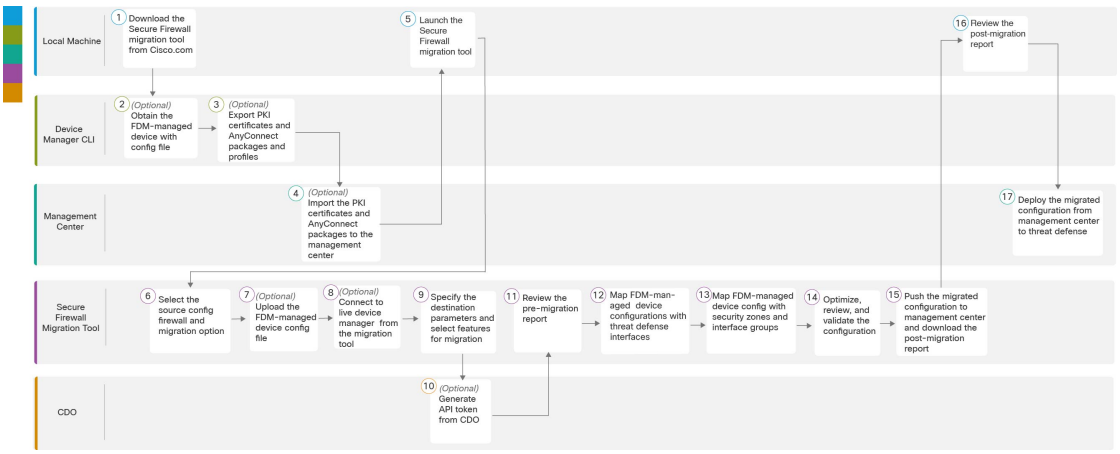
FDM 管理対象デバイスから Threat Defense へのワークフロー

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、FDM 管理対象デバイスを 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。

	ワークスペース	手順
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する：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、「FDM 管理対象デバイス構成ファイルの取得」を参照してください。Cisco Secure Firewall 移行ツールから FDM 管理対象デバイスに接続する場合は、ステップ 3 にスキップします。
3	デバイスマネージャ CLI	（オプション）PKI 証明書および AnyConnect パッケージとプロファイルをエクスポートする：この手順は、サイト間 VPN および RA VPN 機能を FDM 管理対象デバイスから Threat Defense に移行することを計画してい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、「デバイスマネージャからの PKI 証明書のエクスポートと Firewall Management Center へのインポート」を参照してください。AnyConnect パッケージと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、「AnyConnect パッケージとプロファイルの取得」を参照してください。サイト間 VPN および RA VPN を移行する予定がない場合は、手順 7 にスキップします。
4	Management Center	（オプション）PKI 証明書と AnyConnect パッケージを管理センターにインポートする：PKI 証明書を管理センターにインポートするには、「デバイスマネージャからの PKI 証明書のエクスポートと Firewall Management Center へのインポート」および「AnyConnect パッケージとプロファイルの取得」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	Cisco Secure Firewall 移行ツール	送信元構成ファイアウォールと移行オプションを選択するには、「ソース設定とデバイスマネージャ移行オプションの選択」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 構成バンドルのアップロード」を参照してください。ライブ FDM 管理対象デバイスに接続することを計画している場合は、ステップ 8 にスキップします。
8	Cisco Secure Firewall 移行ツール	Cisco Secure Firewall 移行ツールから直接、ライブデバイスマネージャに接続できます。詳細については、「Cisco Secure Firewall 移行ツールから FDM 管理対象デバイスへの接続」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	（オプション）この手順はオプションであり、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、FDM 管理対象デバイス構成を 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、「FDM 管理対象デバイス構成と 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。
13	Cisco Secure Firewall 移行ツール	FDM 管理対象デバイス 構成が正しく移行されるように、FDM 管理対象デバイス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。手順の詳細については、「セキュリティゾーンインターフェイスグループ への FDM 管理対象デバイス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、「移行する構成の最適化、確認および検証」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、「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、「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

FDM 管理対象デバイス 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。

FDM 管理対象デバイス構成ファイルの取得

FDM 管理対象デバイス構成ファイルを取得するには、次のいずれかの方法を使用できます。

- FDM 管理対象デバイス構成ファイルのエクスポート （4 ページ）
- Cisco Secure Firewall 移行ツールから FDM 管理対象デバイスへの接続 （17 ページ）

FDM 管理対象デバイス構成ファイルのエクスポート

このタスクは、FDM 管理対象デバイス構成ファイルを手動でアップロードする場合にのみ必要です。デバイスマネージャの構成ファイルは、Threat Defense API を使用してエクスポートできます。構成をエクスポートすると、ZIP ファイルが作成されます。ZIP ファイルは、ローカ

ルワークステーションにダウンロードできます。構成自体は、JSON 形式のテキストファイルで属性と値のペアを使用して定義されたオブジェクトとして表されます。

エクスポートを実行する場合は、どの構成をエクスポートファイルに含めるかを指定します。完全エクスポートには、エクスポート zip ファイル内のすべての構成が含まれます。

エクスポート zip ファイルには、次のものが含まれる場合があります。

- 設定された各オブジェクトを定義する属性と値のペア。デバイスマネージャで「オブジェクト」と呼ばれるものだけに限らず、構成可能な項目はすべて、オブジェクトとしてモデル化されます。
- リモートアクセス VPN、AnyConnect パッケージおよびその他の参照ファイル（クライアントプロファイル XML ファイル、DAP XML ファイル、Hostscan パッケージなど）。
- カスタムファイルポリシーを設定した場合は、すべての参照済みクリーンリストまたはカスタム検出リスト。

ステップ 1 エクスポート用の JSON オブジェクト本体を作成します。

例：

JSON オブジェクトの例を次に示します。

```
  "diskFileName": "string",
  "encryptionKey": "*********",
  "doNotEncrypt": false,
  "configExportType": "FULL_EXPORT",
  "deployedObjectsOnly": true,
  "entityIds": [
    "string"
  ],
  "jobName": "string",
  "type": "scheduleconfigexport"
}
```

属性は次のとおりです。

- diskFileName：（任意）エクスポート zip ファイルの名前。名前を指定しない場合、デフォルトでシステムによって名前が生成されます。名前を指定した場合でも、一意性を確保するために名前に文字が付加される場合があります。名前の最大長は 60 文字です。
- encryptionKey：zip ファイルの暗号化キー。ファイルを暗号化しない場合は、このフィールドをスキップして、代わりに **doNotEncrypt": true** を指定します。キーを指定する場合は、キーをローカルマシンにダウンロードした後に、キーを使用して zip ファイルを開く必要があります。エクスポートされた構成ファイルでは、秘密鍵、パスワード、およびその他の機密データがクリアテキストで公開されます（そうしないと、インポートできません）。この場合、機密データを保護するために暗号化キーを適用することができます。システムでは AES 256 暗号化が使用されます。
- doNotEncrypt：（任意）エクスポートファイルを暗号化するか（false）または暗号化しないか（true）。デフォルトは false です。つまり、空でない暗号化キー属性を指定する必要があります。true を指定すると、暗号化キー属性は無視されます。

- configExportType：構成ファイルをエクスポートするために、次のエクスポートタイプのいずれかを選択できます。
  - FULL_EXPORT：エクスポートファイルに構成全体を含めます。**これはデフォルトのオプションであり、移行のために選択する必要があります。**

