Cisco Secure Firewall 1210/20 Threat Defense Firewall Management Center

Cisco Secure Firewall 1210CP
Updated NaN,

第

1

章

:

- □□□□□□□□□□□□□□□
- □□□□□□□□□□□□□□□□□□□□□□□□□□□□Firewall Threat Defense □□□ ASA□□□□
- Firewall Threat Defense CLI □□□□□□□
- □□□□□□□□□□□□□□□□
- □□□□□□□□□
- □□□□□□□□□□□□□□□□□□□□□□□□□□□□

ソフトウェアバージョンを確認し、必要に応じて再イメージ化し、ライセンスを取得して、接続できることを確認します。

Cisco Secure Firewall 1200 は、分散した企業を接続して保護します。シスコのエンタープライズセキュリティポリシーと脅威検出を、分散拠点や小規模サイトのユーザーおよびデバイスに拡大します。効率的なネットワークプロセッサを搭載した Cisco Secure Firewall 1200 は、ユーザー体験を損なうことなく、高度なセキュリティポリシーと脅威防御を提供します。

分散拠点にファイアウォールをインストールし、Security Cloud Control（旧称、Cisco Defense Orchestrator）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。
>
> このガイドでは、特に外部管理について説明しますが、管理インターフェイスを使用した管理については、*Cisco Security Cloud Control : Cloud-Delivered Firewall Management Center for Firewall Threat Defense* を参照してください。

Cisco Secure Firewall 1210/20 の電源をオンにして、前面パネルの LED で電源およびシステムのステータスを確認することで、正常に起動していることを確認する方法。

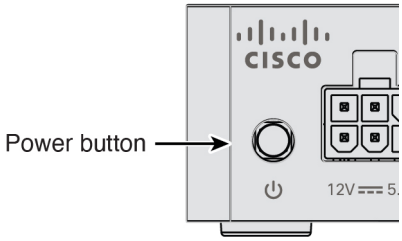
ファイアウォールに対して信頼性の高い電力を供給することが重要です（無停電電源装置（UPS）を使用するなど）。最初のシャットダウンを行わないで電力が失われると、重大なファイルシステムの損傷を引き起こす可能性があります。バックグラウンドでは常に多数のプロセスが実行されていて、電力が失われると、システムをグレースフルシャットダウンできません。

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。

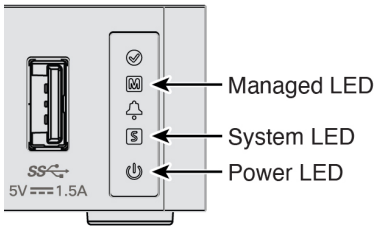
1. 電源コードをファイアウォールに接続し、電源コンセントに接続します。
2. シャーシの背面で、電源コードに隣接する電源ボタンを使用して電源をオンにします。

   1 :



3. LED の現在のステータスを確認します。

   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。

1： S LED

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（14ページ）」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のクラウド接続ステータスを確認します。

2： M LED

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
緑色とオレンジ色で交互に点滅（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

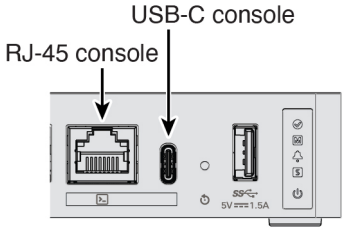
Firewall Threat Defense ASA

コンソールポートに接続し、CLIプロンプトを確認することで、Cisco Secure Firewall 1210/20 が Firewall Threat Defense または ASA を実行しているかどうかを確認する方法について説明します。

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。

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。

3：



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（6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>
   ```

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。

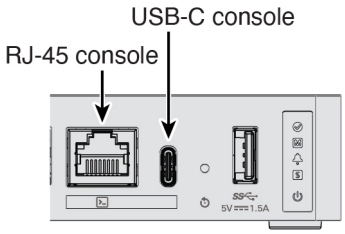
Firewall Threat Defense CLI

必要に応じて FXOS にログインし、FTD CLI に切り替えるなどの、セットアップやトラブルシューティングを行うために、Cisco Secure Firewall 1210/20 上の Firewall Threat Defense CLI にアクセスする方法。

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。

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。

   4 :



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#
```

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 の 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。

```
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。

```
> exit
firepower#
```

設定を開始する前に、現在の Firewall Threat Defense ソフトウェアバージョンを確認する方法、および Cisco Secure Firewall 1210/20 をターゲットリリースに再イメージ化するかどうかを決定する方法について説明します。

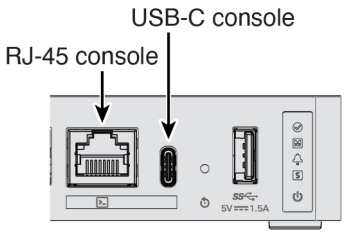
ファイアウォールを設定する前に対象バージョンをインストールすることをお勧めします。別の方法として、稼働後にアップグレードを実行することもできますが、設定を保持するアップグレードでは、この手順を使用するよりも時間がかかる場合があります。

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。

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。

   5 :



2. FXOS CLI で、実行中のバージョンを表示します。

   scope ssa

   show app-instance

```
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
```

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 については、デバイスをオンボーディングする際、すでにパスワードを設定しているため、[パスワードのリセット（Password Reset）] 欄で必ず [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（10ページ） を参照してください。

Cisco Smart Software Manager および Cisco Commerce Workspace で Cisco Secure Firewall 1210/20 ライセンスを取得する方法について説明します。これには、必要なライセンスタイプ、追加の権限を注文するために使用するライセンス PID の特定も含まれます。

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。

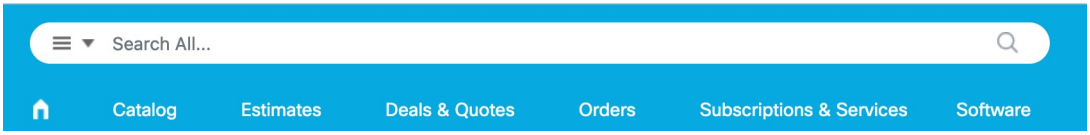
まだの場合は、Smart Software Manager に Security Cloud Control を登録します。登録を行うには、Smart Software Manager で登録トークンを生成する必要があります。詳しい手順については、Security Cloud Control のマニュアルを参照してください。

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。

   6 :



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。

   - Essentials：
     - 自動的に含める
   - IPS、マルウェア防御、および URL の組み合わせ：
     - L-CSF1210CET-TMC=
     - L-CSF1210CPT-TMC=
     - L-CSF1220CXT-TMC=

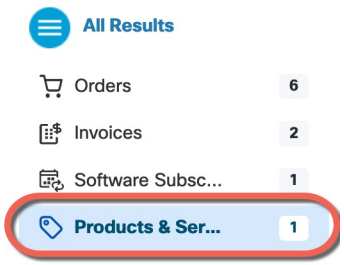
     上記の PID のいずれかを注文に追加すると、次のいずれかの PID に対応する期間ベースのサブスクリプションを選択できます。
     - L-CSF1210CE-TMC-1Y
     - L-CSF1210CE-TMC-3Y
     - L-CSF1210CE-TMC-5Y
     - L-CSF1210CP-TMC-1Y
     - L-CSF1210CP-TMC-3Y
     - L-CSF1210CP-TMC-5Y
     - L-CSF1220CX-TMC-1Y

- L-CSF1220CX-TMC-3Y
- L-CSF1220CX-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。

7 :



FXOS CLI のシャットダウンコマンドまたはクラウド提供型 Firewall Management Center のシャットダウンワークフローを使用して、ファイルシステムの損傷を回避するために Cisco Secure Firewall 1210/20 の電源を安全にオフにする方法。

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。

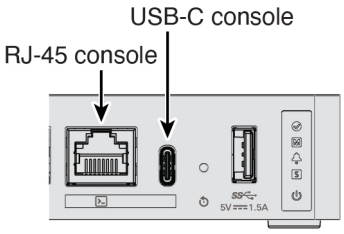
CLI

FXOS CLI を使って Cisco Secure Firewall 1210/20 をシャットダウンし、電源を取り外したり、デバイスを移動したりする前に、システムをクリーンに停止できるようにする方法について説明します。

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。

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。

8 :



2. FXOS CLI でローカル管理モードに接続します。

   firepower # connect local-mgmt

3. システムをシャットダウンします。

firepower(local-mgmt) # **shutdown**

```
firepower(local-mgmt)# shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
```

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]
```

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。

Firewall Management Center

リモートで管理している場合でもデバイスの電源を安全にオフにできるように、Cisco Secure Firewall 1210/20 を クラウド提供型 Firewall Management Center からシャットダウンする方法。

クラウド提供型 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。

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。
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。
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

:

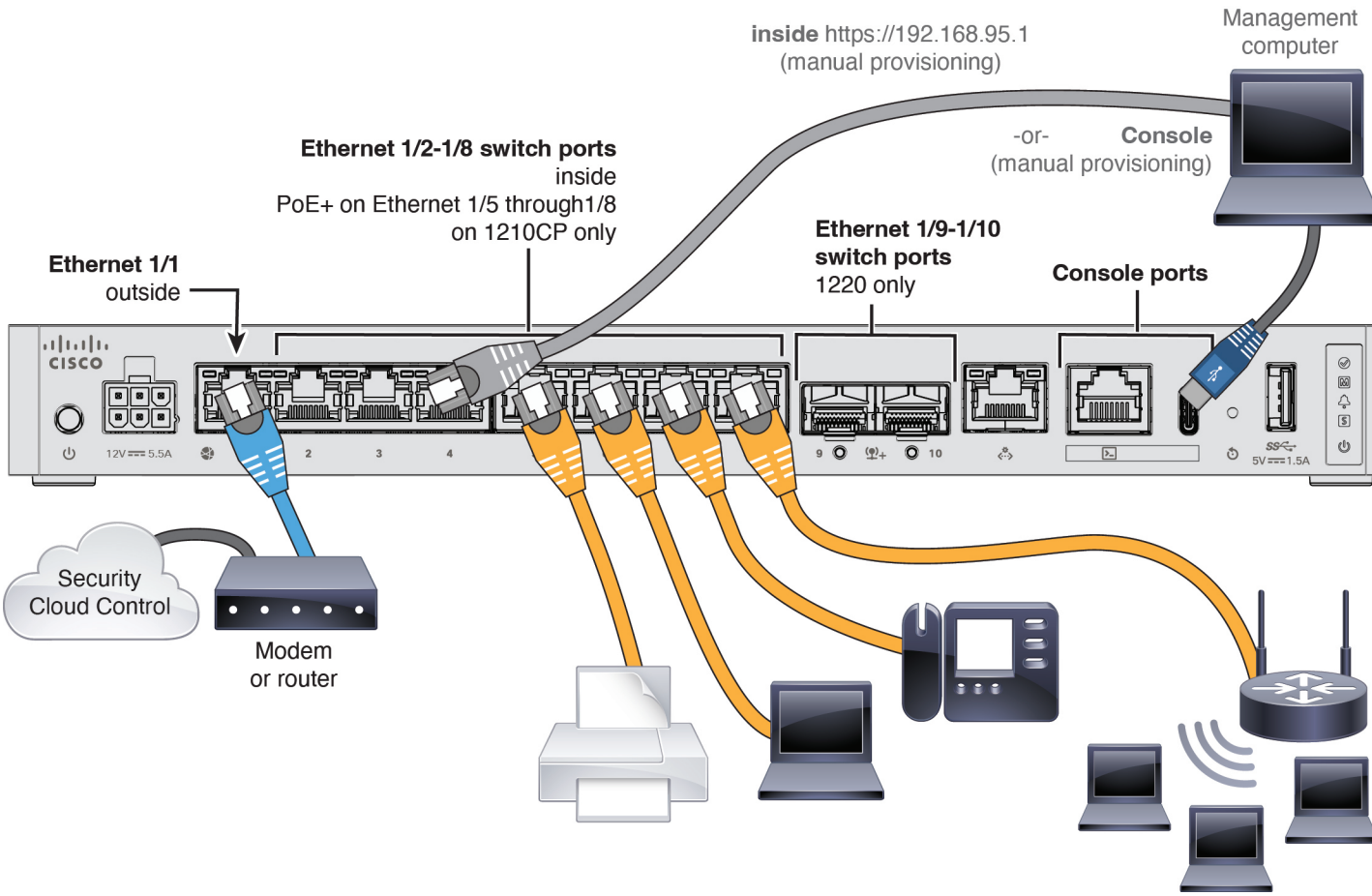
- □□□□□□□□□□□□□□□□
- Security Cloud Control □□□□□□ □□□□□□□□□□□□□□□
- □□□□□□□□□□□□□□□□□□□□□□ □□

