不要なフェールオーバーイベント(SFR/CX/IPS/CSC)を回避するために、ASAのサービスモジュールモニタリング(SM)をディセーブルにします。

内容

概要

このドキュメントでは、適応型セキュリティアプライアンス(ASA)フェールオーバー環境で、モジュールSourceFire(SFR)、コンテキスト認識(CX)、侵入防御システム(IPS)、コンテンツセキュリティおよび制御(CSC)のモニタリングを無効にする方法について説明します。

著者：Cisco TACエンジニア、Cesar Lopez

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 適応型セキュリティアプライアンスの設定。
- ハイアベイラビリティのためのASAフェールオーバーに関する知識。

バージョン9.3(1)から、この機能は設定可能です。前述のバージョンより前は、モジュールは常にモニタされます。このドキュメントで説明されている以前のバージョンでは、回避策を使用できます。

使用するコンポーネント

このドキュメントは、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ASA バージョン 9.3(1) 以降.
- FirePOWERサービス搭載ASA 5500-Xシリーズ、*ASA CX* Context-Aware SecurityまたはIPSモジュール

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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

デフォルトでは、ASAはインストールされたサービスモジュールをモニタします。アクティブユニットモジュールで障害が検出されると、アプライアンスのフェールオーバーがトリガーされます。

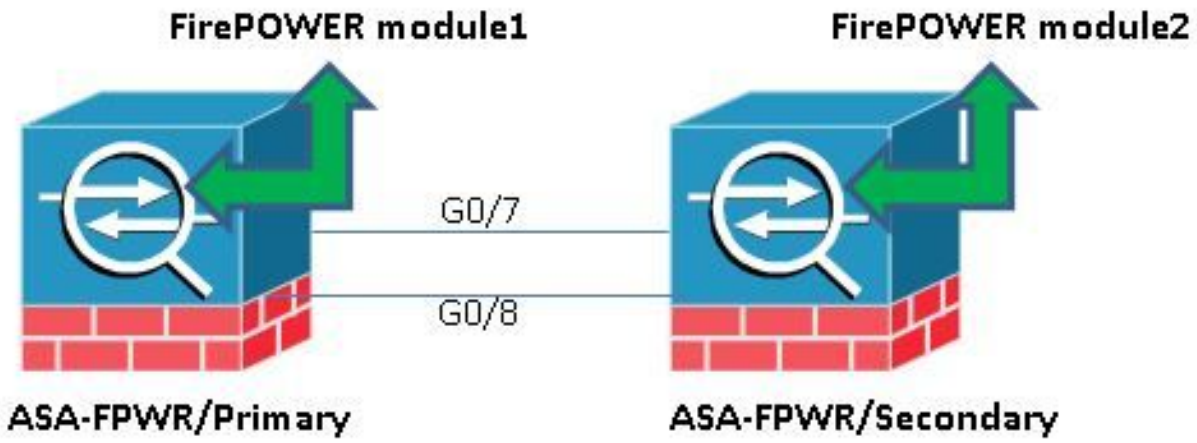
スケジュールされたサービスモジュールのリロードや、ASAフェールオーバーイベントを発生させずに継続的なモジュール障害が発生している場合は、このモニタを無効にすると便利です。

> **注**：フェールオーバープロセスで監視するには、ASAがトラフィックをモジュールに転送する必要があります。

設定

ネットワーク図

このドキュメントでは、次の設定を使用します。



設定

この設定は、このドキュメントで説明されているモニタ機能を実証するためにラボデバイスで使用されます。関連する設定だけが含まれています。この出力の一部の行は省略されています。

```
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
```

モニタされている現在のコンポーネントを確認します。

ASAがフェールオーバーモードの場合、インストールされているサービスモジュールは、アプライアンスインターフェイスと同様にデフォルトでモニタされます。次のコマンドを使用して、モニタされている現在のコンポーネントを確認できます。

