

ASA プラットフォームでの FirePOWER サービス モジュールのインストールと設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[はじめに](#)

[インストール](#)

[ASA への SFR モジュールのインストール](#)

[ASA SFR ブート イメージの設定](#)

[設定](#)

[FirePOWER ソフトウェアの設定](#)

[FireSIGHT Management Center の設定](#)

[SFR モジュールへのトラフィックのリダイレクト](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

はじめに

このドキュメントでは、Cisco ASAにCiscoFirepower(SFR)モジュールをインストールして設定し、Cisco FireSIGHTにSFRモジュールを登録する方法について説明します。

前提条件

要件

このドキュメントで説明している手順を開始する前に、次の推奨要件を満たしていることを確認してください。

- フラッシュ ドライブ (disk0) に 3GB 以上の空き領域とブート ソフトウェアのサイズ分の領域があることを確認します。
- 特権 EXEC モードにアクセスできることを確認します。特権EXECモードにアクセスするには、 `enable` コマンドをCLIに入力します。パスワードが設定されていない場合は、 `Enter`:

```
<#root>
```

```
ciscoasa>
```


enable

Password:
ciscoasa#

使用するコンポーネント

Cisco ASAにFirepowerサービスをインストールするには、次のコンポーネントが必要です。

- Cisco ASA ソフトウェア バージョン 9.2.2 以降
- Cisco ASA プラットフォーム 5512-X ~ ASA 5555-X
- Firepowerソフトウェアバージョン5.3.1以降

 注:Firepower(SFR)サービスをASA 5585-X Hardware Moduleにインストールする場合は、「[ASA 5585-X Hardware ModuleへのSFRモジュールのインストール](#)」を参照してください。

Cisco FireSIGHT Management Center には次のコンポーネントが必要です。


- Firepowerソフトウェアバージョン5.3.1以降
- FireSIGHT Management Center FS2000、FS4000、または仮想アプライアンス

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Cisco ASAFirepowerモジュールはASA SFRとも呼ばれ、次のような次世代ファイアウォールサービスを提供します。

- 次世代侵入防御システム (NGIPS)
- アプリケーションの可視性と制御 (AVC)
- URLのフィルタ
- Advanced Malware Protection (AMP)

 注:ASA SFRモジュールは、シングルコンテキストモードまたはマルチコンテキストモード、およびルーテッドモードまたはトランスペアレントモードで使用できます。

はじめに

このドキュメントで説明している手順を開始する前に、次の重要情報を考慮してください。

- 侵入防御システム (IPS) またはコンテキスト アウェア (CX) モジュール (ASA SFR と交換したモジュール) 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、そのポリシーを削除してから、ASA SFR サービス ポリシーを設定する必要があります。

- 現在動作している他のソフトウェア モジュールをシャットダウンする必要があります。デバイスは一度に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 ソフトウェア モジュール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。

```
<#root>
```

```
ciscoasa#
```

```
sw-module module ips shutdown
```

```
ciscoasa#
```

```
sw-module module ips uninstall
```

```
ciscoasa#
```

```
reload
```

- CXモジュールを削除するために使用するコマンドは、`cxsc` キーワードが使用されます。
 - ips:

```
<#root>
```

```
ciscoasa#
```

```
sw-module module cxsc shutdown
```

```
ciscoasa#
```

```
sw-module module cxsc uninstall
```

```
ciscoasa#
```

```
reload
```

- モジュールを再イメージ化する場合は、同じ `shutdown` と `uninstall` 古いSFRイメージを削除するために使用するコマンド。ランダム データの例は次のとおりです。


```
<#root>
```

```
ciscoasa#
```

```
sw-module module sfr uninstall
```

