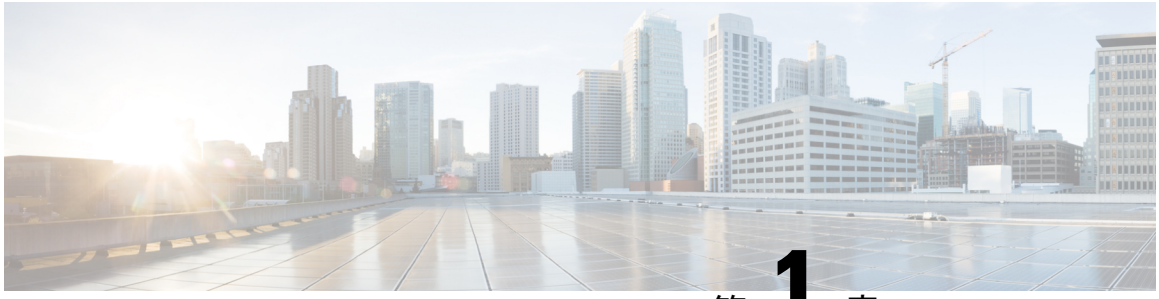
APIC 連携、1.0.3 の Cisco Firepower Threat Defense クイック スタート ガイド

初版：2018 年 4 月 17 日

最終更新：2018 年 5 月 22 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/



第 1 章

はじめに

概要

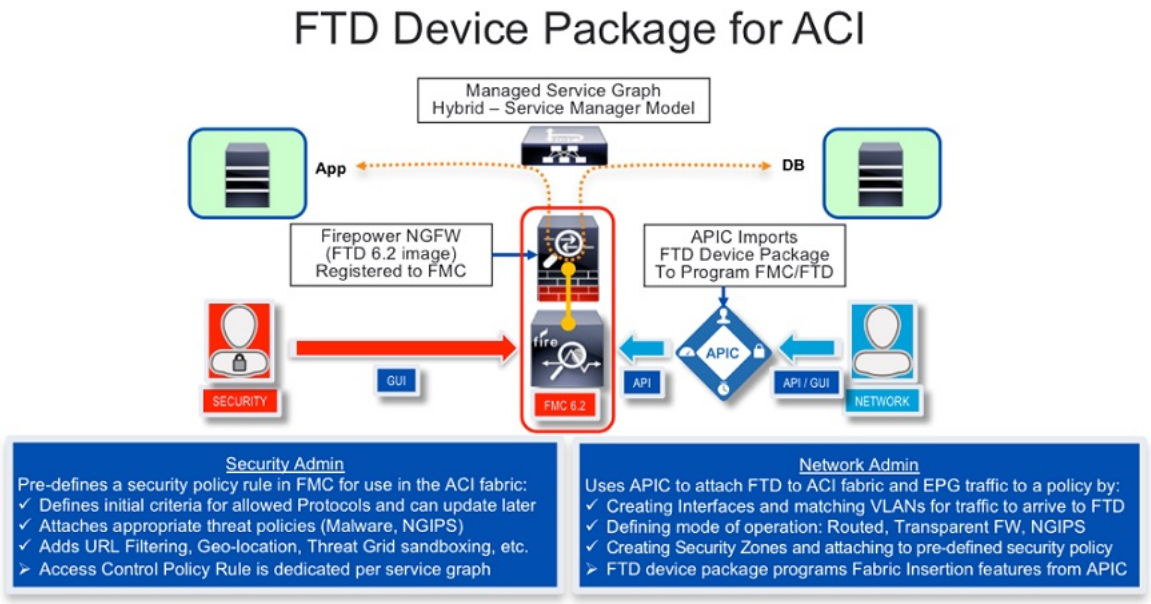
Cisco Application Policy Infrastructure Controller（APIC）は、Cisco Application Centric Infrastructure（ACI）のセントラル 機能を制御するシングルポイントです。APIC では、アプリケーション間の Cisco Firepower Threat Defense（FTD）ノースバウンドなどのサービス挿入を自動化でき、エンドポイント グループ（EPG） とも呼ばれます。APIC は、ネットワークとサービスを設定するためにノースバウンド Application Programming Interfaces（API）を使用します。管理対象オブジェクトを使用して設定を作成、削除、変更するのに、これらの API を使用します。

サービス デバイスを設定しモニタするため、APIC にはデバイス パッケージが必要です。デバイス パッケージはサービス デバイスのクラスを管理し、デバイスに関する情報を APIC に送信するため、APIC はデバイスの動作を認識できます。デバイス パッケージを使用することで、FTD アプライアンスなど、サービス デバイスにネットワーク サービス機能を挿入し設定できます。

FTD ファブリック挿入（FI）デバイス パッケージは、全デバイス設定の責任がセキュリティとネットワーク管理者の間で共有されているハイブリッドモデル（ACI 用語でサービス マネージャ）に基づいています。

- セキュリティ管理者：セキュリティ ゾーンの条件が未設定のまま、新しいサービス グラフにセキュリティ ポリシーを事前定義するため FMC を使用します。新しいポリシー ルールは適切なアクセス（プロトコルを許可）と、NGIPS およびマルウェアのポリシー、URL フィルタリング、Threat Grid など高度な保護設定を定義します。
- ネットワーク管理者。サービス グラフをオーケストレーションし、ACI ファブリックに FTD デバイスを挿入して、この事前定義されたセキュリティ ポリシーにダイレクト トラフィックを接続するため、APIC を使用します。APIC の L4 ～ L7 デバイス パラメータまたは機能のプロファイル内で、ネットワーク管理者は、事前定義された FMC アクセス コントロール ポリシーやルールの一致を含む、このガイドで定義されたパラメータを設定します。

APIC が FMC のアクセス コントロール ポリシー ルール名と一致する場合、ルールに新しく作成されたセキュリティ ゾーンを挿入するだけです。ルールが見つからない場合、APIC はその名前で新しいルールを作成し、セキュリティ ゾーンを接続して、[拒否アクション] を設定します。これは、トラフィックが特定のサービス グラフに許可される前に、セキュリティ管理者が新しいルール基準と適切な保護設定を更新するように強制します。



このドキュメントでは、FTD と ACI の連携方法と、FTD の機能を利用するための APIC の設定法について説明します。

- Firepower Management Center（FMC）で、REST API を有効化にします
- CCO から ACI デバイス パッケージ ソフトウェアの FTD をダウンロードします
- APIC に ACI デバイス パッケージの FTD をインポートします
- FTD アプライアンスを登録します
- FTD アプライアンスを使用するネットワーク サービス グラフを定義します

（注） このドキュメントで使用される例のスクリーン ショットでは、**SampleTenant** という名前の既存のテナントが示されています。このガイドの手順に従って提供されたテンプレートを使用する場合、実際のテナント名を使用します。

サービス機能の挿入

サービス機能がアプリケーション間のサービス グラフに挿入されると、これらのアプリケーションからのトラフィックは APIC で分類され、オーバーレイ ネットワークのタグを使用して

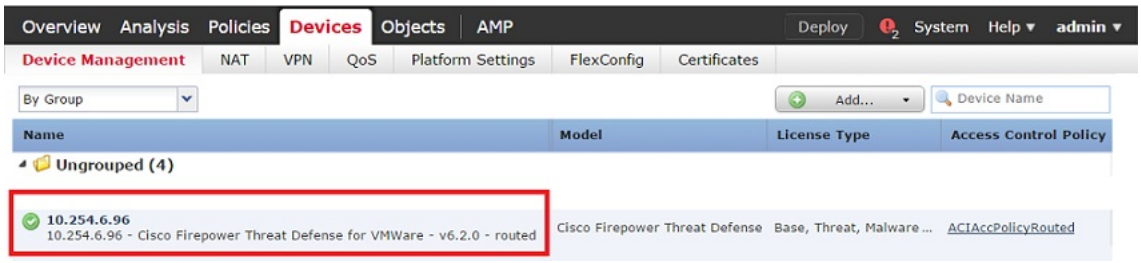
識別されます。サービス機能はタグを使用して、トラフィックにポリシーを適用します。APICとのFTD統合の場合、サービス機能はルーテッド、トランスペアレント、またはインラインファイアウォール動作を使用してトラフィックを転送します。

使用可能なAPIC製品

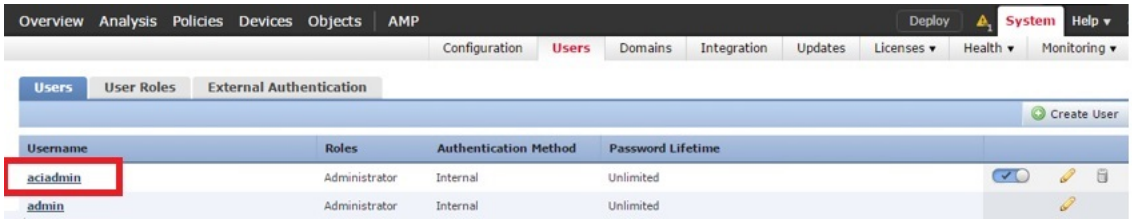
初期のソフトウェア リリースには、ACI用のCisco FTDデバイス パッケージ ファブリック挿入ソフトウェアが含まれています。

前提条件

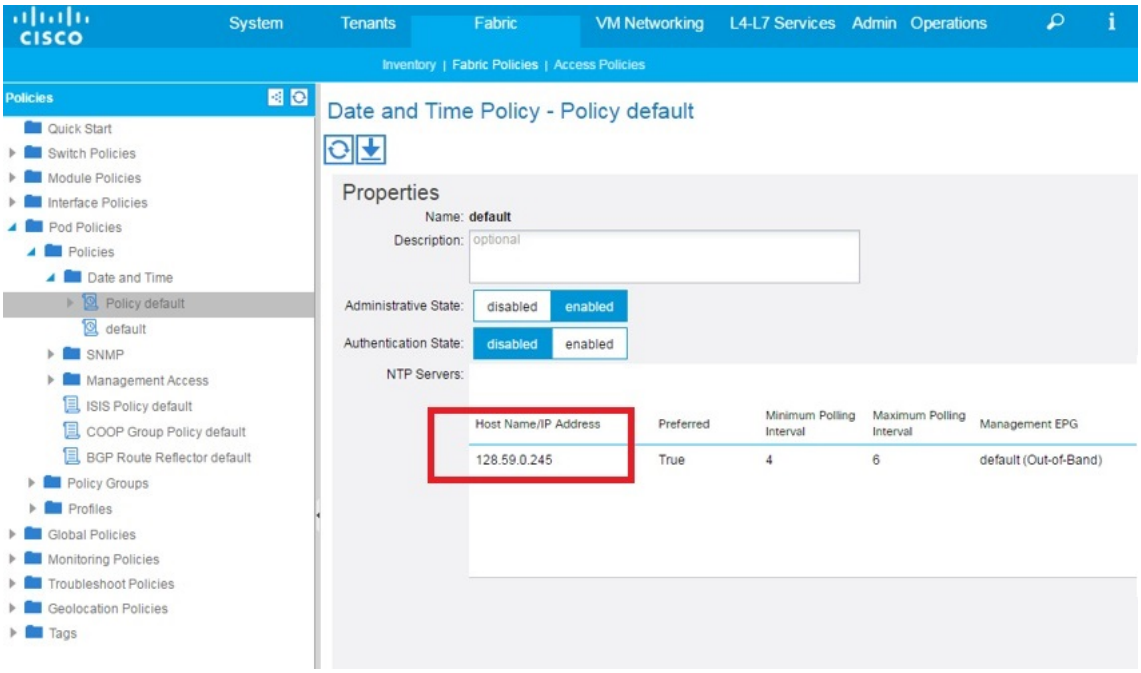
- FMCバージョン6.2.3：FTDのREST APIのサポートが含まれています。
- FTDバージョン6.2.3.
- APICバージョン2.3(1f)：そのデバイス マネージャがデバイスを登録するために使用します。FTDデバイス パッケージは、デバイス マネージャがFMC設定のネットワーク部分をAPICによりインスタンス化することを許可するために使用されます。
- FTDアプライアンスを挿入し、ネットワーク サービスが基本設定のブートストラップとして設定されており、FMCに登録されていることを確認します。たとえば、FTDのFMCのデバイス管理ページを参照してください。



