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 Firepower Threat Defense（FTD）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

このガイドでは、ASA および/または FTD 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。

- ASDM を使用したスタンドアロン ASA
- Firepower Device Manager（FDM）を使用するスタンドアロン FTD
- Firepower Management Center（FMC）を使用する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FTD

このガイドでは以下の展開については説明しませんので、これらについては FXOS、ASA、FDM、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
- Radware DefensePro デコレータ アプリケーション
- CLI 設定

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

Cisco 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

Firepower 4100 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 Firepower Chassis Manager では、シンプルな GUI ベースの管理機能を利用できます。Firepower Chassis Manager 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 configuration guide』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。

Firepower Threat Defense

FTD 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、高度なマルウェア防御（AMP）などの次世代ファイアウォール サービスを提供します。

FTDは、次のいずれかのマネージャを使用して管理できます。

- FMC：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。
- Firepower Device Manager（FDM）：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。

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
- Cisco Security Manager：別のサーバ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 FTD の目の前で実行することができます。vDP は、Firepower 4100 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 FTD 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 コンフィギュレーション 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。

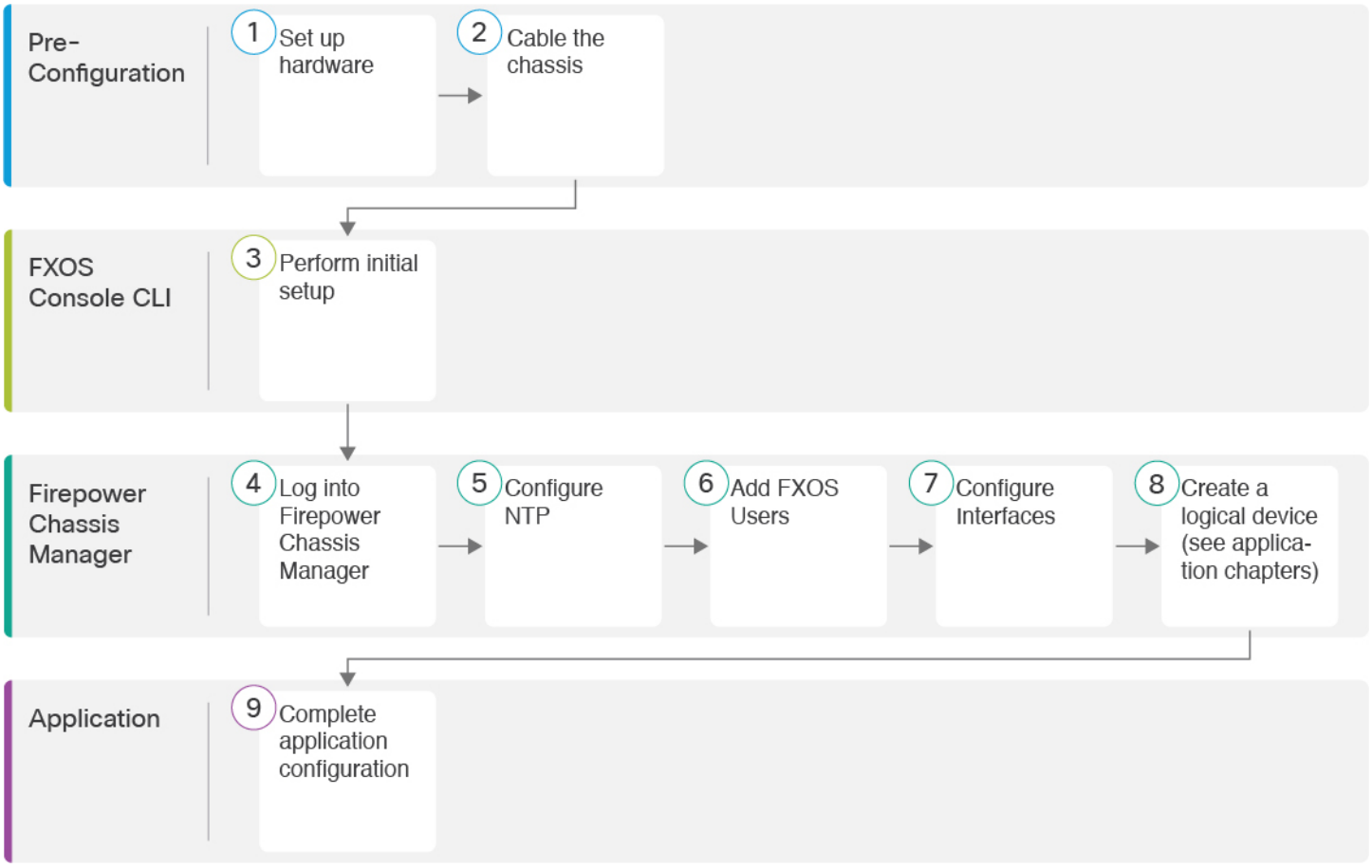
- ネイティブ インスタンス：ネイティブ インスタンスはセキュリティ エンジン のすべてのリソース（CPU、RAM、およびディスク容量）を使用するため、ネイティブ インスタンスを 1 つのみインストールできます。
- コンテナ インスタンス：コンテナ インスタンスでは、セキュリティ エンジン のリソースのサブセットを使用するため、複数のコンテナ インスタンスをインストールできます。
  注：マルチインスタンス機能は、FTD でのみサポートされています。ASA または vDP との組み合わせではサポートされていません。

