

# 不必要なフェールオーバー イベント ( SFR/CX/IPS/CSC ) を避ける ASA のディセーブル サービスモジュール モニタリング。

## 目次

[概要](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[電流によって監視されるコンポーネントをチェックして下さい。](#)

[ASA ユニット サービスモジュール ステータスをチェックして下さい。](#)

[サービスモジュール失敗モード ポリシーを確認して下さい。](#)

[サービスモジュール モニタリングをディセーブルにして下さい。](#)

[確認](#)

[サービスモジュール モニタリングが無効であることを確認して下さい。](#)

[リロードをテストするためアクティブユニット ホストされるモジュール。](#)

[イネーブル サービスモジュール モニタリング。](#)

[サービスモジュールが有効になることを確認して下さい。](#)

[トラブルシューティング](#)

[問題 1. ASA は失敗し続けこのメッセージ「他のユニットのサービスカード」は示されています 失敗しました。](#)

[解決策](#)

[問題 2。 ASA は 9.3\(1\) をサポートしませんまたはそれをアップグレードできません。 どのようにフェールオーバー イベントを避けることができますか。](#)

[解決策](#)

[使用されるクラスマップおよびポリシーを識別して下さい。](#)

[モジュールにトラフィック リダイレクションをディセーブルにして下さい。](#)

[モジュールへの ASA リダイレクションが無効であることを確認して下さい。](#)

[モジュールにトラフィック リダイレクトを有効にして下さい。](#)

## 概要

この資料にわかっているモジュール SourceFire ( SFR ) のモニタリング、コンテキスト ( CX )、適応性があるセキュリティ アプライアンス モデル ( ASA ) フェールオーバー 環境の侵入防御システム ( IPS )、コンテンツ セキュリティおよびコントロール ( CSC ) をディセーブルにする方法を記述されています。

Cesar ローペッツによって貢献される、Cisco TAC エンジニア。

## 前提条件

### 要件

Cisco は次のトピックのナレッジがあることを推奨します:

- 適応性があるセキュリティ アプライアンス モデルの設定。
- [ハイアベイラビリティのための ASA フェールオーバー](#)のナレッジ。

バージョン 9.3(1)から、この機能は設定可能です。述べられたバージョンの前に、モジュールは常に監視されます。回避策はこの資料に説明がある前のバージョンに使用することができます。

### 使用するコンポーネント

この資料はこれらのソフトウェア および ハードウェア バージョンに基づいています:

- Cisco ASA バージョン 9.3(1) および それ 以降。
- FirePOWER サービス、ASA CX コンテキストわかっているセキュリティまたは IPS モジュールとの ASA 5500-X シリーズ。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークがライブである場合、あらゆるコマンドの潜在的影響を理解することをお勧めします。

## 背景説明

デフォルトで、ASA はインストール済みサービスモジュールを監察します。失敗がアクティブユニット モジュールで検出する場合、アプライアンス フェールオーバーは引き起こされます。

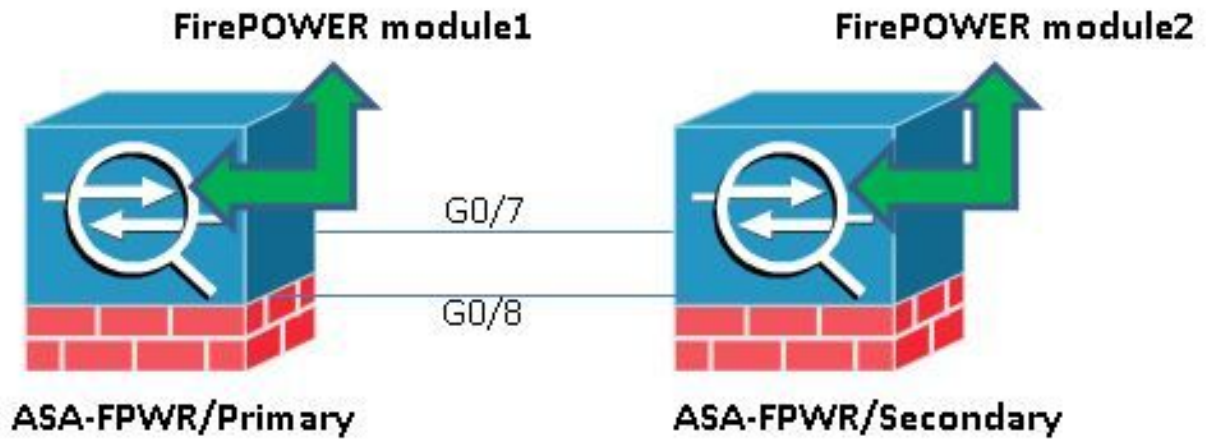
同じのスケジュールされたサービスモジュール リロードまたは連続的なモジュール障害が ASA フェールオーバー イベントを持つことを決定しないときこのモニタをディセーブルにすることは有用である場合もあります。

注: ASA はモジュールにトラフィックをフェールオーバー プロセスによって監察されるために転換する必要があります。

## 設定

### ネットワーク図

この資料はこのセットアップを使用します:



## 設定

ラボ デバイスでこの設定がこの資料で述べられるモニタ機能を示すのに使用されています。関係のある構成だけ含まれています。いくつかのこの出力行は省略されます。

```
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
```

