FMC での FTD の展開

この章の対象読者

使用可能なすべてのオペレーティングシステムとマネージャを確認するには、「最適なオペレーティングシステムとマネージャを見つける方法」を参照してください。この章の内容は、FMC での FTD の展開に適用されます。

この章では、FTD の初期設定の方法と管理ネットワーク上にある FMC へのファイアウォールの登録方法について説明します。FMC が中央の本社にあるリモート支社での展開については、「リモート FTD による FMC の展開」を参照してください。

大規模ネットワークの一般的な導入では、複数の管理対象デバイスがネットワークセグメントにインストールされます。各デバイスは、トラフィックを制御、検査、監視、および分析して、管理 FMC に報告します。FMC は、サービスの管理、分析、レポートのタスクを実行できる Web インターフェイスを備えた集中管理コンソールを提供し、ローカルネットワークを保護します。

ファイアウォールについて

ハードウェアでは、FTD ソフトウェアまたは ASA ソフトウェアを実行できます。FTD と ASA の間で切り替えを行う際には、デバイスの再イメージ化が必要になります。現在インストールされているものとは異なるソフトウェアバージョンが必要な場合も再イメージ化が必要です。「Cisco ASA および Firepower Threat Defense 再イメージ化ガイド」を参照してください。

ファイアウォールは、Firepower eXtensible オペレーティングシステム（FXOS）と呼ばれる基盤となるオペレーティングシステムを実行します。ファイアウォールは FXOS Firepower Chassis Manager をサポートしていません。トラブルシューティング用として限られた CLI のみがサポートされています。詳細については、Cisco FXOS トラブルシューティングガイド（Firepower Threat Defense を実行している Firepower 1000/2100 シリーズ向け）を参照してください。

プライバシー収集ステートメント：ファイアウォール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、ユーザー名などの設定では、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。

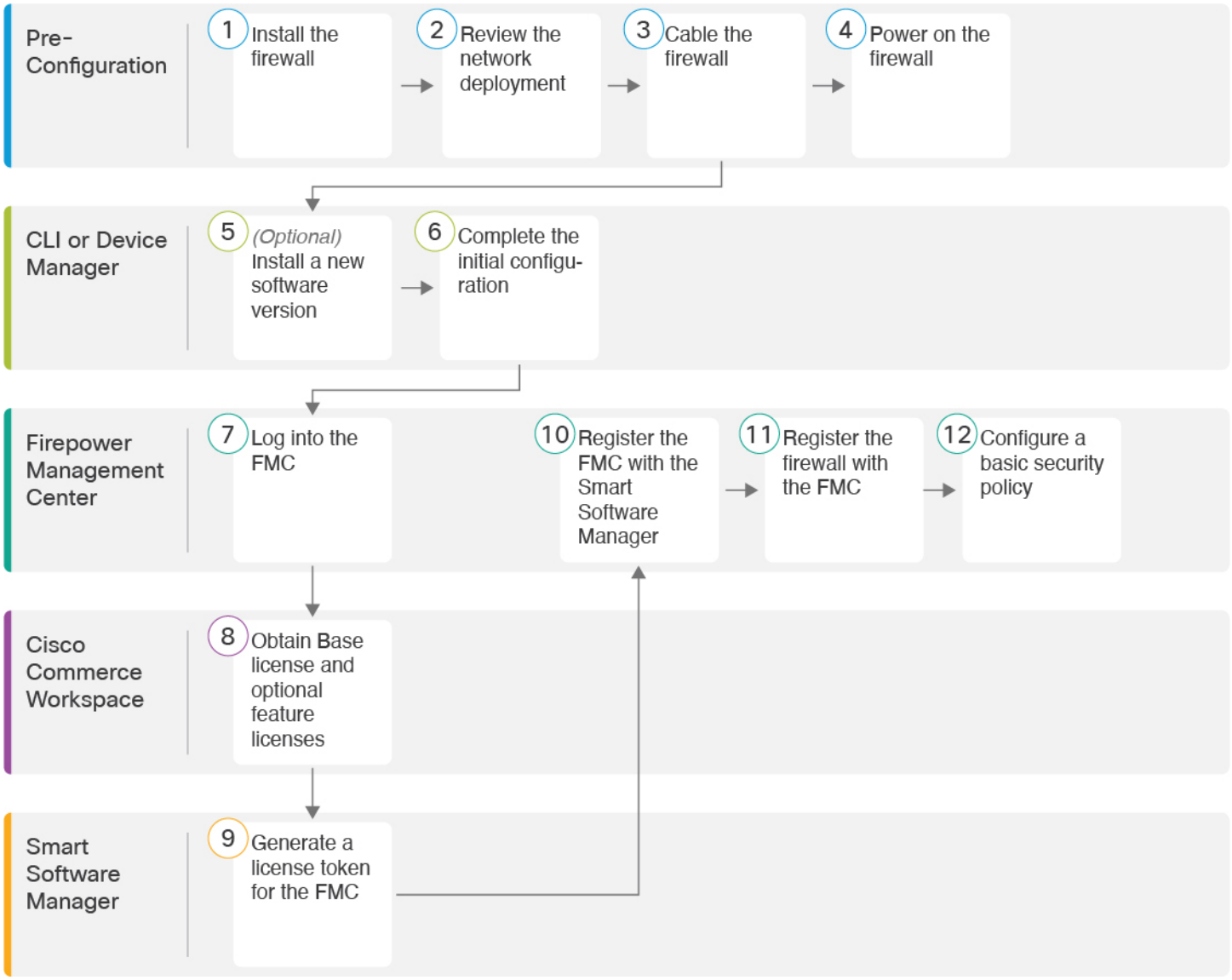
はじめる前に

FMC の初期設定を展開して実行します。Cisco Firepower Management Center 1600, 2600, and 4600 Hardware Installation Guideを参照してください。

エンドツーエンドの手順

シャーシで FMC を使用して FTD を展開するには、次のタスクを参照してください。

図 *1*: エンドツーエンドの手順



1	事前設定	ファイアウォールをインストールします。ハードウェア設置ガイドを参照してください。
2	事前設定	ネットワーク展開の確認 （4 ページ）。
3	事前設定	ファイアウォールのケーブル接続 （6 ページ）。
4	事前設定	ファイアウォールの電源を入れます （8 ページ）。
5	CLI	（任意）ソフトウェアの確認と新しいバージョンのインストール （10 ページ）。

6	CLI または FDM	FTD の初期設定の完了 （11 ページ）。
7	FMC	へのログインFMC （21 ページ）。
8	Cisco Commerce Workspace	基本ライセンスとオプションの機能ライセンスを購入します（「FMC のライセンスの取得 （21 ページ）」）。
9	Smart Software Manager	FMC のライセンストークンを生成します（「FMC のライセンスの取得 （21 ページ）」）。
10	FMC	スマート ライセンシング サーバーに FMC を登録します（「FMC のライセンスの取得 （21 ページ）」）。
11	FMC	FMC への FTD の登録 （23 ページ）。
12	FMC	基本的なセキュリティポリシーの設定 （26 ページ）。

ネットワーク展開の確認

専用の Management 1/1 インターフェイスは、独自のネットワーク設定を持つ特別なインターフェイスです。デフォルトでは、Management 1/1 インターフェイスは有効になっていて、DHCP クライアントとして設定されています。ネットワークに DHCP サーバーが含まれていない場合は、コンソールポートで初期設定時に静的 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できます。FTD を FMC に接続した後、他のインターフェイスを設定できます。

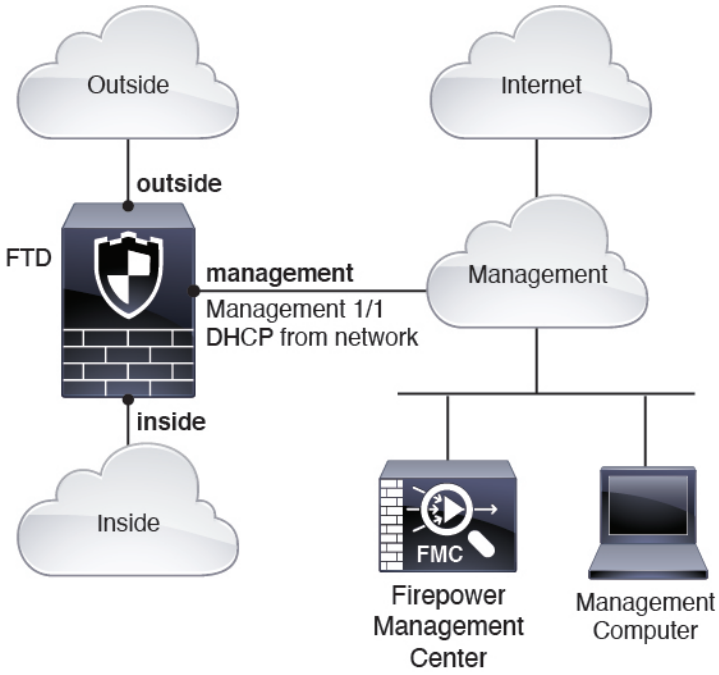
ネットワークに FTD デバイスを配置する方法については、次のネットワークへの展開例を参照してください。

個別の管理ネットワーク

FMC と FTD の両方で、ライセンシングと更新を行うには管理からのインターネットアクセスが必要です。

次の図に、FMC と管理コンピュータが管理ネットワークに接続している Cisco Secure Firewall 3100 について考えられるネットワーク展開を示します。管理ネットワークには、ライセンシングと更新のためのインターネットへのパスがあります。

図 *2 :* 個別の管理ネットワーク



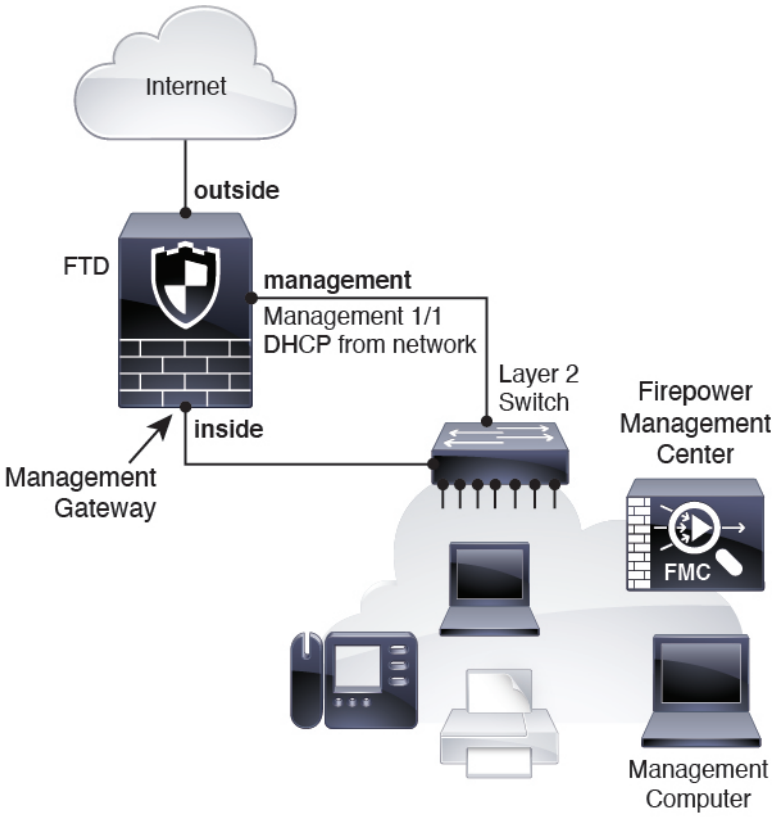
エッジ ネットワークの展開

FMC と FTD の両方で、ライセンシングと更新を行うには管理からのインターネットアクセスが必要です。

次の図に、Cisco Secure Firewall 3100 が FMC と FTD の管理用のインターネットゲートウェイとして機能する Cisco Secure Firewall 3100 について考えられるネットワーク展開を示します。

