

ىلع ةمدخلل ةيظمنلا ةدحولاً ةبقارم لىطعت بوغرملا ريغ لىش فلا زواجت ثادحاً بىنچتل ASA (SFR/CX/IPS/CSC). اهي ف

تايوت حملال

[ةمدقملا](#)

[تابللطتملا](#)

[ةمدختس ملام تانوك ملام](#)

[ةيساسات امولعم](#)

[نىوك تلال](#)

[ةكبش لىل لىطىطختلا ملام](#)

[تانىوك تلال](#)

[.ةيلاجلال ةبقارملا تانوك ملام نم ققحت](#)

[.ASA تادحو ةمدخ ةدحو ةلاخ نم ققحت](#)

[:بولس لىش فى ةيظمن ةدحو ةمدخلال تقود](#)

[.ةمدخلل ةيظمنلا ةدحولال ةبقارم لىطعت](#)

[ةحصلال نم ققحتلا](#)

[.ةيظمنلا ةمدخلال ةدحو ةبقارم لىطعت نم ققحت](#)

[.ةطش نلا ةدحولال ةطساوب ةفاضتس ملام ةيظمنلا ةدحولال لىمحت ةداعا رابتخال](#)

[.ةيظمنلا ةمدخلال ةدحو ةبقارم نىكمت ب مق](#)

[.ةمدخلل ةيظمنلا ةدحولال نىكمت نم ققحت](#)

[اهال صاوا ءاطخال افاشكتسا](#)

[ةمدخلال ةقاطب تلىش ف دقل" ةلاسرلا هذه ضرع متىو، لىش فلا فى ASAs رمتسى 1. ةلاسى ملام
"ىرخا ةدحو فى".](#)

[لحللا](#)

[يننكمى فىك. هتقىرت يننكمى ال وا \(1\)9.3 رادصال ال ب صاخلا ASA معدى ال 2. ةلاسى ملام](#)

[؟ لىش فلا زواجت ثادحو بىنچت](#)

[لحللا](#)

[.ةمدختس ملام ةسايسلاو ةئىفلا ةطىرخ دح](#)

[.ةيظمنلا ةدحولال لىل رورملا ةكرح هيجوت ةداعا لىطعت ب مق](#)

[.قأعم ةيظمن ةدحولال لىل ASA redirection لىل نأ تقود](#)

[.ةيظمنلا ةدحولال لىل تانابلا رورم ةكرح هيجوت ةداعا نىكمت](#)

ةمدقملا

و SourceFire (SFR) ةيظمنلا تادحولال لىل ةبقارملا لىطعت ةي فىك دنتس ملام اذه حضوى
فى (CSC) مكحتلاو يوت حملال نام او (IPS) Intrusion Prevention System و Context Aware (CX)
(ASA). فىكتلل لىل لىل نامال زاوجب ةصاخلا لاطعال لىل بلىغتلال ةئىب

Cisco نام TAC سدنهم، زىبول رازيس هب مهاس

ةيساسأل تابلطتمل

تابلطتمل

ةيلال عيضاوملاب ةفرعم كيدل نوكت نأب Cisco ي صوت:

- ةلدعمل نامأل ةزهجأ ةئيهت.
- [ةيلاع رفوت ةينالما يلع لوصحلل ASA لشف زواجت](#) ةفرعم.

ةدحول لظتس ، روكذمل رادصلال لبقو . نيوكتلل ةلباق ةزيملا هذه نوكت ، (1)9.3 رادصلال نم ةحضوملا ةقباسلا تارادصلال ليدب لح مادختسا نكمي . امئاد ةبقارملل ةعضاخ ةيظمنلا دننتملا اذه يف

ةمدختسملا تانوكملا

ةيلال ةيظمنلا تانوكملا وجماربل تارادصلال دننتملا اذه دننسي

- ثدخال تارادصلال او (1)9.3 رادصلال Cisco ASA.
- ASA CX Context-aware ةيظمنلا ةدحول وأ FirePOWER تامدخ عم ASA 5500-X ةلسلسلا IPS وأ Security.

ةصاخ ةيظمنلا ةئيب يف ةدوحووملا ةزهجأ نم دننتملا اذه يف ةدراول تامولعمل عاشنإ مت تناك اذا . (يضاارتفا) حوسم نيوكتب دننتملا اذه يف ةمدختسملا ةزهجألا عيمج تادب رمأ يال لم تحملا ريثاتلل كمهف نم دكأتف ، ةرشابم كتكبش

ةيساسأ تامولعم

ةيظمنلا ةدحول يف لظع فاشتك ةلاح يف . ةتبثم ةمدخ ةدحوو ASA بقاري ، يضاارتفا لكشب زاهجل لشف زواجت ليغشت متي ، ةطشنلا ةدحول