モデルごとの最大コンテナ インスタンス数

- Firepower 4110：3
- Firepower 4120：3
- Firepower 4140：7
- 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 （5 ページ）。

3	FXOS コンソール CLI	シャーシの初期セットアップの実行 （8 ページ）。
4	Firepower Chassis Manager	Firepower Chassis Manager のログイン （11 ページ）。
5	Firepower Chassis Manager	NTP の設定 （12 ページ）。
6	Firepower Chassis Manager	FXOS ユーザの追加 （14 ページ）。
7	Firepower Chassis Manager	インターフェイスの設定 （16 ページ）。
8	Firepower Chassis Manager	論理デバイスを作成します。 • FTD と FDM：FDM を使用した Firepower Threat Defense の展開を参照してください。 • FTD と FMC：FMC を使用した Firepower Threat Defense の展開を参照してください。 • ASA：ASA 展開 を参照してください。 （注） FTD と FDM のサポートが FXOS 2.7.1/FTD6.5 に追加されました。
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。 • FTD と FDM：FDM を使用した Firepower Threat Defense の展開を参照してください。 • FTD と FMC：FMC を使用した Firepower Threat Defense の展開を参照してください。 • ASA：ASA 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。

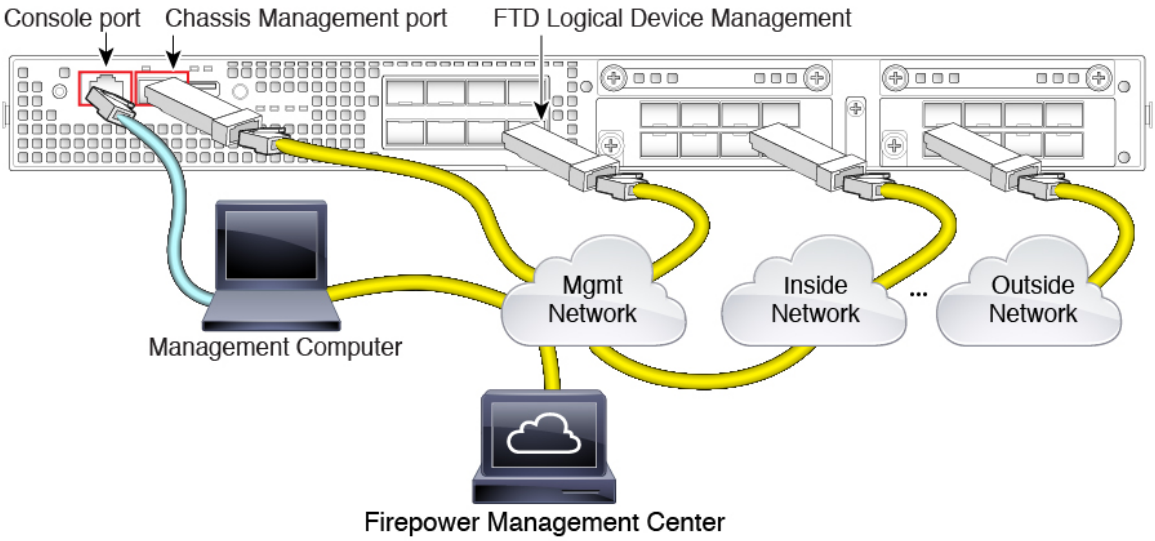
- コンソール ポート：管理コンピュータをコンソール ポートに接続して、シャーシの初期設定を実行します。Firepower 4100 には、RS-232 - RJ-45 シリアル コンソール ケーブルが付属しています。接続には、サードパーティ製のシリアル - USB ケーブルが必要になる場合があります。

