



IPS デバイスの展開と設定

以下のトピックでは、IPS 展開でデバイスを設定する方法について説明します。

- [IPS デバイスの展開と設定の概要 \(1 ページ\)](#)
- [パッシブ IPS 展開 \(1 ページ\)](#)
- [インライン IPS 展開 \(4 ページ\)](#)

IPS デバイスの展開と設定の概要

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。

パッシブ IPS 展開

パッシブ（受動）IPS 展開では、Firepower 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) アウトバウンド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アウトバウンド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。

Firepower システムのパッシブインターフェイス

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せん。

パッシブインターフェイスがトラフィックをモニタすることを可能にする場合、銅線インターフェイスでのみ使用可能なモードおよび MDI/MDIX 設定を指定します。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。

パッシブインターフェイスを無効にする場合、ユーザはセキュリティのためにアクセスできなくなります。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイスタイプによって異なる場合があります。



注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インспекションが一時的に中断されます。インспекションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によって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。詳細については、[Snort® の再起動によるトラフィックの動作](#)を参照してください。

関連トピック

[7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲](#)

[Snort® の再起動シナリオ](#)

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)
脅威	保護	機能に応じて異なる	リーフのみ	Admin/Network Admin

手順

ステップ 1 [Devices] > [Device Management] を選択します。

ステップ 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。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

- ステップ 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。
- ステップ 4** [パッシブ (Passive)] をクリックします。
- ステップ 5** セキュリティ ゾーンにパッシブ インターフェイスを関連付けるには、次のいずれかを実行します。
- [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 ゾーンを選択します。
 - [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。 [セキュリティ ゾーンおよびインターフェイス グループ オブジェクトの作成](#) を参照してください。
- ステップ 6** [有効 (Enabled)] チェックボックスをオンにします。
- 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。
- ステップ 7** 7000 & 8000 シリーズのみ : [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。
- モード設定は銅線インターフェイスにのみ使用できます。
- 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。
- ステップ 8** 7000 & 8000 シリーズのみ : [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) 、または自動 MDIX のいずれかを指定します。
- [MDI/MDIX] 設定は銅線インターフェイスでのみ使用できます。
- デフォルトでは、[MDI/MDIX] は [自動 MDIX (Auto-MDIX)] に設定され、MDI と MDIX の間の切り替えを自動的に処理してリンクを確立します。
- ステップ 9** [MTU] フィールドに最大伝送ユニット (MTU) を入力します。
- MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。
- 注意** デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インспекションが一時的に中断されます。インспекションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によって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。詳細については、[Snort® の再起動によるトラフィックの動作](#) を参照してください。
- ステップ 10** [保存 (Save)] をクリックします。

次のタスク

- 設定変更を展開します。[設定変更の展開](#)を参照してください。

インライン IPS 展開

インライン IPS 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 Firepower 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。

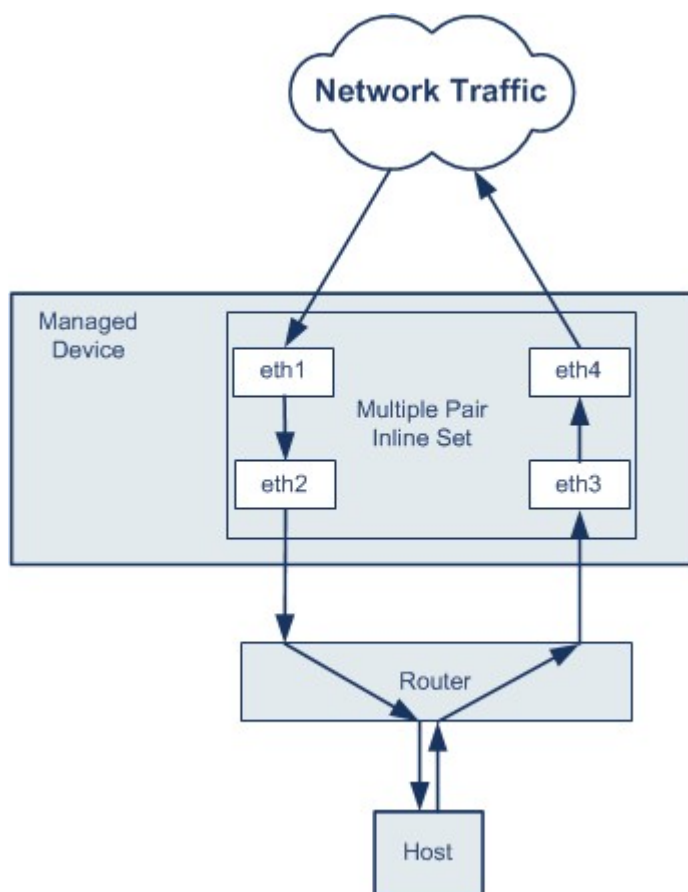


(注) システムがトラフィックに影響を与えるためには、ルーテッド、スイッチド、トランスペアレント インターフェイスまたはインライン インターフェイスのペアを使用して関連する設定を管理対象デバイスに展開する必要があります。

