



Cisco Secure Firewall 4200 スタートアップガイド

初版：2023年9月7日

最終更新：2024年1月14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

最適なアプリケーション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つのアプリケーションのいずれかを実行できます。アプリケーションごとに、マネージャを選択できます。この章では、アプリケーションとマネージャの選択肢について説明します。

- [アプリケーション \(1 ページ\)](#)
- [マネージャ \(1 ページ\)](#)

アプリケーション

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) のいずれかのアプリケーションを使用できます。

- 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 —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。

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。

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 and Secure Firewall Threat Defense Reimage Guide](#)』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



(注) Secure Firewall Device Manager (旧 Firepower Device Manager) は、Cisco Secure Firewall 4200 ではサポートされていません。

表 1: Threat Defense マネージャ

マネージャ	説明
Secure Firewall Management Center (旧 Firepower Management Center)	<p>Management Center はマルチデバイスマネージャで、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。</p> <p>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)」を参照してください。</p> <p>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 (45 ページ)」を参照してください。</p>
Cisco Defense Orchestrator (CDO) クラウド提供型 Firewall Management Center	<p>CDO のクラウド提供型 Firewall Management Center には、オンプレミス管理センターのすべての設定機能があります。分析機能については、クラウドソリューションまたはオンプレミスの管理センターを使用できます。CDO は、ASA などの他のセキュリティデバイスも管理します。</p> <p>CDO プロビジョニングを開始するには、CDO での Threat Defense の展開 (91 ページ) を参照してください。</p>
Cisco Secure Firewall Threat Defense REST API	<p>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。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。</p> <p>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 ガイドを参照してください。</p>
Secure Firewall Management Center REST API	<p>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。</p> <p>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を参照してください。</p>

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)	<p>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。</p> <p>ASDM を使用する前に ASDM を使用した ASA の展開 (137 ページ) を参照してください。</p>
CLI	<p>CLI を使用して、すべての ASA 機能を設定できます。</p> <p>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。</p>
CDO	<p>CDO はクラウドベースのマルチデバイスマネージャです。CDO は Threat Defense などの他のセキュリティデバイスも管理します。</p> <p>ASA の 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。</p>
Cisco Security Manager (CSM)	<p>CSM は、独自のサーバーハードウェア上で動作するマルチデバイスマネージャです。CSM は Threat Defense の管理をサポートしていません。</p> <p>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。</p>
ASA HTTP インターフェイス	<p>HTTP を使用すると、自動化ツールは特定形式の URL にアクセスすることで、ASA でコマンドを実行できます。</p> <p>ASA HTTP インターフェイスについては、このガイドでは取り上げていません。詳細については、「自動化向けの Cisco Secure Firewall ASA HTTP インターフェイス」を参照してください。</p>



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アプリケーションとマネージャを表示するには、[最適なアプリケーション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 での脅威に対する防御の展開に適用されます。

この章では、脅威に対する防御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 \(45 ページ\)](#)」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 Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide](#) 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、[Cisco FXOS トラブルシューティング ガイド \(Firepower Threat Defense を実行している Firepower 1000/2100 および Cisco Secure Firewall 3100/4200 向け\)](#) 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はありません。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タスク (6 ページ)
- ネットワーク展開の確認 (8 ページ)
- ファイアウォールのケーブル接続 (10 ページ)
- ファイアウォールの電源投入 (12 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 (13 ページ)
- CLI を使用した Threat Defense 初期設定の実行の完了, on page 15
- Management Center へのログイン (19 ページ)
- Management Center のライセンスの取得 (19 ページ)
- Management Center への Threat Defense の登録 (21 ページ)
- 基本的なセキュリティポリシーの設定 (25 ページ)
- Threat Defense および FXOS CLI へのアクセス (41 ページ)
- ファイアウォールの電源の切断 (42 ページ)
- 次のステップ, on page 44

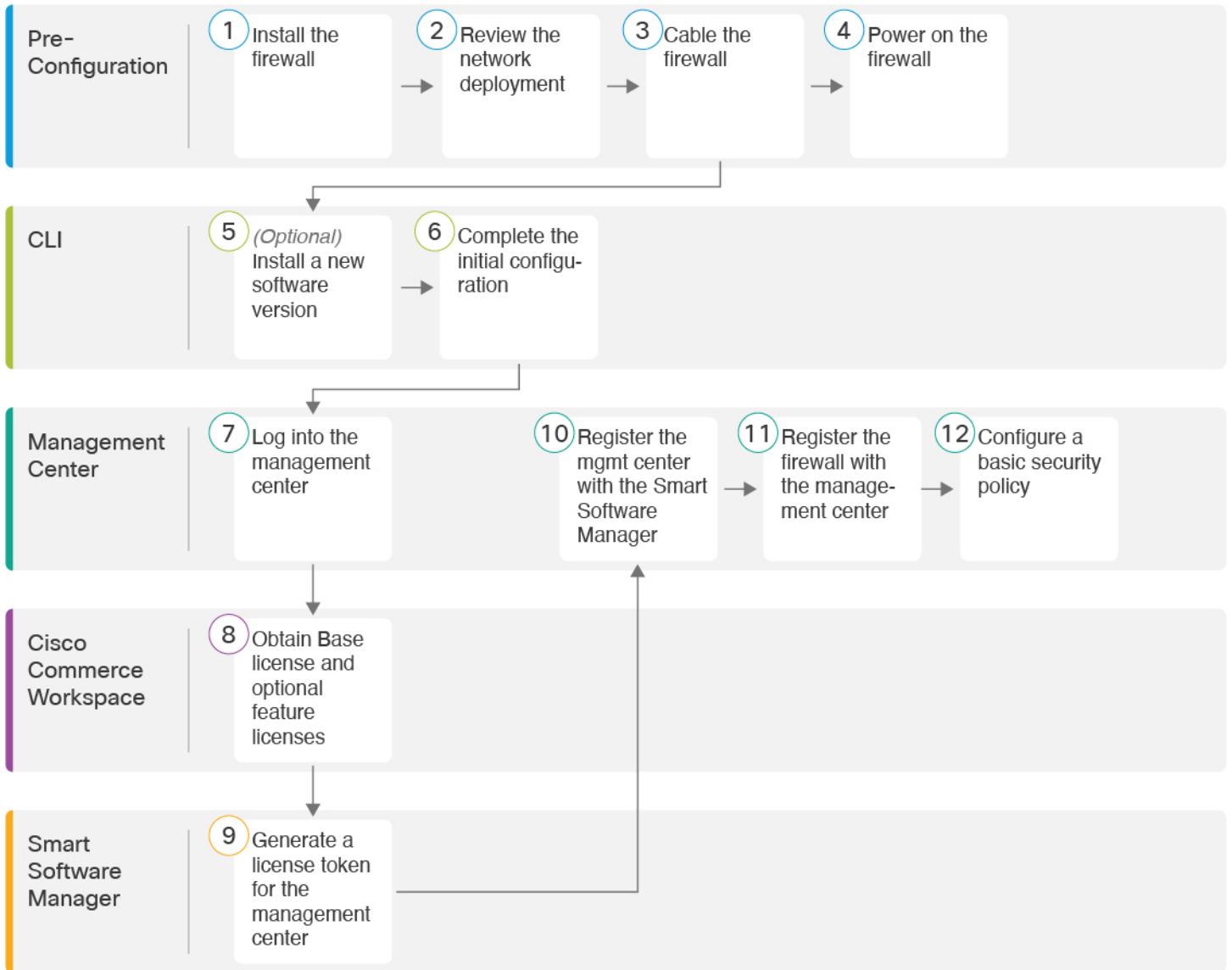
はじめる前に

Management Center の初期設定を展開して実行します。使用モデルのスタートアップガイドを参照してください。

エンドツーエンドのタスク

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 1: エンドツーエンドのタスク



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	ファイアウォールのケーブル接続 (10 ページ)。
④	事前設定	ファイアウォールの電源投入 (12 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 (13 ページ)。

⑥	CLI	CLI を使用した Threat Defense 初期設定の実行の完了 (15 ページ)。
⑦	Management Center	Management Centerへのログイン (19 ページ)。
⑧	Cisco Commerce Workspace	基本ライセンスとオプションの機能ライセンスを購入します (「Management Center のライセンスの取得 (19 ページ)」)。
⑨	Smart Software Manager	Management Center のライセンストークンを生成します (「Management Center のライセンスの取得 (19 ページ)」)。
⑩	Management Center	スマートライセンシングサーバーに Management Center を登録します (「Management Center のライセンスの取得 (19 ページ)」)。
⑪	Management Center	Management Center への Threat Defense の登録 (21 ページ)。
⑫	Management Center	基本的なセキュリティポリシーの設定 (25 ページ)。

ネットワーク展開の確認

管理インターフェイス

Management Center は管理インターフェイス上の Threat Defense と通信します。

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。

- 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。
- ライセンシングと更新を行うには、Threat Defense と Management Center の両方に管理インターフェイスからのインターネットアクセスが必要です。



(注) 管理接続は、それ自身とデバイス間の安全な TLS-1.3 暗号化通信チャネルです。セキュリティ上の理由から、サイト間 VPN などの追加の暗号化トンネル経由でこのトラフィックを実行する必要はありません。たとえば、VPN がダウンすると、管理接続が失われるため、シンプルな管理パスをお勧めします。

データ インターフェイス

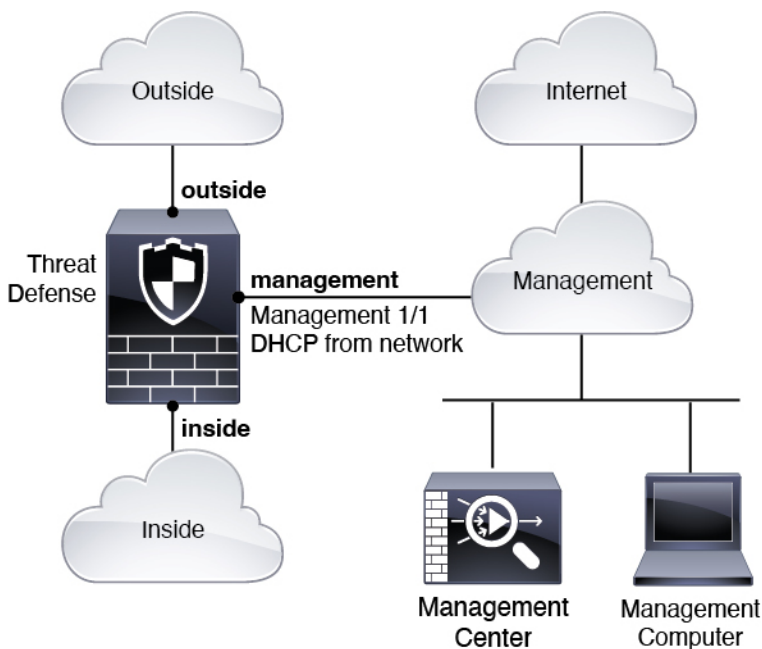
Threat Defense を Management Center に接続した後は、他のインターフェイスを設定できます。

一般的な個別の管理ネットワーク展開

次の図に、ファイアウォールの一般的なネットワーク展開を示します。

- Threat Defense、Management Center、および管理コンピュータは管理ネットワークに接続しています
- 管理ネットワークには、ライセンスと更新のためのインターネットへのパスがあります。

図 2: 個別の管理ネットワーク



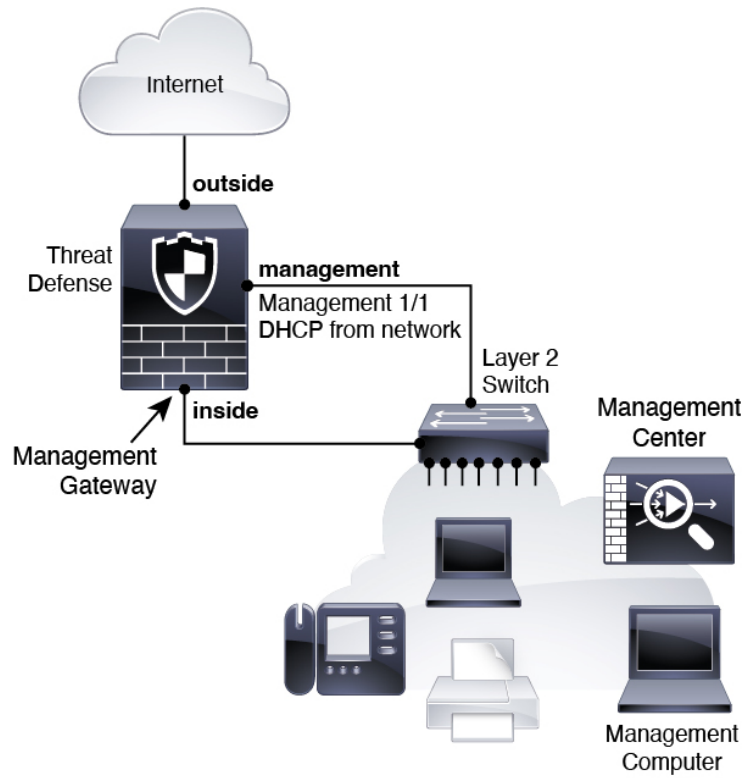
一般的なエッジネットワーク展開

次の図に、ファイアウォールの一般的なネットワーク展開を示します。

- 内部インターフェイスは、管理および Management Center のインターネットゲートウェイとして機能します。
- レイヤ 2 スイッチを介して、Management 1/1 を内部インターフェイスに接続しています。
- Management Center および管理コンピュータをスイッチとに接続しています。

管理インターフェイスには Threat Defense 上の他のインターフェイスとは別のルーティングがあるため、このような直接接続が許可されます。

図 3: エッジネットワークの展開



ファイアウォールのケーブル接続

Cisco Secure Firewall 4200 で推奨シナリオのいずれかに相当するケーブル接続を行うには、次の手順を参照してください。



(注) その他のトポロジも使用可能で、基本的な論理ネットワーク接続、ポート、アドレッシング、構成の要件によって導入方法が異なります。

始める前に

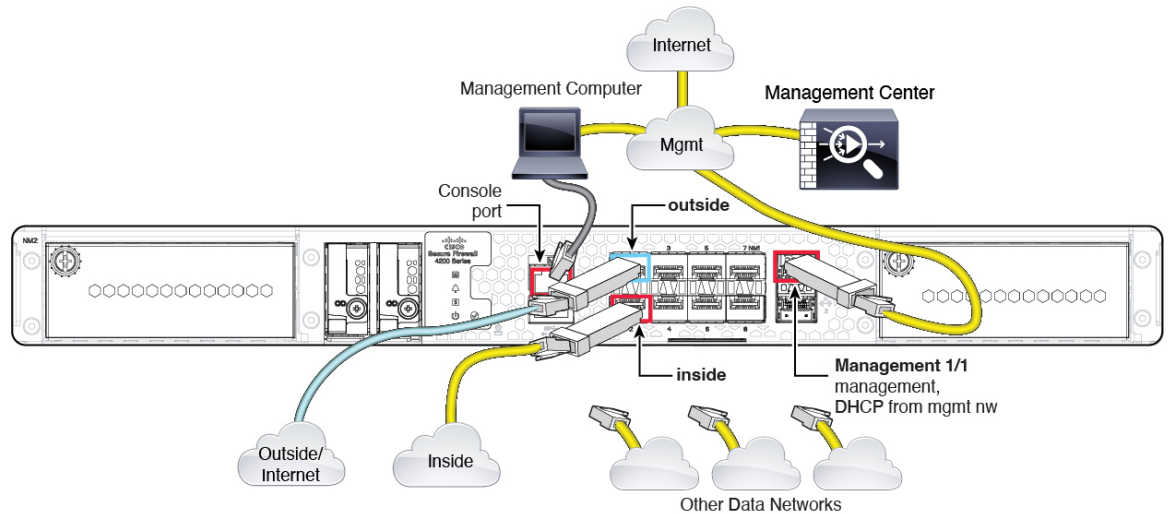
- 管理およびデータ インターフェイス ポートに SFP を取り付けます。組み込みポートは、SFP モジュールを必要とする 1/10/25 Gb SFP ポートです。
- コンソールケーブルを入手します。デフォルトではファイアウォールにコンソールケーブルが付属していないため、サードパーティの USB-to-RJ-45 シリアルケーブルなどを購入する必要があります。

