FMC を使用した Firepower Threat Defense の展開

この章では、Firepower Management Center（FMC）を使用してネットワークに Firepower 1010 FTD を展開する方法、および初期設定の実行方法について説明します。

重要 Firepower 1010 は、Cisco Firepower ソフトウェア バージョン 6.4 以降をサポートしています。

（注） **プライバシー収集ステートメント**：Firepower 1010 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。

この章の対象読者

この章では、Firepower Threat Defense（FTD）デバイスの初期設定の実行方法および Firepower Management Center（FMC）へのデバイスの登録方法について説明します。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。

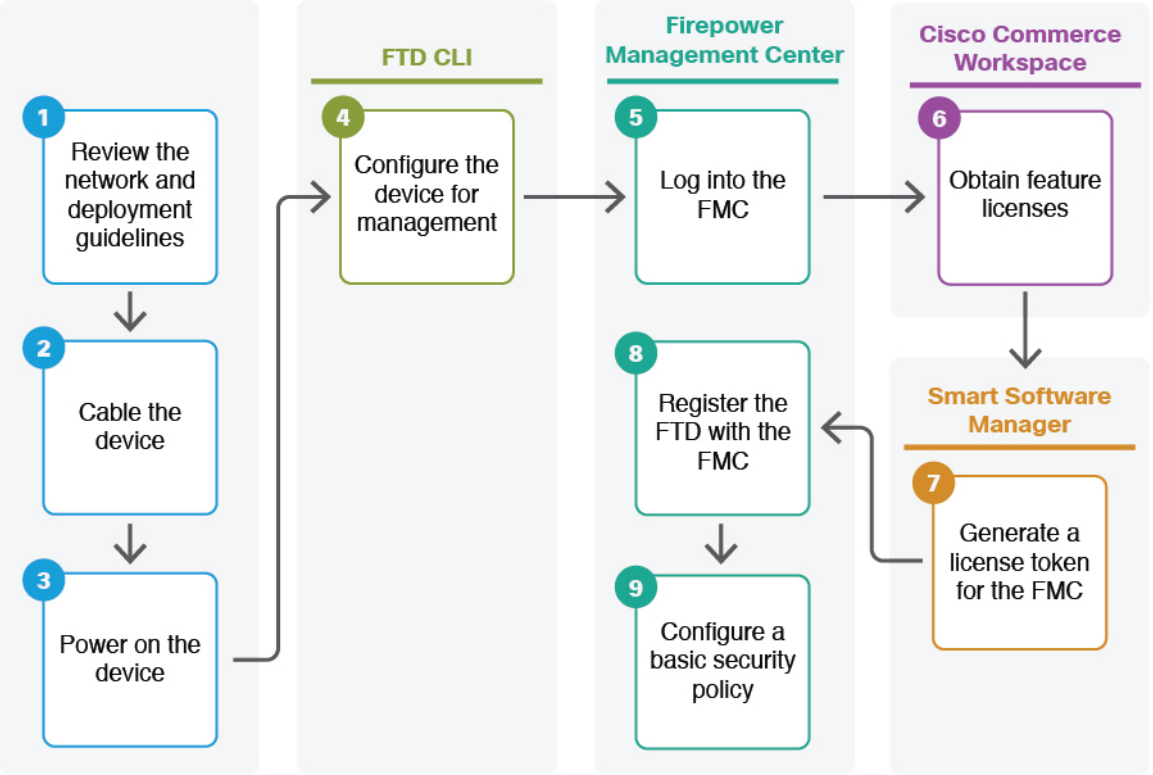
単一またはごく少数のデバイスのみが含まれるネットワークでは、FMC のような高性能の多機能デバイス マネージャを使用する必要がなく、一体型の Firepower Device Manager（FDM）を使用できます。FDM の Web ベースのデバイス セットアップ ウィザードを使用して、小規模ネットワークの導入に最もよく使用されるソフトウェアの基本機能を設定できます（「*FDM* を使用した *Firepower Threat Defense* の展開」を参照）。

はじめる前に

FMCの初期設定を展開して実行します。『FMCスタートアップガイド』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。



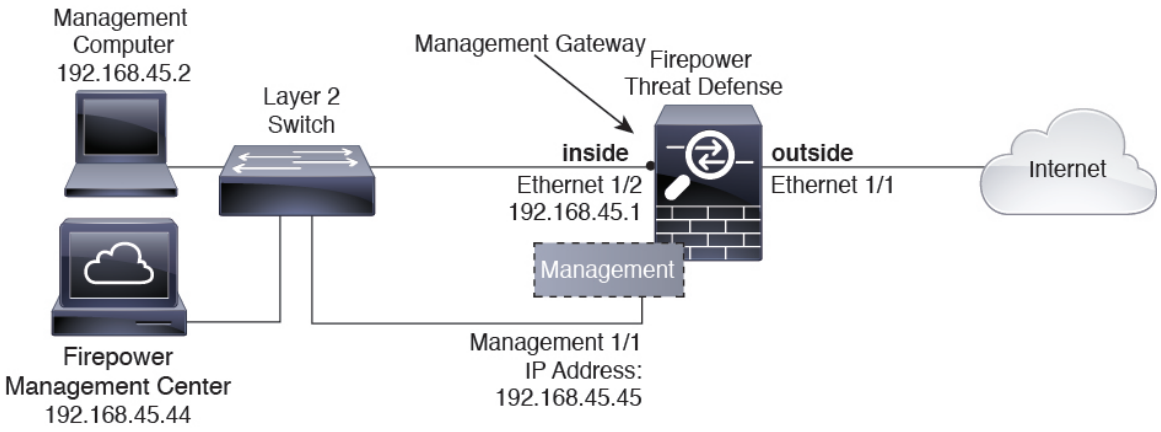
	1	ネットワーク配置と設定に関する注意事項の確認 （4 ページ）。
	2	デバイスの配線 （5 ページ）。
	3	デバイスの電源投入。
FTD CLI	4	Firepower Management 用のデバイス設定 （6 ページ）。
Firepower Management Center	5	Firepower Management Center へのログイン （10 ページ）。
Cisco Commerce Workspace	6	Firepower Management Center のライセンス取得 （11 ページ）：機能ライセンスを購入します。
Smart Software Manager	7	Firepower Management Center のライセンス取得 （11 ページ）： 1. FMC のライセンス トークンを生成します。 2. スマート ライセンシング サーバに FMC を登録します。
Firepower Management Center	8	Firepower Management Center を使用した Firepower Threat Defense の登録 （12 ページ）

Firepower Management Center	9	基本的なセキュリティ ポリシーの設定 （15 ページ）

ネットワーク配置と設定に関する注意事項の確認

次の図に、Firepower 1010 アプライアンスでの FMC を使用した Firepower Threat Defense の推奨のネットワーク配置を示します。

