インターフェースの概要

Firewall 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。Firewall 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。**Devices** > **Device Management** 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 Firewall 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、**Devices** > **Device Management** での IP アドレスを Secure Firewall Management Center 領域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 Firewall 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 （39 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 Firewall 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、Firepower Threat Defense デバイスは BVI と通常のルーテッド インターフェイス間をルーティングします。トランスペアレント モードでは、各ブリッジグループは分離されていて、相互通信できません。

IPS 専用モード

パッシブまたはインラインのいずれかの IPS 展開でデバイスを設定できます。パッシブ展開では、ネットワーク トラフィックのフローからアウトオブバンドでシステムを展開します。インライン展開では、2 つのインターフェイスを一緒にバインドすることで、ネットワーク セグメント上でシステムを透過的に設定します。

セキュリティ ゾーンとインターフェイス グループ

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、[**Objects** > **Object Management**] を選択して、**[インターフェイス（Interface）]** をクリックします。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 ゾーンを使用したトンネル レベルでのアクセス制御の適用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 Feature

For RJ-45 interfaces, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled. For Gigabit Ethernet, when the speed and duplex are set to 1000 and full, then the interface always auto-negotiates; therefore Auto-MDI/MDIX is always enabled and you cannot disable it.

冗長インターフェイス（廃止）

冗長インターフェイスは、ASA 5500-X プラットフォームでのみサポートされます。他のプラットフォームに対して設定することは推奨しません。

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。物理インターフェイスには、スイッチ ポートが含まれます。
- 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Firewall 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Firewall 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。50Gケーブルを介してポートに接続しているピアスイッチが自動ネゴシエーションをサポートしていない場合は、スイッチと Threat Defense インターフェイスでも自動ネゴシエーションを無効にしてください。たとえば、N9K-C93400LD-H1 は 50G ケーブルでの自動ネゴシエーションをサポートしていません。したがって、ポートを接続するには、プラットフォームとスイッチでデフォルトの自動ネゴシエーションを無効にする必要があります。

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 （3 ページ） を参照してください。

手順

ステップ 1　**Objects** > **Object Management** > **Interface**を選択します。

ステップ 2　[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 3　名前を入力します。

ネットワークまたはポート オブジェクトと同じ名前を使用しないでください。これらのオブジェクト名はデバイスに展開されますが、名前が重複すると展開が失敗します。

ステップ 4　[インターフェイス タイプ（Interface Type）] を選択します。

ステップ 5　（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 6　**[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。正確なインターフェイスオプションは、モデルおよびインターフェイスのタイプによって異なります。

（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、Configure a Physical Interfaceを参照してください。

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

[仮想トンネル（Virtual Tunnels）] タブをクリックしても、デバイスのルートベース VPN の動的 VTI と静的 VTI の詳細を確認できます。詳細については、「仮想トンネル情報の表示」を参照してください。

始める前に

Firewall 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。 3100/4200 の場合、ホットスワップがサポートされます。デバイスでインターフェイスを変更する前に、「Cisco Secure Firewall 3100/4200 向けネットワークモジュールを管理する （22 ページ）」を参照してください。

手順

ステップ 1 [**Devices** > **Device Management**] を選択して、Firewall Threat Defense デバイスに対して [**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 **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 文字以内で入力できます。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）。SFP の場合は、**[SFP を検出（Detect SFP）]** を選択して、インストールされた 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および FEC は常に有効です。デュアルスピード トランシーバの場合、低い方の速度が使用されます。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。一部のスイッチおよびトランシーバは、特に高速のインターフェイスの場合、自動ネゴシエーションをサポートしていません。この場合、Firewall Threat Defense のインターフェイスを手動速度に設定し、 **自動ネゴシエーション** も無効にして、リンクがアップ状態になるようにします。

  （注）
  高可用性（HA）またはクラウド制御リンク インターフェイスの速度は変更できません。

- **[自動ネゴシエーション（Auto-negotiation）]** : 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。

  1100 を除き、自動ネゴシエーションは速度とは別に設定します。一部のスイッチは、特に高速のインターフェイスの場合、自動ネゴシエーションをサポートしていません。この場合、 Firewall Threat Defense のインターフェイスを手動速度に設定し、 **自動ネゴシエーション** も無効にして、リンクがアップ状態になるようにします。

- **前方誤り訂正モード**：25Gbps 以上のインターフェイスの場合、[前方誤り訂正（FEC）（Forward Error Correction (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。EtherChannelからインターフェイスを削除する場合は、再起動後にインターフェイスの FEC を再設定する必要があります。

  一部のスイッチでは、特に大規模なインターフェイスの場合、FEC の自動モードをサポートしていません。スイッチのサポートに応じて、FEC を無効にするか、手動で設定してください。

  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
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）**[ハードウェア構成]** > **[ネットワーク接続]** をクリックして、リンク層検出プロトコル (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）**[ハードウェア構成（Hardware Configuration）]** > **[ネットワーク接続（Network Connectivity）]** の順に選択し、**[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）
Firewall 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、**Deploy** > **Deploy** に移動して、ポリシーを割り当てたデバイスにデプロイします。変更内容は導入するまで適用されません。

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、Add an EtherChannel (Port Channel)を参照してください。

About EtherChannels

This section describes EtherChannels.

About EtherChannels

An 802.3ad EtherChannel is a logical interface (called a port-channel interface) consisting of a bundle of individual Ethernet links (a channel group) so that you increase the bandwidth for a single network. A port channel interface is used in the same way as a physical interface when you configure interface-related features.

You can configure up to 48 EtherChannels, depending on how many interfaces your model supports.

Channel Group Interfaces

Each channel group can have up to 8 active interfaces, except for the ISA 3000, which supports 16 active interfaces. For switches that support only 8 active interfaces, you can assign up to 16 interfaces to a channel group: while only 8 interfaces can be active, the remaining interfaces can act as standby links in case of interface failure.

All interfaces in the channel group must be the same type and speed. The first interface added to the channel group determines the correct type and speed.

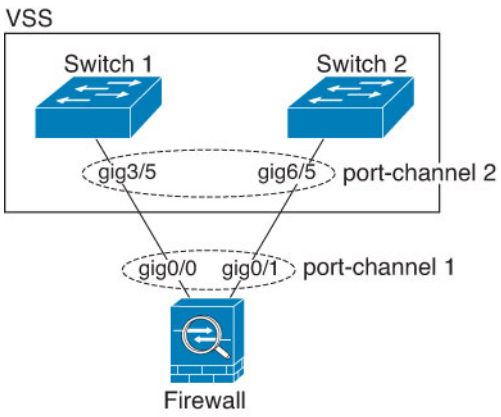
The EtherChannel aggregates the traffic across all the available active interfaces in the channel. The interface is selected using a proprietary hash algorithm, based on source or destination MAC addresses, IP addresses, TCP and UDP port numbers and VLAN numbers.

Connecting to an EtherChannel on Another Device

The device to which you connect the Firewall Threat Defense EtherChannel must also support 802.3ad EtherChannels; for example, you can connect to the Catalyst 6500 switch or the Cisco Nexus 7000.

When the switch is part of a Virtual Switching System (VSS) or Virtual Port Channel (vPC), then you can connect Firewall Threat Defense interfaces within the same EtherChannel to separate switches in the VSS/vPC. The switch interfaces are members of the same EtherChannel port-channel interface, because the separate switches act like a single switch.

