

セキュア・ファイアウォール3100 FDM 7.7.0ハードウェア・バイパスの構成

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[基本：サポートされるプラットフォーム、ライセンス](#)

[機能説明とワークスルー](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[ハードウェアバイパス](#)

[FDMデバイスREST API](#)

[確認](#)

[トラブルシュート](#)

[コマンド](#)

[インラインセット – 作成時の検証](#)

[ハードウェアバイパス – 作成時の検証](#)

[このリリースの実装の制限](#)

[インラインインターフェイスでサポートされていないファイアウォール機能](#)

はじめに

このドキュメントでは、Firepower Device Manager(FDM)管理対象セキュアファイアウォール7.7.0でインラインセットのハードウェアバイパス(HB)を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- インラインセット
- Cisco Secure Firewall 3100 シリーズ
- Firepowerデバイスマネージャ(FDM)のグラフィカルユーザインターフェイス(GUI)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- v7.7.0が稼働するCisco Secure Firewall 3100
- Cisco Secure Firewall Device Manager v7.7.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

インラインセット機能は、7.4.1でFDMに追加されました。インラインセットにより、ルーティングを必要としないL2ネットワークでの検査が可能になります。[インラインペアモードでFTDインターフェイスを設定します。](#)

今回のリリースとの違い

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.

セキュアファイアウォール7.0バイパス機能

最新情報

- ハードウェア検査バイパスにより、停電中もインラインインターフェイスペア間でトラフィックが流れ続けます。
- この機能は、ソフトウェアまたはハードウェアの障害時にネットワーク接続を維持するために使用されます。
- FDM 3100シリーズ・プラットフォームのインライン・セットでハードウェア・バイパスが使用可能になりました。



注: 『[Firepower Management Centerコンフィギュレーションガイド](#)』

導入シナリオ

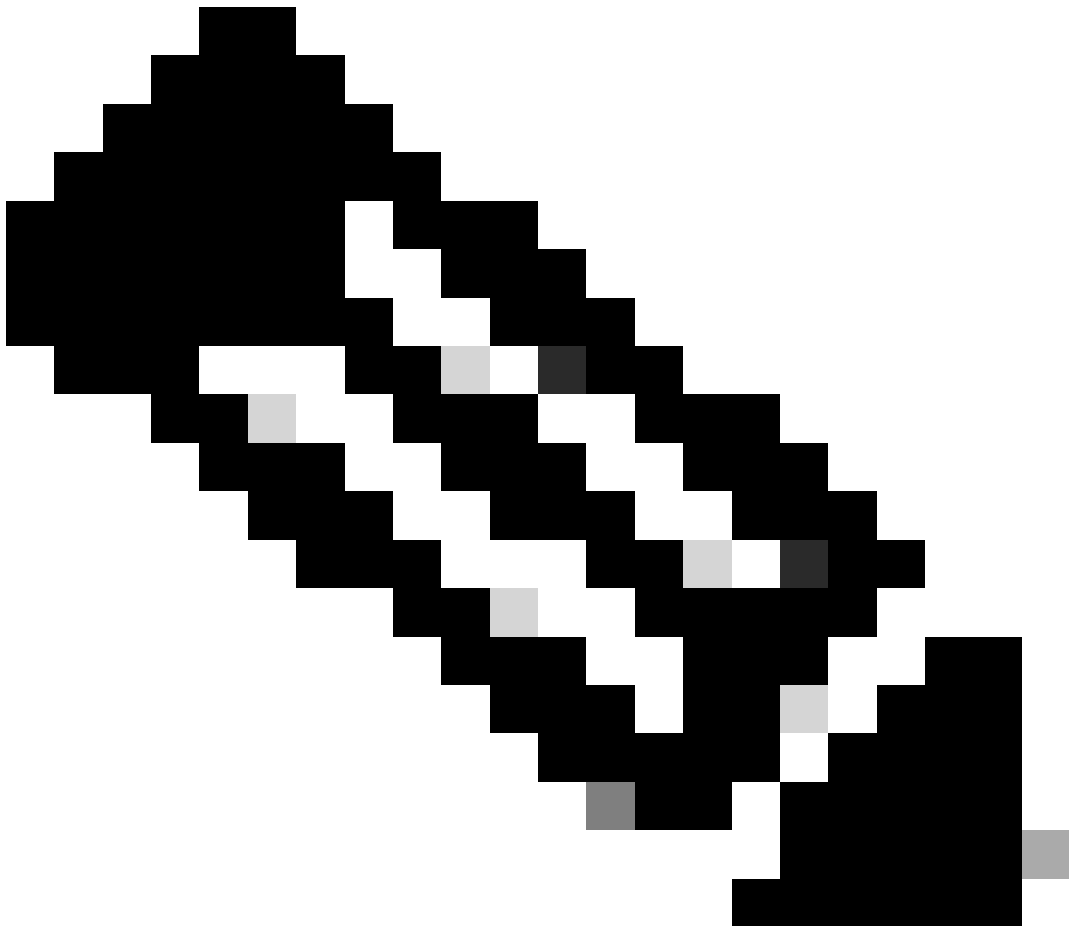
- この機能は実稼働環境の設定にどのように適合しますか。
 - インラインセットは、IPS (またはIDS) のユースケースで使用されます。
 - ルーティング設定を必要とせずにトラフィック検査を可能にします。ユニットがハードウェアバイパス経由で障害が発生した場合にトラフィックフローを許可します。
- 実例 :
 - レイヤ3を必要とせずに、どこでも高速かつ簡単な方法でレイヤ2ネットワーク検査を設定できます。
 - 完全に分離されたネットワークに不可欠 – インターネットアクセスなし。
 - スタンドアロンファイアウォールのディープパケットインスペクションのための透過的なインライン挿入：既存の実稼働レイヤ2アーキテクチャ。

基本：サポートされるプラットフォーム、ライセンス

ソフトウェアとハードウェアのバージョン

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

ソフトウェアとハードウェア



注:3100シリーズとハードウェアバイパスの情報

サポートのその他の側面

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

ライセンスと互換性

機能説明とウォークスルー

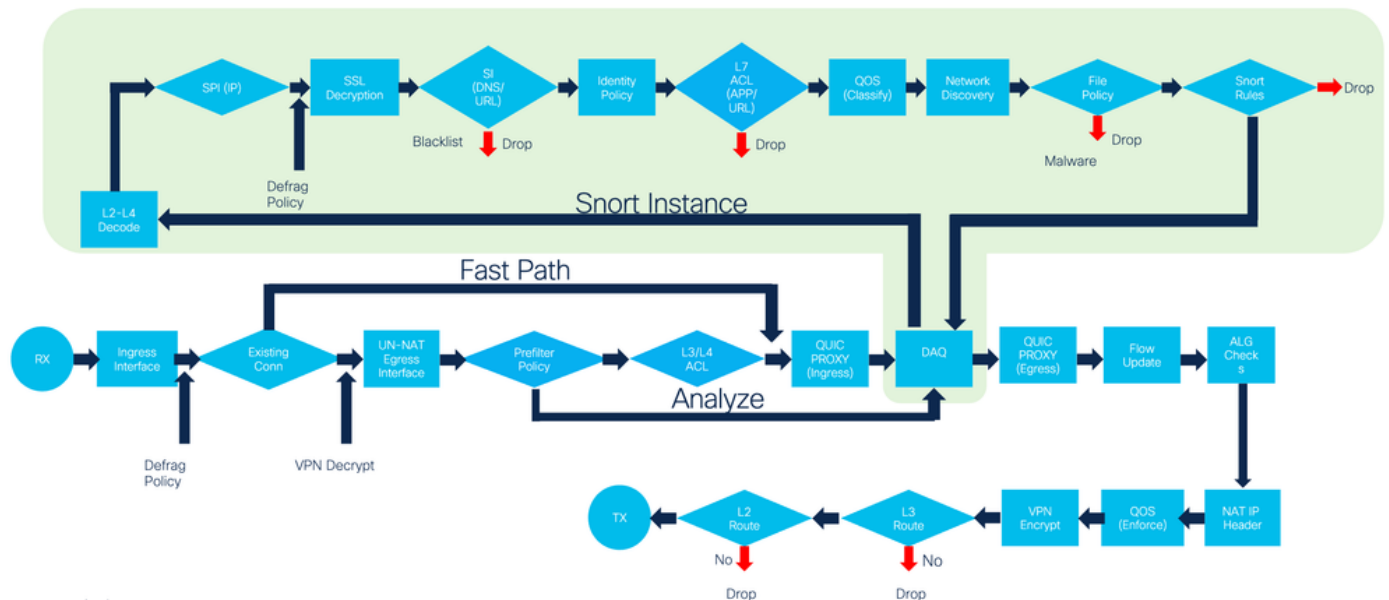
機能の説明

- インラインセットネットワークダイアグラム



インラインセットネットワークダイアグラム

- トラフィックは、物理接続のみを使用して、インターフェイスAおよびBを経由して、ルータ1からルータ2へ流れます。
- FDMインライン・セット・パケット処理フロー図：



