

Instalación y configuración de un módulo de servicios Firepower en una plataforma ASA

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Antes de comenzar](#)

[Instalar](#)

[Instalación del módulo SFR en ASA](#)

[Configuración de la imagen de inicio de ASA SFR](#)

[Configurar](#)

[Configuración del software FirePOWER](#)

[Configuración de FireSIGHT Management Center](#)

[Redirección del tráfico al módulo SFR](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo instalar y configurar un módulo Cisco FirePOWER (SFR) en un Cisco ASA y cómo registrar el módulo SFR con Cisco FireSIGHT.

Prerequisites

Requirements

Cisco recomienda que su sistema cumpla estos requisitos antes de intentar los procedimientos que se describen en este documento:

- Asegúrese de que tiene al menos 3 GB de espacio libre en la unidad flash (disk0), además del tamaño del software de arranque.
- Asegúrese de que tiene acceso al modo EXEC privilegiado. Para acceder al modo EXEC privilegiado, ingrese el `enable` comando en la CLI. Si no se ha establecido ninguna contraseña, pulse `Enter`:


<#root>

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

Componentes Utilizados

Para instalar FirePOWER Services en un Cisco ASA, se necesitan estos componentes:

- Software Cisco ASA versión 9.2.2 o posterior
- Plataformas Cisco ASA 5512-X a 5555-X
- Versión 5.3.1 o posterior del software FirePOWER

 Nota: si desea instalar los servicios FirePOWER (SFR) en un módulo de hardware ASA 5585-X, consulte [Instalación de un módulo SFR en un módulo de hardware ASA 5585-X](#).

Estos componentes son necesarios en Cisco FireSIGHT Management Center:


- Versión 5.3.1 o posterior del software FirePOWER
- FireSIGHT Management Center FS2000, FS4000 o appliance virtual

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El módulo Cisco ASA FirePOWER (también conocido como ASA SFR) proporciona servicios de firewall de última generación, como:

- Sistema de prevención de intrusiones de última generación (NGIPS)
- Visibilidad y control de aplicaciones (AVC)
- Filtrar URL
- Advanced Malware Protection (AMP)

 Nota: Puede utilizar el módulo SFR de ASA en el modo de contexto único o múltiple y en el modo enrutado o transparente.

Antes de comenzar

Tenga en cuenta esta importante información antes de intentar los procedimientos descritos en este documento:

- Si tiene una política de servicio activa que redirige el tráfico a un módulo de sistema de prevención de intrusiones (IPS)/sensible al contexto (CX) (que reemplazó por el SFR de ASA), debe eliminarla antes de configurar la política de servicio del SFR de ASA.
- Debe apagar cualquier otro módulo de software que se esté ejecutando actualmente. Un dispositivo puede ejecutar un único módulo de software a la vez. Debe hacerlo desde la CLI de ASA. Por ejemplo, estos comandos apagan y desinstalan el módulo de software IPS y luego recargan el ASA:

```
<#root>
```

```
ciscoasa#
```

```
sw-module module ips shutdown
```

```
ciscoasa#
```

```
sw-module module ips uninstall
```

```
ciscoasa#
```

```
reload
```

- Los comandos que se utilizan para quitar el módulo CX son los mismos, excepto que se utiliza la palabra `cxsc` clave en lugar de `ips`:

```
<#root>
```

```
ciscoasa#
```

```
sw-module module cxsc shutdown
```

```
ciscoasa#
```

```
sw-module module cxsc uninstall
```

```
ciscoasa#
```

```
reload
```

- Al recrear imágenes de un módulo, utilice los mismos `shutdown` y `uninstall` comandos que se utilizan para eliminar una imagen SFR antigua. Aquí tiene un ejemplo:

```
<#root>
```

```
ciscoasa#
```

```
sw-module module sfr uninstall
```

- Si el módulo SFR de ASA se utiliza en el modo de contexto múltiple, realice los procedimientos que se describen en este documento dentro del espacio de ejecución del sistema.



