Firepower Threat Defense の通常のファイアウォール インターフェイス

この章では、 EtherChannel、VLAN サブインターフェイス、IP アドレスなどを含む通常のファイアウォール FTD インターフェイスの設定について説明します。

（注） Firepower 4100/9300 の最初のインターフェイスの設定については、インターフェイスの設定を参照してください。

- EtherChannel と冗長インターフェイスの設定 （1 ページ）
- VLAN サブインターフェイスと 802.1Q トランキングの設定 （11 ページ）
- ルーテッドモードとトランスペアレントモードのインターフェイスの設定 （14 ページ）
- 高度なインターフェイスの設定 （35 ページ）
- Firepower Threat Defense の通常のファイアウォール インターフェイスの履歴 （48 ページ）

EtherChannel と冗長インターフェイスの設定

このセクションでは、EtherChannel インターフェイスと冗長インターフェイスを設定する方法について説明します。

（注） Firepower 4100/9300 の場合は、FXOS の EtherChannel を設定します。詳細については、EtherChannel（ポート チャネル）の追加を参照してください。冗長インターフェイスはサポートされません。

EtherChannel インターフェイスと冗長インターフェイスについて

ここでは、EtherChannel インターフェイスと冗長インターフェイスについて説明します。

冗長インターフェイスについて

論理冗長インターフェイスは、物理インターフェイスのペア（アクティブ インターフェイスとスタンバイ インターフェイス）で構成されます。アクティブ インターフェイスで障害が発生すると、スタンバイ インターフェイスがアクティブになって、トラフィックを通過させ始めます。冗長インターフェイスを設定してFirepower Threat Defense デバイスの信頼性を高めることができます。

最大 8 個の冗長インターフェイス ペアを設定できます。

冗長インターフェイスの MAC アドレス

冗長インターフェイスでは、追加した最初の物理インターフェイスの MAC アドレスを使用します。コンフィギュレーションでメンバー インターフェイスの順序を変更すると、MAC アドレスは、リストの最初になったインターフェイスの MAC アドレスと一致するように変更されます。または、冗長インターフェイスに手動で MAC アドレスを割り当てることができます。これはメンバー インターフェイスの MAC アドレスに関係なく使用されます。アクティブ インターフェイスがスタンバイ インターフェイスにフェールオーバーすると、トラフィックが中断しないように同じ MAC アドレスが維持されます。

EtherChannels について

802.3ad EtherChannel は、単一のネットワークの帯域幅を増やすことができるように、個別のイーサネット リンク（チャネル グループ）のバンドルで構成される論理インターフェイスです（ポートチャネル インターフェイスと呼びます）。ポートチャネル インターフェイスは、インターフェイス関連の機能を設定するときに、物理インターフェイスと同じように使用します。

モデルでサポートされているインターフェイスの数に応じて、最大 48 個の Etherchannel を設定できます。

チャネル グループ インターフェイス

各チャネル グループには、最大 16 個のアクティブ インターフェイスを持たせることができます。ただし、Firepower 2100 は、8 個のアクティブ インターフェイスをサポートしています。8 個のアクティブ インターフェイスだけをサポートするスイッチの場合、1 つのチャネル グループに最大 16 個のインターフェイスを割り当てることができます。インターフェイスは 8 個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイ リンクとして動作できます。16 個のアクティブ インターフェイスの場合、スイッチがこの機能をサポートしている必要があります（たとえば、Cisco Nexus 7000 と F2 シリーズ 10 ギガビット イーサネット モジュール）。

チャネル グループのインターフェイスはすべて、同じタイプおよび同じ速度である必要があります。チャネル グループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。

EtherChannelによって、チャネル内の使用可能なすべてのアクティブ インターフェイスのトラフィックが集約されます。インターフェイスは、送信元または宛先 MAC アドレス、IP アドレ

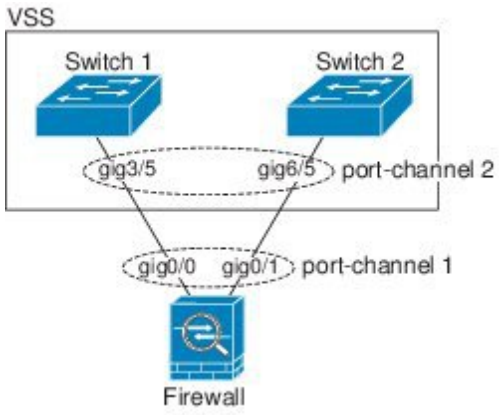
ス、TCP および UDP ポート番号、および VLAN 番号に基づいて、独自のハッシュ アルゴリズムを使用して選択されます。

別のデバイスの EtherChannel への接続

FTD EtherChannel の接続先のデバイスも 802.3ad EtherChannel をサポートしている必要があります。たとえば、Catalyst 6500 スイッチまたは Cisco Nexus 7000 に接続できます。

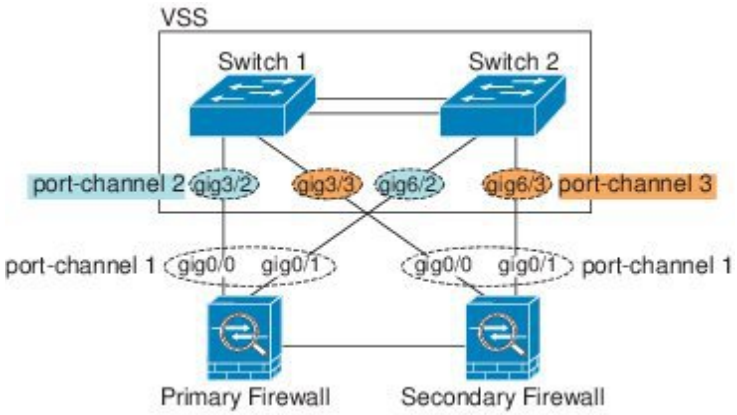
スイッチが仮想スイッチング システム（VSS）または 仮想ポート チャネル（vPC）の一部である場合、同じ EtherChannel 内の FTD インターフェイスを VSS/vPC 内の個別のスイッチに接続できます。スイッチ インターフェイスは同じ EtherChannel ポートチャネル インターフェイスのメンバです。複数の個別のスイッチが単一のスイッチのように動作するからです。

図 *1 : VSS/vPC* への接続



FTD をアクティブ/スタンバイ フェールオーバー配置で使用する場合、FTD ごとに 1 つ、VSS/vPC 内のスイッチで個別の EtherChannel を作成する必要があります。各 FTD で、1 つの EtherChannel が両方のスイッチに接続します。すべてのスイッチ インターフェイスを両方の FTD に接続する単一の EtherChannel にグループ化できる場合でも（この場合、個別の FTD システム ID のため、EtherChannel は確立されません）、単一の EtherChannel は望ましくありません。これは、トラフィックをスタンバイ FTD に送信しないようにするためです。

図 *2 :* アクティブ/スタンバイ フェールオーバーと *VSS/vPC*



リンク集約制御プロトコル

リンク集約制御プロトコル（LACP）では、2 つのネットワーク デバイス間でリンク集約制御プロトコル データ ユニット（LACPDU）を交換することによって、インターフェイスが集約されます。

EtherChannel 内の各物理インターフェイスを次のように設定できます。

- アクティブ：LACP アップデートを送信および受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。
- パッシブ：LACP アップデートを受信します。パッシブ EtherChannel は、アクティブ EtherChannel のみと接続を確立できます。Firepower ハードウェア モデルではサポートされていません。
- オン：EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。

LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバインターフェイスの両端が正しいチャネル グループに接続されていることがチェックされます。「オン」モードではインターフェイスがダウンしたときにチャネル グループ内のスタンバイ インターフェイスを使用できず、接続とコンフィギュレーションはチェックされません。

ロード バランシング

FTD は、パケットの送信元および宛先 IP アドレスをハッシュすることによって、パケットを EtherChannel 内のインターフェイスに分散します（この基準は設定可能です）。生成されたハッシュ値をアクティブなリンクの数で割り、そのモジュロ演算で求められた余りの値によってフローの割り当て先のインターフェイスが決まります。*hash_value* **mod** *active_links* の結果が 0 となるすべてのパケットは、EtherChannel 内の最初のインターフェイスへ送信され、以降は結果が 1 となるものは 2 番目のインターフェイスへ、結果が 2 となるものは 3 番目のインターフェイスへ、というように送信されます。たとえば、15 個のアクティブ リンクがある場合、モジュロ演算では 0 ～ 14 の値が得られます。6 個のアクティブ リンクの場合、値は 0 ～ 5 となり、以降も同様になります。

アクティブ インターフェイスがダウンし、スタンバイ インターフェイスに置き換えられない場合、トラフィックは残りのリンク間で再バランスされます。失敗はレイヤ 2 のスパニングツリーとレイヤ 3 のルーティング テーブルの両方からマスクされるため、他のネットワーク デバイスへのスイッチオーバーはトランスペアレントです。

EtherChannel MAC アドレス

1 つのチャネル グループに含まれるすべてのインターフェイスは、同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワーク アプリケーションとユーザに対してトランスペアレントになります。ネットワーク アプリケーションやユーザから見えるのは 1 つの論理接続のみであり、個々のリンクのことは認識しないからです。

ポートチャネルインターフェイスは、最も小さいチャネル グループ インターフェイスの MAC アドレスをポート チャネル MAC アドレスとして使用します。または、ポート チャネル インターフェイスの MAC アドレスを手動で設定することもできます。グループ チャネル インターフェイスのメンバーシップを変更する場合は、固有の MAC アドレスを設定することを推奨します。ポート チャネル MAC アドレスを提供していたインターフェイスを削除すると、そのポートチャネル MAC アドレスは次に番号が小さいインターフェイスに変わるため、トラフィックが分断されます。

EtherChannel と冗長インターフェイの注意事項

ブリッジ グループ

ルーテッド モードでは、FMC で定義された EtherChannel はブリッジ グループ メンバーとしてサポートされません。Firepower 4100/9300 上の Etherchannel は、ブリッジ グループ メンバーにすることができます。

ハイ アベイラビリティ

- 冗長インターフェイスまたは EtherChannel インターフェイスを ハイ アベイラビリティ リンクとして使用する場合、ハイ アベイラビリティ ペアの両方のユニットでその事前設定を行う必要があります。プライマリ ユニットで設定し、セカンダリ装置に複製されることは想定できません。これは、複製には ハイ アベイラビリティ リンク自体が必要であるためです。
- 冗長インターフェイスまたは EtherChannel インターフェイスをステート リンクに対して使用する場合、特別なコンフィギュレーションは必要ありません。コンフィギュレーションは通常どおりプライマリ装置から複製されます。Firepower 4100/9300 シャーシ では、Etherchannel を含むすべてのインターフェイスを両方のユニットで事前に設定する必要があります。
- **monitor-interface** コマンドを使用して、ハイ アベイラビリティ。アクティブなメンバ インターフェイスがスタンバイ インターフェイスにフェールオーバーした場合、デバイスレベルのハイ アベイラビリティを監視しているときには冗長インターフェイスまたは EtherChannel インターフェイスで障害が発生しているようには見えません。すべての物理インターフェイスで障害が発生した場合にのみ、冗長インターフェイスまたは EtherChannel インターフェイスで障害が発生しているように見えます（EtherChannel インターフェイスでは、障害の発生が許容されるメンバ インターフェイスの数を設定できます）。
- EtherChannel インターフェイスをハイ アベイラビリティ リンクまたはステート リンクに対して使用する場合、順序が不正なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。ハイ アベイラビリティ リンクとして使用中の EtherChannel の設定は変更できません。設定を変更するには、ハイ アベイラビリティを一時的に無効にする必要があります。これにより、ハイ アベイラビリティ がその期間に発生することはありません。

モデルのサポート

- Firepower 4100/9300 または FTDv では FMC に Etherchannel を追加することはできません。Firepower 4100/9300 は Etherchannel をサポートしていますが、シャーシ上の FXOS で Etherchannel のすべてのハードウェア設定を実行する必要があります。
- Firepower 2100、Firepower 4100/9300 シャーシでは、冗長インターフェイスはサポートされていません。

冗長インターフェイスの一般的なガイドライン

- 最大 8 個の冗長インターフェイス ペアを設定できます。
- すべてのFTD コンフィギュレーションは、メンバ物理インターフェイスではなく論理冗長インターフェイスを参照します。
- EtherChannel の一部として冗長インターフェイスを使用することはできません。また、冗長インターフェイスの一部として EtherChannel を使用することはできません。冗長インターフェイスと EtherChannel インターフェイスでは同じ物理インターフェイスを使用できません。ただし、同じ物理インターフェイスを使用するのでなければ、両方のタイプを FTD 上で設定することができます。
- アクティブ インターフェイスをシャットダウンすると、スタンバイ インターフェイスがアクティブになります。
- 冗長インターフェイスは、診断 *slot*/*port* インターフェイスをメンバーとしてサポートしません。ただし、診断インターフェイス以外の複数インターフェイスからなる冗長インターフェイスを、管理専用として設定できます。

