FTD(Firepower Threat Defense) 관리 인터페이스 설정

목차

소개

이 문서에서는 FTD(Firepower Threat Defense)의 관리 인터페이스 작동 및 설정에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

- ASA5508-X 하드웨어 어플라이언스에서 실행되는 FTD
- ASA5512-X 하드웨어 어플라이언스에서 실행되는 FTD
- FPR9300 하드웨어 어플라이언스에서 실행되는 FTD
- 6.1.0에서 실행되는 FMC(빌드 330)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

FTD는 다음 플랫폼에 설치할 수 있는 통합 소프트웨어 이미지입니다.

- 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 라우터 모듈

이 문서의 목적은 다음을 입증하는 것입니다.

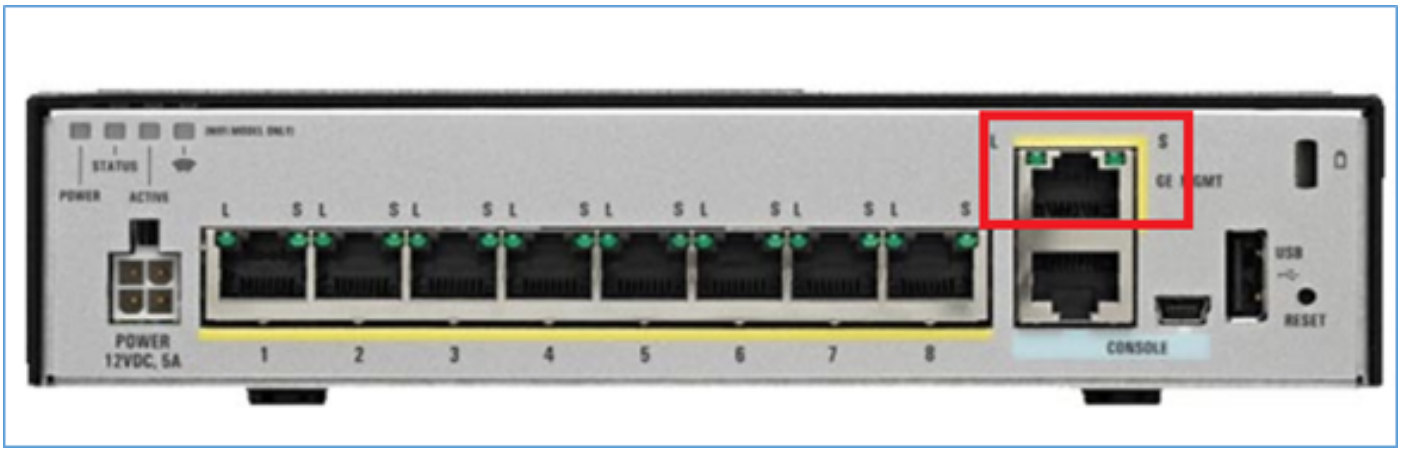
- ASA5500-X 디바이스의 FTD 관리 인터페이스 아키텍처
- FDM 사용 시 FTD 관리 인터페이스
- FP41xx/FP9300 Series의 FTD 관리 인터페이스
- FTD/FMC(Firepower 관리 센터) 통합 시나리오

구성

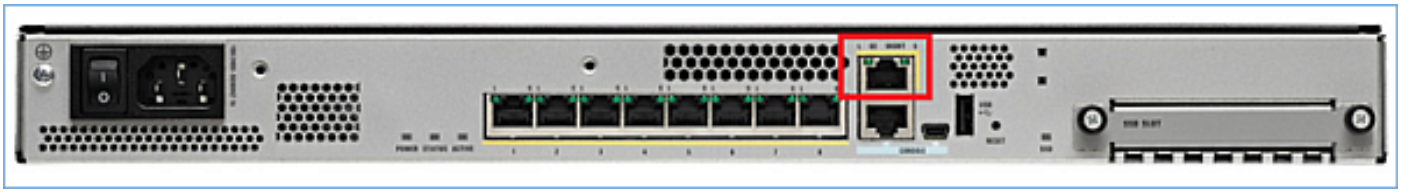
ASA 5500-X 디바이스의 관리 인터페이스

ASA5506/08/16-X 및 ASA5512/15/25/45/55-X 디바이스의 관리 인터페이스.

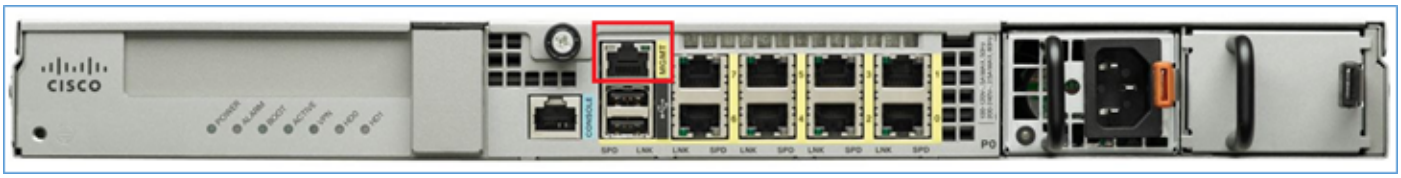
다음은 ASA5506-X의 이미지입니다.



다음은 ASA5508-X의 이미지입니다.



다음은 ASA555-X의 이미지입니다.



FTD 이미지가 5506/08/16에 설치된 경우 관리 인터페이스는 Management1/1로 표시됩니다. 5512/15/25/45/55-X 디바이스에서는 이 디바이스가 Management0/0이 됩니다. FTD CLI(Command Line Interface)에서 show tech-support 출력에서 이를 확인할 수 있습니다.

