ASA FirePOWER（SFR）モジュール

この章では、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

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。

このモジュールは ASA SFR とも呼ばれます。

このモジュールには、初期設定およびトラブルシューティングのための基本的なコマンド ライン インターフェイス（CLI）が用意されていますが、デバイスのセキュリティ ポリシーは、独立したアプリケーションである FireSIGHT 管理センター を使用して設定できます。このアプリケーションは、独立した FireSIGHT 管理センター アプライアンスで、または VMware サーバ上で実行される仮想アプライアンスとしてホストできます（FireSIGHT 管理センター は防御センターとも呼ばれます）。

ASA FirePOWER モジュールを ASA と連携させる方法

ASA FirePOWER モジュールは、ASA と別のアプリケーションを実行します。このモジュールは、ハードウェア モジュール（ASA 5585-X 上）か、ソフトウェア モジュール（5512-X ～ 5555-X）です。ハードウェア モジュールには、独立した管理およびコンソール ポートと、モジュール自体ではなく ASA によって直接使用される追加のデータ インターフェイスがあります。

デバイスは、パッシブ（「モニタ専用」）展開またはインライン展開のいずれかで設定できます。

- パッシブ展開では、トラフィックのコピーがデバイスに送信されますが、ASA には返されません。パッシブ モードでは、デバイスがトラフィックに対して実行したであろう処理を表示し、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することができます。
- インライン展開では、実際のトラフィックがデバイスに送信され、デバイスのポリシーがトラフィックに対する処理に影響します。不要なトラフィックがドロップされ、ポリシーによって適用されるその他のアクションが実行された後、トラフィックはさらなる処理と最終的な送信のために ASA に返されます。

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。

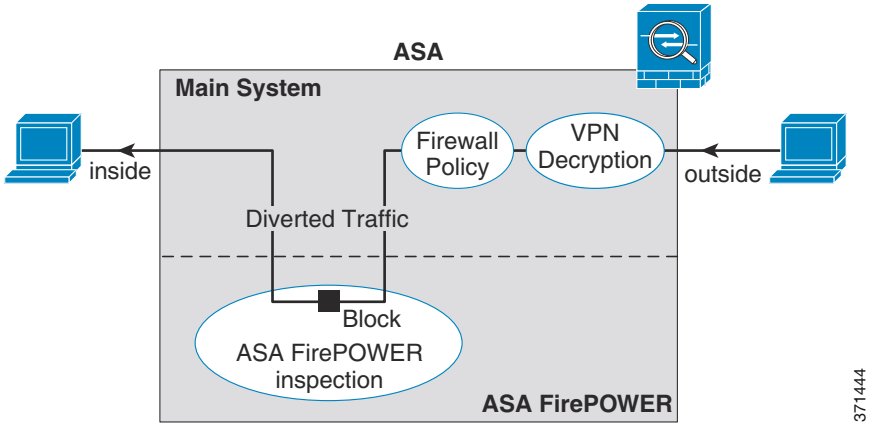
ASA FirePOWER インライン モード

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 インスペクションのトラフィックを識別する場合、トラフィックは次のように ASA およびモジュールを通過します。

1. トラフィックは 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 から出ます。

次の図に、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対して許可されていないトラフィックがモジュールによってブロックされます。それ以外のトラフィックは、ASA を通って転送されます。

図 17-1　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 パッシブ（モニタ専用）モード

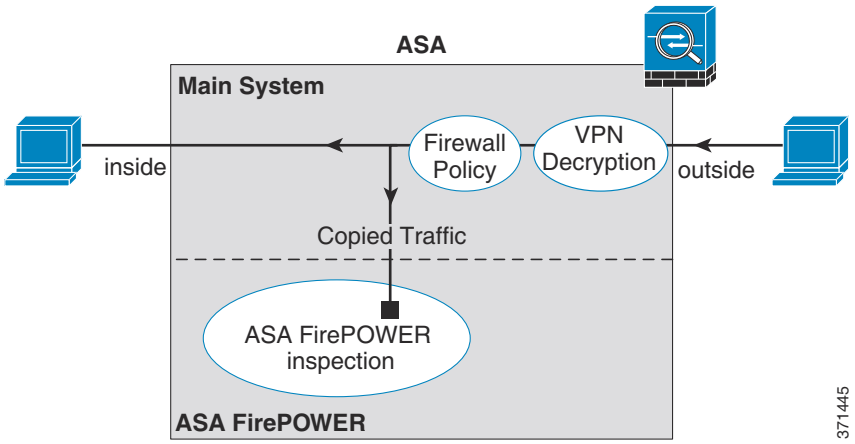
モニタ専用モードのトラフィック フローは、インライン モードのトラフィック フローと同じです。唯一の違いは、ASA FirePOWER モジュールが ASA に戻るトラフィックを通過させないことです。代わりに、モジュールはトラフィックにセキュリティ ポリシーを適用し、インライン モードで動作していた場合に実行したであろう処理をユーザに通知します。たとえば、トラフィックはイベントで「ドロップされていたはず」とマークされる場合があります。この情報をトラフィック分析に使用し、インライン モードが望ましいかどうかを判断するのに役立てることができます。

パッシブ モードを設定するには、モジュールにトラフィックをリダイレクトするサービス ポリシーに monitor-only という指示を追加します。

（注）　ASA 上で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。セキュリティ ポリシーの 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、あるコンテキストについてモニタ専用モードを設定し、それ以外のコンテキストについ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。

次の図に、パッシブ モードで動作している場合のトラフィック フローを示します。

図 17-2　ASA FirePOWER パッシブ（モニタ専用）モード



ASA FirePOWER 管理アクセス

ASA FirePOWER モジュールは、初期設定（およびそれ以降のトラブルシューティング）とポリシー管理の 2 つの独立したアクセス レイヤを使用して管理できます。

