FMC を使用した Firepower Threat Defense の展開

この章の対象読者

この章では、FMC を使用して管理されるスタンドアロンの FTD 論理デバイスを展開する方法について説明します。ハイ アベイラビリティ ペアまたはクラスタを展開する場合は、『FMC configuration guide』を参照してください。

大規模ネットワークにおける一般的な展開では、複数の管理対象デバイスをネットワーク セグメントにインストールし、分析のためにトラフィックをモニタして、管理 FMC にレポートします。これにより、管理、分析、およびレポート タスクの実行に使用できる Web インターフェイスがある集中管理コンソールを使用できます。

単一またはごく少数のデバイスのみが含まれるネットワークでは、FMC のような高性能の多機能デバイス マネージャを使用する必要がなく、一体型の Firepower Device Manager（FDM）を使用できます。FDM の Web ベースのデバイス セットアップ ウィザードを使用して、小規模ネットワークの導入に最もよく使用されるソフトウェアの基本機能を設定できます。

（注） **プライバシー収集ステートメント**：Firepower 4100 には個人識別情報は不要で、積極的に収集することもありません。ただし、ユーザ名などの設定では、個人識別情報を使用できます。この場合、設定作業時や SNMP の使用時に、管理者が個人識別情報を確認できる場合があります。

FMC を使用した Firepower Threat Defense の概要

FTD は、ステートフル ファイアウォール、ルーティング、VPN、Next-Generation Intrusion Prevention System（NGIPS）、Application Visibility and Control（AVC）、URL フィルタリング、高度なマルウェア防御（AMP）などの次世代ファイアウォールサービスを提供します。

FTD を管理するには、別のサーバ上で実行されるフル機能のマルチデバイスマネージャである Firepower Management Center（FMC）を使用します。

FTD は、FTD 論理デバイスに割り当てた管理インターフェイス上の FMC を登録して通信します。

トラブルシューティングの目的で、管理インターフェイス上の SSH を使用して FTD CLI にアクセスすることも、FXOS CLI から FTD に接続することもできます。

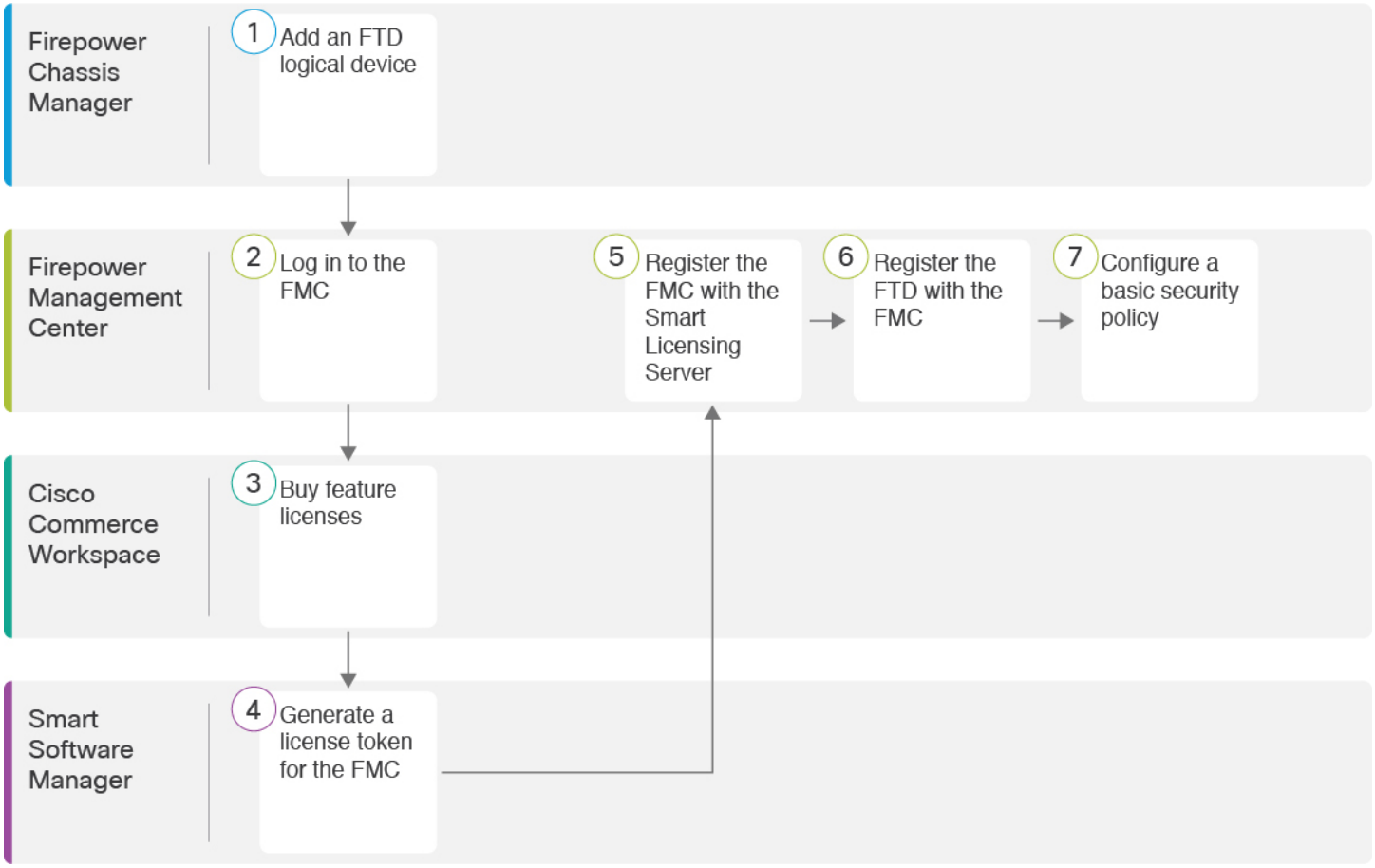
はじめる前に

FMC の初期設定を展開して実行します。『FMC getting started guide』を参照してください。

（注） Firepower デバイスと FMC の両方に同じデフォルトの管理 IP アドレス（192.168.45.45）が設定されています。このガイドでは、初期セットアップ時に異なる IP アドレスをデバイスに設定することを前提としています。

エンドツーエンドの手順

シャーシで FTD を展開して設定するには、次のタスクを参照してください。



	ワークスペース	手順
1	Firepower Chassis Manager	Firepower Chassis Manager：Firepower Threat Defense 論理デバイスを追加します。 （4 ページ）。
2	FMC	Firepower Management Center へのログイン （10 ページ）。
3	Cisco Commerce Workspace	Firepower Management Center のライセンス取得 （10 ページ）：機能ライセンスを購入します。
4	Smart Software Manager	Firepower Management Center のライセンス取得 （10 ページ）：FMC のライセンストークンを生成します。
5	FMC	Firepower Management Center のライセンス取得 （10 ページ）：スマート ライセンシング サーバに FMC を登録します。
6	FMC	Firepower Management Center を使用した Firepower Threat Defense の登録 （12 ページ）。
7	FMC	基本的なセキュリティポリシーの設定 （15 ページ）。

Firepower Chassis Manager：Firepower Threat Defense 論理デバイスを追加します。

FTD をネイティブまたはコンテナのいずれかのインスタンスとして Firepower 4100 から展開できます。セキュリティ エンジン ごとに複数のコンテナ インスタンスを展開できますが、ネイティブインスタンスは1つだけです。モデルごとの最大コンテナインスタンス数については、論理デバイスのアプリケーションインスタンス：コンテナとネイティブを参照してください。

ハイ アベイラビリティ ペアまたはクラスタを追加する場合は、『FMC configuration guide』を参照してください。

この手順では、アプリケーションで使用されるブートストラップ設定を含む、論理デバイスの特性を設定できます。

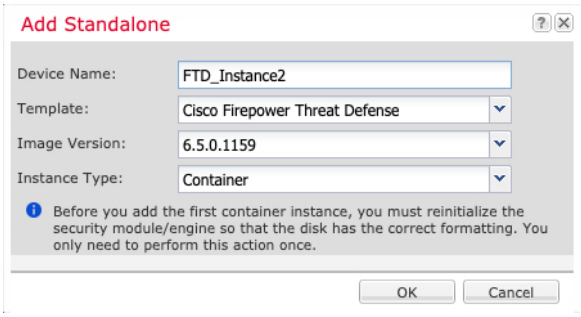
始める前に

- FTD と一緒に使用する管理インターフェイスを設定します。インターフェイスの設定 を参照してください。管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用される（[インターフェイス（Interfaces）] タブの上部に [MGMT] として表示される）シャーシ管理ポートと同じではありません。
- また、少なくとも 1 つのデータ インターフェイスを設定する必要があります。
- コンテナ インスタンスの場合、最小リソースを使用するデフォルト プロファイルを使用しない場合は、**[プラットフォーム設定（Platform Settings）]** > **[リソースプロファイル（Resource Profiles）]** でリソース プロファイルを追加します。
- コンテナ インスタンスの場合、最初にコンテナ インスタンスをインストールする前に、ディスクが正しいフォーマットになるように セキュリティ エンジン を再度初期化する必要があります。このアクションが必要な場合は、論理デバイスを保存できません。**[セキュリティエンジン（Security Engine）]** を選択し、[再初期化（Reinitialize）] アイコン（ ）をクリックします。
- 次の情報を用意します。
  - このデバイスのインターフェイス ID
  - 管理インターフェイス IP アドレスとネットワーク マスク
  - ゲートウェイ IP アドレス
  - FMC 選択した IP アドレスおよび/または NAT ID
  - DNS サーバの IP アドレス。