FTD 콘솔에 연결하고 다음 명령을 실행합니다.

```
<#root>

>

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
```

ASA5512-X

<#root>

>

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

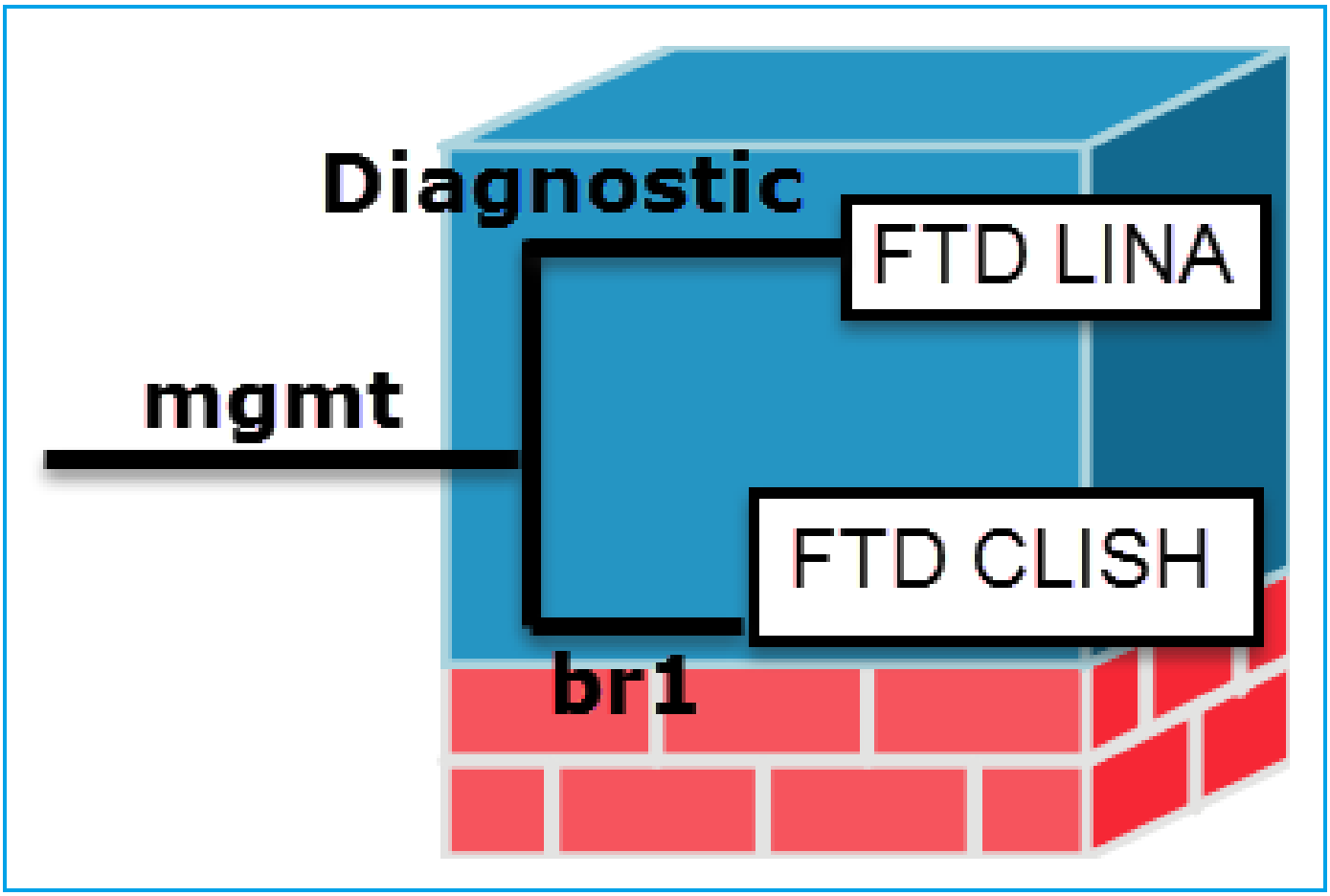
Encryption hardware device: Cisco ASA Crypto on-board accelerator (revision 0x1)
                            Boot microcode        : CNPx-MC-BOOT-2.00
                            SSL/IKE microcode     : CNPx-MC-SSL-SB-PLUS-0005
                            IPSec microcode       : CNPx-MC-IPSEC-MAIN-0026
                            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
```

관리 인터페이스 아키텍처

관리 인터페이스는 br1(FPR2100/4100/9300 어플라이언스의 management0) 및 진단 2개의 논리적 인터페이스로 나뉩니다.



	관리 - br1/management0	관리 - 진단
목적	• 이 인터페이스는 FTD/FMC 통신에 사용되는 FTD IP를 할당하기 위해 사용됩니다. • FMC/FTD 간의 sftunnel을 종료합니다. • 규칙 기반 syslog의 소스로 사용됩니다. • FTD 상자에 대한 SSH 및 HTTPS 액세스를 제공합니다.	• ASA 엔진에 대한 원격 액세스(예: SNMP)를 제공합니다. • LINA 레벨 syslogs, AAA, SNMP 등의 메시지의 소스로 사용됩니다.
필수	예, FTD/FMC 통신에 사용되므로 (sftunnel이 종료됩니다.)	아니요. 구성합니다. 권장 사항은 대신 데이터 인터페이스*(아래 참고 사항 확인)
구성	이 인터페이스는 FTD 설치(설정) 중에 구성됩니다. 나중에 다음과 같이 br1 설정을 수정할 수 있습니다. <#root>	인터페이스를 구성할 수 있습니다 fmc GUI에서: Devices(디바이스) > Device

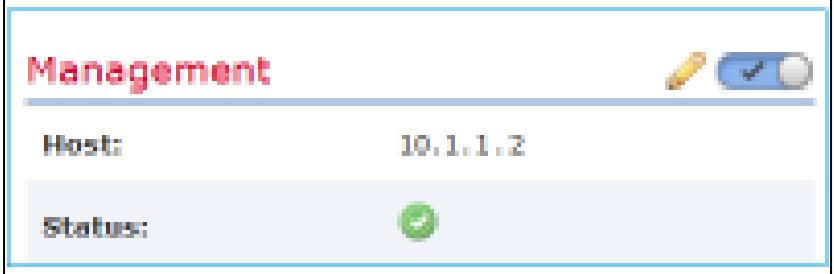
	>