Cisco Secure Firewall 1210/20 をネットワークに接続し、マネージャに登録します。

ファイアウォールをケーブル接続し、Security Cloud Control にオンボードします。

初期ハードウェアセットアップを完了し、設定前にネットワーク接続に必要なポートを準備できるように、Cisco Secure Firewall 1210/20 のケーブル接続方法について説明します。

- Cisco Secure Firewall 1220 の場合、SFP をイーサネット 1/9 および 1/10 に取り付けます。これらは SFP/SFP+ モジュールを必要とする 1/10 Gb SFP+ ポートです。
- 詳細については、ハードウェア設置ガイドを参照してください。
- ゼロタッチプロビジョニングを使用する場合は、外部インターフェイスと管理インターフェイスの両方をケーブル接続しないでください。このガイドは外部インターフェイスでの管理について説明していますが、高可用性を備えた管理でゼロタッチプロビジョニングを使用することもできます。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。



Security Cloud Control

クラウド提供型 Firewall Management Center を使用して管理できるように、Cisco Secure Firewall 1210/20 を Security Cloud Control にオンボードする方法。

ゼロタッチプロビジョニング または手動プロビジョニングを使用してファイアウォールをオンボードします。https://security.cisco.com で Security Cloud Control にログインします。

高速リモート展開を実現できるように、ゼロタッチプロビジョニング とデバイスのシリアル番号を使用して Cisco Secure Firewall 1210/20 を Security Cloud Control にオンボードする方法について説明します。

- 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、ラベルにシャーシのシリアル番号が表示されています。
  - シャーシのシリアル番号は、デバイスの背面の適合性ラベルに記載されています。
  - PCB のシリアル番号は、「S/N」というシャーシのラベルに記載されています。
  - シリアル番号は次の CLI コマンドを使用して表示できます。
    - FXOS：**show chassis detail** は両方のシリアル番号を示します。
    - Firewall Threat Defense：**show inventory** はシャーシのシリアル番号を示します。**show serial-number** は PCB のシリアル番号を示します。

- LED をチェックして、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。

  3 : M LED

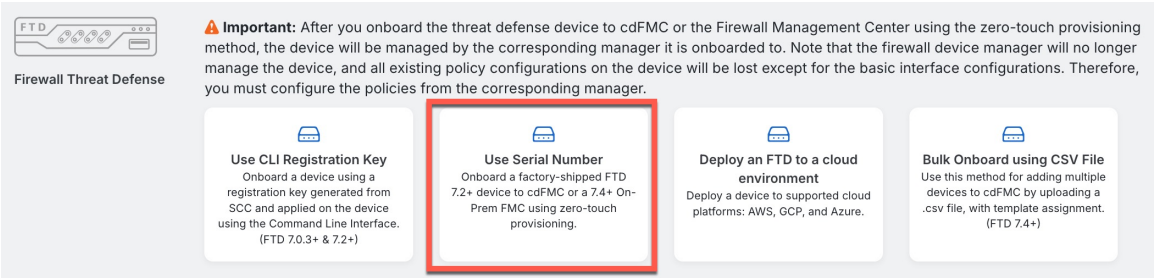
M LED	説明	ファイアウォールの電源を入れた後の時間（分:秒）
緑色で低速点滅	Cisco Cloud に接続され、オンボーディングの準備ができています	15:00 ～ 30:00
緑色とオレンジ色で交互に点滅（エラー条件）	Cisco Cloud に接続できませんでした	15:00 ～ 30:00
緑色で点灯	オンボード済み	20:00 ～ 45:00

ゼロタッチプロビジョニング とデバイスのシリアル番号を使用して Firewall Threat Defense を導入準備します。

1. Security Cloud Control のナビゲーションメニューで **[セキュリティデバイス]** をクリックし、青色のプラスボタン（  ）をクリックしてデバイスの **[Onboard]** をします。
2. [FTD] タイルを選択します。
3. [管理モード] で、[FTD] が選択されていることを確認します。

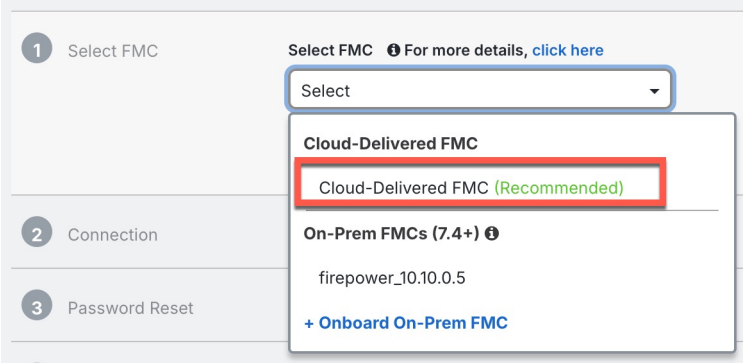
   管理モードとして [FTD] を選択した後はいつでも、[スマートライセンスの管理] をクリックして、デバイスで使用可能な既存のスマートライセンスに登録または変更できます。使用可能なライセンスについては、ライセンスの取得（8ページ） を参照してください。
4. オンボーディング方法として [シリアル番号を使用（Use Serial Number）] を選択します。

   9 :



5. **[Select FMC]** で、リストから **[Cloud-Delivered FMC > Cloud-Delivered FMC]** の順に選択し、**[Next]** をクリックします。

10 : FMC



6. [接続（Connection）]エリアで、[デバイスのシリアル番号（Device Serial Number）]と[デバイス名（Device Serial Number）]を入力し、[次へ（Next）]をクリックします。

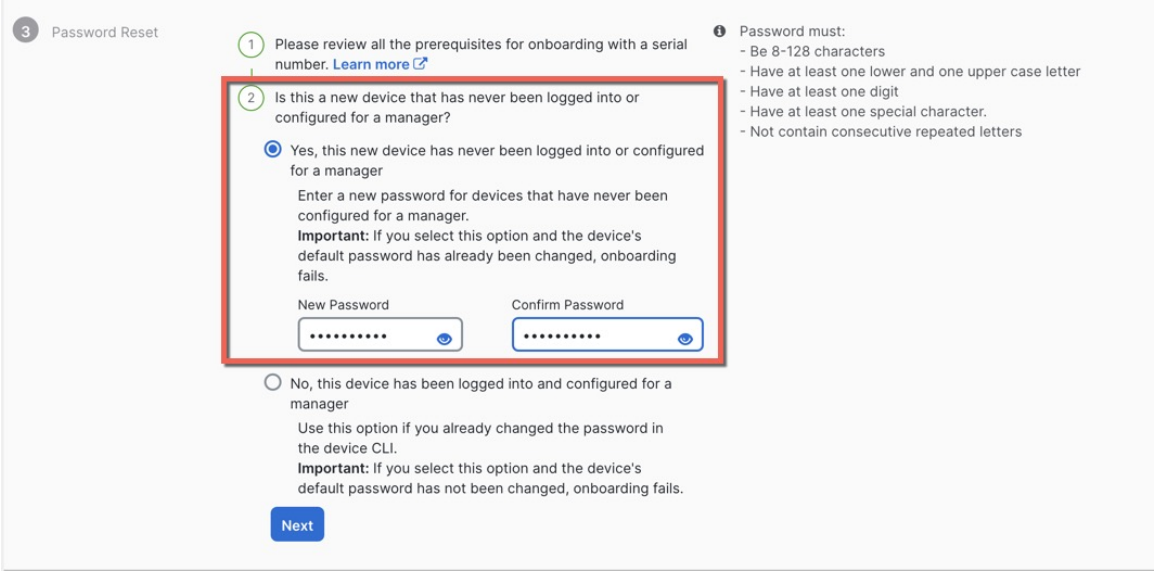
11 :

7. **[パスワードのリセット（Password Reset）]**で、**[はい...（Yes...）]**をクリックします。デバイスの新しいパスワードを入力し、この新しいパスワードを確認して、[次へ（Next）]をクリックします。

ゼロタッチプロビジョニングの場合、デバイスは新規であるか、再イメージ化されている必要があります。

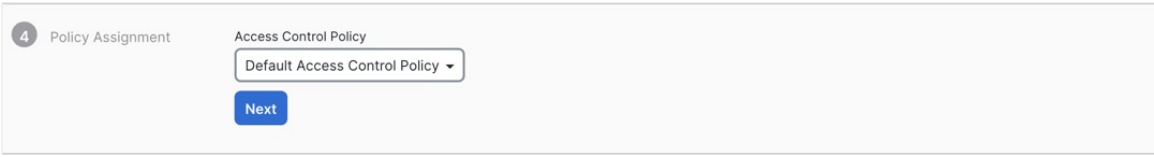
> **注**
>
> デバイスにログインしてパスワードをリセットし、ゼロタッチプロビジョニングを無効にするように設定を変更しなかった場合は、[いいえ...（No...）]オプションを選択する必要があります。ゼロタッチプロビジョニングプロビジョニングを無効にする設定は多数あるため、再イメージ化などの必要がある場合を除き、デバイスにログインすることは推奨されません。

12 :



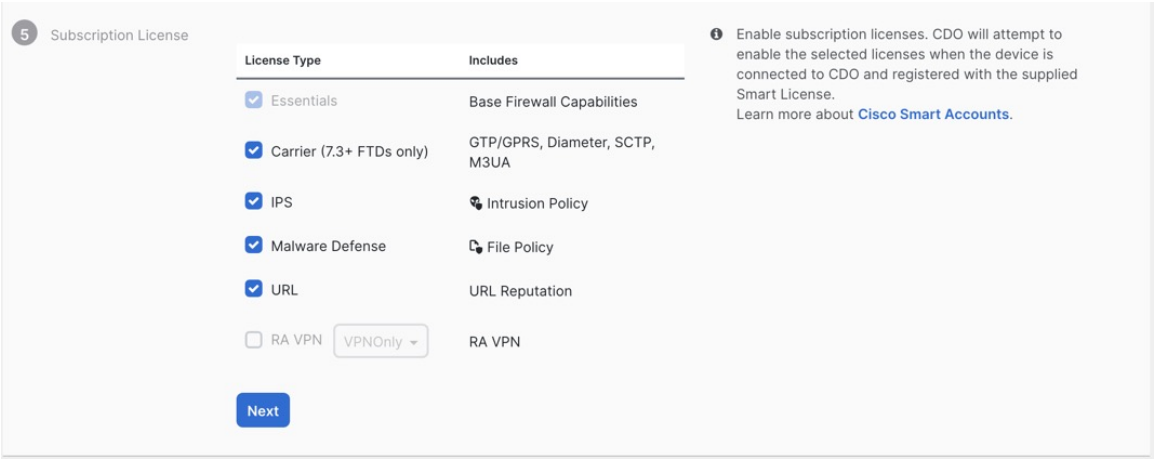
8. [ポリシー割り当て（Policy Assignment）]については、ドロップダウンメニューを使用して、デバイスのアクセス コントロール ポリシーを選択します。ポリシーが設定されていない場合は、[デフォルトのアクセスコントロールポリシー（Default Access Control Policy）] を選択します。

