FTD-beheerinterface (Firepower Threat Defense) configureren

Inhoud

Inleiding

In dit document worden de werking en configuratie van de beheerinterface op Firepower Threat Defense (FTD) beschreven.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

- FTD die werkt op ASA 5508-X hardwareapparaat
- FTD die werkt op ASA5512-X hardwareapparaat
- FTD die op FPR9300 hardwareapparaat loopt
- VCC dat werkt op 6.1.0 (build 330)

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

FTD is een geünificeerd software-image dat op deze platforms kan worden geïnstalleerd:

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR4100, FPR9300
- VMware (ESXi)
- Amazon Web Services (AWS)
- KVM
- ISR-routermodule

Het doel van dit document is aan te tonen:

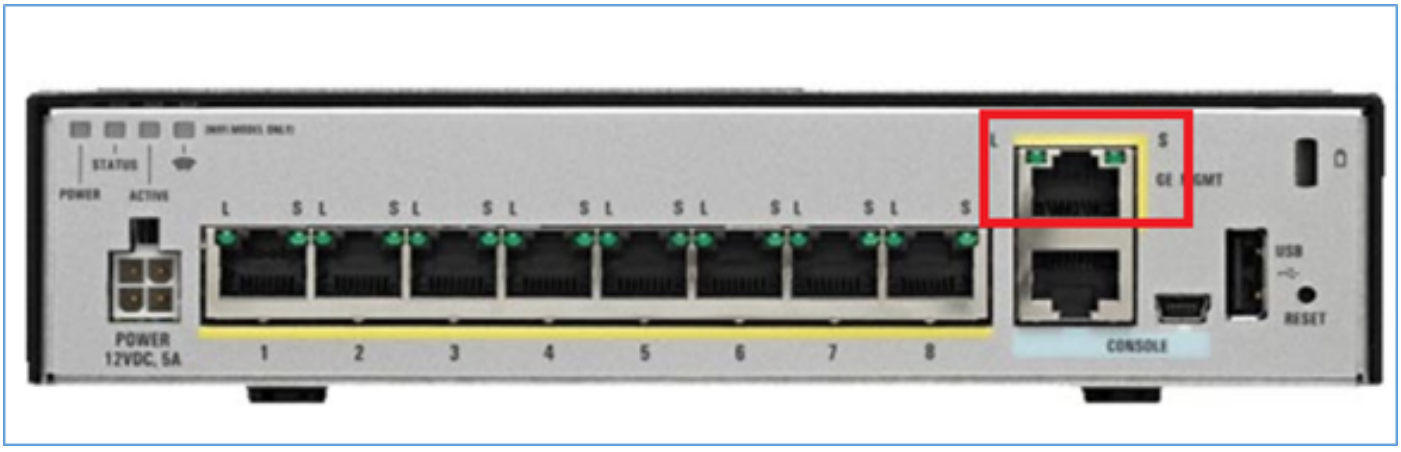
- FTD Management-interfacearchitectuur op ASA 5500-X-apparaten
- FTD-beheerinterface wanneer FDM wordt gebruikt
- FTD-beheerinterface op de FP41xx/FP9300-serie
- Integratiescenario's van FTD/Firepower Management Center (FMC)

Configureren

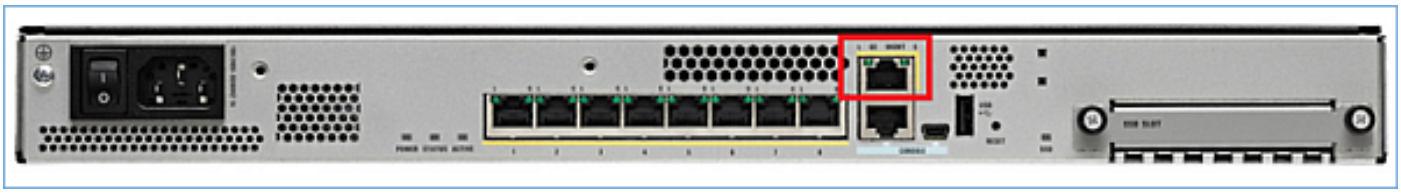
Beheerinterface op ASA 5500-X-apparaten

De beheerinterface op ASA 5506/08/16-X- en ASA 5512/15/25/45/55-X-apparaten.

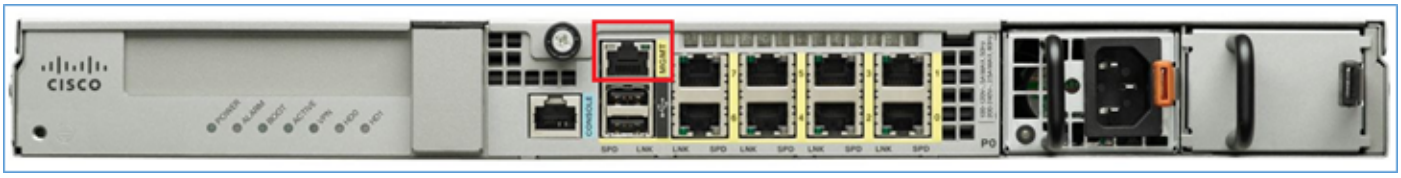
Dit is het beeld van ASA 5506-X:



Dit is het beeld van ASA 5508-X:



Dit is het beeld van ASA 5555-X:



Wanneer een FTD-beeld wordt geïnstalleerd op 5506/08/16 wordt de beheerinterface weergegeven als **Management1/1**. Op 5512/15/25/45/55-X-apparaten wordt dit **Management0/0.** Van de FTD Command Line Interface (CLI) kan dit worden geverifieerd in de **show tech-support** output.