図 *1:* 推奨されるネットワーク配置



Firepower 1010 の設定に関する注意事項

設定例では、次の動作によって上記のネットワーク導入を有効化します。

（注） 導入には、別々の内部スイッチを使用する必要があります。

- **内部 --> 外部**へのトラフィック フロー
- **DHCP** からの**外部 IP** アドレス
- **内部**上のクライアントに対する **DHCP**。
- **管理 1/1** は FTD デバイスを設定し、FMC に登録するために使用されます。

  管理インターフェイスは、更新にインターネットアクセスが必要です。内部インターフェイスと同じネットワーク上に管理インターフェイスを配置すると、内部のスイッチのみを持つ FTD デバイスを導入して、内部インターフェイスをそのゲートウェイとして指定できます。

  物理的な管理インターフェイスは、Management 論理インターフェイスと Diagnostic 論理インターフェイス間で共有されます。Firepower Management Center コンフィギュレーション ガイド の「*Interfaces for Firepower Threat Defense*」の章を参照してください。

- **内部インターフェイス上での FMC アクセス**

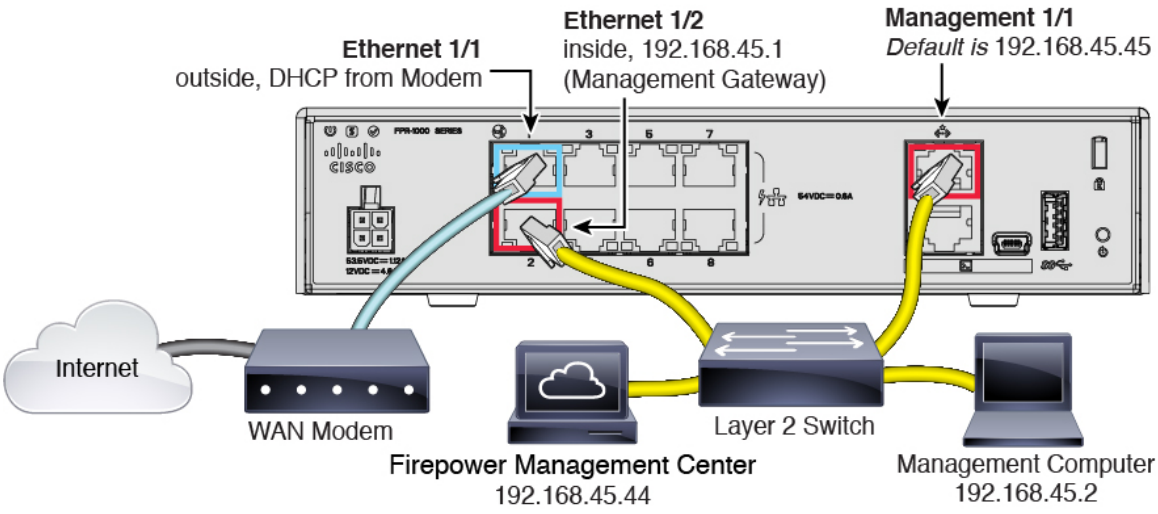
  内部ネットワーク上に別のルータを導入すると、管理と内部インターフェイスの間でルーティングできます。別の導入設定例については、Firepower Management Center コンフィギュレーション ガイド の「*Interfaces for Firepower Threat Defense*」の章を参照してください。

デバイスの配線

推奨の導入では、特定のインターフェイスが内部および外部ネットワークに使用されると仮定しています。これらの前提に基づいてネットワーク ケーブルをインターフェイスに接続すると、初期設定の実行が容易になります。

FP1010 における上記シナリオのケーブル配線については、レイヤ 2 スイッチを使用する簡単なトポロジを示している次の図を参照してください。他のトポロジの使用も可能であり、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。

図 *2 : Firepower 1010* のケーブル配線



手順

ステップ 1 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。

a) イーサネット 1/2 インターフェイス（内部）
b) Management 1/1 インターフェイス（Firepower Management Center 用）
c) ローカルの管理コンピュータ

管理インターフェイスは Firepower Management のみに属する独立したデバイスとして動作するため、内部インターフェイスと管理インターフェイスを同じネットワーク上で接続できます。

ステップ 2 Ethernet 1/1（外部）インターフェイスを ISP/WAN モデムまたはその他の外部デバイスに接続します。デフォルトでは、IP アドレスは DHCP を使用して取得しますが、初期設定時にスタティック アドレスを設定することもできます。

デバイスの電源投入

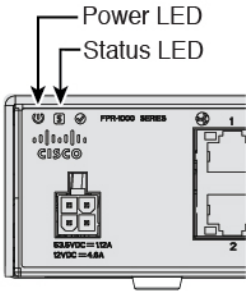
システムの電源は電源コードで制御されます。電源ボタンはありません。

手順

ステップ 1 電源コードをデバイスに接続し、電源コンセントに接続します。

電源コードを差し込むと電源が自動的に入ります。

ステップ 2 デバイスの背面または上部にある電源 LED を確認します。緑色に点灯している場合は、デバイスの電源が入っています。



ステップ 3 デバイスの背面または上部にあるステータス LED を確認します。緑色に点灯している場合は、電源投入時診断に合格しています。

Firepower Management 用のデバイス設定

最初に CLI にアクセスするときに、セットアップ ウィザードによって、Firepower Threat Defense デバイスの設定に必要な基本のネットワーク設定パラメータのプロンプトが表示され、Firepower Management Center（FMC）への登録が要求されます。管理 IP アドレスと関連するゲートウェイ ルートは、インターフェイス リストの FMC Web インターフェイスまたはデバイスのスタティック ルートには**含まれていません**。これらは、セットアップ スクリプトおよび CLI でのみ設定できます。

始める前に

- データ インターフェイスがゲートウェイ デバイス（たとえば、ケーブル モデムやルータなど）に接続されていることを確認します。エッジの導入では、これはインターネット向

けのゲートウェイになります。データセンター導入の場合は、これがバックボーン ルータになります。

- Management インターフェイスは、インターネットにアクセスできるゲートウェイに接続する必要もあります。システムのライセンスおよびデータベースのアップデートにインターネット アクセスが必要です。

手順

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

- モニタとキーボードが取り付けられたデバイスの場合は、コンソールからログインします。
- デバイスの管理インターフェイスへのアクセスでは、管理インターフェイスのデフォルト IPv4 アドレス（192.168.45.45）に SSH を実行します。

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

ステップ 3 Firepower Threat Defense システムが起動すると、セットアップ ウィザードでシステムの設定に必要な次の情報の入力が求められます。

