Instale y configure un Módulo de servicios de la potencia de fuego en una plataforma ASA

Contenido

Introducción

Este documento describe cómo instalar y configurar un módulo de la potencia de fuego de Cisco (SFR) que se ejecute en un dispositivo de seguridad adaptante de Cisco (ASA) y cómo registrar el módulo SFR con el centro de administración de Cisco FireSIGHT.

Prerrequisitos

Requisitos

Cisco recomienda que su reunión del sistema estos requisitos antes de que usted intente los procedimientos que se describen en este documento:

- Asegúrese de que usted tenga por lo menos 3GB del espacio libre en memoria USB (disk0), además del tamaño del software del inicio.
- Asegúrese de que usted tenga acceso al modo EXEC privilegiado. Para acceder al modo EXEC privilegiado, ingrese el **comando enable** en el CLI. Si una contraseña no fue fijada, entonces Presione ENTER:

```
ciscoasa> enablePassword:ciscoasa#
```

Componentes Utilizados

Para instalar los servicios de la potencia de fuego en Cisco ASA, se requieren estos componentes:

- Versión de software 9.2.2 de Cisco ASA o más adelante
- Plataformas ASA de Cisco 5512-X con 5555-X
- Versión de software 5.3.1 de la potencia de fuego o más adelante

  Nota: Si usted quiere instalar los servicios de la potencia de fuego (SFR) en un módulo de hardware ASA 5585-X, lea la instalación de los servicios de la potencia de fuego (SFR) en el módulo de hardware ASA 5585-X.

Estos componentes se requieren en el centro de administración de Cisco FireSIGHT:

- Versión de software 5.3.1 de la potencia de fuego o más adelante
- Centro de administración FS2000, FS4000 o dispositivo virtual de FireSIGHT

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

El módulo de la potencia de fuego de Cisco ASA, también conocido como el ASA SFR, proporciona los servicios del Firewall de la última generación, por ejemplo:

- Sistema de prevención de intrusiones de la última generación (NGIPS)
- Visibilidad y control (AVC) de la aplicación
- Filtrado de URL
- Protección avanzada de Malware (amperio)

  Nota: Usted puede utilizar el módulo ASA SFR en solo o el modo de contexto múltiple, y en ruteado o el modo transparente.

Antes de comenzar

Considere esta información importante antes de que usted intente los procedimientos que se describen en este documento:

- Si usted tiene una directiva de servicio activo que reoriente el tráfico a un módulo enterado del Sistema de prevención de intrusiones (IPS) /Context (CX) (ese usted substituyó por el ASA SFR), usted debe quitarlo antes de que usted configure la política de servicio ASA SFR.

- Usted debe apagar cualquier módulo del otro software que se ejecute actualmente. Un dispositivo puede ejecutar un solo en un momento del módulo de software. Usted debe hacer esto del ASA CLI. Por ejemplo, estos comandos apagan y desinstalan el módulo de software IPS, y después recargan el ASA:

  `ciscoasa# sw-module module ips shutdownciscoasa# sw-module module ips uninstallciscoasa# reload`Los comandos que se utilizan para quitar el módulo CX son lo mismo, a menos que la

palabra clave del **cxsc** se utilice en vez del **IPS**:

```
ciscoasa# sw-module module cxsc shutdownciscoasa# sw-module module cxsc uninstallciscoasa# reload
```

- Cuando usted nueva imagen un módulo, utiliza lo mismo **apaga** y **desinstala los** comandos que se utilizan para quitar una vieja imagen SFR. 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 la ejecución del sistema.

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

Instalar

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

Instale el módulo SFR en el ASA

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

1. Descargue el software del sistema ASA SFR del cisco.com a un HTTP, a un HTTPS, o a un servidor FTP que sea accesible de la interfaz de administración ASA SFR.

2. Descargue la imagen del arranque de sistema al dispositivo. Usted puede utilizar el Cisco Adaptive Security Device Manager (ASDM) o el ASA CLI para descargar la imagen del arranque de sistema al dispositivo. Nota: No transfiera el software del sistema; se descarga más adelante a la unidad de estado sólido (SSD).Complete estos pasos para descargar la imagen del arranque de sistema vía el ASDM:

   Descargue la imagen del arranque de sistema a su puesto de trabajo, o póngala en un servidor FTP, TFTP, HTTP, HTTPS, del Bloque de mensaje del servidor (SMB), o del Secure Copy (SCP).

   Elija las **herramientas > la administración de archivos** en el ASDM.

   Elija el comando apropiado de la transferencia de archivos, o *en medio PC local y el Flash* o *entre el servidor remoto y el Flash*.

   Transferencia el software del inicio a memoria USB (disk0) en el ASA.Complete estos pasos para descargar la imagen del arranque de sistema vía el ASA CLI:

   Descargue la imagen del arranque de sistema en un FTP, un TFTP, un HTTP, o un servidor HTTPS.