次の図では、Management 1/1 をレイヤ 2 スイッチを介して内部のインターフェイスに接続するとともに、FMC と管理コンピュータをスイッチに接続することにより、Cisco Secure Firewall 3100 が管理インターフェイスと FMC のインターネットゲートウェイとして機能しています（管理インターフェイスは FTD 上の他のインターフェイスとは別のものであるため、このような直接接続が許可されます）。

図 *3:* エッジ ネットワークの展開



ファイアウォールのケーブル接続

Cisco Secure Firewall 3100 で推奨シナリオのいずれかに相当するケーブル接続を行うには、次の手順を参照してください。

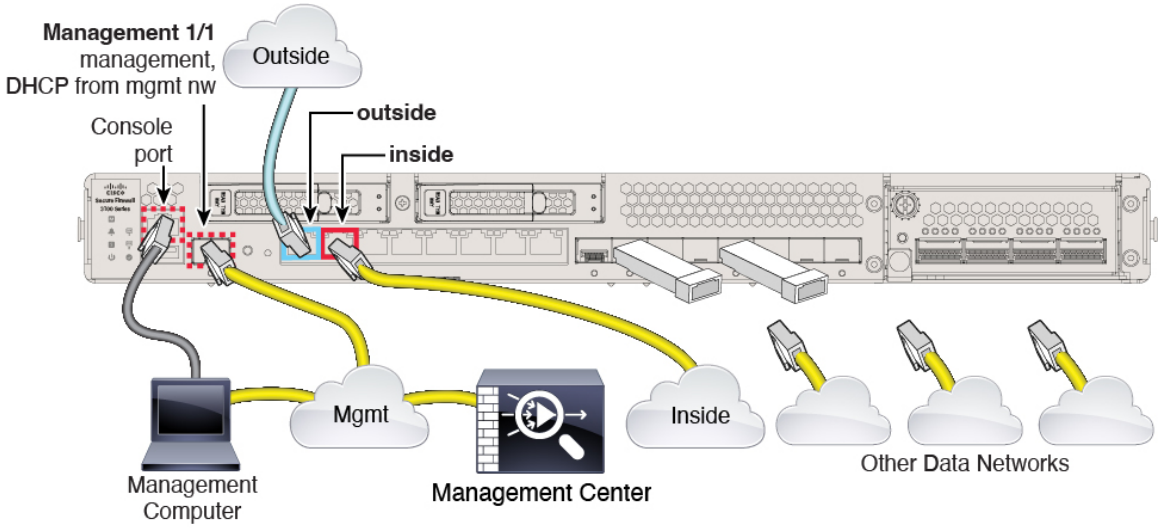
（注） その他のトポロジも使用可能で、基本的な論理ネットワーク接続、ポート、アドレッシング、構成の要件によって導入方法が異なります。

手順

ステップ 1 シャーシを取り付けます。ハードウェア設置ガイドを参照してください。

ステップ 2 別の管理ネットワーク用のケーブル配線：

図 *4 :* 個別の管理ネットワークのケーブル配線



a) 次のように管理ネットワークにケーブルを配線します。

- Management 1/1 インターフェイス

（注） Management 1/1 は、SFP モジュールを必要とする 10 Gb 光ファイバインターフェイスです。

- Firepower Management Center
- 管理コンピュータ

b) 管理コンピュータをコンソールポートに接続します。管理インターフェイスへの SSH を使用しない場合は、コンソールポートを使用して初期設定のために CLI にアクセスする必要があります。

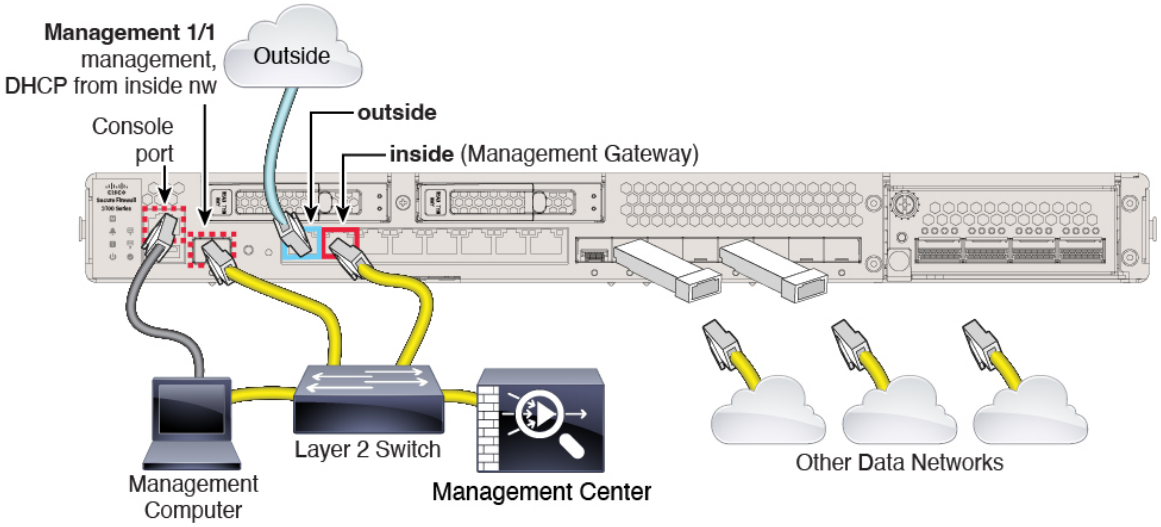
c) 内部インターフェイス（Ethernet 1/2 など）を内部ルータに接続します。

d) 外部インターフェイス（Ethernet 1/1 など）を外部ルータに接続します。

e) 残りのインターフェイスに他のネットワークを接続します。

ステップ 3 エッジ展開用のケーブル配線：

図 *5:* エッジ展開のケーブル配線



a) 以下の機器のケーブルをレイヤ 2 イーサネット スイッチに接続します。

- 内部インターフェイス（Ethernet 1/2 など）
- Management 1/1 インターフェイス

（注） Management 1/1 は、SFP モジュールを必要とする 10 Gb 光ファイバインターフェイスです。

- Firepower Management Center
- 管理コンピュータ

b) 管理コンピュータをコンソールポートに接続します。管理インターフェイスへの SSH を使用しない場合は、コンソールポートを使用して初期設定のために CLI にアクセスする必要があります。

c) 外部インターフェイス（Ethernet 1/1 など）を外部ルータに接続します。

d) 残りのインターフェイスに他のネットワークを接続します。

ファイアウォールの電源を入れます

システムの電源は、ファイアウォールの背面にあるロッカー電源スイッチによって制御されます。電源スイッチは、ソフト通知スイッチとして実装されています。これにより、システムのグレースフル シャットダウンがサポートされ、システム ソフトウェアおよびデータの破損のリスクが軽減されます。

（注） FTD を初めて起動するときは、初期化に約 15 ～ 30 分かかります。

始める前に

ファイアウォールに対して信頼性の高い電力を供給することが重要です（無停電電源装置（UPS）を使用するなど）。最初のシャットダウンを行わないで電力が失われると、重大なファイルシステムの損傷を引き起こす可能性があります。バックグラウンドでは常に多数のプロセスが実行されていて、電力が失われると、システムをグレースフルシャットダウンできません。

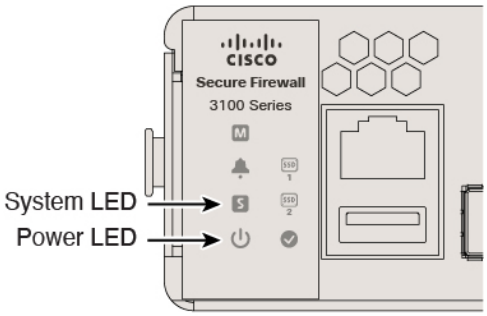
手順

ステップ 1 電源コードをファイアウォールに接続し、電源コンセントに接続します。

ステップ 2 シャーシの背面で、電源コードに隣接する標準的なロッカータイプの電源オン/オフ スイッチを使用して電源をオンにします。

ステップ 3 ファイアウォールの背面にある電源 LED を確認します。緑色に点灯している場合は、ファイアウォールの電源が入っています。

図 *6 :* システムおよび電源 *LED*



ステップ 4 ファイアウォールの背面にあるシステム LED を確認します。緑色に点灯している場合は、電源投入診断に合格しています。

（注） スイッチを ON から OFF に切り替えると、システムの電源が最終的に切れるまで数秒かかることがあります。この間は、シャーシの前面パネルの電源 LED が緑に点滅します。電源 LED が完全にオフになるまで電源を切らないでください。

（任意）ソフトウェアの確認と新しいバージョンのインストール

ソフトウェアのバージョンを確認し、必要に応じて別のバージョンをインストールするには、次の手順を実行します。ファイアウォールを設定する前に対象バージョンをインストールすることをお勧めします。別の方法として、稼働後にアップグレードを実行することもできますが、設定を保持するアップグレードでは、この手順を使用するよりも時間がかかる場合があります。

実行するバージョン

ソフトウェア ダウンロード ページのリリース番号の横にある、金色の星が付いている Gold Star リリースを実行することをお勧めします。https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html に記載されているリリース戦略も参照してください。たとえば、この速報では、（最新機能を含む）短期的なリリース番号、長期的なリリース番号（より長期間のメンテナンスリリースとパッチ）、または非常に長期的なリリース番号（政府認定を受けるための最長期間のメンテナンスリリースとパッチ）について説明しています。

