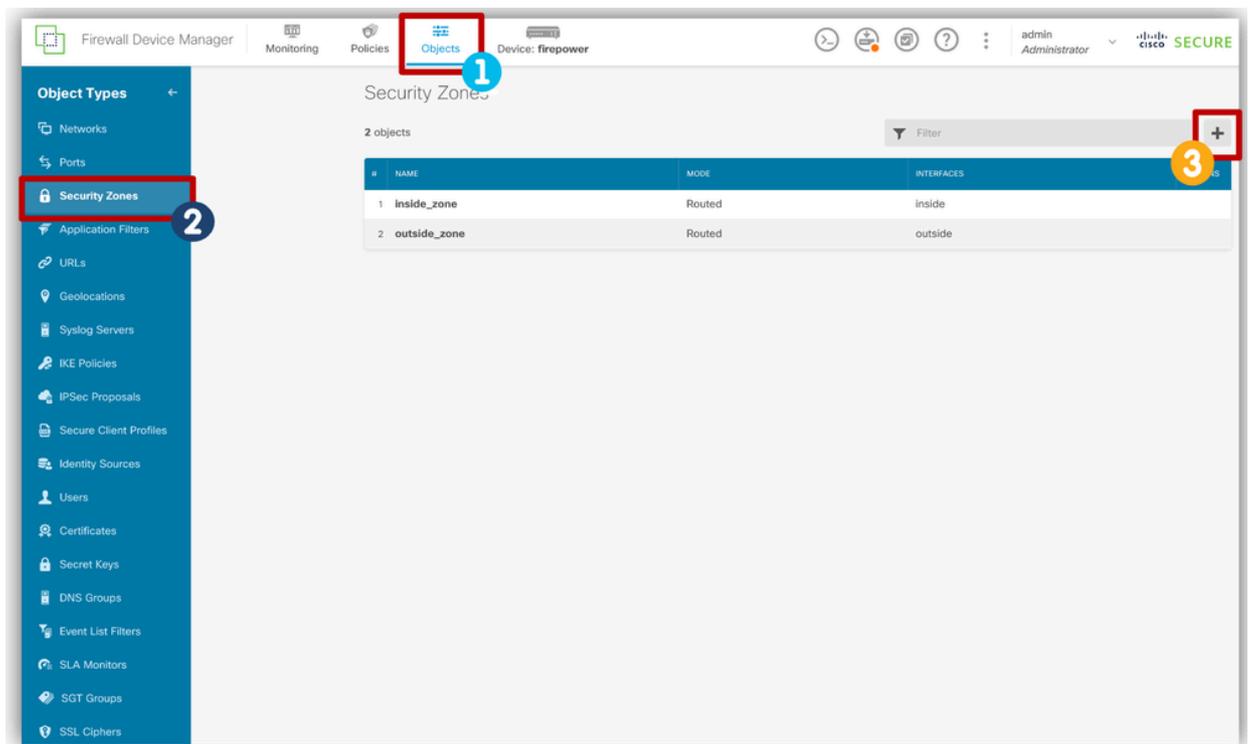
- Snort Fail Open Settings.
 - Sélectionnez les paramètres Snort Fail Open souhaités.
 - Aucun, un ou les deux. Les options Occupé et Désactivé peuvent être définies.
 - Snort Fail Open permet au trafic nouveau et existant de passer sans inspection (activé) ou abandon (désactivé) lorsque le processus Snort est occupé ou arrêté.

Snort Fail Open et Propagate Link State

- État de la liaison propagée.
 - Propagate Link State désactive automatiquement la deuxième interface de la paire Inline lorsque l'une des interfaces est désactivée. Lorsque l'interface désactivée redémarre, la deuxième interface redémarre également automatiquement.
- Cliquez sur OK pour créer le jeu en ligne.

Étape 4 : appliquez-la à une zone de sécurité (facultatif).

1. Dans la barre de navigation supérieure, accédez à Objets.
2. Sélectionnez Zones de sécurité dans le volet de navigation de gauche :
 - Cliquez sur + pour ajouter une zone de sécurité.



Ajouter une zone de sécurité

Configurer la zone de sécurité (facultatif)

1. Nommez la zone de sécurité.
2. Sélectionnez Inline Mode.
Les zones de sécurité et les interfaces doivent avoir le même mode.
3. Sélectionnez Interfaces faisant partie du jeu en ligne.
4. Click OK.

