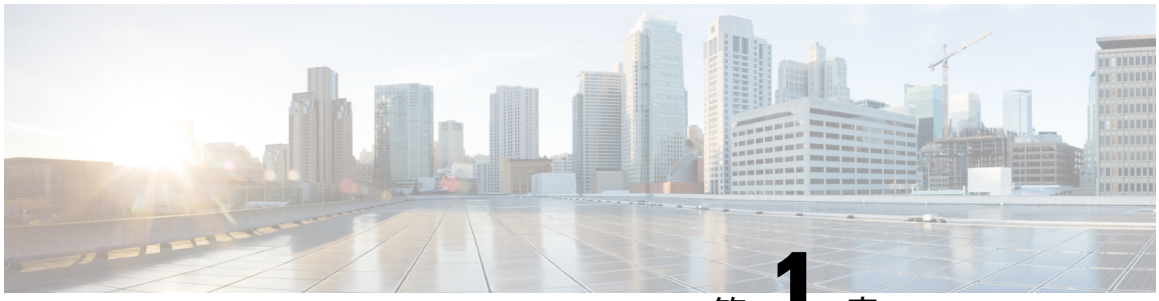
Cisco Secure Firewall 200 Threat Defense スタートアップガイド：中心拠点における Firewall Management Center

最終更新：2026 年 4 月 30 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/



第 1 章

はじめる前に

Cisco Secure Firewall 200 は、分散型企業および小規模ブランチロケーション向けに設計された次世代ファイアウォール（NGFW）機能を提供します。コンパクトなフォームファクタ内で、堅牢かつコスト効率の高いセキュリティとシンプルな管理を可能にし、ネットワークエッジにおけるセキュアで最適化された接続を実現します。Cisco Secure Firewall 200 の特長：

- シスコの Hybrid Mesh Firewall アーキテクチャをブランチエッジまで拡張
- AI を利用した検査と一貫したセキュリティポリシーを提供
- SD-WAN機能を統合して、アプリケーションパフォーマンスを強化し、信頼性の高いユーザーアクセスを実現
- コスト重視の環境に合わせたアプリケーションとユーザーの制御、効率的なセグメンテーション、高度なセキュリティ機能を提供

分散拠点にファイアウォールをインストールし、中央の Cisco Secure Firewall Management Center を使用して外部インターフェイスで管理します。

（注） ゼロタッチプロビジョニングを使用する場合、高可用性のために管理インターフェイスを使用することを推奨します。外部でゼロタッチプロビジョニングを使用して高可用性を使用する場合は、登録後に外部 IP アドレスを静的アドレスに変更する必要があります。

- ファイアウォールの電源の投入 （2 ページ）
- インストールされているアプリケーション（Firewall Threat Defense または ASA）の確認 （4 ページ）
- Firewall Threat Defense CLI へのアクセス （5 ページ）
- バージョンの確認と再イメージ化 （6 ページ）
- ライセンスの取得 （8 ページ）
- （必要な場合）ファイアウォールの電源の切断 （9 ページ）

ファイアウォールの電源の投入

システムの電源は、ファイアウォールの背面にある電源ボタンによって制御されます。電源ボタンは、ソフト通知を提供します。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） ファイアウォールを初めて起動するときは、Firewall Threat Defense の初期化に約 15 ～ 30 分かかります。

始める前に

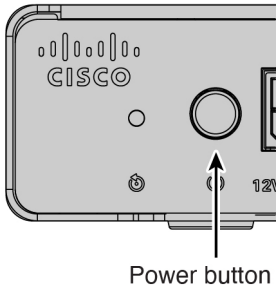
ファイアウォールに対して信頼性の高い電力を供給することが重要です（無停電電源装置（UPS）を使用するなど）。最初のシャットダウンを行わないで電力が失われると、重大なファイルシステムの損傷を引き起こす可能性があります。バックグラウンドでは常に多数のプロセスが実行されていて、電力が失われると、システムをグレースフルシャットダウンできません。

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。

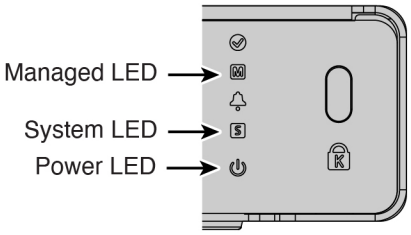
ステップ 2 シャーシの背面で、電源コードに隣接する電源ボタンを使用して電源をオンにします。

図 *1:* 電源ボタン



ステップ 3 LED の現在のステータスを確認します。

図 *2 : LED*



- 電源 LED：緑色で点灯している場合は、ファイアウォールの電源がオンになっていることを意味します。
- システム（S）LED：次の動作を参照してください。

表 *1 :* システム（*S*）*LED* の動作

LED の動作	説明	デバイスの電源を入れた後の時間（分 : 秒）
緑色で高速点滅	起動中	01:00
オレンジ色で高速点滅（エラー状態）	起動に失敗しました	01:00
緑色で点灯	アプリケーションがロードされました	15:00 ～ 30:00
オレンジ色で点灯（エラー状態）	アプリケーションのロードに失敗しました	15:00 ～ 30:00

- 管理対象（M）LED：外部インターフェイスをインターネットに接続した後に（「ファイアウォールのケーブル接続」を参照）、管理対象LEDを確認して、ゼロタッチプロビジョニングに向けたクラウド接続ステータスを確認します。

表 *2 :* ゼロ タッチ プロビジョニング：管理対象（*M*）*LED* の動作

M LED	説明	ファイアウォールの電源を入れた後の時間（分:秒）
緑色で低速点滅	Cisco Cloud に接続され、オンボーディングの準備ができています	15:00 ～ 30:00
グリーンとオレンジに交互に点滅 （エラー条件）	Cisco Cloud に接続できませんでした	15:00 ～ 30:00

M LED	説明	ファイアウォールの電源を入れた後の時間（分:秒）
緑色で点灯	オンボード済み	20:00 ～ 45:00

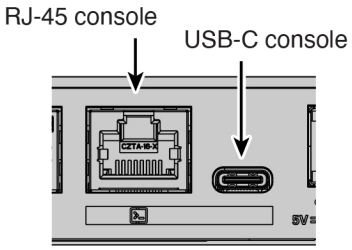
インストールされているアプリケーション（Firewall Threat Defense または ASA）の確認

Firewall Threat Defense と ASA の両方のアプリケーションが、ハードウェアでサポートされています。コンソールポートに接続し、出荷時にインストールされているアプリケーションを確認します。

手順

ステップ 1 いずれかのポートタイプを使用してコンソールポートに接続します。

図 *3:* コンソール ポート



ステップ 2 CLI プロンプトを参照して、ファイアウォールで Firewall Threat Defense または ASA が実行されているかどうかを確認します。

Firewall Threat Defense

Firepower ログイン（FXOS）プロンプトが表示されます。ログインして新しいパスワードを設定せずに、切断することができます。ログインを完了する必要がある場合は、Firewall Threat Defense CLI へのアクセス （5 ページ）を参照してください。

```
firepower login:
```

ASA

ASA プロンプトが表示されます。

```
ciscoasa>
```

ステップ 3 間違ったアプリケーションが実行されている場合は、*Cisco Secure Firewall ASA* および *Secure Firewall Threat Defense* 再イメージ化ガイドを参照してください。

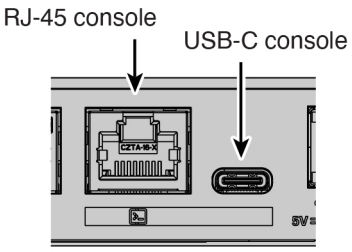
Firewall Threat Defense CLI へのアクセス

設定またはトラブルシューティングのためにCLIにアクセスする必要がある場合があります。

手順

ステップ 1 いずれかのポートタイプを使用してコンソールポートに接続します。

図 *4*：コンソール ポート



ステップ 2 FXOS に接続します。ユーザー名 **admin** とパスワード（デフォルトは **Admin123**）を使用して CLI にログインします。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。

```
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 Firewall Threat Defense CLI に変更します。

（注）

初期セットアップに Firewall Device Manager を使用する場合は、Firewall Threat Defense CLI にアクセスしないでください（アクセスすると、CLI セットアップが開始されます）。

ゼロタッチプロビジョニング の場合、CLI にアクセスし、セットアップスクリプトを実行したときに次のプロンプトメッセージが表示された場合は、**[n]** を選択します：「`Do you want to configure IPv4? (y/n) [y]:`」および「`Do you want to configure IPv6? (y/n) [y]:`」。また、次のプロンプトでデフォルトのローカルマネージャを承認する必要があります：「`Manage the device locally? (yes/no) [yes]:`」。

connect ftd

Firewall Threat Defense CLI に初めて接続すると、初期セットアップを完了するように求められます。

例：

```
firepower# connect ftd
>
```

Firewall Threat Defense 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 プロンプトに戻ります。

例：

```
> exit
firepower#
```

バージョンの確認と再イメージ化

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。

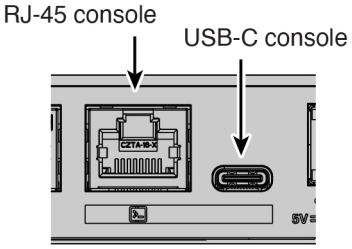
実行するバージョン

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 で説明されているリリース戦略を参照することもできます。

手順

ステップ 1 いずれかのポートタイプを使用してコンソールポートに接続します。

図 *5*：コンソール ポート



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            7.6.0.65        7.6.0.65        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) 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に静的 IP アドレスを設定する必要がある場合は、次のコマンドを入力します。

scope fabric-interconnect a

set out-of-band static ip *ip* **netmask** *netmask* **gw** *gateway*

commit-buffer

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。

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。

ファイアウォールが再起動したら、FXOS CLI に再度接続します。

c) FXOS CLI で、管理者パスワードを再度設定するように求められます。

ゼロタッチプロビジョニングの場合は、デバイスの導入準備をする際に、すでにパスワードが設定されているため、[**パスワードのリセット**（**Password Reset**）] エリアで必ず [**いいえ**（**No**）] を選択してください。

d) ファイアウォールをシャットダウンします。（必要な場合）ファイアウォールの電源の切断 （9 ページ） を参照してください。

ライセンスの取得

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。Smart Software Manager にアカウントがない場合は、リンクをクリック して新しいアカウントを設定します。

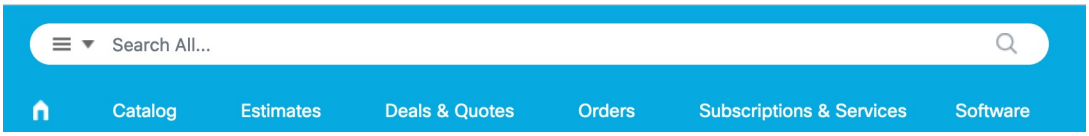
まだの場合は、Smart Software Manager に Firewall Management Center を登録します。登録を行うには、Smart Software Manager で登録トークンを生成する必要があります。詳細な手順については、*Cisco Secure Firewall Management Center* アドミニストレーション ガイドを参照してください。

Firewall Threat Defense には次のライセンスがあります。

- Essentials：必須
- IPS
- マルウェア防御
- URL フィルタリング
- Cisco Secure Client

1. 自身でライセンスを追加する必要がある場合は、Cisco Commerce Workspace で **[すべて検索（Search All）]** フィールドを使用します。

図 *6:* ライセンス検索



2. 次のライセンス PID を検索します。

（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。

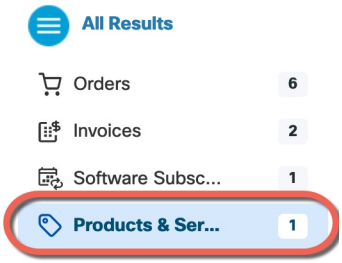
- IPS、マルウェア防御、および URL の組み合わせ：
  - CSF220T-TMC

  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。
  - CSF220T-TMC-1Y
  - CSF220T-TMC-3Y
  - CSF220T-TMC-5Y

- Cisco Secure Client：『Cisco Secure Client Ordering Guide』を参照してください。

3. 結果から、**[製品とサービス（Products & Services）]**を選択します。

図 7 : 結果



（必要な場合）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ません。

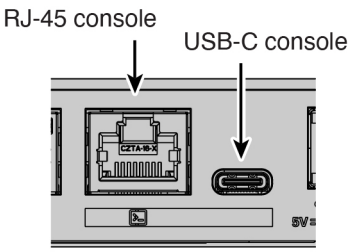
CLI におけるファイアウォールの電源の切断

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ファイアウォールの電源を切断できます。

手順

ステップ 1 いずれかのポートタイプを使用してコンソールポートに接続します。

図 8 : コンソール ポート



ステップ 2 FXOS CLI でローカル管理モードに接続します。

firepower # **connect local-mgmt**

ステップ 3 システムをシャットダウンします。

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 4 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。シャットダウンが完了すると、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 5 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。

Management Center を使用したファイアウォールの電源切断

Firewall Management Center を使用してシステムを適切にシャットダウンします。

手順

ステップ 1 ファイアウォールをシャットダウンします。

a) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**を選択します。
b) 再起動するデバイスの横にある [編集（Edit）]（ ） をクリックします。
c) [デバイス（Device）] タブをクリックします。
d) **[システム（System）]**セクションで[デバイスのシャットダウン（Shut Down Device）]（ ） をクリックします。
e) 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。

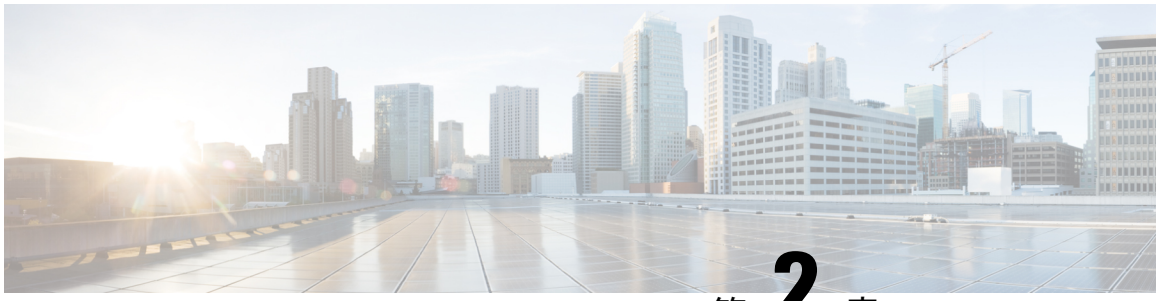
ステップ 2 コンソールからファイアウォールに接続している場合は、ファイアウォールがシャットダウンするときにシステムプロンプトをモニターします。シャットダウンが完了すると、次のプロンプトが表示されます。

