تكوين واجهة إدارة الدفاع ضد تهديدات Firepower (FTD)

المحتويات

المقدمة

يصف هذا المستند عملية تشغيل واجهة الإدارة وتكوينها على Cisco Secure Firewall Threat Defense (المعروف رسميا باسم Firepower Threat Defense (FTD).

ملاحظة: تدعم إصدارات برنامج FTD 7.4 والإصدارات الأحدث الواجهات المدمجة للإدارة والتشخيص، المعروفة أيضا بواجهة الإدارة المتقاربة (CMI).
يتم تمكين CMI بشكل افتراضي، ويمكن تعطيلها بواسطة المستخدمين. لمزيد من التفاصيل، راجع قسم "الواجهات المدمجة للإدارة والتشخيص" على https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/770/management-center-device-config-77/get-started-device-management.html.

تنطبق المعلومات التي يغطيها هذا المستند بشكل رئيسي على جدران الحماية باستخدام واجهة CMI المعطلة (واجهات التشخيص والإدارة غير المدمجة).

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

- FTD يجري تشغيله جهاز المكونات المادية ASA5508-X
- FTD يجري تشغيله جهاز المكونات المادية ASA5512-X
- FTD يجري تشغيله جهاز المكونات المادية FPR9300
- FMC يجري تشغيله بالإصدار 6.1.0 (التحديث 330)

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

والغرض من هذا المستند هو توضيح ما يلي:

- بنية واجهة إدارة FTD على أجهزة ASA5500-X
- واجهة إدارة FTD عند استخدام FDM
- واجهة إدارة FTD على سلسلة FP41xx/FP9300
- واجهة الإدارة على أجهزة جدار الحماية الآمنة من Cisco (1xxx، 12xx، 31xx، 42xx)
- سيناريوهات تكامل FTD/مركز إدارة Firepower (FMC)

التكوين

إصدارات البرامج لما بعد 7.4

اعتبارا من 7.4، يستخدم جدار الحماية بشكل افتراضي وضع واجهة الإدارة المتقاربة (CMI):

```
<#root>

FTD3100#

 show management-interface convergence


management-interface convergence
```

يتم إستخدام NAT كتنفيذ داخلي ل CMI:

- يتم تكوين عنوان IPv4 خاص داخلي (203.0.113.130) تلقائيا في مستوى البيانات ل IPv4.
- يتم تكوين عنوان IPv6 خاص داخلي (fd00:0:1:1::2) تلقائيا في مستوى البيانات ل IPv6.

```
<#root>

FTD3100#

show interface ip brief


Interface                  IP-Address      OK?         Method Status      Protocol
Internal-Data0/1           unassigned      YES         unset  up          up
Port-channel5              192.0.2.1       YES         unset  up          up
Ethernet1/1                unassigned      YES         unset  admin down  down
Ethernet1/2                unassigned      YES         unset  admin down  down
Ethernet1/5                unassigned      YES         unset  admin down  down
Ethernet1/6                unassigned      YES         unset  admin down  down
Ethernet1/7                unassigned      YES         unset  admin down  down
Ethernet1/8                unassigned      YES         unset  admin down  down
Ethernet1/9                unassigned      YES         unset  admin down  down
Ethernet1/10               unassigned      YES         unset  admin down  down
Ethernet1/11               unassigned      YES         unset  admin down  down
Ethernet1/12               unassigned      YES         unset  admin down  down
Ethernet1/13               unassigned      YES         unset  admin down  down
Ethernet1/14               unassigned      YES         unset  admin down  down
Ethernet1/15               unassigned      YES         unset  admin down  down
Ethernet1/16               unassigned      YES         unset  admin down  down
Internal-Control1/1        unassigned      YES         unset  up          up
Internal-Data1/1           169.254.1.1     YES         unset  up          up
Internal-Data1/2           unassigned      YES         unset  up          up

Management1/1              203.0.113.130   YES         unset  up          up  <----
```

لمزيد من التفاصيل ارجع إلى هذا المستند
https://www.cisco.com/c/en/us/support/docs/security/secure-firewall-threat-defense/222680-claifry-the-purpose-of-ip-address-203-0.html

ما قبل 7.4 الإصدارات

واجهة الإدارة على أجهزة ASA 5500-X

ملاحظة: تم الإعلان عن معظم أجهزة ASA 5500-X كنهاية العمر الافتراضي ونهاية البيع: https://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/eos-eol-notice-listing.html

---

عندما يتم تثبيت صورة FTD على جهاز ASA 55xx، يتم عرض واجهة الإدارة على أنها Management1/1. في الأجهزة 5512/15/25/45/55-X، تصبح هذه الواجهة Management0/0. من واجهة سطر الأوامر (CLI) الخاصة ب FTD يمكن التحقق من ذلك في إخراج show tech-support.

