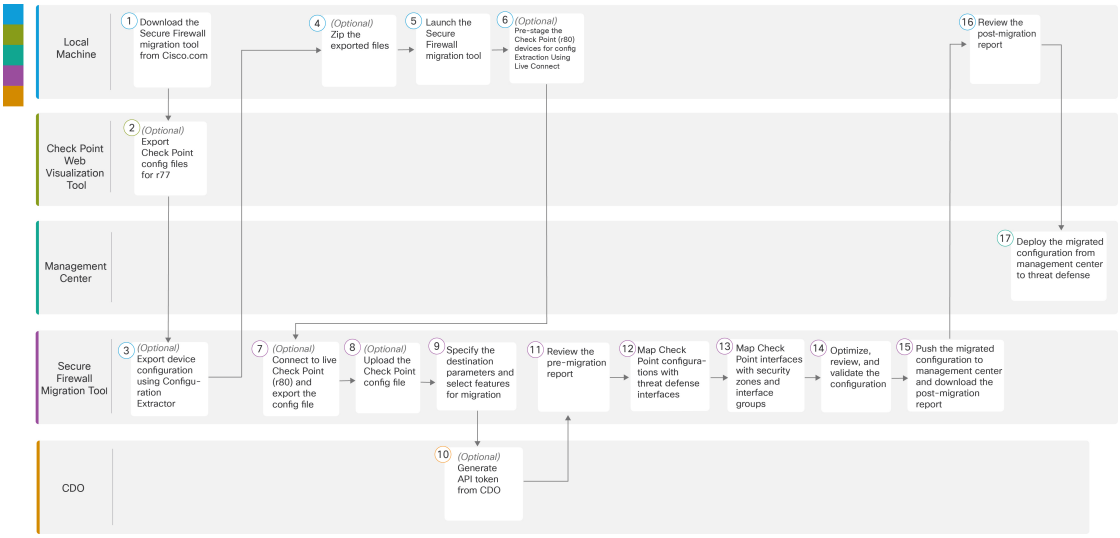
Check Point の Threat Defense への移行ワークフロー

エンドツーエンドの手順

次のフローチャートは、Cisco Secure Firewall 移行ツールを使用して、Check Point ファイアウォールを Threat Defense に移行するワークフローを示しています。



	ワークスペース	手順
1	Local Machine	Cisco.com から Cisco Secure Firewall 移行ツールをダウンロードします。詳細な手順については、「Cisco.com からの Cisco Secure Firewall 移行ツールのダウンロード」を参照してください。
2	Check Point の Web 可視化ツール	（任意）r77 の Check Point 構成ファイルをエクスポートします。r77 の Check Point 構成ファイルをエクスポートするには、「r77 の Check Point 構成ファイルのエクスポート」を参照してください。Cisco Secure Firewall 移行ツールの Live Connect 機能を使用して r80 の構成ファイルをエクスポートする場合は、手順 5 にスキップします。
3	Local Machine	（任意）FMT-CP-Config-Extractor を使用してデバイス構成をエクスポートします。FMT-CP-Config-Extractor_v4.0.1-8248 を使用して r77 のデバイス構成をエクスポートするには、「FMT-CP-Config-Extractor_v4.0.1-8248 ツールを使用したデバイス構成のエクスポート」を参照してください。
4	Local Machine	（任意）エクスポートされたファイルを圧縮します。r77 用にエクスポートされたすべての構成ファイルを選択し、それらを zip ファイルに圧縮します。詳細な手順については、「エクスポートされたファイルの圧縮」を参照してください。
5	Local Machine	ローカルマシンで Cisco Secure Firewall 移行ツールを起動します。「Cisco Secure Firewall 移行ツールの起動」を参照してください。
6	Local Machine	構成抽出のための Check Point（r80）デバイスの事前設定：Firewall の Live Connect を使用する前に、Check Point（r80）デバイスでログイン情報を構成する必要があります。Check Point（r80）デバイスのログイン情報の事前設定については、「Live Connect を使用した構成抽出のための Check Point（r80）デバイスの事前設定」を参照してください。この手順は、r80 デバイスの構成ファイルの移行を計画している場合にのみ必要です。r77 デバイスの構成を移行する予定の場合は、手順 8 にスキップします。
7	Cisco Secure Firewall 移行ツール	（任意）ライブ Check Point（r80）に接続し、構成ファイルをエクスポートします。Live Connect 機能を使用して r80 の Check Point 構成ファイルをエクスポートするには、「r80 の Check Point 構成ファイルをエクスポートする手順」を参照してください。
8	Cisco Secure Firewall 移行ツール	（任意）Check Point 構成ファイルをアップロードします。Check Point 構成ファイルのアップロードの詳細な手順については、「Check Point 構成ファイルのアップロード」を参照してください。

	ワークスペース	手順
9	Cisco Secure Firewall 移行ツール	このステップでは、移行の接続先パラメータを指定できます。詳細な手順については、「Cisco Secure Firewall 移行ツールの接続先パラメータの指定」を参照してください。
10	CDO	（任意）この手順は任意であり、クラウドで提供される Firewall Management Center を移行先管理センターとして選択した場合にのみ必要です。詳細な手順については、「Cisco Secure Firewall 移行ツールの接続先パラメータの指定」を参照してください。
11	Cisco Secure Firewall 移行ツール	移行前レポートをダウンロードした場所に移動し、レポートを確認します。詳細な手順については、「移行前レポートの確認」を参照してください。
12	Cisco Secure Firewall 移行ツール	Cisco Secure Firewall 移行ツールを使用すると、Check Point 構成を Threat Defense インターフェイスにマッピングできます。詳細な手順については、「チェックポイント 構成と Secure Firewall Device Manager Threat Defense インターフェイスのマッピング」を参照してください。
13	Cisco Secure Firewall 移行ツール	Check Point 構成が正しく移行されるように、Check Point インターフェイスを適切な Threat Defense インターフェイス オブジェクト、セキュリティゾーン、およびインターフェイスグループにマッピングします。詳細な手順については、「セキュリティゾーンとインターフェイスグループへの チェックポイント インターフェイスのマッピング」を参照してください。
14	Cisco Secure Firewall 移行ツール	構成を慎重に確認し、それが適切で Threat Defense デバイスの構成内容と一致することを確認します。詳細な手順については、「最適化、 構成の確認と検証」を参照してください。
15	Cisco Secure Firewall 移行ツール	移行プロセスのこのステップでは、移行された構成を管理センターに送信し、移行後レポートをダウンロードできるようにします。詳細な手順については、「移行された構成の以下へのプッシュ：Management Center」を参照してください。
16	Local Machine	移行後レポートをダウンロードした場所に移動し、レポートを確認します。詳細な手順については、「Check Point の移行後レポートの確認と移行の完了」を参照してください。
17	Management Center	移行した構成を管理センターから Threat Defense に展開します。詳細な手順については、「Check Point の移行後レポートの確認と移行の完了」を参照してください。

移行の前提条件

チェックポイント 構成を移行する前に、次のアクティビティを実行します。

Cisco.com からの Cisco Secure Firewall 移行ツールのダウンロード

始める前に

Cisco.com へのインターネット接続が可能な Windows 10 64 ビットまたは macOS バージョン 10.13 以降のマシンが必要です。

ステップ 1 コンピュータで、Cisco Secure Firewall 移行ツール用のフォルダを作成します。

このフォルダには、他のファイルを保存しないことをお勧めします。Cisco Secure Firewall 移行ツールを起動すると、ログ、リソース、およびその他すべてのファイルがこのフォルダに配置されます。

（注） Cisco Secure Firewall 移行ツールの最新バージョンをダウンロードする場合は、必ず新しいフォルダを作成し、既存のフォルダは使用しないでください。

ステップ 2 https://software.cisco.com/download/home/286306503/type を参照し、[Firewall移行ツール（Firewall Migration Tool）] をクリックします。

上記のリンクをクリックすると、[Firewall NGFWバーチャル（Firewall NGFW Virtual）] の [Cisco Secure Firewall移行ツール（Firewall Migration Tool）] に移動します。脅威に対する防御 デバイスのダウンロード領域から Cisco Secure Firewall 移行ツールをダウンロードすることもできます。

ステップ 3 Cisco Secure Firewall 移行ツールの最新バージョンを、作成したフォルダにダウンロードします。

Windows 用または macOS マシン用の適切な Cisco Secure Firewall 移行ツール実行可能ファイルをダウンロードします。

次のタスク

Check Point 構成ファイルのエクスポート

Check Point 構成ファイルのエクスポート

次の Check Point 構成をエクスポートできます。

- r77 の Check Point 構成ファイルのエクスポート
- r80 の Check Point 構成ファイルのエクスポート

r77 の Check Point 構成ファイルのエクスポート

r77 の Check Point 構成ファイルをエクスポートするには、次の手順を実行します。

- Check Point Web Visualization Tool（WVT）を使用した構成のエクスポート
- FMT-CP-Config-Extractor_v4.0.1-8248 ツールを使用したデバイス構成のエクスポート （6 ページ）
- エクスポートされたファイルの圧縮

Check Point Web Visualization Tool（WVT）を使用した構成のエクスポート

ステップ 1 Check Point Management Server にアクセスできるワークステーションでコマンドプロンプトを開きます。

ステップ 2 Check Point Firewall バージョンに適した Check Point Portal から WVT をダウンロードします。

ステップ 3 WVT zip ファイルを解凍します。

ステップ 4 Check Point WVT ツールが抽出された同じルートフォルダの下に新しいサブフォルダを作成します。

ステップ 5 コマンドプロンプトで、ディレクトリを WVT が保存されているディレクトリに変更し、次のコマンドを実行します。

```
C:\Web_Visualisation_Tool> cpdb2web.exe [-s management_server] [-u admin_name | -a certificate_file]
[-p password] [-o output_file_path] [-t table_names] [-c | -m gateway | -l package_names] [-gr]
[-go] [-w Web_Visualization_Tool_installation_directory]
```

次に例を示します。

```
C:\Web_Visualisation_Tool> cpdb2web.exe -s 172.16.0.1  -u admin -p admin123 -o  Outputs
```

