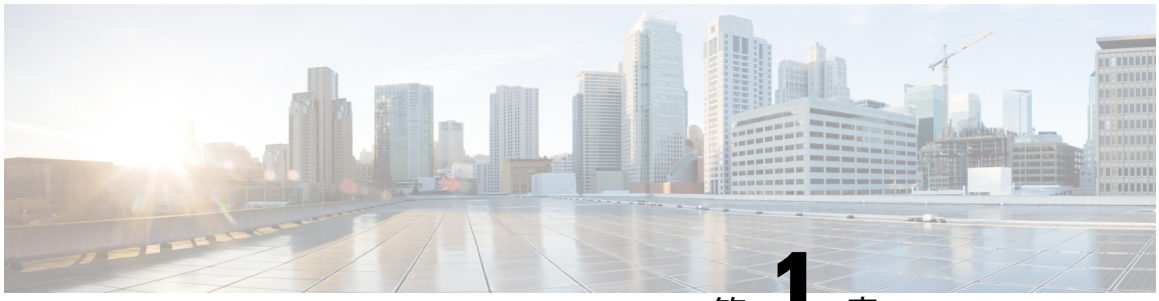
Cisco Defense Orchestrator の Firewall 移行ツールを使用したファイアウォールの移行

初版：2023 年 2 月 21 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

Cisco Defense Orchestrator の Firewall 移行ツールを使用したファイアウォールの移行

このドキュメントは、Cisco Defense Orchestrator（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際に役立ちます。

CDO は、CDO テナントに展開されているクラウド提供型 Firewall Management Center によって管理されている Secure Firewall Threat Defense デバイスに既存のファイアウォール構成を移行するために使用できる Cisco Secure Firewall 移行ツールのクラウドバージョンをホストします。

このガイドの対象読者

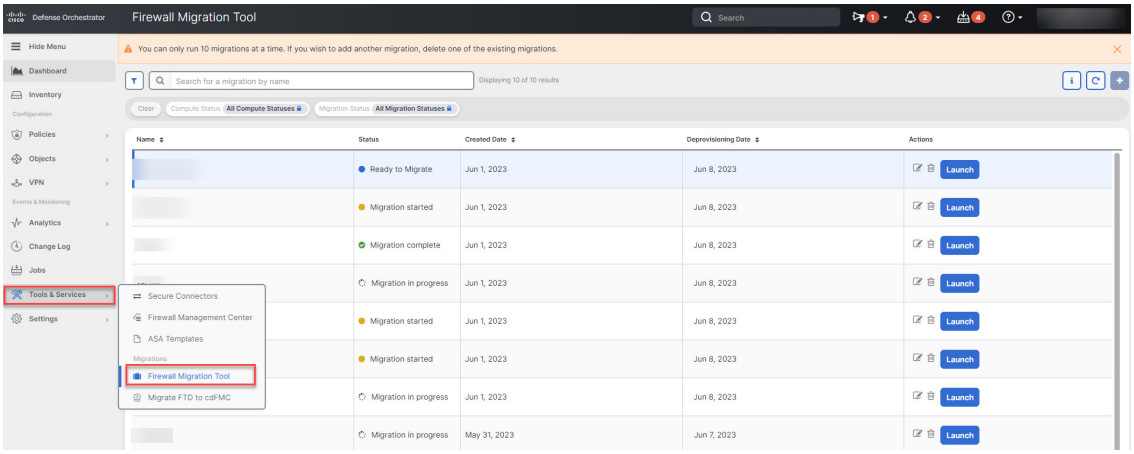
このガイドは、CDO を使用して Cisco Secure Firewall ASA デバイスと FDM 管理対象 Threat Defense デバイスを管理する場合、または Palo Alto Networks、Check Point、Fortinet ファイアウォールなどのサードパーティ製ファイアウォールを使用していて Cisco Secure Firewall Threat Defense に移行する場合に役立ちます。CDO の Cisco Secure Firewall 移行ツールを使用して、既存のすべてのファイアウォール構成を、クラウド提供型 Firewall Management Center によって管理されている Threat Defense デバイスに移行できます。このドキュメントでは、構成を移行するために必要な作業について説明します。

