# Surveillance de module de service de débronchement sur l'ASA pour éviter les événements non désirés de Basculement (SFR/CX/IPS/CSC).

## Contenu


Introduction
Conditions requises
Composants utilisés
**Informations générales**
Configurez
Diagramme du réseau
Configurations
Vérifiez les composants surveillés par courant.
Vérifiez l'état de module de service d'unités ASA.
Vérifiez la stratégie de mode d'échouer de module de service :
Surveillance de module de service de débronchement.
Vérifiez
Vérifiez que la surveillance de module de service est désactivée.
Pour tester la recharge le module hébergé par l'unité d'active.
Surveillance de module de service d'enable.
Vérifiez que le module de service est activé.
Dépannez
La question 1. ASA continuent à basculer, et ce message « carte de service dans l'autre unité a manqué » est affiché.
Solution
Issue 2. Mon ASA ne prend en charge pas 9.3(1) ou je ne peux pas l'améliorer. Comment est-ce que je peux éviter des événements de Basculement ?
Solution
Identifiez le class map et la stratégie utilisés.
Redirection du trafic de débronchement au module.
Vérifiez que la redirection ASA au module est désactivée.
Redirect to du trafic d'enable le module.


## Introduction

Ce document décrit comment désactiver la surveillance sur des modules SourceFire (SFR), le contexte averti (la CX), le Système de prévention d'intrusion (IPS), la sécurité du contenu et le contrôle (CSC) sur un environnement de Basculement de l'appliance de sécurité adaptable (ASA).


Contribué par Cesar Lopez, ingénieur TAC Cisco.

### Conditions préalables

### Conditions requises

Cisco recommande que vous ayez la connaissance des thèmes suivants :

- Configuration d'appliance de sécurité adaptable.
- La connaissance du Basculement ASA pour la Haute disponibilité.

De la version 9.3(1), cette caractéristique est configurable. Avant la version mentionnée, le module sera toujours surveillé. Un contournement peut être utilisé pour des versions préalables décrites dans ce document.

### Composants utilisés

Ce document est basé sur des ces logiciel et versions de matériel :

- Version 9.3(1) et ultérieures de Cisco ASA.
- Gamme 5500-X ASA avec des services de puissance de feu, la Sécurité Contexte-avertie *ASA CX* ou le module IPS.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande

## Informations générales

Par défaut, l'ASA surveille un module de service installé. Si une panne est détectée dans le module d'unité d'active, le Basculement d'appareils est déclenché.

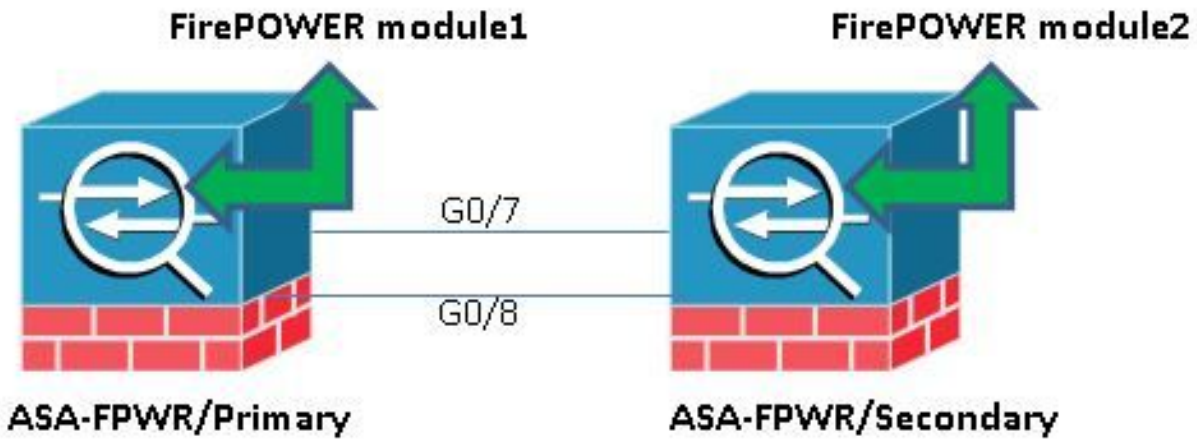
Il peut être utile de désactiver ce moniteur quand il y a une recharge de module de service programmé ou des pannes continues de module de la même chose sans vouloir avoir un événement de Basculement ASA.

> Remarque: L'ASA doit détourner le trafic au module afin de pour être surveillée par le procédé de Basculement.

