Firepower 4100 シャーシの初期設定

この章の対象読者

この章では、Cisco Firepower 4100 シャーシの初期設定の方法について、ASA および 脅威に対する防御 論理デバイスで使用するためのインターフェイスの設定を含めて説明します。

- このガイドの対象読者 （1 ページ）
- Firepower 4100 シャーシについて （2 ページ）
- エンドツーエンドの手順 （4 ページ）
- シャーシのケーブル接続 （6 ページ）
- シャーシの初期セットアップの実行 （10 ページ）
- Chassis Manager へのログイン （14 ページ）
- NTP の設定 （15 ページ）
- FXOS ユーザーの追加 （17 ページ）
- インターフェイスの設定 （19 ページ）
- ソフトウェア イメージのシャーシへのアップロード （26 ページ）
- FXOS の履歴 （27 ページ）

このガイドの対象読者

このガイドでは、ASA および/または 脅威に対する防御 アプリケーションで使用するために Firepower 4100 シャーシを設定する方法について説明します。このガイドでは、次の展開について説明します。

- Management Center を使用したネイティブまたはコンテナインスタンス（マルチインスタンス機能）としてのスタンドアロン 脅威に対する防御
- Device Manager を使用したスタンドアロン 脅威に対する防御

（注） Device Manager はマルチインスタンスをサポートしていません。

- CDO を使用したスタンドアロン 脅威に対する防御

（注） CDO はマルチインスタンスをサポートしていません。

- ASDM を使用したスタンドアロン ASA

このガイドでは以下の展開については取り上げていませんので、FXOS、ASA、FDM、CDO、および FMC のコンフィギュレーション ガイドを参照してください。

- ハイ アベイラビリティ/フェールオーバー
- クラスタリング（ASA、または Management Center のみを使用した 脅威に対する防御 ）
- マルチインスタンス（Management Center のみを使用した 脅威に対する防御 ）
- Radware DefensePro デコレータ アプリケーション
- CLI 設定（ASA または FXOS のみ）

このガイドでは、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、コンフィギュレーション ガイドを参照してください。

Firepower 4100 シャーシについて

Firepower 4100 シャーシは、ネットワークおよびコンテンツ セキュリティ ソリューションの次世代プラットフォームです。Firepower 4100 シャーシには、スーパバイザと、論理デバイスをインストールできる最大 3 つのセキュリティ モジュールが含まれています。また、複数の高パフォーマンス ネットワーク モジュールも組み込むことができます。

論理デバイスの動作方法：Firepower 4100/9300

Firepower 4100/9300 は、Firepower eXtensible Operating System（FXOS）という独自のオペレーティング システムをスーパバイザ上で実行します。オンボックスの シャーシマネージャ では、シンプルな GUI ベースの管理機能を利用できます。シャーシマネージャ を使用して、ハードウェア インターフェイスの設定、スマートライセンシング（ASA 用）、およびその他の基本的な操作パラメータをスーパバイザ上で設定します。FXOS CLI を使用する場合は、『FXOS CLI コンフィグレーション ガイド』を参照してください。

論理デバイスでは、1 つのアプリケーション インスタンスおよび 1 つのオプション デコレータ アプリケーションを実行し、サービス チェーンを形成できます。論理デバイスを導入すると、スーパバイザは選択されたアプリケーション イメージをダウンロードし、デフォルト設定を確立します。その後、アプリケーションのオペレーティング システム内でセキュリティ ポリシーを設定できます。

論理デバイスは互いにサービスチェーンを形成できず、バックプレーンを介して相互に通信することはできません。別の論理デバイスに到達するために、すべてのトラフィックが 1 つのインターフェイス上のシャーシから出て、別のインターフェイスに戻る必要があります。コンテ

ナインスタンスの場合、データインターフェイスを共有できます。この場合にのみ、複数の論理デバイスがバックプレーンを介して通信できます。

サポートされるアプリケーション

次のアプリケーション タイプを使用して、シャーシに論理デバイスを展開できます。

Threat Defense

脅威に対する防御 は、ステートフル ファイアウォール、ルーティング、VPN、Next-Generation Intrusion Prevention System（NGIPS）、Application Visibility and Control（AVC）、URL フィルタリング、マルウェア防御などの次世代ファイアウォールサービスを提供します。

脅威に対する防御 は、次のいずれかのマネージャを使用して管理できます。

- Management Center：別のサーバ上で実行されるフル機能のマルチデバイス マネージャ。
- Device Manager ：デバイスに含まれるシンプルな単独のデバイスマネージャ。
- CDO：クラウドベースのマルチデバイスマネージャ。

ASA

ASA は、高度なステートフル ファイアウォールと VPN コンセントレータの機能を 1 つの装置に組み合わせたものです。次のいずれかのマネージャを使用して ASA を管理できます。

- ASDM：デバイスに含まれるシンプルな単独のデバイス マネージャ。このガイドでは、*ASDM* を使用して *ASA* を管理する方法について説明します。
- CLI
- CDO：クラウドベースのマルチデバイスマネージャ。
- CSM：別のサーバー上のマルチデバイスマネージャ。

Radware DefensePro （デコレータ）

Radware DefensePro（vDP）をインストールし、デコレータアプリケーションとして ASA または 脅威に対する防御 の目の前で実行することができます。vDP は、Firepower 4100/9300 に分散型サービス妨害（DDoS）の検出と緩和機能を提供する KVM ベースの仮想プラットフォームです。ネットワークからのトラフィックは、ASA または 脅威に対する防御 に到達する前に、まず vDP を通過する必要があります。

vDP を展開するには、『FXOS コンフィグレーション ガイド』を参照してください。

論理デバイスのアプリケーションインスタンス：コンテナとネイティブ

論理デバイスのアプリケーション インスタンスは次の展開タイプで実行されます。

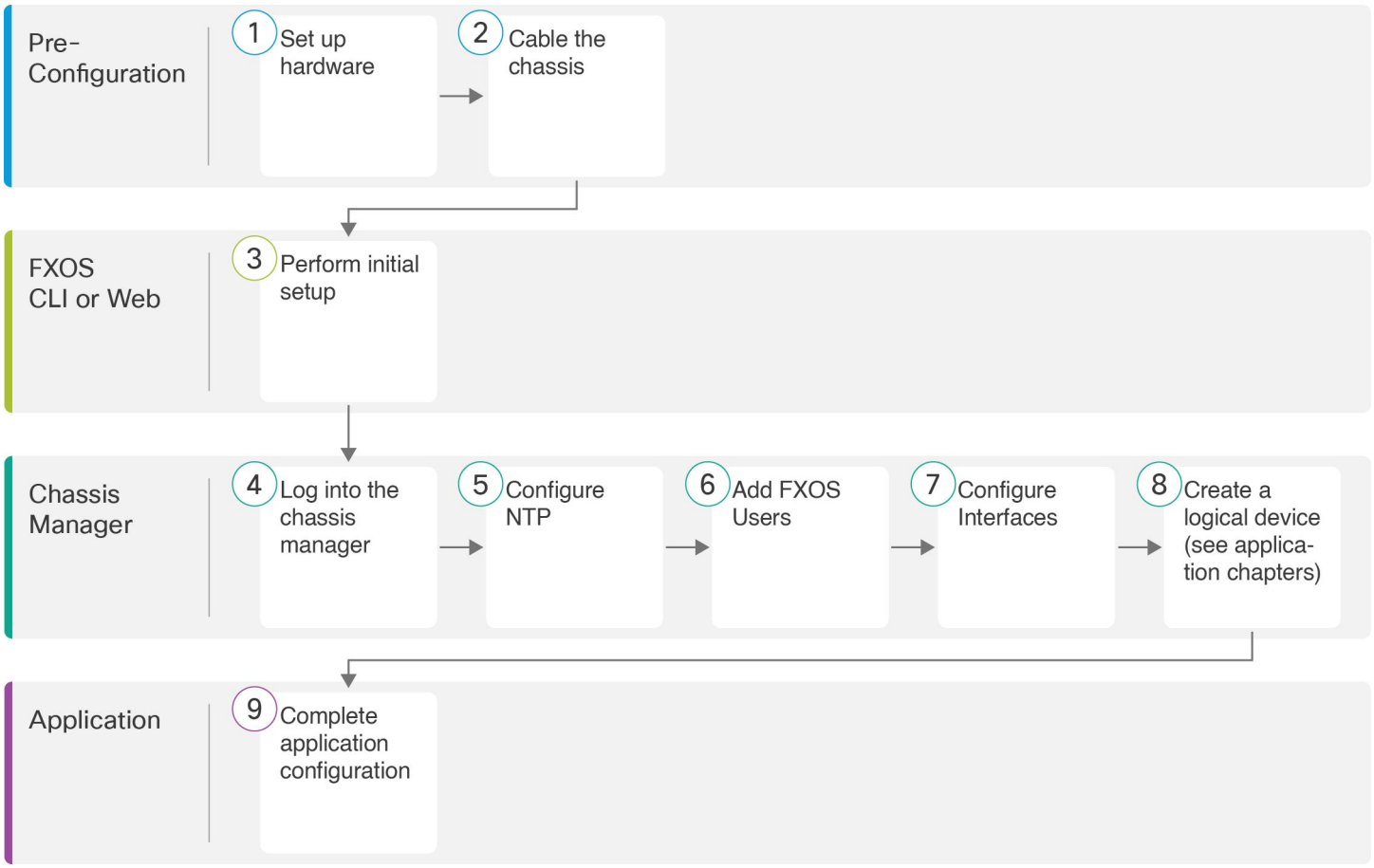
- ネイティブ インスタンス：ネイティブ インスタンスはセキュリティ エンジン のすべてのリソース（CPU、RAM、およびディスク容量）を使用するため、ネイティブ インスタンスを 1 つのみインストールできます。
- コンテナ インスタンス：コンテナ インスタンスでは、セキュリティ エンジン のリソースのサブセットを使用するため、複数のコンテナ インスタンスをインストールできます。
  注：マルチインスタンス機能は、脅威に対する防御 でのみサポートされています。ASA または vDP との組み合わせではサポートされていません。

