Cisco Secure Firewall Management Center への Cisco Secure Firewall Threat Defense デバイスのオンボード

2025 年 9 月

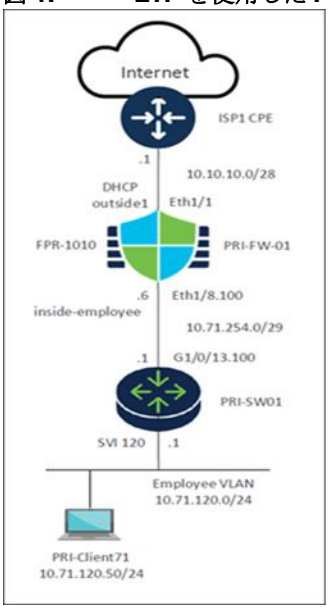
ゼロタッチプロビジョニングを使用した Management Center への Threat Defense デバイスのオンボード

ゼロタッチプロビジョニング（ZTP）を使用して、Management Center にデバイスを登録できます。この方法は、デバイスでの初期設定を行わずに、シリアル番号を使用して単一の Threat Defense デバイスをオンボードする場合に使用します。

ネットワーク トポロジ

ネットワークトポロジ図はこちらになります。

図 1.　　ZTP を使用した PRI-FW-01（Firepower 1010）の Management Center へのオンボード



この例では、ZTP を使用して、Firepower 1010 Threat Defense デバイスを Management Center にオンボードします。このデバイスは、プロビデンスのスポークであり、SD-WAN ネットワークの RI（PRI）ブランチです。

- Threat Defense モデル：Firepower 1010
- デバイス名：PRI-FW-01
- ループバック IP アドレス：10.71.255.1/32
- Eth1/1：ISP1 に接続され、DHCP を使用する外部インターフェイス。
- Eth1/8.100：LAN ネットワークに接続された内部サブインターフェイス。
- シリアル番号：FJC57213ZDZ
- PRI-SW01：Threat Defense デバイスを LAN に接続するレイヤ 3 デバイス。

ZTP を使用した Threat Defense デバイスのオンボーディングの前提条件

- デバイスが未設定または新規インストールである必要があります。ゼロタッチプロビジョニングは、新しいデバイスのみを対象としています。事前設定では、デバイスの設定に応じてゼロタッチプロビジョニングを無効にすることができます。
- デバイスの外部インターフェイスをケーブル接続して、インターネットに接続できるようにします。

- Threat Defense デバイスが Cisco Security Cloud および Management Center に接続できることを確認します。
- Management Center が Smart Software Manager に登録されていることを確認します。有効な評価ライセンスで十分ですが、有効期限が切れると、正常に登録するまで新しいデバイスを追加できなくなります。
- Management Center を Cisco Security Cloud と統合する：Security Cloud Control は、Cisco Security Cloud との統合後にオンプレミスの Management Center をオンボーディングします。ゼロタッチプロビジョニングを使用して Threat Defense デバイスをオンボードするには、この統合が必要です。

  i. Management Center で、[統合（Integration）] > [Cisco Security Cloud] を選択します。

  ii. [Cisco Security Cloudの有効化（Enable Cisco Security Cloud）] をクリックして別のブラウザタブを開き、Cisco Security Cloud アカウントにログインし、表示されたコードを確認します。複数のテナントがある場合は、Management Center をオンボードする必要があるテナントを選択します。

  iii. [ゼロタッチプロビジョニングを有効にする（Enable Zero-Touch Provisioning）] チェックボックスをオンにします。必要に応じて、ポリシーアナライザおよびオプティマイザ、Cisco XDR 自動化、Cisco Security Cloud サポート、Cisco AI Assistant for Security などの他のオプションを確認して有効にします。

  iv. [保存（Save）] をクリックします。

デバイステンプレートを使用するための前提条件

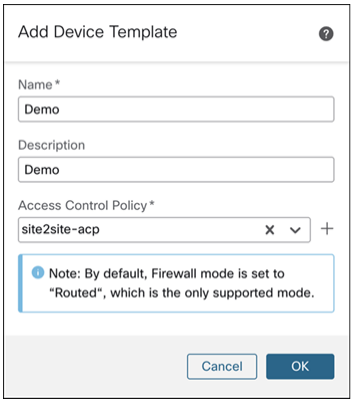
- Management Center はバージョン 7.6 以降である必要があります。
- Threat Defense デバイスは、バージョン 7.4.1 以降であり、次のいずれかのモデルである必要があります。
  - Firepower 1010
  - Firepower 1100
  - Cisco Secure Firewall 1200
  - Firepower 2100
  - Cisco Secure Firewall 3100
- テンプレートを作成、変更、削除できるのは、管理者ユーザーおよびネットワーク管理者ユーザーのみです。

- スマート ライセンス アカウントには、ターゲットデバイスのライセンス利用資格が必要です。

デバイステンプレートの作成

ステップ 1. [デバイス（Devices）] > [テンプレート管理（Template Management）] を選択します。

ステップ 2. [デバイステンプレートの追加（Add Device Template）] をクリックします。



ステップ 3. [デバイステンプレートの追加（Add Device Template）] ダイアログボックスで、次のパラメータを設定します。

i. [名前（Name）] フィールドに、テンプレートの名前を入力します。この例では、テンプレート名は **Demo** です。

ii. （オプション）[説明（Description）] フィールドにテンプレートの説明を入力します。

iii. [アクセス制御ポリシー（Access Control Policy）] ドロップダウンリストから、アクセス制御ポリシーを選択します。

ステップ 4. [OK] をクリックします。

データインターフェイスを使用して管理される **Threat Defense** デバイスのテンプレートの設定

注： データインターフェイスを使用して管理されている Threat Defense デバイスに設定したテンプレートを、データインターフェイスで管理されていないデバイスに適用することはできません。

