インターフェイスの概要

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

管理インターフェイス

バージョン 7.3 以前の場合、 バージョン 7.4 以降では、診断インターフェイスが管理インターフェイスに統合され、ユーザーエクスペリエンスが簡素化されました。

管理インターフェイス

管理インターフェイスは、デバイスの他のインターフェイスとは分離されています。Management Centerにデバイスを設定し、登録するために使用されます。また、固有の IP アドレスとスタティック ルーティングを使用します。管理インターフェイスを設定するには、CLI で **configure network** コマンドを使用します。また、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[デバイス（Devices）]** > **[インターフェイス（Interfaces）]** ページでステータスを表示することもできます。管理インターフェイスを Management Center に追加した後にその IP アドレスを CLI で変更した場合、Secure Firewall Management Center での IP アドレスを **[デ**

バイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Devices）] > [管理（Management）] エリアで一致させることができます。

または、管理インターフェイスの代わりにデータインターフェイスを使用して Threat Defense を管理できます。

診断インターフェイス（レガシー）

7.4 以降を使用している新しいデバイスの場合、レガシー診断インターフェイスは使用できません。マージされた管理インターフェイスのみを使用できます。

7.4 以降にアップグレードし、診断インターフェイスの設定がない場合は、インターフェイスが自動的にマージされます。

7.4 以降にアップグレードし、診断インターフェイスの設定がある場合は、インターフェイスを手動でマージするか、別の診断インターフェイスを引き続き使用できます。診断インターフェイスのサポートは今後のリリースで削除されるため、できるだけ早くインターフェイスをマージする必要があります。管理インターフェイスと診断インターフェイスを手動でマージするには、管理インターフェイスと診断インターフェイスのマージ （43 ページ）を参照してください。自動マージを防止する設定には、次のものが含まれます。

- 「管理」という名前のデータインターフェイス。この名前は、マージされた管理インターフェイスで使用するために予約されています。
- 診断の IP アドレス
- 診断で有効な DNS
- Syslog、SNMP、RADIUS、または AD（リモートアクセス VPN 用）送信元インターフェイスが診断
- 送信元インターフェイスが指定されておらず、管理専用（診断を含む）として設定されているインターフェイスが少なくとも 1 つある RADIUS または AD（リモートアクセス VPN 用）。これらのサービスのデフォルトルートルックアップは、管理専用ルーティングテーブルからデータルーティングテーブルに変更されていて、管理にフォールバックされません。したがって、管理以外の管理専用インターフェイスは使用できません。
- 診断のスタティックルート
- 診断のダイナミックルーティング
- 診断の HTTP サーバー
- 診断の ICMP
- 診断用の DDNS
- 診断を使用した FlexConfig

レガシー診断インターフェイスの動作の詳細については、このガイドの 7.3 バージョンを参照してください。

インターフェイス モードとタイプ

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

通常のファイアウォール モード

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

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

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

IPS 専用モード

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

（注） ファイアウォール モードは通常のファイアウォール インターフェイスにのみ影響を与えます。インライン セットやパッシブ インターフェイスなどの IPS 専用インターフェイスには影響を与えません。IPS 専用インターフェイスは両方のファイアウォール モードで使用可能です。

IPS 専用インターフェイスは以下のタイプとして展開できます。

- インライン セット、タップ モードのオプションあり：インライン セットは「Bump In The Wire」のように動作し、2 つのインターフェイスを一緒にバインドし、既存のネットワー

クに組み込みます。この機能によって、隣接するネットワークデバイスの設定がなくても、任意のネットワーク環境に Threat Defense をインストールすることができます。インラインインターフェイスはすべてのトラフィックを無条件に受信しますが、これらのインターフェイスで受信されたすべてのトラフィックは、明示的にドロップされない限り、インライン セットの外部に再送信されます。

タップモードでは、Threat Defense はインラインで展開されますが、ネットワーク トラフィック フローは妨げられません。代わりに、Threat Defense は各パケットのコピーを作成して、パケットを分析できるようにします。それらのタイプのルールでは、ルールがトリガーされると侵入イベントが生成され、侵入イベントのテーブルビューにはトリガーの原因となったパケットがインライン展開でドロップされたことが示されることに注意してください。インライン展開された FTD でタップモードを使用することには、利点があります。たとえば、Threat Defense がインラインであるかのように Thereat Defense とネットワーク間の接続を設定し、Threat Defense が生成する侵入イベントの種類を分析できます。その結果に基づいて、効率性に影響を与えることなく最適なネットワーク保護を提供するように、侵入ポリシーを変更してドロップ ルールを追加できます。Threat Defense をインラインで展開する準備ができたら、タップモードを無効にして、Threat Defense とネットワーク間の配線を再びセットアップせずに、不審なトラフィックのドロップを開始することができます。

（注） タップモードは、トラフィックによっては Threat Defense のパフォーマンスに大きく影響します。

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

- パッシブまたは ERSPAN パッシブ：パッシブ インターフェイスは、スイッチ SPAN またはミラー ポートを使用してネットワークを流れるトラフィックをモニタします。SPAN またはミラー ポートでは、スイッチ上の他のポートからトラフィックをコピーできます。この機能により、ネットワーク トラフィックのフローに含まれなくても、ネットワークでのシステムの可視性が備わります。パッシブ展開で Threat Defense を構成した場合は、Threat Defense で特定のアクション（トラフィックのブロッキングやシェーピングなど）を実行することができません。パッシブインターフェイスはすべてのトラフィックを無条件で受信します。このインターフェイスで受信されたトラフィックは再送されません。Encapsulated Remote Switched Port Analyzer（ERSPAN）インターフェイスは、複数のスイッチに分散された送信元ポートからのトラフィックをモニタし、GRE を使用してトラフィックをカプセル化します。ERSPAN インターフェイスは、Threat Defense がルーテッド ファイアウォール モードになっている場合にのみ許可されます。

（注） 無差別モードの制限により、SR-IOV ドライバを使用する一部の Intel ネットワークアダプタ（Intel X710 や 82599 など）では、SR-IOV インターフェイスを NGFWv のパッシブインターフェイスとして使用することはできません。このような場合は、この機能をサポートするネットワークアダプタを使用してください。Intel ネットワークアダプタの詳細については、『Intel Ethernet Products』[英語] を参照してください。

セキュリティ ゾーンとインターフェイス グループ

各インターフェイスは、セキュリティゾーンおよびインターフェイスグループに割り当てることができます。その上で、ゾーンまたはグループに基づいてセキュリティ ポリシーを適用します。たとえば、1つ以上のデバイスの「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。次に、同じゾーンを使用するすべてのデバイスについて、トラフィックが内部ゾーンから外部ゾーンに移動できるようにアクセス コントロール ポリシーを設定できます。

各オブジェクトに属するインターフェイスを表示するには、**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**を選択し、[インターフェイス（Interface）] の順に選択します。このページでは、管理対象デバイスで設定されているセキュリティゾーンとインターフェイスグループの一覧が表示されます。各インターフェイス オブジェクトを展開して、各インターフェイス オブジェクトのインターフェイスのタイプを表示できます。

（注） **あらゆる**ゾーンに適用されるポリシー（グローバルポリシー）は、ゾーン内のインターフェイスだけでなく、ゾーンに割り当てられていないインターフェイスにも適用されます。

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

セキュリティゾーンとインターフェイスグループ

インターフェイス オブジェクトには次の 2 つのタイプがあります。

- セキュリティ ゾーン：インターフェイスは、1 つのセキュリティ ゾーンにのみ属することができます。
- インターフェイス グループ：インターフェイスは複数のインターフェイスグループ（および 1 つのセキュリティ ゾーン）に属することができます。

NAT ポリシー、プレフィルタポリシー、および QoS ポリシーでインターフェイスグループを使用できるほか、Syslog サーバーや DNS サーバーなどのインターフェイス名を直接指定できる機能も使用できます。

ポリシーによっては、セキュリティ ゾーンだけをサポートする場合も、ゾーンとグループの両方をサポートする場合もあります。セキュリティゾーンはすべての機能でサポートされているため、インターフェイスグループが提供する機能を必要としないない限り、デフォルトでセキュリティゾーンを使用する必要があります。

既存のセキュリティ ゾーンをインターフェイス グループに、またはその逆に変更することはできません。代わりに、新しいインターフェイス オブジェクトを作成する必要があります。

（注） トンネルゾーンはインターフェイス オブジェクトではありませんが、特定の設定ではセキュリティ ゾーンの代わりにトンネルゾーンを使用できます。トンネル ゾーンおよびプレフィルタリングを参照してください。

インターフェイス オブジェクト タイプ

次のインターフェイス オブジェクト タイプを参照してください。

- パッシブ：IPS 専用パッシブまたは ERSPAN インターフェイスの場合。
- インライン：IPS 専用インライン セット インターフェイスの場合。
- スイッチド：通常のファイアウォール ブリッジ グループ インターフェイスの場合。
- ルーテッド：通常のファイアウォール ルーテッド インターフェイスの場合。
- ASA：（セキュリティゾーンのみ）レガシー ASA FirePOWER デバイスインターフェイスの場合。
- 管理：（インターフェイスグループのみ）管理専用インターフェイスの場合。
- ループバック：（インターフェイスグループのみ）ループバックインターフェイスの場合。

インターフェイス オブジェクト内のすべてのインターフェイスは、同じタイプである必要があります。インターフェイス オブジェクトを作成した後、それに含まれるインターフェイスのタイプを変更することはできません。

インターフェイス名

インターフェイス（またはゾーン名）自体では、セキュリティポリシーに関してデフォルトの動作が提供されません。将来の構成での間違いを防ぐために、わかりやすい名前を使用することをお勧めします。適切な名前とは、論理セグメントまたはトラフィック仕様を表すものです。次に例を示します。

- 内部インターフェイスの名前：InsideV110、InsideV160、InsideV195

- DMZ インターフェイスの名前：DMZV11、DMZV12、DMZV-TEST
- 外部インターフェイスの名前：Outside-ASN78、Outside-ASN91

Auto-MDI/MDIX 機能

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

インターフェイスのデフォルト設定

この項では、インターフェイスのデフォルト設定を示します。

インターフェイスのデフォルトの状態

インターフェイスの状態は、タイプによって異なります。

- 物理インターフェイス：ディセーブル。初期セットアップで有効になる管理インターフェイスは例外です。
- 冗長インターフェイス：イネーブル。ただし、トラフィックが冗長インターフェイスを通過するためには、メンバ物理インターフェイスもイネーブルになっている必要があります。
- VLAN サブインターフェイス：イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。
- EtherChannel ポートチャネル インターフェイス（ISA 3000）：有効。ただし、トラフィックが EtherChannel を通過するためには、チャネル グループ物理インターフェイスもイネーブルになっている必要があります。
- EtherChannel ポートチャネル インターフェイス（Firepower および Cisco Secure Firewall モデル）：無効。

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

デフォルトの速度および二重通信

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

デフォルトでは、光ファイバ（SFP）インターフェイスの速度とデュプレックスは最大速度に設定され、自動ネゴシエーションが有効です。

Cisco Secure Firewall 3100/4200 の場合、速度は、インストールされている SFP の速度を検出するように設定されています。

セキュリティゾーンおよびインターフェイスグループオブジェクトの作成

デバイスインターフェイスを割り当てることができるセキュリティゾーンとインターフェイスグループを追加します。

ヒント 空のインターフェイスオブジェクトを作成し、後からインターフェイスを追加できます。インターフェイスを追加するには、インターフェイスに名前が付いている必要があります。インターフェイスを設定しているときに、セキュリティゾーンを作成することもできます（インターフェイスグループは作成できません）。

始める前に

各種インターフェイス オブジェクトの使用要件および制限を理解します。セキュリティ ゾーンとインターフェイス グループ （5 ページ） を参照してください。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ 2 オブジェクトタイプのリストから、[インターフェイス（Interface）] を選択します。

ステップ 3 [追加（Add）] > [セキュリティゾーン（Security Zone）] または [追加（Add）] > [インターフェイスグループ（Interface Group）] をクリックします。

ステップ 4 名前を入力します。

ステップ 5 [インターフェイス タイプ（Interface Type）] を選択します。

ステップ 6 （任意）**[デバイス（Device）] > [インターフェイス（Interfaces）]** ドロップダウンリストから、追加するインターフェイスを含むデバイスを選択します。

この画面でインターフェイスを割り当てる必要はありません。代わりに、インターフェイスを設定するときに、インターフェイスをゾーンまたはグループに割り当てることができます。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の展開を参照してください。

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

ここでは、次の方法について説明します。

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

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

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

（注） Firepower 1010 のスイッチポートについては、Firepower 1010 のスイッチポートの設定 を参照してください。

始める前に

Management Center に追加した後、デバイスの物理インターフェイスを変更した場合、[インターフェイス（Interfaces）] の左上にある [デバイスからのインターフェイスの同期（Sync Interfaces

from device）] をクリックしてそのインターフェイスリストを更新する必要があります。ホットスワップをサポートする Cisco Secure Firewall 3100/4200 については、デバイスのインターフェイスを変更する前に「Cisco Secure Firewall 3100/4200 のネットワークモジュールの管理（26 ページ）」を参照してください。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Threat Defense デバイス**[編集（Edit）]**（✎）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。