モデルごとの最大コンテナ インスタンス数

- Firepower 4110：3
- Firepower 4112：3
- Firepower 4115：7
- Firepower 4120：3
- Firepower 4125：10
- Firepower 4140：7
- Firepower 4145—14
- Firepower 4150：7

エンドツーエンドの手順

Firepower 4100 シャーシを設定し、シャーシに論理デバイスを展開するには、次のタスクを参照してください。



1	事前設定	Firepower 4100 ハードウェアをセットアップします。『Firepower 4100 hardware guide』を参照してください。
2	事前設定	シャーシのケーブル接続 （6 ページ）。
3	FXOS CLI または Web	シャーシの初期セットアップの実行 （10 ページ）。
4	Chassis Manager	Chassis Manager へのログイン （14 ページ）。
5	Chassis Manager	NTP の設定 （15 ページ）。
6	Chassis Manager	FXOS ユーザーの追加 （17 ページ）。
7	Chassis Manager	インターフェイスの設定 （19 ページ）。

8	Chassis Manager	論理デバイスを作成します。 • Management Center を使用した Threat Defense ：Management Center での Threat Defense の展開を参照してください。 • Device Manager を使用した Threat Defense ：Device Manager での Threat Defense の展開を参照してください。 • CDO を使用した Threat Defense ：CDO での Threat Defense の展開を参照してください。 • ASA：ASDM を使用した ASA の展開 を参照してください。 （注） Device Manager を使用した 脅威に対する防御 のサポートが FXOS 2.7.1/脅威に対する防御 6.5 で追加されました。
9	アプリケーション	アプリケーション構成を完了します。 • Management Center を使用した Threat Defense ：Management Center での Threat Defense の展開を参照してください。 • Device Manager を使用した Threat Defense ：Device Manager での Threat Defense の展開を参照してください。 • CDO を使用した Threat Defense ：CDO での Threat Defense の展開を参照してください。 • ASA：ASDM を使用した ASA の展開 を参照してください。

シャーシのケーブル接続

シャーシの初期設定、継続的なモニタリング、論理デバイスの使用には、次のインターフェイスにケーブルを配線します。

- コンソールポート：（オプション）シャーシ管理ポートで初期セットアプを実行しない場合は、管理コンピュータをコンソールポートに接続して、シャーシの初期セットアップを実行します。Firepower 4100 には、RS-232 - RJ-45 シリアルコンソールケーブルが付属しています。接続には、サードパーティ製のシリアル - USB ケーブルが必要になる場合があります。
- シャーシ管理ポート：シャーシ管理ポートを管理ネットワークに接続し、シャーシの設定と継続的な管理を行います。この管理ポートで DHCP サーバーから IP アドレスを受信する場合は、このポートで初期セットアップを実行できます。
- 論理デバイス管理インターフェイス: 1 つ以上のインターフェイスを使用して論理デバイスを管理します。このガイドでは、独自のインターネットアクセスを持つ別の管理ネットワークがあることを前提としています。シャーシ管理ポート以外は、シャーシ上の任意の

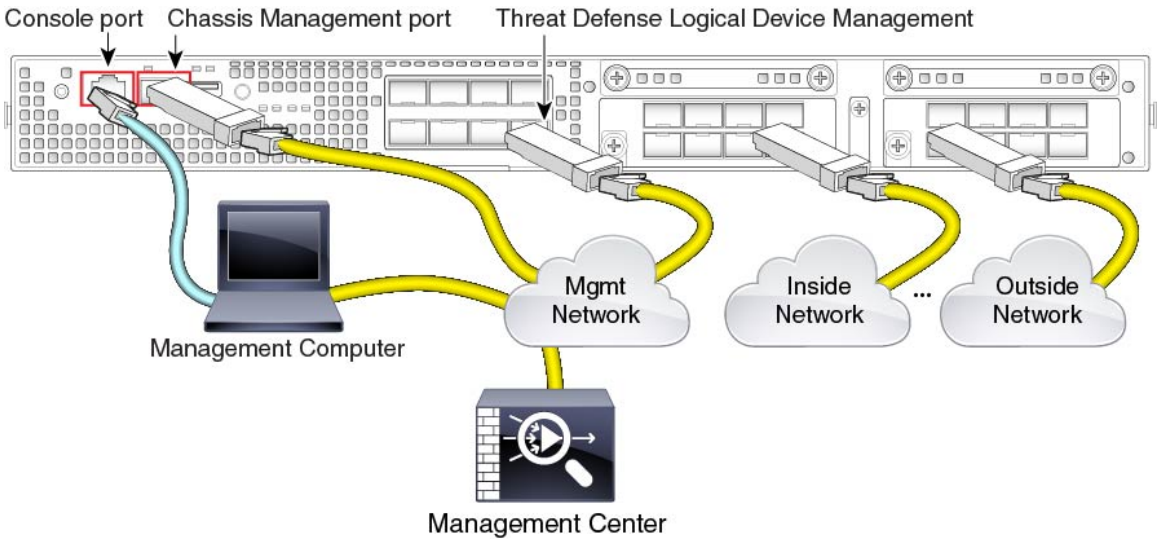
インターフェイスを選択できます。シャーシ管理ポートは、FXOS 管理用に予約されています。マルチインスタンスをサポートする場合、管理インターフェイスを論理デバイス間で共有できます。また、論理デバイスごとに別のインターフェイスを使用することもできます。通常は、管理インターフェイスをすべての論理デバイスと共有します。または、別個のインターフェイスを使用する場合は、それらを単一の管理ネットワークに配置します。ただし、正確なネットワーク要件は場合によって異なります。Threat Defense の場合、管理インターフェイスはデータインターフェイスとは別のインターフェイスであり、独自のネットワーク設定があります。6.7 以降では、管理インターフェイスを使用する代わりに、必要に応じて、データインターフェイスをマネージャアクセス用に設定できます。この場合でも、内部のアーキテクチャ上の理由から管理インターフェイスを論理デバイスに割り当てる必要がありますが、ケーブル接続は必要ありません。Management Center の場合、データインターフェイスからのマネージャアクセスは、高可用性またはクラスタリング展開ではサポートされません。詳細については、『FTD command reference』の **configure network management-data-interface** コマンドを参照してください。

- データインターフェイス：データインターフェイスを論理デバイスデータネットワークに接続します。物理インターフェイス、EtherChannel、VLAN サブインターフェイス（コンテナインスタンスの場合のみ）、およびブレイクアウトポートを設定して、大容量のインターフェイスを分割できます。マルチインスタンスをサポートする場合、ネットワークのニーズに応じて、複数の論理デバイスを同じネットワークまたは異なるネットワークにケーブル接続できます。コンテナインスタンスの場合、データインターフェイスを共有できます。この場合にのみ、複数の論理デバイスがバックプレーンを介して通信できます。それ以外の場合は、別の論理デバイスに到達するために、すべてのトラフィックが 1 つのインターフェイス上のシャーシから出て、別のインターフェイスに戻る必要があります。共有インターフェイスの制限事項とガイドラインの詳細については、『FXOS コンフィグレーション ガイド』を参照してください。