- deployedObjectsOnly：（任意）オブジェクトが展開されている場合にのみ、それらのオブジェクトをエクスポートファイルに含めるかどうか。デフォルトは false です。これは、すべての保留中の変更がエクスポートに含まれることを意味します。保留中の変更を除外するには、true を指定します。

- entityIds：[カッコ] で囲まれた、一連の開始ポイントオブジェクトの ID をカンマで区切ったリスト。このリストは PARTIAL_EXPORT ジョブでは必須です。リスト内の各項目には、UUID 値か、または "id=uuid-value"、"type=object-type"、"name=object-name" などのパターンと一致する属性と値のペアのいずれかを指定できます。たとえば、"type=networkobject" などを指定できます。
  - type は、networkobject などのリーフエンティティ、または一連のリーフタイプのエイリアスのいずれかになります。通常の type エイリアスの例としては、network（NetworkObject と NetworkObjectGroup）、port（すべての TCP/UDP/ICMP ポート、プロトコル、およびグループ タイプ）、url（URL オブジェクトおよびグループ）、ikepolicy（IKE V1/V2 ポリシー）、ikeproposal（Ike V1/V2 プロポーザル）、identitysource（すべてのアイデンティティ ソース）、certificate（すべての証明書タイプ）、object（デバイスマネージャの [オブジェクト（Objects）] ページにリストされるすべてのオブジェクト/グループタイプ）、interface（すべてのネットワーク インターフェイス）、s2svpn（すべてのサイト間 VPN 関連タイプ）、ravpn（すべての RA VPN 関連タイプ）、vpn（s2svpn と ravpn の両方）などがあります。
  - オブジェクトとそれらから送出される参照子孫はすべて、PARTIAL_EXPORT の出力ファイルに含まれます。エクスポート不可能なオブジェクトはすべて、ID を指定した場合でも、出力から除外されます。適切なリソースタイプに対して GET メソッドを使用し、ターゲットオブジェクトの UUID、タイプ、または名前を取得します。

  たとえば、すべてのネットワークオブジェクトと、myaccessrule という名前のアクセスルール、および、UUID で識別される 2 つのオブジェクトをエクスポートする場合、次のように指定できます。

```
"entityIds": [
   "type=networkobject",
   "id=bab3e3cd-8c70-11e9-930a-1f12ee87d473",
   "name=myaccessrule",
   "acc2e3cd-8c70-11e9-930a-1f12ee87b286"
   ]",
```

- jobName：（任意）エクスポートジョブに名前を付けると、ジョブのステータスを取得するときに見つけやすくなります。

- type：ジョブのタイプは常に **scheduleconfigexport** です。

ステップ 2 オブジェクトをポストします。

例：

curl コマンドは次のようになります。

```
curl -X POST --header 'Content-Type: application/json' --header 'Accept: application/json' -d '{
```

```
 \
   "configExportType": "FULL_EXPORT", \
   "type": "scheduleconfigexport" \
}' 'https://10.89.5.38/api/fdm/latest/action/configexport'
```

ステップ 3 応答を確認します。

取得する応答コードは 200 である必要があります。最低限の JSON オブジェクトをポストした場合、正常な応答本文は次のようになります。

```
{
  "version": null,
  "scheduleType": "IMMEDIATE",
  "user": "admin",
  "forceOperation": false,
  "jobHistoryUuid": "c7a8ba61-629a-11e9-8b8d-0fcc3c9d6d0b",
  "ipAddress": "10.24.5.177",
  "diskFileName": "export-config-1",
  "encryptionKey": null,
  "doNotEncrypt": true
  "configExportType": "FULL_EXPORT",
  "deployedObjectsOnly": false,
  "entityIds": null,
  "jobName": "Config Export",
  "id": "c79be920-629a-11e9-8b8d-85231be77de0",
  "type": "scheduleconfigexport",
  "links": {
    "self": "https://10.89.5.38/api/fdm/latest
/action/configexport/c79be920-629a-11e9-8b8d-85231be77de0"
  }
}
```

ステップ 4 構成のエクスポートの状態を確認します。

エクスポートが完了するには多少時間がかかります。構成が大きいほど、ジョブに必要な時間が長くなります。ジョブのステータスをチェックし、ファイルをダウンロードする前に正常に完了していることを確認します。

ステータスを取得するには、**GET /jobs/configexportstatus** を使用する方法が最も簡単です。たとえば、curl コマンドは次のようになります。

```
curl -X GET --header 'Accept: application/json'
'https://10.89.5.38/api/fdm/latest/jobs/configexportstatus'
```

正常に完了したジョブには、次のステータスが表示されます。

```
{
  "version": "hdy62yf5xp3vf",
  "jobName": "Config Export",
  "jobDescription": null,
  "user": "admin",
  "startDateTime": "2019-04-19 13:14:54Z",
  "endDateTime": "2019-04-19 13:14:56Z",
  "status": "SUCCESS",
  "statusMessage": "The configuration was exported successfully",
  "scheduleUuid": "1ef502ad-62a5-11e9-8b8d-074ebc750708",
  "diskFileName": "export-config-1.zip",
  "messages": [],
  "configExportType": "FULL_EXPORT",
  "deployedObjectsOnly": false,
  "entityIds": null,
  "id": "1f0aad8e-62a5-11e9-8b8d-bb1ebb4d1300",
  "type": "configexportjobstatus",
```

```
  "links": {
    "self": "https://10.89.5.38/api/fdm/latest
/jobs/configexportstatus/1f0aad8e-62a5-11e9-8b8d-bb1ebb4d1300"
  }
}
```

ステップ 5 エクスポートファイルをダウンロードします。

エクスポートジョブが完了すると、エクスポートファイルがシステムディスクに書き込まれ、構成ファイルと呼ばれます。このエクスポートファイルは、**GET /action/downloadconfigfile/{objId}** を使用してローカルマシンにダウンロードできます。

使用可能なファイルのリストを取得するには、GET /action/configfiles メソッドを使用します。

```
curl -X GET --header 'Accept: application/json'
'https://10.89.5.38/api/fdm/latest/action/configfiles'
```

応答には項目のリストが表示され、これらはそれぞれが構成ファイルです。たとえば、次のリストは 2 つのファイルを示しています。すべてのファイルの ID はデフォルトであり、ID を無視して代わりに diskFileName を使用するのがベストプラクティスです。

```
{
  "items": [
    {
      "diskFileName": "export-config-2.zip",
      "dateModified": "2019-04-19 13:32:28Z",
      "sizeBytes": 10182,
      "id": "default",
      "type": "configimportexportfileinfo",
      "links": {
        "self": "https://10.89.5.38/api/fdm/latest/action/configfiles/default"
      }
    },
    {
      "diskFileName": "export-config-1.zip",
      "dateModified": "2019-04-19 13:14:56Z",
      "sizeBytes": 10083,
      "id": "default",
      "type": "configimportexportfileinfo",
      "links": {
        "self": "https://10.89.5.38/api/fdm/latest/action/configfiles/default"
      }
    }
  ],
```

diskFileName をオブジェクト ID として使用し、ファイルをダウンロードします。

```
curl -X GET --header 'Accept: application/octet-stream'
'https://10.89.5.38/api/fdm/latest/action/downloadconfigfile/export-config-2.zip'
```

ファイルは、デフォルトのダウンロードフォルダにダウンロードされます。API エクスプローラから GET メソッドを発行していて、ダウンロード場所を指定するよう求めるようにブラウザが設定されている場合は、ファイルを保存するよう求められます。