Verbind met de FTD-console en voer de opdracht uit:

```
> show tech-support
-----------------[ BSNS-ASA5508-1 ]-----------------
Model                     : Cisco ASA5508-X Threat Defense (75) Version 6.1.0 (Build 330)
UUID                      : 04f55302-a4d3-11e6-9626-880037a713f3
Rules update version      : 2016-03-28-001-vrt
VDB version               : 270
------------------------------------------------

Cisco Adaptive Security Appliance Software Version 9.6(2)

Compiled on Tue 23-Aug-16 19:42 PDT by builders
System image file is "disk0:/os.img"
Config file at boot was "startup-config"

firepower up 13 hours 43 mins

Hardware:   ASA5508, 8192 MB RAM, CPU Atom C2000 series 2000 MHz, 1 CPU (8 cores)
Internal ATA Compact Flash, 8192MB
BIOS Flash M25P64 @ 0xfed01000, 16384KB

Encryption hardware device : Cisco ASA Crypto on-board accelerator (revision 0x1)
                             Number of accelerators: 1

 1: Ext: GigabitEthernet1/1  : address is d8b1.90ab.c852, irq 255
 2: Ext: GigabitEthernet1/2  : address is d8b1.90ab.c853, irq 255
 3: Ext: GigabitEthernet1/3  : address is d8b1.90ab.c854, irq 255
 4: Ext: GigabitEthernet1/4  : address is d8b1.90ab.c855, irq 255
 5: Ext: GigabitEthernet1/5  : address is d8b1.90ab.c856, irq 255
 6: Ext: GigabitEthernet1/6  : address is d8b1.90ab.c857, irq 255
 7: Ext: GigabitEthernet1/7  : address is d8b1.90ab.c858, irq 255
 8: Ext: GigabitEthernet1/8  : address is d8b1.90ab.c859, irq 255
 9: Int: Internal-Data1/1    : address is d8b1.90ab.c851, irq 255
10: Int: Internal-Data1/2    : address is 0000.0001.0002, irq 0
11: Int: Internal-Control1/1 : address is 0000.0001.0001, irq 0
12: Int: Internal-Data1/3    : address is 0000.0001.0003, irq 0
13:   Ext: Management1/1       : address is d8b1.90ab.c851, irq 0
14: Int: Internal-Data1/4    : address is 0000.0100.0001, irq 0
```

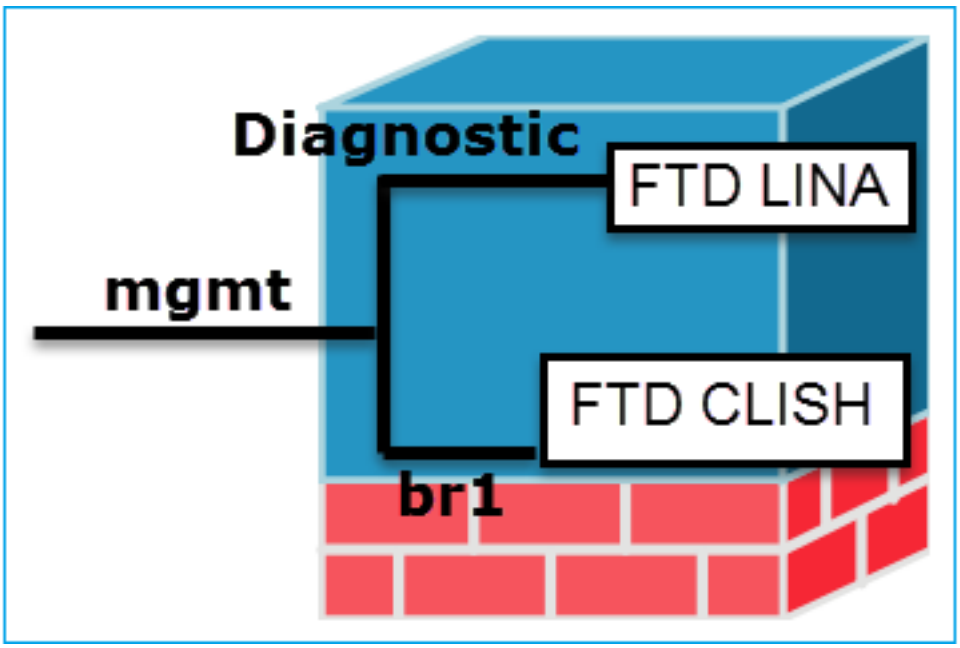
ASA 5512-X:

```
> show tech-support
------------------[ FTD5512-1 ]-------------------
Model                     : Cisco ASA5512-X Threat Defense (75) Version 6.1.0 (Build 330)
UUID                      : 8608e98e-f0e9-11e5-b2fd-b649ba0c2874
Rules update version      : 2016-03-28-001-vrt
VDB version               : 270
```

```
---------------------------------------------------

Cisco Adaptive Security Appliance Software Version 9.6(2)

Compiled on Fri 18-Aug-16 15:08 PDT by builders
System image file is "disk0:/os.img"
Config file at boot was "startup-config"

firepower up 4 hours 37 mins

Hardware:   ASA5512, 4096 MB RAM, CPU Clarkdale 2793 MHz, 1 CPU (2 cores)
            ASA: 1764 MB RAM, 1 CPU (1 core)
Internal ATA Compact Flash, 4096MB
BIOS Flash MX25L6445E @ 0xffbb0000, 8192KB

Encryption hardware device: Cisco ASA Crypto on-board accelerator (revision 0x1)
                            Boot microcode        : CNPx-MC-BOOT-2.00
                            SSL/IKE microcode     : CNPx-MC-SSL-SB-PLUS-0005
                            IPSec microcode       : CNPx-MC-IPSEC-MAIN-0026
                            Number of accelerators: 1
Baseboard Management Controller (revision 0x1) Firmware Version: 2.4

 0: Int: Internal-Data0/0    : address is a89d.21ce.fde6, irq 11
 1: Ext: GigabitEthernet0/0  : address is a89d.21ce.fdea, irq 10
 2: Ext: GigabitEthernet0/1  : address is a89d.21ce.fde7, irq 10
 3: Ext: GigabitEthernet0/2  : address is a89d.21ce.fdeb, irq 5
 4: Ext: GigabitEthernet0/3  : address is a89d.21ce.fde8, irq 5
 5: Ext: GigabitEthernet0/4  : address is a89d.21ce.fdec, irq 10
 6: Ext: GigabitEthernet0/5  : address is a89d.21ce.fde9, irq 10
 7: Int: Internal-Control0/0 : address is 0000.0001.0001, irq 0
 8: Int: Internal-Data0/1    : address is 0000.0001.0003, irq 0
   9: Ext: Management0/0       : address is a89d.21ce.fde6, irq 0
```