フロー図

- インラインセット：
 - インラインセットは、物理インターフェイスとEtherChannelでサポートされます。
- ハードウェアバイパス：
 - ハードウェアバイパスを備えたインラインセットは、事前に定義された物理インターフェイスペアでサポートされます。
 - イーサネット1および2
 - イーサネット2および3
 - イーサネット4および5
 - イーサネット5および6
- インターフェイスサポート：
 - インラインペアの一部であるインターフェイス：
 - 名前を指定する必要があります。
 - 私に何の不自由もないP、DHCP、またはPPPoEの設定
 - パッシブモードであってはなりません。
 - 管理インターフェイスであってはなりません。
 - 同時に1つのインラインペアでのみ使用する必要があります。
- インラインモードの詳細
 - インラインモードは、物理インターフェイス、EtherChannel、およびセキュリティゾーンで使用できます。
 - インラインモードは、インターフェイスとEtherChannelがインラインペアで使用される際に自動的に設定されます。
 - インラインモードは、インラインペアから削除されるまで、関係するインターフェイスとEtherChannelに対して変更が加えられることを防止します。
 - インラインモードのインターフェイスは、インラインモードに設定されたセキュリティゾーンに関連付けることができます。

- インラインモードGUI
 - [インターフェイスを編集]ダイアログに、インターフェイスまたはEtherChannelがインラインモードであることが反映されます。
 - インラインモードのインターフェイスでは、変更は許可されません。[物理インターフェイスの編集] (または[EtherChannelの編集]) ダイアログは読み取り専用です。

Ethernet1/5
Edit Physical Interface

Interface Name: loekhozjo

Mode: Inline

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:

GUIでのインターフェイスの編集

- アップグレード、インポート/エクスポート、バックアップ/リストア、導入
 - アップグレードの影響
 - ユーザーはFDMを制限なくアップグレードできます。
 - 以前のバージョンからアップグレードする場合、既存のインラインセットオブジェクトのバイパスフィールドが無効に設定されます。
 - インポート/エクスポートの影響
 - インラインセットオブジェクトはインポートおよびエクスポートされます。
 - バックアップ/復元
 - インラインセットオブジェクトは、バックアップ/復元中に処理されます。
 - 展開
 - オブジェクトは正常に配置されます。
 - 特定のエラーが実装されました。

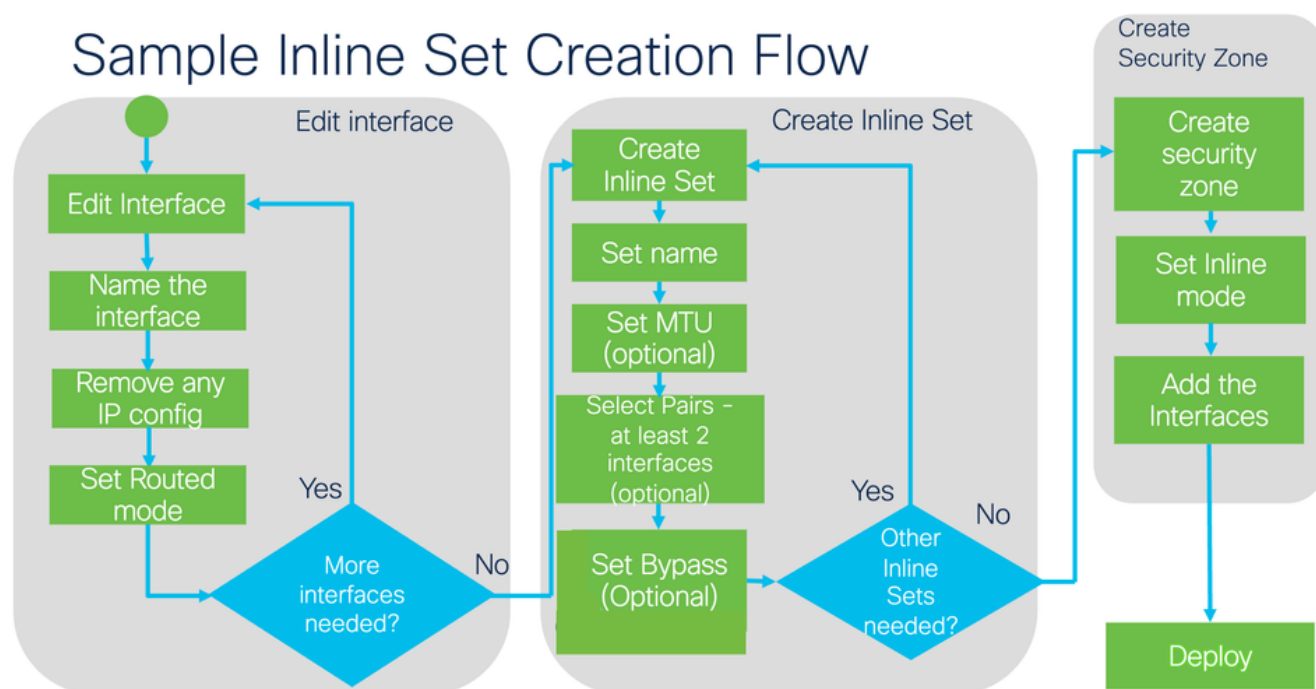
設定

ネットワーク図



ネットワーク図

Sample Inline Set Creation Flow



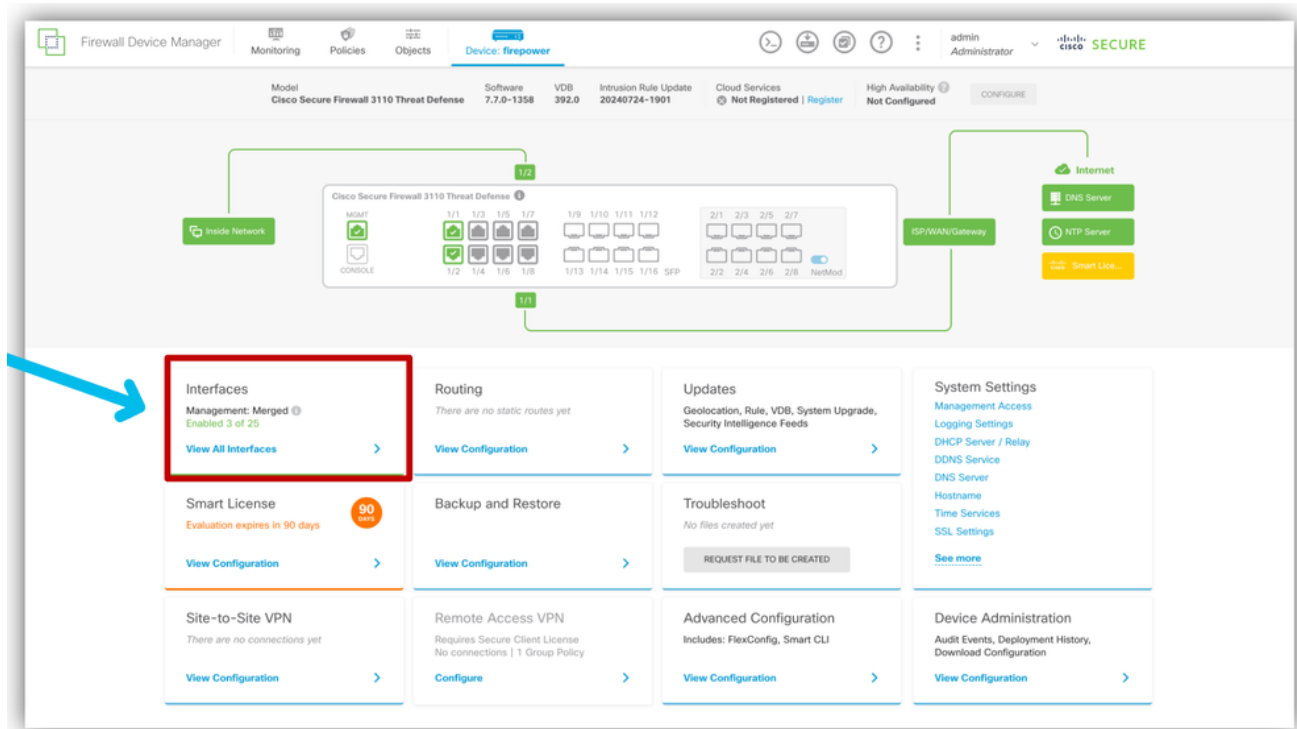
インラインセット作成フロー

コンフィギュレーション

この項では、FDMでハードウェア・バイパスを構成する手順について説明します

手順1：インターフェイスを編集します。

- FDMにログインし、n~を避ける インターフェイス管理。
- FDMダッシュボードで、Interfacesカードをクリックします。



インターフェイスの選択

- ・ インラインセットで使用するインターフェイスを編集します。
- ・ インターフェイスを編集するには、そのインターフェイスの編集 (鉛筆) アイコンをクリックします。