- 「初期設定」（P.17-4）
- 「ポリシー設定および管理」（P.17-5）

初期設定

初期設定には、ASA FirePOWER モジュールの CLI を使用する必要があります。デフォルトの管理アドレスの詳細については、「ASA FirePOWER のデフォルト」（P.17-7）を参照してください。

CLI にアクセスするには、次の方法を使用します。

- ASA 5585-X
  - ASA FirePOWER コンソール ポート：コンソール ポートは、独立した外部コンソール ポートです。
  - ASA FirePOWER Management 1/0 インターフェイス（SSH を使用）：デフォルトの IP アドレスに接続することも、ASDM を使用して管理 IP アドレスを変更してから SSH を使用して接続することもできます。モジュールの管理インターフェイスは、独立した外部ギガビット イーサネット インターフェイスです。

（注）　**session** コマンドを使用して ASA バックプレーンを介して ASA FirePOWER ハードウェア モジュール CLI にアクセスすることはできません。

- ASA 5512-X ～ ASA 5555-X
  - バックプレーンを経由した ASA セッション：ASA に CLI アクセスが可能な場合は、モジュールにセッション接続し、そのモジュール CLI にアクセスできます。
  - ASA FirePOWER Management 0/0 インターフェイス（SSH を使用）：デフォルトの IP アドレスに接続することも、ASDM を使用して管理 IP アドレスを変更してから SSH を使用して接続することもできます。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ます。ASA FirePOWER 管理インターフェイスは、Management 0/0 インターフェイスを ASA と共有します。ASA と ASA FirePOWER モジュールのそれぞれに別の MAC アドレスと IP アドレスがサポートされます。ASA FirePOWER IP アドレスの設定は、ASA FirePOWER オペレーティング システム内で（CLI または ASDM を使用して）実行する必要があります。ただし、物理特性（インターフェイスのイネーブル化など）は、ASA 上で設定されます。ASA インターフェイス コンフィギュレーションを削除して（特にインターフェイス名）、このインターフェイスを ASA FirePOWER 専用インターフェイスとすることができます。このインターフェイスは管理専用です。

ポリシー設定および管理

初期設定を実行した後で、FireSIGHT 管理センター を使用して ASA FirePOWER セキュリティ ポリシーを設定します。次に、ASDM または Cisco Security Manager を使用して、ASA FirePOWER モジュールにトラフィックを送信するための ASA ポリシーを設定します。

ASA の機能との互換性

ASA には、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、HTTP インスペクションもその一つです。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 FirePOWER モジュールの機能を最大限に活用するには、ASA FirePOWER モジュールに送信するトラフィックに関する次のガイドラインを参照してください。

- HTTP トラフィックに対して ASA インスペクションを設定しないでください。
- 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。同じトラフィックに対して ASA FirePOWER CX インスペクションおよびクラウド Web セキュリティ インスペクションの両方を設定した場合、ASA は ASA FirePOWER インスペクションのみを実行します。
- 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。
- Mobile User Security（MUS）サーバをイネーブルにしないでください。これは、ASA FirePOWER モジュールとの間に互換性がありません。
- フェールオーバーをイネーブルにしている場合、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 モジュールがその時点からトラフィックのインスペクションを開始します。古いインスペクションの状態は転送されません。

ASA FirePOWER モジュールのライセンス要件

ASA FirePOWER モジュールと FireSIGHT 管理センター には、追加のライセンスが必要です。これらのライセンスは、ASA のコンテキストではなく、モジュール自体にインストールする必要があります。ASA 自体には、追加ライセンスは必要ありません。

詳細については、『*FireSIGHT System User Guide*』または FireSIGHT 管理センター のオンラインヘルプの「Licensing」の章を参照してください。

ASA FirePOWER のガイドライン

フェールオーバーのガイドライン

フェールオーバーを直接サポートしていません。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 モジュールがその時点からトラフィックのインスペクションを開始します。古いインスペクションの状態は転送されません。

フェールオーバーの動作の一貫性を確保するために、高可用性 ASA ペアの ASA FirePOWER モジュールで一貫性のあるポリシーを維持する必要があります（FireSIGHT 管理センター を使用）。

ASA クラスタリングのガイドライン

このモジュールは、クラスタリングは直接サポートしていませんが、クラスタで使用できます。FireSIGHT 管理センター を使用して、クラスタの ASA FirePOWER モジュールで一貫性のあるポリシーを維持する必要があります。クラスタ内のデバイスに異なる ASA インターフェイス ベースのゾーン定義を使用しないでください。

モデルのガイドライン

- ASA 5585-X（ハードウェア モジュールとして）および 5512-X ～ ASA 5555-X（ソフトウェア モジュールとして）でサポートされています。詳細については、『*Cisco ASA Compatibility Matrix*』を参照してください。

  http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

- 5512-X ～ ASA 5555-X の場合は、シスコのソリッド ステート ドライブ（SSD）を実装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。

その他のガイドラインと制限事項

- 「ASA の機能との互換性」（P.17-5）を参照してください。
- 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のタイプの変更はできません。つまり、購入した ASA FirePOWER モジュールに、後で別のソフトウェアをインストールすることはできません。
- ASA 上で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。セキュリティ ポリシーの 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、あるコンテキストについてモニタ専用モードを設定し、それ以外のコンテキストについ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 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 17-1　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： – ASA 5585-X：Management 1/0 192.168.8.8/24 – ASA 5512-X ～ ASA 5555-X：Management 0/0 192.168.1.2/24
ゲートウェイ	• システム ソフトウェア イメージ：なし • ブート イメージ： – ASA 5585-X：192.168.8.1/24 – ASA 5512-X ～ ASA 5555-X：192.168.1.1/24
SSH またはセッションのユーザ名	admin
パスワード	• システム ソフトウェア イメージ：**Sourcefire** • ブート イメージ：**Admin123**

