Threat Defense 2100 への ASA の移行：例

ASA から Firewall Threat Defense 2100 への移行：例

（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。

メンテナンスウィンドウの前に次のタスクを実行する

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。

手順

ステップ 1 移行する ASA デバイスまたはコンテキストに対して **show running-config** コマンドを使用し、ASA 構成のコピーを保存します。「View the Running Configuration」を参照してください。

または、移行する ASA デバイスまたはコンテキストに対して Adaptive Security Device Manager（ASDM）を使用し、**[ファイル（File）] > [新しいウィンドウに実行構成を表示する（Show Running Configuration in New Window）]** を選択して、構成ファイルを取得します。

（注） マルチコンテキスト ASA の場合は、**show tech-support** コマンドを使用して、すべてのコンテキストの構成を単一ファイルに取得できます。

Threat Defense 2100 への ASA の移行：例

ステップ 2 ASA 構成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 ASA 構成にポートチャネルがある場合は、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 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 Firewall 移行ツールのダウンロード」を参照してください。

ステップ 7 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、「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。

ステップ 8 ASA インターフェイスを Threat Defense インターフェイスにマッピングします。

（注） Firewall 移行ツールでは、ASA インターフェイスタイプを Threat Defense 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、ASA のポートチャネルを Threat Defense 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、「ASA インターフェイスと 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、 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 ASA 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、「ASA 論理インターフェイスとセキュリティゾーンおよびインターフェイス グループへのマッピング」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 Threat Defense に展開し、移行を完了します。

詳細については、「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。

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。

メンテナンスウィンドウ中に次のタスクを実行する

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。「メンテナンスウィンドウの前に次のタスクを実行する （1 ページ）」を参照してください。

手順

ステップ 1 SSH コンソールを介して ASA に接続し、インターフェイス構成モードに切り替えます。

ステップ 2 **shutdown** コマンドを使用して、ASA 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、Firepower 2100 シリーズ デバイスの動的ルーティングを構成します。

詳細については、「Dynamic Routing」を参照してください。

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、ASA デバイスに割り当てられた 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。

メンテナンスウィンドウ中に次のタスクを実行する