次のコマンドを実行すると、合計 7 つのファイルが Outputs ディレクトリに作成されます。

コマンド	説明
C:\Web_Visualisation_Tool	WVT ツールのルートディレクトリ。
172.16.0.1	Check Point Management Server の IP アドレス。
admin	Check Point Management Server のユーザ名。
Admin123	Check Point Management Server のパスワード。
出力	出力ファイルを保存する相対パス。

（注） セキュリティポリシーおよびNATポリシーファイルの名前は、それぞれ`Security_Policy.xml`および`NAT_Policy.xml`である必要があります。ファイル名が異なる場合は、手動で名前を変更します。

複数のセキュリティおよびNATポリシーファイルがある場合は、移行するCheck Pointデバイスの`Security_Policy.xml`および`NAT_Policy.xml`ファイルのみを選択して保持してください。

次のタスク

FMT-CP-Config-Extractor_v4.0.1-8248 ツールを使用したデバイス構成のエクスポート

FMT-CP-Config-Extractor_v4.0.1-8248 ツールを使用したデバイス構成のエクスポート

ステップ 1 Cisco Secure Firewall 移行ツールのソフトウェア ダウンロード ページから FMT-CP-Config-Extractor_v4.0.1-8248.exe をダウンロードします。

ステップ 2 Check Point Security Gateway にアクセスできるワークステーションで、Windows の実行ファイル（.exe）である FMT-CP-Config-Extractor_v4.0.1-8248 ツールを開きます。

ステップ 3 Cisco Secure Firewall 移行ツールを使用してポリシーを移行する Check Point Security Gateway に接続します。

接続するには、次の情報が必要です。

a) [IP アドレス（IP Address）]
b) ポート
c) ユーザ名
d) パスワード

ステップ 4 FMT-CP-Config-Extractor_v4.0.1-8248 ツールから取得した出力ファイルの名前を`networking.txt`ファイルに変更します。

次のコマンドが、FMT-CP-Config-Extractor_v4.0.1-8248 ツールによって実行されます。

- **show hostname**
- **show version product**
- **show interfaces**
- **fw vsx stat**
- **show management interface**
- **show configuration bonding**
- **show configuration bridging**
- **show configuration interface**
- **show configuration static-route**
- **show ipv6-state**

- **show configuration ipv6 static-route**
- **netstat -rnv**

すべてのコマンドは FMT-CP-Config-Extractor_v4.0.1-8248 ツールによってバックグラウンドで実行され、出力は .txt ファイルとして保存されます。

たとえば、172.16.0.1 は、ポリシーを移行する Check Point Firewall Gateway の IP アドレスです。

ステップ 5 Check Point VSX（Virtual System eXtension）バージョン R77 から構成をエクスポートしようとしている場合は、次のコマンドを手動で実行し、出力を .txt ファイルに保存します。

- **show hostname**
- **show version product**
- **show interfaces**
- **fw vsx stat**
- **fw vsx stat <vsid>**
- **set virtual system <vsid>**

  ヒント　**vsid** は、仮想システム ID を示します。

- **fw getifs**
- **show management interface**
- **show configuration bonding**
- **show configuration bridging**
- **show configuration interface**
- **show configuration static-route**
- **show ipv6-state**
- **show configuration ipv6 static-route**
- **netstat -rnv**

ステップ 6 .txt ファイルを `Outputs` フォルダに移動します。

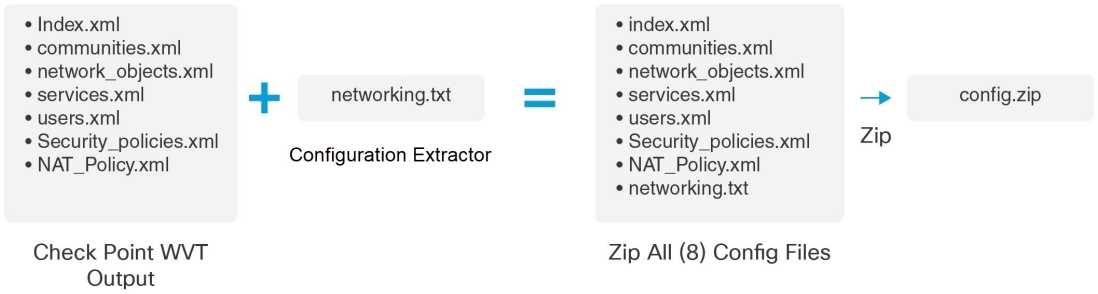
次のタスク

エクスポートされたファイルの圧縮

エクスポートされたファイルの圧縮

8 つすべてのファイル（Web Visualization Tool（WVT）からの 7 つのファイルと、FMT-CP-Config-Extractor_v4.0.1-8248 ツールからの 1 つの .txt ファイル）を選択し、1 つの zip ファイルに圧縮します。

（注） 移行用のファイルを圧縮する前に、`Security_Policy.xml` および `NAT_Policy.xml` のファイルが Threat Defense に移行する Check Point デバイス用であることを確認します。



*Check Point エクストラクタのバージョン：FMT-CP-Config-Extractor_v4.0.1-8248

（注） .tar またはその他の圧縮ファイルタイプはサポートされていません。

次のタスク

Check Point 構成ファイルのアップロード

移行の実行

Cisco Secure Firewall 移行ツールの起動

（注） Cisco Secure Firewall 移行ツールを起動すると、別のウィンドウでコンソールが開きます。移行が進むのに合わせて、Cisco Secure Firewall 移行ツールの現在のステップの進行状況がコンソールに表示されます。画面にコンソールが表示されない場合は、Cisco Secure Firewall 移行ツールの背後にある可能性があります。

始める前に

- Cisco.com からの Cisco Secure Firewall 移行ツールのダウンロード
- サポートされる移行先の管理センターセクションで要件を確認します。

- Cisco Secure Firewall 移行ツールを実行するために、最新バージョンの Google Chrome ブラウザがコンピュータにインストールされていることを確認します。Google Chrome をデフォルトのブラウザとして設定する方法については、「Set Chrome as your default web browser」を参照してください。
- 大規模な構成ファイルを移行する場合は、移行プッシュ中にシステムがスリープ状態にならないようにスリープ設定を構成します。

ステップ 1 コンピュータで、Cisco Secure Firewall 移行ツールをダウンロードしたフォルダに移動します。

ステップ 2 次のいずれかを実行します。

- Windows マシンで、Cisco Secure Firewall 移行ツールの実行可能ファイルをダブルクリックして、Google Chrome ブラウザで起動します。

  プロンプトが表示されたら、[はい（Yes）] をクリックして、Cisco Secure Firewall 移行ツールがシステムに変更を加えることができるようにします。

  Cisco Secure Firewall 移行ツールは、すべての関連ファイルを作成し、Cisco Secure Firewall 移行ツールの存在するフォルダに保存します（ログおよびリソースのフォルダを含む）。

- Mac では、Cisco Secure Firewall 移行ツールの `*.command` ファイルを目的のフォルダに移動し、ターミナルアプリケーションを起動して、Cisco Secure Firewall 移行ツールがインストールされているフォルダを参照し、次のコマンドを実行します。

  ```
  # chmod 750 Firewall_Migration_Tool-version_number.command
  ```

  ```
  # ./Firewall_Migration_Tool-version_number.command
  ```

  Cisco Secure Firewall 移行ツールは、すべての関連ファイルを作成し、Cisco Secure Firewall 移行ツールの存在するフォルダに保存します（ログおよびリソースのフォルダを含む）。

  ヒント Cisco Secure Firewall 移行ツールを開こうとすると、警告ダイアログが表示されます。これは、身元が明らかな開発者によって Cisco Secure Firewall 移行ツールが Apple に登録されていないためです。身元不明の開発者によるアプリケーションを開く方法については、「Open an app from an unidentified developer」を参照してください。

  （注） MAC のターミナルの zip メソッドを使用します。

ステップ 3 [エンドユーザライセンス契約（End User License Agreement）] ページで、テレメトリ情報をシスコと共有する場合は、[Cisco Success Network と情報を共有することに同意（I agree to share data with Cisco Success Network）] をクリックし、それ以外の場合は [後で行う（I'll do later）] をクリックします。

Cisco Success Network に統計を送信することに同意すると、Cisco.com アカウントを使用してログインするように求められます。Cisco Success Network に統計を送信しないことを選択した場合は、ローカルログイン情報を使用して Cisco Secure Firewall 移行ツールにログインします。

ステップ 4 Cisco Secure Firewall 移行ツールのログインページで、次のいずれかを実行します。

- Cisco Success Network と統計を共有するには、[CCOでログイン（Login with CCO）] リンクをクリックし、シングルサインオンログイン情報を使用して Cisco.com アカウントにログインします。

（注） Cisco.com アカウントがない場合は、Cisco.com のログインページで作成します。

- 次のデフォルトログイン情報でログインします。
  - ユーザー名：admin
  - パスワード：Admin123

Cisco.com アカウントを使用してログインしている場合は、ステップ 8 に進みます。

ステップ 5 [パスワードのリセット（Reset Password）] ページで、古いパスワードと新しいパスワードを入力し、新しいパスワードを確認します。

新しいパスワードは 8 文字以上で、大文字と小文字、数字、および特殊文字を含める必要があります。

ステップ 6 [リセット（Reset）] をクリックします。

ステップ 7 新しいパスワードでログインします。

（注） パスワードを忘れた場合は、既存のすべてのデータを <*migration_tool_folder*> から削除し、Cisco Secure Firewall 移行ツールを再インストールします。

ステップ 8 移行前チェックリストを確認し、記載されているすべての項目を完了していることを確認します。

チェックリストの項目を 1 つ以上完了していない場合は、完了するまで続行しないでください。

ステップ 9 [新規移行（New Migration）] をクリックします。

ステップ 10 [ソフトウェアアップデートの確認（Software Update Check）] 画面で、Cisco Secure Firewall 移行ツールの最新バージョンを実行しているかどうかが不明な場合は、リンクをクリックし、Cisco.com でバージョンを確認します。

