



IPS デバイスの設定

パッシブまたはインラインのいずれかの IPS 展開でデバイスを設定できます。パッシブ展開では、ネットワークトラフィックのフローからアウトオブバンドでシステムを展開します。インライン展開では、2つのポートを一緒にバインドすることで、ネットワークセグメント上でシステムを透過的に設定します。

以下の項では、FireSIGHT システムのパッシブ展開とインライン展開用にデバイスを設定する方法について説明します。

- [パッシブ IPS 展開について \(5-1 ページ\)](#)
- [パッシブ インターフェイスの設定 \(5-2 ページ\)](#)
- [インライン IPS 展開について \(5-3 ページ\)](#)
- [インライン インターフェイスの設定 \(5-3 ページ\)](#)
- [インラインセットの設定 \(5-5 ページ\)](#)
- [Blue Coat X シリーズ インターフェイス用の Cisco NGIPS の設定 \(5-13 ページ\)](#)

パッシブ IPS 展開について

ライセンス:Protection

パッシブ(受動)IPS 展開では、FireSIGHT システムは、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監視します。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。これにより、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。パッシブ展開で構成されたシステムでは、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。



(注)

発信トラフィックにはフロー制御パケットが含まれています。そのため、アプライアンスのパッシブインターフェイスに発信トラフィックが表示されることがあり、設定によっては、イベントが生成されることもあります。これは正常な動作です。

パッシブ インターフェイスの設定

ライセンス:Protection

管理対象デバイス上の 1 つ以上の物理ポートをパッシブ インターフェイスとして設定できます。

Cisco パッケージのインストール時に、Blue Coat X-Series 向け Cisco NGIPS インターフェイスをパッシブまたはインラインのいずれかに設定します。FireSIGHT システム Web インターフェイスを使用して、Blue Coat X-Series 向け Cisco NGIPS インターフェイスを再設定することはできません。詳細については、[Blue Coat X シリーズ インターフェイス用の Cisco NGIPS の設定 \(5-13 ページ\)](#)を参照してください。



注意

センシング インターフェイスまたはインラインセットの MTU の任意の値(シリーズ 2)または最高値(シリーズ 3)を変更すると、変更を適用する際、変更したインターフェイスだけではなく、デバイス上のすべてのセンシング インターフェイスに対するトラフィック インспекションが一時的に中断されます。この中断中にトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。[Snort の再開によるトラフィックへの影響 \(1-9 ページ\)](#)を参照してください。

パッシブ インターフェイスを設定する方法:

アクセス:Admin/Network Admin

- 手順 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
[デバイス管理 (Device Management)] ページが表示されます。
- 手順 2 パッシブ インターフェイスを設定するデバイスの横にある編集アイコン(✎)をクリックします。
[インターフェイス (Interfaces)] タブが表示されます。
- 手順 3 パッシブ インターフェイスとして設定するインターフェイスの横にある編集アイコン(✎)をクリックします。
[インターフェイスの編集 (Edit Interface)] ポップアップ ウィンドウが表示されます。
- 手順 4 [パッシブ (Passive)] をクリックして、パッシブ インターフェイスのオプションを表示します。
- 手順 5 オプションで、[セキュリティ ゾーン (Security Zone)] ドロップダウン リストから既存のセキュリティ ゾーンを選択するか、または [新規 (New)] を選択して新しいセキュリティ ゾーンを追加します。
- 手順 6 [有効化 (Enabled)] チェック ボックスをオンにして、パッシブ インターフェイスがトラフィックを監視できるようにします。
このチェック ボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。
- 手順 7 [モード (Mode)] ドロップダウン リストからリンク モードを指定するオプションを選択するか、または [自動ネゴシエーション (Autonegotiation)] を選択して、速度とデュプレックス設定を自動的にネゴシエートするようにインターフェイスを設定します。モード設定は銅インターフェイスでのみ使用可能であることに注意してください。



(注)

8000 シリーズ アプライアンスのインターフェイスは、半二重オプションをサポートしません。

手順 8 [MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI (メディア依存型インターフェイス)、MDIX (メディア依存型インターフェイス クロスオーバー)、または Auto-MDIX のいずれかを指定するオプションを選択します。MDI/MDIX 設定は銅線インターフェイス専用であることに注意してください。