Cisco Defense Orchestrator の Firewall 移行ツールの開始

CDO の移行ツールは、選択した送信元デバイスまたはアップロードした構成ファイルからデバイス構成を抽出し、その構成を検証した後、CDO テナントにプロビジョニングされたクラウド提供型 Firewall Management Center に移行します。移行ツールは、ほとんどの構成をサポー

トしています。サポートされていない構成は、クラウド提供型 Firewall Management Center で手動で設定する必要があります。サポートされている構成 （2 ページ） を参照してください。

[ツールとサービス（Tools & Services）] > [Firewall移行ツール（Firewall Migration Tool）] で新しい移行を初期化して [起動（Launch）] を実行すると、移行ツールのクラウドインスタンスが新しいブラウザタブで開き、ガイド付きワークフローを使用して移行タスクを実行できます。CDO の移行ツールを使用すると、Cisco Secure Firewall 移行ツールのデスクトップバージョンをダウンロードして維持する必要がなくなります。



CDO でホストされている移行ツールを使用して、次のシスコとサードパーティのファイアウォール構成を Secure Firewall Threat Defense デバイスに移行できます。

- Cisco Secure Firewall ASA
- Firewall Device Manager で管理されている Secure Firewall Threat Defense
- Check Point ファイアウォール
- Palo Alto Networks ファイアウォール
- Fortinet ファイアウォール

重要 Firewall 移行ツールを使用するには、CDO の管理者またはネットワーク管理者のユーザーロールが必要です。

サポートされている構成

移行ツールは、次の構成をサポートしています。

- ネットワークオブジェクトおよびグループ
- サービスオブジェクト（送信元と接続先に設定されたものを除く）
- 参照される ACL および NAT ルール

- サービス オブジェクト グループ

（注） クラウド提供型 Management Center はネストをサポートしていないため、ネストされたサービス オブジェクト グループの内容は、移行される前に個々のオブジェクトに分割されます。

- IPv4 および IPv6 FQDN オブジェクトとグループ
- IPv6 変換（インターフェイス、スタティック ルート、オブジェクト、ACL、および NAT）
- 入力インターフェイスに適用されるアクセス ルール
- グローバル ACL
- 自動 NAT、手動 NAT、およびオブジェクト NAT
- スタティック ルート、等コスト マルチパス（ECMP）ルート、およびポリシー ベース ルーティング（PBR）
- 物理インターフェイス
- サブインターフェイス
- ポート チャネル
- 仮想トンネル インターフェイス
- トランスペアレント モードのブリッジ グループ
- IP SLA オブジェクト：移行ツールによって作成され、スタティック ルートにマッピングされ、移行されます。
- 時間ベースのオブジェクト
- サイト間 VPN
  - サイト間 VPN：Cisco Secure Firewall 移行ツールが送信元 ASA または FDM 管理対象デバイスでクリプトマップ構成を検出すると、それを Management Center VPN にポイントツーポイント トポロジとして移行します。
  - ASA および FDM 管理対象デバイスからのクリプトマップ（静的/動的）ベース VPN
  - ルートベース（VTI）の ASA および FDM VPN
  - ASA および FDM 管理対象デバイスからの証明書ベース VPN 移行

重要 送信元デバイスにサイト間 VPN 構成がある場合は、ASA および FDM 管理対象デバイスのトラストポイントまたは証明書がクラウド提供型 Firewall Management Center で手動で設定されていることを確認します。

- リモートアクセス VPN
  - SSL および IKEv2 プロトコル
  - 認証方式：[AAAのみ（AAA only）]、[クライアント証明書のみ（Client Certificate only）]、[SAML]、および [AAAとクライアント証明書（AAA and Client Certificate）]
  - AAA：Radius、ローカル、LDAP、および AD
  - 接続プロファイル、グループポリシー、ダイナミック アクセス ポリシー、LDAP 属性マップ、および証明書マップ
  - 標準および拡張 ACL
  - カスタム属性および VPN ロードバランシング

