

Vervang een ASA-firewall door een Active/Standby failover-paar

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Verschil tussen primaire en secundaire eenheden in de failover-configuratie](#)

[Verschil tussen actieve en stand-by eenheden in de failover-configuratie](#)

[Vervang de secundaire firewallstoring](#)

[Vervang de primaire firewallfout](#)

Inleiding

Dit document beschrijft hoe u een adaptieve security applicatie (ASA) firewall vervangt door een active/stand-by failover-paar.

Achtergrondinformatie

De ASA firewalls ondersteunen twee failover-configuraties, active/active failover en active/stand-by failover.

Er zijn 2 firewalls:

- firewall-a is primair/actief
- firewall-b is secundair/stand-by

Verschil tussen primaire en secundaire eenheden in de failover-configuratie

Deze opdracht betekent dat deze firewall altijd de actieve configuratie naar de secundaire firewall duwt.

```
# failover lan unit primary
```

Deze opdracht betekent dat deze firewall altijd de actieve configuratie ontvangt van de primaire firewall.

```
# failover lan unit secondary
```

Verschil tussen actieve en stand-by eenheden in de failover-configuratie

Deze opdracht betekent dat deze firewall de actieve actieve actieve firewall in het failover-paar is.

```
# failover active
```

Deze opdracht betekent dat deze firewall de stand-by is die een firewall in het failover-paar uitvoert.

```
# failover standby
```

Vervang de secundaire firewallstoring

1. Controleer of de primaire firewall actief en online is. Voorbeeld:

```
firewall-a/pri/act# show failover
Failover On
Failover unit Primary
Failover LAN Interface: sync Port-channel1 (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 0 of 1292 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.12(4)56, Mate 9.12(4)56
Serial Number: Ours JADSERIAL1, Mate JADSERIAL2
Last Failover at: 19:54:29 GMT May 23 2023
  This host: Primary - Active
    Active time: 2204 (sec)
    slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
      Interface inside (10.0.0.1): Normal (Not-Monitored)
      Interface outside (10.1.1.1): Normal (Not-Monitored)
      Interface management (10.2.2.1): Normal (Not-Monitored)
  Other host: Secondary - Failed
    Active time: 0 (sec)
    slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
      Interface inside (10.0.0.2): Normal (Not-Monitored)
      Interface outside (10.1.1.2): Normal (Not-Monitored)
      Interface management (10.2.2.2): Normal (Not-Monitored)
```

2. Sluit de secundaire firewall af en verwijder deze fysiek.
3. Voeg de nieuwe secundaire firewall fysiek toe en schakel deze in.
4. Zodra de nieuwe secundaire firewall met de standaard fabrieksconfiguratie actief is, schakel de failover link in,no shutdownde fysieke failover link.

Voorbeeld:

```
firewall-a/pri/act#conf t
firewall-a/pri/act#(config)#interface Port-channel1
firewall-a/pri/act#(config-if)#no shutdown
firewall-a/pri/act#(config)#exit
firewall-a/pri/act#
firewall-b/sec/stby#conf t
firewall-b/sec/stby#(config)#interface Port-channel1
firewall-b/sec/stby#(config-if)#no shutdown
firewall-b/sec/stby#(config)#exit
firewall-b/sec/stby#
```

5. Configuratie van failover-opdrachten. Voorbeeld:

```
firewall-a/pri/act# sh run | inc fail
failover
failover lan unit primary
failover lan interface sync Port-channel1
failover link sync Port-channel1
failover interface ip sync 10.10.13.9 255.255.255.252 standby 10.10.13.10
no failover wait-disable
firewall-a/pri/act#
```

```
firewall-b/sec/stby# sh run | inc fail
no failover
failover lan unit secondary
failover lan interface sync Port-channel1
failover link sync Port-channel1
failover interface ip sync 10.10.13.9 255.255.255.252 standby 10.10.13.10
no failover wait-disable
firewall-b/sec/stby#
```

