ASA 5585-Xハードウェアモジュールへの SFRモジュールのインストール

内容

概要

ASA FirePOWER モジュールは、ASA SFR ともいい、Next-Generation IPS (NGIPS)、Application Visibility and Control (AVC)、URL フィルタリング、および Advance Malware Protection (AMP) などの次世代のファイアウォール サービスを提供します。 シングルまたはマルチ コンテキスト モード、およびルーテッドまたはトランスペアレント モードでモジュールを使用できます。このドキュメントでは、ASA 5585-X のハードウェア モジュールでの FirePOWER (SFR) モジュールの前提条件およびインストール プロセスを説明します。また、SFR モジュールを FireSIGHT Management Center に登録する手順も紹介します。

> **注：**FirePOWER (SFR) サービスは ASA 5585-X のハードウェア モジュールに存在するのに対して、ASA 5512-X から 5555-X シリーズまでのアプライアンスの FirePOWER サービスはソフトウェア モジュールにインストールされるため、インストール プロセスが異なります。

前提条件

要件

このドキュメントの手順では、特権 EXEC モードにアクセスする必要があります。特権 EXEC モードにアクセスするには、enable コマンドを入力します。パスワードを設定しなかった場合は、単に Enter キーを押します。

```
ciscoasa> enable
Password:
ciscoasa#
```

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。

- ASA ソフトウェア バージョン 9.2.2 以降
- ASA 5585-X プラットフォーム
- FirePOWER モジュールの管理インターフェイスが到達可能な TFTP サーバ
- FireSIGHT Management Center バージョン 5.3.1 以降

注：このドキュメントの情報は、特定のラボ環境に置かれた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、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

コンフィギュレーション

はじめに

ASA SSM は ASA 5585-X シャーシの 2 つのスロットの 1 つを常に占有するので、FirePOWER（SFR）サービス SSP 以外のハードウェア モジュール（SSP-CX（Context Aware）または AIP-SSM（Advanced Inspection and Prevention Security）など）が存在する場合は、もう 1 つのモジュールを取り外して SSP- SFR のためにスペースを空ける必要があります。ハードウェア モジュールを取り外す前に、次のコマンドを実行してモジュールをシャットダウンします。

```
ciscoasa# hw-module module 1 shutdown
```

配線と管理

- ASA 5585-X の ASA のコンソールから SFR モジュールのシリアル ポートにはアクセスできません。
- SFR モジュールがプロビジョニングされれば、「session 1」コマンドを使用して、ブレードへのセッションを開始できます。
- ASA 5585-X で SFR モジュールを完全に再イメージ化するには、管理イーサネット インターフェイスとシリアル管理ポート上のコンソール セッションを使用する必要があります。これらは SFR モジュール上にあり、ASA の管理インターフェイスおよびコンソールとは分かれています。

ヒント：ASA 上のモジュールのステータスを調べるには、「show module 1 detail」コマン

ドを実行し、SFR モジュールの管理 IP および関連する Defense Center を取得します。

ASA への FirePOWER (SFR) モジュールのインストール

1. ASA FirePOWER SFRモジュールの初期ブートストラップイメージをCisco.comから、ASA FirePOWER管理インターフェイスからアクセス可能なTFTPサーバにダウンロードします。イメージ名は「asasfr-boot-5.3.1-152.img」のようになっています。

2. ASA FirePOWERシステムソフトウェアをCisco.comから、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サーバにダウンロードします。

3. SFRモジュールの再起動

オプション 1 : SFR モジュールのパスワードが分からない場合は、ASA から次のコマンドを発行して、モジュールを再起動できます。

```
ciscoasa# hw-module module 1 reload
Reload module 1? [confirm]
Reload issued for module 1
```

オプション 2 : SFR モジュールのパスワードが分かっている場合は、コマンド ラインから直接センサーを再起動できます。

```
Sourcefire3D login: admin
Password:

Sourcefire Linux OS v5.3.1 (build 43)
Sourcefire ASA5585-SSP-10 v5.3.1 (build 152)

>system reboot
```

4. ESCAPEまたはターミナルセッションソフトウェアのブレークシーケンスを使用してSFRモジュールのブートプロセスを中断し、モジュールをROMMONに配置します。

```
The system is restarting...
CISCO SYSTEMS
Embedded BIOS Version 2.0(14)1 15:16:31 01/25/14



Cisco Systems ROMMON Version (2.0(14)1) #0: Sat Jan 25 16:44:38 CST 2014

Platform ASA 5585-X FirePOWER SSP-10, 8GE

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot in 8 seconds.

Boot interrupted.
```

```
Management0/0
Link is UP
MAC Address: xxxx.xxxx.xxxx

Use ? for help.

rommon #0>
```