手順

ステップ 1 Firepower Chassis Manager で、[論理デバイス（Logical Devices）] を選択します。

ステップ 2 **[追加（Add）] > [スタンドアロン（Standalone）]** をクリックし、次のパラメータを設定します。



a) **デバイス名**を入力します。

この名前は、シャーシスーパバイザが管理設定を行ってインターフェイスを割り当てるために使用します。これはアプリケーション設定で使用されるデバイス名ではありません。

b) [Template] では、[Cisco Firepower Threat Defense] を選択します。

c) [Image Version] を選択します。

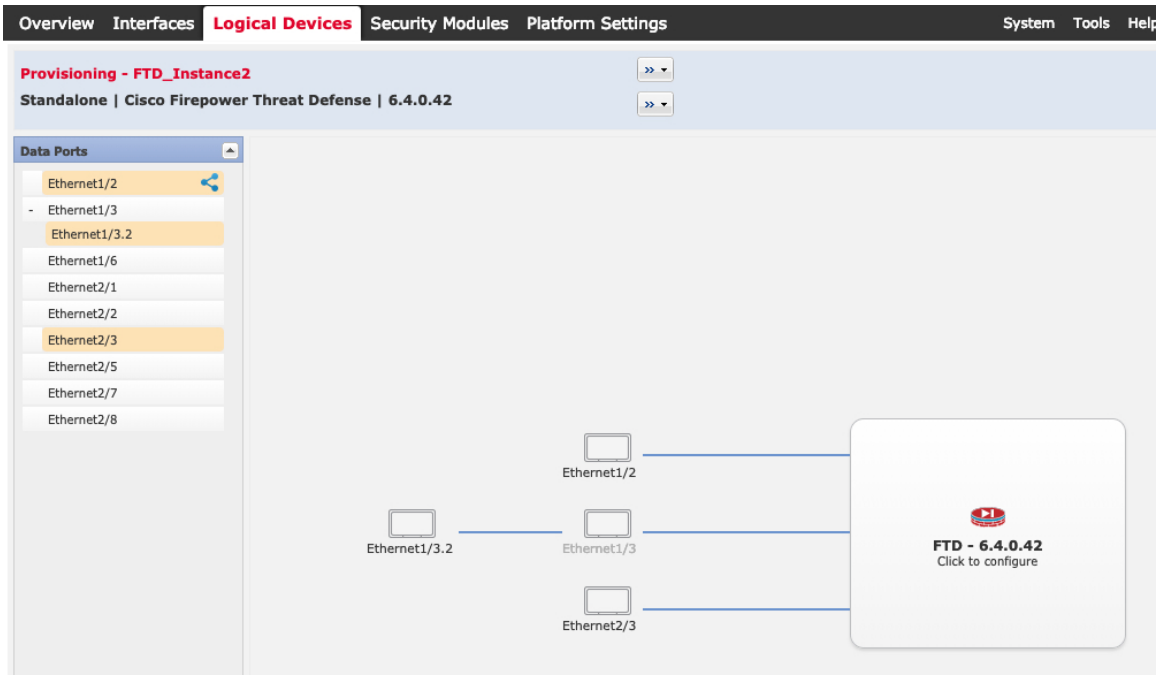
d) [インスタンスタイプ（Instance Type）] で、[コンテナ（Container）] または [ネイティブ（Native）] を選択します。

ネイティブインスタンスはセキュリティモジュール/エンジンのすべてのリソース（CPU、RAM、およびディスク容量）を使用するため、ネイティブ インスタンスを 1 つのみインストールできます。コンテナ インスタンスでは、セキュリティモジュール/エンジンのリソースのサブセットを使用するため、複数のコンテナインスタンスをインストールできます。

e) [OK] をクリックします。

[Provisioning - *device name*] ウィンドウが表示されます。

ステップ 3 [Data Ports] 領域を展開し、デバイスに割り当てるインターフェイスをそれぞれクリックします。



[インターフェイス（Interfaces）]ページで以前に有効にしたデータ インターフェイスとデータ共有インターフェイスのみを割り当てることができます。後ほどFMCでこれらのインターフェイスを有効にして設定します。これには、IP アドレスの設定も含まれます。

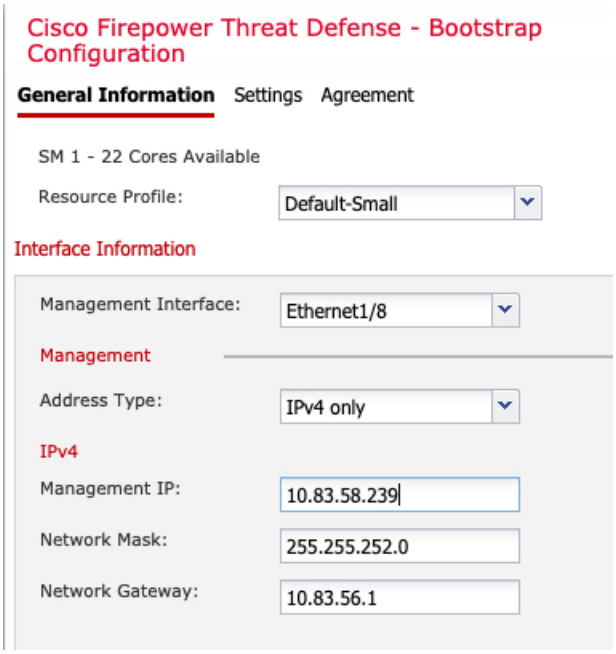
コンテナ インスタンスごとに最大 10 のデータ共有インターフェイスを割り当てることができます。また、各データ共有インターフェイスは、最大 14 個のコンテナ インスタンスに割り当てることができます。データ共有インターフェイスは[Sharing]アイコン（）で示されます。

ハードウェアバイパス対応のポートは次のアイコンで表示されます：。特定のインターフェイス モジュールでは、インライン セット インターフェイスに対してのみハードウェア バイパス機能を有効にできます（インライン セットの詳細については、『FMC configuration guide』を参照）。ハードウェア バイパスは、停電時にトラフィックがインライン インターフェイス ペア間で流れ続けることを確認します。この機能は、ソフトウェアまたはハードウェア障害の発生時にネットワーク接続を維持するために使用できます。ハードウェアバイパス ペアの両方のインターフェイスとも割り当てられていない場合、割り当てが意図的であることを確認する警告メッセージが表示されます。ハードウェアバイパス機能を使用する必要はないため、単一のインターフェイスを割り当てることができます。

ステップ 4 画面中央のデバイス アイコンをクリックします。

ダイアログボックスが表示され、初期のブートストラップ設定を行うことができます。これらの設定は、初期導入専用、またはディザスタ リカバリ用です。通常の運用では、後でアプリケーション CCLI 設定のほとんどの値を変更できます。

ステップ 5 [General Information] ページで、次の手順を実行します。



a) コンテナのインスタンスでは、**リソースのプロファイル**を指定します。

後で異なるリソースプロファイルを割り当てると、インスタンスがリロードされ、約 5 分かかることがあります。確立されたハイアベイラビリティペアまたはクラスタの場合に、異なるサイズのリソースプロファイルを割り当てるときは、すべてのメンバのサイズが同じであることをできるだけ早く確認してください。

b) [Management Interface] を選択します。

このインターフェイスは、論理デバイスの管理に使用されます。このインターフェイスは、シャーシ管理ポートとは別のものです。

c) 管理インターフェイスを選択します。[Address Type]、[IPv4 only]、[IPv6 only]、または [IPv4 and IPv6]。

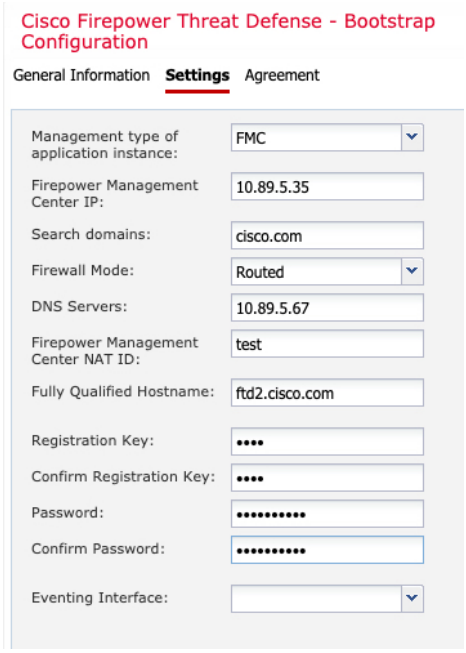
d) [Management IP] アドレスを設定します。

このインターフェイスに一意の IP アドレスを設定します。

e) [Network Mask] または [Prefix Length] に入力します。

f) **ネットワーク ゲートウェイ** アドレスを入力します。

ステップ 6 [設定（Settings）] タブで、次の項目を入力します。



a) ネイティブ インスタンスの場合は、[アプリケーションインスタンスの管理タイプ（Management type of application instance）] ドロップダウン リストで [FMC] を選択します。

