

FTD Multi-Instance High-Availability instellen op Firepower 4100

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Netwerkdigram](#)

[Configuraties](#)

[Stap 1. Interfaces vooraf configureren](#)

[Stap 2. Voeg 2 resourceprofielen toe voor containerinstanties.](#)

[Stap 3. \(Optioneel\) Voeg een MAC Pool Prefix van virtueel MAC-adres toe voor Container Instance Interfaces.](#)

[Stap 4. Voeg een standalone instantie toe.](#)

[Stap 5. Interfaces configureren](#)

[Stap 6. Voeg een hoog beschikbaarheidspaar toe voor elke instantie.](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Referentie](#)

Inleiding

Dit document beschrijft hoe u failover kunt configureren in FTD-containerinstanties (Multi-Instance).

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van Firepower Management Center en Firewall Threat Defence.

Gebruikte componenten

Cisco Firepower Management Center Virtual 7.2.5

Cisco FirePOWER 4145 NGFW-applicatie (FTD) 7.2.5

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.

Alvorens FTD Multi-Instance te implementeren, is het belangrijk om te begrijpen hoe het uw systeemprestaties kan beïnvloeden en dienovereenkomstig te plannen. Raadpleeg altijd de officiële documentatie van Cisco of neem contact op met een technische vertegenwoordiger van Cisco om een optimale implementatie en configuratie te garanderen.

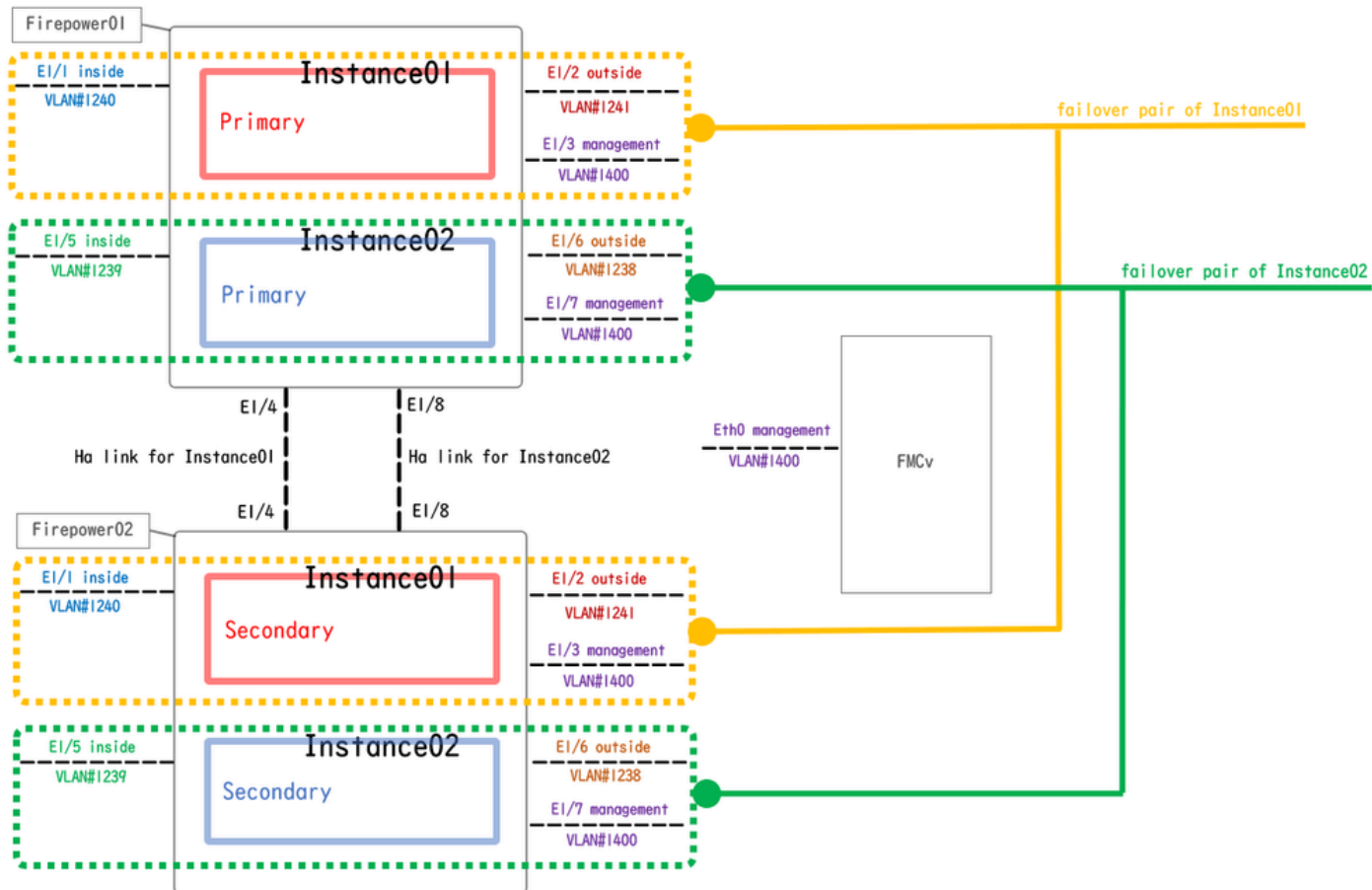
Achtergrondinformatie

Multi-Instance is een functie van Firepower Threat Defence (FTD) die vergelijkbaar is met ASA multiple context mode. Het stelt u in staat om meerdere, aparte container Instanties van FTD op een enkel stuk hardware uit te voeren. Elke container instantie staat voor harde middelen scheiding, afzonderlijk configuratiebeheer, afzonderlijke herladingen, afzonderlijke software-updates, en volledige ondersteuning van bedreigingsverdediging. Dit is met name nuttig voor organisaties die verschillende beveiligingsmaatregelen voor verschillende afdelingen of projecten nodig hebben, maar niet willen investeren in meerdere afzonderlijke hardwareapparatuur. De Multi-Instance optie wordt momenteel ondersteund op het FirePOWER 4100 en 9300 Series security apparaat waarop FTD 6.4 en hoger wordt uitgevoerd.

Dit document gebruikt Firepower4145 die maximaal 14 Container-instanties ondersteunt. Raadpleeg voor de maximale aantal instanties die in FirePOWER-applicatie worden ondersteund [Maximum aantal containerinstanties en -bronnen per model](#).

Netwerkdigram

Dit document introduceert de configuratie en verificatie voor HA in Multi-Instance op dit diagram.



Logisch configuratiediagram

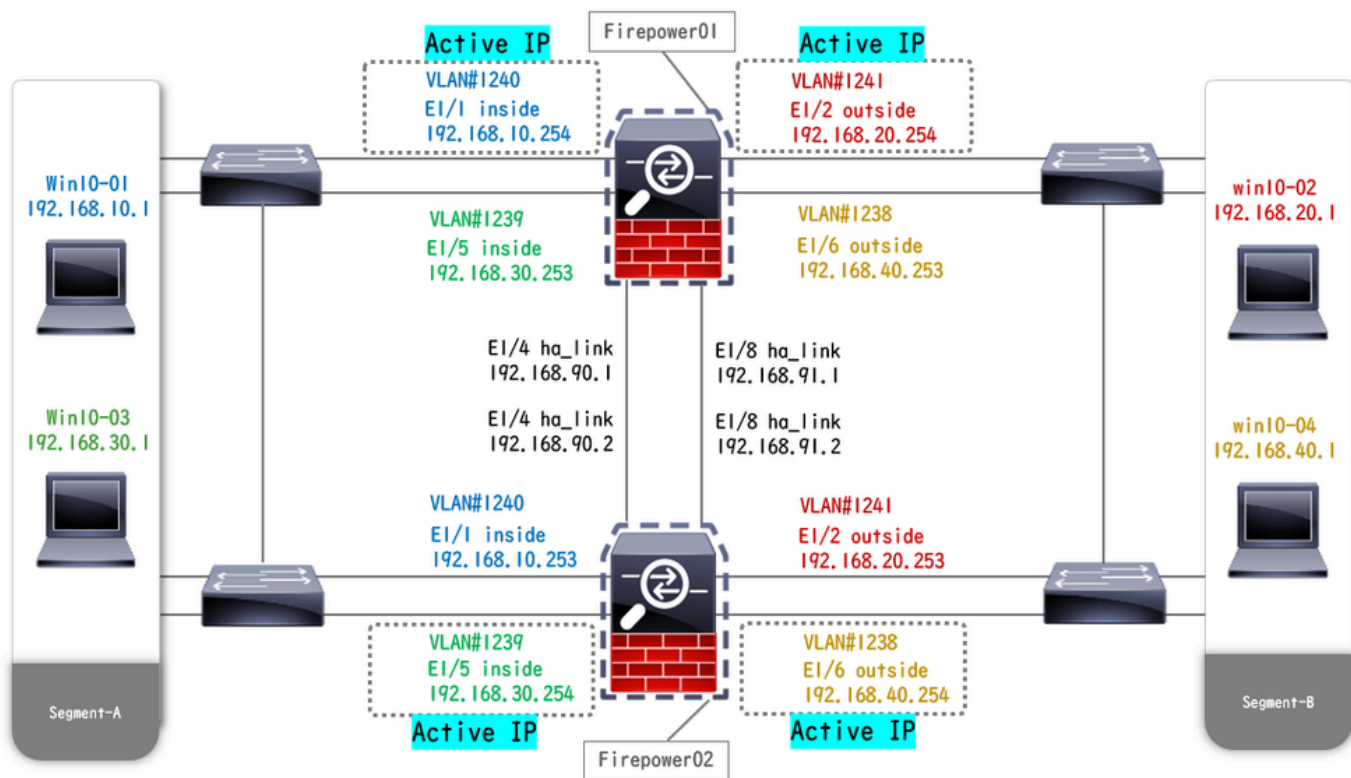
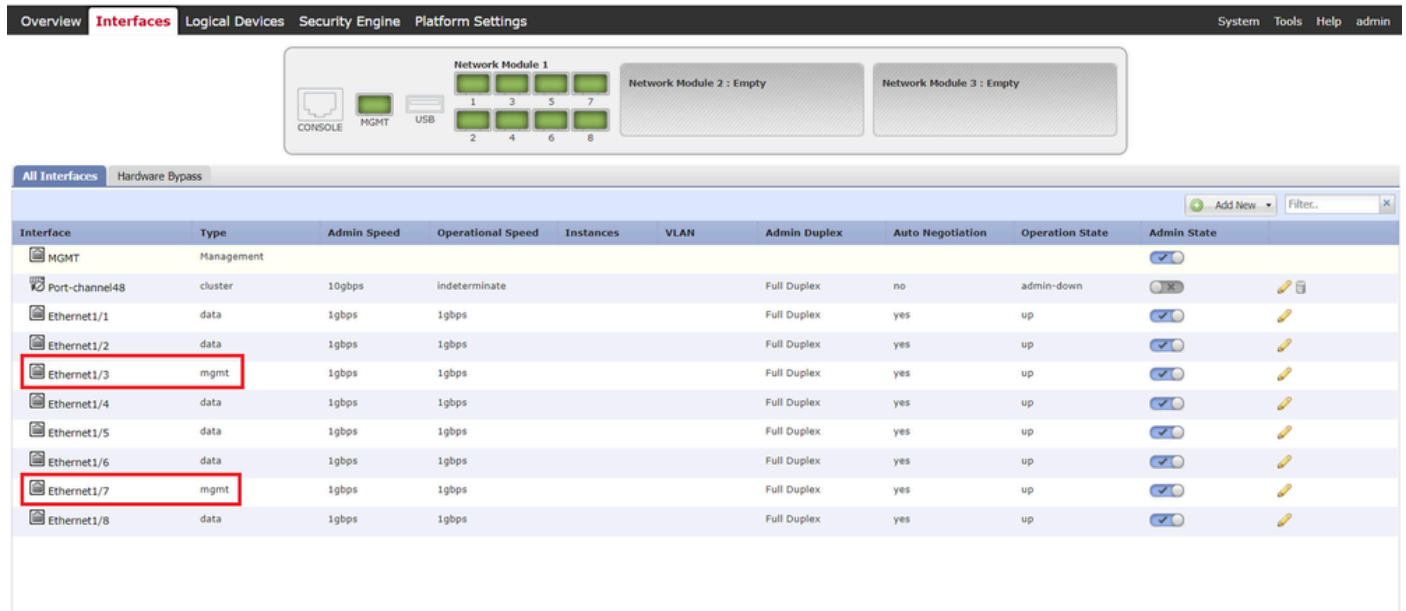