（注） コンソール ポート以外のすべてのインターフェイスには、SFP/SFP+/QSFP のトランシーバーが必要です。サポートされているトランシーバーについては、『Hardware Installation Guide』を参照してください。

（注） このガイドでは説明していませんが、ハイアベイラビリティの場合は、フェールオーバー/ステートリンクにデータインターフェイスを使用します。シャーシ間クラスタリングの場合は、シャーシで定義されている EtherChannel をクラスタ タイプのインターフェイスとして使用します。

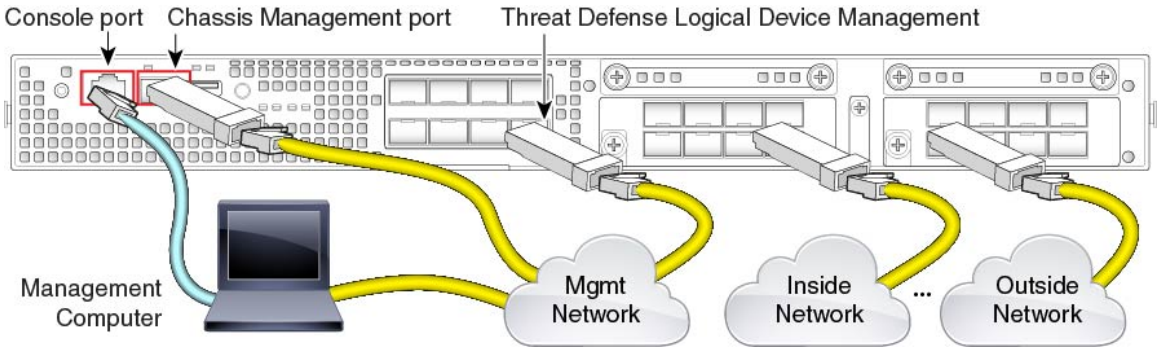
Threat Defense と Management Center のケーブル接続



このガイドでは、独自のインターネットアクセスを持つ別の管理ネットワークがあることを前提としています。デフォルトでは、管理インターフェイスは展開時に事前設定されていますが、データインターフェイスは後で設定する必要があります。

論理デバイス管理ネットワークにManagement Centerを配置（またはアクセス可能に）します。脅威に対する防御 およびManagement Centerは、更新およびライセンシングのために管理ネットワークを介してインターネットにアクセスする必要があります。6.7以降では、管理インターフェイスの代わりに、必要に応じて、データインターフェイスを Management Center の管理用に設定できます。データインターフェイスからの Management Center アクセスは、高可用性またはクラスタリング展開ではサポートされません。Management Center アクセス用のデータインターフェイスの設定の詳細については、FTD コマンドリファレンス [英語] の **configure network management-data-interface** コマンドを参照してください。

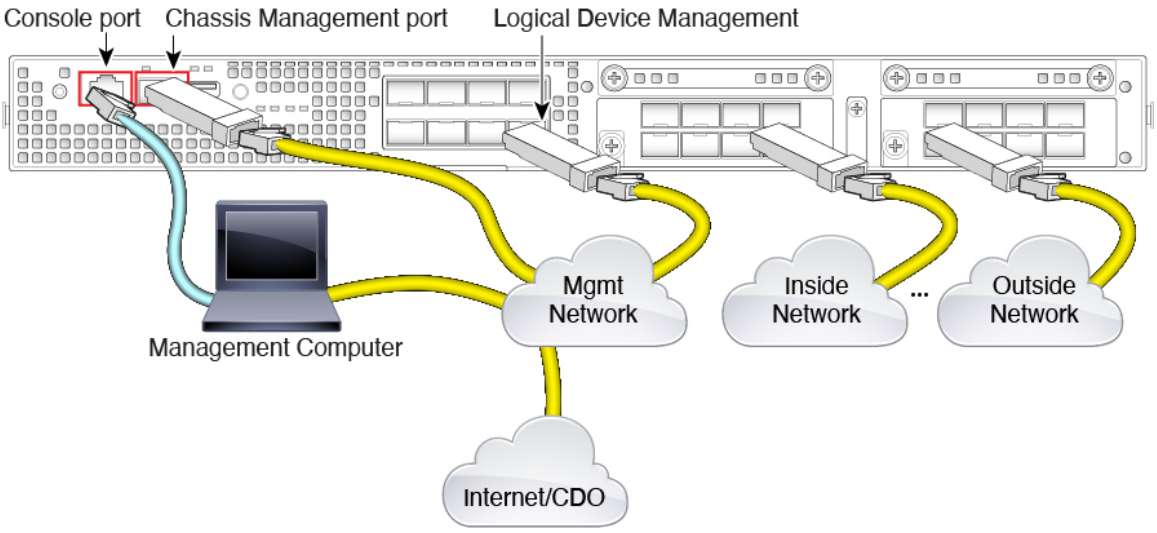
Threat Defense と Device Manager のケーブル接続



このガイドでは、独自のインターネットアクセスを持つ別の管理ネットワークがあることを前提としています。デフォルトでは、管理インターフェイスは展開時に事前設定されていますが、データインターフェイスは後で設定する必要があります。

論理デバイスの管理インターフェイスで 脅威に対する防御 の初期設定を実行します。脅威に対する防御 では、ライセンシング、更新、およびCDOの管理のためにインターネットアクセスが必要です。デフォルトの動作では、脅威に対する防御 の展開時に指定したゲートウェイIPアドレスに管理トラフィックがルーティングされます。後で、任意のデータインターフェイスから Device Manager の管理を有効にできます。

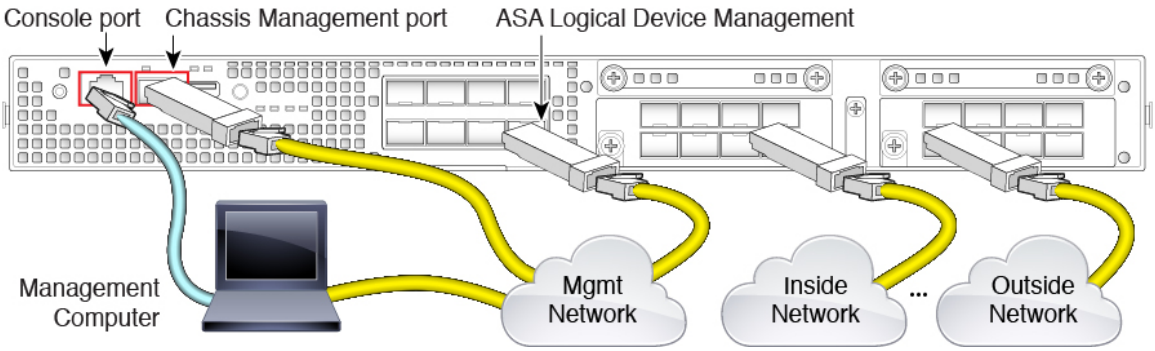
Threat Defense と CDO のケーブル接続



このガイドでは、独自のインターネットアクセスを持つ別の管理ネットワークがあることを前提としています。デフォルトでは、管理インターフェイスは展開時に事前設定されていますが、データインターフェイスは後で設定する必要があります。

論理デバイスの管理ネットワークからインターネットにアクセスできることを確認します。脅威に対する防御 は、CDOの管理、更新、およびライセンシングのために、管理ネットワーク経由でインターネットにアクセスする必要があります。管理インターフェイスの代わりに、必要に応じて、データインターフェイスをCDOの管理用に設定できます。マネージャアクセス用のデータインターフェイスの設定の詳細については、FTD コマンドリファレンス [英語] の **configure network management-data-interface** コマンドを参照してください。

ASA のケーブル接続



このガイドでは、独自のインターネットアクセスを持つ別の管理ネットワークがあることを前提としています。デフォルトでは、管理インターフェイスは展開時に事前設定されていますが、データインターフェイスは後で設定する必要があります。

論理デバイスの管理インターフェイスで ASA の初期設定を実行します。後で、任意のデータインターフェイスから管理を有効にすることができます。

シャーシの初期セットアップの実行

システムの設定と管理に Chassis Manager を使用する前に、いくつかの初期設定タスクを実行する必要があります。初期設定は、コンソールポートで FXOS CLI を使用するか、またはシャーシ管理ポートへの SSH セッションを使用するか、あるいはシャーシ管理ポートで HTTPS を使用して実行できます。

