



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. [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
2. 変更するデバイスの横にある [編集 (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 \(1 ページ\)](#)
- [ライセンス設定の編集 \(9 ページ\)](#)
- [システム情報の表示 \(10 ページ\)](#)
- [検査エンジンの表示 \(11 ページ\)](#)
- [正常性設定の編集 \(12 ページ\)](#)
- [管理設定の編集 \(12 ページ\)](#)
- [インベントリ詳細の表示 \(57 ページ\)](#)
- [適用されたポリシーの編集 \(57 ページ\)](#)
- [詳細設定の編集 \(59 ページ\)](#)
- [展開設定の編集 \(64 ページ\)](#)
- [クラスタのヘルスモニター設定の編集 \(67 ページ\)](#)
- [デバイス設定の履歴 \(73 ページ\)](#)

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

General	
Name:	Thing1
Transfer Packets:	Yes
Mode:	Routed
Compliance Mode:	None
Performance Profile:	Default
TLS Crypto Acceleration:	Disabled
Device Configuration: Import Export Download	

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。
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。
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 (3 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 (5 ページ) を参照してください。

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 [デバイス (Devices)] > [デバイス管理 (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 [編集 (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、[編集 (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を完全な生成をとまなうため、通常の展開よりも時間がかかります。

ステップ 5 [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 \(3 ページ\)](#) および [デバイス設定のエクスポートとインポート \(5 ページ\)](#) を参照してください。

ステップ 6 [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。

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 [デバイス (Devices)] > [デバイス管理 (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 [編集 (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。

- [デバイス設定の取得 (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。
- [デバイス設定のプッシュ (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

[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 からデバイスを削除してから、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 から削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。
- 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。
同じ名前でも値が異なるオブジェクトが存在する。	<p>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。</p> <p>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。</p> <p>他のすべてのオブジェクト：値が異なっても、既存のオブジェクトを再利用します。</p>
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 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

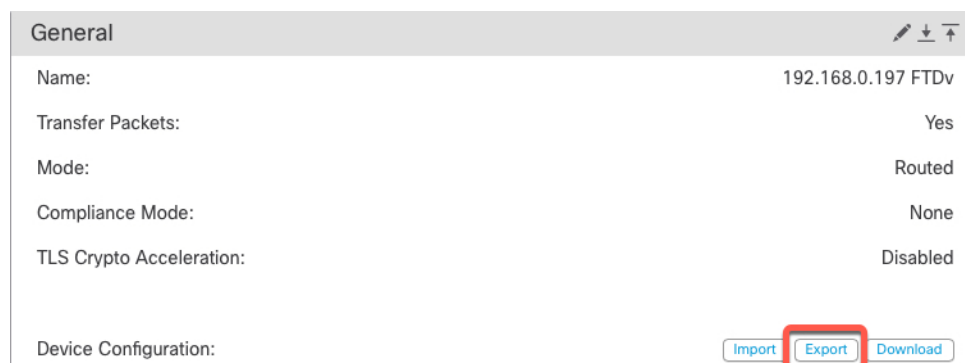
ステップ 2 編集するデバイスの横にある [編集 (Edit)] (✎) をクリックします。

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）。

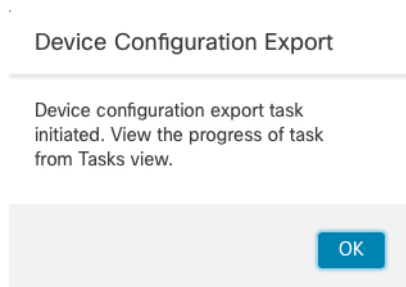
a) [General (全般)] エリアで [エクスポート (Export)] をクリックします。

図 2: 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。

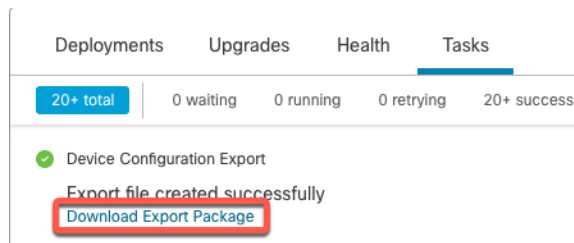
図 3: エクスポートの確認



[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。

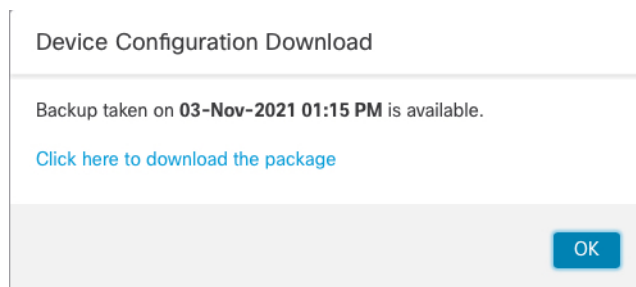
- b) [通知 (Notifications)] > [タスク (Tasks)] ページで、エクスポートが完了したことを確認します。[エクスポートパッケージのダウンロード (Download Export Package)] をクリックします。または、[全般 (General)] エリアの [ダウンロード (Download)] ボタンをクリックすることもできます。

図 4: 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 5: 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 6: デバイス設定のインポート

General	
Name:	192.168.0.197 FTDv
Transfer Packets:	Yes
Mode:	Routed
Compliance Mode:	None
TLS Crypto Acceleration:	Disabled
Device Configuration:	<input type="button" value="Import"/> <input type="button" value="Export"/> <input type="button" value="Download"/>

現在の設定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、設定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 7: パッケージのインポート

Device Configuration Import

This will replace current device configuration with new configuration from imported file. Do you want to continue?

図 8: パッケージに移動

Name
<input type="button" value="Add"/> <input type="button" value="Remove"/> <input type="button" value="Refresh"/>
DeviceExport-0434ef00-15bb-11ec-bb94-93bdde3ad19d.sfo

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 9: インポートの確認

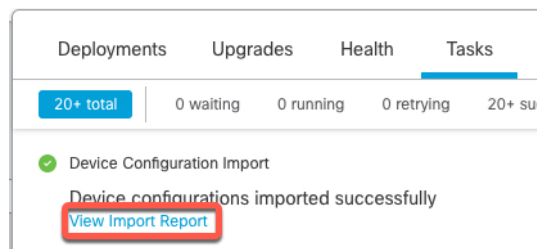
Device Configuration Import

Device configuration import task initiated. View the progress of task from Tasks view.

