



## IPS デバイスインターフェイスの管理

Cisco IOS IPS デバイスは通常のルータ インターフェイス ポリシーを使用して設定しますが、専用 IPS アプライアンスおよびサービス モジュールには、独自のインターフェイス設定があります。この章では、専用 IPS アプライアンスおよびサービス モジュール独自のインターフェイスを設定する方法について説明します。

この章は次のトピックで構成されています。

- [インターフェイスについて \(1 ページ\)](#)
- [インターフェイス モードについて \(3 ページ\)](#)
- [インターフェイスの設定 \(7 ページ\)](#)

## インターフェイスについて



**ヒント** この項では、IPS インターフェイスの概要について説明します。アプライアンスおよびサービス モジュールの各タイプに関する特定のインターフェイスの名前と位置、サポートされているロール、設定上の制限、ハードウェアに関する考慮事項など、詳細な説明については、Cisco.com で、ご使用の IPS ソフトウェアバージョンの『[Installing and Using Cisco Intrusion Prevention System Device Manager](#)』の「Configuring Interfaces」の章を参照してください。この情報は、IME ガイドおよび CLI ガイドでも提供されています。全般情報については、<http://www.cisco.com/go/ips> を参照してください。

センサーのインターフェイスは、インターフェイスの最大速度および物理的な場所に従って名前が付けられています。たとえば、GigabitEthernet2/1 は、1 ギガビットの最大速度をサポートし、下から 2 番目の拡張スロットの右から 2 番目のインターフェイスです。

インターフェイスには、次の 3 つの役割があります。

- **コマンド/コントロール**：コマンド/コントロール インターフェイスは、IP アドレスを持ち、センサーの設定に使用されます。このインターフェイスは、センサーからセキュリティ イベントとステータス イベントを受信し、センサーに統計情報を問い合わせます。

コマンド/制御インターフェイスは、常にイネーブルです。このインターフェイスは特定の物理インターフェイス（センサーのモデルによって異なる）に常時マッピングされています。コマンド/制御インターフェイスを検知インターフェイスや代替 TCP リセット インターフェイスとして使用することはできません。デバイス タイプ別のコマンド/コントロール インターフェイスのリストについては、上記の IPS マニュアルを参照してください。

- **検知**：検知インターフェイスは、セキュリティ違反に関してトラフィックを分析するために、センサーによって使用されます。センサーには、1つ以上の検知インターフェイスがあり、その数はセンサーによって異なります。検知インターフェイスは、無差別モードで個別に動作させるか、またはペアにしてインラインインターフェイスを作成できます。無差別モードでは、パケットはセンサーを通過しません。センサーは、モニタ対象トラフィックのコピーを分析します。インラインモードでは、IPS はトラフィック フローに挿入され、トラフィックに直接影響を与えます。検知モードの詳細については、[インターフェイスモードについて（3 ページ）](#)を参照してください。



(注) アプライアンスでは、すべての検知インターフェイスがデフォルトでディセーブルになっています。これらのインターフェイスを使用するには、イネーブルにする必要があります。モジュールでは、検知インターフェイスは常にイネーブルです。デバイス タイプ別の検知インターフェイスのリストについては、上記の IPS マニュアルを参照してください。

- **代替 TCP リセット**：攻撃者のホストと攻撃のターゲットホストとの間のネットワーク接続をリセットするために、TCP リセットパケットを送信するようにセンサーを設定できます。一部のインストールでは、インターフェイスが無差別モードで動作している場合、攻撃が検出された検知インターフェイスと同じインターフェイスでセンサーが TCP リセットパケットを送信できないことがあります。このような場合は、検知インターフェイスを代替 TCP リセット インターフェイスに関連付けることができます。これにより、無差別モードで動作している場合に通常は検知インターフェイスで送信されるすべての TCP リセットを、関連付けた代替 TCP リセット インターフェイスで送信できます。

検知インターフェイスが代替 TCP リセット インターフェイスに関連付けられている場合、その関連付けは、センサーが無差別モードに設定されている場合は適用されますが、検知インターフェイスがインラインモード（インターフェイスまたは VLAN ペア）に設定されている場合は無視されます。TCP リセットは、これらのモードの検知インターフェイスで常に送信されるためです。



(注) IDSM-2 を除いて、すべての検知インターフェイスは、別の検知インターフェイスの代替 TCP リセット インターフェイスとなることができます。IDSM-2 の代替 TCP リセット インターフェイスは、ハードウェアの制限があるために固定されています。ただし、（ルータまたは ASA デバイス上の）IPS モジュールに存在する検知インターフェイスは1つだけであるため、IPS モジュールでは代替 TCP リセット インターフェイスを指定できません。デバイス タイプ別の適切な代替 TCP リセット インターフェイスのリスト、および代替 TCP リセット インターフェイスを使用する状況の詳細については、上記の IPS マニュアルを参照してください。

# インターフェイス モードについて

検知インターフェイスは、さまざまなモードで動作できます。インターフェイスに設定されたモードによって、検査できるトラフィックおよびイベントへの応答方法が決まります。

ここでは、次の内容について説明します。

- [無差別モード \(3 ページ\)](#)
- [インライン インターフェイス モード \(3 ページ\)](#)
- [インライン VLAN ペア モード \(4 ページ\)](#)
- [VLAN グループ モード \(5 ページ\)](#)

## 無差別モード

無差別モードでは、パケットはセンサーを通過しません。センサーは、実際に転送されるパケットではなく、モニタ対象のトラフィックのコピーを分析します。無差別モードで運用する利点は、転送されるトラフィックでパケットのフローにセンサーが影響を与えないことです。ただし、無差別モードで運用するときは、アトミック アタック (シングル パケット 攻撃) などの特定のタイプの攻撃の場合に、悪意のあるトラフィックがターゲットに到達することをセンサーで阻止できないという短所があります。無差別モードのセンサーデバイスによって実行される応答アクションはイベント後の応答であるため、多くの場合、攻撃に対応するために、ルータやファイアウォールなど、他のネットワークングデバイスによるサポートが必要となります。このような応答アクションは一部の攻撃を防ぐことはできますが、アトミックアタックでは、無差別モードベースのセンサーが管理対象デバイス (ファイアウォール、スイッチ、ルータなど) に ACL 修正を適用する前に、シングルパケットがターゲットシステムに到達する可能性があります。

