Cisco ASA for Firepower 2100 シリーズ スタートアップ ガイド

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

第 1 章

使用する前に

この章では、ネットワーク内の Firepower 2100 に ASA を展開する方法、および初期設定を実行する方法について説明します。

Firepower 2100 用 ASA について

Firepower 2100 ハードウェアは、Cisco ASA ソフトウェアまたは Firepower Threat Defense ソフトウェアを使用して実行できます。このガイドでは、Firepower 2100 での ASA の使用方法について説明します。

（注） ASA と Firepower Threat Defense の間の切り替えには、デバイスの再イメージ化が必要です。「Reimage the Cisco ASA or Firepower Threat Defense Device」を参照してください。

ASA の Firepower 2100 との連携方法

Firepower 2100 は ASA 用の単一アプリケーション アプライアンスです。Firepower 2100 は、Firepower eXtensible Operating System（FXOS）という基礎となるオペレーティング システムを実行します。FXOS では、基本的な動作パラメータとハードウェア インターフェイス設定を設定する必要があります。これらの設定には、インターフェイスの有効化、EtherChannels の確立、NTP、イメージ管理などが含まれます。Firepower Chassis Manager Web インターフェイスまたは FXOS CLI を使用できます。その後、ASDM または ASA CLI を使用して ASA オペレーティング システムにセキュリティ ポリシーを設定できます。

ASA と FXOS の管理

ASA および FXOS のオペレーティング システムは、管理 1/1 インターフェイスを共有します。このインターフェイスには、ASA および FXOS に接続するための個別の IP アドレスがあります。

（注） このインターフェイスは ASA では管理 1/1 と呼ばれます。FXOS では、MGMT、management0、または同様の他の名前で表示されます。このガイドでは、一貫性と簡潔さのため、管理 1/1 としてこのインターフェイスを参照します。

FXOS および ASA で監視する必要がある機能は異なるため、継続的な保守で両方のオペレーティング システムを使用する必要があります。FXOS の初期設定では、SSH またはブラウザ（https://192.168.45.45）を使用してデフォルトの 192.168.45.45 IP アドレスに接続できます。

ASA の初期設定では、ASDM を使用して https://192.168.45.1/admin に接続できます。ASDM では、後で任意のインターフェイスからの SSH アクセスを設定できます。

両方のオペレーティング システムをコンソール ポートから使用できます。初期接続では FXOS CLI にアクセスします。ASA CLI には **connect asa** コマンドを使用してアクセスできます。

ASA データ インターフェイスから FXOS を管理できるようにすること、および SSH、HTTPS、および SNMP の各アクセスを設定することも可能です。この機能はリモート管理に役立ちます。

ライセンス要件

Firepower 2100 上の ASA はシスコ スマート ソフトウェア ライセンシングを使用します。通常のスマート ソフトウェア ライセンシング（インターネット アクセスが必要）を使用できます。または、オフライン管理の場合、永続ライセンス予約またはサテライト サーバを設定できます。これらのオフライン ライセンス方式の詳細については、「Cisco ASA Series Feature Licenses」を参照してください。このガイドは通常のスマート ソフトウェア ライセンシングに適用されます。

License Authority に登録するまでは、特殊なライセンスを必要とする機能の設定変更を行うことはできませんが、操作はその他の点では影響を受けません。ライセンス付与される機能は次のとおりです。

- セキュリティ コンテキスト（3 以上）
- 強力な暗号化（3DES/AES）（通過トラフィック用）

標準ライセンスも必要ですが、デバイスの基本機能は評価モードで実行できます。

ASA には、管理アクセスのみを対象にしてデフォルトで 3DES 機能が含まれています。したがって、License Authority に接続し、すぐに ASDM を使用することもできます。ASDM アクセスの場合、インターフェイスが管理専用に設定されているか、または強力な暗号化（3DES/AES）の完全ライセンスが有効になっている必要があることに注意してください。デフォルトの設定には、管理専用に設定されている管理 1/1 インターフェイスが含まれています。スマート ソフトウェア ライセンシング アカウントから ASA の登録トークンを要求する場合、[Allow export-controlled functionality on the products registered with this token] チェックボックスをオンにして、強力な暗号化の完全ライセンスが適用されるようにします（ご使用のアカウントでその使用が許可されている必要があります）。ライセンスの詳細については、ASDM の起動とライセンスの設定, （8 ページ）を参照してください。

（注） Firepower 4100/9300 シャーシの場合とは異なり、すべてのライセンス設定を FXOS 設定ではなく ASA で実行します。

サポートされない機能

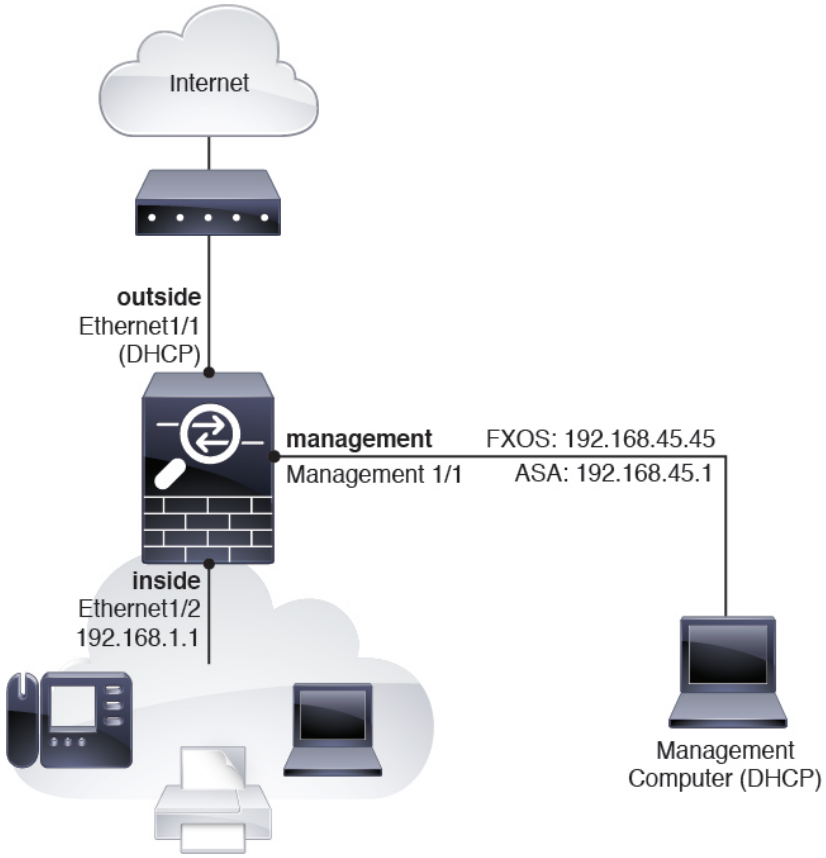
次の機能は、Firepower 2100 ではサポートされていません。

- Integrated Routing and Bridging（IRB）
- クラスタ
- KCD を使用したクライアントレス SSL VPN
- ASA REST API
- ASA FirePOWER モジュール
- Botnet Traffic Filter
- 次のインスペクション：
  - SCTP インスペクション マップ（ACL を使用した SCTP ステートフル インスペクションはサポートされます）
  - Diameter
  - GTP/GPRS

ネットワーク内の Firepower 2100

次の図は、Firepower 2100 上の ASA のデフォルトのネットワーク配置を示しています。

図 *1*：ネットワーク内の *Firepower 2100* 上の *ASA*



このガイドで説明されている初期セットアップを完了すると、デフォルトの設定では上記ネットワーク配置で次の動作が有効になります。

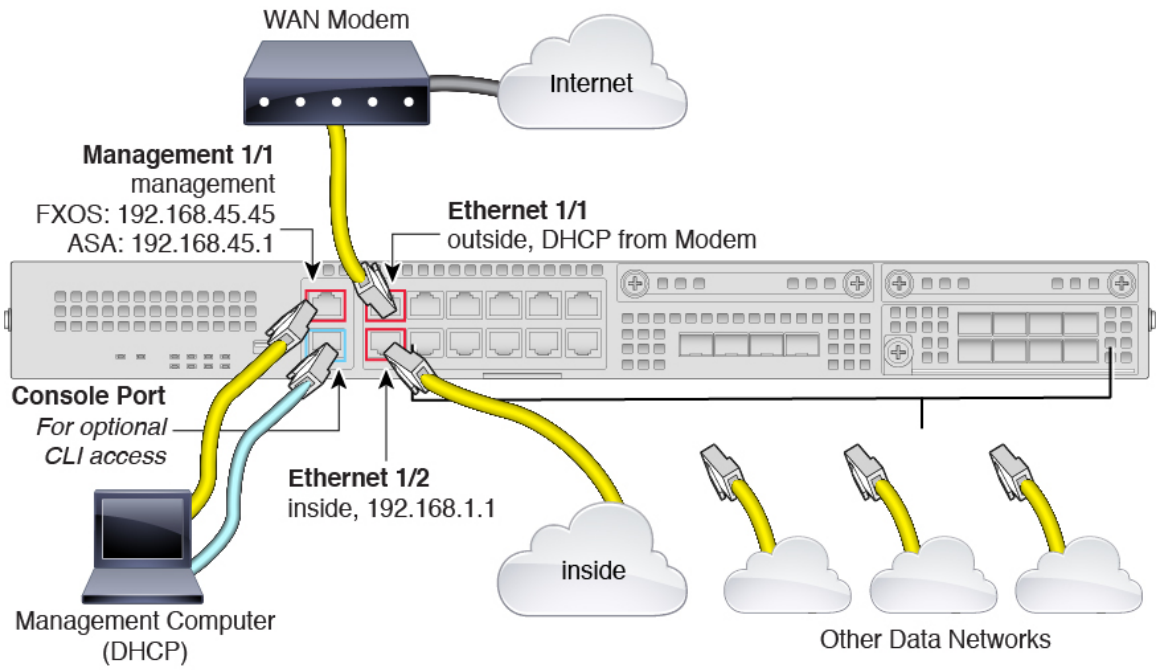
- NAT を含む、**内部 --> 外部**のトラフィック フロー
- **DHCP** からの**外部 IP** アドレス
- FXOS および ASA の管理用の**管理 1/1**。DHCP IP アドレスは、このネットワーク上の管理コンピュータに対して FXOS によって提供されます。

インターフェイスの接続

管理 1/1 インターフェイスで Firepower 2100 を管理します。FXOS と ASA に同じ管理コンピュータを使用できます。FXOS IP アドレスで Firepower Chassis Manager に接続し、シャーシ設定を実行します。次に、ASDM を使用して ASA IP アドレスに接続し、ASA 設定を完了します。

