ASA FirePOWER モジュール

次のトピックでは、ASA で実行される ASA FirePOWER モジュールを設定する方法について説明します。

ASA FirePOWER モジュールについて

ASA FirePOWER モジュールは、次世代侵入防御システム（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。

ASA FirePOWER モジュールは、ASA とは別のアプリケーションとして実行します。 このモジュールは、（ASA 5585-X でのみ）ハードウェア モジュールとして使用することも、（他のすべてのモジュールでは）ソフトウェア モジュールとして使用することもできます。

ASA FirePOWER モジュールがどのように ASA と連携するか

次のいずれかの導入モデルを使用して、ASA FirePOWER モジュールを設定できます。

- インライン モード：インライン導入では、実際のトラフィックが ASA FirePOWER モジュールに送信されるため、トラフィックで発生する内容は、モジュールのポリシーの影響を受けます。望ましくないトラフィックがドロップされ、ポリシーにより適用された他のアク

ションが実行された後、トラフィックは ASA に返されて、追加の処理および最終的な伝送が行われます。

- インライン タップ モニタ専用モード（ASA インライン）：インライン タップ モニタ専用導入では、トラフィックのコピーが ASA FirePOWER モジュールに送信されますが、ASA に戻されることはありません。インライン タップ モードでは、ASA FirePOWER モジュールがトラフィックに対して実行したと思われる内容を確認し、ネットワークに影響を与えずにトラフィックの内容を評価できます。ただし、このモードでは、ASA でそのポリシーをトラフィックに適用するため、アクセス ルール、TCP 正規化などによりトラフィックがドロップされる可能性があります。
- パッシブ モニタ専用（トラフィック転送）モード：FirePOWER サービス デバイスを使用した ASA がトラフィックに影響を与える可能性を回避する場合は、トラフィック転送インターフェイスを設定してスイッチの SPAN ポートに接続できます。このモードでは、トラフィックは ASA 処理なしで ASA FirePOWER モジュールに直接送信されます。モジュールから何も返されず、また ASA が任意のインターフェイスからトラフィックも送信しない点で、トラフィックが「ブラック ホール化」されます。トラフィック転送を設定するには、ASA をシングル コンテキスト トランスペアレント モードで運用する必要があります。

ASA および ASA FirePOWER には、必ず一貫性のあるポリシーを設定してください。両方のポリシーは、トラフィックのインライン モードまたはモニタ専用モードを反映する必要があります。

次の各セクションでは、これらのモードについて詳しく説明します。

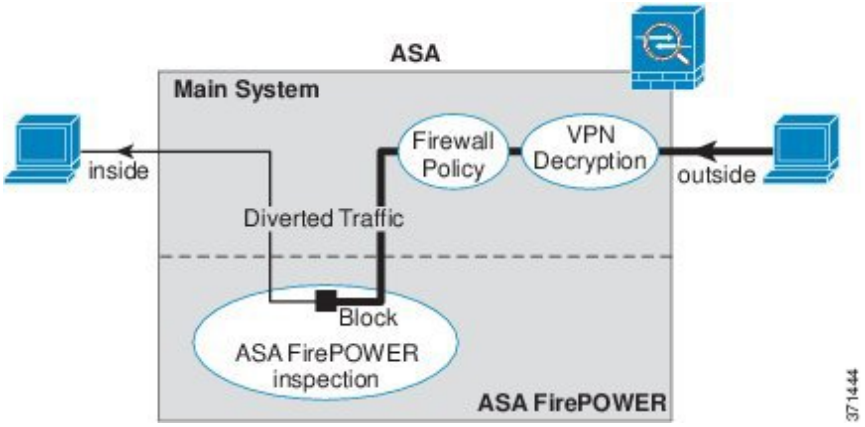
ASA FirePOWER インライン モジュール

インライン モードでは、トラフィックは、ファイアウォール検査を通過してから ASA FirePOWER モジュールへ転送されます。ASA で ASA FirePOWER インスペクション対象として指定されたトラフィックは、次に示すように ASA およびモジュールを通過します。

1. トラフィックが ASA に入ります。
2. 着信 VPN トラフィックが復号化されます。
3. ファイアウォール ポリシーが適用されます。
4. トラフィックが ASA FirePOWER モジュールに送信されます。
5. ASA FirePOWER モジュールはセキュリティ ポリシーをトラフィックに適用し、適切なアクションを実行します。
6. 有効なトラフィックが ASA に返送されます。ASA FirePOWER モジュールは、セキュリティ ポリシーに従ってトラフィックをブロックすることがあり、ブロックされたトラフィックは渡されません。
7. 発信 VPN トラフィックが暗号化されます。
8. トラフィックが ASA を出ます。

次の図は、ASA FirePOWER モジュールをインライン モードで使用する場合のトラフィック フローを示します。この例では、特定のアプリケーションに許可されないトラフィックをモジュールがブロックします。それ以外のトラフィックは、ASA を通って転送されます。

図 *1 : ASA* での *ASA FirePOWER* モジュールのトラフィック フロー



（注） 2 つの ASA インターフェイス上でホスト間が接続されており、ASA FirePOWER のサービス ポリシーがインターフェイスの一方のみについて設定されている場合は、これらのホスト間のすべてのトラフィックが ASA FirePOWER モジュールに送信されます。これには、ASA FirePOWER インターフェイス以外からのトラフィックも含まれます（この機能は双方向であるため）。

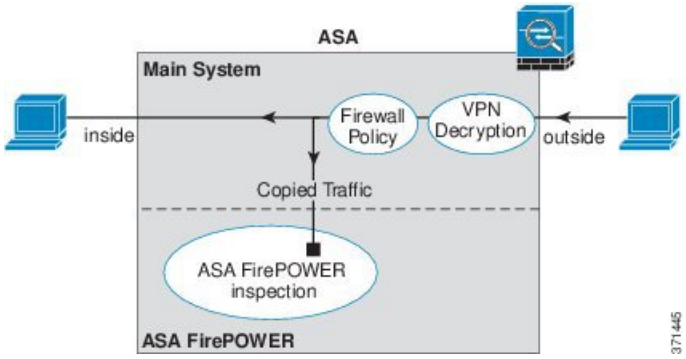
ASA FirePOWER インライン タップ モニタ専用モード

このモードでは、モニタリング目的でのみトラフィックの重複ストリームが ASA FirePOWER モジュールに送信されます。モジュールはトラフィックにセキュリティ ポリシーを適用し、インライン モードで動作していた場合に実行したであろう処理をユーザに通知します。たとえば、トラフィックはイベントで「ドロップされていたはず」とマークされる場合があります。この情報をトラフィック分析に使用し、インライン モードが望ましいかどうかを判断するのに役立てることができます。

（注） ASA 上でインライン タップ モニタ専用モードと通常のインライン モードの両方を同時に設定できません。サービス ポリシー ルールの 1 つのタイプのみが許可されます。マルチ コンテキスト モードでは、一部のコンテキストに対してインライン タップ モニタ専用モードを設定し、残りのコンテキストに対して通常のインライン モードを設定することはできません。

次の図は、インライン タップ モードで実行する場合のトラフィック フローを示します。

図 *2 : ASA FirePOWER* インライン タップ モニタ専用モード



ASA FirePOWER パッシブ モニタ専用トラフィック転送モード

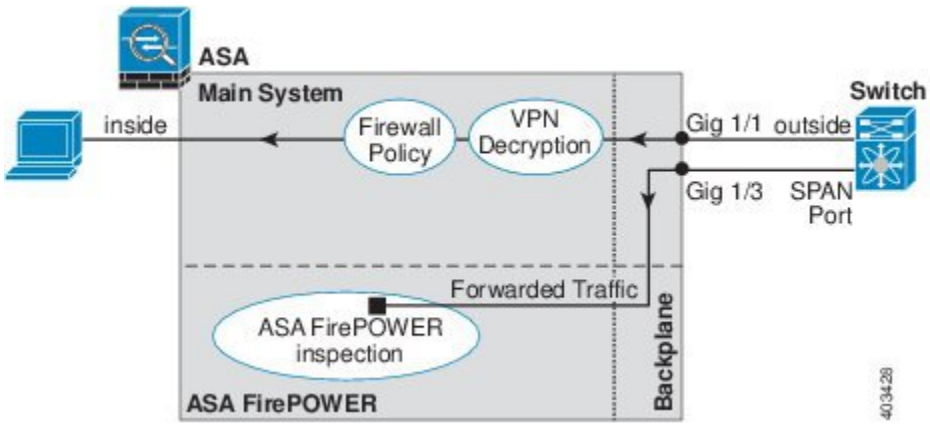
ASA FirePOWER モジュールをトラフィックにまったく影響を与えない純粋な侵入検知システム（IDS）として運用する場合は、トラフィック転送インターフェイスを設定できます。トラフィック転送インターフェイスは、受信したすべてのトラフィックを ASA 処理なしで ASA FirePOWER モジュールに直接送信します。

モジュールはトラフィックにセキュリティ ポリシーを適用し、インライン モードで動作していた場合に実行したであろう処理をユーザに通知します。たとえば、トラフィックはイベントで「ドロップされていたはず」とマークされる場合があります。この情報をトラフィック分析に使用し、インライン モードが望ましいかどうかを判断するのに役立てることができます。

この設定のトラフィックは転送されません。つまり、モジュールも ASA もトラフィックをその最終的な宛先に送信しません。この設定を使用するには、ASA をシングル コンテキスト モードおよびトランスペアレント モードで運用する必要があります。

次の図は、トラフィック転送用に設定されたインターフェイスを示します。このインターフェイスは、ASA FirePOWER モジュールがすべてのネットワーク トラフィックをインスペクションできるように、スイッチの SPAN ポートに接続されます。通常、別のインターフェイスがファイアウォールを介してトラフィックを送信します。

図 *3 : ASA FirePOWER* パッシブ モニタ専用、トラフィック転送モード



ASA FirePOWER 管理

モジュールには、初期設定およびトラブルシューティング専用の基本 CLI（コマンド ライン インタフェース）があります。次のいずれかの方法を使用して、ASA FirePOWER モジュールでセキュリティ ポリシーを設定します。

- Firepower/FireSIGHT Management Center：別の Management Center アプライアンス上でホストするか、または仮想アプライアンスとしてホストできます。Management Center アプリケーションは、バージョン 6.0 からは Firepower と呼ばれています。以前のバージョンでは、FireSIGHT と呼ばれます。
- ASDM（ご使用のモデル/バージョンとの互換性の確認）：オンボックスの ASDM を使用して、ASA とモジュールの両方を管理できます。

ASA の機能との互換性

ASA には、HTTP インスペクションを含む、多数の高度なアプリケーション インスペクション機能があります。ただし、ASA FirePOWER モジュールには ASA よりも高度な HTTP インスペクション機能があり、その他のアプリケーションについても機能が追加されています。たとえば、アプリケーション使用状況のモニタリングと制御です。

