Installieren eines SFR-Moduls auf einem ASA 5585-X-Hardwaremodul

Inhalt

Einleitung

Das ASA FirePOWER-Modul, auch bekannt als ASA SFR, bietet Firewall-Services der nächsten Generation wie Next-Generation IPS (NGIPS), Application Visibility and Control (AVC), URL-Filterung und Advanced Malware Protection (AMP). Sie können das Modul im Einzel- oder Mehrfachkontextmodus sowie im Routing- oder Transparent-Modus verwenden. Dieses Dokument beschreibt die Voraussetzungen und Installationsprozesse für ein FirePOWER (SFR)-Modul auf dem ASA 5585-X-Hardwaremodul. Außerdem werden die Schritte zur Registrierung eines SFR-Moduls beim FireSIGHT Management Center beschrieben.

> **Anmerkung:** Die FirePOWER-Services (SFR) befinden sich auf einem Hardwaremodul in der ASA 5585-X, während die FirePOWER-Services auf den Appliances der Serien ASA 5512-X bis 555-X auf einem Softwaremodul installiert sind, was zu Unterschieden in den Installationsprozessen führt.

Voraussetzungen

Anforderungen

Die Anweisungen in diesem Dokument erfordern den Zugriff auf den privilegierten EXEC-Modus. Um auf den privilegierten EXEC-Modus zuzugreifen, geben Sie den Befehl enable ein. Wenn kein Kennwort festgelegt wurde, drücken Sie die Eingabetaste.

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

Zur Installation von FirePOWER-Services auf einem ASA-Gerät sind folgende Komponenten erforderlich:

- ASA Software Version 9.2.2 oder höher
- ASA 5585-X-Plattform
- Ein TFTP-Server, der über die Verwaltungsschnittstelle des FirePOWER-Moduls erreichbar ist
- FireSIGHT Management Center mit Version 5.3.1 oder höher

Anmerkung: Die Informationen in diesem Dokument werden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konfiguration

Vorbereitungen

Wenn ein ASA SSM immer einen der beiden Steckplätze im ASA 5585-X-Chassis belegt, muss das andere Modul als das FirePOWER (SFR) Services SSP wie SSP-CX (Context Aware) oder AIP-SSM (Advanced Inspection and Prevention Security) deinstalliert werden, um Platz für das SSP-SFR zu schaffen. Führen Sie vor dem Entfernen eines Hardwaremoduls den folgenden Befehl aus, um ein Modul herunterzufahren:

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

Verkabelung und Management

- Sie können nicht über die ASA-Konsole auf der ASA 5585-X auf den seriellen Port des SFR-Moduls zugreifen.
- Nach der Bereitstellung des SFR-Moduls können Sie mithilfe des Befehls "session 1" eine Sitzung mit dem Blade durchführen.
- Um das SFR-Modul auf einem ASA 5585-X vollständig neu abzuspielen, müssen Sie die Management Ethernet-Schnittstelle und eine Konsolensitzung auf dem seriellen Management-Port verwenden, die sich auf dem SFR-Modul befinden und von der Management-Schnittstelle und -Konsole der ASA getrennt sind.

Tipp: Um den Status eines Moduls auf der ASA zu ermitteln, führen Sie den Befehl "show

module 1 details" aus, mit dem die Management-IP des SFR-Moduls und das zugehörige Defense Center abgerufen werden.

Installation des FirePOWER (SFR)-Moduls auf der ASA

1. Laden Sie das erste Bootstrap-Image des ASA FirePOWER-SFR-Moduls von Cisco.com auf einen TFTP-Server herunter, auf den Sie über die ASA FirePOWER-Managementschnittstelle zugreifen können. Der Bildname sieht aus wie "asfr-boot-5.3.1-152.img".

2. Laden Sie die ASA FirePOWER-Systemsoftware von Cisco.com auf einen HTTP-, HTTPS- oder FTP-Server herunter, auf den über die ASA FirePOWER-Managementschnittstelle zugegriffen werden kann.

3. SFR-Modul neu starten

Option 1: Wenn Sie nicht über das Kennwort für das SFR-Modul verfügen, können Sie von der ASA den folgenden Befehl ausführen, um das Modul neu zu starten.