- ASA SFR モジュールをマルチ コンテキスト モードで使用する場合は、このドキュメントで説明している手順を、システム実行スペース内で実行します。

 ヒント:ASA上のモジュールのステータスを確認するには、`show module` コマンドを使用して、

 アップグレードを実行します。


インストール

このセクションでは、ASAにSFRモジュールをインストールする方法と、ASA SFRブートイメージをセットアップする方法について説明します。

ASA への SFR モジュールのインストール

ASA に SFR モジュールをインストールするには、次の手順を実行します。

1. ASA SFR 管理インターフェイスからアクセスできる HTTP、HTTPS、または FTP サーバへ、Cisco.com から ASA SFR システム ソフトウェアをダウンロードします。
2. ブート イメージをデバイスにダウンロードします。ブート イメージをデバイスにダウンロードするには、Cisco Adaptive Security Device Manager (ASDM) または ASA CLI を使用します。

 注：システムソフトウェアは転送しないでください。後でソリッドステートドライブ (SSD)にダウンロードします。

ASDM を介してブート イメージをダウンロードするには、次の手順を実行します。

- a. 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、サーバ メッセージ ブロック (SMB)、またはセキュア コピー (SCP) サーバに配置します。
- b. 選択 **Tools > File Management** ASDM内に配置します。
- c. 適切なファイル転送コマンド ([Between Local PC and Flash] または [Between Remote Server and Flash]) を選択します。
- d. ブート ソフトウェアを ASA 上のフラッシュ ドライブ (disk0) に転送します。

ASA CLI を介してブート イメージをダウンロードするには、次の手順を実行します。

- a. FTP、TFTP、HTTP、または HTTPS サーバでブート イメージをダウンロードします。
- b. config コマンドを入力します copy コマンドをCLIに入力して、ブートイメージをフラッシュドライブにダウンロードします。

HTTPプロトコルを使用する例を次に示します(HTTPサーバのサーバのIPアドレスまたはホスト名を使用)。FTPサーバの場合、URLは次のようになります。ftp://username:password@server-ip/asasfr-5500x-boot-5.3.1-152.img を参照。

```
<#root>  
ciscoasa#  
copy http://
```

```
        /asasfr-5500x-boot-5.3.1-152.img  
disk0:/asasfr-5500x-boot-5.3.1-152.img
```

3. ASA フラッシュ ドライブ上の ASA SFR ブート イメージの場所を設定するため、次のコマンドを入力します。

```
<#root>  
ciscoasa#  
sw-module module sfr recover configure image disk0:/file_path
```

ランダム データの例は次のとおりです。

```
<#root>  
ciscoasa#  
sw-module module sfr recover configure image disk0:  
/asasfr-5500x-boot-5.3.1-152.img
```

