FDM を使用した Firepower Threat Defense の展開

この章の対象読者

この章では、Firepower Device Manager（FDM）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。高可用性ペアを展開する場合は、FDM の設定ガイドを参照してください。

FDM FDM では、小規模ネットワークで最も一般的に使用されるソフトウェアの基本機能を設定できます。また、これは多くの FDM デバイスを含む大規模なネットワークを制御するために強力な複数デバイスのマネージャを使用することがない、単一のデバイスまたは限られた数のデバイスを含むネットワークのために特に設計されています。

多数のデバイスを管理している場合、または FTD で許可される、より複雑な機能や設定を使用する場合は、代わりに Firepower Management Center （FMC）を使用します。

（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。

FDM を使用した Firepower Threat Defense の概要

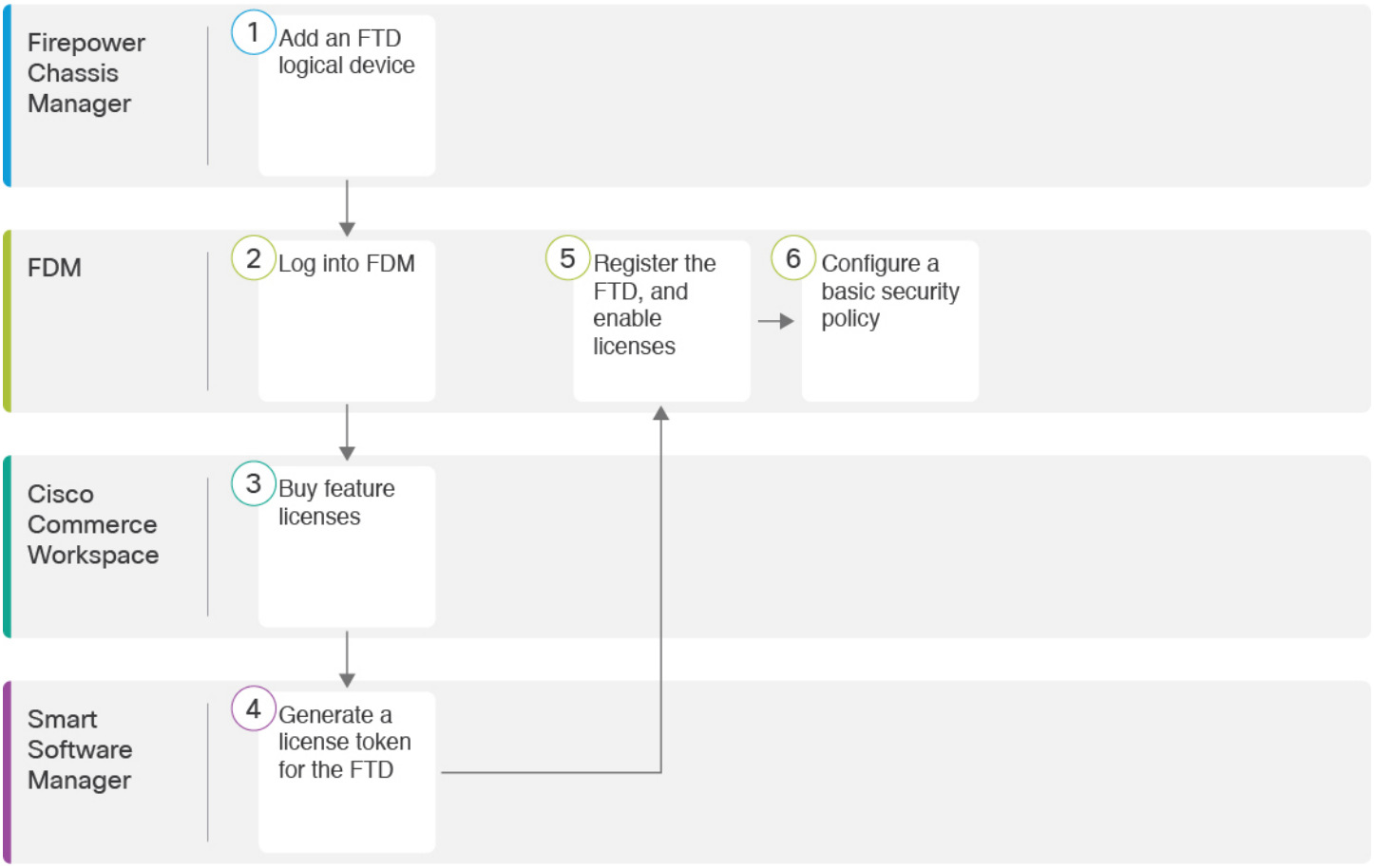
FTD は、ステートフル ファイアウォール、ルーティング、VPN、Next-Generation Intrusion Prevention System（NGIPS）、Application Visibility and Control（AVC）、URL フィルタリング、高度なマルウェア防御（AMP）などの次世代ファイアウォールサービスを提供します。

Firepower Device Manager（FDM）（デバイスに含まれる簡素化された単一のデバイスマネージャ）を使用して FTD を管理できます。FTD の論理デバイスに割り当てた管理インターフェイスに HTTPS を使用します。

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。

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。 （3 ページ）。
2	FDM	FDM へのログイン （7 ページ）。
3	Cisco Commerce Workspace	ライセンスの設定 （8 ページ）：機能ライセンスを購入します。
4	Smart Software Manager	ライセンスの設定 （8 ページ）：FTD のライセンストークンを生成します。
5	FDM	ライセンスの設定 （8 ページ）：FTD をスマート ライセンシング サーバに登録し、機能ライセンスを有効にします。
6	FDM	基本的なセキュリティポリシーの設定 （14 ページ）。

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

FTD をネイティブインスタンスとして Firepower 4100 から展開できます。コンテナ インスタンスはサポートされていません。

ハイアベイラビリティペアを追加する場合は、『FDM configuration guide』を参照してください。

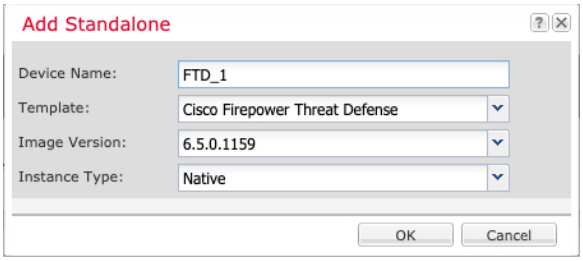
始める前に

- 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。
- 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
  - DNS サーバの IP アドレス
  - FTD ホスト名とドメイン名