手順

ステップ 1 CLI に接続します。詳細については、FTD および FXOS CLI へのアクセス （38 ページ）を参照してください。この手順ではコンソールポートを使用していますが、代わりに SSH を使用することもできます。

admin ユーザとデフォルトパスワードの **Admin123** を使用してログインします。

FXOS CLI に接続します。初めてログインしたとき、パスワードを変更するよう求められます。このパスワードは、SSH の FTD ログインにも使用されます。

（注） パスワードがすでに変更されていて、パスワードがわからない場合は、デバイスを再イメージ化してパスワードをデフォルトにリセットする必要があります。再イメージ化の手順については、『FXOS troubleshooting guide』を参照してください。

例：

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]
```

```
firepower#
```

ステップ 2 FXOS CLI で、実行中のバージョンを表示します。

scope ssa

show app-instance

例：

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name      Slot ID    Admin State     Operational State    Running Version
Startup Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd                   1          Enabled         Online               7.1.0.65
7.1.0.65        Not Applicable
```

ステップ 3 新しいバージョンをインストールする場合は、次の手順を実行します。

a) 管理インターフェイスに静的 IP アドレスを設定する必要がある場合は、「CLI を使用した FTD 初期設定の実行の完了 （11 ページ）」を参照してください。デフォルトでは、管理インターフェイスは DHCP を使用します。

管理インターフェイスからアクセスできるサーバーから新しいイメージをダウンロードする必要があります。

b) FXOS のトラブルシューティング ガイドに記載されている再イメージ化の手順を実行します。

FTD の初期設定の完了

CLI か FDM を使用して FTD の初期設定を完了させることができます。

CLI を使用した FTD 初期設定の実行の完了

FTD CLI に接続して初期設定を実行します。これには、セットアップウィザードを使用した管理 IP アドレス、ゲートウェイ、およびその他の基本ネットワーク設定の指定などが含まれます。専用の管理インターフェイスは、独自のネットワーク設定を持つ特別なインターフェイスです。FMC アクセスに管理インターフェイスを使用しない場合は、代わりに CLI を使用してデータインターフェイスを設定できます。また、FMC 通信の設定を行います。FDM を使用して初期セットアップを実行すると、管理および FMC アクセスインターフェイスの設定に加えて、管理のために FMC に切り替えたときに、FDM で完了したすべてのインターフェイス設定が保持されます。アクセス コントロール ポリシーなどの他のデフォルト設定は保持されないことに注意してください。

手順

ステップ 1 コンソールポートから、または管理インターフェイスへの SSH を使用して、FTD CLI に接続します。デフォルトで DHCP サーバーから IP アドレスが取得されます。ネットワーク設定を変更する場合は、切断されないようにコンソールポートを使用することを推奨します。

コンソールポートは FXOS CLI に接続します。SSH セッションは FTD CLI に直接接続します。

ステップ 2 ユーザー名 **admin** およびパスワード **Admin123** でログインします。

コンソールポートで FXOS CLI に接続します。初めて FXOS にログインしたときは、パスワードを変更するよう求められます。このパスワードは、SSH の FTD ログインにも使用されます。

（注） パスワードがすでに変更されていて、パスワードがわからない場合は、デバイスを再イメージ化してパスワードをデフォルトにリセットする必要があります。再イメージ化の手順については、FXOS のトラブルシューティング ガイドを参照してください。

例：

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

ステップ 3 コンソールポートで FXOS に接続した場合は、FTD CLI に接続します。

connect ftd

例：

```
firepower# connect ftd
>
```

ステップ 4 FTD に初めてログインすると、エンドユーザーライセンス契約（EULA）に同意し、SSH 接続を使用している場合は、管理者パスワードを変更するように求められます。その後、CLI セットアップスクリプトが表示されます。

（注） 設定をクリア（たとえば、イメージを再作成することにより）しないかぎり、CLI セットアップウィザードを繰り返すことはできません。ただし、これらの設定すべては、後から CLI で **configure network** コマンドを使用して変更できます。Secure Firewall Threat Defense のコマンドリファレンスを参照してください。

デフォルト値または以前に入力した値がカッコ内に表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

次のガイドラインを参照してください。

- **管理インターフェイスの IPv4 デフォルトゲートウェイを入力**：[data-interfaces] の設定は、リモートの FMC または FDM の管理にのみ適用されます。管理ネットワークで FMC を使用する場合は、Management 1/1 のゲートウェイ IP アドレスを設定する必要があります。「ネットワークの導入」の項に示されているエッジ展開の例では、内部インターフェイスは管理ゲートウェイとして機能します。この場合、ゲートウェイ IP アドレスを目的の内部インターフェイス IP アドレスに設定する必要があります。後で FMC を使用して内部 IP アドレスを設定する必要があります。
- **ネットワーク情報が変更された場合は再接続が必要**：SSH で接続しているのに、初期セットアップでその IP アドレスを変更すると、接続が切断されます。新しい IP アドレスとパスワードで再接続してください。コンソール接続は影響を受けません。
- [デバイスをローカルで管理しますか（Manage the device locally?）]：FMC を使用するには「**no**」を入力します。**yes** と入力すると、代わりに FDM を使用することになります。
- [ファイアウォールモードを設定しますか（Configure firewall mode?）]：初期設定でファイアウォールモードを設定することをお勧めします。初期設定後にファイアウォールモードを変更すると、実行コンフィギュレーションが消去されます。

例：

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password: ********
Confirm new password: ********
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

Update policy deployment information
    - add device configuration
```

```
    - add network discovery
    - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

ステップ 5 この FTD を管理する FMC を特定します。

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**}—Specifies either the FQDN or IP address of the FMC.FMC を直接アドレス指定できない場合は、**DONTRESOLVE** を使用します。また、*nat_id* も指定します。双方向の SSL 暗号化通信チャネルを 2 台のデバイス間に確立するには、少なくても 1 台以上のデバイス（FMC または FTD）に到達可能な IP アドレスが必要です。このコマンドで **DONTRESOLVE** を指定するには、到達可能な IP アドレスまたはホスト名が FTD に必要です。
- reg_key：FTD を登録するときに FMC でも指定する任意のワンタイム登録キーを指定します。登録キーは37 文字以下にする必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。
- nat_id：一方の側で到達可能な IP アドレスまたはホスト名が指定されていない場合は、FTD を登録するときに FMC にも指定する任意の一意のワンタイム文字列を指定します。この文字列は、 FMC を **DONTRESOLVE** に設定した場合に必要です。NAT ID は 37 文字以下にする必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、FMC に登録する他のデバイスには使用できません。

例：

```
> configure manager add MC.example.com 123456
Manager successfully configured.
```

FMC が NAT デバイスの背後にある場合は、次の例に示すように、一意の NAT ID とともに登録キーを入力し、ホスト名の代わりに DONTRESOLVE を指定します。

例：

```
> configure manager add DONTRESOLVE regk3y78 natid90
Manager successfully configured.
```

FTD が NAT デバイスの背後にある場合は、次の例に示すように、一意の NAT ID とともに FMC IP アドレスまたはホスト名を入力します。

例：

```
> configure manager add 10.70.45.5 regk3y78 natid56
Manager successfully configured.
```

次のタスク

FMC にファイアウォールを登録します。

FDM を使用した FTD の初期設定の完了

FDM に接続して、FTD の初期設定を実行します。FDM を使用して初期セットアップを実行すると、管理と FMC のアクセス設定に加えて、管理のために FMC に切り替えたときに、FDM で完了したすべてのインターフェイス設定が保持されます。アクセス コントロール ポリシーやセキュリティゾーンなどの他のデフォルト設定は保持されないことに注意してください。CLI を使用すると、管理と FMC のアクセス設定のみが保持されます（たとえば、デフォルトの内部インターフェイスの設定は保持されません）。

始める前に

- FMC の初期設定を展開して実行します。Cisco Firepower Management Center 1600, 2600, and 4600 Hardware Installation Guideを参照してください。FTD をセットアップする前に、FMC の IP アドレスまたはホスト名を把握しておく必要があります。
- Firefox、Chrome、Safari、Edge、または Internet Explorer の最新バージョンを使用します。

手順

ステップ 1 FDM にログインします。

a) ブラウザに次の URL のいずれかを入力します。

- 内部（Ethernet 1/2）：**https://192.168.95.1**。
- 管理：**https://***management_ip*。管理インターフェイスは DHCP クライアントであるため、IP アドレスは DHCP サーバーによって異なります。この手順の一環として、管理 IP アドレスを静的アドレスに設定する必要があるため、接続が切断されないように内部インターフェイスを使用することをお勧めします。

b) ユーザー名 **admin**、デフォルト パスワード **Admin123** を使用してログインします。

c) エンドユーザー ライセンス契約書を読んで同意し、管理者パスワードを変更するように求められます。

ステップ 2 初期設定を完了するには、最初に FDM にログインしたときにセットアップウィザードを使用します。必要に応じて、ページの下部にある [デバイスの設定をスキップ（Skip device setup）] をクリックしてセットアップウィザードをスキップできます。

セットアップウィザードを完了すると、内部インターフェイス（Ethernet1/2）のデフォルト設定に加えて、FMC の管理に切り替えるときに維持される外部（Ethernet1/1）インターフェイスも設定できます。

a) 外部インターフェイスおよび管理インターフェイスに対して次のオプションを設定し、[次へ（Next）] をクリックします。

1. [外部インターフェイスアドレス（Outside Interface Address）]：このインターフェイスは通常インターネットゲートウェイであり、FMC アクセスインターフェイスとして使用される場合があります。デバイスの初期設定時に別の外部インターフェイスを選択することはできません。最初のデータ インターフェイスがデフォルトの外部インターフェイスです。

   FMC アクセスに外部（または内部）とは異なるインターフェイスを使用する場合は、セットアップウィザードの完了後に手動で設定する必要があります。

   [IPv4の設定（Configure IPv4）]：外部インターフェイス用の IPv4 アドレスです。DHCP を使用するか、または手動でスタティック IP アドレス、サブネットマスク、およびゲートウェイを入力できます。[オフ（Off）] を選択して、IPv4 アドレスを設定しないという選択肢もあります。セットアップウィザードを使用して PPPoE を設定することはできません。インターフェイスが DSL モデム、ケーブルモデム、または ISP への他の接続に接続されており、ISP が PPPoE を使用して IP アドレスを提供している場合は、PPPoE が必要になる場合があります。ウィザードの完了後に PPPoE を設定できます。

   [IPv6の設定（Configure IPv6）]：外部インターフェイス用の IPv6 アドレスです。DHCP を使用するか、または手動でスタティック IP アドレス、プレフィックス、およびゲートウェイを入力できます。[オフ（Off）] を選択して、IPv6 アドレスを設定しないという選択肢もあります。