4. ASA SFR ブート イメージをロードするには、次のコマンドを入力します。

```
<#root>  
ciscoasa#  
sw-module module sfr recover boot
```

この間にCLIで `debug module-boot asa` では、次のデバッグが出力されます。

```
Mod-sfr 788> *** EVENT: Creating the Disk Image...  
Mod-sfr 789> *** TIME: 05:50:26 UTC Jul 1 2014  
Mod-sfr 790> ***  
Mod-sfr 791> ***  
Mod-sfr 792> *** EVENT: The module is being recovered.  
Mod-sfr 793> *** TIME: 05:50:26 UTC Jul 1 2014  
Mod-sfr 794> ***  
...  
Mod-sfr 795> ***  
Mod-sfr 796> *** EVENT: Disk Image created successfully.  
Mod-sfr 797> *** TIME: 05:53:06 UTC Jul 1 2014  
Mod-sfr 798> ***  
Mod-sfr 799> ***  
Mod-sfr 800> *** EVENT: Start Parameters: Image: /mnt/disk0/vm/vm_3.img,  
ISO: -cdrom /mnt/disk0  
Mod-sfr 801> /asasfr-5500x-boot-5.3.1-152.img, Num CPUs: 6, RAM: 7659MB,
```


```
Mgmt MAC: A4:4C:11:29:
Mod-sfr 802> CC:FB, CP MAC: 00:00:00:04:00:01, HDD: -drive file=/dev/md0,
  cache=none,if=virtio,
Mod-sfr 803> Dev
Mod-sfr 804> ***
Mod-sfr 805> *** EVENT: Start Parameters Continued: RegEx Shared Mem:
  32MB, Cmd Op: r, Shared M
Mod-sfr 806> em Key: 8061, Shared Mem Size: 64, Log Pipe: /dev/ttyS0_vm3,
  Sock: /dev/ttyS1_vm3,
Mod-sfr 807> Mem-Path: -mem-path /hugepages
Mod-sfr 808> *** TIME: 05:53:06 UTC Jul 1 2014
Mod-sfr 809> ***
Mod-sfr 810> IVSHMEM: optarg is key=8061,64,unix:/tmp/nahanni, name is,
  key is 8061, size is 6
...
Mod-sfr 239> Starting Advanced Configuration and Power Interface daemon:
  acpid.
Mod-sfr 240> acpid: starting up with proc fs
Mod-sfr 241> acpid: opendir(/etc/acpi/events): No such file or directory
Mod-sfr 242> starting Busybox inetd: inetd... done.
Mod-sfr 243> Starting ntpd: done
Mod-sfr 244> Starting syslogd/klogd: done
Mod-sfr 245>
Cisco ASA SFR Boot Image 5.3.1
```

5. ASA CX モジュールが起動するまで約 5 ~ 15 分待ってから、動作中の ASA SFR ブート イメージへのコンソール セッションを開きます。

ASA SFR ブート イメージの設定

新しくインストールしたASA SFRブートイメージをセットアップするには、次の手順を実行します。

1. プレス **Enter** ログインプロンプトに到達するためにセッションを開いた後。

 **注** : デフォルトのユーザ名は `admin` を参照。パスワードはソフトウェアリリースによって異なります。Adm!n123 7.0.1 (工場出荷時の新しいデバイスのみ) Admin123 6.0以降の場合、Sourcefire 6.0よりも前のバージョンの場合。

ランダム データの例は次のとおりです。

```
<#root>
```

```
ciscoasa#
```

```
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:ASA SFRモジュールのブートが完了していない場合、sessionコマンドが失敗し、システムがTTYS1経由で接続できないことを示すメッセージが表示されます。このような場合は、モジュールの起動が完了するまで待ってから、再試行してください。

2. config コマンドを入力します setup コマンドを発行して、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。

```
<#root>
```

```
asasfr-boot>
```

```
setup
```

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

次の情報を入力するように求められます。

- **Host name** – ホスト名は最大65文字の英数字 (スペースを含まない) で指定できます。また、ハイフンも使用できます。
- **Network address** – ネットワークアドレスは、スタティックIPv4アドレスまたはIPv6アドレスのいずれかです。また、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もできます。
- **DNS information** – 少なくとも1つのドメインネームシステム(DNS)サーバーを指定する必要があります。また、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** – ネットワークタイムプロトコル(NTP)を有効にして、システム時刻を設定するようにNTPサーバを設定できます。

3. config コマンドを入力します system install システムソフトウェアイメージをインストールするコマンド :

```
<#root>
```

```
asasfr-boot >
```

```
system install [noconfirm] url
```

次の情報を含めます noconfirm 確認メッセージに応答しない場合に選択します。を交換する url キーワードを使用して、.pkg 出力を提供してください。ここでも、FTP、HTTP、または HTTPSサーバを使用できます。ランダム データの例は次のとおりです。