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

Option 2: Wenn Sie über das Kennwort für das SFR-Modul verfügen, können Sie den Sensor direkt von der Befehlszeile aus neu starten.

```
Sourcefire3D login: admin
Password:

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

>system reboot
```

4. Unterbrechen Sie den Bootvorgang des SFR-Moduls mithilfe von ESCAPE oder der Unterbrechungssequenz Ihrer Terminal-Sitzungssoftware, um das Modul in ROMMON zu platzieren.

```
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. Konfigurieren Sie die Verwaltungsschnittstelle des SFR-Moduls mit einer IP-Adresse, und geben Sie den Speicherort des TFTP-Servers und des TFTP-Pfads zum Bootstrap-Image an. Geben Sie die folgenden Befehle ein, um eine IP-Adresse für die Schnittstelle festzulegen und das TFTP-Image abzurufen:

- festlegen
- ADDRESS = Your_IP_Address
- GATEWAY = Ihr_Gateway
- SERVER = Ihr_TFTP_Server
- IMAGE = Ihr_TFTP_Dateipfad
- Synchronisation
- tftp

! Verwendete Beispiel-IP-Adressinformationen. Aktualisieren Sie Ihre Umgebung.

```
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. Melden Sie sich beim ersten Boot-Image an. Melden Sie sich als Administrator und mit dem Kennwort Admin123 an.

```
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. Verwenden Sie das Boot-Image zum Konfigurieren einer IP-Adresse auf der Verwaltungsschnittstelle des Moduls. Geben Sie den Befehl setup ein, um den Assistenten aufzurufen. Sie werden zur Eingabe der folgenden Informationen aufgefordert:

- **Hostname**: Bis zu 65 alphanumerische Zeichen ohne Leerzeichen. Bindestriche sind erlaubt.
- **Netzwerkadresse**: Sie können statische IPv4- oder IPv6-Adressen festlegen oder DHCP (für IPv4) oder IPv6 Stateless Autoconfiguration verwenden.
- **DNS-Informationen**: Sie müssen mindestens einen DNS-Server identifizieren, und Sie können auch den Domänennamen und die Suchdomäne festlegen.
- **NTP-Informationen**: Sie können NTP aktivieren und die NTP-Server konfigurieren, um die Systemzeit festzulegen.

! Verwendete Beispielinformationen. Aktualisieren Sie Ihre Umgebung.

```
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. Verwenden Sie das Boot-Image, um das Systemsoftware-Image mithilfe des Befehls **Systeminstallation** abzurufen und zu installieren. Wenn Sie nicht auf Bestätigungsnachrichten antworten möchten, fügen Sie die **noconfirm-**Option ein. Ersetzen Sie das *url*-Schlüsselwort durch den Speicherort der Datei .pkg.

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

Beispiele,

```
> 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 ...
```

> **Anmerkung:** Wenn die Installation in 20 bis 30 Minuten abgeschlossen ist, werden Sie aufgefordert, zum Neustart die Eingabetaste zu drücken. Die Installation der Anwendungskomponenten und der Start der ASA FirePOWER-Services dauert ca. 10 Minuten. In der Detailausgabe von Modul 1 werden alle Prozesse als Nach oben angezeigt.

Modulstatus während der Installation

```
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
```

Modulstatus nach erfolgreicher Installation

```
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
```

Konfiguration

Konfigurieren der FirePOWER-Software

1. Sie können eine Verbindung zum ASA 5585-X FirePOWER-Modul über einen der folgenden externen Ports herstellen:

- ASA FirePOWER-Konsolenport
- ASA FirePOWER Management 1/0-Schnittstelle mit SSH

Anmerkung: Mit dem Befehl session sfr können Sie nicht über die ASA-Backplane auf die CLI des ASA FirePOWER-Hardwaremoduls zugreifen.

