インラインセットとパッシブインターフェイス

IPS 専用のパッシブインターフェイス、パッシブ ERSPAN インターフェイス、インラインセットを設定できます。

IPS インターフェイスについて

IPS インターフェイスには、パッシブ インターフェイス、パッシブ ERSPAN インターフェイス、インライン セットが含まれます。IPS 専用モードのインターフェイスは、多数のファイアウォールのチェックをバイパスし、IPS セキュリティポリシー（Snort）のみをサポートします。別のファイアウォールがこれらのインターフェイスを保護していて、ファイアウォール機能のオーバーヘッドを避けたい場合、IPS 専用のインターフェイスを実装することがあります。

IPS 専用モードのインターフェイスは、多数のファイアウォールのチェックをバイパスし、IPS セキュリティポリシー（Snort）のみをサポートします。別のファイアウォールがこれらのインターフェイスを保護していて、ファイアウォール機能のオーバーヘッドを避けたい場合、IPS 専用のインターフェイスを実装することがあります。

（注） ファイアウォールモードは通常のファイアウォールインターフェイスにのみ影響を与えます。インライン セットやパッシブ インターフェイスなどの IPS 専用インターフェイスには影響を与えません。IPS 専用インターフェイスは両方のファイアウォール モードで使用可能です。

インライン セット

インラインセットはワイヤ上のバンプのように動作し、1つ以上のインターフェイスペアを一緒にバインドし、既存のネットワークに組み込みます。この機能によって、隣接するネットワークデバイスの設定がなくても、任意のネットワーク環境にFirewall Threat Defenseをインストールすることができます。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され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、インラインペアの他のインターフェイスから、外部に再送信されます。インラインセットに複数のインラインペアがある場合、トラフィックはペアのインターフェイス間でのみ通過できます。異なるペアのインターフェイス間を渡すことはできません。

タップ モードでは、Firewall Threat Defense はインラインで展開されますが、ネットワーク トラフィック フローは妨げられません。代わりに、Firewall Threat Defenseは各パケットのコピーを作成して、パケットを分析できるようにします。それらのタイプのルールでは、ルールがトリガーされると侵入イベントが生成され、侵入イベントのテーブルビューにはトリガーの原因となったパケットがインライン展開でドロップされたことが示されることに注意してください。インライン展開された FTD でタップモードを使用することには、利点があります。たとえば、Firewall Threat Defense がインラインであるかのように Firewall Threat Defense とネットワーク間の配線をセットアップし、Firewall Threat Defense で生成される侵入イベントのタイプを分析することができます。その結果に基づいて、効率性に影響を与えることなく最適なネットワーク保護を提供するように、侵入ポリシーを変更してドロップ ルールを追加できます。Firewall Threat Defenseをインラインで展開する準備ができたら、タップ モードを無効にして、Firewall Threat Defense とネットワーク間の配線を再びセットアップせずに、不審なトラフィックのドロップを開始することができます。

（注） タップモードは、トラフィックによってはFirewall Threat Defenseのパフォーマンスに大きく影響します。

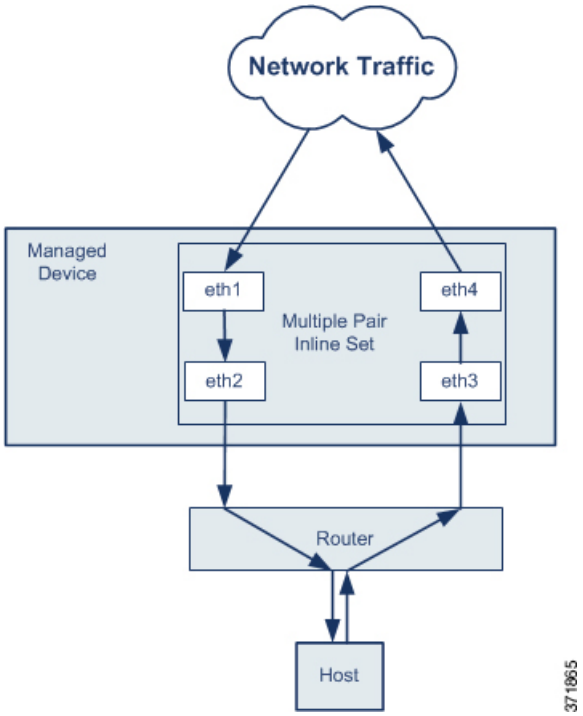
（注） 「透過インライン セット」としてインライン セットに馴染みがある人もいますが、インラインインターフェイスのタイプはトランスペアレントファイアウォールモードやファイアウォール タイプのインターフェイスとは無関係です。