13 :



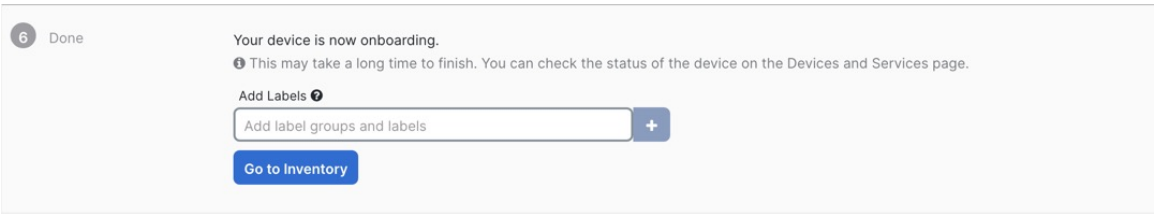
9. [サブスクリプションライセンス（Subscription License）] については、有効にする各機能ライセンスをチェックします。[Next] をクリックします。

14 :



10. オプション: [セキュリティデバイス（Security Devices）] ページの並べ替えとフィルタ処理に役立つラベルをデバイスに追加します。ラベルを入力し、青いプラスボタン（+）を選択します。ラベルは、Security Cloud Control への導入準備後にデバイスに適用されます。

15 :



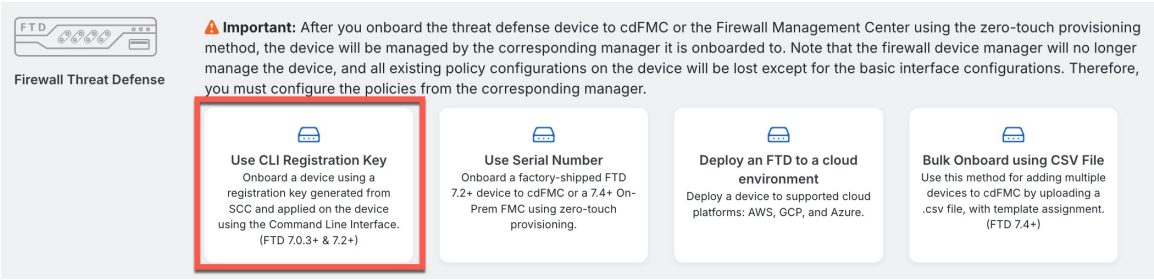
[セキュリティデバイス（Security Devices）] ページから、導入準備したばかりのデバイスを選択し、右側にある [管理（Management）] ペインに一覧表示されているオプションのいずれかを選択します。

CLI 登録キーを使用して Cisco Secure Firewall 1210/20 を Security Cloud Control にオンボードする方法について説明します。

CLI 登録キーを使用してファイアウォールをオンボードします。

1. Security Cloud Control のナビゲーションメニューで **[セキュリティデバイス]** をクリックし、青色のプラスボタン（  ）をクリックしてデバイスの **[Onboard]** をします。
2. [FTD] タイルをクリックします。
3. [管理モード] で、[FTD] が選択されていることを確認します。
4. オンボーディング方法として [CLI登録キーを使用（Use CLI Registration Key）] を選択します。

16 : CLI

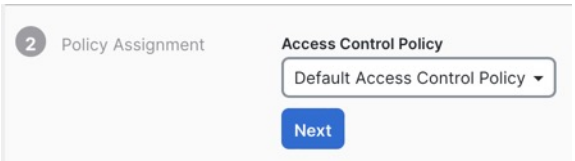


5. [デバイス名（Device Name）] を入力して、[次へ（Next）] をクリックします。

17 :

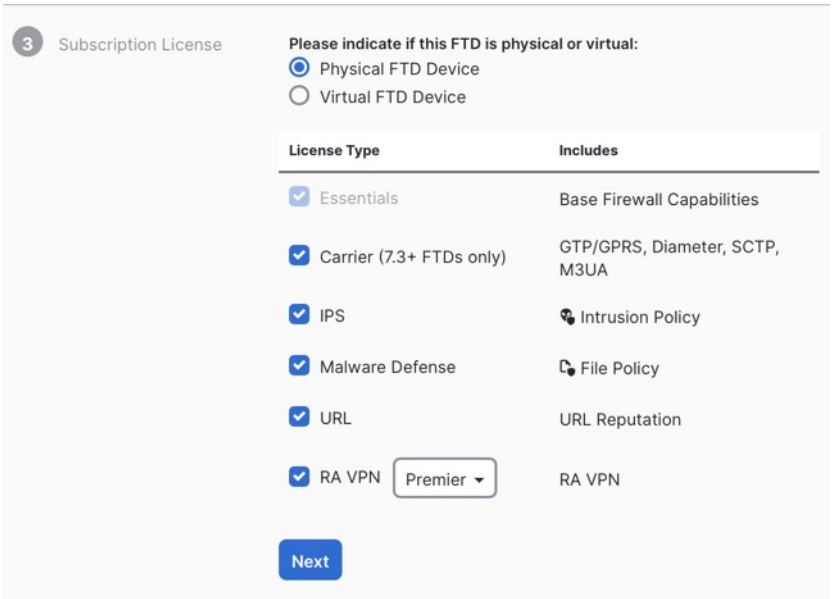
6. [ポリシー割り当て（Policy Assignment）] については、ドロップダウンメニューを使用して、デバイスのアクセス コントロール ポリシーを選択します。ポリシーが設定されていない場合は、[デフォルトのアクセスコントロールポリシー（Default Access Control Policy）] を選択します。

18 :



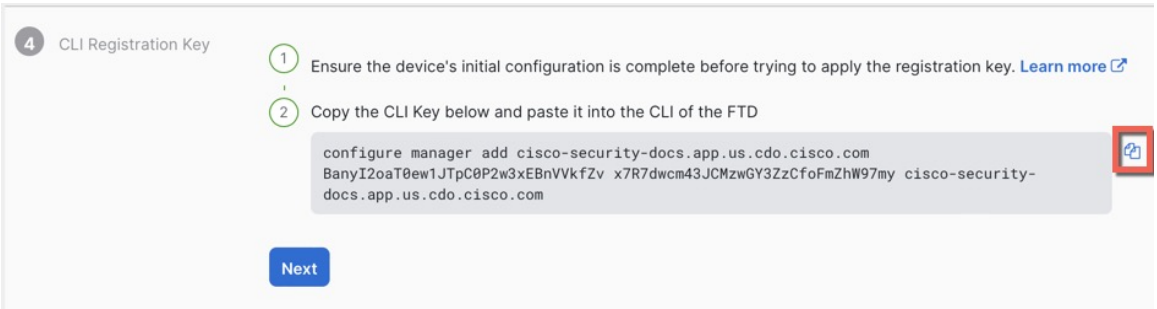
7. [サブスクリプションライセンス（Subscription License）] については、[物理 FTD デバイス（Physical FTD Device）] ラジオ ボタンをクリックし、有効にする各機能ライセンスをチェックします。[Next] をクリックします。

19 :



8. [CLI登録キー（CLI Registration Key）] については、Security Cloud Control は、登録キーとその他のパラメータを使用してコマンドを生成します。このコマンドをコピーして、Firewall Threat Defense の初期設定で使用する必要があります。

20 : CLI



configure manager add Security Cloud Control_*hostname registration_key nat_id display_name*

CLI での、または Firewall Device Manager を使用した初期設定の完了

- 初期設定：CLI（27ページ）：スタートアップスクリプトを完了した後、Firewall Threat Defense CLI でこのコマンドをコピーします。
- 初期設定：Firewall Device Manager（20ページ）：コマンドの *scc_hostname*、*registration_key*、および *nat_id* の部分を、[Management Center/Security Cloud Controlのホスト名/IPアドレス（Management Center/Security Cloud Control Hostname/IP Address）]、[Management Center/Security Cloud Controlの登録キー（Management Center/Security Cloud Control Registration Key）]、および[NAT ID] フィールドにコピーします。

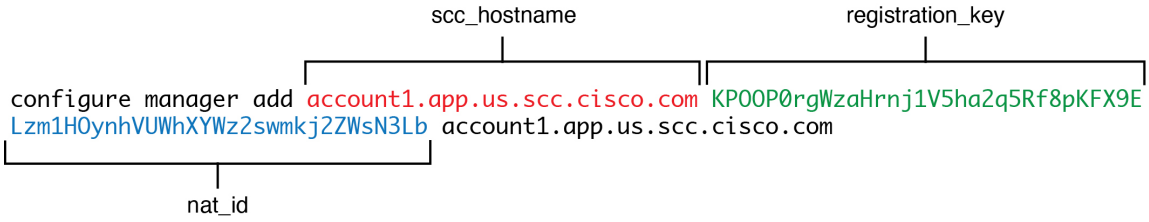
CLI セットアップのサンプルコマンド:

```
configure manager add account1.app.us.scc.cisco.com
```

```
KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.scc.cisco.com
```

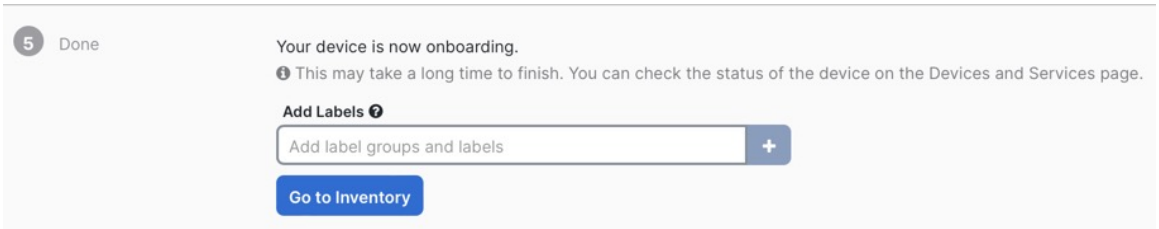
GUI セットアップのサンプル コマンド コンポーネント：

21 : configure manager add



9. オンボーディングウィザードで [次へ（Next）] をクリックして、デバイスの登録を開始します。
10. オプション: [セキュリティデバイス（Security Devices）] ページの並べ替えとフィルタ処理に役立つラベルをデバイスに追加します。ラベルを入力し、青いプラスボタン（+）を選択します。ラベルは、Security Cloud Control への導入準備後にデバイスに適用されます。

22 :



デバイスに基本ネットワーク設定を行い、Security Cloud Control に登録できるように、手動プロビジョニング向けの Cisco Secure Firewall 1210/20 初期セットアップを完了する方法。

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。

Firewall Device Manager

Firewall Device Manager を使用して Cisco Secure Firewall 1210/20 で初期セットアップウィザードを実行し、Security Cloud Control にデバイスを登録する前に外部接続および管理接続を準備する方法について説明します。