- 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。
- 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。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。
- 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 configuration guide』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。

FMC ケーブルを使用した FTD



論理デバイス管理ネットワークに FMC を配置（またはアクセス可能に）します。FTD および FMC は、アップデート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ることに注意してください。

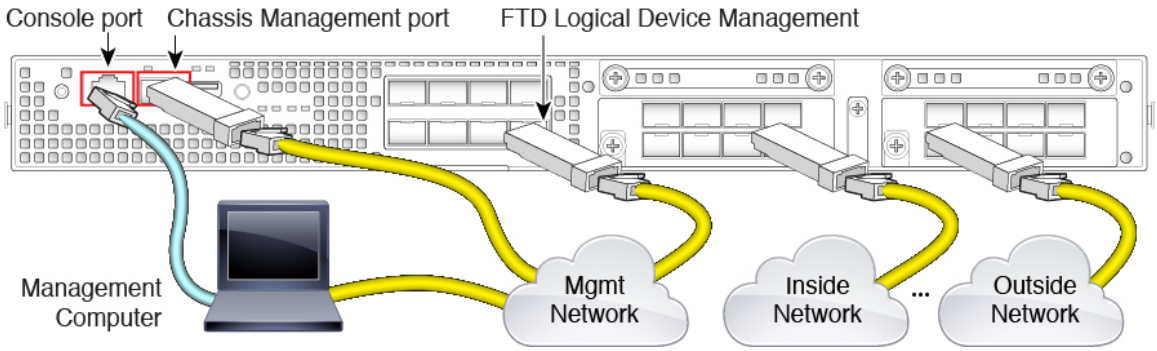
接続を計画する際は、FTD 管理インターフェイスが次の論理インターフェイス間で共有されることに注意してください。

- 管理論理インターフェイス：この管理プレーン インターフェイスは FMC と通信し、アップデートをダウンロードして、FTD CLI への SSH アクセスを提供します。
- 診断論理インターフェイス：このデータ プレーン インターフェイスは、FMC の他のデータ インターフェイスとともに表示されます。このインターフェイスは、トラフィックの通過を許可しない管理専用インターフェイスとして、syslog または SNMP では便利ですが、使用は必須ではありません。

上記の配線例では、FTD がインターネットゲートウェイとして機能するように、管理ネットワークを FTD の内部ネットワーク（またはインターネットアクセスがあるインターフェイス）に接続しています。FTD 管理インターフェイスとその他の管理デバイスを内部インターフェイスに直接（スイッチを使用して）接続するか、管理ネットワークと FTD の内部ネットワークの間にルータを配置することができます。

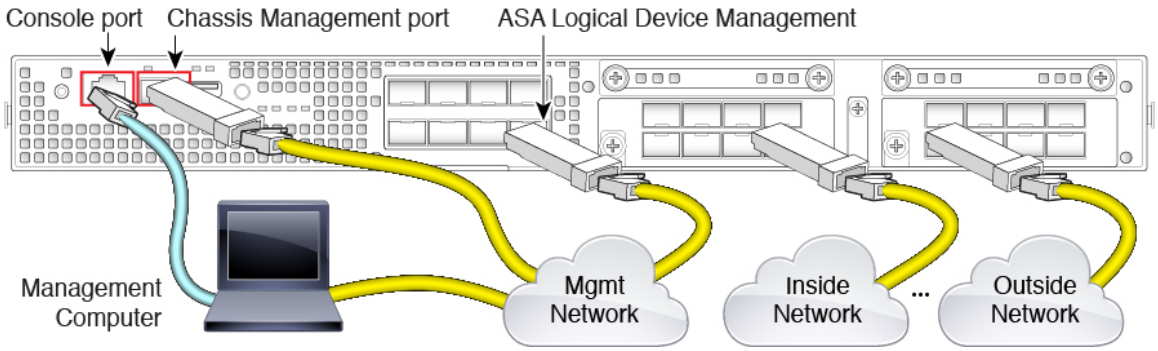
直接接続のシナリオでは、FMC の診断論理インターフェイスの IP アドレスを設定しないことが重要です。FTD 管理論理インターフェイスは通常のインターフェイスではなく、FTD ルーティングに参加しないため、図のように FTD データ ネットワークに直接接続することができます。ただし、IP アドレスを診断インターフェイスに割り当てる場合、それを他のデータ インターフェイスと同じネットワーク上にすることはできません。同じネットワークである場合は、管理/診断と別の FTD インターフェイスの間でルーティングする必要があります。