EtherChannel の一般的なガイドライン

- モデルで使用可能なインターフェイスの数に応じて、最大 48 個の Etherchannel を設定できます。
- 各チャネル グループには、最大 16 個のアクティブ インターフェイスを持たせることができます。ただし、Firepower 2100 は、8 個のアクティブ インターフェイスをサポートしています。8 個のアクティブ インターフェイスだけをサポートするスイッチの場合、1 つのチャネル グループに最大 16 個のインターフェイスを割り当てることができます。インターフェイスは 8 個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイ リンクとして動作できます。16 個のアクティブ インターフェイスの場合、スイッチがこの機能をサポートしている必要があります（たとえば、Cisco Nexus 7000 と F2 シリーズ 10 ギガビット イーサネット モジュール）。
- チャネル グループのインターフェイスはすべて、同じタイプおよび同じ速度である必要があります。チャネル グループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。
- FTD の EtherChannel の接続先デバイスも 802.3ad EtherChannel をサポートしている必要があります。

- FTD は、VLAN タグ付きの LACPDU をサポートしていません。Cisco IOS **vlan dot1Q tag native** コマンドを使用して、隣接スイッチのネイティブ VLAN タギングをイネーブルにすると FTD はタグ付きの LACPDU をドロップします。隣接スイッチのネイティブ VLAN タギングは、必ずディセーブルにしてください。
- 15.1(1)S2 以前の Cisco IOS ソフトウェア バージョンを実行する FTD では、スイッチ スタックへの EtherChannel の接続がサポートされていませんでした。デフォルトのスイッチ設定では、FTD EtherChannel がクロス スタックに接続されている場合、マスター スイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。互換性を高めるため、**stack-mac persistent timer** コマンドを設定して、十分なリロード時間を確保できる大きな値、たとえば 8 分、0（無制限）などを設定します。または、15.1(1)S2 など、より安定したスイッチ ソフトウェア バージョンにアップグレードできます。
- すべての FTD コンフィギュレーションは、メンバ物理インターフェイスではなく論理 EtherChannel インターフェイスを参照します。
- EtherChannel の一部として冗長インターフェイスを使用することはできません。また、冗長インターフェイスの一部として EtherChannel を使用することはできません。冗長インターフェイスと EtherChannel インターフェイスでは同じ物理インターフェイスを使用できません。ただし、同じ物理インターフェイスを使用するのでなければ、両方のタイプを FTD 上で設定することができます。

冗長インターフェイスの設定

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

論理冗長インターフェイスは、物理インターフェイスのペア（アクティブ インターフェイスとスタンバイ インターフェイス）で構成されます。アクティブ インターフェイスで障害が発生すると、スタンバイ インターフェイスがアクティブになって、トラフィックを通過させ始めます。冗長インターフェイスを設定してFTDの信頼性を高めることができます。デフォルトでは、冗長インターフェイスは有効になっています。

- 最大 8 個の冗長インターフェイス ペアを設定できます。
- 両方のメンバー インターフェイスが同じ物理タイプである必要があります。たとえば、両方ともギガビット イーサネットにする必要があります。

（注） 冗長インターフェイスは Firepower 4100/9300 ではサポートされていません。

始める前に

- 名前が設定されている場合は、物理インターフェイスを冗長インターフェイスに追加できません。最初に名前を削除する必要があります。

> ⚠ **注意** コンフィギュレーション内で物理インターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

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 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に従って、メンバー インターフェイスを有効にします。

ステップ 3 **[インターフェイスの追加（Add Interfaces）]** > **[冗長インターフェイス（Redundant Interface）]** をクリックします。

ステップ 4 [一般（General）] タブで、次のパラメータを設定します。

a) [冗長 ID（Redundant ID）]：1 ～ 8 の整数を設定します。

b) [プライマリ インターフェイス（Primary Interface）]：ドロップダウン リストからインターフェイスを選択します。インターフェイスを追加すると、インターフェイスのコンフィギュレーション（IP アドレスなど）はすべて削除されます。

c) [セカンダリ インターフェイス（Secondary Interface）]：2 番目のインターフェイスは、最初のインターフェイスと同じ物理的なタイプである必要があります。

ステップ 5 [OK] をクリックします。

ステップ 6 [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。

ステップ 7 （任意） VLAN サブインターフェイスを追加します。サブインターフェイスの追加 （13 ページ）を参照してください。

ステップ 8 ルーテッドまたはトランスペアレント モード インターフェイスのパラメータを設定します。ルーテッド モードのインターフェイスの設定 （18 ページ）またはのブリッジグループ インターフェイスの設定 （21 ページ）を参照してください。

EtherChannel の設定

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、EtherChannel ポートチャネル インターフェイスの作成、インターフェイスの EtherChannel への割り当て、EtherChannel のカスタマイズ方法について説明します。

ガイドライン

- モデルのインターフェイスの数に応じて、最大 48 個の Etherchannel を設定できます。
- 各チャネル グループには、最大 16 個のアクティブ インターフェイスを持たせることができます。ただし、Firepower 2100 は、8 個のアクティブ インターフェイスをサポートしています。8 個のアクティブ インターフェイスだけをサポートするスイッチの場合、1 つのチャネル グループに最大 16 個のインターフェイスを割り当てることができます。インターフェイスは 8 個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイ リンクとして動作できます。
- チャネル グループのすべてのインターフェイスは、同じタイプ、速度、および二重通信である必要があります。半二重はサポートされません。

（注） Firepower 4100/9300 の場合は、FXOS の EtherChannel を設定します。詳細については、EtherChannel（ポート チャネル）の追加を参照してください。

始める前に

- 名前が設定されている場合は、物理インターフェイスをチャネル グループに追加できません。最初に名前を削除する必要があります。

（注） コンフィギュレーション内で物理インターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

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 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に従って、メンバー インターフェイスを有効にします。

ステップ 3 **[インターフェイスの追加（Add Interfaces）] > [Ether Channel インターフェイス（Ether Channel Interface）]** をクリックします。

ステップ 4 [一般（General）] タブで、[イーサネットチャネルID（Ether Channel ID）] を 1 ～ 48の数値に設定します。

ステップ 5 [使用可能なインターフェイス（Available Interfaces）] 領域でインターフェイスをクリックし、[追加（Add）] をクリックして [選択したインターフェイス（Selected Interface）] 領域にそのインターフェイスを移動します。メンバーを作成するすべてのインターフェイスに対して繰り返します。

すべてのインターフェイスが同じタイプと速度であるようにします。最初に追加するインターフェイスによって、EtherChannel のタイプと速度が決まります。一致しないインターフェイスを追加すると、そのインターフェイスは停止状態になります。FMC では、一致しないインターフェイスの追加は防止されません。

ステップ 6 （任意）[詳細（Advanced）] タブをクリックして EtherChannel をカスタマイズします。[情報（Information）] サブタブで次のパラメータを設定します。

- （ASA 5500-X モデルのみ）[ロードバランシング（Load Balance）]：パケットをグループ チャネル インターフェイス間でロード バランスするために使用する基準を選択します。デフォルトでは、FTD デバイスはパケットの送信元および宛先 IP アドレスに従って、インターフェイスでのパケットのロードをバランスします。パケットが分類される基準になるプロパティを変更する場合は、別の基準のセットを選択します。たとえば、トラフィックが同じ送信元および宛先 IP アドレスに大きく偏っている場合、EtherChannel 内のインターフェイスに対するトラフィックの割り当てがアンバランスになります。別のアルゴリズムに変更すると、トラフィックはより均等に分散される場合があります。ロードバランシングの詳細については、ロード バランシング （4 ページ）を参照してください。
- [LACP モード（LACP Mode）]：[アクティブ（Active）]、[パッシブ（Passive）]、または [オン（On）] を選択します。[アクティブ（Active）] モード（デフォルト）を使用することを推奨します。
- （ASA 5500-X モデルのみ）[アクティブな物理インターフェイス：範囲（Active Physical Interface: Range）]：左側のドロップダウン リストから、EtherChannel をアクティブにするために必要なアクティブ インターフェイスの最小数を 1 ～ 16 の範囲で選択します。デフォルトは 1 です。右側のドロップダウン リストから、EtherChannel で許可されるアクティブ インターフェイスの最大数を 1 ～ 16 の範囲で選択します。デフォルトは 16 です。スイッチが 16 個のアクティブ インターフェイスをサポートしていない場合、このコマンドは必ず 8 以下に設定する必要があります。
- [アクティブな MAC アドレス（Active Mac Address）]：必要に応じて手動 MAC アドレスを設定します。mac_address は、H.H.H 形式で指定します。H は 16 ビットの 16 進数です。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は、000C.F142.4CDE と入力します。

ステップ 7 （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、すべてのメンバーインターフェイスでこれらの設定を上書きします。これらの

パラメータはチャネル グループのすべてのインターフェイスで一致している必要があるため、この方法はこれらのパラメータを設定するショートカットになります。

ステップ 8 [OK] をクリックします。

ステップ 9 [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。

ステップ 10 （任意） VLAN サブインターフェイスを追加します。サブインターフェイスの追加 （13 ページ）を参照してください。

ステップ 11 ルーテッドまたはトランスペアレント モード インターフェイスのパラメータを設定します。ルーテッド モードのインターフェイスの設定 （18 ページ）またはのブリッジグループ インターフェイスの設定 （21 ページ）を参照してください。

VLAN サブインターフェイスと 802.1Q トランキングの設定

VLAN サブインターフェイスを使用すると、1 つの物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスを、異なる VLAN ID でタグ付けされた複数の論理インターフェイスに分割できます。VLAN サブインターフェイスが 1 つ以上あるインターフェイスは、自動的に 802.1Q トランクとして設定されます。VLAN では、所定の物理インターフェイス上でトラフィックを分離しておくことができるため、物理インターフェイスまたはデバイスを追加しなくても、ネットワーク上で使用できるインターフェイスの数を増やすことができます。

VLAN サブインターフェイスのガイドラインと制限事項

高可用性

フェールオーバー リンクまたは状態リンクにサブインターフェイスを使用することはできません。ただし、コンテナ インターフェイスの場合は Firepower 4100/9300 シャーシに定義されているサブインターフェイスを使用できます。

その他のガイドライン

- 物理インターフェイス上のタグなしパケットの禁止：サブインターフェイスを使用する場合、物理インターフェイスでトラフィックを通過させないようにすることもよくあります。物理インターフェイスはタグのないパケットを通過させることができるためです。この特性は、冗長インターフェイス ペアのアクティブな物理インターフェイスと EtherChannel リンクにも当てはまります。サブインターフェイスでトラフィックを通過させるには物理、冗長、または EtherChannel インターフェイスを有効にする必要があるため、インターフェイスに名前を設定しないことでトラフィックを通過させないようにします。物理イン

ターフェイス、冗長インターフェイス、またはEtherChannelインターフェイスでタグのないパケットを通過させる場合は、通常通り名前を設定できます。

- 診断インターフェイスではサブインターフェイスを設定できません。
- 同じ親インターフェイスのすべてのサブインターフェイスは、ブリッジグループメンバーかルーテッドインターフェイスのいずれかである必要があります。混在および一致はできません。
- FTD はダイナミック トランキング プロトコル（DTP）をサポートしないため、接続されているスイッチ ポートを無条件にトランキングするように設定する必要があります。
- 親インターフェイスの同じ Burned-In MAC Address を使用するので、FTD で定義されたサブインターフェイスに一意の MAC アドレスを割り当てることもできます。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。また、IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカル アドレスが可能になり、FTD で特定のインスタンスでのトラフィックの中断を避けることができます。

デバイス モデルによる VLAN サブインターフェイスの最大数

デバイス モデルにより、設定できる VLAN サブインターフェイスの最大数が制限されます。データ インターフェイスでのみサブインターフェイスを設定することができ、管理インターフェイスでは設定できないことに注意してください。

次の表で、各デバイス モデルの制限について説明します。

モデル	VLAN サブインターフェイスの最大数
Firepower 2100	1024
Firepower 4100	1024
Firepower 9300	1024
Firepower Threat Defense Virtual	50
ASA 5508-X	50
ASA 5515-X	100
ASA 5516-X	100
ASA 5525-X	200
ASA 5545-X	300
ASA 5555-X	500
ISA 3000	25

サブインターフェイスの追加

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

1 つ以上のサブインターフェイスを物理インターフェイス、冗長インターフェイス、または PortChannel インターフェイスに追加します。

Firepower 4100/9300 の場合、コンテナインターフェイスで使用するためのサブインターフェイスを FXOS で作成します。コンテナ インスタンスへの VLAN サブインターフェイスの追加を参照してください。これらのサブインターフェイスは FMC のインターフェイス リストに表示されます。FMC にサブインターフェイスを追加することもできますが、FXOS にサブインターフェイスが定義されていない親インターフェイス上に限ります。

（注） 親の物理インターフェイスがタグなしのパケットを渡します。タグなしのパケットを渡さない場合は、セキュリティ ポリシーの親インターフェイスが含まれていないことを確認します。

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 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に従って、親インターフェイスを有効にします。

ステップ 3 **[インターフェイスの追加（Add Interfaces）]** > **[インターフェイス（Sub Interface）]** をクリックします。

ステップ 4 [一般（General）] タブで、次のパラメータを設定します。

a) [インターフェイス（Interface）]：サブインターフェイスを追加する物理、冗長、またはポートチャネル インターフェイスを選択します。

b) [サブインターフェイス ID（Sub-Interface ID）]：サブインターフェイス ID を 1 ～ 4294967295 の範囲の整数で入力します。許可されるサブインターフェイスの番号は、プラットフォームによって異なります。設定後は ID を変更できません。

c) [VLAN ID]：VLAN ID を 1 ～ 4094 の範囲で入力します。これは、このサブインターフェイス上のパケットにタグを付けるために使用されます。