Sugerencia: Para determinar el estado de un módulo en el ASA, ingrese el `show module` comando.

Instalar

En esta sección se describe cómo instalar el módulo SFR en ASA y cómo configurar la imagen de inicio de SFR de ASA.

Instalación del módulo SFR en ASA

Complete estos pasos para instalar el módulo SFR en el ASA:

1. Descargue el software del sistema ASA SFR de Cisco.com a un servidor HTTP, HTTPS o FTP al que se pueda acceder desde la interfaz de gestión ASA SFR.
2. Descargue la imagen de inicio en el dispositivo. Puede utilizar el Cisco Adaptive Security Device Manager (ASDM) o la CLI de ASA para descargar la imagen de inicio en el dispositivo.



Nota: No transfiera el software del sistema; se descarga más tarde a la unidad de estado sólido (SSD).

Complete estos pasos para descargar la imagen de inicio a través del ASDM:

- a. Descargue la imagen de arranque en la estación de trabajo o colóquela en un servidor FTP, TFTP, HTTP, HTTPS, SMB (bloque de mensajes del servidor) o SCP (copia segura).
- b. Elija **Tools > File Management** en el ASDM.
- c. Elija el comando File Transfer apropiado, ya sea **Between Local PC and Flash** o **Between Remote Server and Flash**.
- d. Transfiera el software de arranque a la unidad flash (disk0) en el ASA.

Complete estos pasos para descargar la imagen de inicio a través de la CLI de ASA:

- a. Descargue la imagen de arranque en un servidor FTP, TFTP, HTTP o HTTPS.
- b. Ingrese el `copy` comando en la CLI para descargar la imagen de inicio en la unidad flash.

A continuación se muestra un ejemplo que utiliza el protocolo HTTP (reemplace el por la dirección IP o el nombre de host del servidor). Para el servidor FTP, la dirección URL tiene el siguiente aspecto:`ftp://username:password@server-ip/asasfr-5500x-boot-5.3.1-152.img` .

```
<#root>  
ciscoasa#  
copy http://
```

```
        /asasfr-5500x-boot-5.3.1-152.img  
disk0:/asasfr-5500x-boot-5.3.1-152.img
```

3. Ingrese este comando para configurar la ubicación de la imagen de inicio de ASA SFR en la unidad flash ASA:

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

Aquí tiene un ejemplo:

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

4. Ingrese este comando para cargar la imagen de inicio de SFR de ASA:

```
<#root>  
ciscoasa#  
sw-module module sfr recover boot
```

Durante este tiempo, si habilita `debug module-boot` en ASA, se imprimen estas depuraciones:

```
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. Espere aproximadamente de 5 a 15 minutos para que el módulo SFR de ASA se inicie y luego abra una sesión de consola en la imagen de inicio SFR de ASA operativa.

Configuración de la imagen de inicio de ASA SFR

Complete estos pasos para configurar la imagen de inicio de ASA SFR recién instalada:

1. Presione **Enter** después de abrir una sesión para llegar al mensaje de inicio de sesión.



Nota: El nombre de usuario predeterminado es `admin`. La contraseña difiere en función de la versión de software: `Adm!n123` para 7.0.1 (dispositivo nuevo solo de fábrica), `Admin123` para 6.0 y posterior, `Sourcefire` para la versión anterior a 6.0.

Aquí tiene un ejemplo:

```
<#root>
```

```
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
```



Sugerencia: si el arranque del módulo SFR de ASA no se ha completado, el comando `session` falla y aparece un mensaje para indicar que el sistema no puede conectarse a través de TTY51. Si esto ocurre, espere a que finalice el inicio del módulo e inténtelo de nuevo.

2. Ingrese el `setup` comando para configurar el sistema de modo que pueda instalar el paquete de software del sistema:

```
<#root>
```

```
asasfr-boot>
```

```
setup
```

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

A continuación, se le solicitará esta información:

- **Host name** - El nombre de host puede tener hasta 65 caracteres alfanuméricos, sin espacios. Se permite el uso de guiones.
- **Network address** - La dirección de red puede ser una dirección IPv4 o IPv6 estática. También puede utilizar DHCP para la configuración automática sin información de estado de IPv4 o IPv6.
- **DNS information** - Debe identificar al menos un servidor del Sistema de nombres de dominio (DNS) y también puede establecer el nombre de dominio y el dominio de búsqueda.
- **NTP information** - Puede habilitar el protocolo de tiempo de red (NTP) y configurar los servidores NTP para establecer la hora del sistema.

3. Ingrese el `system install` comando para instalar la imagen de software del sistema:

```
<#root>
```

```
asasfr-boot >
```

```
system install [noconfirm] url
```

Incluya la `noconfirm` opción si no desea responder a los mensajes de confirmación. Reemplace la palabra `url` clave por la ubicación del `.pkg` archivo. De nuevo, puede utilizar un servidor FTP, HTTP o HTTPS. Aquí tiene un ejemplo:

```
<#root>
```

```
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.
```

Para el servidor FTP, la dirección URL tiene el siguiente aspecto: `ftp://username:password@server-ip/asasfr-sys-5.3.1-152.pkg`.

 **Nota** El SFR se encuentra en estado "Recover" durante el proceso de instalación. La instalación del módulo SFR puede tardar aproximadamente una hora. Una vez finalizada la instalación, el sistema se reinicia. Espere diez minutos o más para que se inicie la instalación del componente de la aplicación y los servicios SFR de ASA. El resultado del `show module sfr` comando indica que todos los procesos son Up.


Configurar

En esta sección se describe cómo configurar el software FirePOWER y FireSIGHT Management Center, y cómo redirigir el tráfico al módulo SFR.

Configuración del software FirePOWER

Complete estos pasos para configurar el software FirePOWER:

1. Abra una sesión en el módulo SFR de ASA.

 Nota: Ahora aparece un mensaje de inicio de sesión diferente porque el inicio de sesión se produce en un módulo completamente funcional.

Aquí tiene un ejemplo:

```
<#root>
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. Inicie sesión con el nombre de usuario `admin` y la contraseña difiere en función de la versión de software: `Adm!n123` para 7.0.1 (nuevo dispositivo solo de fábrica), `Admin123` para 6.0 y posterior, `Sourcefire` para la versión anterior a 6.0.
3. Complete la configuración del sistema como se le indica, lo que ocurre en este orden:
 - a. Lea y acepte el Acuerdo de licencia del usuario final (CLUF).
 - b. Cambie la contraseña de administrador.
 - c. Configure la dirección de administración y la configuración de DNS, según se le solicite.

 Nota: Puede configurar direcciones de administración IPv4 e IPv6.

Aquí tiene un ejemplo:

```
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. Espere a que el sistema se reconfigure.

Configuración de FireSIGHT Management Center

Para administrar un módulo SFR y una política de seguridad de ASA, debe registrarlos en un FireSIGHT Management Center. Para obtener más información, consulte [Registro de un dispositivo con FireSIGHT Management Center](#). No puede realizar estas acciones con un FireSIGHT Management Center:

- Configuración de las interfaces del módulo SFR de ASA
- Cierre, reinicie o gestione de otro modo los procesos del módulo SFR de ASA
- Crear copias de seguridad o restaurarlas en los dispositivos del módulo SFR ASA
- Escribir reglas de control de acceso para hacer coincidir el tráfico con el uso de condiciones de etiqueta de VLAN

Redirección del tráfico al módulo SFR

Para redirigir el tráfico al módulo SFR de ASA, debe crear una política de servicio que identifique el tráfico específico. Complete estos pasos para redirigir el tráfico a un módulo SFR de ASA:

1. Seleccione el tráfico que debe identificarse con el `access-list` comando. En este ejemplo, se redirige todo el tráfico de todas las interfaces. También puede hacer esto para tráfico específico.

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

2. Cree un mapa de clase para hacer coincidir el tráfico en una lista de acceso:

```
<#root>
ciscoasa(config)#
class-map sfr

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

3. Especifique el modo de implementación. Puede configurar el dispositivo en modo de implementación pasivo (solo supervisión) o en línea (normal).