ASA FirePOWER モジュールの設定

ASA FirePOWER モジュールの設定は、トラフィックを ASA FirePOWER モジュールに送信するための ASA FirePOWER モジュールでの ASA FirePOWER セキュリティ ポリシーの設定、およびその後の ASA の設定を含むプロセスです。ASA FirePOWER モジュールを設定するには、次の手順に従います。

ステップ 1　「ASA FirePOWER 管理インターフェイスの接続」（P.17-8）。ケーブルで ASA FirePOWER 管理インターフェイスに接続します（任意でコンソール インターフェイスにも）。

ステップ 2　「（ASA 5512-X ～ 5555-X）ソフトウェア モジュールのインストールまたはイメージの再作成」（P.17-11）。

ステップ 3　必要に応じて、「ASA FirePOWER 管理 IP アドレスの変更」（P.17-15）。これは最初の SSH アクセスに必要になる場合があります。

ステップ 4　「ASA FirePOWER CLI での基本的な ASA FirePOWER 設定値の設定」（P.17-15）。これは ASA FirePOWER モジュールで行います。

ステップ 5　「FireSIGHT 管理センター への ASA FirePOWER の追加」（P.17-17）。これはデバイスを管理する FireSIGHT 管理センター を指定します。

ステップ 6　「ASA FirePOWER モジュールへのセキュリティ ポリシーの設定」（P.17-18）。

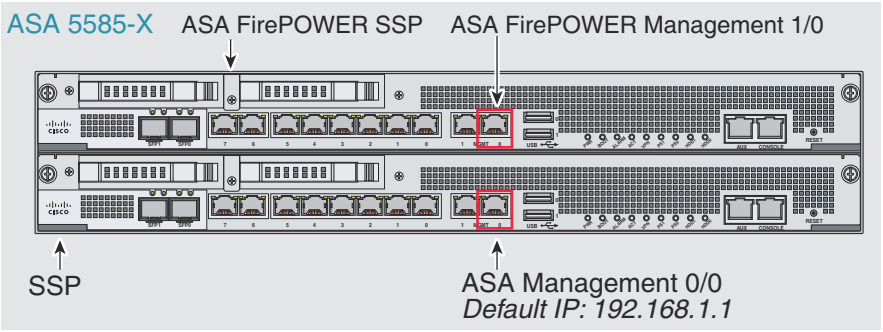
ステップ 7　「ASA FirePOWER モジュールへのトラフィックのリダイレクト」（P.17-18）。

ASA FirePOWER 管理インターフェイスの接続

ASA FirePOWER モジュールへの管理アクセスを提供する以外に、ASA FirePOWER 管理インターフェイスは、HTTP プロキシ サーバまたは DNS サーバおよびインターネットへのアクセスを必要とします。これは、シグニチャ アップデートなどのためです。この項では、推奨されるネットワーク コンフィギュレーションを示します。実際のネットワークでは、異なる可能性があります。

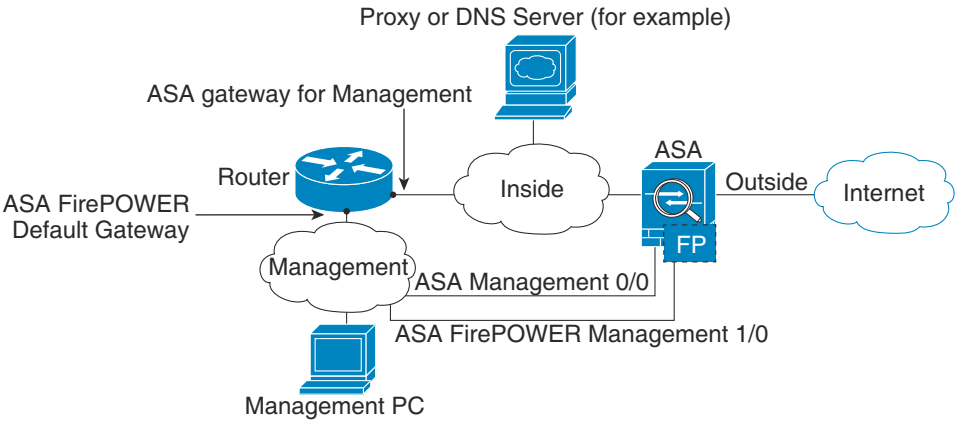
ASA 5585-X（ハードウェア モジュール）

ASA FirePOWER モジュールには、ASA とは別の管理およびコンソール インターフェイスが含まれます。初期設定を行うには、デフォルト IP アドレスを使用して ASA FirePOWER Management 1/0 インターフェイスに SSH で接続できます。デフォルト IP アドレスを使用できない場合は、コンソール ポートを使用するか、ASDM を使用して SSH を使用できるように管理 IP アドレスを変更します（「ASA FirePOWER 管理 IP アドレスの変更」（P.17-15）を参照）。