デフォルトの設定でも、Ethernet1/1 を外部、Ethernet1/2 を内部として設定されています。

図 *2*：*Firepower 2100* インターフェイスにケーブルを接続する



手順

ステップ 1 管理 1/1 へのイーサネットを使用して管理コンピュータに接続します（ラベルは MGMT）。

ステップ 2 （任意） 管理コンピュータをコンソール ポートに接続します。Firepower 2100 には DB-9 to RJ-45 シリアル ケーブルが付属しているため、接続するためにはサード パーティ製のシリアル to USB ケーブルが必要です。ご使用のオペレーティング システムに必要な USB シリアル ドライバを必ずインストールしてください。

ステップ 3 外部ネットワークを Ethernet1/1 ポートに接続します（ラベルは WAN）。スマート ソフトウェア ライセンシングの場合、ASA は License Authority にアクセスできるようにするためにインターネット アクセスを必要とします。

ステップ 4 内部ネットワークを Ethernet1/2、および必要に応じてその他のデータ インターフェイスに接続します。

Firepower 2100 の電源投入

システムの電源は、シャーシ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。電源スイッチは、ソフト通知スイッチとして実装されています。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 Firepower 2100 に接続し、電源コンセントに接続します。

ステップ 2 シャーシ背面の電源スイッチを押して 1 の位置にします。
シャーシの電源をオフにするには、シャーシ背面の電源スイッチを押して 0 の位置にします。スイッチを ON から OFF に切り替えると、システムの電源が最終的に切れるまで数秒かかることがあります。この間は、シャーシの前面パネルの PWR LED が緑に点滅します。PWR LED が完全にオフになるまで電源を抜かないでください。

ステップ 3 シャーシの前面にある PWR LED を確認します。緑色に点灯している場合は、シャーシの電源が入っています。

ステップ 4 シャーシの前面にある SYS LED を確認します。緑色に点灯している場合は、電源投入時診断に合格しています。

（任意）FirepowerChassisManagerで追加のインターフェイスを有効にする

デフォルトでは、管理 1/1、イーサネット 1/1、およびイーサネット 1/2 の各インターフェイスは、シャーシでは物理的に有効、ASA 設定では論理的に有効になっています。追加のインターフェイスを使用するには、次の手順を使用してそのインターフェイスをシャーシで有効にし、その後 ASA 設定で有効にする必要があります。EtherChannel（ポートチャネルとも呼ばれる）を追加することもできます。

はじめる前に

- Firepower 2100 は、アクティブ Link Aggregation Control Protocol（LACP）モードでのみ EtherChannel をサポートします。最適な互換性を得るために、接続スイッチ ポートをアクティブ モードに設定することを推奨します。
- 管理 IP アドレスをデフォルトから変更するには、FXOS 管理 IP アドレスまたはゲートウェイの変更, （16 ページ）を参照してください。

手順

ステップ 1 管理 1/1 インターフェイスに接続している管理コンピュータで、次の URL にアクセスして Firepower Chassis Manager を起動します：**https://192.168.45.45**。

ステップ 2 デフォルトのユーザ名：**admin**、およびパスワード：**Admin123** を入力します。
[System] > [User Management] > [Local Users] ページですぐにパスワードを変更することをお勧めします。

管理 IP アドレスを変更するには、FXOS 管理 IP アドレスまたはゲートウェイの変更，（16 ページ）を参照してください。

ステップ 3 Firepower Chassis Manager で、[Interfaces] タブをクリックします。

ステップ 4 インターフェイスを有効または無効にするには、[Admin State] スライダをクリックします。チェックマークは有効であることを示し、X は無効であることを示します。

（注） 管理 1/1 インターフェイスは、このテーブルで [MGMT] として表示されます。

ステップ 5 （任意） EtherChannel を追加します。

（注） EtherChannel メンバー ポートは ASA に表示されますが、EtherChannel およびポート メンバーシップは FXOS でのみ設定できます。

a) インターフェイス テーブルの上の [Add Port Channel] をクリックします。

b) [Port Channel ID] フィールドに、ポート チャネルの ID を入力します。有効な値は、1 ～ 47 です。

c) ポート チャネルを有効にするには、[Enable] チェックボックスをオンにします。
[Type] ドロップダウン リストは無視します。使用可能なタイプは [Data] のみです。

d) [Admin Speed] ドロップダウン リストで、すべてのメンバー インターフェイスの速度を選択します。
その速度（および選択したその他の設定）に対応していないインターフェイスを選択すると、可能な範囲で最速の速度が自動的に適用されます。

e) すべてのメンバー インターフェイスについて、[Auto Negotiation] で [Yes] または [No] のオプション ボタンをクリックします。

f) [Admin Duplex] ドロップダウン リストで、すべてのメンバー インターフェイスのデュプレックスを選択します。

g) [Available Interface] リストで、追加するインターフェイスを選択し、[Add Interface] をクリックします。
同じタイプと速度の最大 16 のインターフェイスを追加できます。チャネル グループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。

ヒント 複数のインターフェイスを一度に追加できます。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。

h) [OK] をクリックします。

ASDM の起動とライセンスの設定

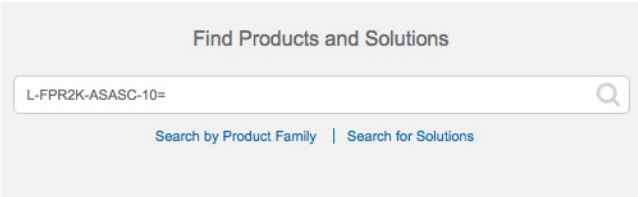
ASDM を起動し、ご使用のデバイスをスマート ソフトウェア ライセンス サーバに登録します。

はじめる前に

- ASDM を実行するための要件については、Cisco.com の『ASDM リリース ノート』を参照してください。
- この手順では、イーサネット 1/1 外部インターフェイスをインターネットに接続し、デフォルト設定を使用していることを想定しています。ネットワーク内の Firepower 2100, （4 ページ）を参照してください。
- Cisco Smart Software Manager にマスター アカウントを持ちます。

  まだアカウントをお持ちでない場合は、リンクをクリックして新しいアカウントを設定してください。Smart Software Manager では、組織のマスター アカウントを作成できます。
- （輸出コンプライアンス フラグを使用して有効化される）機能を使用するには、ご使用のシスコ スマート ソフトウェア ライセンシング アカウントで強力な暗号化（3DES/AES）ライセンスを使用できる必要があります。
- ご使用のアカウントに、必要なライセンスが含まれている（少なくとも標準ライセンスが含まれている）ことを確認してください。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。ただし、主導でライセンスを追加する必要がある場合は、Cisco Commerce Workspace で [Find Products and Solutions] 検索フィールドを使用します。次のライセンス PID を検索します。

図 *3*：ライセンス検索



  - 標準ライセンス：L-FPR2100-ASA=。標準ライセンスは無料ですが、スマート ソフトウェア ライセンシング アカウントに追加する必要があります。
  - 5 コンテキスト ライセンス：L-FPR2K-ASASC-5=。コンテキスト ライセンスは追加的であり、ニーズに合わせて複数のライセンスを購入します。
  - 10 コンテキスト ライセンス：L-FPR2K-ASASC-10=。コンテキスト ライセンスは追加的であり、ニーズに合わせて複数のライセンスを購入します。

- 強力な暗号化（3DES/AES）ライセンス：L-FPR2K-ENC-K9=。このライセンスは無料です。このライセンスが必要になるのは、古いサテライト サーバ バージョン（2.3.0 より前）を使用する ASA に限られますが、追跡目的でこのライセンスをアカウントに追加することをお勧めします。

（注） フェールオーバー ペアの場合、標準ライセンス（および同じ暗号化）を両方のユニットに適用する必要があります。コンテキスト ライセンスの場合、プライマリ ユニットへの適用のみが必要です。

手順

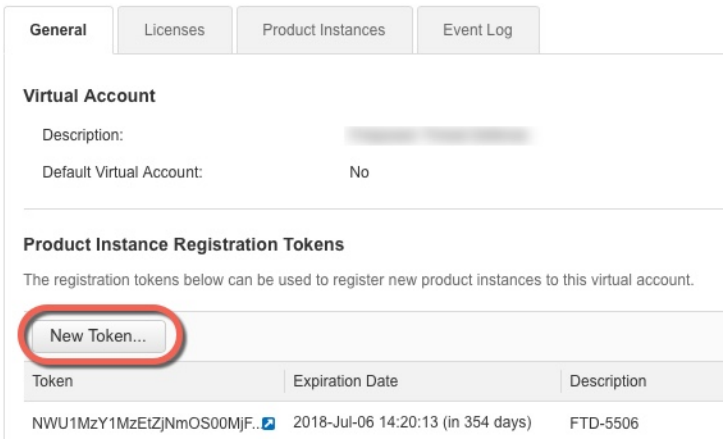
ステップ 1 Smart Software Manager（Cisco Smart Software Manager）で、このデバイスを追加するバーチャル アカウントの登録トークンを要求してコピーします。

a) [Inventory] をクリックします。

図 *4*：インベントリ

b) [General] タブで、[New Token] をクリックします。

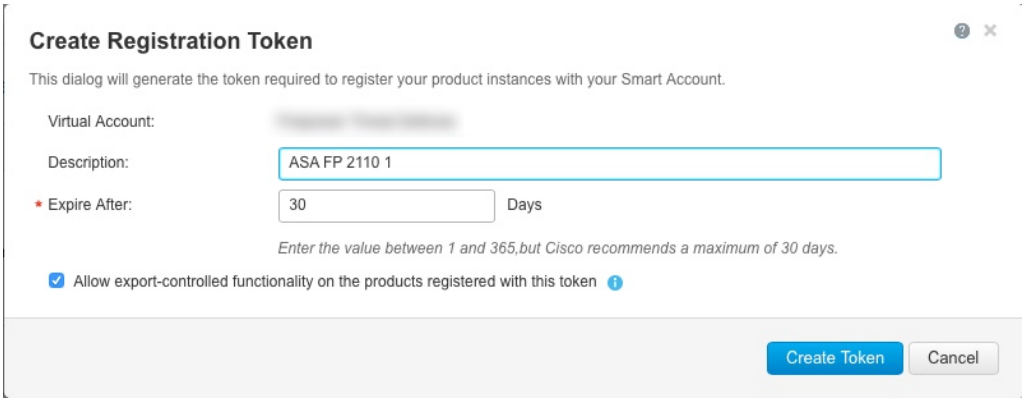
図 *5*：新しいトークン



c) [Create Registration Token] ダイアログボックスで、以下の設定値を入力してから [Create Token] をクリックします。

- 説明
- Expire After：推奨値は 30 日です。
- Allow export-controlled functionaility on the products registered with this token：輸出コンプライアンス フラグを有効にします。

図 *6*：登録トークンの作成



トークンはインベントリに追加されます。

d) トークンの右側にある矢印アイコンをクリックして [Token] ダイアログボックスを開き、トークン ID をクリップボードにコピーできるようにします。ASA の登録が必要なときに後の手順で使用するために、このトークンを準備しておきます。