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。

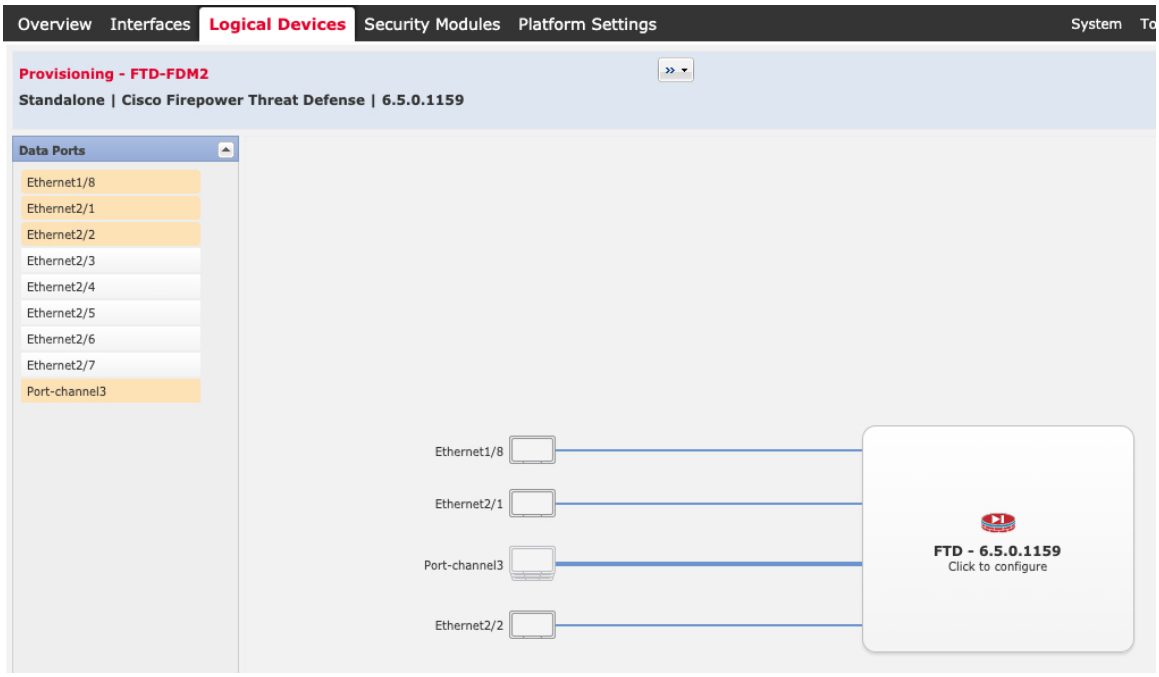
d) [Instance Type] で [Native] を選択します。

コンテナインスタンスは FDM ではサポートされていません。

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。

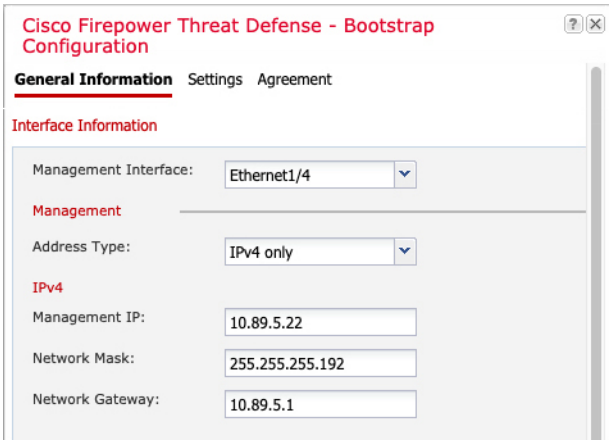


以前に[インターフェイス（Interfaces）]ページで有効にしたデータインターフェイスのみを割り当てることができます。後で、FDM でこれらのインターフェイスを有効にして設定します。これには IP アドレスの設定も含まれます。

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) [Management Interface] を選択します。

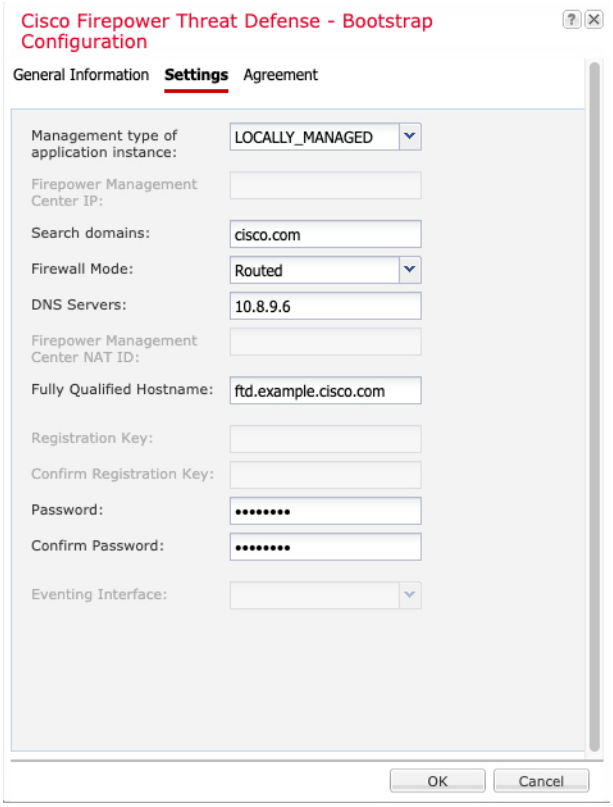
このインターフェイスは、論理デバイスの管理に使用されます。このインターフェイスは、シャーシ管理ポートとは別のものです。

b) 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]。
c) [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。

d) [Network Mask] または [Prefix Length] に入力します。
e) **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 [Settings] タブで、次の手順を実行します。



a) [Management type of application instance] ドロップダウンリストで、[LOCALLY_MANAGED] 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 FMC もサポートしています。論理デバイスを展開した後にマネージャを変更すると、設定が消去され、デバイスが再初期化されます。

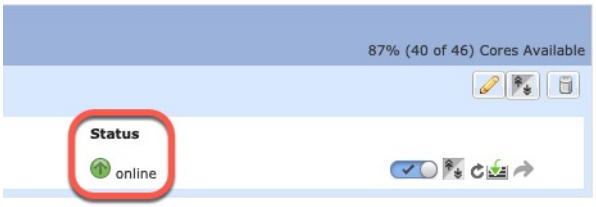
b) カンマ区切りリストとして [検索ドメイン（Search Domains）] を入力します。
c) [Firewall Mode] では [Routed] モードのみサポートされています。
d) [DNS Servers] をカンマ区切りのリストとして入力します。
e) FTD の [Fully Qualified Hostname] を入力します。
f) CLI アクセス用の FTD 管理ユーザの [Password] を入力します。

ステップ 7 [利用規約（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。



FDM へのログイン

FDM にログインして FTD を設定します。

始める前に

- Firefox、Chrome、Safari、Edge、または Internet Explorer の最新バージョンを使用します。
- Firepower Chassis Manager の [論理デバイス（Logical Devices）] ページで、ASA 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。

手順

ステップ 1 ブラウザに次の URL を入力します。

- **https://***management_ip*：ブートストラップ設定に入力した管理インターフェイスの IP アドレス。

ステップ 2 ユーザ名 admin、FTD の展開時に設定したパスワード、 を使用してログインします。

ステップ 3 90 日間の評価ライセンスに同意するように求められます。

ライセンスの設定

FTD は、ライセンスの購入およびライセンス プールの一元管理を可能にするシスコ スマート ソフトウェア ライセンシングを使用します。

シャーシを登録すると、License Authority によって シャーシと License Authority 間の通信に使用される ID 証明書が発行されます。また、適切な仮想アカウントにシャーシが割り当てられます。

基本ライセンスは自動的に含まれます。スマート ライセンシングでは、まだ購入していない製品機能を使用することはできませんが、次のオプション機能ライセンスを購入して準拠する必要があります。

- **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。

システムのライセンシングの詳細については、『FDM Configuration Guide』を参照してください。

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。

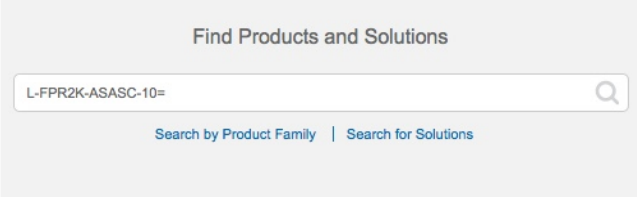
- （輸出コンプライアンス フラグを使用して有効化される）機能を使用するには、ご使用のシスコ スマート ソフトウェア ライセンシング アカウントで強力な暗号化（3DES/AES）ライセンスを使用できる必要があります。

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



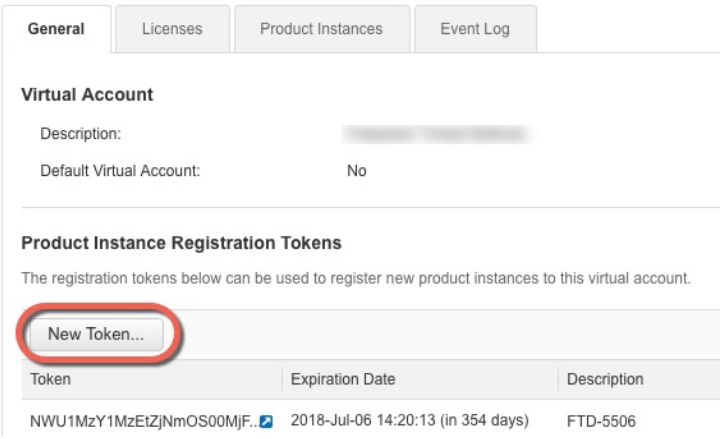
（注） PID が見つからない場合は、注文に手動で PID を追加できます。

- 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。

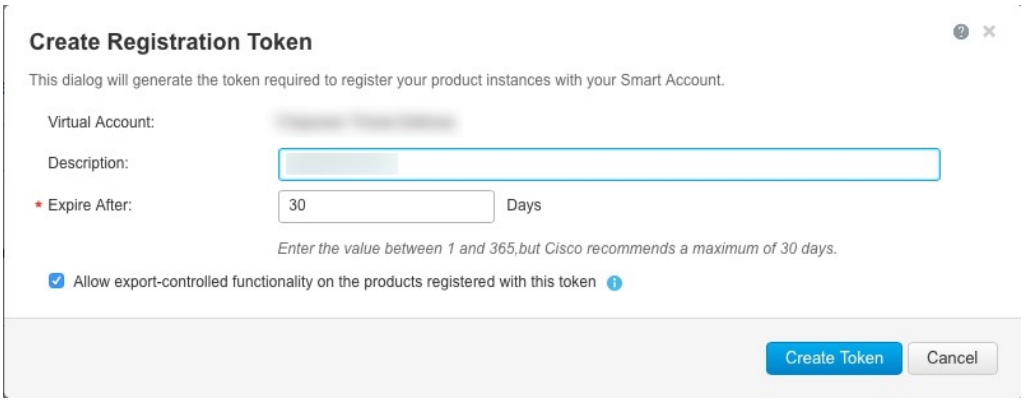
ステップ 2 Smart Software Manager で、このデバイスを追加する仮想アカウントの登録トークンを要求してコピーします。

a) [インベントリ（Inventory）] をクリックします。

b) [全般（General）] タブで、[新規トークン（New Token）] をクリックします。



c) [登録トークンを作成（Create Registration Token）] ダイアログボックスで、以下の設定値を入力してから [トークンを作成（Create Token）] をクリックします。