デバイス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 インターフェイス 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、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。

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。



371865



- (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、デバイス再起動後にパケットを転送するよう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の再起動中にシステムはトラフィックを通過させます。

関連トピック

[7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲](#)

[Snort® の再起動シナリオ](#)

Firepower システムのインライン インターフェイス

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。

(注)

- 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ます。
- 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。
- NGIPSv 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)
脅威	保護	機能に応じて異なる	リーフのみ	Admin/Network Admin

手順

-
- ステップ 1** [Devices] > [Device Management] を選択します。
- ステップ 2** 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。
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。
- ステップ 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。
- ステップ 4** [インライン (Inline)] をクリックします。
- ステップ 5** インライン インターフェイスをセキュリティゾーンと関連付ける場合は、次のいずれかを実行します。
- [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します。
 - [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。 [セキュリティゾーンおよびインターフェイス グループ オブジェクトの作成](#) を参照してください。

- ステップ 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、[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。
- (注) 新しいインラインセットを追加する場合は、インライン インターフェイスを設定した後、設定する必要があります。[インラインセットの追加 \(10 ページ\)](#) を参照してください。
- ステップ 7** [有効 (Enabled)] チェックボックスをオンにします。
- 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。
- ステップ 8** 7000 & 8000 シリーズのみ : [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。
- モード設定は銅線インターフェイスにのみ使用できます。
- 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。
- ステップ 9** 7000 & 8000 シリーズのみ : [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) 、または自動 MDIX のいずれかを指定します。
- [MDI/MDIX] 設定は銅線インターフェイスでのみ使用できます。
- デフォルトでは、[MDI/MDIX]は[自動 MDIX (Auto-MDIX)]に設定され、MDI と MDIX の間の切り替えを自動的に処理してリンクを確立します。
- ステップ 10** [保存 (Save)] をクリックします。

次のタスク

- 設定変更を展開します。[設定変更の展開](#)を参照してください。

Firepower システムのインラインセット

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。

[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。インラインセットの名前を入力する場合は、英数字とスペースを使用できます。



- (注) インラインセットのインターフェイスのセキュリティゾーンを追加する前に、インラインセットを作成します。作成していない場合、セキュリティゾーンは削除され、再度追加する必要があります。

[名前 (Name)]

インラインセットの名前。

インターフェイス

インラインセットに割り当てられているすべてのインラインペアのリスト。[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。

MTU

インラインセットの最大伝送ユニット。MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。



- 注意** デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インспекションが一時的に中断されます。インспекションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によって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。詳細については、[Snort® の再起動によるトラフィックの動作](#)を参照してください。

[フェールセーフ (Failsafe)]

Snort プロセスがビジー状態またはダウンしている場合の、7000 または 8000 シリーズ または NGIPSv デバイス上のインターフェイスの動作。

- [有効 (Enabled)] : Snort プロセスがビジー状態またはダウンしている場合、新規または既存のフローをインспекションなしで受け渡します。
- [無効 (Disabled)] : Snort プロセスがビジー状態の場合は、新規および既存のフローをドロップし、Snort プロセスがダウンしている場合はフローをインспекションなしで受け渡します。

トラフィックバッファが満杯の場合、Snortプロセスがビジー状態のことがあります。つまり、管理対象デバイスが処理可能な量を超えたトラフィックが存在するか、またはその他のソフトウェアに問題があることを示しています。

Snortプロセスを再起動する必要がある設定を展開すると、Snortプロセスはダウンします。詳細については、[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。



- (注) インスペクションを実行せずにトラフィックを受け渡す場合は、Snortプロセスに依存している機能は動作しません。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。

[バイパスモード (Bypass Mode)]

Firepower 7000 または 8000 シリーズのみ：インラインセットの設定済みバイパスモード。この設定により、インターフェイスに障害が発生した場合のインラインインターフェイスのリレーの応答方法が決まります。バイパスモードは、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します。非バイパスモードでは、トラフィックがブロックされます。



- 注意** 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。ハイアベイラビリティペアの7000または8000シリーズデバイスのインラインセット、8000シリーズデバイスの非バイパスNetMod、Firepower 7115または7125デバイスのSFPモジュールには、バイパスモードを設定できません。

関連トピック

[7000 および 8000 シリーズ デバイス および NGIPSv の MTU 範囲](#)
[Snort® の再起動シナリオ](#)

インラインセットの表示

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)
脅威	保護	任意 (Any)	任意 (Any)	Admin/Network Admin

手順

- ステップ 1** [Devices] > [Device Management] を選択します。
- ステップ 2** インラインセットを表示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。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

ステップ3 [インラインセット (Inline Sets)] タブをクリックします。

インラインセットの追加

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)
脅威	保護	機能に応じて異なる	リーフのみ	Admin/Network Admin

手順

ステップ1 [Devices] > [Device Management] を選択します。

ステップ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。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

