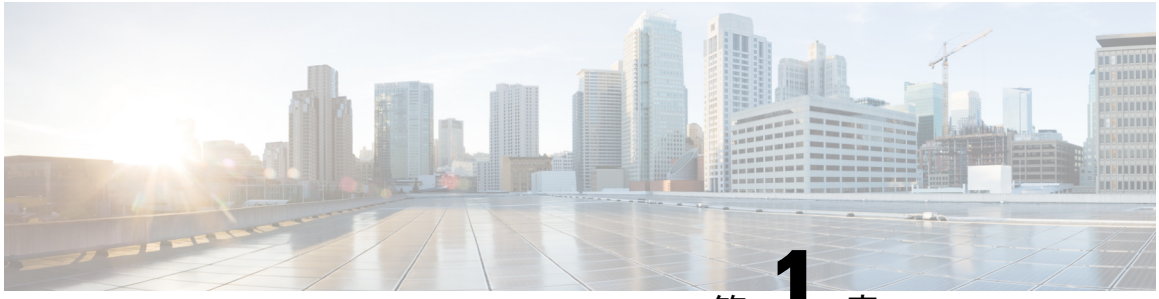
Cisco Firepower 1010 スタートアップガイド

初版：2019 年 6 月 13 日

最終更新：2023 年 4 月 24 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/



第 1 章

最適なオペレーティングシステムとマネージャを見つける方法

ハードウェアプラットフォームは、2 つのオペレーティングシステムのいずれかを実行できます。オペレーティングシステムごとに、マネージャを選択できます。この章では、オペレーティングシステムとマネージャの選択肢について説明します。

- オペレーティングシステム （1 ページ）
- マネージャ （2 ページ）

オペレーティングシステム

ハードウェア プラットフォームでは、Cisco Secure Firewall ASA または Secure Firewall Threat Defense（旧 Firepower Threat Defense） オペレーティングシステムを使用できます。

- ASA：ASA は、従来の高度なステートフル ファイアウォールおよび VPN コンセントレータです。

  Threat Defense の高度な機能が必要ない場合、または Threat Defense ではまだ使用できない ASA 専用の機能が必要な場合は、ASA の使用が適しています。シスコでは、ASA から Threat Defense への移行ツールを提供しています。このツールは、ASA の使用を開始し、後に Threat Defense に再イメージ化する場合に、ASA を Threat Defense に変換するのに役立ちます。

- Threat Defense —脅威防御は、高度なステートフル ファイアウォール、VPN コンセントレータ、および次世代 IPS を組み合わせた次世代ファイアウォールです。つまり、Threat Defense は ASA の機能を最大限に活用し、最適な次世代ファイアウォールと IPS 機能を融合させます。

  Threat Defense には ASA の主要な機能の大部分に加えて、次世代ファイアウォールと IPS 機能が追加されているため、ASA よりも FTD を使用することをお勧めします。

ASA と Threat Defense 間での再イメージ化の方法については、『Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド』[英語] を参照してください。

マネージャ

Threat Defense と ASA は複数のマネージャをサポートします。

Threat Defense マネージャ

表 *1 : Threat Defense* マネージャ

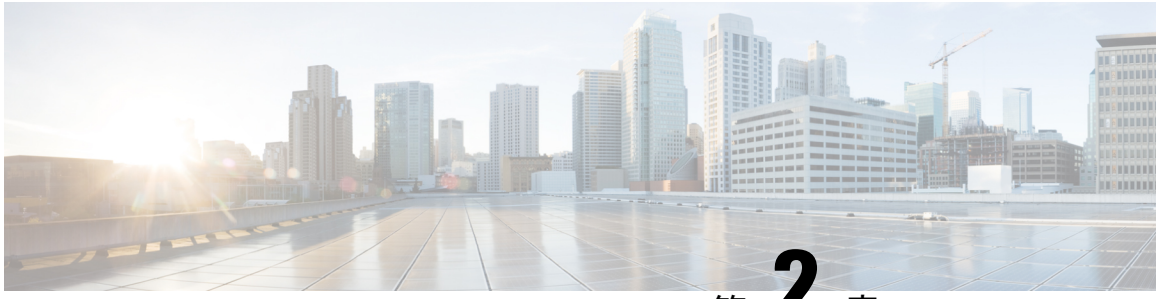
マネージャ	説明
Secure Firewall Management Center（旧 Firepower Management Center）	Management Center は強力な Web ベースのマルチデバイスマネージャです。独自のサーバーハードウェア上で、またはハイパーバイザ上の仮想デバイスとして稼働します。マルチデバイスマネージャを必要とし、Threat Defense のすべての機能が必要な場合は、Management Center を使用する必要があります。Management Center は、トラフィックとイベントの強力な分析とモニタリングも提供します。 6.7 以降、Management Center では、標準の管理インターフェイスではなく、外部（またはその他のデータ）インターフェイスから Threat Defense を管理できます。この機能は、リモート支社の展開に役立ちます。 （注） Management Center は Threat Defense 設定を持ち、Management Center をバイパスして Threat Defense を直接設定することはできないため、Management Center は他のマネージャとの互換性がありません。 管理ネットワークで Management Center を開始するには、「Management Center での Threat Defense の展開 （5 ページ）」[英語] を参照してください。 リモートネットワークで Management Center を開始するには、「リモート Threat Defense による Management Center の展開 （53 ページ）」[英語] を参照してください。
Secure Firewall Device Manager （旧 Firepower Device Manager）	Device Manager は、Web ベースのシンプルなオンデバイスマネージャです。簡素化されているため、一部の Threat Defense 機能は Device Manager では使用できません。少数のデバイスのみを管理し、マルチデバイスマネージャを必要としない場合は、Device Manager を使用するのに適しています。 （注） FDM モードの Device Manager と CDO の両方でファイアウォールの設定を検出できるため、Device Manager と CDO を使用して同じファイアウォールを管理することが可能です。Management Center は他のマネージャと互換性がありません。 Device Manager を開始するには、「Device Manager での Threat Defense の展開（101 ページ）」[英語] を参照してください。

マネージャ	説明
Cisco Defense Orchestrator（CDO）	CDO には 2 つの管理モードがあります。 • （7.2 以降）オンプレミスの管理センターのすべての設定機能を備えたクラウド提供型の管理センターモード。分析機能については、クラウド内の Secure Cloud Analytics またはオンプレミスの管理センターのいずれかを使用できます。 • （既存の CDO ユーザーのみ）ユーザーエクスペリエンスが簡素化されたデバイスマネージャモード。このモードは、すでに CDO を使用してデバイスマネージャモードで Threat Defense を管理しているユーザーのみが使用できます。このモードについては、このガイドでは説明していません。 CDO はクラウドベースであるため、独自のサーバーで CDO を実行する必要はありません。CDO は ASA などの他のセキュリティデバイスも管理するため、すべてのセキュリティデバイスに単一のマネージャを使用できます。 CDO プロビジョニングを開始するには、CDO での Threat Defense の展開 （133 ページ） [英語] を参照してください。
Cisco Secure Firewall Threat Defense REST API	Threat Defense REST API を使用すると、Threat Defense の直接設定を自動化できます。Device Manager と CDO はどちらもファイアウォールで設定を検出できるため、この API はそれらの両方と互換性があります。Management Center を使用して Threat Defense を管理している場合は、この API を使用できません。 このガイドでは、Threat Defense REST API について説明しません。詳細については、Cisco Secure Firewall Threat Defense REST API ガイド[英語] を参照してください。
Secure Firewall Management Center REST API	Management Center REST API を使用すると、管理対象の Threat Defense に適用可能な Management Center ポリシーの設定を自動化できます。この API は、Threat Defense を直接管理しません。 このガイドでは、Management Center REST API について説明しません。詳細については、Cisco Secure Firewall Management Center REST API クイックスタートガイド [英語] を参照してください。

ASA マネージャ

表 *2 : ASA* マネージャ

マネージャ	説明
Adaptive Security Device Manager（ASDM）	ASDM は Java ベースのオンデバイスマネージャであり、ASA のすべての機能を提供します。CLI よりも GUI を使用することを好み、管理が必要な ASA が少数の場合は、ASDM の使用が適しています。ASDM はファイアウォールの設定を検出できるため、ASDM で CLI、CDO、または CSM を使用することも可能です。 ASDM を使用する前にASDM を使用した ASA の展開 （189 ページ）を参照してください。
CLI	GUI よりも CLI を使用することを好む場合は、ASA CLI を使用してください。 CLI については、このガイドでは取り上げていません。詳細については、『ASA 構成ガイド』を参照してください。
CDO	CDO は、シンプルなクラウドベースのマルチデバイスマネージャです。シンプル化されているため、一部の ASA 機能は CDO では使用できません。シンプルな管理エクスペリエンスを提供するマルチデバイスマネージャが必要な場合、CDO を使用するのに適しています。また、CDO はクラウドベースであるため、独自のサーバーで CDO を実行する必要はありません。CDO は Threat Defense などの他のセキュリティデバイスも管理するため、すべてのセキュリティデバイスに単一のマネージャを使用できます。CDO はファイアウォールの設定を検出できるため、CLI や ASDM を使用することも可能です。 CDO については、このガイドでは取り上げていません。CDO を使用する前に、CDO のホームページを参照してください。
Cisco Security Manager（CSM）	CSM は、独自のサーバーハードウェア上で動作する強力なマルチデバイスマネージャです。多数の ASA を管理する必要がある場合、CSM を使用するのに適しています。CSM はファイアウォールの設定を検出できるため、CLI や ASDM を使用することも可能です。CSM は Threat Defense の管理をサポートしていません。 CSM については、このガイドでは取り上げていません。詳細については、『CSM ユーザーガイド』を参照してください。
ASA REST API	ASA REST API を使用すると、ASA の設定を自動化できます。ただし、API にはすべての ASA 機能が搭載されておらず、拡張されることもありません。 ASA REST API については、このガイドでは取り上げていません。詳細については、Cisco ASA REST API クイック スタート ガイドを参照してください。



第 2 章

Management Center での Threat Defense の展開

この章の対象読者

使用可能なすべてのオペレーティングシステムとマネージャを確認するには、「最適なオペレーティングシステムとマネージャを見つける方法 （1 ページ）」を参照してください。この章の内容は、 Management Center での Threat Defense の展開に適用されます。

この章では、Threat Defense の初期設定の方法と管理ネットワーク上にある Management Center へのファイアウォールの登録方法について説明します。 Management Center が中央の本社にあるリモート支社での展開については、「リモート Threat Defense による Management Center の展開 （53 ページ）」を参照してください。

大規模ネットワークの一般的な導入では、複数の管理対象デバイスがネットワークセグメントにインストールされます。各デバイスは、トラフィックを制御、検査、監視、および分析して、管理 Management Center に報告します。Management Center は、サービスの管理、分析、レポートのタスクを実行できる Web インターフェイスを備えた集中管理コンソールを提供し、ローカルネットワークを保護します。

ファイアウォールについて

ハードウェアでは、Threat Defense ソフトウェアまたは ASA ソフトウェアを実行できます。Threat Defense と ASA の間で切り替えを行う際には、デバイスの再イメージ化が必要になります。現在インストールされているものとは異なるソフトウェアバージョンが必要な場合も再イメージ化が必要です。「Cisco ASA および Firepower Threat Defense 再イメージ化ガイド」を参照してください。

ファイアウォールは、Secure Firewall eXtensible オペレーティングシステム（FXOS）と呼ばれる基盤となるオペレーティングシステムを実行します。ファイアウォールは FXOS Secure Firewall Chassis Manager をサポートしていません。トラブルシューティング用として限られた CLI のみがサポートされています。詳細については、Firepower 1000/2100 および Secure Firewall 3100 と Firepower Threat Defense の Cisco FXOS トラブルシューティング ガイドを参照してください。

プライバシー収集ステートメント：ファイアウォールには個人識別情報は不要で、積極的に収集することもありません。ただし、ユーザー名などの設定では、個人識別情報を使用できま

す。この場合、設定作業時やSNMPの使用時に、管理者が個人識別情報を確認できる場合があります。

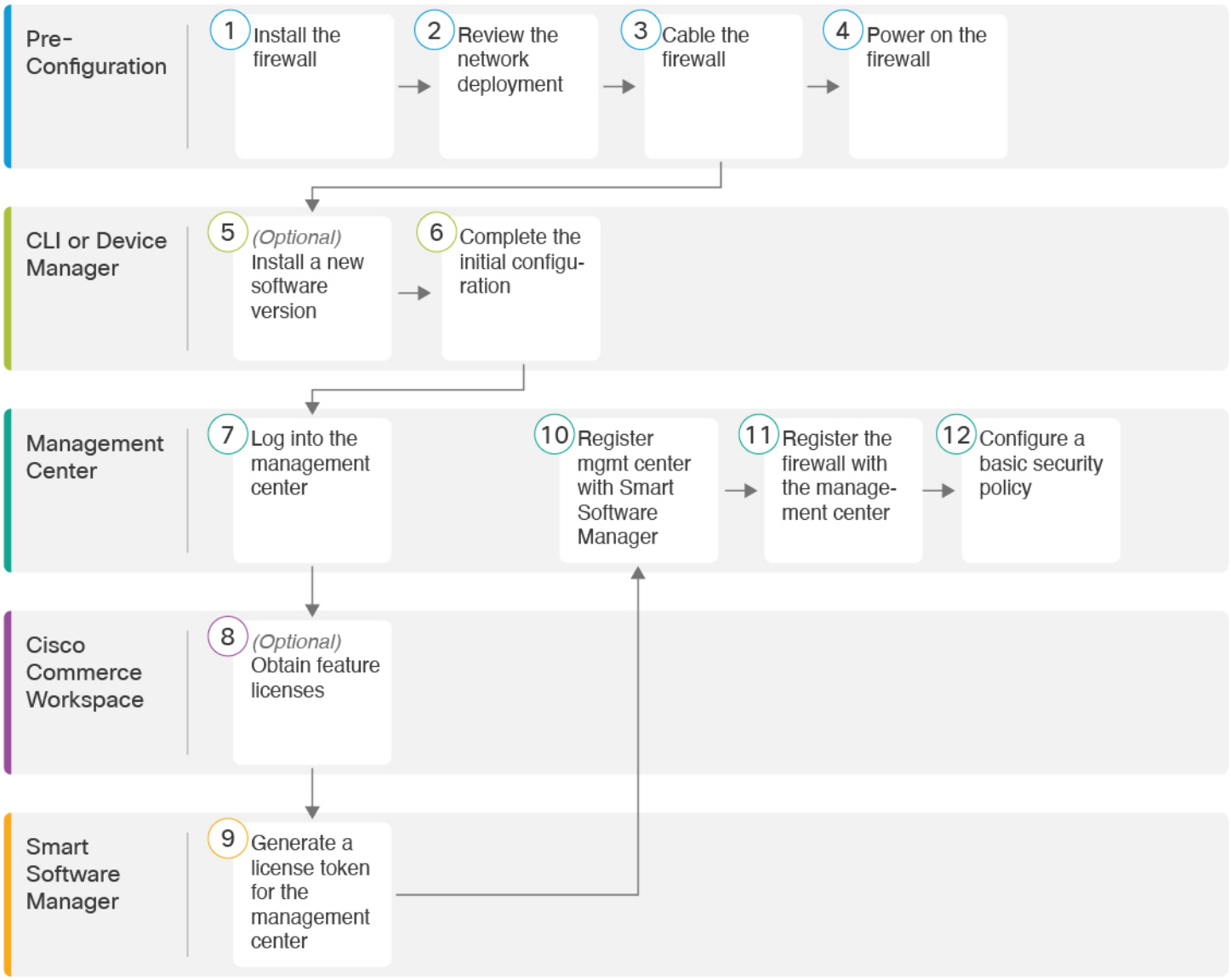
- はじめる前に （6 ページ）
- エンドツーエンドの手順 （6 ページ）
- ネットワーク展開の確認 （8 ページ）
- デバイスのケーブル接続 (6.5 以降) （10 ページ）
- デバイスの配線（6.4） （12 ページ）
- ファイアウォールの電源の投入 （13 ページ）
- （任意）ソフトウェアの確認と新しいバージョンのインストール （14 ページ）
- Threat Defense の初期設定の完了 （16 ページ）
- Management Center へのログイン （25 ページ）
- Management Center のライセンスの取得 （25 ページ）
- Management Center への Threat Defense の登録 （27 ページ）
- 基本的なセキュリティポリシーの設定 （30 ページ）
- Threat Defense および FXOS CLI へのアクセス （48 ページ）
- ファイアウォールの電源の切断 （49 ページ）
- 次のステップ （51 ページ）

はじめる前に

Management Center の初期設定を展開して実行します。Cisco Firepower Management Center 1600, 2600, and 4600 Hardware Installation GuideまたはCisco Secure Firewall Management Center Virtual 入門ガイドを参照してください。

エンドツーエンドの手順

シャーシでManagement Centerを使用してThreat Defenseを展開するには、次のタスクを参照してください。



1	事前設定	ファイアウォールをインストールします。ハードウェア設置ガイドを参照してください。
2	事前設定	ネットワーク展開の確認 （8 ページ）。
3	事前設定	デバイスのケーブル接続 (6.5 以降) （10 ページ） デバイスの配線（6.4） （12 ページ）。
4	事前設定	ファイアウォールの電源の投入 （13 ページ）。
5	CLI	（任意）ソフトウェアの確認と新しいバージョンのインストール （14 ページ）

6	CLI または Device Manager	Threat Defense の初期設定の完了 （16 ページ）。
7	Management Center	Management Center へのログイン （25 ページ）。
8	Cisco Commerce Workspace	Management Center のライセンスの取得 （25 ページ）：機能ライセンスを購入します。
9	Smart Software Manager	Management Center のライセンスの取得 （25 ページ）：Management Center のライセンストークンを生成します。
10	Management Center	Management Center のライセンスの取得 （25 ページ）：スマート ライセンシング サーバーに Management Center を登録します。
11	Management Center	Management Center への Threat Defense の登録 （27 ページ）
12	Management Center	基本的なセキュリティポリシーの設定 （30 ページ）

ネットワーク展開の確認

6.5 以降の展開

専用の Management 1/1 インターフェイスは、独自のネットワーク設定を持つ特別なインターフェイスです。デフォルトでは、Management 1/1 インターフェイスは有効になっていて、DHCP クライアントとして設定されています。ネットワークに DHCP サーバーが含まれていない場合は、コンソールポートで初期設定時に静的 IP アドレスを使用するように管理インターフェイスを設定できます。Threat Defense を Management Center に接続した後は、他のインターフェイスを設定できます。デフォルトでは、Ethernet1/2 ～ 1/8 はスイッチポートとして有効化されているので注意してください。

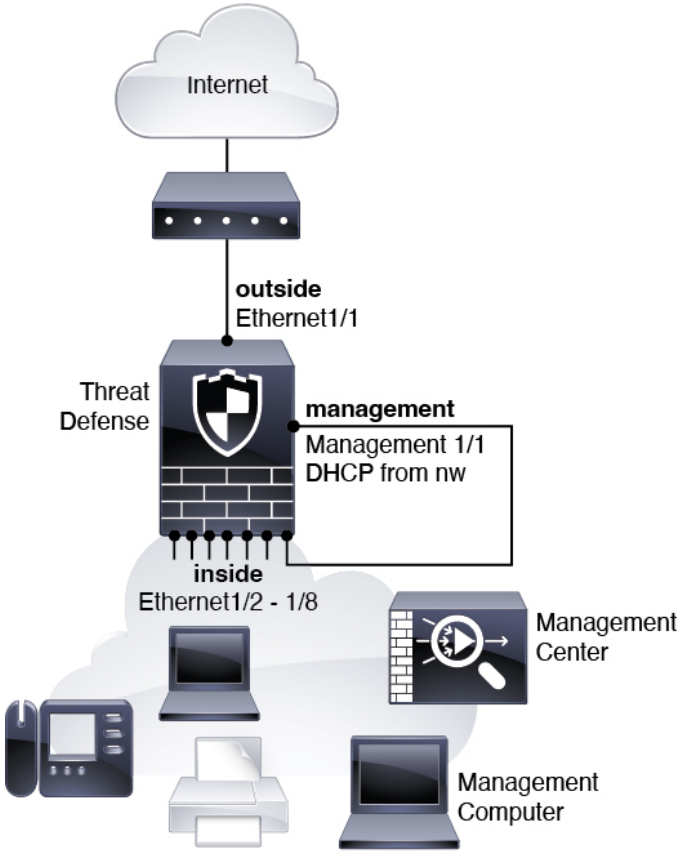
（注） 6.5 以前では、管理インターフェイスに IP アドレス（192.168.45.45）が設定されています。

次の図に、Firepower 1010 で推奨されるネットワーク配置を示します。

Management Center は管理インターフェイス上の Threat Defense のみと通信できます。さらに、Management Center と Threat Defense の両方で、ライセンシングと更新を行うには管理からのインターネットアクセスが必要です。

次の図では、Management 1/1 を直接内部スイッチポートに接続し、また Management Center と管理コンピュータを他の内部スイッチポートに接続することによって、Firepower 1010 が管理インターフェイスと Management Center のインターネットゲートウェイとして機能しています（管理インターフェイスは Threat Defense 上の他のインターフェイスとは別のものであるため、このような直接接続が許可されます）。

図 *1* : 推奨されるネットワーク配置



6.4 の展開

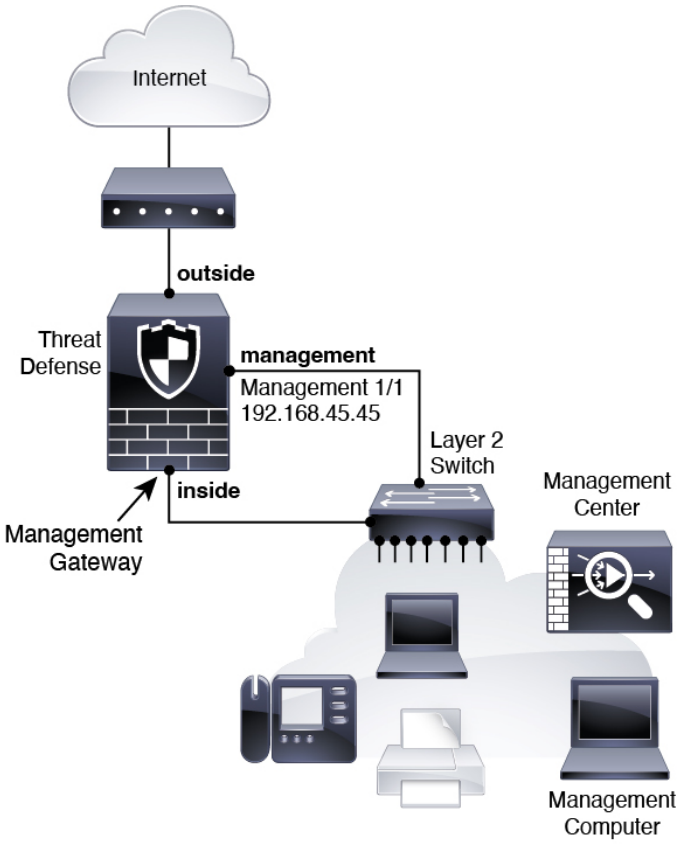
専用の Management 1/1 インターフェイスは、独自のネットワーク設定を持つ特別なインターフェイスです。デフォルトでは、管理 1/1 インターフェイスのみが有効になっており、IP アドレス（192.168.45.45）が設定されています。このインターフェイスは、最初に DHCP サーバーも実行します。初期設定時にマネージャとして Management Center を選択すると、DHCP サーバーは無効になります。Threat Defense を Management Center に接続した後は、他のインターフェイスを設定できます。

次の図に、Firepower 1010 で推奨されるネットワーク配置を示します。

Management Center は管理インターフェイス上の Threat Defense のみと通信できます。さらに、Management Center と Threat Defense の両方で、ライセンシングと更新を行うには管理からのインターネットアクセスが必要です。

次の図では、Management 1/1 をレイヤ 2 スイッチを介して内部のインターフェイスと接続し、また Management Center と管理コンピュータをスイッチに接続することによって、Firepower 1010 が管理インターフェイスと Management Center のインターネットゲートウェイとして機能しています（管理インターフェイスは Threat Defense 上の他のインターフェイスとは別のものであるため、このような直接接続が許可されます）。

図 *2:* 推奨されるネットワーク配置

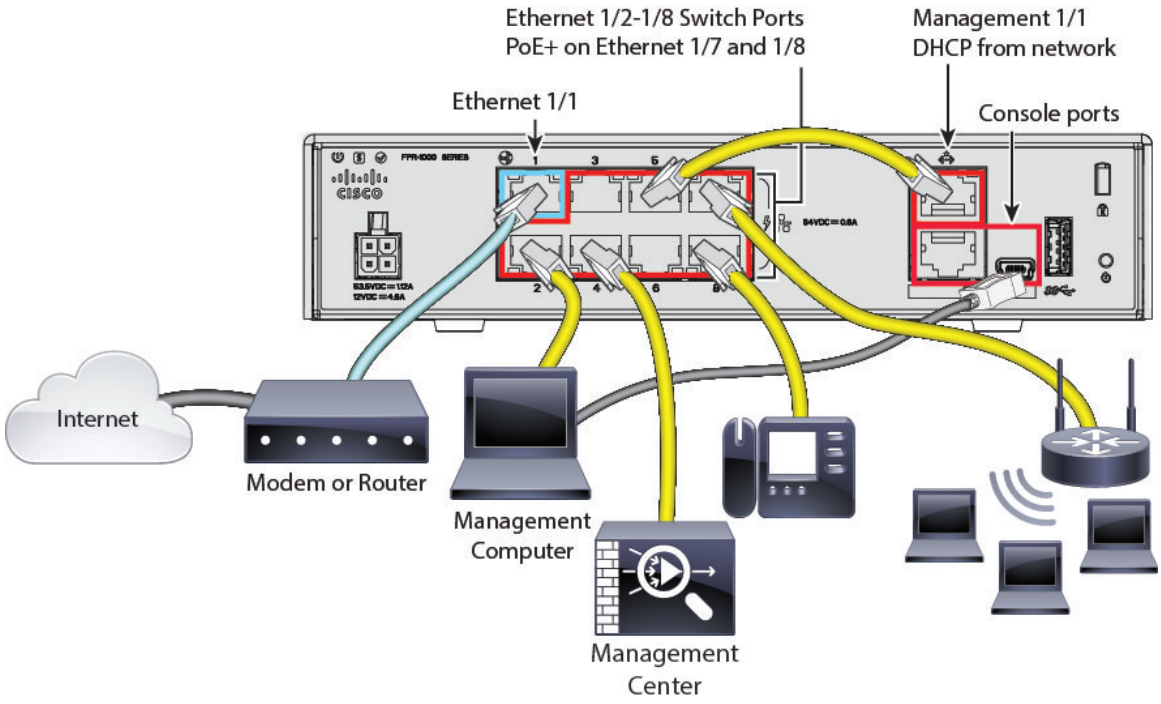


デバイスのケーブル接続 (6.5 以降)

Firepower 1010 で推奨シナリオのケーブル配線を行うには、次の図を参照してください。この図には、Ethernet1/1 を外部インターフェイスとして使用し、残りのインターフェイスを内部ネットワークのスイッチポートとして使用するサンプルトポロジが示されています。

（注） 他のトポロジも使用可能で、要件に応じて展開方法が異なります。たとえば、スイッチポートをファイアウォール インターフェイスに変換できます。

図 *3 : Firepower 1010* のケーブル配線



（注） バージョン 6.5 以前の場合、Management 1/1 のデフォルト IP アドレスは 192.168.45.45 です。

（注） PoE は Firepower 1010E ではサポートされていません。

手順

ステップ 1 シャーシを取り付けます。ハードウェア設置ガイドを参照してください。

ステップ 2 Management1/1 をスイッチ ポート（Ethernet1/2 ～ 1/8）のいずれかに直接接続します。

ステップ 3 次のようにスイッチ ポート（Ethernet1/2 ～ 1/8）にケーブルを配線します。

- Management Center
- 管理コンピュータ
- 追加のエンドポイント

ステップ 4 管理コンピュータをコンソールポートに接続します。管理インターフェイスへの接続に SSH を使用しない場合、または初期セットアップに Device Manager を使用する場合は、コンソールポートを使用して初期セットアップのために CLI にアクセスする必要があります。

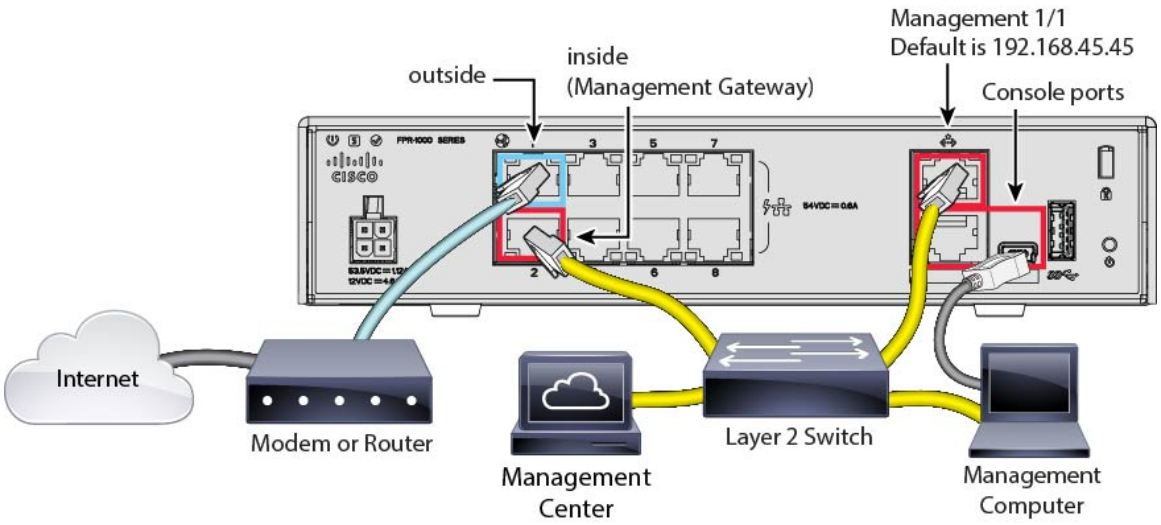
ステップ 5 Ethernet 1/1 を外部ルータに接続します。

デバイスの配線（6.4）

Firepower 1010 における推奨シナリオのケーブル配線については、レイヤ 2 スイッチを使用したサンプルトポロジを示す次の図を参照してください。

（注） 他のトポロジも使用可能で、要件に応じて展開方法が異なります。

図 *4 : Firepower 1010* のケーブル配線



手順

ステップ 1 ハードウェア設置ガイドを使用してハードウェアを設置し、ハードウェアについてよく理解しておきます。

ステップ 2 以下の機器のケーブルをレイヤ 2 イーサネット スイッチに接続します。

- 内部インターフェイス（Ethernet 1/2 など）
- Management 1/1 インターフェイス
- Management Center
- 管理コンピュータ

（注） Firepower 1010 と Management Center の両方に同じデフォルトの管理 IP アドレス（192.168.45.45）が設定されています。このガイドでは、初期セットアップ時に異なる IP アドレスをデバイスに設定することを前提としています。6.5 以降の Management Center は、管理インターフェイス用の DHCP クライアントにデフォルト設定されていることに注意してください。ただし、DHCP サーバーが存在しない場合は、デフォルトで 192.168.45.45 になります。

ステップ 3 管理コンピュータをコンソールポートに接続します。管理インターフェイスへの SSH を使用しない場合は、コンソールポートを使用して初期設定のために CLI にアクセスする必要があります。

ステップ 4 外部インターフェイス（Ethernet 1/1 など）を外部ルータに接続します。

ステップ 5 残りのインターフェイスに他のネットワークを接続します。

ファイアウォールの電源の投入

システムの電源は電源コードで制御されます。電源ボタンはありません。

（注） Threat Defense を初めて起動するときは、初期化に約 15 ～ 30 分かかります。

始める前に

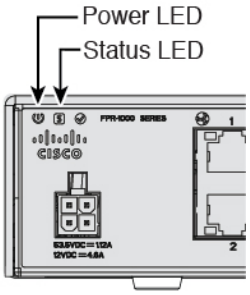
デバイスに対して信頼性の高い電力を供給することが重要です（たとえば、無停電電源装置（UPS）を使用）。最初のシャットダウンを行わないで電力が失われると、重大なファイルシステムの損傷を引き起こす可能性があります。バックグラウンドでは常に多数のプロセスが実行されていて、電力が失われると、システムをグレースフルシャットダウンできません。

手順

ステップ 1 電源コードをデバイスに接続し、電源コンセントに接続します。

電源コードを差し込むと電源が自動的に入ります。

ステップ 2 デバイスの背面または上部にある電源 LED を確認します。緑色に点灯している場合は、デバイスの電源が入っています。



ステップ 3 デバイスの背面または上部にあるステータス LED を確認します。緑色に点灯している場合は、電源投入時診断に合格しています。

（任意）ソフトウェアの確認と新しいバージョンのインストール

ソフトウェアのバージョンを確認し、必要に応じて別のバージョンをインストールするには、次の手順を実行します。ファイアウォールを設定する前に対象バージョンをインストールすることをお勧めします。別の方法として、稼働後にアップグレードを実行することもできますが、設定を保持するアップグレードでは、この手順を使用するよりも時間がかかる場合があります。

実行するバージョン

ソフトウェア ダウンロード ページのリリース番号の横にある、金色の星が付いている Gold Star リリースを実行することをお勧めします。https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html に記載されているリリース戦略も参照してください。たとえば、この速報では、（最新機能を含む）短期的なリリース番号、長期的なリリース番号（より長期間のメンテナンスリリースとパッチ）、または非常に長期的なリリース番号（政府認定を受けるための最長期間のメンテナンスリリースとパッチ）について説明しています。

手順

ステップ 1 CLI に接続します。詳細については、Threat Defense および FXOS CLI へのアクセス （48 ページ）を参照してください。この手順ではコンソールポートを使用していますが、代わりに SSH を使用することもできます。

admin ユーザとデフォルトパスワードの **Admin123** を使用してログインします。

FXOS CLI に接続します。初めてログインしたとき、パスワードを変更するよう求められます。このパスワードは、SSH の Threat Defense ログインにも使用されます。

（注） パスワードがすでに変更されていて、パスワードがわからない場合は、初期設定へのリセットを実行して、パスワードをデフォルトにリセットする必要があります。初期設定へのリセット手順については、『FXOS troubleshooting guide』を参照してください。

例：

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

ステップ 2 FXOS CLI で、実行中のバージョンを表示します。

scope ssa

show app-instance

例：

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name      Slot ID     Admin State      Operational State     Running Version
Startup Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd                   1          Enabled          Online               7.2.0.65
7.2.0.65        Not Applicable
```

ステップ 3 新しいバージョンをインストールする場合は、次の手順を実行します。

a) 管理インターフェイスに静的 IP アドレスを設定する必要がある場合は、「CLI を使用した Threat Defense 初期設定の実行の完了 （21 ページ）」を参照してください。デフォルトでは、管理インターフェイスは DHCP を使用します。

管理インターフェイスからアクセスできるサーバーから新しいイメージをダウンロードする必要があります。

b) FXOS のトラブルシューティング ガイドに記載されている再イメージ化の手順を実行します。

Threat Defense の初期設定の完了

CLI か Device Manager を使用して Threat Defense の初期設定を完了させることができます。

Device Manager を使用した Threat Defense の初期設定の完了

Device Manager に接続して、Threat Defense の初期設定を実行します。Device Manager を使用して初期セットアップを実行すると、管理インターフェイスおよびマネージャアクセス設定に加えて、管理のために Management Center に切り替えたときに、Device Manager で完了したすべてのインターフェイス構成が保持されます。アクセス コントロール ポリシーやセキュリティ ゾーンなどの他のデフォルト設定は保持されないことに注意してください。CLI を使用すると、管理インターフェイスとマネージャアクセス設定のみが保持されます（たとえば、デフォルトの内部インターフェイス構成は保持されません）。

始める前に

- Management Center の初期設定を展開して実行します。Cisco Firepower Management Center 1600, 2600, and 4600 Hardware Installation Guideを参照してください。Threat Defense をセットアップする前に、Management Center の IP アドレスまたはホスト名を把握しておく必要があります。
- Firefox、Chrome、Safari、Edge、または Internet Explorer の最新バージョンを使用します。

手順

ステップ 1 Device Manager にログインします。

a) ブラウザに次の URL のいずれかを入力します。

- 内部（Ethernet 1/2 ～ 1/8）：**https://192.168.95.1**。内部スイッチ ポート（Ethernet1/2 ～ 1/8）の内部アドレスに接続できます。
- 管理：**https://***management_ip*。管理インターフェイスは DHCP クライアントであるため、IP アドレスは DHCP サーバーによって異なります。この手順の一環として、管理 IP アドレスを静的アドレスに設定する必要があるため、接続が切断されないように内部インターフェイスを使用することをお勧めします。

b) ユーザー名 **admin**、デフォルト パスワード **Admin123** を使用してログインします。

c) エンド ユーザー ライセンス契約書を読んで同意し、管理者パスワードを変更するように求められます。

ステップ 2 初期設定を完了するには、最初に Device Manager にログインしたときにセットアップ ウィザードを使用します。必要に応じて、ページの下部にある [デバイスの設定をスキップ（Skip device setup）] をクリックしてセットアップ ウィザードをスキップできます。

セットアップウィザードを完了すると、内部インターフェイス（Ethernet1/2 ～ 1/8（VLAN1 のスイッチポート））のデフォルト設定に加えて、Management Center の管理に切り替えるときに維持される外部（Ethernet1/1）インターフェイスも設定できます。

a) 外部インターフェイスおよび管理インターフェイスに対して次のオプションを設定し、[次へ（Next）] をクリックします。

1. [外部インターフェイスアドレス（Outside Interface Address）]—このインターフェイスは通常インターネット ゲートウェイであり、マネージャ アクセス インターフェイスとして使用される場合があります。デバイスの初期設定時に別の外部インターフェイスを選択することはできません。最初のデータ インターフェイスがデフォルトの外部インターフェイスです。

   マネージャアクセスに外部（または内部）とは異なるインターフェイスを使用する場合は、セットアップウィザードの完了後に手動で設定する必要があります。

   [IPv4の設定（Configure IPv4）]：外部インターフェイス用の IPv4 アドレスです。DHCP を使用するか、または手動でスタティック IP アドレス、サブネットマスク、およびゲートウェイを入力できます。[オフ（Off）] を選択して、IPv4 アドレスを設定しないという選択肢もあります。セットアップウィザードを使用して PPPoE を設定することはできません。インターフェイスが DSL モデム、ケーブルモデム、または ISP への他の接続に接続されており、ISP が PPPoE を使用して IP アドレスを提供している場合は、PPPoE が必要になる場合があります。ウィザードの完了後に PPPoE を設定できます。

   [IPv6の設定（Configure IPv6）]：外部インターフェイス用の IPv6 アドレスです。DHCP を使用するか、または手動でスタティック IP アドレス、プレフィックス、およびゲートウェイを入力できます。[オフ（Off）] を選択して、IPv6 アドレスを設定しないという選択肢もあります。

2. **[管理インターフェイス（Management Interface）]**

   CLI で初期設定を実行した場合、管理インターフェイスの設定は表示されません。管理インターフェイスの IP アドレスの設定は、セットアップウィザードに含まれていないことに注意してください。管理 IP アドレスの設定については、「ステップ 3 （18 ページ）」を参照してください。

   [DNSサーバー（DNS Servers）]：ファイアウォールの管理インターフェイスの DNS サーバーです。名前解決用に 1 つ以上の DNS サーバのアドレスを入力します。デフォルトは OpenDNS パブリック DNS サーバです。フィールドを編集し、デフォルトに戻したい場合は、[OpenDNSを使用（Use OpenDNS）] をクリックすると、フィールドに適切な IP アドレスがリロードされます。

   [ファイアウォールホスト名（Firewall Hostname）]：ファイアウォールの管理インターフェイスのホスト名です。

b) [時刻設定（NTP）（Time Setting (NTP)）] を設定し、[次へ（Next）] をクリックします。

1. [タイムゾーン（Time Zone）]：システムのタイムゾーンを選択します。

2. [NTPタイムサーバ（NTP Time Server）]：デフォルトの NTP サーバを使用するか、使用している NTP サーバのアドレスを手動で入力するかを選択します。バックアップ用に複数のサーバを追加できます。

c) [登録せずに 90 日間の評価期間を開始（Start 90 day evaluation period without registration）]を選択します。

Threat Defense を Smart Software Manager に登録しないでください。すべてのライセンスは Management Center で実行されます。

d) [終了（Finish）] をクリックします。

e) [クラウド管理（Cloud Management）]または [スタンドアロン（Standalone）] を選択するよう求められます。Management Center の管理については、[スタンドアロン（Standalone）] を選択してから、[Got It（了解）] を選択します。

ステップ 3 （必要に応じて）管理インターフェイスの静的IPアドレスを設定します。[デバイス（Device）] を選択し、[システム設定（System Settings）]>[管理インターフェイス（Management Interface）] リンクの順にクリックします。

静的 IP アドレスを設定する場合は、デフォルトゲートウェイもデータインターフェイスではなく一意のゲートウェイに設定してください。DHCP を使用する場合は、何も設定する必要はありません。

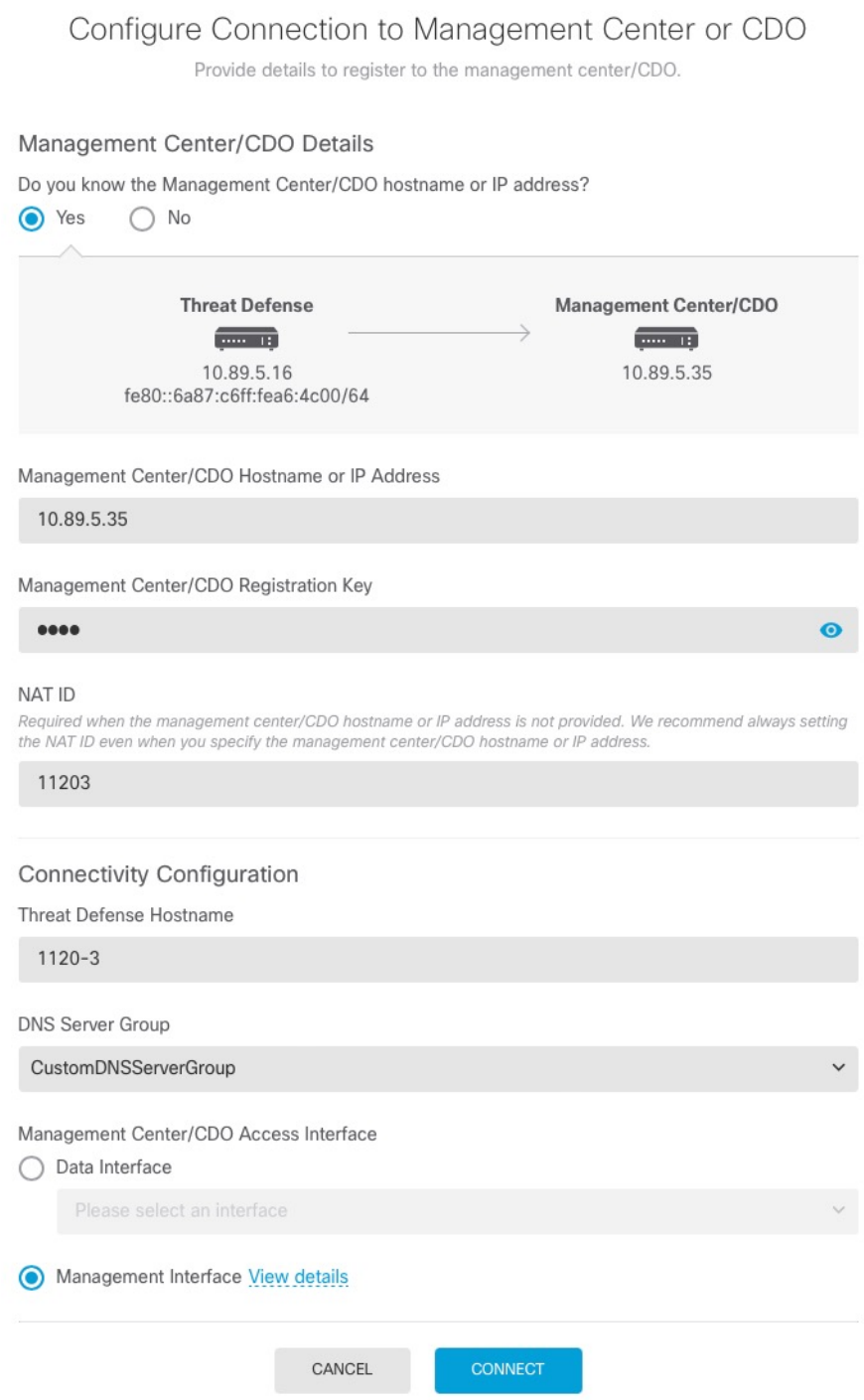
ステップ 4 外部または内部以外のインターフェイスを含む追加のインターフェイスを設定する場合は、[デバイス（Device）] を選択し、[インターフェイス（Interface）] のサマリーにあるリンクをクリックします。

Device Manager におけるインターフェイスの設定の詳細については、「Device Manager でのファイアウォールの設定 （122 ページ）」を参照してください。Management Center にデバイスを登録すると、Device Manager の他の設定は保持されません。

ステップ 5 [デバイス（Device）][システム設定（Device System Settings）][中央管理（Central Management）][Management Center] [Management Center] [デバイス（Device）][システム設定（System Settings）][中央管理（Central Management）] [Management Center] の順に選択し、 [続行（Proceed）] をクリックして Management Center の管理を設定します。

ステップ 6 **[Management Center/CDOの詳細（Management Center/CDO Details）]** を設定します。

図 *5 : Management Center/CDO* の詳細



a) **[Management Center/CDOのホスト名またはIPアドレスを知っていますか（Do you know the FMC hostname or IP address）]** で、IP アドレスまたはホスト名を使用して Management Center に到達できる場合は [はい（Yes）] をクリックし、Management Center が NAT の背

後にあるか、パブリック IP アドレスまたはホスト名がない場合は[いいえ（No）] をクリックします。

双方向の SSL 暗号化通信チャネルを 2 台のデバイス間に確立するには、少なくても 1 台以上のデバイス（Management Center または Threat Defense デバイス）に到達可能な IP アドレスが必要です。

b) [はい（Yes）] を選択した場合は、**管理センター/CDO のホスト名/IP アドレス**を入力します。

c) **Management Center/CDO 登録キー**を指定します。

このキーは、Threat Defense デバイスを登録するときに Management Center でも指定する任意の 1 回限りの登録キーです。登録キーは 37 文字以下にする必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、Management Center に登録する複数のデバイスに使用できます。

d) [NAT ID] を指定します。

この ID は、Management Center でも指定する任意の 1 回限りの文字列です。いずれかのデバイスの IP アドレスのみを指定する場合、このフィールドは必須です。両方のデバイスの IP アドレスがわかっている場合でも、NAT ID を指定することを推奨します。NAT ID は 37 文字以下にする必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、Management Center に登録する他のデバイスには使用できません。NAT ID は、正しいデバイスからの接続であることを確認するために IP アドレスと組み合わせて使用されます。 IP アドレス/NAT ID の認証後にのみ、登録キーがチェックされます。

ステップ 7 [接続の設定（Connectivity Configuration）] を設定します。

a) [FTDホスト名（FTD Hostname）] を指定します。

b) [DNSサーバーグループ（DNS Server Group）] を指定します。

既存のグループを選択するか、新しいグループを作成します。デフォルトの DNS グループは **CiscoUmbrellaDNSServerGroup** と呼ばれ、OpenDNS サーバーが含まれます。

c) **[Management Center/CDOアクセスインターフェイス（Management Center/CDO Access Interface）]**については、[管理（management）] を選択します。

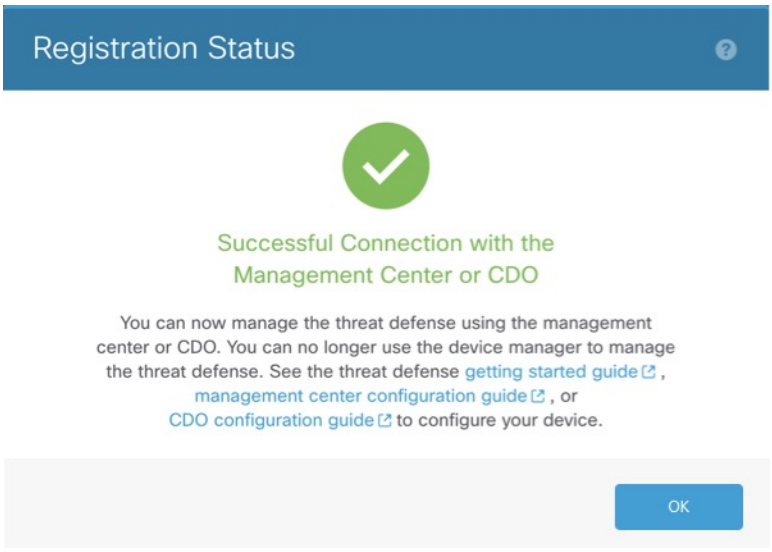
ステップ 8 [接続（Connect）] をクリックします。**[登録ステータス（Registration Status）]** ダイアログボックスには、Management Center への切り替えに関する現在のステータスが表示されます。**[Management Center/CDO登録設定の保存（Saving Management Center/CDO Registration Settings）]** のステップの後、Management Center に移動してファイアウォールを追加します。

Management Center への切り替えをキャンセルする場合は、[登録のキャンセル（Cancel Registration）] をクリックします。キャンセルしない場合は、**[Management Center/CDO登録設定の保存（Saving Management Center/CDO Registration Settings）]** のステップが完了するまで Device Manager のブラウザウィンドウを閉じないでください。閉じた場合、プロセスは一時停止し、Device Manager に再接続した場合のみ再開されます。

[Management Center/CDO登録設定の保存（Saving Management Center/CDO Registration Settings）] のステップの後に Device Manager に接続したままにする場合、その後 **[Management**

CenterまたはCDOとの正常接続（Successful Connection with Management Center or CDO）] ダイアログボックスが表示され、Device Manager から切断されます。

図 *6* : 正常接続



CLI を使用した Threat Defense 初期設定の実行の完了

Threat Defense CLI に接続して初期設定を実行します。これには、セットアップウィザードを使用した管理 IP アドレス、ゲートウェイ、およびその他の基本ネットワーク設定の指定などが含まれます。専用の管理インターフェイスは、独自のネットワーク設定を持つ特別なインターフェイスです。6.7 以降：マネージャアクセスに管理インターフェイスを使用しない場合は、代わりに CLI を使用してデータインターフェイスを設定できます。また、Management Center 通信の設定を行います。（7.1 以降）Device Manager を使用して初期セットアップを実行すると、管理のために Management Center に切り替えたときに、管理インターフェイスおよびマネージャ アクセス インターフェイスの設定に加えて、Device Manager で完了したすべてのインターフェイス設定が保持されます。アクセス コントロール ポリシーなどの他のデフォルト設定は保持されないことに注意してください。

手順

ステップ 1 コンソールポートから、または管理インターフェイスへの SSH を使用して、Threat Defense CLIに接続します。デフォルトでDHCPサーバーからIPアドレスが取得されます。ネットワーク設定を変更する場合は、切断されないようにコンソールポートを使用することを推奨します。

コンソールポートは FXOS CLI に接続します。SSH セッションは Threat Defense CLI に直接接続します。

ステップ 2 ユーザー名 **admin** およびパスワード **Admin123** でログインします。

コンソールポートで FXOS CLI に接続します。初めて FXOS にログインしたときは、パスワードを変更するよう求められます。このパスワードは、SSH の Threat Defense ログインにも使用されます。

（注） パスワードがすでに変更されていて、パスワードがわからない場合は、デバイスを再イメージ化してパスワードをデフォルトにリセットする必要があります。再イメージ化の手順については、FXOS のトラブルシューティング ガイドを参照してください。

例：

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

ステップ 3 コンソールポートで FXOS に接続した場合は、Threat Defense CLI に接続します。

connect ftd

例：

```
firepower# connect ftd
>
```

ステップ 4 Threat Defense に初めてログインすると、エンドユーザーライセンス契約（EULA）に同意し、SSH 接続を使用している場合は、管理者パスワードを変更するように求められます。その後、CLI セットアップスクリプトが表示されます。

（注） 設定をクリア（たとえば、イメージを再作成することにより）しないかぎり、CLI セットアップウィザードを繰り返すことはできません。ただし、これらの設定すべては、後から CLI で **configure network** コマンドを使用して変更できます。Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。

デフォルト値または以前に入力した値がカッコ内に表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

次のガイドラインを参照してください。

- **管理インターフェイスの IPv4 デフォルトゲートウェイを入力**：[data-interfaces] の設定は、リモートの Management Center または Device Manager の管理にのみ適用されます。管理

ネットワークで Management Center を使用する場合は、Management 1/1 のゲートウェイ IP アドレスを設定する必要があります。「ネットワークの導入」の項に示されているエッジ展開の例では、内部インターフェイスは管理ゲートウェイとして機能します。この場合、ゲートウェイ IP アドレスを目的の内部インターフェイス IP アドレスに設定する必要があります。後で Management Center を使用して内部 IP アドレスを設定する必要があります。

- **ネットワーク情報が変更された場合は再接続が必要**：SSH で接続しているのに、初期セットアップでその IP アドレスを変更すると、接続が切断されます。新しい IP アドレスとパスワードで再接続してください。コンソール接続は影響を受けません。
- [デバイスをローカルで管理しますか（Manage the device locally?）]：Management Center を使用するには「**no**」を入力します。**yes** と入力すると、代わりに Device Manager を使用することになります。
- [ファイアウォールモードを設定しますか（Configure firewall mode?）]：初期設定でファイアウォールモードを設定することをお勧めします。初期設定後にファイアウォールモードを変更すると、実行コンフィギュレーションが消去されます。

例：

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password: ********
Confirm new password: ********
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

Update policy deployment information
    - add device configuration
    - add network discovery
    - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.
```

```
When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

ステップ 5 この Threat Defense を管理する Management Center を特定します。

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**}—Specifies either the FQDN or IP address of the Management Center.Management Center を直接アドレス指定できない場合は、**DONTRESOLVE** を使用します。また、*nat_id* も指定します。双方向の SSL 暗号化通信チャネルを2台のデバイス間に確立するには、少なくても1台以上のデバイス（Management Center または Threat Defense ）に到達可能な IP アドレスが必要です。このコマンドで **DONTRESOLVE** を指定するには、到達可能な IP アドレスまたはホスト名が Threat Defense に必要です。
- reg_key：Threat Defense を登録するときに Management Center でも指定する任意のワンタイム登録キーを指定します。登録キーは 37 文字以下にする必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。
- nat_id：一方の側で到達可能な IP アドレスまたはホスト名が指定されていない場合は、Threat Defense を登録するときに Management Center にも指定する任意の一意のワンタイム文字列を指定します。この文字列は、 Management Center を **DONTRESOLVE** に設定した場合に必要です。NAT ID は 37 文字以下にする必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、Management Center に登録する他のデバイスには使用できません。

例：

```
> configure manager add MC.example.com 123456
Manager successfully configured.
```

Management Center が NAT デバイスの背後にある場合は、次の例に示すように、一意の NAT ID とともに登録キーを入力し、ホスト名の代わりに DONTRESOLVE を指定します。

例：

```
> configure manager add DONTRESOLVE regk3y78 natid90
Manager successfully configured.
```

Threat Defense が NAT デバイスの背後にある場合は、次の例に示すように、一意の NAT ID とともに Management Center IP アドレスまたはホスト名を入力します。

例：