```
configure network ipv4 manual 10.1.1.2 255.0.0.0 10.1.1.1

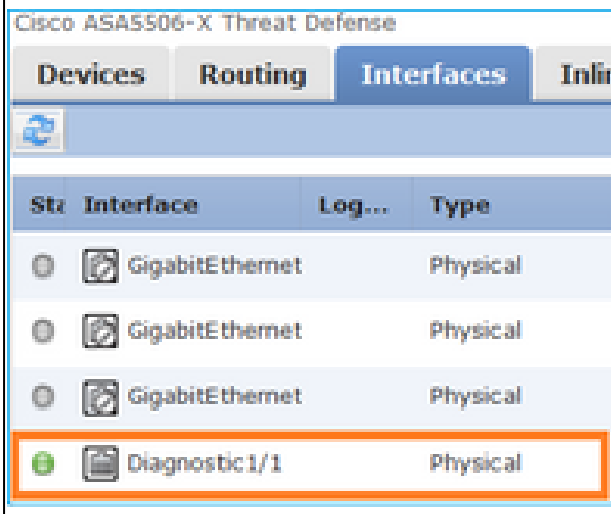
Setting IPv4 network configuration.
Network settings changed.

>
```

2단계. FMC에서 FTD IP를 업데이트합니다.


 | Management(디바이스 관리)로 이동합니다

Edit(편집) 버튼을 선택하고 Interfaces(인터페이스)로 이동합니다


 |
| 액세스 제한 | • 기본적으로 admin 사용자만 FTD br1 하위 인터페이스에 연결할 수 있습니다.
• SSH 액세스를 제한하려면 CLI를 사용합니다

