インラインペアモードでのFDMインタフェースの構成

内容

はじめに

このドキュメントでは、Cisco Secure Firewall 7.4.1で追加されたFDMのインラインセット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を推奨しています。

- FDMの概念および構成
- FDMで管理される1000、2100、3100シリーズ・プラットフォームのFTDに適用されます

使用するコンポーネント

このドキュメントの情報は、FDM 7.4.2に基づいています。

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

インラインセットは、IPS専用インターフェイスを提供します。IPSのみのインターフェイスは、これらのインターフェイスを保護する別のファイアウォールがあり、ファイアウォール機能のオーバーヘッドが不要な場合に実装できます。

インラインセットは、ワイヤ上のバンプのように動作し、2つのインターフェイスを既存のネットワークにスロットにバインドします。この機能により、隣接するネットワークデバイスを設定しなくても、任意のネットワーク環境にデバイスを設置できます。インラインインターフェイスはすべてのトラフィックを無条件に受信しますが、これらのインターフェイスで受信したすべてのトラフィックは、明示的にドロップされない限り、インラインセットから再送信されます。

ガイドラインと制限事項

- インラインセットを設定できるのは、Firepower 1000シリーズ、Firepower 2100、セキュアファイアウォール3100の各デバイスモデルだけです。
- インラインセットで使用できるインターフェイスタイプ：物理、EtherChannel。
- インラインセットに管理インターフェイスを含めることはできません。
- インラインセットで使用されるインターフェイスの属性（名前、モード、インターフェイスID、MTU、IPアドレス）は変更できません。
- タップモードを有効にすると、「Snort Fail Open」は無効になります。
- インラインセットを使用している場合、双方向フォワーディング検出(BFD)エコーパケットはデバイスを通過できません。BFDを実行しているデバイスのいずれかの側に2つのネイバーがある場合は、デバイスはBFDエコーパケットをドロップします。これは、それらのネイバーが同じ送信元IPアドレスと宛先IPアドレスを持ち、LAND攻撃の一部に見えるためです。
- インラインセットおよびパッシブインターフェイスの場合、デバイスはパケットで最大2つの802.1Qヘッダーをサポートします（Q-in-Qサポートとも呼ばれます）。

  注：ファイアウォールタイプのインターフェイスはQ-in-Qをサポートしておらず、802.1Qヘッダーを1つだけサポートしています。

- インラインセット内のインターフェイスは、ルーティング、NAT、DHCP（サーバ、クライアント、またはリレー）、VPN、TCPインターセプト、アプリケーション検査、またはNetflowをサポートしません。

はじめる前に

- 脅威対策のインラインペアインターフェイスに接続するSTP対応スイッチには、STP PortFastを設定することを推奨します。
- インラインセットのメンバにできる物理インターフェイスまたはEtherChannelインターフェイスを設定します。設定できるのは、名前、デュプレックス、速度、およびルーテッドモ