この VLAN ID は一意である必要があります。

ステップ 5 [OK] をクリックします。

ステップ 6 [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。

ステップ 7 ルーテッドまたはトランスペアレント モード インターフェイスのパラメータを設定します。ルーテッド モードのインターフェイスの設定 （18 ページ）またはのブリッジグループ インターフェイスの設定 （21 ページ）を参照してください。

ルーテッド モードとトランス ペアレント モードのインターフェイスの設定

この項では、ルーテッド ファイアウォール モードおよびトランスペアレント ファイアウォール モードで、すべてのモデルに対応する標準のインターフェイス設定を完了するためのタスクについて説明します。

ルーテッド モード インターフェイスとトランスペアレント モード インターフェイスについて

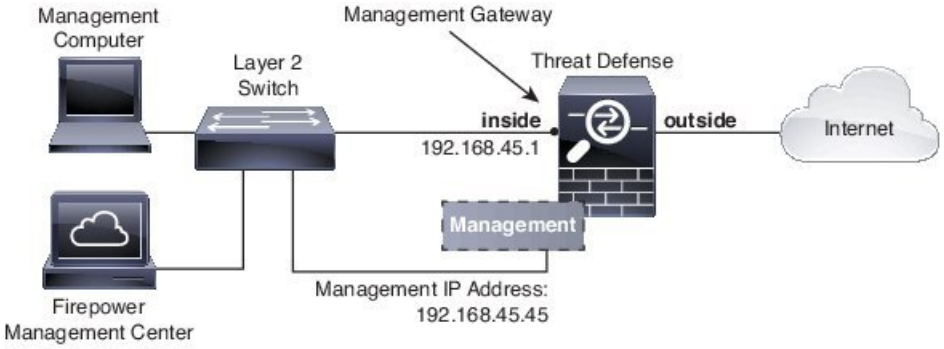
Firepower Threat Defense デバイス は、ルーテッドおよびブリッジという 2 つのタイプのインターフェイスをサポートします。

各レイヤ 3 ルーテッド インターフェイスに、固有のサブネット上の IP アドレスが必要です。

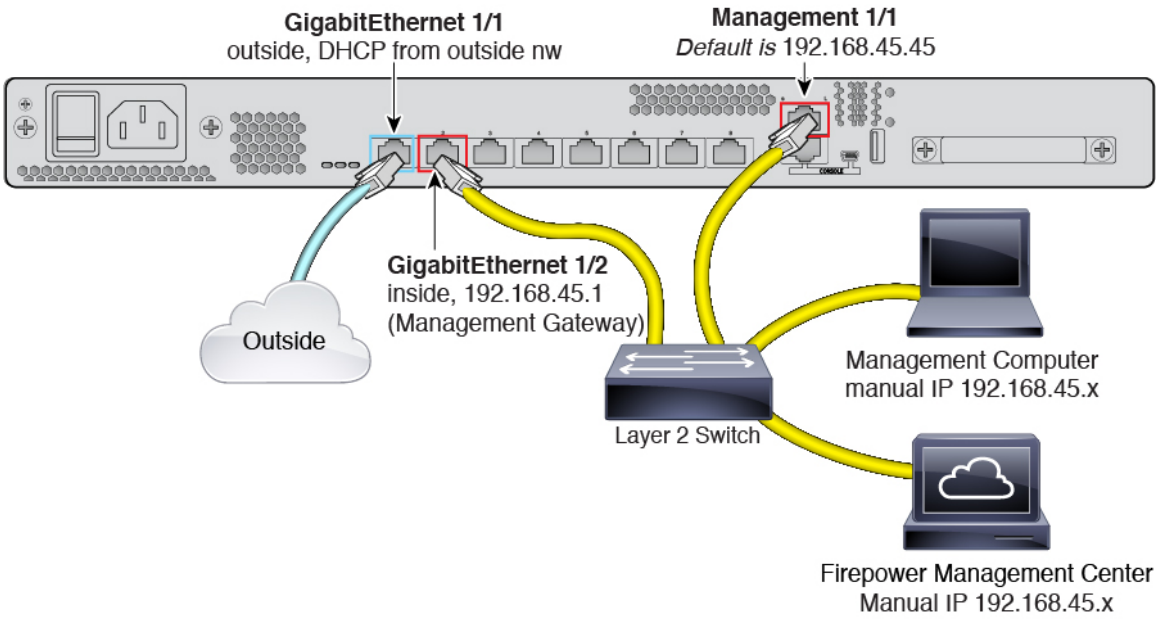
ブリッジされたインターフェイスはブリッジグループに属し、すべてのインターフェイスが同じネットワーク上にあります。ブリッジグループはブリッジ ネットワークに IP アドレスを持つブリッジ仮想インターフェイス（BVI）によって表されます。ルーテッド モードは、ルーテッド インターフェイスとブリッジ インターフェイスの両方をサポートし、ルーテッド インターフェイスと BVI との間のルーティングが可能です。トランスペアレント ファイアウォール モードでは、ブリッジ グループと BVI インターフェイスのみがサポートされます。

ルーテッド モードの導入

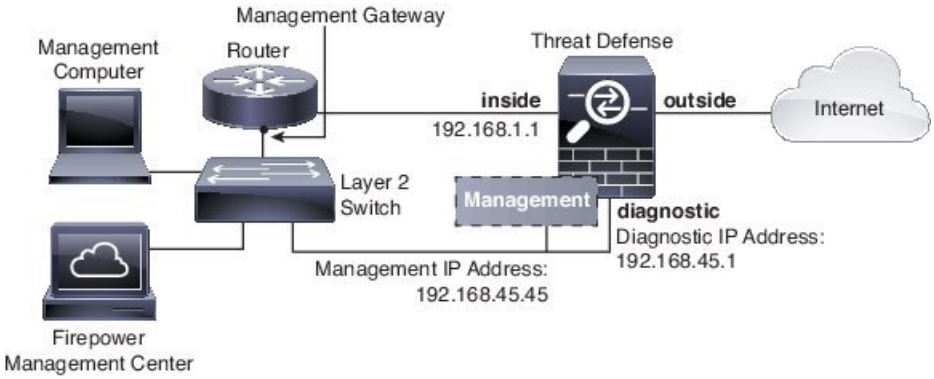
内部ルータがない場合は診断インターフェイスの IP アドレスを設定しないことをお勧めします。診断インターフェイスの IP アドレスを設定しなければ、他のデータ インターフェイスと同じネットワーク上に管理インターフェイスを配置できます。診断インターフェイスを設定すると、一般的にその IP アドレスは管理 IP アドレスと同じネットワークになり、他のデータ インターフェイスと同じネットワーク上に存在できない標準インターフェイスと見なされます。管理インターフェイスは更新のためにインターネットにアクセスする必要があるため、管理インターフェイスを内部インターフェイスと同じネットワーク上に置くと、内部にスイッチのみを持つ FTD デバイスを導入して、そのゲートウェイとして内部インターフェイスを指定できます。内部スイッチを使用する次の導入を参照してください。



ASA 5508-X、またはASA 5516-Xで上記のシナリオをケーブル接続するには、次を参照してください。

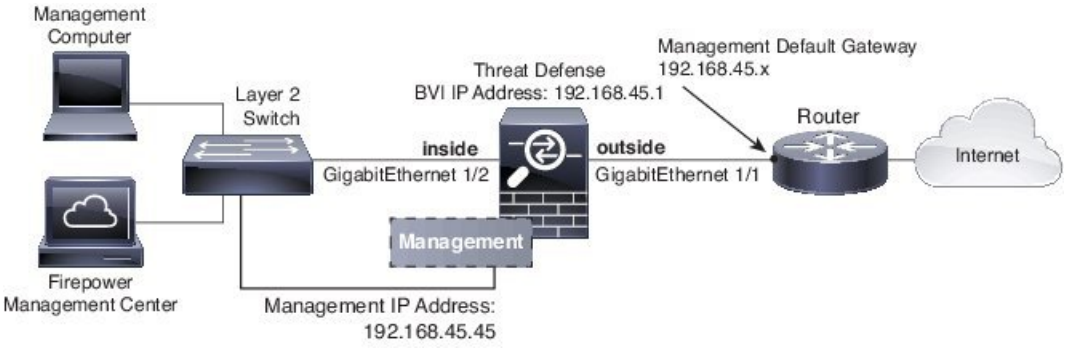


診断IPアドレスを設定する場合は、内部ルータが必要です。

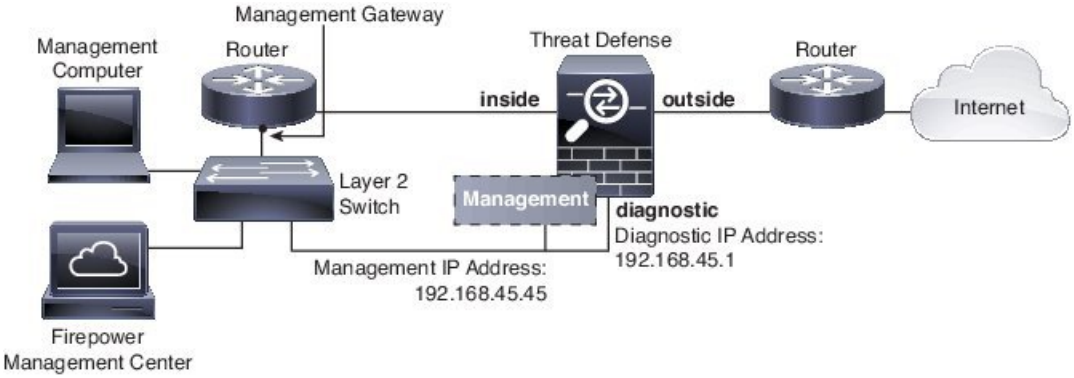


トランスペアレント モードの展開

ルーテッドモードの展開と同様、内部スイッチを使用したデバイスの展開を選択できます。この場合、診断インターフェイスを IP アドレスなしで維持する必要があります。



また、内部ルータを使用して展開することもできます。この場合、追加の管理アクセスのために、IP アドレスを持つ診断インターフェイスを使用できます。



デュアル IP スタック（IPv4 および IPv6）

Firepower Threat Defense デバイス は、インターフェイスで IPv6 アドレスと IPv4 アドレスの両方をサポートしています。IPv4 と IPv6 の両方で、デフォルト ルートを設定してください。

ルーテッド モードおよびトランスペアレント モードのインターフェイスのガイドラインおよび要件

ハイ アベイラビリティ

- フェールオーバー リンクは、この章の手順で設定しないでください。詳細については、「ハイ アベイラビリティ」の章を参照してください。
- ハイ アベイラビリティ を使用する場合、データ インターフェイスの IP アドレスとスタンバイ アドレスを手動で設定する必要があります。DHCP および PPPoE はサポートされません。[Monitored Interfaces] 領域の **[Devices]** > **[Device Management]** > **[High Availability]** タ

ブで、スタンバイ IP アドレスを設定します。詳細については、ハイ アベイラビリティの章も参照してください。

IPv6

- IPv6 はすべてのインターフェイスでサポートされます。
- トランスペアレント モードでは、IPv6 アドレスは手動でのみ設定できます。
- Firepower Threat Defense デバイスは、IPv6 エニーキャスト アドレスはサポートしません。

モデルのサポート

- Firepower 2100 シリーズでは、ルーテッド モードのブリッジ グループはサポートされません。
- Firepower Threat Defense Virtual では、ルーテッド モードのブリッジ グループはサポートされません。

トランスペアレント モードとブリッジ グループのガイドライン

- 64 のインターフェイスをもつブリッジグループを 250 まで作成できます。
- 直接接続された各ネットワークは同一のサブネット上にある必要があります。
- Firepower Threat Defense デバイス では、セカンダリ ネットワーク上のトラフィックはサポートされていません。BVI IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。
- IPv4 の場合は、管理トラフィックと、Firepower Threat Defense デバイス を通過するトラフィックの両方の各ブリッジ グループに対し、BVI の IP アドレスが必要です。IPv6 アドレスは BVI でサポートされますが必須ではありません。
- IPv6 アドレスは手動でのみ設定できます。
- BVI IP アドレスは、接続されたネットワークと同じサブネット内にある必要があります。サブネットにホスト サブネット（255.255.255.255）を設定することはできません。
- 管理インターフェイスはブリッジグループのメンバーとしてサポートされません。
- Firepower 4100/9300 では、データ共有インターフェイスはブリッジ グループのメンバーとしてサポートされません。
- トランスペアレント モードでは、少なくとも 1 つのブリッジ グループを使用し、データ インターフェイスがブリッジ グループに属している必要があります。
- トランスペアレント モードでは、接続されたデバイス用のデフォルト ゲートウェイとして BVI IP アドレスを指定しないでください。デバイスは Firepower Threat Defense デバイス の他方側のルータをデフォルト ゲートウェイとして指定する必要があります。

