Désactivez la surveillance du module de service sur ASA pour éviter les événements de basculement indésirables (SFR/CX/IPS/CSC).

Table des matières

- Introduction
  - Exigences
  - Composants utilisés
- Informations générales
- Configurer
  - Diagramme du réseau
  - Configurations
  - Vérifiez les composants actuellement surveillés.
  - Vérifiez l'état du module de service des unités ASA.
  - Vérifiez la stratégie de mode d'échec du module de service :
  - Désactivez la surveillance du module de service.
- Vérifier
  - Vérifiez que la surveillance du module de service est désactivée.
  - Pour tester le rechargement du module hébergé par l'unité active.
  - Activez la surveillance du module de service.
  - Vérifiez que le module de service est activé.
- Dépannage
  - Problème 1. Les ASA continuent de basculer et le message « La carte de service d'une autre unité est en panne » s'affiche.
  - Solution
  - Problème 2. Mon ASA ne prend pas en charge 9.3(1) ou je ne peux pas le mettre à niveau. Comment éviter les événements de basculement ?
  - Solution
    - Identifiez la carte de classe et la politique utilisées.
    - Désactivez la redirection du trafic vers le module.
    - Vérifiez que la redirection ASA vers le module est désactivée.
    - Activez la redirection du trafic vers le module.

Introduction

Ce document décrit comment désactiver la surveillance sur les modules SourceFire (SFR), Context Aware (CX), Intrusion Prevention System (IPS), Content Security and Control (CSC) sur un environnement de basculement Adaptive Security Appliance (ASA).

Contribution de Cesar Lopez, ingénieur du centre d'assistance technique Cisco.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de l'appliance de sécurité adaptative.
- Connaissance du basculement ASA pour la haute disponibilité.

À partir de la version 9.3(1), cette fonctionnalité est configurable. Avant la version mentionnée, le module doit toujours être surveillé. Une solution de contournement peut être utilisée pour les versions précédentes décrites dans ce document.

Composants utilisés

Ce document est basé sur les versions logicielles et matérielles suivantes :

- Versions 9.3(1) et ultérieure de Cisco ASA.
- Gamme ASA 5500-X avec les services FirePOWER, ASA CX Context-Aware Security ou module 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 votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Par défaut, l'ASA surveille un module de service installé. Si une défaillance est détectée dans le module de l'unité active, le basculement de l'appliance est déclenché.

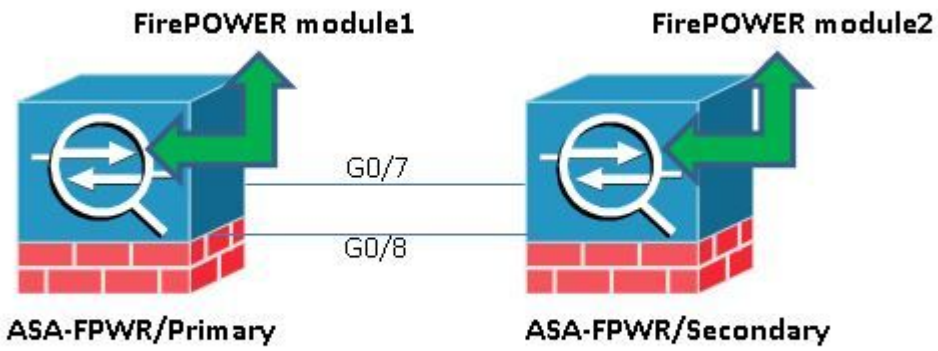
Il peut être utile de désactiver ce moniteur lorsqu'il y a un rechargement de module de service planifié ou des défaillances continues de module de même sans vouloir avoir un événement de basculement ASA.

Remarque : L'ASA doit dévier le trafic vers le module afin d'être surveillé par le processus de basculement.

Configurer

Diagramme du réseau

Ce document utilise cette configuration :



Configurations

Cette configuration est utilisée sur les périphériques des travaux pratiques pour illustrer la fonction de surveillance mentionnée dans ce document. Seule la configuration appropriée est incluse. Certaines 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 actuellement surveillés.

Lorsque les ASA sont en mode de basculement, le module de service installé est surveillé par défaut, tout comme les interfaces de l'appliance. Cette commande peut être utilisée, afin de voir quels composants actuels sont surveillés :

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

Vérifiez l'état du module de service des unités ASA.