ステップ3 [インラインセット (Inline Sets)] タブをクリックします。

ステップ4 [インラインセットの追加 (Add Inline Set)] をクリックします。

ステップ5 [名前 (Name)] を入力します。

ステップ6 [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。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。

ステップ7 [MTU] フィールドに最大伝送ユニット (MTU) を入力します。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイスタイプによって異なる場合があります。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インспекションが一時的に中断されます。インспекションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によって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。詳細については、[Snort® の再起動によるトラフィックの動作](#)を参照してください。

ステップ 8 Snort プロセスが取り込み中またはダウンしているときに検出をバイパスさせ、デバイスにトラフィックを通すには、[フェールセーフ (Failsafe)] を選択します。詳細については、[Firepower システムのインラインセット \(7 ページ\)](#) を参照してください。

内部トラフィックバッファがいっぱいになったが、特定の状況下でデバイスがまだパケットをドロップする可能性がある場合は、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、ドロップされたパケットのリスクが大幅に軽減されます。最悪の場合は、デバイスで一時的にネットワークが停止することがあります。

ステップ 9 7000 および 8000 シリーズ の場合のみ、バイパス モードを指定します:

- 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)] をクリックします。
- トラフィックをブロックするには、[バイパスしない (Non-Bypass)] をクリックします。

(注) 高可用性ペアの 7000 または 8000 シリーズ デバイスのインラインセット、NGIPSv デバイスのインラインセット、8000 シリーズ デバイスの非バイパス ネットワーク モジュール、Firepower 7115 または 7125 デバイスの SFP モジュールには、バイパスモードを設定できません。

ステップ 10 必要に応じて、詳細な設定を行います。[インラインセットの詳細オプション \(11 ページ\)](#) を参照してください。

ステップ 11 [OK] をクリックします。

次のタスク

- 設定変更を展開します。[設定変更の展開](#)を参照してください。

関連トピック

[7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲](#)
[Snort® の再起動シナリオ](#)

インラインセットの詳細オプション

インラインセットを設定する際に考慮できる詳細オプションがいくつかあります。

タップモード

7000 および 8000 シリーズデバイスでは、インライン（またはフェールオープン可能なインライン）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ので、パケットを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及ぼしません。ただし、これらのタイプのルールでは、トリガーされた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、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間の配線をセットアップし、デバイス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。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。

ただし、同じインラインセットに対してこのオプションと厳格な TCP 強制を有効にすることはできません。

リンクステートの伝達 (Propagate Link State)



- (注) リンクステートの伝達は、バーチャルデバイスではサポートされていません。リンクステートの伝達は 7000 および 8000 シリーズデバイスのみでサポートされています。

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、バイパスモードと非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。リンクステートの伝達は、銅線と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。

リンクステートの伝達は、ルータが障害状態のネットワークデバイスを避け、トラフィックを自動的に再ルーティングするよう設定された、復元力の高いネットワーク環境では特に有効です。

高可用性ペアの 7000 および 8000 シリーズ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の伝達を無効にすることはできません。

トランスペアレント インライン モード (Transparent Inline Mode)

[トランスペアレントインラインモード (Transparent Inline Mode)] オプションを使用すると、デバイスを「Bump In The Wire」として機能させることができます。つまり、デバイスは、送信元と宛先に関係なく、認識するすべてのネットワークトラフィックを転送するということができます。7000 および 8000 シリーズ 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



(注) 厳密な TCP 適用は、バーチャルデバイスではサポートされていません。7000 および 8000 シリーズ デバイスでのみ、このオプションを使用できます。また、同じインラインセットに対して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。

最大限の TCP セキュリティを実現するため、厳格な強制を有効にすることができます。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
- 応答側が SYN-ACK を送信する前に TCP 接続の発信側から送信された非 SYN/RST パケット
- SYN の後、セッションの確立前に TCP 接続のレスポンドから送信された非 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

高度なインラインセットオプションの設定

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)
脅威	保護	機能に応じて異なる	リーフのみ	Admin/Network Admin

手順

ステップ 1 [Devices] > [Device Management] を選択します。

ステップ 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。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [インラインセット (Inline Sets)] タブをクリックします。

ステップ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。

ステップ5 [Advanced] タブをクリックします。

ステップ6 [インラインセットの詳細オプション \(11 ページ\)](#) の説明に従ってオプションを設定します。

(注) リンク ステートの伝達と厳密な TCP 適用は、仮想デバイスではサポートされていません。

ステップ7 [OK] をクリックします。

次のタスク

- 設定変更を展開します。[設定変更の展開](#)を参照してください。

インラインセットの削除

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)
脅威	保護	任意 (Any)	リーフのみ	Admin/Network Admin

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ますようになります。それらのインターフェイスは削除されません。

手順

ステップ1 [Devices] > [Device Management] を選択します。

ステップ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。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

ステップ3 [インラインセット (Inline Sets)] タブをクリックします。

ステップ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。

ステップ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。

次のタスク

- 設定変更を展開します。[設定変更の展開](#)を参照してください。