Desactive la supervisión del módulo de servicio en ASA para evitar eventos de conmutación por fallo no deseados (SFR/CX/IPS/CSC).

Contenido

Introducción

Este documento describe cómo inhabilitar la supervisión en los módulos SourceFire (SFR), Context Aware (CX), Intrusion Prevention System (IPS), Content Security and Control (CSC) en un entorno de recuperación ante fallos Adaptive Security Appliance (ASA).

Colaborado por Cesar Lopez, Ingeniero del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que conozca los siguientes temas:

- Configuración de Adaptive Security Appliance.
- Conocimiento de ASA Failover para Alta Disponibilidad.

Desde la versión 9.3(1), esta función es configurable. Antes de la versión mencionada, el módulo siempre será monitoreado. Se puede utilizar una solución alternativa para las versiones anteriores descritas en este documento.

Componentes Utilizados

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

- Cisco ASA Versión 9.3(1) y posterior.
- ASA serie 5500-X con servicios FirePOWER, módulo *ASA CX* Context-Aware Security o IPS.

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 la red está funcionando, debe asegurarse de comprender el posible impacto que puede tener un comando.

Antecedentes

De forma predeterminada, el ASA supervisa un módulo de servicio instalado. Si se detecta una falla en el módulo de la unidad activa, se activa la conmutación por fallas del dispositivo.

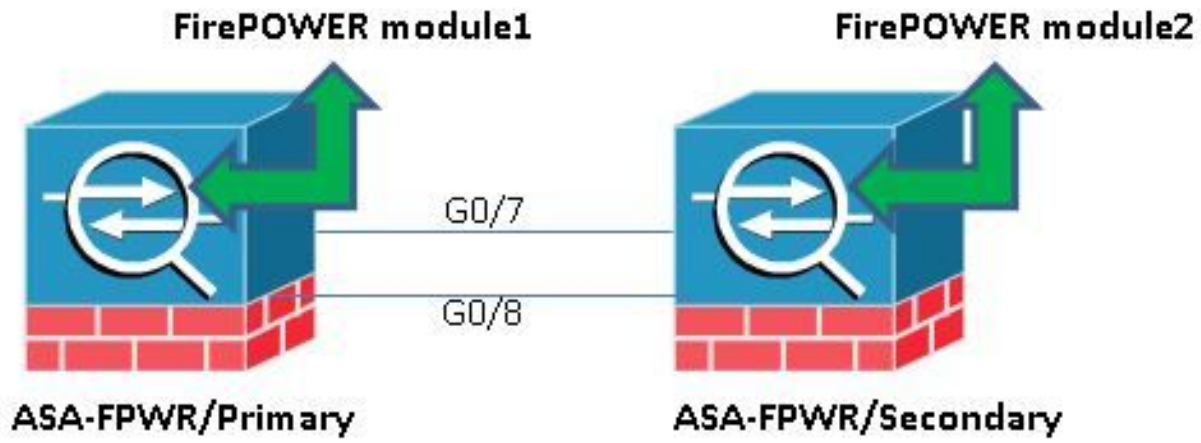
Puede ser útil inhabilitar este monitor cuando hay una recarga de módulo de servicio programada o fallas de módulo continuo de la misma sin querer tener un evento de failover de ASA.

> **Nota:** El ASA necesita desviar el tráfico al módulo para que el proceso de failover lo supervise.

Configurar

Diagrama de la red

Este documento utiliza esta configuración:



Configuraciones

Esta configuración se utiliza en dispositivos de laboratorio para demostrar la función de monitor mencionada en este documento. Solo se incluye la configuración relevante. Se omiten algunas de las líneas de este resultado.

```
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
```

Verifique los componentes supervisados actuales.

Cuando los ASA están en modo de failover, el módulo de servicio instalado se monitorea de forma predeterminada, tal como las interfaces del dispositivo. Este comando se puede utilizar para ver qué componentes actuales se monitorean:

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

Verifique el estado del módulo de servicio de las unidades ASA.