デフォルトでは、すべての検知インターフェイスは無差別モードです。インターフェイスをインラインインターフェイスモードから無差別モードに変更するには、変更対象のインターフェイスを含むすべてのインラインインターフェイスを削除し、インターフェイス設定からそのインターフェイスのすべてのインライン VLAN ペアのサブインターフェイスを削除します。

### 関連項目

- [インターフェイスについて \(1 ページ\)](#)
- [物理インターフェイスの設定 \(13 ページ\)](#)

## インライン インターフェイス モード

インライン インターフェイス ペア モードで運用する場合は、IPS が直接トラフィック フローに挿入され、パケット転送速度に影響を与えます。遅延が加わるため、パケット転送速度は遅くなります。その結果、センサーは、悪意のあるトラフィックがターゲットに到達する前にそ

のトラフィックをドロップして攻撃を阻止できるため、保護サービスが提供されます。インラインデバイスは、レイヤ3および4で情報を処理するだけでなく、より高度な埋め込み型攻撃の packets の内容およびペイロードも分析します（レイヤ3～7）。この詳細な分析では、通常は従来のファイアウォールデバイスを通る攻撃をシステムが識別し、停止またはブロックすることができます。

インラインインターフェイスペアモードでは、パケットはセンサーのペアの1つめのインターフェイスを経由して入り、ペアの2つめのインターフェイスを経由して出ます。パケットは、シグニチャによって拒否または変更されないかぎり、ペアの2つめのインターフェイスに送信されます。

#### (注)

- ペアになっているインターフェイスが同じスイッチに接続されている場合は、それらのインターフェイスをスイッチ上で2つのアクセスポートとして設定し、それぞれが異なる VLAN アクセスを持つようにする必要があります。このようにしないと、トラフィックはインラインインターフェイスを通りません。
- ルータおよび ASA デバイスの IPS モジュールは、検知インターフェイスが1つしかない場合でも、インラインで動作するように設定できます。

#### 関連項目

- [インターフェイスについて \(1 ページ\)](#)
- [インラインインターフェイス ペアの設定 \(18 ページ\)](#)

## インライン VLAN ペア モード

物理インターフェイス上で、VLAN をペアに関連付けることができます。これは、インライン VLAN ペア モードと呼ばれます。ペアの一方の VLAN で受信されたパケットは、分析後にペアのもう一方の VLAN に転送されます。

インライン VLAN ペアモードは、アクティブ検知モードです。このモードでは、検知インターフェイスが 802.1q トランク ポートとして動作し、センサーがトランク上の VLAN のペア間の VLAN ブリッジングを実行します。センサーは、ペアごとに各 VLAN 上で受信するトラフィックを検査し、そのパケットをペアのもう一方の VLAN に転送するか、または侵入の試行が検出された場合はそのパケットをドロップできます。IPS センサーは、各検知インターフェイス上で最大 255 個の VLAN ペアを同時にブリッジするように設定できます。センサーは、受信した各パケットの 802.1q ヘッダー内の VLAN ID フィールドを、センサーがパケットを転送する出力 VLAN の ID に置き換えます。センサーは、インライン VLAN ペアに割り当てられていないすべての VLAN で受信したすべてのパケットをドロップします。

#### (注)

- インライン VLAN ペアでペアになっている VLAN のいずれかとして、デフォルト VLAN を使用することはできません。

- インライン VLAN ペアは、ルータまたは ASA デバイスの IPS モジュールではサポートされていません。

#### 関連項目

- [インターフェイスについて \(1 ページ\)](#)
- [インライン VLAN ペアの設定 \(19 ページ\)](#)

## VLAN グループ モード

各物理インターフェイスまたはインラインインターフェイスは、VLAN グループサブインターフェイスに分けることができます。各サブインターフェイスは、そのインターフェイスの VLAN のグループで構成されます。複数の仮想センサーを設定している場合、各仮想センサーは、これらのインターフェイスの1つまたは複数を実験できます。これにより、複数のポリシーを同じセンサーに適用できます。この利点は、わずかなインターフェイスしかないセンサーを多くのインターフェイスがあるかのように使用できる点にあります。



- (注) インライン VLAN ペアに含まれている物理インターフェイスは、VLAN グループに分けることはできません。

VLAN グループサブインターフェイスによって、物理インターフェイスまたはインラインインターフェイスと VLAN セットが関連付けられます。VLAN を複数の VLAN グループサブインターフェイスのメンバにすることはできません。各 VLAN グループサブインターフェイスは、1 ~ 255 の数値で識別されます。サブインターフェイス 0 は、仮想化されていない物理インターフェイスまたは論理インターフェイス全体を表すために使用される予約済みのサブインターフェイス番号です。サブインターフェイス 0 を作成、削除、または変更することはできません。また、サブインターフェイス 0 に関する統計情報は報告されません。

VLAN グループを作成すると、次のように無差別またはインラインに設定されます。

- 無差別 VLAN グループ：物理インターフェイスで VLAN グループを設定する場合、その VLAN グループは、[無差別モード \(3 ページ\)](#) で説明しているように無差別になります。
- インライン VLAN グループ：インライン インターフェイス ペア（論理インターフェイス）で VLAN グループを設定する場合、VLAN グループは、[インライン インターフェイスモード \(3 ページ\)](#) で説明しているようにインラインになります。

したがって、VLAN グループは、選択した VLAN にインターフェイスの動作を制限することにより、無差別モード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動作を強化します。VLAN グループを物理インターフェイスまたはインライン インターフェイスに割り当てると、そのインターフェイスは単なる無差別またはインライン インターフェイス ペアではなく、インライン VLAN グループに対してだけ使用できるようになります。

未割り当て VLAN グループは、別の VLAN グループに明示的に割り当てられていないすべての VLAN を含んでいる状態で維持されます。未割り当て VLAN グループ内の VLAN を直接指定することはできません。別の VLAN グループ サブインターフェイスに VLAN が追加されたり、または別の VLAN グループ サブインターフェイスから VLAN が削除されたりすると、未割り当て VLAN グループは更新されます。

通常、802.1q トランクのネイティブ VLAN 内のパケットには、そのパケットが属する VLAN 番号を示す 802.1q カプセル化ヘッダーがありません。各物理インターフェイスには、デフォルトの VLAN 変数が関連付けられており、この変数をネイティブ VLAN の VLAN 番号または 0 に設定する必要があります。値 0 は、ネイティブ VLAN が不明であるか、またはネイティブ VLAN の指定の有無は関係ないことを示しています。デフォルトの VLAN 設定が 0 の場合は、次の処理が行われます。