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 別の管理ネットワーク用のケーブル配線：

図 4: 個別の管理ネットワークのケーブル配線



a) 次のように管理ネットワークにケーブルを配線します。

- Management 1/1 インターフェイス

Management Center に専用のイベントインターフェイスがある場合は、Management 1/2 インターフェイスを別のイベントインターフェイスとして使用できます。詳細については、Management Center の管理およびデバイス設定ガイドを参照してください。

- Secure Firewall Management Center
- 管理コンピュータ

b) 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。

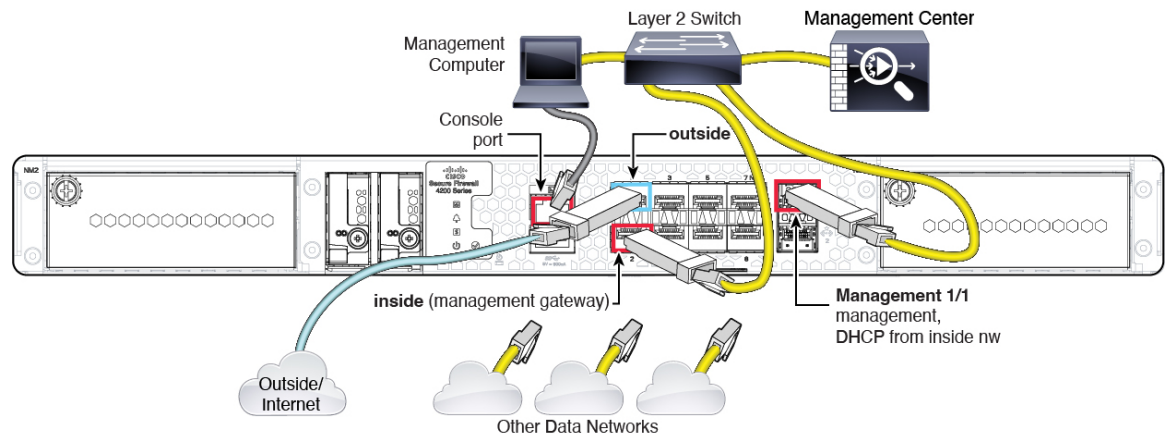
c) 内部インターフェイス (Ethernet 1/2 など) を内部ルータに接続します。

d) 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。

e) 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。

ステップ3 エッジ展開用のケーブル配線：

図 5: エッジ展開のケーブル配線



- a) 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 に専用のイベントインターフェイスがある場合は、Management 1/2 インターフェイスを別のイベントインターフェイスとして使用できます。詳細については、Management Center の管理およびデバイス設定ガイドを参照してください。

 - Secure Firewall Management Center
 - 管理コンピュータ
- b) 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。
- c) 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。
- d) 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投入

システムの電源は、ファイアウォールの背面にあるロッカー電源スイッチによって制御されます。電源スイッチは、ソフト通知スイッチとして実装されています。これにより、システムのグレースフルシャットダウンがサポートされ、システムソフトウェアおよびデータの破損のリスクが軽減されます。



(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。

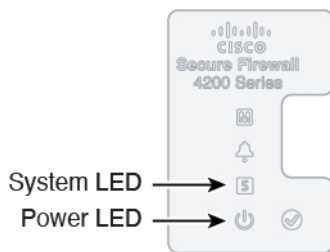
始める前に

ファイアウォールに対して信頼性の高い電力を供給することが重要です（無停電電源装置（UPS）を使用するなど）。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** 電源コードをファイアウォールに接続し、電源コンセントに接続します。
- ステップ 2** シャーシの背面で、電源コードに隣接する標準的なロッカータイプの電源オン/オフ スイッチを使用して電源をオンにします。
- ステップ 3** ファイアウォールの背面にある電源 LED を確認します。緑色に点灯している場合は、ファイアウォールの電源が入っています。

図 6: システムおよび電源 LED



- ステップ 4** ファイアウォールの背面にあるシステム LED を確認します。緑色に点灯している場合は、電源投入診断に合格しています。

(注) スイッチを ON から OFF に切り替えると、システムの電源が最終的に切れるまで数秒かかることがあります。この間は、シャーシの前面パネルの電源 LED が緑に点滅します。電源 LED が完全にオフになるまで電源を切らないでください。

(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 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 \(41 ページ\)](#) 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          7.4.0.65
7.4.0.65     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 \(15 ページ\)](#)」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。

ファイアウォールが再起動したら、FXOS CLI に再度接続します。

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。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。

Procedure

- 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。

Note 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。

Example:

```
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

Example:

```
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。

Note 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。

- [IPv4を設定しますか? (Do you want to configure IPv4?)]、[IPv6を設定しますか? (Do you want to configure IPv6?)]: これらのタイプのアドレスの少なくとも1つに **y** を入力します。
- 管理インターフェイスの **IPv4 デフォルトゲートウェイ** を入力または **管理インターフェイスの IPv6 ゲートウェイ** を入力: 管理ネットワークで Management 1/1 のゲートウェイ IP アドレスを設定します。「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。**data-interfaces** 設定は、リモート Management Center 管理にのみ適用されます。

- 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。
- [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。

Example:

```
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.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [y]: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'
[208.67.222.222,208.67.220.220,2620:119:35::35]:
Enter a comma-separated list of search domains or 'none' []:cisco.com
If your networking information has changed, you will need to reconnect.
Disabling IPv6 configuration: management0
Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
Setting DNS domains:cisco.com
Setting hostname as ftd-1.cisco.com
Setting static IPv4: 10.10.10.15 netmask: 255.255.255.192 gateway: 10.10.10.1 on
management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'

DHCP server is already disabled
DHCP Server Disabled
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

Device is in OffBox mode - disabling/removing port 443 from iptables.
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、少なくとも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нта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 (-) 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нта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 (-) 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。

Example:

```
> 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。

Example:

```
> 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。

Example:

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

What to do next

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 によって脅威に対する防御に提供されます。次のライセンスを購入できます。

- **Essentials** (必須) Essentials ライセンス。
- **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

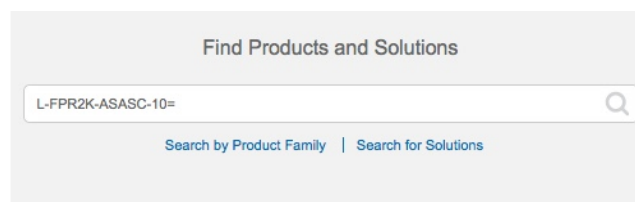
- **Smart Software Manager** にマスターアカウントを持ちます。
まだアカウントをお持ちでない場合は、リンクをクリックして**新しいアカウントを設定**してください。Smart Software Manager では、組織のマスター アカウントを作成できます。
- (輸出コンプライアンスフラグを使用して有効化される) 機能を使用するには、ご使用のスマートソフトウェア ライセンシング アカウントで強力な暗号化 (3DES/AES) ライセンスを使用できる必要があります。

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。

- Essentials ライセンス :
 - L-FPR4215-BSE=
 - L-FPR4225-BSE=
 - L-FPR4245-BSE=
- IPS、マルウェア防御、および URL ライセンスの組み合わせ :

- L-FPR4215T-TMC=
- L-FPR4225T-TMC=
- L-FPR4245T-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-FPR4215T-TMC-1Y
 - L-FPR4215T-TMC-3Y
 - L-FPR4215T-TMC-5Y
 - L-FPR4225T-TMC-1Y
 - L-FPR4225T-TMC-3Y
 - L-FPR4225T-TMC-5Y
 - L-FPR4245T-TMC-1Y
 - L-FPR4245T-TMC-3Y
 - L-FPR4245T-TMC-5Y
- キャリアライセンス :
 - L-FPR4200-FTD-CAR=
 - 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 まだ設定していない場合は、スマートライセンスサーバーに 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。
登録キー方式がデフォルトで選択されています。

図 8: 登録キーを使用したデバイスの追加

Add Device

Select the Provisioning Method:

Registration Key Serial Number

CDO Managed Device

Host:†
10.89.5.40

Display Name:
10.89.5.40

Registration Key:*
....

Group:
None

Access Control Policy:*
inside-outside

Smart Licensing

Note: All virtual Firewall Threat Defense devices require a performance tier license. Make sure your Smart Licensing account contains the available licenses you need. It's important to choose the tier that matches the license you have in your account. Click [here](#) for information about the Firewall Threat Defense performance-tiered licensing. Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.

Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):
Select a recommended Tier

Carrier
 Malware Defense
 IPS
 URL

Advanced

Unique NAT ID:†
test

Transfer Packets

Cancel Register

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一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 \(38 ページ\)](#)」を参照してください。

図 9: New Policy

The screenshot shows the 'New Policy' configuration interface. It includes the following elements:

- Name:** A text input field containing 'ftd-ac-policy'.
- Description:** An empty text input field.
- Select Base Policy:** A dropdown menu currently set to 'None'.
- Default Action:** Three radio button options:
 - Block all traffic (highlighted with a red box)
 - Intrusion Prevention
 - Network Discovery
- Buttons:** 'Cancel' and 'Save' buttons located at the bottom right of the form.

- **スマートライセンス** : 展開する機能に必要なスマートライセンスを割り当てます。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、正常に登録され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 (26 ページ)。
②	DHCP サーバーの設定 (31 ページ)。
③	デフォルトルートの追加 (33 ページ)。
④	NAT の設定 (35 ページ)。
⑤	内部から外部へのトラフィックの許可 (38 ページ)。
⑥	設定の展開 (39 ページ)。

インターフェイスの設定

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。ブレイクアウトポートも設定します。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。

図 10: [インターフェイス (Interfaces)]

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Management0/0	management	Physical				Disabled	Global	🔍 ↕
 GigabitEthernet0/0		Physical				Disabled		✎
 GigabitEthernet0/1		Physical				Disabled		✎
 GigabitEthernet0/2		Physical				Disabled		✎
 GigabitEthernet0/3		Physical				Disabled		✎
 GigabitEthernet0/4		Physical				Disabled		✎
 GigabitEthernet0/5		Physical				Disabled		✎
 GigabitEthernet0/6		Physical				Disabled		✎
 GigabitEthernet0/7		Physical				Disabled		✎

ステップ 3 40 Gb 以上のインターフェイスからブレイクアウトポートを作成するには、インターフェイスの [ブレイク (Break)] アイコンをクリックします。

設定でフルインターフェイスをすでに使用している場合は、ブレイクアウトを続行する前に設定を削除する必要があります。

ステップ 4 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。

図 11 : [General] タブ

Edit Physical Interface

General IPv4 IPv6 Path Monitoring

Name:

Enabled
 Management Only

Description:

Mode:

Security Zone:

Interface ID:

MTU:

(64 - 9000)

Priority:
 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

- 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。
- [有効 (Enabled)] チェックボックスをオンにします。
- [モード (Mode)] は [なし (None)] に設定したままにします。
- [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せんが、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。

図 12: [IPv4] タブ

The screenshot shows the 'Edit Physical Interface' configuration page with the 'IPv4' tab selected. The 'IP Type' dropdown menu is set to 'Use Static IP'. Below it, the 'IP Address' field contains the text '192.168.1.1/24'. A small example text below the field reads 'eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25'.

- [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。

図 13: [IPv6] タブ

The screenshot shows the 'Edit Physical Interface' configuration page with the 'IPv6' tab selected. The 'Basic' sub-tab is active. The 'Enable IPV6:' checkbox is unchecked. The 'Enforce EUI 64:' checkbox is unchecked. The 'Link-Local address:' field is empty. The 'Autoconfiguration:' checkbox is checked. The 'Obtain Default Route:' checkbox is unchecked.

f) [OK] をクリックします。

ステップ 5 「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。

図 14: [General] タブ

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware

Name:

Enabled
 Management Only

Description:

Mode:

Security Zone:

Interface ID:

MTU:

(64 - 9000)

Priority:
 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

- 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。

図 15: [IPv4] タブ

Edit Physical Interface

General IPv4 IPv6 Path Mc

IP Type:
Use DHCP

Obtain default route using DHCP:

DHCP route metric:
1
(1 - 255)

- [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。

図 16: [IPv6] タブ

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware Configu

Basic Address Prefixes Settings DHCP

Enable IPV6:

Enforce EUI 64:

Link-Local address:

Autoconfiguration:

Obtain Default Route:

f) [OK] をクリックします。

ステップ 6 [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 を使用して脅威に対する防御から 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。

図 17: DHCP サーバー

The screenshot shows the DHCP configuration interface. On the left, there is a sidebar with options: DHCP Server, DHCP Relay, and DDNS. The main area is titled 'DHCP' and contains several configuration fields: Ping Timeout (50), Lease Length (3600), Auto-Configuration (unchecked), and Interface (dropdown). Below these are 'Override Auto Configured Settings' for Domain Name, Primary DNS Server, Secondary DNS Server, Primary WINS Server, and Secondary WINS Server. At the bottom, there are tabs for 'Server' and 'Advanced', and a table with columns 'Interface', 'Address Pool', and 'Enable DHCP Server'. A red box highlights the '+ Add' button in the bottom right corner of the table area.

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。

図 18: サーバーの追加 (Add Server)

The 'Add Server' dialog box contains the following fields: Interface* (dropdown menu with 'inside' selected), Address Pool* (text input with '10.9.7.9-10.9.7.25' and '(2.2.2.10-2.2.2.20)' below it), and a checked checkbox for 'Enable DHCP Server'. At the bottom, there are 'Cancel' and 'OK' buttons.

- [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

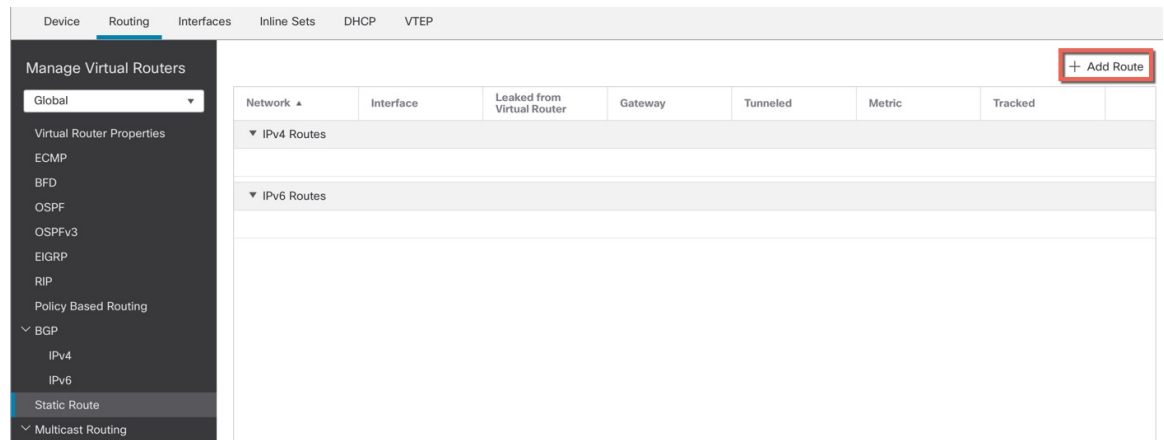
デフォルトルートは通常、外部インターフェイスから到達可能なアップストリームルータを指し示します。外部インターフェイスに DHCP を使用する場合は、デバイスがすでにデフォルトルートを受信している可能性があります。手動でルートを追加する必要がある場合は、次の手順を実行します。DHCP サーバーからデフォルトルートを受信した場合は、[デバイス (Devices)]>[デバイス管理 (Device Management)]>[ルーティング (Routing)]>[スタティックルート (Static Route)]ページの [IPv4ルート (IPv4 Routes)]または [IPv6ルート (IPv6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

図 19: Static Route



ステップ 3 [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。

図 20: 静的ルート追加の設定

Add Static Route Configuration

Type: IPv4 IPv6

Interface*
outside

(Interface starting with this icon signifies it is available for route leak)

Available Network +

Search

any-ipv4

IPv4-Benchmark-Tests

IPv4-Link-Local

IPv4-Multicast

IPv4-Private-10.0.0.0-8

IPv4-Private-172.16.0.0-12

Add

Selected Network

any-ipv4

Gateway*
default-gateway +

Metric:
1

(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:
+

Cancel OK

- [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 4 [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 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。

図 21: New Policy

New Policy

Name:
interface_PAT

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

Selected Devices

Search by name or value

10.10.0.6
10.10.0.7

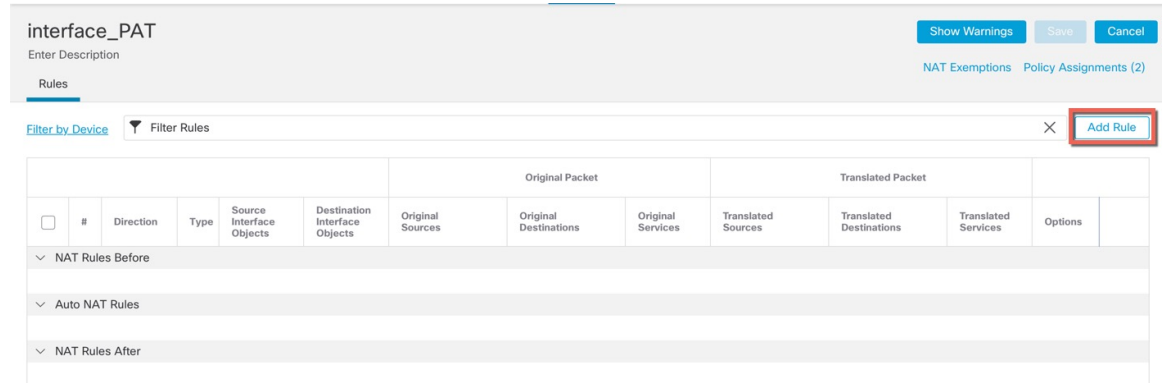
Add to Policy

10.10.0.6
10.10.0.7

Cancel Save

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。

図 22: NAT ポリシー

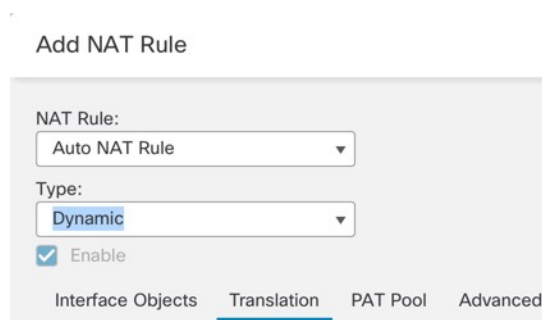


ステップ 3 [ルールの追加 (Add Rule)] をクリックします。

[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。

図 23: 基本ルールのオプション



- [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。

図 24: インターフェイス オブジェクト

The screenshot shows the 'Add NAT Rule' configuration page. The 'NAT Rule' is set to 'Auto NAT Rule' and 'Type' is 'Dynamic'. The 'Enable' checkbox is checked. The 'Interface Objects' tab is active. Under 'Available Interface Objects', 'outside_zone' is selected (1) and 'Add to Destination' is clicked (2). 'outside_zone' is now in the 'Destination Interface Objects' list (3).

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。

図 25: トランスレーション (Translation)

The screenshot shows the 'Add NAT Rule' configuration page, 'Translation' tab. The 'Original Source' is set to 'all-ipv4' and the 'Translated Source' is set to 'Destination Interface IP'. A note indicates that the values selected for Destination Interface Objects in the 'Interface Objects' tab will be used.

- [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。

図 26: 新しいネットワークオブジェクト

(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

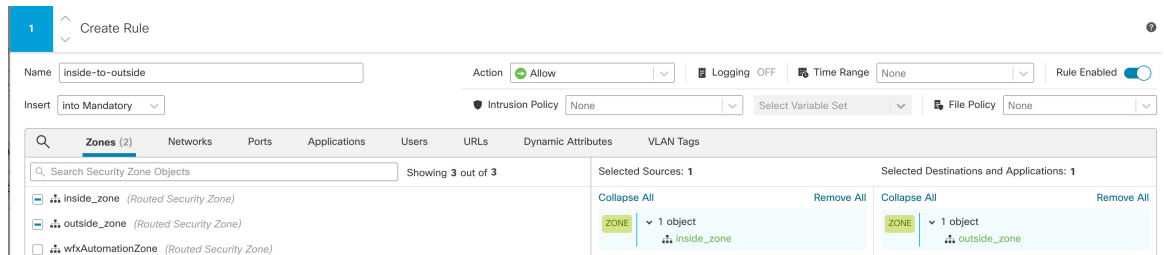
脅威に対する防御 を登録したときに、基本の [すべてのトラフィックをブロック (Block all traffic)] アクセス コントロール ポリシーを作成した場合は、デバイスを通るトラフィックを許可するためにポリシーにルールを追加する必要があります。次の手順では、内部ゾーンから外部ゾーンへのトラフィックを許可するルールを追加します。他にゾーンがある場合は、適切なネットワークへのトラフィックを許可するルールを追加してください。

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、脅威に対する防御 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。

図 27: [ルールを追加 (Add Rule)]



- [名前 (Name)] : このルールに名前を付けます (たとえば、**inside-to-outside**) 。
- [選択した送信元 (Selected Sources)] : [ゾーン (Zones)] から内部ゾーンを選択し、[送信元ゾーンを追加 (Add Source Zone)] をクリックします。
- [選択した宛先とアプリケーション (Selected Destinations and Applications)] : [ゾーン (Zones)] から外部ゾーンを選択し、[宛先ゾーンを追加 (Add Destination Zone)] 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 [Apply] 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

設定の変更を脅威に対する防御に展開します。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 28: [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 29:すべて展開

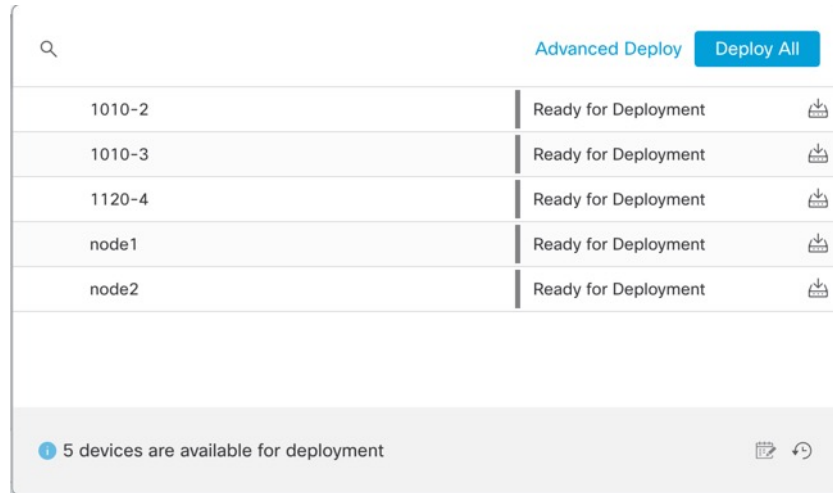


図 30:高度な展開

1 device selected

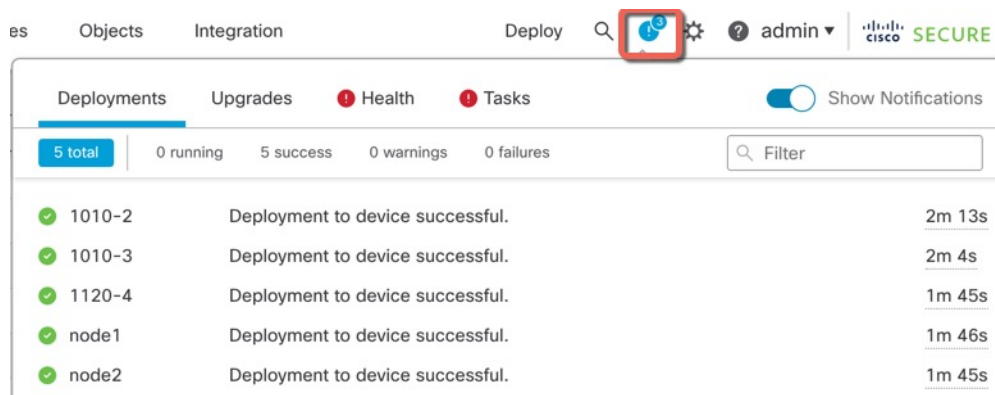
Search using device name, user name, type, group or status

Deploy time: Estimate Deploy

Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
<input checked="" type="checkbox"/> node1	System		FTD		May 23, 2022 6:49 PM		Ready for Deployment
<input type="checkbox"/> 1010-2	admin, System		FTD		May 23, 2022 7:09 PM		Ready for Deployment
<input type="checkbox"/> node2	System		FTD		May 23, 2022 6:49 PM		Ready for Deployment
<input type="checkbox"/> 1010-3	System		FTD		May 23, 2022 6:49 PM		Ready for Deployment
<input type="checkbox"/> 1120-4	System		FTD		May 23, 2022 6:49 PM		Ready for Deployment

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 31: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。デフォルトでは Cisco Secure Firewall 4200 にコンソールケーブルが付属していないため、サードパーティの USB-to-RJ-45 シリアルケーブルなどを購入する必要があります。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。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、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、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。

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 [デバイス (Devices)] > [デバイス管理 (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 (Edit)] (✎) 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 (Shut Down Device)] (✕) 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 必要に応じて電源スイッチをオフにし、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 におけるファイアウォールの電源の切断

FXOS CLI を使用すると、システムを安全にシャットダウンしてデバイスの電源を切断できます。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 \(41 ページ\)](#) 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 必要に応じて電源スイッチをオフにし、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 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アプリケーションとマネージャを表示するには、[最適なアプリケーション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 脅威に対する防御 に適用されます。

各脅威に対する防御は、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 Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide](#) 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、[Cisco FXOS トラブルシューティングガイド](#)

([Firepower Threat Defense を実行している Firepower 1000/2100 および Cisco Secure Firewall 3100/4200 向け](#)) 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はありません。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 \(46 ページ\)](#)
- [はじめる前に \(48 ページ\)](#)
- [エンドツーエンドのタスク \(49 ページ\)](#)

- 中央の管理者による事前設定 (50 ページ)
- 支社へのインストール (58 ページ)
- 中央の管理者による事後設定 (60 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、Management Center マネージャアクセスについて管理インターフェイスの代わりに外部インターフェイスを使用します。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) 管理接続は、それ自身とデバイス間の安全な TLS-1.3 暗号化通信チャンネルです。セキュリティ上の理由から、サイト間 VPN などの追加の暗号化トンネル経由でこのトラフィックを実行する必要はありません。たとえば、VPN がダウンすると、管理接続が失われるため、シンプルな管理パスをお勧めします。

- 中央の本社の管理者が、CLI 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、脅威に対する防御 をケーブルで接続して電源をオンにします。
- 中央管理者は、Management Center を使用して 脅威に対する防御 の登録を完了します。

Threat Defense マネージャ アクセス インターフェイス

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。これは、リモート分散拠点で発生する可能性が最も高いシナリオであるためです。マネージャアクセスは外部インターフェイスで発生しますが、専用の管理インターフェイスも引き続き関連します。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。

マネージャのアクセス要件

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はできません。
- 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。
- 管理インターフェイスとイベント専用インターフェイスを別々に使用することはできません。
- クラスタリング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。

ハイ アベイラビリティ要件

デバイスのハイアベイラビリティを備えたデータインターフェイスを使用する場合は、次の要件を参照してください。

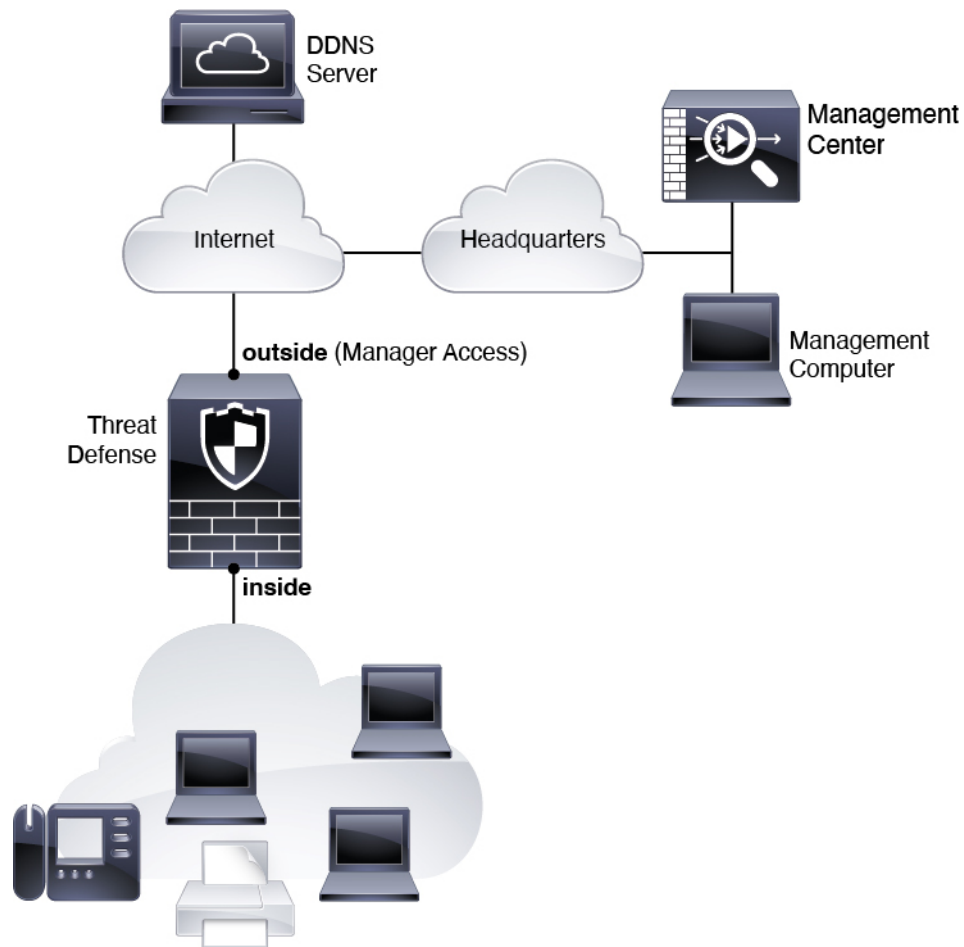
- マネージャアクセスには、両方のデバイスで同じデータインターフェイスを使用します。
- 冗長マネージャアクセス データ インターフェイスはサポートされていません。
- DHCP は使用できません。静的 IP アドレスのみがサポートされています。DDNS やロータッチプロビジョニングなど、DHCP に依存する機能は使用できません。
- 同じサブネット内に異なる静的 IP アドレスがあります。
- IPv4 または IPv6 のいずれかを使用します。両方を設定することはできません。
- 同じマネージャ設定 (**configure manager add** コマンド) を使用して、接続が同じであることを確認します。
- データインターフェイスをフェールオーバーリンクまたはステートリンクとして使用することはできません。

リモート ブランチ ネットワーク

次の図に、ファイアウォールの一般的なネットワーク展開を示します。

- Management Center は中央本社にあります。
- Threat Defense はマネージャアクセスに外部インターフェイスを使用します。
- 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 32:



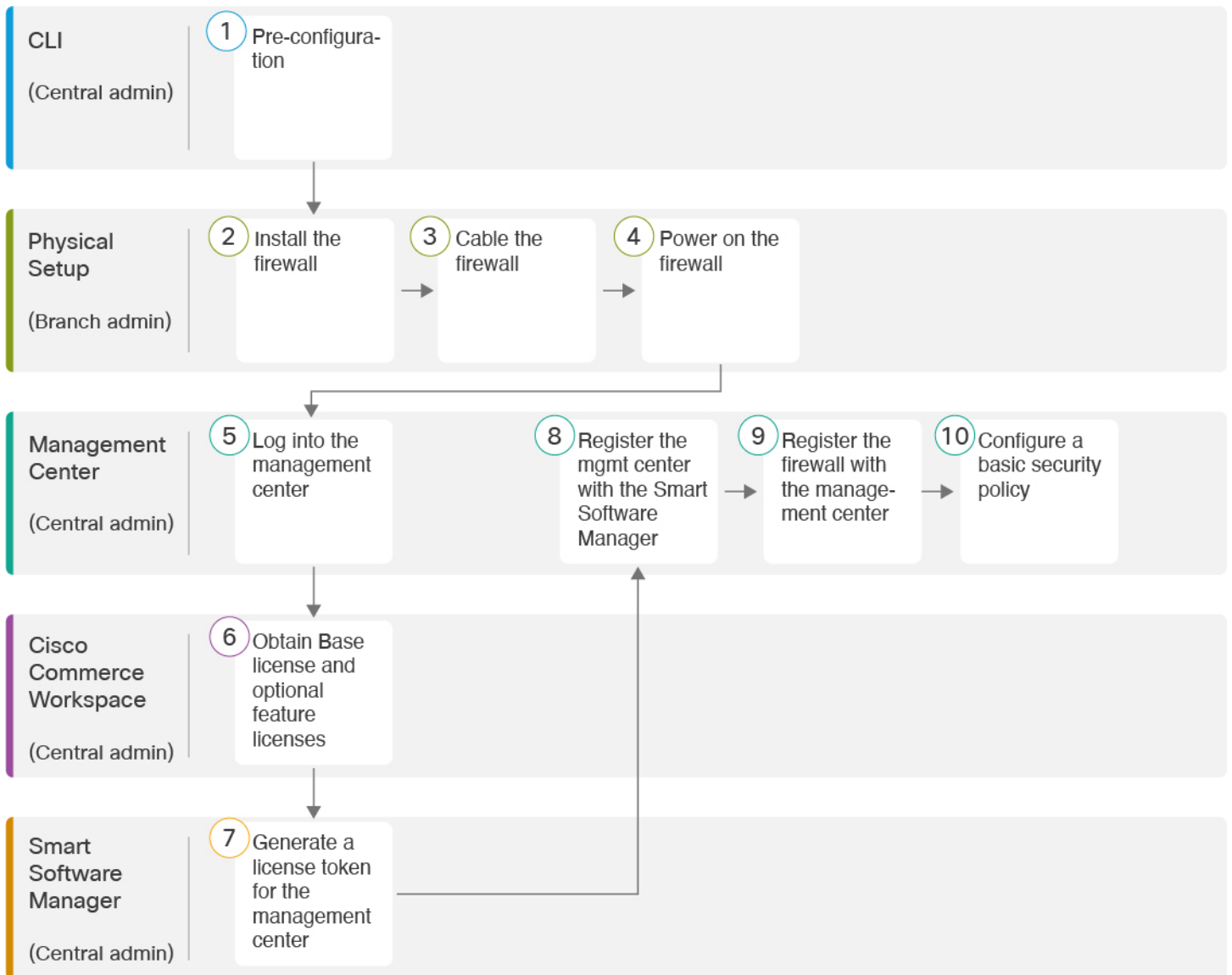
はじめる前に

Management Center の初期設定を展開して実行します。使用モデルのスタートアップガイドを参照してください。

エンドツーエンドのタスク

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 33: エンドツーエンドのタスク



1	CLI (中央の管理者)	<ul style="list-style-type: none"> • (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 (50 ページ) • CLI を使用した事前設定 (52 ページ)。
---	-----------------	--

中央の管理者による事前設定

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 (58 ページ) 。
④	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電源投入 (59 ページ)
⑤	Management Center (中央の管理者)	Management Centerへのログイン (19 ページ) 。
⑥	Cisco Commerce Workspace (中央の管理者)	基本ライセンスとオプションの機能ライセンスを購入します (「 Management Centerのライセンスの取得 (61 ページ) 」)。
⑦	Smart Software Manager (中央の管理者)	Management Center のライセンストークンを生成します (「 Management Center のライセンスの取得 (61 ページ) 」)。
⑧	Management Center (中央の管理者)	スマート ライセンシング サーバーに Management Center を登録します (「 Management Center のライセンスの取得 (61 ページ) 」)。
⑨	Management Center (中央の管理者)	Management Center へのデバイスの追加 (63 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 (66 ページ) 。

中央の管理者による事前設定

Threat Defense は、分散拠点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 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 \(80 ページ\)](#) 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	7.4.0.65
7.4.0.65	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 \(52 ページ\)](#)」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。

ファイアウォールが再起動したら、FXOS CLI に再度接続します。

- c) FXOS CLI で、管理者パスワードを再度設定するように求められます。

ロータッチプロビジョニングの場合は、デバイスをオンボーディングする際、すでにパスワードが設定されているため、[パスワードのリセット (Password Reset)] エリアで必ず [いいえ (No...)] を選択してください。

- d) デバイスをシャットダウンします。[CLIにおけるファイアウォールの電源の切断 \(89 ページ\)](#) を参照してください。

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。

Before you begin

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。

Procedure

ステップ1 ファイアウォールの電源を入れます。

Note 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。

Note 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。

Example:

```
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

Example:

```
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。

Note 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。

- [IPv4を設定しますか? (Do you want to configure IPv4?)], [IPv6を設定しますか? (Do you want to configure IPv6?)] : これらのタイプのアドレスの少なくとも 1 つに **y** を入力します。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。

- IPv4 は DHCP 経由または手動のどちらで設定しますか？ IPv6 は DHCP、ルータ、または手動のどれで設定しますか？ : [手動 (manual)] を選択します。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または管理インターフェイスの IPv6 ゲートウェイを入力 : ゲートウェイが **data-interfaces** になるように設定します。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。
- [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。

Example:

```

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.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [y]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.61]: 10.89.5.17
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]: 1010-3
Enter a comma-separated list of DNS servers or 'none'
[208.67.222.222,208.67.220.220,2620:119:35::35]:
Enter a comma-separated list of search domains or 'none' []: cisco.com
If your networking information has changed, you will need to reconnect.
Disabling IPv6 configuration: management0
Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
Setting DNS domains:cisco.com
Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'

DHCP server is already disabled
DHCP Server Disabled
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

Device is in OffBox mode - disabling/removing port 443 from iptables.
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事前に設定できます。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を加えないようにしてください。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せん。
- 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。

Example:

```
> 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]:
DNS 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.

>
```

Example:

```
> 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 (Optional) 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、少なくとも 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 (-) があります。
- **nat_id** : Management Center でも指定する、任意で一意的の 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 (-) 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。

Example:

```

> 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。

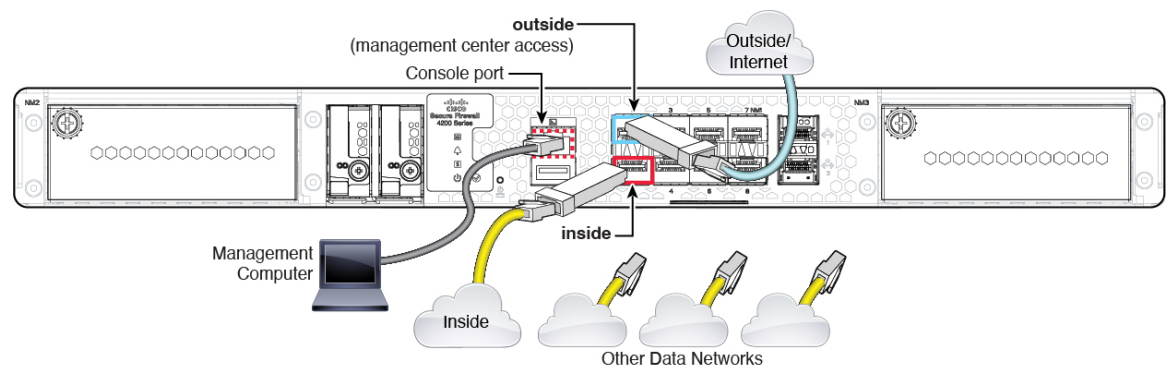
支社へのインストール

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。Cisco Secure Firewall 4200 をケーブル接続するには、次の手順を参照してください。

図 34: リモート管理展開のケーブル接続



始める前に

- データインターフェイスポートに SFP を取り付けます。組み込みポートは、SFP モジュールを必要とする 1/10/25 Gb SFP ポートです。
- (オプション) コンソールケーブルを入手します。デフォルトではファイアウォールにコンソールケーブルが付属していないため、サードパーティの USB-to-RJ-45 シリアルケーブルなどを購入する必要があります。

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 など) を外部ルータに接続します。
- ステップ 3** 内部インターフェイス (Ethernet 1/2 など) を内部スイッチまたはルータに接続します。
- ステップ 4** 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。
- ステップ 5** (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投入

システムの電源は、ファイアウォールの背面にあるロッカー電源スイッチによって制御されます。電源スイッチは、ソフト通知スイッチとして実装されています。これにより、システムのグレースフルシャットダウンがサポートされ、システムソフトウェアおよびデータの破損のリスクが軽減されます。



(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。

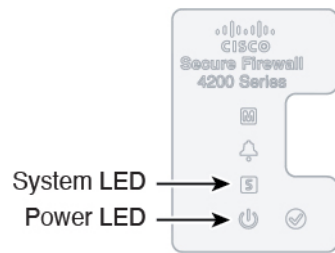
始める前に

ファイアウォールに対して信頼性の高い電力を供給することが重要です (無停電電源装置 (UPS) を使用するなど)。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** 電源コードをファイアウォールに接続し、電源コンセントに接続します。
- ステップ 2** シャーシの背面で、電源コードに隣接する標準的なロッカータイプの電源オン/オフスイッチを使用して電源をオンにします。
- ステップ 3** ファイアウォールの背面にある電源 LED を確認します。緑色に点灯している場合は、ファイアウォールの電源が入っています。

図 35: システムおよび電源 LED



ステップ 4 ファイアウォールの背面にあるシステム LED を確認します。緑色に点灯している場合は、電源投入診断に合格しています。

(注) スイッチを ON から OFF に切り替えると、システムの電源が最終的に切れるまで数秒かかることがあります。この間は、シャーシの前面パネルの電源 LED が緑に点滅します。電源 LED が完全にオフになるまで電源を切らないでください。

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。

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 によって脅威に対する防御に提供されます。オプションで、次の機能ライセンスを購入できます。

- **Essentials** (必須) Essentials ライセンス。
- **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

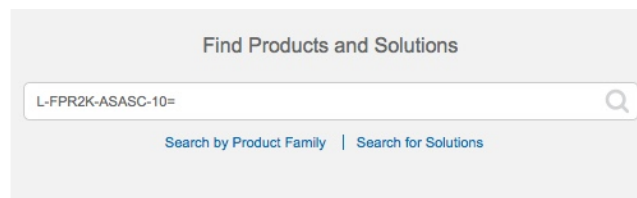
- **Smart Software Manager** にマスターアカウントを持ちます。
まだアカウントをお持ちでない場合は、リンクをクリックして[新しいアカウントを設定](#)してください。Smart Software Manager では、組織のマスターアカウントを作成できます。
- (輸出コンプライアンスフラグを使用して有効化される) 機能を使用するには、ご使用のスマートソフトウェアライセンシングアカウントで強力な暗号化 (3DES/AES) ライセンスを使用できる必要があります。

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 36: ライセンス検索



The screenshot shows a search interface titled "Find Products and Solutions". It features a search input field containing the text "L-FPR2K-ASASC-10=" and a magnifying glass icon. Below the input field, there are two links: "Search by Product Family" and "Search for Solutions".

(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。

- Essentials ライセンス :
 - L-FPR4215-BSE=
 - L-FPR4225-BSE=
 - L-FPR4245-BSE=
- IPS、マルウェア防御、および URL ライセンスの組み合わせ :
 - L-FPR4215T-TMC=
 - L-FPR4225T-TMC=
 - L-FPR4245T-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-FPR4215T-TMC-1Y
 - L-FPR4215T-TMC-3Y
 - L-FPR4215T-TMC-5Y
 - L-FPR4225T-TMC-1Y
 - L-FPR4225T-TMC-3Y
 - L-FPR4225T-TMC-5Y
 - L-FPR4245T-TMC-1Y
 - L-FPR4245T-TMC-3Y
 - L-FPR4245T-TMC-5Y
- キャリアライセンス :
 - L-FPR4200-FTD-CAR=
- 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 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 へのデバイスの追加

デバイスの IP アドレスまたはホスト名と登録キーを使用して、手動で Threat Defense を Management Center

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。
登録キー方式がデフォルトで選択されています。

図 37: 登録キーを使用したデバイスの追加

Add Device ?

Select the Provisioning Method:

Registration Key Serial Number

CDO Managed Device

Host:†

Display Name:

Registration Key:*

Group:

Access Control Policy:*

Smart Licensing

Note: All virtual Firewall Threat Defense devices require a performance tier license. Make sure your Smart Licensing account contains the available licenses you need. It's important to choose the tier that matches the license you have in your account. Click [here](#) for information about the Firewall Threat Defense performance-tiered licensing. Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.

Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):

Carrier

Malware Defense

IPS

URL

Advanced

Unique NAT ID:†

Transfer Packets

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 \(38 ページ\)](#)」を参照してください。

図 38: New Policy

New Policy ?

Name:

Description:

Select Base Policy:

Default Action:
 Block all traffic
 Intrusion Prevention
 Network Discovery

- **スマートライセンス** : 展開する機能に必要なスマートライセンスを割り当てます。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、正常に登録され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スタティック 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部として外部インターフェイスの基本設定を構成しましたが、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

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。ブレイクアウトインターフェイスも設定します。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。

図 39: [インターフェイス (Interfaces)]

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Management0/0	management	Physical				Disabled	Global
GigabitEthernet0/0		Physical				Disabled	
GigabitEthernet0/1		Physical				Disabled	
GigabitEthernet0/2		Physical				Disabled	
GigabitEthernet0/3		Physical				Disabled	
GigabitEthernet0/4		Physical				Disabled	
GigabitEthernet0/5		Physical				Disabled	
GigabitEthernet0/6		Physical				Disabled	
GigabitEthernet0/7		Physical				Disabled	

ステップ 3 (一部のモデルで使用可能な) 40 Gb インターフェイスから4つの 10 Gb ブレイクアウト インターフェイスを作成するには、インターフェイスのブレイクアウトアイコンをクリックします。

設定で 40 Gb インターフェイスをすでに使用している場合は、ブレイクアウトを続行する前に設定を削除する必要があります。

ステップ 4 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。

図 40: [General] タブ

Edit Physical Interface

General IPv4 IPv6 Path Monitoring

Name:

Enabled
 Management Only

Description:

Mode:

Security Zone:

Interface ID:

MTU:

(64 - 9000)

Priority:
 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

- 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。
- [有効 (Enabled)] チェックボックスをオンにします。
- [モード (Mode)] は [なし (None)] に設定したままにします。
- [セキュリティゾーン (SecurityZone)] 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せんが、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。

図 41: [IPv4] タブ

The screenshot shows the 'Edit Physical Interface' configuration page with the 'IPv4' tab selected. The 'IP Type' dropdown menu is set to 'Use Static IP'. Below it, the 'IP Address' text input field contains the value '192.168.1.1/24'. A small example text below the field reads 'eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25'.

- [IPv6] : ステータ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。

図 42: [IPv6] タブ

The screenshot shows the 'Edit Physical Interface' configuration page with the 'IPv6' tab selected. Under the 'Basic' sub-tab, the 'Enable IPV6:' checkbox is unchecked, 'Enforce EUI 64:' is unchecked, 'Link-Local address:' is empty, 'Autoconfiguration:' is checked, and 'Obtain Default Route:' is unchecked.

f) [OK] をクリックします。

ステップ 5 「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。

図 43: [General] タブ

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware

Name:
outside

Enabled
 Management Only

Description:

Mode:
None

Security Zone:
outside_zone

Interface ID:
GigabitEthernet0/0

MTU:
1500
(64 - 9000)

Priority:
0 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

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 6 [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 を使用して脅威に対する防御から 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。

図 44: DHCPサーバー

The screenshot shows the DHCP configuration interface. On the left, there is a sidebar with options: DHCP Server, DHCP Relay, and DDNS. The main area is titled 'DHCP' and contains several configuration fields:

- Ping Timeout: 50 (range 10 - 10000 ms)
- Lease Length: 3600 (range 300 - 10,48,575 sec)
- Auto-Configuration:
- Interface: A dropdown menu.
- Override Auto Configured Settings:
 - Domain Name:
 - Primary DNS Server: +
 - Secondary DNS Server: +
 - Primary WINS Server: +
 - Secondary WINS Server: +

 At the bottom, there are tabs for 'Server' and 'Advanced'. A table below the tabs has columns for 'Interface', 'Address Pool', and 'Enable DHCP Server'. A red box highlights a '+ Add' button in the top right corner of the table area.

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。

図 45: サーバーの追加 (Add Server)

The 'Add Server' dialog box contains the following fields:

- Interface*: A dropdown menu with 'inside' selected.
- Address Pool*: A text input field containing '10.9.7.9-10.9.7.25' with '(2.2.2.10-2.2.2.20)' below it.
- Enable DHCP Server: A checked checkbox.

 At the bottom, there are two buttons: 'Cancel' and 'OK'.