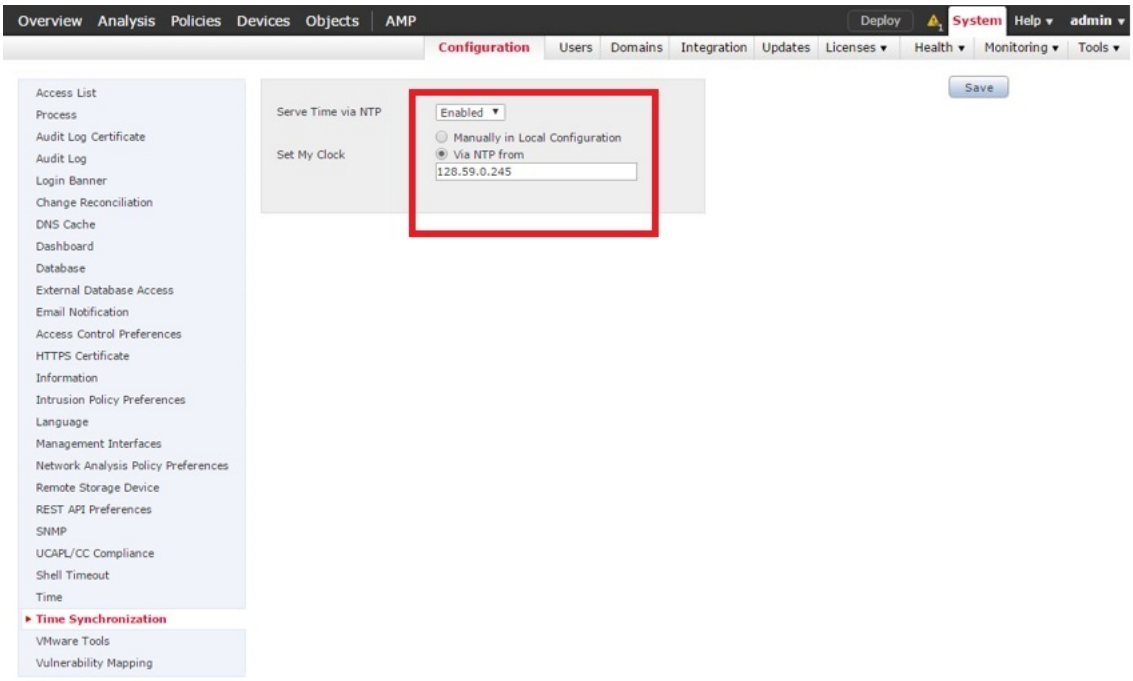
- REST APIトークン生成の競合状態を避けるためには、ACI上での使用専用のFMC管理者を作成します。次に例を示します。



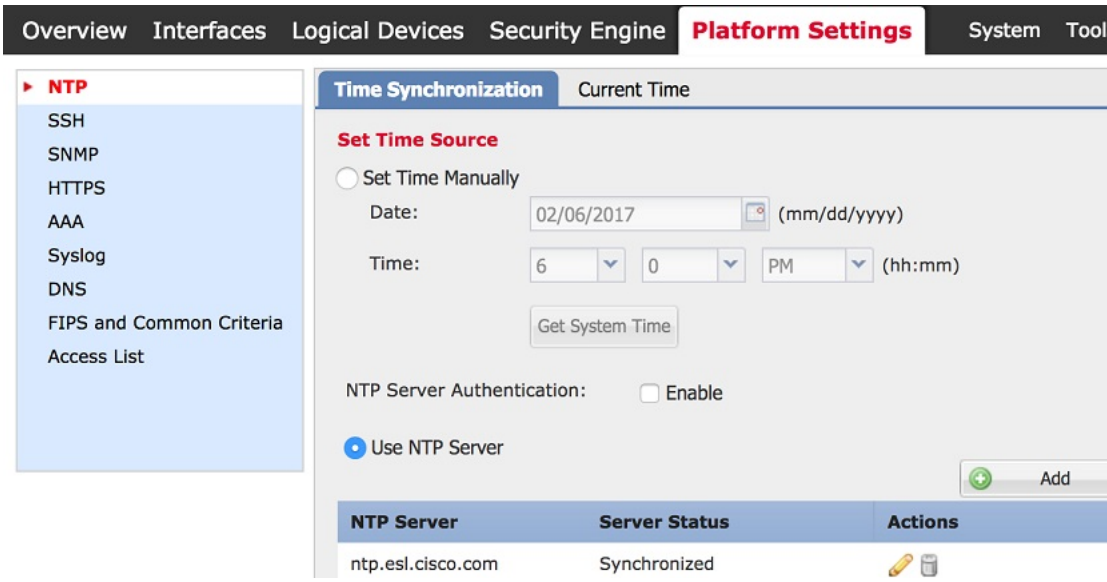
- 展開上の障害とサーバ間で時間差の両方を回避するには、同じNetwork Time Protocol（NTP）サーバを使用するようにAPICとFMCを設定します。Firepower 41xxおよび93xxシリーズのアプライアンス上のFTDでは、シャーシ マネージャも設定するが必要があります。
  - APIC内で、**[ファブリック]>[ファブリック ポリシー]>[ポッド ポリシー]>[ポリシー]>[日付と時刻]**に移動します。同じNTPサーバを設定するには、作成日と時刻ポリシーのウィザードを使用します。



- FMC で、**[システム] > [設定] > [時間同期]** に移動し、同じ NTPサーバを設定します。



- Firepower 41xx および 93xx シリーズ アプライアンスのシャーシ マネージャで、**[プラットフォーム設定] > [NTP] > [時間同期]** に移動し、同じ NTP サーバを追加します。

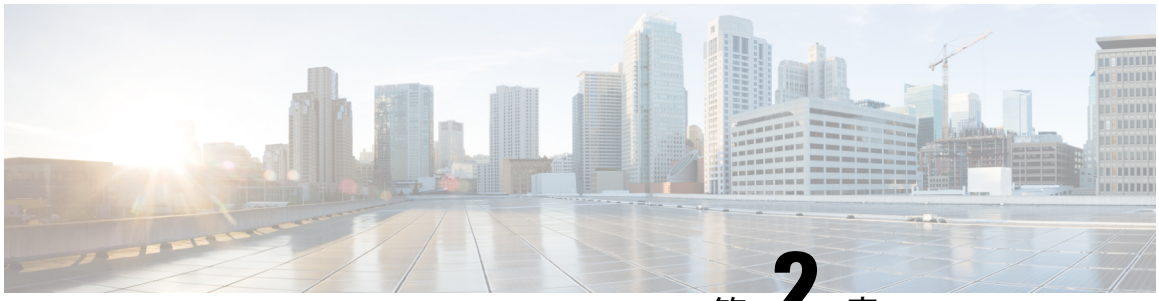


（注） 現在の FMC または FTD バージョンでサポートされていない設定を作成する場合、APIC 上に次と同様のエラーが表示される場合があります。「メジャー スクリプト エラー：設定エラー：ERROR: % Invalid input detected at '^' marker."

関連資料

- 『Cisco Application Centric Infrastructure Fundamentals』
- 『Cisco APIC レイヤ 4 ～ レイヤ 7 サービス導入ガイド』
- Cisco Firepower Threat Defense NGFW
- Cisco Firepower Management Center

関連資料



第 2 章

インストールするもの

FMC REST API が有効になっていることの確認

APIC は REST API を使用して Firepower デバイスに接続します。デフォルトで、REST API は有効になっています。APIC がセットアップされ Firepower デバイスを管理する前に、次の手順を完了して FMC REST API が有効になっていることを確認します。

始める前に

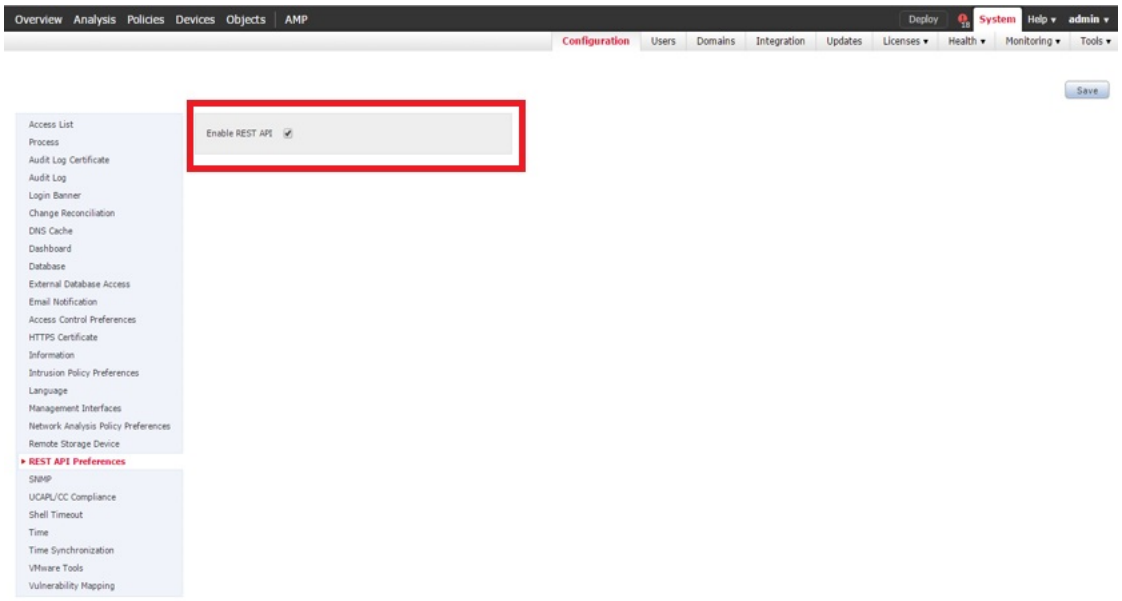
FMC ではバージョン 6.2.0 以降を実行している必要があります。

（注） REST API は、FMC ソフトウェア;ですでにパッケージ化されており、ライセンスは必要ありません。

ステップ 1 管理者のクレデンシャルを使用して FMC にサインインします。

ステップ 2 **[システム] > [設定] > [REST API 設定]** に移動します。

ステップ 3 **[REST API の有効化]** チェック ボックスがまだ選択されていない場合、ボックスをオンにして **[保存]** をクリックします。



次のタスク

REST API が有効になると、FMC は ACI デバイス パッケージの FTD をサポートする準備ができています。

APIC で使用する管理者以外のアカウントを作成します。

デバイス パッケージのインポート

APIC は、サービス デバイスを設定およびモニタするためデバイス パッケージが必要です。APIC が FTD アプライアンスの存在と FTD アプライアンスの機能を認識できるように、ACI デバイス パッケージの FTD を APIC にインポートします。

