Een FirePOWER-servicesmodule installeren en configureren op een ASA-platform

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Achtergrondinformatie](#)
[Voordat u begint](#)
[Installeren](#)
[De SFR-module installeren op de ASA](#)
[De ASA SFR-opstart-image configureren](#)
[Configureren](#)
[De FirePOWER-software configureren](#)
[Het FireSIGHT Management Center configureren](#)
[Verkeer omleiden naar de SFR-module](#)
[Verifiëren](#)
[Problemen oplossen](#)
[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe u een Cisco FirePOWER (SFR)-module installeert en configureert die wordt uitgevoerd op een Cisco adaptieve security applicatie (ASA), en hoe u de SFR-module registreert bij het Cisco FireSIGHT Management Center.

Voorwaarden

Vereisten

Cisco raadt aan dat uw systeem aan de volgende vereisten voldoet voordat u de procedures uitvoert die in dit document worden beschreven:

- Zorg ervoor dat u ten minste 3 GB beschikbare ruimte heeft op het flashstation (disk0), naast de grootte van de opstartsoftware.
- Zorg ervoor dat u toegang heeft tot de modus Privileged EXEC. Voer de geprivilegieerde EXEC-modus in **enable** Opdracht in de CLI. Als er geen wachtwoord is ingesteld, drukt u vervolgens op **Enter**:

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

Gebruikte componenten

Om de FirePOWER-services te installeren op een Cisco ASA, zijn de volgende componenten vereist:

- Cisco ASA-softwareversie 9.2.2 of hoger
- Cisco ASA-platforms 5512-X t/m 5555-X
- FirePOWER-softwareversie 5.3.1 of hoger

Opmerking: Als u FirePOWER (SFR) Services op een ASA 5585-X hardwaremodule wilt installeren, raadpleegt u een SFR-module installeren op een ASA 5585-X hardwaremodule.

De volgende componenten zijn vereist op het Cisco FireSIGHT Management Center:

- FirePOWER-softwareversie 5.3.1 of hoger
- FireSIGHT Management Center FS2000, FS4000 of virtuele applicatie

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De Cisco ASA FirePOWER-module ook bekend als de ASA SFR biedt next-generation firewallservices, zoals:

- Next-generation inbraakpreventiesysteem (NGIPS)
- Application Visibility and Control (AVC)
- URL's filteren
- Advanced Malware Protection (AMP)

Opmerking: U kunt de ASA SFR-module in de modus Single Context of Multiple Context uitvoeren, en in de modus Routed of Transparent.

Voordat u begint

Lees de volgende belangrijke informatie voordat u de procedures uitvoert die in dit document worden beschreven:

- Als u een actief servicebeleid heeft dat verkeer omleidt naar een IPS-/CX-module (inbraakpreventiesysteem/contextbewust) (die u heeft vervangen door de ASA SFR), moet u deze verwijderen voordat u het ASA SFR-servicebeleid configureert.
- U moet andere momenteel actieve softwaremodules uitschakelen. Een apparaat kan één softwaremodule tegelijkertijd uitvoeren. U moet dit via de opdrachtregelinterface van de ASA doen. Met de volgende opdrachten wordt bijvoorbeeld de IPS-softwaremodule uitgeschakeld en verwijderd, waarna de ASA opnieuw wordt geladen:

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

```
ciscoasa# reload
```

- De opdrachten die worden gebruikt om de CX-module te verwijderen, zijn gelijk, behalve de opdrachten die **cxsc** sleutelwoord wordt gebruikt in plaats van **ips**:

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

- Wanneer u een module opnieuw beeldt, gebruikt u hetzelfde **shutdown** en **uninstall** opdrachten die worden gebruikt om een oud SFR-beeld te verwijderen. Hierna volgt een voorbeeld:

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

- Als de ASA SFR-module in de modus Multiple Context wordt gebruikt, voer dan de procedures die in dit document worden beschreven uit binnen de systeemuitvoeringsruimte.

Tip: Om de status van een module op de ASA te bepalen, dient u **show module** uit.