複数のインライン ペアと非同期ルーティング

トラフィックがインバウンドであるかアウトバウンドであるかに応じて、異なるインラインペアを介してネットワーク上のホストと外部ホスト間のトラフィックをルーティングするように、インターフェイスを設定できます。これは非同期ルーティング設定です。非同期ルーティングを展開しても、インライン セットに 1 つのインライン ペアしか含めないと、デバイスがトラフィックの半分しか認識しないため、ネットワーク トラフィックが適切に分析されない可能性があります。

同じインライン セットに複数のインライン ペアを追加すると、システムが着信トラフィックと発信トラフィックを同じトラフィック フローの一部として識別させることができます。パッシブ インターフェイスでのみ、同じセキュリティ ゾーンにインターフェイス ペアを含めることによっても実現できます。

図 *1*: 非同期ルーティング



（注） 複数のインライン ペアを単一のインライン セットに割り当てたときに、重複トラフィックの問題が発生した場合は、個別のインライン セットにインライン ペアを再割り当てするか、セキュリティ ゾーンを変更する必要があります。

パケットのフラグメントが異なるインターフェイス ペアで受信された場合、それらは再構成されず、ドロップされます。パケットのすべてのフラグメントが同じインターフェイス ペアで送受信されるようにしてください。

パッシブ インターフェイス

パッシブ インターフェイスは、スイッチ SPAN またはミラー ポートを使用してネットワーク中のトラフィック フローをモニターします。SPAN またはミラー ポートでは、スイッチ上の他のポートからトラフィックをコピーできます。この機能により、ネットワーク トラフィックのフローに含まれなくても、ネットワークでのシステムの可視性が備わります。パッシブ展開で Firewall Threat Defense を構成した場合は、Firewall Threat Defense は特定のアクション（トラフィックのブロッキングやシェーピングなど）を実行することができません。パッシブインターフェイスはすべてのトラフィックを無条件で受信します。このインターフェイスで受信さ

れたトラフィックは再送されません。Encapsulated Remote Switched Port Analyzer（ERSPAN）インターフェイスは、複数のスイッチに分散された送信元ポートからのトラフィックをモニタし、GREを使用してトラフィックをカプセル化します。ERSPANインターフェイスは、Firewall Threat Defenseがルーテッド ファイアウォール モードになっている場合にのみ許可されます。

（注） 無差別モードの制限により、SR-IOV ドライバを使用する一部の Intel ネットワークアダプタ（Intel X710 や 82599 など）では、SR-IOV インターフェイスを NGFWv のパッシブインターフェイスとして使用することはできません。このような場合は、この機能をサポートするネットワークアダプタを使用してください。Intel ネットワークアダプタの詳細については、『Intel Ethernet Products』[英語] を参照してください。

インライン セットのハードウェア バイパスについて

サポートされているモデルの特定のインターフェイスモジュールでは（インラインセットの要件と前提条件 （5 ページ）を参照）、ハードウェア バイパス 機能を有効にできます。ハードウェア バイパスにより、停電中のインライン インターフェイス ペア間でトラフィックが引き続きフローできるようにします。この機能は、ソフトウェアまたはハードウェア障害の発生時にネットワーク接続を維持するために使用できます。

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ことがあります。

- Firewall Threat Defense のクラッシュ
- Firewall Threat Defense の再起動
- セキュリティ モジュールの再起動
- シャーシのクラッシュ
- Chassis reboot
- 手動トリガー
- シャーシの停電
- セキュリティ モジュールの電力損失

（注） ハードウェアバイパスは、計画外の障害または予期しない障害のシナリオのためのものです。計画されたソフトウェアアップグレード中に自動的にトリガーされることはありません。ハードウェアバイパスは、Firewall Threat Defenseアプリケーションの再起動時に、計画されたアップグレードプロセスの最後にのみ関与します。

