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

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。

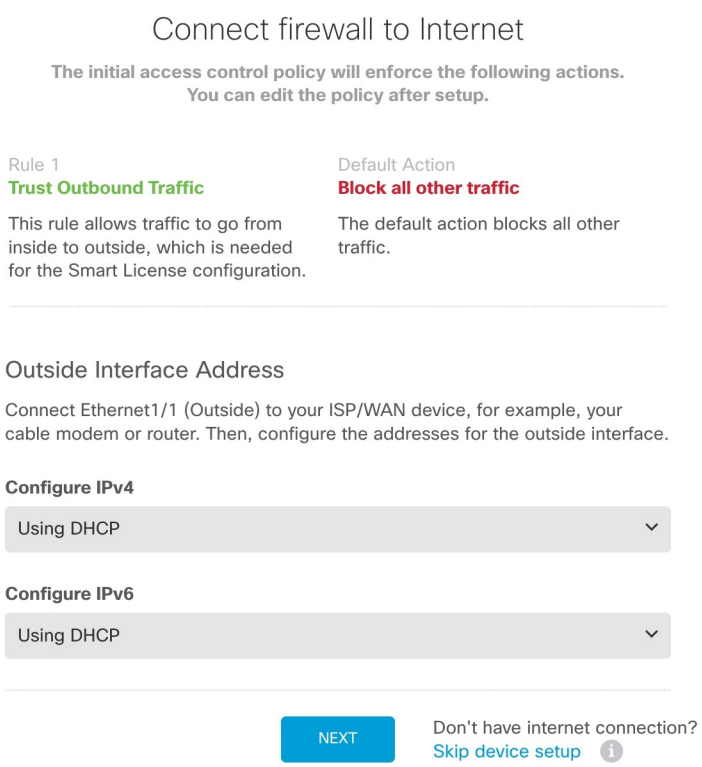
c) 一般規約を読んで同意し、管理者パスワードを変更するように求められます。

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 *1:* 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

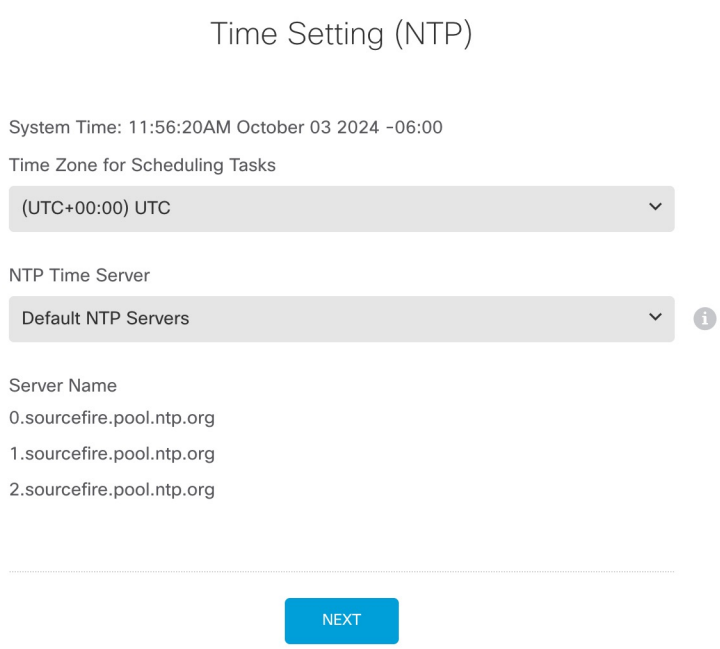
フェイスを介してバックプレーン経由で回送される管理トラフィックは、外部インターフェイスの DNS サーバーではなく、これらの管理インターフェイスの DNS サーバーを使用して FQDN を解決します。