（注）　正常にダウンロードされると、戻りコードが 200 となり、応答本文はなくなります。

デバイスマネージャからの PKI 証明書のエクスポートと Firewall Management Center へのインポート

Cisco Secure Firewall 移行ツールは、証明書ベースの VPN の管理センターへの移行をサポートしています。

インポートされた FDM 管理対象デバイス構成バンドルには、キーとともに証明書ペイロードが含まれています。これは管理センターにインポートできます

インポート先の管理センターで、移行前アクティビティの一環として、トラストポイントまたは VPN 証明書を PKI オブジェクトとして手動で移行します。このアクティビティは、Cisco Secure Firewall 移行ツールを使用した移行を開始する前に実行する必要があります。

ステップ 1 構成バンドルから、証明書ペイロード（-----BEGIN CERTIFICATE----- と -----END CERTIFICATE----- の間の値）とキー（BEGIN RSA PRIVATE KEY----- と -----END RSA PRIVATE KEY----- の間の値）をコピーします。

例：


```
   "type":"identitywrapper",
   "action":"CREATE",
   "data":{
      "version":"girr7veykdjvx",
      "name":"RA_VPN_Cert",
      "cert":"-----BEGIN
[redacted]
 CERTIFICATE-----",
      "privateKey":"-----BEGIN RSA PRIVATE
[redacted]
 RSA PRIVATE KEY-----",
      "issuerCommonName":"mojave-rsa-root-2048-sha384.cisco.com, CN =
mojave-rsa-root-2048-sha384.cisco.com",
      "issuerCountry":"US",
      "issuerOrganization":"Cisco",
      "subjectCommonName":"fdm-ra-vpn-cert.cisco.com, CN = 172.16.10.50",
      "subjectCountry":"US",
      "subjectDistinguishedName":" C = US, O = Cisco, CN = fdm-ra-vpn-cert.cisco.com, CN =
172.16.10.50",
      "subjectOrganization":"Cisco",
      "validityStartDate":"Jan  1 12:00:00 2012 GMT",
      "validityEndDate":"Sep  1 12:00:00 2034 GMT",
      "isSystemDefined":false,
      "keyType":"RSA",
      "keySize":2048,
      "allowWeakCert":false,
      "signatureHashType":"SHA1",
      "weakCertificate":true,
      "id":"9d0a8efb-01fa-11ed-8d7b-1f4809c453ac",
      "type":"internalcertificate"
   }
}
```


ステップ 2 PKI 証明書を管理センターにインポートします（**[オブジェクト管理（ObjectManagement）]** > **[PKIオブジェクト（PKIObjects）]**）。

詳細については、『Firewall Management Center Configuration Guide』[英語] を参照してください。

手動で作成した PKI オブジェクトは、Cisco Secure Firewall 移行ツールの [VPNトンネル（VPN Tunnels）] セクションの [確認と検証（Review and Validate）] ページで使用できます。

AnyConnect パッケージとプロファイルの取得

始める前に

AnyConnect プロファイルはオプションであり、管理センターまたは Cisco Secure Firewall 移行ツールを介してアップロードできます。

- 管理センターのリモートアクセス VPN には、1 つ以上の AnyConnect パッケージが必要です。
- 構成が Hostscan と外部ブラウザパッケージで構成されている場合は、これらのパッケージをアップロードする必要があります。
- 移行前のアクティビティの一環として、すべてのパッケージを管理センターに追加する必要があります。
- Dap.xml と Data.xml は、Cisco Secure Firewall 移行ツールを介して追加する必要があります。

デバイスマネージャでダウンロード可能なパッケージを確認します。

ステップ 1 デバイスマネージャでダウンロード可能なパッケージを確認します。

GET /object/anyconnectpackagefiles API を使用して、デバイス上のパッケージを表示できます。

```
curl -X GET --header 'Accept: application/json' '
 https://10.89.5.38/api/fdm/v6/object/anyconnectpackagefiles'
```

このコマンドは、デバイスマネージャで使用可能な AnyConnect パッケージを取得します。

```
{
  "items": [
    {
      "version": "gx5yk7xkdsosu",
      "name": "anyconnect-win-4.10.02086-webdeploy-k9.pkg",
      "md5Checksum": "63e4a86fc7c68d7769b6a1b2976ffa73",
      "description": null,
      "diskFileName": "12f0988e-01fb-11ed-8d7b-07ecdd54c7bf.pkg",
      "platformType": "WINDOWS",
      "id": "133f2dbf-01fb-11ed-8d7b-89d64ab04e18",
      "type": "anyconnectpackagefile",
      "links": {
        "self": "
https://10.89.5.38/api/fdm/v6/object/anyconnectpackagefiles/133f2dbf-01fb-11ed-8d7b-89d64ab04e18"
      }
    }
  ],
}
```

応答からの diskFilename は、AnyConnect パッケージをダウンロードするために使用されます。

ステップ 2 AnyConnect パッケージをダウンロードします。

GET /action/downloaddiskfile/{objId} を使用して、AnyConnect パッケージをローカルワークステーションにダウンロードできます。使用されるオブジェクト ID は、AnyConnect パッケージの応答の diskFileName（12f0988e-01fb-11ed-8d7b-07ecdd54c7bf.pkg）です。

```
curl -X GET --header 'Accept: application/octet-stream'
' https://10.89.5.38/api/fdm/v6/action/downloaddiskfile/12f0988e-01fb-11ed-8d7b-07ecdd54c7bf.pkg'
```

ステップ 3 デバイスマネージャで使用可能な AnyConnect プロファイルを確認します。

（注） AnyConnect プロファイルは、Cisco Secure Firewall 移行ツールによってデバイスマネージャから自動的に取得されます。この手順は、AnyConnectプロファイルを手動でアップロードする場合にのみ必要です。

GET /object/anyconnectclientprofiles を使用して、デバイスマネージャで使用可能なプロファイルを確認できます。

```
curl -X GET --header 'Accept: application/json'
'https://10.196.155.3:12272/api/fdm/v6/object/anyconnectclientprofiles'
```

次の応答が表示されます。

```
  "items": [

    {
      "version": "jqtwzirf36qke",
      "name": "AnyConnect_VPN_Profile",
      "md5Checksum": "e4ba581f84daec6f24c209f9f7f9e1fb",
      "description": null,
      "diskFileName": "1629395a-0384-11ed-8d7b-ab1a2a5ad583.xml",
      "anyConnectModuleType": "ANY_CONNECT_CLIENT_PROFILE",
      "id": "1754c10b-0384-11ed-8d7b-6b8e36ae1285",
      "type": "anyconnectclientprofile",
    }
  ]
}
```

応答からの diskFilename は、AnyConnect プロファイルをダウンロードするために使用されます。

ステップ 4 AnyConnect プロファイルをダウンロードします。

GET /action/downloaddiskfile/{objId} を使用して、AnyConnect パッケージをローカルワークステーションにダウンロードできます。使用される objId は、AnyConnect プロファイルの応答からの diskFileName（1629395a-0384-11ed-8d7b-ab1a2a5ad583.xml）です。

```
curl -X GET --header 'Accept: application/octet-stream'
'https://10.196.155.3:12272/api/fdm/v6/action/downloaddiskfile/1629395a-0384-11ed-8d7b-ab1a2a5ad583.xml'
```

ステップ 5 ダウンロードしたパッケージを管理センターにインポートします（**[オブジェクト管理（ObjectManagement）]** > **[VPN]** > **[AnyConnectファイル（AnyConnect File）]**）。

1. Dap.xml と Data.xml は、Cisco Secure Firewall 移行ツールの **[確認と検証（Review and Validate）]** > **[リモートアクセスVPN（Remote Access VPN）]** > **[AnyConnectファイル（AnyConnect File）]** セクションから管理センターにアップロードする必要があります。

