Konfigurieren der Managementschnittstelle für Firepower Threat Defense (FTD)

Inhalt

Einleitung

In diesem Dokument werden der Betrieb und die Konfiguration der Managementschnittstelle für Firepower Threat Defense (FTD) beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

- FTD auf ASA5508-X-Hardware-Appliance
- FTD auf ASA5512-X-Hardware-Appliance
- FTD, die auf der FPR9300-Hardware-Appliance ausgeführt wird
- FMC, das auf 6.1.0 läuft (Build 330)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

FTD ist ein einheitliches Software-Image, das auf folgenden Plattformen installiert werden kann:

- ASA 5506-X, ASA 5506W-X, ASA 5506H-X, ASA 5508-X, ASA 5516-X
- ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X
- FPR4100, FPR9300
- VMware (ESXi)
- Amazon Web Services (AWS)
- KVM
- ISR-Router-Modul

Dieses Dokument soll Folgendes veranschaulichen:

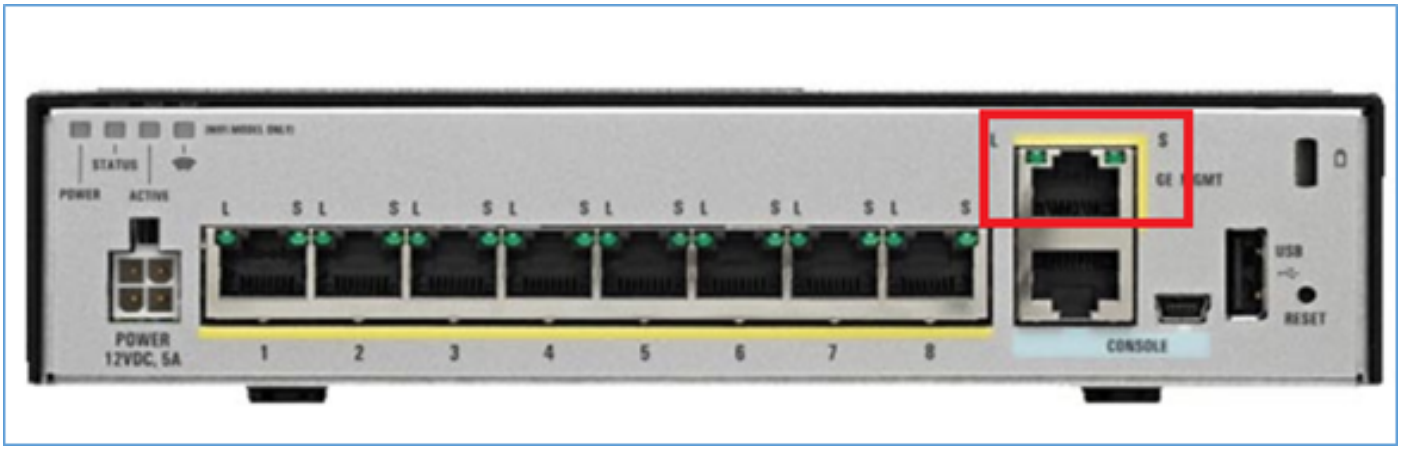
- FTD-Management-Schnittstellenarchitektur auf ASA5500-X-Geräten
- FTD-Management-Schnittstelle bei Verwendung von FDM
- FTD-Verwaltungsschnittstelle der Serie FP41xx/FP9300
- FTD/FirePOWER MANAGEMENT CENTER (FMC)-Integrationsszenarien

Konfigurieren

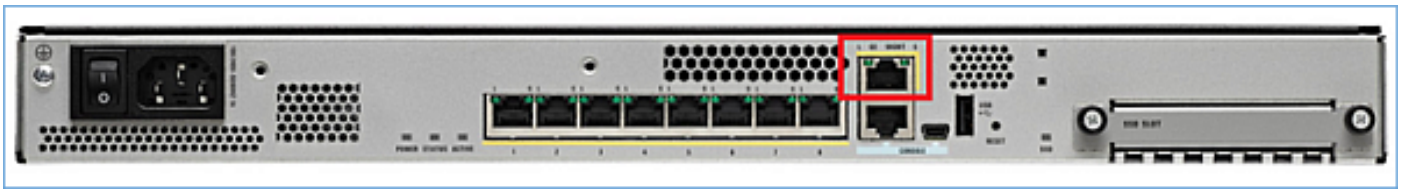
Verwaltungsschnittstelle auf ASA 5500-X-Geräten

Die Management-Schnittstelle von ASA5506/08/16-X- und ASA5512/15/25/45/55-X-Geräten.