Diagram van fysieke configuratie

Configuraties

Stap 1. Interfaces vooraf configureren

a. Navigeren naar interfaces op FCM. Set 2 beheerinterfaces. In dit voorbeeld Ethernet1/3 en Ethernet1/7.



The screenshot shows the FCM configuration interface. At the top, there is a navigation bar with tabs: Overview, Interfaces (selected), Logical Devices, Security Engine, and Platform Settings. On the right, there are links for System, Tools, Help, and admin. Below the navigation bar, there is a hardware overview section showing three network modules: Network Module 1 (with ports 1-8), Network Module 2 (Empty), and Network Module 3 (Empty). Below this, there is a table of interfaces.

Interface	Type	Admin Speed	Operational Speed	Instances	VLAN	Admin Duplex	Auto Negotiation	Operation State	Admin State
MGMT	Management								<input checked="" type="checkbox"/>
Port-channel48	cluster	10gbps	indeterminate			Full Duplex	no	admin-down	<input type="checkbox"/>
Ethernet1/1	data	1gbps	1gbps			Full Duplex	yes	up	<input checked="" type="checkbox"/>
Ethernet1/2	data	1gbps	1gbps			Full Duplex	yes	up	<input checked="" type="checkbox"/>
Ethernet1/3	mgmt	1gbps	1gbps			Full Duplex	yes	up	<input checked="" type="checkbox"/>
Ethernet1/4	data	1gbps	1gbps			Full Duplex	yes	up	<input checked="" type="checkbox"/>
Ethernet1/5	data	1gbps	1gbps			Full Duplex	yes	up	<input checked="" type="checkbox"/>
Ethernet1/6	data	1gbps	1gbps			Full Duplex	yes	up	<input checked="" type="checkbox"/>
Ethernet1/7	mgmt	1gbps	1gbps			Full Duplex	yes	up	<input checked="" type="checkbox"/>
Ethernet1/8	data	1gbps	1gbps			Full Duplex	yes	up	<input checked="" type="checkbox"/>

Interfaces vooraf configureren

Stap 2. Voeg 2 resourceprofielen toe voor containerinstanties.

a. Navigeer naar Platform Instellingen > Resource Profiles > Add on FCM. Stel 1e resourceprofiel in.

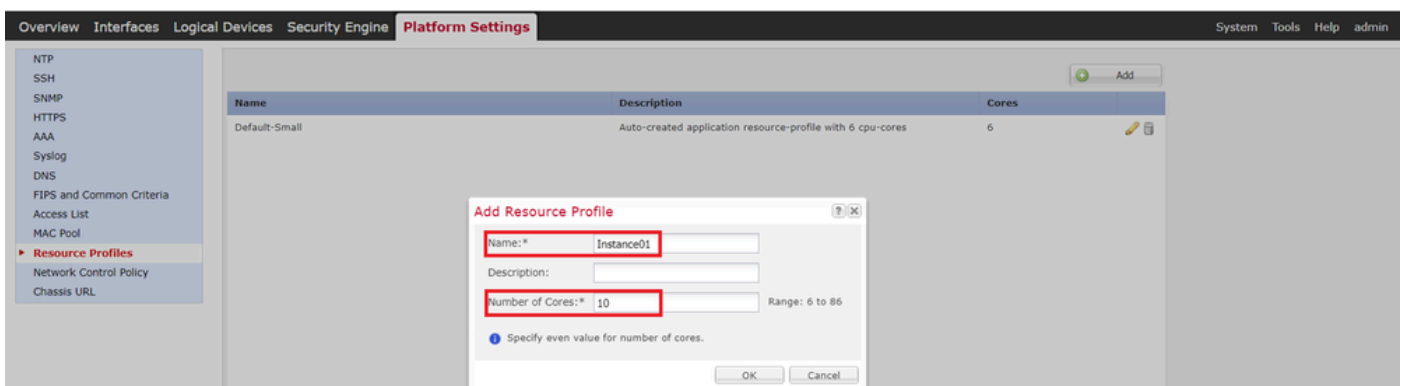
In dit voorbeeld :

- Naam: Instance01
- Aantal kernen: 10

Opmerking: voor HA van het containerinstantiepaar moeten ze dezelfde eigenschappen van het resourceprofiel gebruiken.

Stel de naam van het profiel in tussen 1 en 64 tekens. Merk op dat u de naam van dit profiel niet kunt wijzigen nadat u het hebt toegevoegd.

Stel het aantal kernen voor het profiel in, tussen de 6 en het maximum.

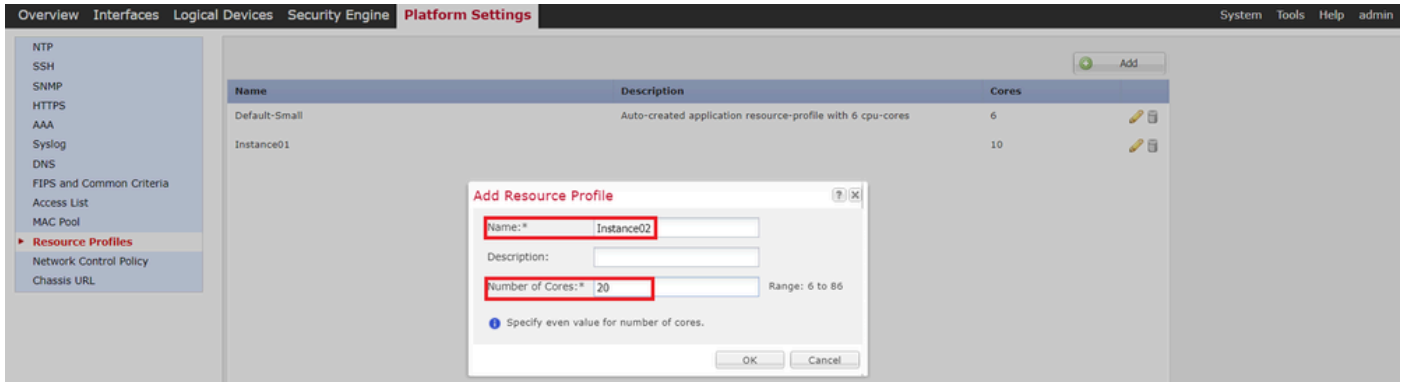


1e resourceprofiel toevoegen

b. Herhaal a. in stap 2 om het tweede resourceprofiel te configureren.