ネイティブインスタンスは、マネージャとしての FDM もサポートしています。論理デバイスの展開後に、マネージャタイプの変更はできません。

b) 管理 FMC の [Firepower Management Center IP] を入力します。FMC の IP アドレスがわからない場合は、このフィールドを空白のままにして、[Firepower Management Center NAT ID] フィールドにパスフレーズを入力します。

c) コンテナ インスタンスに対して、**FTD SSH セッションでエキスパート モードを許可するかどうかを** [Yes] または [No] で指定します。エキスパート モードでは、高度なトラブルシューティングに FTD シェルからアクセスできます。

このオプションで [はい（Yes）] を選択すると、SSH セッションからコンテナインスタンスに直接アクセスするユーザがエキスパートモードを開始できます。[いいえ（No）] を選択すると、FXOS CLI からコンテナインスタンスにアクセスするユーザのみがエキスパートモードを開始できます。インスタンス間の分離を増やすには、[いいえ（No）] を選択することをお勧めします。

マニュアルの手順で求められた場合、または Cisco Technical Assistance Center から求められた場合のみ、エキスパート モードを使用します。このモードを開始するには、FTD CLI で **expert** コマンドを使用します。

d) カンマ区切りリストとして [検索ドメイン（Search Domains）] を入力します。

e) [Firewall Mode] を [Transparen] または [Routed] に選択します。

ルーテッド モードでは、FTDはネットワーク内のルータ ホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。一方、トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォー

ル」のように機能するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。

ファイアウォールモードは初期展開時にのみ設定します。ブートストラップの設定を再適用する場合、この設定は使用されません。

f) [DNS Servers] をカンマ区切りのリストとして入力します。

たとえば、FMCのホスト名を指定する場合、FTDは DNS を使用します。

g) FTD の [Fully Qualified Hostname] を入力します。

h) 登録時に FMC とデバイス間で共有する [Registration Key] を入力します。

このキーには、1 ～ 37 文字の任意のテキスト文字列を選択できます。FTD を追加するときに、FMC に同じキーを入力します。

i) CLI アクセス用の FTD 管理ユーザの [Password] を入力します。

j) Firepower イベントの送信に使用する [Eventing Interface] を選択します。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。

このインターフェイスは、Firepower-eventing インターフェイスとして定義する必要があります。

k) コンテナインスタンスの場合は、[ハードウェア暗号化（Hardware Crypto）] を [有効（Enabled）] または [無効（Disabled）] に設定します。

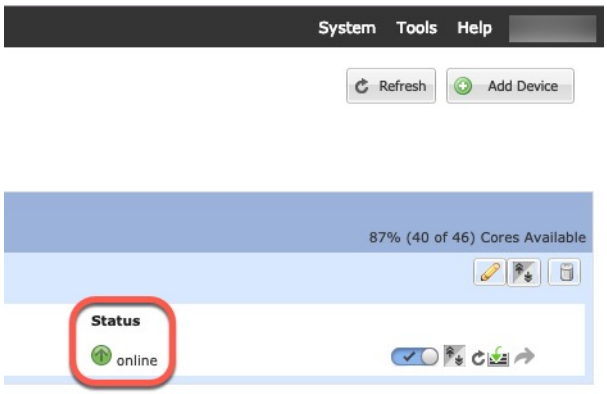
この設定により、ハードウェアの TLS 暗号化アクセラレーションが有効になり、特定タイプのトラフィックのパフォーマンスが向上します。詳細については、FMC のコンフィギュレーション ガイドを参照してください。この機能はネイティブ インスタンスではサポートされていません。このインスタンスに割り当てられているハードウェア暗号化リソースの割合を表示するには、**show hw-crypto** コマンドを入力します。

ステップ 7 [Agreement] タブで、エンド ユーザ ライセンス（EULA）を読んで、同意します。

ステップ 8 [OK] をクリックして、設定ダイアログボックスを閉じます。

ステップ 9 **[保存（Save）]** をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。[**論理デバイス（Logical Devices）**] ページで、新しい論理デバイスのステータスを確認します。論理デバイスの [Status] が [online] と表示されたら、アプリケーションでセキュリティ ポリシーの設定を開始できます。



Firepower Management Center へのログイン

FMC を使用して、 FTD を設定および監視します。

始める前に

サポートされているブラウザの詳細については、使用するバージョンのリリースノート（https://www.cisco.com/go/firepower-notes）を参照してください。

手順

ステップ 1 サポートされているブラウザを使用して、次の URL を入力します。

https://*fmc_ip_address*

ステップ 2 ユーザ名とパスワードを入力します。

ステップ 3 [ログイン（Log In）] をクリックします。

Firepower Management Center のライセンス取得

すべてのライセンスは、FMC によって FTD に提供されます。オプションで、次の機能ライセンスを購入できます。

- **脅威**：セキュリティ インテリジェンスと Cisco Firepower の次世代 IPS
- **マルウェア**：強化されたネットワーク向けの高度なマルウェア防御（AMP）
- **URL**：URL フィルタリング
- **RA VPN**：AnyConnect Plus、AnyConnect Apex、または AnyConnect VPN 専用。

上記のライセンスに加えて、1、3、または5年のアップデートにアクセスするため、該当するサブスクリプションを購入する必要もあります。

始める前に

- Cisco Smart Software Manager にマスター アカウントを持ちます。

  まだアカウントをお持ちでない場合は、リンクをクリックして新しいアカウントを設定してください。Smart Software Manager では、組織のマスター アカウントを作成できます。

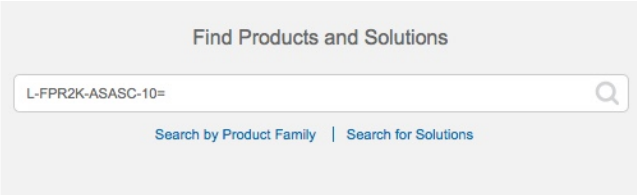
- （輸出コンプライアンスフラグを使用して有効化される）機能を使用するには、ご使用のシスコ スマート ソフトウェア ライセンシング アカウントで強力な暗号化（3DES/AES）ライセンスを使用できる必要があります。

手順

ステップ 1 お使いのスマート ライセンシング アカウントに、必要なライセンスが含まれていることを確認してください。

ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマート ソフトウェア ライセンシング アカウントにリンクされています。ただし、主導でライセンスを追加する必要がある場合は、Cisco Commerce Workspace で [製品とソリューションの検索（Find Products and Solutions）] 検索フィールドを使用します。次のライセンス PID を検索します。

図 *1*: ライセンス検索



（注） PID が見つからない場合は、注文に手動で PID を追加できます。

- 脅威、マルウェア、および URL ライセンスの組み合わせ：
  - L-FPR4110T-TMC=
  - L-FPR4120T-TMC=
  - L-FPR4140T-TMC=
  - L-FPR4150T-TMC=
- 脅威、マルウェア、および URL サブスクリプションの組み合わせ：
  - L-FPR4110T-TMC-1Y
  - L-FPR4110T-TMC-3Y
  - L-FPR4110T-TMC-5Y

- L-FPR4120T-TMC-1Y
- L-FPR4120T-TMC-3Y
- L-FPR4120T-TMC-5Y
- L-FPR4140T-TMC-1Y
- L-FPR4140T-TMC-3Y
- L-FPR4140T-TMC-5Y
- L-FPR4150T-TMC-1Y
- L-FPR4150T-TMC-3Y
- L-FPR4150T-TMC-5Y

- RA VPN：『Cisco AnyConnect Ordering Guide』を参照してください。

ステップ 2 まだ設定していない場合は、スマート ライセンシング サーバに FMC を登録します。

登録を行うには、Smart Software Manager で登録トークンを生成する必要があります。詳細については、『FMC configuration guide』を参照してください。

Firepower Management Center を使用した Firepower Threat Defense の登録

各論理デバイスを同じ FMC に個別に登録します。

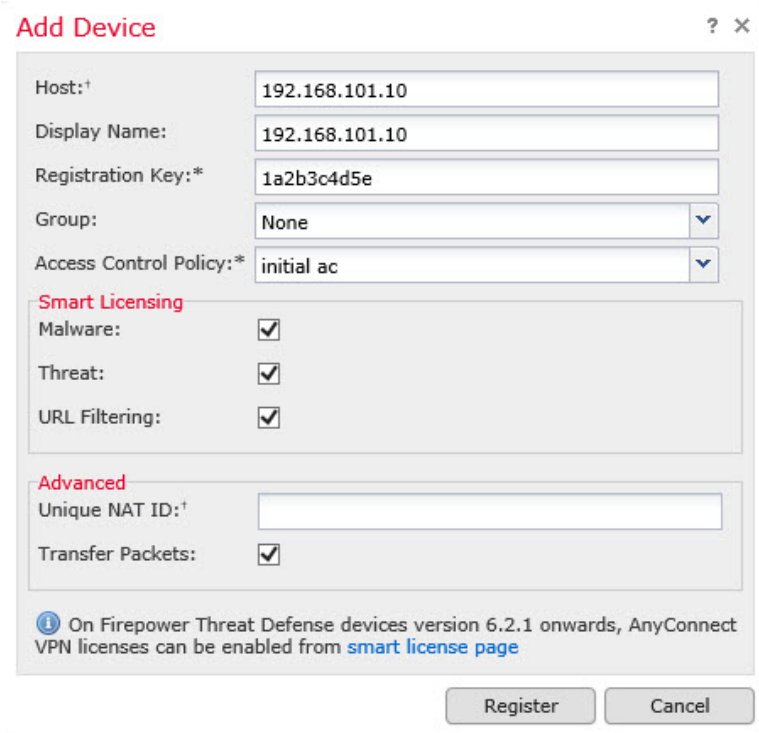
始める前に

- Firepower Chassis Managerの [論理デバイス（Logical Devices）] ページで、FTD 論理デバイスの [ステータス（Status）] が [オンライン（online）] であることを確認します。
- FTD の最初のブートストラップ設定で設定した次の情報を収集します（Firepower Chassis Manager：Firepower Threat Defense 論理デバイスを追加します。 （4 ページ） を参照）。
  - FTD 管理 IP アドレスまたは NAT ID
  - FMC 登録キー

