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 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 インターフェイスについて

このセクションでは、IPS インターフェイスについて説明します。

IPS インターフェイスタイプ

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。

IPS 専用インターフェイスは以下のタイプとして展開できます。

- インライン セット、タップ モードのオプションあり：インライン セットは「Bump In The Wire」のように動作し、2 つのインターフェイス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 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 セットの外部に再送信されます。

  タップモードでは、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、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、Threat Defense がインラインであるかのように Thereat Defense とネットワーク間の接続を設定し、Threat Defense が生成する侵入イベントの種類を分析できます。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。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、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 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。

- パッシブまたは ERSPAN パッシブ：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を流れるトラフィックをモニタします。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 Threat Defense を構成した場合は、Threat Defense で特定のアクション（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、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 （4 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。

- Threat Defense のクラッシュ
- 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、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

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
- 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） 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）

- 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）

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。
- 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、Threat Defense を介して許可されません。BFD を実行している Threat Defense の両側に 2 つのネイバーがある場合、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、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。
- 同じインラインセットに対して ハードウェア バイパス およびリンク状態の伝達を有効にしないでください。

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、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（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。

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、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）[ハードウェア構成（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 [自動（Auto）] 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 [自動（Auto）] 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。変更はポリシーを展開するまで有効になりません。

インラインセットを設定します。

このセクションでは、インラインセットに追加できる 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。また、状況に応じて、サポートされるインターフェイスペアに対して 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。
- 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、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、[なし（None）] を選択します。

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。

ステップ 4 [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。

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。

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。

ステップ 6 （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、改行を入れずに 1 行で入力します。

ステップ 7 （任意） [ハードウェア構成（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 [自動（Auto）] 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 [自動（Auto）] です。

ステップ 8 [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 9 インラインセットに追加する 2 番目のインターフェイスに対し、**[編集（Edit）]**（✎） をクリックします。

ステップ 10 最初のインターフェイスに関する設定を行います。

ステップ 11 [インライン セット（Inline Sets）] をクリックします。

ステップ 12 [インライン セットの追加（Add Inline Set）] をクリックします。
[インラインセットの追加（Add Inline Set）] ダイアログボックスが、[全般（General）] が選択された状態で表示されます。

ステップ 13 [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 14 （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 15 ハードウェア バイパス を設定します。

（注） 同じインラインセットに対して **[バイパス（Bypass）]** および **[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。

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。
- [バイパス強制（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。[インラインセット（Inline Sets）] では、[バイパス強制（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 [はい（Yes）] が表示されます。

b) [使用可能なインターフェイスペア（Available Interfaces Pairs）] 領域でペアをクリックし、[追加（Add）] をクリックして [選択済みインターフェイスペア（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 [なし（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 16 （任意） [詳細（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。

- [タップモード（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 セットに対し、このオプション、および厳密な TCP 強制を同時に有効化することはできません。

  （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 Threat Defense のパフォーマンスに大きく影響します。

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

  リンクステートの伝達によって、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、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。停止したインターフェイスが再び起動すると、2 番目のインターフェイスも自動的に起動します。つまり、1 つのインターフェイスのリンクステートが変化すると、デバイスはその変化を検知し、その変化に合わせて他のインターフェイスのリンクステートを更

新します。ただし、デバイスからリンクステートの変更が伝達されるまで最大4秒かかります。障害状態のネットワークデバイスを自動的に避けてトラフィックを再ルーティングするようにルータが設定されている復元力の高いネットワーク環境では、リンク ステートの伝達が特に有効です。

（注） 同じインラインセットに対して [バイパス（Bypass）] および [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。

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）]：Snort プロセスがビジーであるか、ダウンしている場合に、インスペクション（有効）またはドロップ（無効）されることなく、新規および既存のトラフィックを通過させる場合は、[ビジー（Busy）] オプションおよび [ダウン（Down）] オプションのいずれかまたは両方を有効または無効にします。

  デフォルトでは、Snort プロセスがダウンしている場合、トラフィックはインスペクションなしで通過し、Snort プロセスがビジーの場合、トラフィックはドロップされます。

  Snort プロセスが次の場合。

  - [ビジー（Busy）]：トラフィック バッファが満杯なため、トラフィックを高速処理できません。デバイスの処理量を超えるトラフィックが存在していること、またはその他のソフトウェア リソースの問題があることを示しています。
  - [ダウン（Down）]：再起動が必要な設定が展開されたため、プロセスが再起動しています。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。Snort プロセスでは、誤検出と検出漏れを防ぐために、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 インターフェイスの既存の接続のインスペクションは実行されません。これは、プロセスがダウンしていた間に初期の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 フェール オープン時には、Snort プロセスに依存する機能は働きません。そのような機能には、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 17 [インターフェイス（Interfaces）] をクリックします。

ステップ 18 いずれかのメンバーインターフェイスの **[編集（Edit）]**（✎）をクリックします。

ステップ 19 [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。

ゾーンは、インラインセットにインターフェイスを追加した後にのみ設定できます。インラインセットにインターフェイスを追加することで、インラインのモードが設定され、インラインタイプのセキュリティゾーンを選択できます。

ステップ 20 [OK] をクリックします。

ステップ 21 2 番目のインターフェイスのセキュリティゾーンを設定します。

ステップ 22 **[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。変更はポリシーを展開するまで有効になりません。

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 Management Center	最小 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

機能	最小 Management Center	最小 Threat Defense	詳細
Firepower 4100/9300 の 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）	Firepower 4100/9300 シャーシで、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。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。Threat Defense からの同期がない場合は、たとえば、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、 Threat Defense が処理できるようになる前に外部ルータが 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 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** サポートされるプラットフォーム：Firepower 4100/9300
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
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	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。

機能	最小 Management Center	最小 Threat Defense	詳細
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
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	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、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** サポートされるプラットフォーム：Firepower 4100/9300、Firepower 2100（6.2.1 以降）

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。