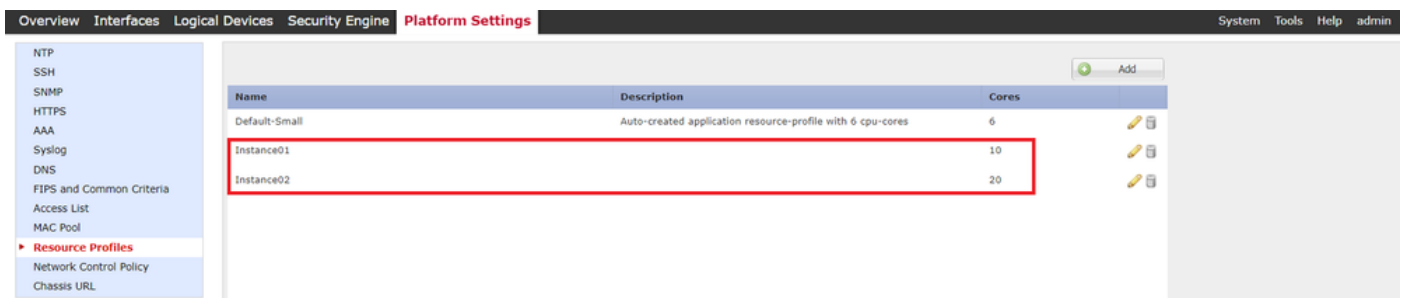
In dit voorbeeld :

- Naam : instantie02
- Aantal kernen: 20



2e resourceprofiel toevoegen

c. Controleer of er twee resourceprofielen zijn toegevoegd.



Resourceprofiel bevestigen

Stap 3. (Optioneel) Voeg een MAC Pool Prefix van virtueel MAC-adres toe voor Container Instance Interfaces.

U kunt het virtuele MAC-adres voor de Active/Standby-interface handmatig instellen. Als de Virtuele Adressen van MAC niet, voor multi-instantie vermogen worden geplaatst, produceert het chassis automatisch de adressen van MAC voor de interfaces van de Instantie, en garandeert dat een gedeelde interface in elke Instantie een uniek adres van MAC gebruikt.

Contr. [Een MAC Pool Prefix toevoegen en MAC-adressen bekijken voor Container Instance Interfaces](#) voor meer details over MAC-adres.

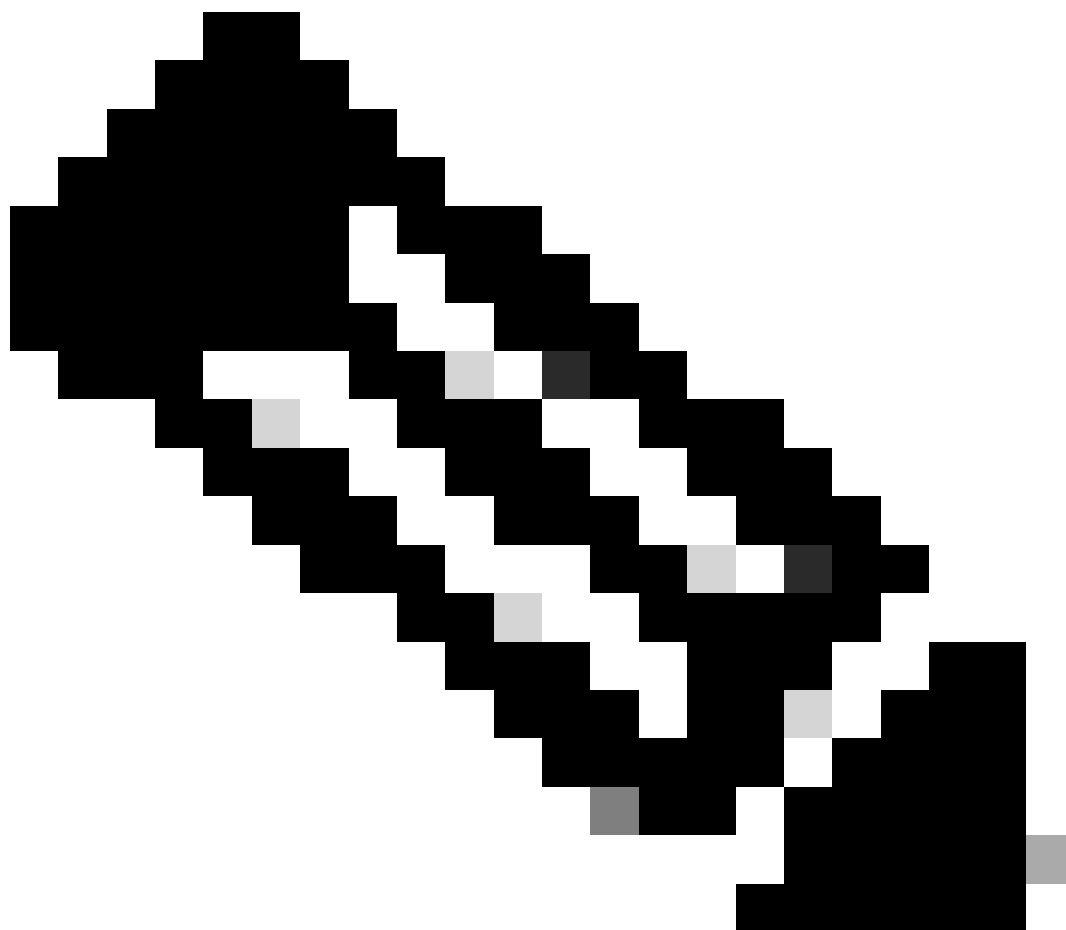
Stap 4. Voeg een standalone instantie toe.

a. Navigeer naar logische apparaten > Standalone toevoegen. Eerste instantie instellen.

In dit voorbeeld :

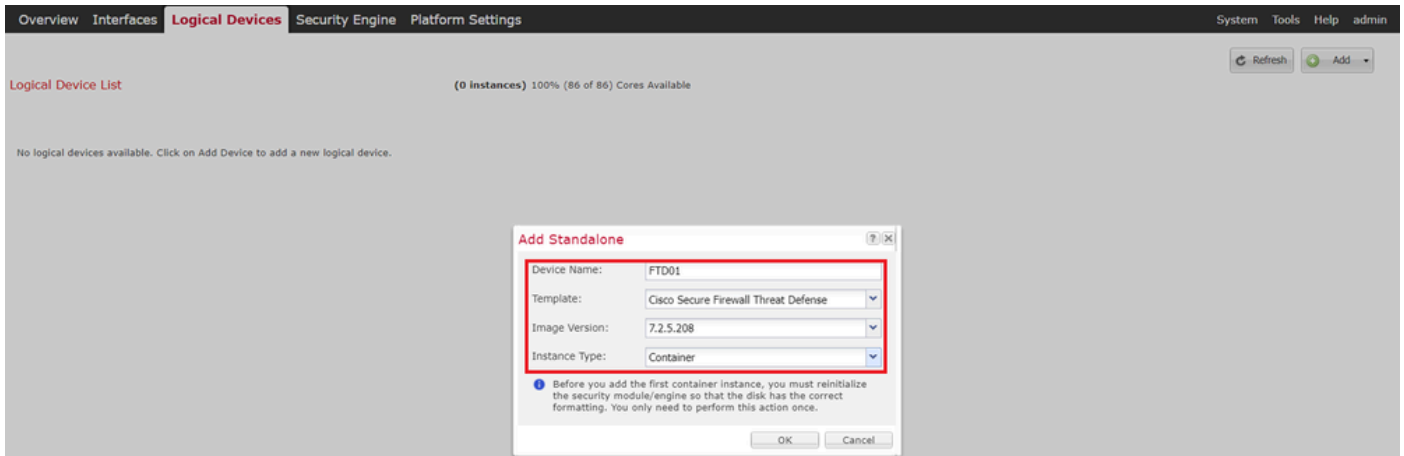
- Apparaatnaam : FTD01

Type instantie: container



Opmerking: de enige manier om een containerapplicatie te implementeren is door een App-Instance vooraf te implementeren met Instance Type ingesteld op Container. Verzeker u ervan dat u Container selecteert.

U kunt deze naam niet wijzigen nadat u het logische apparaat hebt toegevoegd.



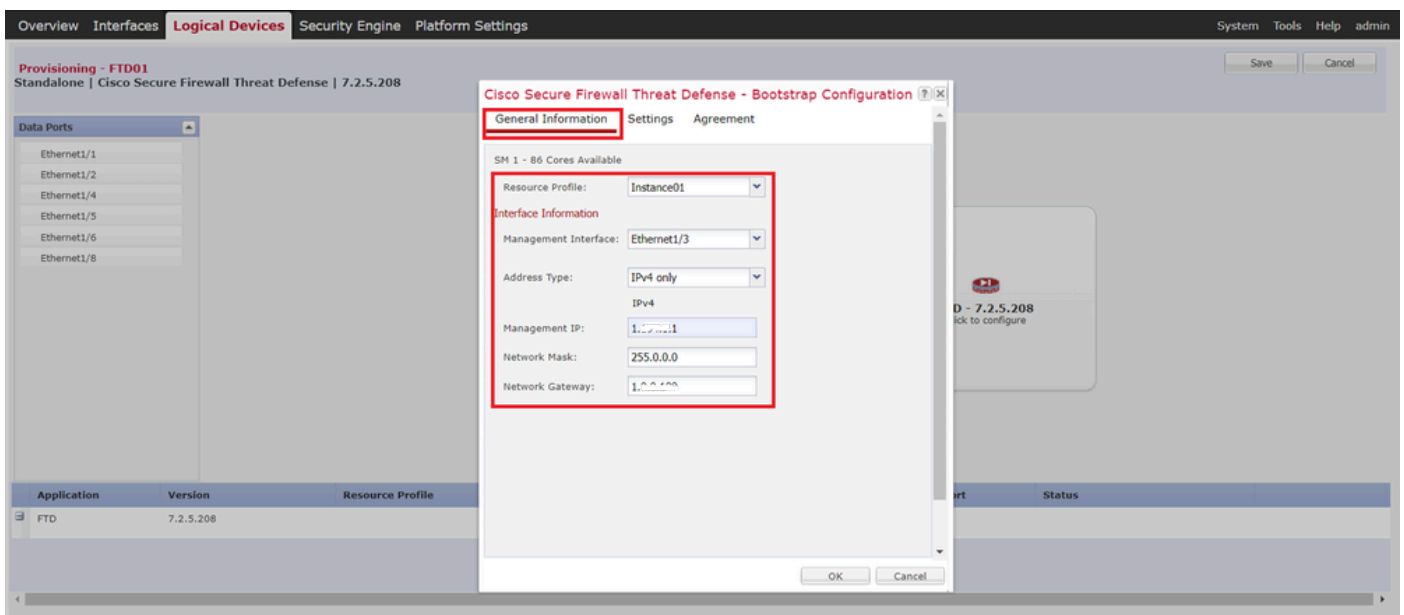
Instantie toevoegen

Stap 5. Interfaces configureren

a. Stel Resource Profile, Management Interface, Management IP in voor Instance01.