Add Security Zone

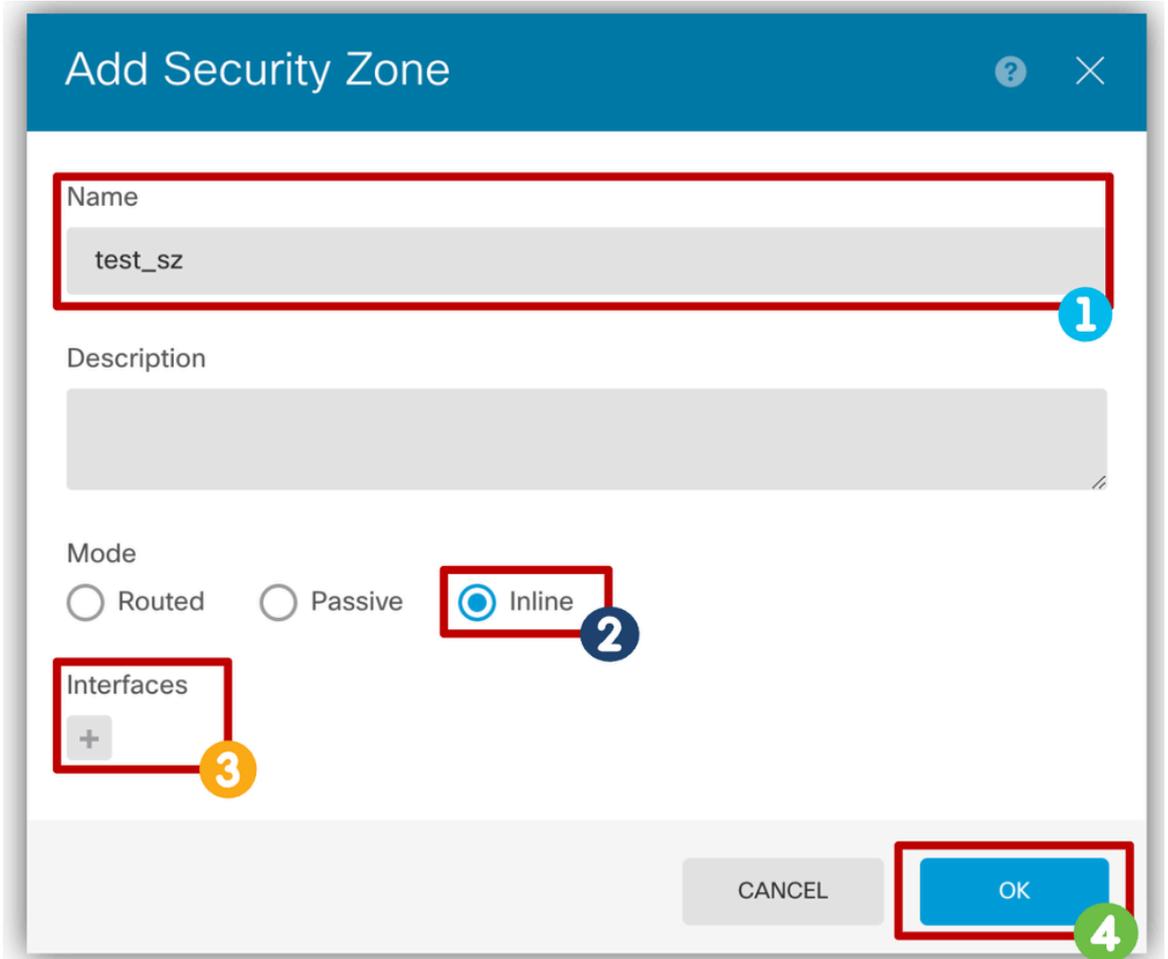
Name
test_sz 1

Description

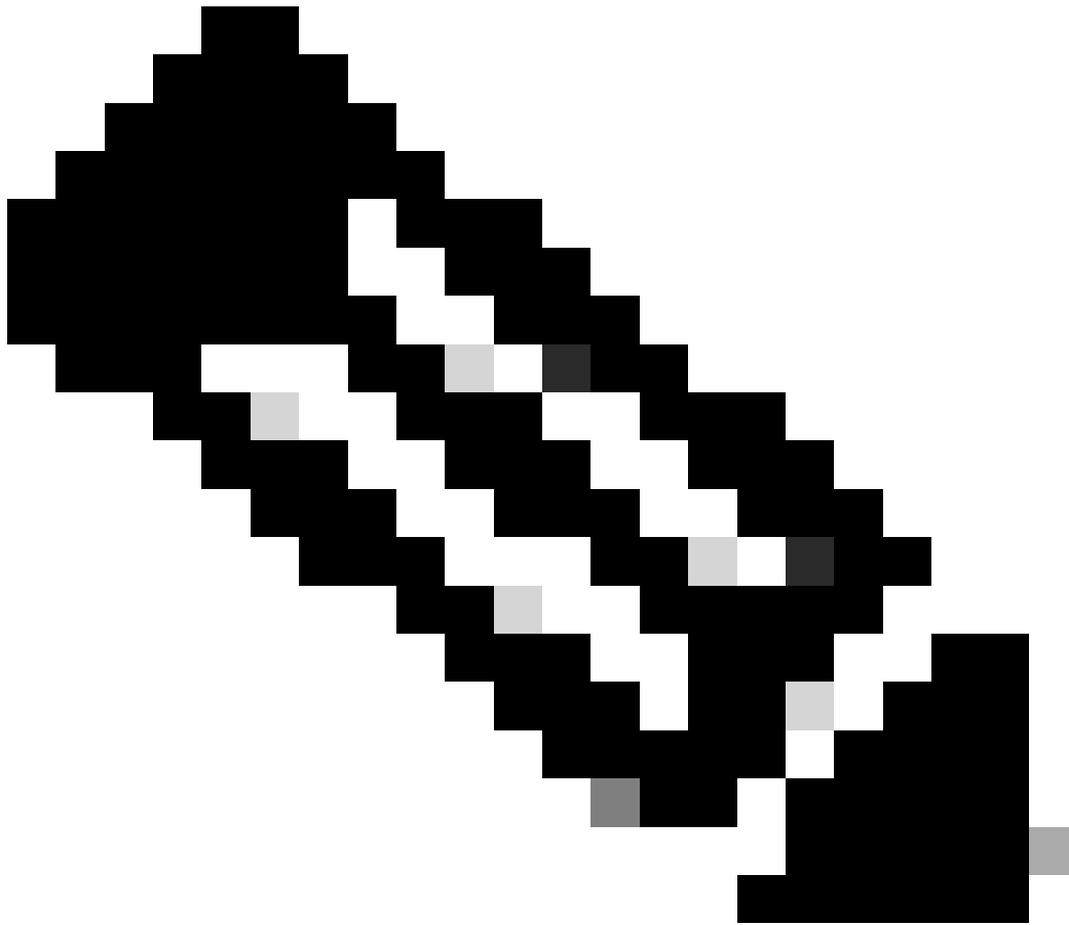
Mode
 Routed Passive Inline 2

Interfaces 3
+

CANCEL OK 4



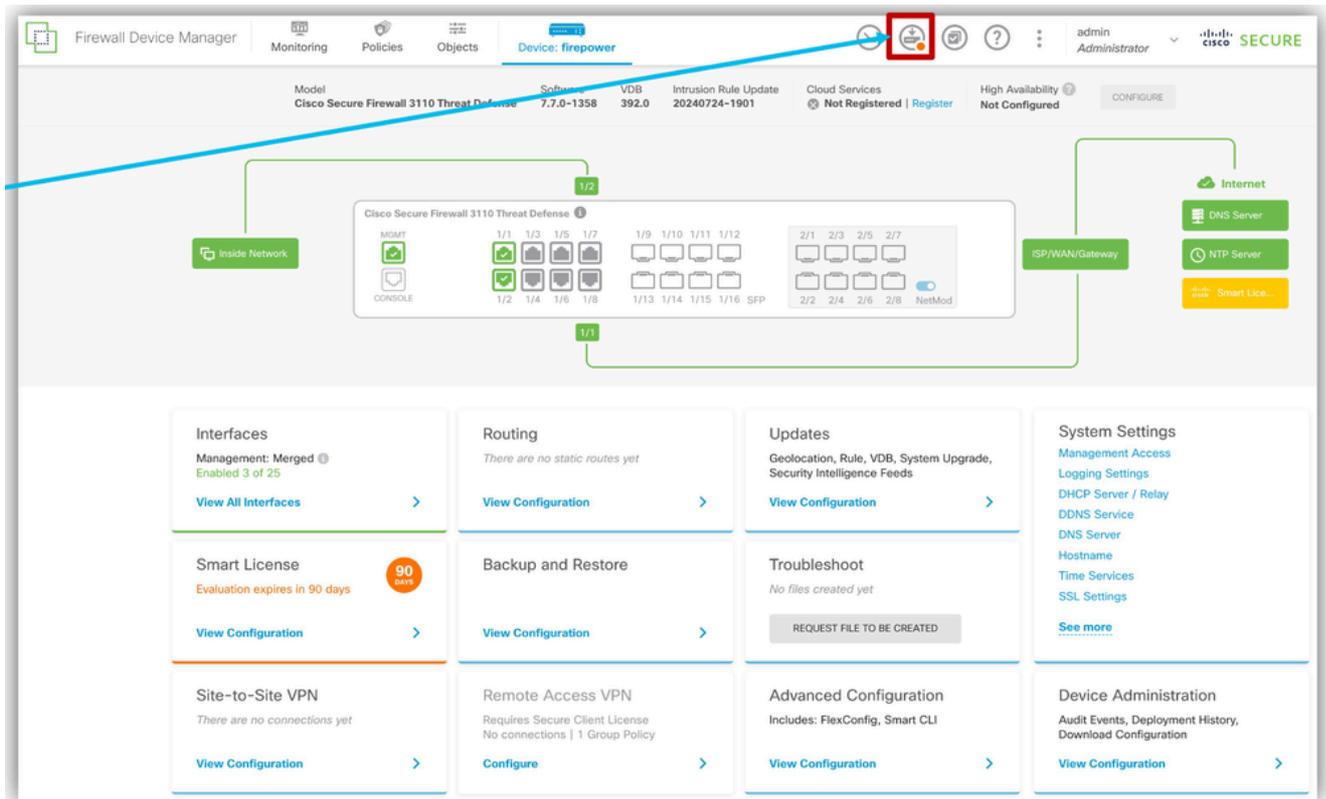
Configurer la zone de sécurité



Remarque : Pour les interfaces, le mode est automatiquement passé à Inline après l'ajout de l'interface dans une paire Inline.

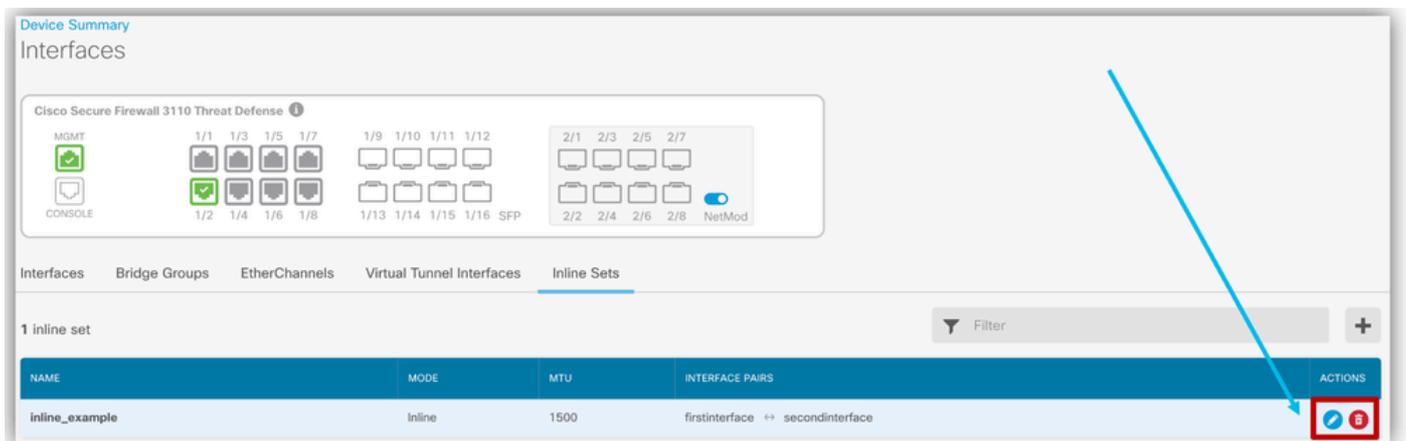
Étape 4 : Déploiement

- Accédez à l'onglet Déploiement et déployez.



Déployer les modifications

- Modifier et supprimer des jeux en ligne.
 - Accédez à Device > Interfaces > Inline sets tab.
 - Les boutons Modifier et Supprimer sont disponibles pour les jeux en ligne.



Modifier et supprimer des jeux en ligne

API REST du périphérique FDM

Terminaux API REST

- GET : /devices/default/inlinesets
Récupère la liste de tous les jeux en ligne existants.

- GET : /devices/default/inlinesets/{objID}
Récupère un objet inline-set spécifique par son ID.
- POST : /devices/default/inlinesets
Créer un nouveau jeu en ligne.
- PUT : /devices/default/inlinesets/{objID}
Mettre à jour l'objet inline-set existant par son ID.
- SUPPRIMER : /devices/default/inlinesets/{objID}
Supprimer l'objet de jeu en ligne existant par son ID.
- GET : /operational/interfaceinfo/{objID}
Récupère la liste de toutes les Infoentités d'interface.
- Pour prendre en charge le contournement matériel, un nouveau champ a été ajouté à l'API InterfaceInfo.