```
> configure manager add 10.70.45.5 regk3y78 natid56
Manager successfully configured.
```

次のタスク

Management Center にファイアウォールを登録します。

Management Center へのログイン

Management Center を使用して、Threat Defense を設定および監視します。

始める前に

サポートされているブラウザの詳細については、使用するバージョンのリリースノート（https://www.cisco.com/go/firepower-notes）を参照してください。

手順

ステップ 1 サポートされているブラウザを使用して、次の URL を入力します。

https://*fmc_ip_address*

ステップ 2 ユーザー名とパスワードを入力します。

ステップ 3 [ログイン（Log In）] をクリックします。

Management Center のライセンスの取得

すべてのライセンスは、Management Center によって Threat Defense に提供されます。次のライセンスを購入できます。

- **IPS**：セキュリティインテリジェンスと次世代 IPS
- **マルウェア防御**：マルウェア防御
- **URL**：URL フィルタリング
- **Cisco Secure Client**：Secure Client Advantage、Secure Client Premier、または Secure Client VPN のみ
- キャリア（Diameter、GTP/GPRS、M3UA、SCTP）

シスコライセンスの概要については詳しくは、cisco.com/go/licensingguide を参照してください。

始める前に

- Smart Software Manager にマスターアカウントを持ちます。

  まだアカウントをお持ちでない場合は、リンクをクリックして新しいアカウントを設定してください。Smart Software Manager では、組織のマスター アカウントを作成できます。

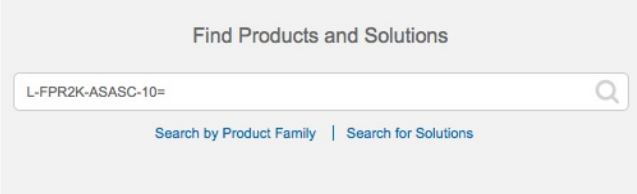
- （輸出コンプライアンスフラグを使用して有効化される）機能を使用するには、ご使用のスマート ソフトウェア ライセンシング アカウントで強力な暗号化（3DES/AES）ライセンスを使用できる必要があります。

手順

ステップ 1 お使いのスマート ライセンシング アカウントに、必要なライセンスが含まれていることを確認してください。

ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマート ソフトウェア ライセンシング アカウントにリンクされています。ただし、主導でライセンスを追加する必要がある場合は、Cisco Commerce Workspace で [製品とソリューションの検索（Find Products and Solutions）] 検索フィールドを使用します。次のライセンス PID を検索します。

図 7: ライセンス検索



（注） PID が見つからない場合は、注文に手動で PID を追加できます。

- IPS、マルウェア防御、および URL ライセンスの組み合わせ：
  - L-FPR1010T-TMC=

  上記の PID のいずれかを注文に追加すると、次のいずれかの PID に対応する期間ベースのサブスクリプションを選択できます。
  - L-FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y
  - L-FPR1010T-TMC-5Y

- Cisco Secure Client：『Cisco Secure Client 発注ガイド』を参照してください。

- キャリアライセンス：

-

ステップ 2 まだ設定していない場合は、スマート ライセンシング サーバーに Management Center を登録します。

登録を行うには、Smart Software Manager で登録トークンを生成する必要があります。詳細な手順については、Cisco Secure Firewall Management Center アドミニストレーション ガイドを参照してください。

Management Center への Threat Defense の登録

デバイスの IP アドレスかホスト名を使用して、手動で Threat Defense を Management Center に登録します。

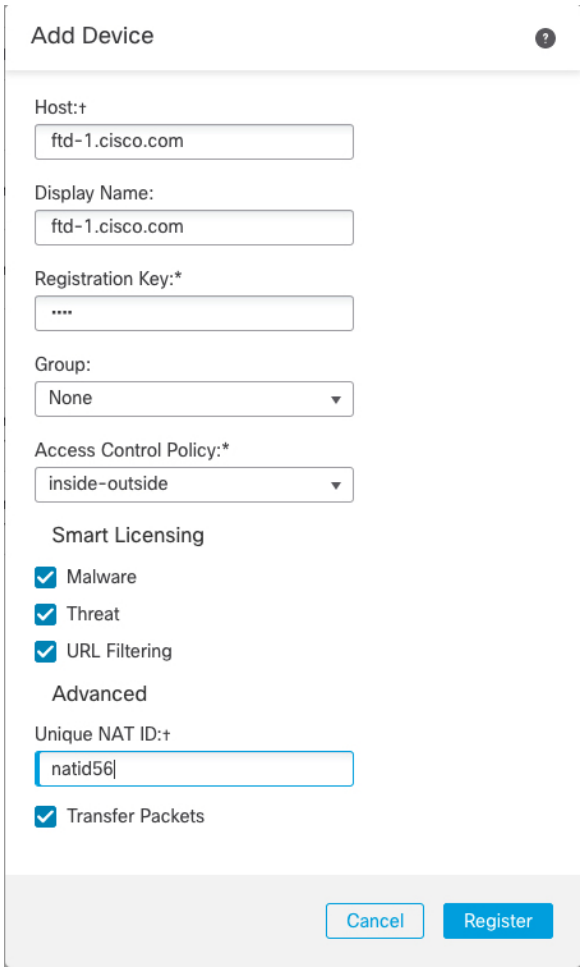
始める前に

- Threat Defense の最初の設定で設定した次の情報を収集します。
  - Threat Defense の管理 IP アドレスまたはホスト名、および NAT ID
  - Management Center の登録キー

手順

ステップ 1 Management Center で、[デバイス（Devices）] > [デバイス管理（Device Management）] の順に選択します。

ステップ 2 [追加（Add）] ドロップダウン リストから、[デバイスの追加（Add Device）] を選択します。



次のパラメータを設定します。

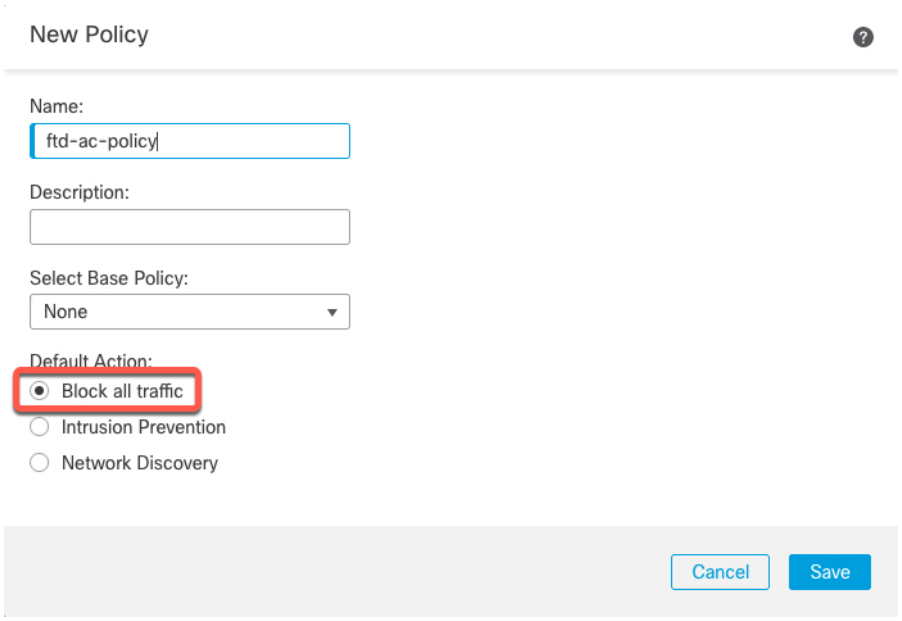
- [ホスト（Host）]：追加する Threat Defense の IP アドレスかホスト名を入力します。Threat Defense の最初の設定で Management Center の IP アドレスと NAT ID の両方を指定した場合は、このフィールドを空のままにしておくことができます。

  （注） HA 環境では、両方の Management Center が NAT の背後にある場合、プライマリ Management Center のホスト IP または名前なしで Threat Defense を登録できます。ただし、Threat Defense をセカンダリ Management Center に登録するには、Threat Defense の IP アドレスかホスト名を指定する必要があります。

- [表示名（Display Name）] フィールドに、Management Center に表示する Threat Defense の名前を入力します。
- [登録キー（Registration key）]：Threat Defense の最初の設定で指定したものと同じ登録キーを入力します。
- [ドメイン（Domain）]：マルチドメイン環境を使用している場合は、デバイスをリーフドメインに割り当てます。

- [グループ（Group）]：グループを使用している場合は、デバイスグループに割り当てます。
- [アクセスコントロールポリシー（Access Control Policy）]：初期ポリシーを選択します。使用する必要があることがわかっているカスタマイズ済みのポリシーがすでにある場合を除いて、[新しいポリシーの作成（Create new policy）] を選択し、[すべてのトラフィックをブロック（Block all traffic）] を選択します。後でこれを変更してトラフィックを許可することができます。「内部から外部へのトラフィックの許可 （45 ページ）」を参照してください。

図 *8 : New Policy*



- [スマートライセンス（Smart Licensing）]：展開する機能に必要なスマートライセンスとして、[マルウェア（Malware）]（マルウェアインスペクションを使用する予定の場合）、[脅威（Threat）]（侵入防御を使用する予定の場合）、および [URL]（カテゴリベースの URL フィルタリングを実行する予定の場合）を割り当てます。**注**：デバイスを追加した後、**[システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）]** ページから セキュアクライアント リモートアクセス VPN のライセンスを適用できます。
- [一意のNAT ID（Unique NAT ID）]：Threat Defense の最初の設定で指定した NAT ID を指定します。
- [パケットの転送（Transfer Packets）]：デバイスから Management Center へのパケット転送を許可します。このオプションを有効にして IPS や Snort などのイベントがトリガーされた場合は、デバイスが検査用としてイベントメタデータ情報とパケットデータを Management Center に送信します。このオプションを無効にした場合は、イベント情報だけが Management Center に送信され、パケットデータは送信されません。

ステップ 3 [登録（Register）]（別のデバイスを追加する場合は [別のデバイスを登録して追加（Register and Add Another）]）をクリックし、登録が成功したことを確認します。

登録が成功すると、デバイスがリストに追加されます。失敗した場合は、エラーメッセージが表示されます。Threat Defense が登録に失敗した場合は、次の項目を確認してください。

- ping：Threat Defense CLIにアクセスし、次のコマンドを使用して Management Center IP アドレスへの ping を実行します。

  ping system *ip_address*

  ping が成功しない場合は、**show network** コマンドを使用してネットワーク設定を確認します。Threat Defense 管理 IP アドレスを変更するには、**configure network** {**ipv4** | **ipv6**} **manual** コマンドを使用します。

- 登録キー、NAT ID、および Management Center IP アドレス：両方のデバイスで同じ登録キーを使用していることを確認し、使用している場合は NAT ID を使用していることを確認します。**configure manager add** コマンドを使用して、Management Center で登録キーと NAT ID を設定することができます。

トラブルシューティングの詳細については、https://cisco.com/go/fmc-reg-error を参照してください。

基本的なセキュリティポリシーの設定

ここでは、次の設定を使用して基本的なセキュリティポリシーを設定する方法について説明します。

- 内部インターフェイスと外部インターフェイス：内部インターフェイスにスタティック IP アドレスを割り当て、外部インターフェイスに DHCP を使用します。
- DHCP サーバー：クライアントの内部インターフェイスで DHCP サーバーを使用します。
- デフォルトルート：外部インターフェイスを介してデフォルトルートを追加します。
- NAT：外部インターフェイスでインターフェイス PAT を使用します。
- アクセスコントロール：内部から外部へのトラフィックを許可します。

基本的なセキュリティ ポリシーを設定するには、次のタスクを実行します。

1	インターフェイスの設定（6.5 以降） （31 ページ） インターフェイスの設定（6.4） （36 ページ）。
2	DHCP サーバーの設定 （39 ページ）。
3	デフォルトルートの追加 （40 ページ）。

4	NAT の設定 （42 ページ）。
5	内部から外部へのトラフィックの許可 （45 ページ）。
6	設定の展開 （46 ページ）。

インターフェイスの設定（6.5 以降）

スイッチポートの VLAN1 インターフェイスを追加するか、スイッチポートをファイアウォール インターフェイスに変換し、セキュリティゾーンにインターフェイスを割り当て、IP アドレスを設定します。通常は、システムで意味のあるトラフィックを通過させるように、少なくとも 2 つのインターフェイスを設定する必要があります。通常は、アップストリームルータまたはインターネットに面した外部インターフェイスと、組織のネットワークの 1 つ以上の内部インターフェイスを使用します。デフォルトでは、Ethernet1/1 は外部用に使用できる通常のファイアウォール インターフェイスであり、残りのインターフェイスは VLAN 1 のスイッチポートです。VLAN1 インターフェイスを追加すると、これを内部インターフェイスにすることができます。または、スイッチポートを他の VLAN に割り当てるか、スイッチポートをファイアウォール インターフェイスに変換することもできます。

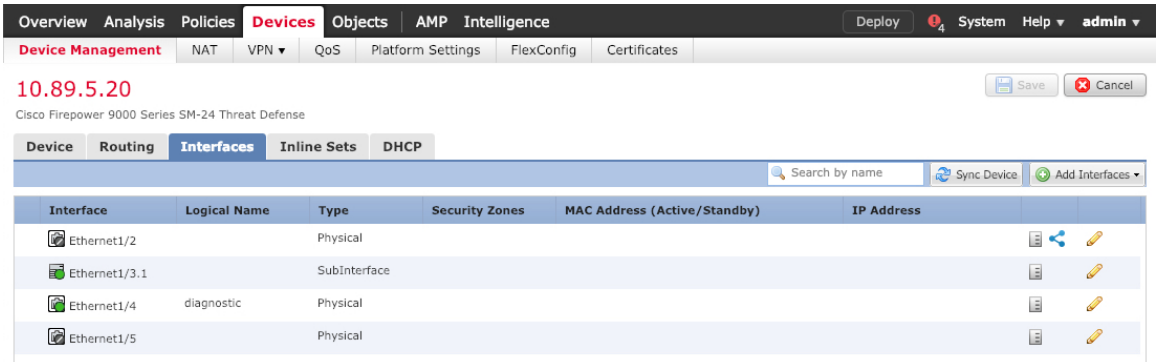
一般的なエッジルーティングの状況は、内部インターフェイスでスタティックアドレスを定義すると同時に、ISP から DHCP を介して外部インターフェイスアドレスを取得することです。

次の例では、DHCP によるスタティックアドレスとルーテッドモードの外部インターフェイスを使用して（Ethernet1/1）、ルーテッドモードの内部インターフェイス（VLAN1）を設定します。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、デバイスをクリックします。

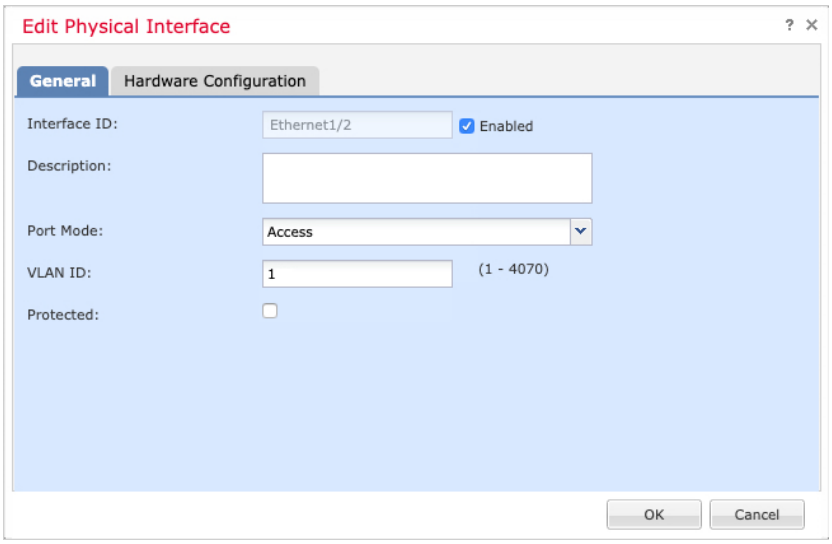
ステップ 2 [インターフェイス（Interfaces）] をクリックします。



ステップ 3 （任意）[スイッチポート（SwitchPort）] 列のスライダをクリックしてスイッチポート（Ethernet1/2 から 1/8）のいずれかのスイッチポートモードを無効にすると、無効（ ）と表示されます。

ステップ 4 スイッチポートを有効にします。

a) スイッチポートのをクリックします。



b) [有効（Enabled）] チェックボックスをオンにして、インターフェイスを有効化します。

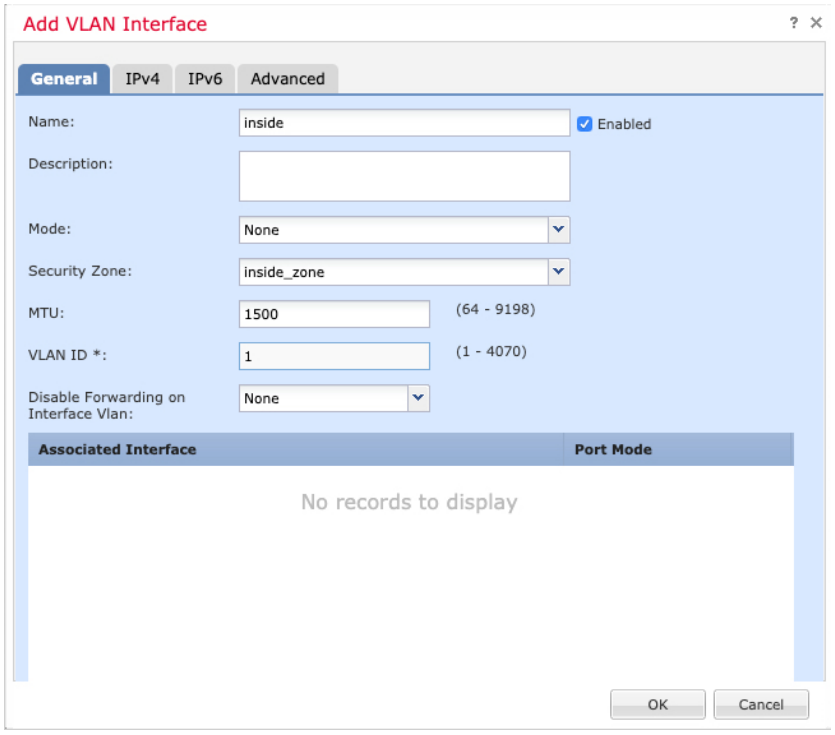
c) （任意） VLAN ID を変更します。デフォルトは 1 です。次に、この ID に一致する VLAN インターフェイスを追加します。

d) [OK] をクリックします。

ステップ 5 内部 VLAN インターフェイスを追加します。

a) **[インターフェイスの追加（Add Interfaces）]** > **[VLANインターフェイス（VLAN Interface）]** をクリックします。

[全般（General）] タブが表示されます。



b) 48 文字までの [名前（Name）] を入力します。

たとえば、インターフェイスに **inside** という名前を付けます。

c) [有効（Enabled）] チェックボックスをオンにします。

d) [モード（Mode）] は [なし（None）] に設定したままにします。

e) [セキュリティゾーン（Security Zone）] ドロップダウンリストから既存の内部セキュリティゾーンを選択するか、[新規（New）] 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。

たとえば、**inside_zone** という名前のゾーンを追加します。各インターフェイスは、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割り当てる必要があります。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も、複数のインターフェイスグループに属することもできます。ゾーンまたはグループに基づいてセキュリティポリシーを適用します。たとえば、内部インターフェイスを内部ゾーンに割り当て、外部インターフェイスを外部ゾーンに割り当てることができます。この場合、トラフィックが内部から外部に移動できるようにアクセス コントロール ポリシーを設定することはできますが、外部から内部に向けては設定できません。ほとんどのポリシーはセキュリティゾーンのみサポートしています。NAT ポリシー、プレフィルタ ポリシー、および QoS ポリシーで、ゾーンまたはインターフェイスグループを使用できます。

f) [VLAN ID] を **1** に設定します。

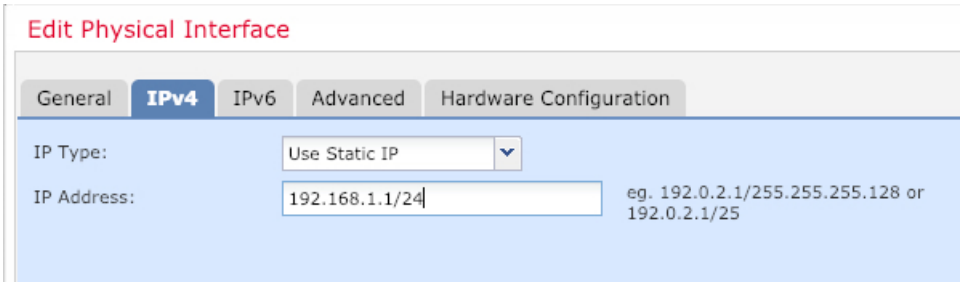
デフォルトでは、すべてのスイッチポートは VLAN 1 に設定されます。ここで別の VLAN ID を選択する場合は、新しい VLAN ID の各スイッチポートを編集する必要があります。

インターフェイスを保存した後、VLAN IDを変更することはできません。ここでのVLAN ID は、使用される VLAN タグと設定内のインターフェイス ID の両方です。

g) [IPv4] タブ、[IPv6] タブ、または両方のタブをクリックします。

- [IPv4]：ドロップダウンリストから [スタティックIPを使用する（Use Static IP）] を選択し、IP アドレスとサブネットマスクをスラッシュ表記で入力します。

  たとえば、**192.168.1.1/24** などと入力します。

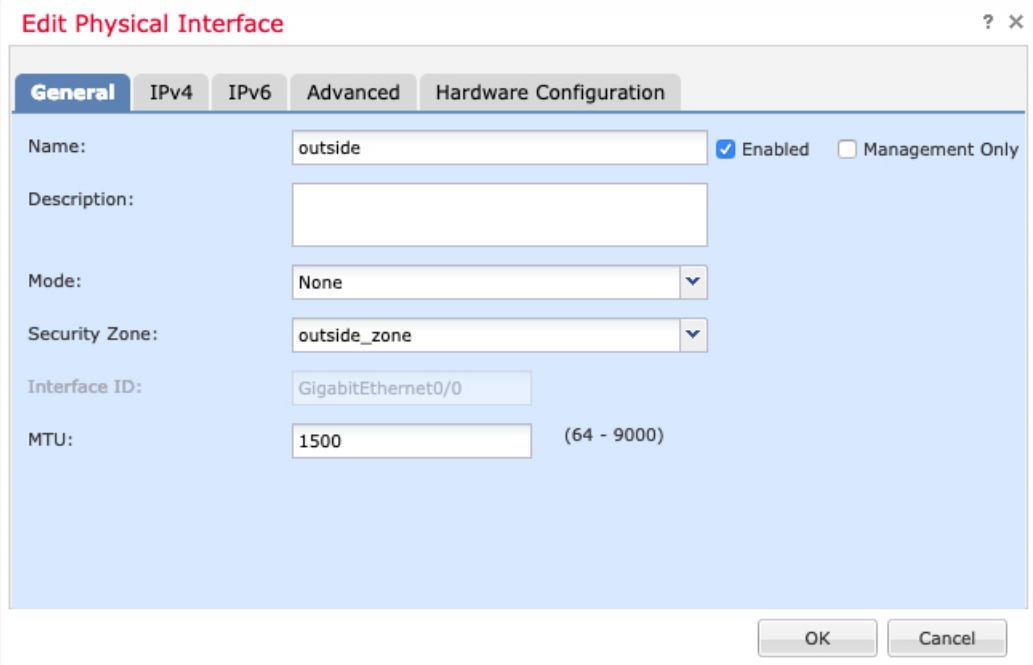


- [IPv6]：ステートレス自動設定の場合は [自動設定（Autoconfiguration）] チェックボックスをオンにします。

h) [OK] をクリックします。

ステップ 6 外部用に使用する Ethernet1/1 のをクリックします。

[全般（General）] タブが表示されます。



（注） 管理アクセス用にこのインターフェイスを事前に設定している場合、インターフェイスにはすでに名前が付けられており、有効化とアドレス指定が完了しています。これらの基本設定は変更しないでください。変更すると、Management Center の管理接続が中断されます。この画面でも、通過トラフィックポリシーのセキュリティゾーンを設定できます。

a) 48 文字までの [名前（Name）] を入力します。

たとえば、インターフェイスに「outside」という名前を付けます。

b) [有効（Enabled）] チェックボックスをオンにします。

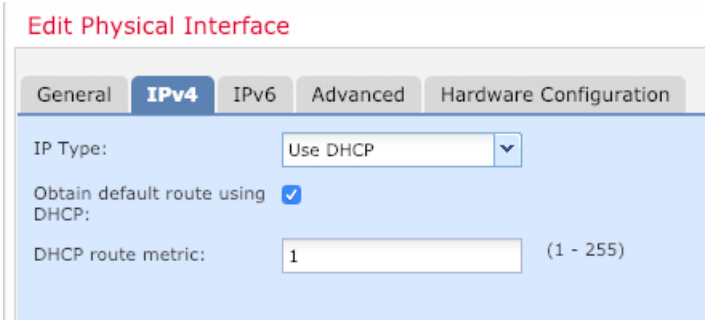
c) [モード（Mode）] は [なし（None）] に設定したままにします。

d) [セキュリティゾーン（Security Zone）] ドロップダウンリストから既存の外部セキュリティゾーンを選択するか、[新規（New）] 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。

たとえば、「outside_zone」という名前のゾーンを追加します。

e) [IPv4] タブ、[IPv6] タブ、または両方のタブをクリックします。

- [IPv4]：[DHCPの使用（Use DHCP）] を選択し、次のオプションのパラメータを設定します。
  - [DHCP を使用してデフォルト ルートを取得（Obtain default route using DHCP）]：DHCP サーバーからデフォルト ルートを取得します。
  - [DHCPルートメトリック（DHCP route metric）]：アドミニストレーティブ ディスタンスを学習したルートに割り当てます（1 ～ 255）。学習したルートのデフォルトのアドミニストレーティブ ディスタンスは 1 です。



- [IPv6]：ステートレス自動設定の場合は [自動設定（Autoconfiguration）] チェックボックスをオンにします。

f) [OK] をクリックします。

ステップ 7 [保存（Save）] をクリックします。

インターフェイスの設定（6.4）

Threat Defense インターフェイスを有効にし、それらをセキュリティゾーンに割り当てて IP アドレスを設定します。通常は、システムで意味のあるトラフィックを通過させるように、少なくとも 2 つのインターフェイスを設定する必要があります。通常は、アップストリームルータまたはインターネットに面した外部インターフェイスと、組織のネットワークの 1 つ以上の内部インターフェイスを使用します。これらのインターフェイスの一部は、Web サーバーなどのパブリックアクセスが可能なアセットを配置する「緩衝地帯」（DMZ）となる場合があります。

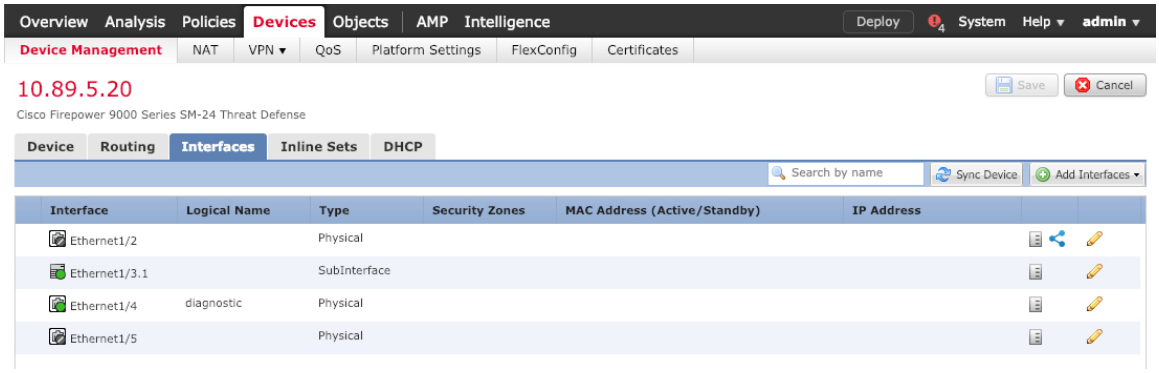
一般的なエッジルーティングの状況は、内部インターフェイスでスタティックアドレスを定義すると同時に、ISP から DHCP を介して外部インターフェイスアドレスを取得することです。

次の例では、DHCP によるスタティックアドレスとルーテッドモードの外部インターフェイスを使用して、ルーテッドモードの内部インターフェイスを設定します。

手順

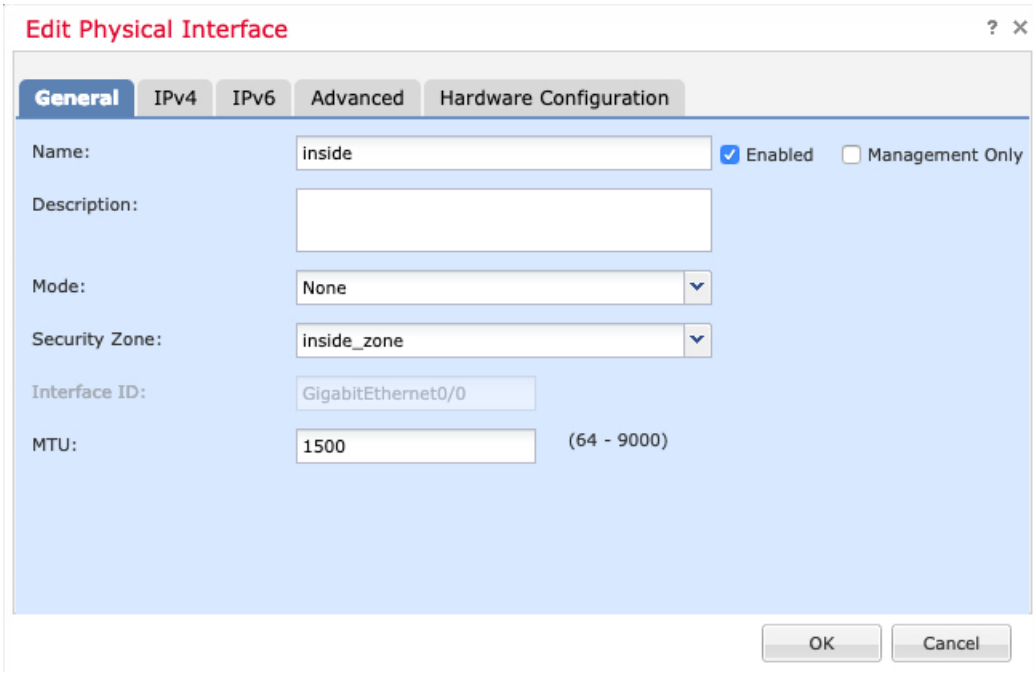
ステップ 1 [デバイス（Devices）]>[デバイス管理（Device Management）] の順に選択し、ファイアウォールの をクリックします。

ステップ 2 [インターフェイス（Interfaces）] をクリックします。



ステップ 3 内部に使用するインターフェイスの をクリックします。

[全般（General）] タブが表示されます。



a) 48 文字までの [名前（Name）] を入力します。

たとえば、インターフェイスに **inside** という名前を付けます。

b) [有効（Enabled）] チェックボックスをオンにします。

c) [モード（Mode）] は [なし（None）] に設定したままにします。

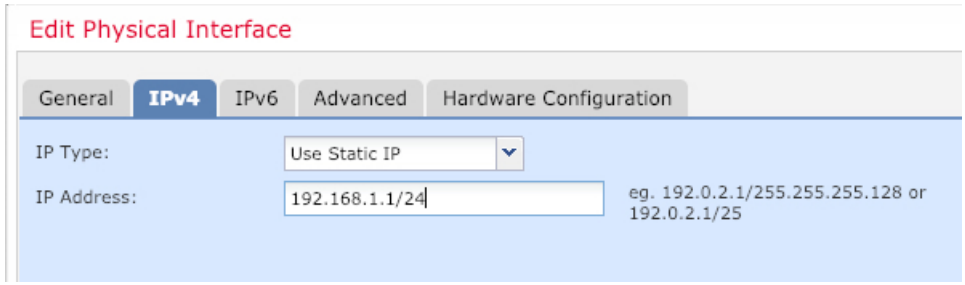
d) [セキュリティゾーン（Security Zone）] ドロップダウンリストから既存の内部セキュリティゾーンを選択するか、[新規（New）] をクリックして新しいセキュリティゾーンを追加します。

たとえば、**inside_zone** という名前のゾーンを追加します。各インターフェイスは、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割り当てる必要があります。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も、複数のインターフェイスグループに属することもできます。ゾーンまたはグループに基づいてセキュリティポリシーを適用します。たとえば、内部インターフェイスを内部ゾーンに割り当て、外部インターフェイスを外部ゾーンに割り当てることができます。この場合、トラフィックが内部から外部に移動できるようにアクセス コントロール ポリシーを設定することはできますが、外部から内部に向けては設定できません。ほとんどのポリシーはセキュリティゾーンのみサポートしています。NAT ポリシー、プレフィルタ ポリシー、および QoS ポリシーで、ゾーンまたはインターフェイスグループを使用できます。

e) [IPv4] タブ、[IPv6] タブ、または両方のタブをクリックします。

- [IPv4]：ドロップダウンリストから [スタティックIPを使用する（Use Static IP）] を選択し、IP アドレスとサブネットマスクをスラッシュ表記で入力します。

  たとえば、**192.168.1.1/24** などと入力します。

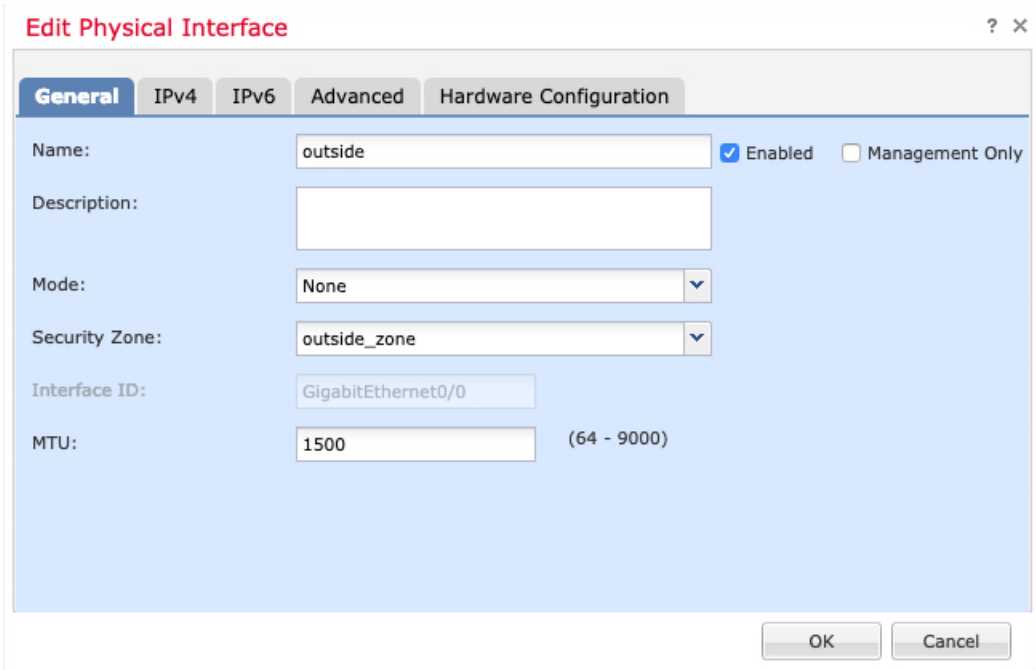


- [IPv6]：ステートレス自動設定の場合は [自動設定（Autoconfiguration）] チェックボックスをオンにします。

f) [OK] をクリックします。

ステップ 4 「外部」に使用するインターフェイスをクリックします。

[全般（General）] タブが表示されます。



（注） 管理アクセス用にこのインターフェイスを事前に設定している場合、インターフェイスにはすでに名前が付けられており、有効化とアドレス指定が完了しています。これらの基本設定は変更しないでください。変更すると、Management Center の管理接続が中断されます。この画面でも、通過トラフィックポリシーのセキュリティゾーンを設定できます。

a) 48 文字までの [名前（Name）] を入力します。

たとえば、インターフェイスに「outside」という名前を付けます。

b) [有効（Enabled）] チェックボックスをオンにします。

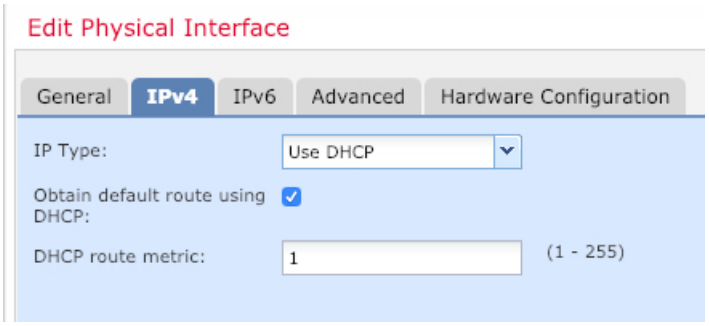
c) [モード（Mode）] は [なし（None）] に設定したままにします。

d) [セキュリティゾーン（Security Zone）] ドロップダウンリストから既存の外部セキュリティゾーンを選択するか、[新規（New）] 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。

たとえば、「outside_zone」という名前のゾーンを追加します。

e) [IPv4] タブ、[IPv6] タブ、または両方のタブをクリックします。

- [IPv4]：[DHCPの使用（Use DHCP）] を選択し、次のオプションのパラメータを設定します。
  - [DHCP を使用してデフォルト ルートを取得（Obtain default route using DHCP）]：DHCP サーバーからデフォルト ルートを取得します。
  - [DHCPルートメトリック（DHCP route metric）]：アドミニストレーティブ ディスタンスを学習したルートに割り当てます（1 ～ 255）。学習したルートのデフォルトのアドミニストレーティブ ディスタンスは 1 です。



- [IPv6]：ステートレス自動設定の場合は [自動設定（Autoconfiguration）] チェックボックスをオンにします。

f) [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックします。

DHCP サーバーの設定

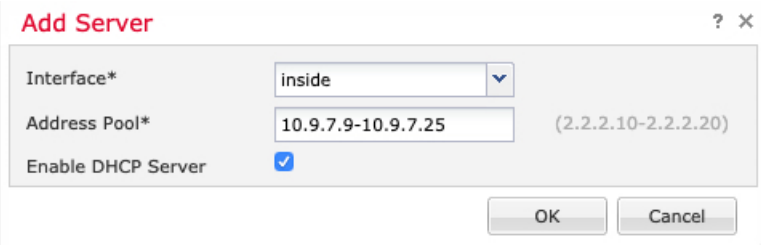
クライアントで DHCP を使用して Threat Defense から IP アドレスを取得するようにする場合は、DHCP サーバーを有効にします。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、デバイスをクリックします。

ステップ 2 **[DHCP] > [DHCPサーバー（DHCP Server）]** を選択します。

ステップ 3 **[サーバー（Server）]** ページで、**[追加（Add）]** をクリックして、次のオプションを設定します。



- [インターフェイス（Interface）]：ドロップダウンリストからインターフェイスを選択します。
- [アドレスプール（Address Pool）]：DHCP サーバーが使用する IP アドレスの最下位から最上位の間の範囲を設定します。IP アドレスの範囲は、選択したインターフェイスと同じサブネット上に存在する必要があり、インターフェイス自身の IP アドレスを含めることはできません。
- [DHCPサーバーを有効にする（Enable DHCP Server）]：選択したインターフェイスの DHCP サーバーを有効にします。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックします。

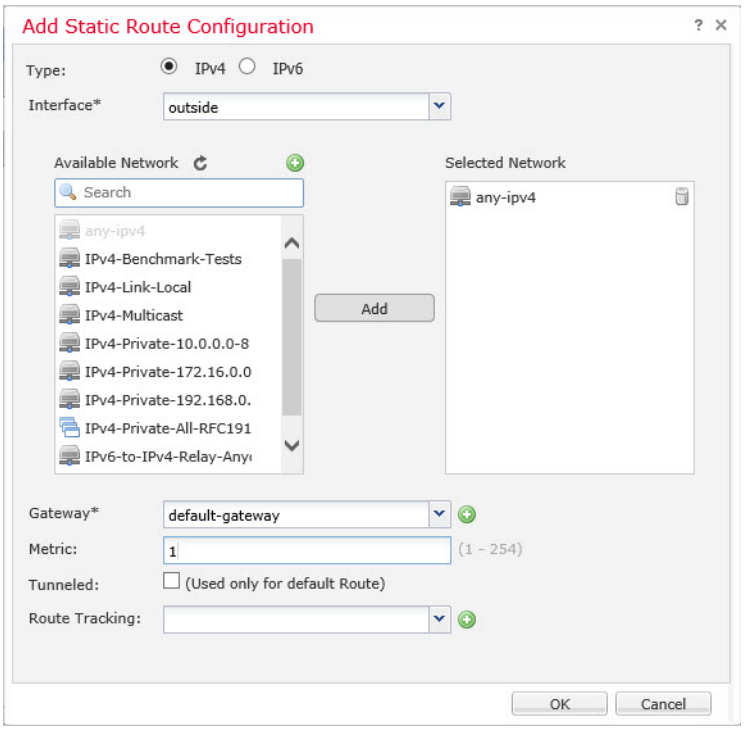
デフォルトルートの追加

デフォルトルートは通常、外部インターフェイスから到達可能なアップストリームルータを指し示します。外部インターフェイスに DHCP を使用する場合は、デバイスがすでにデフォルトルートを受信している可能性があります。手動でルートを追加する必要がある場合は、次の手順を実行します。DHCP サーバーからデフォルトルートを受信した場合は、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[ルーティング（Routing）]** > **[スタティックルート（Static Route）]**ページの [IPv4ルート（IPv4 Routes）] または [IPv6ルート（IPv6 Routes）] テーブルに表示されます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、デバイスをクリックします。

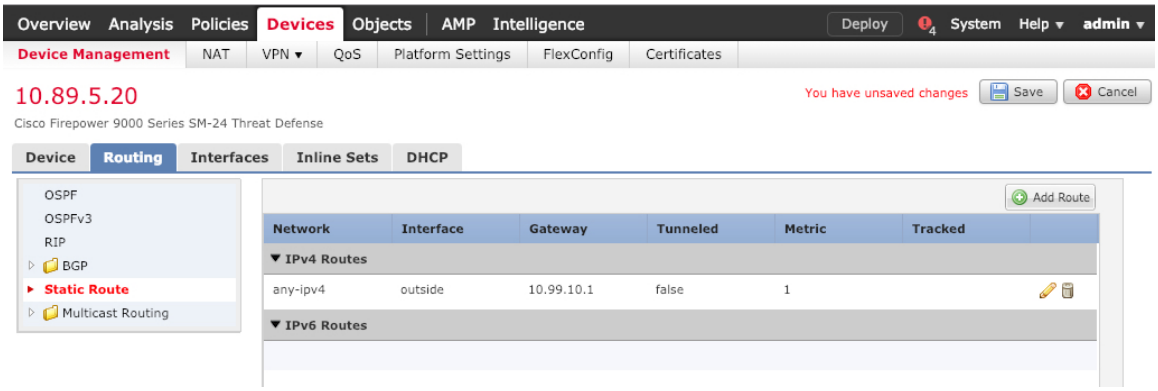
ステップ 2 **[ルーティング（Routing）]** > **[スタティックルート（Static route）]** を選択し、[ルートを追加（Add route）] をクリックして、次のように設定します。



- [タイプ（Type）]：追加するスタティックルートのタイプに応じて、[IPv4] または [IPv6] オプションボタンをクリックします。
- [インターフェイス（Interface）]：出力インターフェイスを選択します。通常は外部インターフェイスです。
- [使用可能なネットワーク（Available Network）]：IPv4 デフォルト ルートの場合は [ipv4] を選択し、IPv6 デフォルト ルートの場合は [any] を選択し、[追加（Add）] をクリックして [選択したネットワーク（Selected Network）] リストに移動させます。
- [ゲートウェイ（Gateway）] または [IPv6ゲートウェイ（IPv6 Gateway）]：このルートのネクストホップであるゲートウェイルータを入力または選択します。IP アドレスまたはネットワーク/ホストオブジェクトを指定できます。
- [メトリック（Metric）]：宛先ネットワークへのホップの数を入力します。有効値の範囲は 1 ～ 255 で、デフォルト値は 1 です。

ステップ 3 [OK] をクリックします。

ルートがスタティックルートテーブルに追加されます。



ステップ 4 [保存（Save）] をクリックします。

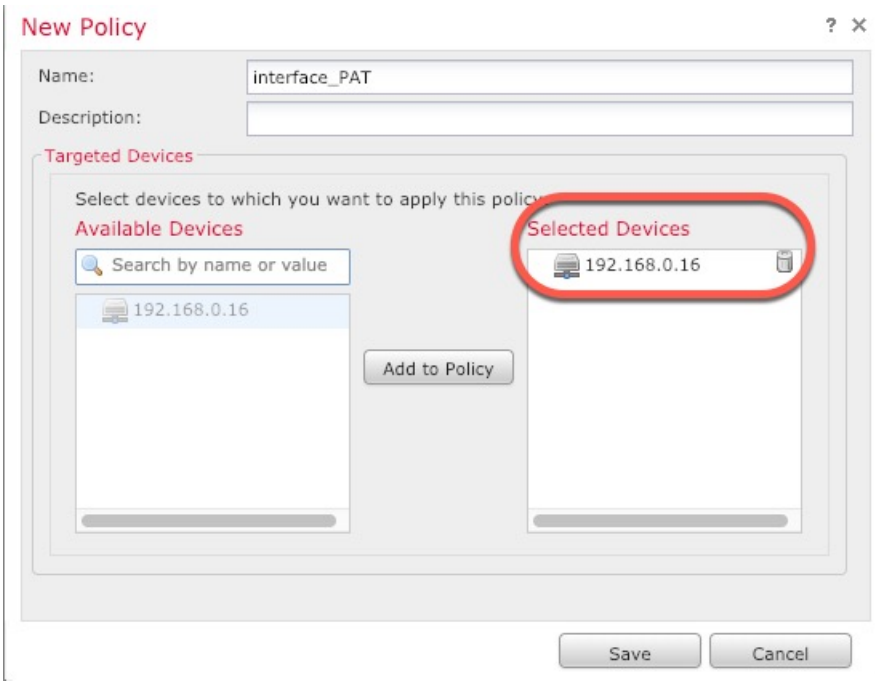
NAT の設定

一般的な NAT ルールでは、内部アドレスを外部インターフェイスの IP アドレスのポートに変換します。このタイプの NAT ルールのことをインターフェイス ポート アドレス変換（PAT）と呼びます。

手順

ステップ 1 **[デバイス（Devices）] > [NAT]** をクリックし、**[新しいポリシー（New Policy）] > [Threat Defense NAT]** をクリックします。

ステップ 2 ポリシーに名前を付け、ポリシーを使用するデバイスを選択し、[保存（Save）] をクリックします。



ポリシーが Management Center に追加されます。引き続き、ポリシーにルールを追加する必要があります。

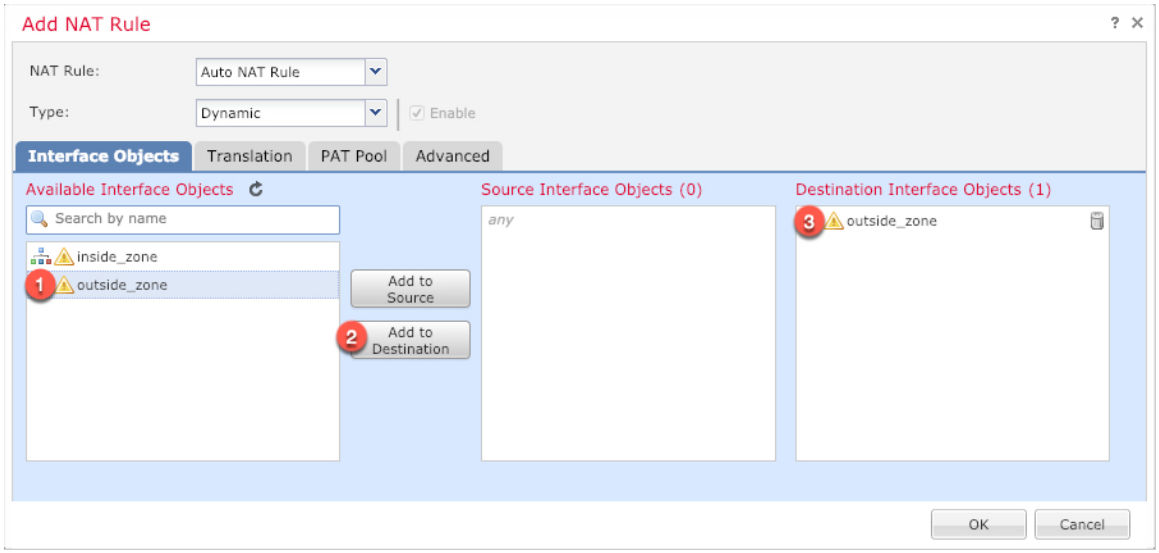
ステップ 3 [ルールの追加（Add Rule）] をクリックします。

[NATルールの追加（Add NAT Rule）] ダイアログボックスが表示されます。

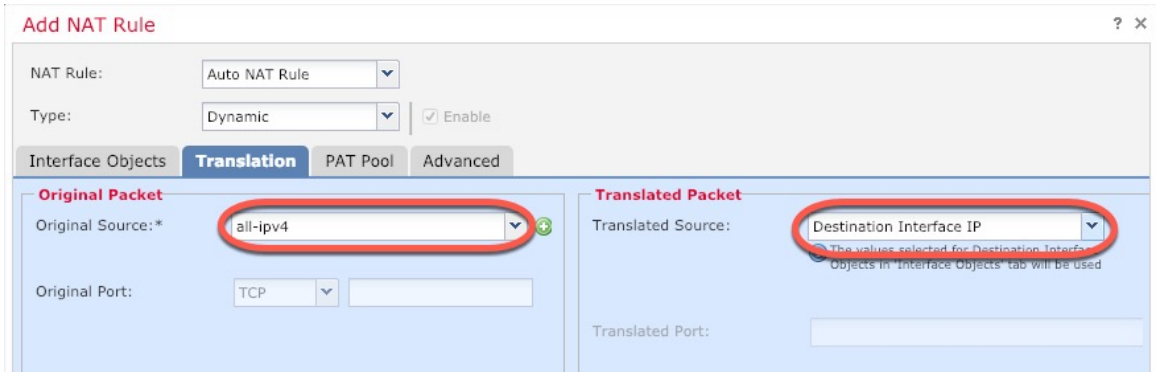
ステップ 4 基本ルールのオプションを設定します。

- [NATルール（NAT Rule）] : [自動NATルール（Auto NAT Rule）] を選択します。
- [タイプ（Type）] : [ダイナミック（Dynamic）] を選択します。

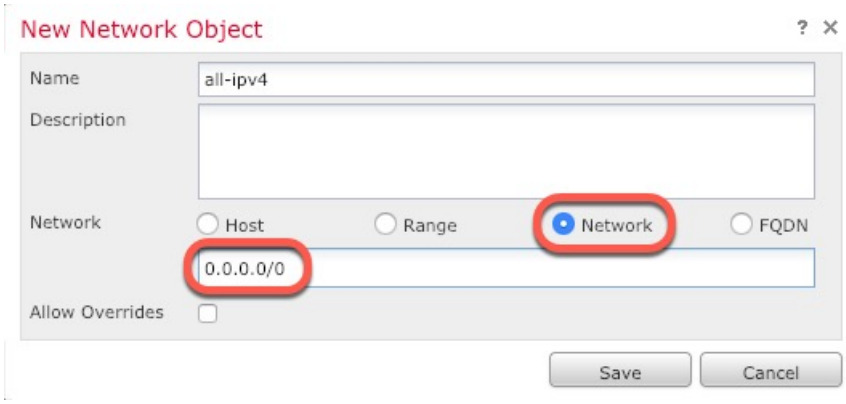
ステップ 5 [インターフェイスオブジェクト（Interface objects）] ページで、[使用可能なインターフェイスオブジェクト（Available Interface Objects）] 領域から [宛先インターフェイスオブジェクト（Destination Interface Objects）] 領域に外部ゾーンを追加します。



ステップ 6 [変換（Translation）] ページで、次のオプションを設定します。



- [元の送信元（Original Source）]：をクリックして、すべての IPv4 トラフィック（0.0.0.0/0）のネットワークオブジェクトを追加します。

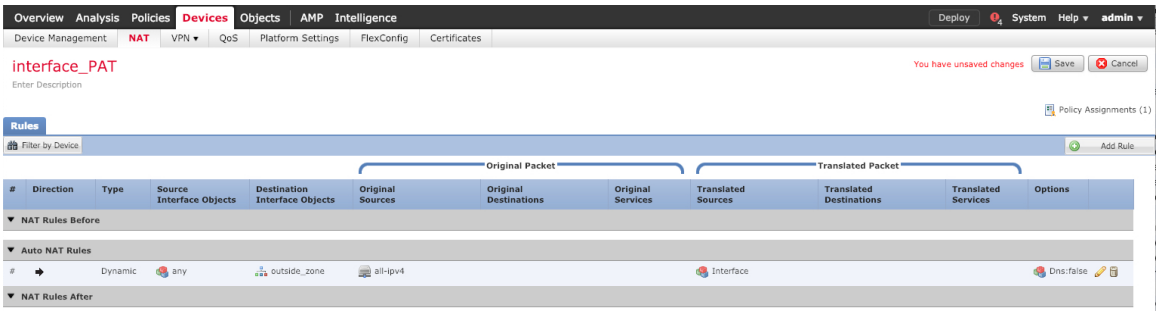


（注） 自動 NAT ルールはオブジェクト定義の一部として NAT を追加するため、システム定義の **any-ipv4** オブジェクトを使用することはできません。また、システム定義のオブジェクトを編集することはできません。

- [変換済みの送信元（Translated Source）]：[宛先インターフェイスIP（Destination Interface IP）] を選択します。

ステップ 7 [保存（Save）] をクリックしてルールを追加します。

ルールが [ルール（Rules）] テーブルに保存されます。



ステップ 8 NAT ページで [保存（Save）] をクリックして変更を保存します。

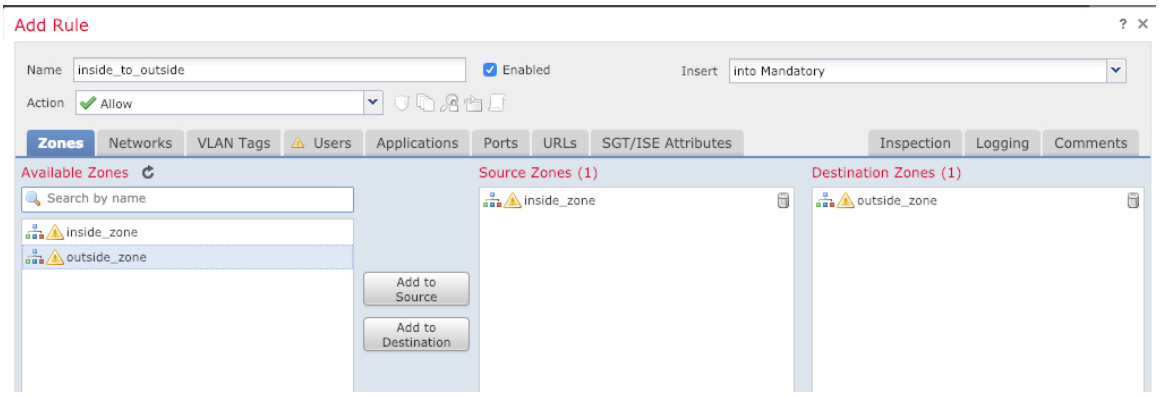
内部から外部へのトラフィックの許可

Threat Defense を登録したときに、基本の [すべてのトラフィックをブロック（Block all traffic）] アクセス コントロール ポリシーを作成した場合は、デバイスを通過するトラフィックを許可するためにポリシーにルールを追加する必要があります。次の手順では、内部ゾーンから外部ゾーンへのトラフィックを許可するルールを追加します。他にゾーンがある場合は、適切なネットワークへのトラフィックを許可するルールを追加してください。

手順

ステップ 1 **[ポリシー（Policy）] > [アクセスポリシー（Access Policy）] > [アクセスポリシー（Access Policy）]**を選択し、Threat Defense に割り当てられているアクセス コントロール ポリシーのをクリックします。

ステップ 2 **[ルールを追加（Add Rule）]** をクリックし、次のパラメータを設定します。

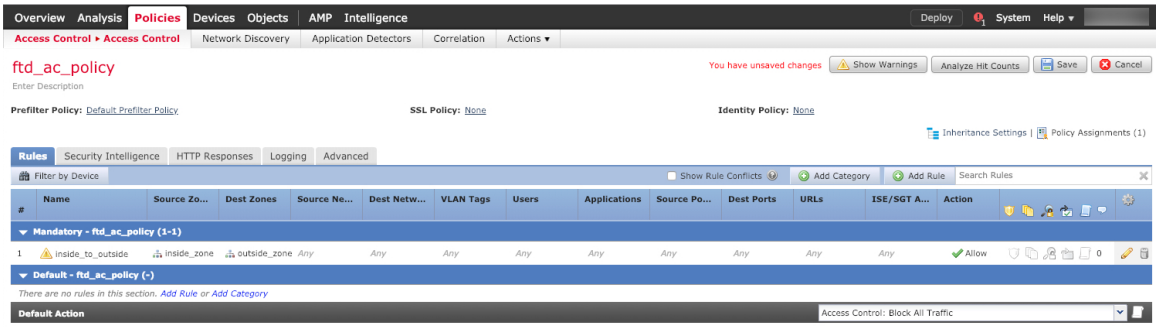


- [名前（Name）]：このルールに名前を付けます（たとえば、**inside_to_outside**）。
- [送信元ゾーン（Source Zones）]：[使用可能なゾーン（Available Zones）] から内部ゾーンを選択し、[送信元に追加（Add to Source）] をクリックします。
- [宛先ゾーン（Destination Zones）]：[使用可能なゾーン（Available Zones）] から外部ゾーンを選択し、[宛先に追加（Add to Destination）] をクリックします。

他の設定はそのままにしておきます。

ステップ 3 [追加（Add）] をクリックします。

ルールが [ルール（Rules）] テーブルに追加されます。



ステップ 4 [保存（Save）] をクリックします。

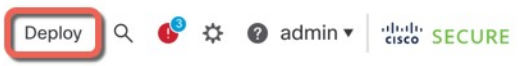
設定の展開

設定の変更を Threat Defense に展開します。変更を展開するまでは、デバイス上でどの変更もアクティブになりません。

手順

ステップ 1 右上の [展開（Deploy）] をクリックします。

図 *9*：[展開（*Deploy*）]



ステップ 2 [すべて展開（Deploy All）] をクリックしてすべてのデバイスに展開するか、[高度な展開（Advanced Deploy）] をクリックして選択したデバイスに展開します。

図 *10* : すべて展開

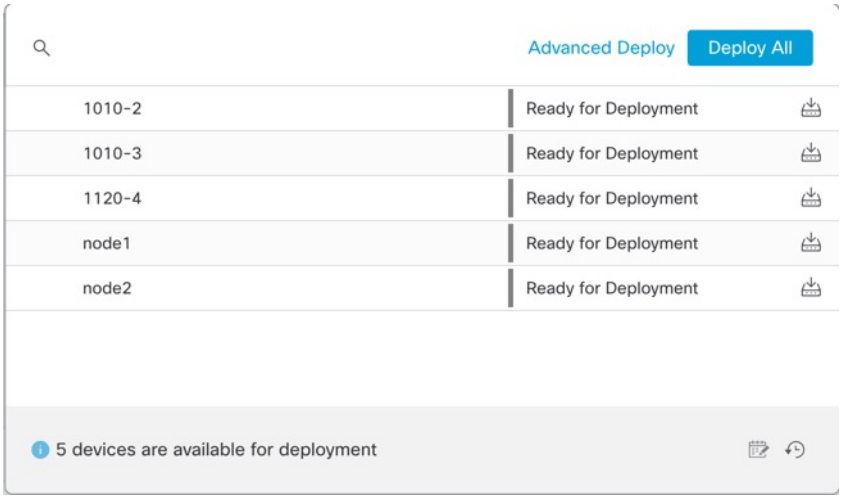
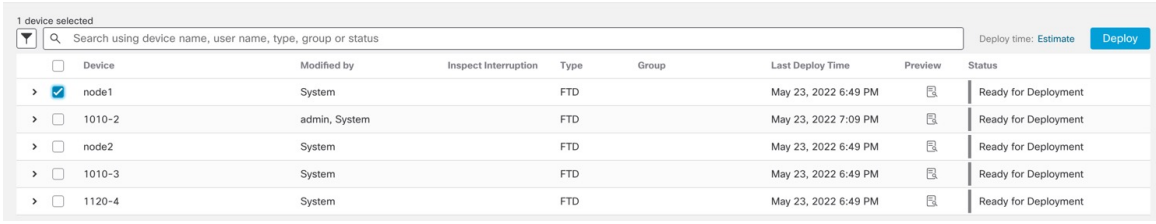
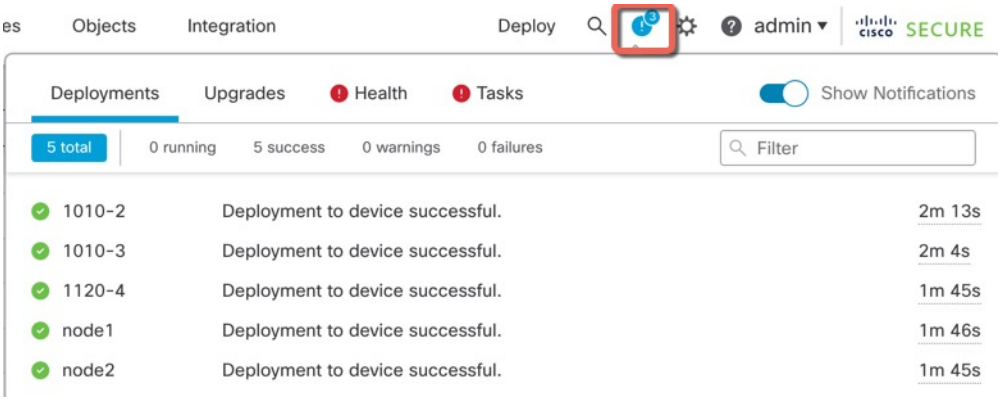


図 *11* : 高度な展開



ステップ 3 展開が成功したことを確認します。展開のステータスを表示するには、メニューバーの [展開（Deploy）] ボタンの右側にあるアイコンをクリックします。

図 *12* : 展開ステータス



Threat Defense および FXOS CLI へのアクセス

コマンドラインインターフェイス（CLI）を使用してシステムのセットアップを行い、基本的なシステムのトラブルシューティングを行います。CLIセッションからポリシーを設定することはできません。CLI には、コンソール ポートに接続してアクセスできます。

トラブルシューティングのためにも FXOS CLI にアクセスできます。

（注） または、Threat Defense デバイスの管理インターフェイスに SSH で接続できます。コンソールセッションとは異なり、SSH セッションはデフォルトで Threat Defense CLI になり、**connect fxos** コマンドを使用して FXOS CLI に接続できます。SSH 接続用のインターフェイスを開いている場合、後でデータインターフェイス上のアドレスに接続できます。データ インターフェイスへの SSH アクセスはデフォルトで無効になっています。この手順では、デフォルトで FXOS CLI となるコンソールポートアクセスについて説明します。

手順

ステップ 1 CLI にログインするには、管理コンピュータをコンソール ポートに接続します。 Firepower 1000 には、USB A to B シリアル ケーブルが付属しています。お使いのオペレーティングシステムに必要な USB シリアルドライバを必ずインストールしてください（Firepower 1010 ハードウェアガイドを参照）。コンソールポートはデフォルトで FXOS CLI になります。次のシリアル設定を使用します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

FXOS CLI に接続します。ユーザー名 **admin** と、初期セットアップ時に設定したパスワードを使用して CLI にログインします（デフォルトは **Admin123**）。

例：

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

ステップ 2 Threat Defense CLI にアクセスします。

connect ftd

例：

```
firepower# connect ftd
>
```

ログイン後に、CLI で使用可能なコマンドの情報を確認するには、**help** または **?** を入力します。使用方法については、『Cisco Secure Firewall Threat Defense コマンドリファレンス』を参照してください。

ステップ 3 Threat Defense CLI を終了するには、**exit** または **logout** コマンドを入力します。

このコマンドにより、FXOS CLI プロンプトに戻ります。FXOS CLI で使用可能なコマンドについては、**?** を入力してください。

例：

```
> exit
firepower#
```

ファイアウォールの電源の切断

システムを適切にシャットダウンすることが重要です。単純に電源プラグを抜いたりすると、重大なファイルシステムの損傷を引き起こすことがあります。バックグラウンドでは常に多数のプロセスが実行されており、電源プラグを抜いたり、電源を切断したりすると、ファイアウォールシステムをグレースフルシャットダウンできないことを覚えておいてください。

Firepower 1010 シャーシには外部電源スイッチはありません。Management Center のデバイス管理ページを使用してデバイスの電源を切断するか、FXOS CLI を使用できます。

Management Center を使用したファイアウォールの電源の切断

システムを適切にシャットダウンすることが重要です。単純に電源プラグを抜いたり、電源スイッチを押したりすると、重大なファイルシステムの損傷を引き起こすことがあります。バックグラウンドでは常に多数のプロセスが実行されていて、電源プラグを抜いたり、電源を切断したりすると、ファイアウォールをグレースフルシャットダウンできないことを覚えておいてください。

Management Center を使用してシステムを適切にシャットダウンできます。

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 再起動するデバイスの横にある編集アイコン（ ）をクリックします。

ステップ 3 [デバイス（Device）] タブをクリックします。

ステップ 4 [システム（System）]セクションでデバイスのシャットダウンアイコン（）をクリックします。

ステップ 5 プロンプトが表示されたら、デバイスのシャットダウンを確認します。

ステップ 6 コンソールからファイアウォールに接続している場合は、ファイアウォールがシャットダウンするときにシステムプロンプトをモニターします。次のプロンプトが表示されます。

```
System is stopped.
It is safe to power off now.