[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します。インポートタスクの[通知 (Notifications)] > [タスク (Tasks)] ページで、[インポートレポートの表示 (View Import Report)] をクリックします。

図 10: 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。

Cisco Firepower Management Center

Device Configuration Import Reports

Device	Shared Policies	Device Configurations
0434ef00-15bb-11ec-bb94-93bde3ad19d	Report does not exist	Device configurations import report

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** [デバイス (Devices)] > [デバイス管理 (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 [編集 (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、[編集 (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 11: システム

System		🔌 🔄
Model:	Cisco Firepower 1010 Threat Defense	
Serial:	JAD253802SG	
Time:	2024-12-03 18:08:13	
Time Zone:	UTC (UTC+0:00)	
Version:	7.7.0	
Time Zone setting for Time based Rules:	UTC (UTC+0:00)	
Inventory:	View	

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
[デバイスのシャットダウン (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。
[デバイスの再起動 (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。

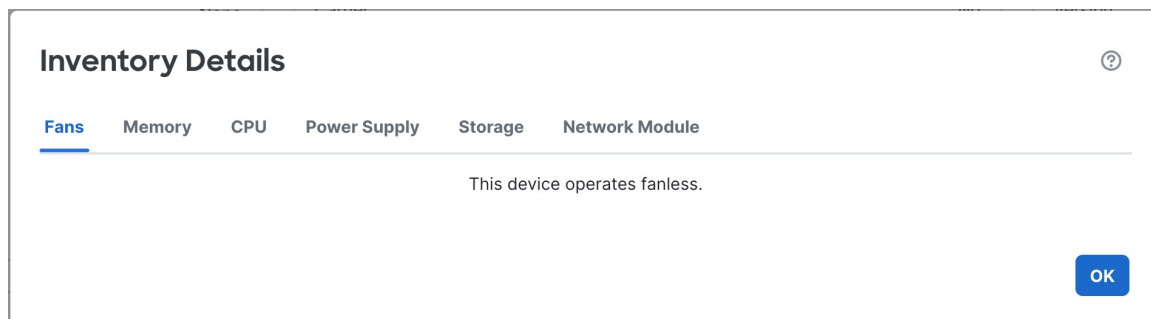
フィールド	説明
Version	管理対象デバイスに現在インストールされているソフトウェアのバージョン。
時刻ベースルールのタイムゾーン設定 (Time Zone setting for time-based rules)	デバイスのプラットフォーム設定で指定されたタイムゾーンでの、デバイスの現在のシステム時刻。
インベントリ	インベントリの詳細を表示します。 デバイスインベントリの表示 を参照してください。

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 12: 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、デバイスが Snort 2 と Snort 3 のデバイスで使用できる唯一のエンジンです。検索エンジンを切り替えるには、[Cisco Secure Firewall Management Center Snort 3 Configuration Guide](#) 個々のデバイス上での Snort 3 の有効化を参照してください。

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。

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。
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。

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 [デバイス (Devices)] > [デバイス管理 (Device Manageme)] ページで、デバイスの [編集 (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 13: 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。[編集 (Edit)] (✎)

図 14: 管理アドレスの編集

Management	
Remote Host Address:	10.89.5.29
Secondary Address:	
Status:	✔
Manager Access Interface:	Data Interface
Manager Access Details:	Configuration

- 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 15: 管理 IP アドレス

Management	
Remote Host Address:	10.89.5.29
Secondary Address:	10.99.11.6
<div> Cancel Save </div>	

- 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。

- [ルーティング (Routing)] をクリックします。
- 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。
- [ECMP] をクリックし、[追加 (Add)] をクリックします。
- [名前 (Name)] に ECMP ゾーンの名前を入力します。
- [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 16: ECMP ゾーンの追加

The screenshot shows a web-based configuration window titled "Add ECMP". At the top, there is a "Name" input field with the text "redundant-mgmt". Below the input field, the window is divided into two main sections: "Available Interfaces" on the left and "Selected Interfaces" on the right. The "Available Interfaces" section is currently empty. The "Selected Interfaces" section contains two entries: "outside" and "redundant", each with a small trash can icon to its right. A blue "Add" button is located between the two sections. At the bottom right of the window, there are two buttons: "Cancel" and "OK".

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 17 : Add/Edit Static Route

Edit Static Route Configuration

Type: ☒ IPv4 ☐ IPv6

Interface*
outside

(Interface starting with this icon signifies it is available for route leak)

Available Network +

Q Search

10.99.11.1
any-ipv4
IPv4-Benchmark-Tests
IPv4-Link-Local
IPv4-Multicast
IPv4-Private-10.0.0.0-8

Add

Selected Network

any-ipv4

Ensure that egress virtualrouter has route to that destination

Gateway
10.89.5.1 +

Metric:
1
(1 - 254)

Tunneled: ☐ (Used only for default Route)

Route Tracking:
+

Cancel OK

- [Static Route] をクリックします。
- [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 [編集 (Edit)] (✎) をクリックします。
- [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。
- 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。
- デフォルトの [ゲートウェイ (Gateway)] を入力します。
- [ルートトラッキング (Route Tracking)] の場合、[追加 (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。
- 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 18: SLA モニターの追加

The screenshot shows the 'New SLA Monitor Object' configuration window. The fields are as follows:

Field	Value
Name	mgmt-secondary
Description	
Frequency (seconds)	60
SLA Monitor ID*	2
Threshold (milliseconds)	
Timeout (milliseconds)	5000
Data Size (bytes)	28
ToS	
Number of Packets	1
Monitor Address*	10.89.5.35
Available Zones	mgmt, outside
Selected Zones/Interfaces	mgmt

Buttons: Cancel, Save

- 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 アドレスを変更する

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（25 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 コマンドリファレンス](#) 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 \(30 ページ\)](#) 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 \(30 ページ\)](#) 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) ハイアベイラビリティ Firewall Management Center 構成では、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、HA 同期後も、セカンダリ Firewall Management Center には変更が反映されません。セカンダリ Firewall Management Center も更新されるようにするには、2 つの Firewall Management Center の間でロールを切り替えて、セカンダリ Firewall Management Center をアクティブユニットにします。現在アクティブな Firewall Management Center のデバイス管理のページで、登録されているデバイスの管理 IP アドレスを変更します。

