インターフェイス

ここでは、Firepower Threat Defense デバイスでのインターフェイスの設定方法について説明します。

Firewall Threat Defense インターフェイスについて

Firewall Threat Defense には、データインターフェイスやManagement/Diagnosticインターフェイスが組み込まれています。

インターフェイス接続（物理的または仮想）のためにケーブルを接続するとき、インターフェイスを設定する必要があります。最小限の作業として、トラフィックを通過させることができるようにインターフェイスを指定して有効化します。インターフェイスがブリッジグループのメンバーである場合、これで十分です。ブリッジ グループのメンバーでない場合、インターフェイスにIPアドレスを割り当てる必要があります。単一の物理インターフェイスではなく、VLANサブインターフェイスを特定のポートで作成する場合、通常、物理インターフェイスではなくサブインターフェイス上で IP アドレスを設定します。VLAN サブインターフェイスを使用すると、物理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。これは、スイッチのトランク ポートに接続する場合に役立ちます。パッシブインターフェイスでは IP アドレスを設定しません。

[インターフェイス（Interfaces）]ページには、インターフェイスタイプのサブページが含まれます。これらは、[インターフェイス（Interfaces）]（物理インターフェイスの場合）、[ブリッジグループ（Bridge Groups）]、[仮想トンネルインターフェイス（Virtual Tunnel Interfaces）]、[EtherChannel]、および[VLAN（VLANs）]（Firepower 1010 の場合）です。Firepower 4100/9300 EtherChannel は [インターフェイス（Interfaces）] ページには表示されますが、[EtherChannel] ページには表示されないことに注意してください。これは、Firewall Device Manager ではなく FXOS の EtherChannel パラメータのみを変更できるためです。各ページに、利用可能なインターフェイスとそれぞれの名前、アドレス、モード、状態が示されます。インターフェイスのステータスは、インターフェイスのリストで直接オン/オフを変更できます。このリストは、設定に基づいたインターフェイス特性を示します。メンバーインターフェイスを参照するには、ブリッジグループ、EtherChannel、または VLAN インターフェイス上で [開く/閉じる（open/close）] 矢印を使用します。メンバーインターフェイスは対応するリストにも表示されます。サポートされている親インターフェイスのサブインターフェイスを表示することもできます。

以下の各トピックでは、Firewall Device Manager を使用してインターフェイスを設定する場合の制限事項、およびインターフェイス管理に関するその他の概念について説明します。

インターフェイス モード

インターフェイスごとに次のモードのいずれかを設定できます。

ルーテッド

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。通常、これらのインターフェイスをスイッチ、別のルータ上のポート、またはISP/WANゲートウェイに接続します。

パッシブ

パッシブ インターフェイスは、スイッチ SPAN（スイッチド ポート アナライザ）またはミラーポートを使用してネットワーク全体を流れるトラフィックをモニターします。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。

スイッチポート（Firepower 1010）

スイッチポートは、ハードウェアのスイッチ機能を使用して、レイヤ2でトラフィックを転送します。同じ VLAN 上のスイッチポートは、ハードウェアスイッチングを使用して相互に通信できます。トラフィックには、Firepower Threat Defense セキュリティポリシーは適用されません。アクセスポートはタグなしトラフィックのみを受け入れ、単一のVLANに割り当てることができます。トランクポートはタグなしおよびタグ付きトラフィックを受け入れ、複数のVLANに属することができます。管理インターフェイスをスイッチポートとして設定することはできません。

BridgeGroupMember

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。すべてのインターフェイスは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。

BVI に名前を付けると、ルーテッド インターフェイスと BVI の間のルーティングを実行できます。この場合、BVI はメンバー インターフェイスとルーテッド インターフェイス間のゲートウェイとして機能します。BVI に名前を指定しない場合、ブリッジ グループメンバーのインターフェイス上のトラフィックはブリッジ グループを離れることができません。通常、インターネットにメンバーインターフェイスをルーティングするため、インターフェイスに名前を付けます。

ルーテッドモードでブリッジグループを使用する方法として、外部スイッチの代わりに Firepower Threat Defense デバイスの予備インターフェイスを使用する方法があります。ブリッジ グループのメンバー インターフェイスにエンドポイントを直接接続できます。また、BVI と同じネットワークにより多くのエンドポイントを追加するために、スイッチを接続できます。

管理/診断インターフェイス

管理ラベル付けされた物理ポート（または、FTDv の場合は Management0/0 仮想インターフェイス）には、2 つの別個のインターフェイスが実際に関連付けられています。

- 管理仮想インターフェイス：この IP アドレスは、システムの通信に使用されます。これはシステムがスマートライセンスに使用し、データベースの更新情報を取得するためのアドレスです。これに対して管理セッションを開くことができます（Firewall Device Manager および CLI）。**[システム設定（System Settings）]**>**[管理インターフェイス（Management Interface）]** で定義されている管理アドレスを設定する必要があります。
- 診断仮想インターフェイス：このインターフェイスを使用して、syslog のメッセージを外部 syslog サーバに送信できます。診断インターフェイスの IP アドレスを設定するかは任意です。インターフェイスを設定する主な理由は、それを syslog メッセージに使用することです。このインターフェイスは、**[デバイス（Device）]**>**[インターフェイス（Interfaces）]** ページに表示され、そこで設定できます。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。

（ハードウェアデバイス）管理/診断を設定する一つの方法は、物理ポートをネットワークに接続しないことです。代わりに、管理 IP アドレスのみを設定し、インターネットからの更新情報を得るためのゲートウェイとして、データインターフェイスを使用するように設定します。次に、HTTPS/SSH トラフィック（デフォルトで HTTPS は有効）への内部インターフェイスを開き、内部 IP アドレスを使用して Firewall Device Manager を開きます（管理アクセス リストの設定 を参照）。

FTDv の推奨設定は、Management0/0 を内部インターフェイスと同じネットワークに接続し、内部インターフェイスをゲートウェイとして使用することです。診断用に別のアドレスを設定しないでください。

個別の管理ネットワークの設定に関する推奨事項

（ハードウェアデバイス）分離した管理ネットワークを使用する場合は、物理的管理インターフェイスをスイッチまたはルータに有線で接続します。

Firewall Threat Defense Virtual では、Management0/0 を任意のデータ インターフェイスから個別のネットワークに接続します。デフォルトの IP アドレスを使用している場合、管理 IP アドレスまたは内部インターフェイス IP アドレスは同一サブネット上にあるため、いずれかを変更する必要があります。

その後、次の設定を行います。

- **[デバイス（Device）] > [システム設定（System Settings）] > [管理インターフェイス（Management Interface）]** を選択して、接続されたネットワークで IPv4 または IPv6 アドレス（あるいはその両方）を設定します。必要に応じて、ネットワーク上の他のエンドポイントに IPv4 アドレスを指定するように DHCP サーバーを設定できます。管理ネットワーク上にインターネットへのルートを持つルータがある場合、それをゲートウェイとして使用します。なければ、データ インターフェイスをゲートウェイとして使用します。
- インターフェイスを介して syslog サーバーに syslog メッセージを送信しようとする場合にのみ、診断インターフェイスのアドレスを設定します（**[デバイス（Device）] > [インターフェイス（Interfaces）]**）。それ以外の場合は、不要なので診断インターフェイスのアドレスは設定しないでください。設定する IP アドレスは、管理 IP アドレスと同じサブネット上に存在する必要があります。DHCP サーバー プールに設定することはできません。たとえば、192.168.45.45 を管理アドレスとして使用し、192.168.45.46 から 192.168.45.254 までを DHCP プールとして使用する場合、診断インターフェイスには、192.168.45.1 から 192.168.45.44 の範囲内にある任意のアドレスを使用できます。

セキュリティ ゾーン

各インターフェイスは単一のセキュリティ ゾーンに割り当てることができます。ゾーンに基づいてセキュリティ ポリシーを適用されます。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。

各ゾーンにはインターフェイスのモードに直接関係するモードがあります。インターフェイスは、同じモードのセキュリティゾーンにのみ追加できます。

ブリッジ グループでは、メンバー インターフェイスをゾーンに追加できますが、ブリッジ仮想インターフェイス（BVI）を追加することはできません。

ゾーンにManagement/Diagnosticインターフェイスは含めないでください。ゾーンは、データ インターフェイスにのみ適用されます。

セキュリティ ゾーンは [オブジェクト（Objects）] ページで作成できます。

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、各メンバー インターフェイスではなくブリッジ仮想インターフェイス（BVI）上でグローバル アドレスを設定します。次のいずれかをグローバル アドレスとして指定することはできません。
  - 内部で予約済みの IPv6 アドレス：fd00::/56 (from=fd00:: to= fd00:0000:0000:00ff:ffff:ffff:ffff:ffff)
  - 未指定のアドレス（::/128 など）
  - ループバック アドレス（::1/128）
  - マルチキャスト アドレス（ff00::/8）
  - リンクローカル アドレス（fe80::/10）
- 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およびネイバー探索などのネットワーク検出機能に使用できます。ブリッジ グループでは、BVI で IPv6 を有効にすると、自動的に各ブリッジ グループのメンバー インターフェイスのリンクローカル アドレスが設定されます。リンクローカル アドレスがセグメントでのみ使用可能であり、インターフェイス MAC アドレスに接続されているため、各インターフェイスは独自のアドレスを持つ必要があります。

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。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。

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。

インターフェイスに関する注意事項と制約事項

ここでは、インターフェイスに関する制限事項について説明します。

インターフェイス設定の制限事項

Firewall Device Manager を使用してデバイスを設定する場合、インターフェイス設定に関するいくつかの制限があります。次の機能のいずれかが必要である場合、デバイスを設定するためにFMCを使用する必要があります。

- ルーテッド ファイアウォール モードのみがサポートされます。トランスペアレント ファイアウォール モードのインターフェイスは設定できません。
- パッシブ インターフェイスの設定は可能ですが、ERSPAN インターフェイスを設定することはできません。
- インターフェイスをインライン（インラインセット内）またはインラインタップ（IPSオンリー処理用）に設定することはできません。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。対照的に、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、TCP の標準化などのファイアウォール機能の対象となります。また、任意で、セキュリティ ポリシーに従ってファイアウォールモードのトラフィックにIPS機能を設定することもできます。
- 冗長インターフェイスは設定できません。
- 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 4100/9300 の Etherchannel は、単一の物理インターフェイスとともに Firewall Device Manager の [Interfaces] ページに表示されます。
- 追加できるブリッジ グループは 1 つだけです。
- Firewall Threat Defense は、ルーテッドインターフェイスでのみ IPv4 PPPoE をサポートします。PPPoE は、ハイアベイラビリティ ユニットではサポートされません。

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 1010	60
Firepower 1120	512
Firepower 1140、1150	1024
Firepower 2100	1024
Firepower 4100	1024
Firepower 9300	1024
FTDv	50
ASA 5508-X	50
ASA 5516-X	100
ISA 3000	100

物理インターフェイスの設定

少なくとも、使用する物理インターフェイスは有効にする必要があります。通常は名前も付けて、IP アドレッシングを設定します。VLAN サブインターフェイスを設定する予定の場合、パッシブ モード インターフェイスを設定している場合、またはインターフェイスをブリッジグループに追加する予定の場合は、IP アドレッシングを設定しません。 Firepower 4100/9300 EtherChannel は、単一の物理インターフェイスとともに Firewall Device Manager の [インターフェイス（Interfaces）] ページに表示され、この手順はそれらの EtherChannel にも適用されます。シャーシ上の FXOS で、Firepower 4100/9300 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。

（注） 物理インターフェイスを Firepower 1010 スイッチポートとして設定するには、VLAN インターフェイスとスイッチポートの構成 （31 ページ）を参照してください。

物理インターフェイスをパッシブインターフェイスとして設定するには、パッシブ モードでの物理インターフェイスの設定 （54 ページ）を参照してください。

接続されたネットワークでの送信を一時的に防ぐために、インターフェイスを無効にできます。インターフェイスの設定を削除する必要はありません。

手順

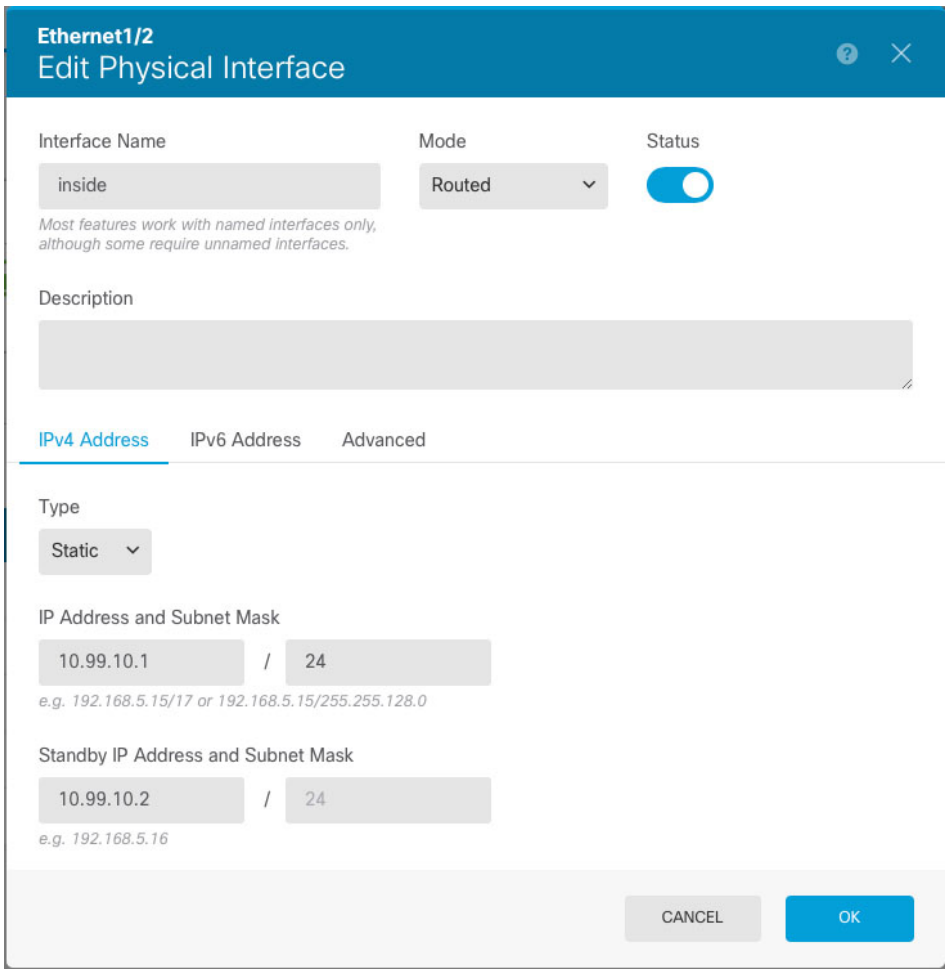
ステップ 1 [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックします。

[インターフェイス（Interfaces）] タブがデフォルトで選択されます。インターフェイスリストに、物理インターフェイスとそれぞれの名前、アドレス、状態が表示されます。

ステップ 2 編集する物理インターフェイスの [編集（edit）] アイコン（）をクリックします。

高可用性設定でフェールオーバー リンクまたはステートフル フェールオーバー リンクとして使用しているインターフェイスを編集することはできません。

ステップ 3 次の設定を行います。



a) [インターフェイス名（Interface Name）] を設定します。

インターフェイスの名前（最大 48 文字）を設定します。英字は小文字にする必要があります。例、[inside] または [outside]。名前を設定しないと、インターフェイスの残りの設定

は無視されます。サブインターフェイスを設定する場合を除き、インターフェイスには名前が必要です。**注**：EtherChannel に追加するインターフェイスの名前は設定しないでください。

（注）
名前を変更すると、その変更は古い名前を使用しているすべての場所（セキュリティゾーン、syslog サーバ オブジェクト、DHCP サーバの定義を含む）に自動的に反映されます。ただし、通常、ポリシーや設定に名前のないインターフェイスは使用できないため、最初に古い名前を使用しているすべての設定を削除しないと、その名前は削除できません。

b) [モード（Mode）]を選択します。

- [ルーテッド（Routed）]：ルーテッド モード インターフェイスでは、トラフィックはフローの維持、IP 層と TCP 層の両方でのフロー状態のトラッキング、IP の最適化、TCP の正規化、ファイアウォール ポリシーなど、すべてのファイアウォール機能の管理下に置かれます。これが通常のインターフェイス モードです。
- [パッシブ（Passive）]：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中のトラフィック フローをモニタします。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。このモードを選択する場合、残りの手順は実行しないでください。代わりに、パッシブ モードでの物理インターフェイスの設定 （54 ページ）を参照してください。パッシブインターフェイスには IP アドレスを設定できません。
- [スイッチポート（Switch Port）]：（Firepower 1010）スイッチポートは、同じ VLAN 上のポート間でのハードウェアスイッチングを可能にします。スイッチングされたトラフィックはセキュリティポリシーの対象にはなりません。このモードを選択する場合、残りの手順は実行しないでください。代わりに、次を参照してください。 VLAN インターフェイスとスイッチポートの構成 （31 ページ）

後でこのインターフェイスをブリッジ グループに追加すると、モードは自動的に「BridgeGroupMember」に変更されます。ブリッジグループのメンバーインターフェイスには IP アドレスを設定できません。

c) [ステータス（Status）] スライダを [有効（enabled）] 設定（  ）に設定します。

Firepower 4100/9300 デバイス上のインターフェイスの場合は、FXOS でもインターフェイスを有効にする必要があります。

この物理インターフェイスのサブインターフェイスを設定する予定の場合、すでに設定している可能性が高いです。[保存（Save）] をクリックして、VLAN サブインターフェイスと 802.1Q トランキングの設定 （45 ページ）に進みます。保存しない場合は、次に進みます。

（注）
サブインターフェイスを設定している場合でも、インターフェイスに名前を付けて、IPアドレスを指定できます。これは一般的な設定ではありませんが、必要だとわかっている場合は設定できます。

d) （任意）[説明（Description）] を設定します。

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 4 [IPv4アドレス（IPv4 Address）] タブをクリックして、IPv4 アドレスを設定します。