ASA では次の設定制限に従う必要があります。

- ASA FirePOWER モジュールに送信する HTTP トラフィックでは ASA インスペクションを設定しないでください。
- ASA FirePOWER モジュールに送信するトラフィックではクラウド Web セキュリティ（ScanSafe）インスペクションを設定しないでください。トラフィックがクラウド Web セキュリティと ASA FirePOWER サービス ポリシーの両方に一致する場合、トラフィックは ASA FirePOWER モジュールのみに転送されます。両方のサービスを実行する場合は、各サービスのトラフィック一致基準間に重複がないことを確認します。
- Mobile User Security（MUS）サーバを有効にしないでください。このサーバは、ASA FirePOWER モジュールとの互換性がありません。

ASA 上の他のアプリケーション インスペクションは ASA FirePOWER モジュールと互換性があり、これにはデフォルト インスペクションも含まれます。

ASA FirePOWER モジュールで URL フィルタリングができないときの対応

ASA FirePOWER モジュールは、管理元である FirePOWER Management Center から HTTP を介して URL フィルタリングのデータを取得します。このデータベースをダウンロードできないと、モジュールは URL フィルタリングを実行できません。

ASA FirePOWER モジュールと FirePOWER Management Center の間にデバイスがあり、それが ASA HTTP インスペクションか、または ASA CX モジュールを使用した HTTP インスペクショ

ンを行っている場合、そのインスペクションにより、ASA FirePOWER モジュールから FirePOWER Management Center への HTTP GET リクエストがブロックされる場合があります。この問題は、ASA FirePOWER モジュールをホストしている ASA に HTTP インスペクションを設定している場合も発生します（これは誤った設定です）。

問題を解決するには、状況に応じて次のいずれかを実行します。

- ASA FirePOWER モジュールをホストしている ASA に HTTP インスペクションを設定している場合は、HTTP インスペクションの設定を削除します。ASA FirePOWER インスペクションと ASA HTTP インスペクションは両立できません。
- ASA HTTP インスペクションを行う中間デバイスがある場合は、HTTP インスペクション ポリシー マップからプロトコル違反をドロップするアクションを削除します。

```
policy-map type inspect http http_inspection_policy
   parameters
      no protocol-violation action drop-connection
```

- 中間に ASA CX モジュールがある場合は、ASA FirePOWER モジュールと FirePOWER Management Center の管理 IP アドレスとの間の接続で CX モジュールをバイパスします。

ASA FirePOWER モジュールのライセンス要件

ASA FirePOWER モジュール機能の一部のエリアでは、追加のライセンスが必要となる場合があります。

Firepower/FireSIGHT Management Center によって管理されている ASA FirePOWER モジュールの場合は、Management Center を使用してモジュールでライセンスを有効にします。詳細については、『*FireSIGHT System User Guide 5.4*』のライセンスの章、『*Firepower Management Center Configuration Guide 6.0*』、または FireSIGHT Management Center のオンライン ヘルプを参照してください。

ASDM を使用して管理されている ASA FirePOWER モジュールの場合は、ASA で FirePOWER モジュール設定を使用してモジュールでライセンスを有効にします。詳細については、『*ASA FirePOWER Module User Guide 5.4*』のライセンスの章、『*ASA FirePOWER Services Local Management Configuration Guide 6.0*』、または ASDM でモジュールのオンライン ヘルプを参照してください。

ASA 自体には、追加のライセンスは不要です。

ASA FirePOWER のガイドライン

フェールオーバーのガイドライン

フェールオーバーは直接サポートされていません。ASA がフェールオーバーすると、既存の ASA FirePOWER フローは新しい ASA に転送されます。新しい ASA の ASA FirePOWER モ

ジュールが、その転送の時点からトラフィックの検査を開始します。古いインスペクションのステートは転送されません。

フェールオーバーの動作の整合性を保つために、ハイアベイラビリティな ASA ペアの ASA FirePOWER モジュールで一貫したポリシーを保持する必要があります。

（注） ASA FirePOWER モジュールを設定する前に、フェールオーバー ペアを作成します。モジュールが両方のデバイスにすでに設定されている場合、高可用性ペアを作成する前にスタンバイ デバイスのインターフェイスの設定をクリアします。スタンバイ デバイスの CLI から、 **clear configure interface** コマンドを入力します。

ASA クラスタリングのガイドライン

クラスタリングは直接サポートされていませんが、クラスタ内でこれらのモジュールを使用できます。クラスタ内の ASA FirePOWER モジュールで一貫したポリシーを保持する必要があります。

（注） ASA FirePOWER モジュールを設定する前に、クラスタを作成します。モジュールがスレーブ デバイスにすでに設定されている場合、クラスタにこれらを追加する前に、デバイスのインターフェイスの設定をクリアします。CLI から **clear configure interface**コマンドを入力します。

モデルのガイドライン

- ASA モデルのソフトウェアおよびハードウェアと ASA FirePOWER モジュールとの互換性については、『Cisco ASA Compatibility』を参照してください。
- ASA 5515-X ～ ASA 5555-X の場合は、シスコ ソリッド ステート ドライブ（SSD）をインストールする必要があります。詳細については、ASA 5500-X のハードウェア ガイドを参照してください。（5508-X、および 5516-X では SSD が標準です）。
- ASA 5585-X ハードウェア モジュールにインストールされているソフトウェア タイプは変更できません。ASA FirePOWER モジュールを購入する場合、そこに他のソフトウェアを後からインストールすることはできません。
- ASA 5585-X ASA FirePOWER のハードウェア モジュール上のインターフェイスでは、ソフトウェアのアップグレード時に発生するリブートを含むモジュールのリブート時に、最大 30 秒間のトラフィックがドロップします。

ASA FirePOWER の管理に関する ASDM のガイドライン

- ASDM の管理でサポートされる ASA、ASDM、および ASA FirePOWER のバージョンはモデルによって異なります。サポートされる組み合わせについては、『Cisco ASA Compatibility』を参照してください。

- モジュールをホストしている ASA でコマンドの権限を有効にする場合は、特権レベル 15 を持つユーザ名でログインして、**ASA FirePOWER** のホーム、設定、およびモニタリングのページを参照できるようにする必要があります。ステータス ページ以外の **ASA FirePOWER** のページに対する読み取り専用またはモニタ専用のアクセス権限は、サポートされていません。
- Java 7 Update 51 から Java 8 までを使用している場合は、ASA と ASA FirePOWER モジュールの両方の ID 証明書を設定する必要があります。『Install an Identity Certificate for ASDM』を参照してください。
- ASDM と Firepower Management Center を両方使用することはできません。いずれか一方を選択する必要があります。

その他のガイドラインと制限事項

- ASA の機能との互換性 （5 ページ）を参照してください。
- ASA. 上で通常のインライン モードとインライン タップ モニタ専用モードの両方を同時に設定できません。サービス ポリシー ルールの 1 つのタイプのみが許可されます。マルチ コンテキスト モードでは、一部のコンテキストに対してインライン タップ モニタ専用モードを設定し、残りのコンテキストに対して通常のインライン モードを設定することはできません。
- ASA で NetFlow を設定し、**flow-export delay flow-create** コマンドを含めると、ASA FirePOWER アクセス コントロール ポリシーで接続をブロックしてリセットする場合でも、接続は接続タイムアウトに達するまで ASA 上に保たれます。この動作を許容できない場合は、NetFlow 設定からコマンドを削除する必要があります。

ASA FirePOWER のデフォルト

次の表に、ASA FirePOWER モジュールのデフォルト設定を示します。

表 *1 : ASA FirePOWER* のデフォルトのネットワーク パラメータ

パラメータ	デフォルト
管理 IP アドレス	システム ソフトウェア イメージ：192.168.45.45/24 ブート イメージ：192.168.8.8/24
Gateway	システム ソフトウェア イメージ：なし ブート イメージ：192.168.8.1/24
SSH または session Username	admin

パラメータ	デフォルト
Password	システム ソフトウェア イメージ： • リリース 6.0 以降：**Admin123** • 6.0 より前のリリース：**Sourcefire** ブート イメージ：**Admin123**

ASA FirePOWER の初期設定の実行

ASA FirePOWER モジュールをネットワークに導入してから、管理方法を選択します。

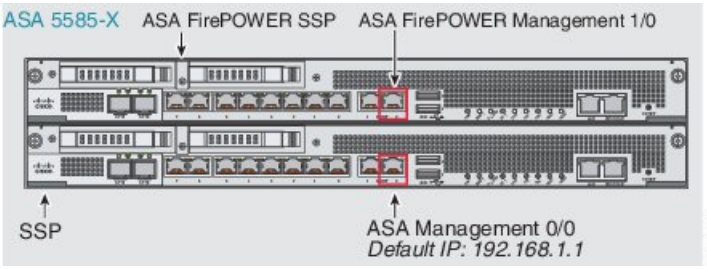
ネットワークでの ASA FirePOWER モジュールの導入

ASA FirePOWER モジュール管理インターフェイスをネットワークに接続する方法を決定するには、ファイアウォール モードおよび ASA モデルのセクションを参照してください。

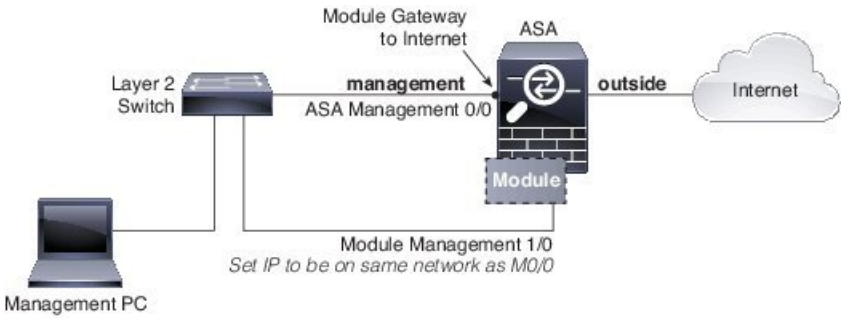
ルーテッド モード

ルーテッド モードの ASA 5585-X（ハードウェア モジュール）

ASA FirePOWER モジュールには、ASA とは別の管理インターフェイスが含まれます。



ASA FirePOWER モジュールとの間のすべての管理トラフィックは、管理 1/0 インターフェイスまたは管理 1/1 インターフェイスで入出力される必要があります。ASA FirePOWER モジュールには、インターネット アクセスも必要です。管理 1/x インターフェイスは ASA データ インターフェイスではないため、トラフィックがバックプレーン上で ASA を通過することができません。したがって、物理的に管理インターフェイスを ASA インターフェイスにケーブルで接続する必要があります。ASA FirePOWER が ASA 管理インターフェイス（またはデータ インターフェイスでも可）経由でインターネットにアクセスできるようにするには、次の標準的なケーブル セットアップを参照してください。ネットワークの接続方法に応じて、その他の選択肢もあります。たとえば、Management 1/0 インターフェイスを外側にしたり、内部ルータがある場合には Management 1/0 インターフェイスと別の ASA インターフェイスとの間でルーティングしたりする方法があります。