```
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 3 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。



第 2 章

ファイアウォールのケーブル接続と登録

ファイアウォールをケーブル接続し、ファイアウォールを Firewall Management Center に登録します。

- ファイアウォールのケーブル接続 （11 ページ）
- 初期設定の実行（手動プロビジョニング） （11 ページ）
- Management Center へのファイアウォールの登録 （21 ページ）

ファイアウォールのケーブル接続

初期設定の実行（手動プロビジョニング）

手動でプロビジョニングを行う場合は、Cisco Secure Firewall Device Manager または CLI を使用して、ファイアウォールの初期設定を実行します。

初期設定：デバイスマネージャ

この方法を使用すると、ファイアウォールを登録した後、管理インターフェイスに加えて次のインターフェイスが事前設定されます。

- イーサネット 1/1：「外部」、DHCP からの IP アドレス、IPv6 自動設定
- ：「内部」、192.168.95.1/24
- デフォルトルート：外部インターフェイスで DHCP を介して取得
- 追加インターフェイス：Firewall Device Manager からのインターフェイス設定はすべて保持されます。

他の設定（内部の DHCP サーバー、アクセス コントロール ポリシー、セキュリティゾーンなど）は保持されません。

手順

ステップ 1 コンピュータを内部インターフェイスに接続します。

ステップ 2 Firewall Device Manager にログインします。

a) https://192.168.95.1に進みます。

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

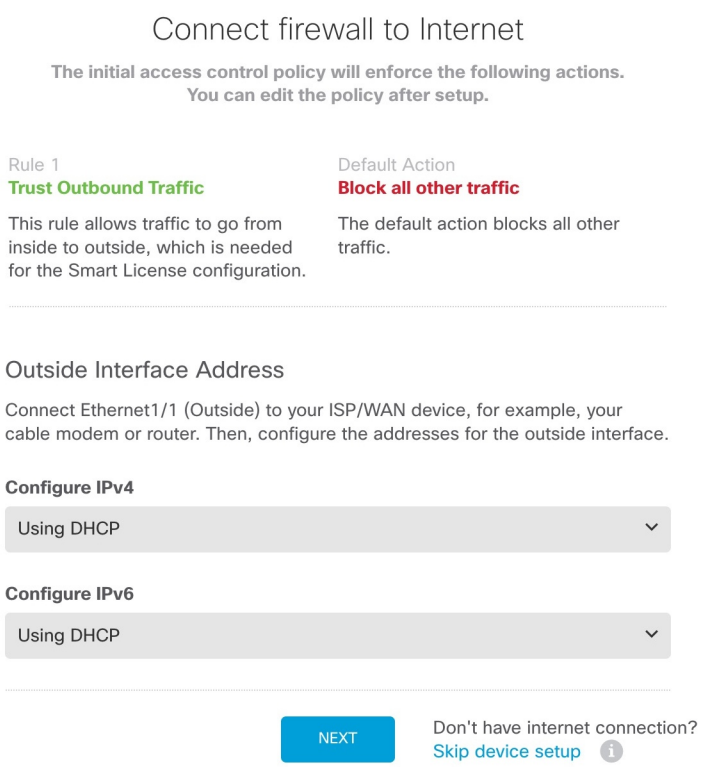
c) 一般規約を読んで同意し、管理者パスワードを変更するように求められます。

ステップ 3 セットアップウィザードを使用します。

（注）
正確なポート設定は、モデルによって異なります。

a) 外部インターフェイスと管理インターフェイスを設定します。

図 *9:* インターネットへのファイアウォールの接続



1. [外部インターフェイスアドレス（Outside Interface Address）]：高可用性の実装を予定している場合は、静的 IP アドレスを使用します。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。ウィザードの完了後に PPPoE を設定できます。
2. [管理インターフェイス（Management Interface）]：外部インターフェイスでマネージャアクセスを使用している場合でも、管理インターフェイスの設定が使用されます。たとえば、外部インター

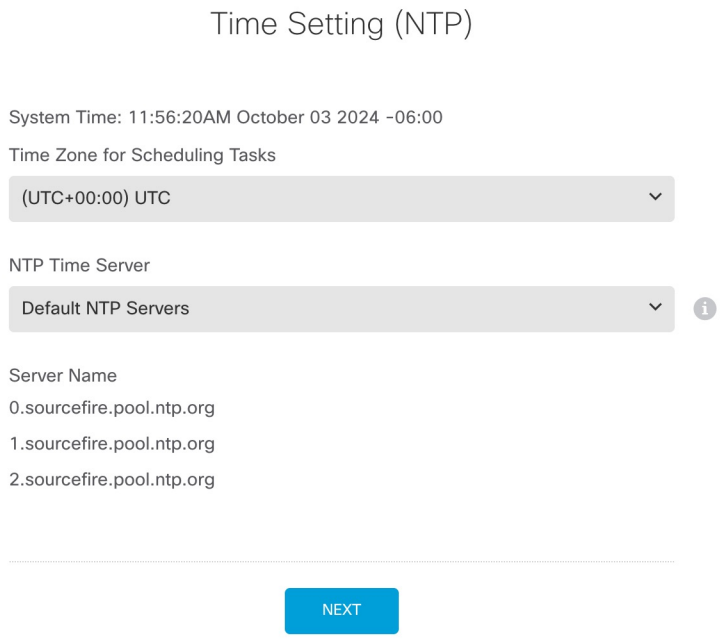
フェイスを介してバックプレーン経由で回送される管理トラフィックは、外部インターフェイスの DNS サーバーではなく、これらの管理インターフェイスの DNS サーバーを使用して FQDN を解決します。

[DNSサーバ（DNS Servers）]：システムの管理アドレス用の DNS サーバ。デフォルトは OpenDNS パブリック DNS サーバです。これらは、両方とも外部インターフェイスからアクセスされるため、後で設定する外部インターフェイスの DNS サーバーと一致する可能性があります。

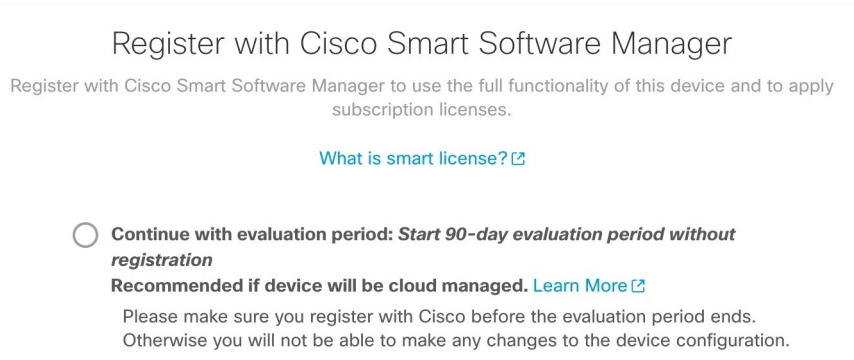
ファイアウォールのホスト名

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

図 *10*：時刻設定（*NTP*）



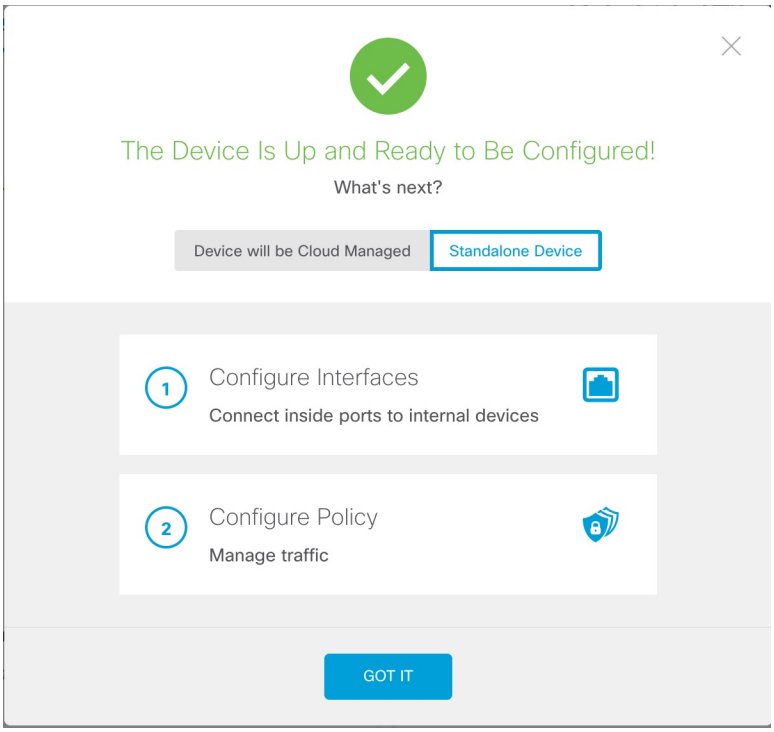
c) [登録せずに 90 日間の評価期間を開始（Start 90 day evaluation period without registration）] を選択します。



Firewall Threat Defense 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 Firewall Management CenterSecurity Cloud Control で実行されます。

d) [終了（Finish）] をクリックします。

図 *11* : 次のステップ



e) [スタンドアロンデバイス（Standalone Device）] を選択し、[了解（Got It）] を選択します。

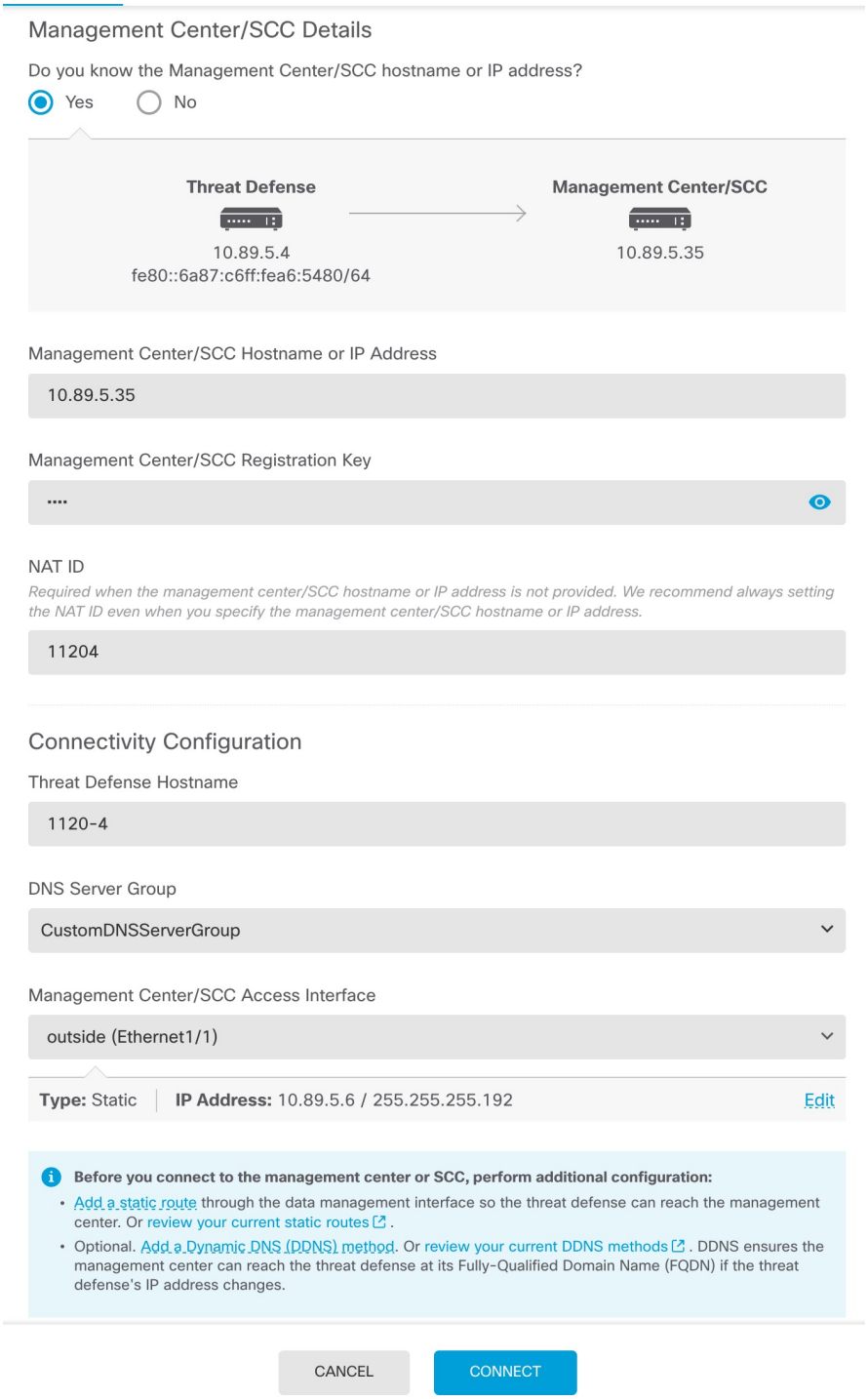
ステップ 4 追加のインターフェイスを設定する場合は、[デバイス（Device）] を選択し、[インターフェイス（Interface）] のサマリーにあるリンクをクリックします。

