Cisco FirePOWER Threat Defense for the Firepower 9300 クイック スタート ガイド

初版:2016 年 3 月 10 日

最終更新日:2018 年 3 月 9 日

1. Firepower Threat Defense セキュリティ サービスについて

Cisco Firepower 9300 セキュリティ アプライアンスは、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。このアプライアンスのモジュール型スタンドアロン シャーシは、複数のセキュリティ サービスの同時実行を可能にする、高性能かつ柔軟な I/O オプションを備えています。Firepower 9300 セキュリティ アプライアンスは、Firepower Threat Defense を実行する、最大 3 つのセキュリティ モジュールを装着できます。

Firepower Threat Defense は、ステートフル ファイアウォール、ルーティング、Next-Generation Intrusion Prevention System(NGIPS)、Application Visibility and Control(AVC)、URL フィルタリング、および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。シングル コンテキスト モードとルーテッドまたはトランスペアレント モードで脅威防御デバイスを使用できます。

Firepower Threat Defense と Firepower 9300 の連携

Firepower 9300 セキュリティ アプライアンスは、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。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 Web インターフェイスまたは CLI 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、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できます。

すべての物理インターフェイスの動作は、外部 EtherChannel の設定を含め、スーパバイザによって所有されます。インターフェイスは、Firepower Threat Defense を実行している論理デバイスに割り当てられます。データ、管理、および Firepower イベントの 3 タイプのインターフェイスがサポートされています。管理インターフェイスのみ、モジュール間で共有できます。Firepower イベント インターフェイスはイベント トラフィックの搬送専用です。導入時に、または必要に応じて後から、Firepower Threat Defense 搭載の Firepower 9300 にインターフェイスを割り当てることができます。これらのインターフェイスは、Firepower Threat Defense 搭載の Firepower 9300 設定と同じ ID をスーパバイザで使用します。

Firepower Threat Defense 搭載の Firepower 9300 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。Firepower Threat Defense 搭載の Firepower 9300 は、スタンドアロンの論理デバイス、または Firepower Threat Defense モジュールのクラスタとして展開できます。クラスタリングを使用する場合は、シャーシのすべてのモジュールがクラスタに属している必要があります。シャーシ内クラスタリングのみサポートされます。

Firepower 9300 ハードウェアでは Cisco Firepower Threat Defense ソフトウェアまたは ASA ソフトウェアを実行できます。このガイドでは、Firepower 9300 での Firepower Threat Defense の使用方法について説明します。

注意:シャーシ内のすべてのモジュールに Firepower Threat Defense ソフトウェアをインストールする必要があります。同じシャーシ上での Firepower Threat Defense ソフトウェアと ASA ソフトウェアの混在はサポートされていない構成であり、予期しない結果を招く可能性があります。モジュールではさまざまなバージョンの Firepower Threat Defense アプリケーションを実行できますが、すべてのモジュールで Firepower Threat Defense を実行する必要があることに注意してください。

Firepower Management Center のサポートと CLI アクセス

Firepower Threat Defense 搭載の Firepower 9300 の導入時に、管理インターフェイスと Firepower Management Center を管理するための登録情報を指定し、Firepower Management Center アクセスを許可できます。Firepower Threat Defense デバイスを管理対象デバイスとして登録し、ポリシーを設定および導入できます。Firepower Management Center には、Firepower Threat Defense 搭載の Firepower 9300 セキュリティ アプライアンスを他の Firepower Threat Defense プラットフォームと差別化するカスタマイズされた機能がいくつかあります。

内部 Telnet 接続を使用して、Firepower 9300 スーパーバイザ CLI から Firepower Threat Defense CLI にアクセスすることもできます。後から、Firepower 9300 セキュリティ アプライアンス内で、管理インターフェイスまたはデータ インターフェイスのいずれかを介した SSH アクセスまたは Telnet アクセスを設定できます。

