移行の実行

Cisco.com から 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、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。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） 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 [Firewall移行ツール（Firewall Migration Tool）] に移動します。Firepower Threat Defense デバイスのダウンロード領域から 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 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 Firewall 移行ツール実行可能ファイルをダウンロードします。

Firewall 移行ツールの起動

（注） 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、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、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 Firewall 移行ツールのダウンロード
- Firewall 移行ツールに関する注意事項と制約事項セクションで要件を確認します。
- Firepower 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、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、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、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。

  Firewall 移行ツールは、すべての関連ファイルを作成し、Firepower 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、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、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
```

Firewall 移行ツールは、すべての関連ファイルを作成し、Firepower 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 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 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 Firewall 移行ツールにログインします。

ステップ 4 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。
  - Username：admin
  - Password：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、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、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。

- Firewall 移行ツールを使用して Fortinet ファイアウォールから情報を抽出する必要がある場合は、「Fortinet ファイアウォールからの構成のエクスポート」に進みます。

Fortinet ファイアウォールからの構成のエクスポート

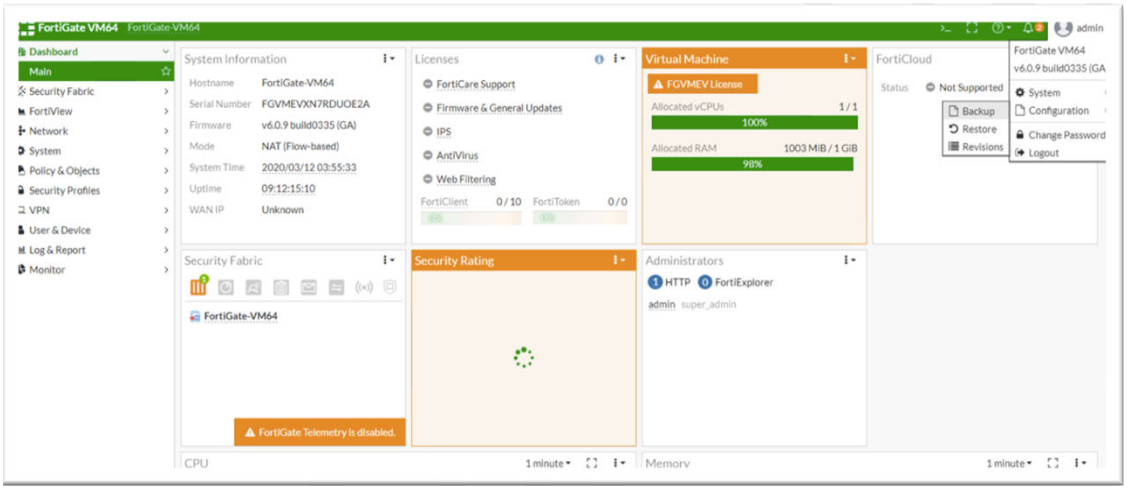
Fortinet ファイアウォールの構成は、次の方法でエクスポートできます。

- Fortinet ファイアウォール GUI からの Fortinet ファイアウォール構成のエクスポート
- Fortimanager からの Fortinet ファイアウォール構成のエクスポート

Fortinet ファイアウォール GUI からの Fortinet ファイアウォール構成のエクスポート

Fortinet ファイアウォール GUI から構成を抽出するには、次の手順を実行します。

ステップ 1 FortiGate VM64 GUI から、**[管理（Admin）]** > **[構成（Configuration）]** > **[バックアップ（Backup）]**を選択します。



ステップ 2 ローカル PC または USB ディスクにバックアップを転送します。

（注） VDOM が有効になっている場合は、バックアップの範囲が FortiGate 構成全体（グローバル）または特定の VDOM 構成のみ（VDOM）のいずれであるかを示します。

ステップ 3 バックアップが VDOM 構成の場合は、[VDOM] リストから VDOM 名を選択します。

（注） Firewall 移行ツールでは、バックアッププロセスを進めるために暗号化されていないファイルが必要です。

ステップ 4 [OK] を選択します。

Web ブラウザにより、構成ファイルの保存場所を指定するように求められます。

構成ファイルの拡張子は **.conf** です。

次のタスク

Fortinet 構成ファイルのアップロード

Fortimanager からの Fortinet ファイアウォール構成のエクスポート

関連するデバイス構成を FortiManager から抽出できます。

ステップ 1 FortiManager にログインします。

ステップ 2 バックアップを実行する必要がある正しい Fortigate デバイスを特定します。

ステップ 3 [構成とインストールのステータス（Configuration and Installation Status）] で、[全リビジョン（Total Revision）] の横にあるアイコンを選択して最新のリビジョンを取得します。

ステップ 4 [ダウンロード（Download）] をクリックして構成ファイルをダウンロードします。

ダウンロードしたファイルのファイルタイプは、拡張子 .conf です。

次のタスク

Fortinet 構成ファイルのアップロード

Fortinet 構成ファイルのアップロード

始める前に

送信元 Fortinet デバイスから構成ファイルを `.cfg` または `.txt` としてエクスポートします。

（注） ハードコーディングした構成ファイルや手動で変更した構成ファイルはアップロードしないでください。テキストエディタは、移行に失敗する原因となる空白行やその他の問題をファイルに追加します。

ステップ 1 ファイアウォール移行ツールは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。コンソールには、解析中の Fortinet 構成行など、行ごとに進行状況のログが表示されます。コンソールが表示されない場合は、ファイアウォール移行ツールの背後にある別のウィンドウで確認できます。[コンテキストの選択（Context Selection）] セクションで、アップロードされた構成がマルチコンテキスト Fortinet に対応するかが識別されます。