ステップ 2 編集するインターフェイス **[編集（Edit）]**（✎）をクリックします。

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

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

説明は 200 文字以内で、改行を入れずに 1 行で入力します。

ステップ 5 （任意）**[ハードウェア構成（Hardware Configuration）]** > **[速度（Speed）]**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。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）] : 速度を選択します（モデルによって異なります）。（Cisco Secure Firewall 3100/4200 のみ）[SFPを検出（Detect SFP）] を選択してインストールされている SFP モジュールの速度を検出し、適切な速度を使用します。デュプレックスは常に全二重で、自動ネゴシエーションは常に有効です。このオプションは、後でネットワークモジュールを別のモデルに変更し、速度を自動的に更新する場合に便利です。
- [自動ネゴシエーション（Auto-negotiation）] : 速度、リンクステータス、およびフロー制御をネゴシエートするようにインターフェイスを設定します。
- [前方誤り訂正モード（Forward Error Correction Mode）] :（Cisco Secure Firewall 3100/4200 のみ）25 Gbps 以上のインターフェイスの場合は、前方誤り訂正（FEC）を有効にします。EtherChannel メンバーインターフェイスの場合は、EtherChannel に追加する前に FEC を設定する必要があります。**自動**を使用する場合に選択する設定は、トランシーバのタイプと、インターフェイスが固定（内蔵）かネットワークモジュールかによって異なります。

表 *1* : 自動設定のデフォルト *FEC*

トランシーバ タイプ	固定ポートのデフォルト FEC（イーサネット 1/9 ～ 1/16）	ネットワークモジュールのデフォルト FEC
25G-SR	第 108 条 RS-FEC	第 108 条 RS-FEC
25G-LR	第 108 条 RS-FEC	第 108 条 RS-FEC
10/25G-CSR	第 108 条 RS-FEC	第 74 条 FC-FEC

トランシーバ タイプ	固定ポートのデフォルト FEC（イーサネット 1/9 ～ 1/16）	ネットワークモジュールのデフォルト FEC
25G-AOC*x*M	第 74 条 FC-FEC	第 74 条 FC-FEC
25G-CU2.5/3M	自動ネゴシエーション	自動ネゴシエーション
25G-CU4/5M	自動ネゴシエーション	自動ネゴシエーション
25/50/100G	第 91 条 RS-FEC	第 91 条 RS-FEC

ステップ 6 （任意）（Firepower 1100/2100、Cisco Secure Firewall 3100/4200）**[ハードウェア設定（Hardware Configuration）]** > **[ネットワーク接続（Network Connectivity）]** の順にクリックして Link Layer Discovery Protocol（LLDP）を有効にします。

- [LLDP受信の有効化（Enable LLDP Receive）]：ファイアウォールがピアから LLDP パケットを受信できるようにします。
- [LLDP送信の有効化（Enable LLDP Transmit）]：ファイアウォールがピアに LLDP パケットを送信できるようにします。

ステップ 7 （任意）（Cisco Secure Firewall 3100/4200）**[ハードウェア設定（Hardware Configuration）]** > **[ネットワーク接続（Network Connectivity）]** をクリックし、[フロー制御送信（Flow Control Send）] をオンにして、フロー制御の一時停止（XOFF）フレームを有効にします。

フロー制御により、接続しているイーサネットポートは、輻輳しているノードがリンク動作をもう一方の端で一時停止できるようにすることによって、輻輳時のトラフィック レートを制御できます。脅威防御ポートで輻輳が生じ（内部スイッチでキューイングリソースが枯渇）、それ以上はトラフィックを受信できなくなった場合、ポーズフレームを送信することによって、その状態が解消されるまで送信を中止するように、そのポートから相手ポートに通知します。ポーズ フレームを受信すると、送信側デバイスはデータ パケットの送信を中止するので、輻輳時のデータ パケット損失が防止されます。

（注） Threat Defense は、リモートピアがトラフィックをレート制御できるように、ポーズフレームの送信をサポートしています。

ただし、ポーズフレームの受信はサポートされていません。

内部スイッチには、それぞれ 250 バイトの 8000 バッファのグローバルプールがあり、スイッチはバッファを各ポートに動的に割り当てます。バッファ使用量がグローバルハイ ウォーターマーク（2 MB（8000 バッファ））を超えると、フロー制御が有効になっているすべてのインターフェイスからポーズフレームが送信されます。また、バッファがポートのハイ ウォーターマーク（.3125 MB（1250 バッファ））を超えると、特定のインターフェイスからポーズフレームが送信されます。ポーズの送信後、バッファ使用量が低ウォーターマークよりも下回ると、XON フレームを送信できます（グローバルでは 1.25MB（5000 バッファ）、ポートごとに 25 MB（1000 バッファ））リンク パートナーは、XON フレームを受信するとトラフィックを再開できます。

802.3x に定義されているフロー制御フレームのみがサポートされています。プライオリティベースのフロー制御はサポートされていません。

ステップ 8 [モード（Mode）] ドロップダウン リストで、次のいずれかを選択します。

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

ステップ 9 [優先度（Priority）] フィールドに、0 ～ 65535 の範囲の数値を入力します。

この値は、ポリシーベースのルーティング構成で使用されます。優先度は、複数の出力インターフェイス間でトラフィックを分散する方法を決定するために使用されます。

ステップ 10 [OK] をクリックします。

ステップ 11 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** 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るようになりました。変更はポリシーを展開するまで有効になりません。

ステップ 12 インターフェイスの構成を続行します。

- 通常のファイアウォール インターフェイス
- インラインセットとパッシブインターフェイス

EtherChannel インターフェイスの設定

ここでは、EtherChannel インターフェイスの設定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。

EtherChannel インターフェイスについて

ここでは、EtherChannel インターフェイスについて説明します。

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には、最大 8 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、ISA 3000 は、16 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。

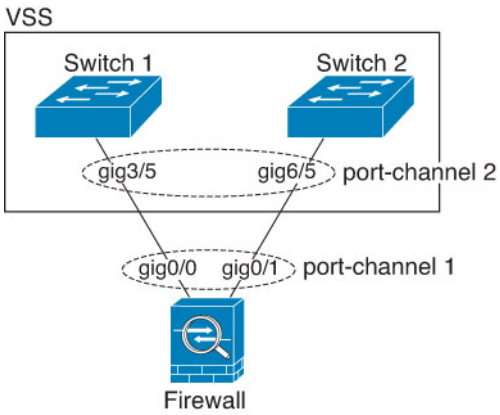
EtherChannel によって、チャネル内の使用可能なすべてのアクティブ インターフェイスのトラフィックが集約されます。インターフェイスは、送信元または宛先 MAC アドレス、IP アドレス、TCP および UDP ポート番号、および VLAN 番号に基づいて、独自のハッシュ アルゴリズムを使用して選択されます。

別のデバイスの EtherChannel への接続

Threat Defense 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 Threat Defense 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。

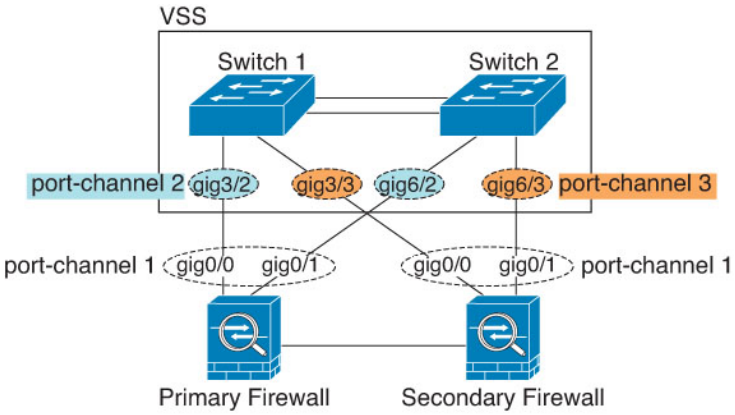
図 *1 : VSS/vPC* への接続



（注） Threat Defense 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 Threat Defense デバイスを配置する場合は、EtherChannel 内で Threat Defense 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。

Threat Defense 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、Threat Defense 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 Threat Defense 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 Threat Defense 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 Threat Defense 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 Threat Defense 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*



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。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

Threat Defense 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 および Secure Firewall 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。

EtherChannel インターフェイスのガイドライン

ブリッジ グループ

ルーテッドモードでは、Management Center 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

- EtherChannel インターフェイスを 高可用性 リンクとして使用する場合、高可用性 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 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高可用性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 が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 Threat Defense Virtual の場合、Management Center で 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。
- 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には、最大 8 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、ISA 3000 は、16 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。
- チャネルグループ内のすべてのインターフェイスは、メディアタイプと速度が同じでなければなりません。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。大容量のインターフェイスで速度を低く設定することでインターフェイス容量（1GB と 10GB のインターフェイスなど）を混在させることはできません。ただし、Cisco Secure Firewall 3100/4200 の場合は、速度が [SFPを検出（Detect SFP）] に設定されている限り、異なるインターフェイス容量をサポートします。この場合、最も低い共通速度が使用されます。
- Threat Defense 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。
- Threat Defense 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、Threat Defense 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。
- Firepower 4100/9300 以外のモデルでは、LACP レートが通常（低速）に設定されており、変更できません。つまり、デバイスは、接続するスイッチに常に低速レートを要求します。デバイスは、接続するスイッチによって要求されるレート（低速または高速）を使用するため、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することをお勧めします。FXOS で EtherChannel を設定する Firepower 4100/9300 の場合、LACP レートはデフォルトで高速に設定されますが、低速に変更できます。FXOS で設定した値と一致するようにスイッチを設定することをお勧めします。

- 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 Threat Defense 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、Threat Defense 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 Threat Defense 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 の設定

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 8 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、ISA 3000 は、16 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。
- チャネルグループ内のすべてのインターフェイスは、メディアタイプと速度が同じでなければなりません。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。大容量のインターフェイスで速度を低く設定することでインターフェイス容量（1GB と 10GB のインターフェイスなど）を混在させることはできません。ただし、Cisco Secure Firewall 3100/4200 の場合は、速度が [SFPを検出（Detect SFP）] に設定されている限り、異なるインターフェイス容量をサポートします。この場合、最も低い共通速度が使用されます。

（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。

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

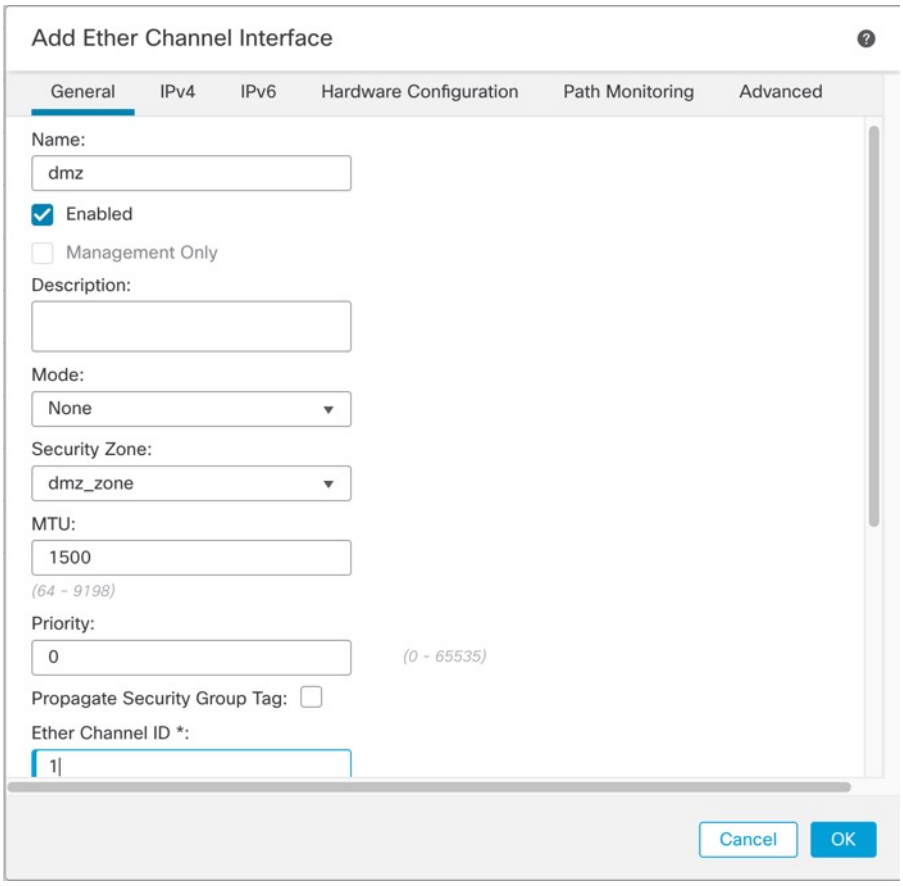
ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Threat Defense デバイス**[編集（Edit）]**（✎）をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

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 （9 ページ）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（Firepower 1010 の場合は 1 ～ 8）の数値に設定します。