[タイプ（Type）] フィールドから次のいずれかのオプションを選択します。

- [DHCP]：ネットワーク上の DHCP サーバからアドレスを取得する場合は、このオプションを選択します。高可用性を設定する場合、このオプションは使用できません。必要に応じて、次のオプションを変更します。
  - [ルートメトリック（Route Metric）]：DHCP サーバからデフォルト ルートを取得する場合、学習済みルートまでのアドミニストレーティブ ディスタンスは 1 ~ 255 の間です。デフォルトは 1 です。
  - [デフォルトルートを取得（Obtain Default Route）]：デフォルト ルートを DHCP サーバから取得するかどうかを指定します。通常は、デフォルトのこのオプションを選択します。
- [スタティック（Static）]：変更されないアドレスを割り当てる場合は、このオプションを選択します。インターフェイスに接続されたネットワークに対するインターフェイスの IP アドレスとサブネット マスクを入力します。たとえば、10.100.10.0/24 ネットワークを接続する場合は、「10.100.10.1/24」と入力します。このアドレスがネットワーク上ですでに使用されていないことを確認します。

  高可用性を設定し、このインターフェイスの HA をモニタしている場合は、同じサブネット上のスタンバイ IP アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。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。

  （注）
  インターフェイスに対して設定されている DHCP サーバがある場合は、その設定が表示されます。DHCP アドレス プールを編集または削除できます。インターフェイスの IP アドレスを別のサブネットに変更する場合は、インターフェイスの変更を保存する前に、DHCP サーバを削除するか、新しいサブネット上にアドレス プールを構成する必要があります。DHCP サーバの設定を参照してください。
- [PPPoE]：イーサネット経由のポイントツーポイント プロトコル（PPPoE）を使用してアドレスを取得する必要がある場合は、このオプションを選択します。インターフェイスが DSL モデム、ケーブルモデム、または ISP への他の接続に接続されており、ISP が PPPoE を使用して IP アドレスを提供している場合は、PPPoE が必要になる場合があります。高可用性を設定する場合、このオプションは使用できません。次の値を設定します。

- [グループ名（Group Name）]：この接続を表すために選択した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（PPPoE Password）]：ISP によって提供されたパスワードを指定します。
- [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の学習済みルートメトリック（PPPoE Learned Route Metric）]：アドミニストレーティブ ディスタンスを既知の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。
- [PPPoEからデフォルトルートを取得（Obtain Default Route from PPPoE）]：PPPoE サーバからのデフォルトルートの取得を有効にするには、このチェックボックスをオンにします。
- [IPアドレスタイプ（IP Address Type）]：PPPoE サーバから IP アドレスを取得するには、[動的（Dynamic）] を選択します。ISP から静的 IP アドレスが割り当てられている場合は、[静的（Static）] を選択することもできます。

ステップ 5 （オプション）[IPv6アドレス（IPv6 Address）] タブをクリックして、IPv6 アドレスを設定します。

- [状態（State）]：グローバル アドレスを設定しない場合に IPv6 処理を有効にしてリンクローカルアドレスを自動的に設定するには、[有効（Enabled）] を選択します。リンクローカル アドレスはインターフェイスの MAC アドレス（*Modified* EUI-64 形式）に基づいて生成されます。

  （注）
  IPv6 を無効にしても、明示的な IPv6 アドレスを指定して設定されているインターフェイス、または自動設定が有効になっているインターフェイスの IPv6 処理は無効になりません。

- [アドレスの自動設定（Address Auto Configuration）]：アドレスを自動的に設定するには、このオプションを選択します。IPv6 ステートレス自動設定では、デバイスが存在するリンクで使用する IPv6 グローバル プレフィックスのアドバタイズメントなどの、IPv6 サービスを提供するようにルータが設定されている場合に限り、グローバルな IPv6 アドレスが生成されます。IPv6 ルーティング サービスがリンクで使用できない場合、リンクローカ

ル IPv6 アドレスのみが取得され、そのデバイスが属するネットワーク リンクの外部にはアクセスできません。リンクローカル アドレスは Modified EUI-64 インターフェイス ID に基づいています。

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。メッセージを抑制して、RFC に準拠するためには、[RA を抑制（Suppress RA）] を選択します。

- [スタティックアドレスとプレフィックス（Static Address/Prefix）]：ステートレス自動設定を使用しない場合、完全なスタティック グローバル IPv6 アドレスとネットワーク プレフィックスを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。IPv6 アドレッシングの詳細については、IPv6 アドレス指定 （5 ページ）を参照してください。

  アドレスをリンクローカル専用として使用する場合は、[リンクローカル（Link - Local）] オプションを選択します。リンクローカル アドレスでは、ローカル ネットワークの外部にはアクセスできません。リンクローカル アドレスはブリッジ グループ インターフェイスには設定できません。

  （注）
  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。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。

- [スタンバイ IP アドレス（Standby IP Address）]：高可用性を設定し、このインターフェイスの HA をモニタリングしている場合は、同じサブネット上にスタンバイ IPv6 アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。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。

- [RA を抑制（Suppress RA）]：ルータ アドバタイズメントを抑制するかどうかを指定します。ネイバー デバイスがデフォルトのルータ アドレスをダイナミックに把握できるように、FTD はルータ アドバタイズメントに参加できます。デフォルトでは、ルータ アドバタイズメント メッセージ（ICMPv6 Type 134）は、設定済みの各 IPv6 インターフェイスに定期的に送信されます。

  ルータ アドバタイズメントもルータ要請メッセージ（ICMPv6 Type 133）に応答して送信されます。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できます。

  FTD 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抑制できます。

ステップ 6 （任意）詳細オプションの設定 （58 ページ）。

詳細設定には、ほとんどのネットワークに適しているデフォルト設定があります。デフォルト設定はネットワークの問題を解決する場合のみ編集します。

ステップ 7 **[OK]** をクリックします。

次のタスク

- インターフェイスを適切なセキュリティゾーンに追加します。セキュリティ ゾーンの設定を参照してください。

ブリッジ グループの設定

ブリッジ グループは 1 つ以上のインターフェイスをグループ化する仮想インターフェイスです。インターフェイスをグループ化する主な理由は、スイッチドインターフェイスのグループを作成することにあります。そのため、ブリッジグループに含まれているインターフェイスにワークステーションやその他のエンドポイントデバイスを直接接続できます。それらは別の物理スイッチを介して接続する必要はありませんが、スイッチをブリッジ グループ メンバーに接続することもできます。

グループ メンバーには IP アドレスはありません。代わりに、すべてのメンバー インターフェイスがブリッジ仮想インターフェイス（BVI）の IP アドレスを共有します。BVI で IPv6 を有効にすると、メンバー インターフェイスには一意のリンクローカル アドレスが自動的に割り当てられます。

メンバーインターフェイスは個別に有効または無効にします。そのため、未使用のインターフェイスはブリッジ グループから削除することなく無効化できます。ブリッジ グループ自体は常に有効になっています。

通常は、メンバー インターフェイス経由で接続されているエンドポイントの IP アドレスを提供するブリッジ グループ インターフェイス（BVI）に DHCP サーバーを設定します。ただし、必要に応じて、メンバー インターフェイスに接続されているエンドポイントにスタティック アドレスを設定できます。ブリッジ グループ内のすべてのエンドポイントには、ブリッジ グループの IP アドレスと同じサブネットの IP アドレスが必要です。

ガイドラインと制約事項

- ブリッジグループを 1 つ追加できます。
- Firewall Device Manager 定義の 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。
- Firepower 2100 シリーズ または Firewall Threat Defense Virtual デバイスにブリッジグループを設定することはできません。
- Firepower 1010 では、同じブリッジグループ内に論理 VLAN インターフェイスと物理ファイアウォール インターフェイスを混在させることはできません。

- ISA 3000 は、ブリッジグループ BVI1 を使用して事前に設定されています（名前は付けられていません。これは、ルーティングに参加しないことを意味します）。BVI1 にはすべてのデータインターフェイス（GigabitEthernet1/1（outside1）、GigabitEthernet1/2（inside1）、GigabitEthernet1/3（outside2）、および GigabitEthernet1/4（inside2））が含まれます。ネットワークに合わせて BVI1 IP アドレスを設定する必要があります。

始める前に

ブリッジグループのメンバーになるインターフェイスを設定します。具体的には、各メンバーインターフェイスは、次の要件を満たしている必要があります。

- インターフェイスには名前が必要です。
- 静的に、または DHCP を介してインターフェイス用に定義された IPv4 または IPv6 アドレスは設定できません。現在使用しているインターフェイスからアドレスを削除する必要がある場合、そのインターフェイスのその他の設定（アドレスを持つインターフェイスに依存するスタティック ルート、DHCP サーバー、NAT ルールなど）も削除する必要がある場合があります。
- インターフェイスをブリッジ グループに追加する前に、セキュリティ ゾーン（ゾーン内にある場合）からそのインターフェイスを削除し、そのインターフェイスのすべての NAT ルールを削除する必要があります。

手順

ステップ 1 [デバイス（Device）] をクリックし、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックし、[ブリッジグループ（Bridge Groups）] をクリックします。

ブリッジグループのリストに、既存のブリッジグループが表示されます。各ブリッジグループのメンバーインターフェイスを表示するには、開/閉矢印をクリックします。また、メンバーインターフェイスは[インターフェイス（Interfaces）]または[VLAN（VLANs）]ページでも個別に表示されます。

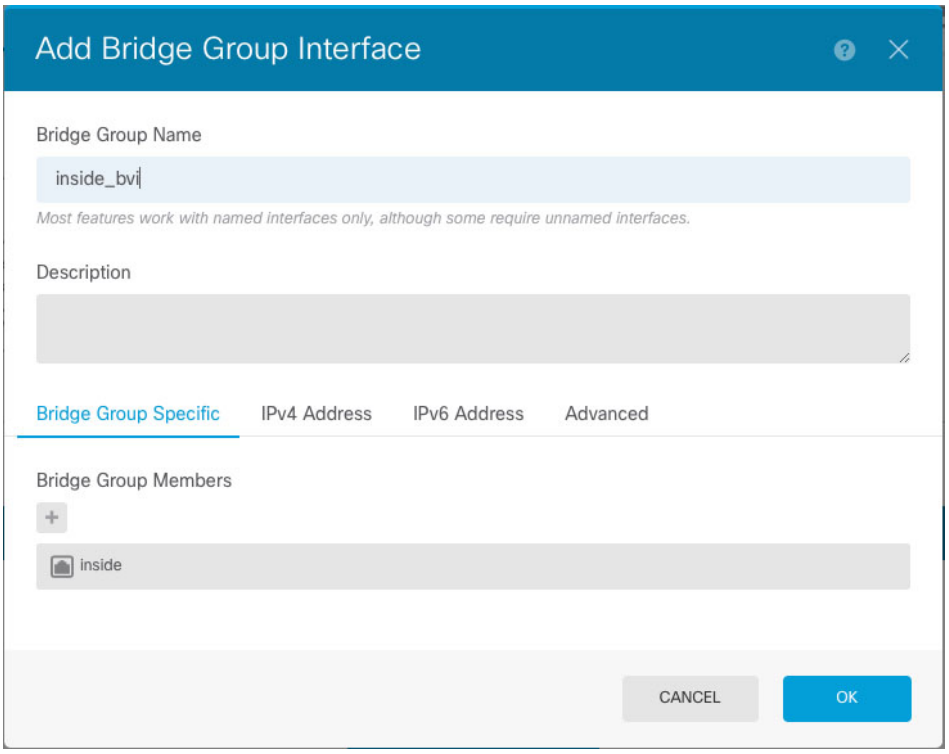
ステップ 2 次のいずれかを実行します。

- BVI1 ブリッジ グループの編集アイコン（  ）をクリックします。
- [ブリッジグループの作成（Create Bridge Group）] をクリックするか、プラス アイコン（  ）をクリックして、新しいグループを作成します。

（注）
ブリッジグループは1つ設定できます。ブリッジグループをすでに定義している場合は、新しいグループ作成するのではなく、そのグループを編集する必要があります。新しいブリッジ グループを作成する必要がある場合は、まず既存のブリッジ グループを削除する必要があります。

- 不要になったブリッジ グループの [削除（delete）] アイコン（）をクリックします。ブリッジ グループを削除すると、そのメンバーは標準のルーテッド インターフェイスになり、NAT ルールまたはセキュリティ ゾーンのメンバーシップはすべて維持されます。インターフェイスを編集して、IP アドレスを付与できます。新しいブリッジ グループにそれらのインターフェイスを追加する場合は、まず NAT ルールを削除し、インターフェイスをセキュリティ ゾーンから削除する必要があります。

ステップ 3 次を設定します。



a) （任意）[インターフェイス名（Interface Name）] を設定します。

ブリッジグループの名前（最大 48 文字）を設定します。英字は小文字にする必要があります。例、[inside] または [outside]。この BVI を他の名前付きインターフェイス間のルーティングに参加させる場合は、名前を設定します。

（注）
名前を変更すると、その変更は古い名前を使用しているすべての場所（セキュリティ ゾーン、syslog サーバ オブジェクト、DHCP サーバの定義を含む）に自動的に反映されます。ただし、通常、ポリシーや設定に名前のないインターフェイスは使用できないため、最初に古い名前を使用しているすべての設定を削除しないと、その名前は削除できません。

b) （任意）[説明（Description）] を設定します。

説明は 200 文字以内で、改行を入れずに 1 行で入力します。

c) [ブリッジグループメンバー（Bridge Group Members）] のリストを編集します。

1 つのブリッジ グループに最大 64 個のインターフェイスまたはサブインターフェイスを追加できます。

- インターフェイスの追加：プラスアイコン（+）をクリックし、1 つ以上のインターフェイスをクリックし、[OK] をクリックします。
- インターフェイスの削除：対象にカーソルを合わせ、右側に表示される [x] をクリックします。

ステップ 4 [IPv4アドレス（IPv4 Address）] タブをクリックして、IPv4 アドレスを設定します。

[タイプ（Type）] フィールドから次のいずれかのオプションを選択します。

- [スタティック（Static）]：変更されないアドレスを割り当てる場合は、このオプションを選択します。ブリッジ グループの IP アドレスとサブネット マスクを入力します。接続されているエンドポイントはすべて、このネットワーク上に存在することになります。このアドレスがネットワーク上ですでに使用されていないことを確認します。

  高可用性を設定し、このインターフェイスの HA をモニタしている場合は、同じサブネット上のスタンバイ IP アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。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。

  （注）
  インターフェイスに対して設定されている DHCP サーバがある場合は、その設定が表示されます。DHCP アドレス プールを編集または削除できます。インターフェイスの IP アドレスを別のサブネットに変更する場合は、インターフェイスの変更を保存する前に、DHCP サーバを削除するか、新しいサブネット上にアドレス プールを構成する必要があります。DHCP サーバの設定を参照してください。

- [ダイナミック（Dynamic）]（DHCP）：ネットワーク上の DHCP サーバーからアドレスを取得する必要がある場合は、このオプションを選択します。これはブリッジグループの一般的なオプションではありませんが、必要に応じて設定できます。高可用性を設定する場合、このオプションは使用できません。必要に応じて、次のオプションを変更します。
  - [ルートメトリック（Route Metric）]：DHCP サーバからデフォルト ルートを取得する場合、学習済みルートまでのアドミニストレーティブ ディスタンスは 1 ~ 255 の間です。デフォルトは 1 です。
  - [デフォルトルートを取得（Obtain Default Route）]：デフォルト ルートを DHCP サーバから取得するかどうかを指定します。通常は、デフォルトのこのオプションを選択します。

ステップ 5 （オプション）[IPv6アドレス（IPv6 Address）] タブをクリックして、IPv6 アドレスを設定します。

- [状態（State）]：グローバル アドレスを設定しない場合に IPv6 処理を有効にしてリンクローカル アドレスを自動的に設定するには、[有効（Enabled）] を選択します。リンクロー

カル アドレスはインターフェイスの MAC アドレス（*Modified* EUI-64 形式）に基づいて生成されます。

（注）
IPv6 を無効にしても、明示的な IPv6 アドレスを指定して設定されているインターフェイス、または自動設定が有効になっているインターフェイスの IPv6 処理は無効になりません。

- [スタティックアドレスとプレフィックス（Static Address/Prefix）]：ステートレス自動設定を使用しない場合、完全なスタティック グローバル IPv6 アドレスとネットワーク プレフィックスを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。IPv6 アドレッシングの詳細については、IPv6 アドレス指定 （5 ページ）を参照してください。

  アドレスをリンクローカル専用として使用する場合は、[リンクローカル（Link - Local）] オプションを選択します。リンクローカル アドレスでは、ローカル ネットワークの外部にはアクセスできません。リンクローカル アドレスはブリッジ グループ インターフェイスには設定できません。

  （注）
  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。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。

- [スタンバイIPアドレス（Standby IP Address）]：高可用性を設定し、このインターフェイスの HA をモニタリングしている場合は、同じサブネット上にスタンバイ IPv6 アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。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。

- [RAを抑制（Suppress RA）]：ルータ アドバタイズメントを抑制するかどうかを指定します。ネイバー デバイスがデフォルトのルータ アドレスをダイナミックに把握できるように、FTD デバイスはルータ アドバタイズメントに参加できます。デフォルトでは、ルータ アドバタイズメント メッセージ（ICMPv6 Type 134）は、設定済みの各 IPv6 インターフェイスに定期的に送信されます。

  ルータ アドバタイズメントもルータ要請メッセージ（ICMPv6 Type 133）に応答して送信されます。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できます。

  FTD 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抑制できます。

ステップ 6 （任意）詳細オプションの設定 （58 ページ）。

ブリッジグループメンバーインターフェイスに対して最も詳細なオプションを設定しますが、一部はブリッジ グループ インターフェイスでも使用できます。

詳細設定には、ほとんどのネットワークに適しているデフォルト設定があります。デフォルト設定はネットワークの問題を解決する場合のみ編集します。

ステップ 7 [OK] をクリックします。

次のタスク

- 使用する予定のすべてのメンバー 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。
- ブリッジ グループの DHCP サーバを設定します。DHCP サーバの設定を参照してください。
- メンバーインターフェイスを適切なセキュリティゾーンに追加します。セキュリティゾーンの設定を参照してください。
- アイデンティティ、NAT、アクセスなどのポリシーにより、ブリッジグループとメンバーインターフェイスに必要なサービスが提供されることを確認します。