Informations d'interface Modèles API REST

- Un nouveau champ `bypassInterfacePeerId` a été ajouté pour faciliter l'intégration du contournement matériel.
- Ce champ représente l'ID de la paire d'interfaces de contournement matériel pour l'interface actuelle.
- Valeurs:
 - Null : l'interface ne prend pas en charge le contournement.
 - ID : l'interface prend en charge le contournement.

```

{ "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 API REST

Exemple d'API REST Interface Info

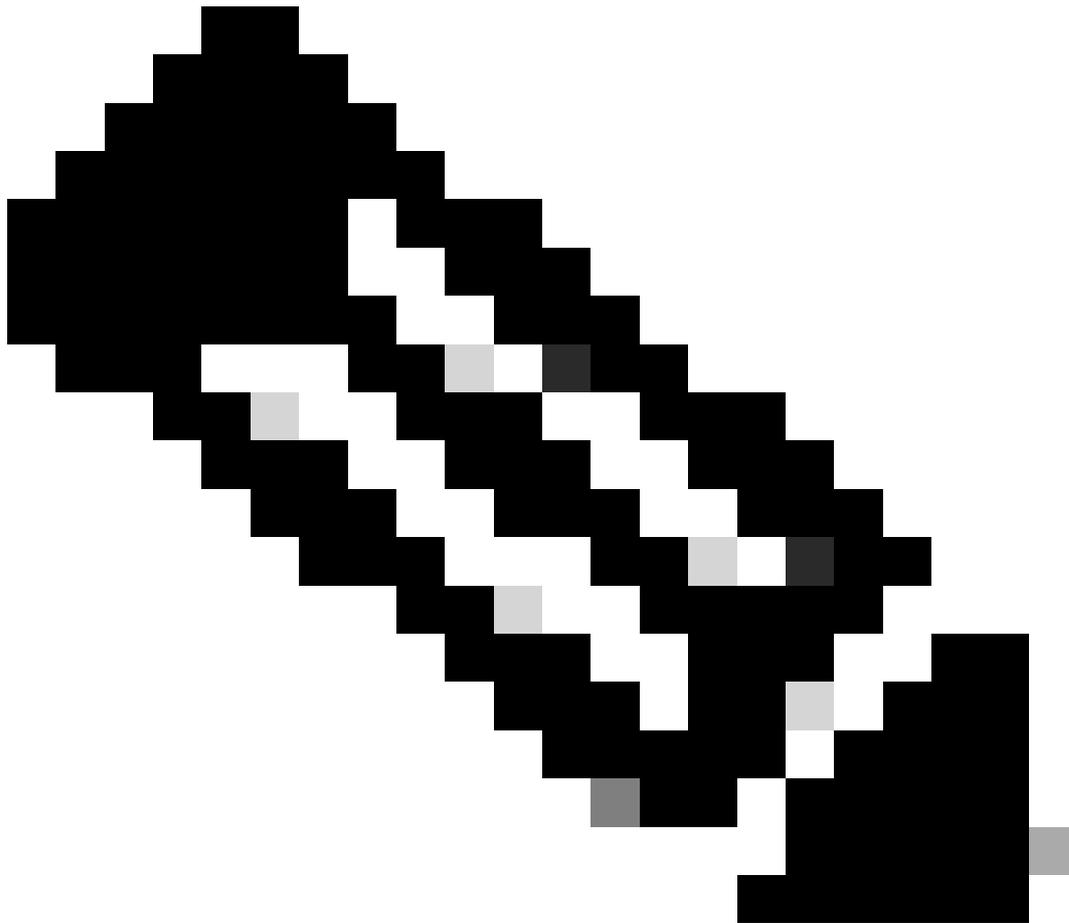
- Exemple d'API REST d'informations d'interface.
 - Interface sans prise en charge du contournement matériel (Ethernet 1/4).
 - Paire d'interfaces avec prise en charge du contournement matériel (Ethernet 2/1 et Ethernet 2/2).

```

{ "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-b764-11d423dbcbd7",
    ...
  },
  {
    "interfaceId": "dc74fbc3-58ba-11ef-b764-11d423dbcbd7",
    "hardwareName": "Ethernet2/2",
    "bypassInterfacePeerId": "dbe9d2c1-58ba-11ef-b764-396644d1c752",
    ...
  }
],
"id": "default",
"type": "interfaceinfo",
"links": { "self": "https://u90c04p02-
vrouter.cisco.com:25455/api/fdm/v6/operational/interfaceinfo/1/default"
}
}

```

Exemple d'API REST Interface Info



Remarque : Il s'agit d'un extrait de l'appel complet, en raison de sa taille.

Modèle API REST du jeu en ligne

- Le modèle Jeu en ligne se compose des éléments suivants :
 - Type
 - Nom
 - Effleurez Mode
 - MTU
 - Propager l'état des liaisons
 - Échec ouverture Snort occupé
 - Ignorer les valeurs : DÉSACTIVÉ, VEILLE, FORCE_CONTOURNEMENT

```

{
  "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

Exemple d'API REST Inline Set

- Exemples de jeux en ligne de base avec :

- Une paire en ligne
- Contourner la veille

```
{
  "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"
    }
  ]
}
```

Pour les autres modes de contournement, remplacez STANDBY par DISABLED ou BYPASS_FORCE.