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	

インターフェイスの編集

- ・ 物理インターフェイスの編集 :

1. Interfaceという名前を付けます。
2. Routed Modeを選択します。
3. IP設定を削除します。

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

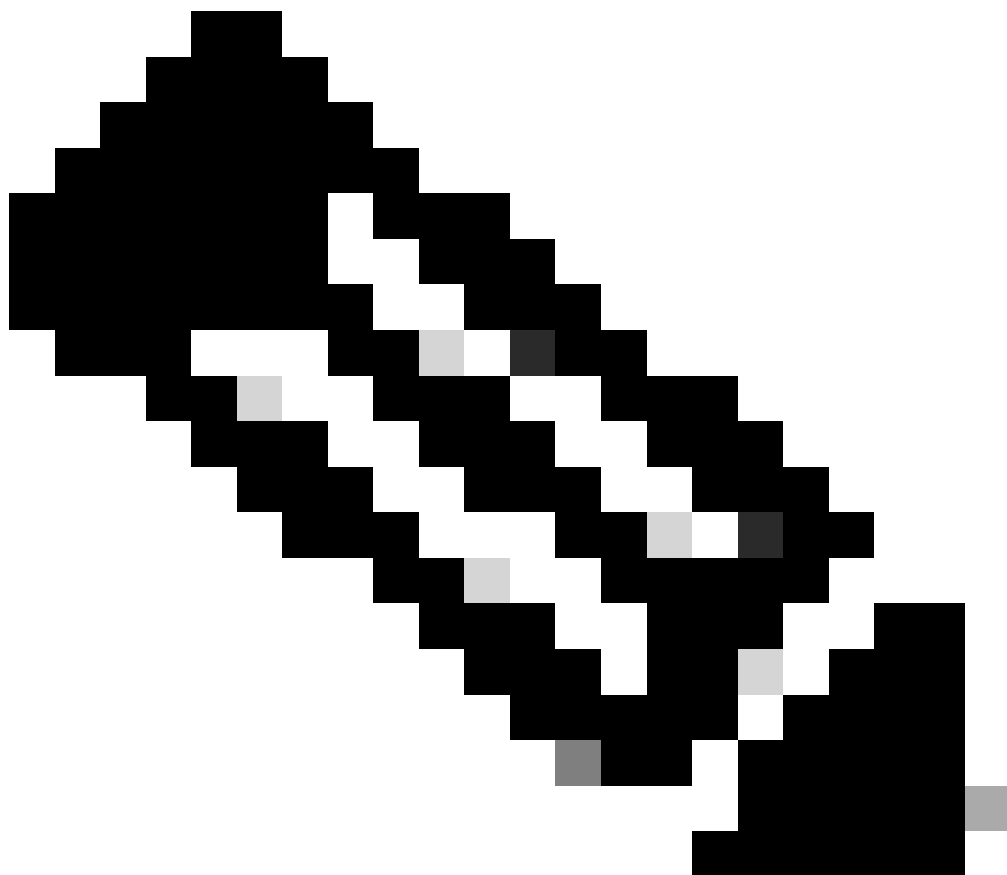
Type
Static

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

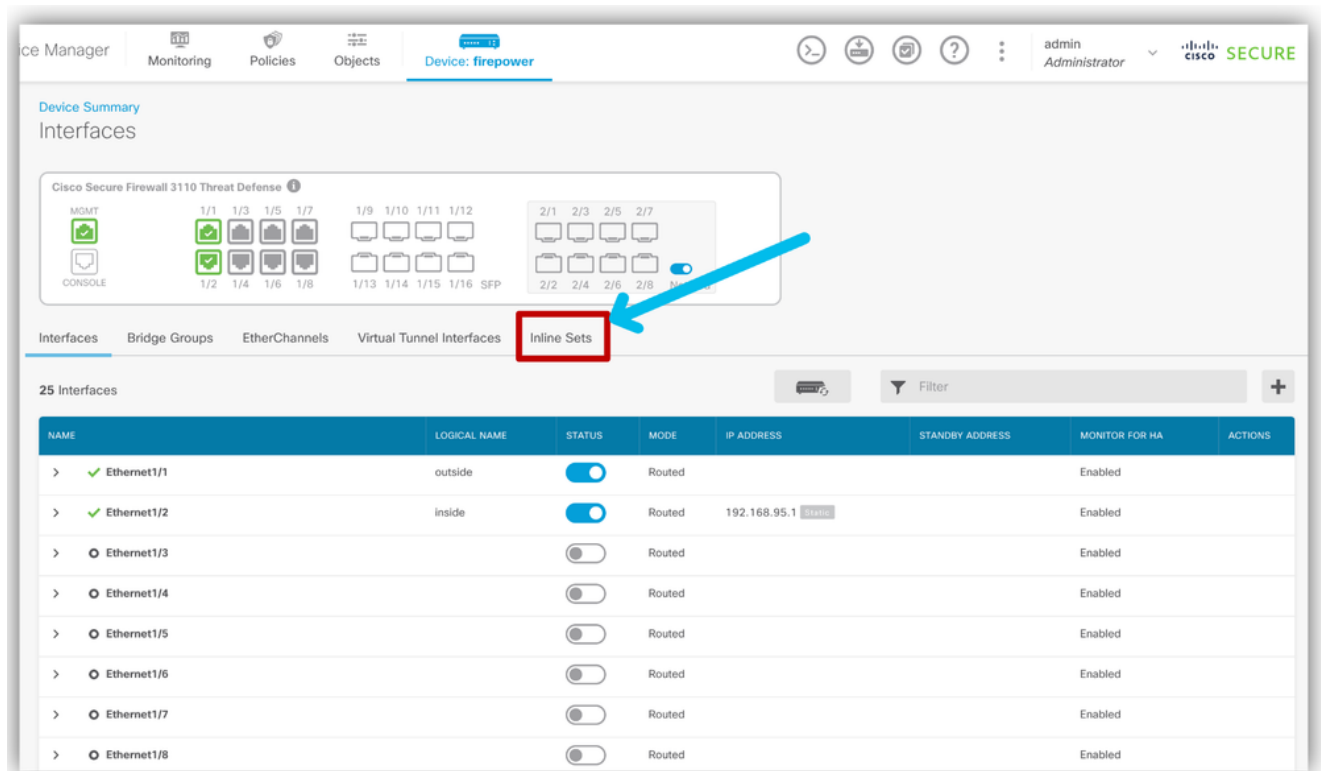
パラメータの設定



注：インラインペアにインターフェイスが追加されると、モードは自動的にインラインに変更されます。

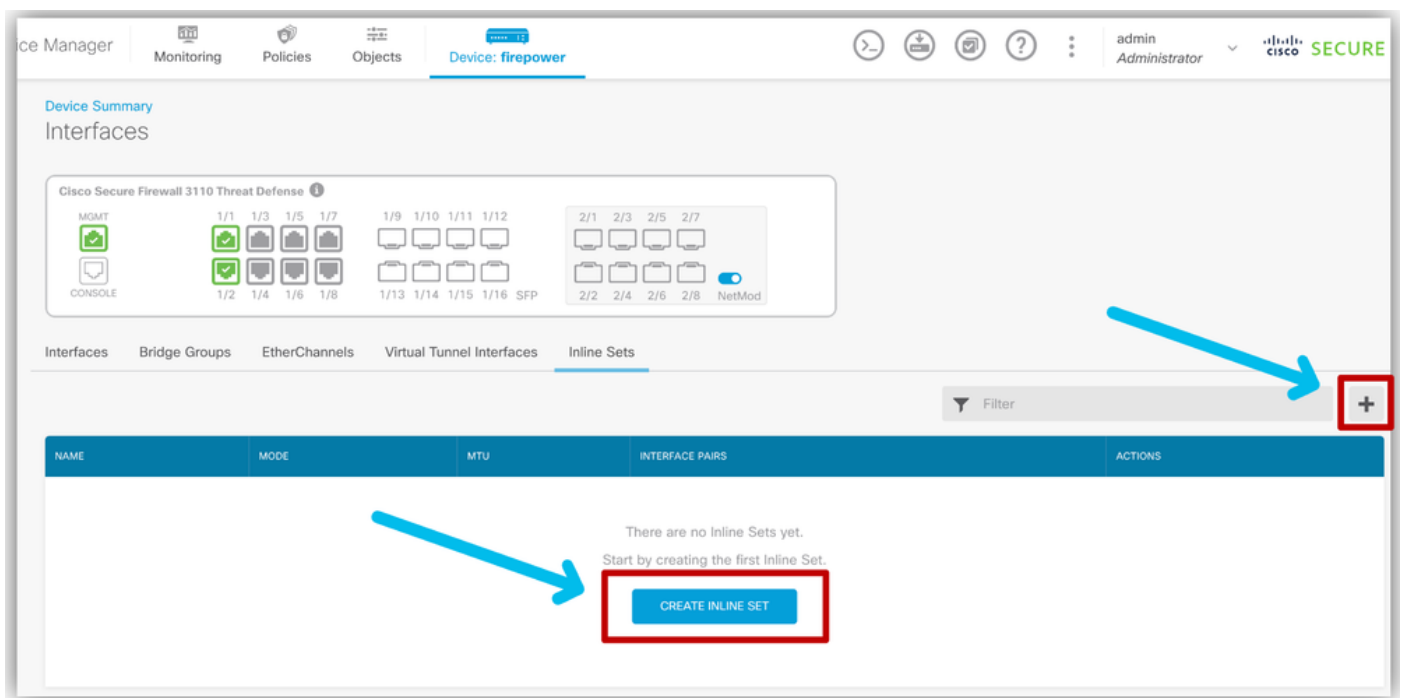
手順2：インラインセットを作成します。

- Device > Interfaces > Inline setsタブに移動します。



インラインセットタブに移動

- 新しいインラインセットを追加します。
- +アイコンまたはCreate Inline Setボタンをクリックします。



インラインセットの作成

- 基本設定を行います。
 1. 名前を設定します。
 2. 必要なMTUを設定します (オプション)。デフォルトは1500で、これはサポートされている最小のMTUです。
 3. ハードウェアバイパス (詳細は次のセクションで説明します) を選択します。バイパス用の新しいドロップダウンメニューが追加されました。