5. SFRモジュール管理インターフェイスにIPアドレスを設定し、ブートストラップイメージへのTFTPサーバとTFTPパスの場所を指定します。次のコマンドを入力して、インターフェイスの IP アドレスを設定し、TFTP イメージを取得します。

- set
- ADDRESS = Your_IP_Address
- GATEWAY = Your_Gateway
- SERVER = Your_TFTP_Server
- IMAGE = Your_TFTP_Filepath
- sync
- TFTP

!使用される IP アドレス情報の例。使用している環境向けの更新。

```
rommon #1> ADDRESS=198.51.100.3
rommon #2> GATEWAY=198.51.100.1
rommon #3> SERVER=198.51.100.100
rommon #4> IMAGE=/tftpboot/asasfr-boot-5.3.1-152.img
rommon #5> sync

Updating NVRAM Parameters...

rommon #6> tftp
ROMMON Variable Settings:
ADDRESS=198.51.100.3
SERVER=198.51.100.100
GATEWAY=198.51.100.1
PORT=Management0/0
VLAN=untagged
IMAGE=/tftpboot/asasfr-boot-5.3.1-152.img
CONFIG=
LINKTIMEOUT=20
PKTTIMEOUT=4
RETRY=20

tftp /tftpboot/asasfr-boot-5.3.1-152.img@198.51.100.100 via 198.51.100.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<truncated output>

Received 41235627 bytes

Launching TFTP Image...

Execute image at 0x14000
```

6.初期ブートイメージにログインします。admin として、パスワード Admin123 を使用してログインします。

```
Cisco ASA SFR Boot Image 5.3.1

asasfr login: admin
Password:

Cisco ASA SFR Boot 5.3.1 (152)
Type ? for list of commands
```

7.初期ブートイメージを使用して、モジュールの管理インターフェイスのIPアドレスを設定します。setup コマンドを入力してウィザードを開始します。次の情報を求めるプロンプトが表示されます。

- **Hostname**：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 サーバを指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。

!使用される情報の例。使用している環境向けの更新。

```
asasfr-boot>setup

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

Enter a hostname [asasfr]: sfr-module-5585
Do you want to configure IPv4 address on management interface?(y/n) [Y]: Y
Do you want to enable DHCP for IPv4 address on management interface?(y/n) [N]: N
Enter an IPv4 address [192.168.8.8]: 198.51.100.3
Enter the netmask [255.255.255.0]: 255.255.255.0
Enter the gateway [192.168.8.1]: 198.51.100.1
Do you want to configure static IPv6 address on management interface?(y/n) [N]: N
Stateless autoconfiguration will be enabled for IPv6 addresses.
Enter the primary DNS server IP address: 198.51.100.15
Do you want to configure Secondary DNS Server? (y/n) [n]: N
Do you want to configure Local Domain Name? (y/n) [n]: N
Do you want to configure Search domains? (y/n) [n]: N
Do you want to enable the NTP service? [Y]: N

Please review the final configuration:
Hostname: sfr-module-5585
Management Interface Configuration

IPv4 Configuration: static
IP Address: 198.51.100.3
Netmask: 255.255.255.0
Gateway: 198.51.100.1

IPv6 Configuration: Stateless autoconfiguration

DNS Configuration:
DNS Server: 198.51.100.15
```

```
Apply the changes?(y,n) [Y]: Y
Configuration saved successfully!
Applying...
Restarting network services...
Restarting NTP service...
Done.
```

8.ブートイメージを使用して、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プルしてイ**ンストール**します。確認メッセージに応答しない場合は、**noconfirm オプションを指定します。***url キーワード*を .pkg ファイルの場所に置き換えます。

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

たとえば、

```
> system install http://Server_IP_Address/asasfr-sys-5.3.1-152.pkg

Verifying
Downloading
Extracting

Package Detail
Description: Cisco ASA-SFR 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 ...
```

> **注：**インストールが 20 ~ 30 分で完了したら、Enter キーを押して再起動するように求められます。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 1 details の出力で、すべてのプロセスが Up と表示されるはずです。

インストール中のモジュール ステータス

```
ciscoasa# show module 1 details

Getting details from the Service Module, please wait...
Unable to read details from module 1

Card Type: ASA 5585-X FirePOWER SSP-10, 8GE
Model: ASA5585-SSP-SFR10
Hardware version: 1.0
Serial Number: JAD18400028
Firmware version: 2.0(14)1
Software version: 5.3.1-152
MAC Address Range: 58f3.9ca0.1190 to 58f3.9ca0.119b
App. name: ASA FirePOWER
App. Status: Not Applicable
App. Status Desc: Not Applicable
App. version: 5.3.1-152
Data Plane Status: Not Applicable
Console session: Not ready
```

```
Status: Unresponsive
```