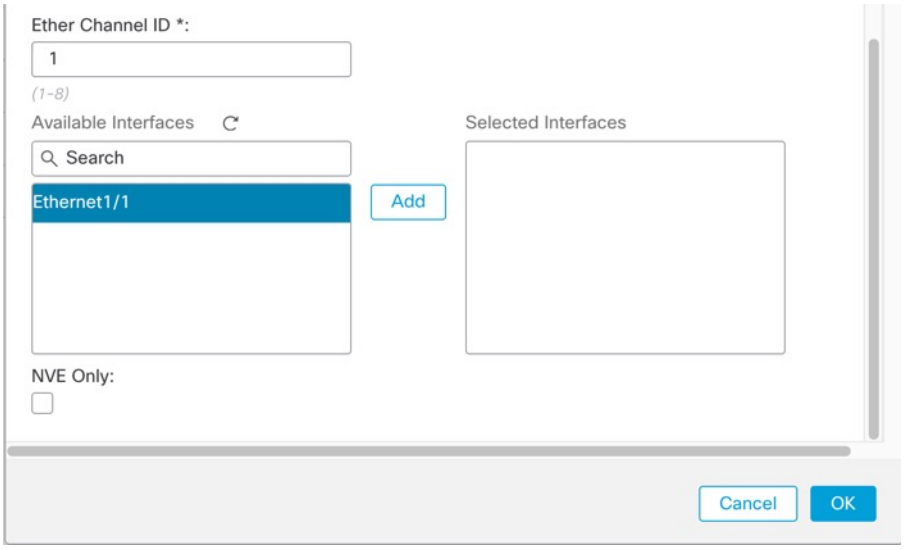
図 *3 : EtherChannel* インターフェイスの追加



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。

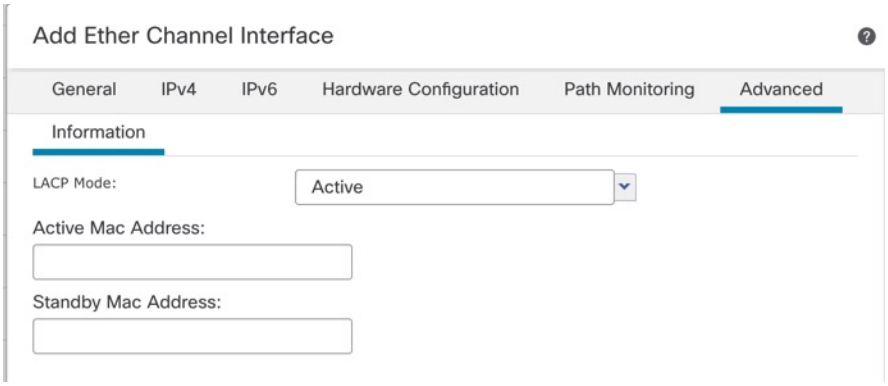
すべてのインターフェイスのタイプと速度が同じになるようにします。

図 *4 : Available Interfaces*



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。

図 *5 :* 作成する *Advanced*



- （ISA 3000 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、Threat Defense 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 （15 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。

- （ISA 3000 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 [ハードウェア構成（Hardware Configuration）] タブをクリックし、すべてのメンバーインターフェイスのデュプレックスと速度を設定します。

ステップ 8 [OK] をクリックします。

ステップ 9 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** 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るようになりました。変更はポリシーを展開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またはブリッジ グループ インターフェイスの設定を参照してください。

Management Center とのインターフェイスの変更の同期

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

- デバイスから送信されたイベント
- Management Center からの展開の同期

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

Management Center の外部で実行されるインターフェイスの変更には、同期が必要な 2 つのタイプがあります。

- 物理インターフェイスの追加または削除：新しいインターフェイスを追加したり、未使用のインターフェイスを削除したりしても、Threat Defense の設定に対する影響は最小限で

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

Management Center が変更を検出すると、[インターフェイス（Interface）] ページの各インターフェイスの左側にステータス（[削除済み（removed）]、[変更済み（changed）]、または [追加済み（added）]）が表示されます。

- Management Center アクセスインターフェイスの変更：**configure network management-data-interface** コマンドを使用して Management Center を管理するためのデータインターフェイスを設定する場合は、Management Center で一致する設定変更を手動で行ってから変更を確認する必要があります。これらのインターフェイスの変更を自動で行うことはできません。

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

始める前に

- ユーザの役割：
  - 管理者
  - アクセス管理者
  - ネットワーク管理者

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Threat Defense デバイス**[編集（Edit）]**（✎） 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。

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

ステップ 3 変更が検出されたら、次の手順を参照してください。

物理インターフェイスの追加または削除

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

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

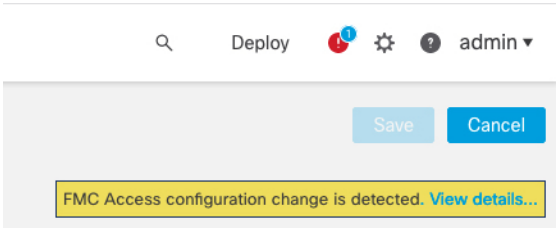
エラーがある場合は、ポリシーを変更して検証に戻る必要があります。

c) **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** 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るようになりました。

FMC アクセスインターフェイスの変更

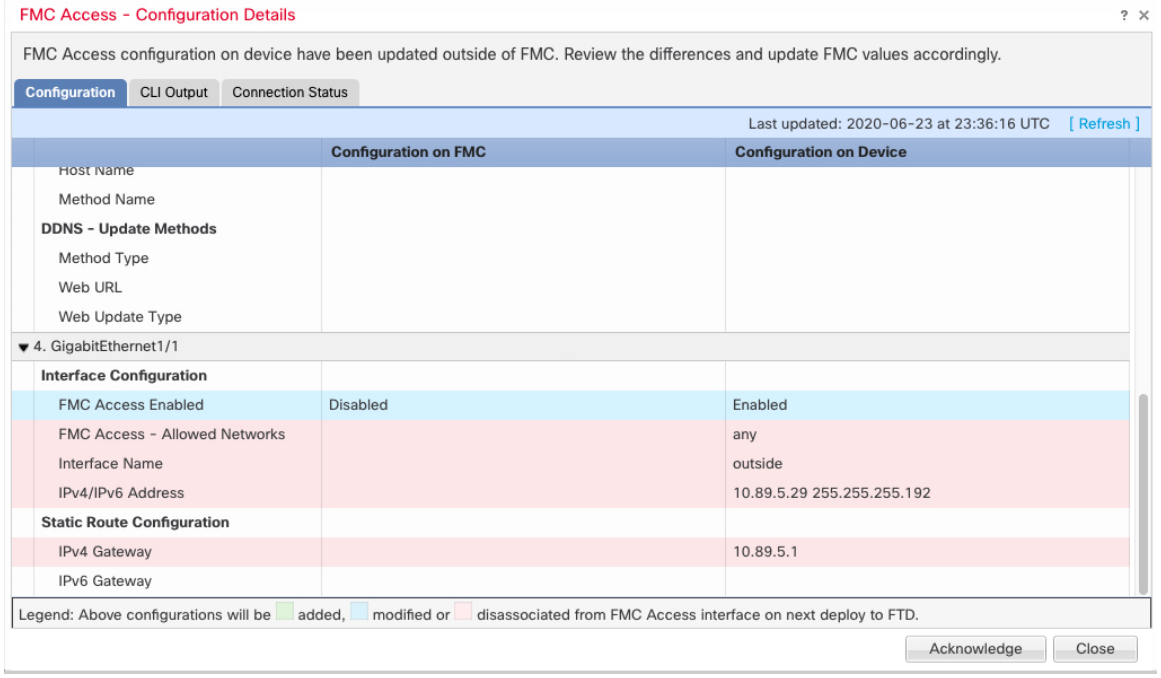
a) Management Center のアクセス設定が変更されたことを示す黄色のバナーが [デバイス（Device）] ページの右上に表示されます。[詳細を表示（View details）] リンクをクリックしてインターフェイスの変更内容を表示します。



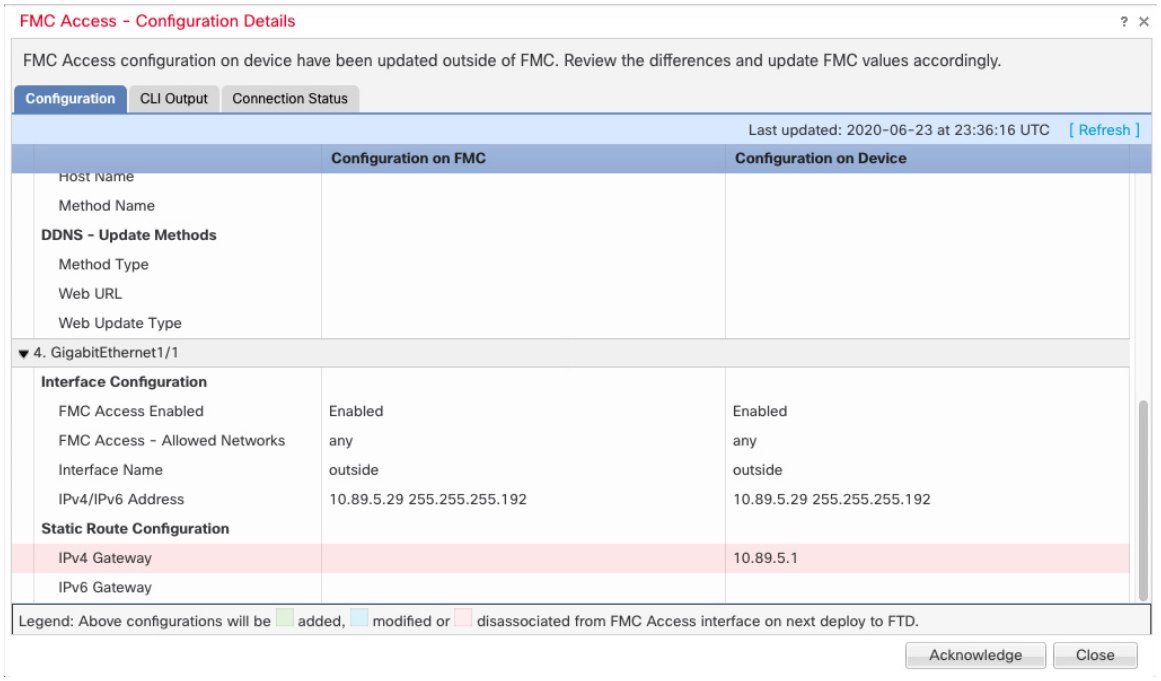
[FMCアクセス-設定の詳細（FMC Access - Configuration Details）] ダイアログボックスが開きます。

b) 強調表示されているすべての設定、特にピンクで強調表示されている設定に注意してください。Management Center で値を手動で設定し、Threat Defense で値を一致させる必要があります。

たとえば、以下のピンク色のハイライトは、Threat Defense に存在するものの、Management Center にはまだ存在しない設定を示しています。



Management Center でインターフェイスを設定した後のこのページの例を以下に示します。インターフェイス設定が一致し、ピンクのハイライトが消えています。



c) [確認（Acknowledge）] をクリックします。

Management Center の設定が完了して展開の準備ができるまで、[確認（Acknowledge）] をクリックしないことをお勧めします。[確認（Acknowledge）] をクリックすると、展開時にブロックが削除されます。Management Center 設定は、次回展開時に Threat Defense の残

りの競合する設定を上書きします。再展開の前に Management Center の設定を手動で修正する必要があります。

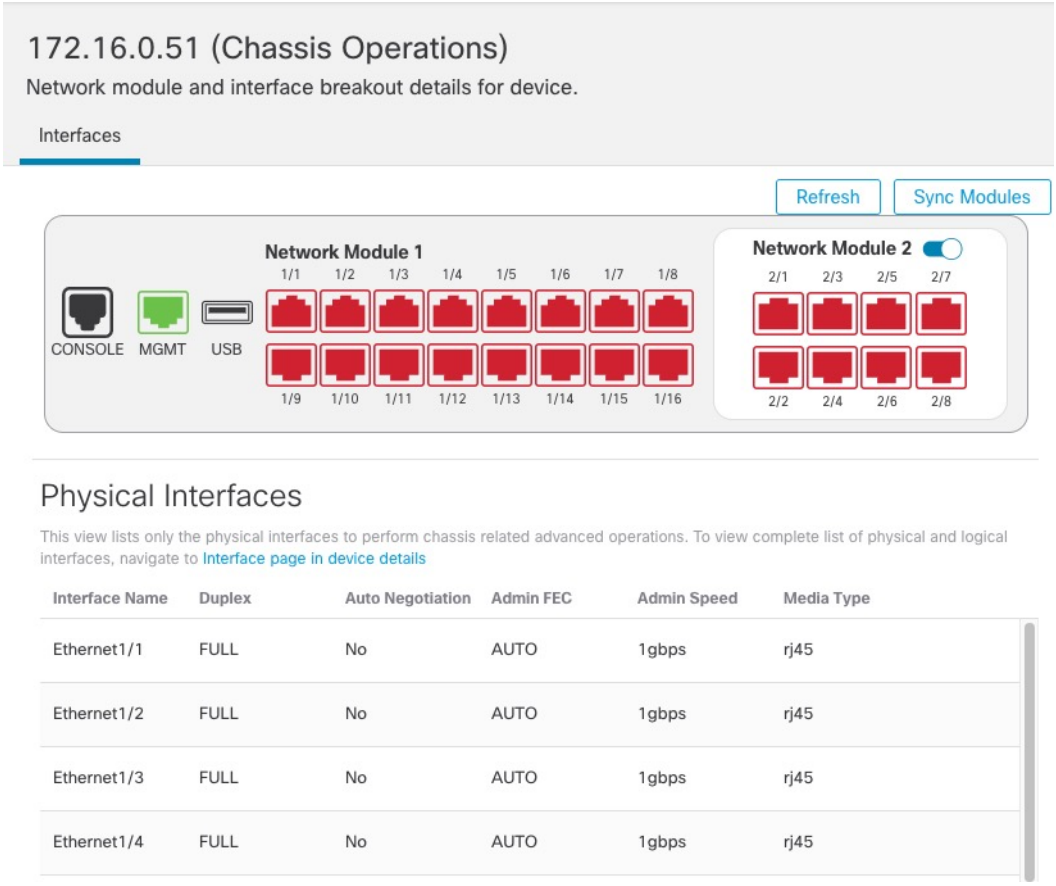
d) これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。

Cisco Secure Firewall 3100/4200 のネットワークモジュールの管理

最初にデバイスの電源をオンにする前にネットワークモジュールをインストールした場合、アクションは不要です。ネットワークモジュールは有効になり、使用できる状態になっています。

デバイスの物理インターフェイスの詳細を表示してネットワークモジュールを管理するには、[シャーシの操作（Chassis Operations）] ページを開きます。[デバイス（Devices）] の [デバイス管理（Device Management）] で、[シャーシ（Chassis）] 列の [管理（Manage）] をクリックします。 > クラスタリングまたは高可用性の場合、このオプションは制御ノード/アクティブユニットでのみ使用できます。デバイスの [シャーシの操作（Chassis Operatio）] ページが開きます。