管理/診断インターフェイスとネットワーク配置

物理的な管理インターフェイスは、管理論理インターフェイスと診断論理インターフェイスの間で共有されます。

Firepower Threat Defense デバイスは、セットアップ IP アドレスを使用して、Firepower Management Center による管理用にルートをゲートウェイに関連付けます。管理 IP アドレスとルートは、インターフェイス リストの Firepower Management Center Web インターフェイスまたはデバイスのスタティック ルートに含まれて**いません**。セットアップ スクリプトおよび CLI によってのみ設定できます。初期設定を実行した後、Firepower Management Center を使用してセキュリティおよびアクセス ポリシー、デバイス設定、およびインターフェイスを設定します。

物理管理ポートを介した syslog または SNMP レポートを選択する場合、Firepower Management Center Web インターフェイスを使用して診断 0/0 または診断 1/1 インターフェイス用に別々の IP アドレスとルート、および外部認証を設定する必要があります。ただし、導入を簡素化するために、レポート用にデータ ポートを使用することをお勧めします。

管理/診断インターフェイスの詳細については、『Firepower Management Center *コンフィギュレーション ガイド*』の Firepower Threat Defense インターフェイスに関する章を参照してください。

Firepower Threat Defense のライセンス要件

Firepower 9300 で Firepower Threat Defense を実行するには、スマート ソフトウェア ライセンシングが必要です。シャーシ内のセキュリティ モジュール上の Firepower Threat Defense インスタンスにはそれぞれライセンスが必要です。Firepower Management Center からセキュリティ サービスのすべてのライセンス資格を設定します。

Firepower Threat Defense デバイスを購入すると、自動的に基本ライセンスが付いてきます。すべての追加ライセンス（Threat、Malware、URL Filtering）はオプションです。基本ライセンスは、登録するすべての Firepower Threat Defense デバイスの Firepower Management Center に追加されます。

- Firepower System システムで使用できる機能ライセンスの概要については、「Cisco Firepower System Feature Licenses」を参照してください。
- Firepower Management Center でライセンスを管理する方法の詳細については、『*Firepower Management Center Configuration Guide*』の「Licensing the Firepower System」を参照してください。
- FXOS シャーシでのライセンス管理の一般的な情報については、『*Cisco FXOS Firepower Chassis Manager Configuration Guide*』の「License Management」を参照してください。

Firepower Chassis Manager Web インターフェイスへのアクセス

Firepower Chassis Manager Web インターフェイスを使用して、スーパバイザ上で、アプリケーション イメージの管理、ハードウェア インターフェイスの設定、その他の基本的なオペレーティング パラメータの設定を実行できます。

手順

1. Firepower Chassis Manager Web インターフェイスにログインするには、次の手順に従います。
   a. サポートされているブラウザを使用し、アドレス バーに次の URL を入力します。

   `https://<chassis_mgmt_ip_address>`

   <chassis_mgmt_ip_address> は、初期設定時に入力した Firepower 9300 の IP アドレスまたはホスト名です。詳細については、Firepower Management の設定（4 ページ）を参照してください。

   b. ユーザ名とパスワードを入力します。

   c. [ログイン（Login）] をクリックします。

   ログインすると、Firepower Chassis Manager Web インターフェイスが開かれ、[概要（Overview）] ページが表示されます。
2. Firepower Chassis Manager Web インターフェイスをログアウトするには、[管理（admin）] > [ログアウト（Logout）] を選択します。Firepower Chassis Manager Web からログアウトすると、ログイン画面に戻ります。

2. Firepower Threat Defense のインストール

Firepower 9300 は、プラットフォーム バンドルとアプリケーションの 2 つの基本タイプのイメージを使用します。プラットフォーム バンドルには、スーパバイザに必要な Firepower FXOS ソフトウェア パッケージが含まれています。アプリケーション イメージは、セキュリティ エンジンに導入するソフトウェア イメージです。

