Installeer een SFR-module op een ASA 5585-X hardwaremodule

Inhoud

Inleiding

De ASA FirePOWER-module, ook bekend als ASA SFR, levert firewallservices van de volgende generatie, waaronder IPS (NGIPS), Application Visibility and Control (AVC), URL-filtering en Advanced Malware Protection (AMP). U kunt de module gebruiken in één of meerdere contextmodus en in routed of Transparent. Dit document beschrijft de vereisten en installatieprocessen van een FirePOWER-module (SFR) op ASA 5585-X hardwaremodule. Het voorziet ook in de stappen om een SFR module met FireSIGHT Management Center te registreren.

> **Opmerking:** De FirePOWER-services (SFR) zijn ondergebracht op een hardwaremodule in de ASA 5585-X, terwijl de FirePOWER-services op de ASA 5512-X tot 5555-X Series-apparaten op een softwaremodule zijn geïnstalleerd, wat resulteert in verschillen in installatieprocessen.

Voorwaarden

Vereisten

De instructies op dit document vereisen toegang tot de bevoorrechte EXEC-modus. Om tot de bevoorrechte EXEC wijze toegang te hebben, voer het toelaten bevel in. Als er geen wachtwoord is ingesteld, klikt u op Voer.

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

Om FirePOWER Services op een ASA te installeren, zijn de volgende onderdelen nodig:

- ASA software versie 9.2.2 of hoger
- ASA 5585-X platform
- Een TFTP-server bereikbaar via de beheerinterface van FirePOWER-module
- FireSIGHT Management Center met versie 5.3.1 of hoger

Opmerking: De informatie in dit document wordt gemaakt van de apparaten in een specifieke labomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configuratie

Voordat u begint

Aangezien een ASA SSM altijd één van de twee slots in het ASA 5585-X chassis bezet houdt, moet, als u een andere hardwaremodule hebt dan de FirePOWER Services SSP zoals SSP-CX (Context Aware) of AIP-SSM (Advanced Inspection and Prevention Security), de andere module niet geïnstalleerd worden om ruimte te maken voor de SSP-SFR. Voordat u een hardwaremodule verwijdert, voert u de volgende opdracht uit om een module af te sluiten:

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

Kabels en beheer

- U hebt geen toegang tot de seriële poort van de SFR-module via de ASA's console op de ASA 5585-X.
- Zodra de SFR-module is voorzien, kunt u met de "sessie 1" opdracht in het lemmet sessie sturen.
- Om de SFR module op een ASA 5585-X volledig te herwaarderen moet u de Ethernet interface van het beheer en een console sessie op de seriële beheerpoort gebruiken, die op de SFR module en gescheiden van de ASA's beheersinterface en console zijn.

Tip: Om de status van een module op de ASA te vinden, voer de "show module 1 details" opdracht uit die het beheer-IP van de SFR module en het bijbehorende Defense Center ophaalt.

Installeer FirePOWER-module (SFR) op ASA

1. Download de ASA FirePOWER SFR module eerste bootstrap-afbeelding van Cisco.com naar een TFTP-server die toegankelijk is vanuit ASA FirePOWER Management Interface. De beeldnaam lijkt op "asfr-booster-5.3.1-152.img"

2. Download de ASA FirePOWER-systeemsoftware van Cisco.com naar een HTTP-, HTTPS- of FTP-server die toegankelijk is vanuit de ASA FirePOWER-beheerinterface.

3. Start de SFR-module opnieuw

Optie 1: Als u het wachtwoord niet voor de SFR-module hebt, kunt u de volgende opdracht uit de ASA geven om de module opnieuw te starten.

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

Optie 2: Als u het wachtwoord voor de SFR-module hebt, kunt u de sensor rechtstreeks vanuit de opdrachtregel opnieuw opstarten.

```
Sourcefire3D login: admin
Password:

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

>system reboot
```

4. Onderbreek het laarsproces van de SFR-module met behulp van ESCAPE of de break sequentie van uw terminalsessiesoftware om de module in ROMMON te plaatsen.

```
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. Het configureren van de SFR-module beheerinterface met een IP-adres en het aangeven van de locatie van de TFTP-server en TFTP-pad naar de bootstrap-afbeelding. Geef de volgende opdrachten op om een IP-adres op de interface in te stellen en haal de TFTP-afbeelding terug:

- instellen
- ADRES = Uw_IP_Address
- GATEWAY = Uw_Gateway
- SERVER = Uw_TFTP_server
- AFBEELDING = Uw_TFTP_bestandspad
- sync
- tftp

! Voorbeeld IP-adresinformatie gebruikt. Update voor uw omgeving.

```
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. Meld u aan bij de startvertraging. Inloggen als beheerder en met het wachtwoord Admin123

```
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. Gebruik het beginboogbeeld om een IP-adres te configureren op de beheerinterface van de module. Typ de setup-opdracht om de wizard in te voeren. U wordt gevraagd de volgende informatie te geven:

- **Hostnaam**: Tot 65 alfanumerieke tekens, geen spaties. Hyphens zijn toegestaan.
- **Netwerkadres**: U kunt statische IPv4- of IPv6-adressen instellen of DHCP (voor IPv4) of IPv6-stateless configuratie gebruiken.
- **DNS-informatie**: U moet minimaal één DNS-server identificeren en u kunt ook de domeinnaam en het zoekdomein instellen.
- **NTP-informatie**: U kunt NTP inschakelen en de NTP-servers configureren, zodat u de systeemtijd kunt instellen.

! Gebruikte voorbeeldinformatie. Update voor uw omgeving.

