Installer et configurer d’un module de services FirePOWER sur une plateforme ASA

Contenu

Introduction

Ce document décrit comment installer et configurer un module Cisco FirePOWER (SFR) qui s'exécute sur un dispositif de sécurité adaptatif Cisco (ASA) et comment enregistrer le module SFR auprès de Cisco FireSIGHT Management Center.

Conditions préalables

Conditions requises

Cisco recommande que votre système réponde à ces exigences avant de tenter les procédures décrites dans ce document :

- Vérifiez que vous disposez d'au moins 3 Go d'espace libre sur le lecteur flash (disk0), en plus de la taille du logiciel de démarrage.
- Vérifiez que vous avez accès au mode d’exécution privilégié. Pour accéder au mode d’exécution privilégié, entrez la commande **enable** dans la CLI. Si aucun mot de passe n'a été défini, appuyez sur **Enter**::

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

Components Used

Pour installer les fonctionnalités FirePOWER sur un Cisco ASA, les composants suivants sont requis :

- Logiciel Cisco ASA version 9.2.2 ou ultérieure
- Plates-formes Cisco ASA 5512-X à 5555-X
- Logiciel FirePOWER version 5.3.1 ou ultérieure

> **Note**: Si vous souhaitez installer les services FirePOWER (SFR) sur un module matériel ASA 5585-X, reportez-vous à Installer un module SFR sur un module matériel ASA 5585-X.

Ces composants sont requis sur Cisco FireSIGHT Management Center :

- Logiciel FirePOWER version 5.3.1 ou ultérieure
- FireSIGHT Management Center FS2000, FS4000 ou appliance virtuelle

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Le module Cisco ASA FirePOWER, également appelé ASA SFR, fournit des services de pare-feu de nouvelle génération, tels que :

- Système de prévention des intrusions de nouvelle génération (NGIPS)
- Visibilité et contrôle des applications (AVC)
- Filtrer les URL
- Advanced Malware Protection (AMP)

> **Note**: Vous pouvez utiliser le module SFR ASA en mode contexte simple ou multiple, et en mode routé ou transparent.

Avant de commencer

Tenez compte de ces informations importantes avant d'essayer les procédures décrites dans ce document :

- Si vous avez une stratégie de service active qui redirige le trafic vers un module IPS (Intrusion Prevention System)/Context Aware (CX) (que vous avez remplacé par ASA SFR), vous devez la supprimer avant de configurer la stratégie de service ASA SFR.
- Vous devez arrêter tous les autres modules logiciels qui s'exécutent actuellement. Un périphérique peut exécuter un seul module logiciel à la fois. Vous devez le faire à partir de l'interface de ligne de commande ASA. Par exemple, ces commandes arrêtent et désinstallent le module logiciel IPS, puis rechargent l'ASA :

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

- Les commandes utilisées pour supprimer le module CX sont les mêmes, à l'exception de **cxsc** mot-clé utilisé à la place de **ips**::
```
ciscoasa# sw-module module cxsc shutdown
ciscoasa# sw-module module cxsc uninstall
ciscoasa# reload
```
- Lorsque vous réinstallez un module, utilisez la même **shutdown** et **uninstall** qui sont utilisées afin de supprimer une ancienne image SFR. Voici un exemple :

```
ciscoasa# sw-module module sfr uninstall
```
- Si le module SFR ASA est utilisé en mode de contexte multiple, exécutez les procédures décrites dans ce document dans l'espace d'exécution du système.

Astuce : Afin de déterminer l'état d'un module sur l'ASA, entrez la commande **show module** erasecat4000_flash:.

Install

Cette section décrit comment installer le module SFR sur l'ASA et comment configurer l'image de démarrage ASA SFR.