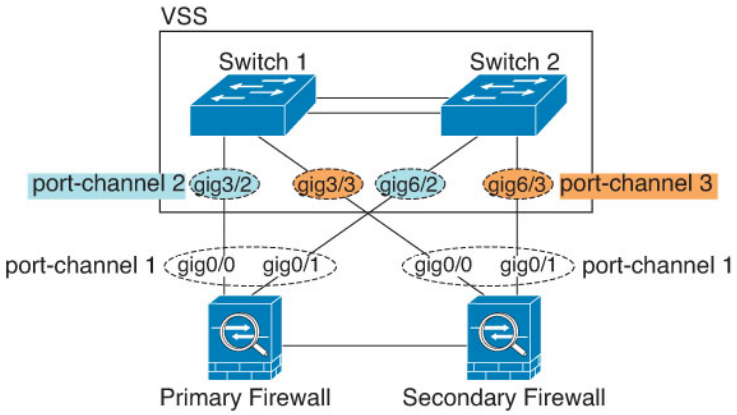
図 1 : Connecting to a VSS/vPC



（注） If the Firewall Threat Defense device is in transparent firewall mode, and you place the Firewall Threat Defense device between two sets of VSS/vPC switches, then be sure to disable Unidirectional Link Detection (UDLD) on any switch ports connected to the Firewall Threat Defense device with an EtherChannel. If you enable UDLD, then a switch port may receive UDLD packets sourced from both switches in the other VSS/vPC pair. The receiving switch will place the receiving interface in a down state with the reason "UDLD Neighbor mismatch".

If you use the Firewall Threat Defense device in an Active/Standby failover deployment, then you need to create separate EtherChannels on the switches in the VSS/vPC, one for each Firewall Threat Defense device. On each Firewall Threat Defense device, a single EtherChannel connects to both switches. Even if you could group all switch interfaces into a single EtherChannel connecting to both Firewall Threat Defense devices (in this case, the EtherChannel will not be established because of the separate Firewall Threat Defense system IDs), a single EtherChannel would not be desirable because you do not want traffic sent to the standby Firewall Threat Defense device.

図 2 : Active/Standby Failover and VSS/vPC



Link Aggregation Control Protocol

The Link Aggregation Control Protocol (LACP) aggregates interfaces by exchanging the Link Aggregation Control Protocol Data Units (LACPDUs) between two network devices.

You can configure each physical interface in an EtherChannel to be:

- Active—Sends and receives LACP updates. An active EtherChannel can establish connectivity with either an active or a passive EtherChannel. You should use the active mode unless you need to minimize the amount of LACP traffic.
- Passive—Receives LACP updates. A passive EtherChannel can only establish connectivity with an active EtherChannel. Not supported on hardware models.
- On—The EtherChannel is always on, and LACP is not used. An “on” EtherChannel can only establish a connection with another “on” EtherChannel.

LACP coordinates the automatic addition and deletion of links to the EtherChannel without user intervention. It also handles misconfigurations and checks that both ends of member interfaces are connected to the correct channel group. “On” mode cannot use standby interfaces in the channel group when an interface goes down, and the connectivity and configurations are not checked.

Load Balancing

The Firewall Threat Defense device distributes packets to the interfaces in the EtherChannel by hashing the source and destination IP address of the packet (this criteria is configurable). The resulting hash is divided by the number of active links in a modulo operation where the resulting remainder determines which interface owns the flow. All packets with a *hash_value* **mod** *active_links* result of 0 go to the first interface in the EtherChannel, packets with a result of 1 go to the second interface, packets with a result of 2 go to the third interface, and so on. For example, if you have 15 active links, then the modulo operation provides values from 0 to 14. For 6 active links, the values are 0 to 5, and so on.

If an active interface goes down and is not replaced by a standby interface, then traffic is rebalanced between the remaining links. The failure is masked from both Spanning Tree at Layer 2 and the routing table at Layer 3, so the switchover is transparent to other network devices.

EtherChannel MAC Address

All interfaces that are part of the channel group share the same MAC address. This feature makes the EtherChannel transparent to network applications and users, because they only see the one logical connection; they have no knowledge of the individual links.

Firepower and Secure Firewall Hardware

The port-channel interface uses the MAC address of the internal interface Internal-Data 0/1. Alternatively you can manually configure a MAC address for the port-channel interface. All EtherChannel interfaces on a chassis use the same MAC address, so be aware that if you use SNMP polling, for example, multiple interfaces will have the same MAC address.

（注） Member interfaces only use the Internal-Data 0/1 MAC address after a reboot. Prior to rebooting, the member interface uses its own MAC address. If you add a new member interface after a reboot, you will have to perform another reboot to update its MAC address.

Guidelines for EtherChannels

Bridge Group

In routed mode, Firewall Management Center-defined EtherChannels are not supported as bridge group members. EtherChannels on the Firepower 4100/9300 can be bridge group members.

High availability

- When you use an EtherChannel interface as a High availability link, it must be pre-configured on both units in the High availability pair; you cannot configure it on the primary unit and expect it to replicate to the secondary unit because *the High availability link itself is required for replication*.
- If you use an EtherChannel interface for the state link, no special configuration is required; the configuration can replicate from the primary unit as normal. For the Firepower 4100/9300 chassis, all interfaces, including EtherChannels, need to be pre-configured on both units.
- You can monitor EtherChannel interfaces for High availability. When an active member interface fails over to a standby interface, this activity does not cause the EtherChannel interface to appear to be failed when being monitored for device-level High availability. Only when all physical interfaces

fail does the EtherChannel interface appear to be failed (for an EtherChannel interface, the number of member interfaces allowed to fail is configurable).

- If you use an EtherChannel interface for a High availability or state link, then to prevent out-of-order packets, only one interface in the EtherChannel is used. If that interface fails, then the next interface in the EtherChannel is used. You cannot alter the EtherChannel configuration while it is in use as a High availability link. To alter the configuration, you need to temporarily disable High availability, which prevents High availability from occurring for the duration.

Model Support

- You cannot add EtherChannels in the Firewall Management Center for the Firepower 4100/9300 or the Firewall Threat Defense Virtual. The Firepower 4100/9300 supports EtherChannels, but you must perform all hardware configuration of EtherChannels in FXOS on the chassis.
- You cannot use Firepower 1010 or Secure Firewall 1210/1220 switch ports or VLAN interfaces in EtherChannels.

General EtherChannel Guidelines

- You can configure up to 48 EtherChannels, depending on how many interfaces are available on your model.
- Each channel group can have up to 8 active interfaces, except for the ISA 3000, which supports 16 active interfaces. For switches that support only 8 active interfaces, you can assign up to 16 interfaces to a channel group: while only 8 interfaces can be active, the remaining interfaces can act as standby links in case of interface failure.
- When you add the first member interface, it sets the required hardware properties of all member interfaces.
  - The media type of member interfaces can be either RJ-45 or SFP; SFPs of different types (copper and fiber) can be mixed. You cannot mix RJ-45 and SFP interfaces.
  - All interfaces must be set to the same speed and duplex.
  - The first interface sets the speed *capacity*, which cannot be changed later.
    - For SFP Detect interfaces—You can include interfaces with different speed capacities as long as they have a common speed. When you set the speed to SFP Detect (the default), the speed will be dynamically set to the highest common speed. If you later change the member interfaces so that the common speed is now higher, the EtherChannel speed will also be higher automatically.

      You can set a specific speed, but only speeds that are available on the first member interface. For example, if your first interface is 1/10GB, then the available speeds for the EtherChannel will be 1GB, 10GB, and SFP Detect. If you later remove the 1/10GB interfaces and replace them with 1/10/25GB interfaces, you cannot manually set the speed to 25GB. In this case, you can use SFP Detect to use the 25GB speed.
    - For non-SFP Detect interfaces—All additional interfaces must have the same speed capacity. For example, if your first interface speed capacity is 10MB/100MB/1GB, you must add other 10MB/100MB/1GB interfaces. You can set the EtherChannel (and its member interfaces) to any of those speeds. You cannot later add 1/10GB interfaces to the EtherChannel, even if you remove the lower capacity interfaces. You also cannot mix

interface capacities (for example 1GB and 10GB interfaces) by setting the speed to be lower on the larger-capacity interface.

