Instalación de un módulo SFR en un módulo de hardware ASA 5585-X

Contenido

Introducción

El módulo ASA FirePOWER, también conocido como ASA SFR, proporciona servicios de firewall de última generación, incluidos IPS de última generación (NGIPS), visibilidad y control de aplicaciones (AVC), filtrado de URL y protección frente a malware avanzado (AMP). Puede utilizar el módulo en modo de contexto único o múltiple, y en modo enrutado o transparente. Este documento describe los requisitos previos y los procesos de instalación de un módulo FirePOWER (SFR) en el módulo de hardware ASA 5585-X. También proporciona los pasos para registrar un módulo SFR con FireSIGHT Management Center.

> Nota: los servicios FirePOWER (SFR) residen en un módulo de hardware del ASA 5585-X, mientras que los servicios FirePOWER de los dispositivos de las series ASA 5512-X a 5555-X están instalados en un módulo de software, lo que provoca diferencias en los procesos de instalación.

Prerequisites

Requirements

Las instrucciones de este documento requieren acceso al modo EXEC privilegiado. Para acceder al modo EXEC privilegiado, ingrese el comando enable. Si no se ha establecido una contraseña, simplemente pulse Intro.

```
<#root>

ciscoasa>

enable


Password:
ciscoasa#
```

Para instalar FirePOWER Services en un ASA, se necesitan los siguientes componentes:

- Software ASA versión 9.2.2 o superior
- Plataforma ASA 5585-X
- Un servidor TFTP accesible mediante la interfaz de administración del módulo FirePOWER
- FireSIGHT Management Center con versión 5.3.1 o superior

Nota: La información de este documento se crea a partir de los dispositivos en un entorno de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Configuración

Antes de comenzar

Dado que ASA SSM siempre ocupa una de las dos ranuras del chasis ASA 5585-X, si tiene un módulo de hardware distinto del SSP de servicios FirePOWER (SFR), como SSP-CX (Context Aware) o AIP-SSM (Advanced Inspection and Prevention Security), el otro módulo debe desinstalarse para dejar espacio para el SSP-SFR. Antes de quitar un módulo de hardware, ejecute el siguiente comando para apagar un módulo:

```
<#root>

ciscoasa#

hw-module module 1 shutdown
```

Cableado y gestión

- No puede acceder al puerto serie del módulo SFR a través de la consola del ASA en el ASA

5585-X.

- Una vez que se ha aprovisionado el módulo SFR, puede iniciar sesión en el servidor blade mediante el comando "session 1".
- Para recrear completamente la imagen del módulo SFR en un ASA 5585-X, debe utilizar la interfaz Ethernet de administración y una sesión de consola en el puerto de administración serie, que se encuentran en el módulo SFR y están separados de la interfaz de administración y la consola de ASA.

Sugerencia: para encontrar el estado de un módulo en el ASA, ejecute el comando "show module 1 details" que recupera la dirección IP del módulo SFR y el centro de defensa asociado.

Instalación del módulo FirePOWER (SFR) en ASA

1. Descargue la imagen de arranque inicial del módulo SFR de ASA FirePOWER desde Cisco.com a un servidor TFTP accesible desde la interfaz de gestión de ASA FirePOWER. El nombre de la imagen es similar a "asasfr-boot-5.3.1-152.img"

2. Descargue el software del sistema ASA FirePOWER desde Cisco.com a un servidor HTTP, HTTPS o FTP al que se pueda acceder desde la interfaz de gestión de ASA FirePOWER.

3. Reinicie el módulo SFR

Opción 1: Si no tiene la contraseña para el módulo SFR, puede ejecutar el siguiente comando desde el ASA para reiniciar el módulo.

<#root>

```
ciscoasa#
```

hw-module module 1 reload

```
Reload module 1? [confirm]
Reload issued for module 1
```

Opción 2: Si tiene la contraseña para el módulo SFR, puede reiniciar el sensor directamente desde su línea de comandos.

<#root>

```
Sourcefire3D login:
```

admin

```
Password:

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

>
```

system reboot

4. Interrumpa el proceso de arranque del módulo SFR usando ESCAPE o la secuencia de interrupción de su software de sesión de terminal para colocar el módulo en ROMMON.

```
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. Configure la interfaz de administración del módulo SFR con una dirección IP e indique la ubicación del servidor TFTP y la ruta TFTP a la imagen de bootstrap. Ingrese los siguientes comandos para establecer una dirección IP en la interfaz y recuperar la imagen TFTP:

- `set`
- ADDRESS = Dirección_IP
- GATEWAY = Su_gateway
- SERVER = Servidor_TFTP
- IMAGE = Ruta_Archivo_TFTP
- `sincrónico`

- tftp

! Ejemplo de información de dirección IP utilizada. Actualización para su entorno.

<#root>

```
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. Inicie sesión en la imagen de arranque inicial. Inicie sesión como admin y con la contraseña Admin123

```
<#root>

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. Utilice la imagen de inicio inicial para configurar una dirección IP en la interfaz de administración del módulo. Introduzca el comando setup para acceder al asistente. Se le solicitará la siguiente información:

- Nombre de host: hasta 65 caracteres alfanuméricos, sin espacios. Se permiten guiones.
- Dirección de red: puede establecer direcciones IPv4 o IPv6 estáticas o utilizar la configuración automática sin estado DHCP (para IPv4) o IPv6.
- Información DNS: debe identificar al menos un servidor DNS y también puede establecer el nombre de dominio y el dominio de búsqueda.
- Información NTP: Puede activar NTP y configurar los servidores NTP para establecer la hora del sistema.

! Ejemplo de información utilizada. Actualización para su entorno.