2. **[管理インターフェイス（Management Interface）]**

   CLI で初期設定を実行した場合、管理インターフェイスの設定は表示されません。管理インターフェイスの IP アドレスの設定は、セットアップウィザードに含まれていないことに注意してください。管理 IP アドレスの設定については、「ステップ 3 （17 ページ）」を参照してください。

   [DNSサーバー（DNS Servers）]：ファイアウォールの管理インターフェイスの DNS サーバーです。名前解決用に 1 つ以上の DNS サーバのアドレスを入力します。デフォルトは OpenDNS パブリック DNS サーバです。フィールドを編集し、デフォルトに戻したい場合は、[OpenDNSを使用（Use OpenDNS）] をクリックすると、フィールドに適切な IP アドレスがリロードされます。

[ファイアウォールホスト名（Firewall Hostname）]：ファイアウォールの管理インターフェイスのホスト名です。

b) [時刻設定（NTP）（Time Setting (NTP)）] を設定し、[次へ（Next）] をクリックします。

1. [タイムゾーン（Time Zone）]：システムのタイムゾーンを選択します。
2. [NTPタイムサーバ（NTP Time Server）]：デフォルトの NTP サーバを使用するか、使用している NTP サーバのアドレスを手動で入力するかを選択します。バックアップ用に複数のサーバを追加できます。

c) [登録せずに 90 日間の評価期間を開始（Start 90 day evaluation period without registration）] を選択します。

FTD を Smart Software Manager に登録しないでください。すべてのライセンスは FMC で実行されます。

d) [終了（Finish）] をクリックします。

e) [クラウド管理（Cloud Management）]または [スタンドアロン（Standalone）] を選択するよう求められます。FMC の管理については、[スタンドアロン（Standalone）] を選択してから、[Got It（了解）] を選択します。

ステップ 3 （必要に応じて）管理インターフェイスの静的 IP アドレスを設定します。[デバイス（Device）] を選択し、[システム設定（System Settings）] > [管理インターフェイス（Management Interface）] リンクの順にクリックします。

静的 IP アドレスを設定する場合は、デフォルトゲートウェイもデータインターフェイスではなく一意のゲートウェイに設定してください。DHCP を使用する場合は、何も設定する必要はありません。

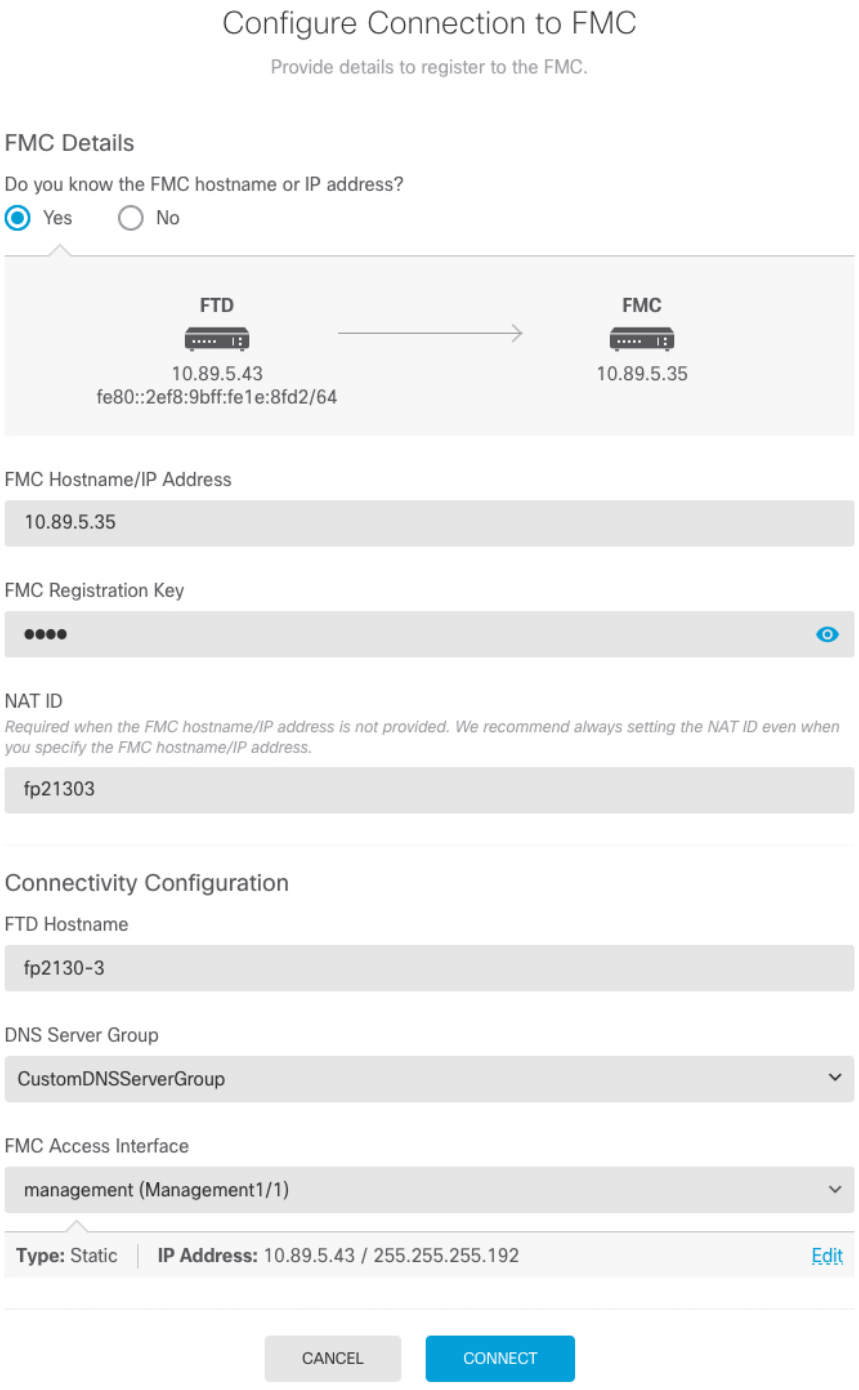
ステップ 4 外部または内部以外のインターフェイスを含む追加のインターフェイスを設定する場合は、[デバイス（Device）] を選択し、[インターフェイス（Interface）] のサマリーにあるリンクをクリックします。

FDM におけるインターフェイスの設定の詳細については、「FDM でのファイアウォールの設定」を参照してください。FMC にデバイスを登録すると、FDM の他の設定は保持されません。

ステップ 5 [デバイス（Device）] > [システム設定（Device System Settings）] > [中央管理 (Central Management)] > [Management Center] > [Management Center] > [デバイス（Device）] > [システム設定（System Settings）] > [中央管理（Central Management）] > [Management Center] を選択し、 [続行（Proceed）] をクリックして FMC の管理を設定します。 > >

ステップ 6 **[FMCの詳細（FMC Details）]** を設定します。

図 *7*: *FMC* の詳細



a) [Management Center/CDOのホスト名またはIPアドレスを知っていますか（Do you know the FMC hostname or IP address）]、[FMCのホスト名またはIPアドレスを知っていますか（Do you know the FMC hostname or IP address）] で、IP アドレスまたはホスト名を使用して FMC/CDO に到達できる場合は [はい（Yes）] をクリックし、FMC/CDO が NAT の背後に

あるか、パブリック IP アドレスまたはホスト名がない場合は [いいえ（No）] をクリックします。

双方向の SSL 暗号化通信チャネルを 2 台のデバイス間に確立するには、少なくても 1 台以上のデバイス（FMC/CDO または FTD デバイス）に到達可能な IP アドレスが必要です。

b) [はい（Yes）] を選択した場合は、、**FMC のホスト名/IP アドレス**を入力します。

c) **FMC 登録キー**を指定します。

このキーは、FTDデバイスを登録するときにFMCでも指定する任意の1回限りの登録キーです。登録キーは 37 文字以下にする必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、FMC に登録する複数のデバイスに使用できます。

d) [NAT ID] を指定します。

この ID は、FMC でも指定する任意の 1 回限りの文字列です。いずれかのデバイスの IP アドレスのみを指定する場合、このフィールドは必須です。両方のデバイスのIPアドレスがわかっている場合でも、NAT ID を指定することを推奨します。NAT ID は 37 文字以下にする必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、FMC に登録する他のデバイスには使用できません。NAT ID は、正しいデバイスからの接続であることを確認するために IP アドレスと組み合わせて使用されます。 IP アドレス/NAT ID の認証後にのみ、登録キーがチェックされます。

ステップ 7 [接続の設定（Connectivity Configuration）] を設定します。

a) [FTDホスト名（FTD Hostname）] を指定します。

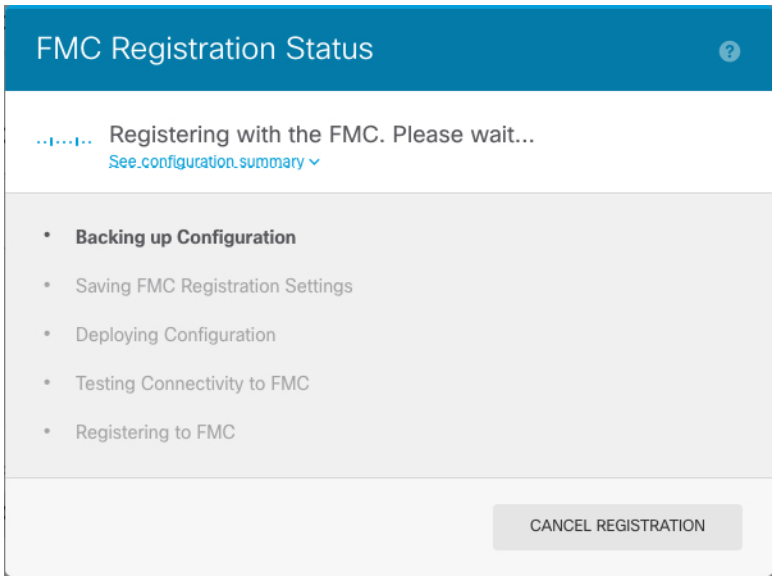
b) [DNSサーバーグループ（DNS Server Group）] を指定します。

既存のグループを選択するか、新しいグループを作成します。デフォルトの DNS グループは **CiscoUmbrellaDNSServerGroup** と呼ばれ、OpenDNS サーバーが含まれます。

c) **[FMCアクセスインターフェイス（FMC Access Interface）]**については、[管理（management）] を選択します。

ステップ 8 [接続（Connect）] をクリックします。[登録ステータス（Registration Status）] [FMC登録ステータス（FMC Registration Status）] [FMC登録ステータス (FMC Registration Status)] ダイアログボックスには、FMC への切り替えの現在のステータスが表示されます。[Management Center/CDO登録設定の保存（Saving Management Center/CDO Registration Settings）] [FMC登録設定の保存（Saving FMC Registration Settings）] [FMC登録設定の保存（Saving FMC Registration Settings）] ステップの後、FMC に移動し、ファイアウォールを追加します。