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

ASAユニットのサービスモジュールのステータスを確認します。

show failoverの出力**は、各ユ**ニットモジュールの現在のステータスを示しています。

```
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: 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すると、フェールオーバーイベントが発生します。アクティブユニットがスタンバイになり、前のスタンバイユニットがアクティブになります。一部のシナリオでは、ステートフルフェールオーバーでサポートされていない一部の機能が再コンバージェンスされます。

サービスモジュールのfail modeポリシーを確認します。

fail-openpolicyを使用してモジュールにトラフィックを送信すると、トラフィックはサービスモジュールに送信されずにASAを通過し続けます。これは、予想されるモジュールのダウン状態を克服するためのより透過的な方法である可能性があります。

> **警告**：fail-closeポリシーが適用されている場合、モジュールへのトラフィックの転送に使用されるクラスマップに一致するすべてのトラフィックがASAによってドロップされます。

使用されているポリシーステータスを確認するには、**show service-policy [sfr|cx|ips|csc]コマンドを実行します。**

```
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 0
```

モジュラポリシーフレームワーク(MPF)の設定を確認しても、同じことが確認できます。

```
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#
```

サービスモジュールの監視を無効にします。

このコマンドを使用すると、フェールオーバープロセスでサービスモジュールのモニタリングが停止されます。モジュールが「Down」または「Unresponsive」になった場合は、モジュールのリロードやトラブルシューティングをフェールオーバーなしで実行できます。

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

確認

サービスモジュールのモニタリングが無効になっていることを確認します。

実行コンフィギュレーションでは、monitor-interfaceコマンドが無効になります。

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

アクティブユニットでホストされているモジュールをテストしてリロードします。

デモンストレーションの目的で、このユニットのFirePOWERモジュールがリロードされ、アクティブフェールオーバーユニットがこのロールに属しているかどうかを確認します。

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.
```

モジュールのリロード中のASAプライマリ/アクティブユニットからの出力。

ユニットはアクティブなロールのままです。

```
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: 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
```

モジュールのリロード中の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、このステータスを障害として検出せず、アクティブな役割を果たしません。

```
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
```

サービスモジュールの監視を有効にします。

モジュールの監視を有効にするには、次のコマンドを実行します。

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

サービスモジュールが有効になっていることを確認します。

サービスモジュールコマンドは無効にされなくなりました。

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

トラブルシュート

問題1:ASAがフェールオーバーし続け、「Service card in other unit has failed」というメッセージが表示されます。

1つ以上のフェールオーバーイベントが検出された場合は、show failover historyを使用して考えられる原因を確認できます。

```
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
```

now standbyユニットに次のメッセージが表示されます。

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

「Service card in other unit has failed」というメッセージが表示された場合、アクティブユニットが自身のモジュールを応答不能として検出したため、フェールオーバーが発生しました。

モジュールのステータスが「Unresponsive」のままである場合、影響を受けるASAは**Failedモード**です。

```
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
```

解決方法

サービスモジュールのモニタリングを無効にしながら、問題のトラブルシューティングをさらに行ってモジュールを回復できます。

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

問題2:ASAが9.3(1)をサポートしていないか、アップグレードできません。フェールオーバーイベントを回避するにはどうすればよいですか。

従来のASA5500シリーズでは9.3(1)バージョンはサポートされておらず、ソフトウェアモジュールをサポートしていない場合でも、一部のASA5500シリーズにはCSCやIPSなどのハードウェア

モジュールがあります。

新しいASA5500-Xシリーズでも、モニタリングの無効化をサポートするバージョン以下のアプライアンスがあります。

解決方法

ASAは、トラフィックを通過させるためのポリシーが設定されている場合にのみモジュールを監視するため、フェールオーバーを回避するためにモジュールポリシーを削除できます。

使用するクラスマップとポリシーを特定します。

この場合、この設定は、FirePOWERモジュールのトラフィックの転用を削除するために使用されます。

```
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]コマンドを使用して、クラスマップと現在のステータスを検出できます。

```
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
```

モジュールへのトラフィックリダイレクションを無効にします。

ポリシーが削除された後、ASAからモジュールにトラフィックが送信されることはありません。

```
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になっていることを確認します。

同じshowコマンドを使用して、トラフィックがモジュールに送信されなくなったことを確認できます。出力は空でなければなりません。

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

モジュールが応答しない場合でも、アクティブユニットは同じロールのままです。

```
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
```

モジュールへのトラフィックリダイレクトを有効にします。

トラフィックをモジュールに返送する必要がある場合は、フェールオープンまたはフェールクローズのポリシーを再度追加できます。

```
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#
```