ステップ 2 [コンテキストの選択（Context Selection）] セクションを確認し、移行する Fortinet VDOM を選択します。

ステップ 3 [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 4 アップロードされた構成ファイルで、ファイアウォール移行ツールが検出および解析した要素の概要を確認します。

ステップ 5 [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

Firewall 移行ツールの接続先パラメータの指定 （6 ページ）

Firewall 移行ツールの接続先パラメータの指定

始める前に

- IP アドレスの取得： Firepower Management Center
- （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 Firepower Threat Defense デバイスを Firepower Management Center に追加します。「Adding Devices to the Firewall Management Center」を参照してください。
- [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 FMC でポリシーを作成することを強くお勧めします。Firewall 移行ツールは接続された FMC 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 [Firewall Management Centerに接続（Connect to Firewall Management Center）] セクションで、Firepower Management Center 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。

ステップ 2 [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。

Firepower Threat Defense 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 Firepower Threat Defense デバイスにのみ移行できます。

ステップ 3 [接続（Connect）] をクリックします。

ステップ 4 [Firewall Management Centerへのログイン（Firewall Management Center Login）] ダイアログボックスで、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。

Firewall 移行ツールは Firepower Management Center にログインし、その Firepower Management Center による管理対象 Firepower Threat Defense 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 5 [続行（Proceed）] をクリックします。

ステップ 6 [Choose FTD] 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、 Fortinet 構成を移行するデバイスをオンにします。

  選択した Firepower 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 Firepower Threat Defense デバイスには、移行する Fortinet 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、Firepower Threat Defense 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。 Fortinet 構成と同じファイアウォールモードでデバイスを設定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。

  リモート展開が有効になっている FMC/FTD 6.7 以降への Fortinet ファイアウォールの移行は、Firewall 移行ツールでサポートされています。ただし、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。

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

  FTD なしで続行すると、Firewall 移行ツールは FTD に構成またはポリシーをプッシュしません。したがって、Firewall 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。

ステップ 7 [続行（Proceed）] をクリックします。

移行先に応じて、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 8 [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 Firepower Threat Defense デバイスに移行する場合、Firewall 移行ツールは、[デバイス設定（Device Configuration）] セクションと [共有設定（Shared Configuration）] セクションで、Fortinet 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。
- Firepower Management Center に移行する場合、Firewall 移行ツールは、[共有設定（Shared Configuration）] セクションで、Fortinet 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 Firepower Threat Defense デバイスを選択していない場合は使用できません。

- Firewall 移行ツールは、移行中に ACL の宛先ゾーンのマッピングを可能にする、宛先セキュリティゾーンをサポートします。

  送信元および接続先のネットワーク オブジェクトまたはグループ、およびサービスオブジェクトまたはグループの性質によっては、Fortinet から FMC への移行時に、この操作によりルールが急増することがあります。

- （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、Fortinet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 9 [続行（Proceed）] をクリックします。

