はじめる前に

Cisco Secure Firewall 200 は、分散型企業および小規模ブランチロケーション向けに設計された次世代ファイアウォール（NGFW）機能を提供します。コンパクトなフォームファクタ内で、堅牢かつコスト効率の高いセキュリティとシンプルな管理を可能にし、ネットワークエッジにおけるセキュアで最適化された接続を実現します。Cisco Secure Firewall 200 の特長：

- シスコの Hybrid Mesh Firewall アーキテクチャをブランチエッジまで拡張
- AI を利用した検査と一貫したセキュリティポリシーを提供
- SD-WAN機能を統合して、アプリケーションパフォーマンスを強化し、信頼性の高いユーザーアクセスを実現
- コスト重視の環境に合わせたアプリケーションとユーザーの制御、効率的なセグメンテーション、高度なセキュリティ機能を提供

分散拠点にファイアウォールをインストールし、中央の Cisco Secure Firewall Management Center を使用して外部インターフェイスで管理します。

（注） ゼロタッチプロビジョニングを使用する場合、高可用性のために管理インターフェイスを使用することを推奨します。外部でゼロタッチプロビジョニングを使用して高可用性を使用する場合は、登録後に外部 IP アドレスを静的アドレスに変更する必要があります。

ファイアウォールの電源の投入

システムの電源は、ファイアウォールの背面にある電源ボタンによって制御されます。電源ボタンは、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。

（注） ファイアウォールを初めて起動するときは、Firewall Threat Defense の初期化に約 15 ～ 30 分かかります。

始める前に

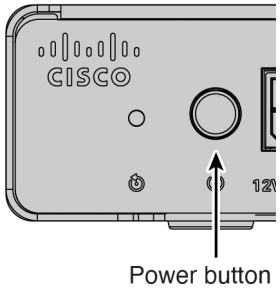
ファイアウォールに対して信頼性の高い電力を供給することが重要です（無停電電源装置（UPS）を使用するなど）。最初のシャットダウンを行わないで電力が失われると、重大なファイルシステムの損傷を引き起こす可能性があります。バックグラウンドでは常に多数のプロセスが実行されていて、電力が失われると、システムをグレースフルシャットダウンできません。

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。

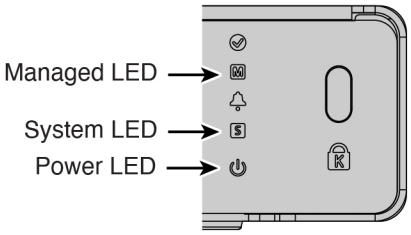
ステップ 2 シャーシの背面で、電源コードに隣接する電源ボタンを使用して電源をオンにします。

図 *1:* 電源ボタン



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

- 管理対象（M）LED：外部インターフェイスをインターネットに接続した後に（「ファイアウォールのケーブル接続」を参照）、管理対象LEDを確認して、ゼロタッチプロビジョニングに向けたクラウド接続ステータスを確認します。

表 *2 :* ゼロ タッチ プロビジョニング：管理対象（*M*）*LED* の動作

M LED	**説明**	**ファイアウォールの電源を入れた後の時間（分:秒）**
緑色で低速点滅	Cisco Cloud に接続され、オンボーディングの準備ができています	15:00 ～ 30:00
グリーンとオレンジに交互に点滅 （エラー条件）	Cisco Cloud に接続できませんでした	15:00 ～ 30:00

M LED	説明	ファイアウォールの電源を入れた後の時間（分:秒）
緑色で点灯	オンボード済み	20:00 ～ 45:00

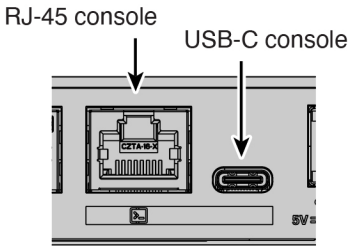
インストールされているアプリケーション（Firewall Threat Defense または ASA）の確認

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 いずれかのポートタイプを使用して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。ログインを完了する必要がある場合は、Firewall Threat Defense CLI へのアクセス （5 ページ）を参照してください。

```
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。

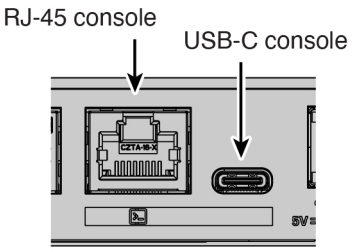
Firewall Threat Defense CLI へのアクセス

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 いずれかのポートタイプを使用して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 FXOS に接続します。ユーザー名 **admin** とパスワード（デフォルトは **Admin123**）を使用して CLI にログインします。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。

```
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 Firewall Threat Defense CLI に変更します。

（注）

初期セットアップに Firewall Device Manager を使用する場合は、Firewall Threat Defense CLI にアクセスしないでください（アクセスすると、CLI セットアップが開始されます）。

