

# ASA actieve/actieve failover configureren in FirePOWER 4100 Series

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Mechanisme van ASA actieve/actieve failover](#)

[Traffic Flow](#)

[Traffic Flow Condition 1](#)

[Traffic Flow Condition 2](#)

[Traffic Flow Condition 3](#)

[Traffic Flow Condition 4](#)

[Selectieregels voor Active/stand-by](#)

[Netwerkdigram](#)

[Configuratie](#)

[Stap 1. Interfaces vooraf configureren](#)

[Stap 2. Configuratie op primaire eenheid](#)

[Stap 3. Configuratie op secundaire eenheid](#)

[Stap 4. Bevestig failover-status na voltooiing van synchronisatie met succes](#)

[Verifiëren](#)

[Stap 1. Start FTP-verbinding van Win10-01 naar Win10-02](#)

[Stap 2. Bevestig FTP-verbinding voor failover](#)

[Stap 3. LinkDOWN E1/1 van primaire eenheid](#)

[Stap 4. Bevestig de failoverstatus](#)

[Stap 5. Bevestig FTP-verbinding na failover](#)

[Stap 6. Gedrag van pre-empt tijd bevestigen](#)

[Virtueel MAC-adres](#)

[Handmatige instelling van virtueel MAC-adres](#)

[Automatisch instellen van virtueel MAC-adres](#)

[Standaardinstelling van virtueel MAC-adres](#)

[Upgraden](#)

[Gerelateerde informatie](#)

---

## Inleiding

Dit document beschrijft hoe u actieve/actieve failover kunt configureren in Cisco Firepower 4145 NGFW applicatie.

# Voorwaarden

## Vereisten

Cisco raadt u aan bekend te zijn met dit onderwerp:

- Active/stand-by failover in Cisco adaptieve security applicatie (ASA).

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco FirePOWER 4145 NGFW-applicatie (ASA) 9.18(3)56
- Firepower eXtensible Operating System (FXOS) 2.12(0.498)
- Windows 10

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie

Active/Active failover is alleen beschikbaar voor security applicaties die in meerdere contextmodi werken. In deze modus is de ASA logisch onderverdeeld in meerdere virtuele apparaten, contexten genoemd. Elke context werkt als een onafhankelijk apparaat, met een eigen beveiligingsbeleid, interfaces en beheerders.

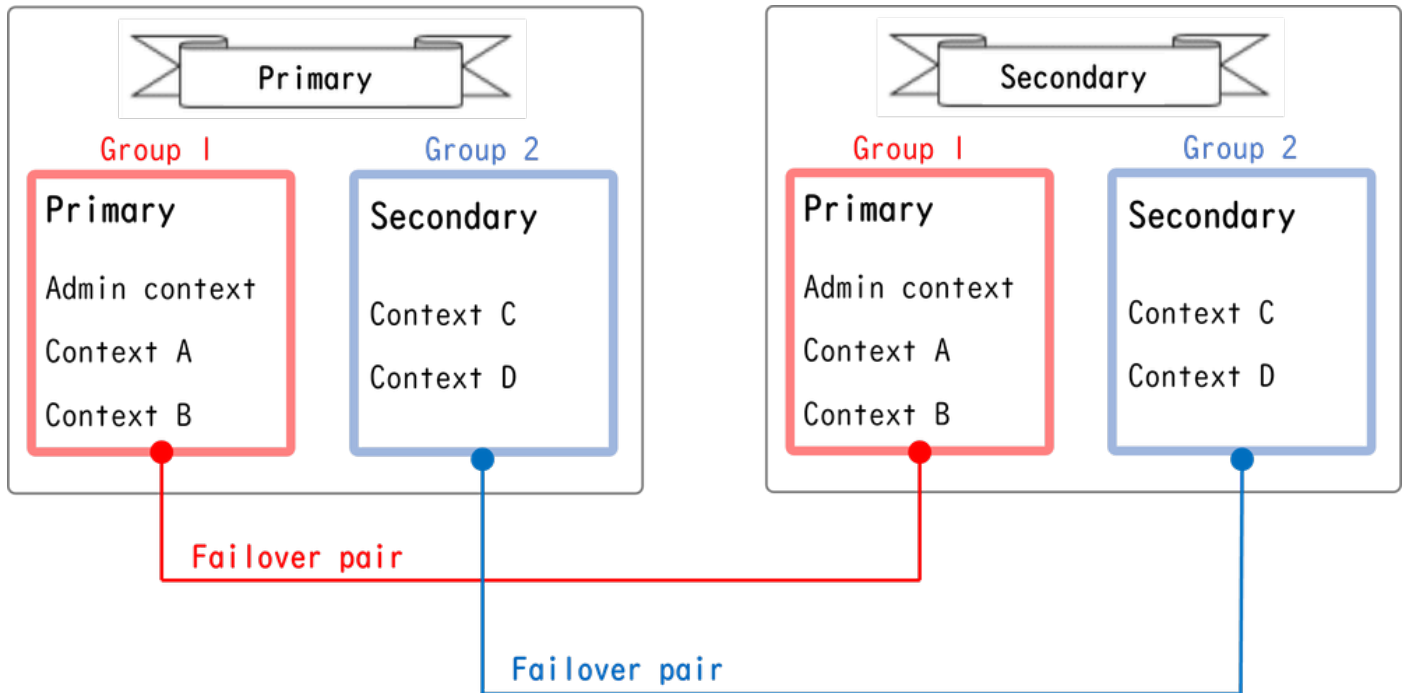
De Active/Active failover is een functie van Adaptieve security applicatie (ASA) die twee FirePOWER-apparaten in staat stelt om het verkeer tegelijkertijd over te gaan. Deze configuratie wordt doorgaans gebruikt voor een taakverdelingsscenario waarin u het verkeer tussen twee apparaten wilt splitsen om de doorvoersnelheid te maximaliseren. Het wordt ook gebruikt voor redundantiedoelinden, zodat als één ASA faalt, de andere kan overnemen zonder een verstoring in de dienst te veroorzaken.

## Mechanisme van ASA actieve/actieve failover

Elke context in Active/Active failover wordt handmatig toegewezen aan groep 1 of groep 2. De Admin-context wordt standaard aan groep 1 toegewezen. Dezelfde groep (groep1 of groep2) in de twee chassis(eenheden) vormen een failover-paar dat de redundantiefunctie realiseert. Het gedrag van elk failover-paar is in principe hetzelfde als het gedrag in een Active/Standby failover. Raadpleeg [Active/stand-by failover configureren](#) voor meer informatie over Active/[stand-by failover](#). Bij actief/actief failover heeft elke groep naast de rol (primair of secundair) van elk chassis ook een rol (primair of secundair). Deze Rollen worden handmatig vooraf ingesteld door de gebruiker en worden gebruikt om de High Availability (HA)-status (Active of Standby) te bepalen

voor elke failover-groep.

De Admin Context is een speciale context die basischassisbeheerverbinding (zoals SSH) behandelt. Dit is een beeld van Active/Active failover.