- 802.1q カプセル化のないパケットによってトリガーされたアラートには、VLAN 値 0 が報告されます。
- 802.1q カプセル化のないトラフィックは未割り当て VLAN グループに関連付けられ、ネイティブ VLAN として他の VLAN グループに割り当てることができません。



(注) スイッチのポートは、アクセスポートまたはトランクポートとして設定できます。アクセスポートでは、すべてのトラフィックは、アクセス VLAN と呼ばれる 1 つの VLAN 内にあります。トランクポートでは、ポートで複数の VLAN を伝送することができ、各パケットには VLAN ID を含む 802.1q ヘッダーと呼ばれる特別なヘッダーが付加されます。このヘッダーは、一般に VLAN タグと呼ばれます。ただし、トランクポートには、ネイティブ VLAN と呼ばれる特別な VLAN があります。ネイティブ VLAN 内のパケットには、802.1q ヘッダーは付加されていません。IDS M-2 は、ネイティブでないすべてのトラフィックの 802.1q ヘッダーを読み取り、そのパケットの VLAN ID を判断することができます。ただし、IDS M-2 は、スイッチ設定内のポートのネイティブ VLAN としてどの VLAN が設定されているかは把握していないため、ネイティブパケットを受信する VLAN も認識できません。したがって、どの VLAN が該当のポートのネイティブ VLAN であるかを IDS M-2 に通知する必要があります。IDS M-2 は、タグが付いていないパケットを、ネイティブ VLAN ID のタグが付いたパケットとして処理します。

#### 関連項目

- [VLAN グループの展開 \(6 ページ\)](#)
- [インターフェイスについて \(1 ページ\)](#)
- [VLAN グループの設定 \(21 ページ\)](#)

## VLAN グループの展開

インラインペアの VLAN グループは、VLAN ID を変換しません。したがって、論理インターフェイスで VLAN グループを使用するには、2 つのスイッチ間にインラインペアインターフェイスが存在する必要があります。アプライアンスの場合、2 つのペアを同じスイッチに接続し、



それらをアクセスポートにして、2つのポートに対して別々にアクセス VLAN を設定できます。この設定では、センサーは2つの VLAN 間を接続します。これは、2つのポートはそれぞれアクセスモードであり、1つの VLAN だけを伝送するためです。この場合、2つのポートは異なる VLAN に存在する必要があります。センサーはこれら2つの VLAN をブリッジし、2つの VLAN 間を流れるすべてのトラフィックをモニタします。IDS/IPS-2 の2つのデータポートは常に同じスイッチに接続されているため、IDS/IPS-2 はこの方法でも動作します。

2つのスイッチ間にアプライアンスを接続することもできます。2つの方法があります。第1の方法では、2つのポートがアクセスポートとして設定されるため、1つの VLAN を伝送できます。この方法では、センサーは2つのスイッチ間で1つの VLAN をブリッジします。

第2の方法では、2つのポートはトランクポートとして設定されるため、複数の VLAN を伝送できます。この設定では、センサーは2つのスイッチ間で複数の VLAN をブリッジします。複数の VLAN がインラインインターフェイスペアで伝送されるため、VLAN をグループに分けることができ、各グループを仮想センサーに割り当てることができます。第2の方法は、IDS/IPS-2 には適用されません。IDS/IPS-2 はこの方法では接続できないためです。

#### 関連項目

- [インターフェイスについて \(1 ページ\)](#)
- [VLAN グループモード \(5 ページ\)](#)
- [VLAN グループの設定 \(21 ページ\)](#)

## インターフェイスの設定

IPS アプライアンスおよびサービスモジュールのインターフェイスポリシーを使用して、デバイスのインターフェイス設定値を設定します。ここでは、さまざまなタイプの設定値を設定する方法について説明します。これらの項は、標準のルータ インターフェイス ポリシーを使用する Cisco IOS IPS デバイスには該当しません。

- [IPS インターフェイス ポリシーについて \(8 ページ\)](#)
- [物理インターフェイスの設定 \(13 ページ\)](#)
- [バイパスモードの設定 \(16 ページ\)](#)
- [CDP モードの設定 \(17 ページ\)](#)
- [インライン インターフェイス ペアの設定 \(18 ページ\)](#)
- [インライン VLAN ペアの設定 \(19 ページ\)](#)
- [VLAN グループの設定 \(21 ページ\)](#)
- [IPS インターフェイス設定のサマリーの表示 \(11 ページ\)](#)

## IPS インターフェイス ポリシーについて

IPS インターフェイス ポリシーを使用して、IPS アプライアンスおよびサービス モジュールで、物理インターフェイス、インライン ペア、VLAN ペア、および VLAN グループを設定できます。このポリシーは、Cisco IOS IPS デバイスには適用されません。

無差別モード、インラインペアモード、インラインVLAN ペアモード、無差別VLAN グループ、またはインラインVLAN グループで動作するように、単一の物理インターフェイスを設定できますが、これらのモードを組み合わせるとインターフェイスを設定することはできません。



**ヒント** ポリシーの内容は、デバイスタイプおよびIPS ソフトウェアバージョンによって異なります。たとえば、一部のデバイスには、物理インターフェイスのタブだけが表示されるため、別のタイプの設定を作成することはできません。次に説明するタブまたはオプションが、設定するポリシーで表示されない場合、そのデバイスには適用されません。

### ナビゲーションパス

(デバイスビューのみ) ポリシーセレクタから [IPS]>[インターフェイス (Interfaces)] を選択します。

### 関連項目

- [インターフェイスについて \(1 ページ\)](#)
- [インターフェイス モードについて \(3 ページ\)](#)
- [Security Manager にすでに存在するデバイス上のポリシーの検出](#)