Do you want to reboot instead? [y/N]
```

コンソールから接続していない場合は、約3分間待ってシステムがシャットダウンしたことを確認します。

ステップ 7 必要に応じて電源プラグを抜いてシャーシから物理的に電源を取り外すことができます。

CLI でのデバイスの電源オフ

FXOS CLI を使用すると、システムを安全にシャットダウンし、デバイスの電源をオフにできます。CLI には、コンソールポートに接続してアクセスします。Threat Defense および FXOS CLI へのアクセス （48 ページ）を参照してください。

手順

ステップ 1 FXOS CLI で local-mgmt に接続します。

firepower # **connect local-mgmt**

ステップ 2 **shutdown** コマンドを発行します。

firepower(local-mgmt) # **shutdown**

例：

```
firepower(local-mgmt)# shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
```

ステップ 3 ファイアウォールのシャットダウン時にシステムプロンプトをモニターします。次のプロンプトが表示されます。

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

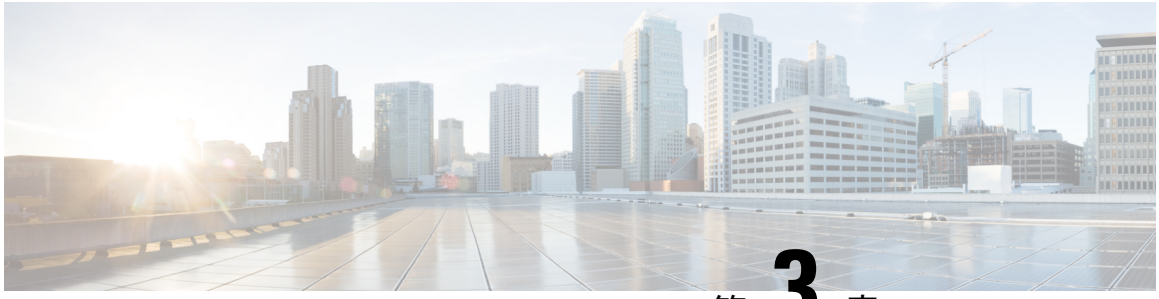
ステップ 4 必要に応じて電源プラグを抜いてシャーシから物理的に電源を取り外すことができます。

次のステップ

Threat Defense の設定を続行するには、「Cisco Firepower ドキュメント一覧」にあるお使いのソフトウェアバージョンのマニュアルを参照してください。

Management Center の使用に関する情報については、「Firepower Management Center コンフィギュレーション ガイド」を参照してください。

次のステップ



第 3 章

リモート Threat Defense による Management Center の展開

この章の対象読者

使用可能なすべてのオペレーティングシステムとマネージャを確認するには、「最適なオペレーティングシステムとマネージャを見つける方法 （1 ページ）」を参照してください。この章は、中央の本社の Management Center を使用するリモート支社の Threat Defense に適用されます。

各 Threat Defense は、トラフィックを制御、検査、監視、および分析して、管理 Management Center に報告します。Management Center は、サービスの管理、分析、レポートのタスクを実行できる Web インターフェイスを備えた集中管理コンソールを提供し、ローカルネットワークを保護します。

- 中央の本社の管理者が、CLI または Device Manager を使用して Threat Defense を事前設定してから、リモート支社に Threat Defense を送信します
- 支社の管理者が、Threat Defense をケーブルで接続して電源をオンにします。
- 中央の管理者が、Management Center を使用して Threat Defense の設定を完了します。

（注） リモート支社への展開には、バージョン 6.7 以降が必要です。

ファイアウォールについて

ハードウェアでは、Threat Defense ソフトウェアまたは ASA ソフトウェアを実行できます。Threat Defense と ASA の間で切り替えを行う際には、デバイスの再イメージ化が必要になります。現在インストールされているものとは異なるソフトウェアバージョンが必要な場合も再イメージ化が必要です。「Cisco ASA および Firepower Threat Defense 再イメージ化ガイド」を参照してください。

ファイアウォールは、Secure Firewall eXtensible オペレーティングシステム（FXOS）と呼ばれる基盤となるオペレーティングシステムを実行します。ファイアウォールは FXOS Secure Firewall Chassis Manager をサポートしていません。トラブルシューティング用として限られた CLI のみ

がサポートされています。詳細については、Firepower 1000/2100 および Secure Firewall 3100 と Firepower Threat Defense の Cisco FXOS トラブルシューティング ガイドを参照してください。

プライバシー収集ステートメント：ファイアウォールには個人識別情報は不要で、積極的に収集することもありません。ただし、ユーザー名などの設定では、個人識別情報を使用できます。この場合、設定作業時やSNMPの使用時に、管理者が個人識別情報を確認できる場合があります。

- リモート管理の仕組み （54 ページ）
- はじめる前に （56 ページ）
- エンドツーエンドの手順 （56 ページ）
- 中央の管理者による事前設定 （58 ページ）
- 支社へのインストール （72 ページ）
- 中央の管理者による事後設定 （74 ページ）

リモート管理の仕組み

Management Center でインターネットを介して Threat Defense を管理できるようにするには、管理インターフェイスの代わりに外部のインターフェイスを使用して Management Center を管理します。ほとんどのリモート支社には 1 つのインターネット接続しかないため、外部から Management Center にアクセスして中央管理を行えるようにします。

（注） マネージャアクセスには任意のデータインターフェイスを使用できます。たとえば、内部 Management Center がある場合は内部インターフェイスを使用できます。ただし、このガイドでは主に外部インターフェイスアクセスについて説明します。これは、リモート支社で最も用いられる可能性が高いシナリオであるためです。

管理インターフェイスは、Threat Defense データインターフェイスとは別に設定される特別なインターフェイスであり、独自のネットワーク設定があります。データインターフェイスでマネージャアクセスを有効にした場合でも、管理インターフェイスのネットワーク設定が使用されます。すべての管理トラフィックは、引き続き管理インターフェイスを発信元または宛先とします。データインターフェイスでマネージャアクセスを有効にすると、Threat Defense はバックプレーンを介して管理インターフェイスに着信管理トラフィックを転送します。発信管理トラフィックの場合、管理インターフェイスはバックプレーンを介してデータインターフェイスにトラフィックを転送します。

データインターフェイスからのマネージャアクセスには、次の制限があります。

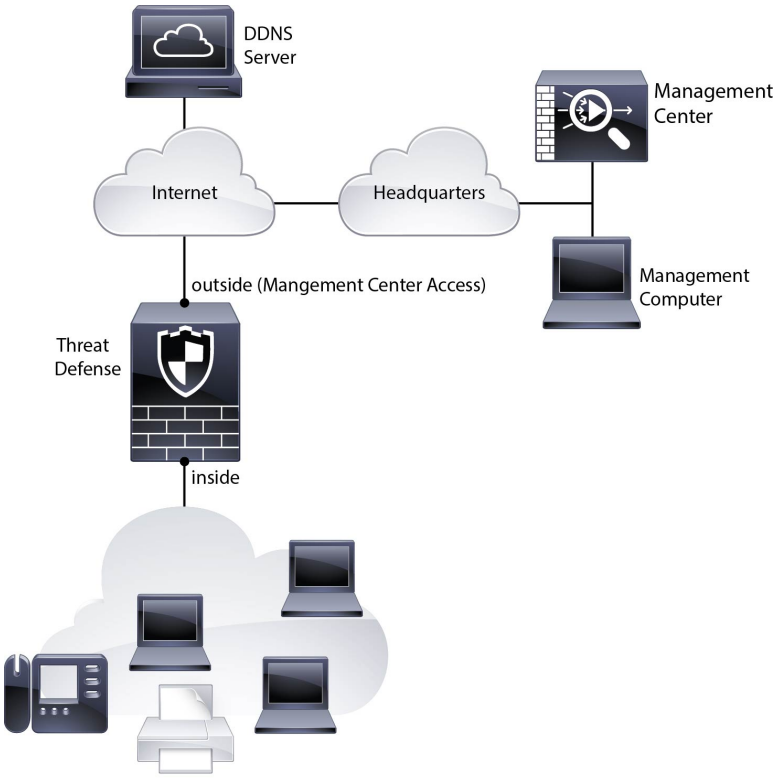
- マネージャアクセスを有効にできるのは、1 つの物理的なデータインターフェイスのみです。サブインターフェイスと EtherChannel は使用できません。冗長性を目的として、Management Center の単一のセカンダリインターフェイスでマネージャアクセスを有効にすることもできます。
- このインターフェイスは管理専用にできません。

- ルーテッドインターフェイスを使用するルーテッドファイアウォールモードのみです。
- PPPoE はサポートされていません。ISP で PPPoE が必要な場合は、PPPoE をサポートするルータを Threat Defense と WAN モデムの間に配置する必要があります。
- インターフェイスを配置する必要があるのはグローバル VRF のみです。
- SSH はデータインターフェイスではデフォルトで有効になっていないため、後で Management Center を使用して SSH を有効にする必要があります。また、管理インターフェイス ゲートウェイがデータインターフェイスに変更されるため、**configure network static-routes** コマンドを使用して管理インターフェイス用の静的ルートを追加しない限り、リモートネットワークから管理インターフェイスに SSH 接続することはできません。
- ハイアベイラビリティはサポートされません。この場合、管理インターフェイスを使用する必要があります。

次の図は、中央の本社にある Management Center と外部インターフェイスでマネージャアクセスを持つ Threat Defense を示しています。

Threat Defense と Management Center ではどちらも、インバウンド管理接続を許可するためのパブリック IP アドレスまたはホスト名が必要であり、初期設定のためにこのような IP アドレスを把握しておかなければなりません。DHCP IP の割り当ての変更に対応するために、オプションで外部インターフェイスのダイナミック DNS（DDNS）を設定することもできます。

図 *13 :*



はじめる前に

Management Center の初期設定を展開して実行します。Cisco Firepower Management Center 1600, 2600, and 4600 Hardware Installation GuideまたはCisco Secure Firewall Management Center Virtual 入門ガイドを参照してください。

エンドツーエンドの手順

シャーシで Management Center を使用して Threat Defense を展開するには、次のタスクを参照してください。

図 *14* : エンドツーエンドの手順

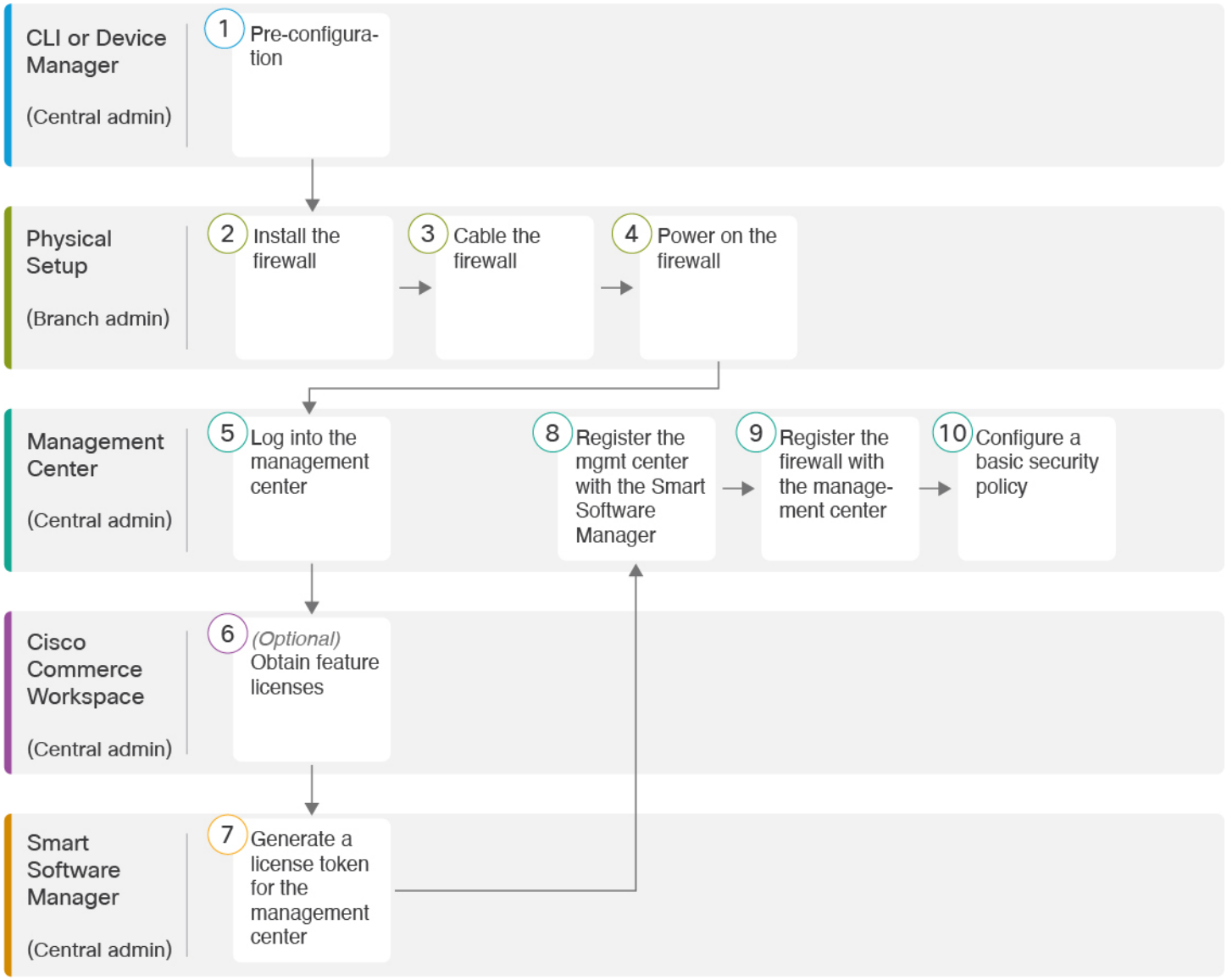


図 *15* : エンドツーエンドの手順

1	CLI または Device Manager （中央の管理者）	• （任意）ソフトウェアの確認と新しいバージョンのインストール （58 ページ） • CLI を使用した事前設定 （66 ページ） • Device Manager を使用した事前設定 （60 ページ）
2	物理的なセットアップ （支社の管理者）	ファイアウォールをインストールします。ハードウェア設置ガイドを参照してください。

3	物理的なセットアップ （支社の管理者）	ファイアウォールのケーブル接続 （72 ページ）。
4	物理的なセットアップ （支社の管理者）	デバイスの電源投入 （73 ページ）
5	Management Center （中央の管理者）	中央の管理者：Management Center へのログイン （25 ページ）。
6	Cisco Commerce Workspace （中央の管理者）	Management Center のライセンスの取得 （74 ページ） ：機能ライセンスを購入します。
7	Smart Software Manager （中央の管理者）	Management Center のライセンスの取得 （74 ページ） ：Management Center のライセンストークンを生成します。
8	Management Center （中央の管理者）	Management Center のライセンスの取得 （74 ページ） ：スマートライセンシング サーバーに Management Center を登録します。
9	Management Center （中央の管理者）	Management Center への Threat Defense の登録 （76 ページ）。
10	Management Center （中央の管理者）	基本的なセキュリティポリシーの設定 （79 ページ）。

中央の管理者による事前設定

Threat Defense は、支社に送信する前に手動で事前に設定する必要があります。

（任意）ソフトウェアの確認と新しいバージョンのインストール

ソフトウェアのバージョンを確認し、必要に応じて別のバージョンをインストールするには、次の手順を実行します。ファイアウォールを設定する前に対象バージョンをインストールすることをお勧めします。別の方法として、稼働後にアップグレードを実行することもできますが、設定を保持するアップグレードでは、この手順を使用するよりも時間がかかる場合があります。

実行するバージョン

ソフトウェア ダウンロード ページのリリース番号の横にある、金色の星が付いている Gold Star リリースを実行することをお勧めします。https://www.cisco.com/c/en/us/products/collateral/

security/firewalls/bulletin-c25-743178.html に記載されているリリース戦略も参照してください。たとえば、この速報では、（最新機能を含む）短期的なリリース番号、長期的なリリース番号（より長期間のメンテナンスリリースとパッチ）、または非常に長期的なリリース番号（政府認定を受けるための最長期間のメンテナンスリリースとパッチ）について説明しています。

手順

ステップ 1 CLI に接続します。詳細については、Threat Defense および FXOS CLI へのアクセス （92 ページ）を参照してください。この手順ではコンソールポートを使用していますが、代わりに SSH を使用することもできます。

admin ユーザとデフォルトパスワードの **Admin123** を使用してログインします。

FXOS CLI に接続します。初めてログインしたとき、パスワードを変更するよう求められます。このパスワードは、SSH の Threat Defense ログインにも使用されます。

（注） パスワードがすでに変更されていて、パスワードがわからない場合は、初期設定へのリセットを実行して、パスワードをデフォルトにリセットする必要があります。初期設定へのリセット手順については、『FXOS troubleshooting guide』を参照してください。

例：

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

ステップ 2 FXOS CLI で、実行中のバージョンを表示します。

scope ssa

show app-instance

例：

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name      Slot ID     Admin State      Operational State     Running Version
Startup Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd                   1          Enabled          Online               7.2.0.65
```

```
7.2.0.65          Not Applicable
```

ステップ 3 新しいバージョンをインストールする場合は、次の手順を実行します。

a) 管理インターフェイスに静的 IP アドレスを設定する必要がある場合は、「CLI を使用した事前設定 （66 ページ）」を参照してください。デフォルトでは、管理インターフェイスは DHCP を使用します。

管理インターフェイスからアクセスできるサーバーから新しいイメージをダウンロードする必要があります。

b) FXOS のトラブルシューティング ガイドに記載されている再イメージ化の手順を実行します。

Device Manager を使用した事前設定

Device Manager に接続して、Threat Defense の初期設定を実行します。Device Manager を使用して初期セットアップを実行すると、管理インターフェイスおよびマネージャアクセス設定に加えて、管理のために Management Center に切り替えたときに、Device Manager で完了したすべてのインターフェイス構成が保持されます。アクセス コントロール ポリシーやセキュリティ ゾーンなどの他のデフォルト設定は保持されないことに注意してください。CLI を使用すると、管理インターフェイスとマネージャアクセス設定のみが保持されます（たとえば、デフォルトの内部インターフェイス構成は保持されません）。

始める前に

- Management Center の初期設定を展開して実行します。Cisco Firepower Management Center 1600, 2600, and 4600 Hardware Installation Guideを参照してください。Threat Defense をセットアップする前に、Management Center の IP アドレスまたはホスト名を把握しておく必要があります。
- Firefox、Chrome、Safari、Edge、または Internet Explorer の最新バージョンを使用します。

手順

ステップ 1 管理コンピュータを内部（Ethernet1/2 ～ 1/8）インターフェイスに接続します

ステップ 2 ファイアウォールの電源を入れます。

（注） Threat Defense を初めて起動するときは、初期化に約 15 ～ 30 分かかります。

ステップ 3 Device Manager にログインします。

a) ブラウザに URL（**https://192.168.95.1**）を入力します。

b) ユーザー名 **admin**、デフォルト パスワード **Admin123** を使用してログインします。

c) エンド ユーザー ライセンス契約書を読んで同意し、管理者パスワードを変更するように求められます。

ステップ 4 初期設定を完了するには、最初に Device Manager にログインしたときにセットアップウィザードを使用します。必要に応じて、ページの下部にある [デバイスの設定をスキップ（Skip device setup）] をクリックしてセットアップウィザードをスキップできます。

セットアップウィザードを完了すると、内部インターフェイス（Ethernet1/2 ～ 1/8（VLAN1 のスイッチポート））のデフォルト設定に加えて、Management Center の管理に切り替えるときに維持される外部（Ethernet1/1）インターフェイスも設定できます。

a) 外部インターフェイスおよび管理インターフェイスに対して次のオプションを設定し、[次へ（Next）] をクリックします。

1. [外部インターフェイスアドレス（Outside Interface Address）]— このインターフェイスは通常インターネット ゲートウェイであり、マネージャ アクセス インターフェイスとして使用される場合があります。デバイスの初期設定時に別の外部インターフェイスを選択することはできません。最初のデータ インターフェイスがデフォルトの外部インターフェイスです。

マネージャアクセスに外部（または内部）とは異なるインターフェイスを使用する場合は、セットアップウィザードの完了後に手動で設定する必要があります。

[IPv4の設定（Configure IPv4）]：外部インターフェイス用の IPv4 アドレスです。DHCP を使用するか、または手動でスタティック IP アドレス、サブネットマスク、およびゲートウェイを入力できます。[オフ（Off）] を選択して、IPv4 アドレスを設定しないという選択肢もあります。セットアップウィザードを使用して PPPoE を設定することはできません。インターフェイスが DSL モデム、ケーブルモデム、または ISP への他の接続に接続されており、ISP が PPPoE を使用して IP アドレスを提供している場合は、PPPoE が必要になる場合があります。ウィザードの完了後に PPPoE を設定できます。

[IPv6の設定（Configure IPv6）]：外部インターフェイス用の IPv6 アドレスです。DHCP を使用するか、または手動でスタティック IP アドレス、プレフィックス、およびゲートウェイを入力できます。[オフ（Off）] を選択して、IPv6 アドレスを設定しないという選択肢もあります。

2. [管理インターフェイス（Management Interface）]

CLI で初期設定を実行した場合、管理インターフェイスの設定は表示されません。

データインターフェイスでマネージャアクセスを有効にした場合でも、管理インターフェイスの設定が使用されます。たとえば、データインターフェイスを介してバックプレーン経由でルーティングされる管理トラフィックは、データインターフェイス DNS サーバーではなく、管理インターフェイス DNS サーバーを使用して FQDN を解決します。

[DNSサーバ（DNS Servers）]：システムの管理アドレス用の DNS サーバ。名前解決用に 1 つ以上の DNS サーバのアドレスを入力します。デフォルトは OpenDNS パブリック DNS サーバです。フィールドを編集し、デフォルトに戻したい場合は、[OpenDNS

を使用（Use OpenDNS）] をクリックすると、フィールドに適切な IP アドレスがリロードされます。

[ファイアウォールホスト名（Firewall Hostname）]：システムの管理アドレスのホスト名です。

b) [時刻設定（NTP）（Time Setting (NTP)）] を設定し、[次へ（Next）] をクリックします。

1. [タイムゾーン（Time Zone）]：システムのタイムゾーンを選択します。
2. [NTPタイムサーバ（NTP Time Server）]：デフォルトの NTP サーバを使用するか、使用している NTP サーバのアドレスを手動で入力するかを選択します。バックアップ用に複数のサーバを追加できます。

c) [登録せずに 90 日間の評価期間を開始（Start 90 day evaluation period without registration）] を選択します。

Threat Defense を Smart Software Manager に登録しないでください。すべてのライセンスは Management Center で実行されます。

d) [終了（Finish）] をクリックします。

e) [クラウド管理（Cloud Management）]または [スタンドアロン（Standalone）] を選択するよう求められます。Management Center の管理については、[スタンドアロン（Standalone）] を選択してから、[Got It（了解）] を選択します。

ステップ 5 （必要に応じて）管理インターフェイスを設定します。[デバイス（Device）]>[インターフェイス（Interfaces）] の管理インターフェイスを参照してください。

管理インターフェイスには、データインターフェイスに設定されたゲートウェイが必要です。デフォルトでは、管理インターフェイスは DHCP から IP アドレスとゲートウェイを受信します。DHCP からゲートウェイを受信しない場合（たとえば、管理インターフェイスをネットワークに接続していない場合）、ゲートウェイはデフォルトでデータインターフェイスになり、何も設定する必要はありません。DHCP からゲートウェイを受信した場合は、代わりに管理インターフェイスに静的 IP アドレスを設定し、ゲートウェイをデータインターフェイスに設定する必要があります。

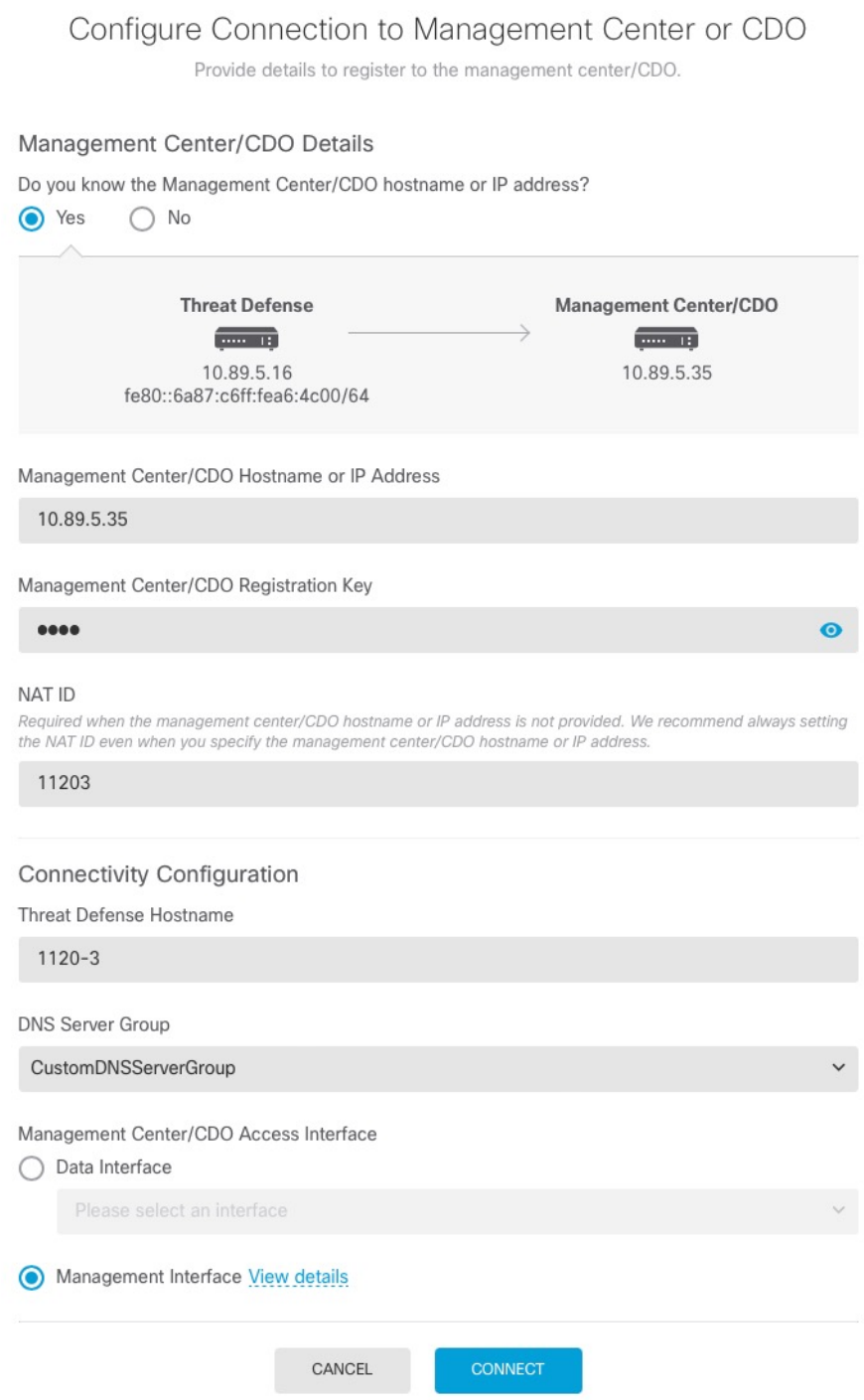
ステップ 6 マネージャアクセスに使用する外部または内部以外のインターフェイスを含む追加のインターフェイスを設定する場合は、[デバイス（Device）] を選択し、[インターフェイス（Interface）] のサマリーのリンクをクリックします。

Device Manager におけるインターフェイスの設定の詳細については、「Device Manager でのファイアウォールの設定（122 ページ）」を参照してください。Management Center にデバイスを登録すると、Device Manager の他の設定は保持されません。

ステップ 7 [デバイス（Device）] [システム設定（Device System Settings）] [中央管理（Central Management）] [Management Center] [Management Center] [デバイス（Device）] [システム設定（System Settings）] [中央管理（Central Management）] [Management Center] の順に選択し、[続行（Proceed）] をクリックして Management Center の管理を設定します。

ステップ 8 **[Management Center/CDOの詳細（Management Center/CDO Details）]** を設定します。

図 *16 : Management Center/CDO* の詳細



a) **[Management Center/CDOのホスト名またはIPアドレスを知っていますか（Do you know the FMC hostname or IP address）]** で、IP アドレスまたはホスト名を使用して Management Center に到達できる場合は [はい（Yes）] をクリックし、Management Center が NAT の背

後にあるか、パブリック IP アドレスまたはホスト名がない場合は[いいえ（No）] をクリックします。

双方向の SSL 暗号化通信チャネルを 2 台のデバイス間に確立するには、少なくても 1 台以上のデバイス（Management Center または Threat Defense デバイス）に到達可能な IP アドレスが必要です。

b) [はい（Yes）] を選択した場合は、**管理センター/CDO のホスト名/IP アドレス**を入力します。

c) **Management Center/CDO 登録キー**を指定します。

このキーは、Threat Defense デバイスを登録するときに Management Center でも指定する任意の 1 回限りの登録キーです。登録キーは 37 文字以下にする必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、Management Center に登録する複数のデバイスに使用できます。

d) [NAT ID] を指定します。

この ID は、Management Center でも指定する任意の 1 回限りの文字列です。いずれかのデバイスの IP アドレスのみを指定する場合、このフィールドは必須です。両方のデバイスの IP アドレスがわかっている場合でも、NAT ID を指定することを推奨します。NAT ID は 37 文字以下にする必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、Management Center に登録する他のデバイスには使用できません。NAT ID は、正しいデバイスからの接続であることを確認するために IP アドレスと組み合わせて使用されます。 IP アドレス/NAT ID の認証後にのみ、登録キーがチェックされます。

ステップ 9 [接続の設定（Connectivity Configuration）] を設定します。

a) [FTDホスト名（FTD Hostname）] を指定します。

この FQDN は、外部インターフェイス、または **Management Center/CDO アクセスインターフェイス**用に選択したインターフェイスに使用されます。

b) [DNSサーバーグループ（DNS Server Group）] を指定します。

既存のグループを選択するか、新しいグループを作成します。デフォルトの DNS グループは **CiscoUmbrellaDNSServerGroup** と呼ばれ、OpenDNS サーバーが含まれます。

この設定により、データインターフェイス DNS サーバーが設定されます。セットアップウィザードで設定した管理 DNS サーバーは、管理トラフィックに使用されます。データ DNS サーバーは、DDNS（設定されている場合）またはこのインターフェイスに適用されるセキュリティポリシーに使用されます。管理トラフィックとデータトラフィックの両方が外部インターフェイス経由で DNS サーバーに到達するため、管理に使用したものと同じ DNS サーバーグループを選択する可能性があります。

Management Center では、この Threat Defense に割り当てるプラットフォーム設定ポリシーでデータインターフェイス DNS サーバーが設定されます。Management Center に Threat Defense を追加すると、ローカル設定が維持され、DNS サーバーはプラットフォーム設定ポリシーに追加されません。ただし、DNS 設定を含む Threat Defense に後でプラットフォーム設定ポリシーを割り当てると、その設定によってローカル設定が上書きされます。

Management Center と Threat Defense を同期させるには、この設定に一致するように DNS プラットフォーム設定をアクティブに設定することをお勧めします。

また、ローカル DNS サーバーは、DNS サーバーが初期登録で検出された場合にのみ Management Center で保持されます。

c) **Management Center/CDO アクセスインターフェイス**については、[外部（outside）] を選択します。

設定済みの任意のインターフェイスを選択できますが、このガイドでは外部を使用していることを前提としています。

ステップ 10 外部とは別のデータインターフェイスを選択した場合は、デフォルトルートを追加します。

インターフェイスを通過するデフォルトルートがあることを確認するように求めるメッセージが表示されます。外部を選択した場合は、セットアップウィザードの一環としてこのルートがすでに設定されています。別のインターフェイスを選択した場合は、Management Center に接続する前にデフォルトルートを手動で設定する必要があります。Device Manager におけるスタティックルートの設定の詳細については、「Device Manager でのファイアウォールの設定（122 ページ）」を参照してください。

ステップ 11 [ダイナミック DNS（DDNS）方式の追加（Add a Dynamic DNS (DDNS) method）] をクリックします。

DDNS は、Threat Defense の IP アドレスが変更された場合に Management Center が完全修飾ドメイン名（FQDN）で Threat Defense に到達できるようにします。[デバイス（Device）] > [システム設定（System Settings）] > [DDNSサービス（DDNS Service）] を参照して DDNS を設定します。

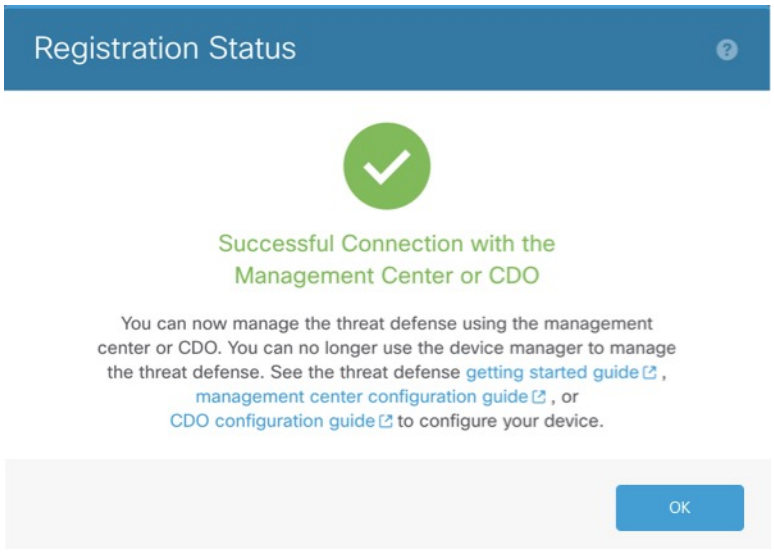
Threat Defense を Management Center に追加する前に DDNS を設定すると、Threat Defense は Cisco Trusted Root CA バンドルからすべての主要 CA の証明書を自動的に追加するため、Threat Defense は HTTPS 接続の DDNS サーバー証明書を検証できます。Threat Defense は、DynDNS リモート API 仕様（https://help.dyn.com/remote-access-api/）を使用するすべての DDNS サーバーをサポートします。

ステップ 12 [接続（Connect）] をクリックします。**[登録ステータス（Registration Status）]** ダイアログボックスには、Management Center への切り替えに関する現在のステータスが表示されます。**[Management Center/CDO登録設定の保存（Saving Management Center/CDO Registration Settings）]** のステップの後、Management Center に移動してファイアウォールを追加します。

Management Center への切り替えをキャンセルする場合は、[登録のキャンセル（Cancel Registration）] をクリックします。キャンセルしない場合は、**[Management Center/CDO登録設定の保存（Saving Management Center/CDO Registration Settings）]** のステップが完了するまで Device Manager のブラウザウィンドウを閉じないでください。閉じた場合、プロセスは一時停止し、Device Manager に再接続した場合のみ再開されます。

[Management Center/CDO登録設定の保存（Saving Management Center/CDO Registration Settings）] のステップの後に Device Manager に接続したままにする場合、その後 **[Management CenterまたはCDOとの正常接続（Successful Connection with Management Center or CDO）]** ダイアログボックスが表示され、Device Manager から切断されます。

図 *17* : 正常接続



CLI を使用した事前設定

Threat Defense CLI に接続して初期設定を行います。初期設定で CLI を使用すると、管理インターフェイスとマネージャ アクセス インターフェイスの設定のみが保持されます。（7.1 以降）Device Manager を使用して初期セットアップを実行すると、管理のために Management Center に切り替えたときに、管理インターフェイスおよびマネージャ アクセス インターフェイスの設定に加えて、Device Manager で完了したすべてのインターフェイス設定が保持されます。アクセス コントロール ポリシーなどの他のデフォルト設定は保持されないことに注意してください。

始める前に

Management Center の初期設定を展開して実行します。Cisco Firepower Management Center 1600, 2600, and 4600 Hardware Installation Guideを参照してください。Threat Defense をセットアップする前に、Management Center の IP アドレスまたはホスト名を把握しておく必要があります。

手順

ステップ 1 ファイアウォールの電源を入れます。

（注） Threat Defense を初めて起動するときは、初期化に約 15 ～ 30 分かかります。

ステップ 2 コンソールポートで Threat Defense CLI に接続します。

コンソールポートは FXOS CLI に接続します。

ステップ 3 ユーザー名 **admin** およびパスワード **Admin123** でログインします。

初めてFXOSにログインしたときは、パスワードを変更するよう求められます。このパスワードは、SSH の Threat Defense ログインにも使用されます。

（注） パスワードがすでに変更されていてわからない場合は、デバイスを再イメージ化してパスワードをデフォルトにリセットする必要があります。再イメージ化の手順については、FXOS のトラブルシューティング ガイドを参照してください。

例：

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

ステップ 4 Threat Defense CLI に接続します。

connect ftd

例：

```
firepower# connect ftd
>
```

ステップ 5 Threat Defense に初めてログインすると、エンドユーザーライセンス契約（EULA）に同意し、SSH接続を使用している場合は、管理者パスワードを変更するように求められます。その後、管理インターフェイスの設定用の CLI セットアップスクリプトが表示されます。

データインターフェイスでマネージャアクセスを有効にした場合でも、管理インターフェイスの設定が使用されます。

（注） 設定をクリア（たとえば、イメージを再作成することにより）しないかぎり、CLI セットアップウィザードを繰り返すことはできません。ただし、これらの設定すべては、後から CLI で **configure network** コマンドを使用して変更できます。Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。

デフォルト値または以前に入力した値がカッコ内に表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

次のガイドラインを参照してください。

- [DHCP経由または手動でIPv4を設定しますか？（Configure IPv4 via DHCP or manually?）]：[手動（manual）] を選択します。管理インターフェイスを使用する予定がない場合でも、

プライベートアドレスなどの IP アドレスを設定する必要があります。管理インターフェイスが DHCP に設定されている場合、管理用のデータインターフェイスを設定することはできません。これは、**data-interfaces** である必要があるデフォルトルートが DHCP サーバーから受信したルートで上書きされる可能性があるためです。

- [管理インターフェイスのIPv4デフォルトゲートウェイを入力（Enter the IPv4 default gateway for the management interface）]：ゲートウェイを [data-interfaces] に設定します。この設定は、マネージャ アクセス データ インターフェイスを通じて回送できるように、バックプレーンを介して管理トラフィックを転送します。
- [ネットワーク情報が変更された場合は再接続が必要（If your networking information has changed, you will need to reconnect）]：SSH で接続している場合は、接続が切断されます。管理コンピュータが管理ネットワーク上にある場合は、新しい IP アドレスとパスワードで再接続できます。（データインターフェイス経由で）デフォルトルートが変更されたため、リモートネットワークからはまだ再接続できません。コンソール接続は影響を受けません。
- [デバイスをローカルで管理しますか（Manage the device locally?）]：Management Center を使用するには「**no**」を入力します。**yes** と入力すると、代わりに Device Manager を使用することになります。
- [ファイアウォールモードを設定しますか？（Configure firewall mode?）]：**routed** と入力します。外部マネージャアクセスは、ルーテッド ファイアウォール モードでのみサポートされています。

例：

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password: ********
Confirm new password: ********
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]:
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...
```

```
Update policy deployment information
    - add device configuration
    - add network discovery
    - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

ステップ 6 マネージャアクセス用の外部インターフェイスを設定します。

configure network management-data-interface

その後、外部インターフェイスの基本的なネットワーク設定を行うように求めるプロンプトが表示されます。このコマンドの使用については、次の詳細を参照してください。

- データインターフェイスを管理に使用する場合、管理インターフェイスではDHCPを使用できません。初期セットアップ時にIPアドレスを手動で設定しなかった場合は、**configure network {ipv4 | ipv6} manual** コマンドを使用して設定できるようになりました。管理インターフェイス ゲートウェイを **data-interfaces** に設定しなかった場合は、ここでこのコマンドで設定します。

- Threat Defense を Management Center に追加すると、Management Center はインターフェイス設定（インターフェイス名と IP アドレス、ゲートウェイへの静的ルート、DNS サーバー、DDNS サーバーなど）を検出して維持します。DNS サーバー設定の詳細については、次を参照してください。Management Center では、後でマネージャ アクセス インターフェイス構成を変更できますが、Threat Defense または Management Center が管理接続の再確立を妨げるような変更は加えないでください。管理接続が中断された場合、Threat Defense には以前の展開を復元する **configure policy rollback** コマンドが含まれます。

- DDNS サーバー更新の URL を設定すると、Threat Defense は Cisco Trusted Root CA バンドルからすべての主要 CA の証明書を自動的に追加するため、Threat Defense は HTTPS 接続の DDNS サーバー証明書を検証できます。Threat Defense は、DynDNS リモート API 仕様（https://help.dyn.com/remote-access-api/）を使用するすべての DDNS サーバーをサポートします。

- このコマンドは、「データ」インターフェイス DNS サーバーを設定します。セットアップスクリプトで（または **configure network dns servers** コマンドを使用して）設定した管

理 DNS サーバーは、管理トラフィックに使用されます。データ DNS サーバーは、DDNS（設定されている場合）またはこのインターフェイスに適用されるセキュリティポリシーに使用されます。

Management Center では、この Threat Defense に割り当てるプラットフォーム設定ポリシーでデータインターフェイス DNS サーバーが設定されます。Management Center に Threat Defense を追加すると、ローカル設定が維持され、DNS サーバーはプラットフォーム設定ポリシーに追加されません。ただし、DNS 設定を含む Threat Defense に後でプラットフォーム設定ポリシーを割り当てると、その設定によってローカル設定が上書きされます。Management Center と Threat Defense を同期させるには、この設定に一致するように DNS プラットフォーム設定をアクティブに設定することをお勧めします。

また、ローカル DNS サーバーは、DNS サーバーが初期登録で検出された場合にのみ Management Center で保持されます。たとえば、管理インターフェイスを使用してデバイスを登録し、後で **configure network management-data-interface** コマンドを使用してデータインターフェイスを設定した場合、Threat Defense 設定と一致するように、DNS サーバーを含むこれらの設定のすべてを Management Center で手動で設定する必要があります。

- 管理インターフェイスは、Threat Defense を Management Center に登録した後に、管理インターフェイスまたは別のデータインターフェイスのいずれかに変更できます。
- セットアップウィザードで設定した FQDN がこのインターフェイスに使用されます。
- コマンドの一部としてデバイス設定全体をクリアできます。このオプションはリカバリシナリオで使用できますが、初期セットアップや通常の操作には使用しないでください。
- データ管理を無効にするには、**configure network management-data-interface disable** コマンドを入力します。

例：

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://deanwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
 change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

例：

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
```

```
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
 change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

ステップ 7 （任意） 特定のネットワーク上の Management Center へのデータ インターフェイス アクセスを制限します。

configure network management-data-interface client *ip_address netmask*

デフォルトでは、すべてのネットワークが許可されます。

ステップ 8 この Threat Defense を管理する Management Center を特定します。

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**}—Specifies either the FQDN or IP address of the Management Center.Management Center を直接アドレス指定できない場合は、**DONTRESOLVE** を使用します。双方向の SSL 暗号化通信チャネルを 2 台のデバイス間に確立するには、少なくても 1 台以上のデバイス（Management Center または Threat Defense ）に到達可能な IP アドレスが必要です。このコマンドで **DONTRESOLVE** を指定するには、到達可能な IP アドレスまたはホスト名が Threat Defense に必要です。
- reg_key：Threat Defense を登録するときに Management Center でも指定する任意のワンタイム登録キーを指定します。登録キーは 37 文字以下にする必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。
- nat_id：Management Center でも指定する、任意で一意の 1 回限りの文字列を指定します。管理にデータインターフェイスを使用する場合は、登録用に Threat Defense と Management Center の両方で NAT ID を指定する必要があります。NAT ID は 37 文字以下にする必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、Management Center に登録する他のデバイスには使用できません。

例：

```
> configure manager add fmc-1.example.com regk3y78 natid56
Manager successfully configured.
```

ステップ 9 デバイスをリモート支社に送信できるように Threat Defense をシャットダウンします。

システムを適切にシャットダウンすることが重要です。単純に電源プラグを抜いたり、電源スイッチを押したりすると、重大なファイルシステムの損傷を引き起こすことがあります。バックグラウンドでは常に多数のプロセスが実行されており、電源プラグを抜いたり、電源を切断したりすると、システムをグレースフルシャットダウンできないことを覚えておいてください。

a) **shutdown** コマンドを入力します。
b) 電源 LED とステータス LED を観察して、シャーシの電源が切断されていることを確認します（LED が消灯）。
c) シャーシの電源が正常に切断されたら、必要に応じて電源プラグを抜き、シャーシから物理的に電源を取り外すことができます。

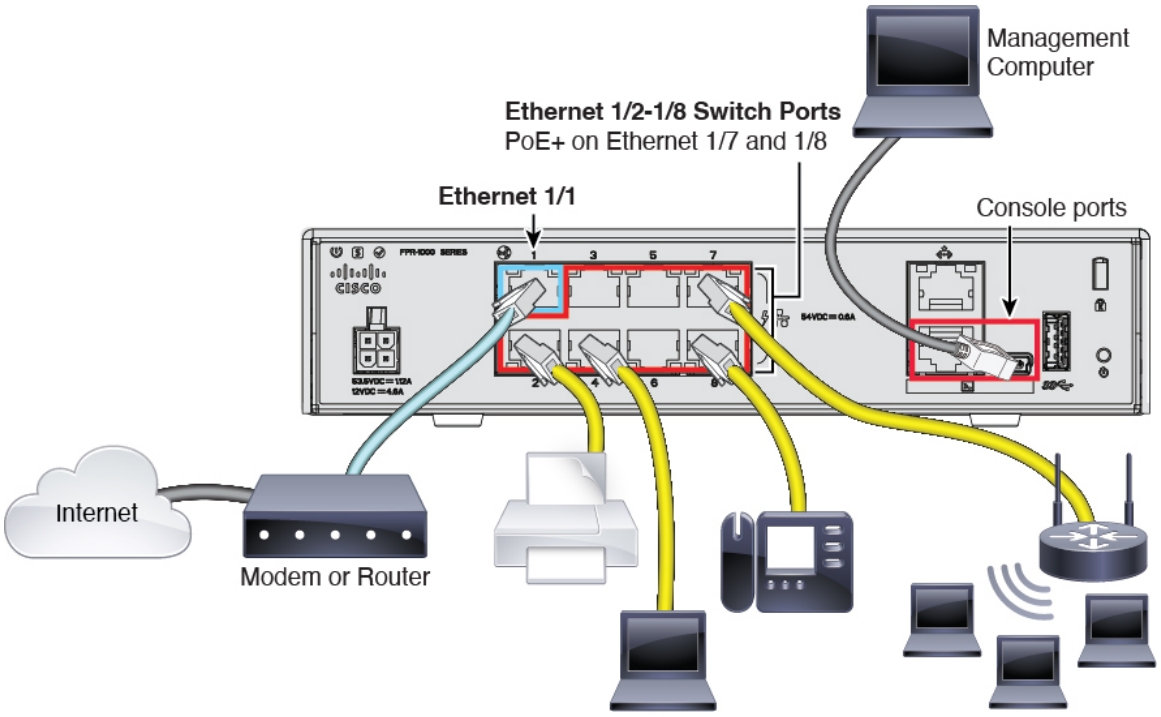
支社へのインストール

中央の本社から Threat Defense を受け取ったら、外部インターフェイスからインターネットにアクセスできるように、ファイアウォールにケーブルを接続して電源をオンにするだけです。そうすると、中央の管理者は設定を完了できます。

ファイアウォールのケーブル接続

Management Center と管理コンピュータはリモートの本社にあり、Threat Defense にはインターネット経由で到達できます。Firepower 1010 でケーブル接続を行うには、次の手順を参照してください。

図 *18 :* リモート管理展開のケーブル接続



（注） PoE は Firepower 1010E ではサポートされていません。

手順

ステップ 1 シャーシを取り付けます。ハードウェア設置ガイドを参照してください。

ステップ 2 外部インターフェイス（Ethernet 1/1）を外部ルータに接続します。

ステップ 3 内部エンドポイントをスイッチポート Ethernet1/2 ー 1/8 にケーブルで接続します。

ステップ 4 （任意） 管理コンピュータをコンソールポートに接続します。

支社では、日常的に使用するためのコンソール接続は必要ありません。ただし、トラブルシューティングに必要な場合があります。

デバイスの電源投入

システムの電源は電源コードで制御されます。電源ボタンはありません。

（注） Threat Defense を初めて起動するときは、初期化に約 15 ～ 30 分かかります。

始める前に

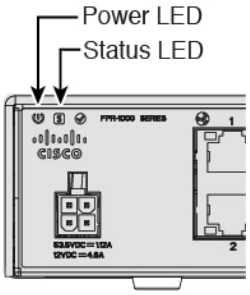
デバイスに対して信頼性の高い電力を供給することが重要です（たとえば、無停電電源装置（UPS）を使用）。最初のシャットダウンを行わないで電力が失われると、重大なファイルシステムの損傷を引き起こす可能性があります。バックグラウンドでは常に多数のプロセスが実行されていて、電力が失われると、システムをグレースフルシャットダウンできません。

手順

ステップ 1 電源コードをデバイスに接続し、電源コンセントに接続します。

電源コードを差し込むと電源が自動的に入ります。

ステップ 2 デバイスの背面または上部にある電源 LED を確認します。緑色に点灯している場合は、デバイスの電源が入っています。



ステップ 3 デバイスの背面または上部にあるステータス LED を確認します。緑色に点灯している場合は、電源投入時診断に合格しています。

中央の管理者による事後設定

外部インターフェイスからインターネットにアクセスできるようにリモート支社の管理者が Threat Defense をケーブル接続すると、Threat Defense を Management Center に登録してデバイスの設定を完了できます。

へのログインManagement Center

Management Center を使用して、Threat Defense を設定および監視します。

始める前に

サポートされているブラウザの詳細については、使用するバージョンのリリースノート（https://www.cisco.com/go/firepower-notes）を参照してください。

手順

ステップ 1 サポートされているブラウザを使用して、次の URL を入力します。

https://*fmc_ip_address*

ステップ 2 ユーザー名とパスワードを入力します。

ステップ 3 [ログイン（Log In）] をクリックします。

Management Center のライセンスの取得

すべてのライセンスは、Management Center によって Threat Defense に提供されます。オプションで、次の機能ライセンスを購入できます。

- **IPS**：セキュリティインテリジェンスと次世代 IPS

- **マルウェア防御**：マルウェア防御
- **URL**：URL フィルタリング
- **Cisco Secure Client**：Secure Client Advantage、Secure Client Premier、または Secure Client VPN のみ
- キャリア（Diameter、GTP/GPRS、M3UA、SCTP）

シスコライセンスの概要については詳しくは、cisco.com/go/licensingguide を参照してください。

始める前に

- Smart Software Manager にマスターアカウントを持ちます。

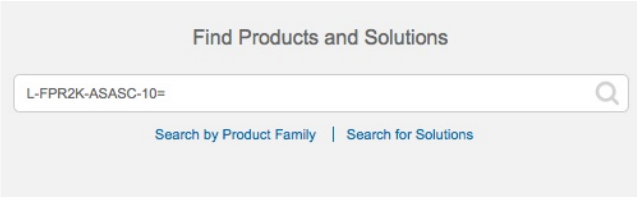
  まだアカウントをお持ちでない場合は、リンクをクリックして新しいアカウントを設定してください。Smart Software Manager では、組織のマスター アカウントを作成できます。
- （輸出コンプライアンスフラグを使用して有効化される）機能を使用するには、ご使用のスマート ソフトウェア ライセンシング アカウントで強力な暗号化（3DES/AES）ライセンスを使用できる必要があります。

手順

ステップ 1 お使いのスマート ライセンシング アカウントに、必要なライセンスが含まれていることを確認してください。

ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマート ソフトウェア ライセンシング アカウントにリンクされています。ただし、主導でライセンスを追加する必要がある場合は、Cisco Commerce Workspace で [製品とソリューションの検索（Find Products and Solutions）] 検索フィールドを使用します。次のライセンス PID を検索します。

図 *19*：ライセンス検索



（注） PID が見つからない場合は、注文に手動で PID を追加できます。

- IPS、マルウェア防御、および URL ライセンスの組み合わせ：
  - L-FPR1010T-TMC=

  上記の PID のいずれかを注文に追加すると、次のいずれかの PID に対応する期間ベースのサブスクリプションを選択できます。

- L-FPR1010T-TMC-1Y
- L-FPR1010T-TMC-3Y
- L-FPR1010T-TMC-5Y

- Cisco Secure Client：『Cisco Secure Client 発注ガイド』を参照してください。
- キャリアライセンス：
  -

ステップ 2 まだの場合は、Smart Software Manager に Management Center を登録します。

登録を行うには、Smart Software Manager で登録トークンを生成する必要があります。詳細については、『Management Center コンフィグレーション ガイド』を参照してください。ロータッチプロビジョニングの場合は、Smart Software Manager に登録するとき、または登録した後に、**ロータッチプロビジョニングのクラウドアシスタンス**を有効にする必要があります。[システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）] ページを参照してください。

Management Center への Threat Defense の登録

Threat Defense を Management Center に登録します。

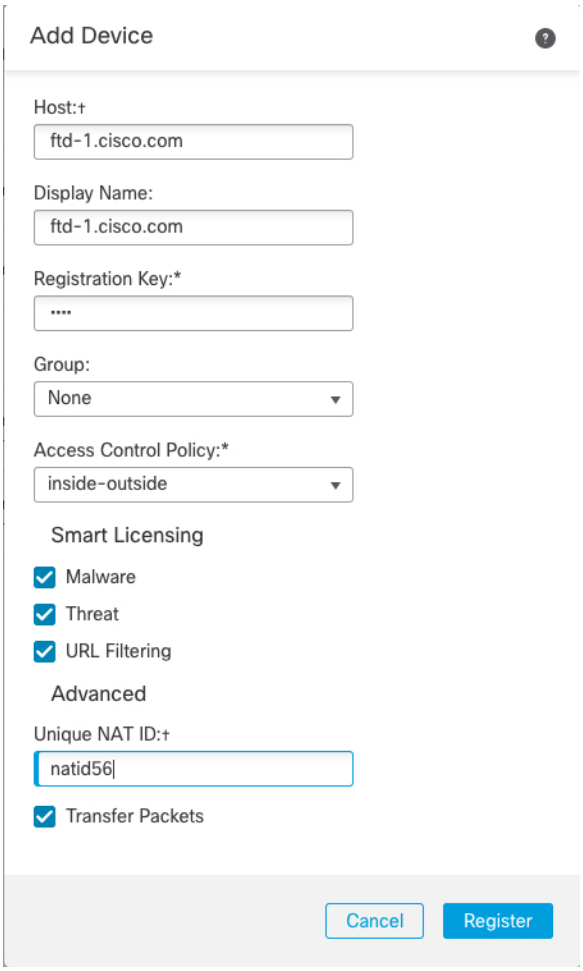
始める前に

- Threat Defense の初期設定で設定した次の情報を収集します。
  - Threat Defense の管理 IP アドレスまたはホスト名、および NAT ID
  - Management Center の登録キー

手順

ステップ 1 Management Center で、[デバイス（Devices）] > [デバイス管理（Device Management）] の順に選択します。

ステップ 2 [追加（Add）] ドロップダウン リストから、[デバイスの追加（Add Device）] を選択します。



次のパラメータを設定します。

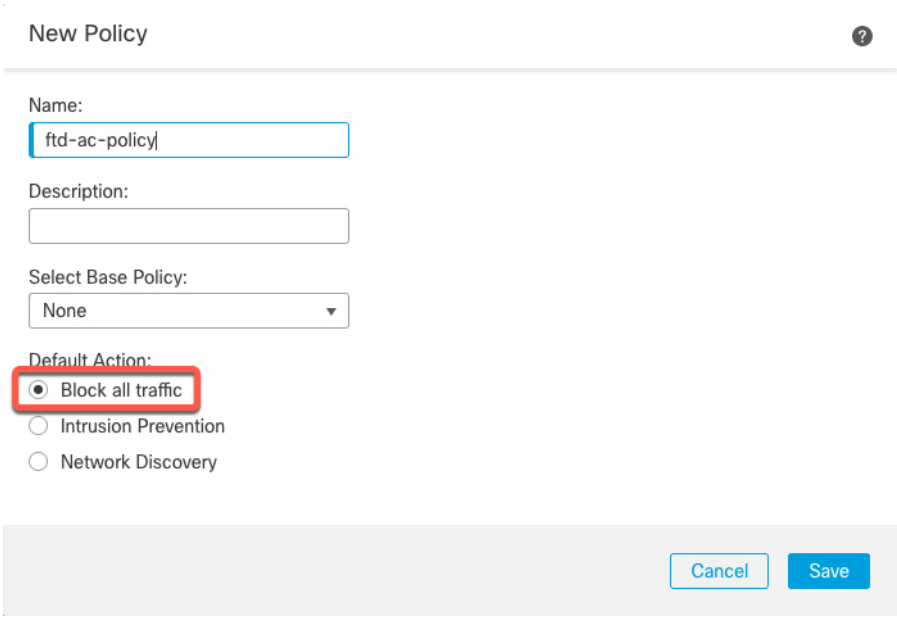
- [ホスト（Host）]：追加する Threat Defense の IP アドレスかホスト名を入力します。Threat Defense の最初の設定で Management Center の IP アドレスと NAT ID の両方を指定した場合は、このフィールドを空のままにしておくことができます。