```
> configure ssh-access-list 10.0.0.0/8
``` | 진단 인터페이스에 대한 액세스

FTD로 제어 가능

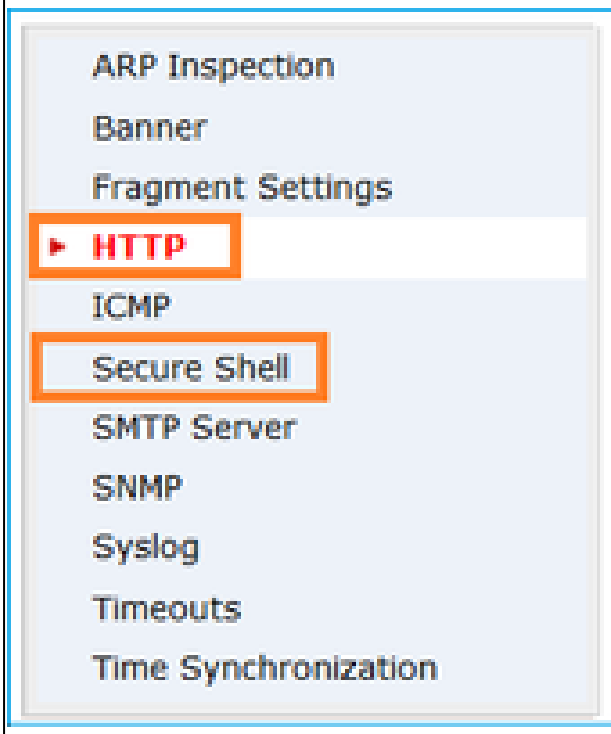
Devices(디바이스) > Platform Settings(플랫폼 설정) >

보안 셸

및

Devices(디바이스) > Platform Settings(플랫폼 설정) > HTTP

각각 |

<table>
<tr>
<td></td>
<td></td>
<td> 
</td>
</tr>
<tr>
<td>다음을 확인합니다.</td>
<td>방법 1 - FTD CLI에서:

<#root>

>

show network

...
=======[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]-----

방법 2 - FMC GUI에서

Devices > Device Management > Device > Management</td>
<td>방법 1 - LINA CLI에서

<#root>

firepower#

show interface ip brief

..
Management1/1 192.168.1.1 YES unset up u

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

방법 2 - FMC GUI에서

Devices(디바이스) > Device Management(디바이스 관리)로 이동합니다

edit(편집) 버튼을 선택하고 Interfaces(인터페이스)로 이동합니다</td>
</tr>
</table>

* FTD 6.1 사용 설명서에서 발췌한 내용.

Routed Mode Deployment

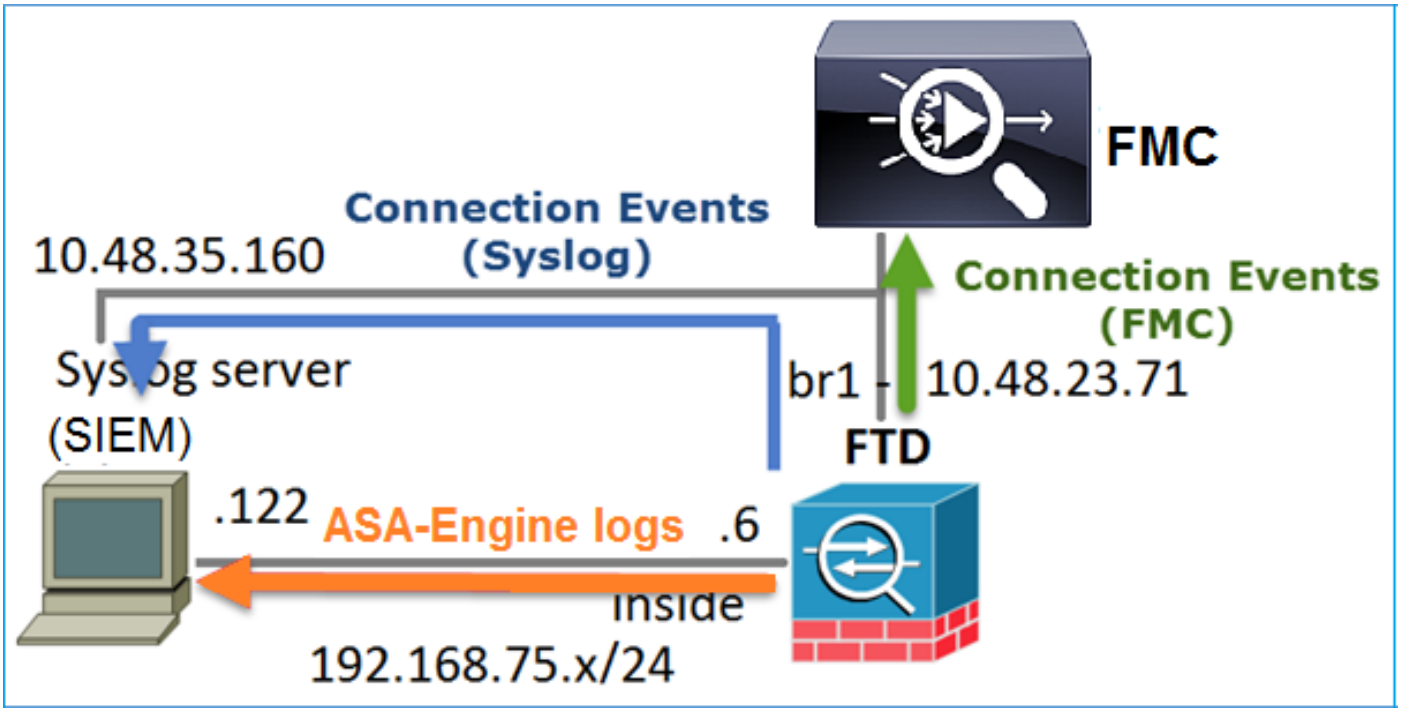
We recommend that you do *not* configure an IP address for the Diagnostic interface if you do not have an inside router. The benefit to leaving the IP address off of the Diagnostic interface is that you can place the Management interface on the same network as any other data interfaces. If you configure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

- 사용자가 플랫폼 설정에서 FTD 로깅을 구성하면 FTD는 Syslog 메시지(기존 ASA와 동일)를 생성하고 모든 데이터 인터페이스를 소스로 사용할 수 있습니다(진단 포함). 이 경우 생성되는 syslog 메시지의 예:

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

- 반면, ACP(Access Control Policy) 규칙 레벨 로깅이 활성화된 경우 FTD는 br1 논리적 인터페이스를 통해 이러한 로그를 소스로 시작합니다. 로그는 FTD br1 하위 인터페이스에서 시작합니다.



FDM으로 FTD 관리(온박스 관리)

firepower 6.1 버전부터 ASA5500-X 어플라이언스에 설치된 FTD는 FMC(Off-Box Management) 또는 FDM(Domain Device Manager)(On-Box Management)을 통해 관리할 수 있습니다.

FDM에서 디바이스를 관리하는 경우 FTD CLISH의 출력:

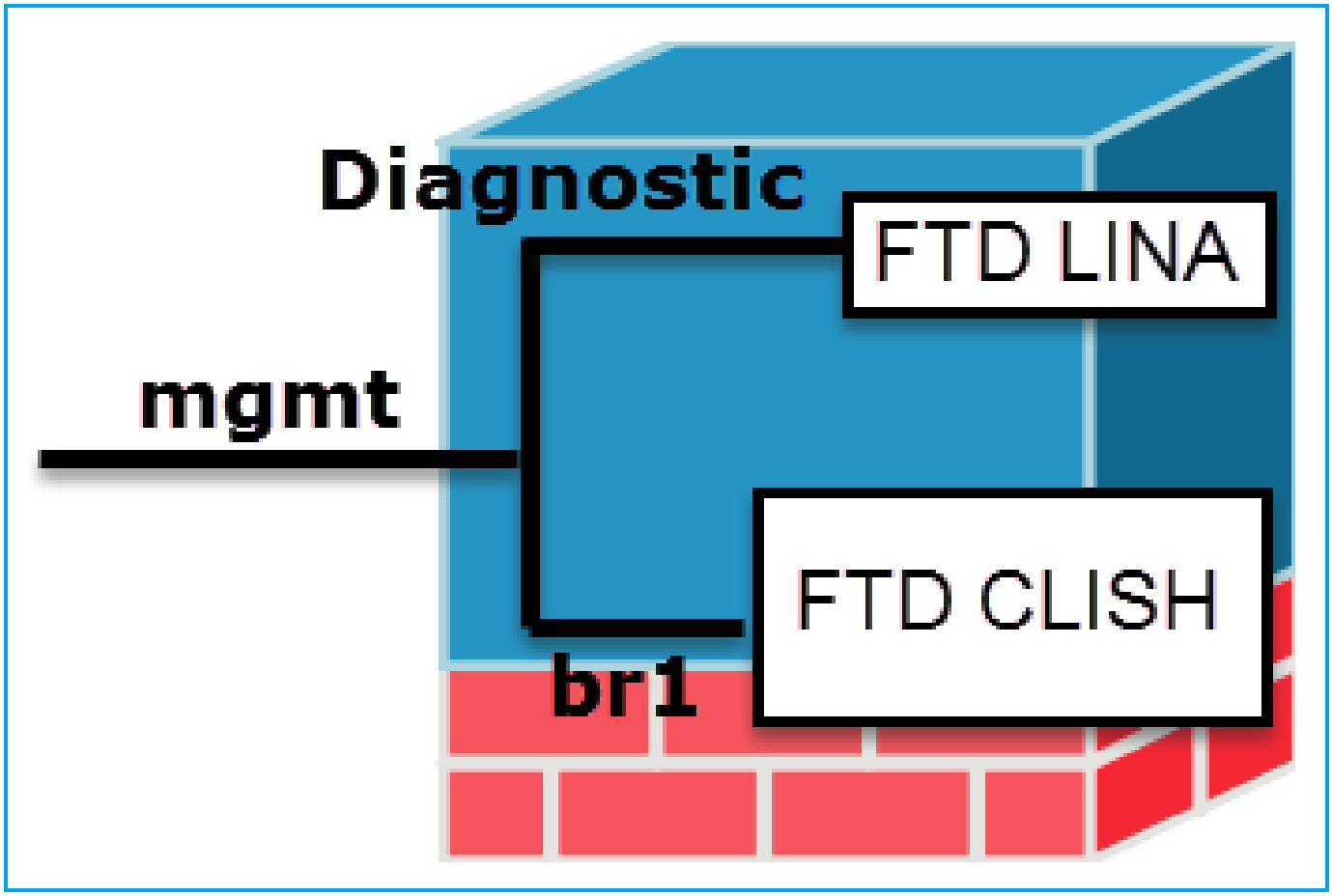
```
<#root>