ステップ 1 http://www.cisco.com/go/software からデバイス パッケージをダウンロードし、ローカル ドライブ上に保存します。

（注） デバイス パッケージは .zip ファイルとしてダウンロードされます。このファイルは解凍しないでください。

ステップ 2 プロバイダ管理者として APIC にサインインします。

ステップ 3 メニュー バーで、**[L4-L7 サービス]** をクリックします。

ステップ 4 サブメニュー バーで、**[パッケージ]** をクリックします。

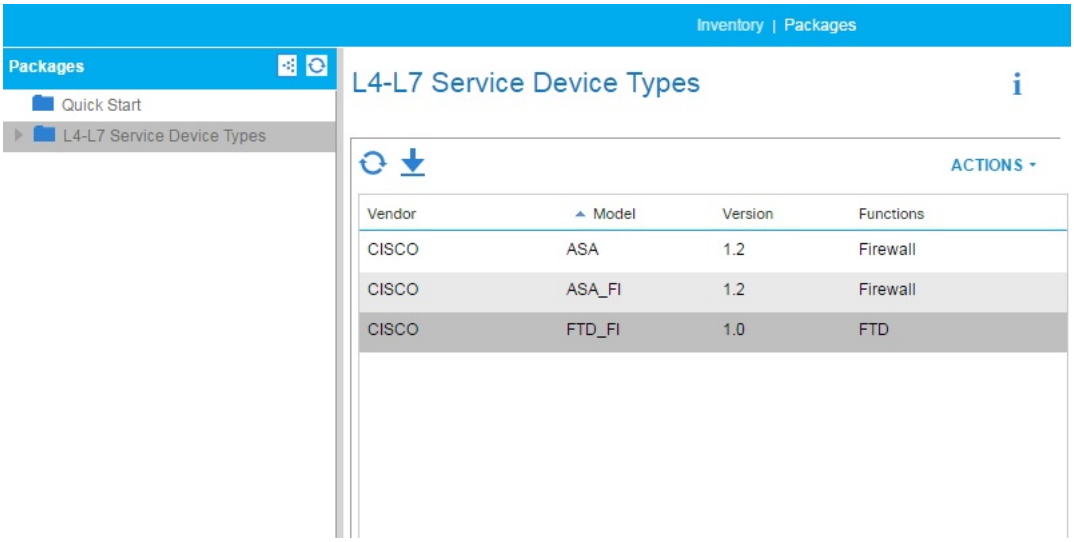
ステップ 5 [ナビゲーション] ペインで、**[L4-L7 サービス デバイス タイプ]** をクリックします。

ステップ 6 **[アクション] > [デバイス パッケージのインポート]** を選択します。

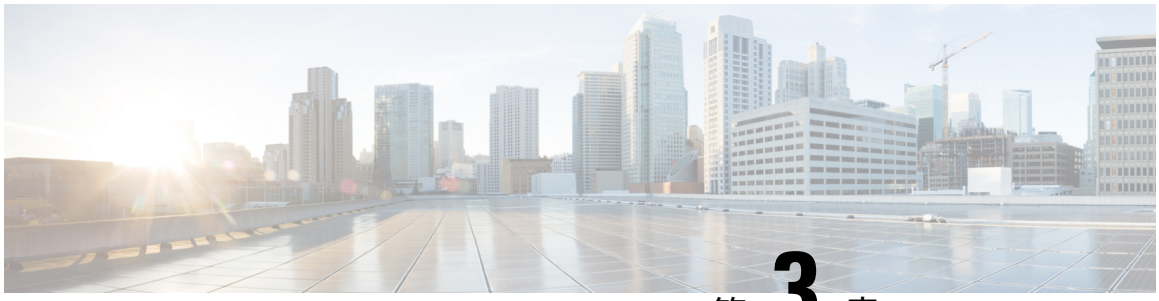
ステップ 7 **[ファイル名]** フィールドで、**手順 1** でダウンロードしたデバイス パッケージを指定し、**[送信]** をクリックします。

次のタスク

[デバイス タイプ] ウィンドウを更新します。新しいデバイスがデバイス タイプのリスト内に表示されます。



（オプション）[ナビゲーション] ウィンドウで、**[デバイス タイプ]** を展開し、デバイス パッケージの機能のパラメータを表示します。



第 3 章

設定

バックグラウンド

アプリケーションの一環として L4 L7 サービスの統合のため、ACI ファブリックを提供します。これは、APIC マネージド サービス グラフ、L4 L7 デバイス パッケージを必要とを使用して行います。インポートされたデバイス パッケージは、apic 内での設定パラメータを公開し、デバイス上に特定の設定を調整することができます。

L4 L7 サービス グラフをインストールするには、APIC に L4 L7 デバイスを登録機能プロファイルまたは L4 L7 サービス パラメータの一部として設定を追加し、サービス グラフに、これらの 2 つのリンクします。契約をこの L4 L7 サービス グラフを適用すると、APIC で表示ファブリックでは、デバイスインターフェイスをタギングおよびそれらを適切なコンシューマとプロバイダー Epg にステッチします。APIC では、自動方式で登録済みデバイスを特定の設定が適用されます。ACI ファブリックおよび L4 L7 デバイスに適用する設定をすべて、ACI ファブリックはインスペクションの特定のデバイスに契約で定義されたトラフィックを送信します。ACI では、1 つのサービス グラフの下に複数のサービスをチェーンすることもできます。

FTD アプライアンスの登録

APIC で FTD デバイスを登録する前に、APIC デバイス マネージャとしてその FMC 管理ステーションを追加します。このハイブリッド サービス グラフのモデルでは、APIC および FMC は FTD 設定の完全な責任を共有します。FMC が EPG 間の通信を制御する脅威ポリシーとルールを定義する一方で、APIC インターフェイス、IP アドレス、セキュリティ ゾーン、BVI、NGIPS インライン ペアの設定をプロビジョニングします。デバイス マネージャとして FMC を追加して、サービス グラフで利用するために APIC で FTD アプライアンスを登録します。

（注） 1 個の FMC は、複数のサービス グラフにプロビジョニングされた複数の FTD デバイスに、デバイス マネージャとして使用できます。

始める前に

- HTTP の通信を許可する APIC 通信ポリシーを設定します。
- 仮想マシン マネージャまたは物理ドメインのいずれかを設定します。
- テナントを設定します。このセクションの手順では、既存のテナントが必要です。

ステップ 1 APIC にサインインします。

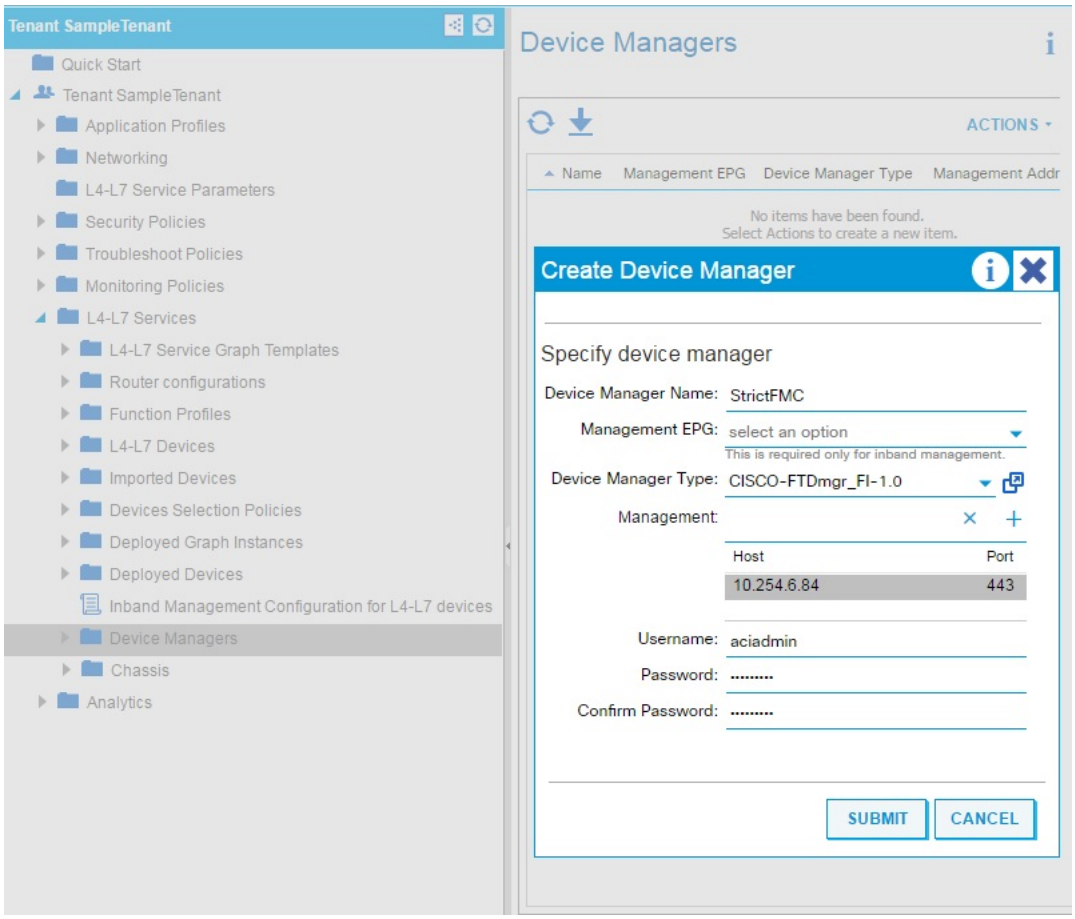
ステップ 2 メニュー バーで、**[テナント]** をクリックします。

ステップ 3 [ナビゲーション] ペインで、**[テナント]** ブランチを展開し、**[L4-L7 サービス]** ブランチを展開して、**[デバイス マネージャ]** をクリックします。