  （注） HA 環境では、両方の Management Center が NAT の背後にある場合、プライマリ Management Center のホスト IP または名前なしで Threat Defense を登録できます。ただし、Threat Defense をセカンダリ Management Center に登録するには、Threat Defense の IP アドレスかホスト名を指定する必要があります。

- [表示名（Display Name）] フィールドに、Management Center に表示する Threat Defense の名前を入力します。
- [登録キー（Registration key）]：Threat Defense の最初の設定で指定したものと同じ登録キーを入力します。
- [ドメイン（Domain）]：マルチドメイン環境を使用している場合は、デバイスをリーフドメインに割り当てます。

- [グループ（Group）]：グループを使用している場合は、デバイスグループに割り当てます。
- [アクセスコントロールポリシー（Access Control Policy）]：初期ポリシーを選択します。使用する必要があることがわかっているカスタマイズ済みのポリシーがすでにある場合を除いて、[新しいポリシーの作成（Create new policy）] を選択し、[すべてのトラフィックをブロック（Block all traffic）] を選択します。後でこれを変更してトラフィックを許可することができます。「内部から外部へのトラフィックの許可 （45 ページ）」を参照してください。

図 *20 : New Policy*



- [スマートライセンス（Smart Licensing）]：展開する機能に必要なスマートライセンスとして、[マルウェア（Malware）]（マルウェアインスペクションを使用する予定の場合）、[脅威（Threat）]（侵入防御を使用する予定の場合）、および [URL]（カテゴリベースの URL フィルタリングを実行する予定の場合）を割り当てます。**注**：デバイスを追加した後、**[システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）]** ページから セキュアクライアント リモートアクセス VPN のライセンスを適用できます。
- [一意のNAT ID（Unique NAT ID）]：Threat Defense の最初の設定で指定した NAT ID を指定します。
- [パケットの転送（Transfer Packets）]：デバイスから Management Center へのパケット転送を許可します。このオプションを有効にして IPS や Snort などのイベントがトリガーされた場合は、デバイスが検査用としてイベントメタデータ情報とパケットデータを Management Center に送信します。このオプションを無効にした場合は、イベント情報だけが Management Center に送信され、パケットデータは送信されません。

ステップ 3 [登録（Register）] をクリックし、登録が成功したことを確認します。

登録が成功すると、デバイスがリストに追加されます。失敗した場合は、エラーメッセージが表示されます。Threat Defense が登録に失敗した場合は、次の項目を確認してください。

- ping：Threat Defense CLI にアクセスし、次のコマンドを使用して Management Center の IP アドレスへの ping を実行します。

  ping system *ip_address*

  ping が成功しない場合は、**show network** コマンドを使用してネットワーク設定を確認します。Threat Defense 管理 IP アドレスを変更する必要がある場合は、**configure network management-data-interface** コマンドを使用します。

- 登録キー、NAT ID、および Management Center IP アドレス：両方のデバイスで同じ登録キーを使用していることを確認し、使用している場合は NAT ID を使用していることを確認します。**configure manager add** コマンドを使用して、Threat Defense で登録キーと NAT ID を設定することができます。

トラブルシューティングの詳細については、https://cisco.com/go/fmc-reg-error を参照してください。

基本的なセキュリティポリシーの設定

ここでは、次の設定を使用して基本的なセキュリティポリシーを設定する方法について説明します。

- 内部インターフェイスと外部インターフェイス：内部インターフェイスに静的 IP アドレスを割り当てます。マネージャアクセス設定の一環として外部インターフェイスの基本設定を設定しましたが、まだそのインターフェイスをセキュリティゾーンに割り当てる必要があります。
- DHCP サーバー：クライアントの内部インターフェイスで DHCP サーバーを使用します。
- NAT：外部インターフェイスでインターフェイス PAT を使用します。
- アクセスコントロール：内部から外部へのトラフィックを許可します。
- SSH：マネージャ アクセス インターフェイスで SSH を有効にします。

インターフェイスの設定

スイッチポートの VLAN1 インターフェイスを追加するか、スイッチポートをファイアウォール インターフェイスに変換し、セキュリティゾーンにインターフェイスを割り当て、IP アドレスを設定します。通常は、システムで意味のあるトラフィックを通過させるように、少なくとも 2 つのインターフェイスを設定する必要があります。通常は、アップストリームルータまたはインターネットに面した外部インターフェイスと、組織のネットワークの 1 つ以上の内部インターフェイスを使用します。デフォルトでは、Ethernet1/1 は外部用に使用できる通常のファイアウォール インターフェイスであり、残りのインターフェイスは VLAN 1 のスイッチポートです。VLAN1 インターフェイスを追加すると、これを内部インターフェイスにするこ

とができます。または、スイッチポートを他のVLANに割り当てるか、スイッチポートをファイアウォール インターフェイスに変換することもできます。

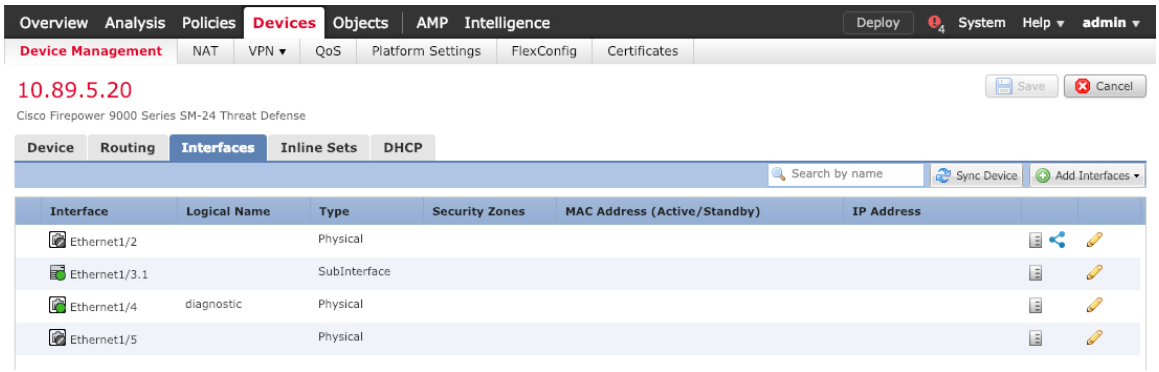
一般的なエッジルーティングの状況は、内部インターフェイスでスタティックアドレスを定義すると同時に、ISP から DHCP を介して外部インターフェイスアドレスを取得することです。

次の例では、DHCPによるスタティックアドレスとルーテッドモードの外部インターフェイスを使用して（Ethernet1/1）、ルーテッドモードの内部インターフェイス（VLAN1）を設定します。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、デバイスをクリックします。

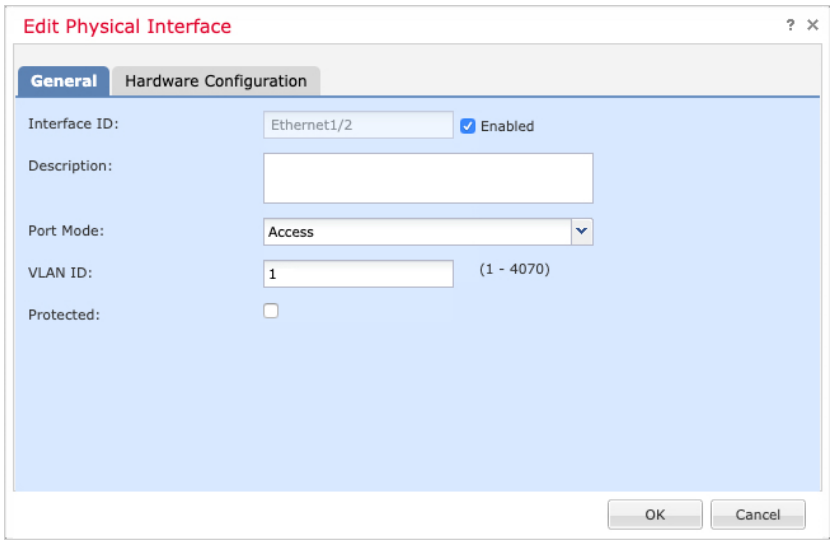
ステップ 2 [インターフェイス（Interfaces）] をクリックします。



ステップ 3 （任意） [スイッチポート（SwitchPort）] 列のスライダをクリックしてスイッチポート（Ethernet1/2 から 1/8）のいずれかのスイッチポートモードを無効にすると、無効（ ）と表示されます。

ステップ 4 スイッチポートを有効にします。

a) スイッチポートのをクリックします。



b) [有効（Enabled）] チェックボックスをオンにして、インターフェイスを有効化します。

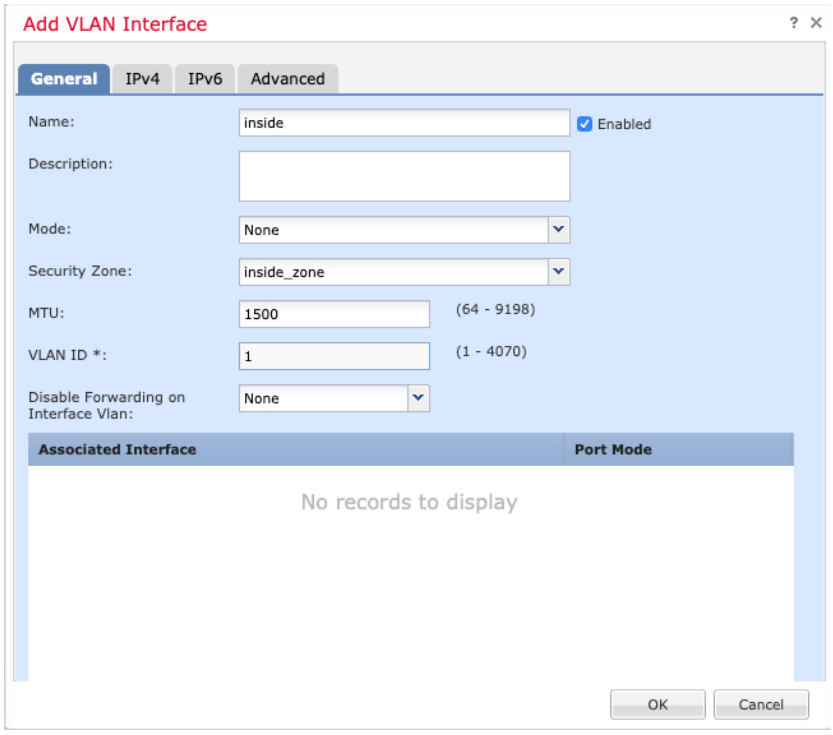
c) （任意） VLAN ID を変更します。デフォルトは 1 です。次に、この ID に一致する VLAN インターフェイスを追加します。

d) [OK] をクリックします。

ステップ 5 内部 VLAN インターフェイスを追加します。

a) **[インターフェイスの追加（Add Interfaces）]** > **[VLANインターフェイス（VLAN Interface）]** をクリックします。

[全般（General）] タブが表示されます。



b) 48 文字までの [名前（Name）] を入力します。

たとえば、インターフェイスに **inside** という名前を付けます。

c) [有効（Enabled）] チェックボックスをオンにします。

d) [モード（Mode）] は [なし（None）] に設定したままにします。

e) [セキュリティゾーン（Security Zone）] ドロップダウンリストから既存の内部セキュリティゾーンを選択するか、[新規（New）] 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。

たとえば、**inside_zone** という名前のゾーンを追加します。各インターフェイスは、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割り当てる必要があります。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も、複数のインターフェイスグループに属することもできます。ゾーンまたはグループに基づいてセキュリティポリシーを適用します。たとえば、内部インターフェイスを内部ゾーンに割り当て、外部インターフェイスを外部ゾーンに割り当てることができます。この場合、トラフィックが内部から外部に移動できるようにアクセス コントロール ポリシーを設定することはできますが、外部から内部に向けては設定できません。ほとんどのポリシーはセキュリティゾーンのみサポートしています。NAT ポリシー、プレフィルタ ポリシー、および QoS ポリシーで、ゾーンまたはインターフェイスグループを使用できます。

f) [VLAN ID] を **1** に設定します。

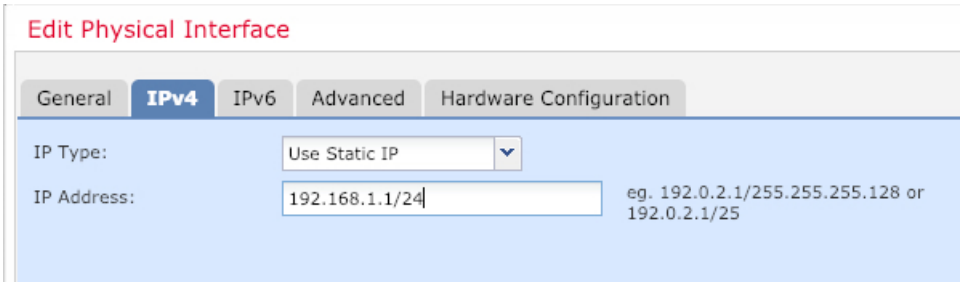
デフォルトでは、すべてのスイッチポートは VLAN 1 に設定されます。ここで別の VLAN ID を選択する場合は、新しい VLAN ID の各スイッチポートを編集する必要があります。

インターフェイスを保存した後、VLAN ID を変更することはできません。ここでの VLAN ID は、使用される VLAN タグと設定内のインターフェイス ID の両方です。

g) [IPv4] タブ、[IPv6] タブ、または両方のタブをクリックします。

- [IPv4]：ドロップダウンリストから [スタティック IP を使用する（Use Static IP）] を選択し、IP アドレスとサブネットマスクをスラッシュ表記で入力します。

  たとえば、**192.168.1.1/24** などと入力します。

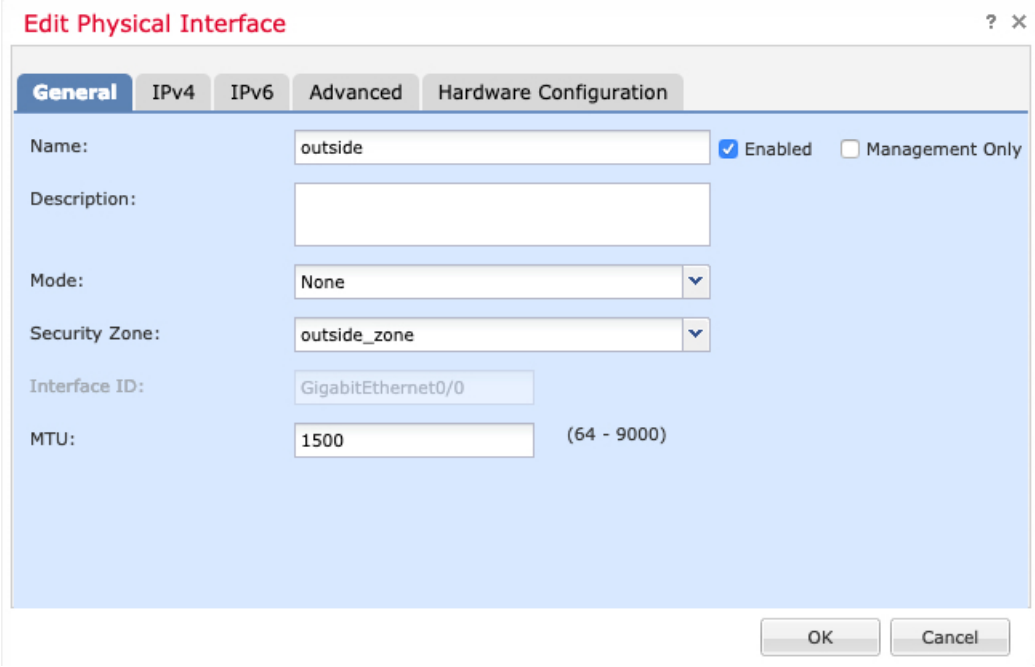


- [IPv6]：ステートレス自動設定の場合は [自動設定（Autoconfiguration）] チェックボックスをオンにします。

h) [OK] をクリックします。

ステップ 6 外部用に使用する Ethernet1/1 のをクリックします。

[全般（General）] タブが表示されます。



マネージャアクセス用にこのインターフェイスを事前に設定しているため、インターフェイスにはすでに名前が付けられており、有効化とアドレス指定が完了しています。これらの基本設定は変更しないでください。変更すると、Management Center の管理接続が中断されます。この画面でも、通過トラフィックポリシーのセキュリティゾーンを設定する必要があります。

a) [セキュリティゾーン（Security Zone）] ドロップダウンリストから既存の外部セキュリティゾーンを選択するか、[新規（New）] 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。

   たとえば、「outside_zone」という名前のゾーンを追加します。

b) [OK] をクリックします。

ステップ 7 [保存（Save）] をクリックします。

DHCP サーバーの設定

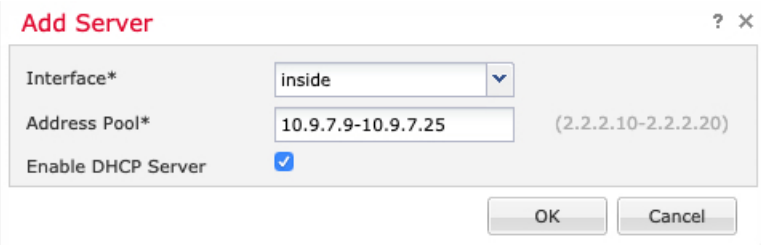
クライアントで DHCP を使用して Threat Defense から IP アドレスを取得するようにする場合は、DHCP サーバーを有効にします。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、デバイスをクリックします。

ステップ 2 **[DHCP]** > **[DHCPサーバー（DHCP Server）]** を選択します。

ステップ 3 **[サーバー（Server）]** ページで、**[追加（Add）]** をクリックして、次のオプションを設定します。



- [インターフェイス（Interface）]：ドロップダウンリストからインターフェイスを選択します。
- [アドレスプール（Address Pool）]：DHCP サーバーが使用する IP アドレスの最下位から最上位の間の範囲を設定します。IP アドレスの範囲は、選択したインターフェイスと同じサブネット上に存在する必要があり、インターフェイス自身の IP アドレスを含めることはできません。
- [DHCPサーバーを有効にする（Enable DHCP Server）]：選択したインターフェイスの DHCP サーバーを有効にします。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックします。

NAT の設定

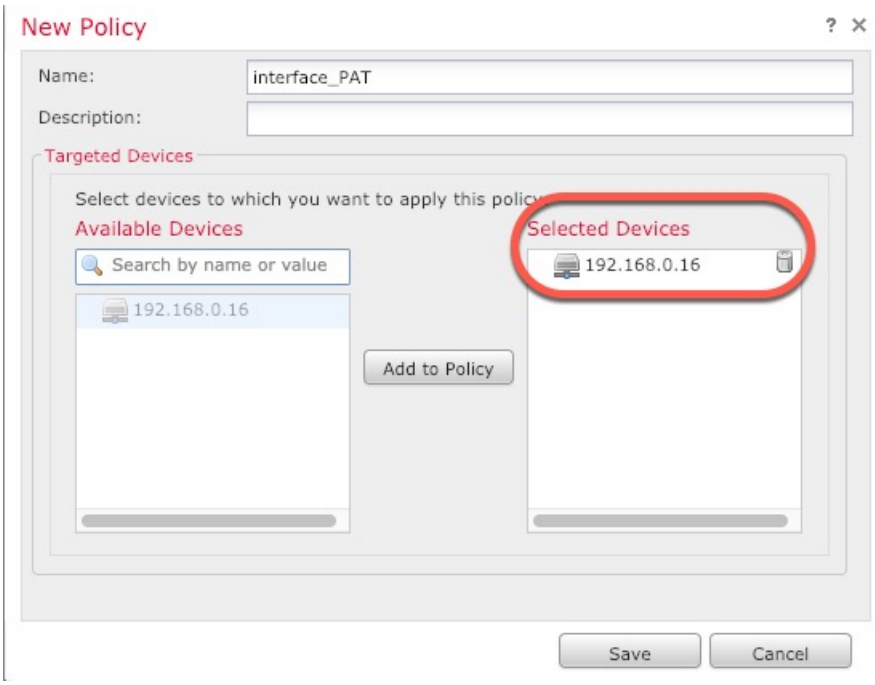
NAT の設定

一般的な NAT ルールでは、内部アドレスを外部インターフェイスの IP アドレスのポートに変換します。このタイプの NAT ルールのことをインターフェイス ポート アドレス変換（PAT）と呼びます。

手順

ステップ 1 **[デバイス（Devices）]** > **[NAT]** をクリックし、**[新しいポリシー（New Policy）]** > **[Threat Defense NAT]** をクリックします。

ステップ 2 ポリシーに名前を付け、ポリシーを使用するデバイスを選択し、[保存（Save）] をクリックします。



ポリシーが Management Center に追加されます。引き続き、ポリシーにルールを追加する必要があります。

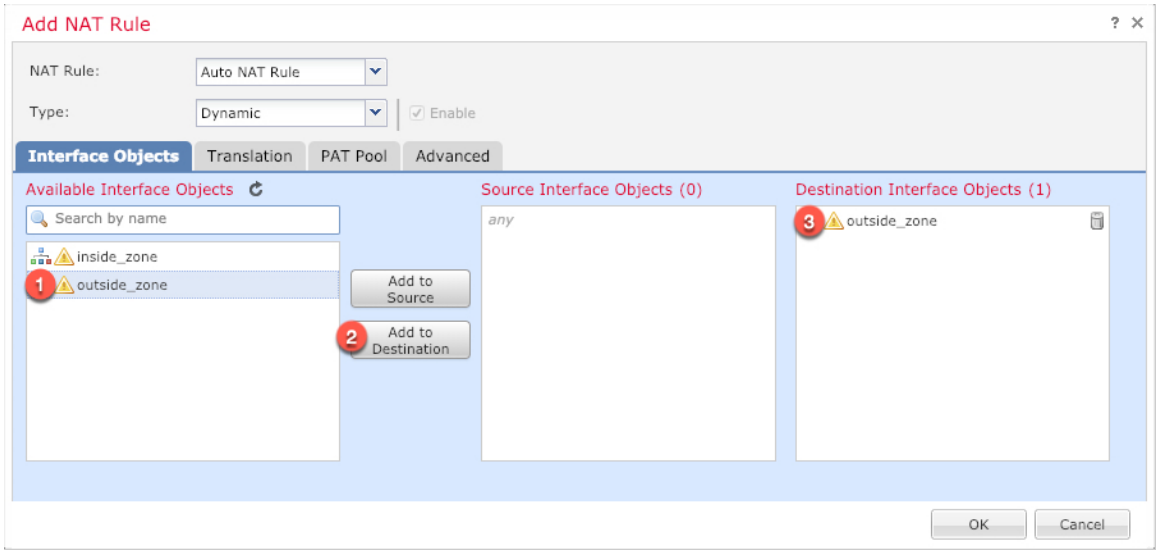
ステップ 3 [ルールの追加（Add Rule）] をクリックします。

[NATルールの追加（Add NAT Rule）] ダイアログボックスが表示されます。

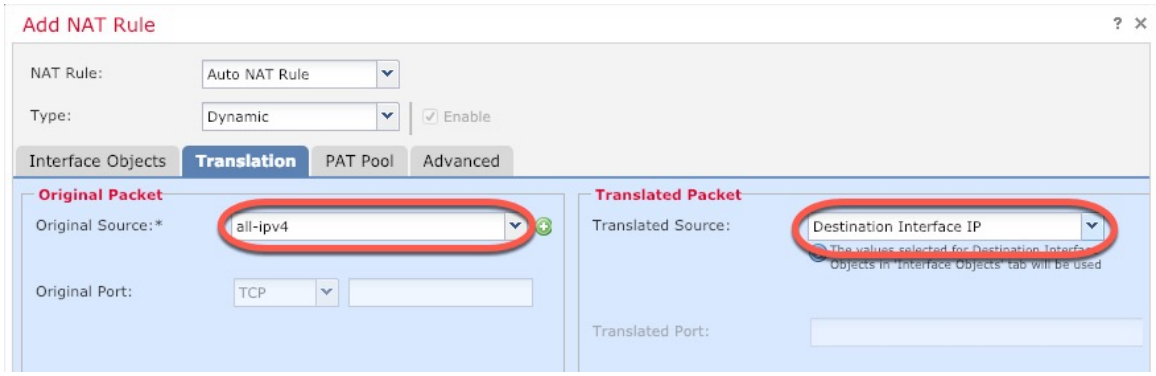
ステップ 4 基本ルールのオプションを設定します。

- [NATルール（NAT Rule）] : [自動NATルール（Auto NAT Rule）] を選択します。
- [タイプ（Type）] : [ダイナミック（Dynamic）] を選択します。

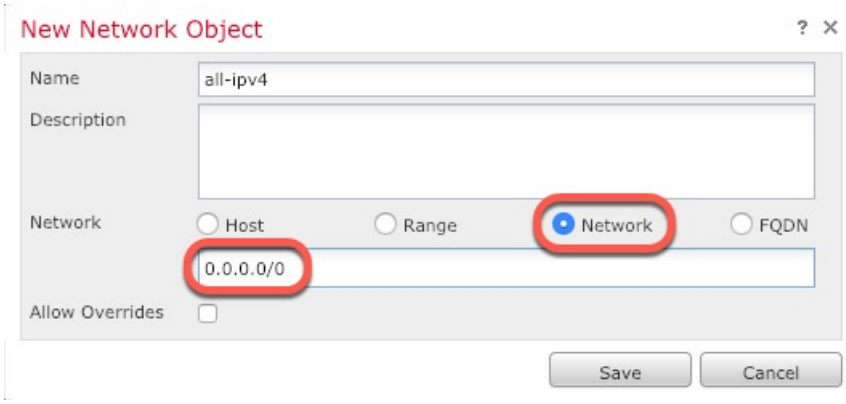
ステップ 5 [インターフェイスオブジェクト（Interface objects）] ページで、[使用可能なインターフェイスオブジェクト（Available Interface Objects）] 領域から [宛先インターフェイスオブジェクト（Destination Interface Objects）] 領域に外部ゾーンを追加します。



ステップ 6 [変換（Translation）] ページで、次のオプションを設定します。



- [元の送信元（Original Source）]：をクリックして、すべての IPv4 トラフィック（0.0.0.0/0）のネットワークオブジェクトを追加します。

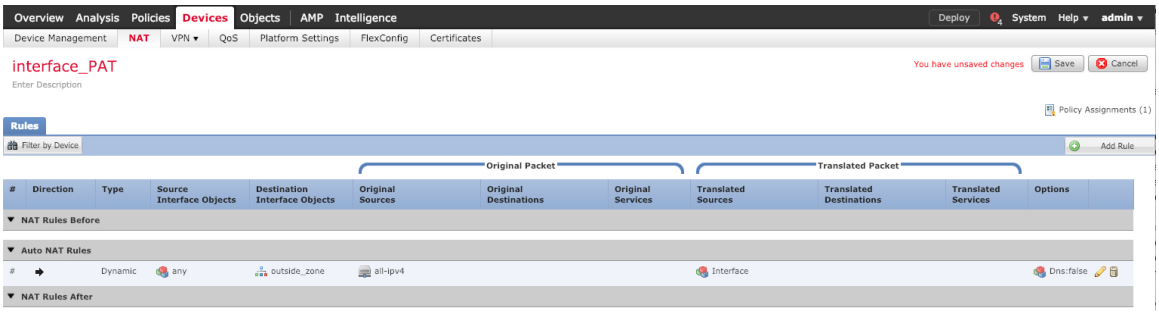


（注） 自動 NAT ルールはオブジェクト定義の一部として NAT を追加するため、システム定義の **any-ipv4** オブジェクトを使用することはできません。また、システム定義のオブジェクトを編集することはできません。

- [変換済みの送信元（Translated Source）]：[宛先インターフェイスIP（Destination Interface IP）] を選択します。

ステップ 7 [保存（Save）] をクリックしてルールを追加します。

ルールが [ルール（Rules）] テーブルに保存されます。



ステップ 8 NAT ページで [保存（Save）] をクリックして変更を保存します。

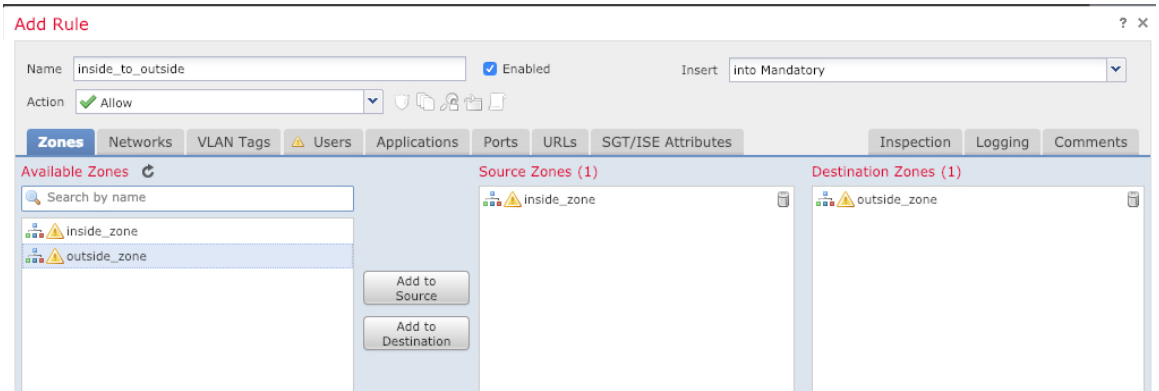
内部から外部へのトラフィックの許可

Threat Defense を登録したときに、基本の [すべてのトラフィックをブロック（Block all traffic）] アクセス コントロール ポリシーを作成した場合は、デバイスを通過するトラフィックを許可するためにポリシーにルールを追加する必要があります。次の手順では、内部ゾーンから外部ゾーンへのトラフィックを許可するルールを追加します。他にゾーンがある場合は、適切なネットワークへのトラフィックを許可するルールを追加してください。

手順

ステップ 1 **[ポリシー（Policy）] > [アクセスポリシー（Access Policy）] > [アクセスポリシー（Access Policy）]**を選択し、Threat Defense に割り当てられているアクセス コントロール ポリシーのをクリックします。

ステップ 2 **[ルールを追加（Add Rule）]** をクリックし、次のパラメータを設定します。

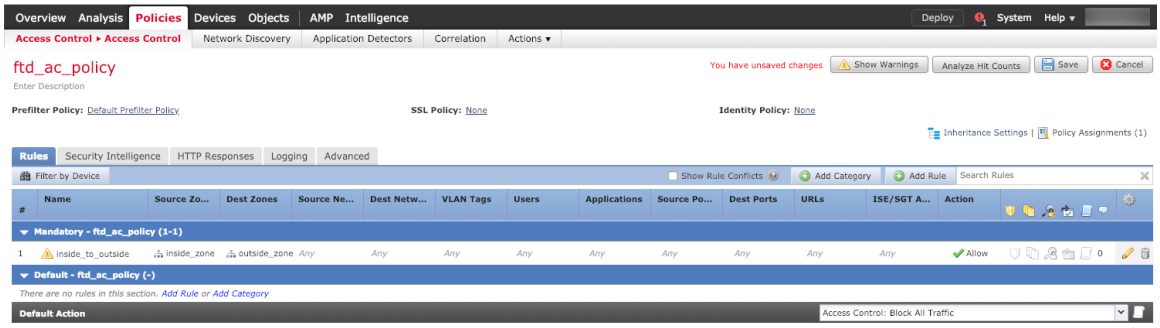


- [名前（Name）]：このルールに名前を付けます（たとえば、**inside_to_outside**）。
- [送信元ゾーン（Source Zones）]：[使用可能なゾーン（Available Zones）] から内部ゾーンを選択し、[送信元に追加（Add to Source）] をクリックします。
- [宛先ゾーン（Destination Zones）]：[使用可能なゾーン（Available Zones）] から外部ゾーンを選択し、[宛先に追加（Add to Destination）] をクリックします。

他の設定はそのままにしておきます。

ステップ 3 [追加（Add）] をクリックします。

ルールが [ルール（Rules）] テーブルに追加されます。



ステップ 4 [保存（Save）] をクリックします。

マネージャ アクセス データ インターフェイスでの SSH の設定

外部インターフェイスなどのデータインターフェイスで Management Center アクセスを有効にした場合は、この手順に従ってそのインターフェイスで SSH を有効にする必要があります。ここでは、Threat Defense で 1 つ以上のデータインターフェイスに対して SSH 接続を有効にする方法について説明します。SSH は診断論理インターフェイスに対してサポートされません。

（注） SSH は管理インターフェイス上でデフォルトで有効になっていますが、この画面は管理 SSH アクセスに影響しません。

管理インターフェイスは、デバイスの他のインターフェイスとは分離されています。Management Centerにデバイスを設定し、登録するために使用されます。データ インターフェイスの SSH は、管理インターフェイスの SSH と内部および外部ユーザ リストを共有します。その他の設定は個別に設定されます。データ インターフェイスでは、この画面を使用して SSH とアクセス リストを有効にします。データ インターフェイスの SSH トラフィックは通常のルーティング設定を使用し、設定時に設定されたスタティック ルートや CLI で設定されたスタティック ルートは使用しません。

管理インターフェイスの場合、SSH アクセスリストを構成するには Cisco Secure Firewall Threat Defense コマンドリファレンス の **configure ssh-access-list** コマンドを参照してください。スタ

ティック ルートを設定するには、**configure network static-routes** コマンドを参照してください。デフォルトでは、初期設定時に管理インターフェイスからデフォルト ルートを設定します。

SSH を使用するには、ホスト IP アドレスを許可するアクセス ルールは必要ありません。このセクションの手順に従って、SSH アクセスを設定する必要があるだけです。

SSHは、到達可能なインターフェイスにのみ使用できます。SSHホストが外部インターフェイスにある場合、外部インターフェイスへの直接管理接続のみ開始できます。

（注） SSH を介した CLI へのログイン試行が 3 回連続して失敗すると、デバイスの SSH 接続は終了します。

始める前に

- SSH内部ユーザーは、**configure user add** コマンドを使用してCLIでのみ設定できます。。デフォルトでは、初期設定時にパスワードを設定した**Admin**ユーザーが存在します。LDAP または RADIUS 上の外部ユーザーは、プラットフォーム設定で [外部認証（External Authentication）] を設定することによっても設定できます。
- デバイスへの SSH 接続を許可するホストまたはネットワークを定義するネットワーク オブジェクトが必要です。オブジェクトをプロシージャの一部として追加できますが、IPアドレスのグループを特定するためにオブジェクト グループを使用する場合は、ルールで必要なグループがすでに存在することを確認します。**[オブジェクト（Objects）]**>**[オブジェクト管理（Object Management）]** を選択して、オブジェクトを設定します。

（注） システムが提供する **any** ネットワーク オブジェクトは使用できません。代わりに、**any-ipv4** または **any-ipv6** を使用します。

手順

ステップ 1 **[デバイス（Devices）]**>**[プラットフォーム設定（Platform Settings）]** を選択し、Threat Defense ポリシーを作成または編集します。

ステップ 2 [セキュア シェル（Secure Shell）] を選択します。

ステップ 3 SSH 接続を許可するインターフェイスと IP アドレスを指定します。

この表を使用して、SSH接続を受け入れるインターフェイス、およびそれらの接続を許可されるクライアントの IP アドレスを制限します。個々の IP アドレスはなく、ネットワーク アドレスを使用できます。

a) [追加（Add）]をクリックして新しいルールを追加するか、[編集（Edit）]をクリックして既存のルールを編集します。

b) ルールのプロパティを設定します。

- [IP Address]：SSH 接続を許可するホストまたはネットワークを特定するネットワークオブジェクトまたはグループ。オブジェクトをドロップダウンメニューから選択するか、または [+] をクリックして新しいネットワークオブジェクトを追加します。
- [セキュリティ ゾーン（Security Zones）]：SSH 接続を許可するインターフェイスを含むゾーンを追加します。ゾーンにないインターフェイスでは、選択されたセキュリティゾーンのリストの下のフィールドにインターフェイス名を入力し、[追加（Add）] をクリックします。選択されているインターフェイスまたはゾーンがデバイスに含まれているときにのみ、これらのルールがデバイスに適用されます。

c) [OK] をクリックします。

ステップ 4 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更はポリシーを展開するまで有効になりません。

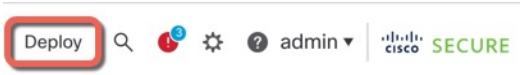
設定の展開

設定の変更を Threat Defense に展開します。変更を展開するまでは、デバイス上でどの変更もアクティブになりません。

手順

ステップ 1 右上の [展開（Deploy）] をクリックします。

図 *21 : [展開（Deploy）]*



ステップ 2 [すべて展開（Deploy All）] をクリックしてすべてのデバイスに展開するか、[高度な展開（Advanced Deploy）] をクリックして選択したデバイスに展開します。

図 *22* : すべて展開

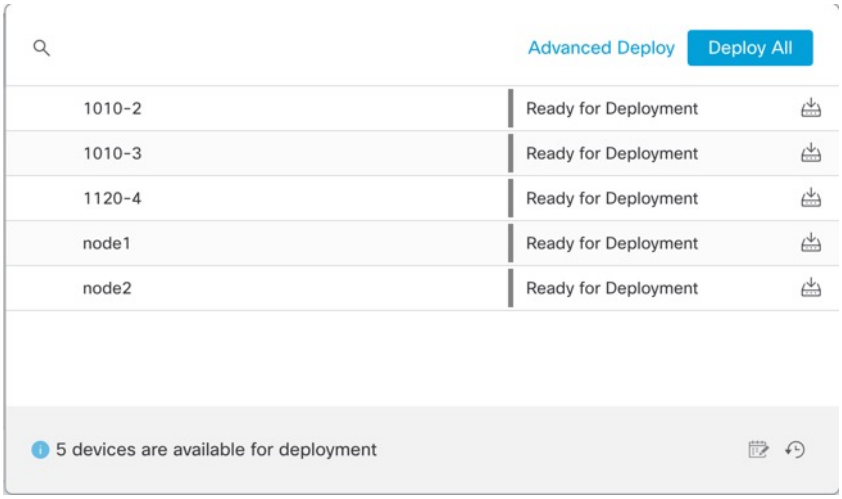
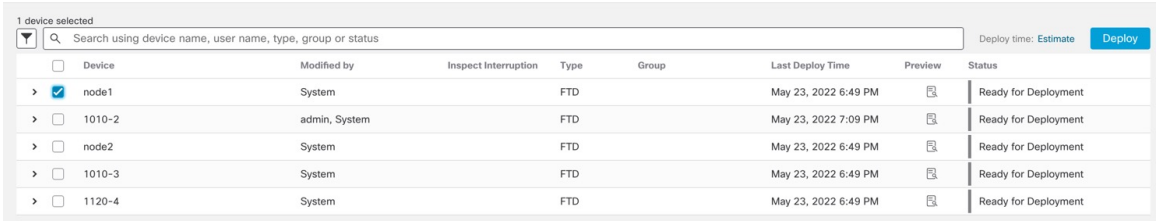
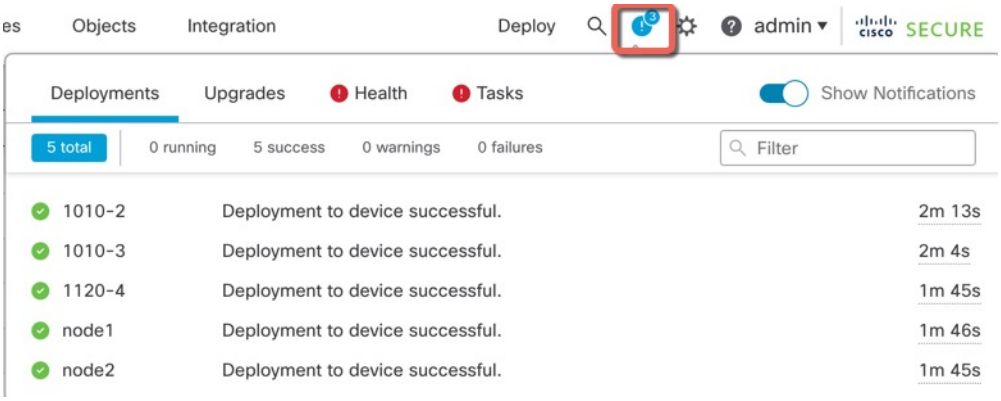


図 *23* : 高度な展開



ステップ 3 展開が成功したことを確認します。展開のステータスを表示するには、メニューバーの [展開（Deploy）] ボタンの右側にあるアイコンをクリックします。

図 *24* : 展開ステータス



Threat Defense および FXOS CLI へのアクセス

コマンドライン インターフェイス（CLI）を使用してシステムのセットアップを行い、基本的なシステムのトラブルシューティングを行います。CLIセッションからポリシーを設定することはできません。CLI には、コンソール ポートに接続してアクセスできます。

トラブルシューティングのためにも FXOS CLI にアクセスできます。

（注） または、Threat Defense デバイスの管理インターフェイスに SSH で接続できます。コンソール セッションとは異なり、SSH セッションはデフォルトで Threat Defense CLI になり、**connect fxos** コマンドを使用して FXOS CLI に接続できます。SSH 接続用のインターフェイスを開いている場合、後でデータインターフェイス上のアドレスに接続できます。データ インターフェイスへの SSH アクセスはデフォルトで無効になっています。この手順では、デフォルトで FXOS CLI となるコンソールポートアクセスについて説明します。

手順

ステップ 1 CLI にログインするには、管理コンピュータをコンソール ポートに接続します。 Firepower 1000 には、USB A to B シリアル ケーブルが付属しています。お使いのオペレーティングシステムに必要な USB シリアルドライバを必ずインストールしてください（Firepower 1010 ハードウェアガイドを参照）。コンソールポートはデフォルトで FXOS CLI になります。次のシリアル設定を使用します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

FXOS CLI に接続します。ユーザー名 **admin** と、初期セットアップ時に設定したパスワードを使用して CLI にログインします（デフォルトは **Admin123**）。

例：

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

ステップ 2 Threat Defense CLI にアクセスします。

connect ftd

例：

```
firepower# connect ftd
>
```

ログイン後に、CLI で使用可能なコマンドの情報を確認するには、**help** または **?** を入力します。使用方法については、『Cisco Secure Firewall Threat Defense コマンドリファレンス』を参照してください。

ステップ 3 Threat Defense CLI を終了するには、**exit** または **logout** コマンドを入力します。

このコマンドにより、FXOS CLI プロンプトに戻ります。FXOS CLI で使用可能なコマンドについては、**?** を入力してください。

例：

```
> exit
firepower#
```

データインターフェイスでの管理接続のトラブルシューティング

モデルのサポート：Threat Defense

専用の管理インターフェイスを使用する代わりに、Management Center にデータインターフェイスを使用する場合は、Management Center で Threat Defense のインターフェイスとネットワークの設定を変更するときに接続を中断しないように注意します。Threat Defense を Management Center に追加した後に管理インターフェイスタイプを変更する場合（データから管理へ、または管理からデータへ）、インターフェイスとネットワークの設定が正しく構成されていないと、管理接続が失われる可能性があります。

このトピックは、管理接続が失われた場合のトラブルシューティングに役立ちます。

管理接続ステータスの表示

Management Center で、[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [管理（Management）] > [FMCアクセスの詳細（FMC Access Details）] > [接続ステータス（Connection Status）] ページの順に選択して管理接続のステータスを確認します。

管理接続のステータスを表示するには、Threat Defense CLI で、**sftunnel-status-brief** コマンドを入力します。**sftunnel-status** を使用して、より完全な情報を表示することもできます。

ダウン状態の接続の出力例を次に示します。ピアチャネルの「接続先」情報やハートビート情報が表示されていません。

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went
```

```
down
```

アップ状態の接続の出力例を次に示します。ピアチャネルとハートビート情報が表示されています。

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to
'10.10.17.202' via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to
'10.10.17.202' via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

Threat Defense ネットワーク情報の表示

Threat Defense CLI で、管理および Management Center アクセス データ インターフェイスのネットワーク設定を表示します。

show network

```
> show network
===============[ System Information ]===============
Hostname                  : 5516X-4
DNS Servers               : 208.67.220.220,208.67.222.222
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces
IPv6 Default route
  Gateway                 : data-interfaces

======================[ br1 ]=======================
State                     : Enabled
Link                      : Up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 28:6F:7F:D3:CB:8D
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.99.10.4
Netmask                   : 255.255.255.0
Gateway                   : 10.99.10.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

===============[ Proxy Information ]================
State                     : Disabled
Authentication            : Disabled

======[ System Information - Data Interfaces ]======
DNS Servers               :
Interfaces                : GigabitEthernet1/1

===============[ GigabitEthernet1/1 ]===============
State                     : Enabled
Link                      : Up
```

```
Name                        : outside
MTU                         : 1500
MAC Address                 : 28:6F:7F:D3:CB:8F
----------------------[ IPv4 ]----------------------
Configuration               : Manual
Address                     : 10.89.5.29
Netmask                     : 255.255.255.192
Gateway                     : 10.89.5.1
----------------------[ IPv6 ]----------------------
Configuration               : Disabled
```

Management Center への Threat Defense の登録の確認

Threat Defense CLI で、Management Center 登録が完了したことを確認します。このコマンドは、管理接続の現在のステータスを表示するものではないことに注意してください。

show managers

```
> show managers
Type                        : Manager
Host                        : 10.89.5.35
Registration                : Completed

>
```

Management Center に ping する

Threat Defense CLI で、次のコマンドを使用して、データインターフェイスから Management Center に ping します。

ping *fmc_ip*

Threat Defense CLI で、次のコマンドを使用して、管理インターフェイスから Management Center に ping します。これは、バックプレーンを介してデータインターフェイスにルーティングされます。

ping system *fmc_ip*

Threat Defense 内部インターフェイスでのパケットのキャプチャ

Threat Defense CLI で、内部バックプレーン インターフェイス（nlp_int_tap）でパケットをキャプチャして、管理パケットが送信されているかどうかを確認します。

capture *name* **interface nlp_int_tap trace detail match ip any any**

show capture*name* **trace detail**

内部インターフェイスのステータス、統計、およびパケット数の確認

Threat Defense CLI で、内部バックプレーン インターフェイス（nlp_int_tap）に関する情報を参照してください。

show interace detail

```
> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
 (Full-duplex), (1000 Mbps)
```

```
 Input flow control is unsupported, output flow control is unsupported
MAC address 0000.0100.0001, MTU 1500
IP address 169.254.1.1, subnet mask 255.255.255.248
37 packets input, 2822 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 pause input, 0 resume input
0 L2 decode drops
5 packets output, 370 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
input queue (blocks free curr/low): hardware (0/0)
output queue (blocks free curr/low): hardware (0/0)
 Traffic Statistics for "nlp_int_tap":
37 packets input, 2304 bytes
5 packets output, 300 bytes
37 packets dropped
     1 minute input rate 0 pkts/sec,  0 bytes/sec
     1 minute output rate 0 pkts/sec,  0 bytes/sec
     1 minute drop rate, 0 pkts/sec
     5 minute input rate 0 pkts/sec,  0 bytes/sec
     5 minute output rate 0 pkts/sec,  0 bytes/sec
     5 minute drop rate, 0 pkts/sec
 Control Point Interface States:
Interface number is 14
Interface config status is active
Interface state is active
```

ルーティングと NAT の確認

Threat Defense CLI で、デフォルトルート（S*）が追加されていること、および管理インターフェイス（nlp_int_tap）に内部 NAT ルールが存在することを確認します。

show route

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C        10.89.5.0 255.255.255.192 is directly connected, outside
L        10.89.5.29 255.255.255.255 is directly connected, outside

>
```

show nat

```
> show nat

Auto NAT Policies (Section 2)
```

```
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface
service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface  service
 tcp ssh ssh
    translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
 ipv6  service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
    translate_hits = 0, untranslate_hits = 0
>
```

その他の設定の確認

次のコマンドを参照して、他のすべての設定が存在することを確認します。これらのコマンドの多くは、Management Center の [デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [管理（Management）] > [FMCアクセスの詳細（FMC Access Details）] > [CLI出力（CLI Output）] ページでも確認できます。

show running-config sftunnel

```
> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305
```

show running-config ip-client

```
> show running-config ip-client
ip-client outside
```

show conn address *fmc_ip*

```
> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
       preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap  10.89.5.29(169.254.1.2):51231 outside  10.89.5.35:8305, idle 0:00:04,
 bytes 86684, flags UxIO
TCP nlp_int_tap  10.89.5.29(169.254.1.2):8305 outside  10.89.5.35:52019, idle 0:00:02,
 bytes 1630834, flags UIO
>
```

DDNS の更新が成功したかどうかを確認する

Threat Defense CLI で、DDNS の更新が成功したかどうかを確認します。

debug ddns

```
> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfuly updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0
```

更新に失敗した場合は、**debug http** コマンドと **debug ssl** コマンドを使用します。証明書の検証が失敗した場合は、ルート証明書がデバイスにインストールされていることを確認します。

show crypto ca certificates *trustpoint_name*

DDNS の動作を確認するには：

show ddns update interface *fmc_access_ifc_name*

```
> show ddns update interface outside

Dynamic DNS Update on outside:
    Update Method Name Update Destination
    RBD_DDNS not available

Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

Management Center ログファイルの確認

https://cisco.com/go/fmc-reg-error を参照してください。

Management Center の接続が失われた場合の構成のロールバック

Management Center で Threat Defense のデータインターフェイスを使用し、ネットワーク接続に影響する Management Center からの構成の変更を展開する場合、Threat Defense の構成を最後に展開した構成にロールバックして、管理接続を復元できます。その後、ネットワーク接続が維持されるように Management Center で構成設定を調整して再展開できます。ロールバック機能は、接続が失われていない場合でも使用でき、このトラブルシューティングの状況以外でも使用できます。

次のガイドラインを参照してください。

- 前回の展開のみ Threat Defense でローカルに使用できます。さらに以前の展開にロールバックすることはできません。
- ロールバックは、高可用性またはクラスタリングの導入ではサポートされていません。
- ロールバックは、Management Center で設定できる構成にのみ影響します。たとえば、ロールバックは、Threat Defense CLI でのみ設定できる専用管理インターフェイスに関連するローカル構成には影響しません。**configure network management-data-interface** コマンドを使用した最後の Management Center 展開後にデータインターフェイス設定を変更し、rollback コマンドを使用すると、それらの設定は保持されないことに注意してください。最後に展開された Management Center 設定にロールバックされます。
- UCAPL/CC モードはロールバックできません。
- 以前の展開中に更新されたアウトオブバンド SCEP 証明書データはロールバックできません。

- ロールバック中に、現在の設定がクリアされるため、接続がドロップされます。

始める前に

モデルのサポート：Threat Defense

手順

ステップ 1 Threat Defense CLI で、以前の構成へロールバックします。

configure policy rollback

ロールバック後、Threat Defense はロールバックが正常に完了したことを Management Center に通知します。Management Center では、構成がロールバックされたことを示すバナーが展開画面に表示されます。

ロールバックが失敗した場合、一般的な展開の問題についてhttps://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.htmlを参照してください。場合によっては、Management Center アクセスの復元後にロールバックが失敗することがあります。この場合、Management Center の構成の問題を解決して、Management Center から再展開できます。

例：

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....................
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
.....................
.....................
>
```

ステップ 2 管理接続が再確立されたことを確認します。

Management Center で、[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [管理（Management）] > [FMCアクセスの詳細（FMC Access Details）] > [接続ステータス（Connection Status）] ページの順に選択して管理接続のステータスを確認します。

管理接続のステータスを表示するには、Threat Defense CLI で、**sftunnel-status-brief** コマンドを入力します。

接続の再確立に 10 分以上かかる場合は、接続のトラブルシューティングを行う必要があります。データインターフェイスでの管理接続のトラブルシューティング （93 ページ） を参照してください。

Management Center を使用したファイアウォールの電源の切断

システムを適切にシャットダウンすることが重要です。単純に電源プラグを抜いたり、電源スイッチを押したりすると、重大なファイルシステムの損傷を引き起こすことがあります。バックグラウンドでは常に多数のプロセスが実行されていて、電源プラグを抜いたり、電源を切断したりすると、ファイアウォールをグレースフルシャットダウンできないことを覚えておいてください。

Management Center を使用してシステムを適切にシャットダウンできます。

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 再起動するデバイスの横にある編集アイコン（ ）をクリックします。

ステップ 3 [デバイス（Device）] タブをクリックします。

ステップ 4 [システム（System）]セクションでデバイスのシャットダウンアイコン（ ）をクリックします。

ステップ 5 プロンプトが表示されたら、デバイスのシャットダウンを確認します。

ステップ 6 コンソールからファイアウォールに接続している場合は、ファイアウォールがシャットダウンするときにシステムプロンプトをモニターします。次のプロンプトが表示されます。

```
System is stopped.
It is safe to power off now.

Do you want to reboot instead? [y/N]
```

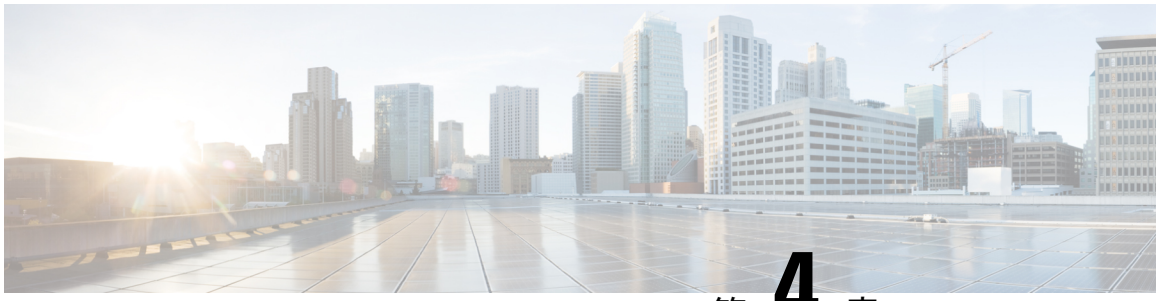
コンソールから接続していない場合は、約 3 分間待ってシステムがシャットダウンしたことを確認します。

ステップ 7 必要に応じて電源プラグを抜いてシャーシから物理的に電源を取り外すことができます。

次のステップ

Threat Defense の設定を続行するには、「Cisco Firepower ドキュメント一覧」にあるお使いのソフトウェアバージョンのマニュアルを参照してください。

Management Center の使用に関する情報については、「Firepower Management Center コンフィギュレーション ガイド」を参照してください。



第 4 章

Device Manager での Threat Defense の展開

この章の対象読者

使用可能なすべてのオペレーティングシステムとマネージャを確認するには、「最適なオペレーティングシステムとマネージャを見つける方法 （1 ページ）」を参照してください。この章の内容は、 Device Manager での Threat Defense の展開に適用されます。

この章では、 Web ベースのデバイス セットアップ ウィザードを使用して、Threat Defense の初期セットアップと設定を完了する方法について説明します。

Device Manager では、小規模ネットワークで最も一般的に使用されるソフトウェアの基本機能を設定できます。また、これは多くの Device Manager デバイスを含む大規模なネットワークを制御するために強力な複数デバイスのマネージャを使用することがない、単一のデバイスまたは限られた数のデバイスを含むネットワークのために特に設計されています。

ファイアウォールについて

ハードウェアでは、Threat Defense ソフトウェアまたは ASA ソフトウェアを実行できます。Threat Defense と ASA の間で切り替えを行う際には、デバイスの再イメージ化が必要になります。現在インストールされているものとは異なるソフトウェアバージョンが必要な場合も再イメージ化が必要です。「Cisco ASA および Firepower Threat Defense 再イメージ化ガイド」を参照してください。

ファイアウォールは、Secure Firewall eXtensible オペレーティングシステム（FXOS）と呼ばれる基盤となるオペレーティングシステムを実行します。ファイアウォールは FXOS Secure Firewall Chassis Manager をサポートしていません。トラブルシューティング用として限られた CLI のみがサポートされています。詳細については、Firepower 1000/2100 および Secure Firewall 3100 と Firepower Threat Defense の Cisco FXOS トラブルシューティング ガイドを参照してください。

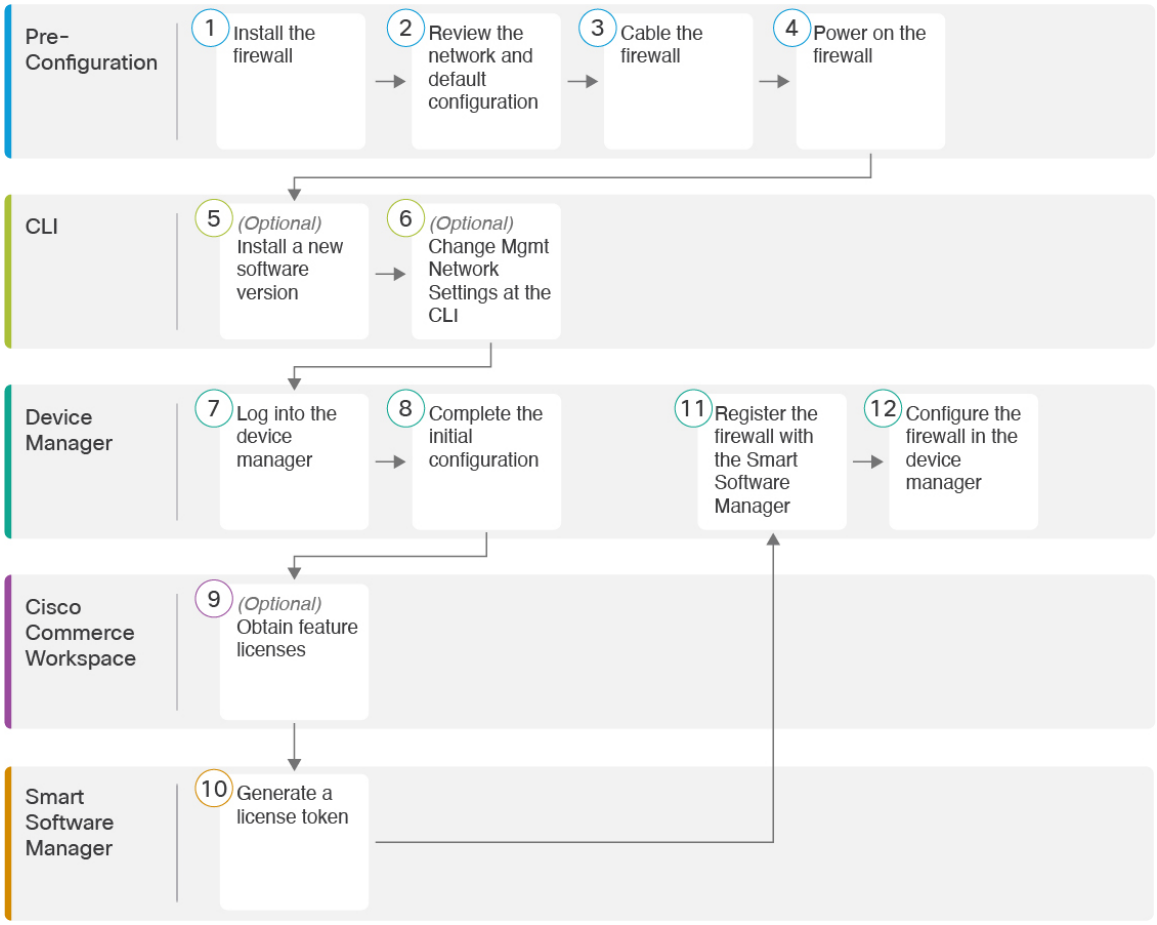
プライバシー収集ステートメント：ファイアウォールには個人識別情報は不要で、積極的に収集することもありません。ただし、ユーザー名などの設定では、個人識別情報を使用できます。この場合、設定作業時や SNMP の使用時に、管理者が個人識別情報を確認できる場合があります。

- エンドツーエンドの手順 （102 ページ）
- ネットワーク配置とデフォルト設定の確認 （103 ページ）
- デバイスの配線 （107 ページ）
- ファイアウォールの電源の投入 （108 ページ）