ステップ 5 **[デバイス（Device）] > [システム設定（System Settings）] > [集中管理（Central Management）]** の順に選択し、[続行（Proceed）] をクリックして Firewall Management CenterSecurity Cloud Control に登録します。

[**Management Center/SCC/Details**] を設定します。

（注）
古いバージョンでは、「SCC」の代わりに「CDO」と表示されることがあります。

図 *12 : Management Center/SCC* の詳細



a) [**Do you know the Management Center/SCC Hostname or IP address**] に対し、IP アドレスまたはホスト名を使用して Firewall Management Center に到達できる場合は [**Yes**] を、Firewall Management Center が NAT の内側にあるか、パブリック IP アドレスまたはホスト名がない場合は [**No**] をクリックします。

b) [**Yes**] を選択した場合は、[**Management Center/SCC Hostname/IP Address**] に入力します。

c) [**Management Center/SCC Registration Key**] を指定します。

このキーは、ファイアウォールを登録するときに Firewall Management Center 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 2 ～ 36 文字である必要があります。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、Firewall Management Center に登録する複数のファイアウォールに使用できます。

d) [NAT ID] を指定します。

この識別子は、Firewall Management Center でも指定する任意の 1 回限りの文字列です。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 2 ～ 36 文字である必要があります。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、Firewall Management Center に登録する他のファイアウォールには使用「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 6 [接続の設定（Connectivity Configuration）] を設定します。

a) [Threat Defenseのホスト名（Threat Defense Hostname）] を指定します。

この FQDN は外部インターフェイスに使用されます。

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。

登録後に外部 DNS サーバー設定を保持するには、Firewall Management Center で DNS プラットフォーム設定を再設定する必要があります。

c) [**Management Center/SCC Access Interface**] で [**Data Interface**] をクリックし、次に [**outside**] を選択します。

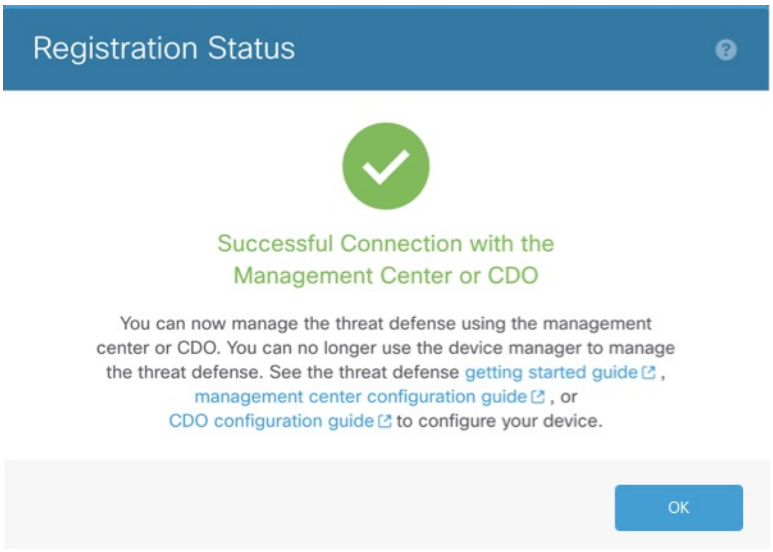
ステップ 7 （任意）[ダイナミックDNS（DDNS）方式の追加（Add a Dynamic DNS (DDNS) method）] をクリックします。

DDNS は、Firewall Threat Defense の IP アドレスが変更された場合に Firewall Management Center が FQDN で Firewall Threat Defense に到達できるようにします。

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）] ダイアログボックスに、Firewall Management CenterSecurity Cloud Control 登録の現在のステータスが表示されます。

図 *13* : 正常接続



ステップ 9 ステータス画面で [**Saving Management Center/ Registration Settings**] の手順を実行したら Firewall Management CenterSecurity Cloud Control に移動し、ファイアウォールを追加します。手動プロビジョニングを使用したデバイスの追加 を参照してください。

初期設定：CLI

CLI セットアップスクリプトを使用して、専用の管理 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を行います。

手順

ステップ 1 コンソールポートに接続して Firewall Threat Defense CLI にアクセスします。Firewall Threat Defense CLI へのアクセスを参照してください。

ステップ 2 管理インターフェイスの設定用の CLI セットアップスクリプトを完了します。

（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 セットアップスクリプト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。*Cisco Secure Firewall Threat Defense* コマンドリファレンスを参照してください。

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
Cisco General Terms
[...]
```

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

System initialization in progress.  Please stand by.
You must configure the network to continue.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [y]: n
```

ガイダンス：これらのタイプのアドレスの少なくとも 1 つについて **y** を入力します。管理インターフェイスを使用する予定がない場合でも、プライベートアドレスなどのIPアドレスを設定する必要があります。

```
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
```

ガイダンス：[手動（manual）] を選択します。マネージャアクセスに外部インターフェイスを使用する場合、DHCPはサポートされません。ルーティングの問題を防ぐために、このインターフェイスがマネージャアクセス インターフェイスとは異なるサブネット上にあることを確認してください。

```
Enter an IPv4 address for the management interface [192.168.45.61]: 10.89.5.17
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]:
```

ガイダンス：ゲートウェイを **data-interfaces** に設定します。この設定は、外部インターフェイスを通じてルーティングできるように、バックプレーンを介して管理トラフィックを転送します。

```
Enter a fully qualified hostname for this system [firepower]: 1010-3
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220,2620:119:35::35]:
Enter a comma-separated list of search domains or 'none' []: cisco.com
If your networking information has changed, you will need to reconnect.
Disabling IPv6 configuration: management0
Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
Setting DNS domains:cisco.com
```

ガイダンス：管理インターフェイスのDNSサーバーを設定します。これらは、両方とも外部インターフェイスからアクセスされるため、後で設定する外部インターフェイスのDNSサーバーと一致する可能性があります。

```
Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
```

ガイダンス：Firewall Management Center を使用する場合は、**no** と入力します。

```
Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'
```

ガイダンス：**routed**と入力します。外部マネージャアクセスは、ルーテッドファイアウォールモードでのみサポートされています。

```
Configuring firewall mode ...


Device is in OffBox mode - disabling/removing port 443 from iptables.
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 3 マネージャアクセス用の外部インターフェイスを設定します。

configure network management-data-interface

その後、外部インターフェイスの基本的なネットワーク設定を行うように求めるプロンプトが表示されます。

手動 IP アドレス

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
```

ガイダンス：登録後に外部 DNS サーバーを保持するには、Firewall Management Center で DNS プラットフォーム設定を再設定する必要があります。

```
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to change the
 manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

DHCP からの IP アドレス

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
```

```
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://dwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to change the
 manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

ステップ 4 Firewall Management Center を指定します。

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 Firewall Management Center.Firewall Management Center を直接アドレス指定できない場合は、**DONTRESOLVE** を使用します。この場合は、ファイアウォールが、到達可能な IP アドレスまたはホスト名を持っている必要があります。
- reg_key：Firewall Threat Defense を登録するときに Firewall Management Center 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 2 ～ 36 文字である必要があります。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：Firewall Management Center でも指定する、任意で一意の 1 回限りの文字列を指定します。NAT ID は 2 ～ 36 文字である必要があります。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、Firewall Management Center に登録する他のデバイスには使用できません。

例：