```
<#root>

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. Utilice la imagen de arranque para extraer e instalar la imagen del software del sistema mediante el comando system install. Incluya la opción noconfirm si no desea responder a los mensajes de confirmación. Reemplace la palabra clave url con la ubicación del archivo .pkg.

<#root>

asasfr-boot>

system install [noconfirm]

url

Por ejemplo,

<#root>

>

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 ...
```

> Nota: cuando la instalación haya finalizado en 20 o 30 minutos, se le solicitará que pulse la tecla Intro para reiniciar. Espere 10 minutos o más para que se instale el componente de la aplicación y para que se inicien los servicios FirePOWER de ASA. El resultado de show module 1 details debería mostrar todos los procesos como Up.

Estado del módulo durante la instalación

<#root>

```
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:
```

Unresponsiv

e

Estado del módulo tras la instalación correcta

<#root>

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

Configuración

Configuración del software FirePOWER

1. Puede conectarse al módulo FirePOWER ASA 5585-X a través de uno de los siguientes puertos externos:

- Puerto de consola de ASA FirePOWER
- Interfaz de administración 1/0 de ASA FirePOWER mediante SSH

Nota: no puede acceder a la CLI del módulo de hardware de ASA FirePOWER a través de la placa base de ASA mediante el comando session sfr.

---

2. Después de acceder al módulo FirePOWER a través de la consola, inicie sesión con el nombre de usuario admin y la contraseña Sourcefire.

<#root>

```
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.

>
```

Configuración de FireSIGHT Management Center

Para gestionar un módulo FirePOWER ASA y una política de seguridad, debe registrarlos en un FireSIGHT Management Center. Con FireSIGHT Management Center no puede hacer lo siguiente:

- No se pueden configurar las interfaces ASA FirePOWER.
- No se pueden apagar, reiniciar ni administrar de ningún otro modo los procesos de ASA FirePOWER.
- No se pueden crear copias de seguridad ni restaurarlas en dispositivos ASA FirePOWER.
- No se pueden escribir reglas de control de acceso para hacer coincidir el tráfico mediante condiciones de etiqueta VLAN.

Redirección del tráfico al módulo SFR

El tráfico se redirige al módulo ASA FirePOWER mediante la creación de una política de servicio que identifica el tráfico específico. Para redirigir el tráfico a un módulo FirePOWER, siga estos pasos:

Paso 1: Seleccionar tráfico

Primero, seleccione el tráfico usando el comando access-list. En el siguiente ejemplo, estamos redireccionando todo el tráfico de todas las interfaces. También podría hacerlo para un tráfico específico.

<#root>

```
ciscoasa(config)#
```

access-list sfr_redirect extended permit ip any any

Paso 2: Coincidencia de tráfico

El ejemplo siguiente muestra cómo crear un mapa de clase y hacer coincidir el tráfico en una lista de acceso:

<#root>

```
ciscoasa(config)#
```

class-map sfr

```
ciscoasa(config-cmap)#
```

match access-list sfr_redirect

Paso 3: Especificar acción

Puede configurar el dispositivo en una implementación pasiva ("solo supervisión") o en línea. No puede configurar el modo de solo supervisión y el modo en línea normal al mismo tiempo en el ASA. Solo se permite un tipo de política de seguridad.

Modo en línea

En una implementación en línea, después de descartar el tráfico no deseado y realizar cualquier otra acción aplicada por la política, el tráfico se devuelve al ASA para su procesamiento posterior y transmisión final. El ejemplo siguiente muestra cómo crear un policy-map y configurar el módulo FirePOWER en modo en línea:

<#root>

```
ciscoasa(config)#
```

policy-map global_policy

```
ciscoasa(config-pmap)#
```

class sfr

```
ciscoasa(config-pmap-c)#
```

sfr fail-open

Modo pasivo

En una implementación pasiva,

- Se envía una copia del tráfico al dispositivo, pero no se devuelve al ASA.
- El modo pasivo le permite ver lo que el dispositivo habría hecho al tráfico y evaluar el contenido del tráfico sin afectar a la red.

Si desea configurar el módulo FirePOWER en modo pasivo, utilice la palabra clave monitor-only como se indica a continuación. Si no incluye la palabra clave, el tráfico se envía en modo en línea.

<#root>

```
ciscoasa(config-pmap-c)#
```

sfr fail-open

monitor-only

Paso 4: Especificar ubicación

El último paso es aplicar la política. Puede aplicar una política de forma global o en una interfaz. Puede anular la política global en una interfaz aplicando una política de servicio a esa interfaz.

La palabra clave global aplica el policy map a todas las interfaces, e interface aplica la política a una interfaz. Solo se permite una política global. En el siguiente ejemplo, la política se aplica globalmente:

<#root>

```
ciscoasa(config)#
```

service-policy global_policy global

Precaución: el policy map global_policy es una política por defecto. Si utiliza esta política y desea eliminarla en su dispositivo para solucionar problemas, asegúrese de comprender sus implicaciones.

Documento relacionado

- Registrar un dispositivo con FireSIGHT Management Center
- Implementación de FireSIGHT Management Center en VMware ESXi
- Escenarios de configuración de gestión de IPS en un módulo IPS 5500-X

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).