FDM ケーブルを使用した FTD



論理デバイスの管理インターフェイスで FTD 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。FTD では、ライセンスと更新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、FTD 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をルーティングします。そうではなく、バックプレーンを介してデータインターフェイスに管理トラフィックをルーティングする必要がある場合は、後で FDM でその設定が行えます。

ASA のケーブル接続



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

コンソールで FXOS CLI に初めてアクセスすると、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 Firepower 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。

（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-9300

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-9300
  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 コンソール ポートからケーブルを取り外します。

Firepower Chassis Manager のログイン

Firepower 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、Firepower 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 ユーザ名 **admin** と新しいパスワードを入力します。

FXOS ユーザの追加 （14 ページ） に従って、後でさらにユーザを追加できます。

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 Firepower 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 サーバを使用することを推奨します。ASA および FTD と FDM 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。FTD と FMC の場合は、シャーシと FMC の間で時刻が一致している必要があります。この場合は、FMC の場合と同じ NTP サーバをシャーシで使用することを推奨します。FMC 自身を NTP サーバ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

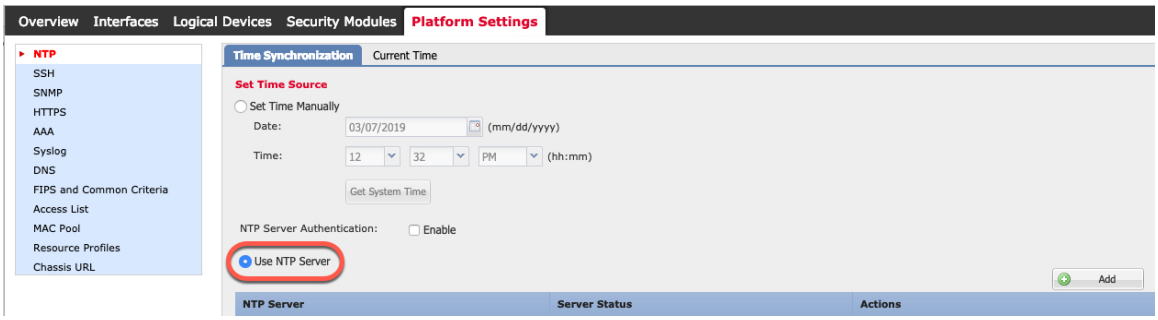
NTP サーバのホスト名を使用する場合は、DNS サーバを設定する必要があります（最初のセットアップで未実施の場合）。**[プラットフォーム設定（Platform Settings）] > [DNS]** を参照してください。

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 [Use NTP Server] オプション ボタンをクリックします。

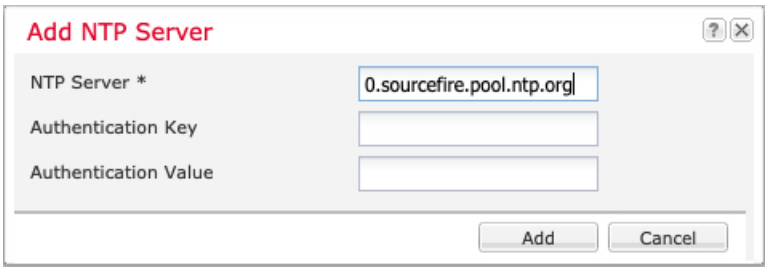


ステップ 3 （任意） NTP サーバで認証が必要な場合は、[NTPサーバ認証：有効（NTP Server Authentication: Enable）] チェックボックスをオンにします。

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 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。