図 *7*：トークンの表示

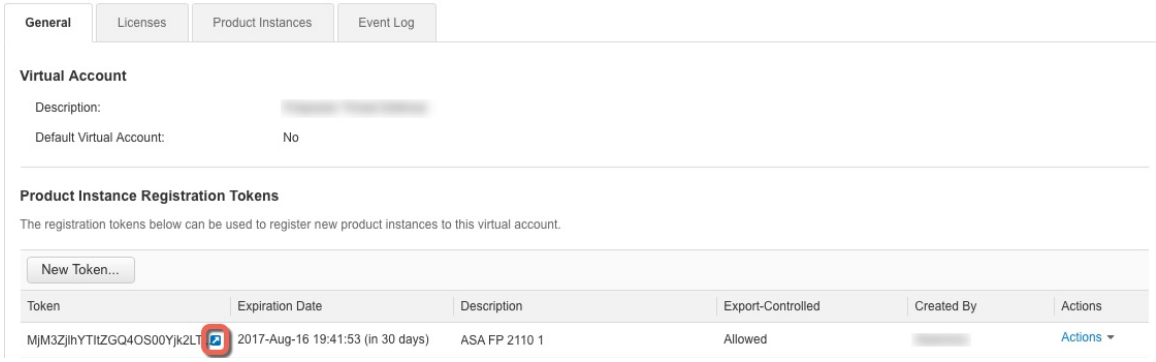
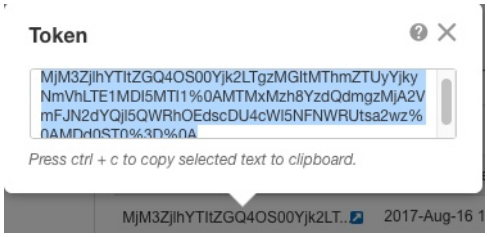


図 *8*：トークンのコピー



ステップ 2 管理 1/1 に接続している管理コンピュータで Web ブラウザを起動し、次の URL にアクセスします：**https://192.168.45.1/admin**。[Cisco ASDM] Web ページが表示されます。

ステップ 3 使用可能なオプション [Install ASDM Launcher] または [Run ASDM] のいずれかをクリックします。

ステップ 4 画面の指示に従ってオプションを選択し、ASDM を起動します。[Cisco ASDM-IDM Launcher] が表示されます。

ステップ 5 ユーザ名とパスワードのフィールドを空のまま残し、[OK] をクリックします。メイン ASDM ウィンドウが表示されます。

ステップ 6 [Configuration] > [Device Management] > [Licensing] > [Smart Licensing] の順に選択します。

ステップ 7 [Enable Smart license configuration] をオンにします。

ステップ 8 [Feature Tier] ドロップダウン メニューから [Standard] を選択します。
使用できるのは標準層だけです。

ステップ 9 （任意） [Context] ライセンスの場合、コンテキストの数を入力します。
コンテキストの最大数は、モデルによって異なります。2 コンテキストはライセンスなしで使用できます。

- Firepower 2110：25 コンテキスト

- Firepower 2120：25 コンテキスト
- Firepower 2130：30 コンテキスト
- Firepower 2140：40 コンテキスト

ステップ 10 [Apply] をクリックします。

ステップ 11 [Register] をクリックします。

ステップ 12 [ID Token] フィールドに登録トークンを入力します。

ステップ 13 [Register] をクリックします。
ASA は、事前設定された外部インターフェイスを使用して License Authority に登録し、設定済みライセンス エンタイトルメントの認証を要求します。License Authority は、ご使用のアカウントが許可すれば強力な暗号化（3DES/AES）ライセンスも適用します。ライセンス ステータスを確認する場合は、[Monitoring] > [Properties] > [Smart License] の順に選択します。

ASA の設定

ASDM を使用する際、基本機能および拡張機能の設定にウィザードを使用できます。ウィザードに含まれていない機能を手動で設定することもできます。

手順

ステップ 1 [Wizards] > [Startup Wizard] の順に選択し、[Modify existing configuration] オプション ボタンをクリックします。

ステップ 2 [Startup Wizard] では、手順を追って以下を設定できます。

- イネーブル パスワード
- インターフェイス（内部および外部のインターフェイス IP アドレスの変更や設定したインターフェイスの有効化など） （任意）Firepower Chassis Manager で追加のインターフェイスを有効にする，（6 ページ）
- スタティック ルート
- DHCP サーバ（管理 1/1 インターフェイスの DHCP サーバは設定しないでください）
- その他...

ステップ 3 （任意） [Wizards] メニューから、その他のウィザードを実行します。

ステップ 4 ASA の設定を続行するには、「Navigating the Cisco ASA Series Documentation」でソフトウェアバージョンに応じたマニュアルを参照してください。

ASA および FXOS の CLI アクセス

このセクションでは、FXOS および ASA のコンソールへの接続方法、ASA データ インターフェイスでの FXOS SSH、HTTPS、および SNMP アクセスの設定方法、および SSH を使用して FXOS に接続する方法を説明します。

ASA または FXOS のコンソールへの接続

Firepower 2100 コンソール ポートで FXOS CLI に接続します。次に、FXOS CLI から ASA コンソールに接続し、再度戻ることができます。

はじめる前に

一度に使用できるコンソール接続は 1 つだけです。FXOS コンソールから ASA のコンソールに接続する場合、Telnet または SSH 接続の場合とは異なり、この接続は永続的接続です。

手順

ステップ 1 管理コンピュータをコンソール ポートに接続します。Firepower 2100 には DB-9 to RJ-45 シリアル ケーブルが付属しているため、接続するためにはサード パーティ製のシリアル to USB ケーブルが必要です。ご使用のオペレーティング システムに必要な USB シリアル ドライバを必ずインストールしてください。次のシリアル設定を使用します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

FXOS CLI に接続します。

ステップ 2 ASA に接続します。
connect asa

例：

```
firepower-2100# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

ステップ 3 FXOS コンソールに戻るには、**Ctrl+a**、**d** と入力します。

データ インターフェイスでの FXOS の管理アクセスの設定

データ インターフェイスから Firepower 2100 の FXOS を管理する場合、SSH、HTTPS、および SNMP アクセスを設定できます。この機能は、デバイスをリモート管理する場合、および管理1/1を隔離されたネットワークに維持する場合に役立ちます。継続してローカル アクセスで管理 1/1 を使用できます。1 つのゲートウェイしか指定できないため、ASA データ インターフェイスへのトラフィック転送用に同時に FXOS の管理 1/1 からのリモート アクセスを許可することはできません。デフォルトでは、FXOS 管理ゲートウェイは ASA への内部パスです。

ASA は、FXOS アクセスに非標準ポートを使用します。標準ポートは同じインタ フェースで ASA が使用するため予約されています。ASA が FXOS にトラフィックを転送するときに、非標準の宛先ポートはプロトコルごとに FXOS ポートに変換されます（FXOS の HTTPS ポートは変更しません）。パケット宛先 IP アドレス（ASA インターフェイス IP アドレス）も、FXOS で使用する内部アドレスに変換されます。送信元アドレスは変更されません。トラフィックを返す場合、ASA は自身のデータ ルーティング テーブルを使用して正しい出力インターフェイスを決定します。管理アプリケーションの ASA データ IP アドレスにアクセスする場合、FXOS ユーザ名を使用してログインする必要があります。ASA ユーザ名は ASA 管理アクセスのみに適用されます。

ASA データ インターフェイスで FXOS 管理トラフィック開始を有効にすることもできます。これは、たとえば、SNMP トラップ、NTP と DNS のサーバ アクセスなどに必要です。デフォルトでは、FXOS 管理トラフィック開始は、DNS および NTP のサーバ通信（スマート ソフトウェア ライセンシング通信で必要）用の ASA 外部インターフェイスで有効になっています。

はじめる前に

- シングル コンテキスト モードのみ。
- ASA 管理専用インターフェイスは除外します。
- ASA データ インターフェイスに VPN トンネルを使用して、FXOS に直接アクセスすることはできません。SSH の回避策として、ASA に VPN 接続し、*ASA* CLI にアクセスし、**connect fxos** コマンドを使用して FXOS CLI にアクセスします。SSH、HTTPS、および SNMPv3 は暗号化できるため、データ インターフェイスへの直接接続は安全です。

手順

ステップ 1 ASDM で、[Configuration] > [Firewall] > [Advanced] > [FXOS Remote Management] を選択します。

ステップ 2 FXOS リモート管理を有効にします。

a) ナビゲーション ウィンドウで、[HTTPS]、[SNMP]、または [SSH] を選択します。

b) [Add] をクリックし、管理を許可する [Interface] を設定し、接続を許可する [IP Address] を設定し、[OK] をクリックします。
プロトコル タイプごとに複数のエントリを作成できます。以下のデフォルト値を使用しない場合は、[Port] を設定します。

- HTTPS デフォルト ポート：3443

- SNMP デフォルト ポート：3061
- SSH デフォルト ポート：3022

ステップ 3 FXOS が ASA インターフェイスから管理接続を開始できるようにします。

a) ナビゲーション ウィンドウで [FXOS Traffic Initiation] を選択します。

b) [Add] をクリックし、FXOS 管理トラフィックを送信する必要がある ASA インターフェイスを有効にします。デフォルトでは、外部インターフェイスは有効になっています。

ステップ 4 [Apply] をクリックします。

ステップ 5 Firepower Chassis Manager に接続します（デフォルトでは、https://192.168.45.45、ユーザ名：**admin**、パスワード：**Admin123**）。

ステップ 6 [Platform Settings] タブをクリックし、[SSH]、[HTTPS]、または [SNMP] を有効にします。
SSH と HTTPS はデフォルトで有効になっています。

ステップ 7 [Platform Settings] タブで、管理アクセスを許可するように [Access List] を設定します。デフォルトでは、SSH および HTTPS は管理 1/1 192.168.45.0 ネットワークのみを許可します。ASA の [FXOS Remote Management] 設定で指定したアドレスを許可する必要があります。

SSH を使用した FXOS への接続

デフォルトの IP アドレス 192.168.45.45 を使用して管理 1/1 の FXOS に接続できます。リモート管理を設定する場合（データ インターフェイスでの FXOS の管理アクセスの設定, （14 ページ））、非標準ポート（デフォルトでは 3022）でデータ インターフェイス IP アドレスに接続することもできます。

SSH を使用して ASA に接続するには、まず、ASA の一般的な操作の設定ガイドに従って SSH アクセスを設定する必要があります。

ASA CLI から FXOS、およびその逆方向に接続することができます。

FXOS は最大 8 個の SSH 接続を許可します。

はじめる前に

管理 IP アドレスを変更するには、FXOS 管理 IP アドレスまたはゲートウェイの変更, （16 ページ）を参照してください。

手順

ステップ 1 管理 1/1 に接続している管理コンピュータで、管理 IP アドレスに SSH 接続します（デフォルトでは、https://192.168.45.45、ユーザ名：**admin**、パスワード：**Admin123**）。
任意のユーザ名でログインできます（ユーザの追加, （45 ページ）を参照）。リモート管理を設定する場合、ASA データ インターフェイス IP にポート 3022（デフォルトのポート）で SSH 接続します。

ステップ 2 ASA CLI に接続します。
connect asa

FXOS CLI に戻るには、**Ctrl+a**、**d** と入力します。

例：