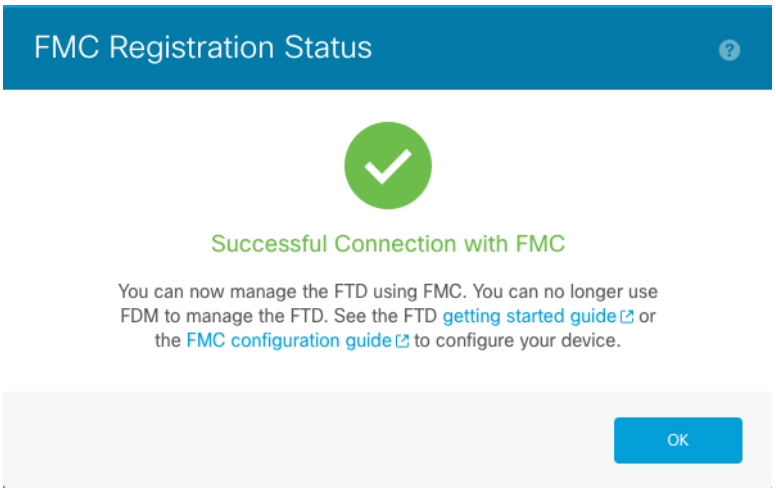
図 *8 : FMC* 登録ステータス



FMC への切り替えをキャンセルする場合は、[登録のキャンセル（Cancel Registration）] をクリックします。キャンセルしない場合は、[Management Center/CDO登録設定の保存（Saving Management Center/CDO Registration Settings）] [FMC登録設定の保存（Saving FMC Registration Settings）] [FMC登録設定の保存（Saving FMC Registration Settings）] のステップが完了するまでFDMブラウザウィンドウを閉じないでください。閉じた場合、プロセスは一時停止し、FDMに再接続した場合のみ再開されます。

[Management Center/CDO登録設定の保存（Saving Management Center/CDO Registration Settings）] [FMC登録設定の保存（Saving FMC Registration Settings）] [FMC登録設定の保存（Saving FMC Registration Settings）] ステップの後に FDM に接続したままにする場合、その後 [Management CenterまたはCDOとの正常接続 (Successful Connection with Management Center or CDO)] [FMCとの正常接続（Successful Connection with FMC）] [FMCとの正常接続（Successful Connection with FMC）] ダイアログボックスが表示され、FDM から切断されます。

図 *9* : *FMC* との正常接続



へのログインFMC

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 ユーザー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。

FMC のライセンスの取得

すべてのライセンスは、FMCによってFTDに提供されます。次のライセンスを購入できます。

- **基本**：（必須）基本ライセンス。
- **脅威**：セキュリティ インテリジェンスと次世代 IPS

- **マルウェア**：マルウェア
- **URL**：URL フィルタリング
- **RA VPN**：AnyConnect Plus、AnyConnect Apex、または AnyConnect VPN 専用

シスコライセンスの概要については詳しくは、cisco.com/go/licensingguide を参照してください。

始める前に

- 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。

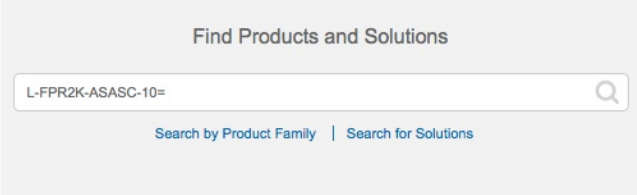
- （輸出コンプライアンスフラグを使用して有効化される）機能を使用するには、ご使用のスマート ソフトウェア ライセンシング アカウントで強力な暗号化（3DES/AES）ライセンスを使用できる必要があります。

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 *10*：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。

- 基本ライセンス：
  - L-FPR3110-BSE=
  - L-FPR3120-BSE=
  - L-FPR3130-BSE=
  - L-FPR3140-BSE=
- 脅威、マルウェア、および URL ライセンスの組み合わせ：

- L-FPR3110T-TMC=
- L-FPR3120T-TMC=
- L-FPR3130T-TMC=
- L-FPR3140T-TMC=

上記の PID のいずれかを注文に追加すると、次のいずれかの PID に対応する期間ベースのサブスクリプションを選択できます。

- L-FPR3110T-TMC-1Y
- L-FPR3110T-TMC-3Y
- L-FPR3110T-TMC-5Y
- L-FPR3120T-TMC-1Y
- L-FPR3120T-TMC-3Y
- L-FPR3120T-TMC-5Y
- L-FPR3130T-TMC-1Y
- L-FPR3130T-TMC-3Y
- L-FPR3130T-TMC-5Y
- L-FPR3140T-TMC-1Y
- L-FPR3140T-TMC-3Y
- L-FPR3140T-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 サーバーに 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。詳細な手順については、Firepower 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。

FMC への FTD の登録

FTD を FMC に登録します。

始める前に

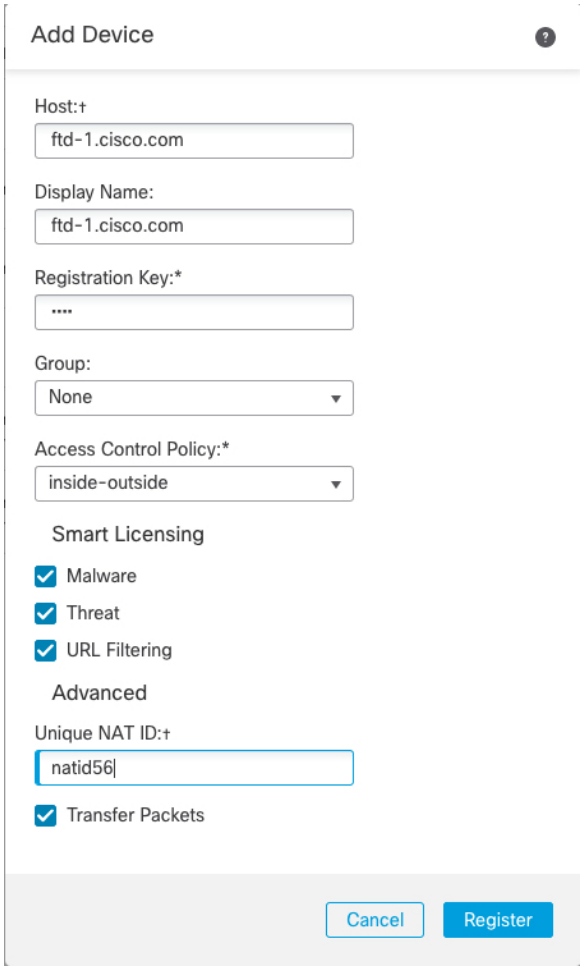
- FTD の最初の設定で設定した次の情報を収集します。
  - FTD の管理 IP アドレスまたはホスト名、および NAT ID

- FMC の登録キー

手順

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

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）] を選択します。



次のパラメータを設定します。

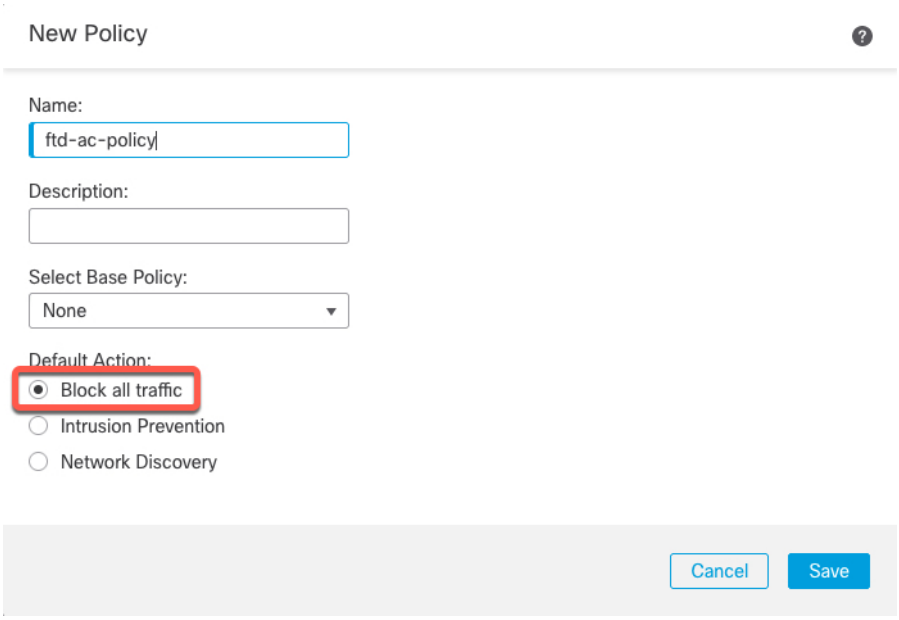
- [ホスト（Host）]：追加する FTD の IP アドレスかホスト名を入力します。FTD の最初の設定で FMC の IP アドレスと NAT ID の両方を指定した場合は、このフィールドを空のままにしておくことができます。

  （注） HA 環境では、両方の FMC が NAT の背後にある場合、プライマリ FMC のホスト IP または名前なしで FTD を登録できます。ただし、FTD をセカンダリ FMC に登録するには、FTD の IP アドレスかホスト名を指定する必要があります。

- [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 （36 ページ）」を参照してください。

図 *11 : New Policy*



- [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）]（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行する予定の場合）を割り当てます。**注**：デバイスを追加した後、**[システム（System）]** > **[ライセンス（Licenses）]** > **[スマートライセンス（Smart Licenses）]** ページから AnyConnect リモートアクセス VPN のライセンスを適用できます。
- [一意のNAT ID（Unique NAT ID）]：FTD の最初の設定で指定した 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、登録が成功し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 管理 IP アドレスを変更するには、**configure network** {**ipv4** | **ipv6**} **manual** コマンドを使用します。

- 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、FMC で登録キーと NAT ID を設定することができます。

トラブルシューティングの詳細については、https://cisco.com/go/fmc-reg-error を参照してください。

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 サーバー：クライアントの内部インターフェイスで DHCP サーバーを使用します。
- 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 （27 ページ）。
2	DHCP サーバーの設定 （30 ページ）。

3	デフォルトルートの追加 （31 ページ）。
4	NAT の設定 （33 ページ）。
5	内部から外部へのトラフィックの許可 （36 ページ）。
6	設定の展開 （37 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 サーバー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。

