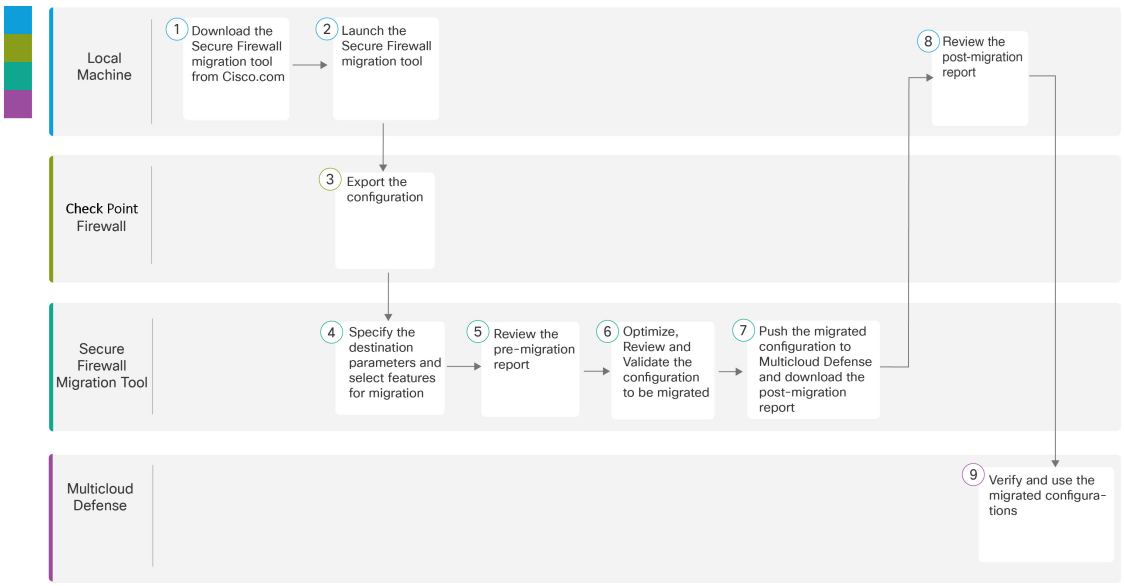
Check Point から Multicloud Defense への移行のワークフロー

Check Point から MultiCloud Defense への移行のワークフロー

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 Multicloud 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	ローカル マシン	Cisco.com から最新バージョンの 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	Local Machine	ローカルマシンで、Cisco.com からダウンロードしたアプリケーションファイルをダブルクリックして、Cisco Secure Firewall 移行ツールを開始します。
3	Check Point ファイアウォール	構成ファイルをエクスポートします。Check Point ファイアウォールから構成をエクスポートするには、r80 の Check Point 構成ファイルのエクスポート （7 ページ）を参照してください。
4	Cisco Secure Firewall 移行ツール	この手順の実行中、Multicloud Defense の接続先パラメータを指定できます。手順の詳細については、Multicloud Defense の接続先パラメータの指定 （20 ページ）を参照してください。
5	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。手順の詳細については、移行前レポートの確認 （22 ページ）を参照してください。
6	Cisco Secure Firewall 移行ツール	構成を慎重に最適化して確認し、それが正しいことを確認します。手順の詳細については、移行する構成の最適化、確認および検証 （23 ページ）を参照してください。
7	Cisco Secure Firewall 移行ツール	移行プロセスのこの手順では、移行済み構成を Multicloud Defense 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。手順の詳細については、Multicloud Defense への構成のプッシュ （26 ページ）を参照してください。
8	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。手順の詳細については、移行後レポートの確認と移行の完了 （27 ページ）を参照してください。
9	Multicloud Defense	移行済み構成を確認し、必要に応じて、ゲートウェイの構成で使用します。

移行の前提条件

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。

CDO でホストされている Cisco Secure Firewall 移行ツールのクラウドバージョンを使用する場合は、手順 4 に進みます。

手順

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。Firewall Threat Defense 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 Cisco Secure Firewall 移行ツールの適切な実行可能ファイルをダウンロードしていることを確認してください。

ステップ 4 CDO ユーザーでそこにホストされている移行ツールを使用する場合は、CDO テナントにログインして、左側のペインで、**[管理（Administration）]**>**[移行（Migration）]**>**[ファイアウォール移行ツール（Firewall Migration Tool）]** に移動して、移行インスタンスを作成します。