重要 送信元ファイアウォールでリモートアクセス VPN を設定している場合は、次のタスクが実行されていることを確認します。

- Management Center で ASA および FDM 管理対象デバイスのトラストポイントを PKI オブジェクトとして手動で設定する
- AnyConnect パッケージ、Hostscan ファイル（dap.xml、data.xml、hostscan パッケージ）、外部ブラウザパッケージ、および AnyConnect プロファイルを送信元 ASA および FDM 管理対象デバイスから取得する
- すべての AnyConnect パッケージおよびプロファイルを Management Center にアップロードする

- 動的ルートオブジェクト、BGP、および EIGRP
  - [ポリシー（Policy）] リスト
  - プレフィックス リスト
  - コミュニティリスト
  - 自律システム（AS）パス
  - ルート マップ

（注） 移行ツールは、名前と構成の両方に基づいてすべてのオブジェクトとオブジェクトグループを分析し、同じ名前と構成を持つオブジェクトを再利用しますが、リモートアクセス VPN 構成の XML プロファイルは名前のみを使用して検証されます。

ライセンス

Cisco Secure Firewall 移行ツールには、CDO からアクセスするための追加ライセンスは必要ありません。

ただし、移行する 脅威に対する防御 機能の CDO 基本サブスクリプションおよびライセンスが必要です。

新しい移行インスタンスの初期化

ステップ 1 CDO テナントにログインします。

ステップ 2 **[ツールとサービス（Tools & Services）] > [Firewall移行ツール（Firewall Migration Tool）]** を選択します。

ステップ 3 青色のプラスボタン  をクリックして、新しい移行インスタンスを初期化します。

（注） Firewall 移行ツールを使用すると、最大 10 個の移行を作成し、それらすべてを同時に起動できます。各移行インスタンスに新しいブラウザタブが開きます。ただし、テナントに複数のユーザーがプロビジョニングされている場合は、自分で作成した移行のみを起動できることに注意してください。

すでに 10 個の移行インスタンスがあるときに新しい移行インスタンスを初期化する場合は、既存の移行インスタンスのいずれかを削除します。

ステップ 4 CDO は移行の名前を自動的に生成します。自動生成された名前を使用するか、必要に応じて変更できます。

ステップ 5 [OK] をクリックし、ステータスが [初期化中（Initializing）] から [移行準備完了（Ready to Migrate）] に変わるまで待ちます。また、移行の準備が整うと、CDO は [通知（Notifications）] ペインに新しいアナウンスを表示します。

ステップ 6 新しい移行で、[起動（Launch）] をクリックします。

移行ツールは新しいブラウザタブで開き、認証は必要ありません。

（注） CDO での移行は、作成日から 7 日間有効で、その後は自動的にプロビジョニング解除されます。これにより、CDO リソースが随時解放されます。[作成日（Created Date）] 列と [プロビジョニング解除日（Deprovisioning Date）] 列で日付を確認できます。

CDO では、[ステータス（Status）] 列にすべての移行のステータスが表示されます。ステータスに基づいて移行をフィルタ処理できます。移行を選択して、作成日時、開始日時、送信元と接続先のデバイス名、作成者などの移行の詳細を右側のペインに表示することもできます。CDO テナントに複数のユーザーがプロビジョニングされている場合は、自分で作成した移行のみを起動できることに注意してください。

移行インスタンスの削除

CDO が自動的にプロビジョニング解除する前に、移行を手動でプロビジョニング解除する場合は、次の手順に従います。たとえば、移行タスクの完了後に移行を削除できます。

ステップ 1 **[ツールとサービス（Tools & Services）]** > **[Firewall移行ツール（Firewall Migration Tool）]** を選択します。
ステップ 2 削除する移行インスタンスで、[アクション（Actions）] ペインの [削除（Delete）] をクリックします。
ステップ 3 [削除（Delete）] をクリックしてアクションを確認します。

Cisco Defense Orchestrator で管理されている Cisco Secure Firewall ASA の移行

CDO の Cisco Secure Firewall 移行ツールを使用すると、CDO によって管理されているライブ ASA デバイスから、または ASA デバイスから抽出された構成ファイルを使用して、構成を移行できます。