 4. Interface Pairsセクションでinterfacesを選択します。
 5. 名前付きインタフェースを選択できます。さらにペアが必要な場合は、Add another pairリンクをクリックします。

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

設定の構成

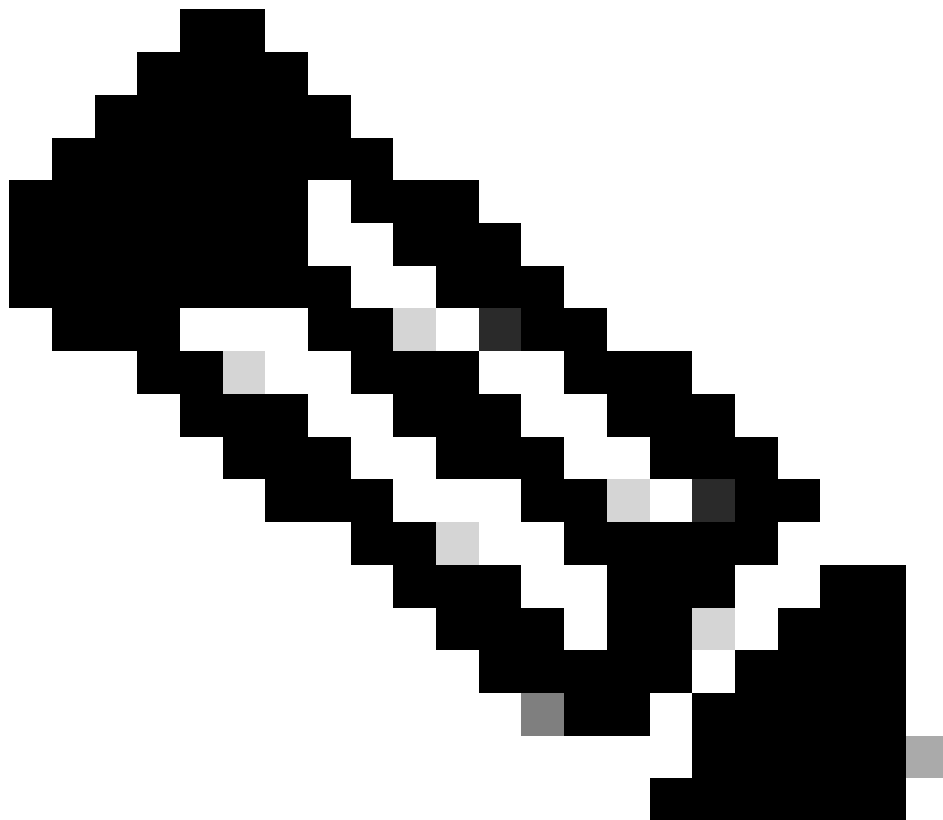
ハードウェアバイパス

機能と制限

- ハードウェアバイパスにより、停電時にもインラインインターフェイスペア間でトラフィック

クの流れが継続されます。この機能を使用すると、ソフトウェアまたはハードウェアに障害が発生した場合にネットワーク接続を維持できます。

- ハードウェアバイパスポートは、インラインセットに対してのみサポートされます。
- ハイアベイラビリティモードでは、ハードウェアバイパスはサポートされません。
- ハードウェアバイパスモード：
 - DISABLED：サポートされているインターフェイスでバイパスを無効にします。サポートされていないインターフェイスのデフォルトモード。
 - STANDBY：スタンバイ状態では、トリガーイベントが発生するまで、インターフェイスは通常動作を継続します。
 - BYPASS FORCE：インターフェイスペアを手動で強制的に検査をバイパスさせます。



注:[FTDインターフェイスタイプとハードウェアバイパスに関する情報](#)

Snortのフェールオープンとハードウェアバイパス

- ハードウェアバイパス機能により、完全な停電や特定の限定されたソフトウェア障害など、ハードウェア障害の発生時にトラフィックを転送できます。
- Snort Fail Openをトリガーするソフトウェア障害は、ハードウェアバイパスをトリガーしません。