2. Melden Sie sich nach dem Zugriff auf das FirePOWER-Modul über die Konsole mit dem Benutzernamen **admin** und dem Kennwort **Sourcefire an**.

```
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.

>
```

Konfigurieren von FireSIGHT Management Center

Um ein ASA FirePOWER-Modul und eine Sicherheitsrichtlinie zu verwalten, **müssen** Sie es bei einem FireSIGHT Management Center registrieren. Mit einem FireSIGHT Management Center können Sie Folgendes nicht tun:

- ASA FirePOWER-Schnittstellen können nicht konfiguriert werden.
- ASA FirePOWER-Prozesse können nicht heruntergefahren, neu gestartet oder anderweitig verwaltet werden.
- Sicherungen von ASA FirePOWER-Geräten können nicht erstellt oder auf diesen wiederhergestellt werden.
- Es können keine Zugriffskontrollregeln geschrieben werden, um Datenverkehr mithilfe von VLAN-Tag-Bedingungen abzugleichen.

Umleitung des Datenverkehrs zum SFR-Modul

Sie leiten Datenverkehr an das ASA FirePOWER-Modul um, indem Sie eine Service-Richtlinie

erstellen, die bestimmten Datenverkehr identifiziert. Führen Sie die folgenden Schritte aus, um Datenverkehr an ein FirePOWER-Modul umzuleiten:

Schritt 1: Datenverkehr auswählen

Wählen Sie zunächst Datenverkehr mithilfe des Befehls access-list aus. Im folgenden Beispiel wird der gesamte Datenverkehr von allen Schnittstellen umgeleitet. Sie können dies auch für bestimmten Datenverkehr tun.

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

Schritt 2: Datenverkehr zuordnen

Im folgenden Beispiel wird veranschaulicht, wie eine Klassenzuordnung erstellt und der Datenverkehr in einer Zugriffsliste zugeordnet wird:

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

Schritt 3: Aktion angeben

Sie können Ihr Gerät entweder in einer passiven ("monitor-only") oder in einer Inline-Bereitstellung konfigurieren. Sie können auf der ASA nicht gleichzeitig sowohl den Monitor-Only-Modus als auch den normalen Inline-Modus konfigurieren. Es ist nur ein Sicherheitstyp zulässig.

Inline-Modus

Bei einer Inline-Bereitstellung wird der Datenverkehr nach dem Verwerfen von unerwünschtem Datenverkehr und dem Ergreifen anderer Richtlinienaktionen an die ASA zurückgegeben, um die Weiterverarbeitung und die endgültige Übertragung durchzuführen. Das folgende Beispiel zeigt, wie Sie eine Richtlinienzuordnung erstellen und das FirePOWER-Modul im Inline-Modus konfigurieren:

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

Passiver Modus

In einer passiven Bereitstellung

- Eine Kopie des Datenverkehrs wird an das Gerät gesendet, jedoch nicht an die ASA zurückgesendet.
- Im passiven Modus können Sie sehen, was das Gerät für den Datenverkehr getan hätte, und den Inhalt des Datenverkehrs ohne Auswirkungen auf das Netzwerk auswerten.

Wenn Sie das FirePOWER-Modul im passiven Modus konfigurieren möchten, verwenden Sie das

Schlüsselwort nur Monitor (siehe unten). Wenn Sie das Schlüsselwort nicht angeben, wird der Datenverkehr im Inline-Modus gesendet.

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

Schritt 4: Speicherort angeben

Der letzte Schritt besteht in der Anwendung der Richtlinie. Sie können eine Richtlinie global oder auf eine Schnittstelle anwenden. Sie können die globale Richtlinie für eine Schnittstelle überschreiben, indem Sie eine Dienstrichtlinie auf diese Schnittstelle anwenden.

Das globale Schlüsselwort wendet die Richtlinienzuordnung auf alle Schnittstellen an, und die Schnittstelle wendet die Richtlinie auf eine Schnittstelle an. Es ist nur eine globale Richtlinie zulässig. Im folgenden Beispiel wird die Richtlinie global angewendet:

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

> **Vorsicht:** Die Richtlinienzuordnung global_policy ist eine Standardrichtlinie. Wenn Sie diese Richtlinie verwenden und diese Richtlinie auf Ihrem Gerät für die Fehlerbehebung entfernen möchten, sollten Sie sich dessen Auswirkungen bewusst sein.

Verwandtes Dokument

- Registrieren eines Geräts mit einem FireSIGHT Management Center
- Bereitstellung von FireSIGHT Management Center auf VMware ESXi
- Konfigurationsszenarien für die IPS-Verwaltung auf einem 5500-X IPS-Modul