ソース構成の選択

CDO から移行インスタンスを起動したら、[ソース構成の選択（Select Source Configuration）] で [Cisco ASA] を選択し、[移行の開始（Start Migration）] をクリックします。ASA 構成ファイルを手動でアップロードするか、[ASAへの接続（Connect to ASA）] ペインにリストされている CDO 管理対象 ASA デバイスのいずれかを選択できます。CDO 管理対象デバイスを選択する場合は、[構成ステータス（Configuration Status）] が [同期済み（Synced）] になっているデバイスのみが移行ツールに表示されることに注意してください。移行するデバイスがリストに表示されない場合は、デバイス構成の変更が最新であり、CDO と同期されているかどうかを確認します。複数のユーザーが同時に 1 つの ASA デバイスをソースデバイスとして選択でき、構成の抽出はシームレスに行われることに注意してください。移行ツールは、デバイス構成を解析し、解析された構成を含む概要を表示します。[Next] をクリックします。

ターゲットの選択（Select Target）

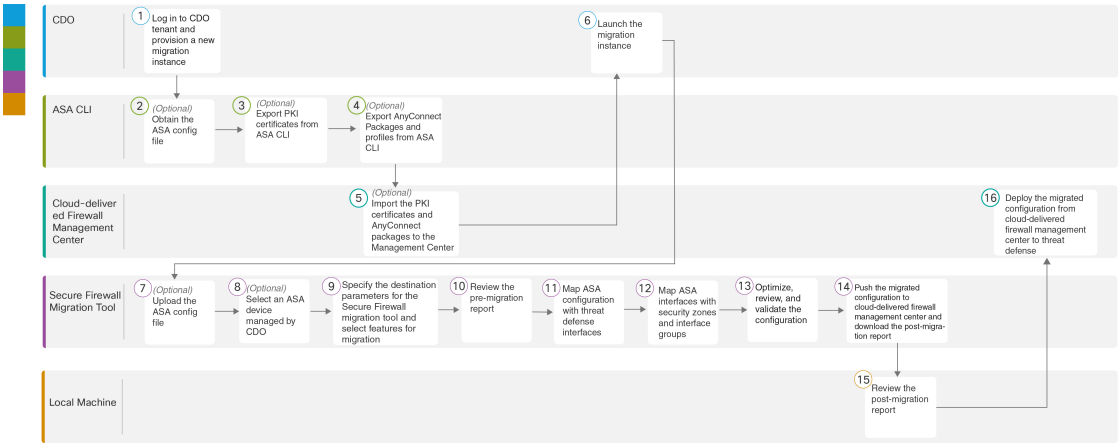
[ターゲットの選択（Select Target）] ページでは、CDO テナントでプロビジョニングされたクラウド提供型 Firewall Management Center がデフォルトで選択され、その Management Center によって管理されている 脅威に対する防御 デバイスが一覧表示されます。ASA 構成の移行先の脅威に対する防御 デバイスを選択するか、[FTDなしで続行（Proceed without FTD）] を選択できます。これらの Threat Defense デバイスは、デバイスが別の移行インスタンスで使用されているかどうかによって、[使用中（In Use）] または [使用可能（Available）] と表示されます。ただし、[デバイスステータスの変更（Change Device Status）] をクリックし、[使用中（In Use）] リストからデバイスを選択し、[続行（Continue）] をクリックすることでオーバーライドを実行できます。これにより、デバイスがターゲットとして選択できるようになります。

注意 デバイスのステータスを [使用中（In Use）] から [使用可能（Available）] に変更すると、すでにデバイスを使用している進行中の移行インスタンスに影響します。この操作を行う場合は、慎重に行うことを推奨します。

[FTDなしで続行（Proceed without FTD）] を選択すると、NAT オブジェクト、ACL、およびポートオブジェクトのみがクラウド提供型 Firewall Management Center にプッシュされます。一般的に使用される ASA 機能とそれに相当する Threat Defense 機能の詳細については、『Cisco Secure Firewall ASA to Threat Defense Feature Mapping』ガイドを参照してください。