In dit voorbeeld :

- Resourceprofiel: Instance01
- Beheerinterface: Ethernet1/3
- ManagementIP: x.x.1.1



Profielen/beheerinterface/IP-beheer configureren

b. Stel data-interfaces in.

In dit voorbeeld :

- Ethernet1/1 (gebruikt voor binnenkant)
- Ethernet1/2 (gebruikt voor buitengebruik)
- Ethernet1/4 (gebruikt voor HA-link)

Overview Interfaces **Logical Devices** Security Engine Platform Settings System Tools Help admin

Provisioning - FTD01 Standalone | Cisco Secure Firewall Threat Defense | 7.2.5.208

Data Ports

- Ethernet1/1
- Ethernet1/2
- Ethernet1/4
- Ethernet1/5
- Ethernet1/6
- Ethernet1/8

Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	7.2.5.208	Instance01	1.1.1.1	1.1.1.1	Ethernet1/3	
Interface Name		Type				
Ethernet1/1		data				
Ethernet1/2		data				
Ethernet1/4		data				

Gegevensinterfaces instellen

c. Navigeer naar logische apparaten. Wachten op bijv. bootup.

Overview Interfaces **Logical Devices** Security Engine Platform Settings System Tools Help admin

Logical Device List (1 Container Instance) 100% (86 of 86) Cores Available

Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	7.2.5.208	Instance01	1.1.1.1	1.1.1.1	Ethernet1/3	Installing

Status van instantie bevestigen01

d. Herhaal a. in stap 4.a en stap 5.a tot en met c om de tweede instantie toe te voegen en geef er een detail voor in te stellen.

In dit voorbeeld :

- Apparaatnaam: FTD11
- Type instantie: Container
- Resourceprofiel: Instance02
- Beheerinterface: Ethernet1/7
- ManagementIP: x.x.10.1
- Ethernet1/5 = binnenkant
- Ethernet1/6 = buiten
- Ethernet1/8 = HA-link

e. Bevestig 2 Instanties zijn online status op FCM.

Logical Device List							(2 Container Instances) 66% (56 of 86) Cores Available	
FTD11 Standalone Status:ok								
Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status		
FTD	7.2.5.208	Instance02	10.10.10.1	1.0.0.0/24	Ethernet1/7	Online		
FTD01 Standalone Status:ok								
Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status		
FTD	7.2.5.208	Instance01	10.10.10.1	1.0.0.0/24	Ethernet1/3	Online		

Instantiestatus op primair apparaat bevestigen

f. (optioneel) Start scope ssa , scope slot 1 en show app-Instance bevestig 2 instanties zijn online status op Firepower CLI.

```
<#root>
```

```
FPR4145-ASA-K9#
```

```
scope ssa
```

```
FPR4145-ASA-K9 /ssa #
```

```
scope slot 1
```

```
FPR4145-ASA-K9 /ssa/slot #
```

```
show app-Instance
```

```
Application Instance: App Name Identifier Admin State Oper State Running Version Startup Version Deplo
Online
```

```
7.2.5 208 7.2.5 208 Container No Instance01 Not Applicable None --> FTD01 Instance is Online ftd FTD11
```

```
Online
```

```
7.2.5 208 7.2.5 208 Container No Instance02 Not Applicable None --> FTD11 Instance is Online
```

g. Doe dit ook met het secundaire apparaat. Bevestig 2 Instanties zijn online status.

Logical Device List							(2 Container Instances) 66% (56 of 86) Cores Available	
FTD12 Standalone Status:ok								
Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status		
FTD	7.2.5.208	Instance02	10.10.10.2	1.0.0.0/24	Ethernet1/7	Online		
FTD02 Standalone Status:ok								
Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status		
FTD	7.2.5.208	Instance01	10.10.10.2	1.0.0.0/24	Ethernet1/3	Online		

Instantiestatus op secundair apparaat bevestigen

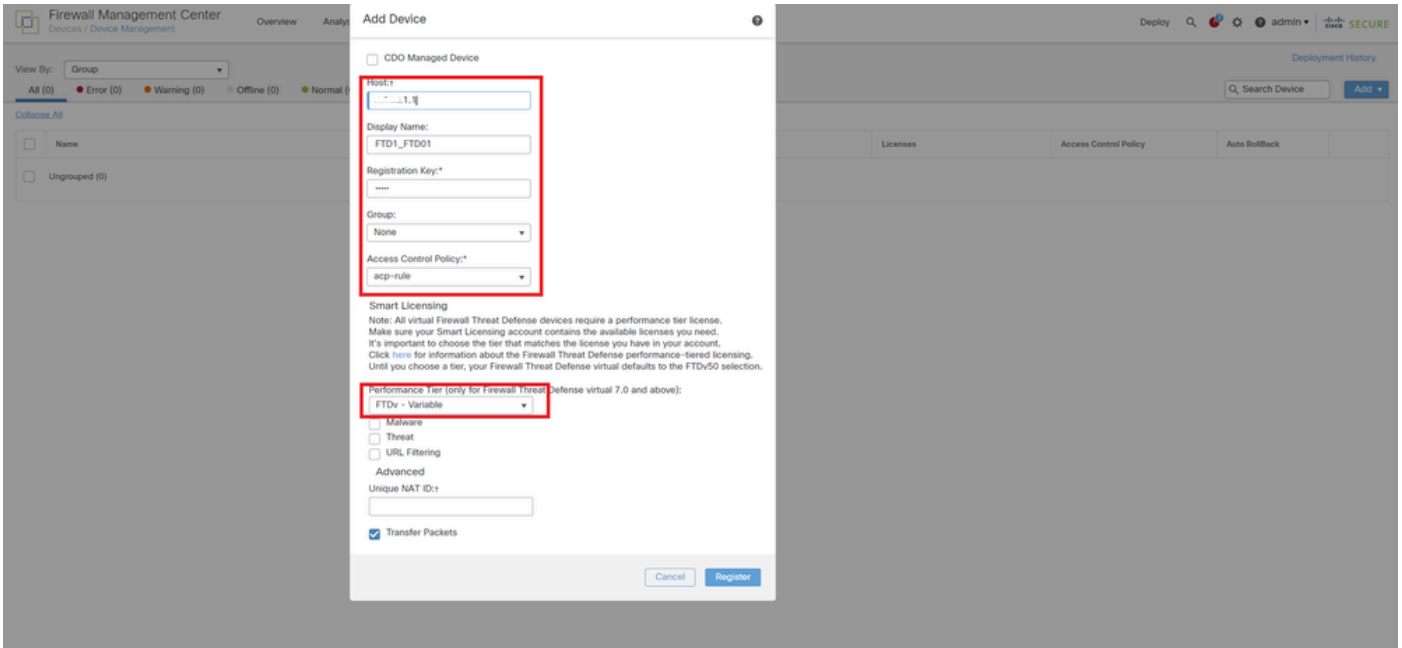
Step 6. Voeg een hoog beschikbaarheidspaar toe voor elke instantie.

a. Ga naar **Apparaten > Apparaat toevoegen** op VCC. Voeg alle instanties toe aan het VCC.

In dit voorbeeld :

- Naam weergeven voor Instance01 van FTD1: FTD1_FTD01
- Naam weergeven voor Instance02 van FTD1: FTD1_FTD11
- Naam weergeven voor Instance01 van FTD2: FTD2_FTD02
- Naam weergeven voor Instance02 van FTD2: FTD2_FTD12

Dit beeld toont de instelling voor **FTD1_FTD01**.



FTD-instantie toevoegen aan FMC

b. Controleer of alle exemplaren normaal zijn.