- The device to which you connect the Firewall Threat Defense EtherChannel must also support 802.3ad EtherChannels.
- The Firewall Threat Defense device does not support LACPDUs that are VLAN-tagged. If you enable native VLAN tagging on the neighboring switch using the Cisco IOS **vlan dot1Q tag native** command, then the Firewall Threat Defense device will drop the tagged LACPDUs. Be sure to disable native VLAN tagging on the neighboring switch.
- The LACP rate depends on the model. When you set the rate (normal or fast), the device requests that rate from the connecting switch. In return, the device will send at the rate requested by the connecting switch. We recommend that you set the same rate on both sides.
  - Firepower 4100/9300—The LACP rate is set to fast by default in FXOS, but you can configure it as normal (also known as slow).
  - Secure Firewall 3100/4200—The LACP rate is set to normal (slow) by default, but you can configure it as fast on the device.
  - All other models—The LACP rate set to normal (also known as slow), and it is not configurable, which means the device will always request a slow rate from the connecting switch. We recommend setting the rate on the switch to slow, so both sides send LACP messages at the same rate.
- In Cisco IOS software versions earlier than 15.1(1)S2, Firewall Threat Defense did not support connecting an EtherChannel to a switch stack. With default switch settings, if the Firewall Threat Defense EtherChannel is connected cross stack, and if the primary switch is powered down, then the EtherChannel connected to the remaining switch will not come up. To improve compatibility, set the **stack-mac persistent timer** command to a large enough value to account for reload time; for example, 8 minutes or 0 for indefinite. Or, you can upgrade to more a more stable switch software version, such as 15.1(1)S2.
- All the Firewall Threat Defense configuration refers to the logical EtherChannel interface instead of the member physical interfaces.

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。

（注） Firepower 4100/9300 の場合は、FXOS の EtherChannel を設定します。詳細については、Add an EtherChannel (Port Channel)を参照してください。

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、Guidelines for EtherChannels （14 ページ） を参照してください。
- 名前が設定されている場合は、物理インターフェイスをチャネル グループに追加できません。最初に名前を削除する必要があります。

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

手順

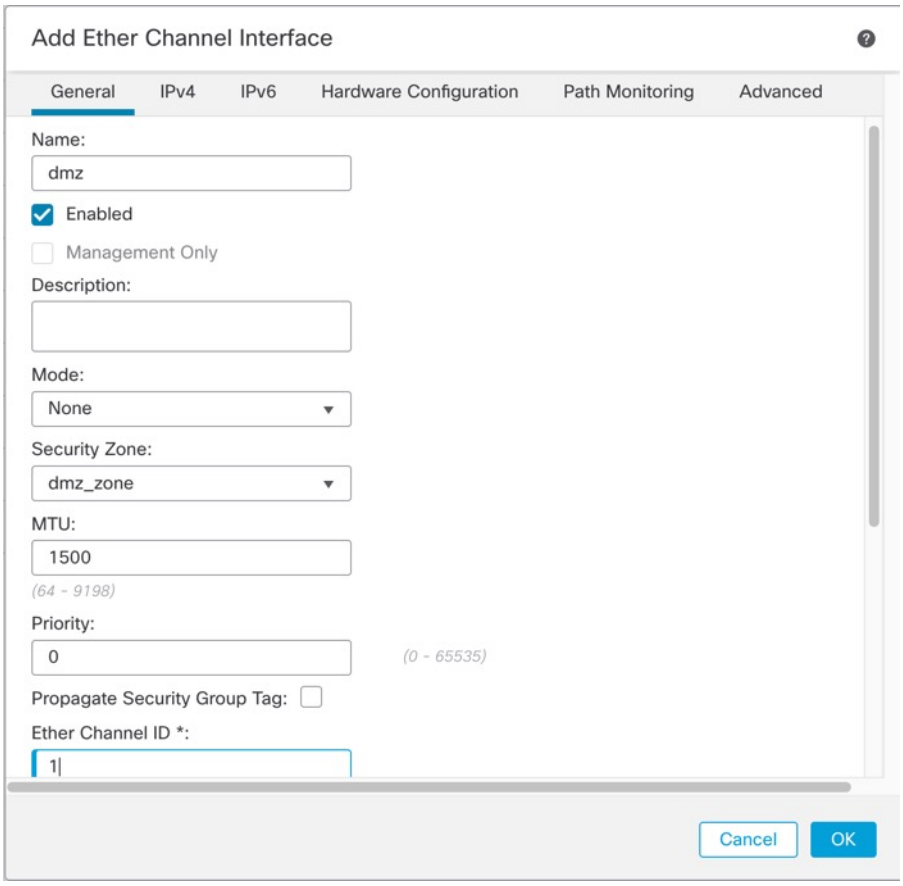
ステップ 1 [**Devices** > **Device Management**] を選択して、Firewall Threat Defense デバイスに対して [**Edit** (✎)] をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

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 （8 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 および Cisco Secure Firewall 1210 の場合は 1 ～ 8、Cisco Secure Firewall 1220 の場合は 1 ～ 10）の数値に設定します。

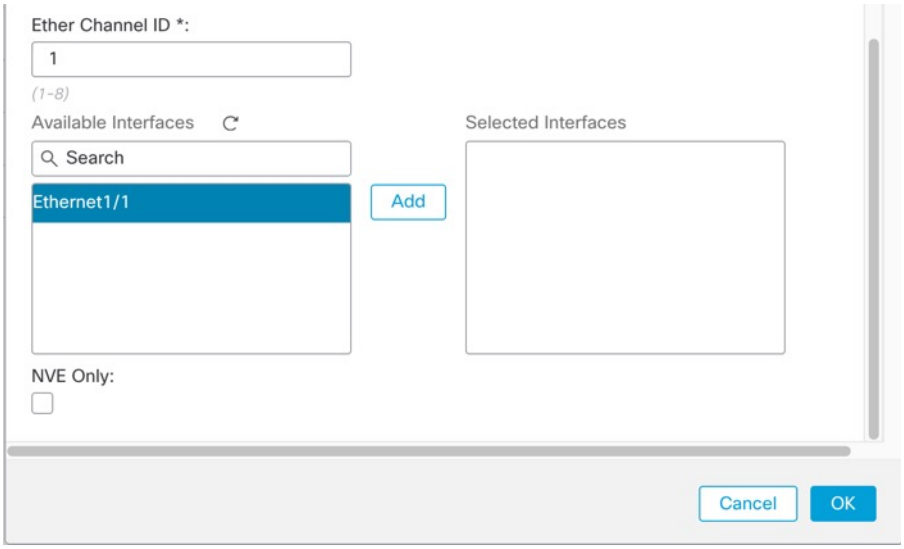
図 *3 : EtherChannel* インターフェイスの追加



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。

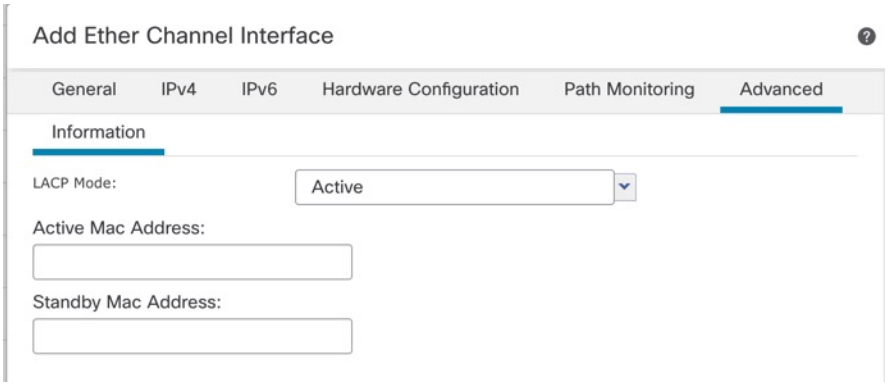
すべてのインターフェイスのタイプと速度が同じになるようにします。

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 : 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、Firewall 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、Load Balancing （14 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。パッシブモードは、ISA 3000 でのみ使用できます。

- （Cisco Secure Firewall 3100/4200 のみ）**[LACP レート（LACP Rate）]**：[デフォルト（Default）]、[標準（Normal）]、または [高速（Fast）] を選択します。デフォルトは [標準（Normal）]（低速とも呼ばれる）です。チャネルグループの物理インターフェイスの LACP データユニット受信レートを設定します。両側で同じレートを設定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、**Deploy** > **Deploy** に移動して、ポリシーを割り当てたデバイスにデプロイします。変更内容は導入するまで適用されません。

ステップ 10 （任意） 通常のファイアウォール インターフェイスの場合は、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 通常のファイアウォールインターフェイスの場合、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）。IPS 専用インターフェイスについては、「インラインセットとパッシブインターフェイス」を参照してください。