次のフローチャートは、CDO の Firewall 移行ツールを使用して ASA を 脅威に対する防御 に移行するためのステップごとの手順を示しています。

図 *1 : CDO* の *Firewall* 移行ツールを使用した *ASA* から *FTD* への移行に関するエンドツーエンドの手順



	ワークスペース	手順
1	CDO	CDO テナントにログインし、**[ツールとサービス（Tools & Services）]** > **[Firewall移行ツール（Firewall Migration Tool）]** に移動し、青いプラスボタン をクリックして、新しい移行インスタンスのプロビジョニングを開始します。
2	ASA CLI	（オプション）ASA 構成ファイルを取得します。ASA CLI から ASA 構成ファイルを取得するには、「Obtain the ASA Configuration File」を参照してください。[ソース構成の選択（Select Source Configuration）] で CDO 管理対象 ASA デバイスを選択する場合は、ステップ 3 に進みます。

	ワークスペース	手順
3	ASA CLI	（オプション）ASA CLI から Public Key Infrastructure（PKI）証明書をエクスポートします。この手順は、サイト間 VPN およびリモートアクセス VPN 設定を ASA から Threat Defense に移行する予定がある場合にのみ必要です。ASA CLI から PKI 証明書をエクスポートするには、「Export PKI Certificate from ASA and Import into Management Center」を参照してください。デバイスにリモートアクセス VPN 設定がない場合、またはサイト間 VPN およびリモートアクセス VPN を移行する予定がない場合は、ステップ 7 に進みます。
4	ASA CLI	（オプション）ASA CLI から AnyConnect パッケージおよびプロファイルをエクスポートします。この手順は、リモートアクセス VPN 機能を ASA から Threat Defense に移行する予定がある場合にのみ必要です。AnyConnect パッケージおよびプロファイルを ASA CLI からエクスポートするには、「Retrieve AnyConnect Packages and Profiles」を参照してください。
5	クラウド提供型 Firewall Management Center	（オプション）PKI 証明書と AnyConnect パッケージを Management Center にインポートします。PKI 証明書を Management Center にインポートするには、「Export PKI Certificate from ASA and Import into Management Center」のステップ 2 および「Retrieve AnyConnect Packages and Profiles」を参照してください。
6	CDO	作成した移行インスタンスのステータスが [移行準備完了（Ready to Migrate）] であることを確認し、[起動（Launch）] をクリックします。Cisco Secure Firewall 移行ツールが新しいブラウザタブで開きます。
7	Cisco Secure Firewall 移行ツール	（オプション）ASA CLI から取得した ASA 構成ファイルをアップロードします。「Upload the ASA Configuration File」を参照してください。CDO で管理されている ASA デバイスから構成を移行する予定の場合は、ステップ 8 に進みます。
8	Cisco Secure Firewall 移行ツール	表示された、CDO テナントによって管理されている ASA デバイスのリストから、構成を移行するデバイスを選択します。
9	Cisco Secure Firewall 移行ツール	[ターゲットの選択（Select Target）] ページでは、CDO テナントでプロビジョニングされたクラウド提供型 Firewall Management Center がデフォルトで選択されています。
10	Cisco Secure Firewall 移行ツール	クラウド提供型 Firewall Management Center によって管理されている Threat Defense デバイスのリストからターゲットデバイスを選択するか、[FTDなしで続行（Proceed without FTD）] を選択して続行します。

	ワークスペース	手順
11	Cisco Secure Firewall 移行ツール	移行前レポートをダウンロードして、解析された構成の詳細なサマリーを確認します。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	**FTD インターフェイス**と ASA 構成をマッピングします。 ASA と Threat Defense デバイスの物理インターフェイスとポートチャネル インターフェイスの名前は必ずしも同じではないため、ASA インターフェイスのマッピング先のターゲット Threat Defense デバイスのインターフェイスを選択できます。詳細については、「Map ASA Configurations with Secure Firewall Device Manager Threat Defense Interfaces」を参照してください。
13	Cisco Secure Firewall 移行ツール	ASA インターフェイスを既存の Threat Defense 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、「Map ASA Interfaces to Security Zones and Interface Groups」を参照してください。
14	Cisco Secure Firewall 移行ツール	**構成の最適化、確認、検証**は慎重に行い、ACL、オブジェクト、NAT、インターフェイス、ルート、サイト間 VPN、およびリモートアクセス VPN ルールが、宛先の Threat Defense デバイス向けに設定されていることを確認します。「Optimize, Review and Validate the Configuration」を参照してください。
15	Cisco Secure Firewall 移行ツール	構成の検証が成功したら、クラウド提供型 Firewall Management Center に**構成をプッシュ**します。詳細については、「Push the Migrated Configuration to 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て確認します。移行後レポートに含まれる情報の詳細については、「Review the Post-Migration Report and Complete the Migration」を参照してください。
17	クラウド提供型 Firewall Management Center	新規に移行した構成を Threat Defense デバイスに展開します。