EtherChannel の設定

ここでは、EtherChannel とそれらの設定方法について説明します。

（注） 次のモデルでは、Firewall Device Manager で EtherChannel を追加できます。

- Firepower 1000
- Firepower 2100
- ISA 3000

EtherChannel で Firepower 1010 または Cisco Secure Firewall 1210/1220 のスイッチポートまたは VLAN インターフェイスを使用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 4100/9300の Etherchannel は、単一の物理インターフェイスとともに Firewall Device Manager の [Interfaces] ページに表示されます。また、Firewall Threat Defense Virtual または ASA 5500-X シリーズなどの他のモデルでは、Firewall Device Manager で EtherChannel を設定できません。

EtherChannel 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 グループは、最大 8 個のアクティブ インターフェイスを設定できます。

チャネル グループのすべてのインターフェイスは、同じタイプと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。

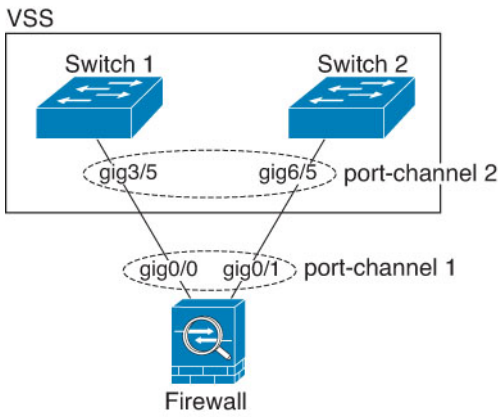
EtherChannel によって、チャネル内の使用可能なすべてのアクティブ インターフェイスのトラフィックが集約されます。インターフェイスは、送信元または宛先 MAC アドレス、IP アドレス、TCP および UDP ポート番号、および VLAN 番号に基づいて、独自のハッシュ アルゴリズムを使用して選択されます。

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。

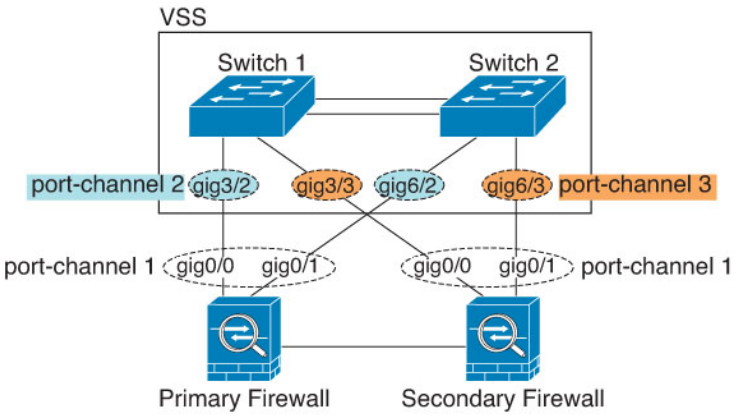
図 *1 : VSS/vPC* への接続



（注） FTD デバイスがトランスペアレント ファイアウォール モードになっており、2 組の VSS/vPC スイッチ間に FTD デバイスを配置する場合は、EtherChannel 内で FTD デバイスに接続されたすべてのスイッチポートで単方向リンク検出（UDLD）を無効にしてください。スイッチポートで UDLD を有効にすると、他の VSS/vPC ペアの両方のスイッチから送信された UDLD パケットを受信する場合があります。受信側スイッチの受信インターフェイスは「UDLD Neighbor mismatch」という理由でダウン状態になります。

FTD デバイスをアクティブ/スタンバイフェールオーバー展開で使用する場合、FTD デバイスごとに 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 デバイスで、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 デバイスに接続する単一の 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 デバイス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*



Link Aggregation Control Protocol（LACP）

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（Active）]：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。
- 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 デバイスは、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に送信され、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に、結果が 2 となるものは 3 番目のインターフェイスに、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。

Firepower ハードウェア

ポートチャネル インターフェイスは、内部インターフェイスの内部データ 0/1 の MAC アドレスを使用します。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。シャーシ上のすべての EtherChannel インターフェイスは同じ MAC アドレスを使用するため、たとえば、SNMP ポーリングを使用する場合、複数のインターフェイスが同じ MAC アドレスを持つことに注意してください。

（注） メンバーインターフェイスは、再起動後に内部データ 0/1 MAC アドレスのみを使用します。再起動する前に、メンバーインターフェイスは独自の MAC アドレスを使用するた再起動後に新しいメンバーインターフェイスを追加する場合、MAC アドレスを更新するためにもう一度再起動する必要があります。

ASA ハードウェア

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 インターフェイスのガイドライン

ブリッジ グループ

Firewall Device Manager 定義の 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。

高可用性（HA）

- EtherChannel インターフェイスを 高可用性（HA） リンクとして使用する場合、高可用性（HA） 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、セカンダリユニットに複製されることは想定できません。これは、複製には高可用性（*HA*） リンク自体が必要であるためです。
- 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ユニットから複製されます。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。
- 高可用性（HA） の EtherChannel インターフェイスをモニターできます。アクティブなメンバー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、デバイスレベルの高可用性（HA）をモニタしているときには、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、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インターフェイスを高可用性（HA）またはステートリンクに対して使用する場合、パケットが順不同にならないように、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。高可用性（HA）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、高可用性（HA） を一時的に無効にする必要があります。これにより、その期間中は 高可用性（HA） が発生することはありません。

モデルのサポート

- 次のモデルでは、Firewall Device Manager で EtherChannel を追加できます。
  - Firepower 1000

- Firepower 2100
- ISA 3000

Firepower 4100/9300 は EtherChannel をサポートしますが、シャーシの FXOS で EtherChannel のすべてのハードウェア構成を実行する必要があります。Firepower 4100/9300 EtherChannel は、Firewall Device Manager インターフェイスページに単一の物理インターフェイスとともに表示されます。また、ASA 5500-X シリーズなどの他のモデルでは、Firewall Device Manager で EtherChannel を設定できません。

- EtherChannel で Firepower 1010 のスイッチポートまたは VLAN インターフェイスを使用することはできません。

EtherChannel の一般的なガイドライン

- モデルで利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 グループは、最大 8 個のアクティブ インターフェイスを設定できます。
- 最初のメンバーインターフェイスを追加すると、すべてのメンバーインターフェイスに必要なハードウェアプロパティが設定されます。
  - メンバーインターフェイスのメディアタイプは RJ-45 または SFP のいずれかです。異なるタイプ（銅と光ファイバ）の SFP を混在させることができます。RJ-45 インターフェイスと SFP インターフェイスを混在させることはできません。
  - すべてのインターフェイスが同じ速度とデュプレックスに設定されている必要があります。
  - 最初のインターフェイスで速度キャパシティを設定しますが、これは後で変更できません。追加のインターフェイスはすべて同じ速度のキャパシティにする必要があります。たとえば、最初のインターフェイスの速度キャパシティが 10MB/100MB/1GB の場合は、他の 10MB/100MB/1GB インターフェイスを追加する必要があります。EtherChannel（およびそのメンバーインターフェイス）をこれらの速度のいずれかに設定できます。容量の小さいインターフェイスを削除しても、後で 1/10GB インターフェイスを EtherChannel に追加することはできません。容量の大きいインターフェイスで速度を低く設定することによってインターフェイスの容量（1 GB インターフェイスと 10 GB インターフェイスなど）を混在させることはできません。
- 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 デバイスは、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 タギングを有効にすると、FTD デバイスはタグ付きの 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、必ず無効化してください。
- LACP レートはモデルによって異なります。レート（通常または高速）を設定すると、デバイスは接続中のスイッチにそのレートを要求します。デバイスの方も接続中のスイッチ

によって要求されたレートで送信します。両側で同じレートを設定することを推奨します。

- Firepower 4100/9300：LACP レートは、FXOS ではデフォルトで高速に設定されていますが、通常（低速とも呼ばれる）に設定することもできます。
- 他のすべてのモデル：LACP レートが通常（低速とも呼ばれる）に設定されており、変更できません。つまり、デバイスは接続中のスイッチに常に低速レートを要求します。スイッチのレートを低速に設定して、両側が同じレートでLACPメッセージを送信するように設定することを推奨します。

- 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、プライマリ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、メンバー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 の追加

EtherChannel を追加して、メンバーインターフェイスを割り当てます。

（注） 次のモデルでは、Firewall Device Manager で EtherChannel を追加できます。

- Firepower 1000
- Firepower 2100
- ISA 3000

EtherChannel でスイッチポートまたは VLAN インターフェイスを使用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 4100/9300の Etherchannel は、単一の物理インターフェイスとともに Firewall Device Manager の [Interfaces] ページに表示されます。また、ASA 5500-X シリーズなどの他のモデルでは、Firewall Device Manager で EtherChannel を設定できません。

始める前に

- 最初のメンバーインターフェイスを追加すると、すべてのメンバーインターフェイスに必要なハードウェアプロパティが設定されます。メンバーインターフェイスの要件の詳細に

ついては、EtherChannel インターフェイスのガイドライン （22 ページ）を参照してください。

- メンバーインターフェイスに名前を付けることはできません。

注意 コンフィギュレーション内で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。

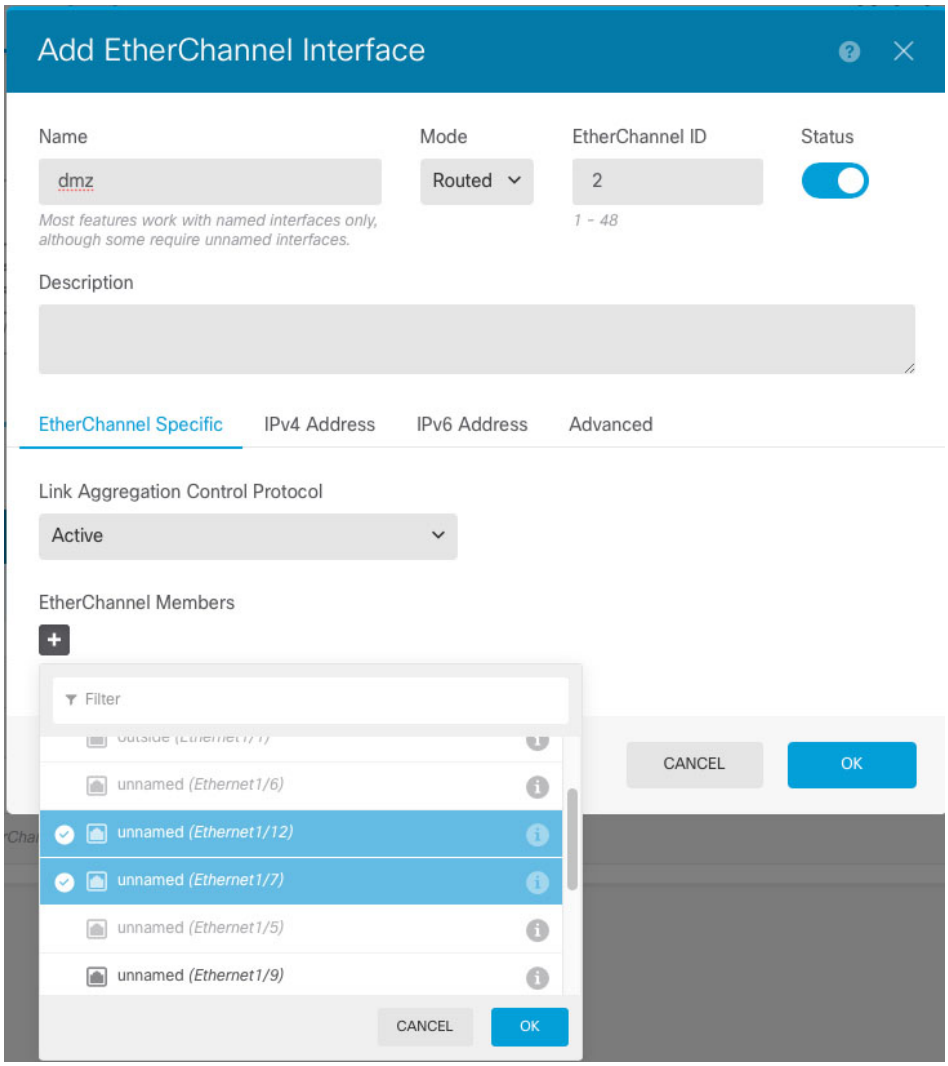
手順

ステップ 1 [デバイス（Device）] をクリックし、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックし、[EtherChannel（EtherChannels）] をクリックします。

[EtherChannel] リストには、既存の EtherChannel、それらの名前、アドレス、および状態が表示されます。各 EtherChannel のメンバーインターフェイスを表示するには、開/閉矢印をクリックします。メンバーインターフェイスは [インターフェイス（Interfaces）] ページにも個別に表示されます。

ステップ 2 [EtherChannelの作成（Create EtherChannel）] をクリックするか（現在の EtherChannel がない場合）、またはプラス アイコン（+）をクリックして [EtherChannel] をクリックし、新しい EtherChannel を作成します。

ステップ 3 次を設定します。



a) [インターフェイス名（Interface Name）] を設定します。

EtherChannel の名前を 48 文字以内で設定します。英字は小文字にする必要があります。例、[inside] または [outside]。

（注）
名前を変更すると、その変更は古い名前を使用しているすべての場所（セキュリティゾーン、syslog サーバ オブジェクト、DHCP サーバの定義を含む）に自動的に反映されます。ただし、通常、ポリシーや設定に名前のないインターフェイスは使用できないため、最初に古い名前を使用しているすべての設定を削除しないと、その名前は削除できません。

b) [モード（Mode）] を設定します。

- [ルーテッド（Routed）]：ルーテッド モード インターフェイスでは、トラフィックはフローの維持、IP 層と TCP 層の両方でのフロー状態のトラッキング、IP の最適化、TCP の正規化、ファイアウォール ポリシーなど、すべてのファイアウォール機能の管

理下に置かれます。トラフィックがインターフェイスを経由するようにする場合は、このモードを使用します。これが通常のインターフェイス モードです。

- [パッシブ（Passive）]：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中のトラフィック フローをモニタします。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。このモードを選択する場合、残りの手順は実行しないでください。代わりに、パッシブ モードでの物理インターフェイスの設定 （54 ページ）を参照してください。

c) [EtherChannel ID] を 1 ～ 48（1 ～ 8（Firepower 1010））の範囲で設定します。

d) [ステータス（Status）] スライダを [有効（enabled）] 設定（  ）に設定します。

e) （任意）[説明（Description）] を設定します。

説明は 200 文字以内で、改行を入れずに 1 行で入力します。

f) [EtherChannelモード（EtherChannel Mode）] を指定します。

- [アクティブ（Active）]：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。
- [オン（On）]：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。

g) [EtherChannel メンバー（EtherChannel Members）] を追加します。

EtherChannel には、最大 8 つの（無名）インターフェイスを追加できます。

- インターフェイスの追加：プラスアイコン（+）をクリックし、1 つ以上のインターフェイスをクリックし、[OK] をクリックします。
- インターフェイスの削除：対象にカーソルを合わせ、右側に表示される [x] をクリックします。

ステップ 4 [IPv4アドレス（IPv4 Address）] タブをクリックして、IPv4 アドレスを設定します。

[タイプ（Type）] フィールドから次のいずれかのオプションを選択します。

- [DHCP]：ネットワーク上の DHCP サーバからアドレスを取得する場合は、このオプションを選択します。高可用性を設定する場合、このオプションは使用できません。必要に応じて、次のオプションを変更します。

- [ルートメトリック（Route Metric）]：DHCP サーバからデフォルト ルートを取得する場合、学習済みルートまでのアドミニストレーティブ ディスタンスは 1 ~ 255 の間です。デフォルトは 1 です。
- [デフォルトルートを取得（Obtain Default Route）]：デフォルト ルートを DHCP サーバから取得するかどうかを指定します。通常は、デフォルトのこのオプションを選択します。

- [スタティック（Static）]：変更されないアドレスを割り当てる場合は、このオプションを選択します。インターフェイスに接続されたネットワークに対するインターフェイスの IP アドレスとサブネット マスクを入力します。たとえば、10.100.10.0/24 ネットワークを接続する場合は、「10.100.10.1/24」と入力します。このアドレスがネットワーク上ですでに使用されていないことを確認します。

  高可用性を設定し、このインターフェイスの HA をモニタしている場合は、同じサブネット上のスタンバイ IP アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。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。

  （注）
  インターフェイスに対して設定されている DHCP サーバがある場合は、その設定が表示されます。DHCP アドレス プールを編集または削除できます。インターフェイスの IP アドレスを別のサブネットに変更する場合は、インターフェイスの変更を保存する前に、DHCP サーバを削除するか、新しいサブネット上にアドレス プールを構成する必要があります。DHCP サーバの設定を参照してください。

- [PPPoE]：イーサネット経由のポイントツーポイント プロトコル（PPPoE）を使用してアドレスを取得する必要がある場合は、このオプションを選択します。インターフェイスが DSL モデム、ケーブルモデム、または ISP への他の接続に接続されており、ISP が PPPoE を使用して IP アドレスを提供している場合は、PPPoE が必要になる場合があります。高可用性を設定する場合、このオプションは使用できません。次の値を設定します。
  - [グループ名（Group Name）]：この接続を表すために選択した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（PPPoE Password）]：ISP によって提供されたパスワードを指定します。
  - [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の学習済みルートメトリック（PPPoE Learned Route Metric）]：アドミニストレーティブディスタンスを既知の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。
- [PPPoEからデフォルトルートを取得（Obtain Default Route from PPPoE）]：PPPoE サーバからのデフォルトルートの取得を有効にするには、このチェックボックスをオンにします。
- [IPアドレスタイプ（IP Address Type）]：PPPoE サーバから IP アドレスを取得するには、[動的（Dynamic）] を選択します。ISP から静的 IP アドレスが割り当てられている場合は、[静的（Static）] を選択することもできます。

ステップ 5 （オプション）[IPv6アドレス（IPv6 Address）] タブをクリックして、IPv6 アドレスを設定します。

- [状態（State）]：グローバル アドレスを設定しない場合に IPv6 処理を有効にしてリンクローカルアドレスを自動的に設定するには、[有効（Enabled）] を選択します。リンクローカル アドレスはインターフェイスの MAC アドレス（*Modified* EUI-64 形式）に基づいて生成されます。

  （注）
  IPv6 を無効にしても、明示的な IPv6 アドレスを指定して設定されているインターフェイス、または自動設定が有効になっているインターフェイスの IPv6 処理は無効になりません。