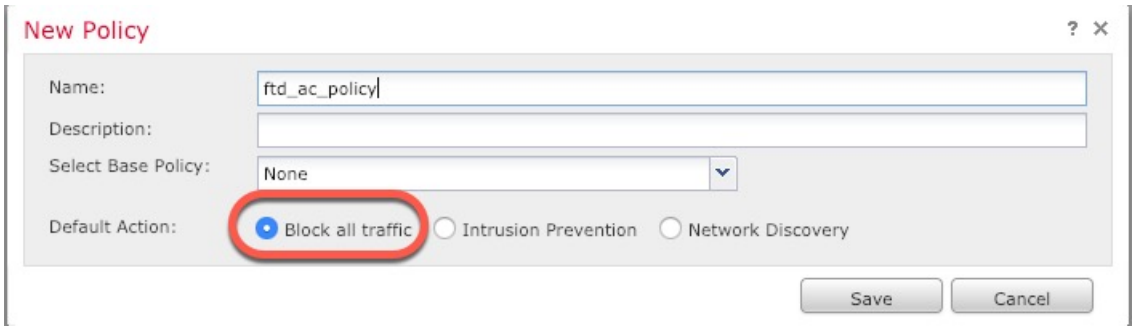
手順

ステップ 1 FMC で、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択します。

ステップ 2 [追加（Add）] ドロップダウンリストから、[デバイスの追加（Add Device）] を選択し、次のパラメータを入力します。



- [ホスト（Host）]：追加する FTD の IP アドレスを入力します。FTD の最初のブートストラップ設定で FMC の IP アドレスと NAT ID の両方を指定した場合は、このフィールドを空のままにしておくことができます。
- [表示名（Display Name）] フィールドに、FMC に表示する FTD の名前を入力します。
- [登録キー（Registration key）]：FTD の最初のブートストラップ設定で指定したものと同じ登録キーを入力します。
- [ドメイン（Domain）]：マルチドメイン環境を使用している場合は、デバイスをリーフドメインに割り当てます。
- [グループ（Group）]：グループを使用している場合は、デバイスグループに割り当てます。
- [アクセスコントロールポリシー（Access Control Policy）]：初期ポリシーを選択します。使用する必要があることがわかっているカスタマイズ済みのポリシーがすでにある場合を除いて、[新しいポリシーの作成（Create new policy）] を選択し、[すべてのトラフィックをブロック（Block all traffic）] を選択します。後でこれを変更してトラフィックを許可することができます。「内部から外部へのトラフィックの許可 （24 ページ）」を参照してください。



- [スマートライセンス（Smart Licensing）]：展開する機能に必要なスマートライセンスとして、[マルウェア（Malware）]（AMP マルウェアインスペクションを使用する予定の場合）、[脅威（Threat）]（侵入防御を使用する予定の場合）、および[URL]（カテゴリベースの URL フィルタリングを実装する予定の場合）を割り当てます。
- [一意の NAT ID（Unique NAT ID）]：FTD の最初のブートストラップ設定で指定した NAT ID を指定します。
- [パケットの転送（Transfer Packets）]：デバイスから FMC へのパケット転送を許可します。このオプションを有効にして IPS や Snort などのイベントがトリガーされた場合は、デバイスが検査用としてイベントメタデータ情報とパケットデータを FMC に送信します。このオプションを無効にした場合は、イベント情報だけが FMC に送信され、パケットデータは送信されません。

ステップ 3 [登録（Register）] をクリックし、正常に登録されたことを確認します。

登録が成功すると、デバイスがリストに追加されます。失敗した場合は、エラーメッセージが表示されます。FTD が登録に失敗した場合は、次の項目を確認してください。

- ping：FTD CLI（Firepower Threat Defense CLI へのアクセス （26 ページ））にアクセスし、次のコマンドを使用して FMC IP アドレスへの ping を実行します。

  ping system *ip_address*

  ping が成功しない場合は、**show network** コマンドを使用してネットワーク設定を確認します。FTD IP アドレスを変更する必要がある場合は、**configure network** {**ipv4** | **ipv6**} **manual** コマンドを実行します。

- NTP：Firepower 4100 NTP サーバが **[システム（System）]** > **[設定（Configuration）]** > **[時刻の同期（Time Synchronization）]** ページの FMC サーバ セットと一致することを確認します。
- 登録キー、NAT ID、および FMC IP アドレス：両方のデバイスで同じ登録キーを使用していることを確認し、使用している場合は NAT ID を使用していることを確認します。**configure manager add** コマンドを使用して、FTD で登録キーと NAT ID を設定することができます。また、このコマンドで FMC IP アドレスを変更することもできます。

基本的なセキュリティポリシーの設定

ここでは、次の設定を使用して基本的なセキュリティポリシーを設定する方法について説明します。

- 内部インターフェイスと外部インターフェイス：内部インターフェイスにスタティック IP アドレスを割り当て、外部インターフェイスに DHCP を使用します。
- DHCP サーバ：クライアントの内部インターフェイスで DHCP サーバを使用します。
- デフォルトルート：外部インターフェイスを介してデフォルトルートを追加します。
- NAT：外部インターフェイスでインターフェイス PAT を使用します。
- アクセスコントロール：内部から外部へのトラフィックを許可します。

基本的なセキュリティ ポリシーを設定するには、次のタスクを実行します。

1	インターフェイスの設定 （15 ページ）。
2	DHCP サーバの設定 （19 ページ）。
3	デフォルトルートの追加 （20 ページ）。
4	NAT の設定 （21 ページ）。
5	内部から外部へのトラフィックの許可 （24 ページ）。
6	設定の展開 （25 ページ）。

インターフェイスの設定

FTD インターフェイスを有効にし、それらをセキュリティゾーンに割り当て、IP アドレスを設定します。通常は、システムで意味のあるトラフィックを通過させるように、少なくとも 2 つのインターフェイスを設定する必要があります。通常は、アップストリームルータまたはインターネットに面した外部インターフェイスと、組織のネットワークの 1 つ以上の内部インターフェイスを使用します。これらのインターフェイスの一部は、Web サーバなどのパブリックアクセスが可能なアセットを配置する「緩衝地帯」（DMZ）となる場合があります。

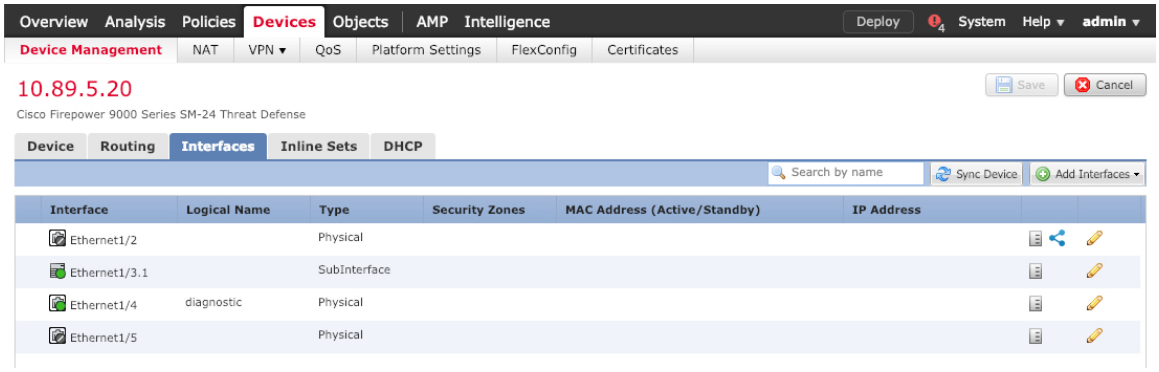
一般的なエッジルーティングの状況は、内部インターフェイスでスタティックアドレスを定義すると同時に、ISP から DHCP を介して外部インターフェイスアドレスを取得することです。