Installation du module SFR sur l'ASA

Complétez ces étapes afin d'installer le module SFR sur l'ASA :

1. Téléchargez le logiciel système ASA SFR de Cisco.com vers un serveur HTTP, HTTPS ou FTP accessible depuis l'interface de gestion ASA SFR.
2. Téléchargez l'image de démarrage sur le périphérique. Vous pouvez utiliser Cisco Adaptive Security Device Manager (ASDM) ou l'interface de ligne de commande ASA afin de télécharger l'image de démarrage sur le périphérique. **Note**: Ne pas transférer le logiciel système ; il est téléchargé ultérieurement sur le disque dur SSD (Solid State Drive).Complétez ces étapes afin de télécharger l'image de démarrage via l'ASDM : Téléchargez l'image de démarrage sur votre station de travail ou placez-la sur un serveur FTP, TFTP, HTTP, HTTPS, SMB (Server Message Block) ou SCP (Secure Copy).Choisir**Tools > File Management** dans l'ASDM.Choisissez la commande File Transfer appropriée, *entre le PC local et le Flash* ou *entre le serveur distant et le Flash*.Transférez le logiciel de démarrage sur le lecteur flash (disk0) de l'ASA.Complétez ces étapes afin de télécharger l'image de démarrage via l'interface de ligne de commande ASA :Téléchargez l'image de démarrage sur un serveur FTP, TFTP, HTTP ou HTTPS.Saisissez le **copy** dans l'interface de ligne de commande afin de télécharger l'image de démarrage sur le lecteur flash. Voici un exemple qui utilise le protocole HTTP (remplacez avec votre adresse IP ou votre nom d'hôte). Pour le serveur FTP, l'URL ressemble à ceci :**ftp://username:password@server-ip/asasfr-5500x-boot-5.3.1-152.img** .
```
ciscoasa# copy http:///asasfr-5500x-boot-5.3.1-152.img disk0:/asasfr-5500x-boot-5.3.1-152.img
```
3. Entrez cette commande afin de configurer l'emplacement de l'image de démarrage ASA SFR dans le lecteur flash ASA :

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

Voici un exemple :

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

4. Entrez cette commande afin de charger l'image de démarrage ASA SFR :

```
ciscoasa# sw-module module sfr recover boot
```

Pendant cette période, si vous activez **debug module-boot** sur l'ASA, ces débogages sont imprimés :

```
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. Attendez environ 5 à 15 minutes que le module ASA SFR démarre, puis ouvrez une session de console sur l'image de démarrage ASA SFR opérationnelle.

Configuration de l'image de démarrage ASA SFR

Complétez ces étapes afin de configurer l'image de démarrage ASA SFR récemment installée :

1. Appuyer **Enter** après avoir ouvert une session afin d'accéder à l'invite de connexion. **Note**: Le nom d'utilisateur par défaut est **admin**. Le mot de passe diffère selon la version du logiciel

:**Adm!n123** pour la version 7.0.1 (nouveau périphérique de l'usine uniquement), **Admin123** pour 6.0 et versions ultérieures, **Sourcefire** pour pré-6.0.Voici un exemple :

```
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
```

Astuce : Si le démarrage du module ASA SFR n'est pas terminé, la commande session échoue et un message apparaît pour indiquer que le système ne peut pas se connecter sur TTYS1. Si cela se produit, attendez que le démarrage du module se termine et réessayez.

2. Saisissez le **setup** afin de configurer le système de sorte que vous puissiez installer le package logiciel système :

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

Vous êtes ensuite invité à fournir ces informations :**Host name** - Le nom d'hôte peut comporter jusqu'à 65 caractères alphanumériques, sans espace. L'utilisation de tirets est autorisée.**Network address** - L'adresse réseau peut être des adresses IPv4 ou IPv6 statiques. Vous pouvez également utiliser DHCP pour la configuration automatique sans état IPv4 ou IPv6.**DNS information** - Vous devez identifier au moins un serveur DNS (Domain Name System) et vous pouvez également définir le nom de domaine et le domaine de recherche.**NTP information** - Vous pouvez activer le protocole NTP (Network Time Protocol) et configurer les serveurs NTP afin de définir l'heure système.

3. Saisissez le **system install** afin d'installer l'image du logiciel système :

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

Inclure le **noconfirm** si vous ne voulez pas répondre aux messages de confirmation. Remplacer **url** avec l'emplacement du **.pkg** fichier. Encore une fois, vous pouvez utiliser un serveur FTP, HTTP ou HTTPS. Voici un exemple :