ブラウザを使用したシャーシの初期セットアップの実行

シャーシ管理ポートは、DHCP を使用して IP アドレスを取得します。初期設定では、Web ブラウザを使用してシャーシの基本設定を行うことができます。DHCP サーバーがない場合は、初期セットアップにコンソールポートを使用する必要があります。

（注） 初期セットアップを繰り返すには、CLI から次のコマンドを使用して既存の設定をすべて消去する必要があります。

```
Firepower-chassis# connect local-mgmt
firepower-chassis(local-mgmt)# erase configuration
```

始める前に

セットアップ スクリプトで使用する次の情報を収集します。

- 新しい管理者パスワード
- 管理 IP アドレスおよびサブネット マスク
- ゲートウェイ IP アドレス
- HTTPS と SSH アクセスを許可するサブネット
- ホスト名とドメイン名
- DNS サーバの IP アドレス

手順

ステップ 1 DHCP サーバーを設定してシャーシ管理ポートに IP アドレスを割り当てます。

シャーシからの DHCP クライアント要求には次の情報が含まれています。

- 管理インターフェイスの MAC アドレス。
- DHCP オプション 60（vendor-class-identifier）：「FPR4100」に設定します。
- DHCP オプション 61（dhcp-client-identifier）：シャーシのシリアル番号に設定します。このシリアル番号は、シャーシの引き出しタブで確認できます。

ステップ 2 シャーシの電源を入れます。

ステップ 3 ブラウザで次の URL を入力します。

https://*ip_address*/**api**

DHCP サーバーによってシャーシ管理ポートに割り当てられた IP アドレスを指定します。

ステップ 4 ユーザー名とパスワードの入力を求められたら、それぞれ **install** と *chassis_serial_number* を入力してログインします。

chassis_serial_number は、シャーシのプルアウトタブで確認できます。

ステップ 5 プロンプトに従ってシステム設定を行います。

- 強力なパスワード適用ポリシー。
- admin アカウントのパスワード。
- システム名。
- スーパーバイザ管理の IPv4 アドレスとサブネット マスク、または IPv6 アドレスとプレフィックス。
- デフォルト ゲートウェイの IPv4 アドレスまたは IPv6 アドレス。
- SSH アクセスが許可されているホスト/ネットワーク アドレスおよびネットマスク/プレフィックス。
- HTTPS アクセスが許可されるホスト/ネットワークアドレスとネットマスク/プレフィックス。
- DNS サーバの IPv4 または IPv6 アドレス。
- デフォルト ドメイン名。

ステップ 6 **[送信（Submit）]** をクリックします。

CLI でのシャーシの初期セットアップの実行

コンソールで FXOS CLI に初めてアクセスするか、またはシャーシ管理ポートに対して SSH セッションを使用すると、セットアップウィザードによって基本的なネットワーク設定を求めるプロンプトが表示され、シャーシ管理ポートから Chassis Manager（HTTPS を使用）または FXOS CLI（SSH を使用）にアクセスできるようになります。

シャーシ管理ポートは、DHCP を使用して IP アドレスを取得します。DHCP サーバーがない場合は、初期セットアップにコンソールポートを使用する必要があります。

（注） 初期設定を繰り返すには、次のコマンドを使用して既存の設定をすべて消去する必要があります。

```
Firepower-chassis# connect local-mgmt
firepower-chassis(local-mgmt)# erase configuration
```

始める前に

セットアップ スクリプトで使用する次の情報を収集します。

- 新しい管理者パスワード
- 管理 IP アドレスおよびサブネット マスク
- ゲートウェイ IP アドレス
- HTTPS および SSH アクセスを許可するサブネット
- ホスト名とドメイン名
- DNS サーバの IP アドレス

手順

ステップ 1 シャーシの電源を入れます。

ステップ 2 ターミナルエミュレータを使用してシリアルコンソールポートに接続するか SSH を使用してシャーシ管理ポートに接続します。

Firepower 4100 には、RS-232 - RJ-45 シリアルコンソールケーブルが付属しています。接続には、サードパーティ製のシリアル - USB ケーブルが必要になる場合があります。次のシリアルパラメータを使用します。

- 9600 ボー
- 8 データ ビット
- パリティなし

- 1 ストップ ビット

ステップ 3 ユーザー名とパスワードの入力を求められたら、それぞれ **admin** と **cisco123** を入力してログインします。

ステップ 4 プロンプトに従ってシステム設定を行います。

例：

```
          ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Only minimal configuration including IP connectivity to
the FXOS Supervisor is performed through these steps.

Type Ctrl-C at any time for more options or to abort configuration
and reboot system.
To back track or make modifications to already entered values,
complete input till end of section and answer no when prompted
to apply configuration.


You have chosen to setup a new Security Appliance.
      Continue? (yes/no): y

Enforce strong password? (yes/no) [y]: n

Enter the password for "admin": Farscape&32
Confirm the password for "admin": Farscape&32
Enter the system name:  firepower-4125

Supervisor Mgmt IP address : 10.80.6.12

Supervisor Mgmt IPv4 netmask : 255.255.255.0

IPv4 address of the default gateway : 10.80.6.1

The system cannot be accessed via SSH if SSH Mgmt Access is not configured.

Do you want to configure SSH Mgmt Access? (yes/no) [y]: y

SSH Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

SSH Mgmt Access IPv4 netmask: 255.0.0.0

Firepower Chassis Manager cannot be accessed if HTTPS Mgmt Access is not configured.

Do you want to configure HTTPS Mgmt Access? (yes/no) [y]: y

HTTPS Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

HTTPS Mgmt Access IPv4 netmask: 255.0.0.0

Configure the DNS Server IP address? (yes/no) [n]: y

  DNS IP address : 10.164.47.13

Configure the default domain name? (yes/no) [n]: y

  Default domain name : cisco.com

Following configurations will be applied:
```

```
    Switch Fabric=A
    System Name=firepower-4125
    Enforced Strong Password=no
    Supervisor Mgmt IP Address=10.89.5.14
    Supervisor Mgmt IP Netmask=255.255.255.192
    Default Gateway=10.89.5.1
    SSH Access Configured=yes
        SSH IP Address=10.0.0.0
        SSH IP Netmask=255.0.0.0
    HTTPS Access Configured=yes
        HTTPS IP Address=10.0.0.0
        HTTPS IP Netmask=255.0.0.0
    DNS Server=72.163.47.11
    Domain Name=cisco.com

  Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): y
  Applying configuration. Please wait...  Configuration file - Ok
.....

Cisco FPR Series Security Appliance
firepower-9300 login:  admin
Password: Farscape&32
Successful login attempts for user 'admin' : 1
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2019, Cisco Systems, Inc. All rights reserved.

[...]

firepower-chassis#
```

ステップ 5 使用している場合はコンソールポートから切断したり、SSHセッションを終了することができます。

Chassis Manager へのログイン

Chassis Manager を使用して、インターフェイスの有効化や論理デバイスの展開など、シャーシの設定を行います。

始める前に

- サポートされるブラウザの詳細については、使用しているバージョンのリリース ノートを参照してください（http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.html を参照）。
- 最初のシャーシのセットアップ時に指定した範囲内の IP アドレスを持つ管理コンピュータからのみ、Chassis Manager にアクセスできます。

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://*chassis_mgmt_ip_address*

- *chassis_mgmt_ip_address*：初期設定時に入力したシャーシ管理ポートの IP アドレスまたはホスト名です。

ステップ 2 ユーザー名 **admin** と新しいパスワードを入力します。

FXOS ユーザーの追加 （17 ページ） に従って、後でさらにユーザーを追加できます。

ステップ 3 [ログイン（Login）] をクリックします。
ログインすると Chassis Manager が開き、[概要（Overview）] ページが表示されます。

NTP の設定

手動で時刻を設定することもできますが、NTP サーバーを使用することを推奨します。ASA および 脅威に対する防御 と Device Manager のスマート ソフトウェア ライセンシングには正しい時刻が必要です。脅威に対する防御 と Management Center の場合は、シャーシと Management Center の間で時刻が一致している必要があります。この場合は、Management Center の場合と同じ NTP サーバーをシャーシで使用することを推奨します。Management Center 自身を NTP サーバーとして使用しないでください。この方法はサポートされていません。