- [アドレスの自動設定（Address Auto Configuration）]：アドレスを自動的に設定するには、このオプションを選択します。IPv6 ステートレス自動設定では、デバイスが存在するリンクで使用する IPv6 グローバル プレフィックスのアドバタイズメントなどの、IPv6 サービスを提供するようにルータが設定されている場合に限り、グローバルな IPv6 アドレスが生成されます。IPv6 ルーティング サービスがリンクで使用できない場合、リンクローカル IPv6 アドレスのみが取得され、そのデバイスが属するネットワーク リンクの外部にはアクセスできません。リンクローカル アドレスは Modified EUI-64 インターフェイス ID に基づいています。

  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。メッセージを抑制して、RFC に準拠するためには、[RA を抑制（Suppress RA）] を選択します。

- [スタティックアドレスとプレフィックス（Static Address/Prefix）]：ステートレス自動設定を使用しない場合、完全なスタティック グローバル IPv6 アドレスとネットワーク プレフィックスを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。IPv6 アドレッシングの詳細については、IPv6 アドレス指定 （5 ページ）を参照してください。

アドレスをリンクローカル専用として使用する場合は、[リンクローカル（Link - Local）] オプションを選択します。リンクローカル アドレスでは、ローカル ネットワークの外部にはアクセスできません。リンクローカル アドレスはブリッジ グループ インターフェイスには設定できません。

（注）
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。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。

- [スタンバイ IP アドレス（Standby IP Address）]：高可用性を設定し、このインターフェイスの HA をモニタリングしている場合は、同じサブネット上にスタンバイ IPv6 アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。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。
- [RA を抑制（Suppress RA）]：ルータ アドバタイズメントを抑制するかどうかを指定します。ネイバー デバイスがデフォルトのルータ アドレスをダイナミックに把握できるように、FTD はルータ アドバタイズメントに参加できます。デフォルトでは、ルータ アドバタイズメント メッセージ（ICMPv6 Type 134）は、設定済みの各 IPv6 インターフェイスに定期的に送信されます。

  ルータ アドバタイズメントもルータ要請メッセージ（ICMPv6 Type 133）に応答して送信されます。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できます。

  FTD 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抑制できます。

ステップ 6 [詳細（Advanced）] をクリックし、速度を設定して、メンバーインターフェイスの速度を設定します。

その他の高度なオプションを設定することもできます。詳細オプションの設定 （58 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。

次のタスク

- EtherChannel を適切なセキュリティゾーンに追加します。セキュリティ ゾーンの設定を参照してください。

VLAN インターフェイスとスイッチポートの構成

内部スイッチを搭載したモデルの場合、通常のファイアウォールインターフェイスとしてまたはレイヤ2ハードウェアスイッチポートとして実行するように各インターフェイスを構成できます。ここでは、スイッチモードの有効化と無効化、VLANインターフェイスの作成、VLANへのスイッチポートの割り当てなど、スイッチポート設定を開始するためのタスクについて説明します。また、この項では、サポート対象のインターフェイスで Power on Ethernet（PoE）をカスタマイズする方法についても説明します。

スイッチポートおよびインターフェイスについて

ポートとインターフェイス

物理インターフェイスごとに、その動作をファイアウォールインターフェイスまたはスイッチポートとして設定できます。物理インターフェイスとポートタイプ、およびスイッチポートを割り当てる論理 VLAN インターフェイスについては、次の情報を参照してください。

- 物理ファイアウォールインターフェイス：ルーテッドモードでは、これらのインターフェイスは、設定済みのセキュリティポリシーを使用してファイアウォールと VPN サービスを適用することによって、レイヤ3のネットワーク間でトラフィックを転送します。ルーテッドモードでは、一部のインターフェイスでブリッジグループメンバーとして、その他のインターフェイスでレイヤ3インターフェイスとして、統合ルーティングおよびブリッジングを使用することもできます。デフォルトでは、イーサネット 1/1 インターフェイスはファイアウォールインターフェイスとして設定されます。また、これらのインターフェイスを IPS 専用（パッシブインターフェイス）に設定することもできます。

- 物理スイッチポート：スイッチポートは、ハードウェアのスイッチ機能を使用して、レイヤ 2 でトラフィックを転送します。同じ VLAN 上のスイッチポートは、ハードウェアスイッチングを使用して相互に通信できます。トラフィックには、FTD セキュリティポリシーは適用されません。アクセスポートはタグなしトラフィックのみを受け入れ、単一のVLANに割り当てることができます。トランクポートはタグなしおよびタグ付きトラフィックを受け入れ、複数の VLAN に属することができます。デフォルトでは、イーサネット 1/2 以上は VLAN 1 のアクセススイッチポートとして構成されています。Management インターフェイスをスイッチポートとして設定することはできません。

- 論理 VLAN インターフェイス：これらのインターフェイスは物理ファイアウォール インターフェイスと同じように動作しますが、サブインターフェイス、IPS 専用インターフェイス（インラインセットおよびパッシブインターフェイス）、または EtherChannel インターフェイスを作成できないという例外があります。スイッチポートが別のネットワークと通信する必要がある場合、FTD デバイスは VLAN インターフェイスにセキュリティポリシーを適用し、別の論理VLANインターフェイスまたはファイアウォールインターフェイスにルーティングします。ブリッジグループメンバーとして VLAN インターフェイスで統合ルーティングおよびブリッジングを使用することもできます。同じ VLAN 上のスイッチポート間のトラフィックにFTDセキュリティポリシーは適用されませんが、ブリッジグループ内の VLAN 間のトラフィックにはセキュリティポリシーが適用されるため、

ブリッジグループとスイッチポートを階層化して特定のセグメント間にセキュリティポリシーを適用できます。

Power Over Ethernet

PoEは、IEEE 802.3af（PoE）および802.3at（PoE+）を使用して、イーサネット1/7およびイーサネット1/8でポートあたり最大30ワットまで供給できます。

PoE +では、Link Layer Discovery Protocol（LLDP）を使用して、電力レベルをネゴシエートします。電力は必要なときのみ供給されます。

インターフェイスをシャットダウンすると、デバイスへの給電が無効になります。

スイッチポートの前提条件

モデルのサポート

- Firepower 1010

スイッチポートのガイドライン

高可用性（HA）

- 高可用性（HA）を使用する場合は、スイッチポート機能を使用しないでください。スイッチポートはハードウェアで動作するため、アクティブユニットとスタンバイユニットの両方でトラフィックを通過させ続けます。高可用性（HA）は、トラフィックがスタンバイユニットを通過するのを防ぐように設計されていますが、この機能はスイッチポートには拡張されていません。通常の高可用性（HA）のネットワーク設定では、両方のユニットのアクティブなスイッチ ポートがネットワーク ループにつながります。スイッチング機能には外部スイッチを使用することをお勧めします。VLANインターフェイスはフェールオーバーによってモニターできますが、スイッチポートはモニターできません。理論的には、1つのスイッチ ポートをVLANに配置して、高可用性（HA）を正常に使用することができますが、代わりに物理ファイアウォールインターフェイスを使用する設定の方が簡単です。
- ファイアウォールインターフェイスはフェールオーバーリンクとしてのみ使用できます。

論理VLANインターフェイス（SVI）

- また、ファイアウォール インターフェイスでVLANサブインターフェイスを使用する場合、論理VLANインターフェイスと同じVLAN IDは使用できません。
- MACアドレス：
  - すべてのVLANインターフェイスが1つのMACアドレスを共有します。接続スイッチがどれもこのシナリオをサポートできるようにします。接続スイッチに固有のMAC

アドレスが必要な場合、手動で MAC アドレスを割り当てることができます。詳細オプションの設定 （58 ページ） を参照してください。

ブリッジ グループ

同じブリッジ グループ内に論理 VLAN インターフェイスと物理ファイアウォール インターフェイスを混在させることはできません。

VLAN インターフェイスおよびスイッチポートでサポートされていない機能

VLAN インターフェイスおよびスイッチポートは、次の機能をサポートしていません。

- ダイナミック ルーティング
- マルチキャスト ルーティング
- 等コストマルチパス（ECMP）ルーティング
- パッシブインターフェイス
- EtherChannel：スイッチのポートを EtherChannel の一部にはできません。PoE も、EtherChannel のポートではサポートされません。
- フェールオーバーおよびステートリンク

その他の注意事項と制約事項

- 最大 60 の名前付きインターフェイスを構成できます。
- Management インターフェイスをスイッチポートとして設定することはできません。

デフォルト設定

- イーサネット 1/1 はファイアウォール インターフェイスです。
- イーサネット 1/2 ～ 1/8 が、VLAN 1 に割り当てられたスイッチポートです。
- デフォルトの速度とデュプレックス：デフォルトでは、速度とデュプレックスは自動ネゴシエーションに設定されます。

VLAN インターフェイスの設定

ここでは、関連付けられたスイッチ ポートで使用するための VLAN インターフェイスの設定方法について説明します。最初に、スイッチポートに割り当てる VLAN ごとに VLAN インターフェイスを設定する必要があります。

（注） 特定の VLAN 上でのスイッチポート間のスイッチングのみを有効にし、VLAN と他の VLAN またはファイアウォール インターフェイス間のルーティングを望まない場合は、VLAN インターフェイス名を空のままにします。この場合、IP アドレスを設定する必要もありません。IP 設定は無視されます。

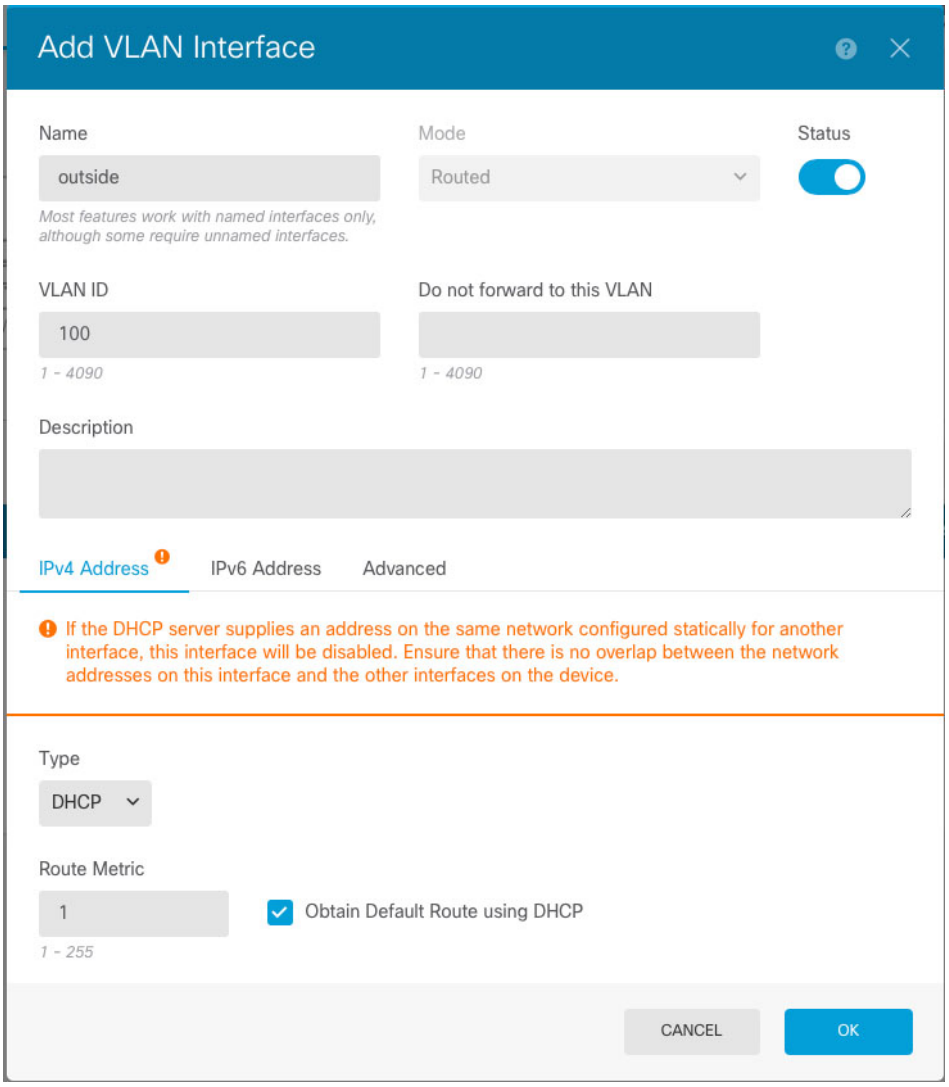
手順

ステップ 1 [デバイス（Device）] をクリックし、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックしてから、[VLAN（VLANs）] をクリックします。

VLAN リストには、既存の VLAN インターフェイスが表示されます。各 VLAN に関連付けられているスイッチポートを表示するには、開/閉矢印をクリックします。また、スイッチポートは [インターフェイス（Interfaces）] ページでも個別に表示されます。

ステップ 2 [VLANインターフェイスの作成（Create VLAN Interface）]（現在の VLAN がない場合）またはプラス アイコン（+）をクリックして、新しい VLAN インターフェイスを作成します。

ステップ 3 次を設定します。



a) [インターフェイス名（Interface Name）] を設定します。

VLAN の名前を 48 文字以内で設定します。英字は小文字にする必要があります。例、[inside] または [outside]。

VLANと他のVLANまたはファイアウォールインターフェイス間でルーティングしない場合は、VLANインターフェイス名を空白のままにします。

（注）
名前を変更すると、その変更は古い名前を使用しているすべての場所（セキュリティゾーン、syslog サーバ オブジェクト、DHCP サーバの定義を含む）に自動的に反映されます。ただし、通常、ポリシーや設定に名前のないインターフェイスは使用できないため、最初に古い名前を使用しているすべての設定を削除しないと、その名前は削除できません。

b) [モード（Mode）] は [ルーテッド（Routed）] のままにします。

後でこの VLAN インターフェイスをブリッジグループに追加すると、モードは自動的に **BridgeGroupMember** に変更されます。ブリッジグループのメンバーインターフェイスには、IP アドレスを設定できません。

c) [ステータス（Status）] スライダを [有効（enabled）] 設定（  ）に設定します。

d) [VLAN ID] を 1 ～ 4070 の間で設定します。

インターフェイスを保存した後、VLAN ID を変更することはできません。ここでの VLAN ID は、使用される VLAN タグと設定内のインターフェイス ID の両方です。

e) （任意）[このVLANに転送しない（Do not forward to this VLAN）] フィールドに、この VLAN インターフェイスがトラフィックを開始できない VLAN ID を入力します。

たとえば、1 つの VLAN をインターネット アクセスの外部に、もう 1 つを内部ビジネス ネットワーク内に、そして 3 つ目をホーム ネットワークにそれぞれ割り当てます。ホーム ネットワークはビジネスネットワークにアクセスする必要がないので、ホーム VLAN で [Block Traffic From this Interface to] オプションを使用できます。ビジネスネットワークはホームネットワークにアクセスできますが、その反対はできません。

f) （任意）[説明（Description）] を設定します。

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 4 [IPv4アドレス（IPv4 Address）] タブをクリックして、IPv4 アドレスを設定します。

[タイプ（Type）] フィールドから次のいずれかのオプションを選択します。

- [DHCP]：ネットワーク上の DHCP サーバからアドレスを取得する場合は、このオプションを選択します。高可用性を設定する場合、このオプションは使用できません。必要に応じて、次のオプションを変更します。
  - [ルートメトリック（Route Metric）]：DHCP サーバからデフォルト ルートを取得する場合、学習済みルートまでのアドミニストレーティブ ディスタンスは 1 ~ 255 の間です。デフォルトは 1 です。
  - [デフォルトルートを取得（Obtain Default Route）]：デフォルト ルートを DHCP サーバから取得するかどうかを指定します。通常は、デフォルトのこのオプションを選択します。
- [スタティック（Static）]：変更されないアドレスを割り当てる場合は、このオプションを選択します。インターフェイスに接続されたネットワークに対するインターフェイスの IP アドレスとサブネット マスクを入力します。たとえば、10.100.10.0/24 ネットワークを接続する場合は、「10.100.10.1/24」と入力します。このアドレスがネットワーク上ですでに使用されていないことを確認します。

  高可用性を設定し、このインターフェイスの HA をモニタしている場合は、同じサブネット上のスタンバイ IP アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。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。

（注）
インターフェイスに対して設定されているDHCPサーバがある場合は、その設定が表示されます。DHCP アドレス プールを編集または削除できます。インターフェイスの IP アドレスを別のサブネットに変更する場合は、インターフェイスの変更を保存する前に、DHCP サーバを削除するか、新しいサブネット上にアドレス プールを構成する必要があります。DHCP サーバの設定を参照してください。

- [PPPoE]：イーサネット経由のポイントツーポイント プロトコル（PPPoE）を使用してアドレスを取得する必要がある場合は、このオプションを選択します。インターフェイスがDSL モデム、ケーブルモデム、または ISP への他の接続に接続されており、ISP が PPPoE を使用して IP アドレスを提供している場合は、PPPoE が必要になる場合があります。高可用性を設定する場合、このオプションは使用できません。次の値を設定します。
  - [グループ名（Group Name）]：この接続を表すために選択した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（PPPoE Password）]：ISP によって提供されたパスワードを指定します。
  - [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の学習済みルートメトリック（PPPoE Learned Route Metric）]：アドミニストレーティブ ディスタンスを既知の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。
  - [PPPoEからデフォルトルートを取得（Obtain Default Route from PPPoE）]：PPPoE サーバからのデフォルトルートの取得を有効にするには、このチェックボックスをオンにします。
  - [IPアドレスタイプ（IP Address Type）]：PPPoE サーバから IP アドレスを取得するには、[動的（Dynamic）] を選択します。ISP から静的 IP アドレスが割り当てられている場合は、[静的（Static）] を選択することもできます。

ステップ 5 （オプション）[IPv6アドレス（IPv6 Address）] タブをクリックして、IPv6 アドレスを設定します。

- [状態（State）]：グローバル アドレスを設定しない場合に IPv6 処理を有効にしてリンクローカルアドレスを自動的に設定するには、[有効（Enabled）] を選択します。リンクロー

カル アドレスはインターフェイスの MAC アドレス（*Modified* EUI-64 形式）に基づいて生成されます。

（注）
IPv6 を無効にしても、明示的な IPv6 アドレスを指定して設定されているインターフェイス、または自動設定が有効になっているインターフェイスの IPv6 処理は無効になりません。