## フィールドリファレンス

表 1:IPS インターフェイス ポリシー

要素	説明
[Physical Interfaces] タブ	<p>デバイスで使用可能な物理インターフェイス。デバイスで使用可能なインターフェイスのみ編集できます（デバイスを選択し、[行の編集（Edit Row）] ボタンをクリックします）。デバイス上でインベントリ検出を実行して、物理インターフェイスの正しいリストを取得する必要があります（インターフェイスカードをデバイスに追加する場合など）。</p> <p>このタブに表示されるカラムは、各インターフェイスの設定を示し、<a href="#">[Modify Physical Interface Map] ダイアログボックス（14 ページ）</a> で説明されています。<a href="#">[Administrative State]</a> カラムは、インターフェイスがイネーブルであるかどうか（[Yes] または [No]）を示していることに注意してください。インターフェイスを動作させるには、インターフェイスをイネーブルにする必要があります。</p> <p>詳細については、<a href="#">物理インターフェイスの設定（13 ページ）</a> を参照してください。</p>
[Inline Pairs] タブ	<p><a href="#">インラインインターフェイスモード（3 ページ）</a> で説明しているように、インラインモード処理を可能にするインラインインターフェイスペア。この表には、ペアの名前、それぞれのインターフェイス、および説明（ある場合）が示されます。詳細については、<a href="#">インラインインターフェイスペアの設定（18 ページ）</a> を参照してください。</p> <ul style="list-style-type: none"> <li>• ペアを追加するには、[行の追加（Add Row）] ボタンをクリックし、[インターフェイスペアの追加（Add Interface Pair）] ダイアログボックスに入力します。</li> <li>• ペアを編集するには、ペアを選択して [行の編集（Edit Row）] ボタンをクリックします。</li> <li>• ペアを削除するには、そのペアを選択して [行の削除（Delete Row）] ボタンをクリックします。</li> </ul>

要素	説明
[VLAN Pairs] タブ	<p>インライン VLAN ペア モード (4 ページ) で説明しているように、各物理インターフェイスの VLAN ペア。この表には、インターフェイスおよびサブインターフェイス、ペアになっている 2 つの VLAN、および説明 (ある場合) を示します。詳細については、<a href="#">インライン VLAN ペアの設定 (19 ページ)</a> を参照してください。</p> <ul style="list-style-type: none"> <li>ペアを追加するには、[行の追加 (Add Row) ] ボタンをクリックし、[VLAN ペアの追加 (Add VLAN Pair) ] ダイアログボックスに入力します。</li> <li>ペアを編集するには、ペアを選択して [行の編集 (Edit Row) ] ボタンをクリックします。</li> <li>ペアを削除するには、そのペアを選択して [行の削除 (Delete Row) ] ボタンをクリックします。</li> </ul>
[VLAN Groups] タブ	<p>VLAN グループ モード (5 ページ) で説明しているように、物理インターフェイスまたはインライン ペアに定義されている VLAN グループ。この表には、インターフェイスまたはペアの名前、VLAN グループ (空白の場合は、未割り当てのすべての VLAN を意味します) 、および説明 (ある場合) を示します。詳細については、<a href="#">VLAN グループの設定 (21 ページ)</a> を参照してください。</p> <ul style="list-style-type: none"> <li>グループを追加するには、[行の追加 (Add Row) ] ボタンをクリックし、[VLAN グループの追加 (Add VLAN Group) ] ダイアログボックスに入力します。</li> <li>グループを編集するには、グループを選択し、[行の編集 (Edit Row) ] ボタンをクリックします。</li> <li>グループを削除するには、グループを選択し、[行の削除 (Delete Row) ] ボタンをクリックします。</li> </ul>
[サマリー (Summary) ] タブ	<p>検知インターフェイスをどのように設定したか (無差別モードに設定したインターフェイス、インラインペアとして設定したインターフェイス、およびインライン VLAN ペアとして設定したインターフェイス) のサマリー。</p> <p>詳細については、<a href="#">IPS インターフェイス設定のサマリーの表示 (11 ページ)</a> を参照してください。</p>

要素	説明
[バイパスモード (Bypass Mode) ]	<p>デバイスのバイパスモード。このモードによって、センサー プロセスがアップグレードのために一時的に停止した場合や、センサー モニタリング プロセスが失敗した場合に、センサーがインライン モード トラフィックを処理する方法が決定されます。これは、デバイス上のすべてのインラインモードに適用されるグローバル設定です。必要なオプションを選択します。各オプションがインライン トラフィックに与える影響の詳細については、 <a href="#">バイパスモードの設定 (16 ページ)</a> を参照してください。</p> <ul style="list-style-type: none"> <li>• [オフ (インライントラフィックを常に検査する) (Off(Always inspect inline traffic)) ]: バイパスモードを無効にします。トラフィックは常に検査され、センサーのモニタリングプロセスがダウンした場合は、トラフィックが通過しなくなります。</li> <li>• [オン (インライントラフィックを検査しない) (On (Never inspect inline traffic)) ]: トラフィックは、分析エンジンをバイパスし、検査されません。</li> <li>• [自動 (分析エンジンが停止している場合は検査をバイパスする) (Auto (Bypass inspection when analysis engine is stopped)) ]: センサーのモニタリングプロセスがダウンしている場合を除き、トラフィックは検査されます。モニタリングプロセスがダウンした場合、トラフィックは検査されずにセンサーを通過し続けます。これがデフォルトです。Auto モードは、センサーのアップグレード時に役立ちます。センサーのアップグレード中でもトラフィック フローが確保されるからです。</li> </ul>
CDP Mode	<p>Cisco Discovery Protocol (CDP) パケットの処理方法。CDP 設定は、デバイス上のすべてのインターフェイスにグローバルに適用されます。ただし、効果があるのはインライン インターフェイス (インライン インターフェイスとインライン VLAN ペア) だけです。詳細については、 <a href="#">CDP モードの設定 (17 ページ)</a> を参照してください。次のうち、適切なオプションを選択します。</p> <ul style="list-style-type: none"> <li>• [CDPパケットを転送 (Forward CDP packets) ]: CDP パケットがセンサーを通過できるようにします。</li> <li>• [CDPパケットをドロップ (Drop CDP packets) ]: センサーにすべての CDP パケットをドロップさせ、センサーを通過できないようにします。これがデフォルト設定です。</li> </ul>

## IPS インターフェイス設定のサマリーの表示

インターフェイス ポリシーの [Summary] タブには、検知インターフェイスを設定した方法 (無差別モードに設定したインターフェイス、インラインペアとして設定したインターフェイス、インライン VLAN ペアとして設定したインターフェイス、インライン VLAN グループ、およ

び無差別 VLAN グループ) のサマリーが含まれています。この表の内容は、インターフェイス設定を変更すると、変わります。

無差別モード、インラインペアモード、またはインライン VLAN ペアモードで動作するように、単一の物理インターフェイスを設定できますが、これらのモードを組み合わせでインターフェイスを設定することはできません。



