Monitoração do módulo de serviço do desabilitação no ASA para evitar os eventos indesejáveis do Failover (SFR/CX/IPS/CSC).

Índice

Introdução

Este documento descreve como desabilitar a monitoração nos módulos SourceFire (SFR), o contexto ciente (CX), o Intrusion Prevention System (IPS), a Segurança satisfeita e o controle (CSC) em um ambiente de failover adaptável da ferramenta de segurança (ASA).

Contribuído por Cesar López, engenheiro de TAC da Cisco.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento dos seguintes assuntos:

- Configuração da ferramenta de segurança adaptável.
- Conhecimento do Failover ASA para a Alta disponibilidade.

Da versão 9.3(1), esta característica é configurável. Antes da versão mencionada, o módulo será monitorado sempre. Uma ação alternativa pode ser usada para as versões anterior descritas neste documento.

Componentes Utilizados

Este documento é baseado nestes versão de software e hardware:

- Versão ASA de Cisco 9.3(1) e mais atrasado.
- 5500-X Series ASA com serviços da potência de fogo, Segurança *ASA CX* ou módulo ips Contexto-ciente.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, entenda o possível impacto de todos os comandos

Informações de Apoio

Àrevelia, o ASA monitora um módulo de serviço instalado. Se uma falha é detectada no módulo da unidade ativa, o Failover do dispositivo está provocado.

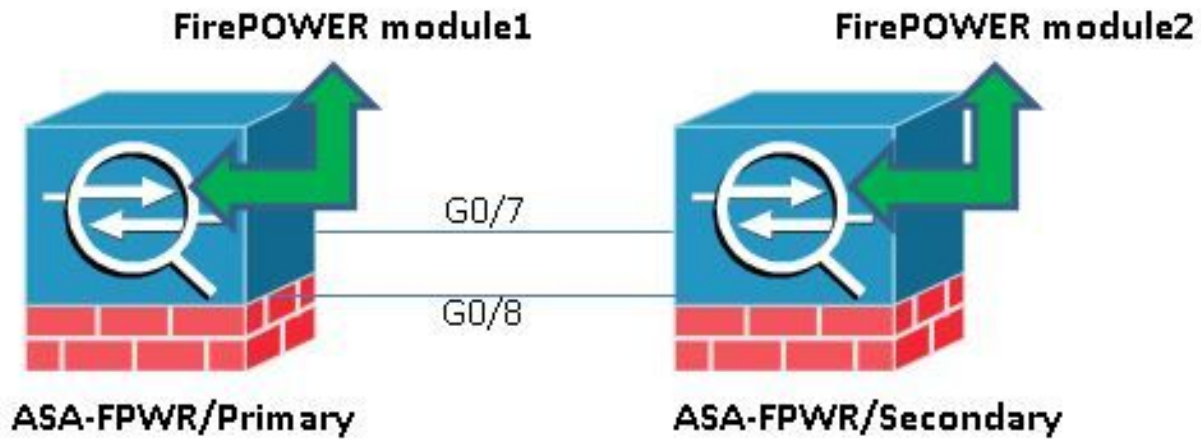
Pode ser útil desabilitar este monitor quando há um reload programado do módulo de serviço ou umas falhas no módulo contínuas do mesmos sem querer ter um evento do Failover ASA.

> Nota: O ASA precisa de desviar o tráfego ao módulo a fim ser monitorado pelo processo do Failover.

Configurar

Diagrama de Rede

Este documento usa esta instalação:



Configurações

Esta configuração é usada em dispositivos do laboratório para demonstrar os recursos de monitoramento mencionados neste documento. Somente a configuração relevante é incluída. Algumas das linhas desta saída são omitidas.

```
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
```

Verifique os componentes monitorados corrente.

Quando os ASA reagem do modo de failover, o módulo de serviço instalado está monitorado à revelia, apenas como o dispositivo conecta. Este comando pode ser usado, a fim considerar que componentes atuais são monitorados:

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

Verifique o estado do módulo de serviço das unidades ASA.

A saída do **Failover da mostra** mostra o status atual de cada módulo da unidade:

```
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
```

Se o módulo de serviço de uma unidade ativa vai para baixo, um evento do Failover ocorre. A unidade ativa torna-se à espera, e a unidade de standby anterior toma o papel ativo. Em algumas encenações, isto causa algumas características que não são apoiadas por uma comutação classificada, ao reconvergir.