デフォルトでは、MDI/MDIX は **Auto-MDIX** に設定され、MDI と MDIX の間のスイッチングを自動的に処理してリンクを確立します。

手順 9 [MTU] フィールドに最大伝送ユニット (MTU) を入力して、パケットの最大許容サイズを指定します。

設定可能な MTU の範囲は、FireSIGHT システムのデバイス モデルおよびインターフェイスのタイプによって異なる場合があります。詳細については、[管理対象デバイスの MTU の範囲 \(4-70 ページ\)](#) を参照してください。

手順 10 [保存 (Save)] をクリックします。

パッシブ インターフェイスが設定されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください (詳しくは [デバイスへの変更の適用 \(4-27 ページ\)](#) を参照してください)。

インライン IPS 展開について

ライセンス: Protection

インライン展開では、2 つのポートを一緒にバインドすることで、ネットワーク セグメント上で FireSIGHT システムを透過的に設定します。これによって、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システム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。

インライン インターフェイスの設定

ライセンス: Protection

管理対象デバイス上の 1 つ以上の物理ポートをインライン インターフェイスとして設定できます。インライン インターフェイスがインライン展開環境のトラフィックを処理できるようにするには、その前に、インライン インターフェイスのペアをインライン セットに割り当てる必要があります。

インライン ペアのインターフェイスをそれぞれ異なる速度に設定した場合、またはインターフェイスが異なる速度にネゴシエートされる場合は、システムによって警告が出されることに注意してください。

Cisco パッケージのインストール時に、Blue Coat X-Series 向け Cisco NGIPS インターフェイスをパッシブまたはインラインのいずれかに設定します。FireSIGHT システム Web インターフェイスを使用して、Blue Coat X-Series 向け Cisco NGIPS インターフェイスを再設定することはできません。詳細については、[Blue Coat X シリーズ インターフェイス用の Cisco NGIPS の設定 \(5-13 ページ\)](#) を参照してください。



(注) インターフェイスをインライン インターフェイスとして設定すると、そのインターフェイスの NetMod 上の隣接ポートも自動的にインライン インターフェイスとなり、インライン インターフェイスのペアが完成します。

仮想デバイスでインライン インターフェイスを設定するには、隣接するインターフェイスを使用してインライン ペアを作成する必要があります。

インライン インターフェイスを設定する方法:

アクセス: Admin/Network Admin

-
- 手順 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
[デバイス管理 (Device Management)] ページが表示されます。
- 手順 2 インライン インターフェイスを設定するデバイスの横にある編集アイコン(✎)をクリックします。
[インターフェイス (Interfaces)] タブが表示されます。
- 手順 3 インライン インターフェイスとして設定するインターフェイスの横にある編集アイコン(✎)をクリックします。
[インターフェイスの編集 (Edit Interface)] ポップアップ ウィンドウが表示されます。
- 手順 4 [インライン (Inline)] をクリックして、インライン インターフェイスのオプションを表示します。
- 手順 5 オプションで、[セキュリティ ゾーン (Security Zone)] ドロップダウン リストから既存のセキュリティ ゾーンを選択するか、または [新規 (New)] を選択して新しいセキュリティ ゾーンを追加します。
- 手順 6 [インライン セット (Inline Set)] ドロップダウン リストから既存のインライン セットを選択するか、または [新規 (New)] を選択して新しいインライン セットを追加します。
新しいインライン セットを追加した場合は、インライン インターフェイスのセットアップ後に、そのインライン セットを [デバイス管理 (Device Management)] ページ ([デバイス (Devices)] > [デバイス管理 (Device Management)] > [インライン セット (Inline Set)]) で設定する必要があることに注意してください。詳細については、[インライン セットの追加 \(5-7 ページ\)](#) を参照してください。
- 手順 7 [有効化 (Enabled)] チェック ボックスをオンにして、インライン インターフェイスがトラフィックを処理できるようにします。
このチェック ボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。
- 手順 8 [モード (Mode)] ドロップダウン リストからリンク モードを指定するオプションを選択するか、または [自動ネゴシエーション (Autonegotiation)] を選択して、速度とデュプレックス設定を自動的にネゴシエートするようにインターフェイスを設定します。モード設定は銅インターフェイスでのみ使用可能であることに注意してください。



(注) 8000 シリーズ アプライアンスのインターフェイスは、半二重オプションをサポートしません。

- 手順 9 [MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI (メディア依存型インターフェイス)、MDIX (メディア依存型インターフェイス クロスオーバー)、または Auto-MDIX のいずれかを指定するオプションを選択します。MDI/MDIX 設定は銅線インターフェイス専用であることに注意してください。

