デバイス設定

デバイスを追加したら、[デバイス（Device）] ページでデバイス関連の設定を編集できます。

1. **Devices** > **Device Management** を選択します。
2. 変更するデバイスの横にある **Edit** (✎) をクリックします。
3. [Device] をクリックします。

全般設定の編集

[デバイス（Device）] タブの [全般（General）] セクションには、以下の表に記載された設定が表示されます。

図 *1*：一般

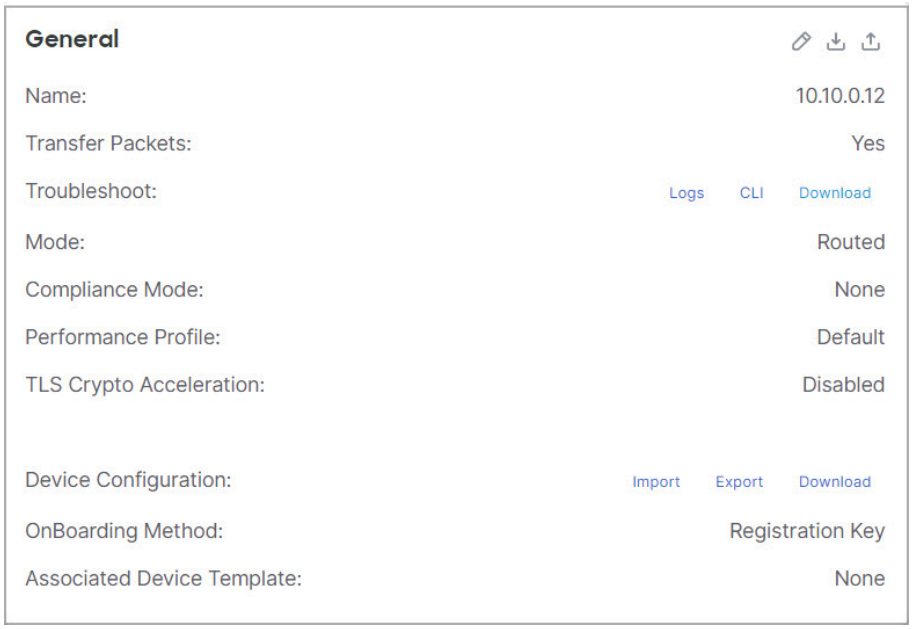


表 *1*：*[*全般（*General*）*]*セクション テーブルのフィールド

フィールド	説明
名前	Firewall Management Center でのデバイスの表示名。
パケット転送（Transfer Packets）	管理対象デバイスがイベントを含むパケット データを Firewall Management Center に送信するかどうかを表示します。
トラブルシューティング（Troubleshoot）	トラブルシューティング ファイルを生成およびダウンロードできます。また、CLI コマンド出力も表示できます。トラブルシューティング ファイルの生成 （4 ページ）およびCLI 出力の表示 （6 ページ）を参照してください。
モード（Mode）	デバイスの管理インターフェイスのモード（[ルーテッド（routed）] または [トランスペアレント（transparent）]）を表示します。
コンプライアンスモード（Compliance Mode）	デバイスのセキュリティ認定準拠が表示されます。有効な値は、CC、UCAPL および None です。
パフォーマンスプロファイル（Performance Profile）	プラットフォーム設定ポリシーで設定された、デバイスのコア割り当てパフォーマンスプロファイルが表示されます。
TLS暗号化アクセラレーション：（TLS Crypto Acceleration:）	TLS 暗号化アクセラレーションが有効か無効かを示します。

フィールド	説明
デバイス設定（Device Configuration）	構成をコピー、エクスポート、またはインポートできます。別のデバイスへの構成のコピー （9 ページ）およびデバイス設定のエクスポートとインポート （11 ページ）を参照してください。
オンボーディング方式（OnBoarding Method）	デバイスが登録キーを使用して登録されたか、シリアル番号（zero-touch provisioning）を使用して登録されたかを示します。

これらの設定の一部は、このセクションから編集できます。

手順

ステップ 1 **Devices** > **Device Management** を選択します。

ステップ 2 変更するデバイスの横にある **Edit** (✎) をクリックします。

ステップ 3 [Device] をクリックします。

ステップ 4 [General] セクションで、**Edit** (✎) をクリックします。

a) [Name] に、管理対象デバイスの名前を入力します。

b) パケットデータをイベントと一緒に Firewall Management Center に保存できるようにするには、[パケットの転送（Transfer Packets）] チェックボックスをオンにします。

c) [Force Deploy] をクリックし、デバイスに現在のポリシーとデバイス設定の展開を強制します。

（注）
強制展開は、Firewall Threat Defense に展開されるポリシールールの完全な生成をともなうため、通常の展開よりも時間がかかります。

ステップ 5 [トラブルシューティング（Troubleshooting）] アクションについては、トラブルシューティング ファイルの生成 （4 ページ）およびCLI 出力の表示 （6 ページ）を参照してください。

ステップ 6 [デバイス構成（Device Configuration）] アクションについては、別のデバイスへの構成のコピー （9 ページ）およびデバイス設定のエクスポートとインポート （11 ページ）を参照してください。

ステップ 7 [Deploy] をクリックします。

次のタスク

- 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。

トラブルシューティング ファイルの生成

各デバイスとすべてのクラスタノードのトラブルシューティング ファイルを生成およびダウンロードできます。クラスタの場合、すべてのファイルを単一の圧縮ファイルとしてダウンロードできます。クラスタノードのクラスタのクラスタログを含めることもできます。

または、**[デバイス（Devices）] > [デバイス管理（Device Management）] > More** (⋮) > [トラブルシューティング ファイル（Troubleshoot Files）] メニューからファイル生成をトリガーできます。

手順

ステップ 1 **Devices** > **Device Management** を選択します。

ステップ 2 表示するデバイスまたはクラスタの横にある **Edit** (✎) をクリックします。

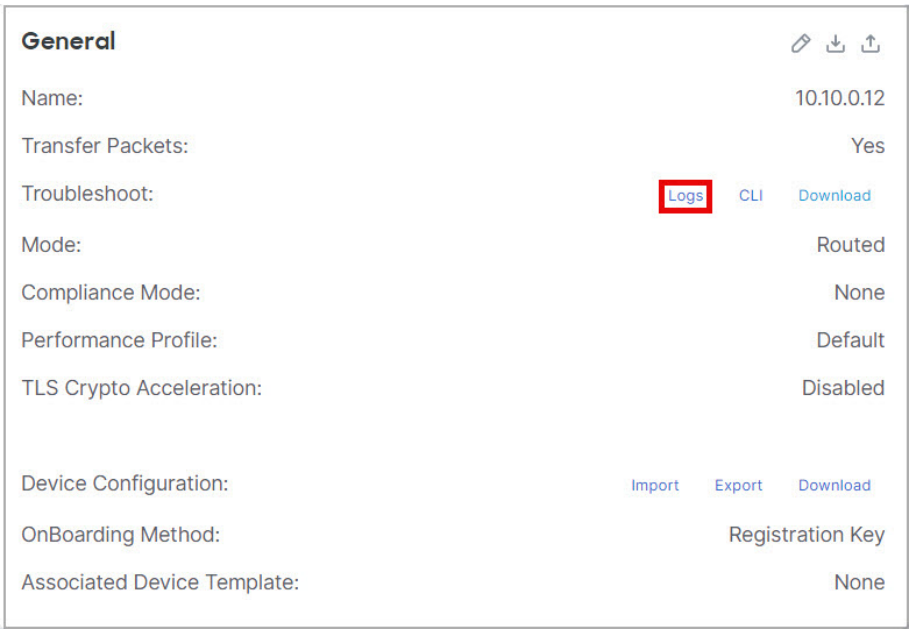
マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス（Device）] または [クラスタ（Cluster）] をクリックします。

ステップ 4 デバイスまたはすべてのクラスタノードのログを生成します。

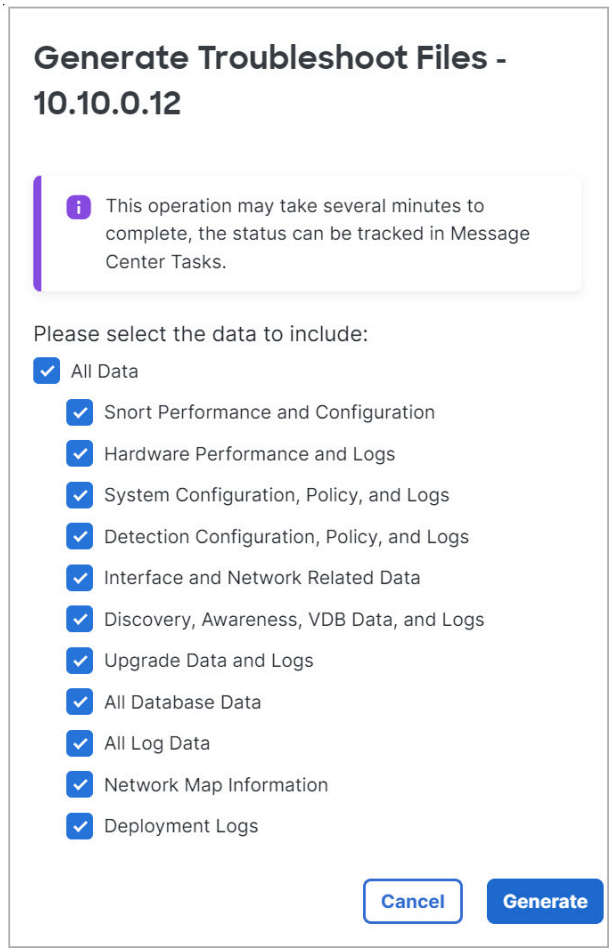
a) [全般（General）] > [トラブルシュート（Troubleshoot）] セクションで、[ログ（Logs）] をクリックします。

図 2: ログ



b) 含めるログを選択するように求められます。クラスタの場合、[デバイス（Device）] で、[すべてのデバイス（All Devices）] または個々のノードを選択できます。クラスタには、使用可能な**クラスタログ**もあります。

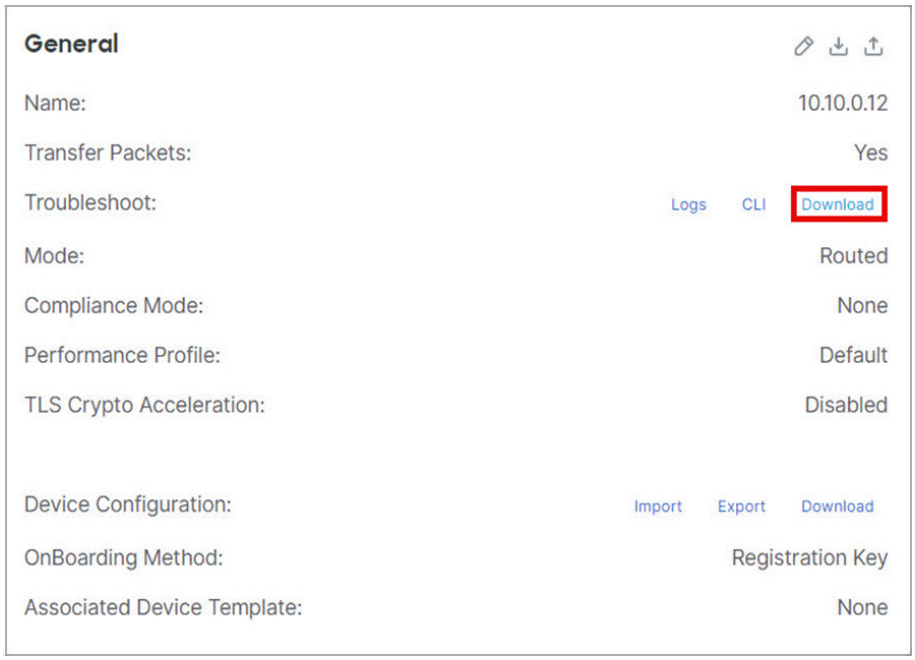
図 *3*: トラブルシューティング ファイルの生成



c) [生成（Generate）] をクリックします。

ステップ 5 生成されたログをダウンロードするには、[全般（General）] > [トラブルシュート（Troubleshoot）] セクションで、[ダウンロード（Download）] をクリックします。

図 *4:* ダウンロード



ログがコンピュータにダウンロードされます。

CLI 出力の表示

デバイスまたはクラスタのトラブルシューティングに役立つ一連の定義済みCLI出力を表示できます。任意の **show** コマンドを入力して、出力を確認することもできます。

デバイスの場合、以下のコマンドが実行されます。

- **show version**
- **show asp drop**
- **show counters**
- **show int ip brief**
- **show blocks**
- **show cpu detailed**

クラスタまたはクラスタノードの場合：

- **show running-config cluster**
- **show cluster info**
- **show cluster info health**

- **show cluster info transport cp**
- **show version**
- **show asp drop**
- **show counters**
- **show arp**
- **show int ip brief**
- **show blocks**
- **show cpu detailed**
- **show interface** *ccl_interface*
- **ping** *ccl_ip* **size** *ccl_mtu* **repeat 2**

手順

ステップ 1 **Devices** > **Device Management** を選択します。

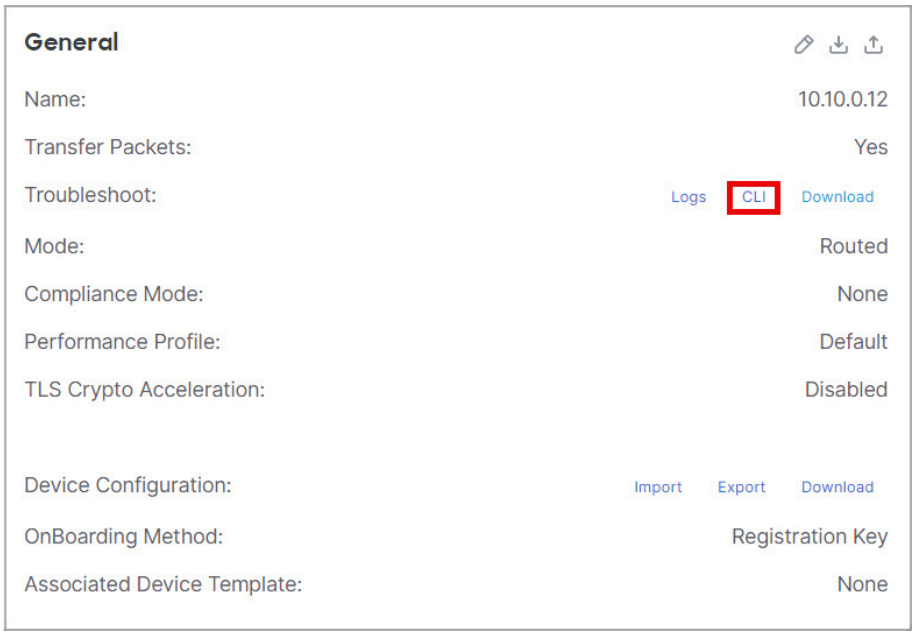
ステップ 2 表示するデバイスまたはクラスタの横にある **Edit** (✎) をクリックします。

マルチドメイン展開では、リーフドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [デバイス（Device）] または [クラスタ（Cluster）] をクリックします。

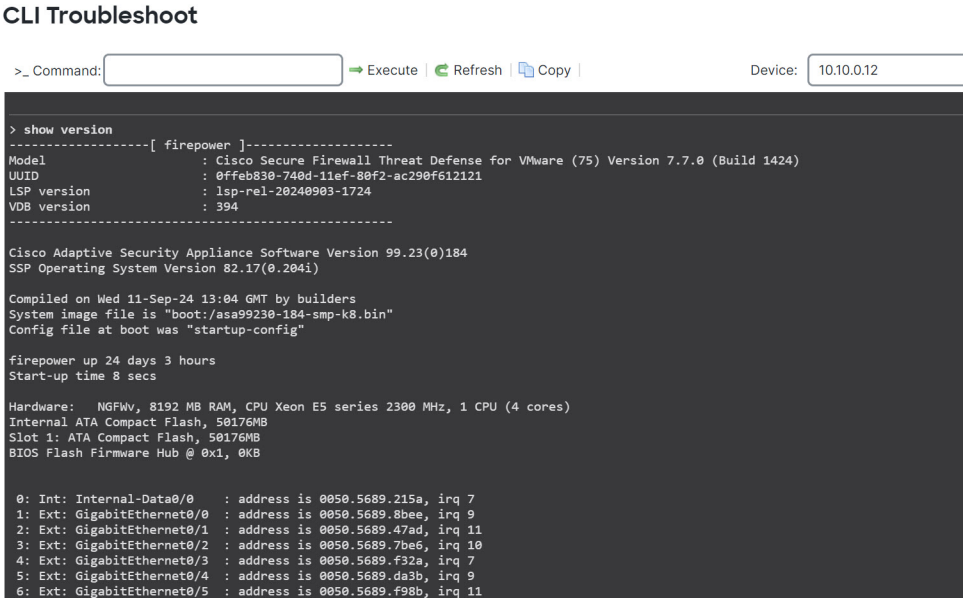
ステップ 4 [全般（General）] > [トラブルシュート（Troubleshoot）] セクションで、 [CLI] をクリックします。

図 *5 : CLI*



[CLI のトラブルシュート（CLI Troubleshoot）] ダイアログボックスが表示され、事前定義された CLI が実行されます。

図 *6 : CLI* のトラブルシュート



ステップ 5 [CLI のトラブルシュート（CLI Troubleshoot）] ダイアログボックスでは、次のタスクを実行できます。

- [コマンド（Command）] フィールドに **show** コマンドを入力して、[実行（Execute）] をクリックします。新しいコマンド出力がウィンドウに追加されます。

- [更新（Refresh）] をクリックして、定義済みの CLI を再実行します。
- [コピー（Copy）] をクリックし、クリップボードに出力をコピーします。
- クラスタの場合は、[デバイス（Device）] ドロップダウンリストから別のノードを選択します。

ステップ 6 [閉じる（Close）] をクリックします。

別のデバイスへの構成のコピー

新しいデバイスをネットワークに展開する場合、新しいデバイスを手動で再設定する代わりに、事前設定されているデバイスの設定とポリシーを簡単にコピーすることができます。

始める前に

次の項目を確認します。

- コピー元とコピー先のデバイスが同じモデルであり、同じバージョンのソフトウェアを実行している。
- コピー元がスタンドアロン デバイスまたは高可用性ペアである。
- コピー先のデバイスがスタンドアロン デバイスである。
- コピー元とコピー先のデバイスに同じ数の物理インターフェイスがある。
- コピー元とコピー先のデバイスが同じファイアウォール モード（ルーテッドまたはトランスペアレント）になっている。
- コピー元とコピー先のデバイスが同じセキュリティ認定コンプライアンス モードになっている。
- コピー元とコピー先のデバイスが同じドメインにある。
- コピー元またはコピー先デバイスのいずれでも設定の展開が進行中ではない。

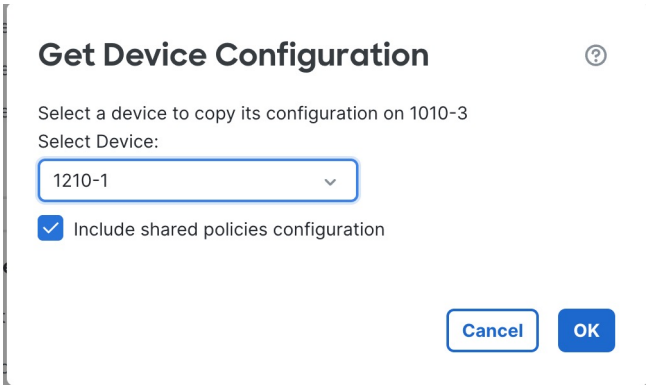
手順

ステップ 1 **Devices** > **Device Management** を選択します。
ステップ 2 変更するデバイスの横にある **Edit** (✎) をクリックします。
ステップ 3 [デバイス（Device）] をクリックします。
ステップ 4 [全般（General）] セクションで、次のいずれかの操作を実行します。

図 *7:* デバイス設定のコピーまたはプッシュ

- **Get Device Configuration** (⬇) をクリックして、別のデバイスのデバイス設定を新しいデバイスにコピーします。[デバイス設定の取得（Get Device Configuration）] ページの [デバイスの選択（Select Device）] ドロップダウン リストで、送信元デバイスを選択します。

  図 *8:* デバイスの選択

- **Push Device Configuration** (⬆) をクリックして、現在のデバイスのデバイス設定を新しいデバイスにコピーします。[デバイス設定のプッシュ（Push Device Configuration）] ページの [ターゲットデバイス（Target Device）] ドロップダウンリストで、設定をコピーする宛先を選択します。

ステップ 5 （オプション）[共有ポリシーの設定を含める（Include shared policies configuration）] チェックボックスをオンにして、ポリシーをコピーします。

AC ポリシー、NAT、プラットフォーム設定、および FlexConfig ポリシーなどの共有ポリシーは、複数のデバイス間で共有できます。

ステップ 6 [OK] をクリックします。

デバイス設定のコピータスクのステータスは、メッセージセンターの [タスク（Tasks）] でモニターできます。

デバイス設定のコピー タスクが開始されると、ターゲット デバイスの設定が削除され、送信元デバイスの設定が宛先のデバイスにコピーされます。

⚠

警告 デバイス設定のコピー タスクの完了後に、ターゲット デバイスを元の設定に戻すことはできません。

デバイス設定のエクスポートとインポート

（注）
- オンプレミスの Firewall Management Center と Cloud-Delivered Firewall Management Center 間のデバイス構成のエクスポートとインポートは、共有ポリシーおよびデバイスポリシーではサポートされていません。
- 異なるドロップのポリシーで基盤となるモデルが変更されている場合、Cloud-Delivered Firewall Management Center のエクスポートとインポートはドロップバージョンではサポートされません。
- デバイス設定のエクスポートとインポートは、デバイスの UUID、モデル、バージョンが同じ場合にのみサポートされます。

[デバイス（Device）]ページで設定可能な、次のようなデバイス固有の設定をすべてエクスポートできます。

- インターフェイス
- インラインセット
- ルーティング
- DHCP
- VTEP
- 関連オブジェクト

次の使用例で、同じデバイスに保存された設定をインポートできます。

- 別の Firewall Management Center へのデバイスの移動：最初に元の Firewall Management Center からデバイスを登録解除 してから、新しい Firewall Management Center にデバイスを追加します。これで保存された設定をインポートできます。
- ドメイン間でのデバイスの移動：ドメイン間でデバイスを移動する場合、サポートするオブジェクト（セキュリティゾーンのインターフェイスグループなど）が新しいドメインに存在しないため、一部のデバイス固有の設定が保持されません。ドメインの移動後に設定をインポートすると、そのドメインに必要なオブジェクトが作成され、デバイス設定が復元されます。
- 古い設定の復元：デバイスの動作に悪影響を与える変更を展開した場合は、既知の動作設定のバックアップコピーをインポートして、以前の動作状態を復元できます。
- デバイスの再登録：デバイスを Firewall Management Center から登録解除した後で追加し直す場合は、保存した設定をインポートできます。

次のガイドラインを参照してください。

- 設定は同じデバイスにのみインポートできます（UUID が一致する必要があります）。同じモデルであっても、設定を別のデバイスにインポートすることはできません。
- エクスポートとインポートの間に、デバイスで実行されているバージョンを変更しないでください。バージョンは一致する必要があります。
- エクスポート後に一覧を変更すると（ネットワークモジュールの追加や削除、ブレークアウトポートの設定や結合など）、デバイス一覧が Firewall Management Center と一致しなくなります。この場合はデバイス一覧が維持され、展開を試行すると、インターフェイスを同期し（「Firewall Management Center とのインターフェイスの変更の同期」を参照）、Firewall Management Center の互換性のない構成を破棄するように求められます。Firewall Management Center で一覧の変更と関連する構成を繰り返す必要があります。
- スタンドアロン設定をエクスポートする場合、高可用性ペアにインポートすることはできません。その逆も同様です。
- 異なる Firewall Management Center にデバイスを移動する場合、ターゲットの Firewall Management Center バージョンは、ソースバージョンと同じである必要があります。
- オブジェクトが存在しない場合は作成されます。オブジェクトが存在するが値が異なる場合は、以下を参照してください。

表 *2:* オブジェクトのインポートアクション

シナリオ	インポートアクション
同じ名前と値のオブジェクトが存在する。	既存のオブジェクトを再利用します。
同じ名前で値が異なるオブジェクトが存在する。	ネットワークおよびポートオブジェクト：このデバイスのオブジェクトオーバーライドを作成します。「オブジェクトのオーバーライド」を参照してください。 インターフェイス オブジェクト：新しいオブジェクトを作成します。たとえば、タイプ（セキュリティゾーンまたはインターフェイスグループ）とインターフェイスタイプ（ルーテッドまたはスイッチドなど）の両方が一致しない場合、新しいオブジェクトが作成されます。 他のすべてのオブジェクト：値が異なっていても、既存のオブジェクトを再利用します。
オブジェクトが存在しない。	新しいオブジェクトを作成します。

手順

ステップ 1 **Devices** > **Device Management**を選択します。

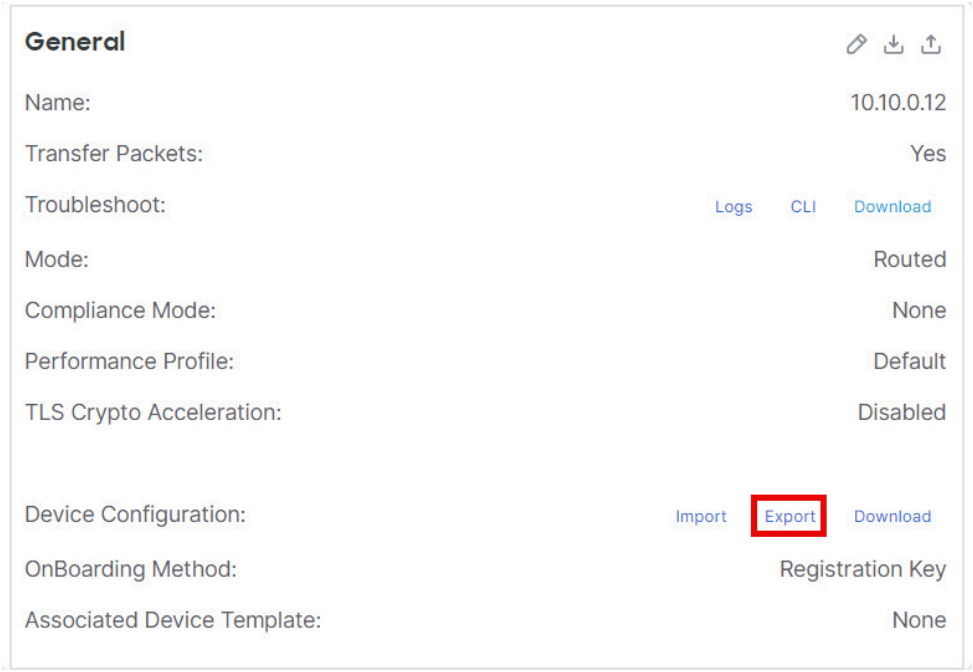
ステップ 2 編集するデバイスの横にある **Edit** (✎) をクリックします。