ルーテッド モジュールの ASA 5508-X ～ ASA 5555-X（ソフトウェア モジュール）

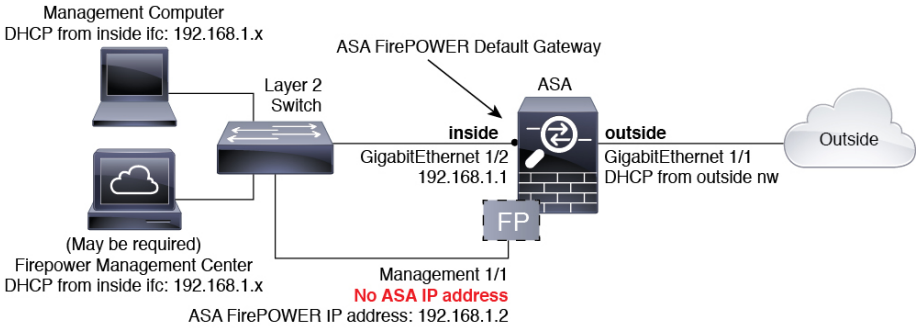
これらのモデルは、ASA FirePOWER モジュールをソフトウェア モジュールとして実行し、ASA FirePOWER モジュールは管理 0/0 または管理 1/1 インターフェイス（モデルに応じて）を ASA と共有します。

ASA FirePOWER モジュールとの間のすべての管理トラフィックは、管理インターフェイスで入出力される必要があります。ASA FirePOWER モジュールには、インターネット アクセスも必要です。管理トラフィックはバックプレーン上で ASA を通過することができません。したがって、インターネットに到達するには、管理インターフェイスを ASA インターフェイスに物理的にケーブルで接続する必要があります。

管理用に ASA 設定で名前と IP アドレスを設定しない場合、インターフェイスはモジュールのみに属します。この場合、管理インターフェイスは通常の ASA インターフェイスではありません。ユーザは以下を行うことができます。

1. 通常の ASA データ インターフェイスと同じネットワークに属するように ASA FirePOWER IP アドレスを設定する。
2. ASA FirePOWER ゲートウェイとしてデータ インターフェイスを指定する。
3. データ インターフェイスに管理インターフェイスを直接接続する（レイヤ 2 スイッチを使用）。

ASA FirePOWER が ASA 内部インターフェイス経由でインターネットにアクセスできるようにするには、次の標準的なケーブル セットアップを参照してください。



ASA 5508-X、および 5516-X の場合、デフォルト設定で上記のネットワーク配置が可能です。必要な変更は、モジュールの IP アドレスを ASA 内部インターフェイスと同じネットワーク上に設定することと、モジュールのゲートウェイ IP アドレスを設定することだけです。

その他のモデルの場合、管理 0/0 または 1/1 の ASA で設定された名前および IP アドレスを削除してから、上記に示すようにその他のインターフェイスを設定する必要があります。

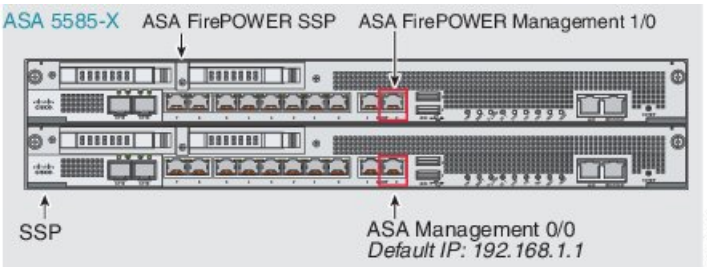
（注） 「ソフト スイッチ」を設定するために内部ブリッジ グループに割り当てることができるその他のインターフェイスがある場合、外部スイッチを使用するのを避けることができます。すべてのブリッジ グループのインターフェイスを同じセキュリティ レベルに設定し、同じセキュリティの通信を許可し、各ブリッジ グループ メンバーの NAT を設定してください。詳細については、ASA インターフェイスの構成ガイドの章を参照してください。

（注） 内部ネットワーク上に別のルータを配置する場合は、管理と内部の間にルーティングできます。この場合は、（ASA FirePOWER モジュール アドレスと同じネットワーク上での）管理インターフェイスの ASA 名および IP アドレスの設定などの適切な設定変更を使用して、管理インターフェイス上の ASA と ASA FirePOWER モジュールの両方を管理できます。

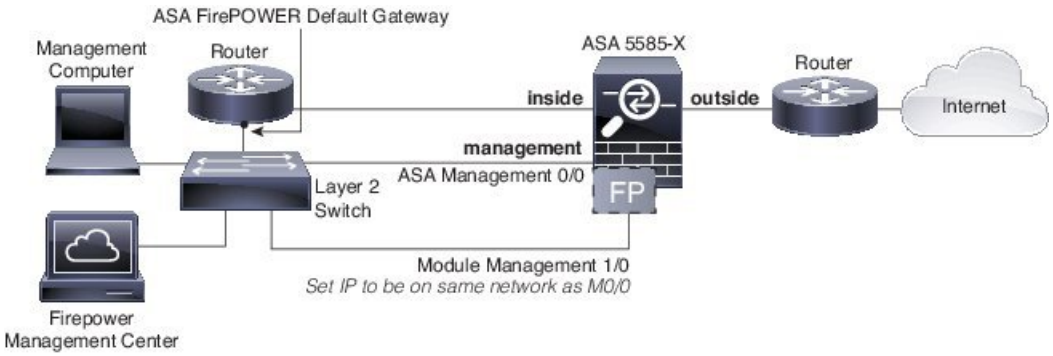
トランスペアレント モード

トランスペアレント モードの ASA 5585-X（ハードウェア モジュール）

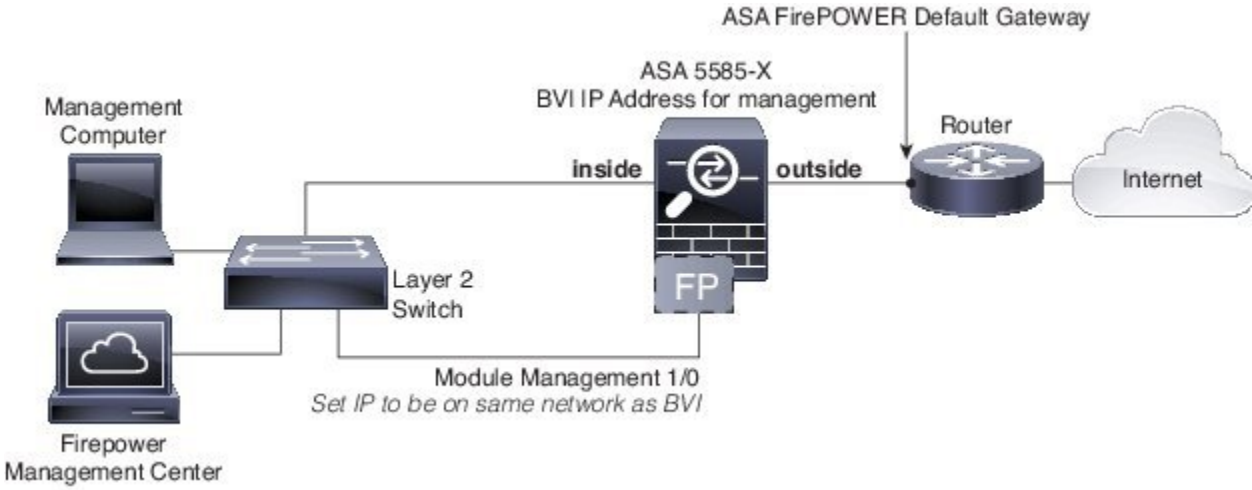
ASA FirePOWER モジュールには、ASA とは別の管理インターフェイスが含まれます。



ASA FirePOWER モジュールとの間のすべての管理トラフィックは、管理 1/0 インターフェイスまたは管理 1/1 インターフェイスで入出力される必要があります。ASA FirePOWER モジュールには、インターネット アクセスも必要です。このインターフェイスは ASA データ インターフェイスではないため、トラフィックがバックプレーン上で ASA を通過することができません。したがって、物理的に管理インターフェイスを ASA インターフェイスにケーブルで接続する必要があります。ASA FirePOWER が ASA 内部インターフェイス経由でインターネットにアクセスできるようにするには、次の標準的なケーブル セットアップを参照してください。



内部ルータを使用しない場合は、Management 0/0 インターフェイスを使用しないで内部インターフェイスを介して ASA を管理できます（BVI IP アドレスを使用）。



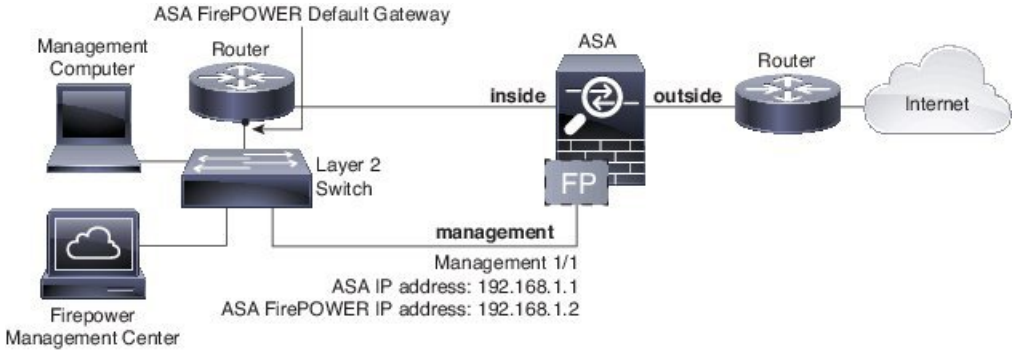
（注） 「ソフト スイッチ」を設定するために内部ブリッジ グループに割り当てることができるその他のインターフェイスがある場合、外部スイッチを使用するのを避けることができます。すべてのブリッジ グループのインターフェイスを同じセキュリティ レベルに設定し、同じセキュリティの通信を許可し、各ブリッジ グループ メンバーの NAT を設定してください。詳細については、ASA インターフェイスの構成ガイドの章を参照してください。

