

# Supervisión del módulo de servicio de la neutralización en el ASA para evitar los eventos de falla indeseados (SFR/CX/IPS/CSC).

## Contenido

[Introducción](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Marque los componentes monitoreados corriente.](#)

[Marque el estatus del módulo de servicio de las unidades ASA.](#)

[Verifique la directiva del modo del fall del módulo de servicio:](#)

[Inhabilite la supervisión del módulo de servicio.](#)

[Verificación](#)

[Verifique que la supervisión del módulo de servicio esté inhabilitada.](#)

[Para probar la recarga el módulo recibido por la unidad activa.](#)

[Supervisión del módulo de servicio del permiso.](#)

[Verifique que el módulo de servicio esté habilitado.](#)

[Troubleshooting](#)

[El problema 1. ASA guarda el fallar encima, y se muestra este mensaje “indicador luminoso LED amarillo de la placa muestra gravedad menor del servicio en la otra unidad ha fallado”.](#)

[Solución](#)

[Problema 2. Mi ASA no soporta 9.3\(1\) o no puedo actualizarlo. ¿Cómo puedo evitar los eventos de falla?](#)

[Solución](#)

[Identifique la correspondencia y la directiva de la clase usadas.](#)

[Inhabilite el cambio de dirección del tráfico al módulo.](#)

[Verifique que el cambio de dirección ASA al módulo esté inhabilitado.](#)

[El tráfico del permiso reorienta al módulo.](#)

## Introducción

Este documento describe cómo inhabilitar la supervisión en los módulos SourceFire (SFR), el contexto enterado (CX), el Sistema de prevención de intrusiones (IPS), la Seguridad contenida y el control (CSC) en un entorno de recuperación tras falla adaptante del dispositivo de seguridad (ASA).

Contribuido por Cesar López, ingeniero de Cisco TAC.

## Prerrequisitos

## Requisitos

Cisco recomienda que usted tiene conocimiento de los temas siguientes:

- Configuración del dispositivo de seguridad adaptante.
- Conocimiento de la [Conmutación por falla ASA para la Alta disponibilidad](#).

De la versión 9.3(1), esta característica es configurable. Antes de la versión mencionada, el módulo será monitoreado siempre. Una solución alternativa se puede utilizar para las versiones anteriores descritas en este documento.

## Componentes Utilizados

Este documento se basa en estas versiones de software y hardware:

- Versión de ASA de Cisco 9.3(1) y posterior.
- 5500-X Series ASA con los servicios de la potencia de fuego, la Seguridad sensible al contexto ASA CX o el módulo ips.

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, debe asegurarse de comprender el posible impacto que puede tener un comando.

## Antecedentes

Por abandono, el ASA monitorea un módulo de servicio instalado. Si detectan a un error en el módulo de la unidad activa, se acciona la Conmutación por falla del dispositivo.

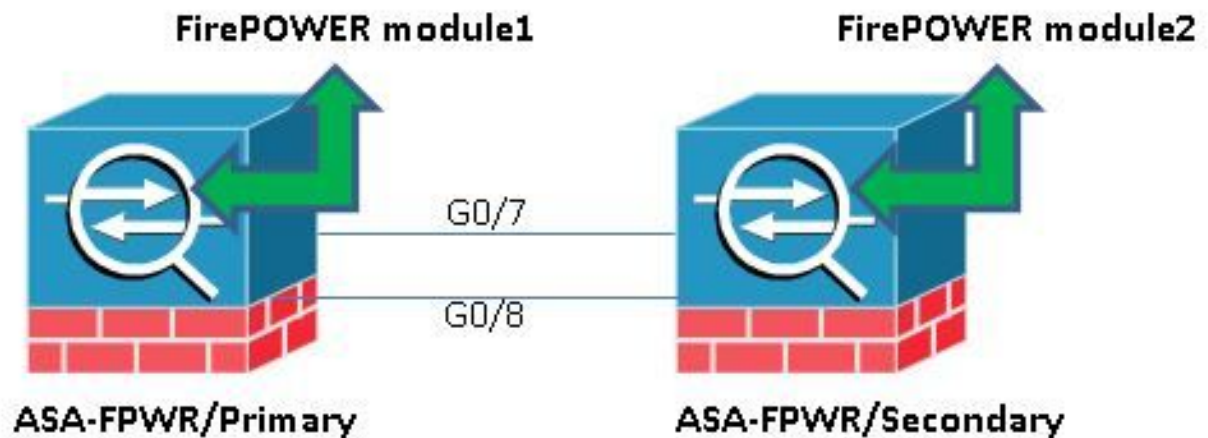
Puede ser útil inhabilitar este monitor cuando hay una recarga programada del módulo de servicio o fallas del módulo continuas lo mismo sin querer tener un evento de falla ASA.