```
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.
```

Pour le serveur FTP, l'URL ressemble à ceci :**ftp://username:password@server-ip/asasfr-sys-5.3.1-152.pkg.**

Remarque Le SFR se trouve dans un "**Recover**" pendant le processus d'installation. L'installation du module SFR peut prendre jusqu'à une heure. Une fois l'installation terminée, le système redémarre. Comptez au moins dix minutes pour l'installation du composant d'application et pour le démarrage des services ASA SFR. Le résultat de **show module sfr** indique que tous les processus sont **Up**.

Configuration

Cette section décrit comment configurer le logiciel FirePOWER et FireSIGHT Management Center, et comment rediriger le trafic vers le module SFR.

Configuration du logiciel FirePOWER

Complétez ces étapes afin de configurer le logiciel FirePOWER :

1. Ouvrez une session sur le module ASA SFR.
   Note: Une autre invite de connexion apparaît maintenant car la connexion se produit sur un module entièrement fonctionnel.Voici un exemple :

   ```
   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. Connectez-vous avec le nom d'utilisateur **admin** et le mot de passe diffère selon la version du logiciel :**Adm!n123** pour la version 7.0.1 (nouveau périphérique de l'usine uniquement), **Admin123** pour 6.0 et versions ultérieures,**Sourcefire** pour pré-6.0.
3. Effectuez la configuration système comme demandé, dans l'ordre suivant : Lire et accepter le Contrat de licence de l'utilisateur final (CLUF).Modifiez le mot de passe admin.Configurez l'adresse de gestion et les paramètres DNS, le cas échéant. **Note**: Vous pouvez configurer les adresses de gestion IPv4 et IPv6.Voici un exemple :

