はじめる前に

ミッドレンジの Cisco Secure Firewall 3100 は、進化する世界をサポートします。これにより、ハイブリッドな作業とゼロトラストが実用化され、高い投資回収率を確保する柔軟性が得られます。Cisco Secure Firewall 3100 は、脅威対策重視型セキュリティアプライアンスです。このアプライアンスは、脅威に対する優れた防御機能とビジネスの復元力を提供します。Advanced Threat 機能が有効になっている場合でも、ファイアウォールの複数のユースケースに対して優れたパフォーマンスを提供します。これらのパフォーマンス機能は、ファイアウォール、暗号化、および脅威検査機能を最適化する専用ハードウェアと組み合わせた最新の CPU アーキテクチャによって実現されています。Cisco Secure Firewall 3100 は、インターネットエッジからデータセンターおよびプライベートクラウドまで幅広いユースケースに対応します。Cisco Secure Firewall 3100 はマルチインスタンスとクラスタリングをサポートしており、組織の成長に伴うニーズに合わせて拡張できるパフォーマンスの向上を実現します。

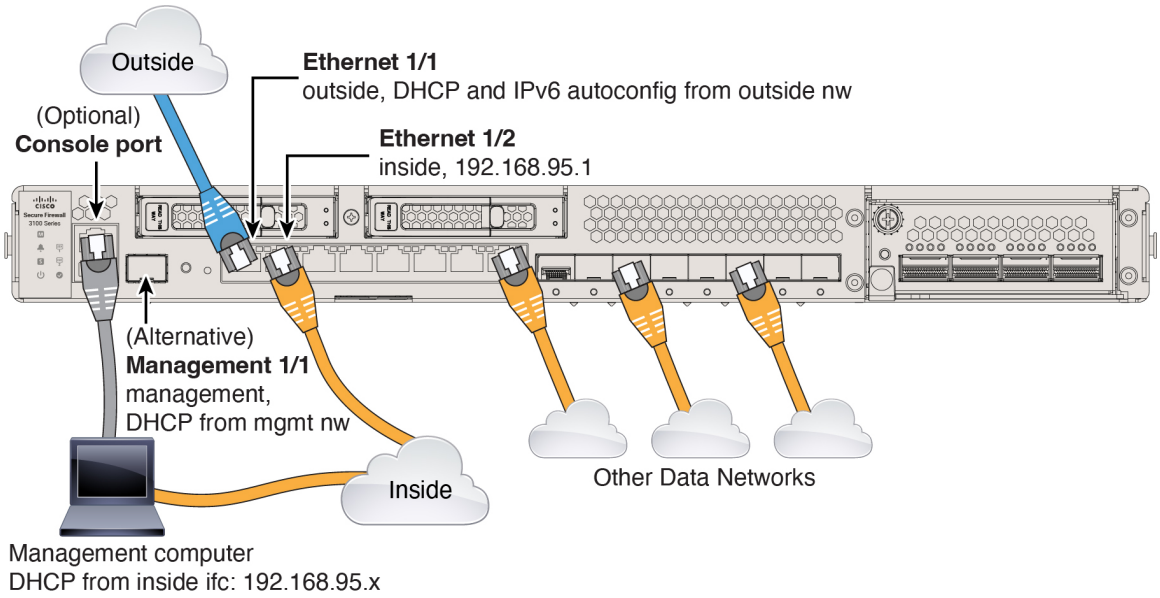
ローカルの Cisco Secure Firewall Device Manager を使用してファイアウォールを管理します。

- ファイアウォールのケーブル接続 （1 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）
- Firewall Threat Defense CLI へのアクセス （5 ページ）
- バージョンの確認と再イメージ化 （6 ページ）
- （任意）CLI での管理ネットワーク設定の変更 （7 ページ）
- ライセンスの取得 （9 ページ）
- （必要な場合）ファイアウォールの電源オフ （9 ページ）

ファイアウォールのケーブル接続

- （オプション）コンソールアダプタを入手します。シャーシには DB-9 - RJ-45 シリアルケーブルが付属しているため、接続するにはサードパーティの DB-9 - USB シリアルケーブルの購入が必要になる場合があります。
- （オプション）管理 1/1 に SFP を取り付けます。これは SFP/SFP+ モジュールを必要とする 1/10-Gbps ポートです。

- SFP をイーサネット 1/9 以上に取り付けます。これらの固定ポートは SFP/SFP+ モジュールを必要とする 1/10-Gbps 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。

（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

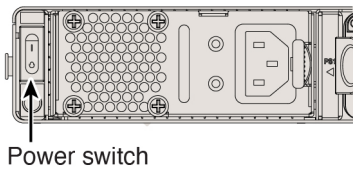
ファイアウォールに対して信頼性の高い電力を供給することが重要です（無停電電源装置（UPS）を使用するなど）。最初のシャットダウンを行わないで電力が失われると、重大なファイルシステムの損傷を引き起こす可能性があります。バックグラウンドでは常に多数のプロセスが実行されていて、電力が失われると、システムをグレースフルシャットダウンできません。