移行の実行

Cisco Secure Firewall 移行ツールの起動

このタスクは、デスクトップバージョンの Cisco Secure Firewall 移行ツールを使用している場合にのみ適用されます。CDO でホストされている移行ツールのクラウドバージョンを使用している場合は、「Check Point 構成ファイルのアップロード」に進みます。

（注） 移行ツールのデスクトップバージョンを起動すると、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
- 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。

手順

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。

  （注）
  ログインポップアップの表示を妨げる可能性があるため、ブラウザのポップアップブロッカーを必ず無効にします。

  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、「開発元が不明な Mac アプリを開く」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。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。

  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。

- インターネットにアクセスできないエアギャップネットワークにファイアウォールを展開した場合は、Cisco TAC に連絡して、管理者のログイン情報で動作するビルドを入手してください。このビルドでは使用状況の統計がシスコに送信されず、TAC がログイン情報を提供できることに注意してください。

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を確認（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、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。

- 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。

Cisco Secure Firewall 移行ツールでのデモモードの使用

Cisco Secure Firewall 移行ツールを起動し、[送信元設定の選択（Select Source Configuration）] ページで、[移行の開始（Start Migration）] を使用して移行を開始するか、[デモモード（Demo Mode）] に入るかを選択できます。

デモモードでは、ダミーデバイスを使用してデモ移行を実行し、実際の移行フローがどのようになるかを可視化できます。移行ツールは、[送信元ファイアウォールベンダー（Source Firewall Vendor）] ドロップダウンでの選択に基づいてデモモードをトリガーします。構成ファイルをアップロードするか、ライブデバイスに接続して移行を続行することもできます。デモ FMC、デモ FTD デバイス、Multicloud Defense などの送信元デバイスや対象デバイスを選択すると、デモの移行を実行できます。

注意 [デモモード（Demo Mode）] を選択すると、既存の移行ワークフローがあれば消去されます。[移行の再開（Resume Migration）] にアクティブな移行があるときにデモモードを使用すると、アクティブな移行は失われ、デモモードを使用した後に最初から再開する必要があります。

移行前レポートをダウンロードして確認し、実際の移行ワークフローで実行するその他のアクションを実行することもできます。ただし、デモ移行は設定の検証までしか実行できません。これはデモモードにすぎないため、選択したデモターゲットデバイスに設定をプッシュすることはできません。検証ステータスと概要を確認し、[デモモードの終了（Exit Demo Mode）] を

クリックして [送信元設定の選択（Select Source Configuration）] ページに再度移動し、実際の移行を開始できます。

（注） デモモードでは、設定のプッシュを除く Cisco Secure Firewall 移行ツールのすべての機能セットを活用して、実際の移行を行う前にエンドツーエンドの移行手順のトライアルを実行できます。

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

（注） Check Point Management Center コマンドライン（CLI）が CLISH モードであることを確認します。Expert モードになっている場合は、Live Connect 経由で構成をエクスポートする前に、Expert モードを終了して CLISH モードに切り替えます。

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：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：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：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。

手順

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 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 のカスタム API ポート」を参照してください。

次のタスク

r80 の Check Point 構成ファイルのエクスポート

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。

手順

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 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 のカスタム API ポート」を参照してください。

次のタスク

r80 の Check Point 構成ファイルのエクスポート

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。

手順

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。

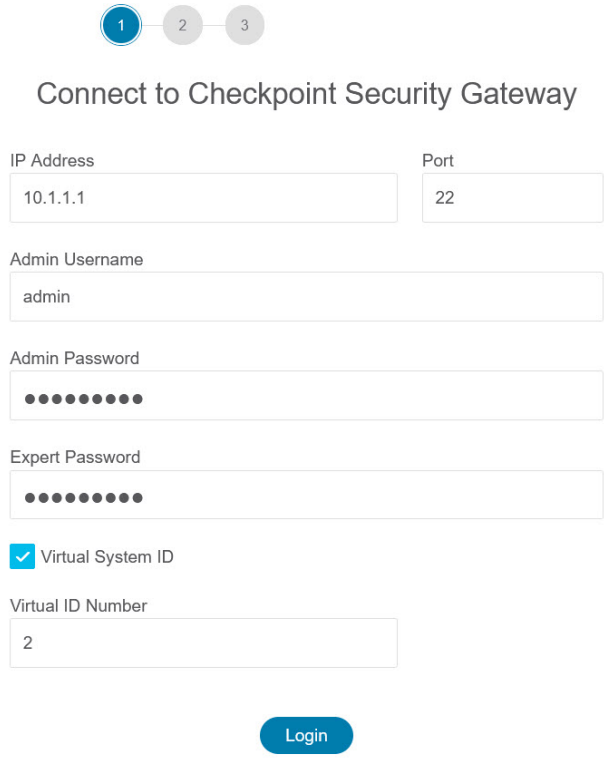
d) Check Point Security Gateway に SSH 接続し、次のコマンドを使用して新しいパスワードを作成します。