デフォルトでは、MDI/MDIX は **Auto-MDIX** に設定され、MDI と MDIX の間のスイッチングを自動的に処理してリンクを確立します。

手順 10 [保存(Save)] をクリックします。

インライン インターフェイスが設定されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください(詳しくは [デバイスへの変更の適用 \(4-27 ページ\)](#) を参照してください)。

インラインセットの設定

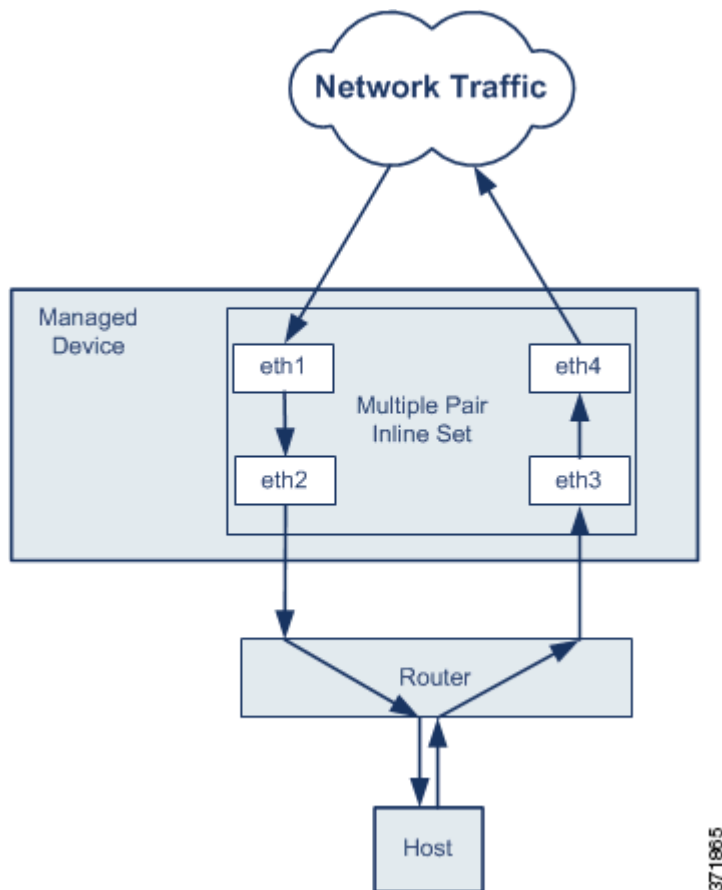
ライセンス:Protection

インライン展開でインライン インターフェイスを使用するには、事前に、インライン セットを設定してインライン インターフェイス ペアをそれらに割り当てる必要があります。インライン セットは、デバイス上の 1 つ以上のインライン インターフェイス ペアからなるグループです。インライン インターフェイス ペアは、一度に 1 つのインライン セットにのみ属することができます。

デバイス トラフィックがインバウンド(着信)であるかアウトバウンド(発信)であるかに応じて、異なるインライン インターフェイス ペアを使用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、管理対象デバイスの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、インライン セットに 1 つのインターフェイス 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 インターフェイス セットに複数のインライン インターフェイス 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できるようになります。パッシブ インターフェイスの場合、これは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。

非同期ルーティング構成を通過するトラフィックから接続イベントが生成された場合、そのイベントは同じインライン インターフェイス ペアの入力インターフェイスと出力インターフェイスを識別できます。たとえば、次の図の構成では、**eth3** を入力インターフェイス、**eth2** を出力インターフェイスとして識別する接続イベントが生成されます。これは、この構成の予期される動作です。



(注)

単一のインライン インターフェイス セットに複数の インターフェイス ペアを割り当てたときに、重複トラフィックの問題が発生した場合は、システムがパケットを一意に識別できるように再設定します。たとえば、別のインライン セットに インターフェイス ペアを再度割り当てるか、セキュリティ ゾーンを変更することができます。

インライン セットを使用するデバイスでは、デバイスの再起動後にパケットを転送する目的でソフトウェアブリッジが自動的にセットアップされます。デバイスが再起動しているときには、実行中のソフトウェアブリッジはありません。インラインセットでバイパス モードを有効にすると、デバイスの再起動中にハードウェアバイパスになります。この場合、システムが停止して再起動する際に、デバイスとのリンクの再ネゴシエーションが原因で数秒間のパケットが失われる可能性があります。ただし、Snort の再起動中には、システムはトラフィックを通過させます。