قم بالاتصال بوحدة تحكُّم FTD وتشغيل الأمر:

```
<#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
```

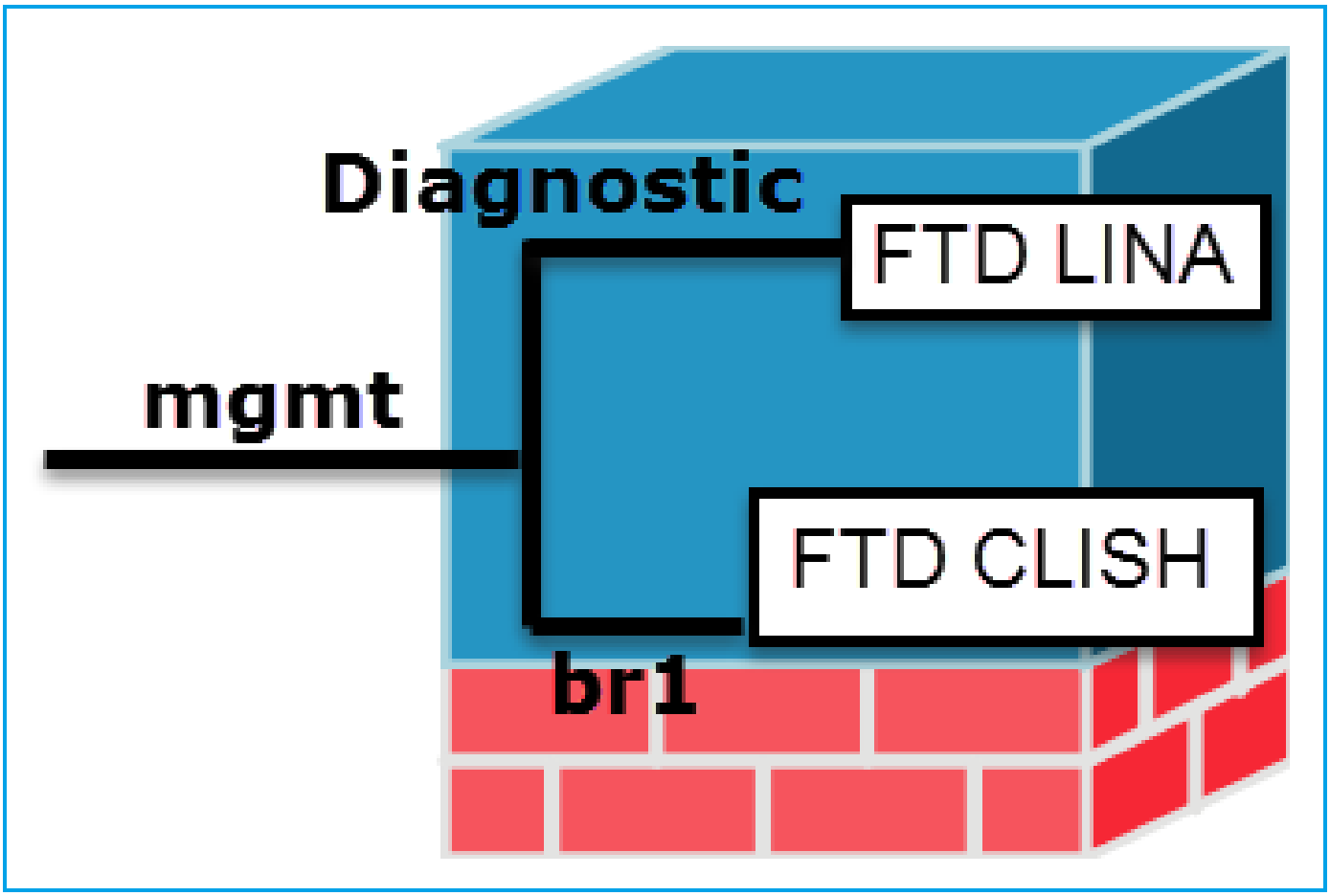
ASA5512-X:

```
<#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)
```

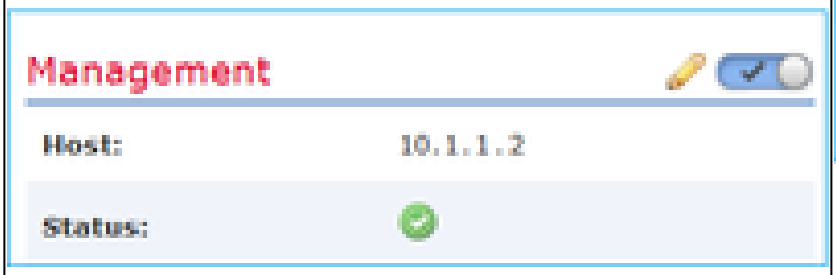
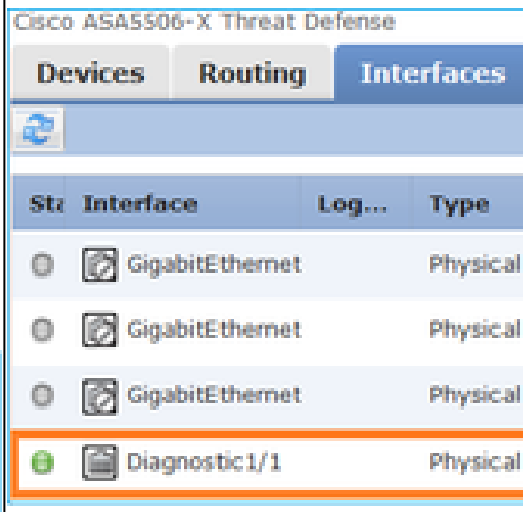
```
Compiled on Fri 18-Aug-16 15:08 PDT by builders
System image file is "disk0:/os.img"
Config file at boot was "startup-config"

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
```