   ```
   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. Attendez que le système se reconfigure.

Configurer FireSIGHT Management Center

Pour gérer un module ASA SFR et une stratégie de sécurité, vous devez l'enregistrer auprès d'un FireSIGHT Management Center. Référez-vous à Enregistrer un périphérique avec FireSIGHT Management Center pour plus d'informations. Vous ne pouvez pas effectuer ces actions avec FireSIGHT Management Center :

- Configurer les interfaces de module ASA SFR
- Arrêter, redémarrer ou gérer autrement les processus du module ASA SFR
- Créer des sauvegardes à partir des périphériques de module ASA SFR ou les restaurer sur ces derniers
- Écrire des règles de contrôle d'accès afin de faire correspondre le trafic avec l'utilisation des conditions de balise VLAN

Rediriger le trafic vers le module SFR

Afin de rediriger le trafic vers le module SFR ASA, vous devez créer une stratégie de service qui identifie le trafic spécifique. Complétez ces étapes afin de rediriger le trafic vers un module SFR ASA :

1. Sélectionnez le trafic qui doit être identifié avec le **access-list** erasecat4000_flash:. Dans cet exemple, tout le trafic provenant de toutes les interfaces est redirigé. Vous pouvez également le faire pour un trafic spécifique.

   ```
   ciscoasa(config)# access-list sfr_redirect extended permit ip any any
   ```
2. Créez une carte-classe afin de correspondre au trafic sur une liste d'accès :

   ```
   ciscoasa(config)# class-map sfr
   ciscoasa(config-cmap)# match access-list sfr_redirect
   ```
3. Spécifiez le mode de déploiement. Vous pouvez configurer votre périphérique en mode de déploiement passif (surveillance uniquement) ou en ligne (normal).
   Note: Vous ne pouvez pas configurer simultanément un mode passif et un mode en ligne sur l'ASA. Un seul type de stratégie de sécurité est autorisé.Dans un déploiement en ligne, le module SFR inspecte le trafic en fonction de la politique de contrôle d'accès et donne le verdict à l'ASA pour prendre les mesures appropriées (Autoriser, Refuser, etc.) sur le flux de trafic. Cet exemple montre comment créer une carte de stratégie et configurer le module SFR ASA en mode en ligne. Veuillez vérifier que **global_policy** est configuré avec une autre configuration de module**(show run policy-map global_policy, show run service-policy)**, puis réinitialisez/supprimez d'abord global_policy pour une autre configuration de module, puis reconfigurez le **global_policy**.

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

   Dans un déploiement passif, une copie du trafic est envoyée au module de service SFR, mais elle n'est pas renvoyée à l'ASA. Le mode passif vous permet d'afficher les actions que le module SFR aurait effectuées en ce qui concerne le trafic. Il vous permet également d'évaluer le contenu du trafic, sans impact sur le réseau.

Si vous souhaitez configurer le module SFR en mode passif, utilisez la **monitor-only** (comme indiqué dans l'exemple suivant). Si vous n'incluez pas le mot clé, le trafic est envoyé en mode en ligne.

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

Avertissement : Les **monitor-only** ne permet pas au module de service SFR de refuser ou de bloquer le trafic malveillant.**Attention** : Il peut être possible de configurer un ASA en mode *moniteur uniquement* avec l'utilisation du niveau interface **traffic-forward sfr monitor-only** commande ; cependant, cette configuration est uniquement destinée à la fonctionnalité de démonstration et ne doit pas être utilisée sur un ASA de production. Les problèmes détectés dans cette fonctionnalité de démonstration ne sont pas pris en charge par le centre d'assistance technique Cisco (TAC). Si vous souhaitez déployer le service SFR ASA en mode passif, configurez-le à l'aide d'une *carte de stratégie*.

4. Spécifiez un emplacement et appliquez la stratégie. Vous pouvez appliquer une stratégie globalement ou sur une interface. Afin de remplacer la stratégie globale sur une interface, vous pouvez appliquer une stratégie de service à cette interface.

   Les **global** applique la carte de stratégie à toutes les interfaces, et **interface** applique la stratégie à une interface. Une seule politique globale est autorisée. Dans cet exemple, la stratégie est appliquée globalement :

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

   Attention : La carte des politiques **global_policy** est une stratégie par défaut. Si vous utilisez cette stratégie et voulez la supprimer sur votre périphérique pour le dépanner, assurez-vous que vous comprenez son implication.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

- Vous pouvez exécuter cette commande (**debug module-boot**) pour activer le débogage au début de l'installation de l'image de démarrage SFR.
- Si l'ASA est resté bloqué en mode de récupération et que la console n'est pas apparue, alors vous essayez cette commande (**sw-module module sfr recover stop**.
- Si le module SFR n'a pas pu sortir de l'état de récupération, vous pouvez essayer de recharger l'ASA **(reload quick)**. (Si le trafic passe, il peut provoquer des perturbations du réseau). Si SFR est bloqué dans l'état de récupération, vous pouvez arrêter l'ASA et **unplug the SSD** et démarrer l'ASA. Vérifiez l'état du module et celui-ci doit être INIT. Encore une fois, arrêtez l'ASA, **insert the SSD** et démarrer l'ASA. vous pouvez refaire l'image du module ASA SFR.

Informations connexes

- Cisco Secure IPS - Fonctionnalités Cisco NGIPS
- Enregistrer un périphérique avec FireSIGHT Management Center
- Guide de démarrage rapide du module Cisco ASA FirePOWER
- Déploiement de FireSIGHT Management Center sur VMware ESXi
- Support et documentation techniques - Cisco Systems