ステップ 10 [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 11 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 12 [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、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 （8 ページ）

移行前レポートの確認

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、ファイアウォール移行ツールの実行中にのみダウンロードできます。

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、ファイアウォール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。

- Firepower Threat Defense に正常に移行できるサポート対象 Fortinet 構成要素と、移行対象として選択された特定の Fortinet 機能のサマリー。
- Configuration Lines with Errors：ファイアウォール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 Fortinet 構成要素の詳細。 Fortinet 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てから、新しい構成ファイルを ファイアウォール移行ツールにアップロードし、続行してください。
- Partially Supported Configuration：部分的にのみ移行可能な Fortinet 構成要素の詳細。これらの構成要素には、詳細オプションを含むルールとオブジェクトが含まれているため、詳細オプションを使用せずにルールまたはオブジェクトを移行できます。これらの行を確認し、詳細オプションが Firepower Management Center 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、ファイアウォール移行ツールを使用して移行を完了した後に、これらのオプションを手動で構成することを計画します。
- Unsupported Configuration：ファイアウォール移行ツールがこれらの機能の移行をサポートしていないため、移行できない Fortinet 構成要素の詳細。これらの行を確認し、各機能が Firepower Management Center 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、ファイアウォール移行ツールを使用して移行を完了した後に、機能を手動で構成することを計画します。
- Ignored Configuration： Firepower Management Center または ファイアウォール移行ツールでサポートされていないために無視される Fortinet 構成要素の詳細。ファイアウォール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 Firepower Management Center 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、機能を手動で構成することを計画します。

Firepower Management Center および Firepower Threat Defense 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、インターフェイス Fortinet で修正を完了し、 Fortinet 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 Fortinet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、ファイアウォール移行ツールに戻り、[次へ（Next）] をクリックして移行を続行します。

次のタスク

Fortinet 構成と Threat Defense インターフェイスのマッピング

Fortinet 構成と Threat Defense インターフェイスのマッピング

Firepower Threat Defense デバイスには、 Fortinet 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。

[FTDインターフェイスのマップ（Map FTD Interface）] 画面で、Firepower Threat Defense 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、Firewall 移行ツールは Fortinet のインターフェイスと Firepower Threat Defense 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。

Fortinet インターフェイスから FTD インターフェイスへのマッピングは、FTD デバイスタイプによって異なります。

- ターゲット FTD がネイティブタイプの場合：
  - FTD には、使用する Fortinet 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（ Fortinet 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 FTD 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 Firewall 移行ツールによって作成されます。
- ターゲット FTD がコンテナタイプの場合：
  - FTD には、使用する Fortinet 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（Fortinet 構成の管理専用を除く）。同数未満の場合は、ターゲット FTD 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 FTD 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 Fortinet での数より 100 少ない場合、ターゲット FTD 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、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

Firepower Management Center に接続し、接続先として Firepower Threat Defense を選択していることを確認します。詳細については、「Firewall 移行ツールの接続先パラメータの指定 （6 ページ）」を参照してください。