トランスペアレント モードの ASA 5508-X ～ ASA 5555-X、ISA 3000（ソフトウェア モジュール）

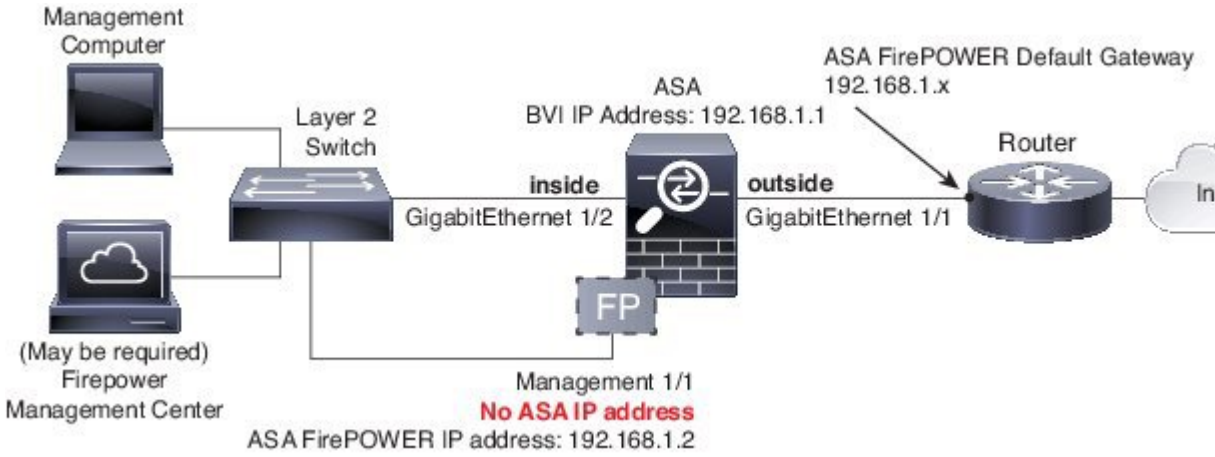
これらのモデルは、ASA FirePOWER モジュールをソフトウェア モジュールとして実行し、ASA FirePOWER モジュールは管理 0/0 または管理 1/1 インターフェイス（モデルに応じて）を ASA と共有します。

ASA FirePOWER モジュールとの間のすべての管理トラフィックは、管理インターフェイスで入出力される必要があります。ASA FirePOWER モジュールには、インターネット アクセスも必要です。

次の図は、ASA FirePOWER モジュールを使用した ASA 5500-X または ISA 3000 の推奨ネットワーク配置を示します。



内部ルータを使用しない場合は、ASA管理用の管理インターフェイスを使用しないで内部インターフェイスを介して ASA を管理できます（BVI IP アドレスを使用）。



（注） 「ソフト スイッチ」を設定するために内部ブリッジ グループに割り当てることができるその他のインターフェイスがある場合、外部スイッチを使用するのを避けることができます。すべてのブリッジ グループのインターフェイスを同じセキュリティ レベルに設定し、同じセキュリティの通信を許可し、各ブリッジ グループ メンバーの NAT を設定してください。詳細については、ASA インターフェイスの構成ガイドの章を参照してください。

Management Center への ASA FirePOWER モジュールの登録

Firepower/FireSIGHT Management Center にモジュールを登録するには、ASA FirePOWER モジュール CLI にアクセスする必要があります。CLI に初めてアクセスすると、基本設定パラメータの入力を求められます。また、Management Center にモジュールを追加する必要があります。

注：

- ASDM を使用してモジュールを管理する場合は、このセクションを省略して、ASDM 管理用の ASA FirePOWER モジュールの設定 （16 ページ）を参照してください。
- モジュールの管理を 1 つの Management Center から別の Management Center に移動する必要がある場合は、まずそのデバイスを Management Center のインベントリから削除します。次に、**configure manager add** コマンドを使用して、新しい Management Center を指します。次に、新しい Management Center から登録を完了できます。このプロセスにより、クリーンなハンドオーバーが確認されます。

ASA FirePOWER CLI へのアクセス

ASA FirePOWER CLI にアクセスするには、次のいずれかの方法を使用します。

手順

ステップ 1 コンソール ポート：

- ASA 5585-X：このモデルには、ASA FirePOWER モジュールの専用コンソール ポートが含まれています。付属の DB-9 to RJ-45 シリアル ケーブルや独自の USB シリアル アダプタを使用してください。
- その他のすべてのモデル：付属の DB-9 to RJ-45 シリアルケーブルや独自の USB シリアル アダプタを使用して ASA コンソールポートに接続します。ASA 5508-X/5516-X には、ミニ USB コンソール ポートもあります。USB コンソール ポートの使用手順については、ハードウェア ガイドを参照してください。

  ASA CLI での ASA FirePOWER モジュールへのセッション：

  session sfr

  ASA からソフトウェア モジュールへのセッション （32 ページ）も参照してください。

ステップ 2 SSH：

モジュールのデフォルト IP アドレス（ASA FirePOWER のデフォルト （8 ページ） を参照）に接続するか、または次の ASA コマンドを 使用して管理 IP アドレスを変更してから、SSH を使用して接続します。

session {1 | sfr} do setup host ip *ip_address*/*mask*,*gateway_ip*

ハードウェア モジュールの場合は **1**、ソフトウェア モジュールの場合は **sfr** を使用します。

ASA FirePOWER の基本設定

ASA FirePOWER モジュールの CLI に最初にアクセスすると、基本設定パラメータの入力を求められます。また、ASDM を使用していない場合は、モジュールを Firepower/FireSight Management Center に追加する必要があります。

始める前に

ASA FirePOWER CLI へのアクセス （14 ページ） に応じてモジュール CLI にアクセスします。

手順

ステップ 1 ASA FirePOWER CLI で、ユーザ名 **admin** でログインします。

初めてログインする場合は、デフォルトのパスワードを使用します。ASA FirePOWER のデフォルト （8 ページ）を参照してください。

ステップ 2 プロンプトに従ってシステム設定を行います。

推奨されるネットワーク配置（ネットワークでの ASA FirePOWER モジュールの導入 （9 ページ））に ASA FirePOWER モジュールの次のネットワーク設定を使用します。

- 管理インターフェイス：192.168.1.2
- 管理サブネット マスク：255.255.255.0
- ゲートウェイ IP：192.168.1.1

例：

```
System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password: <new password>
Confirm new password: <repeat password>
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]: y
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.86.118.3
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.252.0
Enter the IPv4 default gateway for the management interface []: 10.86.116.1
Enter a fully qualified hostname for this system [Sourcefire3D]: asasfr.example.com
Enter a comma-separated list of DNS servers or 'none' []: 10.100.10.15,
10.120.10.14
Enter a comma-separated list of search domains or 'none' [example.net]: example.com
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'
(Wait for the system to reconfigure itself.)

This sensor must be managed by a Defense Center.  A unique alphanumeric
registration key is always required.  In most cases, to register a sensor
to a Defense Center, you must provide the hostname or the IP address along
with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Defense Center are separated by a NAT device,
you must enter a unique NAT ID, along with the unique registration key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Defense Center, you must use the same
registration key and, if necessary, the same NAT ID when you add this
sensor to the Defense Center.
```

ステップ 3 ASA FirePOWER モジュールを Management Center に登録します。

> **configure manager add** {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

値は次のとおりです。

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} は、Management Center の完全修飾されたホスト名または IP アドレスを指定します。Management Center が直接アドレス指定できない場合は、DONTRESOLVE を使用します。
- *reg_key* は、ASA FirePOWER モジュールを Management Center に登録するのに必要な一意の英数字による登録キーです。
- *nat_id* は、Management Center と ASA FirePOWER モジュール間の登録プロセス中に使用されるオプションの英数字文字列です。hostname が DONTRESOLVE に設定されている場合に必要です。

ステップ 4 コンソール接続を閉じます。ソフトウェア モジュールの場合、次を入力します。

> **exit**

ASDM 管理用の ASA FirePOWER モジュールの設定

すべてのバージョンおよびモデルの組み合わせがサポートされるわけではありません。ご使用のモデルおよびバージョンの互換性を確認してください。

ASDM は、ASA バックプレーンを介して ASA FirePOWER モジュールの IPアドレスを変更できますが、すべての追加の管理には、モジュールが到達可能な、ASDMインターフェイスと管理インターフェイスとの間にネットワーク アクセスが必要です。

ASDM を使用してモジュールを管理するには、ASDM を起動し、起動ウィザードを実行します。

手順

ステップ 1 ASA に接続されているコンピュータで、Web ブラウザを起動します。

ステップ 2 [Address] フィールドに URL **https://192.168.1.1/admin** を入力します。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] 、[Run ASDM] 、[Run Startup Wizard]） 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。

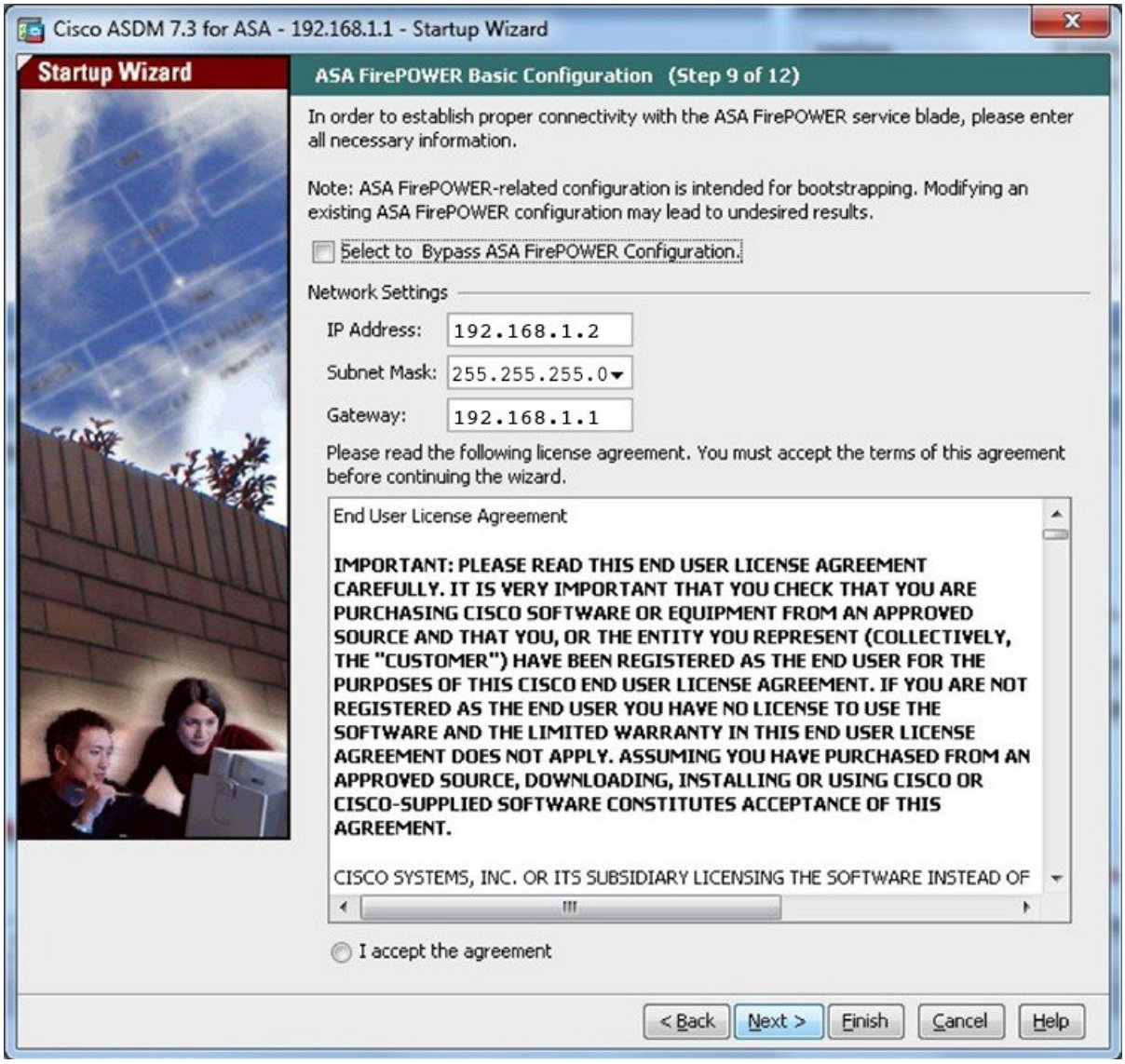
（注） [Install ASDM Launcher] をクリックした場合、場合によっては、『Install an Identity Certificate for ASDM』に従って ASA の ID 証明書と ASA FirePOWER モジュールの証明書をそれぞれインストールすることが必要になります。