**ヒント** すべてのサービス モジュールにサマリーのタブがあるわけではありません。

### ナビゲーションパス

(デバイスビュー) ポリシーセクタから [インターフェイス (Interface) ] を選択します。[サマリー (Summary) ] タブをクリックします。

### 関連項目

- [インターフェイスについて \(1 ページ\)](#)
- [IPS インターフェイス ポリシーについて \(8 ページ\)](#)
- [物理インターフェイスの設定 \(13 ページ\)](#)
- [バイパス モードの設定 \(16 ページ\)](#)
- [CDP モードの設定 \(17 ページ\)](#)
- [インライン インターフェイス ペアの設定 \(18 ページ\)](#)
- [インライン VLAN ペアの設定 \(19 ページ\)](#)
- [VLAN グループの設定 \(21 ページ\)](#)

### フィールド リファレンス

表 2: [IPS Interface Summary] タブ

要素	説明
名前	インターフェイスの名前。 この名前は、無差別インターフェイスの FastEthernet または GigabitEthernet です。インラインインターフェイスの場合、この名前はペアに割り当てた名前になります。
Subinterface Number	インライン VLAN ペアまたは VLAN グループのサブインターフェイス番号です。1 ~ 255 のサブインターフェイス番号を指定できます。
Inline Interface Name	インライン インターフェイス ペアの名前。

要素	説明
[モード (Mode) ]	インターフェイスのモード：無差別、インライン、無差別 VLAN グループ、またはインライン VLAN グループおよび VLAN ペアが存在するかどうか。インターフェイスモードの詳細については、 <a href="#">インターフェイスモードについて (3 ページ)</a> を参照してください。
VLAN A VLAN B	VLAN ペアの 1 番目の VLAN および 2 番目の VLAN の VLAN ID。1 ～ 4095 の VLAN 番号を指定できます。
VLAN の範囲	VLAN グループに属している VLAN ID の範囲 (100 ～ 200 など)。  未割り当てのすべての VLAN に適用するように VLAN グループが設定されている場合、このフィールドは空になります。

## 物理インターフェイスの設定

IPS インターフェイス ポリシーの [Physical Interfaces] タブには、使用しているセンサー上の既存の物理インターフェイスおよび関連付けられている設定が表示されます。このポリシーの物理インターフェイスは追加または削除できません。代わりに、ポリシー検出を使用して、デバイスからインターフェイスの最新リストを取得する必要があります。したがって、(一部のアプリケーションで使用可能な) インターフェイス カードを追加または削除した場合、[Security Manager にすでに存在するデバイス上のポリシーの検出](#)で説明しているように、デバイスを再検出する必要があります。

トラフィックをモニタするようにセンサーを設定するには、この手順を使用してインターフェイスをイネーブルにする必要があります。**setup** コマンドを使用して (IPS でコマンドラインインターフェイスを使用して) センサーを初期化したときに、インターフェイスまたはインラインペアを仮想センサーに割り当て、インターフェイスまたはインラインペアをイネーブルにしています。インターフェイス設定を変更する必要がある場合は、[Physical Interfaces] タブで変更できます。インターフェイスを仮想センサーに割り当てるには、[Virtual Sensors] ポリシーを選択し、必要に応じて仮想センサーを追加または編集します。



**ヒント** 各物理インターフェイスは、VLAN グループサブインターフェイスに分けることができます。各サブインターフェイスは、そのインターフェイスの VLAN のグループで構成されます。詳細については、[VLAN グループの設定 \(21 ページ\)](#) を参照してください。

### 関連項目

- [インターフェイスについて \(1 ページ\)](#)
- [仮想センサーの定義](#)
- [仮想センサーのポリシーの編集](#)
- [仮想センサーへのインターフェイスの割り当て](#)

**[Modify Physical Interface Map] ダイアログボックス**

- [バイパス モードの設定 \(16 ページ\)](#)
- [CDP モードの設定 \(17 ページ\)](#)
- [インライン インターフェイス ペアの設定 \(18 ページ\)](#)

**ステップ 1** (デバイスビュー) ポリシーセクタから[インターフェイス (Interfaces) ]を選択し、[物理インターフェイス (Physical Interfaces) ]タブをクリックします (必要な場合)。

**ステップ 2** 設定を変更するインターフェイスを選択し、[行の編集 (Edit Row) ] ボタンをクリックします。[Modify Physical Interface Map] ダイアログボックスが表示されます。

**ステップ 3** 必要な設定変更を行い、[OK] をクリックします。よく変更される設定を次に示します。すべてのオプションについては、[\[Modify Physical Interface Map\] ダイアログボックス \(14 ページ\)](#) を参照してください。

- [イネーブル (Enabled) ]: インターフェイスがイネーブルであるかどうか ([はい (Yes) ] または [いいえ (No) ])。インターフェイスを動作させるには、[Yes] を選択します。このオプションの値は、[Physical Interfaces] タブの [Administrative State] カラムに表示されます。
- [デフォルト VLAN (Default VLAN) ]: インターフェイスが割り当てられている VLAN。
- [TCP リセットインターフェイスを指定 (Specify Interface for TCP Reset) ]: [インターフェイスについて \(1 ページ\)](#) で説明しているように、代替 TCP リセットインターフェイスを割り当てるには、このオプションを選択してから、[インターフェイス名 (interface-name) ] リストから代替インターフェイスを選択します。

**[Modify Physical Interface Map] ダイアログボックス**

[Modify Physical Interface Map] ダイアログボックスを使用して、IPS センサーの物理インターフェイスの設定を変更します。手順については、[物理インターフェイスの設定 \(13 ページ\)](#) を参照してください。

**ナビゲーションパス**

(デバイスビュー) ポリシーセクタから[インターフェイス (Interface) ]を選択します。[物理インターフェイス (Physical Interfaces) ] タブで、インターフェイスを選択し、[行の編集 (Edit Row) ] ボタンをクリックします。

**関連項目**

- [インターフェイスについて \(1 ページ\)](#)
- [IPS インターフェイス ポリシーについて \(8 ページ\)](#)