（注） Firepower Threat Defense デバイスなしで Firepower 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Fortinet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。Firepower Threat Defenseインターフェイスがすでに Fortinet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。Firewall 移行ツールは、 Fortinet 構成内のすべてのサブインターフェイスについて Firepower Threat Defense 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Fortinetインターフェイスを Firepower Threat Defense 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

Fortinet インターフェイスを適切な Firepower 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。詳細については、「セキュリティゾーン への Fortinet 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へのFortinetインターフェイスのマッピング

Fortinet 構成が正しく移行されるように、 Fortinet インターフェイスを適切な Firepower 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。 Fortinet 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。Firepower 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、Firepower 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。

ファイアウォール移行ツールでは、セキュリティゾーン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、Firepower Management Center では許可されます。Firepower Management Center のセキュリティゾーンの詳細については、「Security Zones」を参照してください。

ステップ 1 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 Firepower 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 2 Firepower Management Center に存在するセキュリティゾーンにインターフェイスをマッピングするには、[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。

ステップ 3 セキュリティゾーンは、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。

セキュリティゾーン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の追加（Add SZ）] をクリックします。

b) [セキュリティゾーンの追加（Add SZ）] 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。

d) [閉じる（Close）] をクリックします。

セキュリティゾーン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、[ゾーンマッピング（Zone Mapping）] をオンにします。

c) [自動作成（Auto-Create）] をクリックします。

[自動作成（Auto-Create）] をクリックすると、送信元ファイアウォールゾーンが自動的にマッピングされます。同じ名前のゾーンが FMC にすでに存在する場合、そのゾーンは再利用されます。マッピングページには、再利用ゾーンに対して "(A)" が表示されます。たとえば、**inside** "(A)" となります。

ステップ 4 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にマッピングしたら、[Next] をクリックします。

最適化、 移行する構成の確認と検証

移行した Fortinet 構成を Firepower 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 Firepower Threat Defense デバイスの構成内容と一致することを確認します。

これで、ファイアウォール移行ツールは、Firepower 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、[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 ファイアウォール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。この画面の前にファイアウォール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 ファイアウォール移行ツールを再起動します。

ファイアウォール移行ツール ACL 最適化の概要

ファイアウォール移行ツール 2.5.2 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。

ファイアウォール移行ツールは、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） Fortinet 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（Source and Destination Port）]

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 FMC 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 ファイアウォール移行ツールで変更されます。

ステップ 1 （オプション）[構成の最適化、確認および検証（Optimize, Review and Validate Configuration）] 画面で、[ACLの最適化（Optimize ACL）] をクリックして最適化コードを実行し、以下の操作を実行します。

a) [はい（Yes）] をクリックして、ACL の最適化を続行します。特定された移行の冗長 ACL ルールとシャドウ ACL ルールが表示されます。

ACL 最適化の分析にかかる時間は、移行元の構成ファイルのサイズによって異なります。予測時間が表示されます。

最適化が考慮された ACL ルールの合計数の概要を示すレポートが表示されます。最適化レポートとそのコンポーネントの詳細については、ACL 最適化のレポート （18 ページ）を参照してください。

[冗長ACL（Redundant ACL）] および [シャドウACL（Shadow ACL）] タブは、ACL 最適化レポートにデータがある場合にのみ表示されます。

ACL は、[冗長ACL（Redundant ACL）] と [シャドウACL（Shadow ACL）] 両方の異なる基本ルールに表示されます。