>

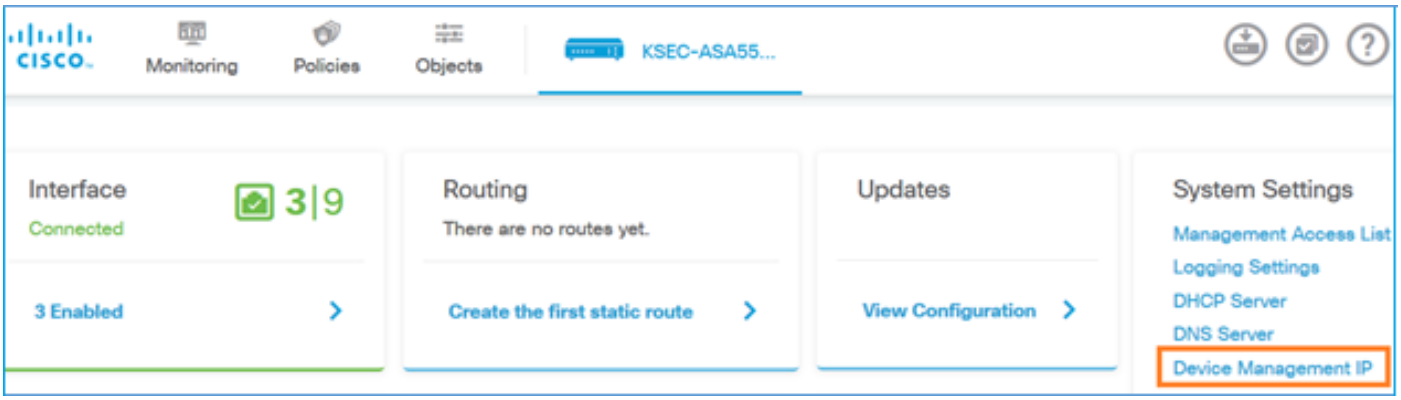
show managers

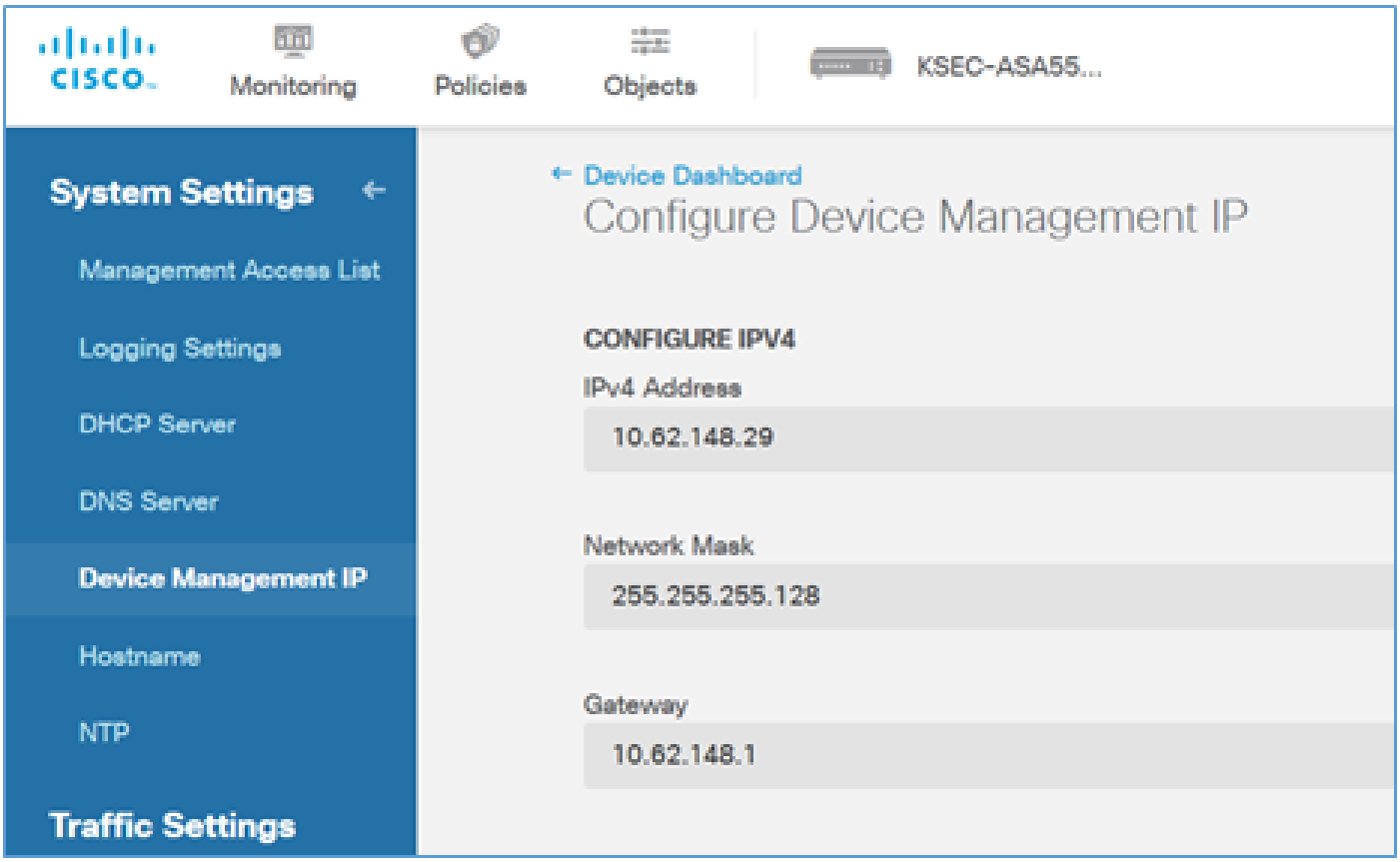
Managed locally.
>
```

FDM은 br1 논리적 인터페이스를 사용합니다. 이는 다음과 같이 시각화할 수 있습니다.



FDM UI에서 관리 인터페이스는 Device Dashboard(디바이스 대시보드) > System Settings(시스템 설정) > Device Management IP에서 액세스할 수 있습니다.





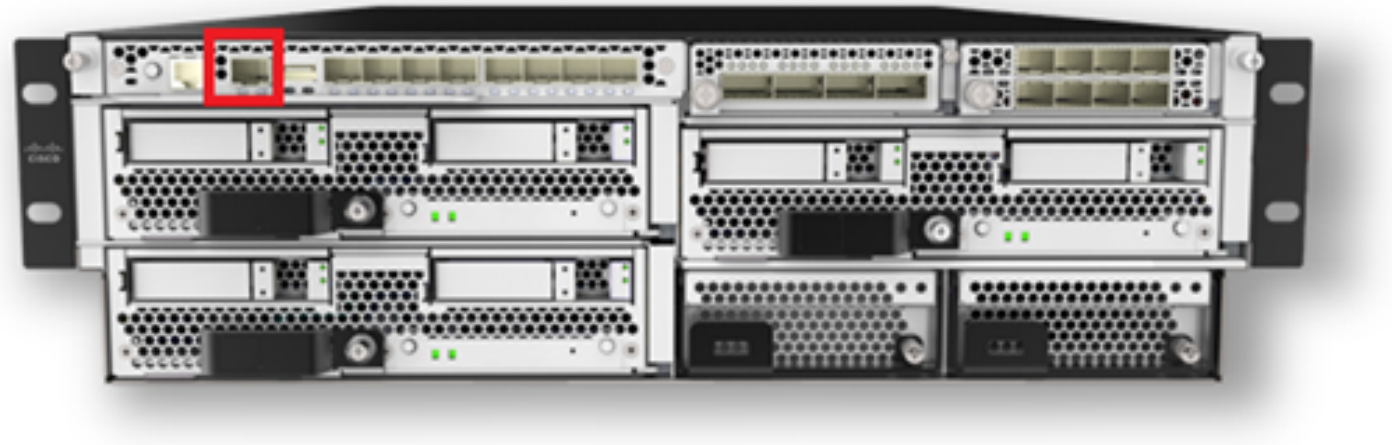
FTD Firepower 하드웨어 어플라이언스의 관리 인터페이스

FTD는 Firepower 2100, 4100 및 9300 하드웨어 어플라이언스에도 설치할 수 있습니다. firepower 섀시는 FTD가 모듈/블레이드에 설치되는 동안 FXOS라는 자체 OS를 실행합니다.