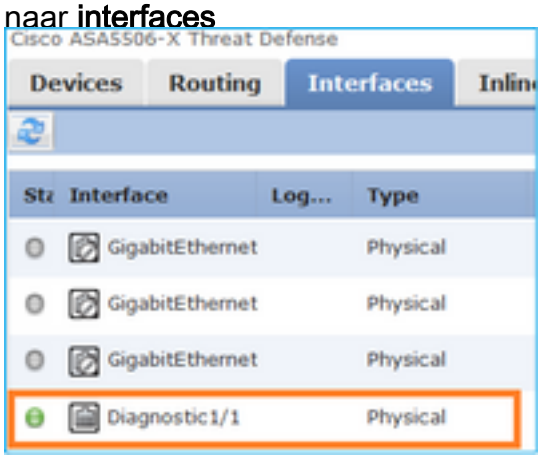
Beheerinterfacearchitectuur

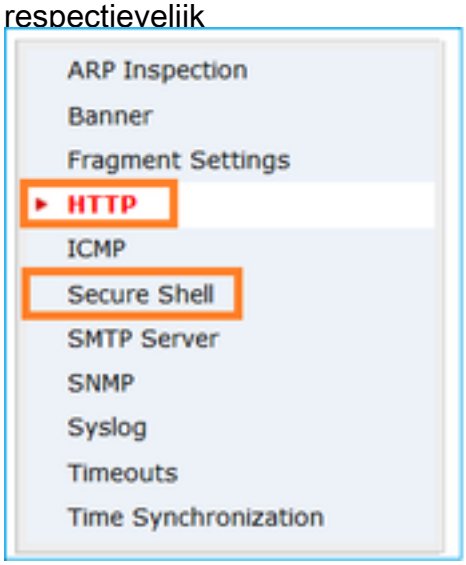
De Management interface is verdeeld in 2 logische interfaces: **br1** (**management0** op FPR2100/4100/9300 toestellen) en **diagnostiek:**



Doel	Beheer - **br1/management0** • Deze interface wordt gebruikt om de FTD IP toe te wijzen die wordt gebruikt voor	Beheer - **Diagnostiek** • Biedt externe toegang (bijvoorbeeld SNMP) tot ASA-engine.

	FTD/FMC-communicatie. • Hiermee wordt de vrijtunnel tussen FMC/FTD beëindigd. • Gebruikt als een bron voor op regels gebaseerde syslogs. • Biedt SSH- en HTTPS-toegang tot het FTD-vak.	• Gebruikt als bron voor LINA-niveau syslogs, AAA, SNMP etc. berichten.
Verplicht	**Ja**, omdat het wordt gebruikt voor FTD/FMC-communicatie (de sftunnel eindigt op hem)	**Nee** en het wordt niet aanbevolen vormen. De aanbeveling is een data-interface* (raadpleeg de onderstaande opmerking)

Configureren	Deze interface wordt geconfigureerd tijdens FTD-installatie (installatie).
	Later kunt u de br1 instellingen als volgt wijzigen:
	`>configure network ipv4 manual 10.1.1.2 255.0.0.0 10.1.1.1`
	`Setting IPv4 network configuration.`
	`Network settings changed.`
	`>`
	Stap 2. Werk het FTD IP bij op het VCC.
	 