ステップ 1. [デバイス（Devices）] > [テンプレート管理（Template Management）] を選択します。

ステップ 2. 必要なテンプレート（Demo）の [編集（Edit）] アイコンをクリックします。

ステップ 3. [テンプレート設定（Template Settings）] タブをクリックします。

ステップ 4. [全般（General）] タイルで、[データインターフェイスでデバイスを管理（Manage device by Data Interface）] ボタンを切り替えます。

ステップ 5. マネージャアクセスのデータインターフェイスを選択するよう求めるポップアップが表示されます。[OK] をクリックします。

ステップ 6. [インターフェイス（Interfaces）] タブをクリックします。

ステップ 7. マネージャアクセスに使用するデータインターフェイスの [編集（Edit）] アイコンをクリックします。

ステップ 8. この例では、Ethernet1/1 がデータインターフェイスです。

ステップ 9. [物理インターフェイスの編集（Edit Physical Interface）] ダイアログボックスで、[全般（General）] タブをクリックします。

ステップ 10. [名前（Name）] フィールドに、インターフェイスの名前を入力します。

ステップ 11. この例では、名前は outside1 です。

ステップ 12. （オプション）[説明（Description）] フィールドに、このインターフェイスの説明を入力します。

ステップ 13. [有効（Enabled）] チェックボックスをオンにします。

ステップ 14. [セキュリティゾーン（Security Zone）] ドロップダウンリストから、セキュリティゾーンを選択します。

この例では、セキュリティゾーンは outside-zone です。

ステップ 15. [IPv4] タブをクリックします。

ステップ 16. [IPタイプ（IP Type）] ドロップダウンリストから、[DHCP] を選択します。

ステップ 17. [パスモニタリング（Path Monitoring）] タブをクリックします。

ステップ 18. [IPベースのモニタリングの有効化（Enable IP based Path Monitoring）] チェックボックスをオンにします。

ステップ 19. [マネージャアクセス（Manager Access）] タブをクリックします。

ステップ 20. [管理アクセスの有効化（Enable management access）] チェックボックスをオンにします。

ステップ 21. [保存（Save）] をクリックします。

テンプレートへの物理インターフェイスの追加

デフォルトでは、デバイステンプレートは次の物理インターフェイスを使用してデバイスを起動できます。

- 管理インターフェイス 0/0
- 内部インターフェイス（Ethernet 1/1）
- 外部インターフェイス（Ethernet 1/2）

この例では、デフォルトの Ethernet1/2 は使用していません。物理インターフェイス Ethernet1/8 を作成します。

ステップ 1. [デバイス（Devices）] > [テンプレート管理（Template Management）] を選択します。

ステップ 2. 物理インターフェイスを追加するテンプレート（**Demo**）の [編集（Edit）] アイコンをクリックします。

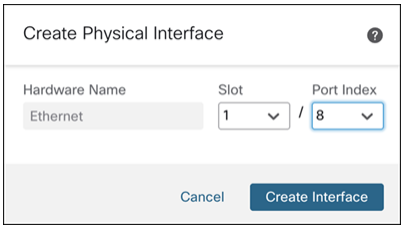
ステップ 3. [インターフェイス（Interfaces）] タブをクリックします。

ステップ 4. [物理インターフェイスの追加（Add Physical Interface）] をクリックします。

ステップ 5. [スロット（Slot）] ドロップダウンリストから [1] を選択します。

ステップ 6. [ポートインデックス（Port Index）] ドロップダウンリストから [8] を選択します。

ステップ 7. [インターフェイスの作成（Create Interface）] をクリックします。



このインターフェイスを編集して、名前を inside-trunk に、説明を「LAN への内部トランクインターフェイス」に設定します。

テンプレートでのインターフェイスのサブインターフェイスの作成

この例では、Ethernet1/8.100 は LAN ネットワークに接続された内部サブインターフェイスです。

ステップ 1. [デバイス（Devices）] > [テンプレート管理（Template Management）] を選択します。

ステップ 2. 物理インターフェイスを追加するテンプレート（Demo）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）] タブをクリックします。

ステップ 4. [インターフェイスの追加（Add Interfaces）] > [サブインターフェイス（Sub Interface）] をクリックします。

ステップ 5. [名前（Name）] フィールドおよび [説明（Description）] フィールドに詳細を入力します。

ステップ 6. [有効（Enabled）] チェックボックスをオンにします。

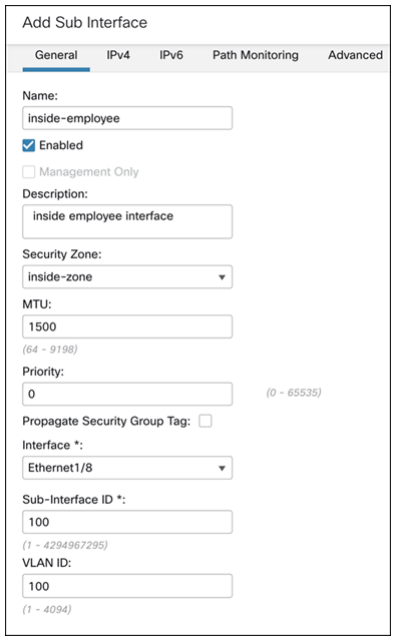
ステップ 7. [セキュリティゾーン（Security Zone）] ドロップダウンリストから、セキュリティゾーンを選択します。