ハードウェア バイパスのスイッチオーバー

通常の運用からハードウェア バイパスに切り替えたとき、またはハードウェア バイパスから通常の運用に戻したときに、トラフィックが数秒間中断する可能性があります。中断時間の長さに影響を与える可能性があるいくつかの要因があります。たとえば、銅線ポートの自動ネゴシエーション、リンク エラーやデバウンスのタイミングをどのように処理するかなどのオプティカル リンク パートナーの動作、スパニング ツリー プロトコルのコンバージェンス、ダイナミック ルーティング プロトコルのコンバージェンスなどです。この間は、接続が落ちることがあります。

また、通常の操作に戻った後で接続のミッドストリームを分析するときに、アプリケーションの識別エラーが原因で接続が切断されることがあります。

Snort フェール オープンと ハードウェア バイパス

タップ モード以外のインライン セットでは、[Snort フェール オープン（Snort Fail Open）] オプションを使用して、トラフィックをドロップするか、Snort プロセスがビジーまたはダウンしている場合に検査なしでトラフィックの通過を許可します。Snort フェール オープンは、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上のみでなく、タップ モードのものを除くすべてのインライン セットでサポートされます。

ハードウェア バイパス機能を使用すると、停電時や特定の限定されたソフトウェア障害などのハードウェア障害時にトラフィックが流れます。Snort フェール オープンをトリガーするソフトウェアの障害は、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 Status

システムの電源が入っている場合、バイパス LED はハードウェア バイパスのステータスを表示します。LED の説明については、Firepower シャーシ ハードウェア インストレーションガイドを参照してください。

インラインセットの要件と前提条件

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者

ハードウェア バイパス サポート

Firewall Threat Defense は、以下のモデルの特定のネットワーク モジュールのインターフェイス ペアで ハードウェア バイパス をサポートします。

- Firepower 2130 および 2140

- Cisco Secure Firewall 3100
- Firepower 4100
- Firepower 9300

（注） ISA 3000 にはハードウェアバイパス用の個別の実装があります。これは、FlexConfig のみを使用して有効にできます（FlexConfig ポリシーを参照）。この章は、ISA 3000 ハードウェアバイパスの設定には使用しないでください。

（注） ハードウェア バイパス 機能を有効にしなくても、ハードウェア バイパス インターフェイスを標準インターフェイスとして使用できます。

これらのモデルでサポートされている ハードウェア バイパス ネットワーク モジュールは以下のとおりです。

- Firepower 2130 および 2140：
  - Firepower 6 ポート 1G SX FTW ネットワーク モジュール シングルワイド（FPR2K-NM-6X1SX-F）
  - Firepower 6 ポート 10G SR FTW ネットワーク モジュール シングルワイド（FPR2K-NM-6X10SR-F）
  - Firepower 6 ポート 10G LR FTW ネットワーク モジュール シングルワイド（FPR2K-NM-6X10LR-F）
- Secure Firewall 3100：
  - 6 ポート 1 G SFP Fail-to-Wire ネットワークモジュール、SX（マルチモード）（FPR3K-XNM-6X1SXF）
  - 6 ポート 10 G SFP Fail-to-Wire ネットワークモジュール、SR（マルチモード）（FPR3K-XNM-6X10SRF）
  - 6 ポート 10 G SFP Fail-to-Wire ネットワークモジュール、LR（シングルモード）（FPR3K-XNM-6X10LRF）
  - 6 ポート 25 G SFP Fail-to-Wire ネットワークモジュール、SR（マルチモード）（FPR3K-XNM-X25SRF）
  - 6 ポート 25 G Fail-to-Wire ネットワークモジュール、LR（シングルモード）（FPR3K-XNM-6X25LRF）
  - 8 ポート 1 G 銅ケーブル Fail-to-Wire ネットワークモジュール（銅ケーブル）（FPR3K-XNM-8X1GF）

- Firepower 4100：
  - Firepower 6 ポート 1G SX FTW ネットワーク モジュール シングルワイド（FPR4K-NM-6X1SX-F）
  - Firepower 6 ポート 10G SR FTW ネットワーク モジュール シングルワイド（FPR4K-NM-6X10SR-F）
  - Firepower 6 ポート 10G LR FTW ネットワーク モジュール シングルワイド（FPR4K-NM-6X10LR-F）
  - Firepower 2 ポート 40G SR FTW ネットワーク モジュール シングルワイド（FPR4K-NM-2X40G-F）
  - Firepower 8 ポート 1G Copper FTW ネットワーク モジュール シングルワイド（FPR-NM-8X1G-F）
- FirePOWER 9300：
  - Firepower 6 ポート 10G SR FTW ネットワーク モジュール シングルワイド（FPR9K-NM-6X10SR-F）
  - Firepower 6 ポート 10G LR FTW ネットワーク モジュール シングルワイド（FPR9K-NM-6X10LR-F）
  - Firepower 2 ポート 40G SR FTW ネットワーク モジュール シングルワイド（FPR9K-NM-2X40G-F）

