Cisco FirePOWER Threat Defensefor Firepower 4100 クイック スタート ガイド

初版:2016 年 3 月 10 日

最終更新日:2017 年 3 月 13 日

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

Cisco Firepower 4100セキュリティ アプライアンスは、Firepower Threat Defense アプリケーションを実行できるネットワークおよびコンテンツ セキュリティ ソリューション向けのスタンドアロン セキュリティ サービス プラットフォームです。

Firepower Threat Defenseを使用してデータセンターに Firepower 4100 を導入し、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 4100で Firepower Threat Defense が動作する仕組み

Firepower 4100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 ベースの管理機能が利用できます。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。Firepower Threat Defenseを実行している論理デバイスにインターフェイスを割り当てられます。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。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 4100 にインターフェイスを割り当てられます。これらのインターフェイスは、Firepower Threat Defense 搭載の Firepower 4100 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 4100 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。スタンドアロン論理デバイスとしてのみ Firepower Threat Defense搭載の Firepower 4100 を導入できますが、クラスタリングはサポートされません。

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

Firepower Threat Defense搭載の Firepower 4100 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。

内部 Telnet 接続を使用して、Firepower 4100スーパバイザ 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 4100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。「6.Firepower Threat DefenseCLI へのアクセス(10 ページ)」を参照してください。

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 CenterWeb 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 レポートを実行する場合は、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 4100で稼働している Firepower Threat Defense にはスマート ソフトウェア ライセンスが必要です。これはFirepower Management Center から設定できます。詳細については、『*Firepower Management Center コンフィギュレーション ガイド*』または Firepower Management Center のオンライン ヘルプを参照してください。

Firepower 4100セキュリティ モジュール上で稼働する Firepower Threat Defense の場合、スマート ソフトウェア ライセンス設定は Firepower 4100 スーパバイザとセキュリティ モジュールの間で分割されます。

- Firepower 4100：License Authority との通信に使用するパラメータなど、スーパバイザのすべてのスマート ソフトウェア ライセンス インフラストラクチャを設定します。Firepower 4100自体の動作にライセンスは必要ありません。
- Firepower Threat Defense：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 4100シャーシはデバイスとして登録されますが、シャーシ内のセキュリティ モジュール上のFirepower Threat Defense には専用のライセンスが要求されます。Firepower 4100のライセンス管理の詳細については、『*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。

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。

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て、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 4100 の IP アドレスまたはホスト名です。詳細については、「初期設定(3 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. [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の導入

Firepower 4100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 4100 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 4100 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 4100セキュリティ アプライアンスへの Firepower Threat Defense の導入を開始する前に、次のガイドラインと要件を確認してください。

- 初期設定(3 ページ)の説明に従って、初期設定ウィザードを使用して Firepower 4100 セキュリティ アプライアンスの初期設定を行います。
- NTP の設定(5 ページ)の説明に従って、Firepower Chassis Manager に NTP を設定します。
- インターフェイスの設定(5 ページ)の説明に従って、管理インターフェイスと少なくとも 1 つのデータ インターフェイスを設定します。
- Firepower Threat Defense論理デバイスの導入(6 ページ)の説明に従って、Firepower Threat Defense スタンドアロン論理デバイスを設定します。
- 3.Firepower Management Center への登録(7 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。

これが Firepower Threat Defenseまたは FXOS のアップグレードの場合、または、別のアプリケーションを導入する場合は、最新の FXOS プラットフォーム バンドル、アプリケーション イメージ、および最新の更新プログラムを Cisco.com から取得する必要があります。「5.アップグレードの考慮事項(8 ページ)」を参照してください。

初期設定

システムの設定と管理に Firepower Chassis Manager または FXOS CLI を使用するには、事前に、コンソール ポートを介してアクセスした FXOS CLI を使用していくつかの初期設定タスクを実行する必要があります。FXOS CLI を使用して FXOS シャーシに初めてアクセスすると、システムの設定に使用できるセットアップ ウィザードが表示されます。

はじめる前に

- FXOS シャーシで次の物理接続を確認します。
  - コンソール ポートがコンピュータ端末またはコンソール サーバに物理的に接続されている。
  - 1 Gbps イーサネット管理ポートが外部ハブ、スイッチ、またはルータに接続されている。

  詳細については、『*Cisco 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。

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 4100CLI 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.Continue? (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-4100
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-4100
   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て、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 4100 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. [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。

NTP の設定

Firepower 4100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. Firepower Chassis Manager インターフェイスから [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. [Set Time Source]で [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 Server] フィールドに入力します。
4. **[Save(保存)]** 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 4100Firepower 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 タイプのインターフェイスを設定する必要があります。

手順

1. Firepower Chassis Manager インターフェイスで、[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. [Add Port Channel]をクリックします。
   b. [Port Channel ID] に、1 ～ 47 の値を入力します。
   c. [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。

   (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 [Edit]アイコンをクリックして、[Edit Interface] ダイアログボックスを開きます。
   b. [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。

Firepower Threat Defense論理デバイスの導入

スタンドアロン論理デバイスとしてFirepower Threat Defenseを設定できます。次の論理デバイス情報を設定します。

- デバイス情報およびアドレッシング
- 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
- インターフェイス情報およびアドレッシング
- エンド ユーザ ライセンス契約書

手順

1. Firepower Chassis Manager インターフェイスから、[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. [Add Device]をクリックして [Add Device] ダイアログボックスを開きます。
3. [Device Name]には、論理デバイスの名前を指定します。この名前は、Firepower 4100スーパバイザが管理設定を構成し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デバイス名ではありません。
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)]では、[スタンドアロン(Standalone)] ラジオ ボタンをクリックします。
7. [OK]をクリックします。[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。
9. 画面中央のデバイス アイコンをクリックします。設定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(Logical Device Information):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。