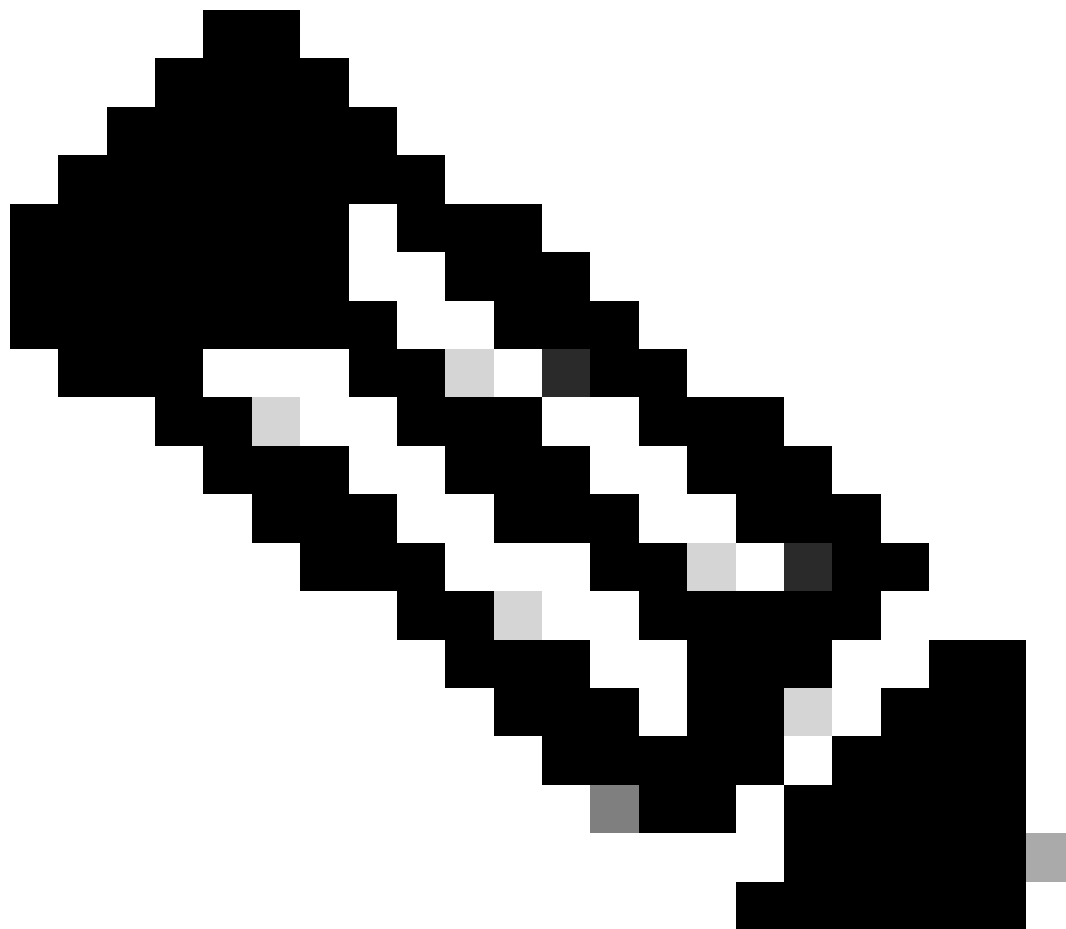
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
FTD1_FTD01 Smart 3 10.1.1.1 - Routed	Firepower 4145 with FTD	7.2.5	FP94145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	⊕
FTD1_FTD11 Smart 3 10.1.1.1 - Routed	Firepower 4145 with FTD	7.2.5	FP94145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	⊕
FTD2_FTD02 Smart 3 10.1.1.2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4145 cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	⊕
FTD2_FTD12 Smart 3 10.1.1.2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4145 cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	⊕

Instantiestatus in VCC bevestigen

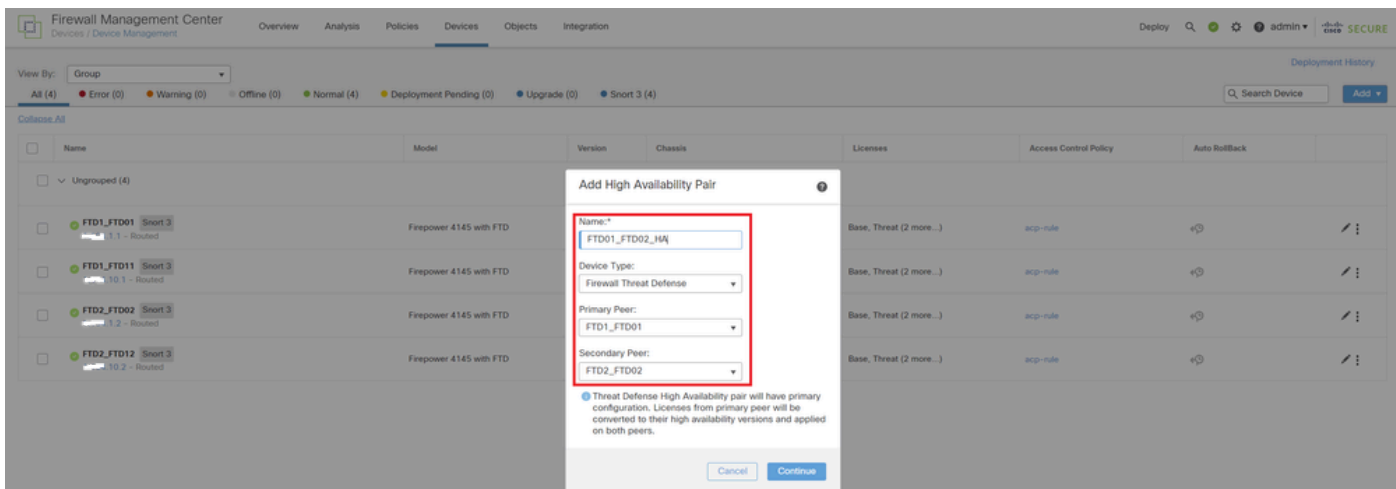
c. Navigeer naar **apparaten > Hoge beschikbaarheid toevoegen**. Stel 1e failover-paar in.

In dit voorbeeld :

- Naam: **FTD01_FTD02_HA**
- Primaire peer: **FTD1_FTD01**



Opmerking: Zorg ervoor dat u de juiste eenheid als primaire eenheid selecteert.



1e failover-paar toevoegen

d. Stel IP voor failover link in als 1e failover-paar.

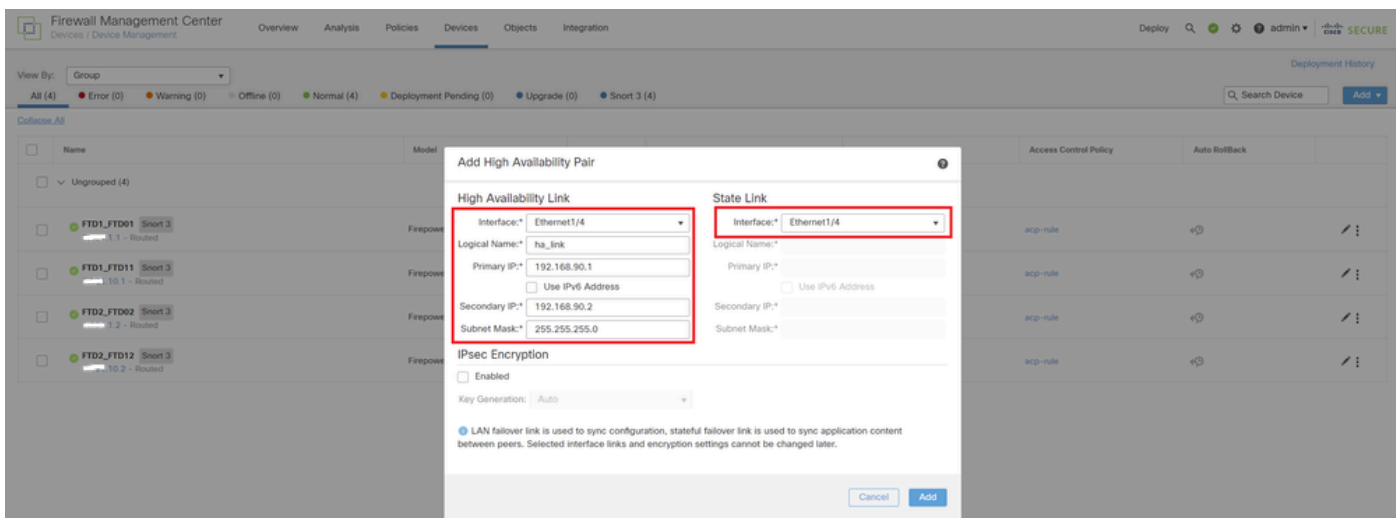
In dit voorbeeld :

High Availability Link: Ethernet1/4

Statuslink: Ethernet1/4

Primair IP-adres: 192.168.90.1/24

Secundair IP-adres: 192.168.90.2/24



HA-interface en IP instellen voor 1e failover-paar

e. Bevestig de status van failover

FTD1_FTD01: Primair, actief

FTD2_FTD02: Secundair, stand-by

View By:	Group	Deployment History
All (4)	Error (0) Warning (0) Offline (0) Normal (4) Deployment Pending (0) Upgrade (0) Snort 3 (4)	Search Device Add
Collector: All		
<input type="checkbox"/>	Ungrouped (3)	
<input type="checkbox"/>	FTD01_FTD02_HA High Availability	
<input type="checkbox"/>	FTD1_FTD01(Primary, Active) Snort 3	Firepower 4145 with FTD 7.2.5 FTB145-ASA-K9-443 Security Module - 1 (Container) Base, Threat (2 more...) acp-rule
<input type="checkbox"/>	FTD2_FTD02(Secondary, Standby) Snort 3	Firepower 4145 with FTD 7.2.5 Firepower4145G.cisco.com:443 Security Module - 1 (Container) Base, Threat (2 more...) acp-rule
<input type="checkbox"/>	FTD1_FTD11 Snort 3	Firepower 4145 with FTD 7.2.5 FTB145-ASA-K9-443 Security Module - 1 (Container) Base, Threat (2 more...) acp-rule
<input type="checkbox"/>	FTD2_FTD12 Snort 3	Firepower 4145 with FTD 7.2.5 Firepower4145G.cisco.com:443 Security Module - 1 (Container) Base, Threat (2 more...) acp-rule

Status van eerste failover-paar bevestigen

f. Navigeren naar **apparaten** > **Klik op FTD01_FTD02_HA** (in dit voorbeeld) > **Interfaces**. Stel actieve IP voor data-interface in.