ステップ 3 [デバイス（Device）] をクリックします。

ステップ 4 設定をエクスポートします（設定のエクスポート）。

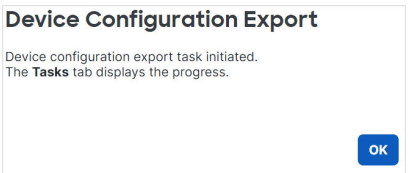
a) [General（全般）] エリアで [エクスポート（Export）] をクリックします。

図 *9*：デバイス設定のエクスポート



エクスポートを確認するよう求められます。[OK] をクリックします。

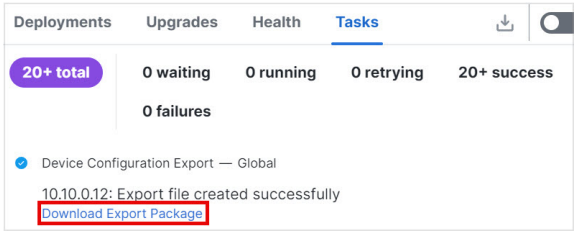
図 *10*：エクスポートの確認



[タスク（Tasks）] ページでエクスポートの進行状況を表示できます。

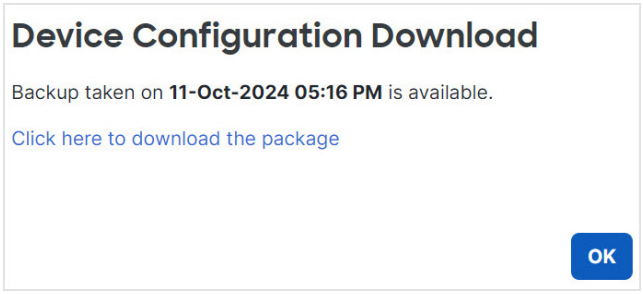
b) [通知（Notifications）]、[タスク（Tasks）] タブの順に選択します。エクスポートが完了したかどうかを確認したら、[エクスポートパッケージのダウンロード（Download Export Package）] をクリックします。または、[全般（General）] エリアの [ダウンロード（Download）] ボタンをクリックすることもできます。

図 *11* : タスクのエクスポート



パッケージをダウンロードするように求められます。[ここをクリックしてパッケージをダウンロード（Click here to download the package）] をクリックしてローカルでファイルを保存し、[OK] をクリックしてダイアログボックスを終了します。

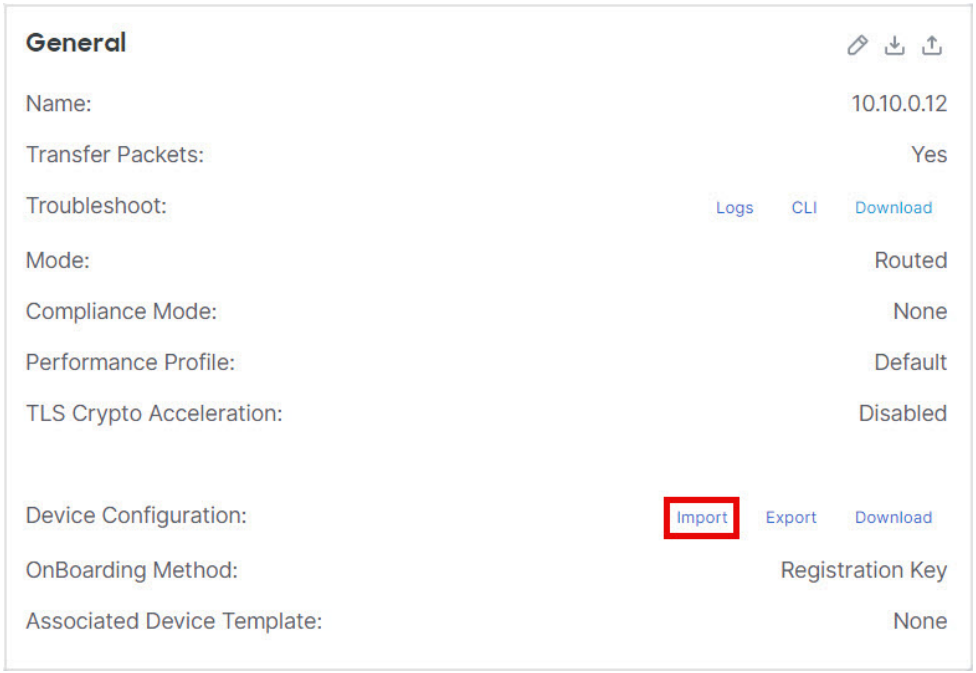
図 *12* : パッケージのダウンロード



ステップ 5 設定をインポートします。

a) [General（全般）] エリアで [インポート（Import）] をクリックします。

図 *13* : デバイス設定のインポート



現在の構成が置き換えられることを確認するよう求められます。[はい（Yes）] をクリックし、構成パッケージに移動します（接尾辞 .sfo が付いています。このファイルはバックアップファイルや復元ファイルとは異なることに注意してください）。

図 *14*：パッケージのインポート

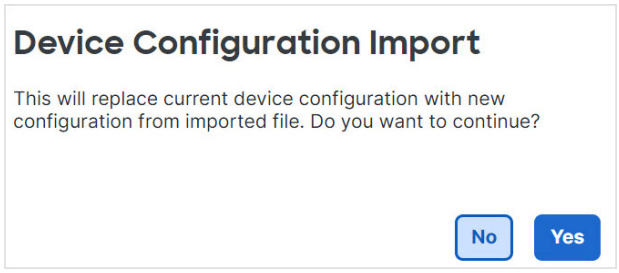
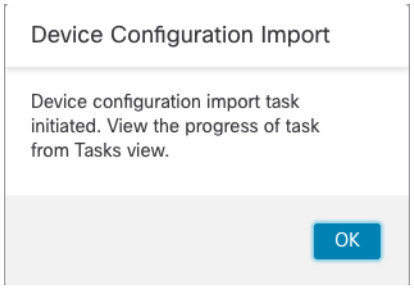


図 *15*：パッケージに移動

インポートを確認するよう求められます。[OK] をクリックします。

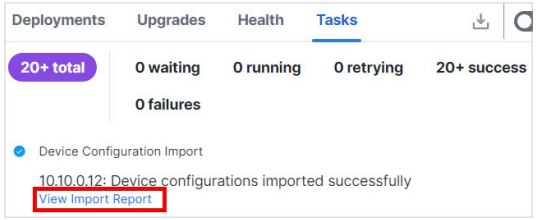
図 *16*：インポートの確認



[タスク（Tasks）] ページでインポートの進行状況を表示できます。

b) インポートレポートを表示して、何がインポートされたかを確認するには、[通知（Notifications）]、[タスク（Tasks）] タブの順に選択します。[インポートレポートの表示（View Import Report）] をクリックします。

図 *17*：インポートレポートの表示



[デバイス設定のインポートレポート（Device Configuration Import Reports）] ページには、利用可能なレポートへのリンクが表示されます。

Device	Shared Policies	Device Configurations
0ffeb830-740d-11ef-80f2-ac290f612121	Report does not exist	Device configurations import report

c) 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。

ライセンス設定の編集

[デバイス（Device）] ページの [ライセンス（License）] セクションでは、そのデバイスに対して有効になっているライセンスが表示されます。

Firewall Management Center で使用可能なライセンスがある場合、デバイスでそのライセンスを有効にすることができます。

手順

ステップ 1 **Devices** > **Device Management**を選択します。

ステップ 2 ライセンスを有効または無効にするデバイスの横にある**Edit** ( )をクリックします。

ステップ 3 [デバイス（Device）] をクリックします。

ステップ 4 [ライセンス（License）] セクションで、**Edit** ( )をクリックします。

ステップ 5 管理対象デバイスに対して有効または無効にするライセンスの横にあるチェックボックスをオンまたはオフにします。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

- 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。

システム情報の表示

[デバイス（Device）] ページの [システム（System）] セクションには、次の表に示すように、システム情報の読み取り専用テーブルが表示されます。

デバイスをシャットダウンまたは再起動することもできます。

図 *18 :* システム

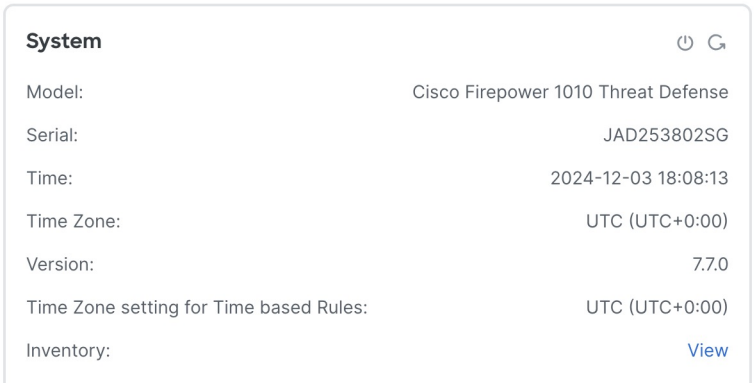


表 *3 : [*システム（*System*）*]* セクション テーブルのフィールド

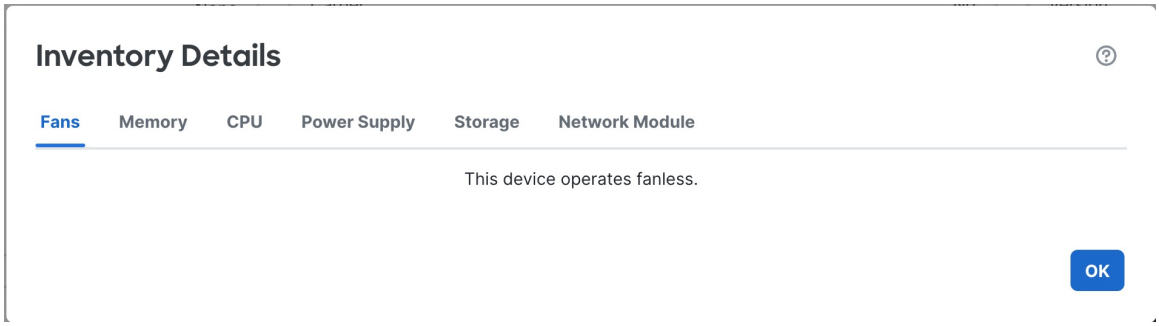
フィールド	説明
Shut Down Device ( )	デバイスをシャットダウンします。「デバイスのシャットダウンまたは再起動」を参照してください。
Restart Device ( )	デバイスを再起動します。「デバイスのシャットダウンまたは再起動」を参照してください。
モデル	管理対象デバイスのモデル名と番号。
シリアル（Serial）	管理対象デバイスのシャーシのシリアル番号。
Time	デバイスの現在のシステム時刻。
タイム ゾーン	タイムゾーンを表示します。
Version	管理対象デバイスに現在インストールされているソフトウェアのバージョン。
時刻ベースルールのタイムゾーン設定（Time Zone setting for time-based rules）	デバイスのプラットフォーム設定で指定されたタイムゾーンでの、デバイスの現在のシステム時刻。
インベントリ	インベントリの詳細を表示します。デバイス インベントリの表示を参照してください。

デバイス インベントリの表示

[システム（System）] セクションの **[インベントリ（Inventory）]** の横にある **[表示（View）]** をクリックして、デバイスインベントリのテーブル（[ファン（Fans）]、[メモリ（Memory）]、[CPU]、[電源（Storage）]、[ネットワークモジュール（Network Modules）]）を表示します。

インベントリの詳細テーブルには、製品識別子（PID）が割り当てられている Threat Defense デバイスにインストールされているすべてのシスコ製品に関する情報が表示されます。PID は、製品を注文できる製品名です。

図 *19 :* インベントリの詳細（*Inventory Details*）



検査エンジンの表示

[デバイス（Device）] ページの [検査エンジン（Inspection Engine）] セクションには、 のどちらを使用しているのかが表示されます。Snort 3 は、バージョン 7.7のデバイスで使用できる唯一のエンジンです。

正常性設定の編集

[デバイス（Device）] ページの [正常性（Health）] セクションには、以下の表に記載された情報が表示されます。

図 *20 :* 健全性

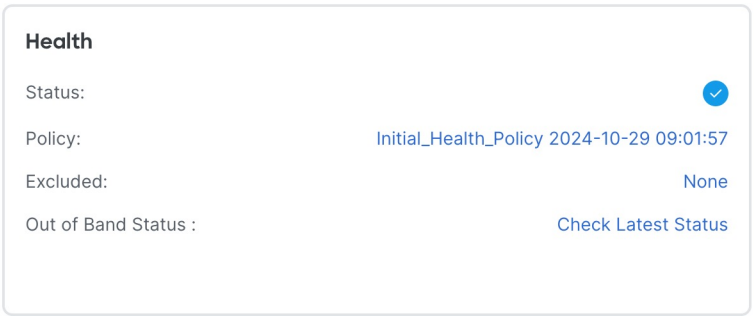


表 *4 : [*ヘルス（*Health*）*]* セクション テーブルのフィールド

フィールド	説明
ステータス	デバイスの現在のヘルス ステータスを表すアイコン。アイコンをクリックすると、アプライアンスのヘルス モニタが表示されます。

フィールド	説明
ポリシー	現在デバイスで展開されている、読み取り専用バージョンの正常性ポリシーへのリンク。
除外	**[正常性除外（Health Exclude）]** ページへのリンク。このページでは、正常性除外モジュールを有効化および無効化できます。
アウトオブバンドステータス	デバイスのCLIで行ったアウトオブバンド設定の変更を表示できる **[アウトオブバンド設定の詳細（Out-of-Band configuration details）]** ダイアログボックスへのリンク。構成の違いを確認し、次の展開までにFirewall Management Centerに保持する変更を手動で一致させる必要があります。「アウトオブバンド設定の検出 （19 ページ）」を参照してください。

アウトオブバンド設定の検出

デバイスへの管理接続が失われた場合は、デバイスCLIで選択設定を直接変更し、以下を行うことができます。

- マネージャアクセスにデータインターフェイスを使用している場合は、管理接続を復元します
- 接続が復元されるまで待つことができない選択設定の変更を行います

注意 リカバリまたは緊急時に必要なコマンドを知っていることが期待されます。この機能を使用して設定変更を実験しないでください。必要なコマンドがわからない場合や、コマンドの効果がわからない場合は、Cisco TAC に問い合わせて指示を受けることを推奨します。

管理接続が復元されると、Firewall Management Centerがデバイス上の設定変更を検出します。Firewall Management Centerでは、デバイス設定は自動的に更新されません。設定の違いを確認し、デバイス設定が異なることを確認してから、展開する前にFirewall Management Centerで同じ変更を手動で行う必要があります。

注意 確認後に展開すると、Firewall Management Center設定に存在しない設定は、デバイス上で上書きされます。

アウトオブバンド設定のガイドライン

リカバリ設定モードでサポートされる機能エリア

診断CLIでは、リカバリ設定モードで次の機能エリアを設定できます。

- インターフェイス

- スタティック ルート
- ダイナミックルーティング：BGP および OSPF
- プレフィルタ
- サイト間 VPN

他の診断 CLI コマンドと同様に、各コマンドの詳細については ASA のコマンドリファレンスを参照してください。

サポートされない機能

- マルチインスタンスモードではサポートされていません。
- EtherChannel を追加または削除できません。
- プラットフォームに依存する一部のインターフェイスコマンド（speed、duplex、fec など）はサポートされていません。

高可用性とクラスタリング

- リカバリ設定モードは、アクティブ/制御ノードでのみ使用できます。
- リカバリ設定モードのセッションを終了する前にフェールオーバーまたはクラスタスイッチオーバーが発生した場合は、Firewall Management Center で新しいアクティブ/制御ノードでの変更が検出されません。以前のすべての変更の検出をトリガーするために、新しいアクティブ/制御ノードでリカバリ設定モードを再度開始し、小さな変更を加えることを推奨します。これを行わないと、Firewall Management Center の変更を手動で照合しない場合、通知なく展開時に上書きされます。
- アクティブ/制御ノードでアウトオブバンド設定に変更を加えても、設定の同期前に、高可用性/クラスタが（フェールオーバー/クラスタ制御リンク障害のために複数のノードがアクティブ/制御になる）「スプリットブレイン」モードになり、高可用性/クラスタが正常な状態に戻り、別のノードがアクティブ/制御になったときに、設定の変更は失われます。
- アクティブなリカバリ設定モードのセッションがある場合、セッションが終了するまで、新しいノードは高可用性/クラスタに参加または再参加できません。

その他のガイドライン

- 既存のルールまたはルートを変更するには、既存のコマンドを、そのコマンドの **no** 形式を使用して削除してから、変更したルールを再度追加する必要があります。この方法により、競合とエラーを回避できます。次に例を示します。

  誤り：

```
firepower# show running-config route
route outside 10.0.0.0 255.0.0.0 20.1.1.1 1
firepower# configure recovery-config
```

```
 CAUTION: The config CLI is for emergency use only. Use the config CLI if the
management center is
unreachable, and use it only under exceptional circumstances, such as loss of
connectivity or
to restore manager access. Do not change management center's auto-generated
configurations.

 After your management center is reachable, manually make the same configuration
changes in the
management center. The management center cannot implement them automatically. When
you deploy
from the management center, out-of-band configuration changes will be overwritten.
Also, node join
will be blocked till config CLI session is active, so make sure to exit from the
config CLI after
changes are made.

Would you like to proceed ? [Y]es/[N]o: y
firepower(recovery-config)# route outside 10.0.0.0 255.0.0.0 30.1.1.1
firepower(recovery-config)# exit
Unsaved changes are not kept if you reboot.Save changes to memory ? [Y]es/[N]o: y
Cryptochecksum: ccfc11a8 4e46d55e 0c99b5ae 3b18a8f1

3939 bytes copied in 0.70 secs
firepower# show running-config route
route outside 10.0.0.0 255.0.0.0 20.1.1.1 1
route outside 10.0.0.0 255.0.0.0 30.1.1.1 1
firepower#
```

この場合、最初のルートが置き換えられる代わりに、2 番めのルートが追加されます。

正しい：

```
firepower# show running-config route
route outside 10.0.0.0 255.0.0.0 20.1.1.1 1
firepower# configure recovery-config

 CAUTION: The config CLI is for emergency use only. Use the config CLI if the
management center is
unreachable, and use it only under exceptional circumstances, such as loss of
connectivity or
to restore manager access. Do not change management center's auto-generated
configurations.

 After your management center is reachable, manually make the same configuration
changes in the
management center. The management center cannot implement them automatically. When
you deploy
from the management center, out-of-band configuration changes will be overwritten.
Also, node join
will be blocked till config CLI session is active, so make sure to exit from the
config CLI after
changes are made.

Would you like to proceed ? [Y]es/[N]o: y
firepower(recovery-config)# no route outside 10.0.0.0 255.0.0.0 20.1.1.1
firepower(recovery-config)# route outside 10.0.0.0 255.0.0.0 30.1.1.1
firepower(recovery-config)# exit
Unsaved changes are not kept if you reboot.Save changes to memory ? [Y]es/[N]o: y
Cryptochecksum: 81bcc51d 43771bbd 15b6dde6 afeb3442

3945 bytes copied in 0.70 secs
```

```
firepower# show running-config route
route outside 10.0.0.0 255.0.0.0 30.1.1.1 1
firepower#
```

- 自動ロールバックが有効になっており（展開設定の編集 （85 ページ）を参照）、展開のために管理接続が失われた場合は、アウトオブバンド設定を開始しないでください。代わりに、以前の展開への自動ロールバックが発生するまで 20 分間待つか、CLI で **configure policy rollback** コマンドを使用して手動でロールバックします（Firewall Management Center の接続が失われた場合の構成の手動ロールバック （70 ページ）を参照）。管理接続がまだダウンしている場合、自動ロールバックにより、アウトオブバンド設定の変更が上書きされます。
- プレフィルタルールの場合、完全に新しいルールを追加することは推奨しません（**access-control advanced** コマンド）。プレフィルタルールを侵入ポリシーおよびロギングと統合するには、ルール ID を生成して他のポリシーと統合する Firewall Management Center が必要です。
- リカバリ設定モードのすべてのセッションは、ユーザー名「enable_15」で syslog に記録されます。

診断 CLI でのリカバリ設定モードへのアクセス

診断 CLI のリカバリ設定モードを使用すると、管理接続がダウンしているときにアウトオブバンド設定を変更できます。必ず、Firewall Management Center で同じ変更を加えてください。ローカルでの変更は常に Firewall Management Center 展開によって上書きされます。

高可用性およびクラスタリングの場合は、アクティブ/制御ノードで変更を加えます。このモードは、マルチインスタンスモードではサポートされていません。

手順

ステップ 1 コンソールポートまたは SSH を使用してデバイス CLI に接続します。

「デバイスのコマンドラインインターフェイス（CLI）へのログイン」を参照してください。

ステップ 2 診断 CLI にアクセスします。

system support diagnostic-cli

enable（パスワードの入力を求められたら、パスワードを入力せずに Enter キーを押します）

例：

```
> system support diagnostic-cli
firepower> enable
Password:
```

ステップ 3 参照用に現在の実行構成を表示します。

show running-config

（注）
recovery-config モードでは、**show** コマンドを入力できません。

ステップ 4 recovery-config モードを開始します。

configure recovery-config

例：

```
firepower# configure recovery-config

 CAUTION: The config CLI is for emergency use only. Use the config CLI if the management
 center is
unreachable, and use it only under exceptional circumstances, such as loss of connectivity
 or
to restore manager access. Do not change management center's auto-generated configurations.


 After your management center is reachable, manually make the same configuration changes
 in the
management center. The management center cannot implement them automatically. When you
deploy
from the management center, out-of-band configuration changes will be overwritten. Also,
 node join
will be blocked till config CLI session is active, so make sure to exit from the config
 CLI after
changes are made.

Would you like to proceed ? [Y]es/[N]o: y
firepower(recovery-config)#
```

ステップ 5 一部の設定コマンドを入力できるようになりました。

使用可能なコマンドを表示するには、**?** を入力します。

サポートされている機能エリアについては、アウトオブバンド設定のガイドライン （19 ページ）を参照してください。

コマンドの詳細については、ASA の設定ガイドまたはコマンドリファレンスを参照してください。

ヒント
変更したすべてのコマンドを記録しておいてください。Firewall Management Center により差分が後で表示されますが、管理接続を復元するために反復的な変更を行う場合に備えて、コマンドの変更を記録しておくことをお勧めします。

例：

```
firepower(recovery-config)# ?

  access-list           Configure an access control element
  as-path               BGP autonomous system path filter
  bfd                   BFD configuration commands
  bfd-template          BFD template configuration
  cluster               Cluster configuration
  community-list        Add a community list entry
  crypto                Configure IPSec, ISAKMP, Certification authority, key
  end                   Exit from configure mode
  exit                  Exit from config mode
```

```
  extcommunity-list     Add a extended community list entry
  group-policy          Configure or remove a group policy
  interface             Select an interface to configure
  ip                    Configure IP address pools
  ipsec                 Configure transform-set, IPSec SA lifetime and PMTU
                        Aging reset timer
  ipv6                  Configure IPv6 address pools
  ipv6                  Global IPv6 configuration commands
  isakmp                Configure ISAKMP options
  jumbo-frame           Configure jumbo-frame support
  mac-address           MAC address options
  management-interface  Management interface
  mtu                   Specify MTU(Maximum Transmission Unit) for an interface

  no                    Negate a command or set its defaults

  policy-list           Define IP Policy list
  prefix-list           Build a prefix list
  route                 Configure a static route for an interface
  route-map             Create route-map or enter route-map configuration mode
  router                Enable a routing process
  sla                   IP Service Level Agreement
  sysopt                Set system functional options
  time-range            Define time range entries
  tunnel-group          Create and manage the database of connection specific
                        records for IPSec connections
  vpdn                  Configure VPDN feature
  vrf                   Configure a VRF
  zone                  Create or show a Zone
firepower(recovery-config)#
```

ステップ 6 リカバリ設定モードを終了すると、変更を保存するように求められます。有効モードに戻るまで、**exit** を入力して各サブモードを終了します。

変更をスタートアップコンフィギュレーションに保存するか、保存しないで実行コンフィギュレーションにのみ変更を保持するかを選択できます。実行コンフィギュレーションの変更は、再起動後は保持されません。後で追加の変更を加え、設定を保存する場合は、実行コンフィギュレーション全体が保存されるため、以前の変更もすべて保存されます。

リカバリ設定モードのセッションが開いている間は、展開がブロックされます。

例：

```
firepower(recovery-config)# interface Ethernet0/1
firepower(config-if)# ip address 10.0.0.2 255.0.0.0
firepower(config-if)# exit
firepower(recovery-config)# exit
Unsaved changes are not kept if you reboot. Save changes to memory ? [Y]es/[N]o: y

Cryptochecksum: 81a9073e f9535916 9c333d7e 9a3e5e76

3756 bytes copied in 0.70 secs
firepower#

Unsaved changes are not kept if you reboot. Save changes to memory ? [Y]es/[N]o:

Cryptochecksum: 81a9073e f9535916 9c333d7e 9a3e5e76

3756 bytes copied in 0.70 secs
firepower#
```

ステップ 7 Ctrl + A キーを押してから D キーを押して Firewall Threat Defense CLI に戻ります。**exit** を入力して各モードを終了することもできます。

（注）
最初にリカバリ設定モードを終了せずに Ctrl + A キーを押してから D キーを押して Firewall Threat Defense CLI に戻ると、リカバリ設定モードのセッションが開いたままになり、展開がブロックされます。

例：

```
firepower# exit

Logoff

User enable_1 logged in to firepower
Logins over the last 1 days: 4.  Last login: 20:42:51 UTC Dec 4 2024 from console
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
firepower> exit
Console connection detached.
>
```

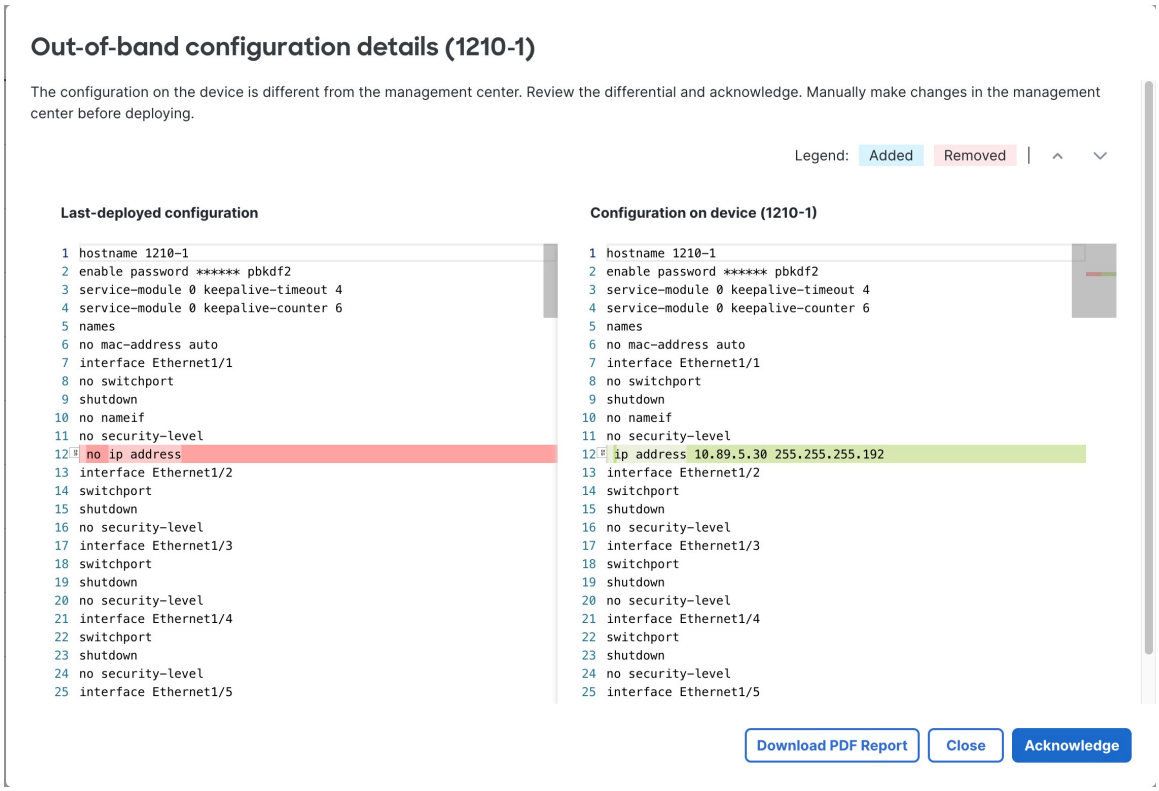
アウトオブバンド設定の確認

Firewall Management Center がデバイスのアウトオブバンド設定変更を検出した場合、変更を確認し、保持する Firewall Management Center 内の設定と照合する必要があります。変更を承認するまで、展開はブロックされます。