（注） 冗長またはシャドー ACL の下に表示される ACL エントリは、基本 ACL とは見なされません。

b) 特定された ACL 最適化ルールをダウンロードするには、[ダウンロード（Download）] をクリックします。

c) ルールを選択し、**[アクション（Actions）]** > **[無効として移行（Migrate as disabled）]** または **[移行しない（Do not migrate）]** を選択して、いずれかのアクションを適用します。

d) **[保存（Save）]** をクリックします。
移行操作が [移行しない（Do not migrate）] から [無効として移行（Migrate as disabled）] またはその逆に変わります。

次のオプションを使用して、ルールの一括選択を実行できます。

- [移行（Migrate）：デフォルトの状態で移行します。
- [移行しない（Do not migrate）]：ACL の移行を無視します。
- [無効として移行（Migrate as disabled）]：[状態（State）] フィールドが [無効（Disable）] に設定されている ACL を移行します。
- [有効として移行（Migrate as enabled）]：[状態（State）] フィールドが [有効（Enable）] に設定されている ACL を移行します。

ステップ 2 [Review and Validate Configuration] 画面で、[Access Control Rules] をクリックし、次の手順を実行します。
最適化、

a) 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。

移行されたアクセスポリシールールは、プレフィックスとして ACL 名を使用し、それに ACL ポリシー ID を追加することで、Fortinet 構成ファイルにマッピングしやすくします。たとえば、Fortinet 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/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、ファイアウォール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、ファイアウォール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。

b) 1 つ以上のアクセス制御リストポリシーを移行しない場合は、該当する行のボックスをオンにし、**[アクション（Actions）]** > **[移行しない（Do not migrate）]** を選択して、[保存（Save）] をクリックします。

移行しないことを選択したすべてのルールは、テーブルでグレー表示されます。

c) Firepower Management Center ファイルポリシーを 1 つ以上のアクセス コントロール ポリシーに適用する場合は、該当する行のボックスをオンにし、**[アクション（Actions）]** > **[ファイルポリシー（File Policy）]** を選択します。

[File Policy] ダイアログで、適切なファイルポリシーを選択し、選択したアクセス コントロール ポリシーに適用して、[Save] をクリックします。

d) Firepower Management Center IPS ポリシーを 1 つ以上のアクセス コントロール ポリシーに適用する場合は、該当する行のボックスをオンにし、**[アクション（Actions）]** > **[IPS ポリシー（IPS Policy）]** を選択します。

[IPS Policy] ダイアログで、適切な IPS ポリシーと対応する変数セットを選択し、選択したアクセス コントロール ポリシーに適用して、[Save] をクリックします。

e) ロギングが有効になっているアクセスコントロールルールのロギングオプションを変更する場合は、該当する行のボックスをオンにし、**[アクション（Actions）]** > **[ログ（Log）]** を選択します。

[Log] ダイアログでは、接続の開始時または終了時、またはその両方でイベントのロギングを有効にできます。ロギングを有効にする場合は、接続イベントを**イベントビューア**または **Syslog** のいずれか、または両方に送信することを選択する必要があります。接続イベントを syslog サーバに送信することを選択した場合、Firepower Management Center ですでに構成されている syslog ポリシーを [Syslog] ドロップダウンメニューから選択できます。

f) [アクセスコントロール（Access Control）] テーブル内の移行されたアクセスコントロールルールのアクションを変更する場合は、該当する行のボックスをオンにし、**[アクション（Actions）]** > **[ルールアクション（Rule Action）]** を選択します。

ヒント アクセスコントロールルールにアタッチされている IPS およびファイルのポリシーは、[許可（Allow）] オプションを除くすべてのルールアクションに対して自動的に削除されます。

ACEカウントを、昇順、降順、等しい、大なり、および小なりのフィルタリング順序シーケンスでフィルタリングできるようになりました。

フィルタリング条件をクリアするには、[フィルタのクリア（Clear Filter）] をクリックします。

（注） ACE に基づいた ACL のソート順序は、表示のみを目的としています。ACL は、発生した時間順に基づいてプッシュされます。

ステップ 3 次のタブをクリックし、構成項目を確認します。

- **NAT Rules**
- **ネットワーク オブジェクト**
- **ポート オブジェクト**
- **Interfaces**
- **ルート（Routes）**
- **[動的ルートオブジェクト（Dynamic-Route-Objects）]**

1 つ以上の NAT ルールまたはルートインターフェイスを移行しない場合は、該当する行のボックスをオンにし、**[アクション（Actions）] > [移行しない（Do not migrate）]** を選択して、[保存（Save）] をクリックします。

移行しないことを選択したすべてのルールは、テーブルでグレー表示されます。

ステップ 4 （任意）構成の確認中に、[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）] タブで **[アクション（Actions）] > [名前の変更（Rename）]** を選択して、ネットワークオブジェクトまたはポートオブジェクトの名前を変更することができます。

名前が変更されたオブジェクトを参照するアクセスルールと NAT ポリシーも、新しいオブジェクト名で更新されます。

ステップ 5 （任意）グリッド内の各構成項目の詳細をダウンロードするには、[ダウンロード（Download）] をクリックします。

ステップ 6 確認が完了したら、[確定（Validate）] をクリックします。