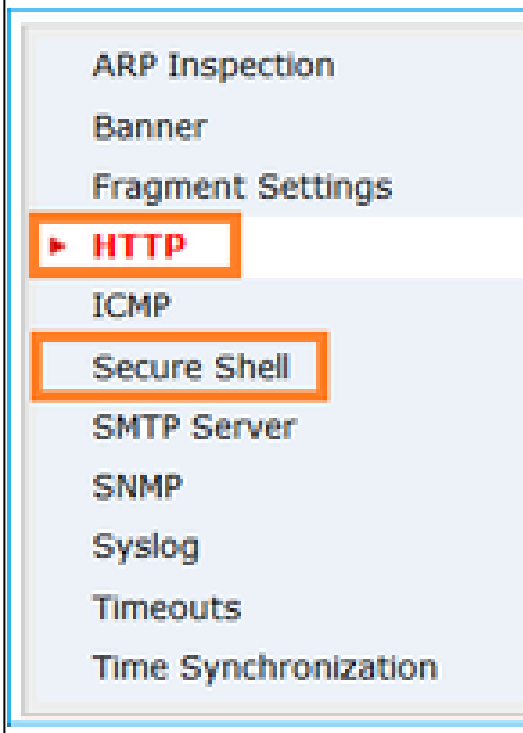
بنية واجهة الإدارة (إصدارات ما قبل 7.4)

تنقسم واجهة الإدارة إلى واجهتين منطقيتين: br1 (management0 على أجهزة FPR2100/4100/9300) والتشخيصية:



	الإدارة - br1/management0	الإدارة - التشخيصية
الغرض	• يتم استخدام هذه الواجهة لتعيين عنوان IP الخاص ببرنامج FTD والمُستخدم من أجل اتصالات FTD/FMC. • تقوم بإنهاء sftunnel بين FMC/FTD. • يتم استخدامها كمصدر لعمليات الدخول إلى النظام (syslogs) المستندة إلى القواعد. • توفر وصول SSH وHTTPS إلى برنامج FTD الداخلي.	• توفر وصولاً عن بُعد (على س المثال، SNMP) إلى محرك ASA • يتم استخدامها كمصدر لرسا عمليات الدخول إلى النظام (sy وAAA وSNMP على مستوى LI إلى ذلك.
إلزامي	هذا صحيح، حيث يتم استخدامها لاتصالات FTD/FMC (وتنتهي عندها sftunnel)	لا والا يُوصى بتكوينها. يُوصى باستخدام واجهة بيانات بدلاً من ذلك* (تحقّق الملاحظة أدناه)
التكوين	يتم تكوين هذه الواجهة أثناء تثبيت FTD (الإعداد). يمكنك تعديل إعدادات br1 لاحقًا على النحو التالي:	كما يمكن تكوين الواجهة من واجهة المستخدم الرسومية الخا

	<#root> > **configure network ipv4 manual 10.1.1.2 255.0.0.0 10.1.1.1** Setting IPv4 network configuration. Network settings changed. > الخطوة 2. قم بتحديث عنوان IP الخاص ببرنامج FTD على مركز إدارة Firepower (FMC).  	بمركز إدارة Firepower (FMC): انتقل إلى الأجهزة > إدارة الجهاز، حدّد الزر تحرير ثم انتقل إلى الواج 
تقييد الوصول	• ويمكن للمستخدم المسؤول فقط الاتصال بالواجهة الفرعية FTD BR1، بشكل افتراضي. • لتقييد SSH، يتحقق الوصول باستخدام واجهة سطر أوامر CLISH > configure ssh-access-list 10.0.0.0/8	إمكانية الوصول إلى واجهة التشخ يمكن التحكّم بها بواسطة FTD الأجهزة > إعدادات النظام الأساسي > طبقة الأمان و الأجهزة > إعدادات المنصة > HTTP على التوالي

<table>
<tr>
<td></td>
<td></td>
<td> 
</td>
</tr>
<tr>
<td>التحقق من الصحة</td>
<td>الطريقة الأولى - من واجهة سطر الأوامر (CLI) من FTD:

<#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]-----

الطريقة الثانية - من واجهة المستخدم الرسومية من FMC

الأجهزة > إدارة الجهاز > الجهاز > الإدارة</td>
<td>الطريقة الأولى - من واجهة سطر ال
(CLI) من LINA:

<#root>

firepower#

show interface ip brief

..
Management1/1 192.168.1.1 YES unse

firepower#

show run interface m1/1

!
interface Management1/1
management-only
nameif diagnostic
security-level 0
ip address 192.168.1.1 255.255.25