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のみ) 2 番目の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、イベントチャン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ン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 アドミニストレーションガイド](#)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 *ip6_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 *ip6_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 *ip6_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 \(20 ページ\)](#)」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。

（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 64～1500、IPv6 を有効にした場合は 1280～1500 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 64～9000、IPv6 を有効にした場合は 1280～9000 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構成されています。HTTP ダイジェスト経由で認証できるプロキシサーバーを使用できます。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 \(30 ページ\)](#) 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 \(30 ページ\)](#) 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 \(30 ページ\)](#) 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に変更を行う必要があります ([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 \(28 ページ\)](#) を参照)。データ管理インターフェ

こ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。



(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 \(18 ページ\)](#) 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 コマンドリファレンス](#) 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 (30 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 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、[デバイス (Devices)]>[デバイス管理 (Device Management)]、[編集 (Edit)] (✎) の順に選択します。[デバイス (Device)]>[管理 (Management)] エリアで、[マネージャアクセス - 構成詳細 (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構成変更を検出し、デプロイへのデプロイメントをブロックします。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。と [構成 (Configuration)] タブのデバイス間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。
- IP アドレスと名前を古いデータ管理インターフェイスから削除し、この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。
 - 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、古いデータ管理インターフェイスのデフォルトのルートを新しいものに変更します。

- 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が、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、ゼロタッチプロビジョニング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お勧めします。CLIで行った変更は、いずれの場合においても GUI で複製される必要があります。

手順

- ステップ 1** [デバイス (Devices)]>[デバイス管理 (Device Management)] を選択し、デバイスの横にある [編集 (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) IPアドレスと名前を古いデータ管理インターフェイスから削除し、この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。
 - 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アドレスを変更してください。
 - 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)] > [スタティックルート (Static Route)] の順に選択し、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。

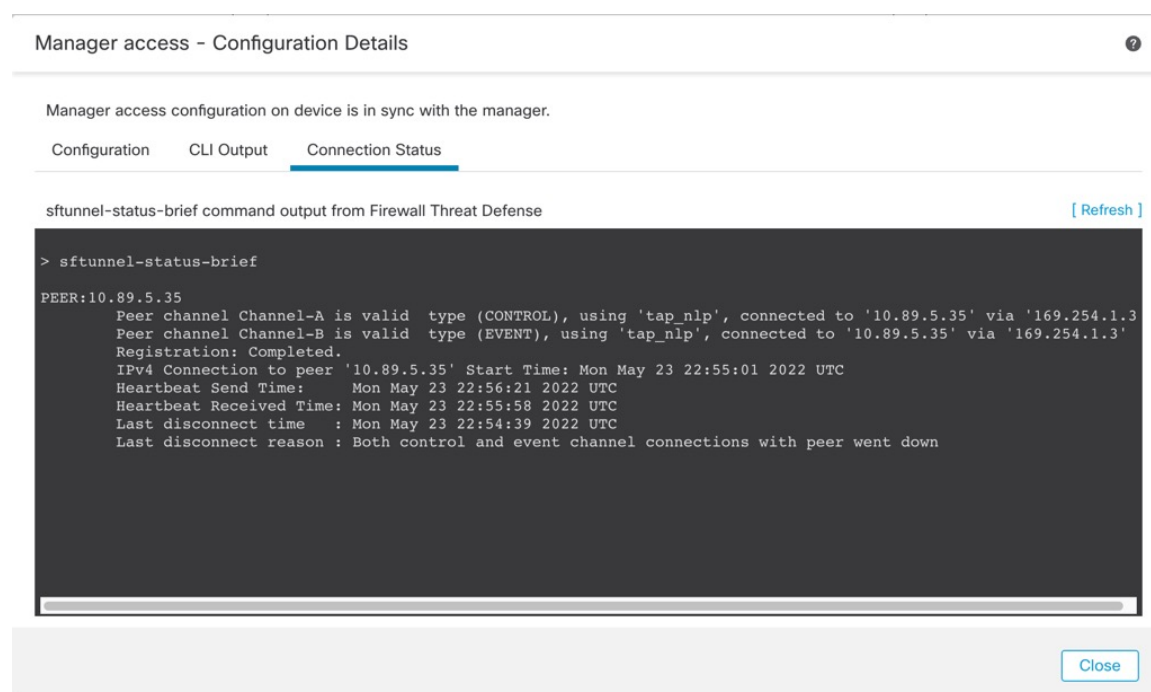
Firewall Management Center が現在の接続経由で構成の変更をデプロイします。デプロイメント後、データインターフェイスには、新しい IP アドレスが割り当てられるため、管理接続を再度確立する必要があります。

- 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 \(30 ページ\)](#)。
- 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)] > [管理 (Management)] エリアで、[マネージャアクセス詳細：構成 (Manager Access Details: Configuration)] をクリックし、[接続ステータス (Connection Status)] をクリックします。

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 19: 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（52 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、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（18 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。

手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (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 [編集 (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。


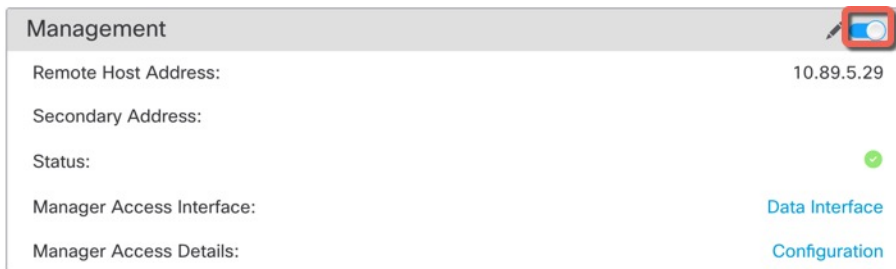
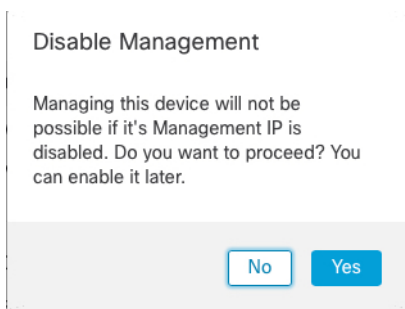
ステップ 4 スライダーをクリックして管理を一時的に無効にすることで、[無効なスライダー (Slider disabled)] () を無効化します。