始める前に

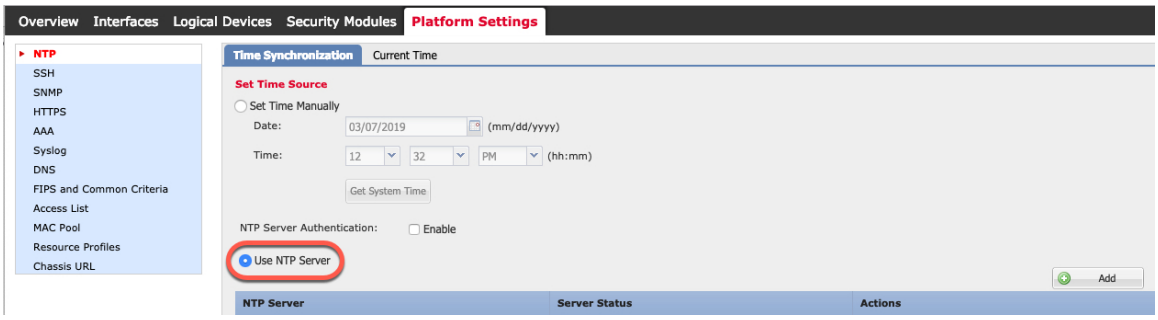
NTP サーバーのホスト名を使用する場合は、DNS サーバーを設定する必要があります（最初のセットアップで未実施の場合）。**[プラットフォーム設定（Platform Settings）]** > **[DNS]** を参照してください。

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[NTP]** を選択します。

[時間同期（Time Synchronization）] ページがデフォルトで選択されています。

ステップ 2 [NTPサーバーを使用する（Use NTP Server）] オプション ボタンをクリックします。

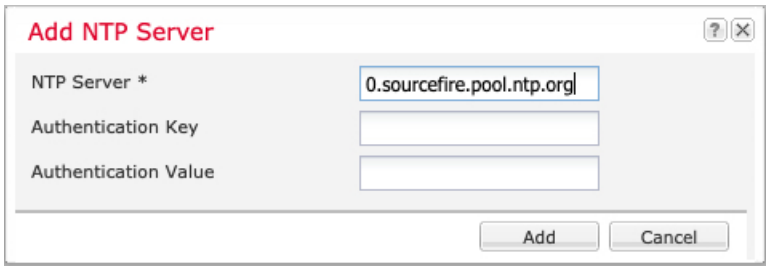


ステップ 3 （任意） NTP サーバーで認証が必要な場合は、[NTPサーバー認証：有効（NTP Server Authentication: Enable）] チェックボックスをオンにします。

NTP 認証を有効にすることが求められます。すべての NTP サーバー エントリで認証キーの ID と値を必要とする場合は、[Yes] をクリックします。

NTP サーバー認証では SHA1 のみがサポートされます。

ステップ 4 [追加（Add）] をクリックし、次のパラメータを設定します。



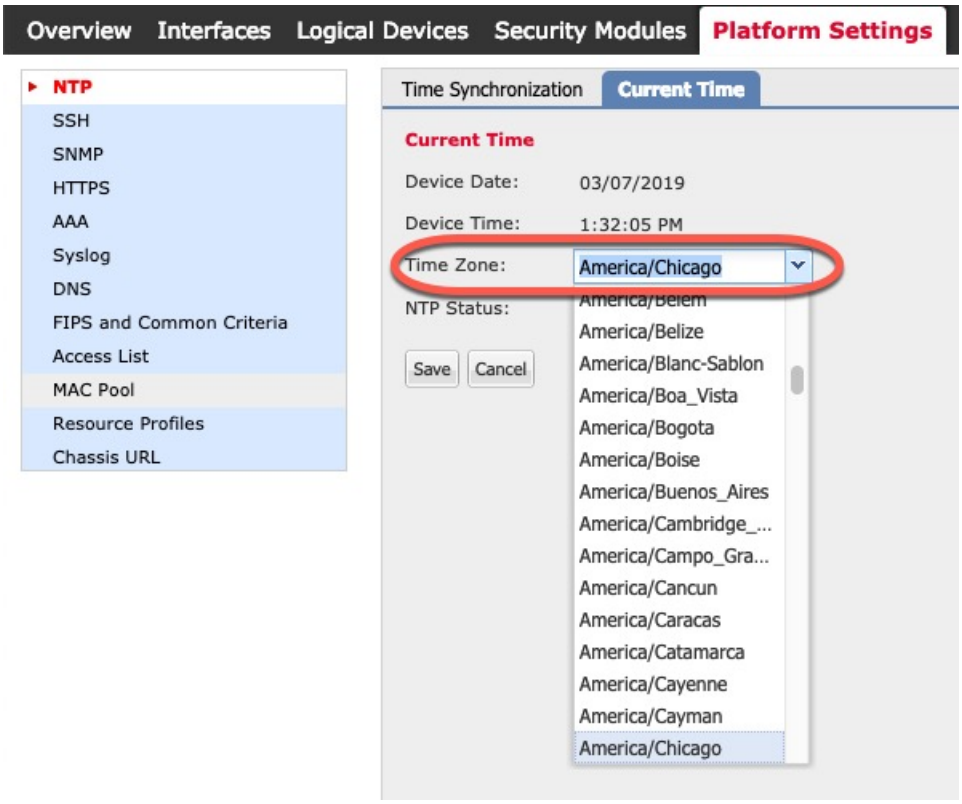
- [NTPサーバー（NTP Server）]：NTP サーバーの IP アドレスまたはホスト名
- [認証キー（Authentication key）] および [認証値（authentication VALUE）]：NTP サーバーからキー ID と値を取得します。たとえば、OpenSSL がインストールされた NTP サーバ バージョン 4.2.8 p8 以降で SHA1 キーを生成するには、**ntp-keygen -M** コマンドを入力して ntp. keys ファイルでキー ID と値を確認します。このキーは、クライアントとサーバの両方に対して、メッセージダイジェストの計算時に使用するキー値を通知するために使用します。

ステップ 5 [追加（Add）] をクリックしてサーバーを追加します。

NTP サーバーは最大 4 つまで追加できます。

ステップ 6 [保存（Save）] をクリックしてサーバーを保存します。

ステップ 7 [現在時刻（Current Time）] をクリックし、[タイムゾーン（Time Zone）] ドロップダウンリストからシャーシに適したタイム ゾーンを選択します。



ステップ 8 [保存（Save）] をクリックします。

（注） システム時刻の変更に10分以上かかると、自動的にログアウトされ、Chassis Manager への再ログインが必要になります。

FXOS ユーザーの追加

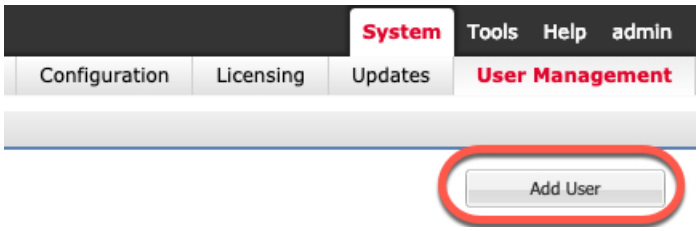
Chassis Manager および FXOS CLI ログインのローカルユーザーを追加します。

手順

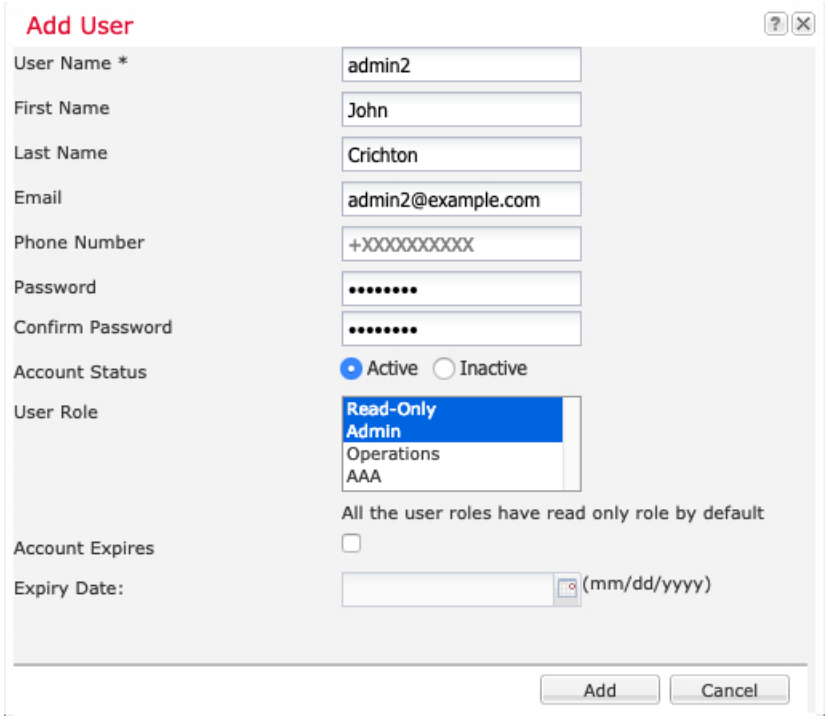
ステップ 1 **[システム（System）] > [ユーザー管理（User Management）]** を選択します。