ード（パッシブは選択しない）の値だけです。 アドレッシングのタイプ（手動IPアドレス、DHCP、またはPoE）は設定しないでください。

インラインモードの詳細

- この機能を使用すると、インラインセットを使用できます。これにより、IP割り当てを行わずにトラフィックを検査できます。

- 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。

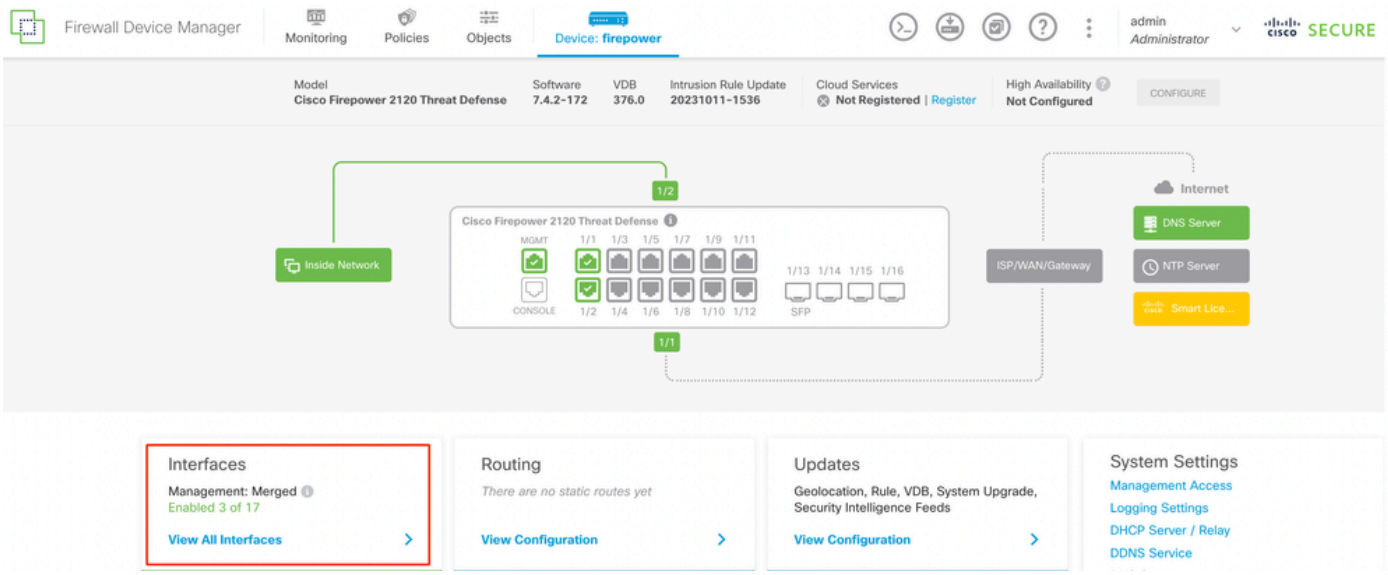
インラインセットネットワークダイアグラム

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Router1からRouter2へ流れます。