図 20: 管理を無効にする



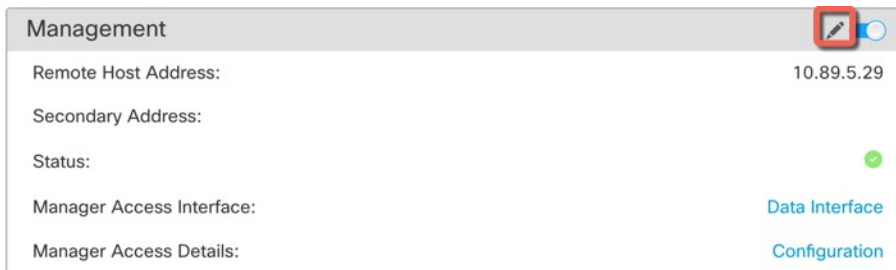
管理の無効化を続行するように求められます。[Yes] をクリックします。



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 からデバイスは削除されません。

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 [編集 (Edit)] () をクリックしてホスト名を編集します。

図 21: 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 \(12 ページ\)](#) を参照してください。

図 22: 管理 IP アドレス

Management

Remote Host Address: 10.89.5.29

Secondary Address: 10.99.11.6

Cancel Save



ステップ 7 スライダーをクリックして管理を再度有効[有効なスライダー (Slider enabled)] () にします。

図 23: 管理接続の有効化

Management

Remote Host Address: 10.89.5.4

Secondary Address:

Status: 

Manager Access Interface: Management Interface

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) [システム (System)] (⚙️) > [設定 (Configuration)] > [管理インターフェイス (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。

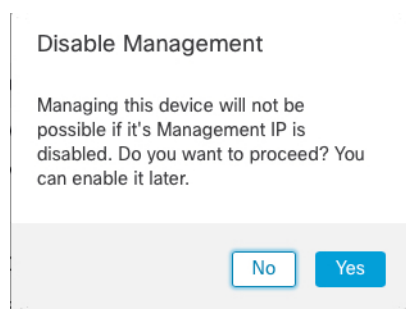
- a) [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

- b) デバイスの横にある [編集 (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 24: 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 [編集 (Edit)] (✎) をクリックしてホスト名を編集します。

図 25: 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 26: 管理 IP アドレス

The screenshot shows a 'Management' dialog box with a question mark icon in the top right corner. It contains two text input fields: 'Remote Host Address' with the value '10.89.5.29' and 'Secondary Address' with the value '10.99.11.6'. At the bottom right, there are two buttons: 'Cancel' and 'Save'.

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) [システム (System)] (⚙️) > [設定 (Configuration)] > [管理インターフェイス (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：

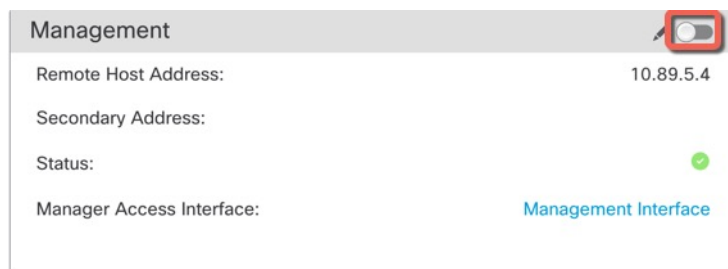
configure network management-data-interface disable

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 27: 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。

- [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。
- [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。
- [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。

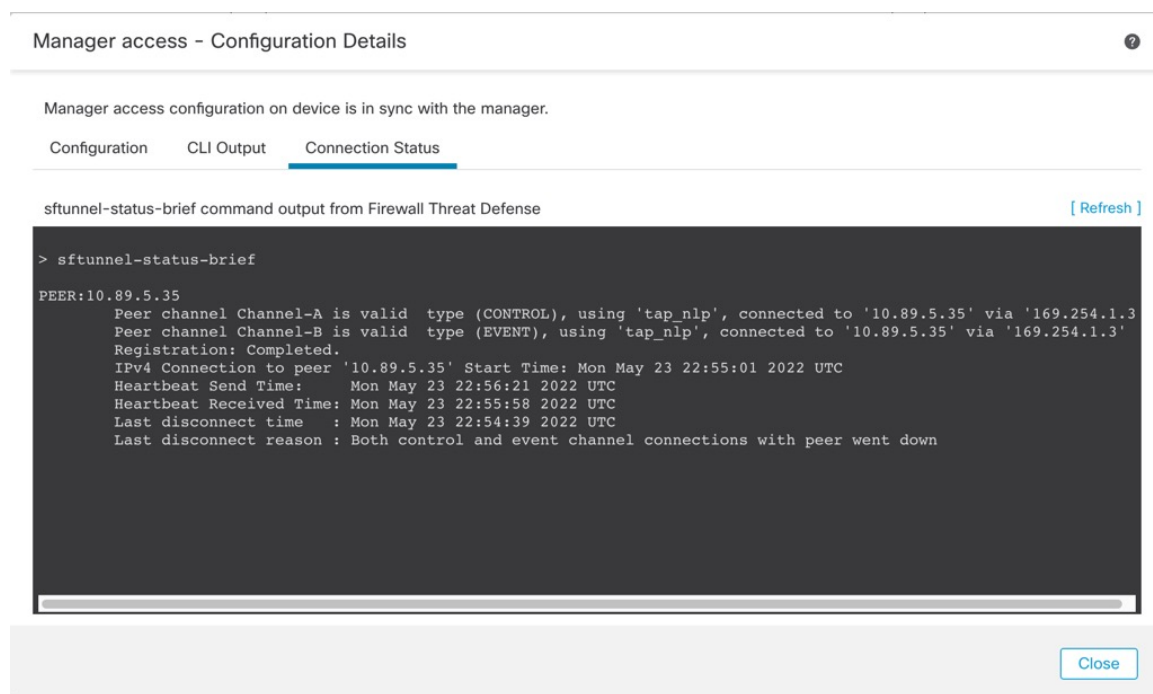
ステップ 8 管理接続が再確立されたことを確認します。

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 28: 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。

- セカンダリ Firewall Management Center IP アドレスを変更します。
- 両方のユニットで新しいピアアドレスを指定します。
- セカンダリユニットをアクティブユニットにします。
- デバイスの管理接続を無効にします。
- Firewall Management Center でデバイスの IP アドレスを変更します。
- 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 \(42 ページ\)](#) 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。

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) **[デバイス (Devices)] > [デバイス管理 (Device Management)]** ページで、デバイスの **[編集 (Edit)]** () をクリックします。**[デバイス (Device)]** をクリックし、**[管理 (Management)]** エリアで、**[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 29: マネージャ アクセス インターフェイス

Manager Access Interface

This is an advanced setting and need to be configured only if needed.
See the [online help](#) for detailed steps.