```
> configure manager add fmc-1.example.com regk3y78 natid56
Manager successfully configured.
```

ステップ 5 デバイスをリモート支社に送信できるように Firewall Threat Defense をシャットダウンします。

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、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。

a) **shutdown** コマンドを入力します。
b) 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）。
c) 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。

Management Center へのファイアウォールの登録

使用している展開方法に応じてファイアウォールを Firewall Management Center に登録します。

シリアル番号を使用したデバイスの追加（ゼロタッチプロビジョニング）

ゼロ タッチ プロビジョニング を使用すると、デバイスで初期設定を実行することなく、シリアル番号でデバイスを Firewall Management Center に登録できます。Firewall Management Center は、この機能のために Cisco Security Cloud および Security Cloud Control と統合されます。

（注） Firewall Management Center バージョン 7.4 では、Security Cloud Control を使用してデバイスを追加する必要があります。詳細については、7.4 のガイドを参照してください。ネイティブ Firewall Management Center ワークフローは 7.6 で追加されました。また、7.4 でのクラウド統合については、Firewall Management Center の [SecureXとの統合（SecureX Integration）] ページを参照してください。

デフォルト設定

ゼロタッチプロビジョニングを使用すると、以下のインターフェイスが事前設定されます。他の設定（内部の DHCP サーバー、アクセスコントロールポリシー、セキュリティゾーンなど）は設定されないことに注意してください。

- イーサネット 1/1：「外部」、DHCP からの IP アドレス、IPv6 自動設定
- イーサネット 1/2（または、VLAN1 インターフェイスの場合）：「内部」、192.168.95.1/24
- デフォルトルート：外部インターフェイスで DHCP を介して取得

要件

マネージャアクセス向けに外部インターフェイスを使用する際は、デフォルトで DHCP が使用されます。高可用性を有効にする前に、IP アドレスを静的アドレスに変更する必要があります。または、代わりに管理インターフェイスを使用することができます。高可用性を備えた管理で DHCP がサポートされます。

始める前に

- デバイスにパブリック IP アドレスまたは FQDN がない場合、Firewall Management Center のパブリック IP アドレス/FQDN を設定し（たとえば、NAT の背後にある場合）、デバイスが管理接続を開始できるようにします。**[システム（System）]**>**[設定（Configuration）]**>**[マネージャのリモートアクセス（Manager Remote Access）]** を参照してください。
- IP アドレスとデフォルトゲートウェイを提供する管理またはイーサネット 1/1 用の DHCP サーバー。

- OpenDNS パブリック DNS サーバーへのネットワークアクセス。IPv4：208.67.220.220 および 208.67.222.222。IPv6：2620:119:35::35。DHCP から取得した DNS サーバーは使用されません。

  次の名前を解決する必要があります。

  表 *3:* ゼロタッチプロビジョニングの *FQDN*

FQDN
*.cisco.com（多くの FQDN）
*.defenseorchestrator.com（多くの FQDN）
*.defenseorchestrator.eu（EU の場合、多くの FQDN）
0.sourcefire.pool.ntp.org、1.sourcefire.pool.ntp.org、2.sourcefire.pool.ntp.org
1.200.159.162.in-addr.arpa
60.19.239.178.in-addr.arpa
connected.by.freedominter.net
time.cloudflare.com
udc.neo4j.org

手順

ステップ 1 シリアル番号を使用してデバイスを初めて追加する場合は、Firewall Management Center と Cisco Security Cloud を統合します。

（注）
Firewall Management Center ハイアベイラビリティペアの場合は、セカンダリ Firewall Management Center を Cisco Security Cloud と統合する必要もあります。

a) **[統合（Integrations）] > [Security Cloud Control]**を選択します。
b) [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。

   このページがポップアップブロッカーによってブロックされていないことを確認してください。Cisco Security Cloud および Security Cloud Control アカウントをまだお持ちでない場合は、この手順の途中で追加できます。

   この統合の詳細については、「」『*Cisco Secure Firewall Management Center* アドミニストレーションガイド』の「System Configuration」の章を参照してください。

   Firewall Management Center と Cisco Security Cloud を統合した後、Security Cloud Control はオンプレミスの Firewall Management Center をオンボーディングします。Security Cloud Control は、ゼロタッチプ

ロビジョニング を動作させるためにインベントリに Firewall Management Center を必要とします。ただし、Security Cloud Control を直接使用する必要はありません。Security Cloud Control を使用する場合、その Firewall Management Center のサポートは、デバイスの導入準備、管理対象デバイスの表示、Firewall Management Center に関連付けられたオブジェクトの表示、および Firewall Management Center の相互起動に限定されています。

