Schakel controle van servicemodule op ASA uit om ongewenste failover-gebeurtenissen (SFR/CX/IPS/CSC) te voorkomen.

Inhoud

Inleiding

Dit document beschrijft hoe u controle op modules SourceFire (SFR), Context Aware (CX), Inbraakpreventiesysteem (IPS), Content Security and Control (CSC) op een failover-omgeving voor adaptieve security applicatie (ASA) kunt uitschakelen.

Bijgedragen door Cesar Lopez, Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt u aan om kennis te hebben van de volgende onderwerpen:

- Configuratie van adaptieve security applicatie.
- Kennis van ASA Failover voor hoge beschikbaarheid.

Vanaf versie 9.3(1), is deze optie configureerbaar. Vóór de genoemde versie wordt de module altijd gevolgd. Een tijdelijke oplossing kan worden gebruikt voor eerdere versies die in dit document zijn beschreven.

Gebruikte componenten

Dit document is gebaseerd op deze software en hardwareversies:

- Cisco ASA versie 9.3(1) en hoger.
- ASA 5500-X Series met FirePOWER Services, *ASA CX* Context Aware Security of IPS-module.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen

Achtergrondinformatie

Standaard controleert de ASA een geïnstalleerde servicemodule. Als er een storing wordt gedetecteerd in de actieve eenheidsmodule, wordt de uitvalfunctie van het apparaat geactiveerd.

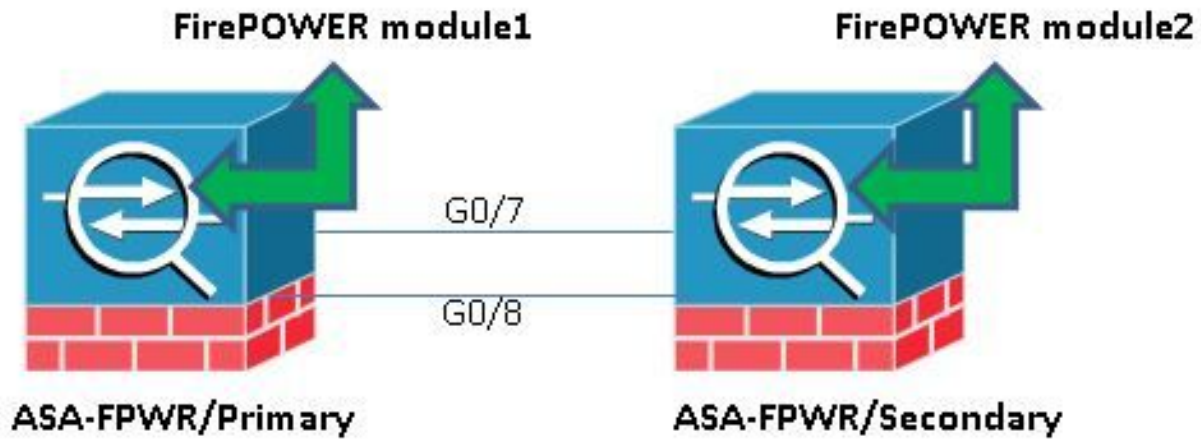
Het kan behulpzaam zijn om deze monitor uit te schakelen wanneer er een geplande herlading van de servicemodule of ononderbroken modulefouten van het zelfde is zonder bereid om een ASA failover-gebeurtenis te hebben.

> Opmerking: De ASA moet verkeer naar de module omleiden om te worden gecontroleerd door het overnameverkeer.

Configureren

Netwerkdiagram

Dit document gebruikt deze instellingen:



Configuraties

Deze configuratie wordt in labapparatuur gebruikt om de in dit document vermelde monitor-functie aan te tonen. Alleen de configuratie in kwestie is opgenomen. Sommige regels van deze output worden weggelaten.

```
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
```

Controleer de huidige gecontroleerde onderdelen.

Wanneer de ASA's in de failover-modus staan, wordt de geïnstalleerde servicemodule standaard gecontroleerd, net zoals de interfaces van het apparaat. Deze opdracht kan worden gebruikt om te zien welke huidige onderdelen worden gemonitord:

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

Controleer de status van de ASA-eenheden-servicemodule.

De **I**-uitvoer toont de huidige status van elke eenheid module:

```
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
```

Als de servicemodule van een actieve eenheid naar beneden gaat, vindt er een failover-gebeurtenis plaats. De actieve eenheid wordt standby en de vorige standby-eenheid speelt een actieve rol. In sommige scenario's, veroorzaakt dit sommige eigenschappen die niet door een stateful failover worden gesteund, om opnieuw samen te vallen.