Manage device by

Data Interface

Switching the manager access interface from Management to Data interface causes the deployment to be blocked. To unblock the deploy, pick a data interface and enable it for manager Access. See the [online help](#) for detailed steps.

Close Save

- 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 30: マネージャアクセス

Management

Remote Host Address: 10.10.1.12


Secondary Address:

Status: ✔

Manager Access Interface: Data Interface

Manager Access Details: Configuration

[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**[編集 (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 \(12 ページ\)](#)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、**[デバイス (Devices)]** > **[デバイス管理 (Device Management)]** > **[DHCP]** > **[DDNS]** ページで Web タイプ DDNS 方式を有効にします。
- [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を介して Firewall Management Center にルーティングできることを確認します。必要に応じて、**[デバイス (Devices)]** > **[デバイス管理 (Device Management)]** > **[ルーティング (Routing)]** > **[スタティックルート (Static Route)]** でスタティックルートを追加します。 > > >
- [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、**[デバイス (Devices)]** > **[プラットフォーム設定 (Platform Settings)]** > **[DNS]** でこのデバイスに適用します。
- [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、**[デバイス (Devices)]** > **[プラットフォーム設定 (Platform Settings)]** > **[セキュアシェル (Secure Shell)]** でこのデバイスに適用します。
- [Shell 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。

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。

- ステップ 10** Firewall Management Center で、管理接続を無効にし、[デバイス (Devices)] > [管理 (Management)] エリアの [デバイス (Devices)] > [デバイス管理 (Device Management)] ページで、Firewall Threat Defense の [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 \(30 ページ\)](#) 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。

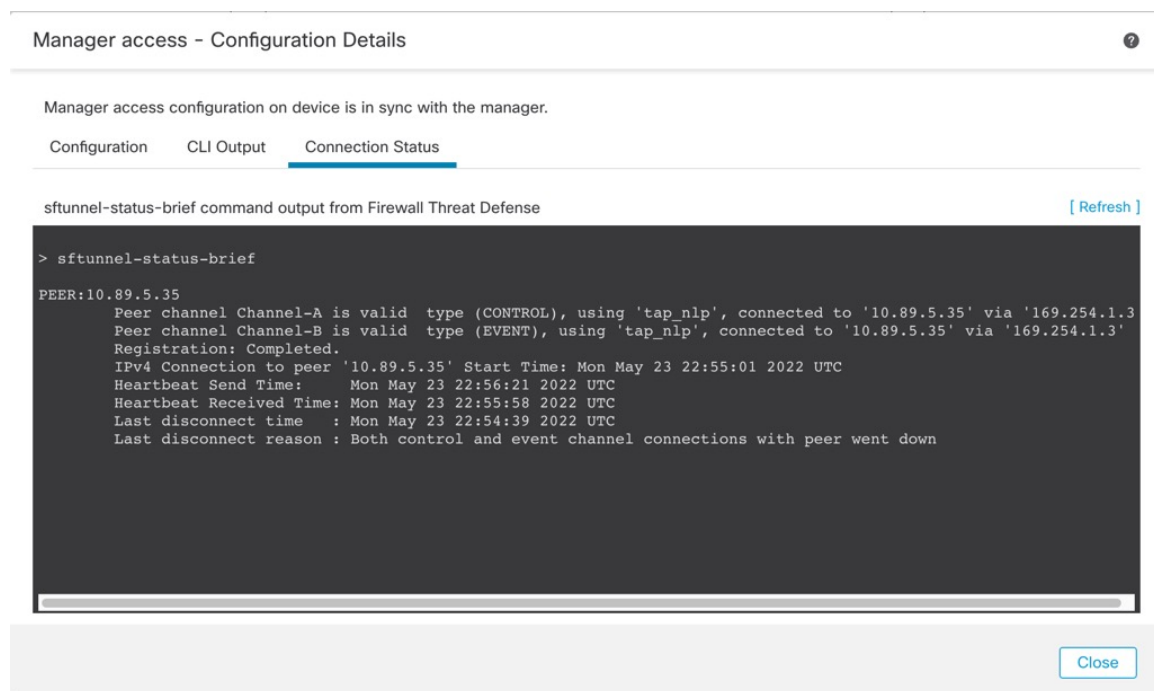
- ステップ 11** 管理接続が再確立されたことを確認します。

[デバイス (Device)] > [管理 (Management)] エリアで、[マネージャアクセス詳細 : 構成 (Manager Access Details: Configuration)] をクリックし、[接続ステータス (Connection Status)] をクリックします。

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 31: 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 \(52 ページ\)](#)」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 \(38 ページ\)](#) 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。

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) [デバイス (Devices)] > [デバイス管理 (Device Management)] ページで、デバイスの [編集 (Edit)] (✎) をクリックします。[デバイス (Device)] をクリックし、[管理 (Management)] エリアで、[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 [管理インターフェイス (Management Interface)] を選択します。

図 32: マネージャ アクセス インターフェイス

Manager Access Interface

This is an advanced setting and need to be configured only if needed.
See the [online help](#) for detailed steps.

Manage device by

Management Interface ▼

Switching the manager access interface from Data to Management causes the deployment to be blocked. To unblock the deployment, ensure none of the data interfaces are set for manager access. See the [online help](#) for detailed steps.

Close Save

- 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 33: 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 [編集 (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、[デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] > [DNS] でこのデバイスに適用します。

[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。

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。

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 (Devices)] > [デバイス管理 (Device Management)] > [デバイス (Device)] > [管理 (Management)] セクションで Firewall Threat Defense の [リモートホストアドレス (Remote Host Address)] IP アドレスとオプションの [セカンダリアドレス (Secondary Address)] を更新して、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 (30 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、[デバイス (Devices)] [デバイス管理 (Device Management)] [デバイス (Device)] [管理 (Management)] [ステータス (Status)] フィールドで管理接続ステータスを確認するか、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 (52 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。
- [インターフェイス (Interfaces)] ページの [同期 (Sync)] ボタン。
- [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。

Manager access - Configuration Details

Manager access configuration on device have been updated outside of Manager. Review the differences and update Manager values accordingly.