検証中、ファイアウォール移行ツールは Firepower Management Center に接続し、既存のオブジェクトを確認して、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 Firepower Management Center にすでに存在する場合、ファイアウォール移行ツールは次のことを行います。

- オブジェクトの名前と構成が同じ場合、ファイアウォール移行ツールは既存のオブジェクトを再利用し、 Firepower Management Center 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、ファイアウォール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 7 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。

ファイアウォール移行ツールは、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 Firepower Management Center 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) [確定（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 8 検証が完了し、[Validation Status] ダイアログボックスに「Successfully Validated」というメッセージが表示されたら、移行された構成の以下へのプッシュ： Firepower Management Center （19 ページ）に進みます。

ACL 最適化のレポート

ACL 最適化レポートには、次の情報が表示されます。

- Summary シート：ACL 最適化のサマリーが表示されます。

	A	B	C	D
1	Sl.no	ACL name	Redundant ACLs	Shadowed ACLs
2	1	outsideACL_#1		outsideACL_#2, outsideACL_#3, outsideACL_#4, outsideACL_#5, outsideACL_#6, outsideACL_#7, outsideACL_#8, outsideACL_#9, outsideACL_#10, outsideACL_#11, outsideACL_#12
3	2	outsideACL_#13		outsideACL_#17, outsideACL_#18
4	3	outsideACL_#14		outsideACL_#15, outsideACL_#16, outsideACL_#17, outsideACL_#18
5	4	outsideACL_#19		outsideACL_#20, outsideACL_#21, outsideACL_#22, outsideACL_#23, outsideACL_#24
6	5	outsideACL_#25		outsideACL_#27, outsideACL_#28, outsideACL_#29, outsideACL_#30
7	6	outsideACL_#26		
8	7	outsideACL_#31		outsideACL_#32, outsideACL_#33
9	8	outsideACL_#34		
10	9	dmzACL_#1		
11	10	dmzACL_#2	dmzACL_#5	
12	11	dmzACL_#3		dmzACL_#5
13	12	dmzACL_#4		
14	13	dmzACL_#6		dmzACL_#7, dmzACL_#8, dmzACL_#9, dmzACL_#10
15	14	dmzACL_#11		dmzACL_#13
16	15	dmzACL_#12		
17	16	extACL_#1		
18	17	extACL_#2		
19	18	extACL_#3		extACL_#4, extACL_#5, extACL_#6
20	19	extACL_#7		
21	20	extACL_#8	extACL_#9, extACL_#10	
22	21	extACL_#11		
23	22	extACL_#12	extACL_#13	
24	23	extACL_#14		
25	24	extACL_#15		
26	25	extACL_#16		
27	26	extACL_#17		extACL_#18, extACL_#19
28	27	localtoremote_#1		
29	28	opt_#1		opt_#3
30	29	opt_#2	opt_#4	opt_#5
31	30	opt_#6-1	opt_#17-1	opt_#7-1, opt_#8-1
32	31	opt_#9-1	opt_#10-1	
33	32	opt_#11-1	opt_#12-1	opt_#13-1
34	33	opt_#14-1		opt_#15-1, opt_#16-1
35	34	opt_#18		
36	35	opt_#19		opt_#20, opt_#21
37	36	opt_#22-1	opt_#23-1	

Summary | Detailed ACL Information | +

- Detailed ACL Information：ベース ACL の詳細が表示されます。各 ACL には、比較対象の基本の ACL と最適化カテゴリとの関連付けを識別する ACL タイプ（シャドウまたは冗長）のタグが付いています。

Sl.no	ACL name	Source zone	Destination zone	Source network	Destination network	Source port	Destination port	Action	ACL type
1	**outsideACL_#1**	**outside**	**ANY**	**any**	**10.0.0.0/8**	**ANY**	**ANY**	**permit**	
	outsideACL_#2	outside	ANY	any	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#3	outside	ANY	192.168.0.1	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#4	outside	ANY	192.168.0.10	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#5	outside	ANY	any	10.1.1.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#6	outside	ANY	any	10.1.1.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#7	outside	ANY	any	10.1.1.0/24	ANY	tcp:80	permit	Shadowed by outsideACL_#1