failover-paar in active/active failover

## Traffic Flow

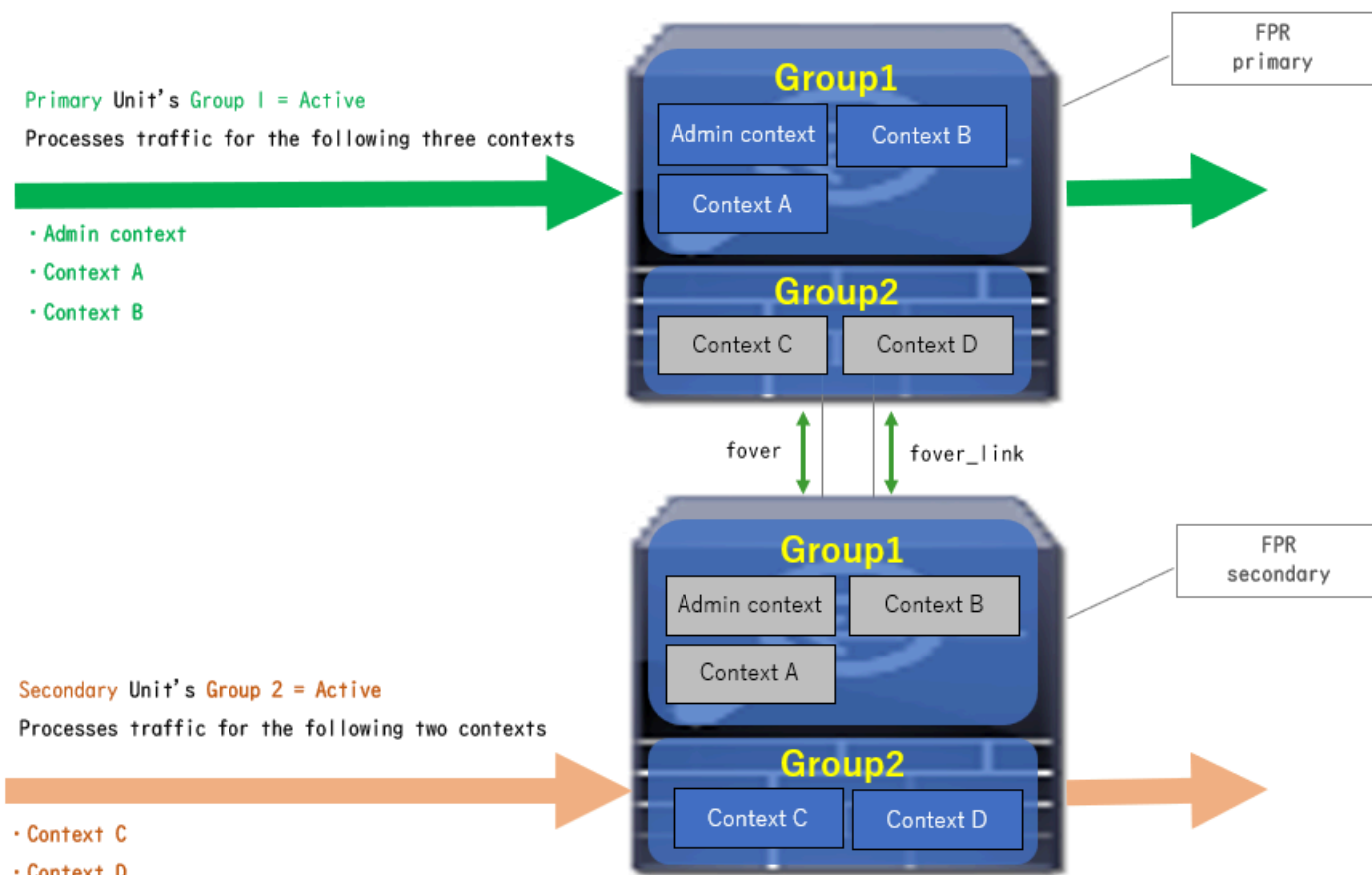
In Active/Active failover kan verkeer in de verschillende patronen worden verwerkt zoals in het volgende beeld wordt getoond.

Group	Primary Unit	Secondary Unit	
Group 1	Active	Standby	Both of ASAs process traffic simultaneously
Group 2	Standby	Active	
Group 1	Active	Standby	Only the Primary Unit processes traffic
Group 2	Active	Standby	
Group 1	Standby	Active	Both of ASAs process traffic simultaneously
Group 2	Active	Standby	
Group 1	Standby	Active	Only the Secondary Unit processes traffic
Group 2	Standby	Active	

Traffic Flow

### Traffic Flow Condition 1

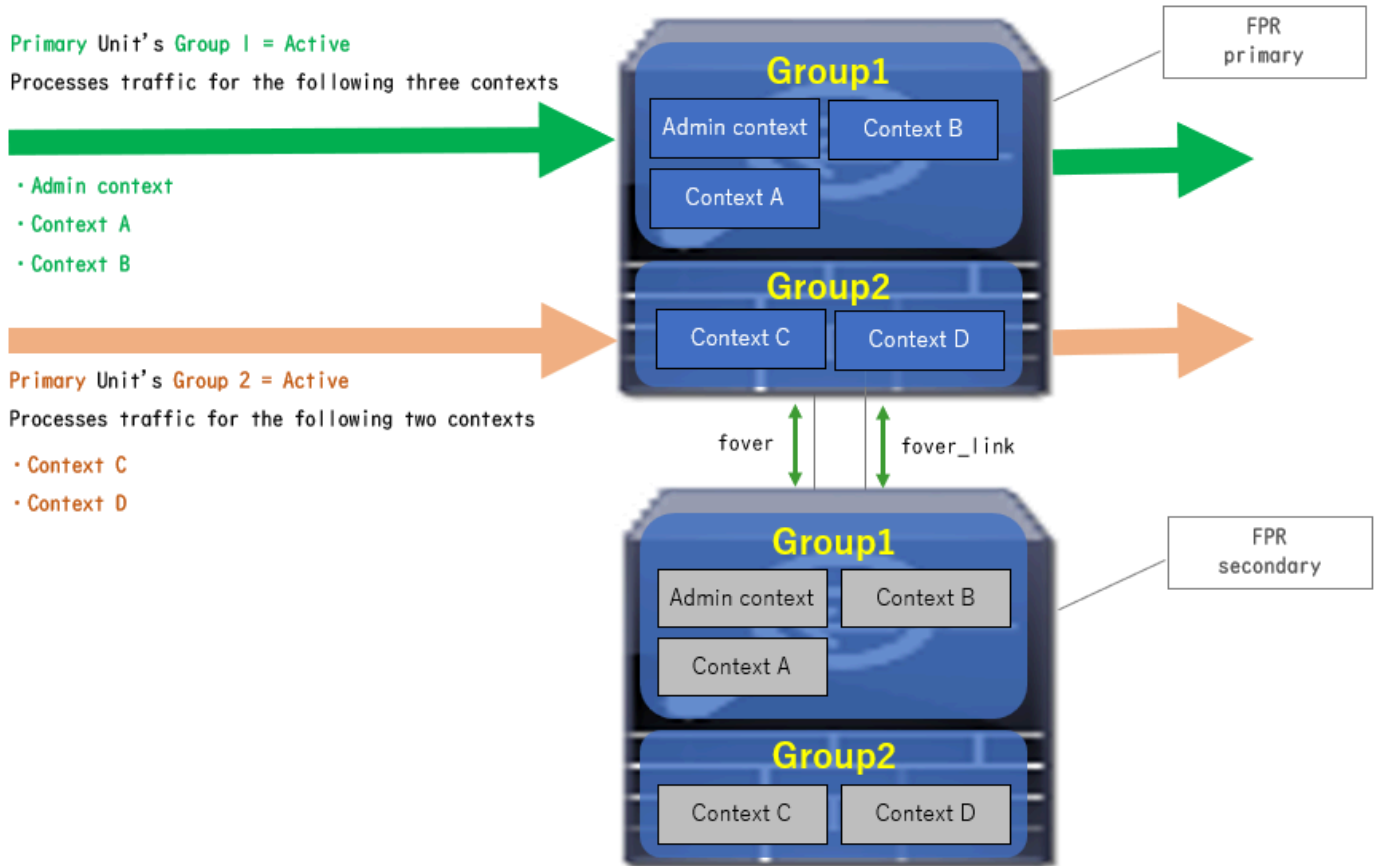
- Primaire eenheid: groep 1 = actief, groep 2 = stand-by
- Secundaire eenheid: Groep 1 = Standby, Groep 2 = Actief