- トランスペアレントモードでは、管理トラフィックの戻りパスを指定するために必要なデフォルトルートは、1つのブリッジグループ ネットワークからの管理トラフィックにだけ適用されます。これは、デフォルト ルートはブリッジグループのインターフェイスとブリッジグループ ネットワークのルータ IP アドレスを指定しますが、ユーザは1つのデフォルト ルートしか定義できないためです。複数のブリッジグループ ネットワークからの管理トラフィックが存在する場合は、管理トラフィックの発信元ネットワークを識別する標準のスタティック ルートを指定する必要があります。
- トランスペアレント モードでは、PPPoE は 診断 インターフェイスでサポートされません。
- ルーテッドモードでは、ブリッジグループと他のルーテッドインターフェイスの間をルーティングするために、BVI を指定する必要があります。
- ルーテッド モードでは、FTD 定義の EtherChannel インターフェイスがブリッジ グループのメンバーとしてサポートされません。Firepower 4100/9300 上の Etherchannel は、ブリッジ グループ メンバーにすることができます。
- Bidirectional Forwarding Detection（BFD）エコー パケットは、ブリッジ グループ メンバを使用するときに、FTD を介して許可されません。BFD を実行している FTD の両側に 2 つのネイバーがある場合、FTD は BFD エコー パケットをドロップします。両方が同じ送信元および宛先 IP アドレスを持ち、LAND 攻撃の一部であるように見えるからです。

ルーテッド モードのインターフェイスの設定

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

この手順では、名前、セキュリティ ゾーン、および IPv4 アドレスを設定する方法について説明します。

始める前に

- **Firepower 4100/9300**
  1. 物理インターフェイスの設定
  2. （任意）特別なインターフェイスを設定します。
     - EtherChannel（ポート チャネル）の追加
     - コンテナ インスタンスへの VLAN サブインターフェイスの追加 FXOS で次を実行します。
     - FMC でのサブインターフェイスの追加 （13 ページ）

- （任意）**他のすべてのモデル**：
  - 冗長インターフェイスの設定 （7 ページ）
  - EtherChannel の設定 （9 ページ）
  - サブインターフェイスの追加 （13 ページ）

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 [名前（Name）] フィールドに、48 文字以内で名前を入力します。

ステップ 4 [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 5 （任意） このインターフェイスを [管理専用（Management Only）] に設定してトラフィックを管理トラフィックに制限します。through-the-box トラフィックは許可されていません。

ステップ 6 （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 7 [モード（Mode）] ドロップダウン リストで、[なし（None）] を選択します。

通常のファイアウォール インターフェイスのモードは [なし（None）] に設定されています。他のモードは IPS 専用インターフェイス タイプ向けです。

ステップ 8 [セキュリティ ゾーン（Security Zone）] ドロップダウン リストからセキュリティ ゾーンを選択するか、[新規（New）] をクリックして、新しいセキュリティ ゾーンを追加します。

ルーテッド インターフェイスは、ルーテッド タイプ インターフェイスであり、ルーテッド タイプのゾーンにのみ属することができます。

ステップ 9 **MTU** についてはMTU の設定 （41 ページ）を参照してください。

ステップ 10 [IPv4] タブをクリックします。IP アドレスを設定するには、[IP タイプ（IP Type）] ドロップダウン リストにある次のオプションのいずれかを使用します。

- [静的 IP を使用する（Use Static IP）]：IP アドレスおよびサブネット マスクを入力します。ハイ アベイラビリティの場合は、静的 IP アドレスのみを使用できます。[モニタ対象インターフェイス（Monitored Interfaces）] エリアの **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[ハイアベイラビリティ（High Availability）]** タブで、スタンバイ IP アドレスを設定します。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステートをトラックすることしかできません。
- [DHCP の使用（Use DHCP）]：次のオプションのパラメータを設定します。

- [DHCP を使用してデフォルト ルートを取得（Obtain default route using DHCP）]：DHCP サーバからデフォルト ルートを取得します。
- [DHCP ルートメトリック（DHCP route metric）]：アドミニストレーティブ ディスタンスを学習したルートに割り当てます（1 ～ 255）。学習したルートのデフォルトのアドミニストレーティブ ディスタンスは 1 です。

- [PPPoE を使用（Use PPPoE）]：インターフェイスが DSL、ケーブル モデム、またはその他の手段で ISP に接続されていて、ISP が PPPoE を使用して IP アドレスを割り当てる場合は、次のパラメータを設定します。
  - [VPDN グループ名（VPDN Group Name）]：この接続を表すために選択するグループ名を指定します。
  - [PPPoE ユーザ名（PPPoE User Name）]：ISP によって提供されたユーザ名を指定します。
  - [PPPoE パスワード/パスワードの確認（PPPoE Password/Confirm Password）]：ISP によって提供されたパスワードを指定し、確認します。
  - [PPP 認証（PPP Authentication）]：[PAP]、[CHAP]、または [MSCHAP] を選択します。

    PAP は認証時にクリアテキストのユーザ名とパスワードを渡すため、セキュアではありません。CHAP では、サーバのチャレンジに対して、クライアントは暗号化された「チャレンジとパスワード」およびクリアテキストのユーザ名を返します。CHAP は PAP よりセキュアですが、データを暗号化しません。MSCHAP は CHAP に似ていますが、サーバが CHAP のようにクリアテキスト パスワードを扱わず、暗号化されたパスワードだけを保存、比較するため、CHAP よりセキュアです。また、MSCHAP では MPPE によるデータの暗号化のためのキーを生成します。
  - [PPPoE ルート メトリック（PPPoE route metric）]：アドミニストレーティブ ディスタンスを学習したルートに割り当てます。有効な値は 1 ～ 255 です。デフォルトでは、学習したルートのアドミニストレーティブ ディスタンスは 1 です。
  - [ルート設定の有効化（Enable Route Settings）]：手動で PPPoE の IP アドレスを設定するには、このチェックボックスをオンにして、[IP アドレス（IP Address）] を入力します。

    [ルート設定を有効化（Enable Route Settings）] チェックボックスをオンにして、[IP アドレス（IP Address）] を空欄にした場合、**ip address pppoe setroute** コマンドが次のように適用されます。

```
interface GigabitEthernet0/2
nameif inside2_pppoe
cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
security-level 0
pppoe client vpdn group test
pppoe client route distance 10
ip address pppoe setroute
```

- [フラッシュにユーザ名とパスワードを保存（Store Username and Password in Flash）]：フラッシュ メモリにユーザ名とパスワードを保存します。

  FTD デバイスは、NVRAM の特定の場所にユーザ名とパスワードを保存します。

ステップ 11 （任意）IPv6 アドレッシングの設定 （28 ページ）を参照して [IPv6] タブでの IPv6 アドレスを設定します。

ステップ 12 （任意）MAC アドレスの設定 （42 ページ）を参照して [詳細設定（Advanced）] タブで MAC アドレスを手動で設定します。

ステップ 13 （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 14 [OK] をクリックします。

ステップ 15 [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。

のブリッジグループ インターフェイスの設定

ブリッジグループは、Firepower Threat Defense デバイス がルーティングではなくブリッジするインターフェイスのグループです。 ブリッジグループはトランスペアレント ファイアウォール モード、ルーテッド ファイアウォール モードの両方でサポートされています。ブリッジグループの詳細については、ブリッジグループについてを参照してください。

ブリッジグループと関連インターフェイスを設定するには、次の手順を実行します。

ブリッジ グループ メンバーの一般的なインターフェイス パラメータの設定

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

この手順は、ブリッジ グループ メンバー インターフェイスの名前とセキュリティ ゾーンを設定する方法について説明します。同じブリッジ グループで、さまざまな種類のインターフェイス（物理インターフェイス、VLAN サブインターフェイス、VNI インターフェイス、EtherChannel、冗長インターフェイス）を含めることができます。診断インターフェイスはサポートされていません。ルーテッド モードでは、EtherChannel はサポートされません。Firepower 4100/9300 では、データ共有タイプのインターフェイスはサポートされていません。

始める前に

- **Firepower 4100/9300**
  1. 物理インターフェイスの設定
  2. （任意）特別なインターフェイスを設定します。
     - EtherChannel（ポート チャネル）の追加
     - コンテナ インスタンスへの VLAN サブインターフェイスの追加 FXOS で次を実行します。
     - FMC でのサブインターフェイスの追加 （13 ページ）
- （任意）**他のすべてのモデル**：
  - 冗長インターフェイスの設定 （7 ページ）
  - EtherChannel の設定 （9 ページ）
  - サブインターフェイスの追加 （13 ページ）

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 [名前（Name）] フィールドに、48 文字以内で名前を入力します。

ステップ 4 [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 5 （任意） このインターフェイスを [管理専用（Management Only）] に設定してトラフィックを管理トラフィックに制限します。through-the-box トラフィックは許可されていません。

ステップ 6 （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 7 [モード（Mode）] ドロップダウン リストで、[なし（None）] を選択します。

通常のファイアウォール インターフェイスのモードは [なし（None）] に設定されています。他のモードは IPS 専用インターフェイス タイプ向けです。このインターフェイスをブリッジ グループに割り当てると、[スイッチド（Switched）] がモードに表示されます。

ステップ 8 [セキュリティ ゾーン（Security Zone）] ドロップダウン リストからセキュリティ ゾーンを選択するか、[新規（New）] をクリックして、新しいセキュリティ ゾーンを追加します。

ブリッジ グループ メンバー インターフェイスは、スイッチドタイプ インターフェイスであり、スイッチドタイプのゾーンにのみ属することができます。このインターフェイスに対して IP アドレス設定は行わないでください。ブリッジ仮想インターフェイス（BVI）に対してのみ IP アドレスを設定します。BVI はゾーンに属しておらず、BVI にはアクセス コントロール ポリシーを適用できないことに注意してください。

ステップ 9 **MTU** についてはMTU の設定 （41 ページ）を参照してください。

ステップ 10 （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 11 （任意） IPv6 アドレッシングの設定 （28 ページ）を参照して [IPv6] タブでの IPv6 アドレスを設定します。

ステップ 12 （任意） MAC アドレスの設定 （42 ページ）を参照して [詳細設定（Advanced）] タブで MAC アドレスを手動で設定します。

ステップ 13 [OK] をクリックします。

ステップ 14 [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。

ブリッジ仮想インターフェイス（BVI）の設定

ブリッジ グループごとに、IP アドレスを設定する BVI が必要です。FTD はブリッジ グループが発信元になるパケットの送信元アドレスとして、この IP アドレスを使用します。BVI IP アドレスは、接続されたネットワークと同じサブネット内にある必要があります。IPv4 トラフィックの場合、すべてのトラフィックを通過させるには、BVI IP アドレスが必要です。IPv6 トラフィックの場合は、少なくとも、トラフィックを通過させるリンクローカル アドレスを設定する必要があります。リモート管理などの管理操作を含めたフル機能を実現するために、グローバル管理アドレスを設定することを推奨します。

ルーテッドモードの場合、BVIに名前を指定すると、BVIがルーティングに参加します。名前を指定しなければ、ブリッジ グループはトランスペアレント ファイアウォール モードの場合と同じように隔離されたままになります。

（注） 個別の 診断 インターフェイスでは、設定できないブリッジ グループ（ID 301）は、設定に自動的に追加されます。このブリッジ グループはブリッジ グループの制限に含まれません。

始める前に

セキュリティ ゾーンに BVI を追加することはできません。そのため、BVI にアクセス コントロール ポリシーを適用することはできません。ゾーンに基づいてブリッジ グループのメンバー インターフェイスにポリシーを適用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 **[インターフェイスの追加（Add Interfaces）]** > **[ブリッジ グループ インターフェイス（Bridge Group Interface）]** を選択します。

ステップ 3 （ルーテッド モード）[名前（Name）] フィールドに、名前を 48 文字以内で入力します。

トラフィックをブリッジ グループ メンバーの外部（たとえば、外部インターフェイスや他のブリッジ グループのメンバー）にルーティングする必要がある場合は、BVI に名前を付ける必要があります。名前は大文字と小文字が区別されません。

ステップ 4 [ブリッジ グループ ID（Bridge Group ID）] フィールドに、1 ～ 250 の間のブリッジ グループ ID を入力します。

ステップ 5 （オプション）[説明（Description）] フィールドに、このブリッジ グループの説明を入力します。

ステップ 6 [インターフェイス（Interfaces）] タブでインターフェイスをクリックし、[追加（Add）] をクリックして [選択したインターフェイス（Selected Interfaces）] 領域にそのインターフェイスを移動します。ブリッジ グループのメンバーにするすべてのインターフェイスに対して繰り返します。

ステップ 7 （トランスペアレント モード）[IPv4] タブをクリックします。[IP アドレス（IP Address）] フィールドに IPv4 アドレスおよびサブネット マスクを入力します。

BVI にはホスト アドレス（/32 または 255.255.255.255）を割り当てないでください。また、/30 サブネットなど（255.255.255.252）、ホスト アドレスが 3 つ未満（アップストリーム ルータ、ダウンストリーム ルータ、トランスペアレント ファイアウォールにそれぞれ 1 つずつ）の他のサブネットを使用しないでください。FTD デバイスは、サブネットの先頭アドレスと最終アドレスで送受信されるすべての ARP パケットをドロップします。たとえば、/30 サブネットを使用し、そのサブネットからアップストリーム ルータへの予約済みアドレスを割り当てた場合、FTD デバイスはダウンストリーム ルータからアップストリーム ルータへの ARP 要求をドロップします。