Le résultat de la commande show failover montre l'état actuel de chaque module d'unité :

<#root>

```
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 active tombe en panne, un événement de basculement se produit. L'unité active devient en veille et l'unité en veille précédente prend le rôle actif. Dans certains scénarios, cela entraîne la reconvergence de certaines fonctionnalités qui ne sont pas prises en charge par un basculement avec état.

Vérifiez la stratégie de mode d'échec du module de service :

Si une politique d'ouverture en cas de panne est utilisée pour envoyer du trafic au module, le trafic continue à transiter par l'ASA sans être envoyé au module de service. Cela peut être un moyen plus transparent de surmonter un état de panne de module attendu.

⚠ Avertissement : Si une stratégie de fermeture en cas d'échec a été appliquée, alors tout le trafic correspondant à la carte-classe utilisée pour détourner le trafic vers le module est abandonné par l'ASA.

Afin de connaître l'état de la stratégie utilisée, exécutez la commande show service-policy [sfr|cx|ips|csc] .

<#root>

```
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
```

La même chose peut être observée en vérifiant la configuration MPF (Modular Policy Framework) :

<#root>

```
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#
```

Désactivez la surveillance du module de service.

Cette commande permet au processus de basculement d'arrêter la surveillance du module de service. Tout rechargement ou dépannage planifié peut être effectué sur le module sans basculement, en cas de module « Down » ou « Unresponsive ».

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

Vérifier

Vérifiez que la surveillance du module de service est désactivée.

Dans la configuration en cours, la commande monitor-interface est inversée.

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

Pour tester le rechargement du module hébergé par l'unité active.

À des fins de démonstration, le module FirePOWER de cette unité est rechargé pour confirmer si l'unité de basculement active conserve ce rôle.

Sortie du module FirePOWER dans l'unité ASA principale/active.

```
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 de l'unité ASA principale/active pendant le rechargement du module.

L'unité reste sur le rôle Actif.

<#root>

```
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 de l'unité secondaire/de secours ASA pendant le rechargement du module :

L'unité en veille ne détecte pas cet état comme une panne et ne joue pas le rôle actif.

<#root>

```
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

Activez la surveillance du module de service.

Pour activer la surveillance des modules, exécutez la commande suivante :

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

Vérifiez que le module de service est activé.

La commande du module de service n'est plus inversée.

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

Dépannage

Problème 1. Les ASA continuent de basculer et le message « La carte de service d'une autre unité est en panne » s'affiche.

Si un ou plusieurs événements de basculement sont détectés, la commande show failover history peut être utilisée pour connaître la raison possible.

<#root>

```
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'unité en veille affiche le message suivant :

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

Si le message « La carte de service d'une autre unité est en panne » s'affiche, le basculement s'est produit car l'unité active a détecté que son propre module ne répond pas.

Si le module reste dans l'état "Unresponse", l'ASA affecté reste dans le mode Failed.

<#root>

```
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 du module de service peut être désactivée tandis que d'autres étapes de dépannage du problème peuvent être effectuées afin de récupérer le module.

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

Problème 2. Mon ASA ne prend pas en charge 9.3(1) ou je ne peux pas le mettre à niveau. Comment éviter les événements de basculement ?

La gamme ASA5500 héritée ne prend pas en charge la version 9.3(1) et, même si elle ne prend pas en charge les modules logiciels, certains d'entre eux possèdent des modules matériels tels que CSC ou IPS.

Même avec la nouvelle gamme ASA5500-X, il existe des appliances dont les versions sont inférieures à celle qui prend en charge la désactivation de la surveillance.

Solution

L'ASA ne surveille le module que si une stratégie est configurée pour lui transmettre le trafic.Ainsi, afin d'éviter un basculement, la stratégie du module peut être supprimée.

Identifiez la carte de classe et la politique utilisées.

Dans ce cas, cette configuration est utilisée pour supprimer le détournement de trafic d'un module FirePOWER.

<#root>

```
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 commande show service-policy [csc|cxsc|ips|sfr] peut être utilisée pour détecter la carte de classe 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
```

Désactivez la redirection du trafic vers le module.

Une fois la stratégie supprimée, aucun autre trafic 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 vers le module est désactivée.

La même commande show peut être utilisée pour vérifier que le trafic n'est plus dirigé vers le module. Le résultat doit être vide.

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

Même si le module ne répond pas, l'unité active reste dans le même rôle.

<#root>

```
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
```

Activez la redirection du trafic vers le module.

Une fois que le trafic doit être renvoyé au module, la stratégie fail-open ou fail-close peut être rajoutée.

```
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#
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.