ステップ 2 [ローカルユーザー（Local Users）] をクリックします。

ステップ 3 [ユーザの追加（Add User）] をクリックして [ユーザの追加（Add User）] ダイアログボックスを開きます。



ステップ 4 ユーザに関して要求される情報を使用して、次のフィールドに値を入力します。



- [ユーザー名（User Name）]：最大 32 文字のユーザー名を設定します。ユーザを保存した後は、ログイン ID を変更できません。ユーザ アカウントを削除し、新しいユーザ アカウントを作成する必要があります。
- （任意）[名（First name）]：ユーザーの名前を最大 32 文字で設定します。
- （任意）[姓（Last name）]：ユーザーの姓を最大 32 文字で設定します。
- （任意）[電子メール（Email）]：ユーザーの電子メール アドレスを設定します。
- （任意）[電話番号（Phone Number）]：ユーザーの電話番号を設定します。
- [パスワード（Password）]および[パスワードの確認（Confirm Password）]：このアカウントに関連付けられているパスワードを設定します。パスワード強度チェックを有効にした場合は、ユーザーパスワードを強固なものにする必要があります。FXOS は強度チェック要件を満たしていないパスワードを拒否します。強力なパスワードのガイドラインについては、『FXOS コンフィグレーション ガイド』を参照してください。

- [アカウントステータス（Account status）]：ステータスを[アクティブ（Active）]または[非アクティブ（Inactive）]に設定します。
- [ユーザーロール（User Role）]：ユーザー アカウントに割り当てる権限を表すロールを設定します。すべてのユーザーはデフォルトでは [読み取り専用（Read-Only）] ロールが割り当てられます。このロールは選択解除できません。別のロールを割り当てるには、ウィンドウ内のロール名をクリックして、そのロールが強調表示されるようにします。次のユーザー ロールのいずれかを使用できます。
  - [管理（Admin）]：システム全体に対する完全な読み取りと書き込みのアクセス権。
  - [読み取り専用（Read-Only）]：システム設定に対する読み取り専用アクセス権。システム状態を変更する権限はありません。
  - [運用（Operations）]：NTP の設定、Smart Licensing のための Smart Call Home の設定、システム ログ（syslog サーバーとエラーを含む）に対する読み取りと書き込みのアクセス権。システムの残りの部分に対する読み取りアクセス権。
  - [AAA管理者（AAA Administrator）]：ユーザー、ロール、および AAA 設定に対する読み取りと書き込みのアクセス権。システムの残りの部分に対する読み取りアクセス権。
- （任意）[アカウント有効期限（Account expires）]：このアカウントの有効期限を設定します。アカウントは、[有効期限（Expiry Date）] フィールドで指定された日付の後には使用できません。ユーザアカウントに有効期限を設定した後、「有効期限なし」に再設定することはできません。ただし、使用できる最新の有効期限日付でアカウントを設定することは可能です。デフォルトでは、ユーザー アカウントの有効期限はありません。
- （任意）[有効期限（Expiry Date）]：アカウントが期限切れになる日付。日付の形式は *yyyy-mm-dd* です。このフィールドの終端にあるカレンダー アイコンをクリックするとカレンダーが表示され、それを使用して期限日を選択できます。

ステップ 5 [追加（Add）] をクリックします。

インターフェイスの設定

デフォルトでは、物理インターフェイスは無効になっています。FXOS では、インターフェイスを有効にし、EtherChannels を追加して、VLAN サブインターフェイスを追加し、インターフェイスプロパティを編集できます。インターフェイスを使用するには、インターフェイスを FXOS で物理的に有効にし、アプリケーションで論理的に有効にする必要があります。

ブレイクアウト ポートを設定するには、『FXOS コンフィグレーション ガイド』を参照してください。

インターフェイス タイプ

各インターフェイスは、次のいずれかのタイプになります。

- Data：通常のデータに使用します。データインターフェイスを論理デバイス間で共有することはできません。また、論理デバイスからバックプレーンを介して他の論理デバイスに通信することはできません。データインターフェイスのトラフィックの場合、すべてのトラフィックは別の論理デバイスに到達するために、あるインターフェイスでシャーシを抜け出し、別のインターフェイスで戻る必要があります。
- Data-sharing：通常のデータに使用します。コンテナインスタンスでのみサポートされ、これらのデータインターフェイスは 1 つまたは複数の論理デバイス/コンテナインスタンス（脅威に対する防御 Management Center 専用）で共有できます。 各コンテナ インスタンスは、このインターフェイスを共有する他のすべてのインスタンスと、バックプレーン経由で通信できます。共有インターフェイスは、展開可能なコンテナインスタンスの数に影響することがあります。共有インターフェイスは、ブリッジグループ メンバーインターフェイス（トランスペアレントモードまたはルーテッドモード）、インラインセット、パッシブインターフェイス、クラスタ、またはフェールオーバーリンクではサポートされません。
- Mgmt：アプリケーション インスタンスの管理に使用します。これらのインターフェイスは、外部ホストにアクセスするために1つまたは複数の論理デバイスで共有できます。論理デバイスが、このインターフェイスを介して、インターフェイスを共有する他の論理デバイスと通信することはできません。各論理デバイスには、管理インターフェイスを1つだけ割り当てることができます。アプリケーションと管理によっては、後でデータインターフェイスから管理を有効にできます。ただし、データ管理を有効にした後で使用する予定がない場合でも、管理インターフェイスを論理デバイスに割り当てる必要があります。

（注） 管理インターフェイスを変更すると、論理デバイスが再起動します。たとえば、e1/1 から e1/2 に1回変更すると、論理デバイスが再起動して新しい管理が適用されます。

- Eventing： Management Center デバイスを使用した 脅威に対する防御 のセカンダリ管理インターフェイスとして使用します。このインターフェイスを使用するには、脅威に対する防御 CLI で IP アドレスなどのパラメータを設定する必要があります。たとえば、イベント（Webイベントなど）から管理トラフィックを分類できます。詳細については、管理センター構成ガイドを参照してください。Eventing インターフェイスは、外部ホストにアクセスするために1つまたは複数の論理デバイスで共有できます。論理デバイスはこのインターフェイスを介してインターフェイスを共有する他の倫理デバイスと通信することはできません。 後で管理用のデータインターフェイスを設定する場合は、別のイベントインターフェイスを使用できません。

（注） 各アプリケーションインスタンスのインストール時に、仮想イーサネットインターフェイスが割り当てられます。アプリケーションがイベントインターフェイスを使用しない場合、仮想インターフェイスは管理上ダウンの状態になります。

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- Cluster：クラスタ化された論理デバイスのクラスタ制御リンクとして使用します。デフォルトでは、クラスタ制御リンクは 48 番のポートチャネル上に自動的に作成されます。クラスタタイプは、EtherChannelインターフェイスのみでサポートされます。マルチインスタンスクラスタリングの場合、デバイス間でクラスタタイプのインターフェイスを共有することはできません。各クラスタが別個のクラスタ制御リンクを使用でできるように、クラスタ EtherChannel に VLAN サブインターフェイスを追加できます。クラスタインターフェイスにサブインターフェイスを追加した場合、そのインターフェイスをネイティブクラスタには使用できません。Device Manager および CDO はクラスタリングをサポートしていません。

論理デバイスを展開する前に、管理インターフェイスと少なくとも 1 つのデータ（またはデータ共有）インターフェイスを設定する必要があります。

物理インターフェイスの設定

インターフェイスを物理的に有効および無効にすること、およびインターフェイスの速度とデュプレックスを設定することができます。インターフェイスを使用するには、インターフェイスをFXOS で物理的に有効にし、アプリケーションで論理的に有効にする必要があります。