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 のカスタム API ポート」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。

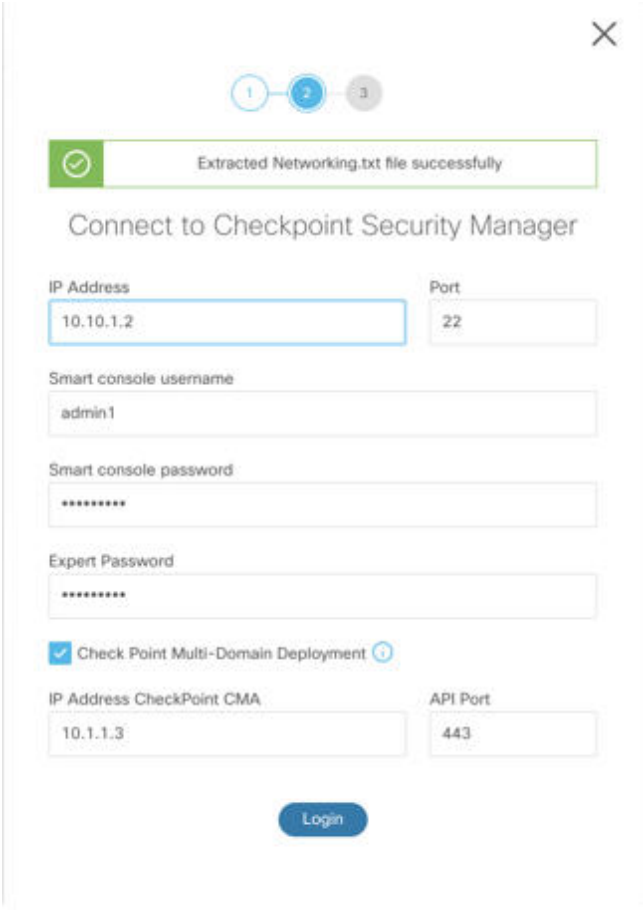
   set expert-password <password>

   （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 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 のカスタム API ポート」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 構成ファイルのエクスポート

Check Point（r80）Security Manager のカスタム API ポートの使用

（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。

手順

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。

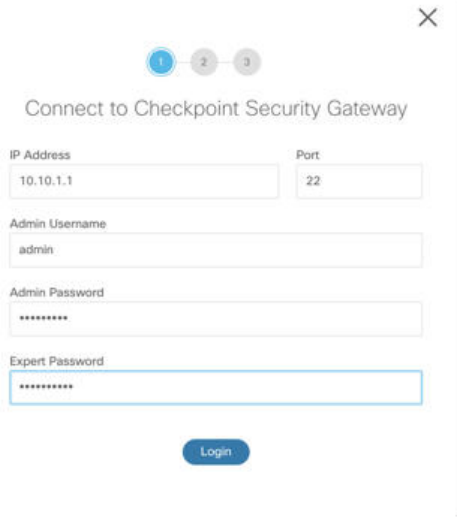
（注）
Live Connect は、Check Point（r80）でのみ使用できます。