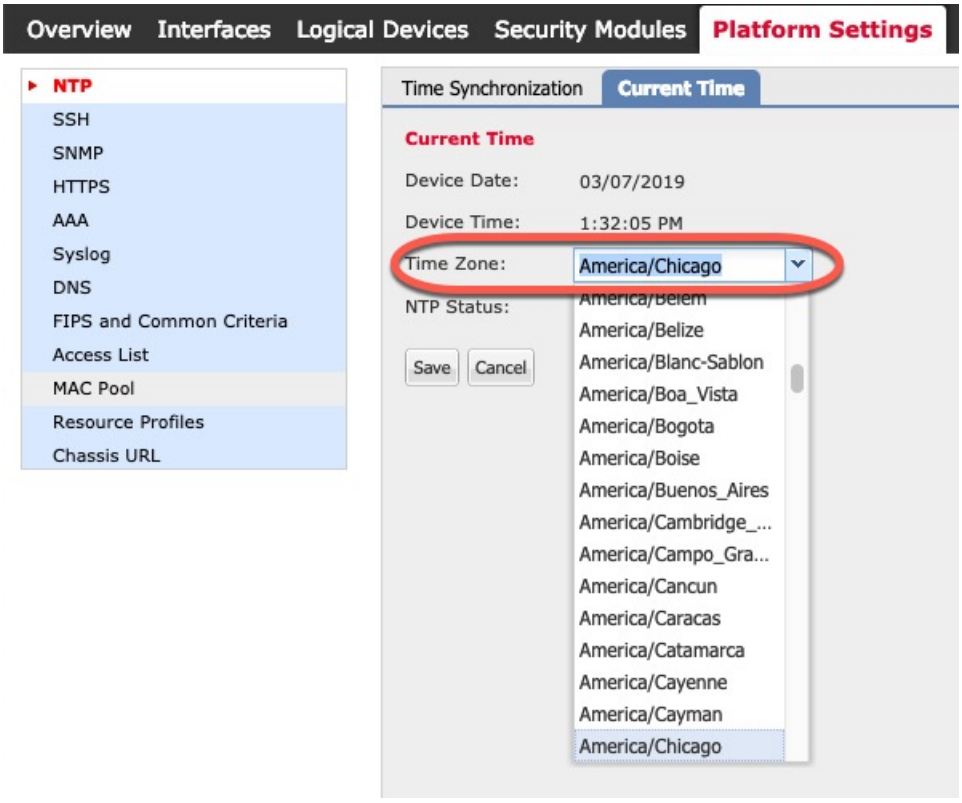
- [NTPサーバ（NTP Server）]：NTP サーバの IP アドレスまたはホスト名
- [認証キー（Authentication key）] および [認証値（authentication VALUE）]：NTP サーバからキー ID と値を取得します。たとえば、OpenSSL がインストールされた NTP サーバ バージョン 4.2.8 p8 以降で SHA1 キーを生成するには、**ntp-keygen -M** コマンドを入力して ntp.keys ファイルでキー ID と値を確認します。このキーは、クライアントとサーバの両方に対して、メッセージ ダイジェストの計算時に使用する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

NTP サーバは最大 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 [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、Firepower Chassis Manager への再ログインが必要になります。

FXOS ユーザの追加

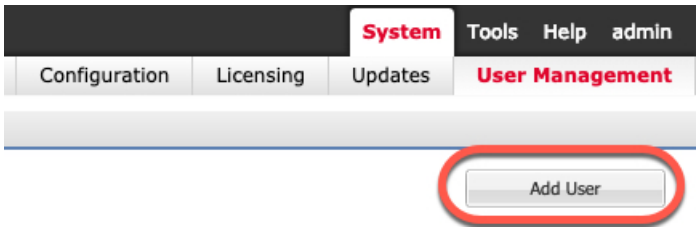
Firepower Chassis Manager および FXOS CLI ログインのローカル ユーザを追加します。