Firepower Threat Defense はアプリケーション イメージとして Firepower 9300 のセキュリティ エンジンに導入されます。アプリケーション イメージは、Cisco Secure Package ファイル（CSP）として提供されます。これは、論理デバイス作成時にセキュリティ モジュールに導入されるまで（または以降の論理デバイス作成に備えて）スーパバイザに保存されます。同じアプリケーション イメージ タイプの複数の異なるバージョンをスーパバイザに保存できます。

[システム（System）] メニューの [更新（Updates）] ページから FXOS プラットフォーム バンドルをダウンロードできます。また、Firepower Threat Defense アプリケーション イメージと最新の更新プログラムは Cisco.com からダウンロードできます。次に、論理デバイスの作成または更新時に使用される Firepower Threat Defense イメージを Firepower 9300 にアップロードします。必ず、スーパバイザで稼働する FXOS バージョンと互換性のある Firepower Threat Defense イメージ バージョンを使用してください。詳細については、『*Cisco FXOS Firepower Chassis Manager コンフィギュレーション ガイド*』を参照してください。

作業の概要

Firepower 9300 セキュリティ アプライアンスへの Firepower Threat Defense のインストールを開始する前に、次のガイドラインと要件を確認してください。

Firepower Threat Defense の新規インストール

初回インストールの場合は、以下を実行します。

- Firepower Management の設定（4 ページ）の説明に従って、初期設定ウィザードで Firepower 9300 にネットワーク接続を設定します。
- Firepower Chassis Manager Web インターフェイスへのアクセス（3 ページ）の説明に従って、Firepower Chassis Manager にログインします。

- Cisco.com からのソフトウェア イメージのダウンロード(5 ページ)の説明に従って、必要な FXOS ソフトウェア パッケージと Firepower Threat Defense アプリケーション イメージを取得します。
- Firepower FXOS スーパバイザ プラットフォームのアップグレード(7 ページ)の説明に従って、スーパーバイザ ソフトウェア バンドルをアップグレードします。
- 3. Firepower Threat Defense の導入(7 ページ)の説明に従って、スタンドアロンまたはクラスタ化モードで Firepower Threat Defense アプリケーション イメージを導入します。
- 5. Firepower Management Center への登録(11 ページ)の説明に従って、Firepower Management Center 内の Firepower Threat Defense ユニットを検出します。

Firepower Threat Defense へのアップグレード

Firepower Threat Defense アップグレードの場合は、以下を実行します。

- Firepower Chassis Manager Web インターフェイスへのアクセス(3 ページ)の説明に従って、Firepower Chassis Manager にログインします。
- Cisco.com からのソフトウェア イメージのダウンロード(5 ページ)の説明に従って、必要な FXOS ソフトウェア パッケージと Firepower Threat Defense アプリケーション イメージを取得します。
- 既存の論理デバイスおよびアプリケーション設定の削除(6 ページ)の説明に従って、すべての既存の論理デバイスと設定(該当する場合)を削除します。
- Firepower FXOS スーパバイザ プラットフォームのアップグレード(7 ページ)の説明に従って、スーパーバイザ ソフトウェア バンドルをアップグレードします。
- 3. Firepower Threat Defense の導入(7 ページ)の説明に従って、スタンドアロンまたはクラスタ化モードで Firepower Threat Defense アプリケーション イメージを導入します。
- 5. Firepower Management Center への登録(11 ページ)の説明に従って、Firepower Management Center 内の Firepower Threat Defense ユニットを検出します。

Firepower Management の設定

(注) この手順は、初めて Firepower 9300 を起動する場合にのみ必要です。

最初に CLI にアクセスするときに、セットアップ ウィザードによって、Firepower Threat Defense の設定に必要な基本のネットワーク設定パラメータのプロンプトが表示され、Firepower Management Center への登録が要求されます。

手順

1. たとえば、コンソール ポートから、または SSH を使用して Firepower 9300 CLI に接続します。
2. ユーザ名 **admin** およびパスワード **cisco123** を使用してログインします。
3. プロンプトに従ってシステム設定を行います。