ハードウェア バイパス では以下のポート ペアのみ使用できます。

- 1 および 2
- 3 および 4
- 5 および 6
- 7 および 8

インラインセットとパッシブインターフェイスのガイドライン

ファイアウォール モード

- ERSPAN インターフェイスは、デバイスがルーテッド ファイアウォール モードになっている場合にのみ許可されます。

クラスタリング

- インラインセットのリンクステートの伝達は、クラスタリングではサポートされていません。

マルチインスタンスモード

- マルチインスタンスの共有インターフェイスはサポートされていません。非共有インターフェイスを使用する必要があります。
- マルチインスタンスのシャーシ定義サブインターフェイスはサポートされていません。物理インターフェイスまたは EtherChannel を使用する必要があります。

一般的な注意事項

- インラインセットとパッシブインターフェイスは物理インターフェイスおよびEtherChannelsのみをサポートし、VLAN、またはその他の仮想インターフェイス（マルチインスタンスのシャーシ定義サブインターフェイスを含む）は使用できません。
- IPS インターフェイスは通常のファイアウォール保護をサポートしていないため、IPS セキュリティ ポリシー（Snort）では、すべてのトラフィックを検査できるようにトラフィック フローが同じ Firewall Threat Defense を通過する必要があります。
- Bidirectional Forwarding Detection（BFD）エコー パケットは、インライン セットを使用するときに、Firewall Threat Defense を介して許可されません。BFD を実行している Firewall Threat Defense の両側に 2 つのネイバーがある場合、Firewall Threat Defense は BFD エコー パケットをドロップします。両方が同じ送信元および宛先 IP アドレスを持ち、LAND 攻撃の一部であるように見えるからです。
- インラインセットとパッシブインターフェイスについては、Firewall Threat Defense ではパケットで 802.1Q ヘッダーが 2 つまでサポートされます（Q-in-Q サポートとも呼ばれます）。ただし、Firepower 4100/9300 は例外で、802.1Q ヘッダーは 1 つだけサポートされます。**注**：ファイアウォールタイプのインターフェイスでは Q-in-Q はサポートされず、802.1Q ヘッダーは 1 つだけサポートされます。

ハードウェア バイパス ガイドライン

- ハードウェア バイパス ポートはインライン セットでのみサポートされます。
- ハードウェア バイパス ポートを EtherChannel の一部にはできません。
- ハードウェア バイパス 高可用性モードではサポートされていません。
- ハードウェア バイパス は Firepower 9300 でのシャーシ内クラスタリングでサポートされます。シャーシ内の最後のユニットに障害が発生すると、ポートはハードウェアバイパスモードになります。シャーシ間クラスタリングはサポートされません。これは、シャーシ間クラスタリングがスパンドEtherChannelのみをサポートするためです。ハードウェア バイパス ポートを EtherChannel の一部にすることはできません。

- Firepower 9300 でのシャーシ内クラスタに含まれるすべてのモジュールに障害が発生すると、最終ユニットで ハードウェア バイパス がトリガーされ、トラフィックは引き続き通過します。ユニットが復帰すると、ハードウェア バイパスはスタンバイ モードに戻ります。ただし、アプリケーショントラフィックと一致するルールを使用すると、それらの接続が切断され、再確立する必要がある場合があります。状態情報がクラスタユニットに保持されず、ユニットがトラフィックを許可されたアプリケーションに属するものとして識別できないため、接続は切断されます。トラフィックのドロップを回避するには、アプリケーションベースのルールの代わりにポートベースのルールを使用します（展開に適している場合）。
- ハードウェア バイパス 機能を有効にしなくても、ハードウェア バイパス インターフェイスを標準インターフェイスとして使用できます。

IPS 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 サーバー
- DHCP リレー
- DHCP クライアント
- TCP Intercept
- ルーティング
- NAT
- VPN
- アプリケーション インスペクション
- QoS
- NetFlow
- VXLAN