図 *6 :* シャーシの操作



[更新（Refresh）]をクリックして、インターフェイスのステータスを更新します。検出する必要があるデバイスでハードウェアの変更を行った場合は、[モジュールを同期（Sync Modules）]をクリックします。

初回ブートアップ後にネットワークモジュールのインストールを変更する必要がある場合は、次の手順を参照してください。

ブレークアウトポートの設定

40GB 以上のインターフェイスごとに 10GB のブレークアウトポートを設定できます。この手順では、ポートの分割と再参加の方法について説明します。ブレークアウトポートは、EtherChannel への追加を含め、他の物理イーサネットポートと同じように使用できます。

変更はすぐに反映され、デバイスに展開する必要はありません。中断または再参加した後は、以前のインターフェイス状態にロールバックできません。

始める前に

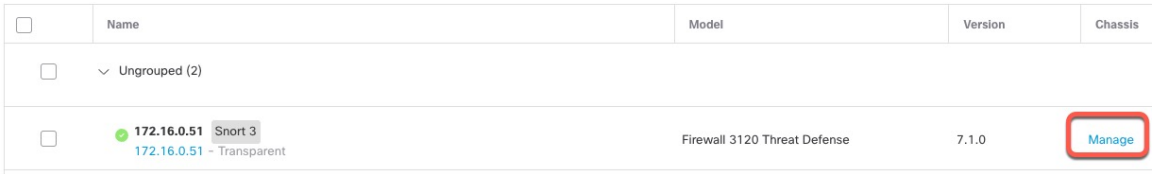
- サポートされているブレークアウトケーブルを使用する必要があります。詳細については、ハードウェア設置ガイドを参照してください。

- 中断または再参加する前に、インターフェイスを次の目的で使用することはできません。
  - フェールオーバー リンク
  - クラスタ制御リンク
  - サブインターフェイスを設定する
  - EtherChannel メンバー
  - BVI メンバー
  - マネージャ アクセス インターフェイス
- セキュリティポリシーで直接使用されているインターフェイスの中断または再参加は、構成に影響を与える可能性がありますが、アクションはブロックされません。

手順

ステップ 1 [デバイス（Devices）] の [デバイス管理（Device Management）] で、[シャーシ（Chassis）] 列の [管理（Manage）] をクリックします。 > クラスタリングまたは高可用性の場合、このオプションは制御ノード/アクティブユニットでのみ使用できます。ネットワークモジュールの変更はすべてのノードに複製されます。

図 7: シャーシの管理



デバイスの [シャーシの操作（Chassis Operations）] ページが開きます（マルチインスタンスモードでは、このページは [シャーシマネージャ（Chassis Manager）] と呼ばれます）。このページには、デバイスの物理インターフェイスの詳細が表示されます。

ステップ 2 40GB 以上のインターフェイスから 10GB ポートを分割します。

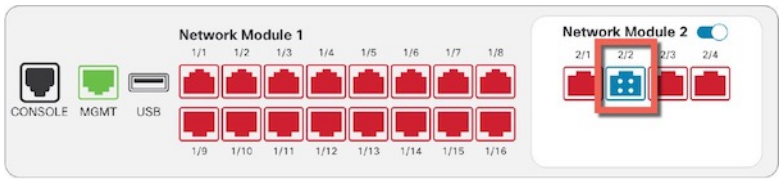
a) インターフェイスの右側の [ブレイク（Break）]（ ）をクリックします。

確認ダイアログボックスで [Yes] をクリックします。インターフェイスが使用中の場合は、エラーメッセージが表示されます。分割を再試行する前に、ユースケースを解決する必要があります。

たとえば、Ethernet2/1 40GB インターフェイスを分割する場合、分割後の子インターフェイスは、Ethernet2/1/1、Ethernet2/1/2、Ethernet2/1/3、および Ethernet2/1/4 として識別されます。

インターフェイスのグラフィックでは、分割されたポートの表示は次のようになります。

図 *8* : ブレークアウト ポート



b) 画面上部のメッセージ内のリンクをクリックして [インターフェイス（Interfaces）] ページに移動し、インターフェイスの変更を保存します。

図 *9* : *[インターフェイス（Interface）]* ページへの移動

c) [インターフェイス（Interfaces）] ページの上部で、[クリックして詳細を表示（Click to know more）] をクリックします。[インターフェイスの変更（Interface Changes）] ダイアログボックスが開きます。

図 *10* : インターフェイスの変更の表示

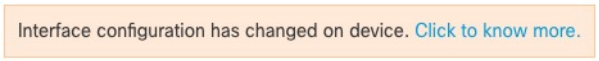
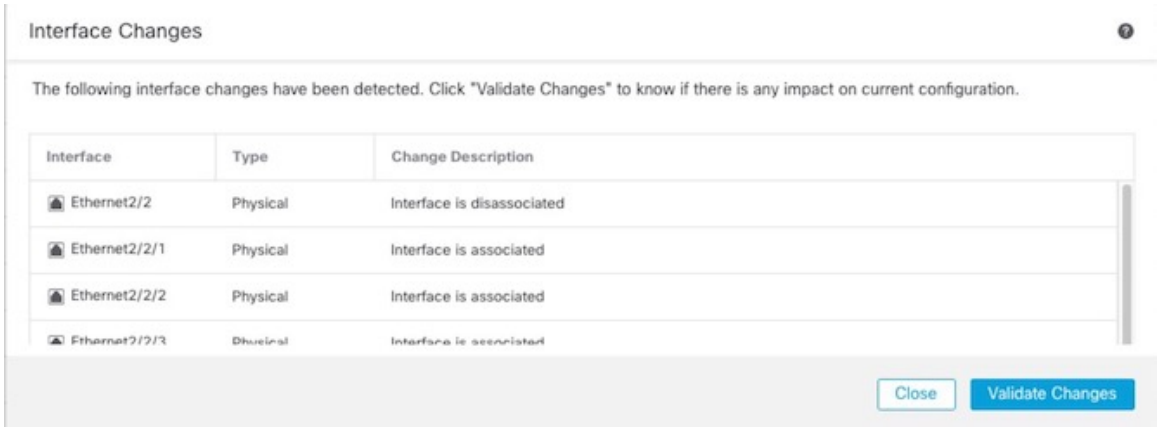


図 *11* : インターフェイスの変更



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

エラーがある場合は、ポリシーを変更して検証に戻る必要があります。

セキュリティポリシーで使用されている親インターフェイスを置き換えると、設定に影響を与える場合があります。インターフェイスは、アクセスルール、NAT、SSL、アイデンティティルール、VPN、DHCP サーバーなど、設定における多くの場所で直接参照されている可能性があります。インターフェイスを削除すると、そのインターフェイスに関連付けられている設定がすべて削除されます。セキュリティゾーンを参照するポリシーは影響を受けません。

e) [閉じる（Close）] をクリックして [インターフェイス（Interfaces）] ページに戻ります。
f) [保存（Save）] をクリックしてインターフェイスの変更をファイアウォールに保存します。
g) 構成を変更する必要があった場合は、**[展開（Deploy）]** > **[展開（Deployment）]** に移動してポリシーを展開します。

ブレークアウトポートの変更を保存するためだけに展開する必要はありません。

ステップ 3 ブレークアウトポートを再結合します。

インターフェイスのすべての子ポートを再結合する必要があります。

a) インターフェイスの右側の [参加（Join）] （ ） をクリックします。

確認ダイアログボックスで [Yes] をクリックします。子ポートが使用中の場合は、エラーメッセージが表示されます。再参加を再試行する前に、ユースケースを解決する必要があります。

b) 画面上部のメッセージ内のリンクをクリックして [インターフェイス（Interfaces）] ページに移動し、インターフェイスの変更を保存します。

図 *12* : [インターフェイス（*Interface*）] ページへの移動

c) [インターフェイス（Interfaces）] ページの上部で、[クリックして詳細を表示（Click to know more）] をクリックします。[インターフェイスの変更（Interface Changes）] ダイアログボックスが開きます。

図 *13* : インターフェイスの変更の表示

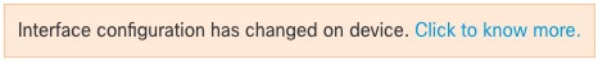
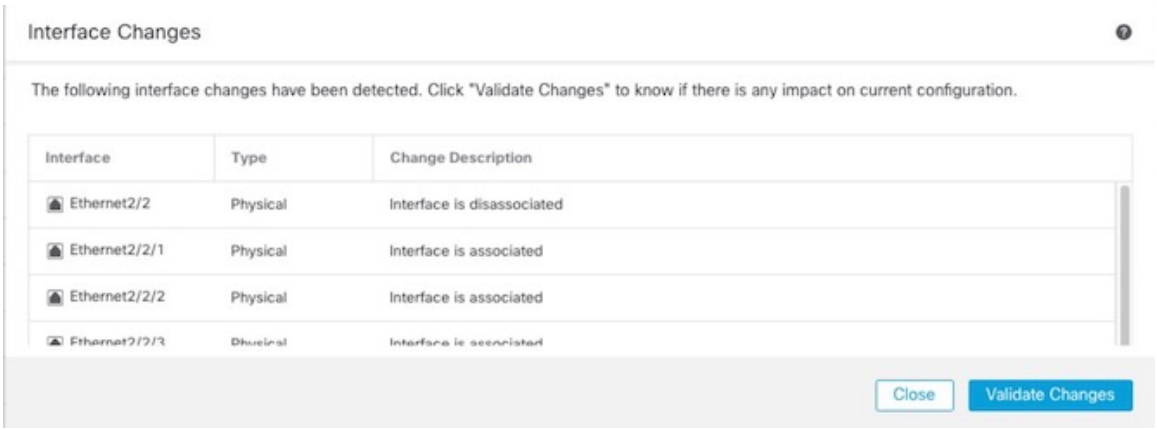


図 *14* : インターフェイスの変更



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

エラーがある場合は、ポリシーを変更して検証に戻る必要があります。

セキュリティポリシーで使用されている子インターフェイスを置き換えると、構成に影響を与える可能性があります。インターフェイスは、アクセスルール、NAT、SSL、アイデンティティルール、VPN、DHCP サーバーなど、設定における多くの場所で直接参照されている可能性があります。インターフェイスを削除すると、そのインターフェイスに関連付けられている設定がすべて削除されます。セキュリティゾーンを参照するポリシーは影響を受けません。

e) [閉じる（Close）] をクリックして [インターフェイス（Interfaces）] ページに戻ります。
f) [保存（Save）] をクリックしてインターフェイスの変更をファイアウォールに保存します。
g) 構成を変更する必要があった場合は、**[展開（Deploy）]** > **[展開（Deployment）]** に移動してポリシーを展開します。

ブレークアウトポートの変更を保存するためだけに展開する必要はありません。

ネットワークモジュールの追加

初回起動後にファイアウォールにネットワークモジュールを追加するには、次の手順を実行します。新しいモジュールを追加するには、再起動が必要です。

手順

ステップ 1 ハードウェア設置ガイドに従ってネットワークモジュールをインストールします。

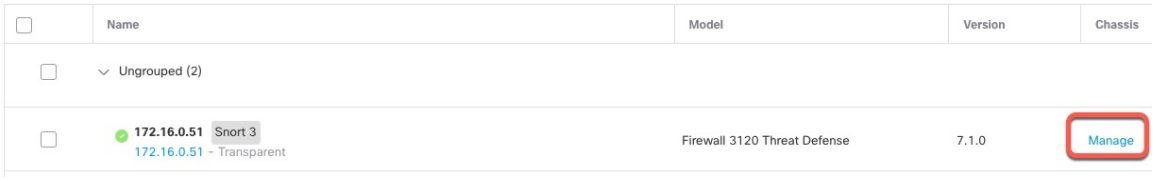
クラスタリングまたは高可用性の場合は、すべてのノードにネットワークモジュールをインストールします。

ステップ 2 ファイアウォールを再起動します。デバイスのシャットダウンまたは再起動を参照してください。

クラスタリングまたは高可用性の場合は、最初にデータノード/スタンバイユニットを再起動し、それらが復旧するのを待ちます。その後、制御ノード（制御ノードの変更を参照）またはアクティブユニット（Threat Defense ハイアベイラビリティペアにおけるアクティブピアの切り替えを参照）を変更し、以前の制御ノードまたはアクティブユニットを再起動できます。

ステップ 3 [デバイス（Devices）] の [デバイス管理（Device Management）] で、[シャーシ（Chassis）] 列の [管理（Manage）] をクリックします。 > クラスタリングまたは高可用性の場合、このオプションは制御ノード/アクティブユニットでのみ使用できます。ネットワークモジュールの変更はすべてのノードに複製されます。