FPR21xx 어플라이언스

FPR41xx 어플라이언스

FPR9300 어플라이언스



FPR4100/9300에서 이 인터페이스는 섀시 관리용으로만 사용되며 FP 모듈 내에서 실행되는 FTD 소프트웨어와 사용/공유할 수 없습니다. FTD 모듈의 경우 FTD 관리를 위한 별도의 데이터 인터페이스를 할당합니다.

FPR2100에서 이 인터페이스는 섀시(FXOS)와 FTD 논리적 어플라이언스 간에 공유됩니다.

<#root>

>

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

>
```

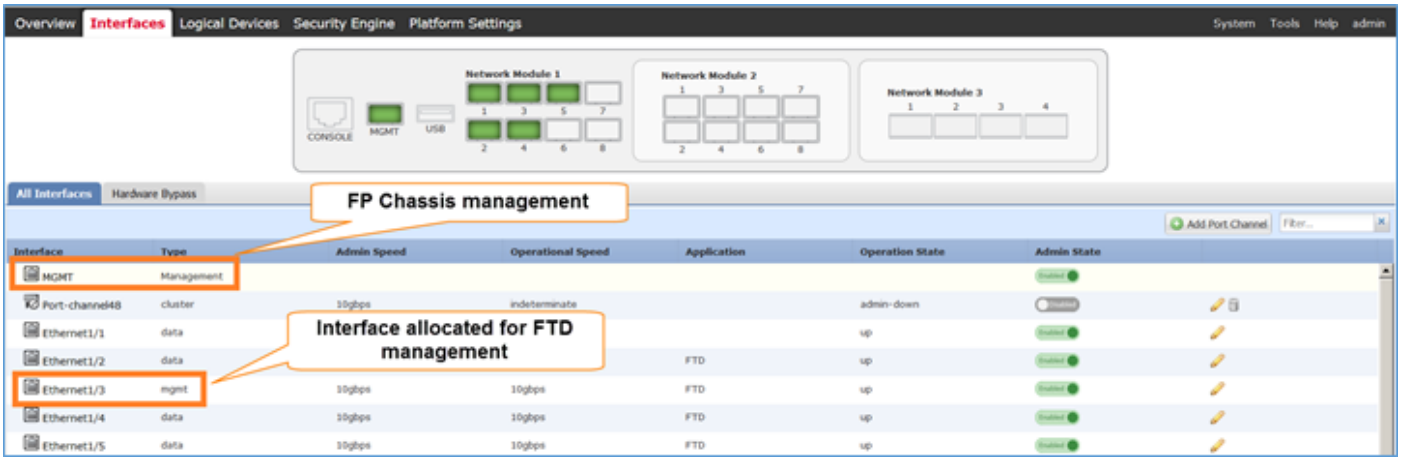
connect fxos

```
Cisco Firepower Extensible Operating System (
```

