Disabilitare il monitoraggio del modulo di servizio sull'appliance ASA per evitare eventi di failover indesiderati (SFR/CX/IPS/CSC).

Sommario

Introduzione

In questo documento viene descritto come disabilitare il monitoraggio sui moduli SourceFire (SFR), Context Aware (CX), Intrusion Prevention System (IPS), Content Security and Control (CSC) in un ambiente di failover Adaptive Security Appliance (ASA).

Contributo di Cesar Lopez, Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di Adaptive Security Appliance.
- Conoscenza del failover ASA per l'alta disponibilità.

Dalla versione 9.3(1), questa funzione è configurabile. Prima della versione indicata, il modulo verrà sempre monitorato. È possibile utilizzare una soluzione alternativa per le versioni precedenti descritte in questo documento.

Componenti usati

Questo documento si basa sulle seguenti versioni software e hardware:

- Cisco ASA versione 9.3(1) e successive.
- ASA serie 5500-X con servizi FirePOWER, *ASA CX* Context-Aware Security o modulo IPS.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi

Premesse

Per impostazione predefinita, l'ASA controlla un modulo di servizio installato. Se viene rilevato un errore nel modulo di unità attivo, viene attivato il failover dell'accessorio.

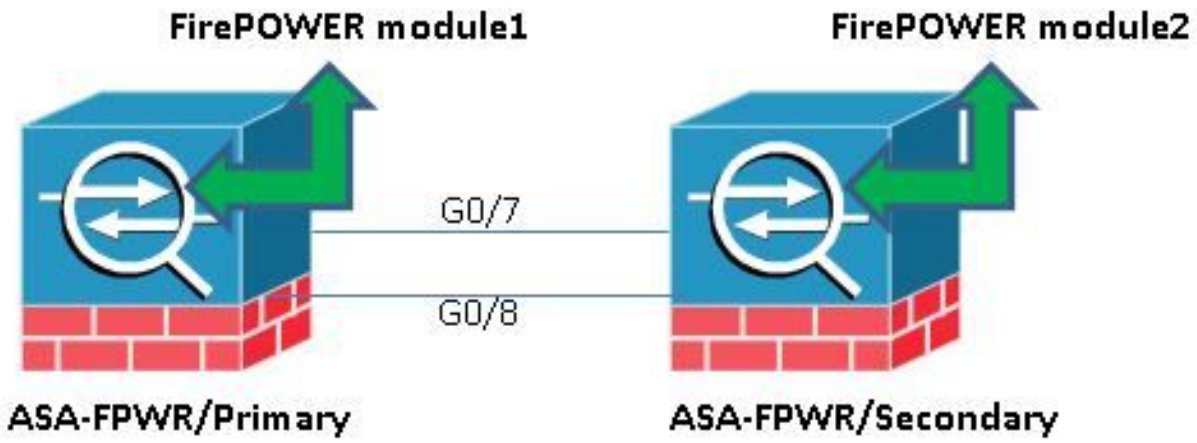
Può essere utile disabilitare questo monitoraggio in caso di ricaricamento pianificato del modulo del servizio o di errori continui del modulo senza che si desideri avere un evento di failover dell'ASA.

> **Nota:** L'ASA deve deviare il traffico al modulo per essere monitorata dal processo di failover.

Configurazione

Esempio di rete

Nel documento viene utilizzata questa impostazione:



Configurazioni

Questa configurazione viene usata nei dispositivi lab per dimostrare la funzionalità di monitoraggio descritta in questo documento. È inclusa solo la configurazione pertinente. Alcune righe di questo output sono omesse.

```
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
```

Controllare i componenti attualmente monitorati.

Quando le appliance ASA sono in modalità di failover, per impostazione predefinita viene monitorato il modulo di servizio installato, proprio come le interfacce dell'appliance. Questo comando può essere usato per verificare quali componenti sono attualmente monitorati:

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

Controllare lo stato del modulo di servizio delle unità ASA.

L'output **show failover** visualizza lo stato corrente di ciascun modulo unità:

```
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
```

Se il modulo di servizio di un'unità attiva diventa inattivo, si verifica un evento di failover. L'unità attiva diventa standby e la precedente unità in standby assume il ruolo attivo. In alcuni scenari ciò determina la riconversione di alcune funzionalità non supportate da un failover con stato.

Verificare il criterio modalità di errore del modulo di servizio:

Se si usa un fail-openpolicy per inviare il traffico al modulo, il traffico continua a passare attraverso l'ASA senza essere inviato al modulo di servizio. Questo può essere un modo più trasparente per superare uno stato di inattività previsto del modulo.