この例では、セキュリティゾーンは inside-zone です。

ステップ 8. [インターフェイス（Interface）] ドロップダウンリストでインターフェイスを選択します。

ステップ 9. [サブインターフェイス（Sub-Interface）] の ID に **100** を入力します。

ステップ 10. [VLAN ID] に **100** を入力します。



ステップ 11. [IPv4] タブをクリックします。

ステップ 12. [IPタイプ（IP Type）] ドロップダウンリストから、[スタティックIPを使用（Use Static IP）] を選択します。

ステップ 13. [IPアドレス（IP Address）] ドロップダウンリストから、IP アドレスの変数を選択するか、[+] をクリックして IP アドレス変数を作成します。この例では、変数は **$inside-employee-if-ip** です。

ステップ 14. [OK] をクリックします。

ステップ 15. [保存（Save）] をクリックします。

データインターフェイスでのダイナミック **DNS** ホスト名の設定

ダイナミック DNS（DDNS）は、IP アドレスまたはホスト名が変更されるたびに DNS のリソースレコードを更新するメカニズムです。外部インターフェイスからゼロタッチプロビジョニングを使用して登録されたデバイスの場合、DDNS は「FMC のみ」方式を使用して自動的に有効になります（Web 方式と同様）。この方法は、ゼロタッチ プロビジョニング デバイスでのみ使用できます。

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

ステップ 2. 物理インターフェイスを追加するテンプレート（Demo）の [編集（Edit）] アイコンをクリックします。

ステップ 3. [DHCP] タブをクリックします。

ステップ 4. 左側のペインで [DDNS] をクリックします。

ステップ 5. [DDNS更新方法（DDNS Update Methods）] タブをクリックします。

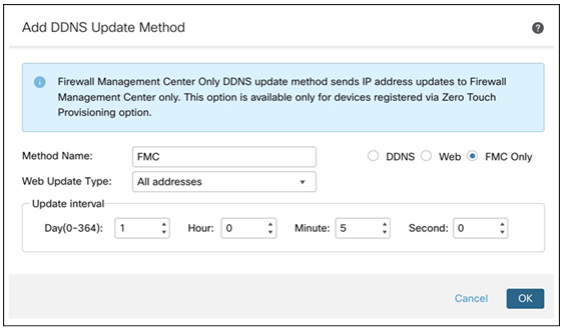
ステップ 6. [+追加（+Add）] をクリックして、DDNS 更新方法を追加します。

ステップ 7. [DDNS更新方法の追加（Add DDNS Update Method）] ウィンドウで、次のパラメータを設定します。

i. [方式名（Method Name）] フィールドに方法の名前を入力します。

ii. [FMCのみ（FMC Only）] オプションボタンをクリックします。

iii. 要件に応じて [更新間隔（Update Interval）] を設定します。この例では、間隔は 5 分です。



ステップ 8. [OK] をクリックします。作成した方法が [DDNS更新方法（DDNS Update Methods）] テーブルに表示されます。

ステップ 9. [DDNSインターフェイス設定（DDNS Interface Settings）] タブをクリックします。

ステップ 10. 動的 DNS 設定を追加する場合は、[+追加（+Add）] をクリックします。

ステップ 11. [ダイナミックDNS設定の追加（Add Dynamic DNS Configuration）] ダイアログボックスで、次のパラメータを設定します。

i. [インターフェイス（Interface）] ドロップダウンリストから、マネージャアクセスが有効なインターフェイスを選択します。この例では、インターフェイスは outside1 です。

ii. [方式名（Method Name）] ドロップダウンリストから、作成した方法を選択します。

iii. [ホスト名（Host Name）] ドロップダウンリストから、ホスト名の変数を選択するか、[+] をクリックしてホスト名変数を作成します。この例では、変数は $hostname です。

iv. [OK] をクリックします。

ステップ 12. [保存（Save）] をクリックします。

テンプレート設定の作成およびデバイスモデルへのテンプレートのマッピング

ステップ 1. [デバイス（Devices）] > [テンプレート管理（Template Management）] を選択します。

ステップ 2.　物理インターフェイスを追加するテンプレートの [編集（Edit）] アイコンをクリックします。

ステップ 3.　[テンプレート設定（Template Settings）] をクリックします。

ステップ 4.　左側のペインで [全般（General）] をクリックして、ライセンスを追加します。

ステップ 5.　左側のペインで [モデルマッピング（Model Mapping）] をクリックして、テンプレートをデバイスモデルにマッピングします。

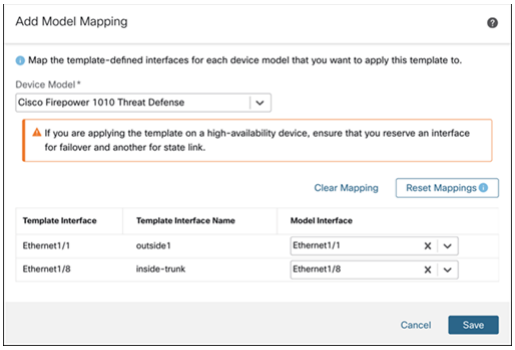
ステップ 6.　[モデルマッピングの追加（Add Model Mapping）] をクリックします。