次の例では、DHCP によるスタティックアドレスとルーテッドモードの外部インターフェイスを使用して、ルーテッドモードの内部インターフェイスを設定します。

手順

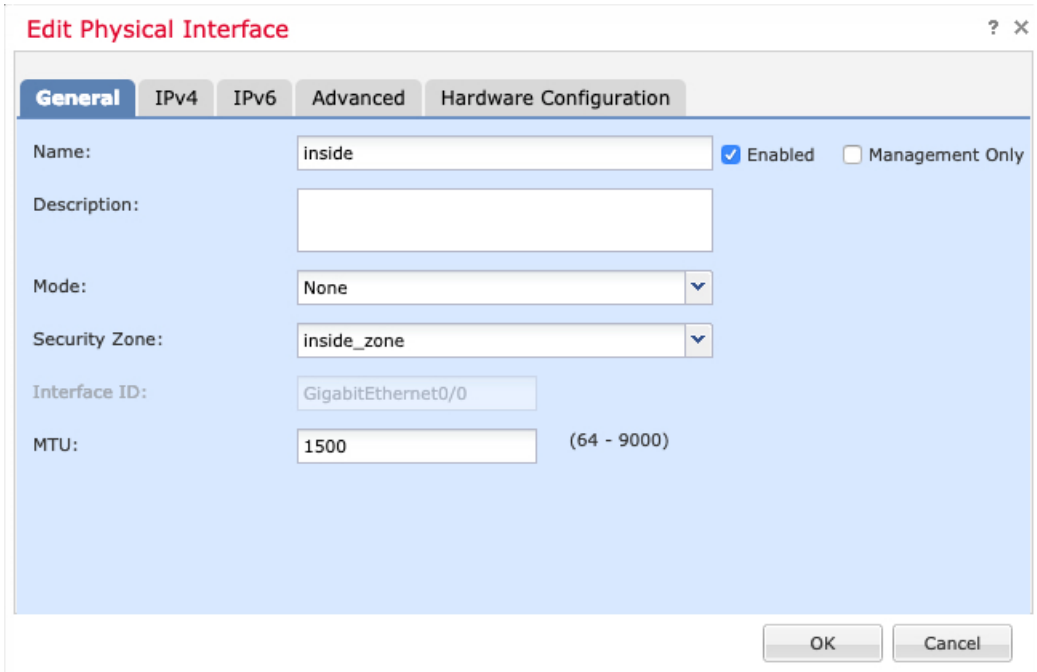
ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、デバイスの [Edit] アイコン（✎）をクリックします。

ステップ 2 [インターフェイス（Interfaces）] をクリックします。



ステップ 3 「内部」に使用するインターフェイスの [Edit] アイコン（✎）をクリックします。

[全般（General）] タブが表示されます。



a) 48 文字までの [名前（Name）] を入力します。

たとえば、インターフェイスに **inside** という名前を付けます。

b) [有効（Enabled）] チェックボックスをオンにします。

c) [モード（Mode）] は [なし（None）] に設定したままにします。

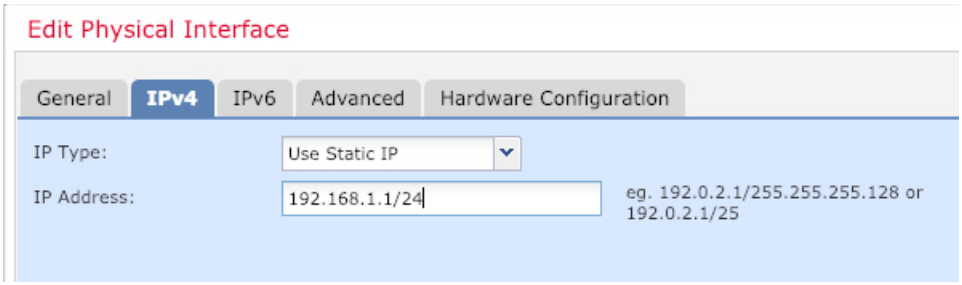
d) [セキュリティゾーン（Security Zone）] ドロップダウンリストから既存の内部セキュリティゾーンを選択するか、[新規（New）] をクリックして新しいセキュリティゾーンを追加します。

たとえば、**inside_zone** という名前のゾーンを追加します。各インターフェイスは、セキュリティゾーンおよびインターフェイスグループに割り当てる必要があります。インターフェイスは、1 つのセキュリティゾーンにのみ属することも、複数のインターフェイスグループに属することもできます。ゾーンまたはグループに基づいてセキュリティポリシーを適用します。たとえば、内部インターフェイスを内部ゾーンに割り当て、外部インターフェイスを外部ゾーンに割り当てることができます。この場合、トラフィックが内部から外部に移動できるようにアクセス コントロール ポリシーを設定することはできますが、外部から内部に向けては設定できません。ほとんどのポリシーはセキュリティゾーンのみサポートしています。NAT ポリシー、プレフィルタ ポリシー、および QoS ポリシーで、ゾーンまたはインターフェイスグループを使用できます。

e) [IPv4] タブ、[IPv6] タブ、または両方のタブをクリックします。

- [IPv4]：ドロップダウンリストから [スタティックIPを使用する（Use Static IP）] を選択し、IP アドレスとサブネットマスクをスラッシュ表記で入力します。

  たとえば、**192.168.1.1/24** などと入力します。

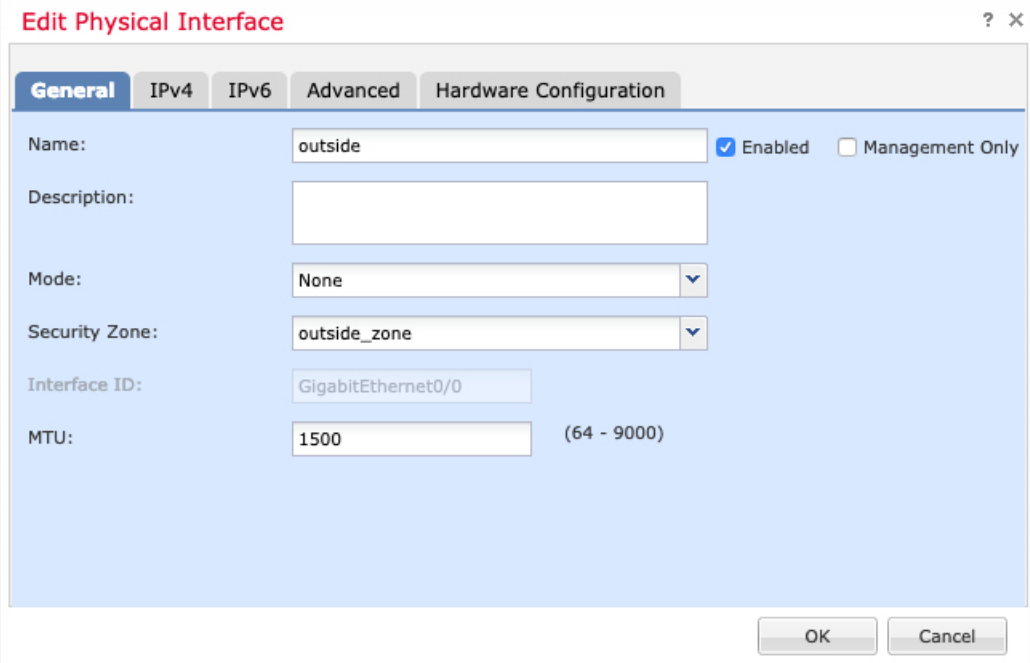


- [IPv6]：ステートレス自動設定の場合は [自動設定（Autoconfiguration）] チェックボックスをオンにします。

f) [OK] をクリックします。

ステップ 4 「外部」に使用するインターフェイスの [Edit] アイコン（）をクリックします。

[全般（General）] タブが表示されます。



a) 48 文字までの [名前（Name）] を入力します。

たとえば、インターフェイスに「outside」という名前を付けます。

b) [有効（Enabled）] チェックボックスをオンにします。

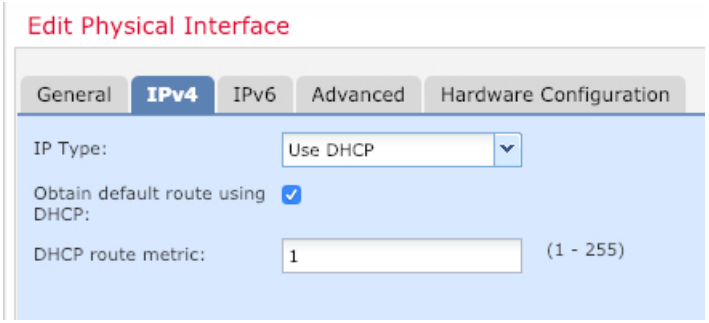
c) [モード（Mode）] は [なし（None）] に設定したままにします。

d) [セキュリティゾーン（Security Zone）] ドロップダウンリストから既存の外部セキュリティゾーンを選択するか、[新規（New）] をクリックして新しいセキュリティゾーンを追加します。

たとえば、「outside_zone」という名前のゾーンを追加します。

e) [IPv4] タブ、[IPv6] タブ、または両方のタブをクリックします。

- [IPv4]：[DHCPの使用（Use DHCP）] を選択し、次のオプションのパラメータを設定します。
  - [DHCP を使用してデフォルト ルートを取得（Obtain default route using DHCP）]：DHCP サーバからデフォルト ルートを取得します。
  - [DHCP ルートメトリック（DHCP route metric）]：アドミニストレーティブ ディスタンスを学習したルートに割り当てます（1～255）。学習したルートのデフォルトのアドミニストレーティブ ディスタンスは 1 です。