ステップ 4 **[アクション] > [デバイス マネージャの作成]** を選択します。

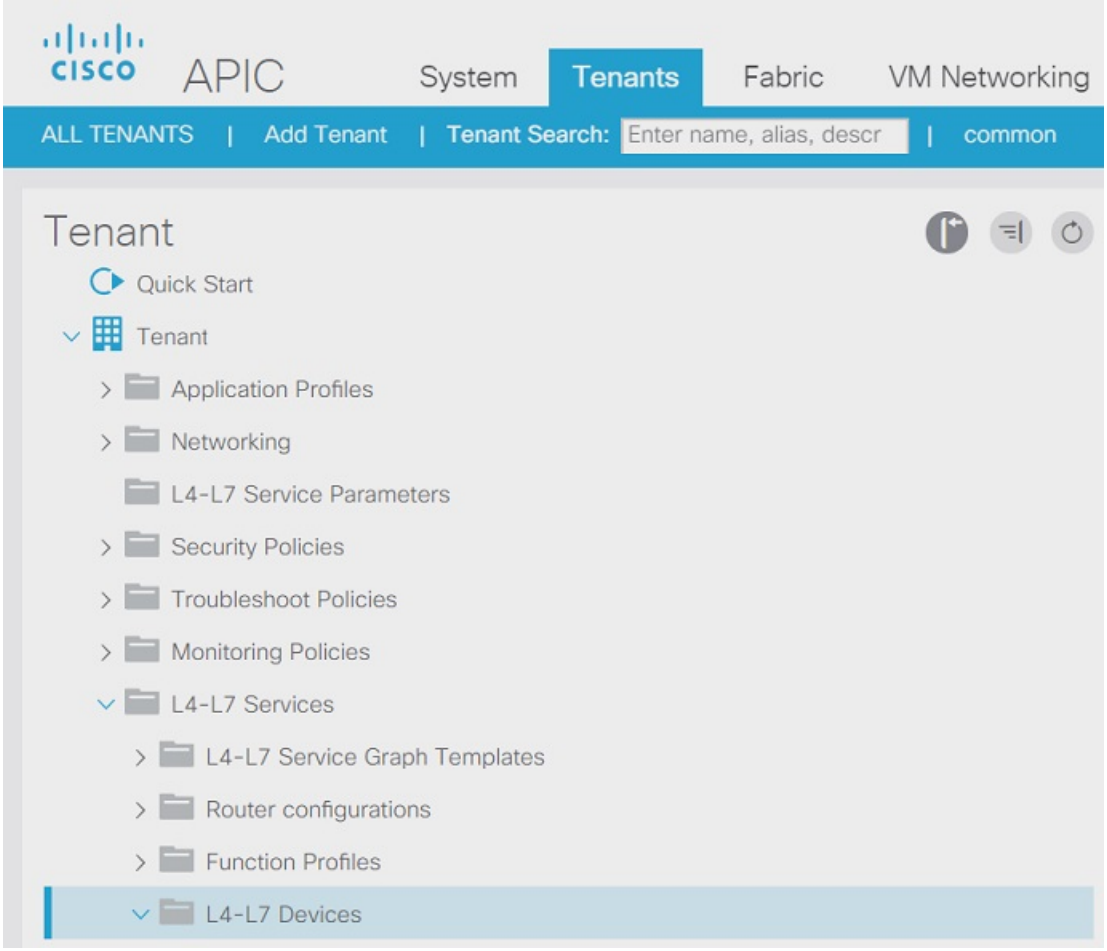
ステップ 5 次のオプションを完了します。

オプション	説明
デバイス マネージャ名	デバイス マネージャの名前。
デバイス マネージャ タイプ	**[CISCO-FTDmgr_FI-1.0]** を選択します。
管理	[+] をクリックして FMC を追加します。これは FTD アプライアンスを管理して、**[ホスト]** および **[ポート]** フィールドに入力します。[Update] をクリックします。
Username	FMC のユーザー名
Password	FMC のパスワード
Confirm Password	FMC のパスワード



ステップ 6 **[送信]** をクリックして、デバイス マネージャを作成します。

ステップ 7 [ナビゲーション]ペインで、**[テナント]** ブランチを展開し、**[L4-L7 サービス]** ブランチを展開して、**[L4-L7 デバイス]** をクリックします。



ステップ 8 **[L4-L7 デバイスの作成]** を右クリックして選択します。**[L4-L7 デバイスの作成]** ダイアログ ボックスが表示され、**[全般]** ページが表示されます。

ステップ 9 次の手順を実行します。

オプション	説明
名前	FTD アプライアンスの名前。 （注） FMC フィールドは 48 文字に制限され、FMC に「<Field Value>_<Tenant Name>_<L4-L7 Device Name>」として保存されるため、この制限に対応するためにテナント、デバイス名の長さを短くすることをお勧めします。
Service Type	**[ファイアウォール]** を選択します。
Device Type	**[物理]** または **[仮想]** を選択します。
デバイス パッケージ	アップロードしたデバイス パッケージを選択します。
モデル	FTD アプライアンスのモデルを選択します。

オプション	説明
コンテキスト認識	テナントにアプライアンスを割り当てます。 （注） 複数は推奨されません。 [単一]は、アプライアンス クラスタをこのプロバイダー ネットワーク上でホストする特定のタイプの複数のテナント全体でアプライアンス クラスタを共有できないことを示しています。 [複数]は、アプライアンス クラスタをこのプロバイダー ネットワーク上でホストする特定のタイプの複数のテナント全体でアプライアンス クラスタを共有できることを示しています。たとえば、同じアプライアンスを共有する 2 つのホスティング会社が存在する可能性があります。テナントの割り当ては、パッケージがバインドされているエンドポイント グループ（EPG）に暗黙的に基づいています。クラスタを作成した場合、アプライアンス管理されるネットワークを判断する管理 EPG を指定する必要があります。
機能タイプ	**[GoThrough]** または **[GoTo]** を選択します。 [GoThrough] アプライアンスは、トランスペアレント ファイアウォール（BVI を使用）または NGIPS モード（IPS 専用ポートを使用）アプライアンスです。ネットワーク パケットは変更に応じてアプライアンスを通過し、エンドポイントはそのアプライアンスを認識しません。[GoTo] アプライアンスはルーテッド ファイアウォール モードであり、特定の L3 宛先から L2 接続 EPG として動作します。
物理的なドメイン	物理 FTD アプライアンスについては、このアプライアンス クラスタを使用するグラフのネットワーク リリースを割り当てる場合に使用するドメインを選択します。既存の物理ドメインを選択するか、新規作成します。 （注） これは、仮想 FTD アプライアンスには必要はありません。
ビュー	単一ノードがデフォルト設定です。設定するデバイス 1 を示します。 （注） 1.0.2 以降、HA ノードはサポートされています。**[HA ノード]** が選択される場合、HA デバイス ペアのデバイス 1 およびデバイス 2 が設定のため表示されます。

オプション	説明
	（注） 1.0.3 以降、クラスタリングがサポートされます。**[クラスタ]** が選択される場合、複数のデバイスを独自の管理アドレスに追加できます。
VMM ドメイン	仮想 FTD アプライアンスについては、Virtual Machine Manager（VMM）ドメイン（vCenter ドメイン）を選択します。既存の VMM ドメインを選択するか、新規作成します。 （注） これは、物理 FTD アプライアンスには必要はありません。
Username	FMC のユーザー名
Password	FMC のパスワード
Confirm Password	FMC のパスワード

ステップ 10 **[デバイス 1]** セクションで次のオプションを入力します。

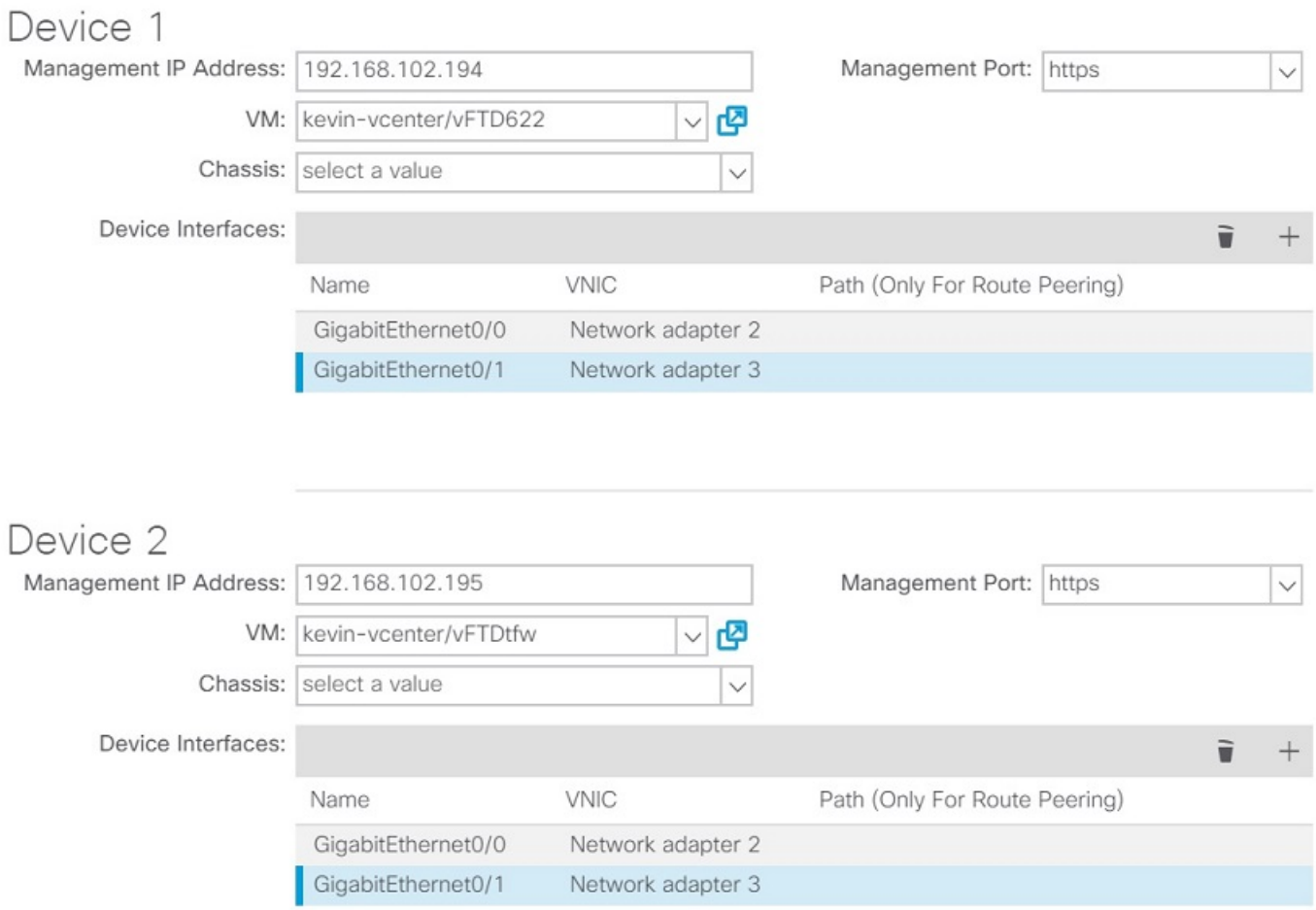
オプション	説明
管理 IP アドレス	アプライアンス クラスタ内の具体的なアプライアンスの管理インターフェイスの IP アドレス。
Management Port	[HTTP] または [HTTPS] を選択します。
VM	仮想 FTD では、アプライアンスがホストされている仮想マシンの名前。 （注） これは、物理 FTD アプライアンスには必要はありません。