الطريقة الثانية - من واجهة المس
الرسومية من FMC

انتقل إلى الأجهزة > إدارة الجهاز،

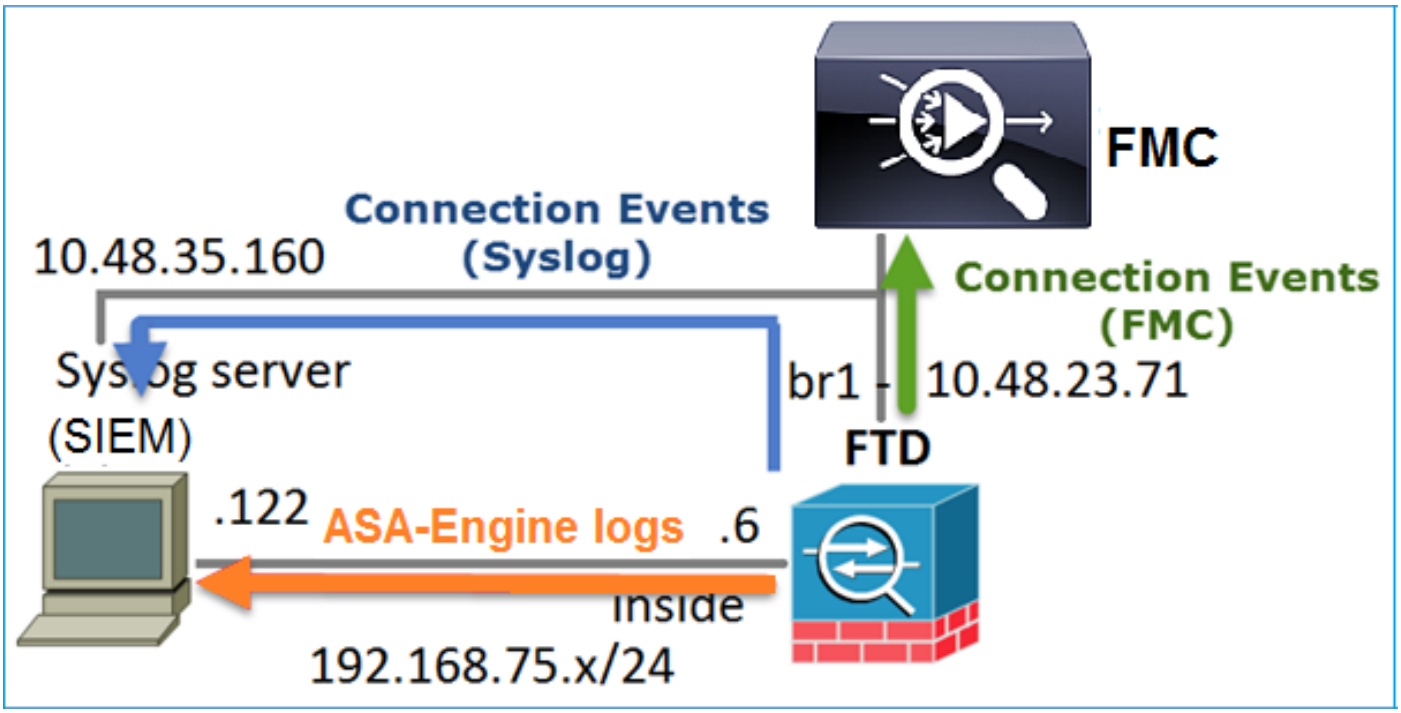
حدّد الزر تحرير ثم انتقل إلى الواج</td>
</tr>
</table>

تسجيل برنامج FTD

- عندما يقوم أحد المستخدمين بتكوين تسجيل FTD من إعدادات المنصة، يقوم FTD (كما هو الحال في ASA التقليدي) بإنشاء رسائل عمليات الدخول إلى النظام (Syslog) وإرسالها إلى خادم Syslog الخارجي (بما في ذلك "التشخيصية"). ومن الأمثلة على إحدى رسائل عمليات الدخول إلى النظام (syslog) التي يتم إنشاؤها في تلك الحالة:

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

- ومن ناحية أخرى، عند تمكين Rule-level logging الخاص بسياسة التحكّم في الوصول (ACP)، يُنشئ FTD هذه السجلات من خلال الواجهة المنطقية br1 كمصدر. يتم إنشاء السجلات من الواجهة الفرعية FTD br1:



إدارة FTD باستخدام FDM (الإدارة الداخلية)

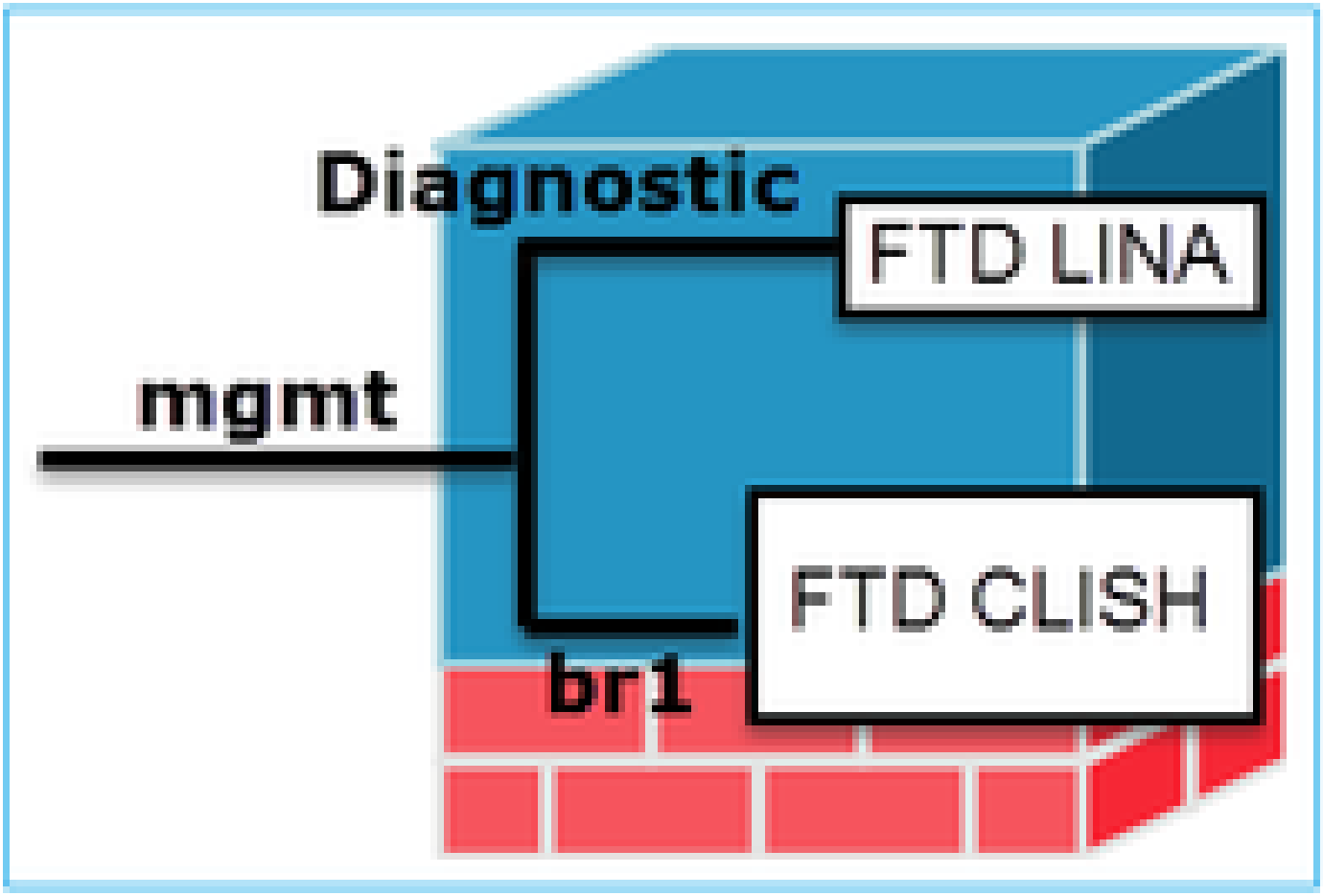
واعتباراً من الإصدار 6.1، يمكن إدارة FTD الذي يتم تثبيته على أجهزة ASA5500-X إما من خلال إدارة FMC (الإدارة الخارجية) أو من خلال إدارة FDM (الإدارة الداخلية).