		De toegang tot de diagnostische interface kan worden gecontroleerd door FTD **Apparaten > Platform-instellingen > Secure Shell**
		en
		Apparaten > Platform-instellingen> HTTP respectieveliik
		 

Toegang beperken	• Standaard kan alleen de **beheerder** verbinding maken met de FTD br1 subinterface. • Om de toegang van SSH te beperken wordt gedaan met het gebruik van de CLISH CLI `> configure ssh-access-list 10.0.0.0/8`	

Verifiëren	Methode 1 - van FTD CLI:
	`> show network`
	`...`
		Methode 1 - van LINA CLI:
		`firepower# show interface ip brief`
		`..`

```
=======[ br1 ]=======
State : Enabled
Channels : Management & Events
Mode :
MDI/MDIX : Auto/MDIX
MTU : 1500
MAC Address : 18:8B:9D:1E:CA:7B
----------------------[ IPv4 ]-----
Configuration : Manual
Address : 10.1.1.2
Netmask : 255.0.0.0
Broadcast : 10.1.1.255
----------------------[ IPv6 ]-----
```

Methode 2 - Van FMC GUI

Apparaten > Apparaatbeheer > Apparaat > Beheer

```
Management1/1 192.168.1.1 YES unset up up

firepower# show run interface m1/1
!
interface Management1/1
management-only
nameif diagnostic
security-level 0
ip address 192.168.1.1 255.255.255.0
```

Methode 2 - Van FMC GUI

Navigeren naar **Apparaten > Apparaatbeheer,**

selecteer de knop **Bewerken** en navigeer naar **interfaces**

* fragment uit FTD 6.1 gebruikershandleiding.

Routed Mode Deployment

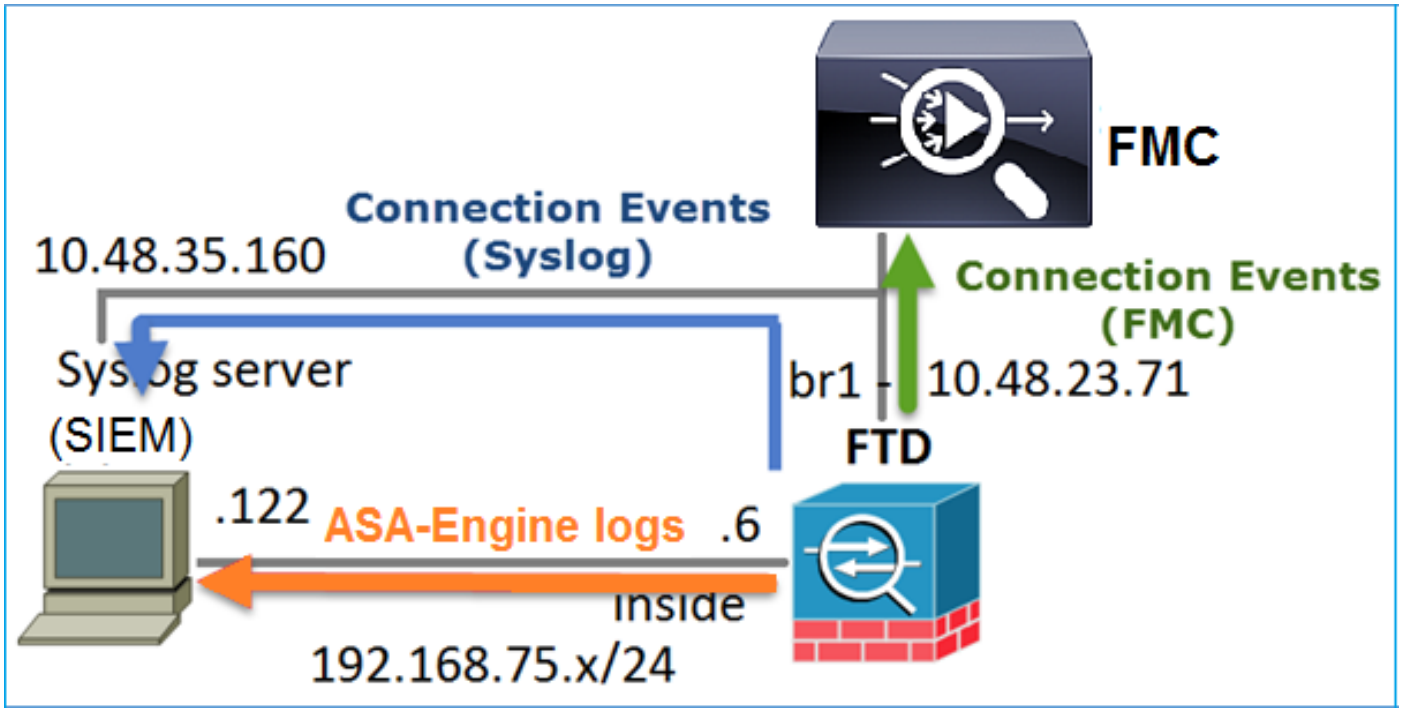
We recommend that you do *not* configure an IP address for the Diagnostic interface if you do not have an inside router. The benefit to leaving the IP address off of the Diagnostic interface is that you can place the Management interface on the same network as any other data interfaces. If you configure the Diagnostic interface, its IP address must be on the same network as the Management IP address, and it counts as a regular interface that cannot be on the same network as any other data interfaces. Because the Management interface requires Internet access for updates, putting Management on the same network as an inside interface means you can deploy the Firepower Threat Defense device with only a switch on the inside and point to the inside interface as its gateway. See the following deployment that uses an inside switch:

FTD-vastlegging

- Wanneer een gebruiker FTD-vastlegging configureren vanuit **Platforminstellingen,** genereert de FTD Syslog-berichten (hetzelfde als bij klassieke ASA) en kan deze elke Data-interface als bron gebruiken (inclusief de Diagnostic). Een voorbeeld van een syslogbericht dat in dat geval wordt gegenereerd:

```
May 30 2016 19:25:23 firepower : %ASA-6-302020: Built inbound ICMP connection for faddr
192.168.75.14/1 gaddr 192.168.76.14/0 laddr 192.168.76.14/0
```

- Aan de andere kant, wanneer de **regel-level logging van** Access Control Policy (ACS) is ingeschakeld, begint het FTD deze logs via de **br1** logische interface als bron. De logs zijn afkomstig van de FTD br1 subinterface:



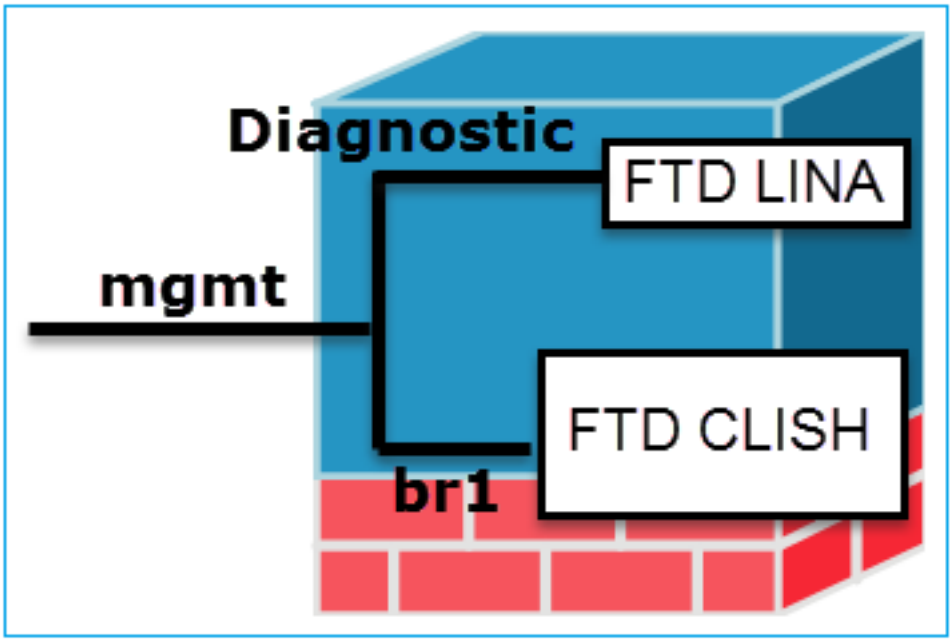
FTD beheren met FDM (on-box beheer)

Vanaf versie 6.1 kan een FTD die is geïnstalleerd op ASA5500-X-apparaten worden beheerd door FMC (off-box management) of door Firepower Device Manager (FDM) (on-box management).

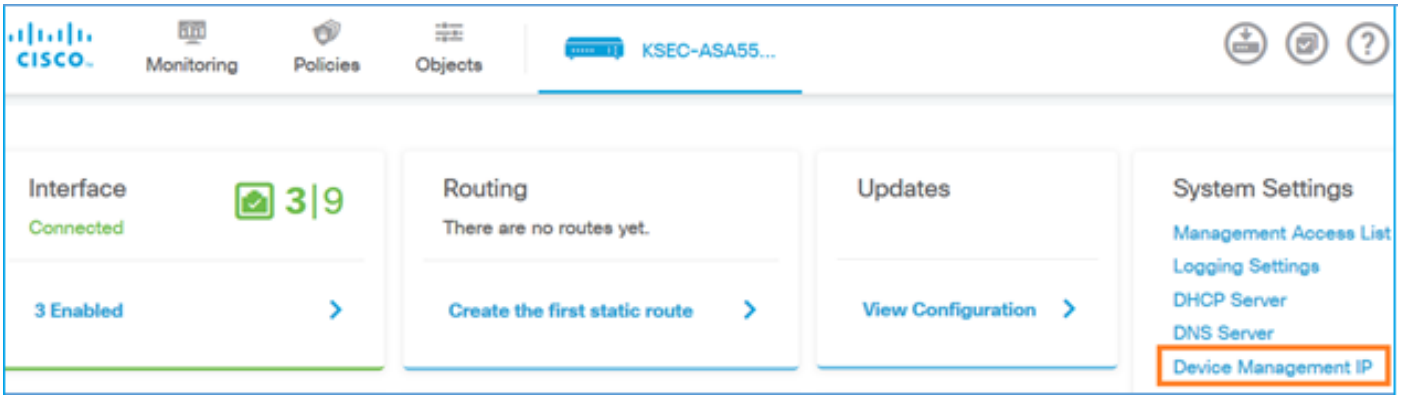
Uitvoer van FTD CLISH wanneer het apparaat wordt beheerd door FDM:

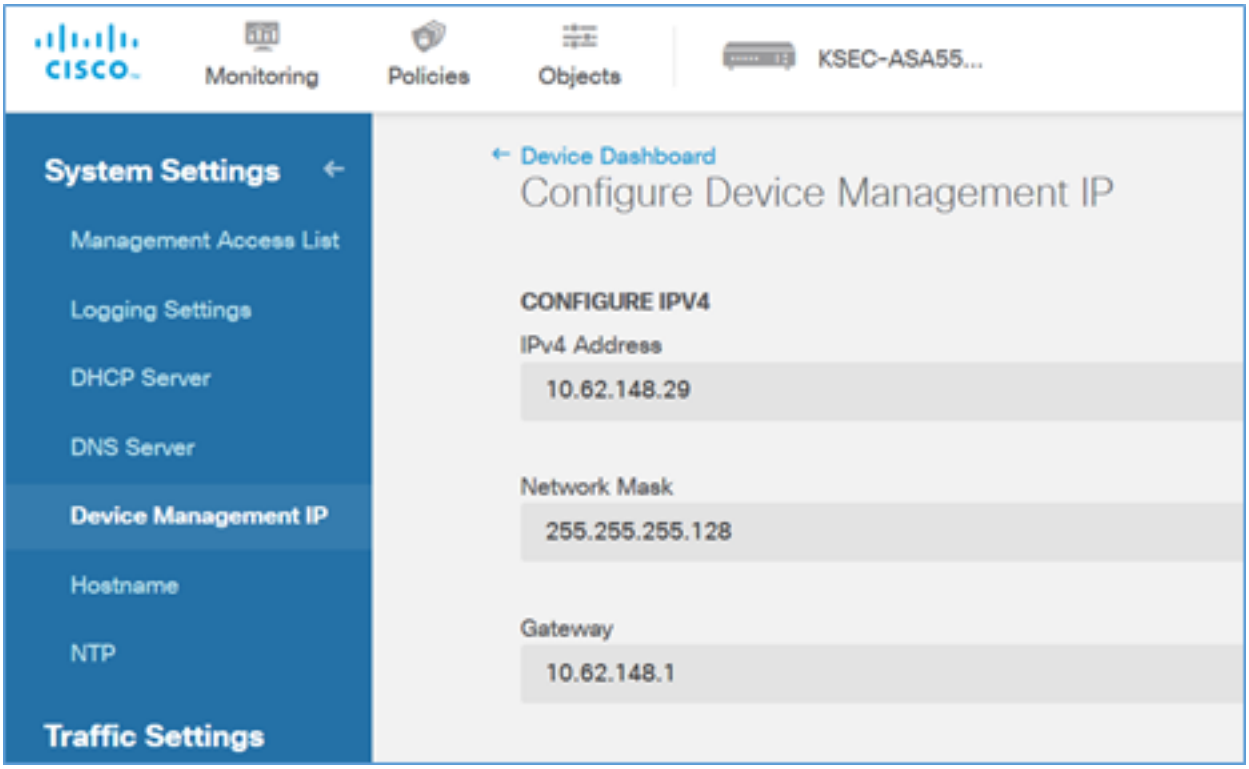
```
> show managers
Managed locally.
>
```

FDM het gebruikt de br1 logische interface. Dit kan worden gevisualiseerd als:



Vanuit de FDM UI is de beheerinterface toegankelijk via het **Dashboard apparaat > Systeeminstellingen > Apparaatbeheer IP**:





Beheerinterface op FTD Firepower hardware applicaties

FTD kan ook worden geïnstalleerd op FirePOWER 2100, 4100 en 9300 hardwareapparatuur. Het Firepower chassis draait zijn eigen OS genaamd FXOS terwijl de FTD is geïnstalleerd op een module/blade.

FPR21xx-apparaat

FPR41xx-apparaat

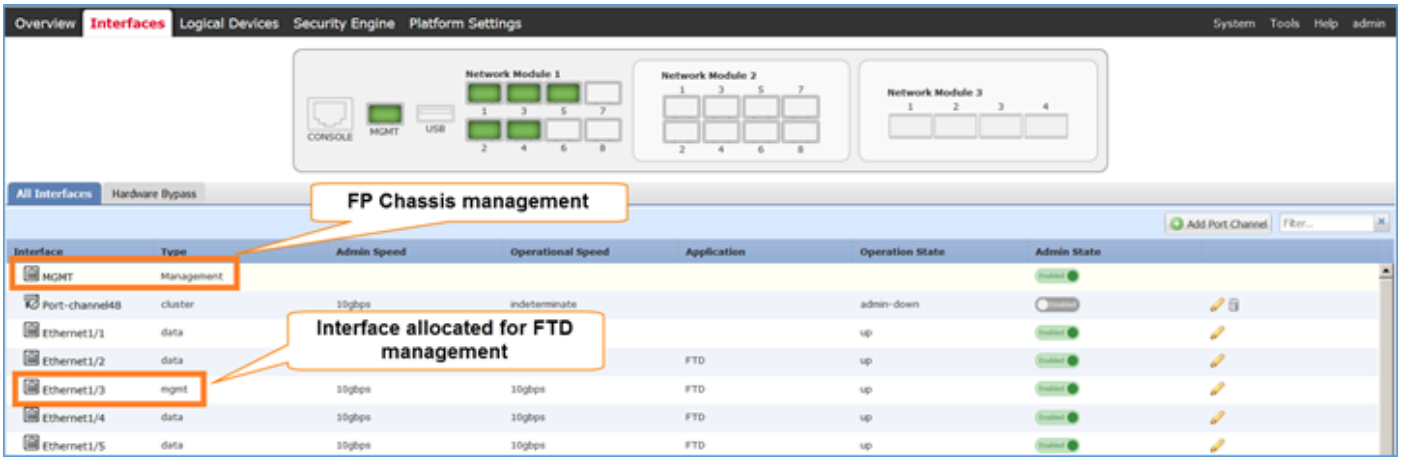
FPR9300 applicatie

Op FPR4100/9300 is deze interface alleen voor het chassisbeheer en kan niet worden gebruikt/gedeeld met de FTD-software die binnen de FP-module werkt. Voor de FTD-module een aparte data-interface toewijzen voor het FTD-beheer.