La salida **show failover** muestra el estado actual de cada módulo de 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 el módulo de servicio de una unidad activa se desactiva, se produce un evento de failover. La unidad activa pasa a estar en espera y la unidad en espera anterior asume la función activa. En algunos escenarios, esto hace que algunas funciones que no son soportadas por una conmutación por fallas stateful vuelvan a converger.

Verifique la política de modo de falla del módulo de servicio:

Si se utiliza una política de fallo-apertura para enviar tráfico al módulo, el tráfico continúa pasando a través del ASA sin ser enviado al módulo de servicio. Esta puede ser una manera más transparente de superar el estado de inactividad esperado del módulo.

> **Advertencia:** Si se ha aplicado una política de cierre por error, el ASA descarta todo el tráfico que coincida con el mapa de clase utilizado para desviar el tráfico al módulo.

Para conocer el estado de la política utilizada, ejecute el comando **show service-policy [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
```

Se puede ver lo mismo si se comprueba la configuración de la estructura de políticas modulares (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#
```

Desactive la supervisión del módulo de servicio.

Este comando, hace que el proceso de failover detenga el monitoreo del módulo de servicio. Cualquier recarga planificada o resolución de problemas se puede realizar en el módulo sin un failover, en el caso de que el módulo pase a "Abajo" o "Sin respuesta".

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

Verificación

Verifique que la supervisión del módulo de servicio esté inhabilitada.

En la configuración en ejecución, se rechaza el comando monitor-interface.

```
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 del módulo alojado por la unidad activa.

A efectos de demostración, el módulo FirePOWER de esta unidad se recarga para confirmar si la unidad de recuperación ante fallos activa permanece en esta función.

Salida del módulo FirePOWER en la unidad principal/activa de ASA.

```
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 de la unidad principal/activa de ASA mientras el módulo se recarga.

La unidad permanece en el 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 de la unidad secundaria/en espera ASA mientras el módulo se recarga:

La unidad standby no detecta este estado como una falla y no asume el 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
```

Habilite la supervisión del módulo de servicio.

Para habilitar la supervisión del módulo, ejecute este comando:

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

Verifique que el módulo de servicio esté habilitado.

El comando Service Module ya no se rechaza.

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

Troubleshoot

Problema 1. Los ASA siguen fallando y se muestra este mensaje "La tarjeta de servicio en otra unidad ha fallado".

Si se detecta uno o varios eventos de failover, el **show failover history** se puede utilizar para conocer la posible razón.

```
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 standby now muestra este mensaje:

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

Si se ve el mensaje "La tarjeta de servicio en otra unidad ha fallado", la conmutación por fallas ocurrió porque la unidad activa detectó que su propio módulo no responde.

Si el módulo permanece en el estado "Sin respuesta", 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 se puede inhabilitar mientras se pueden realizar pasos adicionales para resolver el problema para recuperar el módulo.

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

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

La serie ASA5500 antigua no admite la versión 9.3(1) y, aunque no admita módulos de software,

algunos de ellos tienen módulos de hardware como CSC o IPS.

Incluso con la nueva serie ASA5500-X, hay algunos dispositivos con versiones inferiores a la que admite la supervisión desactivada.

Solución

El ASA sólo monitorea el módulo si hay una política configurada para pasarle tráfico.Por lo tanto, para evitar una conmutación por fallas, la política del módulo puede ser eliminada.

Identifique el mapa de clase y la política utilizada.

En este caso, esta configuración se utiliza para eliminar el desvío de tráfico de un módulo FirePOWER.

```
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
!
```

El comando **show service-policy [csc|cxsc|ips|sfr]** se puede utilizar para detectar el mapa de clase y el estado actual.

```
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
```

Desactive la redirección del tráfico al módulo.

Después de que se elimine la política, no se envía más 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 la redirección ASA al módulo esté inhabilitada.

El mismo comando show se puede utilizar para verificar que el tráfico ya no vaya al módulo. El resultado debe estar vacío.

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

Incluso si el módulo no responde, la unidad activa permanece en la misma función.

```
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
```

Habilite la redirección de tráfico al módulo.

Una vez que el tráfico debe ser enviado de vuelta al módulo, se puede agregar la política de fallo-apertura o cierre de falla.

```
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#
```