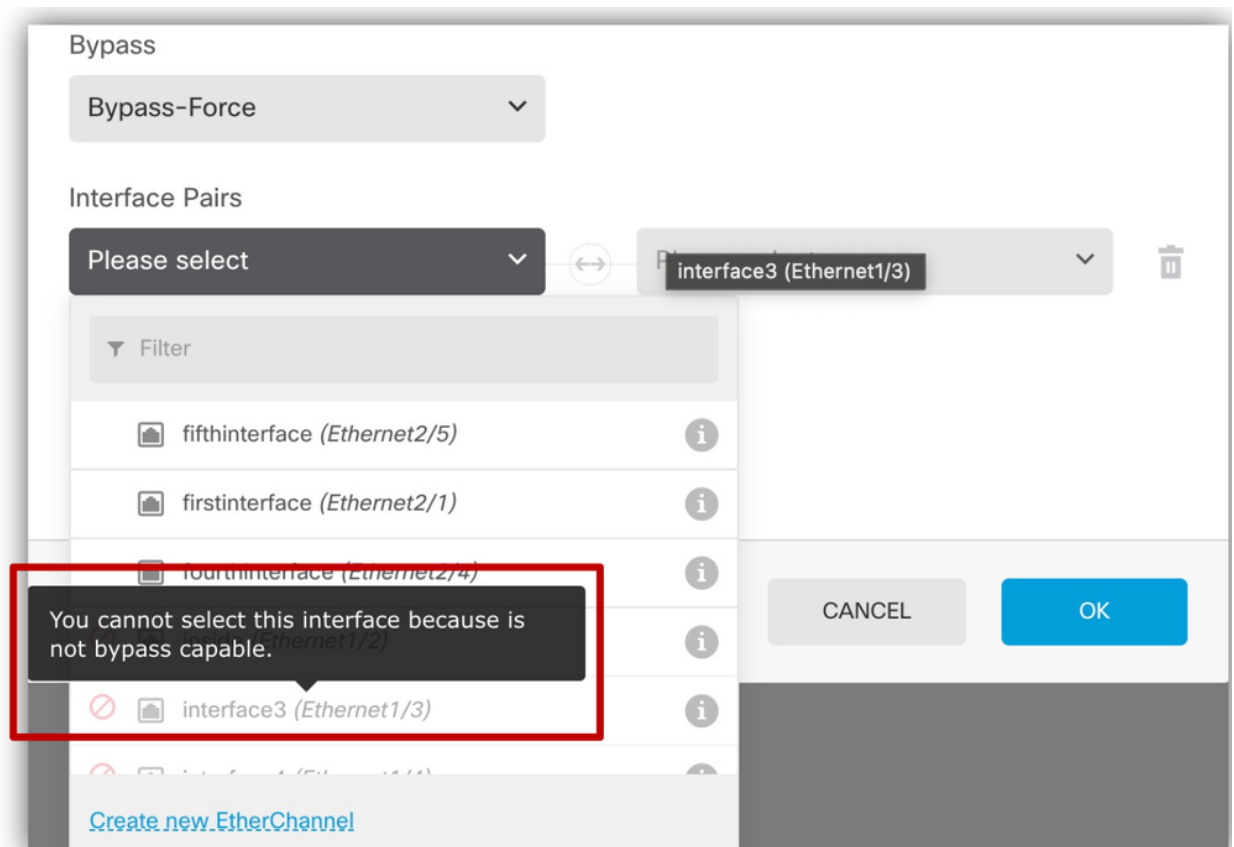
ハードウェアバイパストリガー

ハードウェアバイパスは、次のシナリオでトリガーされる可能性があります。

- アプリケーションクラッシュ
- アプリケーションの再起動
- デバイスのクラッシュ
- デバイスのリブートまたはアップグレード
- 医療機器の電力損失
- 手動トリガー

ハードウェアバイパスをサポートしているインターフェイスを確認するには、次のコマンドを実行します。

- FDMのGUIで、「バイパス」が選択されている場合は、次の手順を実行します：
 - これをサポートするインターフェイスは選択可能です。
 - サポートされていないインターフェイスはグレー表示されます。
 - この例では、次の図でEthernet1/3がグレー表示されています。



ハードウェアバイパスサポートの確認

ステップ3：インラインセットAdvanced設定を設定します。

- Device > Interfaces > Inline setsタブに移動するか、作成済みのインラインセットを編集します。
- [Advanced] タブまで移動します。
 - [詳細設定]タブでは、インラインセットのオプションの設定を構成できます。

- [Advanced] タブをクリックします。

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

インラインセットの設定

- モード
 - Tap: インラインタップモードに設定します。タップモードが有効になっている場合、Snort Fail Openは無効になります。
 - インライン

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

モードの選択

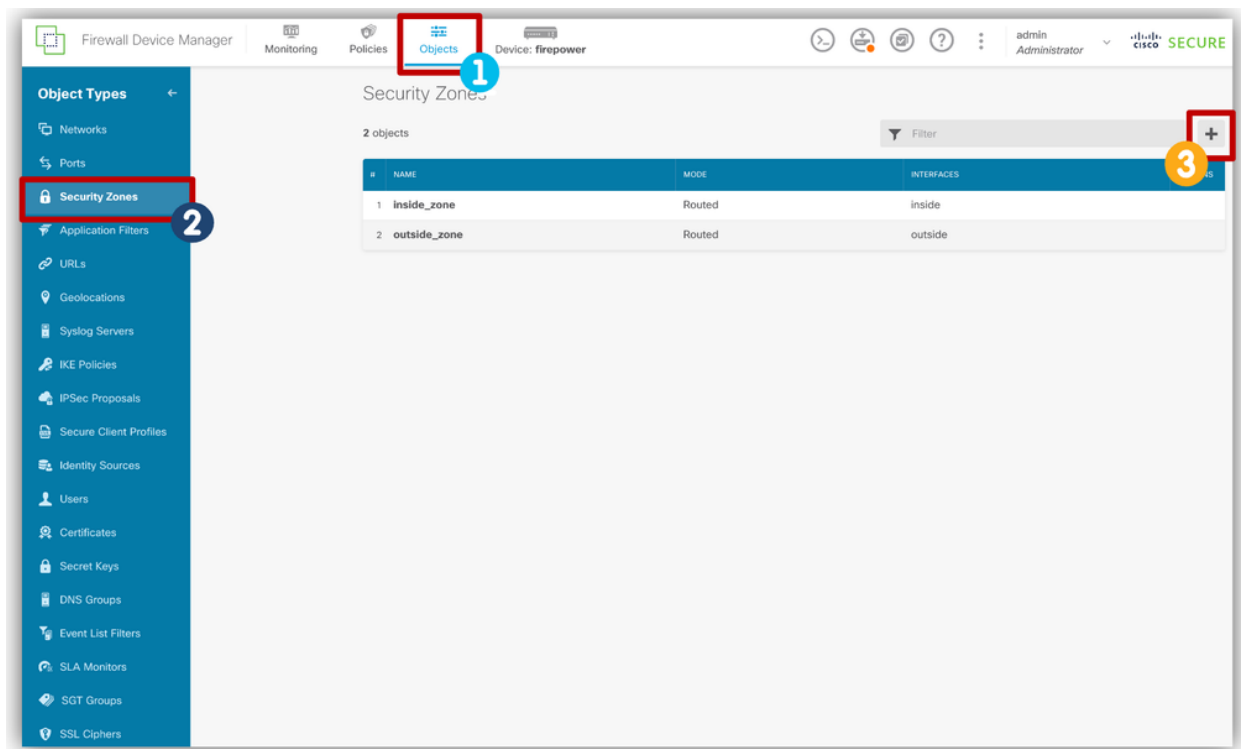
- Snortのフェールオープン設定
 - 必要なSnort Fail Open設定を選択します。
 - None、one、またはboth。BusyオプションとDownオプションを設定できる。
 - Snort Fail Openでは、Snortプロセスがビジーまたはダウンの場合、新規および既存のトラフィックをインスペクションなしで通過させる（有効）か、ドロップする（無効）ことができます。

Snortのフェールオープンとリンクステートの伝播

- 。 リンクステートの伝達。
 - 。 Propagate Link Stateは、インラインペア内の2番目のインターフェイスがダウンしたときに、そのインターフェイスを自動的にダウンさせます。ダウンしたインターフェイスがアップ状態に戻ると、2番目のインターフェイスも自動的にアップ状態に戻ります。
- 。 OKをクリックして、インラインセットを作成します。

ステップ4：セキュリティゾーンに適用します（オプション）。

1. 上部のナビゲーションバーから、Objectsに移動します。
2. 左側のナビゲーションからSecurity Zonesを選択します。
 - ・ +をクリックして、セキュリティゾーンを追加します。