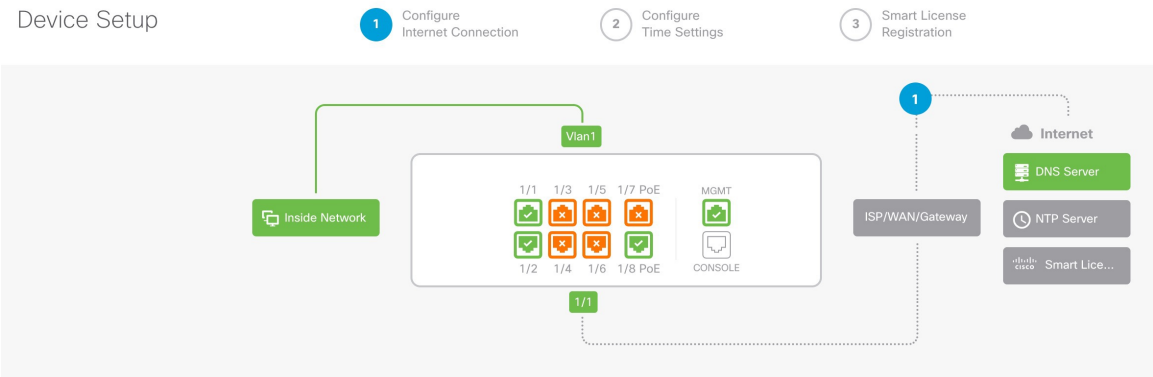
この方法を使用すると、ファイアウォールを登録した後、管理インターフェイスに加えて次のインターフェイスが事前設定されます。

- イーサネット 1/1：「外部」、DHCP からの IP アドレス、IPv6 自動設定
- VLAN1：「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。

1. コンピュータを内部インターフェイス（Ethernet 1/2 ～ 1/8 または Cisco Secure Firewall 1220 の場合は 1/2 ～ 1/10）に接続します。
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。
3. セットアップウィザードを使用します。

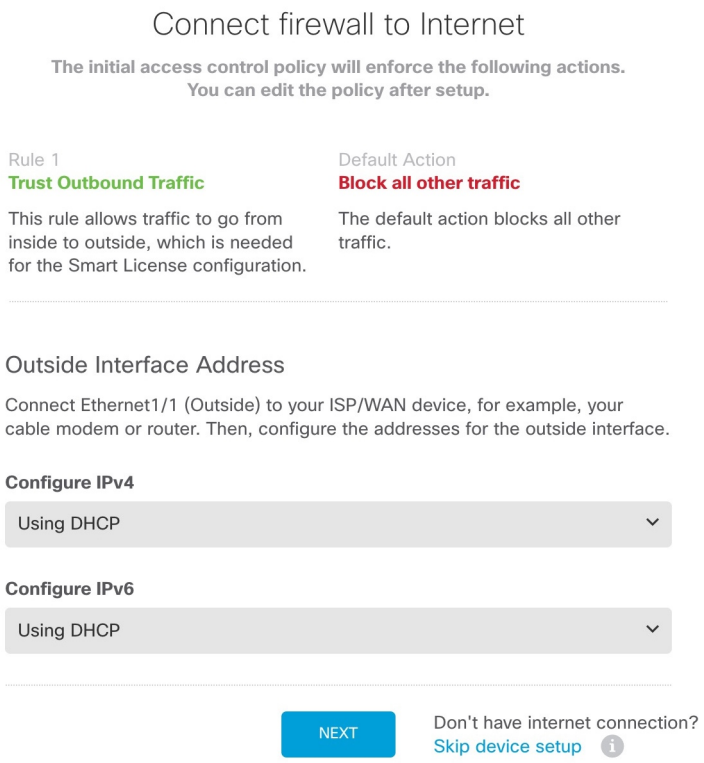
   23 : [Device Setup]



> **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。

      24 :



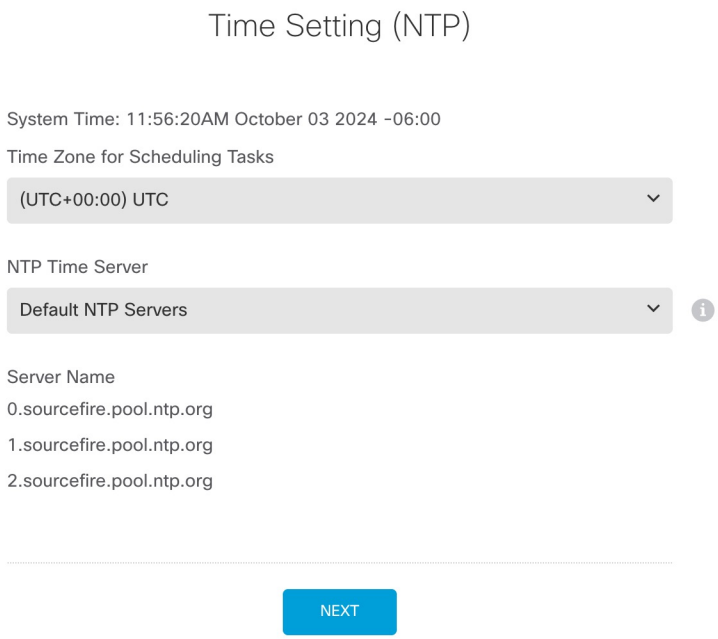
1. [外部インターフェイスアドレス（Outside Interface Address）]：高可用性の実装を予定している場合は、静的 IP アドレスを使用します。セットアップウィザードを使用して PPPoE を設定することはできません。ウィザードの完了後に PPPoE を設定できます。
2. [管理インターフェイス（Management Interface）]：外部インターフェイスでマネージャアクセスを使用している場合でも、管理インターフェイスの設定が使用されます。たとえば、外部インターフェイスを介してバックプレーン経由で回送される管理トラフィックは、外部インターフェイスの DNS サーバーではなく、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。

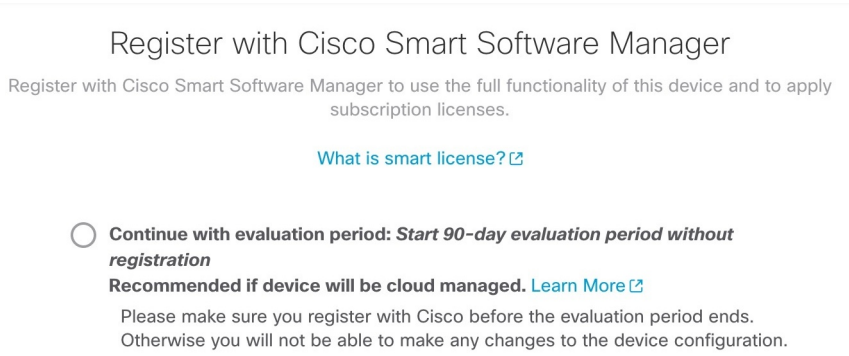
   ファイアウォールのホスト名

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

25： NTP



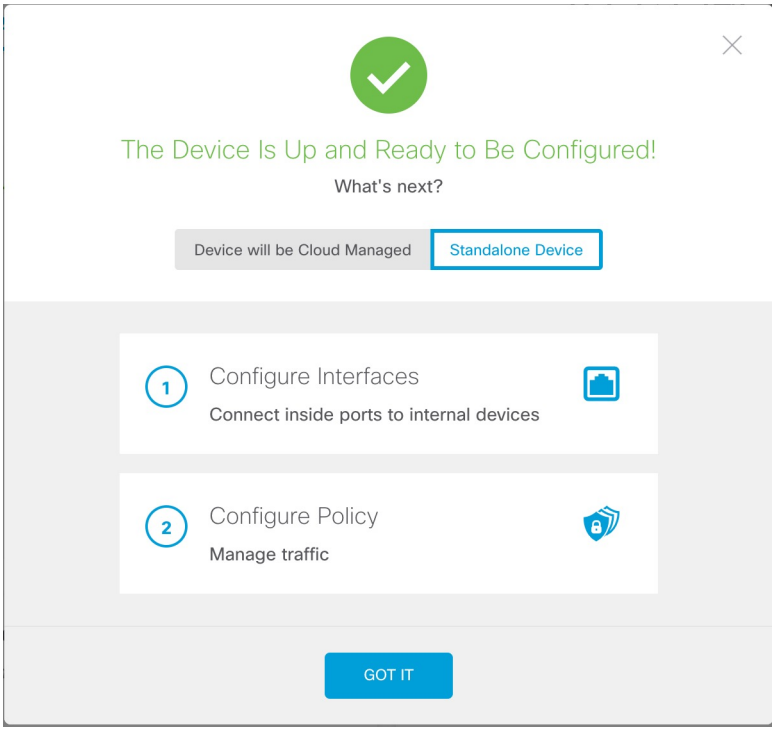
c) [登録せずに 90 日間の評価期間を開始（Start 90 day evaluation period without registration）] を選択します。



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 Security Cloud Control で実行されます。

d) [終了（Finish）] をクリックします。

26 :



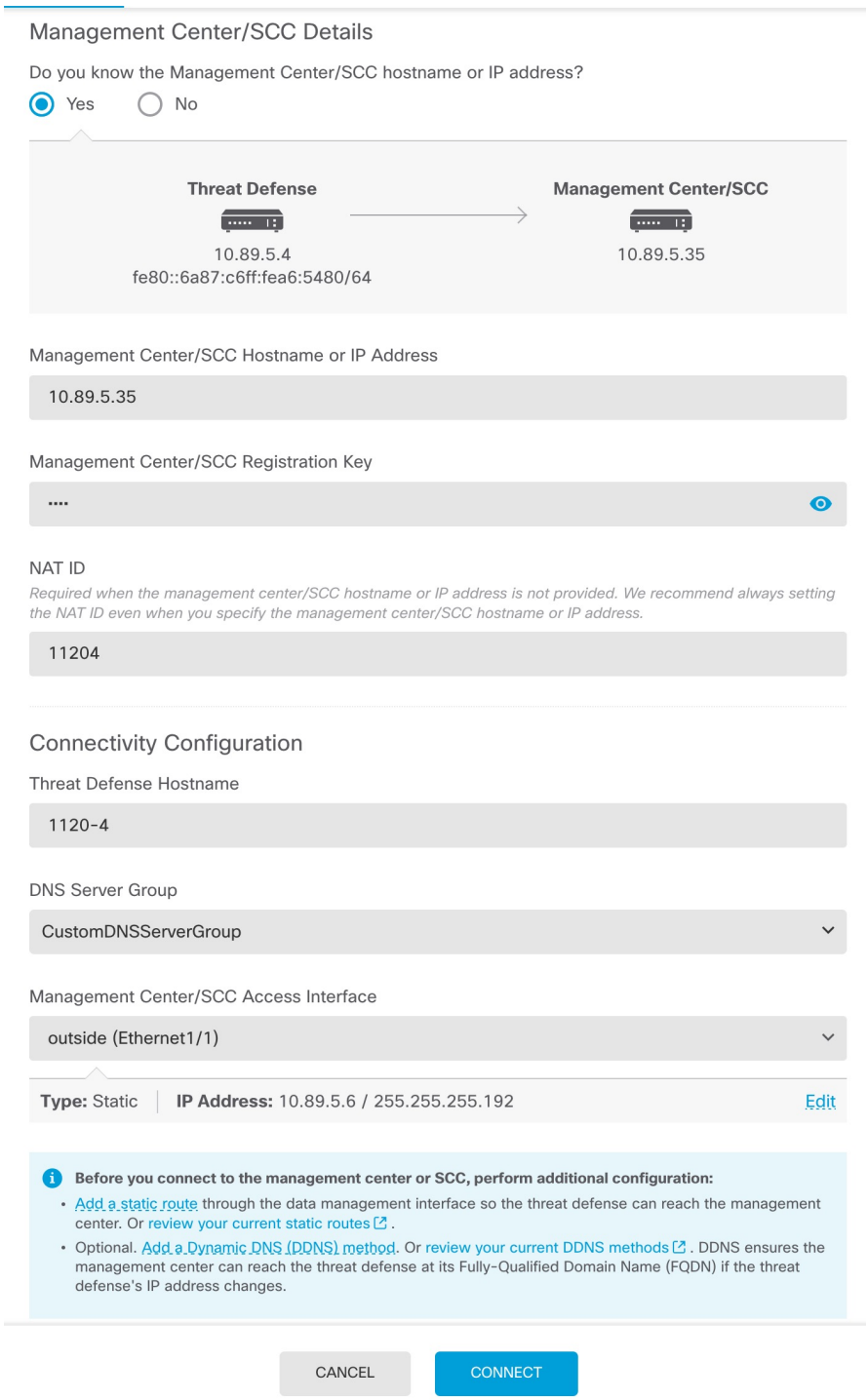
e) [スタンドアロンデバイス（Standalone Device）] を選択し、[了解（Got It）] を選択します。