パッシブ インターフェイスの設定

ここでは、次の方法について説明します。

- インターフェイスを有効にします。デフォルトでは、インターフェイスは無効です。
- インターフェイス モードをパッシブまたはERSPANに設定します。ERSPANインターフェイスの場合は、ERSPAN パラメータと IP アドレスを設定します。
- MTU を交換してください。デフォルトでは、MTU は 1500 バイトに設定されます。MTU の詳細については、MTU についてを参照してください。
- 特定の速度と二重通信（使用できる場合）を設定する。デフォルトでは、速度とデュプレックスは [自動（Auto）] に設定されます。

（注） Secure Firewall Threat Defense（FXOS シャーシに搭載） の場合、Firepower 4100/9300 の基本インターフェイスの設定を行います。詳細については、「物理インターフェイスの設定」を参照してください。

始める前に

- EtherChannel を使用している場合は、「EtherChannel の設定」に従って追加します。

手順

ステップ 1 **[デバイス（Devices）]**>**[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイス[編集（Edit）]（✎） をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス [編集（Edit）]（✎） をクリックします。

ステップ 3 [モード（Mode）] ドロップダウン リストで、[パッシブ（Passive）] または [Erspan] を選択します。

ステップ 4 [有効化（Enable）] チェックボックスをオンにして、インターフェイスを有効にします。

ステップ 5 [名前（Name）] フィールドに、48 文字以内で名前を入力します。

ステップ 6 [セキュリティ ゾーン（Security Zone）] ドロップダウン リストからセキュリティ ゾーンを選択するか、[新規（New）] をクリックして、新しいセキュリティ ゾーンを追加します。

ステップ 7 （任意） [Description] フィールドに説明を追加します。

説明は 200 文字以内で入力できます。改行を入れずに 1 行で入力します。

ステップ 8 （任意） [一般（General）] で、[MTU] を 64 ～ 9198 バイトの間で設定します。Secure Firewall Threat Defense Virtual および Secure Firewall Threat Defense（FXOS シャーシに搭載） の場合、最大値は 9000 バイトです。

デフォルト値は 1500 バイトです。

ステップ 9 ERSPAN インターフェイスの場合は、次のパラメータを設定します:

- [フロー ID（Flow Id）]：ERSPAN トラフィックを特定するために送信元と宛先セッションによって使用される ID を、1 ～ 1023 の間で設定します。この ID は、ERSPAN 宛先セッション設定でも入力する必要があります。
- [ソース IP（Source IP）]：ERSPAN トラフィックの送信元として使用される IP アドレスを設定します。

ステップ 10 ERSPAN インターフェイスの場合は、[IPv4] で IPv4 アドレスとマスクを設定します。

ステップ 11 （任意） [Hardware Configuration] をクリックして、デュプレックスと速度を設定します。

正確な速度とデュプレックスオプションはハードウェアによって異なります。

- [Duplex]：[Full]、[Half]、または[Auto]を選択します。デフォルトは[Auto（自動）]です。
- [速度（Speed）]：[10],[100]、[1000]、または[自動（Auto）]を選択します。デフォルトは[Auto（自動）]です。

ステップ 12 **[OK]** をクリックします。

ステップ 13 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

インライン セットを設定します。

ここでは、インラインセットに追加できるインラインペアごとに2つの物理インターフェイスまたはEtherChannelを有効にして名前を付けます。インラインセットごとに複数のインラインペアを追加できます。また、状況に応じて、サポートされるインラインペアに対して ハードウェア バイパス を有効にすることができます。

（注） Firepower 4100/9300 の場合、シャーシで FXOS の基本インターフェイスの設定を構成します。詳細については、「物理インターフェイスの設定」を参照してください。

始める前に

- EtherChannel を使用している場合は、「EtherChannel の設定」に従って追加します。
- Firewall Threat Defense インライン ペア インターフェイスに接続する STP 対応スイッチに対して STP PortFast を設定することを推奨します。この設定は、ハードウェア バイパスの設定に特に有効でバイパス時間を短縮できます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイス[編集（Edit）]（✎） をクリックします。[インターフェイス（Interfaces）]タブがデフォルトで選択されます。