In dit voorbeeld :

- Ethernet1/1 (binnenkant): 192.168.10.254/24
- Ethernet1/2 (buiten): 192.168.20.254/24
- Ethernet1/3 (diagnostisch): 192.168.80.1/24

Dit beeld toont de instelling voor Active IP van **Ethernet1/1**.

FTD1_FTD01
Cisco Firepower 4145 Threat Defense

Summary High Availability Device Routing **Interfaces** Inline Sn...

Interface	Logi...
<input checked="" type="checkbox"/> Ethernet1/1	inside
<input type="checkbox"/> Ethernet1/2	outside
<input type="checkbox"/> Ethernet1/3	diagnostic
<input type="checkbox"/> Ethernet1/4	

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Advanced

Name: inside

Enabled

Description: Management Only

Mode: None

Security Zone: inside_zone

Interface ID: Ethernet1/1

MTU: 1500 (64 - 9184)

Priority: 0 (0 - 65530)

Propagate Security Group Tag:

NVE Only:

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Advanced

IP Type: Use Static IP

IP Address: 192.168.10.254/24

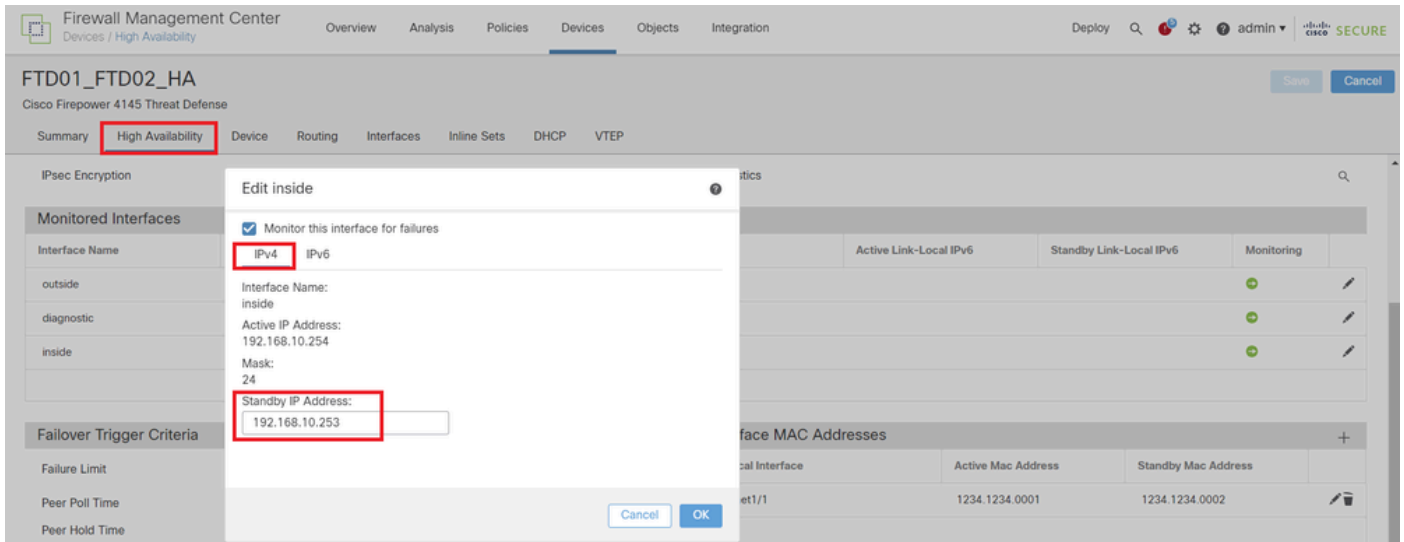
Actieve IP voor data-interface instellen

Ga naar **Apparaten** > **Klik op FTD01_FTD02_HA** (in dit voorbeeld) > **High Availability**. Stel stand-by IP voor data-interface in.

In dit voorbeeld :

- Ethernet1/1 (binnenkant): 192.168.10.253/24
- Ethernet1/2 (buiten): 192.168.20.253/24
- Ethernet1/3 (diagnostisch): 192.168.80.2/24

Dit beeld toont de instelling voor Standby IP van **Ethernet1/1**.



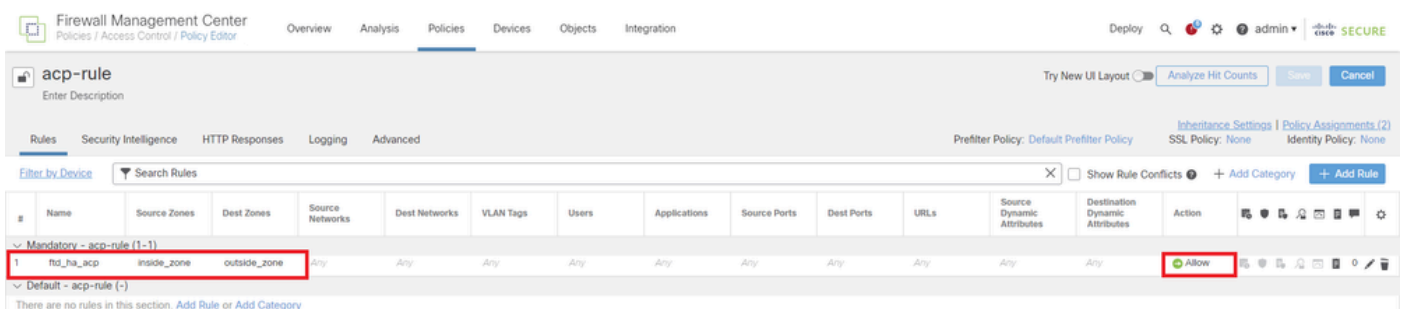
Standby IP voor data-interface instellen

h. Herhaal stap 6.c tot en met g om het tweede failover-paar toe te voegen.

In dit voorbeeld :

- Naam : FTD11_FTD12_HA
- Primaire peer: FTD1_FTD11
- Secundaire peer: FTD2_FTD12
- High Availability Link: Ethernet1/8
- State Link: Ethernet1/8
- Ethernet1/8 (ha_link actief): 192.168.91.1/24
- Ethernet1/5 (in actief): 192.168.30.254/24
- Ethernet1/6 (buiten actief): 192.168.40.254/24
- Ethernet1/7 (diagnostisch actief): 192.168.81.1/24
- Ethernet1/8 (ha_link Standby): 192.168.91.2/24
- Ethernet1/5 (in standby): 192.168.30.253/24
- Ethernet1/6 (buiten Standby): 192.168.40.253/24
- Ethernet1/7 (diagnostische stand-by): 192.168.81.2/24

i. Navigeren naar **logische apparaten > Standalone toevoegen**. Stel de ACS-regel in om het verkeer van binnen naar buiten toe mogelijk te maken.



ACS-regeling instellen

j. Stel de instelling in op FTD.

k. Bevestig de HA-status in CLI

De HA status voor elke instantie wordt ook bevestigd in Firepower CLI die hetzelfde is als ASA.

Start **show running-config failover** en **show failover** opdracht om de HA-status van FTD1_FTD01 (Primaire instantie01) te bevestigen.

```
<#root>
```

```
// confirm HA status of FTD1_FTD01 (Instance01 of Primary Device) >
```

```
show running-config failover
```

```
failover failover lan unit primary failover lan interface ha_link Ethernet1/4 failover replication http
```

```
show failover
```

```
Failover On Failover unit Primary Failover LAN Interface: ha_link Ethernet1/4 (up) ..... This host: P  
..... Other host: Secondary - Standby Ready <---- Instance01 of FPR02 is Standby Interface diagnostic
```

Uitvoeren **show running-config failover** en **show failover** opdracht om de HA-status van FTD1_FTD11 te bevestigen (Primaire instantie02)

```
<#root>
```

```
// confirm HA status of FTD1_FTD11 (Instance02 of Primary Device) >
```

```
show running-config failover
```

```
failover failover lan unit primary failover lan interface ha_link Ethernet1/8 failover replication http
```

```
show failover
```

```
Failover On Failover unit Primary Failover LAN Interface: ha_link Ethernet1/8 (up) ..... This host: P  
Other host: Secondary - Standby Ready <---- Instance02 of FPR02 is Standby Interface diagnostic (192.16
```

Doorlopen **show running-config failover** en **show failover** opdracht geven om de HA-status van FTD2_FTD02 te bevestigen (Secundaire instantie01).

```
<#root>
```

```
// confirm HA status of FTD2_FTD02 (Instance01 of Secondary Device) >
```

```
show running-config failover
```

```
failover failover lan unit secondary failover lan interface ha_link Ethernet1/4 failover replication h
```

```
show failover
```

```
Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/4 (up) ..... This host:
```


Other host: Primary - Active <---- Instance01 of FPR01 is Active Active time: 31651 (sec) slot 0: UCSB-

Start **show running-config failover** en **show failover** opdracht om de HA-status van FTD2_FTD12 (Secundaire instantie02) te bevestigen.

<#root>

// confirm HA status of FTD2_FTD12 (Instance02 of Secondary Device) >

show running-config failover

failover failover lan unit secondary failover lan interface ha_link Ethernet1/8 failover replication h
Other host: Primary - Active <---- Instance02 of FPR01 is Active Active time: 31275 (sec) slot 0: UCSB-

I. Bevestig het gebruik van de vergunning

Alle licenties worden gebruikt per beveiligingsmotor/chassis en niet per container instantie.

·Basislicenties worden automatisch toegewezen: één per beveiligingsmotor/chassis.

·Licenties voor functies worden handmatig toegewezen aan elke instantie, maar u gebruikt slechts één licentie per voordeelmotor/chassis. Voor een specifieke functielicentie hebt u slechts in totaal 1 licentie nodig, ongeacht het aantal gebruikte instanties.