ステップ 7.　[モデルマッピングの追加（Add Model Mapping）] ダイアログボックスで、次のパラメータを設定します。

i.　[デバイスモデル（Device Model）] ドロップダウンリストから、モデルを選択します。この例では、モデルは Cisco Firepower 1010 Threat Defense デバイスです。

ii.　[モデルインターフェイス（Model Interface）] ドロップダウンリストから、データインターフェイスと内部インターフェイスを選択します。

iii.　[保存（Save）] をクリックします。

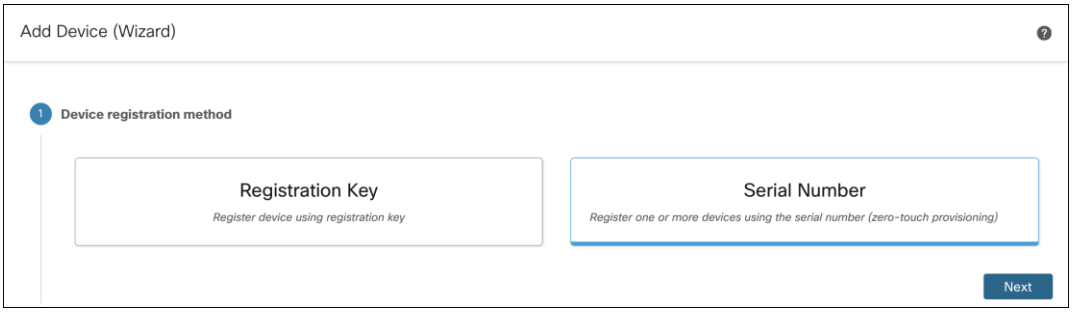


ZTP を使用した Threat Defense デバイスのオンボード

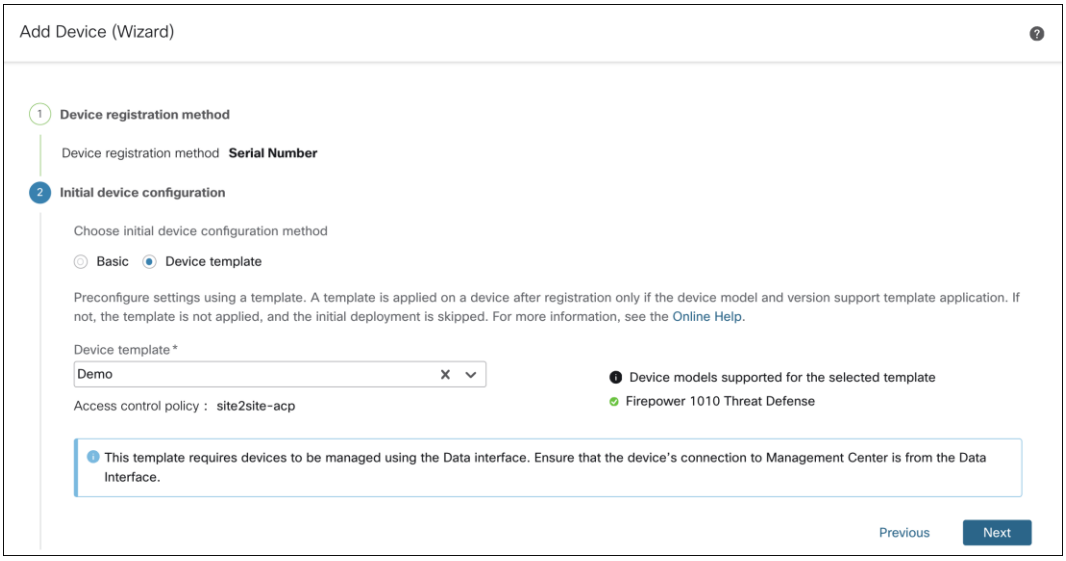
ステップ 1.　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

ステップ 2.　[追加（Add）] > [デバイス（ウィザード）（Device (Wizard)）] をクリックします。

ステップ 3.　[デバイス登録（Device registration）] 方式で、[シリアル番号（Serial Number）] をクリックし、[次へ（Next）] をクリックします。



ステップ 4.　[デバイスの初期設定（Initial device configuration）] で、次のパラメータを設定します。



i. [デバイステンプレート（Device template）] オプションボタンをクリックします。

ii. [デバイステンプレート（Device template）] ドロップダウンリストから、デバイスのデバイステンプレートを選択し、[次へ（Next）] をクリックします。