- [IPv6]：ステートレス自動設定の場合は [自動設定（Autoconfiguration）] チェックボックスをオンにします。

f) [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックします。

DHCP サーバの設定

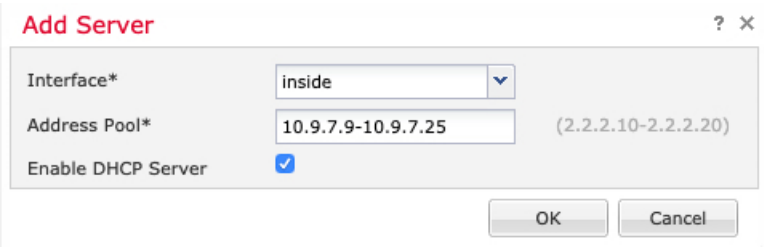
クライアントで DHCP を使用して FTD から IP アドレスを取得するようにする場合は、DHCP サーバを有効にします。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、デバイスの [Edit] アイコン（✎）をクリックします。

ステップ 2 **[DHCP] > [DHCPサーバ（DHCP Server）]** を選択します。

ステップ 3 **[サーバ（Server）]** ページで、**[追加（Add）]** をクリックして、次のオプションを設定します。



- [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。
- [アドレスプール（Address Pool）]：DHCP サーバが使用する IP アドレスの最下位から最上位の間の範囲を設定します。IP アドレスの範囲は、選択したインターフェイスと同じサブネット上に存在する必要があり、インターフェイス自身の IP アドレスを含めることはできません。

- [DHCPサーバを有効にする（Enable DHCP Server）]：選択したインターフェイスの DHCP サーバを有効にします。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックします。

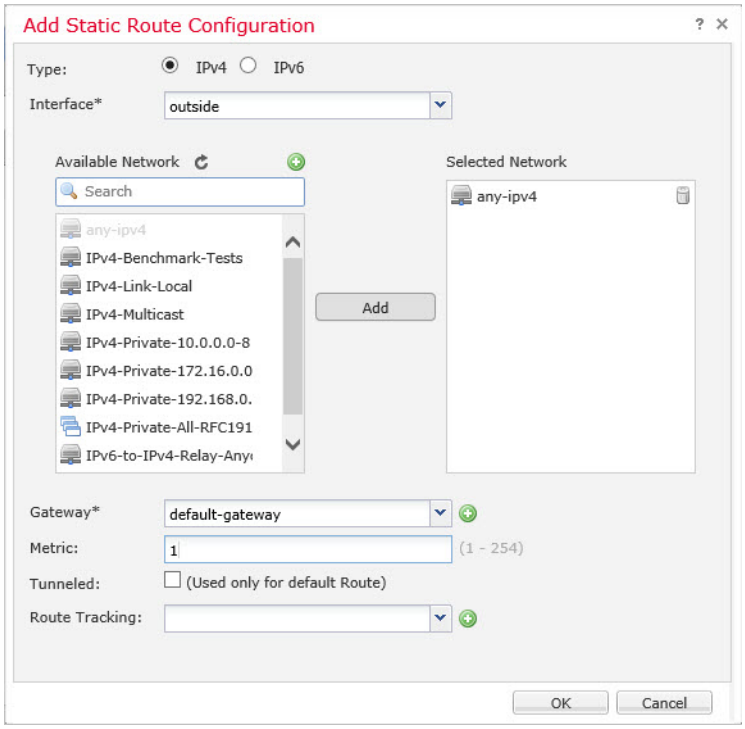
デフォルトルートの追加

デフォルトルートは通常、外部インターフェイスから到達可能なアップストリームルータを指し示します。外部インターフェイスにDHCPを使用する場合は、デバイスがすでにデフォルトルートを受信している可能性があります。手動でルートを追加する必要がある場合は、次の手順を実行します。DHCPサーバからデフォルトルートを受信した場合は、**[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）]** ページの **[IPv4ルート（IPv4 Routes）]** または **[IPv6ルート（IPv6 Routes）]** テーブルに表示されます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、デバイスの [Edit] アイコン（✎）をクリックします。

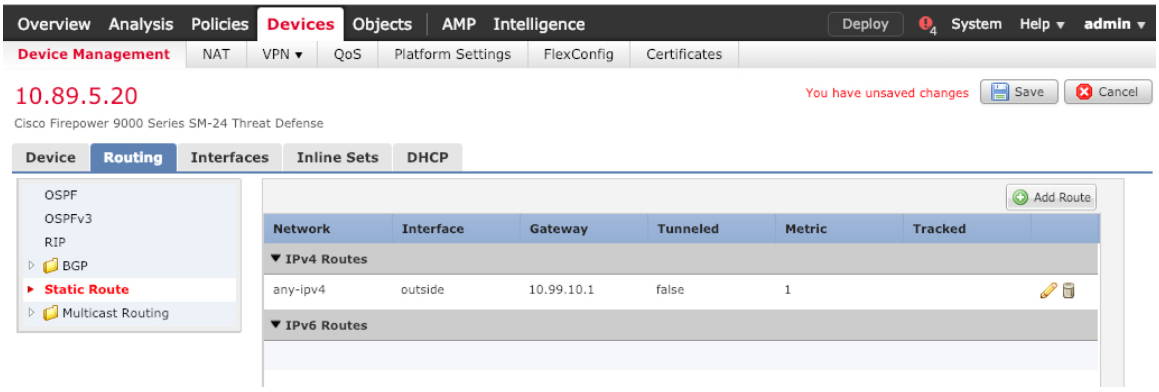
ステップ 2 **[ルーティング（Routing）]** > **[スタティックルート（Static route）]** を選択し、[ルートを追加（Add route）] をクリックして、次のように設定します。



- [タイプ（Type）]：追加するスタティックルートのタイプに応じて、[IPv4] または [IPv6] オプションボタンをクリックします。
- [インターフェイス（Interface）]：出力インターフェイスを選択します。通常は外部インターフェイスです。
- [使用可能なネットワーク（Available Network）]：IPv4 デフォルト ルートの場合は [ipv4] を選択し、IPv6 デフォルト ルートの場合は [any] を選択し、[追加（Add）] をクリックして [選択したネットワーク（Selected Network）] リストに移動させます。
- [ゲートウェイ（Gateway）] または [IPv6ゲートウェイ（IPv6 Gateway）]：このルートのネクストホップであるゲートウェイルータを入力または選択します。IP アドレスまたはネットワーク/ホストオブジェクトを指定できます。
- [メトリック（Metric）]：宛先ネットワークへのホップの数を入力します。有効値の範囲は 1 ～ 255 で、デフォルト値は 1 です。

ステップ 3 [OK] をクリックします。

ルートがスタティックルートテーブルに追加されます。



ステップ 4 [保存（Save）] をクリックします。

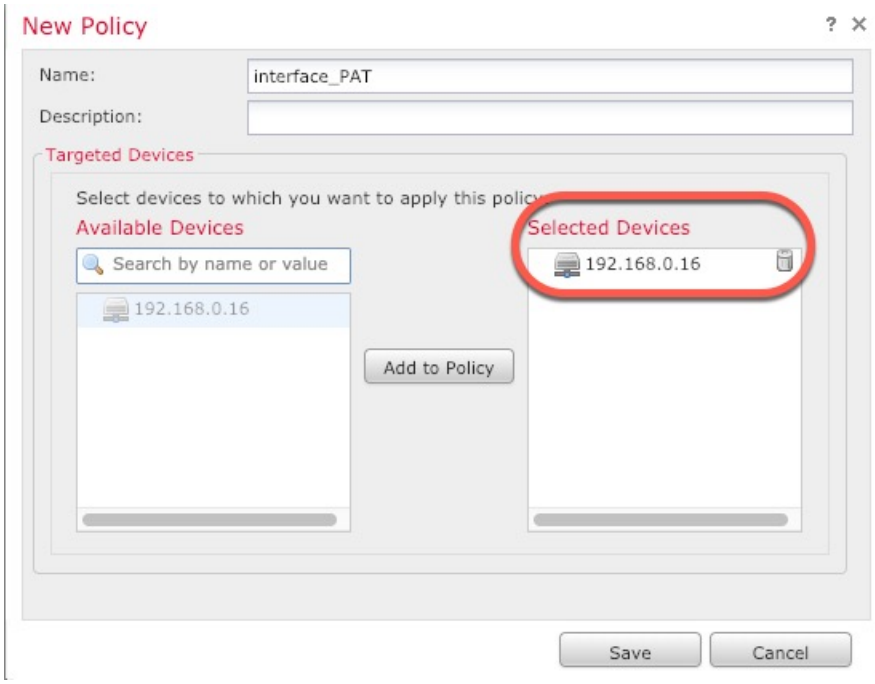
NAT の設定

一般的な NAT ルールでは、内部アドレスを外部インターフェイスの IP アドレスのポートに変換します。このタイプの NAT ルールのことをインターフェイス ポート アドレス変換（PAT）と呼びます。

手順

ステップ 1 **[デバイス（Devices）]** > **[NAT]** をクリックし、**[新しいポリシー（New Policy）]** > **[Threat Defense NAT]** をクリックします。