ステップ 11 [続行（Proceed）] をクリックします。

次のタスク

次のステップに進むことができます。

- Check Point 構成をコンピュータにエクスポートした場合は、「Check Point 構成ファイルのアップロード」に進みます。
- Cisco Secure Firewall 移行ツールを使用して Check Point（r77）から情報を抽出する必要がある場合は、「r77 の Check Point 構成ファイルのエクスポート」に進みます。
- Cisco Secure Firewall 移行ツールを使用して Check Point（r80）から情報を抽出する必要がある場合は、「r80 の Check Point 構成ファイルのエクスポート」に進みます。

r80 の Check Point 構成ファイルのエクスポート

（注） Check Point r80 構成のエクスポートは、Cisco Secure Firewall 移行ツールの Live Connect 機能でのみサポートされます。

Check Point デバイスで移行のために必要なログイン情報を構成したり、Check Point 構成ファイルをエクスポートしたりするには、次の手順を実行します。

- Live Connect を使用した構成抽出のための Check Point（r80）デバイスの事前設定
- r80 の Check Point 構成ファイルをエクスポートする手順

Live Connect を使用した構成抽出のための Check Point（r80）デバイスの事前設定

次のいずれかの手順を使用して、移行前に Check Point（r80）デバイスでログイン情報を構成できます。

- 分散 Check Point 展開からのエクスポート：Check Point Security Gateway と Check Point Security Manager が別々にある場合。
- スタンドアロン Check Point 展開からのエクスポート：Check Point Security Gateway と Check Point Security Manager が単一デバイス上にある場合。
- マルチドメイン Check Point 展開からのエクスポート：Check Point Security Gateway と Check Point Security Manager がマルチドメイン設定されている場合。

分散 Check Point 展開からのエクスポート

Check Point 設定を抽出するには、Cisco Secure Firewall 移行ツールの Live Connect を使用する前に、Check Point（r80）デバイスでログイン情報を構成する必要があります。

分散 Check Point 展開でのログイン情報事前設定手順には、次のステップが含まれます。

ステップ 1 Gaia Console Check Point Security Gateway で、次を作成します。

a) Web ブラウザで、HTTPS セッション経由で Check Point Gaia Console アプリケーションを開き、Check Point Security Gateway に接続します。

b) [ユーザー管理（User Management）] タブに移動し、**[ユーザー（Users）]** > **[追加（Add）]**を選択します。

c) [ユーザの追加（Add User）] ウィンドウで、次の詳細を使用して新しいユーザ名とパスワードを作成します。

- [シェル（Shell）] ドロップダウンから、*/etc/cli.sh* を選択します。
- [利用可能なロール（Available Roles）] から、*adminRole* を選択します。
- 残りのフィールドはデフォルト値のままにします。

- [OK] をクリックします。

d) Check Point Security Gateway に SSH 接続し、次のコマンドを使用して新しいパスワードを作成します。
set expert-password <password>

（注）
- Check Point デバイスでエキスパートパスワードをすでに設定している場合は、それを再利用します。
- 手順 3 に示すように、[Check Point Security Gateway に接続（Connect to Check Point Security Gateway）] ページでこれらのログイン情報が必要となります。

エキスパートパスワードを構成したら、Check Point r80 Gateway でのログイン情報の事前設定が完了します。

詳細については、図 3 : Check Point Security Gateway への接続 を参照してください。

ステップ 2 r80 の Check Point Security Manager でユーザ名とパスワードを作成します。

a) SmartConsole アプリケーションで、次の手順を実行します。

1. Check Point Security Manager にログインします。
2. **[Manage and Settings]** > **[Permissions and Administrators]** > **[Administrators]**に移動します。
3. ***** をクリックして新しいユーザ名とパスワードを作成し、次の手順を実行します。
   - [認証方式（Authentication Method）] に [Check Point パスワード（Check Point Password）] を選択します。
   - [Set New Password] をクリックして、新しいパスワードを設定します。

     （注） [ユーザは次回ログイン時にパスワードの変更が必要（User Must Change Password on the Next Login）] チェックボックスはオンにしないでください。

   - [権限プロファイル（Permission Profile）] に [スーパーユーザ（Super User）] を選択します。
   - [有効期限（Expiration）] に [なし（Never）] を選択します。
4. [パブリッシュ（Publish）] をクリックして、Check Point SmartConsole アプリケーションの構成変更を保存します。

b) Check Point Security Manager の Gaia Console で、次の手順を実行します。

（注） ここで作成するユーザ名とパスワードは、ステップ 2a で SmartConsole アプリケーションで作成したものと同じであること確認してください。

1. Web ブラウザで、HTTPS セッション経由で Gaia Console アプリケーションを開き、Check Point Security Manager に接続します。
2. [User Management] タブに移動し、**[Users]** > **[Add]**を選択します。

3. SmartConsole アプリケーションのステップ 2a（3）で作成したものと同じユーザ名とパスワードを作成します。
   - [シェル（Shell）] ドロップダウンから、*/bin/bash* を選択します。
   - [利用可能なロール（Available Roles）] ドロップダウンから、*adminRole* を選択します。
   - 残りのフィールドはデフォルト値のままにします。
   - [OK] をクリックします。
4. Check Point Security Manager に SSH 接続し、次のコマンドを使用してエキスパートパスワードを作成します。

   set expert-password <password>

   （注）
   - エキスパートパスワードをすでに設定している場合は、そのパスワードを使用できます。
   - ステップ 2b（3）とステップ 2a（3） で作成したユーザ名とパスワードは同じである必要があります。

分散展開の Check Point での、Check Point Security Manager のログイン情報の事前設定が完了しました。

手順 4 に示すように、[Check Point Security Manager に接続（Connect to Check Point Security Manager）] ページでこれらのログイン情報が必要となります。

Check Point Smart Manager でカスタム API ポートを使用している場合は、「Check Point（r80）Security Manager にカスタム API ポートを使用しますか。」を参照してください。

次のタスク

r80 の Check Point 構成ファイルをエクスポートする手順

スタンドアロン Check Point 展開からのエクスポート

Check Point 設定を抽出するには、Cisco Secure Firewall 移行ツールの Live Connect を使用する前に、Check Point（r80）デバイスでログイン情報を構成する必要があります。

スタンドアロン Check Point 展開でのログイン情報事前設定手順には、次のステップが含まれます。

ステップ 1 Web ブラウザで、Gaia Console アプリケーションを開き、Check Point Security Gateway と Check Point Security Manager の両方を管理するスタンドアロン Check Point デバイスに接続します。

ステップ 2 [ユーザー管理（User Management）] タブに移動し、**[ユーザー（Users）] > [追加（Add）]**を選択します。

a) [ユーザの追加（Add User）] ウィンドウで、次の詳細を使用して新しいユーザ名とパスワードを作成します。

- [シェル（Shell）] ドロップダウンから、*/etc/cli.sh* を選択します。
- [利用可能なロール（Available Roles）] ドロップダウンから、*adminRole* を選択します。
- 残りのフィールドはデフォルト値のままにします。
- [OK] をクリックします。

手順 3 に示すように、[Check Point Security Gateway に接続（Connect to Check Point Security Gateway）] ページでこれらのログイン情報が必要となります。

詳細については、図 3 : Check Point Security Gateway への接続 を参照してください。

b) [ユーザの追加（Add User）] ウィンドウで、次の詳細を使用して別のユーザ名とパスワードを作成します。

- [シェル（Shell）] ドロップダウンから、*/bin/bash* を選択します。
- [利用可能なロール（Available Roles）] ドロップダウンから、*adminRole* を選択します。
- 残りのフィールドはデフォルト値のままにします。
- [OK] をクリックします。

ステップ 3 Check Point デバイス上の r80 用 SmartConsole アプリケーションで、次を作成します。

（注） ここで作成するユーザ名とパスワードは、前のステップで Check Point Gaia Console で作成したものと同じであること確認してください。

a) Check Point デバイスの SmartConsole アプリケーションにログインします。
b) **[Manage and Settings]** > **[Permissions and Administrators]** > **[Administrators]**に移動します。
c) ***** をクリックして、次の詳細を使用して新しいユーザ名とパスワードを作成します。

- [認証方式（Authentication Method）] に [Check Point パスワード（Check Point Password）] を選択します。
- [Set New Password] をクリックして、新しいパスワードを設定します。

（注） [ユーザは次回ログイン時にパスワードの変更が必要（User Must Change Password on the Next Login）] チェックボックスはオンにしないでください。

- [権限プロファイル（Permission Profile）] に[スーパーユーザ（Super User）] を選択します。
- [有効期限（Expiration）] に [なし（Never）] を選択します。

ステップ 2 のステップ b とステップ 3 のステップ c で作成したユーザ名とパスワードは同じである必要があります。

手順 4 に示すように、[Check Point Security Manager に接続（Connect to Check Point Security Manager）] ページでこれらのログイン情報が必要となります。

d) [パブリッシュ（Publish）] をクリックして、Check Point SmartConsole アプリケーションの構成変更を保存します。

ステップ 4 Check Point デバイスに SSH 接続し、次のコマンドを使用してエキスパートパスワードを作成します。
set expert-password <password>

（注）
- Check Point デバイスでエキスパートパスワードをすでに設定している場合は、それを再利用します。
- ステップ 2 のステップ b とステップ 3 のステップ c で作成したユーザ名とパスワードは同じである必要があります。

スタンドアロン展開の Check Point デバイスでのログイン情報の事前設定が完了しました。

Check Point Smart Manager でカスタム API ポートを使用している場合は、「Check Point（r80）Security Manager にカスタム API ポートを使用しますか。」を参照してください。

次のタスク

r80 の Check Point 構成ファイルをエクスポートする手順

マルチドメイン Check Point 展開からのエクスポート

Check Point 設定を抽出するには、Cisco Secure Firewall 移行ツールの Live Connect を使用して、Check Point（r80）デバイスでログイン情報を構成する必要があります。

