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

Contenido

Introducción

Este documento describe cómo instalar y configurar un módulo Cisco FirePOWER (SFR) que se ejecute en un Cisco Adaptive Security Appliance (ASA) y cómo registrar el módulo SFR con Cisco FireSIGHT Management Center.

Prerequisites

Requirements

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

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

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

Componentes Utilizados

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

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

Nota: Si desea instalar FirePOWER (SFR) Services 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:

- Software FirePOWER versión 5.3.1 o posterior
- FireSIGHT Management Center FS2000, FS4000 o dispositivo virtual

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. 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 ASA SFR en modo de contexto único o múltiple y en modo enrutado o transparente.

Antes de comenzar

Considere 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)/Context Aware (CX) (que reemplazó por ASA SFR), debe quitarlo antes de configurar la política de servicio ASA SFR.
- Debe apagar cualquier otro módulo de software que se ejecute 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:

```
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 el **cxsc** se utiliza la palabra clave en lugar de **ips**:

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

```
ciscoasa# reload
```

- Cuando vuelva a crear una imagen de un módulo, utilice el mismo **shutdown** y **uninstall** comandos que se utilizan para quitar una imagen SFR antigua. Aquí tiene un ejemplo:

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

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

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

Instalar

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

Instalación del módulo SFR en el ASA

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

1. Descargue el software del sistema ASA SFR desde Cisco.com a un servidor HTTP, HTTPS o FTP al que se puede acceder desde la interfaz de administración de ASA SFR.
2. Descargue la imagen de inicio en el dispositivo. Puede utilizar Cisco Adaptive Security Device Manager (ASDM) o ASA CLI para descargar la imagen de inicio en el dispositivo. **Nota:** No transferir el software del sistema; se descarga más tarde en la unidad de estado sólido (SSD).Complete estos pasos para descargar la imagen de inicio a través del ASDM: Descargue la imagen de inicio en la estación de trabajo o colóquela en un servidor FTP, TFTP, HTTP, HTTPS, Server Message Block (SMB) o Secure Copy (SCP).Elegir**Tools > File Management** en el ASDM.Elija el comando adecuado File Transfer, ya sea *entre el PC local y Flash* o *entre el servidor remoto y la memoria Flash*.Transfiera el software de arranque a la unidad flash (disk0) del ASA.Complete estos pasos para descargar la imagen de inicio a través de ASA CLI:Descargue la imagen de inicio en un servidor FTP, TFTP, HTTP o HTTPS.Escriba el **copy** en la CLI para descargar la imagen de inicio en la unidad flash. Este es un ejemplo que utiliza el protocolo HTTP (reemplace el con la dirección IP o el nombre de host del servidor). Para el servidor FTP, la URL es similar a la siguiente:**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. Ingrese este comando para configurar la ubicación de la imagen de inicio de ASA SFR en la unidad flash ASA:

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

   Aquí tiene un ejemplo:
```
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 ASA SFR:

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

Durante este tiempo, si activa **debug module-boot** en el 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 se inicie el módulo SFR de ASA y, a continuación, abra una sesión de consola a 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 SFR de ASA recién instalada:

1. Pulse **Enter** después de abrir una sesión para alcanzar el mensaje de inicio de sesión. **Nota:** El nombre de usuario predeterminado es **admin**. La contraseña varía según la versión de software:**Adm!n123** 7.0.1 (nuevo dispositivo solo de fábrica), **Admin123** para 6.0 y posteriores, **Sourcefire** para pre-6.0.Aquí tiene un ejemplo:

```
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
```

Consejo: Si el arranque del módulo SFR ASA no se ha completado, el comando session falla y aparece un mensaje que indica que el sistema no puede conectarse sobre TTYS1. Si esto ocurre, espere a que se complete el inicio del módulo e inténtelo de nuevo.

2. Escriba el **setup** para configurar el sistema de modo que pueda instalar el paquete de software del sistema:

```
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 direcciones IPv4 o IPv6 estáticas. También puede utilizar DHCP para la configuración automática sin estado de IPv4 o IPv6.**DNS information** - Debe identificar al menos un servidor DNS y también puede establecer el nombre de dominio y el dominio de búsqueda.**NTP information** - Puede activar el protocolo de tiempo de red (NTP) y configurar los servidores NTP para establecer la hora del sistema.

3. Escriba el **system install** para instalar la imagen del software del sistema:

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

Incluir **noconfirm** si no desea responder a los mensajes de confirmación. Reemplace el **url** con la ubicación del **.pkg** archivo. Una vez más, puede utilizar un servidor FTP, HTTP o HTTPS. Aquí tiene un ejemplo:

```
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 URL es similar a la siguiente:**ftp://username:password@server-ip/asasfr-sys-5.3.1-152.pkg**.