- 使用許諾契約の同意
- 新しい管理者パスワード
- IPv4 または IPv6 の構成
- IPv4 または IPv6 の DHCP 設定
- 管理ポートの IPv4 アドレスとサブネット マスク、または IPv6 アドレスとプレフィックス。

  管理 1/1 インターフェイスで DHCP サーバを有効にして、管理 PC などの管理デバイスに IP アドレスを指定できます。
- システム名
- デフォルト ゲートウェイの IPv4、IPv6、またはその両方。

  上記の設定例では、計画済みの内部インターフェイス IP アドレスをゲートウェイ アドレスとして識別します。このインターフェイスおよびその他のインターフェイス IP アドレスについては、後に FMC で設定します。FMC が別の内部ネットワークにある場合は、ネットワークの設定に応じて、内部ルータの IP アドレスがゲートウェイとして識別されます。
- DNS セットアップ
- HTTP プロキシ
- 管理モード

Firepower Device Manager を使用して、デバイスをローカルで管理するかどうかを尋ねられます。FMC を使用するには no と応答します。

ステップ 4 セットアップ ウィザードの設定を確認します。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。

例：

```
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]: y
Do you want to configure IPv6? (y/n) [n]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]: manual
Enter an IPv4 address for the management interface [192.168.45.45]: 10.133.128.47
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.248.0
Enter the IPv4 default gateway for the management interface []: 10.133.128.1
Enter a fully qualified hostname for this system [firepower]: laurel.example.com
Enter a comma-separated list of DNS servers or 'none' []: 10.33.16.6
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
```

ステップ 5 新しいログイン クレデンシャルを使用して、アプライアンスに再接続します。

ステップ 6 ファイアウォール モードを設定します。次に例を示します。

例：

```
Configure firewall mode? (routed/transparent) [routed]
```

（注） 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。デフォルトモードは**ルーテッド**です。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。詳細については、次のマニュアルの「Transparent or Routed Firewall Mode for Firepower Threat Defense」の章を参照してください。Firepower Management Center コンフィギュレーション ガイド

ステップ 7 デフォルトのシステム設定が処理されるのを待ちます。数分かかることがあります。

例：

```
Update policy deployment information
    - add device configuration

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

When registering the sensor to a Management Center, a unique alphanumeric
registration key is always required.  In most cases, to register a sensor
```

```
to a 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 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 Management Center, you must use the same
registration key and, if necessary, the same NAT ID when you add this
sensor to the Management Center.
```

ステップ 8 Firepower Threat Defense デバイスを管理 FMC に登録します。

例：

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

引数の説明

- {hostname | IPv4_address | IPv6_address | DONTRESOLVE} では、FMC の完全修飾ホスト名または IP アドレスを指定します。FMC を直接アドレス指定できない場合は、**DONTRESOLVE** を使用します。
- *reg_key* は、デバイスを FMC に登録するために必要な一意の英数字の登録キーです。

  （注） 登録キーは、ユーザが生成した 1 回限り使用できる一意のキーで、37 文字を超えてはなりません。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。デバイスを FMC に追加するときに、この登録キーを思い出す必要があります。

- *nat_id* は、一方が IP アドレスを指定しない場合に、FMC とデバイス間の登録プロセス中に使用されるオプションの英数字文字列です。hostname が DONTRESOLVE に設定されている場合に必要です。FMC で同じ NAT ID を入力します。

  （注） NAT ID は、ユーザ生成の 1 回しか使用できないキーで、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。デバイスを FMC に追加する際には、この ID を思い出す必要があります。

例：

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

Firepower Threat Defense デバイスと FMC が NAT デバイスによって分離されている場合は、次のように、登録キーと一緒に一意の NAT ID 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 my_reg_key my_nat_id
Manager successfully configured.
```

FMC およびデバイスでは、初期登録の認証と承認に、登録キーおよびNAT ID（IP アドレスではなく）を使用します。NAT ID は、最初の通信に対する信頼を確立し、正しい登録キーを検索するために、管理対象アプライアンスの登録に使用するすべての NAT ID の中で一意である**必要があります**。

（注） FMC または Firepower Threat Defense のいずれかのセキュリティ アプライアンスのうちの少なくとも 1 つは、2 つのアプライアンス間で双方向の SSL 暗号化通信チャネルを確立するために、パブリック IP アドレスを持つ必要があります。

ステップ 9 CLI を閉じます。

例：