```
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. Gebruik de opstartafbeelding om de systeemsoftwareafbeelding te verwijderen en te installeren met behulp van de opdracht **voor** installatie **van het systeem**. Neem de optie **noconfirm op als u niet wilt reageren op bevestigingsberichten.** Vervang het *url* sleutelwoord met de plaats van .pkg dossier.

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

Bijvoorbeeld:

```
> 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 ...
```

> **Opmerking:** Wanneer de installatie in 20 tot 30 minuten is voltooid, wordt u gevraagd op de ENTER-toets te klikken om te herstarten. Laat 10 of meer minuten staan voor installatie van toepassingscomponenten en voor de ASA FirePOWER-services om te starten. De uitvoer van module 1 van de show zou alle processen als Omhoog moeten tonen.

Module status tijdens installatie

```
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
```

Module status na succesvolle installatie

```
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
```

Configuratie

FirePOWER-software configureren

1.U kunt met de ASA 5585-X FirePOWER-module aansluiten via een van de volgende externe poorten:

- ASA FirePOWER-console poort
- ASA FirePOWER Management 1/0-interface met SSH

  Opmerking: U hebt geen toegang tot de ASA FirePOWER hardwaremodule CLI via de ASA backplane met de opdracht sessie sfr.

2. Nadat u de FirePOWER-module via console hebt benaderd, logt u in met de gebruikersnaam **admin** en het wachtwoord **Sourcefire**.

```
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 configureren

Om een ASA FirePOWER-module en beveiligingsbeleid te beheren **moet** u deze registreren bij een FireSIGHT Management Center. U kunt het volgende niet doen met een FireSIGHT Management Center:

- Kan ASA FirePOWER-interfaces niet configureren.
- Kan ASA FirePOWER-processen niet afsluiten, opnieuw starten of op een andere manier beheren.
- Kan geen back-ups maken van of terugzetten in ASA FirePOWER-apparaten.
- Kan toegangscontroleregels niet schrijven om verkeer aan te passen met behulp van VLAN-tagvoorwaarden.

Verkeer omleiden naar SFR-module

U stuurt verkeer door naar de ASA FirePOWER-module door een servicebeleid te maken dat specifiek verkeer identificeert. Om verkeer terug te sturen naar een FirePOWER-module volgt u de onderstaande stappen:

Stap 1: Selecteren

Selecteer eerst verkeer met de opdracht toegangslijst. In het volgende voorbeeld, richten we al verkeer van alle interfaces op. Je zou het ook kunnen doen voor specifiek verkeer.

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

Stap 2: Overeenkomend verkeer

Het volgende voorbeeld toont hoe te om een class-map te creëren en het verkeer op een toegangslijst aan te passen:

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

Stap 3: Actie specificeren

U kunt uw apparaat in of een passieve ("monitor-only") of inline plaatsing configureren. U kunt niet tegelijkertijd op de ASA zowel de monitor-only modus als de normale inline modus configureren. Er is slechts één type security beleid toegestaan.

Inline modus

In een inline-installatie wordt het verkeer na het wegvallen van het ongewenste verkeer en het nemen van andere door het beleid toegepaste maatregelen teruggebracht naar de ASA voor verdere verwerking en uiteindelijke transmissie. Het volgende voorbeeld toont hoe te om een beleid-kaart te creëren en de module FirePOWER in inline modus te configureren:

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

passieve modus

In een passieve opstelling,

- Een kopie van het verkeer wordt naar het apparaat gestuurd, maar wordt niet teruggegeven aan de ASA.
- Passive modus laat je zien wat het apparaat met het verkeer zou hebben gedaan en laat je de inhoud van het verkeer evalueren zonder het netwerk te beïnvloeden.

Als u de module FirePOWER in passieve modus wilt configureren gebruikt u het woord alleen monitor zoals hieronder. Als u het trefwoord niet opneemt, wordt het verkeer verzonden in de inline modus.

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

Stap 4: Locatie opgeven

De laatste stap is het toepassen van het beleid. U kunt een beleid algemeen of op een interface toepassen. Je kunt het mondiale beleid omzeilen op een interface door een dienstenbeleid op die interface toe te passen.

Het mondiale sleutelwoord past de beleidskaart op alle interfaces toe, en interface past het beleid op één interface toe. Slechts één mondiaal beleid wordt toegestaan. In het volgende voorbeeld wordt het beleid mondiaal toegepast:

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

> **Voorzichtig:** De beleidstoewijzing global_policy is een standaardbeleid. Als u dit beleid gebruikt en dit beleid op uw apparaat wilt verwijderen voor de oplossing van problemen, zorg er dan voor dat u de implicatie ervan begrijpt.

Verwante document

- Een apparaat registreren bij een FireSIGHT Management Center
- Implementatie van FireSIGHT Management Center op VMware ESXi
- Configuratiescenario's voor IPS-beheer op een 5500-X IPS-module