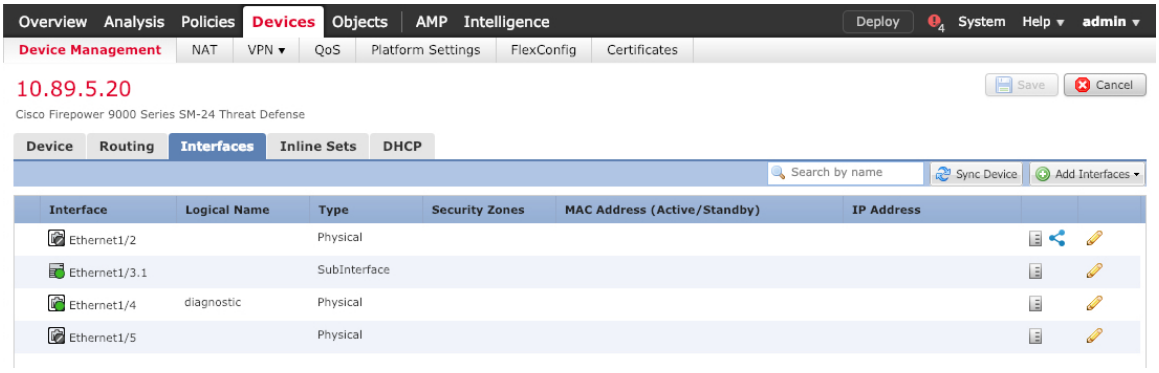
一般的なエッジルーティングの状況は、内部インターフェイスでスタティックアドレスを定義すると同時に、ISP から DHCP を介して外部インターフェイスアドレスを取得することです。

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）] の順に選択し、ファイアウォールの をクリックします。

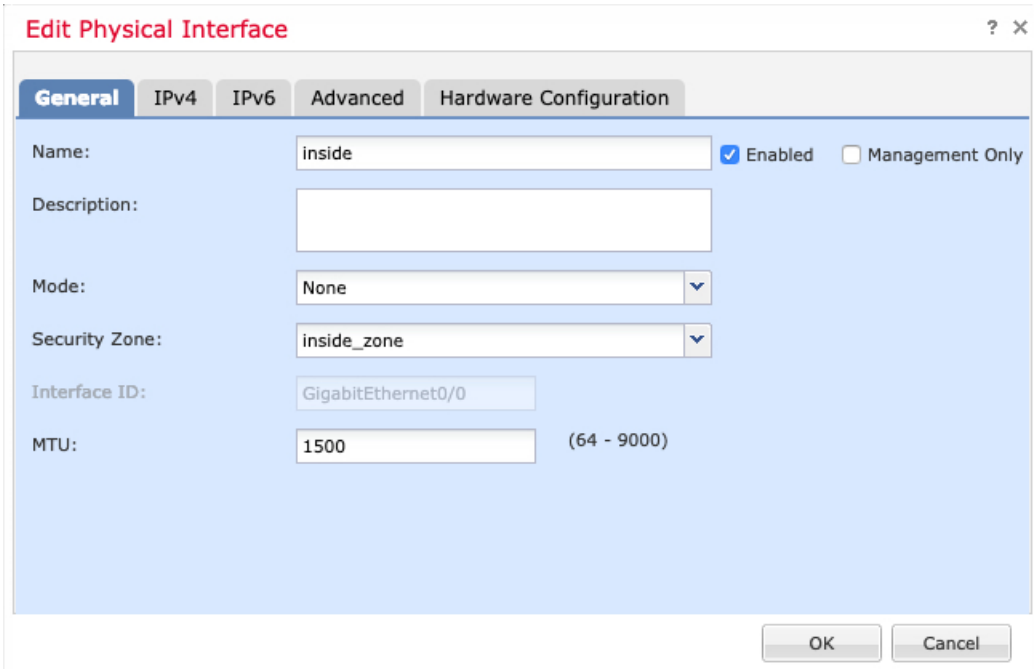
ステップ 2 [インターフェイス（Interfaces）] をクリックします。



ステップ 3

ステップ 4 内部に使用するインターフェイスの 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。

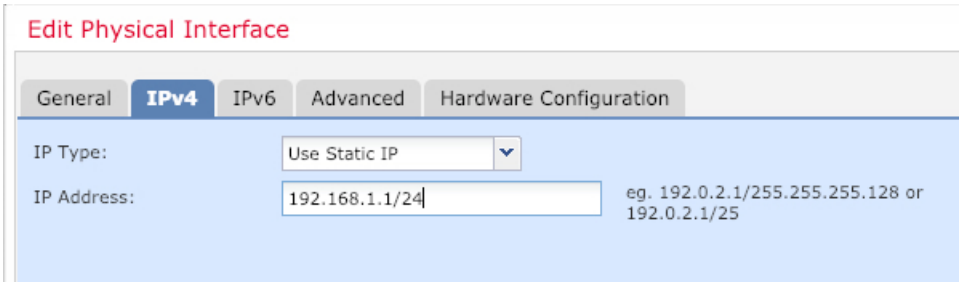
d) [セキュリティゾーン（Security Zone）] ドロップダウンリストから既存の内部セキュリティゾーンを選択するか、[新規（New）] をクリックして新しいセキュリティゾーンを追加します。

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。

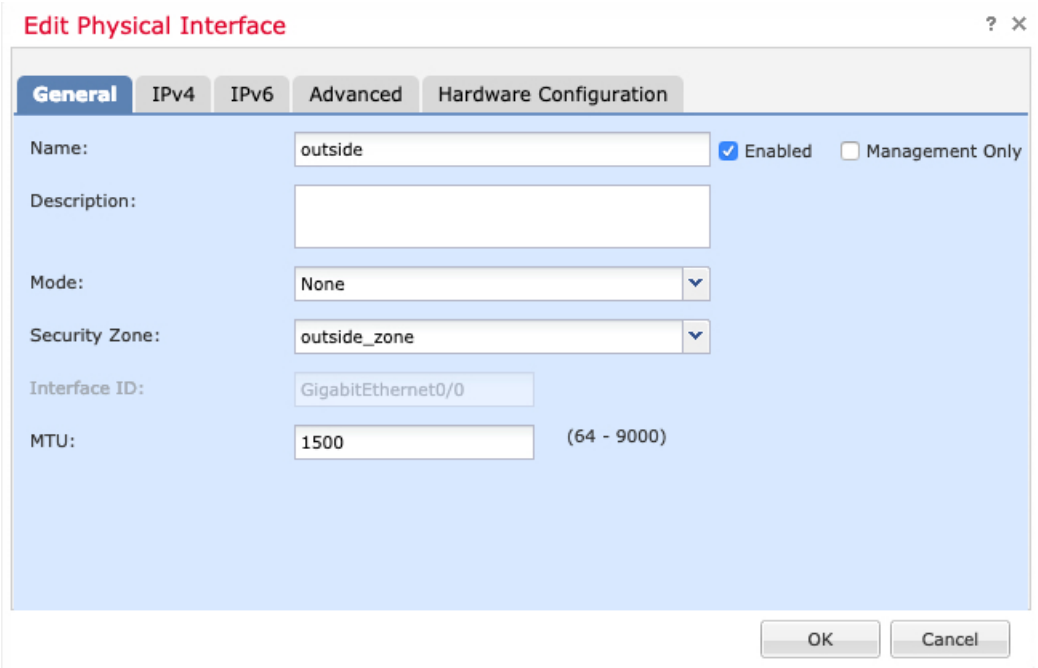


- [IPv6]：ステートレス自動設定の場合は [自動設定（Autoconfiguration）] チェックボックスをオンにします。

f) [OK] をクリックします。

ステップ 5 「外部」に使用するインターフェイスをクリックします。

[全般（General）] タブが表示されます。



（注） FMC アクセス管理用にこのインターフェイスを事前に設定している場合、インターフェイスにはすでに名前が付けられており、有効化とアドレス指定が完了しています。これらの基本設定は変更しないでください。変更すると、FMC の管理接続が中断されます。この画面でも、通過トラフィックポリシーのセキュリティゾーンを設定できます。

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。

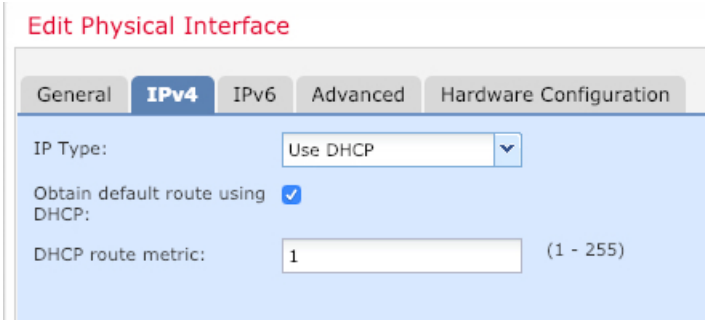
c) [モード（Mode）] は [なし（None）] に設定したままにします。

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 サーバーからデフォルト 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 6 [保存（Save）] をクリックします。

DHCP サーバーの設定

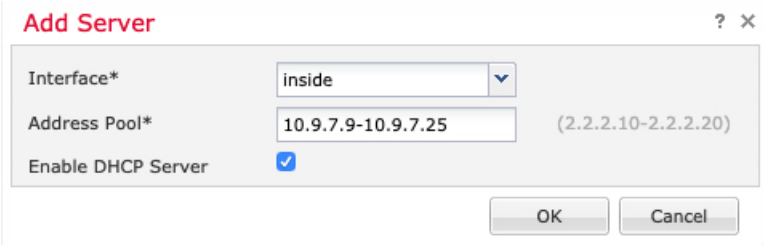
クライアントで DHCP を使用して FTD から IP アドレスを取得するようにする場合は、DHCP サーバーを有効にします。

手順

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

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

ステップ 3 **[サーバー（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 サーバーが使用する 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サーバーを有効にする（Enable DHCP Server）]：選択したインターフェイスの DHCP サーバーを有効にします。

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。

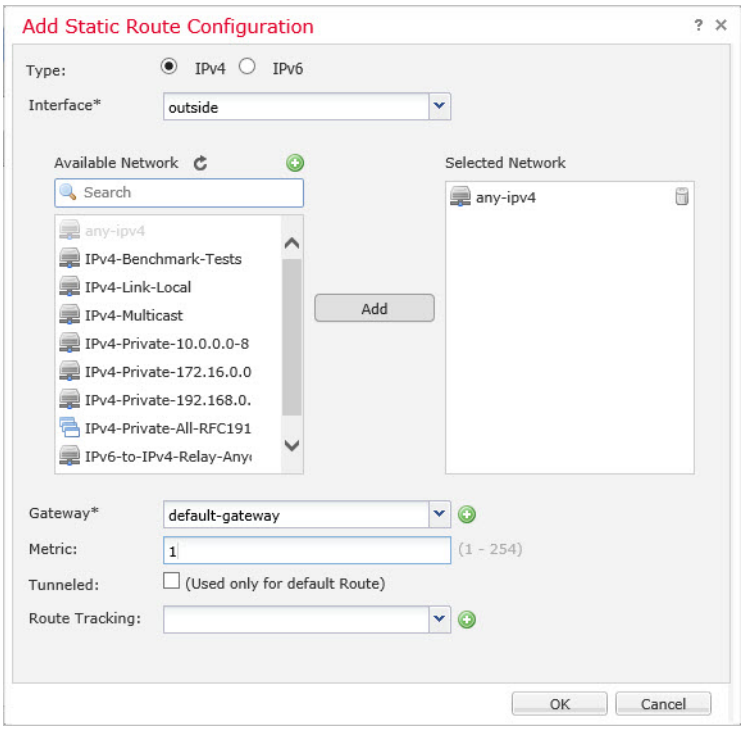
デフォルトルートの追加

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 サーバー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。