Nota: El ASA necesita desviar el tráfico al módulo para ser monitoreado por el proceso de la Conmutación por falla.

## Configurar

### Diagrama de la red

Este documento utiliza esta configuración:



## Configuraciones

Esta configuración se utiliza en los dispositivos del laboratorio para demostrar la función de monitor mencionada en este documento. Solamente la configuración pertinente es incluida. Algunas de las líneas de esta salida se omiten.

```
ASA Version 9.3(3)
!
hostname ASA-FPWR
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.88.247.5 255.255.255.224 standby 10.88.247.6
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.10.111 255.255.255.0 standby 192.168.10.112
!
...
!
interface GigabitEthernet0/6
description LAN Failover Interface
!
interface GigabitEthernet0/7
description STATE Failover Interface
!
...

failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/6
failover link statelink GigabitEthernet0/7
failover interface ip folink 1.1.1.1 255.255.255.0 standby 1.1.1.2
failover interface ip statelink 2.2.2.1 255.255.255.0 standby 2.2.2.2
!
...
```

```

!
class-map SFR
match any
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns migrated_dns_map_1
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns migrated_dns_map_1
inspect ftp
inspect h323 h225
inspect h323 ras
inspect ip-options
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
class SFR
sfr fail-open
!
service-policy global_policy global
prompt hostname context priority state
no call-home reporting anonymous
Cryptochecksum:b268e0095f175a26aa94d120e9041c29
: end

```

## Marque los componentes monitoreados corriente.

Cuando los ASA están en el modo de fallas, el módulo de servicio instalado se monitorea por abandono, apenas como el dispositivo interconecta. Este comando se puede utilizar, para considerar se monitorean qué componentes actuales:

```

ASA-FPWR/pri/act# show run all monitor-interface
monitor-interface outside
monitor-interface inside
monitor-interface service-module

```

## Marque el estatus del módulo de servicio de las unidades ASA.

La salida de la **Conmutación por falla de la demostración** muestra el estado actual de cada módulo de la unidad:

```

ASA-FPWR/pri/act# show failover
Failover On
Failover unit Primary
Failover LAN Interface: folink GigabitEthernet0/6 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 316 maximum

```

```
MAC Address Move Notification Interval not set
Version: Ours 9.3(3), Mate 9.3(3)
Last Failover at: 14:30:44 UTC Aug 6 2015
This host: Primary - Active
Active time: 85 (sec)
slot 0: ASA5545 hw/sw rev (1.0/9.3(3)) status (Up Sys)
Interface outside (10.88.247.5): Normal (Monitored)
Interface inside (192.168.10.111): Normal (Monitored)
  slot 1: SFR5545 hw/sw rev (N/A/5.3.1-152) status (Up/Up)
  ASA FirePOWER, 5.3.1-152, Up
Other host: Secondary - Standby Ready
Active time: 396 (sec)
slot 0: ASA5545 hw/sw rev (1.0/9.3(3)) status (Up Sys)
Interface outside (10.88.247.6): Normal (Monitored)
Interface inside (192.168.10.112): Normal (Monitored)
  slot 1: SFR5545 hw/sw rev (N/A/5.3.1-155) status (Up/Up)
  ASA FirePOWER, 5.3.1-155, Up
```

Si va el módulo de servicio de una unidad activa abajo, un evento de falla ocurre. La unidad activa llega a ser espera, y que antes estaba en espera la unidad toma rol activo. En algunos escenarios, esto causa algunas características que no sean soportadas por una falla de estado, al reconverge.

## Verifique la directiva del modo del fall del módulo de servicio:

Si un fracaso-openpolicy se utiliza para enviar el tráfico al módulo, trafique continúa pasando con el ASA sin el envío al módulo de servicio. Esto puede ser una manera más transparente de superar un estado de inactividad previsto del módulo.

Advertencia: Si se ha aplicado una directiva del fracaso-cierre, después, todo el tráfico que correspondía con el clase-mapa usado para desviar el tráfico al módulo es caído por el ASA.

