Installieren und Konfigurieren eines FirePOWER-Servicemoduls auf einer ASA-Plattform

Inhalt

Einleitung

Dieses Dokument beschreibt die Installation und Konfiguration eines Cisco FirePOWER (SFR)-Moduls, das auf einer Cisco Adaptive Security Appliance (ASA) ausgeführt wird, sowie die Registrierung des SFR-Moduls beim Cisco FireSIGHT Management Center.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Ihr System diese Anforderungen erfüllt, bevor Sie die in diesem Dokument beschriebenen Verfahren durchführen:

- Stellen Sie sicher, dass zusätzlich zur Größe der Boot-Software mindestens 3 GB freier Speicherplatz auf dem Flash-Laufwerk (disk0) vorhanden sind.
- Stellen Sie sicher, dass Sie Zugriff auf den privilegierten EXEC-Modus haben. Um auf den privilegierten EXEC-Modus zuzugreifen, geben Sie die **enable** in die Kommandozeile ein. Wenn kein Kennwort festgelegt wurde, drücken Sie **Enter**:

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

Verwendete Komponenten

Zur Installation der FirePOWER-Services auf einer Cisco ASA sind folgende Komponenten erforderlich:

- Cisco ASA Software Version 9.2.2 oder höher
- Cisco ASA-Plattformen 5512-X bis 5555-X
- FirePOWER Software Version 5.3.1 oder höher

Anmerkung: Wenn Sie FirePOWER-Services (SFR) auf einem ASA 5585-X-Hardwaremodul installieren möchten, lesen Sie Install a SFR module on a ASA 5585-X Hardware Module (SFR-Modul auf einem ASA 5585-X-Hardwaremodul installieren).

Diese Komponenten sind im Cisco FireSIGHT Management Center erforderlich:

- FirePOWER Software Version 5.3.1 oder höher
- FireSIGHT Management Center FS2000, FS4000 oder virtuelle Appliance

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Das Cisco ASA FirePOWER-Modul, auch bekannt als ASA SFR, bietet Firewall-Services der nächsten Generation wie:

- Next-Generation Intrusion Prevention System (NGIPS)
- Application Visibility and Control (AVC)
- URLs filtern
- Advanced Malware Protection (AMP)

Anmerkung: Sie können das ASA SFR-Modul im Single- oder Multiple-Context-Modus sowie im Routed- oder Transparent-Modus verwenden.

Vorbereitungen

Berücksichtigen Sie diese wichtigen Informationen, bevor Sie die in diesem Dokument beschriebenen Verfahren durchführen:

- Wenn Sie über eine aktive Service-Richtlinie verfügen, die den Datenverkehr an ein Intrusion Prevention System (IPS)-/Context Aware (CX)-Modul umleitet (das Sie durch die ASA SFR ersetzt haben), müssen Sie es entfernen, bevor Sie die ASA SFR-Servicerichtlinie konfigurieren.
- Sie müssen alle anderen Softwaremodule herunterfahren, die derzeit ausgeführt werden. Auf einem Gerät kann jeweils nur ein Softwaremodul ausgeführt werden. Dies muss über die ASA-CLI erfolgen. Mit diesen Befehlen wird beispielsweise das IPS-Softwaremodul heruntergefahren, deinstalliert und dann die ASA neu geladen:

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

- Die Befehle, die zum Entfernen des CX-Moduls verwendet werden, sind mit Ausnahme der folgenden **cxsc** anstelle von **ips**:

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

- Wenn Sie ein Modul erneut abbilden, verwenden Sie die gleiche **shutdown** und **uninstall** Befehle, die zum Entfernen eines alten SFR-Images verwendet werden. Hier ein Beispiel:

```
ciscoasa# sw-module module sfr uninstall
```

- Wenn das ASA SFR-Modul im Multiple-Context-Modus verwendet wird, führen Sie die in diesem Dokument beschriebenen Verfahren im System-Ausführungsbereich durch.

Tipp: Um den Status eines Moduls auf der ASA zu bestimmen, geben Sie **show module** aus.

Installieren

In diesem Abschnitt wird beschrieben, wie Sie das SFR-Modul auf der ASA installieren und das ASA SFR-Boot-Image einrichten.