- **[説明（Description）]**
- [有効期限（Expire After）]：推奨値は 30 日です。
- [このトークンに登録された製品で輸出管理機能を許可する（Allow export-controlled functionality on the products registered with this token）]：高度暗号化が許可されている国の場合は輸出コンプライアンスフラグを有効にします。

トークンはインベントリに追加されます。

d) トークンの右側にある矢印アイコンをクリックして [Token] ダイアログボックスを開き、トークン ID をクリップボードにコピーできるようにします。FTD の登録が必要なときに後の手順で使用するために、このトークンを準備しておきます。

図 *2*: トークンの表示

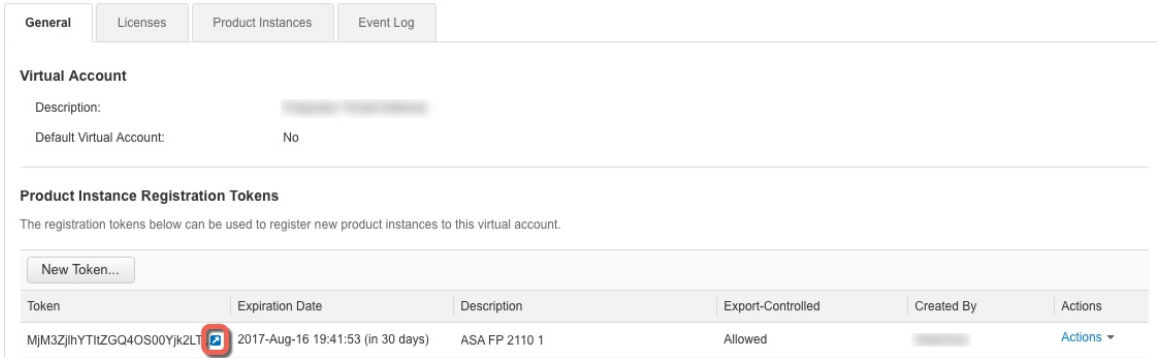
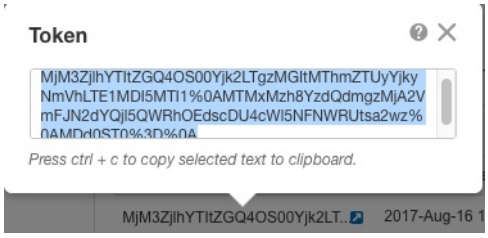


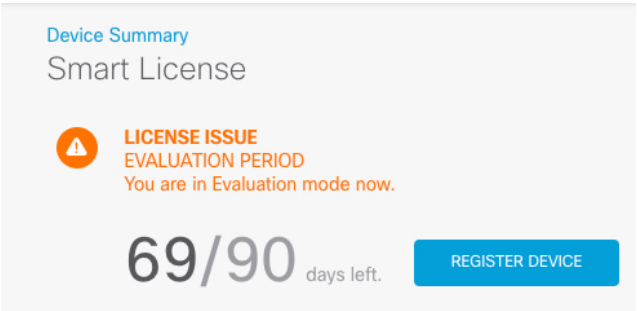
図 *3*: トークンのコピー



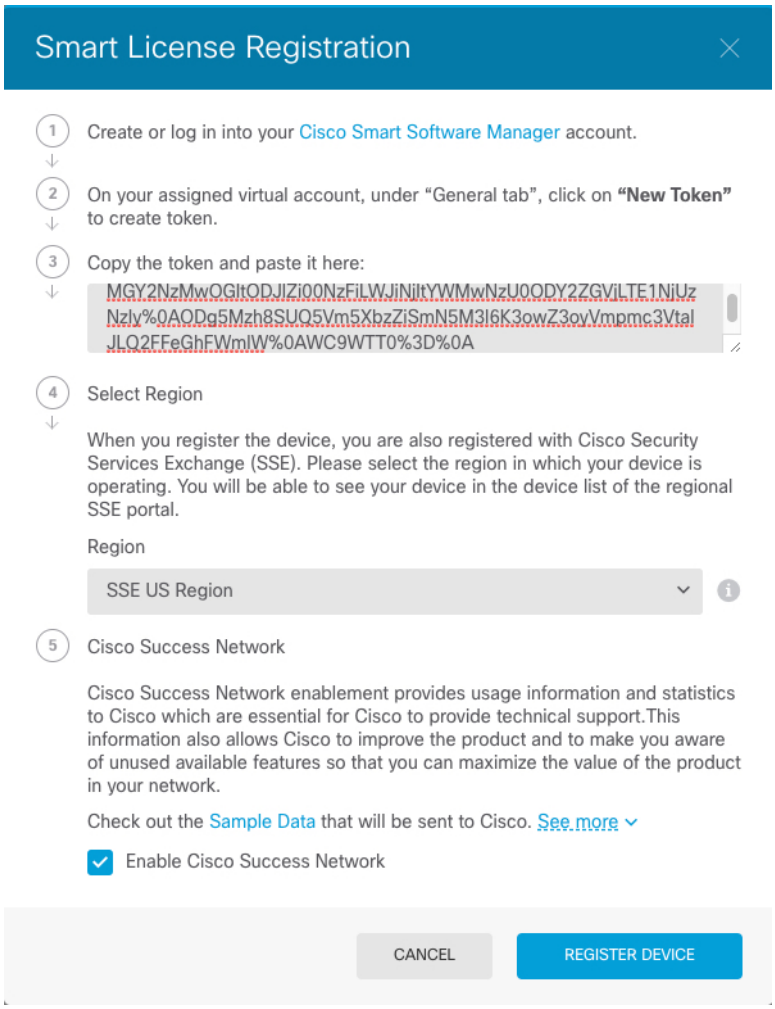
ステップ 3 FDM で、**[デバイス（Device）]** をクリックし、**[スマート ライセンス概要（Smart License summary）]** の **[設定の表示（View Configuration）]** をクリックします。

[スマート ライセンス（Smart License）] ページが表示されます。

ステップ 4 [デバイスの登録（Register Device）] をクリックします。

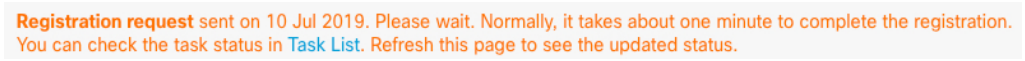


次に、[スマート ライセンス登録（Smart License Registration）] ダイアログボックスの指示に従って、トークンに貼り付けます。

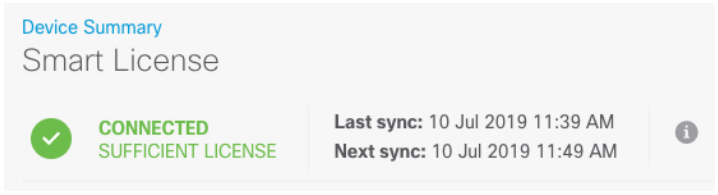


ステップ 5 [デバイスの登録（Register Device）] をクリックします。

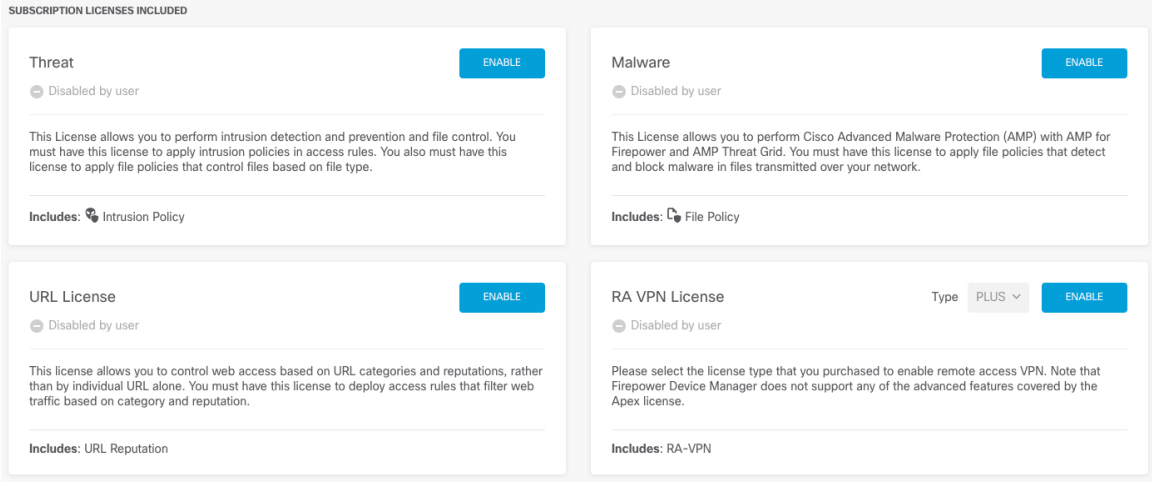
[スマート ライセンス（Smart License）] ページに戻ります。デバイス登録中は次のメッセージが表示されます。