## フィールドリファレンス

表 3: [Modify Physical Interface Map] ダイアログボックス

要素	説明
名前	物理インターフェイスの名前。
メディア タイプ (Media Type)	物理インターフェイスのメディアタイプ。メディアタイプは、次のとおりです。 <ul style="list-style-type: none"> <li>• [TX] : 銅線メディア。</li> <li>• [SX] : ファイバメディア。</li> <li>• [XL] : ネットワーク アクセラレータ カード。</li> <li>• [Backplane interface] : モジュールを親シャーシのバックプレーンに接続する内部インターフェイス。</li> </ul>
Description	インターフェイスの説明。
[有効 (Enabled) ]	インターフェイスがイネーブルであるかどうか ([Yes] または [No]) 。 インターフェイスを動作させるには、[はい (Yes) ] を選択する必要があります。インターフェイスの仮想センサーにインターフェイスを割り当てる必要もあります。[Virtual Sensors] ポリシーを使用します。
デュプレックス	インターフェイスのデュプレックス設定。デュプレックス設定は、次のとおりです。 <ul style="list-style-type: none"> <li>• [Auto] : インターフェイスを自動ネゴシエーションデュプレックスに設定します。</li> <li>• [Full] : インターフェイスを全二重に設定します。</li> <li>• [Half] : インターフェイスを半二重に設定します。</li> </ul>

要素	説明
速度	<p>インターフェイスの速度設定。速度のオプションは、次のとおりです。</p> <ul style="list-style-type: none"> <li>• [Auto] : インターフェイスを自動ネゴシエーション速度に設定します。</li> <li>• [10 MB] : インターフェイスを 10 MB に設定します (TX インターフェイスの場合だけ)。</li> <li>• [100 MB] : インターフェイスを 100 MB に設定します (TX インターフェイスの場合だけ)。</li> <li>• [1 GB] : インターフェイスを 1 GB に設定します (ギガビット インターフェイスの場合だけ)。</li> <li>• [10 GB] : インターフェイスを 10 GB に設定します (10 ギガビット インターフェイスの場合だけ)。</li> </ul>
Default VLAN	<p>ネイティブトラフィックに関連付けられている VLAN ID、または 0 (不明な場合や、どの VLAN であるかは関係ない場合)。</p>
Specify Interface for TCP Reset interface-name	<p>代替インターフェイスが無差別モニタリングに使用され、シグニチャの起動によってリセットアクションがトリガーされた場合に、代替インターフェイスで TCP リセットを送信するかどうか。</p> <p>このオプションを選択した場合は、[interface-name] リストから代替 TCP リセット インターフェイスを選択します。</p> <p>代替 TCP リセットの詳細については、<a href="#">インターフェイスについて (1 ページ)</a> を参照してください。</p>

## バイパス モードの設定

インラインバイパスは、分析ツールとして、およびフェールオーバー保護メカニズムとして使用できます。通常は、センサーの分析エンジンがパケット分析を実行します。インラインバイパスがアクティブである場合、分析エンジンはバイパスされ、トラフィックは検査されることなく、インラインインターフェイスおよびインライン VLAN ペアを通過できます。インラインバイパスによって、センサープロセスがアップグレードのために一時的に停止した場合や、センサーモニタリングプロセスが失敗した場合でも、パケットは引き続きセンサーを通過できます。オン、オフ、および自動という3つのモードがあります。デフォルトでは、バイパスモードは自動に設定されています。

使用するバイパスモードを決定する前に、次のことを考慮してください。

- センサーをバイパスモードにすると、セキュリティ上の影響があります。バイパスモードをオンにすると、トラフィックはセンサーをバイパスし、検査されません。そのため、センサーは悪意のある攻撃を阻止できません。

- インラインバイパス機能は、ソフトウェアで実行されるため、オペレーティングシステムが稼働している場合にだけ動作します。センサーの電源がオフになっている場合、またはシャットダウンされている場合、インラインバイパスは動作しません。つまり、トラフィックはセンサーを通過しません。
- センサーが、シグニチャまたはグローバル関連の更新を適用すると、バイパスがトリガーされる場合があります。バイパスがトリガーされるかどうかは、センサーのトラフィック負荷とシグニチャまたはグローバル関連更新のサイズによって決まります。バイパスモードをオフにすると、インラインセンサーはアップデートの適用中にトラフィックの送信を停止します。

バイパスモードの設定を変更するには、次の手順を実行します。

**ステップ1** (デバイスビュー) ポリシーセクタから [インターフェイス (Interface)] ポリシーを選択します。

**ステップ2** ポリシーの一番下にある [バイパスモード (Bypass Mode)] フィールドで、目的のオプションを選択します。

- [オフ (インライントラフィックを常に検査する) (Off (Always inspect inline traffic))] : バイパスモードを無効にします。

トラフィックは、検査のために、センサーを介して送信されます。センサーのモニタリングプロセスがダウンすると、トラフィックは通過しなくなります。これは、インライントラフィックが常に検査されることを意味します。

- [オン (インライントラフィックを検査しない) (On (Never inspect inline traffic))] : トラフィックは、分析エンジンをバイパスし、検査されません。これは、インライントラフィックが常に検査されないことを意味します。
- [自動 (分析エンジンが停止している場合は検査をバイパスする) (Auto (Bypass inspection when analysis engine is stopped))] : センサーのモニタリングプロセスがダウンしている場合を除き、センサー経由のトラフィックフローは検査されます。これがデフォルトです。

センサーのモニタリングプロセスがダウンすると、センサーが再び動作するまで、トラフィックはセンサーをバイパスします。センサーは、動作を再開すると、トラフィックを検査します。Autoモードは、センサーのアップグレード時に役立ちます。センサーのアップグレード中でもトラフィックフローが確保されるからです。また、Autoモードによって、モニタリングプロセスが失敗した場合でも、トラフィックは引き続きセンサーを通過します。

## CDP モードの設定

Cisco Discovery Protocol (CDP) パケットの転送をイネーブルまたはディセーブルするように、IPSセンサーを設定できます。CDP設定は、デバイス上のすべてのインターフェイスにグローバルに適用されます。ただし、効果があるのはインラインインターフェイス (インラインインターフェイスとインラインVLANペア) だけです。

Cisco Discovery Protocol は、メディアおよびプロトコルに依存しないデバイス検出プロトコルであり、すべてのシスコ製装置（ルータ、アクセスサーバ、ブリッジ、スイッチなど）上で動作します。CDP を使用することにより、デバイスはその存在を他のデバイスにアドバタイズし、同じ LAN 上または WAN のリモート サイト上の他のデバイスに関する情報を受信できます。CDP は、SNAP をサポートするすべてのメディア（LAN、フレーム リレー、ATM メディアなど）で稼働します。