セキュリティゾーンの追加

セキュリティゾーンを設定する（オプション）

1. Security Zoneという名前を付けます。

2. Inline Modeを選択します。

セキュリティゾーンとインターフェイスは、同じモードである必要があります。

3. インラインセットの一部であるインターフェイスを選択します。

4. [OK] をクリックします。

Add Security Zone?×

Name

test_sz

Description

Mode

☐ Routed

☐ Passive

☒ Inline

Interfaces

+

CANCEL

OK

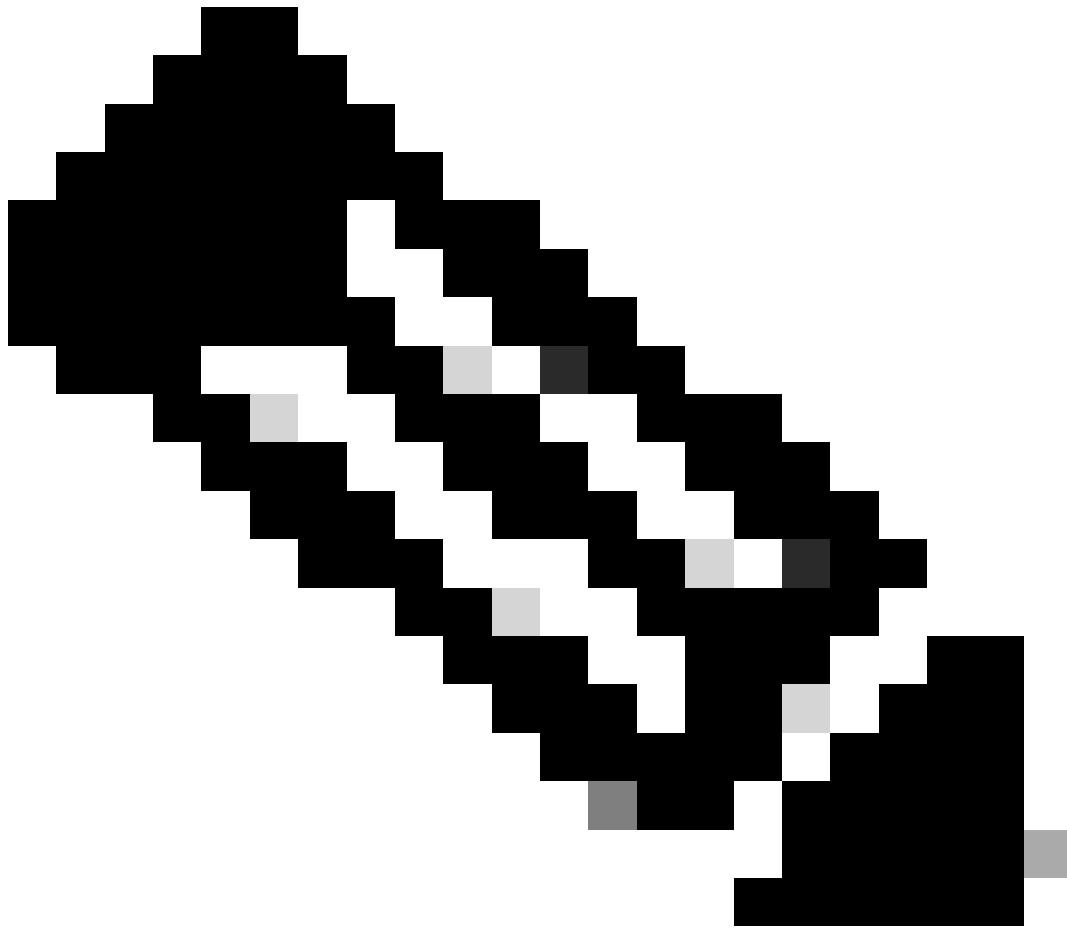
1

2

3

4

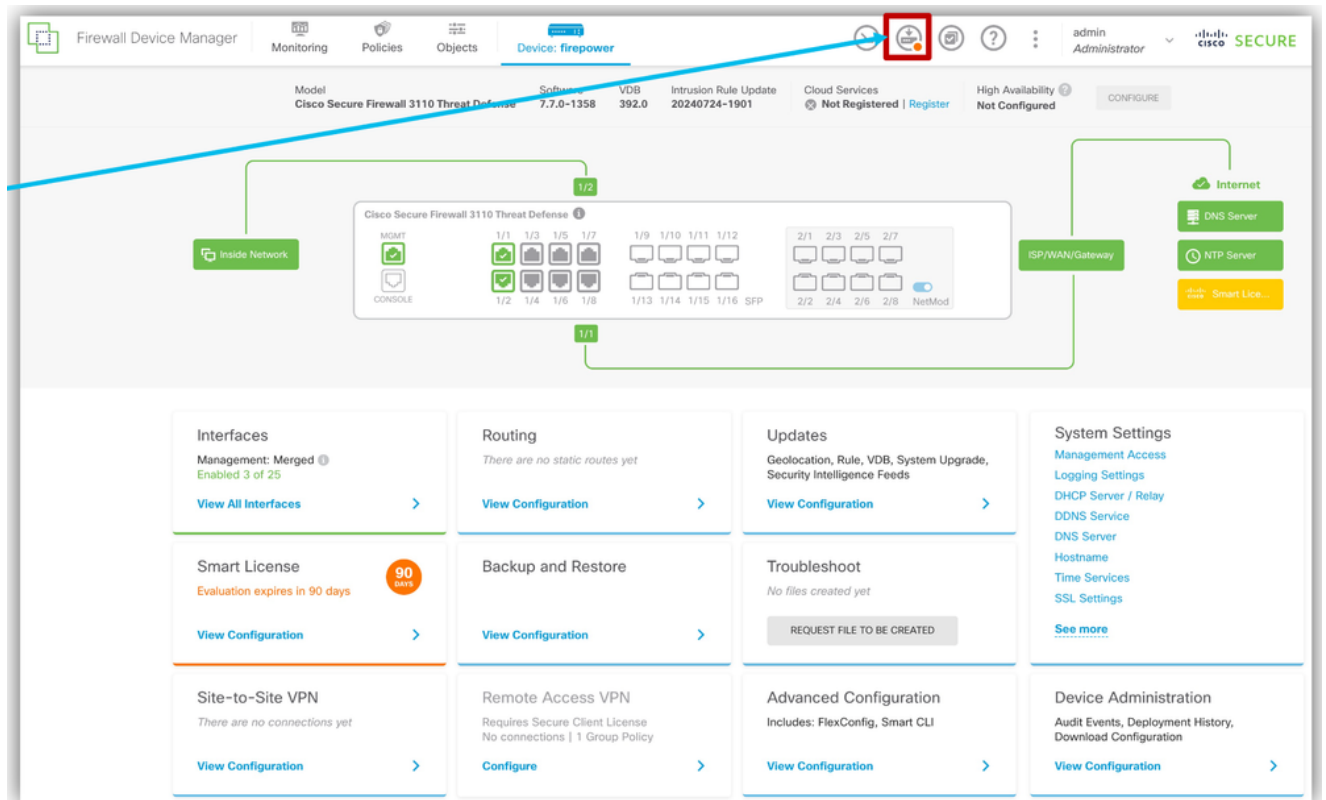
セキュリティゾーンの設定



注：インターフェイスの場合、インラインペアにインターフェイスが追加されると、モードは自動的にインラインに変更されます。

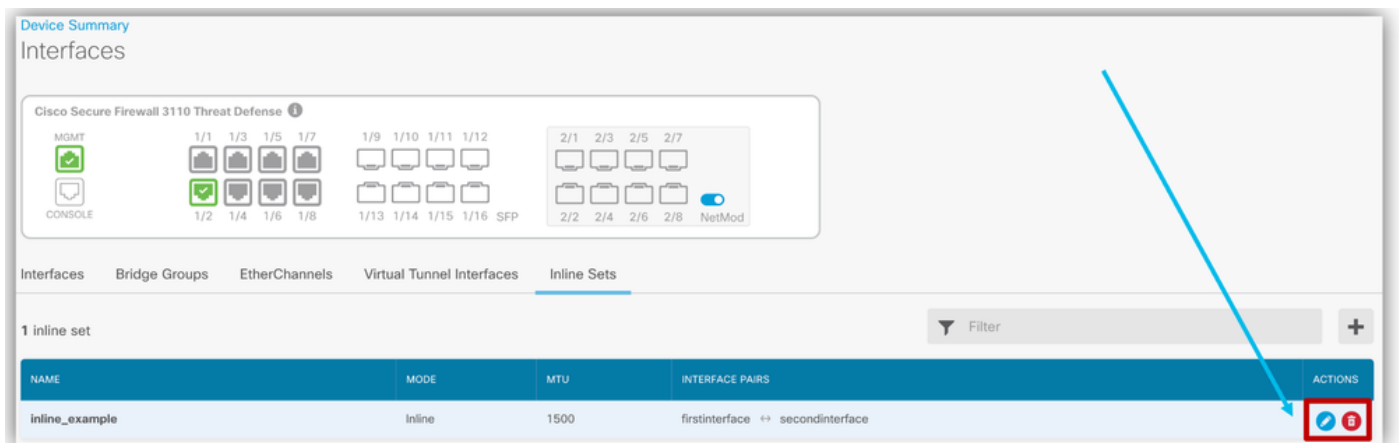
ステップ4：導入

- Deploymentタブに移動し、deployを選択します。



変更の展開

- インラインセットの編集および削除
 - Device > Interfaces > Inline setsタブに移動します。
 - [編集]ボタンと[削除]ボタンは、インラインセットに対して使用できます。



インラインセットの編集および削除

FDMデバイスREST API

REST APIエンドポイント

- GET : /devices/default/inlinesets
既存のすべてのインラインセットのリストを取得します。

- GET :/devices/default/inlinesets/{objID}
特定のインラインセットオブジェクトをIDで取得します。
- POST : /devices/default/inlinesets
新しいインラインセットを作成します。
- PUT : /devices/default/inlinesets/{objID}
既存のインラインセットオブジェクトをそのIDで更新します。
- DELETE :/devices/default/inlinesets/{objID}
既存のインラインセットオブジェクトをそのIDで削除します。
- GET :/operational/interfaceinfo/{objID}
すべてのInterfaceInfoentityのリストを取得します。
- ハードウェアバイパスをサポートするために、InterfaceInfo APIに新しいフィールドが追加されました。