**電流によって監視されるコンポーネントをチェックして下さい。**

ASA がフェールオーバー モードにあるとき、インストールされるサービスモジュールはアプライアンスとして、ちょうどインターフェイスしますデフォルトで監視されます。このコマンドはどの現在のコンポーネントが監視されるか見るために使用することができます:

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

**ASA ユニット サービスモジュール ステータスをチェックして下さい。**

**show failover** 出力は各ユニット モジュールの現在のステータスを表示したものです:

```
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
```

アクティブユニットのサービスモジュールがダウン状態になる場合、フェールオーバー イベントは発生します。アクティブユニットはスタンバイになり、前のスタンバイユニットはアクティブな役割を果たします。あるシナリオでは、これにより再収束しますステートフル フェールオーバーによってサポートされないいくつかの機能は。

## サービスモジュール失敗モード ポリシーを確認して下さい:

モジュールにトラフィックを送信 すればのに故障する openpolicy が使用されている場合トラフィックはサービスモジュールへ送信 されないで ASA を通過し続けます。これは期待されたモジュール ダウン ステータスを克服するより透過的な方法である場合もあります。

**警告：** 故障する終わりポリシーが、転換すればのに使用される class-map と一致するすべてのトラフィック適用されたらモジュールへのトラフィックは ASA によって廃棄されます。

使用されるポリシー ステータスを知るためにコマンド **show service ポリシー[sfr** を実行して下さい|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
```

同じモジュラ 政策の枠組 ( MPF ) 設定のチェックによって見られる場合があります:

```
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#
```

## ディセーブル サービスモジュール モニタリング。

このコマンドはサービスモジュールの、フェールオーバー プロセス停止にモニタリングをします。どの計画されたリロードでも「」ダウン状態になるモジュールの場合にはフェールオーバーなしでモジュールにまたは、することができませんまたは「無理解」解決します。

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

## 確認

### サービスモジュール モニタリングが無効であることを確認して下さい。

実行コンフィギュレーションの下で、モニタ インターフェイス コマンドは否定されます。

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

### リロードをテストするためアクティブユニット ホストされるモジュール。

デモンストレーション目的で、このユニットの FirePOWER モジュールはアクティブなフェールオーバー ユニットがこのロールにとどまるかどうか確認するためにリロードされます。

ASA プライマリ/アクティブユニットの FirePOWER モジュールからの出力。

```
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.
```

ASA プライマリ/アクティブユニットからの出力間モジュール読み込み。

ユニットはアクティブな役割にとどまります。

```
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
```

モジュールがリロードする間、ASA セカンダリ/スタンバイユニットからの出力:

スタンバイユニットは失敗および doesn't がアクティブな役割を果たすと同時にこのステータスを検出する。

```
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
```

## イネーブル サービスモジュール モニタリング。

モジュール モニタリングを有効にするために、このコマンドを実行して下さい:

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

サービスモジュールが有効になることを確認して下さい。

サービスモジュール コマンドはもう否定されません。

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

## トラブルシューティング

**問題 1. ASA は失敗し続けこのメッセージ「他のユニットのサービスカード」は示されています失敗しました。**

1つのまたは多くのフェールオーバー イベントが検出する場合、**show failover 履歴**が考えられる原因を知っているのに使用することができます。

```
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
```

今スタンバイユニットはこのメッセージを表示します:

```
14:47:56 UTC Aug 6 2015
Standby Ready Failed Detect service card failure
「他のユニットのサービスカード」が失敗したらメッセージはアクティブユニットが無理解ように自身のモジュールを検出するので、フェールオーバー起こりました見られます。
```

モジュールが「無理解な」ステータスにとどまる場合、影響を受けた ASA は壊れるモードにとどまります。

```
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
```

## 解決策

サービスモジュール モニタリングは問題を解決するモジュールを回復 するためにそれ以上のステップが実行することができる間、無効である場合もあります。

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

**問題 2。ASA は 9.3(1) をサポートしませんまたはそれをアップグレードできません。どのようにフェールオーバー イベントを避けることができますか。**

レガシー ASA5500 シリーズは 9.3(1) バージョンをサポートしないし、支援 ソフトウェア モジュール、そのうちのいくつかに CSC または IPS のようなハードウェアモジュールがあります。

新しい ASA5500-X シリーズと、デisable モニタリングをサポートするもの以下バージョンのいくつかのライセンスです。

## 解決策

ASA はそれにトラフィックを通過させるために設定されるポリシーがある場合その時だけモジュールを監察します。このように、フェールオーバーを避けるために、モジュール ポリシーは取除くことができます。

使用されるクラスマップおよびポリシーを識別して下さい。

この場合、この設定が FirePOWER モジュールのトラフィック転換を取除くのに使用されていません。

```
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
!
```

コマンド **show service ポリシー**[CSC|cxsc|IPS|sfr が]クラスマップおよび現在のステータスを検出するのに使用することができます。

```
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
```

**モジュールへのディセーブルトラフィックリダイレクション。**

ポリシーが削除された後、それ以上のトラフィックは ASA からモジュールに送信されません。

```
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#
```

**モジュールへの ASA リダイレクションが無効であることを確認して下さい。**

同じ表示コマンドがトラフィックがモジュールにもはや行っていないことを確認するのに使用することができます。出力は空である必要があります。

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

**モジュールが無理解でも、アクティブユニットは同じロールに残ります。**

```
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

## モジュールへのイネーブルトラフィックリダイレクト。

トラフィックがモジュールに送返される必要があれば故障する開いたまたは故障する終わりポリシーは追加することができます。

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#