```
<#root>
```

```
asasfr-boot >
```

```
system install http://
```

```
    /asasfr-sys-5.3.1-152.pkg
```

```
Verifying  
Downloading  
Extracting
```

```
Package Detail
```

```
  Description: Cisco ASA-FirePOWER 5.3.1-152 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 Jun 23 09:28:38 2014):  
The system is going down for reboot NOW!  
Console session with module sfr terminated.
```

FTPサーバの場合、URLは次のようになります。ftp://username:password@server-ip/asasfr-sys-5.3.1-152.pkgを参照。

 注SFRは「Recover」状態になります。SFRモジュールのインストールが完了するまでに、1時間ほどかかることがあります。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 SFRサービスの起動には10分以上かかります。show module sfr コマンドは、すべてのプロセスがUpを参照。


設定

この項では、FirePOWER ソフトウェアと FireSIGHT Management Center を設定する方法、およびトラフィックを SFR モジュールにリダイレクトする方法について説明します。

FirePOWER ソフトウェアの設定

FirePOWER ソフトウェアを設定するには、次の手順を実行します。

1. ASA SFR モジュールへのセッションを開きます。

 注：完全に機能するモジュールでログインが行われるため、別のログインプロンプトが表示されるようになりました。

ランダム データの例は次のとおりです。

```
<#root>
```

```
ciscoasa#
```

```
session sfr
```

```
Opening command session with module sfr.  
Connected to module sfr. Escape character sequence is 'CTRL-^X'.  
Sourcefire ASA5555 v5.3.1 (build 152)  
Sourcefire3D login:
```

2. ユーザ名でログインします。 admin パスワードはソフトウェアリリースによって異なります。
。 Adm!n123 7.0.1 (工場出荷時の新しいデバイスのみ) Admin123 6.0以降の場合、Sourcefire 6.0よりも前のバージョンの場合。
3. プロンプトに従って次の順序でシステム設定を行います。
 - a. エンド ユーザ ライセンス契約書 (EULA) を読んで、内容に同意します。
 - b. admin パスワードを変更します。
 - c. プロンプトに従って管理アドレスと DNS 設定を指定します。

 注:IPv4とIPv6の両方の管理アドレスを設定できます。

ランダム データの例は次のとおりです。

```
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]:198.51.100.3  
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.0  
Enter the IPv4 default gateway for the management interface []: 198.51.100.1  
Enter a fully qualified hostname for this system [Sourcefire3D]: asasfr.example.com  
Enter a comma-separated list of DNS servers or 'none' []:  
198.51.100.15, 198.51.100.14  
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'
```

4. システムが再設定されるまで待機します。

FireSIGHT Management Center の設定

ASA SFR モジュールおよびセキュリティ ポリシーを管理するには、FireSIGHT Management Center に登録する必要があります。詳細については、「[FireSIGHT Management Centerへのデバイスの登録](#)」を参照してください。FireSIGHT Management Center で次の操作を行うことはできません。

- ASA SFR モジュール インターフェイスの設定
- ASA SFR モジュール プロセスのシャットダウン、再起動、または管理
- ASA SFR モジュール デバイスでのバックアップの作成、またはバックアップの復元
- VLAN タグの条件を使用したトラフィック照合目的のアクセス コントロール ルールの記述

SFR モジュールへのトラフィックのリダイレクト

トラフィックを ASA SFR モジュールにリダイレクトするには、特定のトラフィックを識別する サービス ポリシーを作成する必要があります。トラフィックを ASA SFR モジュールにリダイレクトするには、次の手順を実行します。

1. 次のコマンドで識別する必要があるトラフィックを選択します。 `access-list` コマンドを使用して、アップグレードを実行します。この例では、すべてのインターフェイスからのすべてのトラフィックがリダイレクトされます。この操作は、特定のトラフィックに対して実行することもできます。


```
<#root>
ciscoasa(config)#
access-list sfr_redirect extended permit ip any any
```


2. アクセス リストのトラフィックと照合するためにクラス マップを作成します。