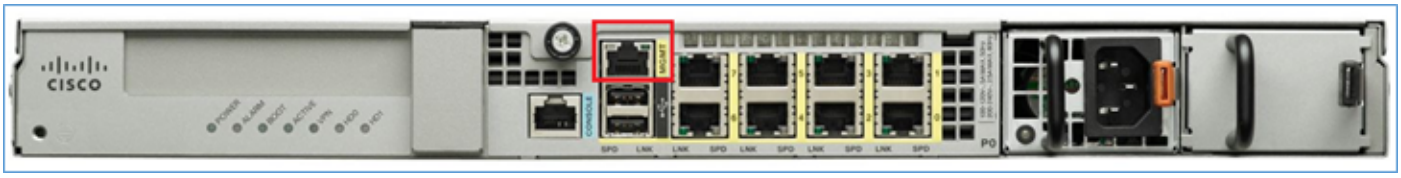
Dies ist das Image der ASA5506-X:



Dies ist das Image der ASA5508-X:



Dies ist das Image der ASA5555-X:



Wenn ein FTD-Image auf 5506/08/16 installiert ist, wird die Verwaltungsschnittstelle als **Management1/1** angezeigt. Auf 5512/15/25/45/55-X-Geräten wird dies zu **Management0/0.** Von der FTD-Befehlszeilenschnittstelle (CLI) kann dies in der **show tech-show unterstützen**.

Stellen Sie eine Verbindung zur FTD-Konsole her, und führen Sie den folgenden Befehl aus:

```
> 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
```

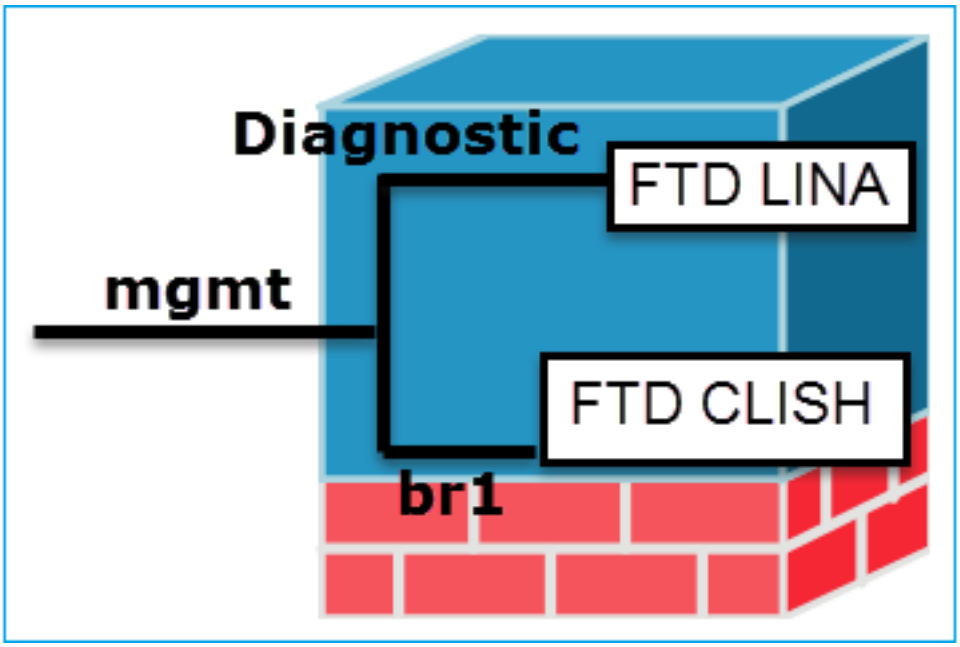
ASA 5512-X:

```
> 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
```

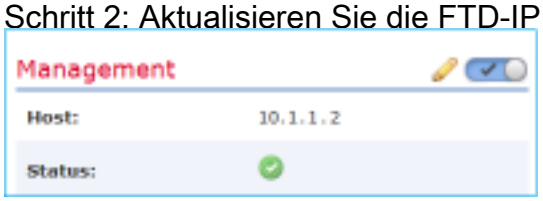
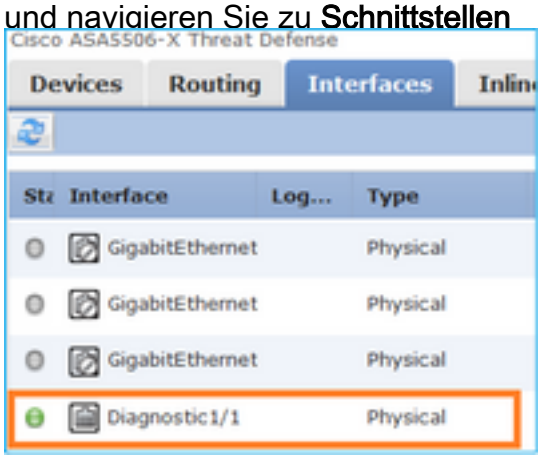
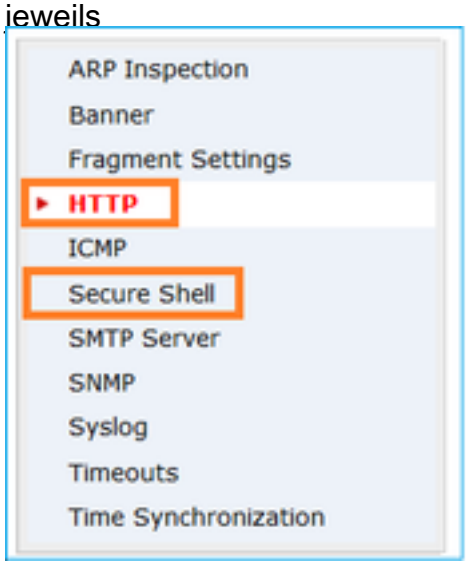
Architektur der Management-Schnittstelle