図 *15 :* シャーシの管理

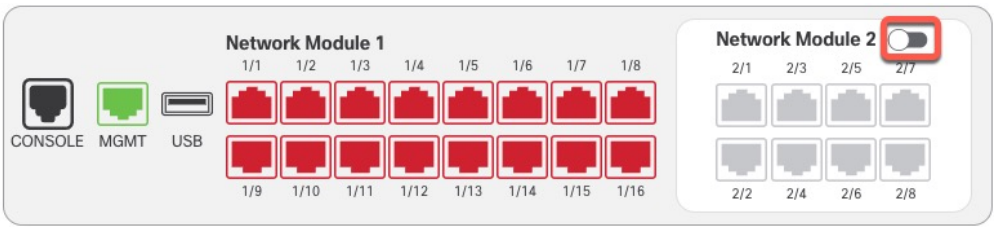


デバイスの [シャーシの操作（Chassis Operatio）] ページが開きます。このページには、デバイスの物理インターフェイスの詳細が表示されます。

ステップ 4 [モジュールの同期（Sync Modules）] をクリックして、ネットワークモジュールの新しい詳細情報でページを更新します。

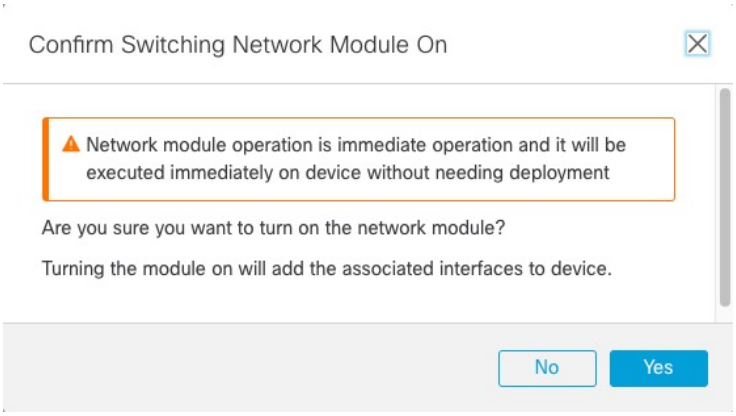
ステップ 5 インターフェイスのグラフィックで、スライダ （ ） をクリックしてネットワークモジュールを有効にします。

図 *16 :* ネットワークモジュールの有効化



ステップ 6 ネットワークモジュールの有効化を確認するプロンプトが表示されます。[Yes] をクリックします。

図 *17 :* 有効化の確認



ステップ 7 画面の上部にメッセージが表示されます。リンクをクリックして [インターフェイス（Interfaces）] ページに移動し、インターフェイスの変更を保存します。

図 *18* : [インターフェイス（*Interface*）] ページへの移動

ステップ 8 （任意）[インターフェイス（Interfaces）] ページの上部に、インターフェイスの設定が変更されたことを示すメッセージが表示されます。[クリックして詳細を表示（Click to know more）] をクリックすると、[インターフェイスの変更（Interface Changes）] ダイアログボックスが開き、変更が表示されます。

図 *19* : インターフェイスの変更の表示

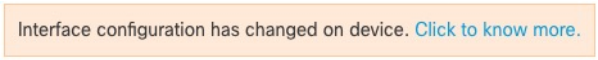
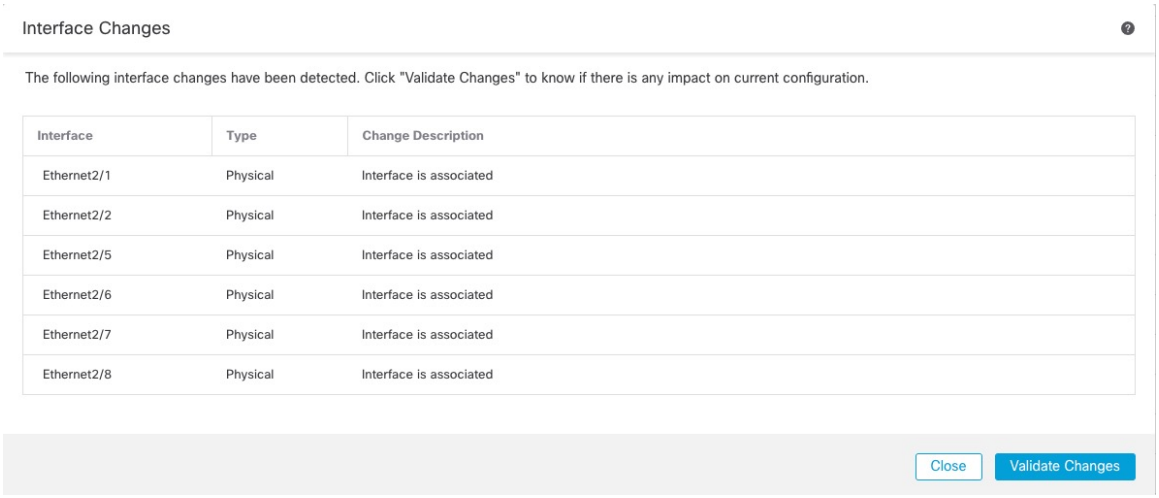


図 *20* : インターフェイスの変更



[閉じる（Close）] をクリックして [インターフェイス（Interfaces）] ページに戻ります（新しいモジュールを追加しているので、設定への影響はないため、[変更の検証（Validate Changes）] をクリックする必要はありません）。

ステップ 9 [保存（Save）] をクリックしてインターフェイスの変更をファイアウォールに保存します。

ネットワークモジュールの交換方法

再起動することなく、同じタイプの新しいモジュールのネットワークモジュールをホットスワップできます。ただし、現在のモジュールを安全に取り外すには、シャットダウンする必要があります。この手順では、古いモジュールをシャットダウンし、新しいモジュールをインストールして有効にする方法について説明します。

クラスタリングまたは高可用性の場合、制御ノード/アクティブユニットでのみシャーシの操作を実行できます。クラスタ制御リンク/フェールオーバーリンクがモジュール上にある場合は、ネットワークモジュールを無効化できません。

始める前に

手順

ステップ 1 クラスタリングまたは高可用性の場合は、次の手順を実行します。

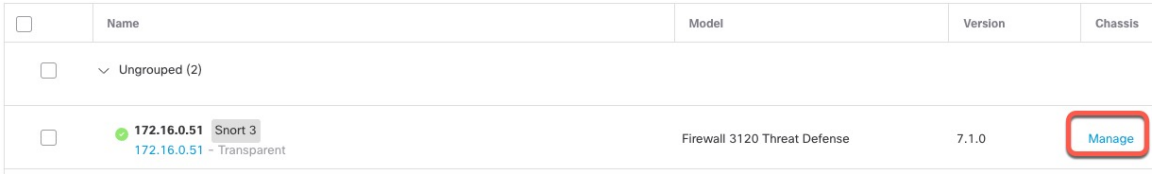
- **クラスタリング**：ホットスワップを実行するユニットがデータノードであることを確認します（制御ノードの変更を参照）。次に、そのノードを分断して、クラスタリングから外します。ノードの除外を参照してください。

  ホットスワップを実行後、ノードをクラスタに追加し直します。または、制御ノードですべての操作を実行できます。ネットワークモジュールの変更はすべてのデータノードに同期されます。ただし、ホットスワップ中は、すべてのノードでインターフェイスが使用できなくなります。

- **高可用性**：ネットワークモジュールを無効にするときにフェールオーバーを回避するには、次の手順を実行します。
  - フェールオーバーリンクがネットワークモジュール上にある場合は、高可用性を分断する必要があります。高可用性ペアの解除を参照してください。アクティブなフェールオーバーリンクがあるネットワークモジュールを無効化することはできません。
  - ネットワークモジュールのインターフェイスのインターフェイスモニタリングを無効にします。スタンバイ IP アドレスとインターフェイス モニタリングの設定を参照してください。

ステップ 2 [デバイス（Devices）] の [デバイス管理（Device Management）] で、[シャーシ（Chassis）] 列の [管理（Manage）] をクリックします。 > クラスタリングまたは高可用性の場合、このオプションは制御ノード/アクティブユニットでのみ使用できます。ネットワークモジュールの変更はすべてのノードに複製されます。

図 *21 :* シャーシの管理



デバイスの [シャーシの操作（Chassis Operatio）] ページが開きます。このページには、デバイスの物理インターフェイスの詳細が表示されます。

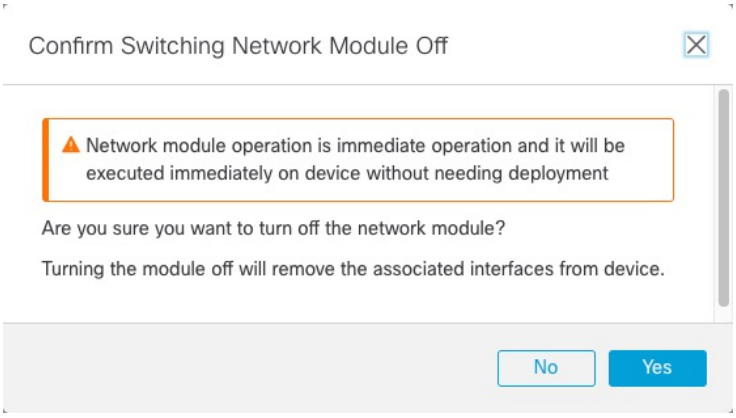
ステップ 3 インターフェイスのグラフィックで、スライダ（ ）をクリックしてネットワークモジュールを無効にします。

図 *22 :* ネットワークモジュールの無効化

[インターフェイス（Interfaces）] ページでは変更を保存しないでください。ネットワークモジュールを交換するため、既存の構成を中断する必要はありません。

ステップ 4 ネットワークモジュールの無効化を確認するプロンプトが表示されます。[Yes] をクリックします。

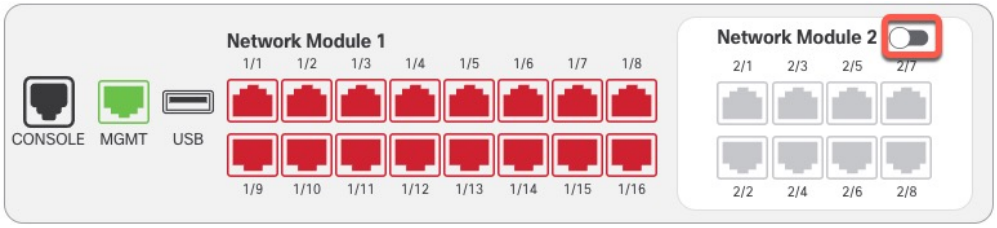
図 *23 :* 無効化の確認



ステップ 5 ハードウェア設置ガイドに従って、デバイスの古いネットワークモジュールを取り外し、新しいネットワークモジュールと交換します。

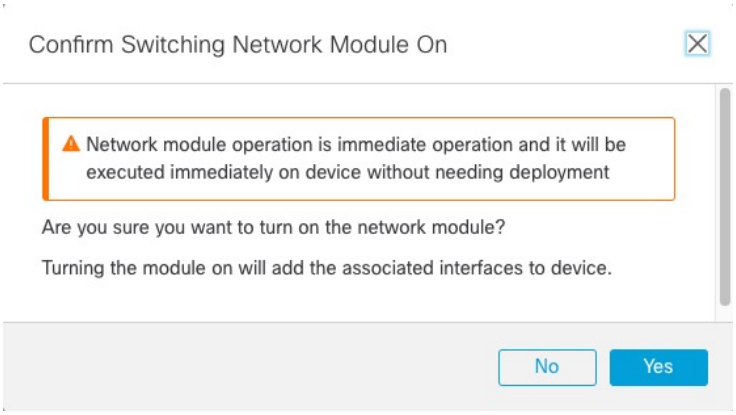
ステップ 6 Management Center で、スライダ （  ） をクリックして新しいモジュールを有効にします。

図 *24 :* ネットワークモジュールの有効化



ステップ 7 ネットワークモジュールの有効化を確認するプロンプトが表示されます。[Yes] をクリックします。

図 *25 :* 有効化の確認



ステップ 8 クラスタリングまたは高可用性の場合は、次の手順を実行します。

- **クラスタリング**：ノードをクラスタに追加して戻します。新しいクラスタノードの追加を参照してください。
- **高可用性**：
  - 高可用性を解除した場合は、高可用性を再構築します。ハイ アベイラビリティ ペアの追加を参照してください。
  - ネットワークモジュールのインターフェイスのインターフェイスモニタリングを再度有効にします。スタンバイ IP アドレスとインターフェイス モニタリングの設定 を参照してください。

ネットワークモジュールを別のタイプに交換する

ネットワークモジュールを別のタイプに交換する場合は、再起動が必要です。新しいモジュールのインターフェイス数が古いモジュールよりも少ない場合は、存在しなくなるインターフェイスに関連する構成を手動で削除する必要があります。

クラスタリングまたは高可用性の場合、制御ノード/アクティブユニットでのみシャーシの操作を実行できます。

始める前に

ハイアベイラビリティの場合、フェールオーバーリンクがモジュール上にあると、ネットワークモジュールを無効化できません。高可用性を解除する必要があります（高可用性ペアの解除を参照）。これにより、アクティブユニットの再起動時にダウンタイムが発生するようになります。ユニットの再起動が完了したら、高可用性を再編成できます。

手順

ステップ 1 クラスタリングまたは高可用性の場合は、次の手順を実行します。

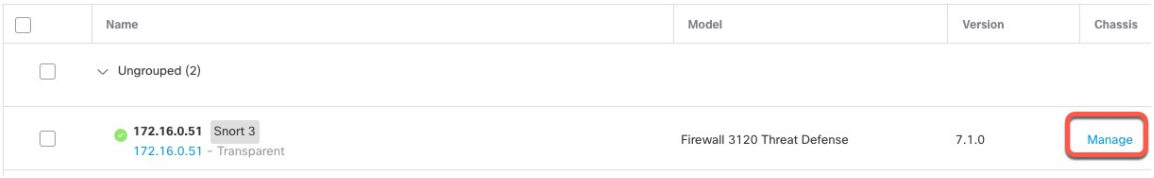
- **クラスタリング**：ネットワークモジュールを交換している間、ダウンタイムを回避するために、各ノードを一度に1つずつ分断し、クラスタから排除することができます。ノードの除外を参照してください。

  交換が完了したら、ノードをクラスタに戻します。

- **高可用性**：ネットワークモジュールを交換している間、フェールオーバーを回避するために、ネットワークモジュール上のインターフェイスのインターフェイスモニタリングを無効にします。スタンバイ IP アドレスとインターフェイス モニタリングの設定を参照してください。