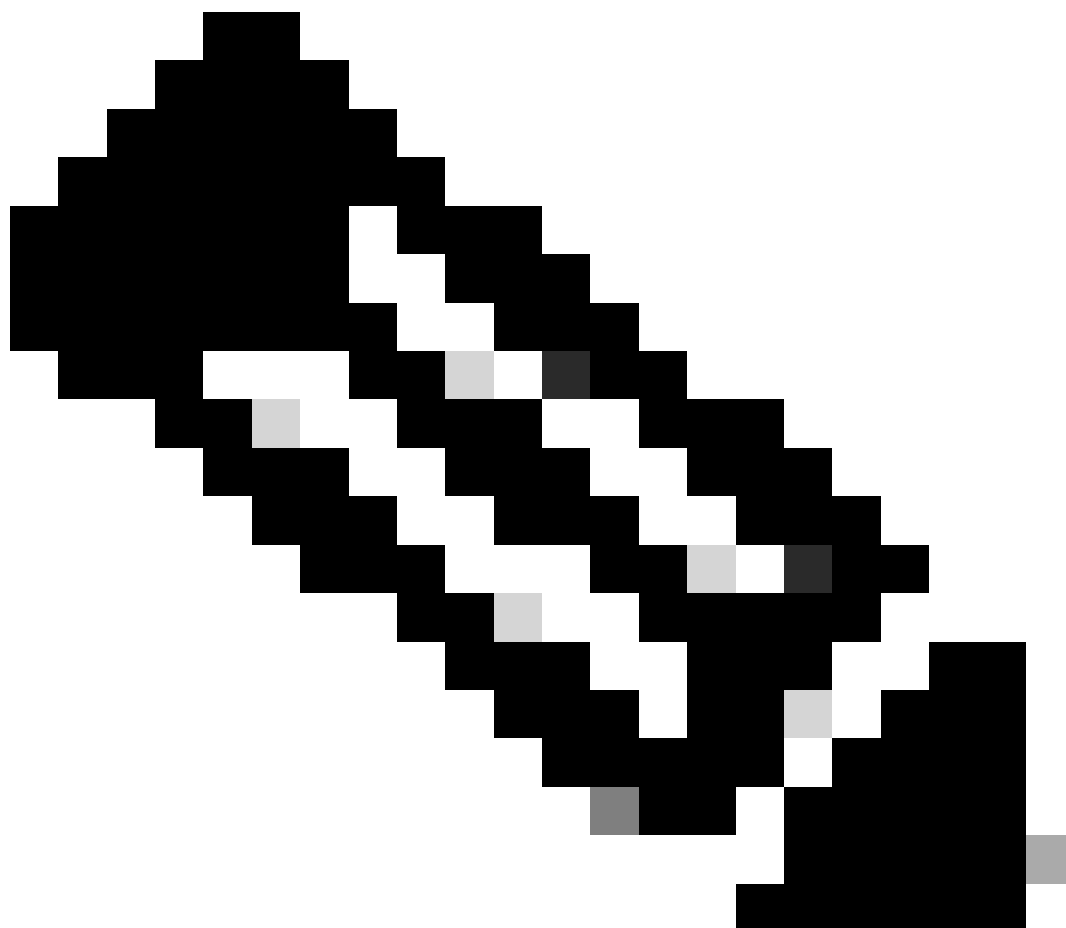
6. Schakel failover op de nieuwe secundaire firewall in. Voorbeeld:

```
firewall-b/sec/stby#conf t
firewall-b/sec/stby#(config)#failover
firewall-b/sec/stby#(config)#exit
firewall-b/sec/stby#
firewall-b/sec/stby# sh run | inc fail
```

failover
firewall-b/sec/stby#

7. Wacht tot de actieve configuratie aan de nieuwe eenheid is gesynchroniseerd en bevestig de juiste failover-status. Voorbeeld:

```
firewall-a/pri/act#  
Beginning configuration replication: Sending to mate.  
End Configuration Replication to mate  
firewall-a/pri/act#  
firewall-b/sec/stby#  
Beginning configuration replication from mate.  
End configuration replication from mate.  
firewall-b/sec/stby#
```



Opmerking: Merk op dat de primaire firewall (firewall-a) de configuratie naar de

secundaire firewall (firewall-b) stuurt.