```
> exit
```

次のタスク

次の項の説明に従って、デバイスを FMC に登録します。

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*

- *fmc_ip_address*：FMC の IP アドレスまたはホスト名を指定します。

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
- **AMP**：ネットワークの高度なマルウェア防御（AMP）
- **URL**：URL フィルタリング

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。

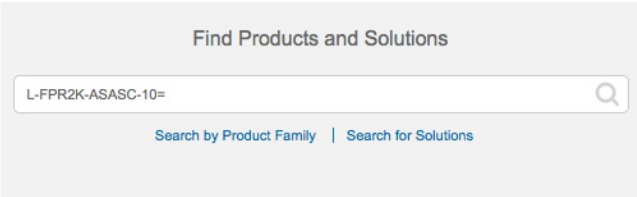
手順

ステップ 1 お使いのスマート ライセンス 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 [Find Products and Solutions] 検索フィールドを使用します。次の組み合わせライセンス PID を検索します。また、昨日ごとに個々のライセンスおよびサブスクリプション（リストに含まれていない）を購入することもできます。

（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。

図 *3*：ライセンス検索



- 脅威、AMP、および URL ライセンスの組み合わせ：

- 脅威、AMP、および URL サブスクリプションの組み合わせ：

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コンフィギュレーション ガイド』を参照してください。

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

FTD を FMC に登録します。

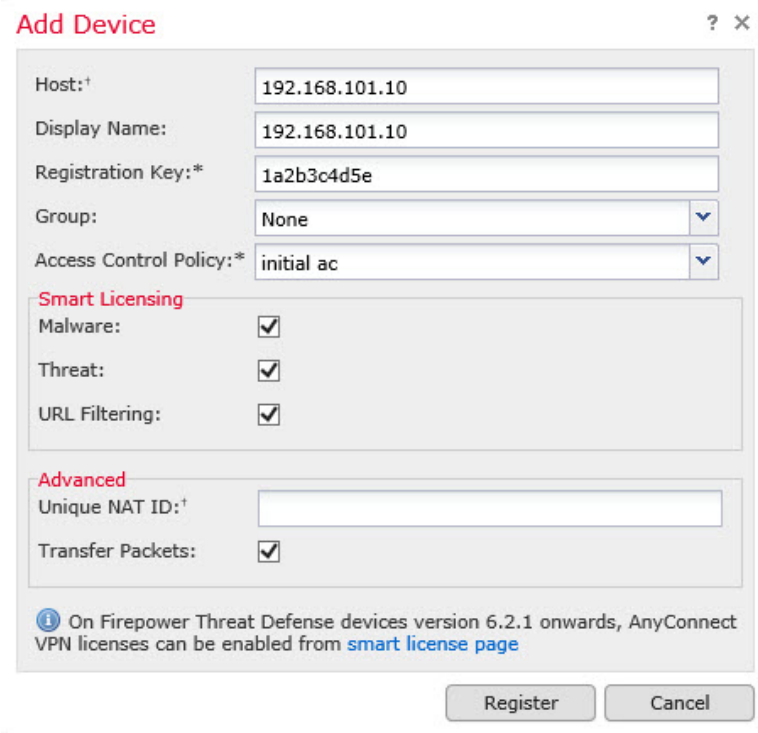
始める前に

- FTD の最初の設定で設定した次の情報を収集します。
  - FTD 管理 IP アドレスまたは NAT ID
  - FMC 登録キー

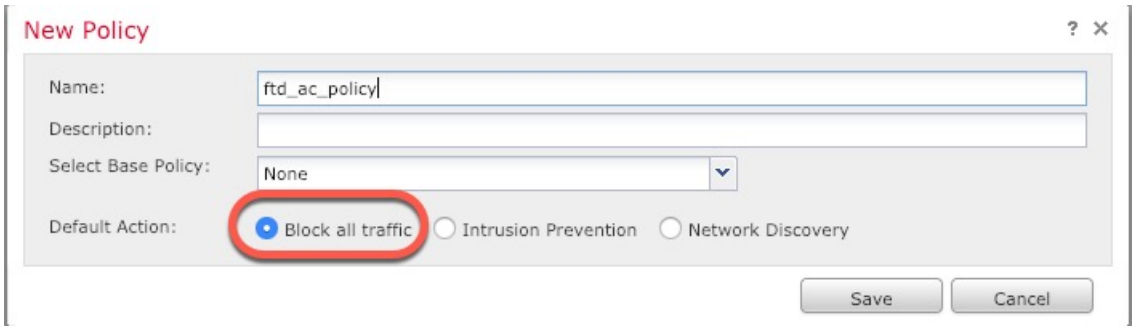
手順

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。「アクセス制御の設定 （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。

- 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。

ステップ 1	インターフェイスの設定 （15 ページ）。
ステップ 2	DHCP サーバの設定 （19 ページ）。
ステップ 3：	デフォルト ルートの追加 （20 ページ）。
ステップ 4：	NAT の設定 （21 ページ）。
ステップ 5	アクセス制御の設定 （24 ページ）。
ステップ 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、それらにセキュリティ 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。