   次に例を示します。

```
Enter the setup mode; setup newly or restore from backup.(setup/restore) ? setup
You have chosen to setup a new Security Appliance.「続行しますか?」というメッセージを示すダイアログボックスが開きます。(y/n): y
Enforce strong password? (y/n): n
Enter the password for "admin": <new password>
Confirm the password for "admin": <repeat password>
Enter the system name: FTD-SSP-3RU
Physical Switch Mgmt0 IP address : 10.127.56.61
Physical Switch Mgmt0 IPv4 netmask : 255.255.255.0
IPv4 address of default gateway : 10.127.56.1
```

```
Configure the DNS Server IP address? (yes/no) [n]: n
Configure the default domain name? (yes/no) [n]: n

Following configurations will be applied:
   Switch Fabic=A
   System Name=FTD-SSP-3RU
   Enforced Strong Password=no
   Physical Switch Mgmt0 IP Address=10.127.56.61
   Physical Switch Mgmt0 IP Netmask=255.255.255.0
   Default Gateway=10.127.56.1
   Ipv6 value=0

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

4. Firepower Chassis Manager Web インターフェイスを起動して、新しいログイン クレデンシャルを使用して接続を確認します。

   a. サポートされているブラウザを使用し、アドレス バーに次の URL を入力します。

   `https://<chassis_mgmt_ip_address>`

   <chassis_mgmt_ip_address> は、初期設定時に入力した Firepower 9300 の IP アドレスまたはホスト名です。

   b. ユーザ名とパスワードを入力します。

   c. [ログイン(Login)] をクリックします。

   ログインすると、Firepower Chassis Manager Web インターフェイスが開かれ、[概要(Overview)] ページが表示されます。

Cisco.com からのソフトウェア イメージのダウンロード

はじめる前に

- Cisco.com アカウントが必要です。
- 設定に必要な互換性のあるプラットフォーム バンドルおよび Firepower Threat Defense アプリケーション イメージのバージョンを熟知している必要があります。
  - FXOS プラットフォーム バンドルは、fxos-k9.xx1.2.xxx.SPA(バージョン 1.2 以上)であることが必要です。
  - Firepower Threat Defense アプリケーション イメージは、cisco-ftd.6.0.0.xxx.SPA.csp(6.0.0 以上)であることが必要です。
- インターネット アクセスが必要です。

手順

1. [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、シャーシで使用可能な Firepower 9300 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。
2. ページ下部の [最新の更新を CCO からダウンロード(Download latest updates from CCO)] リンクをクリックします。ブラウザの新しいタブで、Firepower 9300 のソフトウェア ダウンロード ページが開きます。
3. 該当するソフトウェア イメージを見つけて、ローカル コンピュータにダウンロードします。

   a. 必要な FXOS プラットフォーム バンドルは、fxos-k9.xx1.2.xxx.SPA(バージョン 1.2 以上)です。

   b. 必要な Firepower Threat Defense アプリケーション イメージは cisco-ftd.6.0.0.xxx.SPA.csp(バージョン 6.0.0 以上)です。

Firepower 9300 へのソフトウェア イメージのアップロード

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

1. [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、シャーシで使用可能な Firepower 9300 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。
2. [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。
3. [参照(Browse)] をクリックして、アップロードするイメージに移動して選択します。
