Firepower Threat Defense のインターフェイスの概要

FTD デバイスには、種々のモードで設定できるデータ インターフェイス、および管理/診断インターフェイスが組み込まれています。

管理/診断インターフェイス

物理的な管理インターフェイスは、診断論理インターフェイスと管理論理インターフェイスの間で共有できます。

管理インターフェイス

管理論理インターフェイスはデバイスの他のインターフェイスから切り離されています。これは、Firepower Management Center にデバイスを設定し、登録するために使用されます。また、固有の IP アドレスとスタティック ルーティングを使用します。管理インターフェイスを設定するには、CLI で **configure network** コマンドを使用します。管理インターフェイスを Firepower Management Center に追加した後にその IP アドレスを CLI で変更した場合、Firepower Management Center での IP アドレスを **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Devices）] > [管理（Management）]** 領域で一致させることができます。

診断インターフェイス

診断論理インターフェイスは残りのデータ インターフェイスとともに、**[デバイス（Devices）]**> **[デバイス管理（Device Management）]** > **[インターフェイス（Interfaces）]** 画面で設定できます。診断インターフェイスの使用はオプションです（シナリオについては、ルーテッドモードおよびトランスペアレントモードの展開を参照）。診断インターフェイスは管理トラフィックのみを許可し、トラフィックのスルーは許可しません。これはSSHをサポートしません。データ インターフェイスまたは管理インターフェイスのみに SSH を使用できます。診断インターフェイスは、SNMP や syslog のモニタリングに役立ちます。

インターフェイス モードとタイプ

通常のファイアウォール モードと IPS 専用モードの 2 つのモードで FTD インターフェイスを展開できます。同じデバイスにファイアウォールインターフェイスとIPS専用インターフェイスの両方を含めることができます。

通常のファイアウォール モード

ファイアウォール モードのインターフェイスでは、トラフィックが、フローの維持、IP レイヤおよび TCP レイヤの両方でのフロー状態の追跡、IP 最適化、TCP の正規化などのファイアウォール機能の対象となります。オプションで、セキュリティポリシーに従ってこのトラフィックに IPS 機能を設定することもできます。

設定できるファイアウォール インターフェイスのタイプは、ルーテッド モードとトランスペアレントモードのどちらのファイアウォールモードがそのデバイスに設定されているかによって異なります。詳細については、Firepower Threat Defense 用のトランスペアレントまたはルーテッド ファイアウォール モードを参照してください。

- ルーテッドモードインターフェイス（ルーテッド ファイアウォール モードのみ）：ルーティングを行う各インターフェイスは異なるサブネット上にあります。
- ブリッジグループ インターフェイス（ルーテッドおよびトランスペアレント ファイアウォールモード）：複数のインターフェイスをネットワーク上でグループ化することができ、Firepower Threat Defense デバイスはブリッジング技術を使用してインターフェイス間のトラフィックを通過させることができます。各ブリッジグループには、ネットワーク上で IP アドレスが割り当てられるブリッジ仮想インターフェイス（BVI）が含まれます。ルーテッド モードでは、Firepower Threat Defense デバイスは BVI と通常のルーテッド インターフェイス間をルーティングします。トランスペアレントモードでは、各ブリッジグループは分離されていて、相互通信できません。

IPS 専用モード

IPS専用モードのインターフェイスは、多数のファイアウォールのチェックをバイパスし、IPS セキュリティポリシーのみをサポートします。別のファイアウォールがこれらのインターフェイスを保護していて、ファイアウォール機能のオーバーヘッドを避けたい場合、IPS 専用のインターフェイスを実装することがあります。

（注） ファイアウォール モードは通常のファイアウォール インターフェイスのみに影響し、インライン セットやパッシブ インターフェイスなどの IPS 専用インターフェイスには影響しません。IPS 専用インターフェイスはどちらのファイアウォール モードでも使用できます。

IPS 専用インターフェイスは以下のタイプとして展開できます。

- インライン セット、タップ モードのオプションあり：インライン セットは「Bump In The Wire」のように動作し、2 つのインターフェイスを一緒にバインドし、既存のネットワークに組み込みます。この機能によって、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することができます。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。

  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。ただし、これらのタイプのルールでは、トリガーされた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、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間の配線をセットアップし、デバイスで生成される侵入イベントのタイプ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ドロップ 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。

  （注） 「透過インライン セット」としてインライン セットに馴染みがある人もいますが、インライン インターフェイスのタイプはトランスペアレント ファイアウォール モードやファイアウォール タイプのインターフェイスとは無関係です。

- パッシブまたは ERSPAN パッシブ：パッシブ インターフェイスは、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。この機能により、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。Encapsulated Remote Switched Port Analyzer（ERSPAN）インターフェイスは、複数のスイッチに分散された送信元ポートからのトラフィックをモニタし、GRE を使用してトラフィックをカプセル化します。

