

IPS 5.x 以降/IDSM2 : CLI および IDM を使用したインライン VLAN ペア モードの設定例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[関連製品](#)

[表記法](#)

[VACL キャプチャ設定](#)

[インライン VLAN ペア モードコンフィギュレーション](#)

[CLI 設定](#)

[IDM の設定](#)

[トラブルシューティング](#)

[関連情報](#)

概要

物理インターフェイスのペアの VLAN の関連付けはインライン VLAN ペア モードと呼ばれています。ペアの VLAN の一方で受信したパケットは分析され、ペアのもう一方の VLAN に転送されます。インライン VLAN ペアは NM-CIDS、AIP-SSM-10 および AIP-SSM-20 を除く侵入防御システム (IPS) 5.1 と互換性がある、すべてのセンサーでサポートされます。

インライン VLAN ペア モードは検知インターフェイスが 802.1q トランク ポートとして機能する、センサーはトランクの VLAN のペア間の VLANブリッジングを行いますアクティブな検知モードであり。これは検知インターフェイスに接続されるスイッチがトランク モードにある必要があることを意味します。

センサーは不正侵入試みが検出する場合各ペアの各 VLAN で受信するトラフィックを検査し、ペアの他の VLAN のパケットを転送するか、またはパケットを廃棄できます。同時に各々の検知インターフェイスの 255 までの VLAN ペアを繋ぐために IPS センサーを設定できます。センサーはセンサーがパケットを転送する出力 VLAN の ID と各受け取り パケットの 802.1q ヘッダの VLAN ID フィールドを取り替えます。センサーはインライン VLAN ペアに割り当てられないあらゆる VLAN で受信されるすべてのパケットを廃棄します。

注: IPS-4260 に関しては、故障する開いたハードウェア バイパスはインライン VLAN ペアでサポートされません。詳細については [ハードウェア バイパス 設定の 制限](#)を参照して下さい。

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

この文書に記載されている情報は 5.1 およびそれ以降を使用するに基づいた on Cisco Intrusion Prevention System センサーです。

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たものです。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。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分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

ドキュメント表記の詳細は、『[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。

VACL は設定をキャプチャします

[IDSM-2](#) のスイッチの IDSM にトラフィックを送信するために [設定](#) の [設定 VACL キャプチャ](#) セクションを参照して下さい。

インライン VLAN ペア モードコンフィギュレーション

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

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。

CLI を使用してインライン VLAN ペアを設定するためにサービス インターフェイス サブモードで物理インターフェイス `interface_name` コマンドを使用して下さい。 インターフェイス名は FastEthernet または GigabitEthernet です。

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。

- **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。注: すべてのモジュール上のすべてのバックプレーン検出インターフェイス (IDSM-2 NM-CIDS および AIP-SSM) で、**admin-state** が有効に設定され、保護されます (設定を変更できません)。 **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** — システムデフォルト標準設定に値を設定し直します。
- **description** — インライン インターフェイス ペアの記述。
- **duplex** — インターフェイスの双方向設定。 **自動**—自動にインターフェイスをネゴシエートし

- まず二重を設定します。フルセット 全二重へのインターフェイス。半半二重にインターフェイスを設定します。注: デュプレックス オプションはすべてのモジュールで保護されます。
- 非エントリまたは選択設定を取除きます。
 - 速度—インターフェイスの速度設定。自動—自動にインターフェイスをネゴシエートします速度を設定します。10—10 MB にインターフェイスを設定します (TX インターフェイスだけのために)。100—100 MB にインターフェイスを設定します (TX インターフェイスだけのために)。1000—1 GB にインターフェイスを設定します (ギガビットインターフェイスのために) 注: 速度オプションはすべてのモジュールで保護されます。
 - サブインターフェイス型—インターフェイスがサブインターフェイスであるどのようなサブインターフェイスが定義されること規定し。インライン VLAN ペア—インライン VLAN ペアとサブインターフェイスを定義することを許可します。なし—定義されるサブインターフェイス無し。
 - サブインターフェイス—インライン VLAN ペアとサブインターフェイスを定義します。vlan1—インライン VLAN ペアの最初の VLAN。vlan2—インライン VLAN ペアの第 2 VLAN。