8. Sla de configuratie op in de primaire/actieve modus en valideer het schrijfgeheugen op de nieuwe secundaire/stand-by modus. Voorbeeld:

```
firewall-a/pri/act#write memory
Building configuration...
Cryptochecksum: ad317407 935a773c 6c5fb66a c5edc342
64509 bytes copied in 9.290 secs (7167 bytes/sec)
[OK]
firewall-a/pri/act#
firewall-b/sec/stby#
May 24 2023 15:16:21 firewall-b : %ASA-5-111001: Begin configuration: console writing to memory
May 24 2023 15:16:22 firewall-b : %ASA-5-111004: console end configuration: OK
May 24 2023 15:16:22 firewall-b : %ASA-5-111008: User 'failover' executed the 'write memory' command.
May 24 2023 15:16:22 firewall-b : %ASA-5-111010: User 'failover', running 'N/A' from IP x.x.x.x , executed 'write memory'
firewall-b/sec/stby#
```

9. Controleer of het failover-paar op beide firewalls actief is. Voorbeeld:

```
firewall-a/pri/act# show failover
Failover On
Failover unit Primary
Failover LAN Interface: sync Port-channel1 (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 0 of 1292 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.12(4)56, Mate 9.12(4)56
Serial Number: Ours JADSERIAL1, Mate JADSERIAL2
Last Failover at: 19:54:29 GMT May 23 2023
  This host: Primary - Active
    Active time: 71564 (sec)
    slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
      Interface inside (10.0.0.1): Normal (Not-Monitored)
      Interface outside (10.1.1.1): Normal (Not-Monitored)
      Interface management (10.2.2.1): Normal (Not-Monitored)
  Other host: Secondary - Standby Ready
    Active time: 0 (sec)
    slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
      Interface inside (10.0.0.2): Normal (Not-Monitored)
      Interface outside (10.1.1.2): Normal (Not-Monitored)
      Interface management (10.2.2.2): Normal (Not-Monitored)
```

```
firewall-b/sec/stby# show failover
Failover On
Failover unit Secondary
Failover LAN Interface: sync Port-channel1 (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 0 of 1292 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.12(4)56, Mate 9.12(4)56
Serial Number: Ours JADSERIAL2, Mate JADSERIAL1
Last Failover at: 20:51:27 GMT May 23 2023
  This host: Secondary - Standby Ready
    Active time: 0 (sec)
    slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
      Interface inside (10.0.0.2): Normal (Not-Monitored)
      Interface outside (10.1.1.2): Normal (Not-Monitored)
      Interface management (10.2.2.2): Normal (Not-Monitored)
  Other host: Primary - Active
    Active time: 71635 (sec)
    slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
      Interface inside (10.0.0.1): Normal (Not-Monitored)
      Interface outside (10.1.1.1): Normal (Not-Monitored)
      Interface management (10.2.2.1): Normal (Not-Monitored)
```

Vervang de primaire firewallfout

1. Controleer of de secundaire firewall actief en online is. Voorbeeld:

```
firewall-b/sec/act# show failover
Failover On
Failover unit Secondary
Failover LAN Interface: sync Port-channell (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 0 of 1292 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.12(4)56, Mate 9.12(4)56
Serial Number: Ours JADSERIAL2, Mate JADSERIAL1
Last Failover at: 19:54:29 GMT May 23 2023
  This host: Secondary - Active
    Active time: 2204 (sec)
    slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
      Interface inside (10.0.0.1): Normal (Not-Monitored)
      Interface outside (10.1.1.1): Normal (Not-Monitored)
      Interface management (10.2.2.1): Normal (Not-Monitored)
  Other host: Primary - Failed
    Active time: 0 (sec)
    slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
      Interface inside (10.0.0.2): Normal (Not-Monitored)
      Interface outside (10.1.1.2): Normal (Not-Monitored)
      Interface management (10.2.2.2): Normal (Not-Monitored)
```