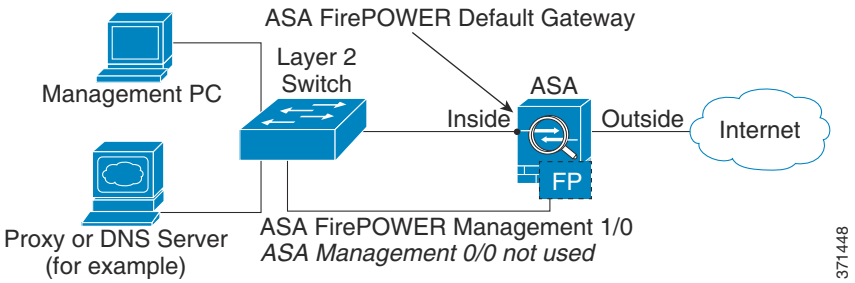
内部ルータがある場合

内部ルータがある場合は、管理ネットワーク（これには ASA Management 0/0 インターフェイスおよび ASA FirePOWER Management 1/0 インターフェイスの両方を含めることができます）と ASA 内部ネットワークとの間でルーティングできます（インターネット アクセス用）。必ず、内部ルータを介して管理ネットワークに到達するためのルートを ASA に追加してください。



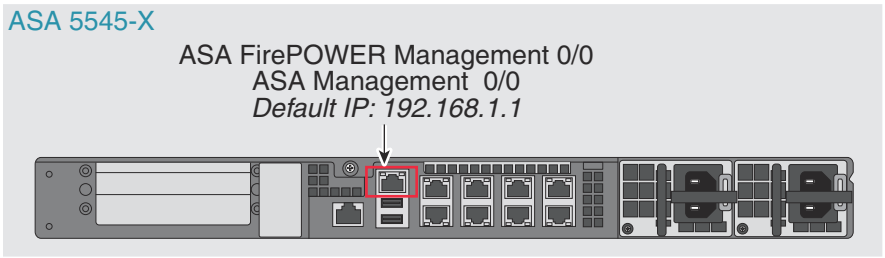
内部ルータがない場合

内部ネットワークが 1 つだけの場合は、別の管理ネットワークも持つことはできません（仮に持つとすれば、内部ルータがネットワーク間のルーティングを行う必要があります）。この場合は、Management 0/0 インターフェイスの代わりに内部インターフェイスから ASA を管理できます。ASA FirePOWER モジュールは ASA とは別のデバイスであるため、内部インターフェイスと同じネットワーク上に ASA FirePOWER Management 1/0 アドレスを設定できます。



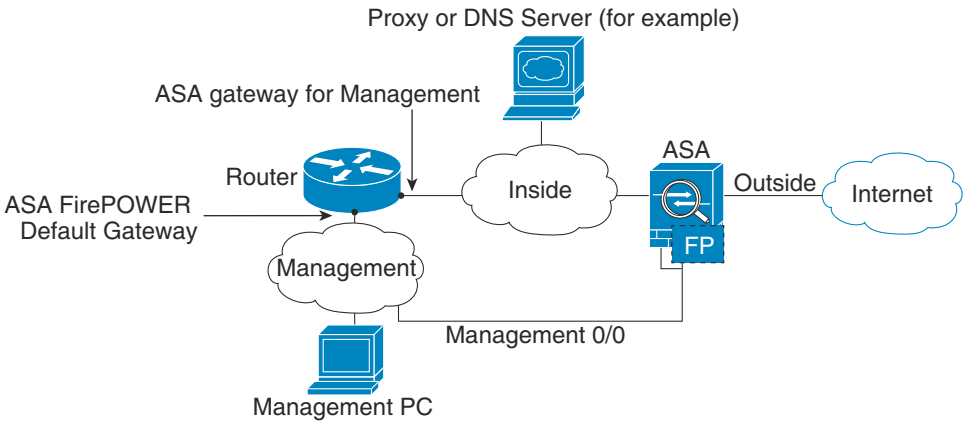
ASA 5512-X ～ ASA 5555-X（ソフトウェア モジュール）

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 管理インターフェイスは Management 0/0 インターフェイスを ASA と共有します。初期設定を行うには、デフォルト IP アドレスを使用して ASA FirePOWER に SSH で接続できます。デフォルト IP アドレスを使用できない場合は、バックプレーンを経由して ASA FirePOWER にセッション接続するか、ASDM を使用して SSH を使用できるように管理 IP アドレスを変更します。



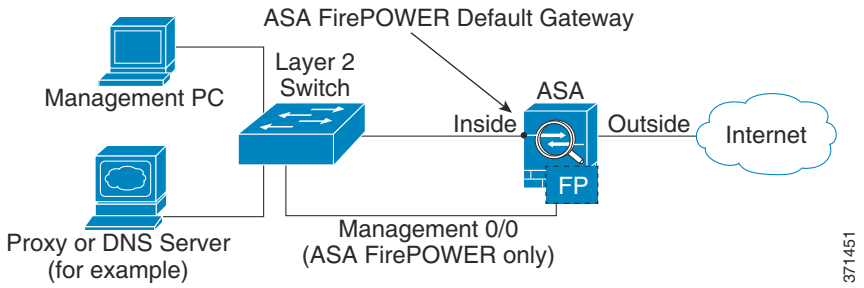
内部ルータがある場合

内部ルータがある場合、Management 0/0 ネットワーク間でルーティングできます。これには、ASA および ASA FirePOWER の両方の管理 IP アドレス、およびインターネット アクセス用の内部ネットワークが含まれます。必ず、内部ルータを介して管理ネットワークに到達するためのルートを ASA に追加してください。



内部ルータがない場合

内部ネットワークが 1 つだけの場合は、別の管理ネットワークも持つことはできません。この場合は、Management 0/0 インターフェイスの代わりに内部インターフェイスから ASA を管理できます。ASA で設定された名前を Management 0/0 インターフェイスから削除した場合も、そのインターフェイスの ASA FirePOWER IP アドレスを設定できます。ASA FirePOWER モジュールは実質的に ASA とは別のデバイスであるため、内部インターフェイスと同じネットワーク上に ASA FirePOWER 管理アドレスを設定できます。