ステップ 11 デバイスインターフェイスでは、[+] をクリックして、具体的なアプライアンス上のインターフェイスである具体的なインターフェイスに情報を入力します。入力する情報は、具象インターフェイスがファブリックに接続され、具象インターフェイスが論理インターフェイスに接続される方法について指定します。[更新] をクリックしてインターフェイスを追加します。次のオプションを完了します。

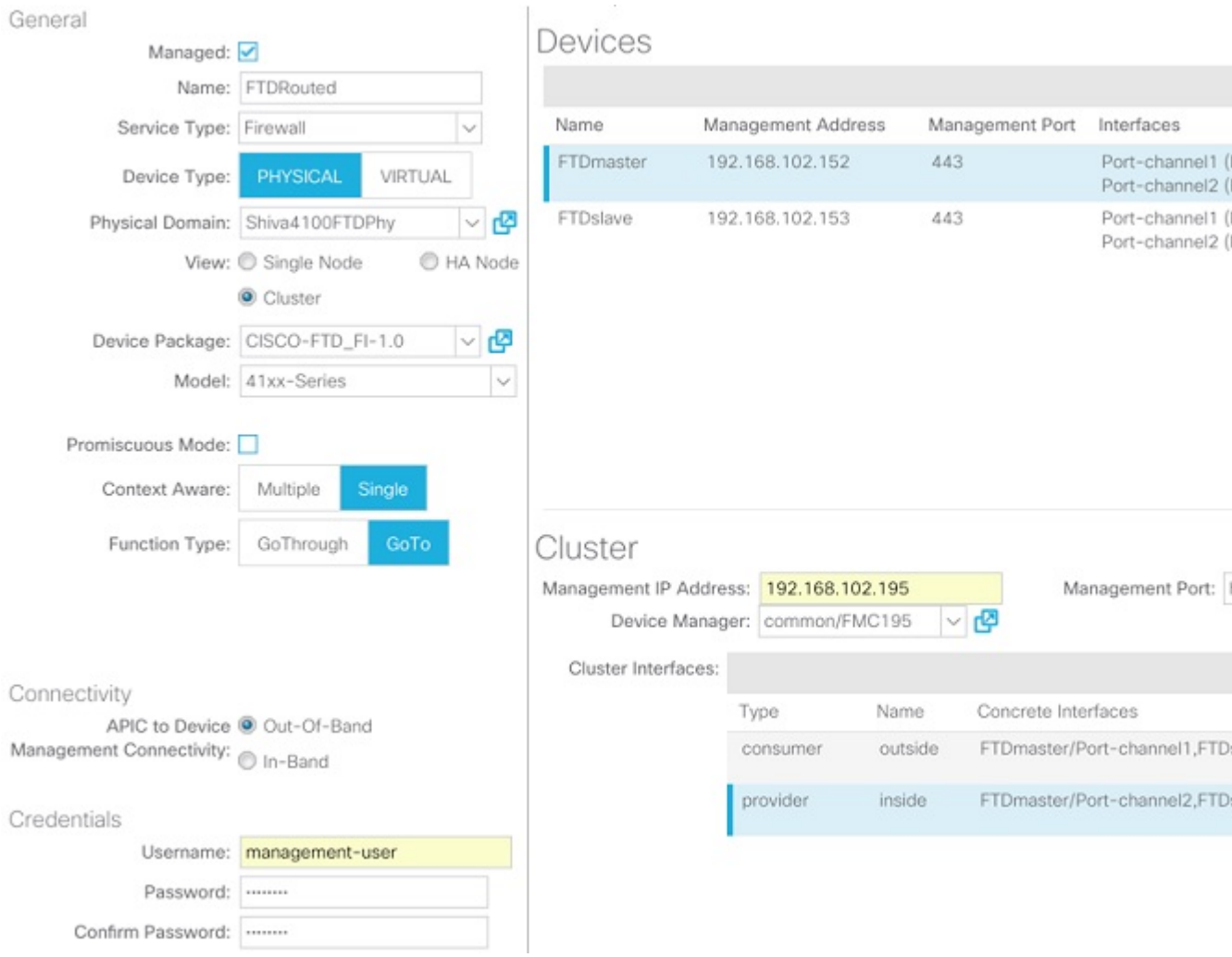
オプション	説明
名前	[名前] フィールドは、具体的なアプライアンスのインターフェイスを特定します。たとえば、GigabitEthernet0/1 または GigabitEthernet0/2 です。
パス	物理アプライアンスは、具体的なインターフェイスがファブリックに接続する方法を指定します。たとえば、具象インターフェイスがアタッチされるリーフ ノード/スロット/ポートです。
vNIC	仮想アプライアンスでは、具体的なアプライアンスの対応するインターフェイスを識別するために vCenter 上で割り当てられたネットワーク アダプタ名。vCenter では通常、x＝1、2、3 の場合 vNIC が **[ネットワーク アダプタ x]** にラベリングされます。 （注） アプライアンス、インターフェイス MAC アドレスをチェックし、[MAC アドレス] フィールドを照合することで vCenter 上の対応するvNIC を識別できます。

ステップ 12 **[ビュー**：**HA ノード]** が選択される場合、**[デバイス 2]** セクションの対応するオプションを入力します。デバイス 1 および 2 は、HA フェールオーバー ペアを形成します。

次に例を示します。



[ビュー：クラスタ] が選択される場合：



ステップ 13 **[クラスタ]** セクションで、次のオプションを入力します。

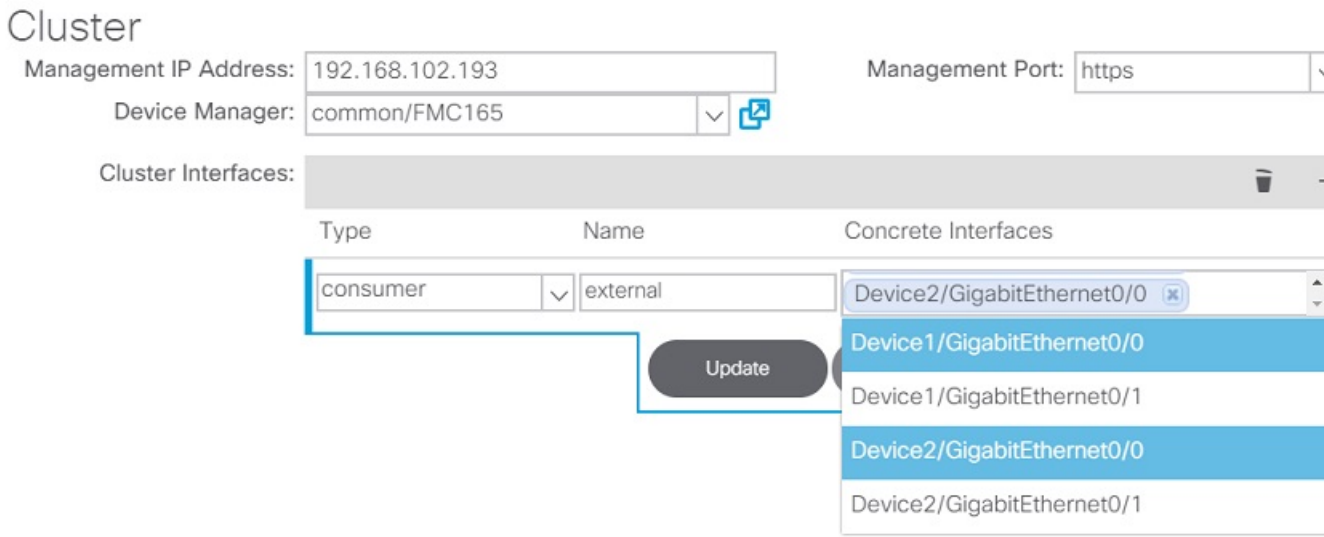
オプション	説明
管理 IP アドレス	FMC の IP アドレス。
Management Port	FMC のポート番号。
Device Manager	デバイス マネージャを選択します。

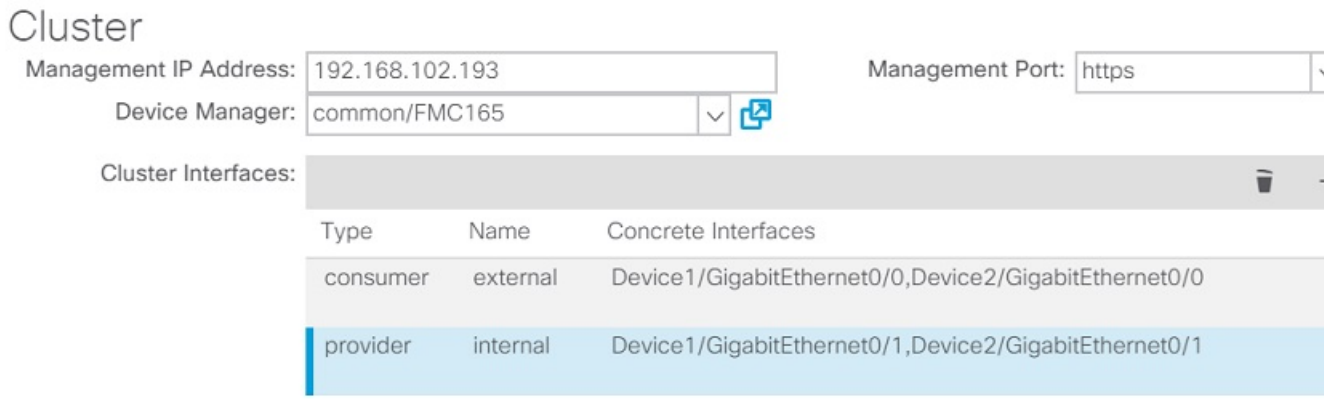
ステップ 14 クラスタ インターフェイスでは、[+] をクリックして、クラスタ論理インターフェイスであるクラスタ インターフェイスに情報を入力します。入力する情報は、論理インターフェイスがファブリックに接続され、論理インターフェイスがアプライアンスの具体的なインターフェイスに接続される方法について指定します。[更新] をクリックしてインターフェイスを追加します。次のオプションを完了します。

オプション	説明
タイプ	クラスタ論理インターフェイスの種類たとえば、**[コンシューマ]** または **[プロバイダ]**。

オプション	説明
名前	[名前] フィールドは、グラフのインターフェイスを特定します。たとえば、**[外部]** または **[内部]**。
具体的なインターフェイス	論理インターフェイスがアプライアンスの具体的なインターフェイスに接続する方法を指定します。

ステップ 15 クラスタのインターフェイスでは、HAデバイスペアの両方のメンバにインターフェイスを指定します。次に例を示します。





ステップ 16 [Next] をクリックします。

ステップ 17 （任意）コンフィギュレーション パラメータを追加します。設定パラメータは具体的なアプライアンスを対象としており、初期化時にワンタイム設定中に使用されます初期化。