الإخراج من FTD CLISH عندما تتم إدارة الجهاز بواسطة FDM:

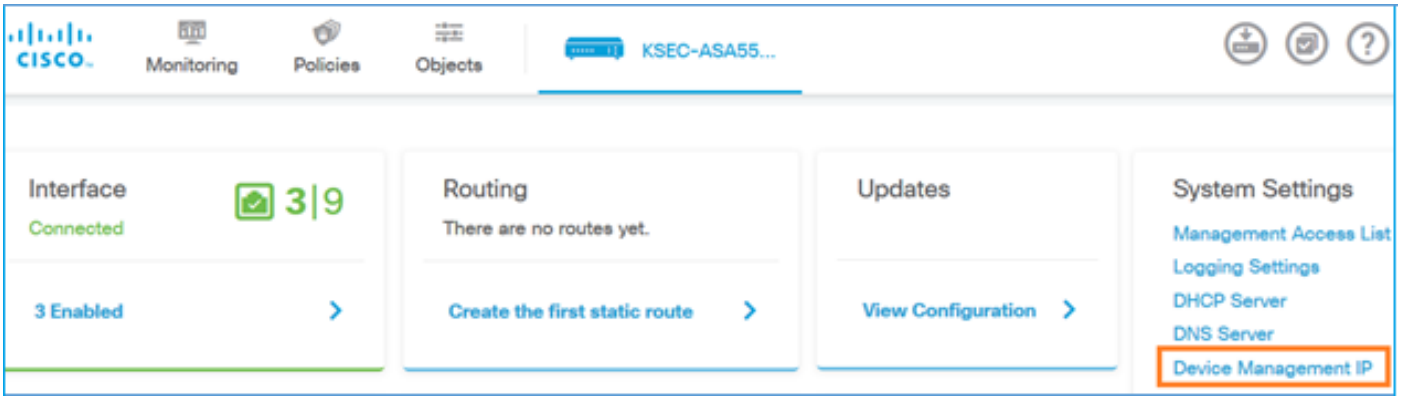
```
<#root>

>

show managers
```

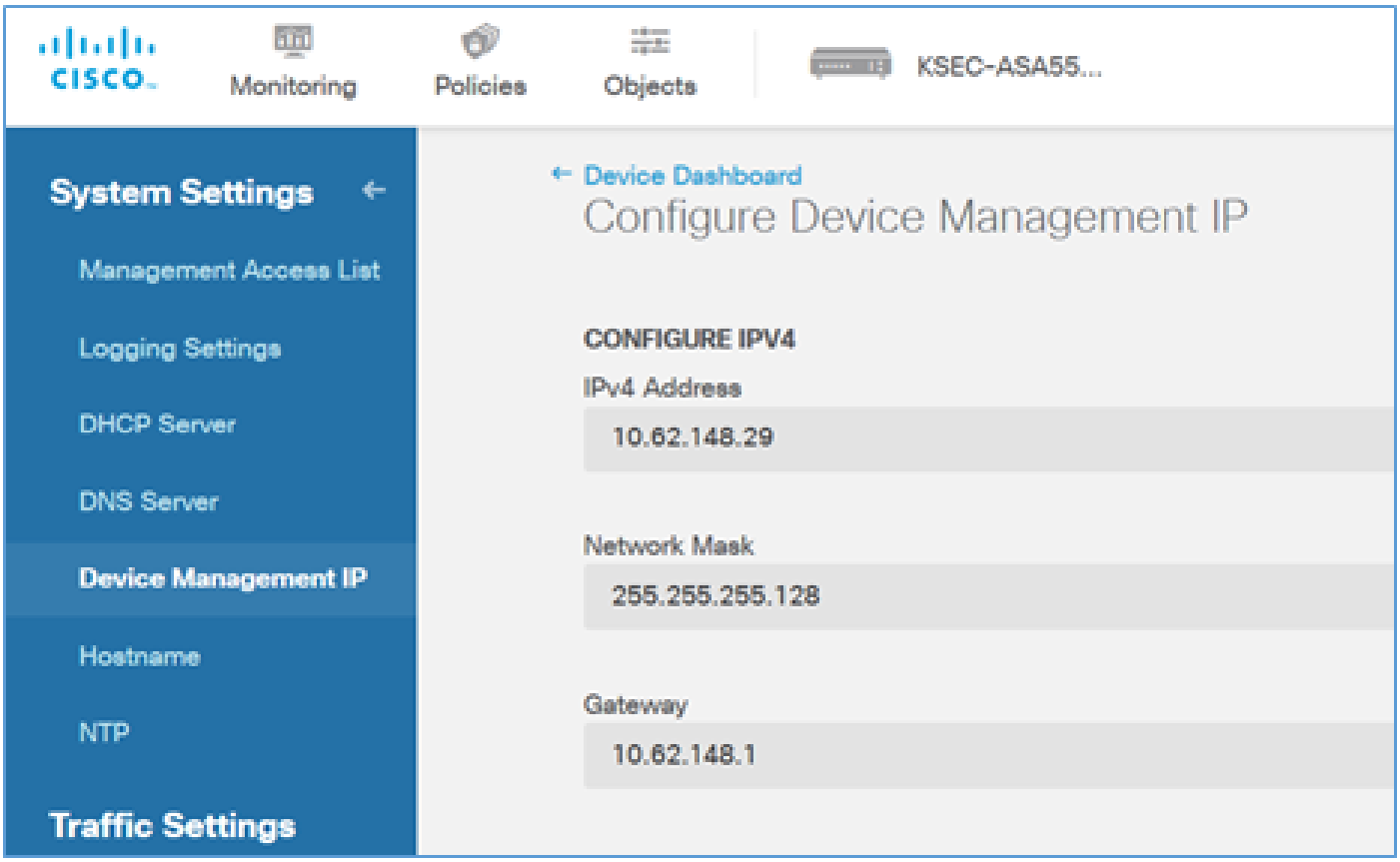
```
Managed locally.
>
```

يستخدم FDM الواجهة المنطقية br1. ويمكن تمثيل ذلك على النحو التالي:



من واجهة مستخدم FDM، يمكن الوصول إلى واجهة الإدارة من لوحة معلومات الجهاز > إعدادات النظام > عنوان IP الخاص بإدارة الجهاز:





واجهة الإدارة على أجهزة FTD Firepower Hardware