Traffic Flow Condition 1

## Traffic Flow Condition 2

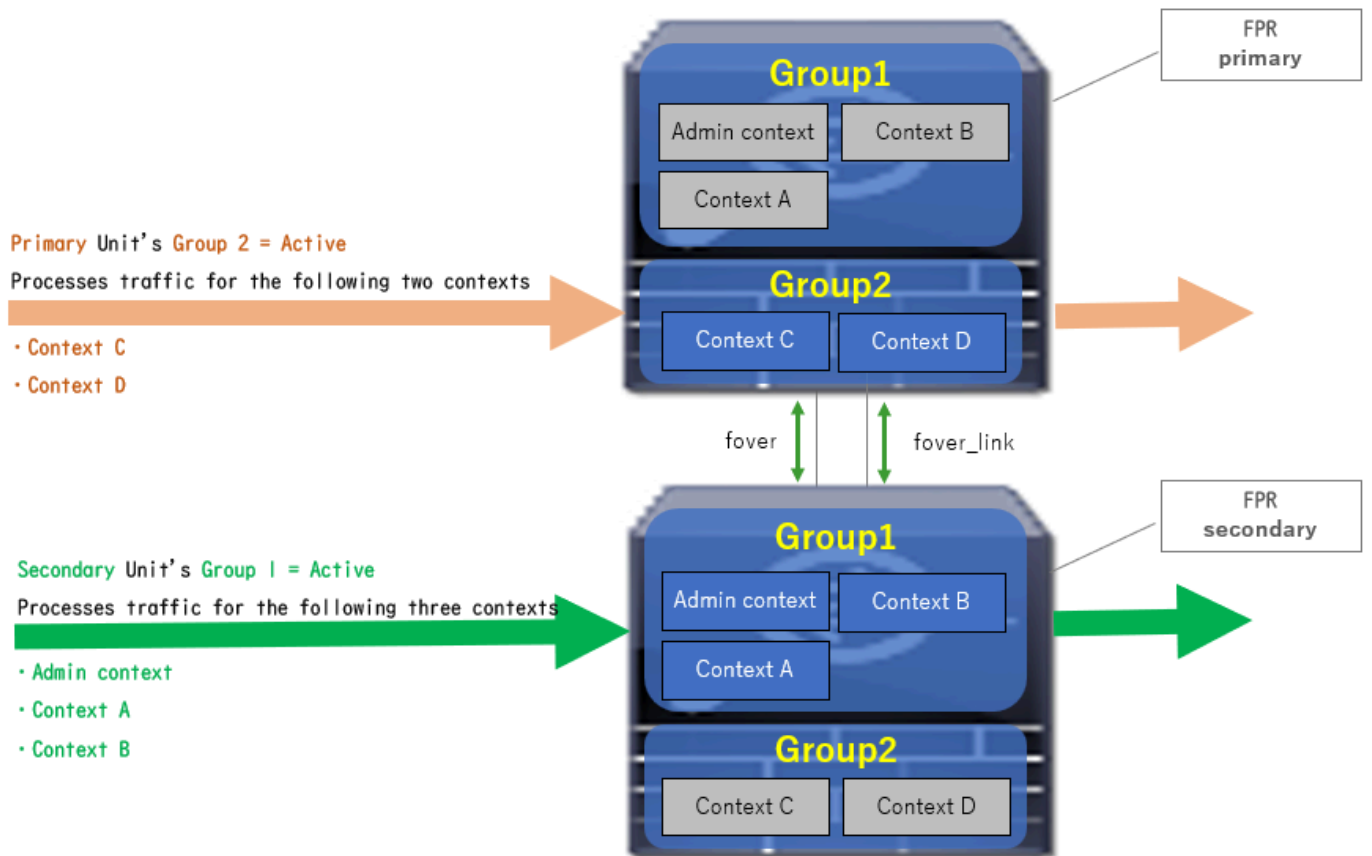
- Primaire eenheid: groep 1 = actief, groep 2 = actief
- Secundaire eenheid: groep 1 = Standby, groep 2 = Standby



Traffic Flow Condition 2

### Traffic Flow Condition 3

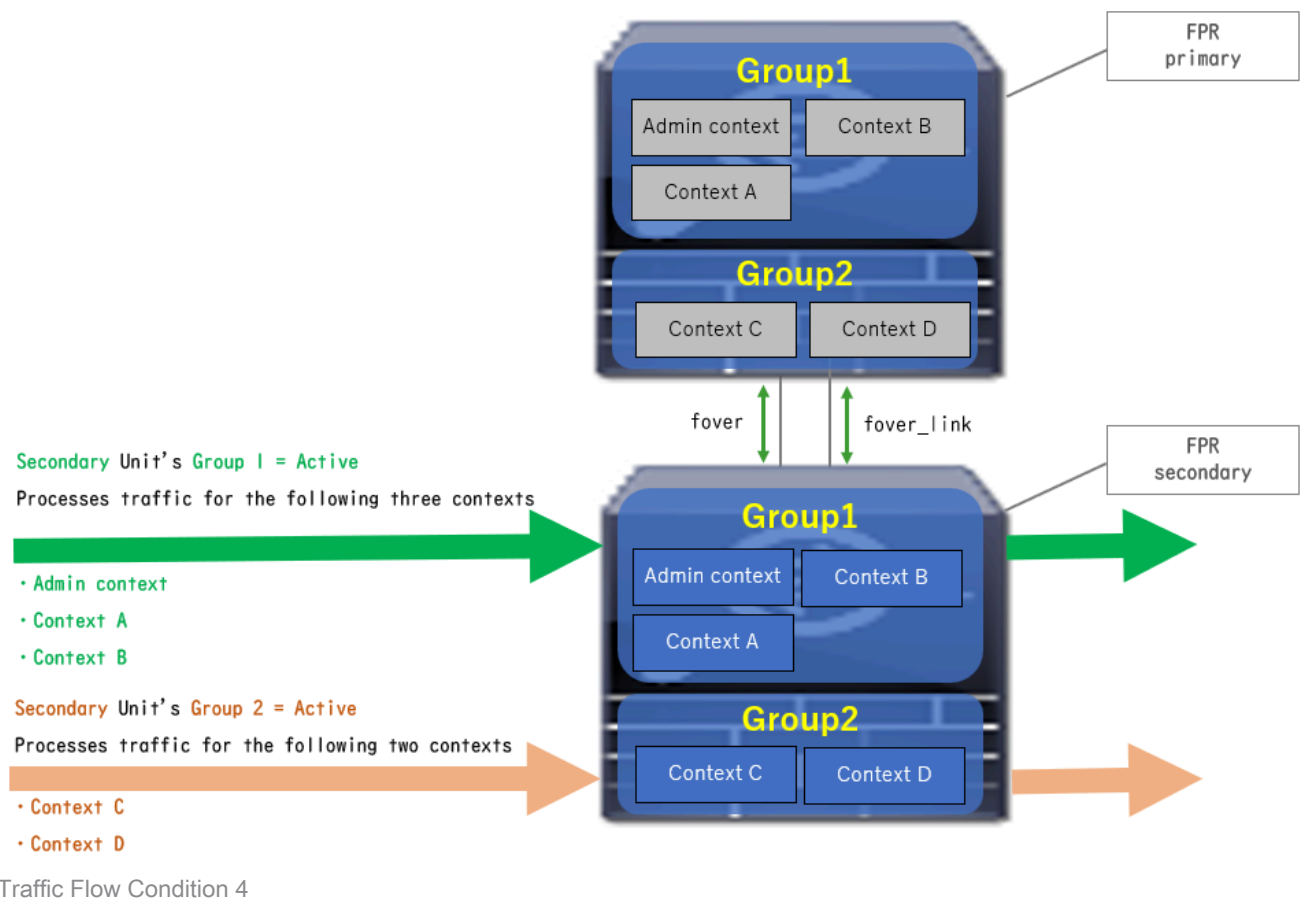
- Primaire eenheid: groep 1 = stand-by, groep 2 = actief
- Secundaire eenheid: groep 1 = actief, groep 2 = stand-by



Traffic Flow Condition 3

#### Traffic Flow Condition 4

- Primaire eenheid: groep 1 = standby, groep 2 = standby
- Secundaire eenheid: groep 1 = actief, groep 2 = actief



## Selectieregels voor Active/stand-by

Bij Active/Active failover wordt de status (active/stand-by) van elke groep bepaald door deze regels:

- Stel dat 2 apparaten bijna tegelijkertijd opstarten, dan wordt een van de eenheden (primair of secundair) eerst actief.
- Na het verstrijken van de voorafgaande tijd wordt de groep die in het chassis en de groep dezelfde rol speelt, actief.
- Wanneer er een failover-gebeurtenis (zoals interface DOWN) is, verandert de status van de groep op dezelfde manier als met Active/Standby failover.
- De voorbereidingstijd werkt niet na het handmatig overdoen van failover.

Dit is een voorbeeld van de statuswijziging.

- Beide apparaten starten bijna tegelijkertijd op. Status A →
- Preempt time is voorbij. Status B →
- Primaire apparaatstoring (failover wordt geactiveerd). Status C →
- Preempt tijd verstreken sinds Primair apparaat herstelde van mislukking. Status D →
- Schakel de failover handmatig in. Status E

Raadpleeg [failover-gebeurtenissen](#) voor informatie over failover-triggers en gezondheidsbewaking.

1. Beide apparaten starten bijna tegelijkertijd op.

Operation	Primary Unit		Secondary Unit	
	Group 1: primary	Group 2: secondary	Group 1: primary	Group 2: secondary
Both devices started simultaneously	Active	Active	Standby	Standby
	or			
	Standby	Standby	Active	Active

Status A

2. Voorlopige tijd (in dit document 30 s) is verstreken.

After 30 seconds (preempt time)	Active	Standby	Standby	Active
---------------------------------	--------	---------	---------	--------

Status B

3. Een storing (zoals Interface Down) trad op in groep 1 van de primaire eenheid.

Failover event	Standby	Standby	Active	Active
----------------	---------	---------	--------	--------

Status C

4. Voorlopige tijd (30 seconden in dit document) verstreken sinds groep 1 van primair apparaat is hersteld van een storing.