ステップ 2 インラインペアの各インターフェイスについて、インターフェイスに名前を付けて有効にします。他のハードウェア設定を指定することもできます。インラインペアの各インターフェイスのハードウェア設定が一致していることを確認してください。インターフェイスの複数のペアを設定できます。

a) 編集するインターフェイス [編集（Edit）]（✎） をクリックします。

b) [名前（Name）] フィールドに、48 文字以内で名前を入力します。
c) [有効（Enabled）] チェック ボックスをオンにして、インターフェイスを有効化します。
d) （任意） [Description] フィールドに説明を追加します。

説明は 200 文字以内で入力できます。改行を入れずに 1 行で入力します。

e) [モード（Mode）] は [なし（None）] のままにします。

このインターフェイスをインラインセットに追加すると、このフィールドにモードのインラインが表示されます。

f) セキュリティゾーンはまだ設定しないでください。後でこの手順でインラインセットを作成してから設定する必要があります。
g) （任意） [Hardware Configuration] をクリックして、デュプレックスと速度を設定します。

正確な速度とデュプレックスオプションはハードウェアによって異なります。

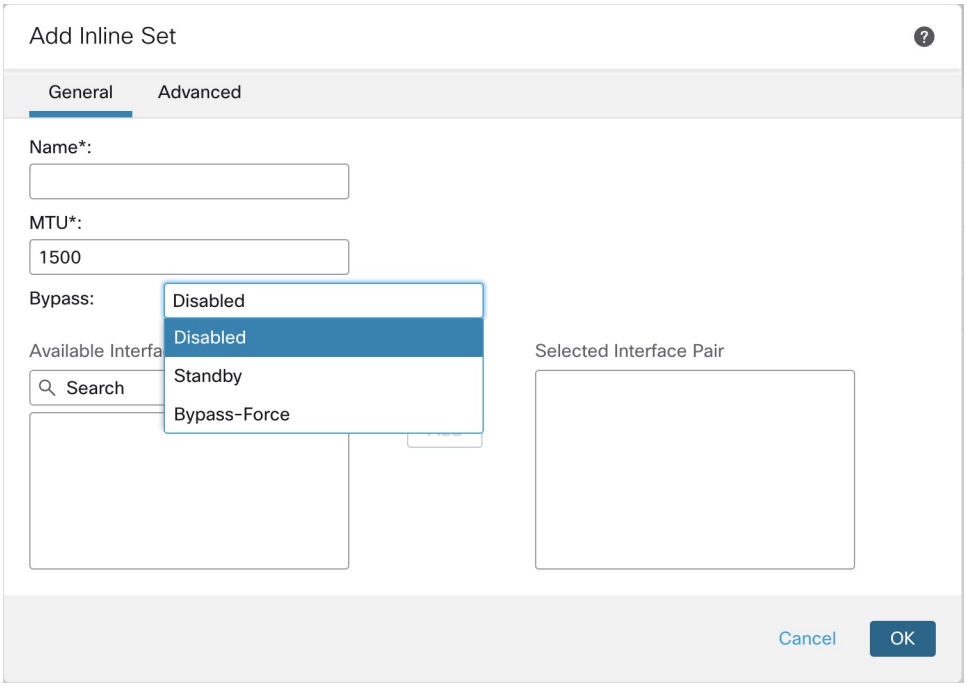
- [Duplex]：[Full]、[Half]、または [Auto] を選択します。デフォルトは [Auto（自動）] です。
- [速度（Speed）]：[10],[100]、[1000]、または [自動（Auto）] を選択します。デフォルトは [Auto（自動）] です。

h) [OK] をクリックします。

このインターフェイスに対して他の設定は行わないでください。

ステップ 3 [Inline Sets] をクリックします。
ステップ 4 [Add Inline Set] をクリックします。

図 *2:* インラインセットの追加



[Add Inline Set] ダイアログボックスが、[General] が選択された状態で表示されます。

ステップ 5 [名前（Name）] フィールドに、セットの名前を入力します。

ステップ 6 （任意） ジャンボフレームを有効にするには、**MTU** を変更します。

インラインセットの MTU の設定は使用されません。ただし、ジャンボフレームの設定はインラインセットに関連します。ジャンボフレームによりインラインインターフェイスは最大9000バイトのパケットを受信できます。ジャンボフレームを有効にするには、デバイスのすべてのインターフェイスの MTU を 1500 バイトより大きい値に設定する必要があります。