Die Management-Schnittstelle ist in zwei logische Schnittstellen unterteilt: **br1** (**management0** auf FPR2100/4100/9300-Appliances) und **Diagnose:**



	Verwaltung - **br1/management0**	Management - **Diagnose**
Zweck	• Diese Schnittstelle wird verwendet, um die FTD-IP zuzuweisen, die für die FTD/FMC-Kommunikation verwendet wird.	• Bietet Remote-Zugriff (z. B. SNMP) auf die ASA-Engine. • Wird als Quelle für LINA-Syslogs,

	• Beendet den Sftunnel zwischen FMC/FTD. • Wird als Quelle für regelbasierte Syslogs verwendet. • SSH- und HTTPS-Zugriff auf die FTD-Box	AAA, SNMP usw. verwendet.
Mandatory (Obligatorisch)	**Ja**, da es für FTD/FMC-Kommunikation verwendet wird (der sftunnel endet darauf)	**Nein**, und es wird nicht empfohlen, konfigurieren. Es wird empfohlen, eine Datenschnittstelle statt* (siehe Hinweis unten)

Konfigurieren	Diese Schnittstelle wird bei der FTD-Installation (Einrichtung) konfiguriert.
	Später können Sie die br1-Einstellungen wie folgt ändern:
	
	`>configure network ipv4 manual 10.1.1.2 255.0.0.0 10.1.1.1`
	`Setting IPv4 network configuration.`
	`Network settings changed.`
	
	`>`
	Schritt 2: Aktualisieren Sie die FTD-IP auf FMC.
	 
	
		Die Schnittstelle kann konfiguriert werden. über die FMC-GUI:
		Navigieren Sie zu **Geräte > Geräteverwaltung,**
		Wählen Sie die Schaltfläche **Bearbeiten**, und navigieren Sie zu **Schnittstellen**
		 
		
		Der Zugriff auf die Diagnoseschnittstelle durch FTD steuerbar
		Geräte > Plattformeinstellungen > Secure Shell
		und
		Geräte > Plattformeinstellungen > HTTP
		jeweils
		 

Zugriff einschränken	• Standardmäßig kann nur der **Administrator** eine Verbindung zur FTD br1-Subschnittstelle herstellen. • Die Beschränkung des SSH-Zugriffs erfolgt mithilfe der CLISH-CLI. `> configure ssh-access-list 10.0.0.0/8`	

Überprüfung	Methode 1 - Von FTD CLI:
	
	`> show network`
	`...`
	`=======[ br1 ]=======`
	`State : Enabled`
	`Channels : Management & Events`
	`Mode :`
		Methode 1 - Von LINA CLI:
		
		`firepower# show interface ip brief`
		`..`
		`Management1/1 192.168.1.1 YES unset up up`
		
		`firepower# show run interface m1/1`
		`!`

```
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 - Von der FMC-GUI
Geräte > Gerätemanagement > Gerät > Management

