禁用在避免不需要的故障切换事件的ASA的服务模块监听(SFR/CX/IPS/CSC)。

目录

简介
要求
使用的组件
背景信息
配置
网络图
配置
检查当前受监视组件。
检查ASA单元服务模块状态。
验证服务模块失败模式策略：
禁用服务模块监听。
验证
验证服务模块监听禁用。
测试重新加载活动装置主机的模块。
Enable (event)服务模块监听。
验证服务模块启用。
故障排除
问题1. ASA继续故障切换，并且此消息“卡在其他单元失败”的服务表示。
解决方案
问题2。我的ASA不支持9.3(1)或我不能升级它。如何能避免故障切换事件？
解决方案
了解使用的类映射和具体政策。
禁用流量重定向到模块。
验证对模块的ASA重定向禁用。
启用流量重定向到模块。

简介

本文描述如何禁用在模块SourceFire (SFR)的意识监听的上下文(CX)，入侵防御系统(IPS)、内容安全和控制(CSC)在一个可适应安全工具(ASA)故障切换环境。

贡献用塞萨尔省卢佩茨， Cisco TAC工程师。

先决条件

要求

思科建议您有以下主题的知识：

- 可适应安全工具的配置。
- ASA故障切换知识高可用性的。

从版本9.3(1)，此功能可配置。在被提及的版本前，模块永远将是受监视。应急方案可以用于描述的以前版本在本文。

使用的组件

本文根据这些软件和硬件版本：

- Cisco ASA版本9.3(1)和以上。
- ASA 5500-X系列用火力服务、*ASA CX上下文*意识安全或者IPS模块。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络实际，请确保您了解所有命令潜在影响

背景信息

默认情况下， ASA监控一个已安装服务模块。如果失败在活动装置模块检测，设备故障切换被触发。

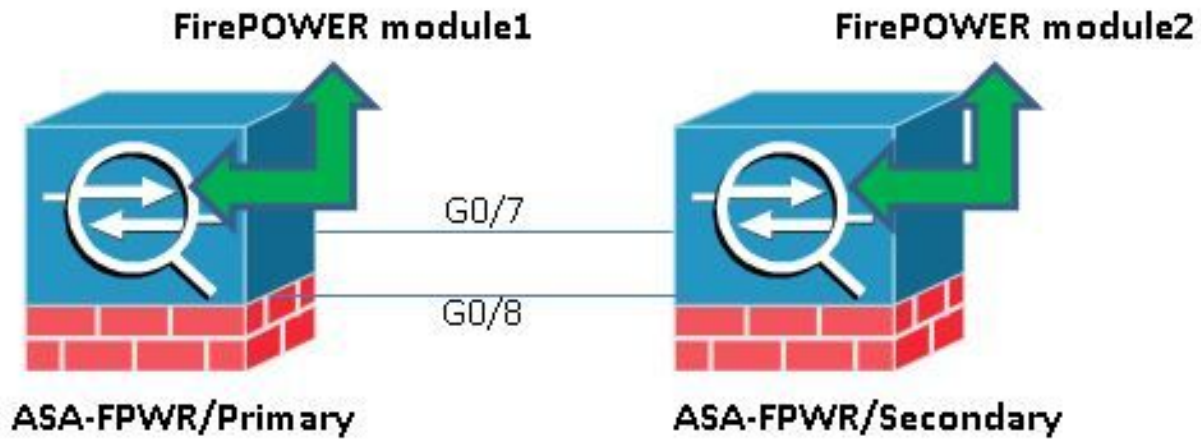
禁用此监视器可以是有用的，当有同样的一个被安排的服务模块重新加载或连续模块故障时，无需愿有ASA故障切换事件。

> **注意**：ASA需要将流量转变为模块为了由故障切换进程监控。

配置

网络图

本文使用此设置：



配置

此配置用于实验室设备展示在本文提及的监控程序功能。仅相关配置包括。某些此输出线路省略。

```
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
```

检查当前受监视组件。

当ASA在故障切换模式时，安装的默认情况下服务模块监控，正设备建立接口。此命令可以用于，为了发现哪些当前组件监控：

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

检查ASA单元服务模块状态。

show failover输出显示每个单元模块当前状态：

```
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
```

如果活动装置的服务模块断开，故障切换事件发生。活动装置变得暂挂，并且上一个备用装置占领现任角色。在某些情况下，这造成有状态故障切换不支持的一些功能，再聚合。

验证服务模块失败模式策略：

如果FAILopenpolicy用于发送流量到模块，流量持续通过ASA没有发送对服务模块。这可以是一个更加透明的方式解决一个预计模块中断状态。

> 警告：如果FAIL close策略应用，则，匹配类映射的所有流量用于牵制对模块的流量由ASA丢弃。

为了认识使用的策略状态，请运行show service命令**策略[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
```

同样能通过检查模块化政策架构(MPF)配置看到：

```
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#
```

禁用服务模块监听。

此命令，做故障切换process stop监听服务模块。所有计划的重新加载或排除故障可以执行到模块，不用故障切换，在断开的模块的情况下“”或“无答复”。

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

验证

验证服务模块监听禁用。

在运行的配置下，接口命令否定。

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

测试重新加载活动装置主机的模块。

演示目的，在此单元的火力模块重新加载确认活动故障切换单元是否在此角色坚持。

从火力模块的输出在主要的ASA/活动装置。

```
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.
```

从主要的ASA的输出/活动装置，当模块重新加载时。

单元在现任角色坚持。

```
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
```

输出从ASA第二/备用装置，当模块重新加载时：

当失败和doen't占领现任角色，备用装置不检测此状态。

```
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
```

Enable (event)服务模块监听。

要启用模块监听，请运行此命令：

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

验证服务模块启用。

服务模块命令不再否定。

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

故障排除

问题1. ASA继续故障切换，并且此消息“卡在其他单元失败”的服务表示。

如果一个或许多故障切换事件检测， **show failover历史记录**可以用于认识可能的来源。

```
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
```

备用装置当前表示此消息：

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

如果“在其他单元的服务卡失败”消息被看到，故障切换发生，因为活动装置检测其自己的模块如无答复。

如果模块在“无答复的”状态坚持，受影响的ASA在**失败的**模式坚持。

```
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
```

解决方案

当排除故障问题的进一步步骤可以被实行为了恢复模块时，服务模块监听可以禁用。

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

问题2。我的ASA不支持9.3(1)或我不能升级它。如何能避免故障切换事件？

ASA5500系列的传统不支持9.3(1)版本，并且，即使他们不支持软件模块，有些有硬件模块例如CSC或IPS。

与新ASA5500-X系列，有有版本的一些设备在支持禁用监听的那个之下。

解决方案

如果有配置的策略通过流量到它， ASA只监控模块。因此，为了避免故障切换，模块策略可以删除。

了解使用的类映射和具体政策。

在这种情况下，此配置用于删除火力模块的流量转换。

```
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命令**策略[csc|cxsc|ips|sfr]**可以用于检测类映射和当前状态。

```
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
```

禁用对模块的流量重定向。

在策略删除后，进一步流量没有从ASA发送到模块。

```
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#
```

验证对模块的ASA重定向禁用。

同样**show命令**可以用于验证流量不再去模块。输出一定是空的。

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

即使模块是无答复的，活动装置在同一个角色依然是。

```
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
```

Enable (event)对模块的流量重定向。

一旦流量需要被退还的到模块，FAIL开放或FAIL close策略可以是被添加的上一步。

```
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#
```