手順

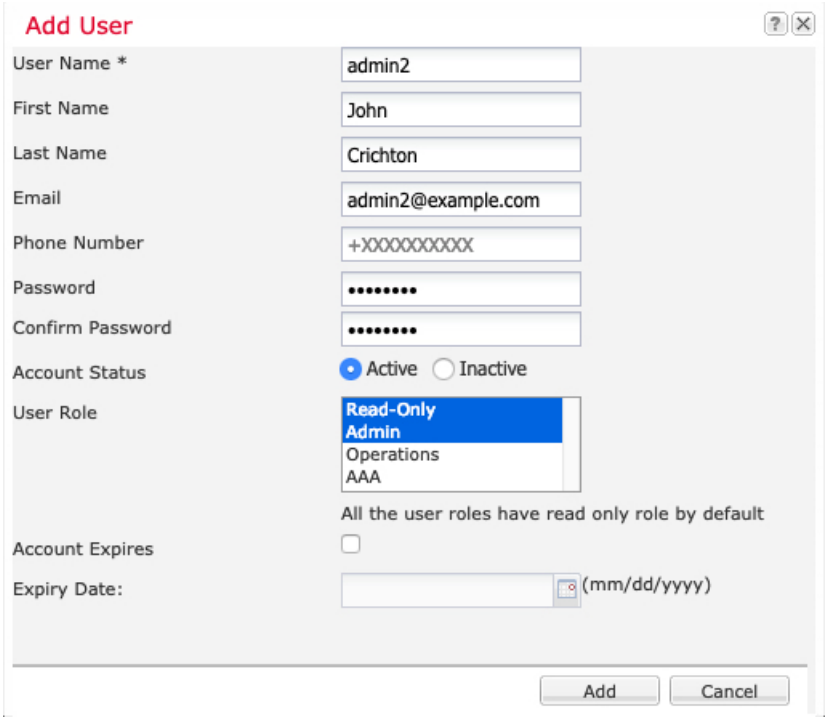
ステップ 1 **[システム（System）] > [ユーザ管理（User Management）]** を選択します。

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

ステップ 3 [Add User] をクリックして [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。



- [ユーザ名（User Name）]：最大32文字のユーザ名を設定します。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）]：ユーザの名前を最大 32 文字で設定します。
- （任意）[姓（Last name）]：ユーザの姓を最大 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 configuration guide』を参照してください。
- [Account status]：ステータスを**アクティブ**または**非アクティブ**に設定します。
- [User Role]：ユーザ 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。すべてのユーザはデフォルトでは [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 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、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 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 [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 configuration guide』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、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。
- 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（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）、これらのデータインターフェイスは 1 つまたは複数のコンテナインスタンス（FTD を使用する FMC 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の使用に関する詳細については、『FXOS configuration guide』を参照してください。共有インターフェイスは、ブリッジ グループ メンバ 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、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。

- Management（Mgmt）：アプリケーション インスタンスの管理に使用します。管理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。このインターフェイスは、シャーシ管理ポートとは別のものです。
- Firepower-eventing：使用時のFMC FTD デバイスの 2 次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、FTD 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。詳細については、『FMC configuration guide』を参照してください。
- 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。詳細については、『FXOS configuration guide』を参照してください。 FDM 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

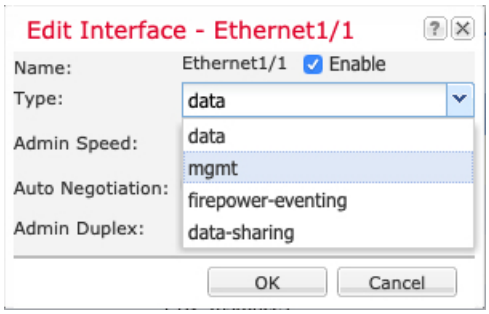
ステップ 1 [インターフェイス（Interfaces）] をクリックします。

[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 [Edit] アイコン（✎） 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 configuration guide』を参照してください。

Firepowerについては、『FMC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（別名ポート チャネル）には、同じタイプのメンバー インターフェイスを最大 16 個含めることができます。