- （任意）ソフトウェアの確認と新しいバージョンのインストール （109 ページ）
- （任意）CLI での管理ネットワーク設定の変更 （111 ページ）
- へのログインDevice Manager （113 ページ）
- 初期設定の完了 （114 ページ）
- ライセンスの設定 （116 ページ）
- Device Manager でのファイアウォールの設定 （122 ページ）
- Threat Defense および FXOS CLI へのアクセス （127 ページ）
- ハードウェア情報の表示 （128 ページ）
- ファイアウォールの電源の切断 （129 ページ）
- 次のステップ （131 ページ）

エンドツーエンドの手順

シャーシで Device Manager を使用して Threat Defense を展開するには、次のタスクを参照してください。



1	事前設定	ファイアウォールをインストールします。ハードウェア設置ガイドを参照してください。

2	事前設定	ネットワーク配置とデフォルト設定の確認 （103 ページ）。
3	事前設定	デバイスの配線 （107 ページ）。
4	事前設定	ファイアウォールの電源の投入 （13 ページ）。
5	CLI	（任意）ソフトウェアの確認と新しいバージョンのインストール （109 ページ）
6	CLI	（任意）CLI での管理ネットワーク設定の変更 （111 ページ）。
7	Device Manager	へのログインDevice Manager （113 ページ）。
8	Device Manager	初期設定の完了 （114 ページ）。
9	Cisco Commerce Workspace	（任意）ライセンスの設定 （116 ページ）：機能ライセンスを取得します。
10	Smart Software Manager	ライセンスの設定 （116 ページ）：ライセンス トークンを生成します。
11	Device Manager	ライセンスの設定 （116 ページ）：スマート ライセンシング サーバーにデバイスを登録します。
12	Device Manager	Device Manager でのファイアウォールの設定 （122 ページ）。

ネットワーク配置とデフォルト設定の確認

Management 1/1 インターフェイスか内部インターフェイスから Device Manager を使用して Threat Defense を管理できます。専用の管理インターフェイスは、独自のネットワーク設定を持つ特別なインターフェイスです。

次の図に、推奨されるネットワーク展開を示します。外部インターフェイスをケーブルモデムか DSL モデムに直接接続する場合は、Threat Defense が内部ネットワークのすべてのルーティングと NAT を実行するように、モデムをブリッジモードにすることをお勧めします。 外部インターフェイスが ISP に接続できるように PPPoE を設定する必要がある場合は、Device Manager で初期セットアップを完了した後に行うことができます。

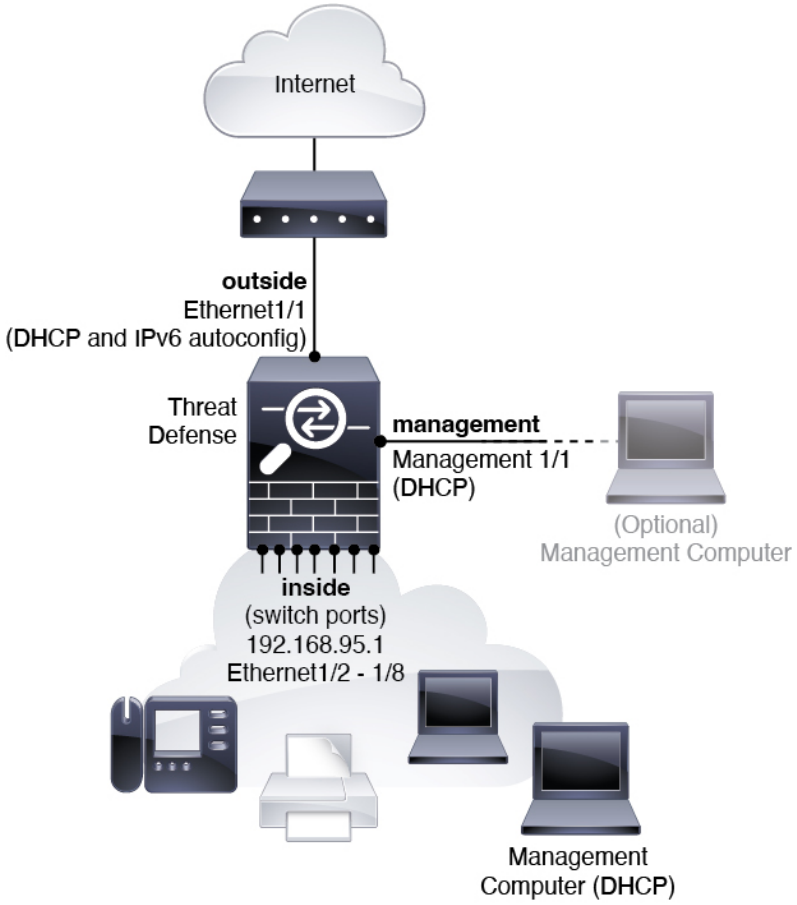
（注） デフォルトの管理 IP アドレスを使用できない場合（管理ネットワークに DHCP サーバーが含まれていない場合など）、コンソールポートに接続して、CLI で初期セットアップ（管理 IP アドレス、ゲートウェイ、およびその他の基本ネットワーク設定の指定など）を実行できます。

内部 IP アドレスを変更する必要がある場合は、Device Manager で初期セットアップを完了した後に変更できます。たとえば、次のような状況において、内部 IP アドレスの変更が必要になる場合があります。

- （7.0 以降）内部 IP アドレスは 192.168.95.1 です。（6.7 以前） 内部 IP アドレスは 192.168.1.1 です。外部インターフェイスが一般的なデフォルトネットワークである 192.168.1.0 ネットワーク上の IP アドレスの取得を試みる場合、DHCP リースが失敗し、外部インターフェイスが IP アドレスを取得しません。この問題は、Threat Defense が同じネットワーク上に 2 つのインターフェイスを持つことができないために発生します。この場合、内部 IP アドレスが新しいネットワーク上に存在するように変更する必要があります。
- Threat Defense を既存の内部ネットワークに追加する場合は、内部 IP アドレスが既存のネットワーク上に存在するように変更する必要があります。

次の図に、Device Manager を使用した Threat Defense でのデフォルトのネットワーク展開を示します（デフォルト設定を使用）。

図 *25 :* 推奨されるネットワーク配置



（注） 6.7 以前の場合、 内部 IP アドレスは 192.168.1.1 です。

6.5 以前の場合、Management 1/1 のデフォルト IP アドレスは 192.168.45.45 です。

デフォルト設定

初期設定後のファイアウォールの設定には、以下が含まれます。

- **内部**：IP アドレス（7.0 以降）192.168.95.1、（7.0 より前）192.168.1.1。
  - （6.5 以降）**ハードウェアスイッチ**：Ethernet 1/2 ～ 1/8 は VLAN 1 に属しています
  - （6.4）**ソフトウェアスイッチ**（統合ルーティングおよびブリッジング機能）：Ethernet 1/2 ～ 1/8 はブリッジ グループ インターフェイス（BVI）1 に属しています
- **外部**：イーサネット 1/1、IPv4 DHCP からの IP アドレス、および IPv6 自動設定
- **内部→外部**トラフィックフロー

- **管理**：Management 1/1（管理）
  - （6.6 以降）DHCP からの IP アドレス
  - （6.5 以前）IP アドレス 192.168.45.45

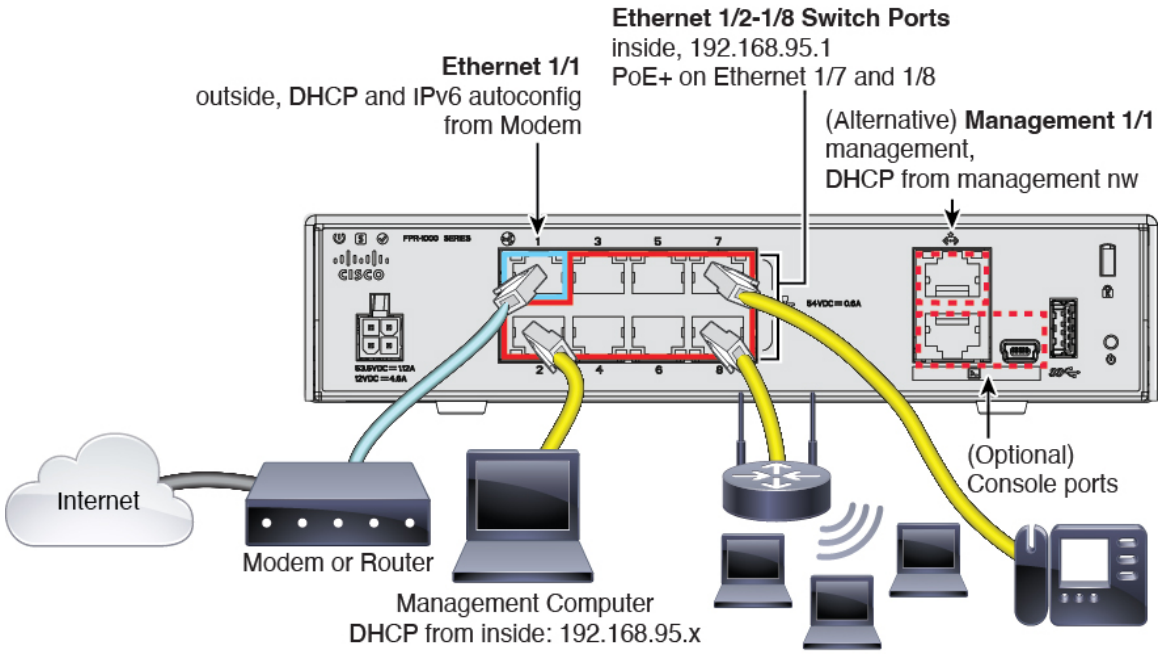
（注） Management 1/1 インターフェイスは、管理、スマートライセンス、およびデータベースの更新に使用されるデータインターフェイスとは別の特別なインターフェイスです。物理インターフェイスは、診断インターフェイスである 2 番目の論理インターフェイスと共有されます。診断はデータインターフェイスですが、syslog や SNMP など、他のタイプの管理トラフィック（デバイスとデバイス間）に限定されます。診断インターフェイスは通常使用されません。詳細については、Cisco Secure Firewall Device Manager Configuration Guideを参照してください。

- **管理用の DNS サーバー**：OpenDNS：（IPv4）208.67.222.222、208.67.220.220、（IPv6）2620:119:35::35、またはセットアップ時に指定したサーバー。DHCP から取得した DNS サーバーは使用されません。
- **NTP**：Cisco NTP サーバー：0.sourcefire.pool.ntp.org、1.sourcefire.pool.ntp.org、2.sourcefire.pool.ntp.org、またはセットアップ時に指定したサーバー
- **デフォルトルート**
  - **データインターフェイス**：外部 DHCP から取得したもの、またはセットアップ時に指定したゲートウェイ IP アドレス
  - **管理インターフェイス**：（6.6 以降）管理 DHCP から取得されます。ゲートウェイを受信しない場合、デフォルトルートはバックプレーンを介してデータインターフェイスを経由します。（6.5 以前）バックプレーンを介してデータインターフェイスを経由します。

    管理インターフェイスでは、バックプレーンを介した場合でも個別のインターネットゲートウェイを使用する場合でも、ライセンス取得や更新のためにインターネットアクセスが必要であることに注意してください。管理インターフェイスから発信されたトラフィックのみがバックプレーンを通過できることに注意してください。それ以外の場合、ネットワークから管理インターフェイスに入るトラフィックの通過は許可されません。
- **DHCP サーバー**：内部インターフェイスおよび（6.5 以前のみ）管理インターフェイスで有効になります。
- **Device Manager アクセス**：すべてのホストが管理インターフェイスと内部インターフェイスで許可されます。
- **NAT**：内部から外部へのすべてのトラフィック用のインターフェイス PAT

デバイスの配線

図 *26 : Firepower 1010* のケーブル配線



（注） 6.7 以前の場合、内部 IP アドレスは 192.168.1.1 です。

バージョン 6.5 以前の場合、Management 1/1 のデフォルト IP アドレスは 192.168.45.45 です。

（注） バージョン 6.5 以降では、イーサネット 1/2 ～ 1/8 はハードウェア スイッチ ポートとして設定されています。PoE+ はイーサネット 1/7 および 1/8 でも使用できます。バージョン 6.4 では、イーサネット 1/2 ～ 1/8 はブリッジ グループ メンバー（ソフトウェア スイッチ ポート）として設定されています。PoE+ は使用できません。最初のケーブル配線は両方のバージョンで同じです。

（注） PoE は Firepower 1010E ではサポートされていません。

Management 1/1 または Ethernet 1/2 ～ 1/8 のいずれかで Firepower 1010 を管理します。デフォルト設定でも、Ethernet1/1 を外部として設定します。

手順

ステップ 1 ハードウェア設置ガイドを使用してハードウェアを設置し、ハードウェアについてよく理解しておきます。

ステップ 2 管理コンピュータを次のいずれかのインターフェイスに接続します。

- イーサネット 1/2 ー 1/8：管理コンピュータを内部スイッチポートのいずれかに直接接続します（イーサネット 1/2 ー 1/8）。内部にはデフォルトの IP アドレス（192.168.95.1）があり、クライアント（管理コンピュータを含む）に IP アドレスを提供するために DHCP サーバーも実行されるため、これらの設定が既存の内部ネットワーク設定と競合しないようにしてください（デフォルト設定 （105 ページ）を参照）。
- Management 1/1（ラベル MGMT）： Management 1/1 を管理ネットワークに接続し、管理コンピュータが管理ネットワーク上にあるか、またはアクセスできることを確認します。Management 1/1 は、管理ネットワーク上の DHCP サーバーから IP アドレスを取得します。このインターフェイスを使用する場合は、Threat Defense に割り当てられる IP アドレスを決定して、管理コンピュータから IP アドレスに接続できるようにする必要があります。

  Management 1/1 IP アドレスをデフォルトから変更し、静的 IP アドレスを設定する必要がある場合は、管理コンピュータをコンソールポートにケーブル接続する必要もあります。「（任意）CLI での管理ネットワーク設定の変更 （111 ページ）」を参照してください。

ステップ 3 外部ネットワークを Ethernet 1/1 インターフェイスに接続します。

デフォルトでは、IP アドレスは IPv4 DHCP および IPv6 自動設定を使用して取得しますが、初期設定時に静的アドレスを設定できます。

ステップ 4 内部デバイスを残りのスイッチ ポート（Ethernet 1/2 ～ 1/8）に接続します。

イーサネット 1/7 および 1/8 は PoE+ ポートです。

ファイアウォールの電源の投入

システムの電源は電源コードで制御されます。電源ボタンはありません。

（注） Threat Defense を初めて起動するときは、初期化に約 15 ～ 30 分かかります。

始める前に

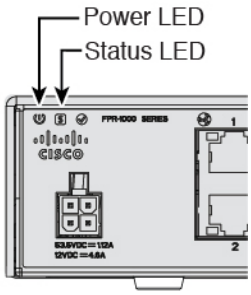
デバイスに対して信頼性の高い電力を供給することが重要です（たとえば、無停電電源装置（UPS）を使用）。最初のシャットダウンを行わないで電力が失われると、重大なファイルシステムの損傷を引き起こす可能性があります。バックグラウンドでは常に多数のプロセスが実行されていて、電力が失われると、システムをグレースフルシャットダウンできません。

手順

ステップ 1 電源コードをデバイスに接続し、電源コンセントに接続します。

電源コードを差し込むと電源が自動的に入ります。

ステップ 2 デバイスの背面または上部にある電源 LED を確認します。緑色に点灯している場合は、デバイスの電源が入っています。



ステップ 3 デバイスの背面または上部にあるステータス LED を確認します。緑色に点灯している場合は、電源投入時診断に合格しています。

（任意）ソフトウェアの確認と新しいバージョンのインストール

ソフトウェアのバージョンを確認し、必要に応じて別のバージョンをインストールするには、次の手順を実行します。ファイアウォールを設定する前に対象バージョンをインストールすることをお勧めします。別の方法として、稼働後にアップグレードを実行することもできますが、設定を保持するアップグレードでは、この手順を使用するよりも時間がかかる場合があります。

実行するバージョン

ソフトウェア ダウンロード ページのリリース番号の横にある、金色の星が付いている Gold Star リリースを実行することをお勧めします。https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html に記載されているリリース戦略も参照してください。たとえば、この速報では、（最新機能を含む）短期的なリリース番号、長期的なリリース番号（より長期間のメンテナンスリリースとパッチ）、または非常に長期的なリリース番号（政府認定を受けるための最長期間のメンテナンスリリースとパッチ）について説明しています。

手順

ステップ 1 CLI に接続します。詳細については、Threat Defense および FXOS CLI へのアクセス （127 ページ）を参照してください。この手順ではコンソールポートを使用していますが、代わりに SSH を使用することもできます。

admin ユーザとデフォルトパスワードの **Admin123** を使用してログインします。

FXOS CLI に接続します。初めてログインしたとき、パスワードを変更するよう求められます。このパスワードは、SSH の Threat Defense ログインにも使用されます。

（注） パスワードがすでに変更されていて、パスワードがわからない場合は、初期設定へのリセットを実行して、パスワードをデフォルトにリセットする必要があります。初期設定へのリセット手順については、『FXOS troubleshooting guide』を参照してください。

例：

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

ステップ 2 FXOS CLI で、実行中のバージョンを表示します。

scope ssa

show app-instance

例：

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name     Slot ID    Admin State     Operational State    Running Version
Startup Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd                  1          Enabled         Online               7.2.0.65
7.2.0.65        Not Applicable
```

ステップ 3 新しいバージョンをインストールする場合は、次の手順を実行します。

a) 管理インターフェイスに静的 IP アドレスを設定する必要がある場合は、「（任意）CLI での管理ネットワーク設定の変更 （111 ページ）」を参照してください。デフォルトでは、管理インターフェイスは DHCP を使用します。

管理インターフェイスからアクセスできるサーバーから新しいイメージをダウンロードする必要があります。

b) FXOS のトラブルシューティング ガイドに記載されている再イメージ化の手順を実行します。

（任意）CLI での管理ネットワーク設定の変更

デフォルトの IP アドレスを使用できない場合（たとえば、デバイスを既存のネットワークに追加する場合）、コンソールポートに接続して、CLI で初期セットアップ（管理 IP アドレス、ゲートウェイ、およびその他の基本ネットワーク設定の指定など）を実行できます。管理インターフェイスのみを設定できます。内部インターフェイスや外部インターフェイスは設定できません。これらは後で GUI を使用して設定できます。

（注） 設定をクリア（たとえば、イメージを再作成することにより）しないかぎり、CLI セットアップスクリプトを繰り返すことはできません。ただし、これらの設定すべては、後から CLI で **configure network** コマンドを使用して変更できます。Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。

手順

ステップ 1 Threat Defense コンソール ポートに接続します。詳細については、Threat Defense および FXOS CLI へのアクセス （127 ページ）を参照してください。

admin ユーザーとデフォルトパスワードの **Admin123** を使用してログインします。

FXOS CLI に接続します。初めてログインしたとき、パスワードを変更するよう求められます。このパスワードは、SSH の Threat Defense ログインにも使用されます。

（注） パスワードがすでに変更されていて、パスワードがわからない場合は、デバイスを再イメージ化してパスワードをデフォルトにリセットする必要があります。再イメージ化の手順については、『FXOS troubleshooting guide』を参照してください。

例：

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]
```

```
Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

ステップ 2 Threat Defense CLI に接続します。

connect ftd

例：

```
firepower# connect ftd
>
```

ステップ 3 Threat Defense に初めてログインすると、エンドユーザーライセンス契約（EULA）に同意するように求められます。その後、CLI セットアップスクリプトが表示されます。

デフォルト値または以前に入力した値がカッコ内に表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

次のガイドラインを参照してください。

- [管理インターフェイスの IPv4 デフォルトゲートウェイを入力します（Enter the IPv4 default gateway for the management interface）]：手動 IP アドレスを設定した場合は、「**data-interfaces**」またはゲートウェイルータの IP アドレスのいずれかを入力します。**data-interfaces** を設定すると、アウトバウンド管理トラフィックがバックプレーン経由で送信され、データインターフェイスが終了します。この設定は、インターネットにアクセスできる個別の管理ネットワークがない場合に役立ちます。管理インターフェイスから発信されるトラフィックには、インターネットアクセスを必要とするライセンス登録とデータベースの更新が含まれます。**data-interfaces** を使用する場合、管理ネットワークに直接接続していれば管理インターフェイスで Device Manager（または SSH）を引き続き使用できますが、特定のネットワークまたはホストのリモート管理の場合は、**configure network static-routes** コマンドを使用して静的ルートを追加する必要があります。データインターフェイスでの Device Manager の管理は、この設定の影響を受けないことに注意してください。DHCP を使用する場合、システムは DHCP によって提供されるゲートウェイを使用します。DHCP がゲートウェイを提供しない場合は、フォールバックメソッドとして **data-interfaces** を使用します。
- [ネットワーク情報が変更された場合は再接続が必要になります（If your networking information has changed, you will need to reconnect）]：SSH でデフォルトの IP アドレスに接続しているのに、初期セットアップでその IP アドレスを変更すると、接続が切断されます。新しい IP アドレスとパスワードで再接続してください。コンソール接続は影響を受けません。

- [デバイスをローカルで管理しますか（Manage the device locally?）]：または Device Manager を使用するには [はい（yes）] を入力します。[いいえ（no）] と応えると、Management Centerデバイスの管理にはオンプレミスまたはクラウド配信を使用することになります。

例：

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: yes

>
```

ステップ 4 新しい管理 IP アドレスで Device Manager にログインしてください。

へのログインDevice Manager

Device Manager にログインして Threat Defense を設定します。

始める前に

- Firefox、Chrome、Safari、Edge、または Internet Explorer の最新バージョンを使用します。

手順

ステップ 1 ブラウザに次の URL を入力します。

- （7.0 以降）内部（イーサネット 1/2 ～ 1/8）：**https://192.168.95.1**。内部スイッチ ポート（Ethernet1/2 ～ 1/8）の内部アドレスに接続できます。
- （6.7 以降）内部（イーサネット 1/2 ～ 1/8）：**https://192.168.1.1**。内部スイッチ ポート（Ethernet1/2 ～ 1/8）の内部アドレスに接続できます。

- （6.6 以降）管理：**https://***management_ip*。管理インターフェイスは DHCP クライアントであるため、IP アドレスは DHCP サーバーによって異なります。CLI セットアップで管理 IP アドレスを変更した場合は、そのアドレスを入力します。
- （6.5 以前）管理：**https://192.168.45.45**。CLI セットアップで管理 IP アドレスを変更した場合は、そのアドレスを入力します。

ステップ 2 ユーザー名 **admin**、デフォルトパスワード **Admin123** を使用してログインします。

次のタスク

- Device Manager セットアップウィザードを実行します。初期設定の完了 （114 ページ）を参照してください。

初期設定の完了

初期設定を完了するには、最初に Device Manager にログインしたときにセットアップウィザードを使用します。セットアップ ウィザードの完了後、いくつかの基本ポリシーが適切に設定された機能しているデバイスが必要です。

- 外部（Ethernet1/1）および内部インターフェイス。Ethernet 1/2 から 1/8 までは、内部 VLAN1 インターフェイス上（6.5 以降）または BVI1 のブリッジグループメンバー内（6.4）のスイッチポートです。
- 内部インターフェイスと外部インターフェイスのセキュリティゾーン。
- 内部から外部へのすべてのトラフィックを信頼するアクセスルール。
- 内部から外部へのすべてのトラフィックを外部インターフェイスの IP アドレスの固有のポートへ変換するインターフェイス NAT ルール。
- 内部インターフェイスで実行されている DHCP サーバー。

（注） （任意）CLI での管理ネットワーク設定の変更 （111 ページ）の手順を実行した場合は、これらのタスクの一部、具体的には管理者パスワードの変更、および外部インターフェイスと管理インターフェイスの設定がすでに完了しているはずです。

手順

ステップ 1 エンド ユーザー ライセンス契約書を読んで同意し、管理者パスワードを変更するように求められます。

続行するには、これらの手順を完了する必要があります。

ステップ 2 外部インターフェイスおよび管理インターフェイスに対して次のオプションを設定し、[次へ（Next）] をクリックします。

（注） [次へ（Next）] をクリックすると、設定がデバイスに展開されます。インターフェイスの名前は「外部」となり、「outside_zone」セキュリティゾーンに追加されます。設定値が正しいことを確認します。

a) [外部インターフェイス（Outside Interface）]：これは、ゲートウェイ ルータに接続するためのデータ ポートです。デバイスの初期設定時に別の外部インターフェイスを選択することはできません。最初のデータインターフェイスがデフォルトの外部インターフェイスです。

[IPv4の設定（Configure IPv4）]：外部インターフェイス用の IPv4 アドレスです。DHCP を使用するか、または手動でスタティック IP アドレス、サブネットマスク、およびゲートウェイを入力できます。[オフ（Off）] を選択して、IPv4 アドレスを設定しないという選択肢もあります。セットアップウィザードを使用して PPPoE を設定することはできません。インターフェイスが DSL モデム、ケーブルモデム、または ISP への他の接続に接続されており、ISP が PPPoE を使用して IP アドレスを提供している場合は、PPPoE が必要になる場合があります。ウィザードの完了後に PPPoE を設定できます。

[IPv6の設定（Configure IPv6）]：外部インターフェイス用の IPv6 アドレスです。DHCP を使用するか、または手動でスタティック IP アドレス、プレフィックス、およびゲートウェイを入力できます。[オフ（Off）] を選択して、IPv6 アドレスを設定しないという選択肢もあります。

b) **[管理インターフェイス（Management Interface）]**

[DNSサーバ（DNS Servers）]：システムの管理アドレス用の DNS サーバ。名前解決用に 1 つ以上の DNS サーバのアドレスを入力します。デフォルトは OpenDNS パブリック DNS サーバです。フィールドを編集し、デフォルトに戻したい場合は、[OpenDNSを使用（Use OpenDNS）] をクリックすると、フィールドに適切な IP アドレスがリロードされます。

[ファイアウォールホスト名（Firewall Hostname）]：システムの管理アドレスのホスト名です。

ステップ 3 システム時刻を設定し、[次へ（Next）] をクリックします。

a) [タイムゾーン（Time Zone）]：システムのタイムゾーンを選択します。
b) [NTPタイムサーバ（NTP Time Server）]：デフォルトの NTP サーバを使用するか、使用している NTP サーバのアドレスを手動で入力するかを選択します。バックアップ用に複数のサーバを追加できます。

ステップ 4 （任意） システムのスマートライセンスを設定します。

Threat Defense デバイスを購入すると、自動的に基本ライセンスが付いてきます。すべての追加ライセンスはオプションです。

スマートライセンスのアカウントを取得し、システムが必要とするライセンスを適用する必要があります。最初は 90 日間の評価ライセンスを使用し、後でスマートライセンスを設定できます。

デバイスを今すぐ登録するには、リンクをクリックして Smart Software Manager のアカウントにログインします。ライセンスの設定 （116 ページ）を参照してください。

評価ライセンスを使用するには、[登録せずに90日間の評価期間を開始する（Start 90 day evaluation period without registration）] を選択します。

ステップ 5 **[終了（Finish）]** をクリックします。

次のタスク

- 評価ライセンスを引き続き使用することもできますが、デバイスを登録し、ライセンスを取得することをお勧めします。を参照してくださいライセンスの設定 （116 ページ）。
- Device Manager を使用してデバイスを設定することもできます。「Device Manager でのファイアウォールの設定 （122 ページ）」を参照してください。

ライセンスの設定

Threat Defense は、ライセンスの購入およびライセンスプールの一元管理が可能なスマート ソフトウェア ライセンシングを使用します。

シャーシを登録すると、Smart Software Manager はシャーシと Smart Software Manager 間の通信用の ID 証明書を発行します。また、適切な仮想アカウントにシャーシが割り当てられます。

シスコライセンスの概要については詳しくは、cisco.com/go/licensingguide を参照してください。

Essentials ライセンスは自動的に含まれます。スマートライセンスでは、まだ購入していない製品の機能を使用できます。Smart Software Manager に登録すると、すぐにライセンスの使用を開始できます。また、後でライセンスを購入することもできます。これによって、機能の展開および使用が可能になり、発注書の承認による遅延がなくなります。次のライセンスを確認してください。

- **IPS**：セキュリティインテリジェンスと次世代 IPS
- **マルウェア防御**：マルウェア防御
- **URL**：URL フィルタリング
- **Cisco Secure Client**：Secure Client Advantage、Secure Client Premier、または Secure Client VPN のみ

始める前に

- Smart Software Manager にマスターアカウントを持ちます。

  まだアカウントをお持ちでない場合は、リンクをクリックして新しいアカウントを設定してください。Smart Software Manager では、組織のマスター アカウントを作成できます。

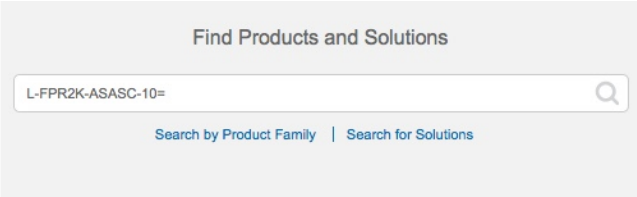
- （輸出コンプライアンスフラグを使用して有効化される）機能を使用するには、ご使用のスマート ソフトウェア ライセンシング アカウントで強力な暗号化（3DES/AES）ライセンスを使用できる必要があります。

手順

ステップ 1 お使いのスマート ライセンシング アカウントに、必要なライセンスが含まれていることを確認してください。

ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマート ソフトウェア ライセンシング アカウントにリンクされています。ただし、主導でライセンスを追加する必要がある場合は、Cisco Commerce Workspace で [製品とソリューションの検索（Find Products and Solutions）] 検索フィールドを使用します。次のライセンス PID を検索します。

図 *27*：ライセンス検索



（注） PID が見つからない場合は、注文に手動で PID を追加できます。

- IPS、マルウェア防御、および URL ライセンスの組み合わせ：
  - L-FPR1010T-TMC=

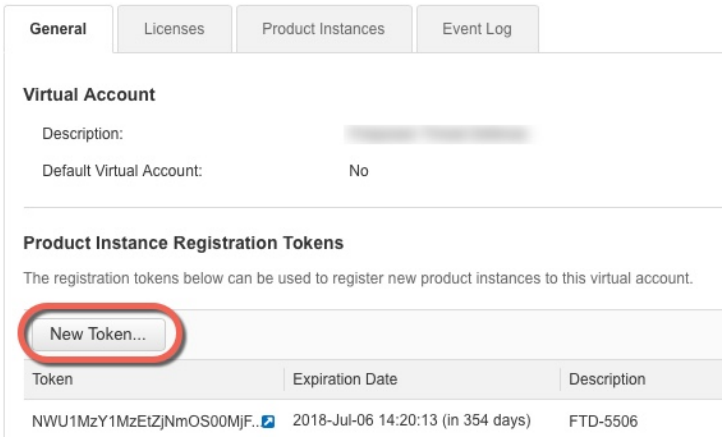
  上記の PID のいずれかを注文に追加すると、次のいずれかの PID に対応する期間ベースのサブスクリプションを選択できます。
  - L-FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y
  - L-FPR1010T-TMC-5Y

- Cisco Secure Client：『Cisco Secure Client 発注ガイド』を参照してください。

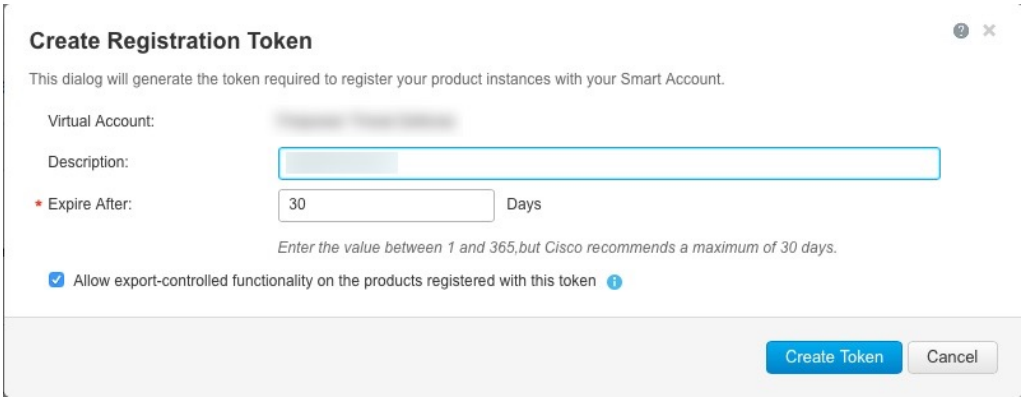
ステップ 2 Smart Software Manager で、このデバイスを追加する仮想アカウントの登録トークンを要求してコピーします。

a) [Inventory] をクリックします。

b) [General] タブで、[New Token] をクリックします。



c) [登録トークンを作成（Create Registration Token）] ダイアログボックスで、以下の設定値を入力してから [トークンを作成（Create Token）] をクリックします。



- **[説明（Description）]**
- [有効期限（Expire After）]：推奨値は 30 日です。
- [このトークンに登録された製品で輸出管理機能を許可する（Allow export-controlled functionality on the products registered with this token）]：高度暗号化が許可されている国の場合は輸出コンプライアンスフラグを有効にします。この機能を使用する予定の場合、このオプションをここで選択する必要があります。後でこの機能を有効にする場合は、デバイスを新しいプロダクトキーで再登録し、デバイスをリロードする必要があります。このオプションが表示されない場合、アカウントは輸出規制機能をサポートしていません。

トークンはインベントリに追加されます。

d) トークンの右側にある矢印アイコンをクリックして [トークン（Token）] ダイアログボックスを開き、トークン ID をクリップボードにコピーできるようにします。Threat Defense の登録が必要なときに後の手順で使用するために、このトークンを準備しておきます。

図 *28* : トークンの表示

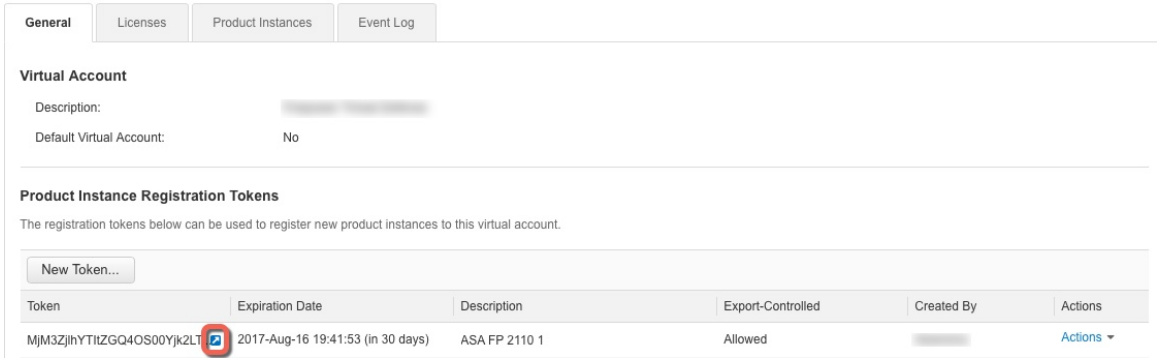
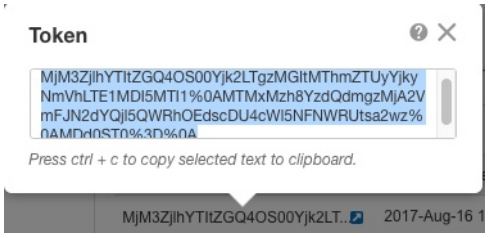


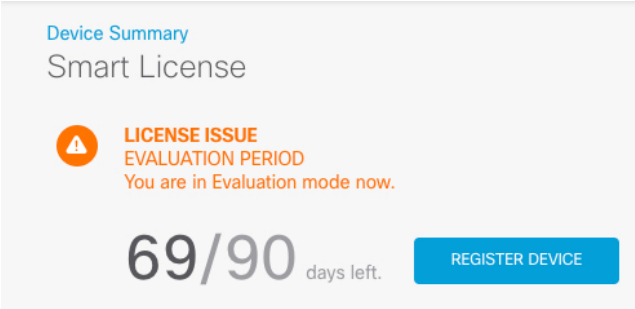
図 *29* : トークンのコピー



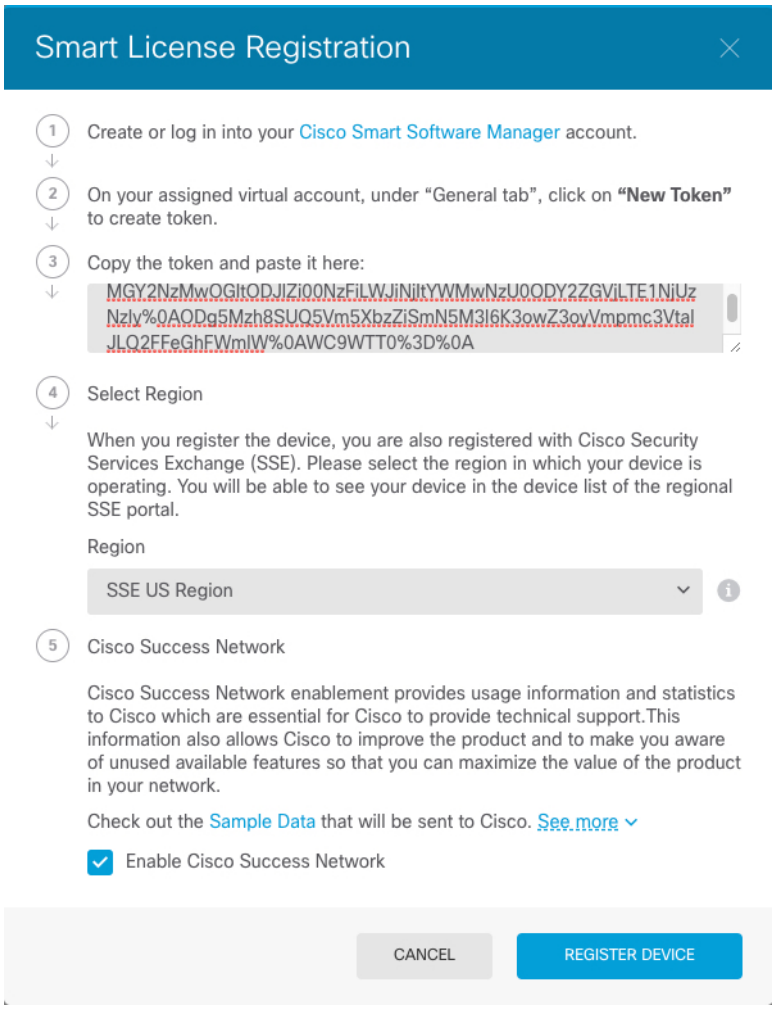
ステップ 3 Device Manager で、[デバイス（Device）] をクリックし、[スマートライセンス（Smart License）] のサマリーで [設定の表示（View Configuration）] をクリックします。

[スマート ライセンス（Smart License）] ページが表示されます。

ステップ 4 [デバイスの登録（Register Device）] をクリックします。

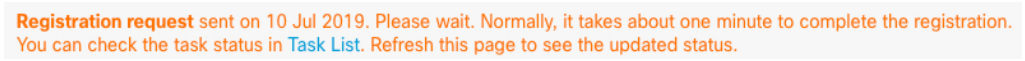


次に、[スマートライセンスの登録（Smart License Registration）] ダイアログボックスの指示に従って、トークンに貼り付けます。

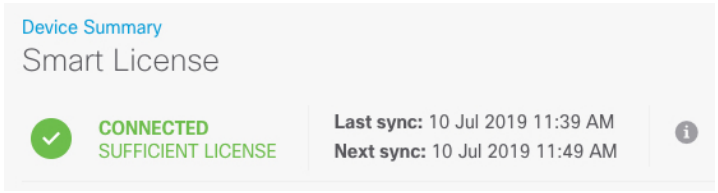


ステップ 5 [デバイスの登録（Register Device）] をクリックします。

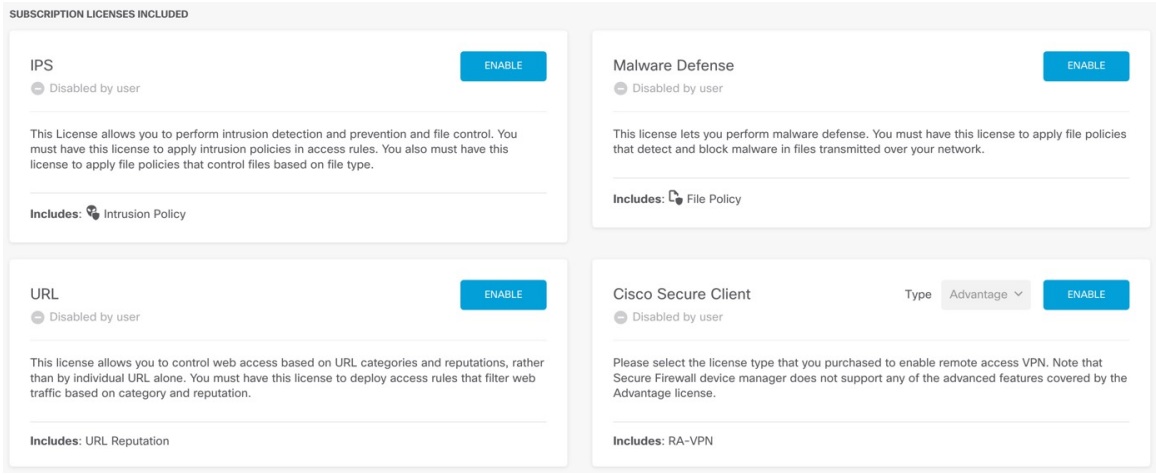
[スマート ライセンス（Smart License）] ページに戻ります。デバイス登録中は次のメッセージが表示されます。



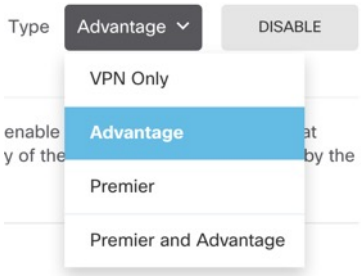
デバイスが正常に登録され、ページが更新されると、次のように表示されます。



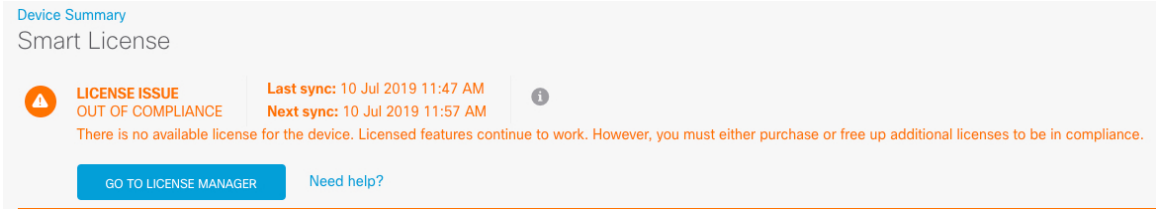
ステップ 6 必要に応じて、それぞれのオプション ライセンスの [有効化/無効化（Enable/Disable）] コントロールをクリックします。



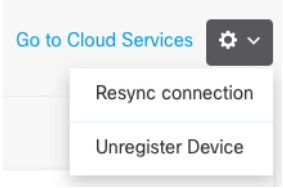
- [有効化（Enable）]：Cisco Smart Software Manager アカウントにライセンスを登録し、制御された機能が有効になります。ライセンスによって制御されるポリシーを設定し、展開できます。
- [無効化（Disable）]：Cisco Smart Software Manager アカウントのライセンスを登録解除し、制御された機能が無効になります。新しいポリシーの機能の設定も、その機能を使用するポリシーの展開もできません。
- [Cisco Secure Client] [RA VPN] ライセンスを有効にした場合は、使用するライセンスのタイプ（[Advantage]、[Plus]、[Premier]、[Apex]、[VPN専用（VPN Only）、または [Premier とAdvantage（Premier and Advantage）] [Apex and Plus（Apex and Plus）] を選択します。



機能を有効にすると、アカウントにライセンスがない場合はページを更新した後に次の非準拠メッセージが表示されます。



ステップ 7 歯車ドロップダウン リストから [接続の再同期（Resync Connection）] を選択して、Cisco Smart Software Manager とライセンス情報を同期させます。



Device Manager でのファイアウォールの設定

次の手順では、追加機能の設定の概要を説明します。各手順について詳細な情報を表示するには、ページのヘルプ ボタン（**?**）をクリックしてください。

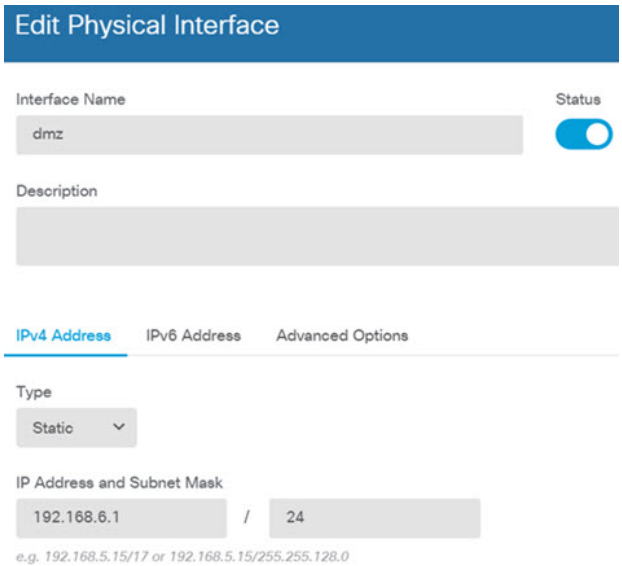
手順

ステップ 1 ブリッジグループインターフェイスを変換する（6.4）またはスイッチポートをファイアウォール インターフェイスに変換する（6.5 以降）場合は、[デバイス（Device）] を選択して [インターフェイス（Interfaces）] の概要のリンクをクリックします。

各インターフェイスの編集アイコン（）をクリックしてモードを設定し、IP アドレスなどの設定を定義します。

次の例では、Web サーバーなどのパブリックアクセス可能な資産を配置する「緩衝地帯」（DMZ）として使用するためのインターフェイスを構成します。完了したら [保存（Save）] をクリックします。

図 *30* : インターフェイスの編集



ステップ 2 新しいインターフェイスを構成する場合は、[オブジェクト（Objects）] を選択し、目次から[セキュリティゾーン（Security Zones）] を選択します。

編集または必要に応じて新しいゾーンを作成します。インターフェイスではなく、セキュリティゾーンに基づいてポリシーを構成するため、各インターフェイスはゾーンに属している必要があります。インターフェイスを構成する場合、ゾーンにインターフェイスを置くことはできません。このため、新しいインターフェイスを作成した後、または既存のインターフェイスの目的を変更した後には常にゾーン オブジェクトを編集する必要があります。

次の例では、DMZインターフェイスのために新しいDMZゾーンを作成する方法を示します。

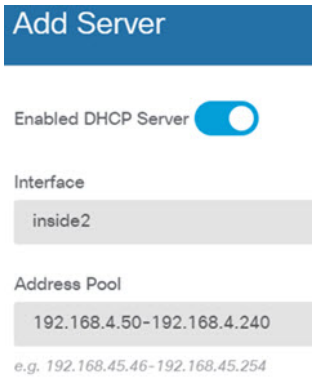
図 *31* : セキュリティ ゾーン オブジェクト

ステップ 3 内部クライアントで DHCP を使用してデバイスから IP アドレスを取得する場合は、**[デバイス（Device）] > [システム設定（System Settings）] > [DHCPサーバー（DHCP Server）]** を選択してから、**[DHCPサーバー（DHCP Servers）]** タブを選択します。

すでに内部インターフェイス用に構成されているDHCPサーバーがありますが、アドレスプールを編集したり、それを削除したりすることができます。他の内部インターフェイスを構成した場合は、それらのインターフェイス上にDHCPサーバーをセットアップするのがごく一般的です。[+]をクリックして各内部インターフェイスのサーバーとアドレスプールを構成します。

[構成（Configuration）] タブでクライアントに提供される WINS および DNS のリストを微調整することもできます。次の例では、アドレス プールの 192.168.4.50 ～ 192.168.4.240 で inside2 インターフェイス上の DHCP サーバーを設定する方法を示しています。

図 *32 : DHCP* サーバー



ステップ 4 [デバイス（Device）] を選択してから、[ルーティング（Routing）] グループで [設定の表示（View Configuration）]（または [最初のスタティックルートを作成（Create First Static Route）]）をクリックし、デフォルトルートを構成します。

デフォルト ルートは通常、外部インターフェイス以外に存在するアップストリームまたは ISP ルータを指しています。デフォルトの IPv4 ルートは任意の ipv4（0.0.0.0/0）、デフォルトの IPv6 ルートは任意の ipv6（::0/0）です。使用する IP バージョンごとにルートを作成します。外部インターフェイスのアドレスの取得に DHCP を使用する場合、必要なデフォルト ルートをすでに持っていることがあります。

（注） このページで定義したルートは、データ インターフェイス用のみです。管理インターフェイスには影響しません。**[デバイス（Device）] > [システム設定（System Settings）] > [管理インターフェイス（Management Interface）]** で管理ゲートウェイを設定します。

次の例に、IPv4 のデフォルト ルートを示します。この例では、isp ゲートウェイは ISP ゲートウェイの IP アドレスを識別するネットワーク オブジェクトです（アドレスは ISP から取得する必要があります）。[ゲートウェイ（Gateway）] の下部の [新しいネットワークを作成する（Create New Network）] ドロップダウン リストをクリックしてこのオブジェクトを作成することができます。

図 *33* : デフォルトルート

ステップ 5 [ポリシー（Policies）] を選択してネットワークのセキュリティ ポリシーを構成します。

デバイス セットアップ ウィザードは、内部ゾーンと外部ゾーンの間のトラフィック フローを有効にします。また、外部インターフェイスを使用する場合に、全インターフェイスに対するインターフェイス NAT も有効にします。新しいインターフェイスを構成した場合でも、内部ゾーン オブジェクトに追加する場合はそれらにアクセス制御ルールが自動的に適用されます。

ただし、複数の内部インターフェイスがある場合は、内部ゾーンから内部ゾーンへのトラフィック フローを許可するアクセス制御ルールが必要です。他のセキュリティ ゾーンを追加する場合は、それらのゾーンとのトラフィックを許可するルールが必要です。これらは最低限の変更になります。

さらに、組織が必要とする結果を得るために、その他のポリシーを設定して、追加サービスの提供や、NAT およびアクセス ルールを微調整できます。次のポリシーを設定できます。

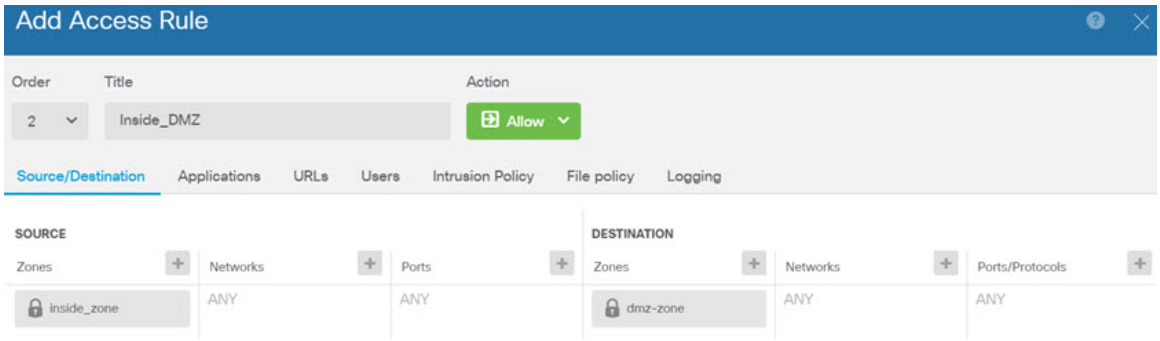
- [SSL復号（SSL Decryption）]：侵入、マルウェアなどについて暗号化された接続（HTTPS など）を検査する場合は、接続を復号化する必要があります。どの接続を復号する必要があるかを判断するにはSSL復号ポリシーを使用します。システムは、検査後に接続を再暗号化します。
- [アイデンティティ（Identity）]：個々のユーザーにネットワーク アクティビティを関連付ける、またはユーザーまたはユーザー グループのメンバーシップに基づいてネットワーク アクセスを制御する場合は、特定のソース IP アドレスに関連付けられているユーザーを判定するためにアイデンティティ ポリシーを使用します。
- [セキュリティインテリジェンス（Security Intelligence）]：ブラックリスト登録済みの IP アドレスまたは URL の接続をただちにドロップするには、セキュリティ インテリジェンス ポリシーを使用します。既知の不正なサイトをブラックリストに登録すれば、アクセス コントロール ポリシーでそれらを考慮する必要がなくなります。Cisco では、セキュリティ インテリジェンスのブラックリストが動的に更新されるように、既知の不正なアドレスや

URL の定期更新フィードを提供しています。フィードを使用すると、ブラックリストの項目を追加または削除するためにポリシーを編集する必要がありません。

- [NAT]（ネットワークアドレス変換）：内部 IP アドレスを外部のルーティング可能なアドレスに変換するために NAT ポリシーを使用します。
- [アクセス制御（Access Control）]：ネットワーク上で許可する接続の決定にアクセス コントロール ポリシーを使用します。セキュリティ ゾーン、IP アドレス、プロトコル、ポート、アプリケーション、URL、ユーザーまたはユーザー グループによってフィルタ処理できます。また、アクセス制御ルールを使用して侵入やファイル（マルウェア）ポリシーを適用します。このポリシーを使用して URL フィルタリングを実装します。
- [侵入（Intrusion）]：侵入ポリシーを使用して、既知の脅威を検査します。アクセス制御ルールを使用して侵入ポリシーを適用しますが、侵入ポリシーを編集して特定の侵入ルールを選択的に有効または無効にできます。

次の例では、アクセス制御ポリシーで内部ゾーンと DMZ ゾーンの間のトラフィックを許可する方法を示します。この例では、[接続の最後で（At End of Connection）] が選択されている場合、[ロギング（Logging）] を除いて他のいずれのタブでもオプションは設定されません。

図 *34*：アクセス コントロール ポリシー



ステップ 6 [デバイス（Device）] を選択してから、[更新（Updates）] グループで [設定の表示（View Configuration）] をクリックし、システムデータベースの更新スケジュールを設定します。

侵入ポリシーを使用している場合は、ルールと VDB のデータベースを定期的な更新を設定します。セキュリティ情報フィードを使用する場合は、それらの更新スケジュールを設定します。一致基準としてセキュリティポリシーで地理位置情報を使用する場合は、そのデータベースの更新スケジュールを設定します。

ステップ 7 メニューの [導入（Deploy）] ボタンをクリックし、[今すぐ導入する（Deploy Now）] ボタン（ ）をクリックして、変更内容をデバイスに展開します。

変更は、それらを展開するまでデバイスで有効になりません。

Threat Defense および FXOS CLI へのアクセス

コマンドラインインターフェイス（CLI）を使用してシステムのセットアップを行い、基本的なシステムのトラブルシューティングを行います。CLI セッションからポリシーを設定することはできません。CLI には、コンソール ポートに接続してアクセスできます。

トラブルシューティングのためにも FXOS CLI にアクセスできます。

（注） または、Threat Defense デバイスの管理インターフェイスに SSH で接続できます。コンソールセッションとは異なり、SSH セッションはデフォルトで Threat Defense CLI になり、**connect fxos** コマンドを使用して FXOS CLI に接続できます。SSH 接続用のインターフェイスを開いている場合、後でデータインターフェイス上のアドレスに接続できます。データインターフェイスへの SSH アクセスはデフォルトで無効になっています。この手順では、デフォルトで FXOS CLI となるコンソールポートアクセスについて説明します。

手順

ステップ 1 CLI にログインするには、管理コンピュータをコンソール ポートに接続します。 Firepower 1000 には、USB A to B シリアル ケーブルが付属しています。お使いのオペレーティングシステムに必要な USB シリアルドライバを必ずインストールしてください（Firepower 1010 ハードウェアガイドを参照）。コンソールポートはデフォルトで FXOS CLI になります。次のシリアル設定を使用します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

FXOS CLI に接続します。ユーザー名 **admin** と、初期セットアップ時に設定したパスワードを使用して CLI にログインします（デフォルトは **Admin123**）。

例：

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

ステップ 2 Threat Defense CLI にアクセスします。

connect ftd

例：

```
firepower# connect ftd
>
```

ログイン後に、CLI で使用可能なコマンドの情報を確認するには、**help** または **?** を入力します。使用方法については、『Cisco Secure Firewall Threat Defense コマンドリファレンス』を参照してください。

ステップ 3 Threat Defense CLI を終了するには、**exit** または **logout** コマンドを入力します。

このコマンドにより、FXOS CLI プロンプトに戻ります。FXOS CLI で使用可能なコマンドについては、**?** を入力してください。

例：

```
> exit
firepower#
```

ハードウェア情報の表示

コマンド ライン インターフェイス（CLI）を使用して、デバイスモデル、ハードウェアバージョン、シリアル番号、シャーシコンポーネント（電源やネットワークモジュールなど）など、ご使用のハードウェアに関する情報を表示します。CLI には、コンソールポートに接続してアクセスできます。Threat Defense および FXOS CLI へのアクセス（127 ページ）を参照してください。

手順

ステップ 1 デバイスのハードウェアモデルを表示するには、**show model** コマンドを使用します。

> show model

例：

```
> show model
Cisco Firepower 1010 Threat Defense
```

ステップ 2 シャーシのシリアル番号を表示するには、**show serial-number** コマンドを使用します。

> show serial-number

例：

```
> show serial-number
JMX1943408S
```

この情報は、**show version system**、**show running-config**、および **show inventory** の出力にも表示されます。

ステップ 3 製品 ID（PID）、バージョン ID（VID）、およびシリアル番号（SN）が割り当てられているネットワークデバイスにインストールされているすべてのシスコ製品に関する情報を表示するには、**show inventory** コマンドを使用します。

> **show inventory**

a) Threat Defense CLI から：

例：

```
> show inventory
Name: "module 0", DESCR: "Firepower 1010 Appliance, Desktop, 8 GE, 1 MGMT"
PID: FPR-1010          , VID: V00     , SN: JMX1943408S
```

b) FXOS CLI から：

例：

```
firepower /chassis # show inventory
Chassis    PID             Vendor            Serial (SN) HW Revision
---------- --------------- ----------------- ----------- -----------
         1 FPR-1010        Cisco Systems, In JMX1943408S 0.3
```

ファイアウォールの電源の切断

システムを適切にシャットダウンすることが重要です。単純に電源プラグを抜いたりすると、重大なファイルシステムの損傷を引き起こすことがあります。バックグラウンドでは常に多数のプロセスが実行されており、電源プラグを抜いたり、電源を切断したりすると、ファイアウォールシステムをグレースフルシャットダウンできないことを覚えておいてください。

Firepower 1010 シャーシには外部電源スイッチはありません。Device Manager を使用してファイアウォールの電源を切断するか、FXOS CLI を使用できます。

Device Manager を使用したファイアウォールの電源の切断

Device Manager を使用してシステムを適切にシャットダウンできます。

手順

ステップ 1 Device Manager を使用してファイアウォールをシャットダウンします。

（注） 6.4 以前の場合は、Device Manager CLI で **shutdown** コマンドを入力します。

a) [デバイス（Device）] をクリックしてから、[システム設定（System Settings）] > [再起動/シャットダウン（Reboot/Shutdown）] リンクをクリックします。
b) [シャットダウン（Shut Down）] をクリックします。

ステップ 2 コンソールからファイアウォールに接続している場合は、ファイアウォールがシャットダウンするときにシステムプロンプトをモニターします。次のプロンプトが表示されます。

```
System is stopped.
It is safe to power off now.

Do you want to reboot instead? [y/N]
```