ハイ アベイラビリティの場合は、[モニタ対象インターフェイス（Monitored Interfaces）] エリアの **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[ハイアベイラビリティ（High Availability）]** タブで、スタンバイ IP アドレスを設定します。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステートをトラックすることしかできません。

ステップ 8 （ルーテッド モード）[IPv4] タブをクリックします。IP アドレスを設定するには、[IP タイプ（IP Type）] ドロップダウン リストにある次のオプションのいずれかを使用します。

- [静的 IP を使用する（Use Static IP）]：IP アドレスおよびサブネット マスクを入力します。ハイ アベイラビリティの場合は、静的 IP アドレスのみを使用できます。[モニタ対象インターフェイス（Monitored Interfaces）] エリアの **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[ハイアベイラビリティ（High Availability）]** タブで、スタンバイ IP アドレスを設定します。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステートをトラックすることしかできません。
- [DHCP の使用（Use DHCP）]：次のオプションのパラメータを設定します。
  - [DHCP を使用してデフォルト ルートを取得（Obtain default route using DHCP）]：DHCP サーバからデフォルト ルートを取得します。
  - [DHCP ルートメトリック（DHCP route metric）]：アドミニストレーティブ ディスタンスを学習したルートに割り当てます（1 ～ 255）。学習したルートのデフォルトのアドミニストレーティブ ディスタンスは 1 です。

ステップ 9 （任意）IPv6 アドレッシングの設定については、IPv6 アドレッシングの設定 （28 ページ）を参照してください。

ステップ 10 （任意）スタティック ARP エントリの追加 （43 ページ）および静的 MAC アドレスの追加とのブリッジ グループの MAC 学習の無効化 （44 ページ）（トランスペアレント モードの場合のみ）を参照して **ARP** と **MAC** を設定します。

ステップ 11 [OK] をクリックします。

ステップ 12 [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。

トランスペアレント モードの診断（管理）インターフェイスの設定

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

トランスペアレント ファイアウォール モードでは、すべてのインターフェイスがブリッジ グループに属している必要があります。唯一の例外は診断 *slot*/*port* インターフェイスです。Firepower 4100/9300 シャーシ では、診断インターフェイス ID は FTD 論理デバイスに割り当てた mgmt-type インターフェイスによって異なります。他のインターフェイス タイプは診断インターフェイスとして使用できません。設定できる診断インターフェイスは 1 つです。

始める前に

このインターフェイスをブリッジ グループに割り当てないでください。設定できないブリッジ グループ（ID 301）は、コンフィギュレーションに自動的に追加されます。このブリッジ グループはブリッジ グループの制限に含まれません。

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 診断 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 [名前（Name）] フィールドに、48 文字以内で名前を入力します。

ステップ 4 [IPv4] タブをクリックします。IP アドレスを設定するには、[IP タイプ（IP Type）] ドロップダウン リストにある次のオプションのいずれかを使用します。

- [静的 IP を使用する（Use Static IP）]：IP アドレスおよびサブネット マスクを入力します。
- [DHCP の使用（Use DHCP）]：次のオプションのパラメータを設定します。
  - [DHCP を使用してデフォルト ルートを取得（Obtain default route using DHCP）]：DHCP サーバからデフォルト ルートを取得します。
  - [DHCP ルートメトリック（DHCP route metric）]：アドミニストレーティブ ディスタンスを学習したルートに割り当てます（1 ～ 255）。学習したルートのデフォルトのアドミニストレーティブ ディスタンスは 1 です。
- [PPPoE の使用（Use PPPoE）]：次のパラメータを設定します。

- [VPDN グループ名（VPDN Group Name）]：グループ名を指定します。
- [PPPoE ユーザ名（PPPoE User Name）]：ISP によって提供されたユーザ名を指定します。
- [PPPoE パスワード/パスワードの確認（PPPoE Password/Confirm Password）]：ISP によって提供されたパスワードを指定し、確認します。
- [PPP 認証（PPP Authentication）]：[PAP]、[CHAP]、または [MSCHAP] を選択します。

  PAP は認証時にクリアテキストのユーザ名とパスワードを渡すため、セキュアではありません。CHAP では、サーバのチャレンジに対して、クライアントは暗号化された「チャレンジとパスワード」およびクリアテキストのユーザ名を返します。CHAP は PAP よりセキュアですが、データを暗号化しません。MSCHAP は CHAP に似ていますが、サーバが CHAP のようにクリアテキスト パスワードを扱わず、暗号化されたパスワードだけを保存、比較するため、CHAP よりセキュアです。また、MSCHAP では MPPE によるデータの暗号化のためのキーを生成します。
- [PPPoE ルート メトリック（PPPoE route metric）]：アドミニストレーティブ ディスタンスを学習したルートに割り当てます。有効な値は 1 ～ 255 です。デフォルトでは、学習したルートのアドミニストレーティブ ディスタンスは 1 です。
- [ルート設定の有効化（Enable Route Settings）]：手動で PPPoE の IP アドレスを設定するには、このチェックボックスをオンにして、[IP アドレス（IP Address）] を入力します。
- [フラッシュにユーザ名とパスワードを保存（Store Username and Password in Flash）]：フラッシュ メモリにユーザ名とパスワードを保存します。

  FTD デバイスは、NVRAM の特定の場所にユーザ名とパスワードを保存します。

ステップ 5 （任意） **IPv6** アドレッシングの設定については、IPv6 アドレッシングの設定 （28 ページ）を参照してください。

ステップ 6 （任意） [詳細設定（Advanced）] タブで、オプションの設定を実行します。

- MAC アドレスの設定 （42 ページ）を参照してください。
- スタティック ARP エントリの追加 （43 ページ）を参照してください。
- セキュリティの設定パラメータの設定 （45 ページ）を参照してください。

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。

IPv6 アドレッシングの設定

ここでは、ルーテッド モードおよびトランスペアレント モードで IPv6 アドレッシングを設定する方法について説明します。

IPv6 について

このセクションには、IPv6 に関する情報が含まれています。

IPv6 アドレス指定

次の 2 種類の IPv6 のユニキャスト アドレスを設定できます。

- グローバル：グローバル アドレスは、パブリック ネットワークで使用可能なパブリック アドレスです。ブリッジ グループの場合、このアドレスは各メンバー インターフェイスごとに設定するのではなく、BVI用に設定する必要があります。また、トランスペアレント モードで管理インターフェイスのグローバルな IPv6 アドレスを設定することもできます。
- リンクローカル：リンクローカルアドレスは、直接接続されたネットワークだけで使用できるプライベート アドレスです。ルータは、リンクローカル アドレスを使用してパケットを転送するのではなく、特定の物理ネットワーク セグメント上で通信だけを行います。ルータは、アドレス設定またはアドレス解決などのネイバー探索機能に使用できます。ブリッジ グループでは、メンバー インターフェイスのみがリンクローカル アドレスを所有しています。BVI にはリンクローカル アドレスはありません。

最低限、IPv6 が動作するようにリンクローカル アドレスを設定する必要があります。グローバル アドレスを設定すると、リンクローカル アドレスがインターフェイスに自動的に設定されるため、リンクローカル アドレスを個別に設定する必要はありません。ブリッジ グループ インターフェイスでは、BVI でグローバル アドレスを設定した場合、Firepower Threat Defense デバイス が自動的にメンバー インターフェイスのリンクローカル アドレスを生成します。グローバル アドレスを設定しない場合は、リンクローカル アドレスを自動的にするか、手動で設定する必要があります。

Modified EUI-64 インターフェイス ID

RFC 3513「Internet Protocol Version 6 (IPv6) Addressing Architecture」（インターネット プロトコル バージョン 6 アドレッシング アーキテクチャ）では、バイナリ値 000 で始まるものを除き、すべてのユニキャスト IPv6 アドレスのインターフェイス識別子部分は長さが 64 ビットで、Modified EUI-64 形式で組み立てることが要求されています。Firepower Threat Defense デバイスでは、ローカル リンクに接続されたホストにこの要件を適用できます。

この機能がインターフェイスで有効化されていると、そのインターフェイス ID が Modified EUI-64 形式を採用していることを確認するために、インターフェイスで受信した IPv6 パケットの送信元アドレスが送信元 MAC アドレスに照らして確認されます。IPv6 パケットがインターフェイス ID に Modified EUI-64 形式を採用していない場合、パケットはドロップされ、次のシステム ログ メッセージが生成されます。

```
325003: EUI-64 source address check failed.
```

アドレス形式の確認は、フローが作成される場合にのみ実行されます。既存のフローからのパケットは確認されません。また、アドレスの確認はローカル リンク上のホストに対してのみ実行できます。

グローバル IPv6 アドレスの設定

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

ルーテッド モードの任意のインターフェイスとトランスペアレント モードまたはルーテッド モードの BVI に対してグローバル IPv6 アドレスを設定するには、次の手順を実行します。

（注） グローバルアドレスを設定すると、リンクローカルアドレスは自動的に設定されるため、別々に設定する必要はありません。ブリッジ グループについて、BVI でグローバル アドレスを設定すると、すべてのメンバー インターフェイスのリンクローカル アドレスが自動的に設定されます。

FTD で定義されているサブインターフェイスの場合、親インターフェイスの同じ Burned-In MAC Address を使用するので、MAC アドレスも手動で設定することをお勧めします。IPv6 リンクローカルアドレスはMACアドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカル アドレスが可能になり、FTD で特定のインスタンスでのトラフィックの中断を避けることができます。MAC アドレスの設定 （42 ページ）を参照してください。

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 [IPv6] タブをクリックします。

ルーテッド モードでは、[基本（Basic）] タブがデフォルトで選択されています。トランスペアレント モードでは、[アドレス（Address）] タブがデフォルトで選択されています。

ステップ 4 グローバル IPv6 アドレスを次のいずれかの方法で設定します。

- （ルーテッドインターフェイス）ステートレス自動設定：[自動設定（Autoconfiguration）] チェックボックスをオンにします。

インターフェイス上でステートレス自動設定を有効にすると、受信したルータ アドバタイズメント メッセージのプレフィックスに基づいて IPv6 アドレスを設定します。ステートレスな自動設定が有効になっている場合、インターフェイスのリンクローカル アドレスは、Modified EUI-64 インターフェイス ID に基づいて自動的に生成されます。

RFC 4862 では、ステートレス自動設定用に設定されたホストはルータ アドバタイズメント メッセージを送信しないと規定されていますが、この場合は、FTD デバイスがルータ アドバタイズメント メッセージを送信します。**[IPv6]** > **[設定（Settings）]** > **[RA の有効化（Enable RA）]** チェックボックスをオフにして、メッセージを抑制します。

- 手動設定：グローバル IPv6 アドレスを手動で設定するには、次の手順を実行します。

  1. [アドレス（Address）] タブをクリックして、[アドレスの追加（Add Address）] をクリックします。

     [アドレスの追加（Add Address）] ダイアログボックスが表示されます。

  2. [アドレス（Address）] フィールドに、インターフェイス ID を含む完全なグローバル IPv6 アドレス、または IPv6 プレフィックス長と IPv6 プレフィックスのいずれかを入力します。（ルーテッドモード）プレフィックスだけを入力した場合は、必ず [EUI-64 を適用（Enforce EUI 64）] チェックボックスをオンにして、Modified EUI-64 形式を使用してインターフェイス ID を生成するようにしてください。たとえば、2001:0DB8::BA98:0:3210/48（完全なアドレス）または 2001:0DB8::/48（プレフィックス、[EUI 64] はオン）。

     （[EUI 64の適用（Enforce EUI 64）] を設定しなかった場合は）ハイ アベイラビリティのために、[モニタ対象インターフェイス（Monitored Interfaces）] エリアの **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[ハイアベイラビリティ（High Availability）]** タブで、スタンバイ IP アドレスを設定します。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステートをトラックすることしかできません。

ステップ 5 ルーテッド インターフェイスの場合は、オプションで [基本（Basic）] タブで次の値を設定できます。

- グローバル アドレスを設定しない場合に自動的にリンクローカル アドレスを設定するには、[IPv6 の有効化（Enable IPv6）] チェックボックスをオンにします。

  グローバル アドレスを設定する必要がなく、リンクローカル アドレスだけを設定する必要がある場合は、リンクローカル アドレスをインターフェイスの MAC アドレスに基づいて作成することもできます（Modified EUI-64 形式。MAC アドレスで使用するビット数は 48 ビットであるため、インターフェイス ID に必要な 64 ビットを埋めるために追加ビットを挿入する必要があります）。

- ローカル リンクの IPv6 アドレスに Modified EUI-64 形式のインターフェイス識別子の使用を適用するには、[EUI-64 を適用（Enforce EUI-64）] チェックボックスをオンにします。

- リンクローカル アドレスを手動で設定するには、[リンクローカル アドレス（Link-Local address）] フィールドにアドレスを入力します。

リンクローカル アドレスは、FE8、FE9、FEA、または FEB で始まっている必要があります。例、fe80::20d:88ff:feee:6a82。グローバル アドレスを設定する必要がなく、リンクローカル アドレスだけを設定する必要がある場合は、リンクローカル アドレスを手動で定義できます。Modified EUI-64 形式に基づくリンクローカル アドレスを自動的に割り当てることを推奨します。たとえば、その他のデバイスで Modified EUI-64 形式の使用が強制される場合、手動で割り当てたリンクローカルアドレスによりパケットがドロップされることがあります。

