CHAPTER 5

インターフェイスの設定

（注） IPS SSP を搭載した Cisco ASA 5585-X は、現在のところ、Cisco IPS 7.1 をサポートする唯一のプラットフォームです。現時点では、他に IPS バージョン 7.1 をサポートしている Cisco IPS センサーはありません。

（注） IPS SSP を搭載した Cisco ASA 5585-X は、ASA 8.2(4.4) 以上および ASA 8.4(2) 以上でサポートされています。ASA 8.3(*x*) では、サポートされていません。

この章では、さまざまなインターフェイス モード、および IPS SSP でのインターフェイスの設定方法について説明します。次の事項について説明します。

IPS SSP インターフェイス

IPS SSP には、管理インターフェイス（コマンド/コントロール）とセンシング インターフェイスの 2 つのインターフェイスがあります。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、IPS SSP の設定に使用されます。これは、IPS SSP がセキュリティおよびステータス イベントを IDM に送信するために使用されます。IPS SSP コマンド/コントロール インターフェイスには、Management 0/0 という名前が付いています。

注意 IPS SSP には、4 種類のポート（コンソール、管理、GigabitEthernet、10GE）があります。IPS SSP の右前面パネルにあるコンソール ポートと管理ポートは、IPS ソフトウェアを使用して設定および制御します。IPS SSP の左前面パネルにある GigabitEthernet ポートと 10GE ポートは、IPS ソフトウェアではなく、ASA ソフトウェアを使用して設定および制御します。ただし、IPS SSP をリセットまたはシャットダウンした場合は、GigabitEthernet ポートと 10GE ポートもリンク ダウンします。スケジュールされたメンテナンスの時間帯は IPS SSP をリセットまたはシャットダウンして、これらのポートがリンク ダウンする影響を最小化する必要があります。

コマンド/コントロール インターフェイスは、常にイネーブルです。これは、特定の物理インターフェイスに永続的にマップされます。コマンド/コントロール 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。

センシング インターフェイスは、セキュリティ違反についてトラフィックを分析するために使用されます。IPS SSP には、センシング インターフェイスは 1 つしかありません。これは PortChannel0/0 という名前で、バックプレーン インターフェイスです。すべてのバックプレーン インターフェイスに、固定速度、デュプレックス、および状態設定があります。これらの設定は、すべてのバックプレーン インターフェイスのデフォルト設定で保護されています。

適応型セキュリティ アプライアンスでのセキュリティ コンテキストによって、IPS SSP インターフェイスを設定します。センシング インターフェイスは永続的にイネーブルにされています。

詳細情報

ASA ソフトウェアの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html

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、他のネットワーキング 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。

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） IPS SSP は、センシング 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。

インターフェイス設定のサマリー

ここでは、[Summary] ペインについて説明します。次の事項について説明します。

[Summary] ペイン

[Summary] ペインには、センシング 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）のサマリーが記載されています。このペインの内容は、インターフェイス設定を変更すると、変わります。

注意　無差別モード、インライン インターフェイス 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てインターフェイスを設定することはできません。

[Summary] ペインのフィールド定義

[Summary] ペインには、次のフィールドがあります。

- [Name]：インターフェイスの名前。IPS SSP の値は PortChannel0/0 です。
- [Details]：インターフェイスがバックプレーン インターフェイスであることを示します。
- [Assigned Virtual Sensor]：仮想センサーはありません。
- [Description]：インターフェイスの説明。

インターフェイスの設定

ここでは、センサーでのインターフェイスの設定方法について説明します。次の事項について説明します。

[Interfaces] ペイン

（注）　センサーでインターフェイスを編集するには、管理者でなければなりません。

[Interfaces] ペインには、センサー上の既存の物理インターフェイスと関連する設定がリストされます。センサーはインターフェイスを検出し、[Interfaces] ペインのインターフェイス リストにデータを設定します。

[Interfaces] ペインのフィールド定義

[Interfaces] ペインには、次のフィールドがあります。

- [Interface Name] : インターフェイスの名前。値は PortChannel0/0 です。
- [Enabled] : インターフェイスがイネーブルにされているかどうか。IPS SSP PortChannel0/0 インターフェイスは常にイネーブルです。
- [Media Type] : メディア タイプを示します。IPS SSP のメディア タイプは、[Backplane Interface] です。これは、適応型セキュリティ アプライアンスのバックプレーンに接続する内部インターフェイスです。
- [Duplex] : インターフェイスのデュプレックス設定を示します。IPS SSP の値は [Full] です。
- [Speed] : インターフェイスの速度設定を示します。値は、PortChannel 0/0 では [10 GB] です。
- [Default VLAN] : インターフェイスを割り当てる VLAN を示します。
- [Alternate TCP Reset Interface] : 選択すると、この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 リセットを送信します。