Firewall Management Center とのインターフェイスの変更の同期

デバイスでの物理インターフェイスの追加または削除は、Firewall Management Centerや、同期外れの原因となることがあります。Firewall 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
- Firewall Management Center からの展開の同期

展開を試行したときにFirewall 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

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、Firewall 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、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、Firewall 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 Firewall 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。

Firewall 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。

この手順では、必要に応じてインターフェイスの変更を手動で同期する方法と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Firewall 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

- User roles：
  - Admin
  - Access Admin
  - Network Admin

手順

ステップ 1 [**Devices** > **Device Management**] を選択して、Firewall Threat Defenseデバイスに対して [**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 **[インターフェイスの同期（Sync Interfaces）]** 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。

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]をクリックして、ポリシーがインターフェイスの変更内容で引き続き機能することを確認します。

エラーが発生した場合は、ポリシーを変更して検証を再実行する必要があります。

c) [Save] をクリックします。

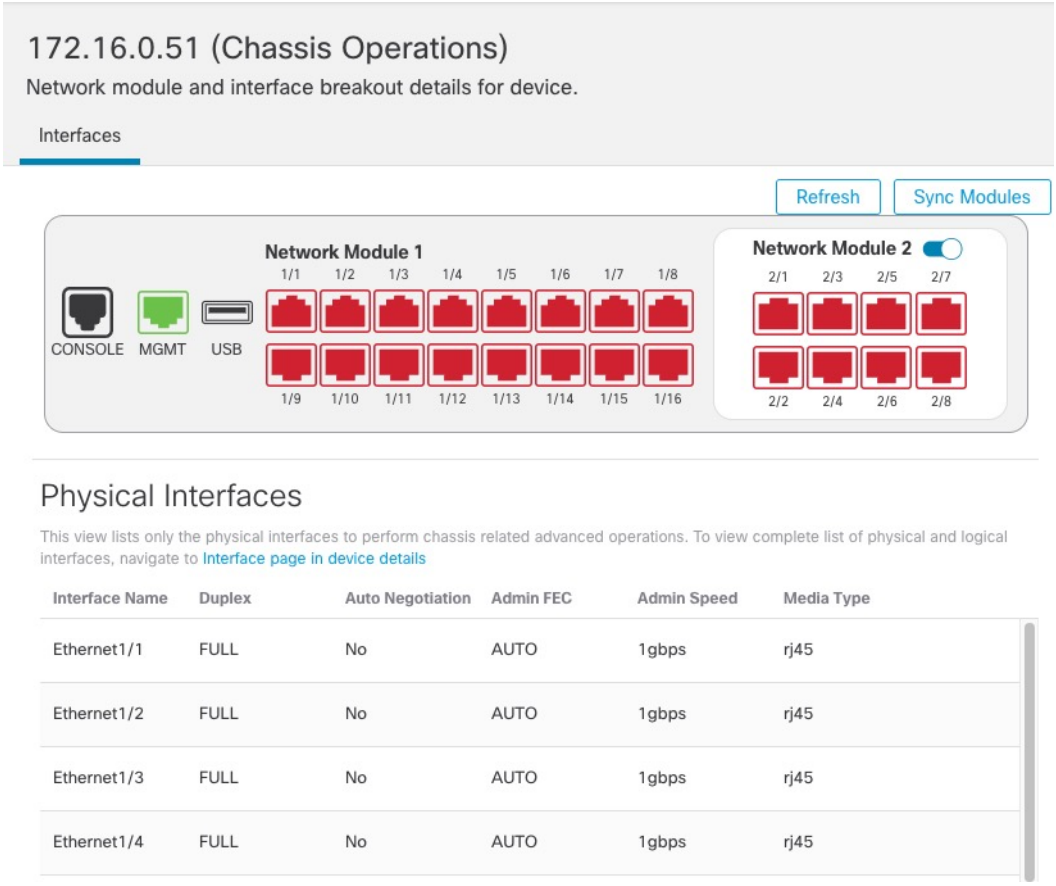
これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。

Cisco Secure Firewall 3100/4200 向けネットワークモジュールを管理する

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。**Devices** > **Device Management** で、**[シャーシ（Chassis）]** 列の **[管理（Namage）]** 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 ポートを構成できます。この手順では、ポートのブレークアウト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。たとえば、40GB インターフェイスから 4 つの 10GB ポートににブレークアウトできます。ポートの正確なサイズと数はモデルによって異なります。

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。

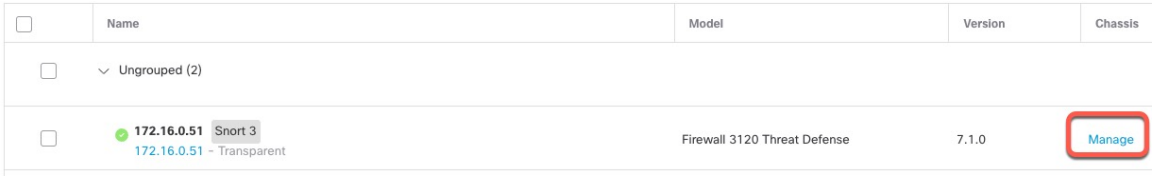
始める前に

- 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 **Devices** > **Device Management** で、**[シャーシ（Chassis）]** 列の **[管理（Namage）]** 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ポートを分割します。

a) インターフェイスの右側の **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

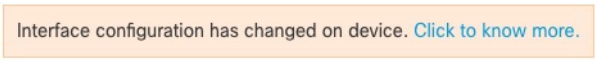
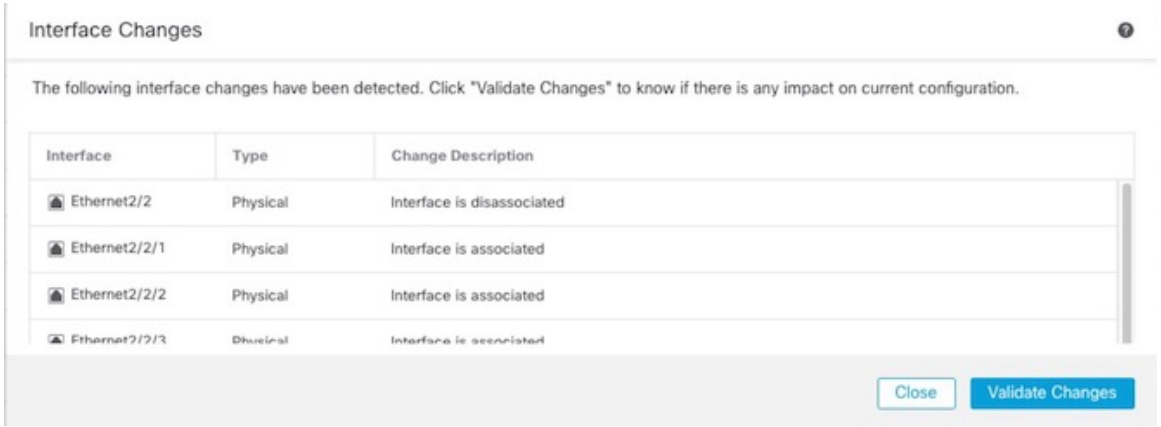


図 *11* : インターフェイスの変更



d) [変更の検証]をクリックして、ポリシーがインターフェイスの変更内容で引き続き機能することを確認します。

エラーが発生した場合は、ポリシーを変更して検証を再実行する必要があります。

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 **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