手順

ステップ 1 **[アウトオブバンド設定の詳細（Out-of-Band configuration details）]** ダイアログボックスを開きます。

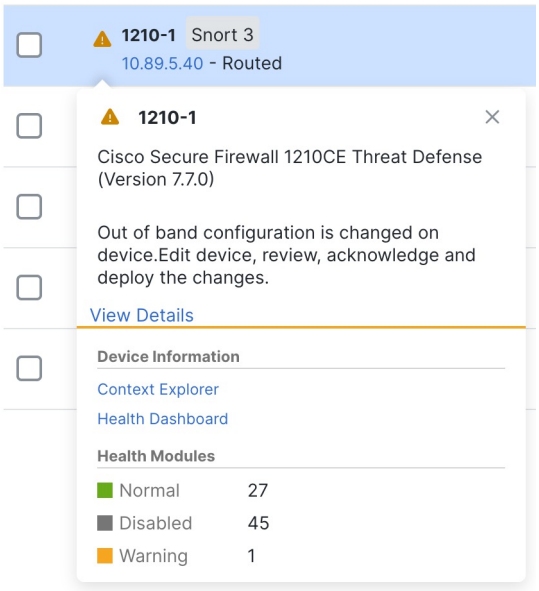
図 *21* : アウトオブバンド設定の詳細



（注）
一部のコマンドは、デフォルト設定に設定されている場合、コマンド出力に表示されません。ただし、デフォルトではないコマンドは、いずれかの側で緑（追加）または赤（削除）で表示されます。たとえば、recovery-config モードでインターフェイスに **no shutdown** を追加すると、**shutdown** コマンドは左側の **[最後に展開された設定（Last-deployed configuration）]** ペインに赤色で表示されますが、 **no shutdown** は右側の **[デバイスの設定（Configuration on device）]** ペインには表示されません 。この場合、インターフェイスのデフォルト設定は **shutdown**ですが、パーサーは **no shutdown** がデフォルトと見なして、表示しません。

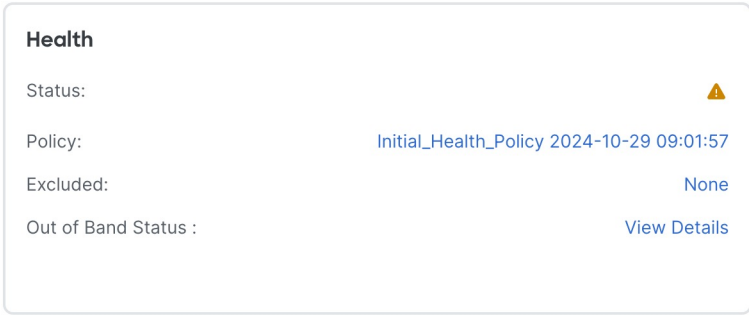
ダイアログボックスは、複数の場所から開くことができます。たとえば、**[デバイス（Devices）]**> **[デバイス管理（Device Management）]** ページには、デバイスの警告が表示されます。[詳細を表示（View Details）] をクリックします。

図 *22* : デバイス管理の警告



または、**[デバイス（Devices）]**>**[デバイス管理（Device Management）]**>**[デバイス（Device）]**>**[正常性（Health）]** タイルから **[詳細の表示（View Details）]** をクリックできます。

図 *23* : 正常性のアウトオブバンド ステータス確認



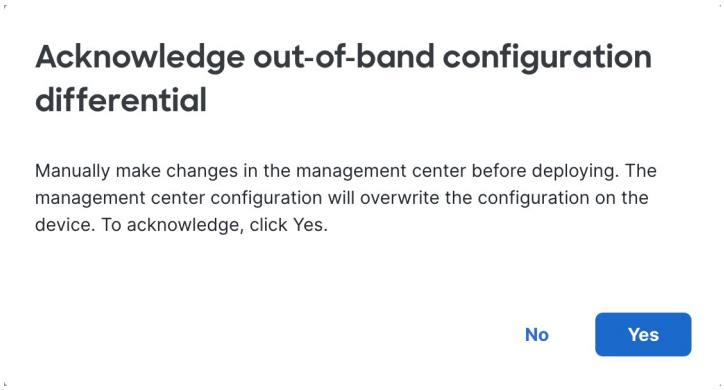
（注）
アウトオブバンド通知がまだ Firewall Management Centerに到達していない場合は、**[アウトオブバンドステータス（Out of Band Status ）]**>**[最新ステータスの確認（Check Latest Status）]** リンクを使用して変更を確認できます。

ステップ 2 **[PDF レポートのダウンロード（Download PDF Report）]** をクリックすると、ダイアログ ボックスを閉じた後に行う必要がある設定の変更を参照できます。

または、いつでもダイアログボックスを表示して、変更を確認できます。

ステップ 3 **[異常の承認（Acknowledge anomalies）]** をクリックし、**[はい（Yes）]** をクリックします。

図 *24 :* 確認

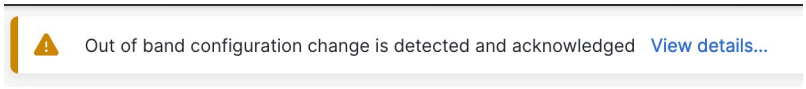


設定変更を行った後の誤った展開を防止したい場合には、すぐに変更する代わりに、戻って **[確認（Acknowledge）]**をクリックすることができます。

ステップ 4 **[閉じる（Close）]** をクリックして、**[アウトオブバンド設定の詳細（Out-of-Band configuration details）]** ダイアログボックスを閉じます。

展開するまでは、再度ダイアログボックスにアクセスして、必要な変更を確認できます。[デバイス（Device）] ページのステータスが変わり、アウトオブバンド設定が承認されたことが示されます。

図 *25 :* 承認ステータス

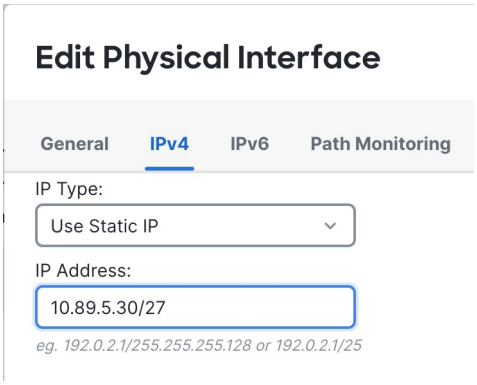


ステップ 5 CLI で行った設定変更を実施します。

構成 CLI を Firewall Management Center 画面に一致させる必要があります。 CLI の変更から画面への直接リンクはありません。

変更を保持しない場合は、単に展開してデバイス設定を上書きできます。管理接続を維持するために必要なすべての変更と、保持するその他の変更を行う必要があります。たとえば、CLI での IP アドレスを変更した場合は、**[インターフェイス（Interfaces）]** ページに移動してインターフェイスを編集し、次のように一致する IP アドレスを設定する必要があります。

図 *26 : IP* アドレス変更の照合



同じ変更を行ったことを確認するメカニズムはありません。必要に応じて、異なる IP アドレスを設定できます。

ステップ 6 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。

展開後、 **System** (⚙) > **Monitoring** > **Audit** ページで、設定の差分（変更の有無にかかわらず）を表示できます。**[デバイス（Device）] > [デバイス管理（Device Management）] > [アウトオブバンド変更（Out of band changes）]** でサブシステムを確認します。

管理設定の編集

これらの設定は、Firewall Management Center とデバイスとの管理接続の確立方法を制御します。

冗長マネージャアクセス用データインターフェイスの設定

マネージャアクセスにデータインターフェイスを使用する場合、プライマリインターフェイスがダウンしたときに管理機能を引き継ぐよう、セカンダリインターフェイスを構成できます。セカンダリインターフェイスは1つだけ構成できます。デバイスは、SLA モニタリングを使用して、スタティックルートの実行可能性と、両方のインターフェイスを含むECMP ゾーンを追跡し、管理トラフィックで両方のインターフェイスが使用できるようにします。

始める前に

- セカンダリインターフェイスは、プライマリインターフェイスとは別のセキュリティゾーンにある必要があります。
- プライマリインターフェイスに適用されるのと同じすべての要件がセカンダリインターフェイスに適用されます。管理のための Firewall Threat Defense データインターフェイスの使用について を参照してください。

手順

ステップ 1 **Devices** > **Device Management** ページで、デバイスの **Edit** (✎) をクリックします。

ステップ 2 セカンダリインターフェイスのマネージャアクセスを有効にします。

この設定は、インターフェイスの有効化、名前の設定、セキュリティゾーンの設定、スタティック IPv4 アドレスの設定など、標準のインターフェイス設定に加えて行うものです。

a) **[インターフェイス（Interfaces）]** > **[物理インターフェイスの編集（Edit Physical Interface）]** > **[マネージャアクセス（Manager Access）]**を選択します。
b) [このインターフェイス上の管理をマネージャに対して有効にする（Enable management on this interface for the Manager）] をオンにします。
c) [OK] をクリックします。

どちらのインターフェイスも、インターフェイスリストに[（マネージャアクセス）（(Manager Access)）] と表示されます。

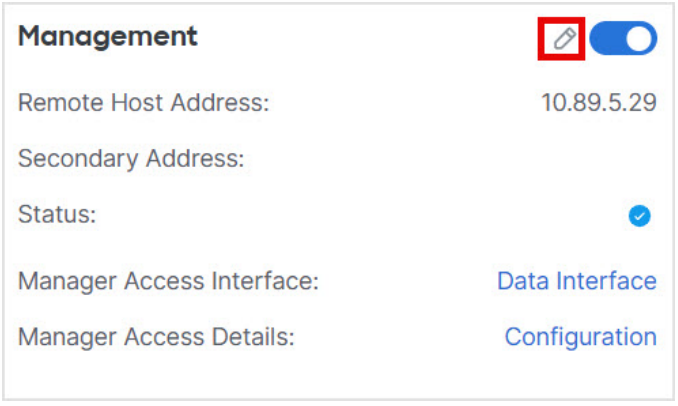
図 *27:* インターフェイスリスト

Interface	Logical Name	Type	Security Zones
Diagnostic1/1	diagnostic	Physical	
Ethernet1/1 (Manager Access)	outside	Physical	outside
Ethernet1/2		Physical	
Ethernet1/3		Physical	
Ethernet1/4		Physical	
Ethernet1/5		Physical	
Ethernet1/6		Physical	
Ethernet1/7		Physical	
Ethernet1/8 (Manager Access)	redundant	Physical	mgmt

ステップ 3 [管理（Management）] 設定にセカンダリアドレスを追加します。

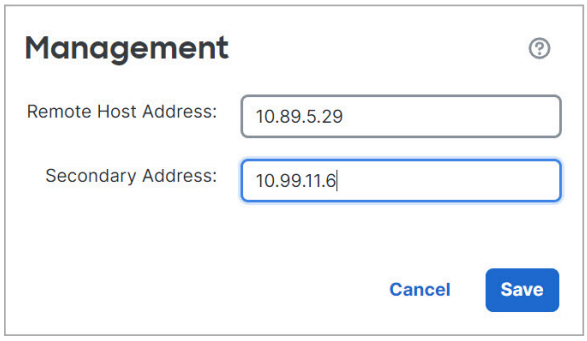
a) [Device] をクリックし、[Management] 領域を表示します。
b) [.] をクリックします。**Edit** (✎)

図 *28* : 管理アドレスの編集



c) [管理（Management）] ダイアログボックスで、[セカンダリアドレス（Secondary Address）] フィールドの名前または IP アドレスを変更します。

図 *29* : 管理 *IP* アドレス

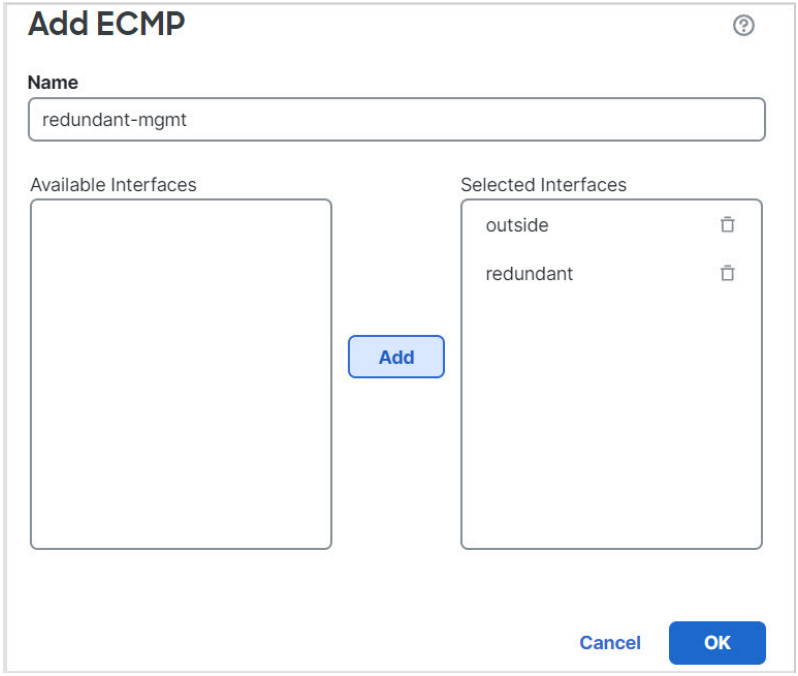


d) [保存（Save）] をクリックします。

ステップ 4 両方のインターフェイスで ECMP ゾーンを作成します。

a) [ルーティング（Routing）] をクリックします。
b) 仮想ルータドロップダウンから、プライマリインターフェイスとセカンダリインターフェイスが存在する仮想ルータを選択します。
c) [ECMP] をクリックし、[追加（Add）] をクリックします。
d) [名前（Name）] に ECMP ゾーンの名前を入力します。
e) [使用可能なインターフェイス（Available Interfaces）] ボックスでプライマリおよびセカンダリインターフェイスを選択し、[追加（Add）] をクリックします。

図 *30 : ECMP* ゾーンの追加

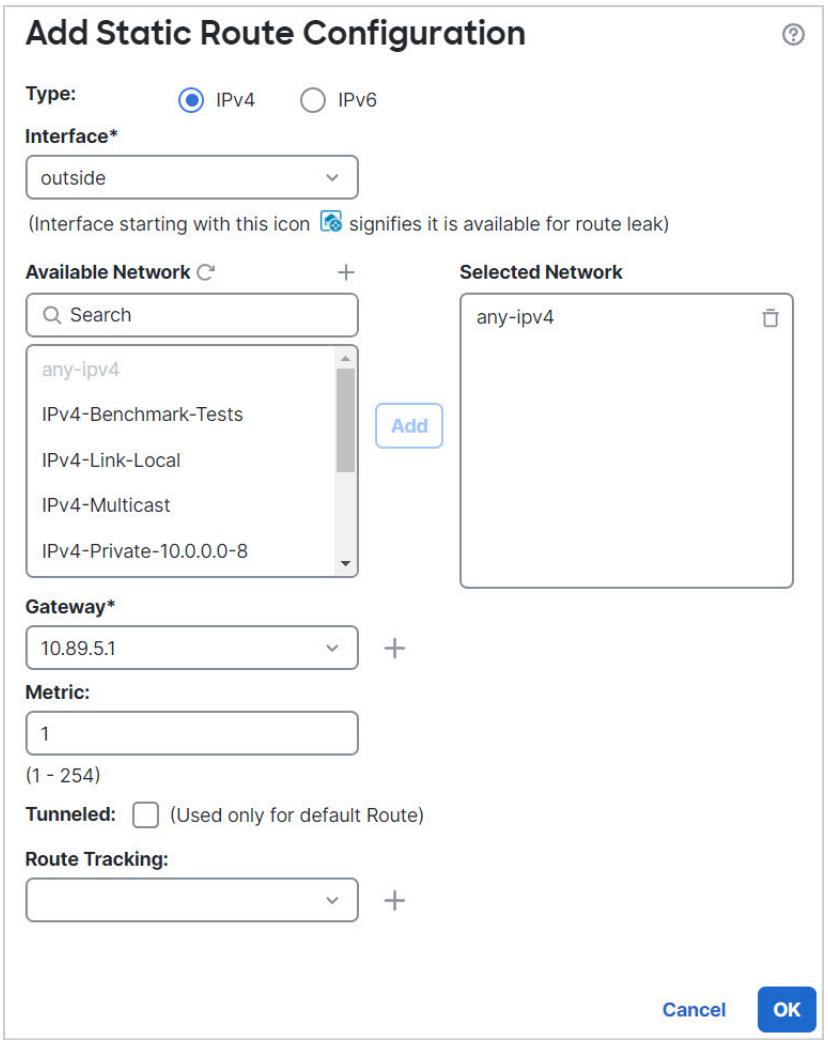


f) [OK] をクリックし、[保存（Save）] をクリックします。

ステップ 5 両方のインターフェイスに等コストのデフォルト スタティック ルートを追加し、両方で SLA トラッキングを有効にします。

ルートは、ゲートウェイを除いて同一であり、両方のメトリックが 1 である必要があります。プライマリインターフェイスには、編集可能なデフォルトルートがすでに存在している必要があります。

図 *31 : Add/Edit Static Route*



a) [Static Route] をクリックします。

b) [ルートを追加（Add Route）] をクリックして新しいルートを追加するか、既存のルートの場合は **Edit** ( )をクリックします。

c) [インターフェイス（Interface）] ドロップダウンリストから、インターフェイスを選択します。

d) 宛先ネットワークとして、[使用可能なネットワーク（Available Networks）] ボックスから [any-ipv4] を選択し、[追加（Add）] をクリックします。

e) デフォルトの [ゲートウェイ（Gateway）] を入力します。

f) [ルートトラッキング（Route Tracking）] の場合、**Add** ( )をクリックして新しい SLA モニターオブジェクトを追加します。

g) 次を含む必要なパラメータを入力します。

- Firewall Management Center IP アドレスとしての [モニターアドレス（Monitor Address）]。

- [使用可能なゾーン（Available Zones）]のプライマリまたはセカンダリ管理インターフェイスのゾーン。たとえば、プライマリインターフェイスオブジェクトには外部ゾーンを選択し、セカンダリインターフェイスオブジェクトには管理ゾーンを選択します。

詳細については、SLA モニタを参照してください。

図 ***32 : SLA*** モニターの追加

h) [保存（Save）] をクリックし、[ルートトラッキング（Route Tracking）] ドロップダウンリストで、作成した SLA オブジェクトを選択します。
i) [OK] をクリックし、[保存（Save）] をクリックします。
j) もう一方の管理インターフェイスのデフォルトルートについてこの手順を繰り返します。

ステップ 6 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。

この機能の展開において、Firewall Management Center は管理トラフィック用のセカンダリインターフェイスを有効にします。これには、管理トラフィックが適切なデータインターフェイスに到達するための自動生成されたポリシーベースのルーティング構成が含まれます。Firewall Management Center は、**configure network management-data-interface** コマンドの 2 番目のインスタンスも展開します。CLI でセカンダリインターフェイスを編集する場合、ゲートウェイを設定したり、デフォルトルートを変更したりすることはできません。このインターフェイスのスタティックルートは Firewall Management Center でしか編集できません。

マネージャ アクセス インターフェイス設定の変更

デバイスまたは Firewall Management Center のマネージャ インターフェイス設定を変更すると、管理接続が中断される可能性があります。インターフェイス設定を変更して管理接続を再確立するには、次のシナリオを参照してください。

デバイス IP アドレスの変更

デバイス IP アドレスを変更し、Firewall Management Center のアドレスを更新します。

デバイス IP アドレスの設定

次のいずれかの方法を使用して、マネージャ アクセス インターフェイスの IP アドレスを設定します。

Firewall Threat Defense 管理インターフェイスの *CLI* での変更

CLI を使用して、管理対象デバイスの管理インターフェイスの設定を変更します。これらの設定の多くは、初期セットアップ時に設定されたものです。この手順に従うことで、それらの設定を変更でき、さらに設定を追加できます（例：モデルでサポートされる場合にイベントインターフェイスを有効化する、スタティック ルートを追加する）。

（注） このトピックは、専用管理インターフェイスに適用されます。代わりに、管理用のデータインターフェイスを設定することもできます。このインターフェイスのネットワーク設定を変更する場合は、CLI ではなく Firewall Management Center 内で行う必要があります。切断された管理接続をトラブルシューティングする必要があり、Firewall Threat Defense で直接変更する必要がある場合は、管理に使用される Firewall Threat Defense データインターフェイスの CLI での変更 （43 ページ） を参照してください。

Firewall Threat Defense CLI の詳細については、*Cisco Secure Firewall Threat Defense Command Reference* を参照してください。

（注） SSH を使用する際は、慎重に管理インターフェイスに変更を加えてください。構成エラーで再接続できなくなると、デバイスのコンソール ポートへのアクセスが必要になります。

（注） デバイス管理 IP アドレスを変更する場合は、**configure manager add** コマンド（新しい Management Center への登録 を参照）を使用してデバイスの初期設定時に Firewall Management Center を特定した方法に応じて、Firewall Management Center 接続に関する次のタスクを参照してください。

- **IP アドレス—アクションなし。**到達可能な IP アドレスを使用して Firewall Management Center を特定した場合、管理接続は数分後に自動的に再確立されます。情報の同期を維持するために、Firewall Management Center に表示されるデバイス IP アドレスも変更することを推奨します。Firewall Management Center でのホスト名または IP アドレスの更新 （49 ページ） を参照してください。このアクションは、接続の再確立を高速化するのに役立ちます。**注**：到達不能な Firewall Management Center IP アドレスを指定した場合は、以下の NAT ID の手順を参照してください。
- **NAT IDのみ：接続を手動で再確立。**NAT ID のみを使用して Firewall Management Center を識別した場合、接続は自動的に再確立されません。この場合、Firewall Management Center でのホスト名または IP アドレスの更新 （49 ページ） に従って Firewall Management Center のデバイス管理 IP アドレスを変更します。

（注） 高可用性構成では、登録されたデバイスの管理 IP アドレスをデバイスの CLI または Firewall Management Center から変更した場合、高可用性同期後も、スタンバイ Firewall Management Center には変更が反映されません。スタンバイ Firewall Management Center も確実に更新されるようにするには修正します。

始める前に

- **configure user add** コマンドを使用して CLI にログイン可能なユーザー アカウントを作成できます。次を参照してください：CLI での内部ユーザーの追加外部認証に従って AAA ユーザーを設定することもできます。

手順

ステップ 1 コンソール ポートから、または SSH を使用して、デバイス CLI に接続します。

「デバイスのコマンドラインインターフェイス（CLI）へのログイン」を参照してください。

ステップ 2 管理者のユーザー名とパスワードでログインします。

ステップ 3 （Firepower 4100/9300/Secure Firewall 4200 のみ）セカンダリ管理インターフェイスをイベント専用インターフェイスとして有効にします。

configure network management-interface enable management1

configure network management-interface disable-management-channel management1

管理トラフィック用の管理インターフェイスが常に必要です。デバイスに 2 番目の管理インターフェイスがある場合は、イベント専用トラフィックに対してそのインターフェイスを有効にすることができます。

必要に応じて、**configure network management-interface disable-events-channel** コマンドを使用してメイン管理インターフェイスのイベントを無効にできます。いずれの場合も、デバイスは、イベントのみのインターフェイス上でイベントを送信しようとします。そのインターフェイスがダウンしていた場合は、イベントチャネルが無効になっていても、管理インターフェイス上でイベントを送信します。

インターフェイス上でイベントチャネルと管理チャンネルの両方を無効にすることはできません。

別のイベントインターフェイスを使用するには、Firewall Management Center でイベントインターフェイスを有効にする必要もあります。*Cisco Secure Firewall Management Center Administration Guide*を参照してください。

例：

```
> configure network management-interface enable management1
Configuration updated successfully

> configure network management-interface disable-management-channel management1
Configuration updated successfully

>
```

ステップ 4 管理インターフェイスまたはイベントインターフェイスの IP アドレスを設定します。

management_interface 引数を指定しない場合は、デフォルトの管理インターフェイスのネットワーク設定を変更します。イベントインターフェイスを設定する際は、必ず*management_interface* 引数を指定してください。イベントインターフェイスは、管理インターフェイスの個別のネットワーク、または同じネットワークに配置できます。自分で設定するインターフェイスに接続すると、切断されます。新しい IP アドレスに再接続できます。

a) IPv4 アドレスを設定します。

- 手動設定

  configure network ipv4 manual *ip_address netmask gateway_ip* [*management_interface*]

  このコマンド内の *gateway_ip* は、デバイスのデフォルトルートを作成するために使用されることに注意してください。イベント専用インターフェイスを設定する場合は、コマンドの一部として *gateway_ip* を入力する必要があります。ただし、このエントリ

は、指定した値にデフォルトルートを設定するだけで、イベントインターフェイスの個別のスタティックルートは作成しません。管理インターフェイスと別のネットワークでイベント専用インターフェイスを使用している場合は、管理インターフェイスと共に使用するように *gateway_ip* を設定し、**configure network static-routes** コマンドを使用してイベント専用インターフェイス用に個別にスタティックルートを作成することを推奨します。

例：

```
> configure network ipv4 manual 10.10.10.45 255.255.255.0 10.10.10.1 management1
Setting IPv4 network configuration.
Network settings changed.

>
```

- DHCP（デフォルト管理インターフェイスのみでサポート）。

  configure network ipv4 dhcp

b) IPv6 アドレスを設定します。

- ステートレス自動設定

  configure network ipv6 router [*management_interface*]

  例：

```
> configure network ipv6 router management0
Setting IPv6 network configuration.
Network settings changed.

>
```

- 手動設定

  configure network ipv6 manual *ip6_address ip6_prefix_length* [*ip6_gateway_ip*] [*management_interface*]