[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。

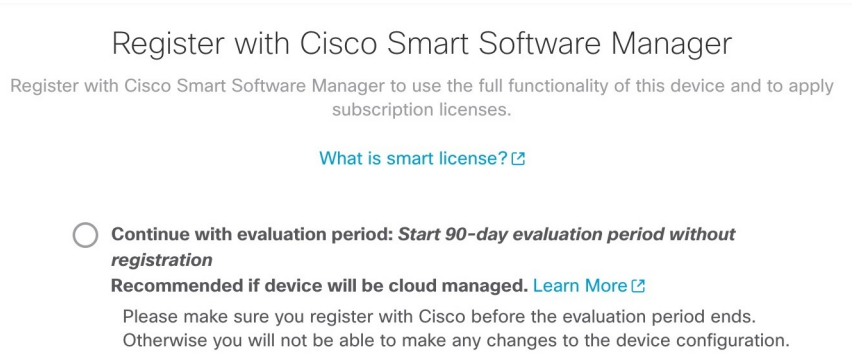
ファイアウォールのホスト名

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 *2*：時刻設定（*NTP*）



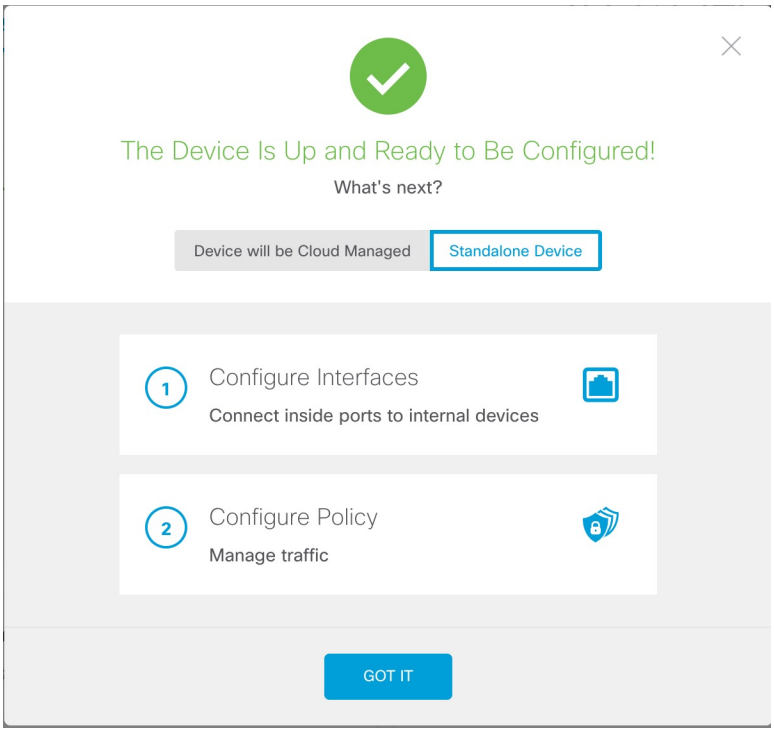
c) [登録せずに 90 日間の評価期間を開始（Start 90 day evaluation period without registration）] を選択します。



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 *3:* 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。

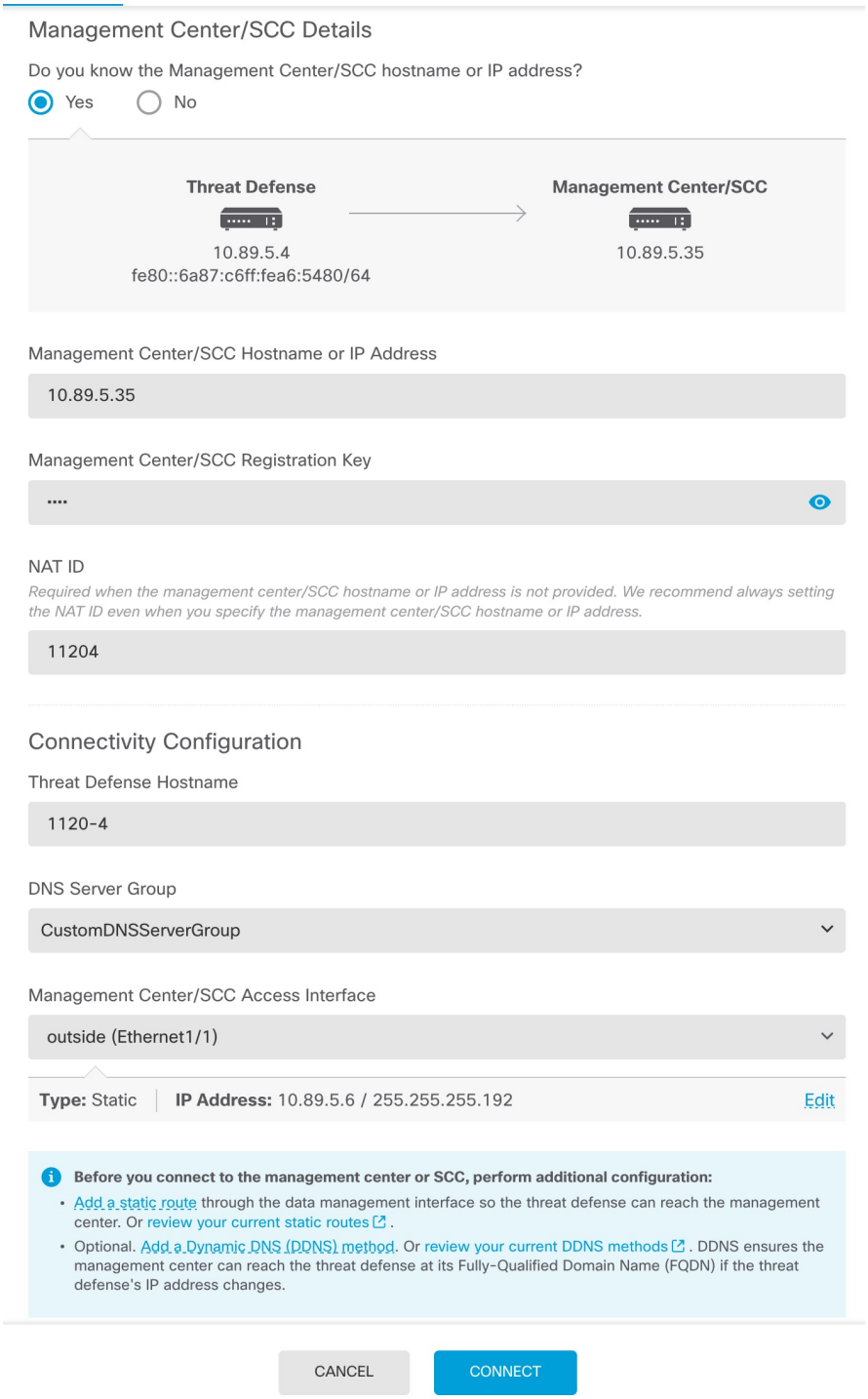
ステップ 4 追加のインターフェイスを設定する場合は、[デバイス（Device）] を選択し、[インターフェイス（Interface）] のサマリーにあるリンクをクリックします。