- [アドレスの自動設定（Address Auto Configuration）]：アドレスを自動的に設定するには、このオプションを選択します。IPv6 ステートレス自動設定では、デバイスが存在するリンクで使用する IPv6 グローバル プレフィックスのアドバタイズメントなどの、IPv6 サービスを提供するようにルータが設定されている場合に限り、グローバルな IPv6 アドレスが生成されます。IPv6 ルーティング サービスがリンクで使用できない場合、リンクローカル IPv6 アドレスのみが取得され、そのデバイスが属するネットワーク リンクの外部にはアクセスできません。リンクローカル アドレスは Modified EUI-64 インターフェイス ID に基づいています。

  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。メッセージを抑制して、RFC に準拠するためには、[RA を抑制（Suppress RA）] を選択します。

- [スタティックアドレスとプレフィックス（Static Address/Prefix）]：ステートレス自動設定を使用しない場合、完全なスタティック グローバル IPv6 アドレスとネットワーク プレフィックスを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。IPv6 アドレッシングの詳細については、IPv6 アドレス指定 （5 ページ）を参照してください。

  アドレスをリンクローカル専用として使用する場合は、[リンクローカル（Link - Local）] オプションを選択します。リンクローカル アドレスでは、ローカル ネットワークの外部にはアクセスできません。リンクローカル アドレスはブリッジ グループ インターフェイスには設定できません。

  （注）
  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。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。

- [スタンバイ IP アドレス（Standby IP Address）]：高可用性を設定し、このインターフェイスの HA をモニタリングしている場合は、同じサブネット上にスタンバイ IPv6 アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。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。

- [RAを抑制（Suppress RA）]：ルータ アドバタイズメントを抑制するかどうかを指定します。ネイバー デバイスがデフォルトのルータ アドレスをダイナミックに把握できるように、FTDはルータ アドバタイズメントに参加できます。デフォルトでは、ルータ アドバタイズメント メッセージ（ICMPv6 Type 134）は、設定済みの各 IPv6 インターフェイスに定期的に送信されます。

  ルータ アドバタイズメントもルータ要請メッセージ（ICMPv6 Type 133）に応答して送信されます。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できます。

  FTD 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抑制できます。

ステップ 6 （任意）詳細オプションの設定 （58 ページ）。

詳細設定には、ほとんどのネットワークに適しているデフォルト設定があります。デフォルト設定はネットワークの問題を解決する場合のみ編集します。

ステップ 7 [OK] をクリックします。

次のタスク

- VLAN を適切なセキュリティゾーンに追加します。セキュリティ ゾーンの設定 を参照してください。

スイッチ ポートのアクセス ポートとしての設定

1 つの VLAN にスイッチ ポートを割り当てるには、アクセス ポートとして設定します。Firepower 1010 および Cisco Secure Firewall 1210 では、イーサネット 1/2 ～ 1/8 スイッチポートがデフォルトで有効になり、VLAN 1。

（注） Firepower 1010 およびでは、ネットワーク内のループ検出のためのスパニングツリープロトコルはサポートされません。したがって、Firewall Threat Defense デバイスとのすべての接続は、ネットワークループ内で終わらないようにする必要があります。

始める前に

アクセスポートを割り当てる VLAN ID に VLAN インターフェイスを追加します。アクセスポートは、タグなしのトラフィックのみを受け入れます。「VLAN インターフェイスの設定（33 ページ）」を参照してください。

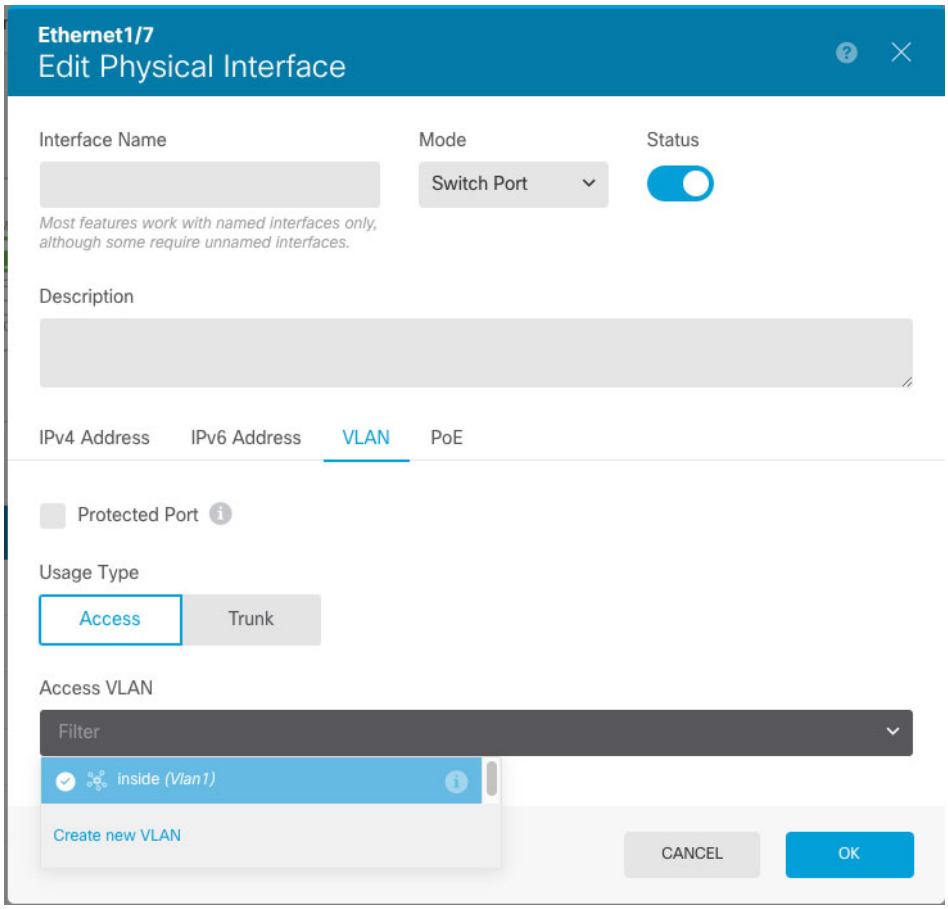
手順

ステップ 1 [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックします。

[インターフェイス（Interfaces）] タブがデフォルトで選択されます。インターフェイスリストに、物理インターフェイスとそれぞれの名前、アドレス、状態が表示されます。

ステップ 2 編集する物理インターフェイスの [編集（edit）] アイコン（）をクリックします。

ステップ 3 次の設定を行います。



a) スイッチポートの [インターフェイス名（Interface Name）] は設定しないでください。関連付けられている VLAN インターフェイスのみが名前付きインターフェイスです。

b) [モード（Mode）] を [スイッチポート（Switch Port）] に設定します。

c) [ステータス（Status）] スライダを [有効（enabled）] 設定（）に設定します。

d) （任意）[説明（Description）] を設定します。

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 4 [VLAN] をクリックして、次のように設定します。

a) （任意） このスイッチポートを保護対象として設定するには、[保護ポート（Protected Port）] チェックボックスをオンにします。これにより、スイッチポートが同じ VLAN 上の他の保護されたスイッチポートと通信するのを防ぐことができます。

スイッチ ポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチ ポートが相互に通信しないようにします。たとえば、3 つの Web サーバーをホストする DMZ がある場合、各スイッチポートにこのオプションを適用すると、Web サーバーを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバーすべてと通信でき、その逆も可能ですが、Web サーバーは相互に通信できません。

b) [使用タイプ（Usage Type）] で、[アクセス（Access）] をクリックします。

c) [アクセスVLAN（Access VLAN）] の場合は、下矢印をクリックして既存の VLAN インターフェイスのいずれかを選択します。

新しい VLAN インターフェイスを追加するには、[新しいVLANの作成（Create new VLAN）] をクリックします。VLAN インターフェイスの設定 （33 ページ）を参照してください。

ステップ 5 [OK] をクリックします。

スイッチ ポートのトランク ポートとしての設定

この手順では、802.1Q タグ付けを使用して複数の VLAN を伝送するトランク ポートの作成方法について説明します。トランクポートは、タグなしトラフィックとタグ付きトラフィックを受け入れます。許可された VLAN のトラフィックは、トランクポートを変更せずに通過します。

トランクは、タグなしトラフィックを受信すると、そのトラフィックをネイティブ VLAN ID にタグ付けして、デバイスが正しいスイッチポートにトラフィックを転送したり、別のファイアウォールインターフェイスにルーティングしたりできるようにします。デバイスは、トランクポートからネイティブ VLAN ID トラフィックを送信する際に VLAN タグを削除します。タグなしトラフィックが同じ VLAN にタグ付けされるように、他のスイッチのトランク ポートに同じネイティブ VLAN を設定してください。

始める前に

トランクポートを割り当てる VLAN ID ごとに VLAN インターフェイスを追加します。「VLAN インターフェイスの設定 （33 ページ）」を参照してください。

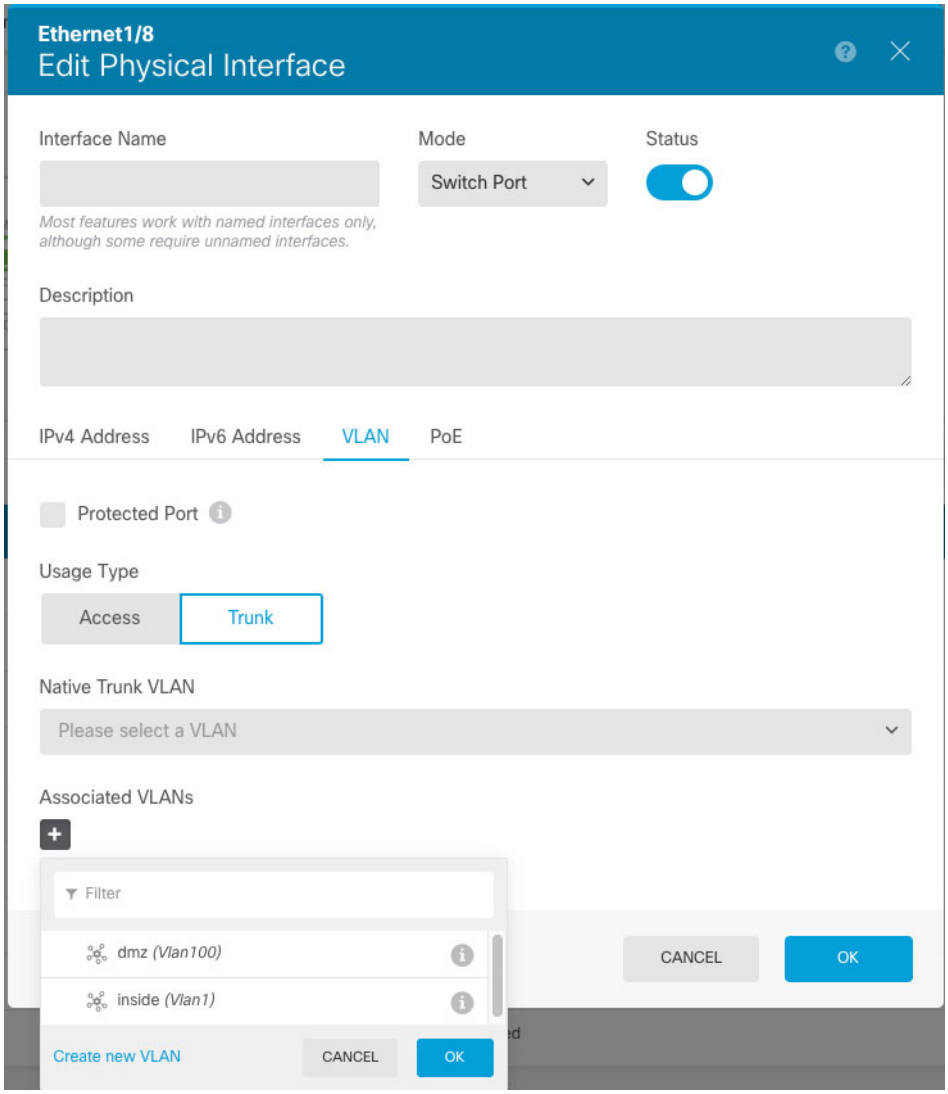
手順

ステップ 1 [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックします。

[インターフェイス（Interfaces）] タブがデフォルトで選択されます。インターフェイスリストに、物理インターフェイスとそれぞれの名前、アドレス、状態が表示されます。

ステップ 2 編集する物理インターフェイスの [編集（edit）] アイコン（）をクリックします。

ステップ 3 次の設定を行います。



a) スイッチポートの [インターフェイス名（Interface Name）] は設定しないでください。関連付けられている VLAN インターフェイスのみが名前付きインターフェイスです。

b) [モード（Mode）] を [スイッチポート（Switch Port）] に設定します。

c) [ステータス（Status）] スライダを [有効（enabled）] 設定（）に設定します。

d) （任意） [説明（Description）] を設定します。

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 4 [VLAN] をクリックして、次のように設定します。

a) （任意） このスイッチポートを保護対象として設定するには、[保護ポート（Protected Port）] チェックボックスをオンにします。これにより、スイッチポートが同じ VLAN 上の他の保護されたスイッチポートと通信するのを防ぐことができます。

スイッチ ポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチ ポートが相互に通信しないようにします。たとえば、3 つの Web サーバーをホストする DMZ がある場合、各スイッチポートにこのオプションを適用すると、Web サーバーを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバーすべてと通信でき、その逆も可能ですが、Web サーバーは相互に通信できません。

b) [使用タイプ（Usage Type）] で、[トランク（Trunk）] をクリックします。

c) （任意） [ネイティブトランクVLAN（Native Trunk VLAN）] の場合は、下矢印をクリックしてネイティブ VLAN の既存の VLAN インターフェイスのいずれかを選択します。

デフォルトのネイティブ VLAN ID は 1 です。

各ポートのネイティブ VLAN は 1 つのみですが、すべてのポートに同じネイティブ VLAN または異なるネイティブ VLAN を使用できます。

新しいVLANインターフェイスを追加するには、[新しいVLANの作成（Create new VLAN）] をクリックします。「VLAN インターフェイスの設定 （33 ページ）」を参照してください。

d) [関連付けられているVLAN（Associated VLANs）] で、プラス アイコン（  ）をクリックして、1 つまたは複数の既存の VLAN インターフェイスを選択します。

このフィールドにネイティブ VLAN を含めても無視されます。トランク ポートは、ネイティブ VLAN トラフィックをポートから送信するときに、常に VLAN タグを削除します。また、まだネイティブ VLAN タグが付いているトラフィックを受信しません。

新しいVLANインターフェイスを追加するには、[新しいVLANの作成（Create new VLAN）] をクリックします。VLAN インターフェイスの設定 （33 ページ）を参照してください。

ステップ 5 [OK] をクリックします。

Power over Ethernet の設定

Power over Ethernet（PoE）ポートは、IP 電話や無線アクセスポイントなどのデバイスに電力を供給します。PoE はデフォルトでイネーブルです。この手順では、PoE を無効および有効にする方法と、オプションパラメータを設定する方法について説明します。

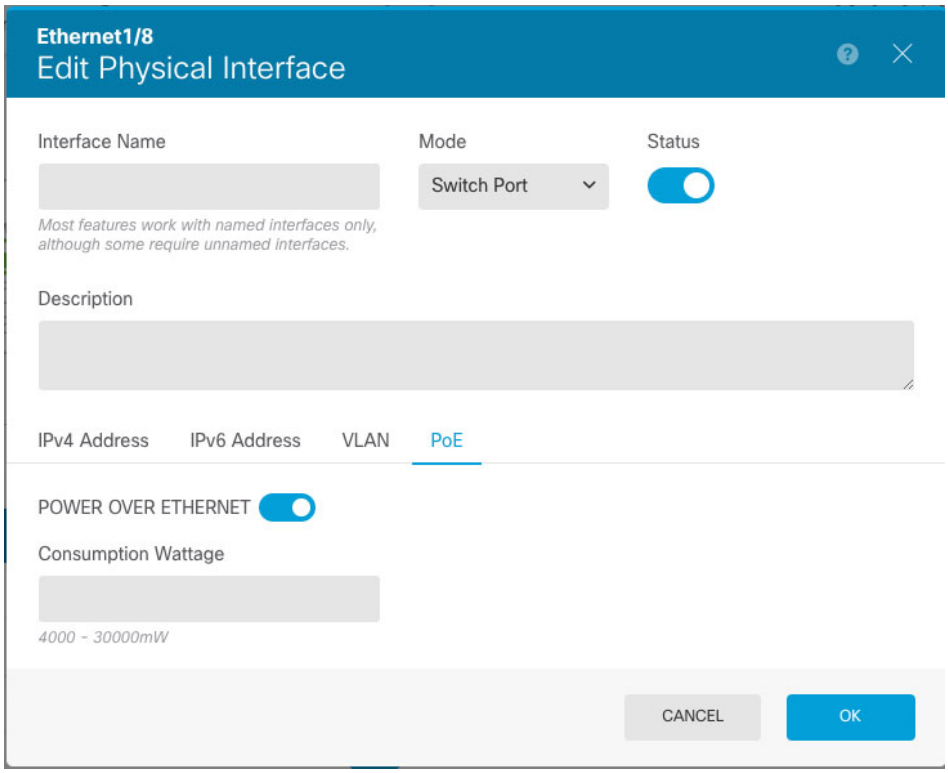
手順

ステップ 1 [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックします。

[インターフェイス（Interfaces）] タブがデフォルトで選択されます。インターフェイスリストに、物理インターフェイスとそれぞれの名前、アドレス、状態が表示されます。

ステップ 2 イーサネット 1/7 または 1/8の編集アイコン（）をクリックします。

ステップ 3 [PoE] をクリックして、次のように設定します。



a) [Power Over Ethernet] を有効にするには、スライダ（）をクリックして有効にします。

PoE はデフォルトでイネーブルです。

b) （任意） 必要なワット数を正確に把握している場合は、[消費ワット数（Consumption Wattage）] を入力します。

消費量を手動で設定するには、ワット数をミリワット単位で指定します。範囲は 4000 から 30000です。ワット数を手動で設定し、LLDP ネゴシエーションを無効にする場合は、このコマンドを使用します。手動割り当ての場合、**show power inline** 出力にクラスが **n/a** と表示されます。これは、クラスが消費電力の決定に使用されないためです。

デフォルトでは、PoE は給電先デバイスのクラスに適したワット数を使用して、給電先デバイスに自動的に電力を供給します。ファイアウォールは LLDP を使用して、さらに適切