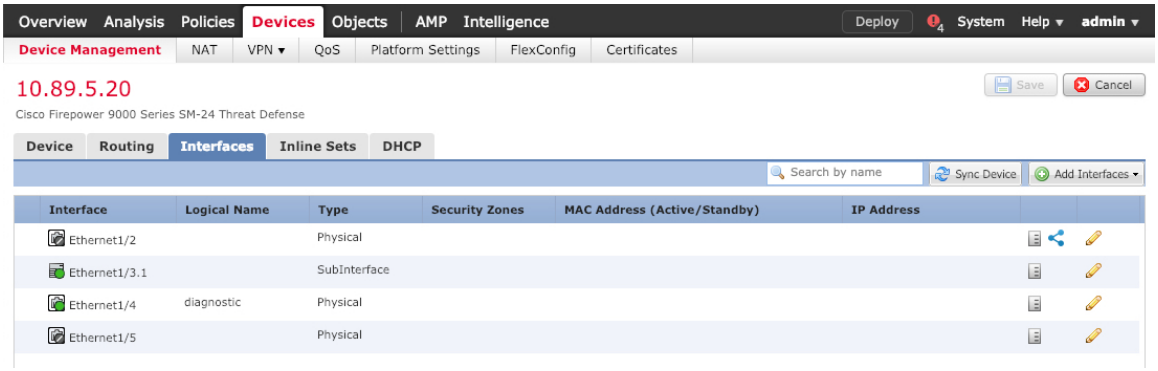
一般的なエッジルーティングの状況は、内部インターフェイスでスタティック アドレスを定義すると同時に、ISP から DHCP を介して外部インターフェイス アドレスを取得することです。

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

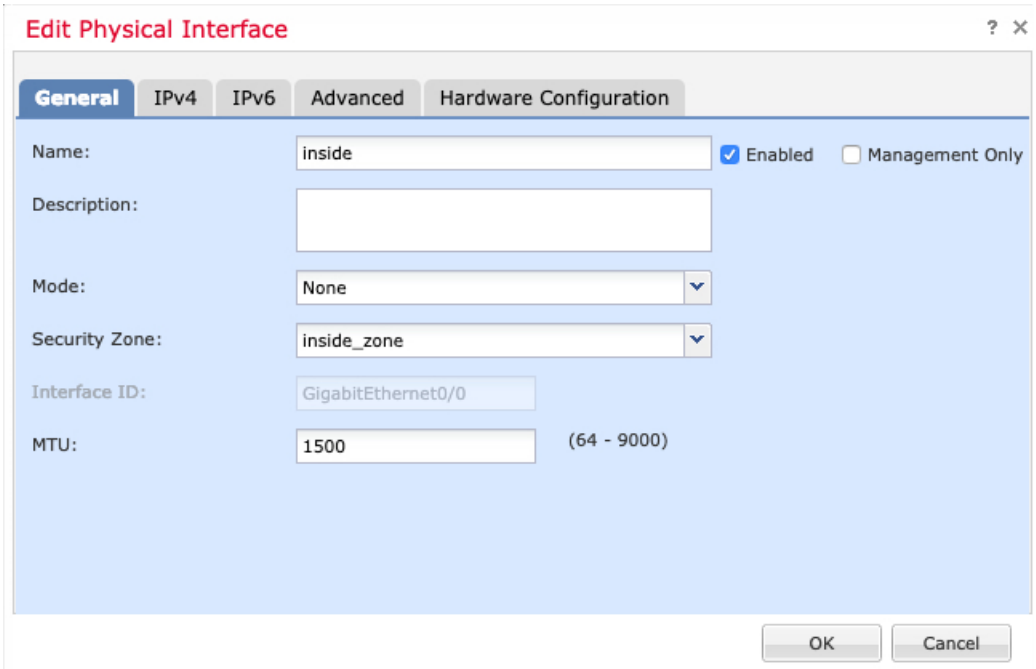
ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、デバイスの編集アイコン（✎）をクリックします。

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編集アイコン（✎）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。

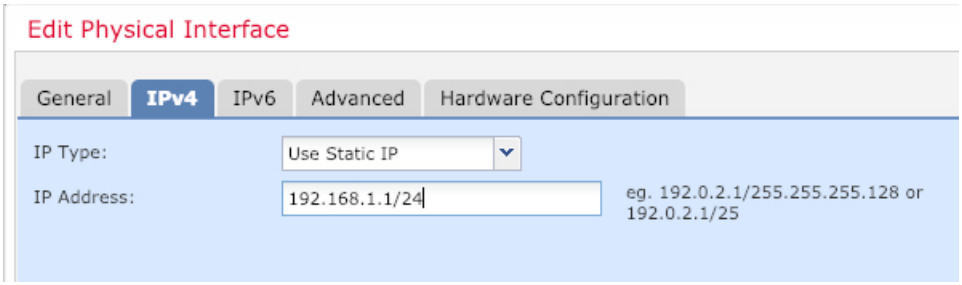
d) [セキュリティ ゾーン（Security Zone）] ドロップダウン リストから既存の内部セキュリティ ゾーンを選択するか、[新規（New）] をクリックして新しいセキュリティ ゾーンを追加します。

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 [静的 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。

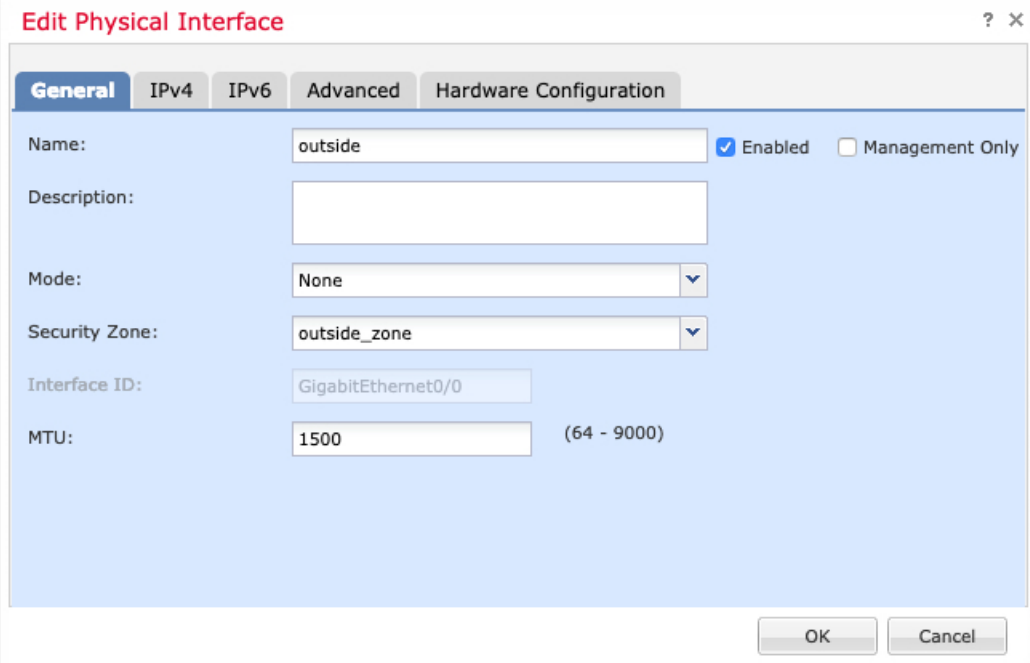


- [IPv6]：ステートレス自動設定の場合は [自動設定（Autoconfiguration）] チェック ボックスをオンにします。

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編集アイコン（✎）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。

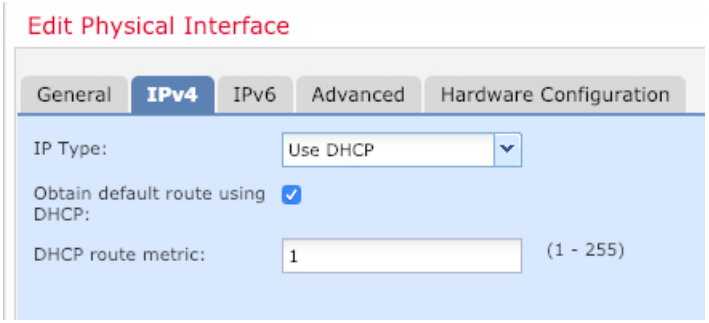
c) [モード（Mode）] は [なし（None）] に設定したままにします。

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

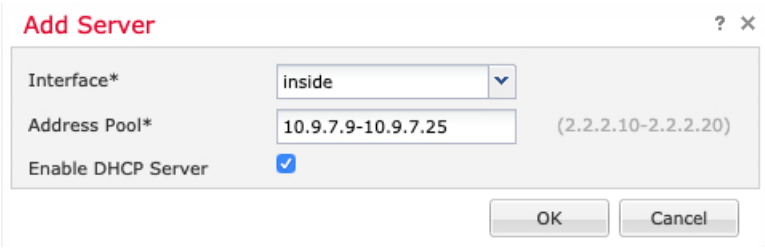
クライアントで DHCP を使用して FTD から IP アドレスを取得するようにする場合は、DHCP サーバを有効にします。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、デバイスの編集アイコン（✎）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。

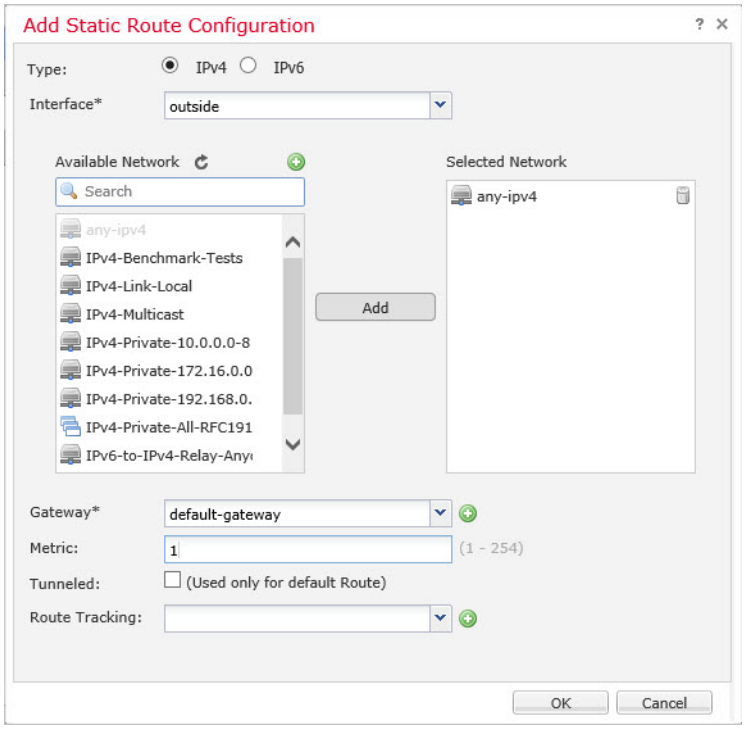
デフォルト ルートの追加

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、デバイスの編集アイコン（✎）をクリックします。