（注）　Management 0/0 に対して ASA で設定された名前を削除する必要があります。この名前が ASA 上で設定されている場合は、ASA FirePOWER のアドレスは ASA と同じネットワーク上にあることが必要になり、その結果、他の ASA インターフェイス上ですでに設定されたネットワークが除外されます。名前が設定されていない場合は、ASA FirePOWER のアドレスが存在するのはどのネットワークでも、たとえば、ASA 内部ネットワークでもかまいません。

（ASA 5512-X ～ 5555-X）ソフトウェア モジュールのインストールまたはイメージの再作成

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、この手順に従って ASA FirePOWER ブート ソフトウェアをインストールし、SSD を分割して、システム ソフトウェアをインストールする必要があります。

モジュールのイメージを再作成する手順は、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ことを除いてこれと同じです。システムのイメージの再作成は、SSD を交換する場合に行います。

物理的に SSD を取り付ける方法の詳細については、『ASA Hardware Guide』を参照してください。

はじめる前に

- フラッシュ（disk0）の空き領域には、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。
- 実行している可能性があるその他のソフトウェア モジュールをシャットダウンする必要があります。デバイスでは、一度に 1 つのソフトウェア モジュールを実行できます。これは ASA CLI から実行する必要があります。たとえば、次のコマンドはIPS モジュール ソフトウェアをシャット ダウンして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コマンドは、**ips** の代わりに **cxsc** キーワードを使用することを除いてこのコマンドと同じです。

```
hostname# sw-module module ips shutdown
hostname# sw-module module ips uninstall
hostname# reload
```

（注）　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、**noservice-policy** *ips_policy* **global** を使用します。ポリシーは、CLI または ASDM を使用して削除できます。

- モジュールのイメージを再作成する場合は、同じシャットダウン/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。
- ASA FirePOWER のブート イメージとシステム ソフトウェア パッケージの両方を Cisco.com から取得します。

手順

ステップ 1　ブート イメージをデバイスに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：まず、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、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] の順に選択し、[Between Local PC and Flash] または [Between Remote Server and Flashnd] のいずれか該当する [File Transfer] コマンドを選択します。ブート ソフトウェアを ASA 上の disk0 に転送します。
- ASA CLI：まず、ブート イメージを TFTP、FTP、HTTP、または HTTPS サーバに配置し、**copy** コマンドを使用してそのブート イメージをフラッシュにダウンロードします。次の例では TFTP を使用しています。<TFTP Server> をお使いのサーバの IP アドレスまたはホスト名に置き換えてください。

```
ciscoasa# copy tftp://<TFTP SERVER>/asasfr-5500x-boot-5.3.1-58.img
disk0:/asasfr-5500x-boot-5.3.1-58.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。

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。

```
hostname# sw-module module sfr recover configure image disk0:file_path
```

（注）「ERROR: Another service (cxsc) is running, only one service is allowed to run at any time」というメッセージが表示される場合は、すでに別のソフトウェア モジュールが設定されています。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。

例：

```
hostname# sw-module module sfr recover configure image
disk0:asasfr-5500x-boot-5.3.1-58.img
```

ステップ 4　次のコマンドを入力して、ASA FirePOWER ブート イメージをロードします。

```
hostname# 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 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。ログイン プロンプトを表示するには、セッションを開いた後に 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
```

ヒント　モジュールのブートが完了していない場合は、**session** コマンドが失敗し、ttyS1 経由で接続できないことに関するメッセージが表示されます。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、**setup** コマンドを使用してシステムを設定します。

```
asasfr-boot> setup


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

次の項目を指定するように求められます。主な設定項目は、管理アドレスとゲートウェイ、および DNS 情報です。

- ホスト名：65 文字までの英数字で、スペースは使用できません。ハイフンを使用できます。
- ネットワーク アドレス：スタティック IPv4 または IPv6 アドレスを設定するか、または DHCP （IPv4 の場合）または IPv6 ステートレス自動設定を使用することができます。
- DNS 情報：少なくとも 1 つの DNS サーバを指定する必要があります。ドメイン名と検索ドメインを設定することもできます。
- NTP 情報：システム時刻を設定するために、NTP をイネーブルにして NTP サーバを設定することができます。

ステップ 7　**system install** コマンドを使用してシステム ソフトウェア イメージをインストールします。

system install [**noconfirm**] *url*

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 を使用してください。ユーザ名とパスワードが必要な場合は、それらを指定するように求められます。

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 サービスの起動には 10 分以上かかります（**show module sfr** の出力で、すべてのプロセスがアクティブであると表示される必要があります）。

次に例を示します。

```
asasfr-boot> system install http://asasfr-sys-5.3.1-44.pkg
Verifying
Downloading
Extracting
Package Detail
        Description:                    Cisco ASA-FirePOWER 5.3.1-44 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.
(Enter キーを押します)
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しようとしているため、別のログイン プロンプトが表示されます。

```
asa3# session sfr
Opening command session with module sfr.
Connected to module sfr.Escape character sequence is 'CTRL-^X'.