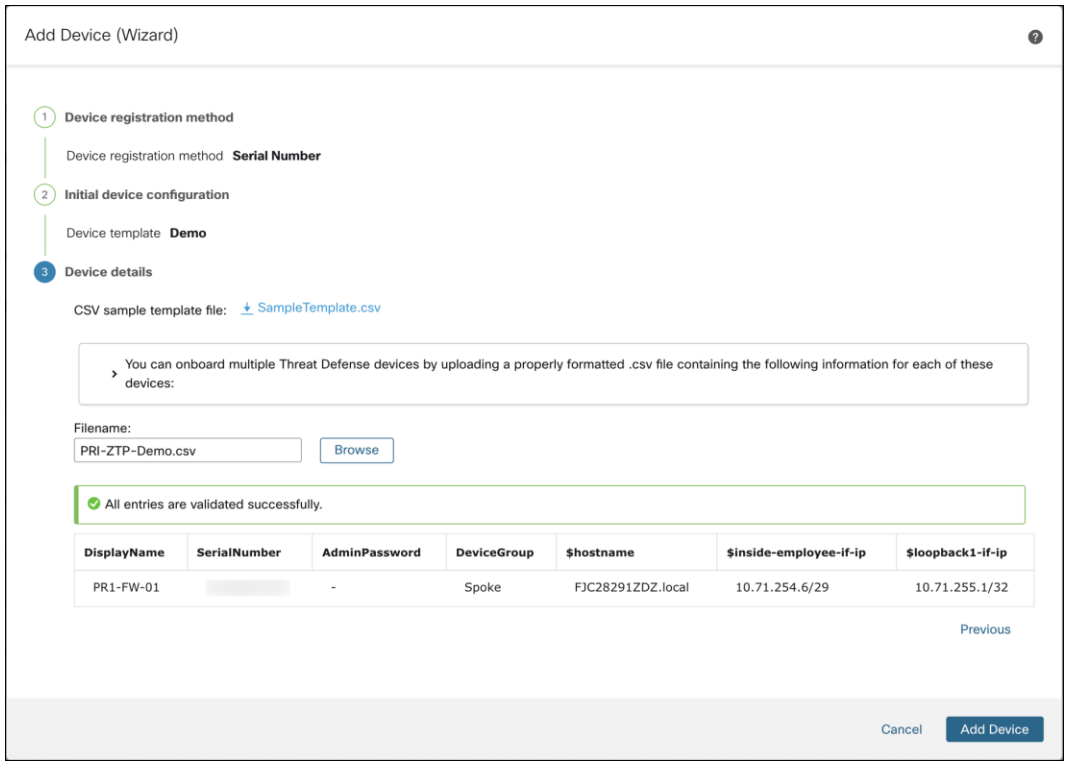
ステップ 5. [デバイスの詳細（Device details）] で、以下を実行します。

i. **SampleTemplate.csv** をダウンロードします。Management Center に CSV ファイルをアップロードする場合は、この形式を使用します。

ii. 各デバイスの必須パラメータ（[表示名（Display Name）]、[シリアル番号（Serial Number）]、[管理者パスワード（Admin Password）] など）と追加の変数を定義します。

iii. CSV テンプレートファイルをドラッグアンドドロップするか、[参照（Browse）] をクリックして、アップロードする CSV テンプレートファイルを選択します。アップロード後にファイルに対して有効性検査が実行されます。

iv. CSV テンプレートファイルが正常にアップロードされると、CSV テンプレートファイルの内容が表形式で表示されます。



ステップ 6. [デバイスの追加（Add Device）] をクリックすると、デバイスの登録が開始されます。

テンプレート設定は、デバイスが Management Center に正常に登録された後に適用されます。

[通知（Notifications）] > [タスク（Tasks）] ウィンドウでは、デバイス登録、デバイス検出、およびデバイステンプレートの適用に関連するメッセージを表示できます。

[デバイステンプレートの適用（Device Template Apply）] レポートは、テンプレートを適用するタスクが完了した後に生成されます。このレポートは、デバイスでのテンプレートの適用が成功した場合と失敗した場合の両方について生成されます。[通知（Notifications）] > [タスク（Tasks）] ウィンドウ内にこのレポートへのリンクが表示されます。

ステップ 7. [デバイス（Devices）] > [デバイス管理（Device Management）] を選択して、オンボーディングされたデバイス PRI-FW-01 を表示します。

登録キーを使用した Management Center への Threat Defense デバイスのオンボード

Management Center で登録キーを指定し、変数を定義することで、個々のデバイスを登録できます。この方法は、デバイステンプレートの有無に関係なく、単一の Threat Defense デバイスをオンボードする場合に使用されます。

注： この例では、テンプレートを使用せずにデバイスをオンボードします。

ネットワーク トポロジ

この例では、登録キー方式を使用して、MCT-FW-01 という単一の仮想 Cisco Secure Firewall デバイスをオンボードします。

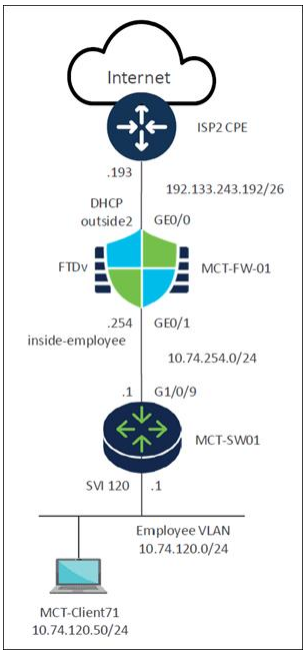


図 2.　　展開のネットワークトポロジ図

このネットワークトポロジ図は、ファイアウォールとスイッチを介して内部ユーザーをインターネットに接続する中小企業向けの一般的なセットアップを示しています。

- インターネット：外部ネットワークまたはパブリックインターネットを表します。
- ISP2 CPE：
  - インターネット サービス プロバイダー（ISP）に接続しているアップストリームデバイス。
  - 内部ネットワークをインターネットに接続します。
- FTDv（MCT-FW-01） - Cisco Firewall Threat Defense Virtual デバイス：
  - このデバイスはファイアウォールとして機能し、セキュリティとネットワークのセグメンテーションを行います。
  - GE0/0 インターフェイス（外部）：ISP2 CPE に接続します。サブネット 192.133.243.192/26 から DHCP（DHCP outside2）を介して IP アドレスを受信するように設定されています。.193 は ISP 側にあります。