Configuration et déploiement d'un jeu en ligne

1. Obtenez les ID d'interface (voir l'Explorateur d'API pour des exemples de données utiles).

GET/périphériques/par défaut/interfaces

2. Create Inline Set (voir API Explorer pour des exemples de données utiles).

POST/périphériques/par défaut/inlinesets

3. Créez une zone de sécurité (voir l'explorateur d'API pour des exemples de données utiles) (facultatif).

Zones POST/objet/sécurité

4. Déployez vers le périphérique (voir l'Explorateur d'API pour des exemples de charge utile).

POST/opérationnel/déploiement

Configuration et déploiement d'un ensemble en ligne avec contournement matériel

1. Obtenez les ID d'interface et les informations sur les paires d'interface de contournement matériel (voir l'Explorateur d'API pour des exemples de charge utile).

GET/opérationnel/interfaceinfo/{objId}

2. Create Inline Set (voir API Explorer pour des exemples de données utiles).

POST/périphériques/par défaut/inlinesets

3. Créez une zone de sécurité (voir l'explorateur d'API pour des exemples de données utiles) (facultatif).

Zones POST/objet/sécurité

4. Déployez vers le périphérique (voir l'Explorateur d'API pour des exemples de charge utile).

POST/opérationnel/déploiement

Modifier un jeu en ligne

1. Obtenez les ID d'interface (voir l'Explorateur d'API pour des exemples de charge utile).

GET/périphériques/par défaut/interfaces

2. Obtenez des jeux en ligne.

GET/périphériques/par défaut/inlinesets

3. Modifiez l'ensemble en ligne (voir l'explorateur d'API pour des exemples de données utiles).

PUT/périphériques/par défaut/inlinesets/{objId}

4. Déployez vers le périphérique (voir l'Explorateur d'API pour des exemples de charge utile).

POST/opérationnel/déploiement

Vérifier

<#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
```

Dépannage

Commandes

- show running-config inline-set
- show inline-set
- show interface
- suivi du support système

Jeu en ligne - Validations lors de la création

- Des erreurs sont présentées sur l'interface graphique utilisateur pour chacun des champs.
 - Le nom doit être renseigné.
 - La taille MTU doit être au moins égale à 1 500.
 - Les deux interfaces d'une paire doivent être sélectionnées.