始める前に

すでに EtherChannel のメンバーであるインターフェイスは個別に変更できません。インターフェイスを EtherChannel に追加する前に、設定を行ってください。

手順

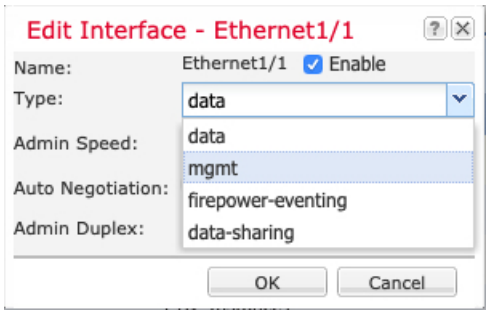
ステップ 1 [インターフェイス（Interfaces）] をクリックします。

[すべてのインターフェイス（All Interfaces）] ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。

ステップ 2 編集するインターフェイスの をクリックし、[インターフェイスを編集（Edit Interface）] ダイアログボックスを開きます。

ステップ 3 **[有効（Enable）]** チェックボックスをオンにします。

ステップ 4 インターフェイスの [タイプ（Type）] を次から選択します。**Data**、**Data-sharing**、**Mgmt**、または **Firepower-eventing**



（注） データ共有タイプのインターフェイスを使用する場合は、制限があります。詳細については、『FXOS コンフィグレーション ガイド』を参照してください。

Firepower-eventing 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。

ステップ 5 （任意） インターフェイスの [速度（Speed）] を選択します。

ステップ 6 （任意） インターフェイスで [自動ネゴシエーション（Auto Negotiation）] がサポートされている場合は、[はい（Yes）] または [いいえ（No）] オプション ボタンをクリックします。

ステップ 7 （任意） インターフェイスの [デュプレックス（Duplex）] を選択します。

ステップ 8 [OK] をクリックします。

EtherChannel（ポート チャネル）の追加

EtherChannel（ポートチャネルとも呼ばれる）は、同じメディアタイプと容量の最大 16 個のメンバーインターフェイスを含むことができ、同じ速度とデュプレックスに設定する必要があります。メディアタイプは RJ-45 または SFP のいずれかです。異なるタイプ（銅と光ファイバ）の SFP を混在させることができます。容量の大きいインターフェイスで速度を低く設定することによってインターフェイスの容量（1 GB インターフェイスと 10 GB インターフェイスなど）を混在させることはできません。

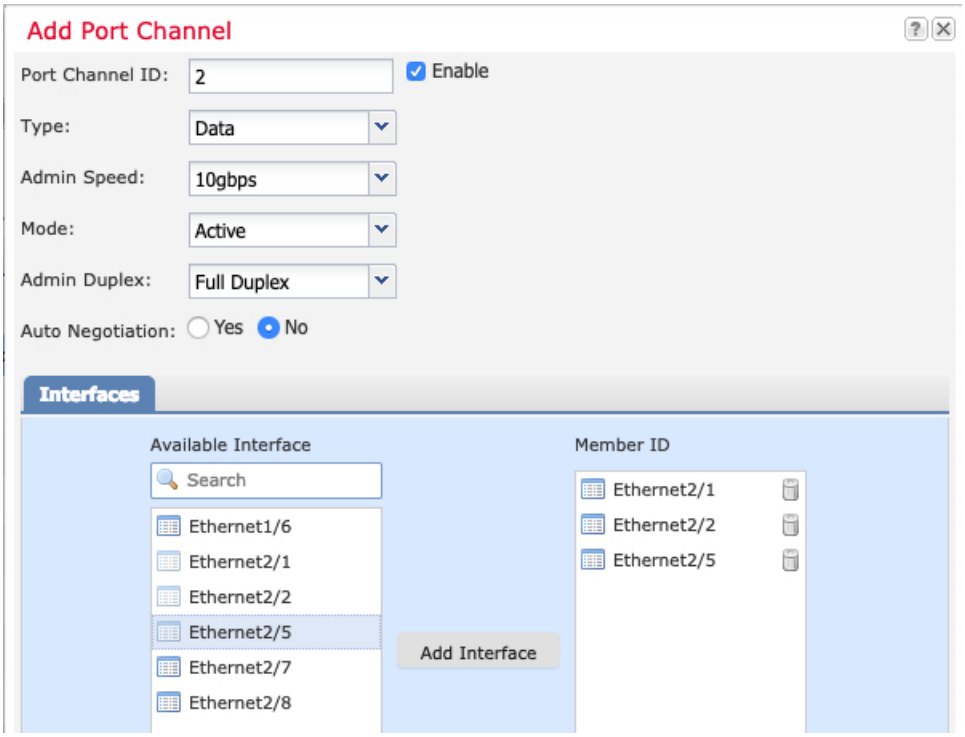
（注） シャーシが EtherChannel を作成すると、EtherChannel は [一時停止（Suspended）] 状態（Active LACP モードの場合）または [ダウン（Down）] 状態（On LACP モードの場合）になり、物理リンクがアップしても論理デバイスに割り当てるまでそのままになります。

手順

ステップ 1 [インターフェイス（Interfaces）] をクリックします。

[すべてのインターフェイス（All Interfaces）] ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。

ステップ 2 **[新規追加（Add New）] > [ポートチャネル（Port Channel）]** をクリックします。



ステップ 3 [ポートチャネルID（Port Channel ID）] に、1 ～ 47 の値を入力します。

ステップ 4 **[有効（Enable）]** チェックボックスをオンにします。

ステップ 5 インターフェイスの [タイプ（Type）] を選択します。

- **データ**
- [データ共有（Data-sharing）]：コンテナインスタンスのみ。
- **管理**
- [Firepower-eventing]：Threat Defense のみ。
- [クラスタ（Cluster）]：クラスタリングの場合のみ。

（注） データ共有タイプのインターフェイスを使用する場合は、制限があります。詳細については、『FXOS コンフィグレーション ガイド』を参照してください。

Firepower-eventing 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。

ステップ 6 ドロップダウン リストでメンバ インターフェイスの [Admin Speed] を設定します。

ステップ 7 データまたはデータ共有インターフェイスに対して、LACP ポートチャネル [Mode]、[Active] または [On] を選択します。

非データまたはデータ共有インターフェイスの場合、モードは常にアクティブです。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。

ステップ 8 ドロップダウン リストから [管理デュプレックス（Admin Duplex）] を設定します。

ステップ 9 インターフェイスをポートチャネルに追加するには、[使用可能なインターフェイス（Available Interface）] リストでインターフェイスを選択し、[インターフェイスの追加（Add Interface）] をクリックして、そのインターフェイスを [メンバID（Member ID）] リストに移動します。

最大 16 個のインターフェイスを追加できます。

ヒント 一度に複数のインターフェイスを追加できます。複数の個別インターフェイスを選択するには、**Ctrl** キーを押しながら目的のインターフェイスをクリックします。一連のインターフェイスを選択するには、その範囲の最初のインターフェイスを選択し、**Shift** キーを押しながら最後のインターフェイスをクリックして選択します。

ステップ 10 ポート チャネルからインターフェイスを削除するには、[メンバID（Member ID）] リストのインターフェイスの右側にある をクリックします。

ステップ 11 [OK] をクリックします。

コンテナ インスタンスの VLAN サブインターフェイスの追加

シャーシには最大500個のサブインターフェイスを追加できます。サブインターフェイスはコンテナ インスタンスでのみサポートされます。詳細については、論理デバイスのアプリケーション インスタンス：コンテナとネイティブ （3 ページ） を参照してください。

マルチインスタンス クラスタリングの場合、クラスタタイプのインターフェイスにサブインターフェイスを追加するだけです。データインターフェイス上のサブインターフェイスはサポートされません。

インターフェイスごとの VLAN ID は一意である必要があります。コンテナ インスタンス内では、VLAN ID は割り当てられたすべてのインターフェイス全体で一意である必要があります。異なるコンテナ インターフェイスに割り当てられている限り、VLAN ID を別のインターフェイス上で再利用できます。ただし、同じ ID を使用していても、各サブインターフェイスが制限のカウント対象になります。

アプリケーション内にサブインターフェイスを追加することもできます。FXOS サブインターフェイスとアプリケーションサブインターフェイスを使用するタイミングの詳細については、「FXOS コンフィグレーション ガイド」を参照してください。