```
firepower-2100# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

ステップ 3 ASA に SSH 接続する場合（ASA で SSH アクセスを設定した後）、FXOS CLI に接続します。
connect fxos

FXOS への認証を求められます。デフォルトのユーザ名：**admin** およびパスワード：**Admin123** を使用します。ASA CLI に戻るには、**exit** と入力するか、または **Ctrl-Shift-6**、**x** と入力します。

例：

```
ciscoasa# connect fxos
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.

FXOS 2.2(2.32) kp2110

kp2110 login: admin
Password: Admin123
Last login: Sat Jan 23 16:20:16 UTC 2017 on pts/1
Successful login attempts for user 'admin' : 4
Cisco Firepower Extensible Operating System (FX-OS) Software

[…]

kp2110#
kp2110# exit
Remote card closed command session. Press any key to continue.
Connection with fxos terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

FXOS 管理 IP アドレスまたはゲートウェイの変更

FXOS CLI から Firepower 2100 シャーシの管理 IP アドレスを変更できます。デフォルトのアドレスは 192.168.45.45 です。デフォルト ゲートウェイを変更することもできます。デフォルト ゲートウェイは 0.0.0.0 に設定されており、トラフィックを ASA に送信します。代わりに管理 1/1 ネットワークでルータを使用する場合、ゲートウェイ IP アドレスを変更します。管理接続のアクセスリストを新しいネットワークに一致するように変更する必要もあります。

通常、FXOS 管理 1/1 IP アドレスは ASA 管理 1/1 IP アドレスと同じネットワーク上にあります。ASA の ASA IP アドレスも必ず変更してください。

はじめる前に

- 管理 IP アドレスを変更した後で、新しいアドレスを使用して Firepower Chassis Manager および SSH 接続を再確立する必要があります。
- DHCP サーバはデフォルトでは管理 1/1 で有効になっているため、管理 IP アドレスを変更する前に DHCP を無効にする必要があります。

手順

ステップ 1 コンソール ポートに接続します（ASA および FXOS の CLI アクセス, （13 ページ）を参照）。接続が失われないようにするために、コンソールに接続することをお勧めします。

ステップ 2 DHCP サーバを無効にします。

scope system

scope services

disable dhcp-server

commit-buffer

管理 IP アドレスを変更した後で、新しいクライアント IP アドレスを使用して DHCP を再び有効にすることができます。Firepower Chassis Manager で DHCP サーバを有効および無効にすることもできます（[Platform Settings] > [DHCP]）。

例：

```
firepower-2100# scope system
firepower-2100 /system # scope services
firepower-2100 /system/services # disable dhcp-server
firepower-2100 /system/services* # commit-buffer
```

ステップ 3 IPv4 管理 IP アドレス、および必要に応じてゲートウェイを設定します。

a) fabric-interconnect a のスコープを設定します。

scopefabric-interconnecta

例：

```
firepower-2100# scope fabric-interconnect a
firepower-2100 /fabric-interconnect #
```

b) 現在の管理 IP アドレスを表示します。

show

例：

```
firepower-2100 /fabric-interconnect # show

Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
 Prefix Operability
    ---- --------------- --------------- --------------- ---------------- ----------------
 ------ -----------
```

```
    A    192.168.45.45    0.0.0.0        0.0.0.0          ::               ::
     64     Operable
```

c) 新しい管理 IP アドレス、および必要に応じて新しいデフォルト ゲートウェイを設定します。
setout-of-band staticip *ip_address***netmask** *network_mask***gw** *gateway_ip_address*

現在設定されているゲートウェイを維持するには、**gw** キーワードを省略します。同様に既存の管理IPアドレスを維持したままゲートウェイを変更するには、**ip** キーワードと **netmask** キーワードを省略します。

例：

```
firepower-2100 /fabric-interconnect # set out-of-band static ip 192.168.4.1 netmask
255.255.255.0
Warning: When committed, this change may disconnect the current CLI session
firepower-2100 /fabric-interconnect* #
```

ステップ 4 IPv6 管理 IP アドレスとゲートウェイを設定します。

a) fabric-interconnect a のスコープ、次に IPv6 設定のスコープを設定します。
scopefabric-interconnecta

scopeipv6-config

例：

```
firepower-2100# scope fabric-interconnect a
firepower-2100 /fabric-interconnect # scope ipv6-config
firepower-2100 /fabric-interconnect/ipv6-config #
```

b) 現在の管理 IPv6 アドレスを表示します。
show ipv6-if

例：

```
firepower-2100 /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
    IPv6 Address                            Prefix     IPv6 Gateway
    ----------------------------------- ---------- ------------
    ::                                      ::         ::
```

c) 新しい管理 IPv6 アドレスとゲートウェイを設定します。
Firepower-chassis /fabric-interconnect/ipv6-config # **setout-of-band staticipv6** *ipv6_address***ipv6-prefix** *prefix_length***ipv6-gw** *gateway_address*

現在設定されているゲートウェイを維持するには、**ipv6-gw** キーワードを省略します。同様に既存の管理 IP アドレスを維持したままゲートウェイを変更するには、**ipv6** キーワードと **ipv6-prefix** キーワードを省略します。

例：

```
firepower-2100 /fabric-interconnect/ipv6-config # set out-of-band static ipv6 2001:DB8::34
 ipv6-prefix 64 ipv6-gw 2001:DB8::1
```

```
firepower-2100 /fabric-interconnect/ipv6-config* #
```

ステップ 5 HTTPS、SSH、および SNMP のアクセス リストを設定して、新しいネットワークからの管理接続を可能にします。

scope system

scope services

IPv4 の場合

enterip-block *ip_address prefix* [**http** | **snmp** | **ssh**]

IPv6 の場合

enteripv6-block *ipv6_address prefix* [**https** | **snmp** | **ssh**]

IPv4 の場合、すべてのネットワークを許可するには **0.0.0.0** とプレフィックス **0** を入力します。IPv6 の場合、すべてのネットワークを許可するには **::** とプレフィックス **0** を入力します。Firepower Chassis Manager でアクセス リストを追加することもできます（[Platform Settings] > [Access List]）。

例：

```
firepower-2100# scope system
firepower-2100 /system # scope services
firepower-2100 /system/services # enter ip-block 192.168.4.0 24 https
firepower-2100 /system/services/ip-block* # exit
firepower-2100 /system/services* # enter ip-block 192.168.4.0 24 ssh
firepower-2100 /system/services/ip-block* # exit
firepower-2100 /system/services* # enter ip-block 192.168.4.0 24 snmp
firepower-2100 /system/services/ip-block* # exit
firepower-2100 /system/services* # enter ipv6-block 2001:DB8:: 64 https
firepower-2100 /system/services/ip-block* # exit
firepower-2100 /system/services* # enter ipv6-block 2001:DB8:: 64 ssh
firepower-2100 /system/services/ip-block* # exit
firepower-2100 /system/services* # enter ipv6-block 2001:DB8:: 64 snmp
firepower-2100 /system/services/ip-block* # exit
firepower-2100 /system/services* #
```

ステップ 6 （任意） IPv4 DHCP サーバを再び有効にします。

scope system

scope services

enable dhcp-server *start_ip_address end_ip_address*

Firepower Chassis Manager で DHCP サーバを有効および無効にすることもできます（[Platform Settings] > [DHCP]）。

例：

```
firepower-2100# scope system
firepower-2100 /system # scope services
firepower-2100 /system/services # enable dhcp-server 192.168.4.10 192.168.4.20
```

ステップ 7 設定を保存します。

commit-buffer

例：

```
firepower-2100 /system/services* # commit-buffer
```

次の例では、IPv4 管理インターフェイスとゲートウェイを設定します。

```
firepower-2100# scope fabric-interconnect a
firepower-2100 /fabric-interconnect # show

Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
 Prefix Operability
    ---- --------------- --------------- --------------- --------------- ---------------
 ------ -----------
    A    192.168.2.112    192.168.2.1     255.255.255.0   2001:DB8::2     2001:DB8::1
  64     Operable
firepower-2100 /fabric-interconnect # set out-of-band static ip 192.168.2.111 netmask
255.255.255.0 gw 192.168.2.1
Warning: When committed, this change may disconnect the current CLI session
firepower-2100 /fabric-interconnect* # commit-buffer
firepower-2100 /fabric-interconnect #
```

次の例では、IPv6 管理インターフェイスとゲートウェイを設定します。