ゼロタッチプロビジョニング の場合、CLI にアクセスし、セットアップスクリプトを実行したときに次のプロンプトメッセージが表示された場合は、**[n]** を選択します：「`Do you want to configure IPv4? (y/n) [y]:`」および「`Do you want to configure IPv6? (y/n) [y]:`」。また、次のプロンプトでデフォルトのローカルマネージャを承認する必要があります：「`Manage the device locally? (yes/no) [yes]:`」。

connect ftd

Firewall Threat Defense CLI に初めて接続すると、初期セットアップを完了するように求められます。

例：

```
firepower# connect ftd
>
```

Firewall 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 プロンプトに戻ります。

例：

```
> exit
firepower#
```

バージョンの確認と再イメージ化

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。

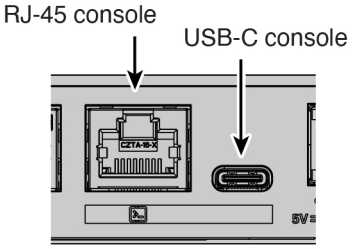
実行するバージョン

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 で説明されているリリース戦略を参照することもできます。

手順

ステップ 1 いずれかのポートタイプを使用してコンソールポートに接続します。

図 *5*: コンソール ポート



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            7.6.0.65        7.6.0.65        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) 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に静的 IP アドレスを設定する必要がある場合は、次のコマンドを入力します。

scope fabric-interconnect a

set out-of-band static ip *ip* **netmask** *netmask* **gw** *gateway*

commit-buffer

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。

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。

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。

ゼロタッチプロビジョニングの場合は、デバイスの導入準備をする際に、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) ファイアウォールをシャットダウンします。（必要な場合）ファイアウォールの電源の切断 （9 ページ） を参照してください。

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。

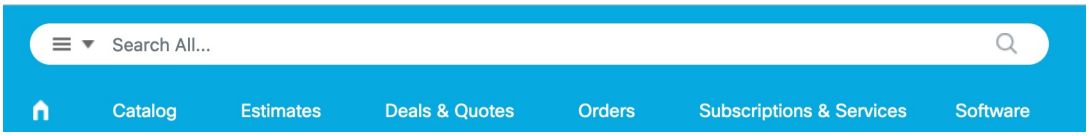
まだの場合は、Smart Software Manager に Firewall Management Center を登録します。登録を行うには、Smart Software Manager で登録トークンを生成する必要があります。詳細な手順については、*Cisco Secure Firewall Management Center* アドミニストレーション ガイドを参照してください。

Firewall Threat Defense には次のライセンスがあります。

- Essentials：必須
- IPS
- マルウェア防御
- URL フィルタリング
- 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 *6:* 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。

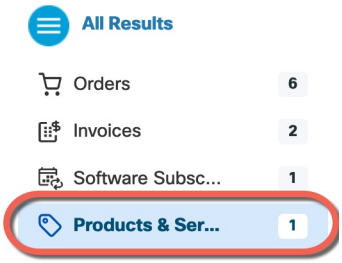
- IPS、マルウェア防御、および URL の組み合わせ：
  - CSF220T-TMC

  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。
  - CSF220T-TMC-1Y
  - CSF220T-TMC-3Y
  - CSF220T-TMC-5Y

- Cisco Secure Client：『Cisco Secure Client Ordering Guide』を参照してください。

3. 結果から、**[製品とサービス（Products & Services）]**を選択します。

図 7 : 結果



（必要な場合）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ません。

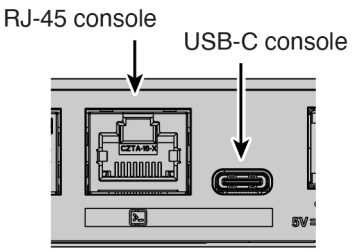
CLI におけるファイアウォールの電源の切断

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ファイアウォールの電源を切断できます。

手順

ステップ 1 いずれかのポートタイプを使用してコンソールポートに接続します。

図 8 : コンソール ポート



ステップ 2 FXOS CLI でローカル管理モードに接続します。

firepower # **connect local-mgmt**

ステップ 3 システムをシャットダウンします。

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 4 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。シャットダウンが完了すると、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 5 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。

Management Center を使用したファイアウォールの電源切断

Firewall Management Center を使用してシステムを適切にシャットダウンします。

手順

ステップ 1 ファイアウォールをシャットダウンします。

a) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**を選択します。
b) 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。
c) [デバイス（Device）] タブをクリックします。
d) **[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。
e) 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 2 コンソールからファイアウォールに接続している場合は、ファイアウォールがシャットダウンするときにシステムプロンプトをモニターします。シャットダウンが完了すると、次のプロンプトが表示されます。

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

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

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

ステップ 3 必要に応じて電源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。

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。

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。