2. AnyConnect プロファイルは、管理センターに直接アップロードするか、または Cisco Secure Firewall 移行ツールの **[確認と検証（Review and Validate）]** > **[リモートアクセスVPN（Remote Access VPN）]** > **[AnyConnectファイル（AnyConnect File）]** セクションを介してアップロードできます。

手動でアップロードされたファイルが Cisco Secure Firewall 移行ツールで使用できるようになりました

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、「FDM 設定バンドルのアップロード」に進みます。

（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。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。

- FDM 管理対象デバイス構成をコンピュータにエクスポートした場合は、「FDM 構成バンドルのアップロード」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 デバイスやデモ FTD デバイスなどのデモのソースデバイスとターゲットデバイスを選択して、デモ移行の実行を進められます。

⚠

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。

また、実際の移行ワークフローと同様に、移行前レポートのダウンロードと確認、インターフェイスのマッピング、セキュリティゾーンのマッピング、インターフェイスグループのマッピングなどのすべて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。

ソース設定とデバイスマネージャ移行オプションの選択

ステップ 1 ドロップダウンリストから [送信元ファイアウォールベンダー（Source Firewall Vendor）] を選択し、[移行の開始（Start Migration）] をクリックします。

ステップ 2 FDM 管理対象デバイスを移行する移行オプションを選択します。

使用可能なオプションは次のとおりです。

- [Firepower Device Managerの移行（共有構成のみ）（Migrate Firepower Device Manager (Shared Configurations only)）]

  このオプションにより、デバイスマネージャから移行先の管理センターへの共有構成の移行が可能になります。共有構成が最初に移行され、後でデバイス構成を移行できるように、このオプションは段階的な移行に使用する必要があります。このユースケースにはダウンタイムはありません。

- [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 and Shared Configurations)）]

  このオプションにより、共有構成およびデバイス構成を移行先の管理センターに移行できます。この移行の一環として、送信元の脅威防御がデバイスマネージャから管理センターに移動されます。移行が正常に完了すると、管理センターは引き続き脅威防御デバイスを管理します。したがって、このユースケースでは、送信元と移行先は同じ脅威防御デバイスです。このユースケースでは、脅威防御デバイスが管理センターに移動するため、ダウンタイムが発生します。

  このオプションを使用して構成を移行するには、移行前のアクティビティの一部として次を実行します。

  1. デバイスマネージャにログインし、[オブジェクト（Objects）] セクションに移動します。
  2. [IDソース（Identity Sources）] をクリックし、[プリセットフィルタ（Preset filters）] から [ADレルム（AD Realm）] を選択します。
  3. [アクション（Actions）] で、暗号化タイプが [LDAPS] または [STARTTLS] である特定のレルムの [編集（Edit）]（✎） をクリックします。
  4. [ディレクトリサーバー構成（Directory Server Configuration）] で、サーバー名の横にあるドロップダウン矢印をクリックします。
  5. [暗号化セクション（Encryption Section）] で、暗号化タイプを [なし（NONE）] に変更し、[OK] をクリックします。
  6. 変更を展開します。

（注） 構成が管理センターに移行されたら、管理センターの AD レルムの暗号化タイプを LDAPS または STARTTLS に戻すことができます。詳細な手順については、「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。

- [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 and Shared Configurations) to FTD Device (New Hardware)）]

  このオプションにより、FDM 管理対象デバイス構成を、移行先の管理センターにすでに登録されている脅威防御に移行できます。送信元 FDM 管理対象デバイスの構成は、移行先の管理センターに登録されているユーザーが選択した移行先脅威防御に移行されます。このユースケースにはダウンタイムはありません。

FDM 構成バンドルのアップロード

始める前に

送信元デバイスマネージャから構成バンドルを `.zip` としてエクスポートします。

（注） 手動アップロードは、以下の 2 つのオプションでサポートされます。

- [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)）]
- [Firepower Device Managerの移行（共有構成のみ）（Migrate Firepower Device Manager (Shared Configurations Only)）]

ステップ 1 [FDM情報の抽出（Extract FDM Information）] 画面の [手動アップロード（Manual Upload）] セクションで、[アップロード（Upload）] をクリックして FDM 管理対象構成バンドルをアップロードします。構成バンドルが暗号化されている場合は、Cisco Secure Firewall 移行ツールのテキストボックスにキーを入力し、バンドルを復号化します。

ステップ 2 FDM 管理対象デバイス構成ファイルの場所を参照し、[開く（Open）] をクリックします。

Cisco Secure Firewall 移行ツールが構成バンド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 FDM 管理対象デバイス構成など、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、Cisco Secure Firewall 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。

ステップ 3 [解析を開始（Start Parsing）] をクリックします。

[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 4 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 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

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

Cisco Secure Firewall 移行ツールから FDM 管理対象デバイスへの接続

始める前に

Cisco Secure Firewall 移行ツールは、移行する FDM 管理対象デバイスに接続し、必要な構成情報を抽出できます。FDM管理対象デバイスへのライブ接続は、3つのユースケースすべてでサポートされています。

- Cisco Secure Firewall 移行ツールをダウンロードして起動します。
- FDM 管理対象デバイスから管理センターに移行するために実行するユースケースを選択します。
- デバイスマネージャの管理 IP アドレス、管理者資格情報を取得します。

ステップ 1 [FDM情報の抽出（Extract FDM Information）] 画面の [FDMへの接続（Connect to FDM）] セクションで、[接続（Connect）] をクリックして、移行する FDM 管理対象デバイスに接続します。

ステップ 2 [FDMログイン（FDM Login）] 画面で、次の情報を入力します。

1. [FDM IPアドレス/ホスト名（FDM IP Address/Hostname）] フィールドに、FDM の管理 IP アドレスまたはホスト名を入力します。[ログイン（Login）] をクリックします。
2. [ユーザー名（Username）]、[パスワード（Password）] フィールドに、適切な管理者用のログイン資格情報を入力します。
3. [ログイン（Login）] をクリックします。

Cisco Secure Firewall 移行ツールが FDM 管理対象デバイスに接続すると、移行を続行する前に、一連のコンプライアンスチェックが FDM 管理対象デバイスで実行されます。これらのチェックについては、前提条件とベストプラクティスのセクションで説明しています。チェックが成功すると、移行は次のステップに進みます。

Cisco Secure Firewall 移行ツールが FDM 管理対象デバイスに接続し、コンプライアンスチェックが成功すると、構成情報の抽出を開始します。抽出が正常に完了すると、解析された概要ページが表示されます。

[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 FDM 管理対象デバイスから、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

- オンプレミス Firewall Management Center の Management Center の IP アドレスを取得します。
- （任意） 選択したフローが [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)）] の場合、ターゲット Threat Defense デバイスを管理センターに追加します 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。

[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)）] を選択した場合は、選択したドメインで使用可能な Threat Defense 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。

[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)）] を選択した場合は、選択したドメインで使用可能な Threat Defense デバイスにのみ移行できます。

[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

このワークフローでは、管理センターの [Threat Defense] セクションは設定されません。共有ポリシー（アクセス制御リスト、NAT、およびオブジェクト）のみがFMCにプッシュされます。管理センターにプッシュする必要がある共有ポリシーを含めるかスキップするかを選択できます。

[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)）] を選択した場合

管理センターに移動される Threat Defense は、デバイスマネージャによって管理されているのと同じデバイスです。この場合、管理センターの Threat Defense 部分は設定されません。