- [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。

図 46: New Policy

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。

図 47: NAT ポリシー

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。

図 48: 基本ルールのオプション

Add NAT Rule

NAT Rule:
Auto NAT Rule

Type:
Dynamic

Enable

Interface Objects Translation PAT Pool Advanced

- [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。

図 49: インターフェイスオブジェクト

Add NAT Rule

NAT Rule:
Auto NAT Rule

Type:
Dynamic

Enable

Interface Objects Translation PAT Pool Advanced

Available Interface Objects

inside_zone Add to Source

1 outside_zone **2** Add to Destination

wfxAutomationZone

Source Interface Objects (0) Destination Interface Objects (1)

any

3 outside_zone

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。

図 50: トランスレーション (Translation)

The screenshot shows the 'Add NAT Rule' configuration interface. The 'Translation' tab is active. In the 'Original Packet' section, the 'Original Source' is set to 'all-ipv4'. In the 'Translated Packet' section, the 'Translated Source' is set to 'Destination Interface IP'. A red box highlights the 'Translated Source' dropdown and the note below it: 'The values selected for Destination Interface Objects in 'Interface Objects' tab will be used'.

- [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。

図 51: 新しいネットワークオブジェクト

The screenshot shows the 'New Network Object' configuration page. The 'Name' field contains 'all-ipv4'. The 'Description' field is empty. Under the 'Network' section, the 'Network' radio button is selected, and the 'Network' field contains '0.0.0.0/0'. The 'Allow Overrides' checkbox is unchecked. At the bottom, there are 'Cancel' and 'Save' buttons.

(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

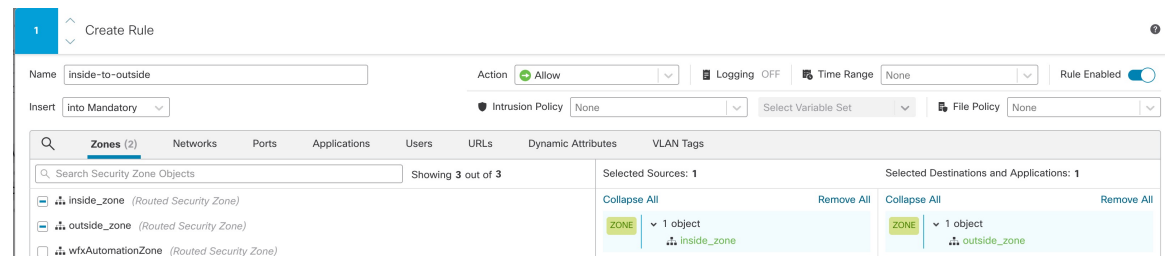
脅威に対する防御を登録したときに、基本の [すべてのトラフィックをブロック (Block all traffic)] アクセスコントロールポリシーを作成した場合は、デバイスを通過するトラフィックを許可するためにポリシーにルールを追加する必要があります。次の手順では、内部ゾーンから外部ゾーンへのトラフィックを許可するルールを追加します。他にゾーンがある場合は、適切なネットワークへのトラフィックを許可するルールを追加してください。

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、脅威に対する防御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。

図 52: [ルールの追加 (Add Rule)]



- [名前 (Name)] : このルールに名前を付けます (たとえば、 **inside-to-outside**) 。
- [選択した送信元 (Selected Sources)] : [ゾーン (Zones)] から内部ゾーンを選択し、[送信元ゾーンを追加 (Add Source Zone)] をクリックします。
- [選択した宛先とアプリケーション (Selected Destinations and Applications)] : [ゾーン (Zones)] から外部ゾーンを選択し、[宛先ゾーンを追加 (Add Destination Zone)] 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 [Apply] 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。



(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 を使用した 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。

Threat Defense 機能の履歴

- 7.4 : SSH のループバック インターフェイスのサポート。

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、ルールに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 [SSHアクセス (SSH Access)] 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。

- [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。
- 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。

- [使用可能なゾーン/インターフェイス (Available Zones/Interfaces)] : 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、[選択したゾーン/インターフェイス (Selected Zones/Interfaces)] 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。ループバックインターフェイスを追加することもできます。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。

- [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。

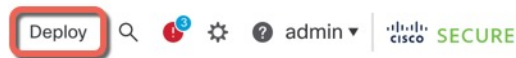
設定の展開

設定の変更を脅威に対する防御に展開します。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 53: [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 54: すべて展開

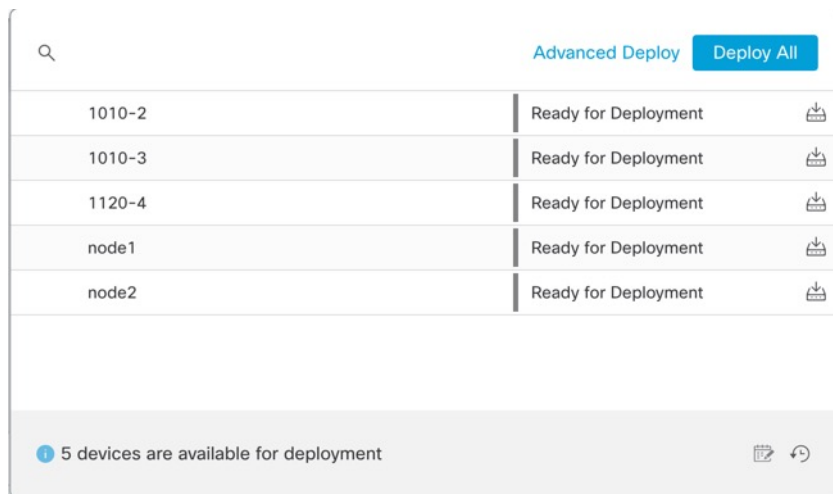
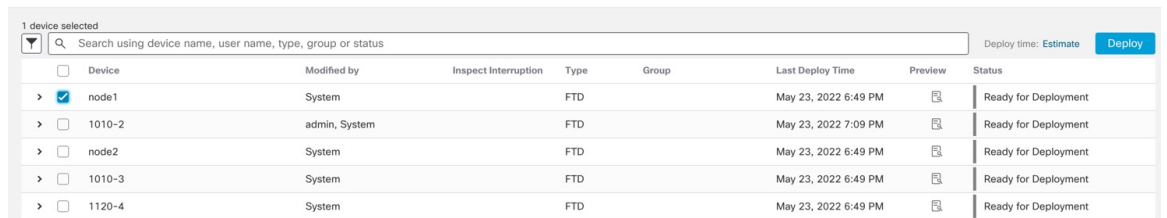
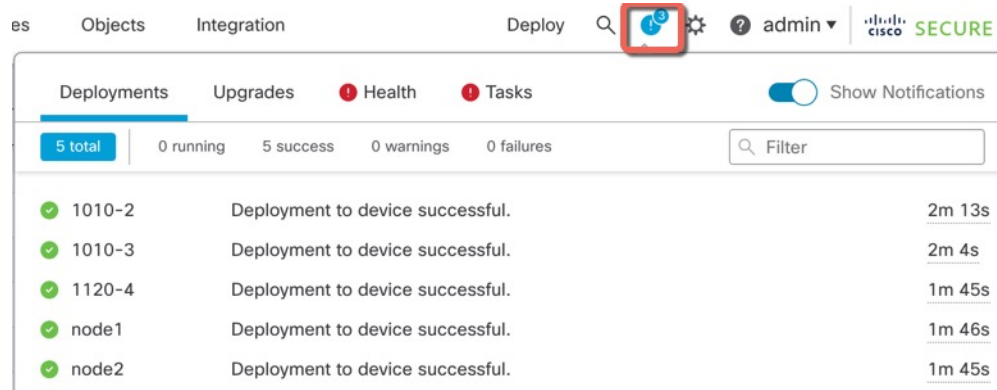


図 55: 高度な展開



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 56: 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。デフォルトでは Cisco Secure Firewall 4200 にコンソールケーブルが付属していないため、サードパーティの USB-to-RJ-45 シリアルケーブルなどを購入する必要があります。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。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、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際、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、**[Devices] > [Device Management] > [Device] > [Management] > [Manager Access - Configuration Details] > [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

```

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                : 10.10.1.4
Display name        : 10.10.1.4
Identifier           : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration        : Completed
Management type     : Configuration

```

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 capturename 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 **[Devices] > [Device Management] > [Device] > [Management] > [Manager Access - Configuration Details] > [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
Successfully 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

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 Management Center 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 Management Center 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、高可用性ではサポートされていますが、クラスタリングの展開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。

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。

(注) ロールバックが失敗し、Management Center 管理が復元された場合、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 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、Management Center 構成の問題を解決して、Management Center 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, 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、**[Devices] > [Device Management] [Device] > [Management] > [Manager Access - Configuration Details] > [FMC Access - Configuration Details] > [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 \(81 ページ\)](#) を参照してください。

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。

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 **[デバイス (Devices)] > [デバイス管理 (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 (Edit)]** (✎) 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 (Shut Down Device)]** (⊗) 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 必要に応じて電源スイッチをオフにし、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 におけるファイアウォールの電源の切断

FXOS CLI を使用すると、システムを安全にシャットダウンしてデバイスの電源を切断できます。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 \(80 ページ\)](#) 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 必要に応じて電源スイッチをオフにし、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

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アプリケーションとマネージャを表示するには、[最適なアプリケーション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 Firewall Management Center を使用する脅威に対する防御を対象としています。

各脅威に対する防御は、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 Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide](#) 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、[Cisco FXOS トラブルシューティングガイド \(Firepower Threat Defense を実行している Firepower 1000/2100 および Cisco Secure Firewall 3100/4200 向け\)](#) 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はありません。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 \(92 ページ\)](#)
- [エンドツーエンドのタスク \(93 ページ\)](#)
- [中央の管理者による事前設定 \(95 ページ\)](#)
- [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 \(103 ページ\)](#)
- [基本的なセキュリティポリシーの設定 \(112 ページ\)](#)

- [トラブルシューティングとメンテナンス \(126 ページ\)](#)
- [次のステップ \(135 ページ\)](#)

CDO による Threat Defense 管理について

クラウド提供型 Firewall Management Center について

クラウド提供型 Firewall 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 を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。オンボーディングウィザードと CLI 登録を使用してデバイスをオンボーディングできます。

Threat Defense マネージャ アクセス インターフェイス

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。これは、リモート分散拠点で発生する可能性が最も高いシナリオであるためです。マネージャアクセスは外部インターフェイスで発生しますが、専用の管理インターフェイスも引き続き関連します。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。

マネージャのアクセス要件

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はできません。
- 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 モデムの上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。
- 管理インターフェイスとイベント専用インターフェイスを別々に使用することはできません。
- クラスタリング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。

ハイ アベイラビリティ要件

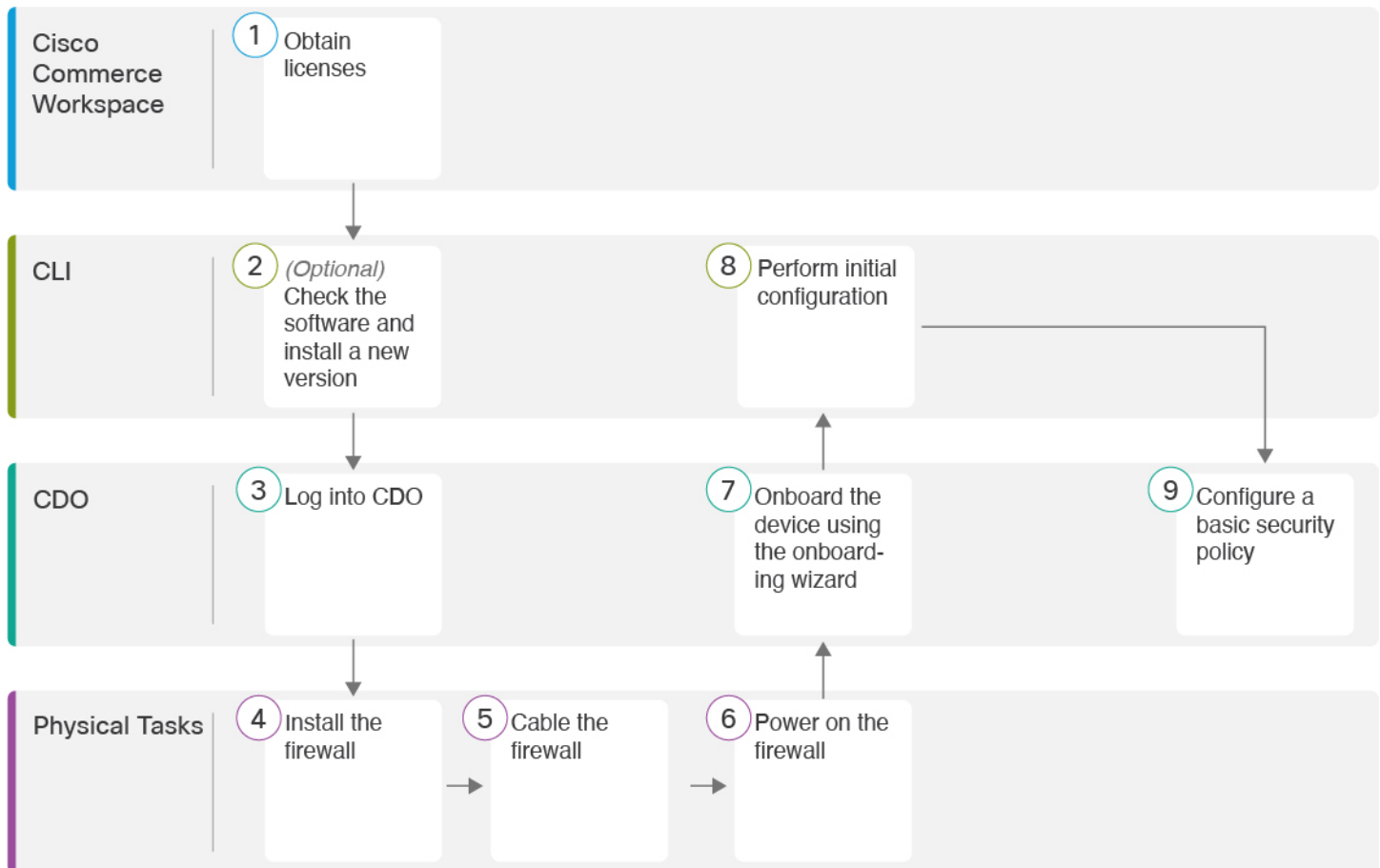
デバイスのハイアベイラビリティを備えたデータインターフェイスを使用する場合は、次の要件を参照してください。

- マネージャアクセスには、両方のデバイスで同じデータインターフェイスを使用します。
- 冗長マネージャ アクセス データ インターフェイスはサポートされていません。
- DHCP は使用できません。静的 IP アドレスのみがサポートされています。DDNS やルーティングプロビジョニングなど、DHCP に依存する機能は使用できません。
- 同じサブネット内に異なる静的 IP アドレスがあります。
- IPv4 または IPv6 のいずれかを使用します。両方を設定することはできません。
- 同じマネージャ設定 (**configure manager add** コマンド) を使用して、接続が同じであることを確認します。
- データインターフェイスをフェールオーバーリンクまたはステートリンクとして使用することはできません。

エンドツーエンドのタスク

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 57: エンドツーエンドのタスク



①	Cisco Commerce Workspace	ライセンスを取得する (95 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 (97 ページ)。
③	CDO	CDO へのログイン (98 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 (103 ページ)。
⑥	物理的なタスク	ファイアウォールの電源投入 (104 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 (105 ページ)。

8	CLI	CLI を使用した初期設定の実行 (107 ページ)。
9	CDO	基本的なセキュリティポリシーの設定 (112 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。

- **Essentials** (必須) Essentials ライセンス。
- **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

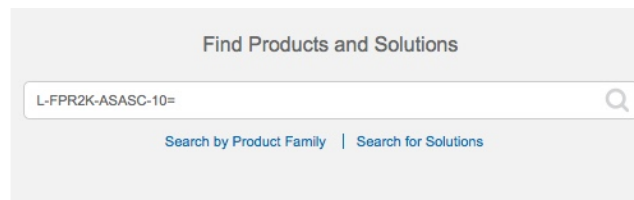
- **Smart Software Manager** にマスターアカウントを持ちます。
まだアカウントをお持ちでない場合は、リンクをクリックして[新しいアカウントを設定](#)してください。Smart Software Manager では、組織のマスターアカウントを作成できます。
- (輸出コンプライアンスフラグを使用して有効化される) 機能を使用するには、ご使用のスマート ソフトウェア ライセンシング アカウントで強力な暗号化 (3DES/AES) ライセンスを使用できる必要があります。