	outsideACL_#8	outside	ANY	any	10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#9	outside	ANY	200.200.200.1	10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#10	outside	ANY	10.10.10.10, 10.10.0.0/16	10.10.0.0/19, 10.99.99.99	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#11	outside	ANY	any	10.99.99.90, 10.99.99.99, 10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#12	outside	ANY	any	10.99.99.90, 10.99.99.99, 10.10.10.10, 10.10.0.0/16, 10.99.99.99, 10.10.10.10, 10.10.0.0/16, 10.10.0.0/19	ANY	ANY	permit	Shadowed by outsideACL_#1
2	**outsideACL_#13**	**outside**	**ANY**	**any**	**192.168.0.0/16**	**ANY**	**ANY**	**permit**	
	outsideACL_#17	outside	ANY	10.10.1.1	192.168.0.0/16	ANY	tcp:443	permit	Shadowed by outsideACL_#13
	outsideACL_#18	outside	ANY	10.10.1.1	192.168.0.0/16	ANY	tcp:80	permit	Shadowed by outsideACL_#13

移行された構成の以下へのプッシュ： Firepower 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 ASA Fortinet 構成を Firepower 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 Firepower Management Center に送信します。Firepower Threat Defense デバイスに構成を展開しません。ただし、Firepower Threat Defense 上の既存の構成はこのステップで消去されます。

（注） ファイアウォール移行ツールが移行された構成を Firepower 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、移行された ASA Fortinet 構成を Firepower Management Center に送信します。

ファイアウォール移行ツールに、移行の進行状況の概要が表示されます。コンソールに、Firepower 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。

移行前レポートのコピーも、ファイアウォール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。

移行後レポートの確認と移行の完了

移行後のレポートには、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。詳細については、最適化、 移行する構成の確認と検証 （13 ページ）を参照してください。

オブジェクトを確認して検証します。

- **カテゴリ**
  - ACL ルール合計数（移行元の構成）
  - 最適化の対象とみなされる ACL ルールの合計数。冗長、シャドウなどがあります。
- 最適化の ACL カウントは、最適化の前後にカウントされた ACL ルールの合計数を示します。

移行中に移行後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。

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

（注） レポートは、ファイアウォール移行ツールの実行中にのみダウンロードできます。

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、 Fortinet 構成がどのように移行されたかを理解します。

- Migration Summary： Fortinet から Firepower Threat Defense へ正常に移行された構成の概要。 Fortinetインターフェイス、Firepower Management Center ホスト名とドメイン、ターゲット Firepower Threat Defense デバイス（該当する場合）、および正常に移行された構成要素に関する情報が含まれます。
- Selective Policy Migration：移行用に選択された特定の Fortinet 機能の詳細は、[デバイス構成機能（Device Configuration Features）]、[共有構成機能（Shared Configuration Features）]、および [最適化（Optimization）] の 3 つのカテゴリ内で使用できます。
- FortinetInterface to FTD Interface Mapping：正常に移行されたインターフェイスの詳細と、 Fortinet 構成のインターフェイスを Firepower Threat Defense デバイスのインターフェイスにマッピングした方法。これらのマッピングが期待どおりであることを確認します。

  （注） このセクションは、宛先 Firepower Threat Defense デバイスを使用しない移行、または移行に**インターフェイス**が選択されて**いない**場合には適用されません。

- Source Interface Names to FTD Security Zones：正常に移行された Fortinet 論理インターフェイスと名前の詳細、およびそれらを Firepower Threat Defense のセキュリティゾーンにマッピングした方法。これらのマッピングが期待どおりであることを確認します。

  （注） **アクセス制御リスト**と **NAT** が移行に選択されて**いない**場合、このセクションは適用されません。

- Object Conflict Handling：Firepower Management Center の既存のオブジェクトと競合していると識別された Fortinet 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、ファイアウォール移行ツールは Firepower Management Center 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。
- Access Control Rules, NAT, and Routes You Chose Not to Migrate：ファイアウォール移行ツールで移行しないように選択したルールの詳細。ファイアウォール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。
- Partially Migrated Configuration：詳細オプションなしでもルールを移行できる詳細オプション付きルールを含む、一部のみ移行された Fortinet ルールの詳細。これらの行を確認し、詳細オプションが Firepower Management Center 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。