Installeren

In deze sectie wordt beschreven hoe u de SFT-module installeert op de ASA en hoe u de ASA SFR-opstart-image configureert.

De SFR-module installeren op de ASA

Voer de volgende stappen uit om de SFR-module op de ASA te installeren:

1. Download de ASA SFR-systeemsoftware van Cisco.com naar een HTTP-, HTTPS- of FTP-server die toegankelijk is via de ASA SFR-beheerinterface.
2. Download de opstart-image naar het apparaat. U kunt Cisco Adaptive Security Device Manager (ASDM) of de opdrachtregelinterface van de ASA gebruiken om de opstart-image naar het apparaat te downloaden. **Opmerking:** Zet niet de systeemsoftware over; deze wordt later gedownload naar de Solid State Drive (SSD).Voer de volgende stappen uit om de opstart-image te downloaden via de ASDM: Download de opstart-image naar uw werkstation of plaats deze op een FTP-, TFTP-, HTTP-, HTTPS-, SMB- (Server Message Block) of SCP-server (Secure Copy).Kies**Tools > File Management** in de ASDM.Kies de juiste opdracht voor bestandsoverdracht: *Between Local PC and Flash* (Tussen lokale pc en flash) of *Between Remote Server and Flash* (Tussen externe server en flash).Zet de opstartsoftware over naar het flashstation (disk0) op de ASA.Voer de volgende stappen uit om de opstart-image te downloaden via de CLI van de ASA:Download de opstart-image naar een FTP-, TFTP-, HTTP- of HTTPS-server.Voer het **copy** Opdracht in de CLI om de opstartafbeelding te downloaden naar de flitsschijf. Dit is een voorbeeld dat HTTP protocol gebruikt (vervang de met uw IP-adres of hostname van de server). Voor FTP Server ziet de URL er zo uit:**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. Geef deze opdracht op om de locatie van de ASA SFR-opstart-image op het ASA-flashstation te configureren:

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

Hierna volgt een voorbeeld:

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

4. Geef deze opdracht op om de ASA SFR-opstart-image te laden:

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

Als u tijdens deze periode het volgende activeert **debug module-boot** op de ASA worden deze debugs afgedrukt:

```
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. Wacht ongeveer 5 tot 15 minuten tot de ASA SFR-module is opgestart en start dan een consolesessie naar de operationele ASA SFR-opstart-image.

De ASA SFR-opstart-image configureren

Voltooi deze stappen om het nieuw geïnstalleerde ASA SFR-boogbeeld in te stellen:

1. Druk **Enter** nadat u een sessie hebt geopend om de inlogmelding te bereiken. **Opmerking:** De

standaardgebruikersnaam is **admin**. Het wachtwoord verschilt op basis van softwarerelease:**Adm!n123** voor 7.0.1 (uitsluitend nieuwe inrichting van de fabriek); **Admin123** voor 6.0 en later, **Sourcefire** voor pre-6.0.Hierna volgt een voorbeeld:

```
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
```

Tip: Als de ASA SFR module start niet is voltooid, faalt de sessieopdracht en een bericht lijkt aan te geven dat het systeem niet kan verbinden via TTYS1. Als dit gebeurt, wacht dan tot de module start en probeer het opnieuw.

2. Voer het **setup** opdracht om het systeem zo te configureren dat u het systeemsoftwarepakket kunt installeren:

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

Vervolgens wordt om de volgende informatie gevraagd:**Host name** - De hostname kan maximaal 65 alfanumerieke tekens zonder spaties zijn. Het gebruik van afbreekstreepjes is toegestaan.**Network address** - Het netwerkadres kan een statische IPv4- of IPv6-adressen zijn. U kunt ook DHCP gebruiken voor IPv4, of automatische stateless configuratie voor IPv6.**DNS information** - U moet minimaal één DNS-server (Domain Name System) identificeren en u kunt ook de domeinnaam en het zoekdomein instellen.**NTP information** - U kunt Network Time Protocol (NTP) inschakelen en de NTP-servers configureren om de systeemtijd in te stellen.

3. Voer het **system install** opdracht om de systeemsoftwareafbeelding te installeren:

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

De **noconfirm** Mocht u niet willen reageren op de bevestigingsberichten. Vervangen **url** sleutelwoord met de locatie van het **.pkg** bestand. Nogmaals, u kunt een FTP-, HTTP- of HTTPS-server gebruiken. Hierna volgt een voorbeeld:

```
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.
```

Voor FTP Server ziet de URL er zo uit:**ftp://username:password@server-ip/asasfr-sys-5.3.1-152.pkg**.

Opmerking: de SFR staat in een "**Recover**" Tijdens het installatieproces. Het kan een uur duren of zo om de installatie van de SFR-module te voltooien. Wanneer de installatie is voltooid, start het systeem opnieuw op. Wacht tien minuten of langer tot de toepassingscomponent is geïnstalleerd en de ASA SFR-services zijn gestart. De output van het **show module sfr** opdracht geeft aan dat alle processen **Up**.

Configureren

In deze sectie wordt beschreven hoe u de FirePOWER-software en het FireSIGHT Management Center configureert en verkeer omleidt naar de SFR-module.

De FirePOWER-software configureren

Voer de volgende stappen uit om de FirePOWER-software te configureren:

1. Start een sessie naar de ASA SFR-module.
   Opmerking: Er wordt nu een andere aanmeldingsprompt getoond omdat de aanmelding plaatsvindt bij een volledig functionele module.Hierna volgt een voorbeeld:

   ```
   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. Inloggen met de gebruikersnaam **admin** en het wachtwoord verschilt op basis van softwarerelease:**Adm!n123** voor 7.0.1 (uitsluitend nieuwe inrichting van de fabriek); **Admin123** voor 6.0 en later,**Sourcefire** voor pre-6.0.
3. Voltooi de systeemconfiguratie zoals wordt gevraagd in deze volgorde: Lees en accepteer de gebruiksrechtovereenkomst (EULA).Verander het wachtwoord van gebruiker admin.Configureer het beheeradres en de DNS-instellingen, zoals aangegeven. **Opmerking:** U kunt zowel IPv4- als IPv6-beheeradressen configureren.Hierna volgt een voorbeeld:

   ```
   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. Wacht tot het systeem zichzelf herconfigureert.

Het FireSIGHT Management Center configureren

Om een ASA SFR-module en security beleid te beheren, moet u deze registreren bij een FireSIGHT Management Center. Raadpleeg een apparaat registreren bij een FireSIGHT Management Center voor meer informatie. U kunt de volgende acties niet uitvoeren met een FireSIGHT Management Center:

- De interface van ASA SFR-modules configureren
- De ASA SFR-moduleprocessen uitschakelen, opnieuw starten of anderszins beheren
- Back-ups maken van, of back-ups terugzetten naar, de ASA SFR-moduleapparaten
- Toegangscontroleregels schrijven om verkeer te matchen met behulp van VLAN-tags

Verkeer omleiden naar de SFR-module

Om verkeer naar de ASA SFR-module om te leiden, moet u een servicebeleid opzetten dat specifiek verkeer identificeert. Voer de volgende stappen uit om verkeer om te leiden naar een ASA SFR-module:

1. Selecteer het verkeer dat met de **access-list** uit. In dit voorbeeld wordt al het verkeer afkomstig van alle interfaces omgeleid. U kunt dit ook voor specifiek verkeer doen.

   ```
   ciscoasa(config)# access-list sfr_redirect extended permit ip any any
   ```
2. Maak een klassetoewijzing om verkeer te laten voldoen aan een toegangslijst:

   ```
   ciscoasa(config)# class-map sfr
   ciscoasa(config-cmap)# match access-list sfr_redirect
   ```
3. Geef de implementatiemodus op. U kunt uw apparaat configureren in een passieve (alleen monitoren) of inline (normaal) implementatiemodus.
   Opmerking: U kunt niet tegelijkertijd zowel een passieve als een inline modus op de ASA configureren. Er is slechts één type security beleid toegestaan.In een inline-toepassing inspecteert de SFR-module het verkeer op basis van het toegangscontrolebeleid en geeft zij de ASA het vonnis om de passende actie (sta toe, Deny, enzovoort) op de verkeersstroom te nemen. In dit voorbeeld wordt getoond hoe u een beleidstoewijzing maakt en de ASA SFR-module configureert in de inline modus. Controleer of het huidige **global_policy** wordt ingesteld met een andere moduleconfiguratie**(show run policy-map global_policy, show run service-policy)**, dan stelt u eerst het global_policy voor de andere moduleconfiguratie in/verwijdert u en zet u het vervolgens opnieuw aan **global_policy**.

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

   Bij een passieve implementatie wordt een kopie van het verkeer naar de SFR-servicemodule verzonden, maar niet teruggestuurd naar de ASA. In de passieve modus kunt u de acties bekijken die de SFR-module zou hebben uitgevoerd met betrekking tot het verkeer. U kunt tevens de inhoud van het verkeer evalueren zonder dat dit een impact heeft op het netwerk.

   Als u de SFR-module in passieve modus wilt configureren gebruikt u de **monitor-only** sleutelwoord (zoals getoond in het volgende voorbeeld). Als u het trefwoord niet opneemt,

wordt het verkeer verzonden in de inline modus.

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

Waarschuwing: Het **monitor-only** De modus staat niet toe dat de SFR-servicemodule kwaadaardig verkeer ontkent of blokkeert.**Voorzichtig:** Het kan mogelijk zijn om een ASA in *monitor-only* modus te configureren met behulp van het interface-niveau **traffic-forward sfr monitor-only** commando; deze configuratie is echter uitsluitend bedoeld voor demonstratiefunctionaliteit en mag niet worden gebruikt voor een productie-ASA. Eventuele problemen met deze demonstratiefunctie worden niet ondersteund door het Cisco Technical Assistance Center (TAC). Om de ASA SFR-service in passieve modus te implementeren, moet deze worden geconfigureerd met behulp van een *beleidstoewijzing*.

4. Geef een locatie op en pas het beleid toe. U kunt een beleid algemeen of op een interface toepassen. Om het algemene beleid op een interface te negeren, kunt u een servicebeleid op die interface toepassen.

   Het **global** sleutelwoord past de beleidslijn op alle interfaces toe, en het **interface** sleutelwoord past het beleid op één interface toe. Er is slechts één algemeen beleid toegestaan. In dit voorbeeld wordt het beleid algemeen toegepast:

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

   Voorzichtig: Het beleidsplan **global_policy** is een beleid van wanbetaling. Als u dit beleid gebruikt en het op uw apparaat om problemen op te lossen wilt verwijderen, zorg er dan voor dat u de implicatie begrijpt.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

- U kunt deze opdracht uitvoeren (**debug module-boot**) om het debug aan het begin van de installatie van het SFR-beginbeeld in te schakelen.
- Als ASA vast zat in Recover-modus en de console niet naar boven kwam, probeer dan deze opdracht (**sw-module module sfr recover stop**).
- Als de SFR-module niet uit de hersteltoestand kon komen, kunt u proberen de ASA te herladen **(reload quick)**. (Als het verkeer doorrijdt, kan dit netwerkstoringen veroorzaken). Als SFR vast zit in de herstelstaat, kun je de ASA sluiten en **unplug the SSD** kaart en start de ASA. Controleer de status van de module en het moet de INIT-status zijn. Nogmaals, sluit de ASA af. **insert the SSD** kaart en start de ASA. Je kunt beginnen met het opnieuw image van de ASA SFR-module.

Gerelateerde informatie

- Cisco Secure IPS - Cisco NGIPS-functies
- Een apparaat registreren bij een FireSIGHT Management Center

- Cisco ASA FirePOWER-module - Snel startgids
- Implementatie van FireSIGHT Management Center op VMware ESXi
- Technische ondersteuning en documentatie – Cisco Systems