Installieren des SFR-Moduls auf der ASA

Gehen Sie wie folgt vor, um das SFR-Modul auf der ASA zu installieren:

1. Laden Sie die ASA SFR-Systemsoftware von Cisco.com auf einen HTTP-, HTTPS- oder FTP-Server herunter, auf den über die ASA SFR-Managementschnittstelle zugegriffen werden kann.
2. Laden Sie das Boot-Image auf das Gerät herunter. Sie können entweder den Cisco Adaptive Security Device Manager (ASDM) oder die ASA CLI verwenden, um das Boot-Image auf das Gerät herunterzuladen. **Anmerkung:** Übertragen Sie die Systemsoftware nicht. Sie wird später auf das Solid-State-Laufwerk (SSD) heruntergeladen.Gehen Sie wie folgt vor, um das Boot-Image über das ASDM herunterzuladen: Laden Sie das Boot-Image auf Ihre Workstation herunter, oder platzieren Sie es auf einem FTP-, TFTP-, HTTP-, HTTPS-, Server Message Block (SMB)- oder Secure Copy (SCP)-Server.Auswählen**Tools > File Management** im ASDM.Wählen Sie den entsprechenden Befehl zur Dateiübertragung aus, entweder *zwischen lokalem PC und Flash* oder *zwischen Remote Server und Flash*.Übertragen Sie die Boot-Software auf das Flash-Laufwerk (disk0) auf der ASA.Gehen Sie wie folgt vor, um das Boot-Image über die ASA-CLI herunterzuladen:Laden Sie das Boot-Image auf einen FTP-, TFTP-, HTTP- oder HTTPS-Server herunter.Geben Sie **copy** in die Kommandozeile ein, um das Boot-Image auf das Flash-Laufwerk herunterzuladen. Im folgenden Beispiel wird das HTTP-Protokoll verwendet (ersetzen Sie die mit Ihrer Server-IP-Adresse oder Ihrem Hostnamen). Für FTP-Server sieht die URL wie folgt aus:**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. Geben Sie diesen Befehl ein, um den Speicherort des ASA SFR-Boot-Image im ASA-Flash-Laufwerk zu konfigurieren:

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

Hier ein Beispiel:

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

4. Geben Sie diesen Befehl ein, um das ASA SFR-Boot-Image zu laden:

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

Wenn Sie während dieser Zeit **debug module-boot** auf der ASA werden diese Debugging-Meldungen ausgegeben:

```
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. Warten Sie etwa 5 bis 15 Minuten, bis das ASA SFR-Modul gestartet wird, und öffnen Sie dann eine Konsolensitzung mit dem betrieblichen ASA SFR-Boot-Image.

Einrichten des ASA SFR-Boot-Image

Gehen Sie wie folgt vor, um das neu installierte ASA SFR-Boot-Image einzurichten:

1. Presse **Enter** nachdem Sie eine Sitzung geöffnet haben, um zur Anmeldungsaufforderung zu gelangen. **Anmerkung:** Der Standardbenutzername ist **admin**. Das Kennwort unterscheidet sich je nach Softwareversion:**Adm!n123** für 7.0.1 (nur neues Gerät ab Werk), **Admin123** für 6.0 und höher, **Sourcefire** für die älter als 6,0.Hier ein Beispiel:

```
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
```

   Tipp: Wenn der Start des ASA SFR-Moduls nicht abgeschlossen wurde, schlägt der Sitzungsbefehl fehl, und es erscheint eine Meldung, die anzeigt, dass das System keine Verbindung über TTYS1 herstellen kann. Wenn dies der Fall ist, warten Sie, bis der Modulstart abgeschlossen ist, und versuchen Sie es erneut.
2. Geben Sie **setup** , um das System so zu konfigurieren, dass das Systemsoftwarepaket installiert werden kann:

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

   Sie werden dann zur Eingabe dieser Informationen aufgefordert:**Host name** - Der Hostname darf bis zu 65 alphanumerische Zeichen ohne Leerzeichen enthalten. Die Verwendung von Bindestrichen ist zulässig.**Network address** - Bei der Netzwerkadresse kann es sich um statische IPv4- oder IPv6-Adressen handeln. Sie können DHCP auch für die IPv4- oder IPv6-Stateless-Autokonfiguration verwenden.**DNS information** - Sie müssen mindestens einen DNS-Server (Domain Name System) identifizieren, und Sie können auch den Domänennamen und die Suchdomäne festlegen.**NTP information** - Sie können das Network Time Protocol (NTP) aktivieren und die NTP-Server konfigurieren, um die Systemzeit festzulegen.
3. Geben Sie **system install** um das Systemsoftware-Image zu installieren:

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

   Integrieren Sie die **noconfirm** , wenn Sie nicht auf Bestätigungsmeldungen reagieren möchten. Ersetzen Sie die **url** Schlüsselwort mit dem Speicherort des **.pkg** Datei. Auch hier können Sie einen FTP-, HTTP- oder HTTPS-Server verwenden. Hier ein Beispiel:

```
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.
```

Für FTP-Server sieht die URL wie folgt aus:**ftp://username:password@server-ip/asasfr-sys-5.3.1-152.pkg**.

Hinweis Der SFR befindet sich in einem "**Recover**" während des Installationsprozesses angezeigt. Die Installation des SFR-Moduls kann bis zu eine Stunde dauern. Nach Abschluss der Installation wird das System neu gestartet. Die Installation der Anwendungskomponenten und der Start der ASA SFR-Services dauert zehn oder mehr Minuten. Die Ausgabe der **show module sfr** gibt an, dass alle Prozesse **Up**.

Konfigurieren

In diesem Abschnitt wird beschrieben, wie die FirePOWER-Software und das FireSIGHT Management Center konfiguriert und der Datenverkehr zum SFR-Modul umgeleitet wird.

Konfigurieren der FirePOWER-Software

Gehen Sie wie folgt vor, um die FirePOWER-Software zu konfigurieren:

1. Öffnen Sie eine Sitzung mit dem ASA SFR-Modul.
   Anmerkung: Eine andere Anmeldeaufforderung wird angezeigt, da die Anmeldung auf einem voll funktionsfähigen Modul erfolgt.Hier ein Beispiel:

   ```
   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. Melden Sie sich mit dem Benutzernamen an. **admin** und das Kennwort hängt von der Softwareversion ab:**Adm!n123** für 7.0.1 (nur neues Gerät ab Werk), **Admin123** für 6.0 und höher,**Sourcefire** für die älter als 6,0.
3. Schließen Sie die Systemkonfiguration bei entsprechender Aufforderung ab, die in dieser Reihenfolge auftritt: Lesen und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung (EULA).Ändern Sie das Administratorkennwort.Konfigurieren Sie bei Aufforderung die Management-Adresse und die DNS-Einstellungen. **Anmerkung:** Sie können sowohl IPv4- als auch IPv6-Managementadressen konfigurieren.Hier ein Beispiel:

   ```
   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. Warten Sie, bis das System sich selbst neu konfiguriert hat.

Konfigurieren des FireSIGHT Management Center

Um ein ASA SFR-Modul und eine Sicherheitsrichtlinie zu verwalten, müssen Sie es bei einem FireSIGHT Management Center registrieren. Weitere Informationen finden Sie unter Gerät bei einem FireSIGHT Management Center registrieren. Sie können diese Aktionen nicht mit einem FireSIGHT Management Center ausführen:

- Konfigurieren der ASA SFR-Modulschnittstellen
- Herunterfahren, Neustart oder anderweitiges Verwalten der ASA SFR-Modulprozesse
- Erstellen Sie Backups von den ASA SFR-Modulgeräten oder stellen Sie Backups auf diese wieder her.
- Schreiben von Zugriffskontrollregeln, um den Datenverkehr mit den VLAN-Tag-Bedingungen abzustimmen

Umleitung des Datenverkehrs zum SFR-Modul

Um Datenverkehr an das ASA SFR-Modul umzuleiten, müssen Sie eine Service-Richtlinie erstellen, die bestimmten Datenverkehr identifiziert. Gehen Sie wie folgt vor, um den Datenverkehr an ein ASA SFR-Modul umzuleiten:

1. Wählen Sie den Datenverkehr aus, der mit dem **access-list** aus. In diesem Beispiel wird der gesamte Datenverkehr von allen Schnittstellen umgeleitet. Dies ist auch für bestimmten Datenverkehr möglich.

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

2. Erstellen Sie eine Klassenzuordnung, um den Datenverkehr in einer Zugriffsliste abzugleichen:

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

3. Geben Sie den Bereitstellungsmodus an. Sie können Ihr Gerät entweder im passiven (Monitor-) oder im Inline- (normalen) Bereitstellungsmodus konfigurieren.
Anmerkung: Sie können auf der ASA nicht gleichzeitig einen passiven Modus und einen Inline-Modus konfigurieren. Es ist nur ein Sicherheitstyp zulässig.Bei einer Inline-Bereitstellung prüft das SFR-Modul den Datenverkehr anhand der Zugriffskontrollrichtlinie und erteilt der ASA das Urteil, die entsprechenden Maßnahmen (Zulassen, Verweigern usw.) für den Datenverkehrsfluss zu ergreifen. Dieses Beispiel zeigt, wie Sie eine Richtlinienzuordnung erstellen und das ASA SFR-Modul im Inline-Modus konfigurieren. Überprüfen Sie, ob die aktuelle **global_policy** wird mit einer anderen Modulkonfiguration konfiguriert**(show run policy-map global_policy, show run service-policy)**zurücksetzen/entfernen die global_policy für andere Modulkonfigurationen und konfigurieren dann die **global_policy**.