ネットワーク図

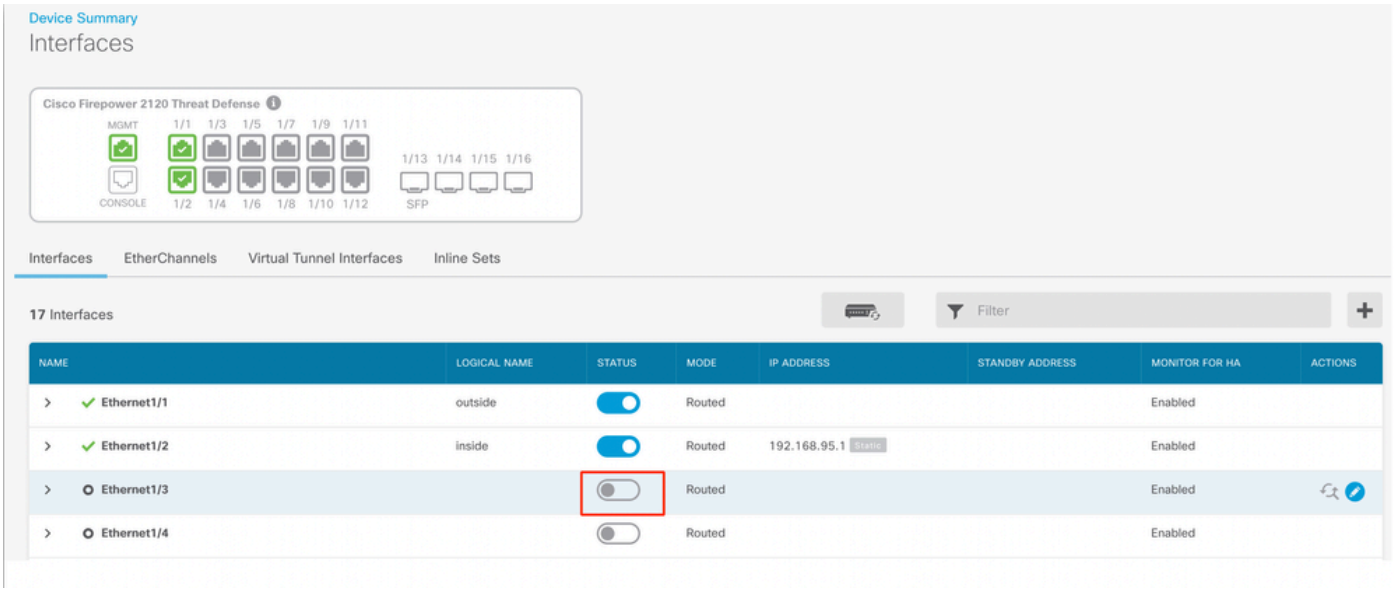
インラインセットの設定

- FDMダッシュボードから、Interfaces cardに移動します。

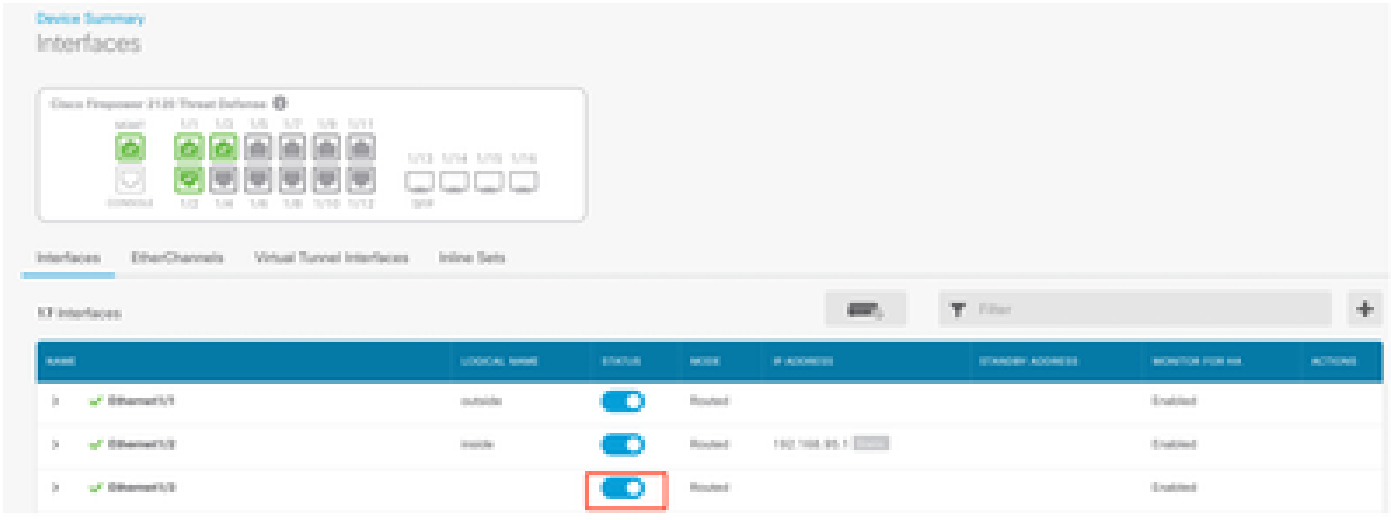


Interfacesタブ

- インターフェイスを有効にするには、インターフェイスのStatusアイコンをクリックする。

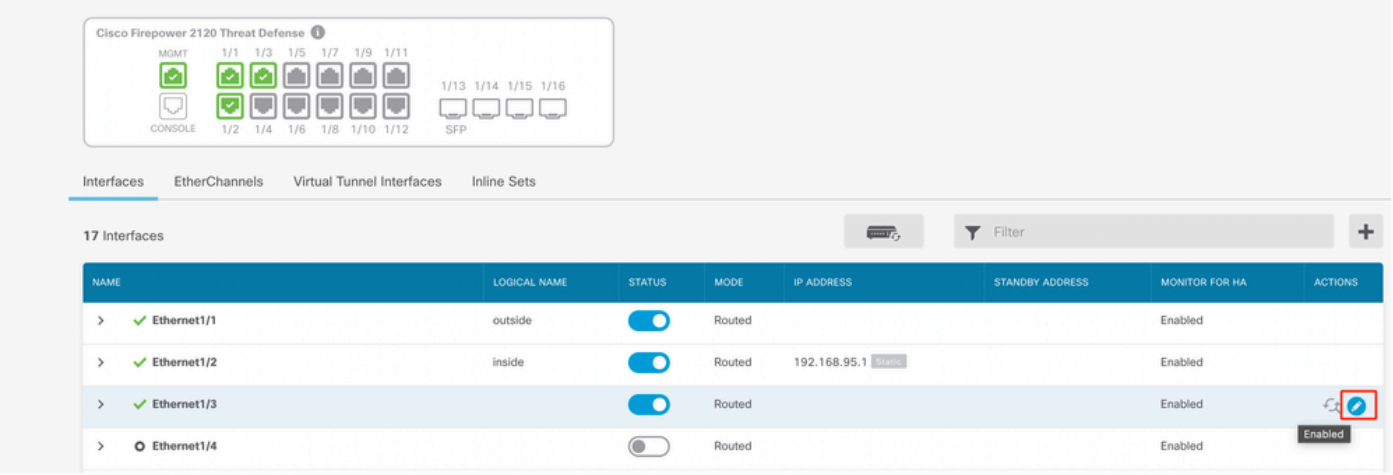


ステータスアイコン