  このコマンド内の *ipv6_gateway_ip* は、デバイスのデフォルトルートを作成するために使用されることに注意してください。イベント専用インターフェイスを設定する場合は、コマンドの一部として *ipv6_gateway_ip* を入力する必要があります。ただし、このエントリは、指定した値にデフォルトルートを設定するだけで、イベントインターフェイスの個別のスタティックルートは作成しません。管理インターフェイスと別のネットワークでイベント専用インターフェイスを使用している場合は、管理インターフェイスと共に使用するように *ipv6_gateway_ip* を設定し、**configure network static-routes** コマンドを使用してイベント専用インターフェイス用に個別にスタティックルートを作成することを推奨します。

  例：

```
> configure network ipv6 manual 2001:0DB8:BA98::3210 64 management1
Setting IPv6 network configuration.
Network settings changed.
```

```
>
```

- DHCPv6（デフォルト管理インターフェイスのみでサポート）。

  configure network ipv6 dhcp

ステップ 5 IPv6 の場合、ICMPv6 エコー応答と宛先到達不能メッセージを有効または無効にします。デフォルトでは、これらのメッセージは有効になっています。

configure network ipv6 destination-unreachable {**enable** | **disable**}

configure network ipv6 echo-reply {**enable** | **disable**}

これらのパケットを無効にすることで、サービス拒否攻撃の可能性から保護します。エコー応答パケットを無効にすると、デバイスの管理インターフェイスにテスト目的で IPv6 ping を使用できなくなります。

例：

```
> configure network ipv6 destination-unreachable disable
> configure network ipv6 echo-reply disable
```

ステップ 6 デフォルト管理インターフェイスの DHCP サーバーが、接続されているホストに IP アドレスを提供することを可能にします。

configure network ipv4 dhcp-server-enable *start_ip_address end_ip_address*

例：

```
> configure network ipv4 dhcp-server-enable 10.10.10.200 10.10.10.254
DHCP Server Enabled

>
```

管理インターフェイスの IP アドレスを手動で設定するときにのみ、DHCP サーバーを設定できます。このコマンドは、Firewall Management Center Virtual ではサポートされません。DHCP サーバーのステータスを表示するには、**show network-dhcp-server** を入力します。

```
> show network-dhcp-server
DHCP Server Enabled
10.10.10.200-10.10.10.254
```

ステップ 7 Firewall Management Center がリモート ネットワーク上にある場合は、イベント専用インターフェイスのスタティック ルートを追加します。追加しないと、すべてのトラフィックが管理インターフェイスを通じてデフォルト ルートと一致します。

configure network static-routes {**ipv4** | **ipv6**} **add** *management_interface destination_ip netmask_or_prefix gateway_ip*

デフォルトルートの場合は、このコマンドを使用しないでください。デフォルト ルート ゲートウェイの IP アドレスの変更は、**configure network ipv4** コマンドまたは **ipv6** コマンドを使用した場合のみ可能です（「ステップ 4 （38 ページ）」を参照）。

例：

```
> configure network static-routes ipv4 add management1 192.168.6.0 255.255.255.0 10.10.10.1
Configuration updated successfully

> configure network static-routes ipv6 add management1 2001:0DB8:AA89::5110 64
2001:0DB8:BA98::3211
Configuration updated successfully

>
```

スタティック ルートを表示するには、**show network-static-routes** を入力します（デフォルトルートは表示されません）。

```
> show network-static-routes
---------------[ IPv4 Static Routes ]---------------
Interface                 : management1
Destination               : 192.168.6.0
Gateway                   : 10.10.10.1
Netmask                   : 255.255.255.0
[…]
```

ステップ 8 ホスト名の設定

configure network hostname *name*

例：

```
> configure network hostname farscape1.cisco.com
```

Syslog メッセージは、再起動するまで新しいホスト名を反映しません。

ステップ 9 検索ドメインを設定します。

configure network dns searchdomains *domain_list*

例：

```
> configure network dns searchdomains example.com,cisco.com
```

カンマで区切ったデバイスの検索ドメインを設定します。これらのドメインは、コマンド（**ping system** など）に完全修飾ドメイン名を指定しない場合にホスト名に追加されます。ドメインは、管理インターフェイスまたは管理インターフェイスを経由するコマンドでのみ、使用されます。

ステップ 10 カンマで区切った 3 つの DNS サーバーを設定します。

configure network dns servers *dns_ip_list*

例：

```
> configure network dns servers 10.10.6.5,10.20.89.2,10.80.54.3
```

ステップ 11 Firewall Management Center で通信のリモート管理ポートを設定します。

configure network management-interface tcpport *number*

例：

```
> configure network management-interface tcpport 8555
```

Firewall Management Center および管理対象デバイスは、双方向の TLS-1.3 暗号化通信チャネル（デフォルトではポート 8305）を使用して通信します。マルチインスタンスモードを使用している場合は、管理ポートを変更しないでください。ポート 8305 のみがサポートされます。

（注）
シスコは、リモート管理ポートをデフォルト設定のままにしておくことを**強く**推奨していますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。管理ポートを変更する場合は、導入内の相互に通信する必要がある**すべての**デバイスの管理ポートを変更する必要があります。

ステップ 12 （Firewall Threat Defense のみ）管理インターフェイスまたはイベントインターフェイスの MTU を設定します。デフォルトの MTU は 1500 バイトです。

configure network mtu [*bytes*] [*interface_id*]

- *bytes*：MTU をバイト単位で設定します。管理インターフェイスでは、IPv4 を有効にした場合は 64ー1500、IPv6 を有効にした場合は 1280ー1500 の値を指定できます。イベントインターフェイスでは、IPv4 を有効にした場合は 64ー9000、IPv6 を有効にした場合は 1280ー9000 です。IPv4 と IPv6 の両方を有効にした場合、最小値は 1280 です。*bytes* を入力しない場合、値の入力を求められます。
- *interface_id*：MTU を設定するインターフェイス ID を指定します。プラットフォームに応じて使用可能なインターフェイス ID（management0、management1、br1、eth0など）を表示するには、**show network** コマンドを使用します。インターフェイスを指定しない場合は、管理インターフェイスが使用されます。

例：

```
> configure network mtu 8192 management1
MTU set successfully to 1500 from 8192 for management1
Refreshing Network Config...
NetworkSettings::refreshNetworkConfig MTU value at start 8192

Interface management1 speed is set to '10000baseT/Full'
NetworkSettings::refreshNetworkConfig MTU value at end 8192
>
```

ステップ 13 HTTP プロキシを設定します。デバイスは、ポート TCP/443（HTTPS）および TCP/80（HTTP）でインターネットに直接接続するように設定されています。HTTP ダイジェスト経由で認証できるプロキシ サーバを使用できます。コマンド発行後に、HTTP プロキシのアドレスとポート、プロキシの認証が必要かどうかをユーザーは尋ねられます。認証が必要な場合はプロキシ

のユーザー名、プロキシのパスワード、およびプロキシのパスワードの確認を入力するよう要求されます。

（注）
Firewall Threat Defense のプロキシパスワードには、A～Z、a～z と 0～9 の文字のみを使用できます。

configure network http-proxy

例：

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address: 10.100.10.10
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]: Y
Enter Proxy Username: proxyuser
Enter Proxy Password: proxypassword
Confirm Proxy Password: proxypassword
```

ステップ 14 デバイス管理 IP アドレスを変更する場合は、**configure manager add** コマンド（新しい Management Center への登録 を参照）を使用してデバイスの初期設定時に Firewall Management Center を特定した方法に応じて、Firewall Management Center 接続に関する次のタスクを参照してください。

- **IP アドレス—アクションなし。**到達可能な IP アドレスを使用して Firewall Management Center を特定した場合、管理接続は数分後に自動的に再確立されます。情報の同期を維持するために、Firewall Management Center に表示されるデバイス IP アドレスも変更することを推奨します。Firewall Management Center でのホスト名または IP アドレスの更新 （49 ページ） を参照してください。このアクションは、接続の再確立を高速化するのに役立ちます。**注**：到達不能な Firewall Management Center IP アドレスを指定した場合は、Firewall Management Center でのホスト名または IP アドレスの更新 （49 ページ） を使用して手動で接続を再確立する必要があります。
- **NAT IDのみ：接続を手動で再確立。**NAT ID のみを使用して Firewall Management Center を識別した場合、接続は自動的に再確立されません。この場合、Firewall Management Center でのホスト名または IP アドレスの更新 （49 ページ） に従って Firewall Management Center のデバイス管理 IP アドレスを変更します。

管理に使用される *Firewall Threat Defense* データインターフェイスの *CLI* での変更

Firewall Threat Defense と Firewall Management Center の間の管理接続が中断され、古いインターフェイスを置き換える新しいデータインターフェイスを指定する場合は、Firewall Threat Defense CLI を使用して新しいインターフェイスを設定します。

管理接続がアクティブな場合は、Firewall Management Center を使用して既存のデータインターフェイスを変更する必要があります（GUI で [管理（Management）] に使用する Firewall Threat Defense データインターフェイスを修正する （46 ページ） を参照）。データ管理インターフェ

イスの初期設定については、「CLI を使用した Firewall Threat Defense 初期設定の実行の完了」の **configure network management-data-interface** コマンドを参照してください。

ハイアベイラビリティペアの場合は、両方のユニットですべての CLI 手順を実行します。Firewall Management Center 内では、アクティブユニットでのみ手順を実行します。設定の変更が展開されると、スタンバイユニットはアクティブユニットから設定およびその他のステート情報を同期します。

（注） このトピックは、専用の管理インターフェイスではなく、管理用に設定したデータインターフェイスに適用されます。管理インターフェイスのネットワーク設定を変更する場合は、Firewall Threat Defense 管理インターフェイスの CLI での変更 （36 ページ）を参照してください。

Firewall Threat Defense CLI の詳細については、*Cisco Secure Firewall Threat Defense Command Reference* を参照してください。

手順

ステップ 1 データ管理インターフェイスを新しいインターフェイスに変更する場合は、現在のインターフェイスケーブルを新しいインターフェイスに移動します。

ステップ 2 デバイスの CLI に接続します。

これらのコマンドを使用する場合は、コンソールポートを使用する必要があります。初期設定の実行中に、管理インターフェイスから切断される可能性があります。管理接続が中断されたために設定を編集しており、専用管理インターフェイスに SSH アクセスできる場合は、その SSH 接続を使用できます。

「デバイスのコマンドラインインターフェイス（CLI）へのログイン」を参照してください。

ステップ 3 **admin** のユーザー名とパスワードでログインします。

ステップ 4 インターフェイスを無効にして、設定を再構成できるようにします。

configure network management-data-interface disable

（注）
同じインターフェイスで新しい IPv4 アドレスを設定するだけで、その他の変更は行わない場合は、この手順をスキップできます。その他の変更では、最初にインターフェイスを無効にする必要があります。

例：

```
> configure network management-data-interface disable

 Configuration updated successfully..!!


Configuration disable was successful, please update the default route to point to a
gateway on management interface using the command 'configure network'
```

ステップ 5 マネージャアクセス用の新しいデータインターフェイスを設定します。

configure network management-data-interface

その後、データインターフェイスの基本的なネットワーク設定を行うように求めるプロンプトが表示されます。

データ管理インターフェイスを同じネットワーク上の新しいインターフェイスに変更する場合は、インターフェイス ID を除き、前のインターフェイスと同じ設定を使用します。さらに、**Do you wish to clear all the device configuration before applying ? (y/n) [n]:** オプションに **y** を選択します。この選択により、古いデータ管理インターフェイスの設定がクリアされるため、IP アドレスとインターフェイス名を新しいインターフェイスで正常に再利用できます。

```
> configure network management-data-interface
Data interface to use for management: ethernet1/4
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]: y

Configuration done with option to allow manager access from any network, if you wish to
 change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

ステップ 6 （任意）特定のネットワーク上の Firewall Management Center へのデータ インターフェイス アクセスを制限します。

configure network management-data-interface client *ip_address netmask*

デフォルトでは、すべてのネットワークが許可されます。

ステップ 7 Firewall Management Center でのホスト名または IP アドレスの更新 （49 ページ）。

接続は自動的に再確立されますが、Firewall Management Center で接続を無効にしてから再度有効にすると、接続の再確立を速く実行できます。または、リンクされた手順を実行して、Firewall Management Center でデバイスのIPアドレスを更新する必要があります。

ステップ 8 管理接続が再確立されたことを確認します。

sftunnel-status-brief

アップ状態の接続の出力例を次に示します。ピアチャネルとハートビート情報が表示されています。

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
```

```
 via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

ステップ 9 Firewall Management Center で、**Devices** > **Device Management**、**Edit** (✎) の順に選択します。[デバイス（Device）] 領域の [管理（Management）] フィールドで、**[マネージャアクセス - 構成の詳細（Manager Access - Configuration Details）]** の横にある [更新（Refresh）] をクリックします。

Firewall Management Center はインターフェイスとデフォルトルートの設定変更を検出し、デバイスへの展開をブロックします。デバイスのデータインターフェイス設定をローカルで変更する場合は、Firewall Management Center でそれらの変更を手動で調整する必要があります。[構成（Configuration）] タブで、Firewall Management Center とデバイスの不一致を確認できます。

ステップ 10 [インターフェイス（Interfaces）] を選択して、次の変更を行います。

a) 古いデータ管理インターフェイスから IP アドレスと名前を削除し、このインターフェイスのマネージャアクセスを無効にします。

b) 新しい設定（CLI で使用したインターフェイス）が適用された新しいデータ管理インターフェイスを構成し、それに対して、マネージャアクセスを有効にします。

ステップ 11 [ルーティング（Routing）]、[スタティックルート（Static Route）] の順に選択し、古い管理インターフェイスのデフォルトルートを新しいルートに変更します。

ステップ 12 [マネージャアクセス - 構成詳細（Manager Access - Configuration Details）] [FMCアクセス - 構成詳細（FMC Access - Configuration Details] ダイアログボックスに戻り、[確認（Acknowledge）] をクリックして展開ブロックを削除します。

Firewall Management Center 設定は、次回展開時に Firewall 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 Firewall Management Center の設定を手動で修正する必要があります。

「Config was cleared」および「Manager Access changed and acknowledged」という想定されるメッセージが表示されます。

GUI で *[*管理（*Management*）*]* に使用する *Firewall Threat Defense* データインターフェイスを修正する

管理接続が稼働しているにもかかわらず、マネージャアクセスに使用するデータインターフェイスの IP アドレスを変更する場合は、次の手順を実行します。たとえば、zero-touch provisioning を使用してデバイスを登録した場合、高可用性を有効にする前に、IP アドレスを静的アドレスに変更する必要があります。

または CLI でインターフェイス設定を変更することもできますが、これは、管理接続が停止している場合にのみ使用することを推奨します。CLI で行った変更は、いずれの場合も GUI で複製する必要があります。

手順

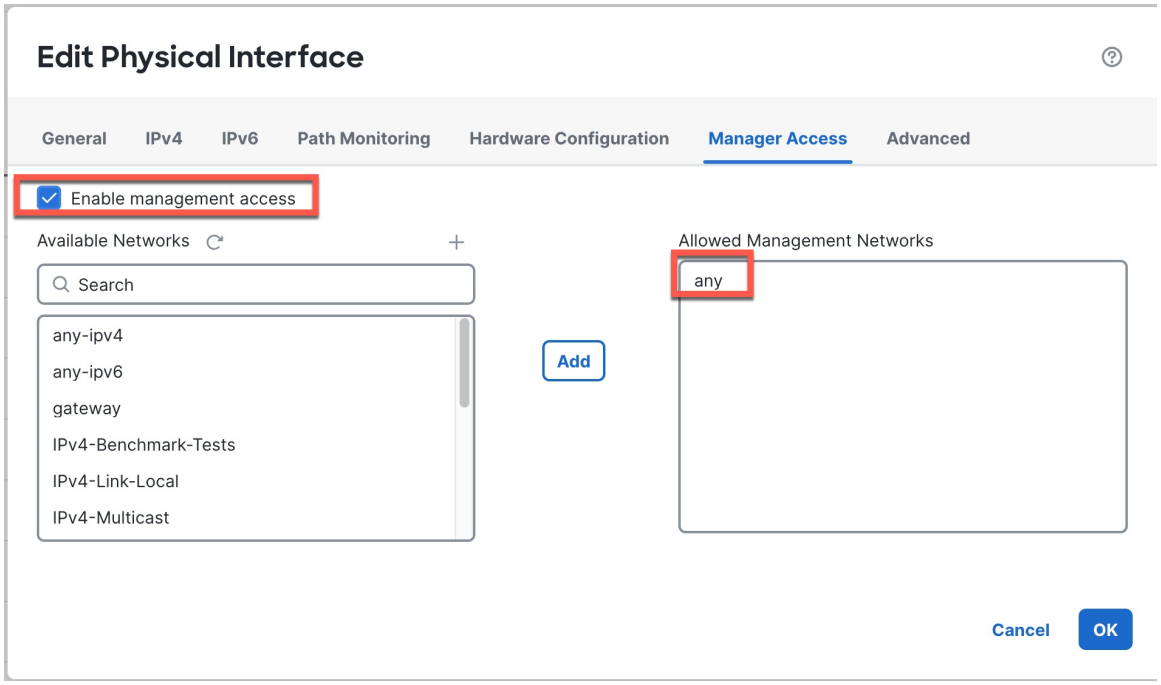
ステップ 1 **Devices** > **Device Management** を選択し、デバイスの横にある **Edit** (✎) をクリックします。

ステップ 2 **[インターフェイス（Interface）]** を選択します。

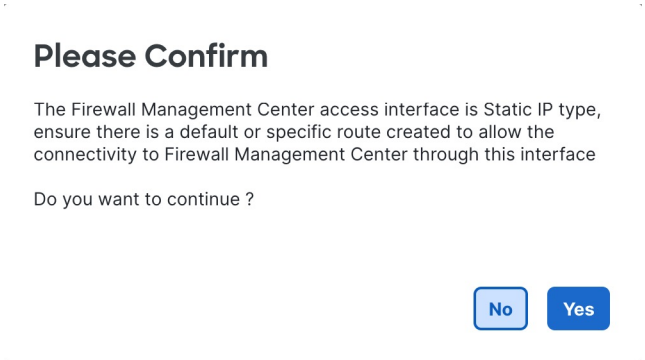
ステップ 3 マネージャアクセスに使用するインターフェイスを変更する場合は、次の手順を実行します。

a) 古いデータ管理インターフェイスから IP アドレスと名前を削除し、このインターフェイスのマネージャアクセスを無効にします。

b) 新しい設定が適用された新しいデータ管理インターフェイスを構成し、それに対して、マネージャアクセスを有効にします。



c) 静的 IP アドレスを使用する場合は、デフォルトルートを使用するようにリマインダが表示されます。[Yes] をクリックします。



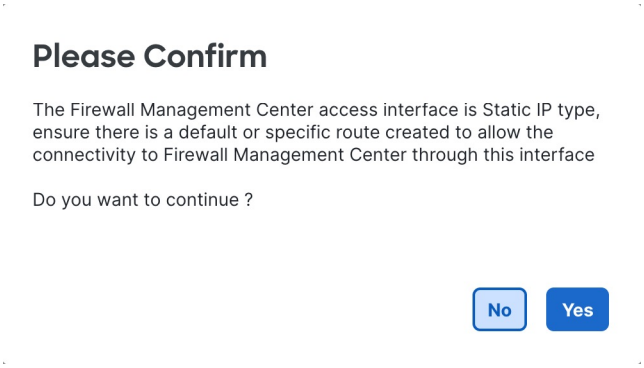
d) [OK] をクリックして、インターフェイスを終了します。

e) [インターフェイス（Interfaces）] ページで [保存（Save）] をクリックします。

ステップ 4 IP アドレスのみを変更する場合は、次の手順を実行します。

a) IP アドレスを変更します。

b) 静的 IP アドレスを使用する場合は、デフォルトルートを使用するようにリマインダが表示されます。[Yes] をクリックします。



c) [OK] をクリックして、インターフェイスを終了します。

d) [インターフェイス（Interfaces）] ページで [保存（Save）] をクリックします。

ステップ 5 [ルーティング（Routing）] タブをクリックして、[スタティックルート（Static Route）] をクリックし、マネージャ アクセス インターフェイスのデフォルトまたはスタティックルートを追加または変更します。

ステップ 6 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。

Firewall Management Center が現在の接続経由で構成の変更を展開します。展開の後、データインターフェイスには新しい IP アドレスが割り当てられるため、管理接続を再度確立する必要があります。

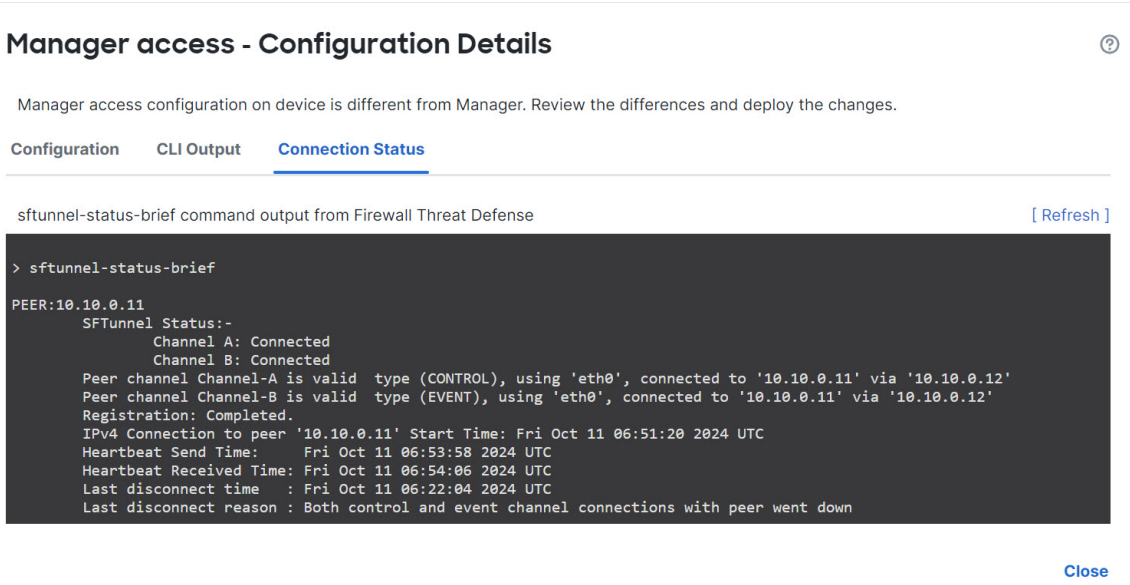
ステップ 7 Firewall Management Center でのホスト名または IP アドレスの更新 （49 ページ）。

ステップ 8 管理接続が再確立されたことを確認します。

[デバイス（Device）] 領域で、[管理（Management）] フィールドに対して、**[マネージャアクセス詳細：構成（Manager Access Details: Configuration）]**、[接続状態（Connection Status）] の順に選択します。

次のステータスは、データインターフェイスの接続が成功したことを示し、内部の「tap_nlp」インターフェイスを示しています。

図 *33* : 接続ステータス



接続の再確立に 10 分以上かかる場合は、接続のトラブルシューティングを行う必要があります。データインターフェイスでの管理接続のトラブルシューティング （72 ページ） を参照してください。

Firewall Management Center でのホスト名または IP アドレスの更新

（デバイスの CLI を使用するなどして）デバイスを Firewall Management Center に追加した後にそのデバイスのホスト名または IP アドレスを編集する場合は、次の手順を使用して管理側の Firewall Management Center のホスト名または IP アドレスを手動で更新する必要があります。

デバイスのデバイス管理 IP アドレスを変更するには、Firewall Threat Defense 管理インターフェイスの CLI での変更 （36 ページ）を参照してください。

デバイスの登録時に NAT ID のみを使用した場合、IP はこのページに [NO-IP] として表示され、IP アドレス/ホスト名を更新する必要はありません。

zero-touch provisioning を使用して外部インターフェイスでデバイスを登録した場合、ホスト名は一致する DDNS 設定とともに自動的に生成されます。この場合、ホスト名は編集できません。

手順

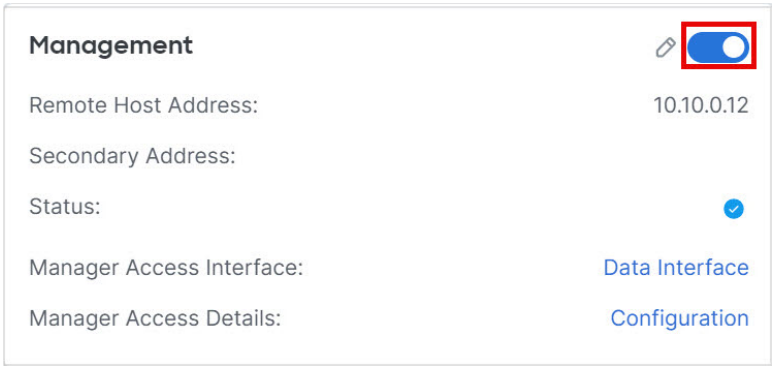
ステップ 1 **Devices** > **Device Management** を選択します。

ステップ 2 管理オプションを変更するデバイスの横にある **Edit** (✎) をクリックします。

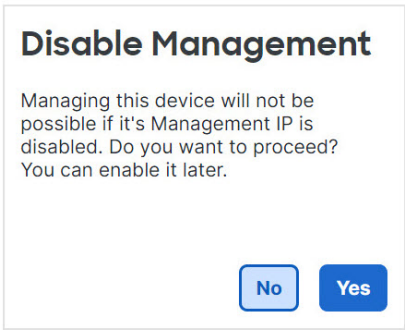
ステップ 3 [Device] をクリックし、[Management] 領域を表示します。

ステップ 4 スライダをクリックして管理を一時的に無効にすることで、**Slider disabled** ( ) を無効化します。

図 *34* : 管理を無効にする



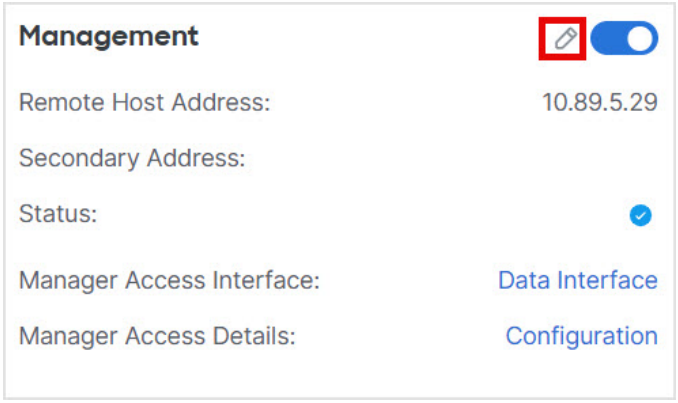
管理の無効化を続行するように求められます。 [Yes] をクリックします。



管理を無効化すると、Firewall Management Center とデバイス間の接続がブロックされますが、Firewall Management Center からデバイスは登録解除**されません**。

ステップ 5 **[リモートホストアドレス（Remote Host Address）]** の IP アドレスおよびオプションの [セカンダリアドレス（Secondary Address）]（冗長データインターフェイスを使用する場合）または **Edit** ( )をクリックしてホスト名を編集します。