After 30 seconds since Primary Unit recovered	Active	Standby	Standby	Active
---	--------	---------	---------	--------

Status D

5. Stel groep 2 van de primaire eenheid handmatig in op Actief.

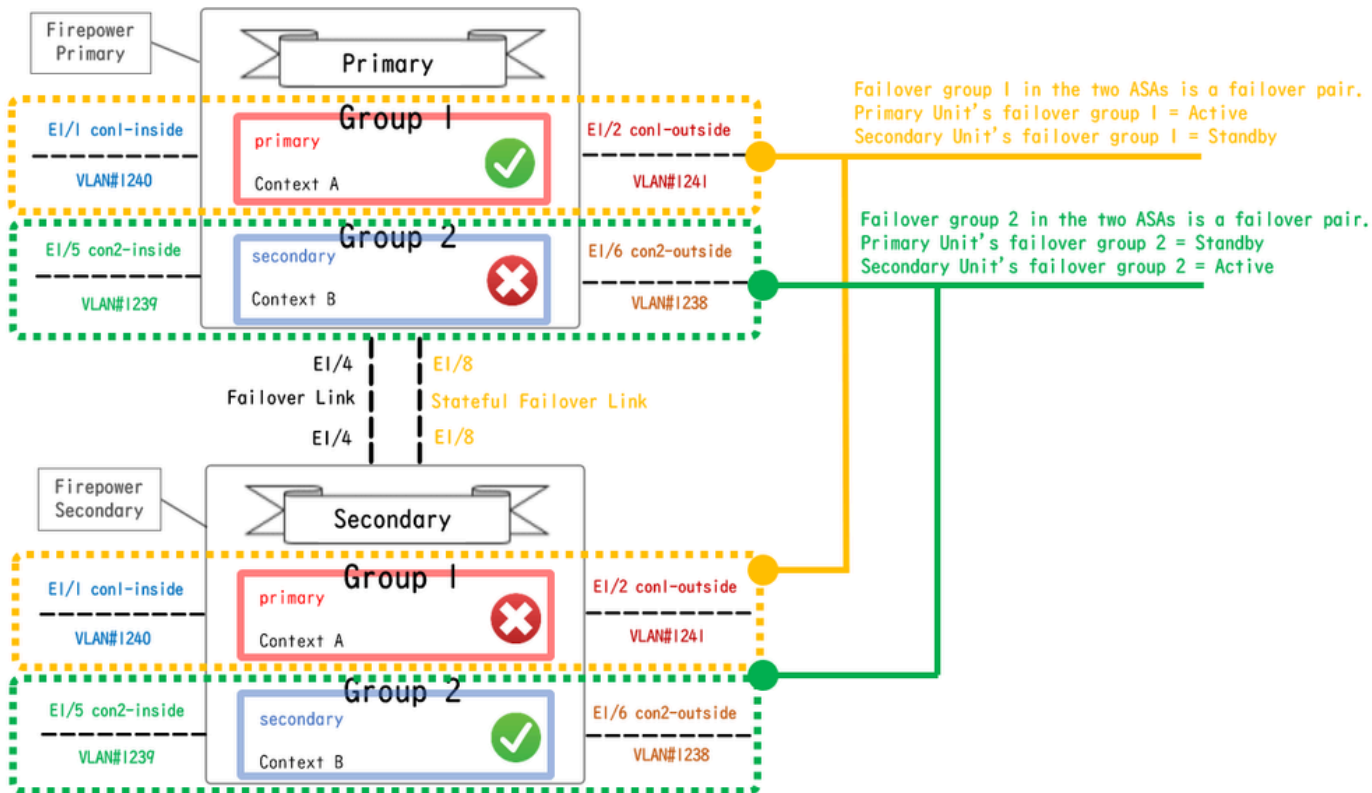
Manual failover	Active	Active	Standby	Standby
-----------------	--------	--------	---------	---------

Status E

## Netwerkdigram

Dit document introduceert de configuratie en verificatie voor Active/Active failover op basis van dit diagram.





Logisch configuratiediagram

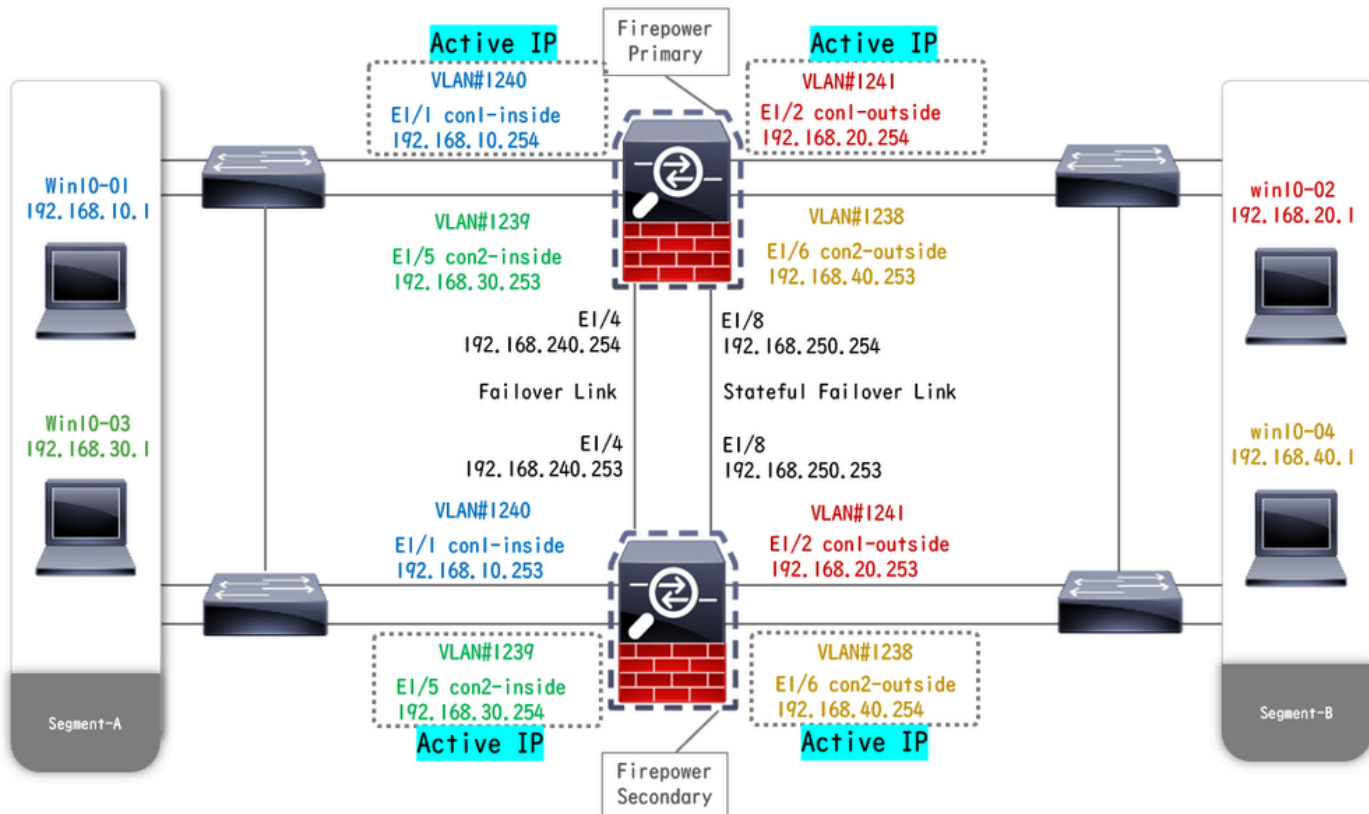
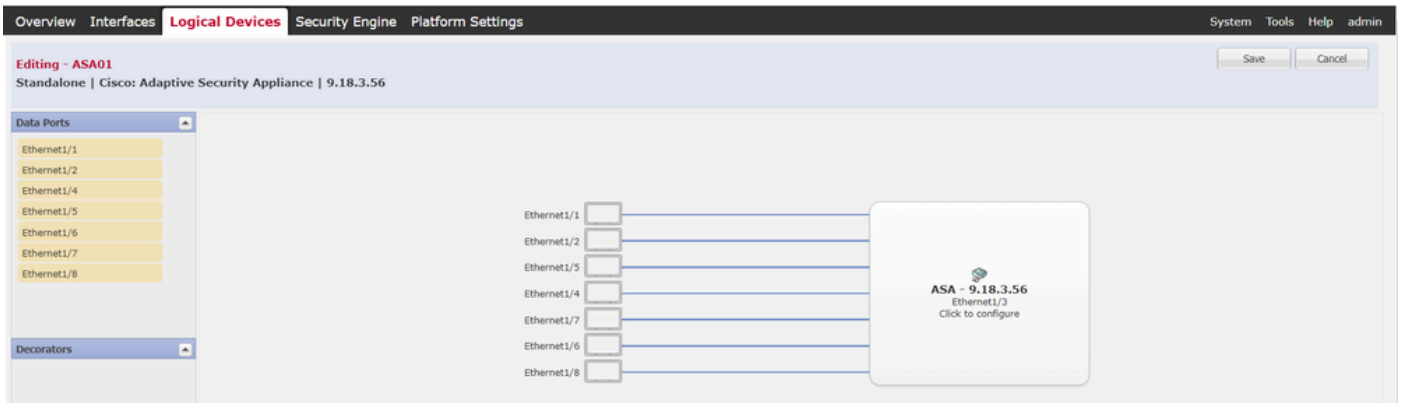


Diagram van fysieke configuratie

## Configuratie

### Stap 1. Interfaces vooraf configureren

Log in op FCM GUI voor beide versies van Firepower. Navigeer naar Logische apparaten > Bewerken. Voeg de gegevensinterface aan ASA toe, zoals in de afbeelding.