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 *4 : 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。

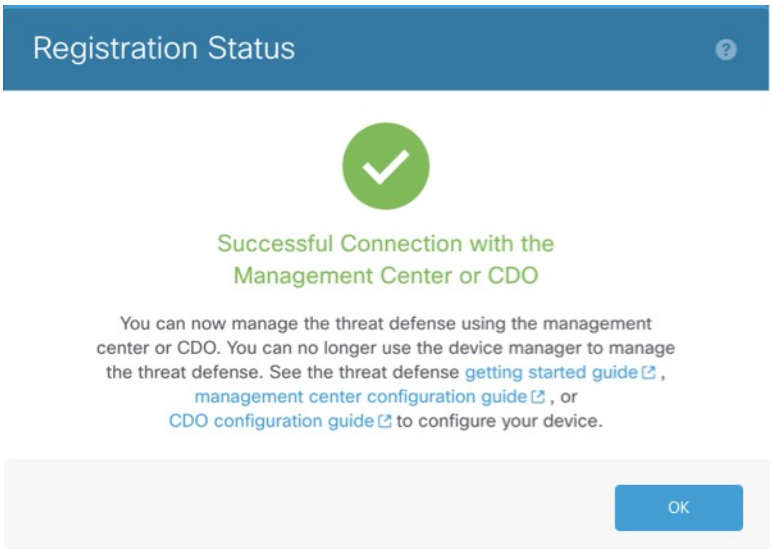
ステップ 7 （任意）[ダイナミックDNS（DDNS）方式の追加（Add a Dynamic DNS (DDNS) method）] をクリックします。

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 *5*：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 *1*：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 *2:* ゼロ タッチ プロビジョニング：管理対象（*M*）*LED* の動作

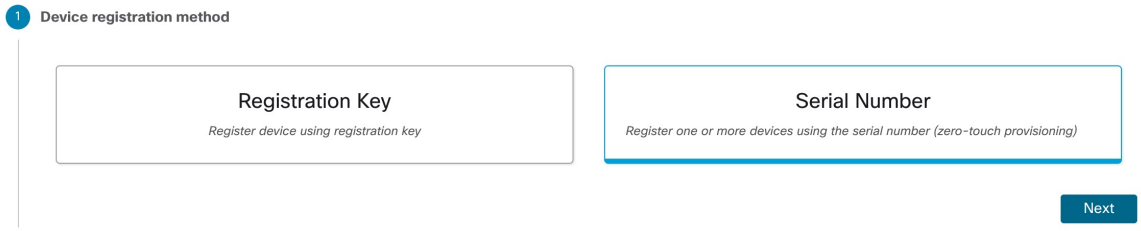
M LED	説明	ファイアウォールの電源を入れた後の時間（分:秒）
緑色で低速点滅	Cisco Cloud に接続され、オンボーディングの準備ができています	15:00 ～ 30:00
グリーンとオレンジに交互に点滅（エラー条件）	Cisco Cloud に接続できませんでした	15:00 ～ 30:00
緑色で点灯	オンボード済み	20:00 ～ 45:00

