IPS 6.X以降/IDSM2:IDMを使用したインライン インターフェイスペアモードの設定例

内容

[はじめに](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[関連製品](#)
[表記法](#)
[インライン インターフェイス ペアの設定](#)
[CLI での設定](#)
[IDM の設定](#)
[インライン モードの IDSM-2 のスイッチの設定](#)
[トラブルシュート](#)
[問題](#)
[解決方法](#)
[関連情報](#)

はじめに

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、侵入防御システム（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パケット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 デバイスを通過する攻撃をシステムが識別し、停止またはブロックできます。

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：これらのモジュールには検出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AIM-IPSとAIP-SSMを設定できます。

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、スイッチ上でそれらのインターフェイスを、2つのポートに対して異なるアクセスVLANを持つアクセスポートとして設定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過しません。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、コマンドライン インターフェイス 6.0 および侵入防御システムデバイス マネージャ（IDM）6.0 を使用する Cisco IPS センサーに基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

関連製品

また、このドキュメントの情報は、侵入検知システム（IDSM-2）サービス モジュールにも適用されます。

表記法

表記法の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

インライン インターフェイス ペアの設定

インライン インターフェイス ペアを作成するサービス インターフェイス サブモードで、インライン インターフェイス name コマンドを使用します。

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool(登録ユーザ専用)を使用してください。

注：AIP-SSMは、インラインインターフェイスモード用にCisco IPS CLIからではなく、Cisco ASA CLIから設定します。

これらのオプションによって、次の設定が割り当てられます。

- inline-interfaces name：論理インライン インターフェイスのペアの名前

  注：すべてのモジュール（IDSM-2 NM-CIDSおよびAIP-SSM）のすべてのバックプレーンセンシングインターフェイスで、admin-stateが有効に設定されており、保護されています（設定を変更することはできません）。admin-state は、コマンド/制御インターフェイスに影響しません（保護されています）。検出インターフェイスにのみ影響します。コマンドおよび制御インターフェイスはモニタできないため、有効にする必要はありません。

- default：値をシステムのデフォルト設定に戻します。

- description：インライン インターフェイス ペアの説明
- interface1 interface_name：インラインインターフェイスペア内の1つめのインターフェイス
- interface2 interface_name：インラインインターフェイスペア内の2つめのインターフェイス
- no：エントリまたは選択設定を削除します
- admin-state {enabled | disabled}：インターフェイスの管理リンク状態。インターフェイスは有効または無効のいずれかです。

CLI での設定

センサーでインライン VLAN ペアを設定するには、次の手順を実行します。

1. 管理者権限を持つアカウントで CLI にログインします。
2. インターフェイス サブモードを入力します。

```
<#root>

sensor#

configure terminal

sensor(config)#

service interface


sensor(config-int)#
```

3. インライン インターフェイスが存在するか確認します。サブインターフェイスのタイプは、インライン インターフェイスが設定されていない場合は none になります。

```
<#root>

sensor(config-int)#

show settings

   physical-interfaces (min: 0, max: 999999999, current: 2)
   ---------------------------------------------
      <protected entry>
      name: GigabitEthernet0/0 <defaulted>
      ---------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <protected>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         ---------------------------------------------
            none
```

```
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
         subinterface-type
         ------------------------------------------------
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
<protected entry>
      name: GigabitEthernet0/1 <defaulted>
      ------------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <defaulted>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         ------------------------------------------------
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
         subinterface-type
         ------------------------------------------------
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
      <protected entry>
      name: GigabitEthernet0/2 <defaulted>
      ------------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <defaulted>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         ------------------------------------------------
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
         subinterface-type
         ------------------------------------------------
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
      <protected entry>
      name: GigabitEthernet0/3 <defaulted>
      ------------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <defaulted>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         ------------------------------------------------
```

```
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
         subinterface-type
         ------------------------------------------------
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
      <protected entry>
      name: Management0/0 <defaulted>
      ------------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <protected>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         ------------------------------------------------
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
         subinterface-type
         ------------------------------------------------
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
   command-control: Management0/0 <protected>
   inline-interfaces (min: 0, max: 999999999, current: 0)
   ------------------------------------------------
   ------------------------------------------------
   bypass-mode: auto <defaulted>
   interface-notifications
   ------------------------------------------------
      missed-percentage-threshold: 0 percent <defaulted>
      notification-interval: 30 seconds <defaulted>
      idle-interface-delay: 30 seconds <defaulted>
   ------------------------------------------------
sensor(config-int)#
```