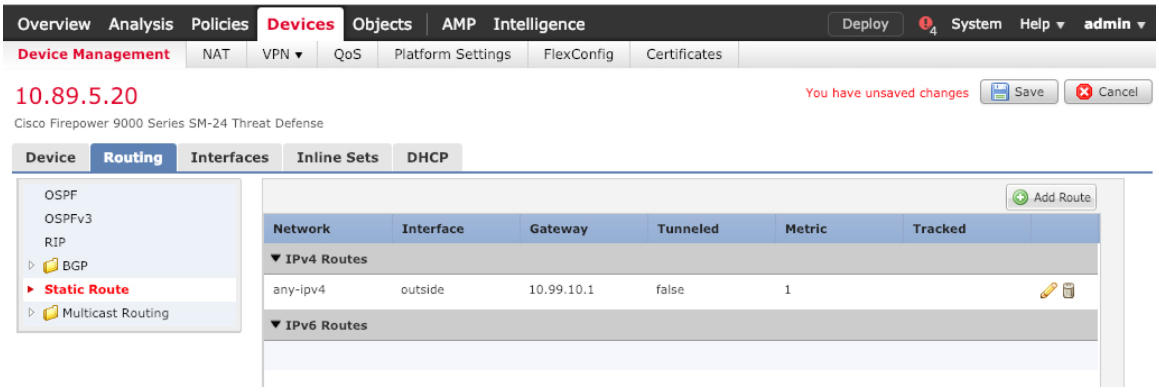
ステップ 2 **[ルーティング（Routing）] > [スタティックルート（Static route）]** を選択し、[ルートを追加（Add route）] をクリックして、次のように設定します。



- [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。

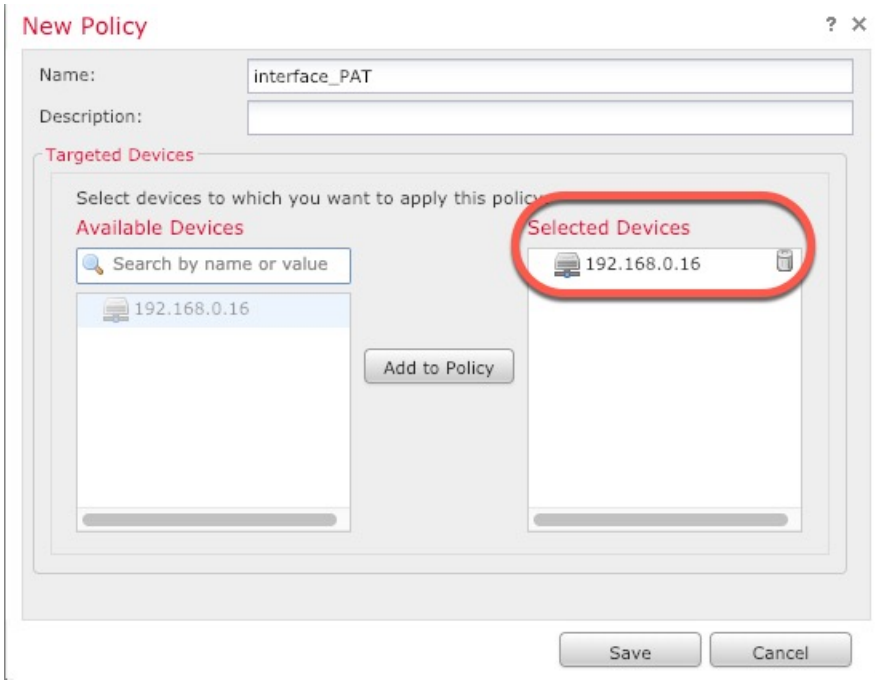
NAT の設定

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。

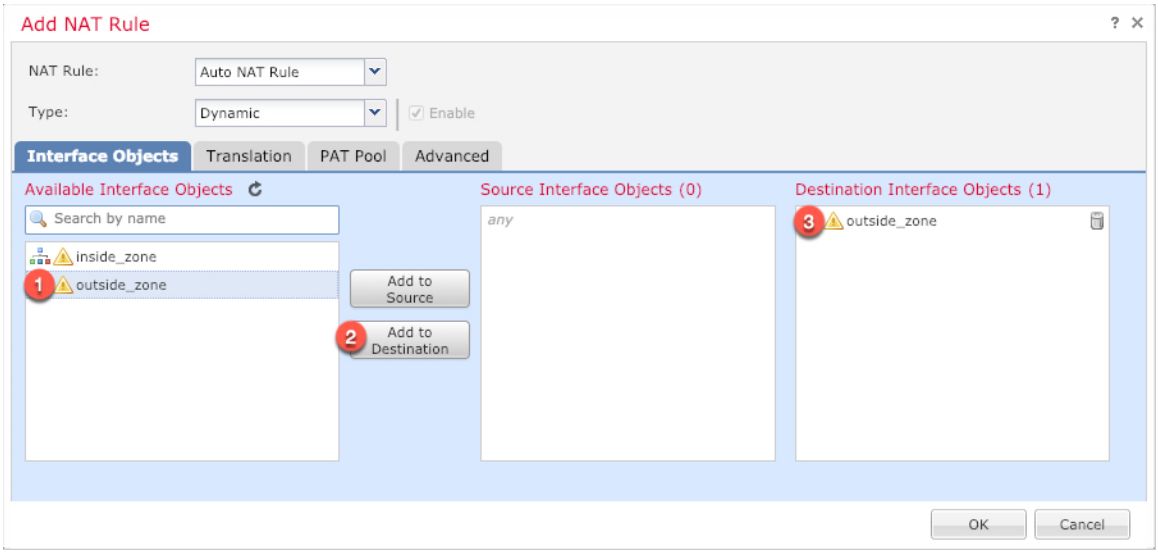
ステップ 3 [ルールの追加（Add Rule）] をクリックします。

[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。

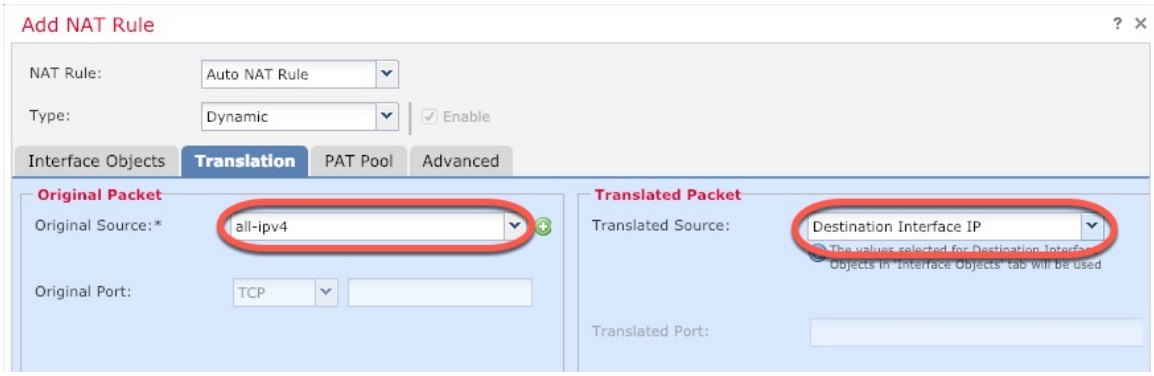
ステップ 4 基本ルールのオプションを設定します。

- [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。

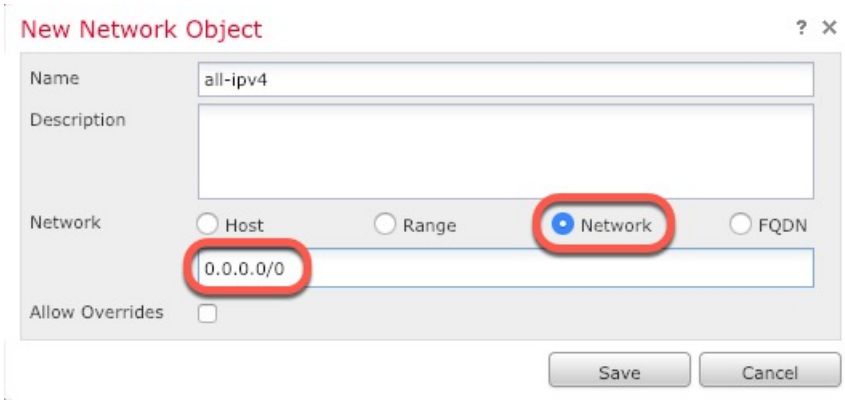
ステップ 5 [インターフェイスオブジェクト（Interface objects）] ページで、[使用可能なインターフェイスオブジェクト（Available Interface Objects）] 領域から [宛先インターフェイスオブジェクト（Destination Interface Objects）] 領域に外部ゾーンを追加します。



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）]：追加アイコン（⊕）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。

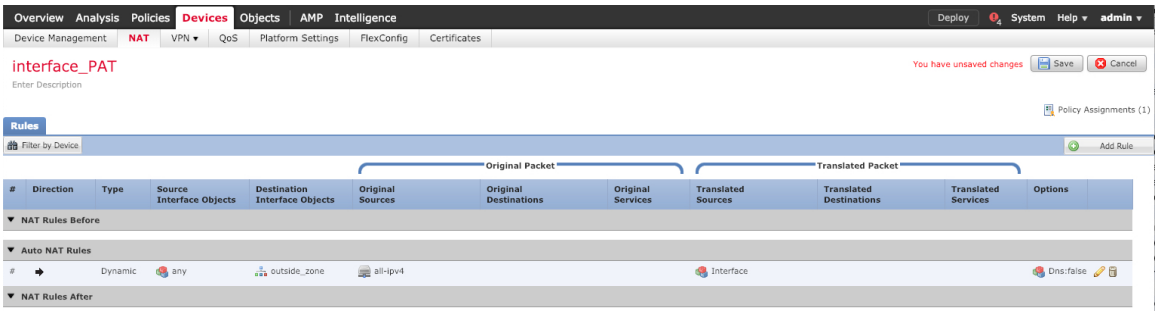


（注） 自動 NAT ルールはオブジェクト定義の一部として NAT を追加するため、システム定義の **any-ipv4** オブジェクトを使用することはできません。また、システム定義のオブジェクトを編集することはできません。

- [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。

アクセス制御の設定

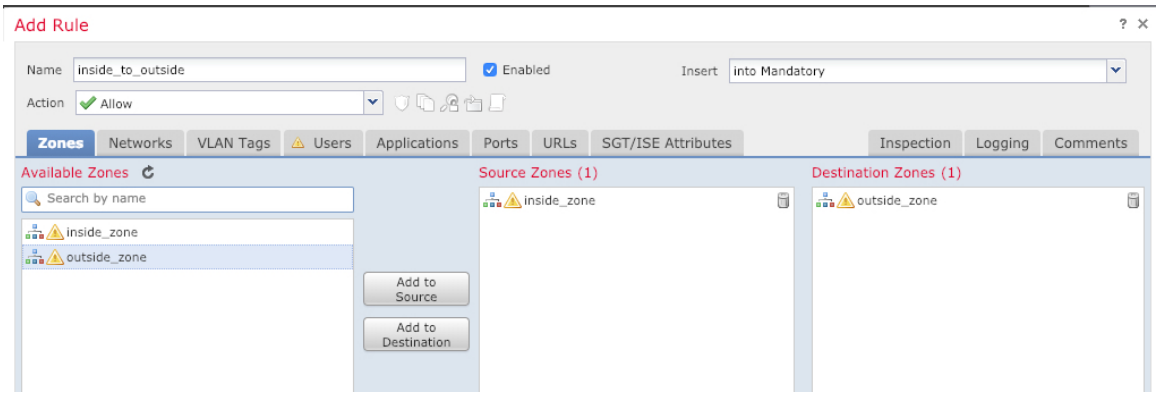
FTD を FMC に登録したときに、基本の [すべてのトラフィックをブロック（Block all traffic）] アクセス コントロール ポリシーを作成した場合は、デバイスを通過するトラフィックを許可するためにポリシーにルールを追加する必要があります。次の手順では、内部ゾーンから外部ゾーンへのトラフィックを許可するルールを追加します。他にゾーンがある場合は、適切なネットワークへのトラフィックを許可するルールを追加してください。