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。

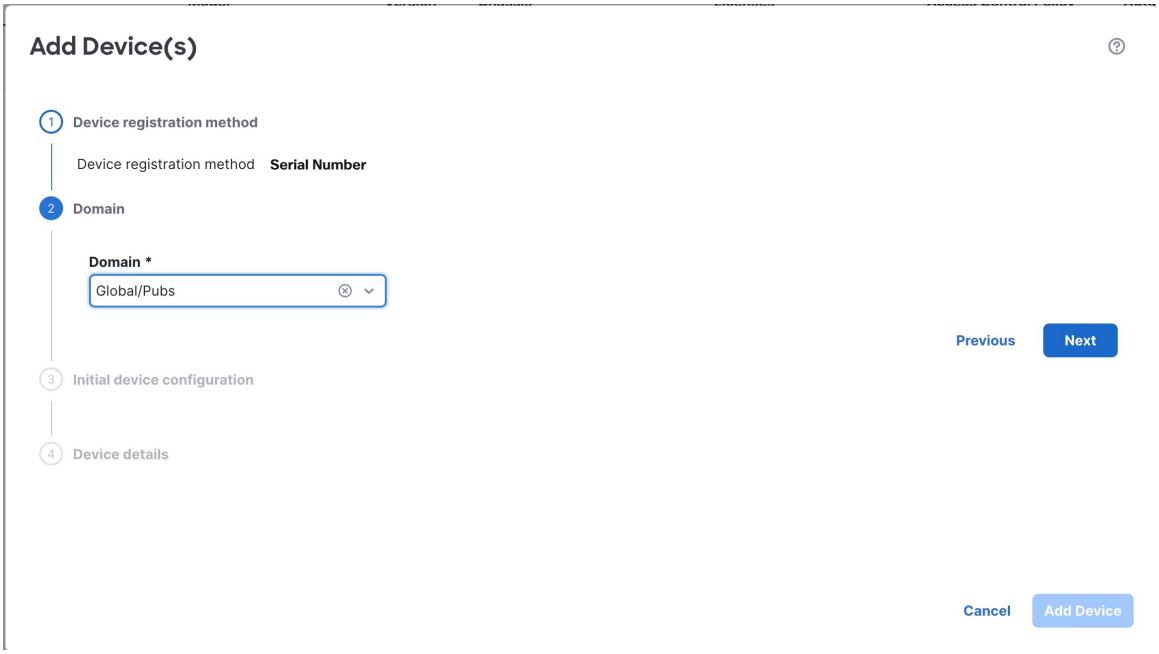
ステップ 6 [シリアル番号を使用（Use Serial Number）] をクリックし、[次へ（Next）] をクリックします。

図 *6*: デバイスの登録方法



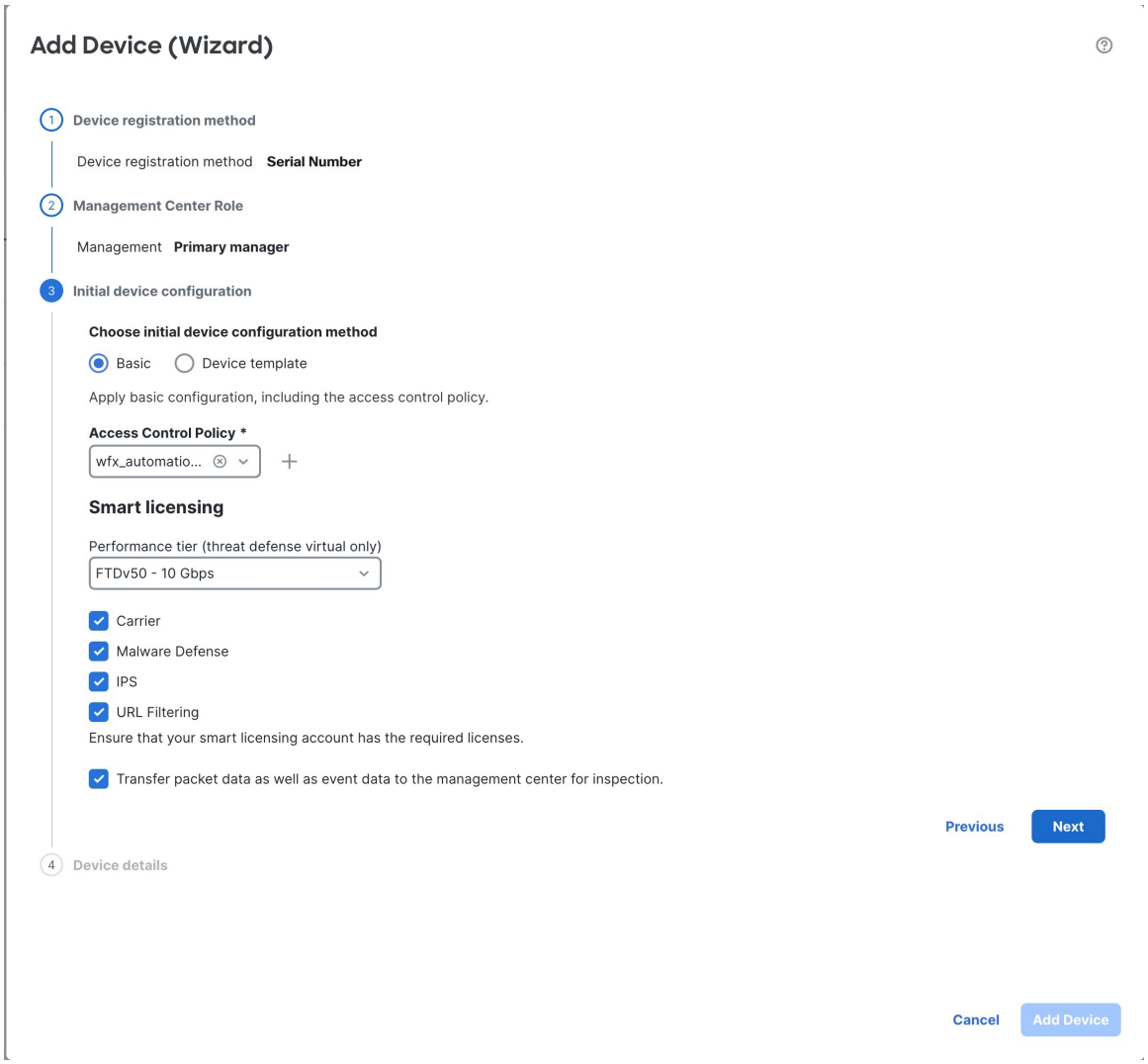
ステップ 7 マルチドメイン環境では、ドロップダウンリストから [ドメイン（Domain）] を選択し、[次へ（Next）] をクリックします。