Interfaces vooraf configureren

## Stap 2. Configuratie op primaire eenheid

Maak verbinding met de primaire FXOS CLI via SSH of console. Uitvoeren `connect module 1 console` en `connect asa` opdracht geven om ASA CLI te starten.

a. Configuratie van failover op de primaire eenheid (voer de opdracht uit in de systeemcontext van de primaire eenheid).

```
<#root>
```

```
failover lan unit primary failover lan interface fover E1/4 failover link fover_link E1/8 failover interface ip fover 192.168.240.254 255.255.255.0 standby 1
```

```
failover group 1
```

```
group 1 is assigned to primary by default preempt 30 failover group 2 secondary preempt 30 failover
```

b. Configureer de failover-groep voor context (voer de opdracht uit in de systeemcontext van de primaire eenheid).

```
<#root>
```

```
admin-context admin
```

```
context admin
```

```
<--- admin context is assigned to group 1 by default allocate-interface E1/3 config-url disk0:/admin.c
```

```
join-failover-group 1
```

```
<--- add con1 context to group 1 ! context con2 allocate-interface E1/5 allocate-interface E1/6 config
```

```
join-failover-group 2
```

```
<--- add con2 context to group 2
```

c. Draaien changeto context con1 om con1 context van systeemcontext te verbinden. Configureer IP voor interface van de con1 context (voer de opdracht in con1 context van primaire eenheid uit).

```
interface E1/1 nameif con1-inside ip address 192.168.10.254 255.255.255.0 standby 192.168.10.253 security-level 100 no shutdown interface E1/2 nameif
```

d. Uitvoeren changeto context con2 om con2 context te verbinden met systeemcontext. Configureer IP voor interface van de con2 context (voer de opdracht uit in con2 context van Primaire eenheid).

```
interface E1/5 nameif con2-inside ip address 192.168.30.254 255.255.255.0 standby 192.168.30.253 security-level 100 no shutdown interface E1/6 nameif
```

### Stap 3. Configuratie op secundaire eenheid

a. Verbinding maken met de secundaire FXOS CLI via SSH of console. Configuratie van failover op de secundaire eenheid (voer de opdracht uit in systeemcontext van de secundaire eenheid).

```
failover lan unit secondary failover lan interface fover E1/4 failover link fover_link E1/8 failover interface ip fover 192.168.240.254 255.255.255.0 standby
```

failover b. Start de opdracht (uitgevoerd in systeemcontext van de secundaire eenheid).

failover

### Stap 4. Bevestig failover-status na voltooiing van synchronisatie met succes

a. Uitvoeren show failover in systeemcontext van secundaire eenheid.

```
<#root>
```

```
asa#
```

```
show failover
```

```
Failover On Failover unit Secondary Failover LAN Interface: fover Ethernet1/4 (up) Version: Ours 9.18(
```

```
Secondary
```

```
<--- group 1 and group 2 are Standby status in Secondary Unit Group 1 State:
```

```
Standby Ready
```

Active time: 0 (sec) Group 2 State:

Standby Ready

Active time: 945 (sec) con1 Interface con1-inside (192.168.10.253): Unknown (Waiting) con1 Interface c

Primary

<--- group 1 and group 2 are Active status in Primary Unit Group 1 State:

Active

Active time: 1637 (sec) Group 2 State:

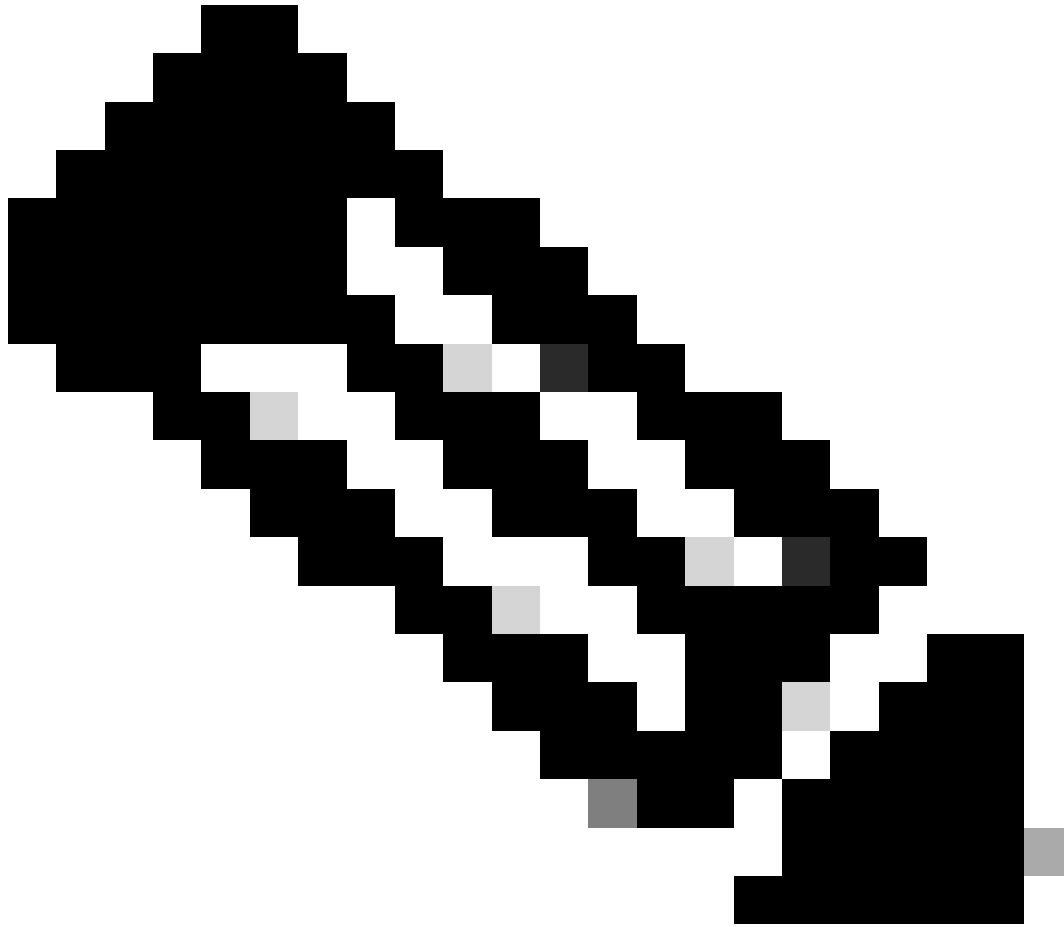
Active

Active time: 93 (sec) con1 Interface con1-inside (192.168.10.254): Normal (Monitored) con1 Interface c

b. (optioneel) Voer de **no failover active group 2** opdracht Uitvoeren uit om groep 2 van de primaire switch handmatig uit te voeren naar de stand-by status (uitgevoerd in systeemcontext van de primaire eenheid). Dit kan de verkeersbelasting door firewall verdelen.