ステップ 2 ポリシーに名前を付け、ポリシーを使用するデバイスを選択し、[保存（Save）] をクリックします。



ポリシーが FMC に追加されます。引き続き、ポリシーにルールを追加する必要があります。

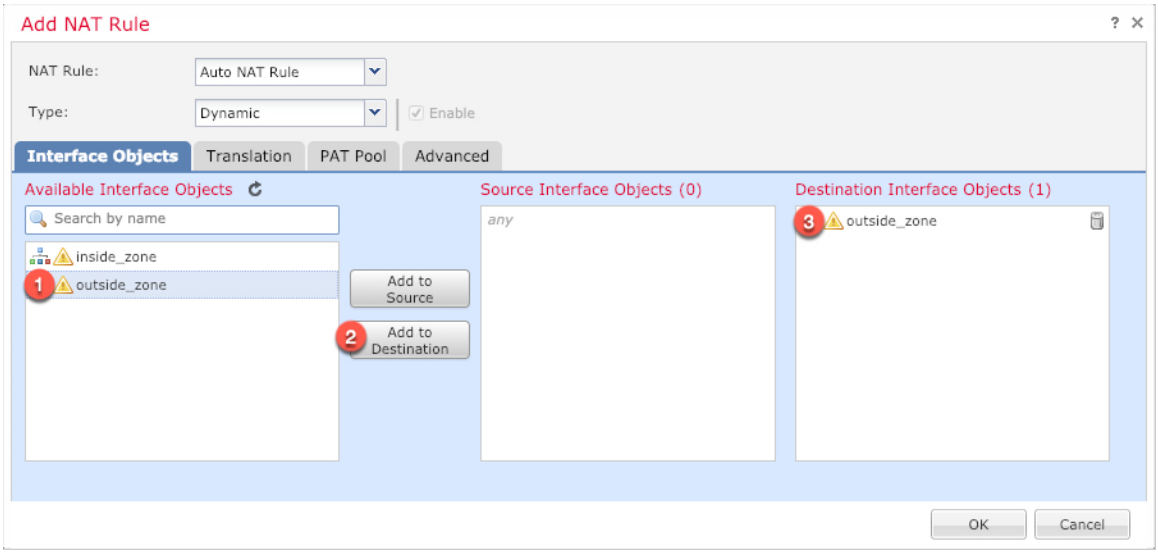
ステップ 3 [ルールの追加（Add Rule）] をクリックします。

[NATルールの追加（Add NAT Rule）] ダイアログボックスが表示されます。

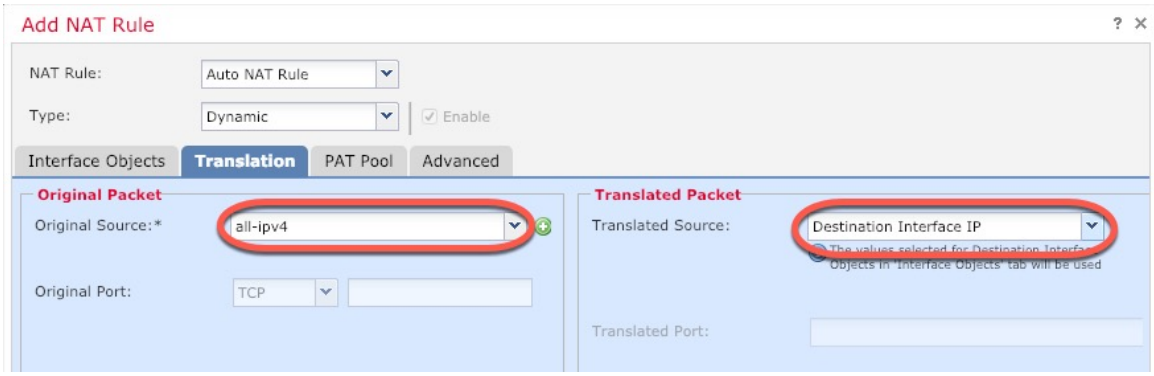
ステップ 4 基本ルールのオプションを設定します。

- [NATルール（NAT Rule）] : [自動NATルール（Auto NAT Rule）] を選択します。
- [タイプ（Type）] : [ダイナミック（Dynamic）] を選択します。

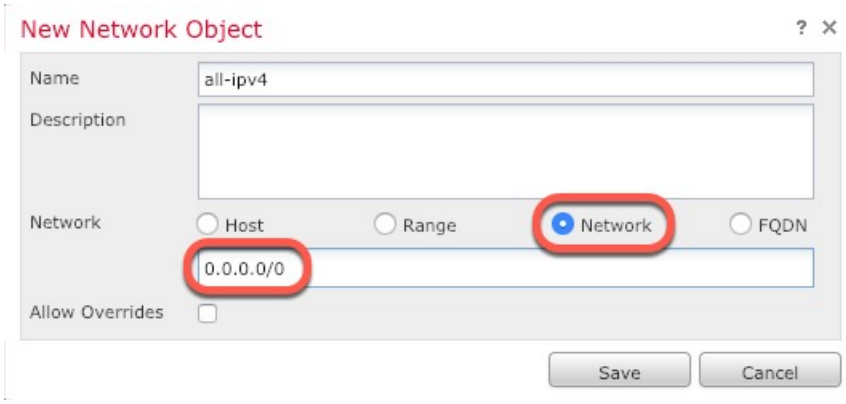
ステップ 5 [インターフェイスオブジェクト（Interface objects）] ページで、[使用可能なインターフェイスオブジェクト（Available Interface Objects）] 領域から [宛先インターフェイスオブジェクト（Destination Interface Objects）] 領域に外部ゾーンを追加します。



ステップ 6 [変換（Translation）] ページで、次のオプションを設定します。



- [元の送信元（Original Source）]：[Add] アイコン（ ）をクリックして、すべての IPv4 トラフィック（0.0.0.0/0）のネットワークオブジェクトを追加します。

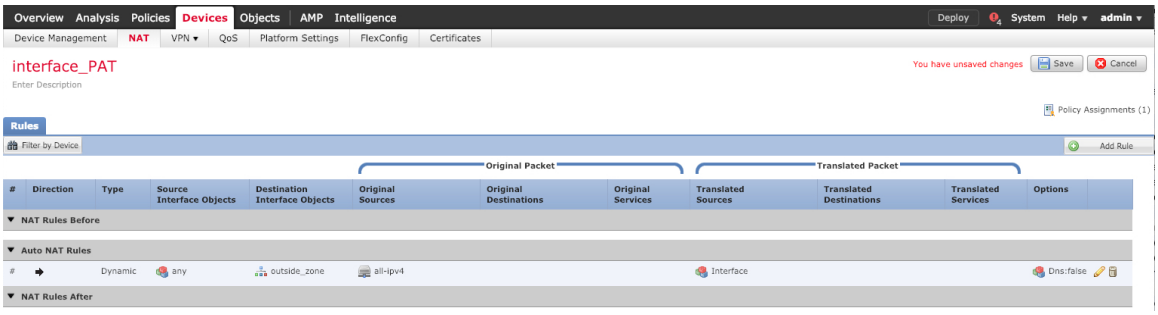


（注） 自動 NAT ルールはオブジェクト定義の一部として NAT を追加するため、システム定義の **any-ipv4** オブジェクトを使用することはできません。また、システム定義のオブジェクトを編集することはできません。

- [変換済みの送信元（Translated Source）]：[宛先インターフェイスIP（Destination Interface IP）] を選択します。

ステップ 7 [保存（Save）] をクリックしてルールを追加します。

ルールが [ルール（Rules）] テーブルに保存されます。



ステップ 8 NAT ページで [保存（Save）] をクリックして変更を保存します。

内部から外部へのトラフィックの許可

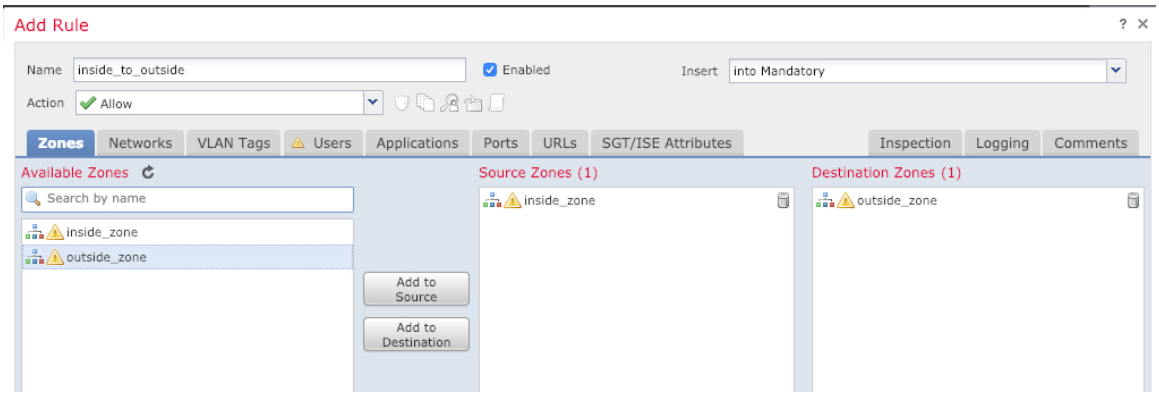
FTD を FMC に登録したときに、基本の [すべてのトラフィックをブロック（Block all traffic）] アクセス コントロール ポリシーを作成した場合は、デバイスを通過するトラフィックを許可するためにポリシーにルールを追加する必要があります。次の手順では、内部ゾーンから外部ゾーンへのトラフィックを許可するルールを追加します。他にゾーンがある場合は、適切なネットワークへのトラフィックを許可するルールを追加してください。