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 インストールする ASA FirePOWER モジュールの IP アドレスを指定するよう求められた場合は、ダイアログボックスをキャンセルします。[Startup Wizard] を使用して、まず、モジュールの IP アドレスを正しい IP アドレスに設定する必要があります。

ステップ 7 **[Wizards]** > **[Startup Wizard]** を選択します。

ステップ 8 必要に応じて追加の ASA 設定を行うか、または、[ASA Firepower Basic Configuration] 画面が表示されるまで、画面を進みます。



デフォルト設定を使用するには、次の値を設定します。

- [IP Address]： 192.168.1.2
- [Subnet Mask] ：255.255.255.0
- [Gateway]：192.168.1.1

ステップ 9 [I accept the agreement] をクリックして、[Next] または [Finish] をクリックすると、ウィザードが終了します。

ステップ 10 ASDM を終了し、再起動します。**ホーム**ページに **ASA Firepower** のタブが表示されます。

ASA FirePOWER モジュールの設定

ASA FirePOWER モジュールでセキュリティ ポリシーを設定してから、トラフィックをモジュールに送信するように ASA を設定します。

ASA FirePOWER モジュールでのセキュリティ ポリシーの設定

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、モジュールで提供されるサービスを制御します。次のいずれかの方法を使用して、ASA FirePOWER モジュールでセキュリティ ポリシーを設定します。

FireSIGHT 管理センター

Web ブラウザを使用して **https://***DC_address* を開きます。ここで *DC_address* は、ASA FirePOWER の基本設定 （14 ページ）で定義したマネージャの DNS 名または IP アドレスです。たとえば、https://dc.example.com とします。

または、ASDM で **[Home]** > **[ASA FirePOWER Status]** を選択し、ダッシュボードの下部のリンクをクリックします。

ASA FirePOWER の設定に関する詳細については、Management Center のオンライン ヘルプ、『*FireSIGHT System User Guide 5.4*』または『*Firepower Management Center Configuration Guide 6.0*』（http://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html で入手可能）を参照してください。

ASDM

ASDM で、**[Configuration]** > **[ASA FirePOWER Configuration]** を選択します。

ASA FirePOWER の設定に関する詳細については、ASDM でモジュールのオンライン ヘルプ、『*ASA FirePOWER Module User Guide 5.4*』または『*ASA FirePOWER Services Local Management Configuration Guide 6.0*』（http://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html で入手可能）を参照してください。

ASA FirePOWER モジュールへのトラフィックのリダイレクト

インライン モードとインライン タップ（モニタ専用）モードの場合、トラフィックをモジュールにリダイレクトするようにサービス ポリシーを設定します。パッシブ モニタ専用モードにする場合は、ASA ポリシーをバイパスするトラフィック リダイレクション インターフェイスを設定します。

ここでは、これらのモードを設定する方法について説明します。

インライン モードまたはインライン タップ モニタ専用モードの設定

送信する特定のトラフィックを識別するサービス ポリシーを作成して、トラフィックを ASA FirePOWER モジュールへリダイレクトします。このモードでは、アクセス ルールなどの ASA ポリシーは、トラフィックがモジュールへリダイレクトされる前に適用されます。

始める前に

- （ASA FirePOWER と交換した）IPS または CX モジュールにトラフィックをリダイレクトするアクティブ サービス ポリシーがある場合は、ASA FirePOWER サービス ポリシーを設定する前にそのポリシーを削除する必要があります。
- ASA および ASA FirePOWER モジュールには、必ず一貫性のあるポリシーを設定してください。両方のポリシーは、トラフィックのインライン モードまたはインライン タップ モードを反映する必要があります。
- マルチ コンテキスト モードでは、各セキュリティ コンテキストでこの手順を実行します。

手順

ステップ 1 モジュールに送信するトラフィックを L3/L4 指定するためのクラス マップを作成します。

```
class-map name
match parameter
```

例：

```
hostname(config)# class-map firepower_class_map
hostname(config-cmap)# match access-list firepower
```

モジュールに複数のトラフィック クラスを送信する場合は、サービス ポリシーで使用するための複数のクラス マップを作成できます。照合ステートメントについては、トラフィックの特定（レイヤ 3/4 クラス マップ） を参照してください。

ステップ 2 クラス マップ トラフィックで実行するアクションを設定するポリシー マップを追加または編集します。**policy-map** *name*

例：

```
hostname(config)# policy-map global_policy
```

デフォルト設定では、global_policy ポリシーマップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。

ステップ 3 この手順の最初に作成したクラス マップを指定します。**class** *name*

例：

```
hostname(config-pmap)# class firepower_class_map
```

ステップ 4 ASA FirePOWER モジュールにトラフィックを送信します。

sfr {**fail-close** | **fail-open**} [**monitor-only**]

それぞれの説明は次のとおりです。

- **fail-close** キーワードを指定すると、ASA FirePOWER モジュールが使用できない場合はすべてのトラフィックをブロックするように ASA が設定されます。
- **fail-open** キーワードを指定すると、モジュールが使用できない場合はすべてのトラフィックを検査なしで通過させるように ASA が設定されます。
- トラフィックの読み取り専用コピーをモジュールに送信するには、**monitor-only** を指定します（インライン タップ モード）。キーワードを指定しない場合、トラフィックはインライン モードで送信されます。詳細については、「ASA FirePOWER インライン タップ モニタ専用モード （3 ページ）」を参照してください。

例：

```
hostname(config-pmap-c)# sfr fail-close
```

ステップ 5 ASA FirePOWER トラフィックに複数のクラス マップを作成した場合、ポリシーに別のクラスを指定して **sfr** リダイレクト アクションを適用できます。

ポリシー マップ内でのクラスの順番が重要であることの詳細については、サービス ポリシー内の機能照合を参照してください。トラフィックを同じアクション タイプの複数のクラスマップに一致させることはできません。

ステップ 6 既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name*}

例：

```
hostname(config)# service-policy global_policy global
```

global キーワードはポリシー マップをすべてのインターフェイスに適用し、**interface** はポリシーを 1 つのインターフェイスに適用します。グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシーマップを 1 つだけ適用できます。

パッシブ トラフィック転送の設定

モジュールがトラフィックのコピーを取得してモジュールも ASA もネットワークに影響を与えないパッシブ モニタ専用モードでモジュールを運用する場合は、トラフィック転送インターフェイスを設定してそのインターフェイスをスイッチの SPAN ポートに接続します。詳細については、ASA FirePOWER パッシブ モニタ専用トラフィック転送モード （4 ページ）を参照してください。

次のガイドラインでは、この導入モードの要件について説明します。

- ASA はシングル コンテキストおよびトランスペアレント モードである必要があります。
- 最大 4 つのインターフェイスを、トラフィック転送インターフェイスとして設定できます。その他の ASA インターフェイスは、通常どおり使用できます。
- トラフィック転送インターフェイスは、VLAN または BVI ではなく、物理インターフェイスである必要があります。また、物理インターフェイスには、それに関連付けられた VLAN を設定することはできません。
- トラフィック転送インターフェイスは、ASA トラフィックには使用できません。これらに名前を付けたり、フェールオーバーや管理専用を含む ASA 機能向けに設定したりすることはできません。
- トラフィック転送インターフェイスとサービス ポリシーの両方を ASA FirePOWER トラフィック用に設定できません。

手順

ステップ 1 トラフィック転送に使用する物理インターフェイスのインターフェイス コンフィギュレーション モードを開始します。

interface physical_interface

例：

```
hostname(config)# interface gigabitethernet 0/5
```

ステップ 2 インターフェイスに設定された名前を削除します。このインターフェイスがいずれかの ASA 設定で使用されていた場合、その設定は削除されます。指定したインターフェイス上でトラフィック転送を設定できません。

no nameif

ステップ 3 トラフィック転送をイネーブルにします。

traffic-forward sfr monitor-only

（注） トラフィック転送に関する警告は、デモンストレーション目的でのみ無視できます。これは、サポートされている生産モードです。

ステップ 4 インターフェイスをイネーブルにします。

no shutdown

追加のインターフェイスについて、この手順を繰り返します。

例

次の例は、GigabitEthernet 0/5 をトラフィック転送インターフェイスとして設定します。

```
interface gigabitethernet 0/5
  no nameif
  traffic-forward sfr monitor-only
  no shutdown
```

アクティブ認証用キャプティブ ポータルの有効化

ASA FirePOWER には、ユーザ ID 情報を収集することができるアイデンティティ ポリシーが含まれています。ユーザ ID 情報を収集することで、アクセス制御ルールを特定のユーザおよびユーザ グループに合わせて、ユーザに基づいてアクセスを選択的に許可および拒否できます。また、ユーザ ID に基づいてトラフィックを分析することもできます。

HTTP/HTTPS 接続の場合は、アクティブな認証を介してユーザ ID を収集するアイデンティティ ルールを定義できます。アクティブ認証アイデンティティ ルールを実装する場合は、認証プロキシ ポートとして機能するように ASA でキャプティブ ポータルを有効にする必要があります。接続がアクティブ認証を要求するアイデンティティ ルールに一致すると、ASA FirePOWER モジュールは、認証要求を ASA インターフェイスの IP アドレス/キャプティブ ポータルにリダイレクトします。デフォルト ポートは 885 ですが、これは変更可能です。