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

Taille de MTU

Contournement matériel - Validation lors de la création

- De nouvelles erreurs sont présentées sur l'interface graphique utilisateur pour chacun des champs, lorsque le contournement est activé :
 - Toutes les interfaces doivent prendre en charge le contournement.
 - Erreur : interfaces non prises en charge.
 - Toutes les paires doivent utiliser la paire d'interfaces prédéterminée.

- Le message d'erreur mentionne les paires d'interfaces de contournement disponibles.

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	MTU
test	1500

General Advanced

Bypass

Standby

Interface Pairs

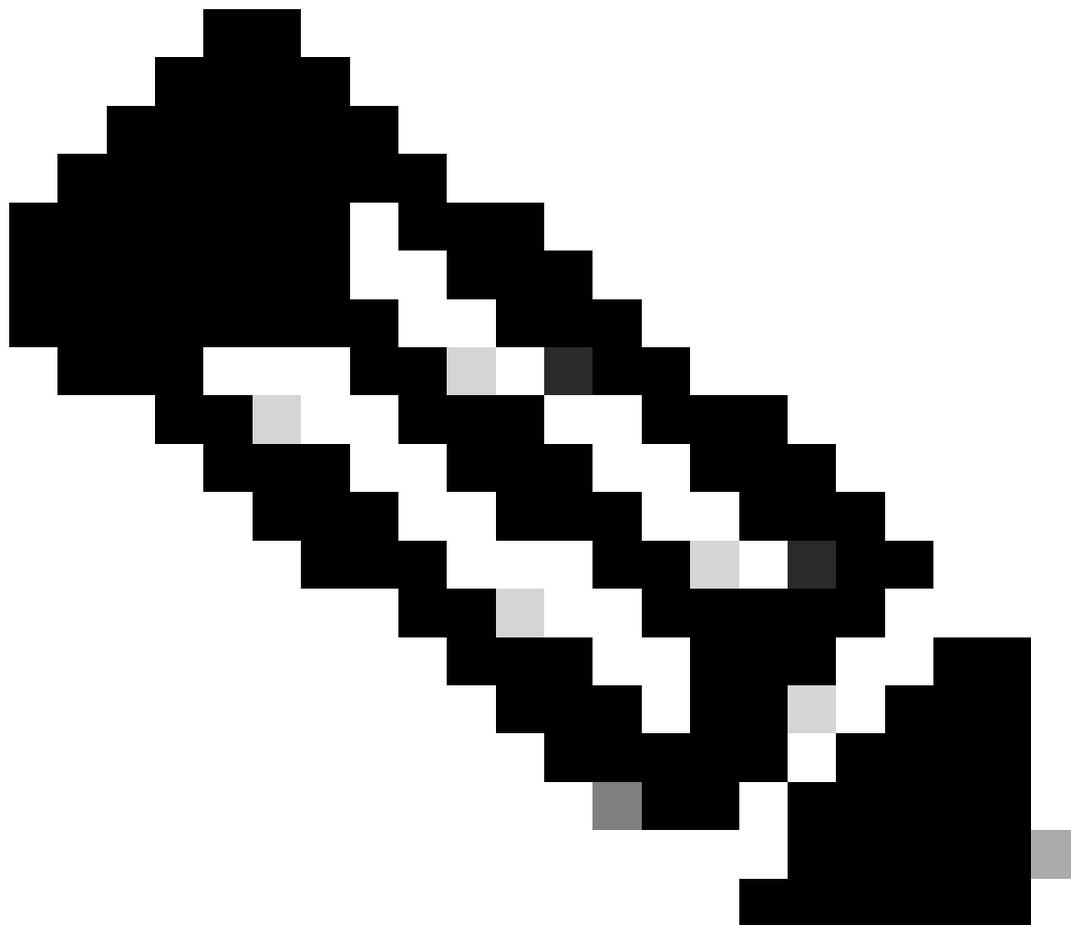
firstinterface (Ethernet2/1)	↔	secondinterf... (Ethernet2/2)	✖
fourthinterfa... (Ethernet2/4)	↔	fifthinterface (Ethernet2/5)	✖
interface3 (Ethernet1/3)	↔	interface4 (Ethernet1/4)	✖

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

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

[Add another pair](#)

CANCEL OK



Remarque : La première paire (Ethernet2/1-Ethernet2/2) est valide.

La réponse REST API affiche des erreurs

- Les erreurs sont présentées dans la réponse de l'API REST.
 - Ici, la valeur MTU n'est pas valide.

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

Validation de l'API REST

Limites de l'implémentation de cette version

- Jeux en ligne : Fonctionne uniquement avec les interfaces physiques et EtherChannel.
- Jeux en ligne avec contournement matériel : Fonctionne uniquement avec les interfaces physiques et nécessite un module réseau.

Fonctions de pare-feu non prises en charge sur les interfaces en ligne

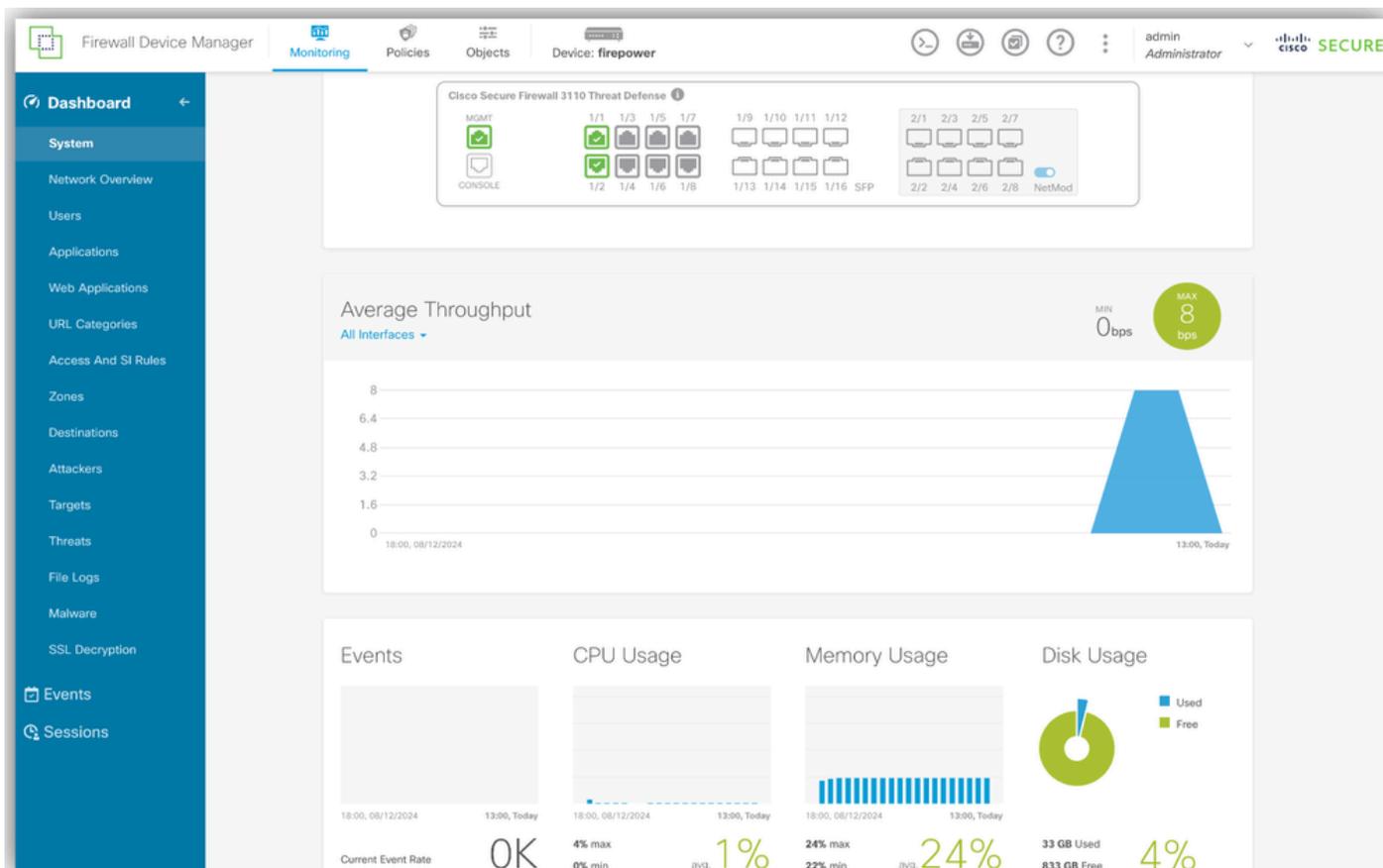
- Serveur DHCP
- Relais DHCP
- Client DHCP
- Interception TCP
- Routage
- NAT
- VPN
- Application
- inspection
- QoS
- NetFlow

Vérification des journaux depuis CLI

- Journalisation.
 - Les journaux sont disponibles à l'adresse `/ngfw/var/log/cisco/ngfw-onbox.log`.
 - Recherchez le jeu en ligne.
 - Exemple d'erreurs possibles trouvées dans les journaux :
 - Deux interfaces ne prennent pas en charge le contournement.
 - Deux interfaces ne constituent pas une paire de dérivation valide.