ステップ 18 **[終了]** をクリックししてアプライアンスを作成します。

次のタスク

L4-L7 デバイスで FTD デバイスを選択するとき、APIC が適切に登録できる場合は「安定」状態を示している必要があります。FMC に到達不可能、または FMC 上の特定の IP アドレスで FTD が登録されている場合、エラーが表示されます。L4-L7 デバイスの障害を理解し解決するには、「**トラブルシューティング**」の章を参照してください。L4 - L7 設定を使用したサービス グラフを作成する前に、FTD デバイスが「安定」状態であることを確認します。

サービス グラフの作成

サービス グラフは、端末セット間の順序付けられた一連の機能ノードで、アプリケーションが必要とする一連のネットワーク サービス機能を識別します。グラフ内のサービス機能は、アプリケーションの要件に基づいたサービス デバイスに自動的にプロビジョニングされます。

アプライアンスを登録した後は、そのアプライアンスおよびそのアプライアンスが提示したすべての機能を使用してサービス グラフを作成できます。サービス グラフは、共通テナントで作成するか、テナント固有にすることができます。これは、プロバイダー管理者またはテナント内のテナント管理者によって実行されます。

サービス機能として FTD を挿入するには、サービス グラフ テンプレートを FTD 関数ノードを使用して作成する必要があります。

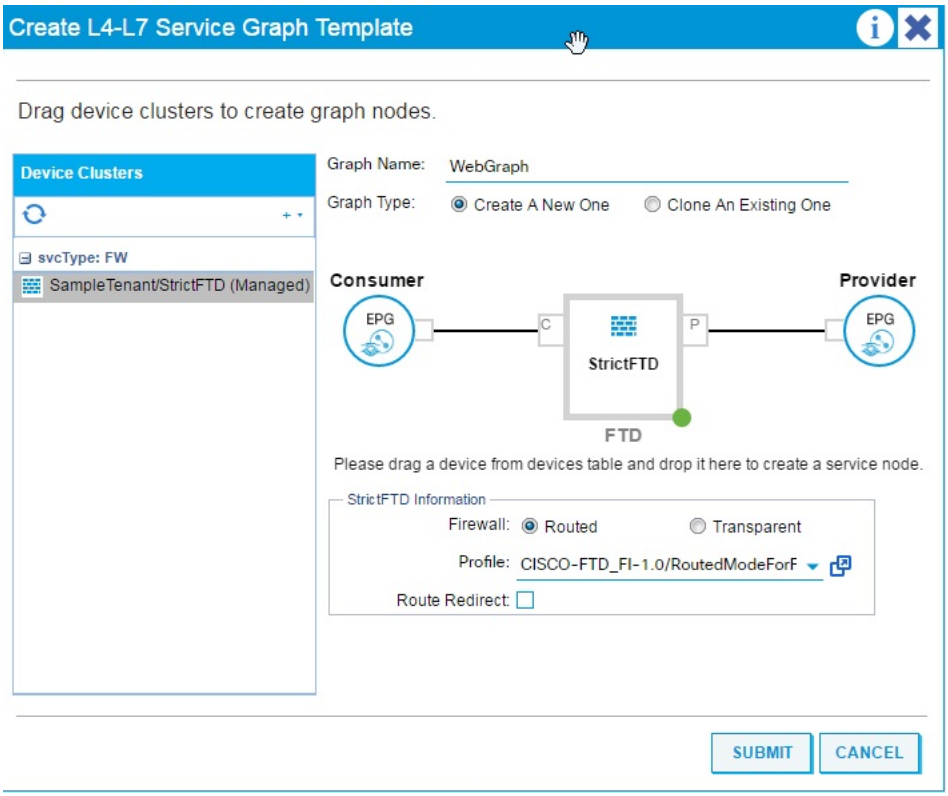
ステップ 1 APIC にサインインします。

ステップ 2 共通テナントまたは特定のテナントに移動します。

ステップ 3 [ナビゲーション] ペインで、**[L4 - L7 サービス]** ブランチを展開し、**[L4 - L7 サービス グラフ テンプレート]** をクリックします。

ステップ 4 **[アクション] > [L4 - L7 サービス グラフ テンプレートの作成]** を選択します。

（注） **[L4 - L7 サービス グラフ テンプレートの作成]** ダイアログ ボックスが表示されます。左側のペインには、APIC が認識しているサービス デバイス、およびデバイスによって提供されるサービス機能が一覧表示されます。APIC は、以前インポートした ACI デバイス パッケージの FTD からこの情報を取得します。



ステップ 5 サービス グラフの名前を **[グラフ名]** フィールドに入力します。

ステップ 6 左ペインから右ペインに FTD サービス機能をドラッグ アンド ドロップして、その機能をサービス グラフに追加します。

ステップ 7 ノードの名前を変更します。

ステップ 8 展開に基づいて、ファイアウォール モードのタイプを **[ルーテッド]** または **[トランスペアレント]** から選択します。

ステップ 9 サービス ノードのプロファイルを選択します。デバイス パッケージに付属しているか、以前作成したデフォルト テンプレートで機能プロファイルを選択します。

ステップ 10 **[送信]** をクリックしてグラフをを作成します。
[サービス グラフ] ダイアログ ボックスは作成した新しいグラフを一覧表示します。

サーサービス グラフ テンプレートの適用ビス グラフ テンプレートの適用

APIC は、サービス グラフに指定されているサービス機能要件に従ってサービスを自動的に設定します。APIC はまた、サービス グラフで指定されるサービス機能のニーズに応じてネットワークを自動的に設定しますが、これによってサービス デバイスでの変更は要求されません。

APIC では、デバイス パッケージ内のアプライアンス スクリプトにパラメータを渡します。アプライアンス スクリプトは、パラメータ データをアプライアンスにダウンロードされる設定に変換します。これは、アプリケーション プロファイル、EPG が特定のテナントに存在していると仮定し、作成したサービス グラフを関連付けます。

次の手順により、コントラクトとサービス グラフを関連付けます。

始める前に

テナントを設定します。

EPG でアプリケーション プロファイルを設定します。

ステップ 1 APIC にサインインします。

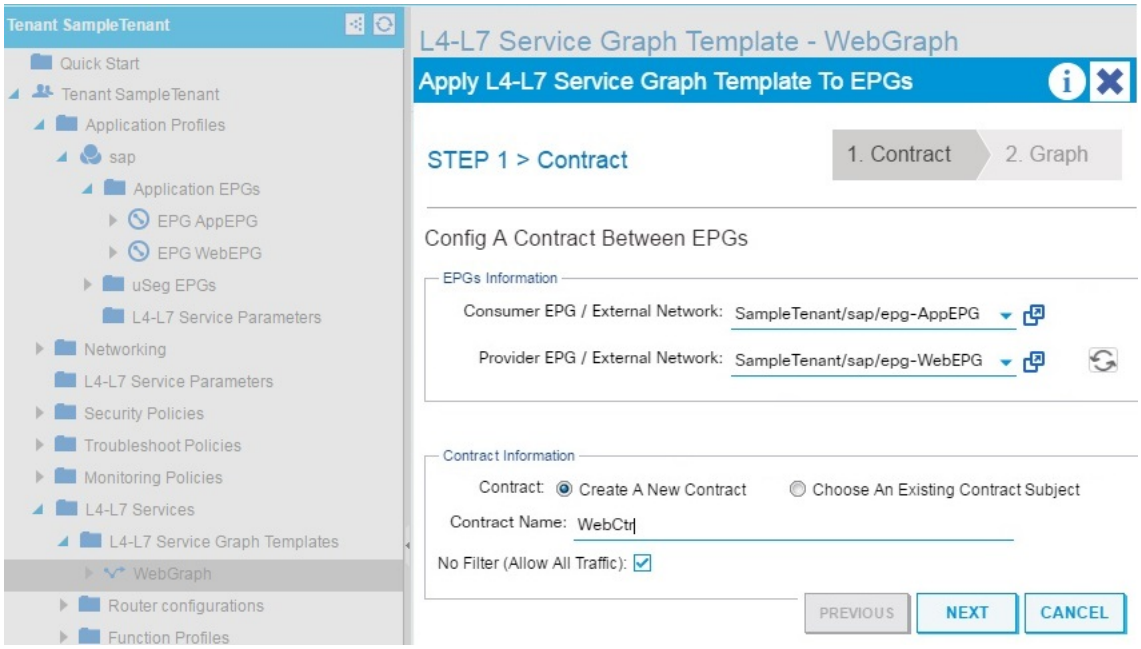
ステップ 2 メニュー バーで、**[テナント]** をクリックします。

ステップ 3 [ナビゲーション] ペインで、テナントのフォルダ ツリーを展開します。

ステップ 4 **[L4-L7 サービス]> [L4-L7 サービス グラフ テンプレート]** ブランチを展開して、サービス グラフ テンプレートを表示します。

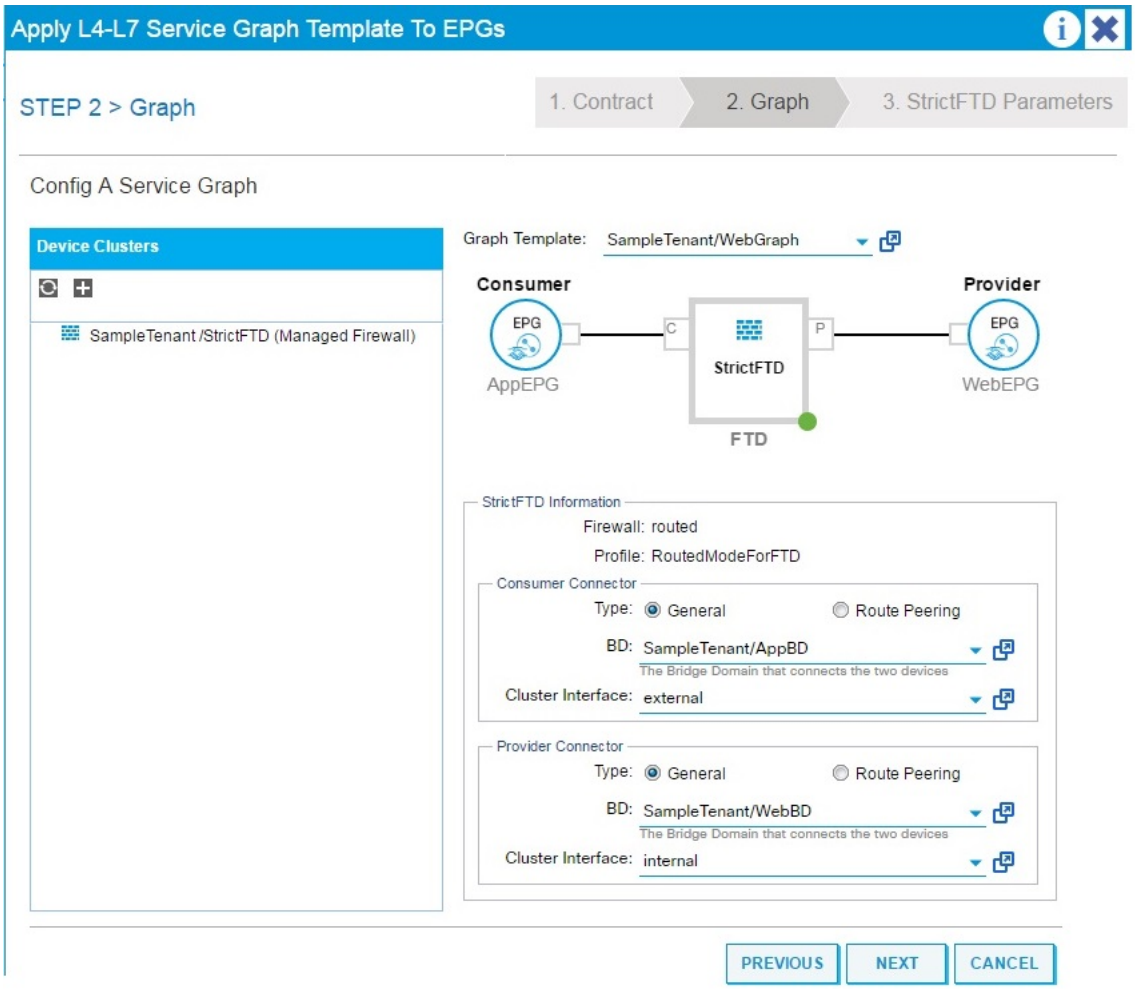
ステップ 5 選択したサービス グラフ テンプレートを右クリックし、表示されるポップアップ メニューで **[L4-L7 サービス グラフ テンプレートの適用]** をクリックします。