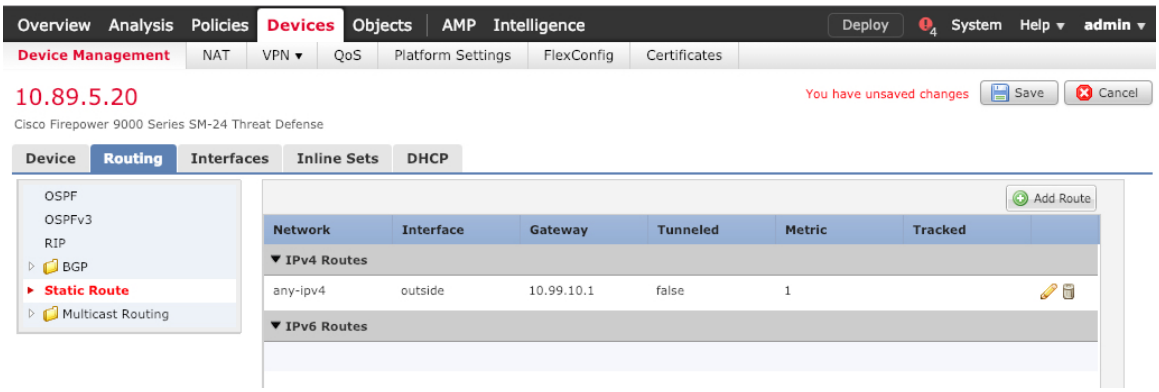
ステップ 2 **[ルーティング（Routing）]** > **[スタティックルート（Static route）]** を選択し、[ルートを追加（Add route）] をクリックして、次のように設定します。



- [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。

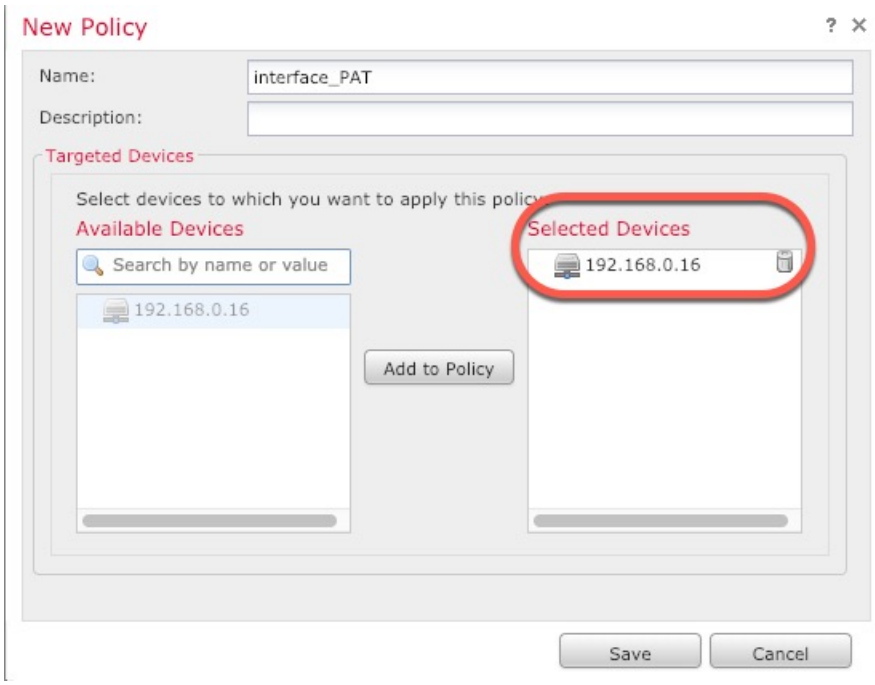
NAT の設定

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。

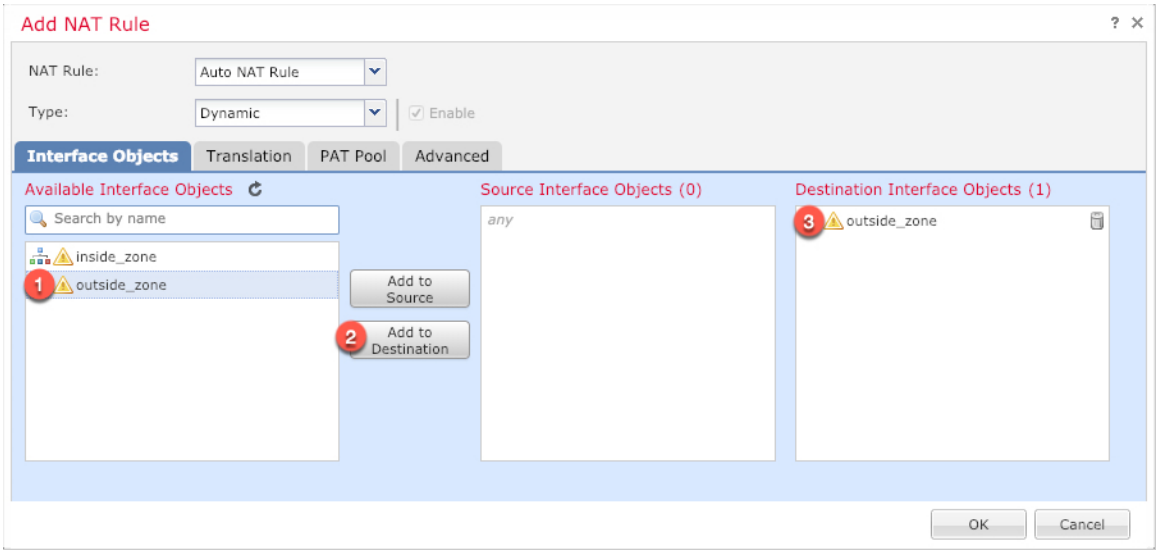
ステップ 3 [ルールの追加（Add Rule）] をクリックします。

[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。

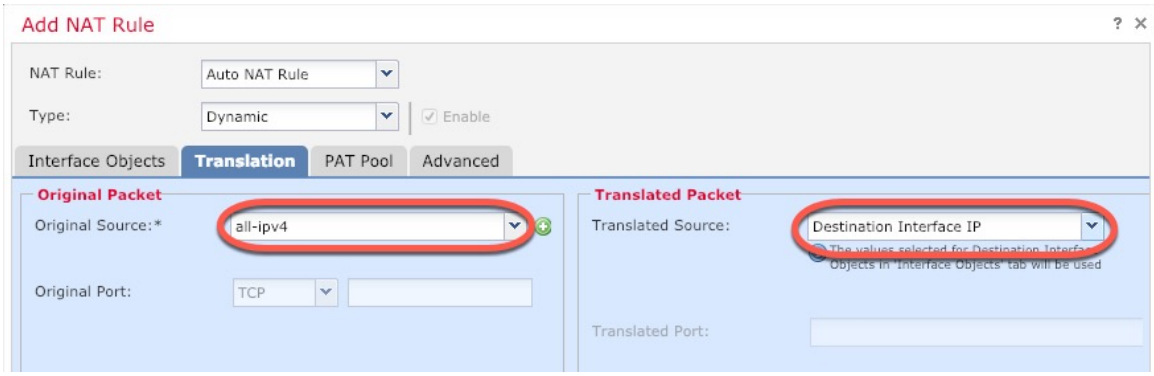
ステップ 4 基本ルールのオプションを設定します。

- [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。

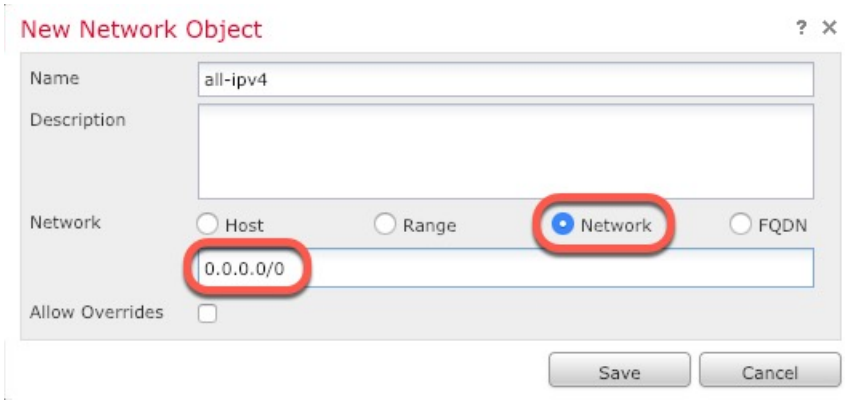
ステップ 5 [インターフェイスオブジェクト（Interface objects）] ページで、[使用可能なインターフェイスオブジェクト（Available Interface Objects）] 領域から [宛先インターフェイスオブジェクト（Destination Interface Objects）] 領域に外部ゾーンを追加します。



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）]：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。

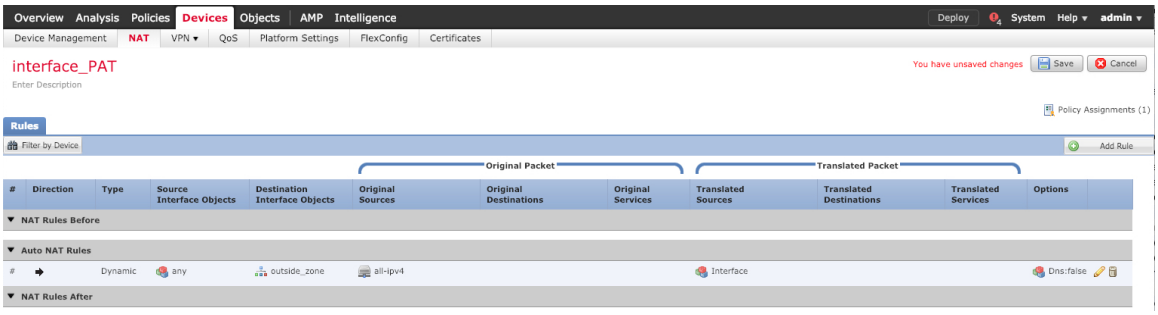


（注） 自動 NAT ルールはオブジェクト定義の一部として NAT を追加するため、システム定義の **any-ipv4** オブジェクトを使用することはできません。また、システム定義のオブジェクトを編集することはできません。