Sourcefire ASA5555 v5.3.1 (build 44)
Sourcefire3D login:
```

ステップ 9　ユーザ名 **admin** およびパスワード **Sourcefire** を使用してログインします。

ステップ 10　プロンプトに従ってシステム設定を完了します。

まず、エンド ユーザ ライセンス契約（EULA）を読み、これに同意する必要があります。次に、プロンプトに従って管理者パスワードを変更し、管理アドレスと DNS 設定を設定します。IPv4 と IPv6 の両方の管理アドレスを設定できます。次に例を示します。

```
System initialization in progress.Please stand by.
You must change the password for 'admin' to continue.
Enter new password: <新しいパスワード>
Confirm new password: <パスワードの再入力>
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'
(システムが自動的に再設定されるまで待機します)

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 11　**configure manager add** コマンドを使用して、このデバイスを管理する FireSIGHT 管理センター アプライアンスを指定します。

登録キーを考え出します。このキーは、デバイスをインベントリに追加するときに FireSIGHT 管理センター で使用します。次に、簡単な例を示します。NAT 境界がある場合は、コマンドが異なります。「FireSIGHT 管理センター への ASA FirePOWER の追加」（P.17-17）を参照してください。

```
> configure manager add 10.89.133.202 123456
Manager successfully configured.
```

ステップ 12　上で入力したホスト名またはアドレスを使用し、ブラウザで HTTPS 接続を使用して FireSIGHT 管理センター にログインします。たとえば、https://DC.example.com などです。

[Device Management]（[Devices] > [Device Management]）ページでデバイスを追加します。詳細については、オンライン ヘルプまたは『*FireSIGHT System User Guide*』の「Managing Devices」の章を参照してください。

ヒント　また、FireSIGHT 管理センター で NTP と時刻設定も設定します。時刻同期設定は、[System] > [Local] > [System Policy] ページからローカル ポリシーを編集する場合に使用します。

ASA FirePOWER 管理 IP アドレスの変更

デフォルトの管理 IP アドレスを使用できない場合、ASA から管理 IP アドレスを設定できます。管理 IP アドレスを設定した後は、追加設定を実行するために SSH を使用して ASA FirePOWER モジュールにアクセスできます。

システムの初期設定時に「ASA FirePOWER CLI での基本的な ASA FirePOWER 設定値の設定」（P.17-15）の説明に従って ASA FirePOWER CLI で管理アドレスをすでに設定している場合は、ASA CLI または ASDM で管理アドレスを設定する必要はありません。

（注）　ソフトウェア モジュールの場合、ASA FirePOWER CLI にアクセスして、ASA CLI からのセッション接続によって設定を実行できます。その後、設定の一部として ASA FirePOWER 管理 IP アドレスを設定できます。ハードウェア モジュールの場合は、コンソール ポートを使用して初期設定を完了できます。

ASA で管理 IP アドレスを変更するには、次のいずれかを実行します。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。

- CLI で、ASA FirePOWER 管理 IP アドレス、マスク、およびゲートウェイを設定するには、次のコマンドを使用します。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。

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

  たとえば、**session 1 do setup host ip 10.1.1.2/24,10.1.1.1** と指定します。

- ASDM で、[Wizards] > [Startup Wizard] の順に選択し、ウィザードで [ASA FirePOWER Basic Configuration] に進みます。このページでは、IP アドレス、マスク、およびデフォルト ゲートウェイを設定できます。

ASA FirePOWER CLI での基本的な ASA FirePOWER 設定値の設定

セキュリティ ポリシーを設定する前に、基本的なネットワーク設定およびその他のパラメータを ASA FirePOWER モジュール上で設定する必要があります。この手順では、完全なシステム ソフトウェア（ブート イメージだけでなく）がインストールされていること（直接インストールしたか、ハードウェア モジュールにインストール済みであること）を前提としています。

ヒント　この手順では、初期設定を実行していることも前提としています。初期設定時に、これらの設定を行うように求められます。これらの設定を後で変更する必要がある場合は、各種の **configure network** コマンドを使用して個々の設定を変更します。**configure network** コマンドの詳細については、**?** コマンドを使用してヘルプを表示し、『*FireSIGHT System User Guide*』または FireSIGHT 管理センター のオンライン ヘルプを参照してください。

手順

ステップ 1　次のどちらかを実行します。

- （すべてのモデル）SSH を使用して ASA FirePOWER 管理 IP アドレスに接続します。
- （ASA 5512-X ～ ASA 5555-X）ASA CLI からモジュールへのセッションを開きます（ASA CLI にアクセスするには、一般的な操作のコンフィギュレーション ガイドの「Getting Started」の章を参照してください）。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。

```
hostname# session sfr
```

ステップ 2　ユーザ名 **admin** およびパスワード **Sourcefire** を使用してログインします。

ステップ 3　プロンプトに従ってシステム設定を完了します。

まず、エンド ユーザ ライセンス契約（EULA）を読み、これに同意する必要があります。次に、プロンプトに従って管理者パスワードを変更し、管理アドレスと DNS 設定を設定します。IPv4 と IPv6 の両方の管理アドレスを設定できます。センサーは FireSIGHT 管理センター で管理する必要があるというメッセージが表示されたら、設定は完了です。

次に例を示します。

```
System initialization in progress.Please stand by.
You must change the password for 'admin' to continue.
Enter new password: <新しいパスワード>
Confirm new password: <パスワードの再入力>
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'
(システムが自動的に再設定されるまで待機します)

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 4　ここで、「FireSIGHT 管理センター への ASA FirePOWER の追加」（P.17-17）の説明に従って、このデバイスを管理する FireSIGHT 管理センター を指定する必要があります。

FireSIGHT 管理センター への ASA FirePOWER の追加

モジュールにポリシーを設定するためのアプリケーションである ASA FirePOWER に FireSIGHT 管理センター モジュールを登録する必要があります。FireSIGHT 管理センター は防御センターとも呼ばれます。

デバイスを登録するには、**configure manager add** コマンドを使用します。FireSIGHT 管理センター にデバイスを登録するには、一意の英数字の登録キーが常に必要です。これはユーザが指定する簡単なキーで、ライセンス キーと同じではありません。

ほとんどの場合、FireSIGHT 管理センター のホスト名または IP アドレスを登録キーと一緒に指定する必要があります。次に例を示します。

```
configure manager add DC.example.com my_reg_key
```

ただし、デバイスと FireSIGHT 管理センター が NAT デバイスによって分離されている場合、一意の NAT ID を登録キーと一緒に入力し、ホスト名の代わりに DONTRESOLVE を指定します。次に例を示します。