كما يمكن تثبيت FTD على أجهزة Firepower 2100 و4100 و9300. يقوم هيكل Firepower القاعدي بتشغيل نظام التشغيل (OS) الخاص به والذي يُسمى FXOS أثناء تثبيت FTD على وحدة/نصل.

جهاز FPR21xx

جهاز FPR41xx

جهاز FPR9300

على FPR4100/9300، هذه الواجهة مخصصة فقط لإدارة الهيكل القاعدي ولا يمكن استخدامها/مشاركتها مع برنامج FTD الذي يعمل داخل وحدة FP. بالنسبة إلى وحدة FTD، قم بتخصيص واجهة بيانات منفصلة خاصة بإدارة FTD.

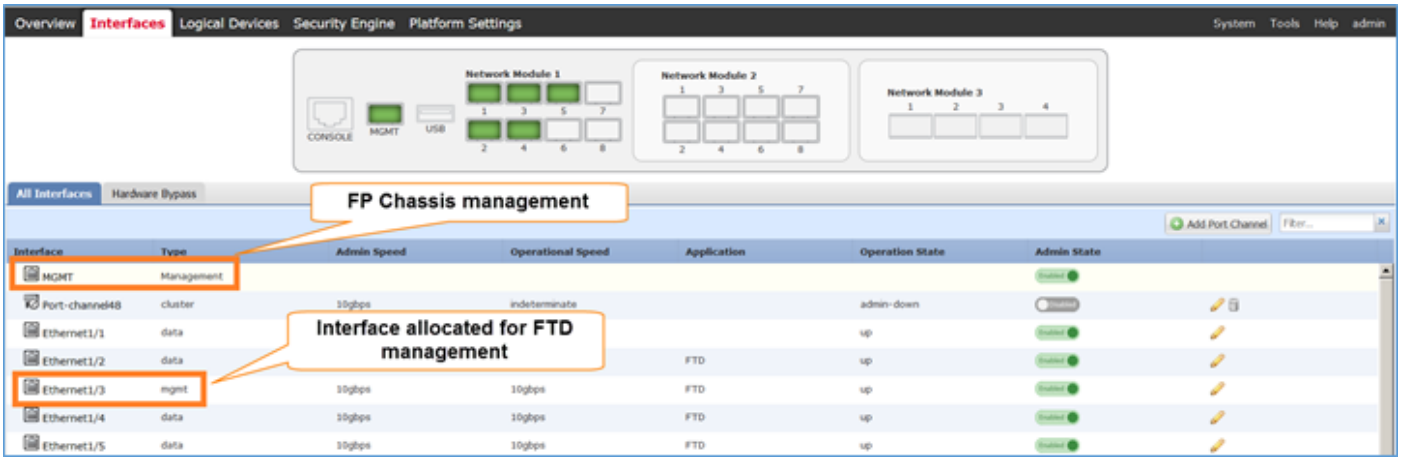
على FPR2100، تتم مشاركة هذه الواجهة بين الهيكل القاعدي (FXOS) والجهاز المنطقي FTD:

```
<#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 (
```