   a. 必要な FXOS プラットフォーム バンドルは、fxos-k9.xx1.2.xxx.SPA(バージョン 1.2 以上)です。
   b. 必要な Firepower Threat Defense アプリケーション イメージは cisco-ftd.6.0.0.xxx.SPA.csp(バージョン 6.0.0 以上)です。
4. [アップロード(Upload)] をクリックします。選択したイメージが Firepower 9300 にアップロードされます。

次の作業

- システム プロンプトに従って、エンドユーザ ライセンス契約書に同意し、続行します。

既存の論理デバイスおよびアプリケーション設定の削除

セキュリティ モジュールにスタンドアロン論理デバイスを作成していた場合は、Firepower Threat Defense をインストールする前に、それらのデバイスを削除し、すべてのアプリケーション設定も削除する必要があります。

(注) これは、すでに設定および導入されている Firepower 9300 セキュリティ アプライアンスにも当てはまります。新しい Firepower 9300 セキュリティ アプライアンスへの Firepower Threat Defense の初回インストールの場合存在する論理デバイスや設定はありません。

手順

1. [論理デバイス(Logical Devices)] を選択して、[論理デバイス(Logical Devices)] ページを開きます。

   [論理デバイス(Logical Devices)] ページに、シャーシに設定されている論理デバイスのリストが表示されます。論理デバイスが設定されていない場合は、これを通知するメッセージが代わりに表示されます。
2. 各論理デバイスに関連付けられている [削除(Delete)] アイコンをクリックします。
3. 論理デバイスを削除することの確認が求められたら、[はい(Yes)] をクリックします。
4. アプリケーション設定を削除することの確認が求められたら、[はい(Yes)] をクリックします。この最後の手順は、Firepower Threat Defense を正常にインストールするために必須です。

次の作業

- セキュリティ モジュール上で稼働する Firepower Threat Defense をサポートするためにアップグレードする必要があるかどうかを判断するには、シャーシで稼働している Firepower FXOS ソフトウェアの実行バージョンを確認します。

Firepower FXOS スーパバイザ プラットフォームのアップグレード

シャーシで稼働している Firepower eXtensible Operating System（FXOS）の現在のバージョンがセキュリティ モジュールで Firepower Threat Defense の実行をサポートするために十分であるかどうかを判断する必要があります。FXOS の実行バージョンは、Firepower Chassis Manager Web インターフェイスの [概要（Overview）] ページの上部に表示されます。[システム（System）] メニューの [更新（Updates）] ページから FXOS プラットフォーム バンドルをアップグレードします。

（注）FXOS スーパーバイザ イメージ バンドルがバージョン 1.2 以上を示し、fxos-k9.xx.1.2.xxx.SPA のようなファイル名を使用している場合は、このセクションをスキップし、3. Firepower Threat Defense の導入（7 ページ）に移動できます。

はじめる前に

- Firepower Chassis Manager Web インターフェイスへのアクセス（3 ページ）の説明に従って、Firepower Chassis Manager にログインします。

手順

1. [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、シャーシで使用可能な Firepower 9300 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。
2. [イメージ名（Image Name）] 列を参照して、ロードする必要がある FXOS プラットフォーム バンドルを見つけます。
3. ロードする必要がある FXOS プラットフォーム バンドルに関連付けられているアップロード/ダウンロード アイコンをクリックします。
4. 選択したバージョンの [バンドル イメージの更新（Update Bundle Image）] ダイアログで [はい（Yes）] をクリックします。[はい（Yes）] をクリックすると、選択したバージョンがインストールされ、デバイスが再起動します。

次の作業

- Firepower 9300 プラットフォームに Firepower Threat Defense を導入します。

3. Firepower Threat Defense の導入

Firepower Chassis Manager を使用して、Firepower 9300 で Firepower Threat Defense が 稼働しているセキュリティ モジュールまたはセキュリティ モジュールのクラスタにスタンドアロンの Firepower Threat Defense を導入できます。

NTP の設定