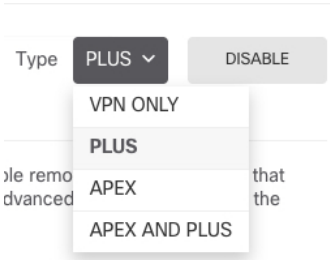
デバイスが正常に登録され、ページが更新されると、次のように表示されます。



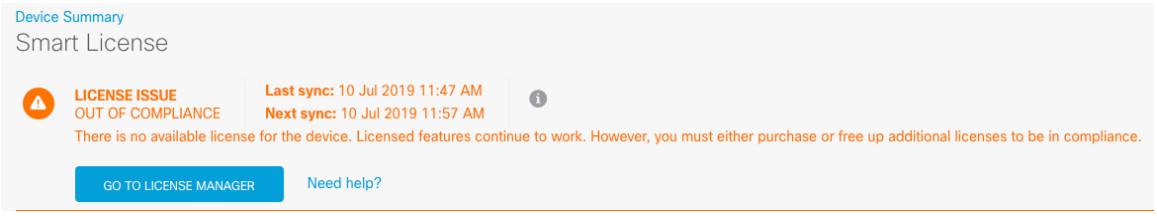
ステップ 6 必要に応じて、それぞれのオプション ライセンスの [有効化/無効化（Enable/Disable）] コントロールをクリックします。



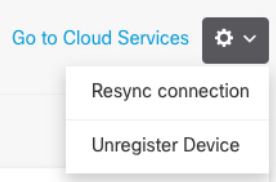
- [有効化（Enable）]：Cisco Smart Software Manager アカウントにライセンスを登録し、制御された機能が有効になります。ライセンスによって制御されるポリシーを設定し、展開できます。
- [無効化（Disable）]：Cisco Smart Software Manager アカウントのライセンスを登録解除し、制御された機能が無効になります。新しいポリシーの機能の設定も、その機能を使用するポリシーの展開もできません。
- **RA VPN** ライセンスを有効にした場合は、使用するライセンスのタイプ（[Plus]、[Apex]、[VPN 専用（VPN Only）]、または [Plus と Apex（Plus and Apex）] を選択します。



機能を有効にすると、アカウントにライセンスがない場合はページを更新した後に次の非準拠メッセージが表示されます。



ステップ 7 歯車ドロップダウン リストから [接続の再同期（Resync Connection）] を選択して、Cisco Smart Software Manager とライセンス情報を同期させます。



基本的なセキュリティポリシーの設定

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）。 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。
2	セキュリティゾーンへのインターフェイスの追加 （17 ページ）。 アクセス制御に必要な内部および外部のセキュリティゾーンに、内部インターフェイスと外部インターフェイスを追加します。
3	デフォルトルートの追加 （19 ページ）。 外部DHCPサーバからデフォルトルートを受け取らない場合は、手動で追加する必要があります。
4	NAT の設定 （21 ページ）。 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。
5	内部から外部へのトラフィックの許可 （23 ページ）。 内部から外部へのトラフィックを許可します。
6	（任意）DHCP サーバの設定 （24 ページ）。 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。
7	（任意）管理ゲートウェイの設定とデータインターフェイスの管理の許可 （27 ページ）。 管理ゲートウェイを変更するか、データインターフェイスからの管理を許可します。
8	設定の展開 （28 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、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外部インターフェイスを使用して、内部インターフェイスを設定します。

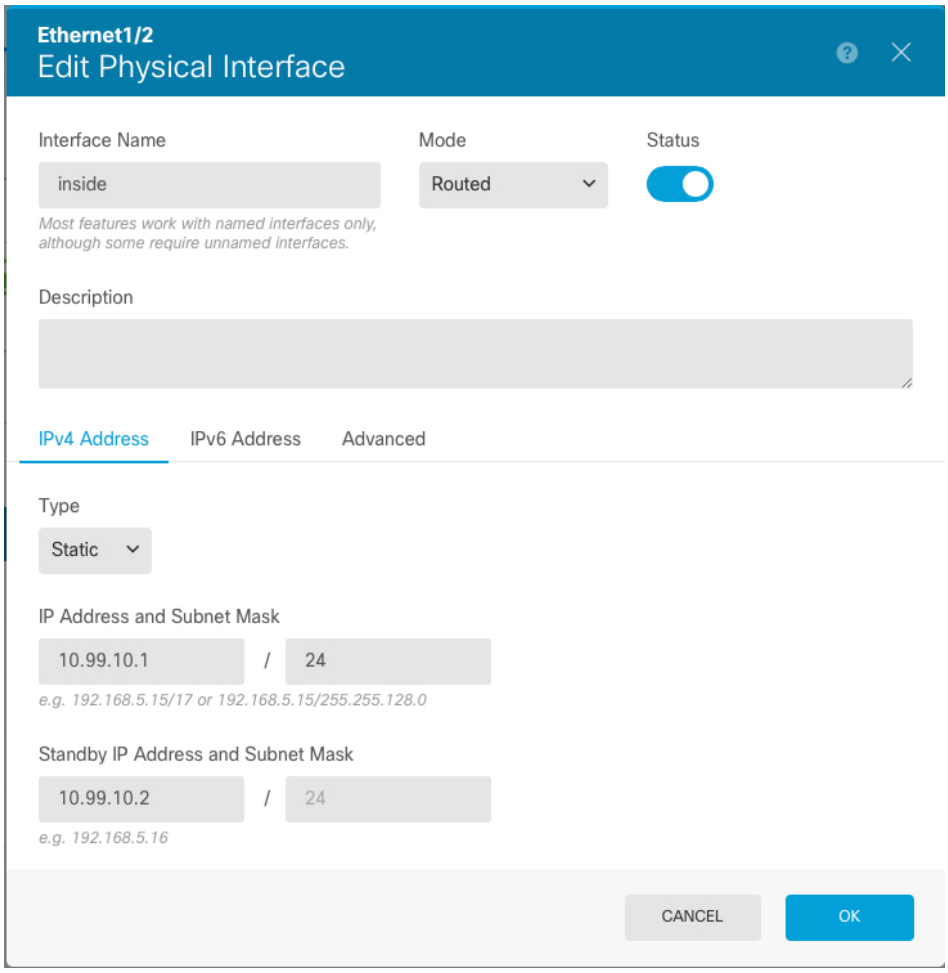
手順

ステップ 1 [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックします。

[インターフェイス（Interfaces）] タブがデフォルトで選択されます。インターフェイスリストに、物理インターフェイスとそれぞれの名前、アドレス、状態が表示されます。