```
firepower-2100# scope fabric-interconnect a
firepower-2100 /fabric-interconnect # scope ipv6-config
firepower-2100 /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
    IPv6 Address                      Prefix     IPv6 Gateway
    --------------------------------- ---------- ------------
    2001:DB8::2                        64         2001:DB8::1
firepower-2100 /fabric-interconnect/ipv6-config # set out-of-band static ipv6 2001:DB8::2
ipv6-prefix 64 ipv6-gw 2001:DB8::1
firepower-2100 /fabric-interconnect/ipv6-config* # commit-buffer
firepower-2100 /fabric-interconnect/ipv6-config #
```

次のステップ

- ASA の設定を続行するには、「Navigating the Cisco ASA Series Documentation」でソフトウェア バージョンに応じたマニュアルを参照してください。
- シャーシを設定するには、「Firepower Chassis Manager の設定, （21 ページ）」を参照してください。

第 2 章

Firepower Chassis Manager の設定

Firepower 2100 は、デバイスの基本的な動作を制御するために FXOS を実行します。GUI の Firepower Chassis Manager または FXOS CLI を使用してこれらの機能を設定できます。このマニュアルでは Firepower Chassis Manager について説明します。すべてのセキュリティ ポリシーおよびその他の動作は、ASA OS で設定される（CLI または ASDM を使用）ことに注意してください。

概要

[Overview] タブで、Firepower 2100 のステータスを簡単にモニタできます。[Overview] タブには次の要素が表示されます。

- Device Information：[Overview] タブの上部には Firepower 2100 に関する次の情報が表示されます。
  - Chassis name：シャーシに割り当てられた名前を表示します。デフォルトでは、名前は **firepower-***model* です（例：firepower-2140）。この名前が CLI プロンプトに表示されます。シャーシ名を変更するには、FXOS CLI **scope system / set name** コマンドを使用します。
  - IP address：シャーシに割り当てられた管理 IP アドレスを表示します。
  - Model：Firepower 2100 モデルを表示します。
  - Version：シャーシで実行されている ASA のバージョン番号を表示します。

- Operational State：シャーシの動作可能ステータスを表示します。
- Chassis uptime：システムが最後に再起動されてからの経過時間を表示します。
- [Uptime Information] アイコン：アイコンにカーソルを合わせると、シャーシおよびASA セキュリティ エンジンの稼働時間を表示します。

- Visual Status Display：[Device Information] セクションの下にはシャーシが視覚的に表示されて、搭載されているコンポーネントとそれらの全般ステータスを示します。[Visual Status Display] に表示されるポートにカーソルを合わせると、インターフェイス名、速度、タイプ、管理状態、動作状態などの追加情報が表示されます。
- Detailed Status Information：[Visual Status Display] の下に表示されるテーブルで、シャーシの詳細なステータス情報を含みます。ステータス情報は、[Faults]、[Interfaces]、[Devices]、[Inventory] の各セクションに分かれています。これらの各セクションの概要をテーブルの上に表示できます。さらに確認する情報の概要エリアをクリックするとそれぞれの詳細を表示できます。

  システムは、シャーシに関する次の詳細なステータス情報を表示します。

  - Faults：システムで発生した障害をリスト表示します。 障害は [Critical]、[Major]、[Minor]、[Warning]、[Info] という重大度でソートされます。リストされた各障害について、重大度、障害の説明、原因、発生回数、最後の発生日時を確認できます。障害が確認済みかどうかもわかります。

    いずれかの障害をクリックして、詳細を表示したり、その障害を確認済みにしたりすることができます。

    （注） 障害の根本原因が解消されると、その障害は次のポーリング間隔中にリストから自動的にクリアされます。特定の障害に対処する場合、現在処理中であることが他のユーザにわかるように、その障害を確認済みにすることができます。

  - Interfaces：システムにインストールされているインターフェイスをリスト表示し、インターフェイス名、動作ステータス、管理ステータス、受信したバイト数、送信したバイト数を示します。

    いずれかのインターフェイスをクリックすると、過去 15 分間にそのインターフェイスが入出力したバイト数がグラフィック表示されます。

  - Devices：ASA を表示し、詳細（デバイス名、デバイス状態、アプリケーション、動作状態、管理状態、イメージ バージョン、および管理 IP アドレス）を示します。
  - Inventory：シャーシに搭載されているコンポーネントをリスト表示し、それらのコンポーネントの関連情報（[component] 名、コアの数、設置場所、動作ステータス、運用性、キャパシティ、電源、温度、シリアル番号、モデル番号、製品番号、ベンダー）を示します。

インターフェイス

FXOS で物理インタ フェースを管理できます。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、ASA で論理的に有効にする必要があります。

Firepower 2100 は、デフォルトで有効になっているジャンボ フレームをサポートします。最大 MTU は 9184 です。

管理インターフェイスの詳細については、ASA と FXOS の管理, （2 ページ）を参照してください。

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、ASA で論理的に有効にする必要があります。

手順

ステップ 1 [Interfaces] タブをクリックします。

ステップ 2 インターフェイスを有効または無効にするには、[Admin State] スライダをクリックします。チェックマークは有効であることを示し、X は無効であることを示します。

（注） 管理 1/1 インターフェイスは、このテーブルで [MGMT] として表示されます。

ステップ 3 速度またはデュプレックスを編集するインターフェイスの [Edit] 鉛筆アイコンをクリックします。

（注） 管理 1/1 インターフェイスを有効または無効にすることのみが可能です。そのプロパティを編集することはできません。

ステップ 4 インターフェイスを有効にするには [Enable] チェックボックスをオンにします。

ステップ 5 [Admin Speed] ドロップダウン リストで、インターフェイスの速度を選択します。

ステップ 6 [Auto Negotiation] で [Yes] または [No] のオプション ボタンをクリックします。

ステップ 7 [Admin Duplex] ドロップダウン リストで、インターフェイスのデュプレックスを選択します。

ステップ 8 [OK] をクリックします。

EtherChannel の追加

EtherChannel（別名ポートチャネル）には、タイプと速度が同じ最大 16 個のメンバー インターフェイスを含めることができます。

（注） EtherChannel メンバー ポートは ASA に表示されますが、EtherChannel およびポート メンバーシップは FXOS でのみ設定できます。

はじめる前に

Firepower 2100 は、アクティブまたはオンの Link Aggregation Control Protocol（LACP）モードで EtherChannel をサポートします。デフォルトでは、LACP モードはアクティブに設定されています。CLI でモードをオンに変更できます。最適な互換性を得るために、接続スイッチ ポートをアクティブ モードに設定することを推奨します。

手順

ステップ 1 [Interfaces] タブをクリックします。

ステップ 2 インターフェイス テーブルの上の [Add Port Channel] をクリックします。

ステップ 3 [Port Channel ID] フィールドに、ポート チャネルの ID を入力します。有効な値は、1 ～ 47 です。

ステップ 4 ポート チャネルを有効にするには、[Enable] チェックボックスをオンにします。
[Type] ドロップダウン リストは無視します。使用可能なタイプは [Data] のみです。

ステップ 5 [Admin Speed] ドロップダウン リストで、すべてのメンバー インターフェイスの速度を選択します。
その速度（および選択したその他の設定）に対応していないインターフェイスを選択すると、可能な範囲で最速の速度が自動的に適用されます。

ステップ 6 すべてのメンバー インターフェイスについて、[Auto Negotiation] で [Yes] または [No] のオプション ボタンをクリックします。

ステップ 7 [Admin Duplex] ドロップダウン リストで、すべてのメンバー インターフェイスのデュプレックスを選択します。

ステップ 8 [Available Interface] リストで、追加するインターフェイスを選択し、[Add Interface] をクリックします。
同じタイプと速度の最大 16 のインターフェイスを追加できます。チャネル グループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。

ヒント 複数のインターフェイスを一度に追加できます。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 9 [OK] をクリックします。

モニタリング インターフェイス

[Interfaces] タブで、シャーシにインストールされているインターフェイスのステータスを表示できます。下部のセクションには、Firepowerシャーシにインストールされているインターフェイスの表が表示されます。上部のセクションには、Firepowerシャーシに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ます。上部セクションでいずれかのインターフェイスにカーソルを合わせると、そのインターフェイスに関する追加情報が表示されます。

インターフェイスは現在のステータスを示すために色分けされています。

- 緑：動作状態は [Up] です。
- 濃い灰色：管理状態は [Disabled] です。
- 赤：動作状態は [Down] です。
- 淡い灰色：SFP がインストールされていません。

論理デバイス

[Logical Devices] ページには、ASA に関する情報とステータスが表示されます。スライダを使用して、トラブルシューティングのために ASA を無効または有効にすることもできます（チェックマークは有効であることを示し、X は無効であることを示します）。

ASA のヘッダーには [Status] が表示されます。

- [ok]：論理デバイスの設定は完了しています。
- [incomplete-configuration]：論理デバイス設定は未完了です。

論理デバイス領域にも ASA の詳細な [Status] が表示されます。

- [Online]：ASA は実行中および動作中です。
- [Offline]：ASA は停止中で、動作不能です。
- [Installing]：ASA のインストールが進行中です。
- [Not Installed]：ASA はインストールされていません。
- [Install Failed]：ASA のインストールに失敗しました。
- [Starting]：ASA は起動中です。
- [Start Failed]：ASA の起動に失敗しました。
- [Started]：ASA は正常に起動し、アプリケーション エージェントのハートビートを待機しています。
- [Stopping]：ASA は停止処理中です。
- [Stop Failed]：ASA をオフラインにできませんでした。

- [Not Responding]：ASA は応答していません。
- [Updating]：ASA ソフトウェアのアップグレードが進行中です。
- [Update Failed]：ASA ソフトウェアのアップグレードに失敗しました。
- [Update Succeeded]：ASA ソフトウェアのアップグレードに成功しました。

Platform Settings

[Platform Settings] タブでは、時間や管理アクセスなどの FXOS の基本的な操作を設定できます。

NTP：時刻の設定

手動でクロックを設定することも、NTP サーバを使用する（推奨）こともできます。最大 4 台の NTP サーバを設定できます。

はじめる前に

- NTP は、デフォルトでは次の Cisco NTP サーバで設定されます：0.sourcefire.pool.ntp.org、1.sourcefire.pool.ntp.org、2.sourcefire.pool.ntp.org。
- 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。DNS：DNS サーバの設定，（39 ページ）を参照してください。

手順

ステップ 1 [Platform Settings] タブをクリックし、左側のナビゲーションで [NTP] をクリックします。[Time Synchronization] タブがデフォルトで選択されています。

ステップ 2 NTP サーバを使用するには：

a) [Use NTP Server] オプション ボタンをクリックします。
b) [Add] をクリックして、IP アドレスまたはホスト名で最大 4 つの NTP サーバを識別します。NTP サーバのホスト名を使用する場合は、この手順の後半で DNS サーバを設定します。