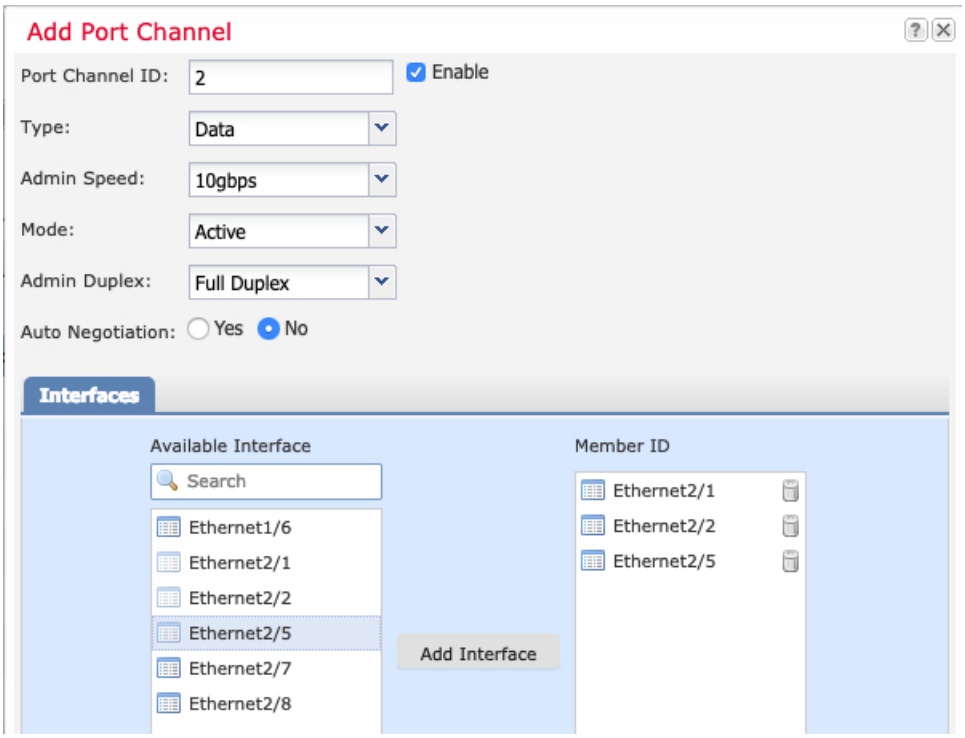
（注） シャーシが EtherChannel を作成すると、EtherChannel は [一時停止（Suspended）] 状態（Active LACP モードの場合）または [ダウン（Down）] 状態（On LACP モードの場合）になり、物理リンクがアップしても論理デバイスに割り当てるまでそのままになります。

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）] を次から選択します。**Data**、**Data-sharing**、**Mgmt**、または **Firepower-eventing**。

[クラスタ（Cluster）] タイプは選択しないでください。

（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 configuration guide』を参照してください。

Firepower については、『FMC configuration guide』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。