```
ciscoasa(config)# policy-map global_policy
```

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

Bei einer passiven Bereitstellung wird eine Kopie des Datenverkehrs an das SFR-Servicemodul gesendet, aber nicht an die ASA zurückgesendet. Im passiven Modus können Sie die Aktionen anzeigen, die das SFR-Modul im Hinblick auf den Datenverkehr abgeschlossen hätte. Außerdem können Sie den Inhalt des Datenverkehrs ohne Beeinträchtigung des Netzwerks bewerten.

Wenn Sie das SFR-Modul im passiven Modus konfigurieren möchten, verwenden Sie die **monitor-only** -Schlüsselwort (wie im nächsten Beispiel gezeigt). Wenn Sie das Schlüsselwort nicht angeben, wird der Datenverkehr im Inline-Modus gesendet.

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

Warnung: Die Fehlermeldung **monitor-only** erlaubt dem SFR-Servicemodul nicht, schädlichen Datenverkehr abzulehnen oder zu blockieren.**Vorsicht:** ASA kann mithilfe der Schnittstellenebene im *Monitor-Only*-Modus konfiguriert werden. **traffic-forward sfr monitor-only** command; Diese Konfiguration dient jedoch ausschließlich der Demonstrationsfunktionalität und darf nicht auf einer Produktions-ASA verwendet werden. Alle Probleme, die in dieser Demonstrationsfunktion festgestellt werden, werden vom Cisco Technical Assistance Center (TAC) nicht unterstützt. Wenn Sie den ASA SFR-Service im passiven Modus bereitstellen möchten, konfigurieren Sie ihn mithilfe einer *Richtlinienzuweisung*.

4. Geben Sie einen Speicherort an, und wenden Sie die Richtlinie an. Sie können eine Richtlinie global oder auf eine Schnittstelle anwenden. Um die globale Richtlinie für eine Schnittstelle zu überschreiben, können Sie eine Dienstrichtlinie auf diese Schnittstelle anwenden.

   Die Fehlermeldung **global** -Schlüsselwort die Richtlinienzuordnung auf alle Schnittstellen anwendet und die **interface** -Schlüsselwort wendet die Richtlinie auf eine Schnittstelle an. Es ist nur eine globale Richtlinie zulässig. In diesem Beispiel wird die Richtlinie global angewendet:

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

   Vorsicht: Richtlinienplan **global_policy** ist eine Standardrichtlinie. Wenn Sie diese Richtlinie verwenden und sie auf Ihrem Gerät entfernen möchten, um Fehler zu beheben, stellen Sie sicher, dass Sie die Auswirkungen verstehen.

Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

- Sie können den folgenden Befehl ausführen:**debug module-boot**), um das Debuggen zu Beginn der Installation des SFR-Boot-Images zu aktivieren.
- Wenn die ASA im Wiederherstellungsmodus steckte und die Konsole nicht hochgefahren wurde, versuchen Sie diesen Befehl (**sw-module module sfr recover stop**).

- Wenn das SFR-Modul nicht aus dem Wiederherstellungsstatus herauskommen konnte, können Sie versuchen, die ASA neu zu laden. **(reload quick)**. (Wenn der Datenverkehr durchläuft, kann dies zu Netzwerkstörungen führen.) Wenn immer noch SFR im Wiederherstellungsstatus feststeckt, können Sie ASA und **unplug the SSD** und starten Sie die ASA. Überprüfen Sie den Status des Moduls, und es muss sich um den INIT-Status handeln. Schalten Sie erneut die ASA aus, **insert the SSD** und starten Sie die ASA. können Sie ein Re-Image des ASA SFR-Moduls starten.

Zugehörige Informationen

- Cisco Secure IPS - Funktionen von Cisco NGIPS
- Registrieren eines Geräts mit einem FireSIGHT Management Center
- Cisco ASA FirePOWER-Modul - Kurzreferenz
- Bereitstellung von FireSIGHT Management Center auf VMware ESXi
- Technischer Support und Dokumentation für Cisco Systeme