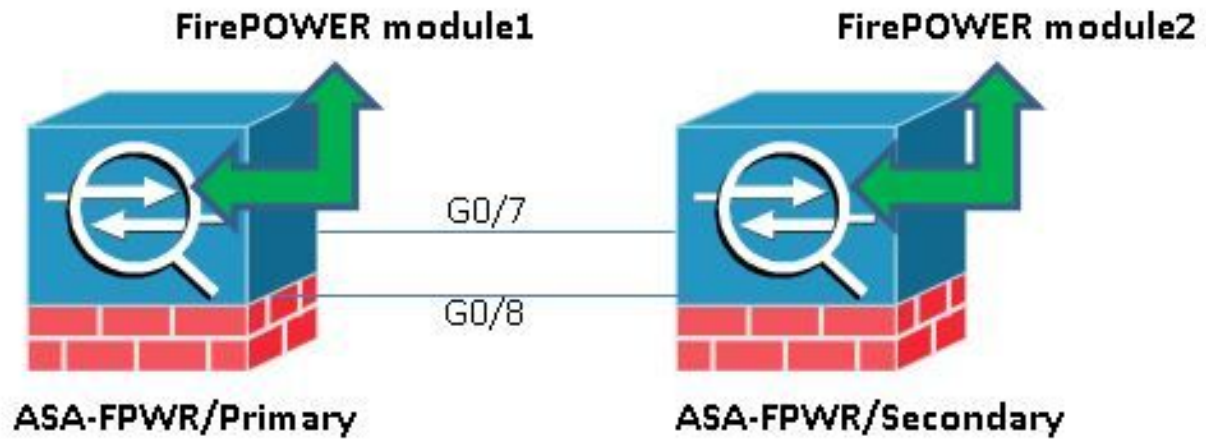
ةمدخل ةدحول ةلودجم ليحت ةداعإ كانه نوكي امدنع ةشاشلا هذه ليظعت ديفملا نم نوكي دق ASA لشف زواجت ثدح ءارجإ يف ةبغر نود اهسفن ةيظمنلا ةدحول ةلصتم لشف تالاح وأ

نكمي يتح ةيظمنلا ةدحول ل تانايبال رورم ةكرح ليوحتب ASA موقوي نأ بجي : **ةظحالم** . لشفال زواجت ةيظمنلا ةطساوب اهتبقارم

نيوكتلا

ةكبشلل يطيظختلا مسرلا

دادعإلا اذه دننتملا اذه مدختسي



تاني وكتال

اذه يف ةروك ذملا ةشاشلا ةزيم حيضوتل رب تخملا ةزهجأ يف ني وكتال اذه مادختسا متي جارخإلا اذه روطس ضعب فذح متي . طقف ةلصلال يذ ني وكتال ني مضت متي . دننتمل

```
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
!
...
```


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

لش ف زواج ت شح شح، ةطشن ةدحوب ةصاخ ل ةمدخل ل ةيطمن ل ةدحول ل طعت ةلاح يف
رودلاب ةقبا س ل ةيطاي ت ح ال ةدحول موقتو، دادعت س ال ع ضو يف ةطشن ل ةدحول ح بصتو
ريغ تازي م ل ضعب براق ةداع يف ك لذ بب س تي، تاهو وي ران ي س ل ضعب يف . طشن ل
ةلاح ل يذ لش ف ال زواج ت ةم و ع دم ل

ببولس أ لش في ةيطمن ةدحو ةمدخل ت ق قد

ةك رح رم ت سي، ةيطمن ةدحول ال رورم ةك رح لس ري نأ نو كي Failed-open Policy تلمعت سا ن
ةقير ط هذه نوكت نأ نكمي. ةيطمن ةدحو ةمدخل ال ال تلسرأ نو كي نأ نو ASA ل ربع رمي رورم
ةةقوت م ل ةيطمن ل ةدحول ضاف خنا ةلاح ال ع بل غت ل ةي ف افش رثك

رورم ل ةك رح عي مج طاق س ا ذئ ني ح متي، لش ف ال ق ال غ ا س ا ي س ق ي ب طت مت اذا: ري ذحت
ةيطمن ل ةدحول ال رورم ل ةك رح لي وحت ل ةمدخت س م ل ةئ ل ةطير خ ق باط تي ل
ASA ةطساوب

show service-policy [sfr|cx|ips|csc] . رم ال ل ي غ شت ب مق، ةمدخت س م ل ج هن ل ةلاح ةفر عم ل

```
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
```