```
configure manager add DONTRESOLVE my_reg_key my_nat_id
```

手順

ステップ 1　次のどちらかを実行します。

- （すべてのモデル）SSH を使用して ASA FirePOWER 管理 IP アドレスに接続します。
- （ASA 5512-X ～ ASA 5555-X）ASA CLI からモジュールへのセッションを開きます（ASA CLI にアクセスするには、一般的な操作のコンフィギュレーション ガイドの「Getting Started」の章を参照してください）。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。

  ```
  hostname# session sfr
  ```

ステップ 2　ユーザ名 **admin** または CLI コンフィギュレーション（管理者）アクセス レベルを持つ別のユーザ名でログインします。

ステップ 3　プロンプトで、**configure manager add** コマンドを使用して FireSIGHT 管理センター にデバイスを登録します。このコマンドの構文は次のとおりです。

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

それぞれの説明は次のとおりです。

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} では、FireSIGHT 管理センター の完全修飾名または IP アドレスを指定します。FireSIGHT 管理センター のアドレスを直接指定できない場合は、DONTRESOLVE を使用します。

- *reg_key* は、FireSIGHT 管理センター にデバイスを登録するために必要な一意の英数字の登録キーです。
- *nat_id* は、FireSIGHT 管理センター とデバイス間の登録プロセス中に使用されるオプションの英数字の文字列です。これは、ホスト名が DONTRESOLVE に設定されている場合に必要です。

ステップ 4　上で入力したホスト名またはアドレスを使用し、ブラウザで HTTPS 接続を使用して FireSIGHT 管理センター にログインします。たとえば、https://DC.example.com などです。

[Device Management]（[Devices] > [Device Management]）ページでデバイスを追加します。詳細については、オンライン ヘルプまたは『*FireSIGHT System User Guide*』の「Managing Devices」の章を参照してください。

ASA FirePOWER モジュールへのセキュリティ ポリシーの設定

ASA FirePOWER モジュールにセキュリティ ポリシーを設定するには、FireSIGHT 管理センター を使用します。セキュリティ ポリシーは、次世代 IPS フィルタリングやアプリケーション フィルタリングなど、モジュールによって提供されるサービスを制御します。ASA FirePOWER CLI、ASA CLI、または ASDM を使用してポリシーを設定することはできません。

FireSIGHT 管理センター を開くには、Web ブラウザを使用して次の URL を開きます。

https://*DC_address*

DC_address は、「FireSIGHT 管理センター への ASA FirePOWER の追加」（P.17-17）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 などです。

セキュリティ ポリシーの設定方法については、『*FireSIGHT System User Guide*』または FireSIGHT 管理センター のオンライン ヘルプを参照してください。

ヒント　FireSIGHT 管理センター は、ASDM の [ASA FirePOWER Status] ダッシュボードから開くこともできます。[Home] > [ASA FirePOWER Status] を選択して、ダッシュボードの下部にあるリンクをクリックします。

ASA FirePOWER モジュールへのトラフィックのリダイレクト

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、ASA FirePOWER モジュールへのトラフィックをリダイレクトします。

デバイスは、パッシブ（「モニタ専用」）展開またはインライン展開のいずれかで設定できます。

- パッシブ展開では、トラフィックのコピーがデバイスに送信されますが、ASA には返されません。パッシブ モードでは、デバイスがトラフィックに対して実行したであろう処理を表示し、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することができます。
- インライン展開では、実際のトラフィックがデバイスに送信され、デバイスのポリシーがトラフィックに対する処理に影響します。不要なトラフィックがドロップされ、ポリシーによって適用されるその他のアクションが実行された後、トラフィックはさらなる処理と最終的な送信のために ASA に返されます。

（注）　ASA 上で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。セキュリティ ポリシーの 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、あるコンテキストについてモニタ専用モードを設定し、それ以外のコンテキストについ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。

はじめる前に

- （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 には、必ず一貫性のあるポリシーを設定してください（FireSIGHT 管理センター を使用）。両方のポリシーに、トラフィックのパッシブ モードまたはインライン モードを反映させる必要があります。
- 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、セキュリティ 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）」（P.1-14）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（パッシブ 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 パッシブ（モニタ専用）モード」（P.17-3）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、ポリシーに対して別のクラスを指定し、**sfr** リダイレクト処理を適用できます。

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」（P.1-5）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 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。

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。

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、**session do** コマンドを使用して ASA から管理者パスワードをリセットできます。

ヒント　ASA 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。

ユーザ **admin** のモジュール パスワードをデフォルトの **Sourcefire** にリセットするには、次のコマンドを使用します。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。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。

```
session {1 | sfr} do password-reset
```

たとえば、**session sfr do password-reset** を使用します。

モジュールのリロードまたはリセット

モジュールをリロード、またはリセットしてからリロードするには、ASA CLI で次のいずれかのコマンドを入力します。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。

- ハードウェア モジュール（ASA 5585-X）：

  ```
  hw-module module 1 {reload | reset}
  ```

- ソフトウェア モジュール（ASA 5512-X ～ ASA 5555-X）：

  ```
  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。モジュールをグレースフル シャットダウンするには、ASA CLI で次のいずれかのコマンドを入力します。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。

（注）　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。

- 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（ASA 5512-X ～ ASA 5555-X）：

  ```
  sw-module module sfr shutdown
  ```

（ASA 5512-X ～ ASA 5555-X）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。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。

```
hostname# 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。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。