   Ingrese el **comando copy** en el CLI para descargar la imagen del arranque de sistema a la

unidad de destello.

Aquí está un ejemplo que utiliza el protocolo HTTP (substituya el **<HTTP_Server>** por su dirección IP del servidor o nombre del host):

```
ciscoasa# copy http://<HTTP_SERVER>/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 del arranque de sistema ASA SFR en la unidad del 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 del arranque de sistema ASA SFR:

   `ciscoasa# sw-module module sfr recover boot`Durante este tiempo, si usted habilita el **arranque del módulo del debug** en el ASA, se imprimen estos debugs:

   ```
   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 5 a 15 minutos el módulo ASA SFR a arrancar, y después para abrir a una sesión de consola en la imagen del arranque de sistema operativa ASA SFR.

Configure la imagen del arranque de sistema ASA SFR

Complete estos pasos para configurar el imagen del arranque de sistema nuevamente instalada ASA SFR:

1. Presione ENTER después de que usted abra una sesión para alcanzar el prompt de inicio de sesión. Nota: El nombre de usuario predeterminado es **admin**, y la contraseña predeterminada es **Admin123**.Aquí tiene un ejemplo:

   ```
   ciscoasa# session sfr consoleOpening console session with module sfr.Connected to module
   sfr. Escape character sequence is 'CTRL-^X'.Cisco ASA SFR Boot Image 5.3.1asasfr login:
   adminPassword: Admin123
   ```
   Consejo: Si el arranque del módulo ASA SFR no ha completado, el comando session falla y un mensaje aparece indicar que el sistema no puede conectar sobre TTYS1. Si ocurre esto, espere el arranque del módulo para completar y para intentar otra vez.
2. Ingrese el **comando setup** para configurar el sistema de modo que usted pueda instalar el paquete del software del sistema:

   ```
   asasfr-boot> setup                          Welcome to SFR Setup
   [hit Ctrl-C to abort]                         Default values are inside []
   ```
   Le entonces indican para esta información:

   Nombre del host - El nombre del host puede ser hasta 65 caracteres alfanuméricos, sin los espacios. El uso de los guiones se permite.

   Dirección de red - La dirección de red puede ser direccionamientos estáticos del IPv4 o del IPv6. Usted puede también utilizar el DHCP para el IPv4, o la autoconfiguración apátrida del IPv6.

   Información DNS - Usted debe identificar por lo menos un servidor del Domain Name System (DNS), y usted puede también fijar el Domain Name y buscar el dominio.

   Información de NTP - Usted puede habilitar el Network Time Protocol (NTP) y configurar a los servidores NTP para fijar el Tiempo del sistema.

3. Ingrese el **comando install del sistema** para instalar la imagen del software del sistema:

   ```
   asasfr-boot >system install [noconfirm] url
   ```
   Incluya la opción del **noconfirm** si usted no quiere responder a los mensajes de confirmación. Substituya la palabra clave **URL** por la ubicación del archivo **.package**. Aquí tiene un ejemplo:

   ```
   asasfr-boot >system install http:/<HTTP_SERVER>/asasfr-sys-5.3.1-
   152.pkgVerifyingDownloadingExtractingPackage Detail Description: Cisco ASA-FirePOWER 5.3.1-
   152 System Install Requires reboot: YesDo you want to continue with upgrade? [y]: yWarning:
   Please do not interrupt the process or turn off the system. Doing so might leave system in
   ```

```
unusable state.UpgradingStarting upgrade process ...Populating new system imageReboot 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.
```

Nota: Cuando la instalación es completa, el sistema reinicia. Permita que diez o más minutos para la Instalación del componente de la aplicación y para que los servicios ASA SFR comiencen. La salida del comando del **sfr del módulo show** debe indicar que todos los procesos están **para arriba**.

Configurar

Esta sección describe cómo configurar el software de la potencia de fuego y el centro de administración de FireSIGHT, y cómo reorientar el tráfico al módulo SFR.

Configure el software de la potencia de fuego

Complete estos pasos para configurar el software de la potencia de fuego:

1. Abra una sesión en el módulo ASA SFR. Nota: Un diverso prompt de inicio de sesión ahora aparece porque el login ocurre en un módulo lleno-funcional.Aquí tiene un ejemplo:

   ```
   ciscoasa# session sfrOpening 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 del usuario administrador y la contraseña **Sourcefire**.
3. Complete la configuración del sistema según lo indicado, que ocurre en esta orden:

   Lea y valide el acuerdo de licencia de usuario final (EULA).

   Cambie la clave del administrador.

   Configure la dirección de administración y las configuraciones DNS, según lo indicado. Nota: Usted puede configurar a las direcciones de administración del IPv4 y del 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]: yDo 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]:198.51.100.3Enter an IPv4 netmask for the
   management interface [255.255.255.0]: 255.255.255.0Enter the IPv4 default gateway for the
   management interface []: 198.51.100.1Enter a fully qualified hostname for this system
   [Sourcefire3D]: asasfr.example.comEnter a comma-separated list of DNS servers or 'none' []:
   198.51.100.15, 198.51.100.14Enter a comma-separated list of search domains or 'none'
   [example.net]: example.comIf your networking information has changed, you will need to
   reconnect.For HTTP Proxy configuration, run 'configure network http-proxy'
   ```
4. Espera para que el sistema se configure de nuevo.