2. Sluit de primaire firewall af en verwijder deze fysiek.
3. Voeg fysiek de nieuwe primaire firewall toe en schakel deze in.
4. Nu, wordt de nieuwe primaire firewall actief met de standaardfabrieksconfiguratie.
5. Schakel de failover link in en sluit de failover fysieke link niet. Voorbeeld:

```
firewall-a/pri/stby#conf t
firewall-a/pri/stby#(config)#interface Port-channel1
firewall-a/pri/stby#(config-if)#no shutdown
firewall-a/pri/stby#(config)#exit
firewall-a/pri/stby#
```

```
firewall-b/sec/act#conf t
firewall-b/sec/act#(config)#interface Port-channel1
firewall-b/sec/act#(config-if)#no shutdown
firewall-b/sec/act#(config)#exit
firewall-b/sec/act#
```

6. Configuratie opslaan. Schrijf geheugen op de secundaire/actieve firewall en zorg ervoor dat de failover LAN unit secundair in de opstartconfiguratie is.

Voorbeeld:

```
firewall-b/sec/act# write memory
Building configuration...
Cryptoschecksum: ad317407 935a773c 6c5fb66a c5edc342

64509 bytes copied in 9.290 secs (7167 bytes/sec)
[OK]
firewall-b/sec/act# show start | inc unit
failover lan unit secondary
firewall-b/sec/act#
```

7. Configuratie van failover-opdrachten.

1. Op de secundaire/actieve firewall moet u eerst de primaire opdracht van de failover LAN unit instellen om er zeker van te zijn dat de actieve configuratie van de secundaire/actieve firewall naar de nieuwe primaire/stand-by firewall wordt geduwd.

Voorbeeld:

```
firewall-b/sec/act# sh run | inc unit
failover lan unit secondary
firewall-b/sec/act#
```

```
firewall-b/sec/act#conf t
firewall-b/sec/act#(config)#failover lan unit primary
firewall-b/sec/act#(config)#exit
firewall-b/sec/act# sh run | inc unit
```

```
failover lan unit primary
firewall-b/pri/act#
```

b. Valideer de failover-configuratie op beide apparaten. Voorbeeld:

```
firewall-b/pri/act# sh run | inc fail
failover
failover lan unit primary
failover lan interface sync Port-channel1
failover link sync Port-channel1
failover interface ip sync 10.10.13.9 255.255.255.252 standby 10.10.13.10
no failover wait-disable
firewall-b/pri/act#
```

```
firewall-a/sec/stby# sh run | inc fail
no failover
failover lan unit secondary
failover lan interface sync Port-channel1
failover link sync Port-channel1
failover interface ip sync 10.10.13.9 255.255.255.252 standby 10.10.13.10
no failover wait-disable
firewall-a/sec/stby#
```

8. Schakel failover in op de nieuwe primaire firewall. Voorbeeld:

```
firewall-a/sec/stby#conf t
firewall-a/sec/stby#(config)#failover
firewall-a/sec/stby#(config)#exit
firewall-a/sec/stby#
```

```
firewall-a/sec/stby# sh run | inc fail
failover
firewall-a/sec/stby#
```

9. Wacht tot de actieve configuratie op de nieuwe eenheid is gesynchroniseerd en bevestig de juiste failover-status. Voorbeeld:

```
firewall-b/pri/act#
Beginning configuration replication: Sending to mate.
End Configuration Replication to mate
firewall-b/pri/act#
firewall-a/sec/stby#
Beginning configuration replication from mate.
End configuration replication from mate.
firewall-a/sec/stby#
```




Opmerking: Merk op dat de primaire firewall (firewall-b) de configuratie naar de secundaire firewall (firewall-a) stuurt. Schrijf geen geheugen op de nu primaire/actieve firewall (firewall-b).

-
10. Herlaad de nu primaire/actieve firewall (firewall-b) zodat deze weer wordt opgestart als de secundaire/stand-by firewall.

`firewall-b/pri/act#reload`

11. Direct nadat u de opdracht "firewall-b reload" hebt uitgevoerd (wacht 15 seconden), switch u naar de nieuwe Primary Firewall (firewall-a) en voer u de opdracht "failover LAN unit primary" in, gevolgd door schrijfgeheugen.