```
interface Management1/1
management-only
nameif diagnostic
security-level 0
ip address 192.168.1.1 255.255.255.0
```

Methode 2 - Von der FMC-GUI
Navigieren Sie zu **Geräte > Geräteverwaltung,**
Wählen Sie die Schaltfläche **Bearbeiten**, und navigieren Sie zu **Schnittstellen.**

* Auszug aus FTD 6.1 Benutzerhandbuch.

Routed Mode Deployment

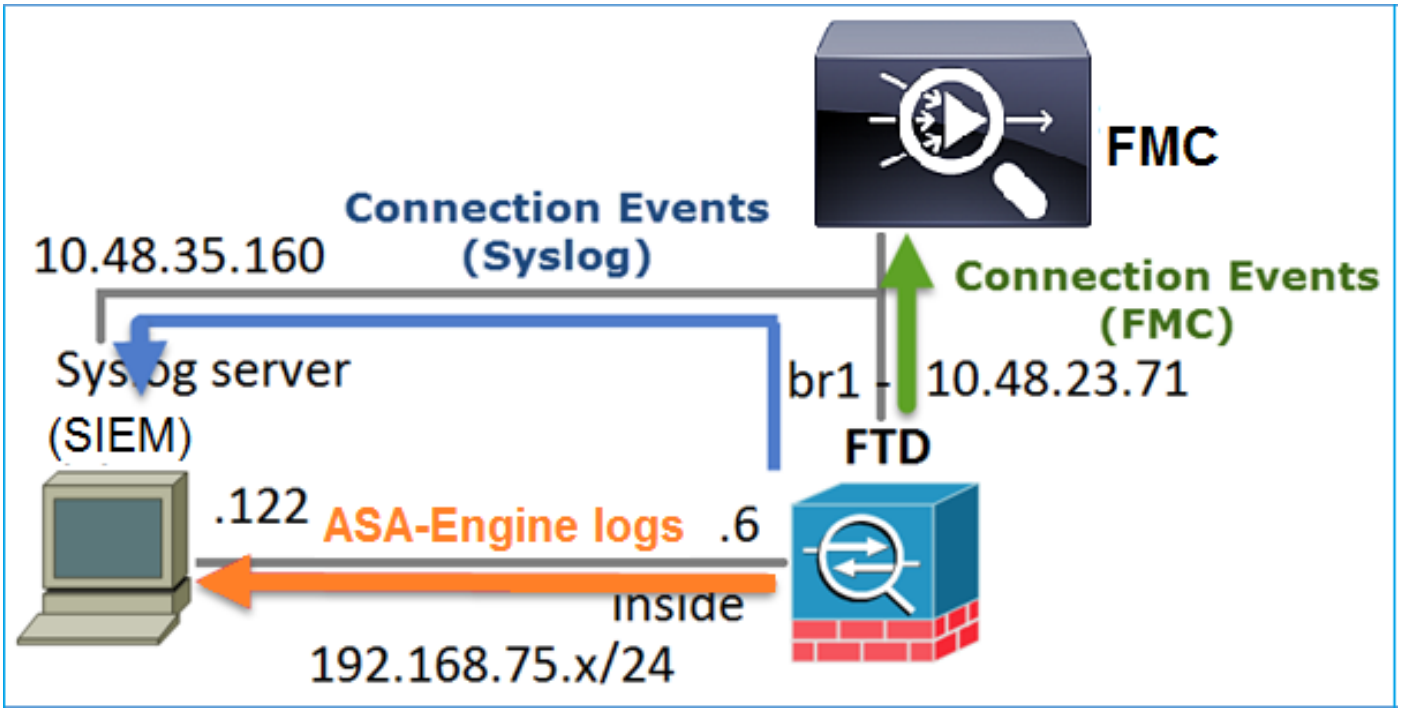
We recommend that you do *not* configure an IP address for the Diagnostic interface if you do not have an inside router. The benefit to leaving the IP address off of the Diagnostic interface is that you can place the Management interface on the same network as any other data interfaces. If you configure 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-Protokollierung

- Wenn ein Benutzer die FTD-Protokollierung über die **Plattformeinstellungen** konfiguriert, generiert die FTD Syslog-Meldungen (wie bei der klassischen ASA) und kann jede Datenschnittstelle als Quelle verwenden (einschließlich der Diagnose). Ein Beispiel für eine Syslog-Meldung, die in diesem Fall generiert wird:

```
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
```

- Wenn dagegen die **Protokollierung auf** der **Ebene der** Zugriffskontrollrichtlinien (ACP) auf **Regelebene** aktiviert ist, erstellt die FTD diese Protokolle über die logische **br1-**Schnittstelle als Quelle. Die Protokolle stammen von der FTD br1-Subschnittstelle:



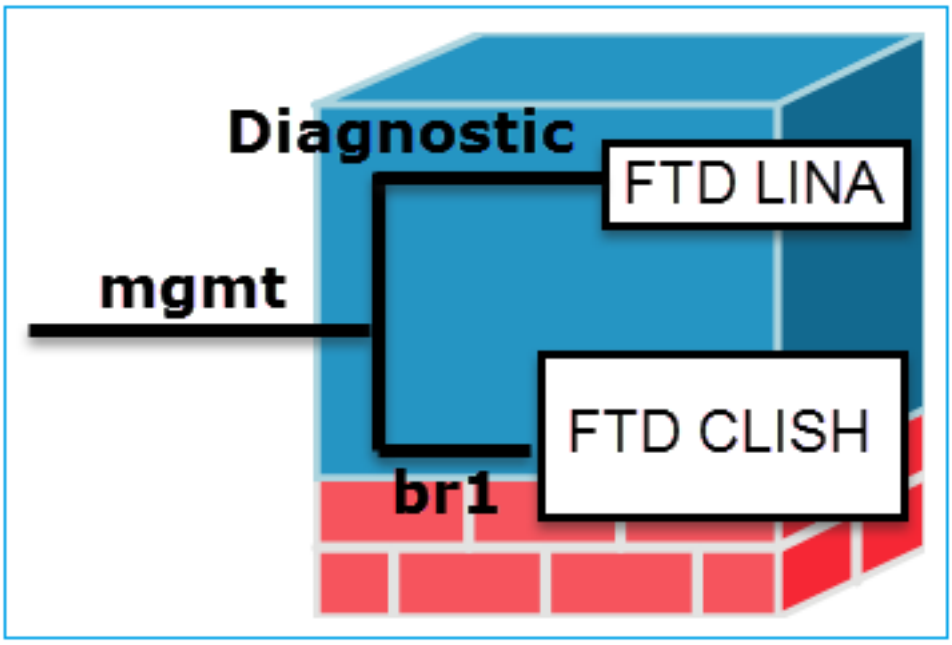
FTD-Management mit FDM (On-Box-Management)

Ab der Version 6.1 kann ein FTD, das auf ASA5500-X-Appliances installiert ist, entweder über FMC (externes Management) oder über FirePOWER Device Manager (FDM) (internes Management) verwaltet werden.

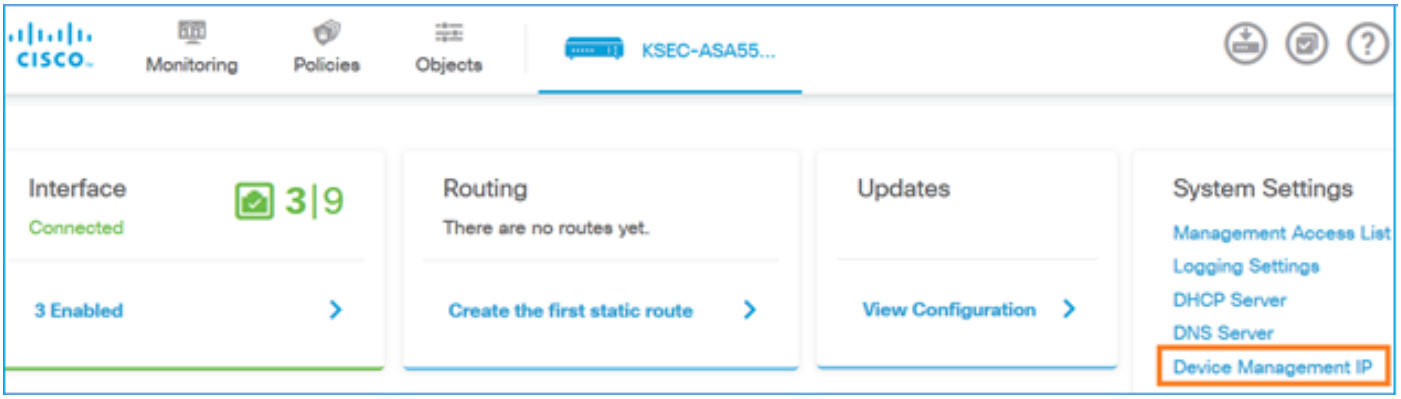
Ausgabe von FTD CLISH, wenn das Gerät von FDM verwaltet wird:

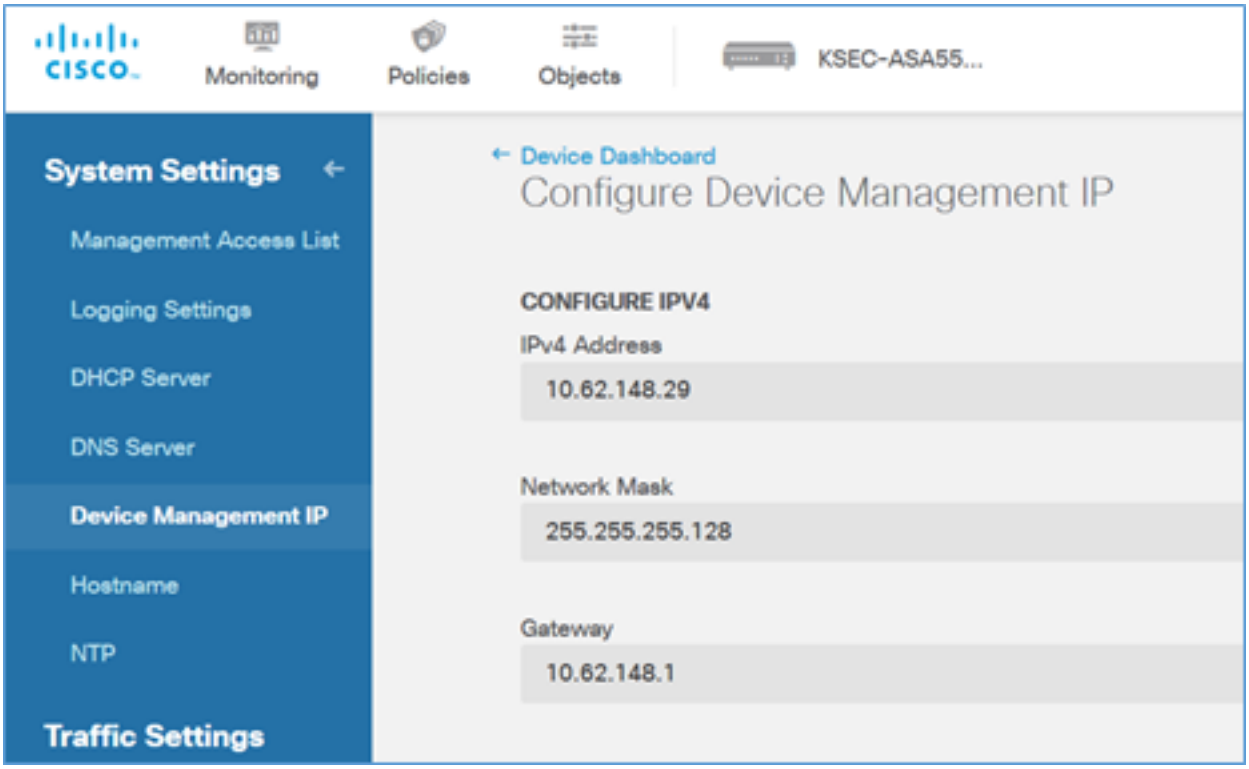
```
> show managers
Managed locally.
>
```

FDM verwendet die logische Schnittstelle br1. Dies kann wie folgt visualisiert werden:



Über die FDM-UI kann über das **Geräte-Dashboard > Systemeinstellungen > Geräte-Management-IP auf die** Verwaltungsschnittstelle zugegriffen werden:





Managementschnittstelle für FTD FirePOWER Hardware-Appliances

FTD kann auch auf Firepower 2100, 4100 und 9300 Hardware-Appliances installiert werden. Das FirePOWER-Chassis führt sein eigenes Betriebssystem FXOS aus, während das FTD auf einem Modul/Blade installiert ist.

FPR21xx-Appliance

FPR41xx-Appliance

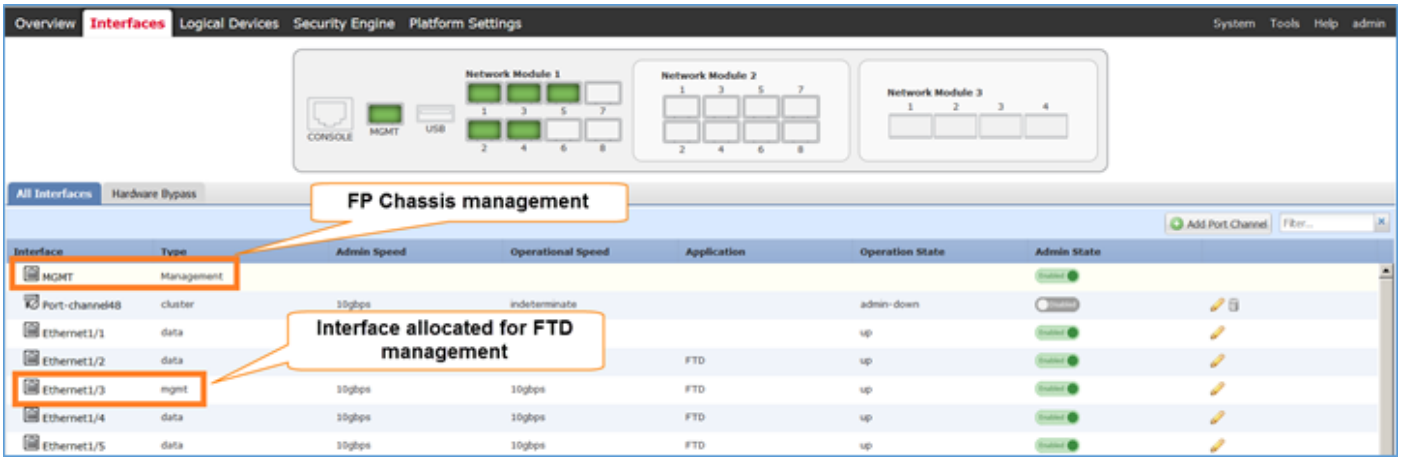
FPR9300-Appliance

Auf FPR4100/9300 ist diese Schnittstelle nur für das Chassis-Management vorgesehen und kann nicht mit der FTD-Software verwendet/gemeinsam genutzt werden, die innerhalb des FP-Moduls ausgeführt wird. Weisen Sie dem FTD-Modul eine separate Datenschnittstelle zu, die dem FTD-Management zugeordnet ist.

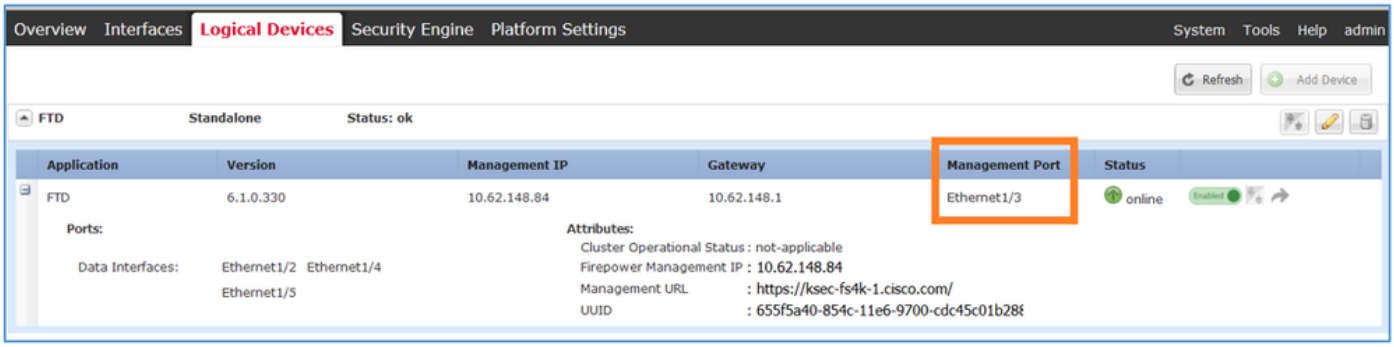
Auf FPR2100 wird diese Schnittstelle vom Chassis (FXOS) und der logischen FTD-Appliance gemeinsam genutzt:

```
> 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#
```

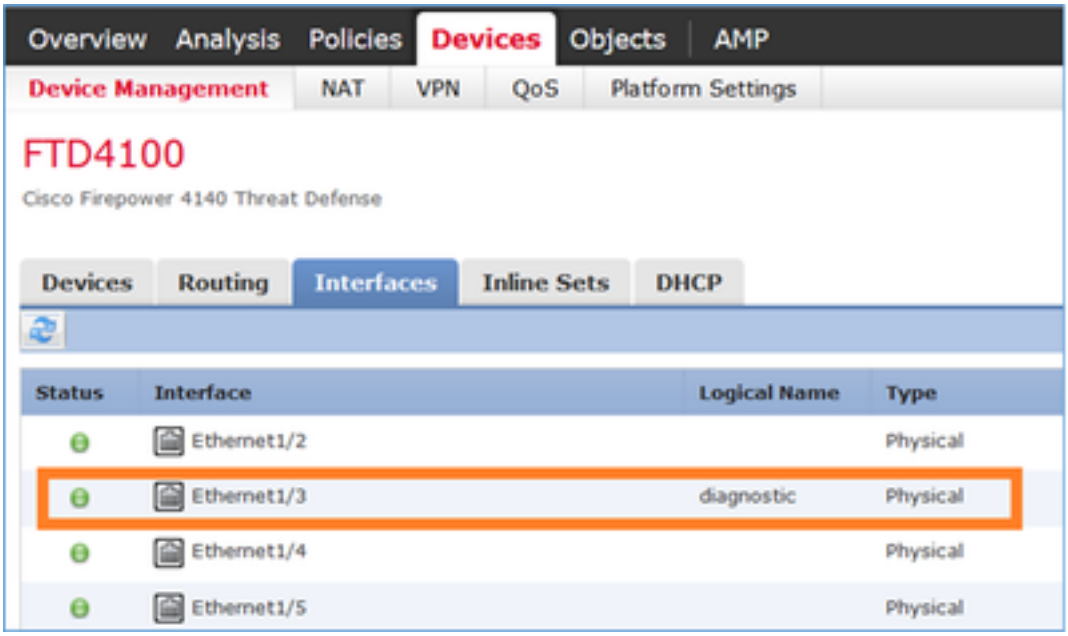
Dieser Screenshot stammt von der Benutzeroberfläche des Firepower Chassis Managers (FCM) auf dem FPR4100, der eine separate Schnittstelle für das FTD-Management zugewiesen ist. In diesem Beispiel wird Ethernet1/3 als FTD-Management-Schnittstelle ausgewählt: P1



Dies ist auch auf der Registerkarte "**Logische Geräte**" zu sehen:p2



Auf FMC wird die Schnittstelle als **Diagnose** angezeigt: p3



CLI-Überprüfung