ステップ 3 手動で時刻を設定するには：

a) [Set Time Manually] オプション ボタンをクリックします。
b) [Date] ドロップダウン リストをクリックしてカレンダーを表示し、そのカレンダーで使用可能なコントロールを使用して日付を設定します。
c) 対応するドロップダウン リストを使用して、時刻を時間、分、および[AM/PM] で指定します。

ステップ 4 [Current Time] タブをクリックし、[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 5 [Save（保存）] 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。

SSH：SSH の設定

次の手順では、Firepower シャーシへの SSH アクセスを有効または無効にする方法、およびシャーシを SSH クライアントとして有効にする方法について説明します。SSH サーバとクライアントはデフォルトで有効になっています。

はじめる前に

手順

ステップ 1 [Platform Settings] > [SSH] > [SSH Server] を選択します。

ステップ 2 Firepower シャーシへの SSH アクセスを SSH サーバが提供できるようにするには、[Enable SSH] チェックボックスをオンにします。

ステップ 3 サーバの [Encryption Algorithm] について、許可される暗号化アルゴリズムごとにチェックボックスをオンにします。

ステップ 4 サーバの [Key Exchange Algorithm] について、許可される Diffie-Hellman（DH）キー交換ごとにチェックボックスをオンにします。
DH キー交換は、いずれかの当事者単独では決定できない共有秘密を提供します。キー交換は署名とホスト キーを組み合わせてホスト認証を提供します。このキー交換方式により、明示的なサーバ認証が可能となります。DH キー交換方法の使用方法の詳細については、RFC 4253 を参照してください。

ステップ 5 サーバの [Mac Algorithm] について、許可される整合性アルゴリズムごとにチェックボックスをオンにします。

ステップ 6 サーバの [Host Key] について、RSA キー ペアのモジュラス サイズを入力します。
モジュラス値（ビット単位）は、1024 ～ 2048 の範囲内の 8 の倍数です。指定するキー係数のサイズが大きいほど、RSA キー ペアの生成にかかる時間は長くなります。値は 2048 にすることをお勧めします。

ステップ 7 サーバの [Volume Rekey Limit] について、FXOS がセッションを切断するまでにその接続で許可されるトラフィックの量を KB 単位で設定します。

ステップ 8 サーバの [Time Rekey Limit] について、FXOS がセッションを切断するまでに SSH セッションがアイドルであることができる時間を分単位で設定します。

ステップ 9 [Save（保存）] をクリックします。

ステップ 10 [SSH Client] タブをクリックして、FXOS シャーシの SSH クライアントをカスタマイズします。

ステップ 11 [Strict Host Keycheck] について、[enable]、[disable]、または [prompt] を選択して、SSH ホスト キー チェックを制御します。

- enable：FXOS が認識するホスト ファイルにそのホスト キーがまだ存在しない場合、接続は拒否されます。 FXOS CLI でシステム スコープまたはサービス スコープの **enter ssh-host** コマンドを使用して、手動でホストを追加する必要があります。
- prompt：シャーシにまだ格納されていないホストキーを許可または拒否するように求められます。
- disable：（デフォルト）シャーシは過去に保存されたことがないホストキーを自動的に許可します。

ステップ 12 クライアントの [Encryption Algorithm] について、許可される暗号化アルゴリズムごとにチェックボックスをオンにします。

ステップ 13 クライアントの [Key Exchange Algorithm] について、許可される Diffie-Hellman（DH）キー交換ごとにチェックボックスをオンにします。
DH キー交換は、いずれかの当事者単独では決定できない共有秘密を提供します。キー交換は署名とホスト キーを組み合わせてホスト認証を提供します。このキー交換方式により、明示的なサーバ認証が可能となります。DH キー交換方法の使用方法の詳細については、RFC 4253 を参照してください。

ステップ 14 クライアントの [Mac Algorithm] について、許可される整合性アルゴリズムごとにチェックボックスをオンにします。

ステップ 15 クライアントの [Volume Rekey Limit] について、FXOS がセッションを切断するまでにその接続で許可されるトラフィックの量を KB 単位で設定します。

ステップ 16 クライアントの [Time Rekey Limit] について、FXOS がセッションを切断するまでに SSH セッションがアイドルであることができる時間を分単位で設定します。

ステップ 17 [Save（保存）] をクリックします。

SNMP

Firepower シャーシに Simple Network Management Protocol（SNMP）を設定するには、[SNMP] ページを使用します。

SNMP の概要

SNMP は、アプリケーション層プロトコルであり、SNMP マネージャと SNMP エージェントとの通信に使用されるメッセージ フォーマットを提供します。SNMP では、ネットワーク内のデバイスのモニタリングと管理に使用する標準フレームワークと共通言語が提供されます。

SNMP フレームワークは 3 つの部分で構成されます。

- SNMP マネージャ：SNMP を使用してネットワーク デバイスのアクティビティを制御し、モニタリングするシステム

- SNMP エージェント：Firepower シャーシ内のソフトウェア コンポーネントで、Firepower シャーシのデータを維持し、必要に応じてそのデータを SNMP マネージャに送信します。Firepower シャーシには、エージェントと一連の MIB が含まれています。
- 管理情報ベース（MIB）：SNMP エージェント上の管理対象オブジェクトのコレクション。

Firepower シャーシは、SNMPv1、SNMPv2c、および SNMPv3 をサポートします。SNMPv1 および SNMPv2c はどちらも、コミュニティベース形式のセキュリティを使用します。

SNMP 通知

SNMP の重要な機能の 1 つは、SNMP エージェントから通知を生成できることです。これらの通知では、要求を SNMP マネージャから送信する必要はありません。通知は、不正なユーザ認証、再起動、接続の切断、隣接ルータとの接続の切断、その他の重要なイベントを表示します。

Firepower シャーシは、トラップまたはインフォームとして SNMP 通知を生成します。SNMP マネージャはトラップ受信時に確認応答を送信せず、Firepower シャーシはトラップが受信されたかどうかを確認できないため、トラップの信頼性はインフォームよりも低くなります。インフォーム要求を受信する SNMP マネージャは、SNMP 応答プロトコル データ ユニット（PDU）でメッセージの受信を確認応答します。Firepower シャーシが PDU を受信しない場合、インフォーム要求を再送できます。

SNMP セキュリティ レベルおよび権限

SNMPv1、SNMPv2c、および SNMPv3 はそれぞれ別のセキュリティ モデルを表します。セキュリティ モデルは、選択したセキュリティ レベルと結合され、SNMP メッセージの処理中に適用されるセキュリティ メカニズムを決定します。

セキュリティ レベルは、SNMP トラップに関連付けられているメッセージを表示するために必要な特権を決定します。権限レベルは、メッセージが開示されないよう保護または認証の必要があるかどうかを決定します。サポートされるセキュリティ レベルは、セキュリティ モデルが設定されているかによって異なります。SNMP セキュリティ レベルは、次の権限の 1 つ以上をサポートします。

- noAuthNoPriv：認証なし、暗号化なし
- authNoPriv：認証あり、暗号化なし
- authPriv：認証あり、暗号化あり

SNMPv3 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。セキュリティ モデルは、ユーザおよびユーザが属するロールを設定する認証方式です。セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ モデルとセキュリティ レベルの組み合わせにより、SNMP パケット処理中に採用されるセキュリティ メカニズムが決まります。

SNMP セキュリティ モデルとレベルのサポートされている組み合わせ

次の表に、セキュリティ モデルとレベルの組み合わせの意味を示します。

表 *1* : *SNMP* セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	結果
v1	noAuthNoPriv	コミュニティ ストリング	なし	コミュニティ ストリングの照合を使用して認証します。
v2c	noAuthNoPriv	コミュニティ ストリング	なし	コミュニティ ストリングの照合を使用して認証します。
v3	noAuthNoPriv	ユーザ名	未対応	ユーザ名の照合を使用して認証します。
v3	authNoPriv	HMAC-SHA	なし	HMAC Secure Hash Algorithm（SHA）に基づいて認証します。
v3	authPriv	HMAC-SHA	DES	HMAC-SHA アルゴリズムに基づいて認証します。データ暗号規格（DES）の 56 ビット暗号化、および暗号ブロック連鎖（CBC）DES（DES-56）標準に基づいた認証を提供します。

SNMPv3 セキュリティ機能

SNMPv3 は、ネットワーク経由のフレームの認証と暗号化を組み合わせることによって、デバイスへのセキュア アクセスを実現します。SNMPv3 は、設定済みユーザによる管理動作のみを許可し、SNMP メッセージを暗号化します。SNMPv3 ユーザベース セキュリティ モデル（USM）は SNMP メッセージレベル セキュリティを参照し、次のサービスを提供します。

- メッセージの完全性：メッセージが不正な方法で変更または破壊されていないことを保証します。また、データ シーケンスが、通常発生するものよりも高い頻度で変更されていないことを保証します。

- メッセージ発信元の認証：受信データを発信したユーザのアイデンティティが確認されたことを保証します。
- メッセージの機密性および暗号化：不正なユーザ、エンティティ、プロセスに対して情報を利用不可にしたり開示しないようにします。

SNMP サポート

Firepower シャーシは SNMP の次のサポートを提供します。

MIB のサポート

Firepower シャーシは MIB への読み取り専用アクセスをサポートします。

SNMPv3 ユーザの認証プロトコル

Firepower シャーシは、SNMPv3 ユーザの HMAC-SHA-96（SHA）認証プロトコルをサポートします。

SNMPv3 ユーザの AES プライバシー プロトコル

SHA ベースの認証に加えて、Firepower シャーシは AES-128 ビット Advanced Encryption Standard を使用したプライバシーも提供します。Firepowerシャーシは、プライバシーパスワードを使用して 128 ビット AES キーを生成します。AES プライバシー パスワードは最小で 8 文字です。パスフレーズをクリア テキストで指定する場合、最大 80 文字を指定できます。

SNMP を設定します。

SNMP を有効にし、トラップおよび SNMPv3 ユーザを追加します。

手順

ステップ 1 [Platform Settings] > [SNMP] を選択します。

ステップ 2 [SNMP] 領域で、次のフィールドに入力します。

名前	説明
[Admin State] チェックボックス	SNMP が有効化かディセーブルか。システムに SNMP サーバとの統合が含まれる場合にだけこのサービスをイネーブルにします。
[Port] フィールド	Firepower シャーシが SNMP ホストと通信するためのポート。デフォルト ポートは変更できません。

名前	説明
[Community/Username] フィールド	Firepower シャーシが SNMP ホストに送信するトラップ メッセージに含める、デフォルトの SNMP v1 または v2c コミュニティ名あるいは SNMP v3 ユーザ名。 1 ～ 32 文字の英数字文字列を入力します。@（アットマーク）、\（バックスラッシュ）、"（二重引用符）、?（疑問符）または空欄スペースは使用しないでください。デフォルトは public です。 [Community/Username] フィールドがすでに設定されている場合、空白フィールドの右側のテキストは [Set: Yes] を読み取ることに注意してください。[Community/Username] フィールドに値が入力されていない場合、空白フィールドの右側のテキストは [Set: No] を読み取ります。
[System Administrator Name] フィールド	SNMP 実装の担当者の連絡先。 電子メール アドレス、名前、電話番号など、255 文字までの文字列を入力します。
[Location] フィールド	SNMP エージェント（サーバ）が実行するホストの場所。 最大 510 文字の英数字を入力します。

ステップ 3 [SNMP Traps] 領域で、[Add] をクリックします。

ステップ 4 [Add SNMP Trap] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Host Name] フィールド	Firepower シャーシからのトラップを受信する SNMP ホストのホスト名または IP アドレス。
[Community/Username] フィールド	Firepower シャーシが SNMP ホストに送信するトラップに含める SNMP v1 または v2 コミュニティ名あるいは SNMP v3 ユーザ名。これは、SNMP サービスに設定されたコミュニティまたはユーザ名と同じである必要があります。 1 ～ 32 文字の英数字文字列を入力します。@（アットマーク）、\（バックスラッシュ）、"（二重引用符）、?（疑問符）または空欄スペースは使用しないでください。
[Port] フィールド	Firepower シャーシが SNMP ホストとのトラップの通信に使用するポート。 1 ～ 65535 の整数を入力します。

名前	説明