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設定ガイド』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 ポリシーの編集アイコン（）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。

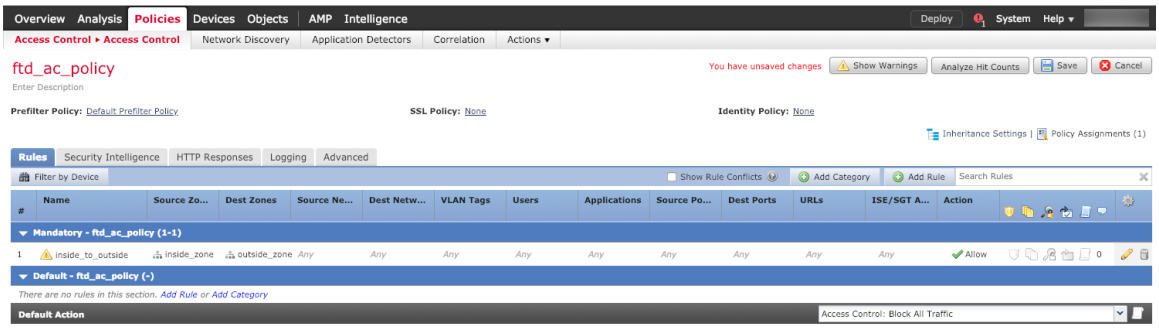


- [名前（Name）]：このルールに名前を付けます（たとえば、「inside_to_outside」）。
- [送信元ゾーン（Source Zones）]：[使用可能なゾーン（Available Zones）] から内部ゾーンを選択し、[送信元に追加（Add to Source）] をクリックします。
- [宛先ゾーン（Destination Zones）]：[使用可能なゾーン（Available Zones）] から外部ゾーンを選択し、[宛先に追加（Add to Destination）] をクリックします。

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。



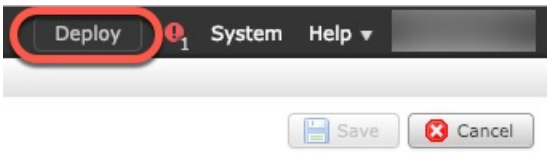
ステップ 4 [保存（Save）] をクリックします。

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。

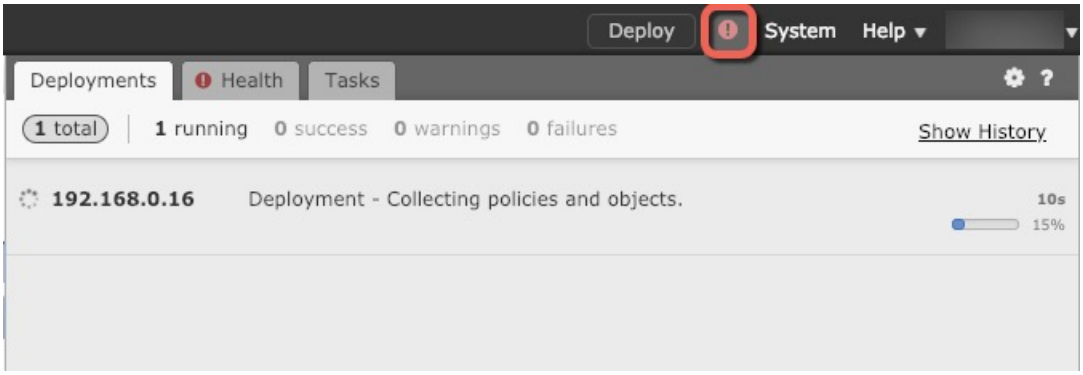
手順

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。



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。

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。SSH 接続用のインターフェイスを開いている場合、データ インターフェイス上のアドレスにも接続できます。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。

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

始める前に

管理ポートの位置、コンソール ポート、電源コード、関連する LED の情報など、シャーシ コンポーネントの詳細については、ご使用のデバイスのハードウェア ガイドを参照してください。

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。コンソール ケーブルの詳細については、デバイスのハードウェア ガイドを参照してください。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

注目 コンソール ポートの CLI は FXOS です。

ステップ 2 プロンプトで、FXOS CLI にログインします。

例：

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

ciscofirepower#
```