マルチドメイン Check Point 展開でのログイン情報事前設定手順には、次のステップが含まれます。

ステップ 1 Gaia Console Check Point Security Gateway で、次を作成します。

a) Web ブラウザで、HTTPS セッション経由で Gaia Console アプリケーションを開き、Check Point Security Gateway に接続します。

b) [User Management] タブに移動し、**[Users]** > **[Add]**を選択します。

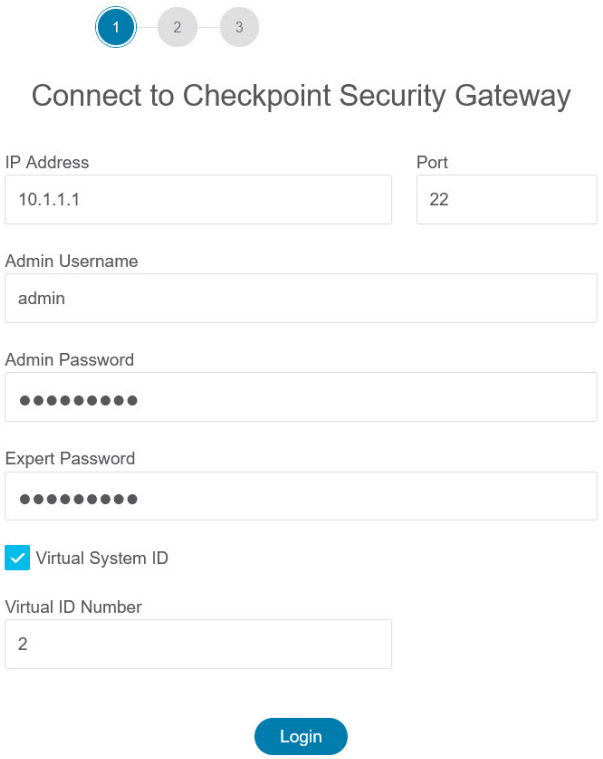
c) [ユーザの追加（Add User）] ウィンドウで、次の詳細を使用して新しいユーザ名とパスワードを作成します。
- [シェル（Shell）] ドロップダウンから、*/etc/cli.sh* を選択します。
- [利用可能なロール（Available Roles）] ドロップダウンから、*adminRole* を選択します。
- 残りのフィールドはデフォルト値のままにします。
- [OK] をクリックします。

d) Check Point Security Gateway に SSH 接続し、次のコマンドを使用して新しいパスワードを作成します。
set expert-password <password>

Check Point Security Gateway でのマルチドメイン展開用のログイン情報の事前設定が完了しました。

e) （任意） Virtual System Extension（VSX）デバイスから構成をエクスポートする場合、[仮想システム ID（Virtual System ID）] チェックボックスをオンにして、仮想システム ID を入力できるようにします。

図 *1 : Checkpoint Security Gateway* への接続：マルチドメイン展開



ステップ 2 Check Point Security Manager でユーザ名とパスワードを作成します。

a) SmartConsole（mds）アプリケーションで、次の手順を実行します。

1. Check Point Security Manager にログインします。
2. **[Manage and Settings]** > **[Permissions and Administrators]** > **[Administrators]**に移動します。
3. ***** をクリックして、次の詳細を使用して新しいユーザ名とパスワードを作成します。
   - [認証方式（Authentication Method）] に [Check Point パスワード（Check Point Password）] を選択します。
   - [Set New Password] をクリックして、新しいパスワードを設定します。

     （注） [ユーザは次回ログイン時にパスワードの変更が必要（User Must Change Password on the Next Login）] チェックボックスはオンにしないでください。

   - [権限プロファイル（Permission Profile）] に[マルチドメインスーパーユーザ（Multi-domain Super User）] を選択します。
   - [有効期限（Expiration）] に [なし（Never）] を選択します。

4. [パブリッシュ（Publish）]をクリックして、Check Point SmartConsole アプリケーションの構成変更を保存します。

   Check Point Smart Manager でカスタム API ポートを使用している場合は、「Check Point（r80）Security Manager にカスタム API ポートを使用しますか。」を参照してください。

b) Check Point Security Manager の Gaia Console で、次の手順を実行します。

（注） ここで作成するユーザ名とパスワードは、ステップ 2a（3） で SmartConsole アプリケーションで作成したものと同じであること確認してください。

1. Web ブラウザで、HTTPS セッション経由で Gaia Console アプリケーションを開き、Check Point Security Manager に接続します。
2. [User Management] タブに移動し、**[Users]** > **[Add]**を選択します。
3. ステップ 2a（3） で SmartConsole アプリケーションで作成したものと同じユーザ名とパスワードを作成します。
   - [シェル（Shell）] ドロップダウンから、*/bin/bash* を選択します。
   - [利用可能なロール（Available Roles）] ドロップダウンから、*adminRole* を選択します。
   - 残りのフィールドはデフォルト値のままにします。
   - [OK] をクリックします。
4. Check Point Security Manager に SSH 接続し、次のコマンドを使用して新しいパスワードを作成します。

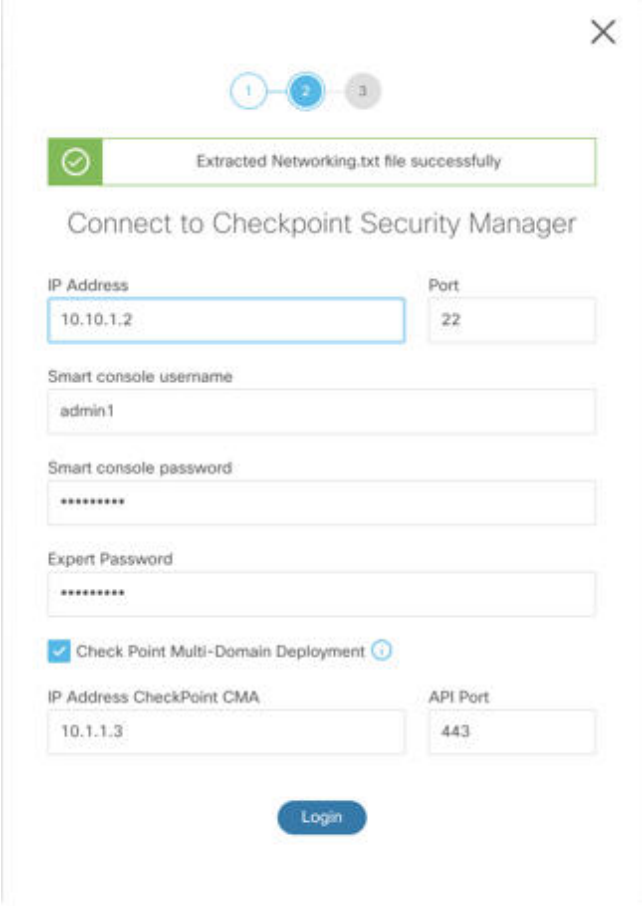
   set expert-password <password>

（注）
- Check Point デバイスでエキスパートパスワードをすでに設定している場合は、それを再利用します。
- ステップ 2a（3） とステップ 2b（3） で作成したユーザ名とパスワードは同じである必要があります。

マルチドメイン展開の Check Point Security Manager でのログイン情報の事前設定が完了しました。

Live Connectに接続するには、図 2 : Checkpoint Security Manager への接続：マルチドメイン展開のようにログイン情報が必要です。

図 *2 : Checkpoint Security Manager* への接続：マルチドメイン展開



（注）

- Check Point Smart Manager でカスタム API ポートを使用している場合は、「Check Point（r80）Security Manager にカスタム API ポートを使用しますか。」を参照してください。
- マルチドメイン展開用のグローバル ポリシー パッケージは取得できません。したがって、Check Point CMA の構成の一部として構成されたオブジェクト、ACE ルール、および NAT ルールは、エクスポートおよび移行のみ行われます。

次のタスク

r80 の Check Point 構成ファイルをエクスポートする手順

Check Point（r80）Security Manager にカスタム API ポートを使用しますか。

（注） Check Point Smart Manager でカスタム API ポートを使用している場合は、次の手順を実行します。

- [Check Point Security Manager] ページの [Check Point マルチドメイン展開（Check Point Multi-domain Deployment）] チェックボックスをオンにします。
- マルチドメイン展開を使用している場合は、Check Point CMA のIP アドレスと API ポートの詳細を追加します。
- 一般的な展開の Check Point Security Manager の場合、Check Point Security Manager の IP アドレスを保持し、カスタム API ポートの詳細を入力します。

r80 の Check Point 構成ファイルをエクスポートする手順

始める前に

Check Point デバイスで以下を事前設定する必要があります。移行前に Check Point（r80）デバイスでログイン情報を構成する詳細については、「Live Connect を使用した構成抽出のための Check Point（r80）デバイスの事前設定」を参照してください。

（注）
- Live Connect を使用して Check Point（r80）構成を抽出することを推奨します。
- Cisco Secure Firewall 移行ツールで構成されていない Check Point（r80）構成を使用すると、構成がサポート対象外として移行されたり、部分的に移行されたり、移行が失敗したりします。

  構成のエクスポートの情報が不完全な場合、特定の構成は移行されず、**サポート対象外**としてマークされます。

r80 の Check Point 構成ファイルをエクスポートするには、次の手順を実行します。

ステップ 1 [Select Source Config] ページから [Check Point (r80)] を選択します。

ステップ 2 [接続（Connect）] をクリックします。

（注） Live Connect は、Check Point（r80）でのみ使用できます。

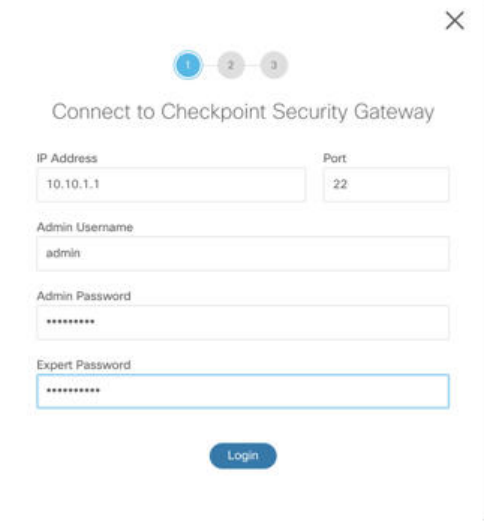
ステップ 3 Check Point Security Gateway に接続します。次の手順を実行します。

a) Check Point r80 Security Gateway に次のように入力します。

- IP アドレス
- SSH ポート

- Admin Username
- Admin Password
- エキスパートパスワード

図 *3 : Check Point Security Gateway* への接続



b) [ログイン（Login）] をクリックします。

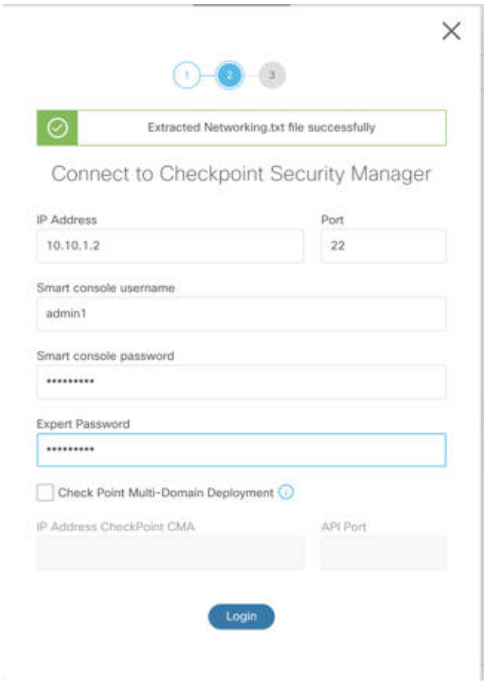
Cisco Secure Firewall 移行ツールは、インターフェイス構成やルート構成などのデバイス固有の構成を含む *networking.txt* ファイルを生成します。Cisco Secure Firewall 移行ツールの現在のセッションのローカルディレクトリに *networking.txt* ファイルを保存します。