[Version] フィールド	トラップに使用される SNMP バージョンおよびモデル。次のいずれかになります。 • [V1] • V2 • V3
[Type] フィールド	バージョンとして [V2] または [V3] を選択した場合に、送信するトラップのタイプ。次のいずれかになります。 • Traps • [nforms]
[v3 Privilege] フィールド	バージョンとして [V3] を選択した場合に、トラップに関連付ける権限。次のいずれかになります。 • [Auth]：認証あり、暗号化なし • [Noauth]：認証なし、暗号化なし • [Priv]：認証あり、暗号化あり

ステップ 5 [OK] をクリックして、[Add SNMP Trap] ダイアログボックスを閉じます。

ステップ 6 [SNMP Users] 領域で、[Add] をクリックします。

ステップ 7 [Add SNMP User] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	SNMP ユーザに割り当てられるユーザ名。 32 文字までの文字または数字を入力します。名前は文字で始まる必要があり、_（アンダースコア）、.（ピリオド）、@（アット マーク）、-（ハイフン）も指定できます。
[Auth Type] フィールド	許可タイプ：[SHA]。
[Use AES-128] チェックボックス	オンにすると、このユーザに AES-128 暗号化が使用されます。
[Password] フィールド	このユーザのパスワード。
[Confirm Password] フィールド	確認のためのパスワードの再入力。

名前	説明
[Privacy Password] フィールド	このユーザのプライバシー パスワード。
[Confirm Privacy Password] フィールド	確認のためのプライバシー パスワードの再入力。

ステップ 8 [OK] をクリックして、[Add SNMP User] ダイアログボックスを閉じます。

ステップ 9 [Save（保存）] をクリックします。

HTTPS：ポートの変更

HTTPS サービスは、デフォルトでポート 443 で有効化になります。HTTPS をディセーブルにすることはできませんが、HTTPS 接続に使用するポートは変更できます。

はじめる前に

ASA データ インターフェイスで HTTPS アクセスを有効にする場合は、HTTPS ポートを 443 から変更しないでください。デフォルトのポートのみがサポートされます。

手順

ステップ 1 [Platform Settings] > [HTTPS] を選択します。

ステップ 2 HTTPS 接続に使用するポートを [Port] フィールドに入力します。1 ～ 65535 の整数を指定します。このサービスは、デフォルトでポート 443 でイネーブルになります。

ステップ 3 [Save（保存）] をクリックします。
指定した HTTPS ポートが Firepower シャーシに設定されます。

HTTPS ポートを変更すると、現在のすべての HTTPS セッションが閉じられます。ユーザは、次のように新しいポートを使用して再度 Firepower Chassis Manager にログインする必要があります。

https://<*chassis_mgmt_ip_address*>:<*chassis_mgmt_port*>

<*chassis_mgmt_ip_address*> は、初期設定時に入力した Firepower シャーシの IP アドレスまたはホスト名で、<*chassis_mgmt_port*> は設定が完了した HTTPS ポートです。

DHCP：管理クライアント用に DHCP サーバを設定する

管理 1/1 インターフェイスに接続しているクライアントに対して DHCP サーバを有効にすることができます。デフォルトでは、サーバはアドレス範囲 192.168.45.10 ～ 192.168.45.12 で有効になっ

ています。管理 IP アドレスを変更する場合、DHCP を無効にする必要があります（FXOS 管理 IP アドレスまたはゲートウェイの変更，（16 ページ）を参照）。その後、新しいネットワークの DHCP を再度有効にすることができます。

手順

ステップ 1 [Platform Settings] > [DHCP] を選択します。
ステップ 2 [Enable DHCP service] チェックボックスをオンにします。
ステップ 3 [Start IP] と [End IP] にアドレスを入力します。
ステップ 4 [Save（保存）] をクリックします。

syslog：syslog メッセージングの設定

システム ロギングは、デバイスから syslog デーモンを実行するサーバへのメッセージを収集する方法です。中央の syslog サーバへロギングは、ログおよびアラートの集約に役立ちます。ログは、ルーチン トラブルシューティングおよびインシデント処理の両方で役立ちます。

これらの syslog メッセージは FXOS シャーシにのみ適用されます。ASA syslog メッセージの場合、ASA 設定でロギングを設定する必要があります。

手順

ステップ 1 [Platform Settings] > [Syslog] を選択します。
ステップ 2 ローカル宛先を設定します。

a) [Local Destinations] タブをクリックします。
b) 次のフィールドに入力します。

名前	説明
コンソール	
Admin State	コンソールに syslog メッセージを表示するには、[Enable] チェックボックスをオンにします。
レベル	コンソールに表示するメッセージの最低レベルをクリックします。Firepower シャーシにはそのレベル以上のメッセージが表示されます。 • Emergencies • Alerts • [Critical]

名前	説明
Platform	
Admin State	プラットフォーム syslog は常に有効です。
レベル	表示するメッセージの最低レベルを選択します。Firepower シャーシにはそのレベル以上のメッセージが表示されます。デフォルトは [Informational] です。 • Emergencies • Alerts • Critical • エラー • Warnings • Notifications • Information • Debugging
ファイル	
Admin State	syslog メッセージをファイルに保存するには、[Enable] チェックボックスをオンにします。
レベル	保存するメッセージの最低レベルを選択します。システムはそのレベル以上のメッセージを保存します。 • Emergencies • Alerts • Critical • エラー • Warnings • Notifications • Information • Debugging
名前	16 文字までのファイル名を設定します。

名前	説明
サイズ	最新のメッセージで最も古いメッセージが上書きされる前の最大ファイルサイズ（バイト単位）を指定します。有効な範囲は 4096 ～ 4194304 バイトです。

c) [Save（保存）] をクリックします。

ステップ 3 リモート宛先を設定します。

a) [Remote Destinations] タブをクリックします。

b) [Remote Destinations] タブで、Firepower シャーシによって生成されたメッセージを保存できる最大 3 つの外部ログについて、次のフィールドに入力します。
syslog メッセージをリモート宛先に送信することで、外部 syslog サーバで利用可能なディスク領域に応じてメッセージをアーカイブし、保存後にロギング データを操作できます。たとえば、特定タイプの syslog メッセージがログに記録されたり、ログからデータが抽出されてレポート用の別のファイルにその記録が保存されたり、あるいはサイト固有のスクリプトを使用して統計情報が追跡されたりした場合に、特別なアクションが実行されるように指定できます。

名前	説明
Admin State	syslog メッセージをリモート ログ ファイルに保存するには、[Enable] チェックボックスをオンにします。
レベル	システムに保存するメッセージの最も低いレベルを選択します。リモート ファイルにそのレベル以上のメッセージが保存されます。 • Emergencies • Alerts • Critical • エラー • Warnings • Notifications • Information • Debugging
Hostname/IP Address	syslog サーバのホスト名または IP アドレスを設定します。 （注） IP アドレスではなく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。

名前	説明
ファシリティ	ファイル メッセージのベースとして使用する syslog サーバのシステム ログ機能を選択します。 • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7

c) [Save（保存）] をクリックします。

ステップ 4 ローカル送信元を設定します。

a) [Local Sources] タブをクリックします。

b) 次のフィールドに入力します。

名前	説明
Faults Admin State	システム障害ロギングを有効化するかどうか。[Enable] チェックボックスをオンにすると、Firepower シャーシはすべてのシステム障害をログに記録します。
Audits Admin State	監査ロギングを有効化するかどうか。[Enable] チェックボックスをオンにすると、Firepower シャーシはすべての監査ログ イベントをログに記録します。
Events Admin State	システム イベント ロギングを有効化するかどうか。[Enable] チェックボックスをオンにすると、Firepower シャーシはすべてのシステム イベントをログに記録します。

c) [Save（保存）] をクリックします。

DNS：DNS サーバの設定

システムでホスト名のIPアドレスへの解決が必要な場合は、DNSサーバを指定する必要があります。最大 4 台の DNS サーバを設定できます。複数の DNS サーバを設定する場合、システムによるサーバの検索順はランダムになります。

はじめる前に

- DNS は、デフォルトでは次の OpenDNS サーバで構成されています：208.67.222.222、208.67.220.220。

手順

ステップ 1 [Platform Settings] > [DNS] を選択します。

ステップ 2 [Enable DNS Server] チェックボックスをオンにします。

ステップ 3 追加する DNS サーバ（最大 4 台）ごとに、それぞれの IP アドレスを [DNS Server] フィールドに入力し、[Add] をクリックします。

ステップ 4 [Save（保存）] をクリックします。

ステップ 5 [Domain Name Configuration] タブをクリックし、Firepower シャーシが非修飾名にサフィックスとして追加する [Domain name] を入力し、[Add] をクリックします。
たとえば、ドメイン名を「example.com」に設定し、syslog サーバとして非修飾名「jupiter」を指定した場合は、Firepowerシャーシによって名前が修飾されて「jupiter.example.com」となります。

FIPSおよびコモンクライテリア：FIPSおよびコモンクライテリアモードの有効化

Firepower2100でFIPSまたはコモン クライテリア（CC）モードを有効にするには、次の手順を実行します。

また、fips enable コマンドを使用して ASA で個別に FIPS モードを有効にする必要もあります。ASA には、コモン クライテリア モードに関する個別の設定はありません。CC または UCAPL のコンプライアンスに関する追加の制限があれば、シスコのセキュリティ ポリシーのマニュアルに従って設定する必要があります。

最初に ASA で FIPS モードを設定し、デバイスのリロードを待ってから、FXOS で FIPS モードを設定することをお勧めします。

手順

ステップ 1 [Platform Settings] > [FIPS and Common Criteria] を選択します。

ステップ 2 [Enable] チェックボックスをオンにすることにより、[FIPS] を有効にします。

ステップ 3 [Enable] チェックボックスをオンにすることにより、[Common Criteria] を有効にします。
コモン クライテリアを有効にすると、[FIPS Enable] チェックボックスはデフォルトでオンになります。

ステップ 4 [Save（保存）] をクリックします。

ステップ 5 プロンプトに従ってシステムをリブートします。

アクセス リスト：管理アクセスの設定

デフォルトでは、Firepower 2100 は、管理 1/1 192.168.45.0/24 ネットワークで、Firepower Chassis Manager への HTTPS アクセス、および SSH アクセスを許可します。他のネットワークからのアクセスを許可、または SNMP を許可する場合は、アクセス リストを追加または変更する必要があります。

IP アドレス（v4 または v6）のブロックごとに、サービスごとに最大 25 個の異なるサブネットを設定できます。

手順

ステップ 1 [Platform Settings] > [Access List] を選択します。

ステップ 2 [IPv4 Access List] 領域で：

a) [Add] をクリックします。

b) 次の値を入力します。

- [IP Address]：IP アドレスを設定します。 すべてのネットワークを許可するには、**0.0.0.0** と入力します。
- [Prefix Length]：サブネット マスクを設定します。 すべてのネットワークを許可するには、**0** と入力します。
- [Protocol]：[HTTPS]、[SNMP]、または [SSH] を選択します。

c) [OK] をクリックします。

d) サービスごとにネットワークを追加するには、これらのステップを繰り返します。

ステップ 3 [IPv6 Access List] 領域で：

a) [Add] をクリックします。

b) 次の値を入力します。

- [IP Address]:IP アドレスを設定します。 すべてのネットワークを許可するには、:: と入力します。
- [Prefix Length]：プレフィックス長を設定します。 すべてのネットワークを許可するには、**0** と入力します。
- [Protocol]：[HTTPS]、[SNMP]、または [SSH] を選択します。

c) [OK] をクリックします。
d) サービスごとにネットワークを追加するには、これらのステップを繰り返します。

ステップ 4 [Save（保存）] をクリックします。

システム アップデート