ステップ 7 ハードウェア バイパス を設定します。

a) [Bypass] モードの場合、次のいずれかのオプションを選択します。

- [Disabled]：ハードウェア バイパス がサポートされているインターフェイスの場合はハードウェア バイパス を無効にするか、またはハードウェア バイパス がサポートされていないインターフェイスを使用します。
- [Standby]：サポートされているインターフェイスの ハードウェア バイパス をスタンバイ状態に設定します。ハードウェア バイパス インターフェイスのペアのみ表示されます。スタンバイ状態の場合、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保ちます。
- **[Bypass-Force]**：インターフェイスペアを手動で強制的にバイパス状態にします。**[Inline Sets]** では、[Bypass-Force] モードになっているインターフェイスペアに対して [Yes] が表示されます。

b) [Available Interfaces Pairs] 領域でペアをクリックし、[Add] をクリックして [Selected Interface Pair] 領域にそのペアを移動します。

この領域には、モードが [None] に設定されている名前付きインターフェイスと有効なインターフェイス間で可能なすべてのペアが表示されます。

ステップ 8 （任意） **[Advanced]** をクリックして、次のオプション パラメータを設定します。

- **[Tap Mode]**：インラインタップ モードに設定します。

  同じインライン セットでこのオプションと厳密な TCP 強制を有効にすることはできないことに注意してください。

  （注）
  タップモードを有効または無効にする必要がある場合は、メンテナンス期間中に行う必要があります。デバイスがトラフィックを渡している間にモードを変更すると、トラフィックが中断される可能性があります。

  （注）
  タップモードは、トラフィックによっては Firewall Threat Defense のパフォーマンスに大きく影響します。

- **[Propagate Link State]**：リンクステートの伝達を設定します。

  インラインセットのインターフェイスの 1 つが停止した場合、リンク ステート伝播によってインライン インターフェイス ペアのもう一方のインターフェイスも自動的に停止します。停止したインターフェイスが再び起動すると、もう一方のインターフェイスも自動的に起動します。つまり、いずれかのインターフェイスのリンク ステートが変更されると、デバイスがその変更を検知し、もう一方のインターフェイスのリンク ステートを更新して両方のインターフェイスのリンク ステートを一致させるということです。リンク ステートの変更が伝播されるまでに最大 4 秒かかることに注意してください。障害状態のネットワーク デバイスを避けてトラフィックを自動的に再ルーティングするようルータが設定された復元力の高いネットワーク環境では、リンク ステート伝播が特に有効です。

  （注）
  クラスタリングを使用する場合は、[リンクステートの伝達（Propagate Link State）] を有効にしないでください。

- [Snort フェール オープン（Snort Fail Open）] : [ビジー（Busy）] オプションと [ダウン（Down）] オプションのいずれか、または両方を有効/無効にして、Snort プロセスがビジーまたはダウンしている場合は新規または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か（有効）、またはトラフィックをドロップします（無効）。

  デフォルトでは、Snort プロセスがダウンしている場合はトラフィックをインスペクションなしで通過させ、ビジーの場合はトラフィックをドロップします。

  Snort プロセスの状態には以下の意味があります。

  - ビジー：トラフィック バッファが満杯であるため十分な速度でトラフィックを処理しきれていません。デバイスが処理できる量を上回るトラフィックがあるか、他のソフトウェア リソースに問題があることを意味します。

- ダウン：再起動が必要となる設定を導入したため、再起動が行われています。展開またはアクティブ化された際に Snort プロセスを再起動する設定を参照してください。

Snort プロセスは、ダウンしてから再起動すると、新しい接続を検査します。誤検知と検出漏れを防ぐために、Snort プロセスはインライン インターフェイス、ルーテッド インターフェイス、またはトランスペアレントインターフェイス上の既存の接続を検査しません。これは、プロセスのダウン中に初期セッション情報が失われている可能性があるためです。

（注）
Snort プロセスが開始できない場合、Snort プロセスに依存する機能は動作しません。該当する機能には、アプリケーション制御とディープインスペクションが含まれます。システムでは、シンプルかつ容易に判断できるトランスポート層とネットワークの特性を使用して、基本的なアクセスコントロールのみ実行されます。

（注）
[厳密なTCPの適用（Strict TCP Enforcement）] オプションはサポートされていません。

ステップ 9 各インターフェイスのセキュリティゾーンを設定します。

a) [インターフェイス（Interfaces）] をクリックします。
b) メンバーインターフェイスの [編集（Edit）]（ ） をクリックします。
c) **[Security Zone]** ドロップダウン リストからセキュリティ ゾーンを選択するか、**[New]** をクリックして、新しいセキュリティゾーンを追加します。