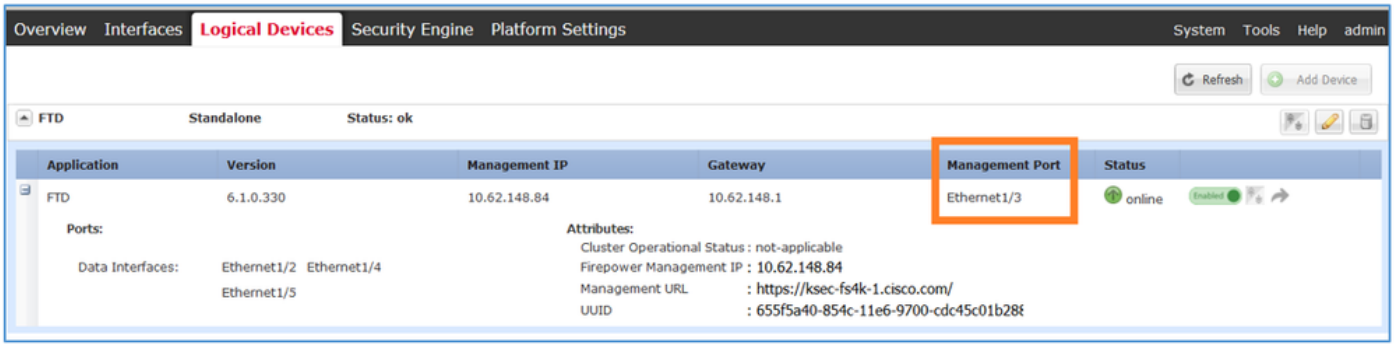
Op FPR2100 wordt deze interface gedeeld tussen het chassis (FXOS) en het logische FTD-apparaat:

```
> show network
===============[ System Information ]===============
Hostname                  : ftd623
Domains                   : cisco.com
DNS Servers               : 192.168.200.100
                            8.8.8.8
Management port           : 8305
IPv4 Default route
  Gateway                 : 10.62.148.129

==================[ management0 ]===================
State                     : Enabled
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 70:DF:2F:18:D8:00
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.62.148.179
Netmask                   : 255.255.255.128
Broadcast                 : 10.62.148.255
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

> connect fxos
Cisco Firepower Extensible Operating System (FX-OS) Software
...
firepower#
```

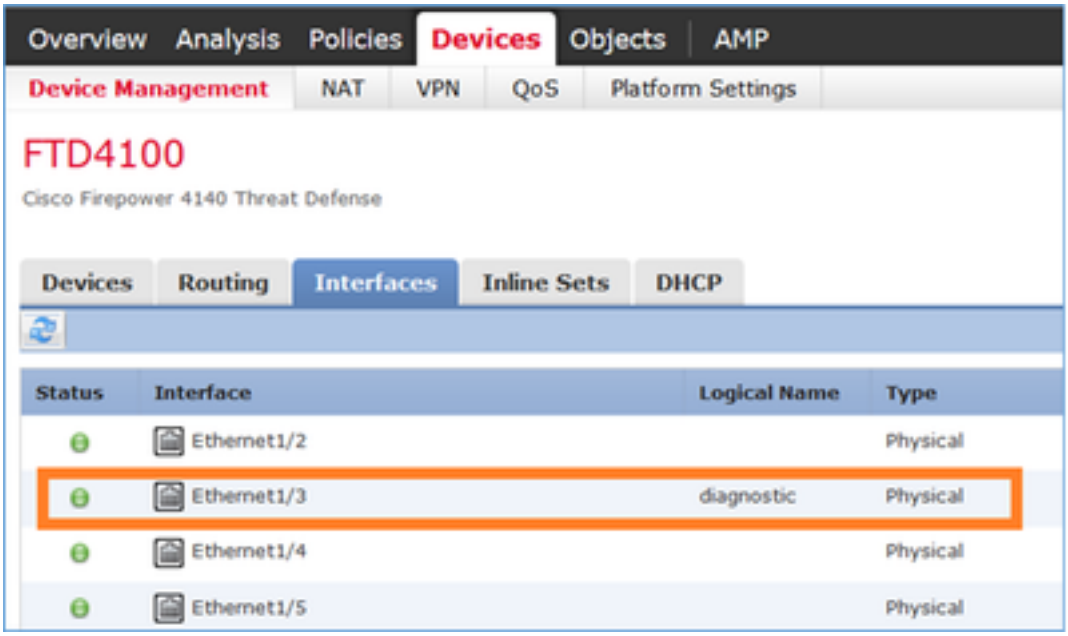
Deze screenshot is van de Firepower Chassis Manager (FCM) UI op FPR4100 waar een afzonderlijke interface voor FTD-beheer is toegewezen. In dit voorbeeld wordt Ethernet1/3 gekozen als de FTD-beheerinterface: p1