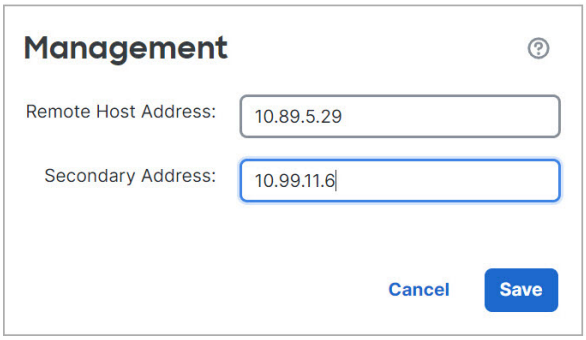
図 *35* : 管理アドレスの編集



ステップ 6 [管理（Management）] ダイアログボックスの **[リモートホストアドレス（Remote Host Address）]** フィールドおよびオプションの [セカンダリアドレス（Secondary Address）] フィールドで名前または IP アドレスを変更し、[保存（Save）] をクリックします。

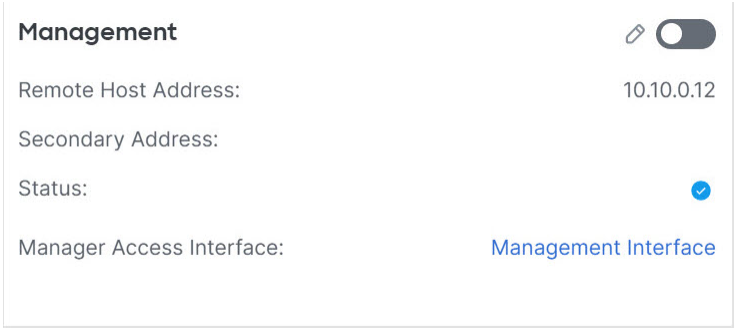
セカンダリ マネージャ アクセス データ インターフェイスの使用については、冗長マネージャアクセス用データインターフェイスの設定 （29 ページ）を参照してください。

図 *36* : 管理 *IP* アドレス



ステップ 7 スライダをクリックして管理を再度有効 **Slider enabled** ( ) にします。

図 *37* : 管理接続の有効化



Firewall Management Center IP アドレスの変更

Firewall Management Center の IP アドレスまたはホスト名を変更する場合は、設定が一致するようにデバイス CLI で値を変更する必要があります。ほとんどの場合、管理接続はデバイスの Firewall Management Center IP アドレスまたはホスト名を変更せずに再確立されますが、少なくともデバイスを Firewall Management Center に追加して NAT ID のみを指定した場合は、接続が再確立されるようにするために、このタスクを実行する必要があります。他の場合でも、Firewall Management Center IP アドレスまたはホスト名を最新の状態に維持して、ネットワークの復元力を高めることを推奨します。

手順

ステップ 1 Firewall Management Center の IP アドレスを変更してください。

注意
Firewall Management Center インターフェイスを変更する場合は十分にご注意ください。設定エラーのために再接続できない場合は、Firewall Management Center コンソールポートにアクセスして、Linux シェルでネットワーク設定を再設定する必要があります。この操作では、Cisco TAC に連絡する必要があります。

a) **System (⚙) > Configuration > Management Interfaces**を選択します。
b) [インターフェイス（Interfaces）] エリアで、設定するインターフェイスの横にある [編集（Edit）] をクリックします。
c) IP アドレスを変更し、[保存（Save）] をクリックします。

ステップ 2 Firewall Threat Defense CLI で、Firewall Management Center 識別子を表示します。

show managers

例：

```
> show managers
Type                      : Manager
Host                      : 10.10.1.4
Display name              : 10.10.1.4
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
Management type           : Configuration
```

ステップ 3 Firewall Threat Defense CLI で、Firewall Management Center IP アドレスまたはホスト名を編集します。

configure manager edit *identifier* {**hostname** {*ip_address* | *hostname*} | **displayname** *display_name*}

Firewall Management Center が **DONTRESOLVE** と NAT ID によって最初に識別された場合、このコマンドを使用して値をホスト名または IP アドレスに変更できます。IP アドレスまたはホスト名を **DONTRESOLVE** に変更することはできません。

管理接続がダウンした後、再確立されます。**sftunnel-status** コマンドを使用して、接続の状態をモニターできます。

例：

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 hostname 10.10.5.1
```

Firewall Management Center と Threat Defense の両方の IP アドレスの変更

Firewall Management Center と Firewall Threat Defense の IP アドレスを新しいネットワークに移動する場合は、両方を変更することをお勧めします。

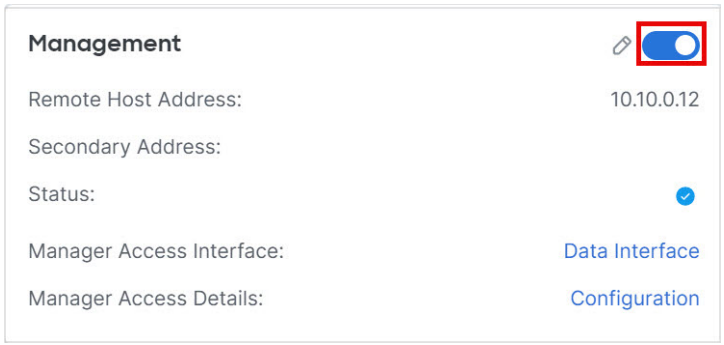
手順

ステップ 1 管理接続を無効にします。

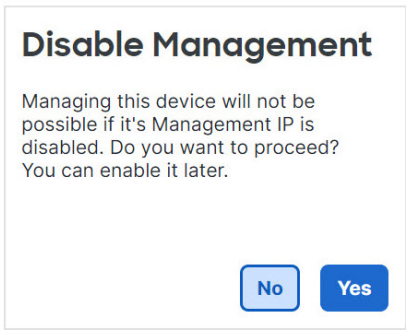
高可用性ペアまたはクラスタの場合は、すべてのユニットでこれらの CLI 手順を実行します。

a) **Devices** > **Device Management**を選択します。
b) デバイスの横にある **Edit** (✎) をクリックします。
c) [Device] をクリックし、[Management] 領域を表示します。
d) スライダをクリックして管理を一時的に無効にすることで、(⬭) を無効化します。

図 *38* : 管理を無効にする



管理の無効化を続行するように求められます。 [Yes] をクリックします。



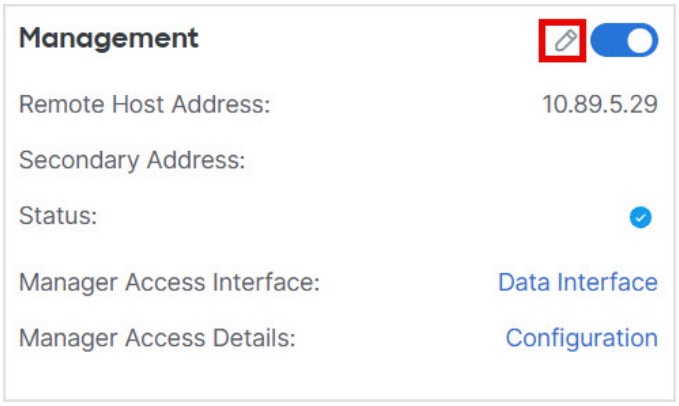
ステップ 2 Firewall Management Center 内のデバイスの IP アドレスを新しいデバイスの IP アドレスに変更します。

デバイスの IP アドレスは後で変更します。

高可用性ペアまたはクラスタの場合は、すべてのユニットでこれらの CLI 手順を実行します。

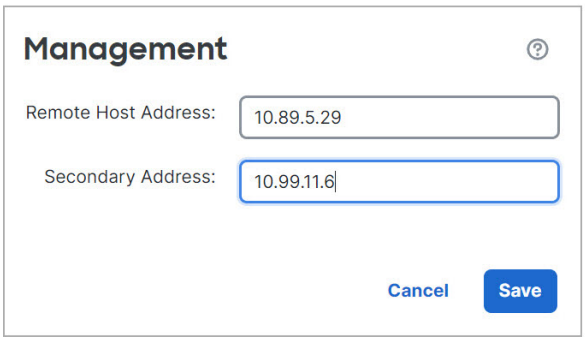
a) **[リモートホストアドレス（Remote Host Address）]** の IP アドレスおよびオプションの [セカンダリアドレス（Secondary Address）]（冗長データインターフェイスを使用する場合）または **Edit** (✎)をクリックしてホスト名を編集します。

図 *39* : 管理アドレスの編集



b) [管理（Management）] ダイアログボックスの **[リモートホストアドレス（Remote Host Address）]** フィールドおよびオプションの [セカンダリアドレス（Secondary Address）] フィールドで名前または IP アドレスを変更し、[保存（Save）] をクリックします。

図 *40* : 管理 *IP* アドレス



ステップ 3 Firewall Management Center の IP アドレスを変更してください。

注意
Firewall Management Center インターフェイスを変更する場合は十分にご注意ください。設定エラーのために再接続できない場合は、Firewall Management Center コンソールポートにアクセスして、Linux シェルでネットワーク設定を再設定する必要があります。この操作では、Cisco TAC に連絡する必要があります。

a) **System** (⚙) > **Configuration** > **Management Interfaces**を選択します。
b) [インターフェイス（Interfaces）] エリアで、設定するインターフェイスの横にある [編集（Edit）] をクリックします。
c) IP アドレスを変更し、[保存（Save）] をクリックします。

ステップ 4 デバイスのマネージャ IP アドレスを変更します。

高可用性ペアまたはクラスタの場合は、すべてのユニットでこれらの CLI 手順を実行します。

a) Firewall Threat Defense CLI で、Firewall Management Center 識別子を表示します。

show managers

例：

```
> show managers
Type                      : Manager
Host                      : 10.10.1.4
Display name              : 10.10.1.4
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
Management type           : Configuration
```

b) Firewall Management Center IP アドレスまたはホスト名を編集します。

configure manager edit *identifier* {**hostname** {*ip_address* | *hostname*} | **displayname** *display_name*}

Firewall Management Center が **DONTRESOLVE** と NAT ID によって最初に識別された場合、このコマンドを使用して値をホスト名または IP アドレスに変更できます。IP アドレスまたはホスト名を **DONTRESOLVE** に変更することはできません。

例：

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 hostname 10.10.5.1
```

ステップ 5 コンソールポートでマネージャ アクセス インターフェイスの IP アドレスを変更します。

高可用性ペアまたはクラスタの場合は、すべてのユニットでこれらの CLI 手順を実行します。

専用管理インターフェイスを使用している場合：

configure network ipv4

configure network ipv6

専用管理インターフェイスを使用している場合：

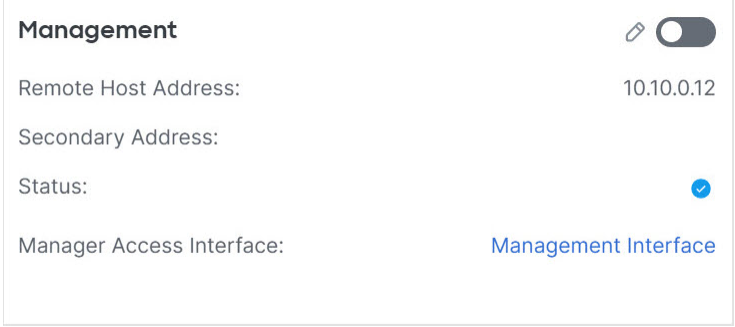
configure network management-data-interface disable

configure network management-data-interface

ステップ 6 スライダをクリックして管理を再度有効 () にします。

高可用性ペアまたはクラスタの場合は、すべてのユニットでこれらの CLI 手順を実行します。

図 *41* : 管理接続の有効化



ステップ 7 （マネージャアクセスにデータインターフェイスを使用している場合）Firewall Management Center でデータインターフェイス設定を更新します。

高可用性ペアの場合は、両方のユニットでこの手順を実行します。

a) **[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 - 構成詳細（Manager Access - Configuration Details）]** を選択し、[更新（Refresh）] をクリックします。

b) **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）]** を選択し、新しいアドレスと一致するように IP アドレスを設定します。

c) [マネージャアクセス - 構成詳細（Manager Access - Configuration Details）] [FMCアクセス - 構成詳細（FMC Access - Configuration Details] ダイアログボックスに戻り、[確認（Acknowledge）] をクリックして展開ブロックを削除します。

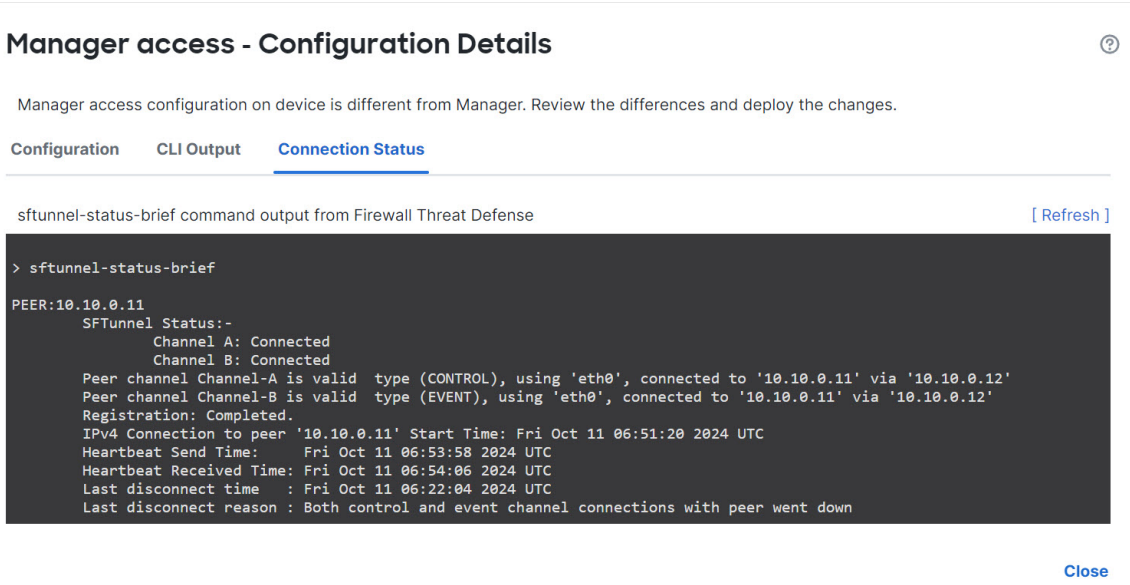
ステップ 8 管理接続が再確立されたことを確認します。

Firewall Management Center で、**[Devices] > [Device Management] > [Device] > [Management] > [Manager Access - Configuration Details] > [Connection Status]** ページで管理接続ステータスを確認します。

管理接続のステータスを表示するには、Firewall Threat Defense CLI で、**sftunnel-status-brief** コマンドを入力します。

次のステータスは、データインターフェイスの接続が成功したことを示し、内部の「tap_nlp」インターフェイスを示しています。

図 *42 :* 接続ステータス



ステップ 9 （高可用性 Firewall Management Center ペアの場合）セカンダリ Firewall Management Center で設定変更を繰り返します。

a) セカンダリ Firewall Management Center IP アドレスを変更します。
b) 両方のユニットで新しいピアアドレスを指定します。
c) セカンダリユニットをアクティブユニットにします。
d) デバイスの管理接続を無効にします。
e) Firewall Management Center でデバイスの IP アドレスを変更します。
f) 管理接続を再度有効にします。

マネージャ アクセス インターフェイスの変更

デバイスを登録したら、マネージャ アクセス インターフェイスを、管理インターフェイスまたは別のデータ インターフェイスに変更できます。

管理アクセスインターフェイスの管理からデータへの変更

専用の管理インターフェイスまたはデータインターフェイスから Firewall Threat Defense を管理できます。デバイスを Firewall Management Center に追加した後にマネージャ アクセス インターフェイスを変更する場合は、次の手順に従って管理インターフェイスからデータインターフェイスに移行します。逆の方向に移行するには、マネージャ アクセス インターフェイスをデータから管理に変更する （63 ページ）を参照してください。

管理からデータへのマネージャアクセスの移行を開始すると、Firewall Management Center は Firewall Threat Defense への展開時にブロックを適用します。ブロックを削除するには、データインターフェイスでマネージャアクセスを有効にします。

次の手順を参照して、データインターフェイスでマネージャアクセスを有効にし、その他の必要な設定も構成します。

始める前に

ハイアベイラビリティペアの場合、特に明記されていない限り、すべての手順はアクティブユニットでのみ実行します。設定の変更が展開されると、スタンバイユニットはアクティブユニットから設定およびその他のステート情報を同期します。

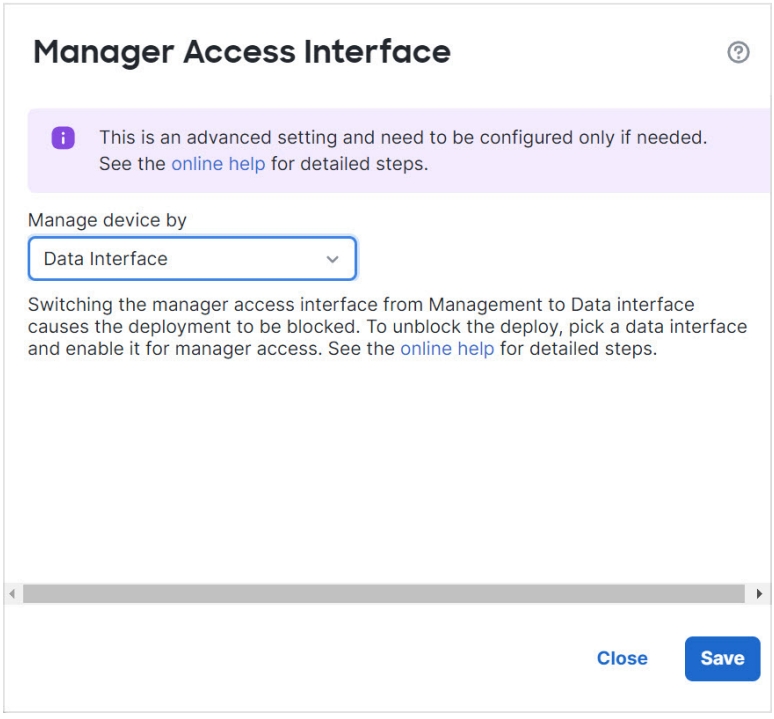
手順

ステップ 1 インターフェイスの移行を開始します。

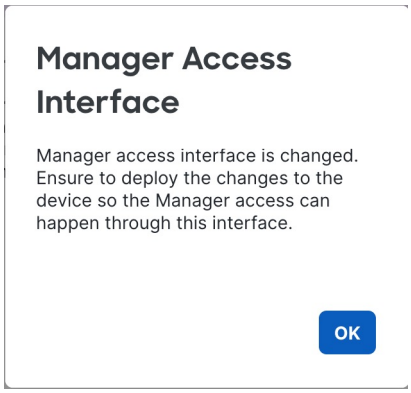
a) **Devices** > **Device Management** ページで、デバイスの **Edit** (✎) をクリックします。[デバイス（Device）] をクリックし、[管理（Management）] 領域で、**[マネージャアクセスインターフェイス（Manager Access Interface）]** リンクをクリックします。

[マネージャ アクセス インターフェイス（Manager Access Interface）] [FMCアクセスインターフェイス（FMC Access Interface）] フィールドには、現在の管理インターフェイスが表示されます。リンクをクリックしたら、[デバイスの管理（Manage device by）] ドロップダウンリストで新しいインターフェイスタイプである [データインターフェイス（Data Interface）] を選択します。

図 *43*：マネージャ アクセス インターフェイス

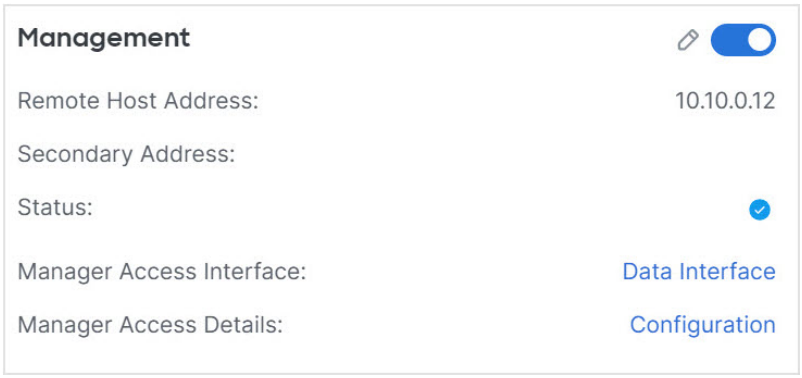


b) [OK] をクリックし、[閉じる（Close）] をクリックします。



データインターフェイスでマネージャアクセスを有効にするには、残りの手順を完了する必要があります。[管理（Management）] 領域には、[マネージャ アクセス インターフェイス：データインターフェイス（Manager Access Interface: Management Interface）] [FMCアクセスインターフェイス：データインターフェイス（FMC Access Interface: Management Interface）] と、[マネージャアクセスの詳細：構成（Manager Access Details: Configuration）] [FMCアクセスの詳細：構成（FMC Access Details: Configuration）] が表示されます。

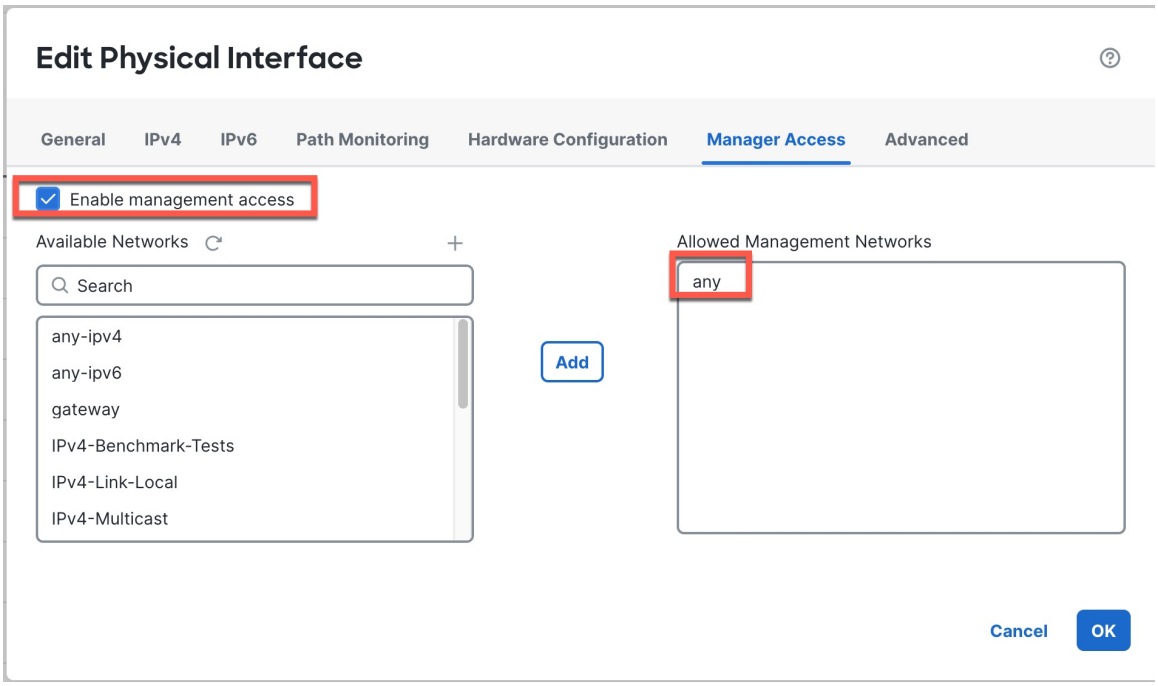
図 *44* : マネージャアクセス



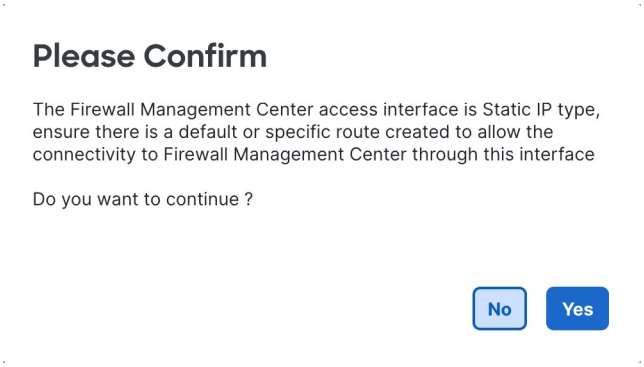
[構成（Configuration）] をクリックすると、[マネージャアクセス - 構成の詳細（Manager Access - Configuration Details）] [FMCアクセス - 構成の詳細（FMC Access - Configuration Details）] ダイアログボックスが開きます。[マネージャアクセスモード（Manager Access Mode）] [FMCアクセスモード（FMC Access Mode）] は、展開保留状態を示しています。

ステップ 2 データインターフェイスでマネージャアクセスを有効化します。[インターフェイス（Interface）]、インターフェイスの **Edit** (✎)、**[マネージャアクセス（Manager Access）]** の順に選択します。

[管理アクセスの有効化（Enable management access）] をオンにして、[OK] をクリックします。デフォルトでは、すべてのネットワークが許可されますが、Firewall Management Center アドレスが許可されている限り、アクセスを制限できます。



マネージャ アクセス インターフェイスが静的 IP アドレスを使用している場合は、そのためのルーティングを設定するように求められます。



[インターフェイス（Interfaces）]ページで[保存（Save）]をクリックします。インターフェイス設定の詳細については、ルーテッドモードのインターフェイスの設定を参照してください。マネージャアクセスは 1 つのルーテッド データ インターフェイスとオプションのセカンダリ インターフェイスで有効にできます。これらのインターフェイスが名前と IP アドレスで完全に構成され、有効になっていることを確認してください。

冗長性のためにセカンダリインターフェイスを使用する場合は、必要な追加構成について冗長マネージャアクセス用データインターフェイスの設定 （29 ページ）を参照してください。

ステップ 3 （任意）インターフェイスに DHCP を使用する場合は、**DDNS** ページで、Web タイプの DDNS 方式を有効にします。**Devices** > **Device Management** に移動し、[DHCP] タブで [DDNS] をクリックします。

ダイナミック DNS の設定を参照してください。DDNS は、FTD の IP アドレスが変更された場合に Firewall Management Center が完全修飾ドメイン名（FQDN）で Firewall Threat Defense に到達できるようにします。

ステップ 4 Firewall Threat Defense がデータインターフェイス経由で Firewall Management Center にルーティングできることを確認し、必要に応じて、スタティックルートページで、スタティックルートを追加します。**Devices** > **Device Management** に移動し、[ルーティング（Routing）] タブの [スタティックルート（Static Route）] をクリックします。

スタティック ルートの追加を参照してください。

ステップ 5 （任意） プラットフォーム設定ポリシーで DNS を構成します。[**Devices** > **Platform Settings**]、[DNS] の順に選択します。このデバイスにポリシーを適用します。

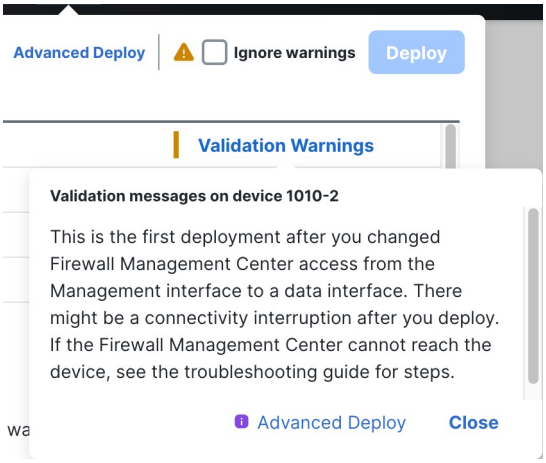
DNSを参照してください。DDNS を使用する場合は DNS が必要です。セキュリティポリシーで FQDN に DNS を使用することもできます。

