



はじめる前に

Cisco Secure Firewall 4200 は、大企業、データセンター、およびサービスプロバイダーのセキュリティ要件を満たすように設計されたハイエンドのファイアウォールです。コンパクトな 1RU フォームファクタ内で優れた脅威防御を提供します。主な特長と利点は以下のとおりです。

- クリプトアクセラレーション対応のアーキテクチャにより、SSL および VPN 復号の際もパフォーマンスを維持できます。
- 省スペース 1 RU フォームファクタ
- 16 ノードクラスタ
- 2 インターフェイスモジュールベイによる付加的なインターフェイスサポート（最大 400G のインターフェイスおよび Fail-To-Wire ネットワークモジュールをサポート）
- イベントストレージおよびマルウェア分析用の 2 つの SSD を装備
- デュアル管理インターフェイスによるレジリエンス
- Cisco SD-WAN 対応。オンデマンドトンネルと、複数の WAN インターフェイスを横断するダイナミックアプリケーションパス選択を使用して、サイト間通信を簡素化
- AI/ML 搭載。シスコネイティブの AI/ML ソリューションを使用して、異常を検出し、脅威を修復し、ポリシーを最適化してピークパフォーマンスを実現

ASDM を使用して ASA を設定します。



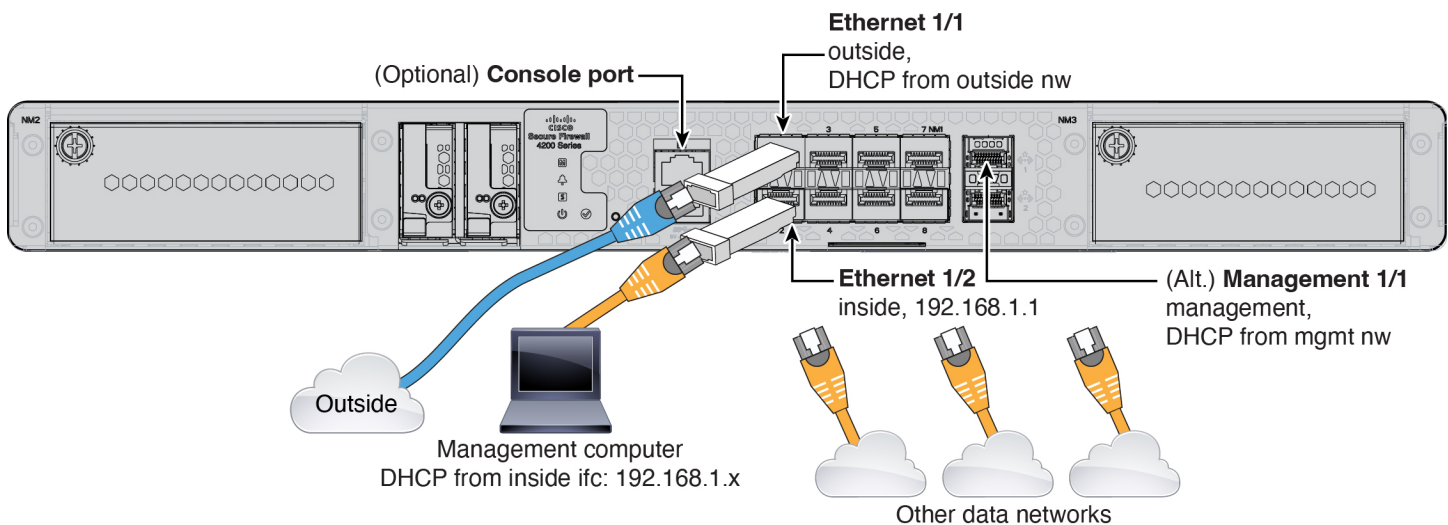
(注) Cisco Secure Firewall 4200 は、アプライアンスモードでのみ実行されます。FXOS をシャーシマネージャとして使用するプラットフォームモードはサポートされていません。アプライアンスモードでは、ASA のすべての設定を行うことができます。FXOS CLI からは、高度なトラブルシューティング コマンドのみ使用できます。

- [ファイアウォールのケーブル接続 \(2 ページ\)](#)
- [ファイアウォールの電源の投入 \(2 ページ\)](#)
- [インストールされているアプリケーション \(Firewall Threat Defense または ASA\) の確認 \(4 ページ\)](#)

- [ASA CLI へのアクセス \(5 ページ\)](#)
- [ライセンスの取得 \(6 ページ\)](#)

ファイアウォールのケーブル接続

- (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。
- 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/SFP+/SFP28 モジュールを必要とする 1/10/25 Gbps SFP28 ポートです。
- 詳細については、[ハードウェア設置ガイド](#)を参照してください。



ファイアウォールの電源の投入

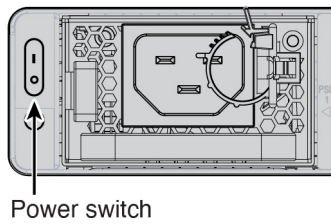
システムの電源は、ファイアウォールの背面にあるロッカー電源スイッチによって制御されます。ロッカー電源スイッチは、ソフト通知を提供します。これにより、システムのグレースフルシャットダウンがサポートされ、システムソフトウェアおよびデータの破損のリスクが軽減されます。