```
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
```

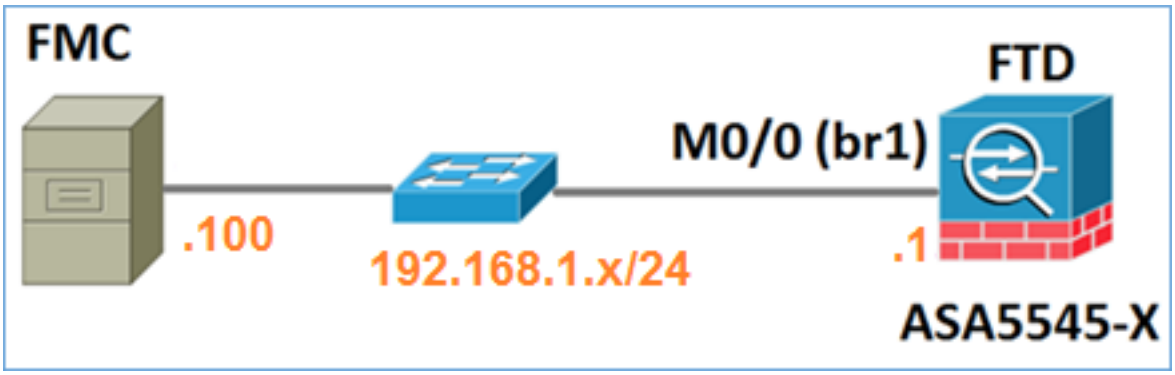
```
  Hardware is EtherSVI, BW 10000 Mbps, DLY 1000 usec
        MAC address 5897.bdb9.3e0e, MTU 1500
        IP address unassigned
  Traffic Statistics for "diagnostic":
        1304525 packets input, 63875339 bytes
        0 packets output, 0 bytes
        777914 packets dropped
      1 minute input 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 mit FMC integrieren - Verwaltungsszenarien