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。
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 Security 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。

27 : Management Center/SCC

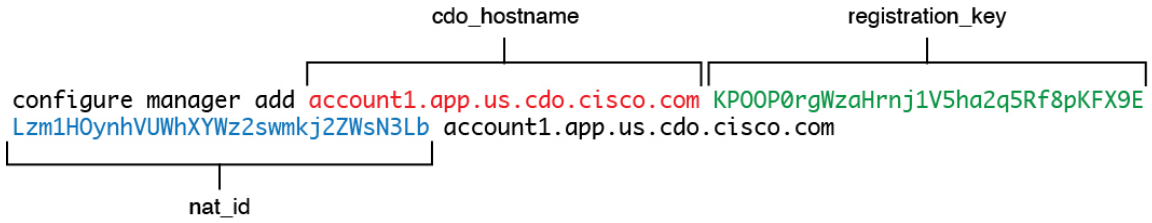


a) **[Do you know the Management Center/SCC Hostname or IP address]** に対し、IP アドレスまたはホスト名を使用して クラウド提供型 Firewall Management Center に到達できる場合は **[Yes]** を。

Security Cloud Control は **configure manager add** コマンドを生成します。コマンドの生成については、手動プロビジョニングによるファイアウォールのオンボーディング（18ページ） を参照してください。

configure manager add *_hostname registration_key nat_id display_name*

28 : configure manager add



b) コマンドの *cdo_hostname*、*registration_key*、および *nat_id* の部分を次のフィールドにコピーします。

- **Management Center/SCC Hostname/IP Address**
- **Management Center/SCC Registration Key**
- **NAT ID**

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。

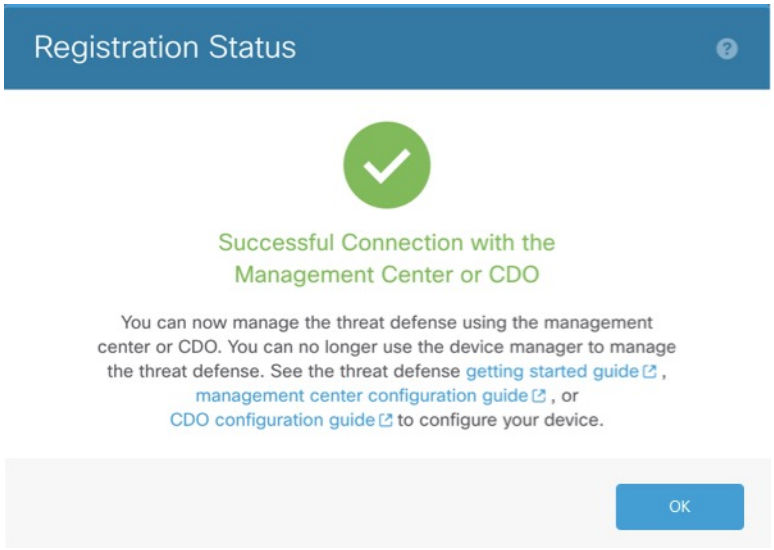
      登録後に外部 DNS サーバー設定を保持するには、クラウド提供型 Firewall Management Center で DNS プラットフォーム設定を再設定する必要があります。

   c) [**Management Center/SCC Access Interface**] で [**Data Interface**] をクリックし、次に [**outside**] を選択します。
7. オプション: [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 クラウド提供型 Firewall Management Center が FQDN で Firewall Threat Defense に到達できるようにします。
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、Security Cloud Control 登録の現在のステータスが表示されます。

29 :



9. ステータス画面で [**Saving Management Center/ Registration Settings**] の手順を実行したら Security 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によるファイアウォールのオンボーディング（18ページ）を参照してください。

CLI

CLI セットアップスクリプトを使用して Cisco Secure Firewall 1210/20 管理アドレッシングを設定し、外部インターフェイス マネージャ アクセスを設定して、デバイスを Security Cloud Control に登録できるようにする方法。

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。

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（6ページ）を参照してください。
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：クラウド提供型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.
>
```

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

   Enter を押すと、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、クラウド提供型 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.

>
```

4. Security Cloud Control が生成した **configure manager add** コマンドを使用して、この Firewall Threat Defense を管理する Security Cloud Control を識別します。コマンドの生成については、手動プロビジョニングによるファイアウォールのオンボーディング（18ページ） を参照してください。

```
> configure manager add account1.app.us.cdo.cisco.com
KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
Manager successfully configured.
```

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。

第 3 章

:

- □□□□□□□ Firewall Management Center □□□□
- □□□□□□□□□□□□
- DHCP □□□□□□□
- NAT □□□
- □□□□□□□□□□□□□
- □□□□□□□□□□□□□ SSH □□□□
- □□□□□□□

Cisco Secure Firewall 1210/20 を起動して稼働させるために、基本的なセキュリティポリシーを設定します。

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。

Firewall Management Center

別の管理タブでポリシーを設定し、Cisco Secure Firewall 1210/20 を管理できるように、Security Cloud Control から クラウド提供型 Firewall Management Center を開く方法。

クラウド提供型 Firewall Management Center は、Security Cloud Control とは別のそれ自体のタブで起動します。

1. Security Cloud Control ホームページから、**[製品（Products）] > [ファイアウォール（Firewall）]**を選択します。
2. **[Administration > Integrations > Firewall Management Center]** の順に選択します。
3. **[Cloud-Delivered FMC]** を選択し、**[Actions]**、**[Management]**、または **[Settings]** ペインのリンクをクリックし、新しいタブで クラウド提供型 Firewall Management Center を開きます。

> **ヒント**
>
> クラウド提供型 Firewall Management Center から Security Cloud Control に戻るには、**[Home]** をクリックします。

内部ゾーンと外部ゾーンの割り当て、ルーテッド展開用の IP アドレッシングの設定など、Cisco Secure Firewall 1210/20 インターフェイスの設定方法について説明します。

初期設定に CLI を使用する代わりに ゼロタッチプロビジョニングまたはFirewall Device Manager を使用する場合、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
- VLAN1：「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

クラウド提供型 Firewall Management Center に登録する前に Firewall Device Manager 内で追加のインターフェイス固有の設定を実行した場合、その設定は保持されます。

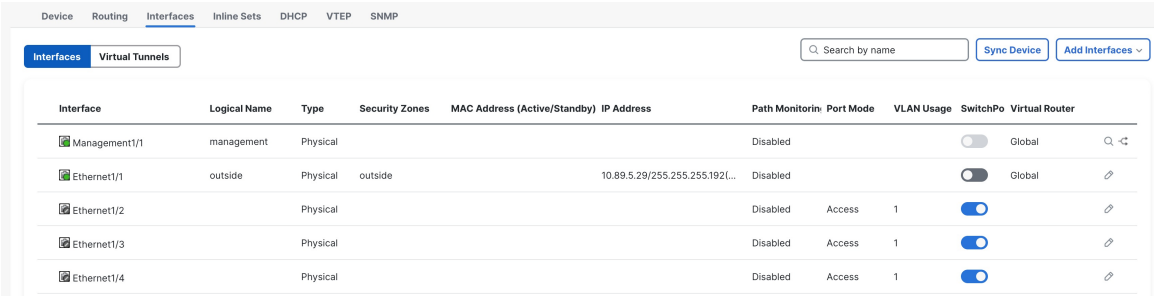
初期設定に CLI を使用した場合、デバイスの事前設定はありません。

どちらの場合も、デバイスの登録後に追加のインターフェイス設定を実行する必要があります。CLIによる初期設定の場合は、内部スイッチポートの VLAN1 インターフェイスを追加する必要があります。追加の設定では、必要に応じてスイッチポートをファイアウォール インターフェイスに変換し、インターフェイスをセキュリティゾーンに割り当てて、IP アドレスを変更します。

次の例では、DHCP によるスタティックアドレスとルーテッドモードの外部インターフェイスを使用して（Ethernet1/1）、ルーテッドモードの内部インターフェイス（VLAN1）を設定します。また、内部 Web サーバー用の DMZ インターフェイスも追加します。

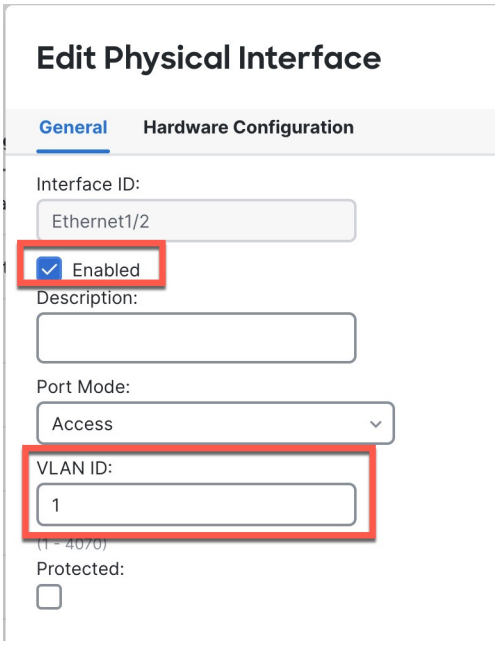
1. [デバイス（Devices）]、[デバイス管理（Device Management）] の順に選択し、デバイスの [編集（Edit）]（ ） をクリックします。 >
2. [インターフェイス（Interfaces）] をクリックします。

30 :