図 *7*: 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 *8* : 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。

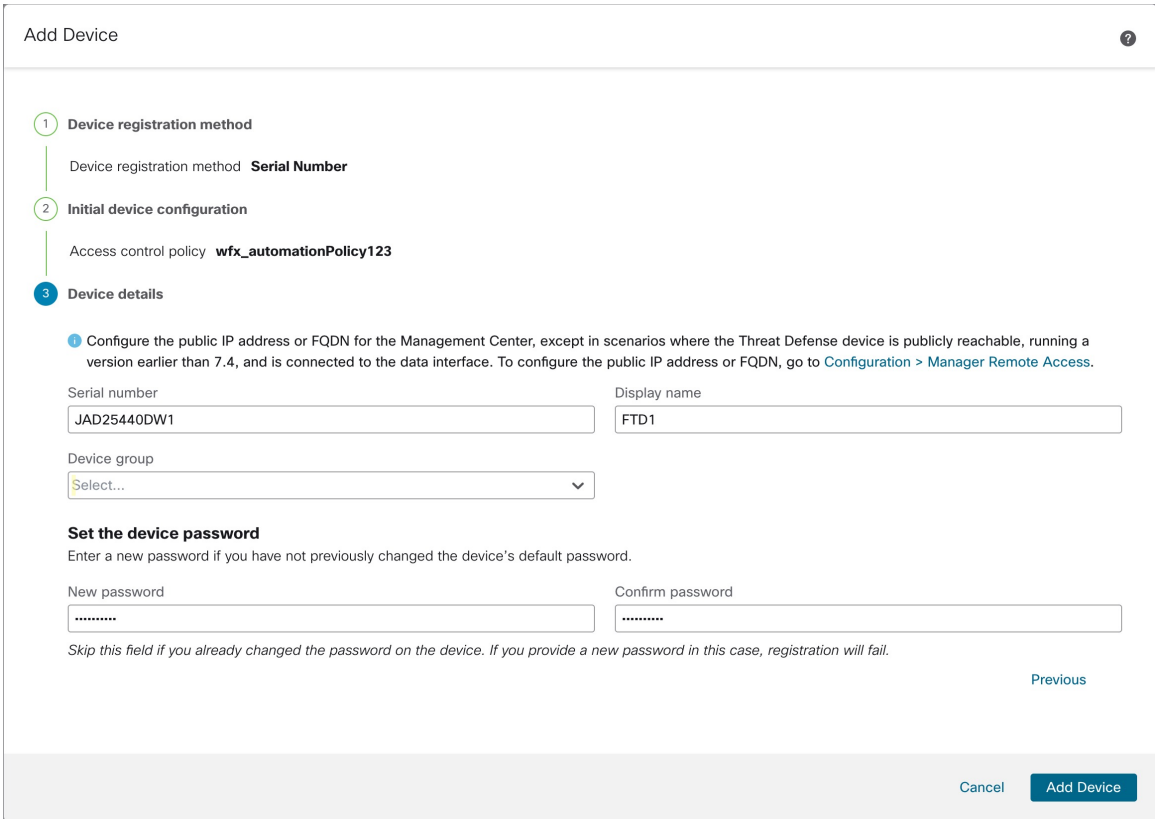
b) デバイスに適用する [スマートライセンス（Smart licensing）] ライセンスを選択します。

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 *9*: 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。