- [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

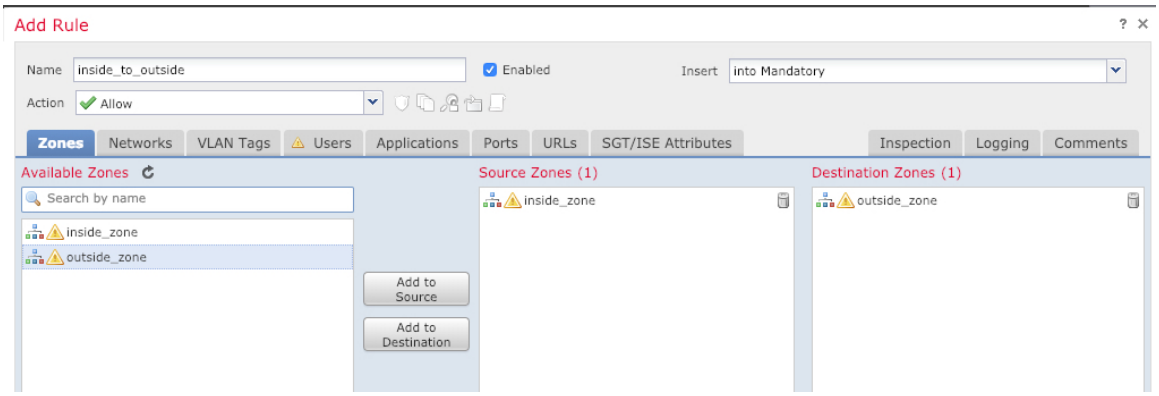
FTD を FMC に登録したときに、基本の [すべてのトラフィックをブロック（Block all traffic）] アクセス コントロール ポリシーを作成した場合は、デバイスを通過するトラフィックを許可するためにポリシーにルールを追加する必要があります。次の手順では、内部ゾーンから外部ゾーンへのトラフィックを許可するルールを追加します。他にゾーンがある場合は、適切なネットワークへのトラフィックを許可するルールを追加してください。

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、『Firepower Management Center 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 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。

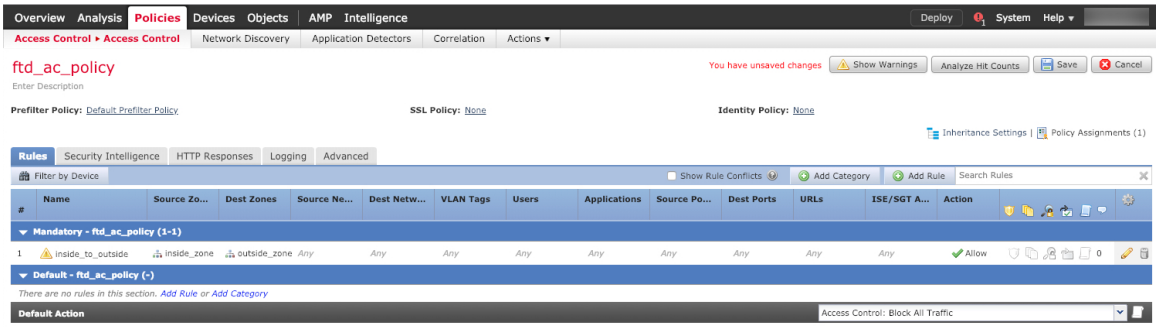


- [名前（Name）]：このルールに名前を付けます（たとえば、**inside_to_outside**）。
- [送信元ゾーン（Source Zones）]：[使用可能なゾーン（Available Zones）] から内部ゾーンを選択し、[送信元に追加（Add to Source）] をクリックします。
- [宛先ゾーン（Destination Zones）]：[使用可能なゾーン（Available Zones）] から外部ゾーンを選択し、[宛先に追加（Add to Destination）] をクリックします。

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。



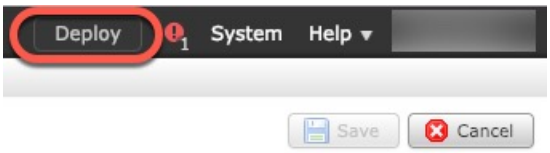
ステップ 4 [保存（Save）] をクリックします。

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。

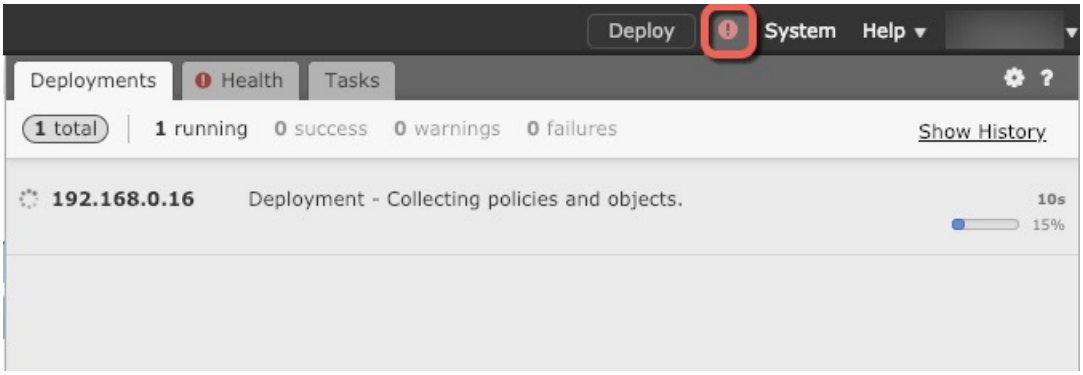
手順

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。



FTD および FXOS CLI へのアクセス

コマンドライン インターフェイス（CLI）を使用してシステムのセットアップを行い、基本的なシステムのトラブルシューティングを行います。CLI セッションからポリシーを設定することはできません。CLI には、コンソール ポートに接続してアクセスできます。

トラブルシューティングのために、FXOS CLI にアクセスすることもできます。

（注） または、FTD デバイスの管理インターフェイスに SSH で接続できます。コンソールセッションとは異なり、SSH セッションはデフォルトで FTD CLI になり、**connect fxos** コマンドを使用して FXOS CLI に接続できます。SSH 接続用のインターフェイスを開いている場合、後でデータインターフェイス上のアドレスに接続できます。データ インターフェイスへの SSH アクセスはデフォルトで無効になっています。この手順では、デフォルトで FXOS CLI となるコンソールポートアクセスについて説明します。

手順

ステップ 1 CLI にログインするには、管理コンピュータをコンソール ポートに接続します。Cisco Secure Firewall 3100 には DB-9 to RJ-45 シリアルケーブルが付属しているため、接続するためにはサードパーティ製のシリアル to USB ケーブルが必要です。お使いのオペレーティングシステムに必要な USB シリアルドライバを必ずインストールしてください（Cisco Secure Firewall 3100 ハードウェアガイドを参照）。コンソールポートはデフォルトで FXOS CLI になります。次のシリアル設定を使用します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

FXOS CLI に接続します。ユーザー名 **admin** と、初期セットアップ時に設定したパスワードを使用して CLI にログインします（デフォルトは **Admin123**）。

例：

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

ステップ 2 FTD CLI にアクセスします。

connect ftd

例：

```
firepower# connect ftd
>
```

ログイン後に、CLI で使用可能なコマンドの情報を確認するには、**help** または **?** を入力します。使用方法については、『Secure Firewall Threat Defense のコマンドリファレンス』を参照してください。

ステップ 3 FTD CLI を終了するには、**exit** または **logout** コマンドを入力します。

このコマンドにより、FXOS CLI プロンプトに戻ります。FXOS CLI で使用可能なコマンドの情報を確認するには、**?** を入力します。

例：

```
> exit
```

```
firepower#
```

ファイアウォールの電源の切断

システムを適切にシャットダウンすることが重要です。単純に電源プラグを抜いたり、電源スイッチを押したりすると、重大なファイルシステムの損傷を引き起こすことがあります。バックグラウンドでは常に多数のプロセスが実行されており、電源プラグを抜いたり、電源を切断したりすると、ファイアウォールシステムをグレースフルシャットダウンできないことを覚えておいてください。

FMC のデバイス管理ページを使用してデバイスの電源を切断するか、FXOS CLI を使用できます。

FMC を使用したファイアウォールの電源の切断

システムを適切にシャットダウンすることが重要です。単純に電源プラグを抜いたり、電源スイッチを押したりすると、重大なファイルシステムの損傷を引き起こすことがあります。バックグラウンドでは常に多数のプロセスが実行されていて、電源プラグを抜いたり、電源を切断したりすると、ファイアウォールをグレースフルシャットダウンできないことを覚えておいてください。

FMC を使用してシステムを適切にシャットダウンできます。

手順

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

ステップ 2 再起動するデバイスの横にある編集アイコン（  ）をクリックします。

ステップ 3 [デバイス（Device）] タブをクリックします。

ステップ 4 [システム（System）]セクションでデバイスのシャットダウンアイコン（  ）をクリックします。

ステップ 5 プロンプトが表示されたら、デバイスのシャットダウンを確認します。

ステップ 6 コンソールからファイアウォールに接続している場合は、ファイアウォールがシャットダウンするときにシステムプロンプトをモニターします。次のプロンプトが表示されます。

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

コンソールから接続していない場合は、約3分間待ってシステムがシャットダウンしたことを確認します。

ステップ 7 必要に応じて電源スイッチをオフにし、電源プラグを抜いてシャーシから物理的に電源を取り外すことができます。

CLI におけるファイアウォールの電源の切断

FXOS CLI を使用すると、システムを安全にシャットダウンしてデバイスの電源を切断できます。CLI には、コンソールポートに接続してアクセスします。FTD および FXOS CLI へのアクセス （38 ページ）を参照してください。

手順

ステップ 1 FXOS CLI でローカル管理に接続します。

firepower # **connect local-mgmt**

ステップ 2 **shutdown** コマンドを発行します。

firepower(local-mgmt) # **shutdown**

例：

```
firepower(local-mgmt)# shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
```

ステップ 3 ファイアウォールのシャットダウン時にシステムプロンプトをモニターします。次のプロンプトが表示されます。

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

ステップ 4 必要に応じて電源スイッチをオフにし、電源プラグを抜いてシャーシから物理的に電源を取り外すことができます。

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」にある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 の使用に関する情報については、「Firepower Management Center Configuration Guide」を参照してください。

次のステップ