3. 初期設定に CLI を使用した場合は、スイッチポートを有効にします。
   a) スイッチポートの [編集（Edit）] （） をクリックします。

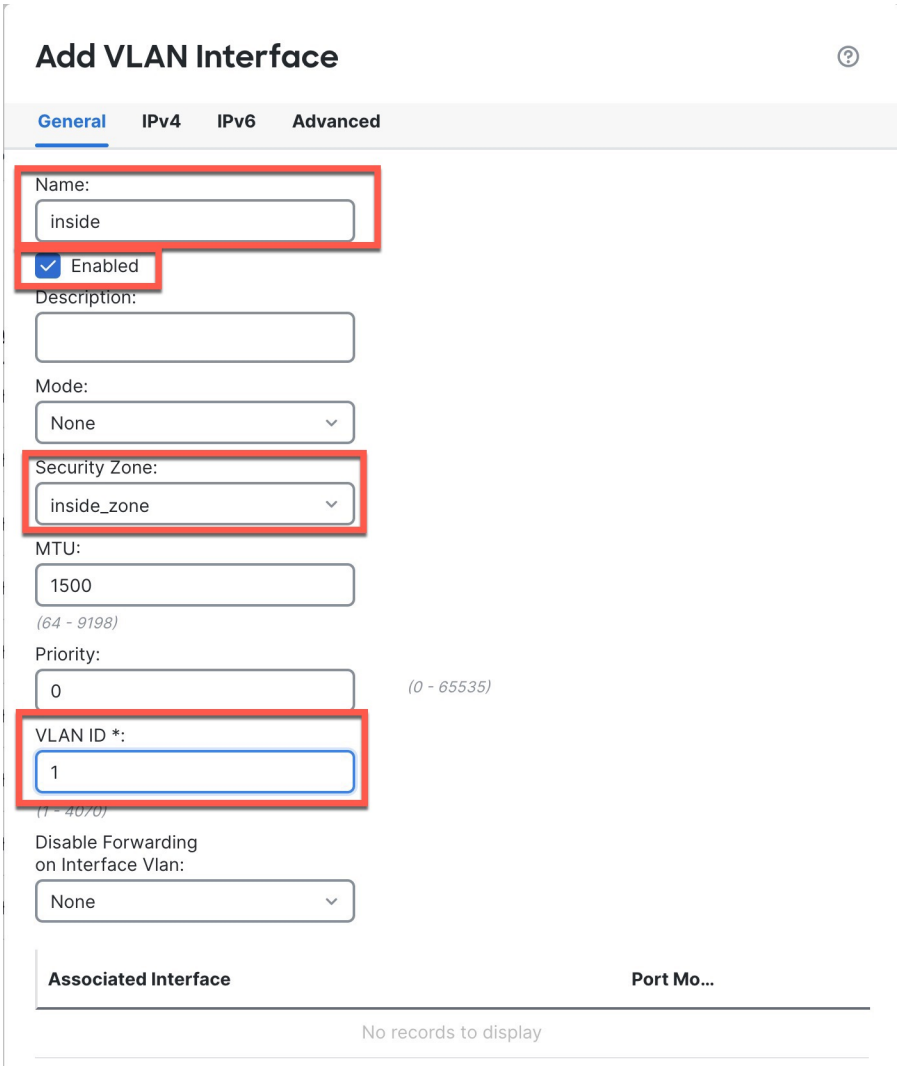
      31 :



   b) [有効（Enabled）] チェックボックスをオンにして、インターフェイスを有効化します。
   c) オプション: VLAN ID を変更します。デフォルトは 1 です。次に、この ID に一致する VLAN インターフェイスを追加します。
   d) [OK] をクリックします。

4. 「内部」VLAN インターフェイスを追加（または編集）します。
   a) **[インターフェイスの追加（Add Interfaces）] > [VLANインターフェイス（VLAN Interface）]** をクリックします。このインターフェイスがすでに存在する場合は、インターフェイスの [編集（Edit）] （） をクリックします。

      32 : VLAN



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

たとえば、**inside_zone** という名前のゾーンを追加します。ゾーンまたはグループに基づいてセキュリティポリシーを適用します。

VLAN1 が事前設定されている場合、これらのフィールドの残りの部分はオプションです。

c) 48 文字までの [名前（Name）] を入力します。

たとえば、インターフェイスに **inside** という名前を付けます。

d) [有効（Enabled）] チェックボックスをオンにします。

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

f) [VLAN ID] を **1** に設定します。

デフォルトでは、すべてのスイッチポートは VLAN 1 に設定されます。ここで別の VLAN ID を選択する場合は、新しい VLAN ID の各スイッチポートを編集する必要があります。

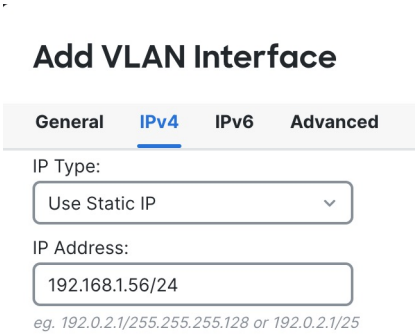
インターフェイスを保存した後、VLAN ID を変更することはできません。ここでの VLAN ID は、使用される VLAN タグと設定内のインターフェイス ID の両方です。

g) [IPv4] タブ、[IPv6] タブ、または両方のタブをクリックします。

- [IPv4]：ドロップダウンリストから [スタティックIPを使用する（Use Static IP）] を選択し、IP アドレスとサブネットマスクをスラッシュ表記で入力します。

たとえば、**192.168.1.56/24** と入力します。

33： IP



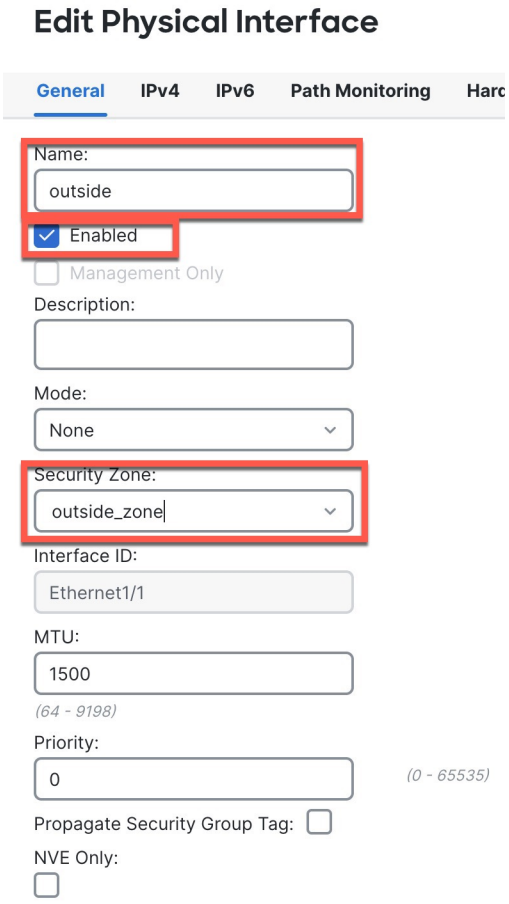
- [IPv6]：ステートレス自動設定の場合は[自動設定（Autoconfiguration）]チェックボックスをオンにします。

h) [OK] をクリックします。

5. 外部用に使用する Ethernet1/1 の[編集（Edit）]（✎）をクリックします。

[全般（General）] ページが表示されます。

34：



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

たとえば、「outside_zone」という名前のゾーンを追加します。

他の基本設定は変更しないでください。変更すると、クラウド提供型 Firewall Management Center の管理接続が中断されます。

b) [OK] をクリックします。

6. たとえば、Web サーバーをホストするように DMZ インターフェイスを設定します。
   a) DMZ に使用するスイッチポートのスイッチポートモードを、[スイッチポート（SwitchPort）] 列のスライダをクリックして無効にすると、無効（）と表示されます。
   b) インターフェイスの [編集（Edit）]（） をクリックします。
   c) [セキュリティゾーン（Security Zone）] ドロップダウンリストから既存の DMZ セキュリティゾーンを選択するか、[新規（New）] をクリックして新しいセキュリティゾーンを追加します。

      たとえば、**dmz_zone** という名前のゾーンを追加します。

   d) 48 文字までの [名前（Name）] を入力します。

      たとえば、インターフェイスに **dmz** という名前を付けます。

   e) [有効（Enabled）] チェックボックスをオンにします。
   f) [モード（Mode）] は [なし（None）] に設定したままにします。
   g) 必要に応じて、[IPv4] タブと [IPv6] タブのいずれかまたは両方をクリックし、IP アドレスを設定します。
   h) [OK] をクリックします。
7. [保存（Save）] をクリックします。

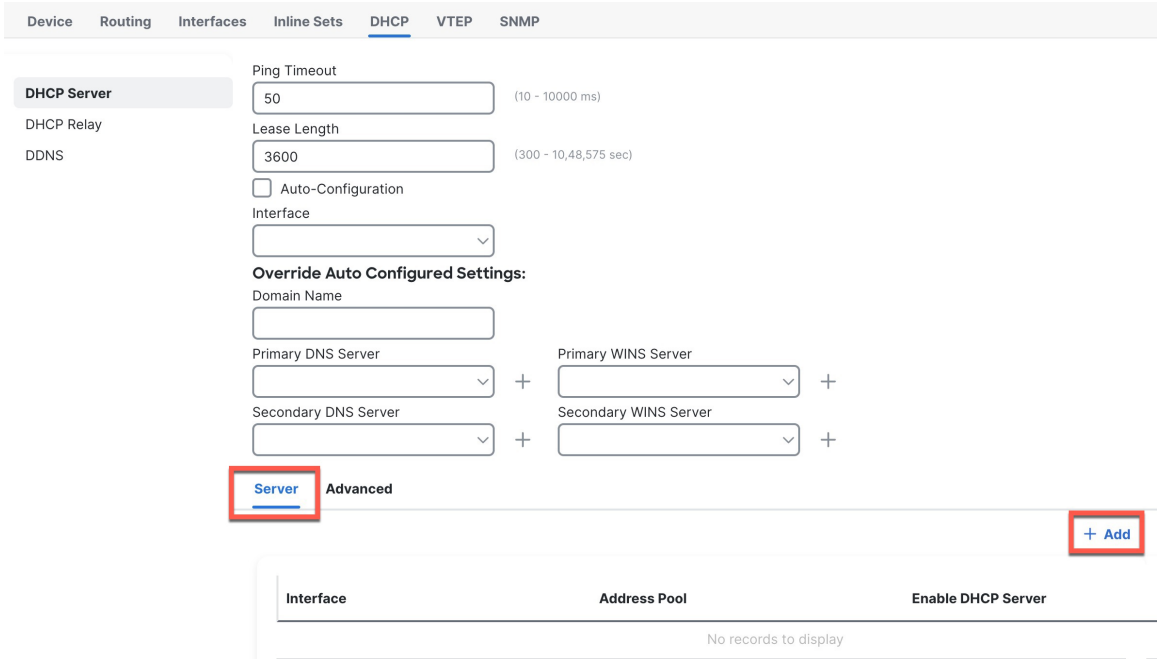
DHCP

Cisco Secure Firewall 1210/20 インターフェイスで DHCP サーバーを有効にし、内部クライアントが IP アドレスおよび関連ネットワーク設定を自動的に受信できるようにする方法。

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。

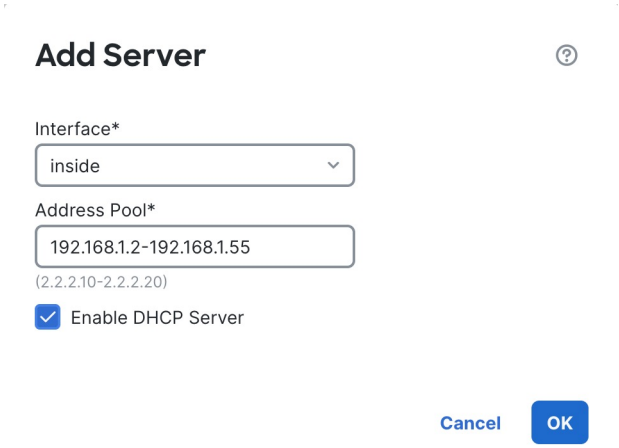
1. [デバイス（Devices）]、[デバイス管理（Device Management）] の順に選択し、デバイスの [編集（Edit）]（） をクリックします。 >
2. **[DHCP] > [DHCPサーバー（DHCP Server）]** を選択します。

35 : DHCP



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。

36 :