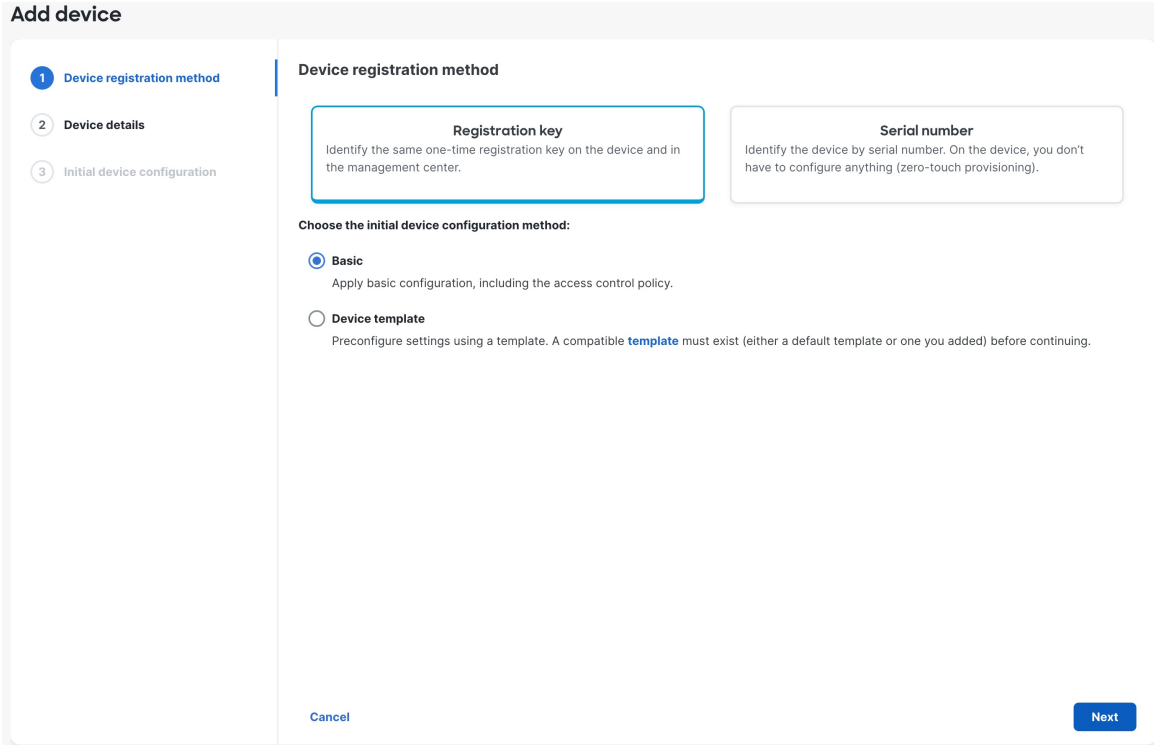
c) [ログイン（Log In）] をクリックします。

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。

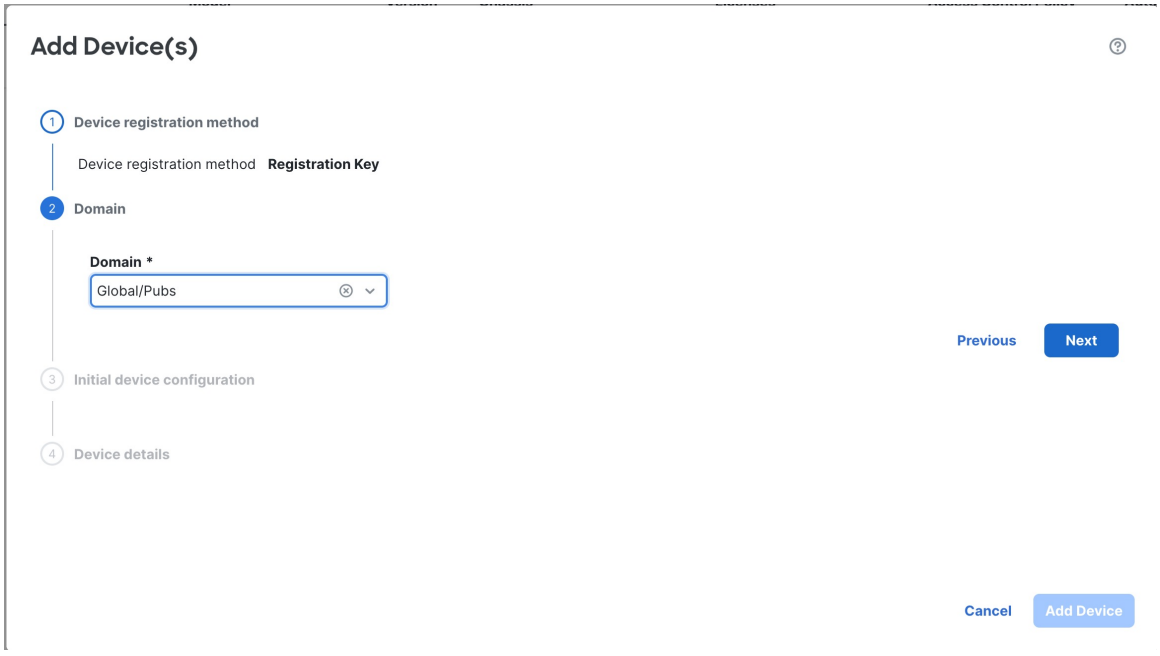
ステップ 4 [登録キー（Registration Key）] をクリックし、[次へ（Next）] をクリックします。