```
hostname# reload
```

（ASA 5512-X ～ ASA 5555-X）ASA からモジュールへのセッション

基本的なネットワーク設定を構成し、モジュールをトラブルシューティングするには、ASA FirePOWER CLI を使用します。

ASA FirePOWER ソフトウェア モジュール CLI に ASA からアクセスするには、ASA からセッションを開始します。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とパスワード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ユーザ名は、フル イメージの場合は **Sourcefire**、ブート イメージの場合は **Admin123** です。

- 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て、ASA プロンプトに戻るための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、ターミナル サーバ プロンプトまで終了することになります。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。

5585-X ASA FirePOWER ハードウェア モジュールのイメージの再作成

何らかの理由で ASA FirePOWER ASA 5585-X アプライアンスのハードウェア 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。

TFTP ブートを行うには、次の手順を実行します。

- ソフトウェア イメージを、ASA FirePOWER 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。
- ROMmon 変数を設定する。ROMmon 変数を設定するには、Esc キーを押して自動ブート プロセスを中断します。

ブート イメージがインストールされたら、システム ソフトウェア パッケージをインストールします。ASA FirePOWER からアクセス可能な HTTP、HTTPS、または FTP サーバに、パッケージを配置する必要があります。

次の手順では、ブート イメージをインストールしてからシステム ソフトウェア パッケージをインストールする方法を説明します。

手順

ステップ 1　コンソール ポートに接続します。ASA 製品に付属のコンソール ケーブルを使用し、9600 ボー、8 データ ビット、パリティなし、1 ストップ ビット、フロー制御なしに設定されたターミナル エミュレータを用いて PC をコンソールに接続します。コンソール ケーブルの詳細については、ASA のハードウェア ガイドを参照してください。

ステップ 2　**system reboot** コマンドを入力してシステムをリロードします。

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、**set** を入力して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。

次に例を示します。

```
ADDRESS=10.5.190.199
SERVER=10.5.11.170
GATEWAY=10.5.1.1
IMAGE=asasfr-boot-5.3.1-26-54.img
```

ステップ 5　**sync** を入力して設定を保存します。

ステップ 6　**tftp** を入力してダウンロードおよびブート プロセスを開始します。

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、**setup** コマンドを使用してシステムを設定します。

次の項目を指定するように求められます。主な設定項目は、管理アドレスとゲートウェイ、および DNS 情報です。

- ホスト名：65 文字までの英数字で、スペースは使用できません。ハイフンを使用できます。
- ネットワーク アドレス：スタティック IPv4 または IPv6 アドレスを設定するか、または DHCP （IPv4 の場合）または IPv6 ステートレス自動設定を使用することができます。
- DNS 情報：少なくとも 1 つの DNS サーバを指定する必要があります。ドメイン名と検索ドメインを設定することもできます。
- NTP 情報：システム時刻を設定するために、NTP をイネーブルにして NTP サーバを設定することができます。

ステップ 9　**system install** コマンドを使用してシステム ソフトウェア イメージをインストールします。

system install [**noconfirm**] *url*

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 分以上かかります次に例を示します。

```
asasfr-boot> system install http://asasfr-sys-5.3.1-54.pkg
```

ステップ 10　ブートが完了したら、パスワード **Sourcefire** を使用して **admin** としてログインします。

プロンプトに従ってシステム設定を完了します。

まず、エンド ユーザ ライセンス契約（EULA）を読み、これに同意する必要があります。次に、プロンプトに従って管理者パスワードを変更し、管理アドレスと DNS 設定を設定します。IPv4 と IPv6 の両方の管理アドレスを設定できます。

ステップ 11　**configure manager add** コマンドを使用して、このデバイスを管理する FireSIGHT 管理センター アプライアンスを指定します。

登録キーを考え出します。このキーは、デバイスをインベントリに追加するときに FireSIGHT 管理センター で使用します。次に、簡単な例を示します。NAT 境界がある場合は、コマンドが異なります。「FireSIGHT 管理センター への ASA FirePOWER の追加」（P.17-17）を参照してください。

```
> configure manager add 10.89.133.202 123456
Manager successfully configured.
```

ステップ 12　上で入力したホスト名またはアドレスを使用し、ブラウザで HTTPS 接続を使用して FireSIGHT 管理センター にログインします。たとえば、https://DC.example.com などです。

[Device Management]（[Devices] > [Device Management]）ページでデバイスを追加します。詳細については、『*FireSIGHT System User Guide*』または FireSIGHT 管理センター のオンライン ヘルプの「Managing Devices」の章を参照してください。

システム ソフトウェアのアップグレード

FireSIGHT 管理センター を使用して ASA FirePOWER モジュールにアップグレード イメージを適用します。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の詳細については、『*FireSIGHT System User Guide*』または FireSIGHT 管理センター のオンライン ヘルプを参照してください。

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」（P.17-25）
- 「モジュールの統計情報の表示」（P.17-27）
- 「モジュール接続のモニタリング」（P.17-27）

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表示するには、1（ハードウェア モジュールの場合）または 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。DC Addr は、このデバイスを管理する FireSIGHT 管理センター 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-5.3.1-44.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。

```
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
```

次に、モニタ専用ポリシーを表示する例を示します。この場合、パケット入力カウンタは増加しますが、ASA に戻されるトラフィックはないので、パケット出力カウンタはゼロのままです。

```
hostname# show service-policy sfr
Global policy:
Service-policy: global_policy
    Class-map: bypass
      SFR: card status Up, mode fail-open, monitor-only
        packet input 2626422041, packet output 0, 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 コマンドには、ASA FirePOWER モジュールに関連する次のドロップの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
```

次に、10.1.1.0 ネットワークおよび 10.2.1.0 ネットワーク宛てのすべての IP 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に障害が発生してもすべてのトラフィックを許可する例を示します。

```
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

機能名	プラットフォームリリース	機能情報
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。