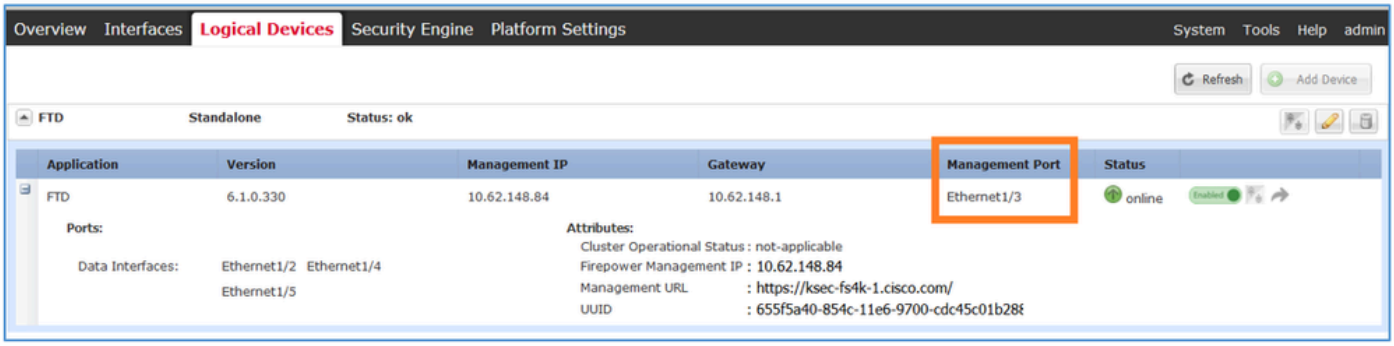
FX-OS

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

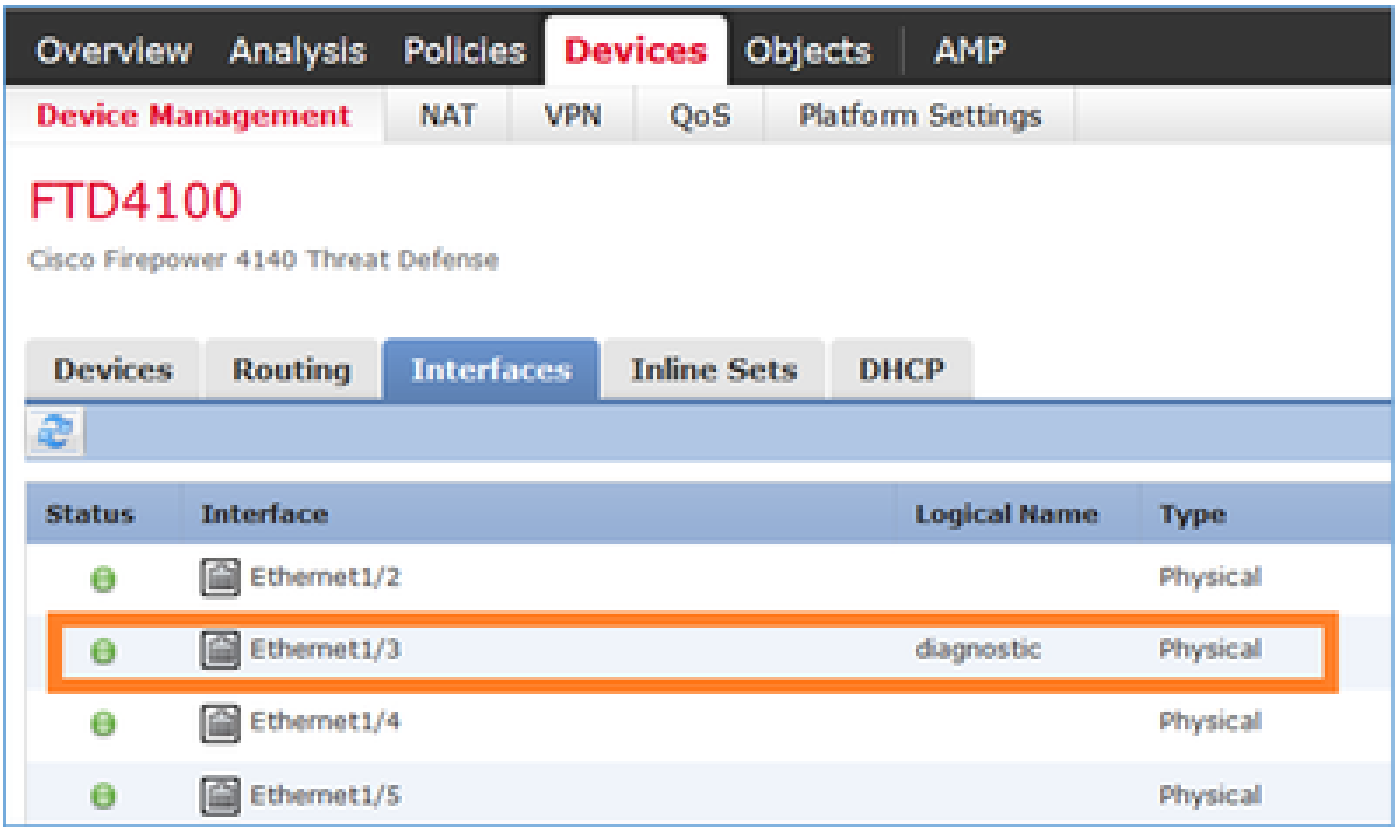
لقطة الشاشة هذه مأخوذة من واجهة مستخدم مدير هيكل Firepower القاعدي (FCM) على FPR4100 حيث يتم تخصيص واجهة منفصلة لإدارة FTD. في هذا المثال، يتم اختيار Ethernet1/3 كواجهة إدارة FTD: p1