インターフェイス情報REST APIモデル

- 新しいフィールドbypassInterfacePeerIdidが追加され、ハードウェアバイパスの統合を支援します。
- このフィールドは、現在のインターフェイスのハードウェアバイパスインターフェイスペアのIDを表します。
- 値 :
 - 特殊 : インターフェイスはバイパスをサポートしていません。
 - ID : インターフェイスはバイパスをサポートします。

```
{ "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"  
  }  
}
```

インターフェイス情報REST API

インターフェイス情報REST APIの例

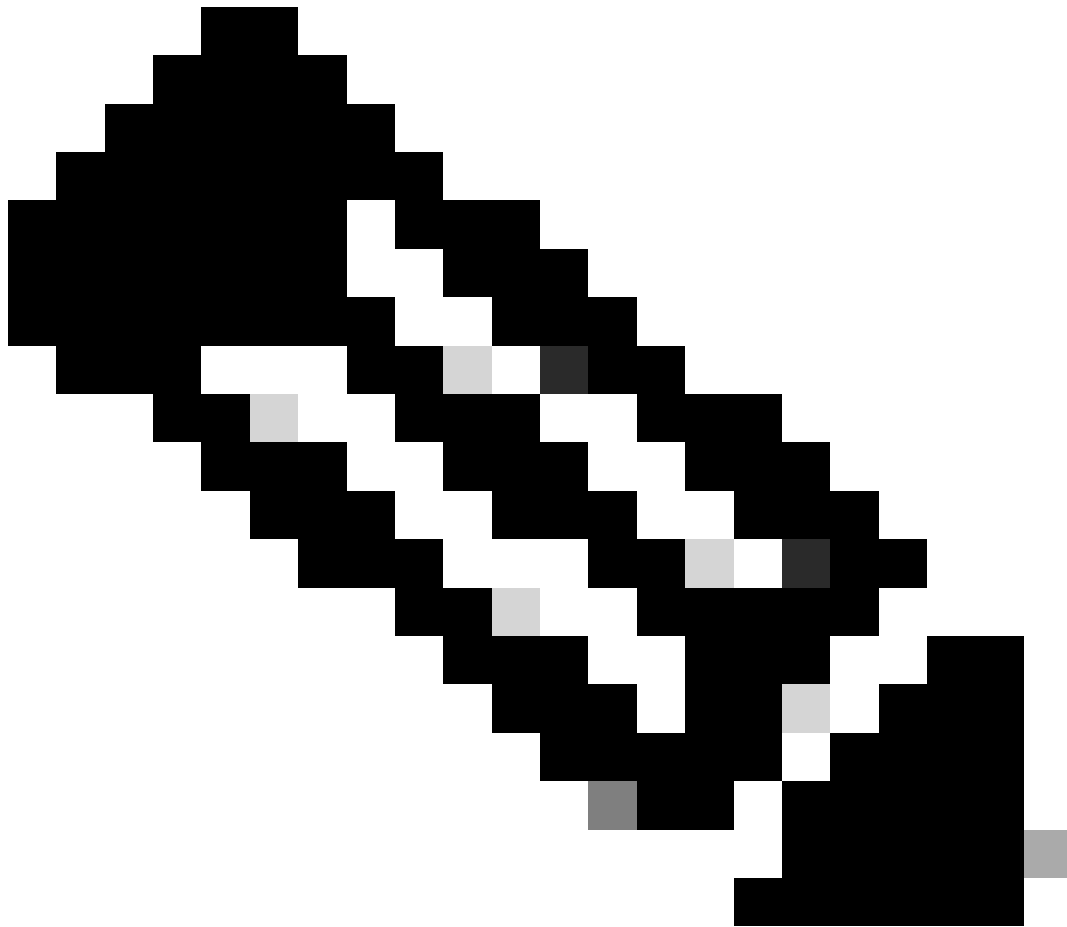
- インターフェイス情報REST APIの例。
 - ハードウェアバイパスをサポートしないインターフェイス(Ethernet 1/4)。
 - ハードウェアバイパスをサポートするインターフェイスペア (Ethernet2/1および Ethernet 2/2) 。

```

{ "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"
}
}

```

インターフェイス情報REST APIの例



注：これはサイズの関係で、フルコールからのスニペットです。

インラインセットREST APIモデル

- インラインセットモデルは次の要素で構成されます。
 - Type
 - [名前(Name)]
 - タップモード
 - MTU
 - リンク ステートの伝達
 - フェールオープンSnortビジー
 - バイパス値：DISABLED、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