同じタイプで同じ速度のインターフェイスを最大 16 個追加できます。

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 [Delete] アイコン（） をクリックします。

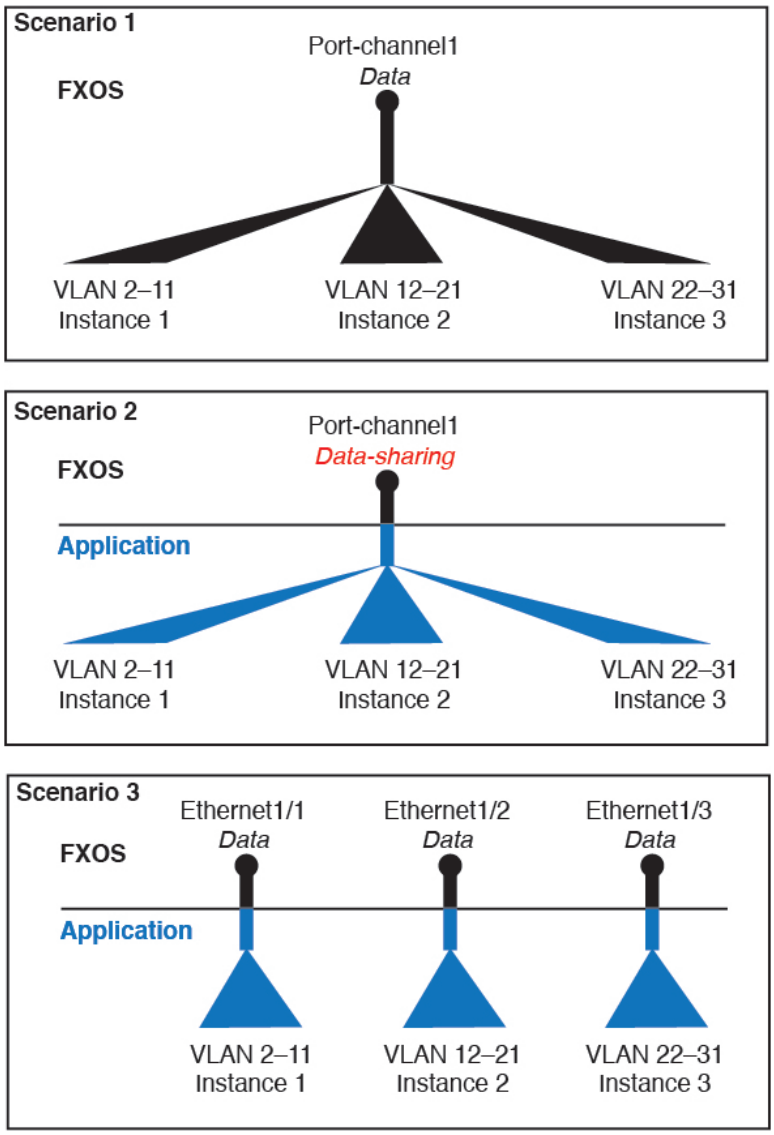
ステップ 11　[OK] をクリックします。

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。

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。

ネイティブ インスタンスの場合、アプリケーション内にのみ VLAN サブインターフェイスを作成できます。コンテナインスタンスの場合、FXOS VLAN サブインターフェイスが定義されていないインターフェイスのアプリケーション内でも VLAN サブインターフェイスを作成できます。これらのサブインターフェイスにはFXOS制限が適用されません。サブインターフェイスを作成するオペレーティング システムの選択は、ネットワーク導入および個人設定によって異なります。たとえば、サブインターフェイスを共有するには、FXOS でサブインターフェイスを作成する必要があります。FXOS サブインターフェイスを優先するもう 1 つのシナリオでは、1 つのインターフェイス上の別のサブインターフェイス グループを複数のインスタンスに割り当てます。たとえば、インスタンス A で VLAN 2-11 を、インスタンス B で VLAN 12-21 を、インスタンス C で VLAN 22-31 を使用して Port-Channel1 を使うとします。アプリケーション内でこれらのサブインターフェイスを作成する場合、FXOS 内で親インターフェイスを共有しますが、これはお勧めしません。同様のシナリオを実現する 3 つの方法については、次の図を参照してください。



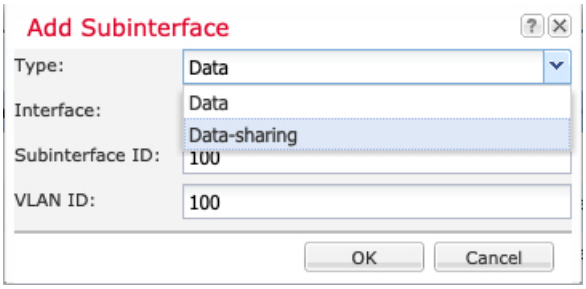
手順

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 **[新規追加（Add New）] > [サブインターフェイス（Subinterface）]** をクリックして [サブインターフェイスの追加（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）] : [データ（Data）] または [データ共有（Data-sharing）] を選択します。



サブインターフェイスは、データまたはデータ共有タイプのインターフェイスでのみサポートされます。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、データ共有タイプの親インターフェイスとデータ タイプのサブインターフェイスを持つことができます。

（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 configuration guide』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 Compatibility Guide』で、FXOS、ASA、および FTD 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。

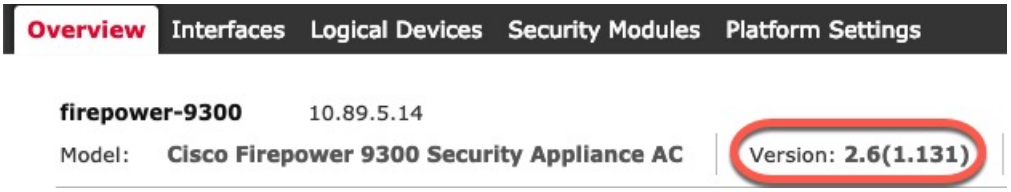
  http://www.cisco.com/go/firepower4100-software

- 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） FTD 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 Firepower 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） FTD 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]**
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]**
FTD インライン セットでの EtherChannel のサポート	2.1(1)	FTD インライン セットで Etherchannel を使用できるようになりました。

機能名	バージョン	機能情報
FTD 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)	FTD 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、FTD 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 FTD	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 Firepower Management Center 画面： **[Devices]** > **[Device Management]** > **[Interfaces]** > **[Edit Physical Interface]**
FTD の Firepower イベント タイプ インターフェイス	1.1.4	FTD 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、FTD 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、FTD 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。Firepower 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 [Firepower Chassis Manager] 画面： **[Interfaces]** > **[All Interfaces]** > **[Type]**