c) [ゼロタッチプロビジョニングの有効化（Enable Zero-Touch Provisioning）] がオンになっていることを確認します。

d) [保存（Save）] をクリックします。

ステップ 2 デバイスのシリアル番号を取得します。

- 梱包箱がある場合は、ラベルにシリアル番号が表示されています。
- シリアル番号は、のラベルに記載されています。
- コンソールにアクセスできる場合は、FXOS で、**show chassis detail** と入力します。正しいシリアル番号は**シリアル（SN）**と呼ばれることに注意してください。**PCB シリアル番号**は使用しないでください。Firewall Threat Defense CLI で、PCB シリアル番号を示す **show serial-number** ではなく、**show inventory** を入力します。Firewall Threat Defense スタートアップスクリプトで特定の設定を入力して、ゼロタッチプロビジョニング を無効にしないよう注意してください。

ステップ 3 LED を確認して、ファイアウォールの登録準備ができていることを確認します。

表 *4*: ゼロ タッチ プロビジョニング：管理対象（*M*）*LED* の動作

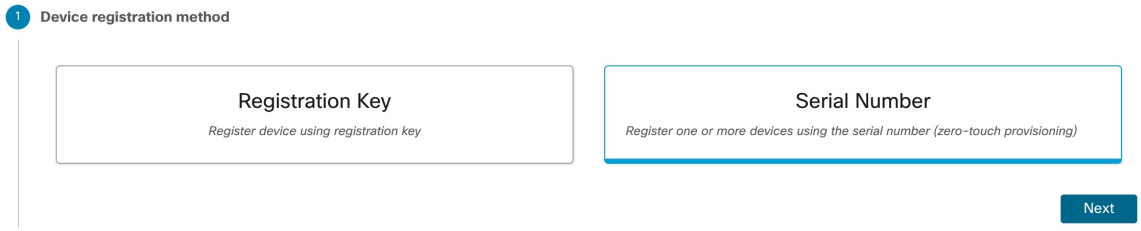
M LED	説明	ファイアウォールの電源を入れた後の時間（分:秒）
緑色で低速点滅	Cisco Cloud に接続され、オンボーディングの準備ができています	15:00 ～ 30:00
グリーンとオレンジに交互に点滅（エラー条件）	Cisco Cloud に接続できませんでした	15:00 ～ 30:00
緑色で点灯	オンボード済み	20:00 ～ 45:00

ステップ 4 **[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択します。

ステップ 5 [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。

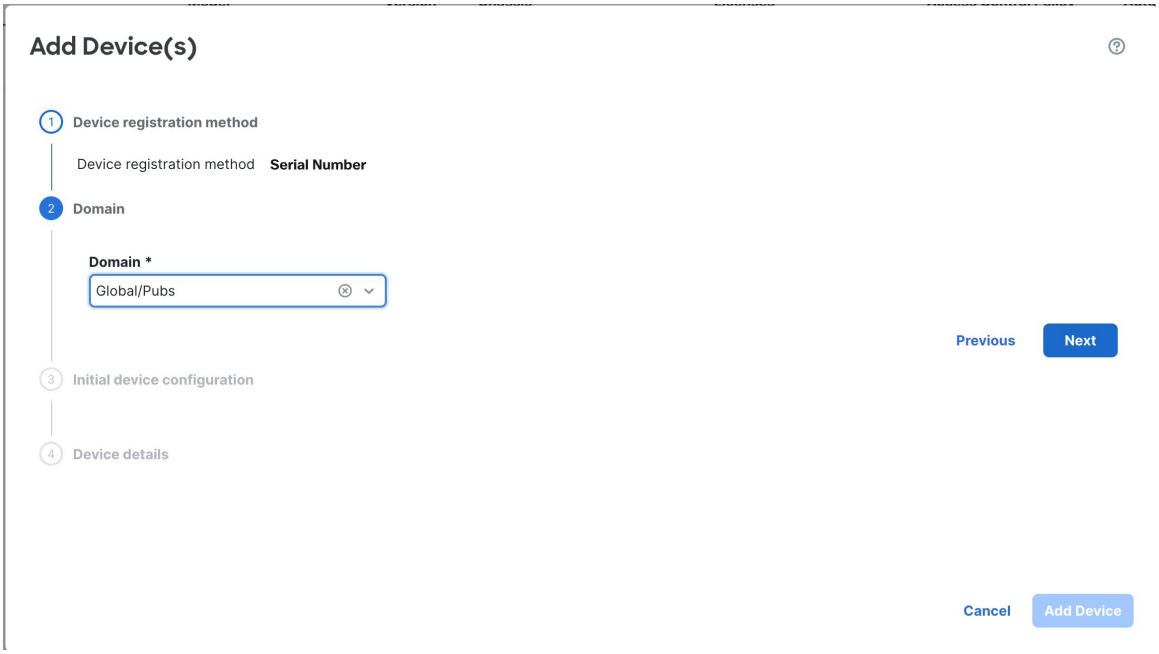
ステップ 6 [シリアル番号を使用（Use Serial Number）] をクリックし、[次へ（Next）] をクリックします。

図 *14* : デバイスの登録方法



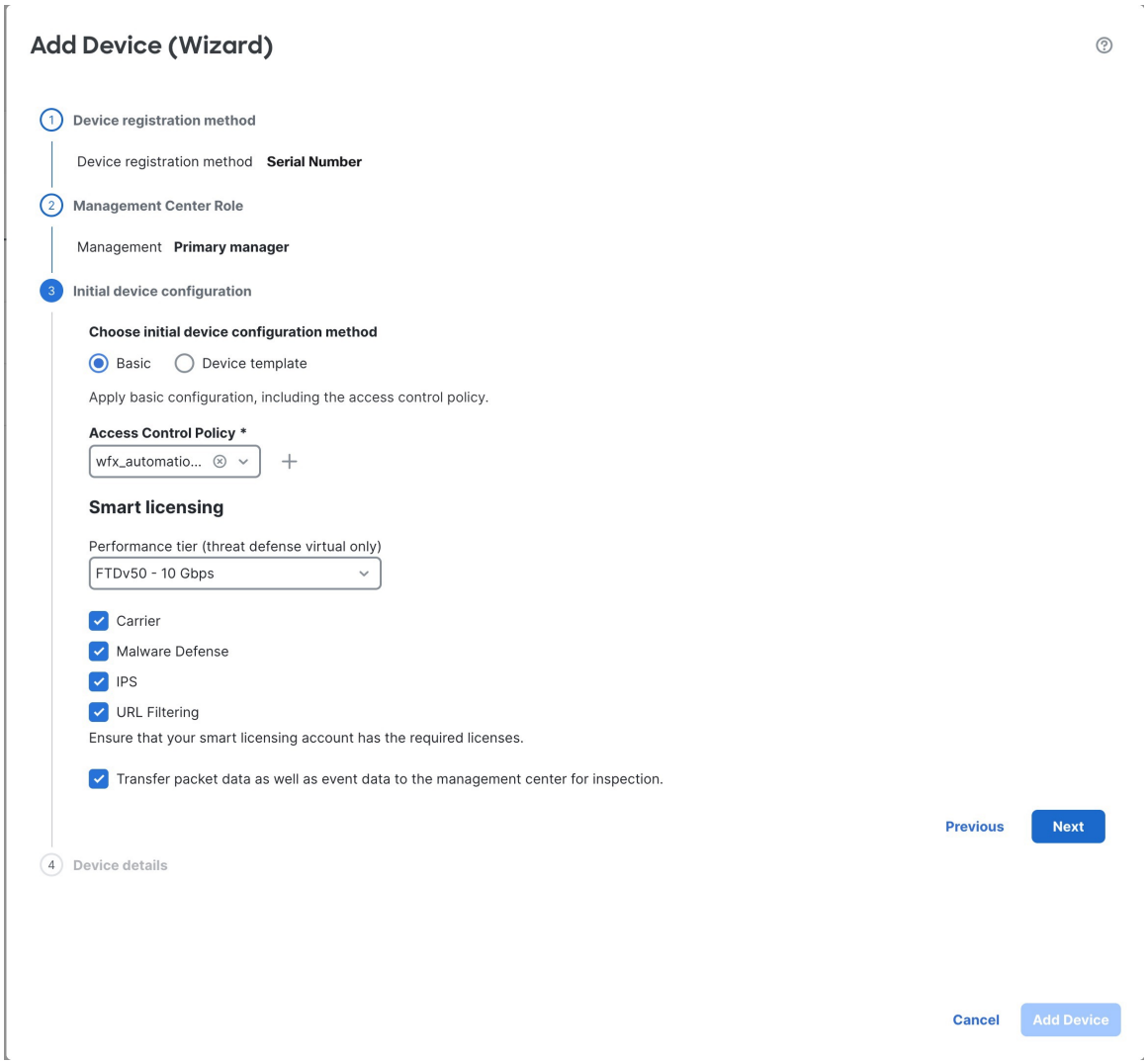
ステップ 7 マルチドメイン環境では、ドロップダウンリストから [ドメイン（Domain）] を選択し、[次へ（Next）] をクリックします。

図 *15* : ドメイン



ステップ 8 [デバイスの初期設定（Initial device configuration）] で、[基本（Basic）] オプションボタンをクリックします。

図 *16* : デバイスの初期設定方法



a) 登録後すぐに、デバイスに展開する最初の [アクセス コントロール ポリシー（Access Control Policy）] を選択するか、新しいポリシーを作成します。

デバイスが選択したポリシーに適合しない場合、展開は失敗します。この不適合には、複数の要因が考えられます。たとえば、ライセンスの不一致、モデルの制限、パッシブとインラインの問題、その他の構成ミスなどです。この障害の原因を解決した後、デバイスに手作業で設定を行います。

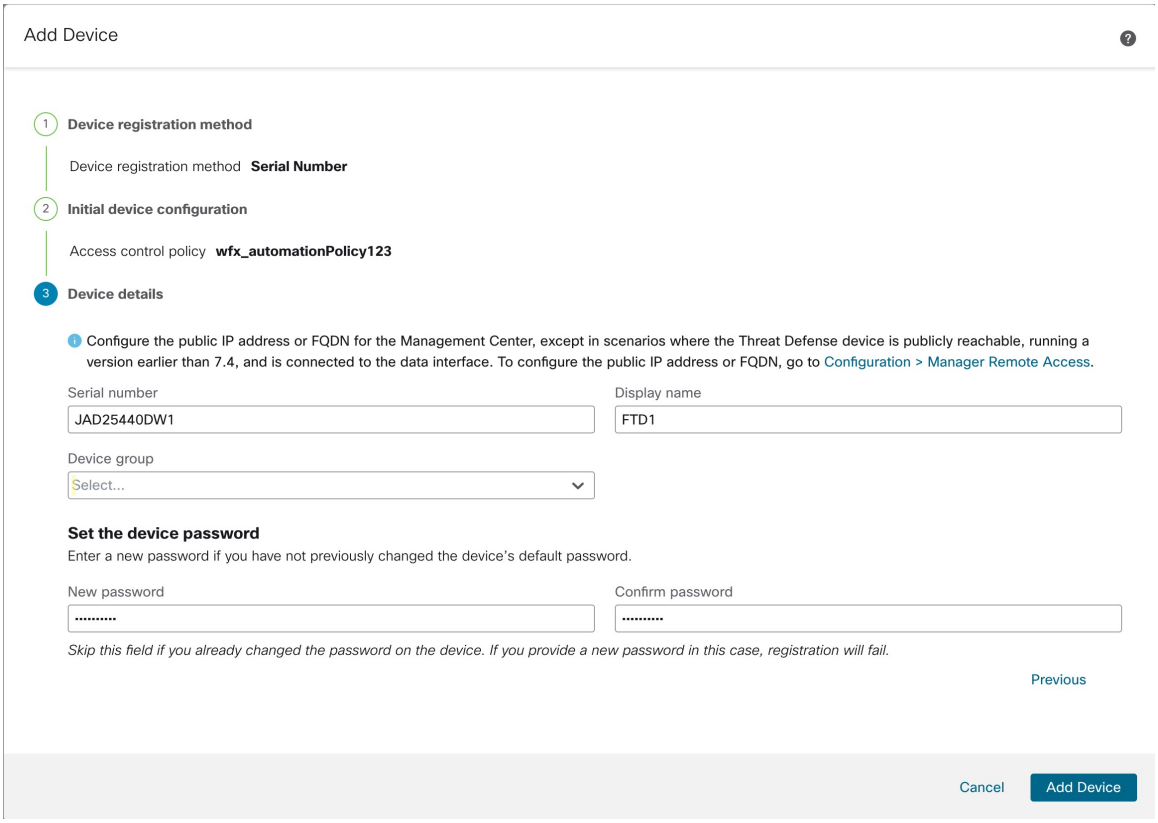
b) デバイスに適用する [スマートライセンス（Smart licensing）] ライセンスを選択します。

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）]** ページからライセンスを適用することもできます。

c) [次へ（Next）] をクリックします。

ステップ 9 [デバイスの詳細（Device details）] を設定します。

図 *17*：デバイスの詳細



a) [シリアル番号（Serial number）] にシリアル番号を入力します。
b) [表示名（Display name）] に、Firewall Management Center に表示する名前を入力します。
c) （任意）[デバイスグループ（Device Group）] を選択します。
d) **デバイスパスワードを設定します。**

このデバイスが未設定の場合、または新規インストールの場合は、新しいパスワードを設定する必要があります。すでにログインしてパスワードを変更している場合は、このフィールドを空白のままにします。そうしなければ、登録が失敗します。

ステップ 10 [Add Device] をクリックします。

Firewall Management Center がデバイスのハートビートを確認して通信を確立するまでに、最大 2 分かかる場合があります。登録が成功すると、デバイスがリストに追加されます。

外部インターフェイスで ゼロタッチプロビジョニング を使用する場合、Security Cloud Control は DDNS プロバイダーとして機能し、以下を実行します。

- [FMCのみ（FMC Only）] 方式を使用して外部で DDNS を有効にします。この方式は、ゼロタッチプロビジョニング デバイスでのみサポートされます。
- 外部 IP アドレスをホスト名 serial-number**.local** にマッピングします。

- IP アドレス/ホスト名マッピングを Firewall Management Center に提供し、ホスト名を正しい IP アドレスに解決できるようにします。
- DHCP リースが更新された場合など、IP アドレスが変更された場合に Firewall Management Center に通知します。

管理インターフェイスでゼロタッチプロビジョニングを使用する場合、DDNS はサポートされません。デバイスが管理接続を開始できるように、Firewall Management Center はパブリックに到達可能である必要があります。

Security Cloud Control を引き続き DDNS プロバイダーとして使用することも、後で Firewall Management Center の DDNS 設定を別の方式に変更することもできます。

手動プロビジョニングを使用したデバイスの追加

デバイスの IP アドレスまたはホスト名と登録キーを使用して、手動でファイアウォールを Firewall Management Center に登録します。

手順

ステップ 1 Firewall Management Center にログインします。

a) 次の URL を入力します。

https://*fmc_ip_address*

b) ユーザー名とパスワードを入力します。

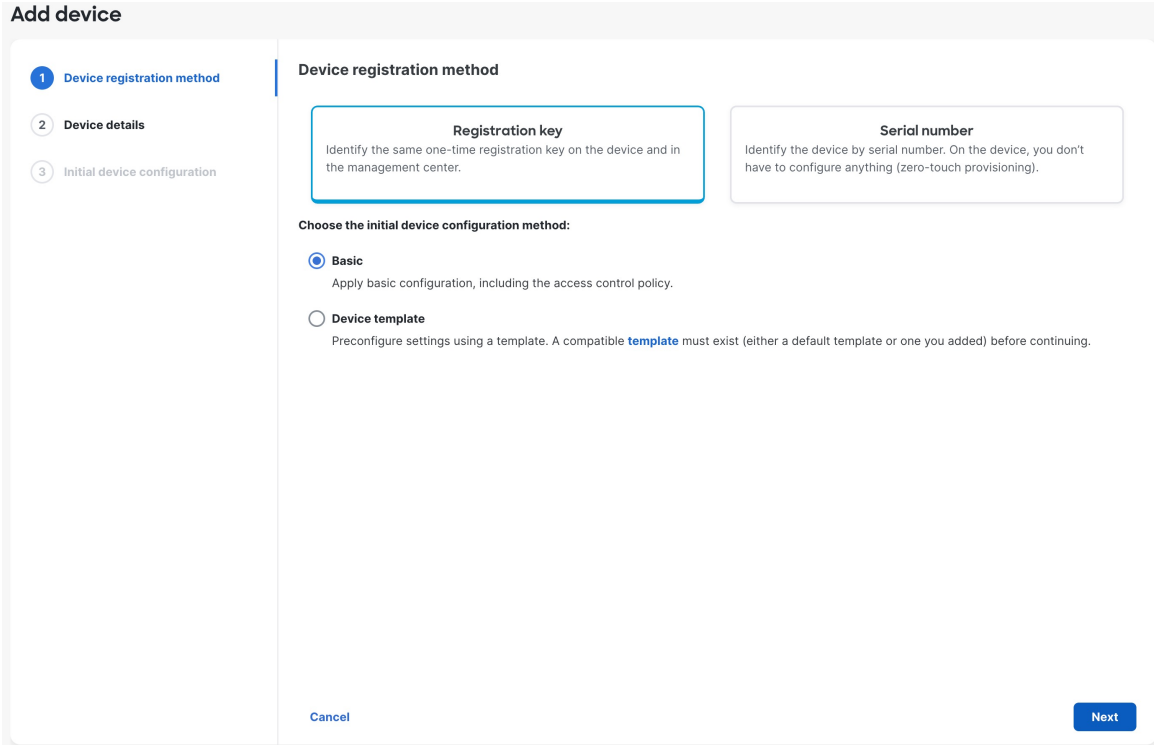
c) [ログイン（Log In）] をクリックします。

ステップ 2 **[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択します。