> **Avviso:** Se è stato applicato un criterio di chiusura degli errori, tutto il traffico corrispondente alla mappa di classe utilizzata per deviare il traffico al modulo viene scartato dall'ASA.

Per conoscere lo stato dei criteri utilizzato, eseguire il 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
```

Per verificare lo stesso comportamento, controllare la configurazione di Modular Policy Framework (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#
```

Disabilitare il monitoraggio del modulo di servizio.

Con questo comando il processo di failover interrompe il monitoraggio del modulo del servizio. Qualsiasi ricaricamento pianificato o risoluzione dei problemi può essere eseguito sul modulo senza failover, nel caso in cui il modulo diventi "inattivo" o "non rispondente".

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

Verifica

Verificare che il monitoraggio del modulo di servizio sia disabilitato.

Nella configurazione corrente, il comando monitor-interface viene negato.

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

Per eseguire il test del ricaricamento del modulo ospitato dall'unità attiva.

A scopo dimostrativo, il modulo FirePOWER su questa unità viene ricaricato per verificare se l'unità di failover attiva rimane su questo ruolo.

Uscita dal modulo FirePOWER nell'unità ASA principale/attiva.

```
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.
```

Uscita dall'unità ASA principale/attiva durante il ricaricamento del modulo.

L'unità rimane nel ruolo Attivo.

```
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
```

Uscita dall'unità secondaria/standby ASA mentre il modulo viene ricaricato:

L'unità di standby non rileva questo stato come guasto e non assume il ruolo attivo.

```
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
```

Abilitare il monitoraggio del modulo di servizio.

Per abilitare il monitoraggio del modulo, eseguire questo comando:

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

Verificare che il modulo di servizio sia abilitato.

Il comando del modulo di servizio non è più negato.

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

Risoluzione dei problemi

Problema 1. Le appliance ASA continuano a eseguire il failover e viene visualizzato il messaggio "Service card in other unit has fail" (La scheda di servizio di un'altra unità non funziona).

Se vengono rilevati uno o più eventi di failover, è possibile utilizzare **show failover history** per conoscere il motivo possibile.

```
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'unità Now standby visualizza questo messaggio:

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

Se viene visualizzato il messaggio "La scheda di servizio in un'altra unità non è riuscita", il failover si è verificato perché l'unità attiva ha rilevato che il proprio modulo non risponde.

Se il modulo rimane nello stato "Non risponde", l'ASA interessata rimane in modalità **Non riuscita**.

```
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
```

Soluzione

Èpossibile disabilitare il monitoraggio del modulo di servizio mentre è possibile eseguire ulteriori passaggi per risolvere il problema e ripristinare il modulo.

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

Problema 2. L'appliance ASA non supporta la versione 9.3(1) o non è possibile aggiornarla. Come evitare gli eventi di failover?

La serie ASA5500 legacy non supporta la versione 9.3(1) e, anche se non supportano i moduli software, alcuni di essi dispongono di moduli hardware come CSC o IPS.

Anche con la nuova serie ASA5500-X, ci sono alcuni accessori con versioni successive che supportano la funzione di monitoraggio disabilitato.

Soluzione

L'ASA monitora il modulo solo se è presente un criterio configurato per passare il traffico al modulo.Quindi, per evitare un failover, il criterio del modulo può essere rimosso.

Identificare la mappa delle classi e i criteri utilizzati.

In questo caso, la configurazione viene utilizzata per rimuovere la deviazione del traffico di un modulo 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
!
```

Per rilevare la mappa della classe e lo stato corrente, è possibile utilizzare il comando **show service-policy [csc|cxsc|ips|sfr]**.

```
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
```

Disabilitare il reindirizzamento del traffico al modulo.

Dopo aver rimosso la policy, non viene inviato altro traffico dall'appliance ASA al modulo.

```
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#
```

Verificare che il reindirizzamento ASA al modulo sia disabilitato.

Èpossibile usare lo stesso comando **show** per verificare che il traffico non vada più al modulo. L'output deve essere vuoto.

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

Anche se il modulo non risponde, l'unità attiva rimane nello stesso ruolo.

```
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
```

Abilitare il reindirizzamento del traffico al modulo.

Quando il traffico deve essere rimandato al modulo, è possibile aggiungere nuovamente il criterio di fail-open o di fail-close.

```
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#
```