より詳細なステップで手順を実行する場合は、『Migrating Cisco Secure Firewall ASA to Threat Defense with the Migration Tool』ガイドの「Obtain the ASA Configuration File」に進みます。

Cisco Defense Orchestrator で管理されている FDM 管理対象デバイスの移行

構成ファイルを使用するか、CDO によって管理されている FDM 管理対象デバイスを選択するだけで、FDM 管理対象デバイスの構成を移行できます。

ソース構成の選択

CDO から移行インスタンスを起動した後、[ソース構成の選択（Select Source Configuration）] で [Cisco Secure Firewall Device Manager] を選択し、次のオプションのいずれかを選択します。

- [Firepower Device Managerの移行（共有構成のみ）（Migrate Firepower Device Manager (Shared Configurations Only)）]
- [Firepower Device Managerの移行（デバイスおよび共有構成を含む）（Migrate Firepower Device Manager (Includes Device & Shared Configurations)）]
- [Firepower Device Manager（デバイスおよび共有構成を含む）のFTDデバイス（新しいハードウェア）への移行（Migrate Firepower Device Manager (Includes Device & Shared Configurations) to FTD Device (New Hardware)）]

[続行（Continue）]をクリックすると、移行ツールを使用して、FDM管理対象デバイスの構成ファイルを手動でアップロードするか、CDOによって管理されているFDM管理対象デバイス（[FDMに接続（Connect to FDM）] ペインに一覧表示されます）のいずれかを選択できます。[次へ（Next）] をクリックします。

ターゲットの選択（Select Target）

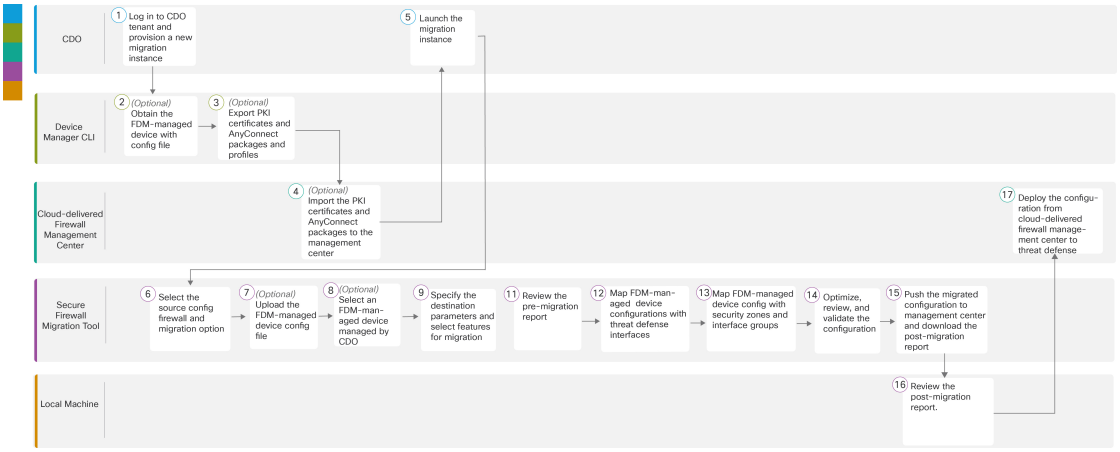
[ターゲットの選択（Select Target）] ページでは、CDO テナントでプロビジョニングされたクラウド提供型 Firewall Management Center がデフォルトで選択され、その Management Center によって管理されている 脅威に対する防御 デバイスが一覧表示されます。構成の移行先の 脅威に対する防御 デバイスを選択して、移行を続行します。