認証プロキシのキャプティブ ポータルをイネーブルにしない場合は、パッシブ認証のみを使用できます。

始める前に

- この機能は、ASA FirePOWER 6.0+ 専用のルーテッド モードでのみ使用可能です。
- マルチ コンテキスト モードでは、各セキュリティ コンテキストでこの手順を実行します。

手順

ステップ 1 キャプティブ ポータルを有効にします。

captive-portal {**global** | **interface** *name*} [**port** *number*]

それぞれの説明は次のとおりです。

- **global** すべてのインターフェイスでキャプティブ ポータルをグローバルにイネーブルにします。
- **interface** *name* は、指定したインターフェイスのみでキャプティブ ポータルをイネーブルにします。コマンドを複数入力して複数のインターフェイスでイネーブルにできます。この方法は、一部のインターフェイスのみのトラフィックを ASA FirePOWER モジュールにリダイレクトする場合に使用します。
- **port** *number* を使用すると、任意で認証ポートを指定できます。キーワードが含まれていない場合は、ポート 885 が使用されます。キーワードを含める場合は、ポート番号を 1025 以上にする必要があります。

例：

たとえば、ポート 885 でキャプティブ ポータルをグローバルに有効にするには、次のように入力します。

```
ciscoasa(config)# captive-portal global
ciscoasa(config)#
```

ステップ 2 ASA FirePOWER アイデンティティ ポリシーで、アクティブ認証設定でキャプティブ ポータル用に設定したポートと同じポートが指定されていることを確認し、アクティブ認証を有効にするために必要なその他の設定を行います。

ASA FirePOWER モジュールの管理

この項には、モジュールの管理に役立つ手順が含まれます。

モジュールのインストールまたは再イメージング

この項では、ソフトウェアまたはハードウェアモジュールのインストール方法または再イメージング方法について説明します。

ソフトウェア モジュールのインストールまたは再イメージング

ASA FirePOWER モジュールとともに ASA を購入した場合、モジュール ソフトウェアおよび必要なソリッド ステート ドライブ（SSD）は事前にインストールされており、すぐに設定できます。既存の ASA に ASA FirePOWER ソフトウェア モジュールを追加する場合、または

SSD を交換する必要がある場合は、ASA FirePOWER ブート ソフトウェアをインストールし、SSD を区分化して、この手順に従ってシステム ソフトウェアをインストールします。

最初に ASA FirePOWER モジュールをアンインストールする必要がある点を除いて、モジュールのイメージの再作成はこれと同じ手順です。SSD を交換する場合は、システムを再イメージングします。

SSD を物理的にインストールする方法については、ASA のハードウェア ガイドを参照してください。

始める前に

- フラッシュ（disk0）空き領域には、少なくとも、ブート ソフトウェアのサイズに 3 GB を加えた大きさが必要です。
- マルチ コンテキスト モードでは、コンテキスト実行スペースでこの手順を実行します。
- ユーザが実行している可能性のある他のソフトウェア モジュールをすべてシャットダウンする必要があります。ASA は、同時に 1 つのソフトウェア モジュールしか実行できません。この処理は ASA CLI から実行する必要があります。たとえば、次のコマンドで IPS ソフトウェア モジュールをシャットダウンおよびアンインストールし、ASA をリロードします。CX モジュールを削除するためのコマンドも同じですが、ips の代わりに cxsc キーワードを使用する点が異なります。

  sw-module module ips shutdown sw-module module ips uninstall reload

  ASA FirePOWER モジュールを再イメージングする場合は、同じシャットダウン コマンドとアンインストール コマンドを使用して古いイメージを削除します。たとえば、sw-module module sfr uninstall を使用します。
- IPS または CX モジュールにトラフィックをリダイレクトするアクティブ サービス ポリシーがある場合、そのポリシーを削除する必要があります。たとえば、ポリシーがグローバル ポリシーの場合、**no service-policy** *ips_policy* **global** を使用できます。サービス ポリシーに保持する必要のある他のルールが含まれている場合は、対象のポリシーマップからリダイレクション コマンドを単純に削除します。またはリダイレクションがそのクラスに対する唯一のアクションの場合はトラフィック クラス全体を削除します。CLI または ASDM を使用してポリシーを削除できます。
- Cisco.com から、ASA FirePOWER のブート イメージおよびシステム ソフトウェア パッケージの両方を取得します。

手順

ステップ 1 ブート イメージを ASA へダウンロードします。システム ソフトウェアは転送しないでください。これは後で SSD にダウンロードされます。次の選択肢があります。

- ASDM：最初にブートイメージをワークステーションにダウンロードするか、またはブート イメージを FTP、TFTP、HTTP、HTTPS、SMB、または SCP サーバに配置します。次に ASDM で、[Tools] > [File management] を選択し、適切な File Transfer コマンドとして

[Between Local PC and Flash] または [Between Remote Server and Flash] のいずれかを選択します。ブート ソフトウェアを ASA 上の disk0 に転送します。

- ASA CLI：最初にブート イメージを TFTP、FTP、HTTP、または HTTPS サーバ上に配置し、次に copy コマンドを使用してフラッシュへダウンロードします。次の例では、TFTP を使用します。

```
ciscoasa# copy tftp://10.1.1.89/asasfr-5500x-boot-5.4.1-58.img
disk0:/asasfr-5500x-boot-5.4.1-58.img
```

ステップ 2 ASA FirePOWER 管理インターフェイスからアクセス可能な HTTP、HTTPS、または FTP サーバに、Cisco.com から ASA FirePOWER システム ソフトウェアをダウンロードします。そのソフトウェアを ASA 上の disk0 にダウンロードしないでください。

ステップ 3 次のコマンドを入力して、ASA disk0 で ASA FirePOWER モジュール ブート イメージの場所を設定します。

sw-module module sfr recover configure image disk0: *file_path*

例：

```
hostname# sw-module module sfr recover configure image disk0:asasfr-5500x-boot-5.4.1-58.img
```

「ERROR: Another service (cxsc) is running, only one service is allowed to run at any time,」のようなメッセージが表示された場合は、別のソフトウェア モジュールがすでに設定されていることを意味します。このソフトウェア モジュールをシャットダウンして削除し、上の前提条件セクションの説明に従って新しいモジュールをインストールする必要があります。

ステップ 4 ASA FirePOWER ブート イメージをロードします。

sw-module module sfr recover boot

ステップ 5 ASA FirePOWER モジュールが起動するまで約 5 ～ 15 分待ってから、現在実行中の ASA FirePOWER ブート イメージへのコンソール セッションを開きます。セッションを開いてログイン プロンプトを表示した後で、Enter キーを押さなければならない場合があります。デフォルトのユーザ名は **admin** で、デフォルトのパスワードは **Admin123** です。

```
hostname# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Cisco ASA SFR Boot Image 5.3.1
asasfr login: admin
Password: Admin123
```

モジュールのブートが完了しない場合は、ttyS1 を介して接続できないというメッセージが表示されて session コマンドが失敗します。しばらく待ってから再試行してください。

ステップ 6 システム ソフトウェア パッケージをインストールできるようにシステムを設定します。

asasfr-boot> **setup**

例：

```
asasfr-boot> setup


                        Welcome to SFR Setup
                          [hit Ctrl-C to abort]
                      Default values are inside []
```

次のプロンプトが表示されます。管理アドレスとゲートウェイ、および DNS 情報が重要な設定であることに注意してください。

- Host name：最大 65 文字の英数字で、スペースは使用できません。ハイフンは使用できます。
- Network address：スタティック IPv4 または IPv6 アドレスを設定するか、DHCP（IPv4 の場合）、または IPv6 ステートレス自動設定を使用します。
- DNS information：少なくとも 1 つの DNS サーバを特定する必要があります。ドメイン名を設定してドメインを検索することもできます。
- NTP information：システム時刻を設定するために、NTP を有効にして NTP サーバを設定できます。

ステップ 7 システム ソフトウェア イメージをインストールします。

asasfr-boot> **system install** [**noconfirm**] *url*

確認メッセージに応答したくない場合は、**noconfirm** オプションを指定します。HTTP、HTTPS、または FTP URL を使用します。ユーザ名とパスワードが必要な場合は、それらを入力するよう示されます。

インストールが完了すると、システムが再起動します。アプリケーション コンポーネントのインストールと ASA FirePOWER サービスが開始するまでに必要な時間は大幅に異なります。ハイエンドプラットフォームでは 10 分以上かかる場合がありますが、ローエンドプラットフォームでは 60 ～ 80 分以上かかることがあります。（**show module sfr** の出力は、すべてのプロセスを Up として示します）。

次に例を示します。

```
asasfr-boot> system install http://upgrades.example.com/packages/asasfr-sys-5.4.1-58.pkg
Verifying
Downloading
Extracting
Package Detail
        Description:                    Cisco ASA-FirePOWER 5.4.1-58 System Install
        Requires reboot:                Yes

Do you want to continue with upgrade? [y]: y
Warning: Please do not interrupt the process or turn off the system.
Doing so might leave system in unusable state.

Upgrading
Starting upgrade process ...
Populating new system image
```

```
Reboot is required to complete the upgrade. Press 'Enter' to reboot the system.
(press Enter)
Broadcast message from root (ttyS1) (Mon Feb 17 19:28:38 2014):

The system is going down for reboot NOW!
Console session with module sfr terminated.
```

ステップ 8 ASA FirePOWER モジュールへのセッションを開きます。フル機能のモジュールにログインするため、別のログイン プロンプトが表示されます。

ciscoasa# **session sfr console**

例：

```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Sourcefire ASA5555 v5.4.1 (build 58)
Sourcefire3D login:
```

ステップ 9 設定を完了するには、ASA FirePOWER の基本設定 （14 ページ）を参照してください。

5585-X ASA FirePOWER ハードウェア モジュールの再イメージング

何らかの理由で ASA 5585-X の ASA FirePOWER ハードウェア モジュールのイメージを再作成する必要がある場合は、ブート イメージとシステム ソフトウェア パッケージの両方をこの順序でインストールする必要があります。システムが機能するには、両方のパッケージをインストールする必要があります。通常の状況では、アップグレードパッケージをインストールするために、システムのイメージを再作成する必要はありません。

ブート イメージをインストールするには、モジュールのコンソール ポートにログインして、ASA FirePOWER SSP の Management-0 ポートからイメージを TFTP ブートする必要があります。Management-0 ポートは SSP の最初のスロットにあるため、Management1/0 とも呼ばれますが、ROMMON では Management-0 または Management0/1 として認識されます。

（注） ASA 5585-X ASA FirePOWER のハードウェア モジュールでは、モジュールの再イメージング時に発生するリブートを含むモジュールのリブート時に、最大30秒間のトラフィックがドロップします。