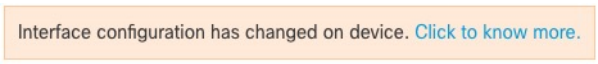
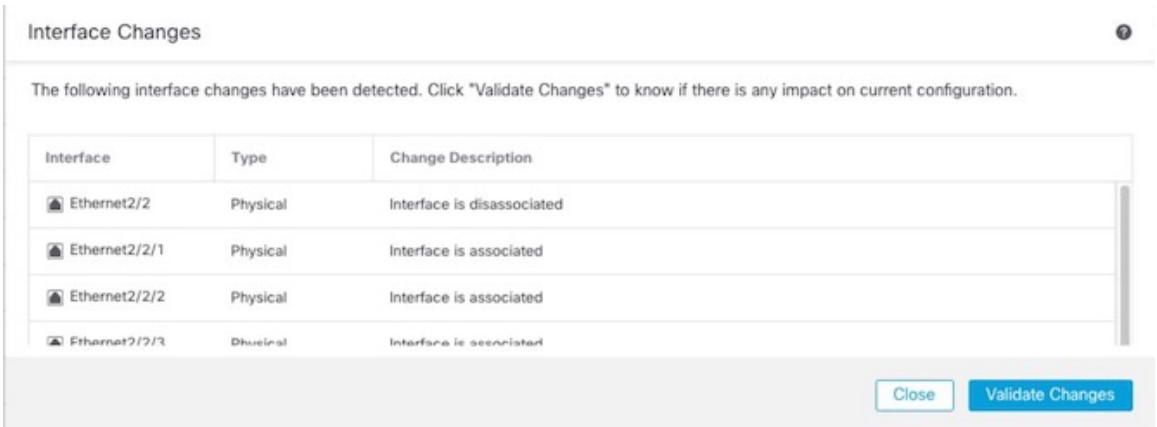


図 *14* : インターフェイスの変更



d) [変更の検証]をクリックして、ポリシーがインターフェイスの変更内容で引き続き機能することを確認します。

エラーが発生した場合は、ポリシーを変更して検証を再実行する必要があります。

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。

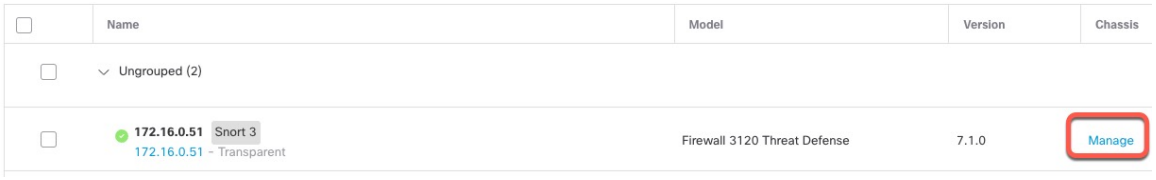
クラスタリングまたは高可用性の場合は、すべてのノードにネットワークモジュールをインストールします。

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（Firewall 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 **Devices** > **Device Management** で、**[シャーシ（Chassis）]** 列の **[管理（Namage）]** 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

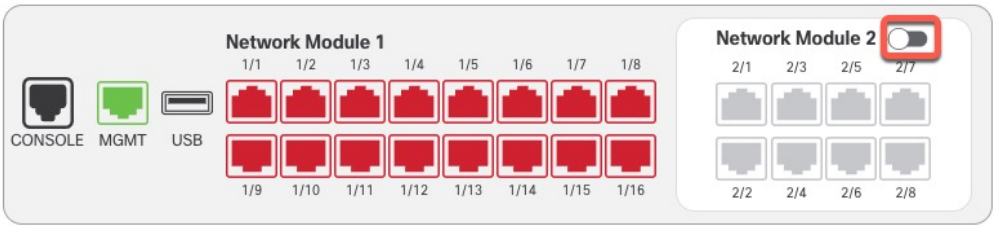


デバイスの [シャーシの操作（Chassis Operatio）] ページが開きます。このページには、デバイスの物理インターフェイスの詳細が表示されます。

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。

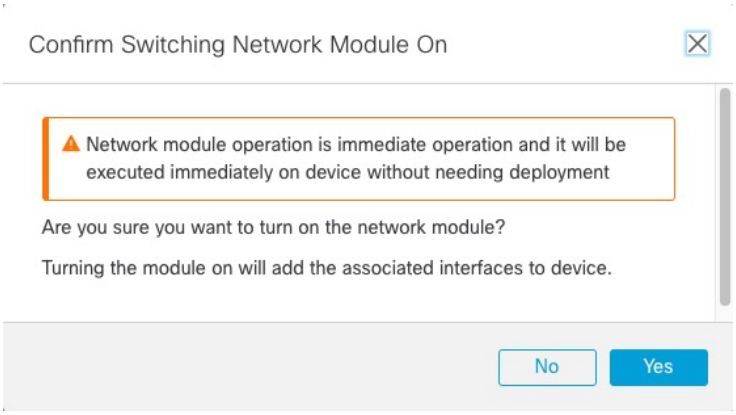
ステップ 5 インターフェイスのグラフィックで、スライダ (⊶) をクリックしてネットワークモジュールを有効にします。

図 *16* : ネットワークモジュールの有効化



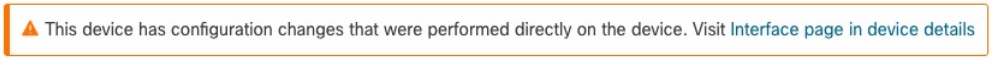
ステップ 6 ネットワークモジュールの有効化を確認するプロンプトが表示されます。[Yes] をクリックします。

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

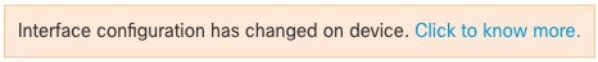
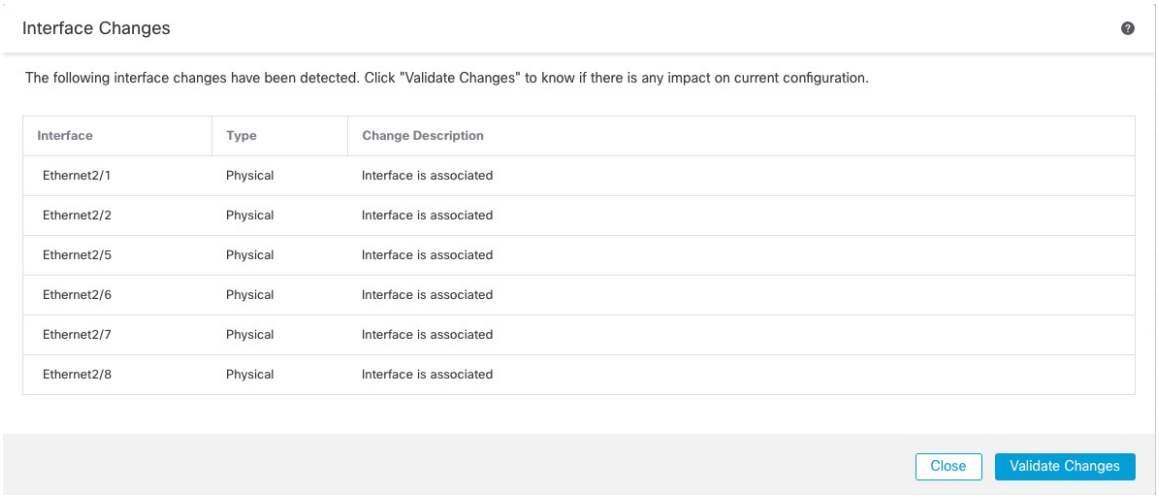


図 *20*：インターフェイスの変更



[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。

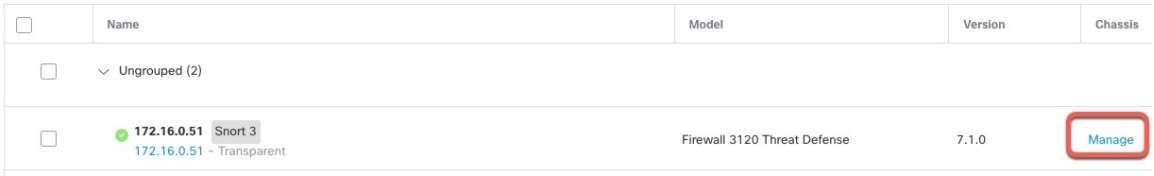
  ホットスワップを実行後、ノードをクラスタに追加し直します。または、制御ノードですべての操作を実行できます。ネットワークモジュールの変更はすべてのデータノードに同期されます。ただし、ホットスワップ中は、すべてのノードでインターフェイスが使用できなくなります。

- **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 **Devices** > **Device Management** で、**[シャーシ（Chassis）]** 列の **[管理（Namage）]** 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。