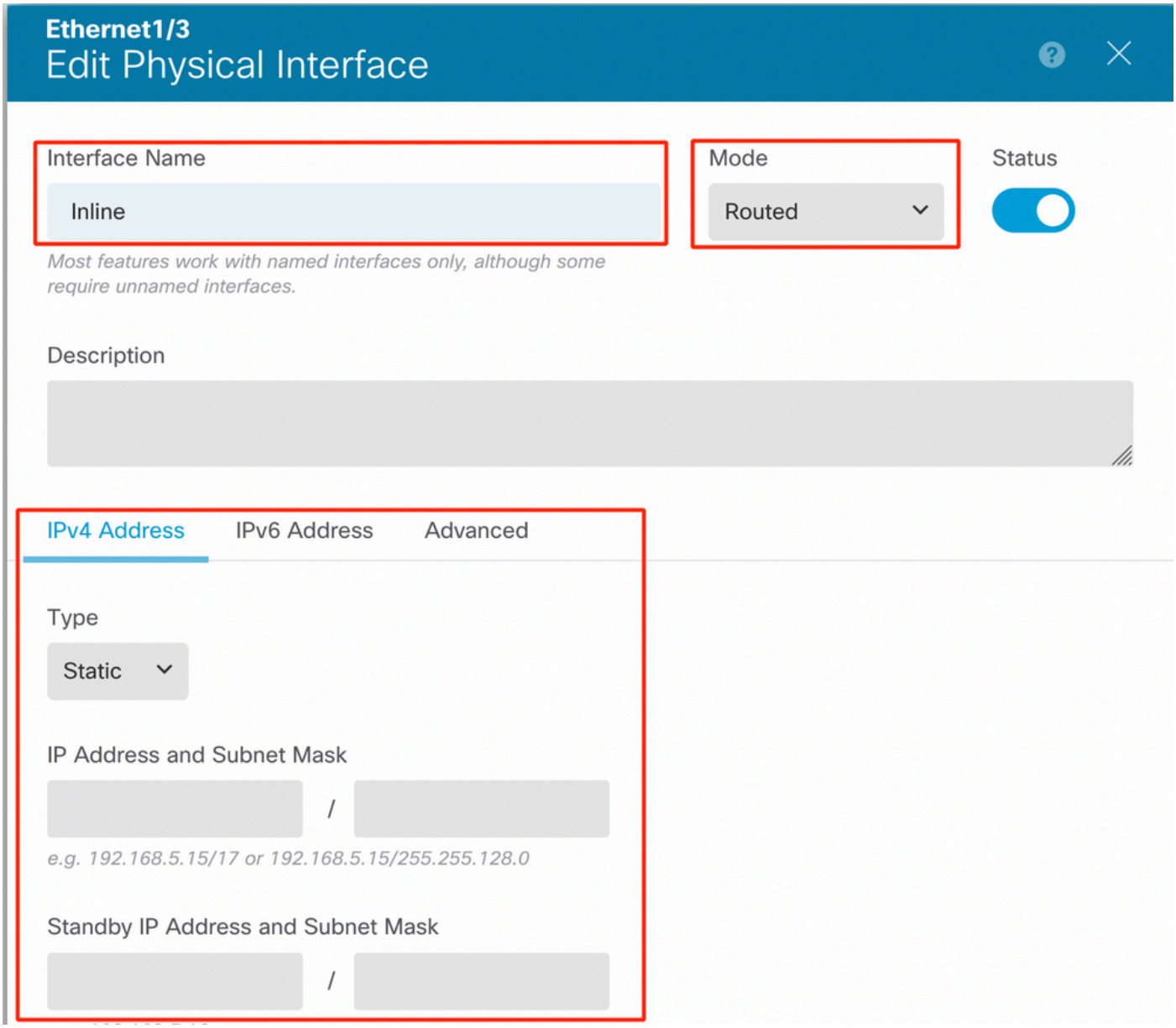
インターフェイスの有効化

- インターフェイスを編集するには、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。



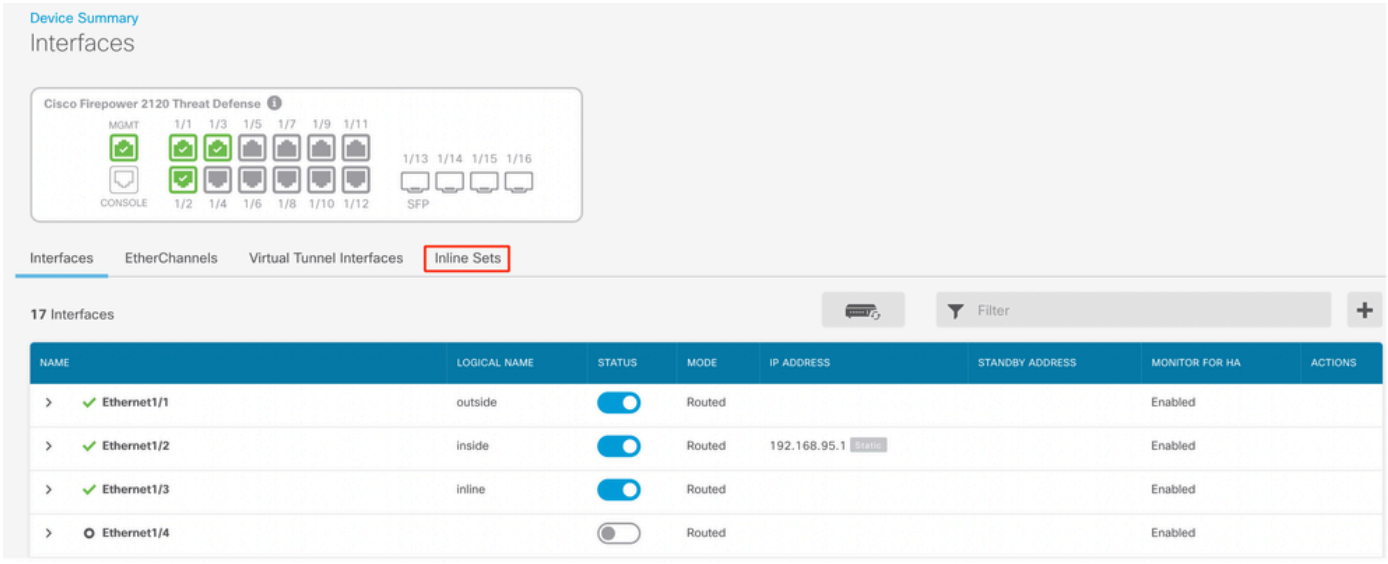
インターフェイスの編集

- インターフェイス名を入力し、モードとしてRoutedを選択します。IPアドレスは設定しないでください。



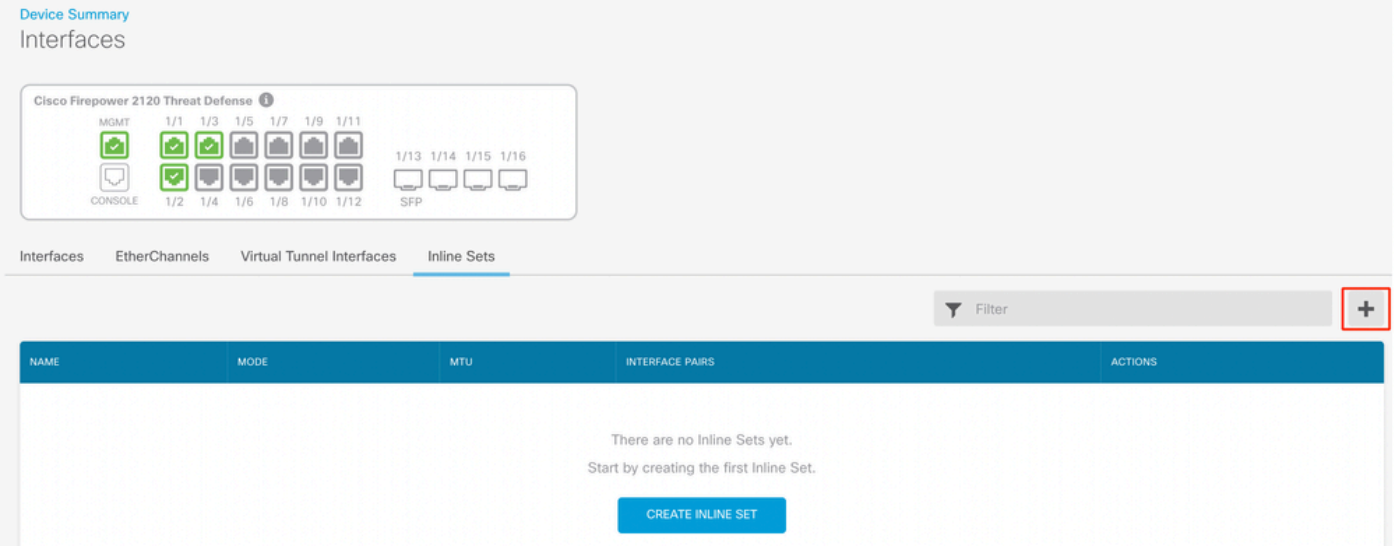
インターフェイスの編集

- インラインセットを作成するには、Inline Setsタブに移動します。