ステップ 6 **[手順 1 コントラクト]** ダイアログ ボックでス、コンシューマとプロバイダ EPG を選択します。

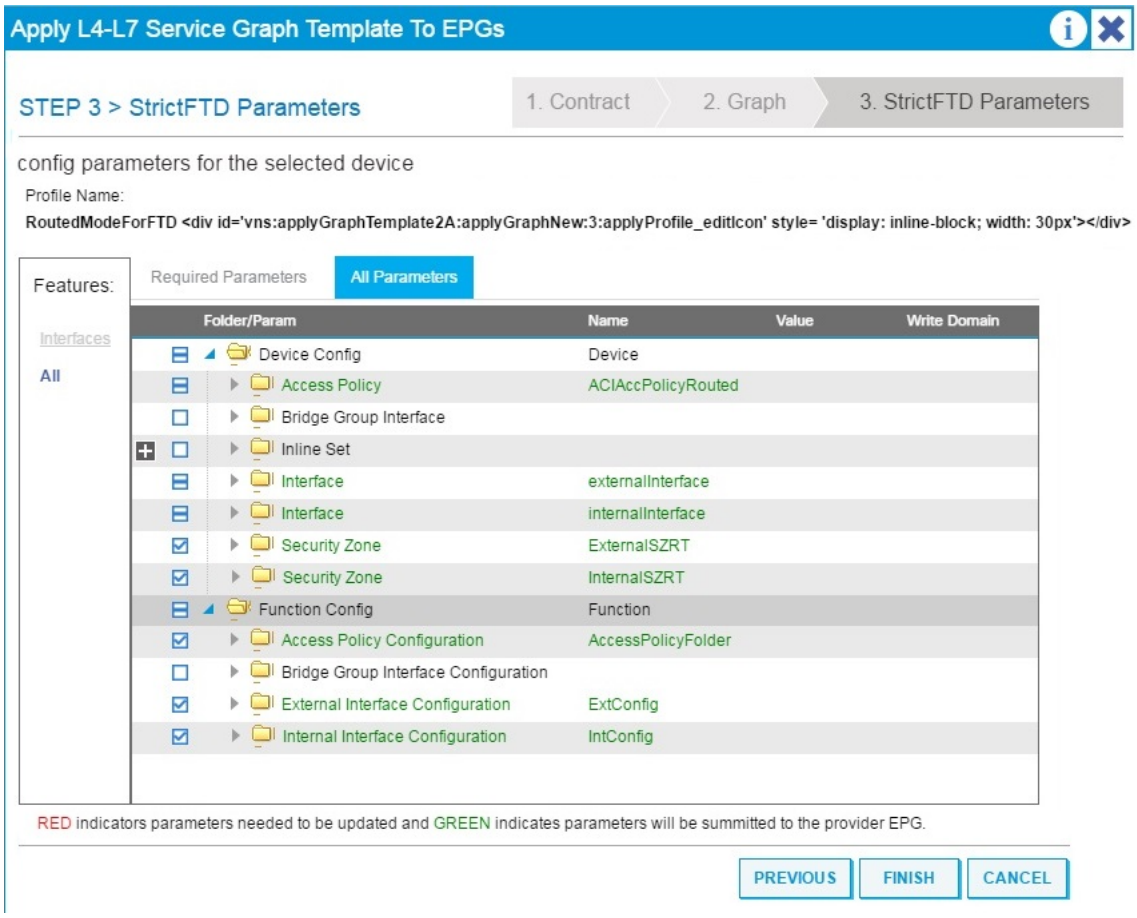


ステップ 7 新しいコントラクトを作成するか、既存のコントラクト件名を選択します。新しいコントラクトの名前を入力します。[Next] をクリックします。

ステップ 8 **[手順 2 グラフ]** ダイアログ ボックスで、ブリッジ ドメイン（BD）とクラスタ インターフェイスを選択します。[Next] をクリックします。



ステップ 9　**[手順3 パラメータ]** ダイアログ ボックスで、**[すべてのパラメータ]** タブをクリックします。



ステップ 10 展開に基づいてパラメータを設定します。組み込みテンプレートに基づいて機能プロファイルを定義し、この手順で使用することができます。機能のサポートと FTD 展開の次のセクションを参照してください。[終了] をクリックしてグラフにコントラクトをアタッチします。

次のタスク

サービス グラフのインスタンスを作成したら、APIC が FTD インターフェイスにプロビジョニングされた設定を FMC に正常にプッシュしていることを確認します。

また、エンド ポイントがプロビジョニング済みの FTD を使用して相互に通信できることを確認します。

Supported Functions

このセクションでは、ACI デバイス パッケージの FTD でサポートされている公開されている機能について説明します。

（注） アスタリスク (「*」)] オプションが必要であることを示します。そうしないと、これはオプションです。

（注） GraphDeploymentSuffix は「_<Tenant name="">_<Device name="">」の値に追加されると以下に指定された where。</Device> </Tenant>

（注） すべてのサポートされていない FTD 機能、サービス グラフを削除またはテナントの削除の前に手動で設定をクリーンアップすることをお勧めします。

機能	パラメータ	Options	説明

アクセス ポリシー	*Name	<name>		Name of the access policy. • APIC では、ポリシーの説明を GraphDeploymentSuffix およびその他の情報を内部的に追加します。 • 既存の FMC アクセス ポリシー名は、APIC を使用するのと一致する必要があります。
	*Access Rules	*Name	<name>	アクセスルールの名前。 • APIC では、ルールのコメントに、GraphDeploymentSuffix およびその他の情報を内部的に追加します。 • 既存の FMC アクセス ルール名は、作成したサービス グラフ セキュリティ ゾーンを更新する APIC の一致する必要があります。
		Source Interface	インターフェイス オブジェクトのセキュリティ ゾーンへの参照	)]:
		Destination Interface	インターフェイス オブジェクトのセキュリティ ゾーンへの参照	)]:
		双方向	true | false	

				設定 true の場合、セキュリティの両方を適用するゾーンでアクセスルール送信元と宛先ゾーン。そうしないと、セキュリティ ゾーンは、個別に適用されている送信元と宛先フィールドです。

Security Zone	*Name	<name>	Name of the security zone. また、APIC他のオブジェクトが参照できるようにするため、セキュリティゾーンのAPICフォルダ名はオブジェクトを。 APIC では、名前に、GraphDeploymentSuffix 内部的に追加します。たとえば、外部のセキュリティゾーンの名前を選択すると、FMC にわかります External_<Tenant name="">_<Device name="">.</Device></Tenant> という名前のセキュリティゾーン （注） Name フィールドとして保存 <Field value="">_<Tenant name="">_<Device name="">> され、合計で 48 文字に制限 されます FMC で </Device></Tenant></Field>。 GraphDeploymentSuffix には、 40 文字を使用できます、た めには、8 文字を名 ()] フィールドの値を制限してみ ます。
	*Type	インライン|ルーティング|スイッチング	セキュリティゾーンのタイプ。 一致しないセキュリティゾーンのタイプおよびインターフェイスのタイプは許可されません。これは、展開モードに基づくものです。

インラインセット	*Name	<name>	Name of the inline set. また、APIC フォルダ セットの名前、インライン オブジェクト、APIC他のオブジェクトが参照できるようにします。 APIC では、名前に、GraphDeploymentSuffix 内部的に追加します。たとえば、外部のインラインセット名を選択する場合、FMC にわかりますインラインセットが External_<Tenant name="">_<Device name="">.</Device></Tenant> という名前 （注） Name フィールドとして保存 <Field value="">_<Tenant name="">_<Device name=""> され、合計で 48 文字に制限されます FMC で </Device></Tenant></Field>。GraphDeploymentSuffix には、40 文字を使用できます、ためには、8 文字を名 ()] フィールドの値を制限してみます。
	*MTU	<integer>	インラインセットの MTU プロパティ。
	*Snort Fail Open Busy	true | false	インラインセットのオープン ビジーの失敗のプロパティを snort します。
	*Snort Fail Open Down	true | false	インラインセットのプロパティが失敗するオープンダウンを snort します。

インターフェイス	*Name	<name>			インターフェイスオブジェクトの APIC フォルダの名前。
	*Enabled	true | false			インターフェイスのプロパティを有効にします。
	*MTU	<integer>			MTU property of the interface.
	*Logical Name	<name>			インターフェイスの論理名(省略可能な限りインライン)。 APIC では、名前に、GraphDeploymentSuffix 内部的に追加します。たとえば、論理名の外部を選択する場合、FMC にわかります論理名の External_<Tenant name="">_<Device name="">.</Device> </Tenant> （注） Name フィールドとして保存 <Field value="">_<Tenant name="">_<Device name="">> され、合計で 48 文字に制限されます FMC で </Device></Tenant></Field>。GraphDeploymentSuffix には、40 文字を使用できます、ためには、8 文字を名 ()] フィールドの値を制限してみます。
	*Inline Set	Inline Set Object			APICインライン設定フォルダ オブジェクトへのリンクを参照します。
	*Security Zone	セキュリティゾーンオブジェクト			セキュリティ ゾーンの APIC フォルダ オブジェクトへのリンクを参照します。
	*IPv4	*static	*address	サブネットマスクを使用した IPv4 アドレス	