Configure el centro de administración de FireSIGHT

Para manejar un módulo y la política de seguridad ASA SFR, usted debe registrarla con un centro de administración de FireSIGHT. Usted no puede realizar estas acciones con un centro de administración de FireSIGHT:

- Configure las interfaces de módulo ASA SFR
- Apague, recomience, o maneje de otra manera los procesos del módulo ASA SFR
- Cree los respaldos, o restablezca los respaldos, a los dispositivos de módulo ASA SFR
- Escriba las reglas del control de acceso para hacer juego el tráfico con el uso de las condiciones de la etiqueta del VLA N

Reoriente el tráfico al módulo SFR

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

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

   ```
   ciscoasa(config)# access-list sfr_redirect extended permit ip any any
   ```
2. Cree un clase-mapa para hacer juego el tráfico en una lista de acceso:

   ```
   ciscoasa(config)# class-map sfrciscoasa(config-cmap)# match access-list sfr_redirect
   ```
3. Especifique el modo del despliegue. Usted puede configurar su dispositivo en un modo (normal) pasivo (monitor-solamente) o en línea del despliegue. Nota: Usted no puede configurar un modo pasivo y el modo en línea al mismo tiempo en el ASA. Se permite a solamente un tipo de política de seguridad.En un despliegue en línea, después de que se caiga el tráfico indeseado y cualquier otra acción que sea aplicada por la directiva se realizan, el tráfico se vuelve al ASA para el procesamiento adicional y la última transmisión. Este ejemplo muestra cómo crear un directiva-mapa y configurar el módulo ASA SFR en el modo en línea:

   ```
   ciscoasa(config)# policy-map global_policyciscoasa(config-pmap)# class sfrciscoasa(config-pmap-c)# sfr fail-open
   ```
   En un despliegue pasivo, una copia del tráfico se envía al módulo de servicio SFR, pero no se vuelve al ASA. El modo pasivo permite que usted vea las acciones que el módulo SFR habría completado con respecto al tráfico. También permite que usted evalúe el contenido del tráfico, sin un impacto a la red.

   Si usted quiere configurar el módulo SFR en el modo pasivo, utilice la palabra clave del **monitor-solamente** (tal y como se muestra en del próximo ejemplo). Si usted no incluye la palabra clave, el tráfico se envía en el modo en línea.

   ```
   ciscoasa(config-pmap-c)# sfr fail-open monitor-only
   ```
   Advertencia: El modo del **monitor-solamente** no permite que el módulo de servicio SFR niegue o bloquee el tráfico malévolo.Precaución: Puede ser que sea posible configurar un ASA en el modo del *monitor-solamente* con el uso del comando tráfico-**delantero del monitor-solamente del sfr del interfaz-**nivel; sin embargo, esta configuración está puramente para las funciones de la demostración y no se debe utilizar en una producción ASA. Ninguna problemas que se

encuentran en esta característica de la demostración no son soportados por el Centro de Asistencia Técnica de Cisco (TAC). Si usted desea de desplegar el servicio ASA SFR en el modo pasivo, configurelo con el uso de un directiva-*mapa*.

4. Especifique una ubicación y aplique la directiva. Usted puede aplicar una directiva global o en una interfaz. Para reemplazar la política global en una interfaz, usted puede aplicar una política de servicio a esa interfaz.

   La palabra clave global aplica la correspondencia de políticas a todas las interfaces, y la palabra clave de la **interfaz** aplica la directiva a una interfaz. Se permite solamente una política global. En este ejemplo, la directiva se aplica global:

   `ciscoasa(config)# service-policy global_policy global` Precaución: **El global_policy de la** correspondencia de políticas es una política predeterminada. Si usted utiliza esta directiva y quiere quitarla en su dispositivo para los propósitos de Troubleshooting, asegúrese de que usted entienda su implicación.

Verificación

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

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Registre un dispositivo con un centro de administración de FireSIGHT
- Despliegue del centro de administración de FireSIGHT en VMware ESXi
- Escenarios de configuración de la Administración de IPS en un módulo ips 5500-X
- Soporte Técnico y Documentación - Cisco Systems