ERSPAN インターフェイスは、デバイスがルーテッド ファイアウォール モードになっている場合にのみ許可されます。

セキュリティ ゾーンとインターフェイス グループ

各インターフェイスは、セキュリティ ゾーンおよび/またはインターフェイス グループに割り当てる必要があります。その上で、ゾーンまたはグループに基づいてセキュリティ ポリシーを適用します。たとえば、内部インターフェイスを内部ゾーンに割り当て、外部インターフェイスを外部ゾーンに割り当てることができます。また、たとえば、トラフィックが内部から外部に移動できるようにアクセス コントロール ポリシーを設定することはできますが、外部から内部に向けては設定できません。 ポリシーによっては、セキュリティ ゾーンだけをサポートする場合も、ゾーンとグループの両方をサポートする場合もあります。詳細については、インターフェイス オブジェクト：インターフェイスグループとセキュリティ ゾーンを参照してください。セキュリティ ゾーンおよびインターフェイス グループは、[オブジェクト（Objects）] ページで作成できます。また、インターフェイスを設定する際にゾーンを追加することもできます。インターフェイスは、そのインターフェイスに適切なタイプのゾーン（パッシブ、インライン、ルーテッド、スイッチド ゾーン タイプ）にのみ追加できます。

診断/管理インターフェイスは、ゾーンまたはインターフェイス グループには属しません。

Auto-MDI/MDIX 機能

RJ-45 インターフェイスでは、デフォルトの自動ネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX を有効にするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションが無効にされ、Auto-MDI/MDIX も無効になります。ギガビット イーサネットの速度と二重通信をそれぞれ 1000 と全二重に設定すると、インターフェイスでは常にオートネゴシエーションが実行されるため、Auto-MDI/MDIX は常に有効になり、無効にできません。

インターフェイスのデフォルト設定

この項では、インターフェイスのデフォルト設定を示します。

インターフェイスのデフォルトの状態

インターフェイスの状態は、タイプによって異なります。

- 物理インターフェイス：ディセーブル。初期セットアップで有効になる診断インターフェイスは例外です。

- 冗長インターフェイス：イネーブル。ただし、トラフィックが冗長インターフェイスを通過するためには、メンバ物理インターフェイスもイネーブルになっている必要があります。
- VLANサブインターフェイス：イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。
- EtherChannelポートチャネルインターフェイス（ASAモデル）：有効。ただし、トラフィックがEtherChannelを通過するためには、チャネルグループ物理インターフェイスもイネーブルになっている必要があります。
- EtherChannel ポートチャネル インターフェイス（Firepower モデル）：無効。

（注） Firepower 4100/9300 の場合、管理上、シャーシおよび FMC の両方で、インターフェイスを有効および無効にできます。インターフェイスを動作させるには、両方のオペレーティング システムで、インターフェイスを有効にする必要があります。インターフェイスの状態は個別に制御されるので、シャーシと FMC の間の不一致が生じることがあります。

デフォルトの速度および二重通信

デフォルトでは、銅線（RJ-45）インターフェイスの速度とデュプレックスは、オートネゴシエーションに設定されます。

物理インターフェイスの有効化およびイーサネット設定の構成

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**）
任意（Any）	該当なし	FTD	任意（Any）	Admin Access Admin Network Admin

ここでは、次の方法について説明します。

- 物理インターフェイスを有効にします。デフォルトでは、物理インターフェイスは無効になっています（診断 インターフェイスを除く）。
- 特定の速度と二重通信を設定します。デフォルトでは、速度とデュプレックスは [自動（Auto）] に設定されます。

この手順は、インターフェイス設定のごく一部にすぎません。この時点では、他のパラメータを設定しないようにします。たとえば、EtherChannel または冗長インターフェイスの一部として使用するインターフェイスには名前を付けることはできません。

（注） Firepower 4100/9300 の場合、FXOS の基本インターフェイスの設定を行います。詳細については、物理インターフェイスの設定を参照してください。

始める前に

FMC に追加した後、デバイスの物理インターフェイスを変更した場合、[インターフェイス（Interfaces）] タブの左上にある [デバイスからのインターフェイスの同期（Sync Interfaces from device）] ボタンをクリックしてそのインターフェイス リストを更新する必要があります。

手順

ステップ 1 **[Devices]** > **[Device Management]** の順に選択し、FTD デバイスの編集アイコン（）をクリックします。デフォルトで [インターフェイス（Interfaces）] タブが選択されています。