Firepower 9300 に Firepower Threat Defense を導入するには、Firepower Chassis Manager で NTP を設定する必要があります。スマート ライセンスを正しく機能させ、デバイス登録の適切なタイムスタンプを確保するには、Firepower Chassis Manager で NTP サーバが設定されている必要があります。

手順

1. [プラットフォーム設定（Platform Settings）] > [NTP] を選択します。
2. [タイムゾーン（Time Zone）] ドロップダウン リストから、Firepower シャーシの適切なタイム ゾーンを選択します。

3. [時刻設定の取得元(Set Time Source)] で [NTPサーバの使用(Use NTP Server)] をクリックし、使用する NTP サーバの IP アドレスまたはホスト名を [NTPサーバ(NTP Server)] フィールドに入力します。
4. [保存(Save)] をクリックします。

   指定した NTP サーバが Firepower シャーシに設定されます。

   (注) システム時刻を 10 分以上変更すると、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。

インターフェイスの設定

スーパバイザで、Firepower 9300 Firepower Threat Defense 用の導入設定に組み込むことのできる管理タイプのインターフェイスを設定します。また、少なくとも 1 つのデータ型インターフェイスを設定する必要があります。

手順

1. [インターフェイス(Interfaces)] を選択して、[インターフェイス(Interfaces)] ページを開きます。
2. EtherChannel を追加するには、次の手順を実行します。
   a. [ポートチャネルの追加(Add Port Channel)] をクリックします。
   b. [ポートチャネル ID(Port Channel ID)] に、1 ～ 47 の値を入力します。

   (注) ポート チャネル 48 はクラスタリングに使用されます。インターフェイスの設定中は、このポートを使用しないことを強くお勧めします。

   c. [有効(Enable)] はオンのままにします。
   d. [タイプ(Type)] で、[管理(Management)]、[データ(Data)]、または [Firepowerイベント(Firepower Eventing)] を選択します。各論理デバイスには、管理インターフェイスを 1 つだけ含めることができます。[クラスタ(Cluster)] は選択しないでください。

   (注) インターフェイス タイプは、プロビジョニングされた論理デバイスに割り当てられた後は変更できません。

   e. 必要に応じて、メンバー インターフェイスを追加します。
   f. [OK] をクリックします。
3. 単一インターフェイスの場合:
   a. インターフェイス行で [編集(Edit)] アイコンをクリックして、[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。
   b. [有効(Enable)] をオンにします。
   c. [タイプ(Type)] で、[管理(Management)]、[データ(Data)]、または [Firepowerイベント(Firepower Eventing)] をクリックします。各論理デバイスには、管理インターフェイスを 1 つだけ含めることができます。
   d. [OK] をクリックします。

スタンドアロンまたはクラスタとしての Firepower Threat Defense の導入

Firepower Threat Defense は、スタンドアロンの論理デバイス、または Firepower Threat Defense モジュールのクラスタとして設定できます。クラスタリングを使用する場合は、シャーシのすべてのセキュリティ モジュールがクラスタに属している必要があります。次の論理デバイス情報を設定します。

- スタンドアロンまたはクラスタ モードのデバイス情報とアドレッシング
- Firepower Management Center 登録情報、ファイアウォール モード、およびイベントを含むデバイス設定
- 各セキュリティ モジュールのインターフェイス情報とアドレッシング
- エンド ユーザ ライセンス契約書Firepower Threat Defense

手順

1. [論理デバイス(Logical Devices)] を選択して、[論理デバイス(Logical Devices)] ページを開きます。
2. [デバイスの追加(Add Device)] をクリックし、[デバイスの追加(Add Device)] ダイアログボックスを表示します。
3. [デバイス名(Device Name)] に、論理デバイスの名前を指定します。この名前は、Firepower 9300 スーパバイザがクラスタリング設定と管理設定を行ってインターフェイスを割り当てるために使用します。これはセキュリティ モジュール設定で使用されるクラスタまたはデバイスの名前ではありません。
4. [テンプレート(Template)] では、[Cisco Firepower Threat Defense] を選択します。
5. [イメージバージョン(Image Version)] では、Firepower Threat Defense ソフトウェア バージョンを選択します。
6. [デバイスモード(Device Mode)] で、[スタンドアロン(Standalone)] または [クラスタ(Cluster)] オプション ボタンをクリックします。