ステップ 2 外部用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

ステップ 3 次の設定を行います。



a) [インターフェイス名（Interface Name）] を設定します。

インターフェイスの名前（最大 48 文字）を設定します。英字は小文字にする必要があります。例、[inside] または [outside]。名前を設定しないと、インターフェイスの残りの設定は無視されます。サブインターフェイスを設定する場合を除き、インターフェイスには名前が必要です。

b) [モード（Mode）] を [ルーテッド（Routed）] に設定します。

パッシブインターフェイスを使用する場合は、『FDM configuration guide』を参照してください。

c) [ステータス（Status）] スライダを [有効（enabled）] 設定（ ）に設定します。

重要 また、FXOS でインターフェイスを有効にする必要があります。

d) （任意）[説明（Description）] を設定します。

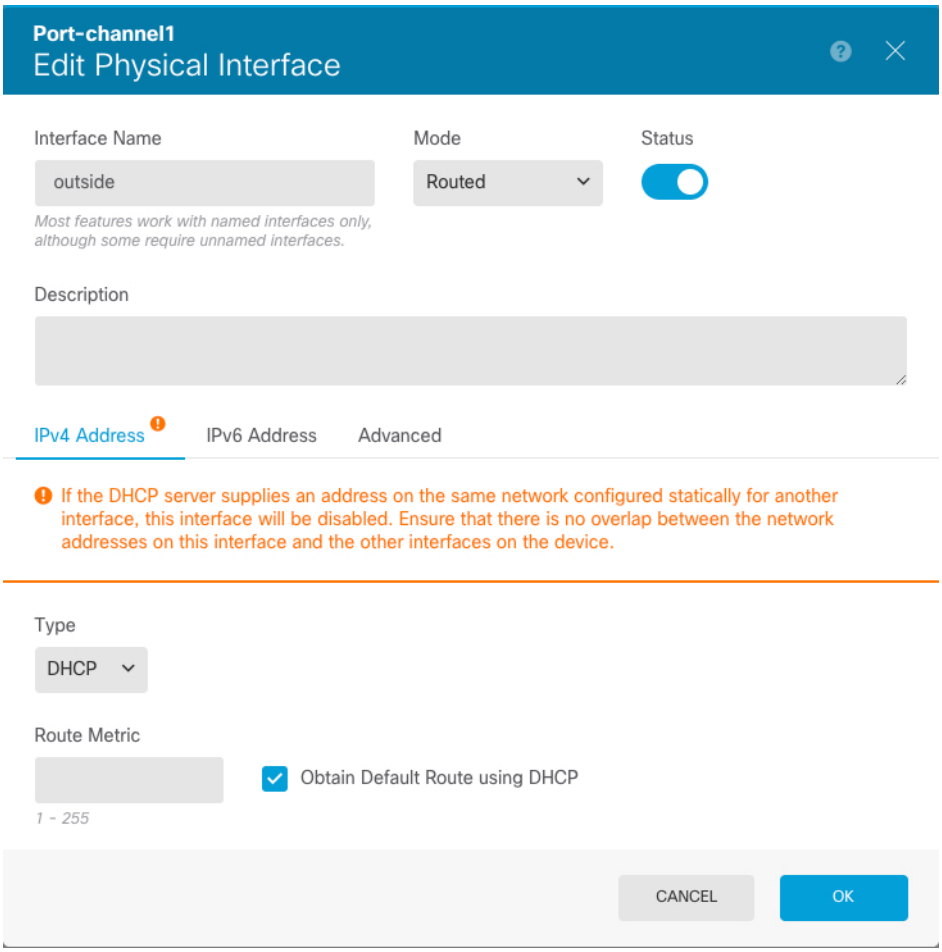
説明は 200 文字以内で、改行を入れずに 1 行で入力します。

e) [IPv4アドレス（IPv4 Address）] ページで、スタティック IP アドレスを設定します。

f) （任意）[IPv6アドレス（IPv6 Address）] をクリックし、IPv6 を設定します。

ステップ 4 [OK] をクリックします。

ステップ 5 外部用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、内部の場合と同じフィールドを設定します。このインターフェイスでは、IPv4 アドレスに [DHCP] を選択します。



（注） スタティック IP アドレスを使用する場合、または DHCP からデフォルトルートを受信しない場合は、デフォルトルートを手動で設定する必要があります。『FDM configuration guide』を参照してください。

セキュリティゾーンへのインターフェイスの追加

セキュリティ ゾーンとはインターフェイスのグループ分けです。ゾーンは、トラフィックの管理と分類に役立つようにネットワークをセグメントに分割します。複数のゾーンを定義できますが、所与のインターフェイスは単一のゾーンの中にのみ存在できます。

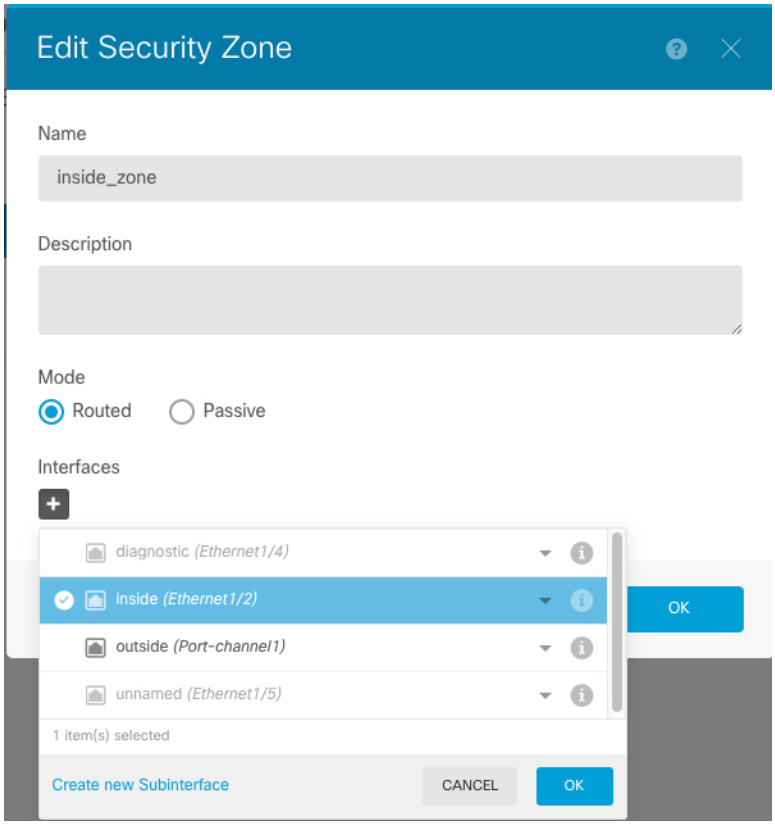
この手順では、次の事前設定ゾーンにインターフェイスを追加する方法について説明します。

- [inside_zone]：このゾーンは、内部ネットワークを表します。
- [outside_zone]：このゾーンは、インターネットなどの制御不可能な外部ネットワークを表します。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、次に目次から [セキュリティゾーン（Security Zones）] を選択します。

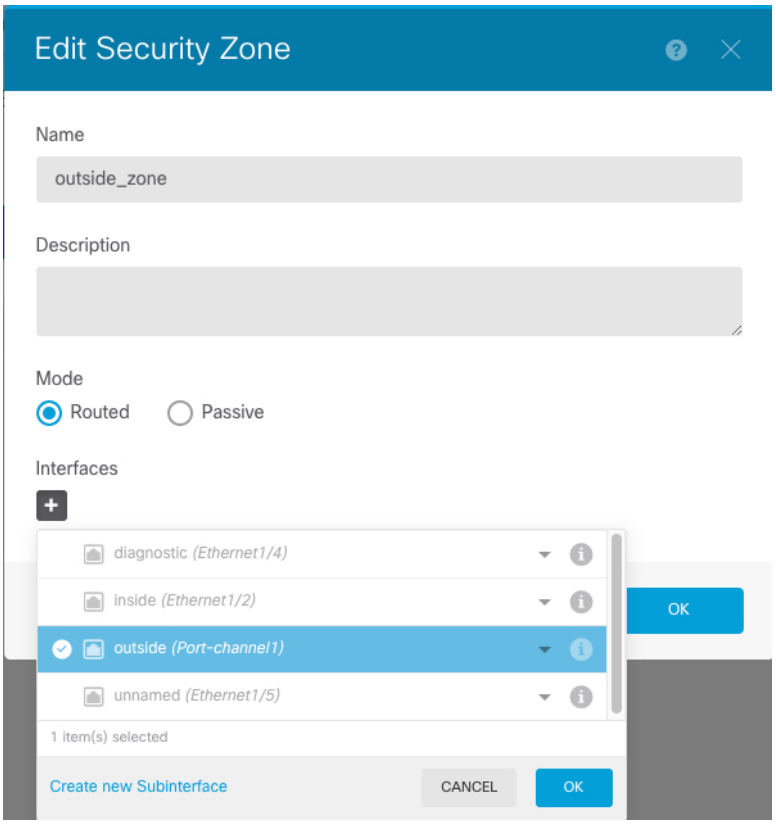
ステップ 2 [inside_zone] の [編集（edit）] アイコン（）をクリックします。



ステップ 3 [インターフェイス（Interfaces）] リストで、をクリックし、ゾーンに追加する内部インターフェイスを選択します。

ステップ 4 [OK] をクリックして変更を保存します。

ステップ 5 外部インターフェイスを [outside_zone] に追加するには、これらの手順を繰り返します。



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、**[デバイスの概要（Device Summary）]** > **[スタティックルーティング（Static Routing）]** ページに表示されます。