ステップ 3 FTD CLI にアクセスします。

connect ftd

例：

```
ciscofirepower# 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。使用法の詳細については、*Cisco Firepower Threat Defense* コマンド リファレンス [英語] を参照してください。

ステップ 4 FTD CLI を終了するには、**exit** または **logout** コマンドを入力します。

例：

```
> exit
ciscofirepower#
```

（注） これで、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。使用法の詳細については、*Cisco Firepower FXOS コマンド リファレンス* [英語] を参照してください。

デバイスの電源切断

Firepower 1010 シャーシには外部電源スイッチはありません。そのため、FTD CLI を使用して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、重大ンなファイル 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、Firepower 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。

Firepower デバイスの電源を切断する必要がある場合は、このトピックの手順に従ってください。

（注） この手順では、初回ログイン時にデフォルトの **admin** ユーザを使用して初期設定プロセスを完了していると仮定しています。

始める前に

Firepower デバイスの電源を切断する前に、次の手順を実行します。

- Firepower ネットワーク データ ポートに接続されているデバイスをシャットダウンまたは切断する必要があるか判断します。
- 管理ポートの位置、コンソール ポート、電源装置、関連する LED の情報など、シャーシコンポーネントの詳細については、ご使用のデバイスのハードウェア ガイドを参照してください。

手順

ステップ 1 管理コンピュータをシャーシの管理ポートまたはコンソール ポートに接続して、FTD CLI にアクセスします。

ステップ 2 コンソール ポートから、または SSH を使用して、FTD CLI に接続します。

- 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。SSH 接続用のインターフェイスを開いている場合、データ インターフェイス上のアドレスにも接続できます。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。
- デバイスのコンソール ポートに直接接続できます。デバイスに付属のコンソール ケーブルを使用し、9600 ボー、8 データ ビット、パリティなし、1 ストップ ビット、フロー制御

なしに設定されたターミナル エミュレータを用いて PC をコンソールに接続します。コンソール ケーブルの詳細については、デバイスのハードウェア ガイドを参照してください。

ステップ 3 **admin** のユーザ名とパスワードでログインします。

（注） コンソール ポートの CLI は FXOS です。FTD CLI には、**connect ftd** コマンドを使用してアクセスできます。FXOS CLI はシャーシ レベルの設定およびトラブルシューティングにのみ使用します。基本設定、モニタリング、およびシステムの通常のトラブルシューティングには FTD CLI を使用します。FXOS コマンドの詳細については、FXOS のマニュアルを参照してください。

ステップ 4 デバイスの電源を切断するには、CLI プロンプト（>）で **shutdown** コマンドを使用します。

例：

```
> shutdown
This command will shutdown the system. Continue?
Please enter 'YES' or 'NO': YES
```

このコマンドは、Firepower システムをグレースフル シャットダウンします。

ステップ 5 電源 LED とステータス LED を観察して、シャーシの電源が切断されていることを確認します（LED が消灯）。

ステップ 6 シャーシの電源が正常に切断されたら、必要に応じて電源プラグを抜き、シャーシから物理的に電源を取り外すことができます。