なワット数をネゴシエートします。特定クラスのデバイスを接続すると、より多くの電力を使用する必要がある場合に備えて、そのクラスの最大値までプロビジョニングが行われます。たとえば、12.95W を要求するクラス 4 デバイスを追加した場合、そのデバイスが現在その電力すべてを使用していなくても、30W が割り当てられます。一部のデバイスは、電力要件を再ネゴシエートできます。デバイスに必要な電力が割り当てられている電力よりも少ないことがわかっている場合は、代わりに [消費ワット数（Consumption Wattage）] を手動で設定して、他のデバイス用に電力を解放できます。

ステップ 4 [OK] をクリックします。

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、物理インターフェイスを異なる VLAN ID が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。

物理インターフェイスをスイッチのトランク ポートに接続する場合は、サブインターフェイスを作成します。スイッチ トランク ポートで表示できる各 VLAN のサブインターフェイスを作成します。物理インターフェイスをスイッチのアクセス ポートに接続する場合は、サブインターフェイスを作成しても意味がありません。

ガイドラインと制約事項

- 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。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的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付け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にタグの付いていないパケットを通過させる場合には、通常のようにインターフェイスに名前を付けることができます。
- 1010：サブインターフェイスは、スイッチポートおよび VLAN インターフェイスではサポートされていません。
- 必要に応じて詳細設定を変更することはできますが、ブリッジグループ メンバーインターフェイスの IP アドレスを設定することはできません。
- 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。

- Firewall Threat Defense 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と同じ組み込みの MAC アドレスを使用するので、Firepower Threat Defense デバイス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制御を行う場合があります。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、Firepower Threat Defense デバイスで特定のインスタンスでのトラフィックの中断を回避できます。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックします。

[インターフェイス（Interfaces）] タブがデフォルトで選択されます。EtherChannel にサブインターフェイスを追加するには、[EtherChannel] をクリックします。インターフェイスリストに、物理インターフェイスとそれぞれの名前、アドレス、状態が表示されます。

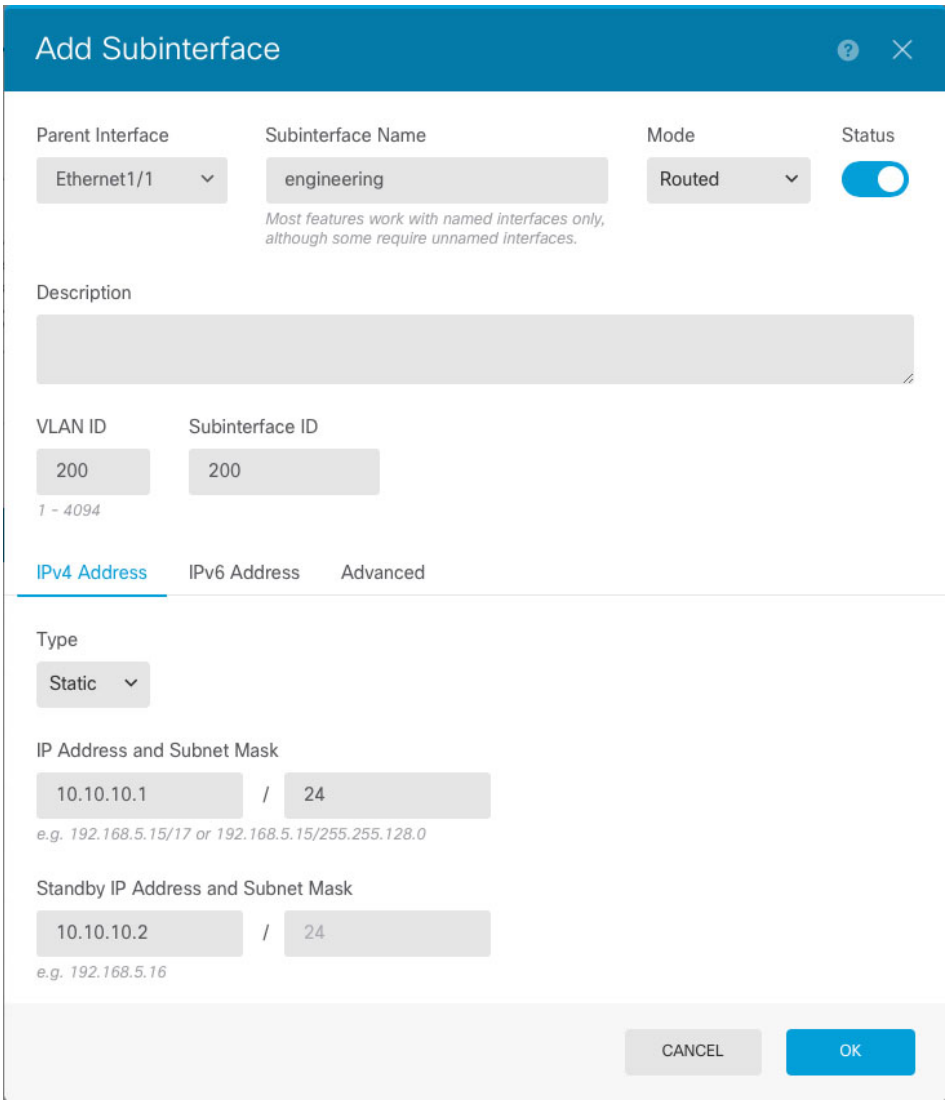
ステップ 2 次のいずれかを実行します。

- [Interfaces] ページで、プラスアイコン（  ）をクリックして、新しいサブインターフェイスを作成します。
- [EtherChannel] ページで、プラスと下矢印のアイコン（  ）をクリックし、[Subinterface] を選択します。
- 編集するサブインターフェイスの編集アイコン（  ）をクリックします。

サブインターフェイスが不要になった場合は、このサブインターフェイスの [削除（delete）] アイコン（  ）をクリックして削除します。

ステップ 3 [ステータス（Status）] スライダを [有効（enabled）] 設定（  ）に設定します。

ステップ 4 親インターフェイス、名前、および説明を設定します。



a) [Parent Interface] を選択します。

親インターフェイスは、サブインターフェイスの追加先となる物理インターフェイスです。いったん作成したサブインターフェイスの親インターフェイスは変更できません。

b) [Subinterface Name]（最大 48 文字）を設定します。

英字は小文字にする必要があります。例、[inside] または [outside]。名前を設定しないと、インターフェイスの残りの設定は無視されます。

（注）
名前を変更すると、その変更は古い名前を使用しているすべての場所（セキュリティゾーン、syslog サーバ オブジェクト、DHCP サーバの定義を含む）に自動的に反映されます。ただし、通常、ポリシーや設定に名前のないインターフェイスは使用できないため、最初に古い名前を使用しているすべての設定を削除しないと、その名前は削除できません。

c) [モード（Mode）] を [ルーテッド（Routed）] に設定します。

後でこのインターフェイスをブリッジグループに追加すると、モードは自動的に「BridgeGroupMember」に変更されます。ブリッジグループのメンバーインターフェイスには IP アドレスを設定できません。

d) （任意） [Description] を設定します。

説明は 200 文字以内で、改行を入れずに 1 行で入力します。

e) [VLAN ID] を設定します。

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する VLAN ID を 1 ～ 4094 の範囲で入力します。

f) [サブインターフェイスID（Subinterface ID）] を設定します。

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。この ID は、インターフェイス ID に追加されます。たとえば、Ethernet1/1.100 のようになります。便宜上 VLAN ID を一致させることもできますが、必須ではありません。いったん作成したサブインターフェイスの ID は変更できません。

ステップ 5 [IPv4アドレス（IPv4 Address）] タブをクリックして、IPv4 アドレスを設定します。

[タイプ（Type）] フィールドから次のいずれかのオプションを選択します。

- [DHCP]：ネットワーク上の DHCP サーバからアドレスを取得する場合は、このオプションを選択します。高可用性を設定する場合、このオプションは使用できません。必要に応じて、次のオプションを変更します。
  - [ルートメトリック（Route Metric）]：DHCP サーバからデフォルト ルートを取得する場合、学習済みルートまでのアドミニストレーティブ ディスタンスは 1 ~ 255 の間です。デフォルトは 1 です。
  - [デフォルトルートを取得（Obtain Default Route）]：デフォルト ルートを DHCP サーバから取得するかどうかを指定します。通常は、デフォルトのこのオプションを選択します。
- [スタティック（Static）]：変更されないアドレスを割り当てる場合は、このオプションを選択します。インターフェイスに接続されたネットワークに対するインターフェイスの IP アドレスとサブネット マスクを入力します。たとえば、10.100.10.0/24 ネットワークを接続する場合は、「10.100.10.1/24」と入力します。このアドレスがネットワーク上ですでに使用されていないことを確認します。

  高可用性を設定し、このインターフェイスの HA をモニタしている場合は、同じサブネット上のスタンバイ IP アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。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。

  （注）
  インターフェイスに対して設定されている DHCP サーバがある場合は、その設定が表示されます。DHCP アドレス プールを編集または削除できます。インターフェイスの IP アドレスを別のサブネットに変更する場合は、インターフェイスの変更を保存する前に、DHCP

サーバを削除するか、新しいサブネット上にアドレス プールを構成する必要があります。DHCP サーバの設定を参照してください。

- [PPPoE]：イーサネット経由のポイントツーポイント プロトコル（PPPoE）を使用してアドレスを取得する必要がある場合は、このオプションを選択します。インターフェイスがDSL モデム、ケーブルモデム、または ISP への他の接続に接続されており、ISP が PPPoE を使用して IP アドレスを提供している場合は、PPPoE が必要になる場合があります。高可用性を設定する場合、このオプションは使用できません。次の値を設定します。
  - [グループ名（Group Name）]：この接続を表すために選択した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（PPPoE Password）]：ISP によって提供されたパスワードを指定します。
  - [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の学習済みルートメトリック（PPPoE Learned Route Metric）]：アドミニストレーティブ ディスタンスを既知の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。
  - [PPPoEからデフォルトルートを取得（Obtain Default Route from PPPoE）]：PPPoE サーバからのデフォルトルートの取得を有効にするには、このチェックボックスをオンにします。
  - [IPアドレスタイプ（IP Address Type）]：PPPoE サーバから IP アドレスを取得するには、[動的（Dynamic）] を選択します。ISP から静的 IP アドレスが割り当てられている場合は、[静的（Static）] を選択することもできます。

ステップ 6 （オプション）[IPv6アドレス（IPv6 Address）] タブをクリックして、IPv6 アドレスを設定します。

- [状態（State）]：グローバル アドレスを設定しない場合に IPv6 処理を有効にしてリンクローカルアドレスを自動的に設定するには、[有効（Enabled）] を選択します。リンクローカル アドレスはインターフェイスの MAC アドレス（*Modified* EUI-64 形式）に基づいて生成されます。

（注）

IPv6 を無効にしても、明示的な IPv6 アドレスを指定して設定されているインターフェイス、または自動設定が有効になっているインターフェイスの IPv6 処理は無効になりません。

- [アドレスの自動設定（Address Auto Configuration）]：アドレスを自動的に設定するには、このオプションを選択します。IPv6 ステートレス自動設定では、デバイスが存在するリンクで使用する IPv6 グローバル プレフィックスのアドバタイズメントなどの、IPv6 サービスを提供するようにルータが設定されている場合に限り、グローバルな IPv6 アドレスが生成されます。IPv6 ルーティング サービスがリンクで使用できない場合、リンクローカル IPv6 アドレスのみが取得され、そのデバイスが属するネットワーク リンクの外部にはアクセスできません。リンクローカル アドレスは Modified EUI-64 インターフェイス ID に基づいています。

  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。メッセージを抑制して、RFC に準拠するためには、[RA を抑制（Suppress RA）] を選択します。

- [スタティックアドレスとプレフィックス（Static Address/Prefix）]：ステートレス自動設定を使用しない場合、完全なスタティック グローバル IPv6 アドレスとネットワーク プレフィックスを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。IPv6 アドレッシングの詳細については、IPv6 アドレス指定 （5 ページ）を参照してください。

  アドレスをリンクローカル専用として使用する場合は、[リンクローカル（Link - Local）] オプションを選択します。リンクローカル アドレスでは、ローカル ネットワークの外部にはアクセスできません。リンクローカル アドレスはブリッジ グループ インターフェイスには設定できません。

  （注）
  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。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。

- [スタンバイ IPアドレス（Standby IP Address）]：高可用性を設定し、このインターフェイスの HA をモニタリングしている場合は、同じサブネット上にスタンバイ IPv6 アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。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。

- [RAを抑制（Suppress RA）]：ルータ アドバタイズメントを抑制するかどうかを指定します。ネイバー デバイスがデフォルトのルータ アドレスをダイナミックに把握できるように、FTDはルータ アドバタイズメントに参加できます。デフォルトでは、ルータ アドバタイズメント メッセージ（ICMPv6 Type 134）は、設定済みの各 IPv6 インターフェイスに定期的に送信されます。

ルータ アドバタイズメントもルータ要請メッセージ（ICMPv6 Type 133）に応答して送信されます。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できます。

FTD 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抑制できます。

ステップ 7 （任意）詳細オプションの設定 （58 ページ）。

詳細設定には、ほとんどのネットワークに適しているデフォルト設定があります。デフォルト設定はネットワークの問題を解決する場合のみ編集します。

ステップ 8 **[OK]** をクリックします。

次のタスク

- サブインターフェイスを適切なセキュリティゾーンに追加します。セキュリティ ゾーンの設定 を参照してください。

パッシブ インターフェイスの設定

パッシブ インターフェイスは、スイッチ SPAN（スイッチド ポート アナライザ）またはミラー ポートを使用してネットワーク全体を流れるトラフィックをモニターします。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。

パッシブ展開で設定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など）を実行できません。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。

パッシブ インターフェイスを使用して、ネットワーク上のトラフィックをモニタし、トラフィックに関する情報を収集します。たとえば、侵入ポリシーを適用して、ネットワークを攻撃する脅威のタイプを特定したり、ユーザーが作成している Web 要求の URL カテゴリを確認できます。さまざまなセキュリティ ポリシーおよびルールを実装して、アクティブに展開されたシステムの動作を確認し、アクセス制御やその他のルールに基づいてトラフィックをドロップできます。

ただし、パッシブ インターフェイスはトラフィックに影響を与えることができないため、多数の設定上の制限が存在します。これらのインターフェイスは、システムがトラフィックをピークすることを可能にするだけです。パッシブ インターフェイスに入るパケットがデバイスを出ることはありません。

ここでは、パッシブ インターフェイスとそれらの設定方法について説明します。

パッシブ インターフェイスを使用する理由

パッシブ インターフェイスの主な目的は、単純なデモンストレーション モードを提供することです。単一の送信元ポートをモニターするようにスイッチをセットアップし、ワークステーションを使用して、パッシブ インターフェイスでモニターしたテスト トラフィックを送信できます。これにより、Firepower Threat Defense システムが接続を評価したり脅威を特定したりする方法を確認できます。システムの実行方法に問題がなければ、その方法をネットワーク内にアクティブに展開して、パッシブ インターフェイスの設定を削除できます。

ただし、次のサービスを提供するために実稼働環境でパッシブインターフェイスを使用することもできます。

- 純粋な IDS 展開：システムをファイアウォールまたは IPS（侵入防御システム）として使用しない場合、IDS（侵入検知システム）としてパッシブに展開できます。この展開方法では、アクセス制御ルールを使用してすべてのトラフィックに侵入ポリシーを適用します。また、システムでスイッチ上の複数の送信元ポートもモニタします。さらに、ダッシュボードを使用してネットワークで見られる脅威をモニターできます。ただし、このモードでは、この脅威を防ぐためにできることはありません。
- 混合展開：アクティブ ルーテッド インターフェイスとパッシブインターフェイスを同じシステム上に混在させることができます。これにより、Firepower Threat Defense デバイスをいくつかのネットワークでファイアウォールとして展開すると同時に、複数のパッシブインターフェイスを他のネットワーク内のトラフィックをモニターするように設定することができます。

パッシブ インターフェイスの制限

パッシブ モード インターフェイスとして定義する物理インターフェイスには次の制限があります。

- パッシブ インターフェイスのサブインターフェイスは設定できません。
- パッシブ インターフェイスをブリッジ グループに含めることはできません。
- パッシブ インターフェイスで IPv4 アドレスまたは IPv6 アドレスを設定することはできません。
- パッシブ インターフェイスに [管理専用（Management Only）] オプションを選択することはできません。
- このインターフェイスはパッシブ モード セキュリティ ゾーンにのみ含めることができます。ルーテッド セキュリティ ゾーンに含めることはできません。
- パッシブ セキュリティ ゾーンをアクセス制御またはアイデンティティ ルールの送信元基準に含めることは可能です。パッシブ ゾーンを宛先基準で使用することはできません。パッシブ ゾーンとルーテッド ゾーンを同じルールに混在させることもできません。
- パッシブ インターフェイスの管理アクセス ルール（HTTPS または SSH）を設定することはできません。

- パッシブ インターフェイスを NAT ルールで使用することはできません。
- パッシブ インターフェイスのスタティック ルートを設定することはできません。パッシブ インターフェイスをルーティング プロトコルの設定で使用することもできません。
- パッシブ インターフェイスで DHCP サーバを設定することはできません。パッシブ インターフェイスを使用して自動設定で DHCP 設定を取得することもできません。
- パッシブ インターフェイスを syslog サーバ設定で使用することはできません。
- パッシブ インターフェイスではどのタイプの VPN も設定することはできません。

ハードウェア FTD パッシブインターフェイスのスイッチの設定

ハードウェア Firepower Threat Defense デバイス上のパッシブインターフェイスは、ネットワークスイッチを正しく設定している場合にのみ機能します。次の手順は、Cisco Nexus 5000 シリーズスイッチに基づいています。別のタイプのスイッチでは、コマンドが異なる可能性があります。

基本的な考え方としては、SPAN（スイッチド ポート アナライザ）またはミラー ポートを設定し、そのポートにパッシブ インターフェイスを接続し、スイッチでモニタリング セッションを設定して、1 つまたは複数の送信元ポートから SPAN またはミラー ポートにトラフィックのコピーを送信します。

手順

ステップ 1 スイッチ上のポートをモニタ（SPAN またはミラー）ポートとして設定します。

```
switch(config)# interface Ethernet1/48
switch(config-if)# switchport monitor
switch(config-if)#
```