ステップ 3 [追加（Add）] ドロップダウンメニューから、[デバイス（Device）] [デバイス（ウィザード）（Device (Wizard)）] を選択します。

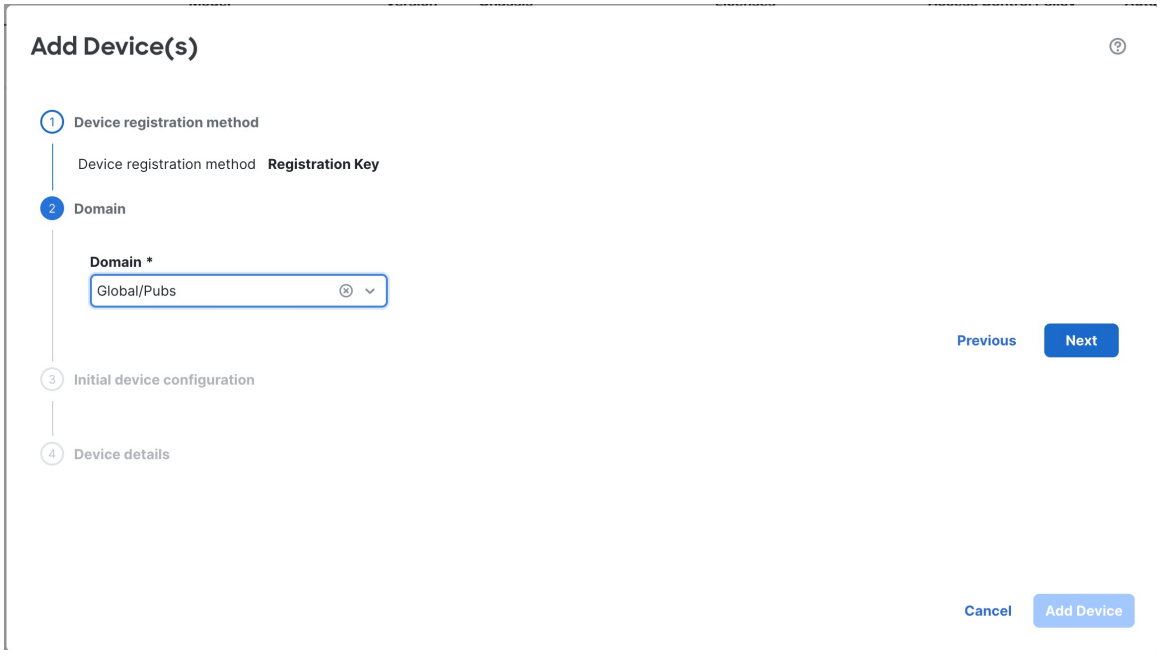
ステップ 4 [登録キー（Registration Key）] をクリックし、[次へ（Next）] をクリックします。

図 *18* : デバイスの登録方法



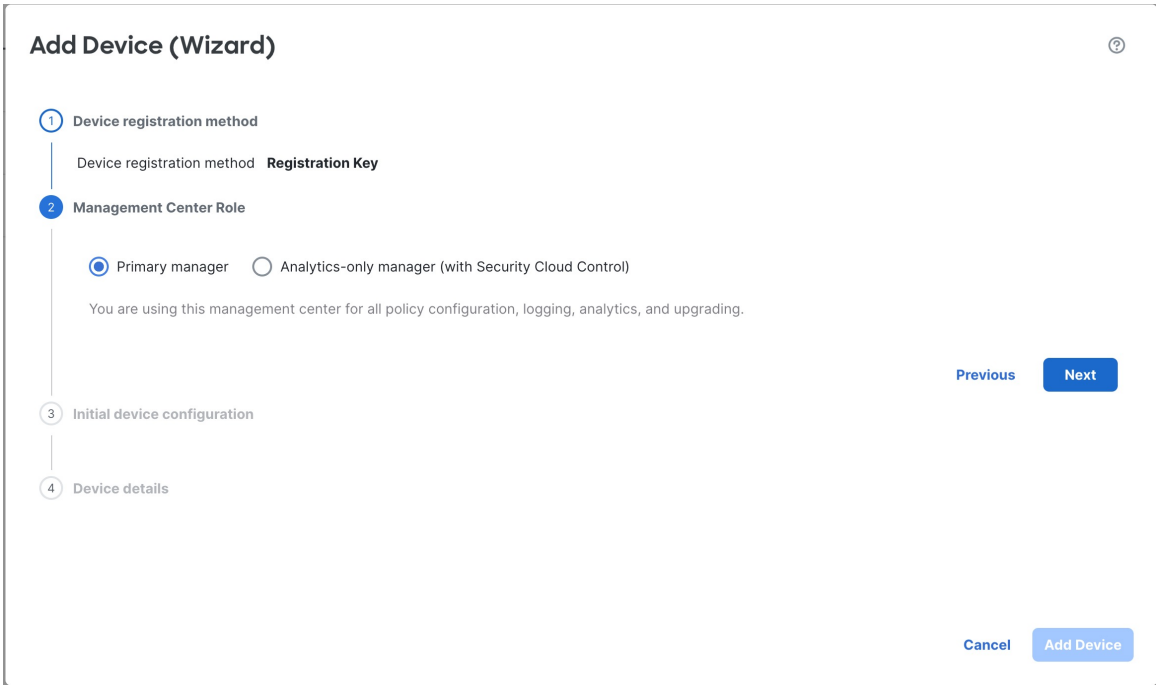
ステップ 5 マルチドメイン環境では、ドロップダウンリストから [ドメイン（Domain）] を選択し、[次へ（Next）] をクリックします。

図 *19* : ドメイン



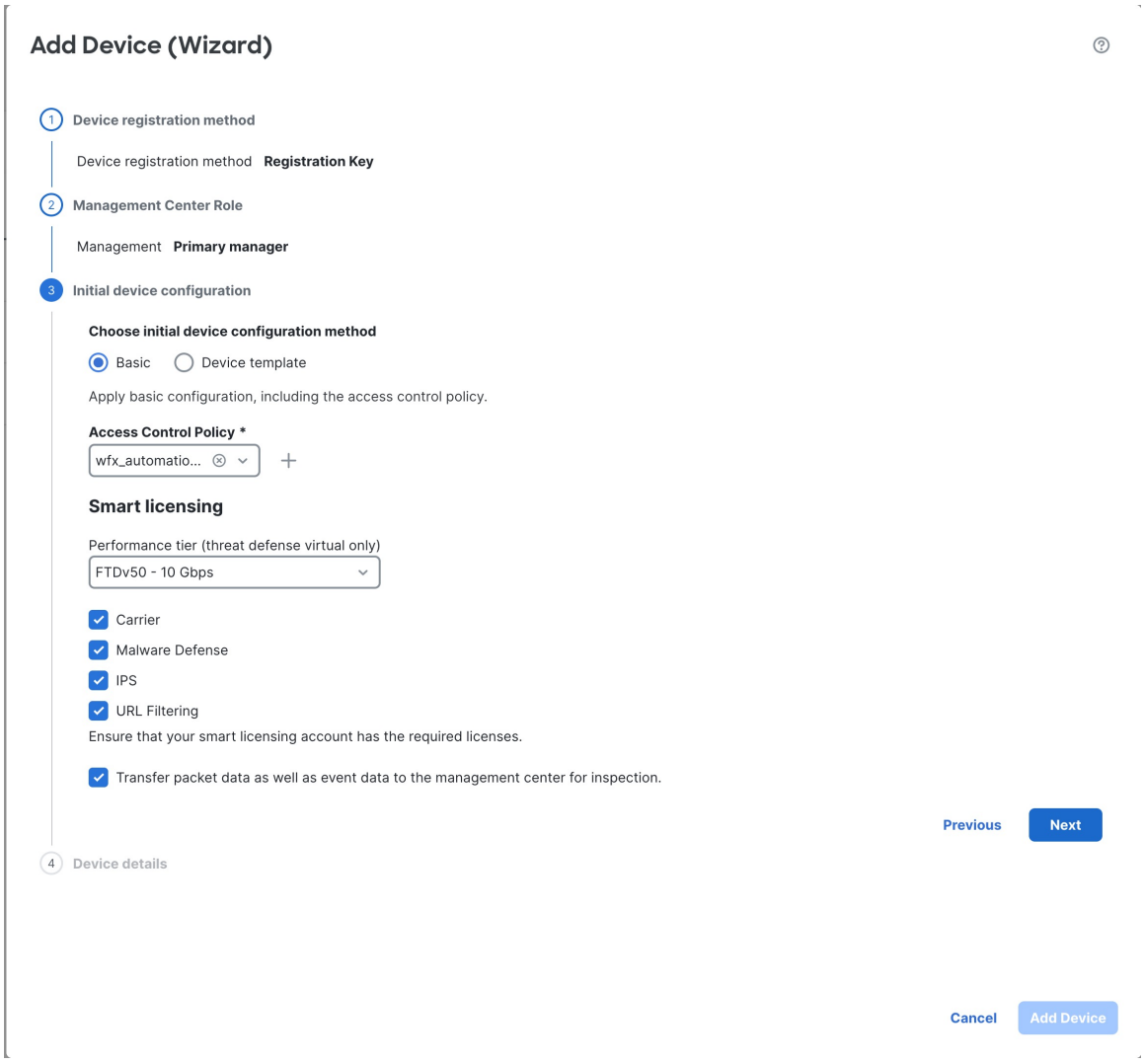
ステップ 6 通常の管理の場合は [プライマリマネージャ（Primary manager）] をクリックし、クラウド提供型 Firewall Management Center で管理されているデバイスの場合は [分析専用マネージャ（Analytics-only manager）] をクリックします。。

図 *20 : Management Center* のロール



ステップ 7 [デバイスの初期設定（Initial Device Configuration）] で、[基本（Basic）] をクリックします。

図 *21* : デバイスの初期設定



a) 登録時にデバイスに展開する最初の [アクセスコントロールポリシー（Access Control Policy）] を選択するか、新しいポリシーを作成します。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。「アクセス制御ルールの設定 （39 ページ）」を参照してください。

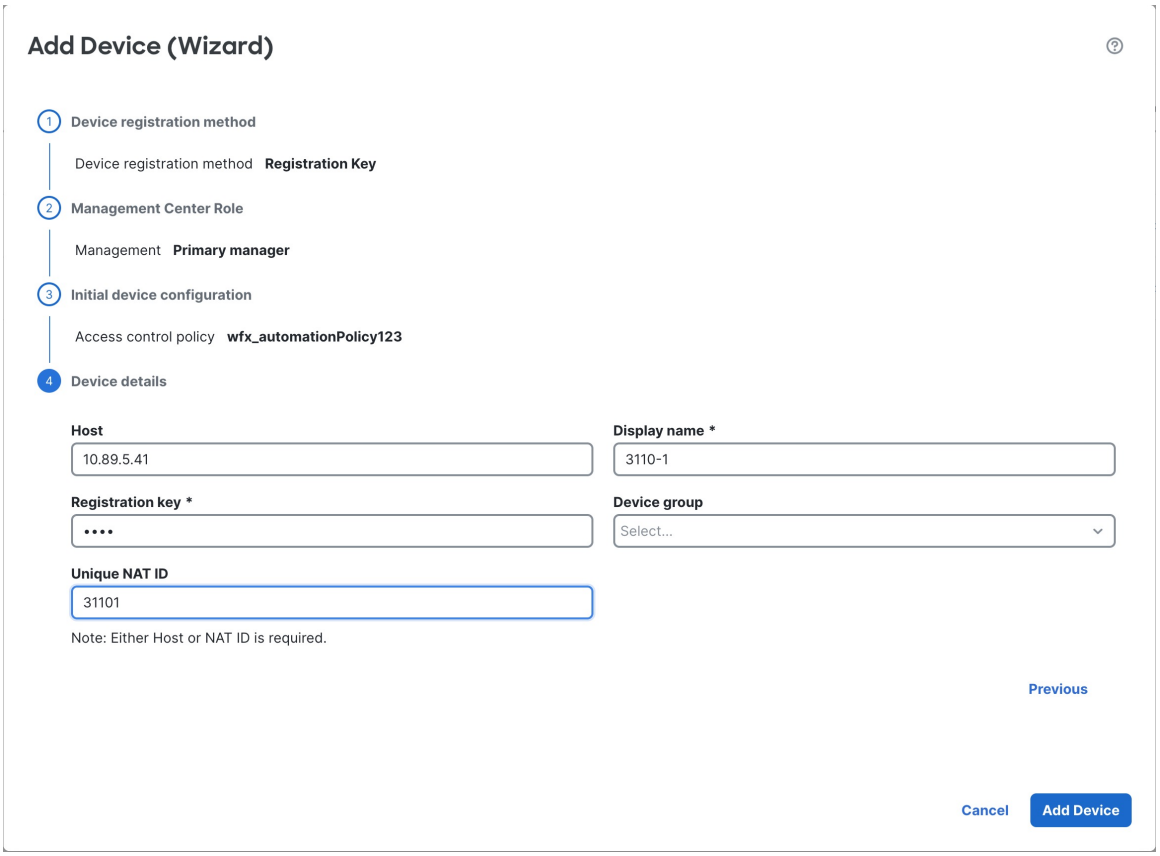
b) デバイスに適用する [スマートライセンス（Smart Licensing）] ライセンスを選択します。

[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、デバイスを追加した後にライセンスを適用することもできます（セキュアクライアント リモートアクセス VPN ライセンスを含む）。

c) [次へ（Next）] をクリックします。

ステップ 8 [デバイスの詳細（Device details）] を指定します。

図 *22* : デバイスの詳細（***Device Details***）



a) [ホスト（Host）] には、追加デバイスの IP アドレスまたはホスト名を入力します。デバイスの IP アドレスが不明な場合（NAT の背後にある場合など）は、このフィールドを空白のままにします。

b) [表示名（Display name）] フィールドに、Firewall Management Center でのデバイスの表示名を入力します。この名前は変更できません。

c) [登録キー（Registration key）] には、初期設定と同じ登録キーを入力します。

d) （任意） デバイスを [デバイスグループ（Device group）] に追加します。

e) [一意のNAT ID（Unique NAT ID）] には、初期設定と同じ ID を入力します。

f) [パケットの転送（Transfer Packets）] チェックボックスをオンにして、侵入イベントが発生するたびに、デバイスが検査のためにパケットを Firewall Management Center に転送するようにします。

侵入イベントごとに、デバイスは、イベント情報とイベントをトリガーしたパケットを検査のために Firewall Management Center 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 Firewall Management Center に送信され、パケットは送信されません。

ステップ 9 [Add Device] をクリックします。

Firewall Management Center がデバイスのハートビートを確認して通信を確立するまでに、最大 2 分かかる場合があります。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。デバイスの登録に失敗した場合は、次の項目を確認してください。

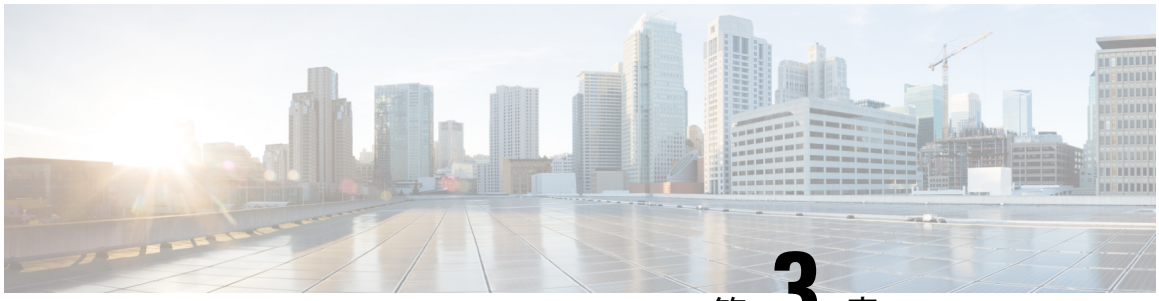
- ping：デバイスの CLI にアクセスし、次のコマンドを使用して Firewall Management Center の IP アドレスへの ping を実行します。

  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。デバイスの IP アドレスを変更する必要がある場合は、**configure network** {**ipv4** | **ipv6**} **manual** コマンドを使用します。

- 登録キー、NAT ID、および Firewall Management Center 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、デバイスで登録キーと 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。



第 3 章

基本ポリシーの設定

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。

セキュリティポリシーをカスタマイズして、より高度な検査を含めることもできます。

- DHCP サーバーの設定 （33 ページ）
- NAT の設定 （35 ページ）
- アクセス制御ルールの設定 （39 ページ）
- 外部インターフェイスでの SSH の有効化 （42 ページ）
- 設定の展開 （43 ページ）

DHCP サーバーの設定

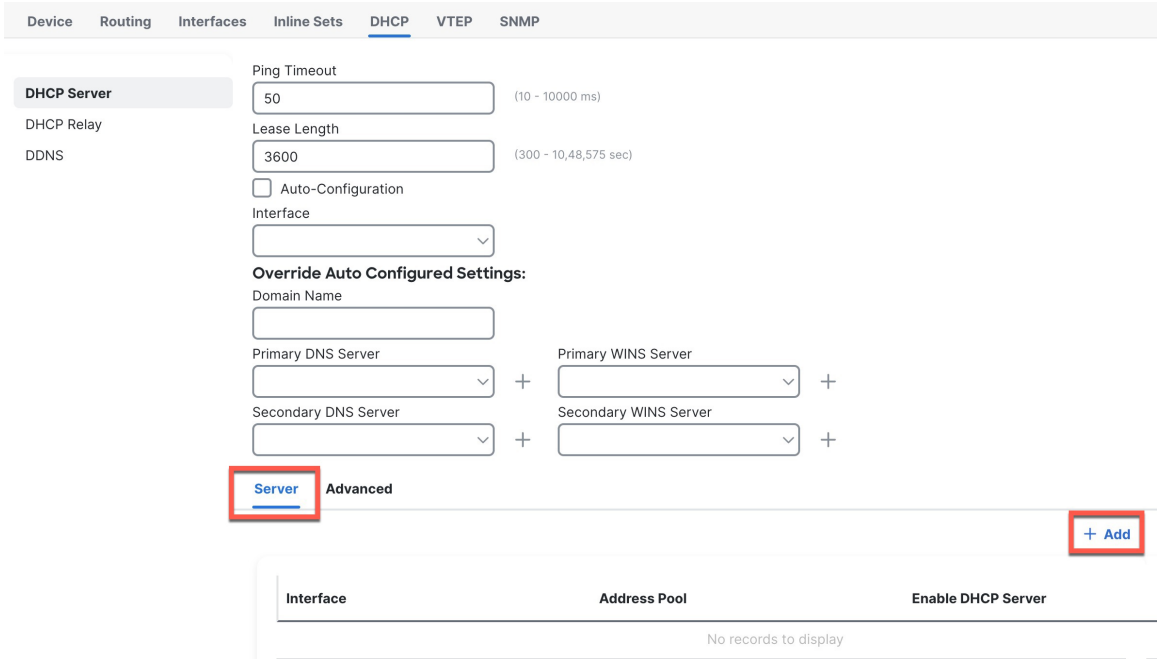
クライアントで DHCP を使用してファイアウォールから IP アドレスを取得するようにする場合は、DHCP サーバーを有効にします。

手順

ステップ 1 [デバイス（Devices）]、[デバイス管理（Device Management）] の順に選択し、デバイスの [編集（Edit）]（✎） をクリックします。 >

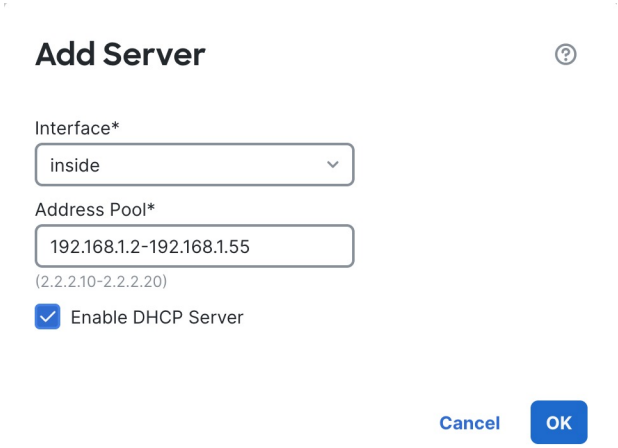
ステップ 2 **[DHCP]** > **[DHCPサーバー（DHCP Server）]** を選択します。

図 *23 : DHCP* サーバー



ステップ 3 [サーバー（Server）] エリアで、[追加（Add）] をクリックし、以下のオプションを設定します。

図 *24 :* サーバーの追加



- [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名を選択します。