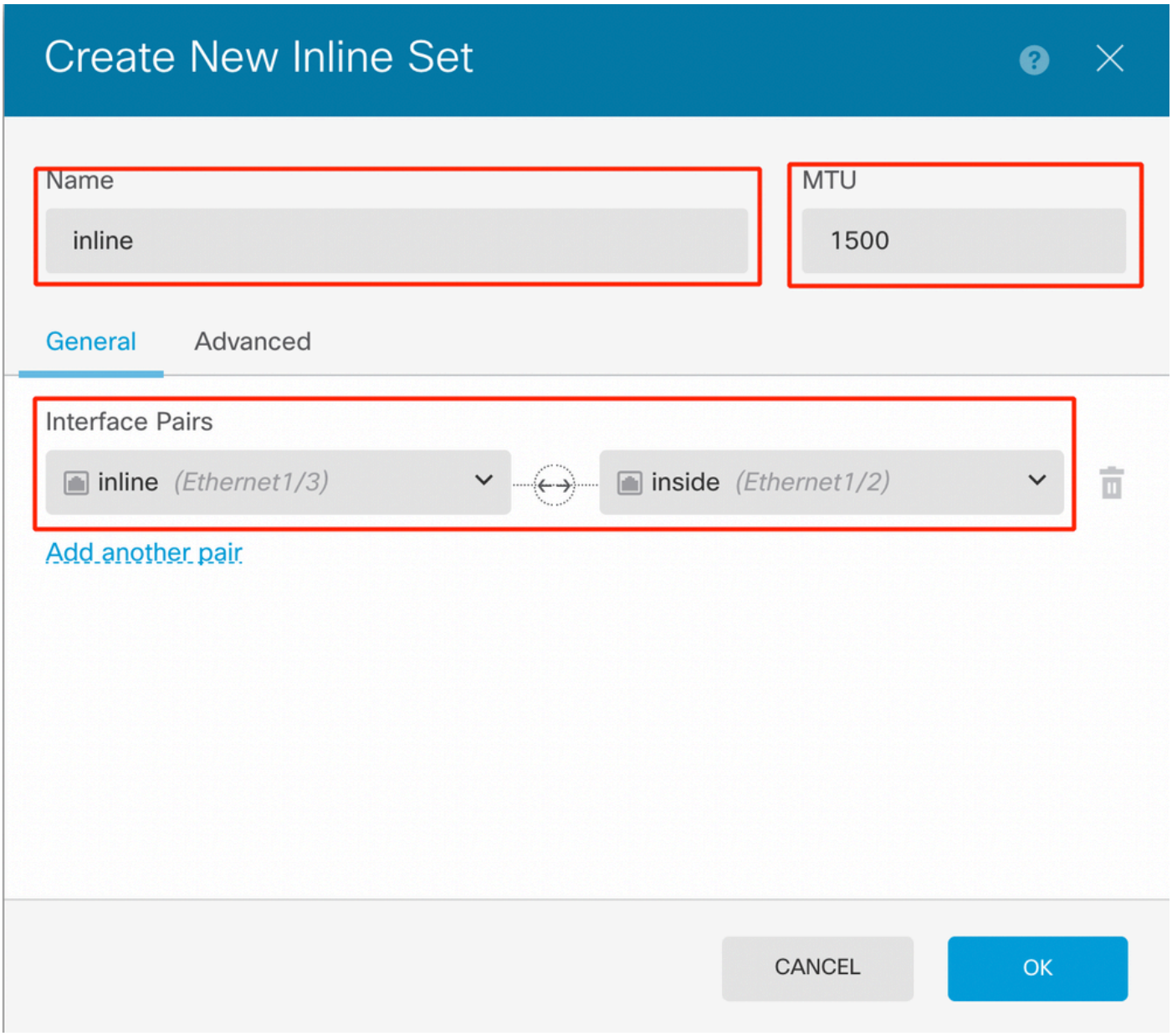
インラインセットの作成

インラインセットを追加するには、追加(+アイコン)をクリックします。



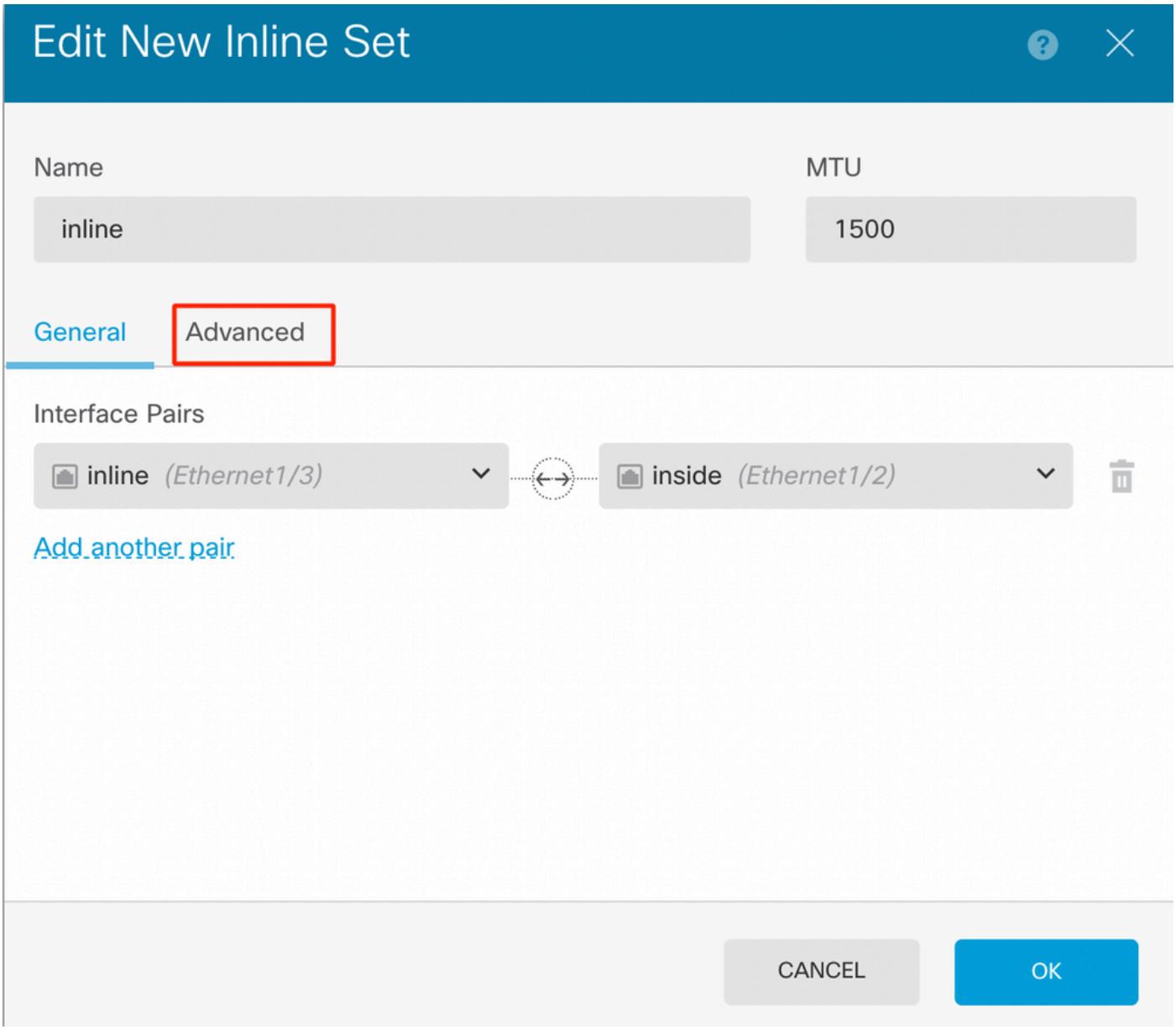
インラインセットの追加

- インラインセットの名前を設定します。
- 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MTUです。
- Interface Pairsセクションで、interfacesを選択します。さらにペアが必要な場合は、「別のペアを追加」リンクをクリックします。