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、 FDM 管理対象デバイス 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） 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。

- [FTD を使用せず続行（Proceed without FTD）] 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 のデバイス固有の校正であるインターフェイスとルート、およびサイト間 VPN は移行されず、Management Center で手動で構成する必要があります。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、FDM管理対象デバイス 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、[デバイス設定（Device Configuration）]、[共有構成（Shared Configuration）]、および [最適化（Optimization）] セクションで、FDM管理対象デバイス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） [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、[デバイス設定（Device Configuration）] セクションは使用できません。

- Cisco Secure Firewall 移行ツールでは、移行中に次のアクセス制御がサポートされています。
  - 宛先セキュリティゾーンの指定：移行中の ACL の宛先ゾーンのマッピングを有効にします。

    ルートルックアップロジックは静的ルートと接続ルートに限定される一方、PBR、動的ルート、および NAT は考慮されません。インターフェイス ネットワーク構成は、接続ルート情報を取得するために使用されます。

    送信元および接続先のネットワーク 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ことがあります。

- • ディープインスペクションの調整：カプセル化トラフィックの場合に、ファストパス処理でのパフォーマンスを向上させます。
  • パフォーマンスの向上：早期処理のメリットがあるその他の接続についても、ファストパスやブロックをすることができます。

  Cisco Secure Firewall 移行ツールは、送信元構成でカプセル化されたトンネルトラフィックルールを識別し、プレフィルタトンネルルールとして移行します。プレフィルタポリシーで移行されたトンネルルールを確認できます。プレフィルタポリシーは、Management Center で移行されたアクセス コントロール ポリシーに関連付けられます。

  プレフィルタトンネルルールとして移行されるプロトコルは次のとおりです。

  • GRE（47）
  • IPv4 カプセル化（4）
  • IPv6 カプセル化（41）
  • Teredo トンネリング（UDP:3544）

  （注） プレフィルタオプションを選択しない場合、すべてのトンネルトラフィックルールがサポートされていないルールとして移行されます。

  FDM 管理対象デバイス 構成の ACL トンネルルール（GRE および IPnIP）は、現在、デフォルトで双方向として移行されます。アクセスコントロールの状態オプションで、接続先のルール方向を双方向または単方向に指定できるようになりました。

- Cisco Secure Firewall 移行ツールは、VPN トンネル移行用に次のインターフェイスとオブジェクトをサポートしています。
  • ポリシーベース（暗号マップ）：ターゲット Management Center と 脅威に対する防御 がバージョン 6.6 以降の場合
  • ルートベース（VTI）：ターゲット Management Center と 脅威に対する防御 がバージョン 6.7 以降の場合

- 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、 FDM 管理対象デバイス 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。

- （任意）[最適化（Optimization）] セクションで、脅威に対する防御 のアクセスポリシーによる最適なメモリ使用率を実現する場合は、[オブジェクトグループの検索（Object group search）] を選択します。
- 移行元の FDM 管理対象デバイスにプラットフォーム設定、ファイル、およびマルウェアポリシーがある場合、移行ツールはそれらを [機能の選択（Select Features）] ページの [共有設定（Shared Configuration）] の下にある [プラットフォーム設定（Platform Settings）] および [デバイス設定（Device Configuration）] の下にある [ファイルおよびマルウェアポリシー（File and Malware Policy）] として表示します。これらのチェックボックスはデフォルトで選択されていることに注意してください。

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。

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、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。

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。

- [全体のサマリー（Overall Summary）]：FDM 管理対象デバイス 構成情報を抽出するため、またはライブ FDM 管理対象デバイス 構成に接続するために使用される方法。

  脅威に対する防御 に正常に移行できるサポート対象 FDM 管理対象デバイス 構成要素と、移行対象として選択された特定の 機能のサマリー。

ライブ FDM 管理対象デバイスに接続している場合、サマリーにはヒットカウント情報（FDM 管理対象デバイス ルールが検出された回数とそのタイムスタンプ情報）が含まれます。

- [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 の構成要素の詳細。 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てから、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、続行してください。
- [部分的なサポート構成（Partially Supported Configuration）]：部分的にのみ移行可能な FDM 管理対象デバイス 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 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、 Cisco Secure Firewall 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。
- [未サポートの構成（Unsupported Configuration）]：Cisco Secure Firewall 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 FDM 管理対象デバイス 構成要素の詳細。これらの行を確認し、各機能が 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、 Cisco Secure Firewall 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。
- [無視される構成（Ignored Configuration）]： Management Center または Cisco Secure Firewall 移行ツールでサポートされていないために無視される FDM 管理対象デバイス 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 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。

Management Center と 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、『Management Center Configuration Guide』[英語] 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 で修正を完了し、 FDM 管理対象デバイス 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 FDM 管理対象デバイス 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。

次のタスク

FDM 管理対象デバイス構成と Threat Defense インターフェイスのマッピング

FDM 管理対象デバイス構成と 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、FDM 管理対象デバイス 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、Cisco Secure Firewall 移行ツールは、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 FDM 管理対象デバイス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、 FDM 管理対象デバイス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。

FDM 管理対象デバイス 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 FDM 管理対象デバイス 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（FDM 管理対象デバイス 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 FDM 管理対象デバイス 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（FDM 管理対象デバイス 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 FDM 管理対象デバイス 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 （18 ページ）」を参照してください。

（注） [Firepower Device Managerの移行（共有構成のみ）（Migrate Firepower Device Manager (Shared Configurations Only)）] を使用して移行する場合、この手順は適用されません。

この手順は、**[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)）]** の情報提供のみを目的とした手順です。

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、**[FTDインターフェイス名（FTD Interface Name）]** のドロップダウンリストをクリックし、その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FDM管理対象デバイス 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、 FDM 管理対象デバイス 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 FDM 管理対象デバイス 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。

セキュリティゾーンインターフェイスグループ への FDM 管理対象デバイスインターフェイスのマッピング

（注） FDM 管理対象デバイス 構成にアクセスリストと NAT ルールが含まれていない場合、またはこれらのポリシーを移行しない場合は、この手順をスキップして「」に進むことができます。移行する構成の最適化、確認および検証 （27 ページ）

FDM管理対象デバイス構成が正しく移行されるように、FDM管理対象デバイス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 にマッピングします。 FDM 管理対象デバイス 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、『*Cisco Secure Firewall Management Center Device Configuration Guide*』の「Security Zones and Interface Groups」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 FDM 管理対象デバイス 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、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、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 4 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 FDM 管理対象デバイス 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、FDM 管理対象デバイス インターフェイスと同じモードがあります。たとえば、 FDM 管理対象デバイス 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 5 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。

移行する構成の最適化、確認および検証

FDM 管理対象デバイス構成の場合、構成はさまざまな方法で検証され、選択した移行フローによって異なります。各種オプションで行われる構成の検証は次のとおりです。

- [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)）]：デバイスと共有構成の両方が 1 つのフローで確認および検証されます。
- [Firepower Device Managerの移行（共有構成のみ）（Migrate Firepower Device Manager (Shared Configurations Only)）]：共有構成のみが確認および検証されます。
- [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)）]：共有構成とデバイス構成が個別のフローで検証されます。

共有構成の最適化、確認および検証

移行した FDM 構成を管理センターにプッシュする前に、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。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。

[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） FDM 管理対象デバイスでは 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。

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) 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。

b) 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。

c) **[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 最適化、 [構成の確認と検証（Review and Validate Configuration）] 画面で、[アクセス制御ルール（Access Control Rules）] をクリックし、次の手順を実行します。