4. インライン ペアの名前：

```
<#root>

sensor(config-int)#

inline-interfaces PAIR1
```

5. 使用可能なインターフェイスのリストが表示されます。

<#root>

```
sensor(config-int)#
```

physical-interfaces ?

```
GigabitEthernet0/0     GigabitEthernet0/0 physical interface.
GigabitEthernet0/1     GigabitEthernet0/1 physical interface.
GigabitEthernet0/2     GigabitEthernet0/2 physical interface.
GigabitEthernet0/3     GigabitEthernet0/3 physical interface.
Management0/0          Management0/0 physical interface.
sensor(config-int)#
```

physical-interfaces

6. 2 つのインターフェイスをペアに設定します。

<#root>

```
sensor(config-int)#
```

interface1 GigabitEthernet0/0

<#root>

```
sensor(config-int-inl)#
```

interface2 GigabitEthernet0/1

トラフィックをモニタする前に、インターフェイスを仮想センサーに割り当てて有効にする必要があります。詳細については、ステップ 10 を参照してください。

7. このインターフェイスの説明を追加します。

<#root>

```
sensor(config-int-phy)#
```

description PAIR1 Gig0/0 and Gig0/1

8. インライン インターフェイス ペアに設定する他のインターフェイスに対して、ステップ 4 ~ 7 を繰り返します。

9. 設定を確認します。

<#root>

```
sensor(config-int-inl)#
show settings
   name: PAIR1
   -----------------------------------------------
      description: PAIR1 Gig0/0 & Gig0/1 default:
      interface1: GigabitEthernet0/0
      interface2: GigabitEthernet0/1
   -----------------------------------------------
```

10. インターフェイス ペアに割り当てられているインターフェイスを有効にします。

```
<#root>
sensor(config-int)#
exit
sensor(config-int)#
physical-interfaces GigabitEthernet0/0
sensor(config-int-phy)#
admin-state enabled
sensor(config-int-phy)#
exit
sensor(config-int)#
physical-interfaces GigabitEthernet0/1
sensor(config-int-phy)#
admin-state enabled
sensor(config-int-phy)#
exit
sensor(config-int)#
```

11. インターフェイスが有効になっていることを確認します。

```
<#root>
sensor(config-int)#
show settings
   physical-interfaces (min: 0, max: 999999999, current: 5)
   -----------------------------------------------
      <protected entry>
      name: GigabitEthernet0/0
      -----------------------------------------------
         media-type: tx <protected>
```

```
   description: <defaulted>
   admin-state: enabled default: disabled
   duplex: auto <defaulted>
   speed: auto <defaulted>
   default-vlan: 0 <defaulted>
   alt-tcp-reset-interface
   ------------------------------------------------
      none
      ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
   subinterface-type
   ------------------------------------------------
      none
      ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
-----------------------------------------------
<protected entry>
name: GigabitEthernet0/1
-----------------------------------------------
   media-type: tx <protected>
   description: <defaulted>
   admin-state: enabled default: disabled
   duplex: auto <defaulted>
   speed: auto <defaulted>
   default-vlan: 0 <defaulted>
   alt-tcp-reset-interface
   ------------------------------------------------
      none
      ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
   subinterface-type
   ------------------------------------------------
      none
      ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
-----------------------------------------------
<protected entry>
name: GigabitEthernet0/2 <defaulted>
-----------------------------------------------
   media-type: tx <protected>
   description: <defaulted>
   admin-state: disabled <defaulted>
   duplex: auto <defaulted>
   speed: auto <defaulted>
   default-vlan: 0 <defaulted>
   alt-tcp-reset-interface
   ------------------------------------------------
      none
      ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
   subinterface-type
   ------------------------------------------------
      none
      ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
-----------------------------------------------
```

```
      <protected entry>
      name: GigabitEthernet0/3 <defaulted>
      ------------------------------------------------
         media-type: tx <protected>
--MORE--
```