コンソールから接続していない場合は、約3分間待ってシステムがシャットダウンしたことを確認します。

ステップ 3 必要に応じて電源プラグを抜いてシャーシから物理的に電源を取り外すことができます。

CLI でのデバイスの電源オフ

FXOS CLI を使用すると、システムを安全にシャットダウンし、デバイスの電源をオフにできます。CLI には、コンソールポートに接続してアクセスします。Threat Defense および FXOS CLI へのアクセス （127 ページ）を参照してください。

手順

ステップ 1 FXOS CLI で local-mgmt に接続します。

firepower # **connect local-mgmt**

ステップ 2 **shutdown** コマンドを発行します。

firepower(local-mgmt) # **shutdown**

例：

```
firepower(local-mgmt)# shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
```

ステップ 3 ファイアウォールのシャットダウン時にシステムプロンプトをモニターします。次のプロンプトが表示されます。

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

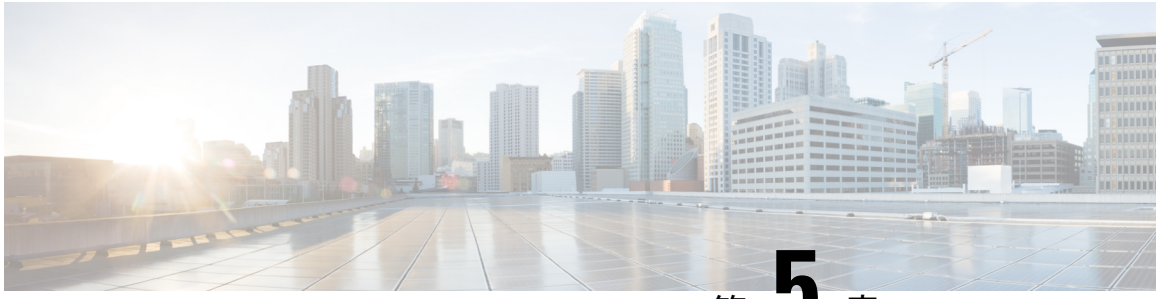
ステップ 4 必要に応じて電源プラグを抜いてシャーシから物理的に電源を取り外すことができます。

次のステップ

Threat Defense の設定を続行するには、「Cisco Firepower ドキュメント一覧」にあるお使いのソフトウェアバージョンのマニュアルを参照してください。

Device Manager の使用に関する情報については、「『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』」を参照してください。

次のステップ



第 5 章

CDO での Threat Defense の展開

この章の対象読者

使用可能なすべてのオペレーティングシステムとマネージャを確認するには、「最適なオペレーティングシステムとマネージャを見つける方法 （1 ページ）」を参照してください。この章は、Cisco Defense Orchestrator（CDO）のクラウド提供型 Secure Firewall Management Center を使用する Threat Defense を対象としています。Device Manager の機能を使用して CDO を使用するには、CDO のマニュアルを参照してください。

（注） クラウド提供型 Management Center は、Threat Defense 7.2 以降をサポートします。以前のバージョンでは、CDO の Device Manager 機能を使用できます。ただし、デバイスマネージャモードは、このモードを使用して Threat Defense をすでに管理している既存の CDO ユーザーのみが使用できます。

各 Threat Defense は、トラフィックを制御、検査、監視、および分析します。CDO は、サービスの管理タスクを実行できる Web インターフェイスを備えた集中管理コンソールを提供し、ローカルネットワークを保護します。

ファイアウォールについて

ハードウェアでは、Threat Defense ソフトウェアまたは ASA ソフトウェアを実行できます。Threat Defense と ASA の間で切り替えを行う際には、デバイスの再イメージ化が必要になります。現在インストールされているものとは異なるソフトウェアバージョンが必要な場合も再イメージ化が必要です。「Cisco ASA および Firepower Threat Defense 再イメージ化ガイド」を参照してください。

ファイアウォールは、Secure Firewall eXtensible オペレーティングシステム（FXOS）と呼ばれる基盤となるオペレーティングシステムを実行します。ファイアウォールは FXOS Secure Firewall Chassis Manager をサポートしていません。トラブルシューティング用として限られた CLI のみがサポートされています。詳細については、Firepower 1000/2100 および Secure Firewall 3100 と Firepower Threat Defense の Cisco FXOS トラブルシューティング ガイドを参照してください。

プライバシー収集ステートメント：ファイアウォールには個人識別情報は不要で、積極的に収集することもありません。ただし、ユーザー名などの設定では、個人識別情報を使用できま

す。この場合、設定作業時やSNMPの使用時に、管理者が個人識別情報を確認できる場合があります。

- CDOによる Threat Defense 管理について （134 ページ）
- エンドツーエンドの手順：ロータッチプロビジョニング （135 ページ）
- エンドツーエンドの手順：オンボーディングウィザード （137 ページ）
- 中央の管理者による事前設定 （139 ページ）
- ロータッチプロビジョニングを使用したファイアウォールの展開 （146 ページ）
- オンボーディングウィザードを使用したファイアウォールの展開 （151 ページ）
- 基本的なセキュリティポリシーの設定 （166 ページ）
- トラブルシューティングとメンテナンス （179 ページ）
- 次のステップ （187 ページ）

CDOによる Threat Defense 管理について

クラウド提供型 Cisco Secure Firewall Management Center

クラウド提供型 Management Center は、オンプレミスの Management Center と同じ機能の多くを提供し、同じルックアンドフィールを備えています。CDO をプライマリマネージャとして使用する場合、オンプレミスの Management Center は分析のみに使用できます。オンプレミスの Management Center は、ポリシーの構成やアップグレードをサポートしていません。

CDO オンボーディング方式

次の方法でデバイスをオンボードできます。

- シリアル番号を使用したロータッチプロビジョニング：
  - 中央の本社の管理者が Threat Defense をリモート支社に送信します。事前設定は必要ありません。実際、ロータッチプロビジョニングは事前設定済みのデバイスでは機能しないため、デバイス上では何も設定しないでください。

（注） 中央管理者は、デバイスをブランチオフィスに送付する前に、Threat Defense のシリアル番号を使用して Threat Defense を CDO で事前に登録できます。

  - 支社の管理者が、Threat Defense をケーブルで接続して電源をオンにします。
  - 中央の管理者が、CDO を使用して Threat Defense の設定を完了します。

すでにデバイスの設定を開始している場合は、Device Manager でシリアル番号を使用して導入準備をすることもできますが、その方法についてはこのガイドでは取り上げていません。

- CLI 登録を使用したオンボーディング ウィザード：事前設定を実行する必要がある場合、またはロータッチプロビジョニングがサポートされていないマネージャインターフェイスを使用している場合は、この手動の方法を使用します。

Threat Defense マネージャ アクセス インターフェイス

マネージャアクセスには、管理インターフェイスまたは外部インターフェイスを使用できます。ただし、このガイドでは、外部インターフェイスアクセスについて説明します。ロータッチプロビジョニングでは、外部インターフェイスのみがサポートされます。

管理インターフェイスは、Threat Defense データインターフェイスとは別に設定される特別なインターフェイスであり、独自のネットワーク設定があります。データインターフェイスでマネージャアクセスを有効にした場合でも、管理インターフェイスのネットワーク設定が使用されます。すべての管理トラフィックは、引き続き管理インターフェイスを発信元または宛先とします。データインターフェイスでマネージャアクセスを有効にすると、Threat Defense はバックプレーンを介して管理インターフェイスに着信管理トラフィックを転送します。発信管理トラフィックの場合、管理インターフェイスはバックプレーンを介してデータインターフェイスにトラフィックを転送します。

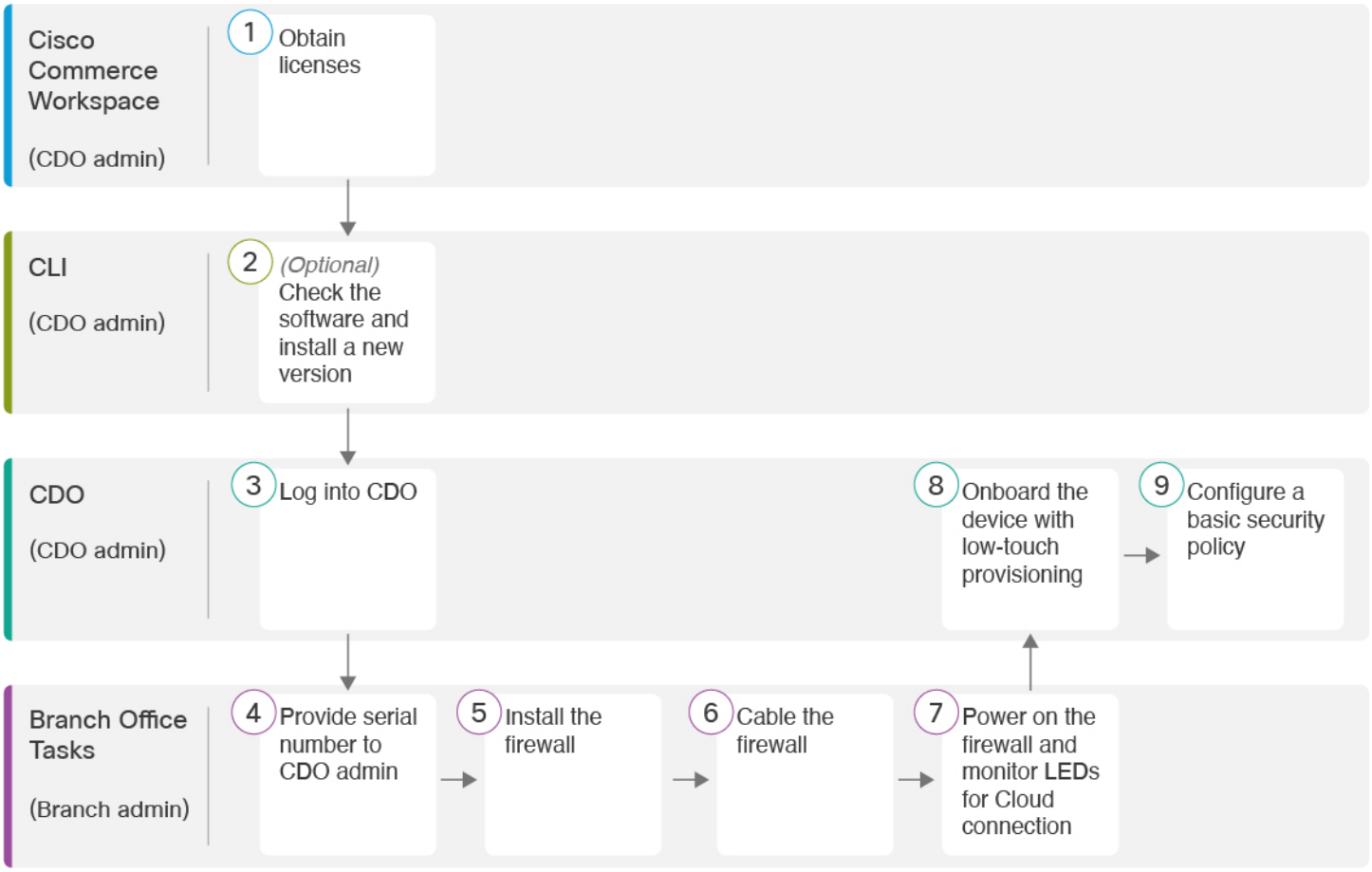
データインターフェイスからのマネージャアクセスには、次の制限があります。

- マネージャアクセスを有効にできるのは、1 つの物理的なデータインターフェイスのみです。サブインターフェイスと EtherChannel は使用できません。冗長性を目的として、Management Center の単一のセカンダリインターフェイスでマネージャアクセスを有効にすることもできます。
- このインターフェイスは管理専用にできません。
- ルーテッドインターフェイスを使用するルーテッドファイアウォールモードのみです。
- PPPoE はサポートされていません。ISP で PPPoE が必要な場合は、PPPoE をサポートするルータを Threat Defense と WAN モデムの間に配置する必要があります。
- インターフェイスを配置する必要があるのはグローバル VRF のみです。
- SSH はデータインターフェイスではデフォルトで有効になっていないため、後で Management Center を使用して SSH を有効にする必要があります。また、管理インターフェイス ゲートウェイがデータインターフェイスに変更されるため、**configure network static-routes** コマンドを使用して管理インターフェイス用の静的ルートを追加しない限り、リモートネットワークから管理インターフェイスに SSH 接続することはできません。

エンドツーエンドの手順：ロータッチプロビジョニング

ロータッチプロビジョニングにより、CDO を使用して Threat Defense を展開するには、次のタスクを参照してください。

図 *35 :* エンドツーエンドの手順：ロータッチプロビジョニング



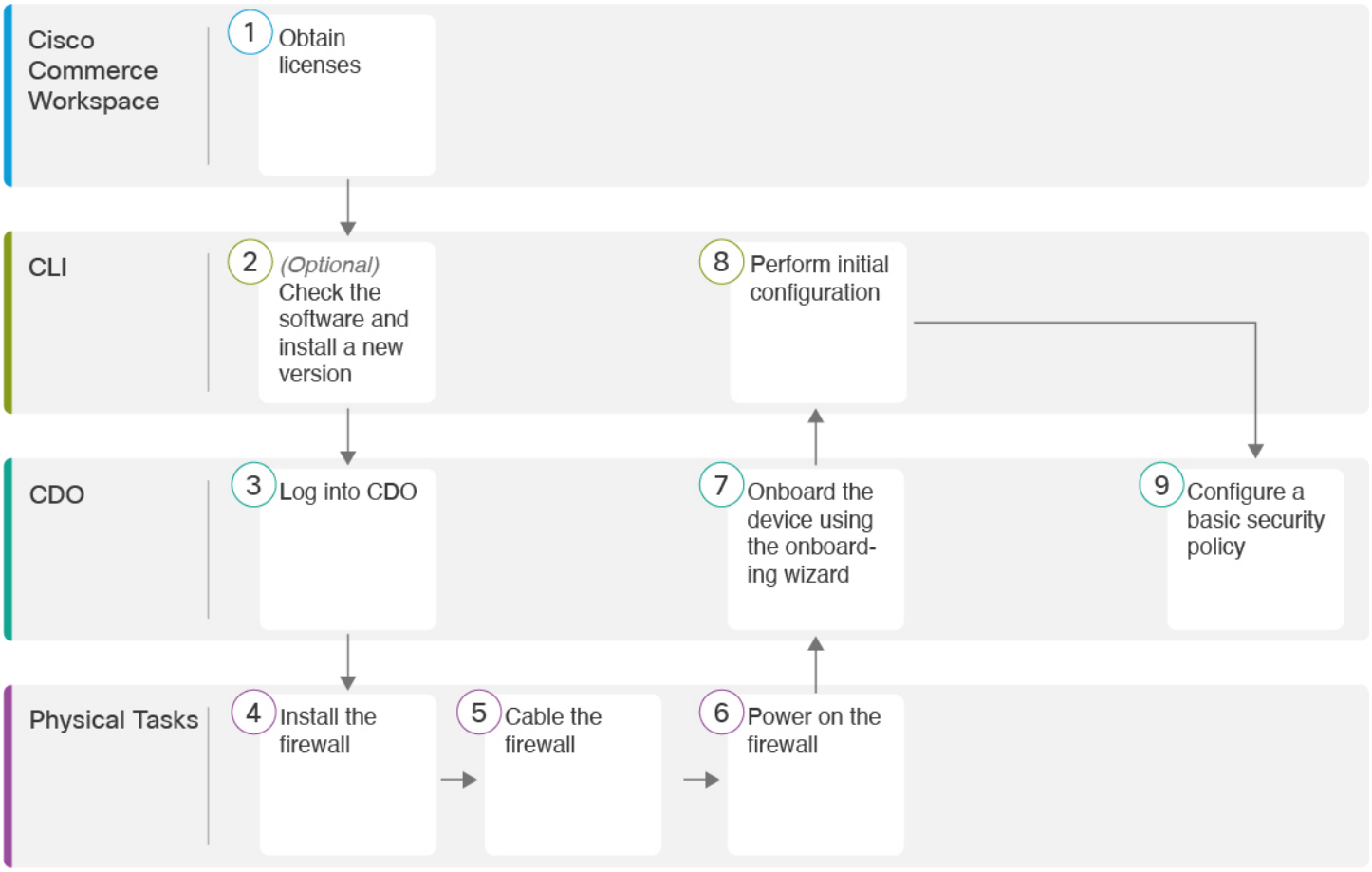
1	Cisco Commerce Workspace （CDO 管理者）	ライセンスを取得する （139 ページ）。
2	CLI （CDO 管理者）	（任意）ソフトウェアの確認と新しいバージョンのインストール（140 ページ）。
3	CDO （CDO 管理者）	CDO へのログイン （142 ページ）。
4	支社のタスク （支社の管理者）	中央の管理者に対するファイアウォールのシリアル番号の提供（146 ページ）。
5	支社のタスク （支社の管理者）	ファイアウォールをインストールします。ハードウェア設置ガイドを参照してください。

6	支社のタスク （支社の管理者）	ファイアウォールのケーブル接続 （147 ページ）。
7	支社のタスク （支社の管理者）	ファイアウォールの電源の投入 （149 ページ）。
8	CDO （CDO 管理者）	ロータッチプロビジョニングによるデバイスの導入準備 （150 ページ）。
9	CDO （CDO 管理者）	基本的なセキュリティポリシーの設定 （166 ページ）。

エンドツーエンドの手順：オンボーディングウィザード

オンボーディングウィザードを使用して Threat Defense を CDO にオンボードするには、次のタスクを参照してください。

図 *36 :* エンドツーエンドの手順：オンボーディングウィザード



1	Cisco Commerce Workspace	ライセンスを取得する （139 ページ）。
2	CLI	（任意）ソフトウェアの確認と新しいバージョンのインストール （140 ページ）。
3	CDO	CDO へのログイン （142 ページ）。
4	物理的なタスク	ファイアウォールをインストールします。ハードウェア設置ガイドを参照してください。
5	物理的なタスク	ファイアウォールのケーブル接続 （151 ページ）。
6	物理的なタスク	ファイアウォールの電源投入 （153 ページ）。
7	CDO	オンボーディングウィザードを使用したデバイスのオンボーディング （154 ページ）。

8	CLI または Device Manager	• CLI を使用した初期設定の実行 （155 ページ）。 • Device Manager を使用した初期設定の実行 （160 ページ）。
9	CDO	基本的なセキュリティポリシーの設定 （166 ページ）。

中央の管理者による事前設定

このセクションでは、ファイアウォールの機能ライセンスを取得する方法、展開する前に新しいソフトウェアバージョンをインストールする方法、CDO にログインする方法について説明します。

ライセンスを取得する

すべてのライセンスは、CDO によって Threat Defense に提供されます。オプションで、次の機能ライセンスを購入できます。

- **IPS**：セキュリティインテリジェンスと次世代 IPS
- **マルウェア防御**：マルウェア防御
- **URL**：URL フィルタリング
- **Cisco Secure Client**：Secure Client Advantage、Secure Client Premier、または Secure Client VPN のみ
- キャリア（Diameter、GTP/GPRS、M3UA、SCTP）

シスコライセンスの概要については詳しくは、cisco.com/go/licensingguide を参照してください。

始める前に

- Smart Software Manager にマスターアカウントを持ちます。

  まだアカウントをお持ちでない場合は、リンクをクリックして新しいアカウントを設定してください。Smart Software Manager では、組織のマスター アカウントを作成できます。

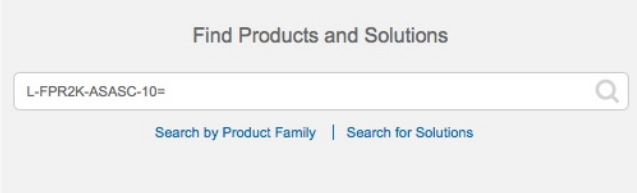
- （輸出コンプライアンスフラグを使用して有効化される）機能を使用するには、ご使用のスマート ソフトウェア ライセンシング アカウントで強力な暗号化（3DES/AES）ライセンスを使用できる必要があります。

手順

ステップ 1 お使いのスマート ライセンシング アカウントに、必要なライセンスが含まれていることを確認してください。

ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマート ソフトウェア ライセンシング アカウントにリンクされています。ただし、主導でライセンスを追加する必要がある場合は、Cisco Commerce Workspace で [製品とソリューションの検索（Find Products and Solutions）] 検索フィールドを使用します。次のライセンス PID を検索します。

図 *37:* ライセンス検索



（注） PID が見つからない場合は、注文に手動で PID を追加できます。

- IPS、マルウェア防御、および URL ライセンスの組み合わせ：
  - L-FPR1010T-TMC=

  上記の PID のいずれかを注文に追加すると、次のいずれかの PID に対応する期間ベースのサブスクリプションを選択できます。
  - L-FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y
  - L-FPR1010T-TMC-5Y
- Cisco Secure Client：『Cisco Secure Client 発注ガイド』を参照してください。
- キャリアライセンス：
  -

ステップ 2 Smart Software Manager に CDO を登録します（まだ登録していない場合）。

登録を行うには、Smart Software Manager で登録トークンを生成する必要があります。詳しい手順については、CDO のマニュアルを参照してください。

（任意）ソフトウェアの確認と新しいバージョンのインストール

ソフトウェアのバージョンを確認し、必要に応じて別のバージョンをインストールするには、次の手順を実行します。ファイアウォールを設定する前に対象バージョンをインストールする

ことをお勧めします。別の方法として、稼働後にアップグレードを実行することもできますが、設定を保持するアップグレードでは、この手順を使用するよりも時間がかかる場合があります。

実行するバージョン

ソフトウェア ダウンロード ページのリリース番号の横にある、金色の星が付いている Gold Star リリースを実行することをお勧めします。https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html に記載されているリリース戦略も参照してください。たとえば、この速報では、（最新機能を含む）短期的なリリース番号、長期的なリリース番号（より長期間のメンテナンスリリースとパッチ）、または非常に長期的なリリース番号（政府認定を受けるための最長期間のメンテナンスリリースとパッチ）について説明しています。

手順

ステップ 1 ファイアウォールの電源をオンにし、コンソールポートに接続します。詳細については、ファイアウォールの電源投入 （153 ページ）およびThreat Defense および FXOS CLI へのアクセス （179 ページ）を参照してください。

admin ユーザとデフォルトパスワードの **Admin123** を使用してログインします。

FXOS CLI に接続します。初めてログインしたとき、パスワードを変更するよう求められます。このパスワードは、SSH の Threat Defense ログインにも使用されます。

（注） パスワードがすでに変更されていて、パスワードがわからない場合は、初期設定へのリセットを実行して、パスワードをデフォルトにリセットする必要があります。初期設定へのリセット手順については、『FXOS troubleshooting guide 』を参照してください。

例：

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

ステップ 2 FXOS CLI で、実行中のバージョンを表示します。

scope ssa

show app-instance

例：

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name      Slot ID     Admin State      Operational State     Running Version
Startup Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd                   1           Enabled          Online                7.2.0.65
7.2.0.65        Not Applicable
```

ステップ 3 新しいバージョンをインストールする場合は、次の手順を実行します。

a) 管理インターフェイスに静的 IP アドレスを設定する必要がある場合は、「CLI を使用した初期設定の実行 （155 ページ）」を参照してください。デフォルトでは、管理インターフェイスは DHCP を使用します。

管理インターフェイスからアクセスできるサーバーから新しいイメージをダウンロードする必要があります。

b) FXOS のトラブルシューティング ガイドに記載されている再イメージ化の手順を実行します。

CDO へのログイン

CDOは、Cisco Secure Sign-On をアイデンティティプロバイダーとして使用し、Duo Security を多要素認証（MFA）に使用します。CDO には MFA が必要です。MFA は、ユーザーアイデンティティを保護するためのセキュリティを強化します。MFA の一種である二要素認証では、CDO にログインするユーザーの ID を確認するために、2 つのコンポーネントまたは要素が必要です。

最初の要素はユーザー名とパスワードで、2 番目の要素は Duo Security からオンデマンドで生成されるワンタイムパスワード（OTP）です。

Cisco Secure Sign-On クレデンシャルを確立したら、Cisco Secure Sign-On ダッシュボードから CDO にログインできます。Cisco Secure Sign-On ダッシュボードから、サポートされている他のシスコ製品にログインすることもできます。

- Cisco Secure Sign-On アカウントをお持ちの場合は、Cisco Secure Sign-On を使用した CDO へのログイン （145 ページ）に進みます。
- Cisco Secure Sign-On アカウントがない場合は、新しい Cisco Secure Sign-On アカウントの作成 （142 ページ）に進んでください。

新しい Cisco Secure Sign-On アカウントの作成

最初のサインオンワークフローは 4 段階のプロセスです。4 段階すべてを完了する必要があります。

始める前に

- **DUO Security のインストール**：Duo Security アプリケーションを携帯電話にインストールすることをお勧めします。Duo のインストールについてご質問がある場合は、『Duo Guide to Two Factor Authentication：Enrollment Guide』を参照してください。
- **時刻の同期**：モバイルデバイスを使用してワンタイムパスワードを生成します。OTP は時間ベースであるため、デバイスのクロックがリアルタイムと同期していることが重要です。デバイスのクロックが正しい時刻に設定されていることを確認します。
- Firefox または Chrome の最新バージョンを使用します。

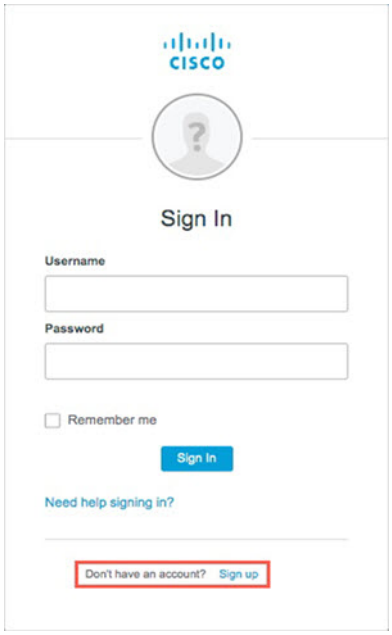
手順

ステップ 1 **新しい Cisco Secure Sign-On アカウントにサインアップします。**

a) https://sign-on.security.cisco.com にアクセスします。

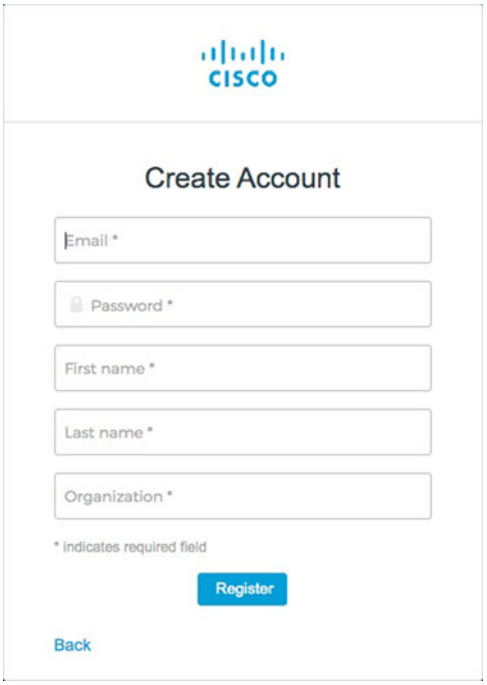
b) [サインイン（Sign In）] 画面の下部にある [サインアップ（Sign up）] をクリックします。

図 *38 : Cisco SSO* へのサインアップ



c) [アカウントの作成（Create Account）] ダイアログのフィールドに入力し、[登録（Register）] をクリックします。

図 *39* : アカウントの作成（***Create Account***）



ヒント　CDOへのログインに使用する予定の電子メールアドレスを入力し、会社を表す組織名を追加します。

d) [登録（Register）]をクリックすると、登録したアドレスに確認メールが送信されます。電子メールを開き、[アカウントの有効化（Activate Account）] をクリックします。

ステップ 2　Duo を使用して多要素認証をセットアップします。

a) [多要素認証の設定（Set up multi-factor authentication）] 画面で、[設定（Configure）] をクリックします。

b) [セットアップの開始（Start setup）]をクリックし、プロンプトに従ってデバイスを選択して、そのデバイスとアカウントのペアリングを確認します。

詳細については、『Duo Guide to Two Factor Authentication：Enrollment Guide』を参照してください。デバイスにDuoアプリケーションがすでにインストールされている場合は、このアカウントのアクティベーションコードが送信されます。Duo は 1 台のデバイスで複数のアカウントをサポートします。

c) ウィザードの最後で、[ログインを続行する（Continue to Login）] をクリックします。

d) 二要素認証を使用して Cisco Secure Sign-On にログインします。

ステップ 3　（任意）追加のオーセンティケータとして Google オーセンティケータを設定します。

a) Googleオーセンティケータとペアリングするモバイルデバイスを選択し、[次へ（Next）] をクリックします。

b) セットアップウィザードのプロンプトに従って、Google オーセンティケータをセットアップします。

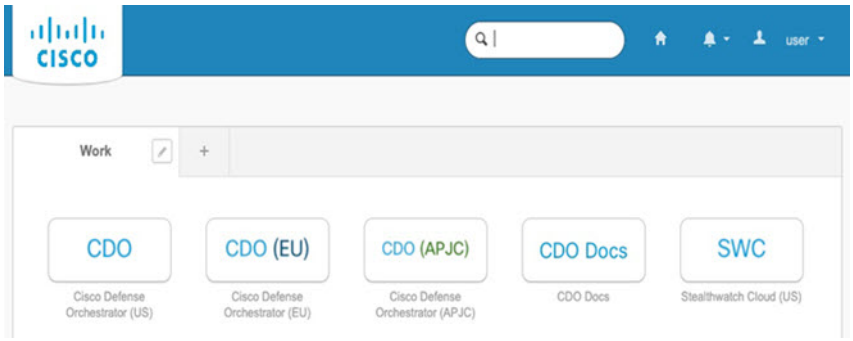
ステップ 4 **Cisco Secure Sign-On アカウントのアカウントリカバリのオプションを設定します。**

a) 「パスワードを忘れた場合（forgot password）」の質問と回答を選択します。
b) SMS を使用してアカウントをリセットするための予備の電話番号を選択します。
c) セキュリティイメージを選択します。
d) [マイアカウントの作成（Create My Account）] をクリックします。

これで、Cisco Security Sign-On ダッシュボードに CDO アプリケーションのタイルが表示されます。他のアプリケーションタイルも表示される場合があります。

ヒント ダッシュボード上でタイルをドラッグして並べ替えたり、タブを作成してタイルをグループ化したり、タブの名前を変更したりできます。

図 *40 : Cisco SSO* ダッシュボード



Cisco Secure Sign-On を使用した CDO へのログイン

CDO にログインし、デバイスのオンボードと管理を行います。

始める前に

Cisco Defense Orchestrator（CDO）は、Cisco Secure Sign-On をアイデンティティ プロバイダーとして使用し、多要素認証（MFA）に Duo Security を使用します。

- CDO にログインするには、まず Cisco Secure Sign-On でアカウントを作成し、Duo を使用して MFA を設定する必要があります。新しい Cisco Secure Sign-On アカウントの作成（142 ページ）を参照してください。
- Firefox または Chrome の最新バージョンを使用します。

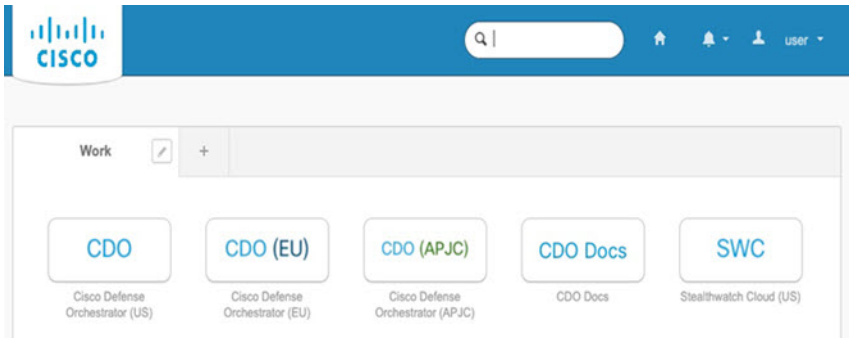
手順

ステップ 1 Web ブラウザで、https://sign-on.security.cisco.com/を開きます。
ステップ 2 [ユーザー名（Username）] と [パスワード（Password）] に入力します。
ステップ 3 [ログイン（Log in）] をクリックします。

ステップ 4 Duo Security を使用して別の認証要素を受け取り、ログインを確認します。システムによってログインが確認され、Cisco Secure Sign-On ダッシュボードが表示されます。

ステップ 5 Cisco Secure Sign-on ダッシュボードで適切な CDO タイルをクリックします。**CDO** タイルをクリックすると https://defenseorchestrator.com に移動し、**CDO（EU）**タイルをクリックすると https://defenseorchestrator.eu に移動します。また、**CDO（APJC）**タイルをクリックすると https://www.apj.cdo.cisco.com に移動します。

図 *41 : Cisco SSO* ダッシュボード



ステップ 6 両方のオーセンティケータを設定している場合は、オーセンティケータのロゴをクリックして [Duo Security] か [Google Authenticator] を選択します。

- 既存のテナントにすでにユーザーレコードがある場合は、そのテナントにログインします。
- すでに複数のテナントにユーザーレコードがある場合は、接続先の CDO テナントを選択できます。
- 既存のテナントにユーザーレコードがない場合は、CDO の詳細を確認するか、またはトライアルアカウントを要求できます。

ロータッチプロビジョニングを使用したファイアウォールの展開

中央の本社から Threat Defense を受け取ったら、外部インターフェイスからインターネットにアクセスできるように、ファイアウォールにケーブルを接続して電源をオンにするだけです。そうすると、中央の管理者は設定を完了できます。

中央の管理者に対するファイアウォールのシリアル番号の提供

ファイアウォールをラックに設置するか配送ボックスを捨てる前に、中央の管理者と連携できるようにシリアル番号を記録しておきます。

手順

ステップ 1 シャーシとシャーシコンポーネントを開梱します。

ケーブルを接続する前、またはファイアウォールの電源を入れる前に、ファイアウォールとパッケージのインベントリを確認します。シャーシのレイアウト、コンポーネント、および LED についても理解しておく必要があります。

ステップ 2 ファイアウォールのシリアル番号を記録します。

ファイアウォールのシリアル番号は、配送ボックスに記載されています。また、ファイアウォールシャーシの底面にあるステッカーにも記載されています。

ステップ 3 ファイアウォールのシリアル番号を IT 部門/中央の本社の CDO ネットワーク管理者に送信します。

ネットワーク管理者は、ロータッチプロビジョニングを容易にし、ファイアウォールに接続してリモートで設定するためにファイアウォールのシリアル番号が必要になります。

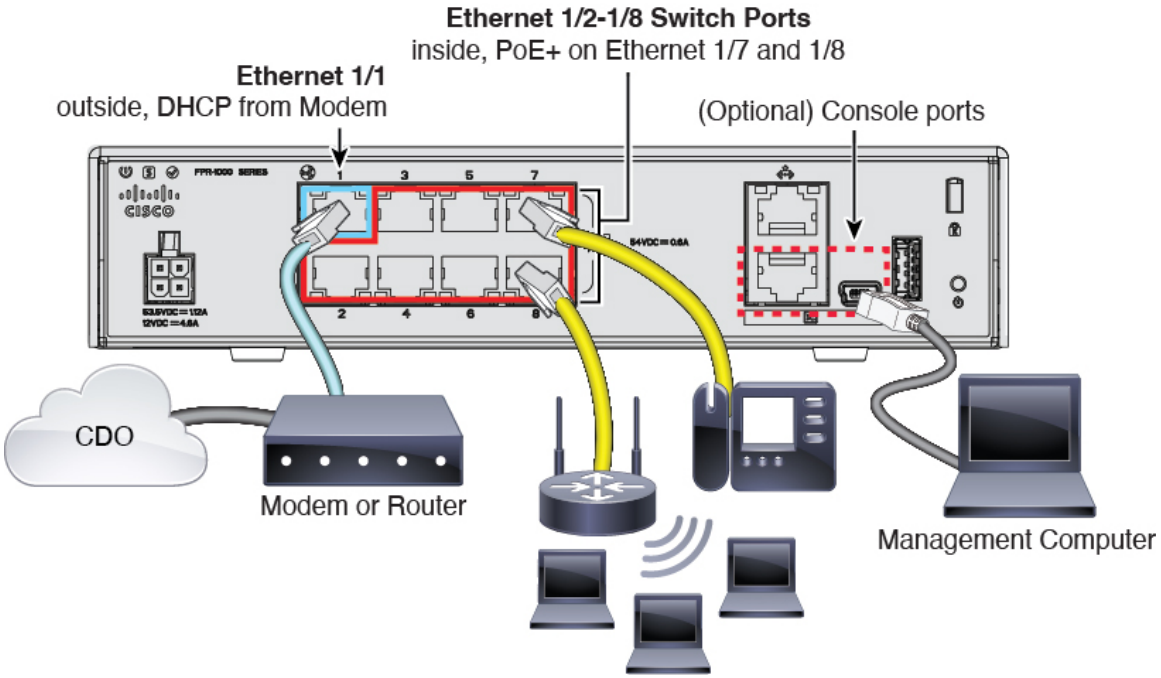
CDO 管理者と連絡を取って、オンボーディングのタイムラインを策定します。

ファイアウォールのケーブル接続

このトピックでは、CDO が管理できるように Firepower 1010 をネットワークに接続する方法について説明します。

支社でファイアウォールを受け取ってネットワークに接続する場合は、このビデオをご覧ください。ビデオでは、ファイアウォールとファイアウォールのステータスを示すファイアウォール上の LED シーケンスについて説明しています。必要に応じて、IT 部門と一緒に LED を見るだけでファイアウォールのステータスを確認できます。

図 *42 : Firepower 1010* のケーブル配線



ロータッチプロビジョニングは、イーサネット 1/1（外部）での CDO への接続をサポートしています。

（注） イーサネット 1/2 ～ 1/8 はハードウェアスイッチポートとして設定されています。PoE+ はイーサネット 1/7 および 1/8 でも使用できます。

（注） PoE は Firepower 1010E ではサポートされていません。

手順

ステップ 1 シャーシを取り付けます。ハードウェア設置ガイドを参照してください。

ステップ 2 イーサネット 1/1 インターフェイスからワイドエリアネットワーク（WAN）モデムにネットワークケーブルを接続します。WAN モデムは、支社とインターネットを接続する機器であり、ファイアウォールからインターネットへのルートにもなります。

ステップ 3 内部エンドポイントをスイッチポート Ethernet1/2 ー 1/8 にケーブルで接続します。

イーサネット 1/7 および 1/8 は PoE+ ポートです。

ステップ 4 （任意） 管理コンピュータをコンソールポートに接続します。

支社では、日常的に使用するためのコンソール接続は必要ありません。ただし、トラブルシューティングに必要な場合があります。

ファイアウォールの電源の投入

システムの電源は電源コードで制御されます。電源ボタンはありません。

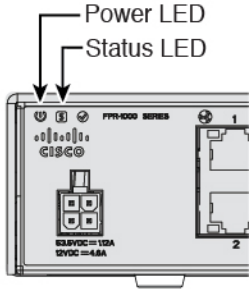
（注） Threat Defense を初めて起動するときは、初期化に約 15 ～ 30 分かかります。

手順

ステップ 1 電源コードをデバイスに接続し、電源コンセントに接続します。

電源コードを差し込むと電源が自動的に入ります。

ステップ 2 デバイスの背面または上部にある電源 LED を確認します。緑色に点灯している場合は、デバイスの電源が入っています。



ステップ 3 デバイスの背面または上部にあるステータス LED を確認します。緑色に点灯している場合は、電源投入時診断に合格しています。

ステップ 4 デバイスの背面または上部にあるステータス LED を確認します。デバイスが正常に起動していると、ステータス LED が緑色にすばやく点滅します。

問題がある場合は、ステータス LED がオレンジ色にすばやく点滅します。この場合は、IT 部門に連絡してください。

ステップ 5 デバイスの背面または上部のステータス LED を確認します。デバイスが Cisco Cloud に接続すると、ステータス LED が緑色にゆっくりと点滅します。

問題がある場合は、ステータス LED がオレンジ色と緑色に点滅し、デバイスが Cisco Cloud に到達しなかったことになります。この場合は、ネットワークケーブルがイーサネット 1/1 インターフェイスと WAN モデムに接続されていることを確認します。ネットワークケーブルを調

整した後、10 分ほど経過してもデバイスが Cisco Cloud に到達しない場合は、IT 部門に連絡してください。

次のタスク

- IT 部門と連絡を取って、導入準備のタイムラインとアクティビティを確認します。本社の CDO 管理者とともにコミュニケーション計画を導入する必要があります。
- このタスクを完了すると、CDO 管理者はデバイスをリモートから設定および管理できるようになります。これで完了です。

ロータッチプロビジョニングによるデバイスの導入準備

ロータッチプロビジョニングとデバイスのシリアル番号を使用した Threat Defense の導入準備

手順

ステップ 1 CDO のナビゲーションウィンドウで [インベントリ（Inventory）] をクリックし、青色のプラスボタン（+）をクリックしてデバイスを [オンボード（Onboard）] します。

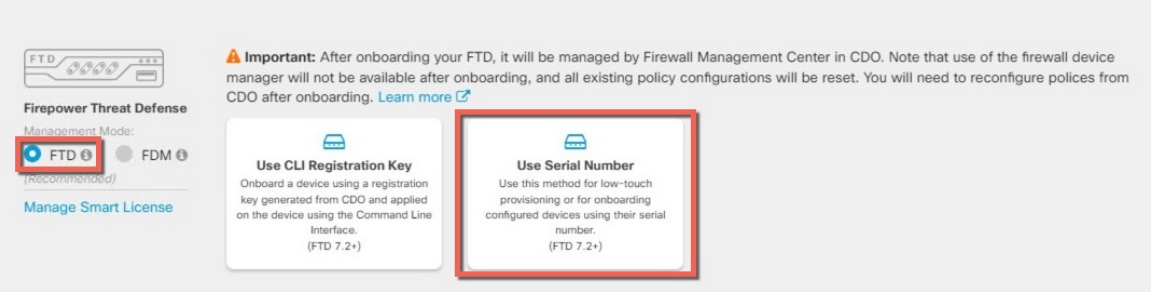
ステップ 2 [FTD] タイルを選択します。

ステップ 3 [管理モード] で、[FTD] が選択されていることを確認します。

管理モードとして [FTD] を選択した後はいつでも、[スマートライセンスの管理（Manage Smart License）] をクリックして、デバイスで使用可能なスマートライセンスを登録したり、既存のスマートライセンスを変更したりできます。使用可能なライセンスについては、ライセンスを取得する （139 ページ） を参照してください。

ステップ 4 オンボーディング方法として [シリアル番号を使用（Use Serial Number）] を選択します。

図 *43 :* シリアル番号を使用



ステップ 5 [接続（Connection）] 領域で、[デバイスのシリアル番号（Device Serial Number）] と [デバイス名（Device Serial Number）] を入力し、[次へ（Next）] をクリックします。

ステップ 6 [パスワードのリセット（Password Reset）] 領域で、[はい、この新しいデバイスはログインもマネージャの設定もされていません（Yes, this new device has never been logged into or configured for a manager）] オプションボタンをクリックし、[次へ（Next）] をクリックします。

ステップ 7 [ポリシー割り当て（Policy Assignment）] については、ドロップダウンメニューを使用して、デバイスのアクセス コントロール ポリシーを選択します。ポリシーが設定されていない場合は、[デフォルトのアクセスコントロールポリシー（Default Access Control Policy）] を選択します。

ステップ 8 [サブスクリプションライセンス（Subscription License）] については、有効にする各機能ライセンスをチェックします。[次へ（Next）] をクリックします。

ステップ 9 （任意）[インベントリ（Inventory）] ページの並べ替えとフィルタ処理に役立つよう、デバイスにラベルを追加します。ラベルを入力し、青いプラスボタン（ ）を選択します。ラベルは、CDO への導入準備後にデバイスに適用されます。

次のタスク

[インベントリ] ページから、導入準備したばかりのデバイスを選択し、右側にある [管理] ペインに一覧表示されているオプションのいずれかを選択します。

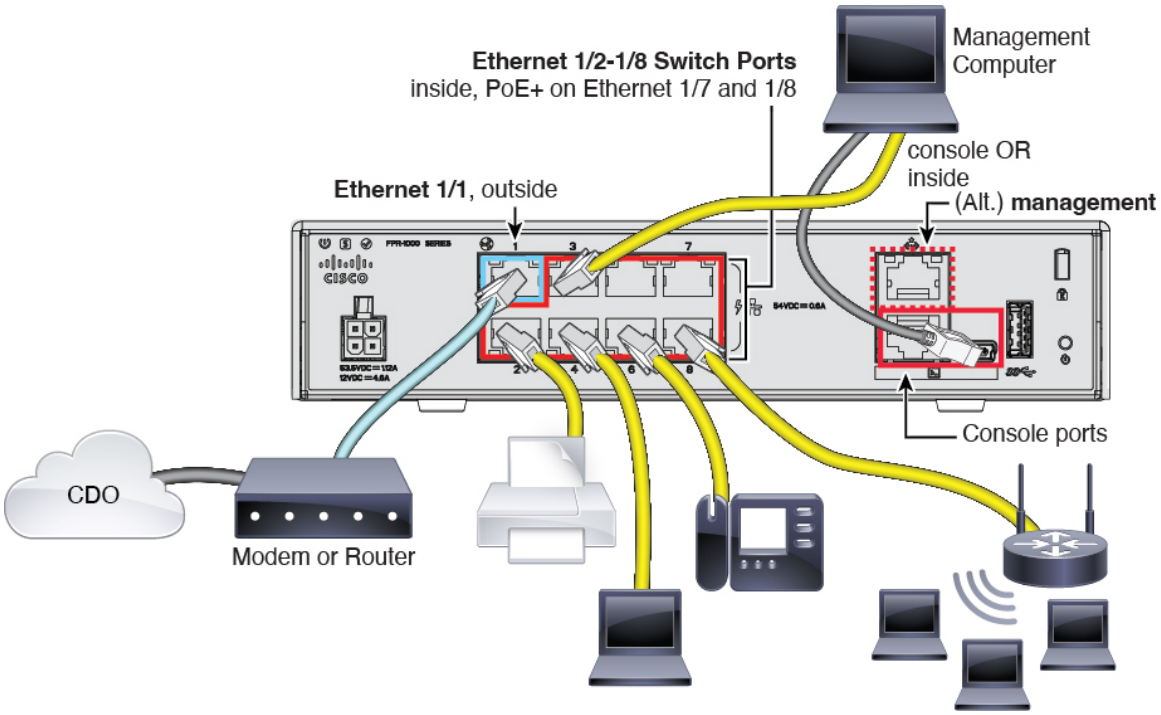
オンボーディングウィザードを使用したファイアウォールの展開

このセクションでは、CDO のオンボーディングウィザードを使用してオンボーディング用にファイアウォールを設定する方法について説明します。

ファイアウォールのケーブル接続

このトピックでは、CDO が管理できるように Firepower 1010 をネットワークに接続する方法について説明します。

図 *44 : Firepower 1010* のケーブル配線



初期セットアップ時にマネージャアクセス用に設定したインターフェイスに応じて、外部インターフェイスまたは管理インターフェイスで CDO に接続できます。このガイドでは、外部インターフェイスを示しています。

（注） イーサネット 1/2 ～ 1/8 はハードウェアスイッチポートとして設定されています。PoE+ はイーサネット 1/7 および 1/8 でも使用できます。

（注） PoE は Firepower 1010E ではサポートされていません。

手順

ステップ 1 シャーシを取り付けます。ハードウェア設置ガイドを参照してください。

ステップ 2 外部インターフェイス（Ethernet 1/1）を外部ルータに接続します。

あるいは、マネージャアクセスには管理インターフェイスを使用できます。ただし、このガイドでは主に外部インターフェイスアクセスについて説明します。これは、リモート支社で最も用いられる可能性が高いシナリオであるためです。

ステップ 3 内部エンドポイントをスイッチポート Ethernet1/2 ー 1/8 にケーブルで接続します。

イーサネット 1/7 および 1/8 は PoE+ ポートです。

ステップ 4 管理コンピュータをコンソールポートまたは内部インターフェイスに接続します。

CLI を使用して初期セットアップを実行する場合は、コンソールポートに接続する必要があります。コンソールポートは、トラブルシューティングの目的でも必要になる場合があります。Device Manager を使用して初期セットアップを実行する場合は、内部インターフェイスに接続します。

ファイアウォールの電源投入

システムの電源は電源コードで制御されます。電源ボタンはありません。

（注） Threat Defense を初めて起動するときは、初期化に約 15 ～ 30 分かかります。

始める前に

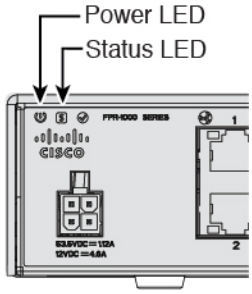
デバイスに対して信頼性の高い電力を供給することが重要です（たとえば、無停電電源装置（UPS）を使用）。最初のシャットダウンを行わないで電力が失われると、重大なファイルシステムの損傷を引き起こす可能性があります。バックグラウンドでは常に多数のプロセスが実行されていて、電力が失われると、システムをグレースフルシャットダウンできません。

手順

ステップ 1 電源コードをデバイスに接続し、電源コンセントに接続します。

電源コードを差し込むと電源が自動的に入ります。

ステップ 2 デバイスの背面または上部にある電源 LED を確認します。緑色に点灯している場合は、デバイスの電源が入っています。



ステップ 3 デバイスの背面または上部にあるステータス LED を確認します。緑色に点灯している場合は、電源投入時診断に合格しています。

オンボーディングウィザードを使用したデバイスのオンボーディング

CLI 登録キーを使用し、CDO のオンボーディングウィザードを使用して Threat Defense をオンボードします。

手順

ステップ 1 CDO のナビゲーションウィンドウで [インベントリ（Inventory）] をクリックし、青色のプラスボタン（+）をクリックしてデバイスを [オンボード（Onboard）] します。

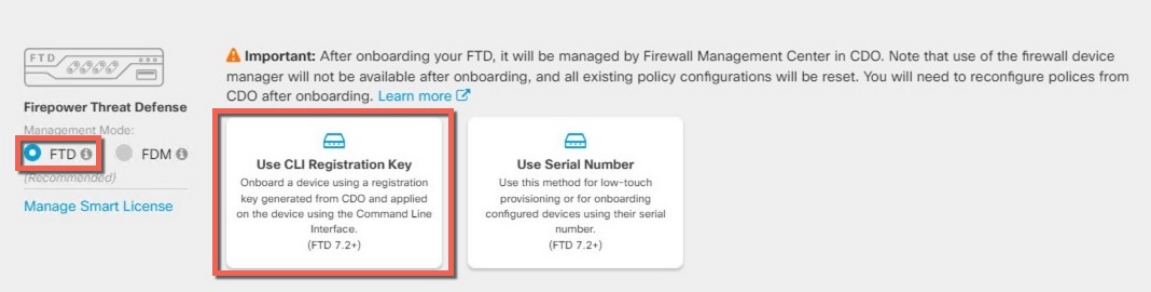
ステップ 2 [FTD] タイルを選択します。

ステップ 3 [管理モード] で、[FTD] が選択されていることを確認します。

管理モードとして [FTD] を選択した後はいつでも、[スマートライセンスの管理（Manage Smart License）] をクリックして、デバイスで使用可能なスマートライセンスを登録したり、既存のスマートライセンスを変更したりできます。使用可能なライセンスについては、ライセンスを取得する （139 ページ） を参照してください。

ステップ 4 オンボーディング方法として [CLI登録キーを使用（Use CLI Registration Key）] を選択します。

図 *45 : CLI* 登録キーを使用



ステップ 5 [デバイス名（Device Name）] を入力して、[次へ（Next）] をクリックします。

ステップ 6 [ポリシー割り当て（Policy Assignment）] については、ドロップダウンメニューを使用して、デバイスのアクセス コントロール ポリシーを選択します。ポリシーが設定されていない場合は、[デフォルトのアクセスコントロールポリシー（Default Access Control Policy）] を選択します。

ステップ 7 [サブスクリプションライセンス（Subscription License）] については、[物理FTDデバイス（Physical FTD Device）] オプションボタンをクリックして、有効にする各機能ライセンスをチェックします。[次へ（Next）] をクリックします。

ステップ 8 [CLI登録キー（CLI Registration Key）] については、CDO は、登録キーとその他のパラメータを使用してコマンドを生成します。このコマンドをコピーして、Threat Defense の初期構成で使用する必要があります。

configure manager add *cdo_hostname registration_key nat_id display_name*

CLI での、または Device Manager を使用した初期設定の完了

- CLI を使用した初期設定の実行 （155 ページ）：起動スクリプトを完了した後、FTD CLI でこのコマンドをコピーします。
- Device Manager を使用した初期設定の実行 （160 ページ）：コマンドの *cdo_hostname*、*registration_key*、*nat_id* の部分を [Management Center/CDOのホスト名/IPアドレス（Management Center/CDO Hostname/IP Address）]、[Management Center/CDOの登録キー（Management Center/CDO Registration Key）]、[NAT ID] フィールドにコピーします。

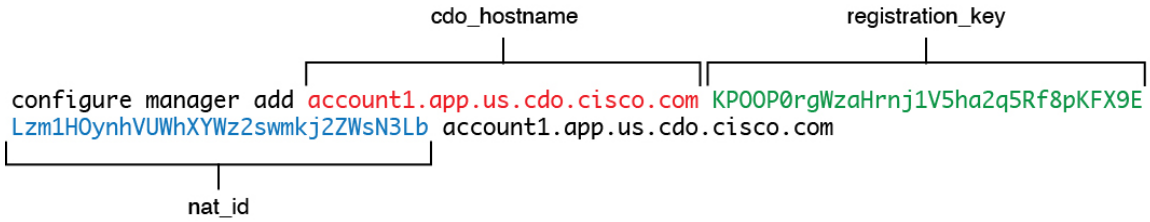
例：

CLI セットアップのサンプルコマンド：

```
configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
```

GUI セットアップのサンプル コマンド コンポーネント：

図 *46 : configure manager add* コマンドコンポーネント



ステップ 9 オンボーディングウィザードで [次へ（Next）] をクリックして、デバイスの登録を開始します。

ステップ 10 （任意）[インベントリ（Inventory）]ページの並べ替えとフィルタ処理に役立つよう、デバイスにラベルを追加します。ラベルを入力し、青いプラスボタン（+）を選択します。ラベルは、CDO への導入準備後にデバイスに適用されます。

次のタスク

[インベントリ]ページから、導入準備したばかりのデバイスを選択し、右側にある [管理] ペインに一覧表示されているオプションのいずれかを選択します。

初期設定

CLI または Device Manager を使用して、Threat Defense の初期設定を実行します。

CLI を使用した初期設定の実行

Threat Defense CLI に接続して初期設定を行います。CLI を使用して初期セットアップを実行すると、管理インターフェイスおよびマネージャ アクセス インターフェイスの設定のみが保持されます。Device Manager を使用して初期セットアップを実行すると、管理インターフェイスおよびマネージャ アクセス インターフェイスの設定に加えて、管理のために CDO に切り替

えたときに、Device Manager で完了したすべてのインターフェイス構成が保持されます。アクセス コントロール ポリシーなどの他のデフォルト設定は保持されないことに注意してください。

手順

ステップ 1 コンソールポートで Threat Defense CLI に接続します。

コンソールポートは FXOS CLI に接続します。

ステップ 2 ユーザー名 **admin** およびパスワード **Admin123** でログインします。

初めて FXOS にログインしたときは、パスワードを変更するよう求められます。このパスワードは、SSH の Threat Defense ログインにも使用されます。

（注） パスワードがすでに変更されていてわからない場合は、デバイスを再イメージ化してパスワードをデフォルトにリセットする必要があります。再イメージ化の手順については、FXOS のトラブルシューティング ガイドを参照してください。

例：

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

ステップ 3 Threat Defense CLI に接続します。

connect ftd

例：

```
firepower# connect ftd
>
```

ステップ 4 Threat Defense に初めてログインすると、シスコ エンドユーザー ライセンス契約（EULA）に同意するよう求められます。その後、管理インターフェイスの設定用の CLI セットアップスクリプトが表示されます。

データインターフェイスでマネージャアクセスを有効にした場合でも、管理インターフェイスの設定が使用されます。

（注） 設定をクリア（たとえば、イメージを再作成することにより）しないかぎり、CLI セットアップウィザードを繰り返すことはできません。ただし、これらの設定すべては、後から CLI で **configure network** コマンドを使用して変更できます。Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。

デフォルト値または以前に入力した値がカッコ内に表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

次のガイドラインを参照してください。

- [DHCP経由または手動でIPv4を設定しますか？（Configure IPv4 via DHCP or manually?）]：[手動（manual）] を選択します。管理インターフェイスを使用する予定がない場合でも、プライベートアドレスなどの IP アドレスを設定する必要があります。管理インターフェイスが DHCP に設定されている場合、管理用のデータインターフェイスを設定することはできません。これは、**data-interfaces** である必要があるデフォルトルートが DHCP サーバーから受信したルートで上書きされる可能性があるためです。
- [管理インターフェイスのIPv4デフォルトゲートウェイを入力（Enter the IPv4 default gateway for the management interface）]：ゲートウェイを [data-interfaces] に設定します。この設定は、マネージャ アクセス データ インターフェイスを通じて回送できるように、バックプレーンを介して管理トラフィックを転送します。
- [デバイスをローカルで管理しますか（Manage the device locally?）]：CDO を使用するには「no」を入力します。**yes** と入力すると、代わりに Device Manager を使用することになります。
- [ファイアウォールモードを設定しますか？（Configure firewall mode?）]：**routed** と入力します。外部マネージャアクセスは、ルーテッド ファイアウォール モードでのみサポートされています。

例：

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password: ********
Confirm new password: ********
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]:
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
```

```
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

Update policy deployment information
    - add device configuration
    - add network discovery
    - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

ステップ 5 マネージャアクセス用の外部インターフェイスを設定します。

configure network management-data-interface

その後、外部インターフェイスの基本的なネットワーク設定を行うように求めるプロンプトが表示されます。このコマンドの使用については、次の詳細を参照してください。

- データインターフェイスを管理に使用する場合、管理インターフェイスではDHCPを使用できません。初期セットアップ時にIPアドレスを手動で設定しなかった場合は、**configure network** {**ipv4** | **ipv6**} **manual** コマンドを使用して設定できるようになりました。管理インターフェイス ゲートウェイを **data-interfaces** に設定しなかった場合は、ここでこのコマンドで設定します。

- Threat Defense を CDO に追加すると、CDO はインターフェイス設定（インターフェイス名と IP アドレス、ゲートウェイへの静的ルート、DNS サーバー、DDNS サーバーなど）を検出して維持します。DNS サーバー設定の詳細については、次を参照してください。CDO では、後でマネージャ アクセス インターフェイス構成を変更できますが、Threat Defense または CDO が管理接続の再確立を妨げるような変更は加えないでください。管理接続が中断された場合、Threat Defense には以前の展開を復元する **configure policy rollback** コマンドが含まれます。

- DDNS サーバー更新の URL を設定すると、Threat Defense は Cisco Trusted Root CA バンドルからすべての主要 CA の証明書を自動的に追加するため、Threat Defense は HTTPS 接続の DDNS サーバー証明書を検証できます。Threat Defense は、DynDNS リモート API 仕様

（https://help.dyn.com/remote-access-api/）を使用するすべての DDNS サーバーをサポートします。

- このコマンドは、「データ」インターフェイス DNS サーバーを設定します。セットアップスクリプトで（または **configure network dns servers** コマンドを使用して）設定した管理 DNS サーバーは、管理トラフィックに使用されます。データ DNS サーバーは、DDNS（設定されている場合）またはこのインターフェイスに適用されるセキュリティポリシーに使用されます。

  CDO では、この Threat Defense に割り当てるプラットフォーム設定ポリシーでデータインターフェイス DNS サーバーが設定されます。CDO に Threat Defense を追加すると、ローカル設定が維持され、DNS サーバーはプラットフォーム設定ポリシーに追加されません。ただし、DNS 設定を含む Threat Defense に後でプラットフォーム設定ポリシーを割り当てると、その設定によってローカル設定が上書きされます。CDO と Threat Defense を同期させるには、この設定に一致するように DNS プラットフォーム設定をアクティブに設定することをお勧めします。

  また、ローカル DNS サーバーは、DNS サーバーが初期登録で検出された場合にのみ CDO で保持されます。たとえば、管理インターフェイスを使用してデバイスを登録し、後で **configure network management-data-interface** コマンドを使用してデータインターフェイスを設定した場合、Threat Defense 設定と一致するように、DNS サーバーを含むこれらの設定すべてを CDO で手動で設定する必要があります。

- 管理インターフェイスは、Threat Defense を CDO に登録した後に、管理インターフェイスまたは別のデータインターフェイスのいずれかに変更できます。
- セットアップウィザードで設定した FQDN がこのインターフェイスに使用されます。
- コマンドの一部としてデバイス設定全体をクリアできます。このオプションはリカバリシナリオで使用できますが、初期セットアップや通常の操作には使用しないでください。
- データ管理を無効にするには、**configure network management-data-interface disable** コマンドを入力します。

例：

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://deanwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
 change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

例：

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
 change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

ステップ 6 CDO が生成した **configure manager add** コマンドを使用して、この Threat Defense を管理する CDO を識別します。コマンドの生成については、オンボーディング ウィザードを使用したデバイスのオンボーディング （154 ページ） を参照してください。

例：