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。

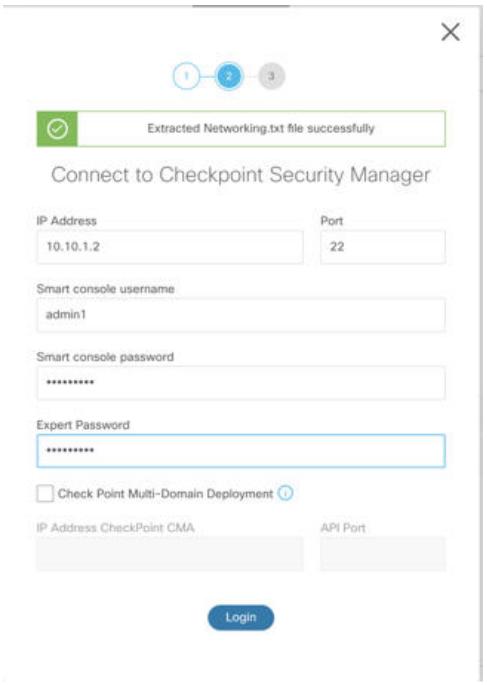
Cisco Secure Firewall 移行ツールは、インターフェイス構成やルート構成などのデバイス固有の構成を含む *networking.txt* ファイルを生成します。Cisco Secure Firewall 移行ツールの現在のセッションのローカルディレクトリに *networking.txt* ファイルを保存します。

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。

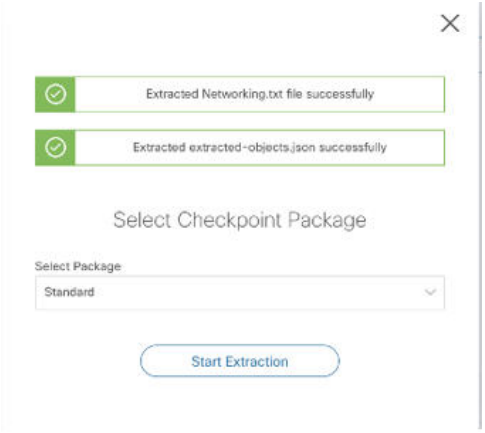
Cisco Secure Firewall 移行ツールは、Check Point Security Manager で使用可能な完全なネットワークおよびサービスオブジェクト構成をキャプチャする *Extracted-objects.json* ファイルを生成します。

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。

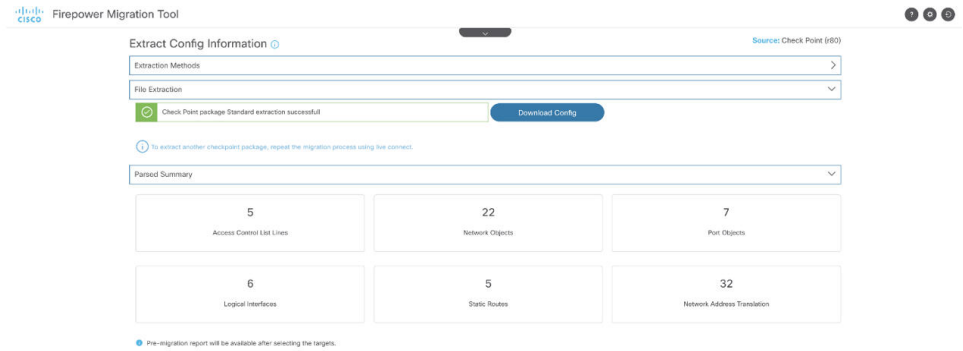
ステップ 5 [Select Check Point Package] リストから移行する Check Point ポリシーパッケージを選択し、[Start Extraction] をクリックします。

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。

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。

Multicloud Defense の接続先パラメータの指定

始める前に

- Multicloud Defense が有効になっている CDO テナントがある。
- Multicloud Defense に必要な運用ライセンスを購入している。

（注） 90 日の無料トライアル期間中でも有料サブスクリプションの完全な機能を体験していただけるため、この期間であっても Multicloud Defense に構成を移行できます。

- Multicloud Defense のベース URL と CDO テナント名を保持している。
- API キーを作成し、API キー作成時に、Multicloud Defense が生成する **API キー ID** と **API キーシークレット**もコピーした。詳細については、「Create an API Key in Multicloud Defense」を参照してください。