					ルーテッドインターフェイスにのみ適用されます。値は、サブネットマスクとIPv4アドレスです。たとえば、1.1.1.1/24というようになります。
□ブリッジグループ インターフェイス	*Name	<name>			ブリッジグループインターフェイスの APIC フォルダの名前。 APIC では、説明を GraphDeploymentSuffix およびその他の情報を内部的に追加します。
	* IPv4 アドレスの設定	*static	*address	IPv4 address with subnet mask	透過インターフェイスにのみ適用されます。値は、サブネットマスクと IPv4アドレスです。For example, 1.1.1.1/24
	*Bridge Group ID	<integer>			)]:
	*Interfaces	)]:			APIC インターフェイス フォルダ オブジェクトへのリンクを参照します。

IPv4 Static Route	*Network	<network>	このルートの外部ネットワーク。A.B.C.D/prefix 形式にする必要があります。For example, 192.168.1.0/24
	*Gateway	<gateway>	外部ネットワークに到達するために使用されるゲートウェイの IPv4 アドレス。For example, 192.168.1.1
	メトリック	<integer>	Distance metric for this route. 有効な範囲は 1 ~ 255 (両端の値を含む) です。
	isTunneled	true | false	)]:
	• ルーテッド モードの FTD の IPv4 スタティック ルートを設定する場合は、設定、物理インターフェイス レベルでします。ただし、物理インターフェイスが BVI インターフェイス (IRB 機能) に配置されます、BVI インターフェイス レベルでの IPv4 スタティック ルートを設定します。 • 透過モードの FTD の IPv4 スタティック ルートを設定する場合は、設定、BVI 設定に関係なく、物理インターフェイス レベルでします。		

FTD 展開

このセクションでは、さまざまな展開モードに必要な機能プロファイル設定の変更について説明します。3 個すべてのモードで、適切なアクセス コントロール ポリシーまたはルールの参照が必要です。

- アクセス ポリシー名が正確に設定されていることを確認します。
- アクセス ポリシーの下のアクセス ルールが、送信元と宛先のセキュリティ ゾーンのマッピングが正しいインターフェイスを指している状態で、正確に設定されていることを確認します。インターフェイスのセキュリティ ゾーンからアクセス ルール ソースおよび宛先ゾーンの両方に、双方向フラグが設定されていることを確認します。

トランスペアレント モード

デフォルトの機能プロファイル **CISCO-FTD_FI-1.0/TransparentModeForFTD** を選択します。

- ブリッジ ドメイン ID（**[デバイス設定] > [□ブリッジ グループ インターフェイス] > [ブリッジ グループ ID] > [値]**）が固有の番号であることを確認します。□ブリッジ グループ インターフェイスの IP アドレスを設定し、インターフェイスが正しく設定されていることを確認します。

- セキュリティ ゾーン名（**[デバイス設定] > [セキュリティ ゾーン] > [名前]**）が正しく設され、そのタイプがスイッチ済みに設定されていることを確認します。
- インターフェイスの論理名が固有であることを確認します（**[デバイス設定] > [インターフェイス（内部または外部)）] > [論理名] > [値]**）。有効フラグが [true] に設定され、セキュリティ ゾーンが正しくマッピングされていることを確認します。

ルーテッド モード

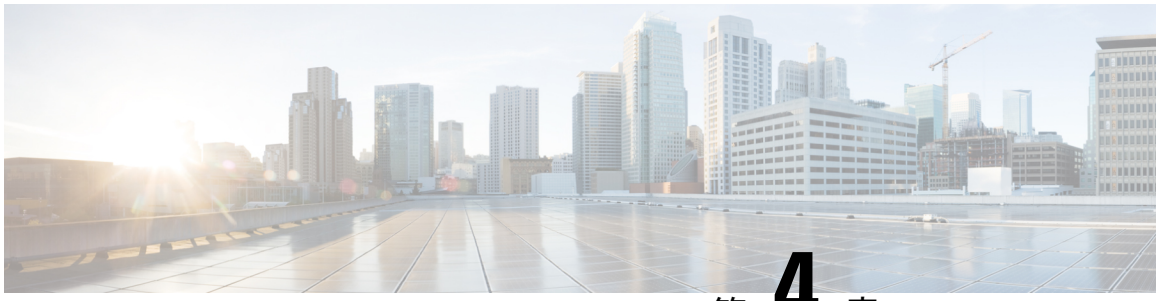
デフォルトの機能プロファイル **CISCO-FTD_FI-1.0/RoutedModeForFTD** を選択します。

- セキュリティ ゾーン名（**[デバイス設定] > [セキュリティ ゾーン] > [名前]**）が正しく設され、そのタイプがルーテッド済みに設定されていることを確認します。
- インターフェイスの論理名が固有であることを確認します（**[デバイス設定] > [インターフェイス（内部または外部)）] > [論理名] > [値]**）。有効フラグが [true] に設定され、セキュリティ ゾーンが正しくマッピングされていることを確認します。インターフェイス IP アドレスを設定します。

インライン モード

デフォルトの機能プロファイル **CISCO-FTD_FI-1.0/InlineModeForFTD** を選択し確認します。

- インライン セット名（**[デバイス設定] > [インライン セット] > [名前]**）が正しく設定されています。
- セキュリティ ゾーン名（**[デバイス設定] > [セキュリティ ゾーン] > [名前]**）が正しく設され、そのタイプがルーテッド済みに設定されていることを確認します。
- インターフェイスの論理名が固有であることを確認します（**[デバイス設定] > [インターフェイス（内部または外部)）] > [論理名] > [値]**）。有効フラグが [true] に設定されており、インライン セットとセキュリティ ゾーンが正しくマッピングされていることを確認します。



第 4 章

Troubleshoot

障害の修復

このセクションでは、一般的な障害を含む基本的なトラブルシューティングの一部と、修復方法について説明します。

パラメータ設定

APIC のネットワーク サービス グラフ上で FTD サービス ノードの設定パラメータを誤ると、次の障害のいずれかを返すことがあります。

障害の形式

グラフ設定の結果「メジャー スクリプト エラー：設定エラー：<error>* for <parameter-name> in context <context-name> on cluster <cluster-name> in tenant <tenant-name>

Fault メッセージ

グラフ設定の結果：テナント SampleTenant のクラスタ StrictFTDvCluster 上のコンテキスト SampleTenantctx1 で有効な「メジャー スクリプト エラー；設定エラー：指定されたインターフェイス タプおよびセキュリティ ゾーン タイプが一致する必要があります」となります。

修復

正しいタイプで新しいセキュリティ ゾーンを作成し、古いゾーンを削除します。作成した後、FMC はセキュリティ ゾーンを変更できません。FMC の予想に基づき、サービス グラフの一致しない設定パラメータを修正します。

Fault メッセージ

グラフの設定の結果：「メジャー スクリプト エラー：設定エラー：名前 DefaultInlineSet の項目はすでに存在しています。別の名前を選択するか、または現在の項目 を削除してください」

修復

DefaultInlineSet の名前を持つインライン設定が FMC で設定されていないことを確認します。すでに存在しているインライン設定はデバイス パッケージでは使用できません。デバイス パッケージは、ワークフローの影響を与えずに削除できるように新規インライン設定を作成する必要があります。

Fault メッセージ

グラフの設定の結果：「メジャー スクリプトのエラー：設定エラー：インターフェイス名は 48 文字以上にすることはできません」

修復

2 個以上の区切り文字（「_」）が含まれるテナント、デバイス、インターフェイス論理またはインライン設定が 48 文字以上にならないことを確認します。

Fault メッセージ

グラフの設定の結果：「メジャー スクリプト エラー：設定エラー：名前は 48 文字より短くする必要があります」

修復

2 個以上の区切り文字（「_」）が含まれるテナント、デバイス、インターフェイス セキュリティ ゾーン名が 48 文字以上にならないことを確認します。

アプライアンス設定

APIC の誤った設定のアプライアンス ログインと IP 情報はにより、次の障害のいずれかが発生する可能性があります。

Fault メッセージ

グラフ設定の結果、 * 重要なスクリプト エラーが発生しました: 設定エラー: アプライアンスにログインできません。設定されているログイン情報が間違っています。* というエラーが発生します。

修復

設定されている FMC ユーザー名とパスワードが正しいか確認してください。

Fault メッセージ

グラフ設定の結果、* 重要なスクリプト エラーが発生しました: 設定エラー: 要求されたデバイスがありません* という障害が発生します。

修復

設定されているデバイスが設定されている FMC に登録されていることを確認します。

Fault メッセージ

グラフの設定の結果、*接続されたパーティが一定時間経過しても適切に応答しなかったか、接続されているホストが応答に失敗したため接続の確立に失敗しました。* というエラーが発生します。

修復

設定されている FMC IP アドレスが正しく、到達可能であることを確認します。

Fault メッセージ

グラフの設定の結果、* 重要なスクリプトのエラー: 設定エラー: 要求されたインターフェイスが見つかりません。* というエラーが発生します。

修復

デバイス クラスタが FMC に存在しており、デバイスに設定されている具体的なインターフェイスを確認します。

Fault メッセージ

グラフ設定の結果、* 重要なスクリプト エラーが発生しました: 設定エラー: 設定の変更をデバイスに展開できません。考えられる理由は、別の展開が進行中か、APIC と FMC の時間が同期してない可能性があります。必ず同じ NTP サービスに時間を同期し、タイム ゾーンをセットアップしてから、サービス グラフを再度接続するようにしてください。* というエラーが発生します。

修復

同じ NTP サービスに ACI と FMC が設定されており、その他の展開は同一のデバイスので進行していないことを確認します。

Fault メッセージ

グラフの設定の結果、* 重要なスクリプトのエラー: 設定エラー: デバイス設定がありません。* というエラーが発生します。

修復

デバイス クラスタのデバイスが正しく設定されていることを確認します。また、デバイス マネージャが 1 つのみ FMC ホストの情報を使用して設定されていることを確認します。

Fault メッセージ

グラフの設定の結果、* 重要なスクリプトのエラー: 設定エラー: デバイスの IP またはポートの設定がありません。* というエラーが発生します。

修復

登録済みのデバイス クラスタまたはアプライアンス IP アドレスとポートが正しく設定されていることを確認します。

Fault メッセージ

グラフの設定の結果、* 重要なスクリプト エラー: 設定エラー: デバイスのユーザ名またはパスワードの設定がありません。*

修復

登録済みのデバイス クラスタのユーザ名とパスワードが正しく設定されていることを確認します。

Fault メッセージ

グラフの設定の結果、* 重要なスクリプト エラー: 設定エラー: デバイスのユーザ名またはパスワードの設定がありません。*

修復

登録済みのデバイス クラスタのユーザ名とパスワードが正しく設定されていることを確認します。

Fault メッセージ

グラフの設定の結果、* 重要なスクリプト エラーが発生しました: 設定エラー: FMC フィールドは 48 文字に制限し、<Field value="">_<Tenant name="">_<L4-L7 device="" name="">」.</L4-L7></Tenant> </Field> として FMC に保存されます。2 つの区切り文字 (「_」) と組み合わせてある現在のテナントとデバイス名が40 文字以上であり、8 文字の関数プロファイル フィールドで終了しています。テナントまたはデバイス名の長さをこの制限に適合させて減らしてください。* というエラーが発生します。

修復

テナントとデバイスの名前を組み合わせた結果が 38 文字以下ではないことを確認します。