**ヒント** CDP モード設定は、一部の IPS アプライアンスおよびサービス モジュールでは使用できません。[CDP Mode] フィールドがインターフェイス ポリシーに表示されない場合、それらの設定は、設定中のデバイスには適用されません。

デバイスで CDP モード設定を変更するには、次の手順を実行します。

**ステップ 1** (デバイスビュー) ポリシーセクタから [インターフェイス (Interface)] ポリシーを選択します。

**ステップ 2** ポリシーの一番下にある [CDPモード (CDP Mode)] フィールドで、必要なオプションを選択します。

- [CDPパケットを転送 (Forward CDP packets)] : CDPパケットがセンサーを通過できるようにします。
- [CDPパケットをドロップ (Drop CDP packets)] : センサーにすべての CDP パケットをドロップさせ、センサーを通過できないようにします。これがデフォルト設定です。

## インラインインターフェイス ペアの設定

センサーでインラインモニタリングを実行できる場合は、センサーでインターフェイスのペアを設定できます。インライン ペアの詳細については、[インライン VLAN ペア モード \(4 ページ\)](#) を参照してください。



**ヒント** ルータおよび ASA デバイスの IPS モジュールでは、モニタリング用のインライン ペアは必要ありません。必要となるのは、物理インターフェイスを仮想センサーに追加することだけです。

### 関連項目

- [インターフェイスについて \(1 ページ\)](#)
- [バイパス モードの設定 \(16 ページ\)](#)
- [CDP モードの設定 \(17 ページ\)](#)
- [物理インターフェイスの設定 \(13 ページ\)](#)
- [VLAN グループの設定 \(21 ページ\)](#)

- [仮想センサーの定義](#)
- [仮想センサーのポリシーの編集](#)
- [仮想センサーへのインターフェイスの割り当て](#)

**ステップ 1** (デバイスビュー) ポリシーセクタから [インターフェイス (Interfaces) ] を選択し、次に [インラインペア (Inline Pairs) ] タブをクリックします。

**ステップ 2** 次のいずれかを実行します。

- ペアを追加するには、[行の追加 (Add Row) ] ボタンをクリックします。[Add Interface Pair] ダイアログボックスが開きます。
- ペアを編集するには、ペアを選択して [行の編集 (Edit Row) ] ボタンをクリックします。[Edit Interface Pair] ダイアログボックスが開きます。

**ヒント** ペアを選択し、[行の削除 (Delete Row) ] ボタンをクリックして削除することもできます。インライン VLAN グループが存在する場合は、インラインペアを削除できません。最初にインライン VLAN グループを [VLAN Groups] タブから削除し、次にインライン ペアを削除します。

**ステップ 3** [Add or Edit Inline Pairs] ダイアログボックスで、次のオプションを設定します。

- [インラインインターフェイス名 (Inline Interface Name) ] : インラインペアに付ける名前。この名前は、32 文字以下とする必要があります。使用できる文字は、英数字とアンダースコアです。この名前は、ペアを作成したあとには編集できません。
- [インターフェイス1および2 (Interface 1 and 2) ] : ペアの形成に使用する 2 つの物理インターフェイスを選択します。このリストには、[Physical Interfaces] タブで定義されたインターフェイスで、かつインラインペア、VLAN ペア、または VLAN グループの一部になっていないインターフェイスだけが表示されます。
- [説明 (Description) ] : ペアの説明 (任意) 。

**ステップ 4** [OK] をクリックして変更を保存します。

## インライン VLAN ペアの設定

IPS インターフェイス ポリシーの [VLAN Pairs] タブを使用して、物理インターフェイス用の VLAN ペアを設定します。このサマリーテーブルには、各物理インターフェイスの既存の VLAN ペアが表示されます。単一の物理インターフェイスに複数の VLAN ペアを作成できます。インライン VLAN ペア モードの詳細については、[インライン VLAN ペア モード \(4 ページ\)](#) を参照してください。

**ヒント**

- インターフェイスが、すでにインライン インターフェイス ペアの一部である場合は、そのインターフェイスの VLAN ペアは作成できません。インライン インターフェイス ペアの VLAN グループを作成します。
- 無差別モードで動作し、仮想センサーに割り当てられているインターフェイス用のインライン VLAN ペアを作成するには、最初にそのインターフェイスを仮想センサーから削除し ([Virtual Sensors] ポリシーを使用)、次にインライン VLAN ペアを作成する必要があります。
- インライン VLAN ペアでペアになっている VLAN のいずれかとして、デフォルト VLAN を使用することはできません。
- 使用しているセンサーが、インライン VLAN ペアをサポートしていない場合、[VLAN Pairs] ペインは表示されません。ルータおよび ASA デバイスの IPS モジュールは、インライン VLAN ペアをサポートしていません。
- インライン VLAN ペアを使用する場合は、VLAN をホストしている、接続されているスイッチで単方向リンク検出 (UDLD) を設定する必要があります。UDLD を使用すると、スイッチがスパンニングツリー転送ループおよび単方向リンクを回避するのに役立ちます。詳細については、[https://www.cisco.com/c/en/us/td/docs/security/ips/7-0/configuration/guide/idm/idmguide7/idm\\_interfaces.html#wp1169508](https://www.cisco.com/c/en/us/td/docs/security/ips/7-0/configuration/guide/idm/idmguide7/idm_interfaces.html#wp1169508)を参照してください。

#### 関連項目

- [インターフェイスについて \(1 ページ\)](#)
- [バイパス モードの設定 \(16 ページ\)](#)
- [CDP モードの設定 \(17 ページ\)](#)
- [物理インターフェイスの設定 \(13 ページ\)](#)
- [VLAN グループの設定 \(21 ページ\)](#)

**ステップ 1** (デバイスビュー) ポリシーセクタから [インターフェイス (Interfaces)] を選択し、次に [VLANペア (VLAN Pairs)] タブをクリックします。

**ステップ 2** 次のいずれかを実行します。

- ペアを追加するには、[行の追加 (Add Row)] ボタンをクリックします。[Add VLAN Pair] ダイアログボックスが開きます。
- ペアを編集するには、ペアを選択して [行の編集 (Edit Row)] ボタンをクリックします。[Edit VLAN Pair] ダイアログボックスが開きます。

**ヒント** ペアを選択し、[行の削除 (Delete Row)] ボタンをクリックして削除することもできます。インライン VLAN ペアは、仮想センサーに割り当てられている場合は削除できません。[Virtual Sensors] ポリシーを使用して最初に仮想センサーへの割り当てを削除してから、インライン VLAN ペアを削除します。