インストールが正常終了した後のモジュール ステータス

```
ciscoasa# show module 1 details

Getting details from the Service Module, please wait...

Card Type: ASA 5585-X FirePOWER SSP-10, 8GE
Model: ASA5585-SSP-SFR10
Hardware version: 1.0
Serial Number: JAD18400028
Firmware version: 2.0(14)1
Software version: 5.3.1-152
MAC Address Range: 58f3.9ca0.1190 to 58f3.9ca0.119b
App. name: ASA FirePOWER
App. Status: Up
App. Status Desc: Normal Operation
App. version: 5.3.1-152
Data Plane Status: Up
Console session: Ready
Status: Up
DC addr: No DC Configured
Mgmt IP addr: 192.168.45.45
Mgmt Network mask: 255.255.255.0
Mgmt Gateway: 0.0.0.0
Mgmt web ports: 443
Mgmt TLS enabled: true
```

コンフィギュレーション

FirePOWER ソフトウェアの設定

1. 次のいずれかの外部ポート経由で ASA 5585-X FirePOWER モジュールに接続できます。

- ASA FirePOWER コンソール ポート
- SSH を使用する ASA FirePOWER Management 1/0 インターフェイス

注：session sfr コマンドを使用し、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。

2.コンソールからFirePOWERモジュールにアクセスした後、ユーザ名adminとパスワード**Sourcefire**を使用してログインします。

```
Sourcefire3D login: admin
Password:

Last login: Fri Jan 30 14:00:51 UTC 2015 on ttyS0

Copyright 2001-2013, Sourcefire, Inc. All rights reserved. Sourcefire is a registered
trademark of Sourcefire, Inc. All other trademarks are property of their respective
owners.
```

```
Sourcefire Linux OS v5.3.1 (build 43)
Sourcefire ASA5585-SSP-10 v5.3.1 (build 152)

Last login: Wed Feb 18 14:22:19 on ttyS0

System initialization in progress.  Please stand by.
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]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]: dhcp
If your networking information has changed, you will need to reconnect.
[1640209.830367] ADDRCONF(NETDEV_UP): eth0: link is not ready
[1640212.873978] e1000e: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
[1640212.966250] ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
For HTTP Proxy configuration, run 'configure network http-proxy'

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.

>
```

FireSIGHT Management Center の設定

ASA FirePOWER モジュールとセキュリティ ポリシーを管理するには、FireSIGHT Management Center に登録することが**必須**です。FireSIGHT Management Center で次の操作を行うことはできません。

- ASA FirePOWER インターフェイスの設定はできません。
- ASA FirePOWER プロセスのシャットダウン、再起動、または管理はできません。
- ASA FirePOWER 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はできません。
- VLAN タグの条件を使用して、トラフィックを照合するためのアクセス コントロール ルールを記述することはできません。

SFR 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。FirePOWER モジュールにトラフィックをリダイレクトするには、次の手順に従います。

ステップ 1：トラフィックの選択

最初に、access-list コマンドを使用してトラフィックを選択します。次の例では、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をリダイレクトします。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。

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

ステップ 2：トラフィックの照合

次の例は、クラス マップを作成し、アクセス リストのトラフィックと照合する方法を示しています。

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

ステップ 3：アクションの指定

デバイスは、パッシブ展開（モニタ専用）またはインライン展開のいずれかで設定できます。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することはできません。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。

インライン モード

インライン展開では、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。次の例は、ポリシー マップを作成し、インライン モードで FirePOWER モジュールを設定する方法を示します。

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class sfr
ciscoasa(config-pmap-c)# sfr fail-open
```

パッシブ モード

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 には戻されません。
- 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。

FirePOWER モジュールをパッシブ モードで設定するには、次のように monitor-only キーワードを使用します。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。

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

ステップ 4：場所の指定

最後の手順は、ポリシーを適用することです。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は、そのインターフェイスへサービス ポリシーを適用することで、グローバル ポリシーを上書きできます。

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は1つのインターフェイスにポリシーを適用します。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。

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

注意：ポリシー マップ global_policy は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目的でこのポリシーをデバイスから削除する際には、必ずその影響を理解しておいてください。

関連資料

- FireSIGHT Management Center へのデバイスの登録
- VMware ESXi への FireSIGHT Management Center の導入
- 5500-X IPS モジュールでの IPS 管理設定のシナリオ