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ス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 58: 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。

- Essentials ライセンス :
 - L-FPR4215-BSE=
 - L-FPR4225-BSE=
 - L-FPR4245-BSE=
- IPS、マルウェア防御、および URL ライセンスの組み合わせ :
 - L-FPR4215T-TMC=
 - L-FPR4225T-TMC=
 - L-FPR4245T-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-FPR4215T-TMC-1Y
- L-FPR4215T-TMC-3Y
- L-FPR4215T-TMC-5Y
- L-FPR4225T-TMC-1Y
- L-FPR4225T-TMC-3Y
- L-FPR4225T-TMC-5Y
- L-FPR4245T-TMC-1Y
- L-FPR4245T-TMC-3Y

- L-FPR4245T-TMC-5Y
- キャリアライセンス :
 - L-FPR4200-FTD-CAR=
- 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 まだの場合は、Smart Software Manager に CDO 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 ファイアウォールデバイスの電源をオンにし、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 \(104 ページ\)](#) および [Threat Defense および FXOS CLI へのアクセス \(126 ページ\)](#) 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。

FXOSCLI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              7.4.0.65
7.4.0.65              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 \(107 ページ\)](#)」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。

ファイアウォールが再起動したら、FXOS CLI に再度接続します。

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 \(102 ページ\)](#) 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 \(99 ページ\)](#) 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 59: 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 60: 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。

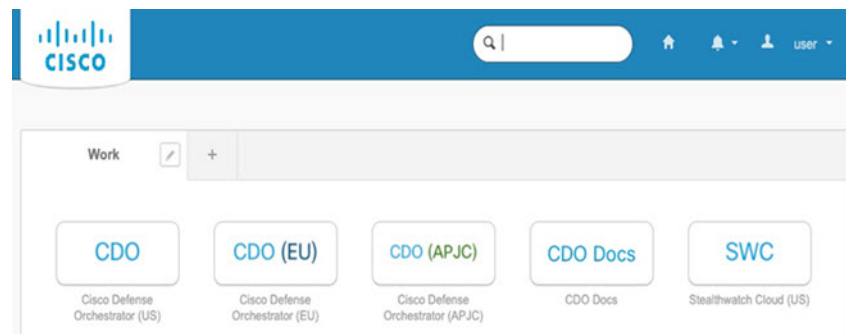
ステップ 4 Cisco Secure Sign-On アカウントのアカウントリカバリのオプションを設定します。

- 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 61: 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 \(99 ページ\)](#) 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。

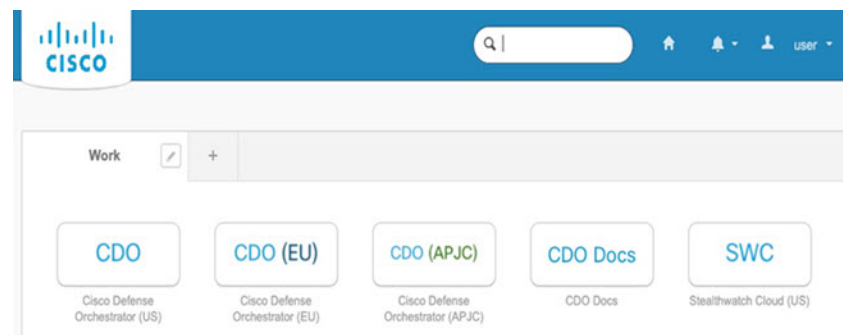
ステップ 2 [ユーザー名 (Username)] と [パスワード (Password)] に入力します。

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 62: 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。

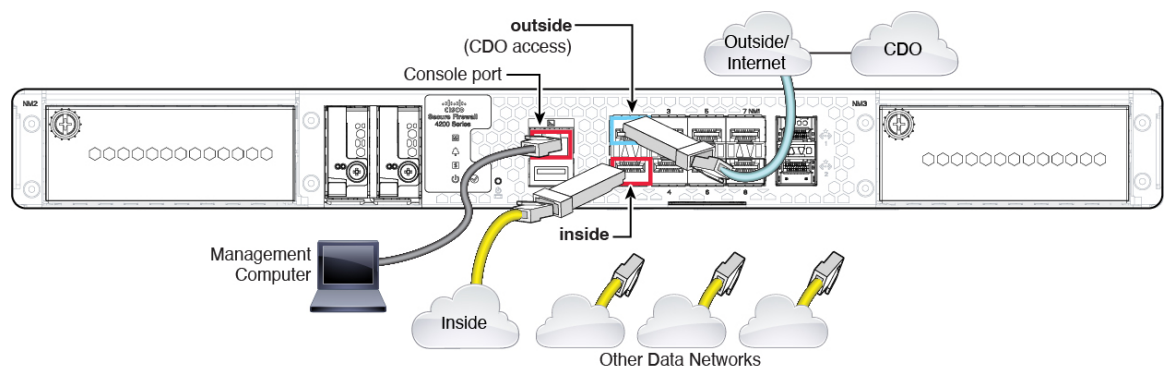
オンボーディングウィザードを使用したファイアウォールの展開

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 Cisco Secure Firewall 4200 をネットワークに接続する方法について説明します。

図 63: Cisco Secure Firewall 4200 のケーブル接続



始める前に

- データインターフェイスポートに SFP を取り付けます。組み込みポートは、SFP モジュールを必要とする 1/10/25 Gb SFP ポートです。
- コンソールケーブルを入手します。デフォルトではファイアウォールにコンソールケーブルが付属していないため、サードパーティの USB-to-RJ-45 シリアルケーブルなどを購入する必要があります。

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 など) を外部ルータに接続します。

- ステップ3** 内部インターフェイス（Ethernet 1/2 など）を内部スイッチまたはルータに接続します。
- ステップ4** 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。
- ステップ5** 管理コンピュータをコンソールポートに接続します。

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。

ファイアウォールの電源投入

システムの電源は、ファイアウォールの背面にあるロッカー電源スイッチによって制御されます。電源スイッチは、ソフト通知スイッチとして実装されています。これにより、システムのグレースフルシャットダウンがサポートされ、システムソフトウェアおよびデータの破損のリスクが軽減されます。



(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。

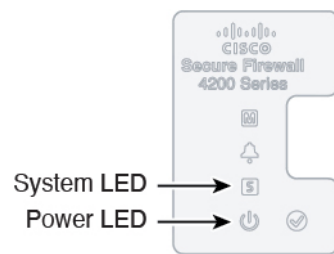
始める前に

ファイアウォールに対して信頼性の高い電力を供給することが重要です（無停電電源装置（UPS）を使用するなど）。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** 電源コードをファイアウォールに接続し、電源コンセントに接続します。
- ステップ2** シャーシの背面で、電源コードに隣接する標準的なロッカータイプの電源オン/オフスイッチを使用して電源をオンにします。
- ステップ3** ファイアウォールの背面にある電源 LED を確認します。緑色に点灯している場合は、ファイアウォールの電源が入っています。

図 64: システムおよび電源 LED



ステップ 4 ファイアウォールの背面にあるシステム LED を確認します。緑色に点灯している場合は、電源投入診断に合格しています。

(注) スイッチを ON から OFF に切り替えると、システムの電源が最終的に切れるまで数秒かかることがあります。この間は、シャーシの前面パネルの電源 LED が緑に点滅します。電源 LED が完全にオフになるまで電源を切らないでください。

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 登録キーを使用した 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。

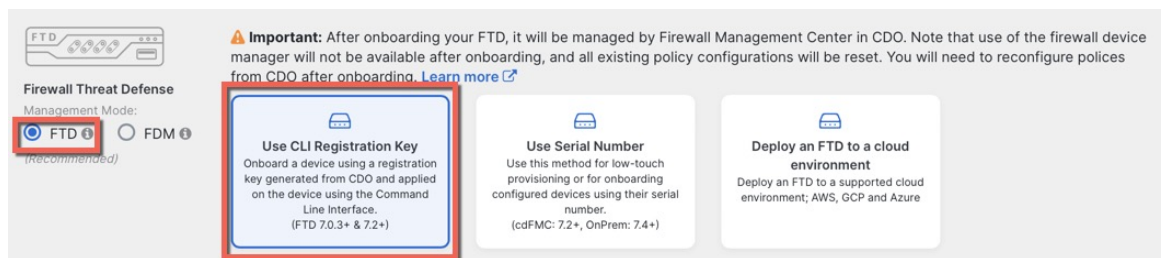
ステップ 2 [FTD] タイルを選択します。

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] をクリックして、デバイスで使用可能な既存のスマートライセンスに登録または変更できます。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 \(95 ページ\)](#) 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 65: 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。

図 66: デバイス名 (Device Name)

- 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。

図 67: アクセスコントロール ポリシー

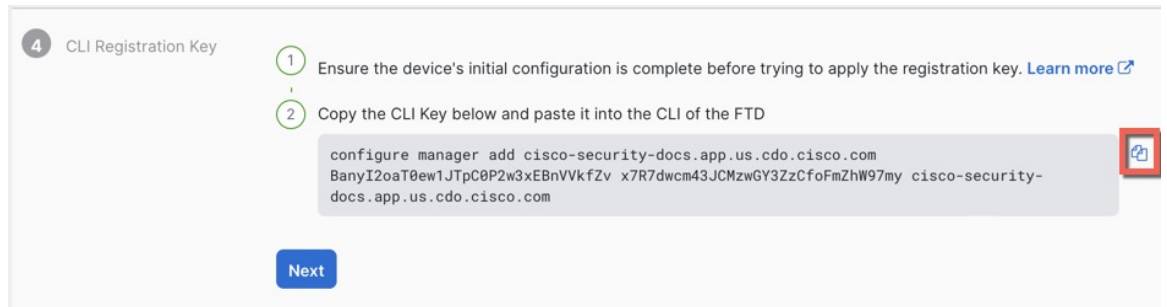
- ステップ 7** [サブスクリプションライセンス (Subscription License)] については、[物理 FTD デバイス (Physical FTD Device)] ラジオ ボタンをクリックし、有効にする各機能ライセンスをチェックします。[Next] をクリックします。

図 68: サブスクリプションライセンス (Subscription License)

License Type	Includes
<input checked="" type="checkbox"/> Essentials	Base Firewall Capabilities
<input checked="" type="checkbox"/> Carrier (7.3+ FTDs only)	GTP/GPRS, Diameter, SCTP, M3UA
<input checked="" type="checkbox"/> IPS	Intrusion Policy
<input checked="" type="checkbox"/> Malware Defense	File Policy
<input checked="" type="checkbox"/> URL	URL Reputation
<input checked="" type="checkbox"/> RA VPN Premier ▾	RA VPN

- 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 の初期設定で使用する必要があります。

図 69: CLI 登録キー



configure manager add cdo_hostname registration_key nat_id display_name

スタートアップスクリプトを完了した後、Threat Defense CLI でこのコマンドをコピーします。[CLI を使用した初期設定の実行 \(107 ページ\)](#) を参照してください。

例：

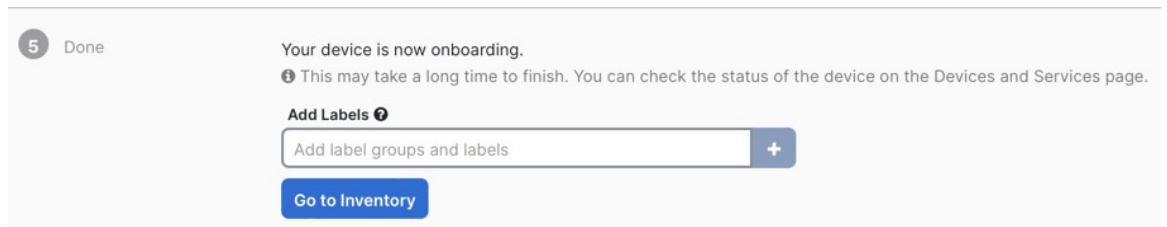
CLI セットアップのサンプルコマンド:

```
configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1H0ynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
```

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。

図 70: 終了 (Done)



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。

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。

Procedure

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。

Note 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。

Example:

```
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
```

Example:

```
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。

Note 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。

- [IPv4を設定しますか? (Do you want to configure IPv4?)]、[IPv6を設定しますか? (Do you want to configure IPv6?)]: これらのタイプのアドレスの少なくとも 1 つに **y** を入力します。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。
- **IPv4 は DHCP 経由または手動のどちらで設定しますか? IPv6 は DHCP、ルータ、または手動のどれで設定しますか? : [手動 (manual)]** を選択します。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または管理インターフェイスの IPv6 ゲートウェイを入力**: ゲートウェイが **data-interfaces** になるように設定します。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。
- [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。

Example:

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

System initialization in progress. Please stand by.
You must configure the network to continue.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [y]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.61]: 10.89.5.17
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]: 1010-3
Enter a comma-separated list of DNS servers or 'none'
[208.67.222.222,208.67.220.220,2620:119:35::35]:
Enter a comma-separated list of search domains or 'none' []: cisco.com
If your networking information has changed, you will need to reconnect.
Disabling IPv6 configuration: management0
Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
Setting DNS domains:cisco.com
Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'
```

```

DHCP server is already disabled
DHCP Server Disabled
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

Device is in OffBox mode - disabling/removing port 443 from iptables.
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を加えないようにしてください。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 構成と一致するように、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。

Example:

```
> 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.

>
```

Example:

```

> 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, on page 105](#) を参照してください。

Example:

```

> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
Manager successfully configured.

```

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ます。マネージャアクセス設定の一部として外部インターフェイスの基本設定を構成しましたが、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

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。ブレイクアウトインターフェイスも設定します。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。

図 71:[インターフェイス (Interfaces)]

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Management0/0	management	Physical				Disabled	Global
GigabitEthernet0/0		Physical				Disabled	
GigabitEthernet0/1		Physical				Disabled	
GigabitEthernet0/2		Physical				Disabled	
GigabitEthernet0/3		Physical				Disabled	
GigabitEthernet0/4		Physical				Disabled	
GigabitEthernet0/5		Physical				Disabled	
GigabitEthernet0/6		Physical				Disabled	
GigabitEthernet0/7		Physical				Disabled	

ステップ 3 (一部のモデルで使用可能な) 40 Gb インターフェイスから4つの 10 Gb ブレイクアウト インターフェイスを作成するには、インターフェイスのブレイクアウトアイコンをクリックします。

設定で 40 Gb インターフェイスをすでに使用している場合は、ブレイクアウトを続行する前に設定を削除する必要があります。

ステップ 4 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。

図 72: [General] タブ

Edit Physical Interface

General IPv4 IPv6 Path Monitoring

Name:

Enabled
 Management Only

Description:

Mode:

Security Zone:

Interface ID:

MTU:

(64 - 9000)

Priority:
 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

- 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。
- [有効 (Enabled)] チェックボックスをオンにします。
- [モード (Mode)] は [なし (None)] に設定したままにします。
- [セキュリティゾーン (SecurityZone)] 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する必要があります。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せんが、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。

図 73: [IPv4] タブ

Edit Physical Interface

General IPv4 IPv6 Path Monitoring

IP Type:
Use Static IP

IP Address:
192.168.1.1/24
eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

- [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。

図 74: [IPv6] タブ

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware Configu

Basic Address Prefixes Settings DHCP

Enable IPV6:

Enforce EUI 64:

Link-Local address:

Autoconfiguration:

Obtain Default Route:

f) [OK] をクリックします。

ステップ 5 「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。

図 75: [General] タブ

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware

Name:

Enabled
 Management Only

Description:

Mode:

Security Zone:

Interface ID:

MTU:

(64 - 9000)

Priority:
 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

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 6 [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 を使用して脅威に対する防御から 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。

図 76: DHCPサーバー

The screenshot shows the DHCP configuration page with the following fields and options:

- Ping Timeout:** 50 (10 - 10000 ms)
- Lease Length:** 3600 (300 - 10,48,575 sec)
- Auto-Configuration
- Interface:** (Dropdown menu)
- Override Auto Configured Settings:**
 - Domain Name:** (Text input)
 - Primary DNS Server:** (Dropdown menu) +
 - Secondary DNS Server:** (Dropdown menu) +
 - Primary WINS Server:** (Dropdown menu) +
 - Secondary WINS Server:** (Dropdown menu) +
- Server / Advanced:** (Tabs)
- + Add:** (Button, highlighted in red)

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。

図 77: サーバーの追加 (Add Server)

The 'Add Server' dialog box contains the following configuration:

- Interface*:** inside
- Address Pool*:** 10.9.7.9-10.9.7.25 (2.2.2.10-2.2.2.20)
- Enable DHCP Server
- Buttons:** Cancel, OK

- [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。

図 78 : New Policy

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。

図 79 : NAT ポリシー

	#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet			Translated Packet			Options	
						Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services		
NAT Rules Before													
Auto NAT Rules													
NAT Rules After													

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。

図 80: 基本ルールのオプション

Add NAT Rule

NAT Rule:
Auto NAT Rule

Type:
Dynamic

Enable

Interface Objects Translation PAT Pool Advanced

- [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。

図 81: インターフェイスオブジェクト

Add NAT Rule

NAT Rule:
Auto NAT Rule

Type:
Dynamic

Enable

Interface Objects Translation PAT Pool Advanced

Available Interface Objects

inside_zone Add to Source

1 outside_zone **2** Add to Destination

wfxAutomationZone

Source Interface Objects (0) Destination Interface Objects (1)

any

3 outside_zone

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。

図 82: トランスレーション (Translation)

Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Dynamic

Enable

Interface Objects Translation PAT Pool Advanced

Original Packet

Original Source:* all-ipv4 +

Original Port: TCP

Translated Packet

Translated Source: Destination Interface IP

The values selected for Destination Interface Objects in 'Interface Objects' tab will be used

Translated Port:

- [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。

図 83: 新しいネットワークオブジェクト

New Network Object

Name: all-ipv4

Description:

Network: Host Range Network FQDN

0.0.0.0/0

Allow Overrides

Cancel Save

(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

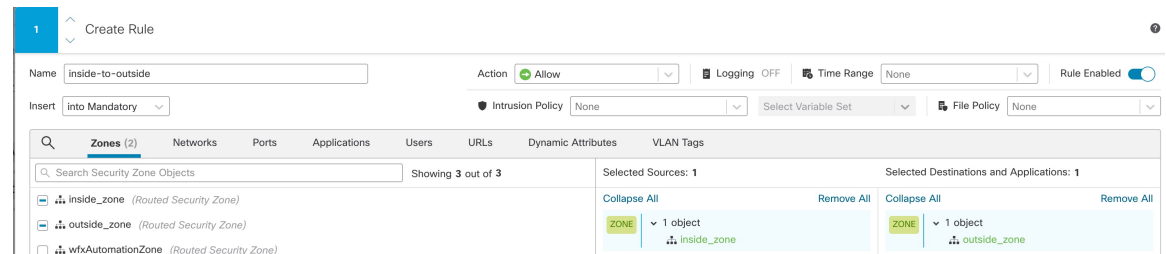
脅威に対する防御を登録したときに、基本の [すべてのトラフィックをブロック (Block all traffic)] アクセスコントロールポリシーを作成した場合は、デバイスを通るトラフィックを許可するためにポリシーにルールを追加する必要があります。次の手順では、内部ゾーンから外部ゾーンへのトラフィックを許可するルールを追加します。他にゾーンがある場合は、適切なネットワークへのトラフィックを許可するルールを追加してください。

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、脅威に対する防御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。

図 84: [ルールを追加 (Add Rule)]



- [名前 (Name)] : このルールに名前を付けます (たとえば、**inside-to-outside**) 。
- [選択した送信元 (Selected Sources)] : [ゾーン (Zones)] から内部ゾーンを選択し、[送信元ゾーンを追加 (Add Source Zone)] をクリックします。
- [選択した宛先とアプリケーション (Selected Destinations and Applications)] : [ゾーン (Zones)] から外部ゾーンを選択し、[宛先ゾーンを追加 (Add Destination Zone)] 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 [Apply] 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。



(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 を使用した 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。

Threat Defense 機能の履歴

- 7.4 : SSH のループバック インターフェイスのサポート。

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、ルールに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 [SSHアクセス (SSH Access)] 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。

- [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。
- 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。

- [使用可能なゾーン/インターフェイス (Available Zones/Interfaces)] : 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、[選択したゾーン/インターフェイス (Selected Zones/Interfaces)] 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。ループバックインターフェイスを追加することもできます。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。

- [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。

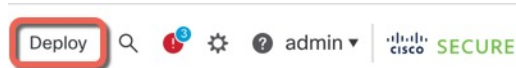
設定の展開

設定の変更を脅威に対する防御に展開します。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 85: [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 86: すべて展開

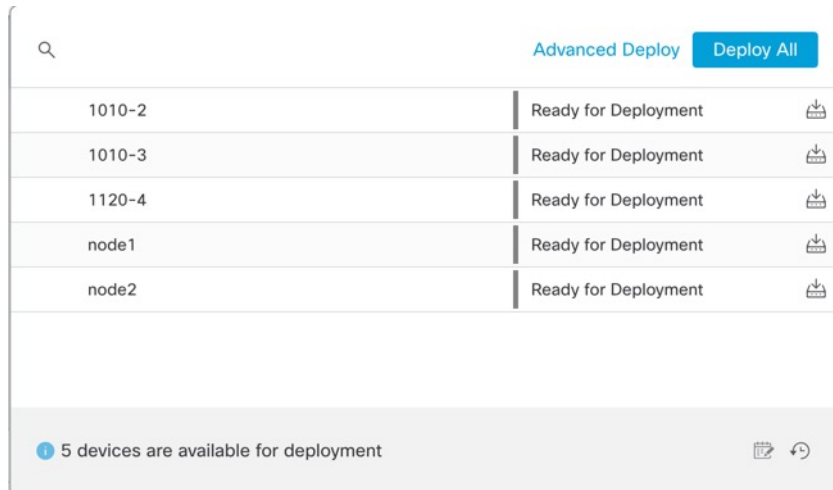
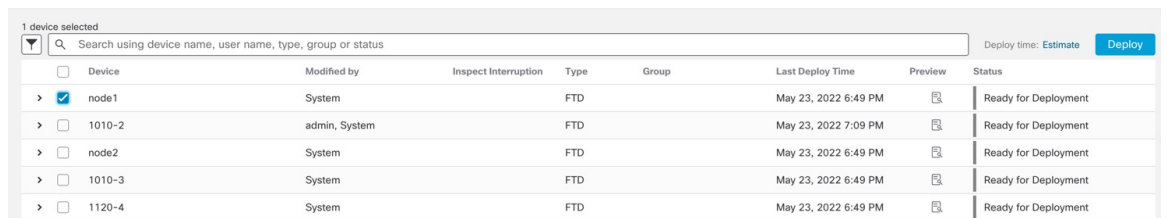
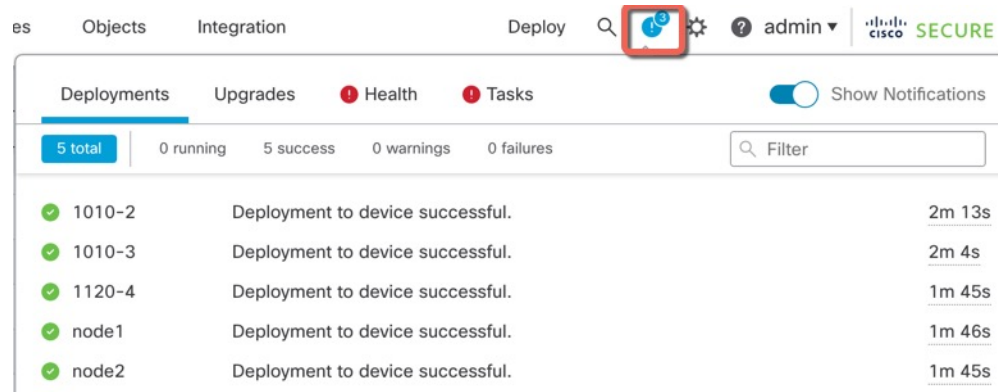


図 87: 高度な展開



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 88: 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。デフォルトでは Cisco Secure Firewall 4200 にコンソールケーブルが付属していないため、サードパーティの USB-to-RJ-45 シリアルケーブルなどを購入する必要があります。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。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                : ftd-1
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

===== [ management0 ] =====
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                              : Ethernet1/1

===== [ Ethernet1/1 ] =====
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

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
Successfully 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 \(127 ページ\)](#) 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。

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 [デバイス (Devices)] > [デバイス管理 (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 (Edit)] (✎) 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 (Shut Down Device)] (✕) 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 必要に応じて電源スイッチをオフにし、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。



第 5 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、「[最適なアプリケーション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、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 Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide](#) 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、[Cisco FXOS トラブルシューティングガイド \(Firepower Threat Defense を実行している Firepower 1000/2100 および Cisco Secure Firewall 3100/4200 向け\)](#) 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はありません。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 \(138 ページ\)](#)
- [エンドツーエンドのタスク \(139 ページ\)](#)
- [ネットワーク配置とデフォルト設定の確認 \(141 ページ\)](#)
- [ファイアウォールのケーブル接続 \(143 ページ\)](#)
- [ファイアウォールの電源投入 \(144 ページ\)](#)
- [\(任意\) IP アドレスの変更 \(145 ページ\)](#)
- [ASDM へのログイン \(146 ページ\)](#)

- [ライセンスの設定](#) (147 ページ)
- [ASA の設定](#) (154 ページ)
- [ASA および FXOS CLI へのアクセス](#) (155 ページ)
- [次のステップ](#) (157 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。

ASA 5500-X 設定の移行

ASA 5500-X の設定をコピーして、Cisco Secure Firewall 4200 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. 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。

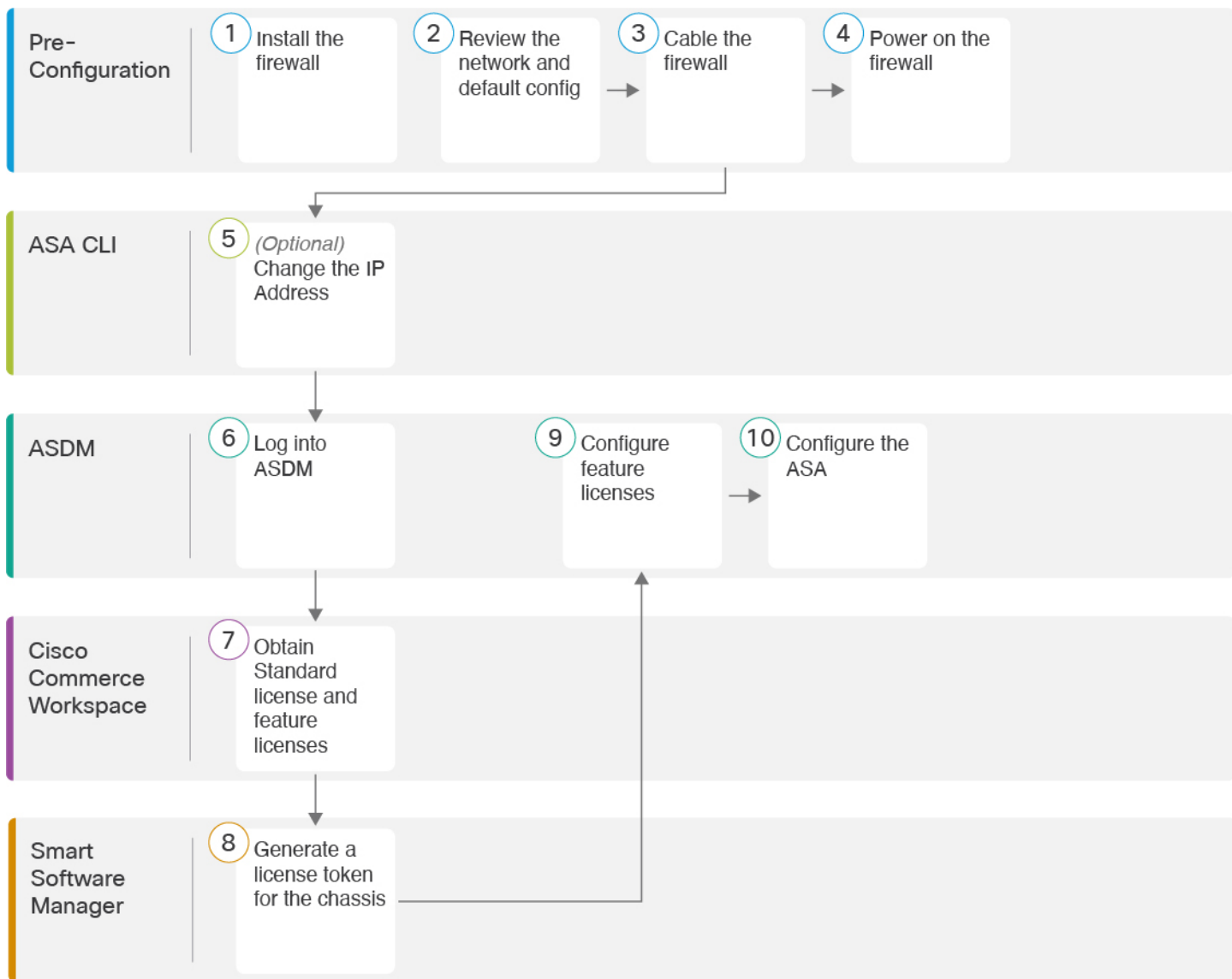
ASA 5500-X 設定	Cisco Secure Firewall 4200 の設定
PAK ライセンス	スマートライセンス 設定をコピーして貼り付けると、PAK ライセンスは適用されません。デフォルトではライセンスはインストールされていません。スマートライセンシングでは、スマートライセンシングサーバーに接続してライセンスを取得する必要があります。スマートライセンシングは、ASDM または SSH アクセスにも影響します (以下を参照)。

ASA 5500-X 設定	Cisco Secure Firewall 4200 の設定
最初の ASDM アクセス	<p>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。</p> <p>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。</p> <p>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。</p>
インターフェイス ID	<p>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。</p>
<p>boot system コマンド</p> <p>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。</p>	<p>Cisco Secure Firewall 4200 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。</p> <p>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。</p>

エンドツーエンドのタスク

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。

図 89: エンドツーエンドのタスク



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 (141 ページ)。
③	事前設定	ファイアウォールのケーブル接続 (143 ページ)。
④	事前設定	ファイアウォールの電源投入 (144 ページ)。
⑤	ASA CLI	(任意) IP アドレスの変更 (145 ページ)。

⑥	ASDM	ASDM へのログイン (146 ページ) 。
⑦	Cisco Commerce Workspace	基本ライセンスとオプションの機能ライセンスを取得します (「 ライセンスの設定 (147 ページ) 」)。
⑧	Smart Software Manager	シャーシのライセンストークンを生成します (「 ライセンスの設定 (147 ページ) 」)。
⑨	ASDM	機能ライセンスを設定します (「 ライセンスの設定 (147 ページ) 」)。
⑩	ASDM	ASA の設定 (154 ページ) 。

ネットワーク配置とデフォルト設定の確認

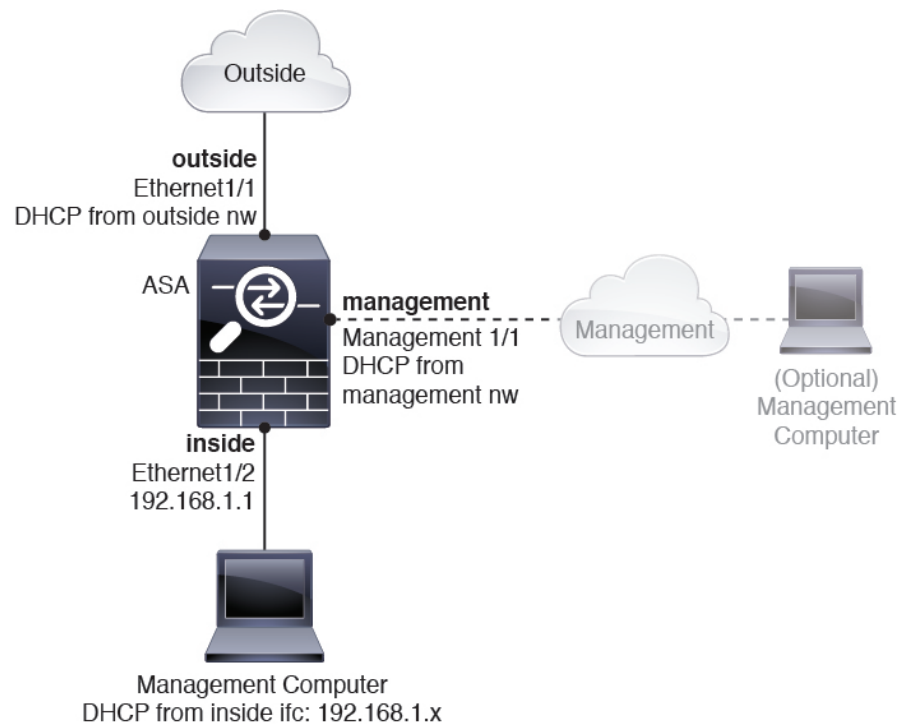
次の図は、ASA でのデフォルトのネットワーク展開を示しています (デフォルト設定を使用)。