  （注）　IPS SSP では、代替 TCP リセット インターフェイスがサポートされていません。

- [Description] : インターフェイスの説明を入力できます。

[Edit Interface] ダイアログボックスのフィールド定義

（注）　IPS SSP で編集できる唯一のインターフェイス フィールドは [Description] フィールドです。

[Edit Interface] ダイアログボックスには、次のフィールドがあります。

- [Interface Name] : インターフェイスの名前。値は PortChannel0/0 です。
- [Enabled] : インターフェイスがイネーブルにされているかどうか。IPS SSP PortChannel0/0 インターフェイスは常にイネーブルです。
- [Media Type] : メディア タイプを示します。メディア タイプは、次のとおりです。
  - [TX] : 銅線メディア
  - [SX] : ファイバ メディア
  - [XL] : ネットワーク アクセラレータ カード
  - [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。
- [Duplex] : インターフェイスのデュプレックス設定を示します。デュプレックス設定は、次のとおりです。
  - [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。

  - [Full]：インターフェイスを全二重に設定します。
  - [Half]：インターフェイスを半二重に設定します。
- [Speed]：インターフェイスの速度設定を示します。速度タイプは、次のとおりです。
  - [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。
  - [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）。
  - [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）。
  - [1000]：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）。
- [Default VLAN]：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）。
- [Alternate TCP Reset Interface]：オンにすると、この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 リセットを送信します。
  - [Select Interface]：TCP リセットを送信するインターフェイスを設定します。

    （注） IPS SSP では、代替 TCP リセット インターフェイスがサポートされていません。

- [Description]：インターフェイスの説明を入力できます。

[Description] フィールドの編集

[Description] フィールドを編集するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して IDM にログインします。

ステップ 2　[Configuration] > [Interfaces] > [Interfaces] を選択します。

ステップ 3　インターフェイスを選択して、[Edit] をクリックします。

（注） インターフェイスをダブルクリックしても、[Edit Interface] ダイアログボックスが表示されます。

ステップ 4　[Description] フィールドで説明を変更できます。

（注） IPS SSP PortChannel0/0 インターフェイスは常にイネーブルです。

（注） IPS SSP では、代替 TCP リセット インターフェイスがサポートされていません。

ヒント 変更を廃棄して、[Edit Interface] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 5　[OK] をクリックします。編集したインターフェイスが、[Interfaces] ペインのリストに表示されます。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 6　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。

トラフィック フロー通知の設定

ここでは、トラフィック フロー通知の設定方法について説明します。次の事項について説明します。

[Traffic Flow Notifications] ペイン

（注）　トラフィック フロー通知を設定するには、管理者でなければなりません。

インターフェイス上のパケットのフローをモニタし、そのフローが指定した間隔中に変更（開始および停止）された場合に通知を送信するようにセンサーを設定できます。特定の通知間隔内に失われたパケットのしきい値を設定でき、ステータス イベントがレポートされる前のインターフェイス アイドル遅延も設定できます。

[Traffic Notifications] ペインのフィールド定義

[Traffic Flow Notifications] ペインには、次のフィールドがあります。

- [Missed Packets Threshold]：通知を送信する前に、指定した期間中に欠落する必要があるパケットの割合。
- [Notification Interval]：センサーが欠落パケットの割合を調べる間隔。
- [Interface Idle Threshold]：通知が送信されるまでに、インターフェイスがアイドルでありパケットを受信しない秒数。

トラフィック フロー通知の設定

トラフィック フロー通知を設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して IDM にログインします。

ステップ 2　[Configuration] > [Interfaces] > [Traffic Flow Notifications] を選択します。

ステップ 3　[Missed Packets Threshold] フィールドに、通知を受信する前に発生する必要がある欠落パケットの割合を指定して、その値を入力します。

ステップ 4　[Notification Interval] フィールドで、欠落パケットの割合を検査する秒数を指定して、その値を入力します。

ステップ 5　[Interface Idle Threshold] フィールドに、通知される前にインターフェイスがアイドルになりパケットを受信しないことができる秒数を指定して、その値を入力します。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 6　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。