Verifique a política do modo da falha do módulo de serviço:

Se uma falha-openpolicy é usada para enviar o tráfego ao módulo, trafique continua a atravessar o ASA sem ser enviada ao módulo de serviço. Esta pode ser uma maneira mais transparente de superar um status baixo previsto do módulo.

> **aviso:** Se uma política do falha-fim foi aplicada, a seguir, todo o tráfego que combina o mapa de classe usado para desviar o tráfego ao módulo está deixado cair pelo ASA.

A fim conhecer o estado da política usado, execute a serviço-**política do** comando show **[sfr|CX|IP|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
```

O mesmos podem ser vistos verificando a configuração modular da estrutura de política (MPF):

```
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#
```

Monitoração do módulo de serviço do desabilitação.

Este comando, faz à parada do processo do Failover a monitoração do módulo de serviço. Todo o reload de planeamento ou pesquisa defeitos pode ser feito ao módulo sem um Failover, em caso do módulo que vai “para baixo” ou “sem resposta”.

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

Verificar

Verifique que a monitoração do módulo de serviço está desabilitada.

Sob a configuração running, o comando da monitor-relação é negado.

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

Para testar o reload o módulo hospedado pela unidade ativa.

Para propósitos de demonstração, o módulo da potência de fogo nesta unidade está recarregado para confirmar se a unidade de failover ativa fica neste papel.

Saída do módulo da potência de fogo no ASA preliminar/unidade ativa.

```
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.
```

Saída do ASA preliminar/unidade ativa quando os reloads do módulo.

A unidade fica no papel ativo.

```
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
```

Saída do ASA secundário/unidade em standby quando o módulo recarregar:

A unidade em standby não detecta este estado como uma falha e um doen't para tomar o papel ativo.

```
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
```

Permita a monitoração do módulo de serviço.

Para permitir a monitoração do módulo, execute este comando:

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

Verifique que o módulo de serviço está permitido.

O comando do módulo de serviço não é negado anymore.

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

Troubleshooting

A edição 1. ASA mantém-se falhar sobre, e esta mensagem do “cartão serviço na outra unidade falhou” é mostrada.

Se um ou muito evento do Failover é detectado, a **história do Failover da mostra** pode ser usada para conhecer a razão possível.

```
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
```

A unidade em standby do now mostra esta mensagem:

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

Se do “o cartão serviço na outra unidade falhou” a mensagem está considerada, o Failover aconteceu porque a unidade ativa detectou seu próprio módulo como sem resposta.

Se o módulo fica no estado “sem resposta”, o ASA afetado fica no modo **falhado**.

```
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
```

Solução

A monitoração do módulo de serviço pode ser desabilitada quando umas etapas mais adicionais para pesquisar defeitos a edição puderem ser executadas a fim recuperar o módulo.

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

Edição 2. Meu ASA não apoia 9.3(1) ou eu não posso promovê-lo. Como posso eu evitar eventos do Failover?

O ASA5500 Series do legado não apoia 9.3(1) a versão e, mesmo se não fazem os módulos de software de suporte, alguns dele têm os módulos de hardware tais como o CSC ou o IPS.

Mesmo com o ASA5500-X Series novo, há alguns dispositivos com versões abaixo de essa que apoia a monitoração do desabilitação.

Solução

O ASA monitora somente o módulo se há uma política configurada para lhe passar o tráfego. Assim, a fim evitar um Failover, a política do módulo pode ser removida.

Identifique o mapa e a política da classe usados.

Neste caso, esta configuração é usada para remover a diversão do tráfego de um módulo da potência de fogo.

```
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
!
```

A serviço-política do comando show [csc|cxsc|IP|o sfr] pode ser usado para detectar o mapa e o status atual da classe.

```
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
```

Reorientação do tráfego do desabilitação ao módulo.

Depois que a política é removida, nenhum tráfego mais adicional está enviado do ASA ao módulo.

```
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#
```

Verifique que a reorientação ASA ao módulo está desabilitada.

O mesmo comando show pode ser usado para verificar que o tráfego já não está indo ao módulo. A saída deve estar vazia.

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

Mesmo se o módulo é sem resposta, a unidade ativa permanece no mesmo papel.

```
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
```

Permita o tráfego reorientam ao módulo.

Uma vez que o tráfego precisa de ser enviado para trás ao módulo, a política falha-aberta ou do falha-fim pode ser adicionada para trás.

```
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#
```