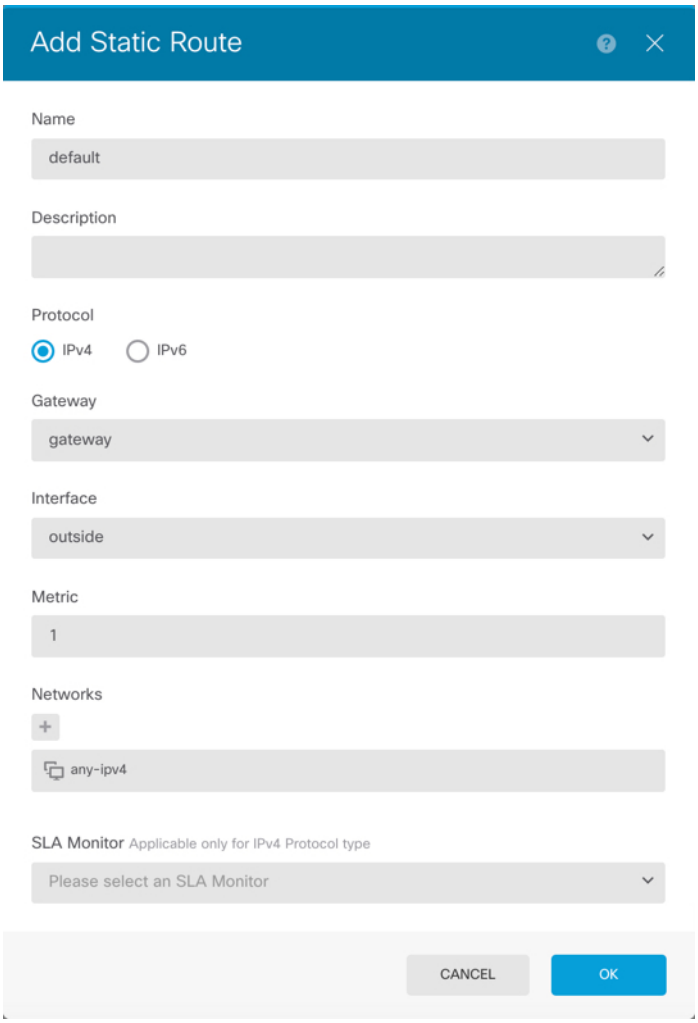
手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーにあるリンクをクリックします。

[スタティックルーティング（Static Routing）] ページが表示されます。

ステップ 2 + または [スタティックルートの作成（Create Static Route）] をクリックします。

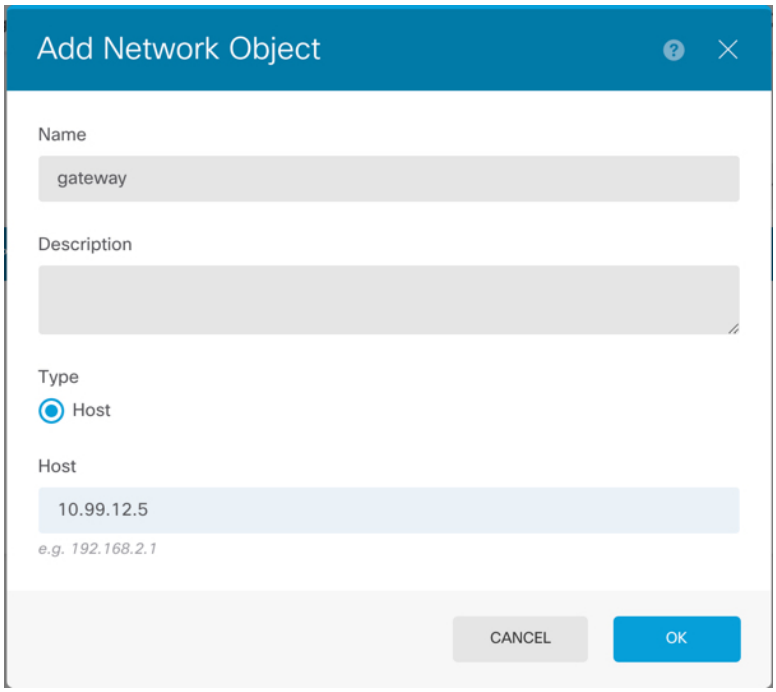
ステップ 3 デフォルトルートのプロパティを設定します。



a) [名前（Name）] を入力します。たとえば「default」とします。
b) [IPv4] または [IPv6] ラジオボタンをクリックします。

   IPv4 と IPv6 に対して個別のデフォルトルートを作成する必要があります。

c) [ゲートウェイ（Gateway）] をクリックしてから [新しいネットワークの作成（Create New Network）] をクリックして、ゲートウェイ IP アドレスをホストオブジェクトとして追加します。



d) ゲートウェイの [インターフェイス（Interface）] （たとえば [外部（outside）]）を選択します。

e) [ネットワーク（Network）] + アイコンをクリックし、IPv4 デフォルトルートの場合は [any-ipv4] 、IPv6 デフォルトルートの場合は [any-ipv6] を選択します。

ステップ 4 [OK] をクリックします。

NAT の設定

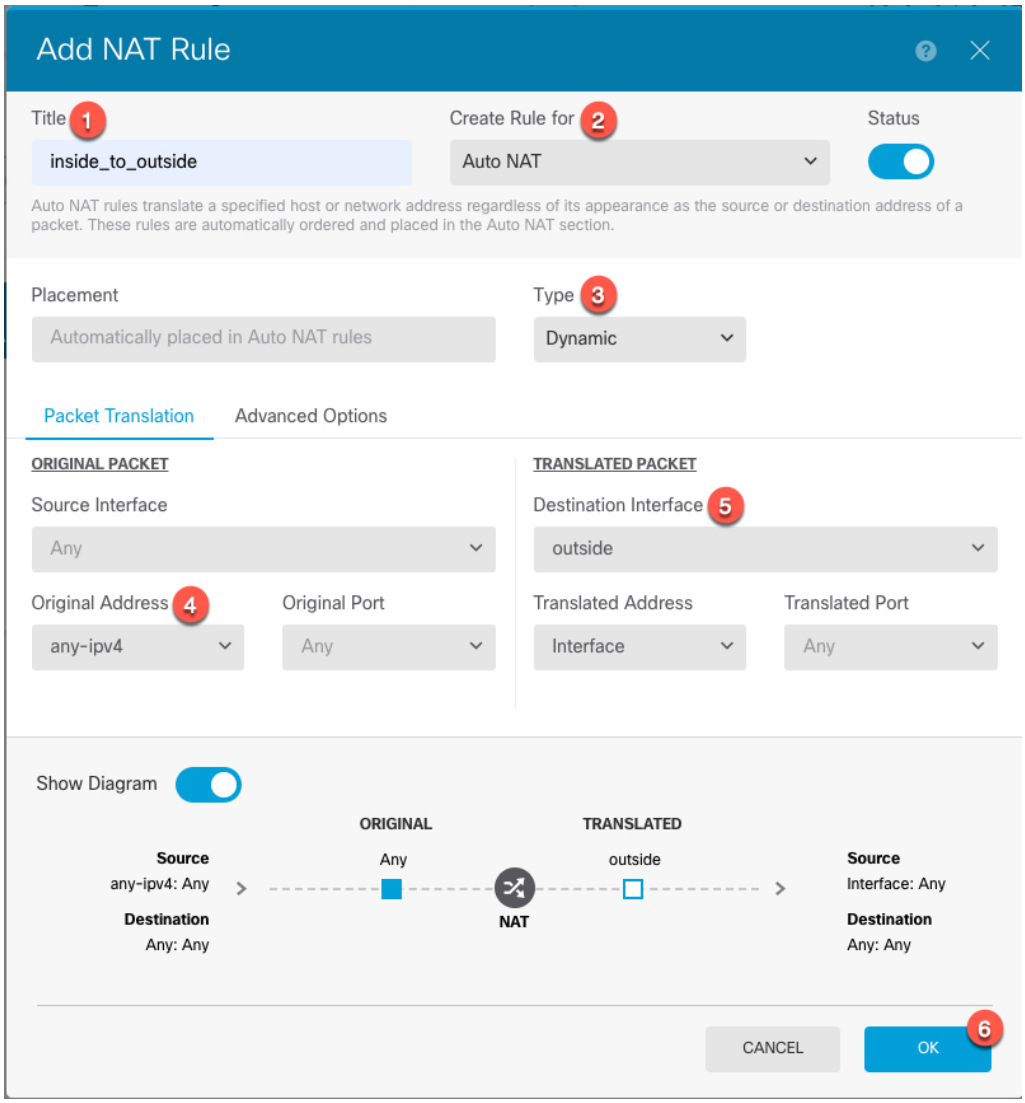
一般的な NAT ルールでは、内部アドレスを外部インターフェイスの IP アドレスのポートに変換します。このタイプの NAT ルールのことをインターフェイス ポート アドレス変換（PAT）と呼びます。IPv6 にインターフェイス PAT は使用できません。