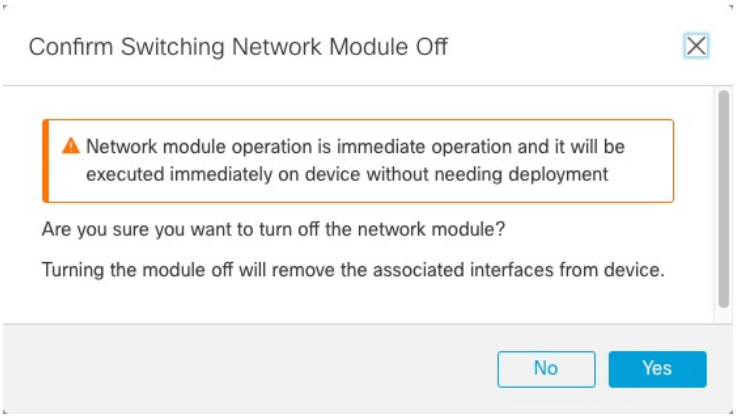
ステップ 3 インターフェイスのグラフィックで、スライダ ( ) をクリックしてネットワークモジュールを無効にします。

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。

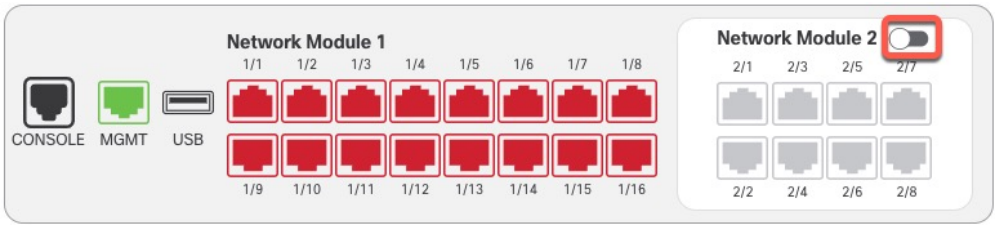
図 *23* : 無効化の確認



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。

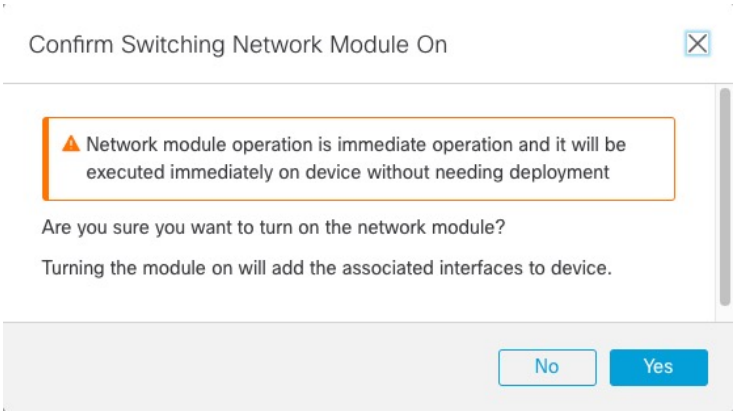
ステップ 6 Firewall Management Center で、スライダ (⊶) をクリックして新しいモジュールを有効にします。

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。

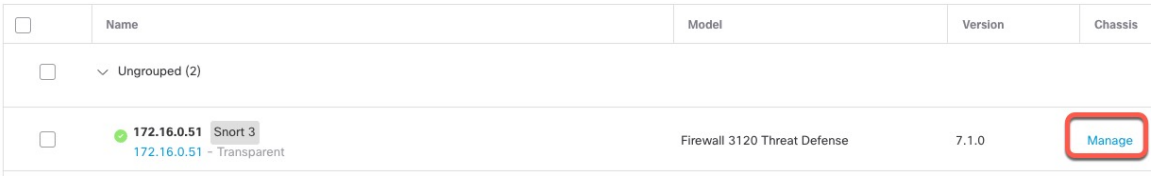
- **クラスタリング**：ネットワークモジュールを交換している間、ダウンタイムを回避するために、各ノードを一度に 1 つずつ分断し、クラスタから排除することができます。ノードの除外を参照してください。

  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 **Devices** > **Device Management** で、**[シャーシ（Chassis）]** 列の **[管理（Namage）]** 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。

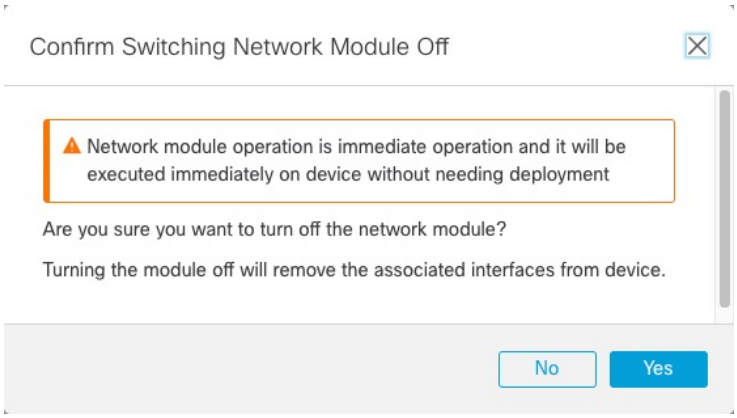
ステップ 3 インターフェイスのグラフィックで、スライダ ( ) をクリックしてネットワークモジュールを無効にします。

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。

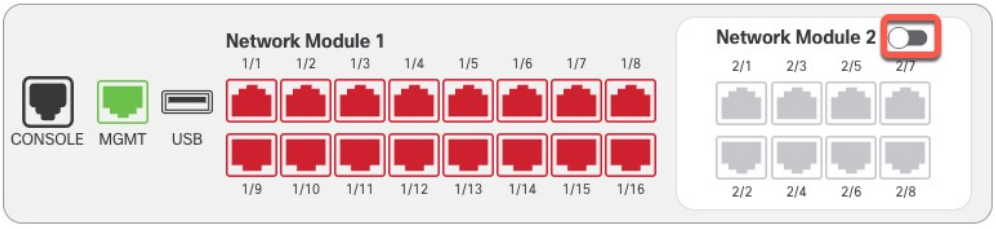
ステップ 6 ファイアウォールを再起動します。デバイスのシャットダウンまたは再起動を参照してください。

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（Firewall 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 Firewall 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。