- [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。

4. [OK] をクリックします。
5. [保存（Save）] をクリックします。

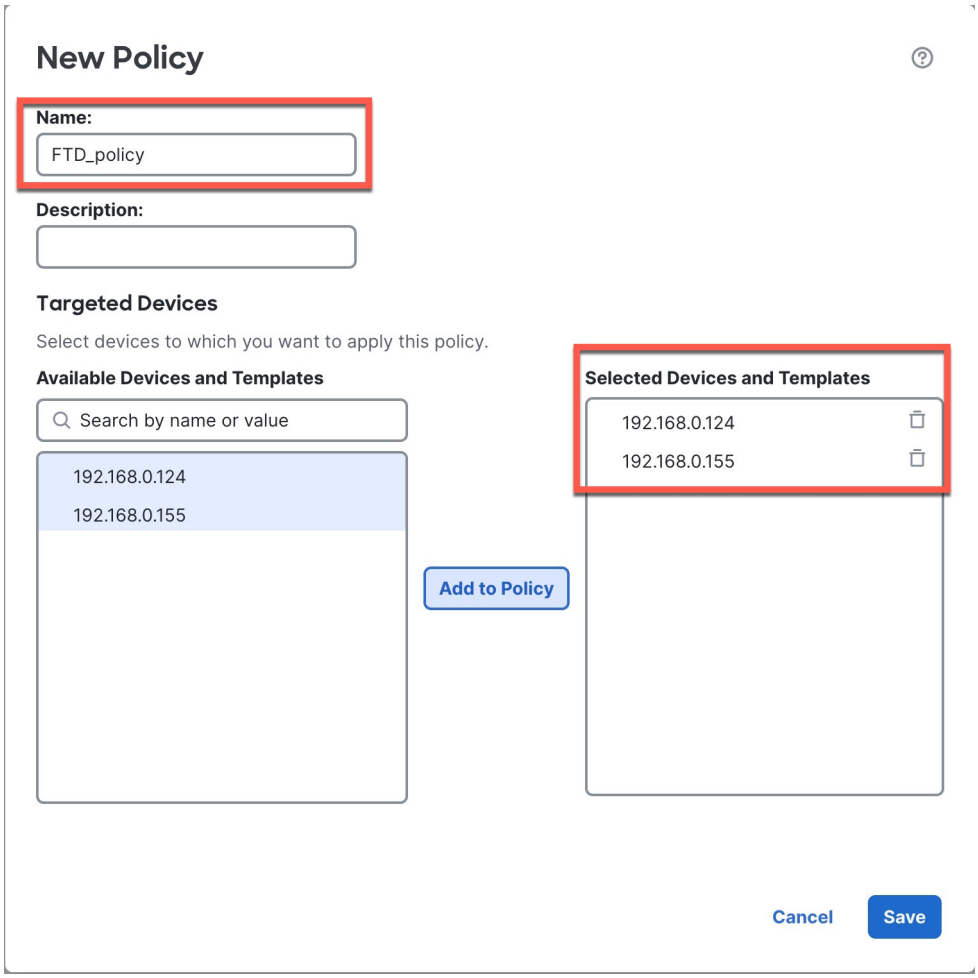
NAT

内部クライアントが外部インターフェイス IP アドレスを使用して外部ネットワークにアクセスできるように、インターフェイス PAT（NAT）ポリシーを作成する方法について説明します。

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。

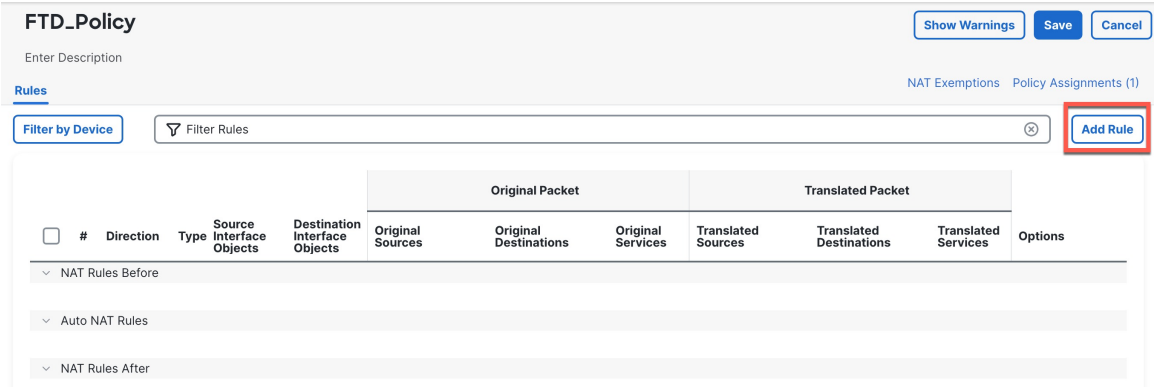
1. **[デバイス（Devices）] > [NAT]** の順に選択し、**[新しいポリシー（New Policy）]** をクリックします。
2. ポリシーに名前を付け、ポリシーを使用するデバイスを選択し、[保存（Save）] をクリックします。

37 :



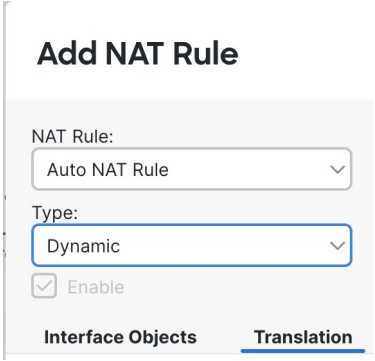
ポリシーが クラウド提供型 Firewall Management Center に追加されます。引き続き、ポリシーにルールを追加する必要があります。

38 : NAT



3. [ルールの追加（Add Rule）] をクリックします。
4. 基本ルールのオプションを設定します。

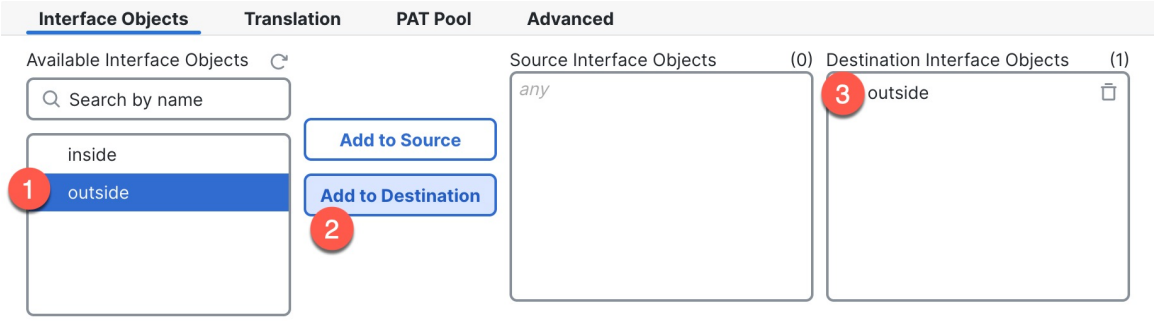
   39 :



- [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。

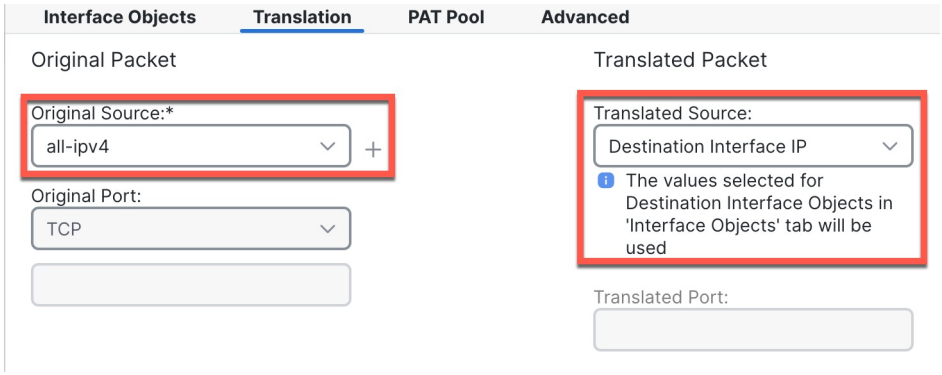
5. [インターフェイスオブジェクト（Interface objects）] ページで、[使用可能なインターフェイスオブジェクト（Available Interface Objects）] 領域から [宛先インターフェイスオブジェクト（Destination Interface Objects）] 領域に外部ゾーンを追加します。

   40 :



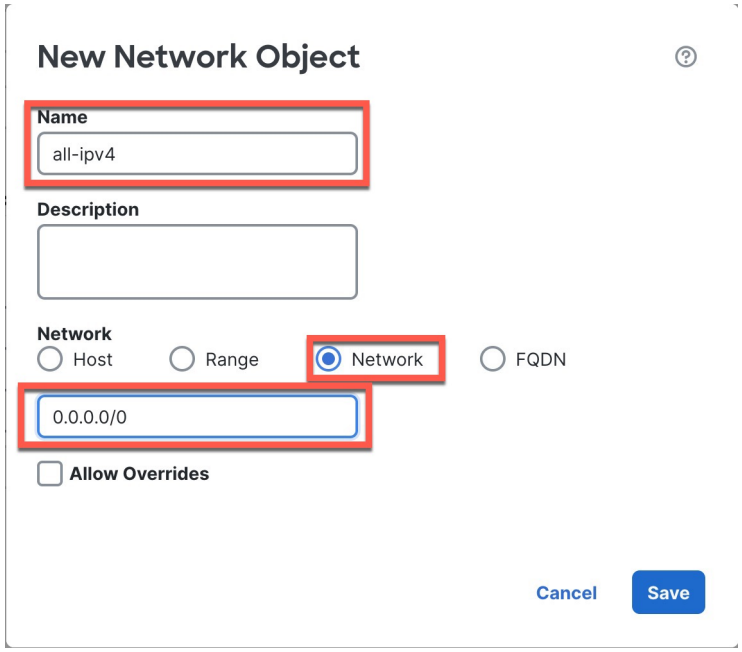
6. [変換（Translation）] ページで、次のオプションを設定します。

   41 :



- **[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。

  42 :



> **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。

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。

8. NATページで[保存（Save）]をクリックして変更を保存します。

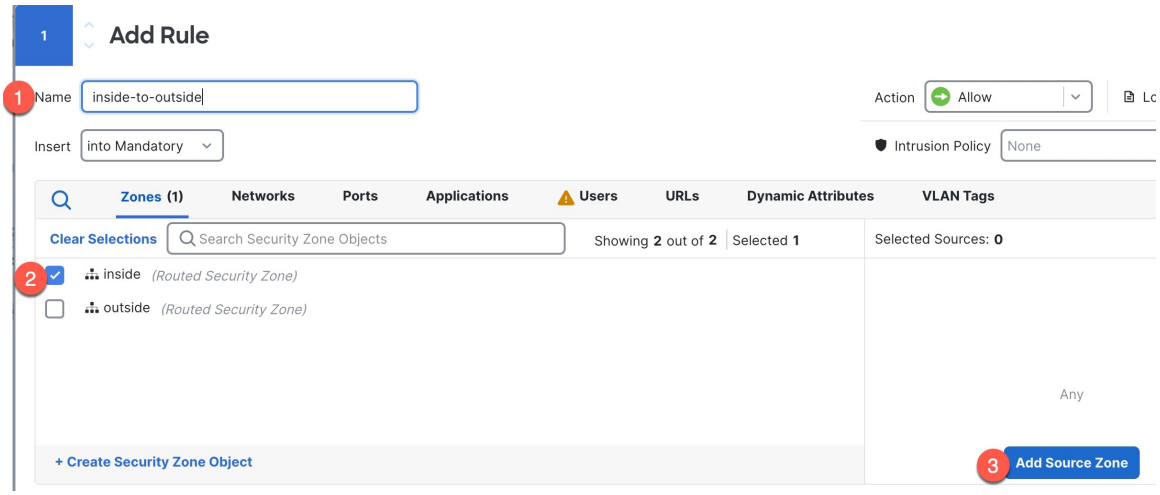
Cisco Secure Firewall 1210/20 の内部ゾーンから外部ゾーンへのトラフィックを許可するアクセス制御ルールを追加し、オプションのセキュリティ検査ポリシーを適用する方法。

ファイアウォールを登録したときに、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、ファイアウォール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。