Nota El SFR está en un "**Recover**" durante el proceso de instalación. Puede tardar hasta una hora en completar la instalación del módulo SFR. Una vez finalizada la instalación, el sistema se reinicia. Espere diez o más minutos para que se inicie la instalación del

componente de aplicación y para que se inicien los servicios ASA SFR. El resultado del **show module sfr** indica que todos los procesos son **Up**.

Configurar

Esta sección describe cómo configurar el software FirePOWER y el 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 ASA SFR.
   Nota: Ahora aparece un mensaje de inicio de sesión diferente porque el login ocurre en un módulo completamente funcional.Aquí tiene un ejemplo:

```
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 varía según la versión de software:**Adm!n123** 7.0.1 (nuevo dispositivo solo de fábrica), **Admin123** para 6.0 y posteriores,**Sourcefire** para pre-6.0.
3. Complete la configuración del sistema según se le solicite, lo que ocurre en este orden: Lea y acepte el acuerdo de licencia del usuario final (EULA).Cambie la contraseña del administrador.Configure la dirección de administración y la configuración de DNS, según se le solicite. **Nota:** Puede configurar las 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 ASA y una política de seguridad, debe registrarlo en FireSIGHT Management Center. Refiérase a Registro de un Dispositivo con FireSIGHT Management Center

para obtener más información. No puede realizar estas acciones con FireSIGHT Management Center:

- Configure las interfaces del módulo SFR ASA
- Apagar, reiniciar o administrar de otro modo los procesos del módulo ASA SFR
- Creación de copias de seguridad o restauración de copias de seguridad en los dispositivos del módulo SFR ASA
- Escriba las reglas de control de acceso para hacer coincidir el tráfico con el uso de las condiciones de etiqueta 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 ASA SFR:

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

   ```
   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:

   ```
   ciscoasa(config)# class-map sfr
   ciscoasa(config-cmap)# match access-list sfr_redirect
   ```
3. Especifique el modo de implementación. Puede configurar el dispositivo en un modo de implementación pasivo (solo monitor) o en línea (normal).
   Nota: No puede configurar tanto un modo pasivo como el modo en línea al mismo tiempo en el ASA. Solo se permite un tipo de directiva de seguridad.En una implementación en línea, el módulo SFR inspecciona el tráfico según la política de control de acceso y proporciona el veredicto al ASA para tomar la acción apropiada (Permitir, Denegar, etc.) en el flujo de tráfico. Este ejemplo muestra cómo crear un policy-map y configurar el módulo ASA SFR en el modo en línea. Compruebe que el **global_policy** se configura con otra configuración de módulo**(show run policy-map global_policy, show run service-policy)**, a continuación, restablezca/elimine primero global_policy para otra configuración de módulo y, a continuación, vuelva a configurar el **global_policy**.

   ```
   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 hubiera completado con respecto al tráfico. También le permite evaluar el contenido del tráfico, sin afectar a la red.

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

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

Advertencia: **monitor-only** el modo no permite que el módulo de servicio SFR niegue o bloquee el tráfico malintencionado.**Precaución:** Puede ser posible configurar un ASA en modo *solo monitor* con el uso del nivel de interfaz **traffic-forward sfr monitor-only** comando; sin embargo, esta configuración es únicamente para la funcionalidad de demostración y no se debe utilizar en un ASA de producción. Los problemas encontrados en esta función de demostración no son compatibles con Cisco Technical Assistance Center (TAC). Si desea implementar el servicio ASA SFR en modo pasivo, configúrelo con el uso de un *policy-map*.

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

   global aplica el policy map a todas las interfaces y el **interface** aplica la política a una interfaz. Sólo se permite una política global. En este ejemplo, la política se aplica globalmente:

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

   Precaución: El mapa de políticas **global_policy** es una política predeterminada. Si utiliza esta política y desea eliminarla en su dispositivo para solucionar problemas, asegúrese de comprender su implicación.

Verificación

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

Troubleshoot

- Puede ejecutar este comando (**debug module-boot**) para habilitar el debug al inicio de la instalación de la imagen de inicio SFR.
- Si el 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 recargar el ASA **(reload quick)**. (Si el tráfico pasa, puede causar perturbaciones en la red). Si Still SFR está atascado en el estado de recuperación, puede apagar el ASA y **unplug the SSD** e inicie ASA. Verifique el estado del módulo y debe ser el estado INIT. De nuevo, cierre el ASA, **insert the SSD** e inicie ASA. puede iniciar la recreación de imágenes del módulo ASA SFR.

Información Relacionada

- Cisco Secure IPS - Funciones de Cisco NGIPS
- Registro de 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