- [アドレス設定の DHCP を有効化（Enable DHCP for address config）] チェックボックスをオンにして、IPv6 ルータ アドバタイズメント パケットの Managed Address Config フラグを設定します。

  IPv6 ルータ アドバタイズメント内のこのフラグは、取得されるステートレス自動設定のアドレス以外のアドレスの取得に DHCPv6 を使用する必要があることを、IPv6 自動設定クライアントに通知します。

- [アドレス設定の DHCP を有効化（Enable DHCP for address config）] チェックボックスをオンにして、IPv6 ルータ アドバタイズメント パケットの Other Address Config フラグを設定します。

  IPv6 ルータ アドバタイズメント内のこのフラグは、DHCPv6 から DNS サーバ アドレスなどの追加情報の取得に DHCPv6 を使用する必要があることを、IPv6 自動設定クライアントに通知します。

ステップ 6 ルーテッドインターフェイスの場合は、[プレフィックス（Prefixes）] タブと [設定（Settings）] タブでの設定についてIPv6 ネイバー探索の設定 （32 ページ）を参照してください。BVI インターフェイスの場合は、[設定（Settings）] タブの以下のパラメータを参照してください。

- [DAD 試行（DAD attempts）]：DAD 試行の最大数（1 ～ 600）。重複アドレス検出（DAD）プロセスをディセーブルにするには、この値を 0 に設定します。この設定では、DAD が IPv6 アドレスで実行されている間に、インターフェイスに連続して送信されるネイバー送信要求メッセージの数を設定します。デフォルトでは 1 になっています。

- [NS 間隔（NS Interval）]：インターフェイスでの IPv6 ネイバー要請再送信の間隔（1000 ～ 3600000 ms）。デフォルト値は 1000 ミリ秒です。

- [到達可能時間（Reachable Time）]：到達可能性確認イベントが発生した後でリモートの IPv6 ノードを到達可能とみなす時間（0 ～ 3600000 ms）。デフォルト値は 0 ミリ秒です。value に 0 を使用すると、到達可能時間が判定不能として送信されます。到達可能時間の値を設定し、追跡するのは、受信デバイスの役割です。ネイバー到達可能時間を設定すると、使用できないネイバーを検出できます。時間を短く設定すると、使用できないネイバーをより早く検出できます。ただし、時間を短くするほど、IPv6 ネットワーク帯域幅とすべての IPv6 ネットワーク デバイスの処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

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。

IPv6 ネイバー探索の設定

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

IPv6 ネイバー探索プロセスは、ICMPv6 メッセージおよび要請ノード マルチキャスト アドレスを使用して、同じネットワーク（ローカル リンク）上のネイバーのリンク層アドレスを特定し、ネイバーの読み出し可能性を確認し、隣接ルータを追跡します。

ノード（ホスト）はネイバー探索を使用して、接続リンク上に存在することがわかっているネイバーのリンク層アドレスの特定や、無効になったキャッシュ値の迅速なパージを行います。また、ホストはネイバー探索を使用して、ホストに代わってパケットを転送しようとしている隣接ルータを検出します。さらに、ノードはこのプロトコルを使用して、どのネイバーが到達可能でどのネイバーがそうでないかをアクティブに追跡するとともに、変更されたリンク層アドレスを検出します。ルータまたはルータへのパスが失われると、ホストは機能している代替ルータまたは代替パスをアクティブに検索します。

始める前に

ルーテッド モードのみでサポートされます。

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 [IPv6] タブをクリックして、[プレフィックス（Prefixes）] タブをクリックします。

ステップ 4 （任意） IPv6 ルータ アドバタイズメントに含める IPv6 プレフィックスを設定するには、次の手順を実行します。

a) [プレフィックスの追加（Add Prefix）] をクリックします。

b) [アドレス（Address）] フィールドに、プレフィックス長の IPv6 アドレスを入力するか、または [デフォルト（Default）] チェックボックスをオンにして、デフォルトのプレフィックスを使用します。

c) （任意） IPv6 プレフィックスをアドバタイズしない場合は、[アドバタイズメント（Advertisement）] チェックボックスをオフにします。

d) [オフ リンク（Off Link）] チェックボックスをオンにして、指定したプレフィックスがリンクに割り当てられたことを示します。指定したプレフィックスを含むアドレスにトラフィックを送信するノードは、宛先がリンク上でローカルに到達可能であると見なします。このプレフィックスは、オンリンクの判別には使用しないでください。

e) 指定されているプレフィックスを自動設定に使用する場合、[自動設定（Autoconfiguration）] チェックボックスをオンにします。

f) [プレフィックス ライフタイム（Prefix Lifetime）] で、[期間（Duration）] または [失効日（Expiration Date）] をクリックします。

- [期間（Duration）] : プレフィックスの [優先ライフタイム（Preferred Lifetime）] を秒単位で入力します。この設定は、指定の IPv6 プレフィックスが有効なものとしてアドバタイズする時間です。最大値は無限大です。有効な値は 0 ～ 4294967295 です。デフォルトは 2592000（30 日間）です。プレフィックスの [有効ライフタイム（Valid Lifetime）] を秒単位で入力します。この設定は、指定の IPv6 プレフィックスが優先であるとしてアドバタイズする時間です。最大値は無限大です。有効な値は 0 ～ 4294967295 です。デフォルト設定は、604800（7 日）です。または、[無限大（Infinite）] チェックボックスをオンにして、時間無制限を設定します。
- [失効日（Expiration Date）] : [有効（Valid）]、[優先（Preferred）] 日時を選択します。

g) [OK] をクリックします。

ステップ 5 [設定（Settings）] タブをクリックします。

ステップ 6 （任意） [DAD 試行（DAD attempts）] の最大数、1 ～ 600 を設定します。デフォルトでは 1 になっています。重複アドレス検出（DAD）プロセスをディセーブルにするには、この値を 0 に設定します。

この設定では、DAD が IPv6 アドレスで実行されている間に、インターフェイスに連続して送信されるネイバー送信要求メッセージの数を設定します。

ステートレス自動設定プロセス中に、重複アドレス検出は、アドレスがインターフェイスに割り当てられる前に、新しいユニキャスト IPv6 アドレスの一意性を確認します。

重複アドレスが検出されると、そのアドレスの状態は DUPLICATE に設定され、アドレスは使用対象外となり、次のエラー メッセージが生成されます。

```
325002: Duplicate address ipv6_address/MAC_address on interface
```

重複アドレスがインターフェイスのリンクローカルアドレスであれば、インターフェイス上で IPv6 パケットの処理は無効になります。重複アドレスがグローバル アドレスであれば、そのアドレスは使用されません。

ステップ 7 （任意） [NS インターバル（NS Interval）] フィールドで、IPv6 ネイバー勧誘再送信の時間の間隔を、1000 ～ 3600000ms で設定します。

デフォルト値は 1000 ミリ秒です。

ローカル リンク上にある他のノードのリンクレイヤ アドレスを検出するため、ノードからネイバー送信要求メッセージ（ICMPv6 Type 135）がローカル リンクに送信されます。ネイバー

送信要求メッセージを受信すると、宛先ノードは、ネイバー アドバタイズメント メッセージ（ICPMv6 Type 136）をローカル リンク上に送信して応答します。

送信元ノードがネイバーアドバタイズメントを受信すると、送信元ノードと宛先ノードが通信できるようになります。ネイバー送信要求メッセージは、ネイバーのリンク層アドレスが識別された後に、ネイバーの到達可能性の確認にも使用されます。ノードがあるネイバーの到達可能性を検証する場合、ネイバー送信要求メッセージ内の宛先アドレスとして、そのネイバーのユニキャスト アドレスを使用します。

ネイバー アドバタイズメント メッセージは、ローカル リンク上のノードのリンク層アドレスが変更されたときにも送信されます。

ステップ 8 （任意） 到達可能性確認イベントが発生した後でリモート IPv6 ノードが到達可能であると見なされる時間を、[到達可能時間（Reachable Time）] フィールドにて、0 ～ 3600000ms で設定します。

デフォルト値は 0 ミリ秒です。value に 0 を使用すると、到達可能時間が判定不能として送信されます。到達可能時間の値を設定し、追跡するのは、受信デバイスの役割です。

ネイバー到達可能時間を設定すると、使用できないネイバーを検出できます。時間を短く設定すると、使用できないネイバーをより早く検出できます。ただし、時間を短くするほど、IPv6 ネットワーク帯域幅とすべての IPv6 ネットワーク デバイスの処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

ステップ 9 （任意） ルータ アドバタイズメントの伝送を抑制にするには、[RA を有効にする（Enable RA）] チェックボックスをオフにします。ルータ アドバタイズメントの伝送を有効にすると、RA ライフタイムと時間間隔を設定できます。

ルータ要請メッセージ（ICMPv6 Type 133）に応答して、ルータ アドバタイズメント メッセージ（ICMPv6 Type 134）が自動的に送信されます。ルータ要請メッセージは、システムの起動時にホストから送信されるため、ホストは、次にスケジュールされているルータ アドバタイズメント メッセージを待つことなくただちに自動設定を行うことができます。

Firepower Threat Defense デバイスで IPv6 プレフィックスを提供する必要がないインターフェイス（外部インターフェイスなど）では、これらのメッセージをディセーブルにできます。

- [RA ライフタイム（RA Lifetime）] : IPv6 ルータ アドバタイズメントのルータのライフタイム値を、0 ～ 9000 秒で設定します。

  デフォルトは 1800 秒です。

- [RA インターバル（RA Interval）] : IPv6 ルータ アドバタイズメントの伝送の間の時間間隔を、3 ～ 1800 秒で設定します。

  デフォルトは 200 秒です。

ステップ 10 [OK] をクリックします。

ステップ 11 [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。

高度なインターフェイスの設定

この項では、通常のファイアウォール モードのインターフェイスの MAC アドレスの設定方法、最大伝送ユニット（MTU）の設定方法、およびその他の詳細パラメータの設定方法について説明します。

インターフェイスの詳細設定について

ここでは、インターフェイスの詳細設定について説明します。

MAC アドレスについて

手動で MAC アドレスを割り当てて、デフォルトを上書きすることができます。 コンテナ インスタンスでは、FXOS シャーシがすべてのインターフェイスに一意の MAC アドレスを自動的に生成します。

（注） 親インターフェイスの同じ Burned-In MAC Address を使用するので、FTD で定義されたサブインターフェイスに一意の MAC アドレスを割り当てることもできます。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。また、IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカル アドレスが可能になり、FTD で特定のインスタンスでのトラフィックの中断を避けることができます。

（注） コンテナ インスタンスでは、MAC アドレスを手動で設定すると、サブインターフェイスを共有していない場合でも、分類が正しく行われるように、同じ親インターフェイス上のすべてのサブインターフェイスで一意の MAC アドレスを使用します。

デフォルトの MAC アドレス

ネイティブ インスタンス向け：

デフォルトの MAC アドレスの割り当ては、インターフェイスのタイプによって異なります。

- 物理インターフェイス：物理インターフェイスは Burned-In MAC Address を使用します。

- 冗長インターフェイス：冗長インターフェイスでは、最初に追加された物理インターフェイスの MAC アドレスが使用されます。構成でメンバー インターフェイスの順序を変更すると、MAC アドレスがリストの先頭にあるインターフェイスの MAC アドレスと一致するように変更されます。冗長インターフェイスに MAC アドレスを割り当てると、メンバー インターフェイスの MAC アドレスに関係なく、割り当てた MAC アドレスが使用されます。
- EtherChannel（Firepower Models）：EtherChannel の場合は、そのチャネル グループに含まれるすべてのインターフェイスが同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワーク アプリケーションとユーザに対してトランスペアレントになります。ネットワーク アプリケーションやユーザから見えるのは 1 つの論理接続のみであり、個々のリンクのことは認識しないためです。ポート チャネル インターフェイスは、プールからの一意の MAC アドレスを使用します。インターフェイスのメンバーシップは、MAC アドレスには影響しません。
- EtherChannel（ASA モデル）：ポート チャネル インターフェイスは、最も小さいチャネル グループ インターフェイスの MAC アドレスをポート チャネル MAC アドレスとして使用します。または、ポート チャネル インターフェイスの MAC アドレスを設定することもできます。グループ チャネル インターフェイス メンバーシップが変更された場合に備えて、一意の MAC アドレスを構成することを推奨します。ポート チャネル MAC アドレスを提供していたインターフェイスを削除すると、そのポート チャネル MAC アドレスは次に番号が小さいインターフェイスに変わるため、トラフィックが分断されます。
- サブインターフェイス（FTD 定義済み）：物理インターフェイスのすべてのサブインターフェイスは同じ Burned-In MAC Address を使用します。サブインターフェイスに固有の MAC アドレスを割り当てることが必要になる場合があります。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。また、IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカル アドレスが可能になり、FTD で特定のインスタンスでのトラフィックの中断を避けることができます。

コンテナ インスタンス向け：

- すべてのインターフェイスの MAC アドレスは MAC アドレス プールから取得されます。サブインターフェイスでは、MAC アドレスを手動で設定した場合、分類が正しく行われるように、同じ親インターフェイス上のすべてのサブインターフェイスで一意の MAC アドレスを使用します。コンテナ インスタンス インターフェイスの自動 MAC アドレスを参照してください。