手順

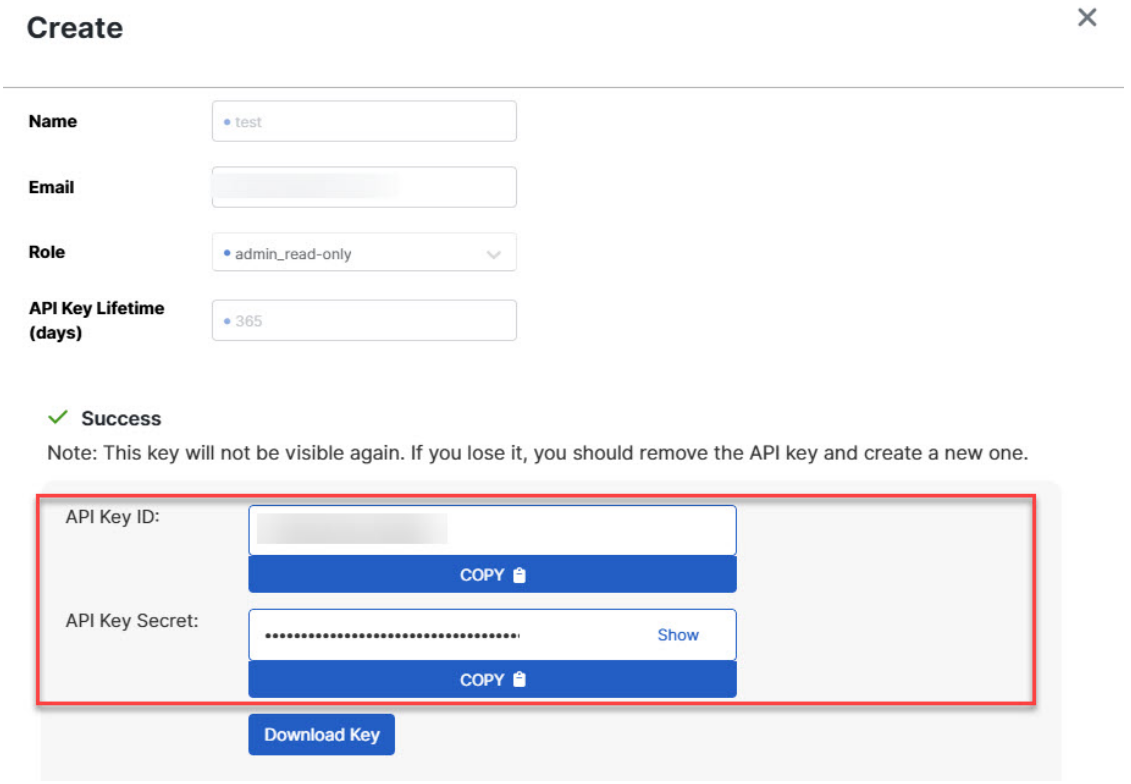
ステップ 1 [ターゲットを選択（Select Target）] ウィンドウで、**Multicloud Defense** を選択します。

ステップ 2 対応するフィールドに次のパラメータを指定して、移行ツールと Multicloud Defense 間の接続を確立します。

- **ベース URL の入力**：これは、Multicloud Defense コントローラに接続する際にブラウザで確認できるベース URL です。たとえば、コントローラダッシュボードで、**/dashboard** の部分を除くブラウザ上のリンクをコピーします。URL は https://xxxx.mcd.apj.cdo.cisco.com のようになります
- **テナント名の入力**：CDO テナントの名前。Multicloud Defense ウィンドウにいる場合は、右上の [プロファイル（Profile）] ドロップダウンから、CDO ウィンドウにいる場合は、**[管理（Administration）] > [一般設定（General Settings）]** からコピーします。

- **API キー ID の入力**：**[システムとアカウント（System and Accounts）]** > **[APIキー（API Keys）]** の順番に選択して、API キーを作成する際に、Multicloud Defense コントローラが生成する **API キー ID**。キーの名前、E メールアドレス、API キーに必要なロール、API キーに付与するロールおよびキーを生成するための API キーの有効期間を指定します。キーのデフォルトの有効期間は、365 日に設定されています。
- **API キーシークレットの入力**：API キーの作成時に Multicloud Defense コントローラが生成する **API キーシークレット**。

（注）
API キーの作成時にのみ表示される **API キー ID** と **API キーシークレット**の両方をコピーしてください。コピーし忘れた場合は、作成した API キーを削除して新しいキーを生成し、今回は必ずコピーしてください。



ステップ 3 [接続（Connect）] をクリックし、Multicloud Defense への接続試行が成功したことを確認する**「正常に収集済み」**メッセージを受信するまで待機します。