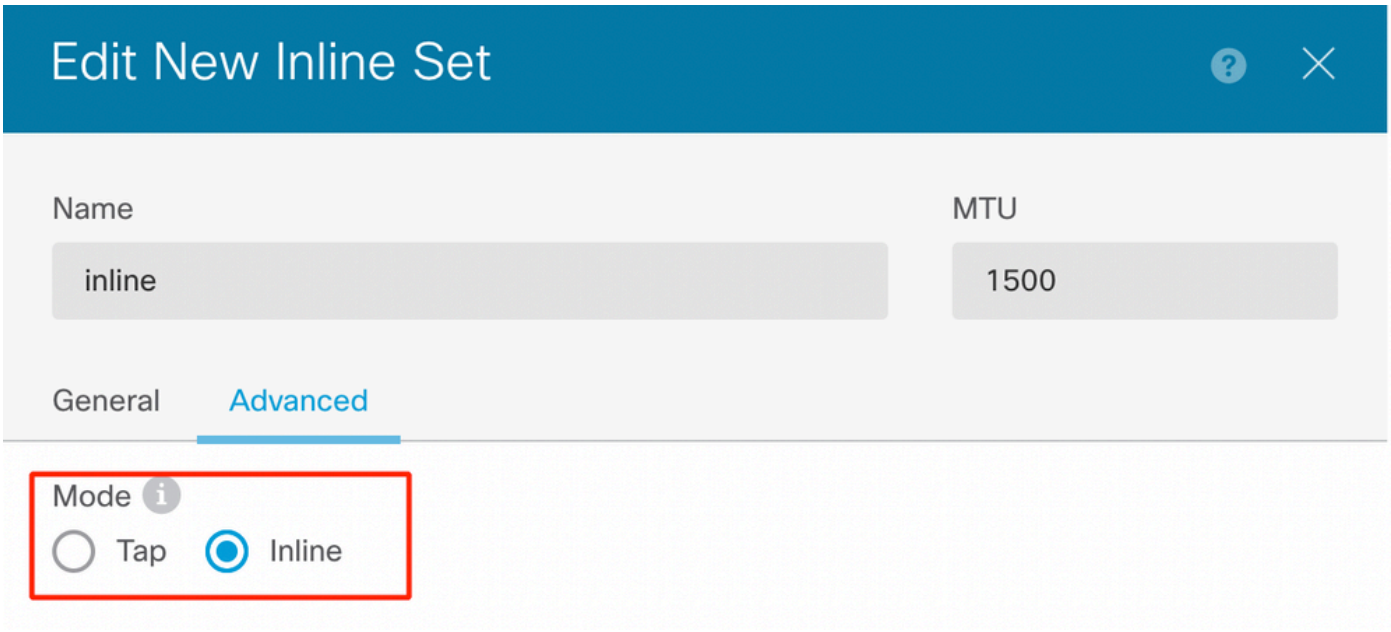
インターフェイスペア

- インラインセットの詳細設定を設定するには、Advancedタブに移動します。



高度な設定

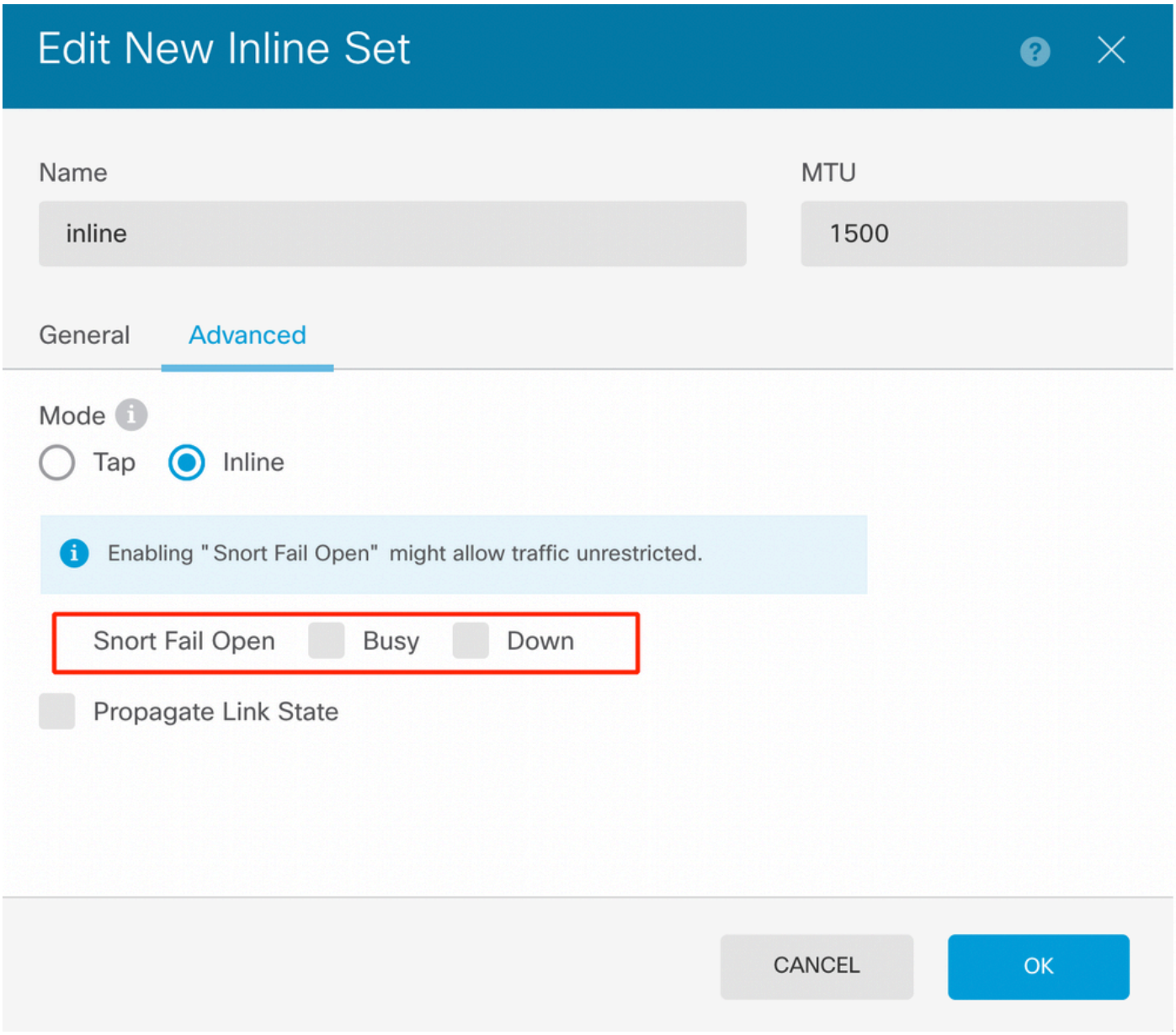
- ModeにInlineを選択します。タップモードが有効な場合、Snort Fail Openは無効になります。