図 *10* : デバイスの登録方法



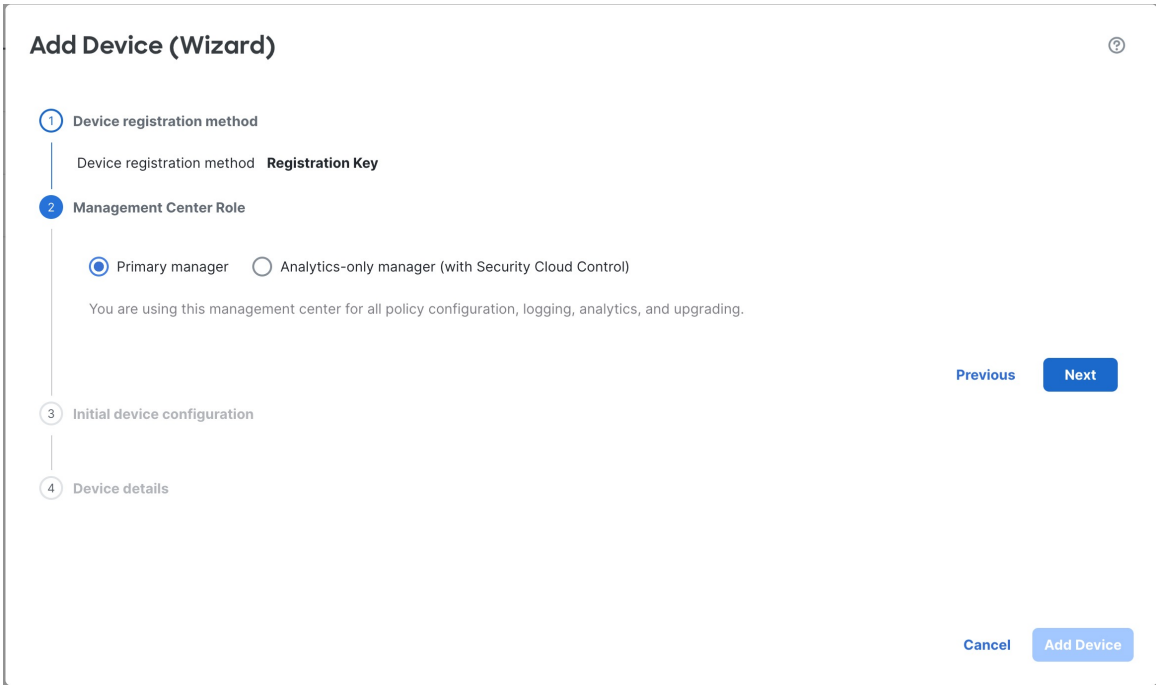
ステップ 5 マルチドメイン環境では、ドロップダウンリストから [ドメイン（Domain）] を選択し、[次へ（Next）] をクリックします。

図 *11* : ドメイン



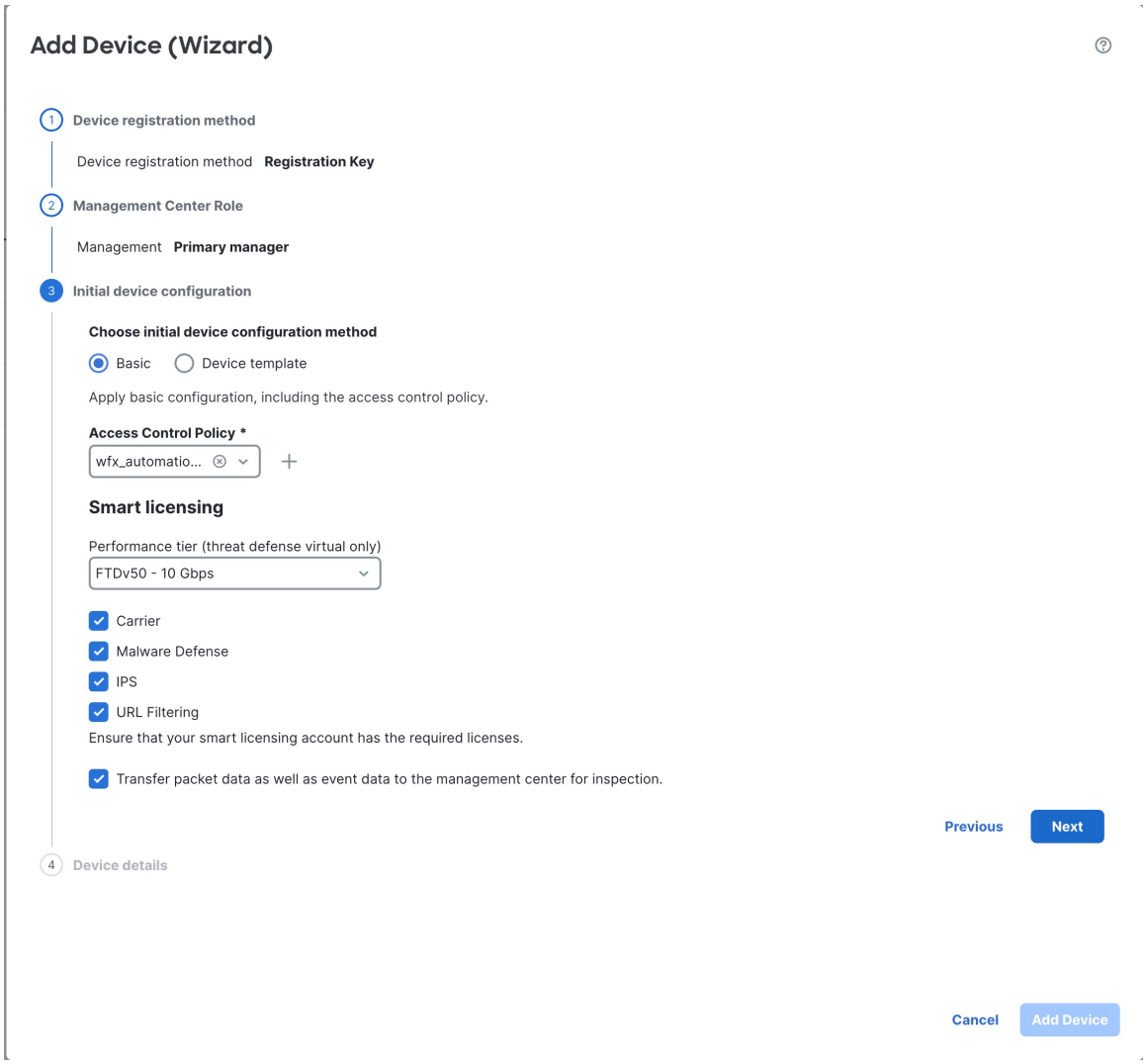
ステップ 6 通常の管理の場合は [プライマリマネージャ（Primary manager）] をクリックし、クラウド提供型 Firewall Management Center で管理されているデバイスの場合は [分析専用マネージャ（Analytics-only manager）] をクリックします。。