手順

ステップ 1 [ポリシー（Policies）] をクリックしてから [NAT] をクリックします。

ステップ 2 + または [NATルールの作成（Create NAT Rule）] をクリックします。

ステップ 3 基本ルールのオプションを設定します。



a) [タイトル（Title）] を設定します。
b) **[ルールの作成対象（Create Rule For）] > [自動NAT（Auto NAT）]** を選択します。
c) **[タイプ（Type）] > [ダイナミック（Dynamic）]** を選択します。

ステップ 4 次のパケット変換オプションを設定します。

a) [元のパケット（Original Packet）] で、[元のアドレス（Original Address）] を [any-ipv4] に設定します。

このルールは、任意のインターフェイスから発信されるすべての IPv4 トラフィックを変換します。インターフェイスまたはアドレスを制限する場合は、特定の [送信元インターフェイス（Source Interface）] を選択し、[元のアドレス（Original Address）] に IP アドレスを指定できます。

b) [変換済みパケット（Translated Packet）] で、[接続先インターフェイス（Destination Interface）] を外部インターフェイスに設定します。

デフォルトでは、インターフェイス IP アドレスが変換済みアドレスに使用されます。

ステップ 5 （任意） [図の表示（Show Diagram）] をクリックして、ルールのビジュアル表現を表示します。

ステップ 6 [OK] をクリックします。

内部から外部へのトラフィックの許可

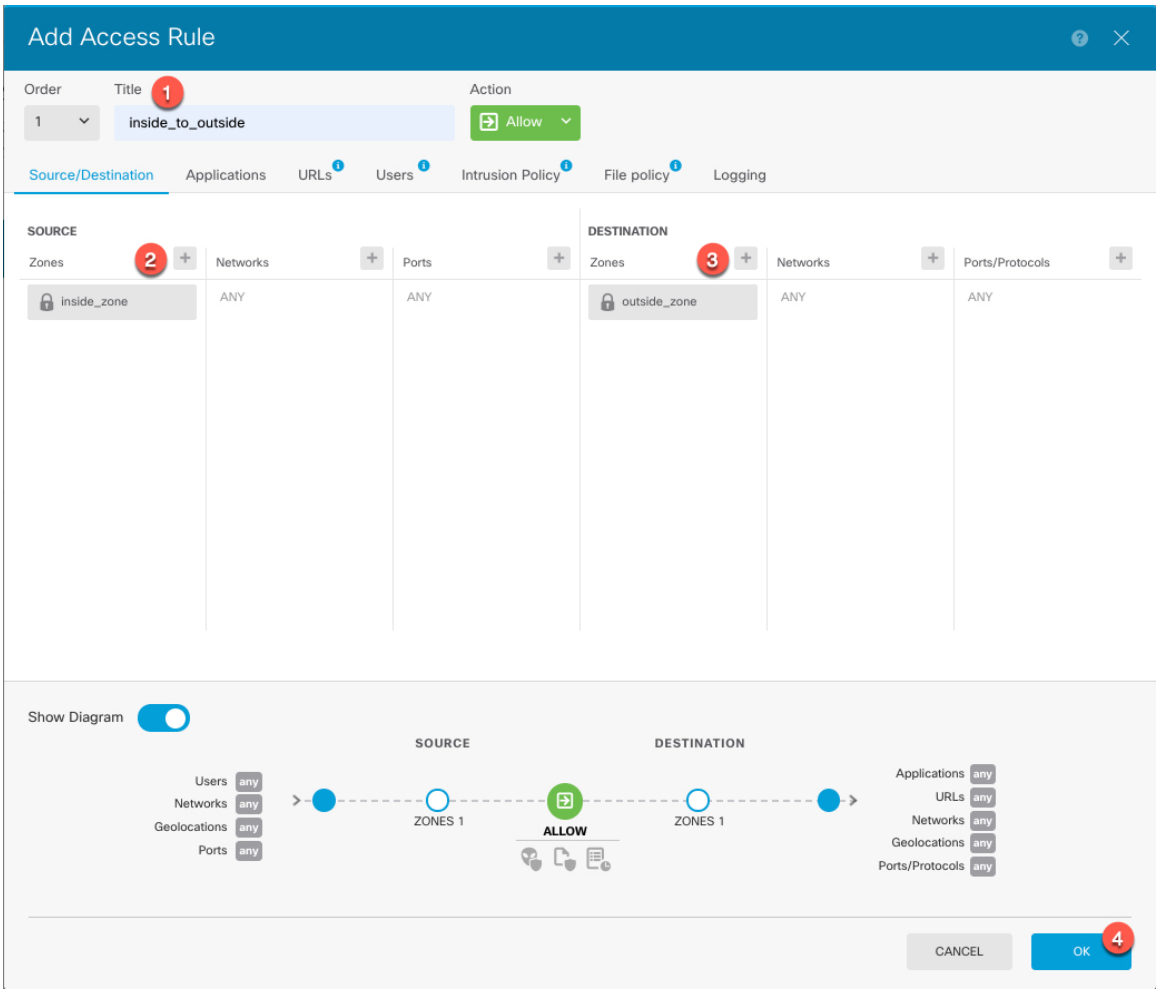
デフォルトでは、セキュリティゾーン間のトラフィックはブロックされます。この手順では、内部から外部へのトラフィックを許可する方法を示します。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）]** を選択します。

ステップ 2 + または [アクセスルールの作成（Create Access Rule）] をクリックします。

ステップ 3 基本ルールのオプションを設定します。



a) [タイトル（Title）] を設定します。

b) [ソース（Source）] で、[ゾーン（Zones）] + アイコンをクリックし、内部ゾーンを選択します。

c) [接続先（Destination）] で、[ゾーン（Zones）] + アイコンをクリックし、外部ゾーンを選択します。

d) （任意）[図の表示（Show Diagram）] をクリックして、ルールのビジュアル表現を表示します。

e) [OK] をクリックします。

（任意）DHCP サーバの設定

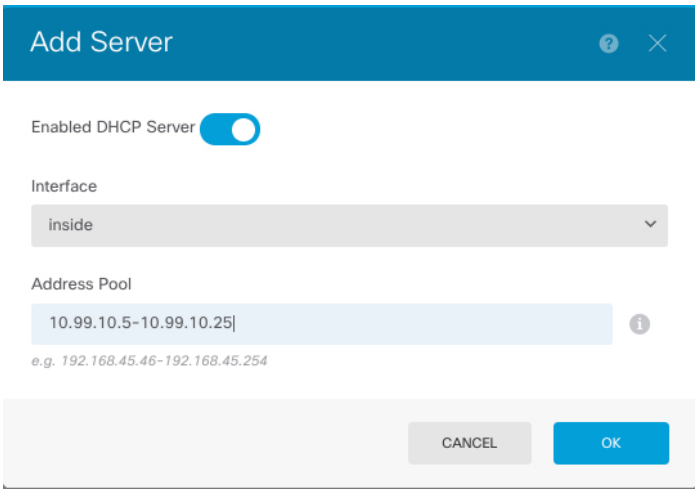
クライアントで DHCP を使用して FTD から IP アドレスを取得するようにする場合は、DHCP サーバを有効にします。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、**[システム設定（System Settings）] > [DHCPサーバ（DHCP Server）]** リンクをクリックします。