Para conocer el estatus de la directiva usado, funcione con la servicio-directiva del comando show [sfr|CX|IPS|csc].

```
ASA-FPWR/pri/act# show service-policy sfr
```

```
Global policy:
Service-policy: global_policy
Class-map: SFR
SFR: card status Up, mode fail-open
packet input 0, packet output 0, drop 0, reset-drop 0
```

Lo mismo pueden ser vistas marcando la configuración modular del Marco de políticas (MPF):

```
ASA-FPWR/pri/act# show run policy-map
!
policy-map type inspect dns migrated_dns_map_1
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns migrated_dns_map_1
inspect ftp
inspect h323 h225
inspect h323 ras
inspect ip-options
inspect netbios
```

```
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
class SFR
sfr fail-open
!
ASA-FPWR/pri/act#
```

## Supervisión del módulo de servicio de la neutralización.

Este comando, hace la parada del proceso de la Conmutación por falla la supervisión del módulo de servicio. Cualquier recarga o Troubleshooting prevista se puede hacer al módulo sin una Conmutación por falla, en caso del módulo que va “abajo” o “insensible”.

```
no monitor-interface service-module
```

## Verificación

### Verifique que la supervisión del módulo de servicio esté inhabilitada.

Bajo configuración corriente, se niega el comando de la monitor-interfaz.

```
ASA-FPWR/pri/act(config)# show run all monitor-interface
monitor-interface outside
monitor-interface inside
no monitor-interface service-module
```

### Para probar la recarga el módulo recibido por la unidad activa.

Como demostración, el módulo de la potencia de fuego en esta unidad se recarga para confirmar si la unidad de transmisión por falla activa permanece en este papel.

Salida del módulo de la potencia de fuego en el ASA primario/unidad activa.

```
Sourcefire ASA5545 v5.3.1 (build 152)

Last login: Thu Aug 6 14:40:46 on ttyS1
>
>system reboot
This command will reboot the system. Continue?
Please enter 'YES' or 'NO': YES

Broadcast message from root (Thu Aug 6 14:40:59 2015):

The system is going down for reboot NOW!

Escape Sequence detected
Console session with module sfr terminated.
```

Salida del ASA primario/unidad activa mientras que las recargas del módulo.

La unidad permanece en rol activo.

```
ASA-FPWR/pri/act# show failover
```

```
Failover On
Failover unit Primary
Failover LAN Interface: folink GigabitEthernet0/6 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 316 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.3(3), Mate 9.3(3)
Last Failover at: 14:30:44 UTC Aug 6 2015
This host: Primary - Active
Active time: 616 (sec)
slot 0: ASA5545 hw/sw rev (1.0/9.3(3)) status (Up Sys)
Interface outside (10.88.247.5): Normal (Monitored)
Interface inside (192.168.10.111): Normal (Monitored)
slot 1: SFR5545 hw/sw rev (N/A/5.3.1-152) status (Unresponsive/Down)
ASA FirePOWER, 5.3.1-152, Not Applicable
Other host: Secondary - Standby Ready
Active time: 396 (sec)
slot 0: ASA5545 hw/sw rev (1.0/9.3(3)) status (Up Sys)
Interface outside (10.88.247.6): Normal (Monitored)
Interface inside (192.168.10.112): Normal (Monitored)
slot 1: SFR5545 hw/sw rev (N/A/5.3.1-155) status (Up/Up)
ASA FirePOWER, 5.3.1-155, Up
```

**Salida del ASA secundario/unidad en espera mientras que el módulo recarga:**

**La unidad en espera no detecta este estatus como un error y doesn't para tomar rol activo.**

```
ASA-FPWR/sec/stby# show failover
Failover On
Failover unit Secondary
Failover LAN Interface: folink GigabitEthernet0/6 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 316 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.3(3), Mate 9.3(3)
Last Failover at: 14:30:59 UTC Aug 6 2015
This host: Secondary - Standby Ready
Active time: 396 (sec)
slot 0: ASA5545 hw/sw rev (1.0/9.3(3)) status (Up Sys)
Interface outside (10.88.247.6): Normal (Monitored)
Interface inside (192.168.10.112): Normal (Monitored)
slot 1: SFR5545 hw/sw rev (N/A/5.3.1-155) status (Up/Up)
ASA FirePOWER, 5.3.1-155, Up
Other host: Primary - Active
Active time: 670 (sec)
slot 0: ASA5545 hw/sw rev (1.0/9.3(3)) status (Up Sys)
Interface outside (10.88.247.5): Normal (Monitored)
Interface inside (192.168.10.111): Normal (Monitored)
slot 1: SFR5545 hw/sw rev (N/A/5.3.1-152) status (Unresponsive/Down)
ASA FirePOWER, 5.3.1-152, Not Applicable
```