Configuration

CLI Output

Connection Status

Last updated: 2022-09-02 at 20:35:58 UTC [Refresh]

	Configuration on Manager	Configuration on Device
4. Ethernet1/1		
Interface Configuration		
FMC Access Enabled	Disabled	Enabled
FMC Access - Allowed Networks		any
Interface Name		outside
IPv4/IPv6 Address		10.89.5.29/26
Static Route Configuration		
IPv4 Gateway		10.89.5.1
IPv6 Gateway		
5. Ethernet1/8		
Legend: Above configurations will be added , modified or disassociated from manager access interface on next deploy to device.		

Close

Acknowledge

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。

Manager access - Configuration Details

Manager access configuration on device is different from Manager. Review the differences and deploy the changes.

[Configuration](#)[CLI Output](#)[Connection Status](#)

Last updated: 2022-09-09 at 07:10:54 UTC [\[Refresh \]](#)

	Configuration on Manager	Configuration on Device
Web Update Type		
4. GigabitEthernet0/0		
Interface Configuration		
FMC Access Enabled	Enabled	Enabled
FMC Access - Allowed Networks	any	any
Interface Name	outside	outside
IPv4/IPv6 Address	10.89.5.29 255.255.255.192	10.89.5.29 255.255.255.192
Static Route Configuration		
IPv4 Gateway		10.89.5.1
IPv6 Gateway		

Legend: Above configurations will be added, modified or disassociated from manager access interface on next deploy to device.

[Close](#)

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 34: CLI 出力

Manager access - Configuration Details

Manager access configuration on device is different from Manager. Review the differences and deploy the changes.

Configuration CLI Output Connection Status

Show command output of Manager Access associated configuration from Firewall Threat Defense

```
> show running-config dns
DNS server-group DefaultDNS

> show sftunnel interfaces
Physical Interface      Name of the Interface

> show running-config interface

> show version
-----[ 1010-2 ]-----
Model       : Cisco Firepower 1010 Threat Defense (78) Version 7.2.0 (Build 2028)
UUID        : eb1f518-d0a0-11ec-bb8f-90ce044ba76f
LSP version : lsp-rel-20220519-1116
VDB version : 354
-----
Cisco Adaptive Security Appliance Software Version 9.18(0)104
```

Close

FMC Access - Configuration Details

FMC Access configuration on device have been updated outside of FMC. Review the differences and update FMC values accordingly.

Configuration CLI Output Connection Status

Show command output of FMC Access associated configuration from FTD

```
> show running-config dns
dns domain-lookup outside
DNS server-group DefaultDNS
DNS server-group RBD_DNS
  name-server 72.163.47.11
  name-server 173.37.137.85
  name-server 173.37.142.73
dns-group RBD_DNS

> show sftunnel interfaces
Physical Interface      Name of the Interface
GigabitEthernet1/1      outside

> show running-config route
route outside 0.0.0.0 0.0.0.0 10.89.5.1 1

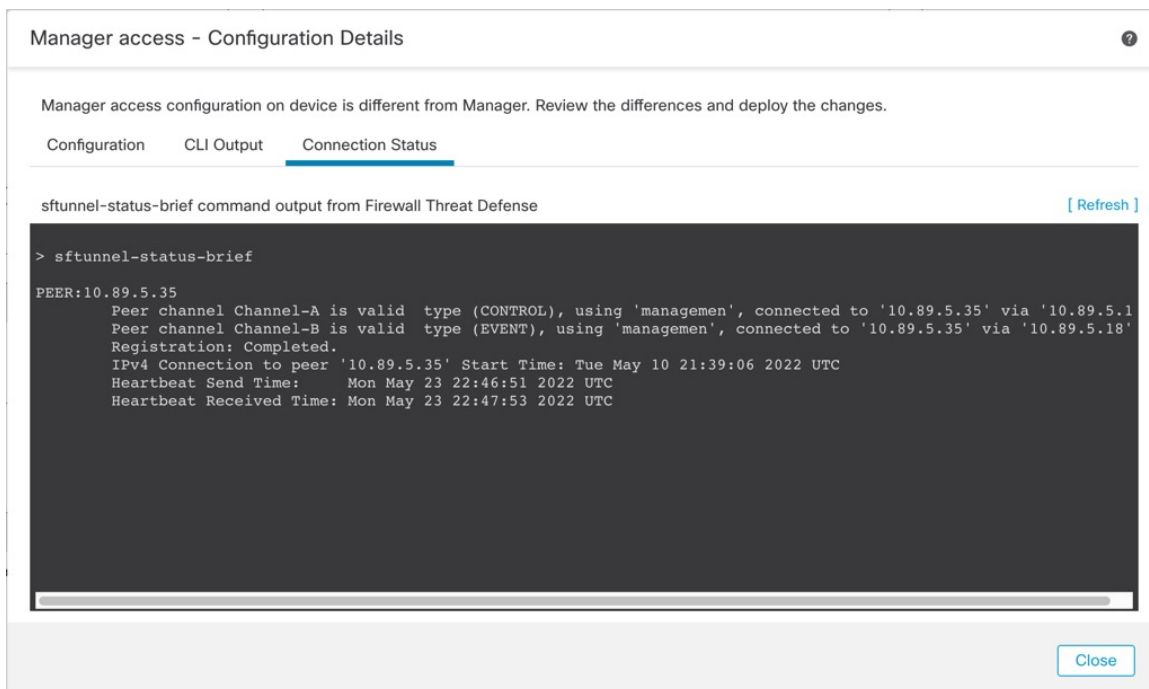
> show running-config interface
!
interface GigabitEthernet1/1
 nameif outside
 cts manual
 propagate sgt preserve-untag
 policy static sgt disabled trusted
 security-level 0
```