インラインのモード

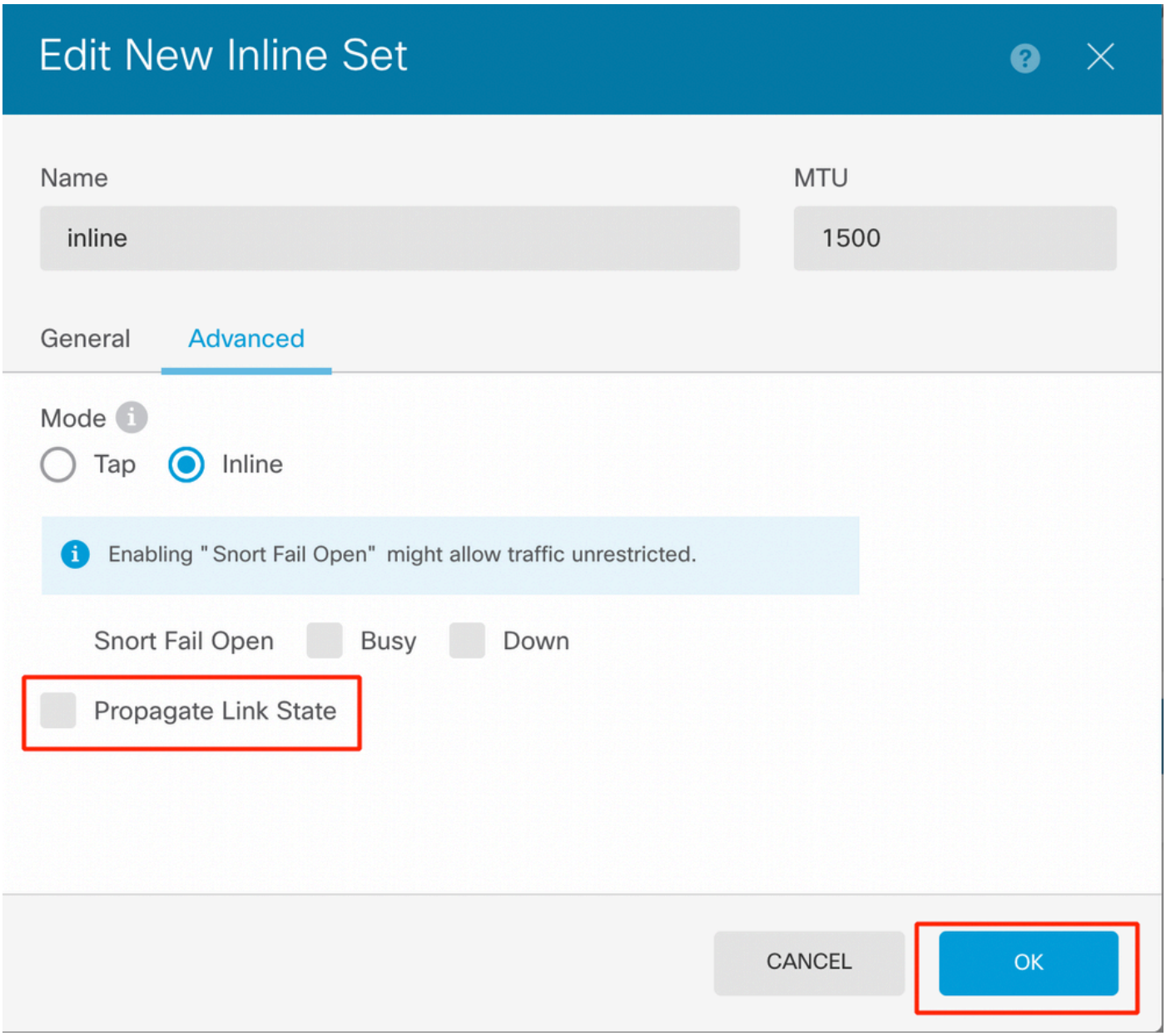
- Snort Fail Openでは、Snortプロセスがビジーまたはダウンの場合、新規および既存のトラフィックをインスペクションなしで通過させる（有効）か、ドロップする（無効）ことができます。

- 必要なSnort Fail Open設定を選択します。
- Busy オプションとDown オプションは、どちらも設定しないか、どちらか一方または両方に設定できます。



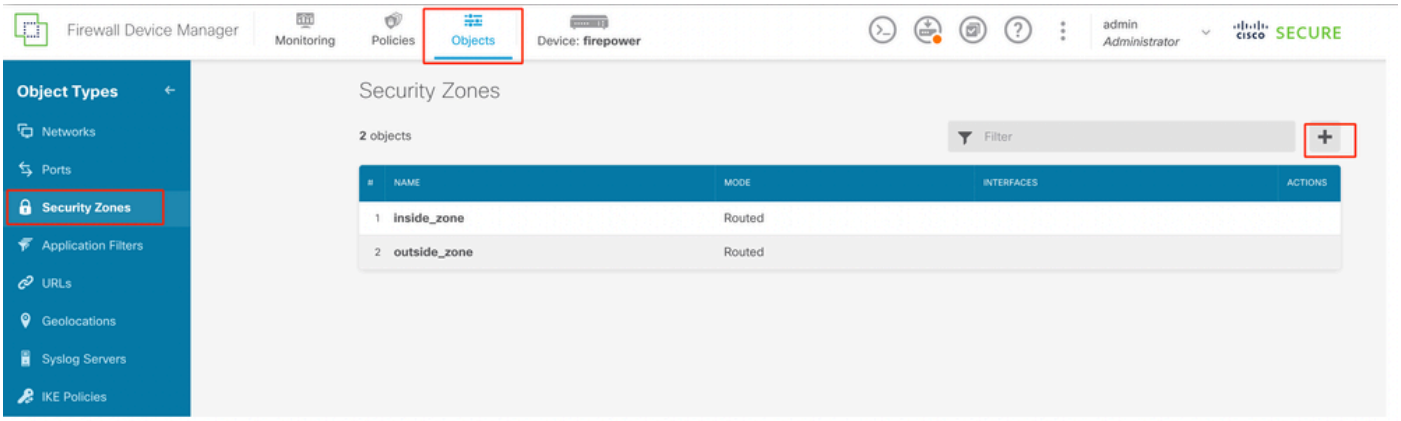
Snortのフェールオープン

- Propagate Link Stateオプションは、インラインペアの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。
- すべての設定が完了したら、OKをクリックして設定を保存します。



