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

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） 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す。

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 インスペクションが一時的に中断されます。インスペクションは、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、それ以上インスペク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（Threat）	Protection	機能に応じて異なる	リーフのみ	Admin/Network Admin

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（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（Auto Negotiation）] 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 インスペクションが一時的に中断されます。インスペクションは、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、それ以上インスペク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

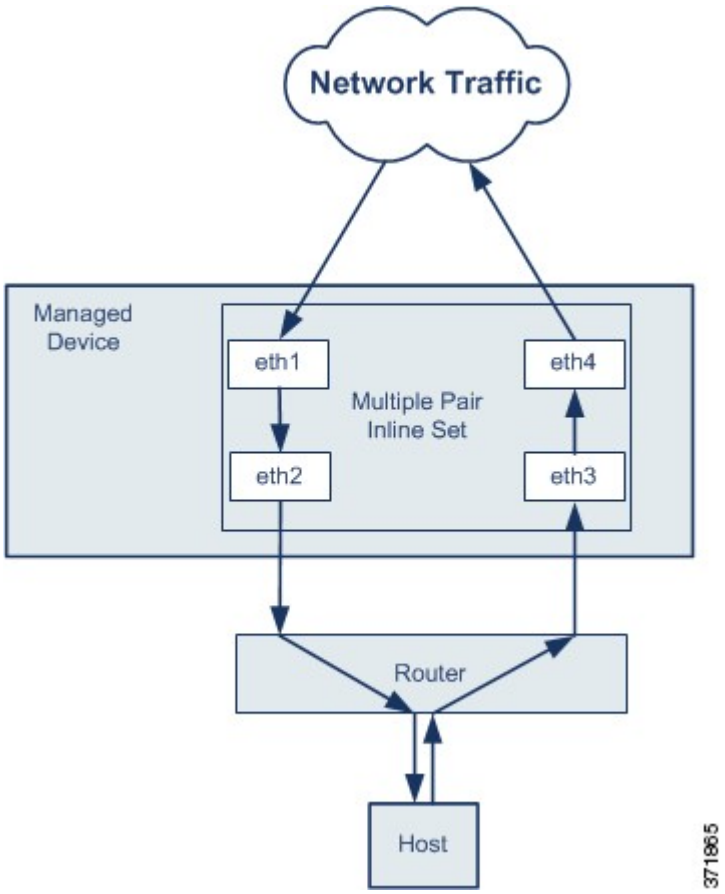
インライン IPS 展開では、2 つのポートを一緒にバインドすることで、ネットワーク セグメント上で Firepower システムを透過的に設定します。これによって、隣接するネットワーク デバイスの設定がなくても、任意のネットワーク環境にシステムをインストールできます。インライン インターフェイスはすべてのトラフィックを無条件に受信しますが、これらのインターフェイスで受信されたすべてのトラフィックは、明示的にドロップされない限り、インラインセットの外部に再送信されます。

（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。



（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 セットでパイパス 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。

（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（Threat）	Protection	機能に応じて異なる	リーフのみ	Admin/Network Admin

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（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（Auto Negotiation）]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 インスペクションが一時的に中断されます。インスペクションは、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、それ以上インスペク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スペク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スペク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 モードは、トラフィックをブロックします。

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。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 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（Threat）	Protection	任意（Any）	任意（Any）	Admin/Network Admin

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（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（Threat）	Protection	機能に応じて異なる	リーフのみ	Admin/Network Admin

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（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 インスペクションが一時的に中断されます。インスペクションは、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、それ以上インスペク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、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。

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。

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ることに注意してください。

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です。7000 および 8000 シリーズ のデバイスではこのオプションを無効にできないことに注意してください。

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。

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
- 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
- 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

なお、このオプションは、7000 および 8000 シリーズ デバイスでのみ使用できます。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。

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（Threat）	Protection	機能に応じて異なる	リーフのみ	Admin/Network Admin

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（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（Threat）	Protection	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。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（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。