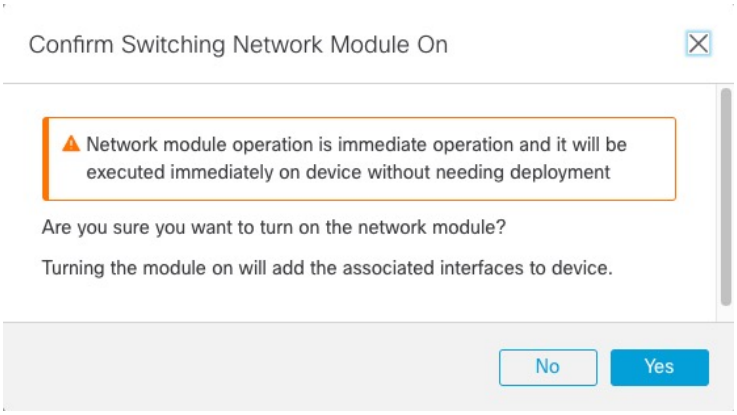
ステップ 8 スライダ (⊂) をクリックして新しいモジュールを有効にします。

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

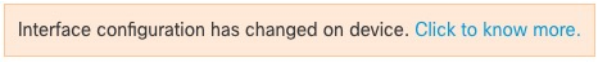
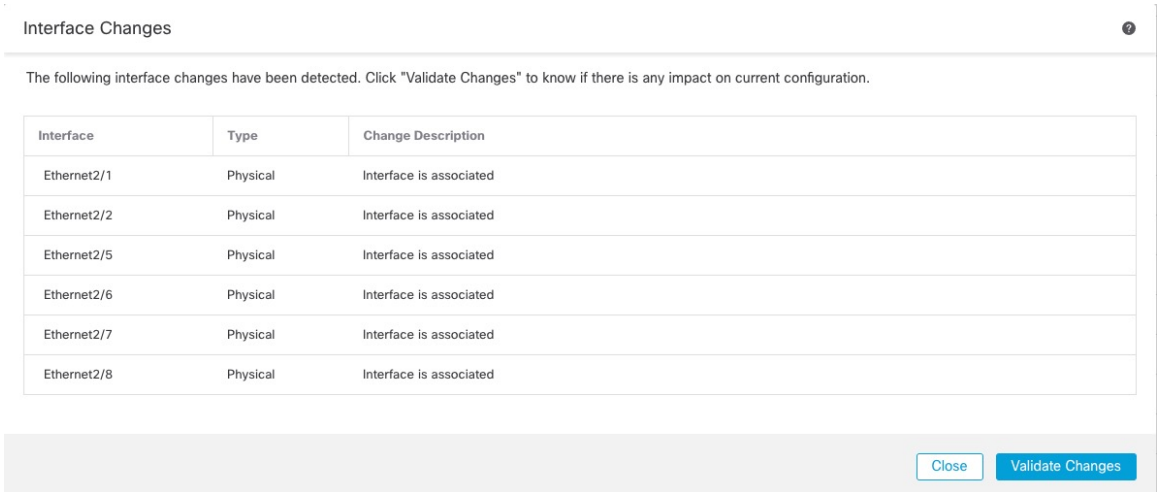


図 *33* : インターフェイスの変更



b) [変更の検証]をクリックして、ポリシーがインターフェイスの変更内容で引き続き機能することを確認します。

エラーが発生した場合は、ポリシーを変更して検証を再実行する必要があります。

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 （8 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。

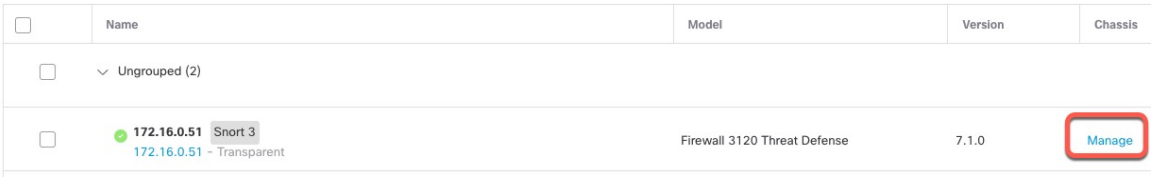
始める前に

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 **Devices** > **Device Management** で、**[シャーシ（Chassis）]** 列の **[管理（Namage）]** 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。

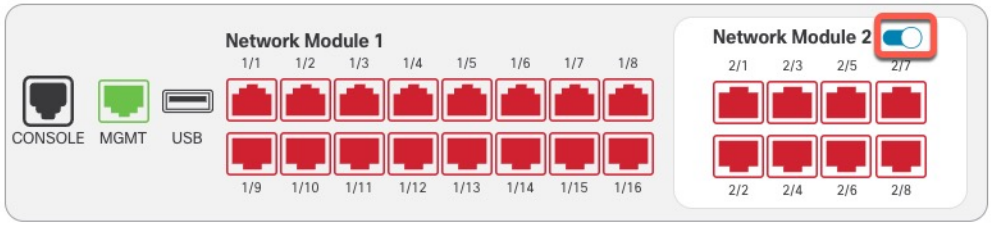
図 *34* : シャーシの管理



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。

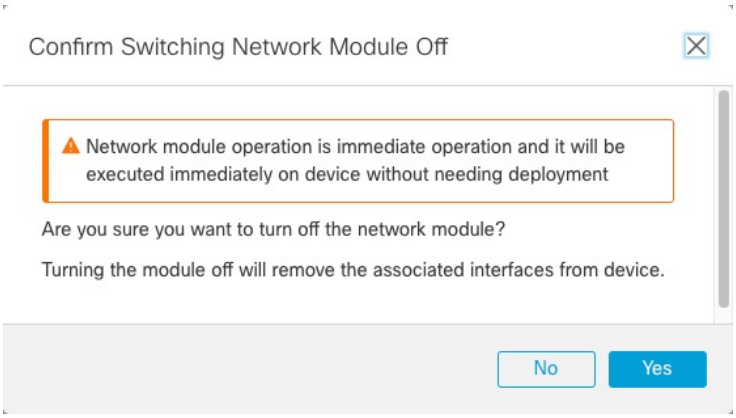
ステップ 2 インターフェイスのグラフィックで、スライダ ( ) をクリックしてネットワークモジュールを無効にします。

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

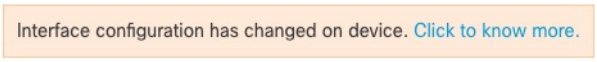


ステップ 4 画面の上部にメッセージが表示されます。リンクをクリックして [インターフェイス（Interfaces）] ページに移動し、インターフェイスの変更を保存します。

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

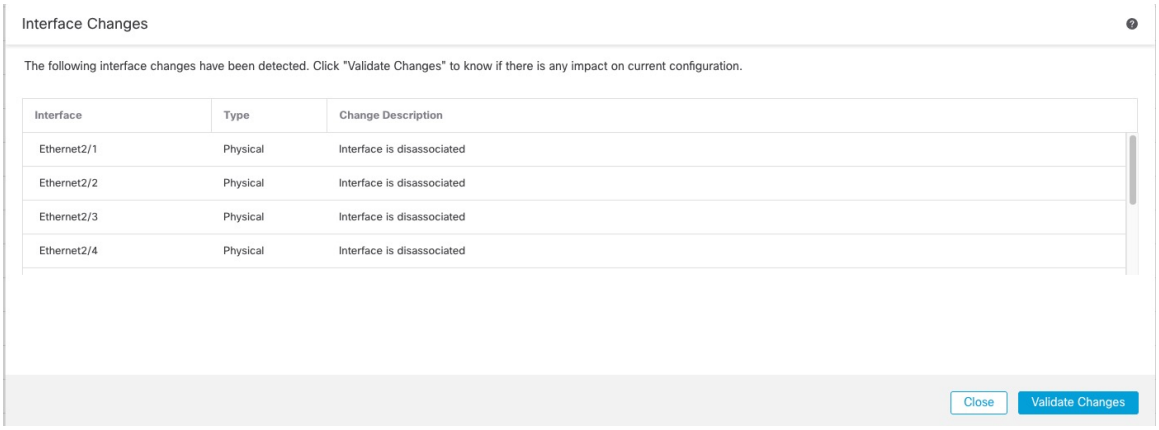
ステップ 5 [インターフェイス（Interfaces）] ページの上部に、インターフェイスの設定が変更されたことを示すメッセージが表示されます。

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]をクリックして、ポリシーがインターフェイスの変更内容で引き続き機能することを確認します。

エラーが発生した場合は、ポリシーを変更して検証を再実行する必要があります。

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（Firewall 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

Firewall 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 Firewall 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 : Firewall 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。Firewall 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、Firewall 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、「Routing Table for Management Traffic」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（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** Firewall 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、Routing Table for Management Traffic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	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、Firewall 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、Firewall 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**

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
DNS サーバ	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。Firewall 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。
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、Firewall 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

