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

Contenu

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 TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître les sujets suivants :

- Configuration d'un dispositif de sécurité adaptatif.
- Connaissance du basculement ASA pour une haute disponibilité.

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

Components Used

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 services FirePOWER, module IPS ou de sécurité sensible au contexte *ASA CX*.

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. If your network is live, make sure that you understand the potential impact of any command

Informations générales

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

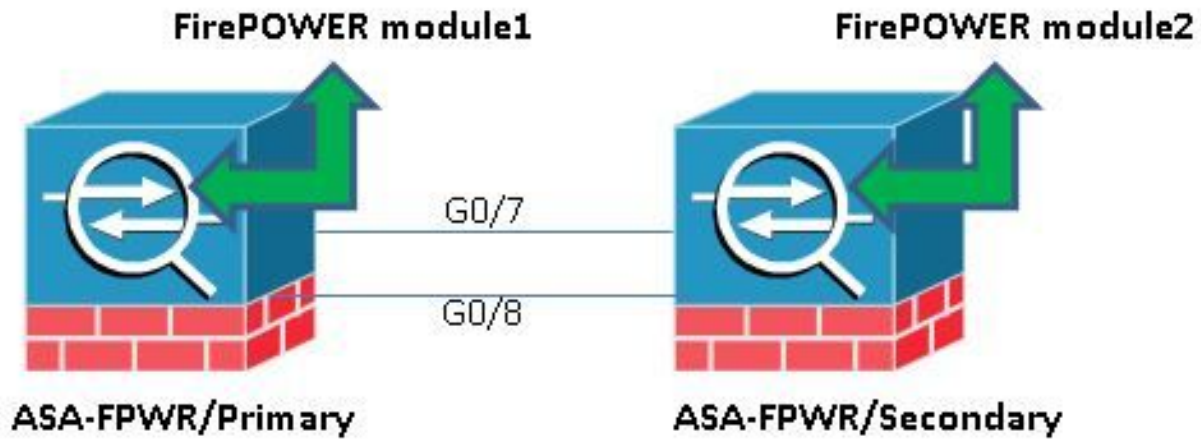
Il peut être utile de désactiver ce moniteur lorsqu'il y a un rechargement de module de service planifié ou des défaillances de module continu identiques sans avoir besoin d'un événement de basculement ASA.

> **Note**: L'ASA doit détourner le trafic vers le module afin d'être surveillé par le processus de basculement.

Configuration

Diagramme du réseau

Ce document utilise cette configuration :



Configurations

Cette configuration est utilisée dans les périphériques des travaux pratiques pour démontrer la fonctionnalité 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 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.

La sortie **show failover** indique 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 active tombe en panne, un événement de basculement se produit. L'unité active devient en veille et l'unité précédente en veille joue le rôle actif. Dans certains scénarios, cela entraîne la reconvergence de certaines fonctionnalités qui ne sont pas prises en charge par un basculement dynamique.

Vérifiez la stratégie de mode échec du module de service :

Si une stratégie d'ouverture des pannes est utilisée pour envoyer le trafic au module, le trafic continue à traverser l'ASA sans être envoyé au module de service. Il peut s'agir d'un moyen plus transparent de surmonter l'état de panne d'un module attendu.

> **Avertissement :** Si une politique de fermeture de panne a été appliquée, alors tout le trafic correspondant à la carte de classe utilisée pour détourner le trafic vers le module est abandonné par l'ASA.

Pour connaître l'état de la stratégie utilisée, exécutez la commande **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
```

Il en est de même en vérifiant la configuration MPF (Modular Policy Framework) :

```
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 panne ou de non-réponse du module.

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

Vérification

Vérifiez que la surveillance du module de service est désactivée.

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

```
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.

Àdes fins de démonstration, le module FirePOWER de cette unité est rechargé pour confirmer si l'unité de basculement actif reste sur ce rôle.

Sortie du module FirePOWER dans l'unité principale/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 de l'unité principale/active ASA pendant le rechargement du 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 de l'unité secondaire/de secours ASA pendant le rechargement du module :

L'unité de secours ne détecte pas cet état comme une défaillance et ne joue pas 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
```

Activez la surveillance du module de service.

Pour activer la surveillance des modules, exécutez cette commande :

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

Vérifiez que le module de service est activé.

La commande Service Module n'est plus annulée.

```
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 à échouer et ce message « La carte de service d'une autre unité a échoué » est affiché.

Si un ou plusieurs événements de basculement sont détectés, l'historique show failover peut être utilisé pour connaître la raison possible.

```
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 ce message :

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

Si le message « Échec de la carte de service dans une autre unité » est affiché, le basculement s'est produit parce que l'unité active a détecté que son propre module ne répond pas.

Si le module reste dans l'état Non réactif, l'ASA affecté reste en mode **Échec**.

```
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 peuvent être effectuées afin de récupérer le module.

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

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

Les anciens ASA5500 ne prennent pas en charge la version 9.3(1) et, même s'ils ne prennent pas en charge les modules logiciels, certains d'entre eux ont des modules matériels tels que CSC ou

l'IPS.

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

Solution

L'ASA surveille uniquement le module s'il existe une stratégie configurée pour lui transmettre le trafic.Ainsi, afin d'éviter un basculement, la stratégie de module peut être supprimée.

Identifiez la carte de classe et la stratégie utilisées.

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

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 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 ne répond pas, l'unité active reste 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
```

Activez la redirection du trafic vers le module.

Une fois que le trafic doit être renvoyé au module, la politique fail-open ou fail-close peut être ajoutée à nouveau.

```
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#
```