```
<#root>
ciscoasa(config)#
class-map sfr

ciscoasa(config-cmap)#
match access-list sfr_redirect
```

3. 導入モードを指定します。デバイスは、パッシブ展開モード (モニタ専用) またはインライン展開モード (通常) のいずれかで設定できます。

 注:ASAでパッシブモードとインラインモードの両方を同時に設定することはできません

 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。

- インライン展開では、SFRモジュールがアクセスコントロールポリシーに基づいてトラフィックを検査し、ASAに判定を行って、トラフィックフローに対して適切なアクション（許可、拒否など）を実行します。この例では、ポリシーマップを作成し、インラインモードでASA SFRモジュールを設定する方法を示します。
- 最新のバージョンの `global_policy` 別のモジュール設定で設定されている (`show run policy-map global_policy, show run service-policy`) その後、最初に他のモジュール設定の `global_policy` をリセット/削除してから、`global_policy` を参照。

```
<#root>
ciscoasa(config)#
policy-map global_policy


ciscoasa(config-pmap)#
class sfr


ciscoasa(config-pmap-c)#
sfr fail-open
```


- パッシブ展開では、トラフィックのコピーが SFR サービス モジュールに送信されませんが、ASA には返されません。パッシブ モードでは、SFR モジュールがトラフィックに関して完了したアクションを表示できます。また、ネットワークに影響を与えることなくトラフィックの内容を評価できます。

SFRモジュールをパッシブモードに設定するには、`monitor-only` キーワードを使用します（次の例を参照）。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。

```
<#root>
ciscoasa(config-pmap-c)#
sfr fail-open monitor-only
```

 **警告:** `monitor-only` モードでは、SFRサービスモジュールは悪意のあるトラフィックを拒否またはブロックできません。


 **注意:** インターフェイスレベルを使用して、モニタ専用モードでASAを設定することができます `traffic-forward sfr monitor-only` コマンドを使用します。ただし、この設定は単なるデモンストレーション機能用であり、実稼働ASAでは使用しないでください。この

 デモ機能で発生した問題については、Cisco Technical Assistance Center (TAC) のサポート対象外です。ASA SFR サービスをパッシブ モードで導入する場合は、policy-map を使用して設定します。

4. 場所を指定し、ポリシーを適用します。ポリシーは、グローバルまたはインターフェイスに適用できます。インターフェイスでグローバル ポリシーを上書きするには、サービス ポリシーをインターフェイスに適用します。

「 global キーワードはすべてのインターフェイスにポリシーマップを適用し、 interface キーワードは、ポリシーを1つのインターフェイスに適用します。許可されるグローバル ポリシーは1つだけです。次の例では、ポリシーがグローバルに適用されます。

```
<#root>
ciscoasa(config)#
service-policy global_policy global
```

 注意：ポリシーマップ global_policy デフォルトのポリシーです。このポリシーを使用していて、トラブルシューティングのためにデバイスから削除する場合は、必ずその意味を理解しておいてください。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

- 次のコマンドを実行できます(debug module-boot)を使用して、SFRブートイメージのインストール開始時のデバッグを有効にします。
- ASAがリカバリモードでスタックし、コンソールが起動しない場合は、次のコマンドを実行します(sw-module module sfr recover stop)。
- SFRモジュールがリカバリ状態から戻れなかった場合は、ASAをリロードしてみてください(reload quick)を参照。(トラフィックが通過すると、ネットワーク障害が発生する可能性があります)。それでもSFRが復旧状態のままになっている場合は、ASAをシャットダウンし、unplug the SSD ASAを起動します。モジュールのステータスを確認します。モジュールはINIT状態である必要があります。再度、ASAをシャットダウンします。 insert the SSD ASA SFRモジュールの再イメージ化を開始できます。

関連情報

- [Cisco Secure IPS - Cisco NGIPSの機能](#)
- [FireSIGHT Management Center へのデバイスの登録](#)

- [Cisco ASA FirePOWER モジュール クイック スタート ガイド](#)
- [VMware ESXi への FireSIGHT Management Center の導入](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。