12. インライン インターフェイス ペアを削除してインターフェイスを無差別モードに戻すには、次のコマンドを発行します。

<#root>

```
sensor(config-int)#
```

no inline-interfaces PAIR1

インライン インターフェイス ペアを、割り当て先の仮想センサーから削除する必要もあります。

13. インライン インターフェイス ペアが削除されたことを確認します。

<#root>

```
sensor(config-int)#
```

show settings

```
  ------------------------------------------------
  command-control: Management0/0 <protected>
  inline-interfaces (min: 0, max: 999999999, current: 0)
  ------------------------------------------------
  ------------------------------------------------
  bypass-mode: auto <defaulted>
  interface-notifications
  ------------------------------------------------
```

14. インターフェイス コンフィギュレーション サブモードを終了します。

<#root>

```
sensor(config-int)#
```

exit

```
Apply Changes:?[yes]:
```

15. 変更を適用する場合はEnter キーを押し、変更を廃棄する場合は [no] を入力します。

IDM の設定

IDM を使用してセンサーでインライン VLAN ペアを設定するには、次の手順を実行します。

1. ブラウザを開き、https://<Management_IP_Address_of_IPS> と入力して、IPS 上の IDM にアクセスします。
2. [Download IDM Launcher and Start IDM] をクリックし、アプリケーションのインストーラをダウンロードします。
3. ホスト名、IP アドレス、バージョン、モデルなどのデバイス情報を表示するには、ホームページに移動します。
4. [Configuration] > [Sensor Setup] の順に移動して、[Network] をクリックします。ホスト名、IP アドレス、デフォルト ルートを指定できます。
5. [Configuration] > [Interface Configuration] の順に移動して、[Summary] をクリックします。

   このページには、検出インターフェイスの構成サマリーが表示されます。
6. [Configuration] > [Interface Configuration] > [Interfaces] の順に移動して、インターフェイス名を選択します。次に、[Enable] をクリックして、検出インターフェイスを有効にします。また、デュプレックス、速度、VLAN 情報を設定します。
7. [Configuration] > [Interface Configuration] > [Interface Pairs] の順に移動して、[Add] をクリックし、インライン ペアを作成します。
8. インライン ペア設定の要約を確認して適用します。
9. [Configuration] > [Analysis Engine] > [Virtual Sensor] の順に移動して、[Edit] をクリックし、新しい仮想センサーを作成します。
10. インライン ペア INLINE を仮想センサー vs0 に割り当てます。
11. 割り当てた仮想センサー情報の要約を表示します。

インライン モードの IDSM-2 のスイッチの設定

インライン モードの IDSM-2 スイッチを設定するには、『IDSM-2 の設定』の「Catalyst シリーズ 6500 スイッチでインライン モードの IDSM-2 を設定する」の項を参照してください。

トラブルシュート

問題

IPS が失敗し、インラインに設定されている場合、インターフェイス フェール オープンを実行するか（トラフィックの通過は続行）、または終了します（トラフィックはドロップ）。

解決方法

フェール オープン状態の IPS を設定できます。したがって、IPS が失敗するとトラフィックは引き続き通過しますが、トラフィックをモニタしません。

関連情報

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco Intrusion Prevention System
- Cisco IPS 4200 シリーズ センサー
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。