CLI 設定

CLI を使用してセンサーのインライン VLAN ペア設定を行うためにこれらのステップを完了して下さい:

1. アドミニストレーター特権のアカウントを使用して CLI へのログイン。
2. インターフェイス サブモードを入力します。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設定されない場合) どのインライン インターフェイスでもあるかどうか確認して下さい (サブインターフェイス型は 「どれも」 読む必要があります

```

: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. この物理インターフェイスを使用するインライン インターフェイスを外して下さい

```

:sensor(config-int)#no inline-interfaces interface_name

```

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。 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. インターフェイスを規定して下さい: sensor(config-int)#physical-interfaces GigabitEthernet0/2

7. インターフェイスの admin の状態を有効に して下さい: sensor(config-int-phy)#admin-state enabled

インターフェイスは仮想 なセンサーに割り当てられ、トラフィックをモニタするために有効に する必要があります。

8. このインターフェイスの説明を追加します。 sensor(config-int-phy)#description INT1

9. 双方向設定を設定して下さい: sensor(config-int-phy)#duplex full

このオプションはモジュールで利用できません。

10. 速度を設定して下さい: sensor(config-int-phy)#speed 1000

このオプションはモジュールで利用できません。

11. インライン VLAN ペアを設定して下さい: sensor(config-int-phy)#subinterface-type inline-vlan-pair

```

sensor(config-int-phy-inl)#subinterface 1 sensor(config-int-phy-inl-sub)#vlan1
52 sensor(config-int-phy-inl-sub)#vlan2 53

```

12. インライン VLAN ペアのための説明を追加して下さい: sensor(config-int-phy-inl-sub)#description pairs vlans 52 and 53

13. インライン VLAN ペア設定を確認して下さい: sensor(config-int-phy-inl-sub)#show settings

```

subinterface-number: 1 ----- description:
VLANpair1 default: vlan1: 52 vlan2: 53 -----
sensor(config-int-phy-inl-sub)#

```

14. インターフェイス サブモードを終了して下さい: sensor(config-int-phy-inl-sub)#exit

```

sensor(config-int-phy-inl)#exit sensor(config-int-phy)#exit sensor(config-int)#exit Apply
Changes:[yes]:

```

15. 変更を加えるために 『Enter』 を押さないかまたはそれらを廃棄するためにいいえ入力して下さい。

16. 仮想 なセンサー コンフィギュレーションモードを開始して下さい: sensor(config)#service analysis-engine

```

sensor(config-ana)#virtual-sensor vs0

```

17. バーチャル センサーにインターフェイスを追加して下さい: sensor(config-ana-vir)#physical-interface GigabitEthernet0/2 subinterface-number 1

18. バーチャル センサー サブモードを終了して下さい: sensor(config-ana-vir)#exit

```

sensor(config-ana)#exit Apply Changes:[yes]:

```

19. 変更を加えるために 『Enter』 を押さないかまたはそれらを廃棄するためにいいえ入力して下さい。

IDM の設定

IDS Device Manager (IDM) を使用してセンサーのインライン VLAN ペア設定を行うためにこれらのステップを完了して下さい:

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. ホスト名のようなデバイス情報を、IP アドレス、バージョンおよびモデル。、等は Home ページに表示するために行きます。
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。このページは検知インターフェイスの設定の要約を表示します。
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. **設定 > インターフェイスコンフィギュレーション > VLAN ペア**に行き、インライン VLAN ペアを作成するために『Add』 をクリックして下さい。
8. 検知インターフェイス (GigabitEthernet0/0) のためのサブインターフェイス数、VLAN A および VLAN B を入力して下さい。インライン VLAN ペア設定の要約を表示できます。
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. 仮想 なセンサー vs0 へのインライン VLAN ペア 52 および 53 を割り当てて下さい。割り当てた仮想センサー情報の要約を表示します。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

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](#)