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 ルール番号を追加することで、FDM 管理対象デバイス構成ファイルにマッピングしやすくします。たとえば、FDM 管理対象デバイス 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。

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) 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。

[ファイルポリシー（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、[保存（Save）] をクリックします。

d) 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 ポリシー（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、[保存（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。

[ログ（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、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。

[ルールアクション（Rule Action）] ダイアログの [アクション（Actions）] ドロップダウンで、[ACP] タブまたは [プレフィルタ（Prefilter）] タブを選択できます。

- ACP：アクセスコントロールルールには、システムが一致するトラフィックをどのように処理し、ログに記録するのかを指定するアクションがあります。アクセスコントロールルールに対して許可、信頼、モニタ、ブロック、またはリセット付きブロックのいずれかのアクションを実行できます。このリストには、ACL に関連付けられたマルウェアおよびファイルポリシーも含まれます。これらの ACL は、移行、適用、または変更しないことを選択できます。
- Prefilter：ルールのアクションによって、一致したトラフィックの処理とログ記録の方法が決まります。ファストパスとブロックを実行できます。

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。

ポリシーのキャパシティと制限の警告：Cisco Secure Firewall 移行ツールは、移行したルールの合計 ACE カウントを、ターゲット プラットフォームでサポートされている ACE 制限と比較します。

Cisco Secure Firewall 移行ツールは比較の結果に基づいて、移行された ACE の総数がしきい値を超えた場合や、ターゲットデバイスのサポートされている制限のしきい値に近づいている場合は、視覚インジケータと警告メッセージを表示します。

ルールが [ACE カウント（ACE Count）] 列を超える場合は、最適化することも、移行しないことを決定することもできます。移行を完了してからこの情報を使用して、Management Center でプッシュしてから展開するまでの間に、ルールを最適化することもできます。

（注） Cisco Secure Firewall 移行ツールは、警告があっても移行をブロックしません。

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。

g) [侵入ポリシー（Intrusion Policy）] では、すべての侵入ポリシーと対応する基本ポリシー、存在するカスタムルール/オーバーライドされたルール、侵入モード、およびACPの参照が表示されます。また、Snort 3 の Snort エンジンと NAP ポリシーも表示します。

管理センターの API 制限により、ルールが上書きされた Snort 2 ポリシーは無視されます。

デフォルト設定の侵入ポリシーは、管理センターで再利用されます。

Snort 3 のオーバーライドされたルール/カスタムルールまたは Snort3/Snort2 の侵入モード検出を含む侵入ポリシーの新しいポリシーは、ポリシー名 _<FDM ホスト名> で作成されます

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 ルール（NAT Rules）]
- [オブジェクト（Objects）]（[アクセスリストオブジェクト（Acess List Objects）]、[ネットワークオブジェクト（Network Objects）]、[ポートオブジェクト（Port Objects）]、[VPNオブジェクト（VPN Objects）]、および[動的ルートオブジェクト（Dynamic-Route-Objects）]）
- [インターフェイス（Interfaces）]
- [ルート（Routes）]
- [サイト間 VPN トンネル（Site-to-Site VPN Tunnels）]
- [リモートアクセス VPN（Remote Access VPN）]

アクセスリストオブジェクトには、BGP、EIGRP、および RA VPN で使用される標準 ACL と拡張 ACL が表示されます。

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、[ポートオブジェクト（Port Objects）] タブ、または [VPNオブジェクト（VPN 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、ポートオブジェクト、またはVPN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 [リモートアクセスVPN（Remote Access VPN）] セクションでは、リモートアクセス VPN に対応するすべてのオブジェクトが FDM 管理対象デバイスから管理センターに移行され、次のように表示されます。

- **Anyconnect ファイル**：AnyConnect パッケージ、Hostscan ファイル（Dap.xml、Data.xml、Hostscan Package）、外部ブラウザパッケージ、およびAnyConnectプロファイルは、送信元FDM管理対象デバイスから取得する必要があり、また、移行に使用できる必要があります。

  移行前のアクティビティの一環として、すべてのAnyConnectパッケージを管理センターにアップロードします。AnyConnectプロファイルは、管理センターに直接アップロードしたり、Cisco Secure Firewall 移行ツールからアップロードしたりできます。

  管理センターから取得した既存の Anyconnect、Hostscan、または外部ブラウザパッケージを選択します。1 つ以上の AnyConnect パッケージを選択する必要があります。送信元の構成で使用可能な場合は、Hostscan、dap.xml、data.xml、または外部ブラウザを選択する必要があります。AnyConnect プロファイルはオプションです。

  dap.xml は、FDM 管理対象デバイスから取得した正しいファイルである必要があります。検証は、構成ファイルで使用可能な dap.xml で実行されます。検証に必要なすべてのファイルをアップロードして選択する必要があります。更新に失敗すると不完全とマークされ、Cisco Secure Firewall 移行ツールは検証に進みません。

- [AAA]：Radius、LDAP、AD、LDAP、SAML、およびローカルレルムタイプの認証サーバーが表示されます。すべての AAA サーバーのキーを更新します。Cisco Secure Firewall 移行ツール 3.0 以降、Live Connect FDM 管理対象デバイスの事前共有キーは自動的に取得されます。**more system: running-config** ファイルを使用して、隠しキーを含む送信元の構成をアップロードすることもできます。AAA 認証キーをクリアテキスト形式で取得するには、次の手順を実行します。

  （注） これらの手順は、Cisco Secure Firewall 移行ツールの外部で実行する必要があります。

  1. SSH コンソールを介して FDM 管理対象デバイスに接続します。
  2. *more system:running-config* コマンドを入力します。
  3. **aaa-server and local user** セクションに移動してクリアテキスト形式のすべての AAA 構成と対応するキー値を見つけます。

```
ciscoFDM#more system:running-config
!
aaa-server Test-RADIUS (inside) host 2.2.2.2
key <key in clear text> <-----The radius key is now displayed in clear text format. aaa-server
 Test-LDAP (inside) host 3.3.3.3
ldap-login-password <Password in clear text> <-----TheLDAP/AD/LDAPS password is now displayed
 in clear text format.
```

```
username Test_User password <Password in clear text> <-----The Local user password is shown
 in clear text.
```

（注） ローカルユーザーのパスワードが暗号化されている場合は、パスワードを内部で確認するか、または Cisco Secure Firewall 移行ツールで新しいパスワードを構成できます。

- LDAPS では、管理センターにドメインが必要です。暗号化タイプ LDAPS のドメインを更新する必要があります。
- AD サーバーの Management Center には、一意の AD プライマリドメインが必要です。一意のドメインが識別されると、Cisco Secure Firewall 移行ツールに表示されます。競合が見つかった場合、オブジェクトを正常にプッシュするには、一意の AD プライマリドメインを入力する必要があります。

  暗号化が LDAPS に設定されている AAA サーバーの場合、FDM 管理対象デバイスは IP とホスト名またはドメインをサポートしますが、管理センターはホスト名またはドメインのみをサポートします。FDM管理対象デバイス構成にホスト名またはドメインが含まれている場合、それらが取得されて表示されます。FDM 管理対象デバイス構成に LDAPS の IP アドレスが含まれている場合は、[リモートアクセスVPN（Remote Access VPN）] の下の [AAA] セクションにドメインを入力します。AAA サーバーの IP アドレスに解決できるドメインを入力する必要があります。