ステップ 2 モニタへのポートを特定するモニタリング セッションを定義します。

SPAN またはミラー ポートを宛先ポートとして定義していることを確認します。次の例では、2 つの送信元ポートがモニタされています。

```
switch(config)# monitor session 1
switch(config-monitor)# source interface ethernet 1/7
switch(config-monitor)# source interface ethernet 1/8
switch(config-monitor)# destination interface ethernet 1/48
switch(config-monitor)# no shut
```

ステップ 3 （任意）**show monitor session** コマンドを使用して、設定を確認します。

次の例に、セッション 1 の概要出力を示します。

```
switch# show monitor session 1 brief
```

```
   session 1
---------------
type               : local
state              : up
source intf        :
    rx             : Eth1/7        Eth1/8
    tx             : Eth1/7        Eth1/8
    both           : Eth1/7        Eth1/8
source VSANs       :
destination ports  : Eth1/48

Legend: f = forwarding enabled, l = learning enabled
```

ステップ 4 Firepower Threat Defense パッシブインターフェイスからスイッチ上の宛先ポートにケーブルを物理的に接続します。

物理接続を行う前後に、パッシブ モードでインターフェイスを設定できます。パッシブ モードでの物理インターフェイスの設定 （54 ページ） を参照してください。

FTDv パッシブインターフェイスの VLAN の設定

FTDv デバイスのパッシブインターフェイスは、仮想ネットワーク上で VLAN を正しく設定した場合にのみ機能します。次の手順を実行してください。

- FTDv インターフェイスを、無差別モードで設定した VLAN に接続します。その後、パッシブ モードでの物理インターフェイスの設定 （54 ページ）での説明に従ってインターフェイスを設定します。パッシブ インターフェイスでは、プロミスキャス VLAN 上のすべてのトラフィックのコピーが認識されます。
- 同じ VLAN に、1 つ以上のエンドポイント デバイス（仮想 Windows システムなど）を接続します。VLAN からインターネットへの接続がある場合は、単一のデバイスを使用できます。それ以外の場合は、トラフィックを通過させるために 2 つ以上のデバイスが必要です。URL カテゴリのデータを取得するには、インターネット接続が必要です。

パッシブ モードでの物理インターフェイスの設定

インターフェイスはパッシブ モードで設定できます。パッシブに機能する場合、インターフェイスは（ハードウェア デバイスの）スイッチそのものまたは（Firewall Threat Defense Virtual の）プロミスキャス VLAN に設定されたモニタリング セッションで送信元ポートからのトラフィックを単にモニターします。スイッチまたは仮想ネットワークで設定する必要がある内容の詳細については、次のトピックを参照してください。

- ハードウェア FTD パッシブインターフェイスのスイッチの設定 （53 ページ）
- FTDv パッシブインターフェイスの VLAN の設定 （54 ページ）

トラフィックに影響を及ぼすことなくモニタ対象スイッチポートからのトラフィックを分析するには、パッシブ モードを使用します。パッシブ モードを使用するエンドツーエンドの例については、ネットワーク上のトラフィックをパッシブにモニタする方法を参照してください。

手順

ステップ 1 [Device] をクリックし、[Interfaces] サマリーにあるリンクをクリックし、[Interfaces] または [EtherChannel] をクリックします。

ステップ 2 編集する物理インターフェイスまたはEtherChannelの編集アイコン（  ）をクリックします。

現在使用されていないインターフェイスを選択します。使用中のインターフェイスをパッシブインターフェイスに変換する場合は、最初にセキュリティゾーンからインターフェイスを削除し、そのインターフェイスを使用する他のすべての設定を削除する必要があります。

ステップ 3 [ステータス（Status）] スライダを [有効（enabled）] 設定（  ）に設定します。

ステップ 4 次を設定します。

- [インターフェイス名（Interface Name）]：最大 48 文字のインターフェイスの名前。英字は小文字にする必要があります。たとえば、monitor などです。
- [モード（Mode）]：[パッシブ（Passive）] を選択します。
- （オプション）[説明（Description）]：説明は 200 文字以内で、改行を入れずに 1 行で入力します。

（注）
IPv4 アドレスまたは IPv6 アドレスを設定することはできません。[詳細（Advanced）] タブで変更できるのは、MTU、デュプレックス、速度設定のみです。

ステップ 5 [OK] をクリックします。

次のタスク

パッシブインターフェイスを作成するだけでは、インターフェイスで確認されるトラフィックの情報を十分にダッシュボードに示すことはできません、次の手順も実行する必要があります。使用例で次の手順について説明します。ネットワーク上のトラフィックをパッシブにモニタする方法を参照してください。

- パッシブ セキュリティ ゾーンを作成し、それにインターフェイスを追加します。セキュリティ ゾーンの設定を参照してください。
- パッシブ セキュリティ ゾーンを送信元ゾーンとして使用するアクセス制御ルールを作成します。通常は、これらのルールに侵入ポリシーを適用して、IDS（侵入検知システム）モニタリングを実装します。アクセス コントロール ポリシーを設定するを参照してください。

- 必要に応じて、パッシブ セキュリティ ゾーン向けに SSL 復号およびアイデンティティ ルールを作成し、セキュリティ インテリジェンス ポリシーを有効にします。

高度なインターフェイス オプションの設定

[詳細（Advanced）] オプションには、MTU、ハードウェア設定、管理専用、MAC アドレス、およびその他の設定が含まれています。

MAC アドレスについて

Media Access Control（MAC）アドレスを手動で設定してデフォルトをオーバーライドできます。

高可用性設定の場合は、インターフェイスのアクティブ MAC アドレスとスタンバイ MAC アドレスの両方を設定できます。アクティブユニットがフェールオーバーしてスタンバイユニットがアクティブになると、その新規アクティブユニットがアクティブな 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。

デフォルトの MAC アドレス

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。
- VLAN インターフェイス（Firepower 1010 および）：すべての VLAN インターフェイスが MAC アドレスを共有します。接続スイッチがどれもこのシナリオをサポートできるようにします。接続スイッチに固有の MAC アドレスが必要な場合、手動で MAC アドレスを割り当てることができます。詳細オプションの設定 （58 ページ）を参照してください。
- EtherChannel：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。
- サブインターフェイス：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バーンドイン MAC アドレスを使用します。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制御を行う場合があります。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。

MTU について

MTUは、FTD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可能な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

FTD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。

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。

UDPまたはICMPの場合、アプリケーションではフラグメント化を避けるためにMTUを考慮する必要があります。

（注） FTD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：ジャンボフレームとは、標準的な最大値1522バイト（レイヤ2ヘッダーおよびVLANヘッダーを含む）より大きく、9216バイトまでのイーサネットパケットのことです。ジャンボフレームに対応するために、MTUを9,000バイト以上に設定できます。最大値はモデルによって異なります。

（注） MTU を増やすとジャンボ フレームに割り当てるメモリが増え、他の機能（アクセスルールなど）の最大使用量が制限される場合があります。ASA 5500-X シリーズ デバイスまたは Firewall Threat Defense Virtual のデフォルト値の 1,500 よりも MTU のサイズを大きくする場合は、システムを再起動する必要があります。高可用性にデバイスが設定されている場合、スタンバイデバイスも再起動する必要があります。ジャンボフレームのサポートが常に有効な場合、その他のモデルを再起動する必要はありません。

詳細オプションの設定

高度なインターフェイス オプションには、ほとんどのネットワークに適合するデフォルト設定が用意されています。ネットワーキングの問題を解決している場合または高可用性を設定する場合にのみ、これを設定します。

次の手順では、インターフェイスが定義済みであることを前提としています。インターフェイスを最初に編集または作成するときに、これらの設定を編集することもできます。

制限事項

- ブリッジ グループの場合は、このほとんどのオプションはメンバー インターフェイスに対して設定します。DAD試行回数とHAモニタリングの有効化を除き、これらのオプションはブリッジ仮想インターフェイス（BVI）では使用できません。
- Firepower 1000および2100デバイス上の管理インターフェイスにMTU、デュプレックス、速度を設定することはできません。
- 拡張オプションは、Firepower 1010 スイッチポートでは使用できません。
- Firepower 4100/9300 のインターフェイスにデュプレックスおよび速度を設定することはできません。インターフェイスのこれらの機能を設定するには、FXOS を使用します。
- パッシブインターフェイスでは、MTU、デュプレックス、速度のみ設定できます。インターフェイスの管理のみを行うことはできません。

手順

ステップ 1 [デバイス（Device）] をクリックし、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックし、次にインターフェイス タイプをクリックして、インターフェイスのリストを表示します。

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 [詳細オプション（Advanced Options）] をクリックします。

ステップ 4 インターフェイスの状態を高可用性設定でピア装置にフェールオーバーするかどうか判断する際の要素にする場合は、[HAモニタリングの有効化（Enable for HA Monitoring）] を選択します。

このオプションは、高可用性を設定しない場合は無視されます。インターフェイスの名前を設定しない場合も、無視されます。

ステップ 5 データ インターフェイスを管理専用に指定する場合は、[管理専用（Management Only）] を選択します。

管理専用インターフェイスはトラフィックの通過を許可しないため、データインターフェイスを管理専用に設定する意味はあまりありません。管理/診断インターフェイスは、常に管理専用であるため、この設定を変更することはできません。

ステップ 6 [MTU]（最大伝送ユニット）を任意の値に設定します。

デフォルトのMTUは1500バイトです。最小値と最大値は、プラットフォームによって異なります。ジャンボフレームが頻繁にやり取りされるネットワークでは、大きな値に設定します。

（注）
ASA 5500-X シリーズデバイス、ISA 3000 シリーズデバイス、FTDv で MTU を 1500 より大きい値に設定する場合は、デバイスを再起動する必要があります。高可用性にデバイスが設定されている場合、スタンバイデバイスも再起動する必要があります。ジャンボフレームのサポートが常に有効な場合、その他のモデルを再起動する必要はありません。

ステップ 7 （物理インターフェイスのみ）速度およびデュプレックスの設定を変更します。

デフォルトでは、インターフェイスは接続相手のインターフェイスに対し、互いに最適なデュプレックスおよび速度をネゴシエートしますが、必要に応じて、特定のデュプレックスおよび速度を強制的に適用することもできます。記載されているオプションは、インターフェイスでサポートされているものだけです。ネットワークモジュールのインターフェイスにこれらのオプションを設定する前に、インターフェイス設定の制限事項 （6 ページ） をお読みください。

- [二重（Duplex）] : [自動（Auto）]、[ハーフ（Half）]、または [フル（Full）] を選択します。SFP インターフェイスは [全二重（Full）] のみをサポートします。
- [速度（Speed）] : 実際のオプションは、モデルとインターフェイスタイプによって異なります。速度、[自動（Auto）]、[ネゴシエーションなし（No Negotiate）]、または [SFPを検出（Detect SFP）] を選択してください。[ネゴシエーションなし（No Negotiate）] を指定すると速度が 1,000 Mbps に設定され、フロー制御パラメータとリモート障害情報のリンクネゴシエーションが無効になります。

ステップ 8 [IPv6設定（IPv6 Configuration）] を変更します。

- **[IPv6アドレス構成のDHCPの有効化（Enable DHCP for IPv6 address configuration）]** : IPv6 ルータのアドバタイズメントパケットに、管理アドレス構成フラグを設定するかどうか。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。

- **[IPv6アドレス以外の構成に対するDHCPの有効化（Enable DHCP for IPv6 non-address configuration）]**：IPv6ルータのアドバタイズメントパケットに、その他のアドレス構成フラグを設定するかどうか。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。
- [DADの試行（DAD Attempts）]：インターネット上で重複アドレス検出（DAD）を実行する頻度（0 ～ 600）。デフォルトは 1 です。ステートレス自動設定プロセスでは、DAD 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検証します。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。インターフェイスは、ネイバー送信要求メッセージを使用して、重複アドレス検出を実行します。重複アドレス検出（DAD）プロセスを無効にするには、この値を 0 に設定します。

ステップ 9 （必要に応じて、サブインターフェイスおよび高可用性装置に推奨されます。）MAC アドレスを設定します。

デフォルトでは、システムはインターフェイスのネットワークインターフェイスカード（NIC）に焼き込まれた MAC アドレスを使用します。したがって、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 MAC アドレスを使用するため、サブインターフェイスごとに一意のアドレスを作成する必要がある場合があります。手動設定されたアクティブ/スタンバイ MAC アドレスも、高可用性を設定する場合に推奨されます。MAC アドレスを定義すると、フェールオーバー時にネットワークの一貫性を維持できます。

- [MACアドレス（MAC Address）]：H.H.H 形式の Media Access Control。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。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。
- [スタンバイMACアドレス（Standby MAC Address）]：高可用性で使用します。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 10 [OK] をクリックします。

インターフェイスの変更のスキャンとインターフェイスの移行

デバイスのインターフェイスを変更すると、デバイスは変更が発生したことを FDM に通知します。インターフェイスのスキャンを実行するまで、設定を展開することはできません。FDM では、セキュリティポリシー内のインターフェイスを別のインターフェイスに移行することができるため、インターフェイスの削除はほぼシームレスに実行できます。

インターフェイスのスキャンと移行について

Scanning

デバイスのインターフェイスを変更すると、デバイスは変更が発生したことを FDM に通知します。インターフェイスのスキャンを実行するまで、設定は展開できません。インターフェイスの追加、削除、または復元を検出するスキャンの後に設定を展開できますが、削除されたインターフェイスを参照している設定の部分は展開されません。

スキャンを必要とするインターフェイスの変更には、インターフェイスの追加や削除が含まれます。たとえば、ネットワークモジュールの変更、Firepower 4100/9300 シャーシ上に割り当てられたインターフェイスの変更、FTDv でのインターフェイスの変更などです。

次の変更は、スキャン後の展開をブロックしません。

- セキュリティゾーンのメンバーシップ
- EtherChannel インターフェイスのメンバーシップ
- Firepower 1010 VLAN インターフェイス スイッチポートのメンバーシップ
- BVI を参照するポリシーのブリッジ グループ インターフェイスのメンバーシップ

（注） syslog サーバーの出力インターフェイスの変更によって展開がブロックされることはありませんが、syslog サーバーの設定は、手動で、またはインターフェイス交換機能を使用して修正する必要があります。

Migrating

新しいインターフェイスの追加や未使用のインターフェイスの削除が、Firepower Threat Defense 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、セキュリティゾーン、NAT、VPN、ルーティング、DHCP サーバーなど、Firepower Threat Defense 設定内の多くの場所で直接参照できます。

Firewall Device Manager では、セキュリティポリシー内のインターフェイスを別のインターフェイスに移行することができるため、インターフェイスの削除はほぼシームレスに実行できます。

（注） 移行機能は、名前、IP アドレス、およびその他の設定をインターフェイス間でコピーしません。この機能は、古いインターフェイスではなく新しいインターフェイスを参照するようにセキュリティポリシーを変更します。移行する前に、新しいインターフェイスの設定を手動で設定する必要があります。

インターフェイスを削除する必要がある場合は、古いインターフェイスを削除する「前に」、新しいインターフェイスを追加し、古いインターフェイスを移行することをお勧めします。インターフェイスの追加と削除を同時に行っても移行プロセスは機能します。ただし、削除されたインターフェイスやそれらを参照するポリシーを「手動で」編集することはできません。そのため、移行を段階的に実行する方が簡単になる場合があります。

同じタイプのインターフェイスを交換する場合（たとえば、ネットワークモジュールを RMA する必要がある場合）は、次のことができます。1. シャーシからモジュールを取り外す。2. スキャンを実行する。3. 削除されたインターフェイスとは関係のない変更を展開する。4. モジュールを交換する。5. 新しいスキャンを実行する。6. インターフェイス関連の変更を含め、設定を展開します。新しいインターフェイスのインターフェイス ID と特性が古いインターフェイスと同じである場合は、移行を実行する必要はありません。

インターフェイスのスキャンと移行に関する注意事項と制限事項

サポートされていないインターフェイスの移行

- BVI への物理インターフェイス
- ファイアウォール インターフェイスへのパッシブインターフェイス
- ブリッジグループメンバー
- EtherChannel インターフェイスメンバー
- ISA 3000 ハードウェア バイパス メンバー
- Firepower 1010 VLAN インターフェイスまたはスイッチポート
- 診断インターフェイス
- HA フェールオーバーおよびステートリンク
- さまざまなタイプのインターフェイスの移行（たとえば、物理インターフェイスを必要とする機能へのブリッジ グループ インターフェイスの移行）

その他のガイドライン

- インターフェイスを削除する必要がある場合は、古いインターフェイスを削除する「前に」、新しいインターフェイスを追加し、古いインターフェイスを移行することをお勧めします。
- FTDv では、インターフェイスリストの末尾でインターフェイスの追加や削除が行われるだけです。他の場所でインターフェイスを追加または削除した場合、ハイパーバイザによってインターフェイスの番号が再設定され、その結果、設定内のインターフェイス ID が誤ったインターフェイスと一致します。
- スキャン/移行が失敗した場合は、シャーシの元のインターフェイスを復元し、元の状態に戻すために再スキャンします。

- バックアップの場合は、新しいインターフェイスを使用して新しいバックアップを作成してください。古い設定で復元すると、古いインターフェイス情報が復元され、スキャン/置換を再度実行する必要が生じます。
- HA の場合は、アクティブユニットでインターフェイススキャンを実行する前に、両方の装置で同じインターフェイスの変更を行います。アクティブユニットでスキャン/移行を実行する必要があるだけです。設定の変更はスタンバイ ユニットに複製されます。

インターフェイスのスキャンと移行

Firewall Device Manager でインターフェイスの変更をスキャンし、削除されたインターフェイスからインターフェイス設定を移行します。インターフェイス設定の移行のみを必要とする場合は（スキャンは不要）、次の手順のうちスキャンに関連するステップを無視してください。

（注） 移行機能は、名前、IP アドレス、およびその他の設定をインターフェイス間でコピーしません。この機能は、古いインターフェイスではなく新しいインターフェイスを参照するようにセキュリティポリシーを変更します。移行する前に、新しいインターフェイスの設定を手動で設定する必要があります。

