



# Firepower Threat Defense の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。

- [インラインセットのハードウェア バイパスについて \(1 ページ\)](#)
- [インラインセットの前提条件 \(3 ページ\)](#)
- [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 \(4 ページ\)](#)
- [パッシブインターフェイスの設定 \(5 ページ\)](#)
- [インラインセットを設定します。 \(7 ページ\)](#)
- [Firepower Threat Defense のインラインセットとパッシブインターフェイスの履歴 \(11 ページ\)](#)

## インラインセットのハードウェア バイパスについて

Firepower 9300、4100、および 2100 シリーズ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前提条件 \(3 ページ\)](#) 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。

- FTD アプリケーションのクラッシュ
- FTD アプリケーションの再起動
- セキュリティ モジュールの再起動

- Firepower のシャーシのクラッシュ
- Firepower のシャーシの再起動またはアップグレード
- 手動トリガー
- Firepower のシャーシの電力損失
- セキュリティ モジュールの電力損失

## 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 セットの前提条件

## ハードウェア バイパス のサポート

FTD 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 9300
- Firepower 4100 シリーズ
- Firepower 2100 シリーズ

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 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 (FPR-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 (FPR-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 (FPR-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 (FPR-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)

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 と 2
- 3 と 4
- 5 と 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。

## 一般的なガイドライン

- 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EtherChannelのみをサポートし、冗長インターフェイス、VLAN などを使用するとはできません。IPS 専用インターフェイスでは、Firepower 4100/9300 サブインターフェイスもサポートされていません。
- インレットセットとパッシブインターフェイスは、シャーシ内およびシャーシ間のクラスタリングでサポートされます。
- 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、FTD を介して許可されません。BFD を実行している FTD の両側に 2 つのネイバーがある場合、FTD 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。

## 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。
- 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ていません。
- クラスタ内のすべてのユニット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 高可用性モードではサポートされていません。

**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 (DHCP server) ]
- 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

スマートライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか (Any)	該当なし	FTD	いずれか (Any)	Admin Access Admin Network Admin

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) FXOS シャーシ上の Firepower Threat Defense の場合、Firepower 4100/9300 シャーシ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。

- 
- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] の順に選択し、FTD デバイスの編集アイコン (✎) をクリックします。デフォルトで [インターフェイス (Interfaces)] タブが選択されています。
- ステップ 2** 編集するインターフェイスの編集アイコン (✎) 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) [説明 (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)] タブで、[MTU] を 64 ~ 9198 バイトの間で設定します。Firepower Threat Defense Virtual および FXOS シャーシ上の Firepower Threat Defense 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] タブで 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)] タブをクリックして、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。
- [デュプレックス (Duplex)]: [全 (Full)]、[半 (Half)]、または [自動 (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、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入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。

スマートライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス
いずれか (Any)	該当なし	FTD	いずれか (Any)	Admin Access Admin Network Admin

ここでは、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) FXOS シャーシ上の Firepower Threat Defense の場合、Firepower 4100/9300 シャーシ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

- Firepower 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 を設定することをお勧めします。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。

**ステップ 1** [デバイス (Devices) ] > [デバイス管理 (Device Management) ] の順に選択し、FTD デバイスの編集アイコン (✎) をクリックします。デフォルトで [インターフェイス (Interfaces) ] タブが選択されています。

**ステップ 2** 編集するインターフェイスの編集アイコン (✎) 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** [名前 (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) [説明 (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。

■ インラインセットを設定します。

**ステップ 7** (任意) [ハードウェア構成 (Hardware Configuration)] タブをクリックして、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。

- [デュプレックス (Duplex)]: [全 (Full)]、[半 (Half)]、または[自動 (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、編集アイコン (✎) 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)] タブをクリックします。

**ステップ 12** [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、[一般 (General)] タブ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** (任意) [バイパス (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)] タブでは、[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。

**ステップ 16** [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 17** (任意) [詳細 (Advanced)] タブをクリックして、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。

- [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。

- [厳密なTCP強制 (Strict TCP Enforcement)] : TCPのセキュリティを最大限に生かすために、厳密な強制を有効にできます。この機能は3ウェイハンドシェイクが完了していない接続をブロックします。

厳密な適用では次のパケットもブロックされます。

- 3ウェイハンドシェイクが完了していない接続の非SYN TCPパケット
  - レスポンダがSYN-ACKを送信する前にTCP接続のイニシエータから送信された非SYN/RSTパケット
  - SYNの後、セッションの確立前にTCP接続のレスポндаから送信された非SYN-ACK/RSTパケット
  - 発信側または応答側のどちらかから送信された、確立されたTCP接続のSYNパケット
- [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。

■ インラインセットを設定します。

Snort プロセスは、ダウンしてから再起動すると、新しい接続のインスペクションを実行します。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、ルールセットインターフェイス、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。

**ステップ 18** [Interfaces] タブをクリックします。

**ステップ 19** いずれかのメンバー インターフェイスの編集 (✎) アイコンをクリックします。

**ステップ 20** [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 21** [OK] をクリックします。

**ステップ 22** 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 23** [Save (保存) ] をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

## Firepower Threat Defense の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	バージョン	詳細
サポート対象ネットワークモジュールに対する Firepower 2100 でのハードウェアバイパスサポート	6.3.0	<p>Firepower 2100 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>新しい/変更された画面：  <b>[Devices] &gt; [Device Management] &gt; [Interfaces] &gt; [Edit Physical Interface]</b></p> <p>サポートされるプラットフォーム：            Firepower 2100</p>
FTD インラインセットでの EtherChannel のサポート	6.2.0	<p>FTD インラインセットで Etherchannel を使用できるようになりました。</p> <p>サポートされ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	<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>新しい/変更された画面：  <b>[Devices] &gt; [Device Management] &gt; [Interfaces] &gt; [Edit Physical Interface]</b></p> <p>サポートされるプラットフォーム：            Firepower 4100/9300</p>

機能	バージョン	詳細
FTD 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	<p>FTD 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、FTD 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 : <b>show fault  grep link-down、show interface detail</b></p> <p>サポートされる プラットフォーム : Firepower 4100/9300</p>