注意

センシング インターフェイスまたはインラインセットの MTU の任意の値(シリーズ 2)または最高値(シリーズ 3)を変更すると、変更を適用する際、変更したインターフェイスだけではなく、デバイス上のすべてのセンシング インターフェイスに対するトラフィック インспекションが一時的に中断されます。この中断中にトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。Snort の再開によるトラフィックへの影響(1-9 ページ)を参照してください。

詳細については、次の各項を参照してください。

- [インラインセットの表示\(5-7 ページ\)](#)
- [インラインセットの追加\(5-7 ページ\)](#)
- [インラインセットの詳細オプションの設定\(5-9 ページ\)](#)
- [インラインセットの削除\(5-12 ページ\)](#)

インラインセットの表示

ライセンス:Protection

[デバイス管理(Device Management)] ページの [インラインセット(Inline Sets)] タブには、デバイスに設定されているすべてのインラインセットのリストが表示されます。仮想デバイスまたは Blue Coat X-Series 向け Cisco NGIPS では、バイパス モードになるようインラインセットを設定することはできません。「インラインセット テーブル ビューのフィールド」表には、各セットの要約情報が含まれています。

表 5-1 インラインセット テーブル ビューのフィールド

フィールド	説明
名前(Name)	インラインセットの名前。
インターフェイス ペア (Interface Pairs)	インラインセットに割り当てられたインライン インターフェイスのすべてのペアを示すリスト。[インターフェイス (Interfaces)] タブでペアのいずれかのインターフェイスを無効にした場合、そのペアは含まれません。
バイパス (Bypass)	インラインセットの設定済みバイパス モード。

インラインセットの追加

ライセンス:Protection

[デバイスの管理(Device Management)] ページの [インラインセット(Inline Sets)] タブからインラインセットを追加できます。または、インライン インターフェイスを設定するときにインラインセットを追加できます。

インラインセットにはインライン インターフェイス ペアのみを割り当てることができます。管理対象デバイスでインライン インターフェイスを設定する前にインラインセットを作成する必要がある場合は、空のインラインセットを作成し、後からそれにインターフェイスを追加できます。

インラインセットを追加する方法:

アクセス:Admin/Network Admin

-
- 手順 1 [デバイス (Devices)] > [デバイス管理(Device Management)] を選択します。
[デバイス管理(Device Management)] ページが表示されます。
- 手順 2 インラインセットを追加するデバイスの横にある編集アイコン(✎)をクリックします。
[インターフェイス (Interfaces)] タブが表示されます。

- 手順 3 [インライン セット (Inline Sets)] をクリックします。
[インライン セット (Inline Sets)] タブが表示されます。
- 手順 4 [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)] ポップアップ ウィンドウが表示されます。
- 手順 5 [名前 (Name)] フィールドに、インライン セットの名前を入力します。英数字とスペースを使用できます。
- 手順 6 インライン セットに追加するインライン インターフェイス ペアを選択する方法として、次の 2 つのオプションがあります。
- [インターフェイス (Interfaces)] の横で、1 つ以上のインライン インターフェイス ペアを選択し、選択項目の追加アイコン (➤) をクリックします。複数のインライン インターフェイス ペアを選択するには、Ctrl キーまたは Shift キーを使用します。
 - すべてのインターフェイス ペアをインライン セットに追加するには、「すべてを追加」アイコン (➤) をクリックします。



ヒント

インライン セットからインライン インターフェイスを削除するには、1 つ以上のインライン インターフェイス ペアを選択して、選択項目の削除アイコン (⬅) をクリックします。インライン セットからすべてのインターフェイス ペアを削除するには、「すべてを削除」アイコン (⬅) をクリックします。また、[インターフェイス (Interfaces)] タブでペアのいずれかのインターフェイスを無効にすると、ペアが削除されます。