ステップ 4 Check Point Security Manager に接続します。次の手順を実行します。

a) Check Point r80 Security Manager に次のように入力します。

- IP アドレス
- SSH ポート
- スマートコンソールのユーザ名
- スマートコンソールのパスワード
- エキスパートパスワード

図 *4 : Check Point Security Manager* への接続



b) [ログイン（Login）] をクリックします。

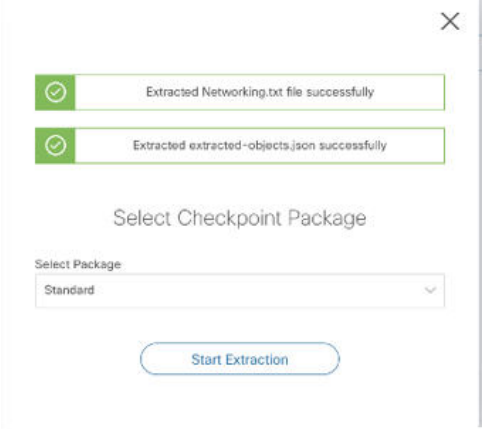
Cisco Secure Firewall 移行ツールは、Check Point Security Manager で使用可能な完全なネットワークおよびサービスオブジェクト構成をキャプチャする *Extracted-objects.json* ファイルを生成します。

Cisco Secure Firewall 移行ツールの現在のセッションのローカルディレクトリに *Extracted-objects.json* ファイルを保存します。

（注） Cisco Secure Firewall 移行ツールを Check Point Security Manager に接続している場合は、Check Point Security Manager で使用可能なポリシーパッケージのリストが表示されます。

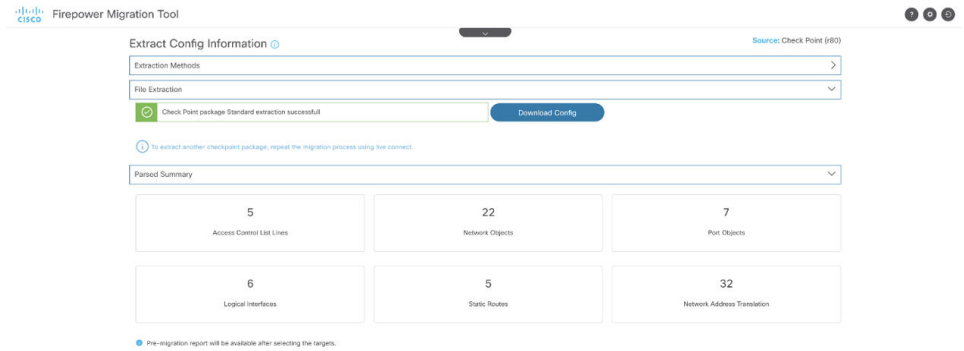
ステップ 5 [Select Check Point Package] リストから移行する Check Point ポリシーパッケージを選択し、[Start Extraction] をクリックします。

図 *5 : Check Point* ポリシーパッケージの抽出



ステップ 6 構成をダウンロードし、移行を続行します。

図 *6 :* 分散展開およびスタンドアロン展開の完全な *Check Point* 構成の抽出



ステップ 7 [次へ（Next）] をクリックして、Check Point（r80）構成の移行を続行します。

次のタスク

Check Point 構成ファイルのアップロード

別の構成ファイルの取得

別の構成ファイルを取得するには、次の手順を実行します。

- 別のポリシーパッケージの新しい構成を取得するか、別の Check Point（r80）ファイアウォールに接続するには、[送信元の選択に戻る（Back to source selection）] をクリックします。
- 取得した Check Point（r80）構成を後で移行する必要がある場合は、現在の構成をダウンロードします。

（注） 現在の構成ファイルは、ブラウザで設定されているデフォルトのダウンロード場所にダウンロードされます。

組立てラインアプローチを使用して、r80 構成を取得できます。

- Live Connect を実行して、ファイアウォールの各パッケージまたはさまざまなファイアウォールの Check Point（r80）構成ファイルを取得します。
- 複数の構成のリポジトリを作成します。
- 後で手動アップロードを使用して移行を続行するには、[後で移行を開始（Start Migration later）] オプションを使用します。

Check Point 構成ファイルのアップロード

始める前に

構成ファイルを .zip 形式でエクスポートします。

ステップ 1 [Extract Config Information] 画面の [Manual Upload] セクションで、[Upload] をクリックして Check Point 構成ファイルをアップロードします。

ステップ 2 構成ファイルが保存されている場所を参照します。Check Point（r77）の構成ファイルが抽出され、Check Point（r80）の Live Connect を使用してダウンロードされます。[開く（Open）] をクリックします。

Cisco Secure Firewall 移行ツールが構成ファイルをアップロードします。大規模な構成ファイルの場合、この手順には時間がかかります。

これで、解析前プロセスが完了しました。

[解析サマリー（Parsed Summary）] セクションに解析ステータスが表示されます。

ステップ 3 アップロードされた構成ファイルで、Cisco Secure Firewall 移行ツールが検出して解析した要素の概要を確認します。

ステップ 4 [次へ（Next）] をクリックして、ターゲットパラメータを選択します。

次のタスク

Cisco Secure Firewall 移行ツールの接続先パラメータの指定

Cisco Secure Firewall 移行ツールの接続先パラメータの指定

始める前に

CDO でホストされるクラウドバージョンの移行ツールを使用している場合は、ステップ 3 に進んでください。

- オンプレミス Firewall Management Center の Management Center の IP アドレスを取得します。
- Cisco Secure Firewall 移行ツール 3.0 以降では、オンプレミスの Firewall Management Center またはクラウド提供型 Firewall Management Center を選択できます。
- クラウド提供型 Firewall Management Center の場合、リージョンと API トークンを指定する必要があります。詳細については、「サポートされる移行先の管理センター」を参照してください。
- （任意）インターフェイスやルートなどのデバイス固有の構成を移行する場合は、ターゲット 脅威に対する防御 を Management Center に追加します。「Adding Devices to the Firewall Management Center」を参照してください。
- [確認と検証（Review and Validate）] ページで IPS またはファイルポリシーを ACL に適用する必要がある場合は、移行前に Management Center でポリシーを作成することを強くお勧めします。Cisco Secure Firewall 移行ツールは接続された Management Center からポリシーを取得するため、同じポリシーを使用します。新しいポリシーを作成して複数のアクセス制御リストに割り当てると、パフォーマンスが低下し、プッシュが失敗する可能性があります。

ステップ 1 [ターゲットの選択（Select Target）] 画面の [ファイアウォール管理（Firewall Management）] セクションで、次の手順を実行します。オンプレミスのファイアウォール管理センターまたはクラウド提供型ファイアウォール管理センターへの移行を選択できます。

- オンプレミスのファイアウォール管理センターに移行するには、次の手順を実行します。

a) [オンプレミス FMC（On-Prem FMC）] オプションボタンをクリックします。
b) 管理センターの IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。
c) [Domain] ドロップダウンリストで、移行先のドメインを選択します。

脅威に対する防御 デバイスに移行する場合は、選択したドメインで使用可能な 脅威に対する防御 デバイスにのみ移行できます。

d) [接続（Connect）] をクリックして、**手順 2** に進みます。

- クラウド提供型 Firewall Management Center に移行するには、次の手順を実行します。

a) [クラウド提供型 FMC（Cloud-delivered FMC）] オプションボタンをクリックします。
b) リージョンを選択し、CDO API トークンを貼り付けます。CDO から API トークンを生成するため、以下の手順に従います。

1. CDO ポータルにログインします。
2. **[設定（Settings）]** > **[全般設定（General Settings）]** に移動して、API トークンをコピーします。

c) [接続（Connect）] をクリックして、**手順 2** に進みます。

ステップ 2 [Firewall Management Centerへのログイン（Firewall Management Center Login）] ダイアログボックスで、Cisco Secure Firewall 移行ツール専用アカウントのユーザー名とパスワードを入力し、[ログイン（Login）] をクリックします。

Cisco Secure Firewall 移行ツールは Management Center にログインし、その Management Center による管理対象 脅威に対する防御デバイスのリストを取得します。この手順の進行状況はコンソールで確認できます。

ステップ 3 [続行（Proceed）] をクリックします。

ステップ 4 [Threat Defense の選択（Choose Threat Defense）] セクションで、次のいずれかを実行します。

- [Firewall Threat Defenseデバイスの選択（Select Firewall Threat Defense Device）] ドロップダウンリストをクリックし、 チェックポイント 構成を移行するデバイスをオンにします。

  選択した Management Center ドメイン内のデバイスが、**IP アドレス**と**名前**でリストされます。

  （注） 少なくとも、選択するネイティブ 脅威に対する防御デバイスには、移行する チェックポイント 構成と同じ数の物理インターフェイスまたはポートチャネルインターフェイスが必要です。少なくとも、脅威に対する防御 デバイスのコンテナインスタンスには、同じ数の物理インターフェイスまたはポートチャネルインターフェイスとサブインターフェイスが必要です。チェックポイント 構成と同じファイアウォールモードでデバイスを構成する必要があります。ただし、これらのインターフェイスは、両方のデバイスで同じ名前である必要はありません。