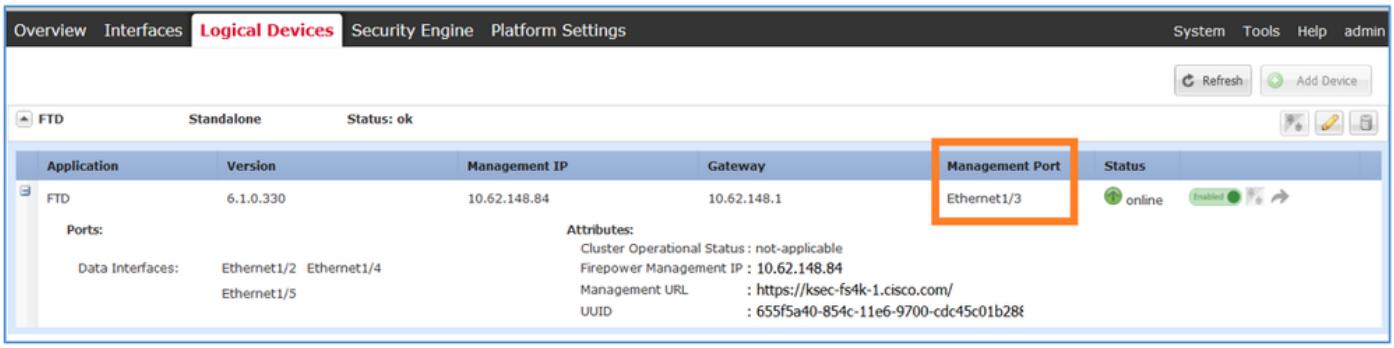
FX-OS

```
) Software
...
firepower#
```

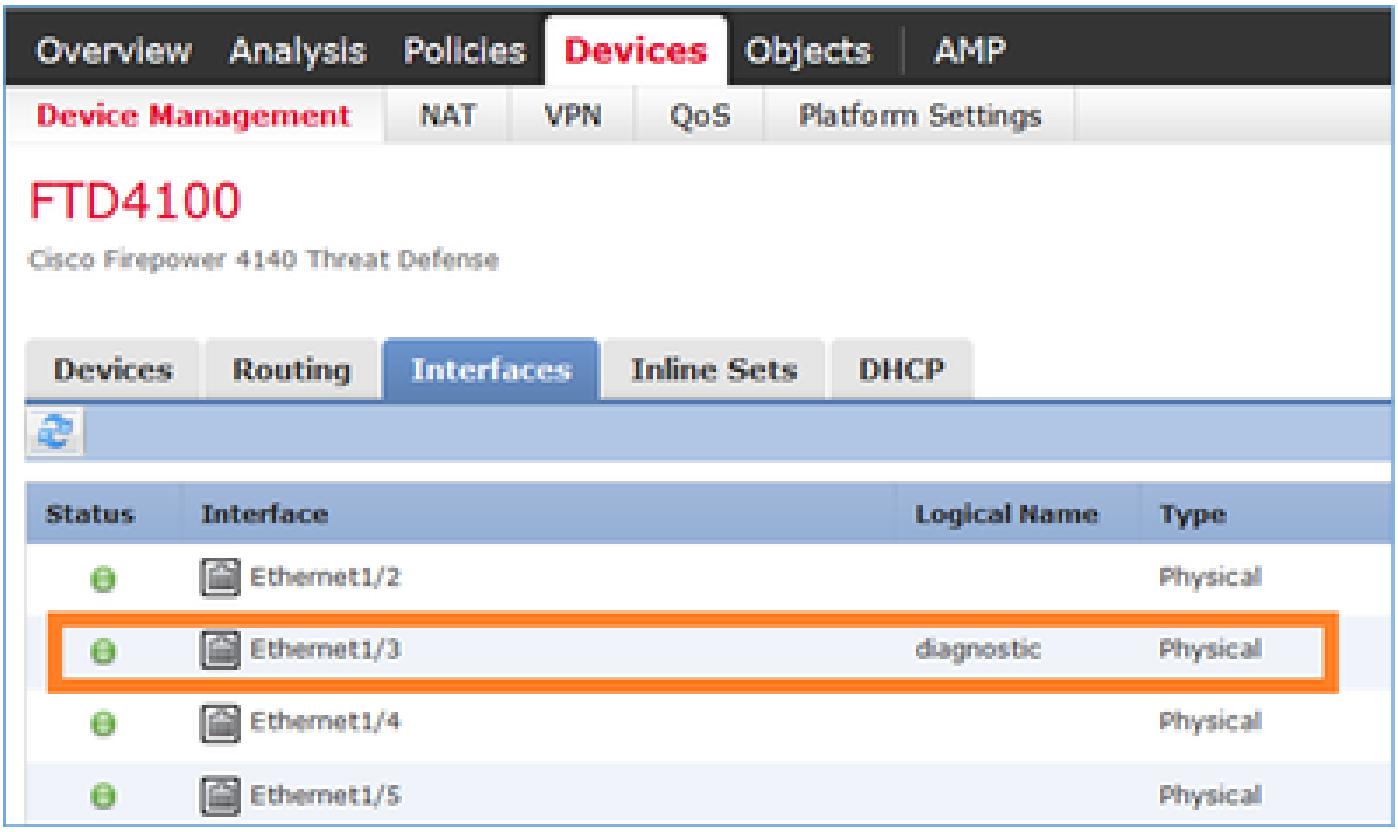
이 스크린샷은 FTD 관리를 위한 별도의 인터페이스가 할당된 FPR4100의 FCM(Firepower 섀시 관리자) UI에서 가져온 것입니다. 이 예에서는 Ethernet1/3이 FTD 관리 인터페이스(p1)로 선택됩니다



이는 Logical Devices 탭(p2)에서도 확인할 수 있습니다.