  タイプが AD の AAA サーバー（サーバータイプは FDM 管理対象デバイス構成で Microsoft）の場合、[ADプライマリドメイン（AD Primary Domain）] は管理センターで構成する必須フィールドです。このフィールドはFDM管理対象デバイスでは個別に構成されず、FDM管理対象デバイスのLDAP-base-dn構成から抽出されます。

  ```
  If the ldap-base-dn is: ou=Test-Ou,dc=gcevpn,dc=com
  ```

  [ADプライマリドメイン（AD Primary Domain）] は、プライマリドメインを形成する dc、dc=gcevpn、dc=com で始まるフィールドです。AD プライマリドメインは gcevpn.com になります。

  LDAP-base-dn のサンプルファイル：

  ```
  cn=FDM,OU=ServiceAccounts,OU=abc,dc=abc,dc=com:
  ```

  ここで、dc=abc と dc=com が abc.com として結合され、AD プライマリドメインが形成されます。

  ```
  cn=admin, cn=users, dc=fwsecurity, dc=cisco, dc=com:
  ```

  AD プライマリドメインは fwsecurity.cisco.com です。

  AD プライマリドメインは自動的に取得され、Cisco Secure Firewall 移行ツールに表示されます。

  （注） AD プライマリドメインの値は、レルムオブジェクトごとに一意である必要があります。競合が検出された場合か、または Firewall 移行ツールが FDM 管理対象デバイス構成で値を見つけられない場合は、特定のサーバーの AD プライマリドメインを入力するように求められます。AD プライマリドメインを入力して構成を検証します。

- [アドレスプール（Address Pool）]：すべての IPv4 プールと IPv6 プールがここに表示されます。
- [グループポリシー（Group-Policy ）]：このセクションには、クライアントプロファイル、管理プロファイル、クライアントモジュール、およびプロファイルのないグループポリシーを含むグループポリシーが表示されます。プロファイルが [AnyConnect ファイル（AnyConnect file）] セクションに追加

されている場合は、事前に選択された状態で表示されます。ユーザープロファイル、管理プロファイル、およびクライアント モジュール プロファイルを選択または削除できます。

- [接続プロファイル（Connection Profile）]：すべての接続プロファイル/トンネルグループがここに表示されます。
- [トラストポイント（Trustpoint）]：FDM 管理対象デバイスから管理センターへのトラストポイントまたは PKI オブジェクトの移行は、移行前アクティビティの一環であり、RA VPN の移行を正常に実行するために不可欠です。[リモート アクセス インターフェイス（Remote Access Interface）] セクションでグローバル SSL、IKEv2、およびインターフェイスのトラストポイントをマッピングして、移行の次の手順に進みます。LDAPS プロトコルが有効になっている場合、グローバル SSL と IKEv2 トラストポイントは必須です。SAML オブジェクトが存在する場合、SAML IDP と SP のトラストポイントを SAML セクションでマッピングできます。SP 証明書はオプションです。特定のトンネルグループについては、トラストポイントをオーバーライドすることもできます。オーバーライドされた SAML トラストポイント構成が送信元 FDM 管理対象デバイスで使用可能な場合は、[SAMLのオーバーライド（Override SAML）] オプションで選択できます。

  FDM 管理対象デバイスからの PKI 証明書のエクスポートについては、「FDM 管理対象デバイス構成ファイルのエクスポート」を参照してください。
- [証明書マップ（Certificate Maps）]：ここに証明書マップが表示されます。

ステップ 6 [SNMP] タブでは、次のタブを確認、検証、および操作できます。

ASA デバイスに SNMPV1/V2 または SNMPV3 設定があるかどうかに基づいて、設定は [SNMPV1/V2] タブまたは [SNMPV3] タブに表示されます。

SNMPV1/V2：

- [ホストサーバー名（Host Server Name）]：SNMP ホストの名前
- [IPアドレス（IP Address）]：SNMP ホストの IP アドレス
- [コミュニティストリング（Community String）]：手動で指定する必要がある SNMP コミュニティストリング。ホストを選択し、**[アクション（Actions）] > [コミュニティストリングの更新（Update Community String）]** に移動して、コミュニティストリングを指定します。これは、SNMP サービスに設定されたコミュニティまたはユーザ名と同じである必要があります。
- [検証状態（Validation State）]：ターゲット管理センターで作成されるホストサーバーの検証状態

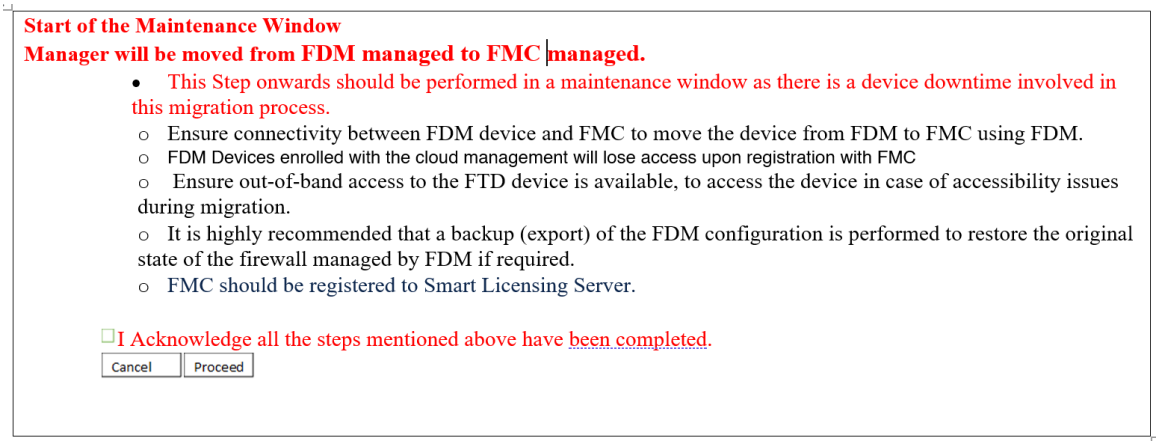
SNMPV3：

- [ユーザー名（User Name）]：SNMP ホストのユーザー名
- [認証パスワード（Authentication Password）]：[アクション（Actions）] をクリックして、ユーザーの認証パスワードを指定します
- [暗号化パスワード（Encryption Password）]：[アクション（Actions）] をクリックして、ユーザーのプライバシーパスワードを指定します

• [検証状態（Validation State）]：ターゲット管理センターで作成されるユーザーの検証状態

メンテナンスの開始とマネージャの移動

共有構成がプッシュされたら、ポップアップを受け入れてメンテナンスウィンドウに移動する必要があります。



[マネージャの移動（Move Manager）] ページでは、次の詳細を指定する必要があります。

• [FTDがNATデバイスの背後にある（FTD is behind NAT Device）]、[FMCがNATデバイスの背後にある（FMC is behind NAT Device）]、[NATの背後にデバイスがない（No Device is behind NAT）]（デフォルト設定）のいずれかを選択します

• [Management Center/CDOホスト名またはIPアドレス（Management Center/CDO Hostname or IP Address）]：すべての詳細がターゲットのマネージャから取得されます。必要に応じて IP を変更できます。

（注） [FMCがNATデバイスの背後にある（FMC is behind NAT Device）] の場合、フィールドは無視されます。

• [Management Center/CDO登録キー（Management Center/CDO Registration Key）]：マネージャの移動中に使用される一意の登録キーを指定する必要があります。

• [NAT ID]：（オプション）。Threat Defense または管理センターが NAT デバイスの背後にある場合に必要です。

• [Threat Defense（FTD）ホスト名（Threat Defense (FTD) Hostname）]：Threat Defense IP/ホスト名は、FDM 管理対象デバイス構成から取得されます。ユーザーは、必要に応じて IP を変更できます。[FTDがNATデバイスの背後にある（FTD is behind NAT Device）] の場合、フィールドは無視されます。