```
> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
Manager successfully configured.
```

Device Manager を使用した初期設定の実行

Device Manager に接続して、Threat Defense の初期設定を実行します。Device Manager を使用して初期セットアップを実行すると、管理インターフェイスおよびマネージャアクセス設定に加えて、管理のために CDO に切り替えたときに、Device Manager で完了したすべてのインターフェイス構成が保持されます。アクセス コントロール ポリシーやセキュリティゾーンなどの他のデフォルト設定は保持されないことに注意してください。CLI を使用すると、管理インターフェイスとマネージャアクセス設定のみが保持されます（たとえば、デフォルトの内部インターフェイス構成は保持されません）。

手順

ステップ 1 管理コンピュータを Ethernet1/2 ～ 1/8 のいずれかに接続します

ステップ 2 Device Manager にログインします。

a) ブラウザに URL（**https://192.168.95.1**）を入力します。
b) ユーザー名 **admin**、デフォルト パスワード **Admin123** を使用してログインします。
c) エンド ユーザー ライセンス契約書を読んで同意し、管理者パスワードを変更するように求められます。

ステップ 3 初期設定を完了するには、最初に Device Manager にログインしたときにセットアップウィザードを使用します。必要に応じて、ページの下部にある [デバイスの設定をスキップ（Skip device setup）] をクリックしてセットアップウィザードをスキップできます。

セットアップウィザードを完了すると、内部インターフェイス（Ethernet1/2 ～ 1/8（VLAN1 のスイッチポート））のデフォルト設定に加えて、CDO の管理に切り替えるときに維持される外部（Ethernet1/1）インターフェイスも設定できます。

a) 外部インターフェイスおよび管理インターフェイスに対して次のオプションを設定し、[次へ（Next）] をクリックします。

1. [外部インターフェイスアドレス（Outside Interface Address）]— このインターフェイスは通常インターネット ゲートウェイであり、マネージャ アクセス インターフェイスとして使用される場合があります。デバイスの初期設定時に別の外部インターフェイスを選択することはできません。最初のデータ インターフェイスがデフォルトの外部インターフェイスです。

マネージャアクセスに外部（または内部）とは異なるインターフェイスを使用する場合は、セットアップウィザードの完了後に手動で設定する必要があります。

[IPv4の設定（Configure IPv4）]：外部インターフェイス用の IPv4 アドレスです。DHCP を使用するか、または手動でスタティック IP アドレス、サブネットマスク、およびゲートウェイを入力できます。[オフ（Off）] を選択して、IPv4 アドレスを設定しないという選択肢もあります。セットアップウィザードを使用して PPPoE を設定することはできません。インターフェイスが DSL モデム、ケーブルモデム、または ISP への他の接続に接続されており、ISP が PPPoE を使用して IP アドレスを提供している場合は、PPPoE が必要になる場合があります。ウィザードの完了後に PPPoE を設定できます。

[IPv6の設定（Configure IPv6）]：外部インターフェイス用の IPv6 アドレスです。DHCP を使用するか、または手動でスタティック IP アドレス、プレフィックス、およびゲートウェイを入力できます。[オフ（Off）] を選択して、IPv6 アドレスを設定しないという選択肢もあります。

2. [管理インターフェイス（Management Interface）]

CLI で初期設定を実行した場合、管理インターフェイスの設定は表示されません。

データインターフェイスでマネージャアクセスを有効にした場合でも、管理インターフェイスの設定が使用されます。たとえば、データインターフェイスを介してバックプレーン経由でルーティングされる管理トラフィックは、データインターフェイス DNS サーバーではなく、管理インターフェイス DNS サーバーを使用して FQDN を解決します。

[DNSサーバ（DNS Servers）]：システムの管理アドレス用の DNS サーバ。名前解決用に 1 つ以上の DNS サーバのアドレスを入力します。デフォルトは OpenDNS パブリック DNS サーバです。フィールドを編集し、デフォルトに戻したい場合は、[OpenDNS を使用（Use OpenDNS）] をクリックすると、フィールドに適切な IP アドレスがリロードされます。

[ファイアウォールホスト名（Firewall Hostname）]：システムの管理アドレスのホスト名です。

b) [時刻設定（NTP）（Time Setting (NTP)）] を設定し、[次へ（Next）] をクリックします。

1. [タイムゾーン（Time Zone）]：システムのタイムゾーンを選択します。
2. [NTPタイムサーバ（NTP Time Server）]：デフォルトの NTP サーバを使用するか、使用している NTP サーバのアドレスを手動で入力するかを選択します。バックアップ用に複数のサーバを追加できます。

c) [登録せずに 90 日間の評価期間を開始（Start 90 day evaluation period without registration）] を選択します。

Threat Defense を Smart Software Manager に登録しないでください。すべてのライセンスは CDO で実行されます。

d) [終了（Finish）] をクリックします。

e) [クラウド管理（Cloud Management）]または [スタンドアロン（Standalone）] を選択するよう求められます。CDO クラウド提供型 Management Center の場合は、[スタンドアロン（Standalone）] を選択してから、[了解（Got It）] を選択します。

[クラウド管理（Cloud Management）] オプションは、レガシーの CDO/FDM 機能用です。

ステップ 4 （必要に応じて）管理インターフェイスを設定します。[デバイス（Device）]>[インターフェイス（Interfaces）] の管理インターフェイスを参照してください。

管理インターフェイスには、データインターフェイスに設定されたゲートウェイが必要です。デフォルトでは、管理インターフェイスは DHCP から IP アドレスとゲートウェイを受信します。DHCP からゲートウェイを受信しない場合（たとえば、管理インターフェイスをネットワークに接続していない場合）、ゲートウェイはデフォルトでデータインターフェイスになり、何も設定する必要はありません。DHCPからゲートウェイを受信した場合は、代わりに管理インターフェイスに静的 IP アドレスを設定し、ゲートウェイをデータインターフェイスに設定する必要があります。

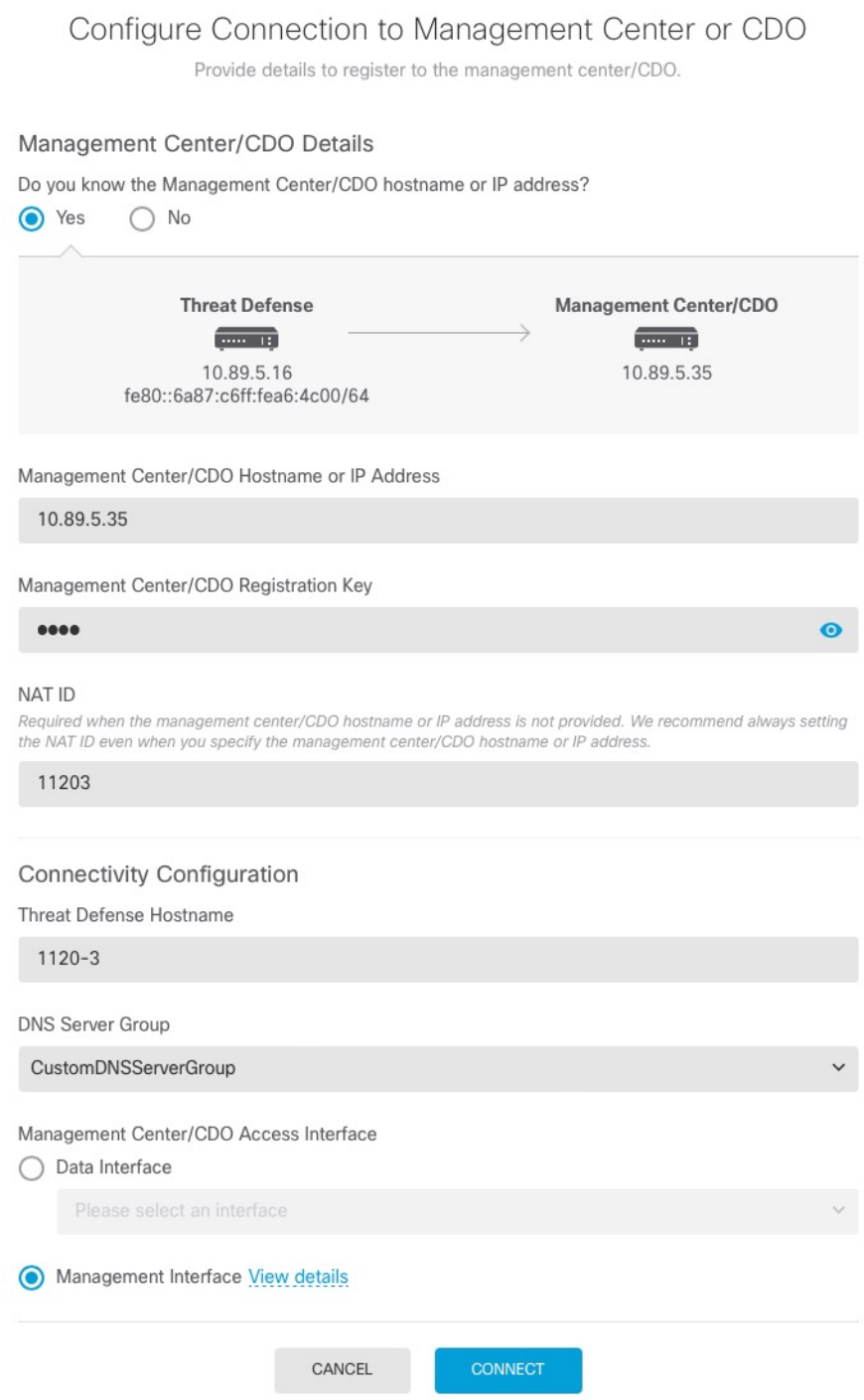
ステップ 5 マネージャアクセスに使用する外部または内部以外のインターフェイスを含む追加のインターフェイスを設定する場合は、[デバイス（Device）] を選択し、[インターフェイス（Interface）] のサマリーのリンクをクリックします。

Device Manager におけるインターフェイスの設定の詳細については、「Device Manager でのファイアウォールの設定 （122 ページ）」を参照してください。CDO にデバイスを登録すると、Device Manager の他の構成は保持されません。

ステップ 6 [デバイス（Device）] [システム設定（Device System Settings）] [中央管理（Central Management）] [Management Center] [Management Center] [デバイス（Device）] [システム設定（System Settings）] [中央管理（Central Management）] [Management Center] の順に選択し、 [続行（Proceed）] をクリックして Management Center の管理を設定します。

ステップ 7 [Management Center/CDOの詳細（Management Center/CDO Details）] を設定します。

図 *47 : Management Center/CDO* の詳細



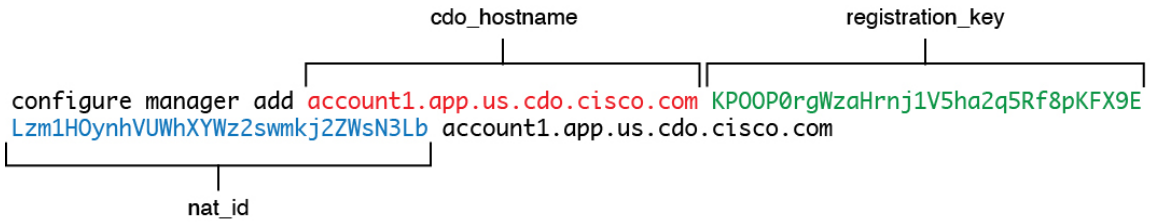
a) [Management Center/CDOホスト名またはIPアドレスを知っていますか（Do you know the Management Center/CDO hostname or IP address）] で、[はい（Yes）] をクリックします。

CDO により **configure manager add** コマンドが生成されます。コマンドの生成については、オンボーディング ウィザードを使用したデバイスのオンボーディング （154 ページ） を参照してください。

configure manager add *cdo_hostname registration_key nat_id display_name*

例：

図 *48 : configure manager add* コマンドコンポーネント



b) コマンドの *cdo_hostname*、*registration_key*、*nat_id* の部分を [Management Center/CDOのホスト名/IPアドレス（Management Center/CDO Hostname/IP Address）]、[Management Center/CDOの登録キー（Management Center/CDO Registration Key）]、[NAT ID] フィールドにコピーします。

ステップ 8 [接続の設定（Connectivity Configuration）] を設定します。

a) [FTDホスト名（FTD Hostname）] を指定します。

この FQDN は、外部インターフェイス、または [Management Center/CDOアクセスインターフェイス（Management Center/CDO Access Interface）] 用に選択したインターフェイスに使用されます。

b) [DNSサーバーグループ（DNS Server Group）] を指定します。

既存のグループを選択するか、新しいグループを作成します。デフォルトの DNS グループは **CiscoUmbrellaDNSServerGroup** と呼ばれ、OpenDNS サーバーが含まれます。

この設定により、データインターフェイス DNS サーバーが設定されます。セットアップウィザードで設定した管理 DNS サーバーは、管理トラフィックに使用されます。データ DNS サーバーは、DDNS（設定されている場合）またはこのインターフェイスに適用されるセキュリティポリシーに使用されます。管理トラフィックとデータトラフィックの両方が外部インターフェイス経由で DNS サーバーに到達するため、管理に使用したものと同じ DNS サーバーグループを選択する可能性があります。

CDO では、この Threat Defense に割り当てるプラットフォーム設定ポリシーでデータインターフェイス DNS サーバーが設定されます。CDO に Threat Defense を追加すると、ローカル設定が維持され、DNS サーバーはプラットフォーム設定ポリシーに追加されません。ただし、DNS 設定を含む Threat Defense に後でプラットフォーム設定ポリシーを割り当てると、その設定によってローカル設定が上書きされます。CDO と Threat Defense を同期させるには、この設定に一致するように DNS プラットフォーム設定をアクティブに設定することをお勧めします。

また、ローカル DNS サーバーは、DNS サーバーが初期登録で検出された場合にのみ CDO で保持されます。

c) [Management Center/CDOアクセスインターフェイス（Management Center/CDO Access Interface）] については、[外部（outside）] を選択します。

設定済みの任意のインターフェイスを選択できますが、このガイドでは外部を使用していることを前提としています。

ステップ 9 外部とは別のデータインターフェイスを選択した場合は、デフォルトルートを追加します。

インターフェイスを通過するデフォルトルートがあることを確認するように求めるメッセージが表示されます。外部を選択した場合は、セットアップウィザードの一環としてこのルートがすでに設定されています。別のインターフェイスを選択する場合は、CDO に接続する前にデフォルトルートを手動で設定する必要があります。Device Manager におけるスタティックルートの設定の詳細については、「Device Manager でのファイアウォールの設定 （122 ページ）」を参照してください。

ステップ 10 [ダイナミックDNS（DDNS）方式の追加（Add a Dynamic DNS (DDNS) method）] をクリックします。

DDNS は、Threat Defense の IP アドレスが変更された場合に CDO が完全修飾ドメイン名（FQDN）で Threat Defense に到達できるようにします。[デバイス（Device）] > [システム設定（System Settings）] > [DDNSサービス（DDNS Service）] を参照して DDNS を設定します。

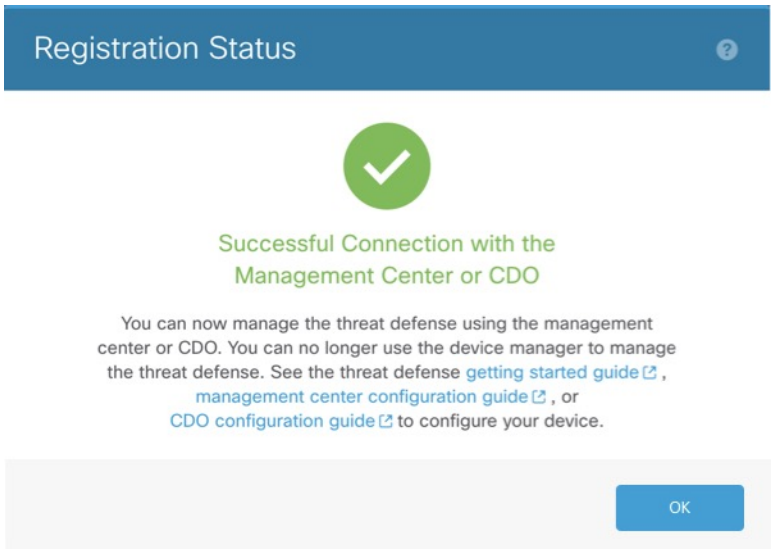
Threat Defense を CDO に追加する前に DDNS を設定すると、Threat Defense は Cisco Trusted Root CA バンドルからすべての主要 CA の証明書を自動的に追加するため、Threat Defense は HTTPS 接続の DDNS サーバー証明書を検証できます。Threat Defense は、DynDNS リモート API 仕様（https://help.dyn.com/remote-access-api/）を使用するすべての DDNS サーバーをサポートします。

ステップ 11 [接続（Connect）] をクリックします。[登録ステータス（Registration Status）] ダイアログボックスに、CDO への切り替えに関する現在のステータスが表示されます。[Management Center/CDO登録設定の保存（Saving Management Center/CDO Registration Settings）] 手順の後、CDO に移動し、ファイアウォールを追加します。

CDO への切り替えをキャンセルする場合は、[登録のキャンセル（Cancel Registration）] をクリックします。それ以外の場合は、[Management Center/CDO登録設定の保存（Saving Management Center/CDO Registration Settings）] 手順が完了するまで、Device Manager ブラウザウィンドウを閉じないでください。閉じた場合、プロセスは一時停止し、Device Manager に再接続した場合のみ再開されます。

[Management Center/CDO登録設定の保存（Saving Management Center/CDO Registration Settings）] の手順後に Device Manager に接続したままにすると、最終的に [Management CenterまたはCDOとの正常接続（Successful Connection with Management Center or CDO）] ダイアログボックスが表示され、Device Manager から切断されます。

図 *49 :* 正常接続



基本的なセキュリティポリシーの設定

ここでは、次の設定を使用して基本的なセキュリティポリシーを設定する方法について説明します。

- 内部インターフェイスと外部インターフェイス：内部インターフェイスに静的 IP アドレスを割り当てます。マネージャアクセス設定の一環として外部インターフェイスの基本設定を設定しましたが、まだそのインターフェイスをセキュリティゾーンに割り当てる必要があります。
- DHCP サーバー：クライアントの内部インターフェイスで DHCP サーバーを使用します。
- NAT：外部インターフェイスでインターフェイス PAT を使用します。
- アクセスコントロール：内部から外部へのトラフィックを許可します。
- SSH：マネージャ アクセス インターフェイスで SSH を有効にします。

インターフェイスの設定

スイッチポートの VLAN1 インターフェイスを追加するか、スイッチポートをファイアウォール インターフェイスに変換し、セキュリティゾーンにインターフェイスを割り当て、IP アドレスを設定します。通常は、システムで意味のあるトラフィックを通過させるように、少なくとも 2 つのインターフェイスを設定する必要があります。通常は、アップストリームルータまたはインターネットに面した外部インターフェイスと、組織のネットワークの 1 つ以上の内部インターフェイスを使用します。デフォルトでは、Ethernet1/1 は外部用に使用できる通常の

ファイアウォール インターフェイスであり、残りのインターフェイスは VLAN 1 のスイッチポートです。VLAN1 インターフェイスを追加すると、これを内部インターフェイスにすることができます。または、スイッチポートを他の VLAN に割り当てるか、スイッチポートをファイアウォール インターフェイスに変換することもできます。

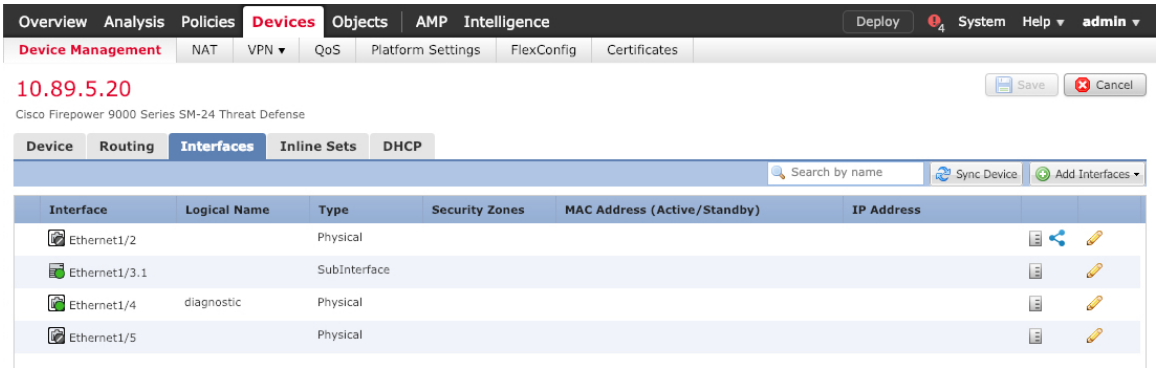
一般的なエッジルーティングの状況は、内部インターフェイスでスタティックアドレスを定義すると同時に、ISP から DHCP を介して外部インターフェイスアドレスを取得することです。

次の例では、DHCP によるスタティックアドレスとルーテッドモードの外部インターフェイスを使用して（Ethernet1/1）、ルーテッドモードの内部インターフェイス（VLAN1）を設定します。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、デバイスをクリックします。

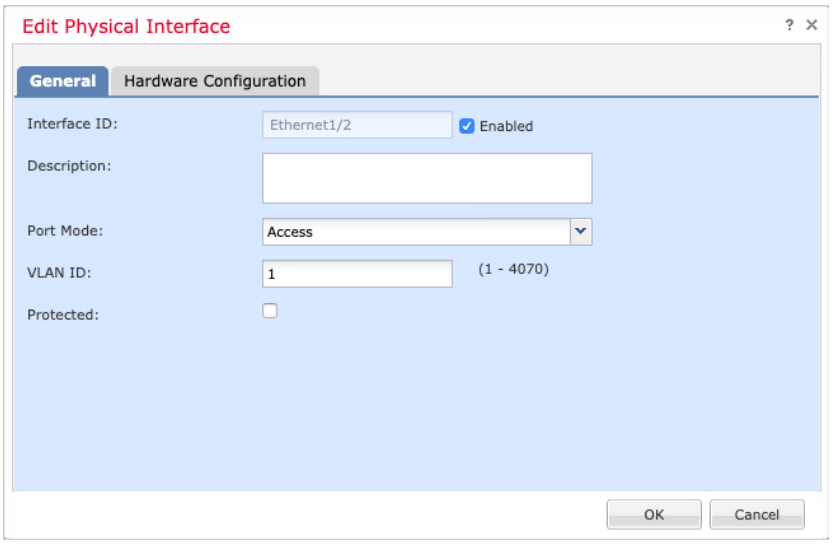
ステップ 2 [インターフェイス（Interfaces）] をクリックします。



ステップ 3 （任意）[スイッチポート（SwitchPort）] 列のスライダをクリックしてスイッチポート（Ethernet1/2 から 1/8）のいずれかのスイッチポートモードを無効にすると、無効（ ）と表示されます。

ステップ 4 スイッチポートを有効にします。

a) スイッチポートのをクリックします。



b) [有効（Enabled）] チェックボックスをオンにして、インターフェイスを有効化します。

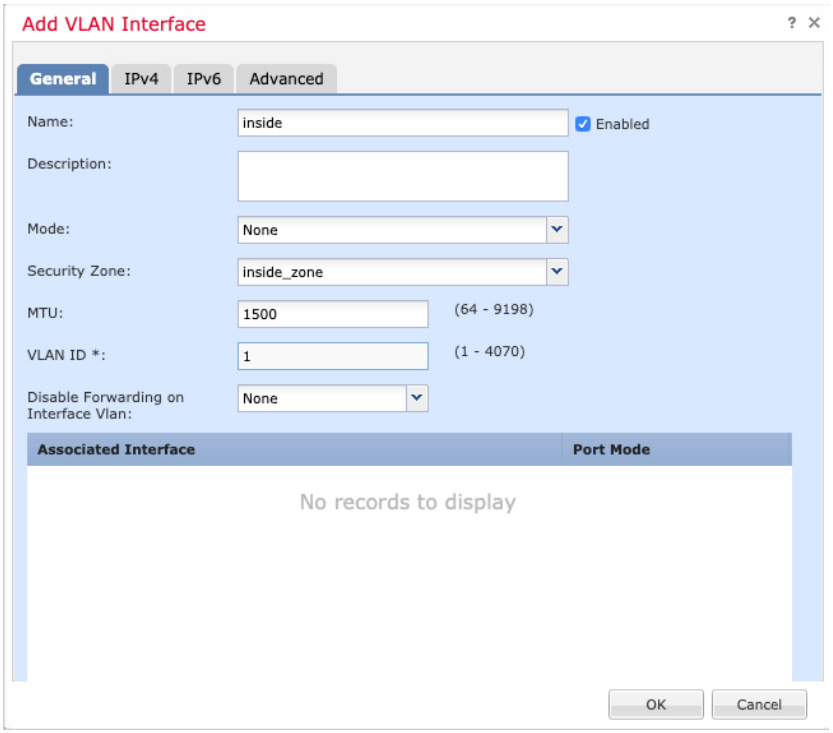
c) （任意） VLAN ID を変更します。デフォルトは 1 です。次に、この ID に一致する VLAN インターフェイスを追加します。

d) [OK] をクリックします。

ステップ 5 内部 VLAN インターフェイスを追加します。

a) **[インターフェイスの追加（Add Interfaces）]** > **[VLANインターフェイス（VLAN Interface）]** をクリックします。

[全般（General）] タブが表示されます。



b) 48 文字までの [名前（Name）] を入力します。

たとえば、インターフェイスに **inside** という名前を付けます。

c) [有効（Enabled）] チェックボックスをオンにします。

d) [モード（Mode）] は [なし（None）] に設定したままにします。

e) [セキュリティゾーン（Security Zone）] ドロップダウンリストから既存の内部セキュリティゾーンを選択するか、[新規（New）] 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。

たとえば、**inside_zone** という名前のゾーンを追加します。各インターフェイスは、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割り当てる必要があります。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も、複数のインターフェイスグループに属することもできます。ゾーンまたはグループに基づいてセキュリティポリシーを適用します。たとえば、内部インターフェイスを内部ゾーンに割り当て、外部インターフェイスを外部ゾーンに割り当てることができます。この場合、トラフィックが内部から外部に移動できるようにアクセス コントロール ポリシーを設定することはできますが、外部から内部に向けては設定できません。ほとんどのポリシーはセキュリティゾーンのみサポートしています。NAT ポリシー、プレフィルタ ポリシー、および QoS ポリシーで、ゾーンまたはインターフェイスグループを使用できます。

f) [VLAN ID] を **1** に設定します。

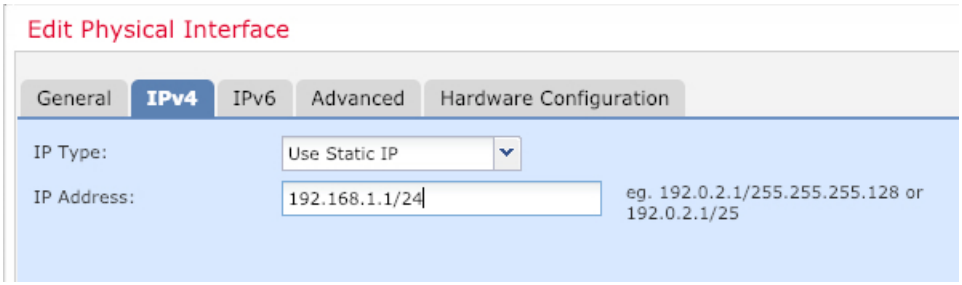
デフォルトでは、すべてのスイッチポートは VLAN 1 に設定されます。ここで別の VLAN ID を選択する場合は、新しい VLAN ID の各スイッチポートを編集する必要があります。

インターフェイスを保存した後、VLAN ID を変更することはできません。ここでの VLAN ID は、使用される VLAN タグと設定内のインターフェイス ID の両方です。

g) [IPv4] タブ、[IPv6] タブ、または両方のタブをクリックします。

- [IPv4]：ドロップダウンリストから [スタティック IP を使用する（Use Static IP）] を選択し、IP アドレスとサブネットマスクをスラッシュ表記で入力します。

  たとえば、**192.168.1.1/24** などと入力します。

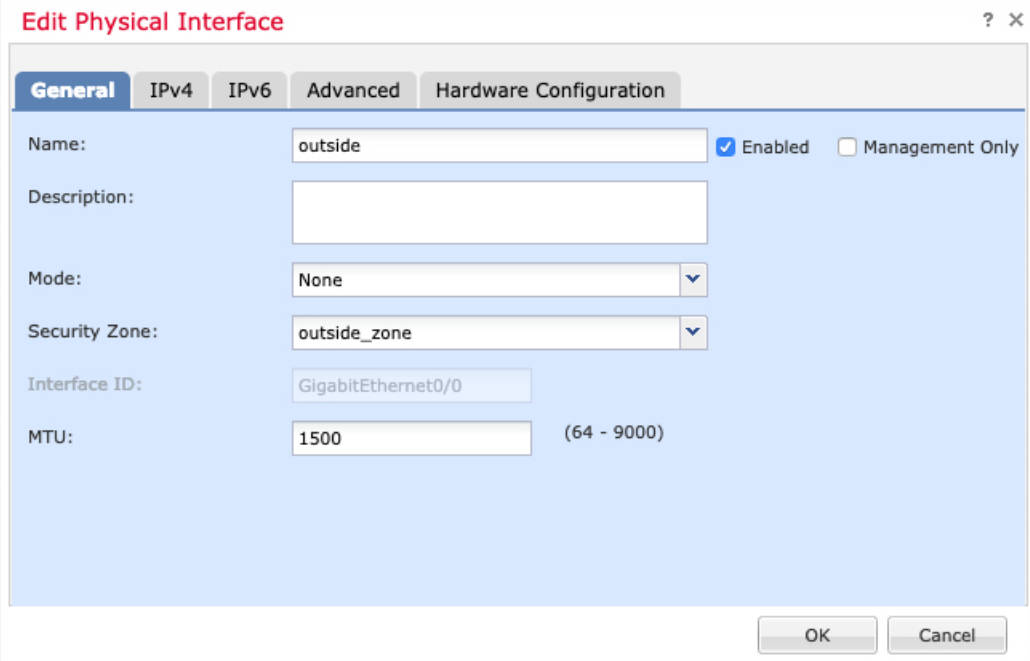


- [IPv6]：ステートレス自動設定の場合は [自動設定（Autoconfiguration）] チェックボックスをオンにします。

h) [OK] をクリックします。

ステップ 6 外部用に使用する Ethernet1/1 のをクリックします。

[全般（General）] タブが表示されます。



マネージャアクセス用にこのインターフェイスを事前に設定しているため、インターフェイスにはすでに名前が付けられており、有効化とアドレス指定が完了しています。これらの基本設定は変更しないでください。変更すると、Management Center の管理接続が中断されます。この画面でも、通過トラフィックポリシーのセキュリティゾーンを設定する必要があります。

a) [セキュリティゾーン（Security Zone）] ドロップダウンリストから既存の外部セキュリティゾーンを選択するか、[新規（New）] 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。

   たとえば、「outside_zone」という名前のゾーンを追加します。

b) [OK] をクリックします。

ステップ 7 [保存（Save）] をクリックします。

DHCP サーバーの設定

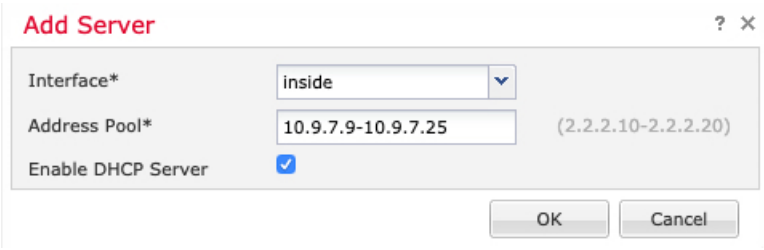
クライアントで DHCP を使用して Threat Defense から IP アドレスを取得するようにする場合は、DHCP サーバーを有効にします。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、デバイスをクリックします。

ステップ 2 **[DHCP]** > **[DHCPサーバー（DHCP Server）]** を選択します。

ステップ 3 **[サーバー（Server）]** ページで、**[追加（Add）]** をクリックして、次のオプションを設定します。



- [インターフェイス（Interface）]：ドロップダウンリストからインターフェイスを選択します。
- [アドレスプール（Address Pool）]：DHCP サーバーが使用する IP アドレスの最下位から最上位の間の範囲を設定します。IP アドレスの範囲は、選択したインターフェイスと同じサブネット上に存在する必要があり、インターフェイス自身の IP アドレスを含めることはできません。
- [DHCPサーバーを有効にする（Enable DHCP Server）]：選択したインターフェイスの DHCP サーバーを有効にします。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックします。

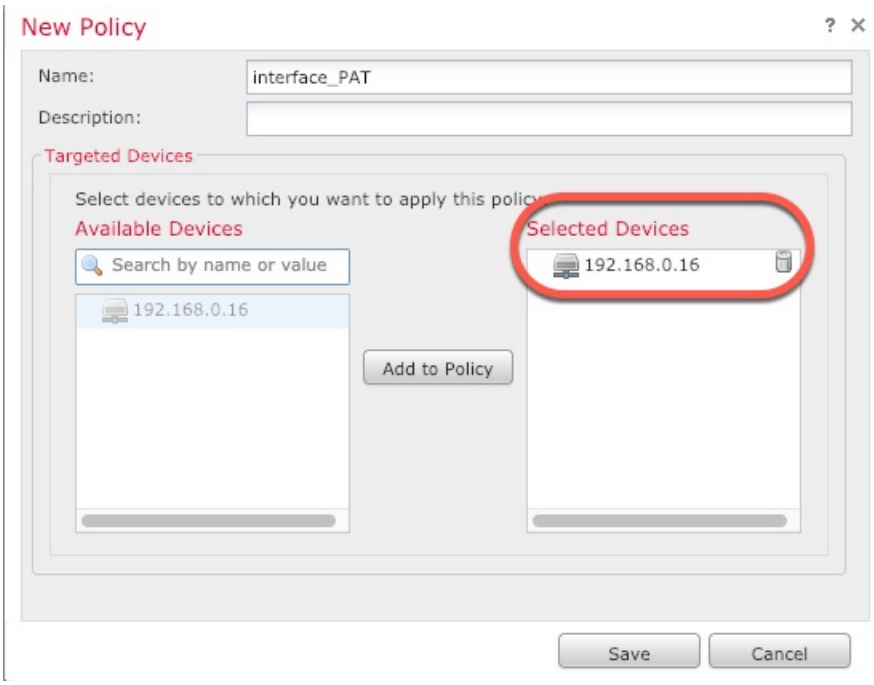
NAT の設定

一般的な NAT ルールでは、内部アドレスを外部インターフェイスの IP アドレスのポートに変換します。このタイプの NAT ルールのことをインターフェイス ポート アドレス変換（PAT）と呼びます。

手順

ステップ 1 **[デバイス（Devices）]** > **[NAT]** をクリックし、**[新しいポリシー（New Policy）]** > **[Threat Defense NAT]** をクリックします。

ステップ 2 ポリシーに名前を付け、ポリシーを使用するデバイスを選択し、[保存（Save）] をクリックします。



ポリシーが Management Center に追加されます。引き続き、ポリシーにルールを追加する必要があります。

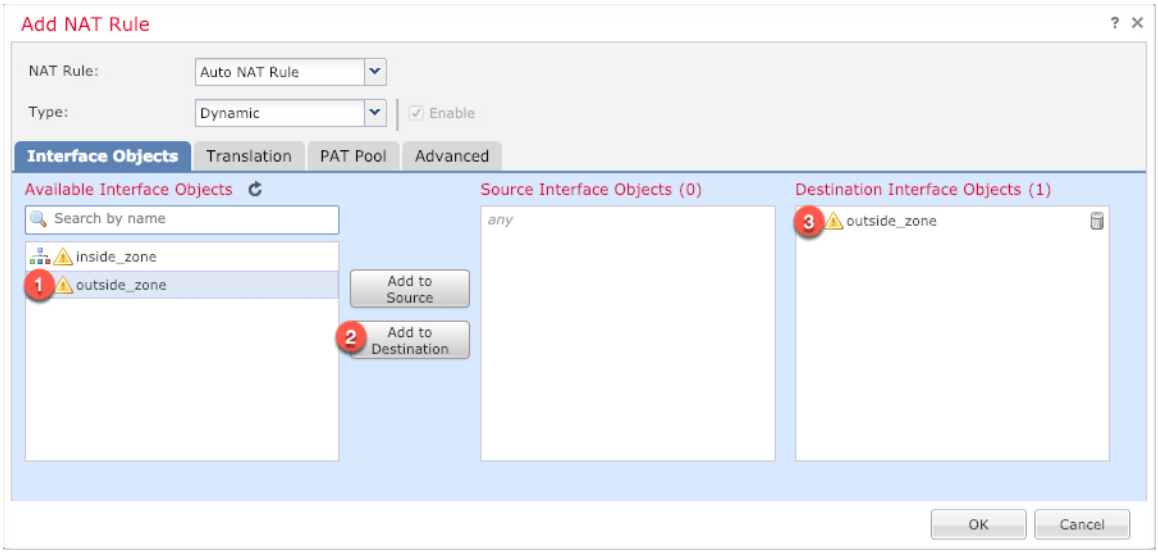
ステップ 3 [ルールの追加（Add Rule）] をクリックします。

[NATルールの追加（Add NAT Rule）] ダイアログボックスが表示されます。

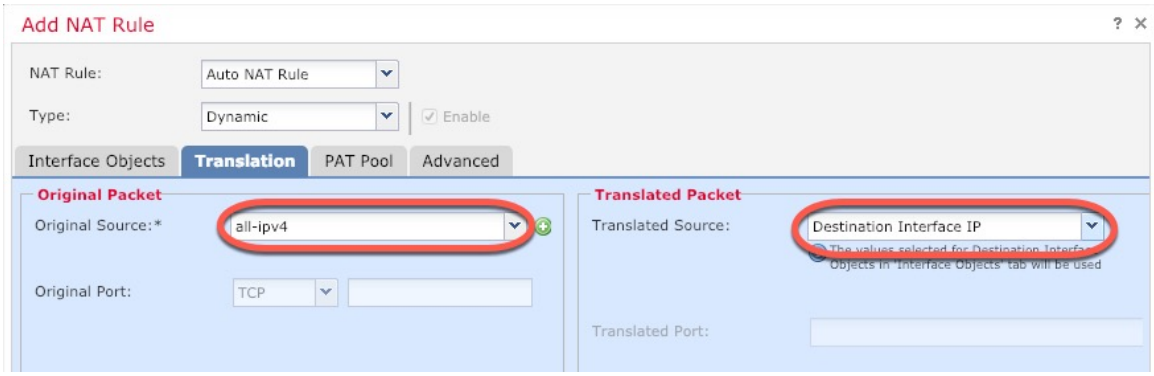
ステップ 4 基本ルールのオプションを設定します。

- [NATルール（NAT Rule）]：[自動NATルール（Auto NAT Rule）] を選択します。
- [タイプ（Type）]：[ダイナミック（Dynamic）] を選択します。

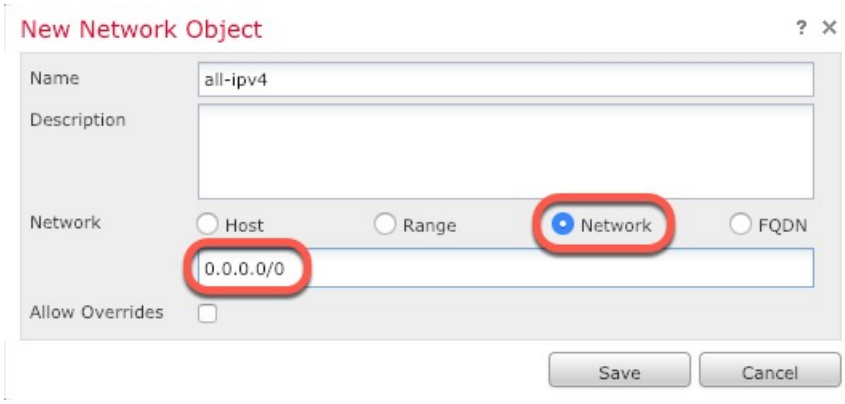
ステップ 5 [インターフェイスオブジェクト（Interface objects）] ページで、[使用可能なインターフェイスオブジェクト（Available Interface Objects）] 領域から [宛先インターフェイスオブジェクト（Destination Interface Objects）] 領域に外部ゾーンを追加します。



ステップ 6 [変換（Translation）] ページで、次のオプションを設定します。



- [元の送信元（Original Source）]：をクリックして、すべての IPv4 トラフィック（0.0.0.0/0）のネットワークオブジェクトを追加します。

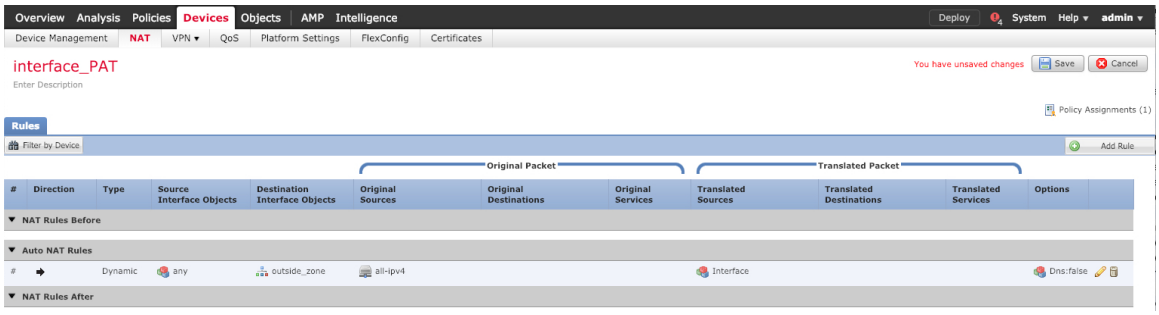


（注） 自動 NAT ルールはオブジェクト定義の一部として NAT を追加するため、システム定義の **any-ipv4** オブジェクトを使用することはできません。また、システム定義のオブジェクトを編集することはできません。

- [変換済みの送信元（Translated Source）]：[宛先インターフェイスIP（Destination Interface IP）] を選択します。

ステップ 7 [保存（Save）] をクリックしてルールを追加します。

ルールが [ルール（Rules）] テーブルに保存されます。



ステップ 8 NAT ページで [保存（Save）] をクリックして変更を保存します。

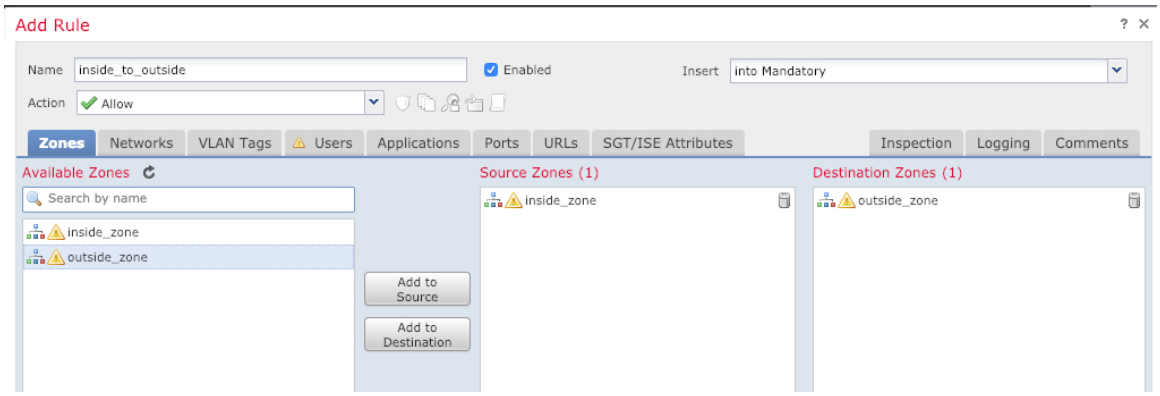
内部から外部へのトラフィックの許可

Threat Defense を登録したときに、基本の [すべてのトラフィックをブロック（Block all traffic）] アクセス コントロール ポリシーを作成した場合は、デバイスを通過するトラフィックを許可するためにポリシーにルールを追加する必要があります。次の手順では、内部ゾーンから外部ゾーンへのトラフィックを許可するルールを追加します。他にゾーンがある場合は、適切なネットワークへのトラフィックを許可するルールを追加してください。

手順

ステップ 1 **[ポリシー（Policy）] > [アクセスポリシー（Access Policy）] > [アクセスポリシー（Access Policy）]**を選択し、Threat Defense に割り当てられているアクセス コントロール ポリシーのをクリックします。

ステップ 2 **[ルールを追加（Add Rule）]** をクリックし、次のパラメータを設定します。

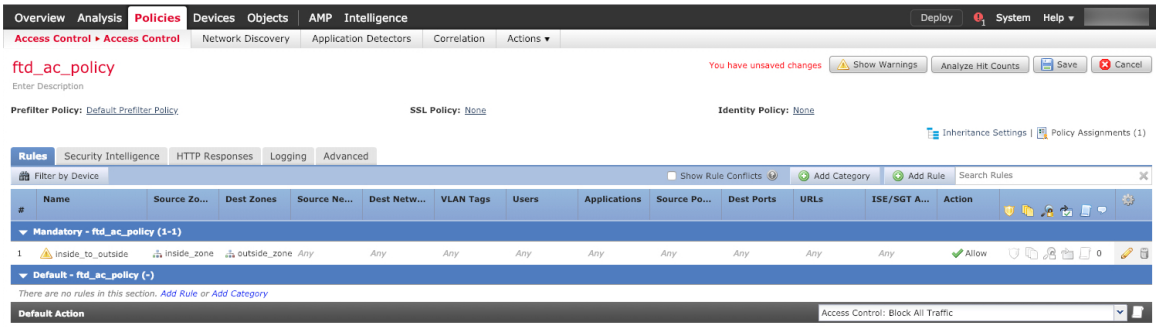


- [名前（Name）]：このルールに名前を付けます（たとえば、**inside_to_outside**）。
- [送信元ゾーン（Source Zones）]：[使用可能なゾーン（Available Zones）] から内部ゾーンを選択し、[送信元に追加（Add to Source）] をクリックします。
- [宛先ゾーン（Destination Zones）]：[使用可能なゾーン（Available Zones）] から外部ゾーンを選択し、[宛先に追加（Add to Destination）] をクリックします。

他の設定はそのままにしておきます。

ステップ 3 [追加（Add）] をクリックします。

ルールが [ルール（Rules）] テーブルに追加されます。



ステップ 4 [保存（Save）] をクリックします。

マネージャ アクセス データ インターフェイスでの SSH の設定

外部インターフェイスなどのデータインターフェイスで Management Center アクセスを有効にした場合は、この手順に従ってそのインターフェイスで SSH を有効にする必要があります。ここでは、Threat Defense で 1 つ以上のデータインターフェイスに対して SSH 接続を有効にする方法について説明します。 SSH は診断論理インターフェイスに対してサポートされません。

（注） SSH は管理インターフェイス上でデフォルトで有効になっていますが、この画面は管理 SSH アクセスに影響しません。

管理インターフェイスは、デバイスの他のインターフェイスとは分離されています。Management Centerにデバイスを設定し、登録するために使用されます。データ インターフェイスの SSH は、管理インターフェイスの SSH と内部および外部ユーザ リストを共有します。その他の設定は個別に設定されます。データ インターフェイスでは、この画面を使用して SSH とアクセス リストを有効にします。データ インターフェイスの SSH トラフィックは通常のルーティング設定を使用し、設定時に設定されたスタティック ルートや CLI で設定されたスタティック ルートは使用しません。

管理インターフェイスの場合、SSH アクセスリストを構成するには Cisco Secure Firewall Threat Defense コマンドリファレンス の **configure ssh-access-list** コマンドを参照してください。スタティック ルートを設定するには、**configure network static-routes** コマンドを参照してください。デフォルトでは、初期設定時に管理インターフェイスからデフォルト ルートを設定します。

SSH を使用するには、ホスト IP アドレスを許可するアクセス ルールは必要ありません。このセクションの手順に従って、SSH アクセスを設定する必要があるだけです。

SSH は、到達可能なインターフェイスにのみ使用できます。SSH ホストが外部インターフェイスにある場合、外部インターフェイスへの直接管理接続のみ開始できます。

（注） SSH を介した CLI へのログイン試行が 3 回連続して失敗すると、デバイスの SSH 接続は終了します。

始める前に

- SSH 内部ユーザーは、**configure user add** コマンドを使用して CLI でのみ設定できます。。デフォルトでは、初期設定時にパスワードを設定した**Admin**ユーザーが存在します。LDAP または RADIUS 上の外部ユーザーは、プラットフォーム設定で [外部認証（External Authentication）] を設定することによっても設定できます。
- デバイスへの SSH 接続を許可するホストまたはネットワークを定義するネットワーク オブジェクトが必要です。オブジェクトをプロシージャの一部として追加できますが、IP アドレスのグループを特定するためにオブジェクト グループを使用する場合は、ルールで必要なグループがすでに存在することを確認します。**[オブジェクト（Objects）]**>**[オブジェクト管理（Object Management）]** を選択して、オブジェクトを設定します。

（注） システムが提供する **any** ネットワーク オブジェクトは使用できません。代わりに、**any-ipv4** または **any-ipv6** を使用します。

手順

ステップ 1 **[デバイス（Devices）]**>**[プラットフォーム設定（Platform Settings）]** を選択し、Threat Defense ポリシーを作成または編集します。

ステップ 2 [セキュア シェル（Secure Shell）] を選択します。

ステップ 3 SSH 接続を許可するインターフェイスと IP アドレスを指定します。

この表を使用して、SSH 接続を受け入れるインターフェイス、およびそれらの接続を許可されるクライアントの IP アドレスを制限します。個々の IP アドレスはなく、ネットワーク アドレスを使用できます。

a) [追加（Add）]をクリックして新しいルールを追加するか、[編集（Edit）]をクリックして既存のルールを編集します。

b) ルールのプロパティを設定します。

- [IP Address]：SSH 接続を許可するホストまたはネットワークを特定するネットワークオブジェクトまたはグループ。オブジェクトをドロップダウンメニューから選択するか、または [+] をクリックして新しいネットワークオブジェクトを追加します。
- [セキュリティ ゾーン（Security Zones）]：SSH 接続を許可するインターフェイスを含むゾーンを追加します。ゾーンにないインターフェイスでは、選択されたセキュリティゾーンのリストの下のフィールドにインターフェイス名を入力し、[追加（Add）]をクリックします。選択されているインターフェイスまたはゾーンがデバイスに含まれているときにのみ、これらのルールがデバイスに適用されます。

c) [OK] をクリックします。

ステップ 4 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更はポリシーを展開するまで有効になりません。

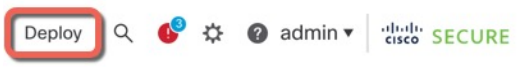
設定の展開

設定の変更を Threat Defense に展開します。変更を展開するまでは、デバイス上でどの変更もアクティブになりません。

手順

ステップ 1 右上の [展開（Deploy）] をクリックします。

図 *50 : [*展開（*Deploy***）*]***



ステップ 2 [すべて展開（Deploy All）] をクリックしてすべてのデバイスに展開するか、[高度な展開（Advanced Deploy）] をクリックして選択したデバイスに展開します。

図 *51* : すべて展開

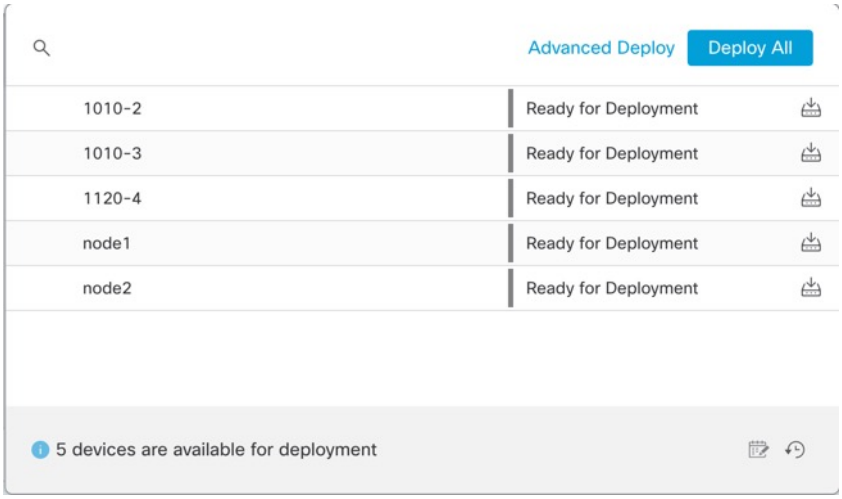
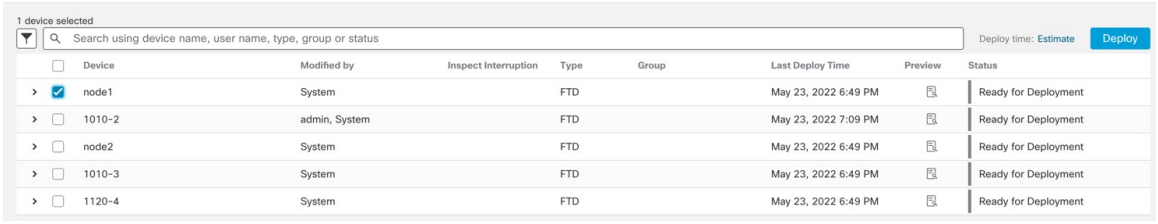
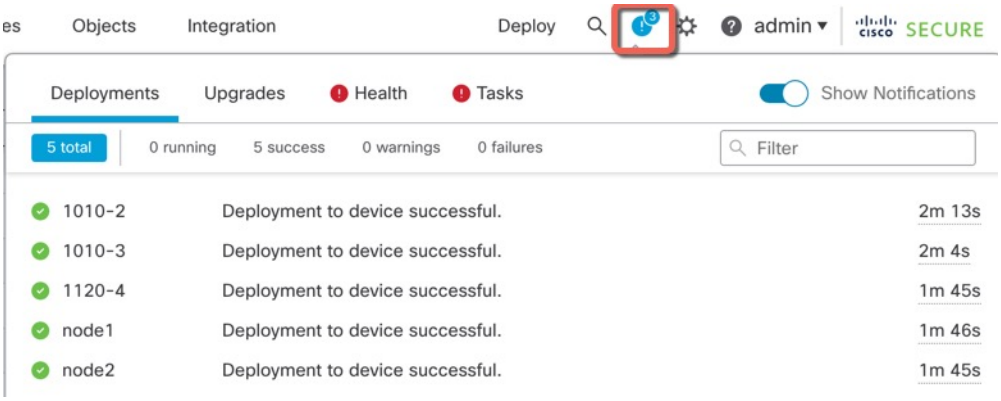


図 *52* : 高度な展開



ステップ 3 展開が成功したことを確認します。展開のステータスを表示するには、メニューバーの [展開（Deploy）] ボタンの右側にあるアイコンをクリックします。

図 *53* : 展開ステータス



トラブルシューティングとメンテナンス

Threat Defense および FXOS CLI へのアクセス

コマンドライン インターフェイス（CLI）を使用してシステムのセットアップを行い、基本的なシステムのトラブルシューティングを行います。CLI セッションからポリシーを設定することはできません。CLI には、コンソール ポートに接続してアクセスできます。

トラブルシューティングのためにも FXOS CLI にアクセスできます。

（注） または、Threat Defense デバイスの管理インターフェイスに SSH で接続できます。コンソール セッションとは異なり、SSH セッションはデフォルトで Threat Defense CLI になり、**connect fxos** コマンドを使用して FXOS CLI に接続できます。SSH 接続用のインターフェイスを開いている場合、後でデータインターフェイス上のアドレスに接続できます。データ インターフェイスへの SSH アクセスはデフォルトで無効になっています。この手順では、デフォルトで FXOS CLI となるコンソールポートアクセスについて説明します。

手順

ステップ 1 CLI にログインするには、管理コンピュータをコンソール ポートに接続します。 Firepower 1000 には、USB A to B シリアル ケーブルが付属しています。お使いのオペレーティングシステムに必要な USB シリアルドライバを必ずインストールしてください（Firepower 1010 ハードウェアガイドを参照）。コンソールポートはデフォルトで FXOS CLI になります。次のシリアル設定を使用します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

FXOS CLI に接続します。ユーザー名 **admin** と、初期セットアップ時に設定したパスワードを使用して CLI にログインします（デフォルトは **Admin123**）。

例：

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

ステップ 2 Threat Defense CLI にアクセスします。

connect ftd

例：

```
firepower# connect ftd
>
```

ログイン後に、CLI で使用可能なコマンドの情報を確認するには、**help** または **?** を入力します。使用方法については、『Cisco Secure Firewall Threat Defense コマンドリファレンス』を参照してください。

ステップ 3 Threat Defense CLI を終了するには、**exit** または **logout** コマンドを入力します。

このコマンドにより、FXOS CLI プロンプトに戻ります。FXOS CLI で使用可能なコマンドについては、**?** を入力してください。

例：

```
> exit
firepower#
```

データインターフェイスでの管理接続のトラブルシューティング

専用の管理インターフェイスを使用する代わりに、マネージャアクセスにデータインターフェイスを使用する場合は、CDO で Threat Defense のインターフェイスとネットワークの設定を変更する際、接続を中断しないように注意します。Threat Defense を CDO に追加した後に管理インターフェイスタイプを変更する場合（データから管理へ、または管理からデータへ）、インターフェイスとネットワークの設定が正しく構成されていないと、管理接続が失われる可能性があります。

このトピックは、管理接続が失われた場合のトラブルシューティングに役立ちます。

管理接続ステータスの表示

CDO で、**[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [管理（Management）] > [マネージャアクセス - 構成詳細（Manager Access - Configuration Details）] > [接続ステータス（Connection Status）]** ページで管理接続ステータスを確認します。

管理接続のステータスを表示するには、Threat Defense CLI で、**sftunnel-status-brief** コマンドを入力します。**sftunnel-status** を使用して、より完全な情報を表示することもできます。

ダウン状態の接続の出力例を次に示します。ピアチャネルの「接続先」情報やハートビート情報が表示されていません。