- GE0/1 インターフェイス（内部 - 従業員内）：スイッチを介して内部ネットワークに接続します。このインターフェイスには、10.74.254.0/24 サブネット内の .254 で終わる IP アドレスがあります。このサブネットは多くの場合、ファイアウォールと内部スイッチ間のトランジットネットワークとして機能します。

- MCT-SW01 - スイッチ：
  - これはネットワークスイッチであり、SVI（スイッチ仮想インターフェイス）が存在する場合はレイヤ 3 デバイスである可能性が高いです。
  - G1/0/9 インターフェイス：FTDv（MCT-FW-01）に接続します。このインターフェイス（または接続されている SVI）の IP アドレスは 10.74.254.0/24 サブネット内の .1 であり、10.74.254.0/24 ネットワークセグメントのデフォルトゲートウェイになります。
  - SVI 120：これは、VLAN 120 のスイッチ仮想インターフェイスです。従業員 VLAN のデフォルトゲートウェイとして機能します。SVI 120 の IP アドレスは、10.74.120.0/24 サブネット内の .1 です。
- MCT-Client71 - 従業員クライアント：
  - これはエンドユーザーデバイス（ラップトップなど）を表します。
  - 10.74.120.0/24 ネットワークを使用する従業員 VLAN（VLAN 120）の一部です。
  - これの固有 IP アドレスは 10.74.120.50/24 です。

ワークフロー

登録キーを使用したオンボーディングには、2 つのステップがあります。

1. Threat Defense CLI で初期設定を完了します。
   a. デバイスに Management Center の詳細を追加します。
      i. Management Center のホスト名または IP アドレスを設定します。
      ii. 登録キー（最大 36 文字の英数字）を指定します。
      iii. （オプション）Management Center またはデバイスが NAT デバイスの背後にある場合は、一意の NAT ID（最大 36 文字の英数字）を入力します。
      iv. （オプション）Management Center の表示名を指定します。
   b. デバイスの管理データインターフェイスが、Management Center との接続を確立するように設定されていることを確認します。このインターフェイスは、インバウンドまたはアウトバウンドのいずれにもなれます。
2. Management Center アプリケーションで、次の手順を実行します。
   a. テンプレートありまたはなしでデバイスを追加し、オプションで、デバイスホスト名または IP アドレスを入力します。
   b. デバイスの表示名を入力します。
   c. 前の手順でデバイスに設定した登録キーを入力します。
   d. （オプション）一意の NAT ID を指定します。
   e. アクセス制御ポリシーを選択します。
   f. （オプション）ライセンスを割り当てます。

Threat Defense デバイスの Management Center への接続

ステップ 1.　管理インターフェイスへの SSH を使用して、Threat Defense CLI に接続します。

ステップ 2.　ユーザー名とパスワードを使用してログインします。デフォルトのユーザー名は admin で、デフォルトのパスワードは **Admin123** です。

```
firepower login: admin
Password:
Last login: Thu Feb 6 15:09
```

ステップ 3.　Threat Defense 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書（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。

ステップ 4.　デバイスに、デバイスを管理するための Management Center が設定されていないことを確認します。

```
> show managers
No managers configured.
```

ステップ 5.　この Threat Defense を管理する Management Center を追加します。

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

この例では、次の情報を指定します。

- Management Center の IPv4 アドレス：192.33.243.243
- 登録キー：cisco。登録キーは、1 回限り使用可能な共有シークレットです。キーは英数字（A～Z、a～z、0～9）、およびハイフン（-）を使用して、37 文字以内で指定します。登録キーはデバイスごとに一意である必要はありません。
- NAT ID：mct（この例では、Management Center は NAT デバイスの背後にあるため、一意の NAT ID を入力する必要があります。
- 表示名：FMC

```
> configure manager add 192.33.243.243 cisco mct FMC
Manager FMC successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

ステップ 6.　マネージャアクセス用のデータインターフェイスを設定します。

この例では、GigabitEthernet0/0 は管理トラフィック用に指定されたデータインターフェイスであり、outside2 はデータインターフェイスの名前です。

```
> configure network management-data-interface
Data interface to use for management: GigabitEthernet0/0
Specify a name for the interface [outside]: outside2
IP address (manual / dhcp) [dhcp]:
Comma-separated list of DNS servers [200.67.222.222,208.67.220.220]:
DDNS server update URL [none]:
```

データインターフェイスは管理トラフィックを処理するように設定されています。

ステップ 7.　デバイスに設定されたマネージャの詳細を確認するには、次のコマンドを実行します。