ステップ 6 （任意） プラットフォーム設定ポリシーでデータインターフェイスの SSH を有効にし、**Devices** > **Device Management** ページでこのデバイスに適用します。デバイスの [**Edit** ()]、[SSHアクセス（SSH Access）] の順に選択します。

SSH アクセスの確保を参照してください。SSH はデータインターフェイスでデフォルトで有効になっていないため、SSH を使用して Firewall Threat Defense を管理する場合は、明示的に許可する必要があります。

ステップ 7 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。

マネージャ アクセス インターフェイスを変更することを確認するための検証エラーが表示されます。[警告を無視（Ignore warnings）] をオンにして、再度展開します。



Firewall Management Center は、現在の管理インターフェイスを介して設定の変更を展開します。展開後、データインターフェイスを使用できるようになりましたが、管理への元の管理接続はアクティブなままです。

ステップ 8 Firewall Threat Defense CLI（できればコンソールポートから）で、静的 IP アドレスを使用するように管理インターフェイスを設定し、データインターフェイスを使用するようにゲートウェイを設定します。ハイアベイラビリティの場合は、両方のユニットでこの手順を実行します。

configure network {**ipv4** | **ipv6**} **manual** *ip_address netmask* **data-interfaces**

- *ip_address netmask*：管理インターフェイスを使用する予定はありませんが、ゲートウェイを [データインターフェイス（data-interfaces）] に設定できるように、プライベートアドレスなどの静的 IP アドレスを設定する必要があります（次の箇条書きを参照）。[data-interfaces] である必要があるデフォルトルートは、DHCP サーバーから受信したルートで上書きされる可能性があるため、DHCP は使用できません。
- **data-interfaces** — この設定は、マネージャ アクセス データ インターフェイスを通じて回送できるように、バックプレーンを介して管理トラフィックを転送します。

管理インターフェイスのネットワーク設定を変更すると、SSH セッションが切断されるため、SSH 接続の代わりにコンソールポートを使用することをお勧めします。

ステップ 9 必要に応じて、データインターフェイスの Firewall Management Center に到達できるように Firewall Threat Defense のケーブルを再接続します。ハイアベイラビリティの場合は、両方のユニットでこの手順を実行します。

ステップ 10 Firewall Management Center で、管理接続を無効にし、[デバイス（Device）] タブの [管理（Management）] 領域にある **Devices** > **Device Management** ページの Firewall Threat Defense に対して **[リモートホストアドレス（Remote Host Address）]**[IP アドレス（IP address）] およびオプションの [セカンダリアドレス（Secondary Address）] を更新し、接続を再度有効にします。

Firewall Management Center でのホスト名または IP アドレスの更新 （49 ページ）を参照してください。Firewall Threat Defense を Firewall Management Center に追加したときに Firewall Threat Defense ホスト名または NAT ID のみを使用した場合は、値を更新する必要はありません。ただし、接続を再開するには、管理接続を無効にしてから再度有効にする必要があります。

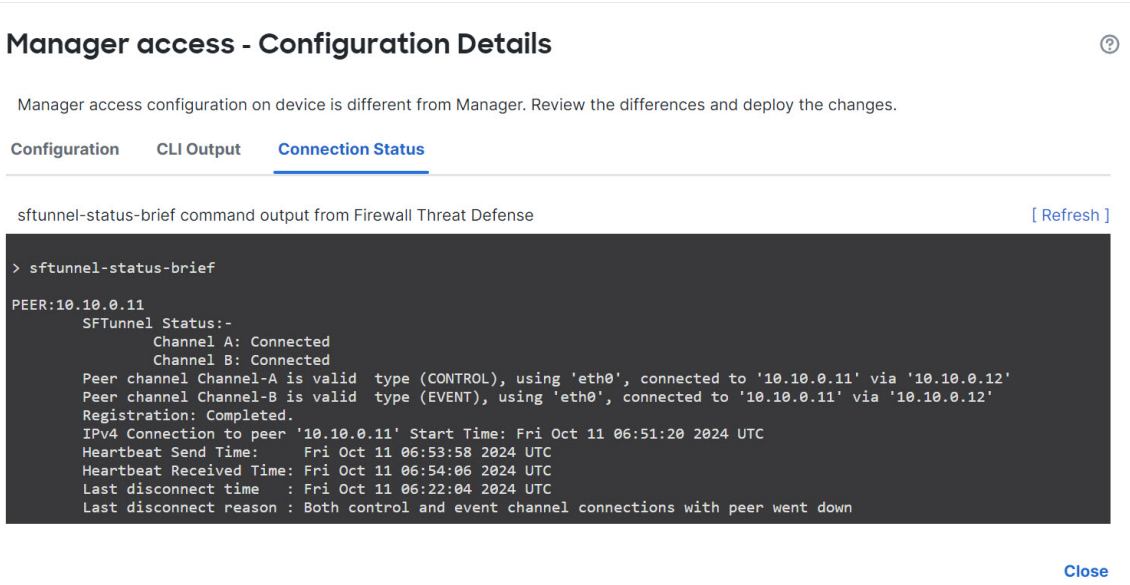
ステップ 11 管理接続が再確立されたことを確認します。

Devices > **Device Management** ページで、**[マネージャアクセス詳細：構成（Manager Access Details: Configuration）]**、[接続状態（Connection Status）] の順に選択します。

または、Firewall Threat Defense CLI で確認できます。管理接続のステータスを表示するには、**sftunnel-status-brief** コマンドを入力します。

次のステータスは、データインターフェイスの接続が成功したことを示し、内部の「tap_nlp」インターフェイスを示しています。

図 *45* : 接続ステータス



接続の再確立に 10 分以上かかる場合は、接続のトラブルシューティングを行う必要があります。データインターフェイスでの管理接続のトラブルシューティング （72 ページ） を参照してください。

マネージャ アクセス インターフェイスをデータから管理に変更する

専用の管理インターフェイスまたはデータインターフェイスから Firewall Threat Defense を管理できます。デバイスを Firewall Management Center に追加した後にマネージャ アクセス インターフェイスを変更する場合は、次の手順に従ってデータインターフェイスから管理インターフェイスに移行します。逆の方向に移行するには、管理アクセスインターフェイスの管理からデータへの変更 （57 ページ）を参照してください。

データから管理へのマネージャアクセスの移行を開始すると、Firewall Management Center は Firewall Threat Defense への展開時にブロックを適用します。ブロックを削除するには、データインターフェイスでマネージャアクセスを無効にする必要があります。

次の手順を参照して、データインターフェイスでマネージャアクセスを無効にし、その他の必要な設定も構成します。

始める前に

ハイアベイラビリティペアの場合、特に明記されていない限り、すべての手順はアクティブユニットでのみ実行します。設定の変更が展開されると、スタンバイユニットはアクティブユニットから設定およびその他のステート情報を同期します。

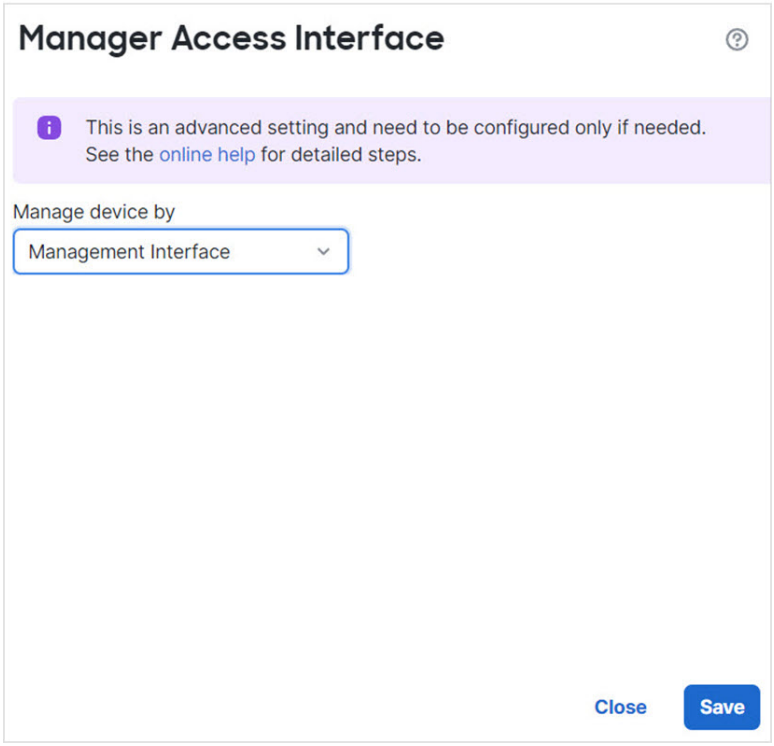
手順

ステップ 1 インターフェイスの移行を開始します。

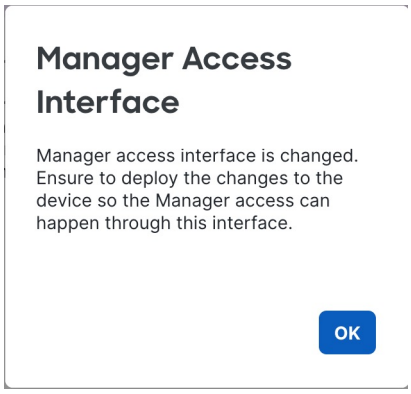
a) **Devices** > **Device Management** ページで、デバイスの **Edit** (✎) をクリックします。[デバイス（Device）] をクリックし、[管理（Management）] 領域で、**[マネージャアクセスインターフェイス（Manager Access Interface）]** のリンクを選択します。

[マネージャ アクセス インターフェイス（Manager Access Interface）] [FMCアクセスインターフェイス（FMC Access Interface）] フィールドには、現在の管理インターフェイスが表示されます。リンクをクリックしたら、[デバイスの管理（Manage device by）] ドロップダウンリストで新しいインターフェイスタイプである [管理インターフェイス（Management Interface）] を選択します。

図 *46* : マネージャ アクセス インターフェイス



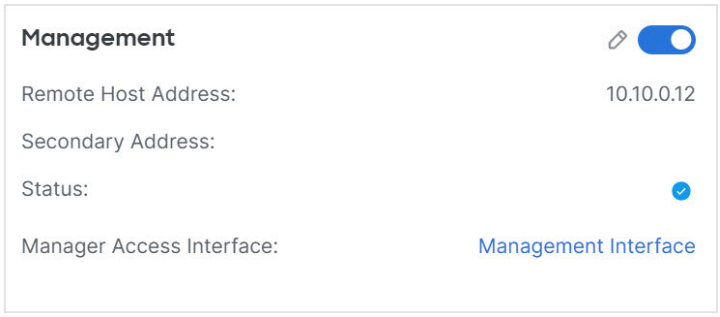
b) [保存（Save）] をクリックします。



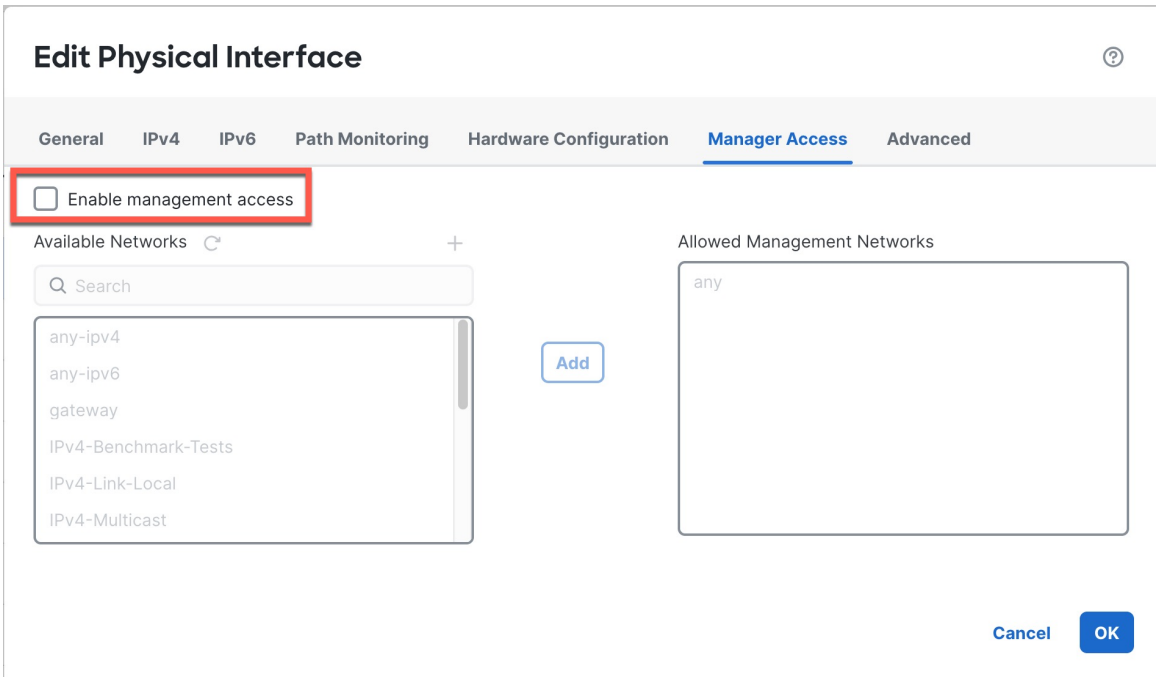
[OK] をクリックし、[閉じる（Close）] をクリックします。

管理インターフェイスでマネージャアクセスを有効にするには、残りの手順を完了する必要があります。[管理（Management）] 領域には、**[マネージャ アクセス インターフェイス：管理インターフェイス（Manager Access Interface: Management Interface）]**が表示されます。

図 *47*：マネージャアクセス



ステップ 2 データインターフェイスでマネージャアクセスを無効にします。[インターフェイス（Interface）]、インターフェイスの **Edit** (✎)、**[マネージャアクセス（Manager Access）]** の順に選択します。



[管理アクセスの有効化（Enable management access）] をオフにして、[OK] をクリックします。[インターフェイス（Interfaces）] ページで [保存（Save）] をクリックします。この手順により、展開時のブロックが削除されます。

ステップ 3 まだ行っていない場合は、プラットフォーム設定ポリシーでデータインターフェイスの DNS 設定を構成し、**Devices** > **Device Management** ページでこのデバイスに適用します。デバイスの **Edit** (✎) をクリックし、[DNS] をクリックします。

DNSを参照してください。データインターフェイスでマネージャアクセスを無効にする Firewall Management Center 展開では、ローカル DNS 設定が削除されます。その DNS サーバーがアクセスルールの FQDN などのセキュリティポリシーで使用されている場合は、Firewall Management Center を使用して DNS 設定を再適用する必要があります。

ステップ 4 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。

Firewall Management Center は、現在のデータインターフェイスを介して設定の変更を展開します。

ステップ 5 必要に応じて、管理インターフェイスの Firewall Management Center に到達できるように Firewall Threat Defense のケーブルを再接続します。ハイアベイラビリティの場合は、両方のユニットでこの手順を実行します。

ステップ 6 Firewall Threat Defense CLI で、静的 IP アドレスまたは DHCP を使用して、管理インターフェイスの IP アドレスとゲートウェイを設定します。ハイアベイラビリティの場合は、両方のユニットでこの手順を実行します。

最初にマネージャアクセス用のデータインターフェイスを設定したとき、管理ゲートウェイはデータインターフェイスに設定されていました。これにより、バックプレーン経由で管理トラフィックが転送され、マネージャ アクセス データ インターフェイスを介してルーティングで

きるようになりました。ここで、管理ネットワーク上のゲートウェイの IP アドレスを設定する必要があります。

スタティック IP アドレス：

configure network {**ipv4** | **ipv6**} **manual** *ip_address netmask gateway_ip*

DHCP：

configure network{**ipv4** | **ipv6**} **dhcp**

ステップ 7 Firewall Management Center で、管理接続を無効にし、[デバイス（Device）] タブの [管理（Management）] セクションにある **Devices** > **Device Management** の Firewall Threat Defense に対して **[リモートホストアドレス（Remote Host Address）**[IPアドレス（IP address）] とオプションの [セカンダリアドレス（Secondary Address）] を更新し、接続を再度有効にします。

Firewall Management Center でのホスト名または IP アドレスの更新 （49 ページ）を参照してください。Firewall Threat Defense を Firewall Management Center に追加したときに Firewall Threat Defense ホスト名または NAT ID のみを使用した場合は、値を更新する必要はありません。ただし、接続を再開するには、管理接続を無効にしてから再度有効にする必要があります。

ステップ 8 管理接続が再確立されたことを確認します。

Firewall Management Center で、**Devices** > **Device Management** の [デバイス（Device）] タブの [管理（Management）] セクションにある [ステータス（Status）] フィールドで管理接続の状態を確認するか、Firewall Management Center で通知を表示します。

管理接続のステータスを表示するには、Firewall Threat Defense CLI で、**sftunnel-status-brief** コマンドを入力します。

接続の再確立に 10 分以上かかる場合は、接続のトラブルシューティングを行う必要があります。データインターフェイスでの管理接続のトラブルシューティング （72 ページ） を参照してください。

データインターフェイス管理用のマネージャアクセスの詳細を表示する

専用の管理インターフェイスを使用する代わりに、Firewall Management Center 管理にデータインターフェイスを使用する場合は、Firewall Management Centerでデバイスのインターフェイスとネットワークの設定を変更するときに接続を中断しないように注意します。デバイスのデータインターフェイス設定をローカルで変更することもできます。その場合は、Firewall Management Center でそれらの変更を手動で調整する必要があります。[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 - 構成詳細（Manager Access - Configuration Details）] [FMCアクセス - 構成詳細（FMC Access - Configuration Details）] ダイアログボックスは、Firewall Management Center と Firewall Threat Defense のローカル設定の間の矛盾を解決するために役立ちます。 > > > >

通常、Firewall Threat Defense を Firewall Management Center に追加する前に、Firewall Threat Defense の初期設定の一環としてマネージャアクセスデータインターフェイスを構成します。Firewall Threat Defense を Firewall Management Center に追加すると、Firewall Management Center はインターフェイス設定（インターフェイス名と IP アドレス、ゲートウェイへの静的ルート、

DNS サーバー、DDNS サーバーなど）を検出して維持します。DNS サーバーの場合、登録中に検出された場合、構成はローカルに保持されます。ただし、Firewall Management Center のプラットフォーム設定ポリシーには追加されません。

Firewall Threat Defense を Firewall Management Center に追加した後、**configure network management-data-interface** コマンドを使用してローカルで Firewall Threat Defense のデータインターフェイス構成を変更すると、Firewall Management Center が構成変更を検出し、Firewall Threat Defense への展開をブロックします。Firewall Management Center は、以下のいずれかの方法を使用して構成の変更を検出します。

- Firewall Threat Defense への展開。Firewall Management Center の展開の前に、構成の差異を検出してデプロイを停止します。
- [マネージャアクセス - 構成の詳細（Manager Access - Configuration Details）] [FMCアクセス - 構成の詳細（FMC Access - Configuration Details）] ダイアログボックスの [更新（Refresh）] ボタン

ブロックを削除するには、[マネージャアクセス - 構成詳細（Manager Access - Configuration Details）] [FMCアクセス - 構成詳細（FMC Access - Configuration Details] ダイアログボックスに移動し、[確認（Acknowledge）] をクリックする必要があります。Firewall Management Center 設定は、次回展開時に Firewall 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 Firewall Management Center の設定を手動で修正する必要があります。

このダイアログボックスに関する以下のページを参照してください。

設定

Firewall Management Center および Firewall Threat Defense のマネージャ アクセス データ インターフェイスの構成比較を表示します。

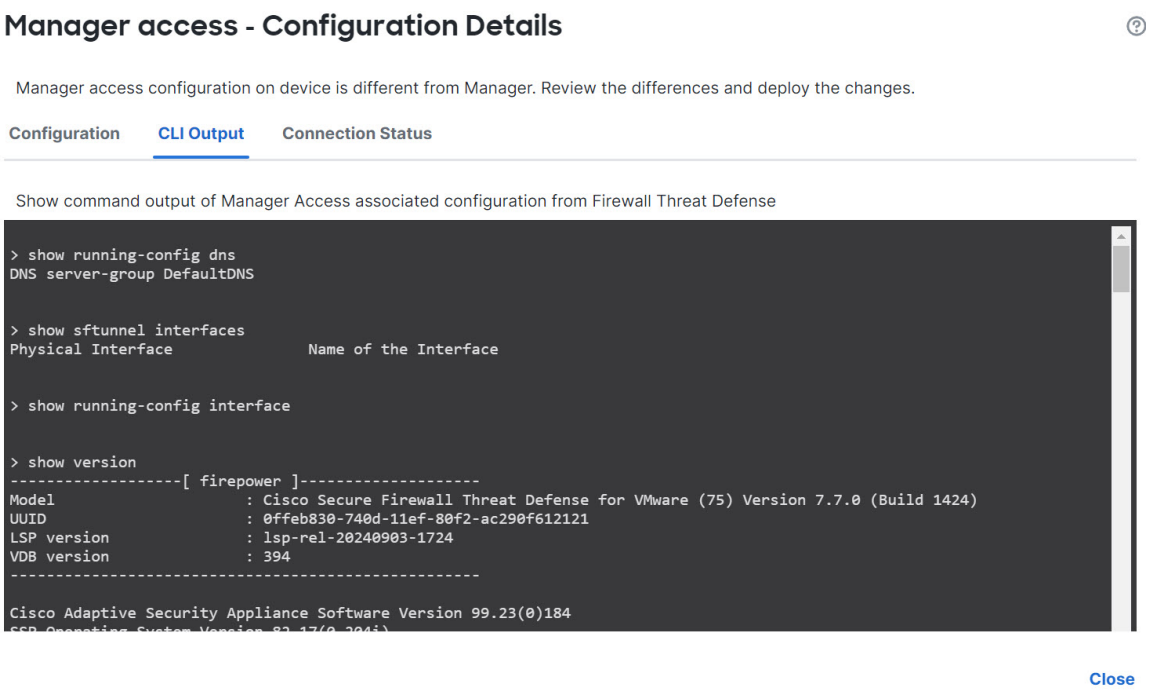
次の例は、**configure network management-data-interface** コマンドが Firewall Threat Defense に入力された Firewall Threat Defense の構成詳細を示しています。ピンクのハイライトは、相違点を**確認**したものの、Firewall Management Center の構成と一致しない場合、Firewall Threat Defense の構成が削除されることを示しています。青色のハイライトは、Firewall Threat Defense で変更される構成を示しています。緑のハイライトは、Firewall Threat Defense に追加される構成を示しています。

Firewall 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。

CLI 出力

マネージャ アクセス データ インターフェイスの CLI 構成を表示します。これは、基盤となる CLI に精通している場合に役立ちます。

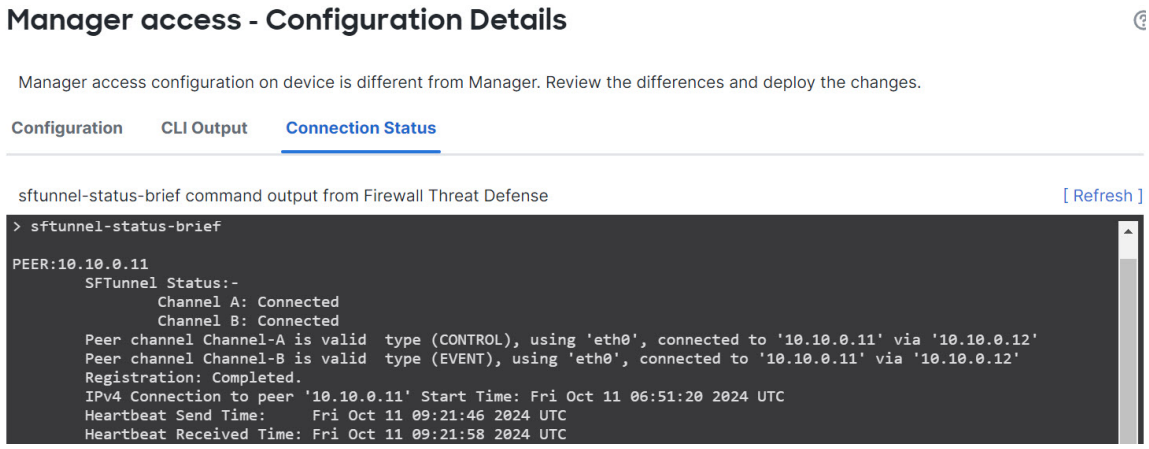
図 *48 : CLI* 出力



接続ステータス

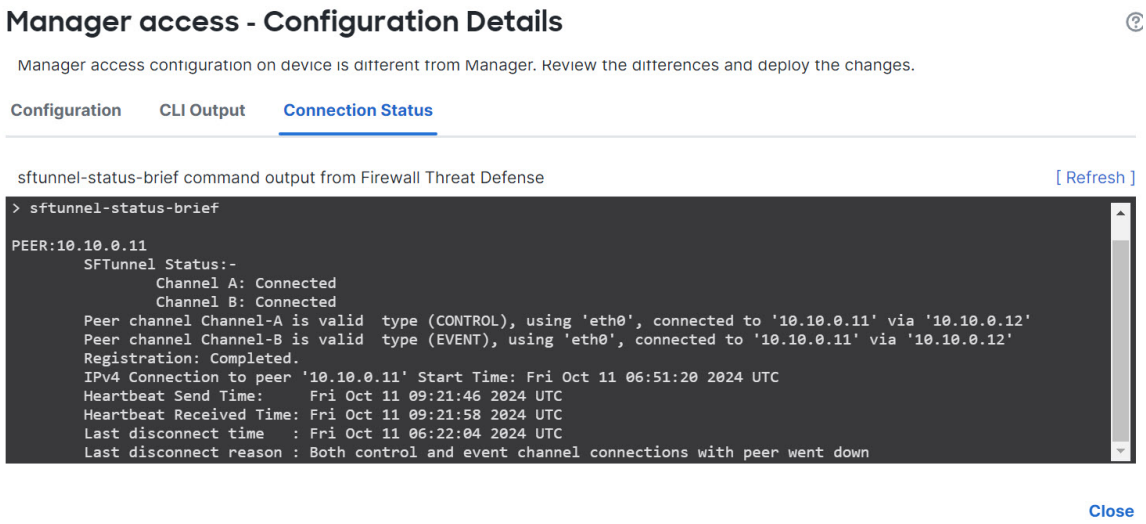
管理接続ステータスの表示次の例は、管理接続で引き続き管理「management0」インターフェースが使用されていることを示しています。

図 *49 :* 接続ステータス



次のステータスは、データインターフェイスの接続が成功したことを示し、内部の「tap_nlp」インターフェイスを示しています。

図 *50* : 接続ステータス



ダウン状態の接続の出力例を次に示します。ピアチャネルの「接続先」情報やハートビート情報が表示されていません。

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

アップ状態の接続の出力例を次に示します。ピアチャネルとハートビート情報が表示されています。

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

管理接続のトラブルシューティング

Firewall Management Center の接続が失われた場合の構成の手動ロールバック

Firewall Threat Defense でマネージャアクセス用にデータインターフェイスを使用し、ネットワーク接続に影響する Firewall Management Center からの構成変更を展開する場合、Firewall