ステップ 4 [機能を選択（Select Features）] を使用すると、Multicloud Defense に移行する構成を選択できます。[アクセス制御（Access Control）] および [参照オブジェクトのみを移行（Migrate Only Reference Objects）] チェックボックスはデフォルトでオンになっています。

この移行では、インターフェイスやルートなどの送信元ファイアウォールからのその他の構成はサポートされていないのでご注意ください。

ステップ 5 [続行（Proceed）]、[変換を開始（Start Conversion）] の順に選択します。移行ツールが送信元の構成を解析するまで待機します。

ステップ 6 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 7 [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。

ステップ 8 [次へ（Next）] をクリックします。

移行前レポートの確認

（注） Cisco Secure Firewall 移行ツールによって解析されない構成は、**移行前レポート**で送信元構成ファイルと同じ XML（r75 ～ r77.30）または json（r80）タグで示されます。

移行中に移行前レポートをダウンロードし忘れた場合は、次のリンクを使用してダウンロードしてください。

移行前レポートのダウンロードエンドポイント：http://localhost:8888/api/downloads/pre_migration_summary_html_format

（注） レポートは、Cisco Secure Firewall 移行ツールの実行中にのみダウンロードできます。

手順

ステップ 1 ダウンロードした**移行前レポート**の場所に移動します。

（注）
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可能性のあ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。

- Firewall Threat Defense または Multicloud Defense への移行に成功したサポートされている構成要素と移行用に選択された特定の 機能のサマリー。
- [エラーのある構成行（Configuration Lines with Errors）]：Cisco Secure Firewall 移行ツールが解析できなかったために正常に移行できない 構成要素の詳細。 構成でこれらのエラー

を修正し、新しい構成ファイルをエクスポートしたら、新しい構成ファイルを Cisco Secure Firewall 移行ツールにアップロードして、続行します。

- [無視される構成（Ignored Configuration）]：Multicloud Defense または Cisco Secure Firewall 移行ツールがサポートしていないために無視された 構成要素の詳細。Cisco Secure Firewall 移行ツールはこれらの行を解析しません。これらの行を確認し、各機能が Multicloud Defense でサポートされているかどうかを確認します。サポートされていない場合は、機能を手動で構成することを計画します。

ステップ 3 （任意） **移行前レポート**で修正措置が推奨されている場合は、インターフェイスで、これらの修正を完了し、再度構成ファイルをエクスポートし、更新された構成ファイルをアップロードして、続行します。

ステップ 4 構成ファイルを正常にアップロードし、解析したら、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。

移行する構成の最適化、確認および検証

始める前に

[設定の最適化、確認および検証（Optimize, Review and Validate Configuration）] ページでは、ターゲット Multicloud Defense に移行しようとしている構成パラメータを確認および検証できます。このステップでは、移行ツールは Multicloud Defense の既存の構成に対して構成を検証し、ターゲット Multicloud Defense での重複を避けるために、アクセス制御ルールの関連付けやオブジェクト名の変更など、移行を成功させるために実行する必要がある変更を提案します。

検証後にタブが点滅している場合は、タブで実行する必要があるアクションがあることを示します。

手順

ステップ 1 すべてのアクセス制御リスト（ACL）エントリを一覧する [アクセス制御（Access Control）] タブで、次を実行します。

- [ACLを最適化（Optimize ACL）] をクリックすると、移行ツールがすべてのシャドウ ACL と冗長 ACL を識別し、無効な ACL として移行するか、移行から除外するかを選択できます。

  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。

- 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。
  - 送信元と宛先のネットワーク
  - 送信元/宛先ポート

[レポートのダウンロード（Download Report）] をクリックして、ACL 名と、対応する冗長 ACL およびシャドウ ACL を Excel ファイルで表形式で確認します。ACL の詳細情報を表示するには、[詳細なACL情報（Detailed ACL Information）] シートを使用します。

[続行（Proceed）] をクリックして、最適化プロセスを開始します。

- テーブル内の各エントリについて、マッピングを確認し、それらが正しいことを確認します。

  移行済みのアクセスポリシールールは、ACL名をプレフィックスとして使用し、ACLルール番号を追加することで、構成ファイルにマッピングしやすくします。たとえば、ACLの名前が "inside_access" の場合、ACL の最初のルール（または ACE）行の名前は "inside_access_#1" になります。TCP または UDP の組み合わせ、拡張サービスオブジェクト、またはその他の理由でルールを拡張する必要がある場合、Cisco Secure Firewall 移行ツールは名前に番号付きサフィックスを追加します。たとえば、許可ルールが移行のために 2 つのルールへ拡張される場合、それらのルールには "inside_access_#1-1" と "inside_access_#1-2" という名前が付けられます。

