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

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 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。

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EtherChannels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 インスペクション
- 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	サポートされるドメイン	アクセス（**Access**）
任意（Any）	該当なし	FTD	任意（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。

手順

ステップ 1 **[Devices]** > **[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、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 [保存（Save）] をクリックします。

これで、[展開（Deploy）] 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	サポートされるドメイン	アクセス（Access）
任意（Any）	該当なし	FTD	任意（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。

手順

ステップ 1 **[Devices]** > **[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、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）] 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 [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、[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。

- [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 接続のレスポンダから送信された非 SYN-ACK/RST パケット
  - イニシエータまたはレスポンダから確立された 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。

  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。

ステップ 18 [インターフェイス（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 [保存（Save）] をクリックします。

これで、[展開（Deploy）] 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（Version）	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	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。 新しい/変更された画面： **[Devices] > [Device Management] > [Interfaces] > [Edit Physical Interface]** サポートされるプラットフォーム：Firepower 2100
FTD インライン セットでの EtherChannel のサポート	6.2.0	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。 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	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。 新しい/変更された画面： **[Devices] > [Device Management] > [Interfaces] > [Edit Physical Interface]** サポートされるプラットフォーム：Firepower 4100/9300

機能	バージョン（Version）	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	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。 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