**Supervisión del módulo de servicio del permiso.**

**Para habilitar la supervisión del módulo, funcione con este comando:**

```
monitor-interface service-module
```

**Verifique que el módulo de servicio esté habilitado.**

El comando del módulo de servicio no se niega más.

```
ASA-FPWR/pri/act(config)# show run all monitor-interface
monitor-interface outside
monitor-interface inside
monitor-interface service-module
```

## Troubleshooting

**El problema 1. ASA guarda el fallar encima, y se muestra este mensaje “indicador luminoso LED amarillo de la placa muestra gravedad menor del servicio en la otra unidad ha fallado”.**

Si se detectan un o mucho eventos de falla, el **historial de la Conmutación por falla de la demostración** se puede utilizar para conocer la razón posible.

```
ASA-FPWR/sec/act# show failover history
=====
From State To State Reason
=====
14:38:58 UTC Aug 5 2015
Bulk Sync Standby Ready Detected an Active mate

14:39:05 UTC Aug 5 2015
Standby Ready Bulk Sync No Error

14:39:17 UTC Aug 5 2015
Bulk Sync Standby Ready No Error

14:48:12 UTC Aug 6 2015
Standby Ready Just Active Service card in other unit has failed

14:48:12 UTC Aug 6 2015
Just Active Active Drain Service card in other unit has failed

14:48:12 UTC Aug 6 2015
Active Drain Active Applying Config Service card in other unit has failed

14:48:12 UTC Aug 6 2015
Active Applying Config Active Config Applied Service card in other unit has failed

14:48:12 UTC Aug 6 2015
Active Config Applied Active Service card in other unit has failed
```

La unidad en espera del now muestra este mensaje:

```
14:47:56 UTC Aug 6 2015
Standby Ready Failed Detect service card failure
```

Si el “indicador luminoso LED amarillo de la placa muestra gravedad menor del servicio en la otra unidad ha fallado” se considera el mensaje, la Conmutación por falla sucedió porque la unidad activa detectó su propio módulo como insensible.

Si el módulo permanece en el estatus “insensible”, el ASA afectado permanece en el modo **fallado**.

```
ASA-FPWR/sec/stby# Waiting for the earlier webvpn instance to terminate...
Previous instance shut down. Starting a new one.
```



Switching to Active

```
ASA-FPWR/sec/act#
ASA-FPWR/sec/act# show failover
Failover On
Failover unit Secondary
Failover LAN Interface: folink GigabitEthernet0/6 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 316 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.3(3), Mate 9.3(3)
Last Failover at: 14:24:23 UTC Aug 6 2015
This host: Secondary - Active
Active time: 38 (sec)
slot 0: ASA5545 hw/sw rev (1.0/9.3(3)) status (Up Sys)
Interface outside (10.88.247.5): Normal (Waiting)
Interface inside (192.168.10.111): Normal (Waiting)
slot 1: SFR5545 hw/sw rev (N/A/5.3.1-155) status (Up/Up)
ASA FirePOWER, 5.3.1-155, Up
Other host: Primary - Failed
Active time: 182 (sec)
slot 0: ASA5545 hw/sw rev (1.0/9.3(3)) status (Up Sys)
Interface outside (10.88.247.6): Normal (Waiting)
Interface inside (192.168.10.112): Normal (Waiting)
slot 1: SFR5545 hw/sw rev (N/A/5.3.1-152) status (Unresponsive/Down)
ASA FirePOWER, 5.3.1-152, Not Applicable
```

## Solución

La supervisión del módulo de servicio puede ser inhabilitada mientras que otros pasos para resolver problemas el problema se pueden hacer para recuperar el módulo.

```
no monitor-interface service-module
```

## Problema 2. Mi ASA no soporta 9.3(1) o no puedo actualizarlo. ¿Cómo puedo evitar los eventos de falla?

Las ASA5500 Series de la herencia no soportan 9.3(1) la versión y, incluso si no lo hacen los módulos del software de soporte, algunas de ellas tienen módulos de hardware tales como CSC o el IPS.

Incluso con las nuevas ASA5500-X Series, hay algunos dispositivos con las versiones debajo de la que soporta la supervisión de la neutralización.

## Solución

El ASA monitorea solamente el módulo si hay una directiva configurada para pasarle el tráfico. Así pues, para evitar una Conmutación por falla, la directiva del módulo puede ser quitada.