In deze tabel wordt aangegeven hoe de licenties in dit document worden gebruikt.

FPR01	Instantie01	Basis, URL-filtering, malware, bedreiging
	Instantie02	Basis, URL-filtering, malware, bedreiging
FPR02	Instantie01	Basis, URL-filtering, malware, bedreiging
	Instantie02	Basis, URL-filtering, malware, bedreiging

Totaal aantal licenties

Basis	URL-filtering	Malware	dreigement
2	2	2	2

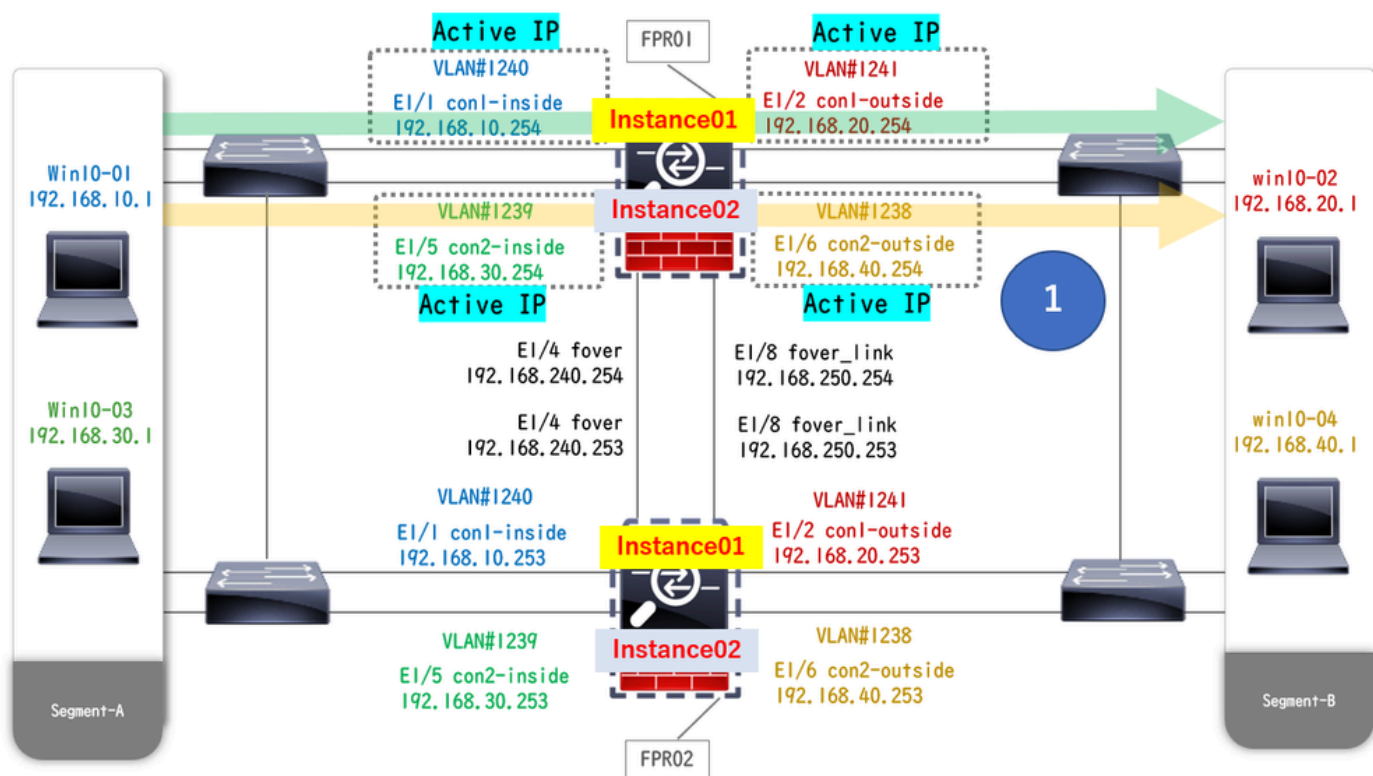
Bevestig het aantal verbruikte licenties in de FMC GUI.

License Type/Device Name	License Status	Device Type	Domain	Group
Base (2)	In-Compliance			
> FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Threat Defense	Global	N/A
> FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Threat Defense	Global	N/A
Malware (2)	In-Compliance			
> FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Threat Defense	Global	N/A
> FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Threat Defense	Global	N/A
Threat (2)	In-Compliance			
> FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Threat Defense	Global	N/A
> FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Threat Defense	Global	N/A
URL Filtering (2)	In-Compliance			
> FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Threat Defense	Global	N/A
> FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Threat Defense	Global	N/A