  サポートされていないオブジェクトを含むルールの場合、Cisco Secure Firewall 移行ツールは名前に "_UNSUPPORTED" というサフィックスを追加します。

- 移行しない場合、または一部の ACL を無効として移行する場合は、行のチェックボックスをオンにし、[アクション（Actions）] をクリックして、該当するオプションを選択します。一括変更を実行するには、[すべてのエントリを選択（Select all entries）] チェックボックスをオンにします。

- アクセス制御リストポリシーを編集するには、ポリシーのチェックボックスをオンにして行を選択し、**[アクション（Actions）]** > **[編集（Edit）]** の順に選択します。

  該当しないすべてのルールは、テーブルでグレーアウトされます。

ステップ 2 [オブジェクト（Objects）] タブでは、次を実行できます。

次のタブを選択し、マッピングを確認します。

- ネットワーク オブジェクト
- ポート オブジェクト
- FQDN オブジェクト

オブジェクト名を変更する場合は、オブジェクトの行のチェックボックスをオンにし、[アクション（Actions）]をクリックして[名前を変更（Rename）]を選択します。一括変更を実行するには、[すべてのエントリを選択（Select all entries）] チェックボックスをオンにします。

ステップ 3 確認が完了したら、[検証（Validate）] をクリックします。注意が必要な必須フィールドは、値を入力するまで点滅し続けることに注意してください。**[検証（Validate）]** ボタンは、すべての必須フィールドに入力した後にのみ有効になります。

検証中、Cisco Secure Firewall 移行ツールは Multicloud Defense に接続し、既存のオブジェクトを確認し、それらのオブジェクトを移行対象オブジェクトのリストと比較します。オブジェクトがすでに Multicloud Defense に存在する場合、Cisco Secure Firewall 移行ツールは次の処理を実行します。

- オブジェクトの名前と構成が同じ場合、Cisco Secure Firewall 移行ツールは既存のオブジェクトを再利用し、Multicloud Defense に新しいオブジェクトを作成しません。
- オブジェクトの名前が同じで構成が異なる場合、Cisco Secure Firewall 移行ツールはオブジェクトの競合を報告します。

検証の進行状況はコンソールで確認できます。

ステップ 4 検証が完了し、[検証ステータス（Validation Status）] ダイアログボックスに 1 つ以上のオブジェクトの競合が表示された場合は、次の手順を実行します。

a) [競合の解決（Resolve Conflicts）] をクリックします。

Cisco Secure Firewall 移行ツールは、オブジェクトの競合が報告された場所に応じて、[ネットワークオブジェクト（Network Objects）] タブまたは [ポートオブジェクト（Port Objects）] タブのいずれかまたは両方に警告アイコンを表示します。

b) タブをクリックし、オブジェクトを確認します。

c) 競合がある各オブジェクトのエントリを確認し、**[アクション（Actions）]** > **[競合の解決（Resolve Conflicts）]** を選択します。

d) [競合の解決（Resolve Conflicts）] ウィンドウで、推奨アクションを実行します。

たとえば、既存の Multicloud Defense オブジェクトとの競合を避けるために、オブジェクト名にサフィックスを追加するように求められる場合があります。デフォルトのサフィックスを受け入れるか、独自のサフィックスに置き換えることができます。

e) [解決（Resolve）] をクリックします。
f) タブ上のすべてのオブジェクトの競合を解決したら、[保存（Save）] をクリックします。
g) [検証（Validate）] をクリックして構成を再検証し、すべてのオブジェクトの競合を解決したことを確認します。

ステップ 5 検証が完了し、[検証状態（Validation Status）] ダイアログボックスに、**「検証成功」**というメッセージが表示されたら、引き続き Multicloud Defense に構成をプッシュします。