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。

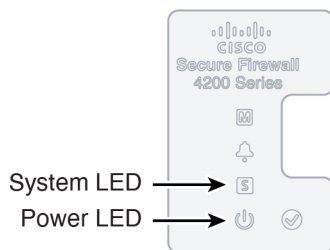
ステップ 2 シャーシの背面で、電源コードに隣接するロッカー電源スイッチを使用して電源をオンにします。

図 1:電源スイッチ



ステップ 3 LED の現在のステータスを確認します。

図 2: LED



- 電源 LED : 緑色で点灯している場合は、ファイアウォールの電源がオンになっていることを意味します。
- システム (S) LED : 次の動作を参照してください。

表 1:システム (S) LED の動作

| LED の動作 | 説明 | デバイスの電源を入れた後の時間 (分:秒) |
|--------------------|---------------------|-----------------------|
| 緑色で高速点滅 | 起動中 | 01:00 |
| オレンジ色で高速点滅 (エラー状態) | 起動に失敗しました | 01:00 |
| 緑色で点灯 | アプリケーションがロードされました | 15:00 ~ 30:00 |
| オレンジ色で点灯 (エラー状態) | アプリケーションのロードに失敗しました | 15:00 ~ 30:00 |

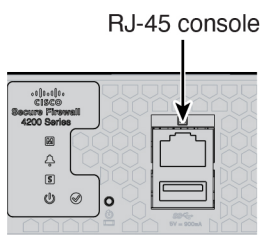
インストールされているアプリケーション（Firewall Threat Defense または ASA）の確認

Firewall Threat Defense と ASA の両方のアプリケーションが、ハードウェアでサポートされています。コンソールポートに接続し、出荷時にインストールされているアプリケーションを確認します。

手順

ステップ1 コンソールポートに接続します。

図 3: コンソールポート



ステップ2 CLI プロンプトを参照して、ファイアウォールで Firewall Threat Defense または ASA が実行されているかどうかを確認します。

Firewall Threat Defense

Firepower ログイン (FXOS) プロンプトが表示されます。ログインして新しいパスワードを設定せずに、切断することができます。

```
firepower login:
```

ASA

ASA プロンプトが表示されます。

```
ciscoasa>
```

ステップ3 間違ったアプリケーションが実行されている場合は、[Cisco Secure Firewall ASA](#) および [Secure Firewall Threat Defense 再イメージ化ガイド](#)を参照してください。

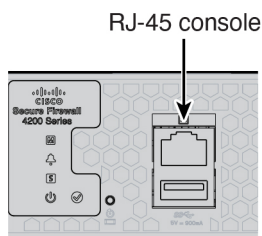
ASA CLI へのアクセス

設定またはトラブルシューティングのために CLI にアクセスする必要がある場合があります。

手順

ステップ 1 コンソールポートに接続します。

図 4: コンソールポート



ステップ 2 ユーザー実行モードで ASA CLI に接続します。このモードでは、多くの **show** コマンドを使用できます。

```
ciscoasa>
```

ステップ 3 特権 EXEC モードにアクセスします。このパスワード保護モードでは、コンフィギュレーションモードへのアクセスなどのさまざまなアクションを実行できます。

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#
```

ステップ 4 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)#
```

ステップ 5 FXOS CLI にアクセスします。この CLI は、ハードウェアレベルでのトラブルシューティングに使用します。

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、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。

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#
```

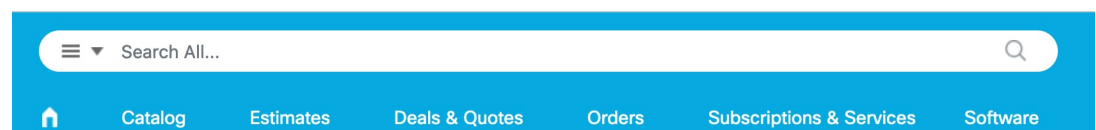
ライセンスの取得

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。[Smart Software Manager](#) にアカウントがない場合は、リンクをクリックして[新しいアカウントを設定](#)します。

Cisco ASA には次のライセンスがあります。

- Essentials : 必須
 - セキュリティ コンテキスト
 - キャリア (Diameter、GTP/GPRS、M3UA、SCTP)
 - Cisco Secure Client
1. 自身でライセンスを追加する必要がある場合は、[Cisco Commerce Workspace](#) で [すべて検索 (Search All)] フィールドを使用します。

図 5: ライセンス検索



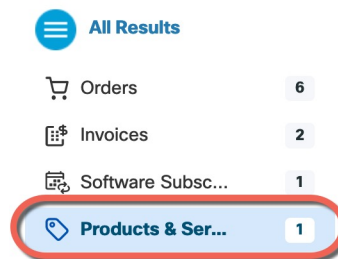
2. 次のライセンス PID を検索します。



(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 : 自動的に含まれます。
 - 5 コンテキスト : L-FPR4200-ASASC-5=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
 - 10 コンテキスト : L-FPR4200-ASASC-10=。コンテキストライセンスは追加的です。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=
 - Cisco Secure Client : 『[Cisco Secure Client Ordering Guide](#)』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。
3. 結果から、[製品とサービス (Products & Services)] を選択します。

図 6: 結果



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。