- 基本的なインラインセットの例：

- 1つのインラインペア
- スタンバイの回避

```
{
  "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. インラインセットを作成します (ペイロードの例については、APIエクスプローラを参照してください) 。

POST/デバイス/デフォルト/インラインセット

3. セキュリティゾーンを作成します (ペイロードの例についてはAPI Explorerを参照してください) (オプション) 。

POST/オブジェクト/セキュリティゾーン

4. デバイスに展開します (ペイロードの例については、APIエクスプローラを参照してください) 。

導入後/運用/導入

ハードウェアバイパスを使用したインラインセットの設定と導入

1. インターフェイスIDとハードウェアバイパスインターフェイスペアに関する情報を取得します (ペイロードの例については、API Explorerを参照してください) 。

GET/operational/interfaceinfo/{objId}

2. インラインセットを作成します (ペイロードの例については、APIエクスプローラを参照してください) 。

POST/デバイス/デフォルト/インラインセット

3. セキュリティゾーンを作成します (ペイロードの例についてはAPI Explorerを参照してください) (オプション) 。

POST/オブジェクト/セキュリティゾーン

4. デバイスに展開します (ペイロードの例については、APIエクスプローラを参照してください) 。

導入後/運用/導入

インラインセットの編集

1. インターフェイスIDを取得します (ペイロードの例については、APIエクスプローラを参照してください) 。

GET/devices/default/interfaces (デバイス/デフォルト/インターフェイス)

2. インラインセットの取得

GET/devices/default/inlinesets (GET/デバイス/デフォルト/インラインセット)

3. インラインセットを編集します (ペイロードの例については、APIエクスプローラを参照してください) 。

PUT/devices/default/inlinesets/{objId}

4. デバイスにデプロイします (ペイロードの例については、APIエクスプローラを参照してください) 。

導入後/運用/導入

確認

<#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

トラブルシュート

コマンド

- show running-config inline-set (インラインセットの実行)
- show inline-set
- show interface
- システムサポートトレース

インラインセット – 作成時の検証

- エラーは、各フィールドのGUIに表示されます。
 - 名前を入力してください。
 - MTUサイズは1500以上である必要があります。
 - ペアの両方のインターフェイスを選択する必要があります。

MTUサイズ

ハードウェアバイパス – 作成時の検証

- バイパスが有効な場合、各フィールドの新しいエラーがGUIに表示されます。
 - すべてのインターフェイスでバイパスがサポートされている必要があります。
 - エラーは、サポートされていないインターフェイスを示します。
 - すべてのペアは、事前に決められたインターフェイスペアを使用する必要があります。
 -

- 。 エラーメッセージは、使用可能なバイパスインターフェイスペアを示しています
- 。

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)

interface3 (Ethernet1/3)

interface4 (Ethernet1/4)

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

interface3 (Ethernet1/3)

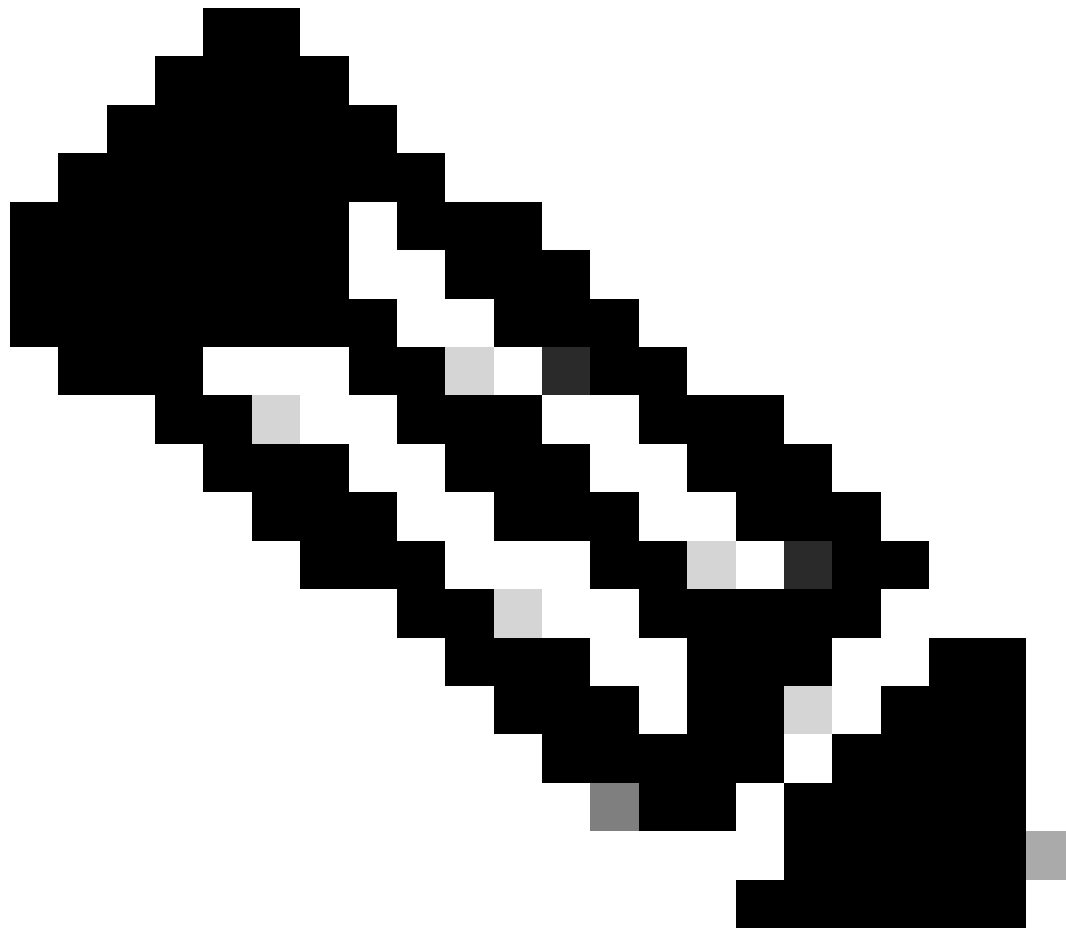
interface4 (Ethernet1/4)

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

[Add another pair](#)

CANCEL

OK



注：最初のペア(Ethernet2/1-Ethernet2/2)は有効です。

REST API応答でエラーが表示される

- エラーはREST API応答に表示されます。
 - この場合、MTU値は無効です。

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の検証

このリリースの実装の制限

- インラインセット：物理インターフェイスおよびEtherChannelでのみ動作します。
- ハードウェアバイパス付きインラインセット：物理インターフェイスでのみ動作し、ネットワークモジュールが必要です。

インラインインターフェイスでサポートされていないファイアウォール機能

- DHCP サーバ
- DHCP リレー
- DHCP Client
- TCP 代行受信
- ルーティング
- NAT
- VPN
- アプリケーション
- 検査
- QoS
- NetFlow

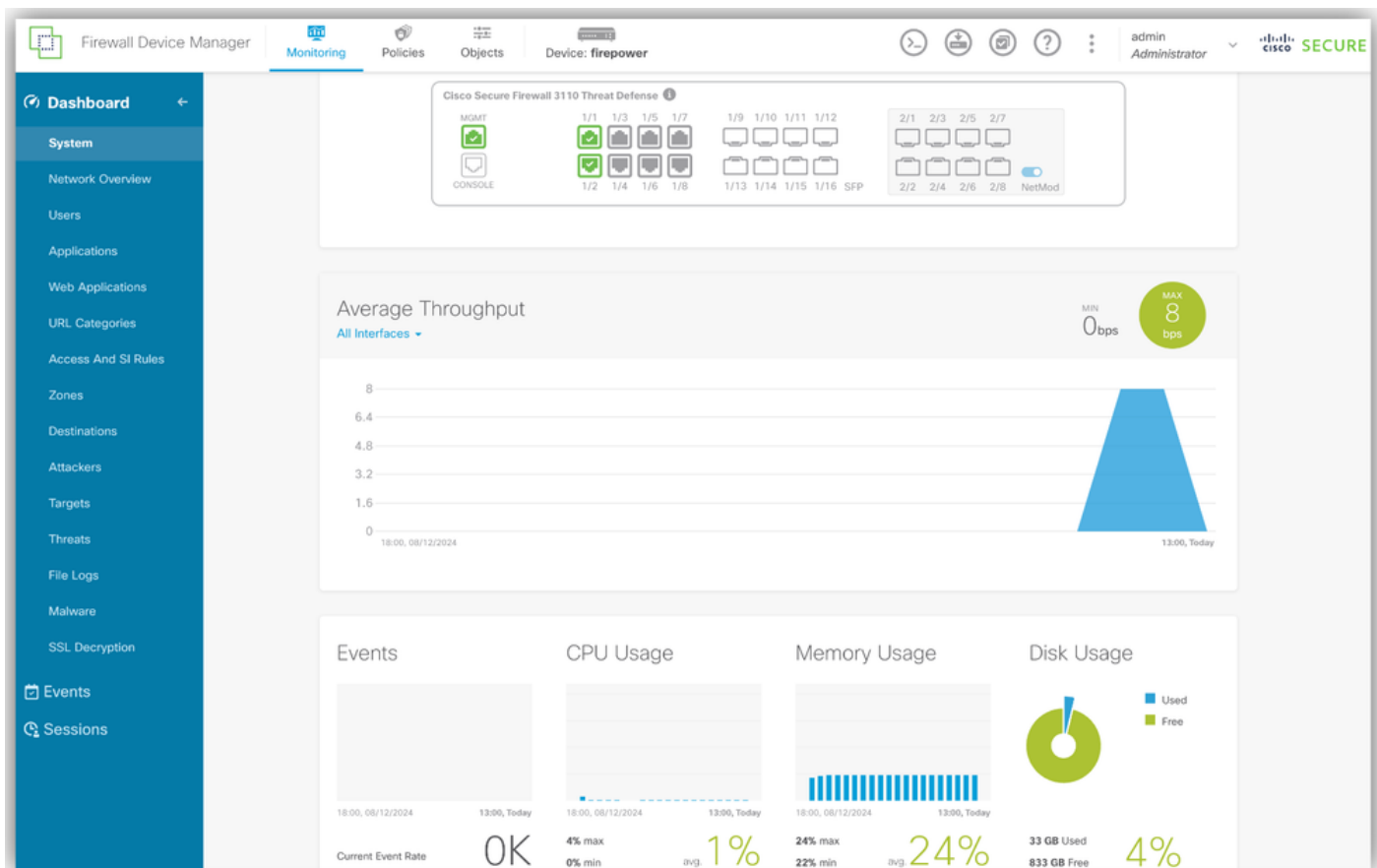
CLIからのログの確認

- ログिंग.

- ログは/ngfw/var/log/cisco/ngfw-onbox.logにあります。
- インラインセットの検索
- ログで見つかったエラーの例：
 - 2つのインターフェイスはバイパスをサポートしていません。
 - 2つのインターフェイスは有効なバイパスペアではありません。

```
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
```

- GUIからのトラフィックを確認します。
 - イベントはGUIに表示されます。
 - ここでは、トラフィックフローの正確さを監視できます。
 - Monitoring > Systemの順に移動します。



FDM監視

- CLIからトラフィックの正確性を確認します。

<#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: FDMのインライン・セットでHAはサポートされますか。

A : バイパスなしのインラインセットがサポートされています。

バイパス付きのインラインセットはサポートされていません。

Q : インラインセットペアでスパンニングツリーBPDUがブロックされていますか。

A : いいえ。ブロックされていません。

Q: FTWカードは3100でサポートされていますか。

A：はい。3100シリーズが7.1/9.17で導入されて以来、FTWのnetmodsはサポートされています。ハードウェアバイパスは7.7.0以降で使用できます。

Q: 3100 FTWカードでは、FMCと同様にDisabled、Standby、Bypass-Forceの各バイパスモードがサポートされていますか。

A：ハードウェアバイパスは、7.7.0以降、FTWカードを搭載した3100台のデバイスで使用できます。

Q：ポートチャネルを経由するトラフィックが非対称の場合でも、ポートチャネルを使用するインラインセットはサポートされていますか。

A:PortChannelで設定されている速度の検証は行われなため、FTDでサポートされている限り、サポートされている必要があります。

Q: Snortのインスペクションが失敗した場合、フェールオープンはサポートされますか。

A：この設定のドキュメントについては、『[Firepower Management Center Configuration Guide](#)』を参照してください。

関連情報

- [インラインペアモードでのFTDインターフェイスの設定](#)
- [Firepower Management Center設定ガイド、バージョン6.3](#)
- [Cisco Secure Firewall 3100シリーズハードウェアインストールガイド](#)
- [Cisco Secure Firewall 3100シリーズデータシート](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。