ステップ 2 [デバイス（Devices）] の [デバイス管理（Device Management）] で、[シャーシ（Chassis）] 列の [管理（Manage）] をクリックします。＞クラスタリングまたは高可用性の場合、このオプションは制御ノード/アクティブユニットでのみ使用できます。ネットワークモジュールの変更はすべてのノードに複製されます。

図 *26* : シャーシの管理



デバイスの [シャーシの操作（Chassis Operatio）] ページが開きます。このページには、デバイスの物理インターフェイスの詳細が表示されます。

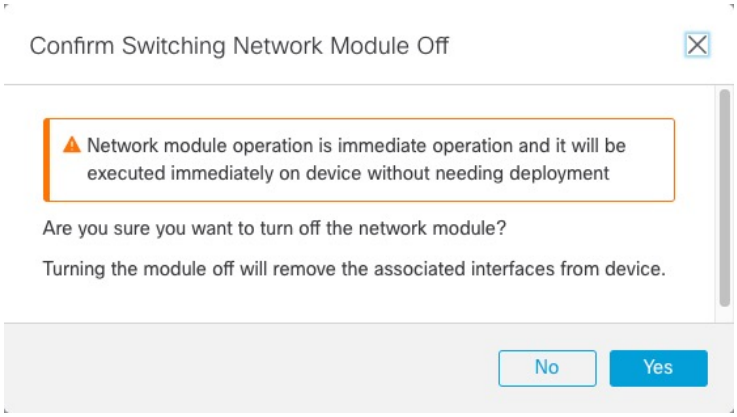
ステップ 3 インターフェイスのグラフィックで、スライダ（）をクリックしてネットワークモジュールを無効にします。

図 *27* : ネットワークモジュールの無効化

[インターフェイス（Interfaces）] ページでは変更を保存しないでください。ネットワークモジュールを交換するため、既存の構成を中断する必要はありません。

ステップ 4 ネットワークモジュールの無効化を確認するプロンプトが表示されます。[Yes] をクリックします。

図 *28* : 無効化の確認



ステップ 5 ハードウェア設置ガイドに従って、デバイスの古いネットワークモジュールを取り外し、新しいネットワークモジュールと交換します。

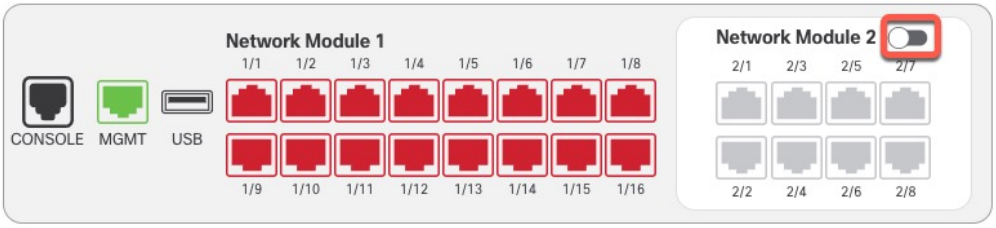
ステップ 6 ファイアウォールを再起動します。デバイスのシャットダウンまたは再起動を参照してください。

クラスタリングまたは高可用性の場合は、最初にデータノード/スタンバイユニットを再起動し、それらが復旧するのを待ちます。その後、制御ノード（制御ノードの変更を参照）またはアクティブユニット（Threat Defense ハイアベイラビリティペアにおけるアクティブピアの切り替えを参照）を変更し、以前の制御ノードまたはアクティブユニットを再起動できます。

ステップ 7 Management Center で、[モジュールの同期（Sync Modules）] をクリックして、ネットワークモジュールの新しい詳細情報でページを更新します。

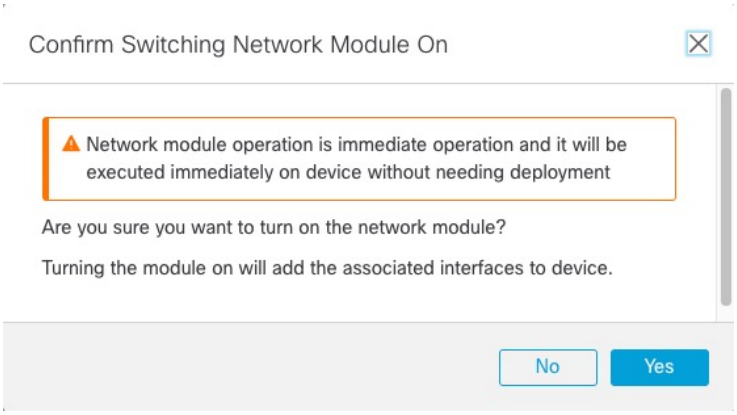
ステップ 8 スライダ （ ） をクリックして新しいモジュールを有効にします。

図 *29* : ネットワークモジュールの有効化



ステップ 9 ネットワークモジュールの有効化を確認するプロンプトが表示されます。[Yes] をクリックします。

図 *30* : 有効化の確認



ステップ 10 画面上部のメッセージ内のリンクをクリックして[インターフェイス（Interfaces）]ページに移動し、インターフェイスの変更を保存します。

図 *31* : *[インターフェイス（**Interface**）]* ページへの移動

ステップ 11 ネットワークモジュールのインターフェイス数が減少した場合：

a) [インターフェイス（Interfaces）]ページの上部で、[クリックして詳細を表示（Click to know more）]をクリックします。[インターフェイスの変更（Interface Changes）]ダイアログボックスが開きます。

図 *32* : インターフェイスの変更の表示

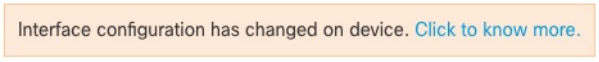
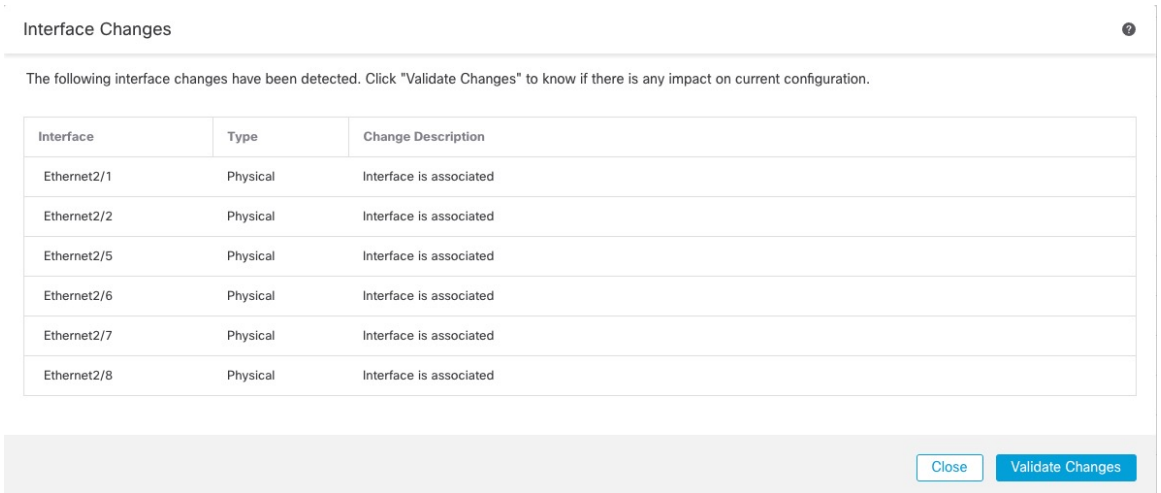


図 *33* : インターフェイスの変更



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

エラーがある場合は、ポリシーを変更して検証に戻る必要があります。

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、設定に影響を与える場合があります。インターフェイスは、アクセスルール、NAT、SSL、アイデンティティルール、VPN、DHCP サーバーなど、設定における多くの場所で直接参照されている可能性があります。インターフェイスを削除すると、そのインターフェイスに関連付けられている設定がすべて削除されます。セキュリティゾーンを参照するポリシーは影響を受けません。

c) [閉じる（Close）] をクリックして [インターフェイス（Interfaces）] ページに戻ります。

ステップ 12 インターフェイス速度を変更するには、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 （9 ページ）を参照してください。

デフォルトの速度は、[SFPを検出（Detect SFP）] に設定されています。これにより、取り付けられている SFP から適切な速度が検出されます。速度を手動で特定の値に設定しており、その速度の変更が必要になった場合にのみ、速度を修正する必要があります。

ステップ 13 [保存（Save）] をクリックしてインターフェイスの変更をファイアウォールに保存します。

ステップ 14 構成を変更する必要があった場合は、**[展開（Deploy）] > [展開（Deployment）]** に移動してポリシーを展開します。

ネットワークモジュールの変更を保存するためだけに展開する必要はありません。

ステップ 15 クラスタリングまたは高可用性の場合は、次の手順を実行します。

- **クラスタリング**：ノードをクラスタに追加して戻します。新しいクラスタノードの追加を参照してください。
- **高可用性**：ネットワークモジュールのインターフェイスのインターフェイスモニタリングを再度有効にします。スタンバイ IP アドレスとインターフェイス モニタリングの設定 を参照してください。

ネットワーク モジュールの取り外し

ネットワークモジュールを完全に削除する場合は、次の手順に従います。ネットワークモジュールを削除するには、再起動が必要です。

クラスタリングまたは高可用性の場合、制御ノード/アクティブユニットでのみシャーシの操作を実行できます。

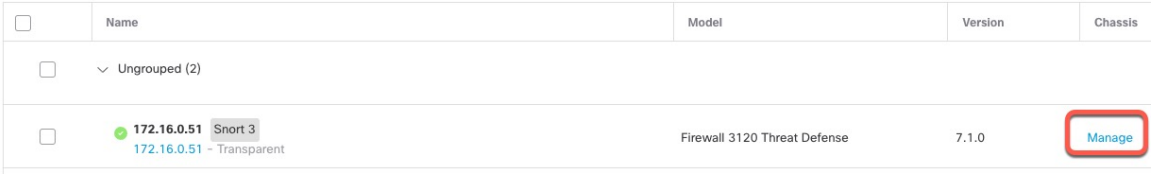
始める前に

クラスタリングまたは高可用性の場合は、クラスタ/フェールオーバーリンクがネットワークモジュール上にないことを確認してください。

手順

ステップ 1 [デバイス（Devices）] の [デバイス管理（Device Management）] で、[シャーシ（Chassis）] 列の [管理（Manage）] をクリックします。 > クラスタリングまたは高可用性の場合、このオプションは制御ノード/アクティブユニットでのみ使用できます。ネットワークモジュールの変更はすべてのノードに複製されます。

図 *34* : シャーシの管理



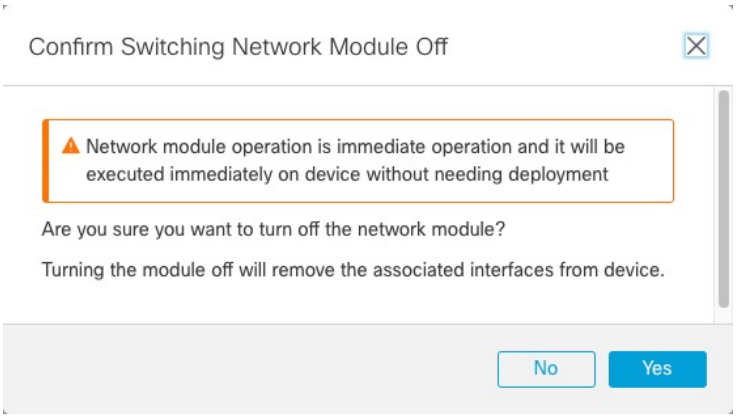
デバイスの [シャーシの操作（Chassis Operatio）] ページが開きます。このページには、デバイスの物理インターフェイスの詳細が表示されます。

ステップ 2 インターフェイスのグラフィックで、スライダ（）をクリックしてネットワークモジュールを無効にします。

図 *35* : ネットワークモジュールの無効化

ステップ 3 ネットワークモジュールの無効化を確認するプロンプトが表示されます。[Yes] をクリックします。

図 *36* : 無効化の確認

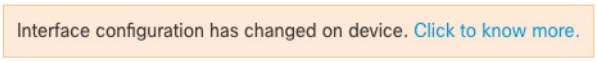


ステップ 4 画面の上部にメッセージが表示されます。リンクをクリックして [インターフェイス（Interfaces）] ページに移動し、インターフェイスの変更を保存します。

図 *37 : [インターフェイス（Interface）] ページへの移動*

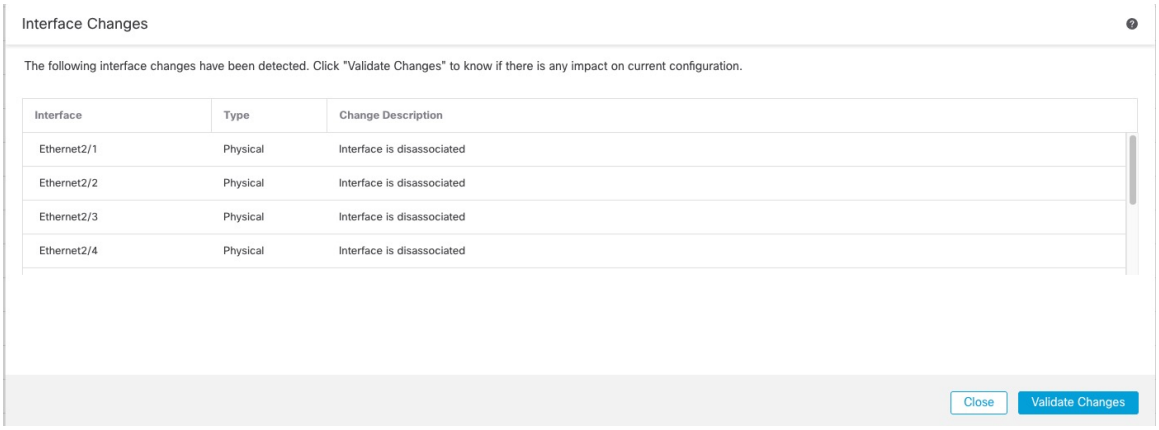
ステップ 5 [インターフェイス（Interfaces）] ページの上部に、インターフェイスの設定が変更されたことを示すメッセージが表示されます。