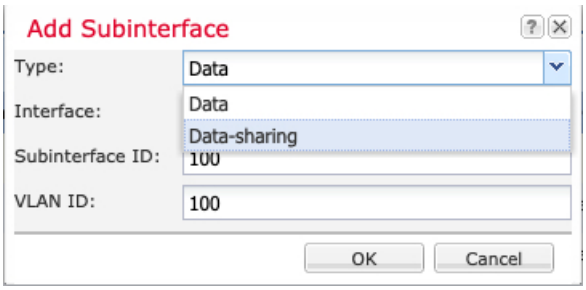
手順

ステップ 1 [インターフェイス（Interfaces）] をクリックします。

[すべてのインターフェイス（All Interfaces）] ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。

ステップ 2 **[Add New** > **Subinterface]** をクリックして [Add Subinterface] ダイアログボックスを開きます。

ステップ 3 インターフェイスの [タイプ（Type）] を選択します。



- **データ**
- **データ共有**
- [クラスタ（Cluster）]：クラスタインターフェイスにサブインターフェイスを追加した場合、そのインターフェイスをネイティブクラスタに使用できません。

データインターフェイスおよびデータ共有インターフェイスの場合：タイプは、親インターフェイスのタイプに依存しません。たとえば、データ共有の親とデータサブインターフェイスを設定できます。

データ共有タイプのインターフェイスを使用する場合は、制限があります。詳細については、『FXOS コンフィグレーション ガイド』を参照してください。

ステップ 4 ドロップダウン リストから親**インターフェイス**を選択します。

現在論理デバイスに割り当てられている物理インターフェイスにサブインターフェイスを追加することはできません。親の他のサブインターフェイスが割り当てられている場合、その親インターフェイス自体が割り当てられていない限り、新しいサブインターフェイスを追加できます。

ステップ 5 [Subinterface ID] を 1 ～ 4294967295 で入力します。

この ID は、*interface_id.subinterface_id* のように親インターフェイスの ID に追加されます。たとえば、サブインターフェイスを ID 100 でイーサネット 1/1 に追加する場合、そのサブインターフェイス ID はイーサネット 1/1.100 になります。利便性を考慮して一致するように設定することができますが、この ID は VLAN ID と同じではありません。

ステップ 6 1 ～ 4095 の間で [VLAN ID] を設定します。

ステップ 7 [OK] をクリックします。

親インターフェイスを展開し、その下にあるすべてのサブインターフェイスを表示します。

ソフトウェア イメージのシャーシへのアップロード

この手順では、FXOS イメージのアップグレード方法だけでなく、新しい FXOS およびアプリケーション イメージをアップロードする方法について説明します。事前にインストールされたイメージが必要なバージョンではない場合は、新しいイメージのアップロードが必要になることがあります。

始める前に

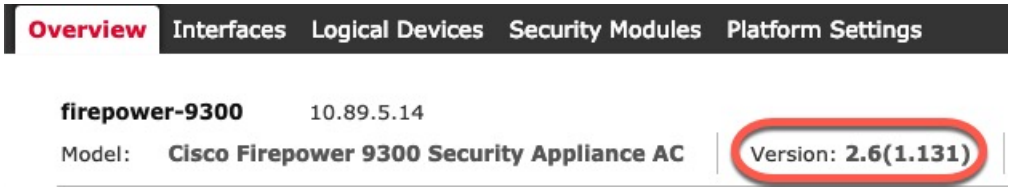
- FXOS 互換性ガイド [英語] で、FXOS、ASA、および 脅威に対する防御 バージョン間の互換性を確認します。
- アップロードするイメージがローカル コンピュータで使用可能であることを確認します。Firepower 4100 の FXOS およびアプリケーション ソフトウェアを取得するには、次を参照してください。

  http://www.cisco.com/go/firepower4100-software
- HTTPS セッション中にアップロードが成功するようにするには、FXOS CLI で絶対タイムアウトを変更する必要があることがあります。絶対タイムアウトは 60 分（最大）であり、大規模なアップロードには 60 分以上かかる場合があります。絶対タイムアウトを無効にするには、次のように入力します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope default-auth
Firepower-chassis /security/default-auth # set absolute-session-timeout 0
Firepower-chassis /security/default-auth* # commit-buffer
```

手順

ステップ 1 現在の FXOS のバージョンを確認するには、[概要（Overview）] ページを参照してください。



次のステップで、シャーシで現在使用可能なアプリケーション イメージを表示できます。

ステップ 2 **[システム（System）] > [更新（Updates）]** を選択します。

[使用可能な更新（Available Updates）] ページに、FXOS のプラットフォーム バンドルのイメージやアプリケーションのイメージのリストが表示されます。

ステップ 3 [イメージのアップロード（Upload Image）] をクリックして、[イメージのアップロード（Upload Image）] ダイアログボックスを開きます。

ステップ 4 [Browse] をクリックし、アップロードするイメージまで移動して選択します。

ステップ 5 [Upload] をクリックします。選択したイメージがシャーシにアップロードされます。

[イメージのアップロード（Upload image）] ダイアログボックスに経過表示バーが表示され、イメージのアップロードが完了すると、[成功（Success）] ダイアログボックスが表示されます。

ステップ 6 FXOS イメージをアップグレードするには、以下を実行します。

a) アップグレードする FXOS プラットフォーム バンドルの アップグレードアイコン（）をクリックします。

b) [はい（Yes）] をクリックして、インストールを続行することを確認します。

シャーシがリロードします。アップグレード プロセスには通常 20 ～ 30 分かかります。

FXOS の履歴

機能名	バージョン	機能情報
コンテナインスタンスで使用される VLAN サブインターフェイス	2.4.1	柔軟な物理インターフェイスの使用を可能にするため、FXOS で VLAN サブインターフェイスを作成し、複数のインスタンス間でインターフェイスを共有することができます。 （注） Threat Defense バージョン 6.3 以降が必要です。 新規/変更された画面： **[Interfaces]** > **[All Interfaces]** > **[Add New]** ドロップダウン メニュー > **[Subinterface]** 新規/変更された Management Center 画面： **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[編集（Edit）]** アイコン > **[インターフェイス（Interfaces）]**
コンテナインスタンスのデータ共有インターフェイス	2.4.1	柔軟な物理インターフェイスの使用を可能にするため、複数のインスタンス間でインターフェイスを共有することができます。 （注） Threat Defense バージョン 6.3 以降が必要です。 新規/変更された画面： **[Interfaces]** > **[All Interfaces]** > **[Type]**

機能名	バージョン	機能情報
オンモードでのデータ EtherChannel のサポート	2.4.1	データおよびデータ共有 EtherChannel をアクティブ LACP モードまたはオン モードに設定できるようになりました。Etherchannel の他のタイプはアクティブ モードのみをサポートします。 新規/変更された画面： **[Interfaces] > [All Interfaces] > [Edit Port Channel] > [Mode]**
Threat Defense インラインセットでの EtherChannel のサポート	2.1.1	Threat Defense インラインセットで EtherChannel を使用できるようになりました。
Threat Defense のインライン セット リンク ステート伝達サポート	2.0(1)	Threat Defense アプリケーションでインライン セットを設定し、リンク ステート伝達を有効にすると、Threat Defense はインライン セット メンバーシップを FXOS シャーシに送信します。リンク ステート伝達により、インライン セットのインターフェイスの 1 つが停止した場合、シャーシは、インライン インターフェイス ペアの 2 番目のインターフェイスも自動的に停止します。 新規/変更されたコマンド：**show fault |grep link-down**、**show interface detail**
ハードウェア バイパス ネットワーク モジュールのサポート Threat Defense	2.0(1)	ハードウェア バイパスは、停電時にトラフィックがインライン インターフェイス ペア間で流れ続けることを確認します。この機能は、ソフトウェアまたはハードウェア障害の発生時にネットワーク接続を維持するために使用できます。 新規/変更された Management Center 画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [物理インターフェイスの編集（Edit Physical Interface）]**
Threat Defense の Firepower-eventing タイプインターフェイス	1.1.4	Threat Defense で使用するために、Firepower イベントとしてインターフェイスを指定できます。このインターフェイスは、Threat Defense デバイスのセカンダリ管理インターフェイスです。このインターフェイスを使用するには、Threat Defense CLI で IP アドレスなどのパラメータを設定する必要があります。たとえば、イベント（Web イベントなど）から管理トラフィックを分類できます。Management Center 構成ガイドのシステム設定の章にある「管理インターフェイス」のセクションを参照してください。 新規/変更された Chassis Manager 画面： **[Interfaces] > [All Interfaces] > [Type]**

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。