



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 \(1 ページ\)](#)
- [インラインセットの要件と前提条件 \(5 ページ\)](#)
- [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 \(8 ページ\)](#)
- [パッシブ インターフェイスの設定 \(10 ページ\)](#)
- [インラインセットを設定します。 \(11 ページ\)](#)
- [インラインセットとパッシブインターフェイスの履歴 \(16 ページ\)](#)

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と一緒にバインドし、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なら、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。



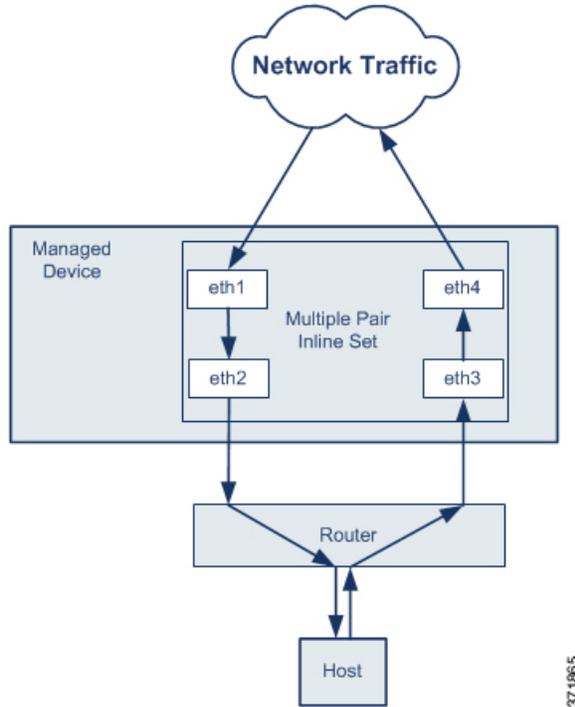
(注) 「透過インラインセット」としてインラインセットに馴染みがある人もいますが、インラインインターフェイスのタイプはトランスペアレントファイアウォールモードやファイアウォールタイプのインターフェイスとは無関係です。

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



371865

- (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ーし、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Hardware Bypass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)、Hardware Bypass 機能を有効にできます。Hardware Bypass 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。

Hardware Bypass トリガー

Hardware Bypass 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ペ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 Hardware Bypass

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、Hardware Bypass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。

Hardware Bypass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、Hardware Bypassをトリガーしません。

Hardware Bypass Status

システムの電源が入っている場合、バイパス LED はHardware Bypass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 インストール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

User roles

- Admin
- Access Admin
- Network Admin

Hardware Bypass 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 Hardware Bypass をサポートします。

- Cisco Secure Firewall 3100
- Firepower 4100

- Cisco Secure Firewall 4200
- 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) Hardware Bypass 機能を有効にしなくても、Hardware Bypass 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 Hardware Bypass ネットワーク モジュールは以下のとおりです。

- 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)
- Secure Firewall 4200 :
 - 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) (FPR4K-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) (FPR4K-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) (FPR4K-XNM-X25SRF)
 - 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) (FPR4K-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)
(FPR4K-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)
(FPR4K-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)

Hardware Bypass 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。
- 個別インターフェイスモードではIPS専用インターフェイスはサポートされません。

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。

Hardware Bypass ガイドライン

- Hardware Bypass ポートはインライン セットでのみサポートされます。
- Hardware Bypass ポートを EtherChannel の一部にはできません。
- Hardware Bypass 高可用性モードではサポートされていません。
- Hardware Bypass 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 Hardware Bypass 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。Hardware Bypass 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 Hardware Bypass 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、Hardware Bypass 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）。
- Hardware Bypass 機能を有効にしなくても、Hardware Bypass 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спек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、[About the MTU](#)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 on the FXOS chassis 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、「[Configure a Physical Interface](#)」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** **[Devices > Device Management]** を選択して、Firewall Threat Defense デバイスに対して **[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 **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 [Ersparn] 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** [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 on the FXOS chassis 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、**Deploy > Deploy** に移動して、ポリシーを割り当てたデバイスにデプロイします。変更内容は導入するまで適用されません。

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 Hardware Bypass 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、「[Configure a Physical Interface](#)」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、Hardware Bypass 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** [Devices > Device Management] を選択して、Firewall Threat Defense デバイスに対して [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。
- 編集するインターフェイス **Edit (✎)** をクリックします。
 - [名前 (Name)] フィールドに、48 文字以内で名前を入力します。
 - [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。
 - (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。
 - [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。
 - 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。
 - (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。
 - [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 Hardware Bypass 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] : Hardware Bypass がサポートされているインターフェイスの場合は Hardware Bypass を無効にするか、または Hardware Bypass 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 Hardware Bypass をスタンバイ状態に設定します。Hardware Bypass 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。

インラインセットを設定します。

- 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できていません。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す。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 **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、**Deploy > Deploy** に移動して、ポリシーを割り当てたデバイスにデプロイします。変更内容は導入するまで適用されません。

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	Minimum Firewall Management Center	Minimum 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 4200 でのハードウェアバイパスのサポート	7.4.0	7.4.0	<p>Cisco Secure Firewall 4200 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します。</p> <p>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)]</p> <p>サポートされるプラットフォーム：Cisco Secure Firewall 4200</p>
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)	<p>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。</p> <p>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)]</p> <p>サポートされるプラットフォーム：Cisco Secure Firewall 3100</p>

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
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	任意 (Any)	<p>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。</p> <p>(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。</p> <p>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)]</p> <p>新規/変更された FXOS コマンド : set link-state-sync enabled、show interface expand detail</p> <p>サポートされているプラットフォーム : Firepower 4100/9300</p>
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	<p>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。</p> <p>新規/変更された画面 :</p> <p>[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)]</p> <p>サポートされるプラットフォーム : Firepower 2130 および 2140</p>

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
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	<p>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。</p> <p>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)]</p> <p>サポートされるプラットフォーム：Firepower 4100/9300</p>
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	<p>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。</p> <p>新規/変更された FXOS コマンド：show fault grep link-down、show interface detail</p>

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。