**Identifique la correspondencia y la directiva de la clase usadas.**

En este caso, esta configuración se utiliza para quitar la diversión del tráfico de un módulo de la potencia de fuego.

```

class-map SFR
match any
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns migrated_dns_map_1
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns migrated_dns_map_1
inspect ftp
inspect h323 h225
inspect h323 ras
inspect ip-options
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
class SFR
sfr fail-open
!

```

**La servicio-directiva del comando show [csc|cxsc|IPS|el sfr] se puede utilizar para detectar la correspondencia y el estado actual de la clase.**

```
ASA-FPWR/pri/act# show service-policy sfr
```

```

Global policy:
Service-policy: global_policy
Class-map: SFR
SFR: card status Up, mode fail-open
packet input 0, packet output 0, drop 0, reset-drop

```

### **Cambio de dirección del tráfico de la neutralización al módulo.**

Después de que se quite la directiva, no se envía ningún otro tráfico del ASA al módulo.

```

ASA-FPWR/pri/act# conf t
ASA-FPWR/pri/act(config)# policy-map global_policy
ASA-FPWR/pri/act(config-pmap)# class SFR
ASA-FPWR/pri/act(config-pmap-c)# no sfr fail-open
ASA-FPWR/pri/act(config-pmap-c)# end
ASA-FPWR/pri/act#

```

### **Verifique que el cambio de dirección ASA al módulo esté inhabilitado.**

El mismo **comando show** puede ser utilizado para verificar que el tráfico va no más al módulo. La salida debe estar vacía.

```

ASA-FPWR/pri/act# show service-policy sfr
ASA-FPWR/pri/act#

```

Incluso si el módulo es insensible, sigue habiendo la unidad activa en el mismo papel.

```
ASA-FPWR/pri/act# show module sfr
```

```
Mod Card Type Model Serial No.
```

```
-----  
sfr FirePOWER Services Software Module ASA5545 FCH18457CNM
```

```
Mod MAC Address Range Hw Version Fw Version Sw Version
```

```
-----  
sfr 74a0.2fa4.6c7a to 74a0.2fa4.6c7a N/A N/A 5.3.1-152
```

```
Mod SSM Application Name Status SSM Application Version
```

```
-----  
sfr ASA FirePOWER Not Applicable 5.3.1-152
```

```
Mod Status Data Plane Status Compatibility
```

```
-----  
sfr Unresponsive Not Applicable
```

```
ASA-FPWR/pri/act# show failover
```

```
Failover On
```

```
Failover unit Primary
```

```
Failover LAN Interface: folink GigabitEthernet0/6 (up)
```

```
Reconnect timeout 0:00:00
```

```
Unit Poll frequency 1 seconds, holdtime 15 seconds
```

```
Interface Poll frequency 5 seconds, holdtime 25 seconds
```

```
Interface Policy 1
```

```
Monitored Interfaces 2 of 316 maximum
```

```
MAC Address Move Notification Interval not set
```

```
Version: Ours 9.3(3), Mate 9.3(3)
```

```
Last Failover at: 14:51:20 UTC Aug 6 2015
```

```
This host: Primary - Active
```

```
Active time: 428 (sec)
```

```
slot 0: ASA5545 hw/sw rev (1.0/9.3(3)) status (Up Sys)
```

```
Interface outside (10.88.247.5): Normal (Monitored)
```

```
Interface inside (192.168.10.111): Normal (Monitored)
```

```
slot 1: SFR5545 hw/sw rev (N/A/5.3.1-152) status (Unresponsive/Down)
```

```
ASA FirePOWER, 5.3.1-152, Not Applicable
```

```
Other host: Secondary - Standby Ready
```

```
Active time: 204 (sec)
```

```
slot 0: ASA5545 hw/sw rev (1.0/9.3(3)) status (Up Sys)
```

```
Interface outside (10.88.247.6): Normal (Monitored)
```

```
Interface inside (192.168.10.112): Normal (Monitored)
```

```
slot 1: SFR5545 hw/sw rev (N/A/5.3.1-155) status (Up/Up)
```

```
ASA FirePOWER, 5.3.1-155, Up
```

## El tráfico del permiso reorienta al módulo.

Una vez que el tráfico necesita ser devuelto al módulo, la directiva fracaso-abierta o del fracaso-cierre se puede agregar detrás.

```
ASA-FPWR/pri/act(config)# policy-map global_policy
```

```
ASA-FPWR/pri/act(config-pmap)# class SFR
```

```
ASA-FPWR/pri/act(config-pmap-c)# sfr fail-open
```

```
ASA-FPWR/pri/act(config-pmap-c)# end
```

```
ASA-FPWR/pri/act#
```