Threat Defense の構成を最後に展開した構成にロールバックして、管理接続を復元できます。その後、ネットワーク接続が維持されるように Firewall Management Center で構成設定を調整し、再展開できます。ロールバック機能は、接続が失われていない場合でも使用でき、このトラブルシューティングの状況以外でも使用できます。

または、展開後に接続が失われた場合は、構成の自動ロールバックを有効にすることもできます。展開設定の編集 （85 ページ） を参照してください。

次のガイドラインを参照してください。

- 前回の展開のみ Firewall Threat Defense でローカルに使用できます。さらに以前の展開にロールバックすることはできません。
- ロールバックは、高可用性ではサポートされていますが、クラスタリングの展開ではサポートされていません。
- ロールバックは、Firewall Management Center で設定できる構成にのみ影響します。たとえば、ロールバックは、Firewall Threat Defense CLI でのみ設定できる専用管理インターフェイスに関連するローカル構成には影響しません。**configure network management-data-interface** コマンドを使用した最後の Firewall Management Center 展開後にデータインターフェイス設定を変更し、rollback コマンドを使用すると、それらの設定は保持されないことに注意してください。最後に展開された Firewall Management Center 設定にロールバックされます。
- UCAPL/CC モードはロールバックできません。
- 以前の展開中に更新されたアウトオブバンド SCEP 証明書データはロールバックできません。
- ロールバック中に、現在の設定がクリアされるため、接続がドロップされます。

手順

ステップ 1 Firewall Threat Defense CLI で、以前の構成へロールバックします。

configure policy rollback

ロールバック後、Firewall Threat Defense はロールバックが正常に完了したことを Firewall Management Center に通知します。Firewall Management Center では、構成がロールバックされたことを示すバナーが展開画面に表示されます。

（注）
ロールバックが失敗し、Firewall Management Center 管理が復元された場合、一般的な展開の問題についてhttps://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.htmlを参照してください。場合によっては、Firewall Management Center 管理アクセスの復元後にロールバックが失敗することがあります。この場合、Firewall Management Center 構成の問題を解決して、Firewall Management Center から再展開できます。

例：

マネージャアクセスにデータインターフェイスを使用する Firewall Threat Defense の場合：

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....................
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
...................
.....................
>
```

ステップ 2 管理接続が再確立されたことを確認します。

Firewall Management Center の接続状態ページで、管理接続の状態を確認します。**Devices** > **Device Management** に移動し、[デバイス（Device）] タブの [管理（Management）] 領域に移動します。**[マネージャアクセス - 構成の詳細（Manager Access - Configuration Details）]** 画面で、[接続状態（Connection Status）] をクリックします。

管理接続のステータスを表示するには、Firewall Threat Defense CLI で、**sftunnel-status-brief** コマンドを入力します。

接続の再確立に 10 分以上かかる場合は、接続のトラブルシューティングを行う必要があります。データインターフェイスでの管理接続のトラブルシューティング （72 ページ） を参照してください。

データインターフェイスでの管理接続のトラブルシューティング

専用の管理インターフェイスを使用する代わりに、マネージャアクセスにデータインターフェイスを使用する場合は、Firewall Management Center で Firewall Threat Defense のインターフェイスとネットワークの設定を変更する際、接続を中断しないように注意します。Firewall Threat Defense を Firewall Management Center に追加した後に管理インターフェイスタイプを変更する場合（データから管理へ、または管理からデータへ）、インターフェイスとネットワークの設定が正しく構成されていないと、管理接続が失われる可能性があります。

このトピックは、管理接続が失われた場合のトラブルシューティングに役立ちます。

管理接続ステータスの表示

Firewall Management Center の **Devices** > **Device Management** ページで、管理接続の状態を確認します。

管理接続のステータスを表示するには、Firewall Threat Defense CLI で、**sftunnel-status-brief** コマンドを入力します。**sftunnel-status** を使用して、より完全な情報を表示することもできます。

ダウン状態の接続の出力例を次に示します。ピアチャネルの「接続先」情報やハートビート情報が表示されていません。

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went
down
```

アップ状態の接続の出力例を次に示します。ピアチャネルとハートビート情報が表示されています。

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to
'10.10.17.202' via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to
'10.10.17.202' via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

Firewall Threat Defense ネットワーク情報の表示

Firewall Threat Defense CLI で、管理および マネージャ アクセス データ インターフェイスのネットワーク設定を表示します。

show network

```
> show network
===============[ System Information ]===============
Hostname                  : FTD-4
Domains                   : cisco.com
DNS Servers               : 72.163.47.11
DNS from router           : enabled
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces

==================[ management0 ]===================
Admin State               : enabled
Admin Speed               : 1gbps
Operation Speed           : 1gbps
Link                      : up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 68:87:C6:A6:54:80
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.89.5.4
Netmask                   : 255.255.255.192
Gateway                   : 169.254.1.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled
```

```
===============[ Proxy Information ]================
State                       : Disabled
Authentication              : Disabled

======[ System Information - Data Interfaces ]======
DNS Servers                 : 72.163.47.11
Interfaces                  : Ethernet1/1

==================[ Ethernet1/1 ]===================
State                       : Enabled
Link                        : Up
Name                        : outside
MTU                         : 1500
MAC Address                 : 68:87:C6:A6:54:A4
----------------------[ IPv4 ]----------------------
Configuration               : Manual
Address                     : 10.89.5.6
Netmask                     : 255.255.255.192
Gateway                     : 10.89.5.1
----------------------[ IPv6 ]----------------------
Configuration               : Disabled
```

Firewall Management Center への Firewall Threat Defense の登録の確認

Firewall Threat Defense CLI で、Firewall Management Center 登録が完了したことを確認します。このコマンドは、管理接続の現在のステータスを表示するものではないことに注意してください。

show managers

```
> show managers
Type                        : Manager
Host                        : 16a3893c-caa7-11ee-8436-0925c06e7608DONTRESOLVE
Display name                : manager-1707852946.80444
Version                     : 7.6.0 (Build 1385)
Identifier                  : a904b8b2-ca9a-11ee-a583-5e804c16b2fd
Registration                : Completed
Management type             : Configuration and analytics
```

Firewall Management Center に ping する

Firewall Threat Defense CLI で、次のコマンドを使用して、データインターフェイスから Firewall Management Center に ping します。

ping *fmc_ip*

Firewall Threat Defense CLI で、次のコマンドを使用して、管理インターフェイスから Firewall Management Center に ping します。これは、バックプレーンを介してデータインターフェイスにルーティングされます。

ping system *fmc_ip*

Firewall Threat Defense 内部インターフェイスでのパケットのキャプチャ

Firewall Threat Defense CLI で、内部バックプレーン インターフェイス（nlp_int_tap）でパケットをキャプチャして、管理パケットが送信されているかどうかを確認します。

capture *name* **interface nlp_int_tap trace detail match ip any any**

show capture*name* **trace detail**

内部インターフェイスのステータス、統計、およびパケット数の確認

Firewall Threat Defense CLI で、内部バックプレーン インターフェイス（nlp_int_tap）に関する情報を参照してください。

show interface detail

```
> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
 (Full-duplex), (1000 Mbps)
 Input flow control is unsupported, output flow control is unsupported
 MAC address 0000.0100.0001, MTU 1500
 IP address 169.254.1.1, subnet mask 255.255.255.248
 37 packets input, 2822 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 pause input, 0 resume input
 0 L2 decode drops
 5 packets output, 370 bytes, 0 underruns
 0 pause output, 0 resume output
 0 output errors, 0 collisions, 0 interface resets
 0 late collisions, 0 deferred
 0 input reset drops, 0 output reset drops
 input queue (blocks free curr/low): hardware (0/0)
 output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
 37 packets input, 2304 bytes
 5 packets output, 300 bytes
 37 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
 Interface number is 14
 Interface config status is active
 Interface state is active
```

ルーティングと NAT の確認

Firewall Threat Defense CLI で、デフォルトルート（S*）が追加されていること、および管理インターフェイス（nlp_int_tap）に内部 NAT ルールが存在することを確認します。

show route

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
```

```
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C        10.89.5.0 255.255.255.192 is directly connected, outside
L        10.89.5.29 255.255.255.255 is directly connected, outside

>
```

show nat

```
> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface
service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface  service
 tcp ssh ssh
    translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
 ipv6  service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
    translate_hits = 0, untranslate_hits = 0
>
```

その他の設定の確認

次のコマンドを参照して、他のすべての設定が存在することを確認します。これらのコマンドの多くは、Firewall Management Center の **Devices** > **Device Management** ページにも表示されます。

show running-config sftunnel

```
> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305
```

show running-config ip-client

```
> show running-config ip-client
ip-client outside
```

show conn address *fmc_ip*

```
> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
       preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap  10.89.5.29(169.254.1.2):51231 outside  10.89.5.35:8305, idle 0:00:04,
 bytes 86684, flags UxIO
TCP nlp_int_tap  10.89.5.29(169.254.1.2):8305 outside  10.89.5.35:52019, idle 0:00:02,
 bytes 1630834, flags UIO
>
```

DDNS の更新が成功したかどうかを確認する

Firewall Threat Defense CLI で、DDNS の更新が成功したかどうかを確認します。

debug ddns

```
> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfully updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0
```

更新に失敗した場合は、**debug http** コマンドと **debug ssl** コマンドを使用します。証明書の検証が失敗した場合は、ルート証明書がデバイスにインストールされていることを確認します。

show crypto ca certificates *trustpoint_name*

DDNS の動作を確認するには：

show ddns update interface *fmc_access_ifc_name*

```
> show ddns update interface outside

Dynamic DNS Update on outside:
    Update Method Name Update Destination
    RBD_DDNS not available

Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

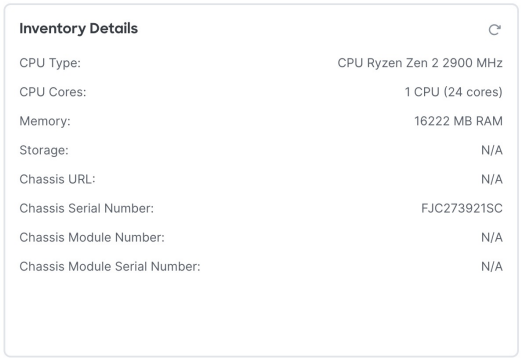
Firewall Management Center ログファイルの確認

https://cisco.com/go/fmc-reg-error を参照してください。

インベントリ詳細の表示

[デバイス（Device）] ページの [インベントリの詳細（Inventory Details）] セクションには、シャーシの詳細情報（CPU やメモリなど）が表示されます。

図 *51* : インベントリの詳細（***Inventory Details***）

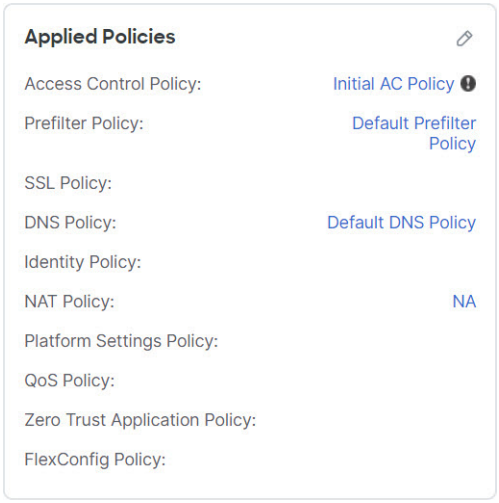


情報を更新するには、**Refresh** ( )をクリックします。

適用されたポリシーの編集

[デバイス（Device）]ページの[適用されたポリシー（Applied Policies）]セクションには、ファイアウォールに適用されている次のポリシーが表示されます。

図 *52* : *[*適用されたポリシー（***Applied Policies***）*]*



リンクのあるポリシーの場合、リンクをクリックしてポリシーを表示できます。

アクセス コントロール ポリシーについては、**Exclamation** ( ) アイコンをクリックして[トラブルシューティングのためのアクセスポリシー情報（Access Policy Information for Troubleshooting）]ダイアログボックスを表示します。このダイアログボックスには、アクセスルールがアクセス コントロール エントリ（ACE）に展開される方法が表示されます。

図 *53 : [*トラブルシューティングのためのアクセスポリシー情報（***Access Policy Information for Troubleshooting***）*]*

[デバイス管理（Device Management）]ページから、個々のデバイスにポリシーを割り当てることができます。

手順

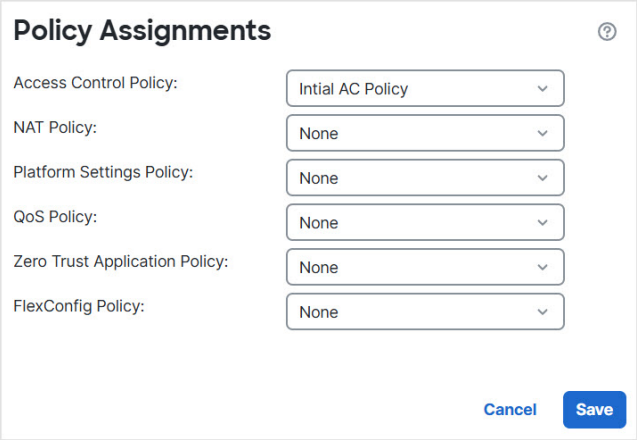
ステップ 1 **Devices** > **Device Management** を選択します。

ステップ 2 ポリシーを割り当てるデバイスの横にある **Edit** (✎) をクリックします。

ステップ 3 [デバイス（Device）] をクリックします。

ステップ 4 [適用されたポリシー（Applied Policies）] セクションで、**Edit** (✎) をクリックします。

図 *54* : ポリシー割り当て



ステップ 5 ポリシータイプごとに、ドロップダウンメニューからポリシーを選択します。既存のポリシーのみが一覧表示されます。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

- 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。

詳細設定の編集

[デバイス（Device）] ページの [詳細設定（Advanced Settings）] セクションには、以下で説明する詳細設定のテーブルが表示されます。これらの設定はいずれも編集できます。

表 *5* : *[*詳細設定（*Advanced*）*]* セクションのテーブルのフィールド

フィールド	説明
アプリケーションバイパス（Application Bypass）	デバイスでの自動アプリケーション バイパスの状態。
バイパスしきい値（Bypass Threshold）	自動アプリケーション バイパスのしきい値（ミリ秒）。

フィールド	説明
オブジェクトグループの検索	デバイスでのオブジェクトグループ検索の状態。動作中、FTD デバイスは、アクセスルールで使用されるネットワークオブジェクトまたはインターフェイス オブジェクトの内容に基づいて、アクセス制御ルールを複数のアクセス制御リストのエントリに展開します。オブジェクトグループ検索を有効にすることで、アクセス制御ルールの検索に必要なメモリを抑えることができます。オブジェクトグループ検索を有効にした場合、システムによってネットワークオブジェクトまたはインターフェイス オブジェクトは拡張されませんが、オブジェクトグループの定義に基づいて一致するアクセスルールが検索されます。オブジェクトグループ検索は、アクセスルールがどのように定義されるか、または Firepower Management Center にどのように表示されるかには影響しません。アクセス制御ルールと接続を照合するときに、デバイスがアクセス制御ルールを解釈して処理する方法のみに影響します。 （注） デフォルトでは、Management Center で初めて Threat Defense を追加すると、[オブジェクトグループ検索（Object Group Search）] が有効になります。
インターフェイス オブジェクトの最適化	デバイスでのインターフェイス オブジェクトの最適化の状態。展開時に、アクセス制御とプレフィルタポリシーで使用されるインターフェイスグループとセキュリティゾーンは、送信元/宛先インターフェイスペアごとに個別のルールを生成します。インターフェイス オブジェクトの最適化を有効にすると、システムはアクセス制御/プレフィルタルールごとに 1 つのルールを展開します。これにより、デバイス設定の簡素化および展開のパフォーマンス向上が可能になります。このオプションを選択する場合は、[オブジェクトグループ検索（Object Group Search）] オプションも選択して、デバイスのメモリ使用量を減らします。

次のトピックでは、デバイスの詳細設定を編集する方法について説明します。

（注） [パケットの転送（Transfer Packets）] 設定については、全般設定の編集 （1 ページ）を参照してください。

自動アプリケーションバイパスの設定

自動アプリケーションバイパス（AAB）を使用すると、Snort がダウンしている場合や、従来型デバイスで、パケットの処理に時間がかかりすぎる場合に、パケットが検出をバイパスでき

ます。AAB により、Snort は障害から 10 分以内に再起動します。また、Snort 障害の原因を調査するために分析できるトラブルシューティング データが生成されます。

注意 AAB のアクティブ化は、いくつかのパケットのインスペクションを一時的に中断する Snort プロセスを部分的に再起動します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、割り当てられたデバイスがトラフィックを処理する方法に応じて異なります。詳細はSnort の再起動によるトラフィックの動作を参照してください。

次の動作を確認してください。

Firewall Threat Defense の動作：Snort がダウンしている場合、指定されたタイマー期間の後に AAB がトリガーされます。Snort が稼働している場合、パケット処理が設定されたタイマーを超えても、AAB はトリガーされません。

従来型デバイスの動作：AAB は、インターフェイスを介してパケットを処理するために許可される時間を制限します。パケット処理の遅延は、ネットワークで許容できるパケット レイテンシとバランスを取って調整します。

この機能は任意の展開で使用できますが、インライン展開ではとりわけ価値があります。

一般に、遅延しきい値を超えた後は、高速パス パケットに対して侵入ポリシーの [ルール遅延しきい値（Rule Latency Thresholding）] を使用します。[ルール遅延しきい値（Rule Latency Thresholding）] により、エンジンがシャットダウンされたり、トラブルシューティング データが生成されることはありません。

検出がバイパスされると、デバイスがヘルス モニタリング アラートを生成します。

AAB はデフォルトで無効になっています。AAB を有効にするには、次の手順を実行します。

手順

ステップ 1 **Devices** > **Device Management**を選択します。

ステップ 2 詳細設定を編集するデバイスの横にある **Edit** (✎) をクリックします。

ステップ 3 [デバイス（Devices）] をクリックし、[詳細設定（Advanced Settings）] セクションの **Edit** (✎) をクリックします。

ステップ 4 [自動アプリケーション バイパス（Automatic Application Bypass）] をオンにします。

ステップ 5 [バイパスしきい値（Bypass Threshold）] に 250 ～ 60,000 ミリ秒を入力します。デフォルト設定は 3000 ミリ秒（ms）です。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

- 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。

オブジェクトグループ検索の構成

動作中、Firewall Threat Defense デバイスは、アクセスルールで使用されるネットワークオブジェクトまたはインターフェイスオブジェクトの内容に基づいて、アクセス制御ルールを複数のアクセス制御リストのエントリに展開します。オブジェクトグループ検索を有効にすることで、アクセス制御ルールの検索に必要なメモリを抑えることができます。オブジェクトグループ検索を有効にした場合、システムによってネットワークオブジェクトまたはインターフェイスオブジェクトは拡張されませんが、オブジェクトグループの定義に基づいて一致するアクセスルールが検索されます。オブジェクトグループ検索は、アクセスルールがどのように定義されているかや、Firewall Management Center にどのように表示されるかには影響しません。アクセス制御ルールと接続を照合するときに、デバイスがアクセス制御ルールを解釈して処理する方法のみに影響します。

オブジェクトグループ検索を有効にすると、ネットワークオブジェクトまたはインターフェイスオブジェクトを含むアクセスコントロールポリシーのメモリ要件が軽減されます。ただし、オブジェクトグループ検索では、ルールルックアップのパフォーマンスが低下して、CPU使用率が増大する可能性があることに注意してください。CPU に対する影響と、特定のアクセスコントロールポリシーに関するメモリ要件の軽減とのバランスをとる必要があります。ほとんどの場合、オブジェクトグループ検索を有効にすると、ネット運用が改善されます。

デフォルトでは、Firewall Management Center で初めて追加された Threat Defense デバイスではオブジェクトグループ検索が有効になっています。アップグレードされたデバイスの場合、デバイスでオブジェクトグループ検索が無効に設定されている場合は、手動で有効にする必要があります。一度に1つのデバイスで有効にできます。グローバルに有効にすることはできません。ネットワークオブジェクトまたはインターフェイスオブジェクトを使用するアクセスルールを展開するすべてのデバイスで有効にすることを推奨します。

（注） オブジェクトグループの検索を有効にしてから、デバイスを設定し、しばらくの間操作した場合、後からこの機能を無効にすると、望ましくない結果になる可能性があることに注意してください。オブジェクトグループの検索を無効にすると、既存のアクセス制御ルールがデバイスの実行コンフィギュレーションで拡張されます。デバイスで使用可能なメモリよりも多くのメモリが拡張に必要な場合、デバイスが不整合状態になり、パフォーマンスに影響する可能性があります。デバイスが正常に動作している場合は、一度有効にしたオブジェクトグループ検索を無効にしないでください。

始める前に

- Model support：Firewall Threat Defense
- 各デバイスでトランザクションコミットも有効にすることを推奨します。デバイスCLIから **asp rule-engine transactional-commit access-group** コマンドを入力します。
- この設定を変更すると、デバイスが ACL を再コンパイルしている間、システムの動作が中断される可能性があります。この設定はメンテナンス期間中にのみ変更することを推奨します。

- FlexConfig を使用して **object-group-search threshold** コマンドを設定し、しきい値を有効にしてパフォーマンスの低下を防止することができます。しきい値を使用した動作では、接続ごとに送信元と宛先の両方のIPアドレスがネットワーク オブジェクトと照合されます。発信元アドレスに一致するオブジェクトの数が、宛先アドレスと一致する数の1万倍を超えると接続が切断されます。一致件数が膨大になることを防ぐためにルールを設定します。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択します。

ステップ 2 ルールを設定する Firewall Threat Defense デバイスの横にある**Edit** (✎)をクリックします。

ステップ 3 [デバイス（Devices）] タブをクリックし、[詳細設定（Advanced Settings）] セクションの**Edit** (✎)をクリックします。

ステップ 4 [オブジェクトグループの検索（Object Group Search）] をオンにします。

ステップ 5 ネットワークオブジェクトに加えてインターフェイス オブジェクトでオブジェクトグループの検索を機能させるには、[インターフェイスオブジェクトの最適化（Interface Object Optimization）] をオンにします。

[インターフェイスオブジェクトの最適化（Interface Object Optimization）] を選択しない場合は、システムで、ルールで使用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が使用されずに、送信元/インターフェイスのペアごとに個別のルールが展開されます。これは、インターフェイスグループがオブジェクトグループの検索処理に使用できないことを意味します。

ステップ 6 [保存（Save）] をクリックします。

インターフェイス オブジェクトの最適化の設定

展開時に、アクセス制御とプレフィルタポリシーで使用されるインターフェイスグループとセキュリティゾーンは、送信元/宛先インターフェイスペアごとに個別のルールを生成します。インターフェイス オブジェクトの最適化を有効にすると、システムはアクセス制御/プレフィルタルールごとに1つのルールを展開します。これにより、デバイス設定の簡素化および展開のパフォーマンス向上が可能になります。このオプションを選択する場合は、[オブジェクトグループ検索（Object Group Search）] オプションも選択して、デバイスのメモリ使用量を減らします。

インターフェイス オブジェクトの最適化はデフォルトで無効になっています。一度に1つのデバイスで有効にできます。グローバルに有効にすることはできません。

（注） インターフェイス オブジェクトの最適化を無効にすると、既存のアクセス制御ルールはインターフェイス オブジェクトを使用せずに展開されるため、展開に時間がかかる場合があります。また、オブジェクトグループ検索が有効になっている場合、その利点はインターフェイスオブジェクトには適用されず、デバイスの実行中の設定のアクセス制御ルールが拡張されることがあります。デバイスで使用可能なメモリよりも多くのメモリが拡張に必要な場合、デバイスが不整合状態になり、パフォーマンスに影響する可能性があります。

始める前に

Model support：Firewall Threat Defense

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択します。

ステップ 2 ルールを設定する FTD デバイスの横にある**Edit** (✎)をクリックします。

ステップ 3 [デバイス（Devices）] タブをクリックし、[詳細設定（Advanced Settings）] セクションの**Edit** (✎)をクリックします。

ステップ 4 [インターフェイスオブジェクトの最適化（Interface Object Optimization）] をオンにします。

ステップ 5 [保存（Save）] をクリックします。

展開設定の編集

[Device] ページの [Deployment Settings] セクションには、以下の表に記載された情報が表示されます。

図 *55 :* 展開設定

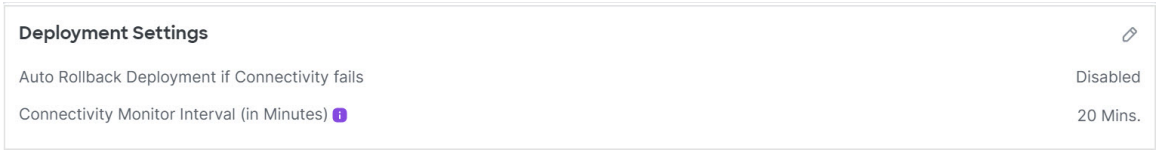


表 *6*: 展開設定

フィールド	説明
Auto Rollback Deployment if Connectivity Fails	[Enabled] と [Disabled] があります。 展開の結果として管理接続が失敗した場合は、自動ロールバックを有効にすることができます。特に、管理センターへのアクセスにデータを使用し、データインターフェイスを誤って構成した場合に当てはまります。
Connectivity Monitor Interval (in Minutes)	構成をロールバックする前に待機する時間を示します。

[デバイス管理（Device Management）]ページから展開設定を設定できます。展開設定には、展開の結果として管理接続が失敗した場合の展開の自動ロールバックの有効化が含まれます。特に、管理センターへのアクセスにデータを使用し、データインターフェイスを誤って構成した場合です。代替として、**configure policy rollback** コマンドを使用して、構成を手動でロールバックすることもできます（Firewall Management Center の接続が失われた場合の構成の手動ロールバック （70 ページ）を参照）。

次のガイドラインを参照してください。

- 前回の展開のみ Firewall Threat Defense でローカルに使用できます。さらに以前の展開にロールバックすることはできません。
- ロールバックは、高可用性ではサポートされていますが、クラスタリングの展開ではサポートされていません。
- ロールバックは、Firewall Management Center で設定できる構成にのみ影響します。たとえば、ロールバックは、Firewall Threat Defense CLI でのみ設定できる専用管理インターフェイスに関連するローカル構成には影響しません。**configure network management-data-interface** コマンドを使用した最後の Firewall Management Center 展開後にデータインターフェイス設定を変更し、rollback コマンドを使用すると、それらの設定は保持されないことに注意してください。最後に展開された Firewall Management Center 設定にロールバックされます。
- UCAPL/CC モードはロールバックできません。
- 以前の展開中に更新されたアウトオブバンド SCEP 証明書データはロールバックできません。
- ロールバック中に、現在の設定がクリアされるため、接続がドロップされます。