<#root>

no failover active group 2

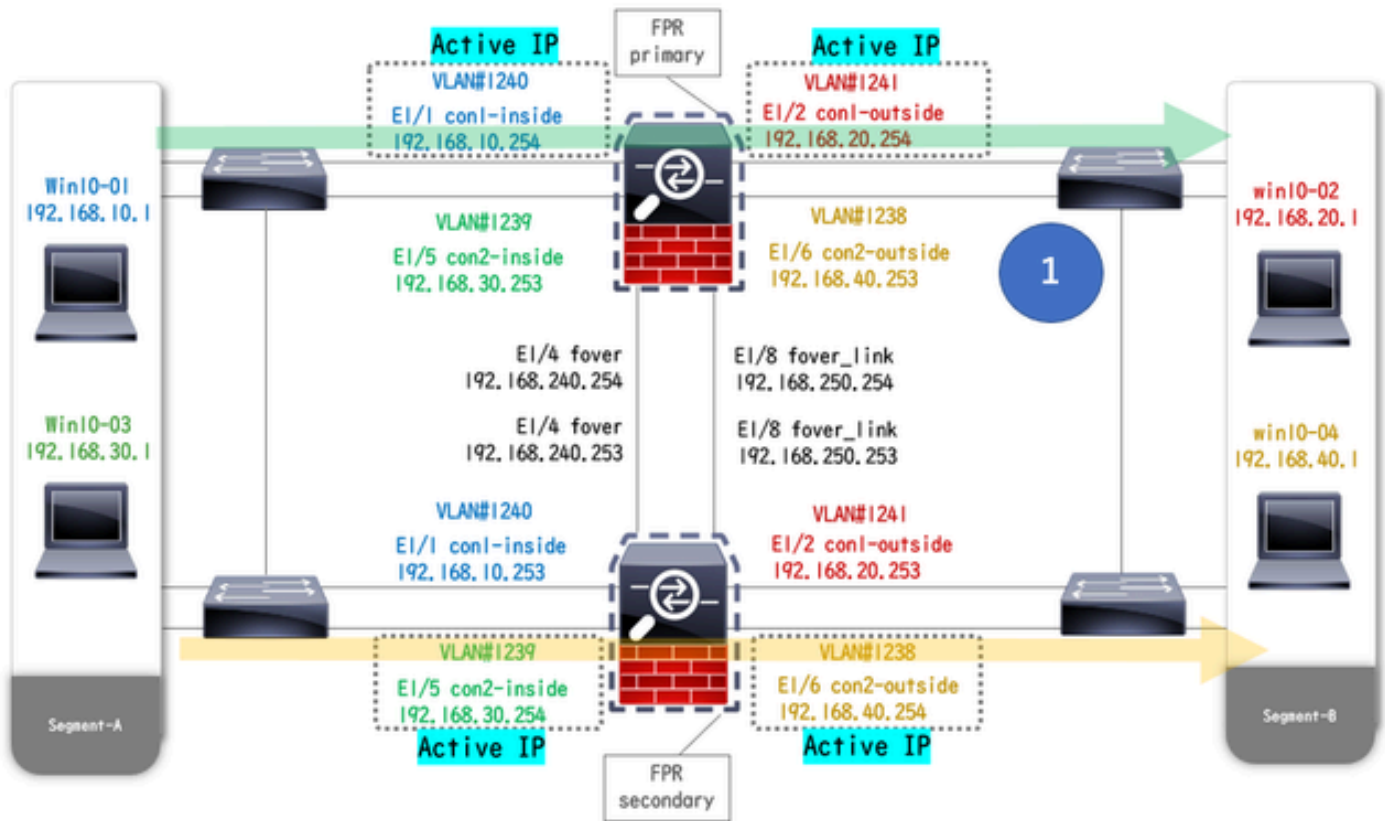


**Opmerking:** als u deze opdracht uitvoert, komt de status van failover overeen met traffic flow voorwaarde 1.

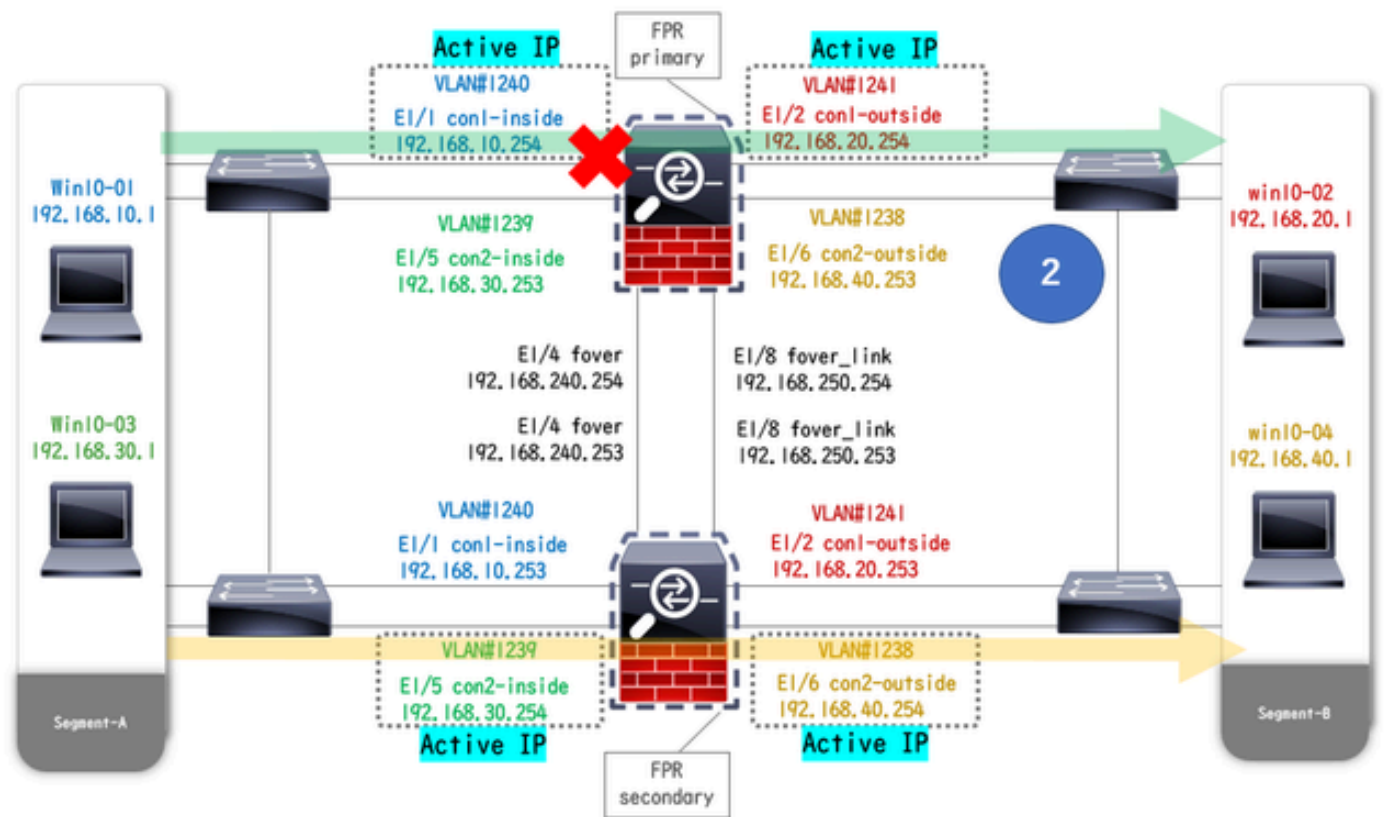
---

Verifiëren

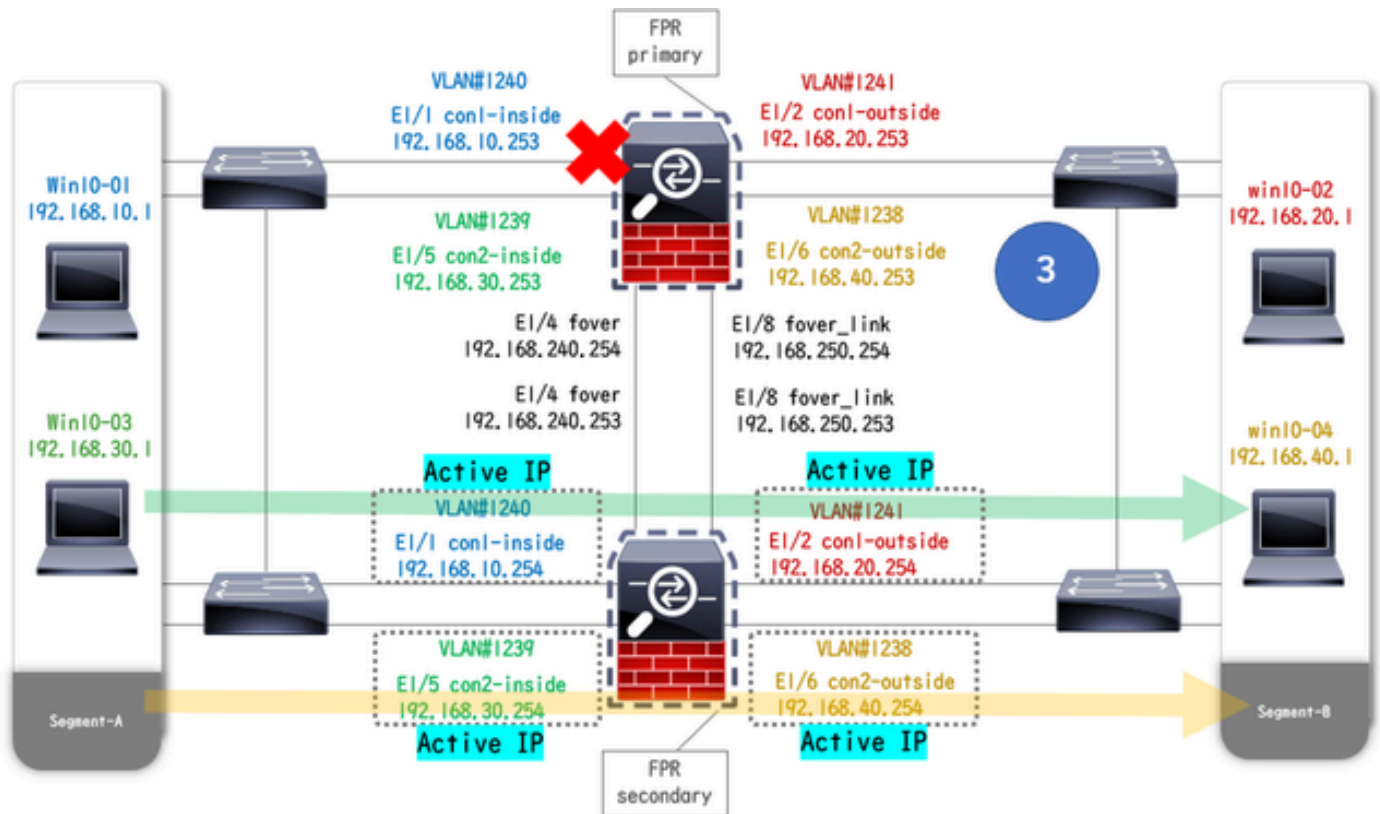
Wanneer E1/1 omlaag gaat, wordt de failover van groep 1 geactiveerd en nemen de gegevensinterfaces aan de Standby-kant (Secundaire Eenheid) het IP- en MAC-adres van de oorspronkelijke actieve interface over, waardoor het verkeer (FTP-verbinding in dit document) continu door ASA's wordt doorgegeven.



Voor link



omlaag tijdens link omlaag



*Uitgeschakeld failover*

Stap 1. Start FTP-verbinding van Win10-01 naar Win10-02

Stap 2. Bevestig FTP-verbinding voor failover

Draai changeto context con1 om con1 context te verbinden van systeemcontext. Bevestig dat in beide ASA-eenheden een FTP-verbinding is gemaakt.

```
<#root>
```

```
asa/act/pri/con1#
```

```
show conn
```

```
5 in use, 11 most used
! --- Confirm the connection in Primary Unit TCP
```

```
con1-outside
```

```
192.168.20.1:21
```

```
con1-inside 192.168.10.1:49703
```

```
, idle 0:00:11, bytes 528, flags UI0 asa/stby/sec/con1#
```

```
show conn
```

```
5 in use, 11 most used
! --- Confirm the connection in Secondary Unit TCP
```

con1-outside 192.168.20.1:21 con1-inside 192.168.10.1:49703

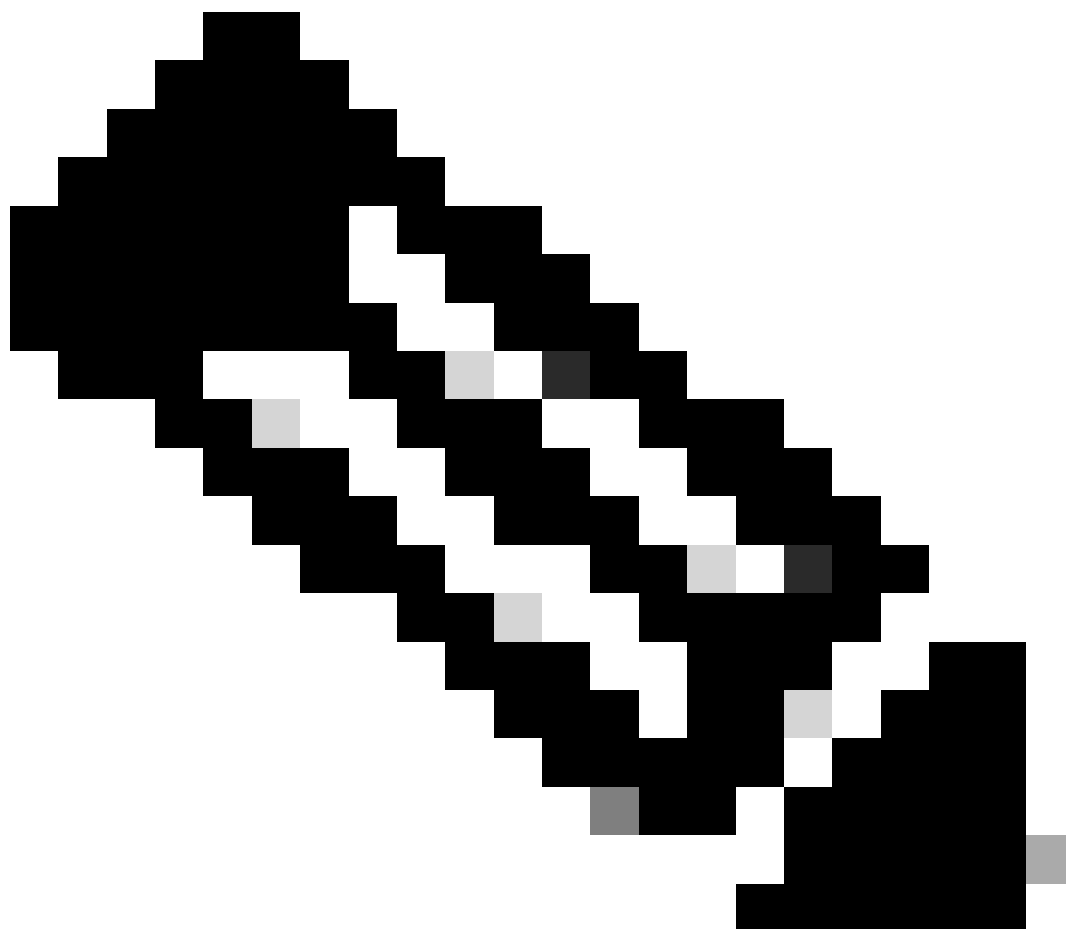
, idle 0:00:14, bytes 528, flags UIO

Stap 3. LinkDOWN E1/1 van primaire eenheid