ステップ3 [Add VLAN Pairs]/[Edit VLAN Pairs] ダイアログボックスで、次のオプションを設定します。

- [物理インターフェイス (Physical Interfaces)] : VLAN ペアを作成する物理インターフェイスを選択します。このリストには、[Physical Interfaces] タブで定義され、かつインラインインターフェイス ペアまたは VLAN グループの一部となっていないインターフェイスだけが含まれています。ただし、単一のインターフェイス上で複数の VLAN ペアを作成できます。
- [サブインターフェイス番号 (Subinterface Number)] : サブインターフェイスとして割り当てる番号を入力します。この番号は、インターフェイスで一意である必要があります。つまり、選択した物理インターフェイス上の別の VLAN ペアにまだ割り当てられていない必要があります。1 ~ 255 のサブインターフェイス番号を指定できます。
- [説明 (Description)] : ペアの説明 (任意)。
- [VLAN A, B (VLAN A, B)] : ペアとして結合する2つの VLAN の番号。VLAN 番号は、1 ~ 4095 の値です。異なる番号を入力する必要があります。また、選択した物理インターフェイス上の別の VLAN ペアの番号と同じ番号は使用できません。

ステップ4 [OK] をクリックして変更を保存します。

## VLAN グループの設定

IPS インターフェイスポリシーの [VLAN Groups] タブを使用して、物理インターフェイスおよびインラインインターフェイス ペア (論理インターフェイス) の VLAN グループを設定します。サマリーテーブルには、既存の VLAN グループが表示されます。単一の物理インターフェイスまたはインラインインターフェイス ペア上に複数の VLAN グループを作成できます。VLAN グループモードの詳細については、[VLAN グループモード \(5 ページ\)](#) を参照してください。

VLAN グループは、インターフェイスに存在する VLAN ID のグループで構成されています。各 VLAN グループは、少なくとも1つの VLAN ID で構成されています。インターフェイス (論理または物理) ごとに最大 255 の VLAN グループを設定できます。各グループには、任意の数の VLAN ID を含めることができます。

VLAN ID を VLAN グループに割り当てたあとに、その VLAN グループを仮想センサーに割り当てて、動作できるようにする必要があります。単一グループは、1つの仮想センサーだけに割り当てることができます。[Virtual Sensors] ポリシーを使用して、割り当てを行います。



- (注) VLAN グループは、IPS 6.0 以降でだけサポートされています。すべての IPS アプライアンスまたはサービスモジュールで VLAN グループがサポートされているわけではありません。[VLAN Groups] タブが [Interfaces] ポリシーに表示されない場合、設定しているそのデバイスではこの機能がサポートされていません。

関連項目

- インターフェイスについて (1 ページ)
- バイパス モードの設定 (16 ページ)
- CDP モードの設定 (17 ページ)
- 物理インターフェイスの設定 (13 ページ)
- 仮想センサーの定義
- 仮想センサーのポリシーの編集
- 仮想センサーへのインターフェイスの割り当て

**ステップ 1** (デバイスビュー) ポリシーセクタから [インターフェイス (Interfaces) ] を選択し、次に [VLAN グループ (VLAN Groups) ] タブをクリックします。

この表には、グループが定義されているインターフェイス、サブインターフェイス番号、説明 (ある場合)、グループに割り当てられている VLAN を含む、既存の VLAN グループが示されます。VLAN のセルが空白の場合、そのグループはインターフェイス上のすべての未割り当て VLAN 用に定義されています。

**ステップ 2** 次のいずれかを実行します。

- ペアを追加するには、[行の追加 (Add Row) ] ボタンをクリックします。[Add VLAN Group] ダイアログボックスが開きます。
- ペアを編集するには、ペアを選択して [行の編集 (Edit Row) ] ボタンをクリックします。[Edit VLAN Group] ダイアログボックスが開きます。

**ヒント** グループを選択し、[行の削除 (Delete Row) ] ボタンをクリックしてグループを削除することもできます。VLAN グループは、仮想センサーに割り当てられている場合は削除できません。[Virtual Sensors] ポリシーを使用して最初に仮想センサーへの割り当てを削除してから、VLAN グループを削除します。

**ステップ 3** [Add VLAN Group] または [Edit VLAN Group] ダイアログボックスで、次のオプションを設定します。

- [物理および論理インターフェイス (Physical and Logical Interfaces) ] : この VLAN グループを作成している物理インターフェイスまたはインラインインターフェイスペアを選択します。このリストには、インライン VLAN ペアがまだ定義されておらず、ペアになっていない物理インターフェイス ([Physical Interfaces] タブで定義) や、[Inline Pairs] タブで定義されているインラインインターフェイスペアだけが表示されます。単一のインターフェイス上で複数の VLAN グループを作成できます。次の点を考慮してください。
  - 物理インターフェイスを選択した場合は、無差別 VLAN グループを作成します。
  - 論理インターフェイスを選択した場合は、インライン VLAN グループを作成します。
- [サブインターフェイス番号 (Subinterface Number) ] : サブインターフェイスとして割り当てる番号を入力します。この番号は、インターフェイスで一意である必要があります。つまり、選択したインター

フェイス上の別の VLAN グループにまだ割り当てられていない必要があります。1 ～ 255 のサブインターフェイス番号を指定できます。

- [説明 (Description) ] : グループの説明 (任意) 。
- [VLAN assignment] : 次のいずれかのオプションを選択します。
  - [すべての割り当てられていない VLAN ID (All Unassigned VLAN IDs) ] : このグループには、他の VLAN グループに割り当てられていないすべての VLAN が含まれます。これはデフォルトのオプションです。
  - [無料VLAN IDの範囲 (Range of free VLAN IDs) ] : このグループには、特定の VLAN が含まれます。[範囲 (Range) ] ボックスに、1 つの VLAN ID または範囲の任意の組み合わせを入力し (ID の先頭と末尾をハイフンで区切る) 、複数のエントリをカンマで区切ります。たとえば、10,12-25, 33-49 のように入力します。VLAN 番号は、1 ～ 4095 の値です。

この VLAN ID には、選択したインターフェイスの別の VLAN グループの VLAN ID は使用できません。また、VLAN は、接続されているスイッチで設定する必要があります。そうしないと、検査するトラフィックが存在しないこととなります。

**ステップ 4** [OK] をクリックして変更を保存します。

---



## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。