원치 않는 장애 조치 이벤트(SFR/CX/IPS/CSC)를 방지하려면 ASA에서 서비스 모듈 모니터링을 비활성화합니다.

목차

소개

이 문서에서는 ASA(Adaptive Security Appliance) 장애 조치 환경에서 모듈 SourceFire(SFR), CX(Context Aware), IPS(Intrusion Prevention System), CSC(Content Security and Control)에 대한 모니터링을 비활성화하는 방법에 대해 설명합니다.

기고자: Cesar Lopez, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

Cisco에서는 다음 주제에 대해 알고 있는 것이 좋습니다.

- Adaptive Security Appliance의 컨피그레이션입니다.
- 고가용성을 위한 ASA 장애 조치에 대한 지식.

버전 9.3(1)에서 이 기능을 구성할 수 있습니다.언급된 버전 이전에 모듈은 항상 모니터링됩니다.이 문서에 설명된 이전 버전에 대한 해결 방법을 사용할 수 있습니다.

사용되는 구성 요소

이 문서는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASA 버전 9.3(1) 이상
- ASA 5500-X Series with FirePOWER Services, *ASA CX* Context-Aware Security 또는 IPS 모듈

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다

배경 정보

기본적으로 ASA는 설치된 서비스 모듈을 모니터링합니다.액티브 유닛 모듈에서 장애가 감지되면 어플라이언스 장애 조치가 트리거됩니다.

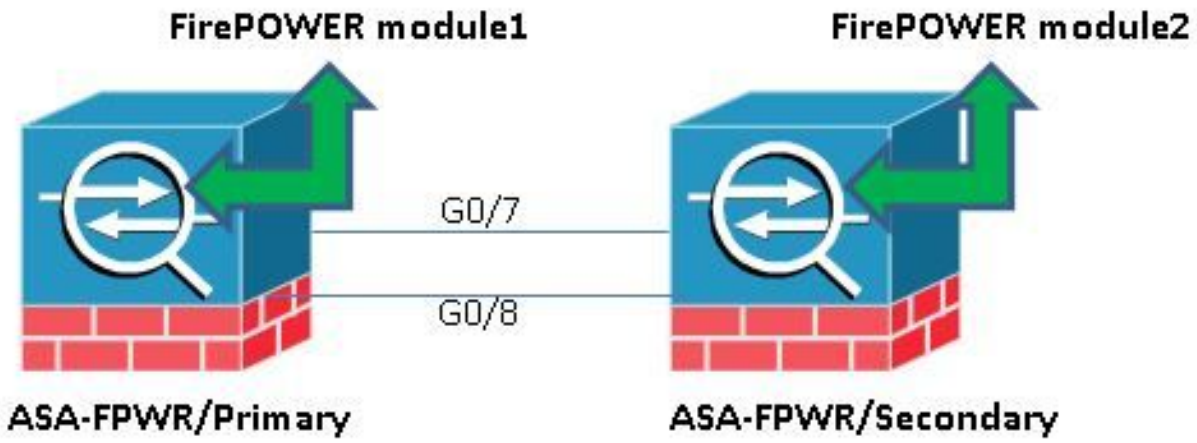
예약된 서비스 모듈이 다시 로드되거나 ASA 장애 조치 이벤트를 원하지 않고 동일한 모듈에 연속 모듈 장애가 발생하는 경우 이 모니터를 비활성화하는 것이 도움이 될 수 있습니다.

> **참고:**장애 조치 프로세스에서 모니터링하려면 ASA에서 모듈로 트래픽을 전환해야 합니다.

구성

네트워크 다이어그램

이 문서에서는 다음 설정을 사용합니다.



구성

이 컨피그레이션은 랩 디바이스에서 이 문서에 언급된 모니터 기능을 시연하는 데 사용됩니다.관련 컨피그레이션만 포함됩니다.이 출력의 일부 행은 생략됩니다.

```
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
```

현재 모니터링되는 구성 요소를 확인합니다.

ASA가 장애 조치 모드에 있을 때 설치된 서비스 모듈은 어플라이언스 인터페이스와 마찬가지로 기본적으로 모니터링됩니다.이 명령을 사용하여 모니터링할 현재 구성 요소를 확인할 수 있습니다.

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

ASA 장치 서비스 모듈 상태를 확인합니다.

show failover 출력에는 각 유닛 모듈의 현재 상태가 표시됩니다.

```
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
```

액티브 유닛의 서비스 모듈이 다운되면 장애 조치 이벤트가 발생합니다.액티브 유닛이 스탠바이 유닛이 되고 이전 스탠바이 유닛이 액티브 역할을 수행합니다.일부 시나리오에서는 상태 기반 장애 조치에서 지원하지 않는 일부 기능이 다시 통합됩니다.

서비스 모듈 실패 모드 정책을 확인합니다.

fail-openpolicy를 사용하여 모듈로 트래픽을 전송하는 경우 트래픽은 서비스 모듈로 전송되지 않고 ASA를 계속 통과합니다.이는 예상되는 모듈 다운 상태를 극복하기 위한 더 투명한 방법이 될 수 있습니다.