Stap 4. Bevestig de failoverstatus

Bevestig in systeemcontext dat failover optreedt in groep 1.

---



**Opmerking:** de status van failover komt overeen met verkeersstroomvoorwaarde 4.

---



<#root>

asa/act/sec#

show failover

Failover On Failover unit Secondary Failover LAN Interface: fover Ethernet1/4 (up) ..... Group 1 last  
Secondary

Group 1 State:

Active

<--- group 1 of Secondary Unit is Switching to Active Active time: 5 (sec) Group 2 State:

Active

Active time: 10663 (sec) con1 Interface con1-inside (192.168.10.254): Normal (Waiting) con1 Interface

Primary

Group 1 State:

Failed

<--- group 1 of Primary Unit is Switching to Failed status Active time: 434 (sec) Group 2 State:

Standby Ready

Active time: 117 (sec) con1 Interface con1-inside (192.168.10.253): Failed (Waiting) con1 Interface co

Stap 5. Bevestig FTP-verbinding na failover

Draai changeto context con1 om con1 context van systeemcontext te verbinden, bevestig dat de FTP-verbinding niet wordt onderbroken.

<#root>

asa/act/sec#

changeneto context con1

asa/act/sec/con1# show conn 11 in use, 11 most used

! --- Confirm the target FTP connection exists in group 1 of the Secondary Unit TCP

con1-outside 192.168.20.1:21 con1-inside 192.168.10.1:49703

, idle 0:00:09, bytes 529, flags UIO

Stap 6. Gedrag van pre-empt tijd bevestigen

LinkUP E1/1 van de primaire eenheid en wacht 30 s (pre-empt tijd), de failover staat keert terug naar de originele staat (de stroom van het overeenkomende verkeer in patroon 1).