セキュリティ ゾーンはインターフェイスをインライン セットに追加してからでないと設定できません。インターフェイスをインラインセットに追加すると、モードがインラインに設定されて、インライン タイプのセキュリティ ゾーンを選択できるようになります。

d) **[OK]** をクリックします。

ステップ 10 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

インラインセットとパッシブインターフェイスの履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
サポート対象ネットワークモジュールに関する Cisco Secure Firewall 3100 でのハードウェアバイパスのサポート	7.2	任意（Any）	Cisco Secure Firewall 3100 は、ハードウェア バイパス ネットワーク モジュールの使用時に、ハードウェアバイパス機能をサポートするようになりました。 新規/変更された画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [物理インターフェイスの編集（Edit Physical Interface）]** サポートされるプラットフォーム：Cisco Secure Firewall 3100
Firepower 4100/9300 の Firewall Threat Defense 動作リンク状態と物理リンク状態の同期	6.7	いずれか	Firepower 4100/9300 シャーシで、Firewall Threat Defense 動作リンク状態をデータインターフェイスの物理リンク状態と同期できるようになりました。現在、FXOS 管理状態がアップで、物理リンク状態がアップである限り、インターフェイスはアップ状態になります。Firewall Threat Defense アプリケーション インターフェイスの管理状態は考慮されません。Firewall Threat Defense からの同期がない場合は、たとえば、Firewall Threat Defense アプリケーションが完全にオンラインになる前に、データインターフェイスが物理的にアップ状態になったり、シャットダウン開始後からしばらくの間アップ状態のままになったりすることがあります。インラインセットの場合、この状態の不一致によりパケットがドロップされることがあります。これは、 Firewall Threat Defense が処理できるようになる前に外部ルータが Firewall Threat Defense へのトラフィックの送信を開始することがあるためです。この機能はデフォルトで無効になっており、FXOS の論理デバイスごとに有効にできます。 （注） この機能は、クラスタリング、コンテナインスタンス、またはRadware vDP デコレータを使用する Firewall Threat Defense ではサポートされていません。ASA でもサポートされていません。 新規/変更された [Firepower Chassis Manager] 画面：**[論理デバイス（Logical Devices）] > [リンク状態の有効化（Enable Link State）]** 新規/変更された FXOS コマンド：**set link-state-sync enabled**、**show interface expand detail** サポートされているプラットフォーム：Firepower 4100/9300

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
サポート対象ネットワークモジュールに関する Firepower 2130 および 2140 でのハードウェアバイパスのサポート	6.3.0	いずれか	Firepower 2130 および 2140 は、ハードウェア バイパス ネットワーク モジュールの使用時に、ハードウェアバイパス機能をサポートするようになりました。 新規/変更された画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [物理インターフェイスの編集（Edit Physical Interface）]** サポートされるプラットフォーム：Firepower 2130 および 2140
Firewall Threat Defense インラインセットまたはパッシブインターフェイスでの EtherChannel のサポート	6.2.0	いずれか	Firewall Threat Defenseインラインセットまたはパッシブインターフェイスで EtherChannel を使用できるようになりました。
サポート対象ネットワーク モジュールに対する Firepower 4100/9300 でのハードウェア バイパス サポート	6.1.0	いずれか	ハードウェア バイパスは、停電時にトラフィックがインライン インターフェイス ペア間で流れ続けることを確認します。この機能は、ソフトウェアまたはハードウェア障害の発生時にネットワーク接続を維持するために使用できます。 新規/変更された画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [物理インターフェイスの編集（Edit Physical Interface）]** サポートされるプラットフォーム：Firepower 4100/9300
Firewall Threat Defense のインライン セット リンク ステート伝達サポート	6.1.0	いずれか	Firewall Threat Defense アプリケーションでインライン セットを設定し、リンク ステート伝達を有効にすると、Firewall Threat Defense はインライン セット メンバーシップを FXOS シャーシに送信します。リンク ステート伝達により、インライン セットのインターフェイスの 1 つが停止した場合、シャーシは、インライン インターフェイス ペアの 2 番目のインターフェイスも自動的に停止します。 新規/変更された FXOS コマンド：**show fault |grep link-down、show interface detail**

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。