Dit is ook te zien op het tabblad **Logische apparaten**:p2



Op het VCC wordt de interface als **diagnostisch** weergegeven: p3



CLI-verificatie

```
FP4100# connect module 1 console
Firepower-module1>connect ftd
Connecting to ftd console... enter exit to return to bootCLI
>
> show interface
… output omitted …

Interface Ethernet1/3 "diagnostic", is up, line protocol is up
```

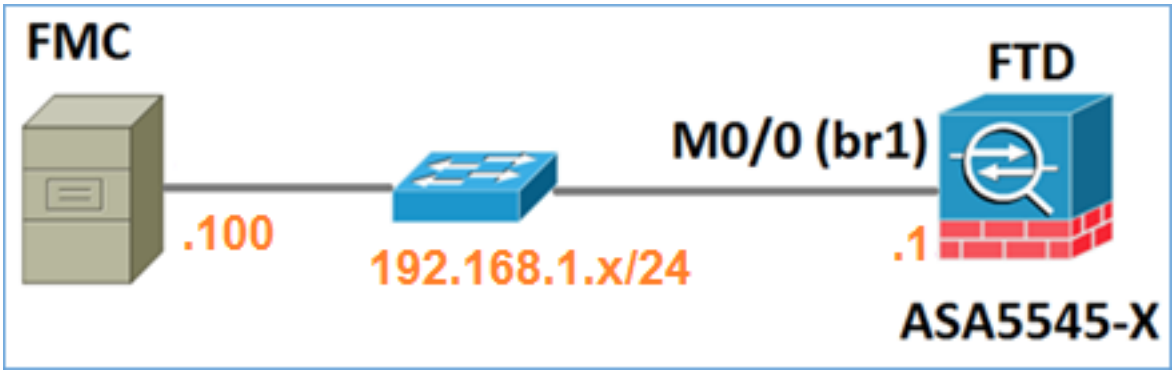
```
  Hardware is EtherSVI, BW 10000 Mbps, DLY 1000 usec
        MAC address 5897.bdb9.3e0e, MTU 1500
        IP address unassigned
  Traffic Statistics for "diagnostic":
        1304525 packets input, 63875339 bytes
        0 packets output, 0 bytes
        777914 packets dropped
      1 minute input rate 2 pkts/sec,  101 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 1 pkts/sec
      5 minute input rate 2 pkts/sec,  112 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 1 pkts/sec
        Management-only interface. Blocked 0 through-the-device packets

… output omitted …
>
```

FTD integreren met het VCC - Managementscenario's

Dit zijn enkele van de implementatieopties die het mogelijk maken om FTD te beheren die op ASA 5500-X-apparaten van FMC loopt.

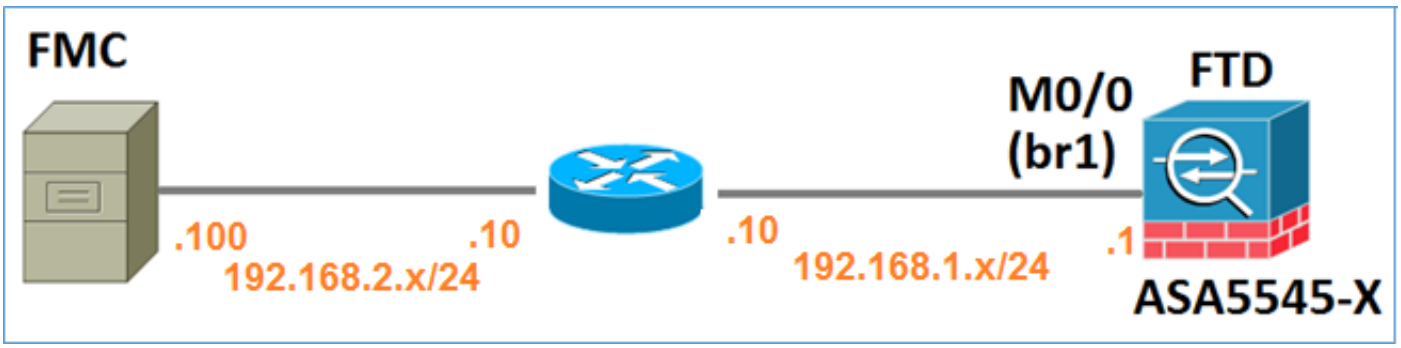
Scenario 1. FTD en FMC op hetzelfde substraat.

Dit is de eenvoudigste implementatie. Zoals in de afbeelding is te zien, bevindt het VCC zich in hetzelfde subnetgebied als de FTD br1-interface:



Scenario 2. FTD en FMC op verschillende subnetten. De stuurvlakken gaan niet door de FTD.

Bij deze inzet moet het FTD een route naar het VCC hebben en omgekeerd. Op FTD is de volgende hop een L3 apparaat (router):



Gerelateerde informatie

- Firepower System release opmerkingen, versie 6.1.0
- Installatie van een nieuwe installatiekopie voor Cisco ASA of FirePOWER Threat Defence Device
- Cisco Firepower Threat Defense Configuration Guide voor Firepower Device Manager, versie 6.1
- Technische ondersteuning en documentatie – Cisco Systems

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.