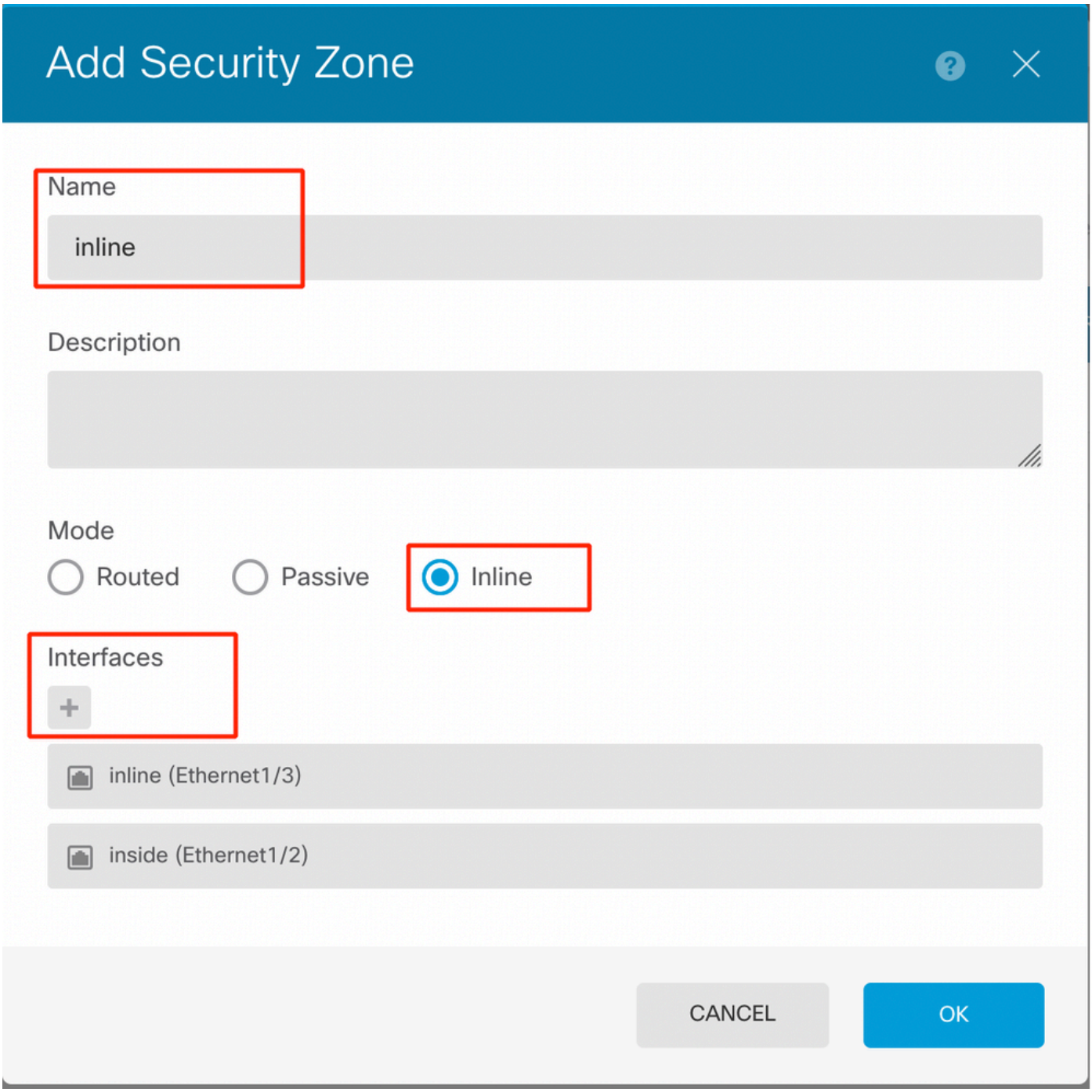
リンク ステートの伝達

- このインラインセットをセキュリティゾーンに追加するには、Objects > Security Zonesの順に選択します。
- Addをクリックして、新しいセキュリティゾーンを作成します。



セキュリティゾーンの追加

- 名前を設定し、モードにインラインを選択して、インラインセットのインターフェイスを追加します。OKをクリックして保存します。

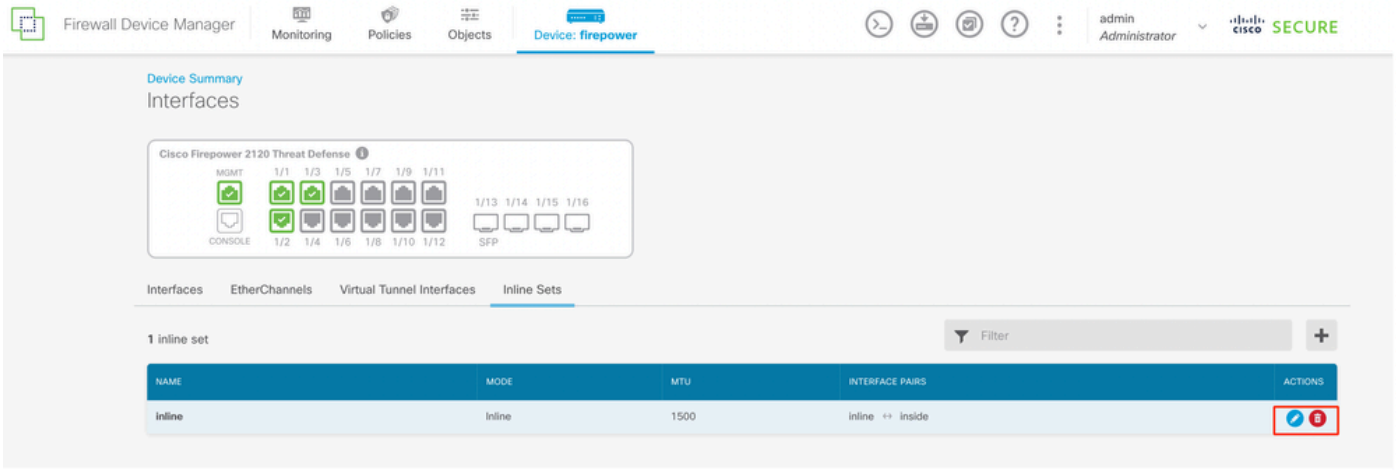


インターフェイスの追加

- Deploymentタブに移動し、変更をDeployします。

インラインセットの変更または削除

インラインセットに対して編集アクションと削除アクションを使用できます。



インラインセットのアクション

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。