Nota: No puede configurar un modo pasivo y un modo en línea al mismo tiempo en el



ASA. Solo se permite un tipo de política de seguridad.

- En una implementación en línea, el módulo SFR inspecciona el tráfico en función de la política de control de acceso y proporciona el veredicto al ASA para que tome las medidas adecuadas (permitir, denegar, etc.) en el flujo de tráfico. Este ejemplo muestra cómo crear un policy-map y configurar el módulo SFR de ASA en el modo en línea.
- Verifique que la actual `global_policy` está configurada con otra configuración (`show run policy-map global_policy`, `show run service-policy`) de módulo, luego primero restablezca/quite la `global_policy` para otra configuración de módulo y luego vuelva a configurar la `global_policy`.

```
<#root>
ciscoasa(config)#
policy-map global_policy

ciscoasa(config-pmap)#
class sfr

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

- En una implementación pasiva, se envía una copia del tráfico al módulo de servicio SFR, pero no se devuelve al ASA. El modo pasivo le permite ver las acciones que el módulo SFR habría completado con respecto al tráfico. También le permite evaluar el contenido del tráfico, sin un impacto en la red.

Si desea configurar el módulo SFR en modo pasivo, utilice la palabra `monitor-only` clave (como se muestra en el siguiente ejemplo). Si no incluye la palabra clave, el tráfico se envía en modo en línea.

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



Advertencia: el `monitor-only` modo no permite al módulo de servicio SFR denegar o bloquear el tráfico malintencionado.



Precaución: puede ser posible configurar un ASA en el modo `monitor-only` con el uso



del `traffic-forward sfr monitor-only` comando `interface-level`; sin embargo, esta configuración es puramente para la funcionalidad de demostración y no se debe utilizar en un ASA de producción. El centro de asistencia técnica Cisco Technical Assistance Center (TAC) no admite ningún problema que se encuentre en esta función de demostración. Si desea implementar el servicio SFR de ASA en modo pasivo, configúrelo mediante un `policy-map`.

4. Especifique una ubicación y aplique la política. Puede aplicar una política de forma global o en una interfaz. Para invalidar la política global en una interfaz, puede aplicar una política de servicio a esa interfaz.

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

```
<#root>
ciscoasa(config)#
service-policy global_policy global
```



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

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

- Puede ejecutar este comando (`debug module-boot`) para habilitar la depuración al inicio de la instalación de la imagen de arranque SFR.
- Si ASA se atascó en el modo de recuperación y la consola no se activó, intente este comando (`sw-module module sfr recover stop`).
- Si el módulo SFR no pudo salir del estado de recuperación, puede intentar volver a cargar el ASA (`reload quick`). (Si el tráfico pasa, puede causar perturbaciones en la red). Si Still SFR se bloquea en el estado de recuperación, puede apagar el ASA y la `unplug the SSD` tarjeta e iniciar el ASA. Compruebe el estado del módulo y debe ser el estado INIT. De nuevo, apague el ASA, la `insert the SSD` tarjeta e inicie el ASA. puede iniciar la recreación de imágenes del módulo SFR de ASA.

Información Relacionada

- [Funciones de Cisco Secure IPS y Cisco NGIPS](#)
- [Registrar un dispositivo con FireSIGHT Management Center](#)
- [Guía de inicio rápido del módulo Cisco ASA FirePOWER](#)
- [Implementación de FireSIGHT Management Center en VMware ESXi](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

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).