MTU について

MTU は、Firepower Threat Defense デバイス が特定のイーサネット インターフェイスで送信する最大フレーム ペイロード サイズを指定します。MTU の値は、イーサネット ヘッダー、VLAN タギング、またはその他のオーバーヘッドを含まないフレーム サイズです。たとえば MTU を 1500 に設定した場合、想定されるフレーム サイズはヘッダーを含めて 1518 バイト、VLAN を

使用する場合は1522バイトです。これらのヘッダーに対応するためにMTU値を高く設定しないでください。

パス MTU ディスカバリ

Firepower Threat Defense デバイス は、Path MTU Discovery（RFC 1191 の定義に従う）をサポートします。つまり、2 台のホスト間のネットワーク パス内のすべてのデバイスで MTU を調整できます。したがってパスの最小 MTU の標準化が可能です。

デフォルト MTU

Firepower Threat Defense デバイス のデフォルト MTU は、1500 バイトです。この値には、イーサネット ヘッダー、VLAN タギングや他のオーバーヘッド分の 18～22 バイトは含まれません。

MTU およびフラグメンテーション

IPv4 では、出力 IP パケットが指定された MTU より大きい場合、2 つ以上のフレームにフラグメント化されます。フラグメントは宛先（場合によっては中間ホップ）で組み立て直されますが、フラグメント化はパフォーマンス低下の原因となります。IPv6 では、通常、パケットをフラグメント化することはできません。したがって、フラグメント化を避けるために、IP パケットを MTU サイズ以内に収める必要があります。

TCP パケットでは、通常、エンドポイントは MTU を使用して TCP の最大セグメント サイズを決定します（MTU - 40 など）。途中で追加の TCP ヘッダーが追加された場合（たとえば、サイト間 VPN トンネル）、TCP MSS はトンネリング エンティティで下方調整しないといけない場合があります。TCP MSS について （38 ページ）を参照してください。

UDP または ICMP では、フラグメンテーションを回避するために、アプリケーションは MTU を考慮する必要があります。

（注） Firepower Threat Defense デバイス はメモリに空きがある限り、設定された MTU よりも大きいフレームを受信します。

MTU とジャンボ フレーム

MTU が大きいほど、大きいパケットを送信できます。パケットが大きいほど、ネットワークの効率が良くなる可能性があります。次のガイドラインを参照してください。

- トラフィック パスの MTU の一致：すべての FTD インターフェイスとトラフィック パス内のその他のデバイスのインターフェイスでは、MTU が同じになるように設定することを推奨します。MTU の一致により、中間デバイスでのパケットのフラグメント化が回避できます。
- ジャンボ フレームへの対応：MTU を最大 9198 バイトに設定できます。Firepower Threat Defense Virtual の最大値は 9000 です。Firepower 4100/9300 の最大値は 9184 です。

TCP MSS について

最大セグメント サイズ（TCP MSS）とは、あらゆる TCP および IP ヘッダーが追加される前の TCP ペイロードのサイズです。UDP パケットは影響を受けません。接続を確立するときの 3 ウェイ ハンドシェイク中に、クライアントとサーバは TCP MSS 値を交換します。

FlexConfig の Sysopt_Basic オブジェクトを使用して Firepower Threat Defense デバイス で TCP MSS を通過トラフィック用に設定できます。「Firepower Threat Defense の FlexConfig ポリシー」を参照してください。デフォルトで、最大 TCP MSS は 1380 バイトに設定されます。この設定は、Firepower Threat Defense デバイス が IPsec VPN カプセル化のパケット サイズを追加する必要がある場合に役立ちます。ただし、非 IPsec エンドポイントでは、Firepower Threat Defense デバイス の最大 TCP MSS を無効にする必要があります。

最大 TCP MSS を設定している場合、接続のいずれかのエンドポイントが Firepower Threat Defense デバイス に設定された値を超える TCP MSS を要求すると、Firepower Threat Defense デバイス は要求パケット内の TCP MSS を Firepower Threat Defense デバイス の最大サイズで上書きします。ホストまたはサーバが TCP MSS を要求しない場合、Firepower Threat Defense デバイス は RFC 793 のデフォルト値 536 バイト（IPv4）または 1220 バイト（IPv6）を想定しますが、パケットは変更しません。たとえば、MTU をデフォルトの 1500 バイトのままにします。ホストは、1500 バイトの MSS から TCP および IP のヘッダー長を減算して、MSS を 1460 バイトに設定するように要求します。Firepower Threat Defense デバイス の最大 TCP MSS が 1380（デフォルト）の場合は、Firepower Threat Defense デバイス は TCP 要求パケットの MSS 値を 1380 に変更します。その後、サーバは、1380 バイトのペイロードを含むパケットを送信します。Firepower Threat Defense デバイス は、最大 120 バイトのヘッダーをパケットに追加しても、1500 バイトの MTU サイズに適応することができます。

TCP の最小 MSS も設定できます。ホストまたはサーバが非常に小さい TCP MSS を要求した場合、Firepower Threat Defense デバイス は値を調整します。デフォルトでは、最小 TCP MSS は有効ではありません。

SSL VPN 接続用を含め、to-the-box トラフィックの場合、この設定は適用されません。Firepower Threat Defense デバイス は MTU を使用して、TCP MSS を導き出します。MTU - 40（IPv4）または MTU - 60（IPv6）となります。

デフォルト TCP MSS

デフォルトでは、Firepower Threat Defense デバイス の最大 TCP MSS は 1380 バイトです。このデフォルトは、ヘッダーが最大 120 バイトの IPv4 IPsec VPN 接続に対応しています。この値は、MTU の デフォルトの 1500 バイト内にも収まっています。

TCP MSS の推奨最大設定

デフォルトでは TCP MSS は、Firepower Threat Defense デバイス が IPv4 IPsec VPN エンドポイントとして機能し、MTU が 1500 バイトであることを前提としています。Firepower Threat Defense デバイス が IPv4 IPsec VPN エンドポイントとして機能している場合は、最大 120 バイトの TCP および IP ヘッダーに対応する必要があります。

MTU 値を変更して、IPv6 を使用するか、または IPsec VPN エンドポイントとして Firepower Threat Defense デバイス を使用しない場合は、FlexConfig の Sysopt_Basic オブジェクトを使用

して TCP MSS 設定を変更する必要があります。 Firepower Threat Defense の FlexConfig ポリシーを参照してください。次のガイドラインを参照してください。

- 通常のトラフィック：TCP MSS の制限を無効にし、接続のエンドポイント間で確立された値を受け入れます。一般に接続エンドポイントは MTU から TCP MSS を取得するため、非 IPsec パケットは通常この TCP MSS を満たしています。
- IPv4 IPsec エンドポイント トラフィック：最大 TCP MSS を MTU - 120 に設定します。たとえば、ジャンボ フレームを使用しており、MTU を 9000 に設定すると、新しい MTU を使用するために、TCP MSS を 8880 に設定する必要があります。
- IPv6 IPsec エンドポイント トラフィック：最大 TCP MSS を MTU - 140 に設定します。

ブリッジグループ トラフィックの ARP インスペクション

デフォルトでは、ブリッジグループのメンバーの間ですべての ARP パケットが許可されます。ARP パケットのフローを制御するには、ARP インスペクションを有効にします。

ARP インスペクションによって、悪意のあるユーザが他のホストやルータになりすます（ARP スプーフィングと呼ばれる）のを防止できます。ARP スプーフィングが許可されていると、「中間者」攻撃を受けることがあります。たとえば、ホストが ARP 要求をゲートウェイ ルータに送信すると、ゲートウェイ ルータはゲートウェイ ルータの MAC アドレスで応答します。ただし、攻撃者は、ルータの MAC アドレスではなく攻撃者の MAC アドレスで別の ARP 応答をホストに送信します。これで、攻撃者は、すべてのホストトラフィックを代行受信してルータに転送できるようになります。

ARP インスペクションを使用すると、正しい MAC アドレスとそれに関連付けられた IP アドレスがスタティック ARP テーブル内にある限り、攻撃者は攻撃者の MAC アドレスで ARP 応答を送信できなくなります。

ARP インスペクションをイネーブルにすると、Firepower Threat Defense デバイスは、すべての ARP パケット内の MAC アドレス、IP アドレス、および送信元インターフェイスを ARP テーブル内のスタティック エントリと比較し、次のアクションを実行します。

- IP アドレス、MAC アドレス、および送信元インターフェイスが ARP エントリと一致する場合、パケットを通過させます。
- MAC アドレス、IP アドレス、またはインターフェイス間で不一致がある場合、Firepower Threat Defense デバイスはパケットをドロップします。
- ARP パケットがスタティック ARP テーブル内のどのエントリとも一致しない場合、パケットをすべてのインターフェイスに転送（フラッディング）するか、またはドロップするように Firepower Threat Defense デバイスを設定できます。

（注） 専用の 診断 インターフェイスは、このパラメータが flood に設定されている場合でもパケットをフラッディングしません。

MAC アドレス テーブル

ブリッジ グループを使用する場合、FTD は、通常のブリッジまたはスイッチと同様に、MAC アドレスを学習して MAC アドレス テーブルを作成します。デバイスがブリッジ グループ経由でパケットを送信すると、FTD が MAC アドレスをアドレス テーブルに追加します。テーブルで MAC アドレスと発信元インターフェイスが関連付けられているため、FTDは、パケットが正しいインターフェイスからデバイスにアドレス指定されていることがわかります。ブリッジ グループ メンバー間のトラフィックには FTD セキュリティ ポリシーが適用されるため、パケットの宛先 MAC アドレスがテーブルに含まれていなくても、通常のブリッジのように、すべてのインターフェイスに元のパケットを FTD がフラッディングすることはありません。代わりに、直接接続されたデバイスまたはリモート デバイスに対して次のパケットを生成します。

- 直接接続されたデバイスへのパケット：FTD は宛先 IP アドレスに対して ARP 要求を生成し、ARP 応答を受信したインターフェイスを学習します。
- リモート デバイスへのパケット：FTD は宛先 IP アドレスへの ping を生成し、ping 応答を受信したインターフェイスを学習します。

元のパケットはドロップされます。

デフォルト設定

- ARP インスペクションを有効にした場合、デフォルト設定では、一致しないパケットはフラッディングします。
- ダイナミック MAC アドレス テーブル エントリのデフォルトのタイムアウト値は 5 分です。
- デフォルトでは、各インターフェイスはトラフィックに入る MAC アドレスを自動的に学習し、Firepower Threat Defense デバイスは対応するエントリを MAC アドレス テーブルに追加します。

ARP インスペクションと MAC アドレス テーブルのガイドライン

- ARP インスペクションは、ブリッジ グループでのみサポートされます。
- MAC アドレス テーブル構成は、ブリッジ グループでのみサポートされます。

MTU の設定

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

たとえば、ジャンボ フレームを許可するようにインターフェイスの MTU をカスタマイズします。

注意 デバイス上で非管理/診断インターフェイスの最大 MTU 値を変更し、設定の変更を展開すると、Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理/診断インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作を参照してください。

始める前に

- MTU を 1500 バイトより大きい値に変更すると、自動的にジャンボ フレームが有効になります。ASA モデルの場合、ジャンボ フレームを使用するには、システムをリロードする必要があります。
- インライン セットでインターフェイスを使用する場合、MTU 設定は使用されません。ただし、ジャンボ フレームの設定はインライン セットに関連します。ジャンボ フレームによりインライン インターフェイスは最大 9000 バイトのパケットを受信できます。ジャンボ フレームを有効にするには、すべてのインターフェイスの MTU を 1500 バイトより大きい値に設定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 [一般（General）] タブで、[MTU] を 64 ～ 9198 バイトに設定します。最大値は Firepower Threat Defense Virtual では 9000、Firepower 4100/9300 シャーシ上の FTD では 9184 です。

デフォルト値は 1500 バイトです。

ステップ 4 **[OK]** をクリックします。

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。

ステップ 6 ASA モデルでは、MTU を 1500 バイトを超える値に設定する場合はシステムをリロードしてジャンボ フレームを有効にします。

MAC アドレスの設定

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

MAC アドレスを手動で割り当てることが必要となる場合があります。また、**[デバイス（Devices）] > [デバイス管理（Device Management）] > [ハイアベイラビリティ（High Availability）]** タブで、アクティブ MAC アドレスとスタンバイ MAC アドレスを設定することもできます。両方の画面でインターフェイスの MAC アドレスを設定した場合は、**[インターフェイス（Interfaces）] > [詳細（Advanced）]** タブのアドレスが優先されます。

（注） コンテナ インスタンスでは、MAC アドレスを手動で設定すると、サブインターフェイスを共有していない場合でも、分類が正しく行われるように、同じ親インターフェイス上のすべてのサブインターフェイスで一意の MAC アドレスを使用します。

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 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 [詳細（Advanced）] タブをクリックします。
[情報（Information）] タブが選択されています。

ステップ 4 [アクティブな MAC アドレス（Active MAC Address）] フィールドに、MAC アドレスを H.H.H 形式で設定します。H は 16 ビットの 16 進数です。

たとえば、MAC アドレスが 00-0C-F1-42-4C-DE の場合、000C.F142.4CDE と入力します。MAC アドレスはマルチキャスト ビット セットを持つことはできません。つまり、左から 2 番目の 16 進数字を奇数にすることはできません。