    (注) 登録キーは、ユーザ生成の 1 回しか使用できないキーです。37 文字以下にする必要があります。有効な文字は、英数字(A–Z、a–z、0–9)、およびハイフン(-)です。デバイスを Firepower Management Centerに追加するときに、この登録キーを思い出す必要があります。

    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) 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. [Save(保存)] をクリックします。Firepower 4100は、指定したソフトウェア バージョンをダウンロードし、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。

3.Firepower Management Center への登録

はじめる前に

- 登録予定の Firepower Threat Defenseセキュリティ モジュールに関して、Firepower Chassis Manager から設定を確認します。
- Firepower 4100で稼働している Firepower Threat Defense にはスマート ソフトウェア ライセンスが必要です。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. [Add]ドロップダウン メニューから、[Add Device] を選択します。
4. [ホスト(Host)]フィールドに、追加する Firepower Threat Defense デバイスの 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 で表示する Firepower Threat Defense デバイスの名前を入力します。
6. [登録キー(Registration Key)]フィールドに、Firepower Chassis Manage で Firepower Threat Defense デバイス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して、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。
   - [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。
   - [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。
   - [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。
   - 制御、マルウェア、および 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、正常に登録されたことを確認します。

4.ポリシーとデバイスの設定

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 4100 上で実行する Firepower Threat Defense のデバイス管理設定の構成や、アクセス制御ポリシーおよび 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。

5.アップグレードの考慮事項

Firepower Threat Defense導入または Firepower スーパバイザをアップグレードする場合、または、別のアプリケーションを導入する場合は、最新の FXOS プラットフォーム バンドル、アプリケーション イメージ、および最新の更新プログラムを Cisco.com から取得する必要があります。

(注) Firepower Threat Defense 論理デバイスをアップグレードするには、Firepower Management Center を使用する必要があります。Firepower Chassis Manager または FXOS CLI を使用して、Firepower Threat Defense 論理デバイスをアップグレードすることはできません。詳細については、『Firepower System Release Notes』を参照してください。

次の手順は、[システム(System)]メニューの [更新(Updates)] ページを使用して FXOS プラットフォーム バンドル、アプリケーション イメージ(Firepower Threat Defense や他のアプリケーションなど)、および最新の更新プログラムを Cisco.com からダウンロードする方法、さらに、イメージをアップロードしてスーパバイザをアップグレードする方法を説明しています。

- 必須の FXOS ソフトウェア パッケージとアプリケーション イメージを取得するには、「Cisco.com からのソフトウェア イメージのダウンロード(8 ページ)」を参照してください。
- アプリケーションまたはプラットフォーム バンドルをアップロードするには、「ソフトウェア イメージの Firepower 4100 へのアップロード(9 ページ)」を参照してください。
- 既存の論理デバイスまたは設定を削除するには、「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(9 ページ)」を参照してください。
- スーパバイザ ソフトウェア バンドルをアップグレードするには、「Firepower スーパバイザ プラットフォームのアップグレード(9 ページ)」を参照してください。

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。
- インターネット アクセスが必要です。

手順

1. Firepower Chassis Manager インターフェイスから [システム(System)] > [更新(Updates)]を選択します。[Available Updates] ページに、シャーシで使用可能な Firepower 4100プラットフォーム バンドル イメージおよびアプリケーション イメージのリストが表示されます。
2. ページ下部の [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 4100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。

ソフトウェア イメージの Firepower 4100 へのアップロード

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. Firepower Chassis Manager インターフェイスから [システム(System)] > [更新(Updates)]を選択します。[Available Updates] ページに、シャーシで使用可能な Firepower 4100プラットフォーム バンドル イメージおよびアプリケーション イメージのリストが表示されます。
2. [Upload Image]をクリックして、[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。
4. [Upload]をクリックします。選択したイメージが Firepower 4100にアップロードされます。
5. 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

Firepower Threat Defense論理デバイスのアップグレードまたは異なる論理デバイスの導入を行うには、既存のデバイスを削除してから、更新したイメージを使用して新しいデバイスを作成します。FXOS プラットフォーム バンドル イメージとアプリケーションの両方をアップグレードする場合は、最初に FXOS プラットフォーム バンドルをアップグレードする必要があります。

手順

1. Firepower Chassis Manager インターフェイスから、[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。

   [Logical Devices] ページに、シャーシに設定された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 エンジン上で稼働する Firepower Threat Defenseまたは他のアプリケーション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 スーパバイザ プラットフォームのアップグレード

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。シャーシで稼働している FXOS の現在のバージョンがセキュリティ エンジンでアプリケーション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。[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。

手順

1. Firepower Chassis Manager インターフェイスから [システム(System)] > [更新(Updates)]を選択します。[Available Updates] ページに、シャーシで使用可能な Firepower 4100プラットフォーム バンドル イメージおよびアプリケーション 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。

6.Firepower Threat DefenseCLI 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 4100FXOS スーパバイザ CLI から Firepower Threat Defense CLI にアクセスできます。

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>
   ```

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 DefenseCLI 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 DefenseCLI に直接接続されます。
4. Firepower Threat Defense接続を終了するには、**exit** と入力します。

   例:

   ```
   > exit
   firepower>
   ```

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

   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#
   ```

7.次の作業

- Firepower 4100 ドキュメンテーションには、すべての Firepower 4100 ドキュメンテーションへのリンクが記載されています。