```
> show managers
Type: Manager
Host: 192.133.243.243
```

```
Display name: FMC
Identifier: mct
Registration: Pending
```

デバイスは、IP アドレスが 192.133.243.243 の Management Center によって管理されるように設定されていることが分かります。

ステップ 8. インターフェイスの詳細を確認するには、次のコマンドを実行します。

```
> show interface ip brief
Interface              IP-Address      OK?   Method   Status  Prot
GigabitEthernet0/0     192.133.243.221 YES   DHCP     up      up
```

データインターフェイス GigabitEthernet0/0 が DHCP IP アドレスを取得していることが分かります。この例のデータインターフェイスの IP アドレスは 192.133.243.221 です。

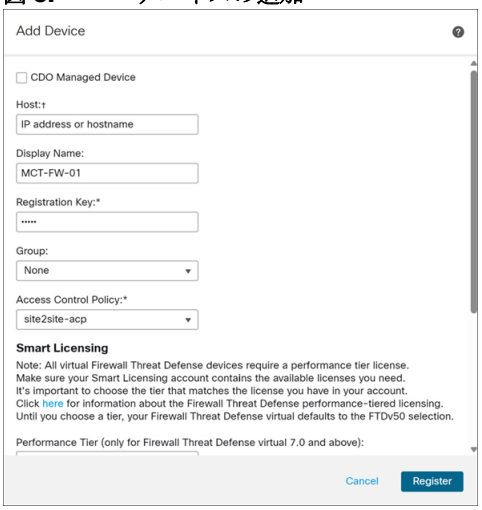
Firewall Management Center へのデバイスの登録

ステップ 1. [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）] ドロップダウンメニューから、[デバイス（Device）] を選択します。

ステップ 3. [登録キー（Registration Key）] をクリックし、[次へ（Next）] をクリックします。

図 3. デバイスの追加



ステップ 4. [デバイスの追加（Add Device）] ダイアログボックスで、次のパラメータを設定します。

i. [ホスト（Host）] フィールドに、追加するデバイスの IP アドレスまたはホスト名を入力します。この例では、デバイスが NAT の背後にあるため、このフィールドは空白のままにします。

ii. [表示名（Display Name）] フィールドに、Firewall Management Center に表示するデバイスの名前を入力します。この名前は変更できません。この例では、表示名は MCT-FW-01 です。

iii. [登録キー（Registration Key）] フィールドには、初期設定と同じ登録キーを入力します。この例では、登録キーは cisco です。前のセクションで、CLI を使用して Threat Defense の初期設定を完了したときに、このキーを指定しました。

iv. [アクセス制御ポリシー（Access Control Policy）] ドロップダウンリストから、アクセス制御ポリシーを選択します。この例では、site2site-acp ポリシーを選択します。

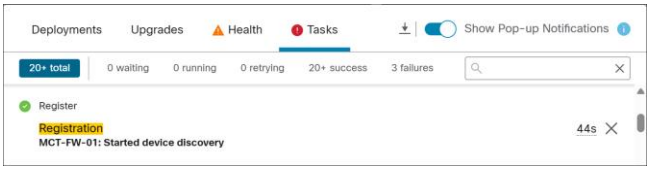
v. [一意のNAT ID（Unique NAT ID）] フィールドに、初期設定と同じ ID を入力します。この例では、NAT ID は mct です。前のセクションで、CLI を使用して Threat Defense の初期設定を完了したときに、識別子としてこの ID を指定しました。

ステップ 5.　[登録（Register）] をクリックします。

デバイス登録が開始されます。

[通知（Notifications）] > [タスク（Tasks）] ウィンドウでは、デバイス登録とデバイス検出に関連するメッセージを表示できます。

図 4.　通知



展開が完了するまでには数分かかります。

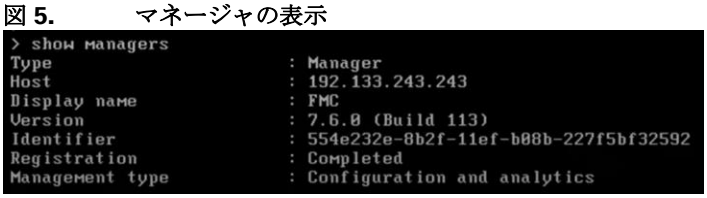
ステップ 6.　[展開（Deployments）] タブをクリックすると、デバイス展開の成功メッセージを確認できます。

ステップ 7.　デバイス登録が完了したことを確認するには、デバイスの CLI で次のコマンドを実行します。