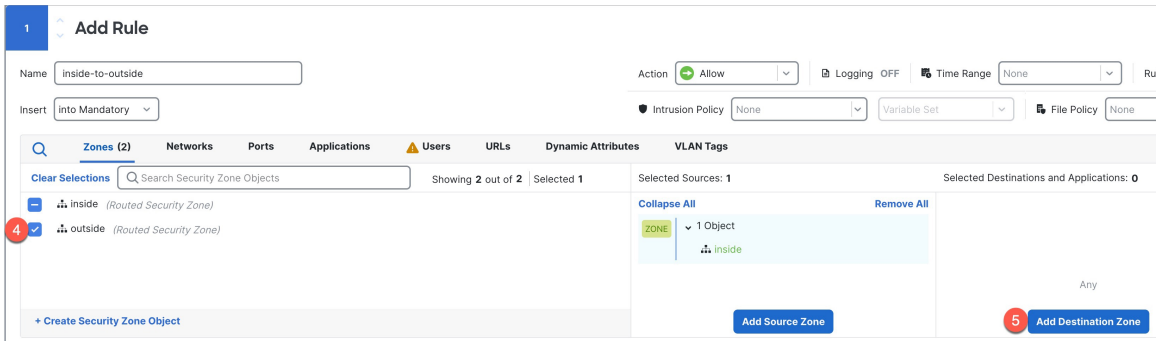
1. **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [アクセス制御（Access Control）]** を選択し、デバイスに割り当てられているアクセス コントロール ポリシーの [編集（Edit）]（✎）をクリックします。
2. [ルールを追加（Add Rule）] をクリックし、次のパラメータを設定します。

43 : 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。

44 : 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。

3. オプション: 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。

   45 :

   - [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。

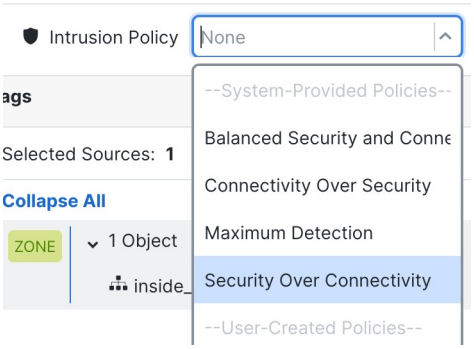
   - [アイデンティティ（Identity）]：アイデンティティはデフォルトでは適用されません。アクセス コントロール ポリシーによるトラフィックの処理を許可する前に、ユーザーに認証を要求できます。

4. オプション: 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。クラウド提供型 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。

46 :



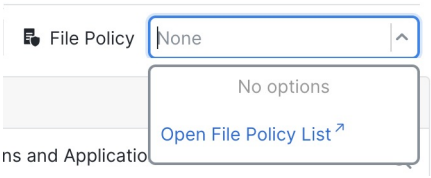
b) リストからシステム提供のポリシーを 1 つ選択します。

ほとんどのユースケースでは、[バランスのとれたセキュリティと接続性（Balanced Security and Connections）] を推奨しています。

5. オプション: 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。

47 : File Policy



新しいポリシーの場合は、**[[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [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* 設定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。

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。

7. [保存（Save）] をクリックします。

SSH

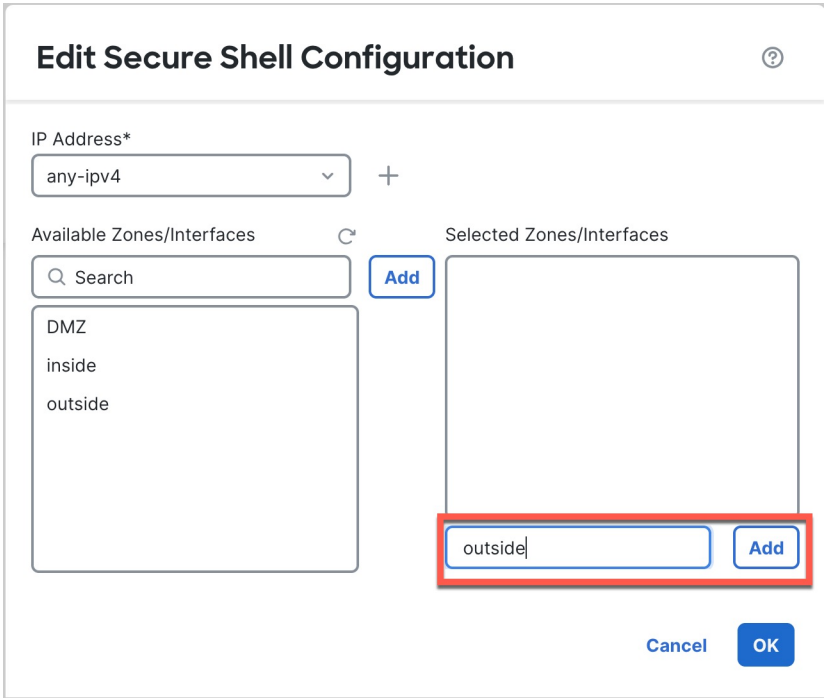
Cisco Secure Firewall 1210/20 の外部インターフェイスへの SSH アクセスを有効にして、承認された IP アドレスからデバイスをリモートで管理できるようにする方法について説明します。

このセクションでは、外部インターフェイスへの SSH 接続を有効にして、ファイアウォールをリモートから管理できるよう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。

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。
2. [SSHアクセス（SSH Access）] を選択します。
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。

48 :　　SSH



   c) [OK] をクリックします。
4. **[Save（保存）]** をクリックします。

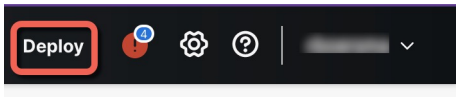
   これで、**[[展開（Deploy）] > [展開（Deploy）]]** に移動して、割り当てたデバイスにポリシーを展開できるようになります。変更はポリシーを展開するまで有効になりません。

インターフェイス、NAT、DHCP、およびアクセス制御の更新がデバイスで有効になるように、ポリシー変更を Cisco Secure Firewall 1210/20 に展開する方法。

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。

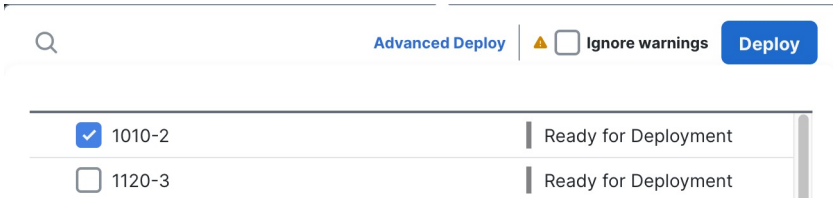
1. 右上の [展開（Deploy）] をクリックします。

49 :



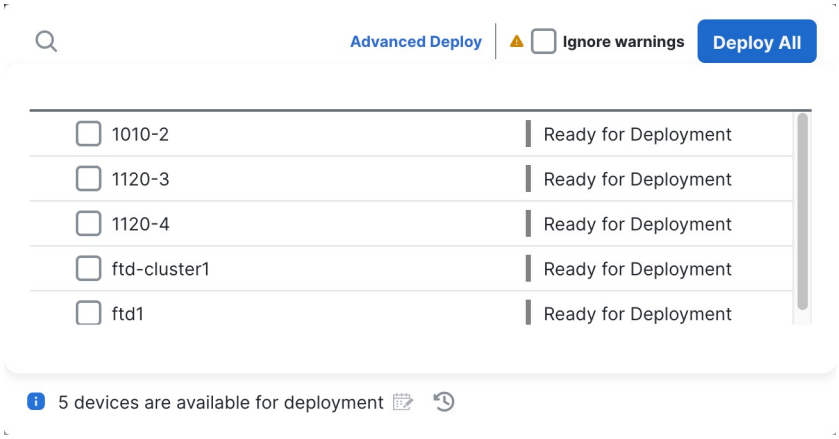
2. 迅速な展開の場合は、特定のデバイスのチェックボックスをオンにして [展開（Deploy）] をクリックします。

50 :



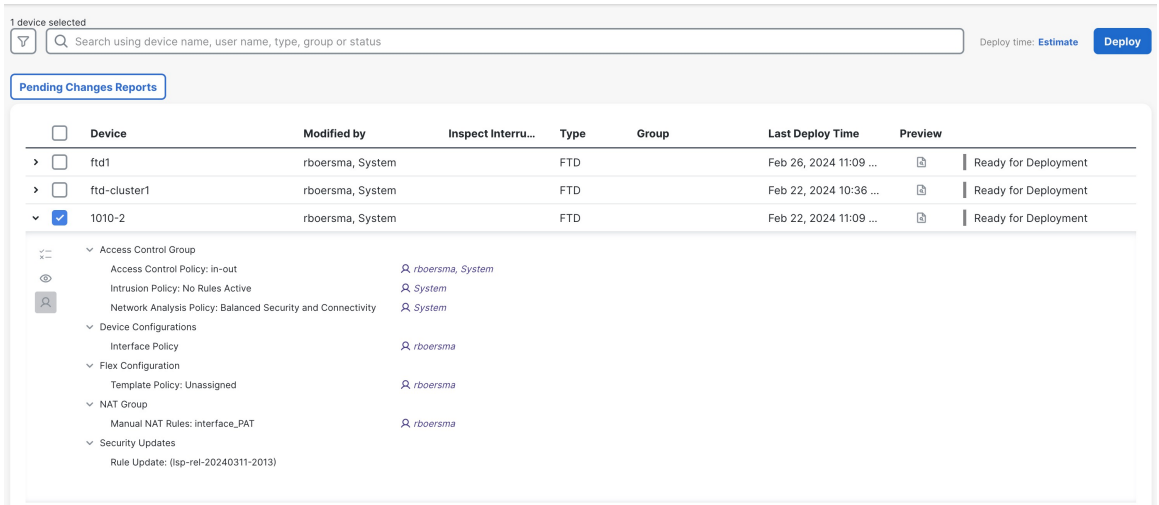
または、[すべて展開（Deploy All）] をクリックしてすべてのデバイスに展開します。

51 :



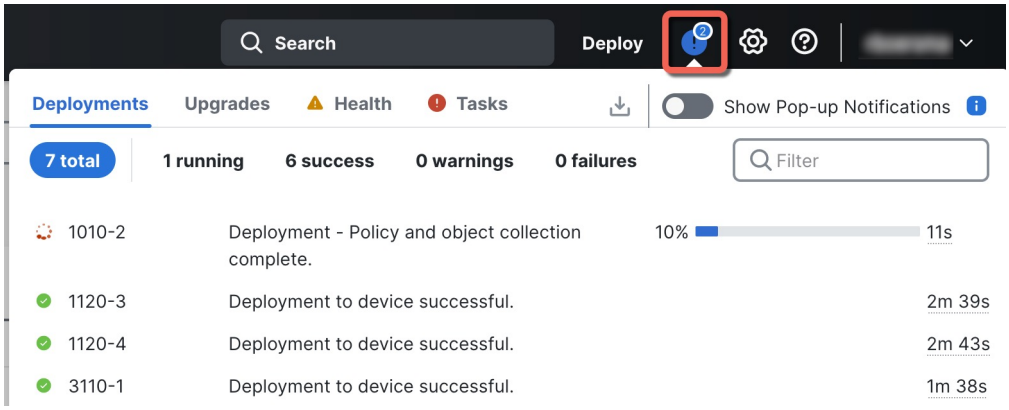
それ以外の場合は、追加の展開オプションを設定するために、[高度な展開（Advanced Deploy）] をクリックします。

52 :



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。

53 :



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。

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。

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。

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。