كما يمكن ملاحظة ذلك من علامة تبويب الأجهزة المنطقية:p2



تظهر الواجهة على مركز إدارة Firepower (FMC) على أنها تشخيصية: p3



التحقّق من واجهة سطر الأوامر (CLI)

<#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
```

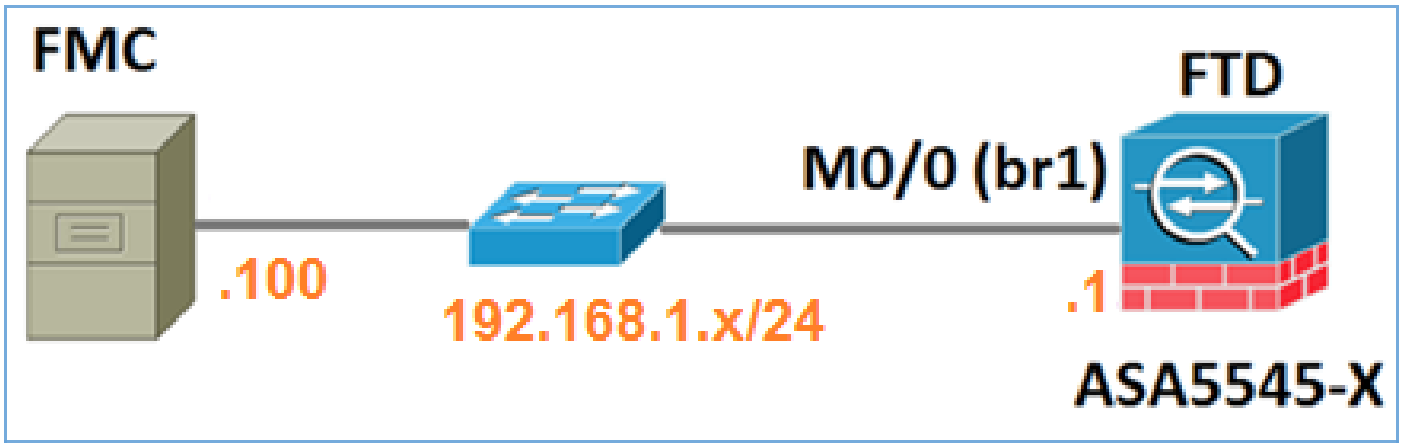
```
        5 minute input rate 2 pkts/sec,  112 bytes/sec
        5 minute output rate 0 pkts/sec,  0 bytes/sec
        5 minute drop rate, 1 pkts/sec
          Management-only interface. Blocked 0 through-the-device packets

… output omitted …
>
```

دمج FTD مع مركز إدارة Firepower (FMC) - سيناريوهات الإدارة

فيما يلي توفر بعض من خيارات النشر التي تتيح إدارة FTD الذي يتم تشغيله على أجهزة ASA5500-X من FMC.

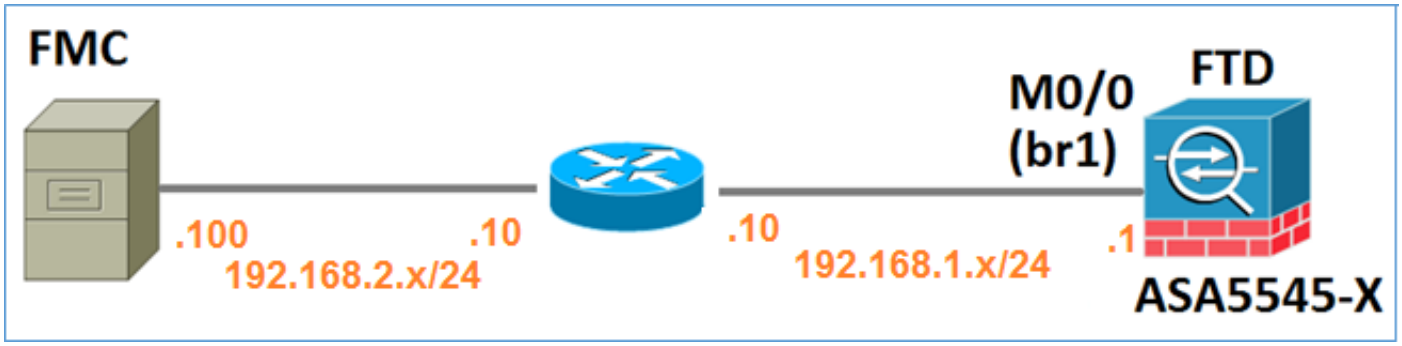
السيناريو الأول. تواجد كل من FTD وFMC على الشبكة الفرعية نفسها.

وهذا هي أبسط عملية نشر. كما هو مُوضح في الشكل، يتوفر FMC على الشبكة الفرعية نفسها الخاصة بواجهة FTD br1:



السيناريو الثاني. يتوفر كل من FTD وFMC على شبكات فرعية مختلفة. لا يمر مستوى التحكّم من خلال FTD.

في هذا النشر، يجب أن يكون لدى FTD مسار نحو FMC والعكس صحيح. في FTD، الخطوة التالية هي جهاز من الطبقة الثالثة (موجّه):



معلومات ذات صلة

- الدعم التقني والمستندات - Cisco Systems
- https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/770/management-center-device-config-77/get-started-device-management.html
- https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/roadmap/management-center-new-features-by-release.html#new-features-fmc-740

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).