この作業はスタンドアロン ASA に適用されます。フェールオーバー ペアをアップグレードする場合は、『Cisco ASA Upgrade Guide』を参照してください。アップグレード プロセスには通常 20 ～ 30 分かかります。

ASA、ASDM、および FXOS のイメージは 1 つのパッケージにバンドルされています。パッケージのアップデートは FXOS によって管理されます。ASA オペレーティング システム内で ASA をアップグレードすることはできません。ASA と FXOS を個別にアップグレードすることはできません。常にバンドルされています。

ASDMの場合は例外です。ASAオペレーティングシステム内からアップグレードできるため、必ずしもバンドルされた ASDM イメージを使用する必要はありません。手動でアップロードする ASDM イメージは FXOS イメージ リストに表示されません。ASA から ASDM イメージを管理する必要があります。

（注） バンドルをアップグレードすると、同じ名前（**asdm.bin**）であるため、バンドル内の ASDM イメージが前の ASDM バンドル イメージを置き換えます。アップロードした別の ASDM イメージ（たとえば、**asdm-782.bin**）を手動で選択した場合、バンドル アップグレード後も継続してそのイメージを使用することになります。互換性のある ASDM バージョンを実行していることを確認するには、バンドルをアップグレードする前にASDMをアップグレードするか、または ASA バンドルをアップグレードする直前に、バンドルされた ASDM イメージ（**asdm.bin**）を使用するように ASA を再設定する必要があります。

はじめる前に

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てください。

手順

ステップ 1 [System] > [Updates] を選択します。
[Available Updates] ページに、シャーシで使用可能なパッケージのリストが表示されます。

ステップ 2 [Upload Image] をクリックします。

ステップ 3 [Browse] をクリックし、アップロードするイメージを見つけて選択します。

ステップ 4 [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。イメージの整合性は、新しいイメージがシャーシに追加されると自動的に確認されます。手動で確認する場合は、[Verify]（チェックマーク アイコン）をクリックします。

ステップ 5 アップグレードする ASA パッケージを選択し、[Upgrade] をクリックします。

ステップ 6 インストールの続行を確定するには [Yes] を、インストールをキャンセルするには [No] をクリックします。
アップグレード中に、Firepower Chassis Manager からログアウトされます。

User Management

ユーザ アカウントは、Firepower 2100 シャーシにアクセスするために使用されます。これらのアカウントは、Firepower Chassis Manager および SSH アクセスで使用されます。ASA には別のユーザ アカウントと認証があります。

ユーザ アカウントの概要

最大 48 のローカル ユーザ アカウントを設定できます。各ユーザ アカウントには、一意のユーザ名とパスワードが必要です。

アカウント タイプ

管理者アカウント

管理者アカウントはデフォルトユーザアカウントであり、変更や削除はできません。このアカウントは、システム管理者またはスーパーユーザ アカウントであり、すべての権限が与えられています。デフォルトのパスワードは Admin123 です。

管理者アカウントは常にアクティブで、有効期限がありません。管理者アカウントを非アクティブに設定することはできません。

ローカル認証されたユーザ アカウント

ローカル認証されたユーザアカウントは、シャーシによって直接認証され、admin権限を持つユーザが有効または無効にできます。ローカルユーザアカウントが無効になっている場合、ユーザはログインできません。無効化されたローカルユーザアカウントの設定の詳細はデータベースから削除されません。無効ローカルユーザアカウントを再度有効にすると、アカウントはユーザ名とパスワードを含め、既存の設定で再びアクティブになります。

ユーザ ロール

システムには、次のユーザ ロールが用意されています。

アドミニストレータ

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。デフォルトのadminアカウントは、デフォルトでこのロールが割り当てられ、変更はできません。

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。

ユーザ アカウントの有効期限

ユーザ アカウントは、事前に定義した時間に有効期限が切れるように設定できます。有効期限の時間になると、ユーザ アカウントはディセーブルになります。

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。

ユーザ アカウントに有効期限日付を設定した後は、アカウントの有効期限をなくすよう再設定できません。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。

ユーザ アカウントに関するガイドライン

ユーザ名

ユーザ名は、Firepower Chassis ManagerおよびFXOS CLIのログインIDとして使用されます。ユーザ アカウントにログイン ID を割り当てるときは、次のガイドラインおよび制約事項を考慮してください。

- ログイン ID には、次を含む 1 ～ 32 の文字を含めることができます。
  - 任意の英字
  - 任意の数字
  - _（アンダースコア）
  - -（ダッシュ）

- . （ドット）

- ログイン ID は一意である必要があります。
- ログイン ID は、英文字で開始する必要があります。数字やアンダースコアなどの特殊文字からは開始できません。
- ログイン ID では、大文字と小文字が区別されます。
- すべて数字のログイン ID は作成できません。
- ユーザ アカウントの作成後は、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。

パスワード

ローカル認証された各ユーザアカウントにパスワードが必要です。admin権限またはAAA権限を持つユーザは、ユーザ パスワードのパスワード強度チェックを実行するようにシステムを設定できます。パスワード強度チェックをイネーブルにすると、各ユーザが強力なパスワードを使用する必要があります。

各ユーザが強力なパスワードを設定することを推奨します。ローカル認証ユーザのパスワード強度チェックを有効にすると、FXOS は次の要件を満たしていないパスワードを拒否します。

- 8 ～ 80 文字を含む。

（注） コモン クライテリア要件に準拠するために、オプションでシステムの最小文字数 15 文字の長さのパスワードを設定できます。詳細については、ユーザ設定値の設定, （46 ページ）を参照してください。

- アルファベットの大文字を少なくとも 1 文字含む。
- アルファベットの小文字を少なくとも 1 文字含む。
- 英数字以外の文字（特殊文字）を少なくとも 1 文字含む。
- aaabbb など連続して 3 回を超えて繰り返す文字を含まない。
- passwordABC や password321 などの 3 つの連続した数字や文字をどのような順序であっても含まない。
- ユーザ名と同一、またはユーザ名を逆にしたものではない。
- パスワード ディクショナリ チェックに合格する。たとえば、パスワードには辞書に記載されている標準的な単語に基づいたものを指定することはできません。
- 次の記号を含まない。$（ドル記号）、?（疑問符）、=（等号）。
- ローカル ユーザ アカウントおよび admin アカウントの場合は空白にしない。

ユーザの追加

Firepower Chassis Manager および FXOS CLI アクセスのローカル ユーザを追加します。

手順

ステップ 1 [System] > [User Management] を選択します。

ステップ 2 [Local Users] タブをクリックします。

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。

名前	説明
[User Name] フィールド	このアカウントにログインするときに使用されるアカウント名。この名前は、固有であり、ユーザアカウント名のガイドラインと制限を満たしている必要があります（ユーザアカウントに関するガイドライン，（43 ページ）を参照）。 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。
[First Name] フィールド	ユーザの名。このフィールドには、32 文字までの値を入力できます。
[Last Name] フィールド	ユーザの姓。このフィールドには、32 文字までの値を入力できます。
[Email] フィールド	ユーザの電子メール アドレス。
[Phone Number] フィールド	ユーザの電話番号。
[Password] フィールド	このアカウントに関連付けられているパスワード。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（ユーザアカウントに関するガイドライン，（43 ページ）を参照）。
[Confirm Password] フィールド	確認のためのパスワードの再入力。
[Account Status] フィールド	ステータスが [Active] に設定されている場合、ユーザはこのログイン ID とパスワードを使用して Firepower Chassis Manager および FXOS CLI にログインできます。

名前	説明
[User Role] リスト	ユーザアカウントに割り当てる権限を表すロール（ユーザ ロール，（43 ページ）を参照）。 すべてのユーザはデフォルトでは読み取り専用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。複数のロールを割り当てるには、Ctrl を押したまま、目的のロールをクリックします。 （注） ユーザ ロールおよび権限の変更は次回のユーザ ログイン時に有効になります。ユーザ アカウントへの新しいロールの割り当てや既存のロールの削除を行うときにユーザがログインしている場合、アクティブなセッションは以前のロールや権限を引き続き使用します。
[Account Expires] チェックボックス	オンにすると、このアカウントは [Expiration Date] フィールドで指定した日付に期限切れになり、それ以降は使用できなくなります。 （注） ユーザ アカウントに有効期限日付を設定した後は、アカウントの有効期限をなくすよう再設定できません。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。
[Expiry Date] フィールド	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。

ステップ 6 ユーザを非アクティブ化するには、次の手順を実行します。

a) 非アクティブ化するユーザについて、[Edit]（鉛筆アイコン）をクリックします。
admin ユーザ アカウントは常にアクティブに設定されます。変更はできません。

b) [Account Status] フィールドで [Inactive] オプション ボタンをクリックします。

c) [Save（保存）] をクリックします。

ユーザ設定値の設定

すべてのユーザのグローバル設定値を設定できます。

手順

ステップ 1 [System] > [User Management] を選択します。

ステップ 2 [Settings] タブをクリックします。

ステップ 3 次のフィールドに必要な情報を入力します。

名前	説明
[Default Authentication] フィールド	リモート ログイン中にユーザが認証されるデフォルトの方法。次のいずれかになります。 • [Local]：ユーザ アカウントは、Firepower シャーシでローカルに定義する必要があります。 • [None]：ユーザ アカウントが Firepower シャーシに対してローカルである場合は、ユーザがリモート ログインするときにパスワードは必要ありません。
ローカル ユーザ設定	
[Password Strength Check] チェックボックス	オンにすると、すべてのローカル ユーザ パスワードは、強力なパスワードのガイドラインに準拠しなければならなくなります（ユーザ アカウントに関するガイドライン，（43 ページ）を参照）。
[History Count] フィールド	自分が以前に使用したパスワードを再使用する前にユーザが作成する必要がある、一意のパスワードの数。履歴カウントは、最も新しいパスワードを先頭に時系列とは逆の順番で表示され、履歴カウントのしきい値に到達すると、最も古いパスワードのみが使用可能になります。 この値は、0 ～ 15 から自由に設定できます。 [History Count] フィールドを 0 に設定して履歴カウントをディセーブルにすると、ユーザは以前のパスワードをいつでも再使用できます。
[Change During Interval] フィールド	ローカル認証されたユーザがパスワードを変更できるタイミングを制御します。ここに表示される値は次のとおりです。 • [Enable]：ローカル認証されたユーザは、[Change Interval] および [Change Count] の設定に基づいて、パスワードを変更できます。 • [Disable]：ローカル認証されたユーザは、[No Change Interval] に指定された期間はパスワードを変更できません。

名前	説明
[Change Interval] フィールド	[Change Count] フィールドで指定したパスワード変更回数が適用される時間数。 この値は、1 ～ 745 時間から自由に設定できます。 たとえば、このフィールドが 48 に設定され、[Change Count] フィールドが2に設定されている場合、ローカル認証されたユーザは48時間以内に2回を超えるパスワード変更を実行することはできません。
[Change Count] フィールド	ローカル認証されたユーザが、[Change Interval] の間に自分のパスワードを変更できる最大回数。 この値は、0 ～ 10 から自由に設定できます。
[No Change Interval] フィールド	ローカル認証されたユーザが、新しく作成したパスワードを変更する前に待機する最小時間数。 この値は、1 ～ 745 時間から自由に設定できます。 この間隔は、[Change During Interval] プロパティが [Disable] に設定されていない場合、無視されます。

ステップ 4 [Save（保存）] をクリックします。