- Unsupported Configuration：ファイアウォール移行ツールがこれらの機能の移行をサポートしていないため、移行されなかった Fortinet 構成要素の詳細。これらの行を確認し、各機能が Firepower Threat

Defense でサポートされているかどうかを確認します。その場合は、Firepower Management Center でこれらの機能を手動で構成します。

- Expanded Access Control Policy Rules：移行時に単一の Fortinet Point ルールから複数の Firepower Threat Defense ルールに拡張された Fortinet アクセス コントロール ポリシー ルールの詳細。
- **Actions Taken on Access Control Rules**
  - [移行しないアクセスルール（Access Rules You Chose Not to Migrate）]：ファイアウォール移行ツールで移行しないように選択した Fortinet アクセスコントロールルールの詳細。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、これらのルールを手動で構成できます。
  - Access Rules with Rule Action Change：ファイアウォール移行ツールツールを使用して「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、これらのルールを手動で構成できます。
  - Access Control Rules that have IPS Policy and Variable Set Applied：IPS ポリシーが適用されているすべての Fortinet アクセス コントロール ポリシー ルールの詳細。これらのルールを慎重に確認し、この機能が Firepower Threat Defense でサポートされているかどうかを確認します。
  - Access Control Rules that have File Policy Applied：ファイルポリシーが適用されているすべての Fortinet アクセス コントロール ポリシー ルールの詳細。これらのルールを慎重に確認し、この機能が Firepower Threat Defense でサポートされているかどうかを確認します。
  - Access Control Rules that have Rule 'Log' Setting Change：ファイアウォール移行ツールを使用して「ログ設定」が変更された Fortinet アクセスコントロールルールの詳細。ログ設定の値は、False、Event Viewer、Syslog 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、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 Firepower Threat Defense によってブロックされるように、Firepower Management Center でルールを構成することを推奨します。

（注） [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 FMC でポリシーを作成することを強くお勧めします。ファイアウォール移行ツール は接続された FMC 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ポリシーに割り当てると、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。

Firepower Management Center および Firepower Threat Defense でサポートされる機能の詳細については、『Firepower Management Center Configuration Guide, Version 6.2.3』を参照してください。

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

ステップ 4 Firepower Management Center で、次の手順を実行します。

a) Firepower Threat Defense デバイスの移行された構成を確認し、次を含むすべての期待されるルールおよびその他の構成項目が移行されたことを確認します。

- アクセス制御リスト（ACL）
- ネットワークアドレス変換規則
- ポートおよびネットワークオブジェクト
- ルート（Routes）
- インターフェイス
- [動的ルートオブジェクト（Dynamic-Route-Objects）]

b) 一部がサポートされている、サポートされていない、無視された、無効化された、および移行されなかったすべての構成項目とルールを構成します。

これらの項目とルールを構成する方法の詳細については、『Firepower Management Center Configuration Guide』を参照してください。手動構成が必要な構成項目の例を次に示します。

- プラットフォーム設定（SSH および HTTPS アクセスを含む）（「Platform Settings for Firepower Threat Defense」を参照）
- Syslog 設定（「Configure Syslog」を参照）
- ダイナミックルーティング（「Routing Overview for Firepower Threat Defense」を参照）
- サービスポリシー（「FlexConfig Policies」を参照）
- VPN 構成（「Firepower Threat Defense VPN」を参照）
- 接続ログ設定（「Connection Logging」を参照）

ステップ 5 確認が完了したら、Firepower Management Center から Firepower Threat Defense デバイスに移行された構成を展開します。

サポートされていないルールと一部がサポートされているルールについて、データが**移行後レポート**に正しく反映されていることを確認します。

ファイアウォール移行ツールでポリシーが Firepower Threat Defense デバイスに割り当てられます。変更が実行中の構成に反映されていることを確認します。移行されるポリシーを識別しやすくするために、これらのポリシーの説明には Fortinet 構成のホスト名が含まれています。

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、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 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 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。Firewall移行ツールのコンソールウィンドウが開いている限り、ログファイルとフォルダは削除できません。