ステップ 5 [スタンバイMACアドレス（Standby MAC Address）] フィールドに、ハイ アベイラビリティで使用する MAC アドレスを入力します。

アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

ステップ 6 [OK] をクリックします。

ステップ 7 [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。

スタティック ARP エントリの追加

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

デフォルトでは、ブリッジグループのメンバーの間ですべてのARPパケットが許可されます。ARP パケットのフローを制御するには、ARP インスペクションを有効にします（ARP インスペクションの設定 参照）。ARP インスペクションは、ARP パケットを ARP テーブルのスタティック ARP エントリと比較します。

ルーテッド インターフェイスの場合、スタティック ARP エントリを入力できますが、通常はダイナミック エントリで十分です。ルーテッド インターフェイスの場合、直接接続されたホストにパケットを配送するために ARP テーブルが使用されます。送信者は IP アドレスでパケットの宛先を識別しますが、イーサネットにおける実際のパケット配信は、イーサネット MAC アドレスに依存します。ルータまたはホストは、直接接続されたネットワークでパケットを配信する必要がある場合、IP アドレスに関連付けられた MAC アドレスを要求する ARP 要求を送信し、ARP 応答に従ってパケットを MAC アドレスに配信します。ホストまたはルータには ARP テーブルが保管されるため、配信が必要なパケットごとに ARP 要求を送信する必要はありません。ARPテーブルは、ARP応答がネットワーク上で送信されるたびにダイナミックに更新されます。一定期間使用されなかったエントリは、タイムアウトします。エントリが正しくない場合（たとえば、所定のIPアドレスのMACアドレスが変更された場合など）、新しい情報で更新される前にこのエントリがタイムアウトする必要があります。

トランスペアレントモードの場合、管理トラフィックなどのFTDデバイスとの間のトラフィックに、FTD は ARP テーブルのダイナミック ARP エントリのみを使用します。

始める前に

この画面は、名前付きインターフェイスについてのみ使用できます。

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 [詳細（Advanced）] タブをクリックして、[ARP] タブをクリックします（トランスペアレントモードでは、[ARP と MAC（ARP and MAC）]）。

ステップ 4 [ARP 設定を追加（Add ARP Config）] をクリックします。
[ARP 設定を追加（Add ARP Config）] ダイアログボックスが表示されます。

ステップ 5 [IP アドレス（IP Address）] フィールドに、ホストの IP アドレスを入力します。

ステップ 6 [MAC アドレス（MAC Address）] フィールドに、ホストの MAC アドレスを入力します。たとえば、「00e0.1e4e.3d8b」のように入力します。

ステップ 7 このアドレスでプロキシ ARP を実行するには、[エイリアスを有効にする（Enable Alias）] チェックボックスをオンにします。

FTD デバイスは、指定された IP アドレスの ARP 要求を受信すると、指定された MAC アドレスで応答します。

ステップ 8 [OK] をクリックし、次にもう一度 [OK] をクリックして、[詳細設定（Advanced settings）] を閉じます。

ステップ 9 [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。

静的 MAC アドレスの追加とのブリッジ グループの MAC 学習の無効化

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

通常、MACアドレスは、特定のMACアドレスからのトラフィックがインターフェイスに入ったときに、MAC アドレス テーブルに動的に追加されます。MAC アドレス ラーニングを無効にすることができます。ただし、MAC アドレスをスタティックにテーブルに追加しないかぎり、トラフィックは FTD デバイスを通過できません。スタティック MAC アドレスは、MAC アドレス テーブルに追加することもできます。スタティック エントリを追加する利点の 1 つに、MAC スプーフィングに対処できることがあります。スタティック エントリと同じ MAC アドレスを持つクライアントが、そのスタティックエントリに一致しないインターフェイスにトラフィックを送信しようとした場合、FTDデバイスはトラフィックをドロップし、システム

メッセージを生成します。スタティック ARP エントリを追加するときに（スタティック ARP エントリの追加 （43 ページ） を参照）、スタティック MAC アドレス エントリは MAC アドレス テーブルに自動的に追加されます。

始める前に

この画面は、名前付きインターフェイスについてのみ使用できます。

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 [詳細（Advanced）] タブをクリックして、[ARP と MAC（ARP and MAC）] タブをクリックします。

ステップ 4 （任意） [MAC ラーニングを有効にする（Enable MAC Learning）] チェックボックスをオフにして MAC ラーニングを無効にします。

ステップ 5 スタティック MAC アドレスを追加するには、[MAC 設定を追加（Add MAC Config）] をクリックします。
[MAC 設定を追加（Add MAC Config）] ダイアログボックスが表示されます。

ステップ 6 [MAC アドレス（MAC Address）] フィールドに、ホストの MAC アドレスを入力します。たとえば、「00e0.1e4e.3d8b」のように入力します。[OK] をクリックします。

ステップ 7 [OK] をクリックして詳細設定を終了します。

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。

セキュリティの設定パラメータの設定

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

この項では、IP スプーフィングの防止方法、完全フラグメント リアセンブルの許可方法、および [プラットフォーム設定（Platform Settings）] でデバイス レベルで設定されるデフォルトのフラグメント設定のオーバーライド方法について説明します。

アンチ スプーフィング

この項では、インターフェイスでユニキャスト リバース パス フォワーディング（ユニキャスト RPF）を有効にします。ユニキャスト RPF は、ルーティング テーブルに従って、すべてのパケットが正しい送信元インターフェイスと一致する送信元 IP アドレスを持っていることを確認して、IP スプーフィング（パケットが不正な送信元 IP アドレスを使用し、実際の送信元を隠蔽すること）から保護します。

通常、FTDデバイスは、パケットの転送先を判定するときに宛先アドレスだけを調べます。ユニキャストRPFは、送信元アドレスも調べるようにデバイスに指示します。そのため、リバース パス フォワーディング（Reverse Path Forwarding）と呼ばれます。FTD デバイスの通過を許可するすべてのトラフィックについて、送信元アドレスに戻るルートをデバイスのルーティング テーブルに含める必要があります。詳細については、RFC 2267 を参照してください。

たとえば、外部トラフィックの場合、FTD デバイスはデフォルト ルートを使用してユニキャスト RPF 保護の条件を満たすことができます。トラフィックが外部インターフェイスから入り、送信元アドレスがルーティング テーブルにない場合、デバイスはデフォルト ルートを使用して、外部インターフェイスを送信元インターフェイスとして正しく識別します。

ルーティングテーブルにあるアドレスから外部インターフェイスにトラフィックが入り、このアドレスが内部インターフェイスに関連付けられている場合、FTD デバイスはパケットをドロップします。同様に、未知の送信元アドレスから内部インターフェイスにトラフィックが入った場合は、一致するルート（デフォルトルート）が外部インターフェイスを示しているため、デバイスはパケットをドロップします。

ユニキャスト RPF は、次のように実装されます。

- ICMP パケットにはセッションがないため、個々のパケットはチェックされません。
- UDP と TCP にはセッションがあるため、最初のパケットは逆ルート ルックアップが必要です。セッション中に到着する後続のパケットは、セッションの一部として保持されている既存の状態を使用してチェックされます。最初のパケット以外のパケットは、最初のパケットと同じインターフェイスに到着したことを保証するためにチェックされます。

パケットあたりのフラグメント

デフォルトでは、FTD デバイスは 1 つの IP パケットにつき最大 24 のフラグメントを許可し、最大 200 のフラグメントのリアセンブリ待ちを許可します。NFS over UDP など、アプリケーションが日常的にパケットをフラグメント化する場合は、ネットワークでフラグメント化を許可する必要があります。ただし、トラフィックをフラグメント化するアプリケーションがない場合は、フラグメントが FTD デバイスを通過できないようにすることをお勧めします。フラグメント化されたパケットは、DoS 攻撃によく使われます。

フラグメントのリアセンブル

FTD デバイスは、次に示すフラグメント リアセンブル プロセスを実行します。

- IP フラグメントは、フラグメント セットが作成されるまで、またはタイムアウト間隔が経過するまで収集されます。
- フラグメントセットが作成されると、セットに対して整合性チェックが実行されます。これらのチェックには、重複、テール オーバーフロー、チェーン オーバーフローはいずれも含まれません。

- FTD デバイスで終端する IP フラグメントは、常に完全にリアセンブルされます。
- [完全フラグメント リアセンブル（Full Fragment Reassembly）] が無効化されている場合（デフォルト）、フラグメントセットは、さらに処理するためにトランスポート層に転送されます。
- [完全フラグメント リアセンブル（Full Fragment Reassembly）] が有効化されている場合、フラグメント セットは、最初に単一の IP パケットに結合されます。この単一の IP パケットは、さらに処理するためにトランスポート層に転送されます。

始める前に

この画面は、名前付きインターフェイスでのみ使用できます。

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 [詳細（Advanced）] タブをクリックして、[セキュリティ設定（Security Configuration）] タブをクリックします。

ステップ 4 ユニキャスト リバース パス フォワーディングを有効にするには、[アンチ スプーフィング（Anti-Spoofing）] チェックボックスをオンにします。

ステップ 5 完全フラグメント リアセンブルを有効化するには、[完全フラグメント リアセンブル（Full Fragment Reassembly）] チェックボックスをオンにします。

ステップ 6 パケットごとに許容するフラグメント数を変更するには、[デフォルト フラグメント設定のオーバーライド（Override Default Fragment Setting）] チェックボックスをオンにして、次に示す値を設定します。

- サイズ（Size）：リアセンブルを待機する IP リアセンブル データベースに格納可能なパケットの最大数を設定します。デフォルトは 200 です。この値を 1 に設定すると、フラグメントが無効化されます。
- チェーン（Chain）：1 つの完全な IP パケットにフラグメント化できる最大パケット数を指定します。デフォルトは 24 パケットです。
- タイムアウト（Timeout）：フラグメント化されたパケット全体が到着するまで待機する最大秒数を指定します。タイマーは、パケットの最初のフラグメントの到着後に開始されます。指定した秒数までに到着しなかったパケット フラグメントがある場合、到着済みのすべてのパケット フラグメントが廃棄されます。デフォルトは 5 秒です。

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。

Firepower Threat Defense の通常のファイアウォール インターフェイスの履歴

機能	バージョン（Version）	詳細
コンテナ インスタンスで使用される VLAN サブインターフェイス	6.3.0	柔軟な物理インターフェイスの使用を可能にするため、FXOS で VLAN サブインターフェイスを作成し、複数のインスタンス間でインターフェイスを共有することができます。 新規/変更された Firepower Management Center 画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [編集（Edit）]** アイコン **> [インターフェイス（Interfaces）]** タブ 新規/変更された Firepower Chassis Manager 画面： **[Interfaces] > [All Interfaces] > [Add New]** ドロップダウン メニュー **> [Subinterface]** 新規/変更された FXOS コマンド：**create subinterface、set vlan、show interface、show subinterface** サポートされるプラットフォーム：Firepower 4100/9300
コンテナ インスタンスのデータ共有インターフェイス	6.3.0	柔軟な物理インターフェイスの使用を可能にするため、複数のインスタンス間でインターフェイスを共有することができます。 新規/変更された Firepower Chassis Manager 画面： **[Interfaces] > [All Interfaces] > [Type]** 新規/変更された FXOS コマンド：**set port-type data-sharing、show interface** サポートされるプラットフォーム：Firepower 4100/9300

機能	バージョン（Version）	詳細
統合ルーティングおよびブリッジング	6.2.0	統合ルーティングおよびブリッジングによって、ブリッジ グループとルーテッド インターフェイスの間でルーティングする機能が提供されます。ブリッジグループは、FTD がルーティングではなくブリッジするインターフェイスのグループです。FTD は、FTD がファイアウォールとして機能し続ける点で本来のブリッジとは異なります。つまり、インターフェイス間のアクセス制御が実行され、通常のファイアウォール検査もすべて実行されます。以前は、トランスペアレント ファイアウォール モードでのみブリッジグループの設定が可能だったため、ブリッジグループ間でのルーティングはできませんでした。この機能を使用すると、ルーテッド ファイアウォール モードのブリッジ グループの設定と、ブリッジグループ間およびブリッジグループとルーテッドインターフェイス間のルーティングを実行できます。ブリッジグループは、ブリッジ仮想インターフェイス（BVI）を使用して、ブリッジグループのゲートウェイとして機能することによってルーティングに参加します。FTD にブリッジグループを割り当てるための追加インターフェイスがある場合、統合ルーティングおよびブリッジングによって、外部のレイヤ2スイッチを使用するのではない別の方法が提供されます。ルーテッドモードでは、BVIは名前付きインターフェイスとなり、アクセス ルールや DHCP サーバなどの一部の機能に、メンバー インターフェイスとは個別に参加できます。 トランスペアレント モードでサポートされるクラスタリングの機能は、ルーテッド モードではサポートされません。マルチキャスト ルーティングとダイナミック ルーティングの機能も、BVI ではサポートされません。 新しい/変更された画面： • **[Devices] > [Device Management] > [Interfaces] > [Edit Physical Interface]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > -[インターフェイスを追加（Add Interfaces）] > [ブリッジ グループ インターフェイス（Bridge Group Interface）]** サポートされるプラットフォーム：すべて（Firepower 2100 と Firepower Threat Defense Virtual を除く）