- 手順 7 [MTU] フィールドに最大伝送ユニット (MTU) を入力して、パケットの最大許容サイズを指定します。
- 設定可能な MTU の範囲は、FireSIGHT システムのデバイス モデルおよびインターフェイスのタイプによって異なる場合があります。詳細については、[管理対象デバイスの MTU の範囲 \(4-70 ページ\)](#) を参照してください。
- 手順 8 オプションで、[フェールセーフ (Failsafe)] を選択すると、トラフィックは検出をバイパスしてデバイスを引き続き通過することが許可されます。管理対象デバイスは、内部トラフィック バッファをモニタし、それらのバッファが満杯である場合は検出をバイパスします。
- 内部トラフィック バッファがいっぱいになった場合、インライン セットでデバイスの [フェールセーフ (Failsafe)] を有効にすると、パケットがドロップされるリスクは大幅に軽減されます。ただし、特定の状況では、デバイスによってパケットがドロップされることがあります。最悪の場合、デバイスでネットワークが一時的に停止することがあります。
- なお、シリーズ 3 および 3D9900 のデバイスでのみ、このオプションを使用できます。
- 手順 9 インターフェイスでの障害発生時にインライン インターフェイスのリレーがどのように応答するかを設定するには、次のようにバイパス モードを選択します。
- トラフィックがインターフェイスを通過し続けることを許可するには、[バイパス (Bypass)] を選択します。
 - トラフィックをブロックするには、[非バイパス (Non-Bypass)] を選択します。



(注)

バイパス モードでは、アプライアンスの再起動時に少数のパケットが失われることがあります。また、クラスタ デバイス上のインライン セット、仮想デバイスまたは Blue Coat X-Series 向け Cisco NGIPS 上のインライン セット、8000 シリーズ デバイス上の非バイパス NetMod、および 3D7115 または 3D7125 デバイス上の SFP モジュールに対しては、バイパス モードを設定できないので注意してください。

手順 10 [OK] をクリックします。

インラインセットが追加されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください(詳しくは[デバイスへの変更の適用 \(4-27 ページ\)](#)を参照してください)。



ヒント

タップモード、リンクステート伝達、トランスペアレントインラインモードなど、インラインセットの詳細設定については、[インラインセットの詳細オプションの設定 \(5-9 ページ\)](#)を参照してください。

インラインセットの詳細オプションの設定

ライセンス:Protection

サポートされるデバイス:機能に応じて異なる

インラインセットを設定する際に考慮できるオプションがいくつかあります。各オプションの詳細については、後述の項を参照してください。

タップモード

サポートされるデバイス:シリーズ 3、3D9900

3D9900 およびシリーズ 3 デバイスでは、インライン(またはフェールオープン付きインライン)インターフェイスセットを作成するときにタップモードを使用できます。

タップモードの場合、デバイスはインラインで展開されますが、パケットがデバイスを通過する代わりに各パケットのコピーがデバイスに送信され、ネットワークトラフィックフローは影響を受けません。パケット自体ではなくパケットのコピーを処理するため、ドロップするように設定したルール、および置換キーワードを使用するルールはパケットストリームに影響を与えません。ただし、これらのタイプのルールでは、トリガー時に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ます。

インライン展開されたデバイスでタップモードを使用することには、いくつかの利点があります。たとえば、デバイスがインラインであるかのようにデバイスとネットワークの間の配線をセットアップし、デバイスが生成するタイプの侵入イベント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廃棄ルールを追加できます。デバイス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、デバイスとネットワークの間の配線を再びセットアップすることなく、不審なトラフィックをドロップし始めることができます。

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

サポートされるデバイス:シリーズ 2、シリーズ 3

リンクステートの伝達は、インラインセットのペアの両方で状態を追跡できるよう、バイパスモードで設定されるインラインセットの機能です。リンクステート伝搬は、銅線および光ファイバの両方の設定可能なバイパスインターフェイスで使用できます。

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、アプライアンスはその変化を検知し、それ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、アプライアンスがリンク ステートの変更を伝達するのに最大 4 秒かかります。



(注)

リンクステート伝達がトリガーされると、シリーズ 2 デバイス (3D9900 を除く) でフェールオープンとして設定された光ファイバインラインセットは、ハードウェア バイパス モードをアクティブ化します。この場合、関連するインターフェイス カードのバイパスは自動的に終了しません。バイパス モードを手動で解除する必要があります。インラインセットの光ファイバ インターフェイスおよびハードウェア バイパスの詳細については、[フェールオープンに設定された光ファイバインラインセットでのバイパス モードの除去 \(5-12 ページ\)](#) を参照してください。

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。

クラスタ化されたデバイスで設定されたインラインセットのリンクステート伝達を無効にすることはできません。

なお、仮想デバイス、Blue Coat X-Series 向け Cisco NGIPS、および Cisco ASA with FirePOWER Services では、リンクステートの伝達はサポートされていません。