これらの Threat Defense デバイスは、デバイスが別の移行インスタンスで使用されているかどうかによって、[使用中（In Use）] または [使用可能（Available）] と表示されます。ただし、[デバイスステータスの変更（Change Device Status）] をクリックし、[使用中（In Use）] リストからデバイスを選択し、[続行（Continue）] をクリックすることでオーバーライドを実行できます。これにより、デバイスがターゲットとして選択できるようになります。

注意 デバイスのステータスを [使用中（In Use）] から [使用可能（Available）] に変更すると、すでにデバイスを使用している進行中の移行インスタンスに影響します。この操作を行う場合は、慎重に行うことを推奨します。

次のフローチャートは、CDO の Firewall 移行ツールを使用して FDM 管理対象デバイスを移行するためのステップごとの手順を示しています。

図 *2 : CDO* の *Firewall* 移行ツールを使用した *FDM* 管理対象デバイスから *FTD* への移行に関するエンドツーエンドの手順



	ワークスペース	手順
1	CDO	CDO テナントにログインし、**[ツールとサービス（Tools & Services）] > [Firewall移行ツール（Firewall Migration Tool）]** に移動し、青いプラスボタン をクリックして、新しい移行インスタンスのプロビジョニングを開始します。
2	デバイスマネージャ CLI	（オプション）FDM 管理対象デバイス構成ファイルを取得します。デバイスマネージャ CLI から FDM 管理対象デバイス構成ファイルを取得するには、「Obtain the FDM-Managed Device Configuration File」を参照してください。[ソース構成の選択（Select Source Configuration）] で CDO 管理対象 FDM デバイスを選択する場合は、ステップ 3 に進みます。
3	デバイスマネージャ CLI	（オプション）PKI 証明書と AnyConnect パッケージおよびプロファイルをエクスポートします。この手順は、サイト間 VPN およびリモートアクセス VPN 機能を FDM 管理対象デバイスから Threat Defense に移行する予定がある場合にのみ必要です。デバイスマネージャ CLI から PKI 証明書をエクスポートするには、「Export PKI Certificate from and Import into Firewall Management Center」のステップ 1 を参照してください。AnyConnect パッケージおよびプロファイルをデバイスマネージャ CLI からエクスポートするには、「Retrieve AnyConnect Packages and Profiles」のステップ 1 を参照してください。サイト間 VPN およびリモートアクセス VPN 構成を移行する予定がない場合は、ステップ 7 に進みます。
4	クラウド提供型 Firewall Management Center	（オプション）PKI 証明書と AnyConnect パッケージを Management Center にインポートします。PKI 証明書を Management Center にインポートするには、「Export PKI Certificate from and Import into Firewall Management Center」のステップ 2 および「Retrieve AnyConnect Packages and Profiles」を参照してください。

	ワークスペース	手順
5	CDO	作成した移行インスタンスのステータスが [準備完了（Ready）] であることを確認し、[起動（Launch）] をクリックします。Cisco Secure Firewall 移行ツールが新しいブラウザタブで開きます。
6	Cisco Secure Firewall 移行ツール	ソース構成のファイアウォールと移行オプションを選択するには、「Select the Source Configuration Firewall and Migration」を参照してください。
7	Cisco Secure Firewall 移行ツール	（オプション）デバイスマネージャ CLI から取得した FDM 管理対象デバイス構成ファイルをアップロードします。「FDM 管理対象デバイス構成ファイルのアップロード」を参照してください。CDO で管理されている FDM 管理対象デバイスから構成を移行する場合は、ステップ 8 に進みます。
8	Cisco Secure Firewall 移行ツール	表示された、CDO テナントによって管理されている FDM 管理対象デバイスのリストから、構成を移行するデバイスを選択します。
9	Cisco Secure Firewall 移行ツール	[ターゲットの選択（Select Target）] ページでは、CDO テナントでプロビジョニングされたクラウド提供型 Firewall Management Center がデフォルトで選択されています。
10	Cisco Secure Firewall 移行ツール	クラウド提供型 Firewall Management Center によって管理されている Threat Defense デバイスのリストからターゲットデバイスを選択するか、[FTDなしで続行（Proceed without FTD）] を選択して続行します。
11	Cisco Secure Firewall 移行ツール	移行前レポートをダウンロードして、解析された構成の詳細なサマリーを確認します。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	**FTD インターフェイス**と FDM 管理対象デバイス構成をマッピングします。 FDM と Threat Defense デバイスの物理インターフェイスとポートチャネル インターフェイスの名前は必ずしも同じではないため、FDM 管理対象デバイスインターフェイスのマッピング先のターゲット Threat Defense デバイスのインターフェイスを選択できます。詳細については、「Map FDM-managed Device Configurations with Secure Firewall Device Manager Threat Defense Interfaces」を参照してください。
13	Cisco Secure Firewall 移行ツール	FDM 管理対象デバイスインターフェイスを既存の Threat Defense 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、「Map FDM-managed Interfaces to Security Zones and Interface Groups」を参照してください。