図 *38 :* インターフェイスの変更の表示



a) [クリックして詳細を表示（Click to know more）] をクリックします。[インターフェイスの変更（Interface Changes）] ダイアログボックスが開き、変更が表示されます。

図 *39 :* インターフェイスの変更



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

エラーがある場合は、ポリシーを変更して検証に戻る必要があります。

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、設定に影響を与える場合があります。インターフェイスは、アクセスルール、NAT、SSL、アイデンティティルール、VPN、DHCP サーバーなど、設定における多くの場所で直接参照されている可能性があります。インターフェイスを削除すると、そのインターフェイスに関連付けられている設定がすべて削除されます。セキュリティゾーンを参照するポリシーは影響を受けません。

c) [閉じる（Close）] をクリックして [インターフェイス（Interfaces）] ページに戻ります。

ステップ 6 [保存（Save）] をクリックしてインターフェイスの変更をファイアウォールに保存します。

ステップ 7 構成を変更する必要があった場合は、**[展開（Deploy）] > [展開（Deployment）]** に移動してポリシーを展開します。

ステップ 8 ファイアウォールを再起動します。デバイスのシャットダウンまたは再起動を参照してください。

クラスタリングまたは高可用性の場合は、最初にデータノード/スタンバイユニットを再起動し、それらが復旧するのを待ちます。その後、制御ノード（制御ノードの変更を参照）またはアクティブユニット（Threat Defense ハイアベイラビリティペアにおけるアクティブピアの切り替えを参照）を変更し、以前の制御ノードまたはアクティブユニットを再起動できます。

管理インターフェイスと診断インターフェイスのマージ

Threat Defense 7.4 以降では、マージされた管理インターフェイスと診断インターフェイスがサポートされます。診断インターフェイスを使用する設定がある場合、インターフェイスは自動的にマージされないため、次の手順を実行する必要があります。この手順では、設定の変更を確認し、場合によっては手動で設定を修正する必要があります。

バックアップ/復元および Management Center 構成ロールバック機能は、マージの状態（マージされていない状態またはマージされた状態）を保存および復元します。たとえば、インターフェイスをマージしてから、古いマージされていない設定を復元すると、復元された設定はマージされていない状態になります。

次の表に、レガシー診断インターフェイスで使用可能な設定と、マージの完了方法を示します。

表 *2 : Management Center* 統合管理インターフェイスのサポート

レガシー診断インターフェイスの設定	マージ動作	管理でサポートされるかどうか
インターフェイス		「管理」インターフェイスが [Interfaces] ページに読み取り専用モードで表示されるようになりました。
• IP アドレス	手動で削除する必要があります。	代わりに現在の管理 IP アドレスが使用されます。 高可用性およびクラスタリングの場合、管理インターフェイスはスタンバイ IP アドレスまたは IP アドレスプールをサポートしません。各ユニットには、フェールオーバー後も維持される独自の IP アドレスがあります。そのため、現在のアクティブ/コントロールユニットとの通信に単一の管理 IP アドレスを使用することはできません。 **configure network ipv4** または **configure network ipv6** コマンドを使用して CLI で設定します。

レガシー診断インターフェイスの設定	マージ動作	管理でサポートされるかどうか
• 「診断」名	自動的に「管理」に変更されます。 （注） 他のインターフェイスに「管理」という名前を付けることはできません。マージを続行するには、名前を変更する必要があります。	「管理」に変更されます。
スタティック ルート	手動で削除する必要があります。	**サポートしない** 管理インターフェイスには、データインターフェイスに基づく個別のLinuxルーティングテーブルがあります。Threat Defenseには、実際のところ、データインターフェイス用と管理専用インターフェイス用の2つの「データ」ルーティングテーブルがあります（以前は診断インターフェイスが含まれていましたが、管理専用に設定されたすべてのインターフェイスも含まれています）。トラフィックタイプに応じて、Threat Defense は1つのルーティングテーブルをチェックし、次に他のルーティングテーブルにフォールバックします。このルートルックアップには、診断インターフェイスは含まれておらず、管理用のLinuxルーティングテーブルも含まれていません。詳細については、「管理トラフィック用ルーティングテーブル」を参照してください。 **configure network static-routes** コマンドを使用して、CLIでLinuxルーティングテーブルのスタティックルートを追加できます。 （注） デフォルトルートは、**configure network ipv4** または **configure network ipv6** コマンドで設定します。
ダイナミック ルーティング	手動で削除する必要があります。	**サポートしない**
HTTP サーバー	変化なし	**サポートしない** この設定はマージされたデバイスでは機能しませんが、プラットフォーム設定からは削除されません。プラットフォーム設定は複数のデバイスに使用できますが、一部のデバイスはまだマージされていない可能性があります。

レガシー診断インターフェイスの設定	マージ動作	管理でサポートされるかどうか
ICMP	変化なし	**サポートしない** この設定はマージされたデバイスでは機能しませんが、プラットフォーム設定からは削除されません。プラットフォーム設定は複数のデバイスに使用できますが、一部のデバイスはまだマージされていない可能性があります。
Syslog サーバー（Syslog Server）	自動的に管理インターフェイスに移動されました。	はい。 syslog サーバーの設定で、管理インターフェイスから syslog を送信するオプションを使用できるようになりました（6.3 以降）。syslog に関して診断インターフェイスを明確に選択していた場合は、管理インターフェイスを使用するように変更されます。 （注） syslog サーバーまたは SNMP ホストのプラットフォーム設定で診断インターフェイスが名前で指定されている場合、マージされたデバイスとマージされていないデバイスに別々のプラットフォーム設定ポリシーを使用する必要があります。 （注） マージされた管理インターフェイスはセキュア syslog をサポートしていません。
SMTP	変化なし	**サポートしない** Threat Defense は SMTP サーバーについてのみデータルーティングテーブルをチェックするため、管理インターフェイスまたは他の管理専用インターフェイスを使用することはできません。詳細については、管理トラフィック用ルーティングテーブルを参照してください。
SNMP	自動的に管理インターフェイスに移動されました。	はい。 SNMP ホスト設定には、すでに管理インターフェイス（6.3 以降）で SNMP ホストを許可するオプションがあります。SNMP に関して診断インターフェイスを明確に選択していた場合は、管理インターフェイスを使用するように変更されます。 （注） syslog サーバーまたは SNMP ホストのプラットフォーム設定で診断インターフェイスが名前で指定されている場合、マージされたデバイスとマージされていないデバイスに別々のプラットフォーム設定ポリシーを使用する必要があります。

レガシー診断インターフェイスの設定	マージ動作	管理でサポートされるかどうか
RADIUS サーバー	自動的に管理インターフェイスに移動されました。	はい。 診断インターフェイスを明確に選択していた場合は、管理インターフェイスを使用するように変更されます。 （注） 送信元インターフェイスを探すためにルートルックアップを指定した場合、Threat Defense は管理専用インターフェイスからトラフィックを送信できなくなります。この場合、送信元インターフェイスとして管理インターフェイスを明示的に選択する必要があります。他の管理専用インターフェイスは使用できません。
AD サーバー	自動的に管理インターフェイスに移動されました。	はい。 診断インターフェイスを明確に選択していた場合は、管理インターフェイスを使用するように変更されます。 （注） 送信元インターフェイスを探すためにルートルックアップを指定した場合、Threat Defense は管理専用インターフェイスからトラフィックを送信できなくなります。この場合、送信元インターフェイスとして管理インターフェイスを明示的に選択する必要があります。他の管理専用インターフェイスは使用できません。
DDNS	手動で削除する必要があります。	**サポートしない**
DHCP サーバー	手動で削除する必要があります。	**サポートしない**
DNS サーバー	自動的に管理インターフェイスに移動されました。	はい。 [Enable DNS Lookup via diagnostic interface also] チェックボックスをオンにした場合、管理インターフェイスを使用するように変更されます。どのインターフェイスも選択しないか、[診断/管理インターフェイス経由のDNSルックアップも有効にする（Enable DNS Lookup via diagnostic/management interface also）] チェックボックスをオンにすると、ルーティングルックアップが変更されます。Threat Defense はデータルーティングテーブルのみを使用し、フォールバックして管理専用ルーティングテーブルを使用することはありません。したがって、DNS には管理インターフェイス以外の管理専用インターフェイスを使用できません。 （注） 管理インターフェイスには、管理トラフィック専用の個別の DNS ルックアップ設定もあります。**configure network dns** コマンドを使用して CLI で設定します。

レガシー診断インターフェイスの設定	マージ動作	管理でサポートされるかどうか
FlexConfig	手動で削除する必要があります。	サポートしない

始める前に

- デバイスの現在のモードを表示するには、Threat Defense CLI で **show management-interface convergence** コマンドを入力します。次の出力は、管理インターフェイスがマージされていることを示しています。

```
> show management-interface convergence
management-interface convergence
>
```

次の出力は、管理インターフェイスがマージされていないことを示しています。

```
> show management-interface convergence
no management-interface convergence
>
```

- 高可用性ペアおよびクラスタの場合は、アクティブ/コントロールユニットでこのタスクを実行します。マージされた設定は、スタンバイ/データユニットに自動的に複製されます。

手順

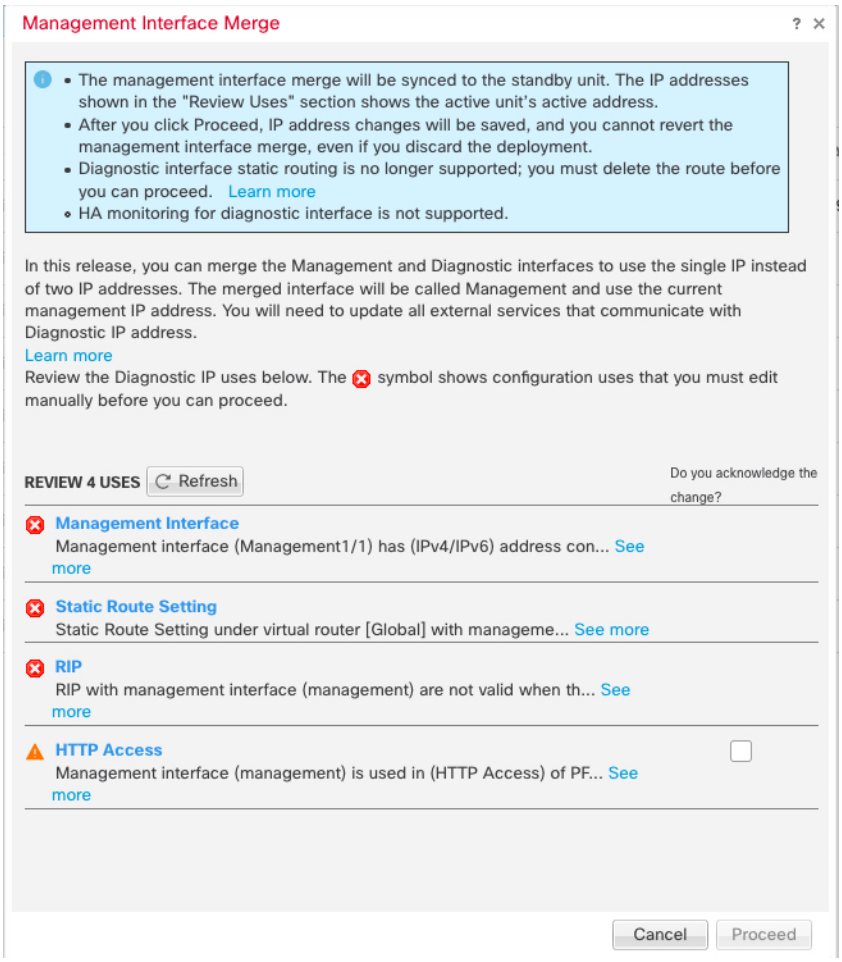
ステップ 1 **[Devices]** > **[Device Management]** を選択し、Threat Defense の **[編集（Edit）]**（✎）をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。.