  （注） サポートされているターゲット Threat Defense プラットフォームが、管理センターバージョン 6.5 以降を備えた Firewall 1010である場合にのみ、FDM 5505 移行サポートは共有ポリシーに適用され、デバイス固有のポリシーには適用されません。Threat Defense なしで続行すると、Cisco Secure Firewall 移行ツールは構成またはポリシーを Threat Defense にプッシュしません。したがって、Threat Defense のデバイス固有の構成であるインターフェイスとルート、およびサイト間 VPN は移行されません。ただし、NAT、ACL、ポートオブジェクトなど、サポートされている他のすべての構成（共有ポリシーとオブジェクト）は移行されます。リモートアクセス VPN は共有ポリシーであり、Threat Defense なしでも移行できます。

  リモート展開が有効になっている Management Center または 脅威に対する防御 6.7 以降への Check Point ファイアウォールの移行は、Cisco Secure Firewall 移行ツールでサポートされています。インターフェイスとルートの移行は手動で行う必要があります。

- [Threat Defense を使用せず続行（Proceed without Threat Defense）] をクリックして、構成を Management Center に移行します。

  脅威に対する防御 なしで続行すると、Cisco Secure Firewall 移行ツールは 脅威に対する防御 に構成またはポリシーをプッシュしません。したがって、脅威に対する防御 のデバイス固有の構成であるインターフェイスとルート、およびサイト間 VPN は移行されません。ただし、NAT、ACL、ポート

オブジェクトなど、サポートされている他のすべての構成（共有ポリシーとオブジェクト）は移行されます。リモートアクセス VPN は共有ポリシーであり、Threat Defense なしでも移行できます。

ステップ 5 [続行（Proceed）] をクリックします。

移行先に応じて、Cisco Secure Firewall 移行ツールを使用して移行する機能を選択できます。

ステップ 6 [機能の選択（Select Features）] セクションをクリックして、移行先に移行する機能を確認して選択します。

- 接続先 脅威に対する防御 デバイスに移行する場合、Cisco Secure Firewall 移行ツールは、[デバイスの構成（Device Configuration）] セクションと [共有構成（Shared Configuration）] セクションで、チェックポイント 構成から移行できる機能を自動的に選択します。要件に応じて、デフォルトの選択をさらに変更できます。
- Management Center に移行する場合、Cisco Secure Firewall 移行ツールは、[共有構成（Shared Configuration）] セクションで、チェックポイント 構成から移行できる機能を自動的に選択します。要件に応じて、デフォルトの選択をさらに変更できます。

  （注） [デバイスの構成（Device Configuration）] セクションは、移行先 脅威に対する防御 デバイスを選択していない場合は使用できません。

  （注） [Firepower Device Managerの移行（共有構成のみ）（Migrate Firepower Device Manager (Shared Configurations Only)）] を選択した場合、[デバイスの構成（Device Configuration）] セクションは使用できません。

- Check Point の場合は、[Shared Configuration] で、関連する [Access Control] オプションを選択します。
  - グローバルポリシー：このオプションを選択すると、ACL ポリシーの送信元ゾーンと宛先ゾーンが**任意**のものとして移行されます。
  - ゾーンベースポリシー：このオプションを選択すると、送信元ゾーンと宛先ゾーンは、送信元と宛先のネットワークオブジェクトまたはグループのルーティングメカニズムによる予測ルートルックアップに基づいて導出されます。

    （注） ルートルックアップは静的ルートと動的ルート（PBR と NAT は考慮されません）に限定され、送信元と宛先のネットワーク オブジェクト グループの性質によっては、この操作によりルールが急増する可能性があります。

    ルーティング情報は、`networking.txt` ファイルから取得されます。このファイルは、**netstat -rnv** コマンドを使用してルーティングテーブルを収集する FMT-CP-Config-Extractor_v4.0.1-8248 ツールの出力です。詳細については、「FMT-CP-Config-Extractor_v4.0.1-8248 ツールを使用したデバイス構成のエクスポート」を参照してください。

    このリリースでは、ゾーンベースポリシーの IPv6 ルートルックアップはサポートされていません。グローバルポリシーまたはゾーンベースポリシーのすべてのルールが正常に移行されていることを確認します。

- Cisco Secure Firewall 移行ツールは、ターゲット管理センターが 7.2 以降の場合はリモートアクセス VPN の移行をサポートします。リモートアクセス VPN は、Threat Defense なしで移行できる共有ポ

リシーです。Threat Defense を使用する移行を選択した場合、Threat Defense のバージョンは 7.0 以降である必要があります。

- （任意）[Optimization] セクションで、[Migrate only referenced objects] を選択して、アクセス コントロール ポリシーと NAT ポリシーで参照されているオブジェクトのみを移行します。

  （注） このオプションを選択すると、チェックポイント構成内の参照されていないオブジェクトは移行されません。これにより、移行時間が最適化され、未使用のオブジェクトが構成から消去されます。

ステップ 7 [続行（Proceed）] をクリックします。

ステップ 8 [Rule Conversion/ Process Config] セクションで、[Start Conversion] をクリックして変換を開始します。

ステップ 9 Cisco Secure Firewall 移行ツールによって変換された要素の概要を確認します。

構成ファイルが正常にアップロードおよび解析されたかどうかを確認するには、移行を続行する前に**移行前レポート**をダウンロードして確認します。

ステップ 10 [レポートのダウンロード（Download Report）] をクリックし、**移行前レポート**を保存します。

移行前レポートのコピーも、Cisco Secure Firewall 移行ツールと同じ場所にある `Resources` フォルダに保存されます。

次のタスク

移行前レポートの確認 （27 ページ）

移行前レポートの確認

ステップ 1 移行前レポートをダウンロードした場所に移動します。

移行前レポートのコピーも、Cisco Secure Firewall 移行ツールと同じ場所にある `Resources` フォルダに保存されます。

ステップ 2 移行前レポートを開き、その内容を慎重に確認して、移行が失敗する原因となる問題を特定します。

移行前レポートには、次の情報が含まれています。

- [移行の概要（Migration Summary）]：Firepower Threat Defense に正常に移行できる、サポートされる Check Point 構成要素の全体的な概要。たとえば、ポリシー名、ルール数などです。
- [解析エラーの詳細（Parse Error Details）]：解析エラーの原因となった構成を強調表示します。こうすることで、構成を編集および更新して再試行しやすくなります。
- [サポートされない構成（Unsupported Configuration）]：FMT による移行がサポートされていないすべての構成アイテムの詳細なリスト。たとえば、ループバック、エイリアスインターフェイス、ドメインオブジェクトなどです。

- [部分的なサポート構成（Partially Supported Configuration）]：部分的にのみ移行可能なすべての Check Point 構成要素のリスト。たとえば、Ping パラメータを使用した静的ルートなどです。
- [スキップされる構成（Skipped Configuration）]：移行中に FMT によって無視され、ターゲットシステムに転送されないすべての Check Point 構成要素のリスト。

Management Center および 脅威に対する防御 でサポートされる機能の詳細については、『Firepower Management Center Configuration Guide』を参照してください。

ステップ 3 **移行前レポート**で修正措置が推奨されている場合は、Check Point で修正を完了し、Check Point 構成ファイルを再度エクスポートしてから、更新された構成ファイルをアップロードし、続行してください。

ステップ 4 Check Point 構成ファイルが正常にアップロードおよび解析されたら、Cisco Secure Firewall 移行ツールに戻り、[次へ（Next）] をクリックして移行を続行します。

チェックポイント 構成と Secure Firewall Device Manager Threat Defense インターフェイスのマッピング

脅威に対する防御 デバイスには、チェックポイント 構成で使用されている数以上の物理インターフェイスとポートチャネルインターフェイスが必要です。これらのインターフェイスは、両方のデバイスで同じ名前である必要はありません。インターフェイスのマッピング方法を選択できます。

[Threat Defenseインターフェイスのマップ（Map Threat Defense Interface）] 画面で、脅威に対する防御 デバイス上のインターフェイスのリストを取得します。デフォルトでは、Cisco Secure Firewall 移行ツールは チェックポイントのインターフェイスと 脅威に対する防御 デバイスをインターフェイス ID に従ってマッピングします。たとえば、チェックポイントインターフェイスの「管理専用」インターフェイスは、脅威に対する防御デバイスの「管理専用」インターフェイスに自動的にマッピングされ、変更できません。

チェックポイント インターフェイスから 脅威に対する防御 インターフェイスへのマッピングは、脅威に対する防御 デバイスタイプによって異なります。

- ターゲット 脅威に対する防御 がネイティブタイプの場合は次のようになります。
  - 脅威に対する防御 には、使用する チェックポイント インターフェイスまたはポートチャネル（PC）データインターフェイスが同数以上必要です（チェックポイント 構成の管理専用とサブインターフェイスを除く）。同数未満の場合は、ターゲット 脅威に対する防御 に必要なタイプのインターフェイスを追加します。
  - サブインターフェイスは、物理インターフェイスまたはポートチャネルマッピングに基づいて Cisco Secure Firewall 移行ツールによって作成されます。
- ターゲット 脅威に対する防御 がコンテナタイプの場合は次のようになります。
  - 脅威に対する防御 には、使用する チェックポイント インターフェイス、物理サブインターフェイス、ポートチャネル、またはポート チャネル サブインターフェイスが同数以上必要です（チェックポイント構成の管理専用を除く）。同数未満の場合は、

ターゲット 脅威に対する防御 に必要なタイプのインターフェイスを追加します。たとえば、ターゲット脅威に対する防御 の物理インターフェイスと物理サブインターフェイスの数が チェックポイント での数より 100 少ない場合、ターゲット 脅威に対する防御 に追加の物理または物理サブインターフェイスを作成できます。

- サブインターフェイスは、Cisco Secure Firewall 移行ツールでは作成されません。物理インターフェイス、ポートチャネル、またはサブインターフェイス間のインターフェイスマッピングのみが許可されます。