Acknowledge Close

接続ステータス

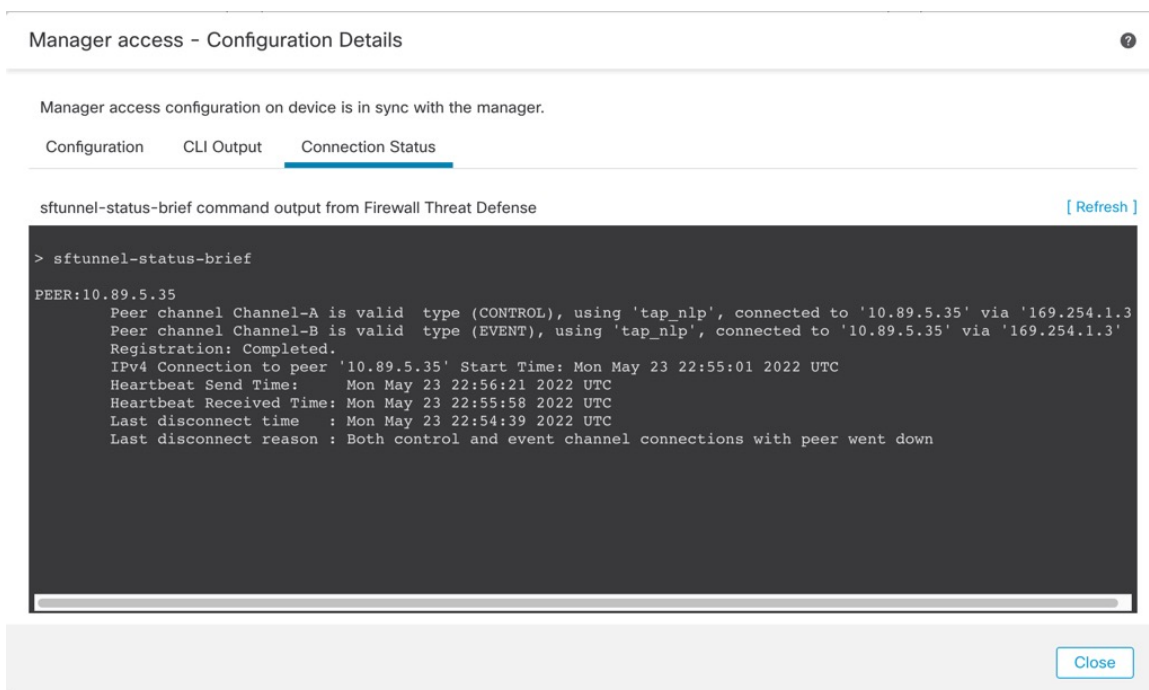
管理接続ステータスの表示次の例は、管理接続で引き続き管理「management0」インターフェイスが使用されていることを示しています。

図 35: 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 36: 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（64 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 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。