ةيطمن ل ةسا ي س ل لم ع راط ا ني وكت نم ق قحت ل ل الخ نم عي ش ل س فن رن نأ ان ع س و ب و
(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#
```

ةمدخل لة طمن الة دحولا ة ب قارم لى طعت

يأ عارجا نكم ي. ةمدخل لة طمن الة دحولا ة ب قارم فوق ل ش فال زواج ة لى لمع لعج ي، رمأ اذ ه ي ف، ل ش فال زواج نود اه ا ل ص او ة دحولا ة ا ط خ ا ف اش ك ت س ا و ا ه ل ط ط خ م لى م ح ت ة د ا ع ا ة لى لمع "ب ب ج ت س م ر ي غ" و ا "ل ف س ا ل" ة طمن الة دحولا ة ج و ر خ ة ل ا ح

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

ة ح ص ل ا ن م ق ق ح ت ل ا

ة طمن الة دحولا ة ب قارم لى طعت ن م ق ق ح ت

monitor-interface رمأ ا ل ص ف ر م ت ي، ه ل ي غ ش ت ي ر ا ج ل ن ي و ك ت ل ا ت ح ت

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

ة ط ش ن ل ا ة د ح و ل ا ة ط س ا و ب ة ف ا ض ت س م ل ا ة ط م ن ل ا ة د ح و ل ا لى م ح ت ة د ا ع ا ر ا ب ت خ ا ل

ة د ح و ل ا ه ذ ه لى ل ع ة د و ج و م ل ا FirePOWER ة د ح و لى م ح ت ة د ا ع ا م ت ي، ي ح ي ض و ت ل ا ض ر ع ل ا ض ا ر غ ا ل ر و د ل ا ا ذ ه لى ل ع ي ق ب ت س ة ط ش ن ل ا ل ا ط ع ا ل ا ز و ا ج ت ة د ح و ت ن ا ك ا ذ ا م م د ك ا ت ل ل

ASA ل ة ط ش ن ل ا / ة ل س ا س ا ل ا ة د ح و ل ا ي ف FirePOWER ة د ح و ن م ج ر خ

```
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.

ةيظمنللا ةدحوللا ليمحت ةداع| ءانثأ ASA ل طشنللا/ةيساسألا ةدحوللا نم جارخ|

طشنللا رودلا يي ةدحوللا يقبت.

```
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
```

ةيظمنللا ةدحوللا ليمحت ةداع| ءانثأ ASA ةيظمايحتحالا/ةيظونثالا ةدحوللا نم جارخ

طشنللا رودلا ذخأت اللولش ف ةلاحك ةلاحلا هذه ةيظمايحتحالا ةدحوللا فشكت ال

```
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

ةيظمنللا ةمدخللا ةدحو ةبقارم نيكم تب مق

رمألا اذه ليغش تب مق ،ةيظمنللا ةدحو لا ةبقارم نيكم متل

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

ةمدخلل ةيظمنللا ةدحو لا نيكم تب نم ققحت

ايغل م ةمدخلل ةيظمنللا ةدحو لا رمأ دعي مل

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

اهحال صإو ءاطخال فاشكتسا

تلش ف دقل " ةلاسرلا هذه ضرع متي و ،لش فال في ASAs رمتسي 1. ةلاسرلا
ب"ىخأ ةدحو في ةمدخللا ةقاطب

show تاطوفحم مادختسا نكمي ،لش فال زواجت ثادحأ نم رثكأ وأ دحاو ثدح نع فشكال مت اذإ
لمتحملا ببسلا ةفرعمل لش فال زواجتل

```
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
```


ليطعت معددي نأ دحاولا تحت ةغيص عم زاهج ضعب كانه ،ةديدلج ASA5500-X ةلسلس عم ىتح ةبقارملا

لحل

رورملا ةكره ريرمتل اهنوكت مت ةسايس كانه ناك اذا طقف ةيطمنلا ةدحولا ASA بقاري ةيطمنلا ةدحولا ةسايس ةلازا نكمي ،لشفال زواجت بنحتل ،لكذل.اهيلا

ةمدختسملا ةسايسلا ةئفلا ةطيرخ دح.

FirePOWER ةدحول تانايبلا رورم ةكره ليوحت ةلازال نيوكتلا اذه مدختسي ،ةلحل هذه في ةيطمنلا

```
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
!
```

ةلحل او ةئفلا ةطيرخ فاشتكال `show service-policy [csc|cxsc|ips|sfr]` رمألا مادختس نكمي ةلحل

```
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
```

ةيطمنلا ةدحولا ل رورملا ةكره هيجوت ةداع ليطعتب مق

ةيظمنلا ءءولا لىل ASA نم ىرأ رورم ءكء لاسرا مءى ال ءهنا ءلازا ءعب

```
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#
```

قأعم ءيظمن ءءولا لىل ASA redirection ل نا ءقءء

ءءولا لىل لقتن ءءء مل رورملا ءكء نا نم ققءءلل هسفن show رمأل ماءءءسا نكمى
أءراف ءارءال نوكى نا بءى . ءيظمنلا

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

هسفن روءلا فى ءطشنلا ءءولا لىقءءء ءبءء ءبءىءءسم رىء ءءولا ءناك اءل ىءء

```
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

ةيظمنلا ةدحوللا ىلإ تانايبلا رورم ةكرح هيجوت ةداعإ نيكمت

ةفاضإ نكمي ،ةيظمنلا ةدحوللا ىلإ ىرخأ ةرم اهلاسرا متي نأ ىلإ رورملا ةكرح جاتحت نأ درجمب
ىرخأ ةرم قالغإ-لشف وأ حتف-لشف جهن

```
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#
```