Multicloud Defense への構成のプッシュ

始める前に

構成を正常に検証しておらず、すべてのオブジェクト競合を解決していない場合、構成を Multicloud Defense にプッシュできません。

（注） Cisco Secure Firewall 移行ツールが構成を Multicloud Defense に送信中は、構成を変更したりデバイスにデプロイしたりしないでください。

手順

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 [構成をプッシュ（Push Configuration）] をクリックして、送信元ファイアウォール構成を Multicloud Defense 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、Multicloud Defense 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。

（注）
一括設定プッシュの実行中にエラーのある設定がある場合、移行ツールは警告をスローし、移行を中止してエラーを手動で修正するか、誤った設定を除外して移行を続行することを求めます。エラーのある設定を表示してから、[移行の続行（Continue with migration）] または [中止（Abort）] を選択できます。移行を中止する場合は、トラブルシューティングバンドルをダウンロードし、分析のために Cisco TAC と共有できます。

移行を続行する場合は、移行ツールは移行を部分的に成功した移行として扱います。移行後レポートをダウンロードして、プッシュエラーが原因で移行されなかった設定のリストを表示できます。

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 移行できなかった場合、移行後レポート、ログファイル、未解析構成ファイルを慎重に確認し、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（Help）] 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 フォルダを解凍して、ログファイル、DB、構成ファイルを確認します。

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。

移行後レポートの確認と移行の完了

始める前に

移行後レポートには、さまざまなカテゴリの ACL カウント、ACL 最適化、および構成ファイルで実行された最適化の全体的なビューに関する詳細が表示されます。

手順

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、ソース構成がどのように移行されたかを理解します。

1. **移行の概要**：Multicloud Defenseへのソースファイアウォールから正常に移行された構成の概要。

   また、移行前の状態と移行後の状態の差異を示す比較チャートも確認できます。

2. **オブジェクト競合処理**：Multicloud Defenseに既存しているオブジェクトと競合していると識別されたオブジェクトの詳細。オブジェクトの名前と設定が同じ場合、Cisco Secure Firewall 移行ツールは Multicloud Defense オブジェクトを再利用しています。オブジェクトの名前が同じで構成が異なる場合は、管理者がそれらのオブジェクトの名前を変更しています。これらのオブジェクトを慎重に確認し、競合が適切に解決されたことを確認します。

3. **移行しないと判断したアクセス制御ルール**：Cisco Secure Firewall ツールを使用して移行しないと判断したルールの詳細。Cisco Secure Firewall 移行ツールによって無効化され、移行されなかったこれらのルールを確認します。これらの行を確認し、選択したすべてのルールがこのセクションにリストされていることを確認します。必要に応じて、これらのルールを手動で構成できます。

4. **一部移行済み構成**：高度なオプションなしで移行できる高度なオプション付きルールを含む、一部のみ移行されたルールの詳細。これらの行を確認し、詳細オプションがMulticloud Defense でサポートされているかどうかを確認します。サポートされている場合は、これらのオプションを手動で構成します。

5. **拡張アクセス制御ポリシー**：移行中に単一ポイントルールから複数Multicloud Defenseルールに拡張されたソースファイアウォールのアクセス制御ポリシーの詳細。

6. **Actions Taken on Access Control Rules**

   - **移行しないと判断したアクセスルール**：Cisco Secure Firewall ツールを使用して移行しないと判断したアクセス制御の詳細。これらの行を確認し、選択したすべてのルールがこのセクションにリストされていることを確認します。必要に応じて、Multicloud Defense でこれらのルールを手動で構成できます。
   - **ルールアクションが変更されたアクセスルール**：Cisco Secure Firewall 移行ツールを使用して「ルールアクション」が変更されたすべてのアクセス コントロール ポリシー ルールの詳細。ルールアクションの値は、Allow、Trust、Monitor、Block、Block with resetです。これらの行を確認し、選択したすべてのルールがこのセクションにリストされていることを確認します。必要に応じて、Multicloud Defense でこれらのルールを手動で構成できます。

（注）

サポートされていないルールが移行されなかった場合、不要なトラフィックがファイアウォールを通過する問題が発生します。このトラフィックがブロックされるように、Multicloud Defense でルールを構成することをお勧めします。

ステップ 3 **移行前レポート**を開き、Multicloud Defense で手動で移行する必要がある構成項目をメモします。

ステップ 4 移行されたすべての構成パラメータが、Multicloud Defense で使用できることを確認します。

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。