```
> show managers
```

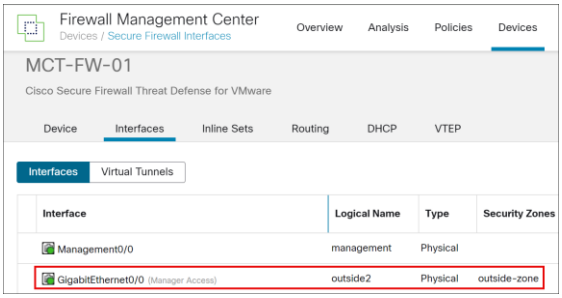
この例では、以下の出力は、デバイスが Management Center に対して設定されていることを示しています。

図 5.　マネージャの表示



- [デバイス（Device）] > [デバイス管理（Device Management）] を選択して、オンボーディングされた MCT-FW-01 デバイスを表示します。
- デバイスをクリックすると、設定済みのデータ管理インターフェイスが表示されます。

図 6.　インターフェイス



インターフェイスの追加

この例では、内部保護ネットワーク用に指定された GigabitEthernet0/1 インターフェイスを設定します。

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

ステップ 2.　設定するデバイスをクリックします。

この例では、MCT-FW-01 のインターフェイスを設定します。

ステップ 3.　[編集（Edit）] アイコンをクリックして、デバイス設定を編集します。

ステップ 4.　[物理インターフェイスの編集 （Edit Physical Interface）] ダイアログボックスで、次のパラメータを設定します。

i. [名前（Name）] フィールドに、インターフェイス名を入力します。この例では、インターフェイス名は inside-employee です。

ii. **[有効（Enable）]** チェックボックスをオンにします。

iii. [セキュリティゾーン（Security Zone）] ドロップダウンリストから、ゾーンを選択します。この例では、inside-zone を選択します。

iv. [IPv4] タブをクリックします。[IPタイプ（IP Type）] は、[スタティックIPを使用（Use Static IP）] にする必要があります。

v. [IPアドレス（IP Address）] フィールドに、スタティック IP アドレスを入力します。この例の IP アドレスは **10.74.254.254/24** です。

vi. [OK] をクリックします。

vii. [保存（Save）] をクリックします。

ループバック インターフェイスの設定

ループバック インターフェイスは、物理インターフェイスをエミュレートするソフトウェア専用インターフェイスであり、複数の物理インターフェイスを介して IPv4 および IPv6 に到達できます。ループバック インターフェイスはパス障害の克服に役立ちます。任意の物理インターフェイスからアクセスできるため、1 つがダウンした場合、別のインターフェイスからループバック インターフェイスにアクセスできます。ループバック インターフェイスの使用方法については、このガイドの後半で説明します。

ステップ 1. [インターフェイスの追加（Add Interfaces）] ドロップダウンリストから、[ループバック インターフェイス（Loopback Interface）] を選択します。

ステップ 2. [一般（General）] タブで、次のパラメータを設定します。

i. [名前（Name）] : ループバック インターフェイスの名前を入力します。この例では、インターフェイス名は loopback1 です。

ii. **[有効（Enabled）]** : ループバック インターフェイスを有効にする場合は、このチェックボックスをオンにします。

iii. [ループバック ID（Loopback ID）] : 1 ～ 1024 のループバック ID を入力します。この例では、ID は 1 です。

ステップ 3. [IPv4] タブをクリックし、[IPアドレス（IP Address）] を指定します。

この例の IP アドレスは 10.74.255.1.32 です。

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。

ステップ 6. Management Center メニューバーで、[展開（Deploy）] をクリックします。

この例では、MCT-FW-01 デバイスをオンにしてから、[展開（Deploy）] をクリックします。

CLI を使用したインターフェイス接続の確認

登録キーを使用してネットワークデバイスをオンボーディングした後は、関連するすべてのインターフェイス（外部、内部、ループバックなど）が、設定された IP アドレスを正常に取得していて、到達可能であることを確認することが重要です。

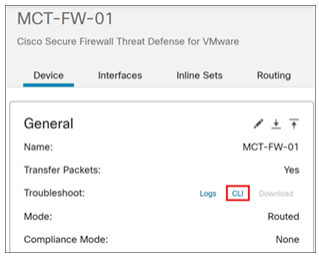
ステップ 1. [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

ステップ 2. 登録キーを使用してオンボーディングしたデバイスをクリックします。

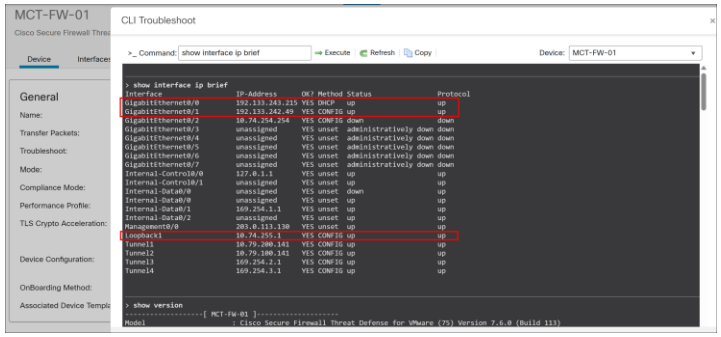
この例では、デバイスは **MCT-FW-01** です。

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.　[全般（General）] エリアで [CLI] をクリックします。



この例では、GigabitEthernet0/0（外部）、GigabitEthernet0/1（内部）、および Loopback1 インターフェイスは動作しており、設定された IP アドレスを正常に取得しています。



ステップ 5.　内部ネットワークへの到達可能性をテストします。

```
> ping 10.74.254.1
Sending 5, 100-byte ICMP Echos to 10.74.254.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

ステップ 6.　外部ネットワークへの到達可能性をテストします。

```
> ping 8.8.8.8
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/10/10 ms
```

ステップ 7.　ループバック インターフェイスへの到達可能性をテストします。

```
> ping 10.74.255.1
Sending 5, 100-byte ICMP Echos to 10.74.255.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

SD-WAN 設計およびその他のユースケースの詳細については、『Cisco Secure Firewall Threat Defense SD-WAN 設計および展開ガイド』を参照してください。

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。