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。

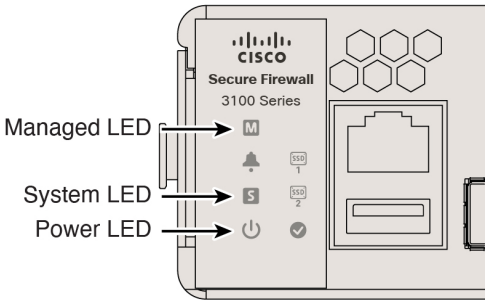
ステップ 2 シャーシの背面で、電源コードに隣接するロッカー電源スイッチを使用して電源をオンにします。

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

LED の動作	説明	デバイスの電源を入れた後の時間（分：秒）
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

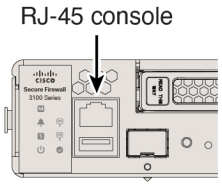
インストールされているアプリケーション（Firewall Threat Defense または ASA）の確認

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。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。

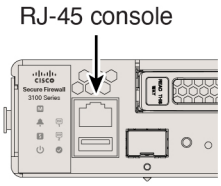
Firewall Threat Defense CLI へのアクセス

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 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）。

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。

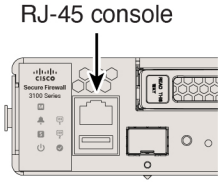
実行するバージョン

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 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。

（任意）CLI での管理ネットワーク設定の変更

デフォルトでは、次のいずれかのインターフェイスでファイアウォールを管理できます。

- イーサネット 1/2：192.168.95.1/24
- 管理 1/1：DHCP からの IP アドレス

デフォルトの IP アドレスを使用できない場合は、コンソールポートに接続して CLI で初期セットアップを実行し、管理 1/1 の IP アドレスを静的アドレスに設定できます。

手順

ステップ 1 コンソール ポートに接続します。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）を参照してください。

ステップ 2 Firewall Threat Defense CLI に接続します。

connect ftd

例：

```
firepower# connect ftd
>
```

ステップ 3 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を完了します。

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
Cisco General Terms
[...]

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
```

ガイダンス：これらのタイプのアドレスの少なくとも 1 つについて **y** を入力します。

```
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
```

ガイダンス：静的 IP アドレスを設定するには [手動（manual）] を選択します。

```
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]: 10.10.10.1
```

ガイダンス：ゲートウェイの IP アドレスを設定します。

```
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'

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

>
```

ガイダンス：Firewall Device Manager を使用する場合は、**yes** と入力します。

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

ライセンスの取得

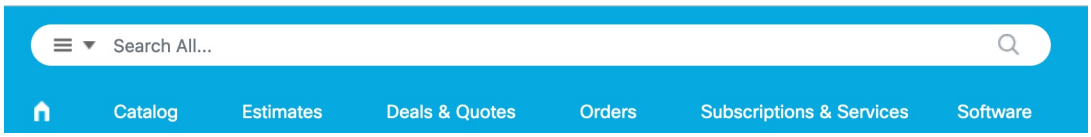
ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマート ソフトウェア ライセンシング アカウントにリンクされています。Smart Software Manager にアカウントがない場合は、リンクをクリック して新しいアカウントを設定します。

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

- 標準：必須
- IPS
- マルウェア防御
- URL フィルタリング
- Cisco Secure Client
- キャリア（Diameter、GTP/GPRS、M3UA、SCTP）

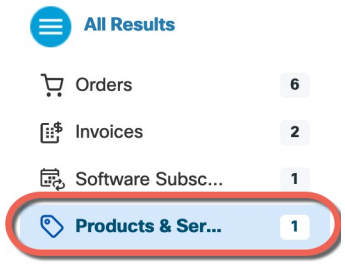
1. 自身でライセンスを追加する必要がある場合は、Cisco Commerce Workspace で [すべて検索（Search All）] フィールドを使用します。

図 *6*：ライセンス検索



2. ライセンス PID を検索します。必要な PID については、発注ガイド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オフ

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。

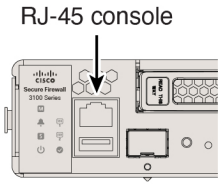
CLI におけるファイアウォールの電源の切断

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 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。

Device Manager を使用したファイアウォールの電源切断

Firewall Device Manager 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（Device）** をクリックしてから、**システム設定（System Settings）** > **再起動/シャットダウン（Reboot/Shutdown）** リンクをクリックします。

b) [シャットダウン（Shut Down）] をクリックします。

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