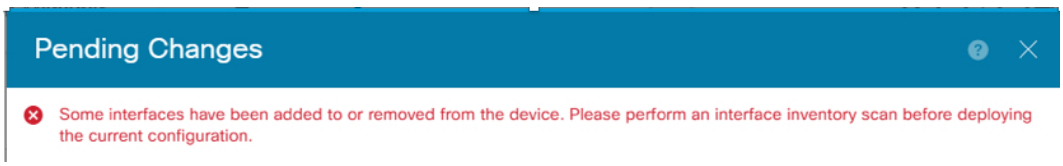
手順

ステップ 1 シャーシでインターフェイスを追加または削除します。

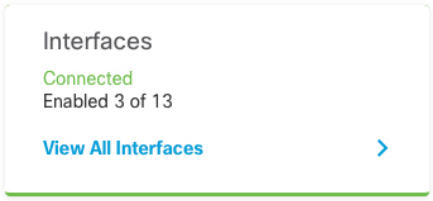
インターフェイスを削除する必要がある場合は、古いインターフェイスを削除する「前に」、新しいインターフェイスを追加し、古いインターフェイスの置き換えを実行することをお勧めします。

ステップ 2 インターフェイスの変更をスキャンします。

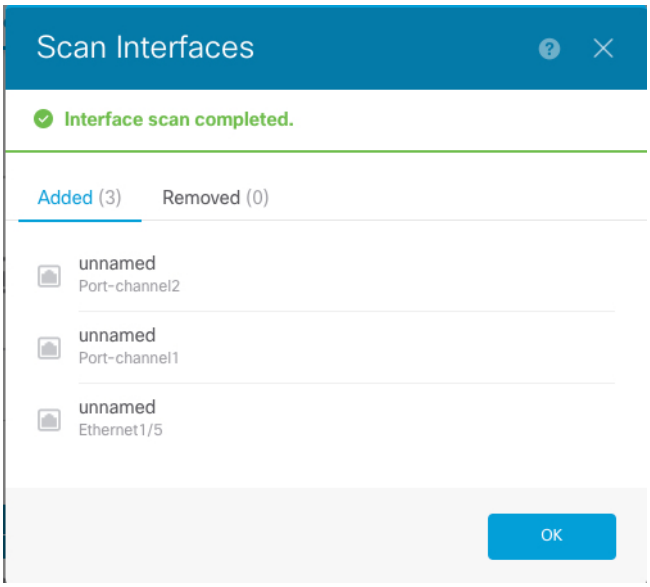
インターフェイスのスキャンを実行するまで、設定は展開できません。スキャンの前に展開しようとすると、次のエラーが表示されます。



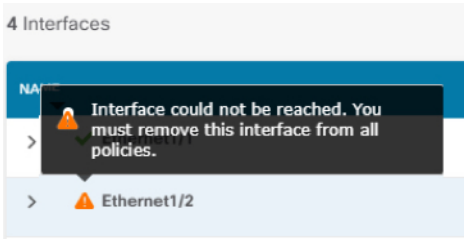
a) [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにある [すべてのインターフェイスを表示（View All Interfaces）] リンクをクリックします。



b) [インターフェイスのスキャン（Scan Interfaces）]アイコン（ ）をクリックします。
c) インターフェイスがスキャンされるのを待ってから、[OK] をクリックします。



スキャン後、削除されたインターフェイスは、[インターフェイス（Interfaces）] ページに注意記号とともに表示されます。



ステップ 3 既存のインターフェイスを新しいインターフェイスに移行するには、次の手順を実行します。

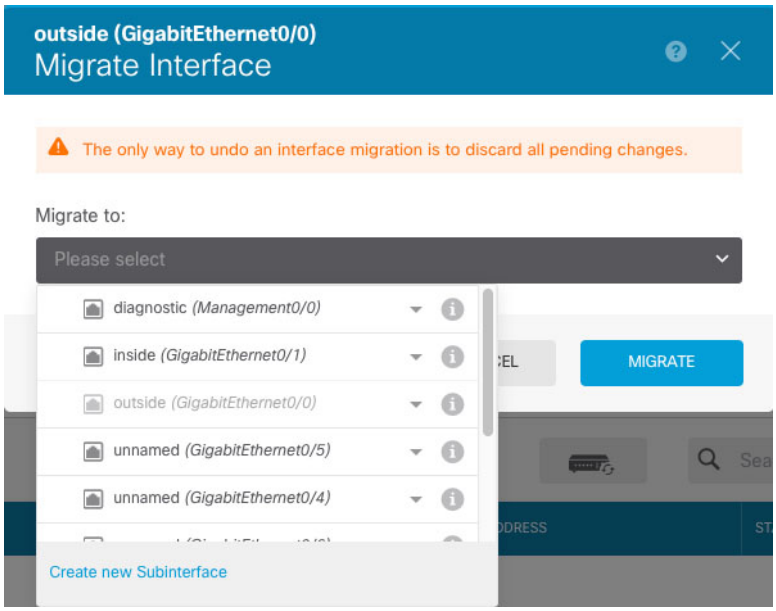
a) 新しいインターフェイスに名前、IP アドレスなどを設定します。

削除するインターフェイスの既存の IP アドレスと名前を使用する場合は、新しいインターフェイスでこれらの設定を使用できるように、まず古いインターフェイスをダミーの名前と IP アドレスで再設定する必要があります。

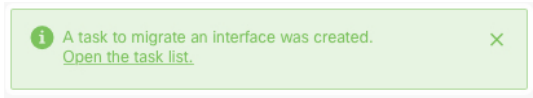
b) 古いインターフェイスの [移行（Migrate）] アイコンをクリックします。

このプロセスによって、インターフェイスを参照しているすべての設定で、古いインターフェイスが新しいインターフェイスに移行されます。

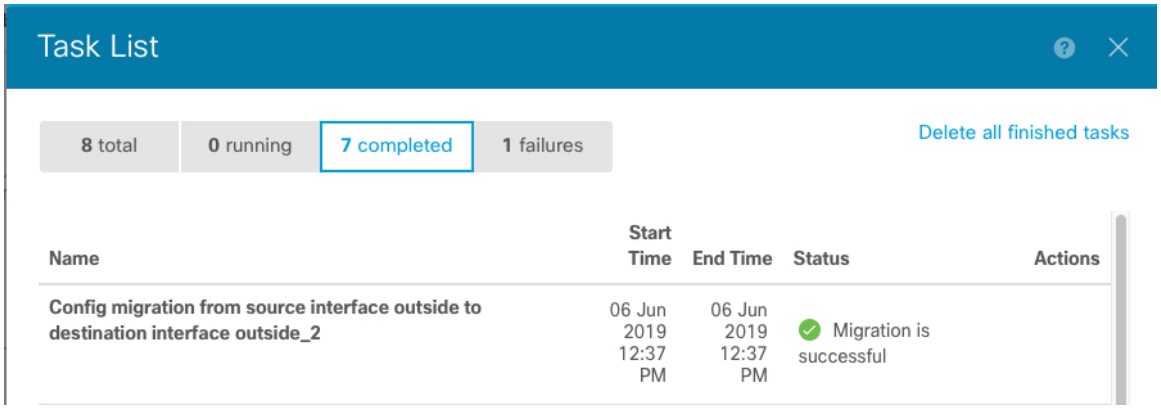
c) [移行先：（Migrate to:）] ドロップダウンリストから新しいインターフェイスを選択します。



d) [インターフェイス（Interfaces）] ページにメッセージが表示されます。メッセージ内のリンクをクリックします。



e) [タスクリスト（Task List）] を調べて、移行が成功したことを確認します。

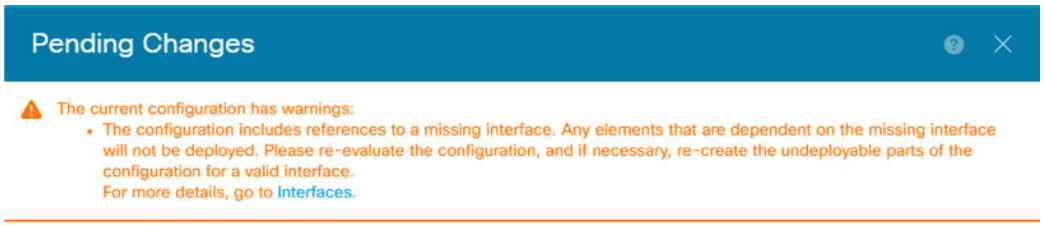


f) 移行が失敗した場合は、API エクスプローラで理由を確認できます。

API エクスプローラを開くには、[詳細オプション（More options）] ボタン（⋮）をクリックし、[APIエクスプローラ（API Explorer）] を選択します。**[インターフェイス（Interface）] > [GET /jobs/interfacemigrations]** を選択し、[試してみる（Try it Out!）] をクリックします。

ステップ 4 設定を展開します。

削除されたインターフェイスを参照する設定の部分は展開されません。その場合、次のメッセージが表示されます。



ステップ 5 シャーシの古いインターフェイスを取り外し、別のスキャンを実行します。

削除されたインターフェイスのうちポリシーで使用されなくなったものは、[インターフェイス（Interfaces）] ページから削除されます。

ステップ 6 設定を再度展開し、使用していないインターフェイスを設定から削除します。

停電時のハードウェアバイパスの設定（ISA 3000）

ハードウェア バイパスを有効にして、停電時でもトラフィックがインターフェイス ペア間を通過できるようにできます。サポートされているインターフェイスペアは銅線インターフェイスの GigabitEthernet 1/1 と 1/2、および GigabitEthernet 1/3 と 1/4 です。光ファイバ イーサネット モデルを保有している場合は、銅線イーサネット ペア（GigabitEthernet 1/1 と 1/2）でのみハードウェア バイパスがサポートされます。デフォルトでは、サポートされている場合、両方のインターフェイスペアに対してハードウェアバイパスが有効になります。

ハードウェア バイパスがアクティブの場合、トラフィックはレイヤ 1 でそれらのインターフェイス ペア間を通過します。Firewall Device Manager と Firewall Threat Defense CLI の両方に、インターフェイスがダウンしていることが表示されます。ファイアウォール機能はないため、トラフィックのデバイス通過を許可することのリスクを理解している必要があります。

（この手順で説明されている）TCP シーケンス番号のランダム化は無効にすることをお勧めします。デフォルトでは、ISA 3000 を通過する TCP 接続の最初のシーケンス番号（ISN）が乱数に書き換えられます。ハードウェア バイパスがアクティブになると、ISA 3000 はデータ パスには入らず、シーケンス番号は変換されません。受信側のクライアントが予期しないシーケンス番号を受信すると接続がドロップされるため、TCP セッションを再確立する必要がありま

す。TCP シーケンス番号のランダム化が無効になっている場合でも、スイッチオーバー中に一時的にダウンするリンクがあるため、一部の TCP 接続は再確立する必要があります。

CLI コンソールまたは SSH セッションで、**show hardware-bypass** コマンドを使用して動作ステータスをモニターします。

始める前に

ハードウェア バイパスを機能させるための前提条件：

- インターフェイス ペアは同じブリッジ グループに配置する必要があります。
- インターフェイスはスイッチのアクセス ポートに接続する必要があります。トランク ポートには接続しないでください。

手順

ステップ 1 [デバイス（Device）] をクリックして、[インターフェイス（Interfaces）] サマリーのリンクをクリックします。

ページの上部にある [ハードウェアバイパス（Hardware Bypass）] セクションは、このデバイスに使用できるインターフェイスペアの現在の設定を示します。

ただし、ハードウェアバイパスを有効にする前に、ペアが同じブリッジグループで設定されていることを確認する必要があります。

ステップ 2 [編集（Edit）] をクリックしてハードウェアバイパスを設定します。

[ハードウェアバイパスの設定（Hardware Bypass Configuration）] ダイアログボックスが表示されます。

ステップ 3 自動ハードウェアバイパス動作を設定するには、インターフェイスペアごとに、[停電時のハードウェアバイパス（Hardware Bypass during Power Down）] エリアで次のいずれかのオプションを選択します。

- [無効化（Disable）]：ハードウェアバイパスを無効にします。トラフィックは、停電時にデバイスを通過しません。
- [有効化（Enable）]：停電時にハードウェアバイパスをアクティブにします。ハードウェアバイパスが、停電時にトラフィックが中断されないように確保します。バイパスされたトラフィックは検査されず、セキュリティポリシーは適用されないことに注意してください。電源が復旧したら、ハードウェアバイパスは自動的に無効になるため、トラフィックフローの通常の状態を維持することができ、検査も行われます。ハードウェアバイパスを無効にすると、トラフィックが一時的に中断する可能性があることに注意してください。
- [永続的に有効化（Enable with Persistence）]：停電時にハードウェアバイパスをアクティブにし、電源の復元後も有効な状態を維持します。電源が復旧したら、[手動ハードウェアバイパス（Manual Hardware Bypass）] スライダを使用してハードウェアバイパスを無効に

する必要があります。このオプションでは、トラフィックに一時的な中断が発生したときに制御することができます。

ステップ 4 （任意） ハードウェアバイパスを手動で有効または無効にするには、[手動ハードウェアバイパス（Manual Hardware Bypass）] スライダをクリックします。

たとえば、システムをテストしたり、何らかの理由でデバイスを一時的にバイパスする必要がある場合があります。ハードウェアバイパスの状態を変更するには、設定を展開する必要があることに注意してください。設定を変更するだけでは不十分です。

ハードウェア バイパスを手動で有効化または無効化すると、次の Syslog メッセージが表示されます。メッセージ内の *pair* は 1/1-1/2 または 1/3-1/4 です。

- %FTD-6-803002: no protection will be provided by the system for traffic over GigabitEthernet *pair*
- %FTD-6-803003: User disabled bypass manually on GigabitEthernet *pair*

ステップ 5 [OK] をクリックします。

変更はすぐには適用されません。設定を展開する必要があります。

ステップ 6 （オプション）TCP シーケンス番号のランダム化を無効にするために必要な FlexConfig オブジェクトとポリシーを作成します。

a) **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

b) 詳細設定の目次で **[FlexConfig]** > **[FlexConfigオブジェクト（FlexConfig Objects）]** をクリックします。

c) 新しいオブジェクトを作成するには、[+] ボタンをクリックします。

d) オブジェクトの名前を入力します。たとえば、**Disable_TCP_Randomization** と入力します。

e) [テンプレート（Template）] エディタに、TCP シーケンス番号のランダム化を無効にするコマンドを入力します。

コマンドは **set connection random-sequence-number disable** ですが、ポリシーマップ内の特定のクラスに対して設定する必要があります。最も簡単なアプローチは、ランダムなシーケンス番号をグローバルに無効にする方法です。この場合、次のコマンドを入力する必要があります。

```
policy-map global_policy
 class default_class
  set connection random-sequence-number disable
```

f) [ネゲートテンプレート（Negate Template）] エディタで、この設定を元に戻すために必要な行を入力します。

たとえば、TCP シーケンス番号のランダム化をグローバルに無効にしている場合、ネゲートテンプレートは次のようになります。

```
policy-map global_policy
 class default_class
  set connection random-sequence-number enable
```

g) [OK] をクリックしてオブジェクトを保存します。

オブジェクトを FlexConfig ポリシーに追加する必要があります。オブジェクトを作成するだけでは十分ではありません。

h) 目次で [FlexConfigポリシー（FlexConfig Policy）] をクリックします。

i) [グループリスト（Group List）] で [+] をクリックします。

j) [Disable_TCP_Randomization] オブジェクトを選択し、[OK] をクリックします。

プレビューはテンプレートのコマンドで更新されます。予想されるコマンドが表示されているか確認します。

k) [保存（Save）] をクリックします。

これでポリシーを展開できます。

モニタリング インターフェイス

次の領域に、インターフェイスに関する一部の基本情報を表示できます。

- [デバイス（Device）]。インターフェイスの現在の状態をモニターするには、ポート グラフィックを使用します。ポートにマウスポインタを合わせると、そのポートの IP アドレス、EtherChannel メンバーシップ、有効ステータス、リンクステータスが表示されます。IP アドレスは DHCP を使用して静的に割り当てたり取得したりできます。

  インターフェイス ポートは、次のカラー コーディングを使用します。

  - 緑：インターフェイスは設定され、有効で、リンクは稼働中です。
  - グレー：インターフェイスは無効です。
  - オレンジ/赤：インターフェイスが設定され、有効ですが、リンクがダウンしています。インターフェイスが有線の場合、これは修正が必要なエラー状態です。インターフェイスが有線でない場合、これは予期されるステータスです。

- **[モニタリング（Monitoring）]** > **[システム（System）]**。[スループット（Throughput）] ダッシュボードには、システムを介して移動するトラフィックに関する情報が表示されます。すべてのインターフェイスに関する情報を表示できます。または、調査する特定のインターフェイスを選択できます。

- **[モニタリング（Monitoring）]** > **[ゾーン（Zones）]**。これらのダッシュボードにはインターフェイスを設定するセキュリティゾーンに基づく統計情報が表示されます。詳細について、この情報を掘り下げることができます。

CLI でのインターフェイスのモニタリング

CLI コンソールを開くか、またはデバイスの CLI にログインして、次のコマンドを使用し、インターフェイス関連の動作と統計情報に関する詳細情報を取得することもできます。

- **show interface** はインターフェイスの統計情報と設定情報を表示します。このコマンドには多数のキーワードがあり、必要な情報を取得するために使用できます。使用可能なオプションを表示するには、「?」をキーワードとして使用します。
- **show ipv6 interface** はインターフェイスに関する IPv6 設定情報を表示します。
- **show bridge-group** は、メンバー情報や IP アドレスを含む、ブリッジ仮想インターフェイス（BVI）に関する情報を表示します。
- **show conn** は現在インターフェイスを通じて確立されている接続に関する情報を表示します。
- **show traffic** は各インターフェイスを介したトラフィックフローに関する統計情報を表示します。
- **show ipv6 traffic** はデバイスを介した IPv6 トラフィックフローに関する統計情報を表示します。
- **show dhcpd** はインターフェイスの DHCP 使用状況に関する統計とその他の情報を表示し、特にインターフェイスで設定されている DHCP サーバーに関する情報が含まれます。
- **show switch vlan** は VLAN とスイッチポートの関連付けを表示します。
- **show switch mac-address-table** はスタティックおよびダイナミック MAC アドレスエントリを表示します。
- **show arp** はダイナミック、スタティック、およびプロキシ ARP エントリを表示します。
- **show power inline** PoE ステータスを表示します。
- **show vpdn group** は PPPoE グループと、設定されているユーザー名と認証を表示します。
- **show vpdn username** は PPPoE のユーザー名とパスワードを表示します。
- **show vpdn session pppoe state** は PPPoE セッションのステータスを表示します。

インターフェイスの例

使用例の章には、次のインターフェイス関連の例が含まれています。

- FDM でデバイスを設定する方法
- サブネットを追加する方法
- ネットワーク上のトラフィックをパッシブにモニタする方法

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。