トランスペアレント インラインモード

トランスペアレント (透過的) インライン モード オプションを使用すると、デバイスは「Bump In The Wire」として機能できます。これは、送信元と宛先に関係なく、認識されるすべてのネットワークトラフィックをデバイスが転送することを意味します。シリーズ 3 および 3D9900 のデバイスではこのオプションを無効にできません。

厳密な TCP の適用

サポートされるデバイス: シリーズ 3

最大の TCP セキュリティを実現するには、厳密な適用 (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

なお、シリーズ 2、仮想デバイス、および Blue Coat X-Series 向け Cisco NGIPS では、このオプションはサポートされていません。また、同じインラインセットで、このオプションとタップモードを有効にすることはできません。

高度なインラインセット オプションを設定する方法:

アクセス: Admin/Network Admin

-
- 手順 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
[デバイス管理 (Device Management)] ページが表示されます。
 - 手順 2 インラインセットを編集するデバイスの横にある編集アイコン(✎)をクリックします。
[インターフェイス (Interfaces)] タブが表示されます。
 - 手順 3 [インラインセット (Inline Sets)] をクリックします。
[インラインセット (Inline Sets)] タブが表示されます。
 - 手順 4 編集するインラインセットの横にある編集アイコン(✎)をクリックします。
[インラインセットの編集 (Edit Inline Set)] ポップアップ ウィンドウが表示されます。
 - 手順 5 [詳細設定 (Advanced)] をクリックします。
[詳細設定 (Advanced)] タブが表示されます。
 - 手順 6 オプションで、シリーズ 3 および 3D9900 デバイスのインライン インターフェイスでタップモードを有効にするために [Tap Mode] を選択します。
なお、仮想デバイス、Blue Coat X-Series 向け Cisco NGIPS、およびシリーズ 2 デバイス (3D9900 を除く) では、このオプションはサポートされていません。さらに、同じインラインセットで、[タップモード (Tap Mode)] と [TCP の厳密な適用 (Strict TCP Enforcement)] を有効にすることはできません。
 - 手順 7 オプションで、シリーズ 2 またはシリーズ 3 デバイスで [リンク ステートの伝達 (Propagate Link State)] を選択します。停止したネットワーク デバイスを避けてトラフィックを再ルーティングする機能がネットワークのルータに備わっている場合、このオプションが特に便利です。
クラスタ化されたデバイスで設定されたインラインセットのリンク ステート伝達を無効にすることはできません。
なお、仮想デバイスおよび Blue Coat X-Series 向け Cisco NGIPS では、このオプションはサポートされていません。
 - 手順 8 オプションで、シリーズ 3 デバイスで TCP の厳密な適用を有効化するには、[TCP の厳密な適用 (Strict TCP Enforcement)] を選択します。
なお、シリーズ 2、仮想デバイス、および Blue Coat X-Series 向け Cisco NGIPS では、このオプションはサポートされていません。また、同じインラインセットで、[TCP の厳密な適用 (Strict TCP Enforcement)] と [タップモード (Tap Mode)] を有効にすることはできません。
 - 手順 9 オプションで、[トランスペアレント インライン モード (Transparent Inline Mode)] を選択します。
シリーズ 3 および 3D9900 のデバイスではこのオプションを無効にできません。
 - 手順 10 [OK] をクリックします。
変更が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください (詳しくは [デバイスへの変更の適用 \(4-27 ページ\)](#) を参照してください)。
-

フェール オープンに設定された光ファイバ インライン セットでのバイパス モードの除去

ライセンス:Protection

サポートされるデバイス:シリーズ 2(3D9900 を除く)

フェール オープンに設定された光ファイバ インライン セットを持つシリーズ 2 デバイスでリンク ステート伝達が有効になっている場合、そのデバイスがバイパス モードになると、すべてのネットワーク トラフィックは分析されずにインライン セットを通過します。リンクが復元した場合、フェール オープンに設定されているほとんどの光ファイバ インライン セットは、自動的にバイパスから戻りません。コマンドライン ツールを使用して、インライン セットのバイパス モードを強制的に解除できます。

このツールは、フェール オープンに設定された光ファイバ インライン インターフェイスを持つインライン セットに対して機能します。フェール オープンに設定された銅線インライン インターフェイスを持つインライン セットでこのツールを使用する必要はありません。