`firewall-a/sec/act#conf t`

```
firewall-a/sec/act#(config)#failover lan unit primary
firewall-a/sec/act#(config)#exit
firewall-a/sec/act# sh run | inc unit
failover lan unit primary
firewall-a/pri/act# write memory
Building configuration...
Cryptochecksum: ad317407 935a773c 6c5fb66a c5edc342
```

64509 bytes copied in 9.290 secs (7167 bytes/sec)

[OK]

```
firewall-a/pri/act# show start | inc unit
failover lan unit primary
firewall-a/pri/act#
```

12. Wacht tot firewall-b volledig is opgestart en voeg het failover-paar toe als secundair/stand-by. Voorbeeld:

```
firewall-a/pri/act#
Beginning configuration replication: Sending to mate.
End Configuration Replication to mate
firewall-a/pri/act#
firewall-b/sec/stby#
Beginning configuration replication from mate.
End configuration replication from mate.
firewall-b/sec/stby#
```

Opmerking: houd er rekening mee dat de primaire firewall (firewall-a) de configuratie naar de secundaire firewall (firewall-b) stuurt.

13. Sla configuratie op, schrijf geheugen op de primaire/actieve, en valideer het schrijfgeheugen op de nieuwe secundaire/stand-by. Voorbeeld:

```
firewall-a/pri/act#write memory
Building configuration...
Cryptochecksum: ad317407 935a773c 6c5fb66a c5edc342
```

```
64509 bytes copied in 9.290 secs (7167 bytes/sec)
```

```
[OK]
```

```
firewall-a/pri/act#
```

```
firewall-b/sec/stby#
```

```
May 24 2023 15:16:21 firewall-b : %ASA-5-111001: Begin configuration: console writing to memory
```

```
May 24 2023 15:16:22 firewall-b : %ASA-5-111004: console end configuration: OK
```

```
May 24 2023 15:16:22 firewall-b : %ASA-5-111008: User 'failover' executed the 'write memory' command.
```

May 24 2023 15:16:22 firewall-b : %ASA-5-111010: User 'failover', running 'N/A' from IP x.x.x.x , executed 'write memory'
firewall-b/sec/stby#

14. Valideren dat het failover-paar op beide firewalls actief is. Voorbeeld:

```
firewall-a/pri/act# show failover
```

```
Failover On
Failover unit Primary
Failover LAN Interface: sync Port-channel1 (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 0 of 1292 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.12(4)56, Mate 9.12(4)56
Serial Number: Ours JADSERIAL1, Mate JADSERIAL2
Last Failover at: 19:54:29 GMT May 23 2023
  This host: Primary - Active
    Active time: 71564 (sec)
    slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
      Interface inside (10.0.0.1): Normal (Not-Monitored)
      Interface outside (10.1.1.1): Normal (Not-Monitored)
      Interface management (10.2.2.1): Normal (Not-Monitored)
  Other host: Secondary - Standby Ready
    Active time: 0 (sec)
    slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
      Interface inside (10.0.0.2): Normal (Not-Monitored)
      Interface outside (10.1.1.2): Normal (Not-Monitored)
      Interface management (10.2.2.2): Normal (Not-Monitored)
```

```
firewall-b/sec/stby# show failover
```

```
Failover On
Failover unit Secondary
Failover LAN Interface: sync Port-channel1 (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 0 of 1292 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.12(4)56, Mate 9.12(4)56
Serial Number: Ours JADSERIAL2, Mate JADSERIAL1
Last Failover at: 20:51:27 GMT May 23 2023
  This host: Secondary - Standby Ready
    Active time: 0 (sec)
    slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
      Interface inside (10.0.0.2): Normal (Not-Monitored)
      Interface outside (10.1.1.2): Normal (Not-Monitored)
      Interface management (10.2.2.2): Normal (Not-Monitored)
  Other host: Primary - Active
    Active time: 71635 (sec)
    slot 0: FPR-2110 hw/sw rev (49.46/9.12(4)56) status (Up Sys)
      Interface inside (10.0.0.1): Normal (Not-Monitored)
      Interface outside (10.1.1.1): Normal (Not-Monitored)
```

Interface management (10.2.2.1): Normal (Not-Monitored)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.