ステップ 2 編集するインターフェイスの編集アイコン（）をクリックします。

ステップ 3 [有効（Enabled）] チェック ボックスをオンにして、インターフェイスを有効化します。

ステップ 4 （任意） [説明（Description）] フィールドに説明を追加します。

説明は 200 文字以内で、改行を入れずに 1 行で入力します。

ステップ 5 （任意） [ハードウェア構成（Hardware Configuration）] タブをクリックして、デュプレックスと速度を設定します。

- [デュプレックス（Duplex）] : [全（Full）]、[半（Half）]、または [自動（Auto）] を選択します。[自動（Auto）]は、インターフェイスによってサポートされる場合のみデフォルトとなります。たとえば、Firepower 2100 シリーズの SFP インターフェイスでは [自動（Auto）] を選択できません。
- [速度（Speed）] : [10]、[100]、[1000]、または [自動（Auto）] を選択します。デフォルトは [自動（Auto）] です。インターフェイスのタイプによって、選択可能なオプションが制限されます。たとえば、Firepower 2100 シリーズ デバイスでは、GigabitEthernet ポートでは 10、100、1000（1Gbps）、SFP ポートでは 1000 または 10000（10 Gbps）を選択できます。Firepower 2100 シリーズ デバイスの SFP インターフェイスは、[自動（Auto）] をサポートしていないことに注意してください。

ステップ 6 [モード（Mode）] ドロップダウン リストで、次のいずれかを選択します。

- [なし（None）]: この設定を通常のファイアウォール インターフェイスおよびインライン セットに選択します。他の設定に基づいて [ルーテッド（Routed）]、[スイッチド（Switched）]、または [インライン（Inline）] にモードが自動的に変更されます。

- [パッシブ（Passive）]：この設定を IPS 専用インターフェイスに選択します。
- [Erspan]：この設定を Erspan パッシブ IPS 専用インターフェイスに選択します。

ステップ 7 [OK] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

これで、[展開（Deploy）] をクリックし、割り当てたデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。

インターフェイスの変更と Firepower Management Center の同期

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**）
任意（Any）	該当なし	FTD	任意（Any）	Admin Access Admin Network Admin

デバイスのインターフェイスの設定を変更することによって FMC とデバイスが同期しなくなる可能性があります。FMC は次の方法のいずれかでインターフェイスの変更を検出できます。

- デバイスから送信されたイベント
- からの展開の同期 FMC

  展開を試行したときに FMC がインターフェイスを検出すると、その展開は失敗します。最初にインターフェイスの変更を承認する必要があります。

- 手動同期

FMC が変更を検出すると、[インターフェイス（Interface）] タブの各インターフェイス アイコンの左側にステータス アイコン（[削除済み（removed）]、[変更済み（changed）]、または [追加済み（added）]）が表示されます。

新しいインターフェイスを追加したり、未使用のインターフェイスを削除したりしても、FTD の設定に与える影響は最小限です。ただし、セキュリティ ポリシーで使用されているインターフェイスを削除すると、設定に影響を与えます。インターフェイスは、アクセス ルール、NAT、SSL、アイデンティティ ルール、VPN、DHCP サーバなど、FTD の設定における多くの場所で直接参照されている可能性があります。インターフェイスを削除すると、そのインターフェイスに関連付けられている設定がすべて削除されます。セキュリティ ゾーンを参照するポリシーは影響を受けません。また、論理デバイスに影響を与えず、かつ FMC での同期を必要とせずに、割り当てられた EtherChannel のメンバーシップを編集できます。

この手順では、必要に応じてデバイスの変更を手動で同期する方法と、検出された変更を保存する方法について説明します。デバイスの変更が一時的なものである場合は、その変更をFMCに保存する必要はありません。デバイスが安定するまで待機してから再同期します。

手順

ステップ 1 **[Devices]** > **[Device Management]** の順に選択し、FTD デバイスの編集アイコン（  ）をクリックします。デフォルトで [インターフェイス（Interfaces）] タブが選択されています。

ステップ 2 必要に応じて、[インターフェイス（Interfaces）] タブの左上にある [デバイスの同期（Sync Device）] ボタンをクリックします。

ステップ 3 変更が検出されると、インターフェイス設定が変更されたことを示す赤色のバナーが [インターフェイス（Interfaces）] タブに表示されます。[クリックして詳細を表示（Click to know more）] リンクをクリックしてインターフェイスの変更内容を表示します。

ステップ 4 [変更の検証（Validate Changes）] をクリックし、インターフェイスが変更されてもポリシーが機能していることを確認します。

エラーがある場合は、ポリシーを変更して検証に戻る必要があります。

ステップ 5 [保存（Save）] をクリックします。

これで、[展開（Deploy）] をクリックし、割り当てたデバイスにポリシーを展開できます。変更はポリシーを導入するまで有効になりません。