外部インターフェイスをケーブルモデムか 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勧めます。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 へのアクセスにデフォルトの内部 IP アドレスを使用できない場合は、ASA CLI で内部 IP アドレスを設定できます。 ([任意](#)) [IP アドレスの変更 \(145 ページ\)](#) を参照してください。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。



Cisco Secure Firewall 4200 のデフォルト設定

Cisco Secure Firewall 4200 の工場出荷時のデフォルト設定は、次のとおりです。

- 内部から外部へのトラフィック フロー：Ethernet 1/1（外部）、Ethernet 1/2（内部）
- DHCP の外部 IP アドレス、内部 IP アドレス：192.168.1.1
- 管理：Management 1/1（管理）、DHCP からの IP アドレス
- 内部インターフェイスの **DHCP サーバー**
- 外部 DHCP、管理 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。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 Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
```



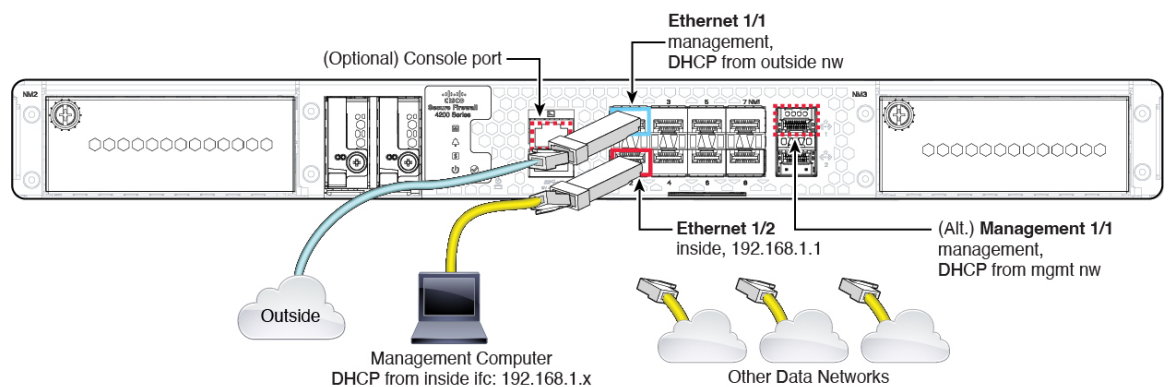
```

!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
  name-server 208.67.222.222 outside
  name-server 208.67.220.220 outside
!

```

ファイアウォールのケーブル接続

図 90: Cisco Secure Firewall 4200 のケーブル接続



Management 1/1 またはイーサネット 1/2 のいずれかで Cisco Secure Firewall 4200 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。

始める前に

- データインターフェイスおよびオプションの管理ポートに SFP を取り付けます。組み込みポートは、SFP モジュールを必要とする 1/10/25 Gb SFP ポートです。

- (オプション) コンソールケーブルを入手します。デフォルトではファイアウォールにコンソールケーブルが付属していないため、サードパーティの USB-to-RJ-45 シリアルケーブルなどを購入する必要があります。

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 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。

- **Management 1/1** : 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、管理コンピュータから IP アドレスに接続できるように、ASA に割り当てられる IP アドレスを決定する必要があります。

別の管理インターフェイスが必要な場合は、後で Management 1/2 を設定できます。

- **Ethernet 1/2** : 初期設定のために、管理コンピュータを Ethernet 1/2 に直接接続します。または、Ethernet 1/2 を内部ネットワークに接続します。内部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そのネットワーク上にあることを確認します。Ethernet 1/2 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 ([Cisco Secure Firewall 4200 のデフォルト設定 \(142 ページ\)](#) を参照)。

また、イーサネット 1/2 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 \(145 ページ\)](#) を参照してください)。

後で他のインターフェイスから ASA 管理アクセスを設定できます。 [ASA の一般的な操作の設定ガイド](#) を参照してください。

ステップ 3 外部ネットワークを Ethernet1/1 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 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。

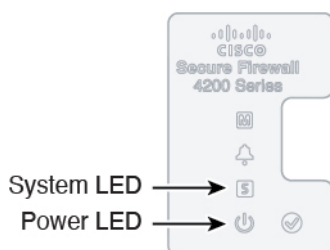
ファイアウォールの電源投入

システムの電源は、ファイアウォールの背面にあるロッカー電源スイッチによって制御されます。電源スイッチは、ソフト通知スイッチとして実装されています。これにより、システムのグレースフルシャットダウンがサポートされ、システム ソフトウェアおよびデータの破損のリスクが軽減されます。

手順

- ステップ1 電源コードをファイアウォールに接続し、電源コンセントに接続します。
- ステップ2 シャーシの背面で、電源コードに隣接する標準的なロッカータイプの電源オン/オフ スイッチを使用して電源をオンにします。
- ステップ3 ファイアウォールの背面にある電源 LED を確認します。緑色に点灯している場合は、ファイアウォールの電源が入っています。

図 91: システムおよび電源 LED



- ステップ4 ファイアウォールの背面にあるシステム LED を確認します。緑色に点灯している場合は、電源投入診断に合格しています。

(注) スイッチを ON から OFF に切り替えると、システムの電源が最終的に切れるまで数秒かかることがあります。この間は、シャーシの前面パネルの電源 LED が緑に点滅します。電源 LED が完全にオフになるまで電源を切らないでください。

(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 で内部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 \(155 ページ\)](#)」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 ethernet1/2
Executing command: nameif inside
INFO: Security level for "inside" set to 100 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。この規則の例外は、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 (Ethernet 1/2) インターフェイスの IP アドレス。
- **https://management_ip** : DHCP から割り当てられた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 [ASDMランチャーのインストール (**Install ASDM Launcher**)] をクリックします。

ステップ 3 画面の指示に従い、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마트ライセンス (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마트ライセンスに適用されます。

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

シェアを登録すると、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

- セキュリティ コンテキスト
- 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、シャーン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

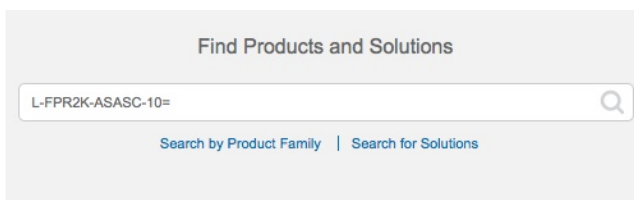
- [Smart Software Manager](#) にマスターアカウントを持ちます。
まだアカウントをお持ちでない場合は、リンクをクリックして[新しいアカウントを設定](#)してください。Smart Software Manager では、組織のマスター アカウントを作成できます。
- （輸出コンプライアンスフラグを使用して有効化される）機能を使用するには、ご使用の Smart Software Manager アカウントで強力な暗号化（3DES/AES）ライセンスを使用する必要があります。

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 92: ライセンス検索



- Essentials ライセンス : L-FPR4215-BSE=. Essentials ライセンスは必須ライセンスです。
- Essentials ライセンス : L-FPR4225-BSE=. Essentials ライセンスは必須ライセンスです。
- Essentials ライセンス : L-FPR4245-BSE=. Essentials ライセンスは必須ライセンスです。
- 5 コンテキストライセンス : L-FPR4200-ASASC-5=. コンテキスト ライセンスは追加的であり、ニーズに合わせて複数のライセンスを購入します。
- 10 コンテキストライセンス : L-FPR4200-ASASC-10=. コンテキスト ライセンスは追加的であり、ニーズに合わせて複数のライセンスを購入します。
- キャリア (Diameter、GTP/GPRS、M3UA、SCTP) : L-FPR4200-ASA-CAR=
- 強力な暗号化 (3DES/AES) ライセンス : L-FPR4200-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。

The screenshot shows the ASA configuration interface with tabs for General, Licenses, Product Instances, and Event Log. Under the 'Product Instance Registration Tokens' section, there is a 'New Token...' button circled in red. Below it is a table with columns for Token, Expiration Date, and Description. One token is listed: 'NWU1MzY1MzEtZjNmOS00MjF...' with an expiration date of '2018-Jul-06 14:20:13 (in 354 days)' and description 'FTD-5506'.

- 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。

The 'Create Registration Token' dialog box contains the following fields and options:

- Virtual Account: [blurred]
- Description: [text input field, highlighted with a blue border]
- Expire After: 30 Days
- Allow export-controlled functionality on the products registered with this token:

 At the bottom right, there are 'Create Token' and 'Cancel' buttons.

- [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 93: トークンの表示

General Licenses Product Instances Event Log

Virtual Account

Description: [redacted]

Default Virtual Account: No

Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this virtual account.

New Token...

Token	Expiration Date	Description	Export-Controlled	Created By	Actions
MjM3ZjYhYTIhZGQ4OS00Yjk2LT...	2017-Aug-16 19:41:53 (in 30 days)	ASA FP 2110 1	Allowed	[redacted]	Actions

図 94: トークンのコピー

Token ⓘ ✕

MjM3ZjYhYTIhZGQ4OS00Yjk2LTgzMGltMThmZTUyYjkyNmVhLTE1MDI5MTI1%0AMTMxMzh8YzdQdmgzMjA2VmFJN2dYQjI5QWRhOEpscDU4cWl5NFNWRUtsa2wz%0AMDd0ST0%3D%0A

Press ctrl + c to copy selected text to clipboard.

MjM3ZjYhYTIhZGQ4OS00Yjk2LT... 2017-Aug-16 1

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。

Configuration > Device Management > Licensing > Smart Licensing

To configure an HTTP proxy for smart licensing, see the [Smart Call-Home](#) page. Note that Smart Call Home is automatically enabled and is required for smart licensing.

Enable Smart license configuration

Feature Tier:

Throughput Level:

Privacy Host Name Version

Transport Call Home Smart Transport

Configure Transport URL

Default URL

Registration

Utility

Proxy URL

Proxy Port

Configure Utility Mode

Enable Standard Utility Mode

Custom ID

Customer Company Identifier

Customer Company Name

Customer Street

Customer City

Customer State

Customer Country

Customer Postal Code

Registration Status: UNREGISTERED

Effective Running Licenses

License Feature	License Value
Maximum VLANs	200
Inside Hosts	Unlimited
Failover	Active/Active
Encryption-DES	Enabled
Encryption-3DES-AES	Enabled
Security Contexts	2
Carrier	Disabled

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。

Smart License Registration

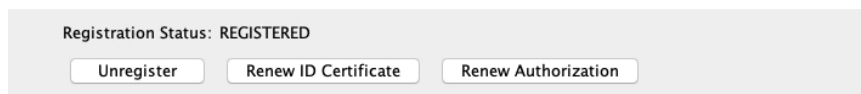
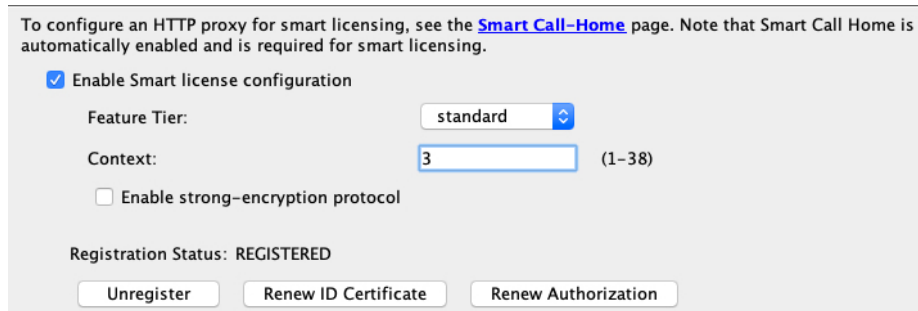
ID Token:

Force registration

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、ライセンスステ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) [Context] ライセンスの場合、コンテキストの数を入力します。
 - Cisco Secure Firewall 4200 : 100 コンテキスト

たとえば、Cisco Secure Firewall 4215 で最大 100 のコンテキストを使用するには、コンテキストの数として 98 を入力します。この値は、デフォルトの 2 に追加されます。

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。

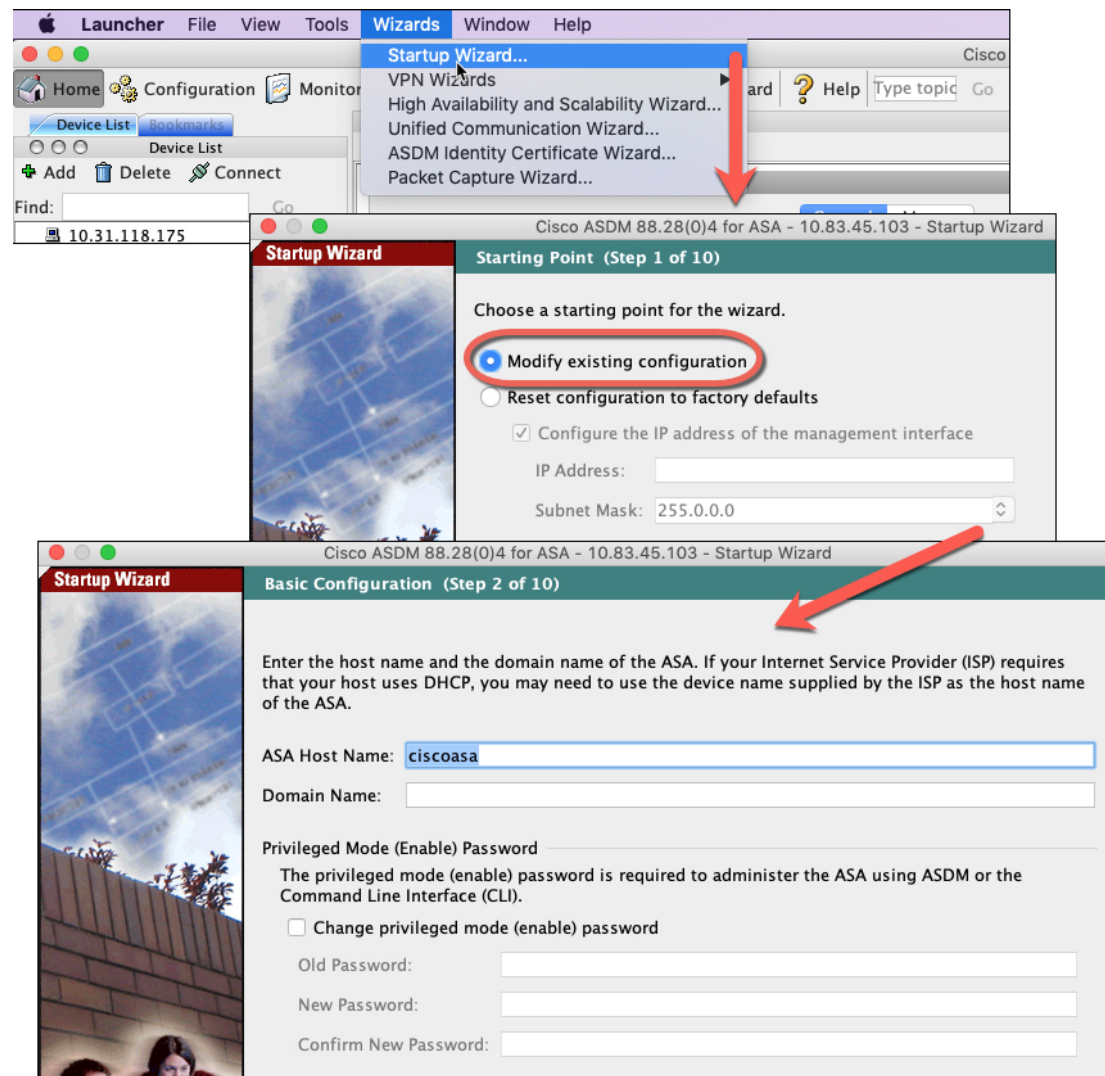
ライセンスを変更する場合、更新された画面を表示するには ASDM を再起動する必要があります。

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 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。ご使用のオペレーティングシステムに必要なシリアルドライバを必ずインストールしてください。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。

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。