- [アドレスプール（Address Pool）]：IP アドレスの範囲を設定します。IP アドレスは、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。

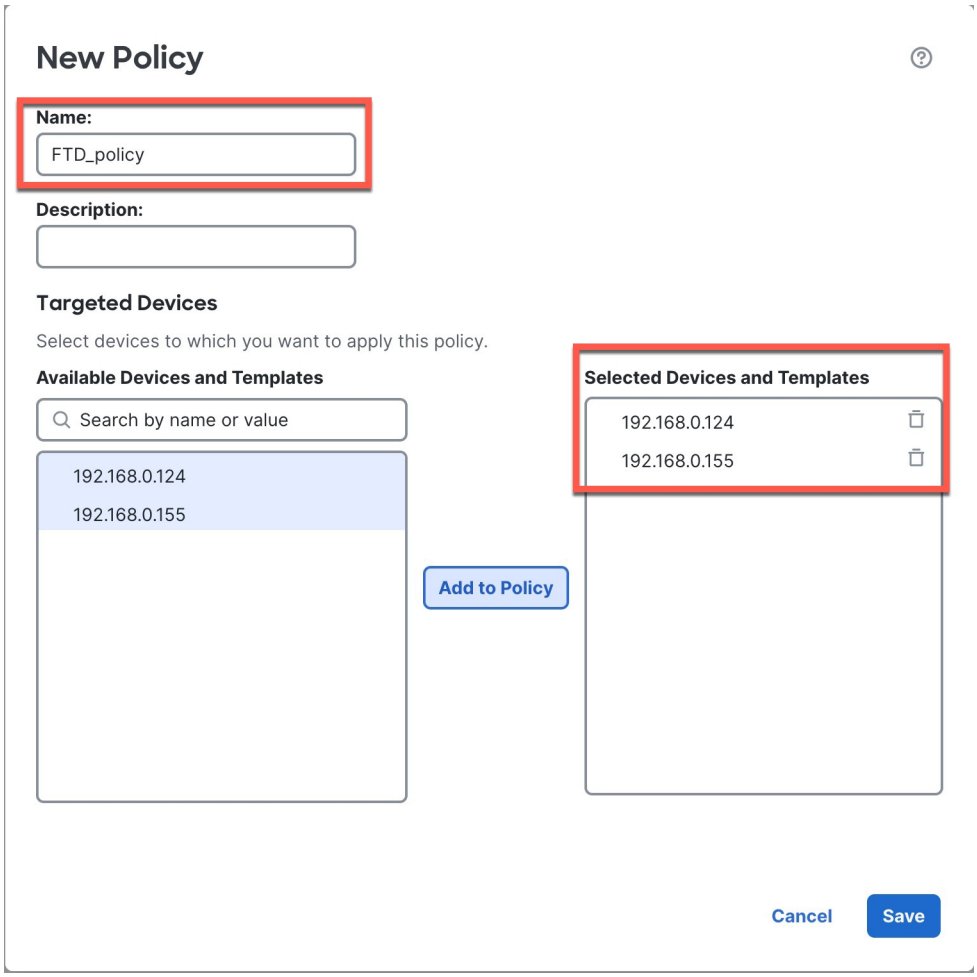
NAT の設定

この手順では、内部クライアントが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する NAT ルールを作成します。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

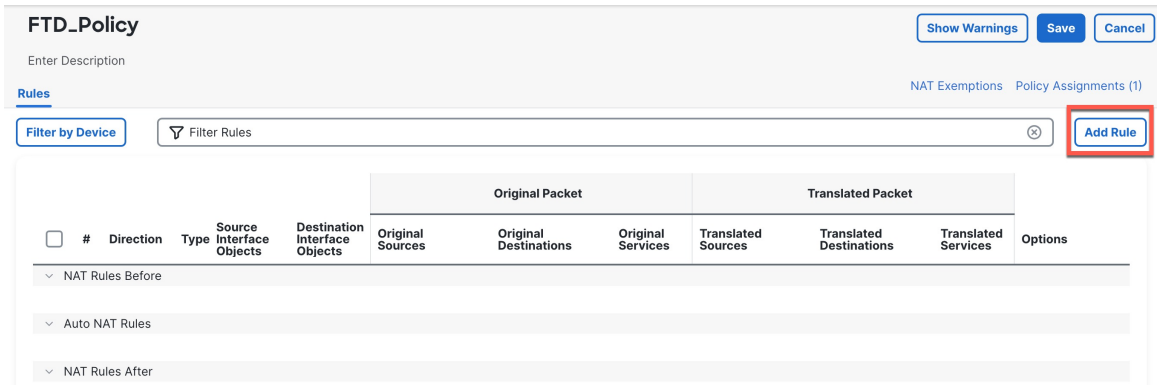
ステップ 1 **[デバイス（Devices）]** > **[NAT]** の順に選択し、**[新しいポリシー（New Policy）]** をクリックします。
ステップ 2 ポリシーに名前を付け、ポリシーを使用するデバイスを選択し、[保存（Save）] をクリックします。

図 *25* : 新しいポリシー



ポリシーが Firewall Management Center 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。

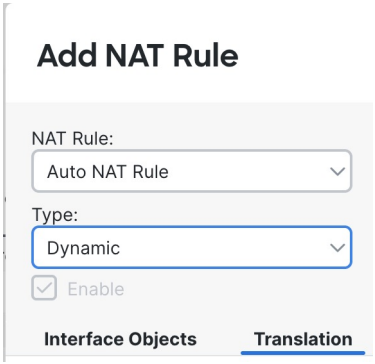
図 *26* : *NAT* ポリシー



ステップ 3 [ルールの追加（Add Rule）] をクリックします。

ステップ 4 基本ルールのオプションを設定します。

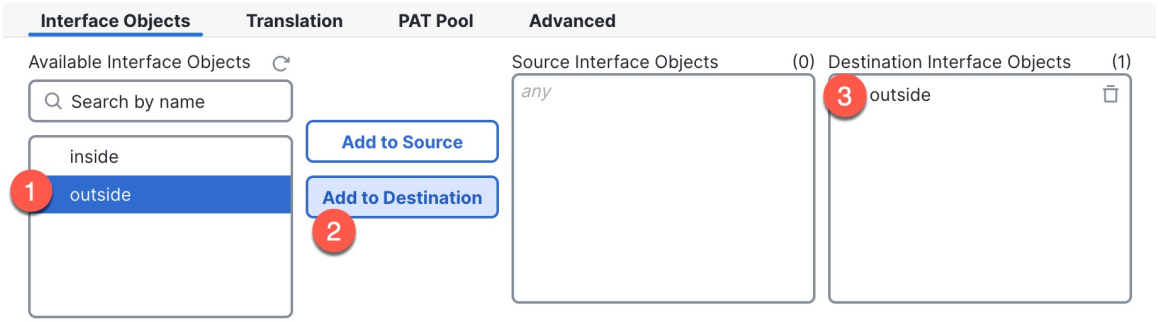
図 27 : 基本ルールのオプション



- [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。

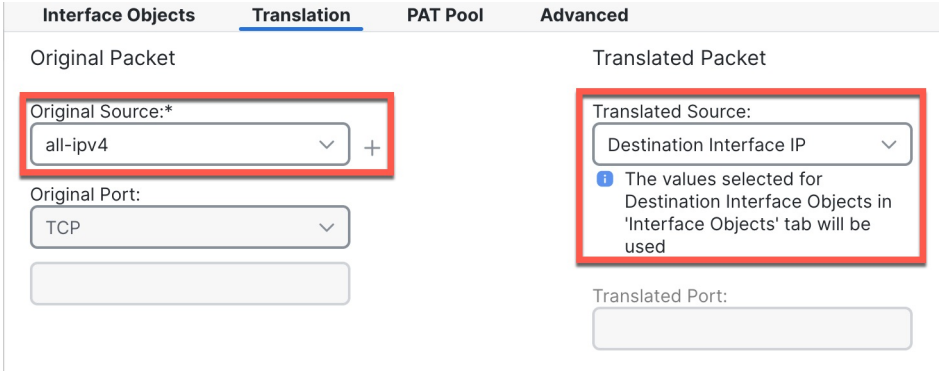
ステップ 5 [インターフェイスオブジェクト（Interface objects）] ページで、[使用可能なインターフェイスオブジェクト（Available Interface Objects）] 領域から [宛先インターフェイスオブジェクト（Destination Interface Objects）] 領域に外部ゾーンを追加します。

図 28 : インターフェイス オブジェクト



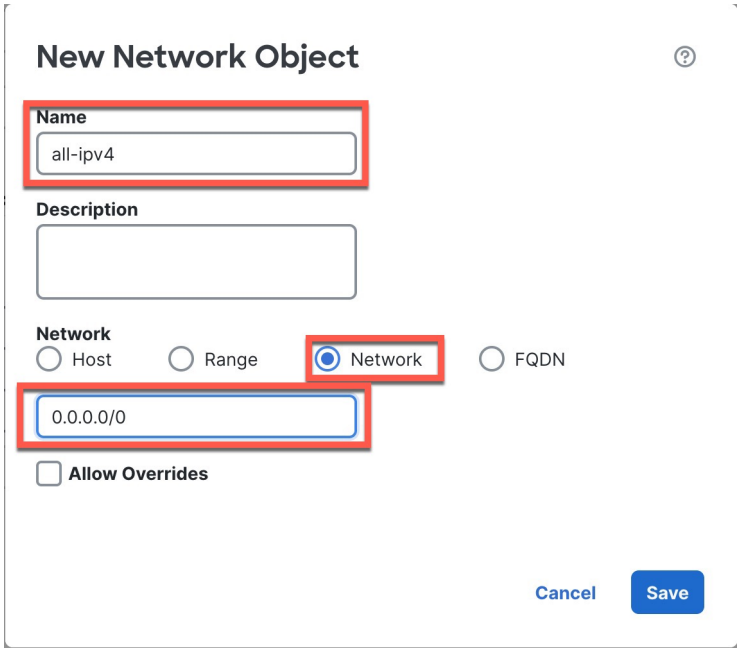
ステップ 6 [変換（Translation）] ページで、次のオプションを設定します。

図 *29* : 変換



- **[元の送信元（Original Source）]**：[追加（Add）]（＋）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。

  図 *30* : 新しいネットワークオブジェクト



（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。

アクセス制御ルールの設定

デバイスを登録したときに、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。アクセス コントロール ポリシーには、順番に評価される複数のルールを含めることができます。

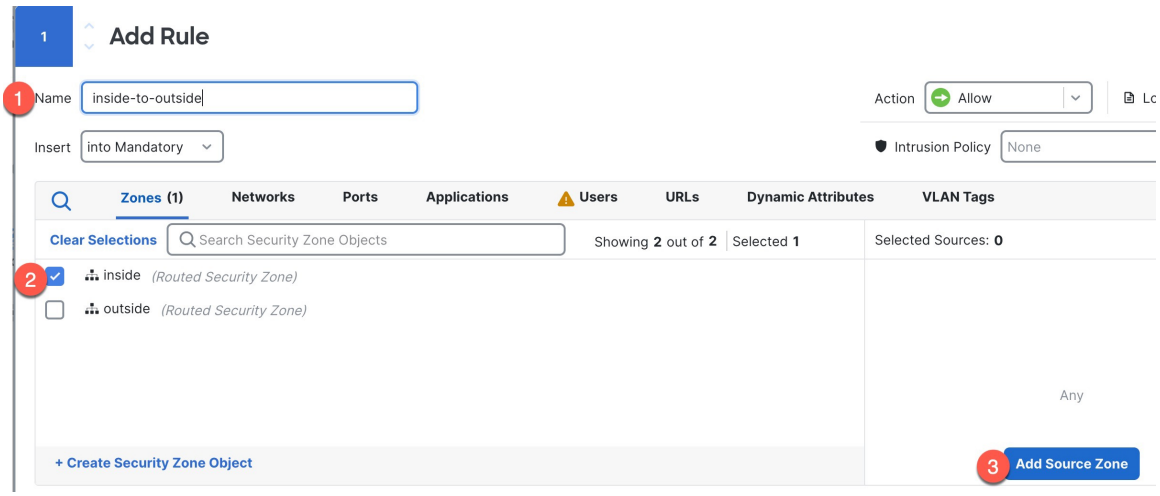
次の手順では、内部ゾーンから外部ゾーンへのすべてのトラフィックを許可するアクセス制御ルールを作成します。

手順

ステップ 1 **[ポリシー（Policies）] > [セキュリティポリシー（Security policies）] > [アクセス制御（Access Control）]** を選択し、デバイス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（Edit）]（✎）をクリックします。

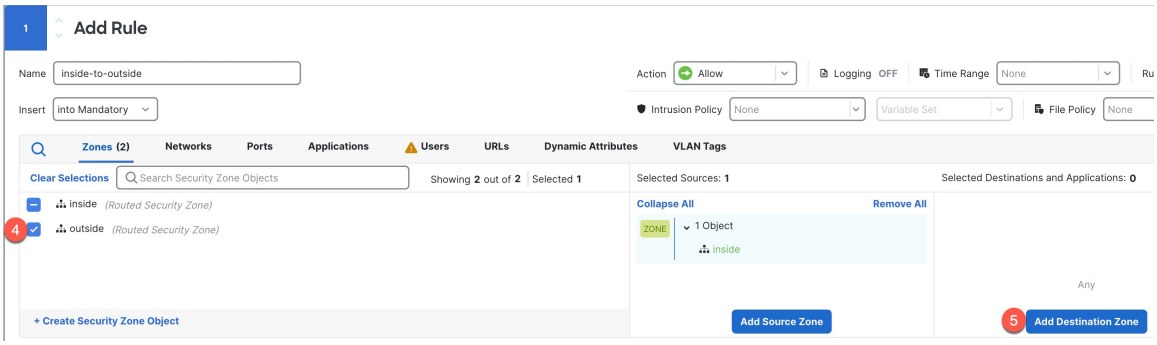
ステップ 2 [ルールを追加（Add Rule）] をクリックし、次のパラメータを設定します。

図 *31* : 送信元ゾーン（*Source Zone*）



1. このルールに名前を付けます（たとえば、**inside-to-outside**）。
2. [ゾーン（Zones）] から内部ゾーンを選択します。
3. [送信元ゾーンの追加（Add Source Zone）] をクリックします。

図 *32* : 宛先ゾーン（***Destination Zone***）



4. [ゾーン（Zones）] から外部ゾーンを選択します。

5. [宛先ゾーンを追加（Add Destination Zone）] 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 （任意）パケットフロー図でポリシータイプをクリックして、関連付けられたポリシーをカスタマイズします。

[プレフィルタ（Prefilter）]、[復号（Decryption）]、[セキュリティインテリジェンス（Security Intelligence）]、および [アイデンティティ（Identity）] ポリシーは、アクセス制御ルールの前に適用されます。これらのポリシーをカスタマイズする必要はありませんが、ネットワークのニーズを把握した後、信頼できるトラフィックに fastpath を適用（処理をバイパス）したりトラフィックをブロックしてその後の処理が不要になるようにすることで、ネットワークのパフォーマンスを向上させることができます。

図 *33* : アクセス制御の前に適用されるポリシー

- [プレフィルタルール（Prefilter Rules）]：デフォルトのプレフィルタポリシーは、他のルールが適用される（分析する）すべてのトラフィックを通過させます。デフォルトポリシーに加えることができる唯一の変更は、トンネルトラフィックを「ブロックする」ことです。それ以外では、新しいプレフィルタポリシーを作成して、分析（通過）、fastpath 処理（以降のチェックをバイパス）、またはブロックできるアクセス コントロール ポリシーに関連付けることができます。

  プレフィルタを使用すると、ブロックまたは fastpath 処理のいずれかによって、トラフィックがさらに進む前に処理することで、パフォーマンスを向上させることができます。新しいポリシーでは、「トンネル」ルールと「プレフィルタ」ルールを追加できます。トンネルルールを使用すると、プレーンテキスト（非暗号化）のパススルートンネルを fastpath 処理、ブロック、または再ゾーン化できます。プレフィルタルールを使用すると、IP アドレス、ポート、およびプロトコルで識別される非トンネルトラフィックを fastpath 処理またはブロックできます。

  たとえば、ネットワーク上のすべての FTP トラフィックをブロックし、管理者からの SSH トラフィックを高速パスする場合は、新しいプレフィルタ ポリシーを追加できます。

- [復号（Decryption）]：デフォルトでは、復号は適用されません。復号は、ネットワークトラフィックをディープインスペクションに公開する方法です。ほとんどの場合、トラフィックを復号する必要はなく、法的に許可されている場合にのみ復号できます。ネットワークを最大限に保護するために、重