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 \(52 ページ\)](#)」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 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。**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 : 10.10.1.4
Display name : 10.10.1.4
Identifier : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration : Completed
Management type : Configuration
```

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] > [Device] > [Management] > [Manager Access - Configuration Details] > [CLI Output]** ページでも確認できます。

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 37: インベントリの詳細 (Inventory Details)

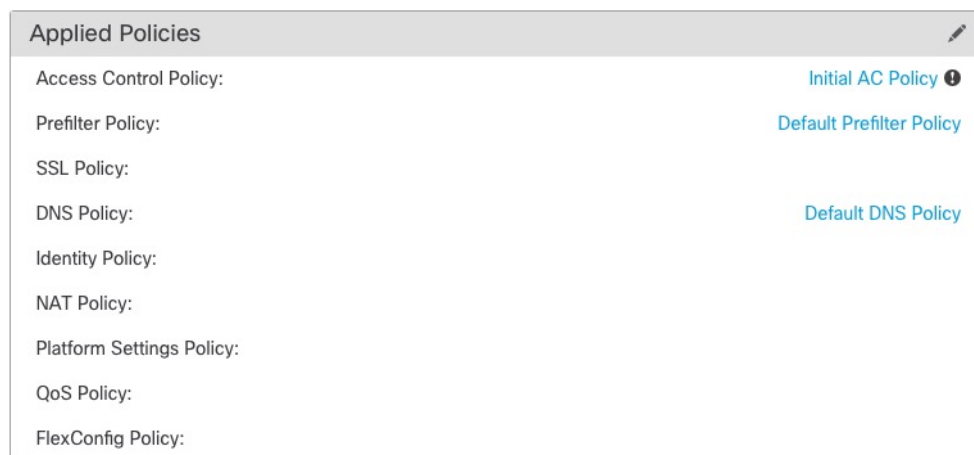
Inventory Details 	
CPU Type:	CPU Xeon E5 series 2300 MHz
CPU Cores:	1 CPU (4 cores)
Memory:	8192 MB RAM
Storage:	N/A
Chassis URL:	N/A
Chassis Serial Number:	N/A
Chassis Module Number:	N/A
Chassis Module Serial Number:	N/A

情報を更新するには、[更新 (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 38: [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、[感嘆符 (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 39: [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 [デバイス (Devices)] > [デバイス管理 (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 [編集 (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、[編集 (Edit)] (✎) をクリックします。

図 40: ポリシー割り当て

Policy Assignments

Access Control Policy: Initial AC Policy

NAT Policy: None

Platform Settings Policy: None

QoS Policy: None

FlexConfig Policy: None

Cancel Save

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。

フィールド	説明
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)。
オブジェクトグループの検索	<p>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。</p> <p>(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。</p>
インターフェイスオブジェクトの最適化	<p>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す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。</p>

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、ターゲット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** [デバイス（Devices）] > [デバイス管理（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 [編集（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 [編集（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 使用率が增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、後からこの機能が無効にすると、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

- モデルのサポート：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[編集 (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[編集 (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す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

モデルのサポート : 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[編集 (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[編集 (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 41: 展開設定

Deployment Settings 	
Auto Rollback Deployment if Connectivity fails	Disabled
Connectivity Monitor Interval (in Minutes) ⓘ	20 Mins.

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 \(50 ページ\)](#) 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 [デバイス (Devices)] > [デバイス管理 (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 [編集 (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、[編集 (Edit)] (✎) をクリックします。

図 42: 展開設定

Deployment Settings

Auto Rollback Deployment if Connectivity Fails: ☐

Connectivity Monitor Interval (in Minutes): 20

The connectivity failure timeout will be applicable from next deployment incase, the deployment for this device is already in progress.

Cancel Save

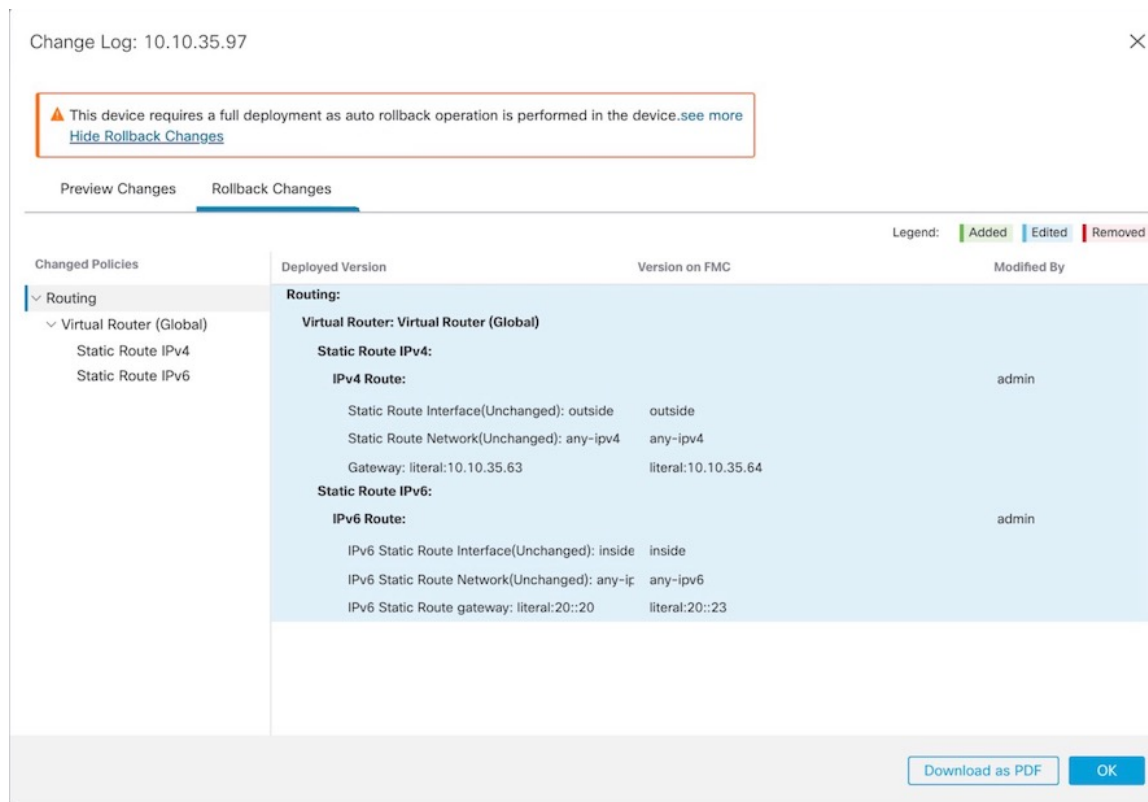
ステップ5 自動ロールバックを有効にするには、[接続が失敗した場合の自動ロールバック展開 (Auto Rollback Deployment if Connectivity Fails)] をオンにします。

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)] 画面に移動し、[プレビュー (Preview)] (🔍) アイコンをクリックして、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 43: 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 で、[デバイス (Devices)] > [デバイス管理 (Device Management)] > [デバイス (Device)] > [管理 (Management)] > [FMCアクセスの詳細 (FMC Access Details)] > [接続ステータス (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。

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 \(52 ページ\)](#)」を参照してください。

クラスタのヘルスマニター設定の編集

[クラスタ (Cluster)] ページの [クラスタヘルスマニターの設定 (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 44: クラスタのヘルスマニターの設定

Cluster Health Monitor Settings			
Timeouts			
Hold Time	3 s		
Interface Debounce Time	9000 ms		
Monitored Interfaces			
Service Application	Enabled		
Unmonitored Interfaces	None		
Auto-Rejoin Settings			
	Attempts	Interval Between Attempts	Interval Variation
Cluster Interface	-1	5	1
Data Interface	3	5	2
System	3	5	2

表 7: [クラスタヘルスマニターの設定 (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思われ、クラスタからノードが削除されるまでの時間です。
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。

フィールド	説明
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。
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 [デバイス (Devices)] > [デバイス管理 (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 [編集 (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 [クラスタのヘルスマニターの設定 (Cluster Health Monitor Settings)] セクションで、[編集 (Edit)] (✎) をクリックします。
- ステップ 5 [ヘルスチェック (Health Check)] スライダーをクリックして、システムのヘルスチェックを無効にします。

図 45: 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

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 46: 自動再結合の設定

▼ Auto-Rejoin Settings

Cluster Interface

Attempts Range: 0-65535 (-1 for unlimited number of attempts)

Interval Between Attempts Range: 2-60 minutes between rejoin attempts

Interval Variation Range: 1-3. Defines if the interval duration increases. 1 (no change); 2 (2 x the previous duration), or 3 (3 x the previous duration).

Data Interface

Attempts Range: 0-65535 (-1 for unlimited number of attempts)

Interval Between Attempts Range: 2-60 minutes between rejoin attempts

Interval Variation Range: 1-3. Defines if the interval duration increases. 1 (no change); 2 (2 x the previous duration), or 3 (3 x the previous duration).

System

Attempts Range: 0-65535 (-1 for unlimited number of attempts)

Interval Between Attempts Range: 2-60 minutes between rejoin attempts

Interval Variation Range: 1-3. Defines if the interval duration increases. 1 (no change); 2 (2 x the previous duration), or 3 (3 x the previous duration).

[クラスインターフェイス (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 47: モニタリング対象インターフェイスの設定

▼ Monitored Interfaces

Monitored Interfaces	Unmonitored Interfaces
GigabitEthernet0/0	
GigabitEthernet0/1	
GigabitEthernet0/2	
GigabitEthernet0/3	
GigabitEthernet0/4	
GigabitEthernet0/5	
GigabitEthernet0/6	
GigabitEthernet0/7	
Diagnostic0/0	

Add

☒ Enable Service Application Monitoring

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。

たとえば、管理インターフェイスなど、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	最小 Firewall Management Center	最小 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	<p>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。</p> <p>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)]</p> <p>(注)</p> <p>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。</p>

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
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	<p>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。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> • [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	<p>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。</p>
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	<p>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。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> • [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	<p>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。</p>

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
デバイス設定のインポート/エクスポート。	7.1.0	7.1.0	<p>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。</p> <ul style="list-style-type: none"> • 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。 <p>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)]</p>
FTD での FMC IP アドレスの更新。	6.7.0	6.7.0	<p>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。</p> <p>新規/変更されたコマンド：configure manager edit</p>

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。