## Configurez

### Diagramme du réseau

Ce document utilise cette installation :




## Configurations

Cette configuration est utilisée dans des périphériques de laboratoire pour expliquer la caractéristique de moniteur mentionnée dans ce document. Seulement la configuration appropriée est incluse. Certaines des lignes de cette sortie sont omises.

```
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
```

## Vérifiez les composants surveillés par courant.

Quand les ASA sont en mode de Basculement, le module de service installé est surveillé par défaut, juste comme l'appliance relie. Cette commande peut être utilisée, afin de voir quels composants en cours sont surveillés :

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

## Vérifiez l'état de module de service d'unités ASA.

La sortie de **Basculement d'exposition** affiche l'état actuel de chaque module d'unité :

```
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 le module de service d'une unité d'active descend, un événement de Basculement se produit. L'unité d'active devient de réserve, et l'équipement de réserve précédent joue le rôle actif. Dans quelques scénarios, ceci fait pour reconverge quelques caractéristiques qui ne sont pas prises en charge par un basculement dynamique.

## Vérifiez la stratégie de mode d'échouer de module de service :

Si un échec-openpolicy est utilisé pour envoyer le trafic au module, trafiquez continue d'aller par l'ASA sans être envoyé au module de service. Ceci peut être une manière plus transparente de surmonter un état inactif prévu de module.

> **Avertissement** : Si une stratégie d'échec-fin a été appliquée, alors, toute trafique appariant le class-map utilisé pour détourner le trafic au module est relâchée par l'ASA.

Afin de connaître l'état de stratégie utilisé, menez le **show service-policy de** commande **[sfr|la 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
```

Les mêmes peuvent être vus en vérifiant la configuration modulaire du cadre de stratégie (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#
```

### Surveillance de module de service de débronchement.

Cette commande, fait au process stop de Basculement la surveillance du module de service. N'importe quelle recharge prévue ou dépannent peut être faite au module sans Basculement, en cas de module allant « vers le bas » ou « insensible ».

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

## Vérifiez

### Vérifiez que la surveillance de module de service est désactivée.

Sous la configuration en cours, la commande d'interface de surveillance est réalisée une inversion.

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

### Pour tester la recharge le module hébergé par l'unité d'active.

Pour la démonstration, le module de puissance de feu sur cette unité est rechargé pour confirmer si l'unité active de Basculement reste sur ce rôle.

Sortie du module de puissance de feu dans unité primaire/d'active 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.
```

Sortie à partir d'unité primaire/d'active ASA tandis que les recharges de module.

L'unité reste sur le rôle actif.

```
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
```

Sortie à partir d'équipement de réserve secondaire/ASA tandis que le module recharge :

L'équipement de réserve ne détecte pas cet état comme panne et le doen't jouent le rôle actif.

```
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
```

## Surveillance de module de service d'enable.

Pour activer la surveillance de module, exécutez cette commande :

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

## Vérifiez que le module de service est activé.

La commande de module de service n'est plus réalisée une inversion.

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

# Dépannez

## La question 1. ASA continuent à basculer, et ce message « carte de service dans l'autre unité a manqué » est affiché.

Si un ou beaucoup d'événements de Basculement sont détectés, l'**historique de Basculement d'exposition** peut être utilisé pour connaître le possible raison.

```
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
```

L'équipement de réserve de now affiche ce message :

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

Si la « carte de service dans l'autre unité a manqué » le message est vu, le Basculement s'est produit parce que l'unité d'active a détecté son propre module comme insensible.

Si le module reste dans l'état « insensible », l'ASA affectée reste en mode **défectueux**.

```
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
```

## Solution

La surveillance de module de service peut être désactivée tandis que d'autres étapes pour dépanner la question peuvent être faites afin de récupérer le module.

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

## Issue 2. Mon ASA ne prend en charge pas 9.3(1) ou je ne peux pas l'améliorer. Comment est-ce que je peux éviter des événements de Basculement ?

La gamme ASA5500 existante ne prend en charge pas 9.3(1) la version et, même si elles ne prennent en charge pas des modules logiciels, certains d'entre eux ont des modules de matériel tels que CSC ou l'IPS.

Même avec la nouvelle gamme ASA5500-X, il y a quelques appliances avec des versions au-dessous de celle qui prennent en charge la surveillance de débronchement.

## Solution

L'ASA surveille seulement le module s'il y a une stratégie configurée pour lui passer le trafic. Ainsi, afin d'éviter un Basculement, la stratégie de module peut être enlevée.

### Identifiez le class map et la stratégie utilisés.

Dans ce cas, cette configuration est utilisée pour retirer le transfert du trafic d'un module de puissance de feu.

```
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
!
```

Le show service-policy de commande [csc|cxsc|IPS|le sfr] peut être utilisé pour détecter le class map et l'état actuel.

```
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
```

### Redirection du trafic de débronchement au module.

Après que la stratégie soit enlevée, aucun trafic supplémentaire n'est envoyé de l'ASA au module.

```
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#
```

### Vérifiez que la redirection ASA au module est désactivée.

La même commande show peut être utilisée pour vérifier que le trafic ne va plus au module. La sortie doit être vide.

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

Même si le module est insensible, l'unité d'active demeure dans le même rôle.

```
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
```

## Redirect to du trafic d'enable le module.

Une fois le trafic doit être renvoyé au module, l'échec-ouvert ou la stratégie d'échec-fin peut être ajoutée de retour.

```
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#
```