始める前に

Management Center に接続し、接続先として 脅威に対する防御 を選択していることを確認します。詳細については、「Cisco Secure Firewall 移行ツールの接続先パラメータの指定 （24 ページ）」を参照してください。

（注） 脅威に対する防御 デバイスなしで Management Center に移行する場合、この手順は適用されません。

ステップ 1 インターフェイスマッピングを変更する場合は、[Threat Defenseインターフェイス名（Threat Defense Interface Name）]のドロップダウンリストをクリックし、そのチェックポイントインターフェイスにマッピングするインターフェイスを選択します。

管理インターフェイスのマッピングは変更できません。脅威に対する防御インターフェイスがすでにチェックポイントインターフェイスに割り当てられている場合は、ドロップダウンリストからそのインターフェイスを選択できません。割り当て済みのすべてのインターフェイスはグレー表示され、使用できません。

サブインターフェイスをマッピングする必要はありません。Cisco Secure Firewall 移行ツールは、チェックポイント構成内のすべてのサブインターフェイスについて 脅威に対する防御デバイスのサブインターフェイスをマッピングします。

ステップ 2 各 チェックポイント インターフェイスを 脅威に対する防御 インターフェイスにマッピングしたら、[次へ（Next）] をクリックします。

次のタスク

チェックポイント インターフェイスを適切な 脅威に対する防御 インターフェイスオブジェクト、セキュリティゾーン、およびインターフェイスグループにマッピングします。詳細については、「セキュリティゾーンとインターフェイスグループへのチェックポイントインターフェイスのマッピング」を参照してください。

セキュリティゾーンとインターフェイスグループへのチェックポイント インターフェイスのマッピング

チェックポイント 構成が正しく移行されるように、チェックポイント インターフェイスを適切な脅威に対する防御インターフェイス オブジェクト、セキュリティゾーン、およびインターフェイスグループにマッピングします。 チェックポイント 構成では、アクセス コントロール ポリシーと NAT ポリシーはインターフェイス名（nameif）を使用します。Management Center では、これらのポリシーはインターフェイス オブジェクトを使用します。さらに、Management Center ポリシーはインターフェイス オブジェクトを次のようにグループ化します。

- セキュリティ ゾーン：インターフェイスは、1 つのセキュリティ ゾーンにのみ属することができます。
- インターフェイスグループ：インターフェイスは複数のインターフェイスグループに属することができます。

Cisco Secure Firewall 移行ツールでは、セキュリティゾーンおよびインターフェイスグループとインターフェイスを 1 対 1 でマッピングできます。セキュリティゾーンまたはインターフェイスグループがインターフェイスにマッピングされている場合、他のインターフェイスへのマッピングには使用できませんが、Management Center では許可されます。Management Center のセキュリティゾーンとインターフェイスグループの詳細については、「Interface Objects: Interface Groups and Security Zones」[英語] を参照してください。

ステップ 1 [セキュリティゾーンとインターフェイスグループへのマッピング（Map Security Zones and Interface Groups）] 画面で、使用可能なインターフェイス、セキュリティゾーン、およびインターフェイスグループを確認します。

ステップ 2 セキュリティゾーンおよびインターフェイスグループが Management Center に存在する場合、またはセキュリティ ゾーン タイプ オブジェクトとして 構成ファイルに存在し、ドロップダウンリストで使用可能な場合、これらにインターフェイスをマッピングするには、次の手順を実行します。

a) [セキュリティゾーン（Security Zones）] 列で、そのインターフェイスのセキュリティゾーンを選択します。

b) [インターフェイスグループ（Interface Groups）] 列で、そのインターフェイスのインターフェイスグループを選択します。

ステップ 3 セキュリティゾーンおよびインターフェイスグループが Management Center に存在する場合、またはセキュリティ ゾーン タイプ オブジェクトとして Check Point（r80）構成ファイルに存在し、ドロップダウンリストで使用可能な場合、これらにインターフェイスをマッピングするには、次の手順を実行します。

a) [セキュリティゾーン（Security Zones）] 列で、そのインターフェイスのセキュリティゾーンを選択します。

b) [インターフェイスグループ（Interface Groups）] 列で、そのインターフェイスのインターフェイスグループを選択します。

ステップ 4 セキュリティゾーンとインターフェイスグループは、手動でマッピングすることも自動で作成することもできます。

ステップ 5 セキュリティゾーンとインターフェイスグループを手動でマッピングするには、次の手順を実行します。

a) [セキュリティゾーンとインターフェイスグループの追加（Add SZ & IG）] をクリックします。
b) [セキュリティゾーンとインターフェイスグループの追加（Add SZ & IG）] ダイアログボックスで、[追加（Add）] をクリックして新しいセキュリティゾーンまたはインターフェイスグループを追加します。
c) [セキュリティゾーン（Security Zone）] 列にセキュリティゾーン名を入力します。使用できる最大文字数は 48 です。同様に、インターフェイスグループを追加できます。
d) [閉じる（Close）] をクリックします。

セキュリティゾーンとインターフェイスグループを自動作成によってマッピングするには、次の手順を実行します。

a) [自動作成（Auto-Create）] をクリックします。
b) [自動作成（Auto-Create）] ダイアログボックスで、[インターフェイスグループ（Interface Groups）] または [ゾーンマッピング（Zone Mapping）] のいずれかまたは両方をオンにします。
c) [自動作成（Auto-Create）] をクリックします。

Cisco Secure Firewall 移行ツールは、これらのセキュリティゾーンに Check Point インターフェイスと同じ名前（**outside** や **inside** など）を付け、名前の後に "(A)" を表示して、Cisco Secure Firewall 移行ツールによって作成されたことを示します。インターフェイスグループには、**outside_ig** や **inside_ig** などの `_ig` サフィックスが追加されます。また、セキュリティゾーンとインターフェイスグループには、Check Point インターフェイスと同じモードがあります。たとえば、Check Point 論理インターフェイスが L3 モードの場合、そのインターフェイス用に作成されたセキュリティゾーンとインターフェイスグループも L3 モードになります。

ステップ 6 すべてのインターフェイスを適切なセキュリティゾーンとインターフェイスグループにマッピングしたら、[次へ（Next）] をクリックします。

最適化、 構成の確認と検証

移行した チェックポイント 構成を Management Center にプッシュする前に、構成を慎重に確認し、それが適切で 脅威に対する防御 デバイスの構成内容と一致することを確認します。点滅しているタブは、次の一連のアクションを実行する必要があることを示しています。

（注） [構成の最適化、確認および検証（Optimize, Review and Validate Configuration）] 画面で Cisco Secure Firewall 移行ツールを閉じると、進行状況が保存され、後で移行を再開できます。この画面の前に Cisco Secure Firewall 移行ツールを閉じると、進行状況は保存されません。解析後に障害が発生した場合、[インターフェイスマッピング（Interface Mapping）] 画面から Cisco Secure Firewall 移行ツールを再起動します。

これで、Cisco Secure Firewall 移行ツールは、Management Center にすでに存在する侵入防御システム（IPS）ポリシーとファイルポリシーを取得し、移行するアクセスコントロールルールにそれらを関連付けることができます。

ファイルポリシーは、システムが全体的なアクセス制御設定の一環として、ネットワークの高度なマルウェア防御とファイル制御を実行するために使用する一連の設定です。この関連付け

により、アクセスコントロールルールの条件と一致するトラフィック内のファイルを通過させる前に、システムは必ずファイルを検査するようになります。

同様に、トラフィックが接続先に向かうことを許可する前に、システムの最終防御ラインとしてIPSポリシーを使用できます。侵入ポリシーは、セキュリティ違反に関するトラフィックの検査方法を制御し、インライン展開では、悪意のあるトラフィックをブロックまたは変更することができます。システムが侵入ポリシーを使用してトラフィックを評価する場合、システムは関連付けられた変数セットを使用します。セット内の大部分の変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先のIPアドレスとポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制および動的ルール状態にある IP アドレスを表すこともできます。

タブで特定の構成項目を検索するには、列の上部にあるフィールドに項目名を入力します。テーブルの行はフィルタ処理され、検索語に一致する項目のみが表示されます。

（注） デフォルトでは、[インライングループ化（Inline Grouping）] オプションが有効になっています。

[構成の最適化、確認および検証（Optimize, Review and Validate Configuration）] 画面で Cisco Secure Firewall 移行ツールを閉じると、進行状況が保存され、後で移行を再開できます。この画面の前に閉じると、進行状況は保存されません。解析後に障害が発生した場合、[インターフェイスマッピング（Interface Mapping）] 画面から Cisco Secure Firewall 移行ツールを再起動します。

Cisco Secure Firewall 移行ツールの ACL 最適化の概要

Cisco Secure Firewall移行ツールは、ネットワーク機能に影響を与えることなく、ファイアウォールルールベースから最適化（無効化または削除）できる ACL を識別および分離するサポートを提供します。

ACL 最適化は、次の ACL タイプをサポートします。

- 冗長 ACL：2 つの ACL の構成とルールのセットが同じ場合、基本以外の ACL を削除してもネットワークに影響はありません。たとえば、2 つのルールが同じネットワーク上で FTP および IP トラフィックを許可し、アクセスを拒否するルールが定義されていない場合、最初のルールを削除できます。
- シャドウ ACL：最初の ACL は、2 番目の ACL の設定を完全にシャドウイングします。2 つのルールに同様のトラフィックがある場合、2 番目のルールはアクセスリストの後半に表示されるため、どのトラフィックにも適用されません。2 つのルールがトラフィックに対して異なるアクションを指定している場合、シャドウイングされたルールを移動するか、いずれかのルールを編集して必要なポリシーを実装できます。たとえば、特定の送信元または宛先に対して、基本ルールで IP トラフィックを拒否し、シャドウイングされたルールで FTP トラフィックを許可できます。

Cisco Secure Firewall 移行ツールは、ACL 最適化のルールを比較する際に次のパラメータを使用します。

（注） チェックポイント ではACP ルールアクションに対してのみ最適化を使用できます

- 無効化された ACL は、最適化プロセス中に考慮されません。
- 送信元の ACL は、対応する ACE（インライン値）に展開された後、次のパラメータについて比較されます。
  - 送信元と宛先のゾーン
  - 送信元と宛先のネットワーク
  - 送信元/宛先ポート