- [DNSサーバーグループ（DNS Server Group）]：デバイスマネージャと管理センター間の接続に使用される DNS サーバーグループ。
- [Management Center/CDOアクセスインターフェイス（データ/管理）（Management Center/CDO Access Interface (Data/Management)）]：マネージャを移動するためのデータ/管理インターフェイスのいずれかを選択します。データインターフェイスは、データインターフェイスを介して適切なルートが構成されている場合にのみサポートされます。

[マネージャの移動（Move Manager）] を選択すると、Cisco Secure Firewall 移行ツールによって、デバイスマネージャから管理センターへのマネージャの移動がトリガーされます。マネージャを移動すると、デバイスマネージャからデバイスにアクセスできなくなります。

移行するデバイス構成の最適化、確認および検証

ステップ 1 次のタブを選択し、構成項目を確認します

- [インターフェイス（Interfaces）]
- [ルート（Routes）]
- [サイト間 VPN トンネル（Site-to-Site VPN Tunnels）]

[動的ルートオブジェクト（Dynamic-Route-Objects）] セクションには、移行されるすべてのサポートされているオブジェクトが表示されます。

- ポリシーリスト
- プレフィックスリスト
- ルートマップ
- コミュニティ リスト
- AS パス
- アクセス リスト

ステップ 2 [ルート（Routes）] セクションには、次のルートが表示されます。

- [スタティック（Static）]：すべての IPv4 および IPv6 スタティックルートを表示します。
- [BGP]：すべての BGP ルートを表示します。
- [EIGRP]：すべての EIGRP ルートを表示します。EIGRP では、more system:running 構成がアップロードされ、キーが暗号化されていない場合、認証キーが取得されます。ソース構成でキーが暗号化されている場合は、EIGRP のインターフェイスセクションでキーを手動で指定できます。認証タイプ（暗号化、非暗号化、認証、またはなし）を選択し、それに応じてキーを指定できます

ステップ 3 確認が完了したら、[検証（Validate）] をクリックします。

検証中、Cisco Secure Firewall 移行ツールは管理センターに接続し、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管理センターに存在する場合、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、管理センター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 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) [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、[検証ステータス（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、[移行された構成を管理センターにプッシュする（Push the Migrated Configuration to Management Center）] に進みます。

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 FDM 管理対象デバイス 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 FDM 管理対象デバイス構成を Management Center に送信します。

Cisco Secure Firewall 移行ツールの新しい最適化機能を使用すると、検索フィルタを使用して移行結果を迅速に取得できます。

Cisco Secure Firewall 移行ツールは、CSV ダウンロードを最適化し、ページビューごとにまたはすべてのルールにアクションを適用することもできます。

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。

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、を参照してください。移行する構成の最適化、確認および検証 （27 ページ）

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、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。

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、 FDM 管理対象デバイス構成がどのように移行されたかを理解します。

- Migration Summary：ASA FDM 管理対象デバイス から 脅威に対する防御 正常に移行された構成の概要。 FDM 管理対象デバイス インターフェイス、Management Center ホスト名とドメイン、ターゲット 脅威に対する防御 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。
- FDM Migration Path：以下の 3 つの移行フローのうち、どのオプションが選択されたかを示します。
  - [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)）]

- Selective Policy Migration：移行用に選択された特定の FDM 管理対象デバイス 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。

- FDM-managed device Interface to Threat Defense Interface Mapping：正常に移行されたインターフェイスの詳細と、 FDM 管理対象デバイス 構成のインターフェイスを 脅威に対する防御 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 脅威に対する防御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 Threat Defense Security Zones and Interface Groups：正常に移行された FDM 管理対象デバイス 論理インターフェイスと名前の詳細、およびそれらを 脅威に対する防御 の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：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 FDM 管理対象デバイス 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 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：Cisco Secure Firewall 移行ツールで移行しないように選択したルールの詳細。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。

- 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 FDM 管理対象デバイス ルールの詳細。これらの行を確認し、詳細オプションが 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：Cisco Secure Firewall 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 FDM 管理対象デバイス 構成要素の詳細。これらの行を確認し、各機能が 脅威に対する防御 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、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 FDM 管理対象デバイス Point ルールから複数の 脅威に対する防御 ルールに拡張された FDM 管理対象デバイス 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**

- Access Rules You Chose Not to Migrate：Cisco Secure Firewall 移行ツールで移行しないように選択した FDM 管理対象デバイス 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：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、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 FDM 管理対象デバイス 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 脅威に対する防御 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 FDM 管理対象デバイス 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 脅威に対する防御 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：Cisco Secure Firewall 移行ツールを使用して「ログ設定」が変更された FDM 管理対象デバイス 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 脅威に対する防御 によってブロックされるように、Management Center でルールを構成することを推奨します。

（注） [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、移行前に管理センター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管理センター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。

Management Center と 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、『Management Center Configuration Guide, Version 6.2.3』[英語] を参照してください。

ステップ 3 **移行前レポート**を開き、脅威に対する防御 デバイスで手動で移行する必要がある FDM 管理対象デバイス構成項目をメモします。

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

a) 脅威に対する防御 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
- IP SLA オブジェクト
- オブジェクトグループの検索
- 時間ベースのオブジェクト
- サイト間 VPN トンネル
- 動的ルートオブジェクト

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、『Management Center Configuration Guide』[英語] 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 アクセスと HTTPS アクセスを含む）（「Threat Defense プラットフォーム設定」を参照）
- Syslog 設定（「Configure Syslog」を参照）
- 動的ルーティング（「Routing Overview for Threat Defense」を参照）
- サービスポリシー（「FlexConfig Policies」を参照）
- VPN 構成（「Threat Defense VPN」を参照）
- 接続ログ設定（「Connection Logging」を参照）

移行前に AD レルムの暗号化を変更した場合は、以下の手順に従って暗号化タイプを LDAPS または STARTTLS に戻します。

1. [統合（Integration）] セクションに移動し、[その他の統合（Other Integrations）] をクリックします。
2. [レルム（Realms）] を選択し、特定のレルムの横にある [編集（Edit）]（✎）をクリックして、暗号化タイプを変更します。
3. [ディレクトリ（Directory）] をクリックし、暗号化タイプを [LDAPS] または [STARTTLS] に変更します。
4. 変更を保存して展開します。

ステップ 5 確認が完了したら、Management Center から 脅威に対する防御 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。

Cisco Secure Firewall 移行ツールは、ポリシーを脅威に対する防御デバイスに割り当てます。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 FDM 管理対象デバイス 構成のホスト名が含まれています。

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： FDM 管理対象デバイス 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 FDM 管理対象構成を取得するか、FDM 管理対象デバイスに接続して構成をフェッチします。

ステップ 2 FDM 管理対象デバイス 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 FDM 管理対象デバイス 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 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 （18 ページ）を参照してください。

ステップ 8 FDM 管理対象デバイス 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、 FDM 管理対象デバイス 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、FDM管理対象デバイスのポートチャネルを 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、「 FDM 管理対象デバイス構成と 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、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 FDM 管理対象デバイス 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インターフェイスグループへのFDM管理対象デバイス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、「移行する構成の最適化、確認および検証 （27 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 （43 ページ）」を参照してください。

ステップ 1 SSH コンソールを介して FDM 管理対象デバイスに接続し、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、FDM 管理対象デバイス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、 FDM 管理対象デバイス 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。

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。