FMC에서는 인터페이스가 diagnostic으로 표시됩니다. p3



CLI 확인

<#root>

```
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

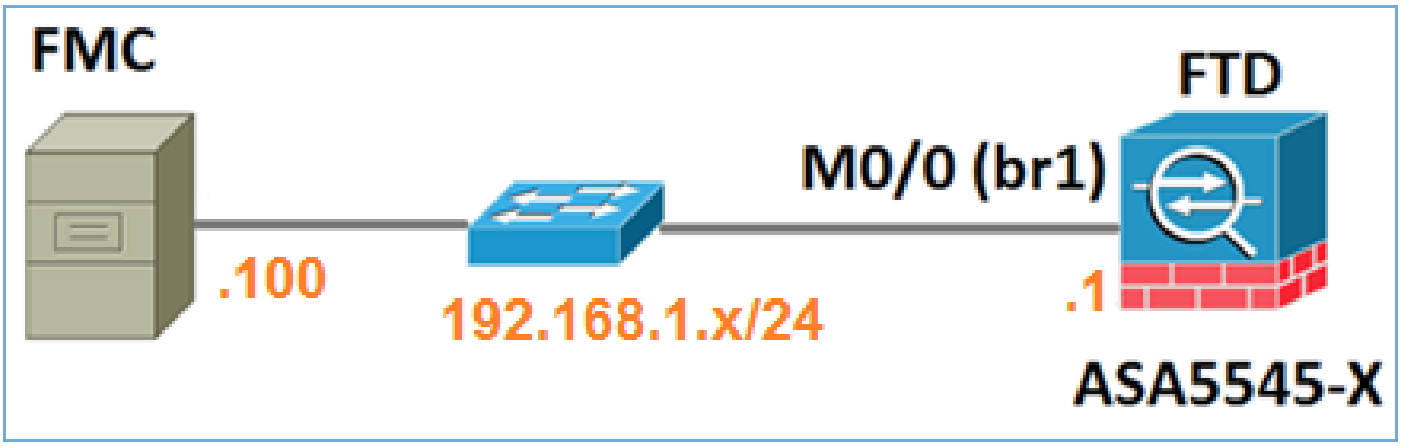
… output omitted …
>
```

FTD를 FMC와 통합 - 관리 시나리오

FMC에서 ASA5500-X 디바이스에서 실행되는 FTD를 관리할 수 있는 구축 옵션 중 일부입니다.

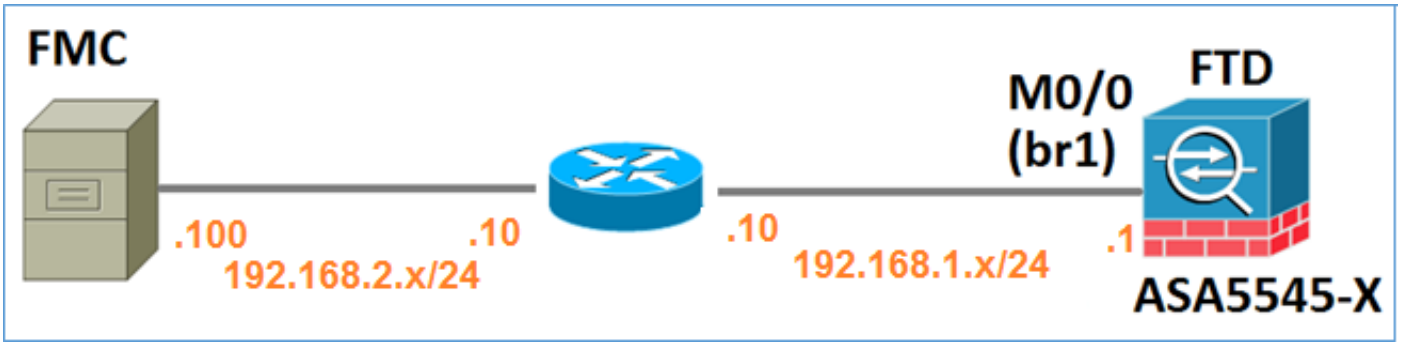
시나리오 1. FTD 및 FMC가 동일한 서브넷에 있습니다.

이는 가장 간단한 구축입니다. 그림에서 볼 수 있듯이 FMC는 FTD br1 인터페이스와 동일한 서브넷에 있습니다.



시나리오 2. FTD 및 FMC가 서로 다른 서브넷에 있습니다. 컨트롤 플레인은 FTD를 통과하지 않습니다.

이 구축에서는 FTD에 FMC로 향하는 경로가 있어야 하며 그 반대의 경우도 마찬가지입니다. FTD에서 다음 홉은 L3 디바이스(라우터)입니다.



관련 정보

- [Firepower 시스템 릴리스 정보, 버전 6.1.0]

- Cisco ASA 또는 Firepower 위협 방어 디바이스 재이미지화
- firepower 디바이스 관리자용 Cisco Firepower Threat Defense 컨피그레이션 가이드, 버전 6.1
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.