ステップ 2 + または [DHCPサーバの作成（Create DHCP Server）] をクリックします。

ステップ 3 サーバのプロパティを設定します。



a) [DHCPサーバを有効にする（Enable DHCP Server）] スライダをクリックして、有効と表示します（ ）。

b) DHCP サーバを有効にする [インターフェイス（Interface）] を選択します。

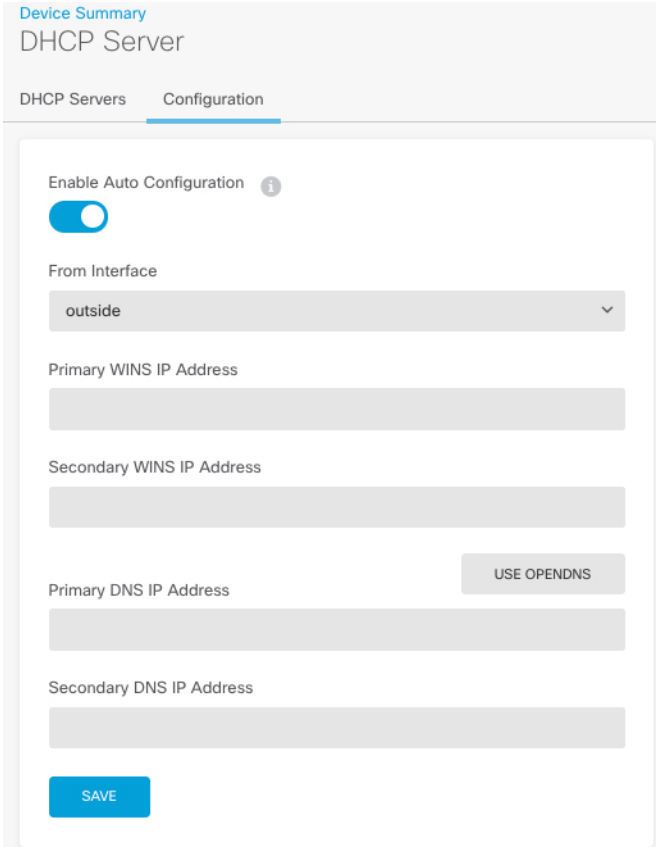
インターフェイスは静的 IP アドレスを持っている必要があります。インターフェイスで DHCP サーバを実行する場合、インターフェイス アドレスの取得に DHCP を使用することはできません。

c) [アドレスプール（Address Pool）] を入力します

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体の IP アドレス、ブロードキャスト アドレス、またはサブネット ネットワーク アドレスを含めることはできません。

d) [OK] をクリックします。

ステップ 4 （任意） [設定（Configuration）] タブをクリックして、自動設定およびグローバル設定を設定します。



DHCP 自動設定では、指定したインターフェイスで動作している DHCP クライアントから取得した DNS サーバ、ドメイン名、および WINS サーバの情報が、DHCP サーバから DHCP クライアントに提供されます。通常、外部インターフェイスで DHCP を使用してアドレスを取得する場合には自動設定を使用しますが、DHCP を介してアドレスを取得するインターフェイスを選択することもできます。自動設定を使用できない場合には、必要なオプションを手動で定義できます。

a) [自動設定を有効にする（Enable Auto Configuration）] スライダをクリックして、有効と表示します（ ）。
b) クライアントがサーバ設定を継承するインターフェイスを[継承元インターフェイス（From Interface）] ドロップダウンメニューで選択します。
c) 自動設定を有効にしない場合、または自動設定された設定を上書きするには、1 つ以上のグローバルオプションを設定します。これらの設定は、DHCP サーバを実行するすべてのインターフェイスで DHCP クライアントに送信されます。
d) [保存（Save）] をクリックします。

（任意）管理ゲートウェイの設定とデータインターフェイスの管理の許可

FTDを展開するときに、管理アドレスと外部ゲートウェイを設定しました。次の手順では、管理インターフェイスではなくデータインターフェイスを介してバックプレーン経由で管理トラフィックを送信するようにFTDを設定できます。この場合、直接接続された管理ネットワーク上にいる場合はFTDを管理できますが、他のネットワーク宛ての管理トラフィックは、管理ではなくデータインターフェイスにルーティングされます。

また、デフォルトでは、管理インターフェイス（FDMまたはCLIアクセス）を介してのみFTDを管理できます。次の手順では、1つ以上のデータインターフェイスで管理を有効にすることもできます。管理インターフェイス ゲートウェイは、データインターフェイスのFDM管理トラフィックには影響しないことに注意してください。この場合、FTDは通常のルーティングテーブルを使用します。

始める前に

インターフェイスの設定 （15 ページ）に従ってデータインターフェイスを設定します。

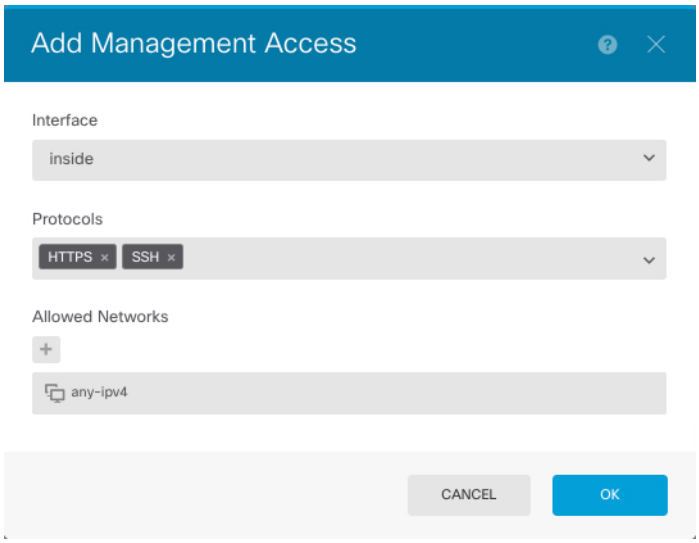
手順

ステップ 1 データインターフェイスからの管理を許可します。

a) [デバイス（Device）] をクリックしてから、**[システム設定（System Settings）] > [管理アクセス（Management Access）]** リンクの順にクリックします。

b) [データインターフェイス（Data Interface）] をクリックします。

c) ＋または[データインターフェイスの作成（Create Data Interface）]をクリックし、インターフェイスごとにルールを作成します。



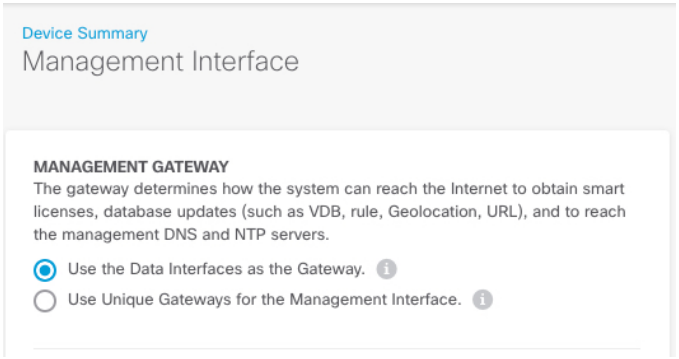
- [インターフェイス（Interface）]：管理アクセスを許可するインターフェイスを選択します。
- [プロトコル（Protocols）]：ルールが HTTPS（ポート 443）または SSH（ポート 22）、またはその両方用かを選択します。
- [許可されたネットワーク（Allowed Networks）]：システムにアクセスできる IPv4 ネットワーク、IPv6 ネットワーク、またはホストを定義するネットワークオブジェクトを選択します。「任意」のアドレスを指定するには、[any-ipv4] (0.0.0.0/0) および [any-ipv6] (::/0) を選択します。

d) [OK] をクリックします。

ステップ 2 データインターフェイスを使用するように管理ゲートウェイを設定します。

a) [デバイス（Device）] をクリックし、次に **[システム設定（System Settings）]** > **[管理インターフェイス（Management Interface）]** リンクをクリックします。

b) [データインターフェイスをゲートウェイとして使用する（Use the Data Interfaces as the Gateway）] を選択します。



c) [保存（Save）] をクリックして警告を読み、[OK] 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 Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

このアイコンは、展開されていない変更がある場合にドット マークで強調表示されます。

[保留中の変更（Pending Changes）] ウィンドウには、設定の展開バージョンと保留中の変更との比較が表示されます。それらの変更は、削除された要素、追加された要素、または編集された要素を示すために色分けされています。色の説明については、ウィンドウの凡例を参照してください。

ステップ 2 変更内容に問題がない場合は、[今すぐ展開（Deploy Now）] をクリックして、ジョブをすぐに開始できます。

ウィンドウに展開が進行中であることが示されます。ウィンドウを閉じるか、または展開が完了するまで待機できます。展開が進行中の間にウィンドウを閉じても、ジョブは停止しません。結果は、タスクリストや監査ログで確認できます。ウィンドウを開いたままにした場合、[展開履歴（Deployment History）] リンクをクリックすると結果が表示されます。

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デバイス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。

FDM の使用に関する詳細については、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』を参照してください。

FDM での FTD の履歴

機能名	バージョン	機能情報
ネイティブインスタンスを使用した FDM のサポート	6.5.0	FDM を使用してネイティブインスタンスを展開できるようになりました。 新しい/変更された画面： **[論理デバイス（Logical Devices）] > [デバイスの追加（Add Device）]** （注） FXOS 2.7.1 が必要です。