Controleer het beleid voor de servicemodule faalt:

Als een failliet-openingsbeleid wordt gebruikt om verkeer naar de module te verzenden, blijft het verkeer door de ASA gaan zonder naar de servicemodule te worden verzonden. Dit kan een transparantere manier zijn om een verwachte onderdrukkingsstatus van een module te boven te komen.

> **Waarschuwing**: Als een failliet beleid is toegepast, dan wordt al verkeer dat de class-map aansluit die wordt gebruikt om verkeer om te leiden naar de module, door ASA laten vallen.

Om de gebruikte beleidsstatus te kennen, voert u het **dienstverleningsbeleid** van de opdrachtshow uit **[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
```

Hetzelfde kan worden gezien door de configuratie van het modulaire beleidskader (MPF) te controleren:

```
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#
```

Controle van servicemodule uitschakelen.

Deze opdracht, maakt het overboekingsproces stop de controle van de servicemodule. Enige geplande herlading of probleemoplossing kan aan de module zonder een failover worden gedaan, in het geval dat de module "Down" of "Unresponsief" gaat.

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

Verifiëren

Controleer of de controle van de servicemodule uitgeschakeld is.

Onder de actieve configuratie, wordt de monitor-interface opdracht genegeerd.

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

Om de module te testen die door de actieve eenheid wordt gehost.

Voor demonstratiedoeleinden wordt de module FirePOWER op deze eenheid opnieuw geladen om te bevestigen of de actieve failliet-eenheid op deze rol blijft staan.

Uitvoer van de FirePOWER-module in ASA Primaire/Actieve eenheid.

```
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.
```

Uitvoer van de ASA Primaire/Actieve eenheid tijdens het herladen van de module.

De eenheid blijft actief.

```
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
```

Uitvoer van de ASA Secundaire/Standby unit terwijl de module opnieuw wordt geladen:

De stand-by unit herkent deze status niet als een mislukking en neemt de actieve rol niet op.

```
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
```

Controle van servicemodule inschakelen.

Laat deze opdracht uitvoeren om module controle in te schakelen:

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

Controleer of de servicemodule is ingeschakeld.

De opdracht voor de servicemodule is niet meer verwaarloosd.

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

Problemen oplossen

Onderdeel 1. ASA's blijven failliet gaan en dit bericht "De servicekaart in andere eenheid is mislukt" wordt weergegeven.

Als een of veel failover gebeurtenissen worden gedetecteerd, kan de show failover geschiedenis worden gebruikt om de mogelijke reden te kennen.

```
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
```

De nu stand-by unit toont dit bericht:

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

Als het bericht "Service card in andere unit heeft gefaald" wordt gezien, is de failover opgetreden omdat de actieve eenheid zijn eigen module heeft gedetecteerd als niet-responsief.

Als de module in "Onresponsieve" status blijft, blijft de getroffen ASA in **mislukte** modus.

```
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
```

Oplossing

De controle van de servicemodule kan worden uitgeschakeld terwijl verdere stappen om de kwestie op te lossen kunnen worden gedaan om de module te herstellen.

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

Vraag 2. Mijn ASA ondersteunt 9.3(1) niet of ik kan het niet upgraden. Hoe kan ik overloopgebeurtenissen voorkomen?

Verouderde ASA 5500 Series ondersteunen geen versie van 9.3(1) en, zelfs als deze geen

softwaremodules ondersteunen, hebben sommigen hardwaremodules zoals CSC of IPS.

Zelfs met de nieuwe ASA 5500-X serie zijn er sommige apparaten met versies onder de serie die schakelt om controle uit te schakelen.

Oplossing

De ASA monitort alleen de module als er een beleid is ingesteld om verkeer door te geven. Dus, om een failover te voorkomen, kan het modulebeleid worden verwijderd.

Identificeer de klassenkaart en het gebruikte beleid.

In dit geval, wordt deze configuratie gebruikt om verkeersversie van een FirePOWER-module te verwijderen.

```
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
!
```

De opdracht **toont een servicepakket [csc|cxsc|ips|sfr]** kan worden gebruikt om de klassenkaart en de huidige status te detecteren.

```
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
```

Verkeersrichting naar de module uitschakelen.

Nadat het beleid is verwijderd, wordt er geen verder verkeer meer verzonden van de ASA naar de 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#
```

Controleer of de ASA-omleiding naar de module uitgeschakeld is.

Dezelfde **show** opdracht kan worden gebruikt om te controleren of het verkeer niet langer naar de module gaat. De uitvoer moet leeg zijn.

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

Zelfs als de module niet reageert blijft de actieve eenheid dezelfde rol spelen.

```
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
```

Schakel verkeer terug naar de module in.

Zodra het verkeer naar de module moet worden teruggestuurd, kan het failopen of faaldicht beleid worden toegevoegd.

```
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#
```