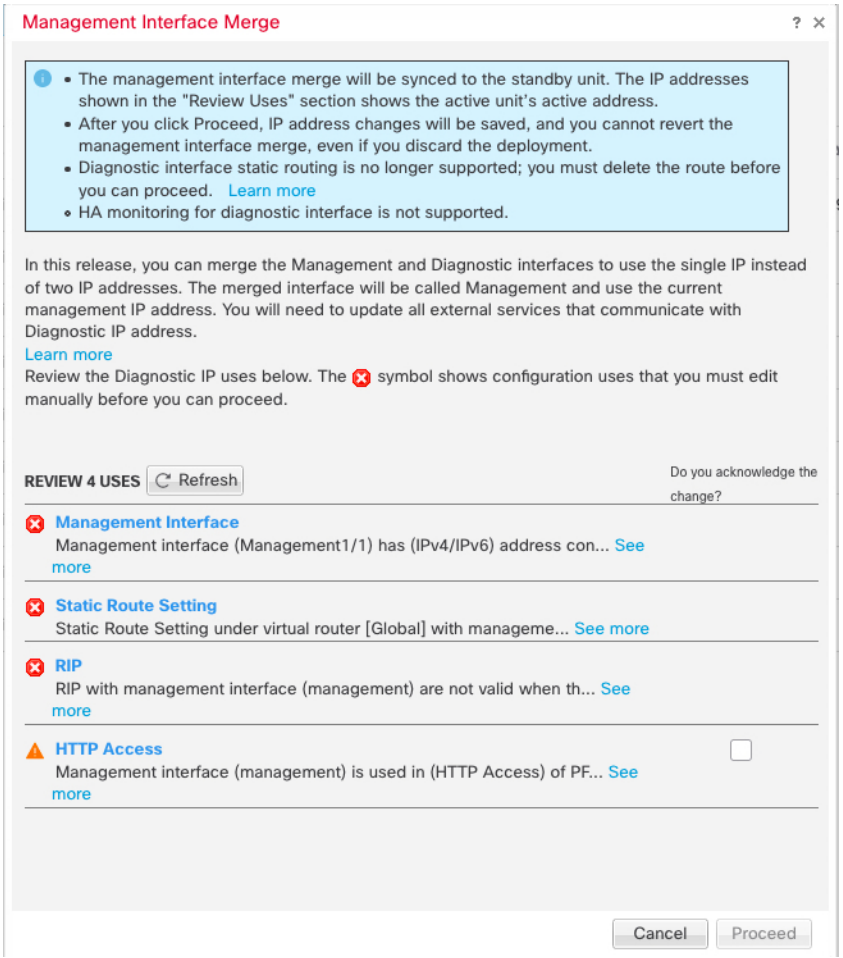
ステップ 1 [**Devices** > **Device Management**] 、Firewall Threat Defense の [**Edit** ()] の順に選択します。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。.

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。

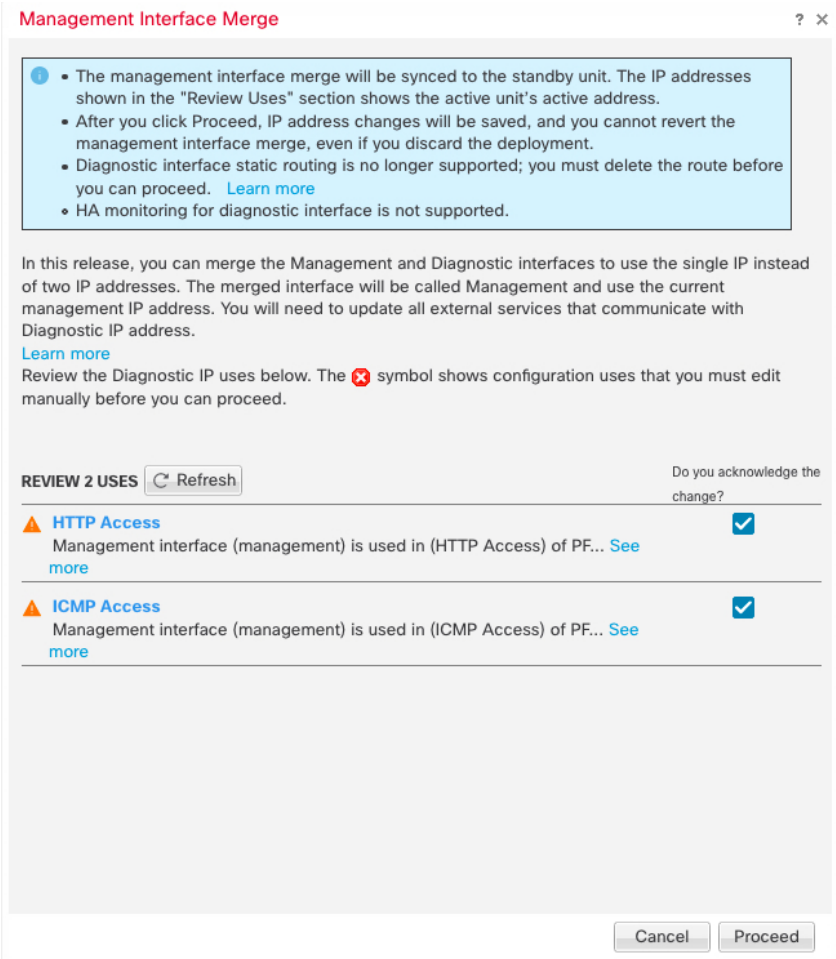
a) [Cancel] をクリックして、[Management Interface Merge] ダイアログボックスを閉じます。

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。

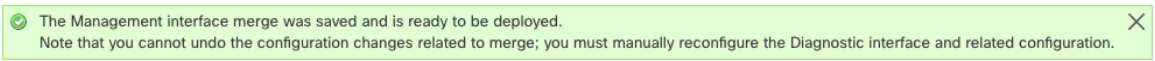
c) [Management Interface Merge] ダイアログボックスを再度開きます。

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、Firewall 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 （46 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

Firewall 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Firewall 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、Firewall 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

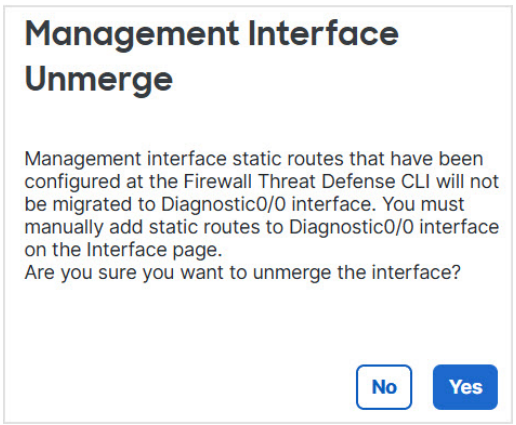
ステップ 1 [**Devices** > **Device Management**] 、Firewall Threat Defense の [**Edit** ()] の順に選択します。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。.

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	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
「同期デバイス」は「同期インターフェイス」と呼ばれるようになりました	7.7.0	7.7.0	この機能がインターフェイスの変更専用であることを示すために、**[デバイスの同期（Sync Device）]** が**[インターフェイスの同期（Sync Interfaces）]**に変更されました。この機能は、マネージャアクセスインターフェイスに加えられた変更を検出しなくなりました。**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[デバイス（Device）]** > **[管理（Management）]** > **[マネージャアクセスの詳細：構成（Manager Access Details：Configuration）]**を参照してください。 リカバリ設定モードの診断CLIで実行されたその他のアウトオブバンド設定の変更は、**[デバイス（Devices）]** > **[デバイス管理（Device Health）]** > **[デバイス（Device）]** > **[正常性（Health）]** > **[アウトオブバンドステータス（Out of Band Status）]** で検出する必要があります。 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）]**
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	7.4.0	7.4.0	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）]**

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
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	7.4.0	7.4.0	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**
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。	7.2.4	7.2.4	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。
Firepower 2100、Cisco Secure Firewall 3100 で LLDP をサポート。	7.2.0	7.2.0	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**

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
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	7.2.0	7.2.0	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）]**
Cisco Secure Firewall 3100 におけるネットワークモジュールのホットスワップのサポート	7.1.0	7.1.0	Cisco Secure Firewall 3100 では、ファイアウォールの電源がオンの状態でネットワークモジュールを追加または削除できます。モジュールを同じタイプの別のモジュールに交換する場合、再起動は必要ありません。最初の起動の後にモジュールを追加するか、モジュールを完全に削除するか、モジュールを新しいタイプのモジュールに交換する場合は、再起動が必要です。 新しい/変更された画面： [デバイス（Devices）]>[デバイス管理（Device Management）]>[シャーシの操作（Chassis Operations）]
Cisco Secure Firewall 3100における前方誤り訂正のサポート	7.1.0	7.1.0	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）]**
Cisco Secure Firewall 3100 における SFP に基づく速度設定のサポート	7.1.0	7.1.0	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）]**

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
Firepower 1100 の LLDP サポート。	7.1.0	7.1.0	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**
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。	7.1.0	7.1.0	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、Firewall 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
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。	6.7.0	6.7.0	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）]

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。