より高度なセキュリティ設定とルールを設定する場合は、『FMC configuration guide』を参照してください。

手順

ステップ 1 **[ポリシー（Policy）] > [アクセスポリシー（Access Policy）] > [アクセスポリシー（Access Policy）]** を選択し、FTD に割り当てられているアクセス コントロール ポリシーの [Edit] アイコン（）をクリックします。

ステップ 2 **[ルールを追加（Add Rule）]** をクリックし、次のパラメータを設定します。

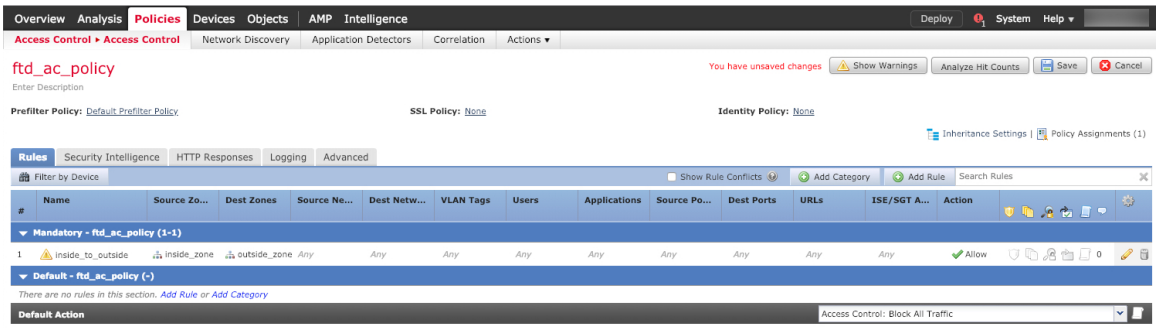


- [名前（Name）]：このルールに名前を付けます（たとえば、**inside_to_outside**）。
- [送信元ゾーン（Source Zones）]：[使用可能なゾーン（Available Zones）] から内部ゾーンを選択し、[送信元に追加（Add to Source）] をクリックします。
- [宛先ゾーン（Destination Zones）]：[使用可能なゾーン（Available Zones）] から外部ゾーンを選択し、[宛先に追加（Add to Destination）] をクリックします。

他の設定はそのままにしておきます。

ステップ 3 [追加（Add）] をクリックします。

ルールが [ルール（Rules）] テーブルに追加されます。



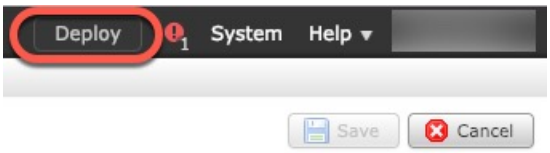
ステップ 4 [保存（Save）] をクリックします。

設定の展開

設定の変更を FTD に展開します。変更を展開するまでは、デバイス上でどの変更もアクティブになりません。

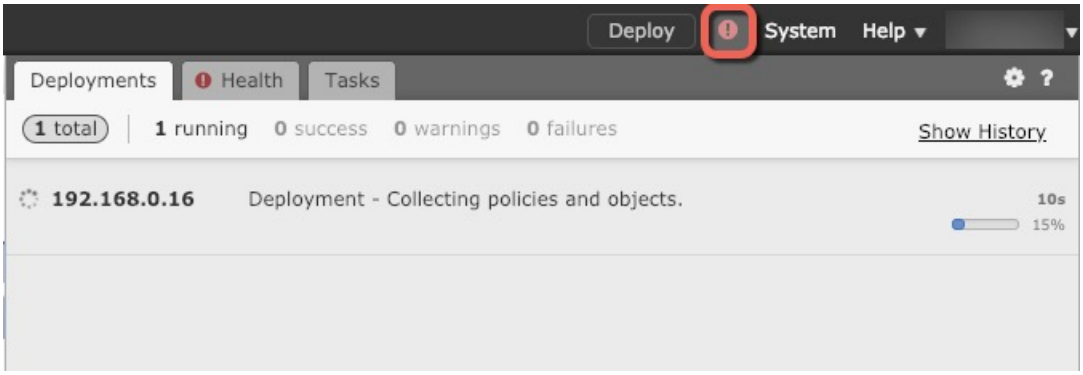
手順

ステップ 1 右上の [展開（Deploy）] をクリックします。



ステップ 2 [ポリシーの展開（Deploy Policies）] ダイアログボックスでデバイスを選択し、[展開（Deploy）] をクリックします。

ステップ 3 展開が成功したことを確認します。展開のステータスを表示するには、メニューバーの [展開（Deploy）] ボタンの右側にあるアイコンをクリックします。



Firepower Threat Defense CLI へのアクセス

FTD CLI を使用して、管理インターフェイスパラメータを変更したり、トラブルシューティングを行ったりできます。CLI にアクセスするには、管理インターフェイスへの SSH を使用するか、FXOS CLI から接続します。

手順

ステップ 1 （オプション 1）FTD 管理インターフェイスの IP アドレスに直接 SSH 接続します。

管理 IP アドレスは、論理デバイスを展開したときに設定したものです。初期展開時に設定した「admin」アカウントとパスワードを使用して FTD にログインします。

パスワードを忘れた場合は、Firepower Chassis Manager で論理デバイスを編集して変更できます。

ステップ 2 （オプション 2）コンソール接続または Telnet 接続を使用して、モジュール CLI に接続します。

a) セキュリティ エンジン に接続します。

connect module 1 {**console** | **telnet**}

Telnet 接続を使用する利点は、モジュールに同時に複数のセッションを設定でき、接続速度が速くなることです。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) FTD コンソールに接続します。

connect ftd *name*

複数のアプリケーションインスタンスがある場合は、インスタンスの名前を指定する必要があります。インスタンス名を表示するには、名前を付けずにコマンドを入力します。

例：

```
Firepower-module1> connect ftd FTD_Instance1

============================ ATTENTION ==============================
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
Otherwise, data cached along the pipe may take up to 12 minutes to be
drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use
'connect module <slot> telnet' to connect to the security module.
=====================================================================

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to
bootCLI
>
```

c) **exit** と入力し、アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

（注） 6.3 より前のバージョンの場合は、**Ctrl-a, d** と入力します。

d) FXOS CLI のスーパバイザ レベルに戻ります。

コンソールを終了するには、以下を実行します。

1. ~ と入力

Telnet アプリケーションに切り替わります。

2. Telnet アプリケーションを終了するには、次を入力します。

   telnet>**quit**

Telnet セッションを終了するには、以下を実行します。

Ctrl-], . と入力

例

次に、FTD に接続してから、FXOS CLI のスーパバイザ レベルに戻る例を示します。

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect ftd FTD_Instance1

============================== ATTENTION ==============================
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
Otherwise, data cached along the pipe may take up to 12 minutes to be
drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use
'connect module <slot> telnet' to connect to the security module.
=======================================================================

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to bootCLI
> ~
telnet> quit
Connection closed.
Firepower#
```

次のステップ

FTD の設定を続行するには、Cisco Firepower ドキュメント一覧 でお使いのソフトウェアバージョンのマニュアルを参照してください。

FMC の使用に関する詳細については、『Firepower Management Center Configuration Guide』を参照してください。

FTD と FMC の履歴

機能名	バージョン	機能情報
ASA および FTD を同じ Firepower 9300 の別のモジュールでサポート	6.4	ASA および FTD 論理デバイスを同じ Firepower 9300 上で展開できるようになりました。 （注） FXOS 2.6.1 が必要です。
Firepower 4100/9300 上の Firepower Threat Defense のマルチインスタンス機能	6.3.0	単一のセキュリティ エンジンまたはモジュールに、それぞれ Firepower Threat Defense コンテナインスタンスがある複数の論理デバイスを展開できるようになりました。以前は、単一のネイティブ アプリケーション インスタンスを展開できるだけでした。 柔軟な物理インターフェイスの使用を可能にするため、FXOS で VLAN サブインターフェイスを作成し、複数のインスタンス間でインターフェイスを共有することができます。リソース管理では、各インスタンスのパフォーマンス機能をカスタマイズできます。 2 台の個別のシャーシ上でコンテナ インスタンスを使用して高可用性を使用できます。クラスタリングはサポートされません。 （注） マルチインスタンス機能は、実装は異なりますが、ASA マルチ コンテキスト モードに似ています。マルチ コンテキスト モードは Firepower Threat Defense では利用できません。 新規/変更された [Firepower Management Center] 画面： • **[Devices]** > **[Device Management]** > **[Edit]** アイコン > [Interfaces] タブ 新規/変更された [Firepower Chassis Manager] 画面： • **[概要（Overview）]** > **[デバイス（Devices）]** • **[インターフェイス（Interfaces）]** > **[すべてのインターフェイス（All Interfaces）]** > **[新規追加（Add New）]** ドロップダウン メニュー > [サブインターフェイス（Subinterface）] • **[Interfaces]** > **[All Interfaces]** > **[Type]** • **[論理デバイス（Logical Devices）]** > **[デバイスの追加（Add Device）]** • **[プラットフォームの設定（Platform Settings）]** > **[Macプール（Mac Pool）]** • **[プラットフォームの設定（Platform Settings）]** > **[リソースのプロファイル（Resource Profiles）]**