オブジェクトの最適化

次のオブジェクトは、移行プロセス中にオブジェクトの最適化について考慮されます。

- 未参照のオブジェクト：移行の開始時に、未参照のオブジェクトを移行しないように選択できます。
- 重複したオブジェクト：オブジェクトがすでに Management Center に存在する場合、重複したオブジェクトを作成する代わりに、ポリシーが再利用されます。
- 一貫しないオブジェクト：名前が似ていても内容が異なるオブジェクトがある場合、オブジェクト名は移行プッシュの前に Cisco Secure Firewall 移行ツールで変更されます。

移行された構成の以下へのプッシュ： Management Center

構成の検証に成功せず、すべてのオブジェクトの競合を解決していない場合は、移行されたチェックポイント 構成を Management Center にプッシュできません。

移行プロセスのこのステップでは、移行された構成を Management Center に送信します。脅威に対する防御 デバイスに構成を展開しません。ただし、脅威に対する防御 上の既存の構成はこのステップで消去されます。

（注） Cisco Secure Firewall 移行ツールが移行された構成を Management Center に送信している間は、構成を変更したり、デバイスに展開したりしないでください。

ステップ 1 [検証ステータス（Validation Status）] ダイアログボックスで、検証の概要を確認します。

ステップ 2 [構成のプッシュ（Push Configuration）] をクリックして、移行した チェックポイント 構成を Management Center に送信します。

Cisco Secure Firewall 移行ツールに、移行の進行状況の概要が表示されます。コンソールに、Management Center にプッシュされているコンポーネントの詳細な進行状況を行ごとに表示できます。

ステップ 3 移行が完了したら、[レポートのダウンロード（Download Report）] をクリックして、移行後レポートをダウンロードして保存します。

移行後レポートのコピーも、Cisco Secure Firewall 移行ツールと同じ場所にある `Resources` フォルダに保存されます。

ステップ 4 移行が失敗した場合は、移行後レポート、ログファイル、および未解析ファイルを慎重に確認して、失敗の原因を把握します。

トラブルシューティングについては、サポートチームに問い合わせることもできます。

移行の失敗のサポート

移行に失敗する場合は、サポートにお問い合わせください。

1. [移行完了（Complete Migration）] 画面で、[サポート（Support）] ボタンをクリックします。

   ヘルプサポートページが表示されます。

2. [サポートバンドル（Support Bundle）] チェックボックスをオンにして、ダウンロードする構成ファイルを選択します。

   （注） ログファイルと DB ファイルは、デフォルトでダウンロード用に選択されています。

3. [ダウンロード（Download）] をクリックします。

   サポートバンドルファイルは、ローカルパスに .zip としてダウンロードされます。Zip フォルダを抽出して、ログファイル、DB、および構成ファイルを表示します。

4. [Email us] をクリックして、テクニカルチームに障害の詳細を電子メールで送信します。

   ダウンロードしたサポートファイルを電子メールに添付することもできます。

5. [TAC ページに移動（Visit TAC page）] をクリックして、シスコのサポートページで TAC ケースを作成します。

   （注） TAC ケースは、移行中にいつでもサポートページからオープンできます。

Check Point の移行後レポートの確認と移行の完了

ステップ 1 移行後レポートをダウンロードした場所に移動します。

ステップ 2 移行後レポートを開き、その内容を慎重に確認して、ASA 構成がどのように移行されたかを理解します。

- [移行の概要（Migration Summary）]：Check Point から Firepower Threat Defense に正常に移行された構成の概要。
- [選択的ポリシー移行（Selective Policy Migration）]：移行およびインターフェースマッピングのために選択された、特定の Check Point 機能の詳細を確認できます。
- [移行の変換（Migration Conversions）]：以下を含む変換とプッシュの詳細：

- ネットワーク/サービスオブジェクトの処理
- 部分的に移行された構成のリストと理由
- サポートされていない構成のリストと理由
- 拡張されたアクセス制御ルール

Cisco Secure Firewall 移行ツールのアンインストール

すべてのコンポーネントは、Cisco Secure Firewall 移行ツールと同じフォルダに保存されます。

ステップ 1 Cisco Secure Firewall 移行ツールを配置したフォルダに移動します。

ステップ 2 ログを保存する場合は、`log` フォルダを切り取りまたはコピーして別の場所に貼り付けます。

ステップ 3 移行前レポートと移行後レポートを保存する場合は、`resources` フォルダを切り取りまたはコピーして別の場所に貼り付けます。

ステップ 4 Cisco Secure Firewall 移行ツールを配置したフォルダを削除します。

ヒント ログファイルはコンソールウィンドウに関連付けられています。Cisco Secure Firewall 移行ツールのコンソールウィンドウが開いている場合、ログファイルとフォルダは削除できません。

移行例： チェックポイントから Threat Defense 2100 へ

（注） 移行の完了後にターゲットデバイスで実行できるテスト計画を作成します。

- メンテナンス期間前のタスク
- メンテナンス期間のタスク

メンテナンス期間前のタスク

始める前に

Management Center をインストールして展開していることを確認します。詳細については、適切な『Management Center Hardware Installation Guide』[英語] および適切な『Management Center Getting Started Guide』[英語] を参照してください。

ステップ 1 Check Point Web Visualization Tool および FMT-CP-Config-Extractor_v4.0.1-8248 ツールを使用して、移行しようとしている Check Point デバイス構成を収集し、Check Point 構成ファイルのコピーを保存します。

ステップ 2 Check Point 構成 zip ファイルを確認します。

ステップ 3 ネットワークに Firepower 2100 シリーズ デバイスを展開し、インターフェイスを接続してアプライアンスの電源をオンにします。

詳細については、『Cisco Threat Defense for the 2100 Series Using Management Center Quick Start Guide』[英語] を参照してください。

ステップ 4 Management Center によって管理される Firepower 2100 シリーズ デバイスを登録します。

詳細については、「Add Devices to the Management Center」を参照してください。

ステップ 5 （任意）送信元チェックポイント構成に結合インターフェイスがある場合は、ターゲット Firepower 2100 シリーズ デバイスでポートチャネル（EtherChannel）を作成します。

詳細については、「Configure EtherChannels and Redundant Interfaces」を参照してください。

ステップ 6 Cisco Secure Firewall 移行ツールの最新バージョンを https://software.cisco.com/download/home/286306503/type からダウンロードして実行します。

詳細については、「Cisco.com からの Cisco Secure Firewall 移行ツールのダウンロード （4 ページ）」を参照してください。

ステップ 7 Cisco Secure Firewall 移行ツールを起動し、接続先パラメータを指定する場合は、Management Center に登録した Firepower 2100 シリーズ デバイスを選択します。

詳細については、「Cisco Secure Firewall 移行ツールの接続先パラメータの指定 （24 ページ）」を参照してください。

ステップ 8 チェックポイント インターフェイスを 脅威に対する防御 インターフェイスにマッピングします。

（注） Cisco Secure Firewall 移行ツールを使用すると、チェックポイント インターフェイスタイプを 脅威に対する防御 インターフェイスタイプにマッピングできます。

たとえば、Check Point の結合インターフェイスを 脅威に対する防御 の物理インターフェイスにマッピングできます。

詳細については、「チェックポイント 構成と Secure Firewall Device Manager Threat Defense インターフェイスのマッピング」を参照してください。

ステップ 9 論理インターフェイスをセキュリティゾーンにマッピングするときに、[自動作成（Auto-Create）] をクリックして、Cisco Secure Firewall 移行ツールで新しいセキュリティゾーンを作成できるようにします。既存のセキュリティゾーンを使用するには、手動でチェックポイント論理インターフェイスをセキュリティゾーンにマッピングします。

詳細については、「セキュリティゾーンとインターフェイスグループへの チェックポイント インターフェイスのマッピング」を参照してください。

ステップ 10 このガイドの手順に従って、移行する構成を順に確認および検証し、構成を Management Center にプッシュします。

ステップ 11 移行後レポートを確認し、手動で他の構成をセットアップして脅威に対する防御 に展開し、移行を完了します。

詳細については、「Check Point の移行後レポートの確認と移行の完了 （34 ページ）」を参照してください。

ステップ 12 移行の計画時に作成したテスト計画を使用して、Firepower 2100 シリーズ デバイスをテストします。

メンテナンス期間のタスク

始める前に

メンテナンスウィンドウの前に実行する必要があるすべてのタスクが完了していることを確認します。「メンテナンス期間前のタスク （35 ページ）」を参照してください。

ステップ 1 Gaia Console を介して Check Point Security Gateway に接続します。

ステップ 2 Gaia Console を介して目的の Security Gateway の Check Point インターフェイスをシャットダウンします。

ステップ 3 （任意）Management Center にアクセスし、Cisco Secure Firewall 移行ツールによって移行されない動的ルーティング、プラットフォーム設定、およびその他の機能を、手動で Firepower 2100 シリーズ デバイス用に構成します。

ステップ 4 周辺スイッチング インフラストラクチャの Address Resolution Protocol（ARP）キャッシュをクリアします。

ステップ 5 周辺スイッチング インフラストラクチャから Firepower 2100 シリーズ デバイスインターフェイスの IP アドレスに対して基本的な ping テストを実行し、アクセス可能であることを確認します。

ステップ 6 Firepower 2100 シリーズ デバイスインターフェイスの IP アドレスに対するレイヤ 3 ルーティングが必要なデバイスから基本的な ping テストを実行します。

ステップ 7 Firepower 2100 シリーズ デバイスに新しい IP アドレスを割り当て、 チェックポイント に割り当てられた IP アドレスを再利用しない場合は、次の手順を実行します。

1. IP アドレスを参照する静的ルートを更新し、Firepower 2100 シリーズ デバイスの IP アドレスを指すようにします。
2. ルーティングプロトコルを使用している場合は、ネイバーが Firepower 2100 シリーズ デバイスの IP アドレスを予期される接続先のネクストホップとして認識していることを確認します。

ステップ 8 包括的なテスト計画を実行し、 Firepower 2100 デバイスの管理 Management Center 内でログをモニタリングします。

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。