<#root>

asa/stby/pri#

### Group 1 preempt mate

□□□□<--- Failover is triggered automatically, after the preempt time has passed asa/act/pri# show fail

### Primary

Group 1 State:

### Active

<--- group 1 of Primary Unit is switching to Active status Active time: 34 (sec) Group 2 State:

### Standby Ready

Active time: 117 (sec) con1 Interface con1-inside (192.168.10.254): Normal (Monitored) con1 Interface

### Secondary

Group 1 State:

### Standby Ready

□□<---- group 1 of Secondary Unit is switching to Standby status Active time: 125 (sec) Group 2 State:

### Active

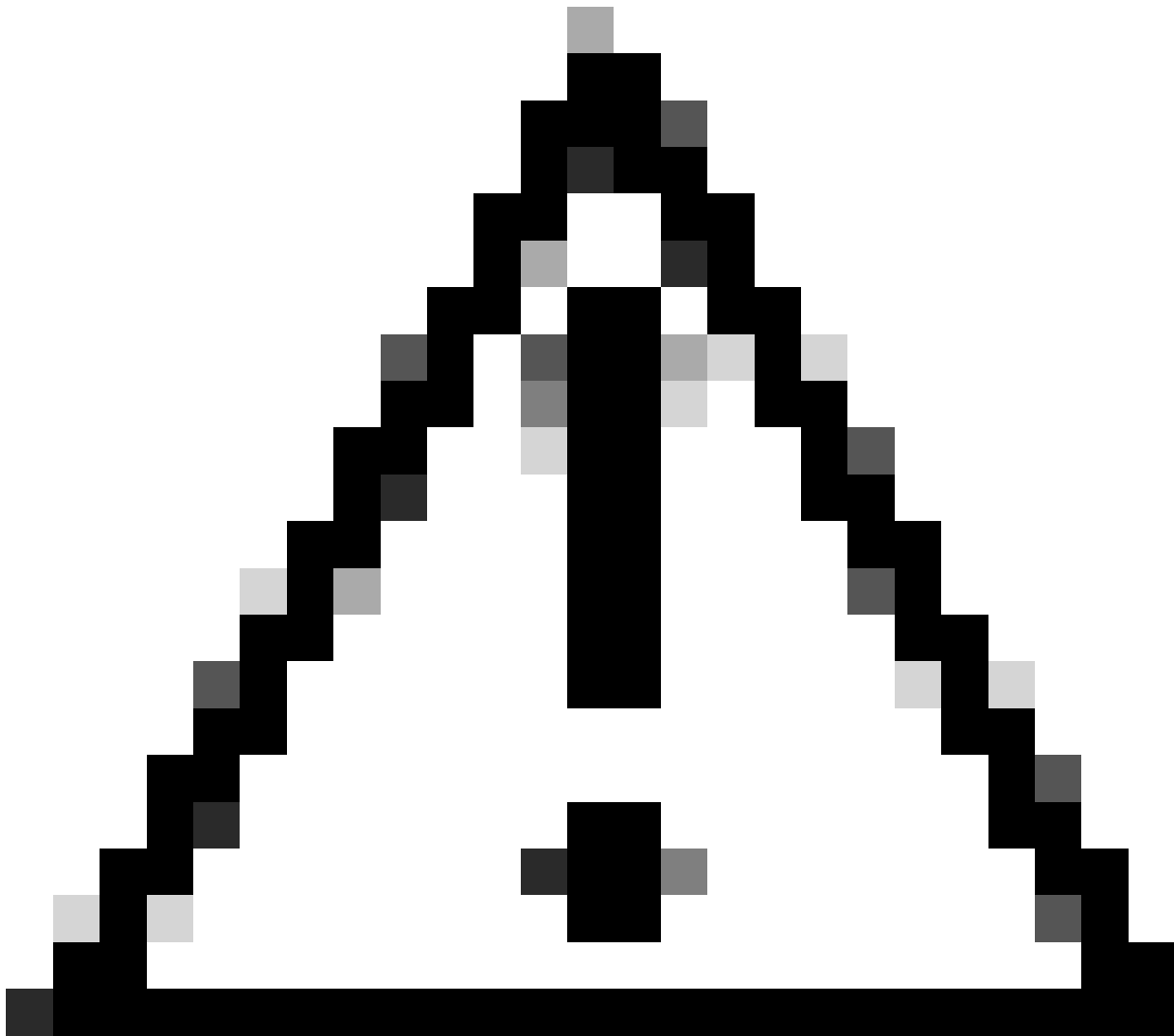
Active time: 10816 (sec) con1 Interface con1-inside (192.168.10.253): Normal (Monitored) con1 Interface

### Virtueel MAC-adres

In Active/Active failover wordt altijd een virtueel MAC-adres (handmatig ingestelde waarde, of automatisch gegenereerde waarde, of standaardwaarde) gebruikt. Het actieve virtuele adres van MAC wordt geassocieerd met de Actieve Interface.

### Handmatige instelling van virtueel MAC-adres

mac address Om het virtuele MAC-adres voor fysieke interfaces handmatig in te stellen, kan de opdracht of de mac-address opdracht (binnen de I/F-instellingsmodus) worden gebruikt. Dit is een voorbeeld van het handmatig instellen van een virtueel MAC-adres voor de fysieke interface E1/1.



**Waarschuwing:** gebruik deze twee typen opdrachten niet binnen hetzelfde apparaat.

---

<#root>

```
asa/act/pri(config)# failover group 1 asa/act/pri(config-fover-group)#
```

```
mac address E1/1 1234.1234.0001 1234.1234.0002
```

```
asa/act/pri(config-fover-group)# changeto context con1 asa/act/pri/con1(config)# show interface E1/1 |
```

```
1234.1234.0001
```

```
, MTU 1500 <--- Checking virtual MAC on the Primary Unit(con1) side asa/stby/sec# changeto context con1
```

```
1234.1234.0002
```

```
, MTU 1500 <--- Checking virtual MAC on the Secondary Unit(con1) side
```

OF

```
<#root>
```

```
asa/act/pri(config)# changeto context con1 asa/act/pri/con1(config)# int E1/1 asa/act/pri/con1(config-if)#
```

```
mac-addr
```

```
1234.1234.0001 standby 1234.1234.0002
```

```
asa/act/pri/con1(config)# show interface E1/1 | in MAC MAC address
```

```
1234.1234.0001
```

```
, MTU 1500 <--- Checking virtual MAC on the Primary Unit(con1) side asa/stby/sec# changeto context con1
```

```
1234.1234.0002
```

```
, MTU 1500<--- Checking virtual MAC on the Secondary Unit(con1) side
```

## Automatisch instellen van virtueel MAC-adres

Het automatisch genereren van een virtueel MAC-adres wordt ook ondersteund. Dit kan worden bereikt met behulp van de `mac-address auto` `<prefix prefix>` opdracht. Het formaat van virtueel MAC-adres is `A2 xx.yzz.zzzz` dat automatisch wordt gegenereerd.

`A2` : vaste waarde

`xx.yy`: gegenereerd door de `<prefix-prefix>` die in de opdracht optie is gespecificeerd (de prefix wordt geconverteerd naar hexadecimaal en vervolgens ingevoegd door de omgekeerde volgorde).

`zz.zzzz` : gegenereerd door een interne teller

Dit is een voorbeeld over het genereren van virtueel MAC-adres door `mac-address auto` opdracht voor interface.

```
<#root>
```

```
asa/act/pri(config)#
```

```
mac-address auto
```

```
INFO: Converted to mac-address auto prefix 31
```

```
asa/act/pri(config)#
```

```
show run all context con1
```

```
<--- Checking the virtual MAC addresses generated on con1 context
allocate-interface Ethernet1/1
mac-address auto Ethernet1/1 a21f.0000.0008 a21f.0000.0009
allocate-interface Ethernet1/2
mac-address auto Ethernet1/2 a21f.0000.000a a21f.0000.000b
config-url disk0:/con1.cfg
join-failover-group 1
```

```
asa/act/pri(config)#
```

```
show run all context con2
```

```
<--- Checking the virtual MAC addresses generated on con2 context
context con2
allocate-interface Ethernet1/5
mac-address auto Ethernet1/5 a21f.0000.000c a21f.0000.000d
allocate-interface Ethernet1/6
mac-address auto Ethernet1/6 a21f.0000.000e a21f.0000.000f
config-url disk0:/con2.cfg
join-failover-group 2
```

## **Standaardinstelling van virtueel MAC-adres**

In het geval dat noch automatische noch handmatige generatie van een virtueel MAC-adres is ingesteld, wordt het standaard virtuele MAC-adres gebruikt.

Raadpleeg voor meer informatie over standaard virtuele MAC-adressen het [Command Default](#) van MAC-adres in de Naslaghandleiding voor Cisco Secure Firewall ASA Series-opdrachten.

## Upgraden

U kunt een upgrade zonder downtime van een Active/Active failover-paar realiseren met CLI of ASDM. Raadpleeg voor meer informatie [Upgrade een actief/actief failover-paar](#).

## Gerelateerde informatie

- [Upgrade een actief/actief failover-paar met de CLI](#)
- [MAC-adres](#)
- [Cisco Technical Support en downloads](#)

## 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.