始める前に

TFTP ブートを行うには、次の手順を実行します。

- ブート イメージおよびソフトウェア イメージを、ASA FirePOWER モジュールの Management1/0 インターフェイスからアクセス可能な TFTP サーバに配置する。

- Management1/0 をネットワークに接続する。このインターフェイスを使用して、ブート イメージを TFTP ブートする必要があります。

手順

ステップ 1 モジュールのコンソール ポートに接続します。

ステップ 2 システムをリロードします。

system reboot

ステップ 3 プロンプトが表示されたら、Esc キーを押してブートから抜け出します。GRUB がシステムをブートするために起動するのが表示された場合は、待ちすぎです。

これにより、ROMMON プロンプトに切り替わります。

ステップ 4 「ROMMON」プロンプトで次を入力します。

set

次のパラメータを設定します。

- ADDRESS：モジュールの管理 IP アドレス。
- SERVER：TFTP サーバの IP アドレス。
- GATEWAY：TFTP サーバのゲートウェイ アドレス。TFTP サーバが Management1/0 に直接接続されている場合は、TFTP サーバの IP アドレスを使用します。TFTP サーバおよび管理アドレスが同じサブネット上にある場合は、ゲートウェイを設定しないでください。設定すると、TFTP ブートが失敗します。
- IMAGE：TFTP サーバ上のブート イメージのパスとイメージ名。たとえば、TFTP サーバの /tftpboot/images/filename.img にファイルを置いた場合、IMAGE の値は images/filename.img となります。

例：

```
ADDRESS=10.5.190.199
SERVER=10.5.11.170
GATEWAY=10.5.1.1
IMAGE=asasfrboot-5.4.1-58.img
```

ステップ 5 設定を保存します。

sync

ステップ 6 ダウンロードおよびブート プロセスを開始します。

tftp

進行状況を示す ! マークが表示されます。数分後にブートが完了すると、ログイン プロンプトが表示されます。

ステップ 7 パスワード **Admin123** を使用して **admin** としてログインします。

ステップ 8 システム ソフトウェア パッケージをインストールできるようにシステムを設定します。

setup

次のプロンプトが表示されます。管理アドレスとゲートウェイ、および DNS 情報が重要な設定であることに注意してください。

- Host name：最大 65 文字の英数字で、スペースは使用できません。ハイフンは使用できます。
- Network address：スタティック IPv4 または IPv6 アドレスを設定するか、DHCP（IPv4 の場合）、または IPv6 ステートレス自動設定を使用します。
- DNS information：少なくとも 1 つの DNS サーバを特定する必要があります。ドメイン名を設定してドメインを検索することもできます。
- NTP information：システム時刻を設定するために、NTP を有効にして NTP サーバを設定できます。

ステップ 9 システム ソフトウェア イメージをインストールします。

system install [noconfirm] *url*

例：

```
asasfr-boot> system install http://upgrades.example.com/packages/asasfr-sys-5.4.1-58.pkg
```

確認メッセージに応答したくない場合は、**noconfirm** オプションを指定します。

インストールが完了すると、システムが再起動します。アプリケーション コンポーネントのインストールと ASA FirePOWER サービスの起動には 10 分以上かかります。

ステップ 10 ブートが完了したら、デフォルトのパスワードを使用して **admin** としてログインします。ASA FirePOWER のデフォルト （8 ページ）を参照してください。

ステップ 11 設定を完了するには、ASA FirePOWER の基本設定 （14 ページ）を参照してください。

パスワードのリセット

管理ユーザのパスワードを忘れた場合は、CLI 設定権限を持つ別のユーザがログインして、パスワードを変更できます。

必要な権限を持つ別のユーザが存在しない場合は、ASA から管理者パスワードをリセットできます。デフォルトのパスワードは、ソフトウェア リリースに応じて異なります。ASA FirePOWER のデフォルト （8 ページ） を参照してください。

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースでこの手順を実行します。

- ASA の hw-module および sw-module コマンドの password-reset オプションは、ASA FirePOWER では機能しません。

手順

ユーザ **admin** のモジュール パスワードをデフォルトにリセットします。

session {1 | sfr} do password-reset

ハードウェア モジュールの場合は **1**、ソフトウェア モジュールの場合は **sfr** を使用します。

モジュールのリロードまたはリセット

ASA からモジュールをリロードしたり、リセットしてからリロードしたりすることができます。

始める前に

マルチ コンテキスト モードでは、コンテキスト実行スペースでこの手順を実行します。

手順

次のいずれかのコマンドを入力します。

- ハードウェア モジュール（ASA 5585-X）：

  hw-module module 1 {reload | reset}

  （注） ASA 5585-X ASA FirePOWER のハードウェア モジュール上のインターフェイスでは、ソフトウェアのアップグレード時に発生するリブートを含むモジュールのリブート時に、最大 30 秒間のトラフィックがドロップします。

- ソフトウェア モジュール（その他すべてのモデル）：

  sw-module module sfr {reload | reset}

モジュールのシャットダウン

モジュール ソフトウェアをシャットダウンするのは、コンフィギュレーション データを失うことなく安全にモジュールの電源をオフにできるように準備するためです。

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースでこの手順を実行します。
- ASAをリロードする場合は、モジュールは自動的にはシャットダウンされないので、ASAのリロード前にモジュールをシャットダウンすることを推奨します。

手順

次のいずれかのコマンドを入力します。

- ハードウェア モジュール（ASA 5585-X）：

  hw-module module 1 shutdown

- ソフトウェア モジュール（その他すべてのモデル）：

  sw-module module sfr shutdown

ソフトウェア モジュール イメージのアンインストール

ソフトウェア モジュール イメージおよび関連するコンフィギュレーションをアンインストールできます。

始める前に

マルチ コンテキスト モードでは、コンテキスト実行スペースでこの手順を実行します。

手順

ステップ 1 ソフトウェア モジュール イメージおよび関連するコンフィギュレーションをアンインストールします。

sw-module module sfr uninstall

例：

```
ciscoasa# sw-module module sfr uninstall

Module sfr will be uninstalled. This will completely remove the disk image
associated with the sw-module including any configuration that existed within it.

Uninstall module sfr? [confirm]
```

ステップ 2 ASA をリロードします。

reload

新しいモジュールをインストールする前に、ASA をリロードする必要があります。

ASA からソフトウェア モジュールへのセッション

ASA FirePOWER CLI を使用して、基本的なネットワーク設定を構成し、モジュールのトラブルシューティングを行います。

ASA から ASA FirePOWER ソフトウェア モジュール CLI にアクセスするには、ASA からセッション接続できます。（5585-X で実行しているハードウェア モジュールへのセッションは確立できません）。

モジュールへのセッションを開始することも（Telnet を使用）、仮想コンソール セッションを作成することもできます。コンソール セッションは、コントロール プレーンがダウンし、Telnet セッションを確立できない場合に便利です。マルチ コンテキスト モードでは、システム実行スペースからセッションを開きます。

Telnet またはコンソール セッションでは、ユーザ名とパスワードの入力を求められます。ASA FirePOWER に設定されている任意のユーザ名でログインできます。最初は、**admin** が唯一の設定済みユーザ名です（このユーザ名は常に使用可能です）。最初のデフォルトのパスワードは、イメージのタイプ（完全なイメージまたはブート イメージ）とソフトウェア リリースに応じて異なります。ASA FirePOWER のデフォルト （8 ページ） を参照してください。

- Telnet セッション：

  session sfr

  ASA FirePOWER CLI にいるときに ASA CLI に戻るには、モジュールからログアウトするコマンド（logout や exit など）を入力するか、Ctrl+Shift+6、x を押します。

- コンソール セッション：

  session sfr console

  コンソール セッションからログアウトする唯一の方法は、Ctrl+Shift+6、x を押すことです。モジュールからログアウトすると、モジュールのログイン プロンプトに戻ります。

（注） session sfr console コマンドは、Ctrl+Shift+6、x がターミナル サーバのプロンプトに戻るエスケープ シーケンスであるターミナル サーバとともに使用しないでください。Ctrl+Shift+6、x は、ASA FirePOWER コンソールをエスケープし ASA プロンプトに戻るシーケンスでもあります。したがって、この状況で ASA FirePOWER コンソールを終了しようとすると、代わりにターミナル サーバ プロンプトに戻ります。ASA にターミナル サーバを再接続すると、ASA FirePOWER コンソール セッションがまだアクティブなままであり、ASA プロンプトに戻ることができません。ASA プロンプトにコンソールを戻すには、直接シリアル接続を使用する必要があります。この状況が発生した場合は、console コマンドの代わりに **session sfr** コマンドを使用します。

システム ソフトウェアのアップグレード

アップグレードを適用する前に、ASAが新しいバージョンに最小限必要なリリースを実行していることを確認します。場合によっては、モジュールをアップグレードする前に ASA をアップグレードする必要があります。アップグレードの適用に関する詳細については、Management Center のオンライン ヘルプ、『*FireSIGHT System User Guide 5.4*』または『*Firepower Management Center Configuration Guide 6.0*』を参照してください。

ASDM 管理では、**[Configuration]** > **[ASA FirePOWER Configuration]** > **[Updates]** を使用して、アップグレードをシステム ソフトウェアおよびコンポーネントに適用できます。詳細については、[Updates] ページの [Help] をクリックします。

ASA FirePOWER モジュールのモニタリング

次の各トピックでは、モジュールのモニタリングに関するガイダンスを示します。ASA FirePOWER 関連の syslog メッセージについては、syslog メッセージ ガイドを参照してください。ASA FirePOWER の syslog メッセージは、メッセージ番号 434001 から始まります。

モジュール ステータスの表示

モジュールのステータスを確認するには、次のいずれかのコマンドを入力します。

- **show module** [**1** | **sfr**] [**details**]

  モジュールのステータスを表示します。ASA FirePOWER モジュールに固有のステータスを確認するには、**1**（ハードウェアモジュールの場合）**sfr**（ソフトウェアモジュールの場合）キーワードを指定します。モジュールを管理するデバイスのアドレスなどの追加情報を取得するには、**details** キーワードを指定します。

- **show module sfr recover**

  モジュールのインストール時に使用されたブート イメージの場所を表示します。

ASA 5585-X に ASA FirePOWER ハードウェア モジュールがインストールされている場合の **show module** コマンドの出力例を次に示します。

```
hostname# show module
Mod  Card Type                                    Model              Serial No.
---- -------------------------------------------- ------------------ -----------
   0 ASA 5585-X Security Services Processor-10 wi ASA5585-SSP-10     JAF1507AMKE
   1 ASA 5585-X FirePOWER Security Services Proce ASA5585-SSP-SFR10  JAF1510BLSA

Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   0 5475.d05b.1100 to 5475.d05b.110b  1.0          2.0(7)0      100.10(0)8
   1 5475.d05b.2450 to 5475.d05b.245b  1.0          2.0(13)0     5.3.1-44

Mod  SSM Application Name           Status           SSM Application Version
---- ------------------------------ ---------------- --------------------------
   1 FirePOWER                      Up               5.3.1-44
```

```
Mod  Status             Data Plane Status     Compatibility
---- ------------------ --------------------- -------------
   0 Up Sys             Not Applicable
   1 Up                 Up
```