ステップ 2 診断インターフェイスを編集し、IP アドレスを削除します。

診断 IP アドレスを削除するまで、マージを完了できません。

ステップ 3 [Management Interface action needed] エリアの [Management Interface Merge] をクリックします。

[管理インターフェイスのマージ（Management Interface Merge）] ダイアログボックスに、構成内の診断インターフェイスのオカレンスがすべて表示されます。手動で設定を削除または変更する必要があるオカレンスは、警告アイコン付きで表示されます。デバイスで動作しなくなったプラットフォーム設定には注意アイコンが表示されるため、確認が必要です。



ステップ 4 リストされている設定を手動で削除または変更する必要がある場合は、次の手順を実行します。

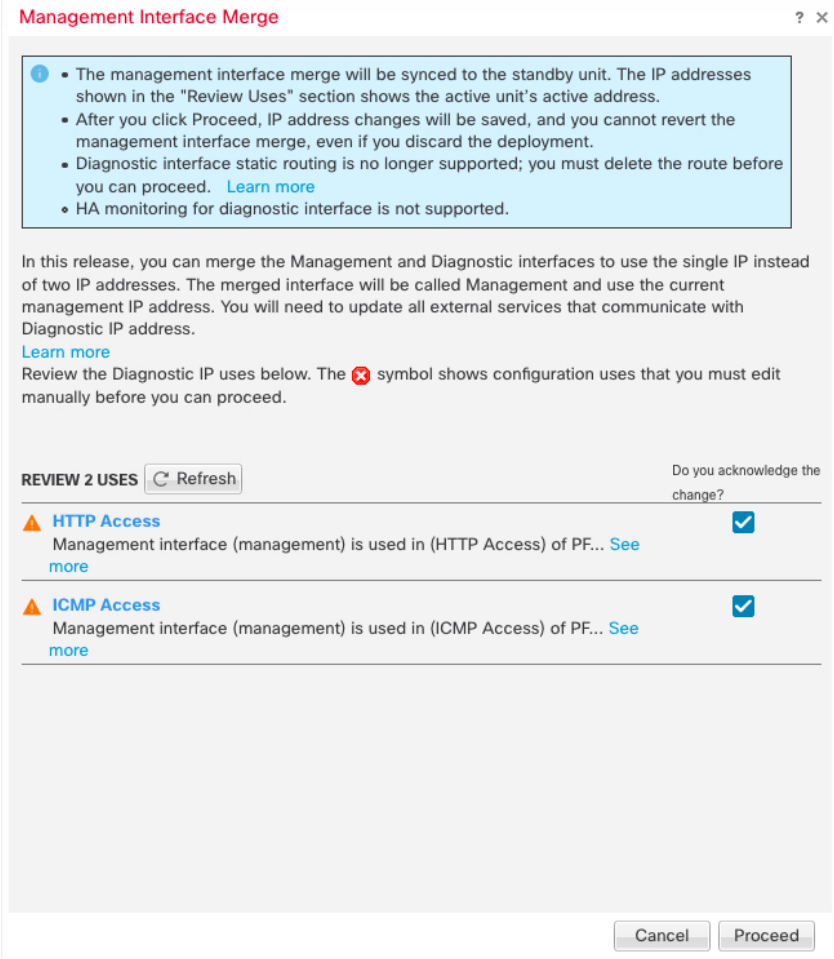
a) [Cancel] をクリックして、[Management Interface Merge] ダイアログボックスを閉じます。

b) 機能領域に移動します。その後、項目を削除したり、データインターフェイスを選択したりできます。

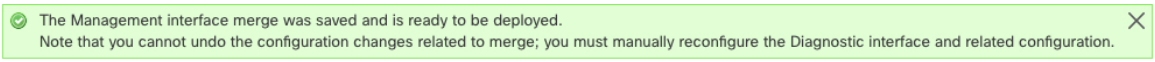
c) [Management Interface Merge] ダイアログボックスを再度開きます。

これで、警告は表示されなくなります。

ステップ 5 各設定の注意事項について、[Do you acknowledge the change?] 列のボックスをクリックしてから、[Proceed] をクリックします。



設定がマージされると、成功バナーが表示されます。



ステップ 6 マージされた新しい設定を展開します。

注意 マージされた設定を展開すると、Management Center からインターフェイスのマージを解除できます。ただし、診断インターフェイスは手動で再設定する必要があります。「管理インターフェイスのマージ解除（50ページ）」を参照してください。また、マージされていない設定を復元するか、またはマージされていない設定にロールバックすると、デバイスはそのマージされていない設定に戻ります。

マージ後、管理インターフェイスは[Interfaces]ページに表示されますが、読み取り専用です。

ステップ 7 マージ後は、診断インターフェイスと通信する外部サービスがある場合、管理インターフェイスの IP アドレスを使用するように設定を変更する必要があります。

次に例を示します。

- SNMP クライアント

- RADIUS サーバー：RADIUS サーバーでは多くの場合、着信トラフィックの IP アドレスが確認されるため、そのIPアドレスを管理アドレスに変更する必要があります。さらに、高可用性ペアの場合、プライマリとセカンダリの両方の管理 IP アドレスを許可する必要があります。診断インターフェイスは、アクティブユニットに存在する単一の「フローティング」IPアドレスをサポートしていましたが、管理インターフェイスはサポートしていません。

管理インターフェイスのマージ解除

Threat Defense 7.4 以降では、マージされた管理インターフェイスと診断インターフェイスがサポートされます。インターフェイスのマージを解除する必要がある場合は、次の手順を実行します。ネットワークをマージモード展開に移行する際は、一時的にマージ解除モードを使用することを推奨します。個別の管理インターフェイスと診断インターフェイスは、将来のすべてのリリースでサポートされなくなる可能性があります。

インターフェイスのマージを解除しても、元の診断設定は復元されません（アップグレードしてからインターフェイスをマージした場合）。診断インターフェイスを手動で再設定する必要があります。また、管理インターフェイスは「管理」という名前になり、名前を「診断」に変更することはできません。

あるいは、バックアップ機能を使用してマージされていない古い設定を保存した場合は、その設定を復元するか、または Management Center 設定ロールバック機能を使用できます。その場合、診断設定は変わらず、デバイスがマージされていない状態になります。

始める前に

- デバイスの現在のモードを表示するには、Threat Defense CLI で **show management-interface convergence** コマンドを入力します。次の出力は、管理インターフェイスがマージされていることを示しています。

```
> show management-interface convergence
management-interface convergence
>
```

次の出力は、管理インターフェイスがマージされていないことを示しています。

```
> show management-interface convergence
no management-interface convergence
>
```

- 高可用性ペアおよびクラスタの場合は、アクティブ/コントロールユニットでこのタスクを実行します。マージされた設定は、スタンバイ/データユニットに自動的に複製されます。

手順

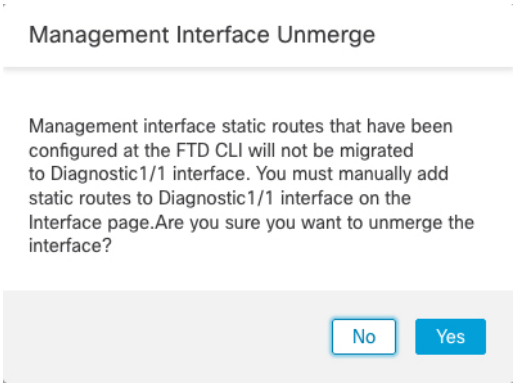
ステップ 1 **[Devices]** > **[Device Management]** を選択し、Threat Defense の **[編集（Edit）]**（✎）をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。.

ステップ 2 管理インターフェイスの場合は、[Unmerge Management Interface]（⇆）をクリックします。

図 *40* : 管理インターフェイスの選択

ステップ 3 [Yes] をクリックして、インターフェイスのマージを解除することを確認します。

図 *41* : マージ解除の確認



ステップ 4 新しいマージされていない設定を展開します。

（注） マージされた設定を復元するか、マージされた設定にロールバックすると、デバイスはそのマージされた設定に戻ります。

マージ後、管理インターフェイスは [Interfaces] ページに表示されなくなります。

インターフェイスの履歴

機能	最小 Management Center	最小 Threat Defense	詳細
ループバックおよび管理タイプのインターフェイス グループ オブジェクト	任意（Any）	7.4	管理専用インターフェイスまたはループバック インターフェイスのみを含むインターフェイス グループ オブジェクトを作成できるようになりました。その後、作成したグループを DNS サーバー、HTTP アクセス、SSH などの管理機能に使用できます。ループバック グループは、ループバック インターフェイスをサポートするすべての機能でサポートされています。DNS では管理インターフェイスはサポートされていません。 新規/変更された画面：**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [インターフェイス（Interface）] > [追加（Add）] > [インターフェイスグループ（Interface Group）]**
マージされた管理インターフェイスと診断インターフェイス	任意（Any）	7.4	7.4 以降を使用している新しいデバイスの場合、レガシー診断インターフェイスは使用できません。マージされた管理インターフェイスのみを使用できます。7.4 以降にアップグレードし、診断インターフェイスの設定がない場合は、インターフェイスが自動的にマージされます。 7.4 以降にアップグレードし、診断インターフェイスの設定がある場合は、インターフェイスを手動でマージするか、別の診断インターフェイスを引き続き使用できます。診断インターフェイスのサポートは今後のリリースで削除されるため、できるだけ早くインターフェイスをマージする必要があります。 マージモードでは、デフォルトでデータルーティングテーブルを使用するように AAA トラフィックの動作も変更されます。管理専用ルーティングテーブルは、設定で管理専用インターフェイス（管理を含む）を指定した場合にのみ使用できるようになりました。 新規/変更された画面：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）]** 新規/変更されたコマンド： **show management-interface convergence**

機能	最小 Management Center	最小 Threat Defense	詳細
Cisco Secure Firewall 3100 固定ポートのデフォルトの前方誤り訂正（FEC）が、25 GB+ SR、CSR、および LR トランシーバの第 74 条 FC-FEC から第 108 条 RS-FEC に変更されました。	任意（Any）	7.2.4/7.3	Cisco Secure Firewall 3100 の固定ポートで FEC を Auto に設定すると、25 GB 以上の SR、CSR、および LR トランシーバのデフォルトタイプが第 74 条 FC-FEC ではなく第 108 条 RS-FEC に設定されるようになりました。 サポートされるプラットフォーム：Cisco Secure Firewall 3100
Firepower 2100、Cisco Secure Firewall 3100 で LLDP をサポート。	いずれか	7.2	Firepower 2100 および Cisco Secure Firewall 3100 のインターフェイスで Link Layer Discovery Protocol（LLDP）を有効にすることができます。 新しい/変更された画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [ハードウェア構成（Hardware Configuration）] > [ネットワーク接続（Network Connectivity）]** 新規/変更されたコマンド：**show lldp status**、**show lldp neighbors**、**show lldp statistics** サポートされるプラットフォーム：Firepower 2100、Cisco Secure Firewall 3100
Cisco Secure Firewall 3100 のフロー制御に対応するためのフレームの一時停止	いずれか	7.2	トラフィック バーストが発生している場合、バーストが NIC の FIFO バッファまたは受信リング バッファのバッファリング容量を超えると、パケットがドロップされる可能性があります。フロー制御用のポーズフレームをイネーブルにすると、このような問題の発生を抑制できます。 新規/変更された画面：**[デバイス（Devices）]**>**[デバイス管理（Device Management）]**>**[インターフェイス（Interfaces）]**>**[ハードウェア構成（Hardware Configuration）]** > **[ネットワーク接続（Network Connectivity）]** サポートされるプラットフォーム：Cisco Secure Firewall 3100
Cisco Secure Firewall 3100 における前方誤り訂正のサポート	いずれか	7.1	Cisco Secure Firewall 3100 25 Gbps インターフェイスは、前方誤り訂正（FEC）をサポートします。FEC はデフォルトで有効になっており、[自動（Auto）] に設定されています。 新規/変更された画面：**[デバイス（Devices）]**>**[デバイス管理（Device Management）]**>**[インターフェイス（Interfaces）]**>**[インターフェイスの編集（Edit Interface）]** > **[ハードウェア構成（Hardware Configuration）] [速度（Speed）]**

機能	最小 Management Center	最小 Threat Defense	詳細
Cisco Secure Firewall 3100 における SFP に基づく速度設定のサポート	いずれか	7.1	Cisco Secure Firewall 3100 は、インストールされている SFP に基づくインターフェイスの速度検出をサポートします。SFP の検出はデフォルトで有効になっています。このオプションは、後でネットワークモジュールを別のモデルに変更し、速度を自動的に更新する場合に便利です。 新規/変更された画面：**[デバイス（Devices）]**>**[デバイス管理（Device Management）]**>**[インターフェイス（Interfaces）]**>**[インターフェイスの編集（Edit Interface）]** > **[ハードウェア構成（Hardware Configuration）] [速度（Speed）]**
Firepower 1100 の LLDP サポート	いずれか	7.1	Firepower 1100 インターフェイスで Link Layer Discovery Protocol（LLDP）を有効にすることができます。 新規/変更された画面：**[デバイス（Devices）]**>**[デバイス管理（Device Management）]**>**[インターフェイス（Interfaces）]**>**[ハードウェア構成（Hardware Configuration）]** > **[LLDP]** 新規/変更されたコマンド：**show lldp status**、**show lldp neighbors**、**show lldp statistics** サポートされるプラットフォーム：Firepower 1100
インターフェイスの自動ネゴシエーションが速度とデュプレックスから独立して設定されるようになり、インターフェイスの同期が改善されました。	いずれか	7.1	インターフェイスの自動ネゴシエーションが速度とデュプレックスから独立して設定されるようになりました。また、Management Center でインターフェイスを同期すると、ハードウェアの変更がより効果的に検出されます。 新規/変更された画面：**[デバイス（Devices）]**>**[デバイス管理（Device Management）]**>**[インターフェイス（Interfaces）]**>**[ハードウェア構成（Hardware Configuration）]** > **[速度（Speed）]** サポートされるプラットフォーム：Firepower 1000、2100、Cisco Secure Firewall 3100

機能	最小 Management Center	最小 Threat Defense	詳細
Firepower 1100/2100 シリーズ ファイバ インターフェイスで、自動ネゴシエーションの無効化がサポートされるようになりました。	いずれか	6.7	フロー制御とリンク ステータス ネゴシエーションを無効化するように Firepower 1100/2100 シリーズ ファイバ インターフェイスを設定できるようになりました。 以前は、これらのデバイスでファイバインターフェイス速度（1000 または 10000 Mbps）を設定すると、フロー制御とリンク ステータス ネゴシエーションが自動的に有効になり、無効にはできませんでした。 [自動ネゴシエーション（Auto-negotiation）] の選択を解除し、速度を 1000 に設定してフロー制御とリンク ステータス ネゴシエーションを無効化できるようになりました。10000 Mbps でネゴシエーションを無効化することはできません。 新規/変更された画面：[デバイス（Devices）]>[デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [ハードウェア構成（Hardware Configuration）] > [速度（Speed）] サポートされるプラットフォーム：Firepower 1100、2100

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。