要なサーバーへのトラフィックや、信頼できないネットワークセグメントからのトラフィックには、復号ポリシーを使用することをお勧めします。

- [セキュリティ インテリジェンス（Security Intelligence）]：（IPS ライセンスが必要）セキュリティ インテリジェンスはデフォルトで有効になっています。セキュリティ インテリジェンスは、悪意のあるアクティビティに対するもう 1 つの早期防御で、さらなる処理のために接続をアクセス コントロール ポリシーに渡す前に適用されます。セキュリティ インテリジェンスは、レピュテーション インテリジェンスを使用して、シスコの脅威インテリジェンス組織である Talos が提供する IP アドレス、URL、およびドメイン名との接続を迅速にブロックします。必要に応じて、IP アドレス、URL、ドメインを追加または削除できます。

  （注）
  IPS ライセンスがない場合、このポリシーは、アクセス コントロール ポリシーで有効と表示されていても展開されません。

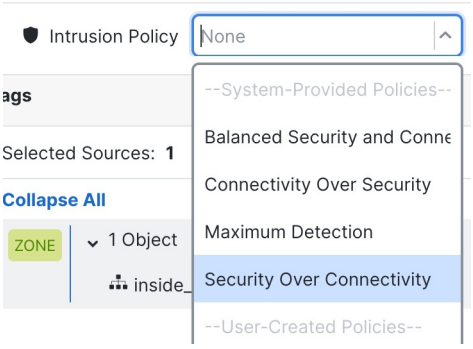
- [アイデンティティ（Identity）]：アイデンティティはデフォルトでは適用されません。アクセス コントロール ポリシーによるトラフィックの処理を許可する前に、ユーザーに認証を要求できます。

ステップ 4 （任意） アクセス制御ルールの後に適用される侵入ポリシーを追加します。

侵入ポリシーは、トラフィックのセキュリティ違反を検査する定義済みの一連の侵入検出および侵入防止設定です。Firewall Management Center には、多数のシステム提供のポリシーが含まれており、そのまま有効にすることもカスタマイズすることもできます。この手順では、システム提供のポリシーを有効にします。

a) [侵入ポリシー（Intrusion Policy）] ドロップダウンリストをクリックします。

図 *34*：システム提供の侵入ポリシー

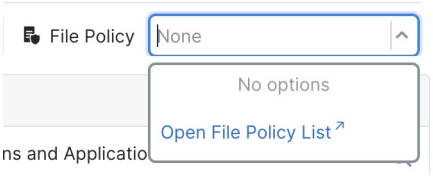


b) リストからシステム提供のポリシーを 1 つ選択します。

ステップ 5 （任意） アクセス制御ルールの後に適用されるファイルポリシーを追加します。

a) [ファイルポリシー（File Policy）] ドロップダウンリストをクリックし、既存のポリシーを選択するか、[ファイルポリシーリストを開く（Open File Policy List）] を選択してポリシーを追加します。

図 *35 :* ファイルポリシー（*File Policy*）



新しいポリシーの場合は、**[[ポリシー（Policies）] > [セキュリティポリシー（Security policies）] > [マルウェアとファイル（Malware & File）]**] ページが別のタブで開きます。

b) ポリシーの作成の詳細については、*Cisco Secure Firewall Device Manager コンフィギュレーション ガイド*を参照してください。

c) [ルールの追加（Add Rule）]ページに戻り、ドロップダウンリストから新しく作成したポリシーを選択します。

ステップ 6 [Apply] 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 7 [保存（Save）] をクリックします。

外部インターフェイスでの SSH の有効化

ここでは、外部インターフェイスへの SSH 接続を有効にする方法について説明します。

デフォルトでは、初期設定時にパスワードを設定した **admin** ユーザーを使用できます。

手順

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択して、Firewall Threat Defense ポリシーを作成するか編集します。

ステップ 2 [SSHアクセス（SSH Access）] を選択します。

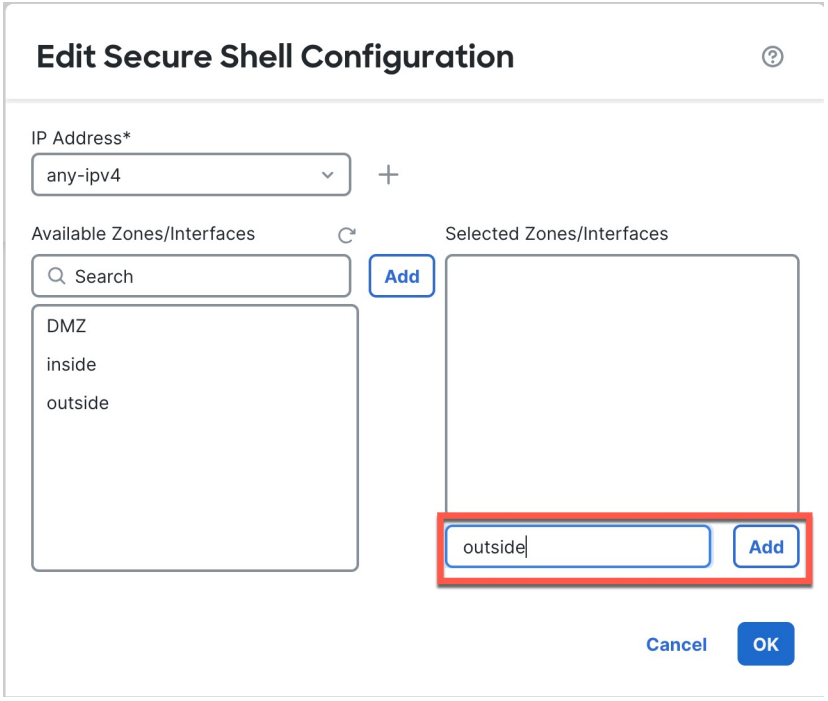
ステップ 3 SSH 接続を許可する外部インターフェイスと IP アドレスを指定します。

a) [追加（Add）] をクリックして新しいルールを追加するか、[編集（Edit）] をクリックして既存のルールを編集します。

b) ルールのプロパティを設定します。

- [IP Address]：SSH 接続を許可するホストまたはネットワークを特定するネットワークオブジェクトまたはグループ。オブジェクトをドロップダウンメニューから選択するか、または[+]をクリックして新しいネットワークオブジェクトを追加します。
- [使用可能なゾーン/インターフェイス（Available Zones/Interfaces）]：[選択したゾーン/インターフェイス（Selected Zones/Interfaces）] リストの下のフィールドに外部ゾーンを追加するか「外部」インターフェイス名を入力し、[追加（Add）] をクリックします。

図 *36* : 外部インターフェイスでの *SSH* の有効化



c) [OK] をクリックします。

ステップ 4 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]**>**[展開（Deploy）]** に移動して、割り当てたデバイスにポリシーを展開できるようになります。変更はポリシーを展開するまで有効になりません。

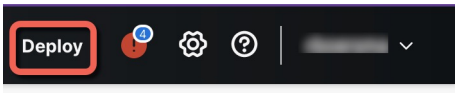
設定の展開

設定の変更をデバイスに展開します。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

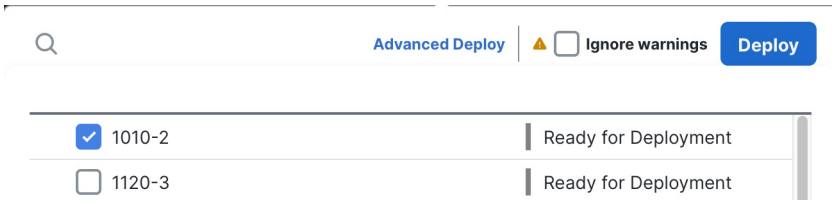
ステップ 1 右上の [展開（Deploy）] をクリックします。

図 *37* : 展開



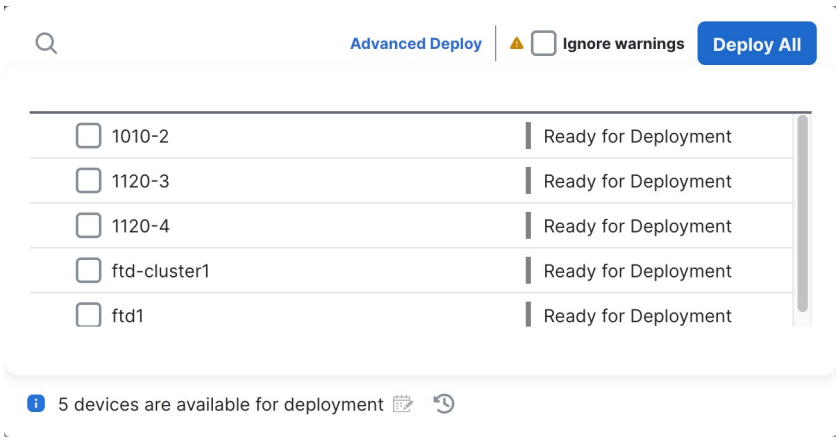
ステップ 2 迅速な展開の場合は、特定のデバイスのチェックボックスをオンにして [展開（Deploy）] をクリックします。

図 *38* : 選択したものを展開



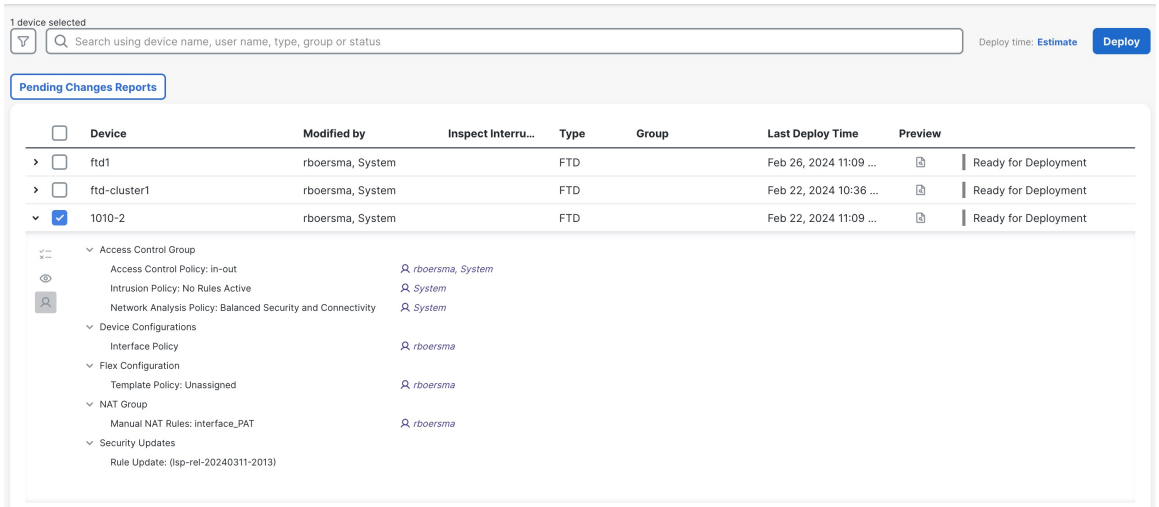
または、[すべて展開（Deploy All）] をクリックしてすべてのデバイスに展開します。

図 *39* : すべて展開



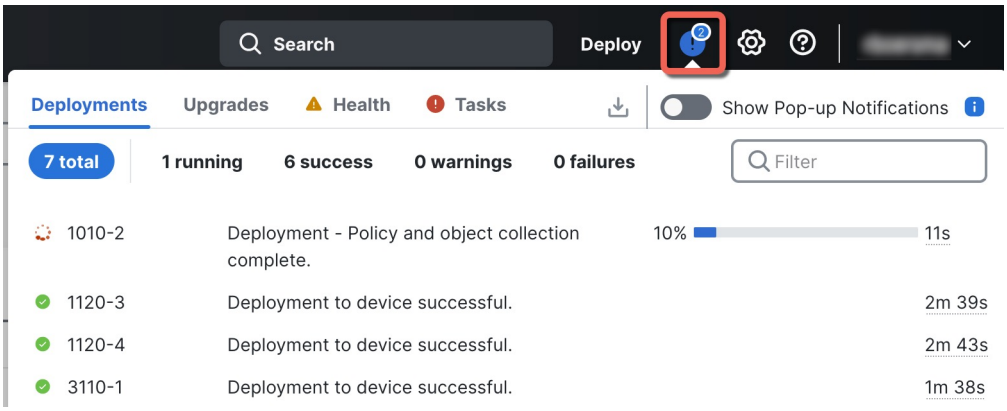
それ以外の場合は、追加の展開オプションを設定するために、[高度な展開（Advanced Deploy）] をクリックします。

図 *40* : 高度な展開



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。

図 *41* : 展開ステータス



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。

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。