7. [OK] をクリックします。[プロビジョニング-デバイス名(Provisioning - device name)] ウィンドウが表示されます。
8. [データポート(Data Ports)] 領域を展開し、Firepower Threat Defense に割り当てるインターフェイスをそれぞれクリックします。クラスタの場合、デフォルトではすべてのインターフェイスがクラスタに割り当てられます。
9. 画面中央のデバイス アイコンをクリックします。[設定(Configuration)] ダイアログボックスが表示されます。
10. 設定ダイアログボックスの各タブで導入オプションを設定します。
    a. [論理デバイス情報(スタンドアロンまたはクラスタ)(Logical Device Information (standalone or cluste)]: この論理デバイスの管理設定を入力します。

    (注) 仮想 IPv4 または IPv6 アドレスは、デバイスの登録後に Firepower Management Center から設定できます。これは、syslog を使用する場合に重要です。

    b. [設定(Settings)]: Firepower Management Center を管理するための登録キー、パスワードおよび IP アドレスを入力します。また、ファイアウォール モード、Firepower イベント インターフェイス(設定されている場合)、および DNS 情報を選択します。

    c. [インターフェイス情報(Interface Information)]: この論理デバイスの管理設定を入力します。

    (注) 各セキュリティ モジュールには専用の IP アドレスが必要です。これは、Firepower Management Center がデバイスを登録するときに使用します。この IP はモジュールを Firepower Management Center に追加するために必須です。

    d. [契約(Agreement)]: エンド ユーザ ライセンス契約書(EULA)を確認し、同意します。

11. [OK] をクリックして、設定ダイアログボックスを閉じます。
12. [保存(Save)] をクリックします。Firepower 9300 スーパバイザは、指定されたソフトウェア バージョンをダウンロードし、指定されたセキュリティ モジュールにブートストラップ コンフィギュレーションと管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。

4. Firepower Threat Defense CLI へのアクセス

初期設定またはトラブルシューティングを行う場合は、Firepower 9300 FXOS スーパバイザ CLI から Firepower Threat Defense CLI にアクセスします。

手順

1. たとえば、コンソール ポートから、または SSH を使用して、スーパバイザ CLI に接続します。
2. セキュリティ モジュールのいずれかに接続します。

   connect module *slot* **console**

   例:

   ```
   cisco-ssp-A# connect module 1 console
   firepower>
   ```

   Firepower Threat Defense クラスタの場合は、設定作業のためにマスター ユニットにアクセスする必要があります。通常、マスター ユニットはスロット 1 にあるため、そのモジュールに接続してどのユニットがマスターであるか確認する必要があります。
3. モジュールへの初回接続時には、Firepower Chassis Manager モジュール CLI に切り替えます(firepower プロンプトで)。その後 Firepower Threat Defense CLI に接続する必要があります。

   connect ftd

   例:

   ```
   firepower> connect ftd
   >
   ```

   後続の接続では Firepower Threat Defense CLI に直接接続されます。
4. Firepower Threat Defense 接続を終了するには、**exit** を入力します。

   例:

   ```
   > exit
   firepower>
   ```
5. システム診断にアクセスするには、**system support diagnostic-cli** を入力します。

   例:

   ```
   firepower> system support diagnostic-cli
   ```
6. コンソール接続を終了するために「**~**」と入力します。Telnet アプリケーションに切り替わります。「**quit**」と入力してスーパバイザ CLI を終了します。

   例:

   ```
   firepower> ~
   telnet> quit
   cisco-ssp-A#
   ```

5. Firepower Management Center への登録

各セキュリティ モジュールを個別に Firepower Management Center に登録します。Management Center にデバイスを登録する前に、Firepower Chassis Manager でネットワーク設定が正しく設定されていることを確認する必要があります。この確認は、一般にインストール プロセスの一環として行われます。