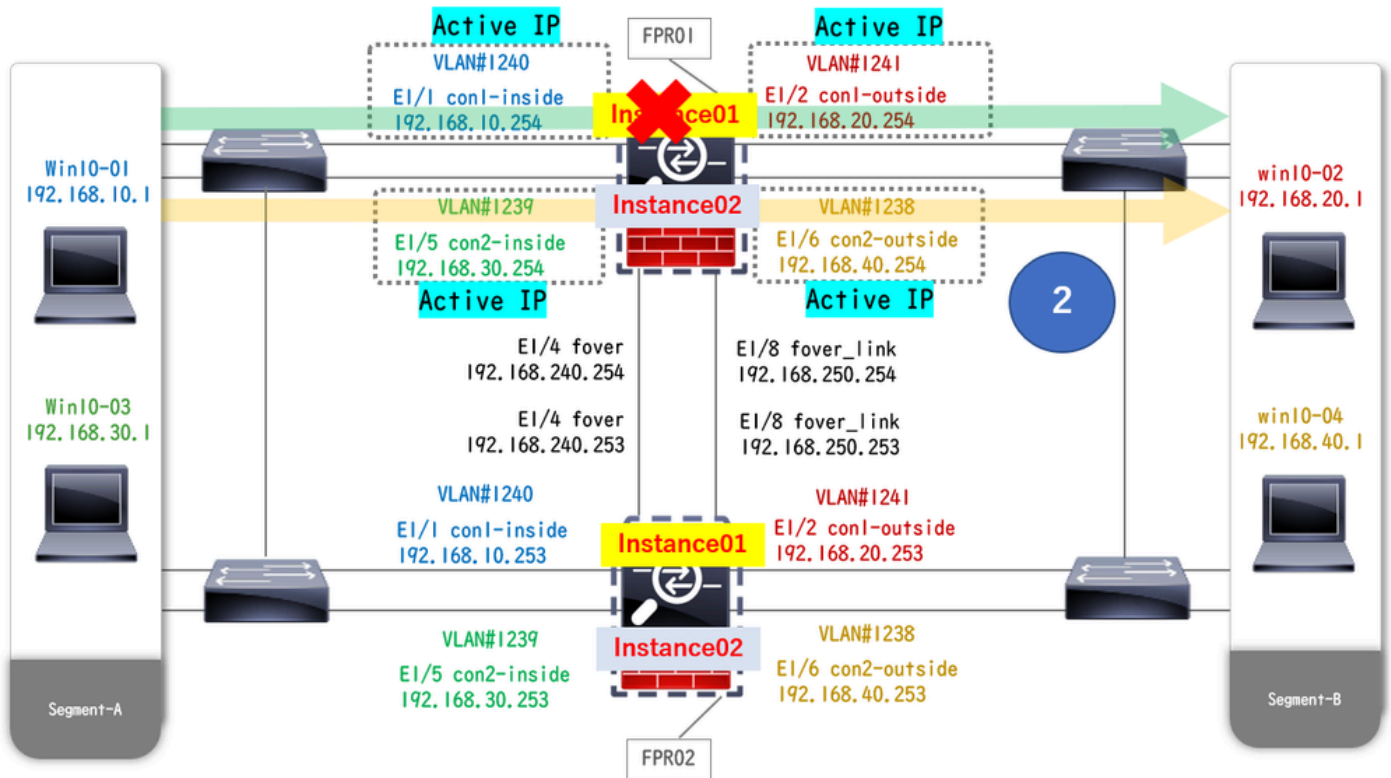
Bevestig verbruikte licenties

Verifiëren

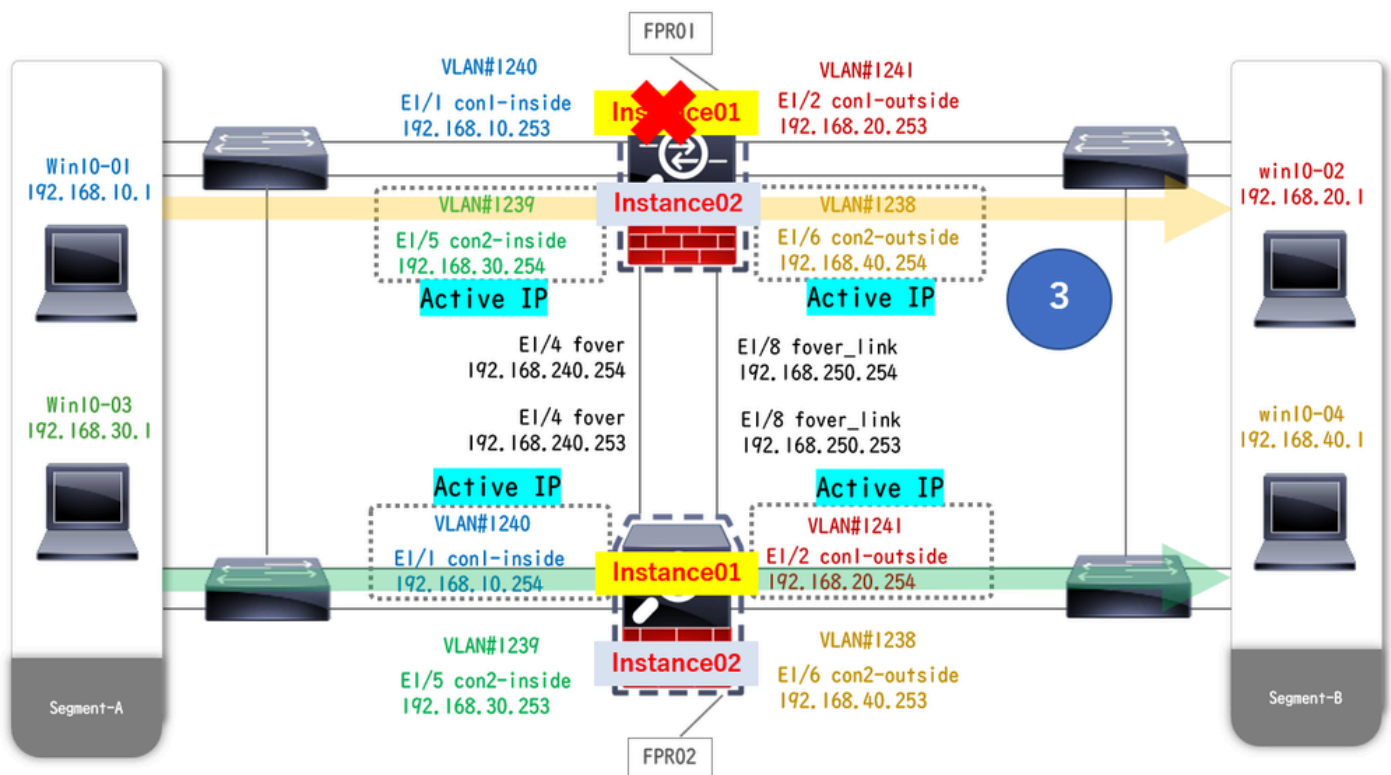
Wanneer de crash plaatsvond op FTD1_FTD01 (Primary Instance01), wordt de failover van Instance01 geactiveerd en nemen de gegevensinterfaces aan de Standby-zijde het IP/MAC-adres van de oorspronkelijke Active Interface over, waardoor het verkeer (FTP-verbinding in dit document) continu door Firepower wordt doorgegeven.



Voor de botsing



tijdens de crash



failover is geactiveerd

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

Stap 2. De show conn opdracht uitvoeren om de FTP-verbinding te bevestigen is in beide gevallen vastgelegd.

<#root>

```
// Confirm the connection in Instance01 of FPR01 >
```

```
show conn
```

```
TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:00:11, bytes 529, flags UIO N1 // Confirm
```

```
show conn
```

```
TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:00:42, bytes 530, flags UIO N1
```

Stap 3. Start FTP verbinding van Win10-03 naar Win10-04.

Stap 4. De **show conn** opdracht Uitvoeren om de FTP-verbinding te bevestigen is in beide gevallen vastgelegd.

```
<#root>
```

```
// Confirm the connection in Instance02 of FPR01 >
```

```
show conn
```

```
TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:00:02, bytes 530, flags UIO N1 // Confirm
```

```
show conn
```

```
TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:00:13, bytes 530, flags UIO N1
```

Stap 5. Start `connect ftd FTD01` en `system support diagnostic-cli` opdracht om ASA CLI te starten. Start `enableen crashinfo force watchdog` commando om crash Instance01 in primaire/actieve eenheid te forceren.

```
<#root>
```

```
Firepower-module1>
```

```
connect ftd FTD01
```

```
>
```

```
system support diagnostic-cli
```

```
FTD01>
```

```
enable
```

```
Password: FTD01# FTD01#
```

```
crashinfo force watchdog
```

```
reboot. Do you wish to proceed? [confirm]:
```

Stap 6. Failover treedt op in Instance01 en de FTP-verbinding wordt niet onderbroken. Draai `show failover` en `show conn` commando om de status van Instance01 in FPR02 te bevestigen.

```
<#root>
```

```
>
```

```
show failover
```

```
Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/4 (up) ..... This host:
Other host: Primary - Failed Interface diagnostic (192.168.80.2): Unknown (Monitored) Interface inside (
```

```
show conn
```

```
TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:02:25, bytes 533, flags U N1
```

Stap 7. De crash in Instance01 had geen effect op Instance02. Draai show failover en show conn commando om de status van Instance02 te bevestigen.

```
<#root>
```

```
>
```

```
show failover
```

```
Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/8 (up) ..... This host:
Other host: Primary - Active Interface diagnostic (192.168.81.1): Normal (Monitored) Interface inside (1
```

```
show conn
```

```
TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:01:18, bytes 533, flags UIO N1
```

Stap 8. Ga naar **Apparaten** > **Alles** op FMC. Bevestig de HA-status.

FTD1_FTD01: Primair, stand-by

FTD2_FTD02: Secundair, actief

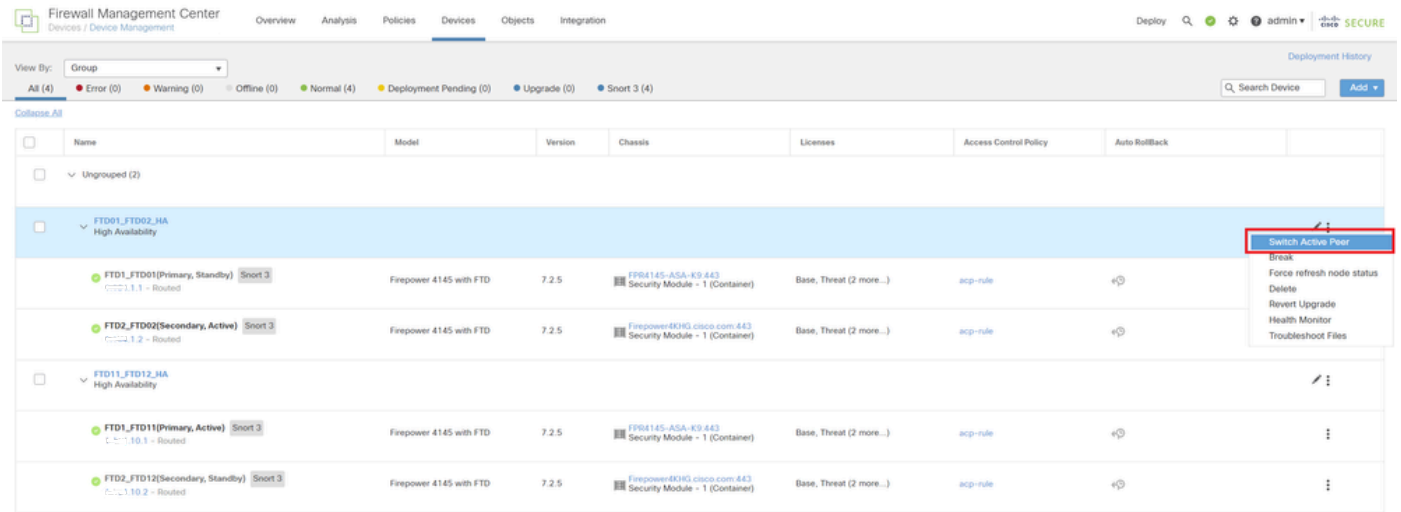
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto Rollback
Ungrouped (2)						
FTD01_FTD02_HA High Availability						
FTD1_FTD01(Primary, Standby) Snort 3	Firepower 4145 with FTD	7.2.5	FPR0145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	+⊞
FTD2_FTD02(Secondary, Active) Snort 3	Firepower 4145 with FTD	7.2.5	Firepower4145.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	+⊞
FTD11_FTD12_HA High Availability						
FTD11_FTD11(Primary, Active) Snort 3	Firepower 4145 with FTD	7.2.5	FPR0145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	+⊞
FTD2_FTD12(Secondary, Standby) Snort 3	Firepower 4145 with FTD	7.2.5	Firepower4145.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	+⊞

HA-status bevestigen

Stap 9. (Optioneel)Nadat de Instance01 van FPR01 terugkeert naar normaal, kunt u de status van HA handmatig switches. Dit kan door FMC

GUI of FRP CLI worden gedaan.

Ga in het VCC naar **Apparaten > Alle**. Klik op **Switch Active Peer** to switch HA status voor **FTD01_FTD02_HA**.



Switch HA-status

Op Firepower CLI, Start connect ftd FTD01 en system support diagnostic-cli opdracht om ASA CLI in te voeren. Start enableen **failover active** commando naar switch HA voor FTD01_FTD02_HA.

```
<#root>
```

```
Firepower-module1>
```

```
connect ftd FTD01
```

```
>
```

```
system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach. Type help or '?' for a list of availab
```

```
enable
```

```
firepower#
```

```
failover active
```

Problemen oplossen

Om de status van failover te valideren, voert u **show failover** de **show failover history** opdracht uit.

```
<#root>
```

```
>
```

```
show failover
```

```
Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/8 (up) ..... This host:
```

Other host: Primary - Active Interface diagnostic (192.168.81.1): Normal (Monitored) Interface inside (I

>

show failover history

===== From State To State Reason =====

Start de opdracht debug fover <optie> om debug-logbestand van failover in te schakelen.

<#root>

>

debug fover

auth Failover Cloud authentication cable Failover LAN status cmd-exec Failover EXEC command execution c

Referentie

<https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.html>

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/multi-Instance/multi-Instance_solution.html

<https://www.cisco.com/c/en/us/support/docs/availability/high-availability/217763-troubleshoot-firepower-threat-defense-hi.html#toc-hId-46641497>

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.