次に、ソフトウェアモジュールの詳細を表示する例を示します。DCAddrは、このデバイスを管理する Management Center のアドレスを示しています。

```
hostname# show module sfr details
Getting details from the Service Module, please wait...

Card Type:          FirePOWER Services Software Module
Model:              ASA5555
Hardware version:   N/A
Serial Number:      FCH1714J6HP
Firmware version:   N/A
Software version:   5.3.1-100
MAC Address Range:  bc16.6520.1dcb to bc16.6520.1dcb
App. name:          ASA FirePOWER
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       5.3.1-100
Data Plane Status:  Up
Status:             Up
DC addr:            10.89.133.202
Mgmt IP addr:       10.86.118.7
Mgmt Network mask:  255.255.252.0
Mgmt Gateway:       10.86.116.1
Mgmt web ports:     443
Mgmt TLS enabled:   true
```

次に、モジュールのインストール時に **sw-module module sfr recover** コマンドで使用された ASA FirePOWER ブート イメージの場所を表示する例を示します。

```
hostname# show module sfr recover
Module sfr recover parameters...
Boot Recovery Image: No
Image File Path:     disk0:/asasfr-5500x-boot-5.4.1-58.img
```

モジュールの統計情報の表示

sfr コマンドを含む各サービス ポリシーの統計情報およびステータスを表示するには、show service-policy sfr コマンドを使用します。カウンタをクリアするには、clear service-policy を使用します。

次に、ASA FirePOWER サービス ポリシーと現在の統計情報およびモジュールのステータスを表示する例を示します。モニタ専用モードでは、入力カウンタはゼロのままです。

```
ciscoasa# show service-policy sfr

Global policy:
  Service-policy: global_policy
    Class-map: my-sfr-class
      SFR: card status Up, mode fail-close
        packet input 2626422041, packet output 2626877967, drop 0, reset-drop 0, proxied
```

0

モジュール接続のモニタリング

ASA FirePOWER モジュールを通過する接続を表示するには、次のいずれかのコマンドを入力します。

- **show asp table classify domain sfr**

  トラフィックを ASA FirePOWER モジュールに送信するために作成された NP ルールを表示します。

- **show asp drop**

  ドロップされたパケットを表示します。ドロップのタイプについては、以下で説明します。

- **show conn**

  「X - inspected by service module」フラグを表示することにより、接続がモジュールに転送されているかどうかを示します。

show asp drop コマンドは、ASA FirePOWER モジュールに関連する次のドロップ理由を含めることができます。

フレーム ドロップ：

- sfr-bad-tlv-received：これが発生するのは、ASA が FirePOWER から受信したパケットにポリシー ID TLV がないときです。非制御パケットのアクション フィールドで Standy/Active ビットが設定されていない場合は、この TLV が存在している必要があります。
- sfr-request：FirePOWER 上のポリシーが理由で、フレームをドロップするよう FirePOWER から要求されました。このポリシーによって、FirePOWER はアクションを Deny Source、Deny Destination、または Deny Pkt に設定します。フレームがドロップべきでなかった場合は、フローを拒否しているモジュールのポリシーを確認します。
- sfr-fail-close：パケットがドロップされたのは、カードが動作中ではなく、設定済みのポリシーが「fail-close」であったからです（対照的に、「fail-open」の場合は、カードがダウンしていてもパケットの通過が許可されます）。カードのステータスを確認し、サービスを再開するか、再起動します。
- sfr-fail：既存のフローに対する FirePOWER コンフィギュレーションが削除されており、FirePOWER で処理できないため、ドロップされます。これが発生することは、ほとんどありません。
- sfr-malformed-packet：FirePOWER からのパケットに無効なヘッダーが含まれます。たとえば、ヘッダー長が正しくない可能性があります。
- sfr-ha-request：セキュリティ アプライアンスが FirePOWER HA 要求パケットを受信し、それを処理できなかった場合、このカウンタが増加し、パケットがドロップされます。

- sfr-invalid-encap：セキュリティ アプライアンスが無効なメッセージ ヘッダーを持つ FirePOWER パケットを受信すると、このカウンタが増加し、パケットがドロップされます。
- sfr-bad-handle-received：FirePOWER モジュールからパケットで不正フロー ハンドルを受信し、フローをドロップしました。FirePOWER フローのハンドルがフロー期間中に変更されると、このカウンタが増加し、フローとパケットが ASA でドロップされます。
- sfr-rx-monitor-only：セキュリティ アプライアンスがモニタ専用モードのときに FirePOWER パケットを受信すると、このカウンタが増加し、パケットがドロップされます。

フロー ドロップ：

- sfr-request：フローを終了させることを FirePOWER が要求しました。アクション ビット 0 が設定されます。
- reset-by-sfr：フローの終了とリセットを FirePOWER が要求しました。アクション ビット 1 が設定されます。
- sfr-fail-close：フローが終了させられたのは、カードがダウン状態であり、設定済みのポリシーが「fail-close」であったからです。

ASA FirePOWER モジュールの例

次に、すべての HTTP トラフィックを ASA FirePOWER モジュールに迂回させ、何らかの理由でモジュールで障害が発生した場合にはすべての HTTP トラフィックをブロックする例を示します。

```
hostname(config)# access-list ASASFR permit tcp any any eq 80
hostname(config)# class-map my-sfr-class
hostname(config-cmap)# match access-list ASASFR
hostname(config-cmap)# policy-map my-sfr-policy
hostname(config-pmap)# class my-sfr-class
hostname(config-pmap-c)# sfr fail-close
hostname(config-pmap-c)# service-policy my-sfr-policy global
```

次の例では、10.1.1.0 ネットワークと 10.2.1.0 ネットワーク宛てのすべての IP トラフィックが ASA FirePOWER モジュールに誘導され、何らかの理由でモジュールに障害が発生した場合は、すべてのトラフィックの通過が許可されます。

```
hostname(config)# access-list my-sfr-acl permit ip any 10.1.1.0 255.255.255.0
hostname(config)# access-list my-sfr-acl2 permit ip any 10.2.1.0 255.255.255.0
hostname(config)# class-map my-sfr-class
hostname(config-cmap)# match access-list my-sfr-acl
hostname(config)# class-map my-sfr-class2
hostname(config-cmap)# match access-list my-sfr-acl2
hostname(config-cmap)# policy-map my-sfr-policy
hostname(config-pmap)# class my-sfr-class
hostname(config-pmap-c)# sfr fail-open
hostname(config-pmap)# class my-sfr-class2
```

```
hostname(config-pmap-c)# sfr fail-open
hostname(config-pmap-c)# service-policy my-sfr-policy interface outside
```

ASA FirePOWER モジュールの履歴

機能	プラットフォーム リリース	説明
ASA 5585-X（すべてのモデル）で適合する ASA FirePOWER SSP ハードウェア モジュールをサポート。 ASA 5512-X ～ ASA 5555-X で ASA FirePOWER ソフトウェア モジュールをサポート。	ASA 9.2(2.4) ASA FirePOWER 5.3.1	ASA FirePOWER モジュールは、次世代 IPS（NGIPS）、アプリケーションの可視性とコントロール（AVC）、URL フィルタリング、高度なマルウェア保護（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。このモジュールは、シングルまたはマルチ 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 モードで使用できます。 **capture interface asa_dataplane**、**debug sfr**、**hw-module module 1 reload**、**hw-module module 1 reset**、**hw-module module 1 shutdown**、**session do setup host ip**、**session do get-config**、**session do password-reset**、**session sfr**、**sfr**、**show asp table classify domain sfr**、**show capture**、**show conn**、**show module sfr**、**show service-policy**、**sw-module sfr** の各コマンドが導入または変更されました。
ASA 5506-X で ASA FirePOWER ソフトウェア モジュールをサポート（ASDM でのモジュールの設定のサポートを含む）	ASA 9.3(2) ASDM 7.3(3) ASA FirePOWER 5.4.1	ASA 5506-X で ASA FirePOWER ソフトウェア モジュールを実行できます。FireSIGHT Management Center を使用してモジュールを管理したり、ASDM を使用したりすることができます。
トラフィック リダイレクション インターフェイスを使用した ASA FirePOWER パッシブ モニタ専用モード	ASA 9.3(2) ASA FirePOWER 5.4.1	サービス ポリシーを使用する代わりに、トラフィックをモジュールに送信するようにトラフィック転送インターフェイスを設定できるようになりました。このモードでは、モジュールも ASA もトラフィックに影響を与えません。 **traffic-forward sfr monitor-only** コマンドが完全にサポートされています。これは、CLI でのみ設定できます。
5506H-X、5506W-X、5508-X、および 5516-X 向けの ASDM を介したモジュール管理のサポート	ASA 9.4(1) ASDM 7.4(1) ASA FirePOWER 5.4.1	FireSIGHT Management Center を使用する代わりに ASDM を使用して、モジュールを管理できます。 新しい画面またはコマンドは追加されていません。

機能	プラットフォーム リリース	説明
5512-X ～ 5585-X 向けの ASDM を介したモジュール管理のサポート	ASA 9.5.(1.5) ASDM 7.5(1.112) ASA FirePOWER 6.0	Firepower Management Center（旧名 FireSIGHT Management Center）を使用する代わりに ASDM を使用して、モジュールを管理できます。 新しい画面またはコマンドは追加されていません。
ASA FirePOWER 6.0 でのアクティブ認証向けキャプティブ ポータル。	ASA 9.5.(2) ASA FirePOWER 6.0	キャプティブ ポータル機能では、ASA FirePOWER 6.0 で始まるアイデンティティ ポリシーを使用してアクティブ認証を有効にする必要があります。 次のコマンドが導入または変更されました。**captive-portal**、**clear configure captive-portal**、**show running-config captive-portal**。
ASA 5506-X シリーズおよび ASA 5512-X の ASA FirePOWER モジュールでは 9.10 (1) はサポートされていません。	9.10(1)	ASA 5506-X シリーズおよび 5512-X では、メモリの制約により、9.10(1) 以降での ASA FirePOWER モジュールはサポートされなくなりました。このモジュールの使用を継続するには、9.9(x) 以前の状態のままにしておく必要があります。その他のモジュール タイプは引き続きサポートされます。9.10(1) にアップグレードすると、FirePOWER モジュールにトラフィックを送信するための ASA 設定が消去されます。アップグレード前に設定を必ずバックアップしてください。FirePOWER イメージとその設定は SSD にそのままの状態で保持されます。ダウングレードする場合は、バックアップから ASA 設定をコピーして機能を復元できます。