(注) デバイス上でフェール オープンに設定されたインライン セットに問題がある場合は、サポート担当に連絡してください。

デバイス上で、フェール オープンに設定された光ファイバ インライン セットのバイパス モードを強制的に解除する方法:

アクセス:Admin/Network Admin

-
- 手順 1 デバイスでターミナル ウィンドウを開き、管理者ユーザとしてサインインします。
- 手順 2 コマンドラインに次のように入力します。
- ```
sudo /var/sf/bin/unbypass_cards.sh
```
- パスワードを求めるプロンプトが表示されます。
- 手順 3 インターフェイスを切り替えてバイパス モードを解除すると、デバイスがトラフィックを分析していることを示すメッセージが `syslog` に表示されます。次に例を示します。
- ```
Fiber pair has been reset by un_bypass
```
-

インライン セットの削除


ライセンス:Protection

インライン セットを削除すると、そのセットに割り当てられたインライン インターフェイスを別のセットに含めることができるようになります。それらのインターフェイスは削除されません。

インライン セットを削除する方法:

アクセス:Admin/Network Admin

-
- 手順 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
[デバイス管理 (Device Management)] ページが表示されます。
- 手順 2 インライン セットを削除するデバイスの横にある編集アイコン(✎)をクリックします。
[インターフェイス (Interfaces)] タブが表示されます。

- 手順 3 [インラインセット (Inline Sets)] をクリックします。
[インラインセット (Inline Sets)] タブが表示されます。
- 手順 4 削除するインラインセットの横にある削除アイコン() をクリックします。
- 手順 5 プロンプトが表示されたら、インラインセットを削除することを確認します。
インラインセットが削除されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください(詳しくは [デバイスへの変更の適用\(4-27 ページ\)](#) を参照してください)。

Blue Coat X シリーズインターフェイス用の Cisco NGIPS の設定

ライセンス:Protection




サポートされるデバイス:X-シリーズ

Blue Coat X-Series 向け Cisco NGIPS パッケージを展開するとき、またはパッケージをインストールした後で、パッシブ インターフェイスまたはインライン インターフェイスを作成します。Blue Coat X-Series 向け Cisco NGIPS を 防御センター に追加する場合、これらのインターフェイスは設定済みです。Blue Coat X-Series 向け Cisco NGIPS は、高度な設定オプションをサポートしていません。

FireSIGHT システム Web インターフェイスを使用して、Blue Coat X-Series 向け Cisco NGIPS インターフェイスを再設定することはできません。再設定するには、まず 防御センター から現在のインターフェイスを削除した後、新しいインターフェイスを作成する必要があります。インターフェイスの作成と削除の詳細については、『*Blue Coat X-Series 向け Cisco NGIPS Installation Guide*』を参照してください。

Blue Coat X-Series 向け Cisco NGIPS でインターフェイスを設定する方法:

アクセス:Admin/Network Admin

- 手順 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
[デバイス管理 (Device Management)] ページが表示されます。
- 手順 2 設定するデバイスの横にある編集アイコン() をクリックします。
[インターフェイス (Interfaces)] タブが表示されます。すべての Blue Coat X-Series 向け Cisco NGIPS インターフェイスでリンクが常にアクティブ() と表示されることに注意してください。
- 手順 3 設定するインターフェイスの横にある編集アイコン() をクリックします。
- 手順 4 [セキュリティ ゾーン (Security Zone)] ドロップダウンリストから、既存のセキュリティ ゾーンを選択するか、または [新規 (New)] を選択して、新しいセキュリティ ゾーンを追加します。
- 手順 5 インライン インターフェイスの場合、オプションで、[インラインセット (Inline Set)] ドロップダウン リストから既存のインライン セットを選択するか、[新規 (New)] を選択して新しいインライン セットを追加します。

新しいインラインセットを追加した場合は、インライン インターフェイスのセットアップ後に、そのインラインセットを [デバイス管理 (Device Management)] ページ([デバイス (Devices)] > [デバイス管理 (Device Management)] > [インラインセット (Inline Set)]) で設定する必要があることに注意してください。詳細については、[インラインセットの追加\(5-7 ページ\)](#) を参照してください。

手順 6 [保存(Save)] をクリックします。

インターフェイスが設定されます。メニューバーの右上にある [変更を適用(Apply Changes)] をクリックしてデバイス設定を適用するまでは、変更内容が有効になりません。