デバイス クラスタを登録するときに、ライセンスを選択することはできますが、それらのライセンスをデバイスの登録時に適用することはできません。これは、ライセンスの不一致による劣化を回避するために、クラスタに適切なライセンスを実行させるための措置です。登録の完了後に、[デバイス管理(Device Management)] ページの一般プロパティでライセンスを評価できます。

はじめる前に

- 登録予定の各セキュリティ モジュールまたはクラスタに関して、Firepower Chassis Manager から設定を確認します。
- Firepower 9300 で稼働している Firepower Threat Defense にはスマート ソフトウェア ライセンシングが必要です。これは Firepower Management Center から設定できます。

手順

1. ブラウザで HTTPS 接続を使用し、設定した Firepower Management Center のホスト名またはアドレスを使用して Firepower Management Center にログインします。たとえば、https://MC.example.com などです。
2. Management Center の Web インターフェイスで、[デバイス(Devices)] > [デバイス管理(Device Management)] を選択します。
3. [追加(Add)] ドロップダウン メニューから、[デバイスの追加(Add Device)] を選択します。

   (注) 各セキュリティ モジュールを個別に追加する必要があることに注意してください。クラスタを追加するときに、各セキュリティ モジュールを個別に追加し、[追加(Add)] > [クラスタの追加(Add Cluster)] を選択して、プライマリ モジュールとセカンダリ モジュールを識別します。
4. [ホスト(Host)] フィールドに、追加するセキュリティ モジュールの IP アドレスを入力します。
5. [表示名(Display Name)] フィールドに、Management Center でのセキュリティ モジュールの表示名を入力します。
6. [登録キー(Registration Key)] フィールドに、Firepower Chassis Manager でセキュリティ モジュールを設定したときに使用したものと同じ登録キーを入力します。
7. マルチドメイン環境でデバイスを追加している場合は、[ドメイン(Domain)] ドロップダウン リストから値を選択することにより、デバイスをリーフ ドメインに割り当てます。
8. [アクセスコントロールポリシー(Access Control Policy)] ドロップダウン リストから、セキュリティ モジュールに導入する初期ポリシーを選択します。
   - [デフォルトアクセスコントロール(Default Access Control)] ポリシーは、すべてのトラフィックをネットワークからブロックします。
   - [デフォルト侵入防御(Default Intrusion Prevention)] ポリシーは、Balanced Security and Connectivity 侵入ポリシーにも合格したすべてのトラフィックを許可します。
   - [デフォルトネットワーク検出(Default Network Discovery)] ポリシーは、すべてのトラフィックを許可し、ネットワーク検出のみでトラフィックを検査します。
   - 既存のユーザ定義アクセス コントロール ポリシーを選択することもできます。詳細については、『*Firepower Management Center Configuration Guide*』の「Managing Access Control Policies」を参照してください。
9. デバイスに適用するライセンスを選択します。次の点に注意してください。
   - コントロール、マルウェア、URL フィルタリングライセンスには、保護ライセンスが必要です。
10. [登録(Register)] をクリックし、デバイスが正常に登録されたことを確認します。

6. ポリシーとデバイス設定の設定

Firepower Threat Defense をインストールして、デバイスを Management Center に追加した後、Firepower Management Center ユーザ インターフェイスを使用して、Firepower 9300 上で実行する Firepower Threat Defense のデバイス管理設定の構成や、アクセス コントロール ポリシーおよび Firepower Threat Defense セキュリティ モジュールを使用してトラフィックを管理するその他の関連ポリシーの設定と適用を行うことができます。

セキュリティ ポリシーは、Next Generation IPS のフィルタリングやアプリケーションのフィルタリングなど、Firepower Threat Defense で提供されるサービスを制御します。Firepower Management Center を使用して、Firepower Threat Defense 上でセキュリティ ポリシーを設定します。セキュリティ ポリシーの設定方法の詳細については、『*Cisco Firepower Configuration Guide*』、または Firepower Management Center のオンライン ヘルプを参照してください。

7. 次の作業

- Firepower 9300 ドキュメンテーションには、すべての Firepower 9300 ドキュメンテーションへのリンクが記載されています。