	ワークスペース	手順
14	Cisco Secure Firewall 移行ツール	**構成の最適化、確認、検証**は慎重に行い、ACL、オブジェクト、NAT、インターフェイス、ルート、サイト間 VPN、およびリモートアクセス VPN ルールが、宛先の Threat Defense デバイス向けに設定されていることを確認します。「Optimize, Review and Validate the Configuration」を参照してください。
15	Cisco Secure Firewall 移行ツール	構成の検証が成功したら、クラウド提供型 Firewall Management Center に**構成をプッシュ**します。詳細については、「Push the Migrated Configuration to 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て確認します。移行後レポートに含まれる情報の詳細については、「Review the Post-Migration Report and Complete the Migration」を参照してください。
17	クラウド提供型 Firewall Management Center	新規に移行した構成を Threat Defense デバイスに展開します。

より詳細なステップで手順を実行する場合は、『Migrating an FDM-managed Device to Secure Firewall Threat Defense with the Migration Tool』ガイドの「Obtain the FDM-managed Device Configuration File」に進みます。

移行の再開

CDO から移行を開始し、後で続行する場合は、[Firewall移行ツール（Firewall migration tool）] タブを閉じることができます。移行を再開する場合は、CDO にログインし、[Firewall移行ツール（Firewall migration tool）] の再開する移行で [起動（Launch）] をクリックします。移行ツールは、移行が実行中だったことを検出するため、中断したところから続行できます。ただし、移行ツールが進行中の移行を検出するには、少なくともソース構成の解析までを実行する必要があります。このステップを実行する前に移行を中断した場合でも、CDO から同じ移行を開始できますが、最初から行う必要があります。

関連資料

CDO の Cisco Secure Firewall 移行ツールを使用したサードパーティ製ファイアウォールの移行の詳細については、要件に基づいて次のドキュメントを参照してください。

- Firewall 移行ツールに関する最新の機能とリリース固有の情報については、『Cisco Secure Firewall Migration Tool Release Notes』を参照してください。

（注） Cisco Defense Orchestrator は、Cisco Secure Firewall 移行ツールの最新バージョンをホストしています。

- Check Point ファイアウォールの構成を Threat Defense に移行するには、『Migrating a Check Point Firewall to Threat Defense』ガイドの「Export the Check Point Configuration Files」を参照してください。
- Palo Alto Networks ファイアウォールの構成を Threat Defense に移行するには、『Migrating a Palo Alto Networks Firewall to Threat Defense』ガイドの「Export the Configuration from Palo Alto Networks Firewall」を参照してください。
- Fortinet ファイアウォールの構成を Threat Defense に移行するには、『Migrating a Fortinet Firewall to Threat Defense』ガイドの「Export the Configuration from Fortinet Firewall」を参照してください。

重要 ASA および FDM 管理対象デバイスの移行とは異なり、サードパーティ製ファイアウォール構成を Threat Defense に移行する場合は、手動で抽出した構成ファイルのみをアップロードできます。

Cisco Secure Firewall 移行ツールとすべての関連ドキュメントに関する全体的な情報については、『Cisco Secure Firewall Migration Tool』を参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。