図 *12 : 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 *13* : 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」を参照してください。

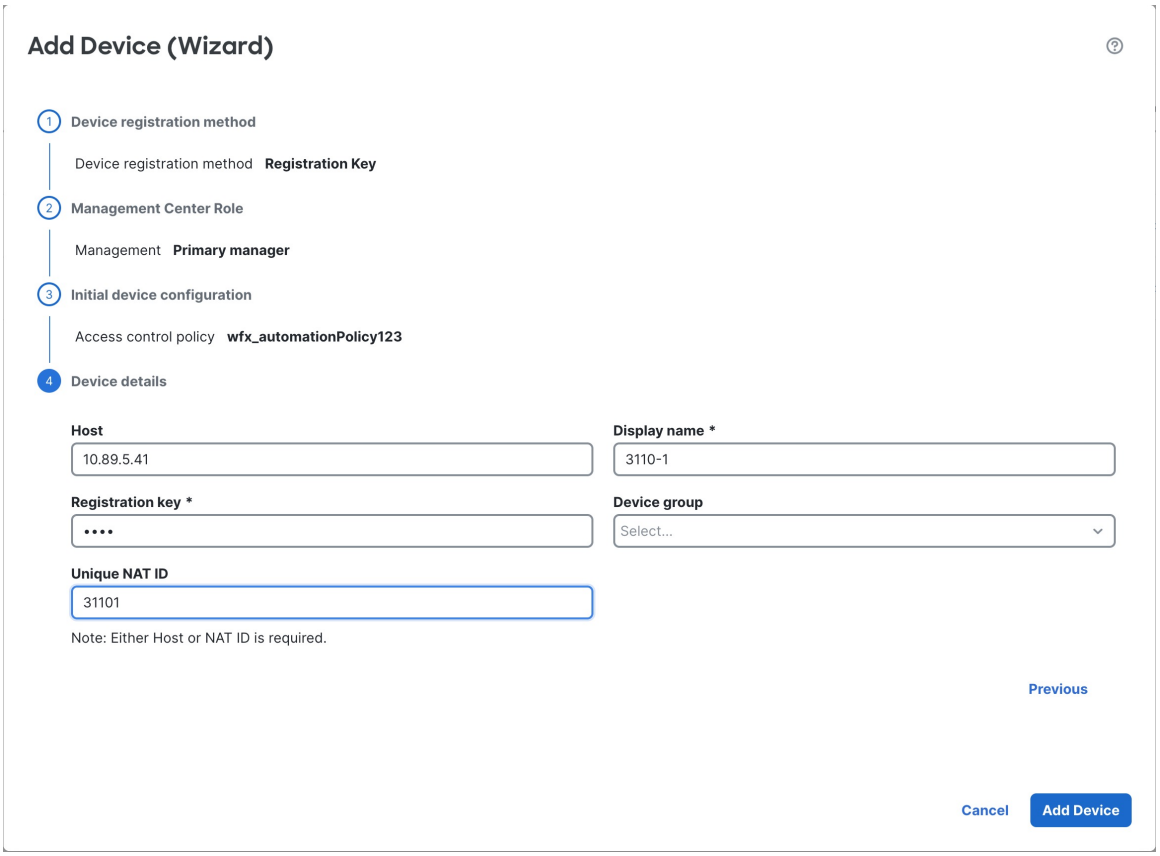
b) デバイスに適用する [スマートライセンス（Smart Licensing）] ライセンスを選択します。

[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 *14* : 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。

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。