Dies sind einige der Bereitstellungsoptionen, mit denen FTD auf ASA5500-X-Geräten von FMC aus verwaltet werden kann.

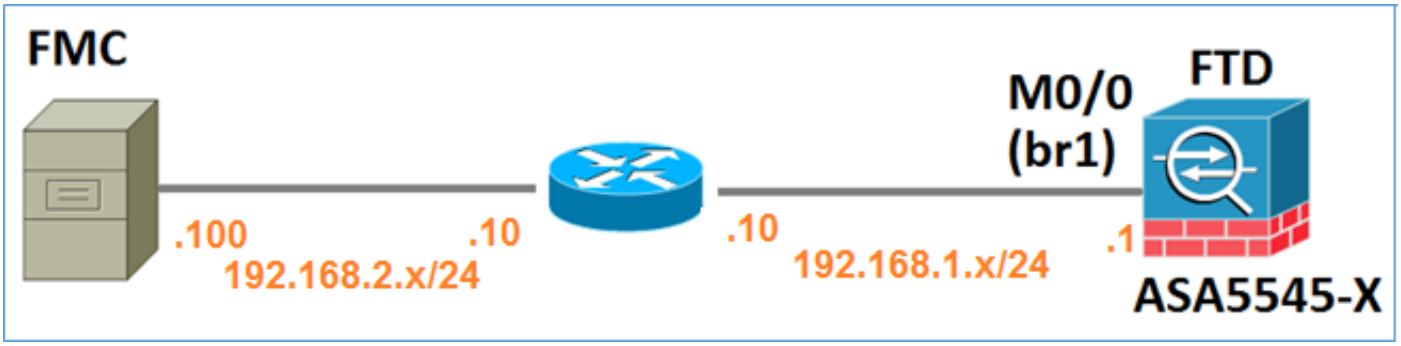
Szenario 1. FTD und FMC im gleichen Subnetz.

Dies ist die einfachste Bereitstellung. Wie aus der Abbildung ersichtlich, befindet sich das FMC im gleichen Subnetz wie die FTD br1-Schnittstelle:



Szenario 2. FTD und FMC auf verschiedenen Subnetzen. Die Kontrollebene geht nicht durch die FTD.

In dieser Bereitstellung muss die FTD eine Route zum FMC haben und umgekehrt. Auf FTD ist der nächste Hop ein L3-Gerät (Router):



Zugehörige Informationen

- Versionshinweise für FirePOWER-System, Version 6.1.0
- Neuerstellung der Cisco ASA oder des FirePOWER Threat Defense-Geräts
- Cisco Firepower Threat Defense - Konfigurationsleitfaden für Firepower Device Manager, Version 6.1
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.