```
> sftunnel-status-brief
```

```
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went
down
```

アップ状態の接続の出力例を次に示します。ピアチャネルとハートビート情報が表示されています。

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to
'10.10.17.202' via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to
'10.10.17.202' via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

Threat Defense ネットワーク情報の表示

Threat Defense CLI で、管理およびマネージャ アクセス データ インターフェイスのネットワーク設定を表示します。

show network

```
> show network
===============[ System Information ]===============
Hostname                  : 5516X-4
DNS Servers               : 208.67.220.220,208.67.222.222
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces
IPv6 Default route
  Gateway                 : data-interfaces

======================[ br1 ]======================
State                     : Enabled
Link                      : Up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 28:6F:7F:D3:CB:8D
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.99.10.4
Netmask                   : 255.255.255.0
Gateway                   : 10.99.10.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

===============[ Proxy Information ]================
State                     : Disabled
Authentication            : Disabled

======[ System Information - Data Interfaces ]======
DNS Servers               :
```

```
Interfaces               : GigabitEthernet1/1

===============[ GigabitEthernet1/1 ]===============
State                    : Enabled
Link                     : Up
Name                     : outside
MTU                      : 1500
MAC Address              : 28:6F:7F:D3:CB:8F
----------------------[ IPv4 ]----------------------
Configuration            : Manual
Address                  : 10.89.5.29
Netmask                  : 255.255.255.192
Gateway                  : 10.89.5.1
----------------------[ IPv6 ]----------------------
Configuration            : Disabled
```

CDO への Threat Defense の登録の確認

Threat Defense CLI で、CDO 登録が完了したことを確認します。このコマンドは、管理接続の現在のステータスを表示するものではないことに注意してください。

show managers

```
> show managers
Type                     : Manager
Host                     : account1.app.us.cdo.cisco.com
Display name             : account1.app.us.cdo.cisco.com
Identifier               : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration             : Completed
Management type          : Configuration
```

CDO への ping

Threat Defense CLI で、次のコマンドを使用して、データインターフェイスから CDO に ping します。

ping *cdo_hostname*

Threat Defense CLI で、次のコマンドを使用して、管理インターフェイスから CDO に ping します。これは、バックプレーンを介してデータインターフェイスにルーティングされます。

ping system *cdo_hostname*

Threat Defense 内部インターフェイスでのパケットのキャプチャ

Threat Defense CLI で、内部バックプレーン インターフェイス（nlp_int_tap）でパケットをキャプチャして、管理パケットが送信されているかどうかを確認します。

capture *name* **interface nlp_int_tap trace detail match ip any any**

show capture*name* **trace detail**

内部インターフェイスのステータス、統計、およびパケット数の確認

Threat Defense CLI で、内部バックプレーン インターフェイス（nlp_int_tap）に関する情報を参照してください。

show interace detail

```
> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
 (Full-duplex), (1000 Mbps)
 Input flow control is unsupported, output flow control is unsupported
 MAC address 0000.0100.0001, MTU 1500
 IP address 169.254.1.1, subnet mask 255.255.255.248
 37 packets input, 2822 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 pause input, 0 resume input
 0 L2 decode drops
 5 packets output, 370 bytes, 0 underruns
 0 pause output, 0 resume output
 0 output errors, 0 collisions, 0 interface resets
 0 late collisions, 0 deferred
 0 input reset drops, 0 output reset drops
 input queue (blocks free curr/low): hardware (0/0)
 output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
 37 packets input, 2304 bytes
 5 packets output, 300 bytes
 37 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
 Interface number is 14
 Interface config status is active
 Interface state is active
```

ルーティングと NAT の確認

Threat Defense CLI で、デフォルトルート（S*）が追加されていること、および管理インターフェイス（nlp_int_tap）に内部 NAT ルールが存在することを確認します。

show route

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C        10.89.5.0 255.255.255.192 is directly connected, outside
L        10.89.5.29 255.255.255.255 is directly connected, outside

>
```

show nat

```
> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface
service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface  service
 tcp ssh ssh
    translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
 ipv6  service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
    translate_hits = 0, untranslate_hits = 0
>
```

その他の設定の確認

次のコマンドを参照して、他のすべての設定が存在することを確認します。これらのコマンドの多くは、CDO の**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[デバイス（Device）]** > **[管理（Management）]** > **[マネージャアクセス - 構成詳細（Manager Access - Configuration Details）]** > **[CLI出力（CLI Output）]** ページでも確認できます。

show running-config sftunnel

```
> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305
```

show running-config ip-client

```
> show running-config ip-client
ip-client outside
```

show conn address *fmc_ip*

```
> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
       preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap  10.89.5.29(169.254.1.2):51231 outside  10.89.5.35:8305, idle 0:00:04,
 bytes 86684, flags UxIO
TCP nlp_int_tap  10.89.5.29(169.254.1.2):8305 outside  10.89.5.35:52019, idle 0:00:02,
 bytes 1630834, flags UIO
>
```

DDNS の更新が成功したかどうかを確認する

Threat Defense CLI で、DDNS の更新が成功したかどうかを確認します。

debug ddns

```
> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfuly updated the DDNS sever with current IP addresses
```

```
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0
```

更新に失敗した場合は、**debug http** コマンドと **debug ssl** コマンドを使用します。証明書の検証が失敗した場合は、ルート証明書がデバイスにインストールされていることを確認します。

show crypto ca certificates *trustpoint_name*

DDNS の動作を確認するには：

show ddns update interface *fmc_access_ifc_name*

```
> show ddns update interface outside

Dynamic DNS Update on outside:
    Update Method Name Update Destination
    RBD_DDNS not available

Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

CDO ログファイルの確認

https://cisco.com/go/fmc-reg-error を参照してください。

CDO の接続が失われた場合の構成のロールバック

Threat Defense でマネージャアクセス用にデータインターフェイスを使用し、ネットワーク接続に影響する CDO からの構成変更を展開する場合、Threat Defense の構成を最後に展開した構成にロールバックして、管理接続を復元できます。その後、ネットワーク接続が維持されるように CDO で構成設定を調整し、再展開できます。ロールバック機能は、接続が失われていない場合でも使用でき、このトラブルシューティングの状況以外でも使用できます。

次のガイドラインを参照してください。

- 前回の展開のみ Threat Defense でローカルに使用できます。さらに以前の展開にロールバックすることはできません。
- ロールバックは、CDO で設定できる設定にのみ影響します。たとえば、ロールバックは、Threat Defense CLI でのみ設定できる専用管理インターフェイスに関連するローカル構成には影響しません。**configure network management-data-interface** コマンドを使用した最後の CDO 展開後にデータインターフェイス設定を変更し、rollback コマンドを使用すると、それらの設定は保持されないことに注意してください。最後に展開された CDO 設定にロールバックされます。
- 以前の展開中に更新されたアウトオブバンド SCEP 証明書データはロールバックできません。
- ロールバック中に、現在の設定がクリアされるため、接続がドロップされます。

手順

ステップ 1 Threat Defense CLI で、以前の構成へロールバックします。

configure policy rollback

ロールバック後、Threat Defense はロールバックが正常に完了したことを CDO に通知します。CDO では、構成がロールバックされたことを示すバナーが展開画面に表示されます。

（注） ロールバックが失敗し、CDO 管理が復元された場合は、一般的な展開の問題についてhttps://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.htmlを参照してください。場合によっては、CDO 管理アクセスの復元後にロールバックが失敗することがあります。この場合、CDO 構成の問題を解決して、CDO から再展開できます。

例：

マネージャアクセスにデータインターフェイスを使用する Threat Defense の場合：

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2022 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....................
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
...................
.....................
>
```

ステップ 2 管理接続が再確立されたことを確認します。

CDO で、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[デバイス（Device）]** > **[管理（Management）]** > **[マネージャアクセス - 構成詳細（Manager Access - Configuration Details）]** > **[接続ステータス（Connection Status）]** ページで管理接続ステータスを確認します。

管理接続のステータスを表示するには、Threat Defense CLI で、**sftunnel-status-brief** コマンドを入力します。

接続の再確立に 10 分以上かかる場合は、接続のトラブルシューティングを行う必要があります。データインターフェイスでの管理接続のトラブルシューティング（180ページ）を参照してください。

CDO を使用したファイアウォールの電源の切断

システムを適切にシャットダウンすることが重要です。単純に電源プラグを抜いたり、電源スイッチを押したりすると、重大なファイルシステムの損傷を引き起こすことがあります。バックグラウンドでは常に多数のプロセスが実行されていて、電源プラグを抜いたり、電源を切断したりすると、ファイアウォールをグレースフルシャットダウンできないことを覚えておいてください。

CDO を使用してシステムを適切にシャットダウンできます。

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 再起動するデバイスの横にある編集アイコン（ ）をクリックします。

ステップ 3 [デバイス（Device）] タブをクリックします。

ステップ 4 [システム（System）]セクションでデバイスのシャットダウンアイコン（ ）をクリックします。

ステップ 5 プロンプトが表示されたら、デバイスのシャットダウンを確認します。

ステップ 6 コンソールからファイアウォールに接続している場合は、ファイアウォールがシャットダウンするときにシステムプロンプトをモニターします。次のプロンプトが表示されます。

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

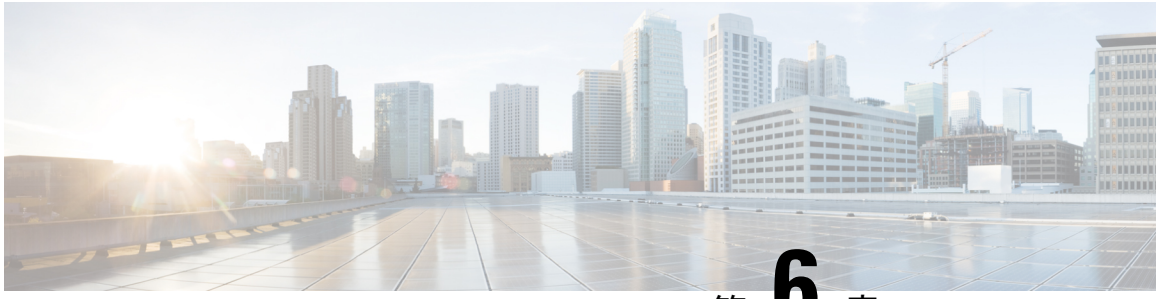
コンソールから接続していない場合は、約3分間待ってシステムがシャットダウンしたことを確認します。

ステップ 7 必要に応じて電源プラグを抜いてシャーシから物理的に電源を取り外すことができます。

次のステップ

CDO を使用した Threat Defense の設定を続行するには、Cisco Defense Orchestrator ホームページを参照してください。

次のステップ



第 6 章

ASDM を使用した ASA の展開

この章の対象読者

使用可能なすべてのオペレーティングシステムとマネージャを確認するには、「最適なオペレーティングシステムとマネージャを見つける方法 （1 ページ）」を参照してください。この章の内容は、ASDM を使用する ASA に適用されます。

この章では以下の展開については取り上げていませんので、『ASA コンフィギュレーションガイド』を参照してください。

- フェールオーバー
- CLI 設定

この章では、基本的なセキュリティポリシーの設定手順についても説明します。より高度な要件がある場合は設定ガイドを参照してください。

ファイアウォールについて

ハードウェアでは、Threat Defense ソフトウェアまたは ASA ソフトウェアを実行できます。Threat Defense と ASA の間で切り替えを行う際には、デバイスの再イメージ化が必要になります。現在インストールされているものとは異なるソフトウェアバージョンが必要な場合も再イメージ化が必要です。「Cisco ASA および Firepower Threat Defense 再イメージ化ガイド」を参照してください。

ファイアウォールは、Secure Firewall eXtensible オペレーティングシステム（FXOS）と呼ばれる基盤となるオペレーティングシステムを実行します。ファイアウォールは FXOS Secure Firewall Chassis Manager をサポートしていません。トラブルシューティング用として限られた CLI のみがサポートされています。詳細については、Firepower 1000/2100 および Secure Firewall 3100 と Firepower Threat Defense の Cisco FXOS トラブルシューティング ガイドを参照してください。

プライバシー収集ステートメント：ファイアウォールには個人識別情報は不要で、積極的に収集することもありません。ただし、ユーザー名などの設定では、個人識別情報を使用できます。この場合、設定作業時や SNMP の使用時に、管理者が個人識別情報を確認できる場合があります。

- ASA について （190 ページ）
- エンドツーエンドの手順 （193 ページ）

• ネットワーク配置とデフォルト設定の確認 （195 ページ）
• デバイスの配線 （198 ページ）
• ファイアウォールの電源の投入 （199 ページ）
• （任意）IP アドレスの変更 （200 ページ）
• ASDM へのログイン （201 ページ）
• ライセンスの設定 （202 ページ）
• ASA の設定 （208 ページ）
• ASA および FXOS CLI へのアクセス （210 ページ）
• 次のステップ （211 ページ）

ASA について

ASA は、1 つのデバイスで高度でステートフルなファイアウォール機能および VPN コンセントレーター機能を提供します。

次のいずれかのマネージャを使用して ASA を管理できます。

- ASDM（このガイドで説明）：デバイスに含まれる単独のデバイスマネージャ。
- CLI
- CDO：シンプルなクラウドベースのマルチデバイスマネージャ。
- Cisco Security Manager：別のサーバー上のマルチデバイス マネージャ。

トラブルシューティングのために、FXOS CLI にアクセスすることもできます。

サポートされない機能

ASA のサポートされない汎用機能

次の ASA 機能は、Firepower 1010 ではサポートされていません。

- マルチ コンテキスト モード
- アクティブ/アクティブ フェールオーバー
- 冗長インターフェイス
- クラスタ
- ASA REST API
- ASA FirePOWER module
- Botnet Traffic Filter
- 次のインスペクション：

- SCTP インスペクション マップ（ACL を使用した SCTP ステートフル インスペクションはサポートされます）
- Diameter
- GTP/GPRS

VLAN インターフェイスおよびスイッチ ポートでサポートされていない機能

VLAN インターフェイスおよびスイッチポートは、次の機能をサポートしていません。

- ダイナミック ルーティング
- マルチキャスト ルーティング
- ポリシーベース ルーティング
- 等コストマルチパス（ECMP）ルーティング
- インラインセットまたはパッシブインターフェイス
- VXLAN
- EtherChannel
- フェールオーバーおよびステートリンク
- トラフィック ゾーン
- セキュリティグループタグ（SGT）

ASA 5500-X 設定の移行

ASA 5500-X の設定をコピーして、Firepower 1010 に貼り付けることができます。ただし、設定を変更する必要があります。また、プラットフォーム間の動作の相違点に注意してください。

1. 設定をコピーするには、ASA 5500-X で **more system:running-config** コマンドを入力します。
2. 必要に応じて設定を編集します（以下を参照）。
3. Firepower 1010 のコンソールポートに接続し、グローバル コンフィギュレーション モードを開始します。

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa# configure terminal
ciscoasa(config)#
```

4. **clear configure all** コマンドを使用して、現在の設定をクリアします。

5. ASA CLI で変更された設定を貼り付けます。

このガイドでは、工場出荷時のデフォルト設定を前提としているため、既存の設定に貼り付ける場合、このガイドの一部の手順は ASA に適用されません。

ASA 5500-X 設定	Firepower 1010 の設定

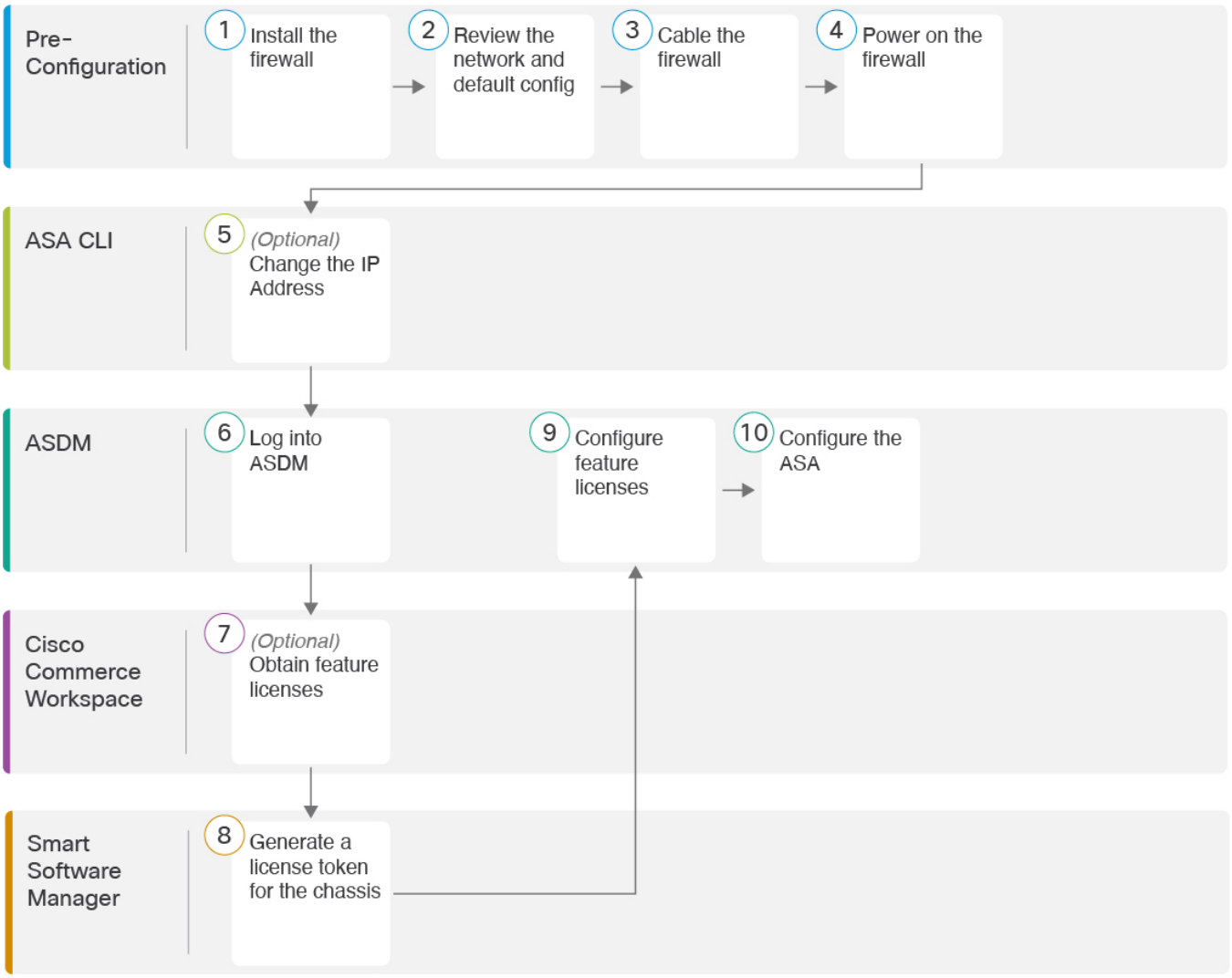
Ethernet 1/2 ～ 1/8 ファイアウォール インターフェイス	Ethernet 1/2 ～ 1/8 スイッチポート
	これらのイーサネットポートは、デフォルトではスイッチポートとして設定されています。設定内のインターフェイスごとに、通常のファイアウォール インターフェイスを作成するための **no switchport** コマンドを追加します。次に例を示します。
	`interface ethernet 1/2`
	`  no switchport`
	`  ip address 10.8.7.2 255.255.255.0`
	`  nameif inside`

PAK ライセンス	スマートライセンス 設定をコピーして貼り付けると、PAK ライセンスは適用されません。デフォルトではライセンスはインストールされていません。スマートライセンシングでは、スマートライセンシング サーバーに接続してライセンスを取得する必要があります。スマートライセンシングは、ASDM または SSH アクセスにも影響します（以下を参照）。
最初の ASDM アクセス	ASDM に接続できないか、スマート ライセンシング サーバーに登録できない場合は、弱い暗号化のみを設定した場合でも、VPN またはその他の強力な暗号化機能の設定を削除します。 強力な暗号化（3DES）ライセンスを取得した後に、これらの機能を再度有効にすることができます。 この問題の原因は、ASA には、管理アクセスに対してのみデフォルトで 3DES 機能が含まれていることです。強力な暗号化機能を有効にすると、ASDM および HTTPS トラフィック（スマートライセンシングサーバーとの間など）がブロックされます。このルールの例外は、管理 1/1 などの管理専用インターフェイスに接続されている場合です。SSH は影響を受けません。

ASA 5500-X 設定	Firepower 1010 の設定
インターフェイス ID	新しいハードウェア ID と一致するようにインターフェイス ID を変更してください。たとえば、ASA 5525-X には、Management 0/0、GigabitEthernet 0/0 ～ 0/5 が含まれています。Firepower 1120 には、Management 1/1 および Ethernet 1/1 ～ 1/8 が含まれています。
boot system コマンド ASA 5500-X では、最大 4 つの **boot system** コマンドを使用して、使用するブートイメージを指定できます。	Firepower 1010 では 1 つの **boot system** コマンドのみが許可されるため、貼り付ける前に 1 つ以外のすべてのコマンドを削除する必要があります。ブートイメージを判別するために起動時に読み込まれないため、実際に任意のコマンドを設定に含める必要はありません。 **boot system** リロード時には、最後にロードされたブート イメージが常に実行されます。 **boot system** コマンドは、入力時にアクションを実行します。システムはイメージを検証して解凍し、ブート場所（FXOS によって管理される disk0 の内部ロケーション）にコピーします。ASA をリロードすると、新しいイメージがロードされます。

エンドツーエンドの手順

シャーシで ASA を展開して設定するには、次のタスクを参照してください。



1	事前設定	ファイアウォールをインストールします。ハードウェア設置ガイド [英語] を参照してください。
2	事前設定	ネットワーク配置とデフォルト設定の確認 （195 ページ）。
3	事前設定	デバイスの配線 （198 ページ）。
4	事前設定	ファイアウォールの電源の投入 （13 ページ）
5	ASA CLI	（任意）IP アドレスの変更 （200 ページ）。
6	ASDM	ASDM へのログイン （201 ページ）。

7	Cisco Commerce Workspace	ライセンスの設定 （202 ページ）：機能ライセンスを取得します。
8	Smart Software Manager	ライセンスの設定 （202 ページ）：シャーシのライセンス トークンを生成します。
9	ASDM	ライセンスの設定 （202 ページ）：機能ライセンスを設定します。
10	ASDM	ASA の設定 （208 ページ）。

ネットワーク配置とデフォルト設定の確認

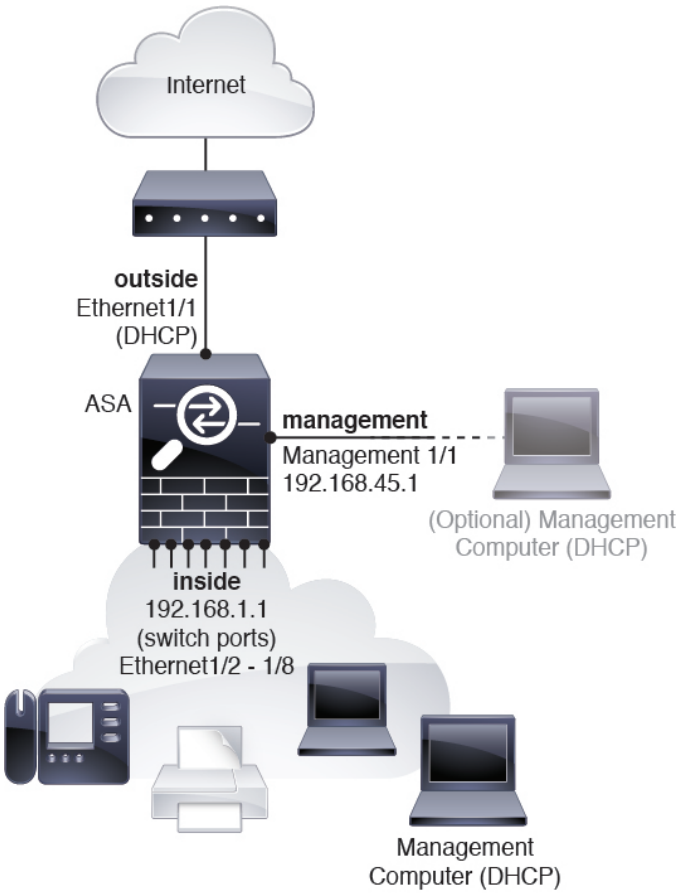
次の図は、Firepower 1010 でのデフォルトのネットワーク配置を示しています（デフォルト設定を使用）。

外部インターフェイスをケーブルモデムまたは DSL モデムに直接接続する場合は、ASA が内部ネットワークのすべてのルーティングと NAT を実行するように、モデムをブリッジモードにすることをお勧めします。外部インターフェイスが ISP に接続するために PPPoE を設定する必要がある場合は、その設定を ASDM スタートアップウィザード内で行うことができます。

（注） ASDM アクセスにデフォルト管理 IP アドレスを使用できない場合は、ASA CLI で管理 IP アドレスを設定できます。「（任意）IP アドレスの変更 （200 ページ）」を参照してください。

内部 IP アドレスを変更する必要がある場合は、ASDM スタートアップウィザードを使用して変更できます。たとえば、次のような状況において、内部 IP アドレスの変更が必要になる場合があります。

- 外部インターフェイスが一般的なデフォルトネットワークである 192.168.1.0 ネットワーク上の IP アドレスの取得を試みる場合、DHCP リースが失敗し、外部インターフェイスが IP アドレスを取得しません。この問題は、ASA が同じネットワーク上に 2 つのインターフェイスを持つことができないために発生します。この場合、内部 IP アドレスが新しいネットワーク上に存在するように変更する必要があります。
- ASA を既存の内部ネットワークに追加する場合は、内部 IP アドレスが既存のネットワーク上に存在するように変更する必要があります。



Firepower 1010 のデフォルト設定

Firepower 1010 の工場出荷時のデフォルト設定は、次のとおりです。

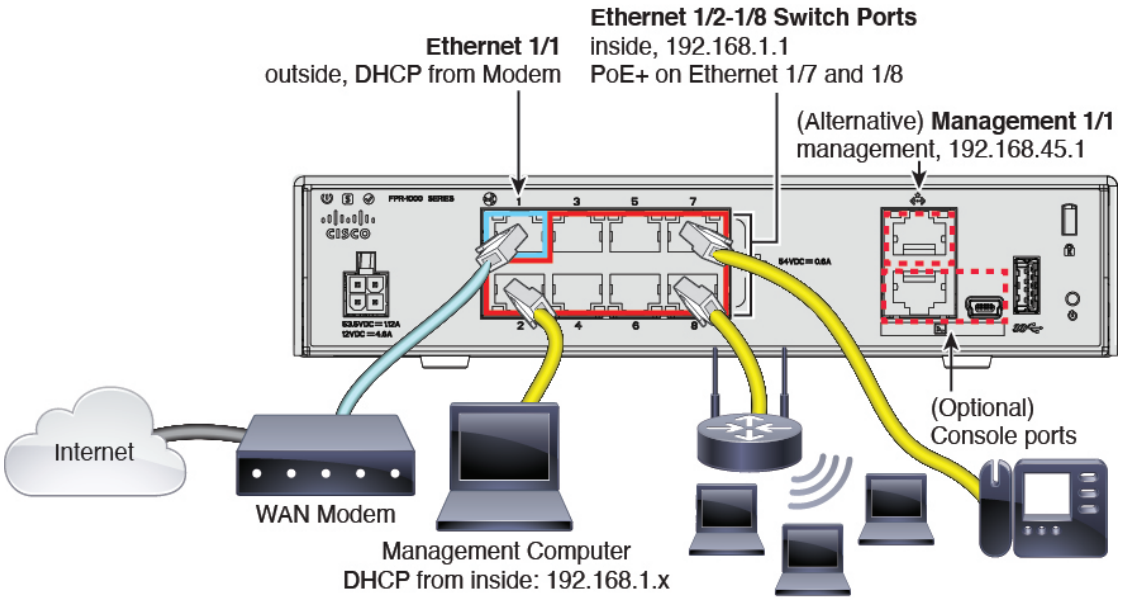
- **ハードウェア スイッチ**：イーサネット 1/2 ～ 1/8 は VLAN 1 に属しています。
- **内部から外部**へのトラフィック フロー：イーサネット 1/1（外部）、VLAN 1（内部）
- **管理**：管理 1/1（管理）、IP アドレス：192.168.45.1
- DHCP の**外部 IP アドレス**、内部 IP アドレス：192.168.1.1
- 内部インターフェイスの **DHCP サーバー**、管理インターフェイス
- 外部 DHCP からの**デフォルト ルート**
- **ASDM** アクセス：管理ホストと内部ホストに許可されます。管理ホストは 192.168.45.0/24 ネットワークに限定され、内部ホストは 192.168.1.0/24 ネットワークに限定されます。
- **NAT**：内部から外部へのすべてのトラフィック用のインターフェイス PAT。
- **DNS** サーバー：OpenDNS サーバーはあらかじめ構成されています。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface Management1/1
managment-only
nameif management
no shutdown
security-level 100
ip address 192.168.45.1 255.255.255.0
!
interface Ethernet1/1
nameif outside
ip address dhcp setroute
no shutdown
!
interface Ethernet1/2
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/3
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/4
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/5
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/6
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/7
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/8
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
object network obj_any
```

```
   subnet 0.0.0.0 0.0.0.0
   nat (any,outside) dynamic interface
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd address 192.168.45.10-192.168.45.12 management
dhcpd enable inside
dhcpd enable management
!
http server enable
http 192.168.45.0 255.255.255.0 management
http 192.168.1.0 255.255.255.0 inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

デバイスの配線



管理 1/1、またはイーサネット 1/2 ～ 1/8（内部スイッチ ポート）のいずれかで Firepower 1010 を管理します。デフォルト設定でも、イーサネット 1/1 は外部として設定されています。

手順

ステップ 1 ハードウェア設置ガイドを使用してハードウェアを設置し、ハードウェアについてよく理解しておきます。

ステップ 2 管理コンピュータを次のいずれかのインターフェイスに接続します。

- イーサネット 1/2 ～ 1/8：管理コンピュータをいずれかの内部スイッチ ポート（イーサネット 1/2 ～ 1/8）に直接接続します。内部インターフェイスにはデフォルトの IP アドレス（192.168.1.1）があり、クライアント（管理コンピュータを含む）に IP アドレスを提供するために DHCP サーバーも実行されるため、これらの設定が既存の内部ネットワークの設定と競合しないようにしてください（Firepower 1010 のデフォルト設定 （196 ページ）を参照）。
- 管理 1/1：管理コンピュータを管理 1/1 に直接接続します。または、管理 1/1 を管理ネットワークに接続します。管理ネットワーク上のクライアントだけが ASA にアクセスできるため、管理コンピュータが管理ネットワーク上にあることを確認します。管理 1/1 にはデフォルトの IP アドレス（192.168.45.1）があり、クライアント（管理コンピュータを含む）に IP アドレスを提供するために DHCP サーバーも実行されるため、これらの設定が既存の管理ネットワークの設定と競合しないようにしてください（Firepower 1010 のデフォルト設定 （196 ページ）を参照）。

  Management 1/1 の IP アドレスをデフォルトから変更する必要がある場合は、管理コンピュータをコンソールポートにケーブル接続する必要もあります。「（任意）IP アドレスの変更 （200 ページ）」を参照してください。

ステップ 3 外部ネットワークを Ethernet 1/1 インターフェイスに接続します。

スマート ソフトウェア ライセンシングの場合、ASA は License Authority にアクセスできるようにするためにインターネット アクセスを必要とします。

ステップ 4 内部デバイスを残りの内部スイッチ ポート（イーサネット 1/2 ～ 1/8）に接続します。

イーサネット 1/7 および 1/8 は PoE+ ポートです。

（注） PoE は Firepower 1010E ではサポートされていません。

ファイアウォールの電源の投入

システムの電源は電源コードで制御されます。電源ボタンはありません。

（注） Threat Defense を初めて起動するときは、初期化に約 15 ～ 30 分かかります。

始める前に

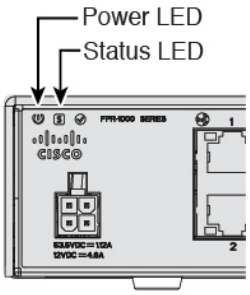
デバイスに対して信頼性の高い電力を供給することが重要です（たとえば、無停電電源装置（UPS）を使用）。最初のシャットダウンを行わないで電力が失われると、重大なファイルシステムの損傷を引き起こす可能性があります。バックグラウンドでは常に多数のプロセスが実行されていて、電力が失われると、システムをグレースフルシャットダウンできません。

手順

ステップ 1 電源コードをデバイスに接続し、電源コンセントに接続します。

電源コードを差し込むと電源が自動的に入ります。

ステップ 2 デバイスの背面または上部にある電源 LED を確認します。緑色に点灯している場合は、デバイスの電源が入っています。



ステップ 3 デバイスの背面または上部にあるステータス LED を確認します。緑色に点灯している場合は、電源投入時診断に合格しています。

（任意）IP アドレスの変更

ASDM アクセスにデフォルトの IP アドレスを使用できない場合は、ASA CLI で管理インターフェイスの IP アドレスを設定できます。

（注） この手順では、デフォルト設定を復元し、選択した IP アドレスも設定します。このため、保持する ASA 設定に変更を加えた場合は、この手順を使用しないでください。

手順

ステップ 1 ASA コンソールポートに接続し、グローバル コンフィギュレーション モードに入ります。詳細については、「ASA および FXOS CLI へのアクセス （210 ページ）」を参照してください。

ステップ 2 選択した IP アドレスを使用してデフォルト設定を復元します。

configure factory-default [*ip_address* [*mask*]]

例：

```
ciscoasa(config)# configure factory-default 10.1.1.151 255.255.255.0
Based on the management IP address and mask, the DHCP address
pool size is reduced to 103 from the platform limit 256
```

```
WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
Executing command: interface management1/1
Executing command: nameif management
INFO: Security level for "management" set to 0 by default.
Executing command: ip address 10.1.1.151 255.255.255.0
Executing command: security-level 100
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.1.1.0 255.255.255.0 management
Executing command: dhcpd address 10.1.1.152-10.1.1.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#
```

ステップ 3 デフォルト コンフィギュレーションをフラッシュメモリに保存します。

write memory

ASDM へのログイン

ASDM を起動して、ASA を設定できるようにします。

ASA には、管理アクセスのみを対象にした 3DES 機能がデフォルトで含まれているので、Smart Software Manager に接続でき、すぐに ASDM を使用することもできます。後に ASA で SSH アクセスを設定する場合は、SSH および SCP を使用することもできます。高度な暗号化を必要とするその他の機能（VPN など）では、最初に Smart Software Manager に登録する必要がある高度暗号化が有効になっている必要があります。

（注） 登録する前に高度な暗号化を使用できる機能の設定を試みると（脆弱な暗号化のみ設定している場合でも）、HTTPS 接続はそのインターフェイスでドロップされ、再接続できません。このルールの例外は、管理 1/1 などの管理専用インターフェイスに接続されている場合です。SSH は影響を受けません。HTTPS 接続が失われた場合は、コンソール ポートに接続して ASA を再設定するか、管理専用インターフェイスに接続するか、または高度暗号化機能用に設定されていないインターフェイスに接続することができます。

始める前に

- ASDM を実行するための要件については、Cisco.com の『ASDM リリース ノート』を参照してください。

手順

ステップ 1 ブラウザに次の URL を入力します。

- **https://192.168.1.1**：内部インターフェイスの IP アドレス。内部スイッチ ポート（Ethernet1/2 ～ 1/8）の内部アドレスに接続できます。
- **https://192.168.45.1**：管理インターフェイスの IP アドレス。

（注） **http://** や IP アドレス（デフォルトは HTTP）ではなく、必ず **https://** を指定してください。ASA は、HTTP リクエストを HTTPS に自動的に転送しません。

[Cisco ASDM] Web ページが表示されます。ASA に証明書がインストールされていないために、ブラウザのセキュリティ警告が表示されることがありますが、これらの警告は無視して、Web ページにアクセスできます。

ステップ 2 使用可能なオプション [Install ASDM Launcher] または [Run ASDM] のいずれかをクリックします。

ステップ 3 画面の指示に従ってオプションを選択し、ASDM を起動します。

[Cisco ASDM-IDM ランチャー（Cisco ASDM-IDM Launcher）] が表示されます。

ステップ 4 ユーザー名とパスワードのフィールドを空のままにして、[OK] をクリックします。

メイン ASDM ウィンドウが表示されます。

ライセンスの設定

ASA はスマート ライセンスを使用します。通常のスマートライセンシング（インターネットアクセスが必要）を使用できます。または、オフライン管理の場合、永続ライセンス予約または Smart Software Manager On-Prem（以前のサテライトサーバ）を設定できます。これらのオフラインライセンス方式の詳細については、「Cisco ASA シリーズの機能ライセンス」を参照してください。このガイドは通常のスマートライセンシングに適用されます。

シスコライセンスの概要については詳しくは、cisco.com/go/licensingguide を参照してください。

シャーシを登録すると、Smart Software Manager はファイアウォールと Smart Software Manager 間の通信用の ID 証明書を発行します。また、該当するバーチャルアカウントにファイアウォールが割り当てられます。Smart Software Manager に登録するまでは、設定変更を行うことはできず、特殊なライセンスを必要とする機能へ、操作はその他の点では影響を受けません。ライセンス付与される機能は次のとおりです。

- Essentials
- Security Plus：アクティブ/スタンバイ フェールオーバーの場合

- 高度な暗号化（3DES/AES）：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。
- Cisco Secure Client：Secure Client Advantage、Secure Client Premier、または Secure Client VPN のみ

ASA には、管理アクセスのみを対象にした 3DES 機能がデフォルトで含まれているので、Smart Software Manager に接続でき、すぐに ASDM を使用することもできます。後に ASA で SSH アクセスを設定する場合は、SSH および SCP を使用することもできます。高度な暗号化を必要とするその他の機能（VPN など）では、最初に Smart Software Manager に登録する必要がある高度暗号化が有効になっている必要があります。

（注） 登録する前に高度な暗号化を使用できる機能の設定を試みると（脆弱な暗号化のみ設定している場合でも）、HTTPS 接続はそのインターフェイスでドロップされ、再接続できません。このルールの例外は、管理 1/1 などの管理専用インターフェイスに接続されている場合です。SSH は影響を受けません。HTTPS 接続が失われた場合は、コンソール ポートに接続して ASA を再設定するか、管理専用インターフェイスに接続するか、または高度暗号化機能用に設定されていないインターフェイスに接続することができます。

Smart Software Manager から ASA の登録トークンを要求する場合、[このトークンを使用して登録した製品でエクスポート制御機能を許可（Allow export-controlled functionality on the products registered with this token）] チェックボックスをオンにして、強力な暗号化の完全ライセンスが適用されるようにします（ご使用のアカウントでその使用が許可されている必要があります）。強力な暗号化ライセンスは、シャーシで登録トークンを適用すると、対象となるお客様の場合自動的に有効化されるため追加の操作は不要です。スマートアカウントで強力な暗号化が許可されていないが、強力な暗号化の使用が許可されているとシスコが判断した場合、強力な暗号化ライセンスをアカウントに手動で追加できます。

始める前に

- Smart Software Manager にマスターアカウントを持ちます。

  まだアカウントをお持ちでない場合は、リンクをクリックして新しいアカウントを設定してください。Smart Software Manager では、組織のマスター アカウントを作成できます。

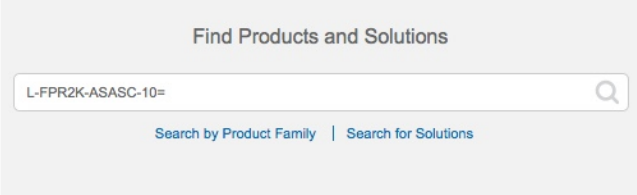
- （輸出コンプライアンスフラグを使用して有効化される）機能を使用するには、ご使用の Smart Software Manager アカウントで強力な暗号化（3DES/AES）ライセンスを使用できる必要があります。

手順

ステップ 1 ご使用のスマート ライセンス アカウントに、必要なライセンスが含まれている（少なくとも Essentials ライセンスが含まれている）ことを確認してください。

ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、Smart Software Manager アカウントにリンクされています。ただし、主導でライセンスを追加する必要がある場合は、Cisco Commerce Workspace で [製品とソリューションの検索（Find Products and Solutions）] 検索フィールドを使用します。次のライセンス PID を検索します。

図 *54* : ライセンス検索

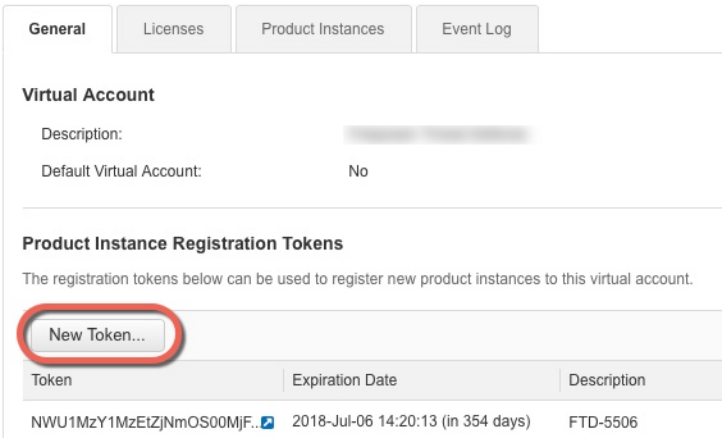


- Essentials ライセンス：L-FPR1000-ASA=。Essentials ライセンスは無料ですが、スマートソフトウェア ライセンシング アカウントに追加する必要があります。
- Security Plus ライセンス：L-FPR1010-SEC-PL=。Security Plus ライセンスによってフェールオーバーが有効になります。
- Strong Encryption（3DES/AES）license—L-FPR1K-ENC-K9=. アカウントに強力な暗号が承認されていない場合にのみ必要です。
- Cisco Secure Client：『Cisco Secure Client 発注ガイド』を参照してください。ASA では、このライセンスを直接有効にしないでください。

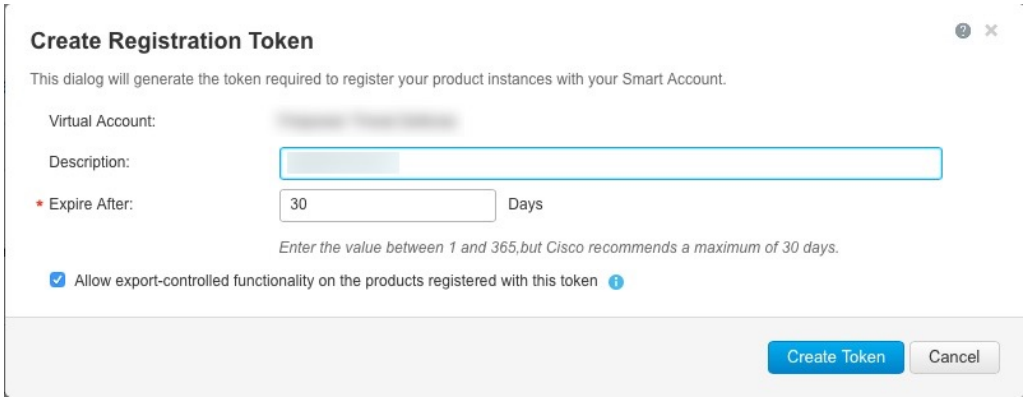
ステップ 2 Smart Software Manager で、このデバイスを追加する仮想アカウントの登録トークンを要求してコピーします。

a) [Inventory] をクリックします。

b) [General] タブで、[New Token] をクリックします。



c) [登録トークンを作成（Create Registration Token）] ダイアログボックスで、以下の設定値を入力してから [トークンを作成（Create Token）] をクリックします。



- **[説明（Description）]**
- [有効期限（Expire After）]：推奨値は 30 日です。
- [このトークンに登録された製品で輸出管理機能を許可する（Allow export-controlled functionality on the products registered with this token）]：輸出コンプライアンス フラグを有効にします。

トークンはインベントリに追加されます。

d) トークンの右側にある矢印アイコンをクリックして [トークン（Token）] ダイアログボックスを開き、トークン ID をクリップボードにコピーできるようにします。ASA の登録が必要なときに後の手順で使用するために、このトークンを準備しておきます。

図 *55 :* トークンの表示

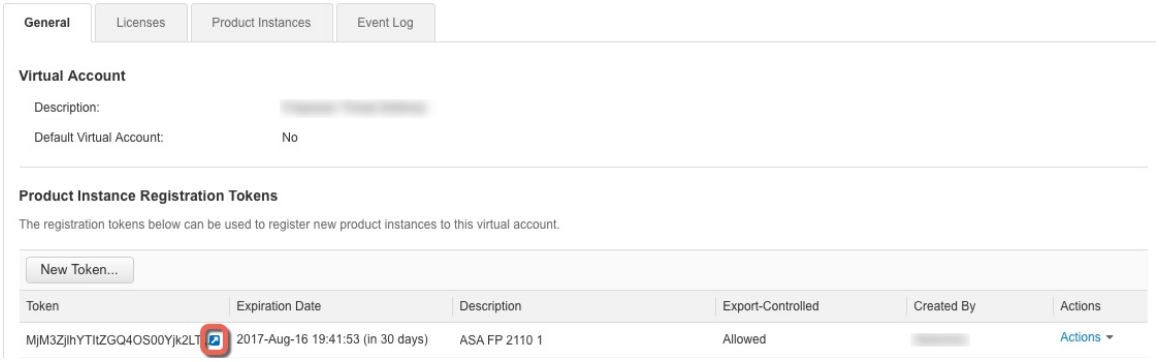
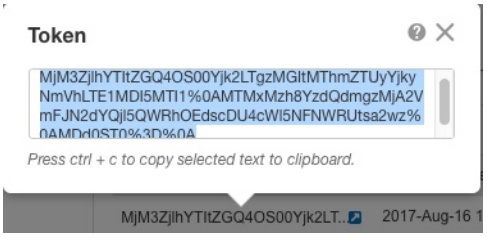
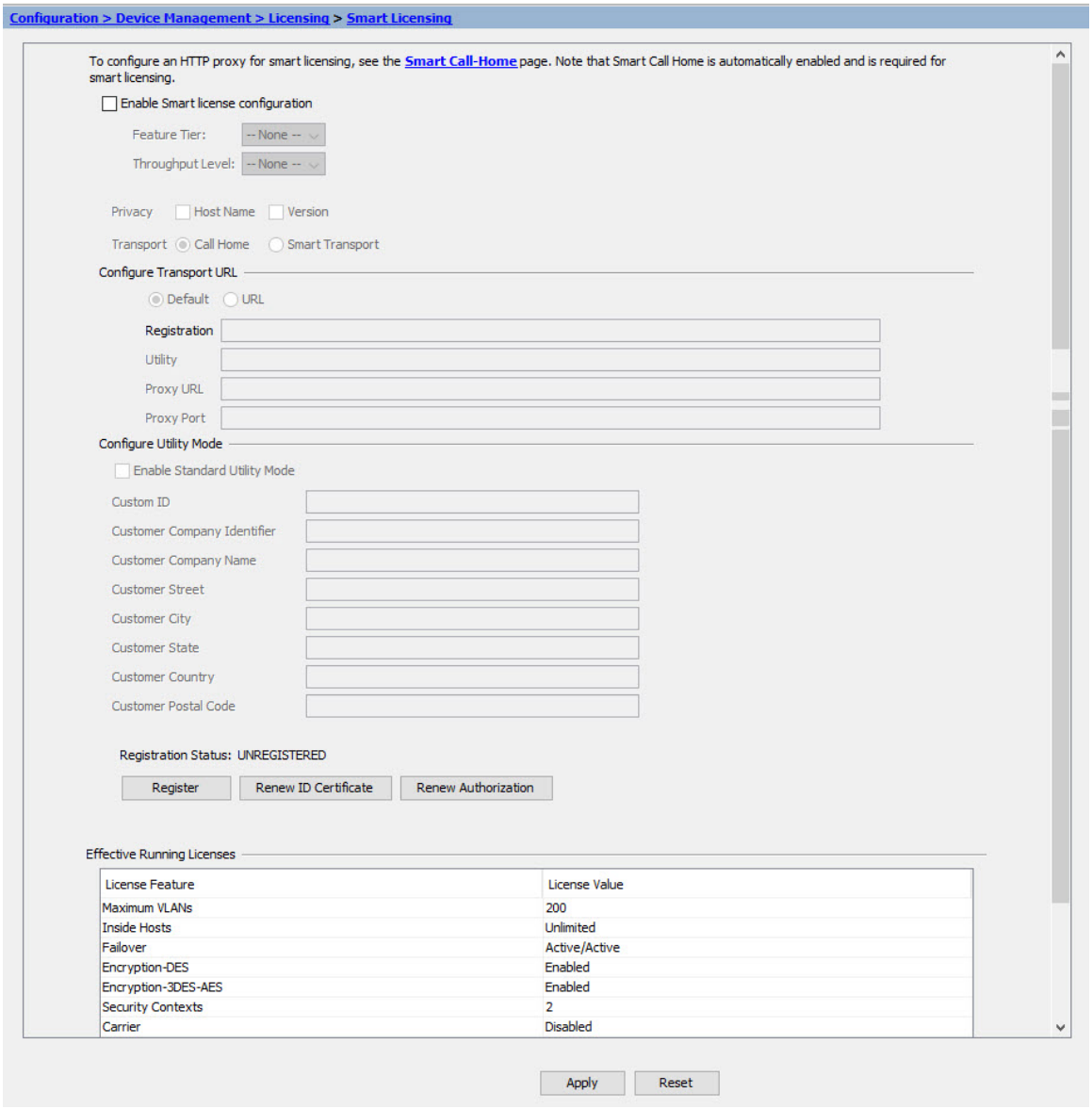


図 *56 :* トークンのコピー

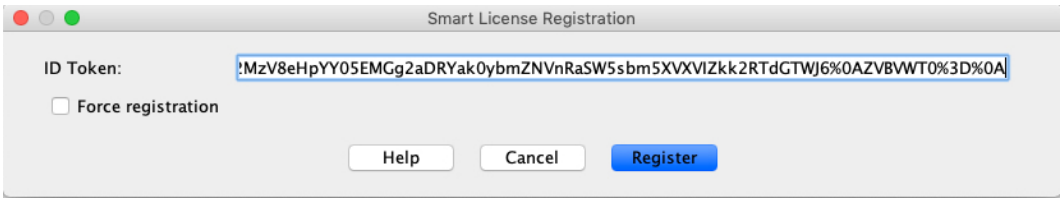


ステップ 3 ASDM で、**[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart Licensing]** の順に選択します。

ステップ 4 [Register] をクリックします。



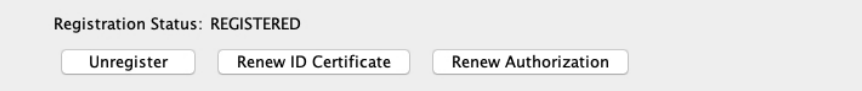
ステップ 5 [ID Token] フィールドに登録トークンを入力します。



必要に応じて、[登録を強制（Force registration）]チェックボックスをオンにして、Smart Software Manager と同期されていない可能性がある登録済みの ASA を登録します。たとえば、ASA が誤って Smart Software Manager から削除された場合に [登録を強制（Force registration） を使用します。

ステップ 6 [Register] をクリックします。

ASA は、事前設定された外部インターフェイスを使用して Smart Software Manager に登録し、設定済みソフトウェア利用資格の認証を要求します。Smart Software Manager は、ご使用のアカウントが許可すれば高度暗号化（3DES/AES）ライセンスも適用します。ライセンス ステータスが更新されると、ASDMによってページが更新されます。また、登録が失敗した場合などには、**[モニターリング（Monitoring）] > [プロパティ（Properties）] > [スマートライセンス（Smart License）]** の順に選択して、ライセンススタータスを確認できます。



ステップ 7 次のパラメータを設定します。

a) [Enable Smart license configuration] をオンにします。

b) [機能層（Feature Tier）] ドロップダウンリストから **[Essentials]** を選択します。

使用できるのは Essentials 層だけです。

c) （任意） [Security Plus の有効化（Enable Security Plus）] をオンにします。

Security Plus 層では、アクティブ/スタンバイ フェールオーバーが有効になります。

ステップ 8 [Apply] をクリックします。

ステップ 9 ツールバーの [Save] アイコンをクリックします。

ステップ 10 ASDM を終了し、再起動します。

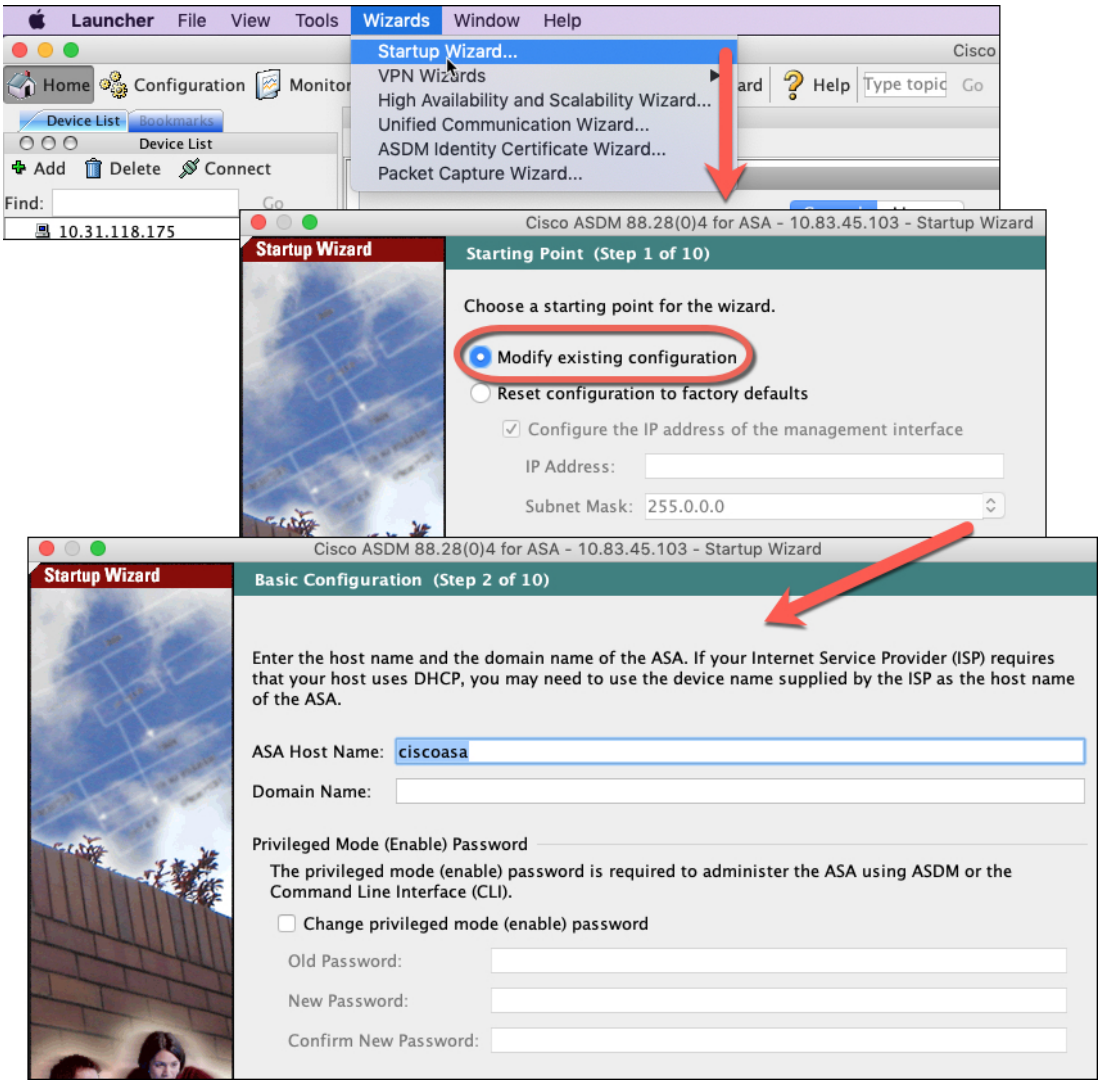
ライセンスを変更する場合、更新された画面を表示するには ASDM を再起動する必要があります。

ASA の設定

ASDMを使用する際、基本機能および拡張機能の設定にウィザードを使用できます。ウィザードに含まれていない機能を手動で設定することもできます。

手順

ステップ 1 [Wizards] > [Startup Wizard] の順に選択し、[Modify existing configuration] オプション ボタンをクリックします。



ステップ 2 [Startup Wizard] では、手順を追って以下を設定できます。

- イネーブル パスワード
- インターフェイス（内部および外部のインターフェイス IP アドレスの設定やインターフェイスの有効化など）
- スタティック ルート
- DHCP サーバー
- その他...

ステップ 3 （任意） [Wizards] メニューから、その他のウィザードを実行します。

ステップ 4 ASA の設定を続行するには、『Navigating the Cisco ASA Series Documentation』でソフトウェアバージョンに応じたマニュアルを参照してください。

ASA および FXOS CLI へのアクセス

ASDM を使用する代わりに、ASA CLI を使用して ASA のトラブルシューティングや設定を行うことができます。CLI には、コンソール ポートに接続してアクセスできます。後で任意のインターフェイスで ASA への SSH アクセスを設定できます。SSH アクセスはデフォルトで無効になっています。詳細については、ASA の一般的な操作の設定ガイドを参照してください。

トラブルシューティングのために、ASA CLI からも FXOS CLI にアクセスできます。

手順

ステップ 1 管理コンピュータをコンソール ポートに接続します。 Firepower 1000 には、USB A to B シリアル ケーブルが付属しています。ご使用のオペレーティングシステムに必要な USB シリアル ドライバを必ずインストールしてください（次を参照『Firepower 1010 hardware guide』）『。次のシリアル設定を使用します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

ASA CLI に接続します。デフォルトでは、コンソール アクセスに必要なユーザー クレデンシャルはありません。

ステップ 2 特権 EXEC モードにアクセスします。

enable

enable コマンドを最初に入力したときに、パスワードを変更するように求められます。

例：

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

ASA で設定したイネーブル パスワードは、FXOS **管理者**のユーザー パスワードでもあり、ASA の起動に失敗した場合は、FXOS フェールセーフ モードに移行します。

設定以外のすべてのコマンドは、特権EXECモードで使用できます。特権EXECモードからコンフィギュレーション モードに入ることもできます。

特権 EXEC モードを終了するには、**disable**、**exit**、または **quit** コマンドを入力します。

ステップ 3 グローバル コンフィギュレーション モードにアクセスします。

configure terminal

例：

```
ciscoasa# configure terminal
ciscoasa(config)#
```

グローバル コンフィギュレーション モードから ASA の設定を開始できます。グローバル コンフィギュレーション モードを終了するには、**exit**、**quit**、または **end** コマンドを入力します。

ステップ 4 （任意） FXOS CLI に接続します。

connect fxos [**admin**]

- **admin**：管理者レベルのアクセスを提供します。このオプションを指定しないと、ユーザーのアクセス権は読み取り専用アクセスになります。管理者モードであっても、コンフィギュレーション コマンドは使用できないことに注意してください。

ユーザーはクレデンシャルの入力を求められません。現在の ASA ユーザー名が FXOS に渡されるため、追加のログインは必要ありません。ASA CLI に戻るには、**exit** と入力するか、**Ctrl+Shift+6** を押し、**x** と入力します。

FXOS 内では、**scope security/show audit-logs** コマンドを使用してユーザーアクティビティを表示できます。

例：

```
ciscoasa# connect fxos admin
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
firepower#
firepower# exit
Connection with FXOS terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

次のステップ

- ASA の設定を続行するには、Cisco ASA シリーズの操作マニュアルの中から、お使いのソフトウェアバージョンに応じたマニュアルを参照してください。
- トラブルシューティングについては、『FXOS トラブルシューティング ガイド』を参照してください。

次のステップ

© 2023 Cisco Systems, Inc. All rights reserved.

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。