> **경고:**fail-close 정책이 적용된 경우, 트래픽을 모듈로 전환하는 데 사용되는 클래스 맵과 일치하는 모든 트래픽은 ASA에 의해 삭제됩니다.

사용된 정책 상태를 확인하려면 show service-policy **[sfr|cx|ips|csc] 명령을 실행합니다**.

```
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
```

MPF(Modular Policy Framework) 컨피그레이션도 확인할 수 있습니다.

```
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#
```

서비스 모듈 모니터링을 비활성화합니다.

이 명령을 사용하면 장애 조치 프로세스가 서비스 모듈의 모니터링을 중지합니다.모듈이 "작동 중지" 또는 "응답하지 않음"으로 이동하는 경우 장애 조치 없이 계획된 모든 다시 로드 또는 문제 해결을 모듈에 수행할 수 있습니다.

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

다음을 확인합니다.

서비스 모듈 모니터링이 비활성화되었는지 확인합니다.

실행 중인 컨피그레이션에서 monitor-interface 명령이 부정됩니다.

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

활성 유닛에서 호스팅하는 모듈을 다시 로드하도록 테스트하려면

데모용으로 이 유닛의 FirePOWER 모듈이 다시 로드되어 액티브 장애 조치 유닛이 이 이 역할을 계속 수행하는지 확인합니다.

ASA Primary/Active 유닛의 FirePOWER 모듈 출력

```
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.
```

모듈이 다시 로드되는 동안 ASA Primary/Active 유닛의 출력입니다.

유닛은 활성 역할에 유지됩니다.

```
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
```

모듈이 다시 로드되는 동안 ASA Secondary/Standby 유닛의 출력:

스탠바이 유닛에서는 이 상태를 오류로 감지하지 못하고 활성 역할을 수행하지 않습니다.

```
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
```

서비스 모듈 모니터링을 활성화합니다.

모듈 모니터링을 활성화하려면 다음 명령을 실행합니다.

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

서비스 모듈이 활성화되어 있는지 확인합니다.

서비스 모듈 명령이 더 이상 부정되지 않습니다.

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

문제 해결

문제점 1. ASA가 계속 장애 조치되고 "다른 유닛의 서비스 카드가 실패함"이라는 메시지가 표시됩니다.

하나 이상의 장애 조치 이벤트가 탐지되면 **show failover history**를 사용하여 가능한 원인을 알 수 있습니다.

```
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
```

이제 대기 유닛에 다음 메시지가 표시됩니다.

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

"Service card in other unit has failed(다른 유닛의 서비스 카드가 실패함)" 메시지가 표시되면 액티브 유닛이 자체 모듈을 응답하지 않는 것으로 감지했기 때문에 장애 조치가 발생했습니다.

모듈이 "Unresponsive(응답 없음)" 상태로 유지되면 영향을 받는 ASA가 **Failed(실패)** 모드**로** 유지됩니다.

```
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
```

솔루션

서비스 모듈 모니터링을 비활성화할 수 있으며, 모듈을 복구하기 위해 문제를 해결하기 위한 추가 단계를 수행할 수 있습니다.

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

2번. ASA에서 9.3(1)을 지원하지 않거나 업그레이드할 수 없습니다.장애 조치 이벤트를 방지하려면 어떻게 해야 합니까?

레거시 ASA5500 Series는 9.3(1) 버전을 지원하지 않으며, 소프트웨어 모듈을 지원하지 않더라도 일부 ASA에는 CSC 또는 IPS와 같은 하드웨어 모듈이 있습니다.

새로운 ASA5500-X 시리즈에서도 모니터링 비활성화를 지원하는 버전 이하의 일부 어플라이언스가 있습니다.

솔루션

ASA는 트래픽을 전달하도록 구성된 정책이 있는 경우에만 모듈을 모니터링합니다. 따라서 장애 조치를 방지하기 위해 모듈 정책을 제거할 수 있습니다.

사용된 클래스 맵 및 정책을 식별합니다.

이 경우 이 컨피그레이션은 FirePOWER 모듈의 트래픽 우회를 제거하는 데 사용됩니다.

```
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
!
```

show service-policy [csc|cxsc|ips|sfr] 명령을 사용하여 클래스 맵 및 현재 상태를 검색할 수 있습니다.

```
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
```

모듈에 대한 트래픽 리디렉션을 비활성화합니다.

정책이 제거된 후에는 ASA에서 모듈로 더 이상 트래픽이 전송되지 않습니다.

```
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#
```

모듈에 대한 ASA 리디렉션이 비활성화되었는지 확인합니다.

동일한 **show** 명령을 사용하여 트래픽이 더 이상 모듈로 이동하지 않는지 확인할 수 있습니다.출력은 비어 있어야 합니다.

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

모듈이 응답하지 않더라도 활성 유닛은 동일한 역할을 유지합니다.

```
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
```

모듈에 대한 트래픽 리디렉션을 활성화합니다.

트래픽을 다시 모듈로 전송해야 할 경우, fail-open 또는 fail-close 정책을 다시 추가할 수 있습니다.

```
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#
```