```
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
```

- Vérifier le trafic à partir de la GUI.
 - Les événements sont présentés sur l'interface utilisateur graphique.
 - L'exactitude du flux de trafic peut être surveillée ici.
 - Accédez à Surveillance > Système.



Surveillance FDM

- Vérifier l'exactitude du trafic depuis 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]

FAQ

Q : La haute disponibilité est-elle prise en charge avec les jeux en ligne sur FDM ?

R : Les jeux en ligne sans contournement sont pris en charge.

Les jeux en ligne avec contournement NE sont PAS pris en charge.

Q : Les unités BPDU Spanning Tree sont-elles bloquées sur la paire d'ensembles en ligne ?

A : Non, ils ne sont pas bloqués.

Q : Les cartes FTW sont-elles prises en charge dans 3100 ?

A : Oui, les modules de réseau FTW sont pris en charge depuis l'introduction de la gamme 3100 avec 7.1/9.17. Le contournement matériel est disponible à partir de la version 7.7.0.

Q : Pour les cartes FTW 3100, les modes de contournement Désactivé, En attente, Contournement forcé sont-ils pris en charge ou non sur FMC ?

A : Le contournement matériel est disponible à partir de la version 7.7.0 sur les périphériques 3100 équipés de cartes FTW.

Q : Les jeux en ligne avec des canaux de port sont-ils également pris en charge lorsque le trafic est asymétrique sur les canaux de port ?

A : Aucune validation n'est effectuée sur le débit configuré PortChannel, donc tant que le FTD le prend en charge, il doit être pris en charge.

Q : Si Snort échoue pour l'inspection, est-ce que failopen est pris en charge ?

A : Reportez-vous à la documentation relative à ce paramètre dans le [Guide de configuration de Firepower Management Center](#).

Informations connexes

- [Configuration des interfaces FTD en mode Inline-Pair](#)
- [Guide de configuration de Firepower Management Center, version 6.3](#)
- [Guide d'installation matérielle de Cisco Secure Firewall 3100](#)
- [Fiche technique sur la gamme Cisco Secure Firewall 3100](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.