手順

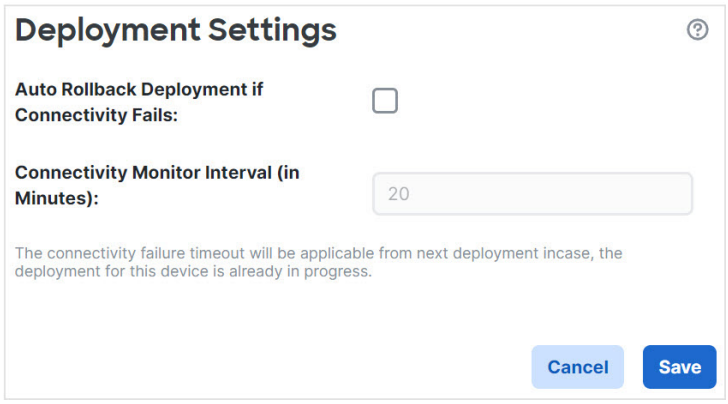
ステップ 1 **Devices** > **Device Management** を選択します。

ステップ 2 ポリシーを割り当てるデバイスの横にある **Edit** (✎) をクリックします。

ステップ 3 [デバイス（Device）] をクリックします。

ステップ 4 [展開設定（Deployment Settings）] セクションで、**Edit** (✎) をクリックします。

図 56 : 展開設定



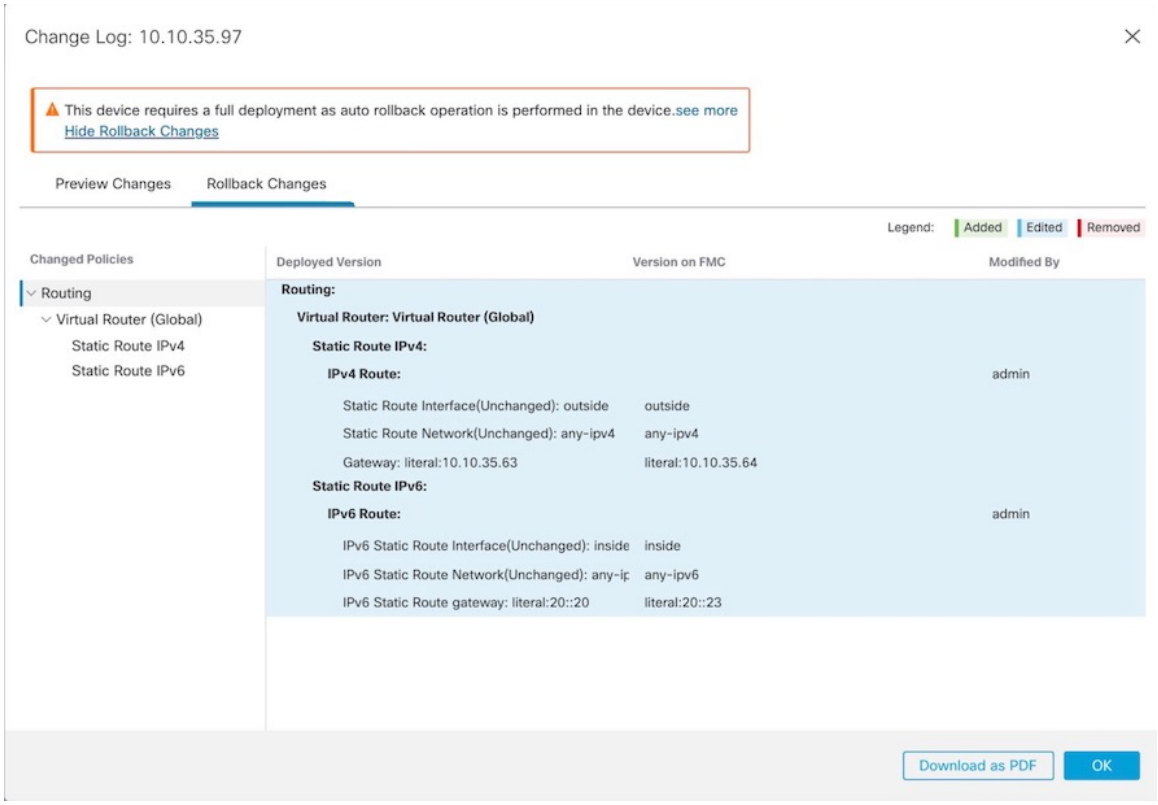
ステップ 5 自動ロールバックを有効にするには、[接続が失敗した場合の自動ロールバック展開（Auto Rollback Deployment if Connectivity Fails）] をオンにします。

ステップ 6 [接続モニタ間隔（分）（Connectivity Monitor Interval (in Minutes)）] を設定して、構成をロールバックする前に待機する時間を設定します。デフォルトは 20 分です。

ステップ 7 ロールバックが発生した場合は、次の手順について以下を参照してください。

- 自動ロールバックが成功した場合は、フル展開を行うように指示する成功メッセージが表示されます。
- [展開（Deploy）]、[高度な展開（Advanced Deploy）] 画面の順に移動し、**Preview** (🔍) アイコンをクリックすると、ロールバックされた設定の一部を表示することもできます（設定変更の展開を参照）。[ロールバックの変更を表示（Show Rollback Changes）] をクリックして変更を表示し、[ロールバックの変更を非表示（Hide Rollback Changes）] をクリックして変更を非表示にします。

図 *57*: ロールバックの変更



- [展開履歴のプレビュー（Deployment History Preview）] で、ロールバックの変更を表示できます。「展開履歴の表示」を参照してください。

ステップ 8 管理接続が再確立されたことを確認します。

Firewall Management Center の接続状態ページで、管理接続の状態を確認します。**Devices** > **Device Management** に移動し、[デバイス（Devices）] タブの [管理（Management）] 領域で、[接続状態（Connection Status）] をクリックして [接続状態（Connection Status）] ページを表示します。

管理接続のステータスを表示するには、Firewall Threat Defense CLI で、**sftunnel-status-brief** コマンドを入力します。

接続の再確立に 10 分以上かかる場合は、接続のトラブルシューティングを行う必要があります。データインターフェイスでの管理接続のトラブルシューティング （72 ページ） を参照してください。

クラスタのヘルスモニター設定の編集

[クラスタ（Cluster）]ページの[クラスタヘルスモニターの設定（Cluster Health Monitor Settings）]セクションには、次の表で説明されている設定が表示されます。

図 *58* : クラスタのヘルスモニターの設定

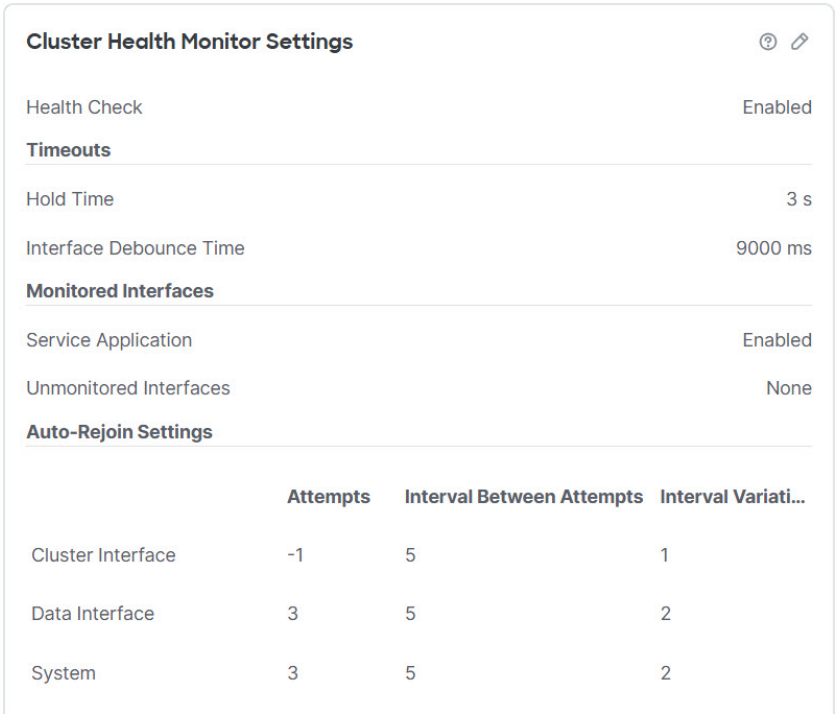


表 *7* : [クラスタヘルスモニターの設定（*Cluster Health Monitor Settings*）]セクションテーブルのフィールド

フィールド	説明
タイムアウト（Timeouts）	
保留時間（Hold Time）	指定できる範囲は0.3～45秒です。デフォルトは3秒です。ノードの状態を確認するため、クラスタノードはクラスタ制御リンクで他のノードにハートビートメッセージを送信します。ノードが保留時間内にピアノードからハートビートメッセージを受信しない場合、そのピアノードは応答不能またはデッド状態と見なされます。
インターフェイスのデバウンス時間（Interface Debounce Time）	指定できる範囲は300～9000ミリ秒です。デフォルトは500 msです。インターフェイスのデバウンス時間は、インターフェイスで障害が発生していると見なされ、クラスタからノードが削除されるまでの時間です。

フィールド	説明
Monitored Interfaces（モニタリング対象インターフェイス）	インターフェイスのヘルス チェックはリンク障害をモニターします。特定の論理インターフェイスのすべての物理ポートが、特定のノード上では障害が発生したが、別のノード上の同じ論理インターフェイスでアクティブポートがある場合、そのノードはクラスタから削除されます。ノードがメンバーをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのノードが確立済みノードであるか、またはクラスタに参加しようとしているかによって異なります。
サービスアプリケーション（Service Application）	Snort プロセスおよび disk-full プロセスが監視されているかどうかを示します。
モニタリング対象外のインターフェイス（Unmonitored Interfaces）	モニタリング対象外のインターフェイスを表示します。
自動再結合の設定（Auto-Rejoin Settings）	
クラスタインターフェイス（Cluster Interface）	クラスタ制御リンクに障害が発生した後に自動再結合の設定を表示します。
試行（*Attempts*）	指定できる範囲は -1 ～ 65535 です。デフォルトは -1（無制限）です。再結合の試行回数を設定します。
試行の間隔（*Interval Between Attempts*）	指定できる範囲は 2 ～ 60 です。デフォルトは 5 分です。再結合試行の間隔を分単位で定義します。
間隔のバリエーション（*Interval Variation*）	指定できる範囲は 1 ～ 3 です。デフォルトは間隔の 1 倍です。試行ごとに間隔を長くするかどうかを定義します。
データインターフェイス（Data Interfaces）	データインターフェイスに障害が発生した後に自動再結合の設定を表示します。
試行（*Attempts*）	指定できる範囲は -1 ～ 65535 です。デフォルトは 3 です。再結合の試行回数を設定します。
試行の間隔（*Interval Between Attempts*）	指定できる範囲は 2 ～ 60 です。デフォルトは 5 分です。再結合試行の間隔を分単位で定義します。
間隔のバリエーション（*Interval Variation*）	指定できる範囲は 1 ～ 3 です。デフォルトは間隔の 2 倍です。試行ごとに間隔を長くするかどうかを定義します。
システム（System）	内部エラーが発生した後に自動再結合の設定を表示します。内部エラーには、アプリケーション同期のタイムアウト、一貫性のないアプリケーションステータスなどがあります。

フィールド	説明
試行（*Attempts*）	指定できる範囲は -1 ～ 65535 です。デフォルトは 3 です。再結合の試行回数を設定します。
試行の間隔（*Interval Between Attempts*）	指定できる範囲は 2 ～ 60 です。デフォルトは 5 分です。再結合試行の間隔を分単位で定義します。
間隔のバリエーション（*Interval Variation*）	指定できる範囲は 1 ～ 3 です。デフォルトは間隔の 2 倍です。試行ごとに間隔を長くするかどうかを定義します。

（注） システムのヘルスチェックを無効にすると、システムのヘルスチェックが無効化されている場合に適用されないフィールドは表示されません。

これらの設定は、このセクションから変更できます。

任意のポートチャネル ID、単一の物理インターフェイス ID、Snort プロセス、および disk-full プロセスを監視できます。ヘルス モニタリングは VLAN サブインターフェイス、または VNI やBVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。

手順

ステップ 1 **Devices** > **Device Management** を選択します。

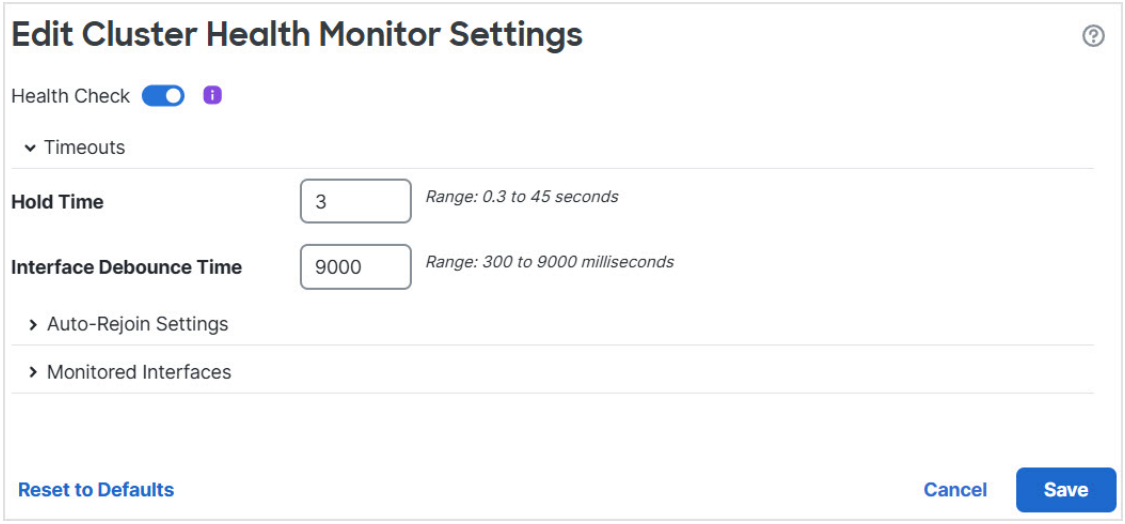
ステップ 2 変更するクラスタの横にある **Edit** (✎) をクリックします。

ステップ 3 [クラスタ（Cluster）] をクリックします。

ステップ 4 [クラスタのヘルスモニターの設定（Cluster Health Monitor Settings）] セクションで、**Edit** (✎) をクリックします。

ステップ 5 [ヘルスチェック（Health Check）] スライダをクリックして、システムのヘルスチェックを無効にします。

図 *59 :* システムヘルスチェックの無効化



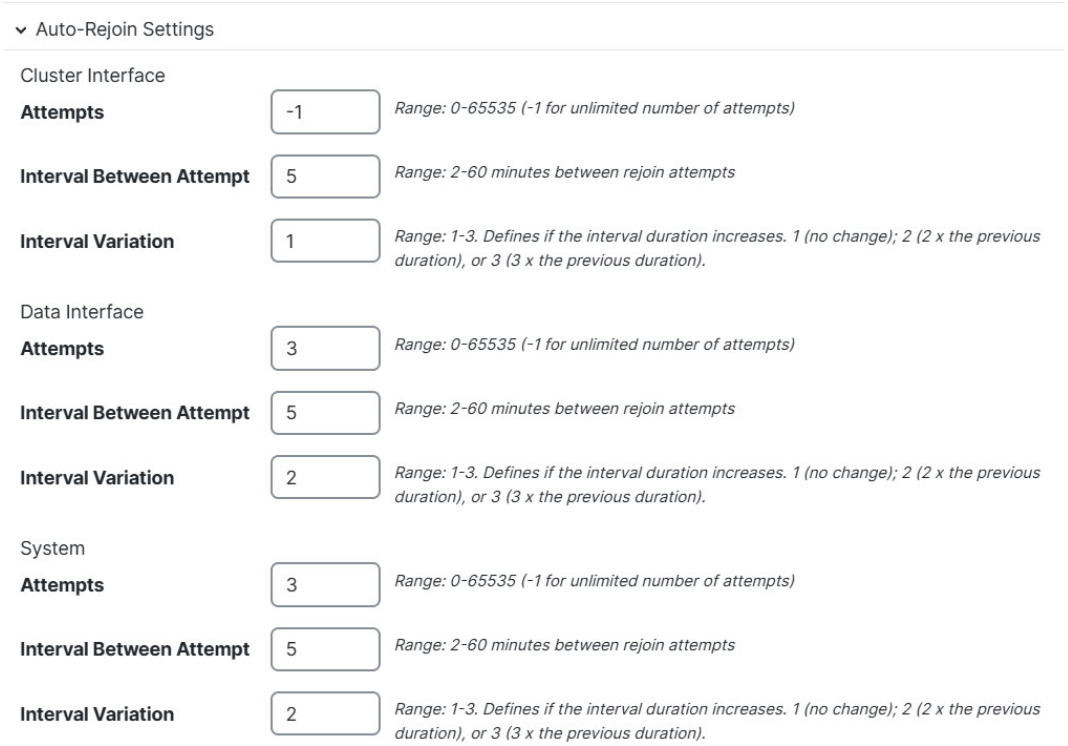
何らかのトポロジ変更（たとえばデータインターフェイスの追加/削除、ノードやスイッチのインターフェイスの有効化/無効化、VSS や vPC（または VNet）を形成するスイッチの追加）を行うときには、システムのヘルスチェック機能を無効にし、無効化したインターフェイスのモニタリングも無効にしてください。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、システムのヘルスチェック機能を再度有効にてインターフェイスをモニタリングできます。

ステップ 6 ホールド時間とインターフェイスのデバウンス時間を設定します。

- [ホールド時間（Hold Time）]：ノードのハートビート ステータス メッセージの時間間隔を指定します。指定できる範囲は 3 ～ 45 秒で、デフォルトは 3 秒です。
- [インターフェイスのデバウンス時間（Interface Debounce Time）]：デバウンス時間は 300 ～ 9000 ms の範囲で値を設定します。デフォルトは 500 ms です。値を小さくすると、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイスのステータス更新が発生すると、インターフェイス障害としてマーク付けされるまで、ノードは指定されたミリ秒数待機します。その後、ノードはクラスタから削除されます。EtherChannel がダウン状態からアップ状態に移行する場合（スイッチがリロードされた、スイッチで EtherChannel が有効になったなど）、デバウンス時間がより長くなり、ポートのバンドルにおいて別のクラスタノードの方が高速なため、クラスタノードでインターフェイスの障害が表示されることを妨げることがあります。

ステップ 7 ヘルス チェック失敗後の自動再結合クラスタ設定をカスタマイズします。

図 *60 :* 自動再結合の設定



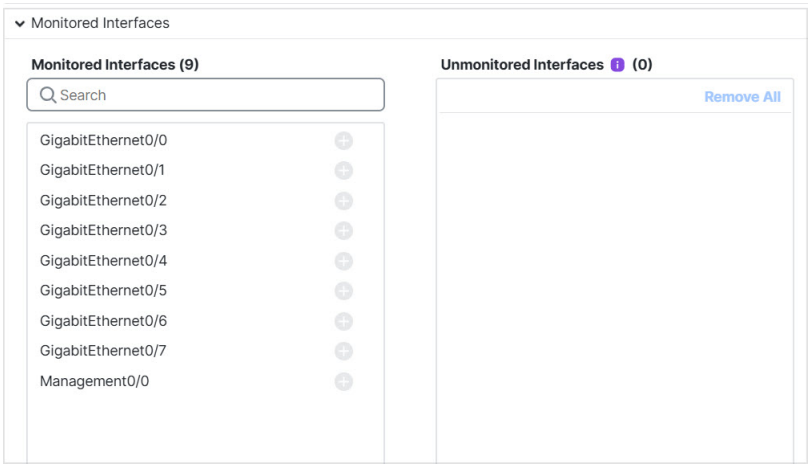
[クラスタインターフェイス（Cluster Interface）]、[データインターフェイス（Data Interface）]、および[システム（System）]に次の値を設定します（内部エラーには、アプリケーションの同期タイムアウト、一貫性のないアプリケーションステータスなどがあります）。

- [試行数（Attempts）]：再結合の試行回数を 0 ～ 65535 の範囲の値に設定します。**0** は自動再結合を無効化します。[クラスタインターフェイス（Cluster Interface）] のデフォルト値は -1（無制限）です。[データインターフェイス（Data Interface）] と [システム（System）] のデフォルト値は 3 です。
- [試行の間隔（Interval Between Attempts）]：再結合試行の間隔を 2 ～ 60 の分単位で定義します。デフォルト値は 5 分です。クラスタへの再参加をノードが試行する最大合計時間は、最後の障害発生時から 14400 分（10 日）に制限されます。
- [間隔のバリエーション（Interval Variation）]：間隔を増加させるかどうかを定義します。1 ～ 3 の範囲で値を設定します（**1**：変更なし、**2**：直前の間隔の 2 倍、**3**：直前の間隔の 3 倍）。たとえば、間隔を 5 分に設定し、変分を 2 に設定した場合は、最初の試行が 5 分後、2 回目の試行が 10 分後（2 x 5）、3 階目の試行が 20 分後（2 x 10）となります。デフォルト値は、[クラスタインターフェイス（Cluster Interface）] の場合は **1**、[データインターフェイス（Data Interface）] および [システム（System）] の場合は **2** です。

ステップ 8 [モニタリング対象のインターフェイス（Monitored Interfaces）] または [モニタリング対象外のインターフェイス（Unmonitored Interfaces）] ウィンドウでインターフェイスを移動して、モニタリング対象のインターフェイスを設定します。[サービスアプリケーションのモニタリング

を有効にする（Enable Service Application Monitoring）] をオンまたはオフにして、Snort プロセスと disk-full プロセスのモニタリングを有効または無効にすることもできます。

図 *61* : モニタリング対象インターフェイスの設定



インターフェイスのヘルスチェックはリンク障害をモニターします。特定の論理インターフェイスのすべての物理ポートが、特定のノード上では障害が発生したが、別のノード上の同じ論理インターフェイスでアクティブポートがある場合、そのノードはクラスタから削除されます。ノードがメンバーをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのノードが確立済みノードであるか、またはクラスタに参加しようとしているかによって異なります。デフォルトでは、ヘルスチェックはすべてのインターフェイス、および Snort プロセスと disk-full プロセスで有効になっています。

必須以外のインターフェイスのヘルス モニタリングを無効にできます。

何らかのトポロジ変更（たとえばデータインターフェイスの追加/削除、ノードやスイッチのインターフェイスの有効化/無効化、VSS や vPC（または VNet）を形成するスイッチの追加）を行うときには、システムのヘルスチェック機能を無効にし、無効化したインターフェイスのモニタリングも無効にしてください。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、システムのヘルスチェック機能を再度有効にてインターフェイスをモニタリングできます。

ステップ 9 [保存（Save）] をクリックします。

ステップ 10 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。

デバイス設定の履歴

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
Firewall Management Center での緊急オンデバイス設定およびアウトオブバンド設定検出用のリカバリ設定モード	7.7.0	7.7.0	デバイスへの管理接続が失われた場合は、デバイス CLI で選択設定を直接変更し、以下を行うことができます。 • マネージャアクセスにデータインターフェイスを使用している場合は、管理接続を復元します • 接続が復元されるまで待つことができない選択ポリシーの変更を行います 管理接続が復元されると、Firewall Management Center がデバイス上の設定変更を検出します。Firewall Management Center では、デバイス設定は自動的に更新されません。設定の違いを確認し、デバイス設定が異なることを確認してから、展開する前に Firewall Management Center で同じ変更を手動で行う必要があります。 新規/変更された診断 CLI（**system support diagnostic-cli**）コマンド：**configure recovery-config** 新規/変更された画面：**[デバイス（Devices）]**>**[デバイス管理（Device Management）]** > **[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）]**
冗長マネージャアクセス データ インターフェイスでサポートされる高可用性	7.7.0	7.7.0	高可用性を備えた冗長マネージャ アクセス データ インターフェイスを使用できるようになりました。
View CLI output for a device or device cluster.	7.4.1	任意	You can view a set of pre-defined CLI outputs that can help you troubleshoot the device or cluster. You can also enter any **show** command and see the output. New/modified screens: **Devices** > **Device Management** > **Cluster** > **General**
Troubleshooting file generation and download available from Device and Cluster pages.	7.4.1	7.4.1	You can generate and download troubleshooting files for each device on the Device page and also for all cluster nodes on the Cluster page. For a cluster, you can download all files as a single compressed file. You can also include cluster logs for the cluster for cluster nodes. You can alternatively trigger file generation from the **Devices** > **Device Management** > **More** > **Troubleshoot Files** menu. New/modified screens: • **Devices** > **Device Management** > **Device** > **General** • **Devices** > **Device Management** > **Cluster** > **General**

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
クラスタのヘルスモニターの設定。	7.3.0	いずれか	クラスタのヘルスモニター設定を編集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）]** > **[クラスタ（Cluster）]** > **[クラスタのヘルスモニターの設定（Cluster Health Monitor Settings）]** （注） 以前にFlexConfigを使用してこれらの設定を行った場合は、展開前に必ずFlexConfigの設定を削除してください。削除しなかった場合は、FlexConfig の設定によって Management Center の設定が上書きされます。
冗長マネージャアクセス データ インターフェイス。	7.3.0	7.3.0	マネージャアクセスにデータインターフェイスを使用する場合、プライマリインターフェイスがダウンしたときに管理機能を引き継ぐよう、セカンダリインターフェイスを構成できます。デバイスは、SLAモニタリングを使用して、スタティックルートの実行可能性と、両方のインターフェイスを含むECMPゾーンを追跡し、管理トラフィックで両方のインターフェイスが使用できるようにします。 新規/変更された画面： • **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[デバイス（Device）]** > **[管理（Management）]** • **[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）]** > **[マネージャアクセス（Manager Access）]**
ポリシーのロールバックは高可用性デバイスでサポートされています。	7.2.0	7.2.0	**configure policy rollback** コマンドは高可用性デバイスでサポートされています。

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
展開で管理接続が失われた場合の自動ロールバック。	7.2.0	7.2.0	展開によって Management Center と Threat Defense 間の管理接続がダウンした場合に備えて、設定の自動ロールバックを有効にできるようになりました。以前は、**configure policy rollback** コマンドを使用して手動で設定をロールバックすることしかできませんでした。 新規/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [展開設定（Deployment Settings）]** • **[展開（Deploy）] > [高度な展開（Advanced Deploy）] > [プレビュー（Preview）]** • **[展開（Deploy）] > [展開履歴（Deployment History）] > [プレビュー（Preview）]**
アクセスコントロールルールではオブジェクトグループ検索がデフォルトで有効です。	7.2.0	7.2.0	バージョン 7.2.0 以降の管理対象デバイスでは、**オブジェクトグループ検索**の設定がデフォルトで有効です。このオプションは、[デバイス管理（Device Management）] ページでデバイス設定を編集するときの [詳細設定（Advanced Settings）] セクションにあります。
デバイス設定のインポート/エクスポート。	7.1.0	7.1.0	次の使用例で、デバイス固有の設定をエクスポートし、同じデバイスに保存された設定をインポートできます。 • デバイスを別の FMC に移動する。 • 古い設定を復元する。 • デバイスを再登録する。 新規/変更された画面：[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [全般（General）]
FTD での FMC IP アドレスの更新。	6.7.0	6.7.0	FMC IP アドレスを変更する場合に、FTD CLI を使用してデバイスを更新できるようになりました。 新規/変更されたコマンド： **configure manager edit**

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。